

New Features Guide

FortiOS 7.0.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



November 01, 2021

FortiOS 7.0.0 New Features Guide

01-700-676234-20211101

TABLE OF CONTENTS

Change Log	9
GUI	11
Dashboards and widgets	11
FortiView application bandwidth widget	11
SSL-VPN and IPsec monitor improvements	12
DNS status widget 7.0.2	16
General usability enhancements	16
New themes and CLI console enhancements	17
Add options for API Preview, Edit in CLI, and References	21
GUI usability enhancements	25
Seven-day rolling counter for policy hit counters	28
FortiGate administrator log in using FortiCloud single sign-on	30
Navigation menu updates	31
UX improvements for objects	32
Interface migration wizard	34
Add GUI-based global search 7.0.1	38
Export firewall policy list to CSV and JSON formats 7.0.2	39
GUI support for configuration save mode 7.0.2	39
Security Fabric	42
Fabric settings	42
Security Fabric support in multi-VDOM environments	42
Enhance Security Fabric configuration for FortiSandbox Cloud	50
FortiWeb integration	51
Show detailed user information about clients connected over a VPN through EMS	53
FortiDeceptor as a Security Fabric device	55
Add FortiAI as a Security Fabric device	59
Improve communication performance between EMS and FortiGate with WebSockets	63
Simplify EMS pairing with Security Fabric so one approval is needed for all devices	65
FortiTester as a Security Fabric device 7.0.1	66
Simplify Fabric approval workflow for FortiAnalyzer 7.0.1	69
Allow deep inspection certificates to be synchronized to EMS and distributed to FortiClient 7.0.1	71
Asset Identity Center page 7.0.2	78
Fabric Management page 7.0.2	80
External connectors	82
Threat feed connectors per VDOM	82
Nutanix connector	86
STIX format for external threat feeds 7.0.2	88
Automation stitches	89
Automation workflow improvements	90
Microsoft Teams Notification action	99
Replacement messages for email alerts	104
Security ratings	109
Security Rating overlays	109
Add test to check for two-factor authentication	112

Add test to check for activated FortiCloud services	113
Add tests for high priority vulnerabilities 7.0.1	114
Network	117
SD-WAN	117
Usability enhancements to SD-WAN Network Monitor service	117
Hold down time to support SD-WAN service strategies	119
Passive WAN health measurement	120
SD-WAN passive health check configurable on GUI 7.0.1	121
ECMP support for the longest match in SD-WAN rule matching 7.0.1	123
Override quality comparisons in SD-WAN longest match rule matching 7.0.1	125
Specify an SD-WAN zone in static routes and SD-WAN rules 7.0.1	128
Display ADVPN shortcut information in the GUI 7.0.1	132
Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1	133
Interface based QoS on individual child tunnels based on speed test results 7.0.1	140
Passive health-check measurement by internet service and application 7.0.2	143
Adaptive Forward Error Correction 7.0.2	147
General	151
Summarize source IP usage on the Local Out Routing page	151
Add option to select source interface and address for Telnet and SSH	156
ECMP routes for recursive BGP next hop resolution	157
BGP next hop recursive resolution using other BGP routes	158
Add SNMP OIDs for shaping-related statistics	159
PRP handling in NAT mode with virtual wire pair	161
NetFlow on FortiExtender and tunnel interfaces	162
Integration with carrier CPE management tools	166
Use file filter rules in sniffer policy	169
Explicit mode with DoT and DoH	172
GUI advanced routing options for BGP	176
GUI page for OSPF settings	178
GUI routing monitor for BGP and OSPF	180
OSPF HMAC-SHA authentication 7.0.1	182
BGP conditional advertisement for IPv6 7.0.1	184
Enable or disable updating policy routes when link health monitor fails 7.0.1	186
Add weight setting on each link health monitor server 7.0.1	189
Enhanced hashing for LAG member selection 7.0.1	192
Add GPS coordinates to REST API monitor output for FortiExtender and LTE modems 7.0.2	193
BGP error handling per RFC 7606 7.0.2	197
Configure IPAM locally on the FortiGate 7.0.2	199
IPv6	206
Configuring IPv6 multicast policies in the GUI	206
GUI support for configuring IPv6	207
FortiGate as an IPv6 DDNS client for generic DDNS	212
FortiGate as an IPv6 DDNS client for FortiGuard DDNS	212
Allow backup and restore commands to use IPv6 addresses	213
VRF support for IPv6 7.0.1	214
IPv6 tunnel inherits MTU based on physical interface 7.0.2	218
Web proxy	220

Explicit proxy authentication over HTTPS	220
Selectively forward web requests to a transparent web proxy	222
mTLS client certificate authentication 7.0.1	225
WAN optimization SSL proxy chaining 7.0.1	230
System	239
General	239
Allow administrators to define password policy with minimum character change	239
Enhance host protection engine	241
ACME certificate support	242
SFTP configuration backup 7.0.1	247
Promote FortiCare registration 7.0.1	247
Add monitoring API to retrieve LTE modem statistics from 3G and 4G FortiGates 7.0.1	249
Add USB support for FortiExplorer Android 7.0.1	251
Warnings for unsigned firmware 7.0.2	253
Enabling individual ciphers in the SSH administrative access protocol 7.0.2	255
ECDSA in SSH administrative access 7.0.2	255
Clear multiple sessions with REST API 7.0.2	257
Disable weak ciphers in the HTTPS protocol 7.0.2	258
Extend dedicated management CPU feature to 1U and desktop models 7.0.2	260
High availability	261
FGSP four-member session synchronization and redundancy	261
Layer 3 unicast standalone configuration synchronization between peers	266
Improved link monitoring and HA failover time	269
HA monitor shows tables that are out of synchronization	271
HA failover due to memory utilization	271
IKE monitor for FGSP	273
Resume IPS scanning of ICCP traffic after HA failover 7.0.1	275
Extended HA VMAC address range 7.0.2	277
FortiGuard	278
Immediate download update option	278
Add option to automatically update schedule frequency	279
Update OUI files from FortiGuard	279
Use only EU servers for FortiGuard updates 7.0.2	280
Policy and Objects	282
Zero Trust Network Access	282
Zero Trust Network Access introduction	282
Basic ZTNA configuration	285
Establish device identity and trust context with FortiClient EMS	293
SSL certificate based authentication	297
ZTNA configuration examples	299
Migrating from SSL VPN to ZTNA HTTPS access proxy	346
ZTNA troubleshooting and debugging	349
ZTNA logging enhancements 7.0.1	354
Logical AND for ZTNA tag matching 7.0.2	357
Implicitly generate a firewall policy for a ZTNA rule 7.0.2	361
Posture check verification for active ZTNA proxy session 7.0.2	366
GUI support for multiple ZTNA features 7.0.2	372

NGFW	375
Filters for application control groups in NGFW mode	375
Policies	378
DNS health check monitor for server load balancing	378
Carrier-grade NAT	379
Allow multiple virtual wire pairs in a virtual wire pair policy	382
Simplify NAT46 and NAT64 policy and routing configurations 7.0.1	384
Cisco Security Group Tag as policy matching criteria 7.0.1	395
Objects	397
Record central NAT and DNAT hit count	397
MAC address wildcard in firewall address	398
Security profiles	400
Antivirus	400
Stream-based antivirus scan in proxy mode for FTP, SFTP, and SCP	400
Configure threat feed and outbreak prevention without AV engine scan	402
AI-based malware detection	404
Malware threat feed from EMS	406
FortiAI inline blocking and integration with an AV profile 7.0.1	408
Application control	415
Application signature dissector for DNP3	415
Web filter	416
FortiGuard web filter categories to block child sexual abuse and terrorism	416
Enhance web filter antiphishing profile	418
Add categories for URL shortening, crypto mining, and potentially unwanted programs 7.0.2	421
IPS	423
Highlight on hold IPS signatures	423
Extend SCTP filtering capabilities 7.0.1	424
SSL/SSH inspection	426
HTTP/2 support in proxy mode SSL inspection	427
Define multiple certificates in an SSL profile in replace mode	428
Others	430
Support secure ICAP clients	430
Add TCP connection pool for connections to ICAP server	431
Improve WAD traffic dispatcher	432
Video filtering	432
DNS filter handled by IPS engine in flow mode	435
DNS inspection with DoT and DoH	436
Flow-based SIP inspection	439
Scanning MSRP traffic 7.0.2	441
VPN	446
IPsec and SSL VPN	446
Configurable IKE port	446
Packet duplication for dial-up IPsec tunnels	449
IPsec global IKE embryonic limit	453
FortiGate as SSL VPN Client	454
Dual stack IPv4 and IPv6 support for SSL VPN	463
Disable the clipboard in SSL VPN web mode RDP connections 7.0.1	473

Use SSL VPN interfaces in zones 7.0.1	478
SSL VPN and IPsec VPN IP address assignments 7.0.1	482
Dedicated tunnel ID for IPsec tunnels 7.0.1	487
User and authentication	503
Authentication	503
Integrate user information from EMS connector and Exchange connector in the user store	503
SAML authentication in a proxy policy	506
Improve FortiToken Cloud visibility 7.0.1	510
Use a browser as an external user-agent for SAML authentication in an SSL VPN connection 7.0.1	511
Add configurable FSSO timeout when connection to collector agent fails 7.0.1	515
Track users in each Active Directory LDAP group 7.0.2	517
Configuring SAML SSO in the GUI 7.0.2	520
Secure access	527
Wireless	527
Configure Agile Multiband Operation	527
Captive portal authentication when bridged via software switch	532
DHCP address enforcement	534
Increase maximum number of supported VLANs	535
Add RADIUS MAC delimiter options	536
Radio transmit power range in dBm	538
Station mode on FortiAP radios to initiate tests against other APs	540
AP operating temperature 7.0.1	542
Allow indoor and outdoor flags to be overridden 7.0.1	542
DNS configuration for local standalone NAT VAPs 7.0.1	544
Backward compatibility with FortiAP models that uses weaker ciphers 7.0.1	546
Disable console access on managed FortiAP devices 7.0.1	548
Captive portal authentication in service assurance management (SAM) mode 7.0.1	550
Provide LBS station information with REST API 7.0.2	553
Allow users to select individual security profiles in bridged SSID 7.0.2	557
Wireless client MAC authentication and MPSK returned through RADIUS 7.0.2	561
FQDN for FortiPresence server IP address in FortiAP profiles 7.0.2	565
Wi-Fi Alliance Hotspot 2.0 Release 3 support 7.0.2	566
Automatic BSS coloring 7.0.2	568
Configure 802.11ax MCS rates 7.0.2	570
Switch controller	571
Forward error correction settings on switch ports	571
Cancel pending or downloading FortiSwitch upgrades	572
Automatic provisioning of FortiSwitch firmware upon authorization	574
Additional FortiSwitch recommendations in Security Rating	576
PoE pre-standard detection disabled by default	577
Cloud icon indicates that the FortiSwitch unit is managed over layer 3	577
GUI support for viewing and configuring shared FortiSwitch ports	578
Ability to re-order FortiSwitch units in the Topology view 7.0.1	579
Support of the DHCP server access list 7.0.1	581
SNMP OIDs added for switch statistics and port status 7.0.1	583
Display port properties of managed FortiSwitch units 7.0.1	584

IGMP-snooping querier and per-VLAN IGMP-snooping proxy configuration 7.0.2	584
Managing DSL transceivers (FN-TRAN-DSL) 7.0.2	586
NAC	588
FortiSwitch NAC VLANs widget	588
Use wildcards in a MAC address in a NAC policy	590
FortiGate NAC engine optimization	592
Wireless NAC support	593
Dynamic port profiles for FortiSwitch ports	598
GUI updates for the switch controller	601
Support dynamic firewall addresses in NAC policies 7.0.1	602
NAC LAN segments 7.0.1	605
Specify FortiSwitch groups in NAC policies 7.0.2	612
FortiExtender	614
Introduce LAN extension mode for FortiExtender 7.0.2	614
Using the backhaul IP when the FortiGate access controller is behind NAT 7.0.2	622
Bandwidth limits on the FortiExtender Thin Edge 7.0.2	629
Log and report	631
Logging	631
Add logs for the execution of CLI commands	631
Logging IP address threat feeds in sniffer mode	632
Enhance TLS logging 7.0.1	633
Generate unique user name for anonymized logs 7.0.2	635
Support TACACS+ accounting 7.0.2	639
Add dstuser field to UTM logs 7.0.2	641
Cloud	645
Public and private cloud	645
Collect only node IP addresses with Kubernetes SDN connectors	645
Unicast HA on IBM VPC Cloud	649
Update AliCloud SDN connector to support Kubernetes filters	656
Synchronize wildcard FQDN resolved addresses to autoscale peers	659
Obtain FortiCare-generated license and certificates for GCP PAYG instances	661
FortiGate VM on KVM running ARM processors 7.0.1	663
Support MIME multipart bootstrapping on KVM with config drive 7.0.1	667
Support GCP gVNIC interface 7.0.1	670
FIPS cipher mode for OCI and GCP FortiGate VMs 7.0.1	671
SD-WAN transit routing with Google Network Connectivity Center 7.0.1	672
Support C5d instance type for AWS Outposts 7.0.1	672
FGSP session sync on FortiGate-VMs on Azure with autoscaling enabled 7.0.1	673
Flex-VM token and bootstrap configuration file fields in custom OVF template 7.0.2	688
Subscription-based VDOM license for FortiGate-VM S-series 7.0.2	690
FortiOS Carrier	693

Change Log

Date	Change Description
2021-11-01	Updated Configure IPAM locally on the FortiGate 7.0.2 on page 199.
2021-10-27	Added Fabric Management page 7.0.2 on page 80.
2021-10-21	Added Adaptive Forward Error Correction 7.0.2 on page 147.
2021-10-20	Initial release of FortiOS 7.0.2.
2021-10-05	Added Support C5d instance type for AWS Outposts 7.0.1 on page 672.
2021-10-01	Added Dedicated tunnel ID for IPsec tunnels 7.0.1 on page 487.
2021-08-25	Added Add USB support for FortiExplorer Android 7.0.1 on page 251.
2021-08-23	Added FGSP session sync on FortiGate-VMs on Azure with autoscaling enabled 7.0.1 on page 673.
2021-08-20	Updated IPsec global IKE embryonic limit on page 453.
2021-08-13	Added ZTNA SSH access proxy example 7.0.1 on page 338.
2021-08-10	Added Allow deep inspection certificates to be synchronized to EMS and distributed to FortiClient 7.0.1 on page 71 and Use a browser as an external user-agent for SAML authentication in an SSL VPN connection 7.0.1 on page 511.
2021-08-09	Updated Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1 on page 133.
2021-07-22	Added SSL VPN and IPsec VPN IP address assignments 7.0.1 on page 482.
2021-07-21	Added Captive portal authentication in service assurance management (SAM) mode 7.0.1 on page 550.
2021-07-20	Added ZTNA IPv6 examples 7.0.1 on page 332.
2021-07-19	Updated Video filtering on page 432.
2021-07-16	Updated Flow-based SIP inspection on page 439.
2021-07-15	Initial release of FortiOS 7.0.1.
2021-06-17	Added Obtain FortiCare-generated license and certificates for GCP PAYG instances on page 661.
2021-06-14	Added Synchronize wildcard FQDN resolved addresses to autoscale peers on page 659.
2021-06-08	Added Highlight on hold IPS signatures on page 423.
2021-05-13	Added GUI usability enhancements on page 25.
2021-05-11	Updated Unicast HA on IBM VPC Cloud on page 649.
2021-05-10	Added Interface migration wizard on page 34.

Date	Change Description
2021-05-05	Added Dual stack IPv4 and IPv6 support for SSL VPN on page 463 .
2021-05-03	Added Migrating from SSL VPN to ZTNA HTTPS access proxy on page 346 .
2021-04-30	Added GUI advanced routing options for BGP on page 176 , GUI routing monitor for BGP and OSPF on page 180 , and ZTNA HTTPS access proxy with basic authentication example on page 308 .
2021-04-21	Added IKE monitor for FGSP on page 273 .
2021-04-09	Added FortiGate as SSL VPN Client on page 454 and Immediate download update option on page 278 .
2021-04-08	Added Dynamic port profiles for FortiSwitch ports on page 598 and GUI updates for the switch controller on page 601 .
2021-04-06	Added GUI page for OSPF settings on page 178 , Add test to check for activated FortiCloud services on page 113 , Station mode on FortiAP radios to initiate tests against other APs on page 540 , and FortiGate administrator log in using FortiCloud single sign-on on page 30 .
2021-04-05	Added New themes and CLI console enhancements on page 17 , Improve communication performance between EMS and FortiGate with WebSockets on page 63 , Simplify EMS pairing with Security Fabric so one approval is needed for all devices on page 65 , Add test to check for two-factor authentication on page 112 , Summarize source IP usage on the Local Out Routing page on page 151 , and Improved link monitoring and HA failover time on page 269 .
2021-04-01	Added Zero Trust Network Access introduction on page 282 , Establish device identity and trust context with FortiClient EMS on page 293 , SSL certificate based authentication on page 297 , ZTNA HTTPS access proxy example on page 299 , ZTNA TCP forwarding access proxy example on page 314 , ZTNA proxy access with SAML authentication example on page 317 , ZTNA IP MAC filtering example on page 322 , and ZTNA troubleshooting and debugging on page 349 .
2021-03-31	Added Basic ZTNA configuration on page 285 , FortiWeb integration on page 51 , and SSL-VPN and IPsec monitor improvements on page 12 .
2021-03-30	Initial release.

GUI

This section includes new features related to the FortiOS GUI:

- [Dashboards and widgets on page 11](#)
- [General usability enhancements on page 16](#)

Dashboards and widgets

This section includes new features related to dashboards and widgets:

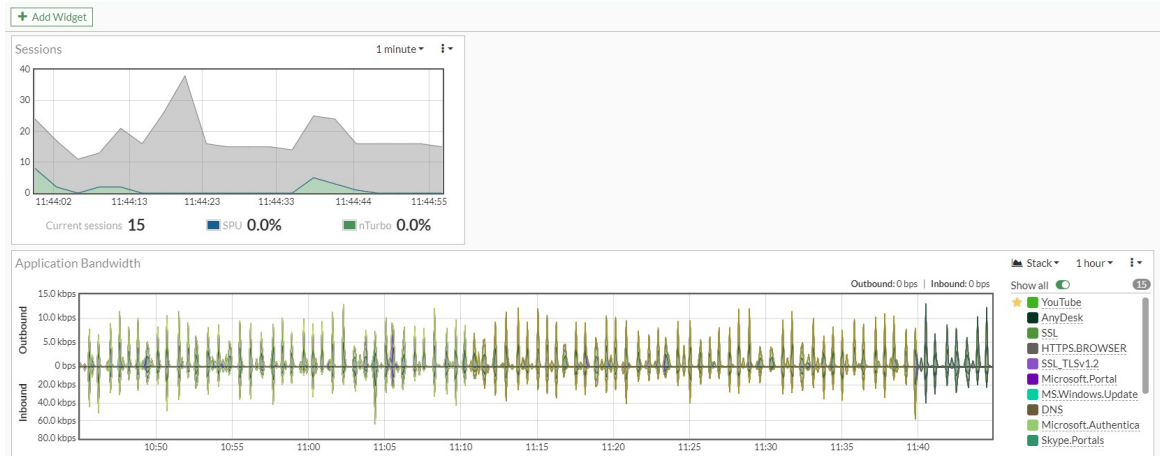
- [SSL-VPN and IPsec monitor improvements on page 12](#)
- [FortiView application bandwidth widget on page 11](#)
- [DNS status widget 7.0.2 on page 16](#)

FortiView application bandwidth widget

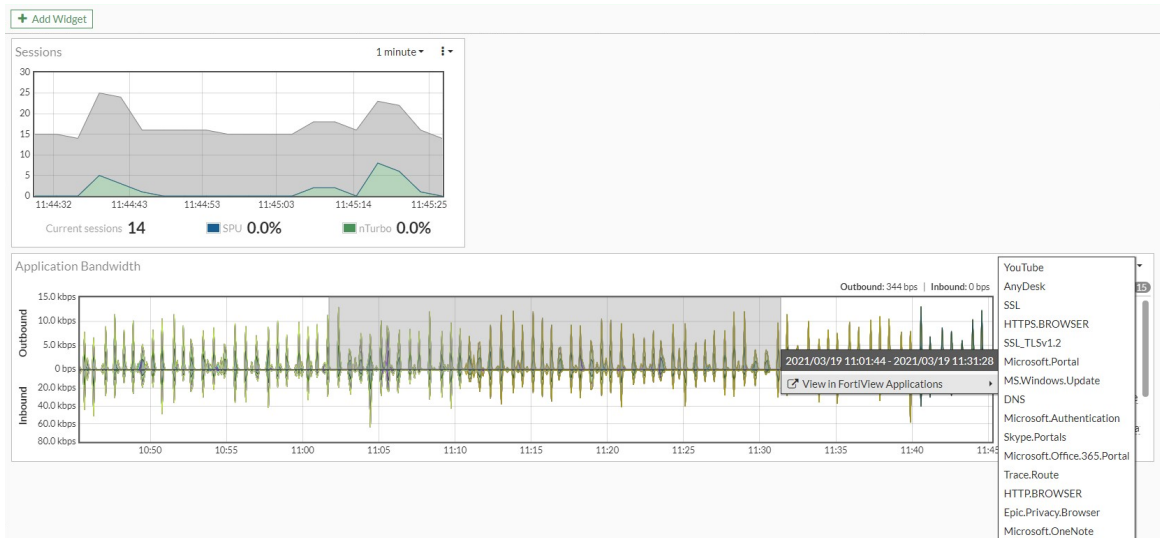
The *FortiView Application Bandwidth* widget can be added to a dashboard to display bandwidth utilization for the top 50 applications. A firewall policy must have an application profile configured for this widget to capture information. Note that when using multi-VDOM mode, this widget is available in the global scope.

To add the application bandwidth widget in the GUI:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *FortiView* section, click the + beside *FortiView Application Bandwidth*.
3. Click *Add Widget* and click *Close*. The *FortiView Application Bandwidth* widget is displayed in the dashboard. The *Outbound* and *Inbound* sections on the chart show real-time bandwidth for all signatures. The data can be filtered by 1 hour, 24 hours, or a week.
4. Click the star icon to mark favorite signatures, which will always appear at the top of the list.
5. Optionally, to customize the signatures in the graph, deselect *Show all* and enable individual signatures. Favorite signatures appear in the graph by default.



6. In non-VDOM mode, select a time frame in the chart, then click *View in FortiView Application* and select an application to view the detailed drilldown on the corresponding FortiView page.



To enable application bandwidth tracking in the CLI:

```
config system settings
    set application-bandwidth-tracking enable
end
```

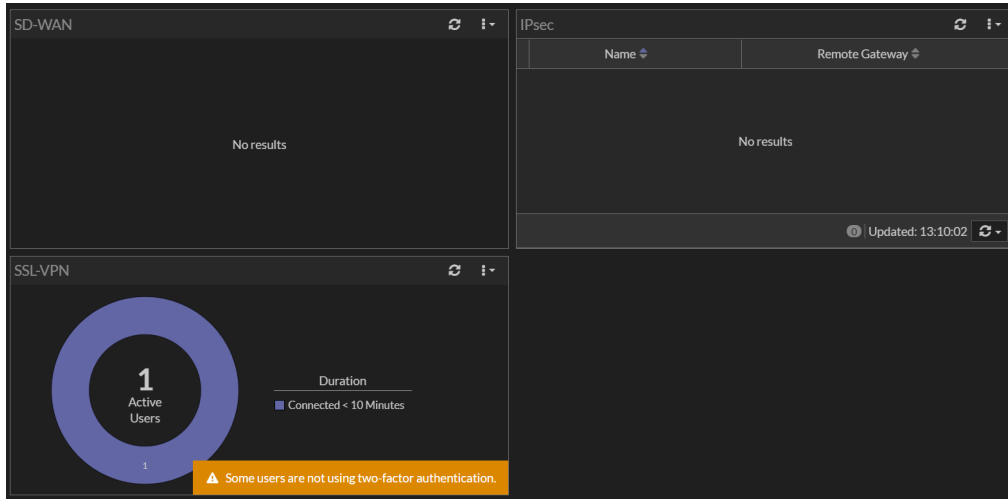
SSL-VPN and IPsec monitor improvements

The *SSL-VPN* monitor now includes *Duration* and *Connection Summary* charts. The *IPsec* monitor displays information about Phase 1 and Phase 2 tunnels. Both monitors also identify users who have not enabled two-factor authentication.

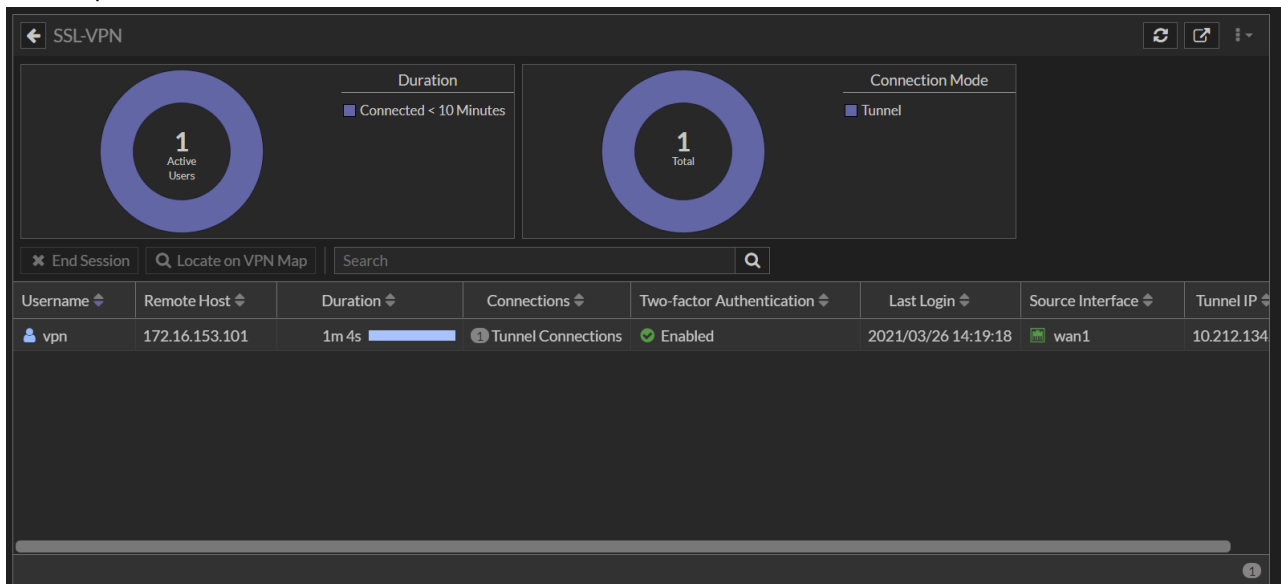
SSL-VPN monitor

To view the SSL-VPN monitor:

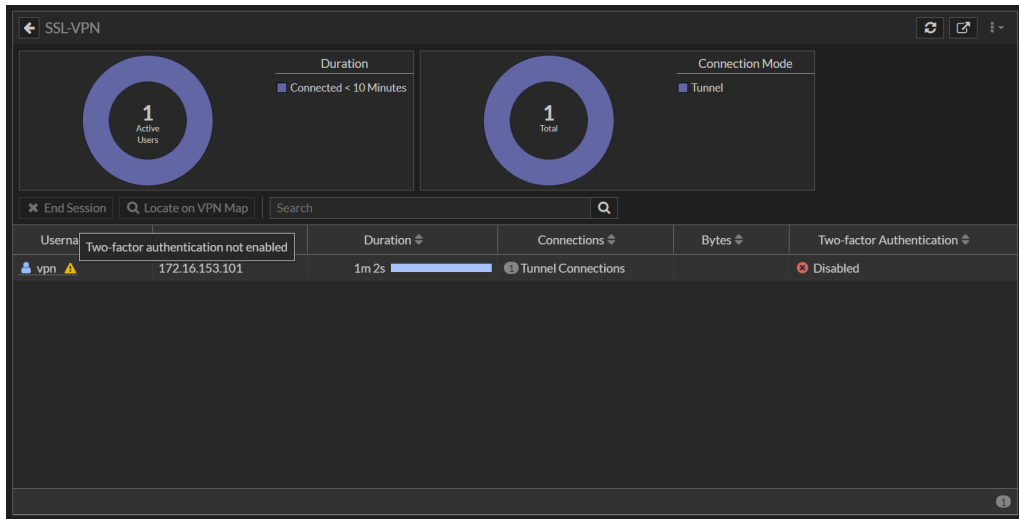
1. Go to *Dashboard > Network*. The *SSL-VPN* overview widget is displayed.
A warning appears when at least one VPN user has not enabled two-factor authentication.



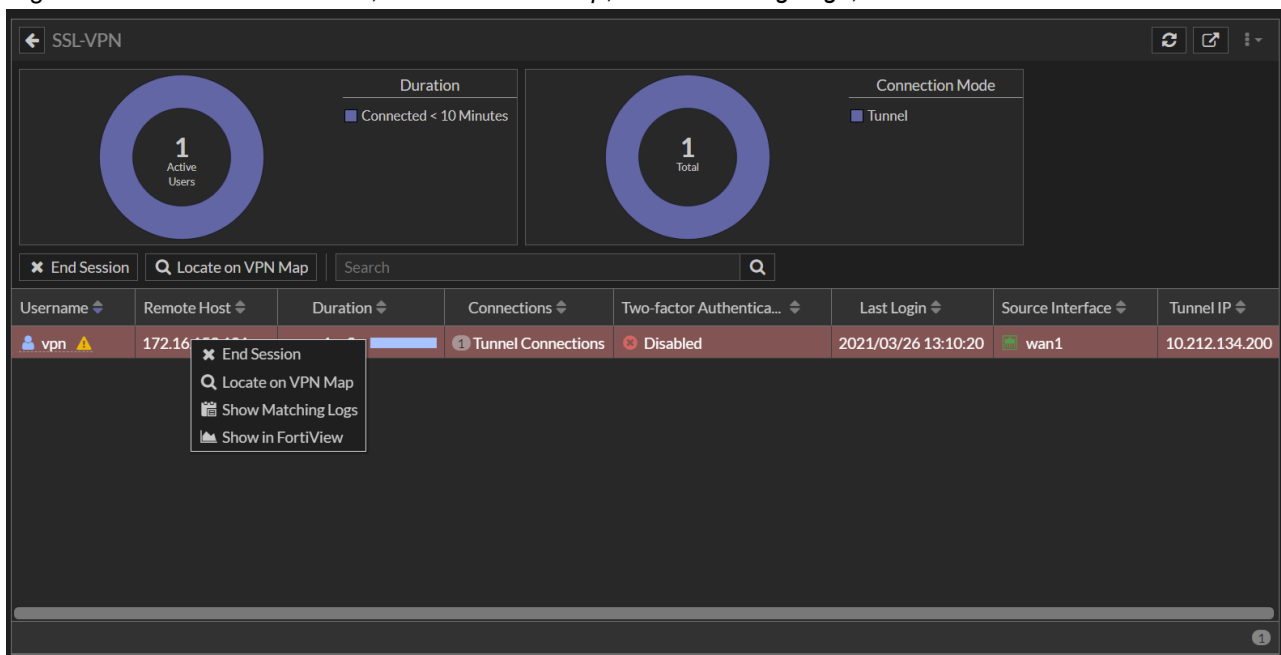
2. Hover over the widget and click *Expand to full screen*. The *Duration* and *Connection Summary* charts are displayed at the top of the monitor.



A warning appears in the *Username* column when a user has not enabled two-factor authentication.



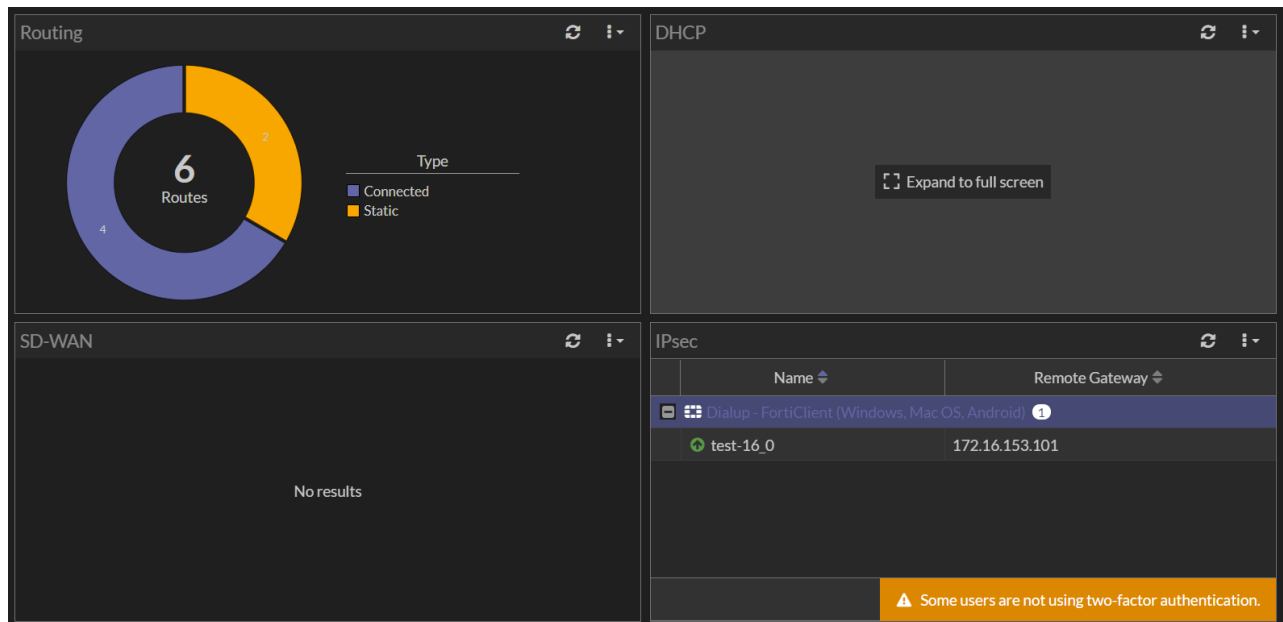
3. Right-click a user to *End Session*, *Locate on VPN Map*, *Show Matching Logs*, and *Show in FortiView*.



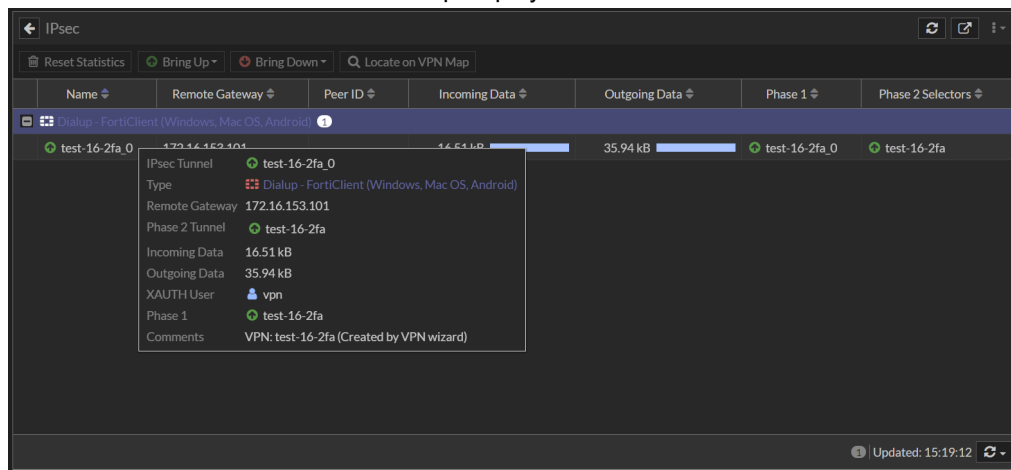
IPSec monitor

To view the IPSec Monitor:

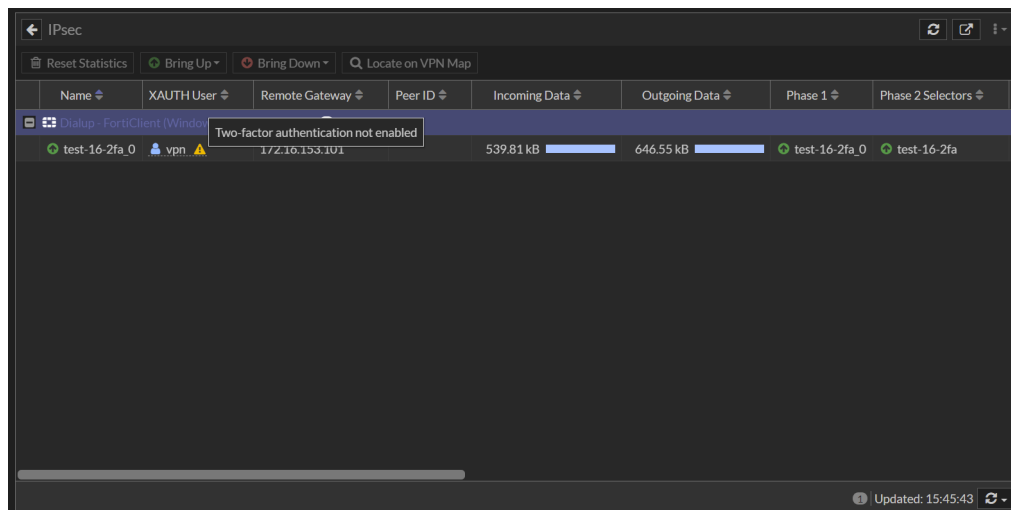
1. Go to *Dashboard > Network*. The *IPsec* overview widget is displayed.
2. Hover over the widget and click *Expand to full screen*. A warning appears when an unauthenticated user is detected.



3. Hover over a record in the table. A tooltip displays the *Phase 1* and *Phase 2* interfaces.



A warning appears next to a user who has not enabled two-factor authentication.

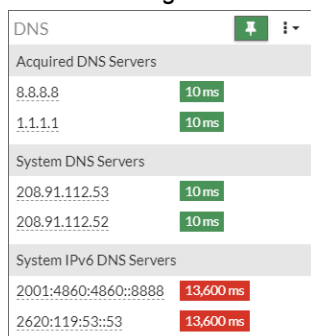


DNS status widget - 7.0.2

The DNS dashboard widget shows latency to configured and dynamically retrieved DNS servers.

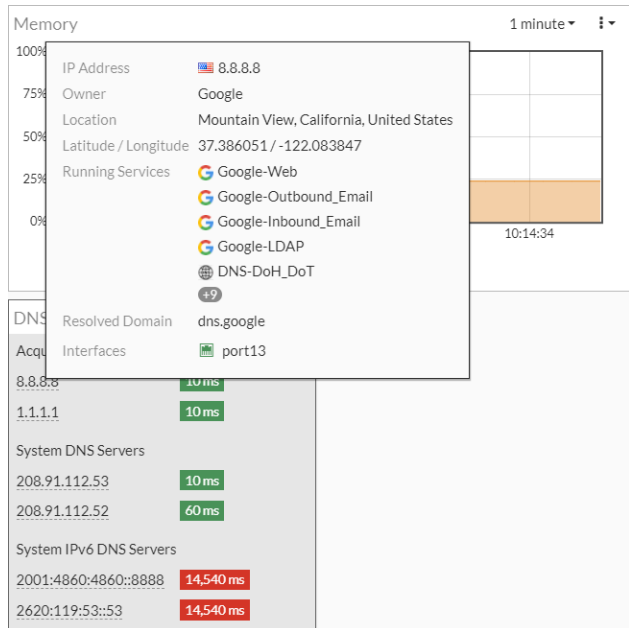
To add the DNS status widget:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *Network* section, click the + beside *DNS*.
3. Click *Add Widget* and click *Close*. The *DNS* widget is displayed in the dashboard.



DNS	
Acquired DNS Servers	
8.8.8.8	10 ms
1.1.1.1	10 ms
System DNS Servers	
208.91.112.53	10 ms
208.91.112.52	10 ms
System IPv6 DNS Servers	
2001:4860:4860::8888	13,600 ms
2620:119:53::53	13,600 ms

4. Hover over a server address to view the tooltip that displays more information.



General usability enhancements

This section includes new features related to general usability enhancements:

- [New themes and CLI console enhancements on page 17](#)
- [Add options for API Preview, Edit in CLI, and References on page 21](#)
- [GUI usability enhancements on page 25](#)

- Seven-day rolling counter for policy hit counters on page 28
- FortiGate administrator log in using FortiCloud single sign-on on page 30
- Navigation menu updates on page 31
- UX improvements for objects on page 32
- Interface migration wizard on page 34
- Add GUI-based global search 7.0.1 on page 38
- Export firewall policy list to CSV and JSON formats 7.0.2 on page 39
- GUI support for configuration save mode 7.0.2 on page 39

New themes and CLI console enhancements

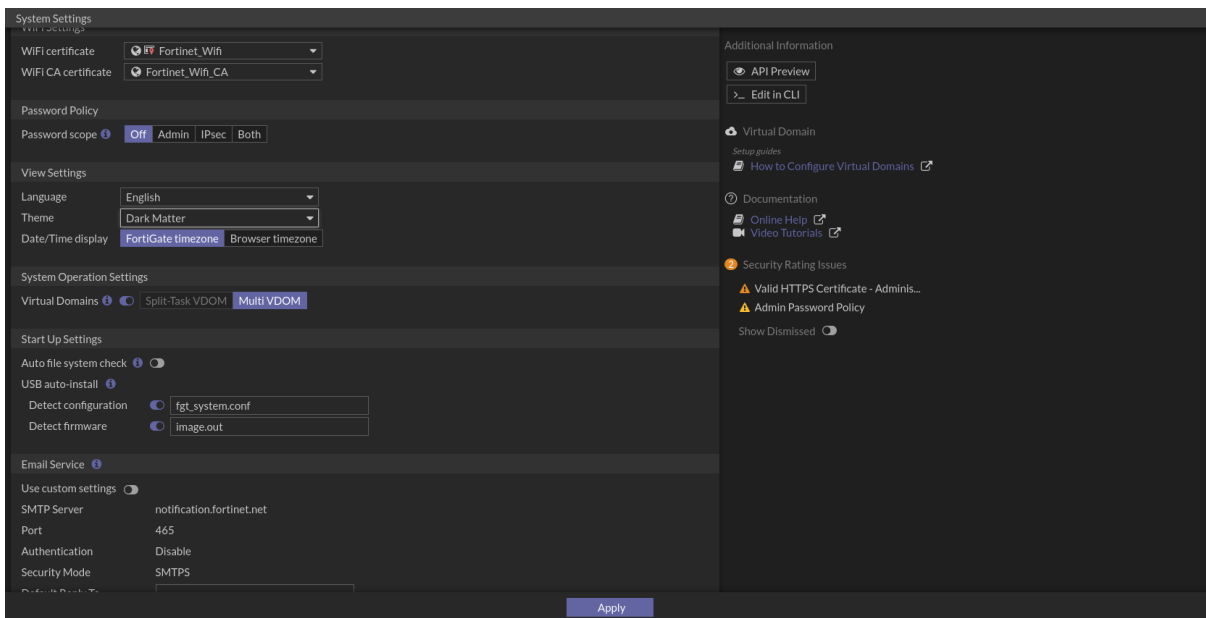
The following GUI enhancements have been added:

- There are several new GUI themes and dark modes (Dark Matter, Onyx, Eclipse, Graphite, Neutrino, Retro).
- The CLI console tab name can be customized.
- The full screen view option is replaced with an option to show or hide the navigation menu.
- VDOM selection is always visible when VDOM mode is enabled.

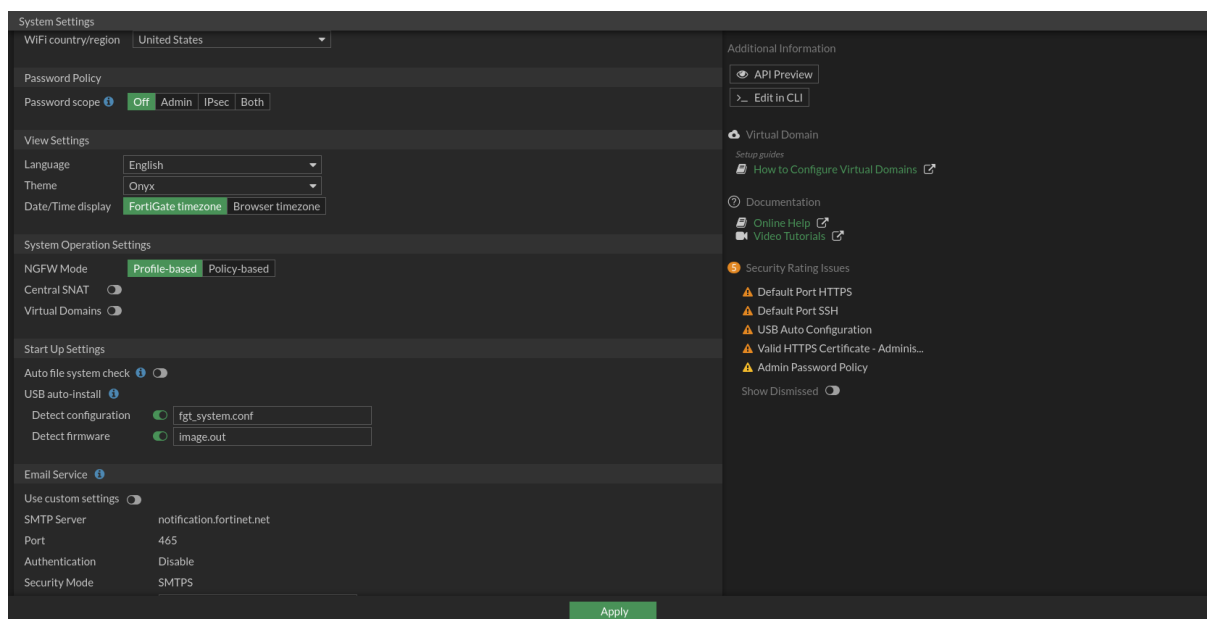
GUI themes

To change the GUI theme, go to *System > Settings*. In the *View Settings* section, select a theme from the dropdown.

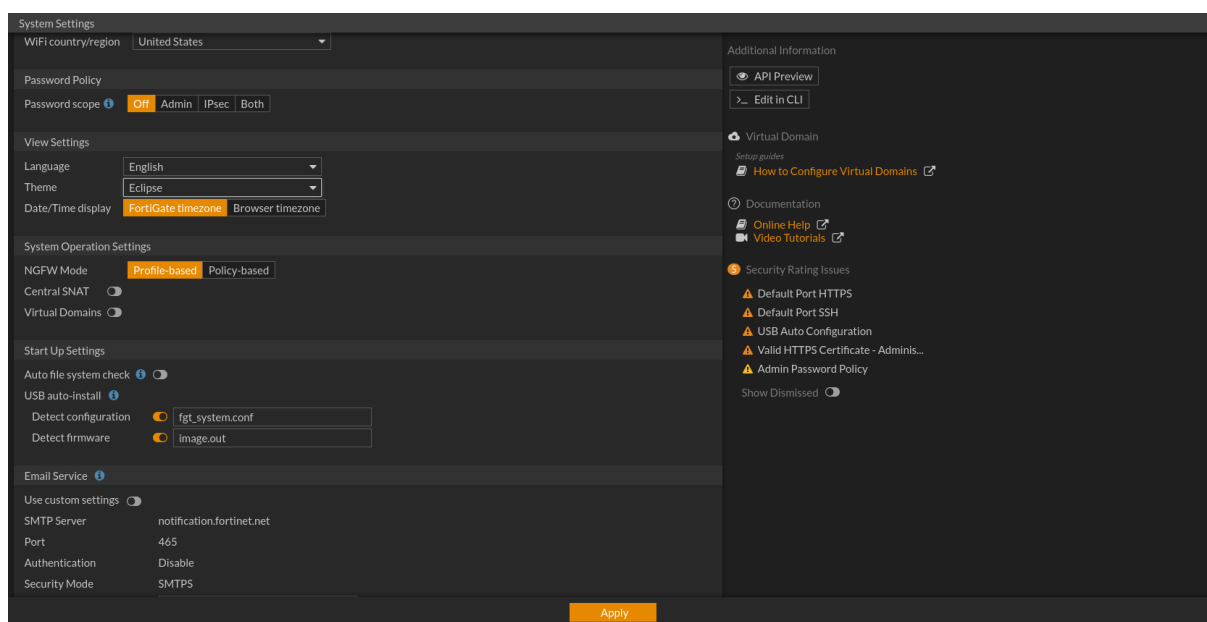
Dark Matter:



Onyx:



Eclipse:



Graphite:

System Settings

WiFi country/region United States

Password Policy

Password scope Off Admin IPsec Both

View Settings

Language English

Theme Graphite

Date/Time display FortiGate timezone Browser timezone

System Operation Settings

NGFW Mode Profile-based Policy-based

Central SNAT ☐

Virtual Domains ☐

Start Up Settings

Auto file system check ☐

USB auto-install ☐

Detect configuration fgt_system.conf

Detect firmware image.out

Email Service

Use custom settings ☐

SMTP Server notification.fortinet.net

Port 465

Authentication Disable

Security Mode SMTSPS

Additional Information

[API Preview](#)

[Edit in CLI](#)

Virtual Domain

[Setup guides](#)

[How to Configure Virtual Domains](#)

Documentation

[Online Help](#)

[Video Tutorials](#)

Security Rating Issues

Default Port HTTPS

Default Port SSH

USB Auto Configuration

Valid HTTPS Certificate - Admins...

Admin Password Policy

Show Dismissed ☐

Apply

Neutrino:

System Settings

WiFi certificate Fortinet_Wifi

WiFi CA certificate Fortinet_Wifi_CA

Password Policy

Password scope Off Admin IPsec Both

View Settings

Language English

Theme Neutrino

Date/Time display FortiGate timezone Browser timezone

System Operation Settings

Virtual Domains Split-Task VDOM Multi VDOM

Start Up Settings

Auto file system check ☐

USB auto-install ☐

Detect configuration fgt_system.conf

Detect firmware image.out

Email Service

Use custom settings ☐

SMTP Server notification.fortinet.net

Port 465

Authentication Disable

Security Mode SMTSPS

Additional Information

[API Preview](#)

[Edit in CLI](#)

Virtual Domain

[Setup guides](#)

[How to Configure Virtual Domains](#)

Documentation

[Online Help](#)

[Video Tutorials](#)

Security Rating Issues

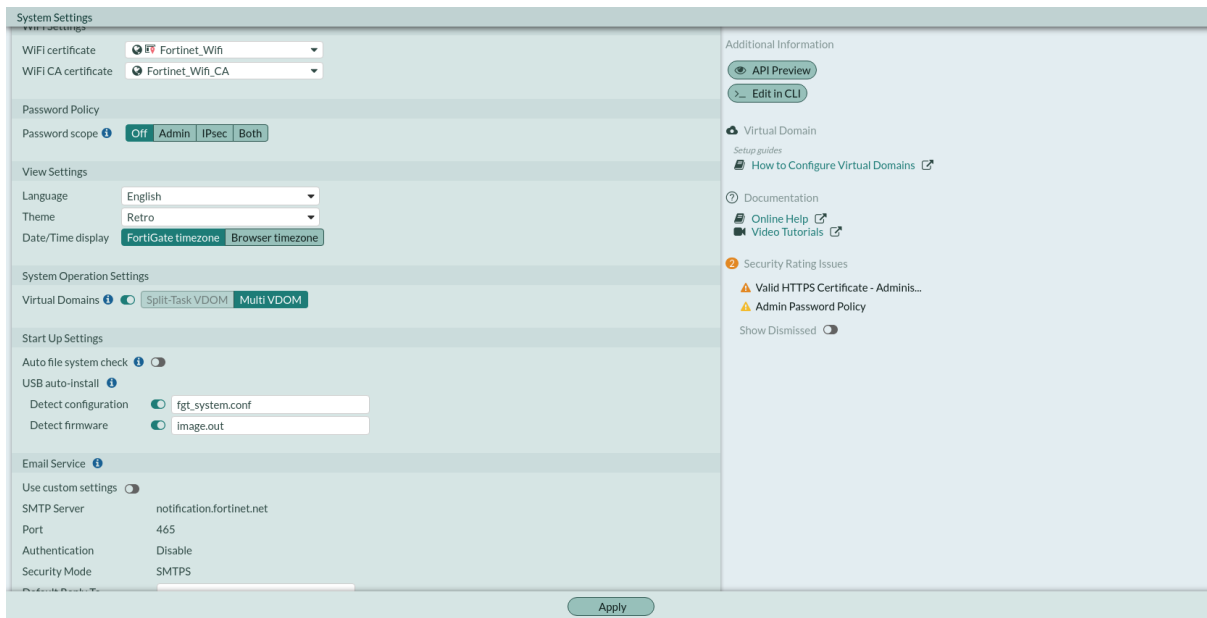
Valid HTTPS Certificate - Admins...

Admin Password Policy

Show Dismissed ☐

Apply

Retro (homage to FortiOS 3.0):



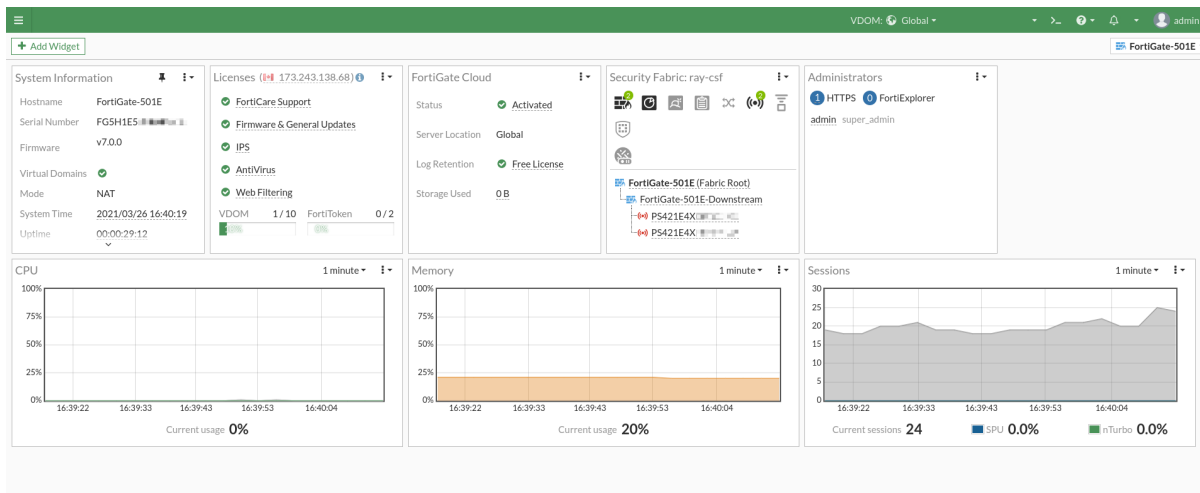
Naming CLI console tabs

After opening a new CLI console tab, click the pencil icon to change the window name.



Showing or hiding the navigation menu

The full screen icon that appeared in the upper-right corner of the GUI has been replaced with three horizontal lines in the upper-left corner. Click the three horizontal lines to show or hide the navigation menu.



Add options for API Preview, Edit in CLI, and References

The *Additional Information* section in the right-side gutter of the GUI includes the following buttons:

- **API Preview:** view all REST API requests being used by the page. Users can make changes on the page that are reflected in the API request preview. This button is not available if the user is logged in as an administrator that has read-only GUI permissions.
- **Edit in CLI:** open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting. This option is applicable for edit pages.
- **References:** open the object usage page to show which other configuration are referencing the object. This option is applicable for edit object pages.

API Preview

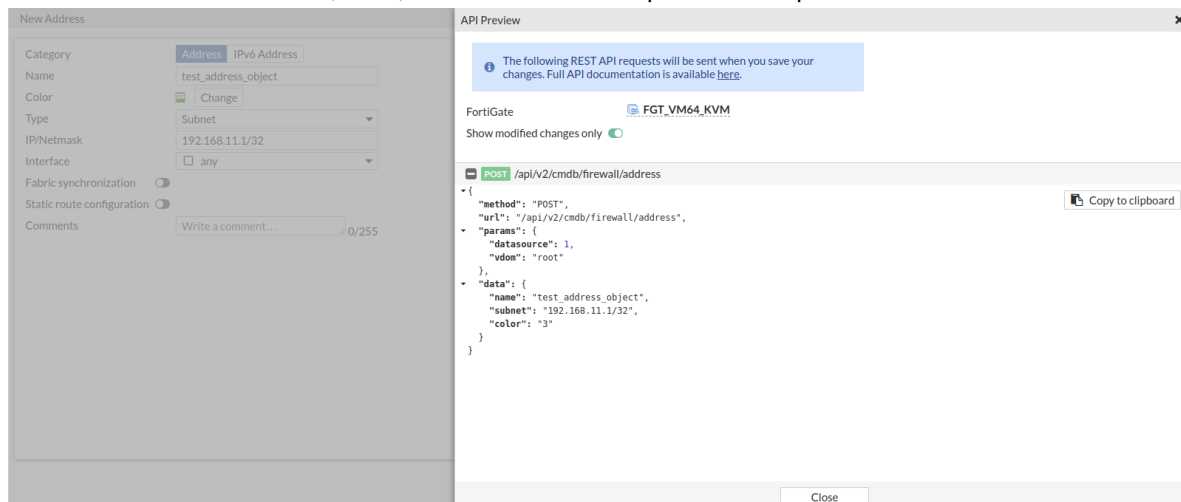
These examples use the *API Preview* when configuring firewall address objects.

To use the API Preview with a new object:

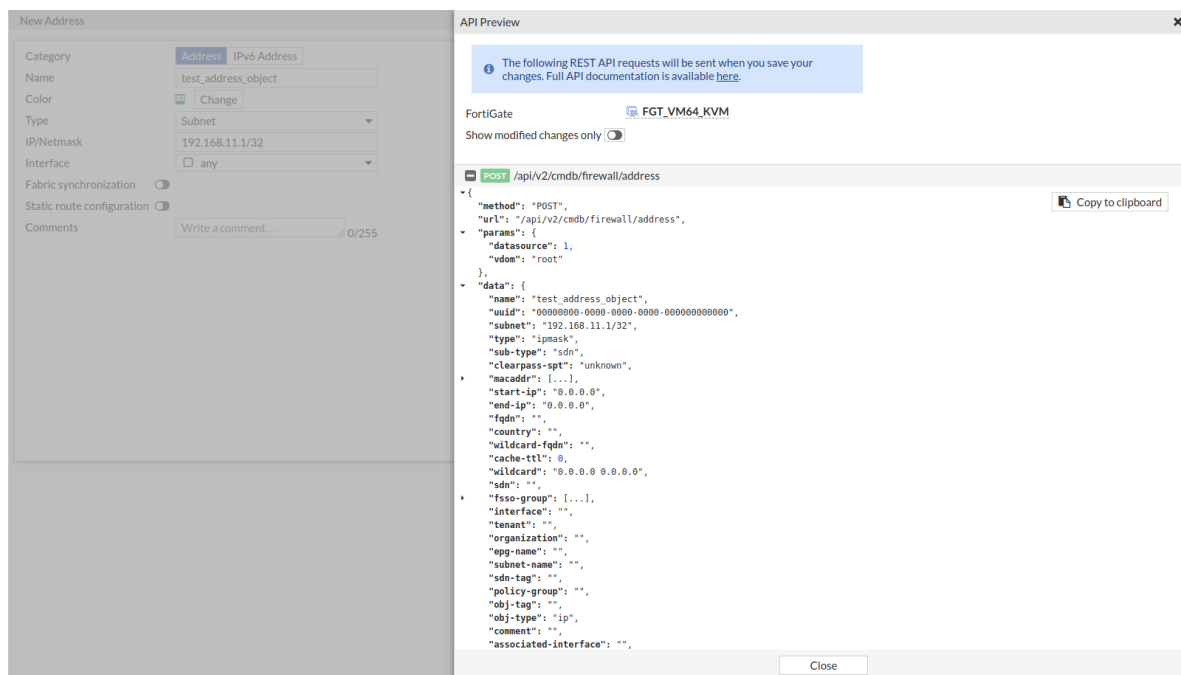
1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Enter the address settings.

The screenshot shows the 'New Address' configuration window. The 'Category' is set to 'Address' and 'IPv6 Address'. The 'Name' is 'test_address_object1'. The 'Color' is 'Change'. The 'Type' is 'Subnet'. The 'IP/Netmask' is '192.168.5.0/24'. The 'Interface' is 'any'. The 'Fabric synchronization' and 'Static route configuration' are both disabled. The 'Comments' field is empty. The 'API Preview' button is visible in the 'Additional Information' section. The 'Dynamic Address' section contains links to guides for configuring dynamic addresses on various cloud platforms. The 'Documentation' section contains links to online help and video tutorials.

3. Click **API Preview**. The **API Preview** pane opens, and the inputted data for the name, color, and IP/netmask are visible (**data**). Since a new object is being created, the POST request is shown for the CMDDB API that creates the firewall address object.
4. Enable **Show modified changes only** to show the modified changes instead of the full configuration in the preview.
5. Click **Close** and edit the address settings.
6. Click **API Preview**. The name, color, and IP/netmask are updated in the preview.



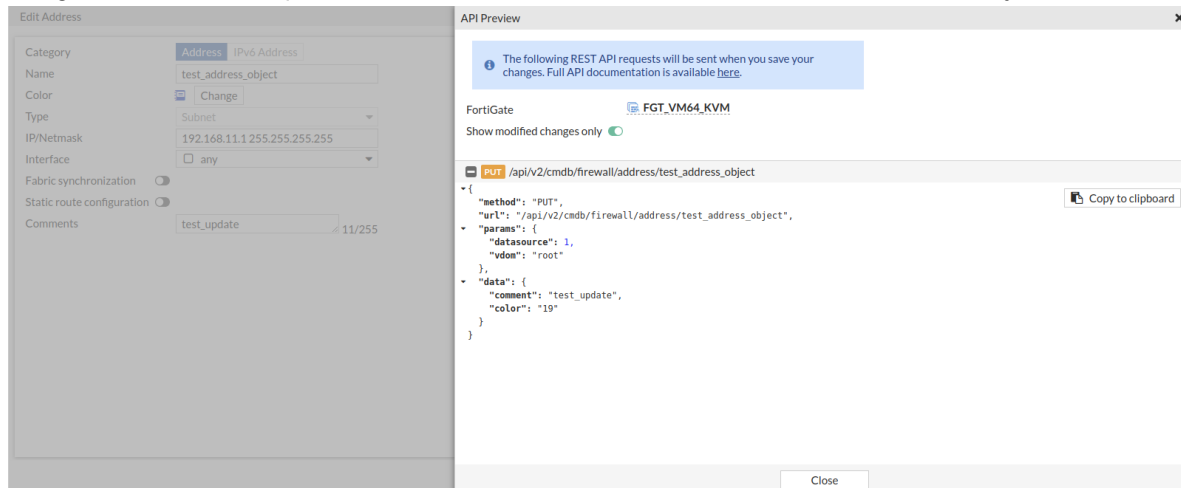
If this option is disabled, the entire object information is displayed.



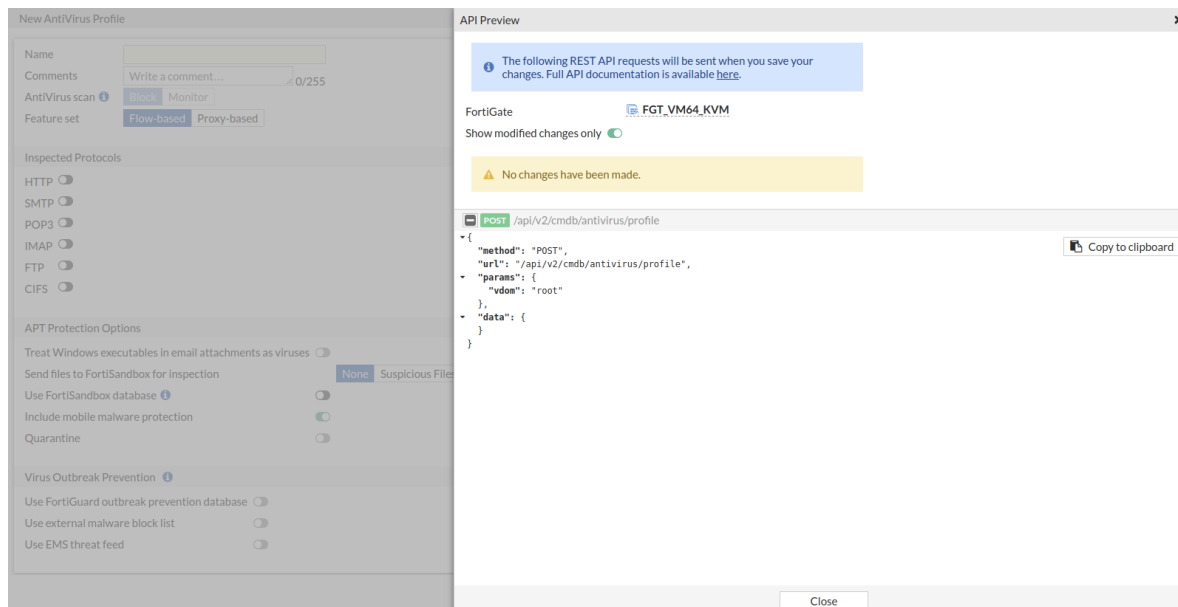
7. Click **Copy to Clipboard** to copy the JSON code shown on the preview screen to the clipboard.
8. Click **Close** to leave the preview.

To use the API Preview with an existing object:

1. Go to *Policy & Objects > Addresses* and double-click an address to edit it.
2. Click *API Preview*. The *API Preview* pane opens, and the input is visible under *data*. Since an existing object is being edited, the PUT request is shown for the CMDDB API that edits the firewall address object.



A prompt, *No changes have been made*, appears in cases where no changes are made, such in the following AV profile.

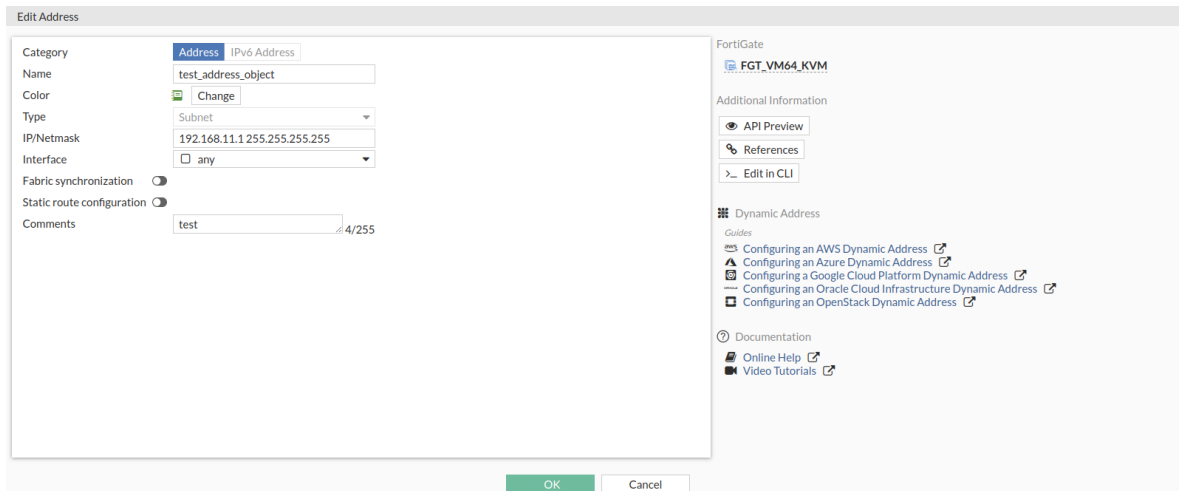


Edit in CLI

This example uses the *Edit in CLI* option to edit an existing firewall address.

To use the Edit in CLI option:

1. Go to *Policy & Objects* > *Addresses* and double-click an address to edit it.
2. Click *Edit in CLI*.



A console tab opens. The address configuration displays and can be modified.

```
CLI Console (1)
FGT_VM64_KVM # config firewall address
FGT_VM64_KVM (address) # edit "test_address_object"
FGT_VM64_KVM (test_address_object) # show
config firewall address
edit "test_address_object"
set uuid 8a928fd4-8e80-51eb-7204-17bec137ef3f
set comment "test"
set color 3
set subnet 192.168.11.1 255.255.255.255
next
end
FGT_VM64_KVM (test_address_object) #
```

References

This example uses the *References* option to view which configurations reference an existing firewall address.

To use the References option:

1. Go to *Policy & Objects* > *Addresses* and double-click an address to edit it.
2. Click *References*. A pane opens with information about the current and possible usage of the address.

3. Click the *Current Usage* or *Possible Uses* buttons to view more information.

Object Name	Ref.
Firewall Policy	
ZTNA Policy (22)	0
LAN to Internet (13) (2 References)	0
DMZ to Internet (2) (2 References)	0
9	0
12	0
Branch1 to Branch2 (17) (2 References)	0
Branch to HQ (18) (2 References)	0
HQ to Branches (19) (2 References)	0
HQ to Internet (20) (2 References)	0
VPN to Internet (26) (2 References)	0
MPLS to INET (27)	0
Proxy Policy	
ZTNA-Rule (1) (2 References)	0
ZTNA_Rule (2)	0

GUI usability enhancements

The following usability enhancements have been added to the GUI:

- Add shortcut on the *Policy & Objects > Virtual IPs* page to create a policy using a virtual IP address or group.
- Add shortcut to show matching event logs for the IPsec tunnel list and monitor widget.
- Add warning message for empty and match all addresses.
- Improve reporting when users encounter configuration errors.

To create a policy with a VIP using the shortcut:

1. Go to *Policy & Objects > Virtual IPs* and select a VIP address or group.
2. Right-click and select *Create firewall policy using this object*.

Name	Details	Interfaces	Services	Ref.
IPv4 Virtual IP				
test	172.16.200.9 → 10.1.100.1			1
IPv6 Virtual IP				
test	2000:172:16:200::9 → 2000:10:1:100::1			1
IPv4 Virtual IP Group				
test_g	test			0
IPv6 Virtual IP Group				
test_g	test			0

You are redirected to the *New Policy* page where the source (if set on the VIP object) and destination fields are already populated.

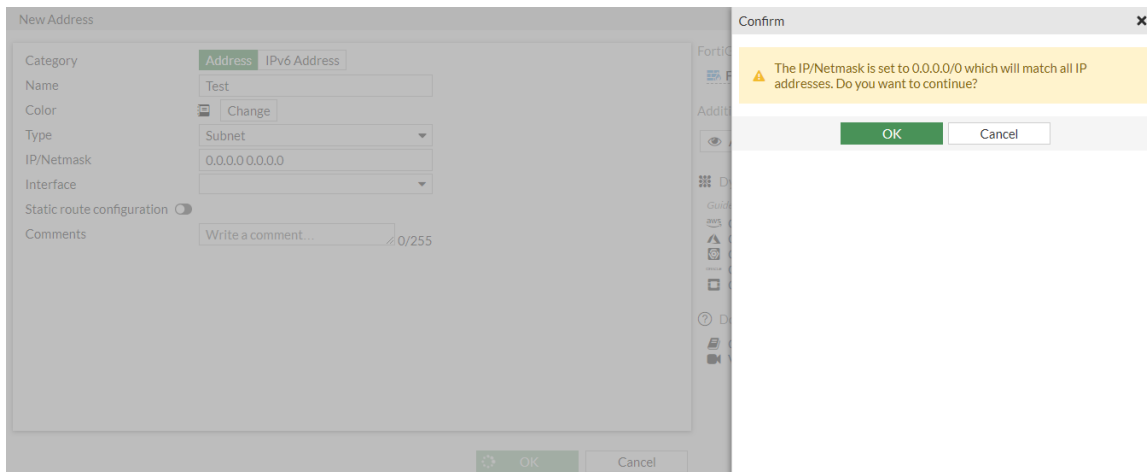
3. Configure the other settings as needed.
4. Click OK.

To view the IPsec related event logs:

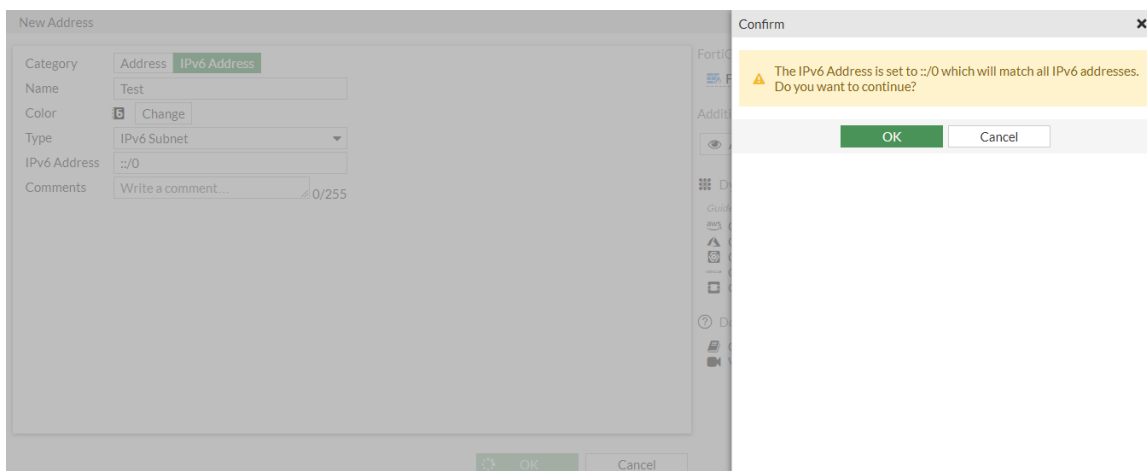
1. Go to *VPN > IPsec Tunnels*, or go to *Dashboard > Network* and click the *IPsec* widget.
2. Select a tunnel.
3. Right-click and select *Show Matching Logs*.

Sample warnings when configuring an address

IPv4 address with 0.0.0.0/0 *IP/Netmask*:



IPv6 address with ::/0 IP/Netmask:



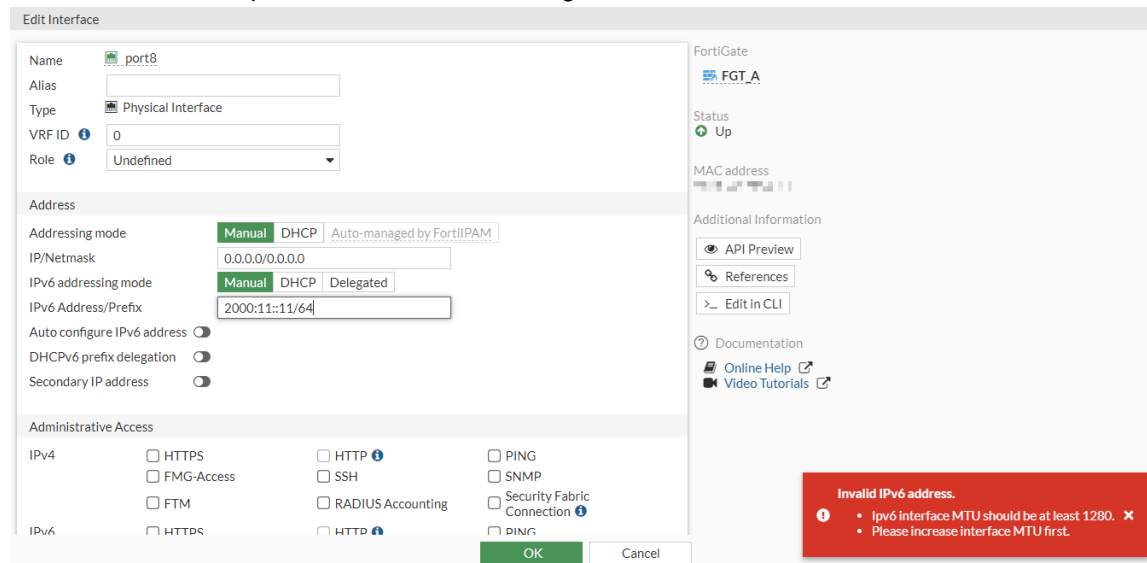
Sample configuration error for MTU override

1. Configure port8 with MTU override enabled:

```
config system interface
    edit "port8"
        set vdom "root"
        set type physical
        set snmp-index 10
        set mtu-override enable
        set mtu 256
    next
end
```

2. Go to *Network > Interfaces* and edit port8.
3. Enter an IPv6 address (2000:11::11/64). An error message appears, *Invalid IPv6 address*, and lists the reasons for

the error. In this example, the interface MTU setting must be at least 1280 for an IPv6 address.



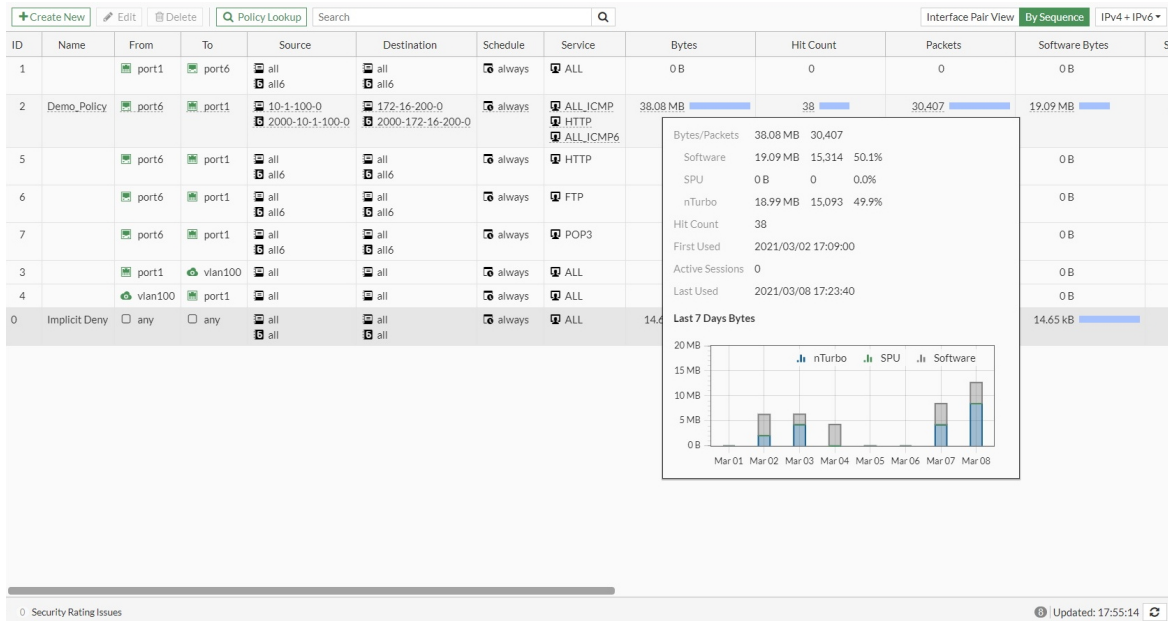
The screenshot shows the 'Edit Interface' configuration window for 'port8'. The 'Address' section is active, showing 'Manual' as the addressing mode and '2000:11::11/64' as the IPv6 Address/Prefix. A red error message is displayed at the bottom right: 'Invalid IPv6 address. • ipv6 interface MTU should be at least 1280. • Please increase interface MTU first.'

Seven-day rolling counter for policy hit counters

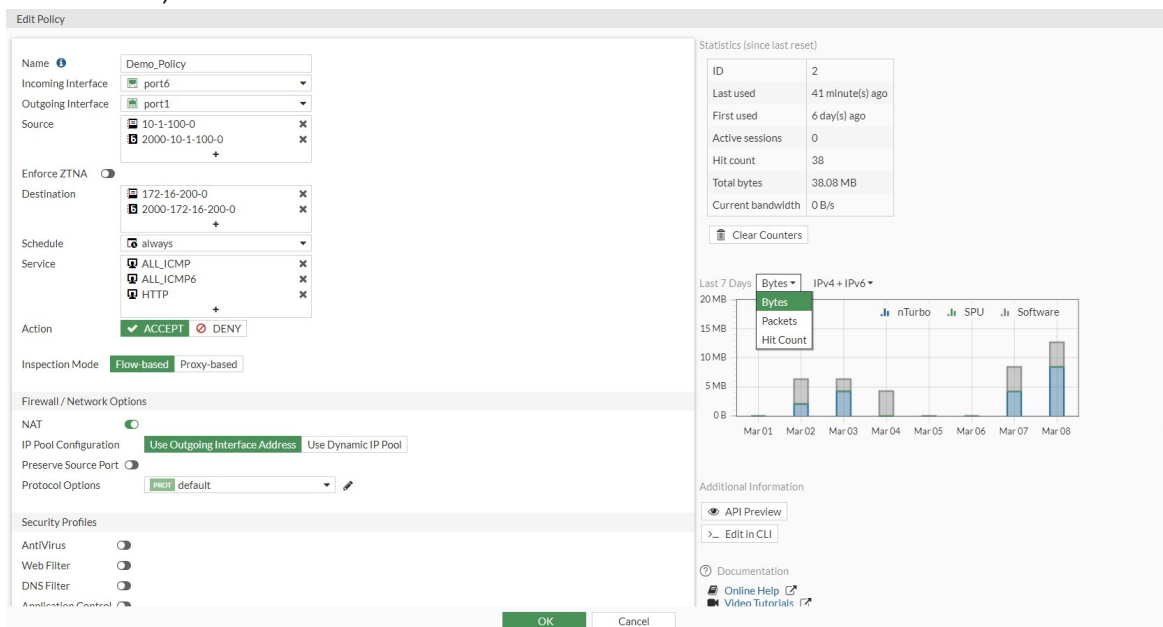
Instead of storing a single number for the hit count and byte count collected since the inception of each policy, seven numbers for the last seven days and an active counter for the current day are stored. The past seven-day hit count is displayed in the policy list and policy pages. A seven-day bar chart shows statistics on each policy page. This feature is currently supported in firewall and multicast policies, but not security policies.

To view the rolling counter information in the GUI:

1. Go to *Policy & Objects > Firewall Policy* or *Policy & Objects > Multicast Policy*.
2. Select a policy and hover over the *Bytes*, *Packets*, or *Hit Count* values to view the tooltip with the corresponding traffic statistics and bar graph (this example uses firewall policies).



- Click *Edit*. The policy traffic statistics appear in the right-hand side of the page.
- Use the dropdowns to filter the bar graph data by counter (*Bytes*, *Packets*, or *Hit Count*) and policy type (*IPv4*, *IPv6*, or *IPv4 + IPv6*).



- Optionally, click *Clear Counters* to delete the traffic statistics for the policy.
- Click *OK*.

To view the rolling counter information in the CLI:

```
# diagnose firewall iprope show 100004 2
idx=2 pkts/bytes=14709/18777329 asic_pkts/asic_bytes=8087/10413737 nturbo_pkts/nturbo_
bytes=8087/10413737 flag=0x0 hit count:19 (4 7 0 1 1 3 3 0)
first:2021-03-02 17:09:00 last:2021-03-08 17:23:40
```

```

established session count:0
  first est:2021-03-02 17:11:20 last est:2021-03-08 17:23:40

# diagnose firewall iprope6 show 100004 2
idx=2 pkts/bytes=15698/19307164 asic_pkts/asic_bytes=7006/8578911 nturbo_pkts/nturbo_
bytes=7006/8578911 flag=0x0 hit count:19 (4 7 0 1 3 2 2 0)
  first:2021-03-02 17:10:32 last:2021-03-08 17:23:33
established session count:0
  first est:2021-03-02 17:11:43 last est:2021-03-08 17:23:33

```

FortiGate administrator log in using FortiCloud single sign-on

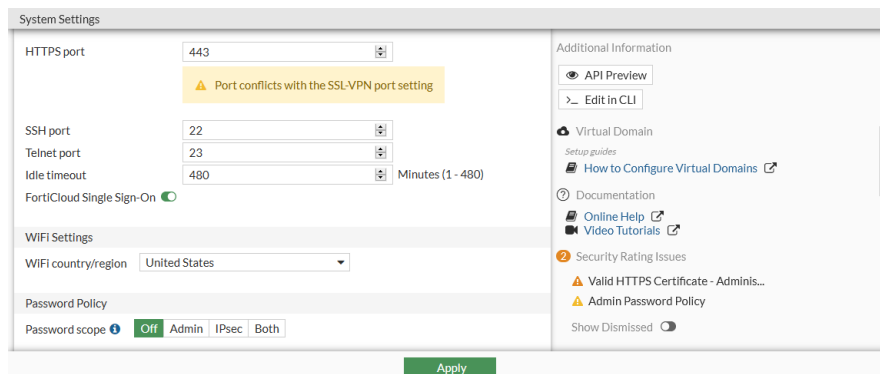
FortiGate can be configured to allow administrators to log in using FortiCloud single sign-on. Both IAM and non-IAM users on the FortiCloud support portal are supported. Non-IAM users must be the FortiCloud account that the FortiGate is registered to.

To configure an IAM user in FortiCloud:

1. Log in to your FortiCloud account at support.fortinet.com.
2. Select *Services > IAM* and click *Add IAM user*.
3. See [Adding an IAM user](#) in the *FortiCloud Identity & Access Management (IAM)* guide for more information. The *Portal Permissions* for *SupportSite*, *IAMPortal*, and *FortiOS SSO* must be configured to allow portal access for administrators.

To enable FortiCloud single sign-On on the FortiGate:

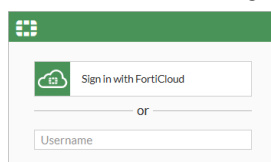
1. Log in to the FortiGate and go to *System > Settings*.
2. Enable *FortiCloud Single Sign-On*.



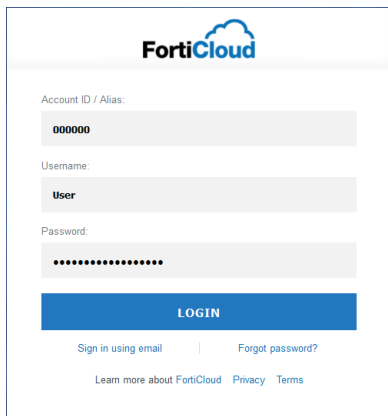
3. Click *Apply*.

To log in to the FortiGate with the FortiCloud user:

1. Go to the FortiGate log in screen.



2. Click *Sign in with FortiCloud*. The FortiCloud sign in screen opens.
3. Do one of the following:
 - Enter the email address and password.
 - Click *Sign in as IAM user* and enter the IAM user information.

The image shows the FortiCloud login interface. At the top is the FortiCloud logo. Below it, there are three input fields: 'Account ID / Alias' with a placeholder '000000', 'Username' with a placeholder 'User', and 'Password' with a placeholder of ten dots. A blue 'LOGIN' button is positioned below these fields. At the bottom, there are two links: 'Sign in using email' and 'Forgot password?'. At the very bottom, there are three small links: 'Learn more about FortiCloud', 'Privacy', and 'Terms'.

4. Click *Login*.
You are logged in to the FortiOS GUI. The SSO username is shown in the top right corner of the GUI.

Navigation menu updates

Navigation menu updates include:

1. Re-order the placement of the *System* and *Security Fabric* menus.
2. Merge *SD-WAN Zones*, *SD-WAN Rules*, and *Performance SLAs* under a single *SD-WAN* menu item.
3. Merge *Traffic Shapers*, *Traffic Shaping Policies*, and *Traffic Shaping Profiles* under a single *Traffic Shaping* menu item.
4. Introduce tabs for the *SD-WAN* and *Traffic Shaping* pages.

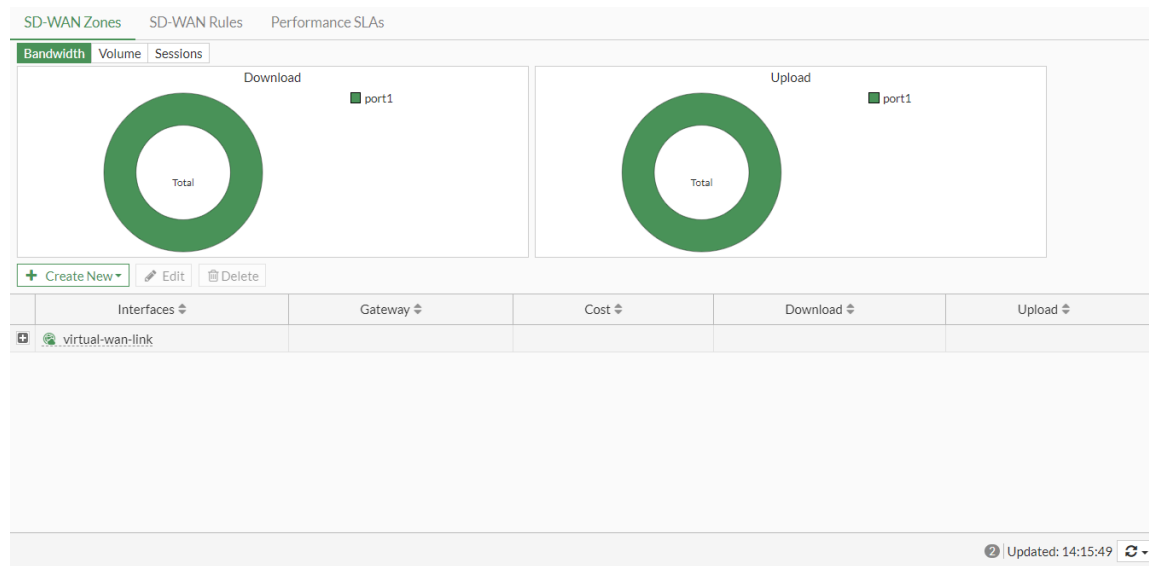
Navigation menu order

The menu order in the GUI is now:

1. *Dashboard*
2. *Network*
3. *Policy & Objects*
4. *Security Profiles*
5. *VPN*
6. *User & Authentication* (includes *WAN Opt* on some platforms with certain features enabled)
7. *WiFi & Switch Controller*
8. *System*
9. *Security Fabric*
10. *Log & Report* (includes *Modem Monitor* with certain features enabled)

SD-WAN page

Go to *Network > SD-WAN* and use the tabs at the top of the screen to create, edit, and manage *SD-WAN Zones*, *SD-WAN Rules*, and *Performance SLAs*.



Traffic Shaping page

Go to *Policy & Objects > Traffic Shaping* and use the tabs at the top of the screen to create, edit, and manage *Traffic Shapers*, *Traffic Shaping Policies*, and *Traffic Shaping Profiles*.

Traffic Shapers						
Traffic Shaping Policies						
Traffic Shaping Profiles						
<div> <div>+ Create New</div> <div>Edit</div> <div>Clone</div> <div>Delete</div> <div>Search</div> </div>						
Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority	Ref.
Shared						
guarantee-100kbps	100.00 kbps	1.05 Gbps	0 bps		High	0
high-priority		1.05 Gbps	0 bps		High	0
low-priority		1.05 Gbps	0 bps		Low	0
medium-priority		1.05 Gbps	0 bps		Medium	0
shared-1M-pipe		1.02 Mbps	0 bps		High	0

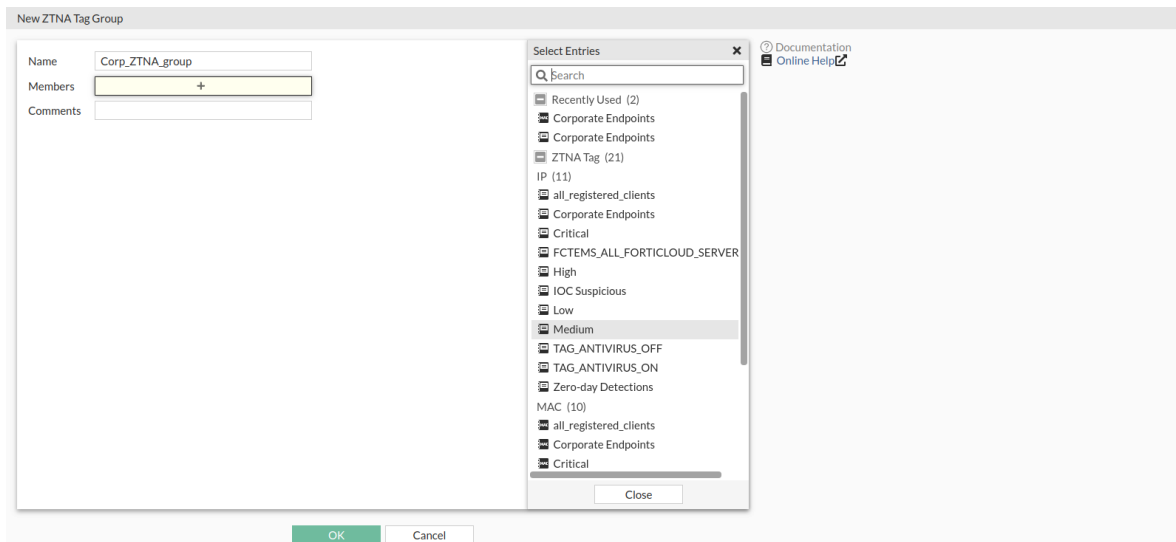
UX improvements for objects

Two UX enhancements have been added for objects:

- Display *Recently Used* items in the omni-select menu when selecting objects.
- Support nested object tooltips.

Recently Used items

In this example, a new ZTNA tag group is being created. After clicking the + to add members, the *Recently Used* section is displayed in the *Select Entries* pane. In previous configurations, the MAC and IP corporate endpoint entries were used so they are listed under *Recently Used*.



Nested object tooltips

In this example, hovering over a ZTNA tag group triggers displaying nested tooltips. This allows the user to check where are the tags coming from and their health source health while staying on the same page.

Hovering over one of the members in the group tooltip (*ZTNA-Corp_group*) shows more information about the ZTNA tag (*MAC Corporate Endpoints*). Hovering over *EMS* in the second tooltip shows more information from FortiClient EMS.

ZTNA Rules ZTNA Servers ZTNA Tags			
+ Create New Group Edit Delete Search			
Name	Details	Comments	Ref.
all_registered_clients			0
Corporate Endpoints			1
Critical			0
FCITEMS_ALL_FORTICLOUD_SERVERS			0
High			0
IOC Suspicious			0
Low			0
Medium			0
TAG_ANTIVIRUS_OFF			0
TAG_ANTIVIRUS_ON			0
Zero-day Detections			0
ZTNA MAC Tag			0
all_registered_clients			0
Corporate Endpoints			1
Critical			0
High			0
IOC Suspicious			0
Low			0
Medium			0
TAG_ANTIVIRUS_C			0
TAG_ANTIVIRUS_C			0
Zero-day Detection			0
ZTNA Tag Group			0
ZTNA-Corp_group			1

Interface migration wizard

The *Integrate Interface* option on the *Network > Interfaces* page helps migrate a physical port into another interface or interface type such as aggregate, software switch, redundant, zone, or SD-WAN zone. The FortiGate will migrate object references either by replacing the existing instance with the new interface, or deleting the existing instance based on the user's choice. Users can also change the VLAN ID of existing VLAN sub-interface or FortiSwitch VLANs.



This feature does not support turning an aggregate, software switch, redundant, zone, or SD-WAN zone interface back into a physical interface.

Integrating an interface

In this example, a DHCP server interface is integrated into a newly created redundant interface, which transfers the DHCP server to a redundant interface.

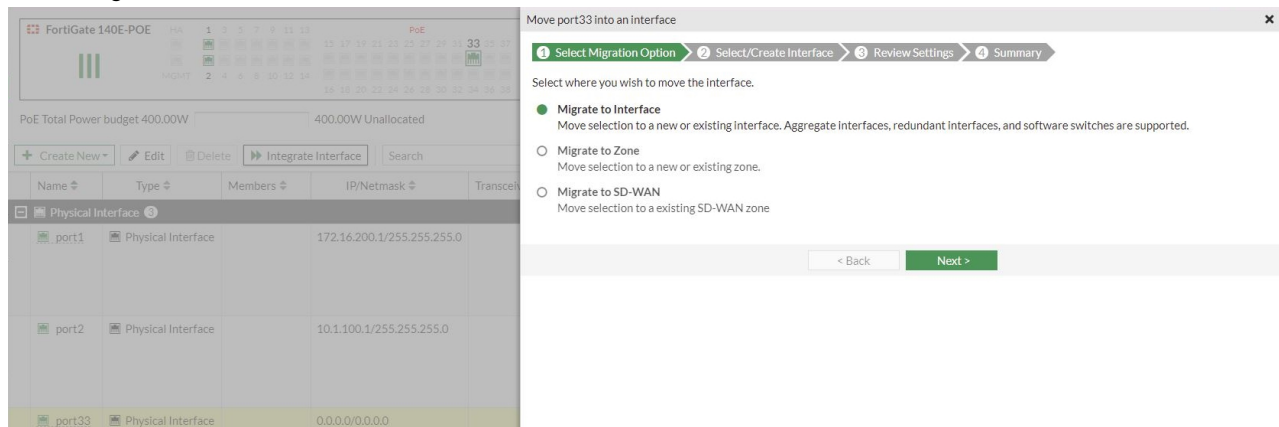
To integrate an interface:

1. Go to *Network > Interfaces* and select an interface in the list.
2. Click *Integrate Interface*. The wizard opens.

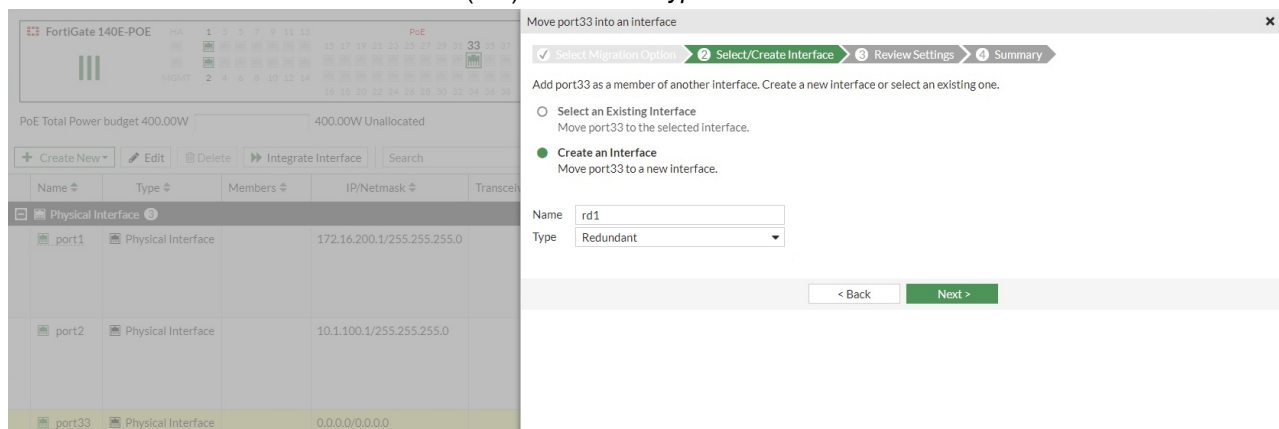


Alternatively, select an interface in the list. Then right-click and select *Integrate Interface*.

3. Select *Migrate to Interface* and click *Next*.

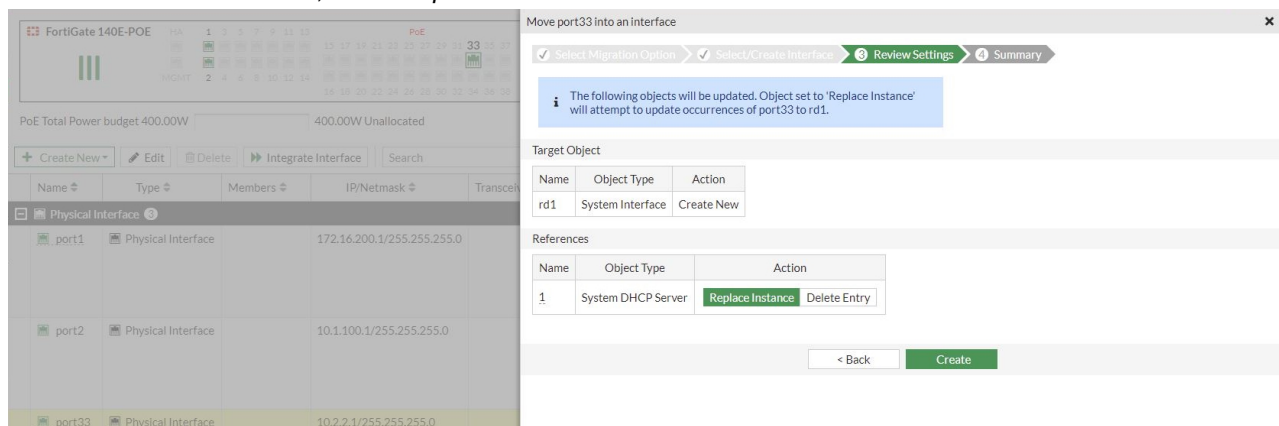


4. Select *Create an Interface*. Enter a name (*rd1*) and set the *Type* to *Redundant*.

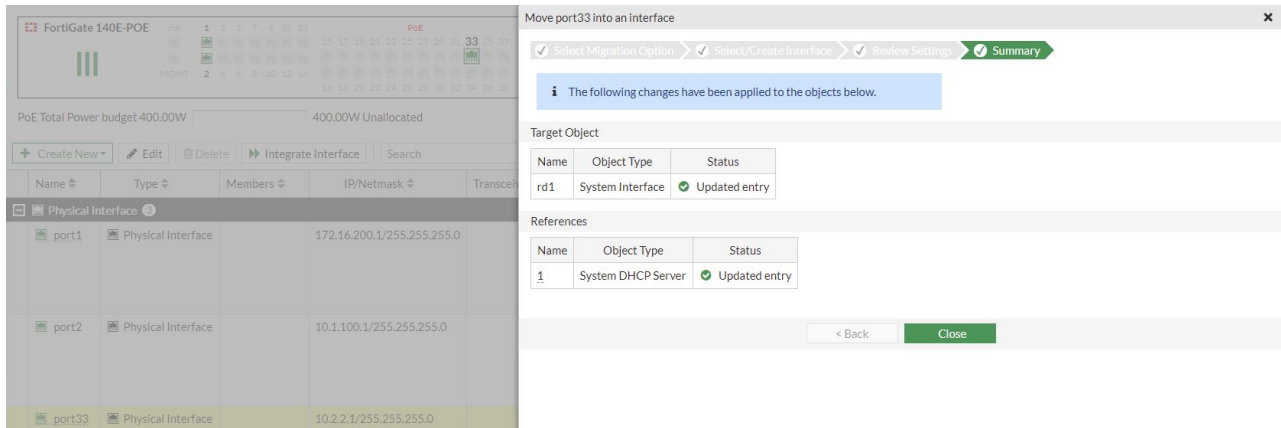


5. Click *Next*. The *References* section lists the associated services with options to *Replace Instance* or *Delete Entry*.

6. For the DHCP server *Action*, select *Replace Instance* and click *Create*.



7. The migration occurs automatically and the statuses for the object and reference change to *Updated entry*. Click *Close*.

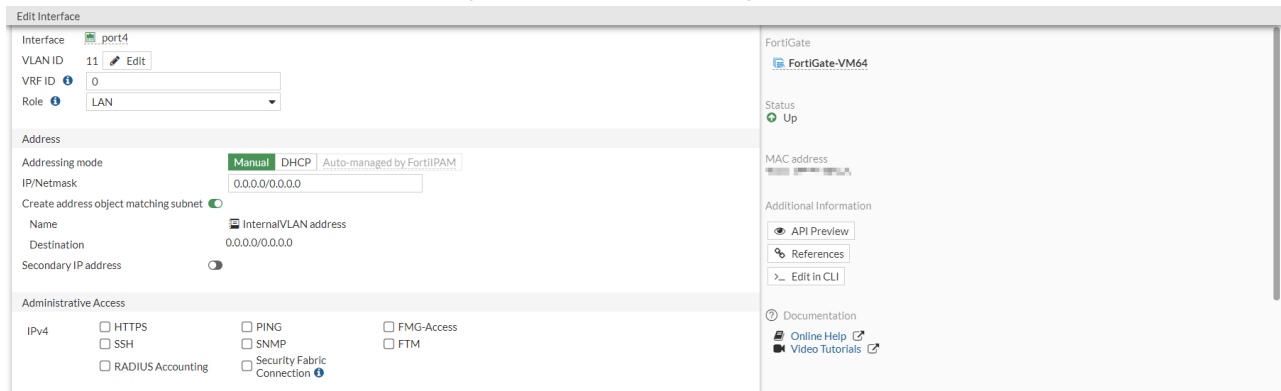


Changing the VLAN ID

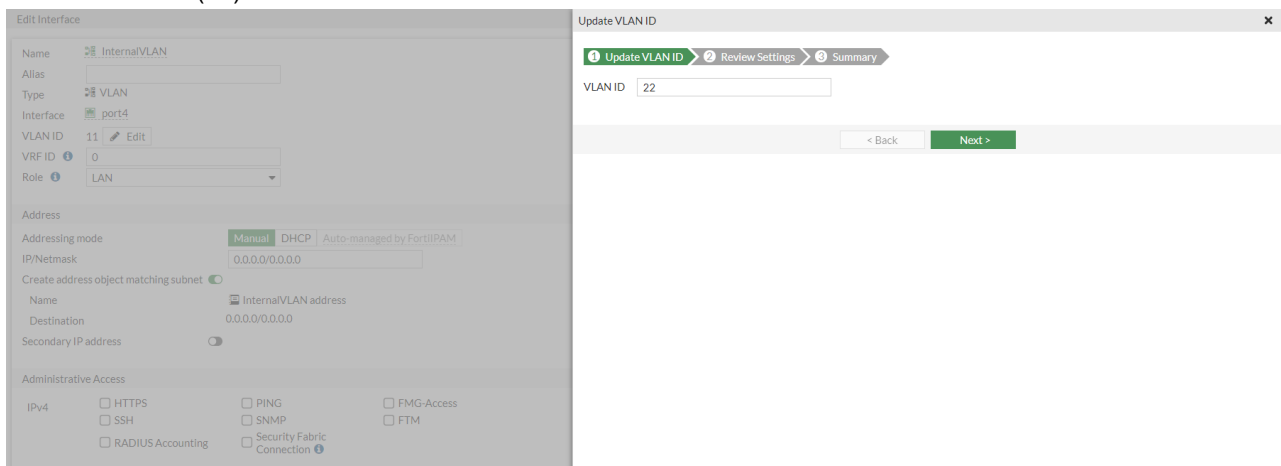
In this example, the VLAN ID of *Internal/VLAN* is changed from 11 to 22.

To change the VLAN ID:

1. Go to *Network > Interfaces* and edit an existing interface.
2. Beside the *VLAN ID* field, click *Edit*. The *Update VLAN ID* window opens.



3. Enter the new ID (22) and click *Next*.



4. Verify the changes, then click *Update* and *OK*.

Edit Interface

Name: InternalVLAN
Alias:
Type: VLAN
Interface: port4
VLAN ID: 11 Edit
VRF ID: 0
Role: LAN

Addressing mode: Manual DHCP Auto-managed by FortiIPAM
IP/Netmask: 0.0.0.0/0.0.0.0
Create address object matching subnet:
Name: InternalVLAN address
Destination: 0.0.0.0/0.0.0.0
Secondary IP address:

Administrative Access
IPv4:
☐ HTTPS ☐ PING ☐ FMG-Access
☐ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ Security Fabric Connection

Update VLAN ID

Update VLAN ID Review Settings Summary

Target Object

Name	Object Type	Action
InternalVLAN	System Interface	Edit

References

Name	Object Type	Action
InternalVLAN address	Address	No changes

Back Update

5. The target object status changes to *Updated entry*. Click *Close*.

Edit Interface

Name: InternalVLAN
Alias:
Type: VLAN
Interface: port4
VLAN ID: 11 Edit
VRF ID: 0
Role: LAN

Addressing mode: Manual DHCP Auto-managed by FortiIPAM
IP/Netmask: 0.0.0.0/0.0.0.0
Create address object matching subnet:
Name: InternalVLAN address
Destination: 0.0.0.0/0.0.0.0
Secondary IP address:

Administrative Access
IPv4:
☐ HTTPS ☐ PING ☐ FMG-Access
☐ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ Security Fabric Connection

Update VLAN ID

Update VLAN ID Review Settings Summary

The following changes have been applied to the objects below.

Target Object

Name	Object Type	Status
InternalVLAN	System Interface	Updated entry

References

Name	Object Type	Status
InternalVLAN address	Address	No changes

Back Close

In the interface settings, the ID displays as 22.

Edit Interface

Name: InternalVLAN
Alias:
Type: VLAN
Interface: port4
VLAN ID: 22 Edit
VRF ID: 0
Role: LAN

Addressing mode: Manual DHCP Auto-managed by FortiIPAM
IP/Netmask: 0.0.0.0/0.0.0.0
Create address object matching subnet:
Name: InternalVLAN address
Destination: 0.0.0.0/0.0.0.0
Secondary IP address:

Administrative Access
IPv4:
☐ HTTPS ☐ PING ☐ FMG-Access
☐ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ Security Fabric Connection

FortiGate
FortiGate-VM64
Status: Up
MAC address:
Additional Information:
API Preview
References
Edit in CLI
Documentation
Online Help
Video Tutorials

Add GUI-based global search - 7.0.1

The global search option in the GUI allows users to search for keywords appearing in objects and navigation menus to quickly access the object and configuration page. Click the magnifying glass icon in the top-left corner of the banner to access the global search.

The global search includes the following features:

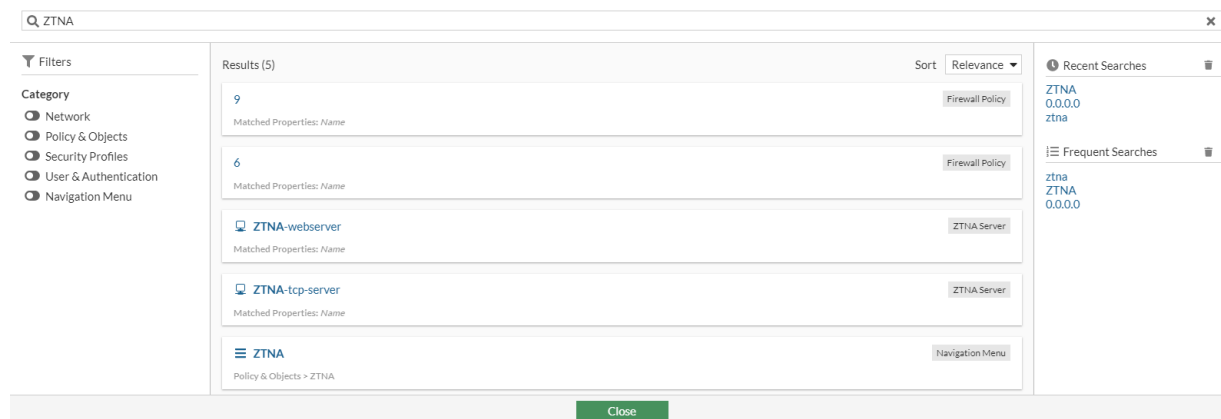
- Keep a history of frequent and recent searches
- Sort results alphabetically by increasing or decreasing order, and relevance by search weight
- Search by category
- Search in Security Fabric members (accessed by the Security Fabric members dropdown menu in the banner)

Examples

In this example, searching for the word *ZTNA* yields the following results:

- Firewall policy object *9*, which contains *ZTNA* in the property value, *Name*. The name of the policy is *ZTNA-TCP*.
- *ZTNA* server object *ZTNA-webserver*, which contains *ZTNA* in the property value, *Name*.
- *ZTNA* navigation menu item under *Policy & Objects > ZTNA*.

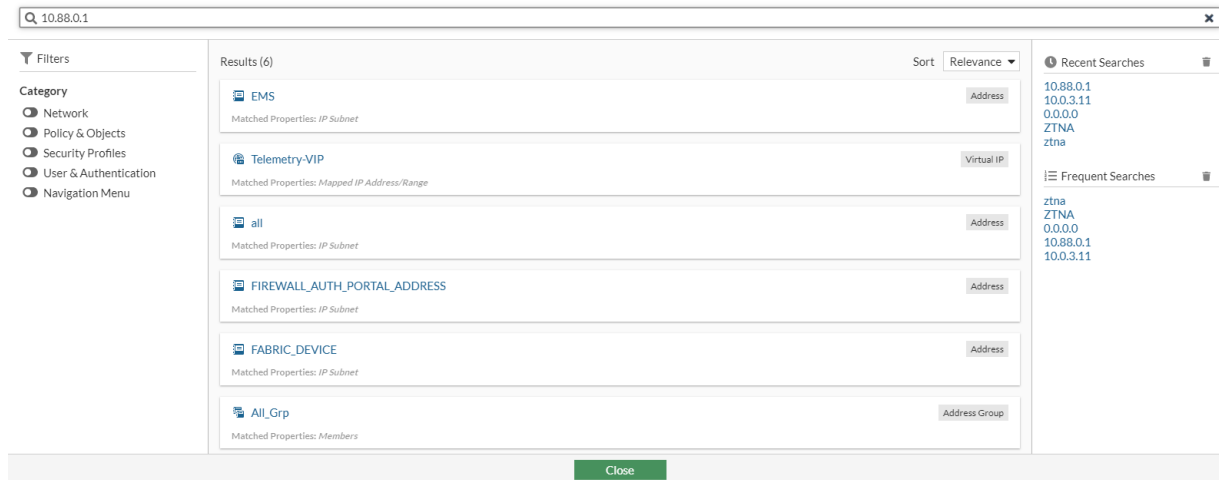
Since CMDB objects have a higher search weight (50) than navigation objects (20), the navigation menu result appears at the bottom.



In this example, searching for the address *10.88.0.1* yields the following results:

- Address object *EMS* that has a subnet of *10.88.0.1/32*, which matches the search term.
- Virtual IP object *Telemetry-VIP* that has a mapped IP range of *10.88.0.1*, which matches the search term.
- Address objects *all*, *FIREWALL_AUTH_PORTAL_ADDRESS*, and *FABRIC_DEVICE* that have IP subnets of *0.0.0.0/0*, which the searched term falls into.
- Address group object *All_Grp* that contains members addresses that have IP subnets of *0.0.0.0/0*, which the searched term falls into.

Sorting by *Relevance* will display address objects that are more closely matched at the top (*10.88.0.1*), and more loosely matched at the bottom (*0.0.0.0*).



Export firewall policy list to CSV and JSON formats - 7.0.2

In the *Firewall Policy* list page, users can export the current view to CSV and JSON formats.

To export the firewall policy list to a CSV or JSON file:

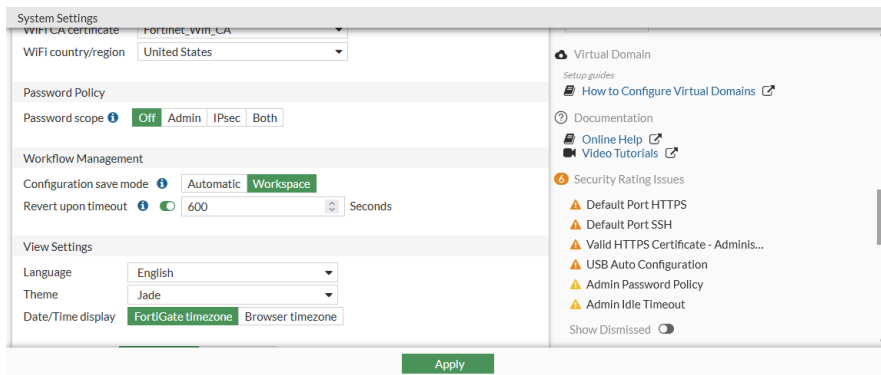
1. Go to *Policy & Objects > Firewall Policy*.
2. In the toolbar above the list, click *Export*.
3. Select CSV or JSON.

Policy Lookup														Export		Interface Pair View	By Sequence	IPv4 + IPv6
ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Size	First Used	Hit Count				
1		port1	port6	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	9.77 kB	2021/09/09 11:29:30	1				
2	policy-name-2	port6	port1	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	746.09 kB	2021/09/06 12:34:25	361				
5		port6	port1	all	all	always	HTTP	ACCEPT	Enabled	no-inspection	UTM	0 B		0				
6		port6	port1	all	all	always	FTP	ACCEPT	Enabled	no-inspection	UTM	0 B		0				
7		port6	port1	all	all	always	POP3	ACCEPT	Enabled	no-inspection	UTM	0 B		0				
3		port1	vlan100	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B		0				
4		vlan100	port1	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B		0				
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	3.06 kB	2021/09/09 11:56:27	51				

The file is automatically downloaded.

GUI support for configuration save mode - 7.0.2

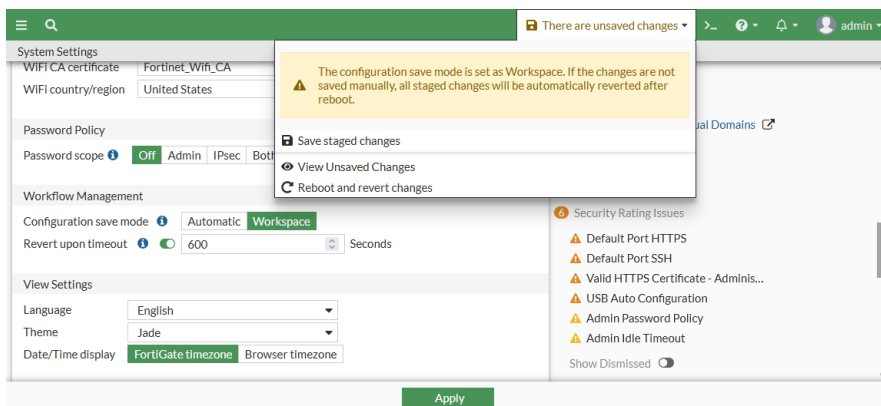
Configuration save, or workspace, mode is supported in the GUI. Administrators can use it to implement strict change control by requiring changes to be manually committed to the flash. To configure the setting, go to *System > Settings*.



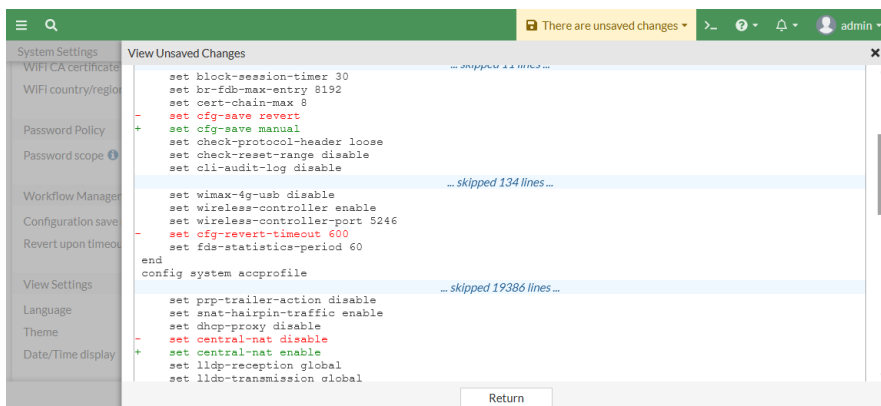
When *Configuration save mode* is set to *Automatic* (default), configuration changes are automatically saved to both memory and flash.

When *Configuration save mode* is set to *Workspace*, configuration changes are saved to memory but not flash. The changes take effect immediately, but must be manually saved to flash. Unsaved changes are reverted when the device is rebooted. If *Revert upon timeout* is enabled, the device automatically reboots after the configured timeout and reverts the changes back to the previous save point. Prior to rebooting, a pop-up warning gives you the option to postpone the reboot by 1 minute, reboot immediately, or save the configuration changes.

In workspace mode, a warning is shown in the banner when there are unsaved changes. Click the warning to save, view, or revert the changes. Reverting the changes requires rebooting the device.



Clicking *View Unsaved Changes* opens a pane highlighting the changes that have not been committed.



This feature is also available in the CLI:

```
config system global
    set cfg-save {automatic | manual | revert}
    set cfg-revert-timeout <integer>
end
# execute cfg {reload | save}
```

Security Fabric

This section includes information about Security Fabric new features:

- [Fabric settings on page 42](#)
- [External connectors on page 82](#)
- [Automation stitches on page 89](#)
- [Security ratings on page 109](#)

Fabric settings

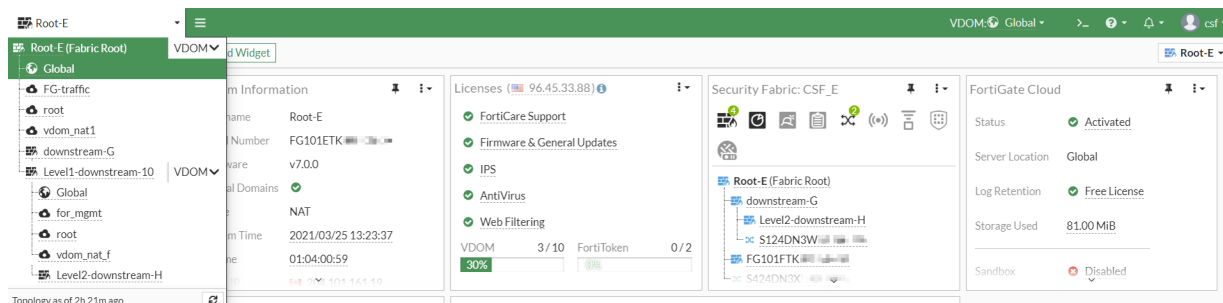
This section includes information about Security Fabric settings related new features:

- [Security Fabric support in multi-VDOM environments on page 42](#)
- [Enhance Security Fabric configuration for FortiSandbox Cloud on page 50](#)
- [FortiWeb integration on page 51](#)
- [Show detailed user information about clients connected over a VPN through EMS on page 53](#)
- [FortiDeceptor as a Security Fabric device on page 55](#)
- [Add FortiAI as a Security Fabric device on page 59](#)
- [Improve communication performance between EMS and FortiGate with WebSockets on page 63](#)
- [Simplify EMS pairing with Security Fabric so one approval is needed for all devices on page 65](#)
- [FortiTester as a Security Fabric device 7.0.1 on page 66](#)
- [Simplify Fabric approval workflow for FortiAnalyzer 7.0.1 on page 69](#)
- [Allow deep inspection certificates to be synchronized to EMS and distributed to FortiClient 7.0.1 on page 71](#)
- [Asset Identity Center page 7.0.2 on page 78](#)
- [Fabric Management page 7.0.2 on page 80](#)

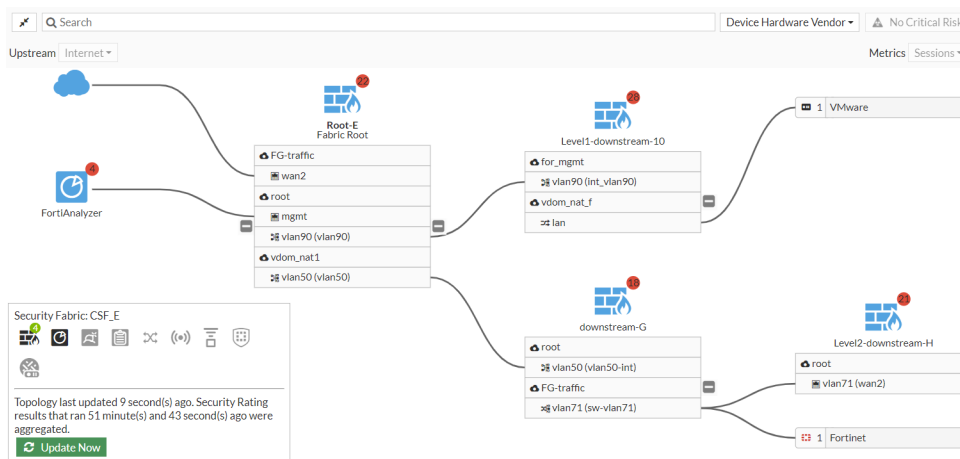
Security Fabric support in multi-VDOM environments

A Security Fabric can be enabled in multi-VDOM environments. This allows access to all of the Security Fabric features, including automation, security rating, and topologies, across the VDOM deployment.

- Users can navigate to downstream FortiGate devices and VDOMs directly from the root FortiGate using the Fabric selection menu.



- The logical topology shows all of the configured VDOMs.

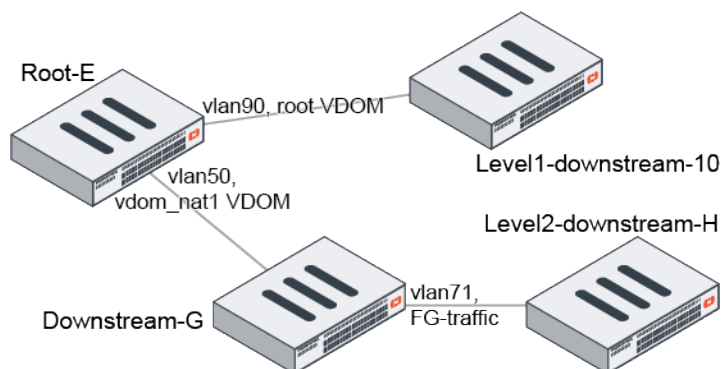


- Security rating reports include results for all of the configured VDOMs as well the entire Fabric.



Downstream FortiGate devices must connect to the upstream FortiGate from its management VDOM.

Topology



In this topology, there is a root FortiGate with three FortiGates connected through two different VDOMs. The root FortiGate is able to manage all devices running in multi-VDOM mode.

This example assumes multi-VDOM mode is already configured on each FortiGate, and that FortiAnalyzer logging is configured on the root FortiGate (see [Configuring FortiAnalyzer](#) and [Configuring the root FortiGate and downstream FortiGates](#) for more details).

To enable multi-VDOM mode:

```
config system global
    set vdom-mode multi-vdom
end
```

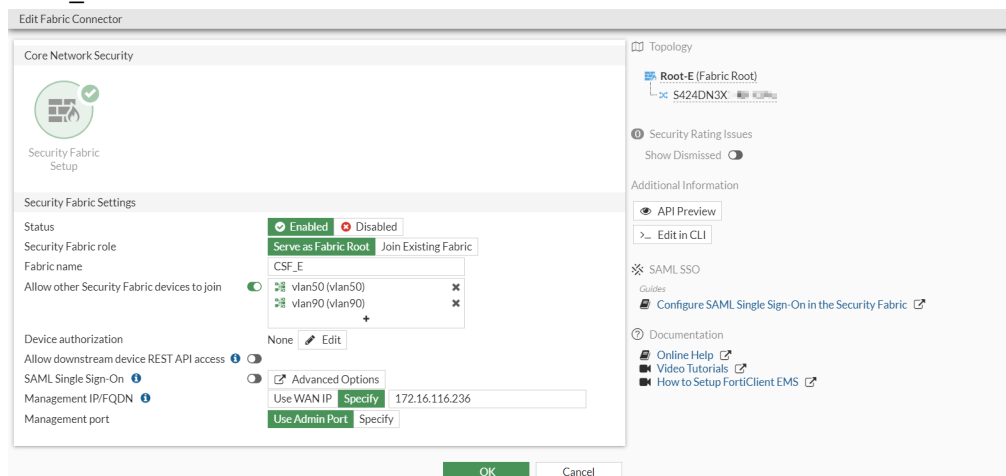
Device configurations

Root FortiGate (Root-E)

The Security Fabric is enabled, and configured so that downstream interfaces from all VDOMs can allow other Security Fabric devices to join.

To configure Root-E in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
2. Ensure that the *Status* is *Enabled* and the *Security Fabric role* is set to *Serve as Fabric Root*.
3. Enable *Allow other Security Fabric devices to join* and click the + to add the interfaces (vlan50 and vlan90) from the vdom_nat1 and root VDOMs.



4. Configure the other settings as needed.
5. Click **OK**.

To configure Root-E in the CLI:

1. Enable the Security Fabric:

```
config system csf
    set status enable
    set group-name "CSF_E"
end
```

2. Configure the interfaces:

```
config system interface
    edit "vlan50"
        set vdom "vdom_nat1"
        ...
        set allowaccess ping https ssh http fgfm fabric
        ...
    next
    edit "vlan90"
        set vdom "root"
        ...
        set allowaccess ping https ssh http fgfm fabric
```

```

    ...
    next
end

```

Downstream FortiGate 1 (Downstream-G)

To configure Downstream-G in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
2. For *Status*, select *Enabled* and set the role to *Join Existing Fabric*.
3. Enter the *Upstream FortiGate IP*, which is the IP of the root FortiGate vdom_nat1 interface (192.168.5.5). Downstream-G must use the interface from the management VDOM to connect to the upstream FortiGate IP.
4. Enable *Allow other Security Fabric devices to join* and click the + to add the downstream interface (sw-vlan71) from the FG-traffic VDOM.

The screenshot shows the 'Edit Fabric Connector' window for 'Security Fabric Setup'. The 'Security Fabric Settings' section is expanded, showing the following configuration:

- Status:** Enabled (radio button selected)
- Security Fabric role:** Join Existing Fabric (radio button selected)
- Upstream FortiGate IP:** 192.168.5.5
- Allow other Security Fabric devices to join:** Enabled (checkbox checked)
- Additional interfaces:** A list containing 'vlan71 (sw-vlan71)' with a '+' button to add more.
- Allow downstream device REST API access:** Disabled (checkbox unchecked)
- SAML Single Sign-On:** Auto (radio button selected)
- Mode:** Disabled
- Management IP/FQDN:** 172.16.116.217 (with 'Specify' button)
- Management port:** Use Admin Port (radio button selected)

On the right side, the 'Fabric Status' section shows 'Pending Authorization' with a 'Review authorization on root FortiGate' button. Below that, the 'Topology' section shows a diagram with 'Root-E' connected to 'downstream-G', which is connected to 'S124DN3W'. The 'Security Rating Issues' section shows 'Show Dismissed' with a toggle switch. The 'Additional Information' section includes links for 'API Preview', 'Edit in CLI', 'SAML SSO', 'Guides', 'Documentation', 'Online Help', 'Video Tutorials', and 'How to Setup FortiClient EMS'.

5. Configure the other settings as needed.
6. Click **OK**.

To configure Downstream-G in the CLI:

1. Enable the Security Fabric:

```

config system csf
    set status enable
    set upstream-ip 192.168.5.5
end

```

2. Configure the interfaces:

```

config system interface
    edit "sw-vlan71"
        set vdom "FG-traffic"
        ...
        set allowaccess ping https ssh http fgfm fabric
        ...
    end
end

```

```

next
end

```

Downstream FortiGate 2 (Level2-downstream-H)

To configure Level2-downstream-H in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
2. For *Status*, select *Enabled* and set the role to *Join Existing Fabric*.
3. Enter the *Upstream FortiGate IP*, which is the IP of the root VDOM on Downstream-G (192.168.71.7).

4. Configure the other settings as needed.
5. Click **OK**.

To configure Level2-downstream-H in the CLI:

```

config system csf
    set status enable
    set upstream-ip 192.168.71.7
end

```

Downstream FortiGate 3 (Level1-downstream-10)

To configure Level1-downstream-10 in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
2. For *Status*, select *Enabled* and set the role to *Join Existing Fabric*.

- Enter the *Upstream FortiGate IP*, which is the IP of the root VDOM on Root-E (192.168.9.5).

- Configure the other settings as needed.

- Click **OK**.

To configure Level1-downstream-10 in the CLI:

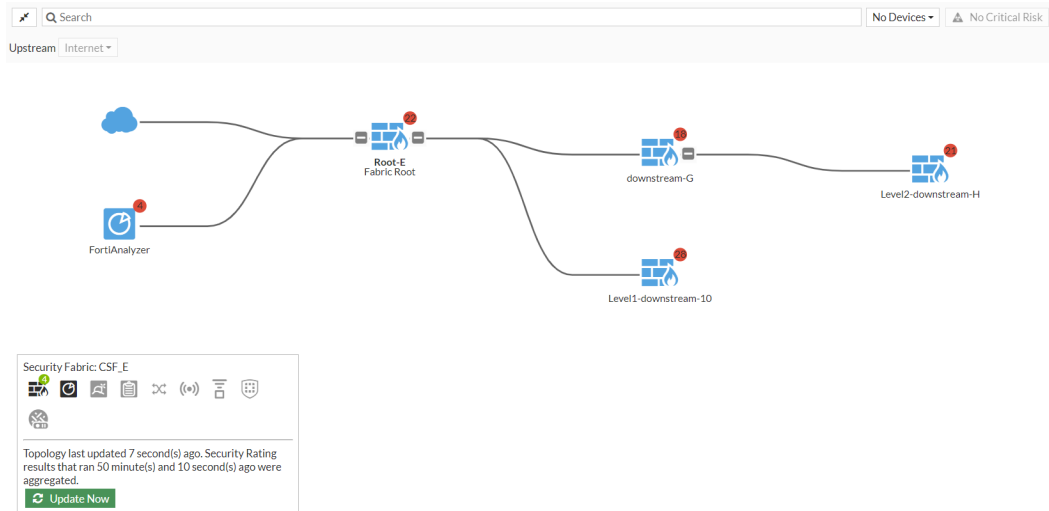
```
config system csf
    set status enable
    set upstream-ip 192.168.9.5
end
```

Device authorization and verification

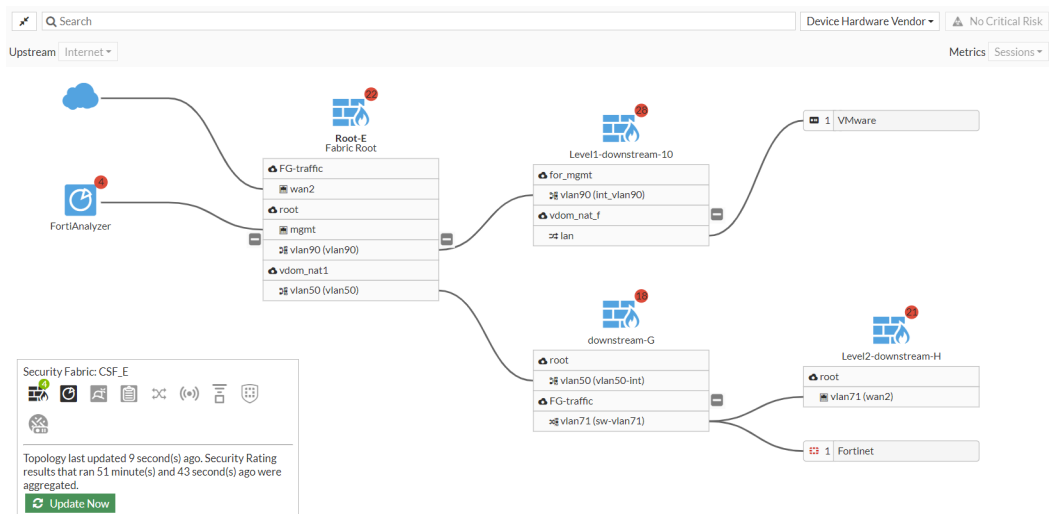
To authorize the downstream devices on the root FortiGate:

- On Root-E, go to *Security Fabric > Fabric Connectors*.
- In the topology tree, click the highlighted serial number and select **Authorize** for each downstream FortiGate. Once all the devices are authorized, the physical topology page shows the root and downstream FortiGates. The logical topology page shows the root and downstream FortiGates connected to interfaces in their corresponding VDOMs.

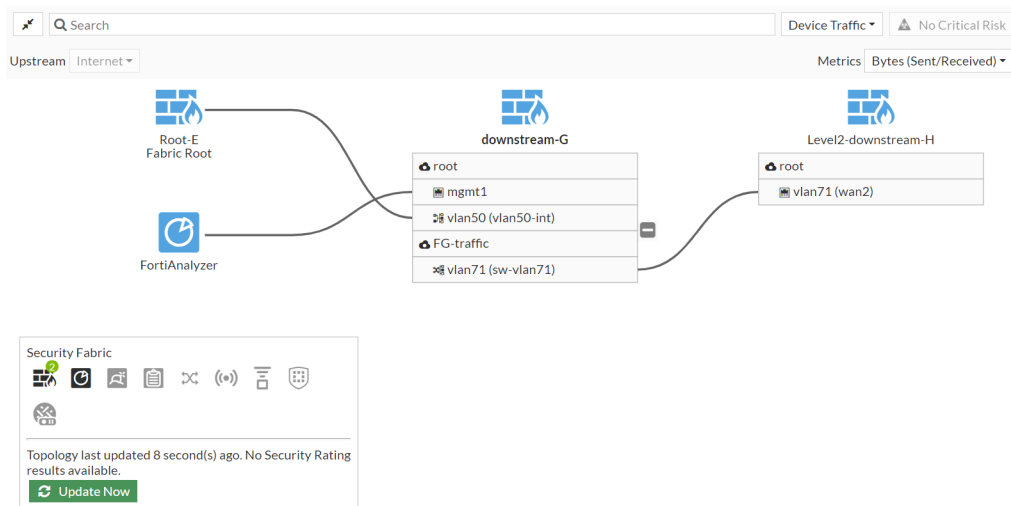
Root-E physical topology:



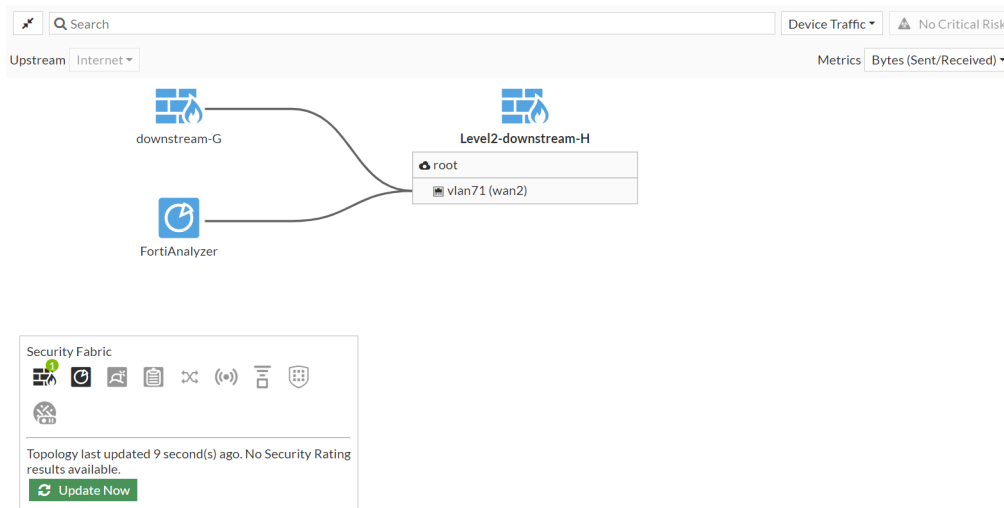
Root-E logical topology:



Downstream-G logical topology:



Level2-downstream-H logical topology:

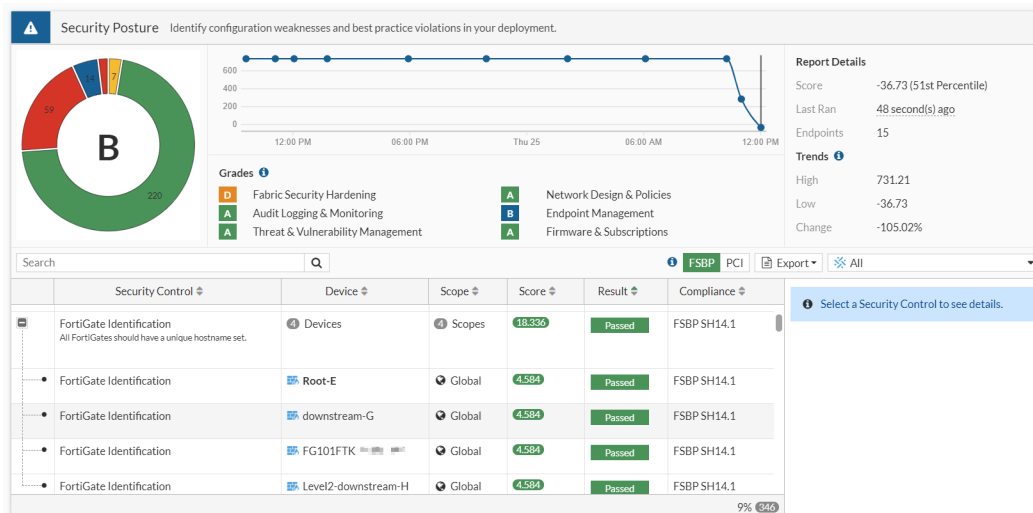


Security rating

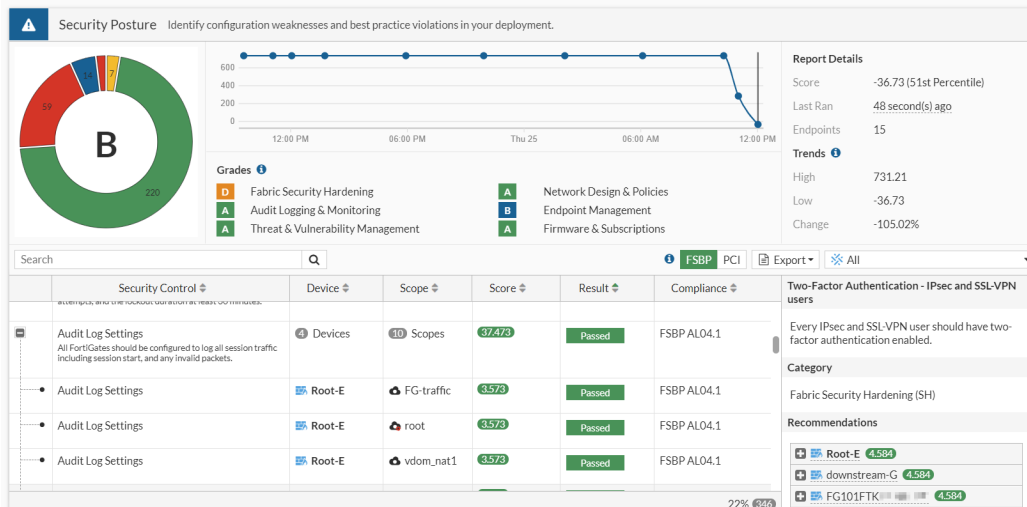
To run a security rating report on the root FortiGate:

1. On Root-E, go to *Security Fabric > Security Rating*.
2. Under *Report Details*, click *Run Now*.
3. Click the *Security Posture* scorecard to view the results. The *Scope* column identifies results for either global or specific VDOMs.

Global scope:



VDOM scope:



Enhance Security Fabric configuration for FortiSandbox Cloud

Creating an instance of FortiSandbox on FortiCloud can be configured from the *Fabric Connectors* page in the GUI. In the *Cloud Sandbox Settings*, you can choose between connecting to FortiGate Cloud or FortiSandbox Cloud. Connecting to FortiSandbox Cloud will automatically use the cloud user ID of the FortiGate to connect to the correct FortiSandbox Cloud account.

Requirements

The following items are required to initialize FortiSandbox Cloud:

- A FortiCloud premium account.
- A valid FSAC contract on the FortiGate. To view contract information in the CLI, enter `diagnose test update info`. The `User ID` at the end of the output lets FortiCloud to know which FortiSandbox Cloud account the FortiGate is connected to.

FortiSandbox Cloud requires the following licenses:

- FortiCloud premium license
- FortiSandbox Cloud entitlement
- FortiGate license (register the FortiGate on the same account as the FortiCloud license)

To configure FortiSandbox Cloud in the GUI:

- Go to *Security Fabric > Fabric Connectors* and double-click the *Cloud Sandbox* card.
- Set *Status* to *Enable*.

- For *Type*, select *FortiSandbox Cloud*.



If the *FortiSandbox Cloud* option is grayed out or not visible, enter the following in the CLI:

```
config system global
    set gui-fortigate-cloud-sandbox enable
end
```

- Click *OK*.

To configure FortiSandbox Cloud in the CLI:

```
config system fortisandbox
    set status enable
    set forticloud enable
    set server "fortisandboxcloud.com"
end
```

To switch from Cloud Sandbox to FortiSandbox in the Security Fabric:

- Go to *Security Fabric > Fabric Connectors* and double-click the *Cloud Sandbox* card.
- Set *Status* to *Disable*.
- Click *OK*.
- In the CLI, enter the following.

```
config system fortisandbox
    set status enable
    set forticloud disable
    set server <address>
end
```

The *FortiSandbox* card is now visible in the *Other Fortinet Products* section.

FortiWeb integration

A FortiWeb can be configured to join a Security Fabric through the root or downstream FortiGate. Once the FortiWeb joins the Fabric, the following features are available:

- View the FortiWeb on topology pages.
- Create a dashboard Fabric Device widget to view FortiWeb data.
- Configure single sign-on using SAML.

In the following example, a FortiWeb is pre-authorized on the root FortiGate using certificate authorization. This is example assumes the Security Fabric has already been configured.

To authorize a FortiWeb to join the Security Fabric:

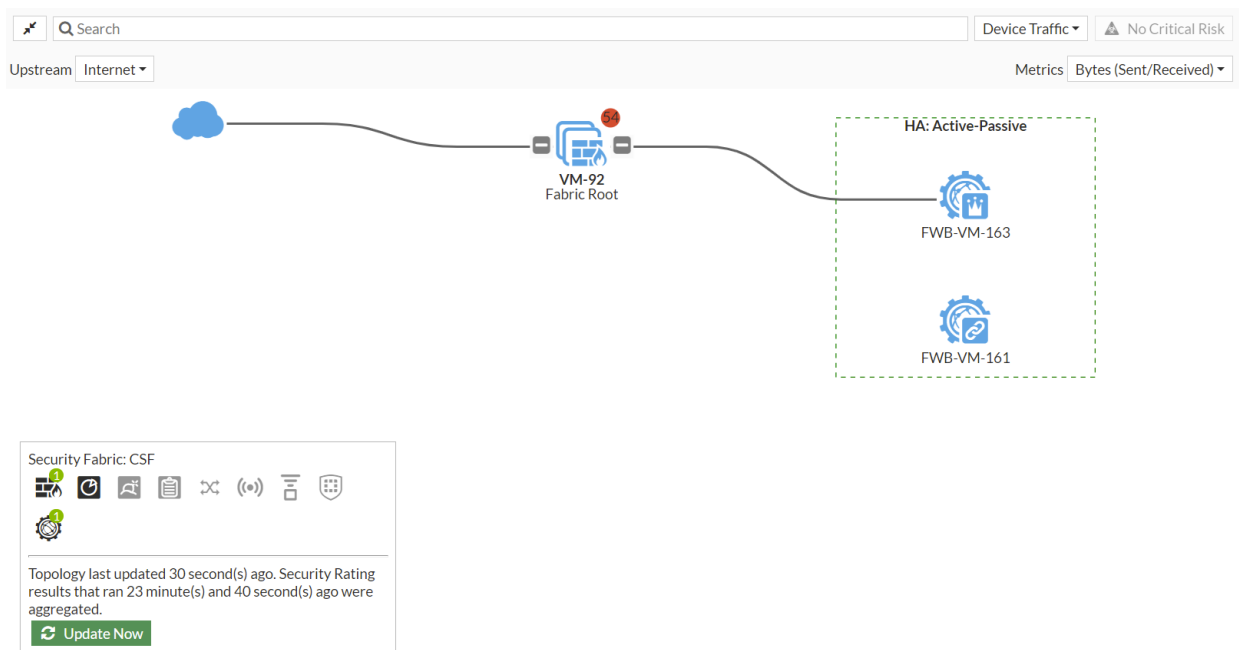
- Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
- Beside *Device authorization*, click *Edit*. The *Device authorization* pane opens.
- Add the FortiWeb:
 - Click *Create New* and enter a device name.
 - For *Authorization type*, select *Certificate*.

- c. Click *Browse* to upload the certificate.
- d. For *Action*, select *Accept*.
- e. Click *OK*. The FortiWeb appears in the table.

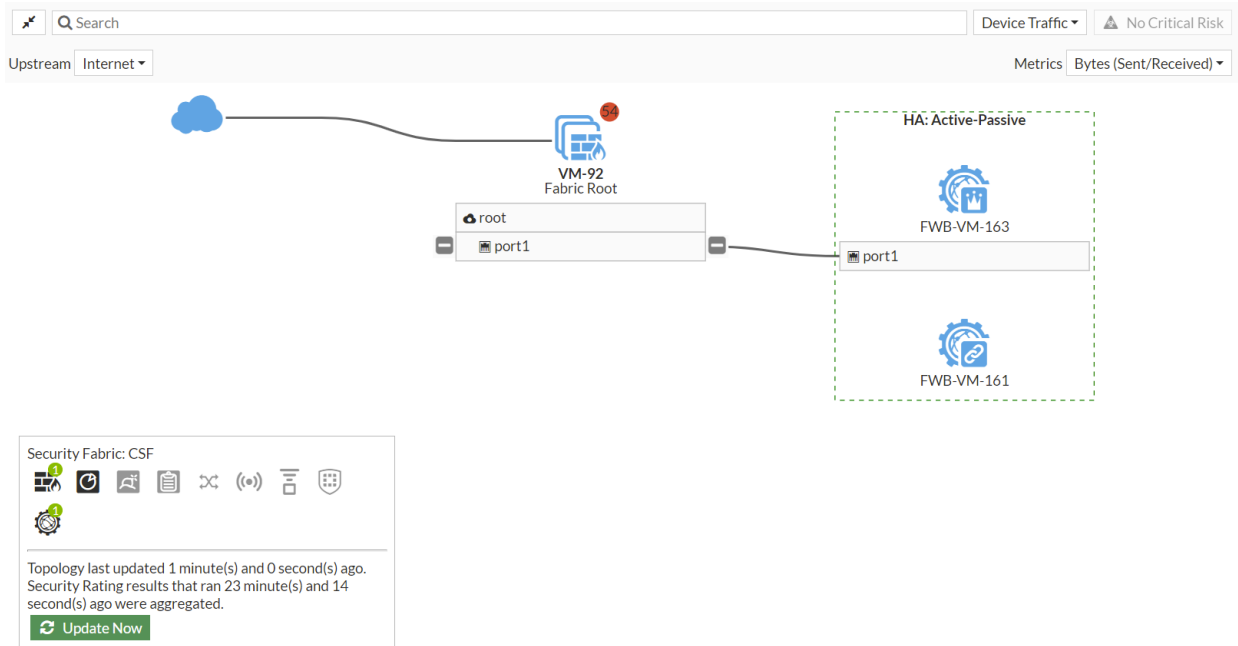
The screenshot shows the 'Edit Fabric Connector' window with the 'Device Authorization' tab selected. The table below shows the authorized devices:

Device	Type	Status	Authorization Type	Serial Number
FWB-VM-163	FortiWeb	Connected	Certificate	

4. Go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology* to view more information.
- Physical topology view:



Logical topology view:



To add a Fabric Device widget for FortiWeb:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *Security Fabric* section, click the + beside *Fabric Device*.
3. For *Device*, select the FortiWeb.
4. Select a *Widget name* and *Visualization type* from the dropdowns.
5. Click *Add Widget* and click *Close*. The *Fabric Device* widget is displayed in the dashboard. This example has a widget with *System Information* and a key-value pair.

[+ Add Widget](#)

System Information - FWB-VM-163

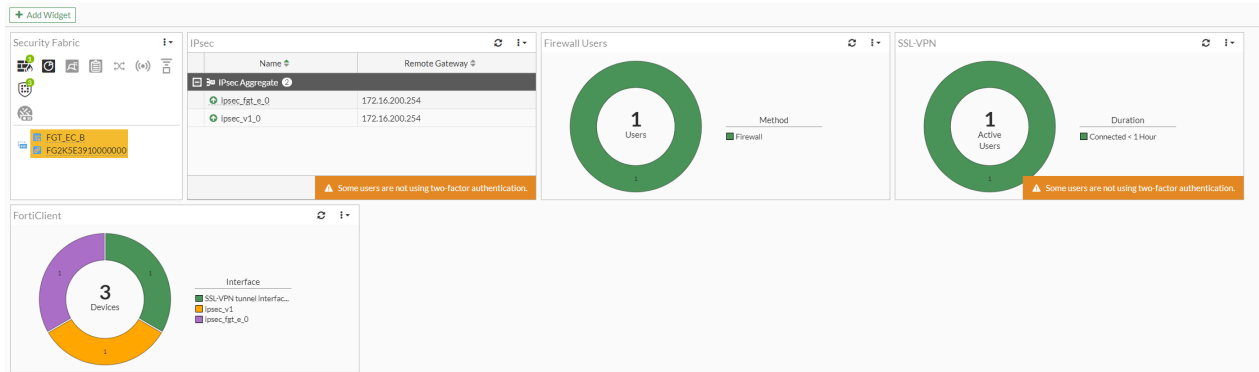
Module	FortiWeb-VM
HA Status	Active-Passive
Firmware Version	FortiWeb-VM 6.35
Host Name	FWB-VM-163
Serial Number	FVVM010000200000
Operation Mode	Reverse Proxy
Support Contract	Register
FortiSandbox Appliance	Disconnected

Show detailed user information about clients connected over a VPN through EMS

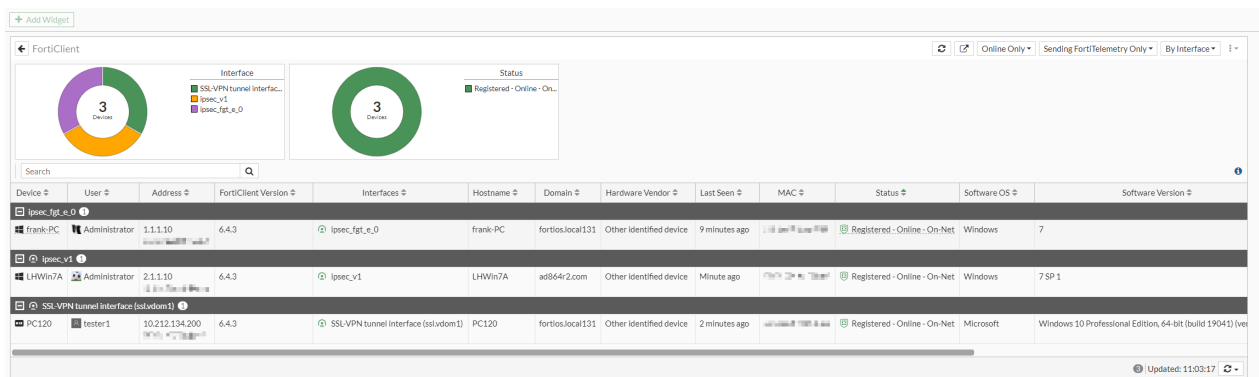
When managed clients are connected over a VPN, EMS collects user information about these registered clients, such as the VPN connection information. The FortiGate can synchronize this user information from EMS and display it in the *FortiClient* widget and logical topology view to provide a detailed picture of clients and their associated VPN interfaces.

To add the FortiClient widget:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *User & Authentication* section, click the + beside *FortiClient*.
3. Click *Add Widget* and click *Close*. The *FortiClient* widget is displayed in the dashboard.

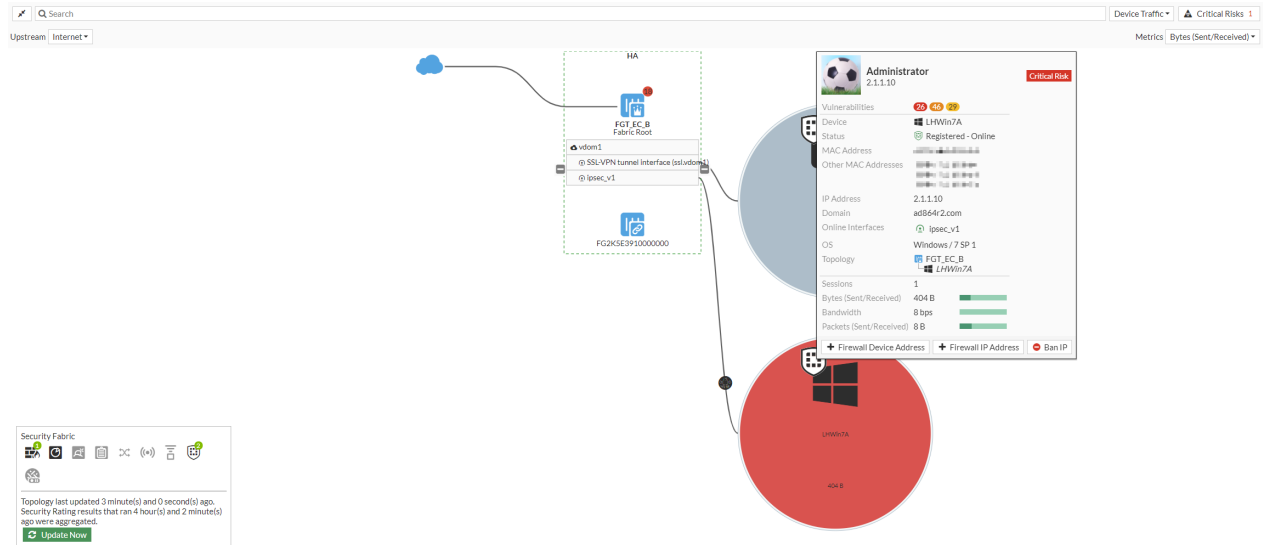


4. Hover over the widget, and click *Expand to Full Screen* to view more information about the clients and associated VPN interfaces.

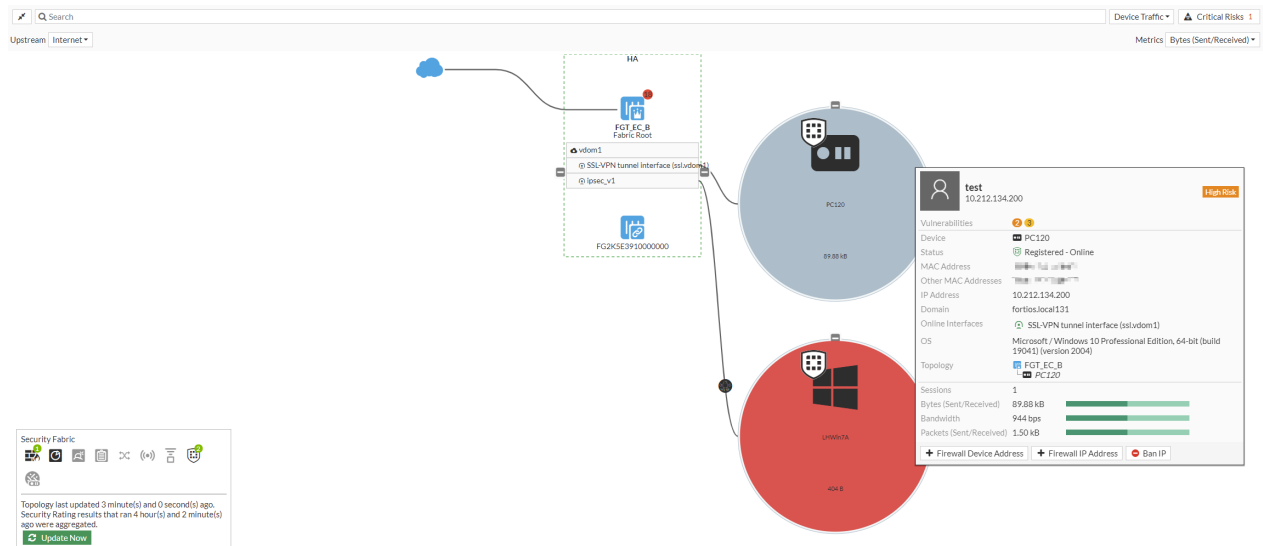


To view the logical topology:

1. Go to *Security Fabric > Logical Topology*.
 2. Hover over a client to view more information.
- Client using IPsec VPN interface:



Client using SSL VPN interface:



FortiDeceptor as a Security Fabric device


FortiDeceptor can be added to the Security Fabric so it appears in the topology views and the dashboard widgets.

To add FortiDeceptor to the Security Fabric in the GUI:

1. Enable the Security Fabric and configure the interface to allow other Security Fabric devices to join (see [Configuring the root FortiGate and downstream FortiGates](#) in the FortiOS Administration Guide).

Edit Fabric Connector

Core Network Security



Security Fabric Setup

Security Fabric Settings

Status: Enabled Disabled

Security Fabric role: Serve as Fabric Root Join Existing Fabric

Fabric name:

Allow other Security Fabric devices to join: ☒ wan1 +

Device authorization: None Edit

Allow downstream device REST API access: ☐

SAML Single Sign-On: ☐ Advanced Options

Management IP/FQDN: ☐ Use WAN IP Specify

Management port: Use Admin Port Specify

Topology

FGTD (Fabric Root)

Security Rating Issues

Show Dismissed: ☐

Additional Information

API Preview

Edit in CLI

SAML SSO

Guides

[Configure SAML Single Sign-On in the Security Fabric](#)

Documentation

[Online Help](#)

[Video Tutorials](#)

[How to Setup FortiClient EMS](#)

OK Cancel

2. In FortiDeceptor, integrate the device:
 - a. Go to *Fabric > Integration Devices*.
 - b. Click *Quarantine Integration With New Device*.
 - c. Click the toggle to enable the device.
 - d. For *Upstream IP Address*, enter the root FortiGate's management IP address.

Fabric Upstream

Enabled: ☒

Upstream IP Address: Port:

Authorization Status: The device is waiting to be authorized by upstream. [FGT81ETK18000000]

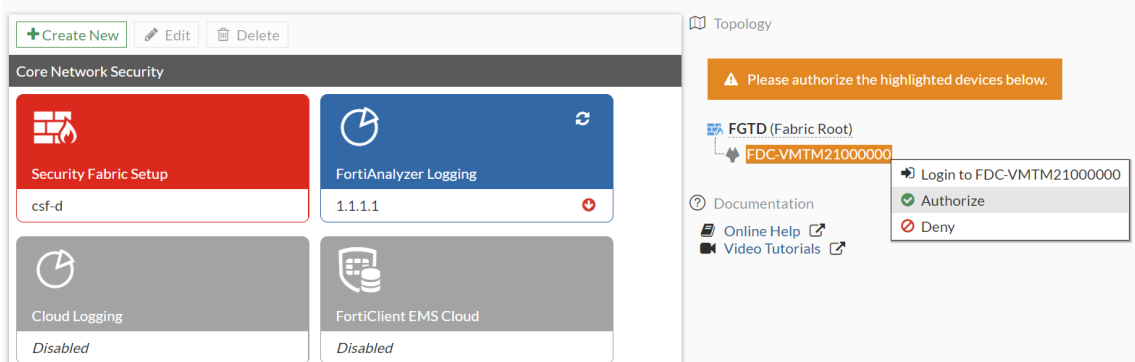
Apply Cancel

+ Quarantine Integration With New Device

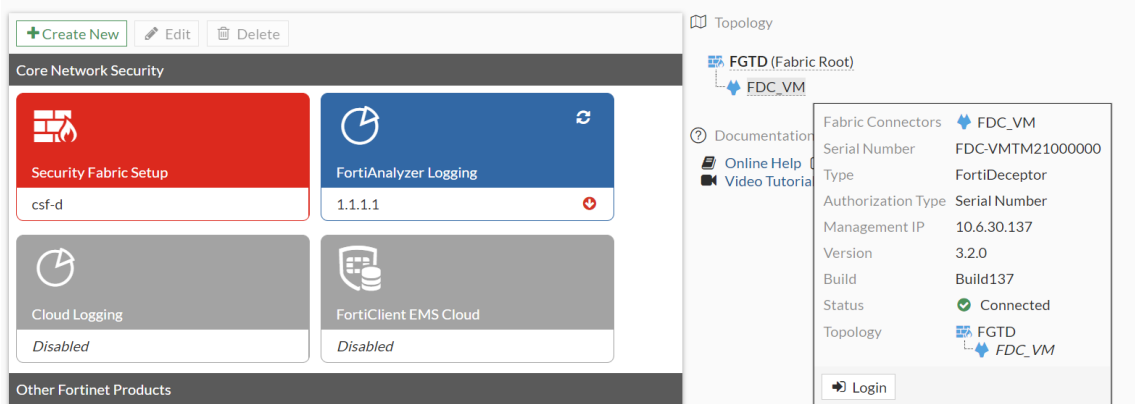
Action	Enabled	Status	Name	Appliance	Integrate Meth...	Severi...	Detail
No records found.							

- e. Click *Apply*.

3. Authorize the FortiDeceptor in FortiOS:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. In the topology tree, click the highlighted FortiDeceptor serial number and select *Authorize*.



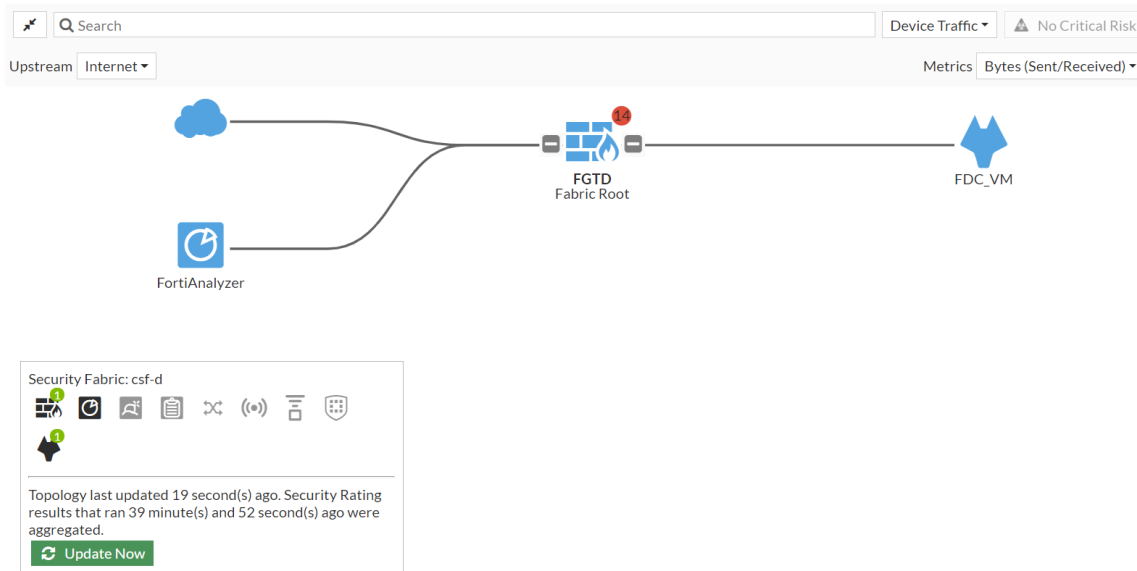
The authorized device appears in the topology tree. Hover over the device name to view the tooltip.



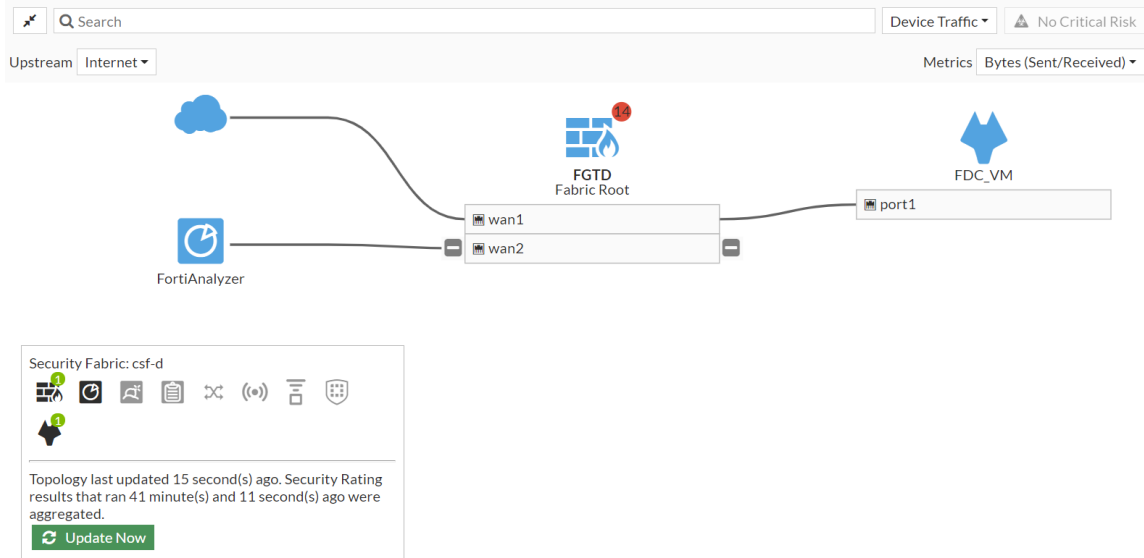
The *Security Fabric* widget on the dashboard also updates when the FortiDeceptor is authorized.

4. Go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology* to view more information.

Physical topology view:



Logical topology view:



To add a Fabric Device widget for FortiDeceptor:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *Security Fabric* section, click the + beside *Fabric Device*.
3. For *Device*, select the FortiDeceptor.
4. Select a *Widget name* and *Visualization type* from the dropdowns. *System Info* and *Key-Value Pair* are used in this example.
5. Click *Add Widget* and click *Close*. The *Fabric Device* widget is displayed in the dashboard.

The screenshot shows the FortiGate dashboard with the Security Fabric section expanded. It includes several widgets:

- System Information:** Hostname: FGTD, Serial Number: FGT81ETK18000000, Firmware: v7.0.0, Mode: NAT, System Time: 2021/03/16 17:24:55, Uptime: 00:08:21:42, WAN IP: 208.91.115.10.
- Licenses (173.243.140.6):** FortiCare Support, Firmware & General Updates, AntiVirus, Web Filtering, Security Rating, FortiToken 0/2.
- Security Fabric: csf-d:** Shows a topology diagram with FGTD (Fabric Root) and FDC_VM.
- Administrators:** 3 HTTPS, 0 FortiExplorer, admin super_admin.
- System Info - FDC_VM:** Hostname: FDC_VM, Appliance Mode: Standalone, Version: 3.2.0, Build: 0137, Serial Number: FDC-VMTM21000000, Model: FDC-VM.

To add FortiDeceptor to the Security Fabric in the CLI:

1. Configure the interface to allow other Security Fabric devices to join:

```
config system interface
edit "wan1"
```



```
...
set allowaccess ping https ssh snmp http fabric
...
next
end
```

2. Enable the Security Fabric:

```
config system csf
  set status enable
  set group-name "csf-d"
end
```

3. In FortiDeceptor, integrate the device:

- a. Go to *Fabric > Integration Devices*.
- b. Click *Quarantine Integration With New Device*.
- c. Click the toggle to enable the device.
- d. For *Upstream IP Address*, enter the root FortiGate's management IP address.
- e. Click *Apply*.

4. Authorize the FortiDeceptor in FortiOS:

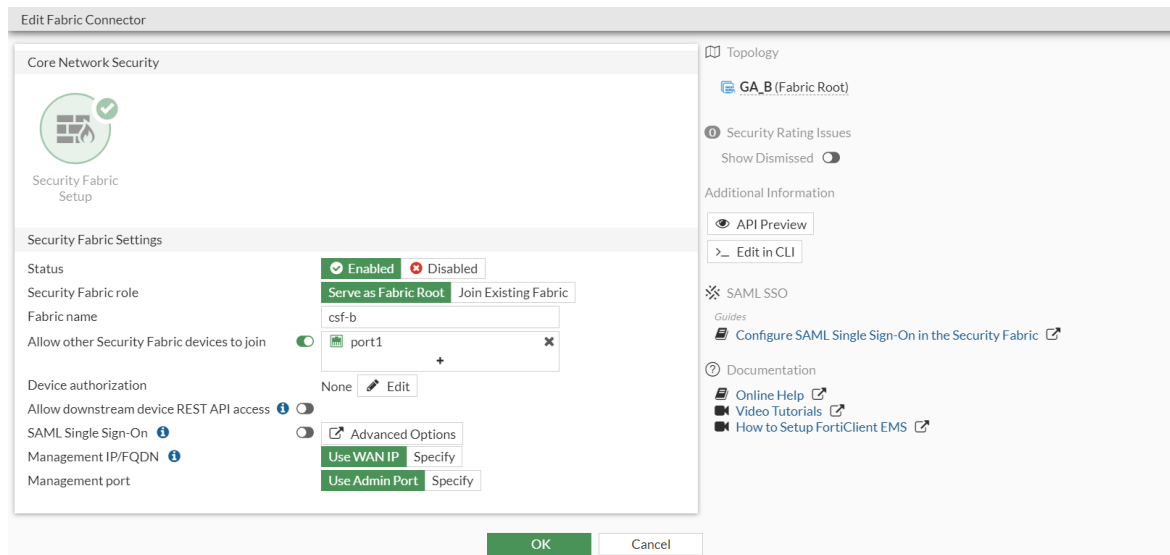
```
config system csf
  set status enable
  set group-name "csf-d"
  config trusted-list
    edit "FDC-VM2M21000000"
      set serial "FDC-VM2M21000000"
    next
  end
end
```

Add FortiAI as a Security Fabric device

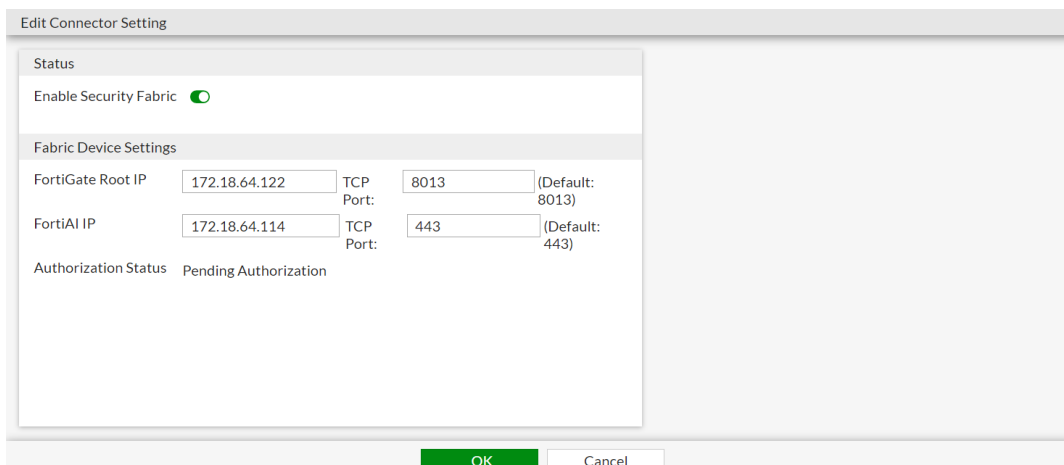
FortiAI can be added to the Security Fabric so it appears in the topology views and the dashboard widgets.

To add FortiAI to the Security Fabric in the GUI:

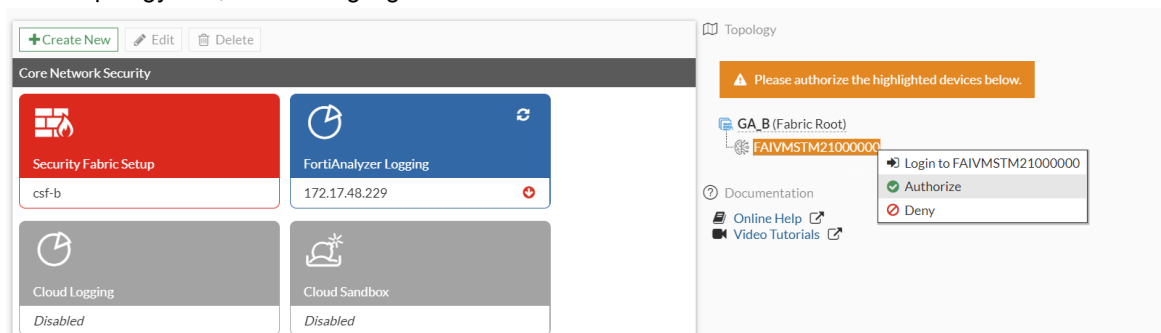
1. Enable the Security Fabric and configure the interface to allow other Security Fabric devices to join (see [Configuring the root FortiGate and downstream FortiGates](#) in the FortiOS Administration Guide).



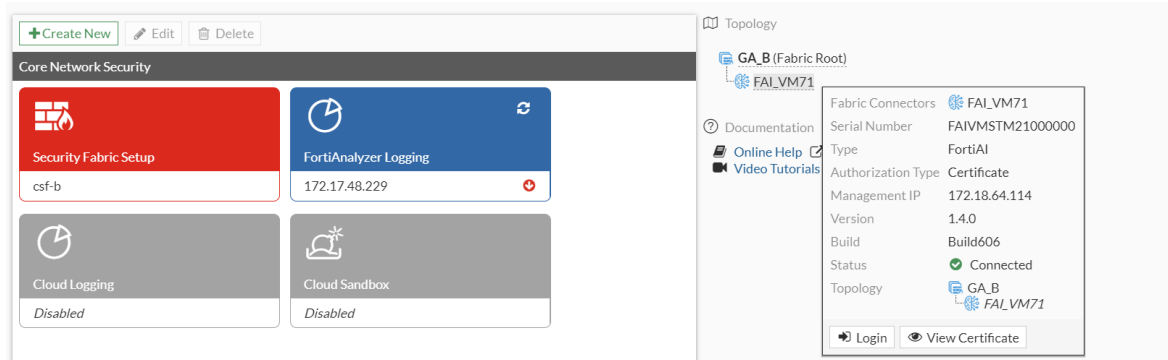
2. In FortiAI, configure the device to join the Security Fabric:
 - a. Go to *Security Fabric > Fabric Connectors* and double-click the connector card.
 - b. Click the toggle to *Enable Security Fabric*.
 - c. Enter the *FortiGate Root IP* address and the *FortiAI IP* address.



- d. Click **OK**.
3. Authorize the FortiAI in FortiOS:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. In the topology tree, click the highlighted FortiAI serial number and select *Authorize*.



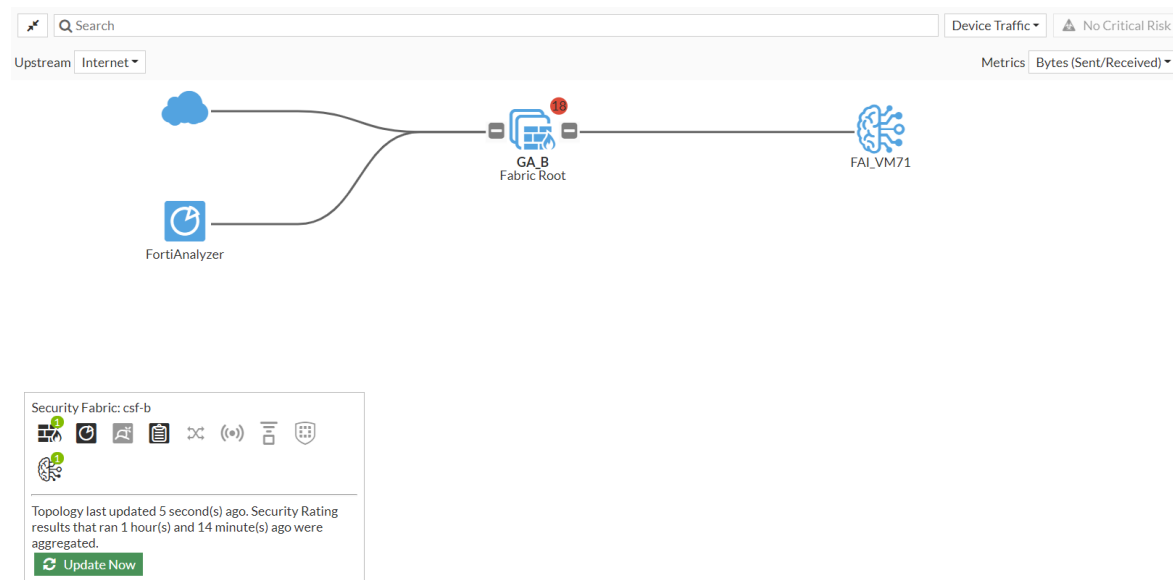
The authorized device appears in the topology tree. Hover over the device name to view the tooltip.



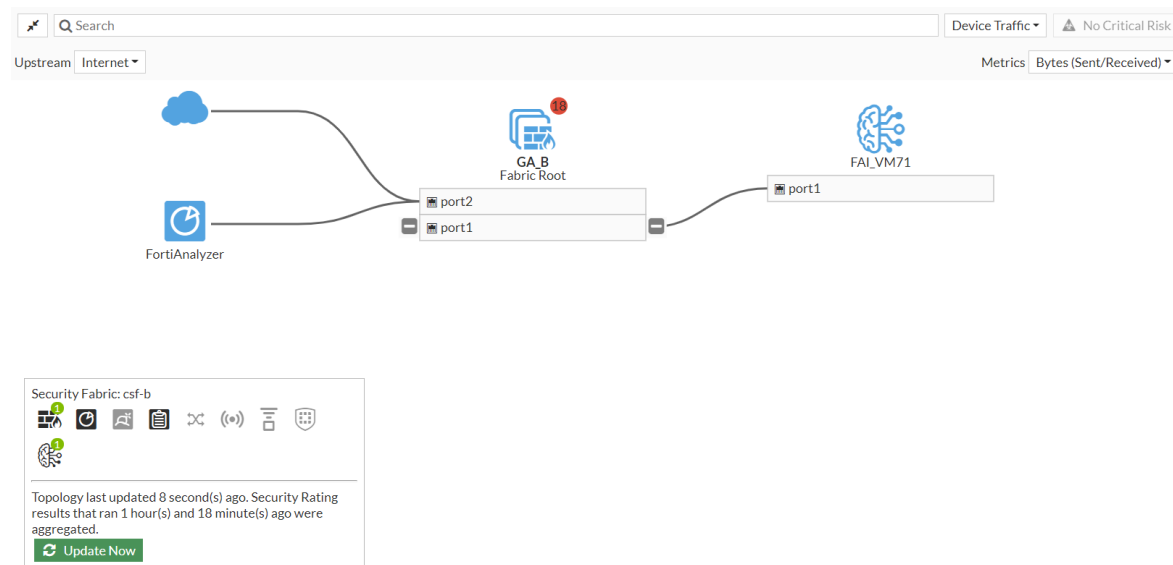
The *Security Fabric* widget on the dashboard also updates when the FortiAI is authorized.

4. Go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology* to view more information.

Physical topology view:

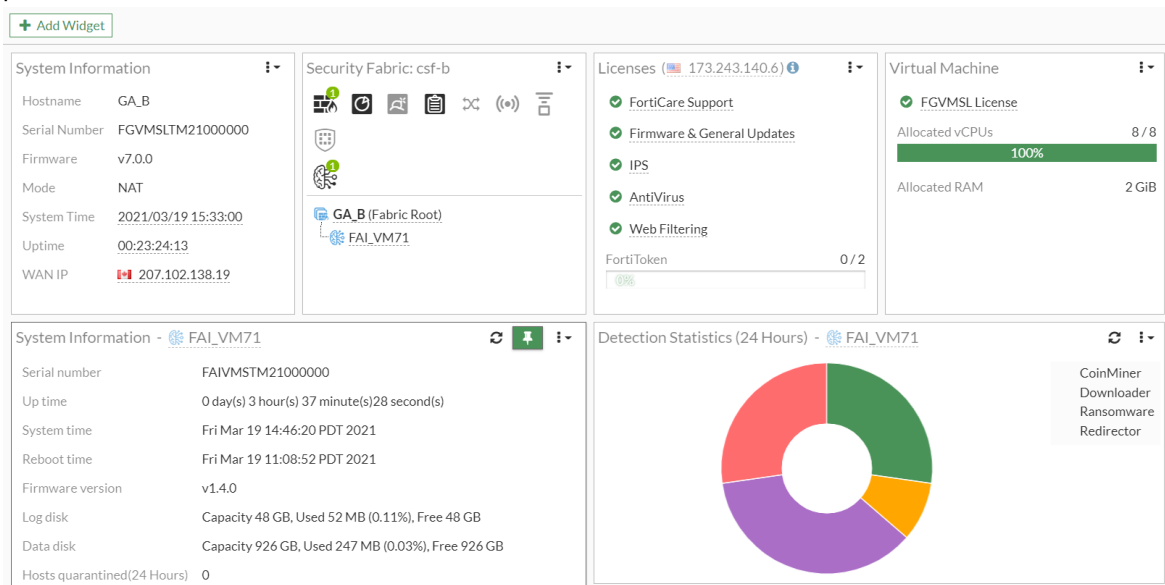


Logical topology view:



To add a Fabric Device widget for FortiAI:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *Security Fabric* section, click the + beside *Fabric Device*.
3. For *Device*, select the FortiAI.
4. Select a *Widget name* and *Visualization type* from the dropdowns.
5. Click *Add Widget* and click *Close*. The *Fabric Device* widget is displayed in the dashboard. This example has two widgets: one with *System Information* and a key-value pair, and another with *Destination Statistics (24 Hours)* and a pie chart.



To add FortiAI to the Security Fabric in the CLI:

1. Configure the interface to allow other Security Fabric devices to join:

```
config system interface
  edit "port1"
    ...
    set allowaccess ping https ssh http fgfm fabric
    ...
  next
end
```

2. Enable the Security Fabric:

```
config system csf
  set status enable
  set group-name "csf-b"
end
```

3. In FortiAI, configure the device to join the Security Fabric:

```
config system csf
  set status enable
  set upstream-ip 172.18.64.122
  set management-ip 172.18.64.114
end
```

4. Authorize the FortiAI in FortiOS:

```
config system csf
    set status enable
    set group-name "csf-b"
    config trusted-list
        edit "FAIVMSTM21000000"
            set authorization-type certificate
            set certificate "*****"
        next
    end
end
```

Improve communication performance between EMS and FortiGate with WebSockets

The performance of updates between the FortiGate and FortiClient EMS is improved by using WebSockets. On supported FortiClient EMS firmware, the FortiGate can open a WebSocket connection with EMS to register for notifications about system information, host tags, avatars, and vulnerabilities. When these tables are updated, EMS pushes notifications to the corresponding FortiGate. The FortiGate then fetches the updated information using the REST API.

When WebSockets are not used (due to an override or unsupported EMS version), updates are triggered on demand from the FortiGate side over the REST API. If the WebSocket capability is detected, the capabilities setting will automatically display the WebSocket option. Users can also use the `diagnose test application fcnacd 2` command to view the status of the WebSocket connection.

Example

WebSockets can be used in a scenario using ZTNA tags. When a FortiClient detects changes in the endpoint client, this information is sent to EMS. EMS may re-tag the client, so a quick notification to the FortiGate and corresponding REST API call from the FortiGate to EMS means the turnaround for the FortiGate to synchronize with current the FortiClient status is much quicker.

To use the WebSocket service:

1. Configure the EMS entry:

```
config endpoint-control fctems
    edit "ems139"
        set fortinetone-cloud-authentication disable
        set server "172.16.200.139"
        set https-port 443
        set source-ip 0.0.0.0
        set pull-sysinfo enable
        set pull-vulnerabilities enable
        set pull-avatars enable
        set pull-tags enable
        set pull-malware-hash enable
        unset capabilities
        set call-timeout 30
        set websocket-override disable
    end
end
```

```
    next
end
```

When the entry is created, the capabilities are unset by default.

2. Authenticate the FortiGate with EMS:

```
# execute fctems verify ems_139
...
```

The FortiGate will enable the WebSocket server based on the EMS supported capabilities.

```
config endpoint-control fctems
  edit "ems139"
    set server "172.18.62.12"
    set capabilities fabric-auth silent-approval websocket
  next
end
```

To verify the WebSocket connection status:

```
# diagnose test application fcnacd 2
EMS context status:
```

```
FortiClient EMS number 1:
  name: ems139 confirmed: yes
  fetched-serial-number: FCTEMS8821000000
```

Websocket status: connected

```
Object ID: 0, base-path: api/v1/system/serial_number, priority: 0.
Description: REST API to get EMS Serial Number..
Not a valid object.
Object ID: 2, base-path: api/v1/fabric_device_auth/fortigate, priority: 3.
Description: REST API to send updates regarding FortiGate Serial numbers..
Not a valid object.
Object ID: 4, base-path: api/v1/fgt/gateway_details/gateway_mac, priority: 3.
Description: REST API to send Gateway MAC info.
Object ID: 5, base-path: api/v1/fgt/gateway_details/vpn, priority: 2.
Description: REST API to send updated regarding VPN updates..
Object ID: 6, base-path: api/v1/report/fct/sysinfo, priority: 4.
Description: REST API to get updates about system info..
Object ID: 7, base-path: api/v1/report/fct/vuln, priority: 5.
Description: REST API to get updates about vulnerabilities..
Object ID: 8, base-path: api/v1/report/fct/avatar, priority: 3.
Description: REST API to get updates about avatars..
Object ID: 9, base-path: api/v1/report/fct/host_tags, priority: 2.
Description: REST API to get updates about host tags..
Object ID: 10, base-path: api/v1/malware/hash, priority: 4.
Description: REST API to get updates about malware hashes.
Object ID: 11, base-path: api/v1/clients/action, priority: 3.
Description: REST API to send client actions.
Object ID: 12, base-path: api/v1/report/fct/subscribe, priority: 3.
Description: REST API to subscribe to/unsubscribe from different UIDs..
Object ID: 13, base-path: api/v1/ztna_certificates/download, priority: 3.
Description: REST API to get ZTNA certificate..
Object ID: 14, base-path: api/v1/settings/server/websocket_port, priority: 3.
Description: REST API to send updates regarding FortiGate Serial numbers..
```

```
Worker 0 is idle.
Worker 1 is idle.
```

Simplify EMS pairing with Security Fabric so one approval is needed for all devices

FortiClient EMS with Fabric authorization and silent approval capabilities will be able to approve the root FortiGate in a Security Fabric once, and then silently approve remaining downstream FortiGates in the Fabric. Similarly in an HA scenario, an approval only needs to be made once to the HA primary unit. The remaining cluster members are approved silently.

To use EMS silent approval:

1. Configure the EMS entry on the root FortiGate or HA primary:

```
config endpoint-control fcitems
  edit "ems139"
    set fortinetone-cloud-authentication disable
    set server "172.16.200.139"
    set https-port 443
    set source-ip 0.0.0.0
    set pull-sysinfo enable
    set pull-vulnerabilities enable
    set pull-avatars enable
    set pull-tags enable
    set pull-malware-hash enable
    unset capabilities
    set call-timeout 30
    set websocket-override disable
  next
end
```

When the entry is created, the capabilities are unset by default.

2. Authenticate the FortiGate with EMS:

```
# execute fcitems verify ems_139
...
```

The FortiGate will enable the Fabric authorization and silent approval based on the EMS supported capabilities.

```
config endpoint-control fcitems
  edit "ems139"
    set server "172.18.62.12"
    set capabilities fabric-auth silent-approval websocket
  next
end
```

3. Configure a downstream device in the Security Fabric (see [Configuring the root FortiGate and downstream FortiGates](#) for more details). The downstream device will be silently approved.
4. Configure a secondary device in an HA system (see [HA active-passive cluster setup](#) and [HA active-active cluster setup](#) for more details). The secondary device will be silently approved.

FortiTester as a Security Fabric device - 7.0.1

FortiTester can be added to the Security Fabric and authorized from the Security Fabric topology views. Once added, the FortiTester will appear in the *Security Fabric* widget on the dashboard. A FortiTester can be added to the dashboard as a Fabric device widget.

To add FortiTester to the Security Fabric in the GUI:

1. Enable the Security Fabric and configure the interface to allow other Security Fabric devices to join (see [Configuring the root FortiGate and downstream FortiGates](#) in the FortiOS Administration Guide).

Edit Fabric Connector

Core Network Security

Security Fabric Setup

Security Fabric Settings

Status: Enabled Disabled

Security Fabric role: Serve as Fabric Root Join Existing Fabric

Fabric name:

Allow other Security Fabric devices to join: Enabled

Device authorization: 0 Connected / 2 Total Edit

Allow downstream device REST API access: Enabled

SAML Single Sign-On: Enabled Advanced Options

Mode: Identity Provider (IdP)

IdP certificate: Download

Management IP/FQDN: Use WAN IP Specify

Management port: Use Admin Port Specify

OK Cancel

Topology

FGT-F-1 (Fabric Root)

Security Rating Issues

Show Dismissed Off

Additional Information

API Preview

Edit in CLI

SAML SSO

Guides

[Configure SAML Single Sign-On in the Security Fabric](#)

Documentation

[Online Help](#) [Video Tutorials](#) [How to Setup FortiClient EMS](#)

2. In FortiTester, enable the Security Fabric:
 - a. Go to *System Settings > Security Fabric > Settings*.
 - b. Click the toggle to enable the device (*Enable Security Fabric*).
 - c. Enter the *FortiGate Root IP Address*.

Edit Connector Setting

Status

Enable Security Fabric Enabled

Fabric Device Settings

FortiGate Root IP Address:

FortiTester Management IP Address: Port:

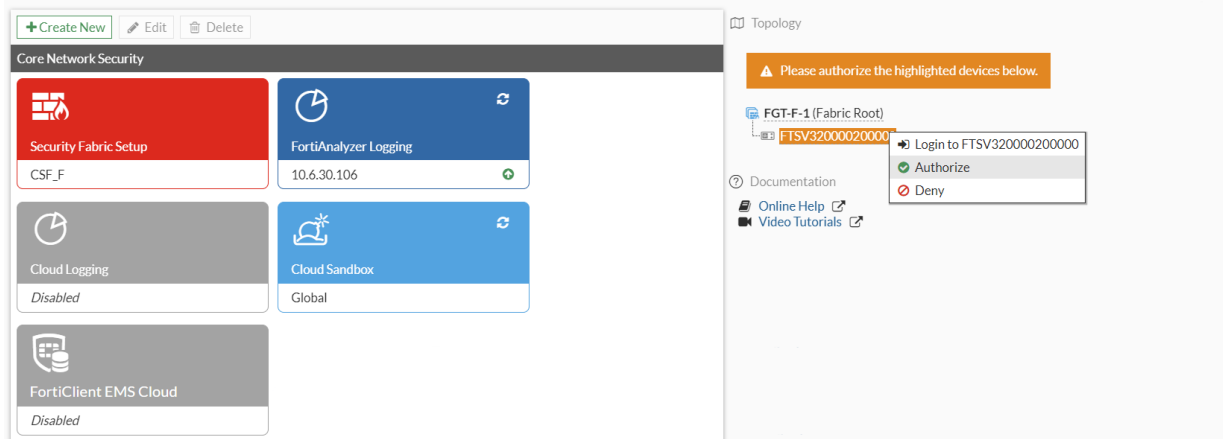
Authorization Status: Pending Authorization

Apply

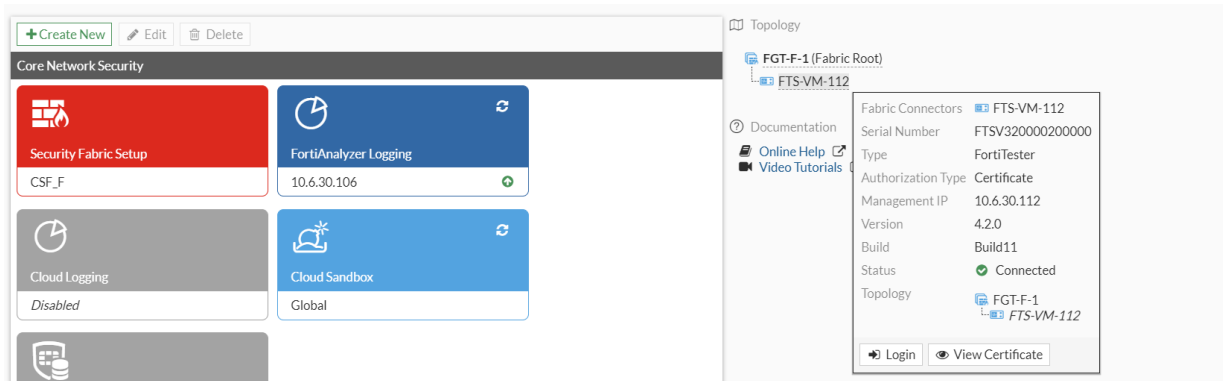
- d. Click *Apply*.

3. Authorize the FortiTester in FortiOS:

- a. Go to *Security Fabric > Fabric Connectors*.
- b. In the topology tree, click the highlighted FortiTester serial number and select *Authorize*.

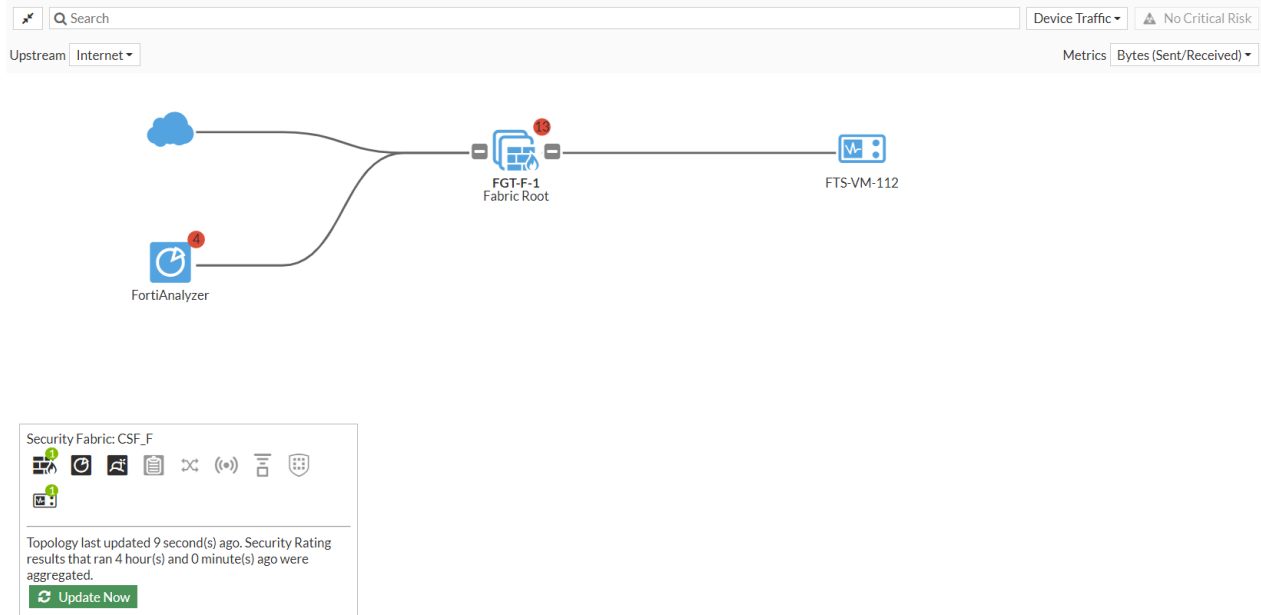


The authorized device appears in the topology tree. Hover over the device name to view the tooltip.

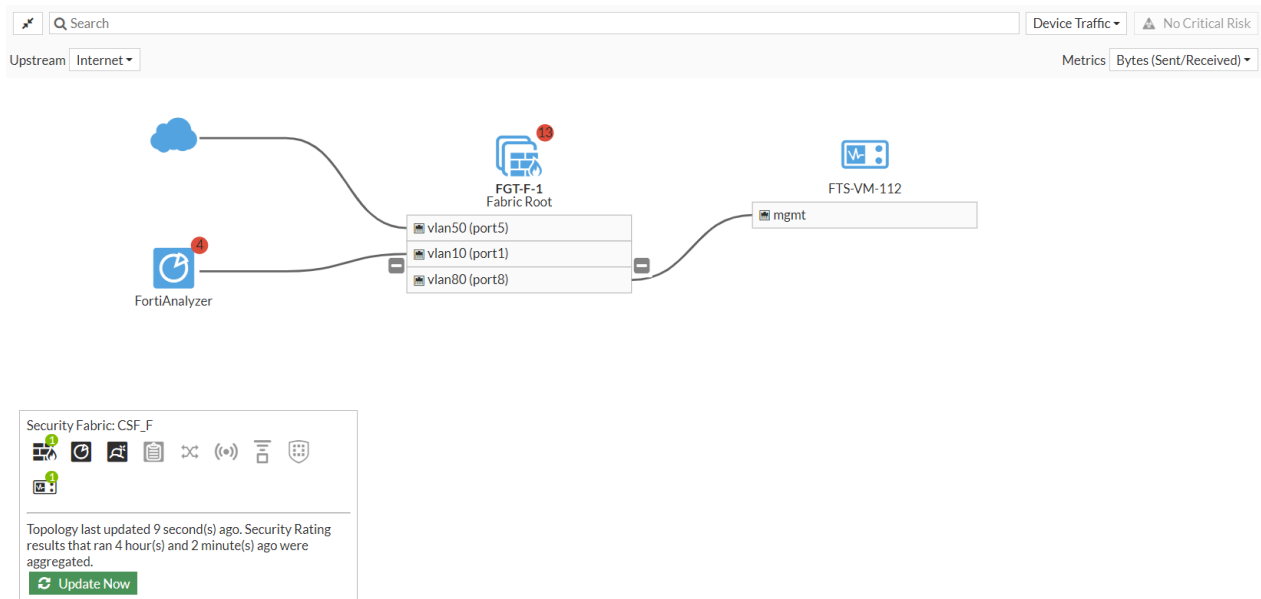


The *Security Fabric* widget on the dashboard also updates when the FortiTester is authorized.

4. Go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology* to view more information.
Physical topology view:



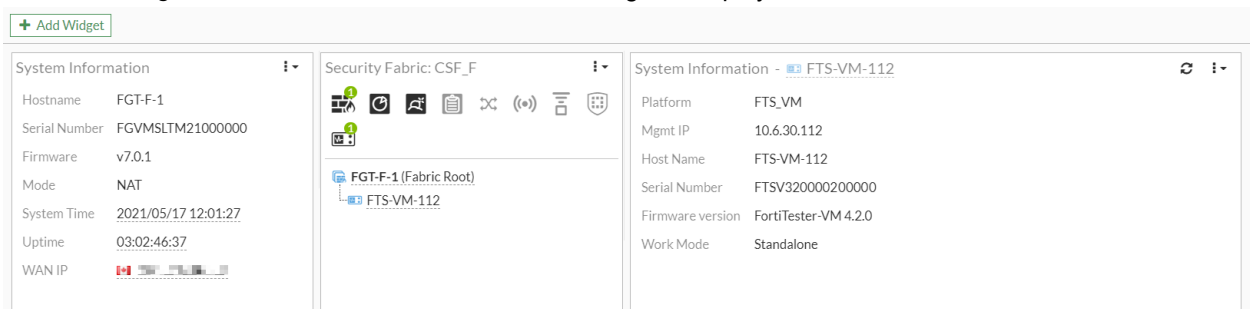
Logical topology view:



To add a Fabric Device widget for FortiTester:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *Security Fabric* section, click the + beside *Fabric Device*.
3. For *Device*, select the FortiTester.
4. Select a *Widget name* and *Visualization type* from the dropdowns. *System Information* and *Key-Value Pair* are used in this example.

5. Click **Add Widget** and click **Close**. The **Fabric Device** widget is displayed in the dashboard.



To add FortiTester to the Security Fabric in the CLI:

1. Configure the interface to allow other Security Fabric devices to join:

```
config system interface
    edit "port8"
        ...
        set allowaccess ping https ssh http fgfm fabric
        ...
    next
end
```

2. Enable the Security Fabric:

```
config system csf
    set status enable
    set group-name "CSF_F"
end
```

3. In FortiTester, enable the Security Fabric:

```
config system csf
    set ip 172.16.116.230
    set port 8013
    set status enable
end
```

4. Authorize the FortiTester in FortiOS:

```
config system csf
    set status enable
    set group-name "CSF_F"
    config trusted-list
        edit "FTSV320000200000"
            set authorization-type certificate
            set certificate "*****"
        next
    end
end
```

Simplify Fabric approval workflow for FortiAnalyzer - 7.0.1

When connecting to FortiAnalyzer in the Security Fabric, an **Authorize** button is displayed when the FortiGate has not been authorized on the FortiAnalyzer side. This opens a shortcut to log in to the FortiAnalyzer and approve the FortiGate.

FortiAnalyzer 7.0.1 is required.

To authorize FortiAnalyzer:

1. In FortiAnalyzer, configure the authorization address and port:
 - a. Go to *System Settings > Admin > Admin Settings*.
 - b. In the *Fabric Authorization* section, enter an *Authorization Address* and *Authorization Port*. This is used to access the FortiAnalyzer login screen.

- c. Click *Apply*.
2. In FortiOS, go to *Security Fabric > Fabric Connectors* and double-click the *FortiAnalyzer Logging* card.
3. Enter the FortiAnalyzer IP.
4. Click *OK*. The *FortiAnalyzer Status* (in the right-side gutter) is *Unauthorized*.

5. Click *Authorize*. You are redirected to a login screen.
6. Enter the username and password, then click *Login*.


⚠ Not secure | 172.16.116.221:2443/fabric-authorization?opener_id=FGVMSLTM21000284



The authorization dialog opens.


7. Select **Approve** and click **OK** to authorize the FortiGate.

▲ Not secure | 172.16.116.221:2443/p/fabric-approval/


**Fortinet
Security
Fabric**

Select an action for the following unregistered devices.


Root-F-HA_FGVMSL
10.6.30.6

Model	FortiGate-VM64
Management Mode	Logging Only
Serial Number	FGVMSLTM- 
Firmware Version	FortiGate 7.0.1 (GA)

8. In FortiOS, refresh the *FortiAnalyzer Logging* page. The *FortiAnalyzer Status* is *Authorized*.

Edit Fabric Connector

Core Network Security



FortiAnalyzer
Logging


FortiAnalyzer Settings

Status: Enabled Disabled

IP address:

Upload option: Real Time Every Minute Every 5 Minutes

Allow access to FortiGate REST API: ☒

Verify FortiAnalyzer certificate: ☒ 

FortiAnalyzer Status

Connection: Connected

FortiAnalyzer Usage

Logging ADOM

root

Storage usage: 3.14 GiB / 50.00 GiB

Analytics usage: 3.13 GiB / 35.00 GiB

Archive usage: 4.57 MiB / 15.00 GiB

Security Rating Issues:

Allow deep inspection certificates to be synchronized to EMS and distributed to FortiClient - 7.0.1

On FortiClient EMS versions that support `push CA certs` capability, the FortiGate will push CA certificates used in SSL deep inspection to the EMS server. On the EMS server, the CA certificates can be selected in the managed endpoint profiles so they can be installed on managed endpoints. FortiClient EMS 7.0.1 is required to use this feature.

Example

To configure deep inspection certificate synchronization to EMS:

1. Configure the EMS Fabric connector:

```
config endpoint-control fctems
  edit "ems138"
    set fortinetone-cloud-authentication disable
    set server "172.16.200.138"
    set https-port 443
    set source-ip 0.0.0.0
    set pull-sysinfo enable
    set pull-vulnerabilities enable
    set pull-avatars enable
    set pull-tags enable
    set pull-malware-hash enable
    set capabilities fabric-auth silent-approval websocket websocket-malware push-
ca-certs
    set call-timeout 30
    set websocket-override disable
    set preserve-ssl-session disable
  next
end
```

2. Apply the certificate to an SSL/SSH profile for deep inspection:

```
config firewall ssl-ssh-profile
  edit "deep-inspection"
    set comment "Read-only deep inspection profile."
    config https
      set ports 443
      set status deep-inspection
    end
    ...
    set server-cert-mode re-sign
    set caname "Fortinet_CA_SSL"
    set untrusted-caname "Fortinet_CA_Untrusted"
  next
end
```

The default deep inspection profile, CA certificate, and untrusted CA certificates are used in this example.

3. Configure the firewall policy:

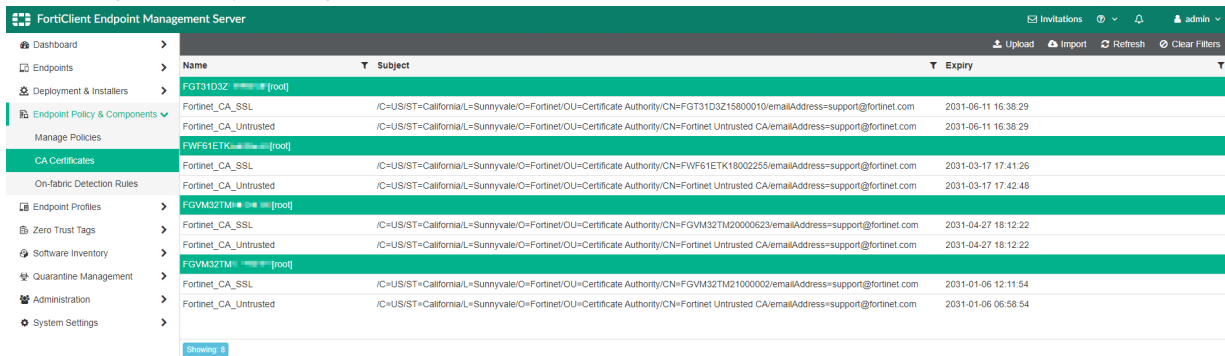
```
config firewall policy
  edit 1
    set name "deep-inspection"
    set srcintf "port14"
    set dstintf "port13"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode proxy
    set ssl-ssh-profile "deep-inspection"
  next
end
```

```

set av-profile "default"
set nat enable
next
end

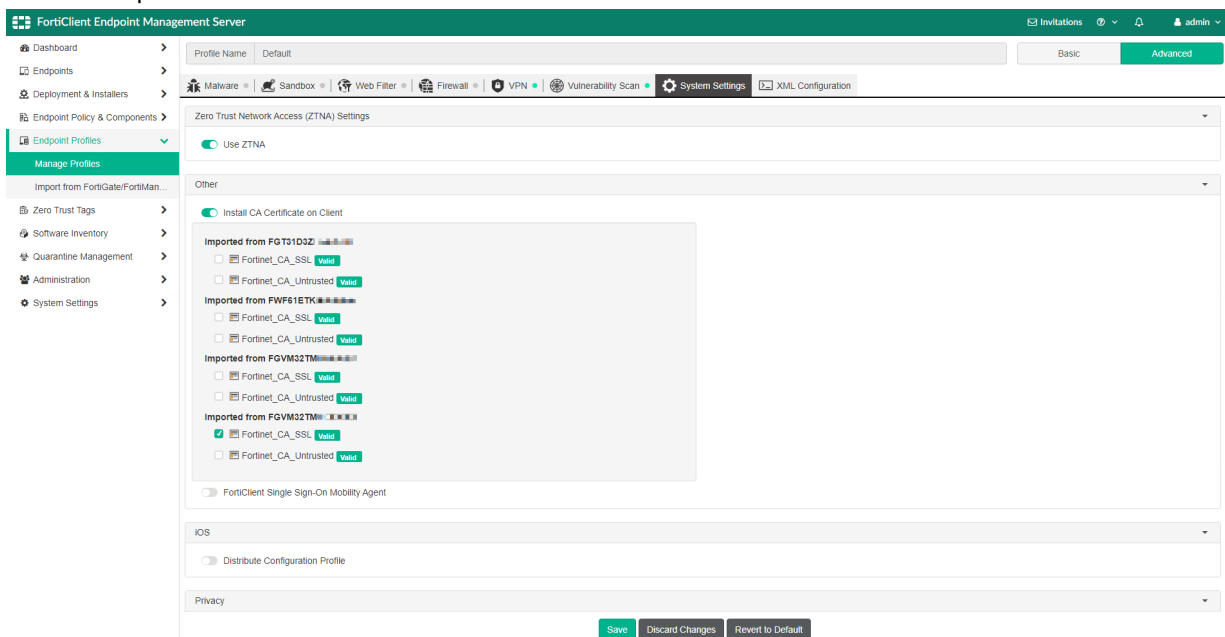
```

4. In EMS, verify that the CA certificate was pushed to EMS:
 - a. Go to *Endpoint Policy & Components > CA Certificates*.



Name	Subject	Expiry
FGT31D3Z	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=FGT31D3Z15800010/emailAddress=support@fortinet.com	2031-06-11 16:38:29
Fortinet_CA_SSL	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=Fortinet Untrusted CA/emailAddress=support@fortinet.com	2031-06-11 16:38:29
FWF61ETK	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=FWF61ETK18002255/emailAddress=support@fortinet.com	2031-03-17 17:41:26
Fortinet_CA_Untrusted	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=Fortinet Untrusted CA/emailAddress=support@fortinet.com	2031-03-17 17:42:48
FGVM32TM	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=FGVM32TM20000623/emailAddress=support@fortinet.com	2031-04-27 18:12:22
Fortinet_CA_SSL	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=Fortinet Untrusted CA/emailAddress=support@fortinet.com	2031-04-27 18:12:22
FGVM32TM	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=FGVM32TM21000002/emailAddress=support@fortinet.com	2031-01-06 12:11:54
Fortinet_CA_Untrusted	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=Fortinet Untrusted CA/emailAddress=support@fortinet.com	2031-01-06 06:58:54

- b. Verify the certificate table to see that the EMS server received the CA certification from the different FortiGates.
5. Select the CA certificate in the endpoint profile:
 - a. Go to *Endpoint Profiles > Manage Profiles* and edit a profile. The default profile is used in this example.
 - b. Click *Advanced* in the top right corner and click the *System Settings* tab.
 - c. In the *Other* section, enable *Install CA Certificate on Client* and select the *Fortinet_CA_SSL* certificate for the desired endpoint.



FortiClient Endpoint Management Server

Profile Name: Default

Basic Advanced

Malware Sandbox Web Filter Firewall VPN Vulnerability Scan System Settings XML Configuration

Zero Trust Network Access (ZTNA) Settings

☒ Use ZTNA

Other

☒ Install CA Certificate on Client

Imported from FGT31D3Z

☐ Fortinet_CA_SSL Valid

☐ Fortinet_CA_Untrusted Valid

Imported from FWF61ETK

☐ Fortinet_CA_SSL Valid

☐ Fortinet_CA_Untrusted Valid

Imported from FGVM32TM

☐ Fortinet_CA_SSL Valid

☐ Fortinet_CA_Untrusted Valid

Imported from FGVM32TM

☒ Fortinet_CA_SSL Valid

☐ Fortinet_CA_Untrusted Valid

☐ FortiClient Single Sign-On Mobility Agent

iOS

☐ Distribute Configuration Profile

Privacy

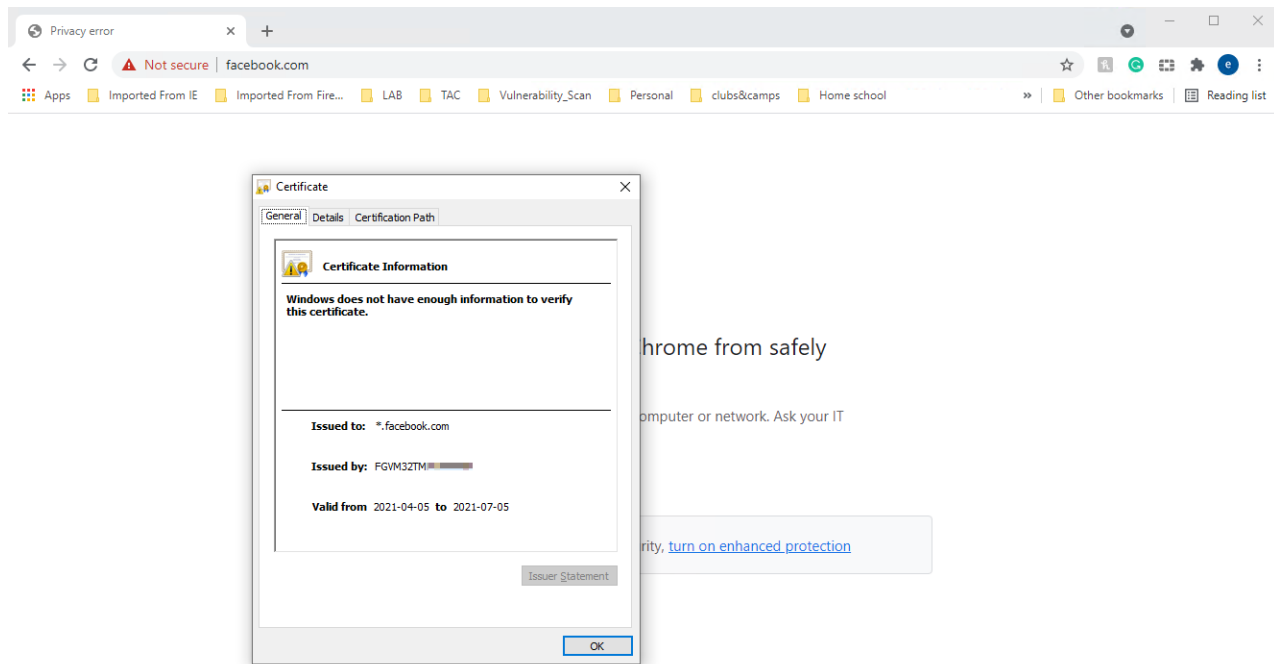
Save Discard Changes Revert to Default

- d. Click **Save**.
- Once the FortiClient endpoint is registered, it receives the CA certificate. When the FortiClient endpoint tries to access the internet through the FortiGate with the firewall policy that has deep inspection, no warning message is displayed. The server certificate is trusted with the installed CA certificate to complete the certificate chain.

Verification

Before configuring deep inspection certificate synchronization, a warning message is displayed when a FortiClient endpoint accesses the internet through the FortiGate with the firewall policy that has deep inspection. The FortiClient certificate store does not have the FortiGate's CA that is used in the deep inspection SSL/SSH profile.

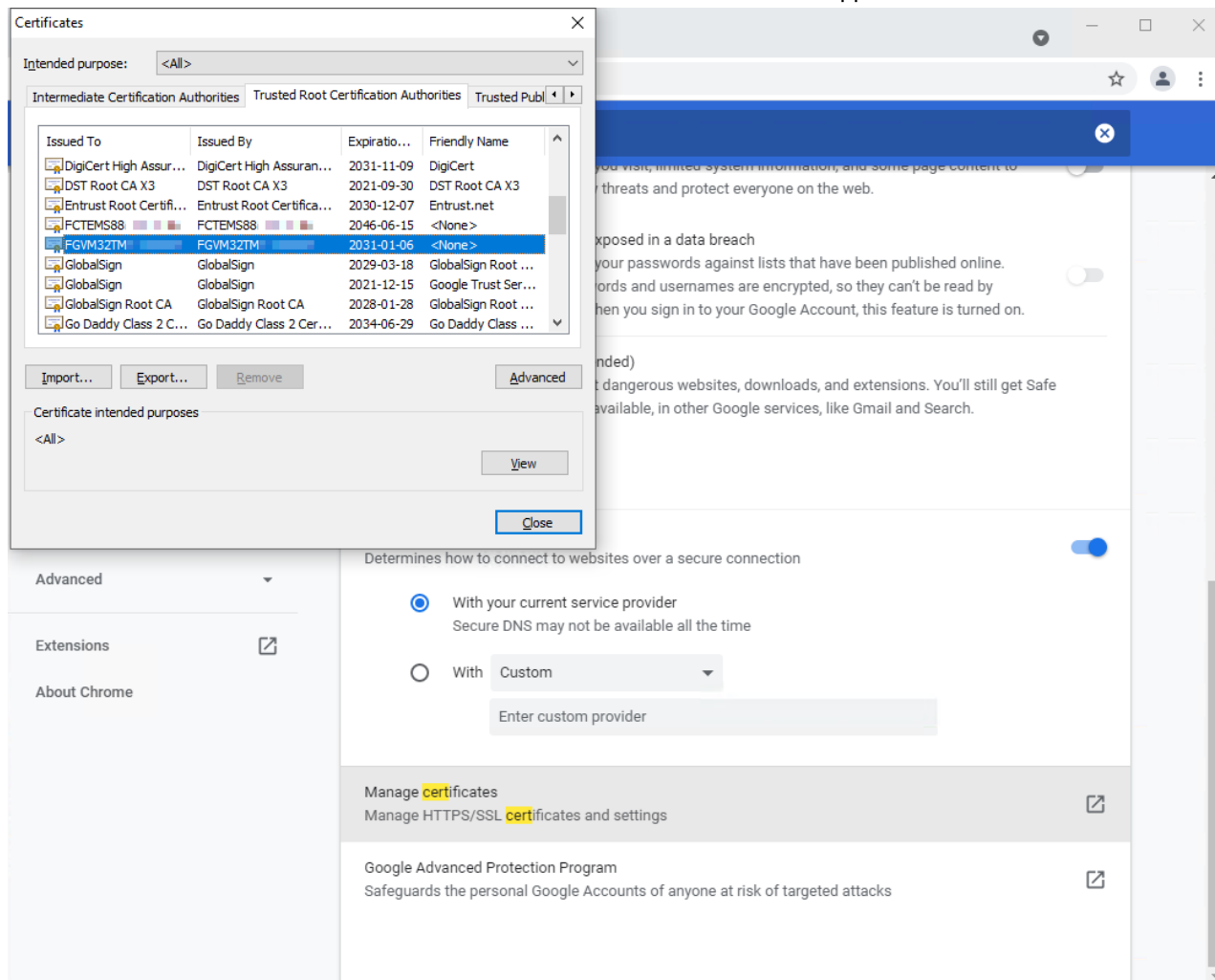
For example, accessing <https://www.facebook.com> in Chrome shows a warning. In the address bar, clicking *Not secure* > *Certificate* opens the *Certificate* dialog, which indicates that *Windows does not have enough information to verify the certificate*.



After the EMS profile is pushed to FortiClient endpoint, the expected FortiGate's certificate is shown in its certificate store.

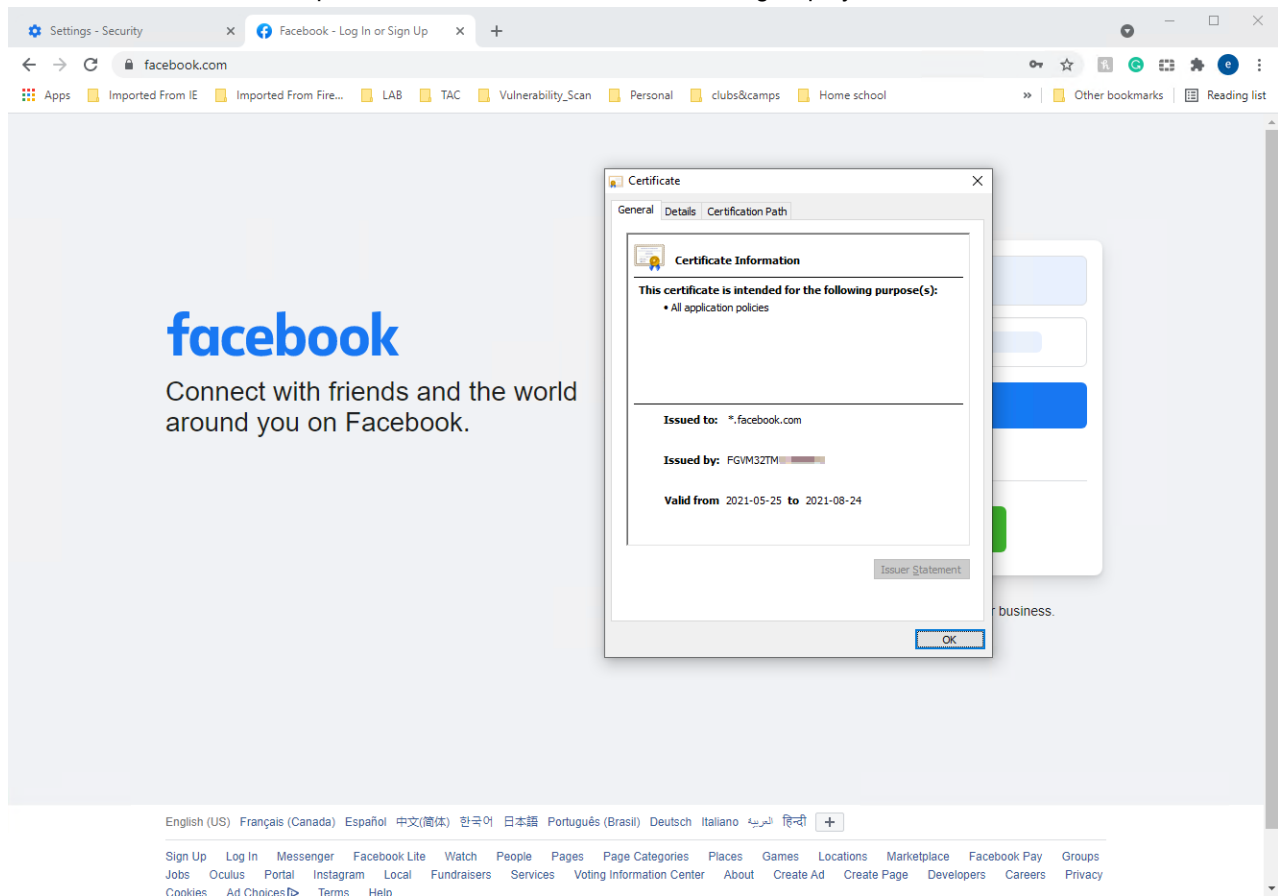
To verify the deep inspection certificate synchronization:

1. In Chrome, go to *Settings > Privacy and security* and open *Manage certificates*.
2. Click the *Trusted Root Certification Authorities* tab. The FortiGate's certificate appears in the list.



3. On the FortiClient endpoint using Chrome, go to <https://www.facebook.com>. The website is displayed.

4. In the address bar, click the padlock, then click *Certificate*. The dialog displays the valid certificate information.



Diagnostics

Use the diagnose endpoint `fctems json deep-inspect-cert-sync` command in FortiOS to verify the certificate information. In the following example, there are multiple VDOMs with FortiGates in HA mode.

To verify the primary FortiGate:

```
FGT_EC_Primary (global) # diagnose endpoint fctems json deep-inspect-cert-sync
JSON:
"""
{
  "fortigates": [
    "FG2K5E39169*****",
    "FG2K5E39169*****"
  ],
  "vdoms": [
    {
      "vdom": "root",
      "certs": [
        {
          "name": "Fortinet_CA_SSL",
          "cert": "-----BEGIN CERTIFICATE-----\nMIID5jCCAs6g...Sfu+Q8zE8Crmt6L1X\ /bv+q\n---
--END CERTIFICATE-----\n"
```

```

    },
    {
        "name": "Fortinet_CA_Untrusted",
        "cert": "-----BEGIN CERTIFICATE-----\\nMIID8DCCAtig...3zBbfzP+nVUPC\\nZDPRZA==\\n--
---END CERTIFICATE-----"
    }
]
},
{
    "vdom": "vdom1",
    "certs": [
        {
            "name": "Fortinet_CA_SSL",
            "cert": "-----BEGIN CERTIFICATE-----\\nMIID5jCCAs6g...Sfu+Q8zE8Crmt6L1X\\n/bv+q\\n--
---END CERTIFICATE-----\\n"
        },
        {
            "name": "Fortinet_CA_Untrusted",
            "cert": "-----BEGIN CERTIFICATE-----\\nMIID8DCCAtig...3zBbfzP+nVUPC\\nZDPRZA==\\n--
---END CERTIFICATE-----"
        }
    ]
}
}
"""

```

To verify the secondary FortiGate:

```
FGT_EC_Secondary(global) # diagnose endpoint fctems json deep-inspect-cert-sync
JSON:
"""
{
  "fortigates":[
    "FG2K5E39169*****",
    "FG2K5E39169*****"
  ],
  "vdoms":[
    {
      "vdom":"root",
      "certs":[
        {
          "name":"Fortinet_CA_SSL",
          "cert":"-----BEGIN CERTIFICATE-----\\nMIID5jCCAs6g...Sfu+Q8zE8Crmt6L1X\\n/bv+q\\n---
--END CERTIFICATE-----\\n"
        },
        {
          "name":"Fortinet_CA_Untrusted",
          "cert":"-----BEGIN CERTIFICATE-----\\nMIID8DCCAtig...3zBbfzP+nVUPC\\nZDPRZA==\\n---
---END CERTIFICATE-----"
        }
      ]
    },
    {
      "vdom":"vdom1",
      "certs":[
```

```

    {
      "name": "Fortinet_CA_SSL",
      "cert": "-----BEGIN CERTIFICATE-----\\nMIID5jCCAs6g...Sfu+Q8zE8Crmt6L1X\\n/bv+q\\n---
--END CERTIFICATE-----\\n"
    },
    {
      "name": "Fortinet_CA_Untrusted",
      "cert": "-----BEGIN CERTIFICATE-----\\nMIID8DCCAtig...3zBbfzP+nVUPC\\nZDPRZA==\\n---
---END CERTIFICATE-----"
    }
  ]
}
]
}
}
""





















```

Asset Identity Center page - 7.0.2

The *Asset Identity Center* page unifies information from detected addresses, devices, and users into a single page, while building a data structure to store the user and device information in the backend. *Asset* view groups information by *Device*, while *Identity* view groups information by *User*. Hover over a device or a user in the GUI to perform different actions relevant to the object, such as adding a firewall device address, adding an IP address, banning the IP, quarantining the host, and more.

To view the Asset Identity Center page:

1. Go to *Security Fabric > Asset Identity Center*.
2. Click *Asset* to view information by device. The default columns are *Device*, *Software OS*, *Hardware*, *FortiClient User*, *User*, *Status*, *Vulnerabilities*, *Last Seen*, *Address*, *Hostname*, and *IP Address*. The optional columns are *Address*, *Firewall Address*, *Hostname*, *IP Address*, and *Server*.

Search									Latest	Asset	Identity
Device	Software OS	Hardware	FortiClient User	User	Status	Vulnerabilities	Last Seen	Address	Hostname	IP address	
 PC72	Microsoft	Other identified device	 fosqa 10.6.30.72	 test1	 Registered - Online - On-Net	   	5 minutes ago	10.6.30.72 192.168.7.72 2000:192:168:7:72	PC72	10.6.30.72	
 PC17	Microsoft	Other identified device	 fosqa 10.6.30.17	 test1	 Registered - Online - On-Net	   	4 minutes ago	10.6.30.17	PC17	10.6.30.17	
	FortiOS	Fortinet / Firewall / FortiGate-101E			 Online		4 minutes ago	192.168.7.3		192.168.7.3	
	Other identified device	Other identified device			 Online		4 seconds ago				

3. Click *Identity* to view information by user. The default columns are *User*, *Device*, and *Properties*. The optional columns are *IP Address*, *Logoff Time*, and *Logon Time*.

Search



1 hour

Asset

Identity






User	Device	Properties	IP Address	Logoff Time	Logon Time
<div> <div></div> <div>qa1</div> </div>	<div> <div></div> <div>PC17</div> </div>	<div>IP Address = 10.6.30.17</div> <div>MAC address = 00:00:00:00:00:00</div>	10.6.30.17		2021/09/20 16:12:21
<div> <div></div> <div>test1</div> </div>	<div> <div></div> <div>PC72</div> <div>PC17</div> </div>	<div>IP Address = 192.168.7.72</div> <div>MAC address = 00:00:00:00:00:00</div>	192.168.7.72		2021/09/20 16:14:24

Each view has a dropdown option to view the information within different time frames (*Latest*, *1 hour*, *24 hours*, and *7 days*). Vulnerability information is displayed when applicable. The page displays user and device relationships, such as which users are logged in to multiple devices or if multiple users are logged in to single devices.

Device	Software OS	Hardware	FortiClient User	User	Status	Vulnerabilities	Last Seen	Address	Hostname	IP Address
PC72	Microsoft	Other identified device	 fosqa 10.6.30.72	test1	Registered - Online - On-Net	19 20 1 2	5 minutes ago	10.6.30.72 192.168.7.72 2000:192:168:7::72	PC72	10.6.30.72
PC17	Microsoft	Other identified device	 fosqa 10.6.30.17	test1	Registered - Online - On-Net	19 20 1 2	4 minutes ago	10.6.30.17	PC17	10.6.30.17

User	Device	Properties	IP Address	Logoff Time	Logon Time
qa1	PC17	IP Address = 10.6.30.17 MAC address = [redacted]	10.6.30.17		2021/09/20 16:12:21
test1	PC72 PC17	IP Address = 192.168.7.72 & 10.6.30.17 MAC address = [redacted]	192.168.7.72 10.6.30.17	2021/09/20 16:11:23	2021/09/20 15:49:18

4. Hover over a device in the list to view the tooltip and possible actions. In this example, the available actions are add firewall device address, add firewall IP address, and quarantine the host.

Device	Software OS	Hardware	FortiClient User	User	Status	Vulnerabilities	Last Seen	Address	Hostname	IP Address
PC72	Microsoft	Other identified device	 fosqa 10.6.30.72	test1	Registered - Online - On-Net	19 20 1 2	8 minutes ago	10.6.30.72 192.168.7.72 2000:192:168:7::72	PC72	10.6.30.72
PC17	Microsoft	Other identified device	 fosqa 10.6.30.17	test1	Registered - Online - On-Net	19 20 1 2	7 minutes ago	10.6.30.17	PC17	10.6.30.17
PC72	Microsoft	Other identified device	 fosqa 10.6.30.72	test1	Online		37 seconds ago	192.168.7.3		192.168.7.3
PC17	Microsoft	Other identified device	 fosqa 10.6.30.17	test1	Online		2 minutes ago			
PC72	Microsoft	Other identified device	 fosqa 10.6.30.72	test1	Offline		34 minutes ago	192.168.7.2		192.168.7.2

Diagnostics for the unified user device store

The following options have been added to diagnose `user-device-store unified <option>`:

Option	Description
<code>device-memory-query</code>	Get device records and associated user records from memory.
<code>device-query</code>	Get device records and associated user records from memory and disk.
<code>user-memory-query</code>	Get user records and associated device records from memory.
<code>user-query</code>	Get user records and associated device records from memory and disk.
<code>re-query</code>	Retrieve query by <code><query-id> <iteration-start> <iteration-count></code> (takes 0-3 arguments).
<code>list</code>	List unified queries.

Option	Description
clear	Delete all unified queries.
dump	Dump unified query stats by <query-id> (takes 0-1 arguments).
delete	Delete unified query by <query-id> (takes 0-1 arguments).
stats	Get statistics for unified queries.
debug	Enable/disable debug logs for unified queries.

Fabric Management page - 7.0.2

The *Fabric Management* page allows administrators to manage the firmware running on each FortiGate, FortiAP, and FortiSwitch in the Security Fabric. A *Fabric Upgrade* can be performed immediately or during a scheduled time. Administrators can choose a firmware from FortiGuard for the Fabric member to download directly to upgrade.



To demonstrate the functionality of this feature, the examples use FortiGates that are running interim builds.

To upgrade individual device firmware:

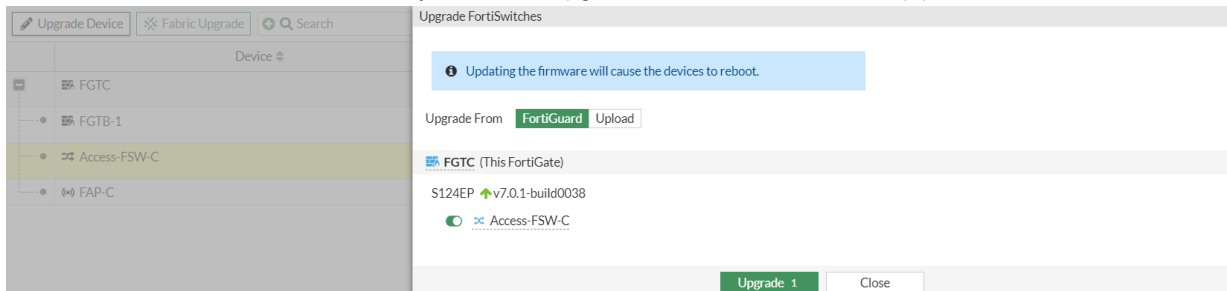
1. Go to *System > Fabric Management*. The devices are displayed in the table with their firmware version and status. In this example, all devices (root FortiGate, downstream FortiGate, FortiSwitch, and FortiAP) have an upgrade available.

Upgrade Device Fabric Upgrade Search			
	Device	Firmware Version	Firmware Status
	FGTC	7.0.1 build0232	v7.0.2 available
	FGTB-1	7.0.1 build0232	v7.0.2 available
	Access-FSW-C	7.0.0 build0022	v7.0.1 available
	FAP-C	6.2.5 build0293	v6.4.7 available

2. Upgrade the root FortiGate to the latest firmware:
 - a. Select the device (FGTC) and click *Upgrade Device*. The *FortiGate Upgrade* pane opens.
 - b. Select *Latest* (other options available are *All Upgrades*, *All Downgrades*, and *File Upload*) and select the option that is displayed.

- c. Click *Confirm and Backup Config* then click *Continue* to initiate the upgrade.

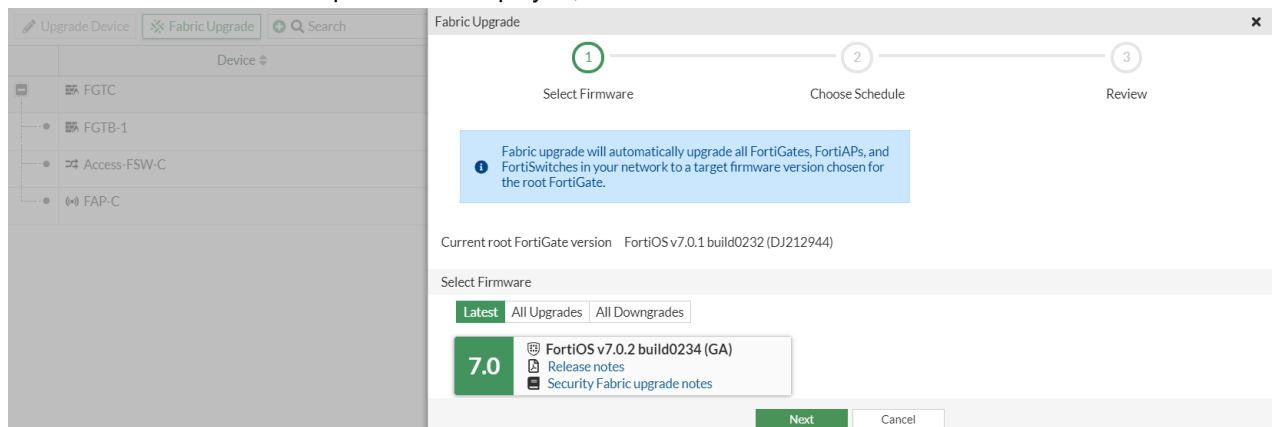
3. After the root reboots, upgrade the FortiSwitch using FortiGuard:
 - a. Go to *System > Fabric Management* and select the device (*Access-FSW-C*), then click *Upgrade Device*. The *Upgrade FortiSwitches* pane opens.
 - b. Select *FortiGuard*, ensure the device you want to upgrade is enabled, then click *Upgrade*.



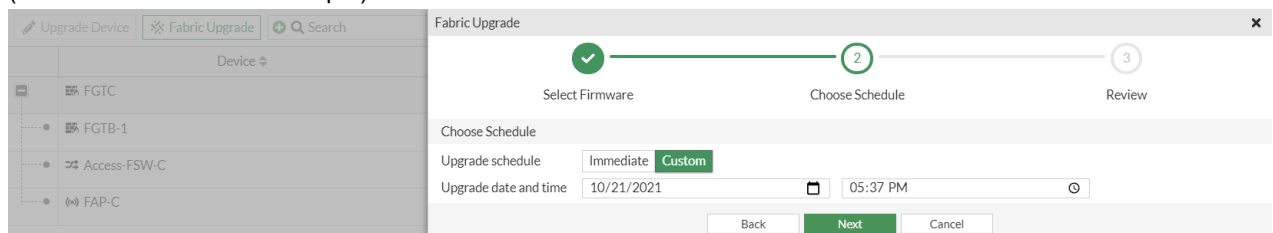
4. Upgrade the FortiAP using local firmware:
 - a. Select the device (*FAP-C*) and click *Upgrade Device*. The *Upgrade FortiAPs* pane opens.
 - b. Select *Upload* and click *Browse* to select the file.
 - c. Ensure the device you want to upgrade is enabled, then click *Upgrade*.

To upgrade all Fabric device firmware:

1. Go to *System > Fabric Management* and click *Fabric Upgrade*. The *Fabric Upgrade* pane opens.
2. Select *Latest* and select the option that is displayed, then click *Next*.

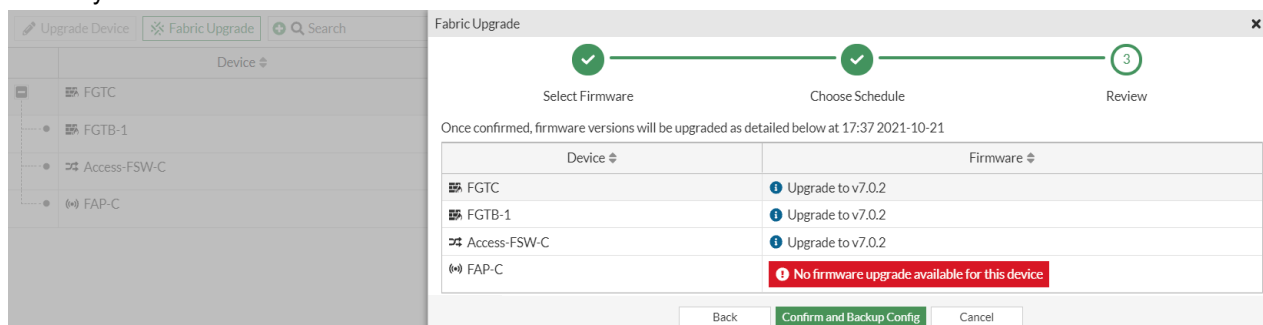


3. Select an upgrade schedule, either *Immediate* or *Custom*. If using *Custom*, enter an upgrade date and time (*Custom* is used in this example).



In a custom upgrade, the configuration backups are saved when the administrator schedules the upgrade. If the scheduled upgrade occurs after further configuration changes are made, the latest changes will not be saved in a new backup configuration file.

4. Click *Next* and review the update schedule. For the FortiAP, a message appears because a firmware upgrade is currently not available.



5. Click *Confirm and Backup Config*. The pane goes into a loading state to wait for all FortiGate configurations to save. Once completed, the pane closes and the device list refreshes to reflect the latest changes.

Upgrade Device	Cancel Fabric Upgrade	Search
Device	Firmware Version	Firmware Status
FGTC	7.0.1 build0232	Upgrade to 7.0.2 shortly
FGTB-1	7.0.1 build0232	Upgrade to 7.0.2 shortly
Access-FSW-C	7.0.0 build0022	Upgrade to 7.0.2 shortly
FAP-C	6.4.7 build0471	Up to date

CLI commands

The following options are available in `execute federated-upgrade <option>`:

Option	Description
cancel	Cancel the currently configured upgrade.
initialize	Set up a federated upgrade.
status	Show the current status of a federated upgrade.

External connectors

This section includes information about SDN connector related new features:

- [Threat feed connectors per VDOM on page 82](#)
- [Nutanix connector on page 86](#)
- [STIX format for external threat feeds 7.0.2 on page 88](#)

Threat feed connectors per VDOM

When multi-VDOM mode is enabled, the threat feed external connector can be defined in global or within a VDOM. Global threat feeds can be used in any VDOM, but cannot be edited within the VDOM. FortiGuard category and domain

name-based external feeds have an added category number field to identify the threat feed. The threat feed name in global must start with `g-`. Threat feed names in VDOMs cannot start with `g-`.

FortiGuard category and domain name-based external feed entries must have a number assigned to them that ranges from 192 to 221. This number can be assigned to both external feed types. However, when a category number is used under a global entry, such as 192 with the name `g-cat-192`, this category number cannot be used in any other global or VDOM entries. If a category is used under a VDOM entry, such as 192 under VDOM1 with the name `cat-192`, the category 192 can be used in another VDOM or root with the name `cat-192`.

A threat feed connector can only be used in profiles in the VDOM that it was created in. Global connectors can be used in all VDOMs.

Each VDOM can have a maximum of 256 threat feed entries. But in total, a FortiGate can only have 511 threat feed entries.

To configure an external threat feed connector under global in the GUI:

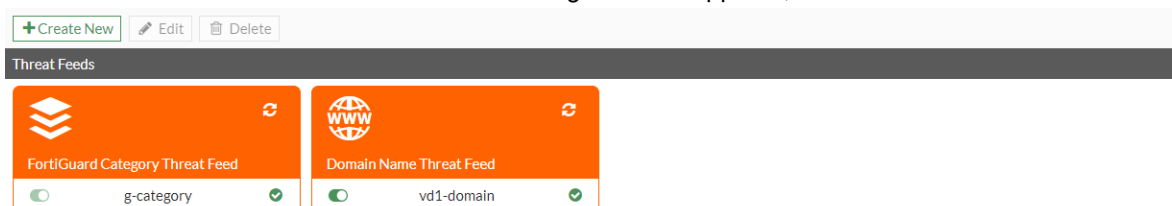
1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *FortiGuard Category*.
3. Enter a name that begins with `g-`.
4. Configure the other settings as needed.
5. Click *OK*.

To configure an external threat feed connector under global in the CLI:

```
config global
  config system external-resource
    edit "g-category"
      set status enable
      set type category
      set category 192
      set comments ''
      set resource "http://172.16.200.55/external-resource-test/513-FDGCATEGORY.txt"
      set refresh-rate 5
    next
  end
end
```

To configure an external threat feed connector under a VDOM in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *Domain Name*.
3. Enter a name that does not begin with `g-`.
4. Configure the other settings as needed.
5. Click *OK*. The threat feed connector created under global also appears, but it is not editable.



To configure an external threat feed connector under a VDOM in the CLI:

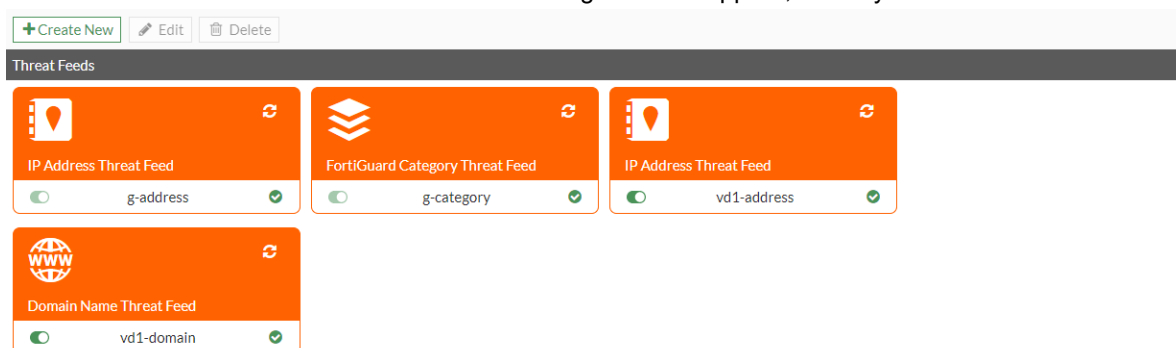
```

config vdom
  edit vd1
    config system external-resource
      edit "vd1-domain"
        set status enable
        set type domain
        set category 193
        set comments ''
        set resource "http://172.16.200.55/external-resource-test/513-Domain.txt"
        set refresh-rate 5
      next
    end
  next
end

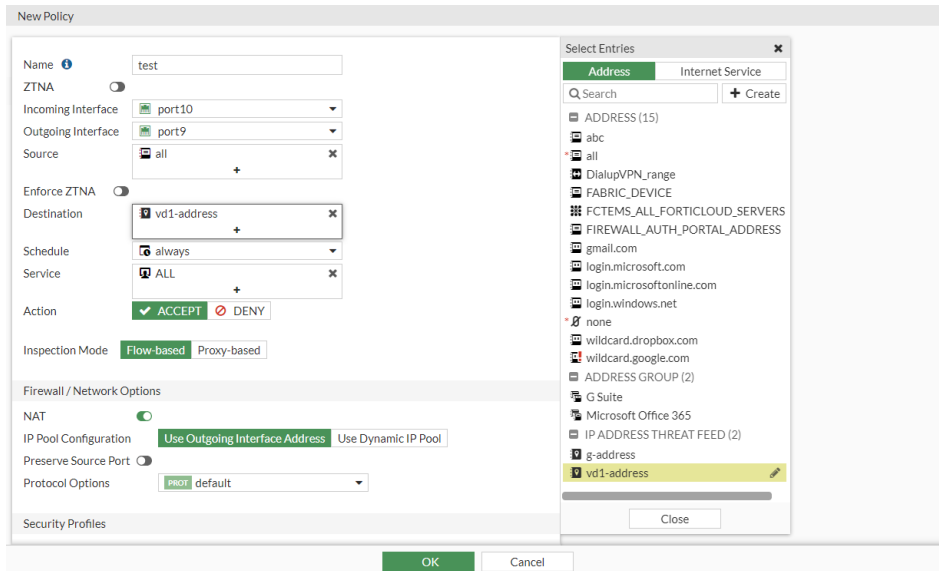
```

To use an IP address threat feed in a policy in the GUI:

1. Configure an IP address connector in global:
 - a. Go to *Security Fabric > External Connectors* and click *Create New*.
 - b. In the *Threat Feeds* section, click *IP Address*.
 - c. Enter a name that begins with g-.
 - d. Configure the other settings as needed.
 - e. Click OK.
2. Configure an IP address connector in the VDOM (vd1):
 - a. Go to *Security Fabric > External Connectors* and click *Create New*.
 - b. In the *Threat Feeds* section, click *IP Address*.
 - c. Enter a name that does not begin with g-.
 - d. Configure the other settings as needed.
 - e. Click OK. The threat feed connectors created under global also appear, but they are not editable.



3. Configure the firewall policy in the VDOM (vd1):
 - a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
 - b. For *Destination*, select *vd1-address*. Since this policy is configured under vd1, *g-address* can also be set as the destination.



- c. Configure the other settings as needed.
- d. Click OK.

To use an IP address threat feed in a policy in the CLI:

1. Configure the IP address connectors:

```
config global
    config system external-resource
        edit "g-address"
            set status enable
            set type address
            set username ''
            set comments ''
            set resource "http://172.16.200.55/external-resource-test/513-IP.txt"
            set refresh-rate 5
        next
    end
end

config vdom
    edit vd1
        config system external-resource
            edit "vd1-address"
                set status enable
                set type address
                set comments ''
                set resource "http://172.16.200.55/external-resource-test/513-IP.txt"
                set user-agent "curl/7.58.0"
                set refresh-rate 5
            next
        end
    next
end
```

2. In the VDOM, configure a firewall policy with the external address as the destination address:

```
config vdom
  edit vd1
    config firewall policy
      edit 1
        set name "test"
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "vd1-address"
        set action accept
        set schedule "always"
        set service "ALL"
        set profile-protocol-options "protocol"
        set nat enable
      next
    end
  next
end
```



Since this firewall policy is configured under `vd1`, `g-address` can also be set as the `dstaddr`.

Nutanix connector

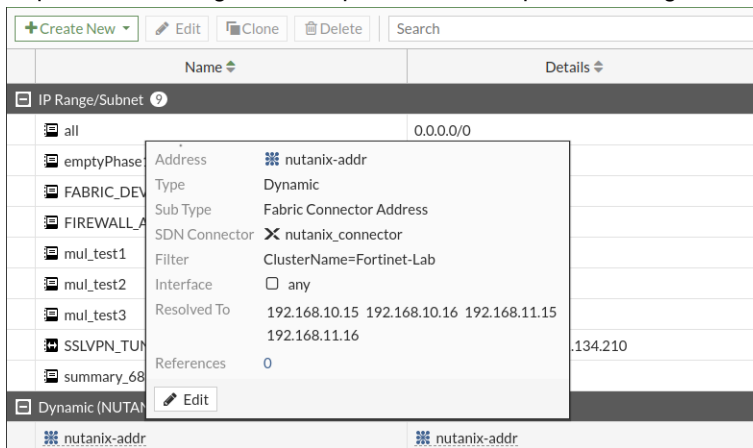
FortiOS automatically updates dynamic addresses for Nutanix using an Nutanix SDN connector, including mapping the following attributes from Nutanix instances to dynamic address groups in FortiOS:

- Cluster name
- Cluster UUID
- Description
- Host name
- Host UUID
- Hypervisor type
- Image name
- Image UUID
- Subnet name
- Subnet UUID
- VM name
- VM UUID

To configure a Nutanix connector using the GUI:

1. Configure the Nutanix SDN connector:
 - a. Go to *Security Fabric > External Connectors*.
 - b. Select *Nutanix*.
 - c. In the *IP address* field, enter the IP address for your Nutanix environment.
 - d. In the *Port* field, enter the desired port.

- e. In the *Username* and *Password* fields, enter the credentials for your Nutanix environment.
 - f. Click OK.
2. Create a dynamic firewall address for the configured Nutanix SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. From the *Type* dropdown list, select *Dynamic*.
 - d. From the *Sub Type* dropdown list, select *Fabric Connector Address*.
 - e. From the *SDN Connector* dropdown list, select the Nutanix connector.
 - f. From the *Filter* dropdown list, select the desired filters.
 - g. Click OK.
3. Ensure that the Nutanix SDN connector resolves dynamic firewall IP addresses:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Hover over the address created in step 2 to see a list of IP addresses for instances that satisfy the filter requirements configured in step 2. In this example, the configured filter is "ClusterName=Fortinet-Lab":



To configure a Nutanix connector using the CLI:

1. Configure the Nutanix SDN connector:

```
config system sdn-connector
  edit "nutanix_connector"
    set status disable
    set type nutanix set server "172.18.33.59"
    set server-port 9440
    set username "admin"
    set password *****
    set update-interval 60
  next
end
```

2. Create a dynamic firewall address for the configured Nutanix SDN connector:

```
config firewall address
  edit "nutanix-addr"
    set type dynamic
    set sdn "nutanix_connector"
    set color 2
    set filter "ClusterName=Fortinet-Lab"
  next
end
```

3. Ensure that the Nutanix SDN connector resolves dynamic firewall IP addresses:

```
config firewall address
  edit "nutanix-addr"
    set type dynamic
    set sdn "nutanix_connector"
    set color 2
    set filter "ClusterName=Fortinet-Lab"
  config list
    edit "192.168.10.15"
    next
    edit "192.168.10.16"
    next
    edit "192.168.11.15"
    next
    edit "192.168.11.16"
    next
  end
end
next
end
```

STIX format for external threat feeds - 7.0.2

The FortiGate's external threat feeds support feeds that are in the STIX/TAXII format. Use the `stix://` prefix in the URI to denote the protocol.

All external threat feeds support the STIX format. In this example, a FortiGuard Category threat feed in the STIX format is configured.

To configure a FortiGuard Category threat feed in the STIX format in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *FortiGuard Category* from the *Threat Feeds* section.
3. Configure the connector:
 - **Name:** *category-taxii*
 - **URI of external resource:** *stix://limo.anomali.com/api/v1/taxii2/feeds/collections/200/objects/*
 - **HTTP basic authentication:** Enable and enter the username and password, such as *guest* and *guest*.

The screenshot shows the 'New External Connector' dialog box. On the left, under 'Threat Feeds', 'FortiGuard Category' is selected with a green checkmark. Below this, the 'Connector Settings' are configured: Name is 'category-taxii', URI of external resource is 'stix://limo.anomali.com/api/v1/taxii2/fe', HTTP basic authentication is enabled, Username is 'guest', Password is masked with dots, Refresh Rate is set to 5 minutes, and Comments are at 0/255. On the right, the 'Additional Information' panel lists various setup guides for public and private SDN connectors, including links for Amazon Web Services, Google Cloud Platform, Microsoft Azure, Oracle Cloud Infrastructure, Cisco Application Centric Infrastructure, Nuge Virtualized Services Platform, OpenStack Connector, VMware NSX, and documentation links for Online Help and Video Tutorials. At the bottom are 'OK' and 'Cancel' buttons.

4. Click **OK**.
5. Edit the connector, and click **View Entries** in the right side bar to view the retrieved entries.

Entry	Validity
www.assculturaleincontri.it	Valid
dancecourt.com	Valid
strangeduckfilms.com	Valid
ukonline.hc0.me	Valid
boschetto-hotel.gr	Valid
tecslide.com	Valid
dl.microword.net	Valid
axisbuild.com	Valid
romvarimarton.hu	Valid
rsluk.co.uk	Valid
www.catgallery.com	Valid

To configure a FortiGuard Category threat feed in the STIX format in the CLI:

```
config system external-resource
  edit "category-taxii"
    set category 194
    set username "guest"
    set password guest
    set resource "stix://limo.anomali.com/api/v1/taxii2/feeds/collections/200/objects/"
  next
end
```

If the connector is used in webfilter that blocks category 194, the traffic that matches the retrieved URLs, such as **rsiuk.co.uk**, is blocked:

```
1: date=2021-10-06 time=18:07:46 eventtime=1633568867163763708 tz="-0700" logid="0316013056"
type="utm" subtype="webfilter" eventtype="ftgd_blk" level="warning" vd="vd1" policyid=1
sessionid=174974 srcip=10.1.100.12 srcport=48284 srcintf="port2" srcintfrole="undefined"
srcuid="c6753ba2-231b-51ec-1675-090f2b5f1384" dstip=78.129.255.151 dstport=443
dstintf="port1" dstintfrole="undefined" dstuid="c6753ba2-231b-51ec-1675-090f2b5f1384"
proto=6 service="HTTPS" hostname="rsiuk.co.uk" profile="test" action="blocked"
reqtype="direct" url="https://rsiuk.co.uk/" sentbyte=75 rcvbyte=0 direction="outgoing"
msg="URL belongs to a denied category in policy" method="domain" cat=194 catdesc="category-
taxii"
```

Automation stitches

This section includes information about automation stitches related new features:

- [Automation workflow improvements on page 90](#)
- [Microsoft Teams Notification action on page 99](#)
- [Replacement messages for email alerts on page 104](#)

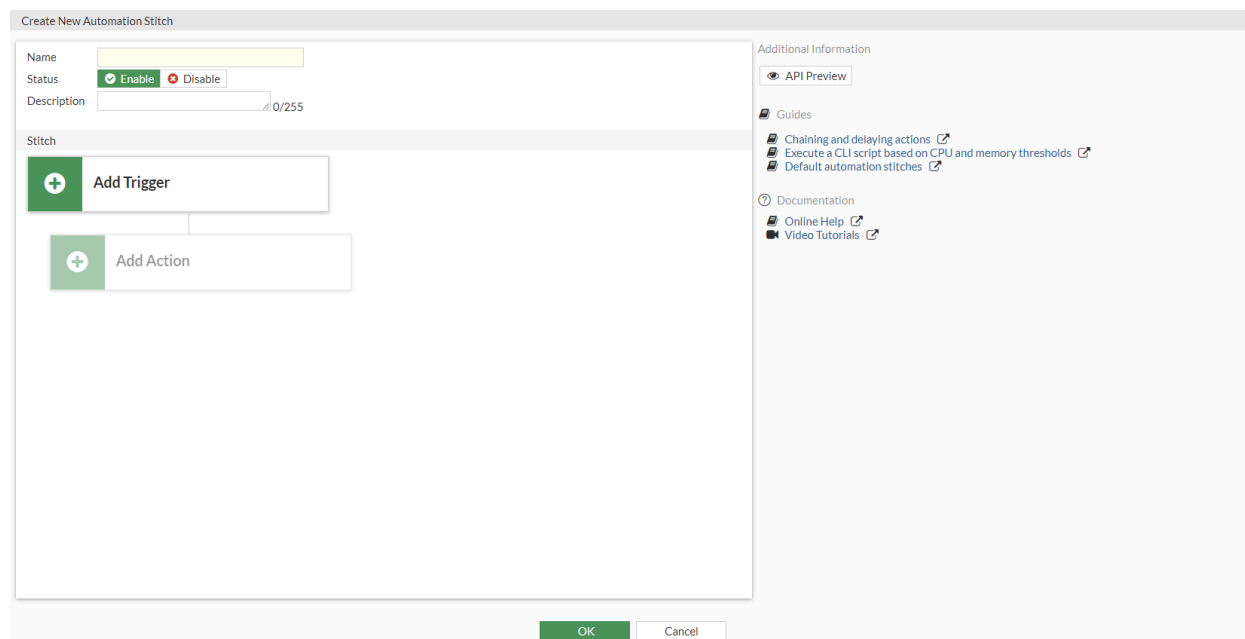
Automation workflow improvements

This redesign simplifies the workflow for managing multiple chained actions, and makes it clearer which order the actions will be processed in. The enhancements include:

- Add new flow for creating and managing automation stitches, triggers, and actions.
- Add tabs for *Stitch*, *Trigger*, and *Action* on the *Automation* page.
- Improve FortiOS Event Log trigger by allowing multiple log IDs and adding a log field filter.
- Add *Any* report type for the Security Rating Summary trigger.
- Simplify the URI configuration for cloud actions.
- Add JSON parameter support for Slack and Microsoft Teams notifications.
- Rename `ios-notification` action type to `fortiexplorer-notification`.

GUI changes to Automation page

Automation stitches, actions, and triggers have separate dialogs and are no longer part of the main stitch dialog. When creating a stitch, clicking *Add Trigger* and *Add Action* displays a list of available triggers and actions, and the option to create a new one.



Once the stitch is configured, a process diagram of the trigger, actions, and delays is displayed.

Create New Automation Stitch

Name:

Status: Enable Disable

Description: 15/255

Stitch

Trigger
aws_no_delay

Action
aws_no_delay

60 Seconds

Action
email_action

Add Action

Additional Information

API Preview

Guides

- Chaining and delaying actions
- Execute a CLI script based on CPU and memory thresholds
- Default automation stitches

Documentation

- Online Help
- Video Tutorials

OK Cancel

Tabs on the Automation page

On the *Security Fabric > Automation* page, there are tabs for *Stitch*, *Trigger*, and *Action*. The *Stitch* tab is the default view that lists the trigger and actions used in each stitch. Individual triggers and actions can be created or edited in the corresponding tabs.

Stitch Trigger Action						
<div> <div>Create New</div> <div>View</div> <div>Delete</div> <div>Clone</div> <div>Search</div> </div>						
Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
Compromised Host						
Access_Layer_Quarantine	Enabled	Access_Layer_Quarantine	Access_Layer_Quarantine_quarantine	All FortiGates	0	
Compromised Host Quarantine	Enabled	Compromised Host Quarantine	Compromised Host Quarantine_quarantine Compromised Host Quarantine_quarantine-forticlient	All FortiGates	0	
Configuration Change						
Configuration_Change_Notification	Enabled	Configuration_Change_Notification	Configuration_Change_Notification_email Configuration_Change_Notification_ios-notification	All FortiGates	0	
FortiOS Event Log						
FortiAnalyzer Connection Down	Enabled	FortiAnalyzer Connection Down	FortiAnalyzer Connection Down_fortilexplorer-notification	All FortiGates	0	
Network Down	Disabled	Network Down	Network Down_email	All FortiGates	0	
HA Failover						
HA Failover	Enabled	HA Failover	HA Failover_email	All FortiGates	0	
Incoming Webhook						
Incoming Webhook Quarantine	Enabled	Incoming Webhook Call	Compromised Host Quarantine_quarantine Compromised Host Quarantine_quarantine-forticlient	All FortiGates	0	
License Expiry						
License Expired Notification	Enabled	License Expired Notification	License Expired Notification_fortilexplorer-notification	All FortiGates	0	
0% (10) Updated: 11:39:36						

Click *Trigger* to view the list of triggers.

Stitch Trigger Action			
+ Create New View Delete Clone <input type="text" value="Search"/>			
Name	Details	Description	Ref
Compromised Host 1			
Access_Layer_Quarantine	SEVR High		1
Compromised Host Quarantine	SEVR High		1
MultiCloud_Quarantine_Compromised	SEVR High		0
Configuration Change 1			
Configuration_Change_Notification			1
FortiAnalyzer Event Handler 2			
Add_Malware_Providers_to_Blacklist	EVENT FOS_Automaton_Blacklist_Malware_Provider		0
MultiCloud_Quarantine_Botnet	EVENT Default-Botnet-Communication-Detection		0
FortiOS Event Log 4			
AWS_Log_Admin_Login_Fail	Admin login failed		0
AWS_Log_HA_Sync_Fail	HA secondary synchronization failed		0
FortiAnalyzer Connection Down	FortiAnalyzer connection down		1
Network Down	Interface status changed		1
HA Failover 2			
AWS_Log_HA_Failover			0
0% (22) Updated: 11:40:14			

Click *Action* to view the list of actions.

Stitch Trigger Action					
+ Create New View Delete Clone <input type="text" value="Search"/>					
Name	Details	Required	Trigger Count	Last Triggered	Ref
Access Layer Quarantine 2					
Access_Layer_Quarantine_quarantine		No	0		1
Compromised Host Quarantine_quarantine		No	0		2
Email 4					
Configuration_Change_Notification_email	EMAIL admin@example.com	No	0		1
HA Failover_email		No	0		1
Network Down_email		No	0		1
Reboot_email		No	0		1
FortiClient Quarantine 1					
Compromised Host Quarantine_quarantine-forticlient		No	0		2
FortiExplorer Notification 3					
FortiAnalyzer Connection Down_fortilexplorer-notification		No	0		1
License Expired Notification_fortilexplorer-notification		No	0		1
Security Rating Notification_fortilexplorer-notification		No	1	Hour ago	1
FortiOS Notification 1					
Configuration_Change_Notification_ios-notification		No	0		1
11 Updated: 11:40:35					

The following example shows how to configure a Security Rating Summary automation stitch with AWS Lambda and Email actions.

To configure the automation stitch in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name and description.
3. Configure the trigger:
 - a. Click *Add Trigger*.
 - b. Click *Create* and select *Security Rating Summary*.

- c. Enter the following:

Name	aws_no_delay
Report	Security Posture

Create New Automation Stitch

Name: aws_no_delay

Status: Enable Disable

Description: aws action test 15/255

Stitch

+ Add Trigger

+ Add Action

Create New Automation Trigger

Security Rating Summary A specified Security Rating report was generated. CHANGE TYPE

Method: Create New Select Existing

Name: aws_no_delay

Description: 0/255

Security Rating Summary

Report: Security Posture

OK Cancel

- d. Click **OK**.
- e. Select the trigger in the list and click *Apply*.
4. Configure the AWS Lambda function action:
- Click *Add Action*.
 - Click *Create* and select *AWS Lambda*.
 - Enter the following:

Name	aws_no_delay
URL	Enter the request API URI
API key	Enter AWS API gateway API key
HTTP header	header2 : header2_value

The screenshot displays two side-by-side configuration windows in the FortiGate Security Fabric interface.

Left Window: Create New Automation Stitch

- Name:** aws_no_delay
- Status:** Enable (selected), Disable
- Description:** aws action test (15/255)
- Stitch:**
 - Trigger: aws_no_delay
 - + Add Action

Right Window: Create New Automation Action

- Header:** AWS Lambda Query an AWS Lambda function.
- Name:** aws_no_delay
- Minimum interval:** 0 second(s)
- Delay:** 0 second(s)
- Required:** (toggle switch)
- Description:** (0/255)
- AWS Lambda:**
 - URL:** https:// (69/1023)
 - API key:** (masked)
 - HTTP header:** header2 : header2_value

At the bottom of the right window are **OK** and **Cancel** buttons.

- d. Click **OK**.
 - e. Select the action in the list and click *Apply*.
5. Configure the Email notification action:
- a. Click *Add Action*.
 - b. Click *Create* and select *Email*.
 - c. Enter the following:

Name	email_action
Delay	60
To	Enter an email address
Subject	email action for test
Replacement message	Enable

The left screenshot shows the 'Create New Automation Stitch' window. It has a 'Name' field with 'aws_no_delay', a 'Status' dropdown set to 'Enable', and a 'Description' field with 'aws action test'. Below this is a 'Stitch' section with a 'Trigger' block labeled 'aws_no_delay' and an 'Action' block labeled 'aws_no_delay'. There is an 'Add Action' button at the bottom.

The right screenshot shows the 'Create New Automation Action' window for an 'Email' action. It has a 'Name' field with 'email_action', a 'Minimum Interval' field with '0' and a unit dropdown set to 'second(s)', a 'Delay' field with '60' and a unit dropdown set to 'second(s)', a 'Required' toggle set to 'On', and a 'Description' field with 'email action for test'. Below this is an 'Email' section with a 'To' field containing 'test@fortinet.com', a 'Subject' field with 'email action for test', a 'Body' field with '%%log%%', a 'Replacement message' toggle set to 'On', and a 'Customize messages' toggle set to 'Off'. There are 'OK' and 'Cancel' buttons at the bottom.

d. Click **OK**.

e. Select the action in the list and click **Apply**.

6. Click **OK**.

To configure the automation stitch in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "aws_no_delay"
        set event-type security-rating-summary
    next
end
```

2. Configure the actions:

```
config system automation-action
    edit "aws_no_delay"
        set action-type aws-lambda
        set aws-api-key xxxxxxxxxxxx
        set uri "xxxxxxxxxx.execute-api.us-east-1.amazonaws.com/xxxxxxxxxx"
        set headers "header2:header2_value"
    next
    edit "email_action"
        set description "email action for test"
        set action-type email
        set email-to "test@fortinet.com"
        set email-subject "email action for test"
        set delay 60
        set replacement-message enable
    next
end
```

3. Configure the stitch:

```
config system automation-stitch
  edit "aws_no_delay"
    set description "aws action test"
    set trigger "aws_no_delay"
    set action "aws_no_delay" "email_action"
  next
end
```

FortiOS Event Log trigger

To configure a FortiOS Event Log trigger in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name and description.
3. Configure the trigger:
 - a. Click *Add Trigger*.
 - b. Click *Create* and select *FortiOS Event Log*.
 - c. Enter a name and description.
 - d. In the *Event* field, click the + to select multiple event log IDs.
 - e. In the *Field filter(s)* field, click the + to add multiple field filters. The configured filters must match in order for the stitch to be triggered.

- f. Click *OK*.
 - g. Select the trigger in the list and click *Apply*.
4. Configure the rest of the stitch as needed.

To configure a FortiOS Event Log trigger in the CLI:

```
config system automation-trigger
  edit "event_login_logout"
```

```

set description "trigger for login logout event"
set event-type event-log
set logid 32001 32003
config fields
  edit 1
    set name "user"
    set value "csf"
  next
  edit 2
    set name "ip"
    set value "10.6.30.254"
  next
end
next
end

```

Any report type for Security Rating Summary trigger

To configure a Security Rating Summary trigger in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name and description.
3. Configure the trigger:
 - a. Click *Add Trigger*.
 - b. Click *Create* and select *Security Rating Summary*.
 - c. Enter a name and description.
 - d. In the *Report* field, select *Any*.

The screenshot displays two side-by-side configuration windows in the FortiOS GUI. The left window, titled 'Create New Automation Stitch', has a 'Name' field containing 'rating_any', a 'Status' field with 'Enable' selected, and a 'Description' field with '0/255'. Below these are 'Add Trigger' and 'Add Action' buttons. The right window, titled 'Create New Automation Trigger', shows the configuration for a 'Security Rating Summary' trigger. It includes a 'Method' dropdown set to 'Create New', a 'Name' field with 'rating_any', a 'Description' field with 'rating any type', and a 'Report' dropdown set to 'Any'. A message at the top of the right window states 'A specified Security Rating report was generated.' with a 'CHANGE TYPE' link. At the bottom of the right window are 'OK' and 'Cancel' buttons.

- e. Click *OK*.
 - f. Select the trigger in the list and click *Apply*.
4. Configure the rest of the stitch as needed.

To configure a Security Rating Summary trigger in the CLI:

```
config system automation-trigger
  edit "rating_any"
    set description "rating any type"
    set event-type security-rating-summary
    set report-type any
  next
end
```

URI configuration for cloud actions

For AWS Lambda, Google Cloud, Azure, and AliCloud functions, the URI has been combined into a single attribute instead of having separate attributes for each URI path segment. In the GUI, use the *URL* field. In the CLI, use the *set uri* parameter.

JSON option for Slack and Microsoft Teams notifications

Users have the option to select either a text or JSON message for Slack and Microsoft Teams notifications. The following example shows how to configure a Slack notification with a JSON message.

To configure a Slack notification action with a JSON message in the GUI:

1. Go to *Security Fabric > Automation* and click the *Action* tab.
2. Click *Create New* and select *Slack Notification*.
3. For *Message*, select *JSON*, and enter the message in the text box.
4. Configure the other settings as needed.

The screenshot shows the 'Create New Automation Action' window for a 'Slack Notification'. The 'Name' field is 'slack_json'. 'Minimum interval' is 0 seconds, and 'Delay' is 30 seconds. The 'Required' checkbox is checked. The 'Description' field is empty. In the 'Slack Notification' section, the 'URL' field contains a Slack webhook URL. The 'Message' type is set to 'JSON', and the text box below it contains a JSON payload: `{\"text\": \"%log%\"}`. The right sidebar shows 'Additional Information' with links to 'API Preview', 'Guides' (including FortiNAC Quarantine, VMware NSX Security Tag, Slack Notification, AWS Lambda, Azure Function, Google Cloud Function, AliCloud Function, CLI Script, and Webhook), and 'Documentation' (including Online Help and Video Tutorials).

5. Click *OK*.

To configure a Slack notification action with a JSON message in the CLI:

```
config system automation-action
  edit "slack_json"
    set action-type slack-notification
    set delay 30
```



```

set message-type json
set uri "hooks.slack.com/services/xxxxxxxxx/xxxxxxxxx/xxxxxxxxxxxxxxxxxxxxxxxxx"
set http-body "{\"text\": \"'%log%'\"}"
next
end

```

FortiExplorer notification

To configure a FortiExplorer notification action in the GUI:

1. Go to *Security Fabric > Automation* and click the *Action* tab.
2. Click *Create New* and select *FortiExplorer Notification*.
3. Configure the settings as needed.

4. Click *OK*.

To configure a FortiExplorer notification action in the CLI:

```

config system automation-action
edit "fortiexplore_notification1"
set description "fortiexplore_notification action"
set action-type fortiexplorer-notification
next
end

```

Microsoft Teams Notification action


Microsoft Teams Notification actions can be configured to send notifications to channels in Microsoft Teams. To trigger the notifications, you need to add an Incoming Webhook connector to a channel in Microsoft Teams, then you can configure the automation stitch with the webhook URL.

In the following example, you will configure an automation stitch with a Security Rating Summary trigger and two Microsoft Teams Notification actions with different notification messages. One message is for the Security Rating Summary log, and the other is a custom message with a ten second delay.

To add the Incoming Webhook connector in a Microsoft Teams channel:

1. In Microsoft Teams, click the ... (*More options*) beside the channel name, and select *Connectors*.
2. Search for *Incoming Webhook* and click *Configure*.
3. Enter a name for the webhook, upload an image for the webhook, and click *Create*.
4. Copy the webhook to the clipboard and save it.

Connectors for "General" channel in "Alert-myself" team

 Incoming Webhook
 Send feedback


The Incoming Webhook connector enables external services to notify you about activities that you want to track. To use this connector, you'll need to create certain settings on the other service, which needs to support a webhook that's compatible with the Office 365 connector format.

Fields marked with * are mandatory


Enter a name for your IncomingWebhook connection.*

Customize the image to associate with the data from this Incoming Webhook.

[Upload Image](#)



Copy the URL below to save it to the clipboard, then select Save. You'll need this URL when you go to the service that you want to send data to your group.



5. Click *Done*.

To configure an automation stitch with Microsoft Teams Notification actions in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name.
3. Configure the Security Rating Summary trigger:
 - a. Click *Add Trigger*.
 - b. Click *Create* and select *Security Rating Summary*.

- c. Enter a name, and for *Report*, select *Security Posture*.

- d. Click **OK**.

- e. Select the trigger in the list and click *Apply*.

4. Configure the first Microsoft Teams Notification action:

- a. Click *Add Action*.
- b. Click *Create* and select *Microsoft Teams Notification*.
- c. Enter the following:

Name	teams_1
URL	Paste the webhook URI from the clipboard
Message	Text
Message text	%%log%%

- d. Click **OK**.
 - e. Select the action in the list and click **Apply**.
5. Configure the second Microsoft Teams Notification action:
- a. Click **Add Action**.
 - b. Click **Create** and select **Microsoft Teams Notification**.
 - c. Enter the following:

Name	teams_2
Delay	10
URL	Paste the webhook URI from the clipboard
Message	Text
Message text	This is for test.

The screenshot shows two windows. The left window, 'Create New Automation Stitch', displays a trigger 'Teams_action' and an action 'teams_1'. The right window, 'Create New Automation Action', shows the configuration for a 'Microsoft Teams Notification' action. The configuration includes:

- Name:** teams_2
- Minimum Interval:** 0 second(s)
- Delay:** 10 second(s)
- Required:** (toggle off)
- Description:** (empty)
- Microsoft Teams Notification:**
 - URL:** https://outlook.office.com/webhook/211c1c1c-1c1c-1c1c-1c1c-1c1c1c1c1c1c/IncomingWebhook/1c1c1c1c-1c1c-1c1c-1c1c-1c1c1c1c1c1c/
 - Message:** Text (selected), JSON (available)
 - Message text:** This is for test.

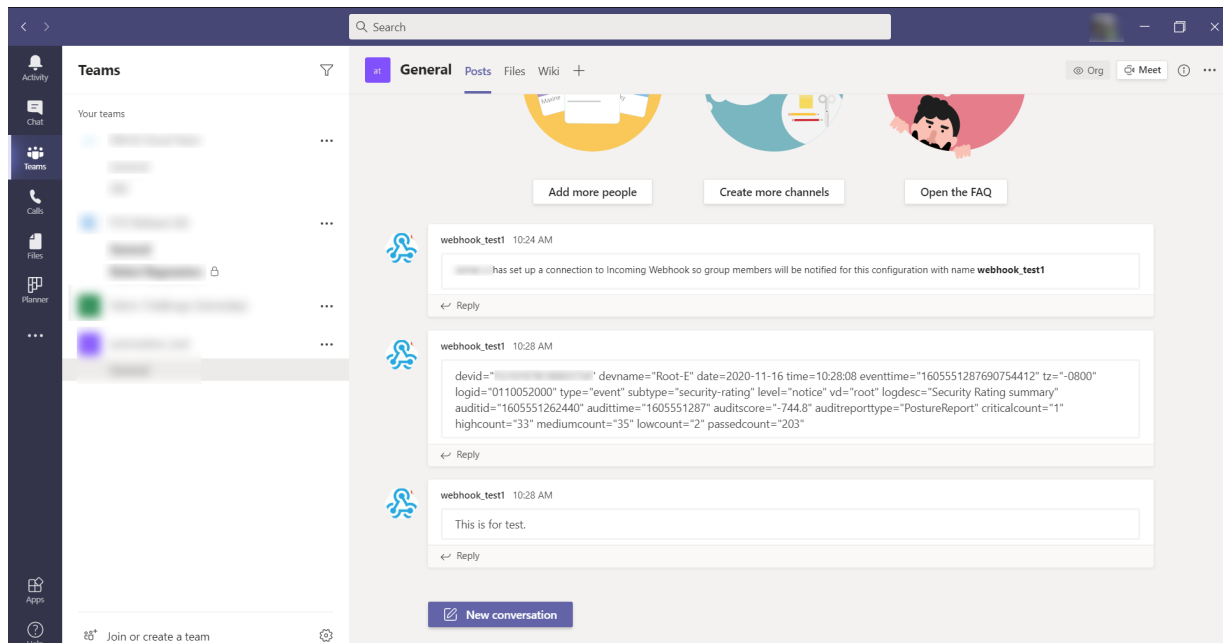
 At the bottom of the right window are 'OK' and 'Cancel' buttons.

- d. Click **OK**.
 - e. Select the action in the list and click **Apply**.
6. Click **OK**.
7. Trigger the automation stitch:
- a. Right-click the automation stitch and select **Test Automation Stitch**.

The screenshot shows the 'Security Rating Summary' table in the FortiGate Security Fabric interface. The table has columns: Name, Status, Trigger, Actions, FortiGate(s), Trigger Count, and Last Triggered. The data row shows:

- Name:** Teams_action
- Status:** Enabled
- Trigger:** Teams_action
- Actions:** teams_1, teams_2
- FortiGate(s):** All FortiGates
- Trigger Count:** 0
- Last Triggered:** (empty)

After the Security Rating report is finished, the automation is triggered and an event log is created by the FortiGate. The two notifications are sent to the Microsoft Teams channel.



To configure an automation stitch with Microsoft Teams Notification actions in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
  edit "Teams_action"
    set event-type security-rating-summary
  next
end
```

2. Configure the automation actions:

```
config system automation-action
  edit "teams_1"
    set action-type microsoft-teams-notification
    set message-type text
    set message "%log%"
    set uri "outlook.office.com/webhook/xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx@xxxxxxxx-
            xxx-xxxx-xxxx-
            xxxxxxxxxxxx/IncomingWebhook/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/xxxxxxx-xxxx-
            xxx-xxxx-xxxxxxxxxxxxx"
  next
  edit "teams_2"
    set action-type microsoft-teams-notification
    set delay 10
    set message-type text
    set message "This is for test."
    set uri "outlook.office.com/webhook/xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx@xxxxxxxx-
            xxx-xxxx-xxxx-
            xxxxxxxxxxxx/IncomingWebhook/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/xxxxxxx-xxxx-
            xxx-xxxx-xxxxxxxxxxxxx"
  next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
  edit "Teams_action"
    set trigger "Teams_action"
```

```

        set action "teams_1" "teams_2"
    next
end
4. Verify that the automation action was triggered:
# diagnose test application autod 3
stitch: Teams_action
  local hit: 2 relayed to: 0 relayed from: 0
  last trigger: Mon Nov 16 10:28:08 2020
  last relay:
  actions:
    teams_1:
      done: 2 relayed to: 0 relayed from: 0
      last trigger: Mon Nov 16 10:28:08 2020
      last relay:
    teams_2:
      done: 2 relayed to: 0 relayed from: 0
      last trigger: Mon Nov 16 10:28:08 2020
      last relay:
  logid2stitch mapping:
  id: 52000 local hit: 22 relayed hits: 0
  Teams_action

```

Replacement messages for email alerts

Automation stitches with an Email action can now leverage the formatting options provided by replacement messages to create branded email alerts.

You can enable a replacement message and edit the message body or select a customized replacement message group when you configure the automation action. When the automation stitch is triggered, the FortiGate will send the email with the defined replacement message.

In this example, a Security Rating report triggers an Email notification action. The email uses a customized replacement message group.

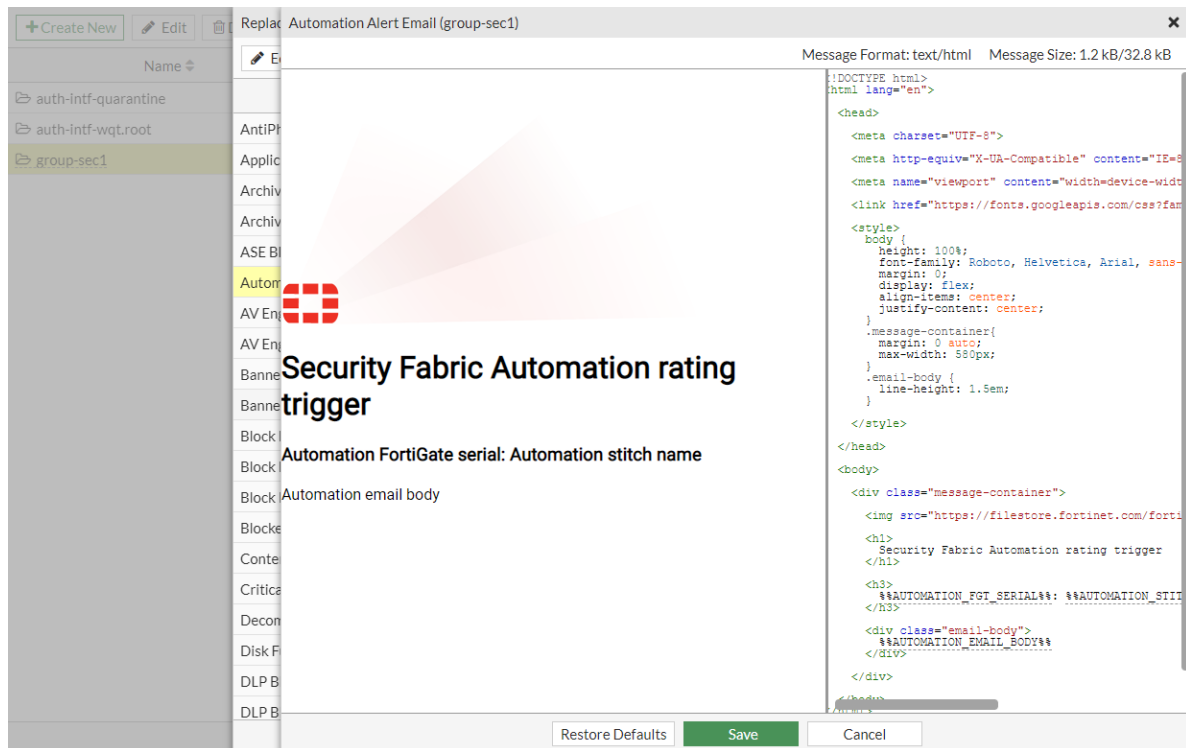
To configure the replacement message group in the GUI:

1. Go to *System > Replacement Message Groups* and click *Create New*.
2. Enter the following:

Name	group-sec1
Group Type	Security

3. Click *OK*.
4. Select the group in the list and click *Edit*.

5. Select *Automation Alert Email* and click *Edit*.



6. Edit the HTML code as needed, then click *Save*.

To configure the email action in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
 - a. Click *Add Trigger*.
 - b. Click *Create* and select *Security Rating Summary*.
 - c. Enter the following:

Name	rating_posture
Description	rating test
Report	Security Posture

Create New Automation Trigger

Name: auto_rating
Status: Enable
Description:
Stitch:
Add Trigger
Add Action

Security Rating Summary A specified Security Rating report was generated. CHANGE TYPE

Method: **Create New** Select Existing
Name: rating_posture
Description:
0/255
Security Rating Summary
Report: Security Posture

OK Cancel

- d. Click **OK**.
- e. Select the trigger in the list and click *Apply*.
4. Configure the Email notification action:
 - a. Click *Add Action*.
 - b. Click *Create* and select *Email*.
 - c. Enter the following:

Name	email-group1
To	Enter an email address
Subject	CSF stitch alert group1
Replacement message	Enable
Customize messages	Enable and select group-sec1 from the dropdown

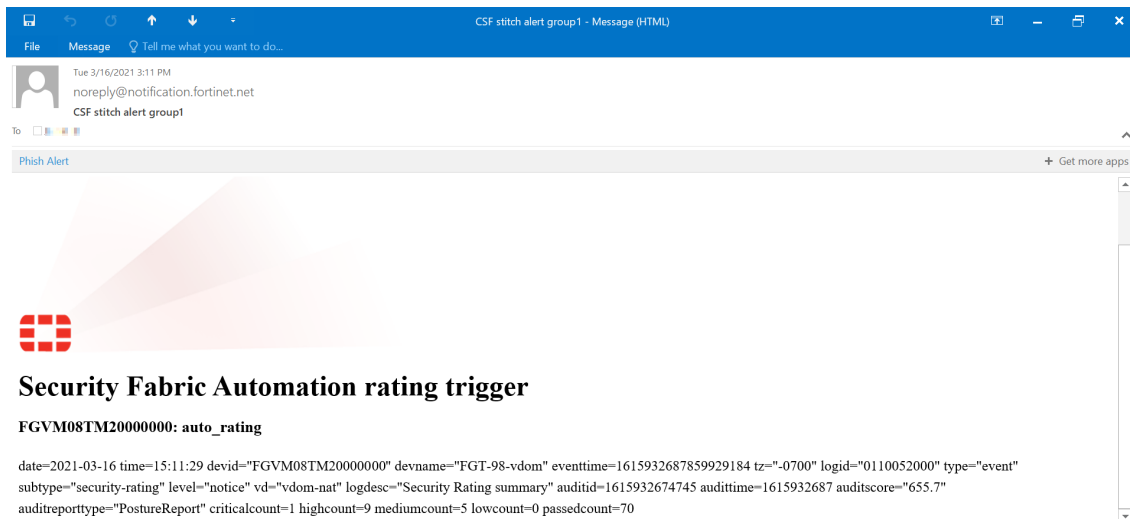
d. Click **OK**.

e. Select the action in the list and click **Apply**.

5. Click **OK**.

6. Right-click the automation stitch, and click **Test Automation Stitch**.

After the Security Rating report is finished, the automation is triggered, and the email is delivered with the customized replacement message in the email body.



To configure the replacement message group in the CLI:

```
config system replacemsg-group
  edit "group-sec1"
    set comment ""
```

```
        set group-type utm
    config automation
        edit "automation-email"
            set buffer "...<h1> Security Fabric Automation rating trigger </h1>..."
            ...
        next
    end
next
end
```

To configure the email action in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
    edit "rating_posture"
        set description "rating test"
        set event-type security-rating-summary
    next
end
```

2. Configure the automation action:

```
config system automation-action
    edit "email-group1"
        set action-type email
        set email-to "admin@fortinet.com"
        set email-subject "CSF stitch alert group1"
        set replacement-message enable
        set replacemsg-group "group-sec1"
    next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
    edit "auto_rating"
        set trigger "rating_posture"
        set action "email-group1"
    next
end
```

4. To view the automation stitch information after it is triggered:

```
# diagnose test application autod 3
stitch: auto_rating
    local hit: 1 relayed to: 0 relayed from: 0
    last trigger: Tue Mar 16 15:11:29 2021
    last relay:
    actions:
        email-group1:
            done: 1 relayed to: 0 relayed from: 0
            last trigger: Tue Mar 16 15:11:29 2021
            last relay:

logid2stitch mapping:
id:52000  local hit: 1 relayed hits: 0
    auto_rating
```

Security ratings

This section includes information about security rating related new features:

- [Security Rating overlays on page 109](#)
- [Add test to check for two-factor authentication on page 112](#)
- [Add test to check for activated FortiCloud services on page 113](#)
- [Add tests for high priority vulnerabilities 7.0.1 on page 114](#)

Security Rating overlays

Security Rating notifications are shown on settings pages, which list configuration issues determined by the Security Rating report. You can open the recommendations to see which configuration items need to be fixed. This frees you from going back and forth between the *Security Rating* page and the specific settings page. Notifications appear either in the gutter, footer, or as a mutable.

There are overlay checks for the following test cases:

- Duplicate policy objects
- NTP is synchronized
- System uptime
- Local log disk space is full
- Certificate expiry date

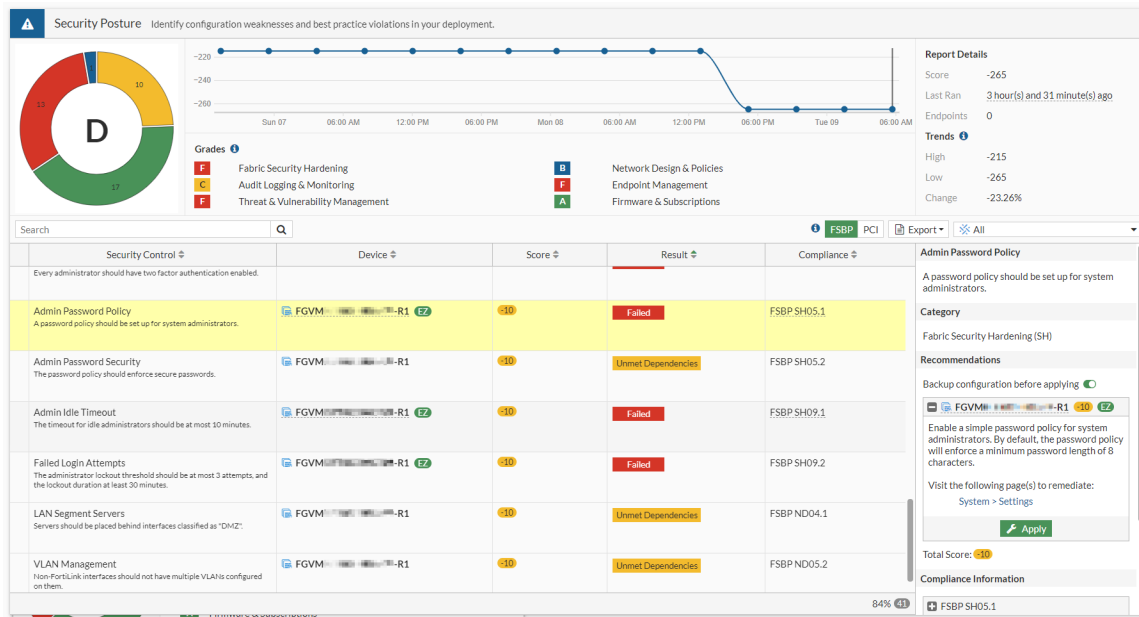
Notifications can be dismissed in the GUI. Dismissed issues are unique for each administrator. Hashes for dismissed notifications are saved in local storage. If a user clears the local storage, all issues will show up again as not dismissed.



A Security Rating license is required for some of the overlays and associated pages to function. These Security Rating overlays are available on downstream and multi-VDOM FortiGates.

Scorecard links

On the *Security Fabric > Security Rating* page, if there is a failed check on the scorecard, there is a link in the description that takes you to the page to resolve the problem. In this example, there is an issue with the administrator password policy that can be resolved on the *System > Settings* page.



Notification locations

On the *System > Settings* page, there is a *Security Rating Issues* section in the right-side gutter. To dismiss a notification, hover over the issue and click the X beside it. To view dismissed notifications, enable *Show Dismissed*.

System Settings

Host name: FGVM-R1

System Time

Current system time: 2021/02/09 09:18:34

Time zone: [GMT-8:00] Pacific Time (US & Canada)

Set Time: NTP PTP Manual settings

Select server: FortiGuard Custom

Sync Interval: 60 Minutes (1 - 1440)

Setup device as local NTP server: ☐

Administration Settings

HTTP port: 80

Redirect to HTTPS: ☒

HTTPS port: 443

Port conflicts with the SSL-VPN port setting

HTTPS server certificate: self-sign

SSH port: 22

Telnet port: 23

Idle timeout: 480 Minutes (1 - 480)

Allow concurrent sessions: ☒

Redirect to HTTPS: ☒

FortiCloud Single Sign-On: ☐

WiFi Settings

WiFi certificate: Fortinet_Wifi

WiFi CA certificate: Fortinet_Wifi_CA

WiFi country/region: United States

Password Policy

Additional Information

API Preview

Edit in CLI

Virtual Domain

How to Configure Virtual Domains

Documentation

Online Help

Video Tutorials

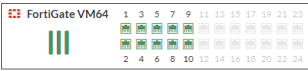
Security Rating Issues

- Default Port HTTPS
- Default Port SSH
- USB Auto Configuration
- Valid HTTPS Certificate - Adminis..
- Admin Password Policy
- Admin Idle Timeout

Show Dismissed: ☐

Apply

On the *Network > Interfaces* page, there is a *Security Rating Issues* section in the table footer. Click *Security Rating Issues* to view the list of issues. To dismiss a notification, click the X beside it. To view dismissed notifications, click *Show Dismissed*.

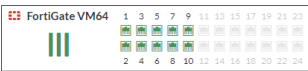


Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Physical Interface 22							
port1	Physical Interface		172.16.151.87/255.255.255.0	PING HTTPS SSH SNMP			16
port2	Physical Interface		192.168.2.87/255.255.255.0	PING HTTPS SSH SNMP HTTP			5
port3	Physical Interface		192.168.102.1/255.255.255.0	PING HTTPS HTTP			7
port4	Physical Interface		192.168.80.87/255.255.255.0				4
port5	Physical Interface		0.0.0.0/0.0.0.0				1
port6	Physical Interface		0.0.0.0/0.0.0.0				0
Software Switch 1							
wqt.root	Software Switch	wqtn.28.test	10.253.255.254/255.255.240.0			10.253.240.1-10.253.255.253	1
Virtual Wire Pair 2							
vwp78	Virtual Wire Pair						0
vwp910	Virtual Wire Pair						0
WiFi SSID 2							
fortinet	WiFi SSID		0.0.0.0/0.0.0.0	HTTP			?

Security Rating Issues 0% Updated: 18:27:53

Notification pop-ups

When you click a Security Rating notification, a pop-up appears and the related setting is highlighted in the GUI. The pop-up contains a description of the problem and a timestamp of when the issue was found.



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Physical Interface 22							
port1	Physical Interface		172.16.151.87/255.255.255.0	PING HTTPS SSH SNMP			16
port2	Physical Interface		192.168.2.87/255.255.255.0	PING HTTPS SSH SNMP HTTP			5
port3	Physical Interface		192.168.102.1/255.255.255.0	PING HTTPS HTTP			7
port4	Physical Interface		192.168.80.87/255.255.255.0				4
port5	Physical Interface		0.0.0.0/0.0.0.0				1
port6	Physical Interface		0.0.0.0/0.0.0.0				0
Software Switch 1							
wqt.root	Software Switch	wqtn.28.test	10.253.255.254/255.255.240.0			10.253.240.1-10.253.255.253	1
Virtual Wire Pair 2							
vwp78	Virtual Wire Pair						0
vwp910	Virtual Wire Pair						0
WiFi SSID 2							
fortinet	WiFi SSID		0.0.0.0/0.0.0.0	HTTP			?

Security Rating Issues 0% Updated: 18:27:53

Interface Classification 1/2

Define a role for this interface.

As of 50 minutes ago.

← → ×

face

face

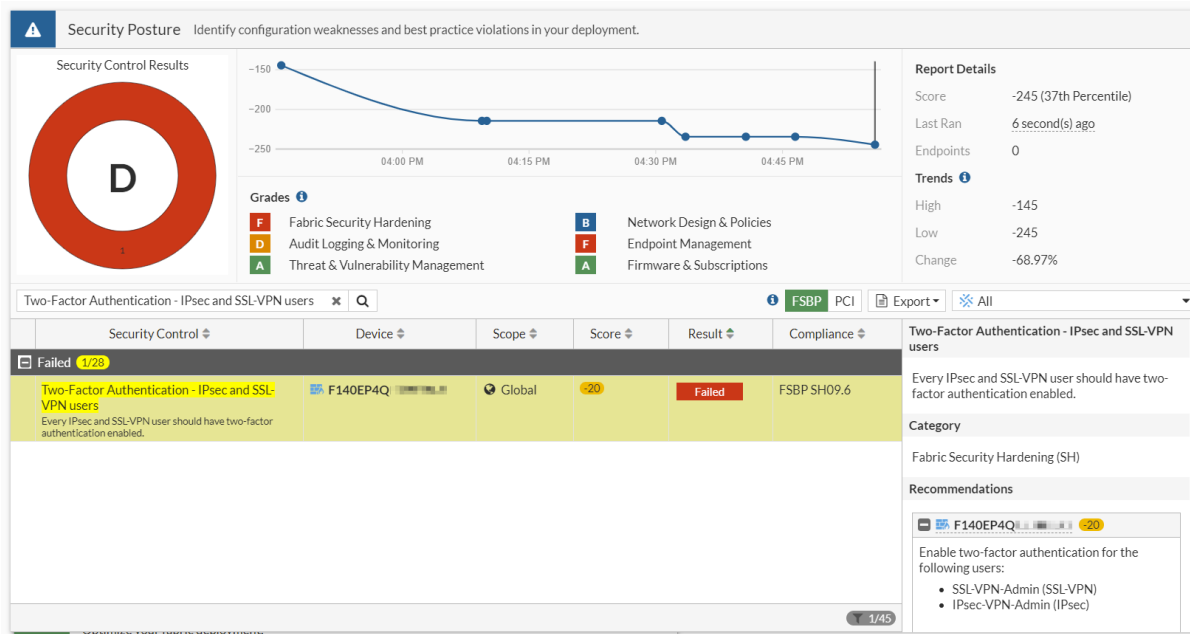
face

Once an issue is resolved, the notification disappears after the next Security Rating report runs.

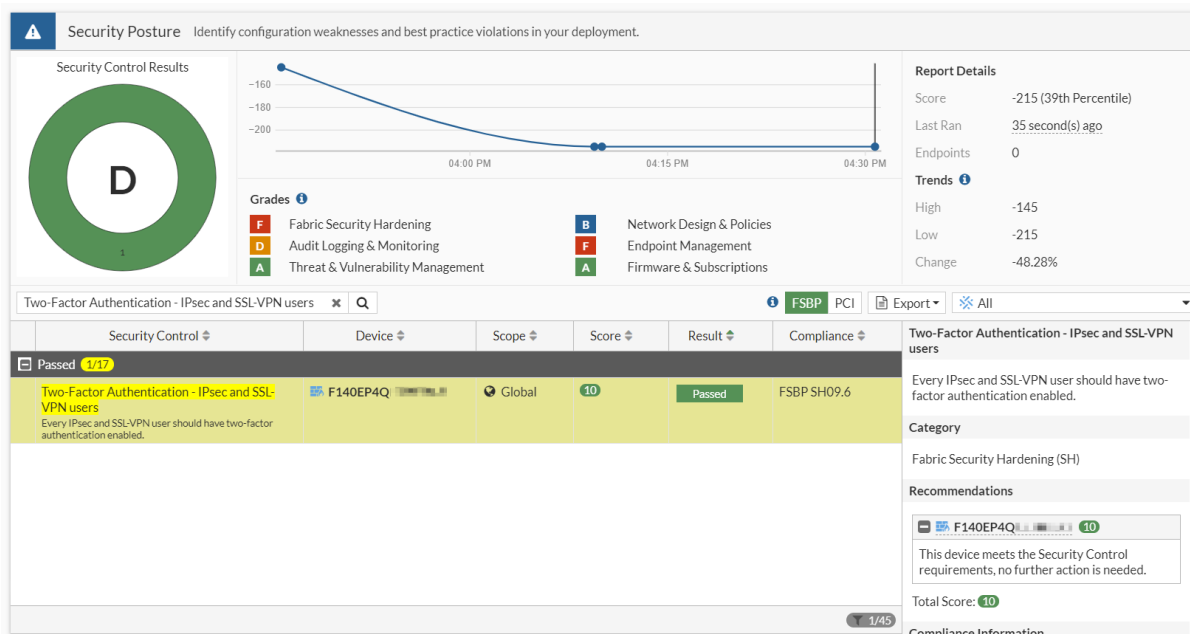
Add test to check for two-factor authentication

There is a new Security Rating test to check if two-factor authentication is enabled for each active SSL VPN and IPsec user. This test is located in the *Security Posture* scorecard.

In this result, the test is marked as *Failed* because not all users have two-factor authentication enabled.



In this result, the test is marked as *Passed* because all users have two-factor authentication enabled.

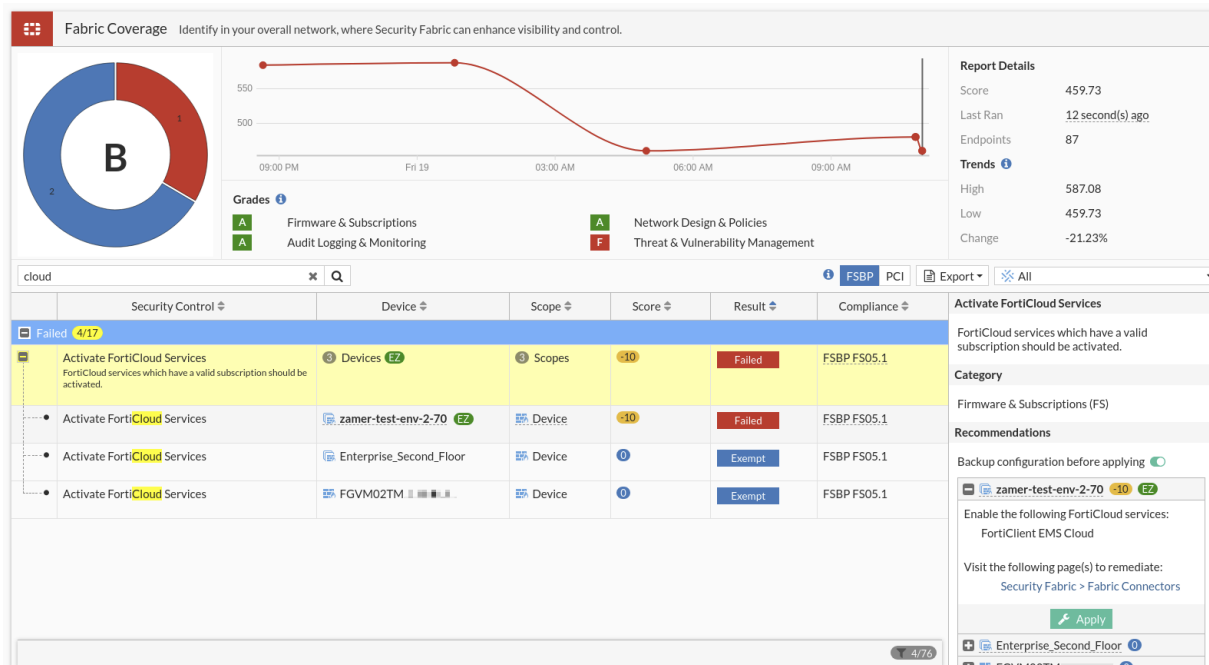


Add test to check for activated FortiCloud services

There is a new Security Rating test, *Activate FortiCloud Services*, that checks whether FortiCloud services can be activated for FortiAnalyzer Cloud, FortiManager Cloud, FortiClient EMS Cloud, and FortiSandbox Cloud. This test is located in the *Fabric Coverage* scorecard.

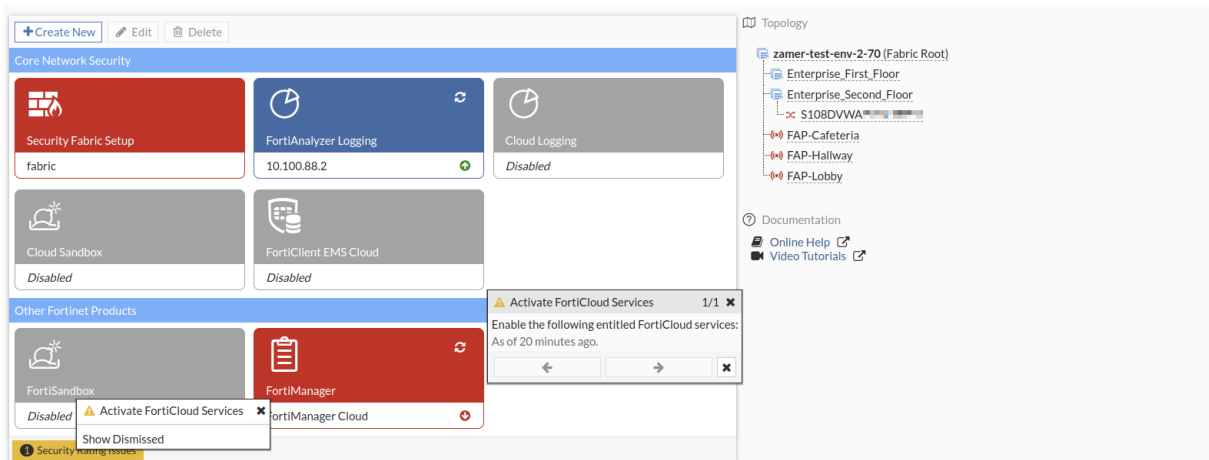
The test fails if the account has a valid subscription to a service or cloud appliance, but has not enabled the Fabric connection to it on the FortiGate. The test is exempt if there are no licenses for FortiCloud services on the particular device.

In this result, the test is marked as *Failed* because FortiClient EMS Cloud is not activated.

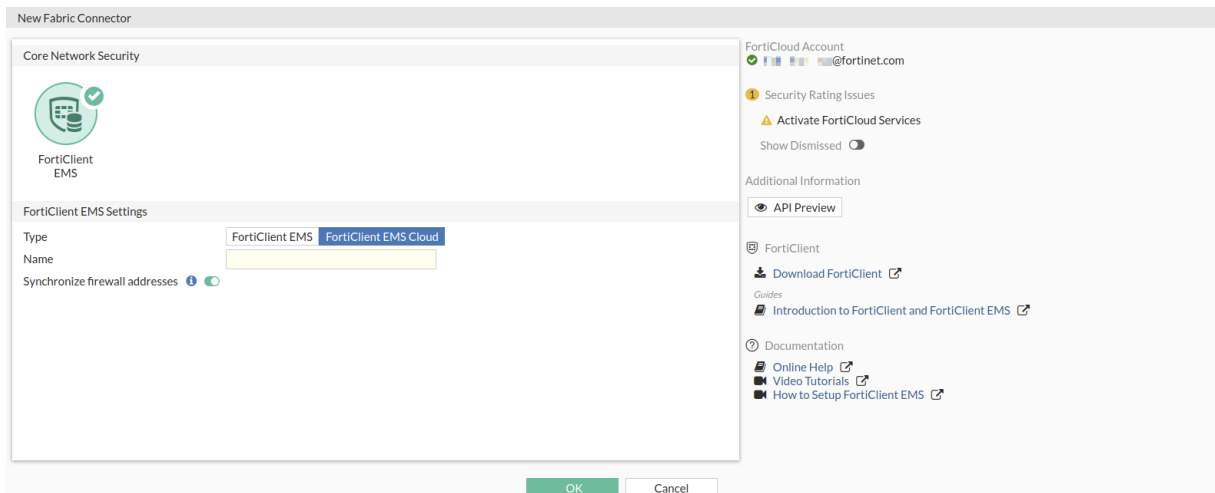


Click *Apply* to fix the issue, or click the link to go to the *Security Fabric > Fabric Connectors* page to view the Security Rating notifications.

Click *Security Rating Issues* to view the list of issues, then click *Activate FortiCloud Services*.



This brings you to the FortiClient EMS Fabric connector page where you can enable the service.

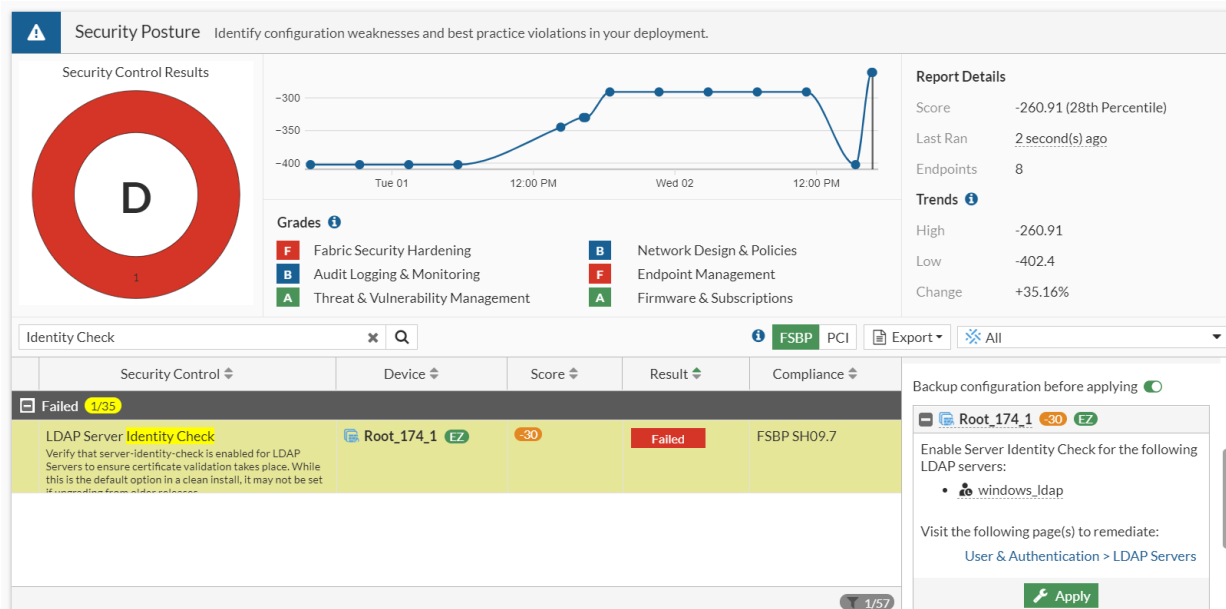


Add tests for high priority vulnerabilities - 7.0.1

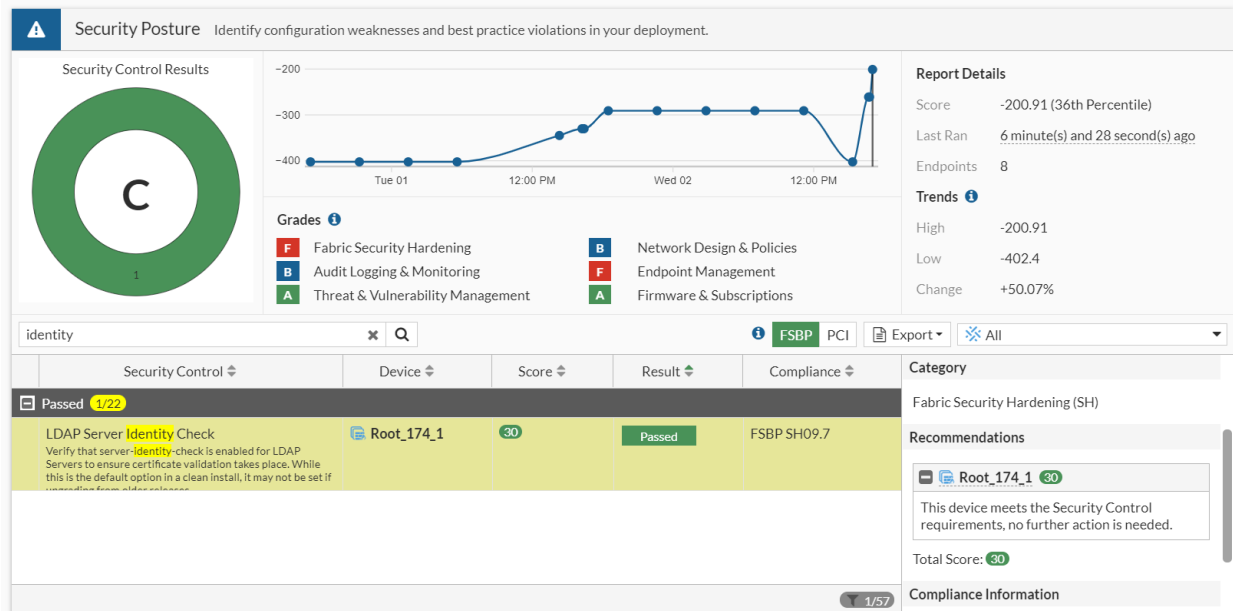
Two new Security Rating tests pertaining to access control and authentication have been added to mitigate high priority vulnerabilities: *LDAP Server Identity Check* and *Disable Username Sensitivity Check*. These tests are located in the *Security Posture* scorecard.

LDAP Server Identity Check ensures that certificate validation takes place against an LDAP server.

In this result, the test is marked as *Failed* because the *Server identity check* setting (`set server-identity-check`) is disabled in the LDAP server settings.

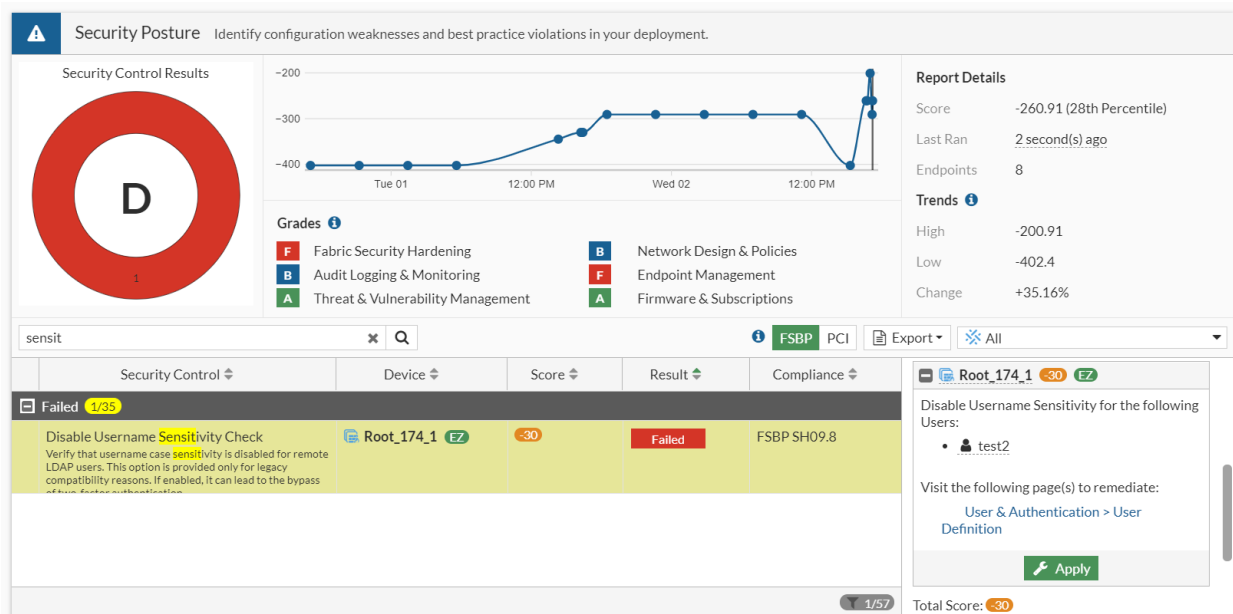


In this result, the test is marked as *Passed* because the *Server identity check* setting (`set server-identity-check`) is enabled in the LDAP server settings.

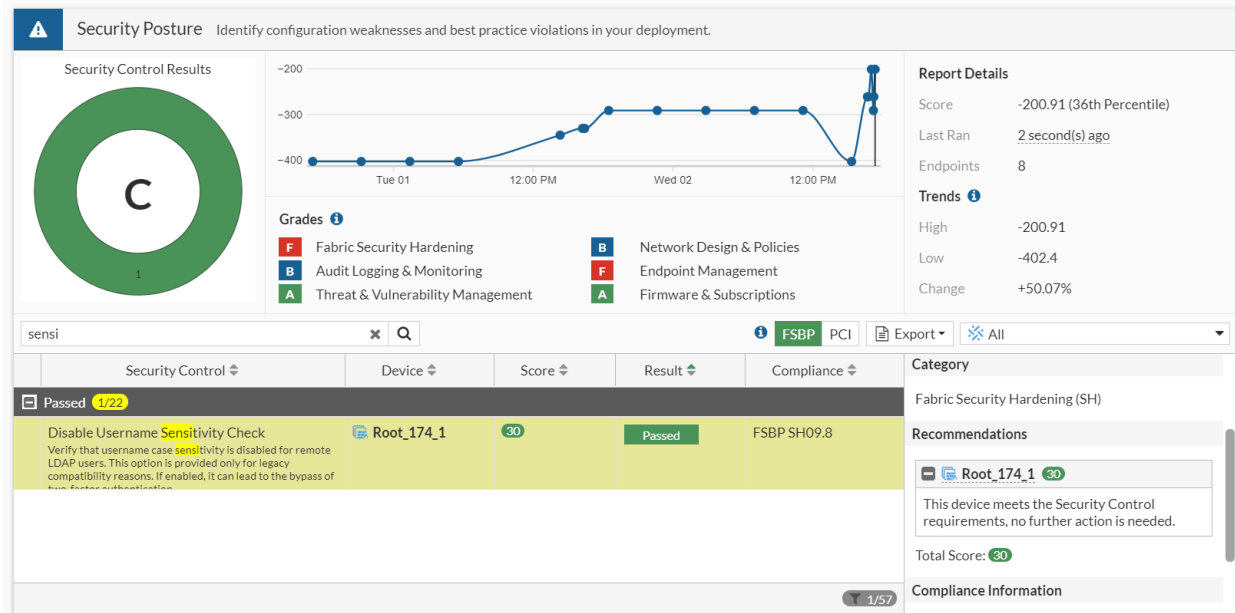


Disable Username Sensitivity Check ensures that users cannot bypass two-factor authentication with a username that has a different case than the configured user object.

In this result, the test is marked as *Failed* because in the local user settings, `username-sensitivity` is set to enable.



In this result, the test is marked as *Passed* because in the local user settings, `username-sensitivity` is set to disable.



Network

This section includes information about network related new features:

- [SD-WAN on page 117](#)
- [General on page 151](#)
- [IPv6 on page 206](#)
- [Web proxy on page 220](#)

SD-WAN

This section includes information about SD-WAN related new features:

- [Usability enhancements to SD-WAN Network Monitor service on page 117](#)
- [Hold down time to support SD-WAN service strategies on page 119](#)
- [Passive WAN health measurement on page 120](#)
- [SD-WAN passive health check configurable on GUI 7.0.1 on page 121](#)
- [ECMP support for the longest match in SD-WAN rule matching 7.0.1 on page 123](#)
- [Override quality comparisons in SD-WAN longest match rule matching 7.0.1 on page 125](#)
- [Specify an SD-WAN zone in static routes and SD-WAN rules 7.0.1 on page 128](#)
- [Display ADVPN shortcut information in the GUI 7.0.1 on page 132](#)
- [Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1 on page 133](#)
- [Interface based QoS on individual child tunnels based on speed test results 7.0.1 on page 140](#)
- [Passive health-check measurement by internet service and application 7.0.2 on page 143](#)
- [Adaptive Forward Error Correction 7.0.2 on page 147](#)

Usability enhancements to SD-WAN Network Monitor service

The SD-WAN Network Monitor service now supports running a speed test based on a schedule. The test results are automatically updated in the interface `measured-upstream-bandwidth` and `measured-downstream-bandwidth` fields. These fields do not impact the interface inbound bandwidth, outbound bandwidth, estimated upstream bandwidth, or estimated downstream bandwidth settings.

When the scheduled speed tests run, it is possible to temporarily bypass the bandwidth limits set on the interface and configure custom maximum or minimum bandwidth limits. These configurations are optional.

```
config system speed-test-schedule
edit <interface>
    set schedules <schedule> ...
    set update-inbandwidth enable {enable | disable}
    set update-outbandwidth enable {enable | disable}
    set update-inbandwidth-maximum <integer>
    set update-inbandwidth-minimum <integer>
    set update-outbandwidth-maximum <integer>
    set update-outbandwidth-minimum <integer>
```

```

    next
end

```

<code>update-inbandwidth enable {enable disable}</code>	Enable/disable bypassing the interface's inbound bandwidth setting.
<code>update-outbandwidth enable {enable disable}</code>	Enable/disable bypassing the interface's outbound bandwidth setting.
<code>update-inbandwidth-maximum <integer></code>	Maximum downloading bandwidth to be used in a speed test, in Kbps (0 - 16776000).
<code>update-inbandwidth-minimum <integer></code>	Minimum downloading bandwidth to be considered effective, in Kbps (0 - 16776000).
<code>update-outbandwidth-maximum <integer></code>	Maximum uploading bandwidth to be used in a speed test, in Kbps (0 - 16776000).
<code>update-outbandwidth-minimum <integer></code>	Minimum uploading bandwidth to be considered effective, in Kbps (0 - 16776000).

In the following example, a speed test is scheduled on port1 at 10:00 AM, and another one at 14:00 PM.

To run a speed test based on a schedule:

1. Configure the recurring schedules:

```

config firewall schedule recurring
    edit "10"
        set start 10:00
        set end 12:00
        set day monday tuesday wednesday thursday friday
    next
    edit "14"
        set start 14:00
        set end 16:00
        set day monday tuesday wednesday thursday friday
    next
end

```

2. Configure the speed test schedule:

```

config system speed-test-schedule
    edit "port1"
        set schedules "10" "14"
        set update-inbandwidth enable
        set update-outbandwidth enable
        set update-inbandwidth-maximum 60000
        set update-inbandwidth-minimum 10000
        set update-outbandwidth-maximum 50000
        set update-outbandwidth-minimum 10000
    next
end

```

3. View the speed test results:

```

config system interface
    edit port1

```

```

get | grep measure
  measured-upstream-bandwidth: 23691
  measured-downstream-bandwidth: 48862
  bandwidth-measure-time: Wed Jan 27 14:00:39 2021
next
end

```

Hold down time to support SD-WAN service strategies

In a hub and spoke SD-WAN topology with shortcuts created over ADVPN, a downed or recovered shortcut can affect which member is selected by an SD-WAN service strategy. When a downed shortcut tunnel recovers and the shortcut is added back into the service strategy, the shortcut is held at a low priority until the hold down time has elapsed.

By default, the hold down time is zero seconds. It can be set to 0 - 10000000 seconds.

To configure the hold down time:

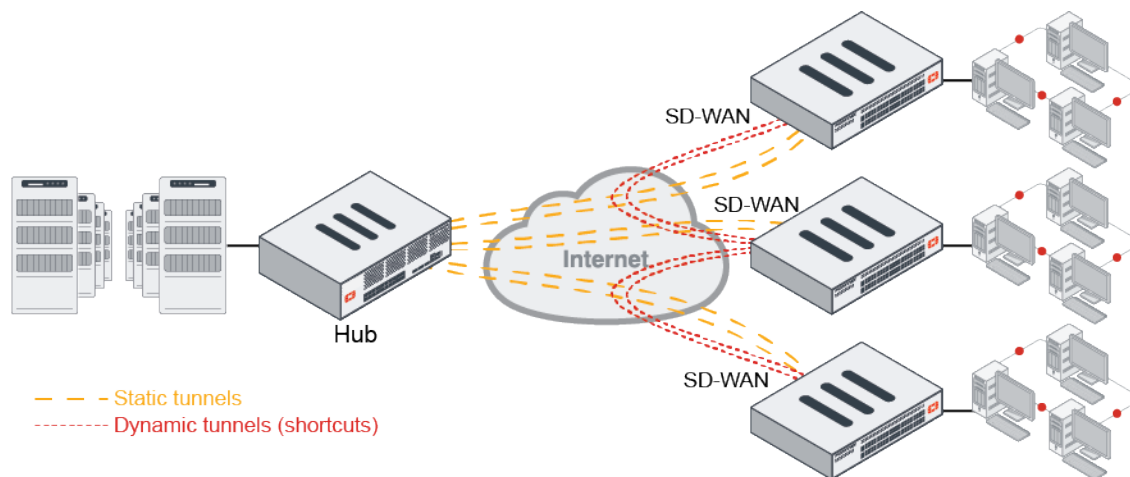
```

config system sdwan
  config service
    edit 1
      set hold-down-time <integer>
    next
  end
end

```

Example

In this example, the hold down time is set to 15 seconds, and then the SD-WAN service is looked at before and after the hold down elapses after a downed shortcut recovers.



To configure the hold down time:

```

config system sdwan
  config service
    edit 1
      set hold-down-time 15
    next
  end
end

```

```

        next
    end
end

```

To view which SD-WAN member is selected before and after the hold down time elapses:

Before the hold down time has elapsed:

```

# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
    Gen(34), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(ping)
Hold down time(15) seconds, Hold start at 2003 second, now 2010
Member sub interface(4):
    1: seq_num(1), interface(vd2-1):
        1: vd2-1_0(86)
    3: seq_num(2), interface(vd2-2):
        1: vd2-2_0(88)

Members(4):
    1: Seq_num(1 vd2-1), alive, packet loss: 27.000%, selected
    2: Seq_num(2 vd2-2_0), alive, packet loss: 0.000%, selected
    3: Seq_num(2 vd2-2), alive, packet loss: 0.000%, selected
    4: Seq_num(1 vd2-1_0), alive, packet loss: 61.000%, selected
Dst address(1):
    33.1.1.101-33.1.1.200

```

After the hold down time has elapsed:

```

# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
    Gen(35), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(ping)
Hold down time(15) seconds, Hold start at 2018 second, now 2019
Member sub interface(4):

    2: seq_num(2), interface(vd2-2):
        1: vd2-2_0(88)
    3: seq_num(1), interface(vd2-1):
        1: vd2-1_0(86)
Members(4):
    1: Seq_num(2 vd2-2_0), alive, packet loss: 0.000%, selected
    2: Seq_num(2 vd2-2), alive, packet loss: 0.000%, selected
    3: Seq_num(1 vd2-1), alive, packet loss: 24.000%, selected
    4: Seq_num(1 vd2-1_0), alive, packet loss: 44.000%, selected
Dst address(1):
    33.1.1.101-33.1.1.200\

```

Passive WAN health measurement

SD-WAN passive WAN health measurement determines the health check measurements using session information that is captured on firewall policies that have `passive-wan-health-measurement` enabled.

Using passive WAN health measurement reduces the amount of configuration required and decreases the traffic that is produced by health check monitor probes doing active measurements. Active WAN health measurement using a detection server might not reflect the real-life traffic.

By default, active WAN health measurement is enabled.

To configure passive WAN health check:

```
config system sdwan
  config health-check
    edit "1"
      set server <ip_address>
      set detect-mode {passive | prefer-passive}
      set members <members>
    next
  end
end
```

passive	Health is measured using traffic, without probes. No link health monitor needs to be configured.
prefer-passive	Health is measured using traffic when there is traffic, and using probes when there is no traffic. A link health monitor must be configured, see Link health monitor for details.

To enable passive WAN health measurement in a policy:

```
config firewall policy
  edit 1
    set passive-wan-health-measurement enable
  next
end
```



When `passive-wan-health-measurement` is enabled, `auto-asic-offload` will be disabled.

SD-WAN passive health check configurable on GUI - 7.0.1

SD-WAN passive WAN health can be configured in the GUI.

By enabling passive health check in a policy, TCP traffic on that policy will be used in health check measurements.

To configure passive WAN health check in the GUI:

1. Go to *Network > SD-WAN* and select the *Performance SLAs* tab.
2. Edit an existing health check, or create a new one.
3. Set *Probe mode* to *Passive* or *Prefer Passive*.

Edit Performance SLA

Name

test

Probe mode

Active | **Passive** | Prefer Passive

Participants

All SD-WAN Members

Specify

port12

To_Juniper_ge-0/0/2 (port13)

SLA Target

Latency threshold

5

ms

Jitter threshold

5

ms

Packet Loss threshold

0

%

Actions when inactive

Update static route

OK Cancel

SLA Details

	Packet Loss	Latency	Jitter
To_Juniper_ge-0/0/2 (port13)	0.00%	10.00ms	0.00ms
port12	0.00%	0.00ms	0.00ms

Additional Information

API Preview

Edit in CLI

Performance SLA Setup Guides

Link Monitoring

SLA Targets

Documentation

Online Help

Video Tutorials

Edit Performance SLA

Name

preferpassive

Probe mode

Active | Passive | **Prefer Passive**

Protocol

Ping | HTTP | DNS

Server

10.100.2.22

Participants

All SD-WAN Members | Specify

SLA Target

Link Status

Check Interval

500

ms

Failures before inactive

5

Restore link after

5

check(s)

Actions when inactive

Update static route

OK Cancel

SLA Details

	Packet Loss	Latency	Jitter
To_Juniper_ge-0/0/2 (port13)	0.00%	10.73ms	0.00ms
port12	0.00%	0.22ms	0.05ms

Additional Information

API Preview

Edit in CLI

Performance SLA Setup Guides

Link Monitoring

SLA Targets

Documentation

Online Help

Video Tutorials

4. Configure the remaining settings as needed.

5. Click **OK**.

The SLA list shows the probe mode in the *Detect Server* column, if the probe mode is passive or prefer passive.

SD-WAN Zones SD-WAN Rules Performance SLAs							
Packet Loss	Latency	Jitter					
0.01ms							port12
0.01ms							port13
0ms							
0ms							
0ms							
<div> <div>Create New</div> <div>Edit</div> <div>Delete</div> <div>Search</div> </div>							
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold	
preferpassive	10.100.2.22 (Prefer Passive)	port12: 0.00% To_Juniper_ge-0/0/2 (port13): 0.00%	port12: 0.19ms To_Juniper_ge-0/0/2 (port13): 0.94ms	port12: 0.03ms To_Juniper_ge-0/0/2 (port13): 0.00ms	5	5	
test	(Passive)	port12: 0.00% To_Juniper_ge-0/0/2 (port13): 0.00%	port12: 0.00ms To_Juniper_ge-0/0/2 (port13): 1.80ms	port12: 0.00ms To_Juniper_ge-0/0/2 (port13): 0.00ms	22	44	



Probe packets can only be disabled in the CLI and when the probe mode is not passive.

To enable passive WAN health measurement in a policy in the GUI:

1. Go to *Policy & Objects > Firewall Policy*.
2. Edit an existing policy, or create a new one.
3. Set *Outgoing Interface* to an SD-WAN zone. Passive health check can only be enabled in a policy when the outgoing interface is an SD-WAN zone.
4. Enable *Passive Health Check*.

5. Configure the remaining settings as needed.
6. Click OK.

ECMP support for the longest match in SD-WAN rule matching - 7.0.1

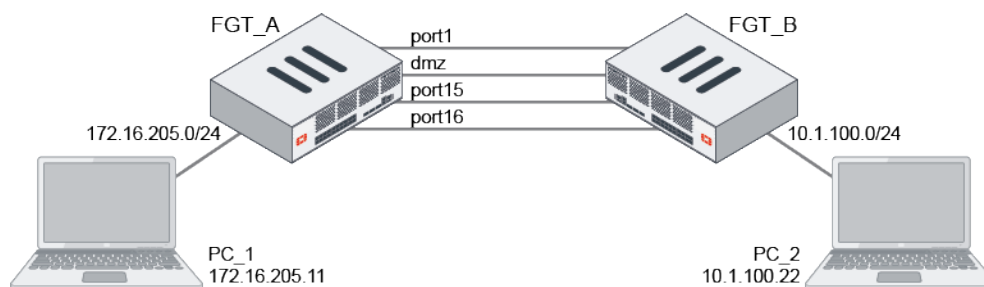
The longest match SD-WAN rule can match ECMP best routes. The rule will select the egress ports on ECMP specific routes, and not the less specific routes, to transport traffic.

The service mode determines which egress port on the ECMP specific routes is selected to forward traffic:

- Manual (`manual`): The first configured alive port is selected.
- Best Quality (`priority`): The best quality port is selected.
- Lowest Cost (`sla`): The first configured or lower cost port in SLA is selected.

Example

By default, SD-WAN selects the outgoing interface from all of the links that have valid routes to the destination. In some cases, it is required that only the links that have the best (or longest match) routes (single or ECMP) to the destination are considered.



In this example, four SD-WAN members in two zones are configured. The remote PC (PC_2 - 10.1.100.22) is accessible on port15 and port16, even though there are valid routes for all of the SD-WAN members. A single SD-WAN service rule is configured that allows traffic to be balanced between all four of the members, but only chooses between port15 and port16 for the specific 10.1.100.22 address.

A performance SLA health check is configured to monitor 10.1.100.2. An SD-WAN service rule in Lowest Cost (SLA) mode is configured to select the best interface to steer the traffic. In the rule, the method of selecting a member if more than one meets the SLA (`tie-break`) is configured to select members that meet the SLA and match the longest prefix

in the routing table (`fib-best-match`). If there are multiple ECMP routes with the same destination, the FortiGate will take the longest (or best) match in the routing table, and choose from those interface members.

To configure the SD-WAN:

```
config system sdwan
  config zone
    edit "virtual-wan-link"
    next
    edit "z1"
    next
  end
  config members
    edit 1
      set interface "port1"
      set gateway 172.16.200.2
    next
    edit 2
      set interface "dmz"
      set gateway 172.16.208.2
    next
    edit 3
      set interface "port15"
      set zone "z1"
      set gateway 172.16.209.2
    next
    edit 4
      set interface "port16"
      set zone "z1"
      set gateway 172.16.210.2
    next
  end
  config health-check
    edit "1"
      set server "10.1.100.2"
      set members 0
      config sla
        edit 1
          next
        end
      next
    end
  next
end
config service
  edit 1
    set name "1"
    set mode sla
    set dst "all"
    set src "172.16.205.0"
    config sla
      edit "1"
        set id 1
      next
    end
    set priority-members 1 2 3 4
    set tie-break fib-best-match
  next
```

```
end
end
```

To check the results:

1. The debug shows the SD-WAN service rule. All of the members meet SLA, and because no specific costs are attached to the members, the egress interface is selected based on the interface priority order that is configured in the rule:

```
FGT_A (root) # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Members(4):
  1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected
  2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  3: Seq_num(3 port15), alive, sla(0x1), gid(0), cfg_order(2), cost(0), selected
  4: Seq_num(4 port16), alive, sla(0x1), gid(0), cfg_order(3), cost(0), selected
Src address(1):
  172.16.205.0-172.16.205.255
Dst address(1):
  0.0.0.0-255.255.255.255
```

2. The routing table shows that there are ECMP default routes on all of the members, and ECMP specific (or best) routes only on port15 and port16:

```
FGT_A (root) # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 172.16.200.2, port1
          [1/0] via 172.16.208.2, dmz
          [1/0] via 172.16.209.2, port15
          [1/0] via 172.16.210.2, port16
S       10.1.100.22/32 [10/0] via 172.16.209.2, port15
          [10/0] via 172.16.210.2, port16
```

Because tie-break is set to fib-best-match, the first configured member from port15 and port16 is selected to forward traffic to PC_2. For all other traffic, the first configured member from all four of the interfaces is selected to forward traffic.

3. On PC-1, generate traffic to PC-2:

```
ping 10.1.100.22
```

4. On FGT_A, sniff for traffic sent to PC_2:

```
# diagnose sniffer packet any 'host 10.1.100.22' 4
interfaces=[any]
filters=[host 10.1.100.22]
2.831299 port5 in 172.16.205.11 -> 10.1.100.22: icmp: echo request
2.831400 port15 out 172.16.205.11 -> 10.1.100.22: icmp: echo request
```

Traffic is leaving on port15, the first configured member from port15 and port16.

Override quality comparisons in SD-WAN longest match rule matching - 7.0.1

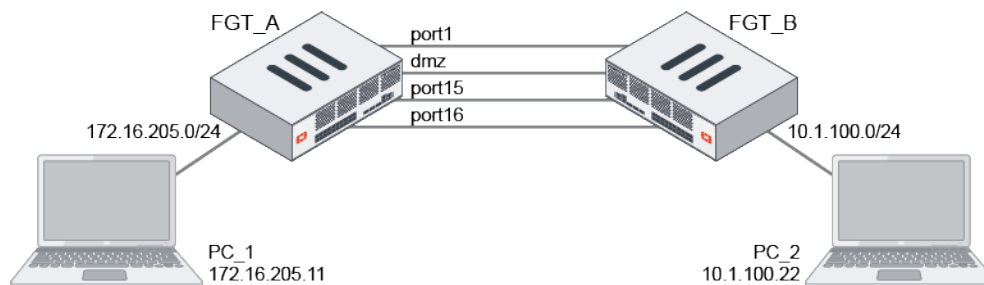
In SD-WAN rules, the longest match routes will override the quality comparisons when all of the specific routes are out of SLA.

With this feature in an SD-WAN rule:

- **Lowest Cost (sla):** Even though all of the egress ports on specific routes (longest matched routes) are out of SLA, the SD-WAN rule still selects the first configured or lower-cost port from the egress ports to forward traffic.
- **Best Quality (priority):** Even though the egress ports on specific routes (longest matched routes) have worse quality than all other ports on less specific routes, the SD-WAN rule still selects the best quality port from the ports on specific routes to forward traffic.

This feature avoids a situation where, if the members on specific routes (longest matched routes) are out of SLA or have worse quality, the traffic might be forwarded to the wrong members in SLA (higher quality) on the default or aggregate routes.

Example



In this example, four SD-WAN members in two zones are configured. The remote PC (PC_2 - 10.1.100.22) is accessible on port15 and port16, even though there are valid routes for all of the SD-WAN members. A single SD-WAN service rule is configured that allows traffic to be balanced between all four of the members, but only chooses between port15 and port16 for the specific 10.1.100.22 address. If neither port15 nor port16 meet the SLAs, traffic will be forwarded on one of these interfaces, instead of on port1 or dmz.

A performance SLA health check is configured to monitor 10.1.100.2. An SD-WAN service rule in Lowest Cost (SLA) mode is configured to select the best interface to steer the traffic. In the rule, the method of selecting a member if more than one meets the SLA (tie-break) is configured to select members that meet the SLA and match the longest prefix in the routing table (fib-best-match). If there are multiple ECMP routes with the same destination, the FortiGate will take the longest (or best) match in the routing table, and choose from those interface members.

To configure the SD-WAN:

```
config system sdwan
  config zone
    edit "virtual-wan-link"
    next
    edit "z1"
    next
  end
  config members
    edit 1
      set interface "port1"
      set gateway 172.16.200.2
    next
    edit 2
      set interface "dmz"
      set gateway 172.16.208.2
```

```

    next
    edit 3
        set interface "port15"
        set zone "z1"
        set gateway 172.16.209.2
    next
    edit 4
        set interface "port16"
        set zone "z1"
        set gateway 172.16.210.2
    next
end
config health-check
    edit "1"
        set server "10.1.100.2"
        set members 0
        config sla
            edit 1
                next
            end
        next
    end
next
end
config service
    edit 1
        set name "1"
        set mode sla
        set dst "all"
        set src "172.16.205.0"
        config sla
            edit "1"
                set id 1
            next
        end
        set priority-members 1 2 3 4
        set tie-break fib-best-match
    next
end
end

```

To check the results:

1. The debug shows the SD-WAN service rule. Both port15 and port16 are up, but out of SLA:

```

FGT_A (root) # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(3), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Members(4):
  1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected
  2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  3: Seq_num(3 port15), alive, sla(0x0), gid(0), cfg_order(2), cost(0), selected
  4: Seq_num(4 port16), alive, sla(0x0), gid(0), cfg_order(3), cost(0), selected
Src address(1):
  172.16.205.0-172.16.205.255

Dst address(1):
  0.0.0.0-255.255.255.255

```

- The routing table shows that there are ECMP default routes on all of the members, and ECMP specific (or best) routes only on port15 and port16:

```
FGT_A (root) # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 172.16.200.2, port1
          [1/0] via 172.16.208.2, dmz
          [1/0] via 172.16.209.2, port15
          [1/0] via 172.16.210.2, port16
S       10.1.100.22/32 [10/0] via 172.16.209.2, port15
          [10/0] via 172.16.210.2, port16
```

Because tie-break is set to fib-best-match, even though both port15 and port16 are out of SLA, the first configured member of the two (port15) is selected to forward traffic to PC_2. For all other traffic, the first configured member from all of the interfaces that are in SLA is selected to forward traffic (port1).

- On PC-1, generate traffic to PC-2:

```
ping 10.1.100.22
```

- On FGT_A, sniff for traffic sent to PC_2:

```
# diagnose sniffer packet any 'host 10.1.100.22' 4
interfaces=[any]
filters=[host 10.1.100.22]
2.831299 port5 in 172.16.205.11 -> 10.1.100.22: icmp: echo request
2.831400 port15 out 172.16.205.11 -> 10.1.100.22: icmp: echo request
```

Traffic is leaving on port15, the first configured member from port15 and port16, even though both are out of SLA.

Specify an SD-WAN zone in static routes and SD-WAN rules - 7.0.1

SD-WAN zones can be used in IPv4 and IPv6 static routes, and in SD-WAN service rules. This makes route configuration more flexible, and simplifies SD-WAN rule configuration. The `sdwan-zone` command replaces the `sdwan {enable | disable}` command.

A new predefined SD-WAN zone called SASE is also available.

To configure an SD-WAN zone in a static route:

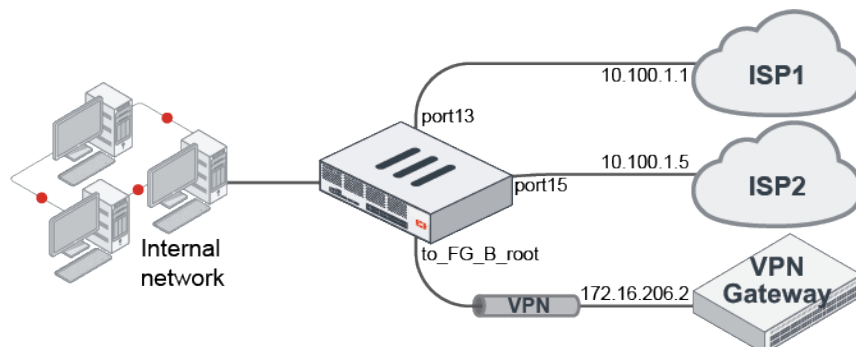
```
config router {static | static6}
  edit 1
    set sdwan-zone <zone> <zone> ...
  next
end
```

To configure an SD-WAN zone in an SD-WAN rule:

```
config system sdwan
  config service
    edit 1
      set priority-zone <zone>
    next
  end
end
```

Examples

In these two examples, three SD-WAN members are created. Two members, port13 and port15, are in the default zone (*virtual-wan-link*), and the third member, to_FG_B_root, is in the *SASE* zone.



Example 1

In this example:

- Two service rules are created. Rule 1 uses the *virtual-wan-link* zone, and rule 2 uses the *SASE* zone.
- Two IPv4 static routes are created. The first route uses the *virtual-wan-link* zone, and the second route uses the *SASE* zone.

To configure the SD-WAN:

1. Assign port13 and port15 to the *virtual-wan-link* zone and to_FG_B_root to the *SASE* zone:

```

config system sdwan
    set status enable
    config members
        edit 1
            set interface "port13"
            set zone "virtual-wan-link"
            set gateway 10.100.1.1
        next
        edit 2
            set interface "port15"
            set zone "virtual-wan-link"
            set gateway 10.100.1.5
        next
        edit 3
            set interface "to_FG_B_root"
            set zone "SASE"
        next
    end
end

```

2. Create two service rules, one for each SD-WAN zone:

```

config system sdwan
    config service
        edit 1
            set dst "10.100.20.0"

```

```

        set priority-zone "virtual-wan-link"
    next
    edit 2
        set internet-service enable
        set internet-service-name "Fortinet-FortiGuard"
        set priority-zone "SASE"
    next
end
end
end

```

3. Configure static routes for each of the SD-WAN zones:

```

config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
    edit 2
        set dst 172.16.109.0 255.255.255.0
        set distance 1
        set sdwan-zone "SASE"
    next
end
end

```

To verify the results:

1. Check the service rule 1 diagnostics:

```

# diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
    1: Seq_num(1 port13), alive, selected
    2: Seq_num(2 port15), alive, selected
Dst address(1):
    10.100.20.0-10.100.20.255

```

Both members of the *virtual-wan-link* zone are selected. In manual mode, the interface members are selected based on the member configuration order. In SLA and priority mode, the order depends on the link status. If all of the link statuses pass, then the members are selected based on the member configuration order.

2. Check the service rule 2 diagnostics:

```

# diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(1):
    1: Seq_num(3 to_FG_B_root), alive, selected
Internet Service(1): Fortinet-FortiGuard(1245324,0,0,0)

```

The member of the *SASE* zone is selected.

3. Review the routing table:

```

# get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.100.1.1, port13

```



```

[1/0] via 10.100.1.5, port15
S      172.16.109.0/24 [1/0] via 172.16.206.2, to_FG_B_root

```

The default gateway has the members from the *virtual-wan-link* zone, and the route to 172.16.10.9.0/24 has the single member from the *SASE* zone.

Example 2

In this example, two IPv6 static routes are created. The first route uses the *virtual-wan-link* zone, and the second route uses the *SASE* zone.

To configure the SD-WAN:

1. Configure port13 and port15 with IPv6 addresses and assign them to the *virtual-wan-link* zone, and assign to_FG_B_root to the *SASE* zone:

```

config system sdwan
  set status enable
  config members
    edit 1
      set interface "port13"
      set zone "virtual-wan-link"
      set gateway6 2004:10:100:1::1
      set source6 2004:10:100:1::2
    next
    edit 2
      set interface "port15"
      set zone "virtual-wan-link"
      set gateway6 2004:10:100:1::5
      set source6 2004:10:100:1::6
    next
    edit 3
      set interface "to_FG_B_root"
      set zone "SASE"
    next
  end
end

```

2. Configure IPv6 static routes for each of the SD-WAN zones:

```

config router static6
  edit 1
    set distance 1
    set sdwan-zone "virtual-wan-link"
  next
  edit 2
    set dst 2003:172:16:109::/64
    set distance 1
    set sdwan-zone "SASE"
  next
end

```

To verify the results:**1. Review the routing table:**

```
# get router info6 routing-table static
Routing table for VRF=0
S*      ::/0 [1/0] via 2004:10:100:1::1, port13, 00:20:51, [1024/0]
        [1/0] via 2004:10:100:1::5, port15, 00:20:51, [1024/0]
S       2003:172:16:109::/64 [1/0] via ::ac10:ce02, to_FG_B_root, 00:20:51, [1024/0]
S       2003:172:16:209::/64 [5/0] via ::ac10:ce02, to_FG_B_root, 14:40:14, [1024/0]
```

The IPv6 default route includes the members from the *virtual-wan-link* zone, and the route to 2003:172:16:109::/64 has the single member from the *SASE* zone.

Display ADVPN shortcut information in the GUI - 7.0.1

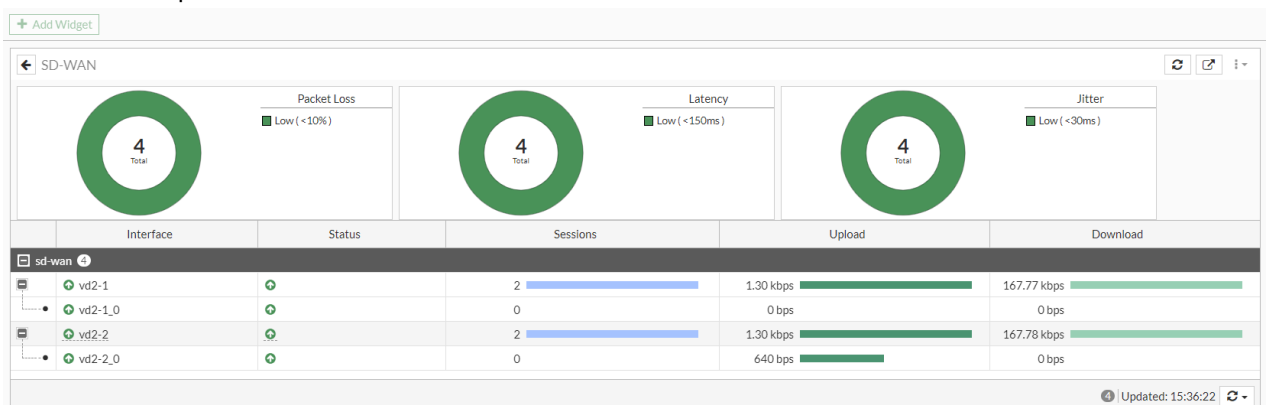
ADVPN shortcut tunnel information is displayed in the *SD-WAN* and *IPsec* dashboard widgets.

The following command has been added to check the dynamic tunnel status:

```
diagnose sys link-monitor interface <name> <name>_0
```

To view the SD-WAN widget:

1. Go to *Dashboard > Network*.
2. Hover over the *SD-WAN* widget and click *Expand to full screen*.
3. Click the + to expand the SD-WAN members and view the child ADVPN shortcuts.



To view the IPsec widget:

1. Go to *Dashboard > Network*.
2. Hover over the *IPsec* widget and click *Expand to full screen*.

+ Add Widget

IPsec

Reset Statistics Bring Up Bring Down Locate on VPN Map

	Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom							
	vd2-1	11.1.1.11		5.29 MB	2.38 MB	vd2-1	vd2-1
	vd2-1_0	13.1.1.3		0 B	0 B	vd2-1_0	vd2-1
	vd2-2	11.1.2.11		5.31 MB	2.45 MB	vd2-2	vd2-2
	vd2-2_0	113.1.1.3		16.39 kB	81.56 kB	vd2-2_0	vd2-2

To verify the dynamic tunnel status:

```
# diagnose sys link-monitor interface vd2-2
Interface(vd2-2): state(up, since Tue Jun 15 12:31:28 2021), bandwidth(up:1299bps,
down:0bps), session count(IPv4:2, IPv6:0), tx(2409919 bytes), rx(5292290 bytes), latency
(0.03), jitter(0.00), packet-loss(0.00).

# diagnose sys link-monitor interface vd2-2 vd2-2_0
Interface(vd2-2_0): state(up, since Tue Jun 15 15:21:52 2021), bandwidth(up:640bps,
down:0bps), session count(IPv4:0, IPv6:0), tx(102242 bytes), rx(16388 bytes), latency(0.03),
jitter(0.00), packet-loss(0.00).
```

Speed tests run from the hub to the spokes in dial-up IPsec tunnels - 7.0.1

In a hub and spoke SD-WAN topology that uses dial-up VPN overlays, QoS can be applied on individual tunnels based on the measured bandwidth between the hub and spokes. The FortiGate can use the built in speed test to dynamically populate the egress bandwidth to individual dial-up tunnels from the hub.

SD-WAN members on a spoke can switch routes when the speed test is running from the hub to the spoke. The speed test results can be cached for reuse when a tunnel comes back after going down.

CLI commands

Allow upload speed tests to be run from the hub to spokes on demand for dial-up IPsec tunnel:

```
config system speed-test-schedule
  edit <interface>
    set dynamic-server {enable | disable}
  next
end
```

<interface>	The dial-up IPsec tunnel interface on the hub.
dynamic-server {enable disable}	Enable/disable the dynamic speed test server (default = disable).



To limit the maximum and minimum bandwidth used in the speed test, enable `set update-inbandwidth` and `set update-outbandwidth`. See [Scheduled interface speedtest](#) for more information.

```
config system global
    set speed-test-server {enable | disable}
end
```

<pre>speed-test-server {enable disable}</pre>	Enable/disable the speed test server on the spoke (default = disable). This setting must be enabled on spoke FortiGates. This enables iPerf in server mode, which listens on the default iPerf TCP port 5201.
---	---

Allow an SD-WAN member on the spoke to switch routes when it is on speed test from the hub to spokes:

```
config system sdwan
    set speedtest-bypass-route {enable | disable}
    config neighbor
        edit <bgp neighbor>
            set mode speedtest
        next
    end
end
```

<pre>speedtest-bypass-route {enable disable}</pre>	Enable/disable bypass routing when doing a speed test on an SD-WAN member (default = disable).
<pre>set mode speedtest</pre>	Use the speed test to select the neighbor.

Manually run uploading speed test on the physical interfaces of each tunnel of an dial-up IPsec interface:

```
execute speed-test-dynamic <interface> <tunnel_name> <'y'/'n'> <max-out> <min-out>
```

<interface>	IPsec phase1 interface name.
<tunnel_name>	The tunnel name, or all for all tunnels.
<'y'/'n'>	Apply the result to the tunnels' shaper or not.
<max-out>	The maximum speed used in a speed test, in kbps.
<min-out>	The minimum speed used in a speed test, in kbps.

Manually run a non-blocking uploading speed test:

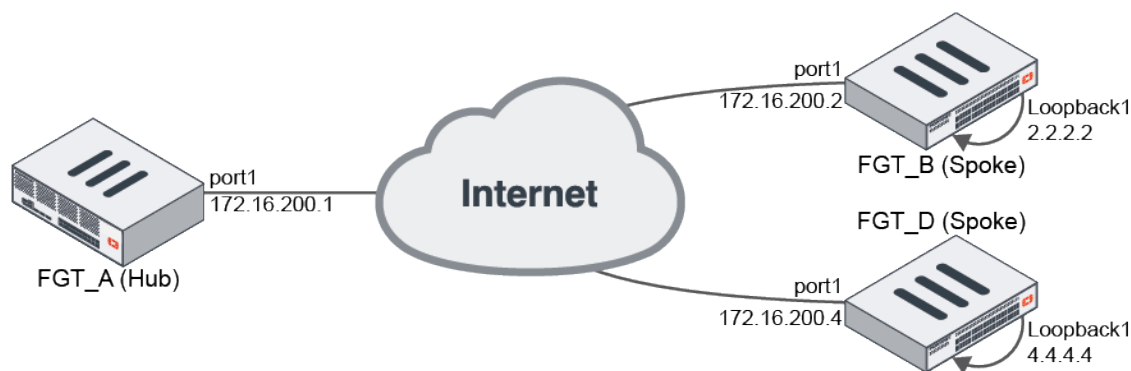
```
diagnose netlink interface speed-test-tunnel <interface> <tunnel_name>
```

Debug and test commands:

<pre>diagnose debug application speedtest <int></pre>	Enable debug of the speed test module in the forticron daemon.
<pre>diagnose debug application speedtestd <int></pre>	Enable debug of the speed test server daemon.
<pre>diagnose test application forticron 9</pre>	List the scheduled speed tests.

diagnose test application forticron 10	Show the cached speed test results.
diagnose test application forticron 11	Write the cached speed test results to disk.
diagnose test application forticron 12	Load the speed test results from disk.
diagnose test application forticron 99	Cancel all pending speed tests.

Example



In this example, the hub is configured as a VPN dial-up server and both of the spokes are connected to the hub. It is assumed that the VPN configuration is already done, with a dynamic gateway type and kernel device creation (`net-device`) disabled. Only one SD-WAN interface is used, so there is only one VPN overlay member in the SD-WAN zone. Multiple WAN interfaces and VPN overlays could be used.

The VPN interfaces and IP addresses are:

FortiGate	Interface	IP Address
FGT_A (Hub)	hub-phase1	10.10.100.254
FGT_B (Spoke)	spoke11-p1	10.10.100.2
FGT_D (Spoke)	spoke21-p1	10.10.100.3

A recurring speed test is configured that runs on the hub over the dial-up interfaces. The speed tests are performed over the underlay interface from the hub to the spoke. Each spoke is configured to operate as a speed test server and to allow the speed test to run on its underlay interface. The spokes establish BGP peering with the hub over the VPN interface, and advertises its loopback network to the hub. The specific configuration is only shown for FGT_B.

When the speed test is running, routing through the VPN overlay can be bypassed, and route maps are used to filter the routes that are advertised to peers. The spoke's route map does not advertise any routes to the peer, forcing the hub to use others paths to reach the spoke's network.

When no speed tests are running, the spoke's route map allows its network to be advertised on the hub.

When the speed test is complete, the measured egress bandwidth is dynamically applied to the VPN tunnel on the hub, and the result is cached for future use, in case the tunnel is disconnected and reconnected again.

To configure the hub FortiGate (FGT_A):**1. Configure a shaping profile:**

```
config firewall shaping-profile
  edit "profile_1"
    config shaping-entries
      edit 1
        set class-id 2
        set priority low
        set guaranteed-bandwidth-percentage 10
        set maximum-bandwidth-percentage 10
      next
    end
    set default-class-id 2
  next
end
```

Three classes are used in the profile for low, medium, and high priority traffic. Each class is assigned a guaranteed and maximum bandwidth as a percentage of the measured bandwidth from the speed test.

2. Use the shaping profile in the interface:

```
config system interface
  edit "hub-phase1"
    set egress-shaping-profile "profile_1"
  next
end
```

3. Configure a schedule to use for the speed tests:

```
config firewall schedule recurring
  edit "speedtest_recurring"
    set start 01:00
    set end 23:00
    set day monday tuesday wednesday thursday friday saturday
  next
end
```

4. Configure the speed test schedule:

```
config system speed-test-schedule
  edit "hub-phase1"
    set schedules "speedtest_recurring"
    set dynamic-server enable
  next
end
```

To configure the spoke FortiGates (FGT_B and FGT_D):**1. Enable the speed test daemon:**

```
config system global
  set speedtest-server enable
end
```

2. Allow speed tests on the interface:

```
config system interface
  edit "port1"
```

```

        append allowaccess speed-test
    next
end

```

3. Configure SD-WAN with bypass routing enabled for speed tests on member *spoke11-p1*:

```

config system sdwan
    set speedtest-bypass-routing enable
    config members
        edit 1
            set interface "spoke11-p1"
        next
    end
    config neighbor
        edit "10.10.100.254"
            set member 1
            set mode speedtest
        next
    end
end

```

4. Configure BGP routing:

```

config router route-map
    edit "No_Speed-Test"
        config rule
            edit 1
                set action permit
            next
        end
    next
    edit "Start_Speed-Test"
        config rule
            edit 1
                set action deny
            next
        end
    next
end

config router bgp
    set as 65412
    config neighbor
        edit "10.10.100.254"
            set remote-as 65412
            set route-map-out "Start_Speed-Test"
            set route-map-out-preferable "No_Speed-Test"
        next
    end
    config network
        edit 1
            set prefix 2.2.2.2 255.255.255.255
        next
        edit 2
            set prefix 10.1.100.0 255.255.255.0
        next
    end
end

```

To manually run the speed test:

```
# execute speed-test-dynamic hub-phase1 all y 1000 100
Start testing the speed of each tunnel of hub-phase1
[6400d9] hub-phase1_0: physical_intf=port1, local_ip=172.16.200.1, server_ip=172.16.200.2
Wait for test 6400d9 to finish...
Speed-test result for test ID 6400d9:
    Completed
    measured upload bandwidth is 1002 kbps
    measured time Sun Jun 20 15:56:34 2021
```

The tested out-bandwidth is more than the set maximum accepted value 1000. Will update the tunnel's shaper by the set update-outbandwidth-maximum.

Apply shaping profile 'profile_1' with bandwidth 1000 to tunnel hub-phase1_0 of interface hub-phase1

```
[6400e0] hub-phase1_1: physical_intf=port1, local_ip=172.16.200.1, server_ip=172.16.200.4
Wait for test 6400e0 to finish...
Speed-test result for test ID 6400e0:
    Completed
    measured upload bandwidth is 1002 kbps
    measured time Sun Jun 20 15:56:39 2021
```

The tested out-bandwidth is more than the set maximum accepted value 1000. Will update the tunnel's shaper by the set update-outbandwidth-maximum.

Apply shaping profile 'profile_1' with bandwidth 1000 to tunnel hub-phase1_1 of interface hub-phase1

```
# diagnose netlink interface speed-test-tunnel hub-phase1 all
send speed test request for tunnel 'hub-phase1_0' of 'hub-phase1': 172.16.200.1 ->
172.16.200.2
send speed test request for tunnel 'hub-phase1_1' of 'hub-phase1': 172.16.200.1 ->
172.16.200.4
```

Results**1. Before the speed test starts, FGT_A can receive the route from FGT_B by BGP:**

```
# get router info routing-table bgp
Routing table for VRF=0
B      2.2.2.2/32 [200/0] via 10.10.100.2 (recursive via 172.16.200.2, hub-phase1),
00:00:10
B      10.1.100.0/24 [200/0] via 10.10.100.2 (recursive via 172.16.200.2, hub-phase1),
00:00:10
```

2. At the scheduled time, the speed test starts for the hub-phase1 interface from hub to spoke:

```
# diagnose test application forticron 9
Speed test schedules:
    Interface      Server      Update      Up/Down-limit (kbps)      Days
H:M      TOS      Schedule
-----
    hub-phase1      dynamic
14:41      0x00      speedtest_recurring      1111111
Active schedules:
    64002f: hub-phase1(port1) 172.16.200.2      hub-phase1_1
    64002e: hub-phase1(port1) 172.16.200.4      hub-phase1_0
```


The diagnose debug application speedtest -1 command can be used on both the hub and spokes to check the speed test execution.

3. While the speed test is running, FGT_A does not receive the route from FGT_B by BGP:

```
# get router info routing-table bgp
Routing table for VRF=0
```

4. Speed tests results can be dynamically applied to the dial-up tunnel for egress traffic shaping:

```
# diagnose vpn tunnel list
-----
name=hub-phase1_0 ver=2 serial=c 172.16.200.1:0->172.16.200.4:0 tun_id=172.16.200.4 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
    bandwidth=737210 (kbps) lock_hit=0 default_class=2 n_active_class=3
    class-id=2 allocated-bandwidth=73720 (kbps) guaranteed-
bandwidth=73720 (kbps)
    max-bandwidth=73720 (kbps) current-bandwidth=0 (kbps)
    priority=low forwarded_bytes=52
    dropped_packets=0 dropped_bytes=0
    class-id=3 allocated-bandwidth=221163 (kbps) guaranteed-
bandwidth=221162 (kbps)
    max-bandwidth=294883 (kbps) current-bandwidth=0 (kbps)
    priority=medium forwarded_bytes=0
    dropped_packets=0 dropped_bytes=0
    class-id=4 allocated-bandwidth=442325 (kbps) guaranteed-
bandwidth=147441 (kbps)
    max-bandwidth=442325 (kbps) current-bandwidth=0 (kbps)
    priority=high forwarded_bytes=0
    dropped_packets=0 dropped_bytes=0
-----
name=hub-phase1_1 ver=2 serial=d 172.16.200.1:0->172.16.200.2:0 tun_id=172.16.200.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
    bandwidth=726813 (kbps) lock_hit=0 default_class=2 n_active_class=3
    class-id=2 allocated-bandwidth=72681 (kbps) guaranteed-
bandwidth=72681 (kbps)
    max-bandwidth=72681 (kbps) current-bandwidth=0 (kbps)
    priority=low forwarded_bytes=123
    dropped_packets=0 dropped_bytes=0
    class-id=3 allocated-bandwidth=218044 (kbps) guaranteed-
bandwidth=218043 (kbps)
    max-bandwidth=290725 (kbps) current-bandwidth=0 (kbps)
    priority=medium forwarded_bytes=0
    dropped_packets=0 dropped_bytes=0
    class-id=4 allocated-bandwidth=436087 (kbps) guaranteed-
bandwidth=145362 (kbps)
    max-bandwidth=436087 (kbps) current-bandwidth=0 (kbps)
    priority=high forwarded_bytes=0
    dropped_packets=0 dropped_bytes=0
```

5. Speed test results can be cached, indexed, and written to disk:

```
# diagnose test application forticron 10
Speed test results:
```

```

1: vdom=root, phaselintf=hub-phase1, peer-id='spoke11-p1', bandwidth=737210, last_
log=1624226603
2: vdom=root, phaselintf=hub-phase1, peer-id='spoke21-p1', bandwidth=726813, last_
log=1624226614

# diagnose test application forticron 11
Write 2 logs to disk.

# diagnose test application forticron 12
load 2 results.

```

Disable then reenable the IPsec VPN tunnel and the cached speed test results can be applied to the tunnel again:

```

# diagnose vpn tunnel list
-----
name=hub-phase1_0 ver=2 serial=c 172.16.200.1:0->172.16.200.4:0 tun_id=172.16.200.4 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
    bandwidth=737210(kbps) lock_hit=0 default_class=2 n_active_class=3
-----
name=hub-phase1_1 ver=2 serial=d 172.16.200.1:0->172.16.200.2:0 tun_id=172.16.200.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
    bandwidth=726813(kbps) lock_hit=0 default_class=2 n_active_class=3

```

Interface based QoS on individual child tunnels based on speed test results - 7.0.1

In a hub and spoke SD-WAN topology that uses dial-up VPN overlays, QoS can be applied on individual tunnels based on the measured bandwidth between the hub and spokes. The FortiGate can use the built in speed test to dynamically populate the egress bandwidth to individual dial-up tunnels from the hub.

A bandwidth limit, derived from the speed test, and a traffic shaping profile can be applied on the dial-up IPsec tunnel interface on the hub. A class ID and percentage based QoS settings can be applied to individual child tunnels using a traffic shaping policy and profile.

CLI commands

If the interface is an IPsec dial-up server, then egress shaping profile type can only be set to `policing`; it cannot be set to `queuing`:

```

config firewall shaping-profile
  edit <profile-name>
    set type policing
  next
end

```

The `outbandwidth` value is dynamically obtained from the speed test results for each individual child tunnel, and should not be set manually:

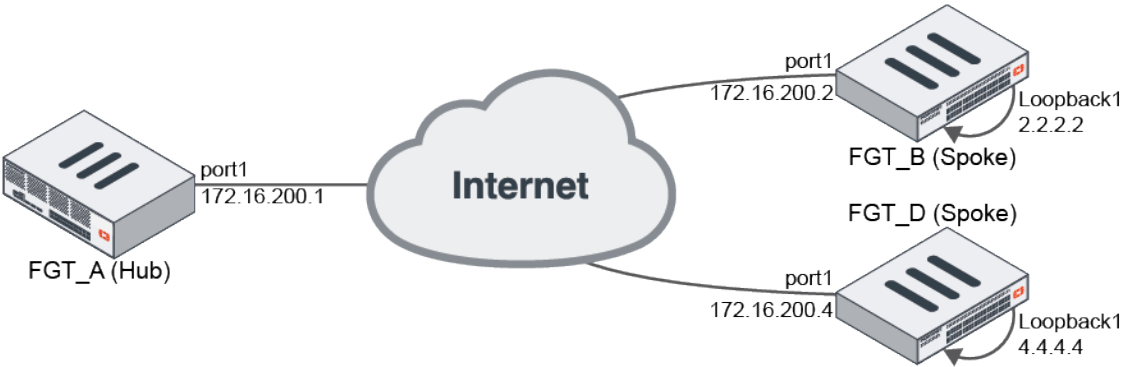
```

config system interface
  edit <dialup-server-phase1-name>
    set egress-shaping-profile <profile-name>
    set outbandwidth <bandwidth>

```

next
end

Example



In this example, the hub is configured as a VPN dial-up server and both of the spokes are connected to the hub. It is assumed that the VPN configuration is already done, with a dynamic gateway type and kernel device creation (`net-device`) disabled. Only one SD-WAN interface is used, so there is only one VPN overlay member in the SD-WAN zone. Multiple WAN interfaces and VPN overlays could be used.

The VPN interfaces and IP addresses are:

FortiGate	Interface	IP Address
FGT_A (Hub)	hub-phase1	10.10.100.254
FGT_B (Spoke)	spoke11-p1	10.10.100.2
FGT_D (Spoke)	spoke21-p1	10.10.100.3

The hub VPN has two child tunnels, one to each spoke.

The speed test configuration is shown in [Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1 on page 133](#). This example shows applying a shaping profile to the hub's tunnel interface in order to apply interface based traffic shaping to the child tunnels.

A traffic shaping policy is used to match and assign traffic to the classes in the shaping profile.

To configure the hub FortiGate (FGT_A) and check the results:

1. Configure the hub FortiGate (FGT_A) as in [Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1 on page 133](#).
2. Configure the shaping profile:

```
config firewall shaping-profile
  edit "profile_1"
    config shaping-entries
      edit 1
        set class-id 2
        set priority low
        set guaranteed-bandwidth-percentage 10
        set maximum-bandwidth-percentage 10
```

```

        next
        edit 2
            set class-id 3
            set priority medium
            set guaranteed-bandwidth-percentage 30
            set maximum-bandwidth-percentage 40
        next
        edit 3
            set class-id 4
            set priority high
            set guaranteed-bandwidth-percentage 20
            set maximum-bandwidth-percentage 60
        next
    end
    set default-class-id 2
next
end

```

3. Configure a traffic shaping policy:

```

config firewall shaping-policy
    edit 2
        set service "ALL"
        set schedule "always"
        set dstintf "hub-phase1"
        set class-id 3
        set srcaddr "all"
        set dstaddr "all"
    next
end

```

In this example, all traffic through the hub-phase1 interface is put into class ID 3. Class IDs can be assigned based on your traffic requirements.

4. At the scheduled time, the speed test will start for the hub-phase1 interface from the hub to the spokes. The speed test results can then be dynamically applied on individual child tunnels as egress traffic shaping, and the class ID percentage based QoS settings is applicable on them as templates.

```

# diagnose vpn tunnel list
-----
name=hub-phase1_0 ver=2 serial=c 172.16.200.1:0->172.16.200.4:0 tun_id=172.16.200.4 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
    bandwidth=737210 (kbps) lock_hit=0 default_class=2 n_active_class=3
    class-id=2 allocated-bandwidth=73720 (kbps) guaranteed-
bandwidth=73720 (kbps)
    max-bandwidth=73720 (kbps) current-bandwidth=0 (kbps)
    priority=low forwarded_bytes=52
    dropped_packets=0 dropped_bytes=0
    class-id=3 allocated-bandwidth=221163 (kbps) guaranteed-
bandwidth=221162 (kbps)
    max-bandwidth=294883 (kbps) current-bandwidth=0 (kbps)
    priority=medium forwarded_bytes=0
    dropped_packets=0 dropped_bytes=0
    class-id=4 allocated-bandwidth=442325 (kbps) guaranteed-
bandwidth=147441 (kbps)

```

```

max-bandwidth=442325 (kbps)      current-bandwidth=0 (kbps)
priority=high    forwarded_bytes=0
dropped_packets=0    dropped_bytes=0
-----
name=hub-phasel_1 ver=2 serial=d 172.16.200.1:0->172.16.200.2:0 tun_id=172.16.200.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
    bandwidth=726813 (kbps) lock_hit=0 default_class=2 n_active_class=3
    class-id=2    allocated-bandwidth=72681 (kbps)    guaranteed-
bandwidth=72681 (kbps)
    max-bandwidth=72681 (kbps)    current-bandwidth=0 (kbps)
    priority=low    forwarded_bytes=123
    dropped_packets=0    dropped_bytes=0
    class-id=3    allocated-bandwidth=218044 (kbps)    guaranteed-
bandwidth=218043 (kbps)
    max-bandwidth=290725 (kbps)    current-bandwidth=0 (kbps)
    priority=medium    forwarded_bytes=0
    dropped_packets=0    dropped_bytes=0
    class-id=4    allocated-bandwidth=436087 (kbps)    guaranteed-
bandwidth=145362 (kbps)
    max-bandwidth=436087 (kbps)    current-bandwidth=0 (kbps)
    priority=high    forwarded_bytes=0
    dropped_packets=0    dropped_bytes=0

```

The guaranteed and maximum bandwidths equal 10% of the speed test result, as expected.

Passive health-check measurement by internet service and application - 7.0.2

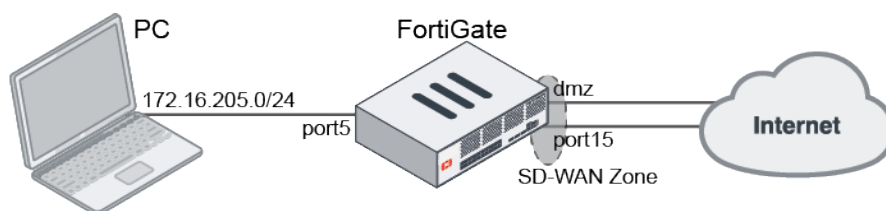
Passive health measurement supports passive detection for each internet service and application.

If internet services or applications are defined in an SD-WAN rule with passive health check, SLA information for each service or application will be differentiated and collected. SLA metrics (latency, jitter, and packet loss) on each SD-WAN member in the rule are then calculated based on the relevant internet service's or application's SLA information.

In this example, three SD-WAN rules are created:

- Rule 1: Best quality (latency) using passive SLA for the internet services Alibaba and Amazon.
- Rule 2: Best quality (latency) using passive SLA for the applications Netflix and YouTube.
- Rule 3: Best quality (latency) using passive SLA for all other traffic.

After passive application measurement is enabled for rules one and two, the SLA metric of rule one is the average latency of the internet services Alibaba and Amazon, and the SLA metric of rule two is the average latency of the applications Netflix and YouTube.



To configure the SD-WAN:**1. Configure the SD-WAN members:**

```

config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "dmz"
            set gateway 172.16.208.2
        next
        edit 2
            set interface "port15"
            set gateway 172.16.209.2
        next
    end
end

```

2. Configure the passive mode health check:

```

config health-check
    edit "Passive_HC"
        set detect-mode passive
        set members 1 2
    next
end

```

3. Configure SD-WAN service rules:

```

config service
    edit 1
        set name "1"
        set mode priority
        set src "172.16.205.0"
        set internet-service enable
        set internet-service-name "Alibaba-Web" "Amazon-Web"
        set health-check "Passive_HC"
        set priority-members 1 2
        set passive-measurement enable //Enable "passive application measurement", it
is a new command which is introduced in this project.
    next
    edit 2
        set name "2"
        set mode priority
        set src "172.16.205.0"
        set internet-service enable
        set internet-service-app-ctrl 18155 31077
        set health-check "Passive_HC"
        set priority-members 1 2
        set passive-measurement enable ////Enable "passive application measurement"
    next
    edit 3
        set name "3"
        set mode priority

```

```

        set dst "all"
        set src "172.16.205.0"
        set health-check "Passive_HC"
        set priority-members 1 2
    next
end

```

4. Configure SD-WAN routes:

```

config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end

```

5. Configure the firewall policy with passive WAN health measurement enabled:

```

config firewall policy
    edit 1
        set uuid 972345c6-1595-51ec-66c5-d705d266f712
        set srcintf "port5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "172.16.205.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "g-default"
        set auto-asic-offload disable
    next
end

```

To verify the results:

1. On the PC, open the browser and visit the internet services and applications.
2. On the FortiGate, check the collected SLA information to confirm that each server or application on the SD-WAN members was measured individually:

```

# diagnose sys link-monitor-passive interface

Interface dmz (5):
    Default(0x00000000): latency=3080.0   11:57:54, jitter=5.0       11:58:08,
    pktloss=0.0 % NA
    Alibaba-Web(0x00690001): latency=30.0   11:30:06, jitter=25.0      11:29:13,
    pktloss=0.0 % NA
    YouTube(0x00007965): latency=100.0   12:00:35, jitter=2.5       12:00:30,
    pktloss=0.0 % NA
    Netflix(0x000046eb): latency=10.0   11:31:24, jitter=10.0      11:30:30,
    pktloss=0.0 % NA
    Amazon-Web(0x00060001): latency=80.0   11:31:52, jitter=35.0      11:32:07,
    pktloss=0.0 % NA

Interface port15 (27):

```

```

    Default(0x00000000): latency=100.0    12:00:42, jitter=0.0    12:00:42,
pktloss=0.0 % NA
    Amazon-Web(0x00060001): latency=30.0    11:56:05, jitter=0.0    11:55:21,
pktloss=0.0 % NA
    Alibaba-Web(0x00690001): latency=0.0    11:26:08, jitter=35.0    11:27:08,
pktloss=0.0 % NA
    YouTube(0x00007965): latency=100.0    11:33:34, jitter=0.0    11:33:50,
pktloss=0.0 % NA
    Netflix(0x000046eb): latency=0.0    11:26:29, jitter=0.0    11:29:03,
pktloss=0.0 % NA

```

3. Verify that the SLA metrics on the members are calculated as expected:

```

# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x600 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor
(latency), link-cost-threshold(10), heath-check(Passive_HC)
  Members(2):
    1: Seq_num(2 port15), alive, latency: 15.000, selected           // Average latency
of "Alibaba-Web" and "Amazon-Web" on port15:    15.000 = (0.0+30.0)/2
    2: Seq_num(1 dmz), alive, latency: 55.000, selected           // Average latency
of "Alibaba-Web" and "Amazon-Web" on dmz:    55.000 = (30.0+80.0)/2
  Internet Service(2): Alibaba-Web(6881281,0,0,0) Amazon-Web(393217,0,0,0)
  Src address(1):
    172.16.205.0-172.16.205.255

Service(2): Address Mode(IPV4) flags=0x600 use-shortcut-sla
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor
(latency), link-cost-threshold(10), heath-check(Passive_HC)
  Members(2):
    1: Seq_num(1 dmz), alive, latency: 55.000, selected           // Average latency
of "Netflix" and "YouTube" on dmz:    55.000 = (10.0+100.0)/2
    2: Seq_num(2 port15), alive, latency: 50.000, selected           // Average latency
of "Netflix" and "YouTube" on port15:    50.000 = (0.0+100.0)/2
  Internet Service(2): Netflix(4294837427,0,0,0 18155) YouTube(4294838283,0,0,0 31077)
  Src address(1):
    172.16.205.0-172.16.205.255

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(9), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor
(latency), link-cost-threshold(10), heath-check(Passive_HC)
  Members(2):
    1: Seq_num(2 port15), alive, latency: 46.000, selected           // Average latency
of all TCP traffic on port15:    46 = (100.0+30.0+0.0+100.0+0.0)/5
    2: Seq_num(1 dmz), alive, latency: 660.000, selected           // Average latency of
all TCP traffic on dmz:    660 = (3080.0+30.0+100.0+10.0+80.0)/5
  Src address(1):
    172.16.205.0-172.16.205.255

  Dst address(1):
    0.0.0.0-255.255.255.255

```


Adaptive Forward Error Correction - 7.0.2

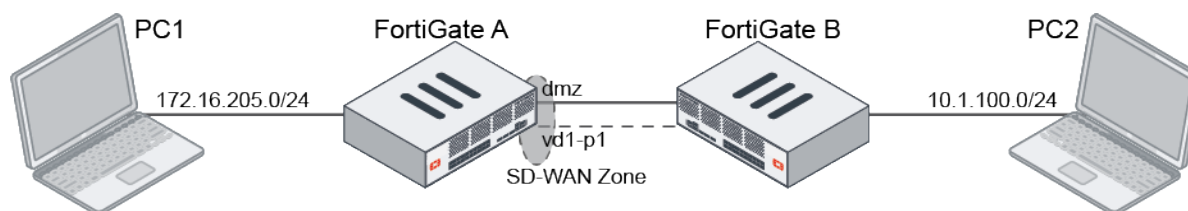
Forward Error Correction (FEC) is used to control and correct errors in data transmission by sending redundant data across the VPN in anticipation of dropped packets occurring during transit. The mechanism sends out x number of redundant packets for every y number of base packets.

Adaptive FEC considers link conditions and dynamically adjusts the FEC packet ratio:

- The FEC base and redundant packet relationship is dynamically adjusted based on changes to the network SLA metrics defined in the SD-WAN SLA health checks. For example, when there is no or low packet loss in the network, FEC can work on a low redundant level sending only one redundant packet for every 10 base packets. As packet loss increases, the number of redundant packets sent can rise accordingly.
- FEC can be applied only to streams that are sensitive to packet loss. For Example, policies that allow the UDP based VoIP protocol can enable FEC, while TCP based traffic policies do not. This reduces unnecessary bandwidth consumption by FEC.
- Because FEC does not support NPU offloading, the ability to specify streams and policies that do not require FEC allows those traffic to be offloaded. This means that all traffic suffers a performance impact.

In this example, an IPsec tunnel is configured between two FortiGates that both have FEC enabled. The tunnel is an SD-WAN zone, and an SLA health-check is used to monitor the quality of the VPN overlay. The intention is to apply FEC to UDP traffic that is passing through the VPN overlay, while allowing all other traffic to pass through without FEC. An FEC profile is configured to adaptively increase redundant levels if the link quality exceeds a 10% packet loss threshold, or the bandwidth exceeds 950 Mbps.

The DMZ interface and IPsec tunnel vd1-p1 are SD-WAN members. FEC is enabled on vd1-p1, and health-check works on vd1-p1.



To configure the FortiGates:

1. On both FortiGates, enable FEC and NPU offloading on the IPsec tunnel vd1-p1:

```
config vpn ipsec phase1-interface
  edit "vd1-p1"
    set npu-offload enable
    set fec-egress enable
    set fec-ingress enable
  next
end
```

2. On FortiGate A, configure SD-WAN:

The VPN overlay member (vd1-p1) must be included in the health-check and configured as the higher priority member in the SD-WAN rule.

```
config system sdwan
  set status enable
```

```
config zone
    edit "virtual-wan-link"
    next
end
config members
    edit 1
        set interface "dmz"
        set gateway 172.16.208.2
    next
    edit 2
        set interface "vdl-p1"
    next
end
config health-check
    edit "1"
        set server "2.2.2.2"
        set members 2
        config sla
            edit 1
            next
        end
    next
end
config service
    edit 1
        set name "1"
        set dst "all"
        set src "172.16.205.0"
        set priority-members 2 1
    next
end
end
```

3. On FortiGate A, create a policy to specify performing FEC on UDP traffic, and a policy for other traffic:

```
config firewall policy
    edit 1
        set srcintf "port5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "172.16.205.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL_UDP"
        set fec enable
    next
    edit 2
        set srcintf "any"
        set dstintf "any"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

4. On FortiGate A, configure FEC mapping to bind network SLA metrics and FEC base and redundant packets:

```
config vpn ipsec fec
  edit "m1"
    config mappings
      edit 1
        set base 8
        set redundant 2
        set packet-loss-threshold 10
      next
      edit 2
        set base 9
        set redundant 3
        set bandwidth-up-threshold 950000
      next
    end
  next
end
```

The mappings are matched from top to bottom: packet loss greater than 10% with eight base and two redundant packets, and then uploading bandwidth greater than 950 Mbps with nine base and three redundant packets.

5. On FortiGate A, apply the FEC mappings on vd1-p1:

```
config vpn ipsec phase1-interface
  edit "vd1-p1"
    set fec-health-check "1"
    set fec-mapping-profile "m1"
    set fec-base 10
    set fec-redundant 1
  next
end
```

The FEC base and redundant values are used when the link quality has not exceeded the limits specified in the FEC profile mapping. If `fec-codec` is set to `xor` the base and redundant packet values will not be updated.

To verify the results:

1. Send TCP and UDP traffic from PC1 to PC2, then check the sessions on FortiGate A:

```
# diagnose sys session list

session info: proto=6 proto_state=01 duration=12 expire=3587 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=112/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=15->102/102->15
gwy=172.16.209.2/172.16.205.11
hook=pre dir=org act=noop 172.16.205.11:39176->10.1.100.22:5001(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.22:5001->172.16.205.11:39176(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=719 auth_info=0 chk_client_info=0 vd=0
serial=00020f7a tos=ff/ff app_list=0 app=0 url_cat=0
```

```

sdwan_mbr_seq=2 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x5000c00
npu info: flag=0x82/0x81, offload=8/8, ips_offload=0/0, epid=249/74, ipid=74/86,
vlan=0x0000/0x0000
vlifid=74/249, vtag_in=0x0000/0x0001 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=5/5

session info: proto=17 proto_state=00 duration=0 expire=180 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty fec
statistic(bytes/packets/allow_err): org=100366/67/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=15->102/102->15 gwy=172.16.209.2/0.0.0.0
hook=pre dir=org act=noop 172.16.205.11:49052->10.1.100.22:5001(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.22:5001->172.16.205.11:49052(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=593 auth_info=0 chk_client_info=0 vd=0
serial=000210fa tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=2 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x5040000
no_ofld_reason: non-npu-intf

```

Non-FEC protected TCP traffic is offloaded, while FEC protected UDP traffic is not offloaded

2. On FortiGate A, check the health-check result and the corresponding FEC base and redundant packets:

```

# diagnose sys sdwan health-check
Health Check(1):
Seq(2 vd1-p1): state(alive), packet-loss(0.000%) latency(0.168), jitter(0.021),
bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x1

```

Because bandwidth-up is more than 950000kbps, base and redundant are set to 9 and 3:

```

# diagnose vpn tunnel fec vd1-p1
egress:
    enabled=1 base=9 redundant=3 codec=0 timeout=10(ms)
    encode=6621 encode_timeout=6621 encode_fail=0
    tx_data=6880 tx_parity=18601
ingress:
    enabled=1 timeout=50(ms)
    fasm_cnt=0 fasm_full=0
    ipsec_fec_chk_fail=0 complete=0
    rx_data=0 rx_parity=0
    recover=0 recover_timeout=0 recover_fail=0
    rx=0 rx_fail=0

```

3. Make packet loss more than 10%, then check the health-check result and the corresponding FEC base and redundant packets again:

```

# diagnose sys sdwan health-check
Health Check(1):
Seq(2 vd1-p1): state(alive), packet-loss(15.000%) latency(0.168), jitter(0.017),
bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x0

```

Because packet loss is more than 10%, entry one in FEC mapping is first matched, and base and redundant are set to 8 and 2:

```
# diagnose vpn tunnel fec vdl-p1
egress:
  enabled=1 base=8 redundant=2 codec=0 timeout=10(ms)
  encode=6670 encode_timeout=6670 encode_fail=0
  tx_data=6976 tx_parity=18748
ingress:
  enabled=1 timeout=50(ms)
  fasm_cnt=0 fasm_full=0
  ipsec_fec_chk_fail=0 complete=0
  rx_data=0 rx_parity=0
  recover=0 recover_timeout=0 recover_fail=0
  rx=0 rx_fail=0
```

General

This section includes information about general network related new features:

- [Summarize source IP usage on the Local Out Routing page on page 151](#)
- [Add option to select source interface and address for Telnet and SSH on page 156](#)
- [ECMP routes for recursive BGP next hop resolution on page 157](#)
- [BGP next hop recursive resolution using other BGP routes on page 158](#)
- [Add SNMP OIDs for shaping-related statistics on page 159](#)
- [PRP handling in NAT mode with virtual wire pair on page 161](#)
- [NetFlow on FortiExtender and tunnel interfaces on page 162](#)
- [Integration with carrier CPE management tools on page 166](#)
- [Use file filter rules in sniffer policy on page 169](#)
- [Explicit mode with DoT and DoH on page 172](#)
- [GUI advanced routing options for BGP on page 176](#)
- [GUI page for OSPF settings on page 178](#)
- [GUI routing monitor for BGP and OSPF on page 180](#)
- [OSPF HMAC-SHA authentication 7.0.1 on page 182](#)
- [BGP conditional advertisement for IPv6 7.0.1 on page 184](#)
- [Enable or disable updating policy routes when link health monitor fails 7.0.1 on page 186](#)
- [Add weight setting on each link health monitor server 7.0.1 on page 189](#)
- [Enhanced hashing for LAG member selection 7.0.1 on page 192](#)
- [Add GPS coordinates to REST API monitor output for FortiExtender and LTE modems 7.0.2 on page 193](#)
- [BGP error handling per RFC 7606 7.0.2 on page 197](#)
- [Configure IPAM locally on the FortiGate 7.0.2 on page 199](#)

Summarize source IP usage on the Local Out Routing page

The *Local Out Routing* page consolidates features where a source IP and an outgoing interface attribute can be configured to route local-out traffic. The outgoing interface has a choice of *Auto*, *SD-WAN*, or *Specify* to allow granular

control over the interface in which to route the local-out traffic. *Local Out Routing* must be enabled from *System > Feature Visibility*, and it supports multi-VDOM mode.

When VDOMs are enabled, the following entries are available in global view on the *Network > Local Out Routing* page.

Enable Service	Edit	Search	Q
Name	Source IP	Outgoing Interface	
External Resource			
AWS_IP_Blacklist	Dynamic	Auto	
AWS_Malware_Hash	Dynamic	Auto	
Log			
Log FortiAnalyzer Setting	Dynamic	Auto	
Log FortiAnalyzer Cloud Setting	Dynamic	Auto	
FortiGate Cloud Log Settings	Dynamic	Auto	
Log Syslogd Setting	Dynamic	Auto	
System			
System DNS	Dynamic	Auto	
System FortiGuard	Dynamic	Auto	
System FortiSandbox	Dynamic	Auto	

When VDOMs are enabled, the following entries are available in VDOM view on the *Network > Local Out Routing* page.

Enable Service	Edit	Search	Q
Name	Source IP	Outgoing Interface	
LDAP Servers			
ldap	Dynamic	Auto	
Log			
Log FortiAnalyzer Override Settings	Dynamic	Auto	
Log Syslogd Override Settings	Dynamic	Auto	
RADIUS Servers			
rac_radius_server	Dynamic	Auto	
TACACS+			
TACACS	Dynamic	Auto	

If a service is disabled, it is grayed out. To enable it, select the service and click *Enable Service*. If a service is enabled, there is a *Local Out Setting* button in the gutter of that service's edit page to directly configure the local-out settings.

A new static REST API shows the existing local-out routing tables.

Examples

To configure DNS local-out routing:

1. Go to *Network > Local Out Routing* and double-click *System DNS*.
2. For *Outgoing interface*, select one of the following:

Auto	Select the outgoing interface automatically based on the routing table.
SD-WAN	Select the outgoing interface using the configured SD-WAN interfaces and rules.
Specify	Select the outgoing interface from the dropdown.

3. If *Specify* is selected, select a setting for *Source IP*:

Use Interface IP	Use the primary IP, which cannot be configured by the user.
Manually	Selected an IP from the list, if the selected interface has multiple IPs configured.

Edit Local Out Setting

Name: LDAP Servers

Outgoing interface: Auto | SD-WAN | Specify

Source IP: Use Interface IP | Manually

10.100.64.101

OK Cancel

Servers
12.12.12.1
[Edit Service]

Documentation
[Online Help] [Video Tutorials]

4. Click **OK**.

To edit local-out settings from a RADIUS server entry:

1. Go to *User & Authentication > RADIUS Servers* and double-click an entry to edit it.
2. Click *Local Out Setting*.

Edit RADIUS Server

Name: fac_radius_server

Authentication method: Default | Specify

NAS IP:

Include in every user group: ☒

Primary Server

IP/Name: 10.100.88.9

Secret: *****

Connection status: ☒ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name:

Secret:

Test Connectivity

Test User Credentials

OK Cancel

FortiGate
admin-fortinet

Additional Information
[API Preview]
[References]
[Edit in CLI]
[Local Out Setting]

Documentation
[Online Help] [Video Tutorials]

The *Edit Local Out Setting* pane opens.

3. Configure the settings for *Outgoing interface* and *Source IP*.

Edit Local Out Setting

Name: fac_radius_server

Outgoing interface: Auto | SD-WAN | Specify

Source IP: Use Interface IP | Manually

OK Cancel

4. Click **OK**.

api/v2/static/local_out_policy_source_metadata.json

```
{
  "system.dns": {
    "path": "system",
    "name": "dns",
    "groupBy": "system",
    "scope": "global",
    "complex": true,
    "dependencies": ["primary", "secondary"],
    "enabledRequired": false
  },
  "system.fortiguard": {
    "path": "system",
    "name": "fortiguard",
    "groupBy": "system",
    "scope": "global",
    "complex": true,
    "dependencies": ["server"],
    "enabledRequired": false
  },
  "system.external-resource": {
    "path": "system",
    "name": "external-resource",
    "groupBy": "external resource",
    "scope": "global",
    "complex": false,
    "dependencies": [],
    "enabledRequired": false
  },
  "system.fortisandbox": {
    "path": "system",
    "name": "fortisandbox",
    "groupBy": "system",
    "scope": "global",
    "complex": true,
    "dependencies": ["server"],
    "enabledRequired": false
  },
  "log.fortianalyzer.setting": {
    "path": "log.fortianalyzer",
    "name": "setting",
    "groupBy": "Log",
    "scope": "global",
    "complex": true,
    "dependencies": ["server"],
    "enabledRequired": false
  },
  "log.fortianalyzer.override-setting": {
    "path": "log.fortianalyzer",
    "name": "override-setting",
    "groupBy": "Log",
    "scope": "vdom",
    "complex": true,
    "dependencies": ["server"],
    "enabledRequired": true
  }
}
```



```
    },
    "log.fortianalyzer-cloud.setting": {
      "path": "log.fortianalyzer-cloud",
      "name": "setting",
      "groupBy": "Log",
      "scope": "global",
      "complex": true,
      "dependencies": ["server"],
      "enabledRequired": false
    },
    "log.fortianalyzer-cloud.override-setting": {
      "path": "log.fortianalyzer-cloud",
      "name": "override-setting",
      "groupBy": "Log",
      "scope": "vdom",
      "complex": true,
      "dependencies": ["server"],
      "enabledRequired": true
    },
    "log.fortiguard.setting": {
      "path": "log.fortiguard",
      "name": "setting",
      "groupBy": "Log",
      "scope": "global",
      "complex": true,
      "dependencies": ["server"],
      "enabledRequired": false
    },
    "log.fortiguard.override-setting": {
      "path": "log.fortiguard",
      "name": "override-setting",
      "groupBy": "Log",
      "scope": "vdom",
      "complex": true,
      "dependencies": ["server"],
      "enabledRequired": true
    },
    "log.syslogd.setting": {
      "path": "log.syslogd",
      "name": "setting",
      "groupBy": "Log",
      "scope": "global",
      "complex": true,
      "dependencies": ["server"],
      "enabledRequired": false
    },
    "log.syslogd.override-setting": {
      "path": "log.syslogd",
      "name": "override-setting",
      "groupBy": "Log",
      "scope": "vdom",
      "complex": true,
      "dependencies": ["server"],
      "enabledRequired": true
    },
    "user.ldap": {
```

```
    "path": "user",
    "name": "ldap",
    "groupBy": "ldap",
    "scope": "vdom",
    "complex": false,
    "dependencies": ["server"],
    "enabledRequired": false
  },
  "user.radius": {
    "path": "user",
    "name": "radius",
    "groupBy": "radius",
    "scope": "vdom",
    "complex": false,
    "dependencies": ["server"],
    "enabledRequired": false
  },
  "user.tacacs+": {
    "path": "user",
    "name": "tacacs+",
    "groupBy": "tacacs",
    "scope": "vdom",
    "complex": false,
    "dependencies": ["server"],
    "enabledRequired": false
  }
}
```

Add option to select source interface and address for Telnet and SSH

The new commands `execute telnet-options` and `execute ssh-options` allow administrators to set the source interface and address for their connection:

```
# execute telnet-options {interface <outgoing interface> | reset | source <source interface IP> | view-settings}

# execute ssh-options {interface <outgoing interface> | reset | source <source interface IP> | view-settings}
```

To edit the Telnet options:

```
# execute telnet-options interface port1
# execute telnet-options source 1.1.1.1
```

To confirm that the Telnet packets are using the configured port and address:

```
# diagnose sniffer packet any "port 23" 4
4.070426 port1 out 1.1.1.1.13938 -> 15.15.15.2.23: syn 400156130
4.070706 port1 in 15.15.15.2.23 -> 1.1.1.1.13938: syn 2889776642 ack 400156131
```

To edit the SSH options:

```
# execute ssh-options interface port1
# execute ssh-options source 1.1.1.1
```

To confirm that the SSH packets are using the configured port and address:

```
# diagnose sniffer packet any "port 22" 4
6.898985 port1 out 1.1.1.1.20625 -> 15.15.15.2.22: syn 1704095779
6.899286 port1 in 15.15.15.2.22 -> 1.1.1.1.20625: syn 753358246 ack 1704095780
```

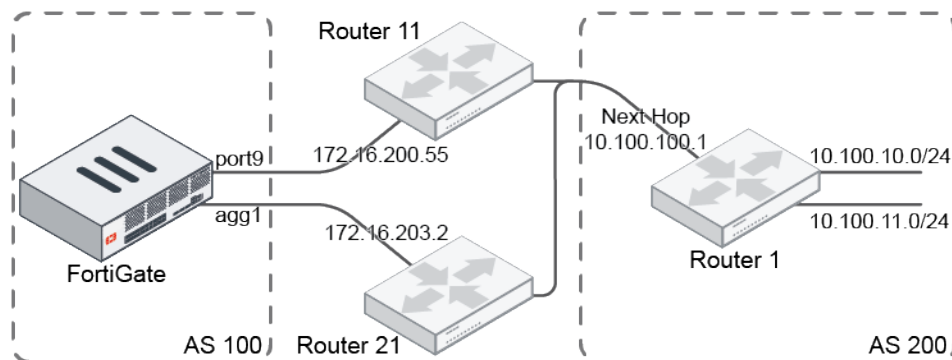
ECMP routes for recursive BGP next hop resolution

When there are multiple ECMP routes to a BGP next hop, all of them are considered for the next hop recursive resolution. This ensures that the outgoing traffic can be load balanced.



To support multipath, either EGBP or IGBP multipath must be enabled:

```
config router bgp
    set ebgp-multipath enable
    set ibgp-multipath enable
end
```



In this example, there are two static routes. The FortiGate has learned two BGP routes from Router 1 that have the same next hop at 10.100.100.1. The next hop is resolved by the two static routes.

To verify that the routes are added to the BGP routing table:

1. Check the two static routes:

```
# get router info routing-table static
Routing table for VRF=0
S    10.100.100.0/24 [10/0] via 172.16.200.55, port9
                                     [10/0] via 172.16.203.2, agg1
```

2. Confirm that both routes are in the BGP routing table:

```
# get router info routing-table bgp
Routing table for VRF=0
B    10.100.10.0/24 [20/200] via 10.100.100.1 (recursive via 172.16.200.55, port9),
00:00:07                                     (recursive via 172.16.203.2, agg1),
00:00:07
B    10.100.11.0/24 [20/200] via 10.100.100.1 (recursive via 172.16.200.55, port9),
00:00:07
```

```
(recursive via 172.16.203.2, agg1),
```

```
00:00:07
```

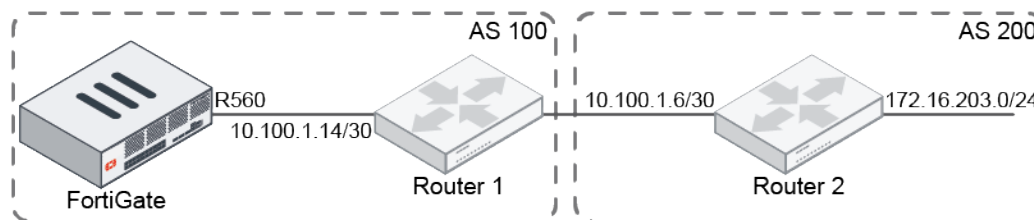
BGP next hop recursive resolution using other BGP routes

By default, BGP routes are not considered when a BGP next hop requires recursive resolution. They are considered when `recursive-next-hop` is enabled.

To consider BGP routes for recursive resolution of next hops:

```
config router bgp
    set recursive-next-hop enable
end
```

Example



To see the change in the routing table when the option is enabled:

1. Check the BGP routing table:

```
# get router info routing-table bgp
Routing table for VRF=0
B      10.100.1.4/30 [200/0] via 10.100.1.14 (recursive is directly connected, R560),
00:02:06
```

2. Enable BGP routes for recursive resolution of next hops:

```
config router bgp
    set recursive-next-hop enable
end
```

3. Check the BGP routing table again:

```
# get router info routing-table bgp
Routing table for VRF=0
B      10.100.1.4/30 [200/0] via 10.100.1.14 (recursive is directly connected, R560),
00:02:15
B      172.16.203.0/24 [200/0] via 10.100.1.6 (recursive via 10.100.1.14, R560),
00:00:06
```

The second BGP route's next hop is now recursively resolved by another BGP route.

Add SNMP OIDs for shaping-related statistics

Four SNMP OIDs have been added for polling the number of packets and bytes that either conform or discard by traffic shaping.

SNMP OID	Description
fgIntfBcQPackets 1.3.6.1.4.1.12356.101.7.5.4.1.1	Packets conform by shaping in the interface, policy, and class.
fgIntfBcQBytes 1.3.6.1.4.1.12356.101.7.5.4.1.2	Bytes conform by shaping in the interface, policy, and class.
fgIntfBcQPDrops 1.3.6.1.4.1.12356.101.7.5.4.1.3	Packets discard by shaping in the interface, policy, and class.
fgIntfBcQBDrops 1.3.6.1.4.1.12356.101.7.5.4.1.4	Bytes discard by shaping in the interface, policy, and class.

To configure an OID related to traffic shaping:

1. Configure SNMP:

```
config system snmp community
  edit 1
    set name "SNMP-TEST"
    config hosts
      edit 1
        set ip 10.1.100.11 255.255.255.255
      next
      edit 2
        set ip 172.16.200.55 255.255.255.255
      next
    end
  config hosts6
    edit 1
      set ipv6 2000:172:16:200::55/128
    next
    edit 2
      set ipv6 2000:10:1:100::11/128
    next
  end
  set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch
  ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented
  fm-if-change fm-conf-change ha-member-up ha-member-down ent-conf-change av-conserve av-
  bypass av-oversize-passed av-oversize-blocked ips-pkg-update faz-disconnect
  next
end
```

2. Configure the traffic shaping profile:

```
config firewall shaping-profile
  edit "eth-shape-hierarchical"
    set comment "output shaper"
    set type queuing
    set default-class 31
```

```
config classes
  edit 31
    set class-id 31
    set priority low
    set maximum-bandwidth-percentage 100
  next
  edit 11
    set class-id 11
    set priority top
    set guaranteed-bandwidth-percentage 50
    set maximum-bandwidth-percentage 50
    set limit 5
  next
  edit 12
    set class-id 12
    set priority critical
    set guaranteed-bandwidth-percentage 20
    set maximum-bandwidth-percentage 100
    set red-probability 10
    set min 5
    set max 10
  next
end
next
end
```

3. Configure the traffic shaping policy:

```
config firewall shaping-policy
  edit 11
    set comment "DIAMOND - 26 - AF31"
    set service "ALL"
    set dstintf "WAN"
    set diffserv-forward enable
    set diffservcode-forward 011010
    set class-id 11
    set srcaddr "HOST_10.71.15.2"
    set dstaddr "HOST_10.72.15.2"
  next
  edit 25
    set comment "GOLD - 20 - AF22"
    set service "ALL"
    set dstintf "WAN"
    set diffserv-forward enable
    set diffservcode-forward 010100
    set class-id 12
    set srcaddr "HOST_10.71.15.3"
    set dstaddr "HOST_10.72.15.3"
  next
end
```

4. Configure the traffic class:

```
config firewall traffic-class
  edit 11
    set class-name "a"
  next
```

```

edit 12
    set class-name "b"
next
edit 13
    set class-name "c"
next
edit 14
    set class-name "d"
next
end

```

5. Configure the interface:

```

config system interface
    edit "wan1"
        set vdom "root"
        set ip 172.16.200.1 255.255.255.0
        set allowaccess ping
        set type physical
        set outbandwidth 1024
        set egress-shaping-profile "eth-shape-hierarchical"
        set role lan
        set snmp-index 1
    next
end

```

Sample query

```

$ snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.7.5.4.1.1
FORTINET-FORTIGATE-MIB::fgIntfBcQPackets.1.12 = Counter64: 11992
FORTINET-FORTIGATE-MIB::fgIntfBcQPackets.1.13 = Counter64: 2015
FORTINET-FORTIGATE-MIB::fgIntfBcQPackets.1.14 = Counter64: 2014
FORTINET-FORTIGATE-MIB::fgIntfBcQPackets.1.15 = Counter64: 1062

$ snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.7.5.4.1.2
FORTINET-FORTIGATE-MIB::fgIntfBcQBytes.1.12 = Counter64: 3021984
FORTINET-FORTIGATE-MIB::fgIntfBcQBytes.1.13 = Counter64: 507780
FORTINET-FORTIGATE-MIB::fgIntfBcQBytes.1.14 = Counter64: 507528
FORTINET-FORTIGATE-MIB::fgIntfBcQBytes.1.15 = Counter64: 266272

$ snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.7.5.4.1.3
FORTINET-FORTIGATE-MIB::fgIntfBcQPDrops.1.12 = Counter64: 15211
FORTINET-FORTIGATE-MIB::fgIntfBcQPDrops.1.13 = Counter64: 0
FORTINET-FORTIGATE-MIB::fgIntfBcQPDrops.1.14 = Counter64: 0
FORTINET-FORTIGATE-MIB::fgIntfBcQPDrops.1.15 = Counter64: 15267

$ snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.7.5.4.1.4
FORTINET-FORTIGATE-MIB::fgIntfBcQBDrops.1.12 = Counter64: 3833172
FORTINET-FORTIGATE-MIB::fgIntfBcQBDrops.1.13 = Counter64: 0
FORTINET-FORTIGATE-MIB::fgIntfBcQBDrops.1.14 = Counter64: 0
FORTINET-FORTIGATE-MIB::fgIntfBcQBDrops.1.15 = Counter64: 3816750

```

PRP handling in NAT mode with virtual wire pair

PRP (Parallel Redundancy Protocol) is supported in NAT mode for a virtual wire pair. This preserves the PRP RCT (redundancy control trailer) while the packet is processed by the FortiGate.

To configure PRP handling on a device in NAT mode:**1. Enable PRP in the VDOM settings:**

```
(root) # config system settings
      set prp-trailer-action enable
end
```

2. Enable PRP in the NPU attributes:

```
(global) # config system npu
      set prp-port-in "port15"
      set prp-port-out "port16"
end
```

3. Configure the virtual wire pair:

```
(root) # config system virtual-wire-pair
      edit "test-vwp-1"
        set member "port15" "port16"
      next
end
```

NetFlow on FortiExtender and tunnel interfaces

NetFlow sampling is supported on FortiExtender and VPN tunnel interfaces.

VPN tunnel interfaces can be IPsec, IP in IP, or GRE tunnels. NetFlow sampling is supported on both NPU and non-NPU offloaded tunnels.

To configure NetFlow sampling on an interface:

```
config system interface
  edit <interface>
    set netflow-sampler {disable | tx | rx | both}
  next
end
```

disable	Disable NetFlow protocol on this interface.
tx	Monitor transmitted traffic on this interface.
rx	Monitor received traffic on this interface.
both	Monitor transmitted and received traffic on this interface.

Examples

In the following examples, a FortiExtender and a VPN tunnel interface are configured with NetFlow sampling.

To configure a FortiExtender interface with NetFlow sampling:

1. Configure a FortiExtender interface with NetFlow sampling enabled for both transmitted and received traffic:

```
config system interface
    edit "fext-211"
        set vdom "root"
        set mode dhcp
        set type fext-wan
        set netflow-sampler both
        set role wan
        set snmp-index 8
        set macaddr 2a:4e:68:a3:f4:6a
    next
end
```

2. Check the NetFlow status and configuration:

Device index 26 is the FortiExtender interface fext-211.

```
# diagnose test application sflowd 3
===== Netflow Vdom Configuration =====
Global collector:172.18.60.80:[2055] source ip: 0.0.0.0 active-timeout(seconds):60
inactive-timeout(seconds):600
_____ vdom: root, index=0, is master, collector: disabled (use global config) (mgmt vdom)
|_ coll_ip:172.18.60.80[2055],src_ip:10.6.30.105,seq_num:300,pkts/time to next
template: 18/29
|_ exported: Bytes:3026268, Packets:11192, Sessions:290 Flows:482
|_____ interface:fext-211 sample_direction:both device_index:26 snmp_index:8
```

3. Check the network interface list:

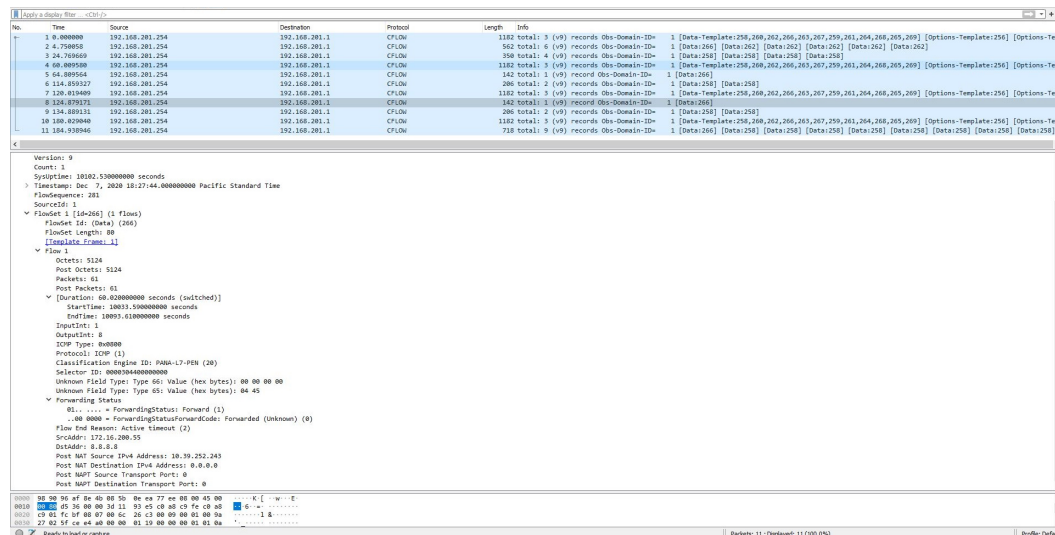
```
# diagnose netlink interface list
...
if=fext-211 family=00 type=1 index=26 mtu=1500 link=0 master=0
ref=27 state=start present fw_flags=60000 flags=up broadcast run multicast
...
```

4. Check the session list for the FortiExtender interface and NetFlow flowset packet:

```
# diagnose sys session list
session info: proto=1 proto_state=00 duration=1732 expire=59 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty netflow-origin netflow-reply
statistic(bytes/packets/allow_err): org=145572/1733/1 reply=145572/1733/1 tuples=2
tx speed(Bps/kbps): 83/0 rx speed(Bps/kbps): 83/0
orgin->sink: org pre->post, reply pre->post dev=5->26/26->5
gwy=10.39.252.244/172.16.200.55
hook=post dir=org act=snat 172.16.200.55:61290->8.8.8.8:8(10.39.252.243:61290)
hook=pre dir=reply act=dnat 8.8.8.8:61290->10.39.252.243:0(172.16.200.55:61290)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00001298 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

```
no_ofld_reason: non-npu-intf
total session 1
```

5. The flowset packet can be captured on UDP port 2055 by a packet analyzer, such as Wireshark:



To configure a VPN tunnel interface with NetFlow sampling:

1. Configure a VPN interface with NetFlow sampling enabled for both transmitted and received traffic:

```
config system interface
    edit "A-to-B_vpn"
        set vdom "vdom1"
        set type tunnel
        set netflow-sampler both
        set snmp-index 42
        set interface "port3"
    next
end
```

2. Configure the VPN tunnel:

```
config vpn ipsec phase1-interface
    edit "A-to-B_vpn"
        set interface "port3"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: A-to-B_vpn [Created by VPN wizard]"
        set wizard-type static-fortigate
        set remote-gw 10.2.2.2
        set psksecret ENC
    next
end

config vpn ipsec phase2-interface
    edit "A-to-B_vpn"
        set phase1name "A-to-B_vpn"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
        aes256gcm chacha20poly1305
```

```

        set comments "VPN: A-to-B_vpn [Created by VPN wizard]"
        set src-addr-type name
        set dst-addr-type name
        set src-name "A-to-B_vpn_local"
        set dst-name "A-to-B_vpn_remote"
    next
end

```

3. Check the NetFlow status and configuration:

Device index 52 is the VPN interface A-to-B_vpn.

```

# diagnose test application sflowd 3
===== Netflow Vdom Configuration =====
Global collector:172.18.60.80:[2055] source ip: 0.0.0.0 active-timeout(seconds):60
inactive-timeout(seconds):15
_____ vdom: vdom1, index=1, is master, collector: disabled (use global config) (mgmt
vdom)
|_ coll_ip:172.18.60.80[2055],src_ip:10.1.100.1,seq_num:60,pkts/time to next
template: 15/6
|_ exported: Bytes:11795591, Packets:48160, Sessions:10 Flows:34
|_____ interface:A-to-B_vpn sample_direction:both device_index:52 snmp_index:42

```

4. Check the session list for the VPN interface and NetFlow flowset packet (unencapsulated traffic going through the VPN tunnel):

```

# diagnose sys session list
session info: proto=6 proto_state=01 duration=6 expire=3599 timeout=3600 flags=00000000
socketype=0 socketport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu netflow-origin netflow-reply
statistic(bytes/packets/allow_err): org=6433/120/1 reply=884384/713/1 tuples=2
tx speed(Bps/kbps): 992/7 rx speed(Bps/kbps): 136479/1091
origin->sink: org pre->post, reply pre->post dev=10->52/52->10 gwy=10.2.2.2/10.1.100.22
hook=pre dir=org act=noop 10.1.100.22:43714->172.16.200.55:80(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.200.55:80->10.1.100.22:43714(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:0c:29:ac:ae:4f
misc=0 policy_id=5 auth_info=0 chk_client_info=0 vd=1
serial=00003b6c tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000001 no_offload
npu info: flag=0x82/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason: disabled-by-policy
total session 1

```

5. The flowset packet can be captured on UDP port 2055 by a packet analyzer, such as Wireshark:

The screenshot displays a network traffic analysis interface. The top section shows a list of flows with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom section provides a detailed view of a selected flow, including packet details, flow statistics, and flow reason.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data-Template:258,268,262,266,263,267,259,261,264,266,265,269] [Options-Template:256] [Options-Template:256]
2	0.334599	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
3	0.334600	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
4	0.338395	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
5	0.344179	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
6	0.400346	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
7	0.342007	192.168.201.254	192.168.201.1	CFLN	206	total: 2 (v9) records Obs-Domain-ID= 2 [Data:258] [Data:258]
8	0.342040	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
9	0.346650	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
10	0.346154	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
11	0.347569	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
12	0.400774	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) records Obs-Domain-ID= 2 [Data-Template:258,268,262,266,263,267,259,261,264,266,265,269] [Options-Template:256] [Options-Template:256]
13	0.347575	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
14	0.349056	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
15	0.350907	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
16	0.352722	192.168.201.254	192.168.201.1	CFLN	206	total: 2 (v9) records Obs-Domain-ID= 2 [Data:258] [Data:258]
17	0.352720	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]
18	0.411104	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) records Obs-Domain-ID= 2 [Data-Template:258,268,262,266,263,267,259,261,264,266,265,269] [Options-Template:256] [Options-Template:256]
19	0.356884	192.168.201.254	192.168.201.1	CFLN	182	total: 1 (v9) record Obs-Domain-ID= 2 [Data:256]

Flow Details:

- Octets: 53077
- Post Octets: 53077
- Packets: 993
- Post Packets: 993
- Duration: 00.010000000 seconds (switched)
- SrcPort: 43214
- DstPort: 80
- OutputInt: 42
- Protocol: TCP (6)
- Port To Self Serv Code Point: 255
- Classification Engine ID: PABA-L7-PEN (20)
- Selector ID: 0000000000000000
- Unknown Field Type: Type 66: Value (hex bytes): 00 00 00 00
- Unknown Field Type: Type 65: Value (hex bytes): 0c 15
- Forwarding Status: 01: = ForwardingStatus: Forward (1)
- Flow End Reason: Active timeout (2)
- SrcAddr: 192.168.201.254
- DstAddr: 192.168.201.1
- Padding: 00

Count of packets in flow (flow-packets), 4bytes

Packets: 19 - Deployed: 19 (100.0%) - Dropped: 0 (0.0%)

Profile: Default

Integration with carrier CPE management tools

The following enhancements allow better integration with carrier CPE (customer premises equipment) management tools:

- Add SNMP OIDs to collect the reason for a FortiGate reboot.
- Add SNMP OIDs to collect traffic shaping profile and policy related configurations.
- Add a description field on the modem interface that can be fetched over SNMP.
- Bring a loopback or VLAN interface down when the link monitor fails.
- Add DSCP and shaping class ID support on the link monitor probe.
- Allow multiple link monitors with the same source and destination address, but different ports or protocols.

SNMP OIDs

Use the following SNMP OIDs to collect the reason for a FortiGate reboot:

- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgSystem.fgSystemInfo.fgSysUpTimeDetail
1.3.6.1.4.1.12356.101.4.1.22
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgSystem.fgSystemInfo.fgSysRebootReason
1.3.6.1.4.1.12356.101.4.1.23

Use the following SNMP OIDs to collect traffic shaping profile and policy related configurations:

SNMP OID	Comments	Related FOS configuration
fgIntfBcCfgIfTable 1.3.6.1.4.1.12356.101.7.5.5.1	The OID index is interface's SNMP index.	The SNMP result matches config system interface with the ingress/egress shaping profile set.

SNMP OID	Comments	Related FOS configuration
fgIntfCfgSproTable 1.3.6.1.4.1.12356.101.7.5.5.2	The OID index has format: .<vdom_index>.<profile_index>.	The SNMP result matches the main configuration of config firewall shaping-profile.
fgIntfBcCfgSentTable 1.3.6.1.4.1.12356.101.7.5.5.3	The OID index has format: .<vdom_index>.<profile_index>.<class_id>.	The SNMP result matches config firewall shaping-profile > config shaping-entries.
fgIntfBcCfgSpolTable 1.3.6.1.4.1.12356.101.7.5.5.4	The OID index has format: .<vdom_index>.<policy_id>.	The SNMP result is matches config firewall shaping-policy.

CLI updates

To add a description on a modem interface:

1. Configure the interface:

```
config system interface
  edit "modem"
    set vdom "root"
    set mode pppoe
    set type physical
    set description "this the is modem"
    set snmp-index 37
  next
end
```

2. Run the SNMP walk in a third-party console:

```
ubuntu90:~$ snmpwalk -v2c -cpublic 172.18.18.160 1.3.6.1.2.1 | grep odem
iso.3.6.1.2.1.2.2.1.2.37 = STRING: "this is the modem"
iso.3.6.1.2.1.31.1.1.1.1.37 = STRING: "modem"
iso.3.6.1.2.1.47.1.1.1.1.7.4 = STRING: "modem"
```

To bring a loopback or VLAN interface down when the link monitor fails:

1. Configure the interfaces:

```
config system interface
  edit "loopback1"
    set vdom "root"
    set ip 1.2.3.4 255.255.255.255
    set type loopback
  next
  edit "port1"
    set fail-detect enable
    set fail-detect-option detectserver link-down
    set fail-alert-interfaces loopback1
```

```

    next
end

```

2. Configure the link monitor:

```

config system link-monitor
    edit linkmon1
        set server 159.1.1.1
        set interface "port1"
        set gateway-ip 28.1.1.159
        set source-ip 28.1.1.160
    next
end

```

To configure DSCP and a shaping class ID on a link monitor:

```

config system link-monitor
    edit "monitor1"
        set srcintf "port1"
        set server "8.8.8.8"
        set gateway-ip 172.16.200.254
        set source-ip 172.16.200.1
        set diffservcode <binary>
        set class-id <id>
        set service-detection {enable | disable}
    next
end

```

<code>diffservcode <binary></code>	Enter the differentiated services code point (DSCP) in the IP header of the probe packet, 6 bits binary (000000 - 111111) .
<code>class-id <id></code>	Enter the class ID (taken from <code>config firewall traffic-class</code>).
<code>service-detection {enable disable}</code>	Set the service detection: <ul style="list-style-type: none"> enable: only use monitor for service-detection disable: monitor will update routes/interfaces on link failure

If the traffic generated by the probe matches the configured shaping traffic class, it will honor the priority, guaranteed bandwidth percentage, and maximum bandwidth percentage of the queue.

To configure multiple link monitors with the same source and destination address:

```

config system link-monitor
    edit "monitor1"
        set srcintf "port1"
        set server "159.1.1.1"
        set protocol twamp
        set port 81
        set gateway-ip 28.1.1.159
        set source-ip 28.1.1.160
    next
    edit "monitor2"
        set srcintf "port1"
        set server "159.1.1.1"
        set protocol twamp
        set port 82

```

```

set gateway-ip 28.1.1.159
set source-ip 28.1.1.160
set service-detection enable
next
end

```

In this example, different ports are used in each link monitor.

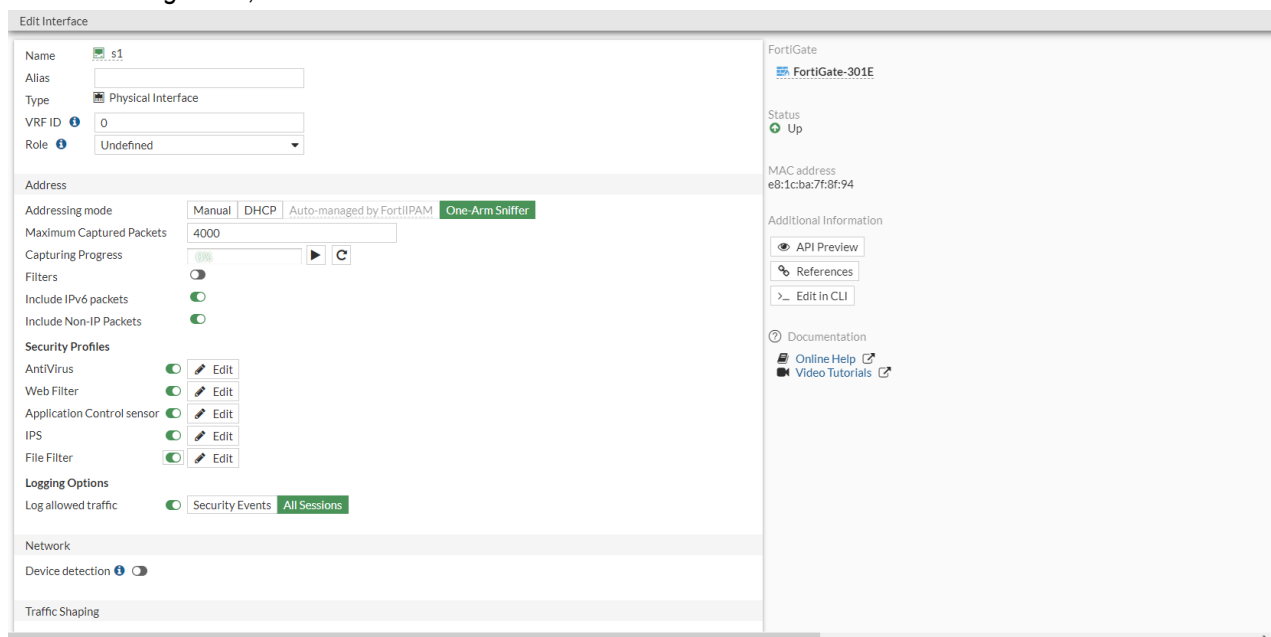
Use file filter rules in sniffer policy

File filter rules can be used in one-arm sniffer policies in the GUI and CLI.

The following example shows how to configure a file filter profile that blocks PDF and RAR files used in a one-arm sniffer policy.

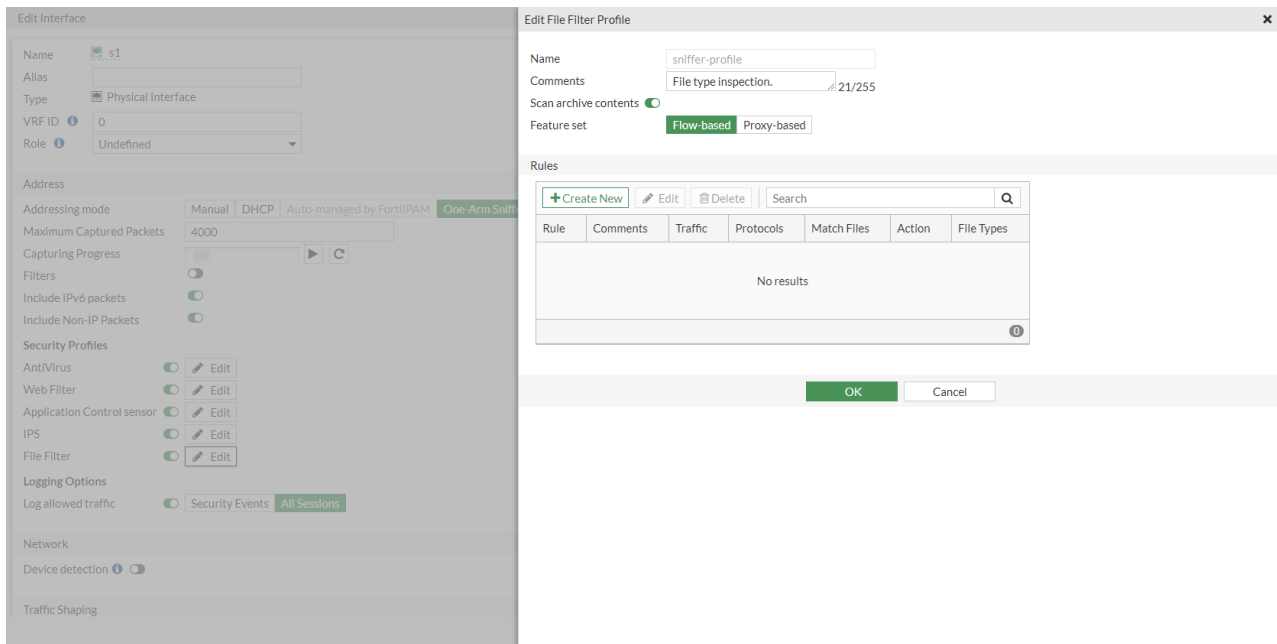
To configure a one-arm sniffer policy in the GUI:

1. Go to **Network > Interfaces** and double-click a physical interface to edit it.
2. For **Role**, select either **LAN**, **DMZ**, or **Undefined**.
3. For **Addressing Mode**, select **One-Arm Sniffer**.

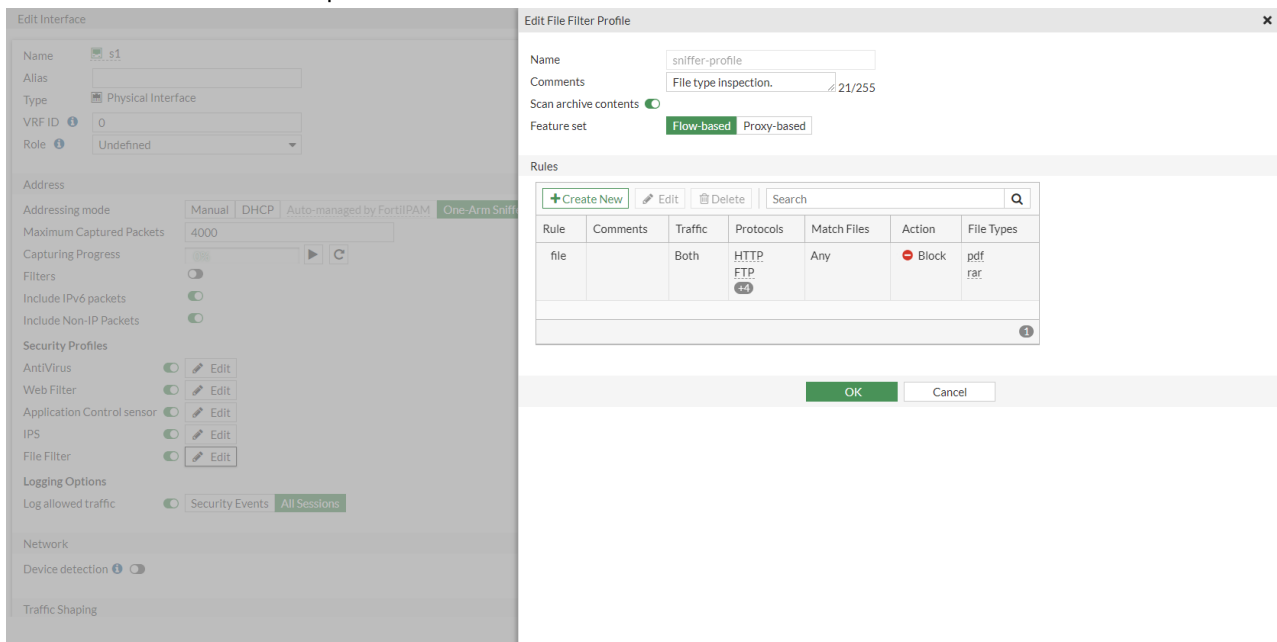


4. In the **Security Profiles** section, enable **File Filter** and click **Edit**. The **Edit File Filter Profile** pane opens.

5. In the *Rules* table, click *Create New*.



6. Configure the rule:
 - a. For *File types*, click the + and select *pdf* and *rar*.
 - b. For *Action*, select *Block*.
 - c. Click *OK* to save the rule.
7. Click *OK* to save the file filter profile.



8. Click *OK* to save the interface settings.

9. Go to *Log & Report > File Filter* to view the logs.

Add Filter								
Date/Time	Service	Action	URL	File Name	Matched file name	File Type	Matched file type	Filter Name
9 minutes ago	FTP	passthrough		hello2.pdf		pdf		file
10 minutes ago	FTP	passthrough		test.rar		rar		file

To configure a one-arm sniffer policy in the CLI:

1. Configure the interface:

```
config system interface
    edit "s1"
        set vdom "root"
        set ips-sniffer-mode enable
        set type physical
        set role undefined
        set snmp-index 31
    next
end
```

2. Configure the file filter profile:

```
config file-filter profile
    edit "sniffer-profile"
        set comment "File type inspection."
        config rules
            edit "1"
                set protocol http ftp smtp imap pop3 cifs
                set action block
                set file-type "pdf" "rar"
            next
        end
    next
end
```

3. Configure the firewall sniffer policy:

```
config firewall sniffer
    edit 1
        set interface "s1"
        set file-filter-profile-status enable
        set file-filter-profile "sniffer-profile"
    next
end
```

4. View the log:

```
# execute log filter category 19
# execute log display
1 logs found.
1 logs returned.

1: date=2020-12-29 time=09:14:46 eventtime=1609262086871379250 tz="-0800"
logid="1900064000" type="utm" subtype="file-filter" eventtype="file-filter"
level="warning" vd="root" policyid=1 sessionid=792 srcip=172.16.200.55 srcport=20
srcintf="s1" srcintfrole="undefined" dstip=10.1.100.11 dstport=56745 dstintf="s1"
dstintfrole="undefined" proto=6 service="FTP" profile="sniffer-profile"
```

```
direction="outgoing" action="blocked" filtername="1" filename="hello.pdf" filesize=9539
filetype="pdf" msg="File was blocked by file filter."
```

Explicit mode with DoT and DoH

DNS over TLS (DoT) and DNS over HTTPS (DoH) are supported in explicit mode where the FortiGate acts as an explicit DNS server that listens for DoT and DoH requests. Local-out DNS traffic over TLS and HTTPS is also supported.

Basic configurations for enabling DoT and DoH for local-out DNS queries

To enable DoT and DoH DNS in the GUI:

1. Go to *Network > DNS*.
2. Enter the primary and secondary DNS server addresses.
3. In the *DNS Protocols* section, enable *TLS (TCP/853)* and *HTTPS (TCP/443)*.

4. Configure the other settings as needed.
5. Click *Apply*.

To enable DoT and DoH DNS in the CLI:

```
config system dns
    set primary 1.1.1.1
    set secondary 1.0.0.1
    set protocol {cleartext dot doh}
end
```

To enable DoH on the DNS server in the GUI:

1. Go to *Network > DNS Servers*.
2. In the *DNS Service on Interface* section, edit an existing interface, or create a new one.
3. Select a *Mode*, and *DNS Filter* profile.

4. Enable *DNS over HTTPS*.

Edit DNS Service

Interface

port1

Mode

Recursive

Non-Recursive

Forward to System DNS

DNS Filter

☒ DNS

dnsfilter

DNS over HTTPS
☒

OK

Cancel

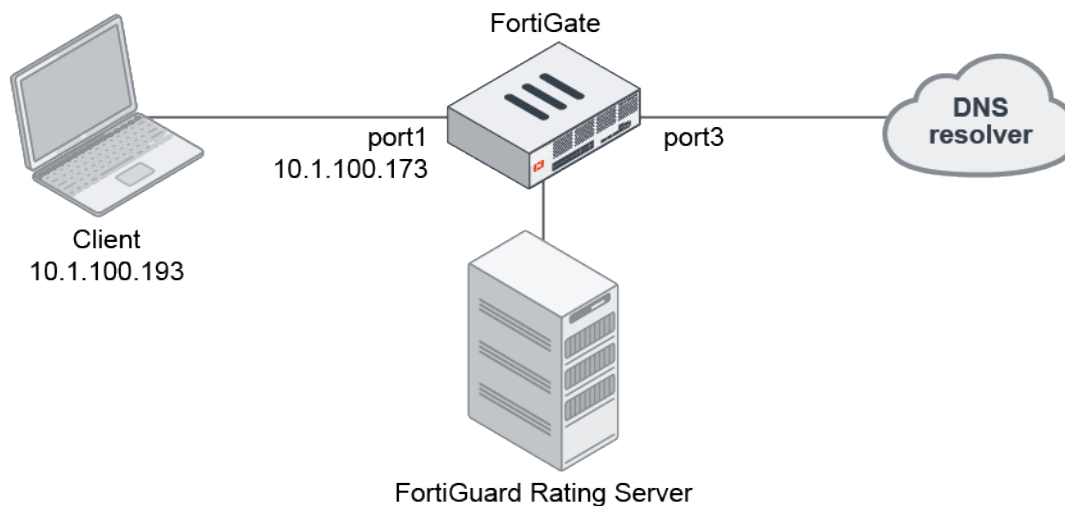
5. Click *OK*.

To enable DoH on the DNS server in the CLI:

```
config system dns-server
  edit "port1"
    set dnsfilter-profile "dnsfilter"
    set doh enable
  next
end
```

Examples

The following examples demonstrate how configure DNS settings to support DoT and DoH queries made to the FortiGate.



DoT

The following example uses a DNS filter profile where the education category is blocked.

To enable scanning DoT traffic in explicit mode with a DNS filter:

1. Configure the DNS settings:

```
config system dns
  set primary 1.1.1.1
```

```

        set secondary 1.0.0.1
    set protocol dot
end

```

2. Configure the DNS filter profile:

```

config dnsfilter profile
    edit "dnsfilter"
        config ftgd-dns
            config filters
                edit 1
                    set category 30
                    set action block
                next
            end
        end
    next
end

```

3. Configure the DNS server settings:

```

config system dns-server
    edit "port1"
        set dnsfilter-profile "dnsfilter"
    next
end

```

4. Send a DNS query over TLS (this example uses kdig on an Ubuntu client) using the FortiGate as the DNS server. The **www.ubc.ca** domain belongs to the education category:

```

root@client:/tmp# kdig -d @10.1.100.173 +tls +header +all www.ubc.ca
;; DEBUG: Querying for owner(www.ubc.ca.), class(1), type(1), server(10.1.100.173), port
(853), protocol(TCP)
;; DEBUG: TLS, received certificate hierarchy:
;; DEBUG: #1,
C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=FortiGate,CN=FG3H1E5818903681,EMAIL=support
@fortinet.com
;; DEBUG:      SHA-256 PIN: XhkpV9ABEhxDLtWG+lGEndNrBR7BlxjRYlGn2ltlkb8=
;; DEBUG: #2, C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate
Authority,CN=fortinet-subca2001,EMAIL=support@fortinet.com
;; DEBUG:      SHA-256 PIN: 3T8EqFBjpRSkxQNPfagjUNeEUghXOEYp904ROlJM8yo=
;; DEBUG: #3, C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate
Authority,CN=fortinet-ca2,EMAIL=support@fortinet.com
;; DEBUG:      SHA-256 PIN: /QfV4N3k5oxQR5RHtW/rbn/HrHgKpMLN0DEaeXY5yPg=
;; DEBUG: TLS, skipping certificate PIN check
;; DEBUG: TLS, skipping certificate verification
;; TLS session (TLS1.2)-(ECDHE-RSA-SECP256R1)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 56719
;; Flags: qr rd; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.ubc.ca.                IN      A

;; ANSWER SECTION:
www.ubc.ca.                60     IN     A       208.91.112.55

;; Received 44 B
;; Time 2021-03-12 23:11:27 PST

```

```
;; From 10.1.100.173@853(TCP) in 0.2 ms
root@client:/tmp#
```

The IP returned by the FortiGate for ubc.ca belongs to the FortiGuard block page, so the query was blocked successfully.

DoH

The following example uses a DNS filter profile where the education category is blocked.

To configure scanning DoH traffic in explicit mode with a DNS filter:

1. Configure the DNS settings:

```
config system dns
    set primary 1.1.1.1
    set secondary 1.0.0.1
    set protocol doh
end
```

2. Configure the DNS filter profile:

```
config dnsfilter profile
    edit "dnsfilter"
        config ftgd-dns
            config filters
                edit 1
                    set category 30
                    set action block
                next
            end
        end
    next
end
```

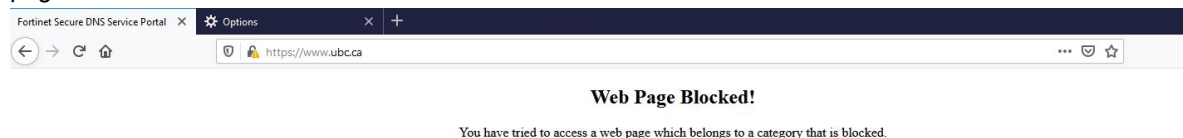
3. Configure the DNS server settings:

```
config system dns-server
    edit "port1"
        set dnsfilter-profile "dnsfilter"
        set doh enable
    next
end
```

4. In your browser, enable DNS over HTTPS.

5. On your computer, edit the TCP/IP settings to use the FortiGate interface address as the DNS server.

6. In your browser, go to a website in the education category (www.ubc.ca). The website is redirected to the block page.



GUI advanced routing options for BGP

Users can configure advanced BGP routing options on the *Network > BGP* page. The *BGP > Routing Objects* page allows users to create new *Route Map*, *Access List*, *Prefix List*, *AS Path List*, and *Community List*.

BGP page enhancements

The *Password*, *Interface*, *Update source*, *Graceful restart time*, *Activate IPv4/IPv6*, and *IPv4/IPv6 Filtering* options are available when creating a new neighbor.

The 'Add Neighbor' dialog box displays the following configuration options:

- IP:
- Remote AS:
- Password: Change
- Interface: ☐
- Update source: ☐
- Graceful restart time:
- Activate IPv4: ☒
- Activate IPv6: ☒
- IPv4 Filtering section:
 - Filter list in: ☐
 - Filter list out: ☐
 - Distribute list in: ☐
 - Distribute list out: ☐
 - Prefix list in: ☐
 - Prefix list out: ☐

Buttons: OK Cancel

The 'Add Neighbor' dialog box displays the following advanced configuration options:

- IPv4 Filtering section:
 - Filter list in: ☐
 - Filter list out: ☐
 - Distribute list in: ☐
 - Distribute list out: ☐
 - Prefix list in: ☐
 - Prefix list out: ☐
 - Route map in: ☐
 - Route map out: ☐
- Allow AS in: ☐
- Max prefix: ☐
- Attribute unchanged: ☐
- Advanced options (checkboxes):
 - Route reflector client
 - Soft reconfiguration
 - Capability: graceful restart
 - Next hop self
 - AS override
 - Capability: route refresh
 - Remove private AS
 - Route Server Client
 - Capability: default originate

Buttons: OK Cancel

Tables are added to create new neighbor groups and neighbor ranges.

Local BGP Options

Neighbor Groups

[+ Create New](#) [Edit](#) [Delete](#)

Name	Remote AS
advpn	65412
dialup-vpn	65412
2	

Neighbor Ranges

[+ Create New](#) [Edit](#) [Delete](#)

Prefix	Neighbor Group	Maximum Neighbor Number
10.10.100.0 255.255.255.0	advpn	0
10.10.200.0 255.255.255.0	advpn	0

10.10.100.2
10.10.100.3
10.10.200.2
10.10.200.3
10.100.1.1
10.100.1.5
10.100.10.1
10.100.10.5

[View Routing Monitor](#)

Paths
[23 Paths](#)

Additional Information

[API Preview](#)

[Edit in CLI](#)

[Documentation](#)

[Online Help](#) [Video Tutorials](#)

[Apply](#)

There are settings for *IPv6 Networks* and *IPv4/IPv6 Redistribute* with filter options.

Local BGP Options

[+](#)

IPv6 Networks

IP/Netmask [x](#)

[+](#)

IPv4 Redistribute

Connected ☒

RIP ☒

OSPF ☒

Static ☒

ISIS ☒

All Filter

All Filter

All Filter

All Filter

All Filter

10.10.100.2
10.10.100.3
10.10.200.2
10.10.200.3
10.100.1.1
10.100.1.5
10.100.10.1
10.100.10.5

[View Routing Monitor](#)

Paths
[23 Paths](#)

Additional Information

[API Preview](#)

[Edit in CLI](#)

[Documentation](#)

[Online Help](#) [Video Tutorials](#)

[Apply](#)

There are settings for *Dampening* and *Graceful restart*.

Local BGP Options

☒ Dampening

Route map ☐

Unreachability half-life

Reachability half-life

Reuse threshold

Suppress

Max suppress time

☒ Graceful Restart

Restart timer

Stale path timer

Update delay

☒ Advanced Options

☒ Best Path Selection

10.10.100.2
 10.10.100.3
 10.10.200.2
 10.10.200.3
 10.100.1.1
 10.100.1.5
 10.100.10.1
 10.100.10.5

Paths
[23 Paths](#)

Additional Information

Documentation
[Online Help](#)
[Video Tutorials](#)

Expand the *Advanced Options* and *Best Path Selection* sections to configure additional settings, such as *Default Local Preference*, *Distance external*, *Distance internal*, and *Distance local*.

Local BGP Options

☒ Advanced Options

Cluster ID

Default Local Preference

Distance external

Distance internal

Distance local

Keepalive

Holdtime ☒

Background scan ☒

☒ Best Path Selection

Always compare med ☐

AS path ignore ☐

Compare confederation AS path ☐

Compare router ID ☐

Med confederation ☐

10.10.100.2
 10.10.100.3
 10.10.200.2
 10.10.200.3
 10.100.1.1
 10.100.1.5
 10.100.10.1
 10.100.10.5

Paths
[23 Paths](#)

Additional Information

Documentation
[Online Help](#)
[Video Tutorials](#)

GUI page for OSPF settings

Users can configure advanced OSPF routing options on the *Network > OSPF* page.

The OSPF page includes the following settings:

- Create new areas, networks, and interfaces.

OSPF

Router ID:

Neighbors

[View Routing Monitor](#)

Additional Information

[API Preview](#)

[Edit in CLI](#)

Documentation

[Online Help](#)

[Video Tutorials](#)

Areas

[+ Create New](#) [Edit](#) [Delete](#)

Area ID	Type	Authentication
0.0.0.0	Regular	None
0.0.0.1	Not-so-stubby (NSSA)	MD5
0.0.0.2	Stub	Plain-Text

Networks

[+ Create New](#) [Edit](#) [Delete](#)

Network	Area
172.16.200.0/24	0.0.0.0
172.16.203.0/24	0.0.0.1
10.1.100.0/24	0.0.0.2

Interfaces

[+ Create New](#) [Edit](#) [Delete](#)

Name	Interfaces	Cost	Apply To IP	Authentication	Passive
port1	To_VLAN_30 (port1)	0	Any IP	Plain-Text	Disabled
agg2	To_FGT_B_agg1 (agg1)	0	Any IP	MD5	Disabled

[Apply](#)

- Create new IP address summary configurations.
- Edit the router default settings (metric type, metric value, and route map).
- Configure the redistribute attributes for each route type.

OSPF

Summary Addresses

[+ Create New](#) [Edit](#) [Delete](#)

Prefix	Advertise	Tag
172.16.0.0/15	Enable	0

Default Settings

Inject default route: ☐ Never ☒ Regular Areas ☐ Always

Metric type: ☐ Type 1 ☒ Type 2

Metric value:

Route map: ☐ All ☐ Filter

Redistribute Connected: ☒

Metric value:

Metric type: ☐ Type 1 ☒ Type 2

Tag:

Route map: ☐ All ☐ Filter

☐ test1

Redistribute Static: ☐

Redistribute RIP: ☐

Redistribute BGP: ☐

Redistribute ISIS: ☐

Advanced Settings

[Apply](#)

- Configure advanced settings (ABR type, default metric, restart mode, and BFD).
- Configure distance and overflow settings.

- Configure advanced OSPF interface settings (prefix length, priority, BFD, network type, passive interface, DB filter out, MTU, MTU ignore, and so on).

GUI routing monitor for BGP and OSPF

BGP Neighbors, *BGP Paths*, and *OSPF Neighbors* data is visible in the *Routing monitor* widget.

To view the Routing widget:

1. Go to *Dashboard > Network* and click the *Routing* widget.
2. Select one of the following options from the dropdown to view the data:
 - a. *BGP Neighbors*

[+ Add Widget](#)

Routing				
Neighbor IP	Local IP	Remote AS	State	Admin Status
IPv4 (8)				
10.10.100.2	10.10.100.254	65412	Established	✓ Enabled
10.10.100.3	10.10.100.254	65412	Established	✓ Enabled
10.10.200.2	10.10.200.254	65412	Established	✓ Enabled
10.10.200.3	10.10.200.254	65412	Established	✓ Enabled
10.100.1.1	10.100.1.2	20	Established	✓ Enabled
10.100.1.5	10.100.1.6	20	Established	✓ Enabled
10.100.10.1	0.0.0.0	20	Idle	✗ Disabled
10.100.10.5	0.0.0.0	20	Idle	✗ Disabled
IPv6 (0)				
35% (12) Updated: 19:03:03				

b. BGP Paths

[+ Add Widget](#)

Routing				
Prefix	Learned From	Next Hop	Origin	Best Path
2.2.2.2/32	10.10.100.2	10.10.100.2	IGP	✓ Yes
2.2.2.2/32	10.10.200.2	10.10.200.2	IGP	✓ Yes
4.4.4.4/32	10.10.100.3	10.10.100.3	IGP	✓ Yes
4.4.4.4/32	10.10.200.3	10.10.200.3	IGP	✓ Yes
7.0.0.0/24	10.100.1.1	10.100.1.1	IGP	✓ Yes
7.0.0.0/24	10.100.1.5	10.100.1.5	IGP	✓ Yes
8.0.0.0/24	10.100.1.1	10.100.1.1	IGP	✓ Yes
8.0.0.0/24	10.100.1.5	10.100.1.5	IGP	✓ Yes
9.0.0.0/24	0.0.0.0	0.0.0.0	IGP	✓ Yes
0% (23) Updated: 19:03:46				

c. IPv6 BGP Paths

[+ Add Widget](#)

Routing Refresh Share IPv6 BGP Paths ⋮

View Q

Prefix	Learned From	Next Hop Local	Next Hop Global	Origin	Best Path
2000::7:0:0/124	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✖ No
2000::7:0:0/124	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✔ Yes
2000::9:0:0/124	::	::	::	IGP	✔ Yes
2000:10:100:1::/126	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✔ Yes
2000:10:100:1::4/126	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✔ Yes
2000:10:100:1::200/120	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✔ Yes
2000:10:100:2::/64	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✖ No
2000:10:100:2::/64	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✔ Yes
2000:10:100:10::/126	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✔ Yes

0% 10 Updated: 19:04:05 Refresh

d. OSPF Neighbors

[+ Add Widget](#)

Routing Refresh Share OSPF Neighbors ⋮

View Q

Neighbor IP	Router ID	State
172.16.209.2	2.2.2.2	Full
172.16.210.2	2.2.2.2	Full

2 Updated: 19:02:38 Refresh

OSPF HMAC-SHA authentication - 7.0.1

This enhancement adds support for RFC 5709 HMAC-SHA cryptographic authentication for OSPF. Prior to 7.0.1, only MD5 was supported.

An option to set the algorithm is available in the router key chain configuration:

```
config router key-chain
  edit <name>
    config key
```

```

        edit <id>
            ...
            set algorithm {md5 | hmac-sha1 | hmac-sha256 | hmac-sha384 | hmac-sha512}
        next
    end
next
end

```



The available options for `set authentication` in the OSPF settings are now `none`, `text`, and `message-digest`.

To configure HMAC-SHA cryptographic authentication for OSPF:

1. Configure the router key chain:

```

config router key-chain
    edit "11"
        config key
            edit "1"
                set accept-lifetime 01:01:01 01 01 2021 2147483646
                set send-lifetime 01:01:01 01 01 2021 2147483646
                set key-string *****
                set algorithm hmac-sha512
            next
        end
    next
end

```

2. Configure OSPF:

```

config router ospf
    set router-id 2.2.2.2
    config area
        edit 0.0.0.0
            set authentication message-digest
        next
    end
    config ospf-interface
        edit "1"
            set interface "port1"
            set authentication message-digest
            set md5-keychain "11"
        next
    end
end

```

3. Verify that the OSPF neighbor can be established:

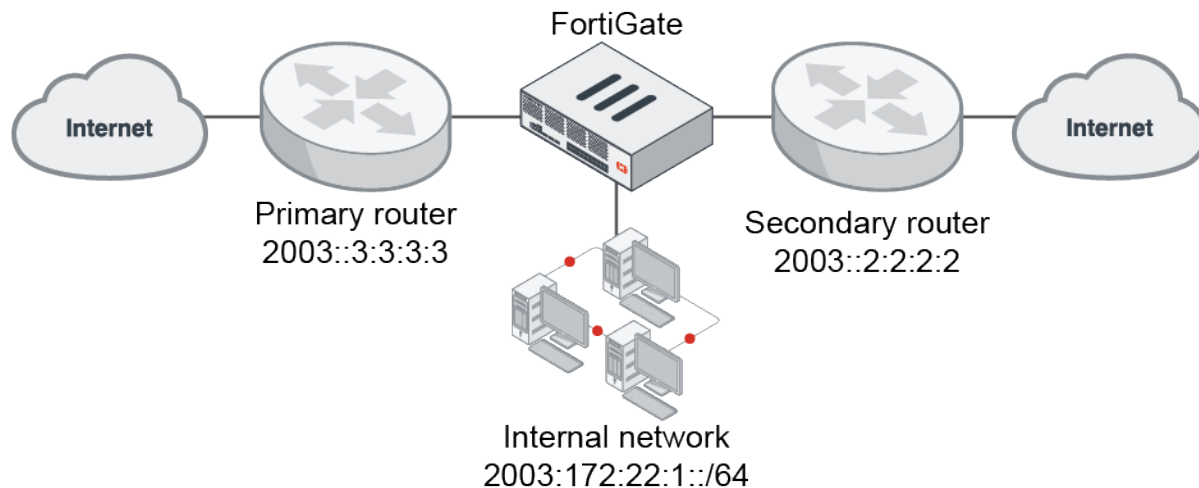
```

# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID      Pri   State           Dead Time   Address        Interface
1.1.1.1          1    Full/DR         00:00:37   12.1.1.1      port1

```

BGP conditional advertisement for IPv6 - 7.0.1

BGP conditional advertisement allows the router to advertise a route only when certain conditions are met. Starting in 7.0.1, this capability is supported for IPv6. IPv4 BGP conditional advertisement is supported in earlier versions.



Example 1

In this example, the FortiGate advertises its local network to the secondary router when the primary router is down. The FortiGate detects the primary router is down in the absence of a learned route.

- When the FortiGate learns route 2003:172:28:1::/64 from the primary router, it does not advertise its local route (2003:172:22:1::/64) to the secondary router.
- When the FortiGate does not learn route 2003:172:28:1::/64 from the primary router, it advertises its local route (2003:172:22:1::/64) to the secondary router.
- The BGP conditional advertisement condition is set to be true if the condition route map (2003:172:28:1::/64) is not matched (`non-exist`).

To configure BGP conditional advertisement with IPv6:

1. Configure the IPv6 prefix lists:

```
config router prefix-list6
  edit "adv-222"
    config rule
      edit 1
        set prefix6 2003:172:22:1::/64
        unset ge
        unset le
      next
    end
  next
  edit "lrm-281"
    config rule
      edit 1
        set prefix6 2003:172:28:1::/64
        unset ge
```

```

        unset le
    next
end
next
end

```

2. Configure the route maps:

```

config router route-map
    edit "map-221"
        config rule
            edit 1
                set match-ip6-address "adv-222"
            next
        end
    next
    edit "map-281"
        config rule
            edit 1
                set match-ip6-address "lrn-281"
            next
        end
    next
end

```

3. Configure BGP:

```

config router bgp
    set as 65412
    set router-id 1.1.1.1
    set ibgp-multipath enable
    set network-import-check disable
    set graceful-restart enable
    config neighbor
        edit "2003::2:2:2:2"
            set soft-reconfiguration6 enable
            set remote-as 65412
            set update-source "loopback1"
            config conditional-advertise6
                edit "map-221"
                    set condition-routemap "map-281"
                    set condition-type non-exist
                next
            end
        next
    next
    edit "2003::3:3:3:3"
        set soft-reconfiguration6 enable
        set remote-as 65412
        set update-source "loopback1"
    next
end

```

In this configuration, if route map `map-281` does not exist, then the FortiGate advertises route map `map-221` to neighbor `2003::2:2:2:2`.

4. Verify the routing table:

```
# get router info6 routing-table bgp
B      2003:172:28:1::/64 [200/0] via 2003::3:3:3:3 (recursive via
****:***:***:***:***:****, port9), 01:23:45
B      2003:172:28:2::/64 [200/0] via 2003::3:3:3:3 (recursive via
****:***:***:***:***:****, port9), 23:09:22
```

When the FortiGate learns 2003:172:28:1::/64, it will not advertise its local route 2003:172:22:1::/64 to neighbor 2003::2:2:2:2. If the FortiGate has not learned 2003:172:28:1::/64, it will advertise its local route 2003:172:22:1::/64 to neighbor 2003::2:2:2:2.

Example 2

With the same IPv6 prefix lists and route maps, when the FortiGate does learn 2003:172:28:1::/64, it advertises local route 2003:172:22:1::/64 to the secondary router. The BGP conditional advertisement condition is set to be true if the condition route map is matched (`exist`).

To configure BGP conditional advertisement with IPv6:**1. Configure BGP:**

```
config router bgp
  config neighbor
    edit "2003::2:2:2:2"
      config conditional-advertise6
        edit "map-221"
          set condition-routemap "map-281"
          set condition-type exist
        next
      end
    next
  end
end
```

2. Verify the routing table:

```
# get router info6 routing-table bgp
B      2003:172:28:1::/64 [200/0] via 2003::3:3:3:3 (recursive via
****:***:***:***:***:****, port9), 01:23:45
B      2003:172:28:2::/64 [200/0] via 2003::3:3:3:3 (recursive via
****:***:***:***:***:****, port9), 23:09:22
```

When the FortiGate learns 2003:172:28:1::/64, it will advertise its local route 2003:172:22:1::/64 to neighbor 2003::2:2:2:2. If the FortiGate has not learned route 2003:172:28:1::/64, it will not advertise its local route 2003:172:22:1::/64 to neighbor 2003::2:2:2:2.

Enable or disable updating policy routes when link health monitor fails - 7.0.1

An option has been added to toggle between enabling or disabling policy route updates when a link health monitor fails. By disabling policy route updates, a link health monitor failure will not cause corresponding policy-based routes to be removed.

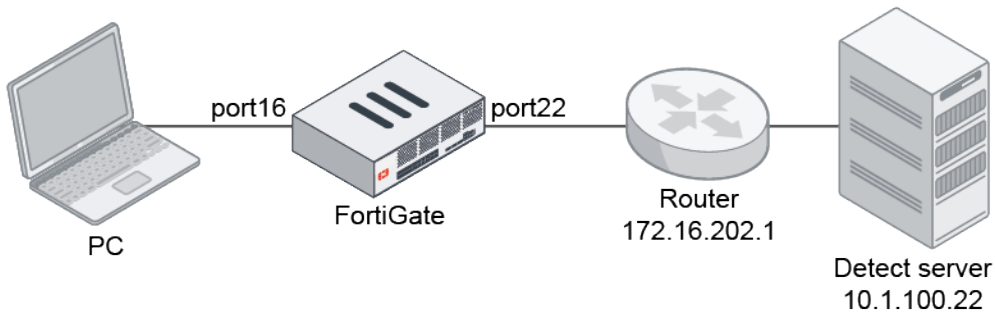

```

config system link-monitor
  edit <name>
    set update-policy-route {enable | disable}
  next
end

```

Example

In the following topology, the FortiGate is monitoring the detect server, 10.1.100.22. The FortiGate has a policy-based route to destination 172.16.205.10 using the same gateway (172.16.202.1) and interface (port22). By configuring `update-policy-route disable`, the policy-based route is not removed when the link health monitor detects a failure.



To disable updating policy routes when the link health monitor fails:

1. Configure the link health monitor:

```

config system link-monitor
  edit "test-1"
    set srcintf "port22"
    set server "10.1.100.22"
    set gateway-ip 172.16.202.1
    set failtime 3
    set update-policy-route disable
  next
end

```

2. Configure the policy route:

```

config router policy
  edit 1
    set input-device "port16"
    set dst "172.16.205.10/255.255.255.255"
    set gateway 172.16.202.1
    set output-device "port22"
    set tos 0x14
    set tos-mask 0xff
  next
end

```

3. When the health link monitor status is up, verify that the policy route is active.

a. Verify the link health monitor status:

```
# diagnose sys link-monitor status
Link Monitor: test-1, Status: alive, Server num(1), HA state: local(alive), shared
(alive)
Flags=0x1 init, Create time: Fri May 28 15:20:15 2021
Source interface: port22 (14)
Gateway: 172.16.202.1
Interval: 500 ms
Service-detect: disable
Diffservcode: 000000
Class-ID: 0
  Peer: 10.1.100.22(10.1.100.22)
    Source IP(172.16.202.2)
    Route: 172.16.202.2->10.1.100.22/32, gwy(172.16.202.1)
    protocol: ping, state: alive
      Latency(Min/Max/Avg): 0.374/0.625/0.510 ms
      Jitter(Min/Max/Avg): 0.008/0.182/0.074
      Packet lost: 0.000%
      Number of out-of-sequence packets: 0
      Fail Times(0/3)
      Packet sent: 7209, received: 3400, Sequence(sent/rcvd/exp):
7210/7210/7211
```

b. Verify the policy route list:

```
# diagnose firewall proute list
list route policy info(vf=root):
id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x14 tos_mask=0xff protocol=0 sport=0-0 iif=41
dport=0-65535 oif=14(port22) gwy=172.16.202.1
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 172.16.205.10/255.255.255.255
hit_count=1 last_used=2021-05-27 23:04:33
```

4. When the health link monitor status is down, verify that the policy route is active:

a. Verify the link health monitor status:

```
# diagnose sys link-monitor status
Link Monitor: test-1, Status: die, Server num(1), HA state: local(die), shared(die)
Flags=0x9 init log_downgateway, Create time: Fri May 28 15:20:15 2021
Source interface: port22 (14)
Gateway: 172.16.202.1
Interval: 500 ms
Service-detect: disable
Diffservcode: 000000
Class-ID: 0
  Peer: 10.1.100.22(10.1.100.22)
    Source IP(172.16.202.2)
    Route: 172.16.202.2->10.1.100.22/32, gwy(172.16.202.1)
    protocol: ping, state: die
      Packet lost: 11.000%
      Number of out-of-sequence packets: 0
      Recovery times(0/5) Fail Times(0/3)
      Packet sent: 7293, received: 3471, Sequence(sent/rcvd/exp):
7294/7281/7282
```

b. Verify the policy route list:

```
# diagnose firewall proute list
list route policy info(vf=root):
id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x14 tos_mask=0xff protocol=0 sport=0-0 iif=41
dport=0-65535 oif=14(port22) gwy=172.16.202.1
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 172.16.205.10/255.255.255.255
hit_count=1 last_used=2021-05-27 23:04:33
```

If the `update-policy-route` setting is enabled, the link health monitor would be down and the policy-based route would be disabled:

```
# diagnose firewall proute list
list route policy info(vf=root):
id=1 dscp_tag=0xff 0xff flags=0x8 disable tos=0x14 tos_mask=0xff protocol=0 sport=0-0
iif=41 dport=0-65535 oif=14(port22) gwy=172.16.202.1
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 172.16.205.10/255.255.255.255
hit_count=1 last_used=2021-05-27 23:04:33
```

Add weight setting on each link health monitor server - 7.0.1

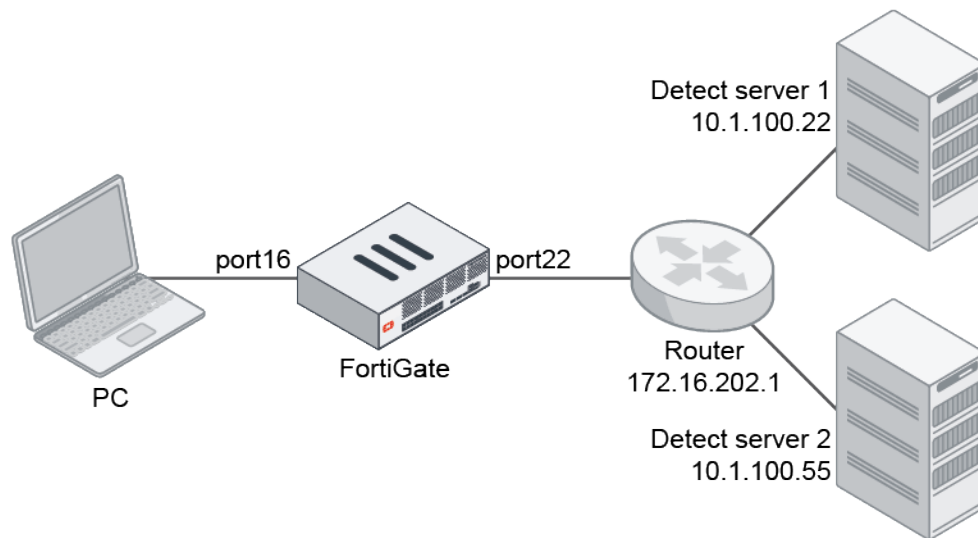
Prior to FortiOS 7.0.1, the link health monitor is determined to be dead when all servers are unreachable. Starting in 7.0.1, the link health monitor can configure multiple servers and allow each server to have its own weight setting. When the link health monitor is down, it will trigger static route updates and cascade interface updates if the weight of all dead servers exceeds the monitor's fail weight threshold.

```
config system link-monitor
  edit <name>
    set srcintf <interface>
    set server-config {default | individual}
    set fail-weight <integer>
    config server-list
      edit <id>
        set dst <address>
        set weight <integer>
      next
    end
  next
end
```

server-config	Set the server configuration mode: <ul style="list-style-type: none"> default: all servers share the same attributes. individual: some attributes can be specified for individual servers.
fail-weight <integer>	Threshold weight to trigger link failure alert (0 - 255, default = 0).
server-list	Configure the servers to be monitored by the link monitor.
dst <address>	Enter the IP address of the server to be monitored.
weight <integer>	Weight of the monitor to this destination (0 - 255, default = 0).

Examples

In the following topology, there are two detect servers that connect to the FortiGate through a router: server 1 (10.1.100.22) and server 2 (10.1.100.55).



Alive link health monitor

In this configuration, one server is dead and one server alive. The failed server weight is not over the threshold, so the link health monitor status is alive.

To configure the weight settings on the link health monitor:

1. Configure the link health monitor:

```

config system link-monitor
  edit "test-1"
    set srcintf "port22"
    set server-config individual
    set gateway-ip 172.16.202.1
    set failtime 3
    set fail-weight 40
    config server-list
      edit 1
        set dst "10.1.100.22"
        set weight 60
      next
      edit 2
        set dst "10.1.100.55"
        set weight 30
      next
    end
  next
end

```

2. Trigger server 2 to go down. The link monitor is still alive because the fail weight threshold has not been reached.

3. Verify the link health monitor status:

```
# diagnose sys link-monitor status test-1
Link Monitor: test-1, Status: alive, Server num(2), HA state: local(alive), shared
(alive)
Flags=0x1 init, Create time: Fri Jun  4 17:23:29 2021
Source interface: port22 (14)
Gateway: 172.16.202.1
Interval: 500 ms
Service-detect: disable
Diffservcode: 000000
Class-ID: 0
Fail-weight (40): not activated
  Peer: 10.1.100.22(10.1.100.22)
    Source IP(172.16.202.2)
    Route: 172.16.202.2->10.1.100.22/32, gwy(172.16.202.1)
    protocol: ping, state: alive
      Latency(Min/Max/Avg): 0.417/0.585/0.530 ms
      Jitter(Min/Max/Avg): 0.007/0.159/0.057
      Packet lost: 0.000%
      Number of out-of-sequence packets: 0
      Fail Times(0/3)
      Packet sent: 239, received: 236, Sequence(sent/rcvd/exp): 240/240/241
  Peer: 10.1.100.55(10.1.100.55)
    Source IP(172.16.202.2)
    Route: 172.16.202.2->10.1.100.55/32, gwy(172.16.202.1)
    Fail weight 30 applied
    protocol: ping, state: dead
      Packet lost: 100.000%
      Number of out-of-sequence packets: 0
      Recovery times(0/5) Fail Times(1/3)
      Packet sent: 239, received: 3, Sequence(sent/rcvd/exp): 240/4/5
```

Dead link health monitor

In this configuration, one server is dead and one server alive. The failed server weight is over the threshold, so the link health monitor status is dead.

To configure the weight settings on the link health monitor:

1. Configure the link health monitor:

```
config system link-monitor
  edit "test-1"
    set srcintf "port22"
    set server-config individual
    set gateway-ip 172.16.202.1
    set failtime 3
    set fail-weight 40
  config server-list
    edit 1
      set dst "10.1.100.22"
      set weight 30
    next
    edit 2
      set dst "10.1.100.55"
```

```

        set weight 50
    next
end
next
end

```

2. Trigger server 2 to go down. The link monitor is dead because the fail weight threshold has been reached.
3. Verify the link health monitor status:

```

# diagnose sys link-monitor status test-1
Link Monitor: test-1, Status: dead, Server num(2), HA state: local(dead), shared(dead)
Flags=0x9 init log_downgateway, Create time: Fri Jun  4 17:23:29 2021
Source interface: port22 (14)
Gateway: 172.16.202.1
Interval: 500 ms
Service-detect: disable
Diffservcode: 000000
Class-ID: 0
Fail-weight (40): activated
  Peer: 10.1.100.22(10.1.100.22)
    Source IP(172.16.202.2)
    Route: 172.16.202.2->10.1.100.22/32, gwy(172.16.202.1)
    protocol: ping, state: alive
      Latency(Min/Max/Avg): 0.393/0.610/0.520 ms
      Jitter(Min/Max/Avg): 0.009/0.200/0.095
      Packet lost: 0.000%
      Number of out-of-sequence packets: 0
      Fail Times(0/3)
      Packet sent: 680, received: 677, Sequence(sent/rcvd/exp): 681/681/682
  Peer: 10.1.100.55(10.1.100.55)
    Source IP(172.16.202.2)
    Route: 172.16.202.2->10.1.100.55/32, gwy(172.16.202.1)
    Fail weight 50 applied
    protocol: ping, state: dead
      Packet lost: 100.000%
      Number of out-of-sequence packets: 0
      Recovery times(0/5) Fail Times(1/3)
      Packet sent: 680, received: 3, Sequence(sent/rcvd/exp): 681/4/5

```

Enhanced hashing for LAG member selection - 7.0.1

FortiGate models that have an internal switch that supports modifying the distribution algorithm can use enhanced hashing to help distribute traffic evenly, or load balance, across links on the Link Aggregation (LAG) interface.

The enhanced hashing algorithm is based on a 5-tuple of the IP protocol, source IP address, destination IP address, source port, and destination port.

Different computation methods allow for more variation in the load balancing distribution, in case one algorithm does not distribute traffic evenly between links across different XAUIs. The available methods are:

xor16	Use the XOR operator to make a 16 bit hash.
xor8	Use the XOR operator to make an 8 bit hash.
xor4	Use the XOR operator to make a 4 bit hash.

crc16

Use the CRC-16-CCITT polynomial to make a 16 bit hash.



The following NP6 non-service FortiGate models support this feature: 1200D, 1500D, 1500DT, 3000D, 3100D, 3200D, 3700D, and 5001D.

To configure the enhanced hashing:

```
config system npu
    set lag-out-port-select {enable | disable}
    config sw-eh-hash
        set computation {xor4 | xor8 | xor16 | crc16}
        set ip-protocol {include | exclude}
        set source-ip-upper-16 {include | exclude}
        set source-ip-lower-16 {include | exclude}
        set destination-ip-upper-16 {include | exclude}
        set destination-ip-lower-16 {include | exclude}
        set source-port {include | exclude}
        set destination-port {include | exclude}
        set netmask-length {0 - 32}
    end
end
```

For example, to use XOR16 and include all of the fields in the 5-tuple to compute the link in the LAG interface that the packet is distributed to:

```
config system npu
    set lag-out-port-select enable
    config sw-eh-hash
        set computation xor16
        set ip-protocol include
        set source-ip-upper-16 include
        set source-ip-lower-16 include
        set destination-ip-upper-16 include
        set destination-ip-lower-16 include
        set source-port include
        set destination-port include
        set netmask-length 32
    end
end
```

Add GPS coordinates to REST API monitor output for FortiExtender and LTE modems - 7.0.2

When querying a FortiExtender or LTE modem through the FortiGate REST API, the GPS coordinates are included in the response.

FortiExtender

GPS reading must be enabled in the FortiExtender profile to use this feature.

To enable GPS reading in the GUI:

1. Go to *Network > FortiExtenders* and select the *Profiles* tab.
2. Double-click a profile to edit it.
3. In the *Modem 1* section, enable *GPS*.
4. Click *OK*.

To enable GPS reading in the CLI:

```
config extender-controller extender-profile
  edit <name>
    config cellular
      config modem1
        set gps enable
      end
    end
  next
end
```

api/v2/monitor/extender-controller/extender

```
api/v2/monitor/extender-controller/extender?id=FX004TQ21000000
{
  "http_method": "GET",
  "results": [
    {
      "name": "FX004TQ21000000",
      "id": "FXA11FTQ21000000",
      "system": {
        "cpu": 0,
        "memory": 15,
        "ip": "192.168.1.110",
        "software_version": "FXTA11F-v7.0.1-build614",
        "hardware_version": "P26794-01",
        "mac": "***:**:**:**:**:**",
        "netmask": "255.255.255.0",
        "gateway": "192.168.1.99",
        "addr_type": "",
        "fgt_ip": "",
        "gps_lat": "49.304016",
        "gps_long": "-122.817596"
      },
      "modem1": {
        "data_plan": "Generic-plan",
        "physical_port": "1-2:1.3",
        "manufacturer": "Quectel",
        "product": "Quectel",
        "model": "EM06A",
        "revision": "EM06ALAR03A05M4G",
        "imsi": "111111111111111",
        "pin_status": "disable",
        "service": "LTE",
        "signal_strength": "52",
        "rssi": "-74",
        "connect_status": "CONN_STATE_CONNECTED",

```



```
"gsm_profile":[
],
"cdma_profile":{
  "NAI":"",
  "idx":"",
  "status":"",
  "home_addr":"",
  "primary_ha":"",
  "secondary_ha":"",
  "aaa_spi":"",
  "ha_spi":""
},
"esn_imei":"222222222222222",
"activation_status":"Attached [profile 12]",
"roaming_status":"Registered, home network",
"usim_status":"",
"oma_dm_version":"",
"plmn":"",
"band":"LTE BAND 2",
"signal_rsrq":"-13",
"signal_rsrp":"-104",
"lte_sinr":"17",
"lte_rssi":"-74",
"lte_rs_throughput":"",
"lte_ts_throughput":"",
"lte_physical_cellid":"61D050E",
"modem_type":"EM06A",
"drc_cdma_evdo":"",
"current_snr":"",
"wireless_operator":"Fido",
"operating_mode":"",
"wireless_signal":"52",
"usb_wan_mac":"",
"sim1":{
  "carrier":"",
  "phone_number":"",
  "status":"disable",
  "is_active":0,
  "imsi":"N/A",
  "iccid":"",
  "maximum_allowed_data":0,
  "overage_allowed":"disable",
  "next_billing_date":"N/A",
  "data_usage":0,
  "slot":1,
  "modem":1
},
"sim2":{
  "carrier":"Fido",
  "phone_number":"+*****",
  "status":"enable",
  "is_active":1,
  "imsi":"111111111111111",
  "iccid":"33333333333333333333",
  "maximum_allowed_data":70,
  "overage_allowed":"disable",
```

```
        "next_billing_date":"2021-10-10",
        "data_usage":69,
        "slot":2,
        "modem":1
    }
}
},
"vdom":"root",
"path":"extender-controller",
"name":"extender",
"action":"",
"status":"success",
"serial":"FG81EPTK000000000",
"version":"v7.0.2",
"build":211
}
```

LTE modem

GPS reading must be enabled on 3G4G models to use this feature.

To enable GPS reading:

```
config system lte-modem
    set gps-service enable
end
```

[api/v2/monitor/system/lte-modem/status](#)

```
{
  "http_method":"GET",
  "results":{
    "status":"enabled",
    "billing_date":1,
    "gps_status":true,
    "data_limit":20,
    "data_usage_tracking":true,
    "sim_auto_switch":true,
    "sim_auto_switch_time":"5-minutes",
    "manufacturer":"Sierra Wireless, Incorporated",
    "model":"EM7565",
    "revision":"SWI9X50C_01.14.02.00 2e210b jenkins 2020\08\19 14:18:39",
    "msisdn":"11111111111",
    "esn":"0",
    "imei":"222222222222222",
    "meid":"",
    "cell_id":"",
    "hw_revision":"1.0",
    "sw_revision":"S.AT.2.5.1-00666-9655_GEN_PACK-1",
    "sku":"",
    "fsn":"UF0000000000000000",
    "operating_mode":"QMI_DMS_OPERATING_MODE_ONLINE",
    "roaming":false,
  }
}
```

```

"signal":{
  "wcdma":{
    "rssi":-102,
    "ecio":29
  },
  "lte":{
    "rssi":-72,
    "rsrq":-14,
    "rsrp":-103,
    "snr":120
  }
},
"active_sim":{
  "slot":2,
  "status":"SIM_STATE_PRESENT",
  "iccid":"3333333333333333",
  "imsi":"4444444444444444",
  "carrier":"Rogers AT&T Wireless",
  "country":"Canada"
},
"usage":{
  "rx":3209284,
  "tx":110981
},
"connection_status":"QMI_WDS_CONNECTION_STATUS_DISCONNECTED",
"gps":{
  "latitude":49.281737116666662,
  "longitude":-122.86043441666668,
  "timestamp":11871443012
}
},
"vdom":"root",
"path":"system",
"name":"lte-modem",
"action":"status",
"status":"success",
"serial":"FG40FITK2000000",
"version":"v7.0.2",
"build":205
}

```

BGP error handling per RFC 7606 - 7.0.2

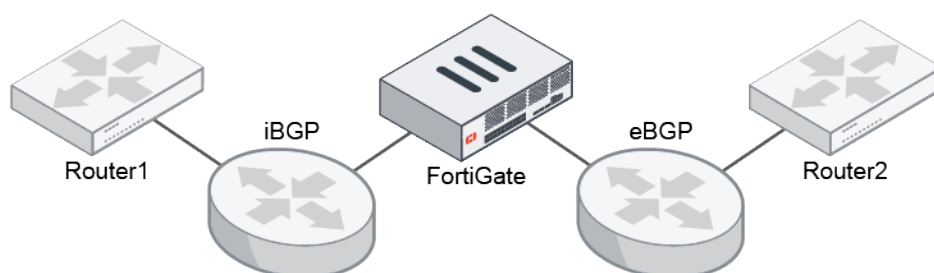
BGP error handling on malformed attributes in BGP UPDATE messages is extended to additional techniques referenced in RFC 7606 (see [RFC 7606](#) for details). The FortiGate uses one of the three approaches to handle malformed attribute, in order of decreasing severity:

1. Notification and Session reset
2. Treat-as-withdraw
3. Attribute discard

When a BGP UPDATE message contains multiple malformed attributes, the most severe approach that is triggered by one of the attributes is followed.

The following table lists the BGP attributes, and how FortiGate handles a malformed attribute in the UPDATE message:

BGP attribute	Handling
origin	Handled by the treat-as-withdraw approach.
AS path	Handled by the treat-as-withdraw approach.
AS 4 path	Handled by the attribute discard approach.
aggregator	Handled by the attribute discard approach.
aggregator 4	Handled by the attribute discard approach.
next-hop	Handled by the treat-as-withdraw approach.
multiple exit discriminator	Handled by the treat-as-withdraw approach.
local preference	Handled by the treat-as-withdraw approach.
atomic aggregate	Handled by the attribute discard approach.
community	Handled by the treat-as-withdraw approach.
extended community	Handled by the treat-as-withdraw approach.
originator	Handled by the treat-as-withdraw approach.
cluster	Handled by the treat-as-withdraw approach.
PMSI	Handled by the treat-as-withdraw approach.
MP reach	Handled by the notification message approach.
MP unreachable	Handled by the notification message approach.
attribute set	Handled by the treat-as-withdraw approach.
AIGP	Handled by the treat-as-withdraw approach.
Unknown	If the BGP flag does not indicate that this is an optional attribute, this malformed attribute is handled by the notification message approach.



This example shows how the ORIGIN attribute can be malformed, and how it is handled.

Reason for malformed attribute	Handling
ORIGIN attribute length not one	The prefix will be gone and the BGP session will not be reset.
ORIGIN attribute value is invalid	The prefix will be gone and the BGP session will not be reset.

Reason for malformed attribute	Handling
Two ORIGIN attributes with different values	The attributes are ignored, the BGP session will not be reset, and the BGP route will remain.
ORIGIN attribute is absent	The BGP session will be reset

For example, if the FortiGate receives a malformed UPDATE packet from the neighbor at 27.1.1.124 that has no ORIGIN attribute, the BGP session is reset and the state of the neighbor is shown as `Idle`, the first state of the BGP neighborhood connection.

```
# get router info bgp summary
VRF 0 BGP router identifier 27.1.1.125, local AS number 125
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent   TblVer   InQ OutQ Up/Down State/PfxRcd
3.3.3.3        4      33      33       0         0   0   0   never Active
27.1.1.124    4      124     94     126       0   0   0   never Idle

Total number of neighbors 2
```

Configure IPAM locally on the FortiGate - 7.0.2

IPAM (IP address management) is now available locally on the FortiGate. A standalone FortiGate, or a Fabric root in the Security Fabric, can act as the IPAM server. Interfaces configured to be auto-managed by IPAM will receive an address from the IPAM server's address/subnet pool. *DHCP Server* is automatically enabled in the GUI, and the address range is populated by IPAM. Users can customize the address pool subnet and the size of a subnet that an interface can request.

To configure IPAM settings:

```
config system ipam
    set pool-subnet <class IP and netmask>
    set status {enable | disable}
end
```

<code>pool-subnet <class IP and netmask></code>	Set the IPAM pool subnet, class A or class B subnet.
---	--

<code>status {enable disable}</code>	Enable/disable IP address management services.
--	--

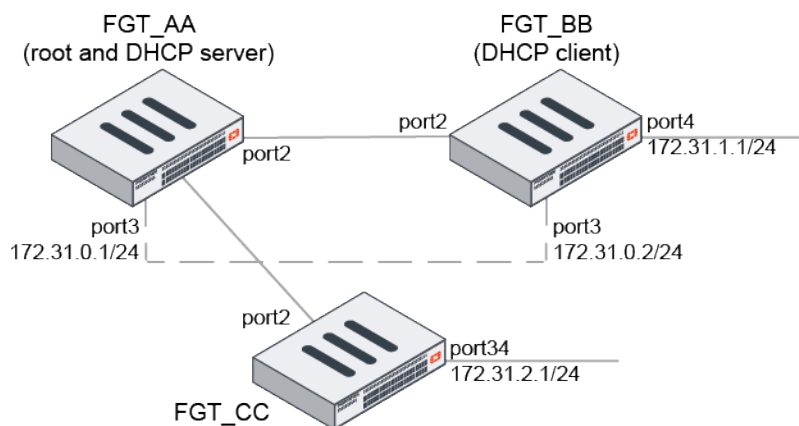
In previous FortiOS versions, the `set fortiipam-integration` option was configured under `config system global`.

Three additional options are available (32, 64, and 128) for allocating the subnet size:

```
config system interface
    set managed-subnetwork-size {32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 |
16384 | 32768 | 65536}
end
```

Example

In this example, FGT_AA is the Security Fabric root with IPAM enabled. FGT_BB and FGT_CC are downstream Fabric devices and retrieve IPAM information from FGT_AA. The Fabric interface on all FortiGates is port2. FGT_AA acts as the DHCP server, and FGT_BB acts as the DHCP client.



To configure IPAM locally in the Security Fabric:

1. On the root FortiGate, go to *Network > Interfaces* and edit port3.
2. For *Addressing Mode*, select *Auto-Managed by IPAM*. *DHCP Server* is automatically enabled.

Edit Interface

Name

port3

Alias

Type

Physical Interface

VRF ID

0

Virtual domain

root

Role

Undefined

Address

Addressing mode

Manual DHCP **Auto-managed by IPAM** One-Arm Sniffer

⚠ IPAM is not enabled.

Enable IPAM

IP/Netmask

Not allocated

Network size

256 (255.255.255.0)

ℹ IPAM will allocate an IP subnet with the selected size.

Administrative Access

IPv4

☐ HTTPS
☐ HTTP
☐ PING

☐ FMG-Access
☐ SSH
☐ SNMP

☐ FTM
☐ RADIUS Accounting
☐ Security Fabric Connection

☐ Speed Test

Receive LLDP

Use VDOM Setting

Enable

Disable

DHCP Server

DHCP status

Enabled

Disabled

Address range

Not allocated

Netmask

0.0.0.0

Default gateway

Same as Interface IP

Specify

DNS server

Same as System DNS

Same as Interface IP

Specify

Lease time

604800

second(s)

FortiGate

FGT-AA

Status

Up

MAC address

Additional Information

API Preview

References

Edit in CLI

Documentation

Online Help

Video Tutorials

- In this example, IPAM is not enabled yet. Click *Enable IPAM*. The *Edit Fabric Connector* pane opens.

FortiOS 7.0.0 New Features Guide
Fortinet Technologies Inc.

201

The screenshot shows two overlapping configuration windows in FortiGate. The 'Edit Interface' window on the left is for 'port3', a physical interface in the 'root' virtual domain. It shows the 'Address' section with 'Auto-managed IP' selected, and a warning that 'IPAM is not enabled'. The 'DHCP Server' section is also visible. The 'Edit Fabric Connector' window on the right is titled 'Core Network Security' and shows 'IP Address Management (IPAM)' settings. It includes a status toggle set to 'Enabled' and a 'Pool subnet' field set to '172.31.0.0 255.255.0.0'. A blue information box states: 'This FortiGate will be the IPAM server in the Security Fabric.' At the bottom are 'OK' and 'Cancel' buttons.

4. Enter the *Pool subnet* (only class A and B are allowed) and click **OK**. The root FortiGate is now the IPAM server in the Security Fabric. The following is configured in the backend:

```
config system interface
    edit "port3"
        set vdom "root"
        set ip 172.31.0.1 255.255.255.0
        set type physical
        set device-identification enable
        set snmp-index 5
        set ip-managed-by-fortiipam enable
    end
next
end

config system ipam
    set status enable
end
```

IPAM is managing a 172.31.0.0/16 network and assigned port3 a /24 network by default.

The *IP/Netmask* field in the *Address* section has been automatically assigned a class C IP by IPAM. The *Address range* and *Netmask* fields in the *DHCP Server* section have also been automatically configured by IPAM.

Edit Interface

Name: port3

Alias:

Type: Physical Interface

VRF ID:

Virtual domain: root

Role:

Address

Addressing mode: ☐ Manual ☐ DHCP ☒ Auto-managed by IPAM ☐ One-Arm Sniffer

IP/Netmask:

Network size:

Administrative Access

IPv4: ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection ☐ Speed Test

Receive LLDP: ☒ Use VDOM Setting ☐ Enable ☐ Disable

DHCP Server

DHCP status: ☒ Enabled ☐ Disabled

Address range:

Netmask:

Default gateway: ☒ Same as Interface IP ☐ Specify

DNS server: ☒ Same as System DNS ☐ Same as Interface IP ☐ Specify

Lease time: second(s)

FortiGate

FGT AA

Status: Up

MAC address:

Additional Information

Documentation

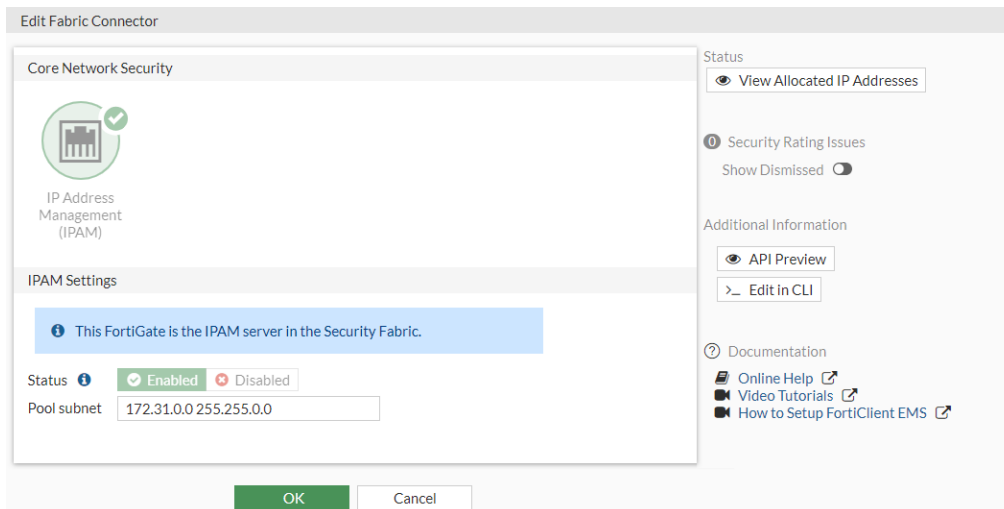
5. Click **OK**.
6. Log in to FGT-BB and set the *Addressing Mode* of port4 to *Auto-Managed by IPAM*. The subnet assigned from the pool on the root is 172.31.1.1/24.
7. Log in to FG_CC and set the *Addressing Mode* of port34 to *Auto-Managed by IPAM*. The subnet assigned from the pool on the root is 172.31.2.1/24.



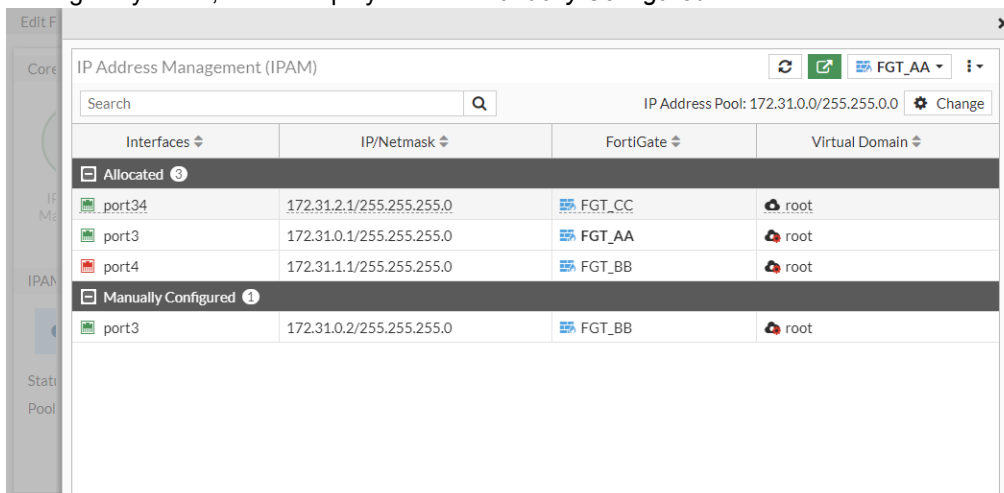
Any interface on a downstream FortiGate can be managed by the IPAM server. The interface does not have to be directly connected to the Fabric root FortiGate.

To edit the IPAM subnet:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *IP Address Management (IPAM)* card.
2. Edit the pool subnet if needed.



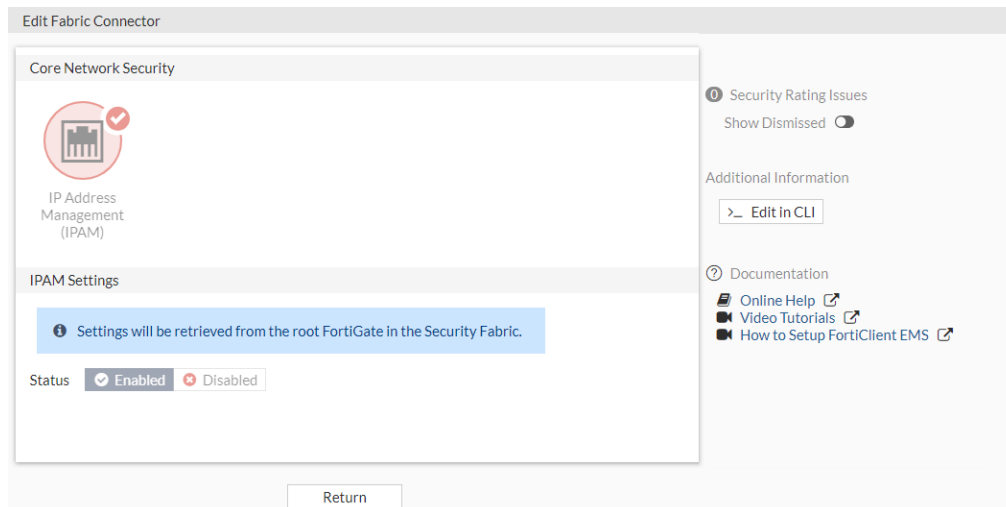
- In the right-side pane, click *View Allocated IP Addresses* to view the subnet allocations (port34, port3, and port3) and DHCP lease information. On FGT_BB, port3 is a DHCP client and the DHCP server interface (FGT_AA port3) is managed by IPAM, so it is displayed in the *Manually Configured* section.



The same allocated IP address information is available in the *IP Address Management (IPAM)* widget that can be added to the *Dashboard > Status* page.

- Click **OK**.

On downstream FortiGates, the settings on the *IP Address Management (IPAM)* card cannot be changed if IPAM is enabled on the root FortiGate.



Diagnostics

Use the following commands to view IPAM related diagnostics.

To view the largest available subnet size:

```
# diagnose sys ipam largest-available-subnet
Largest available subnet is a /17.
```

To verify IPAM allocation information:

```
# diagnose sys ipam dump-ipams-entries
IPAM Entries: (sn, vdom, interface, subnet/mask, flag)
F140EP4Q17000000 root port34 172.31.2.1/24 0
FG5H1E5818900001 root port3 172.31.0.1/24 0
FG5H1E5818900002 root port4 172.31.1.1/24 0
FG5H1E5818900003 root port3 172.31.0.2/24 1
```

To verify the available subnets:

```
# diagnose sys ipam dump-ipams-free-subnets
IPAM free subnets: (subnet/mask)
172.31.3.0/24
172.31.4.0/22
172.31.8.0/21
172.31.16.0/20
172.31.32.0/19
172.31.64.0/18
172.31.128.0/17
```

To remove a device from IPAM in the Security Fabric:

```
# diagnose sys ipam delete-device-from-ipams F140EP4Q17000000
Successfully removed device F140EP4Q17000000 from ipam
```

IPv6

This section includes information about IPv6 related new features:

- [Configuring IPv6 multicast policies in the GUI on page 206](#)
- [GUI support for configuring IPv6 on page 207](#)
- [FortiGate as an IPv6 DDNS client for generic DDNS on page 212](#)
- [FortiGate as an IPv6 DDNS client for FortiGuard DDNS on page 212](#)
- [Allow backup and restore commands to use IPv6 addresses on page 213](#)
- [VRF support for IPv6 7.0.1 on page 214](#)
- [IPv6 tunnel inherits MTU based on physical interface 7.0.2 on page 218](#)

Configuring IPv6 multicast policies in the GUI

IPv6 multicast policies can be configured in the GUI. Comments can be configured for IPv4 and IPv6 multicast policies.

To configure an IPv6 multicast policy in the GUI:

1. Enable the IPv6 and multicast features:
 - a. Go to *System > Feature Visibility*.
 - b. Under *Core Features*, enable *IPv6*.
 - c. Under *Additional Features*, enable *Multicast Policy*.
 - d. Click *Apply*.
2. Create an IPv6 multicast address object:
 - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
 - b. For *Category*, select *IPv6 Multicast Address*.
 - c. Enter a name and IPv6 address.

The screenshot shows the 'New Address' configuration window in the FortiGate GUI. The 'Category' tab is active, and 'IPv6 Multicast Address' is selected. The 'Name' field is filled with 'test-ipv6-multicast-addr1'. The 'IPv6 Address' field contains 'ff02::5/128'. The 'Comments' field is empty with a character count of 0/255. On the right, there are links for 'FortiGate', 'FGDocs', and 'API Preview'. Below these are links to various guides for configuring dynamic addresses from AWS, Azure, Google Cloud Platform, Oracle Cloud Infrastructure, and OpenStack. At the bottom of the window are 'OK' and 'Cancel' buttons.

- d. Click *OK*.

3. Create an IPv6 multicast policy:
 - a. Go to *Policy & Objects > IPv6 Multicast Policy* and click *Create New*.
 - b. Configure the settings as needed.

- c. Click OK.

GUI support for configuring IPv6

FortiOS 7.0.0 adds GUI support for configuring IPv6 settings for IPv6 MAC address, SNMP, DHCPv6 server and client, DHCPv6 SLAAC and prefix delegation. Updates include:

- When IPv6 is enabled, a user can view, edit, and create IPv6 host entries.
- General IPv6 options can be set on the *Interface* page, including the ability to configure SLAAC and DHCPv6.
- Ability to retrieve IPv6 information for a DHCPv6 client similar to the existing DHCP support for IPv4.
- IPv6 MAC is available from the address creation context menu.

The following lists example scenarios for using these features.

Enabling autoconfiguration with DHCPv6 stateless server

IPv6 must be enabled in *System > Feature Visibility*.

In this scenario, FortiGate A (server) is connected to FortiGate B (client).

To enable IPv6 autoconfiguration with DHCPv6 stateless server:

1. Configure FortiGate A:
 - a. On FortiGate A, go to *Network > Interfaces*.
 - b. Edit the desired server interface.
 - c. Select *Manual* for *IPv6 addressing mode*.
 - d. Enable *Stateless Address Auto-configuration (SLAAC)*.
 - e. Enable *IPv6 prefix list*.
 - f. Populate the *IPv6 Address/Prefix* and *IPv6 prefix* fields with the desired prefix.
 - g. Click OK.

2. Configure FortiGate B:
 - a. On FortiGate B, go to *Network > Interfaces*.
 - b. Edit the server interface.
 - c. Enable *Auto configure IPv6 address*. FortiGate B uses the prefix that it obtains from the server interface and automatically generates an IPv6 address.

Configuring a DHCPv6 stateful server

In this scenario, FortiGate A (server) is connected to FortiGate B (client).

To configure a DHCPv6 stateful server:

1. Configure FortiGate A:
 - a. On FortiGate A, go to *Network > Interfaces*.
 - b. Edit the desired server interface.
 - c. Enable *DHCPv6 Server*.
 - d. In the *IPv6 subnet* field, enter the desired subnet.
 - e. For *DNS service*, select *Specify*. Enter the desired DNS service address.
 - f. Enable *Stateful server*.
 - g. For *IP mode*, select *IP Range*.
 - h. In the *Address range* field, enter the desired IP address range.

i. Click OK.

Edit Interface

Name port33

Alias

Type Physical Interface

VRF ID 0

Virtual domain vdom1

Role Undefined

Address

Addressing mode **Manual** DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask

IPv6 addressing mode **Manual** DHCP Delegated

IPv6 Address/Prefix

Auto configure IPv6 address ☐

DHCPv6 prefix delegation ☐

Secondary IP address ☐

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP ☒ PING
☐ FMG-Access ☒ SSH ☒ SNMP
☒ TELNET ☐ FTM ☐ RADIUS Accounting
☐ Security Fabric Connection

IPv6 ☐ HTTPS ☐ HTTP ☐ PING
☐ FMG-Access ☐ SSH ☐ SNMP
☐ Security Fabric Connection

Receive LLDP **Use VDOM Setting** Enable Disable

Transmit LLDP **Use VDOM Setting** Enable Disable

☐ DHCP Server

☐ Stateless Address Auto-configuration (SLAAC)

☒ DHCPv6 Server

IPv6 subnet

DNS service Delegated Same as System DNS **Specify**

Stateful server ☒

IP mode **IP Range** Delegated

Address range

2. Configure FortiGate B:

- a. On FortiGate B, go to *Network > Interfaces*.
- b. Edit the server interface.
- c. Set *IPv6 addressing mode* to *DHCP*. FortiGate B obtains and populates the interface address information from FortiGate A.

Edit Interface

Name port33

Alias

Type Physical Interface

VRF ID 0

Virtual domain vdom1

Role Undefined

Address

Addressing mode **Manual** **DHCP** Auto-managed by FortiIPAM PPPoE

IP/Netmask

IPv6 addressing mode **Manual** **DHCP** Delegated

Status Connected

Obtained IP/Netmask

Expiry Date

Acquired DNS

DHCPv6 prefix delegation ☐

Configuring a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server

In this scenario, a DHCPv6 server is connected to a FortiGate via an upstream interface. In this example, port1 is the upstream interface. This scenario configures a delegate interface (port2 in this example) to obtain the IPv6 prefix from the upstream interface.

To configure a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server:

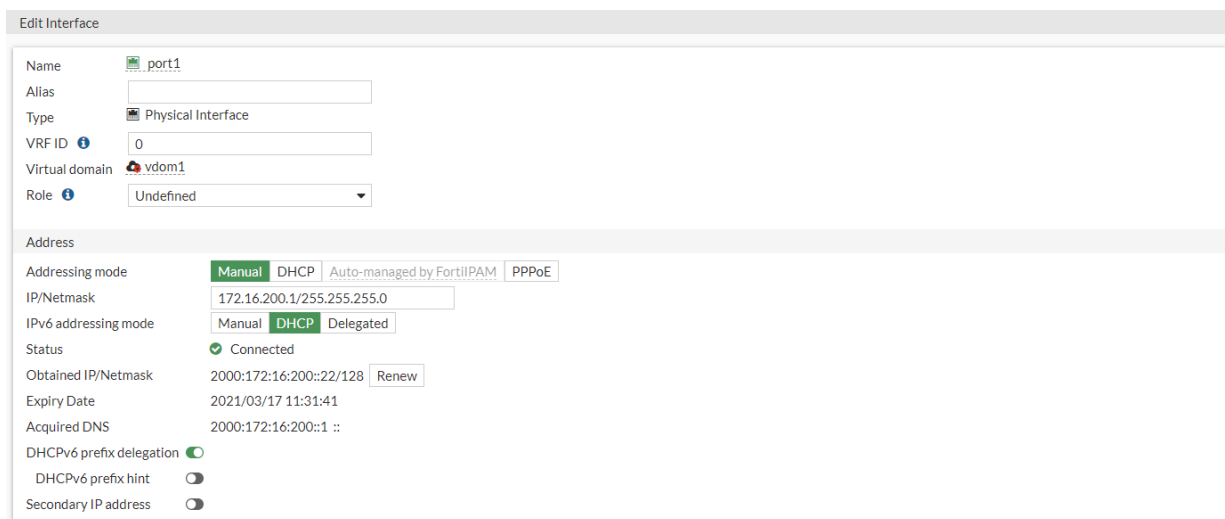
1. Go to *Network > Interfaces*.
2. Edit port1.
3. Enable *DHCPv6 prefix delegation*.
4. Click *OK*.
5. Edit port2.
6. Set *IPv6 addressing mode* to *Delegated*. The interface obtains the IPv6 prefix from the upstream DHCPv6 server and forms its IPv6 address using the subnet configured on the interface.

Configuring a downstream FortiGate to obtain the IPv6 prefix and DNS from an upstream DHCPv6 server

In this scenario, a DHCPv6 server is connected to FortiGate A via an upstream interface. In this example, port1 is the upstream interface. FortiGate A is connected to FortiGate B via a downstream interface (port2 in this example).

To configure a downstream FortiGate to obtain the IPv6 prefix and DNS from an upstream DHCPv6 server:

1. Configure the upstream interface:
 - a. On FortiGate A, go to *Network > Interfaces*.
 - b. Edit port1.
 - c. For *IPv6 addressing mode*, select *DHCP*.
 - d. Enable *DHCPv6 prefix delegation*.
 - e. Click *OK*.



Edit Interface

Name port1

Alias

Type Physical Interface

VRF ID 0

Virtual domain vdom1

Role Undefined

Address

Addressing mode Manual DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask 172.16.200.1/255.255.255.0

IPv6 addressing mode Manual DHCP Delegated

Status Connected

Obtained IP/Netmask 2000::172:16:200::22/128 Renew

Expiry Date 2021/03/17 11:31:41

Acquired DNS 2000::172:16:200::1 ::

DHCPv6 prefix delegation

DHCPv6 prefix hint

Secondary IP address

2. Configure the downstream interface:
 - a. On FortiGate A, edit port2.
 - b. Enable *DHCPv6 Server*.
 - c. Set *DNS service* and *IP mode* to *Delegated*.
 - d. Enable *Stateful server*.
 - e. From the *Upstream interface* dropdown list, select port1.
 - f. Click OK.

Edit Interface

Name: port2
 Alias:
 Type: Physical Interface
 VRF ID: 0
 Virtual domain: vdom1
 Role: Undefined

Address

Addressing mode: Manual | DHCP | Auto-managed by FortiPAM | PPPoE
 IP/Netmask: 10.1.100.1/255.255.255.0
 IPv6 addressing mode: Manual | DHCP | Delegated
 IPv6 Address/Prefix: 2000:10:1:100::1/64
 Auto configure IPv6 address: ☐
 DHCPv6 prefix delegation: ☐
 Secondary IP address: ☐

Administrative Access

IPv4: ☒ HTTPS, ☐ FMG-Access, ☒ TELNET, ☐ Security Fabric Connection, ☒ HTTP, ☒ SSH, ☐ FTM, ☒ PING, ☒ SNMP, ☐ RADIUS Accounting

IPv6: ☒ HTTPS, ☐ FMG-Access, ☒ TELNET, ☐ Security Fabric Connection, ☒ HTTP, ☒ SSH, ☐ Security Fabric Connection, ☒ PING, ☒ SNMP

Receive LLDP: Use VDOM Setting | Enable | Disable
 Transmit LLDP: Use VDOM Setting | Enable | Disable

☐ DHCP Server

☐ Stateless Address Auto-configuration (SLAAC)

☒ DHCPv6 Server

IPv6 subnet: 0:0:0:100::/64
 DNS service: Delegated | Same as System DNS | Specify
 Stateful server: ☒
 IP mode: IP Range | Delegated
 Upstream interface: port1

3. Configure the FortiGate B interface:
 - a. On FortiGate B, go to *Network > Interfaces*.
 - b. Edit the desired interface.

- c. Set IPv6 addressing mode to DHCP. FortiGate B obtains the IPv6 prefix and DNS from the DHCPv6 server.

FortiGate as an IPv6 DDNS client for generic DDNS

When configuring the generic DDNS service provider as a DDNS server, the server type and address type can be set to IPv6. This allows the FortiGate to connect to an IPv6 DDNS server and provide the FortiGate's IPv6 interface address for updates.

```
config system ddns
  edit <name>
    set ddns-server genericDDNS
    set server-type {ipv4 | ipv6}
    set ddns-server-addr <address>
    set addr-type ipv6 {ipv4 | ipv6}
    set monitor-interface <port>
  next
end
```

To configure an IPv6 DDNS client with generic DDNS:

```
config system ddns
  edit 1
    set ddns-server genericDDNS
    set server-type ipv6
    set ddns-server-addr "2004:16:16:16::2" "16.16.16.2" "ddns.genericddns.com"
    set ddns-domain "test.com"
    set addr-type ipv6
    set monitor-interface "port3"
  next
end
```

FortiGate as an IPv6 DDNS client for FortiGuard DDNS

When configuring the FortiGuard DDNS service as a DDNS server, the server type and address type can be set to IPv6. This allows the FortiGate to connect to FortiGuard over IPv6 and provide the FortiGate's IPv6 interface address for updates.

```
config system ddns
  edit <name>
    set ddns-server FortiGuardDDNS
    set server-type {ipv4 | ipv6}
    set ddns-domain <name>.fortiddns.com
    set addr-type ipv6 {ipv4 | ipv6}
    set monitor-interface <port>
  next
end
```

To configure an IPv6 DDNS client with FortiGuard DDNS:

```
config system ddns
  edit 1
    set ddns-server FortiGuardDDNS
    set server-type ipv6
    set ddns-domain "fgtatest001.fortiddns.com"
    set addr-type ipv6
    set monitor-interface "port1"
  next
end
```

Allow backup and restore commands to use IPv6 addresses

IPv6 is supported in the `execute backup` and `execute restore` commands to TFTP and FTP servers.

To back up a configuration file to an IPv6 TFTP server:

```
# execute backup config tftp fgta.conf 2000:172:16:200::55
Please wait...
Connect to tftp server 2000:172:16:200::55 ...
```

Send config file to tftp server OK.

To restore a configuration file from an IPv6 TFTP server:

```
# execute restore config tftp fgta.conf 2000:172:16:200::55
This operation will overwrite the current setting and could possibly reboot the system!
Do you want to continue? (y/n)y
```

```
Please wait...
Connect to TFTP server 2000:172:16:200::55 ...
```

```
Get file from TFTP server OK.
File check OK.
The system is going down NOW !!
```

To back up a configuration file to an IPv6 FTP server:

```
# execute backup config ftp fgta.conf 2000:172:16:200::55 root xxxxxxxxxxxx
Please wait...
```

```
Connect to ftp server 2000:172:16:200::55 ...
Send config file to ftp server OK.
```

To restore a configuration file from an IPv6 FTP server:

```
# execute restore config ftp fgta.conf 2000:172:16:200::55 root xxxxxxxxxx
This operation will overwrite the current setting and could possibly reboot the system!
Do you want to continue? (y/n)y
```

```
Please wait...
Connect to ftp server 2000:172:16:200::55 ...
```

```
Get config file from ftp server OK.
File check OK.
The system is going down NOW !!
```

VRF support for IPv6 - 7.0.1

IPv6 routes now support VRF. Static, connected, OSPF, and BGP routes can be isolated in different VRFs. BGP IPv6 routes can be leaked from one VRF to another.

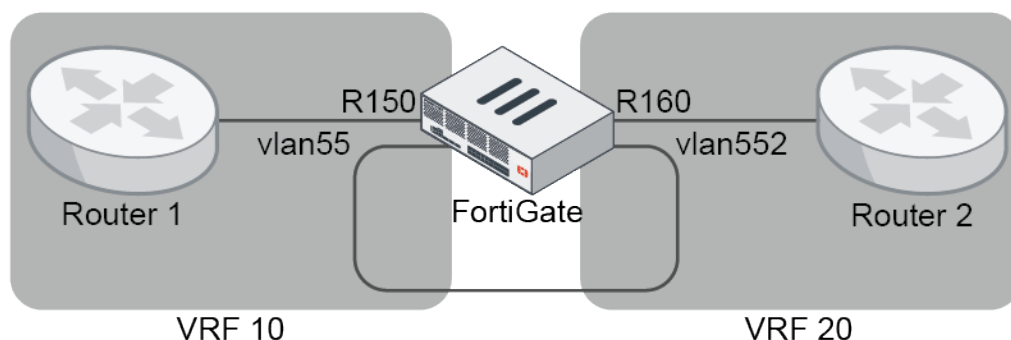
```
config router bgp
  config vrf-leak6
    edit <origin vrf id>
      config target
        edit <target vrf id>
          set route-map <route-map>
          set interface <interface>
        next
      end
    next
  end
end
```

The origin or target VRF ID is an integer value from 0 - 31.

```
config router static6
  edit <id>
    set vrf <vrf id>
  next
end
```

Using a VRF leak on BGP

In this example, the route 2000:5:5:5::/64 learned from Router 1 is leaked to VRF 20 through the interface vlan552. Conversely, the route 2009:3:3:3::/64 learned from Router 2 is leaked to VRF 10 through interface vlan55.



To configure VRF leaking in BGP:

1. Configure the BGP neighbors:

```
config router bgp
  set as 65412
  config neighbor
    edit "2000:10:100:1::1"
      set activate disable
      set remote-as 20
      set update-source "R150"
    next
    edit "2000:10:100:1::5"
      set activate disable
      set soft-reconfiguration enable
      set interface "R160"
      set remote-as 20
    next
  end
end
```

2. Configure the VLAN interfaces:

```
config system interface
  edit "vlan55"
    set vdom "root"
    set vrf 10
    set ip 55.1.1.1 255.255.255.0
    set device-identification enable
    set role lan
    set snmp-index 51
    config ipv6
      set ip6-address 2000:55::1/64
    end
    set interface "npu0_vlink0"
    set vlanid 55
  next
  edit "vlan552"
    set vdom "root"
    set vrf 20
    set ip 55.1.1.2 255.255.255.0
    set device-identification enable
    set role lan
    set snmp-index 53
  end
end
```

```
        config ipv6
            set ip6-address 2000:55::2/64
        end
        set interface "npu0_vlink1"
        set vlanid 55
    next
end
```

3. Configure the IPv6 prefixes:

```
config router prefix-list6
    edit "1"
        config rule
            edit 1
                set prefix6 2000:5:5:5::/64
                unset ge
                unset le
            next
        end
    next
    edit "2"
        config rule
            edit 1
                set prefix6 2009:3:3:3::/64
                unset ge
                unset le
            next
        end
    next
end
```

4. Configure the route maps:

```
config router route-map
    edit "from106"
        config rule
            edit 1
                set match-ip6-address "1"
            next
        end
    next
    edit "from206"
        config rule
            edit 1
                set match-ip6-address "2"
            next
        end
    next
end
```

5. Configure the IPv6 route leaking (leak route 2000:5:5:5::/64 learned from Router 1 to VRF 20, then leak route 2009:3:3:3::/64 learned from Router 2 to VRF 10):

```
config router bgp
    config vrf-leak6
        edit "10"
            config target
                edit "20"
```

```

        set route-map "from106"
        set interface "vlan55"
    next
end
next
edit "20"
    config target
        edit "10"
            set route-map "from206"
            set interface "vlan552"
        next
    end
next
end
end
end

```

To verify the VRF leaking:

1. Check the routing table before the leak:

```

# get router info6 routing-table bgp
Routing table for VRF=10
B      2000:5:5:5::/64 [20/0] via fe00::2000:0000:0000:00, R150, 00:19:45

Routing table for VRF=20
B      2008:3:3:3::/64 [20/0] via fe00::3000:0000:0000:00, R160, 00:18:49
B      2009:3:3:3::/64 [20/0] via fe00::3000:0000:0000:00, R160, 00:18:49

```

2. Check the routing table after the leak:

```

# get router info6 routing-table bgp
Routing table for VRF=10
B      2000:5:5:5::/64 [20/0] via fe00::2000:0000:0000:0, R150, 00:25:45
B      2009:3:3:3::/64 [20/0] via fe80::10:0000:0000:4245, vlan55, 00:00:17

Routing table for VRF=20
B      2000:5:5:5::/64 [20/0] via fe80::10:0000:0000:4244, vlan552, 00:00:16
B      2008:3:3:3::/64 [20/0] via fe00::3000:0000:0000:00, R160, 00:24:49
B      2009:3:3:3::/64 [20/0] via fe00::3000:0000:0000:00, R160, 00:24:49

```

Using VRF on a static route

In this example, a VRF is defined on static route 22 so that it will only appear in the VRF 20 routing table.

To configure the VRF on the static route:

```

config router static6
    edit 22
        set dst 2010:2:2:2::/64
        set blackhole enable
        set vrf 20
    next
end

```

IPv6 tunnel inherits MTU based on physical interface - 7.0.2

The MTU of an IPv6 tunnel interface is calculated from the MTU of its parent interface minus headers.

Example



In this topology, FortiGate B and FortiGate D are connected over an IPv6 network. An IPv6 tunnel is formed, and IPv4 can be used over the IPv6 tunnel. The tunnel interface MTU is based on the physical interface MTU minus the IP and TCP headers (40 bytes). On FortiGate B's physical interface port5, the MTU is set to 1320. The IPv6 tunnel is based on port5, and its MTU value of 1280 is automatically calculated from the MTU value of its physical interface minus the header. The same is true for port3 on FortiGate D.

To verify the MTU for the IPv6 tunnel on FortiGate B:

1. Configure port5:

```

config system interface
  edit "port5"
    set vdom "root"
    set type physical
    set snmp-index 7
    config ipv6
      set ip6-address 2000:172:16:202::1/64
      set ip6-allowaccess ping
    end
    set mtu-override enable
    set mtu 1320
  next
end

```

2. Configure the IPv6 tunnel:

```

config system ipv6-tunnel
  edit "B_2_D"
    set source 2000:172:16:202::1
    set destination 2000:172:16:202::2
    set interface "port5"
  next
end

```

3. Configure the tunnel interface:

```

config system interface
  edit "B_2_D"
    set vdom "root"
    set ip 172.16.210.1 255.255.255.255
    set allowaccess ping https http
    set type tunnel
  end
end

```



```

set remote-ip 172.16.210.2 255.255.255.255
set snmp-index 33
config ipv6
    set ip6-address 2000:172:16:210::1/64
    set ip6-allowaccess ping
    config ip6-extra-addr
        edit fe80::2222/10
        next
    end
end
set interface "port5"
next
end

```

4. Verify the interface lists:

```

# diagnose netlink interface list port5
if=port5 family=00 type=1 index=13 mtu=1320 link=0 master=0
ref=68 state=start present fw_flags=0 flags=up broadcast run multicast
Qdisc=mq hw_addr=**:**:**:**:**:** broadcast_addr=**:**:**:**:**
stat: rxp=1577 txp=1744 rxb=188890 txb=203948 rxe=0 txe=0 rxd=0 txd=0 mc=825 collision=0
@ time=1631647112
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=68

# diagnose netlink interface list B_2_D
if=B_2_D family=00 type=769 index=41 mtu=1280 link=0 master=0
ref=25 state=start present fw_flags=0 flags=up p2p run noarp multicast
Qdisc=noqueue local=0.0.0.0 remote=0.0.0.0
stat: rxp=407 txp=417 rxb=66348 txb=65864 rxe=0 txe=61 rxd=0 txd=0 mc=0 collision=60 @
time=1631647126
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=25

```

To verify the MTU for the IPv6 tunnel on FortiGate D:

1. Configure port3:

```

config system interface
    edit "port3"
        set vdom "root"
        set type physical
        set snmp-index 5
        config ipv6
            set ip6-address 2000:172:16:202::2/64
            set ip6-allowaccess ping
        end
        set mtu-override enable
        set mtu 1320
    next
end

```

2. Configure the IPv6 tunnel:

```
config system ipv6-tunnel
  edit "D_2_B"
    set source 2000:172:16:202::2
    set destination 2000:172:16:202::1
    set interface "port3"
  next
end
```

3. Configure the tunnel interface:

```
config system interface
  edit "D_2_B"
    set vdom "root"
    set ip 172.16.210.2 255.255.255.255
    set allowaccess ping https http
    set type tunnel
    set remote-ip 172.16.210.1 255.255.255.255
    set snmp-index 36
    config ipv6
      set ip6-address 2000:172:16:210::2/64
      set ip6-allowaccess ping
      config ip6-extra-addr
        edit fe80::4424/10
        next
      end
    end
    set interface "port3"
  next
end
```

4. Verify the interface lists:

```
# diagnose netlink interface list port3

# diagnose netlink interface list D_2_B
```

Web proxy

This section includes information about web proxy related new features:

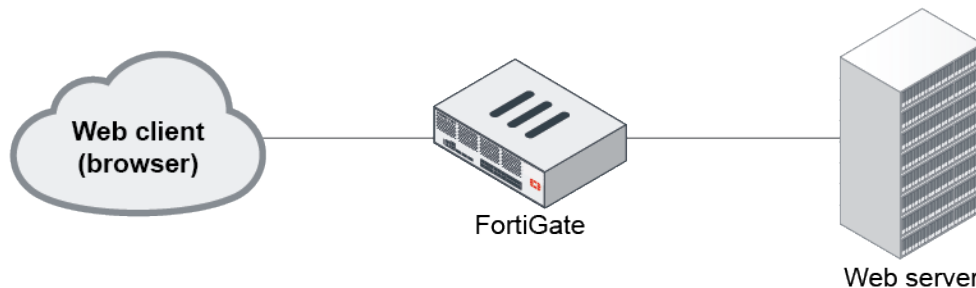
- [Explicit proxy authentication over HTTPS on page 220](#)
- [Selectively forward web requests to a transparent web proxy on page 222](#)
- [mTLS client certificate authentication 7.0.1 on page 225](#)
- [WAN optimization SSL proxy chaining 7.0.1 on page 230](#)

Explicit proxy authentication over HTTPS

When a HTTP request requires authentication in an explicit proxy, the authentication can be redirected to a secure HTTPS captive portal. Once authentication is complete, the client can be redirected back to the original destination over HTTP.

Example

A user visits a website via HTTP through the explicit web proxy on a FortiGate. The user is required to authenticate by either basic or form IP-based authentication for the explicit web proxy service. The user credentials need to be transmitted over the networks in a secured method over HTTPS rather than in plain text. The user credentials are protected by redirecting the client to a captive portal of the FortiGate over HTTPS for authentication where the user credentials are encrypted and transmitted over HTTPS.



In this example, explicit proxy authentication over HTTPS is configured with form IP-based authentication. Once configured, you can enable authorization for an explicit web proxy by configuring users or groups in the firewall proxy policy.

To configure explicit proxy authentication over HTTPS:

1. Configure the authentication settings:

```
config authentication setting
    set captive-portal-type fqdn
    set captive-portal "fgt-cp"
    set auth-https enable
end
```

2. Configure the authentication scheme:

```
config authentication scheme
    edit "form"
        set method form
        set user-database "local-user-db"
    next
end
```

3. Configure the authentication rule:

```
config authentication rule
    edit "form"
        set srcaddr "all"
        set active-auth-method "form"
    next
end
```



If a session-based basic authentication method is used, enable `web-auth-cookie`.

4. Configure the firewall address:

```
config firewall address
  edit "fgt-cp"
    set type fqdn
    set fqdn "fgt.fortinetqa.local"
  next
end
```

5. Configure the interface:

```
config system interface
  edit "port10"
    set ip 10.1.100.1 255.255.255.0
    set explicit-web-proxy enable
    set proxy-captive-portal enable
  next
end
```

6. Configure a firewall proxy policy with users or groups (see [Explicit web proxy](#)).**Verification**

When a client visits a HTTP website, the client will be redirected to the captive portal for authentication by HTTPS. For example, the client could be redirected to a URL by a HTTP 303 message similar to the following:

HTTP/1.1 303 See Other

Connection: close

Content-Type: text/html

Cache-Control: no-cache

Location:

<https://fgt.fortinetqa.local:7831/XX/YY/ZZ/cpauth?scheme=http&Tmthd=0&host=172.16.200.46&port=80&rule=75&uri=Lw==&>

Content-Length: 0

The captive portal URL used for authentication is <https://fgt.fortinetqa.local:7831/...> Once the authentication is complete with all user credentials protected by HTTPS, the client is redirected to the original HTTP website they intended to visit.

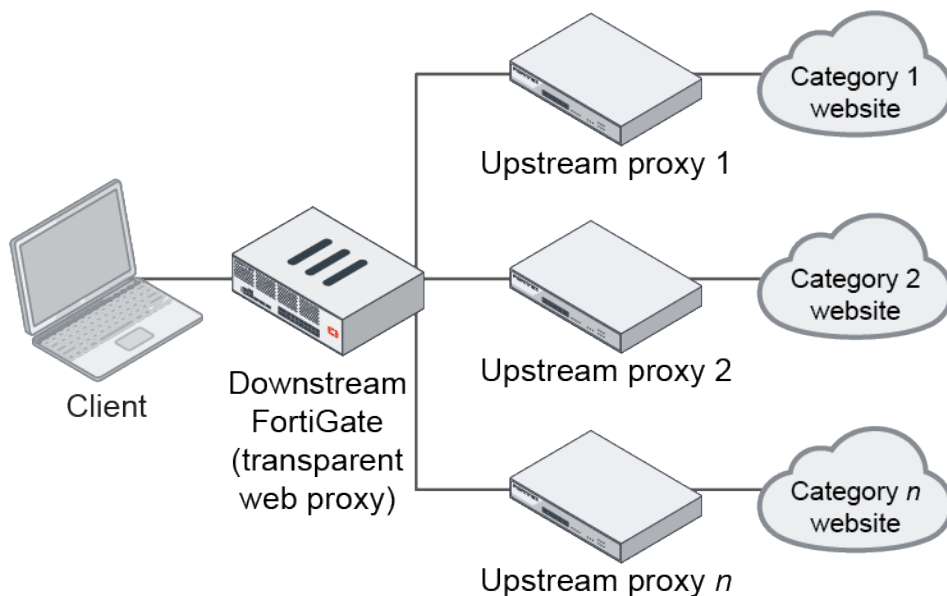
Selectively forward web requests to a transparent web proxy

Web traffic over HTTP/HTTPS can be forwarded selectively by the FortiGate's transparent web proxy to an upstream web proxy to avoid overwhelming the proxy server. Traffic can be selected by specifying the proxy address (`set webproxy-forward-server`), which can be based on a FortiGuard URL category.



The FortiGuard web filter service must be enabled on the downstream FortiGate.

Topology



Forwarding behavior

The forward server will be ignored if the proxy policy matching for a particular session needs the FortiGate to see authentication information inside the HTTP (plain text) message. For example, assume that user authentication is required and a forward server is configured in the transparent web proxy, and the authentication method is an active method (such as basic). When the user or client sends the HTTP request over SSL with authentication information to the FortiGate, the request cannot be forwarded to the upstream proxy. Instead, it will be forwarded directly to the original web server (assuming deep inspection and `http-policy-redirect` are enabled in the firewall policy).

The FortiGate will close the session before the client request can be forwarded if all of the following conditions are met:

- The certificate inspection is configured in the firewall policy that has the `http-policy-redirect` option enabled.
- A previously authenticated IP-based user record cannot be found by the FortiGate's memory during the SSL handshake.
- Proxy policy matching needs the FortiGate to see the HTTP request authentication information.

This means that in order to enable user authentication and use `webproxy-forward-server` in the transparent web proxy policy at the same time, the following best practices should be followed:

- In the firewall policy that has the `http-policy-redirect` option enabled, set `ssl-ssh-profile` to use the `deep-inspection` profile.
- Use IP-based authentication rules; otherwise, the `webproxy-forward-server` setting in the transparent web proxy policy will be ignored.
- Use a passive authentication method such as FSSO. With FSSO, once the user is authenticated as a domain user by a successful login, the web traffic from the user's client will always be forwarded to the upstream proxy as long as the authenticated user remains unexpired. If the authentication method is an active authentication method (such as basic, digest, NTLM, negotiate, form, and so on), the first session containing authentication information will bypass the forward server, but the following sessions will be connected through the upstream proxy.

Sample configuration

On the downstream FortiGate proxy, there are two category proxy addresses used in two separate transparent web proxy policies as the destination address:

- In the policy with `upstream_proxy_1` as the forward server, the proxy address `category_infotech` is used to match URLs in the information technology category.
- In the policy with `upstream_proxy_2` as the forward server, the proxy address `category_social` is used to match URLs in the social media category.

To configure forwarding requests to transparent web proxies:

1. Configure the proxy forward servers:

```
config web-proxy forward-server
  edit "upStream_proxy_1"
    set ip 172.16.200.20
  next
  edit "upStream_proxy_2"
    set ip 172.16.200.46
  next
end
```

2. Configure the web proxy addresses:

```
config firewall proxy-address
  edit "category_infotech"
    set type category
    set host "all"
    set category 52
  next
  edit "category_social"
    set type category
    set host "all"
    set category 37
  next
end
```

3. Configure the firewall policy:

```
config firewall policy
  edit 1
    set srcintf "port10"
    set dstintf "port9"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode proxy
    set http-policy-redirect enable
    set ssl-ssh-profile "deep-inspection"
    set av-profile "av"
    set nat enable
  next
end
```

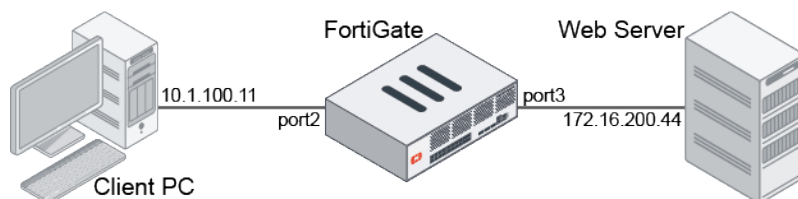
4. Configure the proxy policies:

```
config firewall proxy-policy
  edit 1
    set proxy transparent-web
    set srcintf "port10"
    set dstintf "port9"
    set srcaddr "all"
    set dstaddr "category_infotech"
    set service "webproxy"
    set action accept
    set schedule "always"
    set logtraffic all
    set webproxy-forward-server "upStream_proxy_1"
    set utm-status enable
    set ssl-ssh-profile "deep-inspection"
    set av-profile "av"
  next
  edit 2
    set proxy transparent-web
    set srcintf "port10"
    set dstintf "port9"
    set srcaddr "all"
    set dstaddr "category_social"
    set service "webproxy"
    set action accept
    set schedule "always"
    set logtraffic all
    set webproxy-forward-server "upStream_proxy_2"
    set utm-status enable
    set ssl-ssh-profile "deep-inspection"
    set av-profile "av"
  next
end
```

mTLS client certificate authentication - 7.0.1

FortiGate supports client certificate authentication used in mutual Transport Layer Security (mTLS) communication between a client and server. Clients are issued certificates by the CA, and an access proxy configured on the FortiGate uses the new certificate method in the authentication scheme to identify and approve the certificate provided by the client when they try to connect to the access proxy. The FortiGate can also add the HTTP header X-Forwarded-Client-Cert to forward the certificate information to the server.

Examples



In these examples, the access proxy VIP IP address is 10.1.100.200.

Example 1

In this example, clients are issued unique client certificates from your CA. The FortiGate authenticates the clients by their user certificate before allowing them to connect to the access proxy. The access server acts as a reverse proxy for the web server that is behind the FortiGate.

This example assumes that you have already obtained the public CA certificate from your CA, the root CA of the client certificate has been imported (CA_Cert_1), and the client certificate has been distributed to the endpoints.

To configure the FortiGate:

1. Configure user authentication. Both an authentication scheme and rule must be configured, as the authentication is applied on the access proxy:

```
config authentication scheme
    edit "mtls"
        set method cert
        set user-cert enable
    next
end

config authentication rule
    edit "mtls"
        set srcintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set active-auth-method "mtls"
    next
end
```

2. Select the CA or CAs used to verify the client certificate:

```
config authentication setting
    set user-cert-ca "CA_Cert_1"
end
```

3. Configure the users. Users can be matched based on either the common-name on the certificate or the trusted issuer.

- Verify the user based on the common name on the certificate:

```
config user certificate
    edit "single-certificate"
        set type single-certificate
        set common-name "client.fortinet.com"
    next
end
```

- Verify the user based on the CA issuer:

```
config user certificate
    edit "trusted-issuer"
        set type trusted-issuer
        set issuer "CA_Cert_1"
    next
end
```

4. Configure the access proxy VIP. The SSL certificate is the server certificate that is presented to the user as they connect:


```
config firewall vip
  edit "mTLS"
    set type access-proxy
    set extip 10.1.100.200
    set extintf "port2"
    set server-type https
    set extport 443
    set ssl-certificate "Fortinet_CA_SSL"
  next
end
```

5. Configure the access proxy policy, including the real server to be mapped. To request the client certificate for authentication, `client-cert` is enabled:

```
config firewall access-proxy
  edit "mTLS-access-proxy"
    set vip "mTLS"
    set client-cert enable
    set empty-cert-action accept
    config api-gateway
      edit 1
        config realservers
          edit 1
            set ip 172.16.200.44
          next
        end
      next
    end
  next
end
```

6. Configure the firewall policy to allow the client to connect to the access proxy:

```
config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "any"
    set action accept
    set srcaddr "all"
    set dstaddr "mTLS"
    set schedule "always"
    set service "ALL"
    set inspection-mode proxy
    set logtraffic all
    set nat enable
  next
end
```

7. Configure the proxy policy to apply authentication and the security profile, selecting the appropriate user object depending on the user type:

```
config firewall proxy-policy
  edit 3
    set proxy access-proxy
    set access-proxy "mTLS-access-proxy"
    set srcintf "port2"
    set srcaddr "all"
    set dstaddr "all"
```

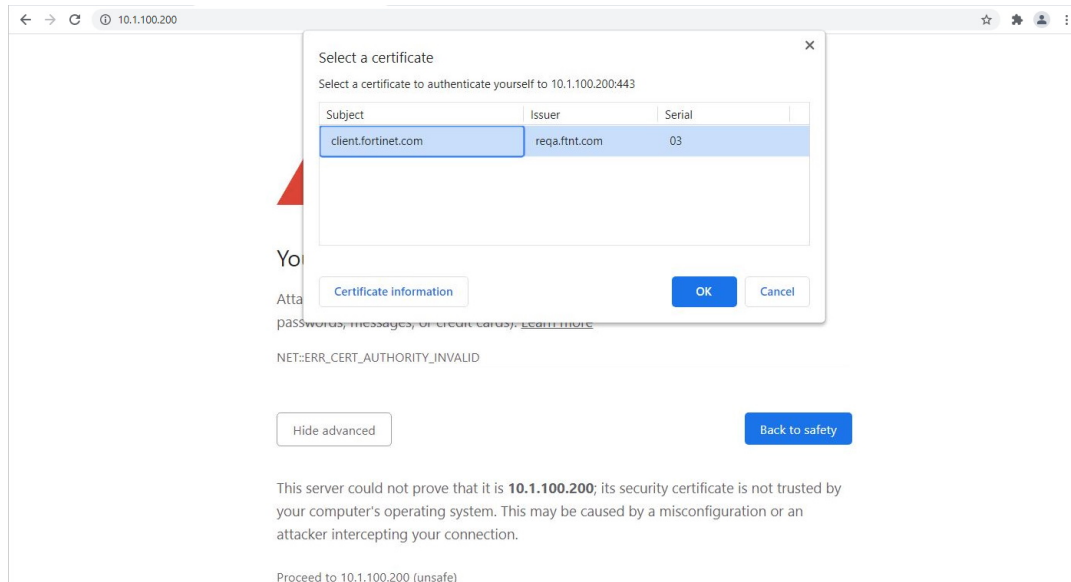
```

set action accept
set schedule "always"
set users {"single-certificate" | "trusted-issuer"}
set utm-status enable
set ssl-ssh-profile "deep-inspection-clone"
set av-profile "av"
next
end

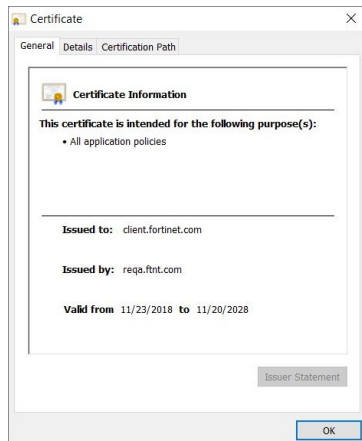
```

To verify the results:

1. In a web browser, access the VIP address. This example uses Chrome.
2. When prompted, select the client certificate, then click **OK**.



3. Click **Certificate information** to view details about the certificate.



4. On the FortiGate, check the traffic logs.
 - If client certificate authentication passes:

```

1: date=2021-06-03 time=15:48:36 eventtime=1622760516866635697 tz="-0700"
logid="0000000010" type="traffic" subtype="forward" level="notice" vd="vdom1"

```

```
srcip=10.1.100.11 srcport=45532 srcintf="port2" srcintfrole="undefined"
dstcountry="Reserved" srccountry="Reserved" dstip=172.16.200.44 dstport=443
dstintf="vdom1" dstintfrole="undefined" sessionid=154900 service="HTTPS"
wanoptapptype="web-proxy" proto=6 action="accept" policyid=3 policytype="proxy-
policy" poluuid="af5e2df2-c321-51eb-7d5d-42fa58868dcb" duration=0 user="single-
certificate" wanin=2550 rcvdbyte=2550 wanout=627 lanin=4113 sentbyte=4113 lanout=2310
appcat="unscanned"
```

- If the CA issuer is used to verify the client:

```
1: date=2021-06-03 time=15:43:02 eventtime=1622760182384776037 tz="-0700"
logid="0000000010" type="traffic" subtype="forward" level="notice" vd="vdom1"
srcip=10.1.100.11 srcport=45514 srcintf="port2" srcintfrole="undefined"
dstcountry="Reserved" srccountry="Reserved" dstip=10.1.100.200 dstport=443
dstintf="vdom1" dstintfrole="undefined" sessionid=153884 service="HTTPS"
wanoptapptype="web-proxy" proto=6 action="accept" policyid=3 policytype="proxy-
policy" poluuid="af5e2df2-c321-51eb-7d5d-42fa58868dcb" duration=0 user="trusted-
issuer" wanin=0 rcvdbyte=0 wanout=0 lanin=4089 sentbyte=4089 lanout=7517
appcat="unscanned" utmaction="block" countweb=1 crscore=30 craction=8 utmref=65535-0
```

- If the client certificate authentication fails, and the traffic is blocked:

```
1: date=2021-06-03 time=15:45:53 eventtime=1622760353789703671 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1"
srcip=10.1.100.11 srcport=45518 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.44 dstport=443 dstintf="vdom1" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=154431 proto=6 action="deny"
policyid=0 policytype="proxy-policy" user="single-certificate" service="HTTPS"
trandisp="noop" url="https://10.1.100.200/" agent="curl/7.68.0" duration=0 sentbyte=0
rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" crscore=30 craction=131072
crlevel="high" msg="Traffic denied because of explicit proxy policy"
```

Example 2

In this example, the same configuration as in [Example 1](#) is used, with a web proxy profile added to enable adding the client certificate to the HTTP header X-Forwarded-Client-Cert. The header is then forwarded to the server.

To configure the FortiGate:

1. Repeat steps 1 to 6 of [Example 1](#), using the common name on the certificate to verify the user.
2. Configure a web proxy profile that adds the HTTP x-forwarded-client-cert header in forwarded requests:

```
config web-proxy profile
  edit "mtls"
    set header-x-forwarded-client-cert add
  next
end
```

3. Configure the proxy policy to apply authentication, the security profile, and web proxy profile:

```
config firewall proxy-policy
  edit 3
    set uuid af5e2df2-c321-51eb-7d5d-42fa58868dcb
    set proxy access-proxy
    set access-proxy "mTLS-access-proxy"
    set srcintf "port2"
    set srcaddr "all"
```

```

        set dstaddr "all"
        set action accept
        set schedule "always"
        set logtraffic all
        set users "single-certificate"
        set webproxy-profile "mtls"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection-clone"
        set av-profile "av"
    next
end

```

To verify the results:

The WAD debug shows that the FortiGate adds the client certificate information to the HTTP header. The added header cannot be checked using the sniffer, because the FortiGate encrypts the HTTP header to forward it to the server.

1. Enable WAD debug on all categories:

```
# diagnose wad debug enable category all
```

2. Set the WAD debug level to verbose:

```
# diagnose wad debug enable level verbose
```

3. Enable debug output:

```
# diagnose debug enable
```

4. Check the debug output.

- When the FortiGate receives the client HTTP request:

```

[0x7fc8d4bc4910] Received request from client: 10.1.100.11:45544

GET / HTTP/1.1
Host: 10.1.100.200
User-Agent: curl/7.68.0
Accept: */*

```

- When the FortiGate adds the client certificate in to the HTTP header and forwards the client HTTP request:

```

[0x7fc8d4bc4910] Forward request to server:
GET / HTTP/1.1
Host: 172.16.200.44
User-Agent: curl/7.68.0
Accept: */*
X-Forwarded-Client-Cert: -----BEGIN CERTIFICATE-----
MIIFXzCCA0egAwI...aCFHDHlR+wb39s=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFpTCCA42gAwI...OtDtetkNoFLbvb
-----END CERTIFICATE-----

```

WAN optimization SSL proxy chaining - 7.0.1

An SSL server does not need to be defined for WAN optimization (WANOpt) SSL traffic offloading (traffic acceleration). The server side FortiGate uses an SSL profile to resign the HTTP server's certificate, both with and without an external

proxy, without an SSL server configured. GCM and ChaCha ciphers can also be used in the SSL connection.

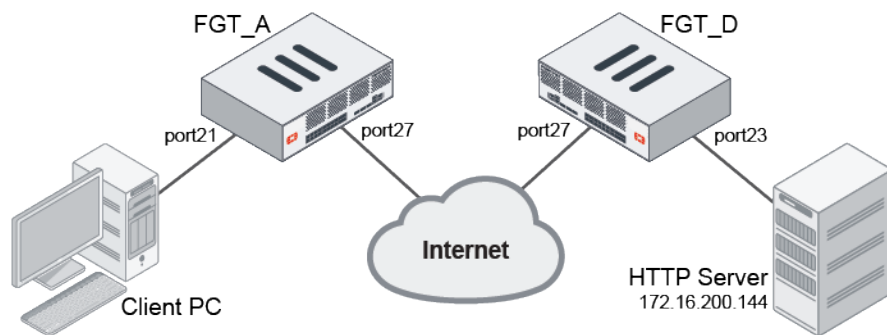
Examples

In these examples, HTTPS traffic is accelerated without configuring an SSL server, including with a proxy in between, and when the GCM or ChaCha ciphers are used.

Example 1

In this example, the server certificate is resigned by the server side FortiGate, and HTTPS traffic is accelerated without configuring an SSL server.

HTTPS traffic with the GCM or ChaCha cipher can pass through WANOpt tunnel.



To configure FGT_A:

1. Configure the hard disk to perform WANOpt:

```

config system storage
  edit "HDD2"
    set status enable
    set usage wanopt
    set wanopt-mode mix
  next
end

```

2. Configure the WANOpt peer and profile:

```

config wanopt peer
  edit "FGT-D"
    set ip 120.120.120.172
  next
end

config wanopt profile
  edit "test"
    config http
      set status enable
      set ssl enable
    end
  next
end

```

3. Create an SSL profile with deep inspection on HTTPS port 443:

```
config firewall ssl-ssh-profile
  edit "ssl"
    config https
      set ports 443
      set status deep-inspection
    end
  next
end
```

4. Configure a firewall policy in proxy mode with WANOpt enabled and the WANOpt profile selected:

```
config firewall policy
  edit 1
    set name "WANOPT-A"
    set srcintf "port21"
    set dstintf "port27"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode proxy
    set profile-protocol-options "protocol"
    set ssl-ssh-profile "ssl"
    set wanopt enable
    set wanopt-profile "test"
    set nat enable
  next
end
```

To configure FGT_D:

1. Configure the hard disk to perform WANOpt:

```
config system storage
  edit "HDD2"
    set status enable
    set usage wanopt
    set wanopt-mode mix
  next
end
```

2. Configure the WANOpt peer:

```
config wanopt peer
  edit "FGT-A"
    set ip 110.110.110.171
  next
end
```

3. Create an SSL profile with deep inspection on HTTPS port 443. The default *Fortinet_CA_SSL* certificate is used to resign the server certificate:

```
config firewall ssl-ssh-profile
  edit "ssl"
    config https
      set ports 443
```

```

        set status deep-inspection
    end
next
end

```

4. Configure a firewall policy in proxy mode with WANOpt enabled and passive WANOpt detection:

```

config firewall policy
    edit 1
        set name "WANOPT-B"
        set srcintf "port27"
        set dstintf "port23"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set wanopt enable
        set wanopt-detection passive
        set nat enable
    next
end

```

5. Configure a proxy policy to apply the SSL profile:

```

config firewall proxy-policy
    edit 100
        set proxy wanopt
        set dstintf "port23"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set action accept
        set schedule "always"
        set utm-status enable
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "ssl"
    next
end

```

To confirm that traffic is accelerated:

1. On the client PC, curl a 10MB test sample for the first time:

```

root@client:/tmp# curl -k https://172.16.200.144/test_10M.pdf -O
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 9865k  100 9865k    0     0   663k      0  0:00:14  0:00:15 --:--:-- 1526k

```

It takes 15 seconds to finish the download.

2. On FGT_A, check the WAD statistics:

```

# diagnose wad stats worker.tunnel
comp.n_in_raw_bytes      10155840
comp.n_in_comp_bytes     4548728

```

```

comp.n_out_raw_bytes      29624
comp.n_out_comp_bytes     31623

# diagnose wad stats worker.protos.http
wan.bytes_in              0
wan.bytes_out             0
lan.bytes_in              760
lan.bytes_out             10140606
tunnel.bytes_in           4548728
tunnel.bytes_out          31623

```

3. Curl the same test sample a second time:

```

root@client:/tmp# curl -k https://172.16.200.144/test_10M.pdf -O
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 9865k  100 9865k    0      0   663k      0  0:00:01  0:00:01 --:--:-- 1526k

```

It now takes less than one second to finish the download.

4. On FGT_A, check the WAD statistics again:

```

# diagnose wad stats worker.tunnel
comp.n_in_raw_bytes      10181157
comp.n_in_comp_bytes     4570331
comp.n_out_raw_bytes     31627
comp.n_out_comp_bytes    34702

# diagnose wad stats worker.protos.http
wan.bytes_in              0
wan.bytes_out             0
lan.bytes_in             1607
lan.bytes_out           20286841
tunnel.bytes_in          4570331
tunnel.bytes_out         34702

```

The tunnel bytes are mostly unchanged, but the LAN bytes are doubled. This means that the bytes of the second curl come from the cache, showing that the traffic is accelerated.

To confirm that a curl using the GCM cipher is accepted and accelerated:

1. On the client PC, curl a 10MB test sample with the GCM cipher:

```

root@client:/tmp# curl -v -k --ciphers DHE-RSA-AES128-GCM-SHA256
https://172.16.200.144/test_10M.pdf -O
* Trying 172.16.200.144...
* TCP_NODELAY set
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
  0    0    0    0    0    0      0      0  --:--:--  --:--:--  --:--:--    0*
Connected to 172.16.200.144 (172.16.200.144) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* Cipher selection: DHE-RSA-AES128-GCM-SHA256
* successfully set certificate verify locations:
*  CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
} [5 bytes data]
* TLSv1.3 (OUT), TLS handshake, Client hello (1):

```



```

} [512 bytes data]
* TLSv1.3 (IN), TLS handshake, Server hello (2):
{ [100 bytes data]
* TLSv1.2 (IN), TLS handshake, Certificate (11):
{ [1920 bytes data]
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
{ [783 bytes data]
* TLSv1.2 (IN), TLS handshake, Server finished (14):
{ [4 bytes data]
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
} [262 bytes data]
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
} [1 bytes data]
* TLSv1.2 (OUT), TLS handshake, Finished (20):
} [16 bytes data]
* TLSv1.2 (IN), TLS handshake, Finished (20):
{ [16 bytes data]
* SSL connection using TLSv1.2 / DHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: CN=ubuntu
*  start date: Sep 20 21:38:01 2018 GMT
*  expire date: Sep 17 21:38:01 2028 GMT
*  issuer: C=US; ST=California; L=Sunnyvale; O=Fortinet; OU=Certificate Authority;
CN=Fortinet Untrusted CA; emailAddress=support@fortinet.com
*  SSL certificate verify result: self signed certificate in certificate chain (19),
continuing anyway.
} [5 bytes data]
> GET /test_10M.pdf HTTP/1.1
> Host: 172.16.200.144
> User-Agent: curl/7.64.1
> Accept: */*
>
{ [5 bytes data]
< HTTP/1.1 200 OK
< Date: Sat, 12 Jun 2021 00:31:08 GMT
< Server: Apache/2.4.37 (Ubuntu)
< Upgrade: h2,h2c
< Connection: Upgrade
< Last-Modified: Fri, 29 Jan 2021 20:10:25 GMT
< ETag: "9a2572-5ba0f98404aa5"
< Accept-Ranges: bytes
< Content-Length: 10102130
< Content-Type: application/pdf
<
{ [5 bytes data]
100 9865k 100 9865k 0 0 16.7M 0 --:--:-- --:--:-- --:--:-- 16.8M
* Connection #0 to host 172.16.200.144 left intact
* Closing connection 0

```

To confirm that a curl using the ChaCha cipher is accepted and accelerated:

1. On the client PC, curl a 10MB test sample with the ChaCha cipher:

```

root@client:/tmp# curl -v -k --ciphers ECDHE-RSA-CHACHA20-POLY1305
https://172.16.200.144/test.doc -O

```

```

* Trying 172.16.200.144...
* TCP_NODELAY set
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
  0      0    0     0    0     0      0      0  --:--:-- --:--:-- --:--:--    0*
Connected to 172.16.200.144 (172.16.200.144) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* Cipher selection: ECDHE-RSA-CHACHA20-POLY1305
* successfully set certificate verify locations:
*  CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
} [5 bytes data]
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
} [512 bytes data]
* TLSv1.3 (IN), TLS handshake, Server hello (2):
{ [100 bytes data]
* TLSv1.2 (IN), TLS handshake, Certificate (11):
{ [1920 bytes data]
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
{ [300 bytes data]
* TLSv1.2 (IN), TLS handshake, Server finished (14):
{ [4 bytes data]
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
} [37 bytes data]
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
} [1 bytes data]
* TLSv1.2 (OUT), TLS handshake, Finished (20):
} [16 bytes data]
* TLSv1.2 (IN), TLS handshake, Finished (20):
{ [16 bytes data]
* SSL connection using TLSv1.2 / ECDHE-RSA-CHACHA20-POLY1305
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: CN=ubuntu
*  start date: Sep 20 21:38:01 2018 GMT
*  expire date: Sep 17 21:38:01 2028 GMT
*  issuer: C=US; ST=California; L=Sunnyvale; O=Fortinet; OU=Certificate Authority;
CN=Fortinet Untrusted CA; emailAddress=support@fortinet.com
*  SSL certificate verify result: self signed certificate in certificate chain (19),
continuing anyway.
} [5 bytes data]
> GET /test.doc HTTP/1.1
> Host: 172.16.200.144
> User-Agent: curl/7.64.1
> Accept: */*
>
{ [5 bytes data]
< HTTP/1.1 200 OK
< Date: Sat, 12 Jun 2021 00:32:11 GMT
< Server: Apache/2.4.37 (Ubuntu)
< Upgrade: h2,h2c
< Connection: Upgrade
< Last-Modified: Wed, 05 May 2021 21:59:49 GMT
< ETag: "4c00-5c19c504b63f4"
< Accept-Ranges: bytes

```

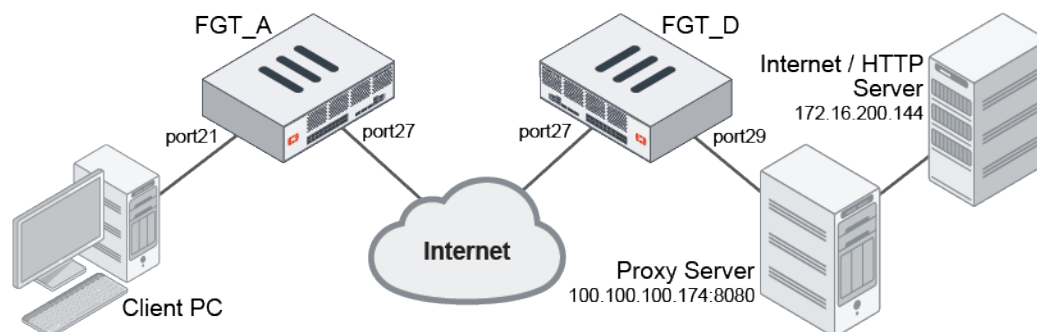
```

< Content-Length: 19456
< Content-Type: application/msword
<
{ [5 bytes data]
100 19456 100 19456 0 0 137k 0 --:--:-- --:--:-- --:--:-- 138k
* Connection #0 to host 172.16.200.144 left intact
* Closing connection 0

```

Example 2

In this example, an external proxy is added to the configuration in [Example 1](#).



To reconfigure FGT_A:

```

config firewall profile-protocol-options
  edit "protocol"
    config http
      set ports 80 8080
      unset options
      unset post-lang
    end
  next
end

```

To reconfigure FGT_D:

1. Configure a new firewall policy for traffic passing from port27 to port29:

```

config firewall policy
  edit 1
    set name "WANOPT-B"
    set srcintf "port27"
    set dstintf "port29"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode proxy
    set wanopt enable
    set wanopt-detection passive
    set nat enable

```

```
    next
end
```

2. Configure a proxy policy for traffic on destination interface port29:

```
config firewall proxy-policy
    edit 100
        set proxy wanopt
        set dstintf "port29"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set action accept
        set schedule "always"
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "ssl"
    next
end
```

To confirm that HTTPS traffic is still being accelerated:

1. On the client PC, curl the same 10MB test sample through the explicit proxy:

```
root@client:/tmp# curl -x 100.100.100.174:8080 -v -k https://172.16.200.144/test_10M.pdf
-O
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100 9865k  100 9865k    0     0  663k      0  0:00:01  0:00:01 --:--:-- 1526k
```

It takes less than a second to finish the download.

System

This section includes information about system related new features:

- [General on page 239](#)
- [High availability on page 261](#)
- [FortiGuard on page 278](#)

General

This section includes information about general system related new features:

- [Allow administrators to define password policy with minimum character change on page 239](#)
- [Enhance host protection engine on page 241](#)
- [ACME certificate support on page 242](#)
- [SFTP configuration backup 7.0.1 on page 247](#)
- [Promote FortiCare registration 7.0.1 on page 247](#)
- [Add monitoring API to retrieve LTE modem statistics from 3G and 4G FortiGates 7.0.1 on page 249](#)
- [Add USB support for FortiExplorer Android 7.0.1 on page 251](#)
- [Warnings for unsigned firmware 7.0.2 on page 253](#)
- [Enabling individual ciphers in the SSH administrative access protocol 7.0.2 on page 255](#)
- [ECDSA in SSH administrative access 7.0.2 on page 255](#)
- [Clear multiple sessions with REST API 7.0.2 on page 257](#)
- [Disable weak ciphers in the HTTPS protocol 7.0.2 on page 258](#)
- [Extend dedicated management CPU feature to 1U and desktop models 7.0.2 on page 260](#)

Allow administrators to define password policy with minimum character change

In previous FortiOS versions, password policies were restricted to only enable or disable a minimum of four new characters in new password. Administrators can now set a minimum number of unique characters in the new password that do not exist in the old password. This setting overrides the password reuse option if both are enabled.

To configure the password policy in the GUI:

1. Go to *System > Settings* and navigate to the *Password Policy* section.
2. For *Password scope*, select *Admin*.

3. Enter a value for *Minimum number of new characters*.

The screenshot shows the 'System Settings' page. Under the 'Password Policy' section, the 'Minimum number of new characters' is set to 6. Other settings include 'Password scope' set to 'Admin', 'Minimum length' set to 8, and 'Character requirements' set to 'Off'. The 'Additional Information' section on the right lists various links and security issues.

4. Click *Apply*.

To change an administrator password in the GUI:

1. Go to *System > Administrators* and double-click the *admin* profile.
2. Click *Change Password*.
3. Enter the old and new password. An error appears if there are not enough new characters, and the password rules are displayed:

The screenshot shows the 'Edit Password' dialog box. A yellow warning message states: 'Changing the password of the current administrator account will require you to login again.' Below this, the 'New Password' field is highlighted with a red border, and a red error message reads: 'The password must conform to the system password policy.' The 'Confirm Password' field is also highlighted. The 'Password must conform to the following rules:' section lists 'Minimum length' and 'Minimum number of new characters'.

If the new password matches the policy, there is no error message:

The screenshot shows the 'Edit Password' dialog box. A yellow warning message states: 'Changing the password of the current administrator account will require you to login again.' Below this, the 'New Password' and 'Confirm Password' fields are filled with dots. The 'Password must conform to the following rules:' section lists 'Minimum length' and 'Minimum number of new characters'.

4. Re-enter the new password to confirm it.
5. Click *OK* to save the new password.
6. Click *OK* to save the admin profile settings.

To configure the password policy in the CLI:

```
config system password-policy
    set status enable
    set min-change-characters 6
end
```

To change an administrator password in the CLI:

When the administrator changes the password, an error appears if there are not enough new characters, and the password rules are displayed.

```
config system admin
    edit admin
        set password oldpassword oldpassword
        New password must conform to the password policy enforced on this device:
        minimum-length=8; the new password must have at least 6 unique character(s) which
don't exist in the old password.
        node_check_object fail! for password *
        value parse error before 'oldpassword'
        Command fail. Return code -49
        set password newchangepassword oldpassword
    next
end
```

Enhance host protection engine

The host protection engine (HPE) has been enhanced to add monitoring and logging capabilities when the HPE is triggered. Users can enable or disable HPE monitoring, and configure intervals and multipliers for the frequency when event logs and attack logs are generated. These logs and monitors help administrators analyze the frequency of attack types and fine-tune the desired packet rates in the HPE shaper.

```
config monitoring npu-hpe
    set status {enable | disable}
    set interval <integer>
    set multipliers <m1>, <m2>, ... <m12>
end
```

status {enable disable}	Enable/disable NPU HPE status monitoring.
interval <integer>	Set the NPU HPE status check interval, in seconds (1 - 60, default = 1).
multipliers <m1>, <m2>, ... <m12>	<p>Set the HPE type interval multipliers (12 integers from 1 - 255, default = 4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, 8).</p> <ul style="list-style-type: none"> • m1: interval multiplier for maximum TCP SYN packet type. • m2: interval multiplier for maximum TCP SYN and ACK flags packet type. • m3: interval multiplier for maximum TCP carries SYN FIN or RST flags packet type. • m4: interval multiplier for maximum TCP packet type. • m5: interval multiplier for maximum UDP packet type. • m6: interval multiplier for maximum ICMP packet type. • m7: interval multiplier for maximum SCTP packet type.

- m8: interval multiplier for maximum ESP packet type.
- m9: interval multiplier for maximum fragmented IP packet type.
- m10: interval multiplier for maximum other IP packet types.
- m11: interval multiplier for maximum ARP packet type.
- m12: interval multiplier for maximum L2 other packet types.

An event log is generated after every (interval × multiplier) seconds for any HPE type when drops occur for that HPE type.

An attack log is generated after every (4 × multiplier) number of continuous event logs.

HPE functionality is disabled by default. Users must enable HPE for the related NP6 chips and configure the desired packet rates that would trigger the HPE monitoring (see [config system np6](#) in the FortiOS CLI Reference).

To configure HPE monitoring:

```
config monitoring npu-hpe
    set status enable
    set interval 1
    set multipliers 4 4 4 4 8 8 8 8 8 8 8 8
end
```

Sample logs

```
1: date=2021-01-13 time=16:00:01 eventtime=1610582401563369503 tz="-0800" logid="0100034418"
type="event" subtype="system" level="warning" vd="root" logdesc="NP6 HPE is dropping
packets" msg="NPU HPE module is stop dropping packet types of:udp in NP6_0."

2: date=2021-01-13 time=16:00:00 eventtime=1610582400562601540 tz="-0800" logid="0100034418"
type="event" subtype="system" level="warning" vd="root" logdesc="NP6 HPE is dropping
packets" msg="NPU HPE module is likely dropping packets of one or more of these types:udp
in NP6_0."

3: date=2021-01-13 time=15:59:59 eventtime=1610582399558325686 tz="-0800" logid="0100034419"
type="event" subtype="system" level="critical" vd="root" logdesc="NP6 HPE under a packets
flood" msg="NPU HPE module is likely under attack of:udp in NP6_0."
```

ACME certificate support

The Automated Certificate Management Environment (ACME), as defined in [RFC 8555](#), is used by the public Let's Encrypt certificate authority (<https://letsencrypt.org>) to provide free SSL server certificates. The FortiGate can be configured to use certificates that are managed by Let's Encrypt, and other certificate management services, that use the ACME protocol. The server certificates can be used for secure administrator log in to the FortiGate.

- The FortiGate must have a public IP address and a hostname in DNS (FQDN) that resolves to the public IP address.
- The configured ACME interface must be public facing so that the FortiGate can listen for ACME update requests. It must not have any VIPs, or port forwarding on port 80 (HTTP) or 443 (HTTPS).
- The Subject Alternative Name (SAN) field is automatically filled with the FortiGate DNS hostname. It cannot be edited, wildcards cannot be used, and multiple SANs cannot be added.

This example shows how to import an ACME certificate from Let's Encrypt, and use it for secured remote administrator access to the FortiGate.



To configure certificates in the GUI, go to *System > Feature Visibility* and enable *Certificates*.

To import an ACME certificate in the GUI:

1. Go to *System > Certificates* and click *Import > Local Certificate*.
2. Set *Type* to *Automated*.
3. Set *Certificate name* to an appropriate name for the certificate.
4. Set *Domain* to the public FQDN of the FortiGate.
5. Set *Email* to a valid email address. The email is not used during the enrollment process.
6. Ensure that *ACME service* is set to *Let's Encrypt*.

7. Configure the remaining settings as required, then click *OK*.
8. If this is the first time enrolling a server certificate with Let's Encrypt on this FortiGate, the *Set ACME Interface* pane opens.

Select the interface that the FortiGate communicates with Let's Encrypt on, then click *OK*.

The ACME interface can later be changed in *System > Settings*.

9. The new server certificate is added to the *Local Certificate* list.
Click *View Details* to verify that the FortiGate's FQDN is in the certificate's *Subject: Common Name (CN)*.

The screenshot shows the FortiGate GUI with the 'Remote CA Certificate' list selected. The list includes various certificates, with 'ACME_CA_Cert_1' highlighted. The details panel on the right shows the following information:

Certificate Details	
Subject:	
Common Name (CN)	test.ftntlab.de
Issuer:	
Common Name (CN)	R3
Organization (O)	Let's Encrypt
Country/Region (C)	US
Validity Period:	
Valid From	
Valid To	
Fingerprints:	
MD5 Fingerprint	9A:03:0F:41:29:D7:01:45:04:F3:16:C0:BD:63:A2:DB
Extensions:	
X509v3 Key Usage	Digital Signature, Key Encipherment
X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Basic Constraints	CA:FALSE
X509v3 Subject Key Identifier	00:D7:D9:59:88:6E:98:54:F8:25:D0:5C:33:4D:40:6C:97:D5:DC:8B
X509v3 Authority Key Identifier	keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
Authority Information Access	OCSP - URL:http://r3.o.lencr.org CA Issuers - URL:http://r3.i.lencr.org/

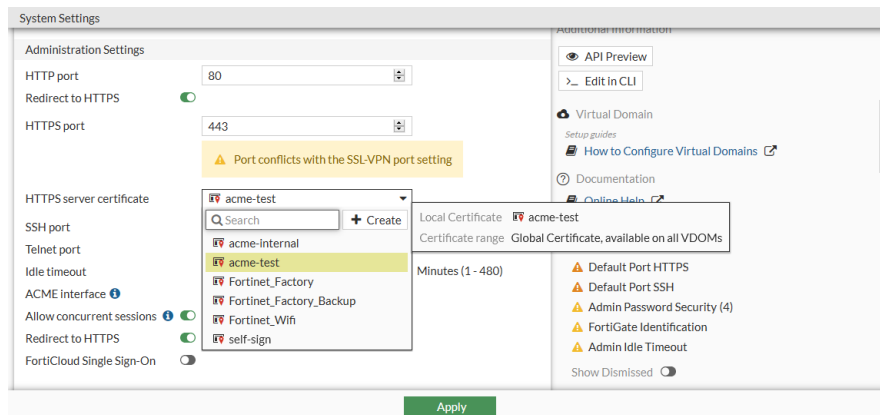
The **Remote CA Certificate** list includes the issuing Let's Encrypt intermediate CA, issued by the public CA ISRG Root X1 from Digital Signature Trust Company.

The screenshot shows the FortiGate GUI with the 'Remote CA Certificate' list selected. The list includes various certificates, with 'ACME_CA_Cert_1' highlighted. The details panel on the right shows the following information:

Certificate Details	
Subject:	
Common Name (CN)	R3
Organization (O)	Let's Encrypt
Country/Region (C)	US
Issuer:	
Common Name (CN)	ISRG Root X1
Organization (O)	Digital Signature Trust Co.
Validity Period:	
Valid From	
Valid To	
Fingerprints:	
MD5 Fingerprint	31:21:28:F5:A0:ED:7B:A5:4B:65:82:92:87:56:BA:83
Extensions:	
X509v3 Key Usage	Digital Signature, Key Encipherment
X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Basic Constraints	CA:FALSE
X509v3 Subject Key Identifier	00:D7:D9:59:88:6E:98:54:F8:25:D0:5C:33:4D:40:6C:97:D5:DC:8B
X509v3 Authority Key Identifier	keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
Authority Information Access	OCSP - URL:http://r3.o.lencr.org CA Issuers - URL:http://r3.i.lencr.org/

To exchange the default FortiGate administration server certificate for the new public Let's Encrypt server certificate in the GUI:

1. Go to *System > Settings*.
2. Set *HTTPS server certificate* to the new certificate.



3. Click *Apply*.
4. Log in to the FortiGate using an administrator account from any internet browser. There should be no warnings related to non-trusted certificates, and the certificate path should be valid.

To import an ACME certificate in the CLI:

1. Set the interface that the FortiGate communicates with Let's Encrypt on:

```
config system acme
    set interface "port1"
end
```

2. Make sure that the FortiGate can contact the Let's Encrypt enrollment server:

```
# execute ping acme-v02.api.letsencrypt.org
PING ca80aladb12a4fbdac5ffcbc944e9a61.pacloudflare.com (172.65.32.248): 56 data bytes
64 bytes from 172.65.32.248: icmp_seq=0 ttl=60 time=2.0 ms
64 bytes from 172.65.32.248: icmp_seq=1 ttl=60 time=1.7 ms
64 bytes from 172.65.32.248: icmp_seq=2 ttl=60 time=1.7 ms
64 bytes from 172.65.32.248: icmp_seq=3 ttl=60 time=2.1 ms
64 bytes from 172.65.32.248: icmp_seq=4 ttl=60 time=2.0 ms

--- ca80aladb12a4fbdac5ffcbc944e9a61.pacloudflare.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.9/2.1 ms
```

3. Configure the local certificate request:

```
config vpn certificate local
    edit "acme-test"
        set enroll-protocol acme2
        set acme-domain "test.ftntlab.de"
        set acme-email "techdoc@fortinet.com"
    next
```

```
By enabling this feature you declare that you agree to the Terms of Service at
https://acme-v02.api.letsencrypt.org/directory
Do you want to continue? (y/n)y
end
```

4. Verify that the enrollment was successful:

```
# get vpn certificate local details acme-test
path=vpn.certificate, objname=local, tablename=(null), size=2632
```

```

== [ acme-test ]
    Name:      acme-test
    Subject:    CN = test.ftntlab.de
    Issuer:     C = US, O = Let's Encrypt, CN = R3
    Valid from: 2021-03-11 17:43:04 GMT
    Valid to:   2021-06-09 17:43:04 GMT
    Fingerprint: 9A:03:0F:41:29:D7:01:45:04:F3:16:C0:BD:63:A2:DB
    Serial Num: 03:d3:55:80:d2:e9:01:b4:ca:80:3f:2e:fc:24:65:ad:7c:0c
ACME details:
    Status: The certificate for the managed domain has been renewed successfully and
can be used (valid since Thu, 11 Mar 2021 17:43:04 GMT).
    Staging status: Nothing in staging

```

5. Check the ACME client full status log for the CN domain:

```

# diagnose sys acme status-full test.ftntlab.de
{
  "name": "test.ftntlab.de",
  "finished": true,
  "notified": false,
  "last-run": "Thu, 11 Mar 2021 18:43:02 GMT",
  "valid-from": "Thu, 11 Mar 2021 17:43:04 GMT",
  "errors": 0,
  "last": {
    "status": 0,
    "detail": "The certificate for the managed domain has been renewed successfully and
can be used (valid since Thu, 11 Mar 2021 17:43:04 GMT). A graceful server restart now
is recommended.",
    "valid-from": "Thu, 11 Mar 2021 17:43:04 GMT"
  },
  "log": {
    "entries": [
      {
        "when": "Thu, 11 Mar 2021 18:43:05 GMT",
        "type": "message-renewed"
      },
      ...
      {
        "when": "Thu, 11 Mar 2021 18:43:02 GMT",
        "type": "starting"
      }
    ]
  }
}

```

To exchange the default FortiGate administration server certificate for the new public Let's Encrypt server certificate in the CLI:

```

config system global
  set admin-server-cert "acme-test"
end

```

When you log in to the FortiGate using an administrator account there should be no warnings related to non-trusted certificates, and the certificate path should be valid.

SFTP configuration backup - 7.0.1

In CLI, administrators have the option to backup the configuration file using SFTP:

```
# execute backup config sftp <file name> <SFTP server>[:SFTP port] <user> <password>
[<content password>]
```

To backup the configuration file using SFTP IPv4:

```
# execute backup config sftp fgt.conf 172.16.200.55 root *****
Please wait...
Connect to sftp server 172.16.200.55 ...
Connect to sftp server 172.16.200.55 ...
Send config file to sftp server OK.
```

To backup the configuration file using SFTP IPv6:

```
# execute backup config sftp fgt.conf 2000:172:16:200::55 root *****
Please wait...
Connect to sftp server 2000:172:16:200::55 ...
Connect to sftp server 2000:172:16:200::55 ...
Send config file to sftp server OK.
```

Promote FortiCare registration - 7.0.1

Shortcuts have been added to various locations in the GUI to help users register their FortiGate to FortiCare. This option is also added for newly authorized Fabric FortiGates.

To register a FortiGate on the FortiGuard page:

1. Go to *System > FortiGuard*. A message appears in the *License Information* section to log in to FortiCare Support to activate the license.

The screenshot displays the FortiGuard Distribution Network interface. On the left, a table lists various services and their status:

Entitlement	Status	Actions
FortiCare Support	Not Registered	Actions
Firmware & General Updates	Not Licensed	Purchase
AntiVirus	Expired (Expiration Date: 2020/10/31)	Renew
Web Filtering	Expired (Expiration Date: 2021/02/04)	Renew
Outbreak Prevention	Not Licensed	Purchase
SD-WAN Network Monitor	Not Licensed	Purchase
Security Rating	Not Licensed	Purchase
Industrial DB	Not Licensed	Purchase
FortiPAM	Not Licensed	Purchase
IoT Detection Service	Not Licensed	Purchase
FortiGate Cloud	Not Activated	Activate
Virtual Domain	60% 6 / 10	Upgrade

At the bottom left, a blue banner states: "Please log in to FortiCare Support to enable license activation and view contract status." with a "Login to FortiCare" button.

On the right, the "Fortinet Service Communications" section shows a table of services and their traffic volume (Last 24 hours):

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiGate Cloud Log	161.53 kB
FortiGuard.com	2.13 MB
FortiGuard Download	13.77 MB
FortiGuard Query	46.50 kB
FortiGate Cloud Sandbox	0 B
OCVPN	0 B
SDNS	0 B
FortiToken Registration	0 B
SMS Service	0 B

Below this, the "FortiGuard Filter Rating Servers" section shows a table with Service and Status columns.

At the bottom right, a green "Apply" button is visible.

- Click *Login to FortiCare*. The registration pane opens.
- Enter the required information (email address, password, country/region, reseller).

- Optionally, enable *Sign in to FortiGate Cloud using the same account*.
- Click **OK**.

To register a FortiGate on the Fabric Connectors page:

- On the root FortiGate, go to *Security Fabric > Fabric Connectors*.
- In the topology tree, click the highlighted unauthorized device and select *Authorize*. The *Authorize Devices* pane opens.
- Click *Authorize*. The *Authorization Summary* pane opens.
- The FortiGate is now authorized, so click *Register*.

Name	Model	Type	Status	Registration
FG201E	FG201E	FortiGate	Authorized	Not Registered

The *FortiCloud Account* pane opens.

- Enter the required information (password, country/region, reseller). On the *Fabric Connectors* page, the same account name is implied for registration.

6. Click *Submit*. The *Registration Summary* pane opens.
7. Click *Close*.

Add monitoring API to retrieve LTE modem statistics from 3G and 4G FortiGates - 7.0.1

The REST API can retrieve dynamic information about LTE modems, such as RSSI signal strength, SIM information, data session, and usage levels from 3G and 4G FortiGates.

Sample LTE modem configuration

```
config system lte-modem
    set status enable
    set extra-init ''
    set manual-handover disable
    set force-wireless-profile 0
    set authtype none
    set apn "pda.bell.ca"
    set modem-port 255
    set billing-date 10
    set data-limit 200
    set network-type auto
    set auto-connect disable
    set gps-service enable
    set gps-port 255
    set data-usage-tracking enable
    set band-restrictions ''
    set image-preference auto-sim
    set allow-modify-wireless-profile-table enable
    set allow-modify-mtu-size enable
    set sim-hot-swap enable
    set connection-hot-swap 5-minutes
end
```

api/v2/monitor/system/lte-modem/status

The REST API from the sample LTE modem configuration has the following output:

```
{
  "http_method": "GET",
```

```
"results":{
  "status":"enabled",
  "billing_date":10,
  "gps_status":true,
  "data_limit":200,
  "data_usage_tracking":true,
  "sim_auto_switch":true,
  "sim_auto_switch_time":"5-minutes",
  "manufacturer":"Sierra Wireless, Incorporated",
  "model":"EM7565",
  "revision":"SWI9X50C_01.14.02.00 2e210b jenkins 2020\08\19 14:18:39",
  "msisdn":"17782284617",
  "esn":"0",
  "imei":"353533100871675",
  "meid":"",
  "cell_id":"28373369",
  "hw_revision":"1.0",
  "sw_revision":"S.AT.2.5.1-00666-9655_GEN_PACK-1",
  "sku":"",
  "fsn":"UF01037177021047",
  "operating_mode":"QMI_DMS_OPERATING_MODE_ONLINE",
  "roaming":false,
  "signal":{
    "lte":{
      "rssi":-61,
      "rsrq":-13,
      "rsrp":-95,
      "snr":150
    }
  },
  "active_sim":{
    "slot":1,
    "status":"SIM_STATE_PRESENT",
    "iccid":"89302610104305638831",
    "imsi":"302610030602455",
    "carrier":"Bell Mobility",
    "country":"Canada"
  },
  "usage":{
    "rx":5001728,
    "tx":1311493
  },
  "connection_status":"QMI_WDS_CONNECTION_STATUS_CONNECTED",
  "ipv4":{
    "address":"100.114.242.233",
    "gateway":"100.114.242.234",
    "address_netmask":"255.255.255.252",
    "gateway_netmask":"255.255.255.252"
  },
  "interface":"wwan",
  "profile":{
    "profile_name":"profile3",
    "apn":"pda.bell.ca"
  }
},
"vdom":"root",
```



```
"path":"system",
"name":"lte-modem",
"action":"status",
"status":"success",
"serial":"FG40FITK20000000",
"version":"v7.0.1",
"build":138
}
```

The API output matches output from the following commands:

- `diagnose sys lte-modem modem-details`
- `diagnose sys lte-modem signal-info`
- `diagnose sys lte-modem sim-info`
- `diagnose sys lte-modem data-usage`
- `diagnose sys lte-modem data-session-info`
- `execute lte-modem wireless-profile list`

Add USB support for FortiExplorer Android - 7.0.1

FortiOS can connect to FortiExplorer Android over USB.

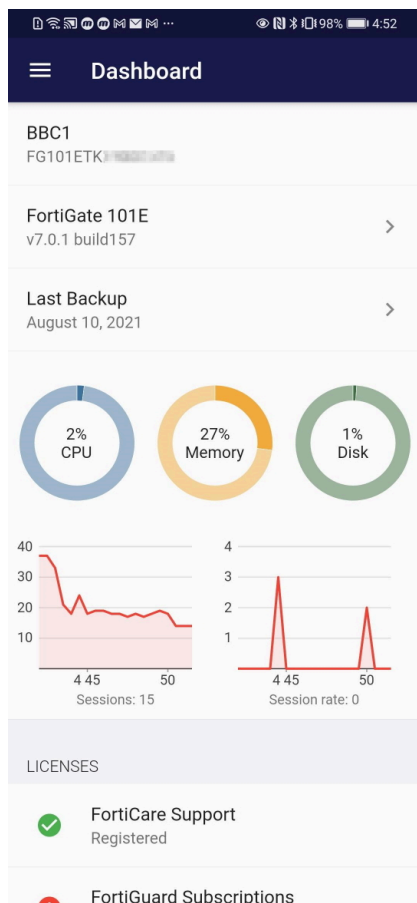


Android 4.4W and later is required to use this feature.

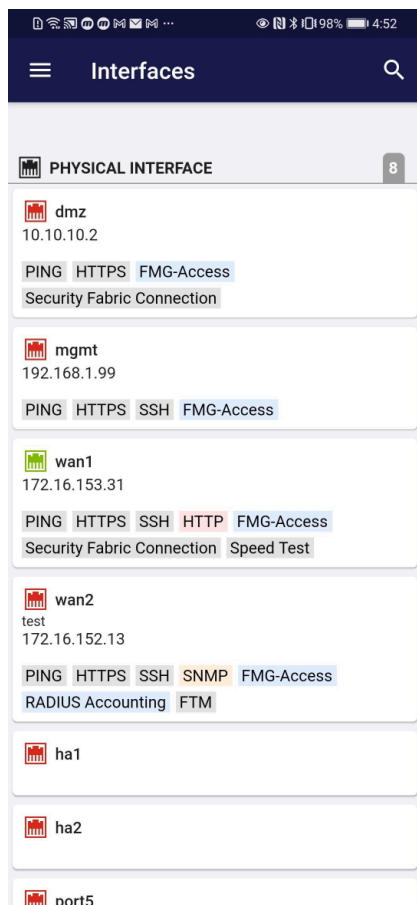
To connect and configure a FortiGate with FortiExplorer using a USB connection:

1. Download the FortiExplorer app from the [Google Play](#) store and install it on your Android device.
2. Connect the Android device to the FortiGate with a USB cable. FortiExplorer detects the FortiGate and the login screen appears.
3. Log in to the FortiGate.
4. Tap the menu icon in the upper left corner of the screen to manage or configure settings.

Dashboard screen:



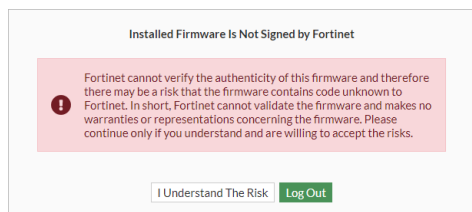
Network > Interfaces screen:



Warnings for unsigned firmware - 7.0.2

New warnings have been added to inform users when an installed firmware is not signed by Fortinet. A warning message appears when logging in to the FortiGate from the GUI, and in the CLI when the uploaded firmware fails the signature validation. Additional messages appear in various places once a user is logged in to the GUI to remind them of the unsigned firmware.

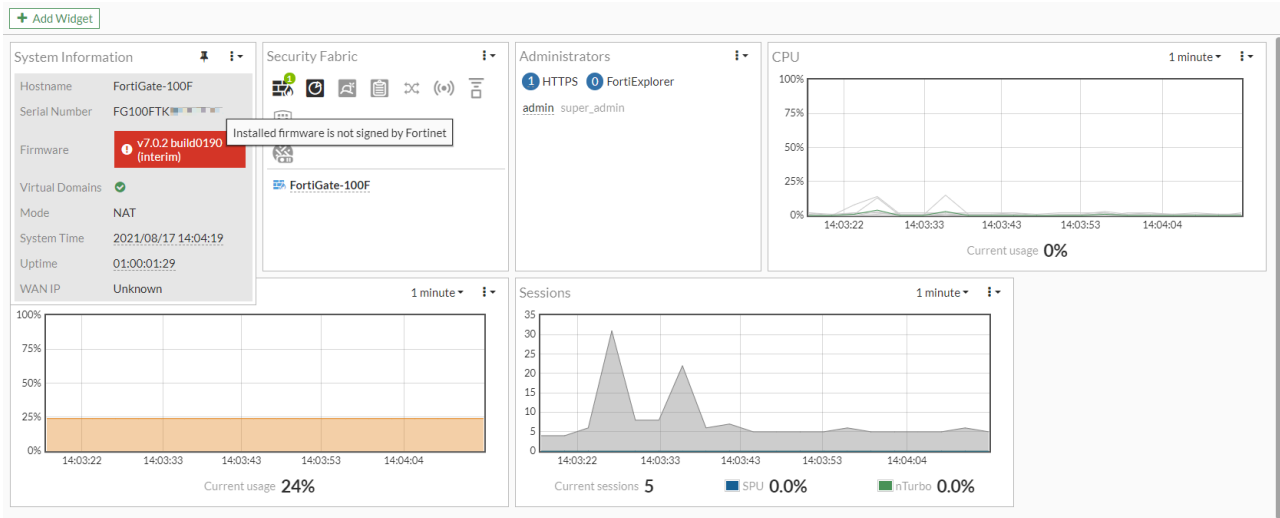
Warning message after logging in to the GUI



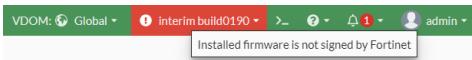
Click *I Understand the Risk* to continue.

Sample GUI warnings

Dashboard > Status page:



Banner:



System > Firmware page:



Warning message after updating the firmware in the CLI

```
# execute restore image tftp FGT_100F-v7-build0197-FORTINET.out 172.16.200.55
This operation will replace the current firmware version!
Do you want to continue? (y/n)y
Please wait...
Connect to tftp server 172.16.200.55 ...
#####
Get image from tftp server OK.
Verifying the signature of the firmware image.
*****WARNING: This firmware failed signature validation.*****
Fortinet cannot verify the authenticity of this firmware and therefore
there may be a risk that the firmware contains code unknown to Fortinet.
In short, Fortinet cannot validate the firmware and makes no warranties
or representations concerning the firmware.
Please continue only if you understand and are willing to accept the risks.
Do you want to continue? (y/n)y

Checking new firmware integrity ... pass
Please wait for system to restart.
```

```
Firmware upgrade in progress ...
Done.
```

Enabling individual ciphers in the SSH administrative access protocol - 7.0.2

Configuring individual ciphers to be used in SSH administrative access can now be done from the CLI. Administrators can select the ciphers and algorithms used for SSH encryption, key exchange, and MAC using the following settings:

```
config system global
    set strong-crypto enable
    set ssh-enc-algo {chacha20-poly1305@openssh.com aes256-ctr aes256-gcm@openssh.com}
    set ssh-kex-algo {diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org}
    set ssh-mac-algo {hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-512-etm@openssh.com}
end
```

If **strong-crypto** is disabled, the **diffie-hellman-group14-sha1** and **diffie-hellman-group-exchange-sha1** options are available for **ssh-kex-algo**.

The following settings have been removed from FortiOS:

```
config system global
    set ssh-cbc-cipher {enable | disable}
    set ssh-hmac-md5 {enable | disable}
    set ssh-kex-sha1 {enable | disable}
    set ssh-mac-weak {enable | disable}
end
```

To configure individual ciphers in the SSH administrative access protocol:

1. Configure the ciphers:

```
config system global
    set ssh-enc-algo chacha20-poly1305@openssh.com
    set ssh-kex-algo diffie-hellman-group-exchange-sha256
    set ssh-mac-algo hmac-sha2-256
end
```

2. On the client PC, open an SSH connection to the FortiGate using the configured ciphers:

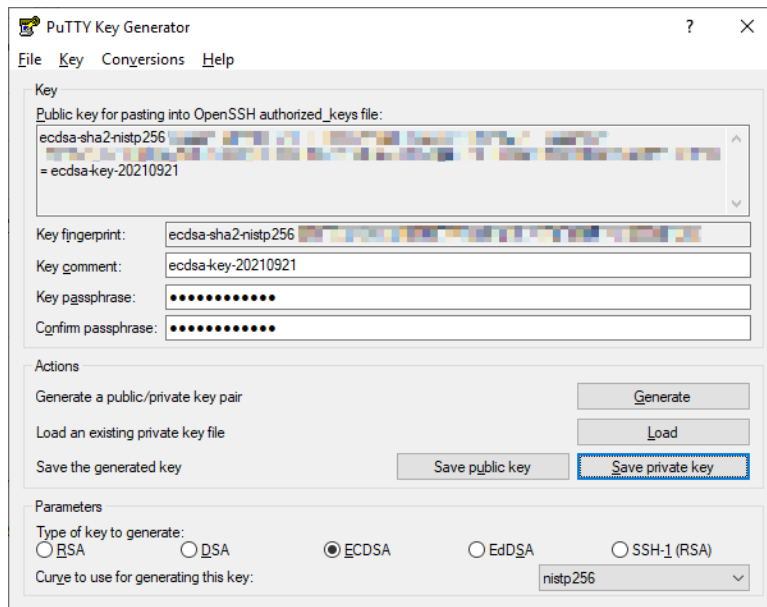
```
# ssh -c chacha20-poly1305@openssh.com -m hmac-sha2-256 -o KexAlgorithms=diffie-hellman-group-exchange-sha256 admin@FGT_IPaddress
admin@172.16.200.1's password:
FortiGate-101F # get system status
Version: FortiGate-101F v7.0.2,build0197,210827 (interim)
```

ECDSA in SSH administrative access - 7.0.2

ECDSA (Elliptic Curve Digital Signature Algorithm) is now supported in SSH administrative access. Administrative users can connect using an ECDSA key pair or an ECDSA-based certificate.

To log in to the FortiGate with an ECDSA public key:

1. On the PC, use a key generator (such as PuTTY) to generate an SSH public/private key pair using ECDSA encryption.



2. In FortiOS, configure the key for ssh-public-key1:

```
config system admin
  edit "admin1"
    set accprofile "prof_admin"
    set vdom "root"
    set ssh-public-key1 "ecdsa-sha2-nistp256 *****/*****=
root@PC05.qa.fortinet.com"
    set password *****
  next
end
```

3. On the PC, verify that the administrator can log in to the FortiGate with the private key:

```
# ssh -o StrictHostKeyChecking=no admin1@172.16.200.1 -i ~/.ssh/id_ecdsa
FortiGate-101F $ get system status
Version: FortiGate-101F v7.0.2,build0206,210910 (interim)
```

To log in to the FortiGate with a certificate private key:

1. On the PC, generate a certificate with keys encrypted by ECDSA.

2. In FortiOS, import the PEM file for the remote certificate:

```
# execute vpn certificate remote import tftp certificate.pem 172.16.200.55
```

3. Display the imported remote certificate:

```
config certificate remote
  edit "REMOTE_Cert_1"
  next
end
```

4. Apply the remote certificate to the administrative user:

```
config system admin
  edit "admin1"
    set accprofile "prof_admin"
    set vdom "root"
```

```

        set ssh-certificate "REMOTE_Cert_1"
        set password *****
    next
end

```

5. On the PC, verify that the administrator can log in to the FortiGate with the SSH certificate:

```

root@PC05:~# ssh -i certificate-private.pem admin1@172.16.200.1
FortiGate-101F $ get system status
Version: FortiGate-101F v7.0.2,build0206,210910 (interim)

```

Clear multiple sessions with REST API - 7.0.2

The following REST APIs can be used to close multiple IPv4 or IPv6 sessions at once (previously, only a single session could be closed each time):

- POST <https://<FortiGate IP>/api/v2/monitor/firewall/session/close-multiple>
- POST <https://<FortiGate IP>/api/v2/monitor/firewall/session6/close-multiple>
- POST <https://<FortiGate IP>/api/v2/monitor/firewall/session6/close-all>

For more information about the API schemas, refer to the [FortiAPI](#) documentation.

api/v2/monitor/firewall/session/close-multiple

POST https://172.18.70.127:443/api/v2/monitor/firewall/session/close-multiple?vdom=vdom2&daddr=***.125.35.134&dport=8&pro=icmp&saddr=192.168.4.158&sport=13045

```

{'action': 'close-multiple',
 'api_version': 'v7.0',
 'build': 206,
 'http_method': 'POST',
 'http_status': 200,
 'name': 'session',
 'path': 'firewall',
 'serial': 'FG4H1E5*****',
 'status': 'success',
 'vdom': 'vdom2',
 'version': 'v7.0.2'}

```

Equivalent CLI commands:

```

# diagnose sys session filter
# diagnose sys session clear

```

api/v2/monitor/firewall/session6/close-multiple

POST <https://172.18.70.127:443/api/v2/monitor/firewall/session6/close-multiple?vdom=vdom2&daddr=2000:172:16:200::254&sport=13176>

```

{'action': 'close-multiple',
 'api_version': 'v7.0',
 'build': 206,

```

```
'http_method': 'POST',
'http_status': 200,
'name': 'session6',
'path': 'firewall',
'serial': 'FG4H1E5*****',
'status': 'success',
'vdom': 'vdom2',
'version': 'v7.0.2'}
```

Equivalent CLI commands:

```
# diagnose sys session6 filter
# diagnose sys session6 clear
```

api/v2/monitor/firewall/session6/close-all

```
POST https://172.18.70.127:443/api/v2/monitor/firewall/session6/close-all
```

```
{'action': 'close-all',
'api_version': 'v7.0',
'build': 206,
'http_method': 'POST',
'http_status': 200,
'name': 'session',
'path': 'firewall',
'serial': 'FG4H1E5*****',
'status': 'success',
'vdom': 'vdom2',
'version': 'v7.0.2'}
```

Error handling

If there is no filter, the REST API backend responds with a 424 error. If there is filter and the filter name is not valid, the REST API backend responds with a 424 error. If there is filter and the filter value does not exist, the REST API backend responds with a 500 error.

Disable weak ciphers in the HTTPS protocol - 7.0.2

Administrators can select what ciphers to use for TLS 1.3 in administrative HTTPS connections, and what ciphers to ban for TLS 1.2 and below.

To select the ciphers to use for TLS 1.3 and ban for TLS 1.2 and lower:

```
config system global
    set admin-https-ssl-ciphersuites {TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-
CHACHA20-POLY1305-SHA256 TLS-AES-128-CCM-SHA256 TLS-AES-128-CCM-8-SHA256}
    set admin-https-ssl-banned-ciphers {RSA DHE ECDHE DSS ECDSA AES AESGCM CAMELLIA 3DES
SHA1 SHA256 SHA384 STATIC CHACHA20 ARIA AESCCM}
end
```



```
admin-https-ssl-
  ciphersuites {TLS-
    AES-128-GCM-SHA256
    TLS-AES-256-GCM-
    SHA384 TLS-CHACHA20-
    POLY1305-SHA256 TLS-
    AES-128-CCM-SHA256
    TLS-AES-128-CCM-8-
    SHA256}
```

Select one or more TLS 1.3 cipher suites to enable. Ciphers in TLS 1.2 and below are not affected. At least one must be enabled. To disable all, remove TLS1.3 from admin-https-ssl-versions.

TLS-AES-128-CCM-SHA256 and TLS-AES-128-CCM-8-SHA256 are only available when strong-crypto is disabled.

```
admin-https-ssl-banned-
  ciphers {RSA DHE
    ECDHE DSS ECDSA AES
    AESGCM CAMELLIA 3DES
    SHA1 SHA256 SHA384
    STATIC CHACHA20 ARIA
    AESCCM}
```

Select one or more cipher technologies that cannot be used in GUI HTTPS negotiations. Only applies to TLS 1.2 and below.

To test connecting from a PC using one of the cipher suites:

1. Disable strong-crypto and select all five cipher suites:

```
config system global
  set admin-https-redirect disable
  set admin-https-ssl-ciphersuites TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-
  CHACHA20-POLY1305-SHA256 TLS-AES-128-CCM-SHA256 TLS-AES-128-CCM-8-SHA256
  set strong-crypto disable
end
```

2. Connect from a PC using TLS_AES_128_CCM_SHA256:

```
~$ openssl s_client -connect 172.16.200.101:443 -tls1_3 -ciphersuites TLS_AES_128_CCM_
SHA256
CONNECTED(00000005)
Can't use SSL_get_servername
depth=0 O = Fortinet Ltd., CN = FortiGate
...
---
New, TLSv1.3, Cipher is TLS_AES_128_CCM_SHA256
Server public key is 2048 bit
....
```

3. Enable strong-crypto:

```
config system global
  set strong-crypto enable
end
TLS cipher suite 'TLS-AES-128-CCM-SHA256' can not be supported so removed.
TLS cipher suite 'TLS-AES-128-CCM-8-SHA256' can not be supported so removed.
```

4. Try to connect from the PC again using TLS_AES_128_CCM_SHA256:

```
~$ openssl s_client -connect 172.16.200.101:443 -tls1_3 -ciphersuites TLS_AES_128_CCM_
SHA256
CONNECTED(00000005)
139694547268800:error:14094410:SSL routines:ssl3_read_bytes:ssl3 alert handshake
failure:../ssl/record/rec_layer_s3.c:1528:SSL alert number 40
---
no peer certificate available
```

```

---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 211 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
....

```

The connection fails because TLS_AES_128_CCM_SHA256 is not supported when strong-ctypto is enabled.

Extend dedicated management CPU feature to 1U and desktop models - 7.0.2

The dedicated management CPU feature ensures that CPU 0 is only used for management traffic. This feature, which was previously available for 2U models and higher, is now available on 1U and desktop models. Two settings must be configured to use this feature:

- Enabling `dedicated-management-cpu` under `config system npu` prevents the NPU from hashing non-management traffic to CPU 0.
- Enabling `ips-reserve-cpu` under `config ips global` prevents NTurbo and IPS from sending non-management traffic to CPU 0.

To configure dedicated CPU management:

1. Configure the NPU setting:

```

config system npu
    set dedicated-management-cpu enable
end

```

2. Configure the IPS global setting:

```

config ips global
    set ips-reserve-cpu enable
end

```

3. Configure the firewall policy with IPS enabled:

```

config firewall policy
    edit 1
        set srcintf "any"
        set dstintf "any"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ips-sensor "all_default"
    next
end

```

4. Once HTTP traffic passes through the FortiGate, verify that CPU 0 is not taking any traffic load:

```

# get system performance status
CPU states: 45% user 5% system 0% nice 36% idle 0% iowait 0% irq 14% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq

```

```
CPU1 states: 50% user 0% system 0% nice 2% idle 0% iowait 0% irq 48% softirq
CPU2 states: 50% user 8% system 0% nice 31% idle 0% iowait 0% irq 11% softirq
CPU3 states: 51% user 6% system 0% nice 33% idle 0% iowait 0% irq 10% softirq
CPU4 states: 51% user 6% system 0% nice 31% idle 0% iowait 0% irq 12% softirq
CPU5 states: 48% user 7% system 0% nice 31% idle 0% iowait 0% irq 14% softirq
CPU6 states: 53% user 6% system 0% nice 31% idle 0% iowait 0% irq 10% softirq
CPU7 states: 54% user 6% system 0% nice 32% idle 0% iowait 0% irq 8% softirq
Memory: 3807328k total, 1224912k used (32.2%), 2243616k free (58.9%), 338800k freeable
(8.9%)
Average network usage: 57576 / 56881 kbps in 1 minute, 1112 / 0 kbps in 10 minutes, 757
/ 0 kbps in 30 minutes
Average sessions: 365 sessions in 1 minute, 6 sessions in 10 minutes, 6 sessions in 30
minutes
Average session setup rate: 344 sessions per second in last 1 minute, 0 sessions per
second in last 10 minutes, 0 sessions per second in last 30 minutes
Average NPU sessions: 358 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
Average nTurbo sessions: 358 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days, 23 hours, 22 minutes
```

High availability

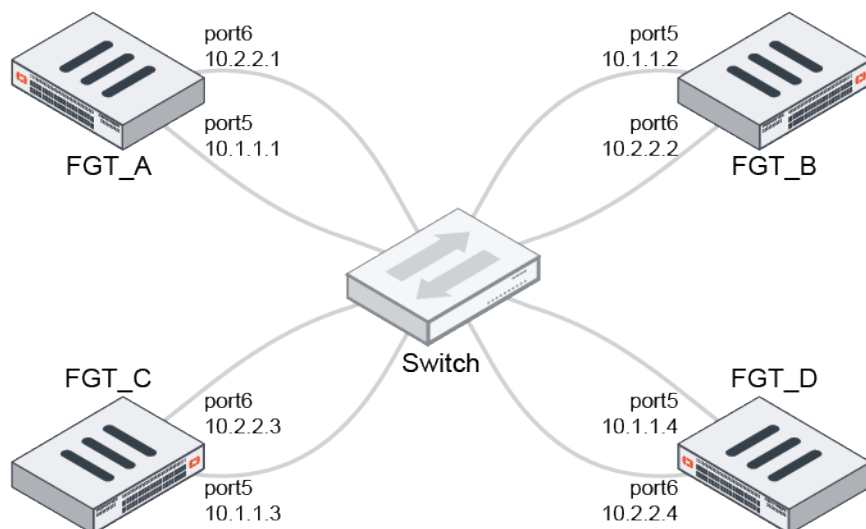
This section includes information about HA related new features:

- [FGSP four-member session synchronization and redundancy on page 261](#)
- [Layer 3 unicast standalone configuration synchronization between peers on page 266](#)
- [Improved link monitoring and HA failover time on page 269](#)
- [HA monitor shows tables that are out of synchronization on page 271](#)
- [HA failover due to memory utilization on page 271](#)
- [IKE monitor for FGSP on page 273](#)
- [Resume IPS scanning of ICCP traffic after HA failover 7.0.1 on page 275](#)
- [Extended HA VMAC address range 7.0.2 on page 277](#)

FGSP four-member session synchronization and redundancy

By using `session-sync-dev` to offload session synchronization processing to the kernel, four-member FGSP session synchronization can be supported to handle heavy loads.

Topology



In this topology, there are three FGSP peer groups for each FortiGate. Sessions are synchronized between each FortiGate and its peer groups. Redundancy is achieved by using two dedicated session sync device links for each peer setup. There are a total of six peer IPs for each session synchronization device link in each FGSP peer. When one link is fails, session synchronization is not affected.

For optimization, `sync-packet-balance` is enabled to distribute synchronization packets processing to multiple CPUs. The session synchronization process is offloaded to the kernel, and sessions are synchronized over layer 2 over the connected interfaces (`set session-sync-dev "port5" "port6"`). Jumbo frame MTU 9216 is configured on each session synchronization device link to reduce the number of packets; however, setting MTU to 9216 is entirely optional.

To configure FGT_A:

1. Configure HA:

```
config system ha
    set sync-packet-balance enable
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set session-pickup-nat enable
end
```

2. Configure the layer 2 session synchronization links:

```
config system standalone-cluster
    set session-sync-dev "port5" "port6"
end
```

3. Configure the session TTL default timeout:

```
config system session-ttl
    set default 300
end
```

4. Configure the interfaces:

```
config system interface
  edit port5
    set ip 10.1.1.1/24
    set mtu-override enable
    set mtu 9216
  next
  edit port6
    set ip 10.2.2.1/24
    set mtu-override enable
    set mtu 9216
  next
end
```

5. Configure FGSP session synchronization:

```
config system cluster-sync
  edit 1
    set peerip 10.1.1.2
  next
  edit 2
    set peerip 10.2.2.2
  next
  edit 3
    set peerip 10.1.1.3
  next
  edit 4
    set peerip 10.2.2.3
  next
  edit 5
    set peerip 10.1.1.4
  next
  edit 6
    set peerip 10.2.2.4
  next
end
```

To configure FGT_B:**1. Configure HA:**

```
config system ha
  set sync-packet-balance enable
  set session-pickup enable
  set session-pickup-connectionless enable
  set session-pickup-expectation enable
  set session-pickup-nat enable
end
```

2. Configure the layer 2 session synchronization links:

```
config system standalone-cluster
  set session-sync-dev "port5" "port6"
end
```

3. Configure the session TTL default timeout:

```
config system session-ttl
    set default 300
end
```

4. Configure the interfaces:

```
config system interface
    edit port5
        set ip 10.1.1.2/24
        set mtu-override enable
        set mtu 9216
    next
    edit port6
        set ip 10.2.2.2/24
        set mtu-override enable
        set mtu 9216
    next
end
```

5. Configure FGSP session synchronization:

```
config system cluster-sync
    edit 1
        set peerip 10.1.1.1
    next
    edit 2
        set peerip 10.2.2.1
    next
    edit 3
        set peerip 10.1.1.3
    next
    edit 4
        set peerip 10.2.2.3
    next
    edit 5
        set peerip 10.1.1.4
    next
    edit 6
        set peerip 10.2.2.4
    next
end
```

To configure FGT_C:**1. Configure HA:**

```
config system ha
    set sync-packet-balance enable
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set session-pickup-nat enable
end
```

2. Configure the layer 2 session synchronization links:

```
config system standalone-cluster
    set session-sync-dev "port5" "port6"
end
```

3. Configure the session TTL default timeout:

```
config system session-ttl
    set default 300
end
```

4. Configure the interfaces:

```
config system interface
    edit port5
        set ip 10.1.1.3/24
        set mtu-override enable
    set mtu 9216
    next
    edit port6
        set ip 10.2.2.3/24
        set mtu-override enable
        set mtu 9216
    next
end
```

5. Configure FGSP session synchronization:

```
config system cluster-sync
    edit 1
        set peerip 10.1.1.1
    next
    edit 2
        set peerip 10.2.2.1
    next
    edit 3
        set peerip 10.1.1.2
    next
    edit 4
        set peerip 10.2.2.2
    next
    edit 5
        set peerip 10.1.1.4
    next
    edit 6
        set peerip 10.2.2.4
    next
end
```

To configure FGT_D:**1. Configure HA:**

```
config system ha
    set sync-packet-balance enable
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
```

```
    set session-pickup-nat enable
end
```

2. Configure the layer 2 session synchronization links:

```
config system standalone-cluster
    set session-sync-dev "port5" "port6"
end
```

3. Configure the session TTL default timeout:

```
config system session-ttl
    set default 300
end
```

4. Configure the interfaces:

```
config system interface
    edit port5
        set ip 10.1.1.4/24
        set mtu-override enable
        set mtu 9216
    next
    edit port6
        set ip 10.2.2.4/24
        set mtu-override enable
        set mtu 9216
    next
end
```

5. Configure FGSP session synchronization:

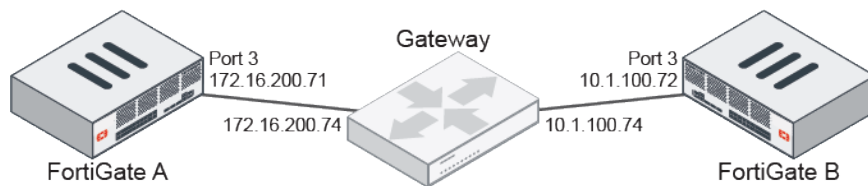
```
config system cluster-sync
    edit 1
        set peerip 10.1.1.1
    next
    edit 2
        set peerip 10.2.2.1
    next
    edit 3
        set peerip 10.1.1.2
    next
    edit 4
        set peerip 10.2.2.2
    next
    edit 5
        set peerip 10.1.1.3
    next
    edit 6
        set peerip 10.2.2.3
    next
end
```

Layer 3 unicast standalone configuration synchronization between peers

Unicast standalone configuration synchronization is supported on layer 3, allowing peers to be synchronized in cloud environments that do not support layer 2 networking. Configuring a unicast gateway allows peers to be in different subnets.

Example

In this example, two FortiGates in different subnets are connected through a unicast gateway. Both cluster members use the same port for the heartbeat interface.



To configure unicast synchronization between peers:

1. Configure FortiGate A:

```

config system ha
    set group-name "testcs"
    set hbdev "port3" 50
    set standalone-config-sync enable
    config unicast-peers
        edit 1
            set peer-ip 10.1.100.72
        next
    end
    set override enable
    set priority 200
    set unicast-status enable
    set unicast-gateway 172.16.200.74
end

```

2. Configure FortiGate B:

```

config system ha
    set group-name "testcs"
    set hbdev "port3" 50
    set standalone-config-sync enable
    config unicast-peers
        edit 1
            set peer-ip 172.16.200.71
        next
    end
    set override enable
    set priority 100
    set unicast-status enable
    set unicast-gateway 10.1.100.74
end

```

3. Check the HA status on FortiGate A:

```

# get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: ConfigSync
Group: 0
Debug: 0
Cluster Uptime: 2 days 3:40:25

```

```

Cluster state change time: 2021-03-08 12:00:38
Primary selected using:
    <2021/03/08 12:00:38> FGVMSTLM00000001 is selected as the primary because its
    override priority is larger than peer member FGVMSTLM00000002.
    <2021/03/06 11:50:35> FGVMSTLM00000001 is selected as the primary because it's the
    only member in the cluster.
ses_pickup: disable
override: enable
Configuration Status:
    FGVMSTLM21000151(updated 5 seconds ago): in-sync
    FGVMSTLM21000152(updated 5 seconds ago): in-sync
System Usage stats:
    FGVMSTLM21000151(updated 5 seconds ago):
        sessions=7, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=24%
    FGVMSTLM21000152(updated 5 seconds ago):
        sessions=5, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=23%
HBDEV stats:
    FGVMSTLM21000151(updated 5 seconds ago):
        port3: physical/1000auto, up, rx-
        bytes/packets/dropped/errors=466060007/1049137/0/0, tx=429538329/953028/0/0
    FGVMSTLM21000152(updated 5 seconds ago):
        port3: physical/1000auto, up, rx-
        bytes/packets/dropped/errors=48805199/85441/0/0, tx=33470286/81425/0/0
Primary      : FGT-71          , FGVMSTLM00000001, HA cluster index = 1
Secondary    : FGT-72          , FGVMSTLM00000002, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 0.0.0.0
Primary: FGVMSTLM00000001, HA operating index = 0
Secondary: FGVMSTLM00000002, HA operating index = 1

```

4. Check the HA checksums on FortiGate A:

```

# diagnose sys ha checksum cluster

===== FGVMSTLM00000001 =====

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 4f 2c a2 04 07 57 46 c4 47 28 ca d2 5a c5 98 ee
root: 16 af 5d a4 ac cf a5 4b b7 22 93 ce f9 02 68 bc
all: 6e 28 7f 8a 74 f7 37 43 8f 32 73 68 1e d6 ca cd

checksum
global: 4f 2c a2 04 07 57 46 c4 47 28 ca d2 5a c5 98 ee
root: 16 af 5d a4 ac cf a5 4b b7 22 93 ce f9 02 68 bc
all: 6e 28 7f 8a 74 f7 37 43 8f 32 73 68 1e d6 ca cd

===== FGVMSTLM00000002 =====

is_manage_primary()=0, is_root_primary()=1
debugzone
global: 4f 2c a2 04 07 57 46 c4 47 28 ca d2 5a c5 98 ee
root: 16 af 5d a4 ac cf a5 4b b7 22 93 ce f9 02 68 bc
all: 6e 28 7f 8a 74 f7 37 43 8f 32 73 68 1e d6 ca cd

checksum
global: 4f 2c a2 04 07 57 46 c4 47 28 ca d2 5a c5 98 ee

```

```
root: 16 af 5d a4 ac cf a5 4b b7 22 93 ce f9 02 68 bc
all:  6e 28 7f 8a 74 f7 37 43 8f 32 73 68 1e d6 ca cd
```

5. Verify that configuration changes on the primary FortiGate are synchronized to the secondary FortiGate:

a. Adjust the administrator timeout value on FortiGate A:

```
config system global
    set admintimeout 100
end
```

b. Check the debug messages on FortiGate B:

```
# diagnose debug cli 7
Debug messages will be on for 30 minutes.

# diagnose debug enable

create pid=15639, clictyno=0, last=1615246288
0: conf sys global
0: set admintimeout 100
0: end
```

Improved link monitoring and HA failover time

When a link monitor fails, only the routes specified in the link monitor are removed from the routing table, instead of all the routes with the same interface and gateway. If no route is specified, then all of the routes are removed. Only IPv4 routes are supported.

On supported models, the HA heartbeat interval unit can be changed from the default, 100ms, to 10ms. This allows for a failover time of less than 50ms, depending on the configuration and the network.

```
config system ha
    set hb-interval-in-milliseconds {100ms | 10ms}
end
```

Route based monitoring

In this example, the FortiGate has several routes to 23.2.2.2/32 and 172.16.202.2/24, and is monitoring the link *agg1* by pinging the server at 10.1.100.22. The link monitor uses the gateway 172.16.203.2.

When the link monitor fails, only the routes to the specified subnet using interface *agg1* and gateway 172.16.203.2 are removed.

To configure the link monitor:

```
config system link-monitor
    edit "22"
        set srcintf "agg1"
        set server "10.1.100.22"
        set gateway-ip 172.16.203.2
        set route "23.2.2.2/32" "172.16.202.0/24"
    next
end
```

To check the results:**1. When the link monitor is alive:**

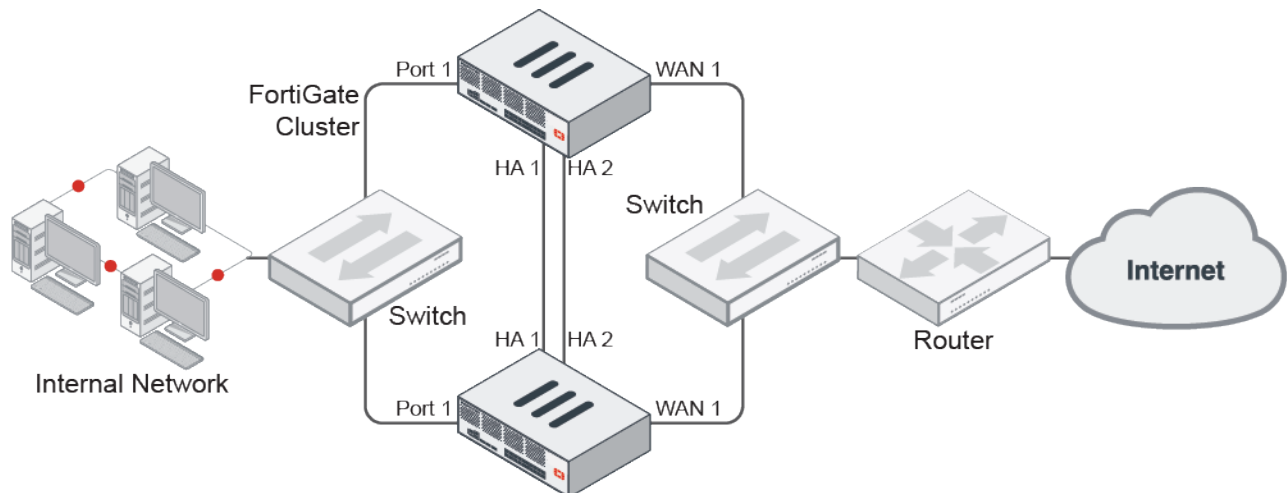
```
# get router info routing-table static
Routing table for VRF=0
S*   0.0.0.0/0 [5/0] via 10.100.1.249, port12
S    10.1.100.0/24 [10/0] via 172.16.203.2, agg1
S    23.2.2.2/32 [10/0] via 172.16.203.2, agg1
S    23.2.3.2/32 [10/0] via 172.16.203.2, agg1
S    172.16.201.0/24 [10/0] via 172.16.200.4, port9
S    172.16.202.0/24 [10/0] via 172.16.203.2, agg1
S    172.16.204.0/24 [10/0] via 172.16.200.4, port9
                        [10/0] via 172.16.203.2, agg1
                        [10/0] via 172.16.206.2, vlan100, [100/0]
```

2. When the link monitor is dead:

```
# get router info routing-table static
Routing table for VRF=0
S*   0.0.0.0/0 [5/0] via 10.100.1.249, port12
S    10.1.100.0/24 [10/0] via 172.16.203.2, agg1
S    23.2.3.2/32 [10/0] via 172.16.203.2, agg1
S    172.16.201.0/24 [10/0] via 172.16.200.4, port9
S    172.16.204.0/24 [10/0] via 172.16.200.4, port9
                        [10/0] via 172.16.203.2, agg1
                        [10/0] via 172.16.206.2, vlan100, [100/0]
```

HA failover time

In this example, the HA heartbeat interval unit is changed from 100ms to 10ms. As the default heartbeat interval is two, this means that a heartbeat is sent every 20ms. The number of lost heartbeats that signal a failure is also changed to two. So, after two consecutive heartbeats are lost, a failover will be detected in 40ms.

**To configure the HA failover:**

```
config system ha
  set group-id 240
```

```

set group-name "300D"
set mode a-p
set hbdev "port3" 50 "port5" 100
set hb-interval 2
set hb-interval-in-milliseconds 10ms
set hb-lost-threshold 2
set override enable
set priority 200
end

```

HA monitor shows tables that are out of synchronization

When units are out of synchronization in an HA cluster, the GUI will compare the HA checksums and display the tables that caused HA to be out of synchronization. This can be visualized on the HA monitor page and in the HA status widget.

Go to **System > HA** and hover the cursor over the unsynchronized device. The pop-up shows the tables that caused HA to be out of synchronization, including the checksum values.

Go to **Dashboard > Status** and in the **HA Status** widget, hover the cursor over the unsynchronized device (highlighted in red). The pop-up includes the tables that out of synchronization.

HA Status		Status	Not Synchronized
Mode	Active-Pass	Serial Number	FG3K6ETB00000000
Group	QA-DEV-FC	Checksum	ce93c760676f18d411fc160c3aa36403
Primary	Van_Off	Table(s) Out of Sync	switch-controller.managed-switch, switch-controller.nac-device
Secondary	Van_Office_FW1		
Uptime	158:17:44:37		
State Changed	00:20:06:08		

HA failover due to memory utilization

An HA failover can be triggered when memory utilization exceeds the threshold for a specific amount of time.

Memory utilization is checked at the configured sample rate (`memory-failover-sample-rate`). If the memory usage is above the threshold (`memory-failover-threshold`) every time that it is sampled for the entire monitor period (`memory-failover-monitor-period`), then a failover is triggered.

If the FortiGate meets the memory usage conditions to cause failover, the failover does not occur if the last failover on that FortiGate was triggered by high memory usage within the timeout period (`memory-failover-flip-timeout`). Other HA cluster members can still trigger memory based failovers if they meet the criteria and have not already failed within the timeout period.

After a memory based failover from FortiGate A to FortiGate B, if the memory usage on FortiGate A goes down below the threshold but the memory usage on FortiGate B is still below the threshold, then a failover is not triggered, as the cluster is working normally using FortiGate B as the primary device.

When memory based failover is disabled, a new HA primary selection occurs to determine the primary device.

To configure memory based HA failover:

```

config system ha
set memory-based-failover {enable | disable}
set memory-failover-threshold <integer>
set memory-failover-monitor-period <integer>

```

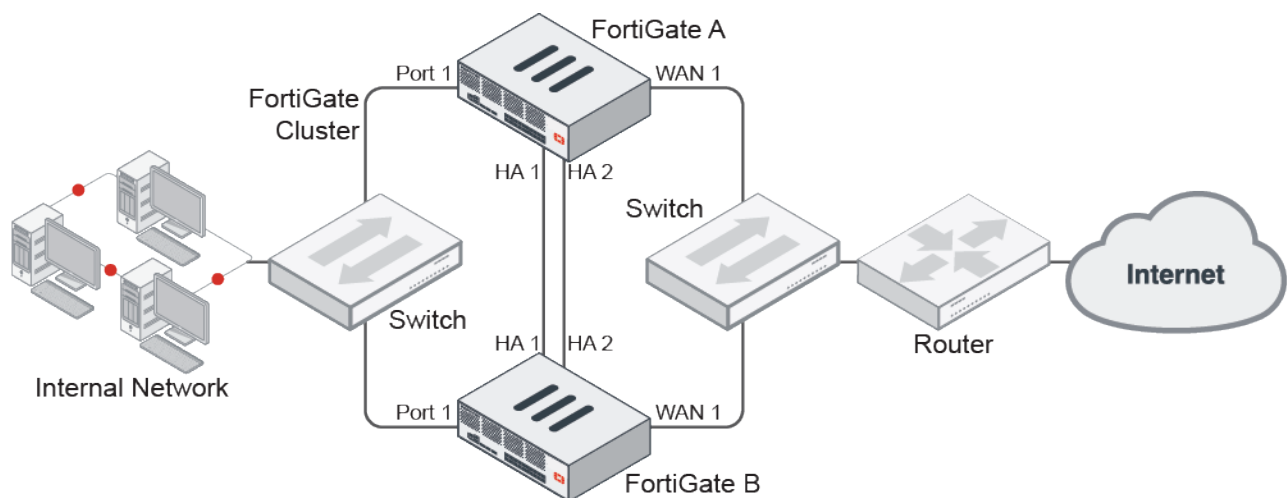
```

set memory-failover-sample-rate <integer>
set memory-failover-flip-timeout <integer>
end

```

memory-based-failover {enable disable}	Enable/disable memory based failover (default = disable).
memory-failover-threshold <integer>	The memory usage threshold to trigger a memory based failover, in percentage (0 - 95, 0 = use the conserve mode threshold, default = 0).
memory-failover-monitor-period <integer>	The duration of the high memory usage before a memory based failover is triggered, in seconds (1 - 300, default = 60).
memory-failover-sample-rate <integer>	The rate at which memory usage is sampled in order to measure memory usage, in seconds (1 - 60, default = 1).
memory-failover-flip-timeout <integer>	The time to wait between subsequent memory based failovers, in minutes (6 - 2147483647, default = 6).

Example



In this example, FortiGate A is the primary unit and FortiGate B is the secondary unit. When the memory usage on FortiGate A exceeds 50% for 300 seconds, a failover occurs and FortiGate B becomes the primary device.

If the memory usage drops below 50% on FortiGate A and rises above 50% of FortiGate B, a second failover will occur only after the timeout period of six minutes has elapsed.

If the memory usage on both FortiGate A and B is above 50%, no failover will be triggered.

To configure the memory based failover:

```

config system ha
    set memory-based-failover enable
    set memory-failover-threshold 50
    set memory-failover-monitor-period 300
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 6
end

```

IKE monitor for FGSP

Split-brain situations occur in a scenario where session synchronization is down between two FGSP peers. This can have an effect if IKE fails over from one unit to another, causing the tunnel to be invalid due to the IKE session and role being out of sync, and ESP anti-replay detection. In split-brain situations, the IKE monitor provides a mechanism to maintain the integrity of the state tables and primary/secondary roles for each VPN gateway. It continues to provide fault tolerance by keeping track of the timestamp of the latest received traffic, and it uses the ESP sequence number jump ahead value to preserve the sequence number per gateway. Once the link is up, the cluster resolves the role and synchronizes the session and IKE data. During this process, if the IKE fails over from one unit to another, the tunnel will remain valid and traffic continues to flow.



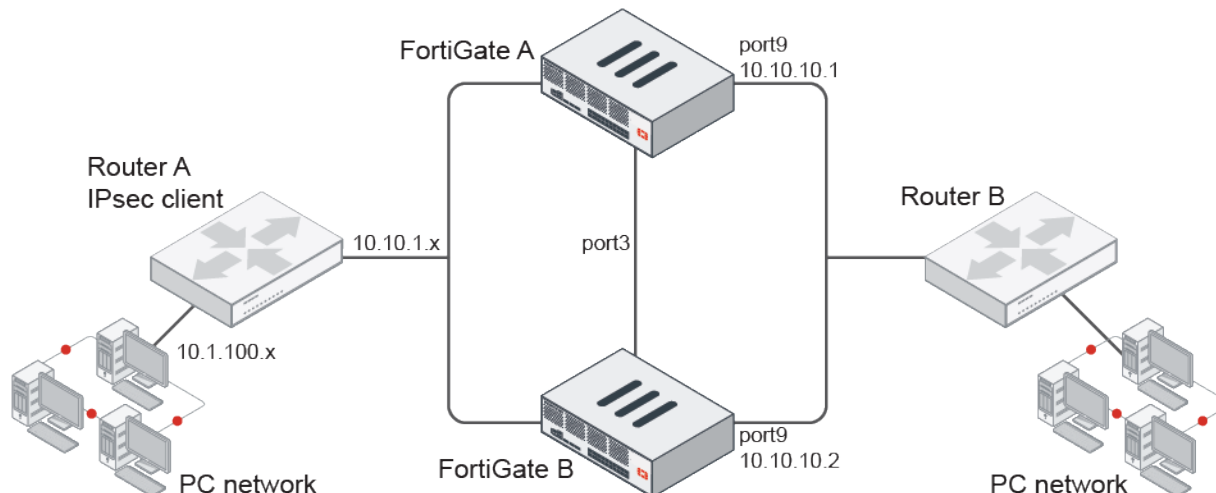
The IKE monitor only works with 2 peers in FGSP.

To configure the IKE monitor:

```
config system cluster-sync
  edit <id>
    set peerip <address>
    set ike-monitor {enable | disable}
    set ike-monitor-interval <integer>
    set ike-heartbeat-interval <integer>
    set ike-seqjump-speed <integer>
  next
end
```

ike-monitor {enable disable}	Enable/disable IKE HA monitor (default = disable).
ike-monitor-interval <integer>	Set the monitoring interval for determining how fast the cluster members detect split-brain mode, in seconds (10 - 300, default = 15).
ike-heartbeat-interval <integer>	Set the heartbeat message interval for sending the heartbeat per gateway to the other peers, in seconds (1 - 60, default = 3).
ike-seqjump-speed <integer>	Set the ESP jump ahead factor, in packets per second equivalent (1 - 10, default = 10). A value of 10 means it is the factor for a 10G interface.

Example



In this example, FortiGate A and FortiGate B are FGSP peers with port3 as the session synchronization link. The FortiGates act as IPsec dial-up servers and PCs on the 10.1.100.0 subnet are the IPsec dial-up clients. Router A acts as the external load balancer for IKE sessions between the FortiGates. Dynamic routing OSPF is configured for the FortiGates and routers.

When PC2 and other clients form IPsec dial-up tunnels to the FGSP peers, these tunnels terminate on either FortiGate A or FortiGate B, not both. For each tunnel, one FortiGate is the primary and the other is the secondary.

When the session synchronization link goes down, the FGSP split-brain scenario occurs. Without using the IKE monitor mechanism, the IKE and ESP information becomes out of sync between the two FortiGates. The secondary FortiGate for a tunnel does not receive any information about updated tunnel status. If there is a failover and tunnel traffic begins to flow to the secondary FortiGate, the tunnel will be invalidated because its state tables for that session are out of sync.

By using the IKE monitor when a split-brain scenario occurs, each unit starts periodically monitoring traffic flows and managing the sequence number jump ahead on standby units. Using a combination of timers with ESP sequence number jump ahead lets the units maintain integrity of the shared SA runtime state table, including ESP anti-replay sequence numbers.

Once the session synchronization link is up, the FGSP peers synchronize the state tables and resume regular operations.

To configure the IKE monitor:

```
config system cluster-sync
  edit 1
    set peerip 10.10.10.2
    set ike-monitor enable
    set ike-monitor-interval 12
    set ike-heartbeat-interval 2
    set ike-seqjump-speed 2
  next
end
```


Resume IPS scanning of ICCP traffic after HA failover - 7.0.1

After HA failover occurs, the IPS engine will resume processing ICCP sessions and keep the traffic going on the new primary unit. `session-pickup` must be enabled in an active-passive cluster to pick up the ICCP sessions.

Example

The following example uses an active-passive cluster. See [HA active-passive cluster setup](#) for more information.

To configure HA:

```
config system ha
  set group-name "HA-APP"
  set mode a-p
  set password *****
  set hbdev "port3" 100
  set session-pickup enable
  set override enable
end
```

Session states before failover

When HA is working, the ICCP session information is stored in the HA session cache on the secondary FortiGate.

To verify the HA session cache on the secondary FortiGate:

```
# diagnose ips share list
HA Session Cache
client=10.1.100.178:57218 server=172.16.200.177:102
service=39, ignore_app_after=0, last_app=76919, buffer_len=32
stock tags: nr=981, hash=e68dc8120970448
custom tags: nr=0, hash=1a49b996b6a42aa2
tags [count=2]: s-737, s-828,
```

The ICCP session information can be found in the IPS session list and the session table on the primary FortiGate.

To verify the IPS session information on the primary FortiGate:

```
# diagnose ips session list
SESSION id:1 serial:35487 proto:6 group:6 age:134 idle:1 flag:0x800012a6
  feature:0x4 encap:0 ignore:0,0 ignore_after:204800,0
  tunnel:0 children:0 flag:..s.-....-....
C-10.1.100.178:57218, S-172.16.200.177:102
state: C-ESTABLISHED/13749/0/0/0/0, S-ESTABLISHED/48951/0/0/0/0 pause:0, paws:0
expire: 3599
app: unknown:0 last:44684 unknown-size:0
cnfm: cotp
set: cotp
asm: cotp
```

To verify the system information on the primary FortiGate:

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=209 expire=3585 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=5
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu syn_ses app_valid
statistic(bytes/packets/allow_err): org=11980/104/1 reply=57028/164/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=10->9/9->10 gwy=172.16.200.177/10.1.100.178
hook=post dir=org act=snat 10.1.100.178:57218->172.16.200.177:102(172.16.200.4:57218)
hook=pre dir=reply act=dnat 172.16.200.177:102->172.16.200.4:57218(10.1.100.178:57218)
hook=post dir=reply act=noop 172.16.200.177:102->10.1.100.178:57218(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=1
serial=00008a9f tos=ff/ff app_list=2003 app=44684 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=71/71, ipid=134/132,
vlan=0x0000/0x0000
vlifid=134/132, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=10/10
```

Sample log on current primary FortiGate:

```
# execute log display
304 logs found.
10 logs returned.
28.8% of logs has been searched.

1: date=2021-06-04 time=16:54:40 eventtime=1622850881110547135 tz="-0700" logid="1059028704"
type="utm" subtype="app-ctrl" eventtype="signature" level="information" vd="vd1" appid=44684
srcip=10.1.100.178 dstip=172.16.200.177 srcport=57218 dstport=102 srcintf="port2"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 service="tcp/102"
direction="incoming" policyid=2 sessionid=35487 applist="test" action="pass"
appcat="Industrial" app="ICCP_Transfer.Reporting" incidentserialno=61868187 msg="Industrial:
ICCP_Transfer.Reporting," apprisk="elevated"
```

Session states after failover

After HA failover, the IPS engine on the new primary picks up the related ICCP sessions and continues passing the traffic. The HA session cache disappears on the new primary. The ICCP session now appears on the IPS session list and session table on the new primary.

To verify the IPS session information on the new primary FortiGate:

```
# diagnose ips session list
SESSION id:1 serial:35487 proto:6 group:6 age:90 idle:2 flag:0x820012a3
feature:0x4 encap:0 ignore:1,0 ignore_after:204800,0
tunnel:0 children:0 flag:....-....-..i.
C-10.1.100.178:57218, S-172.16.200.177:102
state: C-ESTABLISHED/9114/0/0/0/0, S-ESTABLISHED/0/0/0/0/0 pause:0, paws:0
```

```
expire: 28
app: unknown:0 last:44684 unknown-size:0
```

The server and client IPs, ports, and protocols remain the same.

To verify the system information on the primary FortiGate:

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=569 expire=3577 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=5
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu syn_ses app_valid
statistic(bytes/packets/allow_err): org=38629/308/1 reply=160484/483/1 tuples=3
tx speed(Bps/kbps): 158/1 rx speed(Bps/kbps): 1139/9
origin->sink: org pre->post, reply pre->post dev=10->9/9->10 gwy=172.16.200.177/10.1.100.178
hook=post dir=org act=snat 10.1.100.178:57218->172.16.200.177:102(172.16.200.4:57218)
hook=pre dir=reply act=dnat 172.16.200.177:102->172.16.200.4:57218(10.1.100.178:57218)
hook=post dir=reply act=noop 172.16.200.177:102->10.1.100.178:57218(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=1
serial=00008a9f tos=ff/ff app_list=2003 app=44684 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdn_link_id=00000000 rpdn_svc_id=0 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=71/71, ipid=134/132,
vlan=0x0000/0x0000
vlifid=134/132, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=10/10
```

The server and client IPs, ports, and NPU state remain the same.

Sample log on new primary FortiGate:

```
# execute log display
653 logs found.
10 logs returned.
65.8% of logs has been searched.

1: date=2021-06-04 time=17:05:20 eventtime=1622851521364635480 tz="-0700" logid="1059028704"
type="utm" subtype="app-ctrl" eventtype="signature" level="information" vd="vd1" appid=44684
srcip=10.1.100.178 dstip=172.16.200.177 srcport=57218 dstport=102 srcintf="port2"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 service="tcp/102"
direction="incoming" policyid=2 sessionid=35487 applist="test" action="pass"
appcat="Industrial" app="ICCP_Transfer.Reporting" incidentserialno=198181218
msg="Industrial: ICCP_Transfer.Reporting," apprisk="elevated"
```

Extended HA VMAC address range - 7.0.2

The number of HA group IDs is increased to 1024, extending the HA vMAC address range to support 1024 groups. Groups 0 to 255 use the same vMAC as in previous versions. Groups 256 to 1023 use vMAC addresses with the prefix e0:23:ff:fc. This avoids MAC address conflicts in cases where there are more than 256 FortiGate HA clusters on a network.

- When the group ID is between 0 and 255, the vMAC starts with 00:09:0f:09:

```
config system ha
    set group-id 255
end

# diagnose hardware deviceinfo nic port1
Description :FortiASIC NP6 Adapter
Driver Name :FortiASIC Unified NPU Driver
```

```
Current_HWaddr 00:09:0f:09:ff:02
Permanent_HWaddr 08:5b:0e:72:3b:b2
```

- When the group ID is between 256 and 1023, the vMAC starts with e0:23:ff:fc:

```
config system ha
    set group-id 256
end

# diagnose hardware deviceinfo nic wan1
Description :FortiASIC NP6LITE Adapter
```

```
Current_HWaddr e0:23:ff:fc:00:02
Permanent_HWaddr 90:6c:ac:fb:b3:80
```

FortiGuard

This section includes information about FortiGuard related new features:

- [Immediate download update option on page 278](#)
- [Add option to automatically update schedule frequency on page 279](#)
- [Update OUI files from FortiGuard on page 279](#)
- [Use only EU servers for FortiGuard updates 7.0.2 on page 280](#)

Immediate download update option

The FortiGuard *Accept push updates* option has been removed. On 2U models and larger (excluding VMs), the *Immediately download updates* option is added. This allows the FortiGate to form a secure persistent connection with FortiGuard to get notifications of new updates. Once notified, the FortiGate downloads the updates immediately.

The option can be enabled when the FortiGuard are servers are connected in anycast mode. Once there is updated information on subscribed contracts or object versions for the FortiGate, FortiGuard sends a notification to the FortiGate via a HTTPS connection. The FortiGate uses the `fds_notify` daemon to wait for this information, then the FortiGate makes another connection to the FortiGuard server to download the updates.



The `config system autoupdate push-update` command is no longer available in 7.0. See [Add option to automatically update schedule frequency on page 279](#) for more information about updating the schedule frequency.

To enable the immediate download update option in the GUI:

1. Go to **System > FortiGuard**.
2. In the **FortiGuard Updates** section, enable **Immediately download updates**.

The screenshot shows the FortiGuard Distribution Network interface. On the left, a list of services is shown with their license status: AntiVirus (Licensed), Web Filtering (Licensed), Outbreak Prevention (Not Licensed), SD-WAN Network Monitor (Not Licensed), Security Rating (Licensed), Industrial DB (Not Licensed), FortiIPAM (Not Licensed), IoT Detection Service (Not Licensed), and FortiGate Cloud (Not Activated). Each service has a 'Purchase' or 'Activate' button. On the right, a table lists various FortiGuard services and their sizes: FortiCare (0 B), FortiCloud Log (0 B), FortiGuard.com (1.28 MB), FortiGuard Download (52.52 MB), FortiGuard Query (14.05 kB), FortiGate Cloud Sandbox (0 B), OCVPN (0 B), SDNS (0 B), FortiToken Registration (0 B), and SMS Service (0 B). Below the table, the 'FortiGuard Updates' section is expanded, showing 'Immediately download updates' as a toggle switch that is turned on. Other options include 'Scheduled updates' (off), 'Improve IPS quality' (off), 'Use extended IPS signature package' (on), and 'Update server location' (US only, Lowest latency locations). On the far right, there is an 'Additional Information' section with links for 'API Preview', 'Edit in CLI', 'Documentation', 'Online Help', 'Video Tutorials', and 'How to Purchase/Renew Fortinet Service Subscriptions'.

3. Click **Apply**.

To enable the immediate download update option in the CLI:

```
config system fortiguard
    set fortiguard-anycast enable
    ...
    set persistent-connection enable
end
```

Add option to automatically update schedule frequency

The default auto-update schedule for FortiGuard packages has been updated. Previously, the frequency was a reoccurring random interval within two hours. Starting in 7.0, the frequency is automatic, and the update interval is calculated based on the model and percentage of valid subscriptions. The update interval is within one hour.

```
config system autoupdate schedule
    set frequency {every | daily | weekly | automatic}
end
```

For example, an FG-501E has 78% valid contracts. Based on this device model, FortiOS calculates the update schedule to be every 10 minutes. If you verify the system event logs (ID 0100041000), they are generated approximately every 10 minutes.

Update OUI files from FortiGuard

FortiGuard updates for OUI files are used to identify device vendors by the MAC address. This database is used in WiFi and device detection.

When the FortiGate has a *Firmware & General Updates* entitlement in FortiCare, FortiGuard will have the MADB contract.

To verify the contacts on the FortiGate:

```
# diagnose test update info contract
...
System contracts:
...
    MADB,Sun Oct  3 16:00:00 2021
...
Object versions:
...
    07000000MADB00100-00001.00047-2101190900
```

To verify the database status:

```
# diagnose autoupdate versions
....
Mac Address Database
-----
Version: 1.00047
Contract Expiry Date: Sat Oct  2 2021
Last Updated using manual update on Tue Jan 19 09:00:00 2021
Last Update Attempt: Fri Jan 29 11:55:54 2021
Result: No Updates
```

Use only EU servers for FortiGuard updates - 7.0.2

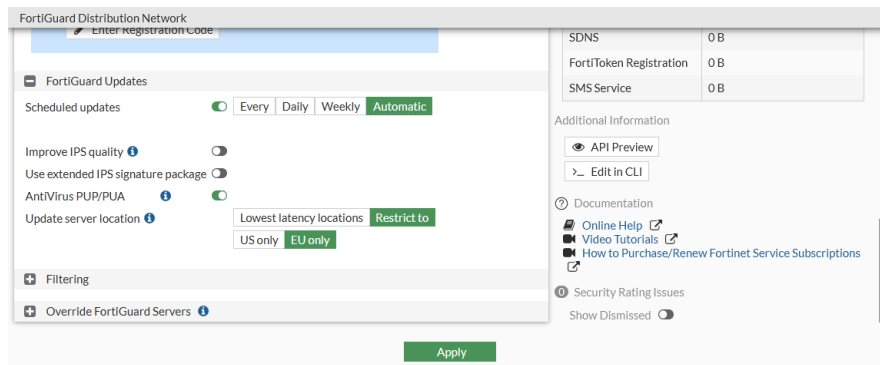
FortiGuard updates and queries can be sent only to servers located in the European Union (EU).

In EU locations, it can be required that certain traffic is only handled by servers located in the EU. By setting the update server location to EU only, the FortiGate will use EU domains to resolve to EU servers for FortiGuard traffic to update, URL rating, and IoT servers.

Server location	Anycast domain name	Non-Anycast FQDN addresses
EU only	euupdate.fortinet.net euguardservice.fortinet.net	
US only	usupdate.fortinet.net usguardservice.fortinet.net	usupdate.fortiguard.net UDP: usservice.fortiguard.net HTTPS: ussecurewf.fortiguard.net
Lowest latency (automatic)	globalupdate.fortinet.net globalguardservice.fortinet.net	update.fortiguard.net UDP: service.fortiguard.net HTTPS: securewf.fortiguard.net

To configure update server locations to EU only in the GUI:

1. Go to System > FortiGuard.
2. In the *FortiGuard Updates* section, set *Update server location* to *Restrict to*, then select *EU only*.



3. Click *Apply*.

To configure update server locations to EU only in the CLI:

```
config system fortiguard
    set update-server-location eu
end
```

Policy and Objects

This section includes information about policy and object related new features:

- [Zero Trust Network Access on page 282](#)
- [NGFW on page 375](#)
- [Policies on page 378](#)
- [Objects on page 397](#)

Zero Trust Network Access

This section includes information about ZTNA related new features:

- [Zero Trust Network Access introduction on page 282](#)
- [Basic ZTNA configuration on page 285](#)
- [Establish device identity and trust context with FortiClient EMS on page 293](#)
- [SSL certificate based authentication on page 297](#)
- [ZTNA configuration examples on page 299](#)
 - [ZTNA HTTPS access proxy example on page 299](#)
 - [ZTNA HTTPS access proxy with basic authentication example on page 308](#)
 - [ZTNA TCP forwarding access proxy example on page 314](#)
 - [ZTNA proxy access with SAML authentication example on page 317](#)
 - [ZTNA IP MAC filtering example on page 322](#)
 - [ZTNA TCP forwarding access proxy without encryption example 7.0.1 on page 328](#)
 - [ZTNA IPv6 examples 7.0.1 on page 332](#)
 - [ZTNA SSH access proxy example 7.0.1 on page 338](#)
- [Migrating from SSL VPN to ZTNA HTTPS access proxy on page 346](#)
- [ZTNA troubleshooting and debugging on page 349](#)
- [ZTNA logging enhancements 7.0.1 on page 354](#)
- [Logical AND for ZTNA tag matching 7.0.2 on page 357](#)
- [Implicitly generate a firewall policy for a ZTNA rule 7.0.2 on page 361](#)
- [Posture check verification for active ZTNA proxy session 7.0.2 on page 366](#)
- [GUI support for multiple ZTNA features 7.0.2 on page 372](#)

Zero Trust Network Access introduction

Zero Trust Network Access (ZTNA) is an access control method that uses client device identification, authentication, and Zero Trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for On-net local users and Off-net remote users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust tags.

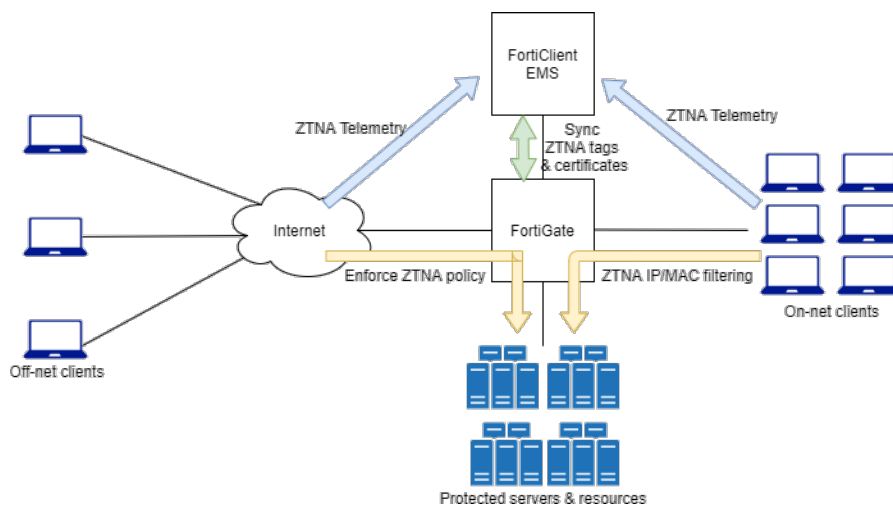
Traditionally, a user and a device have different sets of rules for on-net access and off-net VPN access to company resources. With a distributed workforce and access that spans company networks, data centers, and cloud, managing the rules can become complex. User experience is also affected when multiple VPNs are needed to get to various resources.

Full ZTNA and IP/MAC filtering

ZTNA has two modes: Full ZTNA and IP/MAC filtering:

- Full ZTNA allows users to securely access resources through a SSL encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.
- IP/MAC filtering uses ZTNA tags to provide an additional factor for identification and security posture check to implement role-based zero trust access.

ZTNA telemetry, tags, and policy enforcement

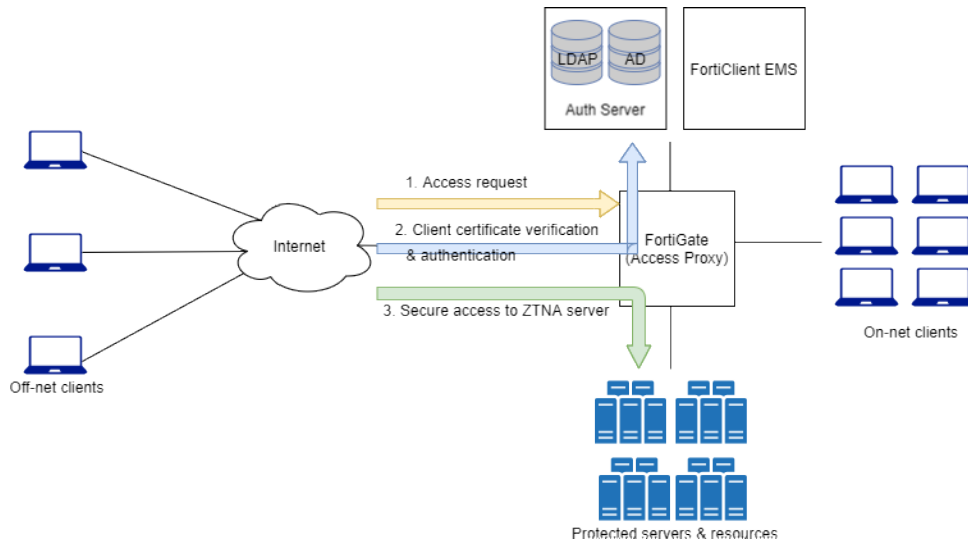


When On-net and Off-net FortiClient endpoints register to FortiClient EMS, device information, log on user information, and security posture are all shared over ZTNA telemetry with the EMS server. Clients also make a certificate signing request to obtain a client certificate from the EMS that is acting as the ZTNA Certificate Authority (CA).

Based on the client information, EMS applies matching Zero Trust tagging rules to tag the clients. These tags, and the client certificate information, are synchronized with the FortiGate in real-time. This allows the FortiGate to verify the client's identity using the client certificate, and grant access based on the ZTNA tags applied in the ZTNA rule.

For more information, see [Establish device identity and trust context with FortiClient EMS on page 293](#).

Access proxy



The FortiGate access proxy can proxy HTTP and TCP traffic over secure HTTPS connections with the client. This enables seamless access from the client to the protected servers, without needing to form IPsec or SSL VPN tunnels.

HTTPS access proxy

The FortiGate HTTPS access proxy works as a reverse proxy for the HTTP server. When a client connects to a webpage hosted by the protected server, the address resolves to the FortiGate's access proxy VIP. The FortiGate proxies the connection and takes steps to authenticate the user. It prompts the user for their certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the EMS. If an authentication scheme, such as SAML authentication, is configured, the client is redirected to a captive portal for sign-on. If this passes, traffic is allowed based on the ZTNA rules, and the FortiGate returns the webpage to the client.

For example configurations, see [ZTNA HTTPS access proxy example on page 299](#), [ZTNA HTTPS access proxy with basic authentication example on page 308](#), and [ZTNA proxy access with SAML authentication example on page 317](#).

TCP forwarding access proxy (TFAP)

TCP forwarding access proxy works as a special type of HTTPS reverse proxy. Instead of proxying traffic to a web server, TCP traffic is tunneled between the client and the access proxy over HTTPS, and forwarded to the protected resource. The FortiClient endpoint configures the ZTNA connection by pointing to the proxy gateway, and then specifying the destination host that it wants to reach. An HTTPS connection is made to the FortiGate's access proxy VIP, where the client certificate is verified and access is granted based on the ZTNA rules. TCP traffic is forwarded from the FortiGate to the protected resource, and an end to end connection is established.

For an example configuration, see [ZTNA TCP forwarding access proxy example on page 314](#).

Basic ZTNA configuration components

The basic that are require to configure full ZTNA on the FortiGate are:

1. FortiClient EMS fabric connector and ZTNA tags.
2. FortiClient EMS running version 7.0.0 or later.

3. FortiClient running 7.0.0 or later.
4. ZTNA server
5. ZTNA rule
6. Firewall policy

For configuration details, see [Basic ZTNA configuration on page 285](#).

Basic ZTNA configuration

To deploy full ZTNA, configure the following components on the FortiGate:

1. [Configure a FortiClient EMS connector on page 285](#)
2. [Configure a ZTNA server on page 287](#)
3. [Configure a ZTNA rule on page 289](#)
4. [Configure a firewall policy for full ZTNA on page 290](#)
5. [Optional authentication on page 291](#)



To configure ZTNA in the GUI, go to *System > Feature Visibility* and enable *Zero Trust Network Access*.

Configure a FortiClient EMS connector

To add an on-premise FortiClient EMS server in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New* and click *FortiClient EMS*.
3. Enter a name for the connector and the IP address or FQDN of the EMS.
4. Click *OK*.
5. A window appears to verify the EMS server certificate. Click *Accept*.
See [FortiClient EMS](#) for more information.

To add an on-premise FortiClient EMS server in the CLI:

```
config endpoint-control fctems
  edit <name>
    set server <server IP or domain>
  next
end
```

ZTNA tags

After the FortiGate connects to the FortiClient EMS, it automatically synchronizes ZTNA tags.

To view the synchronized ZTNA tags in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.
2. Hover the cursor over a tag name to view more information about the tag, such as its resolved addresses.

ZTNA Rules ZTNA Servers ZTNA Tags			
+ Create New Group Edit Delete Search			
Name	Details	Comments	Ref.
ZTNA IP Tag 24			
all_registered_clients			0
Critical			0
ems138_av_enable_tag			1
ems138_EMS_managed_tag			0
ems138_linux_tag			0
ems138_vuln_critical_tag			0
ems138_win7_tag			0
ems138_win10_tag			0
ZTNA MAC Tag 23			
all_registered_clients			0
Critical			0

To create a ZTNA tag group in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.
2. Click *Create New Group*.
3. Enter a name for the group and select the group members.

New ZTNA Tag Group

Name

grp_ems138

Members

ems138_av_enable_tag

ems138_EMS_managed_tag

ems138_linux_tag

ems138_vuln_critical_tag

ems138_win7_tag

ems138_win10_tag

+

Comments

Select Entries

Search

ZTNA Tag (47)

IP (24)

all_registered_clients

Critical

ems138_av_enable_tag

ems138_EMS_managed_tag

ems138_linux_tag

ems138_vuln_critical_tag

ems138_win7_tag

ems138_win10_tag

FCTEMS_ALL_FORTICLOUD_SERVER

FCTEMSTA20002318_all_registered_s

FCTEMSTA20002318_Critical

FCTEMSTA20002318_ems135_linux_t

FCTEMSTA20002318_ems135_macO

FCTEMSTA20002318_ems135_vuln_t

FCTEMSTA20002318_ems135_winO

FCTEMSTA20002318_ems135_winscp

FCTEMSTA20002318_High

FCTEMSTA20002318_Low

FCTEMSTA20002318_Medium

High

Close

Documentation

Online Help

OK

Cancel

4. Click **OK**.

To view the synchronized ZTNA tags in the CLI:

```
# diagnose firewall dynamic address
# diagnose firewall dynamic list
```

To create a ZTNA tag group in the CLI:

```
config firewall addrgrp
  edit <group name>
    set category ztna-ems-tag
    set member <members>
  next
end
```

Configure a ZTNA server

To configure a ZTNA server, define the access proxy VIP and the real servers that clients will connect to. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service/server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

To create a ZTNA server and access proxy VIP in the GUI:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Enter a name for the server.
4. Select an external interface, enter the external IP address, and select the external port that the clients will connect to.
5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.

6. Add server mapping:
 - a. In the *Service/server mapping* table, click *Create New*.
 - b. Set *Virtual Host* to *Any Host* or *Specify*.
 - *Any Host*: Any request that resolves to the access proxy VIP will be mapped to your real servers. For example, if both `www.example1.com` and `www.example2.com` resolve to the VIP, then both requests are mapped to your real servers.

- **Specify:** Enter the name or IP address of the host that the request must match. For example, if `www.example1.com` is entered as the host, then only requests to `www.example1.com` will match.

c. Configure the path as needed.

The path can be matched by substring, wildcard, or regular expression. For example, if the virtual host is specified as `www.example1.com`, and the path substring is `map1`, then `www.example1.com/map1` will be matched.

The screenshot shows two overlapping windows in the FortiGate GUI. The background window is titled 'New ZTNA Server' and contains fields for Name (ZTNA_server01), Comments, Network (Service: HTTPS, External Interface: any, External IP: 172.18.62.32, External port: 8443), Services and Servers (Default certificate: Fortinet_CA_SSL), and a Service/Server mapping table (empty). The foreground window is titled 'New Service/Server Mapping' and contains fields for Service (HTTPS), Virtual Host (Any Host, Specify), Match by (Substring, Wildcard), Host (www.example1.com), Use certificate (Fortinet_CA_SSL), Match path by (Substring, Wildcard, Regular Expression), and Path (map1). Below these fields is a 'Servers' table with columns IP, Port, and Status, and a 'Create New' button. At the bottom of both windows are 'OK' and 'Cancel' buttons.

d. Add a server:

- In the **Servers** table, click *Create New*.
- Enter the server IP address and port number.
- Set the server status.
- Click **OK**.
- Add more servers as needed.

e. Click OK.

f. Add more server mappings as needed.

7. Click OK.

To create a ZTNA server and access proxy VIP in the CLI:

1. Configure an access proxy VIP:

```
config firewall vip
  edit <name>
    set type access-proxy
    set extip <external IP>
    set extintf <external interface>
    set server-type { https | ssh }
    set extport <external port>
    set ssl-certificate <certificate>
  next
end
```

2. If the virtual host is specified, configure the virtual host:

```
config firewall access-proxy-virtual-host
  edit <auto generated when configured from GUI>
    set ssl-certificate <certificate>
    set host <host name or IP>
    set host-type { sub-string | wildcard }
```

```
    next
end
```

3. Configure the server and path mapping:

```
config firewall access-proxy
    edit <name>
        set vip <vip name>
        set client-cert { enable | disable }
        set empty-cert-action { accept | block }
        config api-gateway
            edit 1
                set url-map <mapped path>
                set service { http | https | tcp-forwarding | samlsp }
                set virtual-host <name of virtual-host if specified>
                set url-map-type { sub-string | wildcard | regex }
                config realservers
                    edit 1
                        set ip <ip of real server>
                        set port <port>
                        set status { active | standby | disable }
                        set health-check { enable | disable }
                    next
                end
                set ldb-method static
                set persistence none
                set ssl-dh-bits 2048
                set ssl-algorithm high
                set ssl-min-version tls-1.1
                set ssl-max-version tls-1.3
            next
        end
    next
end
```

The load balance method for the real servers can only be specified in the CLI.

Configure a ZTNA rule

A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic.

To configure a ZTNA rule in the GUI:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Rules* tab.
2. Click *Create New*.
3. Enter a name for the rule.
4. Add the ZTNA tags or tag groups that are allowed access.
5. Select the ZTNA server.

6. Configure the remaining options as needed.
7. Click OK.

To configure a ZTNA rule in the CLI:

```
config firewall proxy-policy
  edit 1
    set name <ZTNA rule name>
    set proxy access-proxy
    set access-proxy <access proxy>
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag <ZTNA tag(s)>
    set action accept
    set schedule "always"
    set logtraffic all
    set utm-status enable
    set ssl-ssh-profile <inspection profile>
  next
end
```

Configure a firewall policy for full ZTNA

The firewall policy matches and redirects client requests to the access proxy VIP. The source interface and addresses that are allowed access to the VIP can be defined. By default, the destination is any interface, so once a policy is configured for full ZTNA, the policy list will be organized by sequence.

UTM processing of the traffic happens at the ZTNA rule.

To configure a firewall policy for full ZTNA in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Enter a name for the policy.
3. Enable *ZTNA* and select *Full ZTNA*.

4. Set ZTNA Server to the configured ZTNA server.

5. Configure the remaining settings as needed.

6. Click OK.

To configure a firewall policy for full ZTNA in the CLI:

```
config firewall policy
  edit <policy ID>
    set name <policy name>
    set srcintf <source interface>
    set dstintf "any"
    set srcaddr <source address>
    set dstaddr <access proxy VIP>
    set action accept
    set schedule "always"
    set service "ALL"
    set inspection-mode proxy
    set logtraffic all
    set nat enable
  next
end
```

Optional authentication

To configure authentication to the access proxy, you must configure an authentication scheme and authentication rule in the CLI. They are used to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

The authentication scheme defines the method of authentication that is applied. For ZTNA, basic HTTP and SAML methods are supported. Each method has additional settings to define the data source to check against. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. For ZTNA, active authentication method is supported. The active authentication method references a scheme where users are actively prompted for authentication, like with basic authentication.

After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to. In the ZTNA rule and proxy policy you can define a user or user group as the allowed source. Only users that match that user or group are allowed through the proxy policy.

To configure a basic authentication scheme:

```
config authentication scheme
    edit <name>
        set method basic
        set user-database <auth server>
    next
end
```

To configure an authentication rule:

```
config authentication rule
    edit <name>
        set status enable
        set protocol http
        set srcintf <interface>
        set srcaddr <address>
        set dstaddr <address>
        set ip-based enable
        set active-auth-method <active auth scheme>
    next
end
```

To apply a user group to a ZTNA rule in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Edit an existing rule, or click *Create New* to create a new rule.
3. Click in the *Source* field, select the *User* tab, and select the users and user groups that will be allowed access.
4. Configure the remaining settings as required.
5. Click *OK*.

To apply a user group to a ZTNA rule in the CLI:

```
config firewall proxy-policy
    edit <policy ID>
        set name <ZTNA rule name>
        set proxy access-proxy
        set access-proxy <access proxy>
        set srcaddr "all"
        set dstaddr "all"
```

```

set ztna-ems-tag <ZTNA tags>
set action accept
set schedule "always"
set logtraffic all
set groups <user group>
set utm-status enable
set ssl-ssh-profile <inspection profile>
next
end

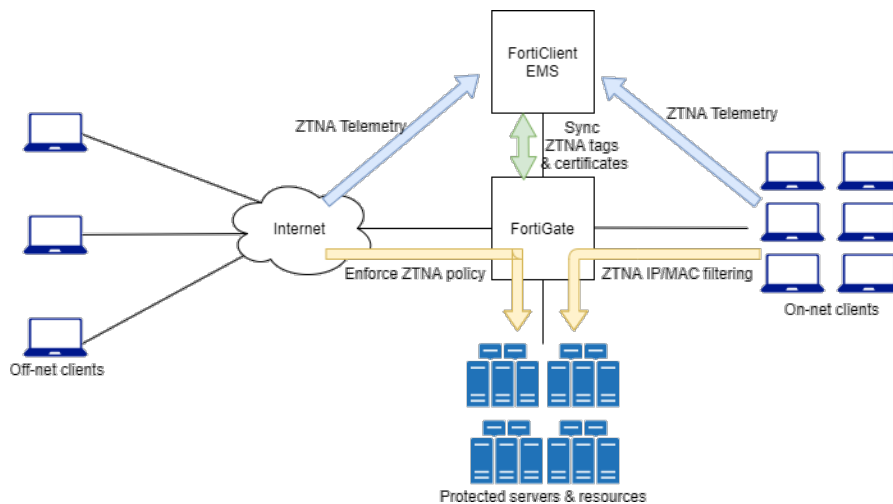
```

The authentication rule and scheme defines the method used to authenticate users. With basic HTTP authentication, a sign in prompt is shown after the client certificate prompt. After the authentication passes, the returned groups that the user is a member of are checked against the user groups that are defined in the ZTNA rule. If a group matches, then the user is allowed access after passing a posture check.

For more information, see [ZTNA HTTPS access proxy with basic authentication example on page 308](#) and [ZTNA proxy access with SAML authentication example on page 317](#).

Establish device identity and trust context with FortiClient EMS

How device identity is established through client certificates, and how device trust context is established between FortiClient, FortiClient EMS, and the FortiGate, are integral to ZTNA.



Device roles

FortiClient

FortiClient endpoints provide the following information to FortiClient EMS when they register to the EMS:

- Device information (network details, operating system, model, and others)
- Logged on user information
- Security posture (On-net/Off-net, antivirus software, vulnerability status, and others)

It also requests and obtains a client device certificate from the EMS ZTNA Certificate Authority (CA) on its first attempt to connect to the access proxy. The client uses this certificate to identify itself to the FortiGate.

FortiClient EMS

FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. The certificate is then synchronized to the FortiGate. EMS also shares its EMS ZTNA CA certificate with the FortiGate, so that the FortiGate can use it to authenticate the clients.

FortiClient EMS uses zero trust tagging rules to tag endpoints based on the information that it has on each endpoint. The tags are also shared with the FortiGate.

FortiGate

The FortiGate maintains a continuous connection to the EMS server to synchronize endpoint device information, including primarily:

- FortiClient UID
- Client certificate SN
- EMS SN
- Device credentials (user/domain)
- Network details (IP and MAC address and routing to the FortiGate)

When a device's information changes, such as when a client moves from on-net to off-net, or their security posture changes, EMS is updated with the new device information and then updates the FortiGate. The FortiGate's WAD daemon can use this information when processing ZTNA traffic.

Certificate management on FortiClient EMS

FortiClient EMS has a *default_ZTNARootCA* certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiGate and FortiClient endpoints by generating new certificates for each client.

FortiClient Endpoint Management Server

EMS Settings

Custom hostname: Optional

Management IP and Port: Optional (e.g. 443)

Redirect HTTP request to HTTPS: ☒

SSL certificate: FCTEHS8821001322-1 (2038-01-19)

Show FortiGate Server List: ☐

EMS CA certificate (ZTNA): default_ZTNARootCA.pem (2046-03-17)
Certificate was created on 2021-03-23T20:25:36.480

Reset Stalled Deployment Interval: 12 hours

EMS Settings

☐ EMS for Chromebooks Settings ⓘ

Endpoints Settings

FortiClient telemetry connection key: Optional BB

Keep alive interval: 60 seconds

License timeout: 45 days

Automatically upload avatars: ☒
When this is enabled, FortiClient will upload user avatars to all FortiGates, FortiAnalyzers, and EMS servers it is registered to.

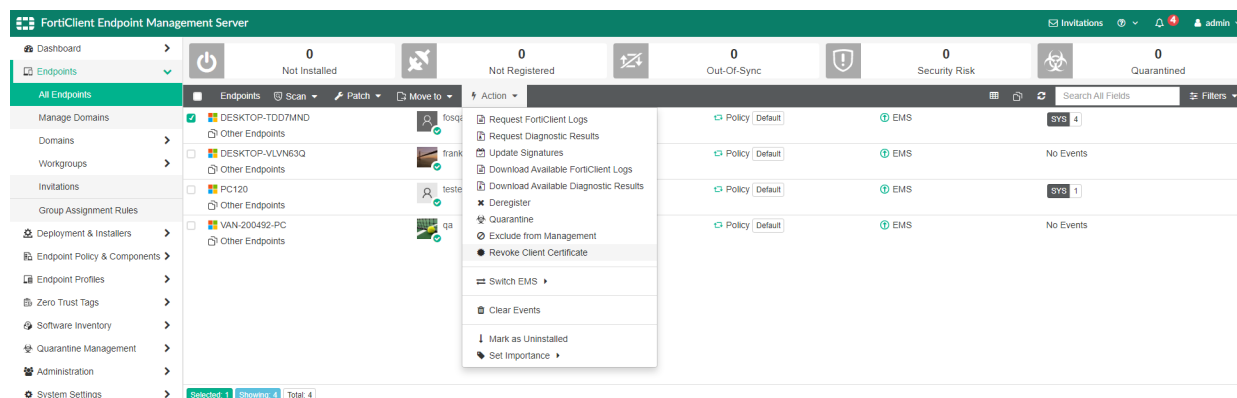
Enable endpoint snapshot reports: ☐

Save



Do not confuse the EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by EMS for HTTPS access and fabric connectivity to the EMS server.

EMS can also manage individual client certificates. To revoke the current client certificate that is used by the endpoint: go to *Endpoint > All Endpoints*, select the client, and click *Action > Revoke Client Certificate*.



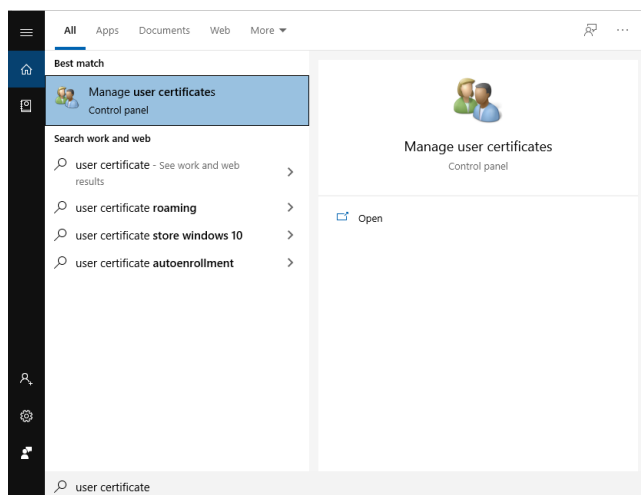
Locating and viewing the client certificate on an endpoint

In Windows, FortiClient automatically installs certificates into the certificate store. The certificate information in the store, such as certificate UID and SN, should match the information on EMS and the FortiGate.

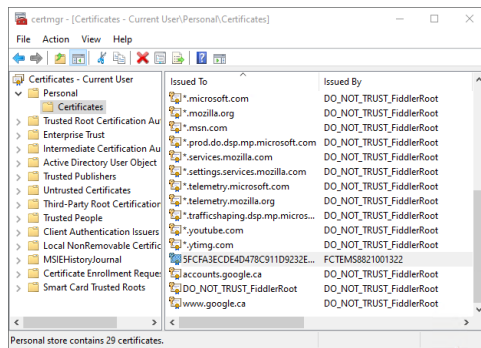
To locate certificates on other operating systems, consult the vendor documentation.

To locate the client certificate and EMS ZTNA CA certificate on a Windows PC:

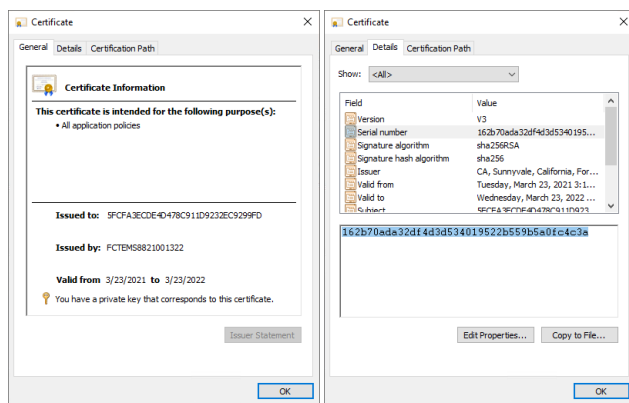
1. In the Windows search box, enter *user certificate* and click *Manage user certificates* from the results.



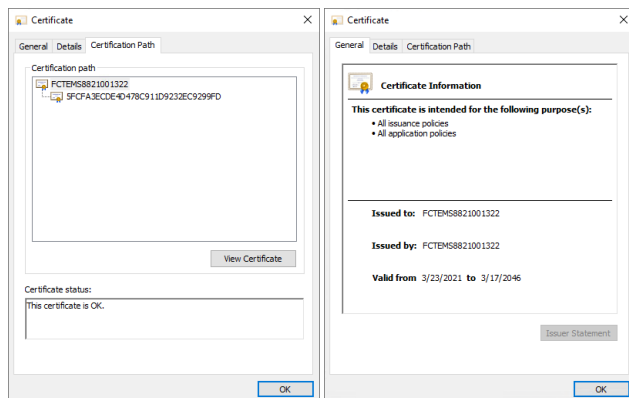
2. In the certificate manager, go to *Certificates - Current User > Personal > Certificates* and find the certificate that is issued by the FortiClient EMS.



3. Right-click on it and select Properties.
4. The **General** tab shows the client certificate UID and the issue and expiry dates. The **Details** tab show the certificate SN.



5. Go to the **Certificate Path** tab to see the full certificate chain.
6. Select the root CA and click **View Certificate** to view the details about the EMS ZTNA CA certificate.



Verifying that the client information is synchronized to the FortiGate

The following diagnose commands help to verify the presence of matching endpoint record, and information such as the client UID, client certificate SN, and EMS certificate SN on the FortiGate. If any of the information is missing or incomplete, client certificate authentication might fail because the corresponding endpoint entry is not found. More in-depth diagnosis would be needed to determine the reason for the missing records.

Command	Description
# diagnose endpoint record list <ip>	Show the endpoint record list. Optionally, filter by the endpoint IP address.
# diagnose endpoint wad-comm find-by uid <uid>	Query endpoints by client UID.
# diagnose endpoint wad-comm find-by ip-vdom <ip> <vdom>	Query endpoints by the client IP-VDOM pair.
# diagnose wad dev query-by uid <uid>	Query from WAD diagnose command by UID.
# diagnose wad dev query-by ipv4 <ip>	Query from WAD diagnose command by IP address.
# diagnose test application fcnacd 7 # diagnose test application fcnacd 8	Check the FortiClient NAC daemon ZTNA and route cache.

To check the endpoint record list for IP address 10.6.30.214:

```
# diagnose endpoint record list 10.6.30.214
```

Record #1:

```

IP Address = 10.6.30.214
MAC Address = 00:0c:29:ba:1e:61
MAC list = 00:0c:29:ba:1e:61;00:0c:29:ba:1e:6b;
VDOM = root (0)
EMS serial number: FCTEMS8821001322
Client cert SN: 17FF6595600A1AF53B87627AB4EBEDD032593E64
Quarantined: no
Online status: online
Registration status: registered
On-net status: on-net
Gateway Interface: port2
FortiClient version: 7.0.0
AVDB version: 84.778
FortiClient app signature version: 18.43
FortiClient vulnerability scan engine version: 2.30
FortiClient UID: 5FCFA3ECDE4D478C911D9232EC9299FD
...
Number of Routes: (1)
    Gateway Route #0:
        - IP:10.1.100.214, MAC: 00:0c:29:ba:1e:6b, Indirect: no
        - Interface:port2, VFID:0, SN: FG5H1E5819902474

```

online records: 1; offline records: 0; quarantined records: 0

SSL certificate based authentication

A client certificate is obtained when an endpoint registers to EMS. FortiClient automatically submits a CSR request and the FortiClient EMS signs and returns the client certificate. This certificate is stored in the operating system's certificate store for subsequent connections. The endpoint information is synchronized between the FortiGate and FortiClient EMS.

When an endpoint disconnects or is unregistered from EMS, its certificate is removed from the certificate store and revoked on EMS. The endpoint obtains a certificate again when it reconnected the EMS.

By default, client certificate authentication is enabled on the access proxy, so when the HTTPS request is received the FortiGate's WAD process challenges the client to identify itself with its certificate. The FortiGate makes a decision based on the following possibilities:

1. If the client responds with the correct certificate that the client UID and certificate SN can be extracted from:
 - If the client UID and certificate SN match the record on the FortiGate, the client is allowed to continue with the ZTNA proxy rule processing.
 - If the client UID and certificate SN do not match the record on the FortiGate, the client is blocked from further ZTNA proxy rule processing.
2. If the client cancels and responds with an empty client certificate:
 - If `empty-cert-action` is set to `accept`, the client is allowed to continue with ZTNA proxy rule processing.
 - If `empty-cert-action` is set to `block`, the client is blocked from further ZTNA proxy rule processing.

To configure the client certificate actions:

```
config firewall access-proxy
  edit <name>
    set client-cert {enable | disable}
    set empty-cert-action {accept | block}
  next
end
```

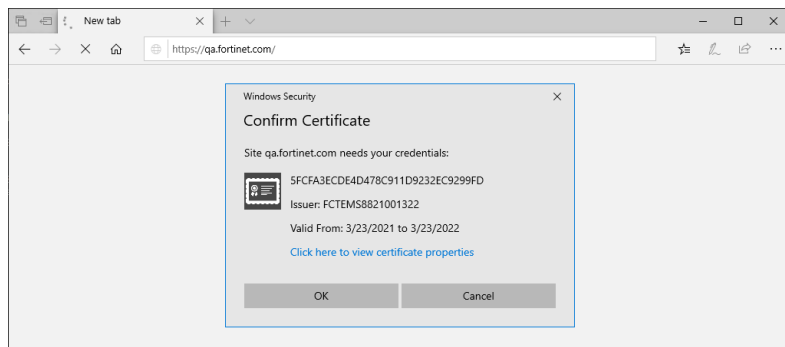
Example

In this example, a client connects to *qa.fortinet.com* and is prompted for a client certificate.

- `client-cert` is set to `enable`, and `empty-cert-action` is set to `block`.
- The ZTNA server is configured, and a ZTNA rule is set to allow this client.
- The domain resolves to the FortiGate access proxy VIP.

Scenario 1:

When prompted for the client certificate, the client clicks *OK* and provides a valid certificate that is verified by the FortiGate.

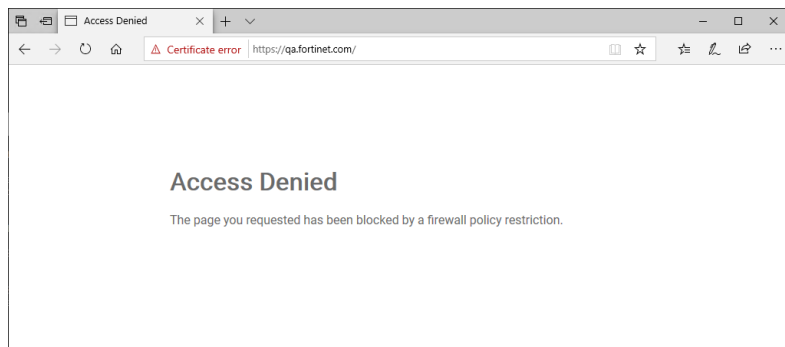


Result:

The client passes SSL certificate authentication and is allowed to access the website.

Scenario 2:

When prompted for the client certificate, the client clicks *Cancel*, resulting in an empty certificate response to the access proxy.

**Result:**

Because the certificate response is empty and `empty-cert-action` is set to `block`, the WAD daemon blocks the connection.



Currently, the Microsoft Edge and Google Chrome browsers are supported by ZTNA.

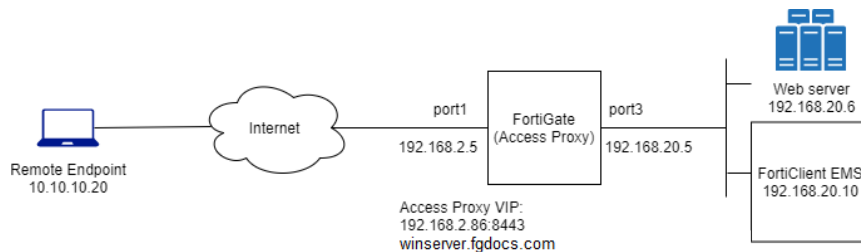
ZTNA configuration examples

This section includes the following ZTNA configuration examples:

- [ZTNA HTTPS access proxy example on page 299](#)
- [ZTNA HTTPS access proxy with basic authentication example on page 308](#)
- [ZTNA TCP forwarding access proxy example on page 314](#)
- [ZTNA proxy access with SAML authentication example on page 317](#)
- [ZTNA IP MAC filtering example on page 322](#)
- [ZTNA TCP forwarding access proxy without encryption example 7.0.1 on page 328](#)
- [ZTNA IPv6 examples 7.0.1 on page 332](#)
- [ZTNA SSH access proxy example 7.0.1 on page 338](#)

ZTNA HTTPS access proxy example

In this example, an HTTPS access proxy is configured to demonstrate its function as a reverse proxy on behalf of the web server it is protecting. It verifies user identity, device identity, and trust context, before granting access to the protected source.



This example shows access control that allows or denies traffic based on ZTNA tags. Traffic is allowed when the FortiClient endpoint is tagged as *Low* risk, and denied when the endpoint is tagged with *Malicious-File-Detected*.

This example assumes that the FortiGate EMS fabric connector is already successfully connected.



To configure ZTNA in the GUI, go to *System > Feature Visibility* and enable *Zero Trust Network Access*.

To configure a Zero Trust tagging rule on the FortiClient EMS:

1. Log in to the FortiClient EMS.
2. Go to *Zero Trust Tags > Zero Trust Tagging Rules*, and click *Add*.
3. In the *Name* field, enter *Malicious-File-Detected*.
4. In the *Tag Endpoint As* dropdown list, select *Malicious-File-Detected*.

EMS uses this tag to dynamically group together endpoints that satisfy the rule, as well as any other rules that are configured to use this tag.

5. Click *Add Rule* then configure the rule:
 - a. For OS, select *Windows*.
 - b. From the *Rule Type* dropdown list, select *File* and click the + button.
 - c. Enter a file name, such as *C:\virus.txt*.
 - d. Click *Save*.

FortiClient Endpoint Management Server

Zero Trust Tagging Rule Set

Name: Malicious-File-Detected

Tag Endpoint As: Malicious-File-Detected

Enabled: ☒

Comments: Detect presence of a malicious file

Type	Value
Windows (1)	
File	C:\virus.txt

Save Cancel

6. Click *Save*.

To configure HTTPS access proxy VIP in the GUI:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Set *Name* to *WIN2K16-P1*.

4. Configure the network settings:
 - a. Set *External interface* to *port1*.
 - b. Set *External IP* to *192.168.2.86*.
 - c. Set *External port* to *8443*.
5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.
6. Add server mapping:
 - a. In the *Service/server mapping* table, click *Create New*.
 - b. Set *Virtual Host* to *Any Host*.
 - c. Configure the path as needed. For example, to map to *winserver.fgdocs.com/fortigate*, enter */fortigate*.
 - d. Add a server:
 - i. In the *Servers* table, click *Create New*.
 - ii. Set *IP* to *192.168.20.6*.
 - iii. Set *Port* to *443*.
 - iv. Click *OK*.

The screenshot shows two overlapping configuration windows. The background window is 'Edit ZTNA Server' with the following settings: Name: WIN2K16-P1, Comments: (empty), Network: Service: HTTPS, External interface: port1, External IP: 192.168.2.86, External port: 8443, Services and Servers: Default certificate: Fortinet_SSL, Service/server mapping: (empty table with 'Create New', 'Edit', 'Delete' buttons). The foreground window is 'Edit Service/Server Mapping' with: Service: HTTPS, Virtual Host: Any Host, Match path by: Substring, Path: /, and a Servers table with one entry: IP: 192.168.20.6, Port: 443, Status: Active.

- e. Click *OK*.

The screenshot shows the 'Edit ZTNA Server' window with the same settings as the previous screenshot. The 'Service/server mapping' table now contains one entry: Service: HTTPS, URL: /.

7. Click *OK*.

To configure ZTNA rules to allow and deny traffic based on ZTNA tags in the GUI:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Rules* tab.
2. Create a rule to deny traffic:
 - a. Click *Create New* again to create another rule.
 - b. Set *Name* to *ZTNA-Deny-malicious*.
 - c. Add the ZTNA tag *Malicious-File-Detected*.
This tag is dynamically retrieved from EMS when you first created the Zero Trust Tagging Rule.
 - d. Select the ZTNA server *WIN2K16-P1*.
 - e. Set *Action* to *DENY*.
 - f. Enable *Log Violation Traffic*.

The screenshot shows the 'Edit ZTNA Rule' dialog box. The 'Name' field is 'ZTNA-Deny-malicious'. The 'Source' is 'all'. The 'ZTNA Tag' is 'Malicious-File-Detected'. The 'ZTNA Server' is 'WIN2K16-P1'. The 'Action' is 'DENY'. The 'Log Violation Traffic' checkbox is checked. The 'Comments' field is empty. The 'Enable this policy' checkbox is checked. The 'Additional Information' section on the right includes 'API Preview' and 'Documentation' links.

- g. Click *OK*.
3. Create a rule to allow traffic:
 - a. Click *Create New*.
 - b. Set *Name* to *proxy-WIN2K16-P1*.
 - c. Add the ZTNA tag *Low*.
 - d. Select the ZTNA server *WIN2K16-P1*.

The screenshot shows the 'Edit ZTNA Rule' dialog box. The 'Name' field is 'proxy-WIN2K16-P1'. The 'Source' is 'all'. The 'ZTNA Tag' is 'Low'. The 'ZTNA Server' is 'WIN2K16-P1'. The 'Action' is 'ACCEPT'. The 'Log Violation Traffic' checkbox is checked. The 'Security Profiles' section includes 'AntiVirus', 'Web Filter', 'Video Filter', 'Application Control', 'IPS', 'File Filter', and 'SSL Inspection'. The 'Logging Options' section includes 'Log Allowed Traffic', 'Security Events', and 'All Sessions'. The 'Comments' field is empty. The 'Enable this policy' checkbox is checked. The 'Additional Information' section on the right includes 'API Preview' and 'Documentation' links.

- e. Configure the remaining options as needed.
- f. Click *OK*.
4. On the ZTNA rules list, make sure that the deny rule (*ZTNA-Deny-malicious*) is above the allow rule (*proxy-WIN2K16-P1*).

To configure a firewall policy for full ZTNA in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Set *Name* to *ZTNA-P1*.
3. Enable *ZTNA* and select *Full ZTNA*.
4. Set *Incoming Interface* to *port1*.
5. Set *ZTNA Server* to *WIN2K16-P1*.
6. Configure the remaining settings as needed.
UTM processing of the traffic happens at the ZTNA rule.
7. Click *OK*.

To configure HTTPS access in the CLI:

1. Configure the access proxy VIP:

```
config firewall vip
    edit "WIN2K16-P1"
        set type access-proxy
        set extip 192.168.2.86
        set extintf "port1"
        set server-type https
        set extport 8443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the server and path mapping:

```
config firewall access-proxy
    edit "WIN2K16-P1"
        set vip "WIN2K16-P1"
        set client-cert enable
        config api-gateway
            edit 1
                set service https
                config realservers
                    edit 1
                        set ip 192.168.20.6
                        set port 443
                    next
                end
            next
        end
    next
end
```

3. Configure ZTNA rules:

```
config firewall proxy-policy
    edit 3
        set name "ZTNA-Deny-malicious"
        set proxy access-proxy
        set access-proxy "WIN2K16-P1"
        set srcaddr "all"
        set dstaddr "all"
```

```
        set ztna-ems-tag "FCTEMS0000109188_Malicious-File-Detected"
        set schedule "always"
        set logtraffic all
    next
    edit 2
        set name "proxy-WIN2K16-P1"
        set proxy access-proxy
        set access-proxy "WIN2K16-P1"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "FCTEMS0000109188_Low"
        set action accept
        set schedule "always"
        set logtraffic all
    next
end
```

4. Configure a firewall policy for full ZTNA:

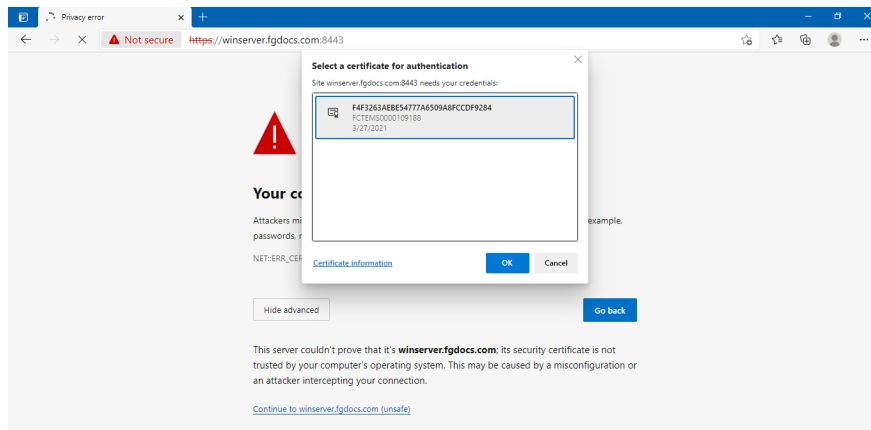
```
config firewall policy
    edit 24
        set name "ZTNA-P1"
        set srcintf "port1"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "WIN2K16-P1"
        set action accept
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set nat enable
    next
end
```

Testing the remote access to the HTTPS access proxy

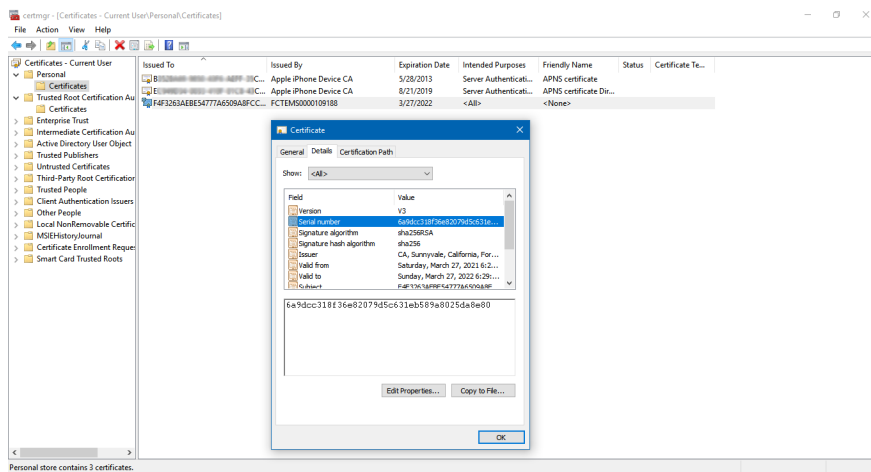
After FortiClient EMS and FortiGate are configured, the HTTPS access proxy remote connection can be tested.

Access allowed:

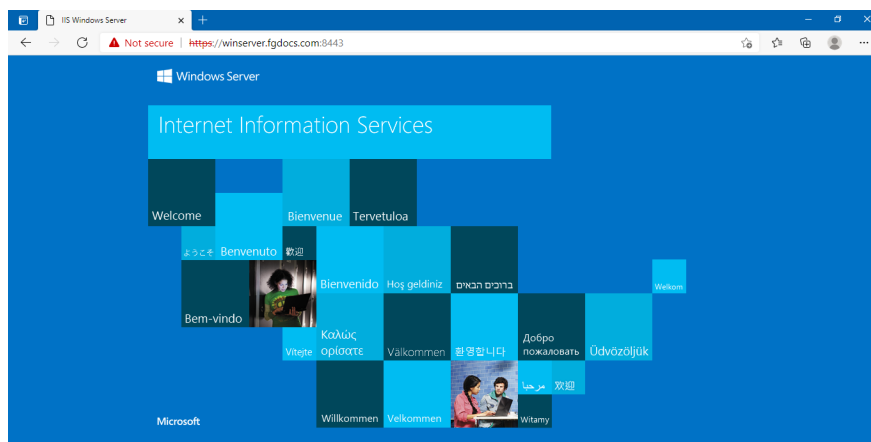
1. On the remote Windows PC, open FortiClient.
2. On the *Zero Trust Telemetry* tab, make sure that you are connected to the EMS server.
3. Open a browser and enter the address of the server and the access port. When entering the FQDN, make sure that the DNS can resolve the address to the IP address of the FortiGate. In this example, winserver.fgdocs.com resolves to 192.168.2.86.
4. The browser prompts for the client certificate to use. Select the EMS signed certificate, then click *OK*.



The certificate is in the *User Configuration* store, under *Personal > Certificates*. The details show the SN of the certificate, which matches the record on the FortiClient EMS and the FortiGate.



5. The client is verified by the FortiGate to authenticate your identity.
6. The FortiGate matches your security posture by verifying your ZTNA tag and matching the corresponding ZTNA rule, and you are allowed access to the web server.



Access denied:

1. On the remote Windows PC, trigger the Zero Trust Tagging Rule by creating the file in C:\virus.txt.
2. Open a browser and enter the address <http://winserver.fgdocs.com:8443>.
3. The client is verified by the FortiGate to authenticate your identity.
4. FortiGate checks your security posture. Because EMS has tagged the PC with the *Malicious-File-Detected* tag, it matches the *ZTNA-Deny-malicious* rule.
5. You are denied access to the web server.

**Access Denied**

The page you requested has been blocked by a firewall policy restriction.

Logs and debugs**Access allowed:**

```
# diagnose endpoint record list
```

```
Record #1:
```

```
IP Address = 10.10.10.20
MAC Address = 9c:b7:0d:2d:5c:d1
MAC list = 24:b6:fd:fa:54:c1;06:15:cd:45:f1:2e;9c:b7:0d:2d:5c:d1;
VDOM = (-1)
EMS serial number: FCTEMS0000109188
Client cert SN: 6A9DCC318F36E82079D5C631EB589A8025DA8E80
Public IP address: 192.157.105.35
Quarantined: no
Online status: online
Registration status: registered
On-net status: on-net
Gateway Interface:
FortiClient version: 7.0.0
AVDB version: 0.0
FortiClient app signature version: 0.0
FortiClient vulnerability scan engine version: 2.30
FortiClient UID: F4F3263AEBE54777A6509A8FCCDF9284
Host Name: Fortinet-KeithL
OS Type: WIN64
```

```
...
```

```
Number of Routes: (0)
```

```
online records: 1; offline records: 0; quarantined records: 0
```

```
# diagnose test application fcnacd 7
```

```
ZTNA Cache:
```

```
-uid F4F3263AEBE54777A6509A8FCCDF9284: { "tags": [ "all_registered_clients", "Low" ], "user_
name": "keithli", "client_cert_sn": "6A9DCC318F36E82079D5C631EB589A8025DA8E80", "ems_sn":
"FCTEMS0000109188" }
```



```
# diagnose endpoint wad-comm find-by uid F4F3263AEBE54777A6509A8FCCDF9284
UID: F4F3263AEBE54777A6509A8FCCDF9284
    status code:ok
    Domain:
    User: keithli
    Cert SN:6A9DCC318F36E82079D5C631EB589A8025DA8E80
    EMS SN: FCTEMS0000109188
    Routes(0):
    Tags(2):
        - tag[0]: name=all_registered_clients
        - tag[1]: name=Low

# execute log display
1: date=2021-03-28 time=00:46:39 eventtime=1616917599923614599 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.10.10.20 srcport=60185
srcintf="port1" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved"
dstip=192.168.20.6 dstport=443 dstintf="root" dstintfrole="undefined" sessionid=29515
srcuid="2d8e1736-8ec6-51eb-885c-009bdf9c31d7" dstuid="5445be2e-5d7b-51ea-e2c3-
ae6b7855c52f" service="HTTPS" wanoptapptype="web-proxy" proto=6 action="accept" policyid=2
policytype="proxy-policy" poluid="5aba29de-8ec6-51eb-698f-25b59d5bf852" duration=6
wanin=104573 rcvdbyte=104573 wanout=2274 lanin=3370 sentbyte=3370 lanout=104445
srchwvendor="Fortinet" devtype="Network" srcfamily="Firewall" osname="Windows"
srchwversion="FortiWiFi-30E" appcat="unscanned"
```

Access denied:

```
# diagnose test application fcnacd 7
ZTNA Cache:
-uid F4F3263AEBE54777A6509A8FCCDF9284: { "user_name": "keithli", "client_cert_sn":
"6A9DCC318F36E82079D5C631EB589A8025DA8E80", "ems_sn": "FCTEMS0000109188", "tags": [
"Malicious-File-Detected", "all_registered_clients", "Low" ] }

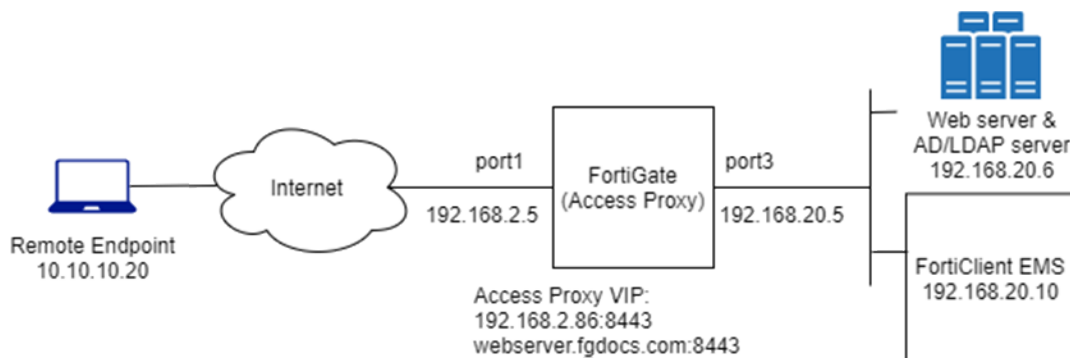
# diagnose endpoint wad-comm find-by uid F4F3263AEBE54777A6509A8FCCDF9284
UID: F4F3263AEBE54777A6509A8FCCDF9284
    status code:ok
    Domain:
    User: keithli
    Cert SN:6A9DCC318F36E82079D5C631EB589A8025DA8E80
    EMS SN: FCTEMS0000109188
    Routes(0):
    Tags(3):
        - tag[0]: name=Malicious-File-Detected
        - tag[1]: name=all_registered_clients
        - tag[2]: name=Low

# execute log display
1: date=2021-03-28 time=01:21:55 eventtime=1616919715444980633 tz="-0700" logid="0000000013"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.10.10.20 srcport=60784
srcintf="port1" srcintfrole="wan" dstip=192.168.20.6 dstport=443 dstintf="root"
dstintfrole="undefined" srcuid="2d8e1736-8ec6-51eb-885c-009bdf9c31d7" dstuid="5445be2e-
5d7b-51ea-e2c3-ae6b7855c52f" srccountry="Reserved" dstcountry="Reserved" sessionid=33933
proto=6 action="deny" policyid=3 policytype="proxy-policy" poluid="762ca074-8f9e-51eb-7614-
03a8801c6477" service="HTTPS" trandisp="noop" url="https://winserver.fgdocs.com/"
agent="Chrome/89.0.4389.90" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
appcat="unscanned" crscore=30 craction=131072 crlevel="high" msg="Traffic denied because of
explicit proxy policy"
```

ZTNA HTTPS access proxy with basic authentication example

This example expands on the previous example ([ZTNA HTTPS access proxy example on page 299](#)), adding LDAP authentication to the ZTNA rule. Users are allowed based on passing the client certificate authentication check, user authentication, and security posture check.

Users that are in the AD security group *ALLOWED-VPN* are allowed access to the access proxy. Users that are not part of this security group are not allowed access.



This example assumes that the FortiGate EMS fabric connector is already successfully connected.

LDAP/Active Directory Users and Groups:

- Domain: KLHOME.local
- Users (Groups):
 - radCurtis (Domain Users, ALLOWED-VPN)
 - radKeith (Domain Users)

To configure a secure connection to the LDAP server in the GUI:

1. Go to *User & Authentication > LDAP Servers* and click *Create New*.
2. Configure the following settings:

Name	WIN2K16-KLHOME-LDAPS
Server IP/Name	192.168.20.6
Server Port	636
Common Name Identifier	sAMAccountName
Distinguished Name	dc=KLHOME,dc=local
Exchange server	Disabled
Bind Type	Regular Enter the <i>Username</i> and <i>Password</i> for LDAP binding and lookup.
Secure Connection	Enabled <ul style="list-style-type: none"> • Set <i>Protocol</i> to <i>LDAPS</i> • Enable <i>Certificate</i> and select the CA certificate to validate the server certificate.

Server identity check

Optionally, enable to verify the domain name or IP address against the server certificate.

3. Click *Test Connectivity* to verify the connection to the server.
4. Click *OK*.

To configure a secure connection to the LDAP server in the CLI:

```
config user ldap
    edit "WIN2K16-KLHOME-LDAPS"
        set server "192.168.20.6"
        set cnid "sAMAccountName"
        set dn "dc=KLHOME,dc=local"
        set type regular
        set username "KLHOME\Administrator"
        set password <password>
        set secure ldaps
        set ca-cert "CA_Cert_1"
        set port 636
    next
end
```

To configure a remote user group from the LDAP server in the GUI:

1. Go to *User & Authentication > User Groups* and click *Create New*.
2. Set the name to *KLHOME-ALLOWED-VPN*.
3. Set *Type* to *Firewall*.
4. In the *Remote Groups* table click *Add*:
 - a. Set *Remote Server* to *WIN2K16-KLHOME-LDAPS*.
 - b. Locate the *ALLOWED-VPN* group, right-click on it, and click *Add Selected*.
 - c. Click *OK*.

5. Click OK.

To configure a remote user group from the LDAP server in the CLI:

```
config user group
  edit "KLHOME-ALLOWED-VPN"
    set member "WIN2K16-KLHOME-LDAPS"
    config match
      edit 1
        set server-name "WIN2K16-KLHOME-LDAPS"
        set group-name "CN=ALLOWED-VPN,DC=KLHOME,DC=local"
      next
    end
  next
end
```

Authentication scheme and rules

After the LDAP server and user group have been configured, an authentication scheme and rule must be configured.



To configure authentication schemes and rules in the GUI, go to *System > Feature Visibility* and enable *Explicit Proxy*.

Authentication scheme

The authentication scheme defines the method of authentication that is applied. In this example, basic HTTP authentication is used so that users are prompted for a username and password the first time that they connect to a website through the HTTPS access proxy.

To configure an authentication scheme in the GUI:

1. Go to *Policy & Objects > Authentication Rules* and click *Create New > Authentication Scheme*.
2. Set the name to *ZTNA-Auth-scheme*.
3. Set *Method* to *Basic*.
4. Set *User database* to *Other* and select *WIN2K16-KLHOME-LDAPS* as the LDAP server.
5. Click OK.

To configure an authentication scheme in the CLI:

```
config authentication scheme
  edit "ZTNA-Auth-scheme"
    set method basic
    set user-database "WIN2K16-KLHOME-LDAPS"
  next
end
```

Authentication rule

The authentication rule defines the proxy sources and destination that require authentication, and what authentication scheme is applied. In this example, active authentication through the basic HTTP prompt is used and applied to all sources.

To configure an authentication rule in the GUI:

1. Go to *Policy & Objects > Authentication Rules* and click *Create New > Authentication Rule*.
2. Set the name to *ZTNA-Auth-rule*.
3. Set *Source Address* to *all*.
4. Set *Protocol* to *HTTP*.
5. Enable *Authentication Scheme* and select *ZTNA-Auth-scheme*.
6. Click *OK*.

To configure an authentication rule in the CLI:

```
config authentication rule
  edit "ZTNA-Auth-rule"
    set srcaddr "all"
    set active-auth-method "ZTNA-Auth-scheme"
  next
end
```

Applying the user group to a ZTNA rule

A user or user group must be applied to the ZTNA rule that you need to control user access to. The authenticated user from the authentication scheme and rule must match the user or user group in the ZTNA rule.

In this example, the user group is applied to the two ZTNA rules that were configured in [ZTNA HTTPS access proxy example on page 299](#).

To apply a user group to the ZTNA rules in the GUI:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Rules* tab.
2. Edit the *ZTNA-Deny-malicious* rule.
3. Click in the *Source* field, select the *User* tab, select the *KLHOME-ALLOWED-VPN* group, then click *Close*.
4. Click *OK*.
5. Edit the *proxy-WIN2K16-P1* rule.
6. Click in the *Source* field, select the *User* tab, select the *KLHOME-ALLOWED-VPN* group, then click *Close*.
7. Click *OK*.

To apply a user group to the ZTNA rules in the CLI:

```

config firewall proxy-policy
  edit 3
    set name "ZTNA-Deny-malicious"
    set proxy access-proxy
    set access-proxy "WIN2K16-P1"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag "FCTEMS0000109188_Malicious-File-Detected"
    set schedule "always"
    set logtraffic all
    set groups "KLHOME-ALLOWED-VPN"
  next
  edit 2
    set name "proxy-WIN2K16-P1"
    set proxy access-proxy
    set access-proxy "WIN2K16-P1"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag "FCTEMS0000109188_Low"
    set action accept
    set schedule "always"
    set logtraffic all
    set groups "KLHOME-ALLOWED-VPN"
  next
end

```

Testing remote access to the HTTPS access proxy with user authentication**Scenario 1: access allowed - user radCurtis**

1. On a remote Windows PC, open the FortiClient app, select the *Zero Trust Telemetry* tab, and confirm that you are connected to the EMS server.
2. In a browser, enter the address of the server and the access port.
If entering an FQDN, make sure that DNS can resolve the address to the IP address of the FortiGate. In this example, *winserver.fgdocs.com* resolves to 192.168.2.86.
3. When the browser asks for the client certificate to use, select the EMS signed certificate, then click *OK*.
The client certificate is verified by the FortiGate to authenticate your identity.
4. When prompted, enter the username *radCurtis* and the password, and click *Sign in*.
As *radCurtis* is a member of the *ALLOWED-VPN* group in Active Directory, it will match the *KLHOME-ALLOWED-VPN* user group. After the user authentication passes, the FortiGate performs a posture check on the ZTNA group. When that passes, you are allowed access to the website.

Verifying the results

```

# diagnose firewall auth list

10.10.10.20, radCurtis
  type: fw, id: 0, duration: 13, idled: 13
  expire: 587, allow-idle: 600
  packets: in 0 out 0, bytes: in 0 out 0

```

```

group_id: 8 16777220
group_name: KLHOME-ALLOWED-VPN grp_16777220

# diagnose test application fcnacd 7
ZTNA Cache:
-uid F4F3263AEBE54777A6509A8FCCDF9284: { "tags": [ "all_registered_clients", "Low" ], "user_
name": "keith", "client_cert_sn": "6C7433E8E2CEDEB49B6C3C3C03677A3521EA4486", "ems_sn":
"FCTEMS0000109188" }

```



The `user_name` is the windows log in username learned by FortiClient. It might not match the username used in firewall user authentication.

```

# execute log display

1: date=2021-04-13 time=00:11:56 eventtime=1618297916023667886 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.10.10.20 srcport=51513
srcintf="port1" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved"
dstip=192.168.20.6 dstport=443 dstintf="root" dstintfrole="undefined" sessionid=2319197
srcuuid="2d8e1736-8ec6-51eb-885c-009bdf9c31d7" dstuuid="5445be2e-5d7b-51ea-e2c3-
ae6b7855c52f" service="HTTPS" wanoptaptype="web-proxy" proto=6 action="accept" policyid=2
policytype="proxy-policy" poluuid="5aba29de-8ec6-51eb-698f-25b59d5bf852" duration=10
user="radCurtis" group="KLHOME-ALLOWED-VPN" authserver="WIN2K16-KLHOME-LDAPS" wanin=104573
rcvdbyte=104573 wanout=2364 lanin=3538 sentbyte=3538 lanout=104445 appcat="unscanned"

```

Scenario 2: access denied – user radKeith

- If scenario 1 has just been tested, log in to the FortiGate and deauthenticate the user:
 - Go to *Dashboard > Users & Devices* and expand the *Firewall Users* widget.
 - Right-click on the user *radCurtis* and select deauthenticate.
- On a remote Windows PC, open the FortiClient app, select the *Zero Trust Telemetry* tab, and confirm that you are connected to the EMS server.
- In a browser, enter the address *winserver.fgdocs.com*.
- When the browser asks for the client certificate to use, select the EMS signed certificate, then click *OK*. This option might not appear if you have already selected the certificate when testing scenario 1.
The client certificate is verified by the FortiGate to authenticate your identity.
- When prompted, enter the username *radKeith* and the password, and click *Sign in*.
As *radKeith* is not a member of the *ALLOWED-VPN* group in Active Directory, it will not match the *KLHOME-ALLOWED-VPN* user group. Because no other policies are matched, this user is implicitly denied

Verifying the results

Go to *Dashboard > Users & Devices*, expand the *Firewall Users* widget, and confirm that user *radKeith* is listed, but no applicable user group is returned.

```

# execute log display

1: date=2021-04-13 time=12:29:21 eventtime=1618342161821542277 tz="-0700" logid="0000000013"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.10.10.20 srcport=52571
srcintf="port1" srcintfrole="wan" dstip=192.168.20.6 dstport=443 dstintf="root"
dstintfrole="undefined" srcuuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f" srccountry="Reserved"

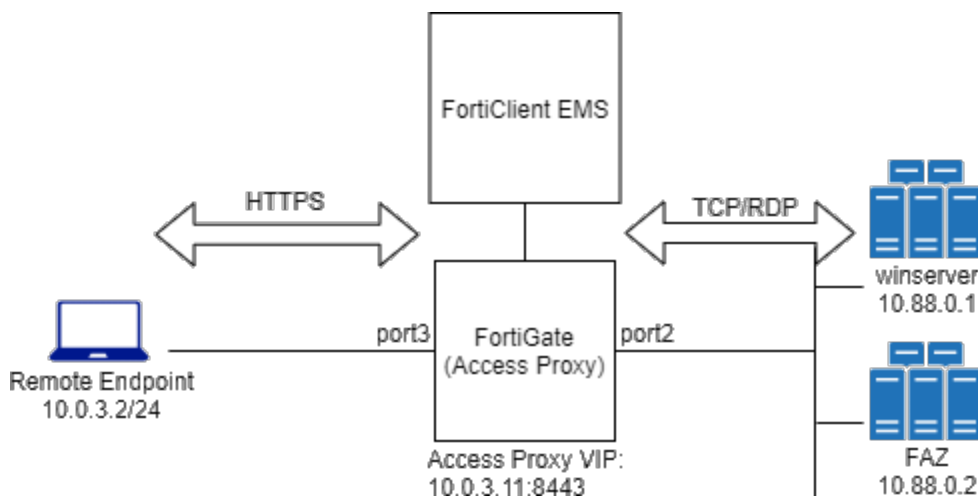
```

```
dstcountry="Reserved" sessionid=2394329 proto=6 action="deny" policyid=0 policytype="proxy-policy" user="radKeith" authserver="WIN2K16-KLHOME-LDAPS" service="HTTPS" trandisp="noop" url="https://winserver.fgdocs.com/" agent="Chrome/89.0.4389.114" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" crscore=30 craction=131072 crlevel="high" msg="Traffic denied because of explicit proxy policy"
```

ZTNA TCP forwarding access proxy example

In this example, a TCP forwarding access proxy (TFAP) is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and the FortiGate over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source.

RDP access is configured to one server, and SSH access to the other.



This example assumes that the FortiGate EMS fabric connector is already successfully connected.

To configure the access proxy VIP:

```
config firewall vip
    edit "ZTNA-tcp-server"
        set type access-proxy
        set extip 10.0.3.11
        set extintf "port3"
        set server-type https
        set extport 8443
        set ssl-certificate "Fortinet_SSI"
    next
end
```

To configure the server addresses:

```
config firewall address
    edit "FAZ"
        set subnet 10.88.0.2 255.255.255.255
    next
    edit "winserver"
        set subnet 10.88.0.1 255.255.255.255
    next
end
```



```
    next
end
```

To configure access proxy server mappings:

```
config firewall access-proxy
    edit "ZTNA-tcp-server"
        set vip "ZTNA-tcp-server"
        set client-cert enable
        config api-gateway
            edit 1
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "FAZ"
                        set mappedport 22
                    next
                edit 2
                    set address "winserver"
                    set mappedport 3389
                next
            end
        next
    end
end
next
end
```

The mapped port (`mappedport`) restricts the mapping to the specified port or port range. If `mappedport` is not specified, then any port will be matched.

To configure a ZTNA rule (proxy policy):

```
config firewall proxy-policy
    edit 0
        set name "ZTNA_remote"
        set proxy access-proxy
        set access-proxy "ZTNA-tcp-server"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
    next
end
```

To configure a firewall policy for full ZTNA:

```
config firewall policy
    edit 1
        set name "Full_ZTNA_policy"
        set srcintf "port3"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "ZTNA-tcp-server"
        set action accept
```

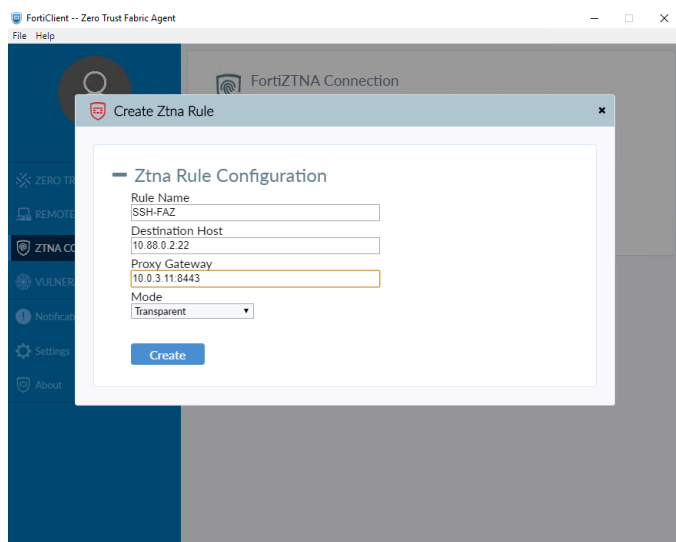
```
set schedule "always"  
set service "ALL"  
set inspection-mode proxy  
set logtraffic all  
next  
end
```

Test the connection to the access proxy

Before connecting, users must create a ZTNA rule in FortiClient.

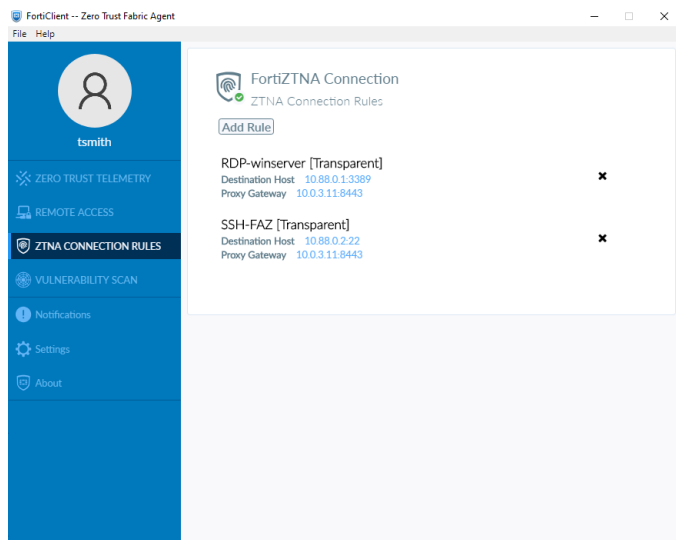
To create a ZTNA rule in FortiClient:

1. On the *ZTNA Connection Rules* tab, click *Add Rule*.
2. Set *Rule Name* to *SSH-FAZ*.
3. Set *Destination Host* to *10.88.0.2:22*. This is the real IP address and port of the server.
4. Set *Proxy Gateway* to *10.0.3.11:8443*. This is the access proxy address and port that are configured on the FortiGate.

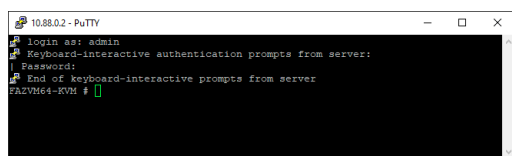


5. Click *Create*.
6. Create a second rule with the following settings:
 - *Rule Name*: *RDP_winserver*
 - *Destination Host*: *10.88.0.1:3389*

- **Proxy Gateway: 10.0.3.11:8443**



After creating the ZTNA connection rules, you can SSH and RDP directly to the server IP address and port.



Logs

RDP:

```
1: date=2021-03-24 time=23:42:35 eventtime=1616654555724552835 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.0.3.2 srcport=50284
srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved"
dstip=10.88.0.1 dstport=3389 dstintf="root" dstintfrole="undefined" sessionid=109099
service="RDP" wanoptapptype="web-proxy" proto=6 action="accept" policyid=3
policytype="proxy-policy" poluuid="fe0e1ae8-bdf9-51eb-b86f-c5e2adb934b3" duration=13
wanin=1751 rcvdbyte=1751 wanout=1240 lanin=3034 sentbyte=3034 lanout=3929 appcat="unscanned"
```

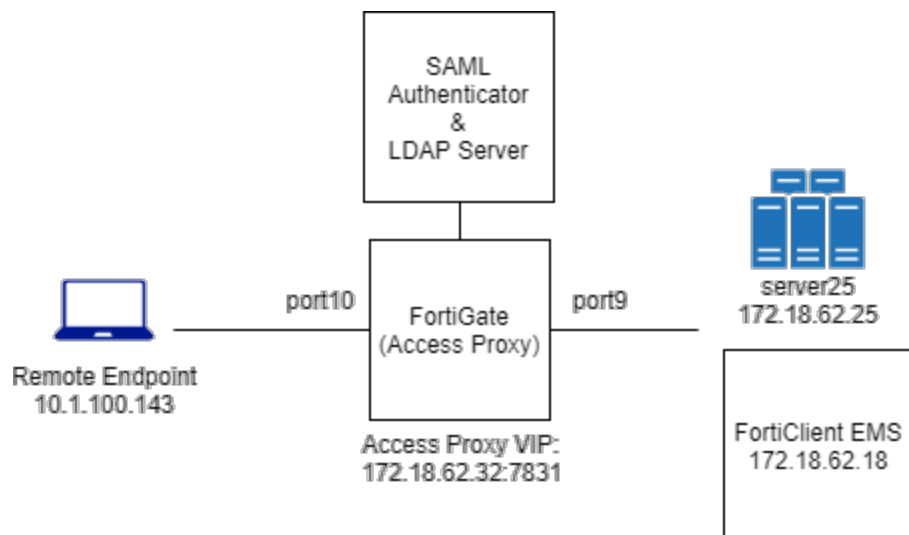
SSH:

```
1: date=2021-03-24 time=23:44:13 eventtime=1616654653388681007 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.0.3.2 srcport=50282
srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved"
dstip=10.88.0.2 dstport=22 dstintf="root" dstintfrole="undefined" sessionid=109027
service="SSH" wanoptapptype="web-proxy" proto=6 action="accept" policyid=3
policytype="proxy-policy" poluuid="fe0e1ae8-bdf9-51eb-b86f-c5e2adb934b3" duration=134
wanin=5457 rcvdbyte=5457 wanout=2444 lanin=4478 sentbyte=4478 lanout=7943 appcat="unscanned"
```

ZTNA proxy access with SAML authentication example

In this example, an HTTPS access proxy is configured, and SAML authentication is applied to authenticate the client. The FortiGate acts as the SAML SP and a SAML authenticator serves as the IdP. In addition to verifying the user and

device identity with the client certificate, the user is also authorized based on user credentials to establish a trust context before granting access to the protected resource.



This example assumes that the FortiGate EMS fabric connector is already successfully connected.

To configure the access proxy VIP:

```

config firewall vip
    edit "ZTNA_server01"
        set type access-proxy
        set extip 172.18.62.32
        set extintf "any"
        set server-type https
        set extport 7831
        set ssl-certificate "Fortinet_CA_SSL"
    next
end
  
```

To configure access proxy server mappings:

```

config firewall access-proxy
    edit "ZTNA_server01"
        set vip "ZTNA_server01"
        set client-cert enable
        config api-gateway
            edit 1
                set service https
                config realservers
                    edit 1
                        set ip 172.18.62.25
                        set port 443
                    next
                end
            next
        end
    next
end
next
end
  
```

To configure a firewall policy for full ZTNA:

```
config firewall policy
  edit 2
    set name "Full_ZTNA_policy"
    set srcintf "port10"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "ZTNA_server01"
    set action accept
    set schedule "always"
    set service "ALL"
    set inspection-mode proxy
    set nat enable
  next
end
```

To configure a SAML server:

```
config user saml
  edit "saml_ztna"
    set cert "Fortinet_CA_SSL"
    set entity-id "https://fgt9.myqalab.local:7831/samlap"
    set single-sign-on-url "https://fgt9.myqalab.local:7831/XX/YY/ZZ/saml/login/"
    set single-logout-url "https://fgt9.myqalab.local:7831/XX/YY/ZZ/saml/logout/"
    set idp-entity-id "http://MYQALAB.LOCAL/adfs/services/trust"
    set idp-single-sign-on-url "https://myqalab.local/adfs/ls"
    set idp-single-logout-url "https://myqalab.local/adfs/ls"
    set idp-cert "REMOTE_Cert_4"
    set digest-method sha256
    set adfs-claim enable
    set user-claim-type upn
    set group-claim-type group-sid
  next
end
```

To map the SAML server into an access proxy configuration:

```
config firewall access-proxy
  edit "ZTNA_server01"
    config api-gateway
      edit 3
        set service samlsp
        set saml-server "saml_ztna"
      next
    end
  next
end
```

To configure an LDAP server and an LDAP server group to verify user groups:

```
config user ldap
  edit "ldap-10.1.100.198"
    set server "10.1.100.198"
    set cnid "cn"
```

```
        set dn "dc=myqalab,dc=local"
        set type regular
        set username "cn=fosqa1,cn=users,dc=myqalab,dc=local"
        set password *****
        set group-search-base "dc=myqalab,dc=local"
    next
end

config user group
    edit "ldap-group-saml"
        set member "ldap-10.1.100.198"
    next
end
```

To configure the authentication settings, rule, and scheme to match the new SAML server:

```
config authentication setting
    set active-auth-scheme "saml_ztna"
    set captive-portal "fgt9.myqalab.local"
end

config authentication rule
    edit "saml_ztna"
        set srcintf "port10"
        set srcaddr "all"
        set ip-based disable
        set active-auth-method "saml_ztna"
        set web-auth-cookie enable
    next
end

config authentication scheme
    edit "saml_ztna"
        set method saml
        set saml-server "saml_ztna"
        set saml-timeout 30
        set user-database "ldap-10.1.100.198"
    next
end
```

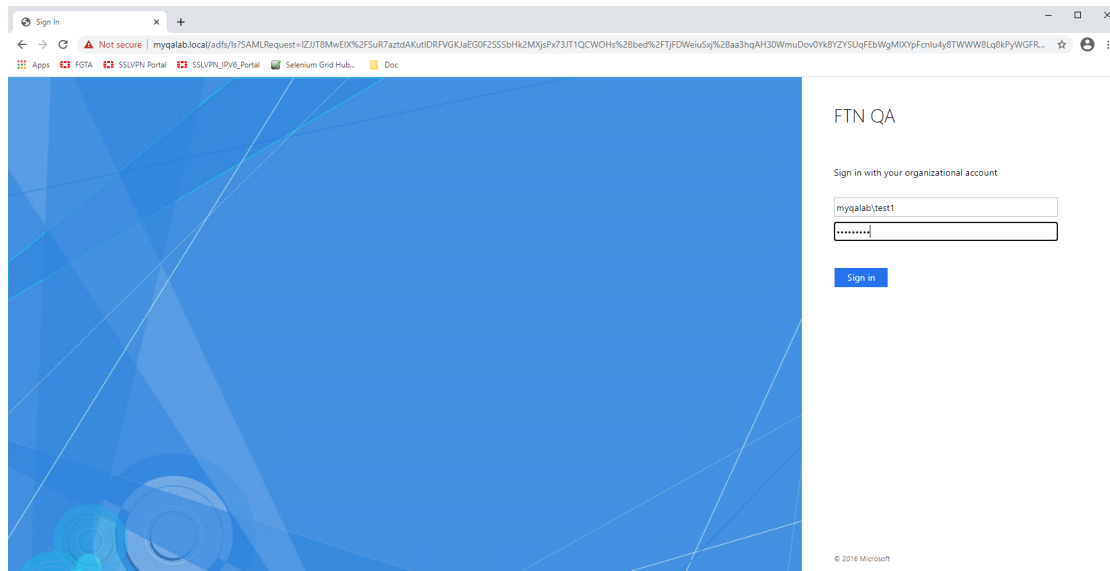
To enable user group authentication in an access-proxy type firewall proxy-policy:

```
config firewall proxy-policy
    edit 6
        set name "ZTNA_remote"
        set proxy access-proxy
        set access-proxy "ZTNA_server01"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set groups "ldap-group-saml"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
    next
end
```

Testing the connection

To test the connection:

1. On a client PC, try to access the webpage through the HTTPS access proxy. For example, go to `http://172.18.62.32:7831` in a browser.
2. The client PC is prompted for a client certificate. After the certificate is validated, you are redirected to a SAML log in portal.



3. Enter your user credentials. The SAML server authenticates and sends a SAML assertion response message to the FortiGate.
4. The FortiGate queries the LDAP server for the user group, and then verifies the user group against the groups or groups defined in the proxy policy.
5. The user is proxied to the webpage on the real web server.

Logs and debugs

Use the following command to check the user information after the user has been authenticated:

```
# diagnose wad user list
ID: 7, VDOM: vdom1, IPv4: 10.1.100.143
  user name   : test1@MYQALAB.local
  worker      : 0
  duration    : 124
  auth_type   : Session
  auth_method : SAML
  pol_id      : 6
  g_id        : 13
  user_based  : 0
  expire      : no
LAN:
  bytes_in=25953 bytes_out=14158
WAN:
  bytes_in=8828 bytes_out=6830
```

Event log:

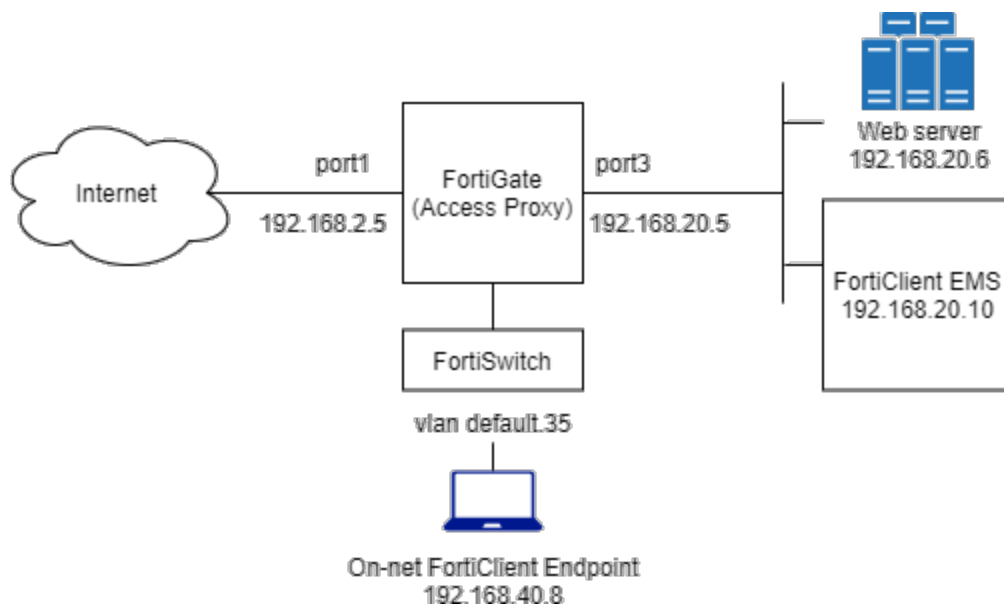
```
1: date=2021-03-24 time=19:02:21 eventtime=1616637742066893182 tz="-0700" logid="0102043025"
type="event" subtype="user" level="notice" vd="vdom1" logdesc="Explicit proxy authentication
successful" srcip=10.1.100.143 dstip=172.18.62.32 authid="saml" user="test1@MYQALAB.local"
group="N/A" authproto="HTTP(10.1.100.143)" action="authentication" status="success"
reason="Authentication succeeded" msg="User test1@MYQALAB.local succeeded in authentication"
```

Traffic log:

```
1: date=2021-03-24 time=19:09:06 eventtime=1616638146541253587 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="vdom1" srcip=10.1.100.143 srcport=58084
srcintf="port10" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.62.25 dstport=443 dstintf="vdom1" dstintfrole="undefined" sessionid=8028
service="HTTPS" wanoptapptype="web-proxy" proto=6 action="accept" policyid=6
policytype="proxy-policy" poluid="8dcfe762-8d0b-51eb-82bf-bfbee59b89f2" duration=8
user="test1@MYQALAB.local" group="ldap-group-saml" authserver="ldap-10.1.100.198"
wanin=10268 rcvdbyte=10268 wanout=6723 lanin=7873 sentbyte=7873 lanout=10555
appcat="unscanned"
```

ZTNA IP MAC filtering example

In this example, firewall policies in ZTNA IP/MAC filtering mode are configured that use ZTNA tags to control access between on-net devices and an internal web server. This mode does not require the use of the access proxy, and only uses ZTNA tags for access control. Traffic is passed when the FortiClient endpoint is tagged as *Low* risk only. Traffic is denied when the FortiClient endpoint is tagged with *Malicious-File-Detected*.



This example assumes that the FortiGate EMS fabric connector is already successfully connected.



To configure ZTNA in the GUI, go to *System > Feature Visibility* and enable *Zero Trust Network Access*.

To configure a Zero Trust tagging rule on the FortiClient EMS:

1. Log in to the FortiClient EMS.
2. Go to *Zero Trust Tags > Zero Trust Tagging Rules*, and click *Add*.
3. In the *Name* field, enter *Malicious-File-Detected*.
4. In the *Tag Endpoint As* dropdown list, select *Malicious-File-Detected*.

EMS uses this tag to dynamically group together endpoints that satisfy the rule, as well as any other rules that are configured to use this tag.

5. Click *Add Rule* then configure the rule:
 - a. For OS, select *Windows*.
 - b. From the *Rule Type* dropdown list, select *File* and click the + button.
 - c. Enter a file name, such as *C:\virus.txt*.
 - d. Click *Save*.

FortiClient Endpoint Management Server

Invitations 3 admin

Dashboard > Endpoints > Deployment & Installers > Endpoint Policy & Components > Endpoint Profiles > **Zero Trust Tags** > **Zero Trust Tagging Rules** > Zero Trust Tag Monitor > Fabric Device Monitor > Quarantine Management > Administration > System Settings >

Zero Trust Tagging Rule Set

Name:

Tag Endpoint As:

Enabled: ☒

Comments:

Rules + Add Rule

Type	Value
Windows (1)	c:\virus.txt

6. Click *Save*.

To configure a firewall policy in ZTNA IP/MAC filtering mode to block access in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Set *Name* to *block-internal-malicious-access*.
3. Enable *ZTNA* and select *IP/MAC filtering*.
4. Set *ZTNA Tag* to *Malicious-File-Detected*.
5. Set *Incoming Interface* to *default.35*.
6. Set *Outgoing Interface* to *port3*.
7. Set *Source* and *Destination* to *all*.
8. Set *Service* to *ALL*.
9. Set *Action* to *DENY*.
10. Enable *Log Violation Traffic*.
11. Configuring the remaining settings as needed.
12. Click *OK*.

To configure a firewall policy in ZTNA IP/MAC filtering mode to allow access in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Set *Name* to *allow-internal-access*.
3. Enable *ZTNA* and select *IP/MAC filtering*.

4. Set *ZTNA Tag* to *Low*.
5. Set *Incoming Interface* to *default.35*.
6. Set *Outgoing Interface* to *port3*.
7. Set *Source* and *Destination* to *all*.
8. Set *Service* to *ALL*.
9. Set *Action* to *ACCEPT*.
10. Enable *Log Violation Traffic* and set it to *All Sessions*.
11. Configuring the remaining settings as needed.
12. Click *OK*.

To configure a firewall policies in ZTNA IP/MAC filtering mode to block and allow access in the CLI:

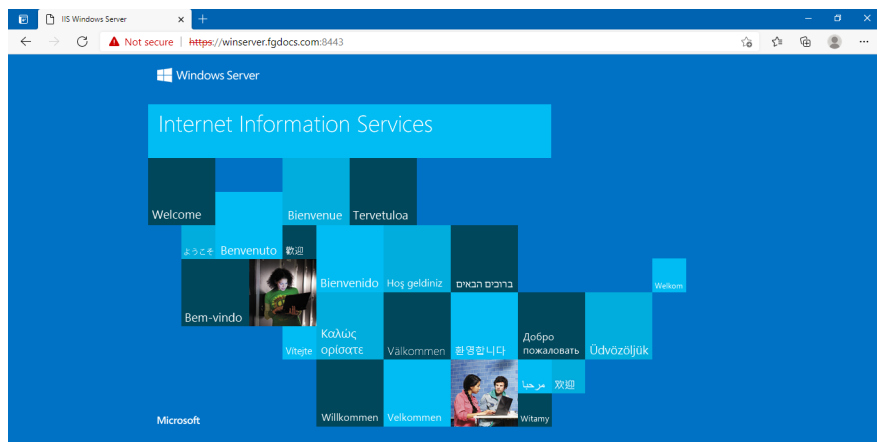
```
config firewall policy
  edit 29
    set name "block-internal-malicious-access"
    set srcintf "default.35"
    set dstintf "port3"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-status enable
    set ztna-ems-tag "FCTEMS0000109188_Malicious-File-Detected"
    set schedule "always"
    set service "ALL"
    set logtraffic all
  next
  edit 30
    set name "allow-internal-access"
    set srcintf "default.35"
    set dstintf "port3"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-status enable
    set ztna-ems-tag "FCTEMS0000109188_Low"
    set action accept
    set schedule "always"
    set service "ALL"
    set inspection-mode proxy
    set logtraffic all
    set nat enable
  next
end
```

Testing the access to the web server from the on-net client endpoint

Access allowed:

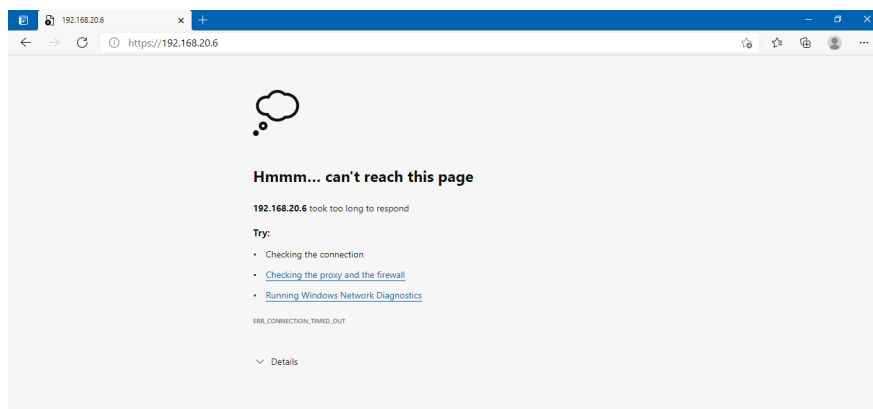
1. On the remote Windows PC, open FortiClient.
2. On the *Zero Trust Telemetry* tab, make sure that you are connected to the EMS server.
3. Open a browser and enter the address of the server.
4. The FortiGate matches your security posture by verifying your ZTNA tag and matching the corresponding `allow-`

internal-access firewall policy, and you are allowed access to the web server.



Access denied:

1. On the remote Windows PC, trigger the Zero Trust Tagging Rule by creating the file in C:\virus.txt.
2. Open a browser and enter the address of the server.
3. FortiGate checks your security posture. Because EMS has tagged the PC with the *Malicious-File-Detected* tag, it matches the *block-internal-malicious-access* firewall policy.
4. You are denied access to the web server.



Logs and debugs

Access allowed:

```
# diagnose endpoint record list
Record #1:
```

```
IP Address = 192.168.40.8
MAC Address = 24:b6:fd:fa:54:c1
MAC list = 24:b6:fd:fa:54:c1;54:15:cd:3f:f8:30;9c:b7:0d:2d:5c:d1;
VDOM = root (0)
EMS serial number: FCTEMS0000109188
Client cert SN: 563DA313367608678A3633E93C574F6F8BCB4A95
Public IP address: 192.157.105.35
Quarantined: no
Online status: online
```

```

    Registration status: registered
    On-net status: on-net
    Gateway Interface: default.35
    FortiClient version: 7.0.0
    AVDB version: 0.0
    FortiClient app signature version: 0.0
    FortiClient vulnerability scan engine version: 2.30
    FortiClient UID: F4F3263AEBE54777A6509A8FCCDF9284
    ...
    Number of Routes: (1)
        Gateway Route #0:
            - IP:192.168.40.8, MAC: 24:b6:fd:fa:54:c1, Indirect: no
            - Interface:default.35, VFID:0, SN: FGVMO4TM21000144
online records: 1; offline records: 0; quarantined records: 0

# diagnose endpoint wad-comm find-by ip-vdom 192.168.40.8 root
UID: F4F3263AEBE54777A6509A8FCCDF9284
    status code:ok
    Domain:
    User: keithli
    Cert SN:563DA313367608678A3633E93C574F6F8BCB4A95
    EMS SN: FCTEMS0000109188
    Routes(1):
        - route[0]: IP=192.168.40.8, VDom=root
    Tags(2):
        - tag[0]: name=all_registered_clients
        - tag[1]: name=Low

# diagnose firewall dynamic list
List all dynamic addresses:
FCTEMS0000109188_all_registered_clients: ID(51)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...

FCTEMS0000109188_Low: ID(78)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...

FCTEMS0000109188_Malicious-File-Detected: ID(190)
...

# diagnose test application fcnacd 7
ZTNA Cache:
-uid F4F3263AEBE54777A6509A8FCCDF9284: { "tags": [ "all_registered_clients", "Low" ], "user_
name": "keithli", "client_cert_sn": "563DA313367608678A3633E93C574F6F8BCB4A95", "gateway_
route_list": [ { "gateway_info": { "fgt_sn": "FGVM04TM21000144", "interface": "default.35",
"vdom": "root" }, "route_info": [ { "ip": "192.168.40.8", "mac": "24-b6-fd-fa-54-c1",
"route_type": "direct" } ] } ], "ems_sn": "FCTEMS0000109188" }

# execute log display
49 logs found.
10 logs returned.
3.5% of logs has been searched.
38: date=2021-03-28 time=23:07:38 eventtime=1616998058790134389 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=192.168.40.8 srcname="Fortinet-KeithL" srcport=51056 srcintf="default.35"

```

```
srcintfrole="undefined" dstip=192.168.20.6 dstport=443 dstintf="port3"
dstintfrole="undefined" srcuuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f" dstuuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f" srccountry="Reserved" dstcountry="Reserved" sessionid=161585
proto=6 action="close" policyid=30 policytype="policy" poluuid="8f6ea492-9034-51eb-f197-c00d803b7489" policyname="allow-internal-access" service="HTTPS" trandisp="snat"
transip=192.168.20.5 transport=51056 duration=2 sentbyte=3374 rcvdbyte=107732 sentpkt=50
rcvdpkt=80 fctuid="F4F3263AEBE54777A6509A8FCCDF9284" unauthuser="keithli"
unauthusersource="forticlient" appcat="unscanned" mastersrcmac="24:b6:fd:fa:54:c1"
srcmac="24:b6:fd:fa:54:c1" srcserver=0 dstosname="Windows" dstswversion="10"
masterdstmac="52:54:00:e3:4c:1a" dstmac="52:54:00:e3:4c:1a" dstserver=0
```

Access denied:

```
# diagnose endpoint wad-comm find-by ip-vdom 192.168.40.8 root
UID: F4F3263AEBE54777A6509A8FCCDF9284
    status code:ok
    Domain:
    User: keithli
    Cert SN:563DA313367608678A3633E93C574F6F8BCB4A95
    EMS SN: FCTEMS0000109188
    Routes(1):
    - route[0]: IP=192.168.40.8, VDom=root
Tags(3):
    - tag[0]: name=Malicious-File-Detected
    - tag[1]: name=all_registered_clients
    - tag[2]: name=Low

# diagnose firewall dynamic list
List all dynamic addresses:
FCTEMS0000109188_all_registered_clients: ID(51)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...
FCTEMS0000109188_Low: ID(78)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...
FCTEMS0000109188_Malicious-File-Detected: ID(190)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...

# diagnose test application fcnacd 7
ZTNA Cache:
-uid F4F3263AEBE54777A6509A8FCCDF9284: { "user_name": "keithli", "client_cert_sn":
"563DA313367608678A3633E93C574F6F8BCB4A95", "gateway_route_list": [ { "gateway_info": {
"fgt_sn": "FGVM04TM21000144", "interface": "default.35", "vdom": "root" }, "route_info": [ {
"ip": "192.168.40.8", "mac": "24-b6-fd-fa-54-c1", "route_type": "direct" } ] } ], "ems_sn":
"FCTEMS0000109188", "tags": [ "Malicious-File-Detected", "all_registered_clients", "Low" ] }

# execute log display
49 logs found.
10 logs returned.
3.5% of logs has been searched.

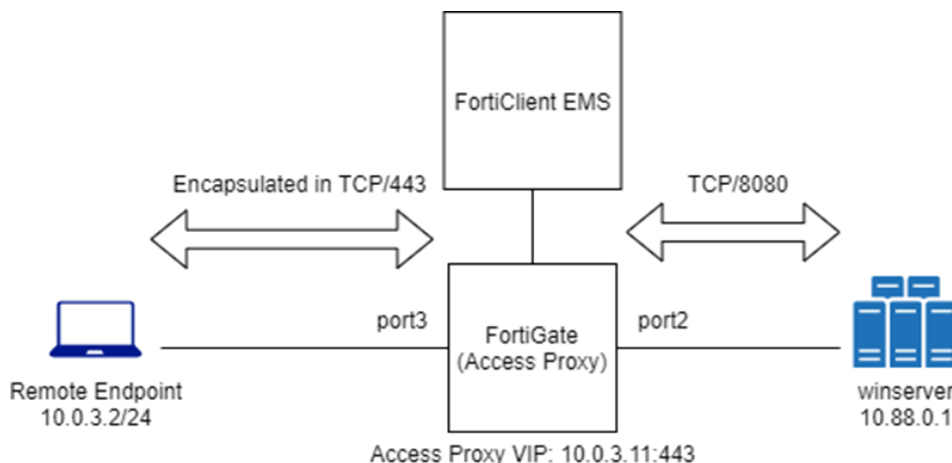
11: date=2021-03-28 time=23:14:41 eventtime=1616998481409744928 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
```

```
srcip=192.168.40.8 srcname="Fortinet-KeithL" srcport=51140 srcintf="default.35"
srcintfrole="undefined" dstip=192.168.20.6 dstport=443 dstintf="port3"
dstintfrole="undefined" srcuuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f" dstuuid="5445be2e-
5d7b-51ea-e2c3-ae6b7855c52f" srccountry="Reserved" dstcountry="Reserved" sessionid=162808
proto=6 action="deny" policyid=29 policytype="policy" poluuid="2835666c-9034-51eb-135d-
2f56e5f0f7a2" policyname="block-internal-malicious-access" service="HTTPS" trandisp="noop"
duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 fctuid="F4F3263AEBE54777A6509A8FCCDF9284"
unauthuser="keithli" unauthusersource="forticlient" appcat="unscanned" crscore=30
craction=131072 crlevel="high" mastersrcmac="24:b6:fd:fa:54:c1" srcmac="24:b6:fd:fa:54:c1"
srcserver=0
```

ZTNA TCP forwarding access proxy without encryption example - 7.0.1

TCP forwarding access proxy supports communication between the client and the access proxy without SSL/TLS encryption. The connection still begins with a TLS handshake. The client uses the HTTP 101 response to switch protocols and remove the HTTPS stack. Further end to end communication between the client and server are encapsulated in the specified TCP port, but not encrypted by the access proxy. This improves performance by reducing the overhead of encrypting an already secured underlying protocol, such as RDP, SSH, or FTPS. Users should still enable the encryption option for end to end protocols that are insecure.

In this example, the encryption option to access the web server on HTTP/8080 is disabled to show that traffic for an insecure connection protocol can be viewed in plain text in a protocol analyzer (such as Wireshark). In a real life application, the encryption option should be used for an insecure protocol.



To configure the access proxy VIP:

```
config firewall vip
  edit "ZTNA-tcp-server"
    set type access-proxy
    set extip 10.0.3.11
    set extintf "port3"
    set server-type https
    set extport 443
    set ssl-certificate "Fortinet_SSL"
  next
end
```

To configure the server addresses:

```
config firewall address
  edit "winserver"
    set subnet 10.88.0.1 255.255.255.255
  next
end
```

To configure access proxy server mappings:

```
config firewall access-proxy
  edit "ZTNA-tcp-server"
    set vip "ZTNA-tcp-server"
    set client-cert enable
    config api-gateway
      edit 1
        set service tcp-forwarding
        config realservers
          edit 2
            set address "winserver"
          next
        end
      next
    end
  next
end
```

The mapped port (mappedport) is not specified so that it will map any ports that are defined in FortiClient's ZTNA connection rule.

To configure a ZTNA rule (proxy policy):

```
config firewall proxy-policy
  edit 0
    set name "ZTNA-TCP"
    set proxy access-proxy
    set access-proxy "ZTNA-tcp-server"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set logtraffic all
  next
end
```

To configure a firewall policy for full ZTNA:

```
config firewall policy
  edit 0
    set name "ZTNA-TCP"
    set srcintf "port3"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "ZTNA-tcp-server"
    set action accept
    set schedule "always"
```

```

set service "ALL"
set inspection-mode proxy
set logtraffic all
next
end

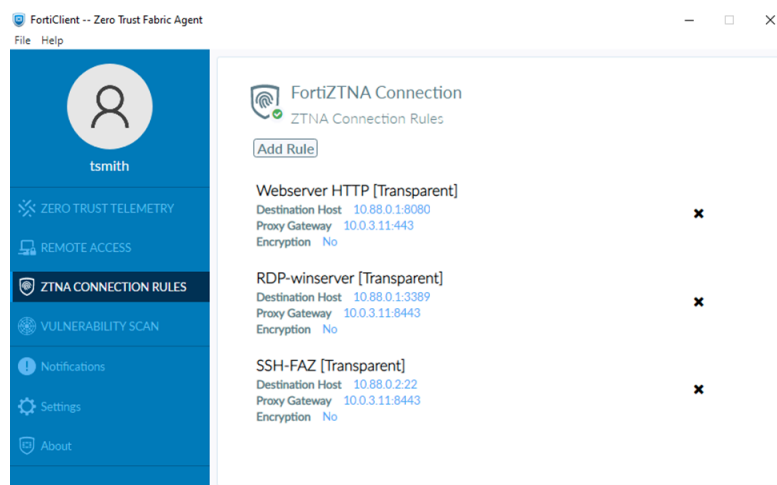
```

Test the connection to the access proxy

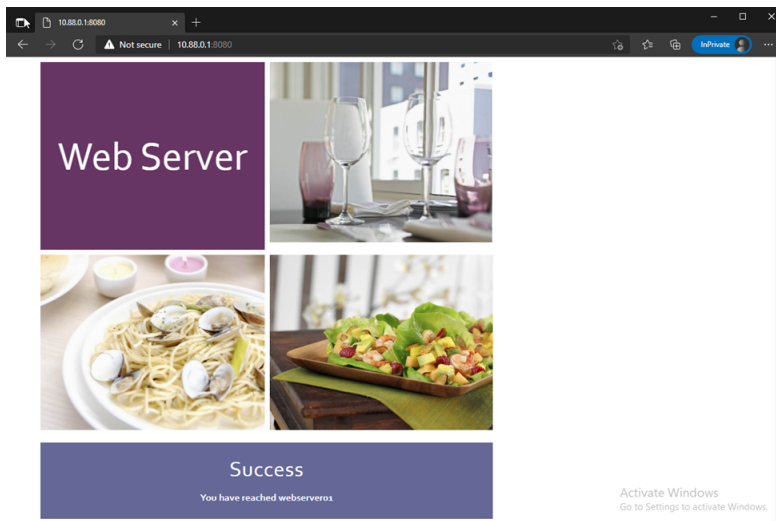
Before connecting, create a ZTNA rule in FortiClient.

To create a ZTNA rule in FortiClient:

1. Go to the *ZTNA Connection Rules* tab and click *Add Rule*.
2. Set *Rule Name* to *Webserver HTTP*.
3. Set *Destination Host* to *10.88.0.1:8080*. This is the real IP address and port of the server.
4. Set *Proxy Gateway* to *10.0.3.11:443*. This is the access proxy address and port that are configured on the FortiGate.
5. Set *Encryption* to *Disable*. This option determines whether or not the Client to FortiGate access proxy connection is encrypted in HTTPS.
6. Click *Create*.



After creating the ZTNA connection rule, open a browser and access the web page at <http://10.88.0.1:8080>.



Logs and debugs

1. The forward traffic log will show a log similar to this:

```
27: date=2021-07-13 time=13:05:00 eventtime=1626206700290129558 tz="-0700"
logid="0000000024" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.0.3.2 srcport=61409 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=10.88.0.1 dstport=8080 dstintf="root"
dstintfrole="undefined" sessionid=46959 service="tcp/8080" proto=6 action="accept"
policyid=3 policytype="proxy-policy" poluuid="fe0e1ae8-bdf9-51eb-b86f-c5e2adb934b3"
policyname="ZTNA-TCP" duration=114 wanin=38471 rcvdbyte=38471 wanout=775 lanin=2450
sentbyte=2450 lanout=40643 appcat="unscanned"
```

2. Use the following WAD debugs to capture the details about the connection as seen by the FortiGate WAD daemon. Notice that the HTTP request has `tls=0`, indicating that the proxy connection between the client and access proxy is not encrypted.

```
# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable

[1][p:224][s:46086][r:16777237] wad_dump_http_request :2542
hreq=0x7f20bdaf5950 Received request from client: 10.0.3.2:62067

GET /tcp?address=10.88.0.1&port=8080&tls=0 HTTP/1.1
Host: 10.0.3.11:443
User-Agent: Forticlient
Accept: */*
Cookie:
Authorization: Basic
...
```

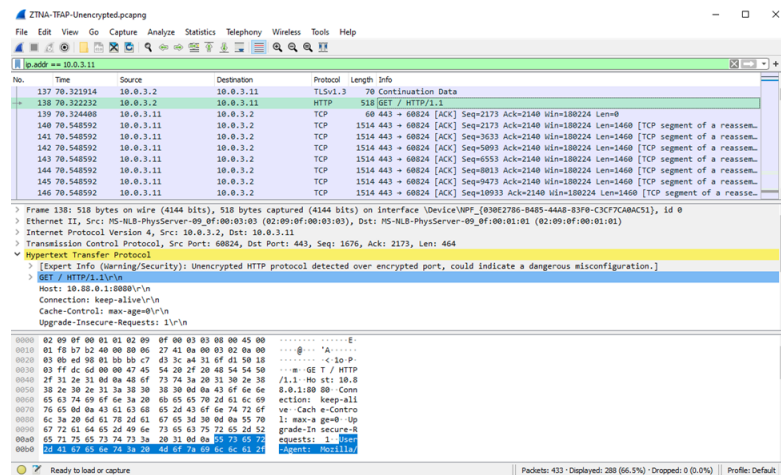
After reviewing the details, disable or reset the debugs:

```
# diagnose debug reset
```

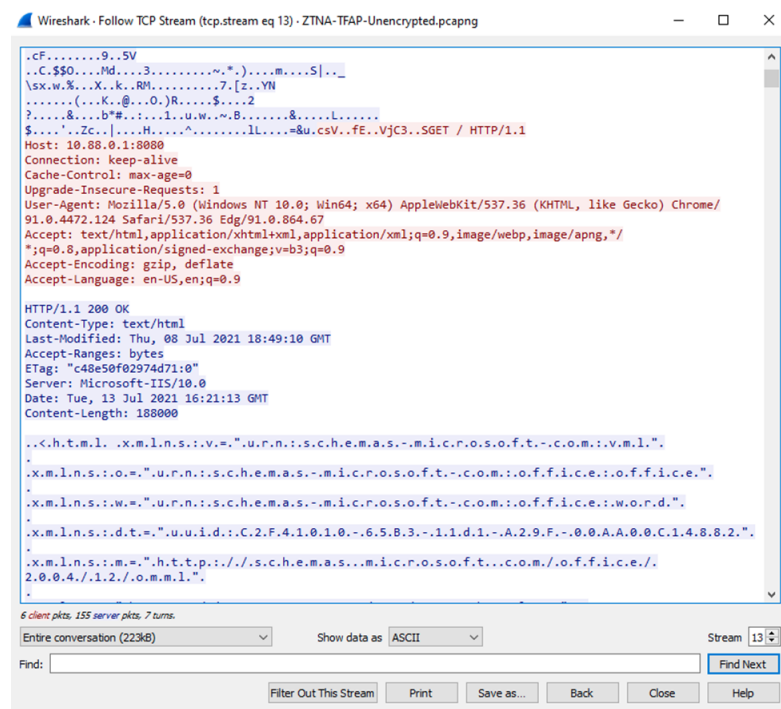
3. On the client PC, perform a packet capture to review the traffic flow between the client (10.0.3.2) and the access proxy (10.0.3.11) in detail. While the traffic is encapsulated in port 443, the underlying HTTP/8080 requests and

traffic are decoded as clear text.

Packet capture of traffic between 10.0.3.2:60824<->10.0.3.11:443:



Traffic stream:

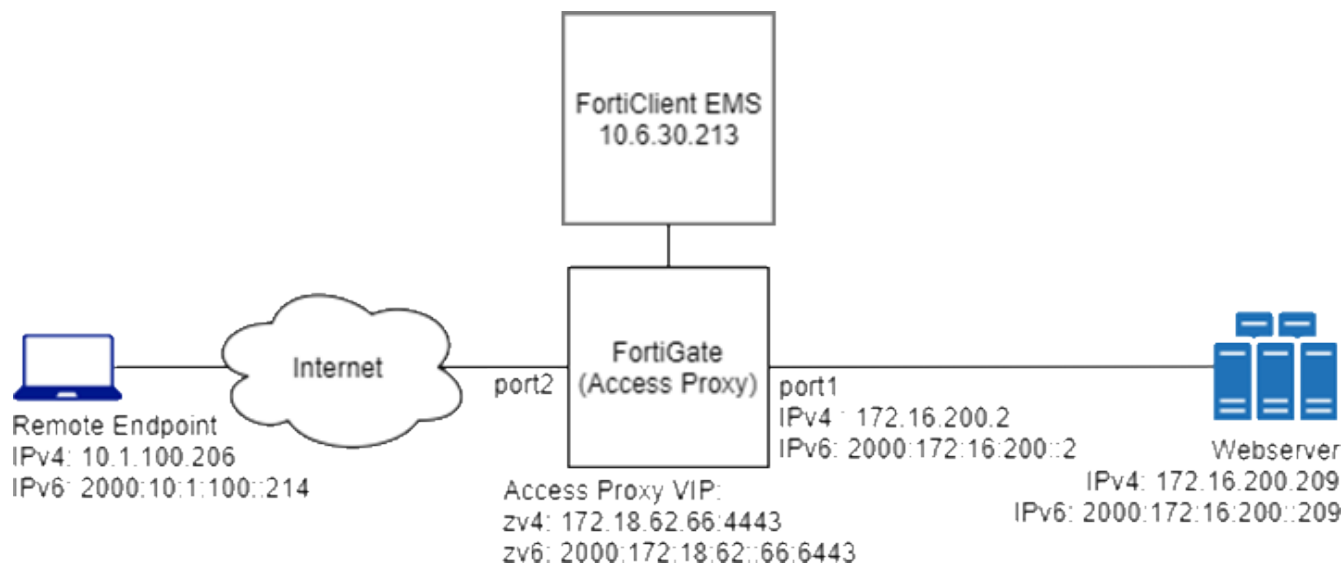


ZTNA IPv6 examples - 7.0.1

IPv6 can be configured in ZTNA in several scenarios:

- IPv6 Client — IPv6 Access Proxy — IPv6 Server
- IPv6 Client — IPv6 Access Proxy — IPv4 Server
- IPv4 Client — IPv4 Access Proxy — IPv6 Server

These examples show the basic configuration for each scenario. It is assumed that the EMS fabric connector is already successfully connected.



Example 1: IPv6 Client — IPv6 Access Proxy — IPv6 Server

To configure the FortiGate:

1. Configure the IPv6 access proxy VIP:

```
config firewall vip6
    edit "zv6"
        set type access-proxy
        set extip 2000:172:18:62::66
        set server-type https
        set extport 6443
        set ssl-certificate "cert"
    next
end
```

2. Configure a virtual host:

```
config firewall access-proxy-virtual-host
    edit "vhost_ipv6"
        set ssl-certificate "cert"
        set host "qa6.test.com"
    next
end
```

The client uses this address to connect to the access proxy.

3. Configure an IPv6 access proxy and IPv6 api-gateway, apply the VIP6 and virtual host to it, and assign an IPv6 address to the realserver:

```
config firewall access-proxy6
    edit "zs6"
        set vip "zv6"
        config api-gateway6
            edit 1
                set virtual-host "vhost_ipv6"
                config realservers
                    edit 1
```

```

        set ip 2000:172:16:200::209
      next
    end
  next
end
next
end

```

4. Apply the IPv6 access proxy to a proxy policy:

```

config firewall proxy-policy
  edit 1
    set name "ztna_rule"
    set proxy access-proxy
    set access-proxy6 "zs6"
    set srcintf "port2"
    set action accept
    set schedule "always"
    set logtraffic all
    set srcaddr6 "all"
    set dstaddr6 "all"
    set utm-status enable
    set ssl-ssh-profile "custom-deep-inspection"
    set webfilter-profile "monitor-all"
  next
end

```

5. Apply the IPv6 VIP to a firewall policy:

```

config firewall policy
  edit 4
    set name "ZTNA"
    set srcintf "port2"
    set dstintf "any"
    set action accept
    set srcaddr6 "all"
    set dstaddr6 "zv6"
    set schedule "always"
    set service "ALL"
    set inspection-mode proxy
    set logtraffic all
    set nat enable
  next
end

```

To test the configuration:

1. On an IPv6 client, ensure that the address qa6.test.com resolves to the IPv6 VIP address of 2000:172:18:62::66.
2. In a browser, connect to <https://qa6.test.com:6443>.
3. After device certificate verification, the browser will open up the webpage on the IPv6 real server.
4. In the Forward Traffic Log, the following log is available:

```

3: date=2021-06-25 time=13:38:18 eventtime=1624653498459580215 tz="-0700"
logid="0000000024" type="traffic" subtype="forward" level="notice" vd="root"
srcip=2000:10:1:100::214 srcport=55957 srcintf="port2" srcintfrole="undefined"
dstcountry="Reserved" srccountry="Reserved" dstip=2000:172:16:200::209 dstport=443
dstintf="root" dstintfrole="undefined" sessionid=92406 service="HTTPS" proto=6

```

```

action="accept" policyid=1 policytype="proxy-policy" poluid="7afdac8c-d5db-51eb-dfc6-
67bb86e4bdcf" policyname="ztna_rule" duration=5 wanin=2031 rcvdbyte=2031 wanout=1332
lanin=1247 sentbyte=1247 lanout=950 appcat="unscanned" utmaction="allow" countweb=1
utmref=65445-0

```

Example 2: IPv6 Client — IPv6 Access Proxy — IPv4 Server

To configure the FortiGate:

1. Configure the IPv6 access proxy VIP:

```

config firewall vip6
    edit "zv6"
        set type access-proxy
        set extip 2000:172:18:62::66
        set server-type https
        set extport 6443
        set ssl-certificate "cert"
    next
end

```

2. Configure a virtual host:

```

config firewall access-proxy-virtual-host
    edit "vhost_ipv6"
        set ssl-certificate "cert"
        set host "qa6.test.com"
    next
end

```

The client uses this address to connect to the access proxy.

3. Configure an IPv6 access proxy and IPv6 api-gateway, apply the VIP6 and virtual host to it, and assign an IPv4 address to the realserver:

```

config firewall access-proxy6
    edit "zs6"
        set vip "zv6"
        config api-gateway6
            edit 1
                set virtual-host "vhost_ipv6"
                config realservers
                    edit 1
                        set ip 172.16.200.209
                    next
                end
            next
        end
    next
end

```

4. Apply the IPv6 access proxy to a proxy policy:

```

config firewall proxy-policy
    edit 1
        set name "ztna_rule"
        set proxy access-proxy
        set access-proxy6 "zs6"
    next
end

```

```
set srcintf "port2"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set logtraffic all
set srcaddr6 "all"
set dstaddr6 "all"
set utm-status enable
set ssl-ssh-profile "custom-deep-inspection"
set webfilter-profile "monitor-all"
next
end
```

5. Apply the IPv6 VIP to a firewall policy:

```
config firewall policy
edit 4
set name "ZTNA"
set srcintf "port2"
set dstintf "any"
set action accept
set srcaddr6 "all"
set dstaddr6 "zv6"
set schedule "always"
set service "ALL"
set inspection-mode proxy
set logtraffic all
set nat enable
next
end
```

To test the configuration:

1. On an IPv6 client, ensure that the address qa6.test.com resolves to the IPv6 VIP address of 2000:172:18:62::66.
2. In a browser, connect to <https://qa6.test.com:6443>.
3. After device certificate verification, the browser will open up the webpage on the IPv4 real server.
4. In the Forward Traffic Log, the following log is available:

```
2: date=2021-06-25 time=13:46:54 eventtime=1624654014129553521 tz="-0700"
logid="0000000024" type="traffic" subtype="forward" level="notice" vd="root"
srcip=2000:10:1:100::214 srcport=60530 srcintf="port2" srcintfrole="undefined"
dstcountry="Reserved" srccountry="Reserved" dstip=172.16.200.209 dstport=443
dstintf="root" dstintfrole="undefined" sessionid=219 service="HTTPS" proto=6
action="accept" policyid=1 policytype="proxy-policy" poluuid="7afdac8c-d5db-51eb-dfc6-
67bb86e4bdcf" policyname="ztna_rule" duration=5 wanin=2028 rcvdbyte=2028 wanout=1321
lanin=1236 sentbyte=1236 lanout=947 appcat="unscanned" utmaction="allow" countweb=1
utmref=65443-14
```

Example 3: IPv4 Client — IPv4 Access Proxy — IPv6 Server

To configure the FortiGate:

1. Configure the IPv4 access proxy VIP:

```
config firewall vip
  edit "zv4"
    set type access-proxy
    set extip 172.18.62.66
    set extintf "any"
    set server-type https
    set extport 4443
    set ssl-certificate "cert"
  next
end
```

2. Configure a virtual host:

```
config firewall access-proxy-virtual-host
  edit "vhost_ipv4"
    set ssl-certificate "cert"
    set host "qa.test.com"
  next
end
```

The client uses this address to connect to the access proxy.

3. Configure an IPv4 access proxy and IPv6 api-gateway, apply the VIP and virtual host to it, and assign an IPv6 address to the realserver:

```
config firewall access-proxy
  edit "zs4"
    set vip "zv4"
    config api-gateway6
    edit 1
      set virtual-host "vhost_ipv4"
      config realservers
        edit 1
          set ip 2000:172:16:200::209
        next
      end
    next
  end
next
end
```

4. Apply the IPv4 access proxy to a proxy policy:

```
config firewall proxy-policy
  edit 1
    set name "ztna_rule"
    set proxy access-proxy
    set access-proxy "zs4"
    set srcintf "port2"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
```

```

        set logtraffic all
        set srcaddr6 "all"
        set dstaddr6 "all"
        set utm-status enable
        set ssl-ssh-profile "custom-deep-inspection"
        set webfilter-profile "monitor-all"
    next
end

```

5. Apply the IPv4 VIP to a firewall policy:

```

config firewall policy
    edit 4
        set name "ZTNA"
        set srcintf "port2"
        set dstintf "any"
        set action accept
        set srcaddr "all"
        set dstaddr "zv4"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set nat enable
    next
end

```

To test the configuration:

1. On an IPv4 client, ensure that the address qa6.test.com resolves to the IPv4 VIP address of 172.18.62.66.
2. In a browser, connect to <https://qa6.test.com:6443>.
3. After device certificate verification, the browser will open up the webpage on the IPv6 real server.
4. In the Forward Traffic Log, the following log is available:

```

1: date=2021-06-25 time=13:52:30 eventtime=1624654350689576485 tz="-0700"
logid="0000000024" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.206 srcport=53492 srcintf="port2" srcintfrole="undefined"
dstcountry="Reserved" srccountry="Reserved" dstip=2000:172:16:200::209 dstport=443
dstintf="root" dstintfrole="undefined" sessionid=726 service="HTTPS" proto=6
action="accept" policyid=1 policytype="proxy-policy" poluid="7afdac8c-d5db-51eb-dfc6-
67bb86e4bdcf" policyname="ztna_rule" duration=0 wanin=1901 rcvdbyte=1901 wanout=736
lanin=569 sentbyte=569 lanout=3040 appcat="unscanned" utmaction="allow" countweb=1
utmref=65443-28

```

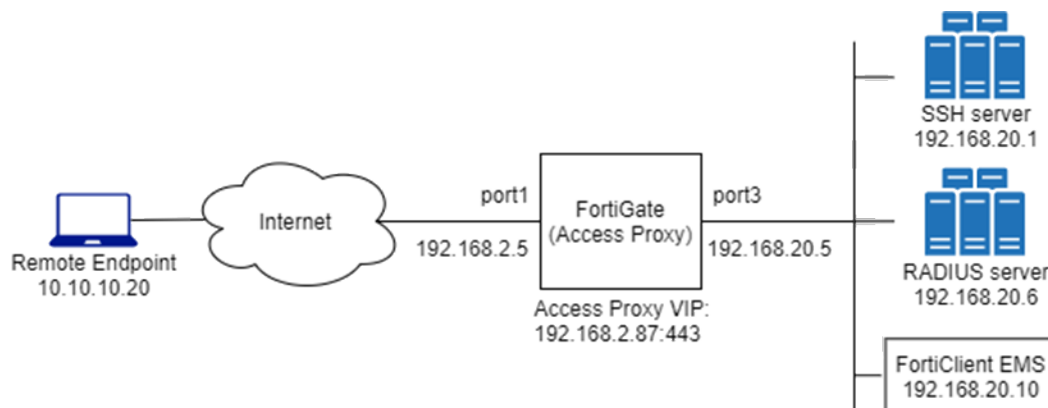
ZTNA SSH access proxy example - 7.0.1

ZTNA can be configured with SSH access proxy to provide a seamless SSH connection to the server.

Advantages of using an SSH access proxy instead of a TCP forwarding access proxy include:

- Establishing device trust context with user identity and device identity checks.
- Applying SSH deep inspection to the traffic through the SSH related profile.
- Performing optional SSH host-key validation of the server.

- Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection.

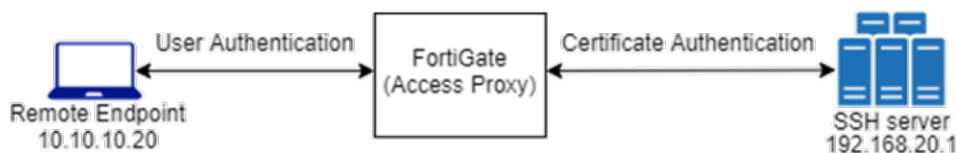


Perform SSH host-key validation of the server

To act as a reverse proxy for the SSH server, the FortiGate must perform SSH host-key validation to verify the identity of the SSH server. The FortiGate does this by storing the public key of the SSH server in its SSH host-key configurations. When a connection is made to the SSH server, if the public key matches one that is used by the server, then the connection is established. If there is no match, then the connection fails.

One-time user authentication

SSH access proxy allows user authentication to occur between the client and the access proxy, while using the same user credentials to authenticate with the SSH server. The following illustrates how this works:



1. The remote endpoint registers to FortiClient EMS and receives the client certificate.
2. The remote endpoint tries to connect to the SSH access proxy. It must use the same username that is later used for access proxy authentication.
3. The FortiGate challenges the endpoint with device identity validation.
4. The remote endpoint provides the EMS issued certificate for device identification.
5. The FortiGate challenges the endpoint with user authentication. For example, this could be done with basic or SAML authentication.
6. The user enters their credentials on the remote endpoint.
7. The FortiGate authenticates the user and collects the username.
8. Using the FortiGate's CA or the customer's CA certificate, the FortiGate signs an SSH certificate and embeds the username in its principal.
9. The FortiGate attempts to connect to the SSH server using the certificate authentication.
10. The SSH server verifies the authenticity of the certificate, and matches the username principal against its `authorized_keys` file.
11. If the username matches a record in the file, then the SSH connection is established. If no match is found, then the SSH connection fails.

Example

In this example, an SSH connection is established using SSH access proxy with host-key validation and one-time authentication.

- The SSH server is a Linux based server that uses sshd to provide remote access
- For SSH host-key validation, the public key of the SSH server has been imported into the FortiGate.
- For one-time authentication using certificate authentication:
 - The SSH server must allow certificate authentication.
 - The SSH server must have the proper entry in its `authorized_keys` file that contains the user principal and the FortiGate CA's public key.
 - The entry is present in the user directory corresponding to the user that is trying to log in.

To pre-configure the Linux SSH server:

1. Retrieve the public key used for host-key validation:

a. Locate the public key files in the SSH server:

```
$ ls -la /etc/ssh/*.pub
-rw-r--r-- 1 root root 186 Mar 29 2020 /etc/ssh/ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root 106 Mar 29 2020 /etc/ssh/ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 406 Mar 29 2020 /etc/ssh/ssh_host_rsa_key.pub2
```

b. Choose the publish key file based on the hash type (in this case, ECDSA), and show it's content:

```
$ cat /etc/ssh/ssh_host_ecdsa_key.pub
ecdsa-sha2-nistp256 AAAAE2*****IpEik=
```

This key will be used when configuring the FortiGate.

2. Retrieve the FortiGate CA's public key from the FortiGate:

```
# show full firewall ssh local-ca Fortinet_SSH_CA
config firewall ssh local-ca
    edit "Fortinet_SSH_CA"
        set password ENC <hidden password>
        set private-key "-----BEGIN OPENSSSH PRIVATE KEY-----
<hidden private key>
-----END OPENSSSH PRIVATE KEY-----"
        set public-key "ssh-rsa AAAAB3*****JLX1xj3"
        set source built-in
    next
end
```

3. On the Linux server, enable the SSH service to use the `authorized_keys` file:

a. Locate and edit the `/etc/ssh/sshd_config` file.

b. Ensure that the `AuthorizedKeysFile` line is uncommented, for example:

```
AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```

4. Allow remote SSH log in with certificate authentication and principal name:

a. Log in to the SSH server using the account that will be granted remote SSH access (in this example: *radCurtis*):

b. Locate the account's `authorized_keys` file in the `~/.ssh` directory:

```
$ ls -la ~/.ssh
total 12
```

```
drwxrwxr-x 2 radCurtis radCurtis 4096 Aug 10 19:14 .
drwxr-xr-x 5 radCurtis radCurtis 4096 Aug 10 19:13 ..
-rw-rw-r-- 1 radCurtis radCurtis 419 Aug 10 19:14 authorized_keys
```

- c. If the directory and file do not exist, create the directory:

```
$ mkdir ~/.ssh
```

- d. Create an entry containing the following keywords and add them to the `authorized_keys` file:

```
echo 'cert-authority,principals="radCurtis" ssh-rsa AAAAB3*****JLX1xj3' >>
authorized_keys
```

Where:

- `cert-authority` - indicates that this entry is used in certificate authentication by validating the certificate using the public key provided in this entry.
- `principals="radCurtis"` - indicates the user that must match with the username embedded in the SSH certificate.
- `ssh-rsa AAAAB3*****JLX1xj3` - indicates the FortiGate CA's public key that is used to validate the SSH certificate.

5. Restart the `sshd` service:

```
$ sudo systemctl stop sshd
$ sudo systemctl start sshd
```

The SSH server can now accept SSH connection from `radCurtis@<server IP>`, where the SSH certificate used by the FortiGate to log in contains `radCurtis` embedded as a principal.



When a user connects from a SSH client using `<username>@<server IP>`, `sshd` will locate the `authorized_keys` file in the directory `/home/<username>/.ssh/authorized_keys`. If the `authorized_keys` is not in that directory, authentication will fail on the SSH server side.

If you suspect that authentication is failing on the SSH server, use the following commands to manually start `sshd` in debug mode to troubleshoot:

```
$ sudo systemctl stop sshd
$ /usr/sbin/sshd -ddd -p 22
```

To configure the FortiGate :

1. Configure a new VIP to allow access to the SSH access proxy over 192.168.2.87:443:

```
config firewall vip
edit "ZTNA_SSH"
set type access-proxy
set extip 192.168.2.87
set extintf "any"
set server-type https
set extport 443
set ssl-certificate "Fortinet_CA_SSL"
next
end
```

2. Configure the address object for the SSH server:

```
config firewall address
  edit "SSH_server"
    set subnet 192.168.20.1 255.255.255.255
  next
end
```

3. Configure the host-key that will be used to authenticate the SSH server. The public-key was retrieved when pre-configure the Linux SSH server (step 1b).

```
config firewall ssh host-key
  edit "ecdsa"
    set type ECDSA
    set usage access-proxy
    set public-key "AAAAE2*****IpEik="
  next
end
```

4. Configure the access proxy SSH client certificate:

A CA certificate is assigned to sign the SSH certificate that will be used in the SSH authentication. The SSH certificate will have the username embedded in the certificate principal.

```
config firewall access-proxy-ssh-client-cert
  edit "ssh-access-proxy"
    set source-address enable
    set auth-ca "Fortinet_SSH_CA"
  next
end
```

5. Configure the access-proxy server setting:

```
config firewall access-proxy
  edit "ZTNA_SSH"
    set vip "ZTNA_SSH"
    set client-cert enable
    config api-gateway
      edit 1
        set url-map "tcp"
        set service tcp-forwarding
        config realservers
          edit 1
            set address "SSH_server"
            set type ssh
            set ssh-client-cert "ssh-access-proxy"
            set ssh-host-key-validation enable
            set ssh-host-key "ed25519"
          next
        end
      next
    end
  next
end
```

6. Configure the RADIUS setting, user setting, and user group to apply user authentication to the access proxy connection using RADIUS:

```
config user radius
  edit "Win2k16-Radius"
    set server "192.168.20.6"
```

```
        set secret ENC <secret>
    next
end
config user local
    edit "radCurtis"
        set type radius
        set radius-server "Win2k16-Radius"
    next
end
config user group
    edit "radius_group"
        set member "radCurtis" "Win2k16-Radius"
    next
end
```

7. Create the authentication scheme and rule to perform the authentication:

```
config authentication scheme
    edit "basic_auth"
        set method basic
        set user-database "Win2k16-Radius"
    next
end
config authentication rule
    edit "ztna-basic"
        set srcaddr "all"
        set ip-based disable
        set active-auth-method "basic_auth"
        set web-auth-cookie enable
    next
end
```

8. Configure the ZTNA rule to allow traffic to the SSH server, and apply user authentication, posture check, and a security profile where necessary:

```
config firewall proxy-policy
    edit 5
        set name "SSH-proxy"
        set proxy access-proxy
        set access-proxy "ZTNA_SSH"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "FCTEMS8821001056_ems138_av_tag"
        set action accept
        set schedule "always"
        set groups "radius_group"
        set utm-status enable
        set ssl-ssh-profile "custom-deep-inspection"
    next
end
```

9. Configure the firewall policy to allow the client connection to the SSH access proxy over the VIP:

```
config firewall policy
    edit 35
        set name "full-ztna-ssh"
        set srcintf "port1"
        set dstintf "any"
```

```
set action accept
set srcaddr "all"
set dstaddr "ZTNA_SSH"
set schedule "always"
set service "ALL"
set inspection-mode proxy
set logtraffic all
set nat enable
next
end
```

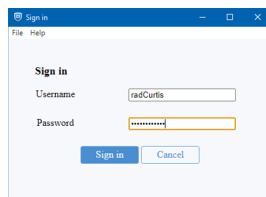
To check the results:

1. On the remote client, open FortiClient, go to the *Zero Trust Telemetry* tab, and make sure that it is connected to the EMS server.
2. Go to the *ZTNA Connection Rules* tab and click *Add Rule*.
3. Configure the rule, then click *Create*:

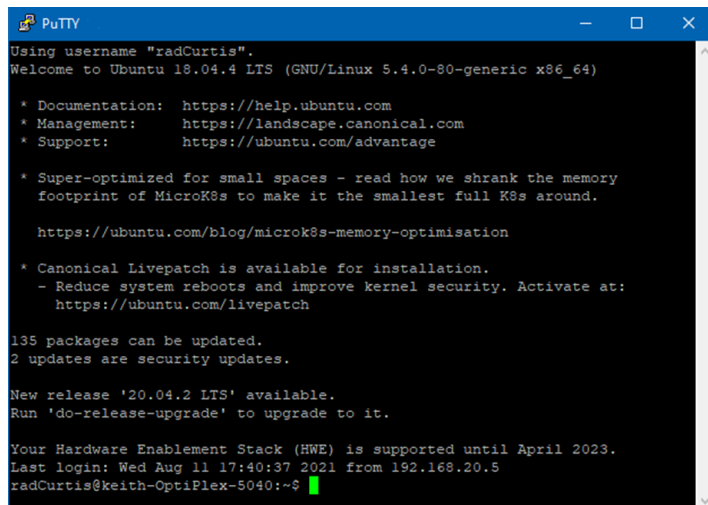
Rule Name	SSH-Linux
Destination Host	192.168.20.1:22
Proxy Gateway	192.168.2.87:443
Mode	Transparent
Encryption	Disabled (recommended)

When Encryption is disabled, the connection between the client and FortiGate access proxy is not encapsulated in HTTPS after the client and FortiGate connection is established. This allows for less overhead, because SSH is already a secure connection. This option is available in FortiClient 7.0.1 and later releases.

4. Open an SSH client, such as PuTTY, and make an SSH connection to *radCurtis@192.168.20.1* on port 22.
5. After device authentication is performed and passes in the background, FortiClient prompts the user to sign in. Enter the username, *radCurtis*, and password, then click *Sign in*.



After successful user authentication, the SSH connection is established without an additional log in.



```

PuTTY
Using username "radCurtis".
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.
   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
   https://ubuntu.com/livepatch

135 packages can be updated.
2 updates are security updates.

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Wed Aug 11 17:40:37 2021 from 192.168.20.5
radCurtis@keith-OptiPlex-5040:~$

```

6. On the FortiGate, check the logged in user:
 - a. Go to *Dashboard > Users & Devices* and expand the *Firewall Users* widget.
 - b. Check the WAD proxy user list:

```

# diagnose wad user list
ID: 2, VDOM: root, IPv4: 10.10.10.25
  user name      : radCurtis
  worker         : 0
  duration       : 614
  auth_type      : Session
  auth_method    : Basic
  pol_id         : 5
  g_id           : 12
  user_based     : 0
  expire         : 53
  LAN:
    bytes_in=3403 bytes_out=5699
  WAN:
    bytes_in=3681 bytes_out=3132

```

7. The successful connection is logged in the forward traffic logs after the SSH connection has disconnected:

```

# execute log display
25 logs found.
10 logs returned.

1: date=2021-08-11 time=17:59:56 eventtime=1628729996110159120 tz="-0700"
logid="0000000024" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.10.10.25 srcport=50627 srcintf="port1" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=192.168.20.1 dstport=22 dstintf="root"
dstintfrole="undefined" sessionid=1926338 srcuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f"
service="SSH" proto=6 action="accept" policyid=5 policytype="proxy-policy"
poluid="16fb5550-e976-51eb-e76c-d45e96dfa5dc" policyname="SSH-proxy" duration=67
user="radCurtis" group="radius_group" authserver="Win2k16-Radius" wanin=3681
rcvdbyte=3681 wanout=3132 lanin=3403 sentbyte=3403 lanout=5699 appcat="unscanned"

```

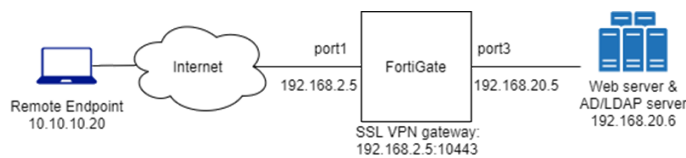
Migrating from SSL VPN to ZTNA HTTPS access proxy

ZTNA can be used to replace VPN based teleworking solutions. Teleworking configurations that use SSL VPN tunnel or web portal mode access with LDAP user authentication can be migrated to ZTNA with HTTPS access proxy.

Scenarios

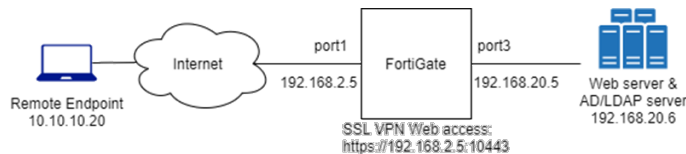
SSL VPN tunnel mode access with LDAP user authentication

Remote users that are in the *ALLOWED-VPN* active directory group have access to a specific web server when they connect through the SSL VPN tunnel. The FortiGate enables split tunneling to the web server so that only traffic to that destination is routed through the tunnel. The web server hosts internal websites that are only accessible by employees.



SSL VPN Web mode access with LDAP user authentication

Remote users that are in the *ALLOWED-VPN* active directory group have access to a specific web server when they connect through the SSL VPN web portal. The FortiGate The web server hosts internal websites that are only accessible by employees. The pre-defined bookmark to the internal website is the only site that allows remote access.



Configuration

To configure an LDAP server:

```
config user ldap
  edit "WIN2K16-KLHOME-LDAPS"
    set server "192.168.20.6"
    set server-identity-check disable
    set cnid "sAMAccountName"
    set dn "dc=KLHOME,dc=local"
    set type regular
    set username "KLHOME\\Administrator"
    set password *****
    set secure ldaps
    set ca-cert "CA_Cert_1"
    set port 636
  next
end
```


To configure a user group:

```
config user group
  edit "KLHOME-ALLOWED-VPN"
    set member "WIN2K16-KLHOME-LDAPS"
    config match
      edit 1
        set server-name "WIN2K16-KLHOME-LDAPS"
        set group-name "CN=ALLOWED-VPN,DC=KLHOME,DC=local"
      next
    end
  next
end
```

To configure the tunnel mode portal and SSL VPN settings:

```
config vpn ssl web portal
  edit "tunnel-access"
    set tunnel-mode enable
    set ip-pools "SSLVPN_TUNNEL_ADDR1"
  next
end

config vpn ssl settings
  set servercert "Fortinet_Factory"
  set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
  set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
  set source-interface "port1"
  set source-address "all"
  set source-address6 "all"
  set default-portal "no-access"
  config authentication-rule
    edit 1
      set groups "KLHOME-ALLOWED-VPN"
      set portal "tunnel-access"
    next
  end
end
```

To configure the web mode portal and SSL VPN settings:

```
config vpn ssl web portal
  edit "web-access"
    set web-mode enable
    set user-bookmark disable
    config bookmark-group
      edit "gui-bookmarks"
        config bookmarks
          edit "winserver"
            set url "https://192.168.20.6"
          next
        end
      next
    end
  next
end
set display-connection-tools disable
```

```
    next
end

config vpn ssl settings
    set servercert "Fortinet_Factory"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "no-access"
    config authentication-rule
        edit 1
            set groups "KLHOME-ALLOWED-VPN"
            set portal "web-access"
        next
    end
end
```

To configure a firewall address and policy:

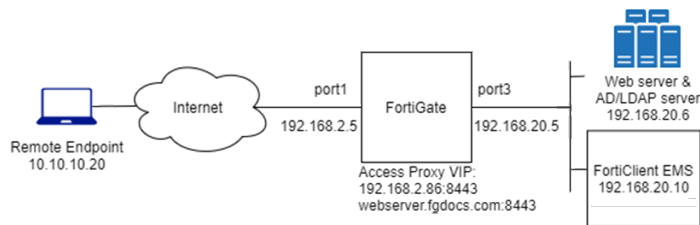
```
config firewall address
    edit "winserver"
        set subnet 192.168.20.6 255.255.255.255
    next
end

config firewall policy
    edit 32
        set name "SSLVPNtoWinserver"
        set srcintf "ssl.root"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "winserver"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set groups "KLHOME-ALLOWED-VPN"
    next
end
```

With both the SSL VVPN tunnel and web portals, the remote user can connect through the SSL VPN and access the website at <https://192.168.20.6>. To monitor their access, go to *Dashboard > Network* and expand the *SSL-VPN* widget.

Migrating to ZTNA HTTPS access proxy

Both the SSL VPN tunnel and web portals can be migrated into a ZTNA configuration using the same LDAP server and user group for authentication. The ZTNA solution provides multi-factor authentication using the client certificate, and additional security posture checks.



Instead of connecting to the SSL VPN tunnel or web portal, the remote user connects to the HTTPS access proxy that forwards traffic to the web server after authentication and security posture checks are completed. This provides granular control over who can access the web resource using role-based access control. It also gives the user transparent access to the website using only their browser.

For more information, see [ZTNA HTTPS access proxy example on page 299](#) and [ZTNA HTTPS access proxy with basic authentication example on page 308](#).

ZTNA troubleshooting and debugging

The following debug commands can be used to troubleshoot ZTNA issues:

Command	Description
# diagnose endpoint fctems test-connectivity <EMS>	Verify FortiGate to FortiClient EMS connectivity.
# execute fctems verify <EMS>	Verify the FortiClient EMS's certificate.
# diagnose test application fcnacd 2	Dump the EMS connectivity information.
# diagnose debug app fcnacd -1 # diagnose debug enable	Run real-time FortiClient NAC daemon debugs.
# diagnose endpoint record list <ip>	Show the endpoint record list. Optionally, filter by the endpoint IP address.
# diagnose endpoint wad-comm find-by uid <uid>	Query endpoints by client UID.
# diagnose endpoint wad-comm find-by ip-vdom <ip> <vdom>	Query endpoints by the client IP-VDOM pair.
# diagnose wad dev query-by uid <uid>	Query from WAD diagnose command by UID.
# diagnose wad dev query-by ipv4 <ip>	Query from WAD diagnose command by IP address.
# diagnose firewall dynamic list	List EMS ZTNA tags and all dynamic IP and MAC addresses.
# diagnose test application fcnacd 7 # diagnose test application fcnacd 8	Check the FortiClient NAC daemon ZTNA and route cache.
# diagnose wad debug enable category all # diagnose wad debug enable level verbose # diagnose debug enable	Run real-time WAD debugs.
# diagnose debug reset	Reset debugs when completed



The WAD daemon handles proxy related processing. The FortiClient NAC daemon (fncacd) handles FortiGate to EMS connectivity.

Troubleshooting usage and output

1. Verify the FortiGate to EMS connectivity and EMS certificate:

```
# diagnose endpoint fctems test-connectivity WIN10-EMS
Connection test was successful:

# execute fctems verify WIN10-EMS
Server certificate already verified.

# diagnose test application fncacd 2
EMS context status:
FortiClient EMS number 1:
    name: WIN10-EMS confirmed: yes
    fetched-serial-number: FCTEMS0000109188
Websocket status: connected
```

2. If fncacd does not report the proper status, run real-time fncacd debugs:

```
# diag debug app fncacd -1
# diag debug enable
```

3. Verify the following information about an endpoint:

- Network information
- Registration information
- Client certificate information
- Device information
- Vulnerability status
- Relative position with the FortiGate

```
# diagnose endpoint record list 10.6.30.214
Record #1:
    IP Address = 10.6.30.214
    MAC Address = 00:0c:29:ba:1e:61
    MAC list = 00:0c:29:ba:1e:61;00:0c:29:ba:1e:6b;
    VDOM = root (0)
    EMS serial number: FCTEMS8821001322
    Client cert SN: 17FF6595600A1AF53B87627AB4EBEDD032593E64
    Quarantined: no
    Online status: online
    Registration status: registered
    On-net status: on-net
    Gateway Interface: port2
    FortiClient version: 7.0.0
    AVDB version: 84.778
    FortiClient app signature version: 18.43
    FortiClient vulnerability scan engine version: 2.30
    FortiClient UID: 5FCFA3ECDE4D478C911D9232EC9299FD
    Host Name: ADPC
...

```

```

        Number of Routes: (1)
            Gateway Route #0:
                - IP:10.1.100.214, MAC: 00:0c:29:ba:1e:6b, Indirect: no
                - Interface:port2, VFID:0, SN: FG5H1E5819902474
online records: 1; offline records: 0; quarantined records: 0

```

4. Query the endpoint information, include ZTNA tags, by UID or IP address:

```

# diagnose endpoint wad-comm find-by uid 5FCFA3ECDE4D478C911D9232EC9299FD
UID: 5FCFA3ECDE4D478C911D9232EC9299FD
    status code:ok
    Domain: qa.wangd.com
    User: user1
    Cert SN:17FF6595600A1AF53B87627AB4EBEDD032593E64
    EMS SN: FCTEMS8821001322
    Routes(1):
        - route[0]: IP=10.1.100.214, VDom=root
    Tags(3):
        - tag[0]: name=ZT_OS_WIN
        - tag[1]: name=all_registered_clients
        - tag[2]: name=Medium

# diagnose endpoint wad-comm find-by ip-vdom 10.1.100.214 root
UID: 5FCFA3ECDE4D478C911D9232EC9299FD
    status code:ok
    Domain: qa.wangd.com
    User: user1
    Cert SN:17FF6595600A1AF53B87627AB4EBEDD032593E64
    EMS SN: FCTEMS8821001322
    Routes(1):
        - route[0]: IP=10.1.100.214, VDom=root
    Tags(3):
        - tag[0]: name=ZT_OS_WIN
        - tag[1]: name=all_registered_clients
        - tag[2]: name=Medium

```

5. Query endpoint information from WAD by UID or IP address:

```

# diagnose wad dev query-by uid 5FCFA3ECDE4D478C911D9232EC9299FD
Attr of type=0, length=32, value(ascii)=5FCFA3ECDE4D478C911D9232EC9299FD
Attr of type=4, length=30, value(ascii)=MAC_FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=26, value(ascii)=FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=43, value(ascii)=MAC_FCTEMS8821001322_all_registered_clients
Attr of type=4, length=39, value(ascii)=FCTEMS8821001322_all_registered_clients
Attr of type=4, length=27, value(ascii)=MAC_FCTEMS8821001322_Medium
Attr of type=4, length=23, value(ascii)=FCTEMS8821001322_Medium
Attr of type=5, length=18, value(ascii)=FOSQA@qa.wangd.com
Attr of type=6, length=40, value(ascii)=17FF6595600A1AF53B87627AB4EBEDD032593E64

# diagnose wad dev query-by ipv4 10.1.100.214
Attr of type=0, length=32, value(ascii)=5FCFA3ECDE4D478C911D9232EC9299FD
Attr of type=4, length=30, value(ascii)=MAC_FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=26, value(ascii)=FCTEMS8821001322_ZT_OS_WIN
Attr of type=4, length=43, value(ascii)=MAC_FCTEMS8821001322_all_registered_clients
Attr of type=4, length=39, value(ascii)=FCTEMS8821001322_all_registered_clients
Attr of type=4, length=27, value(ascii)=MAC_FCTEMS8821001322_Medium
Attr of type=4, length=23, value(ascii)=FCTEMS8821001322_Medium

```

```
Attr of type=5, length=18, value(ascii)=FOSQA@qa.wangd.com
Attr of type=6, length=40, value(ascii)=17FF6595600A1AF53B87627AB4EBEDD032593E64
```

6. List all the dynamic ZTNA IP and MAC addresses learned from EMS:

```
# diagnose firewall dynamic list
List all dynamic addresses:
FCTEMS0000109188_all_registered_clients: ID(51)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...
FCTEMS0000109188_Low: ID(78)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...
FCTEMS0000109188_Malicious-File-Detected: ID(190)
    ADDR(172.17.194.209)
    ADDR(192.168.40.8)
...
```

7. Check the FortiClient NAC daemon ZTNA and route cache:

```
# diagnose test application fcnacd 7
ZTNA Cache:
-uid 5FCFA3ECDE4D478C911D9232EC9299FD: { "tags": [ "ZT_OS_WIN", "all_registered_
clients", "Medium" ], "domain": "qa.wangd.com", "user_name": "user1", "client_cert_sn":
"17FF6595600A1AF53B87627AB4EBEDD032593E64", "owner": "FOSQA@qa.wangd.com", "gateway_
route_list": [ { "gateway_info": { "fgt_sn": "FG5H1E5819902474", "interface": "port2",
"vdom": "root" }, "route_info": [ { "ip": "10.1.100.214", "mac": "00-0c-29-ba-1e-6b",
"route_type": "direct" } ] } ], "ems_sn": "FCTEMS8821001322" }

# diagnose test application fcnacd 8
IP-VfID Cache:
IP: 10.1.100.206, vfid: 0, uid: 3DED29B54386416E9888F2DCBD2B9D21
IP: 10.1.100.214, vfid: 0, uid: 5FCFA3ECDE4D478C911D9232EC9299FD
```

8. Troubleshoot WAD with real-time debugs to understand how the proxy handled a client request:

```
# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable

[0x7fbd7a46bb60] Received request from client: 10.10.10.20:56312
GET / HTTP/1.1 Host: 192.168.2.86:8443 Connection: keep-alive Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36 Edg/89.0.774.57
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-
Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-
Language: en-US,en;q=0.9 [p:29957][s:458767][r:1] wad_http_marker_uri(1269): path=/
len=1
[p:29957][s:458767][r:1] wad_http_parse_host(1641): host_len=17
[p:29957][s:458767][r:1] wad_http_parse_host(1677): len=12
[p:29957][s:458767][r:1] wad_http_parse_host(1686): len=4
[p:29957][s:458767][r:1] wad_http_str_canonicalize(2180): path=/ len=1 changes=0
[p:29957][s:458767][r:1] wad_http_str_canonicalize(2189): path=/ len=1 changes=0
[p:29957][s:458767][r:1] wad_http_normalize_uri(2232): host_len=12 path_len=1 query_
```

```

len=0
[p:29957][s:458767][r:1] wad_vs_proxy_match_gwy(2244): 6:WIN2K16-P1: matching gwy with
vhost(_def_virtual_host_)
[p:29957][s:458767][r:1] wad_vs_proxy_match_vhost(2293): 6:WIN2K16-P1: matching vhost
by: 192.168.2.86
[p:29957][s:458767][r:1] wad_vs_matcher_map_find(477): Empty matcher!
[p:29957][s:458767][r:1] wad_vs_proxy_match_vhost(2296): 6:WIN2K16-P1: no host matched.
[p:29957][s:458767][r:1] wad_vs_proxy_match_gwy(2263): 6:WIN2K16-P1: matching gwy by (/)
with vhost(_def_virtual_host_).
[p:29957][s:458767][r:1] wad_pattern_matcher_search(1210): pattern-match succ:/
[p:29957][s:458767][r:1] wad_vs_proxy_match_gwy(2271): 6:WIN2K16-P1: Matched gwy(1) type
(https).
[p:29957][s:458767][r:1] wad_http_vs_check_dst_ovrd(776): 6:WIN2K16-P1:1: Found server:
192.168.20.6:443
[p:29957][s:458767][r:1] wad_http_req_exec_act(9296): dst_addr_type=3 wc_nontp=0 sec_
web=1 web_cache=0 req_bypass=0
[p:29957][s:458767][r:1] wad_http_req_check_policy(8117): starting policy matching(vs_
pol= 1):10.10.10.20:56312->192.168.20.6:443
[p:29957][s:458767][r:1] wad_fw_addr_match_ap(1524): matching ap:WIN2K16(7) with vip
addr:WIN2K16-P1(10)
[p:29957][s:458767][r:1] wad_fw_addr_match_ap(1524): matching ap:WIN2K16-P1(10) with vip
addr:WIN2K16-P1(10)
[p:29957][s:458767][r:1] wad_http_req_policy_set(6811): match pid=29957 policy-id=2 vd=0
in_if=3, out_if=7 10.10.10.20:56312 -> 192.168.20.6:443
[p:29957][s:458767][r:1] wad_cifs_profile_init(93): CIFS Profile 0x7fbd7a5bf200 [] of
type 0 created
[p:29957][s:458767][r:1] wad_http_req_proc_policy(6622): web_cache(http/https=0/0, fwd_
srv=<nil>).
[p:29957][s:458767][r:1] wad_auth_inc_user_count(1668): increased user count,
quota:128000, n_shared_user:2, vd_used: 2, vd_max: 0, vd_guarantee: 0
[p:29957][s:458767][r:1] __wad_fmем_open(563): fmem=0xaaee3e8, fmem_name='cmem 336
bucket', elm_sz=336, block_sz=73728, overhead=20, type=advanced
[p:29957][s:458767][r:1] __wad_hauth_user_node_hold(2107): wad_hauth_user_node_alloc
(1568): holding node 0x7fbd76d48060
mapping user_node:0x7fbd76d48060, user_ip:0x7fbd7a57b408(0), user:0x7fbd7a5cf420(0)
[p:29957][s:458767][r:1] __wad_hauth_user_node_hold(2107): wad_user_node_stats_hold
(483): holding node 0x7fbd76d48060
[p:29957][s:458767][r:1] __wad_hauth_user_node_hold(2107): wad_http_session_upd_user_
node (4813): holding node 0x7fbd76d48060
[p:29957][s:458767][r:1] wad_http_req_proc_policy(6698): policy result:vf_id=0:0 sec_
profile=0x7fbd7a5bef00 set_cookie=0
[p:29957][s:458767][r:1] wad_http_urlfilter_check(381): uri_norm=1 inval_host=0 inval_
url=0 scan_hdr/body=1/0 url local=0 block=0 user-cat=0 allow=0 ftgd=0 keyword=0 wisp=0
[p:29957][s:458767][r:1] wad_http_req_proc_waf(1309): req=0x7fbd7a46bb60 ssl.deep_scan=1
proto=10 exempt=0 waf=(nil) body_len=0 ua=Chrome/89.0.4389.90 skip_scan=0
[p:29957][s:458767][r:1] wad_http_req_proc_antiphish(5376): Processing antiphish request
[p:29957][s:458767][r:1] wad_http_req_proc_antiphish(5379): No profile
[p:29957][s:458767][r:1] wad_http_connect_server(4696): http session 0x7fbd7a532ac8
req=0x7fbd7a46bb60
[p:29957][s:458767][r:1] wad_http_srv_still_good(4575): srv((nil)) nontp(0) dst_type(3)
req: dst:192.168.20.6:443, proto:10)
hcs: dst:N/A:0, proto:1)

```



Always reset the debugs after using them:

diagnose debug reset

ZTNA logging enhancements - 7.0.1

The ZTNA log subtype is added to UTM logs and a traffic log ID is added for ZTNA related traffic.

There are six events that generate logs in the subtype:

1. Received an empty client certificate
2. Received a client certificate that fails to validate
3. API gateway cannot be matched
4. None of the real servers can be reached
5. ZTNA rule (proxy policy) cannot be matched
6. HTTPS SNI virtual host does not match the HTTP host header

ZTNA related traffic will generate logs when logging all allowed traffic is enabled in the policy.

To enable logging all traffic in a policy in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and edit a policy.
2. Set *Log Allowed Traffic* to *All Sessions*.
3. Click *OK*.

To enable logging all traffic in a policy in the CLI:

```
config firewall policy
  edit <policy number>
    ...
    set logtraffic all
  next
end
```

Log samples

A client PC (10.1.100.206) is connected to port2 on the FortiGate. The FortiGate is also connected to a FortiClient EMS, and a real server that is defined in the ZTNA server API gateway.

- Access proxy server: zs2
- Access proxy VIP: zv2
- Access proxy VIP external IP address: 172.18.62.112
- Mapped real server IP address: 172.18.60.65

UTM and traffic log samples for each of the six event types:

1. Received an empty client certificate:
When connecting to the ZTNA access proxy, the client did not send a client certificate to the FortiGate for verification. The empty certificate is disallowed and blocked.
Traffic log:


```
1: date=2021-06-09 time=16:36:54 eventtime=1623281814371412983 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.206 srcport=56494 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=21453 proto=6 action="deny"
policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0
sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: empty
client certificate" utmref=65483-0
```

UTM log:

```
1: date=2021-06-09 time=16:36:54 eventtime=1623281814371409480 tz="-0700"
logid="2100060500" type="utm" subtype="ztna" eventtype="ztna-clt-cert" level="warning"
vd="root" msg="Client sends an empty certificate" policyid=5 sessionid=21453
srcip=10.1.100.206 dstip=172.18.62.112 srcport=56494 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked"
service="HTTPS" vip="zv2" accessproxy="zs2"
```

2. Received a client certificate that fails to validate:

When connecting to the ZTNA access proxy, the client sends a client certificate to the FortiGate for verification, but the certificate fails validation.

Traffic log:

```
2: date=2021-06-09 time=15:06:47 eventtime=1623276407372012365 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.206 srcport=55910 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=16810 proto=6 action="deny"
policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0
sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: client
certificate authentication failed" utmref=65491-0
```

UTM log:

```
1: date=2021-06-09 time=15:06:47 eventtime=1623276407372009447 tz="-0700"
logid="2100060501" type="utm" subtype="ztna" eventtype="ztna-clt-cert" level="warning"
vd="root" msg="Client certificate has security problem" policyid=5 sessionid=16810
srcip=10.1.100.206 dstip=172.18.62.112 srcport=55910 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked"
service="HTTPS" vip="zv2" accessproxy="zs2" desc="cert auth failed, cert-
cn:qa.wangd.com, cert-issuer:qa.wangd.com, cert-status:failure "
```

3. API gateway cannot be matched:

When connecting to the ZTNA access proxy, the client tries to connect to an API gateway that does not match any virtual host.

Traffic log:

```
1: date=2021-06-09 time=15:15:39 eventtime=1623276939601851410 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.206 srcport=55974 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=17152 proto=6 action="deny"
policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0
```

```
sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block" countzttna=2 msg="Denied: failed to match an API-gateway" utmref=65490-0
```

UTM log:

```
2: date=2021-06-09 time=15:15:39 eventtime=1623276939601849940 tz="-0700"
logid="2102060522" type="utm" subtype="zttna" eventtype="zttna-error" level="warning"
vd="root" msg="Unable to match an API-gateway" policyid=5 sessionid=17152
srcip=10.1.100.206 dstip=172.18.62.112 srcport=55974 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked"
service="HTTPS" vip="zv2" accessproxy="zs2" desc="HTTP url
(https://qbcd.test.com/test123456) failed to match an API-gateway with vhost
(name/hostname: _def_virtual_host/_def_virtual_host_)"
```

4. None of the real servers can be reached:

When connecting to the ZTNA access proxy, the client tries to connect to an API gateway but the real server cannot be reached.

Traffic log:

```
1: date=2021-06-09 time=15:17:49 eventtime=1623277069371491908 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.206 srcport=55988 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=17233 proto=6 action="deny"
policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="zttna" service="HTTPS" trandisp="noop" duration=0 sentbyte=0 rcvbyte=0
sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block" countzttna=2 msg="Denied: failed to match an API-gateway" utmref=65489-0
```

UTM log:

```
2: date=2021-06-09 time=15:17:49 eventtime=1623277069371490614 tz="-0700"
logid="2102060522" type="utm" subtype="zttna" eventtype="zttna-error" level="warning"
vd="root" msg="Unable to match an API-gateway" policyid=5 sessionid=17233
srcip=10.1.100.206 dstip=172.18.62.112 srcport=55988 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked"
service="HTTPS" vip="zv2" accessproxy="zs2" desc="HTTP url
(https://qbcd.test.com/test123456) failed to match an API-gateway with vhost
(name/hostname: _def_virtual_host/_def_virtual_host_)"
```

5. ZTNA rule (proxy policy) cannot be matched:

When connecting to the ZTNA access proxy, a ZTNA rule (proxy policy) cannot be matched. For example, no ZTNA rule is matched for the ZTNA tag assigned to the endpoint.

Traffic log:

```
1: date=2021-06-09 time=15:20:20 eventtime=1623277220133106783 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.206 srcport=56010 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=17456 proto=6 action="deny"
policyid=0 policytype="proxy-policy" service="HTTPS" trandisp="noop" duration=0
sentbyte=0 rcvbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block"
countzttna=2 msg="Denied: failed to match a proxy-policy" utmref=65488-26
```

UTM log:

```
2: date=2021-06-09 time=15:20:20 eventtime=1623277220133105204 tz="-0700"
logid="2101060510" type="utm" subtype="zttna" eventtype="zttna-policy-match"
```

```
level="warning" vd="root" msg="Connection is blocked due to unable to match a proxy-policy" policyid=0 sessionid=17456 srcip=10.1.100.206 dstip=172.18.62.112 srcport=56010 dstport=443 srcintf="port2" srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked" service="HTTPS" gatewayid=1 vip="zv2" accessproxy="zs2"
```

6. HTTPS SNI virtual host does not match the HTTP host header:

Traffic log:

```
1: date=2021-06-09 time=15:24:25 eventtime=1623277465275004842 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.1.100.206 srcport=56040 srcintf="port2" srcintfrole="undefined"
dstip=172.18.62.112 dstport=443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=17614 proto=6 action="deny"
policyid=5 policytype="policy" poluid="b4d4c466-8b64-51eb-2292-5defbb0e34e5"
policyname="ztna" service="HTTPS"trandisp="noop" duration=0 sentbyte=0 rcvbyte=0
sentpkt=0 rcvpkt=0 appcat="unscanned" utmaction="block" countztna=2 msg="Denied: failed to match an API-gateway" utmref=65486-0
```

UTM log:

```
2: date=2021-06-09 time=15:24:25 eventtime=1623277465275003194 tz="-0700"
logid="2102060522" type="utm" subtype="ztna" eventtype="ztna-error" level="warning"
vd="root" msg="Unable to match an API-gateway" policyid=5 sessionid=17614
srcip=10.1.100.206 dstip=172.18.62.112 srcport=56040 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="root" dstintfrole="undefined" proto=6 action="blocked"
service="HTTPS" vip="zv2" accessproxy="zs2" desc="HTTP url (https://aq4.test.com/) failed to match an API-gateway with vhost(name/hostname:_def_virtual_host/_def_virtual_host_)"
```

Logical AND for ZTNA tag matching - 7.0.2

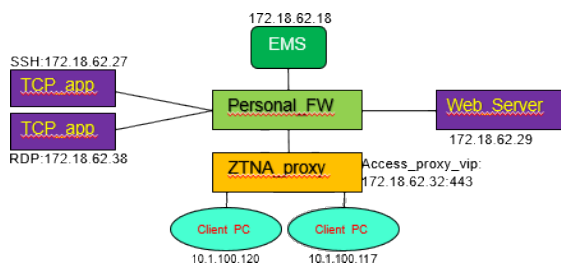
When specifying ZTNA tags in a rule, logical AND can be used for tag matching.

When editing a ZTNA rule:

- If *Match ZTNA Tags* is set to *All* the client must match all of the tags (logical AND).
- If *Match ZTNA Tags* is set to *Any* the client can match any of the tags (logical OR).

In these examples, there are two PCs with FortiClient: PC120 at 10.1.100.120 and PC117 at 10.1.100.117. There are two ZTNA EMS tags: `ems138_av_tag` and `ems138_running_app_tag`. PC120 has both of them, and PC117 only has one.

It is assumed that ZTNA has already been configured. For information, see [Zero Trust Network Access](#) in the FortiOS Administration Guide.



Logical AND example

To configure a ZTNA rule that requires both ZTNA EMS tags in the GUI:

1. Go to *Policy & Objects* > *ZTNA*, select the *ZTNA Rules* tab, and click *Create New*.
2. Configure the rule, adding both ZTNA EMS tags to *ZTNA Tag*, and setting *Match ZTNA Tags* to *All*.

3. Click **OK**.

To configure a ZTNA rule that requires both ZTNA EMS tags in the CLI:

```
config firewall proxy-policy
  edit 1
    set name "r1"
    set proxy access-proxy
    set access-proxy "ZTNA_S1"
    set srcintf "port2"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag "FCTEMS8821001056_ems138_av_tag" "FCTEMS8821001056_ems138_running_
app_tag"
    set ztna-tags-match-logic and
    set action accept
    set schedule "always"
  next
end
```

To check the results:

- PC117 only has one tag, so ZTNA traffic is blocked:

```
# diagnose test application fcnacd 7
```

ZTNA Cache V2:

Entry #2:

```
- UID: 083078C718674C72B7C8CA0C09EB99C7
- Domain:
```

```

- User: frank_117
- Owner:
- Certificate SN: 03CBD682154035C5E5FEA27F83DFC8F7398CDC60
- EMS SN: FCTEMS8821001056
- online: true
- Routes (2):
-- Route #0: IP=10.1.100.117, vfid=0
- Tags (4):
-- Tag (#0): Low
-- Tag (#1): all_registered_clients
-- Tag (#2): ems138_av_tag
-- Tag (#3): ems138_management_tag
lls_idx_mask = 0x00000001,

```

The WAD debug shows:

```

[V][p:296][s:413990][r:117440514] wad_fw_policy_match_dev_grp      :4651 dev tag
matching, info=0x7efff2ea7430, tag_cnt=8, on_line=1, conf ems-tag size=2
[V][p:296][s:413990][r:117440514] wad_dev_addr_match              :275  conf tag
name:FCTEMS8821001056_ems138_av_tag(30) matched, id=12! <----HERE
[V][p:296][s:413990][r:117440514] wad_fw_policy_match_dev_grp      :4687 pol_id = 1
unmatched dev id = 12
[V][p:296][s:413990][r:117440514] wad_fw_policy_match_dev         :4705 pol_id = 1
matched = 0
[V][p:296][s:413990][r:117440514] wad_fw_addr_match_ap           :1035 matching
ap:ZTNA_S2(7) with vip addr:ZTNA_S1(7)
[I][p:296][s:413990][r:117440514] wad_http_req_policy_set        :8009 match pid=296
policy-id=0 vd=0 in_if=4, out_if=13 10.1.100.117:49341 -> 172.18.62.27:443
[V][p:296][s:413990][r:117440514] wad_https_ap_pol_info_get      :7946 policy info
created, req=0x7efff02b6048, ses_ctx=0x7efff2f2e3a8, info=0x7efff32a8288
[I][p:296][s:413990][r:117440514] wad_http_req_proc_policy       :7735 web_cache
(http/https=0/0, fwd_srv=<nil>).
[E][p:296][s:413990][r:117440514] wad_http_req_proc_policy       :7755 POLICY DENIED

```

- PC120 has both tags, so ZTNA traffic is passed:

```
# diagnose test application fcnacd 7
```

ZTNA Cache V2:

Entry #1:

```

- UID: 5721ED0374564878BFA1725C5555CEBA
- Domain: fortios.local131
- User: tester1
- Owner:
- Certificate SN: 48EC63DCF1234D41AEE2B4301017F74893FC291A
- EMS SN: FCTEMS8821001056
- online: true
- Routes (2):
-- Route #0: IP=10.1.100.120, vfid=0

- Tags (6):
-- Tag (#0): ems138_running_app_tag
-- Tag (#1): all_registered_clients
-- Tag (#2): ems138_av_tag
-- Tag (#3): ems138_vulnerability_tag
-- Tag (#4): ems138_management_tag

```

```
-- Tag (#5): Low
lls_idx_mask = 0x00000001,
```

The WAD debug shows:

```
[V][p:293][s:413402][r:67108866] wad_fw_policy_match_dev_grp      :4651 dev tag
matching, info=0x7f918e62e608, tag_cnt=12, on_line=1,conf ems-tag size=2
[V][p:293][s:413402][r:67108866] wad_dev_addr_match              :275  conf tag
name:FCTEMS8821001056_ems138_av_tag(30) matched, id=12!
[V][p:293][s:413402][r:67108866] wad_dev_addr_match              :275  conf tag
name:FCTEMS8821001056_ems138_running_app_tag(39) matched, id=13!
[V][p:293][s:413402][r:67108866] wad_fw_policy_match_dev         :4705 pol_id = 1
matched = 1
[I][p:293][s:413402][r:67108866] wad_http_req_policy_set         :8009 match pid=293
policy-id=1 vd=0 in_if=4, out_if=13 10.1.100.120:57150 -> 172.18.62.27:443
```

Logical OR example

To configure a ZTNA rule that requires one of the ZTNA EMS tags in the GUI:

1. Go to *Policy & Objects > ZTNA*, select the *ZTNA Rules* tab, and click *Create New*.
2. Configure the rule, adding both ZTNA EMS tags to *ZTNA Tag*, and setting *Match ZTNA Tags* to *Any*.
3. Click *OK*.

To configure a ZTNA rule that requires one of the ZTNA EMS tags in the CLI:

```
config firewall proxy-policy
  edit 1
    set name "r1"
    set proxy access-proxy
    set access-proxy "ZTNA_S1"
    set srcintf "wan2"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag "FCTEMS8821001056_ems138_av_tag" "FCTEMS8821001056_ems138_running_
app_tag"
    set ztna-tags-match-logic or
    set action accept
    set schedule "always"
  next
end
```

To check the results:

Traffic on both PC120 and PC117 is passed successfully.

The WAD debugs show:

```
[[V][p:294][s:650635][r:83886096] wad_fw_policy_match_dev_grp      :4651 dev tag matching,
info=0x7f863d7e3430, tag_cnt=8, on_line=1,conf ems-tag size=2
[V][p:294][s:650635][r:83886096] wad_fw_policy_match_dev_grp      :4666 pol_id = 1 matched
dev id = 18
[V][p:294][s:650635][r:83886096] wad_fw_policy_match_dev         :4705 pol_id = 1 matched
= 1
[I][p:294][s:650635][r:83886096] wad_http_req_policy_set         :8009 match pid=294
policy-id=1 vd=0 in_if=4, out_if=13 10.1.100.117:55597 -> 172.18.62.27:443
```

```

[V][p:294][s:650635][r:83886096] wad_https_ap_pol_info_get      :7946  policy info
created, req=0x7f863d90a048, ses_ctx=0x7f863fc79ad8, info=0x7f863d7f7bb0

[V][p:290][s:650172][r:16777220] wad_fw_policy_match_dev_grp  :4651  dev tag matching,
info=0x7f1ad65a1228, tag_cnt=12, on_line=1, conf_ems-tag size=2
[V][p:290][s:650172][r:16777220] wad_fw_policy_match_dev_grp  :4666  pol_id = 1 matched
dev id = 18
[V][p:290][s:650172][r:16777220] wad_fw_policy_match_dev      :4705  pol_id = 1 matched
= 1
[I][p:290][s:650172][r:16777220] wad_http_req_policy_set      :8009  match pid=290
policy-id=1 vd=0 in_if=4, out_if=13 10.1.100.120:50865 -> 172.18.62.27:443
[V][p:290][s:650172][r:16777220] wad_https_ap_pol_info_get      :7946  policy info
created, req=0x7f1ad3ef1048, ses_ctx=0x7f1ad652ead8, info=0x7f1ad3e76048

```

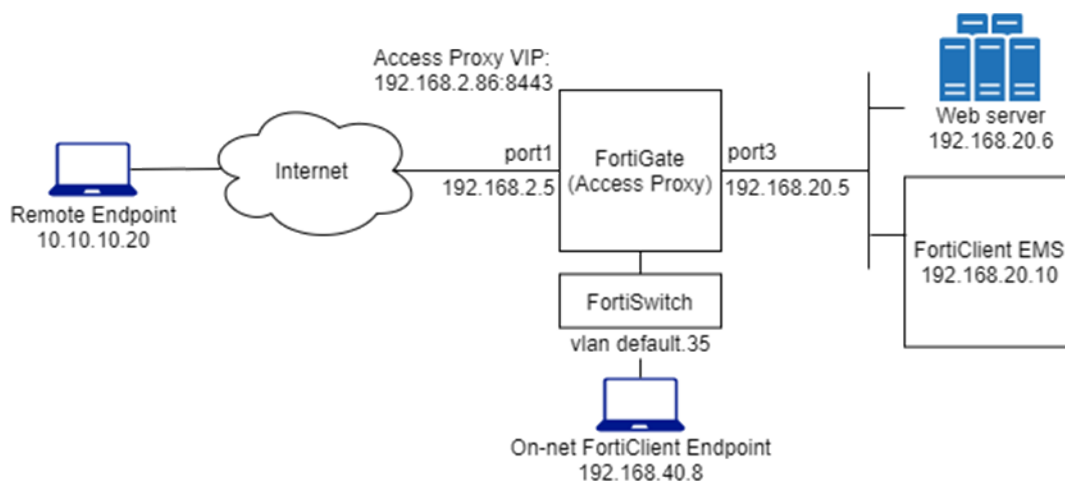
Implicitly generate a firewall policy for a ZTNA rule - 7.0.2

The firewall policy to forward traffic to the access proxy VIP is implicitly generated based on the ZTNA rule configuration, and does not need to be manually created.

To configure a ZTNA access proxy in the GUI, create the ZTNA server and then use the server in a ZTNA rule. Rules must include a source interface to indicate where the traffic is sourced from.

When upgrading to FortiOS 7.0.2, the ZTNA rule source interface will be set to *any* and all full ZTNA firewall policies will automatically be removed.

To perform IP/MAC filtering with ZTNA tags in a firewall policy, assign tags in the *IP/MAC Based Access Control* field. The toggle to select *Full ZTNA* or *IP/MAC filtering* is removed.



These examples assume that the FortiGate EMS fabric connector is already successfully connected.

Example 1 - Configuring a ZTNA HTTPS access proxy

In this example, a ZTNA access proxy is configured for HTTP access to the Web server from a remote endpoint.

To configure the ZTNA server in the GUI:

1. Go to *Policy & Objects > ZTNA*, select the *ZTNA Servers* tab, and click *Create New*.
2. Set *Name* to *WIN2K16-P1*.

3. Configure the *Network* settings:
 - a. Set *External interface* to *port1*.
 - b. Set *External IP* to *192.168.2.86*.
 - c. Set *External port* to *8443*.
4. Select a *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.
5. Add a server mapping:
 - a. In the *Service/server mapping* table click *Create New*.
 - b. Set *Service* to *HTTPS*
 - c. Set *Virtual Host* to *Any Host*.
- d. Add a server:
 - i. In the *Servers* table click *Create New*.
 - ii. Set *IP* to *192.168.20.6*.
 - iii. Set *Port* to *443*.
 - iv. Set *Status* as *Active*.
 - v. Click *OK*.
- e. Click *OK*.
6. Click *OK*.

To configure a ZTNA rule in the GUI:

1. Go to *Policy & Objects > ZTNA*, select the *ZTNA Rules* tab, and click *Create New*.
2. Set *Name* to *proxy-WIN2K16-P1*.
3. Set *Incoming Interface* to *port1*.
4. Set *Source* to *all*.
5. In *ZTNA Tag* add *Low*
6. In *ZTNA Server* add *WIN2K16-P1*.
7. Set *Destination* to *all*.
8. Set *Action* to *ACCEPT*.

New ZTNA Rule

Name	proxy-WIN2K16-P1
Incoming Interface	port1
Source	all
ZTNA Tag	Low
Match ZTNA Tags	Any All
ZTNA Server	WIN2K16-P1
Destination	all
Schedule	always
Action	ACCEPT DENY

Additional Information

API Preview

Documentation

- Online Help
- Video Tutorials
- Consolidated Policy Configuration

Security Profiles

OK Cancel

9. Configure the remaining options as needed.
10. Click *OK*.

To configure HTTPS access in the CLI:**1. Configure the access proxy VIP:**

```
config firewall vip
    edit "WIN2K16-P1"
        set type access-proxy
        set extip 192.168.2.86
        set extintf "port1"
        set server-type https
        set extport 8443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the server and path mapping:

```
config firewall access-proxy
    edit "WIN2K16-P1"
        set vip "WIN2K16-P1"
        set client-cert enable
        config api-gateway
            edit 1
                config realservers
                    edit 1
                        set ip 192.168.20.6
                    next
                end
            next
        end
    next
end
```

3. Configure the ZTNA rule:

```
config firewall proxy-policy
    edit 1
        set name "proxy-WIN2K16-P1"
        set proxy access-proxy
        set access-proxy "WIN2K16-P1"
        set srcintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "FCTEMS0000109188_Low"
        set action accept
        set schedule "always"
        set logtraffic all
    next
end
```

To test the remote access to the HTTPS access proxy:

1. On the remote endpoint, open FortiClient.
2. On the *Zero Trust Telemetry* tab, make sure that you are connected to the EMS server.
3. Open a browser and go to the address of the server, in this case <https://winserver.fgdocs.com:8443>, which resolves to 192.168.2.86:8443.
4. The browser prompts for the client certificate to use. Select the EMS signed certificate then click *OK*.

The client is verified by the FortiGate to authenticate your identity.

The FortiGate matches your security posture by verifying your ZTNA tag and matching the corresponding ZTNA rule, and you are allowed access to the web server.

5. Check the access in the Traffic log on the FortiGate:

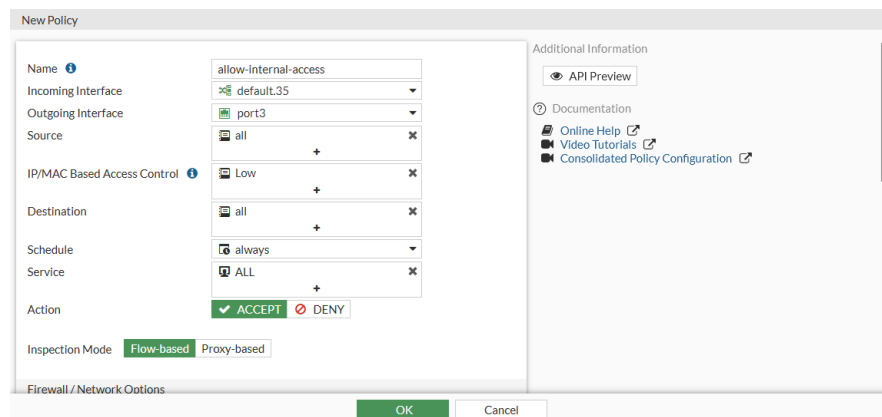
```
# execute log filter category 0
# execute log display
...
1: date=2021-10-17 time=23:45:42 eventtime=1634539543024700086 tz="-0700"
logid="0001000014" type="traffic" subtype="local" level="notice" vd="root"
srcip=10.10.10.20 srcport=65474 srcintf="port1" srcintfrole="wan" dstip=192.168.2.86
dstport=8443 dstintf="root" dstintfrole="undefined" srcuuid="5445be2e-5d7b-51ea-e2c3-
ae6b7855c52f" srccountry="Reserved" dstcountry="Reserved" sessionid=278276 proto=6
action="close" policyid=1 policytype="proxy-policy" poluuid="1aafa942-2fdc-51ec-b89f-
47fb64264865" polycname="proxy-WIN2K16-P1" service="tcp/8443" trandisp="noop"
app="tcp/8443" duration=18 sentbyte=5606 rcvbyte=108762 sentpkt=47 rcvpkt=80
appcat="unscanned" mastersrcmac="08:5b:0e:ea:7f:d4" srcmac="08:5b:0e:ea:7f:d4"
srcserver=0
```

Example 2 - Configuring a policy to perform posture checks using ZTNA tags

In this example, IP/MAC based access control is configured to allow traffic from an internal subnet when the endpoint is tagged as *Low* risk.

To configure a firewall policy to use IP/MAC based access control in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Set *Name* to *allow-internal-access*.
3. Set *Incoming Interface* to *default.35*.
4. Set *Outgoing Interface* to *port3*.
5. Set *Source* to *all*.
6. In *IP/MAC Based Access Control* add the ZTNA tag *Low*.
7. Set *Destination* to *all*.
8. Set *Service* to *ALL*.
9. Set *Action* to *ACCEPT*.
10. Enable *Log Allowed Traffic* and set it to *All Sessions*.



11. Configuring the remaining options as needed.
12. Click OK.

To configure a firewall policy to use IP/MAC based access control in the CLI:

```
config firewall policy
  edit 30
    set name "allow-internal-access"
    set srcintf "default.35"
    set dstintf "port3"
    set action accept
    set ztna-status enable
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag "FCTEMS0000109188_Low"
    set schedule "always"
    set service "ALL"
    set inspection-mode proxy
    set logtraffic all
    set nat enable
  next
end
```

To test the access to the web server from the on-net client endpoint:

1. On the on-net endpoint, open FortiClient.
2. On the *Zero Trust Telemetry* tab, make sure that you are connected to the EMS server.
3. Open a browser and go to the address of the server.

The FortiGate matches your security posture by verifying your ZTNA tag and matching the corresponding firewall policy (*allow-internal-access*), and you are allowed access to the web server.

4. Check the access in the Traffic log on the FortiGate:

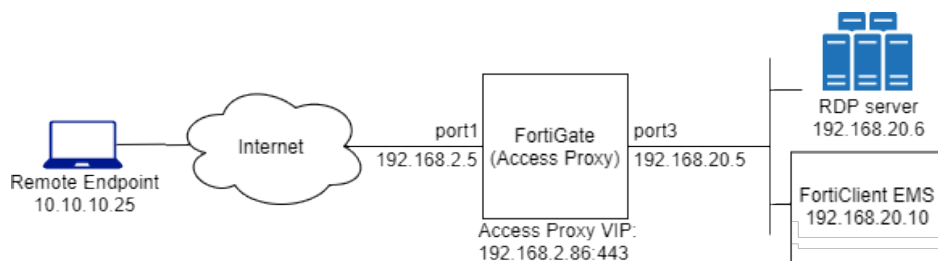
```
# execute log filter category 0
# execute log filter field dstip 192.168.20.6
# execute log display
...
1: date=2021-10-18 time=09:17:19 eventtime=1634573839454698399 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=192.168.40.6 srcname="Fortinet-KeithL" srcport=62756 srcintf="default.35"
srcintfrole="undefined" dstip=192.168.20.6 dstport=443 dstintf="port3"
dstintfrole="undefined" srcuuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f"
dstuuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f" srccountry="Reserved"
dstcountry="Reserved" sessionid=330678 proto=6 action="close" policyid=30
policytype="policy" poluid="8f6ea492-9034-51eb-f197-c00d803b7489" policyname="allow-
internal-access" service="HTTPS" trandisp="snat" transip=192.168.20.5 transport=62756
duration=6 sentbyte=3468 rcvdbyte=107732 sentpkt=50 rcvdpkt=80
fctuid="F4F3263AEBE54777A6509A8FCCDF9284" unauthuser="keithli"
unauthusersource="forticlient" appcat="unscanned" mastersrcmac="24:b6:fd:fa:54:c1"
srcmac="24:b6:fd:fa:54:c1" srcserver=0 dstosname="Windows" dstswversion="10"
masterdstmac="52:54:00:e3:4c:1a" dstmac="52:54:00:e3:4c:1a" dstserver=0
```

Posture check verification for active ZTNA proxy session - 7.0.2

Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy.

The FortiGate monitors changes to the endpoint tags that are updated by EMS with the fcnacd process. When a change is detected, the endpoint's active ZTNA sessions must match the ZTNA policy again before data can pass.

Changes to the ZTNA policy, such as changing the ZTNA tag matching logic, will also trigger re-verification of the client device against the policy.



The remote endpoint accesses the RDP server through the TCP forwarding access proxy. The proxy is managed by the FortiClient EMS server, which has a ZTNA tagging rule that assigns the *AV-enabled* tag to endpoints that have Windows antivirus enabled, and the *Low risk host* tag to endpoints that are low risk.

These examples assume that the FortiGate EMS fabric connector has already connected successfully, and a ZTNA server named WIN2K16-P1-RDP that forwards traffic to the RDP server has been configured.

Example 1 - The ZTNA tag status changes on the endpoint

In this example, a ZTNA rule is configured to allow access for endpoints that have the *AV-enabled* tag. After an RDP session is established, Windows antivirus is disabled on the remote endpoint. The FortiGate re-verifies the session and the active RDP session is removed from the FortiGate session table, causing the RDP session to be disconnected.

To configure the ZTNA rule in the GUI:

1. Go to *Policy & Objects > ZTNA*, select the *ZTNA Rules* tab, and click *Create New*.
2. Set *Name* to *TCP-forward-WIN2K16*.
3. Set *Incoming Interface* to *port1*.
4. Set *Source* to *all*.
5. In *ZTNA Tag* add *AV-enabled*
6. In *ZTNA Server* add *WIN2K16-P1-RDP*.
7. Set *Destination* to *all*.
8. Set *Action* to *ACCEPT*.
9. Configure the remaining options as needed.
10. Click *OK*.

To configure the ZTNA rule in the CLI:

```
config firewall proxy-policy
  edit 4
```

```

        set name "TCP-forward-WIN2K16"
        set proxy access-proxy
        set access-proxy "WIN2K16-P1-RDP"
        set srcintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "FCTEMS0000109188_AV-enabled"
        set action accept
        set schedule "always"
        set logtraffic all
    next
end

```

To test the example:

1. On the remote endpoint, open FortiClient.
2. On the *Zero Trust Telemetry* tab, make sure that you are connected to the EMS server.
3. Add a ZTNA rule:
 - a. On the *ZTNA Connection Rules* tab, click *Add Rule*.
 - b. Configure the ZTNA rule:

Rule Name	RDP-WIN2K16
Destination Host	192.168.20.6:3389
Proxy Gateway	192.168.2.86:443
Encryption	Disabled

- c. Click *Create*.
4. Ensure that the endpoint has Windows antivirus enabled.
5. Open an RDP session to connect to the RDP server at 192.168.20.6.
6. After a successful connection, on the FortiGate:
 - a. The endpoint is detected and marked with the *AV-enabled* tag:

```

# diagnose test application fcnacd 7

ZTNA Cache V2:
Entry #1:

- UID: F4F3263AEBE54777A6509A8FCCDF9284
- Domain:
- User: keithli
- Owner:
- Certificate SN: 1626C2C10E6AD97D71FA9E2D9C314C1F5C03D68B
- EMS SN: FCTEMS0000109188
- online: true
- Tags (3):
  -- Tag (#0): AV-enabled
  -- Tag (#1): all_registered_clients
  -- Tag (#2): Low
lls_idx_mask = 0x00000001,

```

- b. A session is created:

```
# diagnose sys session filter dst 192.168.2.86
# diagnose sys session filter src 10.10.10.25
# diagnose sys session list

session info: proto=6 proto_state=01 duration=191 expire=3599 timeout=3600
flags=00000000 socktype=0 sockport=1012 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log local may_dirty f24
statistic(bytes/packets/allow_err): org=58031/376/1 reply=66864/351/1 tuples=2
tx speed(Bps/kbps): 303/2 rx speed(Bps/kbps): 349/2
orgin->sink: org pre->in, reply out->post dev=3->7/7->3 gwy=192.168.2.86/0.0.0.0
hook=pre dir=org act=noop 10.10.10.25:60668->192.168.2.86:443(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.2.86:443->10.10.10.25:60668(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:ea:7f:d4
misc=7 policy_id=4 pol_uuid_idx=14853 auth_info=0 chk_client_info=0 vd=0
serial=00000c0b tos=00/00 app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=00000000
total session 1
```

c. The forward traffic log indicates that traffic is allowed:

```
# execute log filter category 0
# execute log filter field dstip 192.168.20.6
# execute log display
...
11: date=2021-10-18 time=11:22:16 eventtime=1634581336644493852 tz="-0700"
logid="0000000024" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.10.10.25 srcport=60660 srcintf="port1" srcintfrole="wan"
dstcountry="Reserved" srccountry="Reserved" dstip=192.168.20.6 dstport=3389
dstintf="root" dstintfrole="undefined" sessionid=2550 srcuuid="5445be2e-5d7b-51ea-
e2c3-ae6b7855c52f" service="RDP" proto=6 action="accept" policyid=4
policytype="proxy-policy" poluuid="ce8f82d0-8fb3-51eb-0a17-5e6a6a51ff27"
policyname="TCP-forward-WIN2K16" duration=0 wanin=1578 rcvdbyte=1578 wanout=1107
lanin=2788 sentbyte=2788 lanout=3750 srchwvendor="Fortinet" devtype="Network"
srcfamily="Firewall" osname="FortiOS" srchwversion="FortiWiFi-30E" appcat="unscanned"
```

7. On the remote endpoint, disable Windows antivirus.

FortiClient EMS detects a change in ,and removes the *AV-enabled* tag on the FortiClient endpoint.

8. Due to the change in posture, the RDP session is disconnected:

a. The endpoint is no longer marked with the *AV-enabled* tag:

```
# diagnose test application fcnacd 7

ZTNA Cache V2:
Entry #1:

- UID: F4F3263AEBE54777A6509A8FCCDF9284
- Domain:
- User: keithli
- Owner:
```

```

- Certificate SN: 1626C2C10E6AD97D71FA9E2D9C314C1F5C03D68B
- EMS SN: FCTEMS0000109188
- online: true
- Tags (2):
  -- Tag (#0): all_registered_clients
  -- Tag (#1): Low
lls_idx_mask = 0x00000001,

```

b. The previous session is removed:

```

# diagnose sys session filter dst 192.168.2.86
# diagnose sys session filter src 10.10.10.25
# diagnose sys session list
total session 0

```

c. The forward traffic log indicates that traffic is denied:

```

# execute log display
7: date=2021-10-18 time=11:31:45 eventtime=1634581905530844852 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.10.10.25 srcport=60668 srcintf="port1" srcintfrole="wan" dstip=192.168.20.6
dstport=3389 dstintf="root" dstintfrole="undefined" srcuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f"
dstuid="5445be2e-5d7b-51ea-e2c3-ae6b7855c52f" srccountry="Reserved"
dstcountry="Reserved" sessionid=3083 proto=6 action="deny" policyid=4
policytype="proxy-policy" poluid="ce8f82d0-8fb3-51eb-0a17-5e6a6a51ff27"
policyname="TCP-forward-WIN2K16" service="RDP" trandisp="noop" duration=0 sentbyte=0
rcvbyte=0 sentpkt=0 rcvpkt=0 appcat="unscanned" utmaction="block" countztina=1
msg="Denied: failed to match a proxy-policy" utmref=65349-5754

```

d. The ZTNA log indicates that traffic is denied:

```

# execute log filter category 21
# execute log display
6: date=2021-10-18 time=11:31:45 eventtime=1634581905530840484 tz="-0700"
logid="2101060510" type="utm" subtype="ztna" eventtype="ztna-policy-match"
level="warning" vd="root" msg="Connection is blocked due to unable to match a proxy-
policy" policyid=4 sessionid=3083 srcip=10.10.10.25 dstip=192.168.20.6 srcport=60668
dstport=3389 srcintf="port1" srcintfrole="wan" dstintf="root" dstintfrole="undefined"
proto=6 action="blocked" service="HTTPS" gatewayid=1 vip="WIN2K16-P1-RDP"
accessproxy="WIN2K16-P1-RDP" clientdeviceid="F4F3263AEBE54777A6509A8FCCDF9284"
clientdevicetags="MAC_FCTEMS0000109188_Low/FCTEMS0000109188_all_registered_
clients/MAC_FCTEMS0000109188_all_registered_clients/FCTEMS0000109188_Low"

```

Example 2 - The ZTNA rule tag checking logic changes

In this example, a ZTNA rule is configured to allow access to endpoints that have at least one of the *AV-enabled* or *Low* ZTNA tags. A remote user who has Windows antivirus disabled, but is low risk, successfully establishes an RDP session over the ZTNA access proxy. An administrator changes the ZTNA rule's tag matching logic from *Any* to *All*, causing the RDP session to be disconnected.

To configure the ZTNA rule in the GUI:

1. Go to *Policy & Objects > ZTNA*, select the *ZTNA Rules* tab.
2. Edit the *TCP-forward-WIN2K16* rule.
3. In *ZTNA Tag*, add *Low*.

4. Ensure that *Match ZTNA Tags* is set to *Any*.
5. Click OK.

To configure the ZTNA rule in the CLI:

```
config firewall proxy-policy
  edit 4
    set name "TCP-forward-WIN2K16"
    set proxy access-proxy
    set access-proxy "WIN2K16-P1-RDP"
    set srcintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag "FCTEMS0000109188_AV-enabled" "FCTEMS0000109188_Low"
    set ztna-tags-match-logic or
    set action accept
    set schedule "always"
    set logtraffic all
  next
end
```

To test the example:

1. On the remote Windows PC, disable antivirus protection.
2. Open an RDP session to connect to the RDP server at 192.168.20.6.
3. After a successful connection, on the FortiGate:
 - a. The endpoint is detected and marked with the *Low* tag, but not the *AV-enabled* tag:

```
# diagnose test application fcnacd 7

ZTNA Cache V2:
Entry #1:

- UID: F4F3263AEBE54777A6509A8FCCDF9284
- Domain:
- User: keithli
- Owner:
- Certificate SN: 1626C2C10E6AD97D71FA9E2D9C314C1F5C03D68B
- EMS SN: FCTEMS0000109188
- online: true
- Tags (2):
  -- Tag (#0): all_registered_clients
  -- Tag (#1): Low
lls_idx_mask = 0x00000001,
```

- b. A session is created:

```
# diagnose sys session filter dst 192.168.2.86
# diagnose sys session filter src 10.10.10.25
# diagnose sys session list

session info: proto=6 proto_state=01 duration=29 expire=3598 timeout=3600
flags=00000000 socktype=0 sockport=1012 av_idx=0 use=3
origin-shaper=
reply-shaper=
```



```

per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log local may_dirty f24
statistic(bytes/packets/allow_err): org=54763/299/1 reply=90223/313/1 tuples=2
tx speed(Bps/kbps): 1860/14 rx speed(Bps/kbps): 3064/24
origin->sink: org pre->in, reply out->post dev=3->7/7->3 gwy=192.168.2.86/0.0.0.0
hook=pre dir=org act=noop 10.10.10.25:55147->192.168.2.86:443(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.2.86:443->10.10.10.25:55147(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:ea:7f:d4
misc=7 policy_id=4 pol_uuid_idx=14853 auth_info=0 chk_client_info=0 vd=0
serial=00003255 tos=00/00 app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_link_id=00000000 rpd_svc_id=0 ngfwid=n/a

```

c. The forward traffic log indicates that traffic is allowed:

```

# execute log filter category 0
# execute log display
...
1: date=2021-10-18 time=12:46:01 eventtime=1634586361077487880 tz="-0700"
logid="0000000024" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.10.10.25 srcport=55140 srcintf="port1" srcintfrole="wan"
dstcountry="Reserved" srccountry="Reserved" dstip=192.168.20.6 dstport=3389
dstintf="root" dstintfrole="undefined" sessionid=12542 srcuuid="5445be2e-5d7b-51ea-
e2c3-ae6b7855c52f" service="RDP" proto=6 action="accept" policyid=4
policytype="proxy-policy" poluuid="ce8f82d0-8fb3-51eb-0a17-5e6a6a51ff27"
policyname="TCP-forward-WIN2K16" duration=138 wanin=140349 rcvdbyte=140349
wanout=47118 lanin=48799 sentbyte=48799 lanout=142521 appcat="unscanned"

```

4. On the FortiGate, edit the ZTNA rule *TCP-forward-WIN2K16*:

- In the GUI, set *Match ZTNA Tags* to *All*.
- In the CLI, set `ztna-tags-match-logic` to `and`.

5. Due to the ZTNA rule update, the FortiGate re-verifies the session, and the RDP session is disconnected:

a. The previous session is removed:

```

# diagnose sys session filter dst 192.168.2.86
# diagnose sys session filter src 10.10.10.25
# diagnose sys session list
total session 0

```

b. The ZTNA log indicates that traffic is denied:

```

# execute log filter category 21
# execute log display
1: date=2021-10-18 time=12:53:57 eventtime=1634586837921889075 tz="-0700"
logid="2101060510" type="utm" subtype="ztna" eventtype="ztna-policy-match"
level="warning" vd="root" msg="Connection is blocked due to unable to match a proxy-
policy" policyid=0 sessionid=13865 srcip=10.10.10.25 dstip=192.168.2.86 srcport=55162
dstport=443 srcintf="port1" srcintfrole="wan" dstintf="root" dstintfrole="undefined"
proto=6 action="blocked" service="HTTPS" gatewayid=1 vip="WIN2K16-P1-RDP"
accessproxy="WIN2K16-P1-RDP" clientdeviceid="F4F3263AEBE54777A6509A8FCCDF9284"
clientdevicetags="MAC_FCTEMS0000109188_Low/FCTEMS0000109188_all_registered_
clients/MAC_FCTEMS0000109188_all_registered_clients/FCTEMS0000109188_Low"

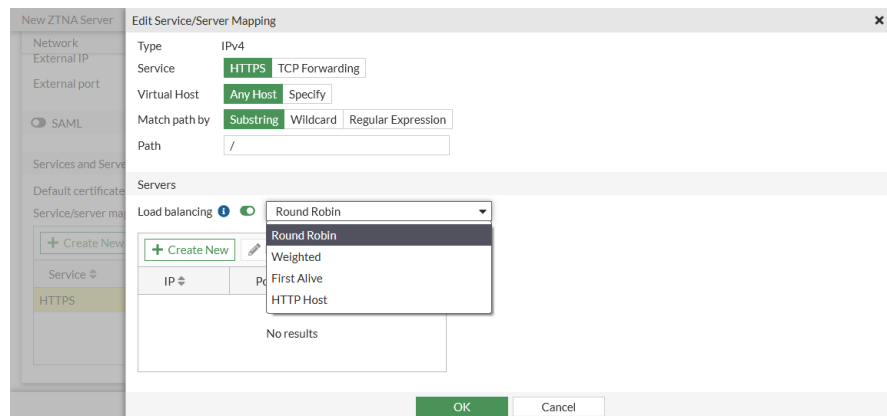
```

GUI support for multiple ZTNA features - 7.0.2

When configuring a ZTNA server, load balancing, TCP forwarding, and SAML can be configured in the GUI.

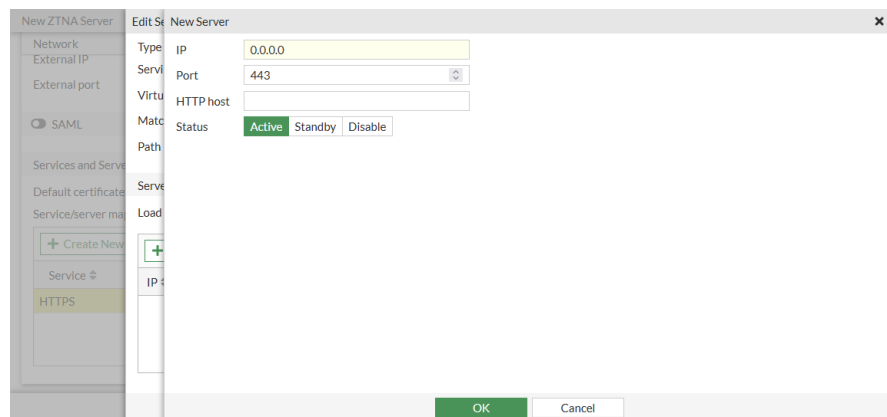
Load balancing

Load balancing can be configured when adding or editing a service or server mapping.



When adding a load balancing server:

- If the load balancing method is *Weighted* then the weight can be included.
- If the method is *HTTP Host* an HTTP host server domain name can be included in the HTTP header that is forwarded to the real server.



TCP forwarding and SSH

TCP forwarding can be selected as the service when adding or editing a service or server mapping.

New ZTNA Server

New Service/Server Mapping

Type: IPv4

Service: HTTPS TCP Forwarding

Servers

+ Create New Edit Delete

Address	Ports
No results	

OK Cancel

Add servers from firewall addresses. Enable *Enable Additional SSH Option* to configure a client certificate and host key validation.

New ZTNA Server

New Server

Type: Address

Ports: Comma separated port or port range

Server

Enable Additional SSH Options

Client certificate: [Dropdown]

Host key validation: [Checked]

Host key: [Field with + button]

OK Cancel

A client certificate allows users to perform one-time user authentication to authenticate the SSH access proxy. See [ZTNA SSH access proxy example](#) for details. Select a certificate from the drop-down list, or create a new one.

New ZTNA Server

New Server Edit ZTNA Server SSH Client Certificate

Type: Name

Port: CA certificate

Server

Enable Additional SSH Options

Client

Name	Type
No results	

Append source address: [Checked]

Allow X11 forwarding: [Checked]

Allow agent forwarding: [Checked]

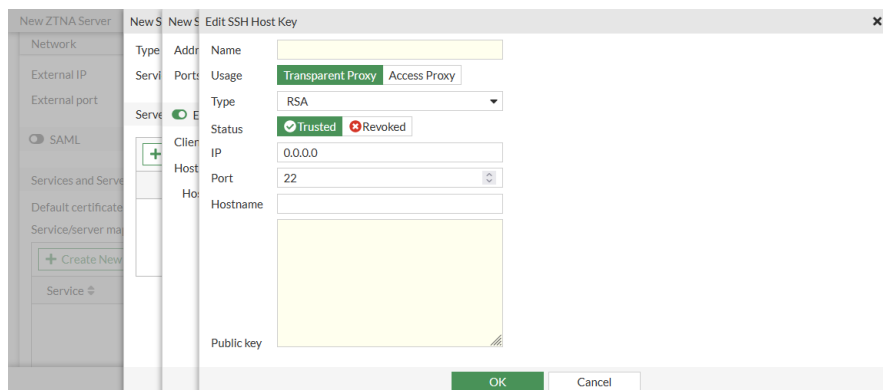
Allow port forwarding: [Checked]

Allow PTY: [Checked]

Allow user RC: [Checked]

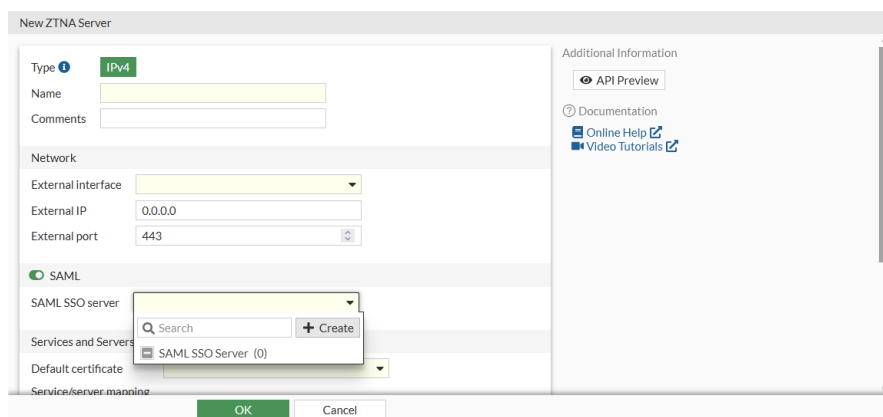
OK Cancel

Host key validation allows the ZTNA proxy to validate the SSH server using the host key before forwarding traffic to it. Click in the *Host key* field to add or create an SSH host key.

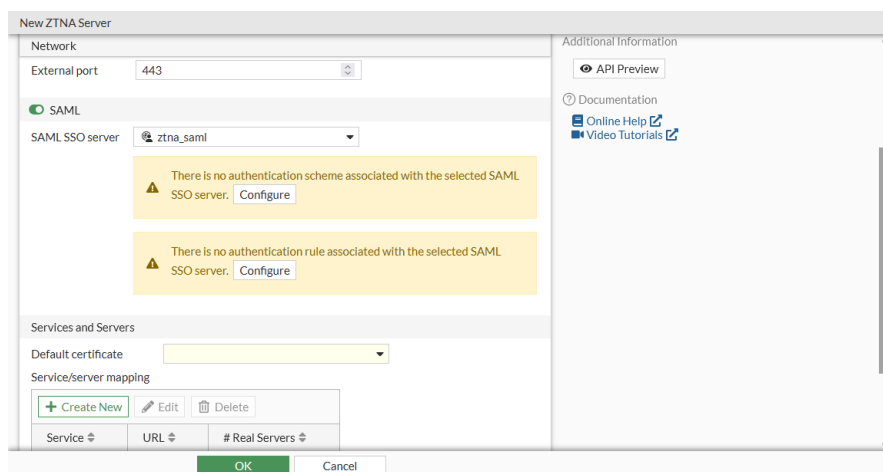


SAML

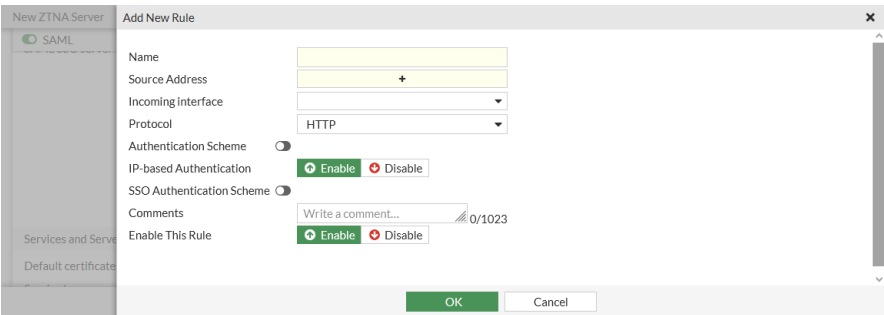
SAML can be enabled when configuring a ZTNA server, and a SAML SSO server can be selected or created.



If the SAML SSO server does not have an authentication scheme or rule associated with it, warnings are shown.



Click **Configure** in each warning to add an authentication scheme and rule.



NGFW

This section includes information about NGFW policy mode related new features:

- [Filters for application control groups in NGFW mode on page 375](#)

Filters for application control groups in NGFW mode

When defining application groups in NGFW policy mode, the following group filters are now available: protocols, risk, vendor, technology, behavior, popularity, and category.

```
config application group
  edit <name>
    set type filter
    set protocols <integer>
    set risk <integer>
    set vendor <id>
    set technology <id>
    set behavior <id>
    set popularity <integer>
    set category <id>
  next
end
```

protocols <integer>	Application protocol filter (0 - 47, or all).
risk <integer>	Risk or impact of allowing traffic from this application to occur (1 - 5; low (1), elevated (2), medium (3), high (4), and critical (5)).
vendor <id>	Application vendor filter (0 - 25, or all).
technology <id>	Application technology filter: <ul style="list-style-type: none">• all• 0 (network-protocol)• 1 (browser-based)• 2 (client-server)• 4 (peer-to-peer)
behavior <id>	Application behavior filter:

	<ul style="list-style-type: none"> • all • 2 (botnet) • 3 (evasive) • 5 (excessive bandwidth) • 6 (tunneling) • 9 (cloud)
popularity <integer>	Application popularity filter (1 - 5, from least to most popular).
category <id>	Application category filter: <ul style="list-style-type: none"> • 2 (P2P) • 3 (VoIP) • 5 (video/audio) • 6 (proxy) • 7 (remote access) • 8 (game) • 12 (general interest) • 15 (network service) • 17 (update) • 21 (email) • 22 (storage backup) • 23 (social media) • 25 (web client) • 26 (industrial) • 28 (collaboration) • 29 (business) • 30 (cloud IT) • 31 (mobile) • 32 (unknown applications)

Sample configurations

In this example, a single filter (risk level 1) is configured in the application group, so only signatures matching this filter will match the security policy.

To configure the application group:

```
config application group
    edit "risk_1"
        set type filter
        set risk 1
    next
end
```

To configure the security policy:

```
config firewall security-policy
    edit 1
        set srcintf "port2"
```

```
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set status enable
        set schedule "always"
        set enforce-default-app-port disable
        set service "ALL"
        set app-group risk_1
        set logtraffic all
    next
end
```

In this example, the application group is configured so that only signatures matching both filters, category 5 (video/audio) and technology 1 (browser-based), will match the security policy. The application group can also be configured in a traffic shaping policy.

To configure the application group:

```
config application group
    edit "two"
        set type filter
        set category 5
        set technology 1
    next
end
```

To configure the security policy:

```
config firewall security-policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set status enable
        set schedule "always"
        set enforce-default-app-port disable
        set service "ALL"
        set app-group two
        set logtraffic all
    next
end
```

To configure the traffic shaping policy:

```
config firewall shaping-policy
    edit 1
        set ip-version 4
        set service "ALL"
        set app-group two
        set dstintf port1
        set traffic-shaper "max-100"
        set traffic-shaper-reverse "max-100"
        set srcaddr "all"
```

```

        set dstaddr "all"
    next
end

```

Policies

This section includes information about policy related new features:

- [DNS health check monitor for server load balancing on page 378](#)
- [Carrier-grade NAT on page 379](#)
- [Allow multiple virtual wire pairs in a virtual wire pair policy on page 382](#)
- [Simplify NAT46 and NAT64 policy and routing configurations 7.0.1 on page 384](#)
- [Cisco Security Group Tag as policy matching criteria 7.0.1 on page 395](#)

DNS health check monitor for server load balancing

A DNS health check monitor can be configured for server load balancing. The monitor uses TCP or UDP DNS as the probes. The request domain is matched against the configured IP address to verify the response.

The DNS health check monitor does not support IPv6.

To create a DNS health check monitor:

```

config firewall ldb-monitor
    edit <name>
        set type dns
        set port <string>
        set dns-protocol {udp | tcp}
        set dns-request-domain <string>
        set dns-match-ip <class_ip>
    next
end

```

type	The monitor type that is used by the health check monitor to check the health of the server.
port <string>	The service port that is used to perform the health check (0 - 65535, default = 0). If type is set to dns, port is set to 53.
dns-protocol {udp tcp}	The protocol used by the DNS health check monitor to check the health of the server (default = udp).
dns-request-domain <string>	The fully qualified domain name to resolve for the DNS probe (default = www.example.com).
dns-match-ip <class_ip>	The response IP address expected from the DNS server (default =

Example

In this example, a DNS health check monitor is created and used in a VIP.

The FortiGate sends the DNS request on UDP port 53 to the configured real servers every 30 seconds. If the DNS response from a real server matches the DNS match IP address, then the real server is marked as Active. Otherwise, it is marked as Down.

To configure the health check monitor:

1. Create a new DNS health check monitor:

```
config firewall ldb-monitor
  edit "dns-monitor-1"
    set type dns
    set interval 30
    set port 53
    set src-ip 172.16.200.10
    set dns-request-domain "pc4.qa.fortinet.com"
    set dns-match-ip 172.16.200.44
  next
end
```

2. Apply the monitor to a virtual server:

```
config firewall vip
  edit "test-vs-ip-1"
    set type server-load-balance
    set extip 10.1.100.153
    set extintf "wan2"
    set server-type ip
    set monitor "dns-monitor-1"
    set ldb-method round-robin
    config realservers
      edit 1
        set ip 172.16.200.44
      next
      edit 2
        set ip 172.16.200.55
      next
    end
  next
end
```

Carrier-grade NAT

Users can control concurrent TCP/UDP connections through a connection quota in the per-IP shaper, and can control the port quota in the fixed port range IP pool.

```
config firewall shaper per-ip-shaper
  edit <name>
    set max-concurrent-tcp-session <integer>
    set max-concurrent-udp-session <integer>
  next
end
```

max-concurrent-tcp-session <integer>

Maximum number of concurrent TCP sessions allowed by this shaper (0 - 2097000, 0 = no limit).

<pre>max-concurrent-udp- session <integer></pre>	<p>Maximum number of concurrent UDP sessions allowed by this shaper (0 - 2097000, 0 = no limit).</p>
--	--

```
config firewall ippool
  edit <name>
    set type fixed-port-range
    set port-per-user <integer>
  next
end
```

<pre>set port-per-user <integer></pre>	<p>Number of ports for each user (32 - 60416, 0 = default).</p>
--	---

To configure a connection quota in the GUI:

1. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shapers* tab, and click *Create New*.
2. For *Type*, select *Per IP Shaper*.
3. Enable *Max concurrent TCP connections* and enter a value.
4. Enable *Max concurrent UDP connections* and enter a value.

5. Configure the other settings as needed.
6. Click **OK**.

To configure a connection quota in the CLI:

```
config firewall shaper per-ip-shaper
  edit "per-ip-shaper256kbps"
    set max-bandwidth 256
    set max-concurrent-session 10
    set max-concurrent-tcp-session 5
    set max-concurrent-udp-session 5
  next
end
```

To configure a port quota in the GUI:

1. Go to *Policy & Objects > IP Pools* and click *Create New*.
2. For *Type*, select *Fixed Port Range*.

3. Enter the external and internal IP ranges.
4. Enable *Ports Per User* and enter a value.

FortiGate
KVM64-3639

Additional Information
API Preview
References
Edit in CLI

Documentation
Online Help
Video Tutorials

OK Cancel

5. Configure the other settings as needed.
6. Click OK.

To configure a port quota in the GUI:

```
config firewall ippool
    edit "test-ippool-fpr-1"
        set type fixed-port-range
        set startip 172.16.200.125
        set endip 172.16.200.125
        set source-startip 10.1.100.41
        set source-endip 10.1.100.42
        set port-per-user 30208
    next
end
```

To verify the fixed range IP pool:

```
# diagnose firewall ippool-fixed-range list natip 172.16.200.125
ippool name=test-ippool-fpr-1, ip shared num=2, port num=30208
internal ip=10.1.100.41, nat ip=172.16.200.125, range=5117~35324
internal ip=10.1.100.42, nat ip=172.16.200.125, range=35325~65532
```

To verify the SNAT behavior when the IP pool is used in a policy:

```
# diagnose sniffer packet any 'host 172.16.200.55'
Using Original Sniffing Mode
interfaces=[any]
filters=[host 172.16.200.55]
32.204955 wan2 in 10.1.100.42.21001 -> 172.16.200.55.80: syn 797929945
32.205027 wan1 out 172.16.200.125.51209 -> 172.16.200.55.80: syn 797929945
32.205328 wan1 in 172.16.200.55.80 -> 172.16.200.125.51209: syn 4191137758 ack 797929946
32.205568 wan2 out 172.16.200.55.80 -> 10.1.100.42.21001: syn 4191137758 ack 797929946
32.205766 wan2 in 10.1.100.42.21001 -> 172.16.200.55.80: ack 4191137759
32.205770 wan1 out 172.16.200.125.51209 -> 172.16.200.55.80: ack 4191137759
```

Allow multiple virtual wire pairs in a virtual wire pair policy

This enhancement allows users to create a virtual wire pair policy that includes different virtual wire pairs (VWPs). This reduces overhead to create multiple similar policies for each VWP. This feature is supported in NGFW profile and policy mode. In NGFW policy mode, multiple VWPs can be configured in a *Security Virtual Wire Pair Policy*, and *Virtual Wire Pair SSL Inspection & Authentication* policy.

The VWP settings must have wildcard VLAN enabled. When configuring a policy in the CLI, the VWP members must be entered in `srcintf` and `dstintf` as pairs.

On the *Firewall Virtual Wire Pair Policy*, *Security Virtual Wire Pair Policy*, and *Virtual Wire Pair SSL Inspection & Authentication* pages, there is a dropdown option to view policies with an individual VWP or all VWPs.

If *All VWPs* is selected, the *Interface Pair View* is disabled. The list displays all policies with an individual VWP or multiple VWPs.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	vwp1&2-policy	port19 To_vlan20 (wan2)	port20 To_vlan30 (wan1)	all	all	always	ALL	ACCEPT	Disabled	no-inspection	All	32.14 kB
2	vwp1-policy	To_vlan20 (wan2)	To_vlan30 (wan1)	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
3	vwp2-policy	port20	port19	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
4	vwp1&2&3-policy	port15 port16 To_vlan30 (wan1) port19 To_vlan20 (wan2) port20	port15 port16 To_vlan20 (wan2) port20 To_vlan30 (wan1) port19	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B

0 Security Rating Issues Updated: 10:02:40

If an individual VWP is selected, the *Interface Pair View* is disabled if at least one policy has other VWP members. The list displays all policies with the selected VWP (the policy may have members of other VWPs).

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	vwp1&2-policy	port19 To_vlan20 (wan2)	port20 To_vlan30 (wan1)	all	all	always	ALL	ACCEPT	Disabled	no-inspection	All	32.14 kB
2	vwp1-policy	To_vlan20 (wan2)	To_vlan30 (wan1)	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
4	vwp1&2&3-policy	port15 port16 To_vlan30 (wan1) port19 To_vlan20 (wan2) port20	port15 port16 To_vlan20 (wan2) port20 To_vlan30 (wan1) port19	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B

0 Security Rating Issues Updated: 10:09:50

To configure multiple VWPs in a policy in the GUI:

1. Configure the VWPs:
 - a. Go to *Network > Interfaces* and click *Create New > Virtual Wire Pair*.
 - b. Create a pair with the following settings:

Name	test-vwp-1
Interface members	wan1, wan2
Wildcard VLAN	Enable

- c. Click OK.

- d. Click *Create New > Virtual Wire Pair* and create another pair with the following settings:

Name	test-vwp-2
Interface members	port19, port20
Wildcard VLAN	Enable

- e. Click *OK*.

2. Configure the policy:

- Go to *Policy & Objects > Firewall Virtual Wire Pair Policy* and click *Create New*.
- In the *Virtual Wire Pair* field, click the + to add *test-vwp-1* and *test-vwp-2*. Arrow buttons appear below the entries to set the direction for each of the selected virtual wire pairs.

- c. Configure the other settings as needed.

- d. Click *OK*.

To configure multiple VWP in a policy in the CLI:

1. Configure the VWPs:

```
config system virtual-wire-pair
  edit "test-vwp-1"
    set member "wan1" "wan2"
    set wildcard-vlan enable
  next
  edit "test-vwp-2"
    set member "port19" "port20"
    set wildcard-vlan enable
  next
end
```

2. Configure the policy:

```
config firewall policy
  edit 1
    set name "vwp1&2-policy"
```

```
set srcintf "port19" "wan1"
set dstintf "port20" "wan2"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set logtraffic all
next
end
```

Simplify NAT46 and NAT64 policy and routing configurations - 7.0.1

Multiple NAT46 and NAT64 related objects are consolidated into regular objects. A new per-VDOM virtual interface, `naf.<vdom>`, is automatically added to process NAT46/NAT64 traffic. The new changes and additions include:

- Consolidate `vip46` and `vip64` setting into `vip` and `vip6` configurations.
- Consolidate `policy46` and `policy64` settings into `firewall policy` settings.
- Introduce `nat46/nat64` in `firewall policy` settings.
- Extend `ippool` and `ippool6` to support NAT46 and NAT64 (when enabled, the IP pool should match a subnet).
- Extend central SNAT to support NAT46 and NAT64.
- Remove `firewall vip46/vip64`, `vipgrp46/vipgrp64`, and `policy46/policy64` settings and GUI pages.
- Rename `system.nat64` to `system.dns64`.
- Add option for `add-nat46-route` in `ippool6` and `add-nat64-route` in `ippool`, which are enabled by default. The FortiGate will generate a static route that matches the IP range in `ippool6` or `ippool` for the `naf` tunnel interface.

To configure NAT46/NAT64 translation, use the standard `vip/vip6` setting, apply it in a firewall policy, enable NAT46/NAT64, and enter the IP pool to complete the configuration.



Automatic processing of the `naf` tunnel interface is not supported in security policies.

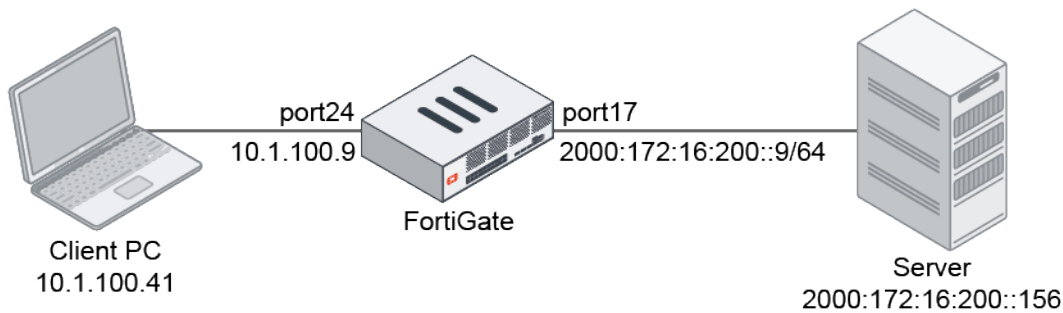
Examples

IPv6 must be enabled to configure these examples. In the GUI, so go to *System > Feature Visibility* and enable *IPv6*. In the CLI, enter the following:

```
config system global
    set gui-ipv6 enable
end
```

NAT46 policy

In this example, a client PC is using IPv4 and an IPv4 VIP to access a server that is using IPv6. The FortiGate uses NAT46 to translate the request from IPv4 to IPv6 using the virtual interface `naf.root`. An `ippool6` is applied so that the request is SNATed to the `ippool6` address (2000:172:16:101::1 - 2000:172:16:101::1).



To create a NAT46 policy in the GUI:

1. Configure the VIP:
 - a. Go to *Policy & Objects > Virtual IPs* and click *Create New > VIP*.
 - b. Enter the following:

VIP type	IPv4
Name	test-vip46-1
Interface	To_vlan20
Type	Static NAT
External IP address/range	10.1.100.150
Map to IPv6 address/range	2000:172:16:200::156

New Virtual IP

VIP type: ☒ IPv4 ☐ IPv6

Name: test-vip46-1

Comments: Write a comment... 0/255

Color: Change

Network

Interface:

Type: ☒ Static NAT ☐ FQDN

External IP address/range:

Map to

IPv4 address/range:

IPv6 address/range:

☐ Optional Filters

☐ Port Forwarding

FortiGate

FGT-1500D

Statistics (since last reset)

ID	
Last used	N/A
First used	N/A
Hit count	0

Clear Counters

Additional Information

API Preview

Documentation

Online Help

Video Tutorials

OK

Cancel

- c. Click OK.
2. Configure the IPv6 pool:
 - a. Go to *Policy & Objects > IP Pools* and click *Create New*.
 - b. Enter the following:

IP Pool Type	IPv6 Pool
Name	test-ippool6-1

External IP address/range	2000:172:16:101::1-2000:172:16:101::1
NAT46	Enable

New Dynamic IP Pool

IP Pool Type
IPv4 Pool
IPv6 Pool

Name
test-ippool6-1

Comments
Write a comment...
0/255

External IP address/range
2000:172:16:101::1-2000:172:16:101:

NAT46

FortiGate
FGT-1500D

Additional Information
API Preview
Documentation
Online Help
Video Tutorials

OK
Cancel

c. Click **OK**.

3. Configure the firewall policy:

- a. Go to **Policy & Objects > Firewall Policy** and click **Create New** or edit an existing policy.
- b. Enter the following:

Name	policy46-1
Incoming Interface	To_vlan20
Outgoing Interface	To_vlan30
Source	all
Destination	test-vip46-1
Schedule	always
Service	ALL
Action	ACCEPT
NAT	NAT46
IP Pool Configuration	test-ippool6-1

c. Configure the other settings as needed.

Edit Policy

ID: 2
 Name: policy46-1
 ZTNA: ☐
 Incoming Interface: To_vlan20 (port24)
 Outgoing Interface: To_vlan30 (port17)
 Source: all
 Negate Source: ☐
 Destination: test-vip46-1
 Negate Destination: ☐
 Schedule: always
 Service: ALL
 Action: ☒ ACCEPT ☐ DENY ☐ IPsec
 Inspection Mode: **Flow-based** Proxy-based

Firewall / Network Options
 NAT: ☒ NAT NAT46 NAT64
 IP Pool Configuration: test-ippool6-1
 Preserve Source Port: ☐
 Protocol Options: **PROT** default

Disclaimer Options
 Display Disclaimer: ☐

Statistics (since last reset)

ID	2
Last used	7 hour(s) ago
First used	10 day(s) ago
Active sessions	0
Hit count	199
Total bytes	39.62 MB
Current bandwidth	0 B/s

[Clear Counters](#)

Last 7 Days Bytes IPv4 + IPv6

Bar chart showing traffic volume in MB for the last 7 days (Jun 07 to Jun 14). The chart shows a significant spike on Jun 08 and Jun 11, reaching approximately 15 MB. The legend indicates traffic is categorized by nTurbo, SPU, and Software.

Additional Information
[API Preview](#)
[Edit in CLI](#)
[Documentation](#)
[Online Help](#)

OK **Cancel**

d. Click OK.

To create a NAT46 policy in the CLI:

1. Configure the VIP:

```
config firewall vip
  edit "test-vip46-1"
    set extip 10.1.100.150
    set nat44 disable
    set nat46 enable
    set extintf "port24"
    set arp-reply enable
    set ipv6-mappedip 2000:172:16:200::156
  next
end
```

2. Configure the IPv6 pool:

```
config firewall ippool6
  edit "test-ippool6-1"
    set startip 2000:172:16:101::1
    set endip 2000:172:16:101::1
    set nat46 enable
    set add-nat46-route enable
  next
end
```

3. Configure the firewall policy:

```
config firewall policy
  edit 2
    set name "policy46-1"
    set srcintf "port24"
```

```

        set dstintf "port17"
        set action accept
        set nat46 enable
        set srcaddr "all"
        set dstaddr "test-vip46-1"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set auto-asic-offload disable
        set ippool enable
        set poolname6 "test-ippool6-1"
    next
end

```

To verify the traffic and session tables:

1. Verify the traffic by the sniffer packets:

```

(root) # diagnose sniffer packet any 'icmp or icmp6' 4
interfaces=[any]
filters=[icmp or icmp6]
2.593302 port24 in 10.1.100.41 -> 10.1.100.150: icmp: echo request
2.593344 naf.root out 10.1.100.41 -> 10.1.100.150: icmp: echo request
2.593347 naf.root in 2000:172:16:101::1 -> 2000:172:16:200::156: icmp6: echo request seq
1
2.593383 port17 out 2000:172:16:101::1 -> 2000:172:16:200::156: icmp6: echo request seq
1
2.593772 port17 in 2000:172:16:200::156 -> 2000:172:16:101::1: icmp6: echo reply seq 1
2.593788 naf.root out 2000:172:16:200::156 -> 2000:172:16:101::1: icmp6: echo reply seq
1
2.593790 naf.root in 10.1.100.150 -> 10.1.100.41: icmp: echo reply
2.593804 port24 out 10.1.100.150 -> 10.1.100.41: icmp: echo reply
11 packets received by filter
0 packets dropped by kernel

```

2. Verify the session tables for IPv4 and IPv6:

```

(root) # diagnose sys session list
session info: proto=1 proto_state=00 duration=2 expire=59 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty f00 netflow-origin netflow-reply
statistic(bytes/packets/allow_err): org=252/3/1 reply=252/3/1 tuples=2
tx speed(Bps/kbps): 106/0 rx speed(Bps/kbps): 106/0
orgin->sink: org pre->post, reply pre->post dev=24->53/53->24
gwy=10.1.100.150/10.1.100.41
hook=pre dir=org act=noop 10.1.100.41:29388->10.1.100.150:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.150:29388->10.1.100.41:0(0.0.0.0:0)
peer=2000:172:16:101::1:29388->2000:172:16:200::156:128 naf=1
hook=pre dir=org act=noop 2000:172:16:101::1:29388->2000:172:16:200::156:128( :::0)
hook=post dir=reply act=noop 2000:172:16:200::156:29388->2000:172:16:101::1:129( :::0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0

```

```

serial=00012b77 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040001 no_offload
no_ofld_reason: disabled-by-policy non-npu-intf
total session 1

(root) # diagnose sys session6 list
session6 info: proto=58 proto_state=00 duration=5 expire=56 timeout=0 flags=00000000
sockport=0 socktype=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty
statistic(bytes/packets/allow_err): org=312/3/0 reply=312/3/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=53->17/17->53
hook=pre dir=org act=noop 2000:172:16:101::1:29388->2000:172:16:200::156:128(:::0)
hook=post dir=reply act=noop 2000:172:16:200::156:29388->2000:172:16:101::1:129(:::0)
peer=10.1.100.150:29388->10.1.100.41:0 naf=2
hook=pre dir=org act=noop 10.1.100.41:29388->10.1.100.150:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.150:29388->10.1.100.41:0(0.0.0.0:0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00001bbc tos=ff/ff ips_view=1024 app_list=0 app=0 url_cat=0
rpd_b_link_id = 00000000 ngfwid=n/a
npu_state=0x000001 no_offload
no_ofld_reason: disabled-by-policy
total session 1

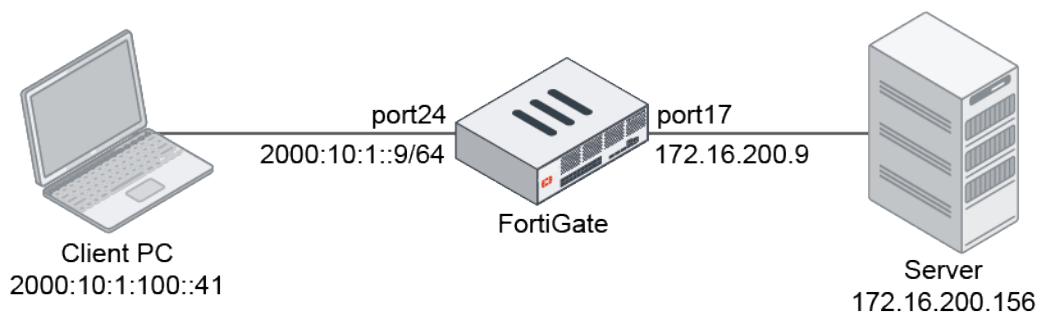
```

The IPv4 session is between the incoming physical interface port24 and naf.root. The IPv6 session is between the naf.root and the outgoing physical interface port17.

NAT64 policy

In this example, a client PC is using IPv6 and an IPv6 VIP to access a server that is using IPv4. The FortiGate uses NAT64 to translate the request from IPv6 to IPv4 using the virtual interface naf.root. An `ippool6` is applied so that the request is SNATed to the `ippool` address (172.16.101.2 - 172.16.101.3).

An embedded VIP64 object is used in this configuration so a specific IPv4 mapped IP does not need to be set. The lower 32 bits of the external IPv6 address are used to map to the IPv4 address. Only an IPv6 prefix is defined. In this example, the IPv6 prefix is 2001:10:1:100::, so the IPv6 address 2001:10:1:100::ac10:c89c will be translated to 172.16.200.156.



To create a NAT64 policy in the GUI:

1. Configure the VIP:
 - a. Go to *Policy & Objects > Virtual IPs* and click *Create New > VIP*.
 - b. Enter the following:

VIP type	IPv6
Name	test-vip64-1
External IP address/range	2000:10:1:100::150
Map to IPv4 address/range	Specify: 172.16.200.156

- c. Click **OK**.
2. Configure the VIP with the embedded IPv4 address enabled:
 - a. Go to *Policy & Objects > Virtual IPs* and click *Create New > VIP*.
 - b. Enter the following:

VIP type	IPv6
Name	test-vip64-2
External IP address/range	2001:10:1:100::-2001:10:1:100::ffff:ffff
Map to IPv4 address/range	Use Embedded

c. Click OK.

3. Configure the IP pool:

- a. Go to *Policy & Objects > IP Pools* and click *Create New*.
- b. Enter the following:

IP Pool Type	IPv4 Pool
Name	test-ippool4-1
Type	Overload
External IP address/range	172.16.101.2-172.16.101.3
NAT64	Enable

c. Click OK.

4. Configure the firewall policy:

- a. Go to *Policy & Objects > IP Pools* and click *Create New* or edit an existing policy.
- b. Enter the following:

Name	policy64-1
Incoming Interface	To_vlan20
Outgoing Interface	To_vlan30
Source	all
Destination	test-vip64-1 test-vip64-2

Schedule	always
Service	ALL
Action	ACCEPT
NAT	NAT64
IP Pool Configuration	test-ippool4-1

- c. Configure the other settings as needed.

- d. Click OK.

To create a NAT64 policy in the CLI:

1. Configure the VIP:

```
config firewall vip6
  edit "test-vip64-1"
    set extip 2000:10:1:100::150
    set nat66 disable
    set nat64 enable
    set ipv4-mappedip 172.16.200.156
  next
end
```

2. Configure the VIP with the embedded IPv4 address enabled:

```
config firewall vip6
  edit "test-vip64-2"
    set extip 2001:10:1:100::-2001:10:1:100::ffff:ffff
    set nat66 disable
    set nat64 enable
    set embedded-ipv4-address enable
```

```
    next
end
```

3. Configure the IP pool:

```
config firewall ippool
    edit "test-ippool4-1"
        set startip 172.16.101.2
        set endip 172.16.101.3
        set nat64 enable
        set add-nat64-route enable
    next
end
```

4. Configure the firewall policy:

```
config firewall policy
    edit 1
        set name "policy64-1"
        set srcintf "port24"
        set dstintf "port17"
        set action accept
        set nat64 enable
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "test-vip64-1" "test-vip64-2"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set auto-asic-offload disable
        set ippool enable
        set poolname "test-ippool4-1"
    next
end
```

To verify the traffic and session tables:

1. Verify the VIP64 traffic by the sniffer packets:

```
(root) # diagnose sniffer packet any 'icmp or icmp6' 4
interfaces=[any]
filters=[icmp or icmp6]
20.578417 port24 in 2000:10:1:100::41 -> 2000:10:1:100::150: icmp6: echo request seq 1
20.578495 naf.root out 2000:10:1:100::41 -> 2000:10:1:100::150: icmp6: echo request seq 1
20.578497 naf.root in 172.16.101.2 -> 172.16.200.156: icmp: echo request
20.578854 port17 out 172.16.101.2 -> 172.16.200.156: icmp: echo request
20.579083 port17 in 172.16.200.156 -> 172.16.101.2: icmp: echo reply
20.579093 naf.root out 172.16.200.156 -> 172.16.101.2: icmp: echo reply
20.579095 naf.root in 2000:10:1:100::150 -> 2000:10:1:100::41: icmp6: echo reply seq 1
20.579377 port24 out 2000:10:1:100::150 -> 2000:10:1:100::41: icmp6: echo reply seq 1
11 packets received by filter
0 packets dropped by kernel
```

2. Verify the session tables for IPv6 and IPv4:

```
(root) # diagnose sys session6 list
session6 info: proto=58 proto_state=00 duration=5 expire=56 timeout=0 flags=00000000
sockport=0 socktype=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty
statistic(bytes/packets/allow_err): org=312/3/0 reply=312/3/0 tuples=2
tx speed(Bps/kbps): 55/0 rx speed(Bps/kbps): 55/0
orgin->sink: org pre->post, reply pre->post dev=24->53/53->24
hook=pre dir=org act=noop 2000:10:1:100::41:29949->2000:10:1:100::150:128(:::0)
hook=post dir=reply act=noop 2000:10:1:100::150:29949->2000:10:1:100::41:129(:::0)
peer=172.16.101.2:45392->172.16.200.156:8 naf=1
hook=pre dir=org act=noop 172.16.101.2:45392->172.16.200.156:8(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.200.156:45392->172.16.101.2:0(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000021ec tos=ff/ff ips_view=1024 app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000 ngfwid=n/a
npu_state=0x040001 no_offload
no_ofld_reason: disabled-by-policy non-npu-intf
total session 1

(root) # diagnose sys session list
session info: proto=1 proto_state=00 duration=7 expire=54 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=252/3/1 reply=252/3/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=53->17/17->53
gwy=172.16.200.156/172.16.101.2
hook=pre dir=org act=noop 172.16.101.2:45392->172.16.200.156:8(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.200.156:45392->172.16.101.2:0(0.0.0.0:0)
peer=2000:10:1:100::150:29949->2000:10:1:100::41:129 naf=2
hook=pre dir=org act=noop 2000:10:1:100::41:29949->2000:10:1:100::150:128(:::0)
hook=post dir=reply act=noop 2000:10:1:100::150:29949->2000:10:1:100::41:129(:::0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0001347f tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000001 no_offload
no_ofld_reason: disabled-by-policy
total session 1
```

The IPv6 session is between the incoming physical interface port24 and naf.root. The IPv4 session is between the naf.root and the outgoing physical interface port17.

3. Verify the embedded VIP64 traffic by the sniffer packets:

```
(root) # diagnose sniffer packet any 'icmp or icmp6' 4
interfaces=[any]
filters=[icmp or icmp6]
```



```

7.696010 port24 in 2000:10:1:100::41 -> 2001:10:1:100::ac10:c89c: icmp6: echo request
seq 1
7.696057 naf.root out 2000:10:1:100::41 -> 2001:10:1:100::ac10:c89c: icmp6: echo request
seq 1
7.696060 naf.root in 172.16.101.2 -> 172.16.200.156: icmp: echo request
7.696544 port17 out 172.16.101.2 -> 172.16.200.156: icmp: echo request
7.696821 port17 in 172.16.200.156 -> 172.16.101.2: icmp: echo reply
7.696839 naf.root out 172.16.200.156 -> 172.16.101.2: icmp: echo reply
7.696841 naf.root in 2001:10:1:100::ac10:c89c -> 2000:10:1:100::41: icmp6: echo reply
seq 1
7.697167 port24 out 2001:10:1:100::ac10:c89c -> 2000:10:1:100::41: icmp6: echo reply seq
1
11 packets received by filter
0 packets dropped by kernel

```

Cisco Security Group Tag as policy matching criteria - 7.0.1

The FortiGate can read the Cisco Security Group Tag (SGT) in Ethernet frames, and use them as matching criteria in firewall policies. A policy can match based on the presence of a SGT, or the detection of a specific ID or IDs.

When a packet with a SGT passes through and a session is established, the `ext_header_type=0xc5:0xc5` flag is included in the session table.

This feature is available in flow mode policies for virtual wire pair policies or policies in transparent mode VDOMs.

To configure a firewall policy to detect SGTs in Ethernet frames:

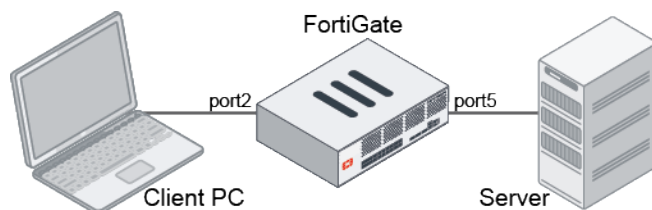
```

config firewall policy
  edit 1
    set sgt-check {enable | disable}
    set sgt <ID numbers>
  next
end

```

Examples

In these examples, port2 and port5 are in a virtual wire pair. Firewall policies are created that pass traffic with SGTs with a specific ID number, any ID number, or either of two specific ID numbers.



To configure the virtual wire pair:

```

config system virtual-wire-pair
  edit "test-vwp-1"
    set member "port5" "port2"
    set wildcard-vlan enable
  end

```

```
    next
end
```

To configure a firewall policy to match frames that have an SGT with ID 20 and allow them through:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port5"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set sgt-check enable
        set sgt 20
    next
end
```

To configure a firewall policy to match frames that have an SGT with any ID:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port5"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set sgt-check enable
    next
end
```

To configure a firewall policy to match frames that have the SGT with IDs 20 or 21:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port5"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set sgt-check enable
        set sgt 20 21
    next
end
```

To check the session list:

```
# diagnose sys session list
```

```
session info: proto=6 proto_state=01 duration=10 expire=3593 timeout=3600 flags=00000000
```

```
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty br dst-vis f00
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 10/0 rx speed(Bps/kbps): 5/0
origin->sink: org pre->post, reply pre->post dev=13->10/10->13 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.1.11:36970->10.1.2.11:80(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.2.11:80->10.1.1.11:36970(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
dst_mac=00:b0:e1:22:cf:e4
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=1
serial=0000183c tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x000001 no_offload
no_ofld_reason: disabled-by-policy
ext_header_type=0xc5:0xc5
total session 1
```

Objects

This section includes information about object related new features:

- [Record central NAT and DNAT hit count on page 397](#)
- [MAC address wildcard in firewall address on page 398](#)

Record central NAT and DNAT hit count

Daily hit counts for central NAT and DNAT can be displayed in the CLI for IPv4 and IPv6.

To view the central SNAT counter:

```
# diagnose firewall iprope show 10000d <id>
# diagnose firewall iprope6 show 10000d <id>
```

To view the DNAT counter:

```
# diagnose firewall iprope show 100000 <id>
# diagnose firewall iprope6 show 100000 <id>
```

To clear the counters:

```
# diagnose firewall iprope clear 10000d <id>
# diagnose firewall iprope clear 100000 <id>
# diagnose firewall iprope6 clear 10000d <id>
```

```
# diagnose firewall iprope6 clear 100000 <id>
```

Sample output

```
# diagnose firewall iprope show 10000d 1
idx=1 hit count:6 (2 4 0 0 0 0 0 0)
first:2021-01-23 12:10:37 last:2021-01-24 12:12:24
```

For entry ID 1, there are a total of six counts since the last time the counter was cleared. There are six times where the traffic matches the central SNAT entry. The hit count of the present day and last seven days is displayed in parentheses.

```
# diagnose firewall iprope show 100000 1
idx=1 hit count:3 (1 2 0 0 0 0 0 0)
first:2021-01-23 12:10:37 last:2021-01-24 12:12:23
```

For entry ID 1, there are a total of three counts since the last time the counter was cleared. There are three times where the traffic matches the DNAT (VIP) entry. The hit count of the present day and last seven days is displayed in parentheses.



The hit counters can be used for NP offloaded traffic.

MAC address wildcard in firewall address

Wildcard MAC addresses can be used in firewall address so users can easily use pattern matching, like vendor prefix, to define a group of addresses. The MAC address range is now defined by specifying a <start>-<end> in a single field separated by a space, instead of defining a `start-mac` and `end-mac`. Multiple addresses can be defined in a single line.

To configure multiple wildcard MAC addresses in the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Enter a name.
3. For *Type*, select *Device (MAC Address)*.

4. In the *MAC address* field, enter the wildcard address. Click the + to add more addresses.

New Address

Category: **Address** | IPv6 Address | Multicast Address | IPv6 Multicast Address | Proxy Address

Name: Demo-wildcard-mac-1

Color: Change

Type: Device (MAC Address) ▼

MAC address: 00:0c:29:b5:**:8d ✕
00:0a:29:b5:c2:** ✕
04:d5:90:04:?:?:? ✕

Interface: ☐ any ▼

Comments: Write a comment... 0/255

OK Cancel

FortiGate
FGDocs

Additional Information
API Preview

Dynamic Address

Guides

- Configuring an AWS Dynamic Address
- Configuring an Azure Dynamic Address
- Configuring a Google Cloud Platform Dynamic Address
- Configuring an Oracle Cloud Infrastructure Dynamic Address
- Configuring an OpenStack Dynamic Address

Documentation

- Online Help
- Video Tutorials

5. Click OK.

To configure multiple wildcard MAC addresses in the CLI:

```
config firewall address
  edit "Demo-wildcard-mac-1"
    set type mac
    set macaddr "00:0c:29:b5:**:8d" "00:0a:29:b5:c2:**" "04:d5:90:04:?:?:?"
  next
end
```

Security profiles

This section includes information about security profile related new features:

- [Antivirus on page 400](#)
- [Application control on page 415](#)
- [Web filter on page 416](#)
- [IPS on page 423](#)
- [SSL/SSH inspection on page 426](#)
- [Others on page 430](#)

Antivirus

This section includes information about antivirus related new features:

- [Stream-based antivirus scan in proxy mode for FTP, SFTP, and SCP on page 400](#)
- [Configure threat feed and outbreak prevention without AV engine scan on page 402](#)
- [AI-based malware detection on page 404](#)
- [Malware threat feed from EMS on page 406](#)
- [FortiAI inline blocking and integration with an AV profile 7.0.1 on page 408](#)

Stream-based antivirus scan in proxy mode for FTP, SFTP, and SCP

Stream-based antivirus scanning in proxy mode is supported for FTP, SFTP, and SCP protocols.

- Stream-based antivirus scanning optimizes memory utilization for large archive files by decompressing the files on the fly and scanning the files as they are extracted.
- File types can be determined after scanning a few KB, without buffering the entire file.
- Viruses can be detected even if they are hiding in the middle or end of a large archive.
- When scanning smaller files, traffic throughput is improved by scanning the files directly on the proxy based WAD daemon, without invoking scanunit.

Stream-based scanning is the default scan mode when an antivirus is in proxy mode. To disable steam-based scanning, the scan mode can be set to legacy mode, and archive will only be scanned after the entire file has been received.

To configure stream-based scan:

```
config antivirus profile
  edit <string>
    ...
    set feature-set proxy
    set scan-mode {default* | legacy}
    ...
  next
end
```

TCP windows

Some file transfer applications can negotiate large TCP windows. For example, WinSCP can negotiate an initial TCP window size of about 2GB.

The TCP window options can be used to prevent overly large initial TCP window sizes, helping avoid channel flow control issues. It allows stream-based scan's flow control to limit peers from sending data that exceeds a policy's configured oversize limit.

To configure TCP window size options:

```
config firewall profile-protocol-options
  edit <string>
    config {ftp | ssh}
      ...
      set stream-based-uncompressed-limit <integer>
      set tcp-window-type {system | static | dynamic}
      set tcp-window-size <integer>
      set tcp-window-minimum <integer>
      set tcp-window-maximum <integer>
      ...
    end
  next
end
```

{ftp ssh}	<ul style="list-style-type: none"> ftp: Configure FTP protocol options. ssh: Configure SFTP and SCP protocol options.
stream-based-uncompressed-limit <integer>	<p>The maximum stream-based uncompressed data size that will be scanned, in MB (default = 0 (unlimited)).</p> <p>Stream-based uncompressed used only under certain conditions.).</p>
tcp-window-type {system static dynamic}	<p>The TCP window type to use for this protocol.</p> <ul style="list-style-type: none"> system: Use the system default TCP window size for this protocol (default). static: Manually specify the TCP window size. dynamic: Vary the TCP window size based on available memory within the limits configured in tcp-window-minimum and tcp-window-maximum.
tcp-window-size <integer>	<p>The TCP static window size (65536 - 33554432, default = 262144).</p> <p>This option is only available when tcp-window-type is static.</p>
tcp-window-minimum <integer>	<p>The minimum TCP dynamic window size (65536 - 1048576, default = 131072).</p> <p>This option is only available when tcp-window-type is dynamic.</p>
tcp-window-maximum <integer>	<p>The maximum TCP dynamic window size (1048576 - 33554432, default = 8388608).</p> <p>This option is only available when tcp-window-type is dynamic.</p>

Configure threat feed and outbreak prevention without AV engine scan

In the CLI, users can enable malware threat feeds and outbreak prevention without performing an AV scan. In GUI and CLI, users can choose to use all malware thread feeds, or specify the ones that they want to use. Replacement messages have been updated for external block lists.

```
config antivirus profile
  edit <name>
    config http
      set av-scan {disable | block | monitor}
      set outbreak-prevention {disable | block | monitor}
      set external-blocklist {disable | block | monitor}
      set quarantine {enable | disable}
    end
    ...
    set outbreak-prevention-archive-scan {enable | disable}
    set external-blocklist-archive-scan {enable | disable}
    set external-blocklist-enable-all {enable | disable}
    set external-blocklist <source>
  next
end
```

To configure malware threat feeds and outbreak prevention without performing an AV scan in the CLI:

```
config antivirus profile
  edit "Demo"
    set feature-set proxy
    set mobile-malware-db enable
    config http
      set av-scan disable
      set outbreak-prevention block
      set external-blocklist block
      set quarantine enable
      set emulator enable
      set content-disarm disable
    end
    config ftp
      set av-scan disable
      set outbreak-prevention block
      set external-blocklist block
      set quarantine enable
      set emulator enable
    end
    config imap
      set av-scan monitor
      set outbreak-prevention block
      set external-blocklist block
      set quarantine enable
      set emulator enable
      set executables default
      set content-disarm disable
    end
    config pop3
      set av-scan monitor
      set outbreak-prevention block
      set external-blocklist block
```



```
        set quarantine enable
        set emulator enable
        set executables default
        set content-disarm disable
    end
    config smtp
        set av-scan monitor
        set outbreak-prevention block
        set external-blocklist block
        set quarantine enable
        set emulator enable
        set executables default
        set content-disarm disable
    end
    config mapi
        set av-scan monitor
        set outbreak-prevention block
        set external-blocklist block
        set quarantine enable
        set emulator enable
        set executables default
    end
    config nntp
        set av-scan disable
        set outbreak-prevention disable
        set external-blocklist disable
        set quarantine disable
        set emulator enable
    end
    config cifs
        set av-scan monitor
        set outbreak-prevention block
        set external-blocklist block
        set quarantine enable
        set emulator enable
    end
    config ssh
        set av-scan disable
        set outbreak-prevention disable
        set external-blocklist disable
        set quarantine disable
        set emulator enable
    end
    set outbreak-prevention-archive-scan enable
    set external-blocklist-archive-scan enable
    set external-blocklist-enable-all disable
    set external-blocklist "malhash1"
    set av-virus-log enable
    set av-block-log enable
    set extended-log disable
    set scan-mode default
next
end
```

In this example, configuring the quarantine setting is done in each protocol (`set quarantine`). The malware threat feed is also specified (`set external-blocklist-enable-all disable`) to the threat connector, `malhash1` (`set external-blocklist "malhash1"`).

To specify a malware threat feed and quarantine in the GUI:

1. Go to *Security Profiles > AntiVirus* and click *Create New*.
2. Enable the protocols you want to inspect.
3. Enable *Use external malware block list* and click *Specify*.
4. Click the + in the field and select a threat feed.
5. Optionally, enable *Quarantine*.

The screenshot shows the 'New AntiVirus Profile' configuration window. The 'Name' field is set to 'Demo'. The 'AntiVirus scan' is set to 'Block' and 'Monitor'. The 'Feature set' is set to 'Flow-based' and 'Proxy-based'. The 'Inspected Protocols' section shows various protocols with checkboxes: HTTP, SMTP, POP3, IMAP, FTP, CIFS, MAPI, and SSH. The 'APT Protection Options' section includes 'Content Disarm and Reconstruction', 'Treat Windows executables in email attachments as viruses', 'Include mobile malware protection', and 'Quarantine'. The 'Virus Outbreak Prevention' section includes 'Use FortiGuard outbreak prevention database', 'Use external malware block list' (which is checked and has a 'Specify' button), and 'Use EMS threat feed'. A list of threat feeds is shown below, with 'malhash1' selected. The 'OK' and 'Cancel' buttons are at the bottom.

6. Configure the other settings as needed.
7. Click *OK*.

AI-based malware detection

The AV Engine AI malware detection model integrates into regular AV scanning to help detect potentially malicious Windows Portable Executables (PEs) in order to mitigate zero-day attacks. Previously, this type of detection was handled by heuristics that analyzed file behavior. With AV Engine AI, the module is trained by FortiGuard AV against many malware samples to identify file features that make up the malware. The AV Engine AI package can be downloaded by FortiOS via FortiGuard on devices with an active AV subscription.

When upgrading from 6.4 to 7.0, the previous heuristic settings are not kept. In 7.0, the `machine-learning-detection` setting is enabled by default at a per-VDOM level:

```
config antivirus settings
    set machine-learning-detection {enable| monitor | disable}
end
```

Files detected by the AV Engine AI are identified with the W32/AI.Pallas.Suspicious virus signature.

To verify the AV Engine AI contract information:

```
# diagnose autoupdate versions

AV Engine
-----
Version: 6.00256
Contract Expiry Date: Wed Jan  1 2025
Last Updated using manual update on Tue Mar  9 15:29:31 2021
Last Update Attempt: Thu Mar 11 13:50:32 2021
Result: No Updates

Virus Definitions
-----
Version: 84.00635
Contract Expiry Date: Wed Jan  1 2025
Last Updated using scheduled update on Thu Mar 11 13:50:32 2021
Last Update Attempt: Thu Mar 11 13:50:32 2021
Result: Updates Installed

...

AI/Machine Learning Malware Detection Model
-----
Version: 2.00021
Contract Expiry Date: Wed Jan  1 2025
Last Updated using manual update on Wed Mar 10 10:21:25 2021
Last Update Attempt: Thu Mar 11 13:50:32 2021
Result: No Updates

...

# get system status
...
Firmware Signature: certified
Virus-DB: 84.00632(2021-03-11 10:16)
Extended DB: 84.00632(2021-03-11 10:16)
AV AI/ML Model: 2.00021(2021-03-08 13:56)
...
```

Sample log

```
date=2021-03-10 time=15:41:02 eventtime=1615419662027720720 tz="-0800" logid="0211008192"
type="utm" subtype="virus" eventtype="infected" level="warning" vd="vdom1" policyid=1
msg="File is infected." action="blocked" service="HTTP" sessionid=18050 srcip=10.1.100.221
dstip=172.16.200.224 srcport=42092 dstport=80 srcintf="wan2" srcintfrole="wan"
dstintf="wan1" dstintfrole="wan" proto=6 direction="incoming" filename="1132999808"
quarskip="Quarantine-disabled" virus="W32/AI.Pallas.Suspicious" dtype="Virus"
ref="http://www.fortinet.com/ve?vn=W32%2FAI.Pallas.Suspicious" virusid=8187637
url="http://172.16.200.224/avengine_ai/clean/1132999808" profile="av" agent="Wget/1.20.3"
analyticscksum="01ca5e5d9ealbb615bd0d8ae8e62f210e50b6339db25013ec367b34f5f2ff043"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"
```

Malware threat feed from EMS

A FortiGate can pull malware threat feeds from FortiClient EMS, which in turn receives malware hashes detected by FortiClients. The malware hash can be used in an antivirus profile when AV scanning is enabled with block or monitor actions. This feature is supported in proxy mode in 7.0.0, and in proxy and flow mode in 7.0.1.



If an external malware blocklist and the FortiGuard outbreak prevention database are also enabled in the antivirus profile, the checking order is: AV local database, EMS threat feed, external malware blocklist, FortiGuard outbreak prevention database. If the EMS threat feed and external malware blocklist contain the same hash value, then the EMS infection will be reported if both of them are blocked.

To configure an EMS threat feed in an antivirus profile in the GUI:

1. Enable the EMS threat feed:
 - a. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiClient EMS* card.
 - b. Enable *EMS Threat Feed*.
 - c. Configure the other settings as needed.

- d. Click OK.
2. Create the antivirus profile:
 - a. Go to *Security Profiles > AntiVirus* and click *Create New*.
 - b. In the *Virus Outbreak Prevention* section, enable *Use EMS threat feed*.

c. Configure the other settings as needed.

d. Click OK.

To configure an EMS threat feed in an antivirus profile in the CLI:

1. Enable the EMS threat feed:

```
config endpoint-control fctems
  edit "WIN10-EMS"
    set fortinetone-cloud-authentication disable
    set server "192.168.20.10"
    set https-port 443
    set source-ip 0.0.0.0
    set pull-sysinfo enable
    set pull-vulnerabilities enable
    set pull-avatars enable
    set pull-tags enable
    set pull-malware-hash enable
    unset capabilities
    set call-timeout 30
    set websocket-override disable
  next
end
```

2. Create the antivirus profile:

```
config antivirus profile
  edit "av"
    config http
      set av-scan block
    end
    config ftp
      set av-scan block
    end
  end
```

```

end
config imap
    set av-scan block
end
config pop3
    set av-scan block
end
config smtp
    set av-scan block
end
config cifs
    set av-scan block
end
set external-blocklist-enable-all enable
set ems-threat-feed enable
next
end

```

Sample log

```

# execute log filter category utm-virus
# execute log display

```

```

1: date=2021-03-19 time=16:06:46 eventtime=1616195207055607417 tz="-0700" logid="0208008217"
type="utm" subtype="virus" eventtype="ems-threat-feed" level="notice" vd="vd1" policyid=1
msg="Detected by EMS threat feed." action="monitored" service="HTTPS" sessionid=1005
srcip=10.1.100.24 dstip=172.16.200.214 srcport=54674 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 direction="incoming"
filename="creditcardSSN.pdf" quarskip="Quarantine-disabled" virus="Email scan" dtype="File
Hash" filehash="22466078c2d52dfd5ebbbd6c4207ddec6ac61aa82f960dc54cfbc83b8eb42ed1"
filehashsrc="test" url="https://172.16.200.214/hash/creditcardSSN.pdf" profile="av"
agent="curl/7.68.0" analyticssubmit="false" crscore=10 craction=2 crlevel="medium"

```

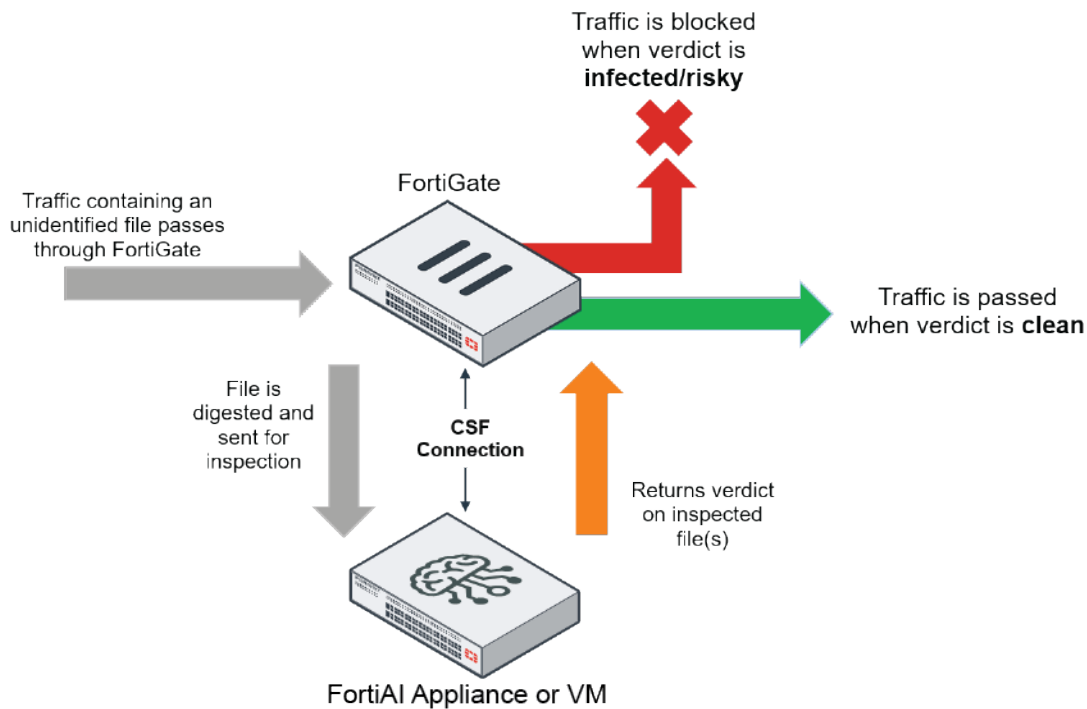
```

2: date=2021-03-19 time=16:06:13 eventtime=1616195173832494609 tz="-0700" logid="0208008216"
type="utm" subtype="virus" eventtype="ems-threat-feed" level="warning" vd="vd1" policyid=1
msg="Blocked by EMS threat feed." action="blocked" service="HTTPS" sessionid=898
srcip=10.1.100.24 dstip=172.16.200.214 srcport=54672 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 direction="incoming"
filename="BouncingButton.pdf" quarskip="Quarantine-disabled" virus="Email scan" dtype="File
Hash" filehash="a601431acd5004c37bf8fd02fccfdacbb54b27c8648d1d41ad14fa3eaf8651d3"
filehashsrc="test" url="https://172.16.200.214/hash/BouncingButton.pdf" profile="av"
agent="curl/7.68.0" analyticssubmit="false" crscore=10 craction=2 crlevel="medium"

```

FortiAI inline blocking and integration with an AV profile - 7.0.1

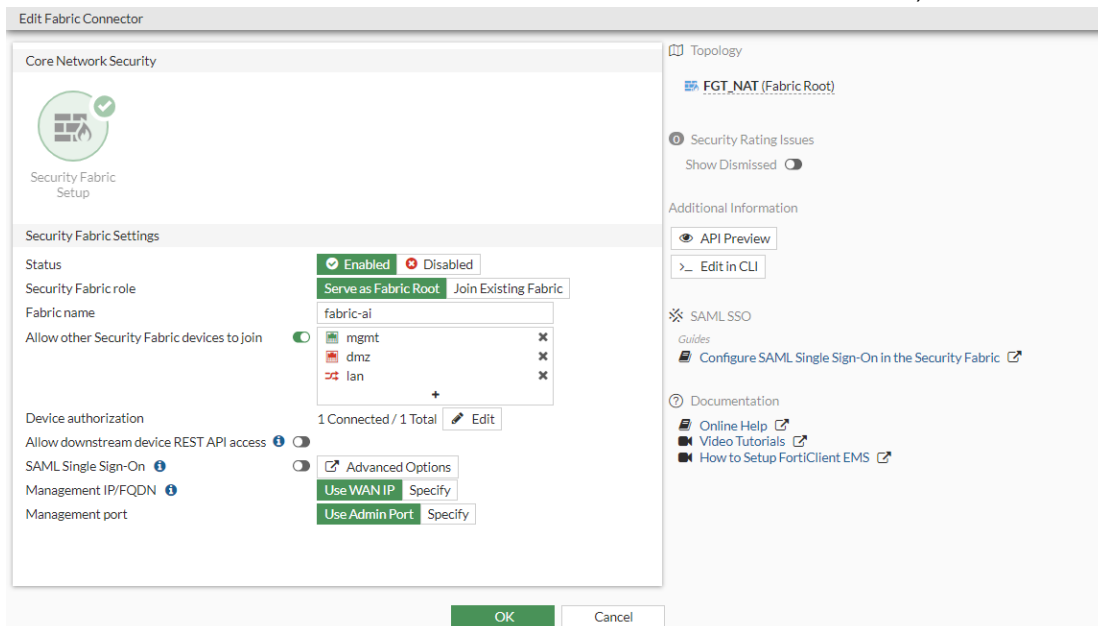
This enhancement allows FortiAI to be used with antivirus profiles in proxy inspection mode (flow mode is currently not supported). FortiAI inspects high-risk files and issues a verdict to the firewall based on how close the file features match those of malware. When enabled, FortiAI can log, block, ignore, or monitor (allow) the file based on the verdict.



A licensed FortiAI appliance with version 1.5.1 or later is required to use this feature.

To configure FortiAI inline inspection with an AV profile:

1. Enable the Security Fabric and configure the interface to allow other Security Fabric devices to join (see [Configuring the root FortiGate and downstream FortiGates](#) in the FortiOS Administration Guide).



2. Install the FortiAI appliance and activate the product with a valid license (see [Registering products](#) in the Asset Management Guide). A license file is provided after the product is registered.

The screenshot displays the FortiCloud Asset Management interface. The left sidebar shows the 'ASSET MANAGEMENT' menu with options: Register Product, Products (selected), Product List, My Assets, More Views, and Online Renew. The main content area is titled 'View Products > FAIVMSTM'. It contains several panels:

- Product Information:**
 - Product Model: FortiAI Subscription
 - Serial Number: FAIVMSTM
 - Registration Date: 2021-04-06
 - Description: FortiAI VM
 - Partner: Internal RnD
 - IP Address: 10.6.30.251
 - License File: [License File Download](#)
- Entitlement:**
 - Firmware & General Updates
 - Enhanced Support
 - Telephone Support
 - FortiGuard Neural Networks engine updates & baseline
- Registration:**
 - [Renew Contract](#)
- License & Key:**

There are no licenses registered to this product.

Key	License Number	Description
Get The License File	N/A	FortiAI Subscription
- Manage Cloud Services:**
 - FortiGate
 - FortiAnalyzer
- Tickets:**

No Tickets Available.
- Location:** (Empty field with a location pin icon)

The footer contains links for Corporate, How to Buy, Products, Services & Support, Legal, Privacy, and Terms of Use. It also shows the Pacific Time zone and copyright information for 2021 Fortinet, Inc.

3. In FortiAI, go to *System > FortiGuard* and verify that the pre-trained models (engines) are up to date. Refer to the [FortiGuard website](#) for the latest FortiAI ANN versions.

FortiGuard Distribution Network

License Information

Entitlement	Status
FortiCare Support	Registered
Firmware & General Updates	Licenses - expires on 2022/04/09 Firmware Upgrade
Virtual Machine	Valid - expires on 2022/04/09 FortiAI VM License
Allocated vCPUs	25% 8/32
Text AI Feature DB	Version 1.068 Update Available
Text AI Group DB	Version 1.068 Update Available
Binary AI Feature DB	Version 1.068 Update Available
Binary AI Group DB	Version 1.068 Update Available
Scenario AI DB	Version 1.068 Update Available
Text AI Learning Feature DB	Version 1.068 Update Available
Binary AI Learning Feature DB	Version 1.068 Update Available
Binary Behavior DB	Version 1.068 Update Available
Text AI Engine	Version 1.026 Up to Date
Binary AI Engine	Version 1.033 Up to Date
Scenario AI Engine	Version 1.001 Up to Date
Text AI Learning Engine	Version 1.004 Up to Date
Binary AI Learning Engine	Version 1.013 Up to Date

FortiGuard Updates

Manual Update Check update Update FortiGuard Neural Networks Engine

Scheduled Updates ☐

Apply

4. Configure and authorize the FortiGate in the FortiAI GUI to join the Security Fabric:
 - a. Go to *Security Fabric > Fabric Connectors* and double-click the connector card.
 - b. Click the toggle to *Enable Security Fabric*.
 - c. Enter the *FortiGate Root IP* address and the *FortiAI IP* address.

Edit Connector Setting

Status

Enable Security Fabric ☐

Fabric Device Settings

FortiGate Root IP TCP Port: (Default: 8013)

FortiAI IP TCP Port: (Default: 443)

Authorization Status Pending Authorization

OK Cancel

- d. Click OK. The FortiAI is now authorized.

Edit Connector Setting

Status

Enable Security Fabric ☒

Fabric Device Settings

FortiGate Root IP TCP Port: (Default: 8013)

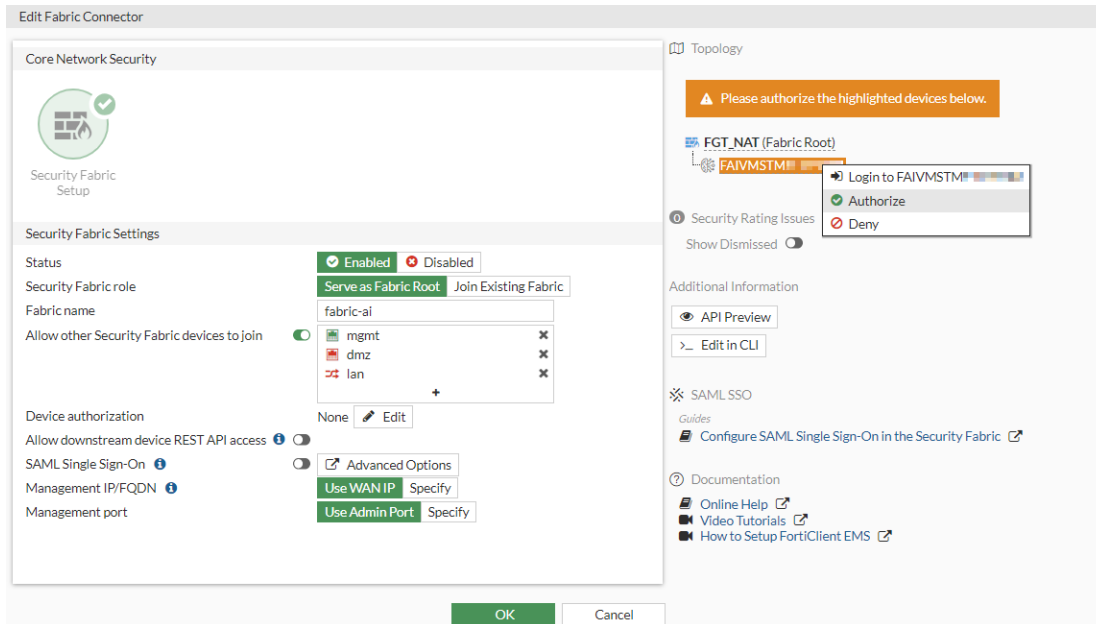
FortiAI IP TCP Port: (Default: 443)

Authorization Status Authorized

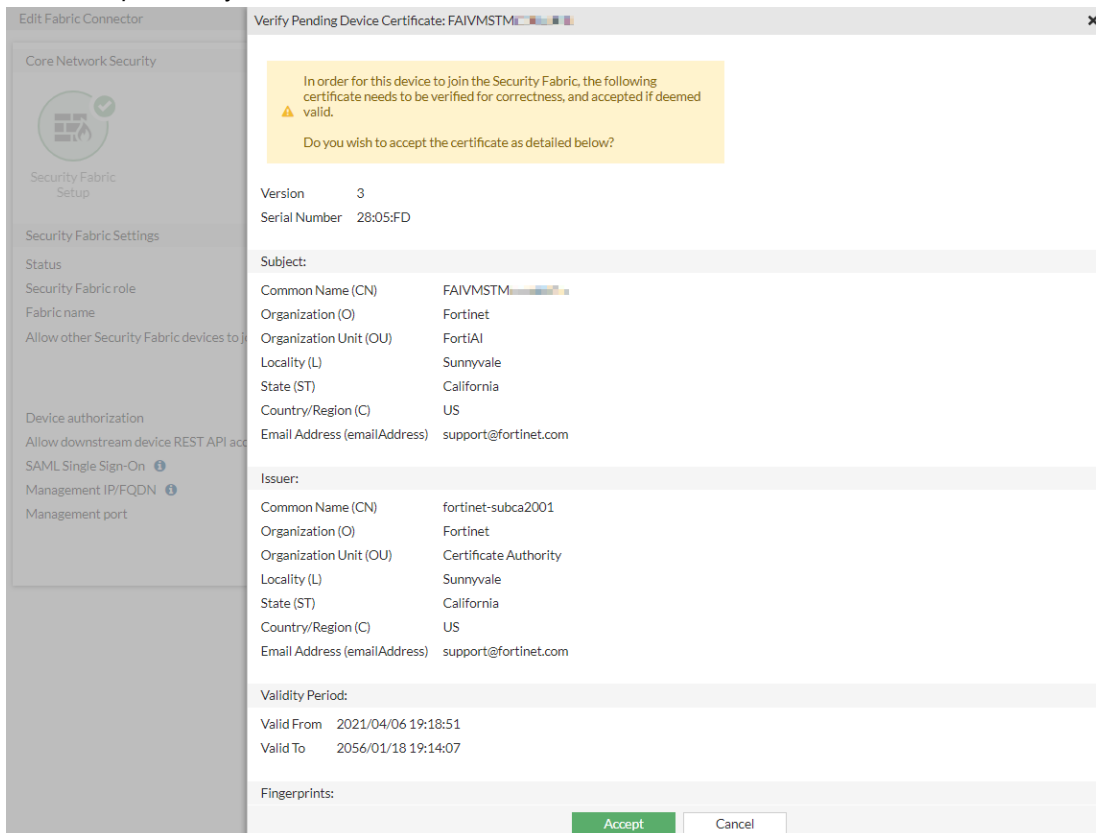
OK Cancel

5. Authorize the FortiAI in FortiOS:

- Go to **Security Fabric > Fabric Connectors** and double-click the **Security Fabric Setup** card.
- In the topology tree, click the highlighted FortiAI serial number and select **Authorize**.



- Click **Accept** to verify the device certificate.



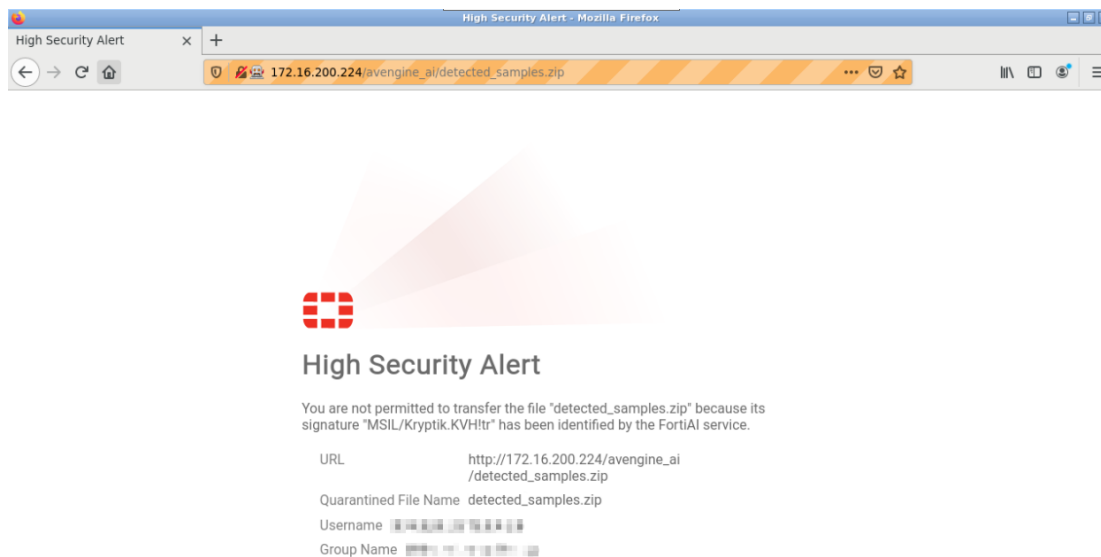
6. In the CLI, enable FortiAI inline inspection:

```
config system fortiai
    set status enable
end
```

7. Configure an AV profile to use inline inspection and block detected infections:

```
config antivirus profile
    edit "av"
        set feature-set proxy
        config http
            set fortiai block
        end
        config ftp
            set fortiai block
        end
        config imap
            set fortiai block
        end
        config pop3
            set fortiai block
        end
        config smtp
            set fortiai block
        end
        config mapi
            set fortiai block
        end
        config nntp
            set fortiai block
        end
        config cifs
            set fortiai block
        end
        config ssh
            set fortiai block
        end
    next
end
```

8. Add the AV profile to a firewall policy. When potential infections are blocked by FortiAI inline inspection, a replacement message appears (*FortiAI Block Page*, see [Replacement messages](#) for more information). An infection blocked over HTTP looks similar to the following:



Sample log

```
date=2021-04-29 time=15:12:07 eventtime=1619734327633022960 tz="-0700" logid="0209008221"
type="utm" subtype="virus" eventtype="fortiai" level="notice" vd="vdom1" policyid=1
msg="Detected by FortiAI." action="monitored" service="HTTP" sessionid=13312
srcip=10.1.100.221 dstip=172.16.200.224 srcport=50792 dstport=80 srcintf="wan2"
srcintfrole="wan" dstintf="wan1" dstintfrole="wan" proto=6 direction="incoming"
filename="detected_samples.zip" quarskip="File-was-not-quarantined"
virus="MSIL/Kryptik.KVH!tr" dtype="FortiAI"
ref="http://www.fortinet.com/ve?vn=MSIL%2FKryptik.KVH%21tr" virusid=0
url="http://172.16.200.224/avengine_ai/detected_samples.zip" profile="av"
agent="curl/7.68.0" analyticssubmit="false" crscore=50 craction=2 crlevel="critical"
```

FortiAI inline inspection with other AV inspection methods

The following inspection logic applies when FortiAI inline inspection is enabled simultaneously with other AV inspection methods. The AV engine inspection and its verdict always takes precedence because of performance. The actual behavior depends on which inspected protocol is used.

HTTP, FTP, SSH, and CIFS protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
 - a. FortiAI inline inspection occurs simultaneously.
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
 - a. FortiAI inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
 - a. FortiAI inline inspection occurs simultaneously.



If any AV inspection method returns an infected verdict, the FortiAI inspection is aborted.

POP3, IMAP, SMTP, NNTP, and MAPI protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
 - a. FortiAI inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
 - a. FortiAI inline inspection occurs simultaneously.



In an AV profile, use `set fortiai-error-action {log-only | block | ignore}` to configure the action to take if FortiAI encounters an error.

Accepted file types

The following file types are sent to FortiAI for inline inspection:

7Z	HTML	RTF
ARJ	JS	TAR
BZIP	LZH	VBA
BZIP2	LZW	VBS
CAB	MS Office documents (XML and non-	WinPE (EXE)
ELF	XML)	XZ
GZIP	PDF	ZIP
	RAR	

Application control

This section includes information about application control related new features:

- [Application signature dissector for DNP3 on page 415](#)

Application signature dissector for DNP3

The DNP3 application signature dissector supports detecting DNP3 traffic that is encapsulated by the RealPort protocol (Net.CX). DNP3 is used in industrial solutions over serial ports, USB ports, printers, and so on. RealPort encapsulation allows transportation of the underlying protocols over TCP/IP. The FortiGate industrial signatures must be enabled to use RealPort.DNP3 signatures:

```
config ips global
    set exclude-signatures none
end
```

IPS engine version 7.0015 and later support RealPort.DNP3 dissectors.

Sample logs

```
119: date=2021-03-09 time=18:56:35 eventtime=1615344995698958507 tz="-0800"
logid="1059028704" type="utm" subtype="app-ctrl" eventtype="signature" level="information"
vd="vd1" appid=49890 srcip=10.1.100.191 dstip=172.16.200.159 srcport=43946 dstport=771
srcintf="port10" srcintfrole="undefined" dstintf="port9" dstintfrole="undefined" proto=6
service="RLDNP3" direction="incoming" policyid=1 sessionid=1204 applist="test" action="pass"
appcat="Industrial" app="RealPort.DNP3" incidentserialno=88083610 msg="Industrial:
RealPort.DNP3," apprisk="elevated"

1: date=2021-03-09 time=18:56:08 eventtime=1615344968811546102 tz="-0800" logid="1059028704"
type="utm" subtype="app-ctrl" eventtype="signature" level="information" vd="vd1" appid=49899
srcip=10.1.100.191 dstip=172.16.200.159 srcport=43946 dstport=771 srcintf="port10"
srcintfrole="undefined" dstintf="port9" dstintfrole="undefined" proto=6 service="RLDNP3"
direction="outgoing" policyid=1 sessionid=1204 applist="test" action="pass"
appcat="Industrial" app="RealPort.DNP3_Confirm" incidentserialno=88083404 msg="Industrial:
RealPort.DNP3_Confirm," clouduser="34 -> 34" filename="Null" apprisk="elevated"
cloudaction="others"
```

Web filter

This section includes information about web filter related new features:

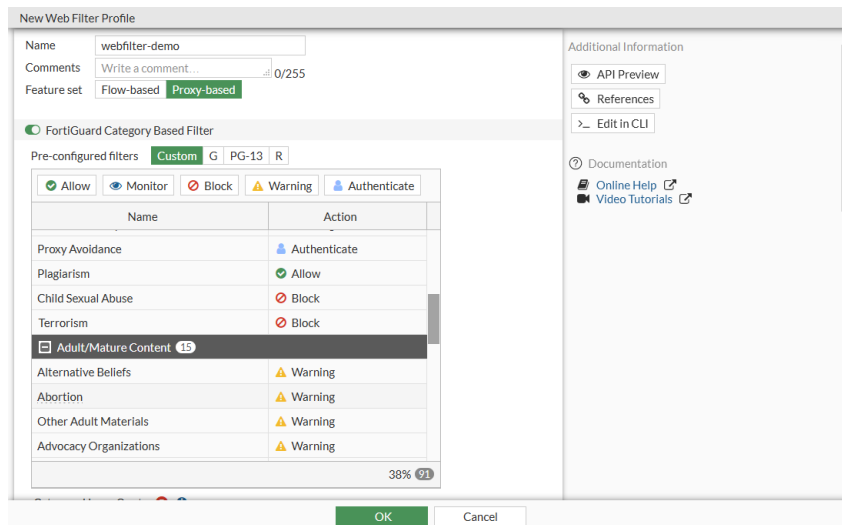
- [FortiGuard web filter categories to block child sexual abuse and terrorism on page 416](#)
- [Enhance web filter antiphishing profile on page 418](#)
- [Add categories for URL shortening, crypto mining, and potentially unwanted programs 7.0.2 on page 421](#)

FortiGuard web filter categories to block child sexual abuse and terrorism

Web filter categories 83 (Child Sexual Abuse, formerly Child Abuse) and 96 (Terrorism) can be used to enforce blocking and logging the Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) lists, respectively.

To create a web filter profile to block the Child Sexual Abuse and Terrorism categories in the GUI:

1. Go to *Security Profiles > Web Filter* and click *Create New*.
2. Enter a name for the new filter, such as *webfilter-demo*.
3. In the category table, in the *Potentially Liable* section, set the *Action* for the *Child Sexual Abuse* and *Terrorism* categories to *Block*.



4. Configure the remaining settings as required.
5. Click OK.

To create a web filter profile to block category 83 (Child Sexual Abuse) and 96 (Terrorism) in the CLI:

```
config webfilter profile
  edit "webfilter-demo"
    config ftgd-wf
      unset options
      config filters
        ...
        edit 83
          set category 83
          set action block
        next
        edit 96
          set category 96
          set action block
        next
        ...
      end
    end
  next
end
```

To test the web filter:

1. Use the web filter profile in a policy.
2. On a device that is connected through the FortiGate and that uses the policy, visit the test URLs for each category:

```
http://wfurltest.fortiguard.com/wftest/83.html
http://wfurltest.fortiguard.com/wftest/96.html
```

3. Log in to the FortiGate, and go to *Log & Report > Web filter* to view the logs for the blocked websites.

Date/Time	Source	Action	URL	Category Description	Sent / Received
2021/01/18 09:04:51	1.1.1.2	blocked	http://wfuritest.fortiguards.com/wftest/96.html	Terrorism	526 B / 0 B
2021/01/18 09:04:38	1.1.1.2	blocked	http://wfuritest.fortiguards.com/wftest/83.html	Child Sexual Abuse	526 B / 0 B
2021/01/18 09:01:39	1.1.1.2	blocked	http://wfuritest.fortiguards.com/wftest/83.html	Child Sexual Abuse	2.77 kB / 77.38 kB

Enhance web filter antiphishing profile

The following enhancements have been made to the antiphishing profile:

- Allow username and password field patterns to be fetched from FortiGuard.
- Add DNS support for domain controller IP fetching.
- Add support to specify a source IP or port for the fetching domain controller.
- Add LDAP server as a credential source (only the OpenLDAP server is supported).
- Block or log valid usernames regardless of password match.
- Add literal custom patterns type for username and password.
- Add support for Active Directory Lightweight Directory Services (AD LDS).



In previous versions of FortiOS, the domain controller for antiphishing is configured under `config credential-store domain-controller`. Starting in 7.0.0, it is configured under `config user domain-controller`.

Configuration examples

To update the antiphish pattern database:

1. Go to *System > FortiGuard* and in the right-side pane, click *Update Licenses & Definitions Now*.
2. Enter the following in the CLI:

```
# diagnose autoupdate versions
...
AntiPhish Pattern DB
-----
Version: 1.00002
Contract Expiry Date: n/a
Last Updated using manual update on Sun Nov 22 10:31:00 2020
Last Update Attempt: Tue Jan 12 16:54:06 2021
Result: No Updates
```

To enable DNS service lookup:

```
config user domain-controller
edit "win2016"
set ad-mode ds
set dns-srv-lookup enable
set hostname "win2016"
set username "replicate"
set password *****
```



```
        set domain-name "SMB2016.LAB"
    next
end
```

To specify the source IP and port for the fetching domain controller:

```
config user domain-controller
    edit "win2016"
        set ad-mode ds
        set hostname "win2016"
        set username "replicate"
        set password *****
        set ip-address 172.18.52.188
        set source-ip-address 172.16.100.1
        set source-port 2000
        set domain-name "SMB2016.LAB"

    next
end
```

To use an LDAP server as a credential store:**1. Configure the LDAP server:**

```
config user ldap
    edit "openldap"
        set server "172.18.60.214"
        set cnid "cn"
        set dn "dc=qafsso,dc=com"
        set type regular
        set username "cn=Manager,dc=qafsso,dc=com"
        set password *****
        set antiphish enable
        set password-attr "userPassword"

    next
end
```

2. Configure the web filter profile:

```
config webfilter profile
    edit "webfilter"
        set feature-set proxy
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set action block
                next
            end
        end
        config antiphish
            set status enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
        end
    end
```

```
        end
        set authentication ldap
        set ldap "openldap"
    end
    set log-all-url enable
next
end
```

To configure username-only credential matching:

```
config webfilter profile
    edit "webfilter"
        set feature-set proxy
        config ftgd-wf
            unset options
            ...
        end
        config antiphish
            set status enable
            set check-username-only enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
            set domain-controller "win2016"
        end
        set log-all-url enable
    next
end
```

To configure different custom pattern types for usernames and passwords:

```
config webfilter profile
    edit "webfilter"
        set feature-set proxy
        config ftgd-wf
            unset options
            ...
        end
        config antiphish
            set status enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
        config custom-patterns
            edit "qwer"
                set type literal
            next
            edit "[0-6]Dat*"
            next
            edit "dauw9"
```

```
        set category password
        set type literal
    next
    edit "[0-5]foo[1-4]"
        set category password
    next
end
set domain-controller "win2016"
end
set log-all-url enable
next
end
```

In this example, the `qwer` and `dauw9` entries use the `literal` type, while `[0-6]Dat*` and `[0-5]foo[1-4]` use the default `regex` type.

To configure Active Directory in LDS mode:

```
config user domain-controller
    edit "win2016adlds"
        set hostname "win2016adlds"
        set username "foo"
        set password *****
        set ip-address 192.168.10.9
        set domain-name "adlds.local"
        set ad-mode lds
        set adlds-dn "CN=adlds1part1,DC=ADLDS,DC=COM"
        set adlds-ip-address 192.168.10.9
        set adlds-port 3890
    next
end
```

Add categories for URL shortening, crypto mining, and potentially unwanted programs - 7.0.2

Three new web filter categories have been added to the FortiOS and FortiGuard servers: URL shortening (97), crypto mining (98), and potentially unwanted program (99). For detailed category descriptions and test pages, refer to the [FortiGuard Labs](#) documentation.

In the following example, a web filter profile is created to monitor URL shortening (97), and to block crypto mining (98) and potentially unwanted program (99).

To create a web filter profile in the GUI:

1. Go to *Security Profiles > Web Filter* and click *Create New*.
2. Enter a name for the filter.
3. In the category table, in the *Potentially Liable* section, set the *Action* for the *Crypto Mining* and *Potentially Unwanted Program* categories to *Block*.

New Web Filter Profile

Feature set: **Flow-based** Proxy-based

FortiGuard Category Based Filter

Allow Monitor Block Warning Authenticate

Name	Action
Explicit Violence	Allow
Extremist Groups	Warning
Proxy Avoidance	Allow
Plagiarism	Allow
Child Sexual Abuse	Allow
Terrorism	Block
Crypto Mining	Block
Potentially Unwanted Program	Block
Adult/Mature Content (15)	Allow
Bandwidth Consuming (6)	Allow

35% 93

☐ Allow users to override blocked categories

Static URL Filter

Block invalid URLs ☐

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☐

OK Cancel

Additional Information

API Preview

Documentation

Online Help

Video Tutorials

In the *General Interest - Business* section, set the *URL Shortening* category to *Monitor*.

New Web Filter Profile

Comments: Write a comment... 0/255

Feature set: **Flow-based** Proxy-based

FortiGuard Category Based Filter

Allow Monitor Block Warning Authenticate

Name	Action
Web Hosting	Allow
Secure Websites	Allow
Web-based Applications	Allow
Charitable Organizations	Allow
Remote Access	Allow
Web Analytics	Allow
Online Meeting	Allow
URL Shortening	Monitor
Unrated (1)	Allow

100% 93

☐ Allow users to override blocked categories

Static URL Filter

Block invalid URLs ☐

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☐

OK Cancel

Additional Information

API Preview

Documentation

Online Help

Video Tutorials

4. Configure the remaining settings as needed.
5. Click OK.

To create a web filter profile in the CLI:

```
config webfilter profile
edit "test"
config ftgd-wf
```

```

unset options
config filters
    ...
    edit 98
        set category 98
        set action block
    next
    edit 99
        set category 99
        set action block
    next
    edit 97
        set category 97
    next
end
end
next
end

```

To test the web filter:

1. Use the web filter profile in a policy.
2. On a device that is connected through the FortiGate and uses the policy, visit the test URLs for each category:

<http://wfurltest.fortiguard.com/wftest/97.html>

<http://wfurltest.fortiguard.com/wftest/98.html>

<http://wfurltest.fortiguard.com/wftest/99.html>

3. Log in to the FortiGate, and go to *Log & Report > Web filter* to view the logs.

Add Filter								
Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received	Category
18 seconds ago		10.1.100.12	passthrough	https://fortiguard.com/wftest/97.html	URL Shortening		764 B / 4.01 kB	97
22 seconds ago		10.1.100.12	blocked	https://fortiguard.com/wftest/99.html	Potentially Unwanted Program		764 B / 4.01 kB	99
25 seconds ago		10.1.100.12	blocked	https://fortiguard.com/wftest/98.html	Crypto Mining		764 B / 4.01 kB	98

IPS

This section includes information about IPS related new features:

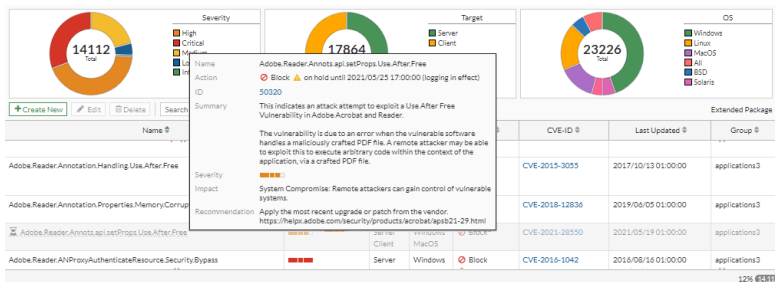
- [Highlight on hold IPS signatures on page 423](#)
- [Extend SCTP filtering capabilities 7.0.1 on page 424](#)

Highlight on hold IPS signatures

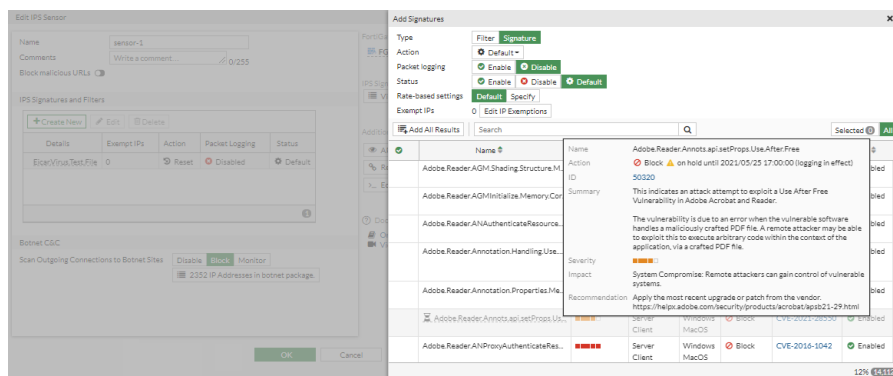
IPS signatures that are on hold (administrator-added delay for activation time) are highlighted in the GUI as follows:

- On hold signatures are grayed out with an hourglass icon beside the signature name.
- The signature tooltip displays the on hold expiry time.
- Users can still use on hold signatures in an IPS sensor profile; however, the profile will not block matching traffic. It will monitor it instead (logging in effect) until the on hold time expires.

After a hold time is configured in the CLI, go to **Security Profiles > IPS Signatures**. In this example, the *Adobe.Reader.Annots.api.setProps.Use.After.Free* signature is on hold. Hover over the grayed-out entry to view the tooltip, which includes the action and hold time expiry. On this page, all on hold signatures are displayed as on hold regardless of whether `override-signature-hold-by-id` is enabled.

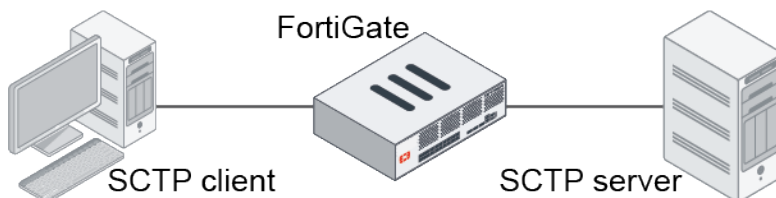


The same tooltip is available on the **Edit IPS Sensor (Security Profiles > Intrusion Prevention)** page when creating or editing the IPS signatures. In the **Add Signatures** pane when the **Type** is **Signature**, signatures on hold are only displayed as on hold if `override-signature-hold-by-id` is enabled.



Extend SCTP filtering capabilities - 7.0.1

A Stream Control Transmission Protocol (SCTP) dissector and Payload Protocol Identifier (PPID) filter can be used to either terminate the SCTP session, or replace the offending data chunk with zeros to keep the client and server sequence numbers synchronized. The SCTP filter action can also pass the data chunk.



To configure and test an SCTP filter:

1. Configure an SCTP filter profile that uses the reset action:

```

config sctp-filter profile
  edit "sctp"
    set comment "Demo profile"
  config ppid-filters

```

```

edit 1
    set ppid 112233
    set action reset
    set comment "test chunk"
next
end
next
end

```

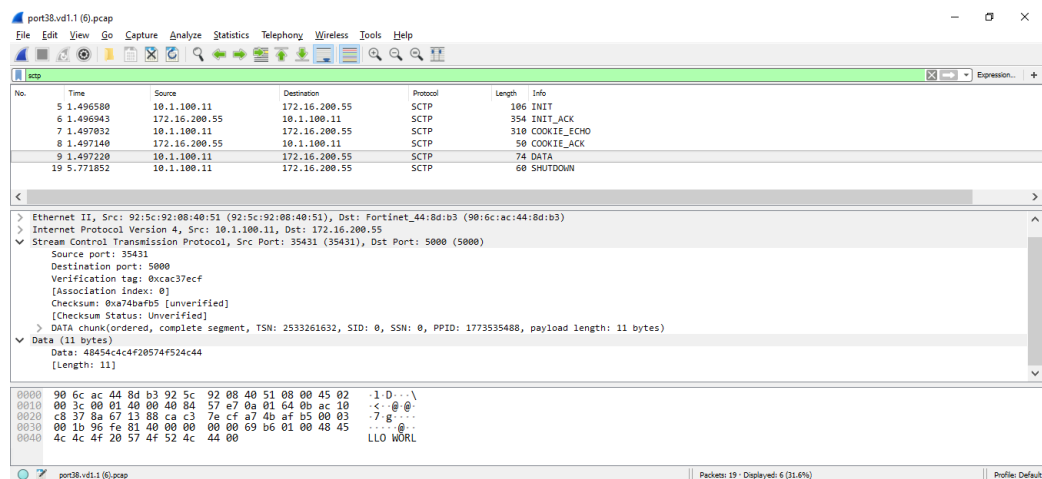
2. Use the SCTP filter profile in a firewall policy:

```

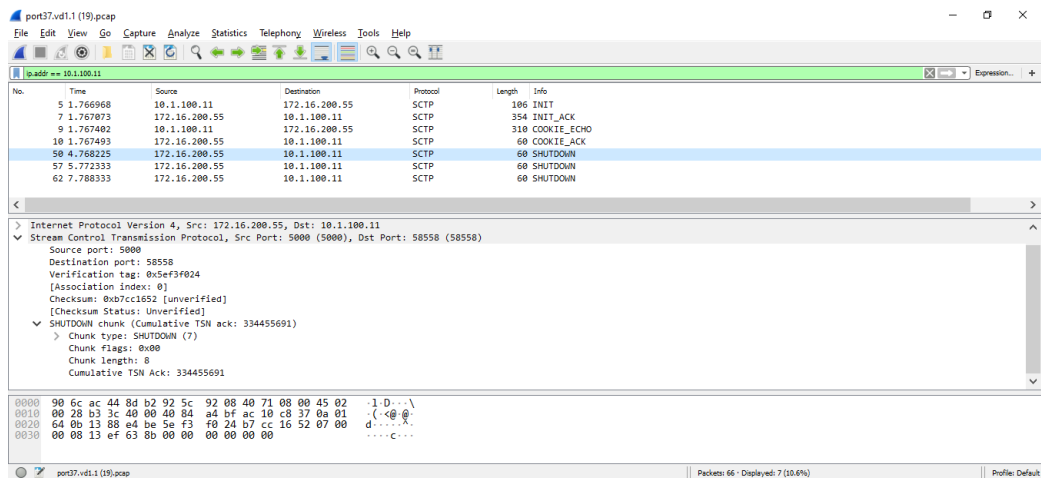
config firewall policy
edit 1
    set name "1"
    set srcintf "port38"
    set dstintf "port37"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set ssl-ssh-profile "new-deep-inspection"
    set sctp-filter-profile "sctp"
    set logtraffic all
next
end

```

3. On the SCTP client, confirm that the connection works and send a data chunk with PPID 112233.



4. The IPS engine detects the data chunk. The PPID matches the PPID filter, and the filter action is reset, so the data chunk is not received on the server, and the session is terminated.

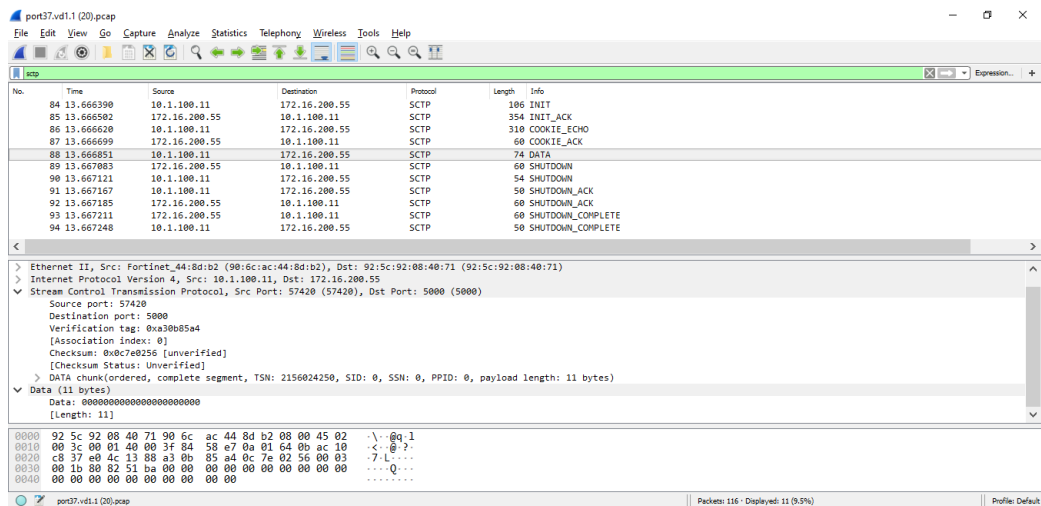


5. Change the filter action to replace:

```
config sctp-filter profile
edit "sctp"
    config ppid-filters
        edit 1
            set action replace
        next
    end
next
end
```

6. Resend the data chunk.

7. The IPS engine detects the data chunk. The PPID matches the PPID filter, and the filter action is replace, so the data chunk is replaced with zeros.



SSL/SSH inspection

This section includes information about SSL/SSH inspection related new features:

- [HTTP/2 support in proxy mode SSL inspection on page 427](#)
- [Define multiple certificates in an SSL profile in replace mode on page 428](#)

HTTP/2 support in proxy mode SSL inspection

Security profiles in proxy mode can perform SSL inspection on HTTP/2 traffic that is secured by TLS 1.2 or 1.3 using the Application-Layer Protocol Negotiation (ALPN) extension.

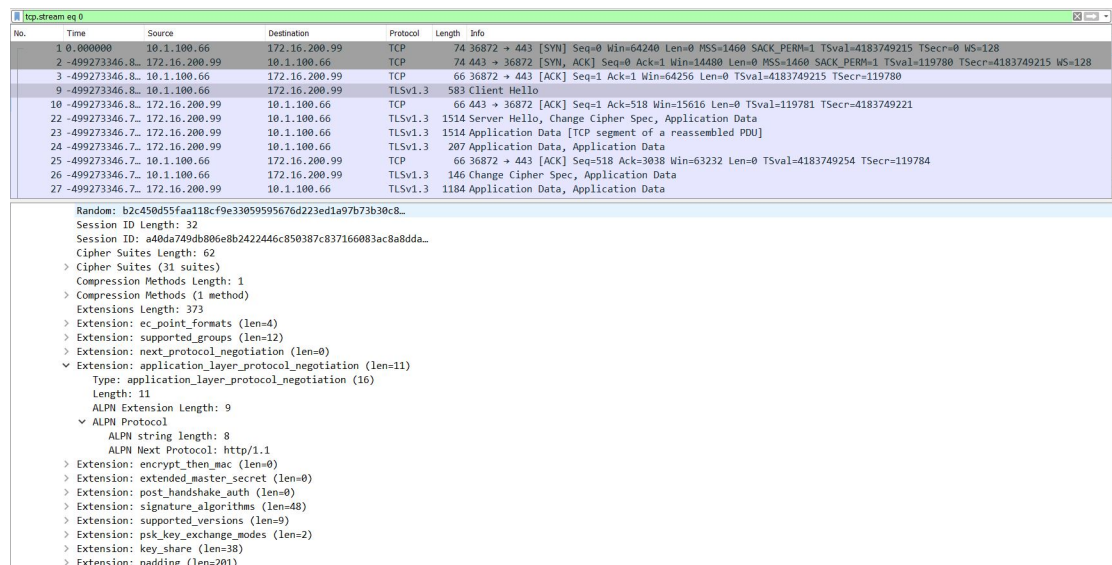
To set the ALPN support:

```
config firewall ssl-ssh-profile
    edit <profile>
        set supported-alpn {all | http1-1 | http2 | none}
    next
end
```

all	The FortiGate forwards ALPN extensions that use either HTTP/2 or HTTP/1.1. This is the default value.
http1-1	The FortiGate only forwards ALPN extensions that use HTTP/1.1. If the ALPN extension uses HTTP/2, then the FortiGate strips the ALPN header from the Client Hello.
http2	The FortiGate only forwards ALPN extensions that use HTTP/2. If the ALPN extension uses HTTP/1.1, then the FortiGate strips the ALPN header from the Client Hello.
none	The FortiGate always strips the ALPN header from the Client Hello when forwarding.

For example, if `supported-alpn` is set to `http2`, but the extension uses HTTP/1.1, the ALPN header is stripped from the Client Hello:

- Incoming packet capture:



- Outgoing packet capture:

No.	Time	Source	Destination	Protocol	Length	Info
6	4.99273346.8..	172.16.200.7	172.16.200.99	TCP	74	36872 → 443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=119781 TSecr=0 WS=512
7	4.99273346.8..	172.16.200.99	172.16.200.7	TCP	74	443 → 36872 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2720210585 TSecr=119781 WS=128
8	4.99273346.8..	172.16.200.7	172.16.200.99	TCP	66	36872 → 443 [ACK] Seq=1 Ack=1 Win=14848 Len=0 TSval=119781 TSecr=2720210585
11	4.99273346.8..	172.16.200.7	172.16.200.99	TLSv1.3	343	Client Hello
12	4.99273346.8..	172.16.200.99	172.16.200.7	TCP	66	443 → 36872 [ACK] Seq=1 Ack=278 Win=64896 Len=0 TSval=2720210589 TSecr=119781
13	4.99273346.8..	172.16.200.99	172.16.200.7	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
14	4.99273346.8..	172.16.200.7	172.16.200.99	TCP	66	36872 → 443 [ACK] Seq=278 Ack=1449 Win=17920 Len=0 TSval=119782 TSecr=2720210599
15	4.99273346.8..	172.16.200.99	172.16.200.7	TLSv1.3	798	Application Data, Application Data, Application Data
16	4.99273346.8..	172.16.200.7	172.16.200.99	TCP	66	36872 → 443 [ACK] Seq=278 Ack=2181 Win=20480 Len=0 TSval=119782 TSecr=2720210599
17	4.99273346.8..	172.16.200.7	172.16.200.99	TLSv1.3	140	Application Data
18	4.99273346.8..	172.16.200.99	172.16.200.7	TLSv1.3	337	Application Data

Ethernet II, Src: Fortinet_45:cd:7c (70:4c:a5:45:cd:7c), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 172.16.200.7, Dst: 172.16.200.99

Transmission Control Protocol, Src Port: 36872, Dst Port: 443, Seq: 1, Ack: 1, Len: 277

Transport Layer Security

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 272

▼ Handshake Protocol: Client Hello (1)

Handshake Type: Client Hello (1)

Length: 268

Version: TLS 1.2 (0x0303)

Random: fbf6d7fcd3143ec402d8f7909b445d53b3ef615b6194...

Session ID Length: 32

Session ID: f351fd57e62a89e9f351fd57e62a89e9f351fd57e62a89e9...

Cipher Suites Length: 62

▼ Cipher Suites (31 suites)

Compression Methods Length: 1

▼ Compression Methods (1 method)

Extensions Length: 133

▼ Extension: supported_versions (len=9)

▼ Extension: ec_point_formats (len=2)

▼ Extension: supported_groups (len=12)

▼ Extension: signature_algorithms (len=48)

▼ Extension: extended_master_secret (len=0)

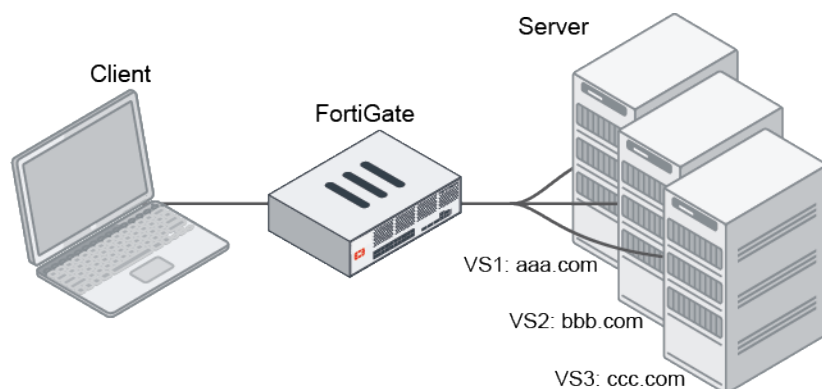
▼ Extension: key_share (len=38)

Define multiple certificates in an SSL profile in replace mode

Multiple certificates can be defined in an SSL inspection profile in replace mode (*Protecting SSL Server*). This allows multiple sites to be deployed on the same protected server IP address, and inspection based on matching the SNI in the certificate.

When the FortiGate receives the client and server hello messages, it will compare the SNI and CN with the certificate list in the SSL profile, and use the matched certificate as a replacement. If there is no matched server certificate in the list, then the first server certificate in the list is used as a replacement.

Example



To configure an SSL profile in replace mode with multiple certificates:

```
config firewall ssl-ssh-profile
  edit "multi-cert"
    set server-cert-mode replace
```

```

        set server-cert "bbb" "aaa"
    next
end

```

To configure a policy that uses the SSL profile:

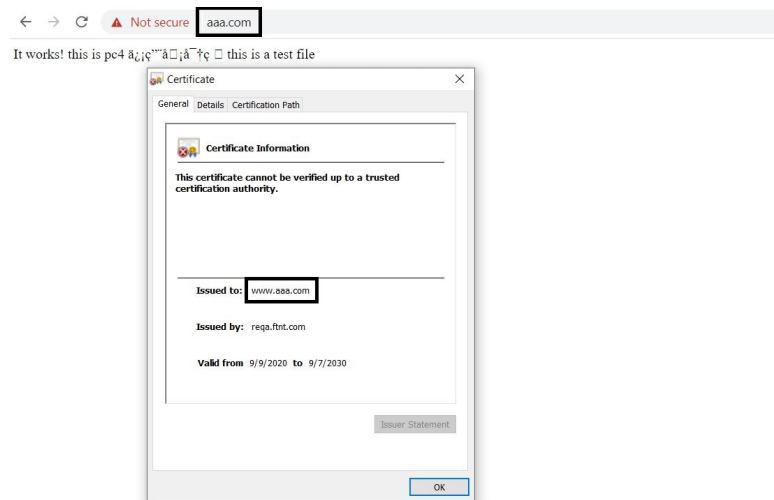
```

config firewall policy
    edit 1
        set name "multi-cert"
        set srcintf "port6"
        set dstintf "port11"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "multi-cert"
        set av-profile "default"
        set webfilter-profile "default"
        set logtraffic all
        set nat enable
    next
end

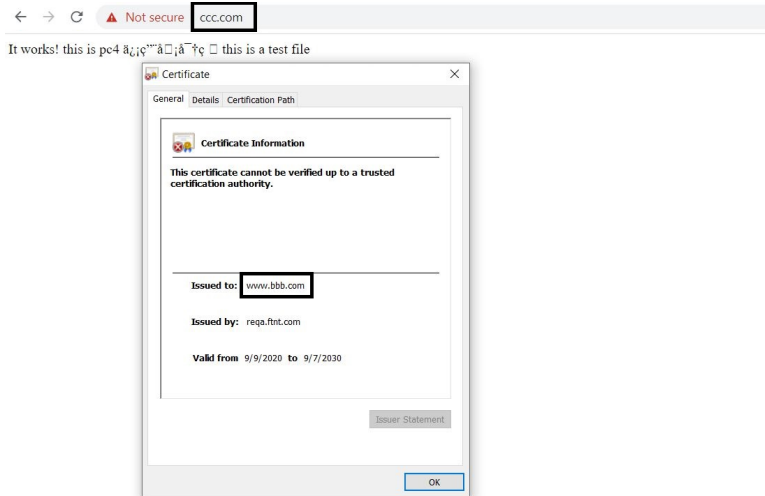
```

Results

If the Server Name Identification (SNI) matches the Common Name (CN) in the certificate list in the SSL profile, then the FortiGate uses the matched server certificate. In this example, when the client accesses *www.aaa.com*, the FortiGate will use the *aaa* certificate as a replacement.



If the Server Name Identification (SNI) does not match the Common Name (CN) in the certificate list in the SSL profile, then the FortiGate uses the first server certificate in the list. In this example, when the client accesses *www.ccc.com*, because there is no certificate for *www.ccc.com*, the FortiGate will use the *bbb* certificate as a replacement.



Others

This section includes information about other security profile related new features:

- [Support secure ICAP clients on page 430](#)
- [Add TCP connection pool for connections to ICAP server on page 431](#)
- [Improve WAD traffic dispatcher on page 432](#)
- [Video filtering on page 432](#)
- [DNS filter handled by IPS engine in flow mode on page 435](#)
- [DNS inspection with DoT and DoH on page 436](#)
- [Flow-based SIP inspection on page 439](#)
- [Scanning MSRP traffic 7.0.2 on page 441](#)

Support secure ICAP clients

A secure SSL connection from the FortiGate to the ICAP server can be configured as follows:

```
config icap server
    edit "server"
        set secure {enable | disable}
        set ssl-cert <certificate>
    next
end
```

To configure a secure ICAP client:

1. Configure the ICAP server:

```
config icap server
    edit "icap_server1"
        set ip-version 4
```

```

        set ip-address 192.168.10.2
        set port 11344
        set max-connections 100
        set secure enable
        set ssl-cert "ACCVRAIZ1"
    next
end

```



Port 11344 is the standard port for secure ICAP. This must be configured manually if the secure connection is enabled.

2. Configure the ICAP profile:

```

config icap profile
    edit "icap_profile1"
        set request enable
        set response enable
        set streaming-content-bypass enable
        set request-server "icap_server1"
        set response-server "icap_server1"
    next
end

```

3. Configure the firewall policy:

```

config firewall policy
    edit 1
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "protocols"
        set icap-profile "icap_profile1"
    next
end

```

Add TCP connection pool for connections to ICAP server

A TCP connection pool can maintain local-out TCP connections to the external ICAP server due to a backend update in FortiOS. TCP connections will not be terminated once data has been exchanged with the ICAP server, but instead are reused in the next ICAP session to maximize efficiency.

Use case

In this scenario, an ICAP profile is used as a UTM profile in an explicit web proxy policy, and a client visits web servers through this proxy policy.

Once the WAD is initialized, when a HTTP request is sent from the client to the server through the FortiGate with an ICAP profile applied to the matched proxy policy, a TCP connection is established between the FortiGate and the ICAP server to exchange data.

When an ICAP session is finished, the TCP connection is kept in the WAD connection pool. When another ICAP session needs to be established, the WAD will check if there are any idle connections available in the connection pool. If an idle connection is available, then it will be reused; otherwise, a new TCP connection is established for the ICAP session. This process can be checked in the WAD debug log.

Improve WAD traffic dispatcher

The WAD traffic dispatcher now allows incoming traffic to be directly distributed to the workers. This enhancement also allows source addresses to be exempt from proxy affinity, which allows traffic from the same source and different server to be distributed to workers in a round-robin configuration.

Use the following debugging command to verify that the WAD dispatcher distributed the traffic to the WAD workers:

```
# diagnose test application wad 12<integer><integer>
```



Use the index 1299 for all listeners.

To distribute traffic to different WAD workers:

```
config web-proxy global
    set proxy-fqdn "default.fqdn"
    set src-affinity-exempt-addr <IPv4 address> ...
    set src-affinity-exempt-addr6 <Pv6 address> ...
end
```

To verify the WAD dispatcher traffic distribution:

```
# diagnose test application wad 1204
Listener info: vf_id=0 local=0 port=(443) addr=[0.0.0.0]
    dispatcher fallback conn=0
    worker_idx=0 num_conn=3
    worker_idx=1 num_conn=1
```

In this example, the WAD dispatcher distributed traffic to two WAD workers.

Video filtering

With the video filter profile, you can filter YouTube videos by channel ID for a more granular override of a single channel, user, or video. The video filter profile is currently supported in proxy-based policies and requires SSL deep inspection.



In 7.0.1, restricting YouTube access is configured in the web filter profile. See [Restrict YouTube access](#) in the FortiOS Administration Guide for more information.

To configure a video filter in the GUI:

1. Go to *Security Profiles > Video Filter* and click *Create New*.
2. In the *Channel override list* section, click *Create New*. The *New Channel Override Entry* pane opens.
 - a. Enter a *Channel ID* and select an *Action*.

- b. Click *OK*.
3. Optionally, enable *Restrict YouTube access* and select a setting (*Moderate* or *Strict*).

4. Click *OK*.
5. In the CLI, enable the YouTube API query:

```
config videofilter youtube-key
edit 1
set key *****
set status enable
next
end
```

6. Create the firewall policy:
 - a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
 - b. For *Inspection Mode*, select *Proxy-based*.
 - c. Enable *Video Filter* and select the profile you created.

- d. For *SSL Inspection*, select *deep-inspection*.

The screenshot shows the 'New Policy' configuration window in FortiGate. The 'Inspection Mode' is set to 'Proxy-based'. Under 'Security Profiles', 'Video Filter' is enabled and set to 'channel_filter'. 'SSL Inspection' is enabled and set to 'deep-inspection'. The 'Additional Information' panel on the right shows links for API Preview, Edit in CLI, Documentation, Online Help, Video Tutorials, and Consolidated Policy Configuration.

- e. Configure the other settings as needed and click OK.

To configure a video filter in the CLI:

1. Create the channel filter:

```
config videofilter youtube-channel-filter
  edit 1
    set name "channel_filter"
    config entries
      edit 1
        set action block
        set channel-id "UCJHo4AuVomwMRzgkA5DQEOA"
      next
    end
  next
end
```

2. Create the video filter profile:

```
config videofilter profile
  edit "channel_filter"
    set youtube-channel-filter 1
    set youtube-restrict strict
  next
end
```

3. Enable the YouTube API query:

```
config videofilter youtube-key
  edit 1
    set key *****
    set status enable
  next
end
```


4. Create the firewall policy:

```

config firewall policy
  edit 1
    set name "video-filter"
    set srcintf "port1"
    set dstintf "port5"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode proxy
    set ssl-ssh-profile "deep-inspection"
    set videofilter-profile "channel_filter"
    set nat disable
  next
end

```

Vimeo

The video filter profile includes a setting to restrict Vimeo access, which can only be configured in the CLI.

To restrict Vimeo access:

```

config videofilter profile
  edit <name>
    set vimeo-restrict {7 | 134}
  next
end

```

```
vimeo-restrict {7 | 134}
```

Set the Vimeo restriction:

- 7: do not show mature content
- 134: do not show unrated and mature content

In 7.0.1, this setting has moved to the web filter profile:



```

config webfilter profile
  edit <name>
    config web
      set vimeo-restrict {7 | 134}
    end
  next
end

```

DNS filter handled by IPS engine in flow mode

In FortiOS 6.4, the DNS proxy daemon handles the DNS filter in flow and proxy mode policies. Starting in 7.0, the IPS engine handles the DNS filter in flow mode policies and queries the FortiGuard web filter server for FortiGuard

categories. In proxy mode, the DNS proxy daemon handles the DNS filter and queries the FortiGuard SDNS server for FortiGuard categories.

All features previously supported in the DNS filter profile are supported in flow mode:

- FortiGuard category rating
- Static domain filtering
- Remote category rating
- External IP block list
- Botnet domain and IP filtering
- DNS translation
- Safe search enforcement

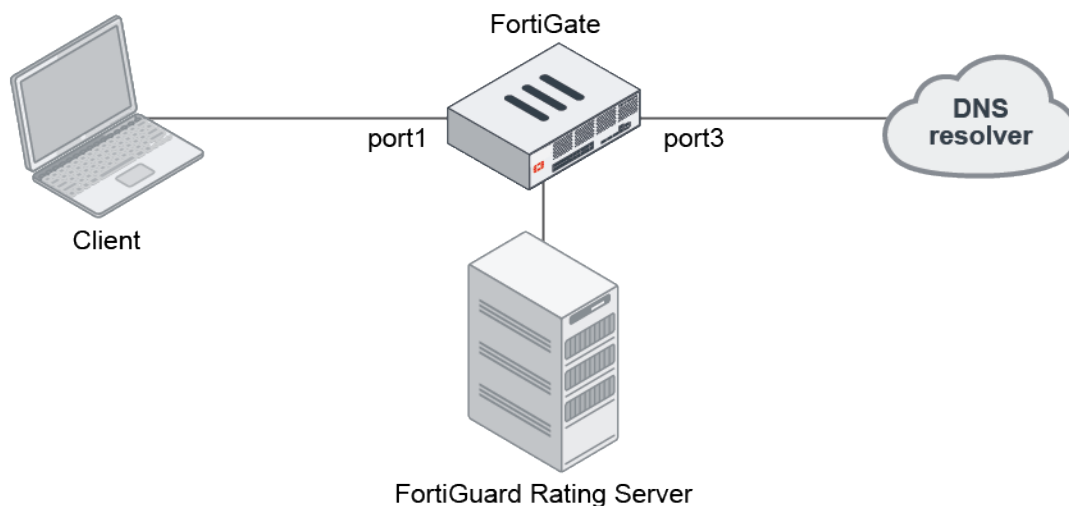


When a DNS filter profile is enabled in `config system dns-server`, the DNS proxy daemon handles the traffic.

DNS inspection with DoT and DoH

DNS over TLS (DoT) and DNS over HTTPS (DoH) are supported in DNS inspection. Prior to 7.0, DoT and DoH traffic silently passes through the DNS proxy. In 7.0, the WAD is able to handle DoT and DoH, and redirect DNS queries to the DNS proxy for further inspection.

In the following examples, the FortiGate inspects DNS queries made over DoT and DoH to a Cloudflare DNS server. The DNS filter profile blocks the education category.



To configure DNS inspection of DoT and DoH queries in the GUI:

1. Configure the SSL-SSH profile:
 - a. Go to *Security Profiles > SSL/SSH Inspection* and click *Create New*.
 - b. Set *Inspection method* to *Full SSL Inspection*. DoT and DoH can only be inspected using doing deep inspection.

- c. In the *Protocol Port Mapping* section, enable *DNS over TLS*.

- d. Configure the other settings as needed.

- e. Click **OK**.

2. Configure the DNS filter profile:

- a. Go to *Security Profiles > DNS Filter* and click *Create New*.

- b. Enable *Redirect botnet C&C requests to Block Portal*.

- c. Enable *FortiGuard Category Based Filter* and set the *Action* for the *Education* category to *Redirect to Block Portal*.

- d. Configure the other settings as needed.

- e. Click **OK**.

3. Configure the firewall policy:

- a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.

- b. Enable *DNS Filter* and select the profile you created.

- c. For *SSL Inspection*, select the profile you created.

- d. Configure the other settings as needed.

- e. Click **OK**.

To configure DNS inspection of DoT and DoH queries in the CLI:

1. Configure the SSL-SSH profile:

```
config firewall ssl-ssh-profile
  edit "ssl"
    config dot
      set status deep-inspection
      set client-certificate bypass
      set unsupported-ssl-cipher allow
      set unsupported-ssl-negotiation allow
```

```
        set expired-server-cert block
        set revoked-server-cert block
        set untrusted-server-cert allow
        set cert-validation-timeout allow
        set cert-validation-failure block
    end
next
end
```

2. Configure the DNS filter profile:

```
config dnsfilter profile
    edit "dnsfilter"
        config ftgd-dns
            config filters
                edit 1
                    set category 30
                    set action block
                next
            end
        end
        set block-botnet enable
    next
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "ssl"
        set webfilter-profile "webfilter"
        set dnsfilter-profile "dnsfilter"
        set nat enable
    next
end
```

Testing the connection

To query DNS over TLS:

1. Send a DNS query over TLS to the Cloudflare server 1.1.1.1 (this example uses `kdig` on an Ubuntu client). The `www.ubc.ca` domain belongs to the education category:

```
~$ kdig -d @1.1.1.1 +tls-ca +tls-host=cloudflare-dns.com www.ubc.ca
;; DEBUG: Querying for owner(www.ubc.ca.), class(1), type(1), server(1.1.1.1), port
(853), protocol(TCP)
;; DEBUG: TLS, imported 128 system certificates
```

```
;; DEBUG: TLS, received certificate hierarchy:
;; DEBUG: #1, C=US,ST=California,L=San Francisco,O=Cloudflare\, Inc.,CN=cloudflare-
dns.com
;; DEBUG:      SHA-256 PIN: elpYCnCs9ZtkQBI4+cb2QtZcyOl5UI9jMkSvbTsTad0=
;; DEBUG: #2, C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=Certificate
Authority,CN=FG3H1E5818903681,EMAIL=support@fortinet.com
;; DEBUG:      SHA-256 PIN: s48VtdODlNZfAG2g/92hMLhitU51qsP9pkHAUtTJ+f4=
;; DEBUG: TLS, skipping certificate PIN check
;; DEBUG: TLS, The certificate is trusted.
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(ECDSA-SECP256R1-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 56850
;; Flags: qr rd; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.ubc.ca.                IN      A

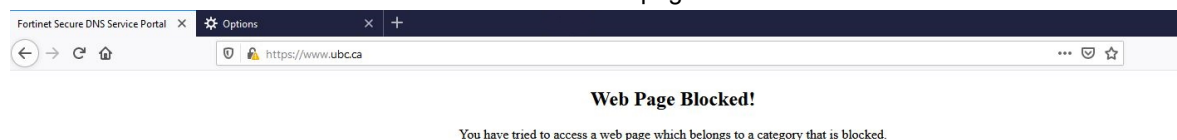
;; ANSWER SECTION:
www.ubc.ca.                60      IN      A      208.91.112.55

;; Received 44 B
;; Time 2021-03-12 06:53:37 UTC
;; From 1.1.1.1@853(TCP) in 6.0 ms
```

In this query, the FortiGate inspects the DNS query to the Cloudflare DNS server. It replaces the result with the IP of the FortiGuard block page, which successfully blocks the query.

To query DNS over HTTPS:

1. In your browser, enable DNS over HTTPS.
2. Go to www.ubc.ca. The website is redirected to the block page.



Flow-based SIP inspection

Flow-based SIP inspection is done by the IPS engine. This optimizes memory and CPU usage when VoIP profiles with SIP inspection are configured with other UTM profiles in a flow-based firewall policy because inspection is done entirely by the IPS engine. Proxy ALG features that are supported in flow mode include blocking scenarios, rate-limitation, and malformed header detection.

The inspection mode is selected in the firewall policy.

When upgrading to FortiOS 7.0.0:

- If `default-voip-alg-mode` is set to `proxy-based` (the default setting), all flow mode policies will be converted to proxy mode.
- If `default-voip-alg-mode` is set to `kernel-helper-based`, all flow mode policies that have a VoIP profile configured will be converted to proxy mode.



To configure the default VoIP ALG mode:

```
config system settings
    set default-voip-alg-mode {proxy-based | kernel-helper-based}
end
```

When upgrading to FortiOS 7.0.1:

- All firewall policies with a VoIP profile selected will be converted to proxy-based inspection.
- All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

Proxy ALG features available in flow mode:

```
config voip profile
    edit "demo_sip"
        set feature-set flow
        set comment "flow_based"
        config sip
            set status enable
            set register-rate-track {none | src-ip | dest-ip}
            set invite-rate-track {none | src-ip | dest-ip}
            set subscribe-rate-track {none | src-ip | dest-ip}
            set message-rate-track {none | src-ip | dest-ip}
            set notify-rate-track {none | src-ip | dest-ip}
            set refer-rate-track {none | src-ip | dest-ip}
            set update-rate-track {none | src-ip | dest-ip}
            set options-rate-track {none | src-ip | dest-ip}
            set ack-rate-track {none | src-ip | dest-ip}
            set prack-rate-track {none | src-ip | dest-ip}
            set info-rate-track {none | src-ip | dest-ip}
            set publish-rate-track {none | src-ip | dest-ip}
            set bye-rate-track {none | src-ip | dest-ip}
            set cancel-rate-track {none | src-ip | dest-ip}
            set malformed-header-no-require {discard | pass}
            set malformed-header-no-proxy-require {discard | pass}
            set ips-rtp {enable | disable}
        end
    end
next
end
```

```
...-rate-track {none |
    src-ip | dest-ip}
```

Track the packet protocol field.

- `none`: None (default)
- `src-ip`: Source IP
- `dest-ip`: Destination IP

malformed-header-no-require {discard pass}	Action for malformed SIP messages without a Require header. <ul style="list-style-type: none"> discard: Discard malformed messages. pass: Bypass malformed messages (default).
malformed-header-no-proxy-require {discard pass}	Action for malformed SIP messages without a Proxy-Require header (default = pass).
ips-rtp {enable disable}	Enable/disable allow IPS on RTP (default = enable).

To create and use a VoIP profile in a policy:

1. Create a VoIP profile that uses SIP with the flow-mode feature set and enable block register requests:

```
config voip profile
  edit "sip-flow"
    set feature-set flow
    config sip
      set block-register enable
    end
  next
end
```

2. Use the VoIP profile in a flow-based firewall policy:

```
config firewall policy
  edit 4
    set srcintf "port1"
    set dstintf "port9"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode flow
    set profile-protocol-options "protocol"
    set ssl-ssh-profile "ssl"
    set voip-profile "sip-flow"
    set nat enable
  next
end
```

Scanning MSRP traffic - 7.0.2

An MSRP (Message Session Relay Protocol) decoder in the IPS engine scans for IPS signatures against the application data. Malicious payload in the text message can be blocked. A VoIP profile using flow inspection mode must be configured in the firewall policy. An IPS profile must be configured in the firewall policy to inspect the payload.

```
config voip profile
  edit <name>
    set feature-set flow
    config msrp
      set status {enable | disable}
```

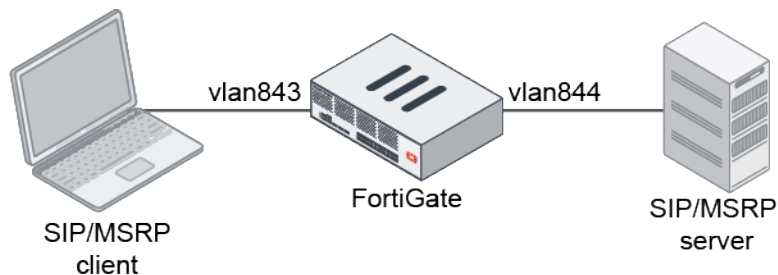
```

        set log-violations {enable | disable}
        set max-msg-size <integer>
        set max-msg-size-action {pass | block | reset | monitor}
    end
next
end

```

<code>status {enable disable}</code>	Enable/disable MSRP.
<code>log-violations {enable disable}</code>	Enable/disable logging of MSRP violations.
<code>max-msg-size <integer></code>	Maximum allowable MSRP message size, in bytes (0 - 65535, default = 0).
<code>max-msg-size-action {pass block reset monitor}</code>	Action for violating maximum MSRP message size: <ul style="list-style-type: none"> • pass: pass or allow matching traffic (default) • block: block or drop matching traffic • reset: reset sessions for matching traffic • monitor: pass and log matching traffic

Examples



In this first example, MSRP messages larger than 10 bytes will be blocked. The client sends an oversized MSRP message to the server. Message Automation & Protocol Simulation (MAPS™) is used, and a client-server model was configured to use the software to send MSRP traffic from vlan843 (client) to vlan844 (server) with plain text placed in the message field. The software uses the content of the `MsrpInputMessage.txt` file located in the default folder, where anything in that file will be sent by MSRP. The following text is used:

GL's Message Automation & Protocol Simulation (MAPS™) is a protocol simulation and conformance test tool that supports a variety of protocols such as SIP, MEGACO, MGCP, SS7, ISDN, GSM, MAP, CAS, LTE, UMTS, SS7 SIGTRAN, ISDN SIGTRAN, SIP I, GSM AoIP, Diameter and others. This message automation tool covers solutions for both protocol simulation and protocol analysis. The application includes various test plans and test cases to support the testing of real-time entities. Along with automation capability, the application gives users the unlimited ability to edit messages and control scenarios (message sequences).

To configure MSRP traffic scanning:

1. Configure the VoIP profile:

```

config voip profile
    edit msrp_test
        set feature-set flow
        config msrp
            set status enable

```



```
        set log-violations enable
        set max-msg-size 10
        set max-msg-size-action block
    end
next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 1
        set name "vdom3"
        set srcintf "vlan843"
        set dstintf "vlan844"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set voip-profile "msrp_test"
        set logtraffic all
    next
end
```

3. Verify the log:

```
# execute log filter category 4
# execute log display
1 logs found.
1 logs returned.
```

```
1: date=2021-06-10 time=17:21:19 eventtime=1623370879840284165 tz="-0700"
logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert"
vd="vdom3" severity="info" srcip=192.168.12.212 srccountry="Reserved"
dstip=192.168.12.213 srcintf="vlan843" srcintfrole="lan" dstintf="vlan844"
dstintfrole="lan" sessionid=27700 action="dropped" proto=6 service="MSRP" policyid=1
attack="MSRP.Max.Message.Size.Exceeded" srcport=20036 dstport=20036 direction="outgoing"
attackid=1000000 profile="g-default" ref="http://www.fortinet.com/ids/VID1000000"
incidentserialno=189792275 psrport=0 pdstport=0 msg="msrp_decoder:
MSRP.Max.Message.Size.Exceeded, msg_size=270 exceeds config maximum=10"
```

4. In MAPS, verify that the call was terminated:

The screenshot shows the MAPS application window. The top part is a table with columns: Sr No, Script Name, Profile, Call Info, Script Execution, Status, Events, Events Profile, Result, Total Iterations, and Completed Iterations. The bottom part shows a detailed call log for a specific test case, with columns for MAPS and DUT, and a list of SIP messages and timestamps.

Sr No	Script Name	Profile	Call Info	Script Execution	Status	Events	Events Profile	Result	Total Iterations	Completed Iterations
1	SipRegistrationControl.gls	Profile0001	CGPofScriptId:98-693436402-2281-7316	Start		None		Unknown	1	1
2	SipCallControl.gls	Profile0001	GLMAPS-113-633431911-2277-86208192-168-12-212	Start	Call Terminated	None		Pass	1	1

MAPS	DUT
INVITE	11:32:33.127000
100 Trying	11:32:33.190000
180 Ringing	11:32:33.207000
200 OK	11:32:33.340000
ACK	11:32:33.365000
BYE	11:32:38.201000
200 OK	11:32:38.244000

In this second example, malicious files will be blocked. The client sends an EICAR test sample to the server in an MSRP message. Message Automation & Protocol Simulation (MAPS™) is used, and a client-server model was configured to use the software to send MSRP traffic from vlan843 (client) to vlan844 (server) with a plain text EICAR file containing a virus in the message field. The following text is used:

X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

To configure MSRP traffic scanning:

1. Configure the VoIP profile:

```
config voip profile
  edit msrp_test
    set feature-set flow
  config msrp
    set status enable
    set log-violations enable
    set max-msg-size 0
    set max-msg-size-action pass
  end
next
end
```

2. Configure the IPS profile:

```
config ips sensor
  edit "msrp"
    set extended-log enable
    config entries
      edit 1
        set rule 7470 29844
        set status enable
        set action block
      next
    end
  next
end
```

3. Configure the firewall policy:

```
config firewall policy
  edit 1
    set name "vdom3"
    set srcintf "vlan843"
    set dstintf "vlan844"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set ssl-ssh-profile "certificate-inspection"
    set ips-sensor "msrp"
    set voip-profile "msrp_test"
    set logtraffic all
  next
end
```

4. Verify the log:

```
# execute log filter category 4
# execute log display
1 logs found.
1 logs returned.

1: date=2021-09-16 time=11:29:48 eventtime=1631816988947762597 tz="-0700"
logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert"
vd="vdom3" severity="info" srcip=192.168.12.212 srccountry="Reserved"
dstip=192.168.12.213 srcintf="vlan843" srcintfrole="lan" dstintf="vlan844"
dstintfrole="lan" sessionid=41344 action="dropped" proto=6 service="MSRP" policyid=1
attack="Eicar.Virus.Test.File" srcport=20069 dstport=20069 direction="outgoing"
attackid=29844 profile="msrp" ref="http://www.fortinet.com/ids/VID29844"
incidentserialno=123731970 psrport=0 pdstport=0 msg="file_transfer:
Eicar.Virus.Test.File,"
```

VPN

This section includes information about VPN related new features:

- [IPsec and SSL VPN on page 446](#)

IPsec and SSL VPN

This section includes information about IPsec and SSL VPN related new features:

- [Configurable IKE port on page 446](#)
- [Packet duplication for dial-up IPsec tunnels on page 449](#)
- [IPsec global IKE embryonic limit on page 453](#)
- [FortiGate as SSL VPN Client on page 454](#)
- [Dual stack IPv4 and IPv6 support for SSL VPN on page 463](#)
- [Disable the clipboard in SSL VPN web mode RDP connections 7.0.1 on page 473](#)
- [Use SSL VPN interfaces in zones 7.0.1 on page 478](#)
- [SSL VPN and IPsec VPN IP address assignments 7.0.1 on page 482](#)
- [Dedicated tunnel ID for IPsec tunnels 7.0.1 on page 487](#)

Configurable IKE port

Some ISPs block UDP port 500, preventing an IPsec VPN from being established. To accommodate this, the IKE and IKE NAT-T ports can be changed.

To set the IKE ports:

```
config system settings
    set ike-port <integer>
    set ike-natt-port <integer>
end
```

ike-port	UDP port for IKE/IPsec traffic (1024 - 65535, default = 500).
ike-natt-port	UDP port for IKE/IPsec traffic in NAT-T mode (1024 - 65535, default = 4500).

Example

In this example, the IKE port is set to 6000 and the IKE NAT-T port is set to 5000. A site to site VPN and a dial-up VPN with NAT are configured to show that the specified ports are used.

To set the IKE ports:

```
config system settings
    set ike-port 6000
    set ike-natt-port 5000
end
```

To configure and check the site to site VPN:**1. Configure the phase1 and phase2 interfaces:**

```
config vpn ipsec phase1-interface
    edit "s2s"
        set interface "port27"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
        chacha20poly1305-prfsha256
        set wizard-type static-fortigate
        set remote-gw 11.101.1.1
        set psksecret *****
    next
end
config vpn ipsec phase2-interface
    edit "s2s"
        set phaselname "s2s"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
        aes256gcm chacha20poly1305
        set src-addr-type name
        set dst-addr-type name
        set src-name "s2s_local"
        set dst-name "s2s_remote"
    next
end
```

2. Check the IKE gateway list and confirm that the specified port is used:

```
# diagnose vpn ike gateway list

vd: root/0
name: s2s
version: 2
interface: port27 17
addr: 173.1.1.1:6000 -> 11.101.1.1:6000
tun_id: 11.101.1.1
remote_location: 0.0.0.0
created: 194s ago
PPK: no
IKE SA: created 1/2 established 1/2 time 0/4500/9000 ms
IPsec SA: created 1/2 established 1/2 time 0/4500/9000 ms
...
```

3. Check the VPN tunnel list:

```
# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
```

```

-----
name=s2s ver=2 serial=1 173.1.1.1:6000->11.101.1.1:6000 tun_id=11.101.1.1 dst_mtu=1500
dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=17 lgwy=static/1 tun=tunnel/15 mode=auto/1 encap=none/520 options[0208]=npu
frag-rfc run_state=0 accept_traffic=1 overlay_id=0
...

```

To configure and check the dialup VPN with NAT:

1. Configure the phase1 and phase2 interfaces:

```

config vpn ipsec phase1-interface
    edit "server"
        set type dynamic
        set interface "port27"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set dpd on-idle
        set wizard-type static-fortigate
        set psksecret *****
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit "server"
        set phaselname "server"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set src-addr-type name
        set dst-addr-type name
        set src-name "server_local"
        set dst-name "server_remote"
    next
end

```

2. Check the IKE gateway list and confirm that the specified port is used:

```

# diagnose vpn ike gateway list

vd: root/0
name: server_0
version: 2
interface: port27 17
addr: 173.1.1.1:5000 -> 173.1.1.2:65416
tun_id: 173.1.1.2
remote_location: 0.0.0.0
created: 90s ago
nat: peer
PPK: no
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 1/1 established 1/1 time 0/0/0 ms
...

```

3. Check the VPN tunnel list:

```
# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=server_0 ver=2 serial=a 173.1.1.1:5000->173.1.1.2:65416 tun_id=173.1.1.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=17 lgwy=static/1 tun=tunnel/15 mode=dial_inst/3 encap=none/904 options
[0388]=npu rgwy-chg rport-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0
...
```

Packet duplication for dial-up IPsec tunnels

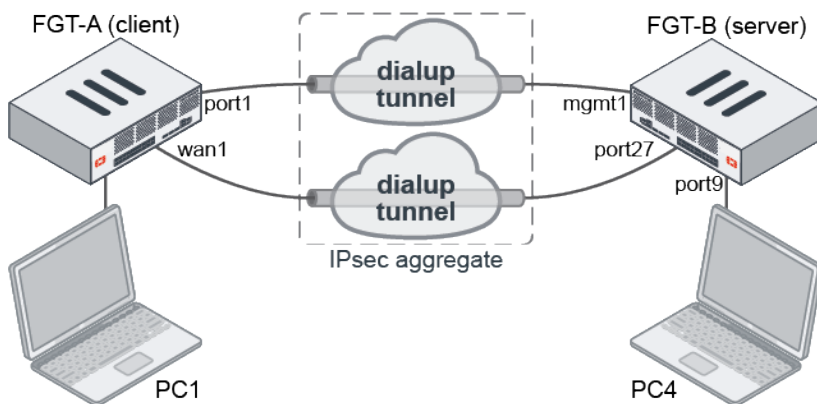
To support packet duplication on dial-up IPsec tunnels between sites, each spoke must be configured with a location ID. On the hub, packet duplication is performed on the tunnels in the IPsec aggregate that have the same location ID.

Multiple dial-up VPN tunnels from the same location can be aggregated on the VPN hub and load balanced based on the configured load balance algorithm.

IPsec traffic cannot be offloaded to the NPU.

Example

In this example, an IPsec aggregate tunnel is formed between two dial-up IPsec tunnels in order to support packet duplication.



To configure the client FortiGate (FGT-A):

1. Configure the IPsec tunnels:

```
config vpn ipsec phase1-interface
  edit "client1"
    set interface "port1"
    set peertype any
    set net-device disable
    set aggregate-member enable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set remote-gw 172.16.200.4
    set psksecret *****
  next
  edit "client2"
```

```
        set interface "wan1"
        set peertype any
        set net-device disable
        set aggregate-member enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 173.1.1.1
        set psksecret *****
    next
end
```

2. Configure an aggregate of the IPsec tunnels:

```
config system ipsec-aggregate
    edit "agg1"
        set member "client1" "client2"
    next
end
```

3. Configure the location ID:

```
config system settings
    set location-id 1.1.1.1
end
```

To configure the server FortiGate (FGT-B):

1. Configure the IPsec tunnels:

```
config vpn ipsec phase1-interface
    edit "server1"
        set type dynamic
        set interface "mgmt1"
        set peertype any
        set net-device disable
        set aggregate-member enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set psksecret *****
        set dpd-retryinterval 60
    next
    edit "server2"
        set type dynamic
        set interface "port27"
        set peertype any
        set net-device disable
        set aggregate-member enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set psksecret *****
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit "server1"
        set phase1name "server1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
        aes256gcm chacha20poly1305
    next
```



```

edit "server2"
    set phase1name "server2"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
next
end

```

2. Configure an aggregate of the IPsec tunnels:

```

config system ipsec-aggregate
    edit "server"
        set member "server1" "server2"
    next
end

```

3. Configure a firewall policy:

```

config firewall policy
    edit 1
        set srcintf "server"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end

```

To check the IPsec tunnel and aggregate state:

1. List all of the VPN tunnels:

```

FGDocs # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=server1 ver=1 serial=1 172.16.200.4:500->0.0.0.0:500 tun_id=1.0.0.0 dst_mtu=0 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=4 lgwy=static/1 tun=tunnel/15 mode=dialup/2 encap=none/4616 options[1208]=npu
frag-rfc accept_traffic=1 overlay_id=0

proxyid_num=0 child_num=2 refcnt=4 ilast=14210 olast=14210 ad=/0
stat: rxp=798921 txp=819074 rxb=121435992 txb=68802216
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
-----
name=server2 ver=1 serial=2 173.1.1.1:500->0.0.0.0:500 tun_id=2.0.0.0 dst_mtu=0 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=17 lgwy=static/1 tun=tunnel/15 mode=dialup/2 encap=none/4616 options[1208]=npu
frag-rfc accept_traffic=1 overlay_id=0

proxyid_num=0 child_num=1 refcnt=3 ilast=14177 olast=14177 ad=/0
stat: rxp=836484 txp=819111 rxb=137429352 txb=80046050
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
-----

```

```
name=server1_0 ver=1 serial=8 172.16.200.4:500->172.16.200.1:500 tun_id=172.16.200.1
dst_mtu=1500 dpd-link=on remote_location=1.1.1.1 weight=1
bound_if=4 lgwy=static/1 tun=tunnel/15 mode=dial_inst/3 encap=none/4744 options
[1288]=npu rgwy-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0

parent=server1 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=45 olast=45 ad=/0
stat: rxp=17176 txp=17176 rxb=2610752 txb=1442784
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=12
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=server1 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.1.100.0-10.1.100.255:0
  SA: ref=3 options=2a6 type=00 soft=0 mtu=1438 expire=42342/0B replaywin=2048
    seqno=4319 esn=0 replaywin_lastseq=00004319 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43186/43200
  dec: spi=0aef2a07 esp=aes key=16 12738c8a1db02c23bfed73eb3615a5a1
    ah=sha1 key=20 0f3edd28e3165d184292b4cd397a6edeef9d20dc
  enc: spi=2cb75665 esp=aes key=16 982b418e40f0bb18b89916d8c92270c0
    ah=sha1 key=20 08cbf9bf78a968af5cd7647dfa2a0db066389929
  dec:pkts/bytes=17176/1442784, enc:pkts/bytes=17176/2610752
  npu_flag=00 npu_rgwy=172.16.200.1 npu_lgwy=172.16.200.4 npu_selid=6 dec_npuid=0 enc_
npuid=0
-----
name=server1_1 ver=1 serial=a 172.16.200.4:500->172.16.200.3:500 tun_id=172.16.200.3
dst_mtu=0 dpd-link=on remote_location=2.2.2.2 weight=1
bound_if=4 lgwy=static/1 tun=tunnel/15 mode=dial_inst/3 encap=none/4744 options
[1288]=npu rgwy-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0

parent=server1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=27 olast=27 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=server1 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA: ref=3 options=2a6 type=00 soft=0 mtu=1280 expire=43167/0B replaywin=2048
    seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=0aef2a0a esp=aes key=16 4b7a17ba9d239e4ae5fe95ec100fca8b
    ah=sha1 key=20 7d3e058088f21e0c4f1c13c297293f06c8b592e7
  enc: spi=7e961809 esp=aes key=16 ecd1aa8657c5a509662aed45002d3990
    ah=sha1 key=20 d159e06c1cf0ded18a4e4ac86cbe5aa0315c21c9
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=172.16.200.3 npu_lgwy=172.16.200.4 npu_selid=9 dec_npuid=0 enc_
npuid=0
-----
name=server2_0 ver=1 serial=7 173.1.1.1:500->11.101.1.1:500 tun_id=11.101.1.1 dst_
mtu=1500 dpd-link=on remote_location=1.1.1.1 weight=1
bound_if=17 lgwy=static/1 tun=tunnel/15 mode=dial_inst/3 encap=none/4744 options
[1288]=npu rgwy-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0

parent=server2 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=45 olast=45 ad=/0
stat: rxp=16001 txp=17179 rxb=2113664 txb=1594824
```

```

dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=12
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=server2 proto=0 sa=1 ref=2 serial=1 add-route
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:10.1.100.0-10.1.100.255:0
SA: ref=6 options=2a6 type=00 soft=0 mtu=1438 expire=42342/0B replaywin=2048
seqno=431a esn=0 replaywin_lastseq=00003e80 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=43185/43200
dec: spi=0aef2a08 esp=aes key=16 394d4e444e90ccb5184e744d49aabe3c
ah=sha1 key=20 faabea35c2b9b847461cbd263c4856cfb679f342
enc: spi=2cb75666 esp=aes key=16 0b3a2fbac4d5610670843fa1925d1207
ah=sha1 key=20 97e99beff3d8f61a8638f6ef887006a9c323acd4
dec:pkts/bytes=16001/2113596, enc:pkts/bytes=17179/2762792
npu_flag=03 npu_rgwy=11.101.1.1 npu_lgwy=173.1.1.1 npu_selid=7 dec_npuid=1 enc_npuid=1

```

2. List the IPsec aggregate members:

```

# diagnose sys ipsec-aggregate list
server
members(3):
    server1_1
    server1_0
    server2_0

```

3. In the GUI, go to *Dashboard > Network* and expand the *IPsec* widget to review the traffic distributed over the aggregate members:

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
server2_0	11.101.1.1		2.11 MB	1.34 MB	server2_0	server2
server1_0	172.16.200.1		2.15 MB	1.19 MB	server1_0	server1
server1_1	172.16.200.3		0 B	0 B	server1_1	server1

Updated: 14:12:20

IPsec global IKE embryonic limit

When trying to establish thousands of tunnels simultaneously, a situation can arise where new negotiations starve other SAs from progressing to an established state in IKEv2. Enhancements to the IKE daemon includes prioritizing established SAs, offloading groups 20 and 21 to CP9, and optimizing the default embryonic limits for mid- and high-end platforms. The IKE embryonic limit is now configurable from the CLI.

```

config system ike
    set embryonic-limit <integer>
end

```

embryonic-limit <integer> Set the maximum number of IPsec tunnels to negotiate simultaneously (50 - 20000, default = 1000).

The following examples compare the number of established tunnels using an IKE embryonic limit of 50 and 10000 with 500 connections opened per second.

To configure an IKE embryonic limit of 50:

```
config system ike
    set embryonic-limit 50
end
```

To view the tunnel diagnostics:

```
# diagnose vpn tunnel stat
dev=1 attached=2087 tunnel=0 proxyid=2087 sa=2087 conc=0 up=2087 fenc=0 fdec=0 fasm=0
crypto_work=0 crypto_work_dropped=0
mr_grps=0 mr_children=0 mr_flood_list=0 mr_fw_list=0

# diagnose debug application ike -1
...
ike 0:a5d766dc52ebb36e/0000000000000000:3672: SA proposal chosen, matched gateway ph1
ike 0: embryonic limit 50 reached, dropping request 10.10.1.1->1.0.0.73:500
ike 0:a5d766dc52ebb36e/0000000000000000:3672: failed to create a connection
```

To configure an IKE embryonic limit of 10000:

```
config system ike
    set embryonic-limit 10000
end
```

To view the tunnel diagnostics:

```
# diagnose vpn tunnel stat
dev=1 attached=2952 tunnel=0 proxyid=2952 sa=2952 conc=0 up=2952 fenc=0 fdec=0 fasm=0
crypto_work=0 crypto_work_dropped=0
mr_grps=0 mr_children=0 mr_flood_list=0 mr_fw_list=0
```

FortiGate as SSL VPN Client

The FortiGate can be configured as an SSL VPN client, using an *SSL-VPN Tunnel* interface type. When an SSL VPN client connection is established, the client dynamically adds a route to the subnets that are returned by the SSL VPN server. Policies can be defined to allow users that are behind the client to be tunneled through SSL VPN to destinations on the SSL VPN server.

FortiOS can be configured as an SSL VPN server that allows IP-level connectivity in tunnel mode, and can act as an SSL VPN client that uses the protocol used by the FortiOS SSL VPN server. This allows hub-and-spoke topologies to be configured with FortiGates as both the SSL VPN hub and spokes.

For an IP-level VPN between a device and a VPN server, this can be useful to avoid issues caused by intermediate devices, such as:

- ESP packets being blocked.
- UDP ports 500 or 4500 being blocked.
- Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation.

If the client specified destination is *all*, a default route is effectively dynamically created on the SSL VPN client, and the new default route is added to the existing default route in the form of ECMP. Some examples how to configure routing are:

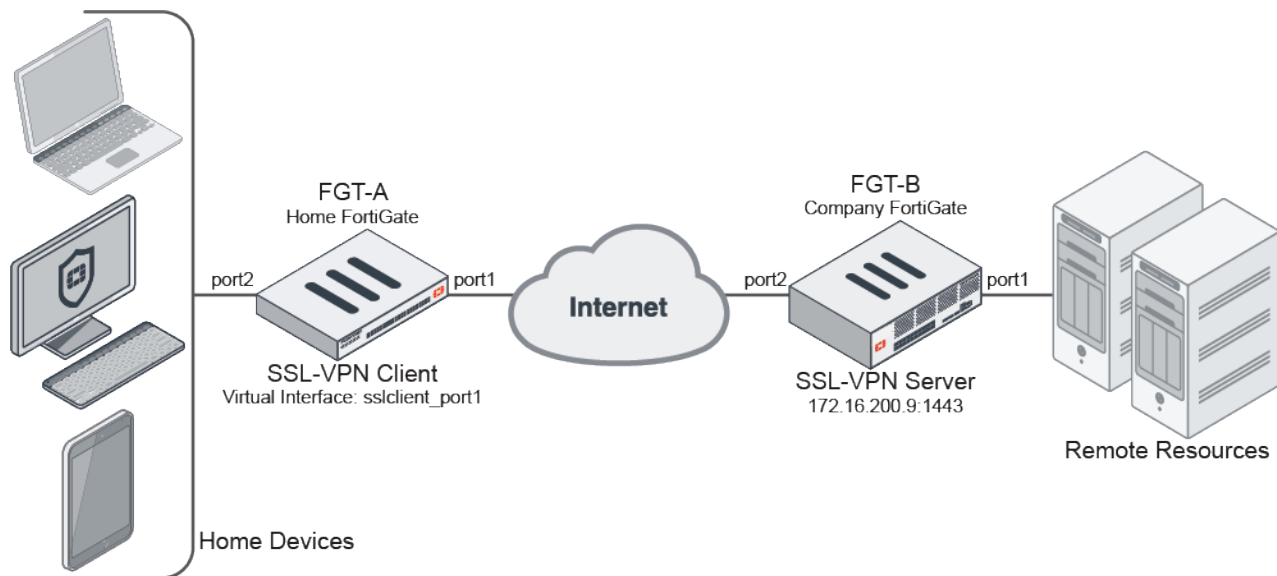
- To make all traffic default to the SSL VPN server and still have a route to the server's listening interface, on the SSL VPN client set a lower distance for the default route that is learned from the server.
- To include both default routes in the routing table, with the route learned from the SSL VPN server taking priority, on the SSL VPN client set a lower distance for the route learned from the server. If the distance is already zero, then increase the priority on the default route.
- To avoid a default being learned on the SSL VPN client, on the SSL VPN server define a specific destination.

Example

In this example, the home FortiGate (FGT-A) is configured as an SSL VPN client, and the company FortiGate (FGT-B) is configured as an SSL VPN server. After FGT-A connects to FGT-B, the devices that are connected to FGT-A can access the resources behind FGT-B.

The SSL VPN server has a custom server certificate defined, and the SSL VPN client user uses PSK and a PKI client certificate to authenticate. The FortiGates must have the proper CA certificate installed to verify the certificate chain to the root CA that signed the certificate.

Split tunneling is used so that only the destination addresses defined in the server's firewall policies are routed to the server, and all other traffic is connected directly to the internet.



Configure the SSL VPN server

To create a local user in the GUI:

1. Go to *User & Authentication > User Definition* and click *Create New*.
2. Use the wizard to create a local user named *client2*.

To create a PKI user in the GUI:



The PKI menu is only available in the GUI after a PKI user has been created using the CLI, and a CN can only be configured in the CLI.

1. Go to *User & Authentication > PKI* and click *Create New*.
2. Set the *Name* to *pki*.
3. Set *CA* to the CA certificate that is used to verify the client certificate.

4. Click *OK*.
5. In the CLI, specify the CN that must be matched. If no CN is specified, then any certificate that is signed by the CA will be valid and matched.

```
config user peer
    edit "pki"
        set cn "*.fos.automation.com"
    next
end
```

To create an SSL VPN portal in the GUI:

1. Go to *VPN > SSL-VPN Portals* and click *Create New*.
2. Set the *Name* to *testportal2*.
3. Set *Enable Split Tunneling* to *Enabled Based on Policy Destination*.
4. Set *Source IP Pools* to *SSLVPN_TUNNEL_ADDR1*.
5. Click *OK*.

To configure SSL VPN settings in the GUI:

1. Go to *VPN > SSL-VPN Settings*.
2. Set *Server Certificate* to *fgt_gui_automation*.
3. In the *Authentication/Portal Mapping* table click *Create New*:
 - a. Set *Users/Groups* to *client2*.
 - b. Set *Portal* to *testportal2*.
 - c. Click *OK*.
4. Click *OK*.
5. In the CLI, enable SSL VPN client certificate restrictive and set the user peer to *pki*:

```
config vpn ssl settings
    config authentication-rule
        edit 1
            set client-cert enable
            set user-peer "pki"
        next
    end
end
```

To create a firewall address in the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Set the *Name* to *bing.com*.
3. Set *Type* to *FQDN*.
4. Set *FQDN* to *www.bing.com*.
5. Click *OK*.

To create a firewall policy in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Configure the policy:

Name	<i>sslvpn2</i>
Incoming Interface	<i>SSL-VPN tunnel interface (ssl.root)</i>
Outgoing Interface	<i>port1</i>
Source	<i>Address: all</i> <i>User: client2</i>
Destination	<i>bing.com</i> : This FQDN resolves to 13.107.21.200 and 204.79.197.200. Traffic to these addresses is directed to the SSL VPN, while other traffic is routed to the remote devices' default adapters or interfaces. <i>mantis</i>
Schedule	<i>always</i>
Service	<i>ALL</i>
Action	<i>Accept</i>

3. Click *OK*.

To configure the SSL VPN server (FGT-B) in the CLI:

1. Create a local user:

```
config user local
  edit "client2"
    set passwd *****
  next
end
```

2. Create a PKI user:

```
config user peer
  edit "pki"
    set ca "CA_Cert_3"
    set cn "*.fos.automation.com"
  next
end
```

3. Create a new SSL VPN portal:

```

config vpn ssl web portal
  edit "testportal2"
    set tunnel-mode enable
    set ipv6-tunnel-mode enable
    set ip-pools "SSLVPN_TUNNEL_ADDR1"
    set split-tunneling enable
    set ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set ipv6-split-tunneling enable
    ....
  next
end

```

4. Configure SSL VPN settings, including the authentication rule for user mapping:

```

config vpn ssl settings
  set ssl-min-proto-ver tls1-1
  set servercert "fgt_gui_automation"
  set auth-timeout 0
  set login-attempt-limit 10
  set login-timeout 180
  set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
  set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
  set dns-suffix "sslvpn.com"
  set port 1443
  set source-interface "port2"
  set source-address "all"
  set source-address6 "all"
  set default-portal "testportal1"
  config authentication-rule
    edit 1
      set users "client2"
      set portal "testportal2"
      set client-cert enable
      set user-peer "pki"
    next
  end
end

```

5. Create a firewall address and policy. The destination addresses used in the policy are routed to the SSL VPN server.

```

config firewall address
  edit "bing.com"
    set type fqdn
    set fqdn "www.bing.com"
  next
end

config firewall policy
  edit 2
    set name "sslvpn2"
    set srcintf "ssl.root"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "mantis" "bing.com"
    set action accept
    set schedule "always"
  end

```



```
        set service "ALL"
        set nat enable
        set users "client2"
    next
end
```

Configure the SSL VPN client

To create a PKI user in the GUI:



The PKI menu is only available in the GUI after a PKI user has been created using the CLI, and a CN can only be configured in the CLI.

1. Go to *User & Authentication > PKI* and click *Create New*.
2. Set the *Name* to *fgt_gui_automation*.
3. Set *CA* to the CA certificate. The CA certificate allows the FortiGate to complete the certificate chain and verify the server's certificate, and is assumed to already be installed on the FortiGate.
4. Click *OK*.
5. In the CLI, specify the CN of the certificate on the SSL VPN server:

```
config user peer
    edit "fgt_gui_automation"
        set cn "*.fos.automation.com"
    next
end
```

To create an SSL VPN client and virtual interface in the GUI:

1. Go to *VPN > SSL-VPN Clients* and click *Create New*.
2. Expand the *Interface* drop down and click *Create* to create a new virtual interface:
 - a. Set the *Name* to *sslclient_port1*.
 - b. Set *Interface* to *port1*.
 - c. Under *Administrative Access*, select *HTTPS* and *PING*.

d. Click OK.

3. Configure the SSL VPN client:

Name	<i>sslclientTo9</i>
Interface	<i>sslclient_port1</i>
Server	<i>172.16.200.9</i>
Port	<i>1443</i>
Username	<i>client2</i>
Pre-shared Key	<i>*****</i>
Client Certificate	<i>fgtb_gui_automation</i> This is the local certificate that is used to identify this client, and is assumed to already be installed on the FortiGate. The SSL VPN server requires it for authentication.
Peer	<i>fgt_gui_automation</i>
Administrative Distance	Configure as needed.
Priority	Configure as needed.
Status	Enabled

4. Click OK.

To create a firewall policy in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Configure the policy:

Name	<i>policy_to_sslvpn_tunnel</i>
Incoming Interface	<i>port2</i>
Outgoing Interface	<i>sslclient_port1</i>

Source	<i>all</i>
Destination	<i>all</i>
Schedule	<i>always</i>
Service	<i>ALL</i>
Action	<i>Accept</i>

3. Click OK.

To configure the SSL VPN client (FGT-A) in the CLI:

1. Create the PKI user. Use the CA that signed the certificate *fgt_gui_automation*, and the CN of that certificate on the SSL VPN server.

```
config user peer
    edit "fgt_gui_automation"
        set ca "GUI_CA"
        set cn "*.fos.automation.com"
    next
end
```

2. Create the SSL interface that is used for the SSL VPN connection:

```
config system interface
    edit "sslclient_port1"
        set vdom "vdom1"
        set allowaccess ping https
        set type ssl
        set role lan
        set snmp-index 46
        set interface "port1"
    next
end
```

3. Create the SSL VPN client to use the PKI user and the client certificate *fgtb_gui_automation*:

```
config vpn ssl client
    edit "sslclientTo9"
        set interface "sslclient_port1"
        set user "client2"
        set psk 123456
        set peer "fgt_gui_automation"
        set server "172.16.200.9"
        set port 1443
        set certificate "fgtb_gui_automation"
    next
end
```

4. Create a firewall policy:

```
config firewall policy
    edit 1
        set name "policy_to_sslvpn_tunnel"
        set srcintf "port2"
        set dstintf "sslclient_port1"
        set srcaddr "all"
```

```

        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

```

Verification

After the tunnel is established, the route to 13.107.21.200 and 204.79.197.200 on FGT-A connects through the SSL VPN virtual interface *sslclient_port1*.

To check the routing table details:

```

(vdom1) # get router info routing-table details
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default

```

```

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 172.16.200.254, port1
C        10.0.1.0/24 is directly connected, link_11
C        10.1.100.0/24 is directly connected, port2
           is directly connected, port2
C        10.212.134.200/32 is directly connected, sslclient_port1
S        13.107.21.200/32 [10/0] is directly connected, sslclient_port1
C        172.16.200.0/24 is directly connected, port1
S        192.168.100.126/32 [10/0] is directly connected, sslclient_port1
S        204.79.197.200/32 [10/0] is directly connected, sslclient_port1

```

To check the added routing for an IPv6 tunnel:

```

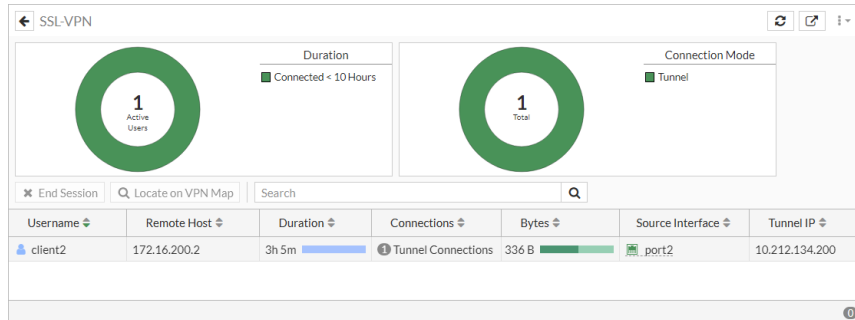
(vdom1) # get router info6 routing-table database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
        IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, B - BGP
        > - selected route, * - FIB route, p - stale info
Timers: Uptime

S      *> ::/0 [10/0] via 2000:172:16:200::254, port1, 00:00:01, [1024/0]
        *>      [10/0] via ::, sslclient_port1, 00:00:01, [1024/0]
C      *> ::1/128 via ::, vdom1, 03:26:35
C      *> 2000:10:0:1::/64 via ::, link_11, 03:26:35
C      *> 2000:10:1:100::/64 via ::, port2, 03:26:35
C      *> 2000:172:16:200::/64 via ::, port1, 03:26:35
C      *> 2001:1::1:100/128 via ::, sslclient_port1, 00:00:01
C      *> fe80::/64 via ::, port2, 03:26:35

```

To check the connection in the GUI:

1. On the SSL VPN server FortiGate (FGT-B), go to *Dashboard > Network* and expand the *SSL-VPN* widget.



2. On the SSL VPN client FortiGate (FGT-A), go to *VPN > SSL-VPN Clients* to see the tunnel list.

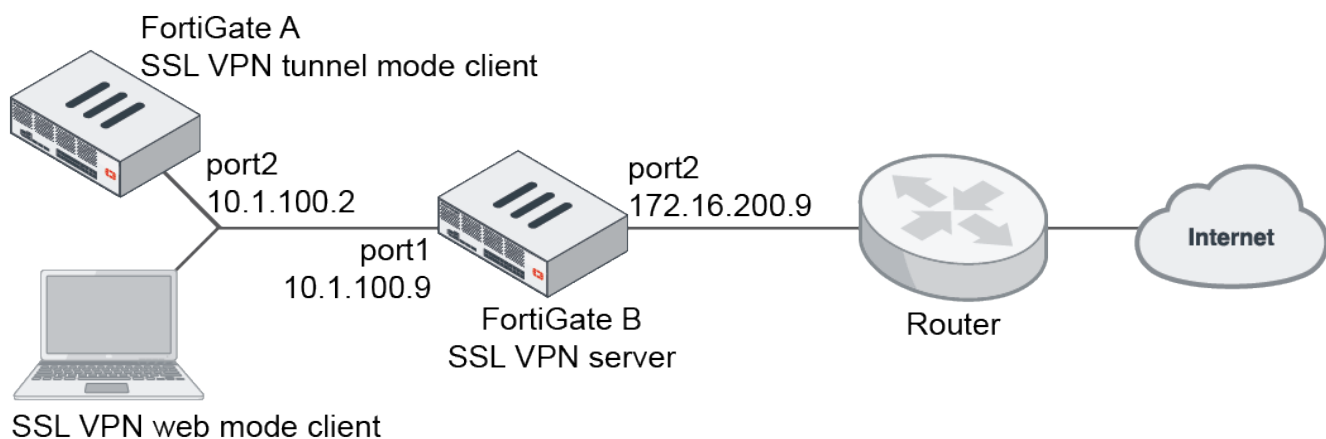
Dual stack IPv4 and IPv6 support for SSL VPN

Dual stack IPv4 and IPv6 support for SSL VPN servers and clients enables a client to establish a dual stack tunnel to allow both IPv4 and IPv6 traffic to pass through. FortiGate SSL VPN clients also support dual stack, which allows it to establish dual stack tunnels with other FortiGates.

Users connecting in web mode can connect to the web portal over IPv4 or IPv6. They can access bookmarks in either IPv4 or IPv6, depending on the preferred DNS setting of the web portal.

Example

In this example, FortiGate B works as an SSL VPN server with dual stack enabled. A test portal is configured to support tunnel mode and web mode SSL VPN.



FortiGate A is an SSL VPN client that connects to FortiGate B to establish an SSL VPN tunnel connection. It attempts to access www.bing.com and www.apple.com via separate IPv4 and IPv6 connections. Two addresses are configured on FortiGate B:

- *bing.com* uses IPv4 FQDN and resolves to 13.107.21.200 and 204.79.197.200.
- *apple_v6* uses IPv6 FQDN and resolves to 2600:140a:c000:385::1aca and 2600:140a:c000:398::1aca.

The server certificate used is `fgt_gui_automation`, and the CN is `*.fos.automation.com`.

A PC serves as a client to connect to FortiGate B in SSL VPN web mode. The PC can connect to the SSL VPN server over IPv4 or IPv6. Based on the preferred DNS setting, it will access the destination website over IPv4 or IPv6.



Dual stack tunnel mode support requires a supported client. In 7.0.0, a FortiGate in SSL VPN client mode can support dual stack tunnels. The current FortiClient 7.0.0 release does not support dual stack.

To configure an SSL VPN server in tunnel and web mode with dual stack support in the GUI:

1. Create a local user:
 - a. Go to *User & Authentication > User Definition* and click *Create New*. The *Users/Groups Creation Wizard* opens.
 - b. Set the *User Type* to *Local User* and click *Next*.
 - c. Enter the *Username* (*client2*) and password, then click *Next*.
 - d. Optionally, configure the contact information and click *Next*.
 - e. Click *Submit*.
2. Configure the addresses:
 - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
 - b. Enter the following for the IPv4 address:

Category	Address
Name	bing.com
Type	FQDN
FQDN	www.bing.com

- c. Click *OK*.
- d. Click *Create New > Address* and enter the following for the IPv6 address:

Category	IPv6 Address
Name	apple_v6
Type	FQDN
FQDN	www.apple.com

- e. Click *OK*.
3. Configure the SSL VPN portal:
 - a. Go to *VPN > SSL-VPN Portals* and click *Create New*.
 - b. Enter a name (*testportal1*).
 - c. Enable *Tunnel Mode* and for *Enable Split Tunneling*, select *Enable Based on Policy Destination*.
 - d. For *Source IP Pools*, add *SSLVPN_TUNNEL_ADDR1*.
 - e. Enable *IPv6 Tunnel Mode* and for *Enable Split Tunneling*, select *Enable Based on Policy Destination*.
 - f. For *Source IP Pools*, add *SSLVPN_TUNNEL_IPv6_ADDR1*.

g. Enable *Enable Web Mode*.

New SSL-VPN Portal

Name

Limit Users to One SSL-VPN Connection at a Time ☐

☒ Tunnel Mode

Enable Split Tunneling

☐ Disabled
All client traffic will be directed over the SSL-VPN tunnel.

☒ **Enabled Based on Policy Destination**
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

☐ Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override

Source IP Pools

☒ IPv6 Tunnel Mode

Enable IPv6 Split Tunneling

☐ Disabled
All client traffic will be directed over the SSL-VPN tunnel.

☒ **Enabled Based on Policy Destination**
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

☐ Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

IPv6 Routing Address Override

Source IPv6 Pools

FortiGate

[FGDocs](#)

Additional Information

[Online Help](#)

[Video Tutorials](#)

h. Click OK.

4. Configure the SSL VPN settings:

- a. Go to
- VPN > SSL-VPN Settings**
- and configure the following:

Listen on Interface(s)	port1
Listen on Port	1443
Restrict Access	Allow access from any host
Server Certificate	fgt_gui_automation
Address Range	Automatically assign addresses
DNS Server	Same as client system DNS
Authentication/Portal Mapping	Edit the <i>All Other Users/Groups</i> entry to use <i>testportal1</i> .

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s) port1 + ×

Listen on Port 1443

Web mode access will be listening at <https://10.1.100.9:1443>
[https://\[2000:10:1:100::9\]:1443](https://[2000:10:1:100::9]:1443)

Redirect HTTP to SSL-VPN ☐

Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout ☒

Inactive For 300 Seconds

Server Certificate fgt_gui_automation

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range Automatically assign addresses Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210, fdff:ffff::/120

DNS Server Same as client system DNS Specify

Specify WINS Servers ☐

Authentication/Portal Mapping ⓘ

+ Create New Edit Delete Send SSL-VPN Configuration

Users/Groups	Realm	Portal
All Other Users/Groups	/	testportal1

Apply

Additional Information

API Preview

Edit in CLI

SSL VPN Setup Guides

Web Mode

Web Mode for Remote User

Tunnel Mode

Full Tunnel for Remote User

Split Tunnel for Remote User

Tunnel Mode Host Check

Multi-Realm

Multi-Realm

Authentication

Certificate Authentication

LDAP-Integrated Certificate Authentication

FortiToken Mobile Push Authentication

RADIUS on FortiAuthenticator

RADIUS and FortiToken Mobile Push on FortiAuthenticator

Local User Password Policy

RADIUS Password Renew on FortiAuthenticator

LDAP User Password Renew

VPN Setup on FortiClient

Configuring an SSL VPN Connection

Troubleshooting

Troubleshooting

Documentation

Online Help

Video Tutorials

Security Rating Issues

Show Dismissed

- b. Click
- Apply**
- .

- c. Enable dual stack in the CLI:

```
config vpn ssl settings
    set dual-stack-mode enable
end
```


5. Configure the firewall policy:
 - a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
 - b. Enter the following:

Name	sslvpn
Incoming Interface	ssl.root
Outgoing Interface	port2
Source	all (IPv4), all (IPv6), client2
Destination	bing.com, apple_v6
Schedule	Always
Service	All
NAT	Enabled

- c. Click *OK*.

To configure FortiGate A as an SSL VPN client in the GUI:

1. Create a peer to verify the server certificate:



The PKI menu is only available in the GUI (*User & Authentication > PKI*) after a PKI user has been created using the CLI, and a CN can only be configured in the CLI.
If the CA is not known or is public, import the CA that signed the server certificate.

- a. Go to *User & Authentication > PKI* and click *Create New*.
 - b. Set the *Name* to *fgt_gui_automation*.
 - c. Set *CA* to the CA certificate that is used to verify the server certificate.
 - d. Click *OK*.
 - e. In the CLI, specify the CN that must be matched:

```
config user peer
  edit "fgt_gui_automation"
    set ca "GUI_CA"
    set cn "/*.fos.automation.com"
  next
end
```

2. Configure the SSL VPN client:
 - a. Go to *VPN > SSL-VPN Clients* and click *Create New*.
 - b. In the *Interface* dropdown, click *Create*.
 - i. Enter a Name (*sslclient_port2*).
 - ii. Set *Interface* to *port2*.

iii. Set *Role* to *LAN*.

The screenshot shows the 'New SSL-VPN Client' configuration window. The 'New Interface' tab is selected. The configuration includes:

- Name:** sslclient_port2
- Alias:** (empty)
- Type:** SSL-VPN Tunnel
- Interface:** port2
- VRF ID:** 0
- Virtual domain:** vdom1
- Role:** LAN
- Administrative Access:**
 - IPv4:**
 - ☐ HTTPS
 - ☐ FMG-Access
 - ☐ FTM
 - IPv6:**
 - ☐ HTTPS
 - ☐ FMG-Access
 - ☐ Security Fabric Connection
 - HTTP:** ☐ HTTP
 - SSH:** ☐ SSH
 - RADIUS Accounting:** ☐ RADIUS Accounting
 - PING:** ☐ PING
 - SNMP:** ☐ SNMP
 - Security Fabric Connection:** ☐ Security Fabric Connection
- Stateless Address Auto-configuration (SLAAC):** ☐ SLAAC
- DHCPv6 Server:** ☐ DHCPv6 Server
- Network:**
 - Explicit web proxy:** ☐ Explicit web proxy
 - Explicit FTP proxy:** ☐ Explicit FTP proxy
- Traffic Shaping:**
 - Outbound shaping profile:** ☐ Outbound shaping profile
- Miscellaneous:**
 - Comments:** (empty)
 - Status:** ☒ Enabled ☐ Disabled

Buttons: OK, Cancel

iv. Click *OK*.

c. Configure the SSL VPN client:

Name	sslclientTo9
Interface	sslclient_port2
Server	Either IPv4 address <i>10.1.100.9</i> or IPv6 address <i>2000:10:1:100::9</i> can be used and will have the same results.
Port	1443
Username	client2
Pre-shared Key	*****
Peer	fgt_gui_automation
Status	Enabled

d. Click *OK*.

To configure an SSL VPN server in tunnel and web mode with dual stack support in the CLI:**1. Create a local user:**

```
config user local
    edit "client1"
        set type password
        set passwd *****
    next
end
```

2. Configure the addresses:

```
config firewall address
    edit "bing.com"
        set type fqdn
        set fqdn "www.bing.com"
    next
end

config firewall address6
    edit "apple_v6"
        set type fqdn
        set fqdn "www.apple.com"
    next
end
```

3. Configure the SSL VPN portal:

```
config vpn ssl web portal
    edit "testportal1"
        set tunnel-mode enable
        set ipv6-tunnel-mode enable
        set web-mode enable
        set ip-pools "SSLVPN_TUNNEL_ADDR1"
        set ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
        set split-tunneling enable
        set ipv6-split-tunneling enable
    next
end
```

4. Configure the SSL VPN settings:

```
config vpn ssl settings
    set servercert "fgt_gui_automation"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 1443
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "testportal1"
    set dual-stack-mode enable
end
```

5. Configure the firewall policy:

```
config firewall policy
    edit 1
        set name "sslvpn"
```

```

        set srcintf "ssl.root"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "bing.com"
        set srcaddr6 "all"
        set dstaddr6 "apple_v6"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
        set users "client2"
    next
end

```

To configure FortiGate A as an SSL VPN client in the CLI:

1. Create a peer to verify the server certificate:

```

config user peer
    edit "fgt_gui_automation"
        set ca "GUI_CA"
        set cn "*.fos.automation.com"
    next
end

```

2. Configure the interface:

```

config system interface
    edit "sslclient_port2"
        set vdom "vdom1"
        set type ssl
        set role lan
        set snmp-index 46
        set interface "port2"
    next
end

```

3. Configure the SSL VPN client. Either IPv4 address 10.1.100.9 or IPv6 address 2000:10:1:100::9 can be used and will have the same results:

```

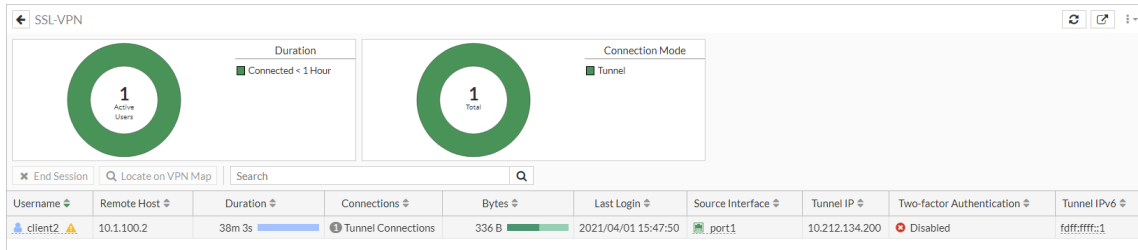
config vpn ssl client
    edit "sslclientTo9"
        set interface "sslclient_port2"
        set user "client2"
        set psk *****
        set peer "fgt_gui_automation"
        set server {10.1.100.9 | 2000:10:1:100::9}
        set port 1443
    next
end

```

Testing dual stack with tunnel mode

To verify the SSL VPN tunnel connection in the GUI:

1. On FortiGate B, go to *Dashboard > Network*.
2. Expand the *SSL-VPN* widget.



To verify the SSL VPN tunnel connection in the CLI:

1. On FortiGate B, verify that the client is assigned with both IPv4 and IPv6 addresses:

```
(root) # get vpn ssl monitor
SSL VPN Login Users:
  Index  User   Group   Auth Type      Timeout      Auth-Timeout  From      HTTP
  in/out  HTTPS in/out   Two-factor Auth
  0      client2
0/0      0/0      0
          1 (1)
          292
          2147483647
          10.1.100.2

SSL VPN sessions:
  Index  User   Group   Source IP      Duration      I/O Bytes      Tunnel/Dest IP
  0      client2
10.212.134.200, fdff:ffff::1
          10.1.100.2
          5427
          1756/1772
```

2. On FortiGate A, verify the routing tables.
 - a. IPv4 with resolved addresses for www.bing.com:

```
(vdom1) # get router info routing-table database
...
Routing table for VRF=0
S    *> 0.0.0.0/0 [10/0] via 172.16.200.254, port1
C    *> 10.0.1.0/24 is directly connected, link_11
C    *> 10.1.100.0/24 is directly connected, port2
C    *> 10.212.134.200/32 is directly connected, sslclient_port2
S    *> 13.107.21.200/32 [10/0] is directly connected, sslclient_port2
C    *> 172.16.200.0/24 is directly connected, port1
S    *> 204.79.197.200/32 [10/0] is directly connected, sslclient_port2
```

- b. IPv6 with resolved addresses for www.apple.com:

```
(vdom1) # get router info6 routing-table database
...
S    *> ::/0 [10/0] via 2000:172:16:200::254, port1, 01:57:23, [1024/0]
C    *> ::1/128 via ::, vdom1, 06:12:54
C    *> 2000:10:0:1::/64 via ::, link_11, 06:12:54
C    *> 2000:10:1:100::/64 via ::, port2, 06:12:54
C    *> 2000:172:16:200::/64 via ::, port1, 06:12:54
S    *> 2600:140a:c000:385::1aca/128 [10/0] via ::, sslclient_port2, 01:33:08,
[1024/0]
```

```
S    *> 2600:140a:c000:398::1aca/128 [10/0] via ::, sslclient_port2, 01:33:08,
[1024/0]
C    *> fdff:ffff::/120 via ::, sslclient_port2, 01:33:08
C    *> fe80::/64 via ::, port2, 06:12:54
```

To test the address connections using ping:

1. On FortiGate A, ping www.bing.com using IPv4 ping:

```
# execute ping www.bing.com
PING www-bing-com.dual-a-0001.a-msedge.net (13.107.21.200): 56 data bytes
64 bytes from 13.107.21.200: icmp_seq=0 ttl=117 time=1.8 ms
...
```

2. On FortiGate B, sniff for IPv4 ICMP packets and observe the results:

```
# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
9.675101 ssl.root in 10.212.134.200 -> 13.107.21.200: icmp: echo request
9.675219 port2 out 172.16.200.9 -> 13.107.21.200: icmp: echo request
9.676698 port2 in 13.107.21.200 -> 172.16.200.9: icmp: echo reply
9.676708 ssl.root out 13.107.21.200 -> 10.212.134.200: icmp: echo reply
...
```

3. On FortiGate A, ping www.apple.com using IPv6 ping:

```
# execute ping6 www.apple.com
PING www.apple.com (2600:140a:c000:385::1aca): 56 data bytes
64 bytes from 2600:140a:c000:385::1aca: icmp_seq=1 ttl=52 time=1.88 ms
...
```

4. On FortiGate B, sniff for IPv6 ICMP packets and observe the results:

```
# diagnose sniffer packet any icmp6 4
interfaces=[any]
filters=[icmp6]
3.564296 ssl.root in fdff:fff::1 -> 2600:140a:c000:385::1aca: icmp6: echo request seq 1
3.564435 port2 out 2000:172:16:200::9 -> 2600:140a:c000:385::1aca: icmp6: echo request
seq 1
3.565929 port2 in 2600:140a:c000:385::1aca -> 2000:172:16:200::9: icmp6: echo reply seq
1 [flowlabel 0x1fdff]
3.565953 ssl.root out 2600:140a:c000:385::1aca -> fdff:fff::1: icmp6: echo reply seq 1
[flowlabel 0x1fdff]
...
```

Testing dual stack with web mode

In SSL VPN web mode, users can access both IPv4 and IPv6 bookmarks in the portal. The attribute, `prefer-ipv6-dns` can be enabled to prefer querying IPv6 DNS first, or disabled to prefer querying IPv4.

To test an IPv4 connection to the web portal and access www.bing.com over IPv6:

1. On FortiGate B, prioritize resolving IPv6 addresses:

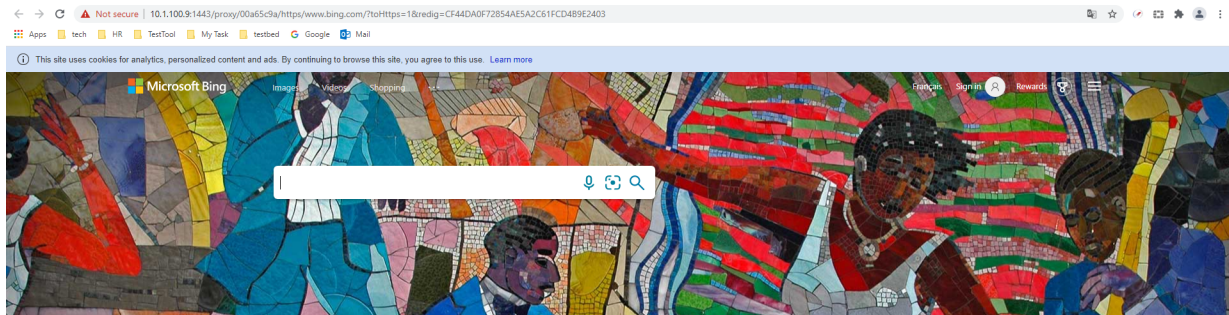
```
config vpn ssl web portal
  edit "testportal1"
    set prefer-ipv6-dns enable
```

```

next
end

```

2. Log in to the web portal in the browser over the IPv4 address 10.1.100.9.
3. Create a new HTTP/HTTPS bookmark named *bing* for the URL www.bing.com.
4. Click the *bing* bookmark. The bing page will open over IPv6.



To test an IPv6 connection to the web portal and access www.apple.com over IPv4:

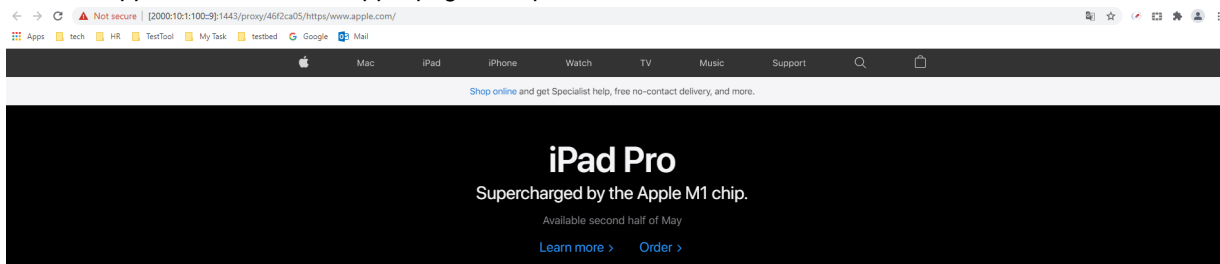
1. On FortiGate B, prioritize resolving IPv4 addresses:

```

config vpn ssl web portal
  edit "testportal1"
    set prefer-ipv6-dns disable
  next
end

```

2. Log in to the web portal in the browser over the IPv6 address [2000:10:1:100::9].
3. Create a new HTTP/HTTPS bookmark named *apple* for the URL www.apple.com.
4. Click the *apple* bookmark. The apple page will open over IPv4.

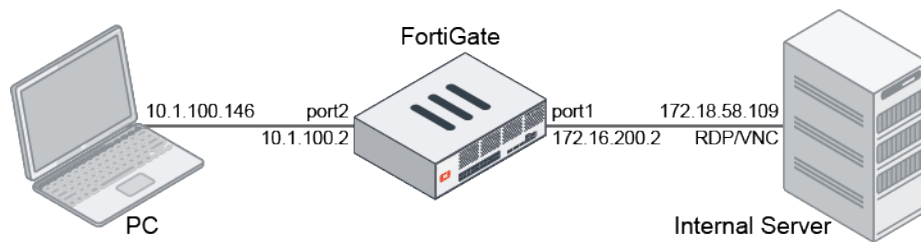


Disable the clipboard in SSL VPN web mode RDP connections - 7.0.1

In web portal profiles, the clipboard can be disabled for SSL VPN web mode RDP/VNC connections. User will not be able to copy and paste content to or from the internal server.

Example

In this example, two groups of users are using SSL VPN web mode to access internal servers with RDP/VNC. One group is allowed to copy and paste content to and from the internal server using the clipboard, while the other is not.



To configure the SSL VPN portals in the GUI:

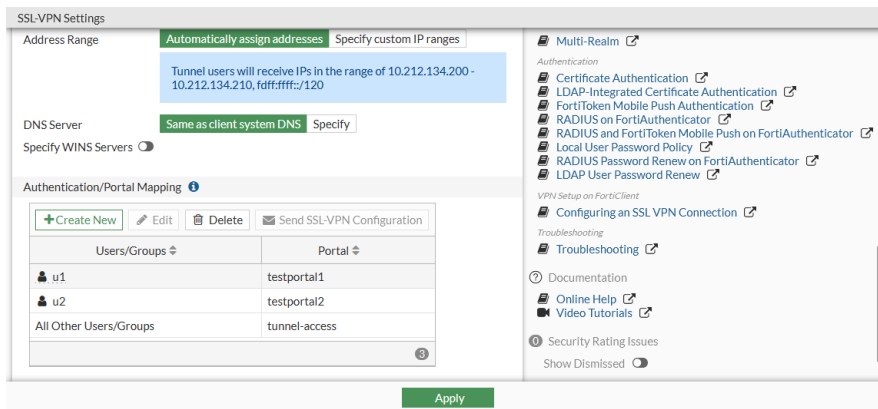
1. Go to **VPN > SSL-VPN Portals** and click **Create New**.
2. Enter a name for the portal, such as *testportal1*.
3. Enable **Enable Web Mode** and enable **RDP/VNC clipboard** to allow copying and pasting.
4. Configure the remaining settings as needed.

5. Click **OK**.
6. Click **Create New** again.
7. Enter a name for the portal, such as *testportal2*.
8. Enable **Enable Web Mode** and disable **RDP/VNC clipboard** to prevent copying and pasting.
9. Configure the remaining settings as needed.

10. Click **OK**.

To configure the SSL VPN settings in the GUI:

1. Go to *VPN > SSL-VPN Settings*.
2. Set *Listen on Interface* to port2.
3. In the *Authentication/Portal Mapping* table, add the users to each of the portals:
 - a. Click *Create New*.
 - b. Set *Users/Groups* to *u1* and *Portal* to *testportal1*.
 - c. Click *OK*, then click *Create New* again.
 - d. Set *Users/Groups* to *u2* and *Portal* to *testportal2*.
 - e. Click *OK*.
4. Configure the remaining settings as needed.



5. Click *Apply*.

To configure a firewall policy for SSL VPN in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Set a name for the policy, such as *policy_to_sslvpn_tunnel*.
3. Set *Incoming Interface* to the SSL VPN tunnel interface and *Outgoing Interface* to port1.
4. Set *Source* to the users, *u1* and *u2*, and all addresses.
5. Set *Destination* to all addresses.
6. Set *Schedule* to *always*, *Service* to *All*, and *Action* to *Accept*.
7. Configure the remaining settings as needed.
8. Click *OK*.

To test if the users can use the clipboard:

1. On the PC, open a web browser and log in to the web portal as user *u1*.
2. Access the internal server using RDP/VNC.

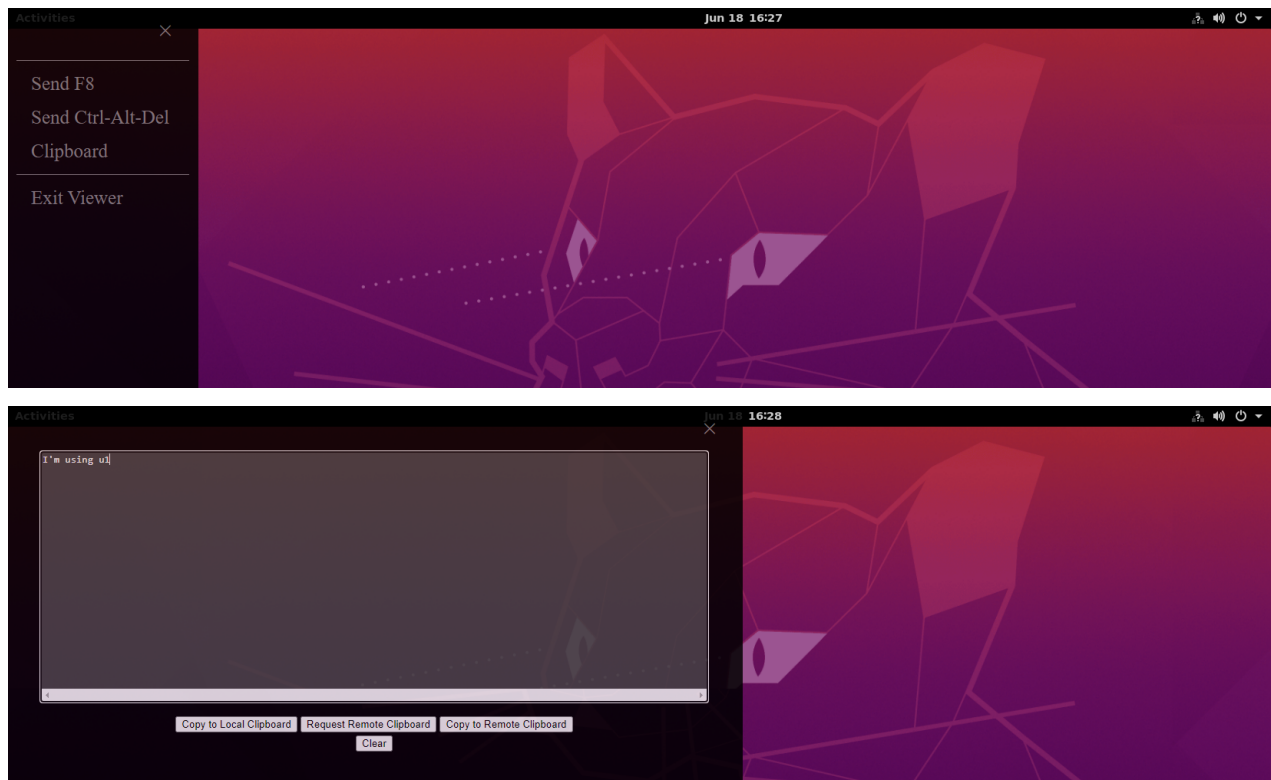
< Edit Bookmark

HTTP/HTTPS FTP RDP SSH
SMB/CIFS VNC Telnet
SFTP

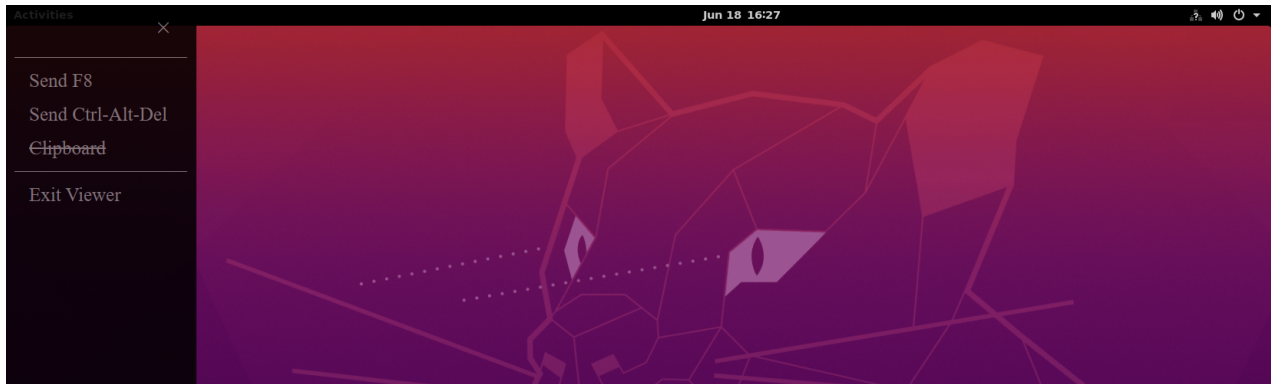
Name: RDP109
Host: 172.18.58.109
Port: 3389
Description:
Use SSL-VPN Credentials: ☒
Username: auto
Password:
Color Depth Per Pixel: 32bits per pixel.
Keyboard Layout: English, United States.
Security: Standard RDP encryption.
Send Preconnection ID: ☐
Load Balancing Information:
Restricted Admin Mode: ☒

Save Cancel

3. The clipboard is available and you can copy and paste content to and from the remote server.



4. Log out of the web portal, then log back in as user *u2* and access the internal server using RDP/VNC. The clipboard is disabled.



To configure the SSL-VPN portals and settings in the CLI:

1. Configure the SSL VPN portals:

```
config vpn ssl web portal
  edit "testportal1"
    set web-mode enable
    set clipboard enable
    ...
  next
  edit "testportal2"
    set web-mode enable
    set clipboard disable
    ...
  next
end
```

2. Configure the SSL VPN settings:

```
config vpn ssl settings
  set port 1443
  set source-interface "port2"
  set source-address "all"
  set source-address6 "all"
  set default-portal "tunnel-access"
  config authentication-rule
    edit 1
      set users "u1"
      set portal "testportal1"
    next
    edit 2
      set users "u2"
      set portal "testportal2"
    next
  end
end
```

3. Configure a firewall policy for SSL VPN:

```
config firewall policy
  edit 1
    set name "policy_to_sslvpn_tunnel"
    set srcintf "ssl.vdom1"
```

```

        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set users "u1" "u2"
    next
end

```

4. On the PC, open a web browser, log in to the web portal as user *u1*, access the internal server using RDP/VNC, and use the clipboard.
5. Check the SSL VPN session monitor:

```
# get vpn ssl monitor
```

SSL-VPN Login Users:

Index	User	Group	Auth Type	Timeout	Auth-Timeout	From	HTTP
in/out	HTTPS	in/out	Two-factor	Auth			
0	u1		1(1)	N/A	10.1.100.146	0/0	0/364 0

SSL-VPN sessions:

Index	User	Group	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	u1		10.1.100.146	64	0/700	RDP 172.18.58.109

6. On the PC, open a web browser, log in to the web portal as user *u2*, access the internal server using RDP/VNC, and note that the clipboard is not available.
7. Check the SSL VPN session monitor:

```
# get vpn ssl monitor
```

SSL-VPN Login Users:

Index	User	Group	Auth Type	Timeout	Auth-Timeout	From	HTTP
in/out	HTTPS	in/out	Two-factor	Auth			
0	u2		1(1)	N/A	10.1.100.146	0/0	0/2681 0

SSL-VPN sessions:

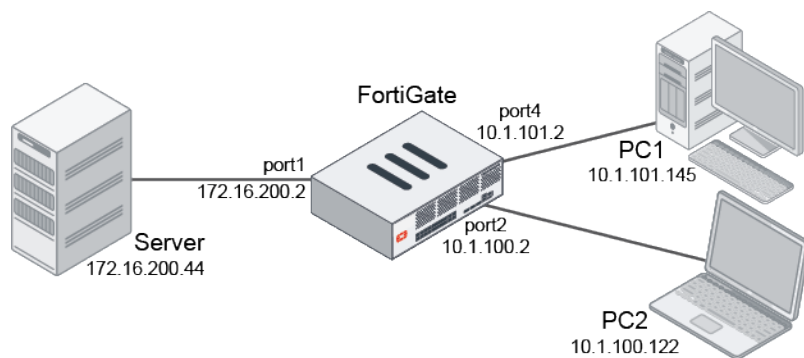
Index	User	Group	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	u2		10.1.100.146	7	0/553	RDP 172.18.58.109

Use SSL VPN interfaces in zones - 7.0.1

SSL VPN interfaces can be used in zones, simplifying firewall policy configuration in some scenarios.

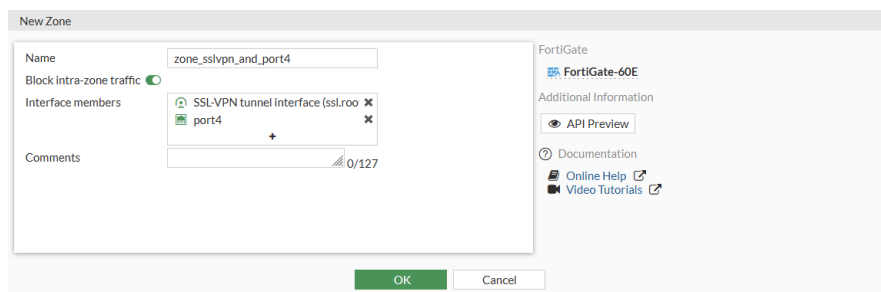
Example

In this example, a zone is created that includes a physical interface (port4) and an SSL VPN interface. The zone is used as the source interface in a firewall policy. PC1 is used for regular access with a firewall policy, and PC2 uses the SSL VPN for access.



To create a zone that includes the port4 and ssl.root interfaces in the GUI:

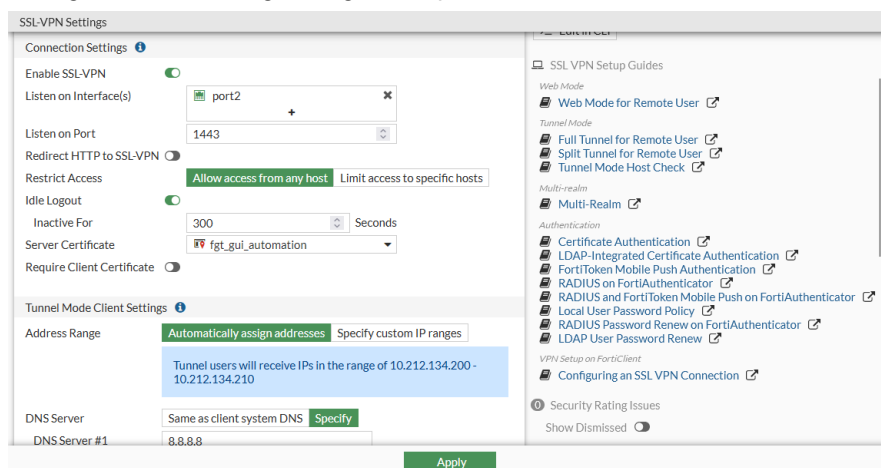
1. Go to *Network > Interfaces* and click *Create New > Zone*.
2. Set the name of the zone, such as *zone_sslvpn_and_port4*.
3. Add *port4* and *ssl.root* to the *Interface members*.



4. Click **OK**.

To configure SSL VPN settings in the GUI:

1. Go to *VPN > SSL-VPN Settings*.
2. Set *Listen on Interface(s)* to *port2*.
3. Set *Listen on Port* to *1443*.
4. Configure the remaining settings as required.



5. Click **Apply**.

To configure a firewall policy with the zone as the source interface in the GUI:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Set the policy name, such as *policy_to_sslvpn_tunnel*.
3. Set *Incoming Interface* to *zone_sslvpn_and_port4*.
4. Set *Outgoing Interface* to *port1*.
5. Configure the remaining settings as required.

6. Click **OK**.

To configure the zone, SSL VPN, and policy in the CLI:

1. Create a zone that includes the port4 and ssl.root interfaces:

```
config system zone
    edit "zone_sslvpn_and_port4"
        set interface "port4" "ssl.root"
    next
end
```

2. Configure SSL VPN settings with port2 as the source interface:

```
config vpn ssl settings
    set servercert "fgt_gui_automation"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set dns-server1 8.8.8.8
    set dns-server2 8.8.4.4
    set port 1443
    set source-interface "port2"
    set source-address "all"
    set source-address6 "all"
    set default-portal "web-access"
end
```

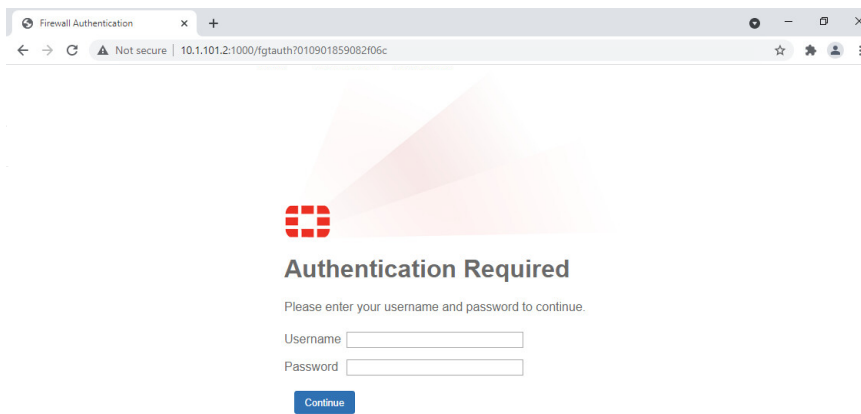
3. Configure a firewall policy with the zone as the source interface:

```
config firewall policy
    edit 2
        set name "policy_to_sslvpn_tunnel"
        set srcintf "zone_sslvpn_and_port4"
        set dstintf "port1"
```

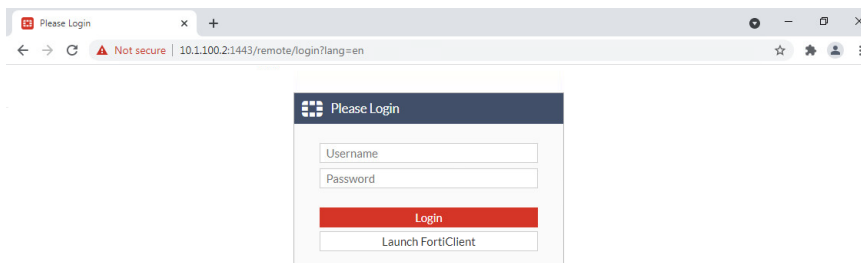
```
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set users "u1"
    next
end
```

To test the configuration:

1. On PC1, open a browser and try to access the server at 172.16.200.44.
You are redirected to the authentication page.

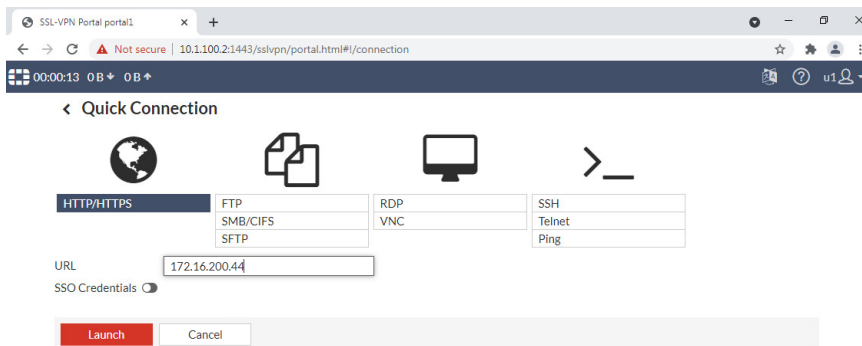


2. Enter the *Username* and *Password*, then click *Continue*.
You are redirected back to the server.
3. On PC2, access the SSL VPN web portal.



4. Enter the *Username* and *Password*, then click *Login*.

5. Access the server using the bookmark.



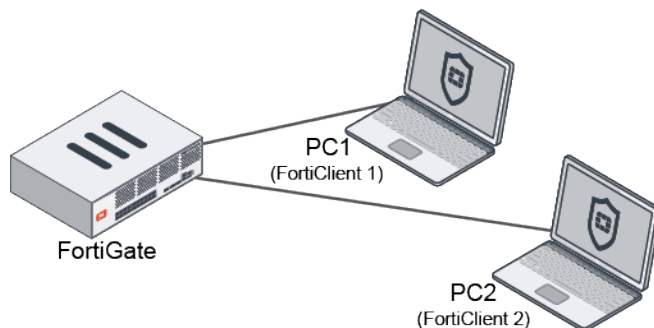
SSL VPN and IPsec VPN IP address assignments - 7.0.1

When a user disconnects from a VPN tunnel, it is not always desirable for the released IP address to be used immediately.

- In SSL VPN, IP addresses can be assigned from the pool in a round robin fashion, instead of the default first-available address method.
- In IPsec VPN, IP addresses can be held for the specified delay interval before being released back into the pool for assignment. The first-available address assignment method is still used.

Example topology

In these examples, two PCs connect to the VPN.



SSL VPN example

In this example, SSL VPN is configured to use round robin IP address assignment. Dual stack address assignment (both IPv4 and IPv6) is used.

After a tunnel is disconnected, freeing a low IP address, the next client that connects gets the next address in the round robin instead of the lowest address.

To configure SSL VPN with round robin and dual stack:**1. Create IPv4 and IPv6 address ranges:**

```
config firewall address
    edit "sslvpn_ipv4_pool"
        set type iprange
        set start-ip 173.10.1.1
        set end-ip 173.10.1.3
    next
end

config firewall address6
    edit "sslvpn_ipv6_pool"
        set type iprange
        set start-ip 2000::ad0a:101
        set end-ip 2000::ad0a:103
    next
end
```

2. Set the address ranges as IP pools in the SSL VPN settings:

```
config vpn ssl settings
    set tunnel-ip-pools "sslvpn_ipv4_pool"
    set tunnel-ipv6-pools "sslvpn_ipv6_pool"
end
```

When round-robin is used, any address pools defined in the web portal are ignored and the tunnel IPv4 and IPv6 pool addresses in the SSL VPN settings are used. Only one set of IP pool addresses can be applied.

3. Enable round-robin and dual stack in the SSL VPN settings:

```
config vpn ssl settings
    set dual-stack-mode enable
    set tunnel-addr-assigned-method round-robin
end
```

By default, the IP pool assignment follows the first available rule.

4. Create two users and assign them to an SSL VPN policy:

```
config user local
    edit "u1"
        set type password
        set passwd *****
    next
    edit "u2"
        set type password
        set passwd *****
    next
end

config firewall policy
    edit 1
        set name "sslvpnd"
        set srcintf "ssl.vdom1"
        set dstintf "link_11" "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
```

```

        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set users "u1" "u2"
    next
end

```

To test the results:

1. Log in to the SSL VPN on PC1 using user u1 and then check its assigned IP address:

```

# get vpn ssl monitor
SSL-VPN Login Users:
  Index  User  Group  Auth Type  Timeout  Auth-Timeout  From  HTTP
in/out  HTTPS in/out  Two-factor Auth
  0      u1           1(1)      N/A      10.1.100.145  0/0  0/0  0

SSL-VPN sessions:
  Index  User  Group  Source IP  Duration  I/O Bytes  Tunnel/Dest IP
  0      u1           10.1.100.145  13  49935/35251
173.10.1.1,2000::ad0a:101

```

2. Log in to the SSL VPN on PC1 using user u2 and then check its assigned IP address:

```

# get vpn ssl monitor
SSL-VPN Login Users:
  Index  User  Group  Auth Type  Timeout  Auth-Timeout  From  HTTP
in/out  HTTPS in/out  Two-factor Auth
  0      u1           1(1)      N/A      10.1.100.145  0/0  0/0  0
  1      u2           1(1)      N/A      10.1.100.254  0/0  0/0  0

SSL-VPN sessions:
  Index  User  Group  Source IP  Duration  I/O Bytes  Tunnel/Dest IP
  0      u1           10.1.100.145  44  90126/70405
173.10.1.1,2000::ad0a:101
  1      u2           10.1.100.254  10  10563/8158
173.10.1.2,2000::ad0a:102

```

3. Log user u1 off of PC1, then log them back in and check that the assigned IP address is not the same as was previously assigned:

```

# get vpn ssl monitor
SSL-VPN Login Users:
  Index  User  Group  Auth Type  Timeout  Auth-Timeout  From  HTTP
in/out  HTTPS in/out  Two-factor Auth
  0      u1           1(1)      N/A      10.1.100.145  0/0  0/0  0
  1      u2           1(1)      N/A      10.1.100.254  0/0  0/0  0

SSL-VPN sessions:
  Index  User  Group  Source IP  Duration  I/O Bytes  Tunnel/Dest IP
  0      u1           10.1.100.145  10  50992/41159
173.10.1.3,2000::ad0a:103
  1      u2           10.1.100.254  43  30374/21860
173.10.1.2,2000::ad0a:102

```

IPsec VPN example

In this example, the IP address reuse delay interval is used to prevent a released address from being reused for at least four minutes. After the interval elapses, the IP address becomes available to clients again. Dual stack address assignment (both IPv4 and IPv6) is used.

To configure IPsec VPN with an IP address reuse delay interval:

1. Configure the IPsec phase1 interface, setting the IP address reuse delay interval to 240 seconds:

```
config vpn ipsec phase1-interface
  edit "FCT"
    set type dynamic
    set interface "port27"
    set mode aggressive
    set peertype any
    set net-device disable
    set mode-cfg enable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set wizard-type dialup-forticlient
    set xauthtype auto
    set authusrgrp "local-group"
    set ipv4-start-ip 10.20.1.1
    set ipv4-end-ip 10.20.1.100
    set dns-mode auto
    set ipv4-split-include "FCT_split"
    set ipv6-start-ip 2001::1
    set ipv6-end-ip 2001::2
    set ip-delay-interval 240
    set save-password enable
    set psksecret *****
  next
end
```

2. Configure the IPsec phase2 interface:

```
config vpn ipsec phase2-interface
  edit "FCT"
    set phasename "FCT"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
    aes256gcm chacha20poly1305
  next
  edit "FCT6"
    set phasename "FCT"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
    aes256gcm chacha20poly1305
    set src-addr-type subnet6
    set dst-addr-type subnet6
  next
end
```

To test the results:

1. Connect to the VPN with FortiClient 1 on PC1 then check the assigned IP address:

```
# diagnose vpn ike gateway list

vd: root/0
name: FCT_0
version: 1
interface: port27 17
addr: 173.1.1.1:4500 -> 173.1.1.2:60417
tun_id: 173.1.1.2
remote_location: 0.0.0.0
virtual-interface-addr: 169.254.1.1 -> 169.254.1.1
created: 14s ago
xauth-user: userc
2FA: no
FortiClient UID: 7C0897D80C8E4B6DAC775DD6B0F93BAA
assigned IPv4 address: 10.20.1.1/255.255.255.255
assigned IPv6 address: 2001::1/128
nat: peer
IKE SA: created 1/1 established 1/1 time 100/100/100 ms
IPsec SA: created 2/2 established 2/2 time 0/5/10 ms

id/spi: 2 66140ba3e38b9b07/b64668f110ca4a48
direction: responder
status: established 14-14s ago = 100ms
proposal: aes256-sha256
key: 356637ee6e9a9cb5-fade432c09efb8aa-54be307fc1eeeab5-6e4b9ef19f98d5fa
lifetime/rekey: 86400/86115
DPD sent/recvd: 00000000/00000394
```

2. Disconnect FortiClient 1 and connect with FortiClient 2. The IP address assigned to FortiClient 1 is not released to the pool, and a different IP address is assigned to FortiClient 2:

```
# diagnose vpn ike gateway list

vd: root/0
name: FCT_0
version: 1
interface: port27 17
addr: 173.1.1.1:4500 -> 173.1.1.2:64916
tun_id: 173.1.1.2
remote_location: 0.0.0.0
virtual-interface-addr: 169.254.1.1 -> 169.254.1.1
created: 6s ago
xauth-user: usera
2FA: no
FortiClient UID: EAF90E297393456AB546A041066C0720
assigned IPv4 address: 10.20.1.2/255.255.255.255
assigned IPv6 address: 2001::2/128
nat: peer
IKE SA: created 1/1 established 1/1 time 110/110/110 ms
IPsec SA: created 2/2 established 2/2 time 0/5/10 ms

id/spi: 3 b25141d5a915e67e/b32decdb8cf98318
direction: responder
```

```

status: established 6-6s ago = 110ms
proposal: aes256-sha256
key: 374ab753f3207ea0-83496b5cb24b5a8d-c51da1fd505cf3a4-727884839897808a
lifetime/rekey: 86400/86123
DPD sent/recvd: 00000000/00000453

```

3. Wait for 240 seconds, then disconnect and reconnect FortiClient 2. The IP address previously assigned to FortiClient 1 has been released back to the pool, and is assigned to FortiClient 2:

```

# diagnose vpn ike gateway list

vd: root/0
name: FCT_0
version: 1
interface: port27 17
addr: 173.1.1.1:4500 -> 173.1.1.2:64916
tun_id: 173.1.1.2
remote_location: 0.0.0.0
virtual-interface-addr: 169.254.1.1 -> 169.254.1.1
created: 20s ago
xauth-user: usera
2FA: no
FortiClient UID: EAF90E297393456AB546A041066C0720
assigned IPv4 address: 10.20.1.1/255.255.255.255
assigned IPv6 address: 2001::1/128
nat: peer
IKE SA: created 1/1 established 1/1 time 100/100/100 ms
IPsec SA: created 2/2 established 2/2 time 0/0/0 ms

id/spi: 4 fb1fbad0c12f5476/aa06a2de76964f63
direction: responder
status: established 20-20s ago = 100ms
proposal: aes256-sha256
key: af43f1bb876dc79c-16448592fe608dc3-f251746d71b2c35d-c848e8c03bf738e9
lifetime/rekey: 86400/86109
DPD sent/recvd: 00000000/000000a9

```



Instead of waiting for 240 seconds, you can instead use the `diagnose vpn ike gateway flush` command to release the previously used IP addresses back into the pool.

Dedicated tunnel ID for IPsec tunnels - 7.0.1

The IPsec kernel now uses dedicated tunnel IDs as identifiers for each tunnel.

Routes are linked to the tunnels by the tunnel IDs, replacing the need to have a route tree in the IPsec tunnel list for selecting tunnels by next hop when net-device is disabled. Consequently, the tunnel search option in phase1 removed, because tunnels are now clearly identified by the tunnel ID and referenced in the routing table.

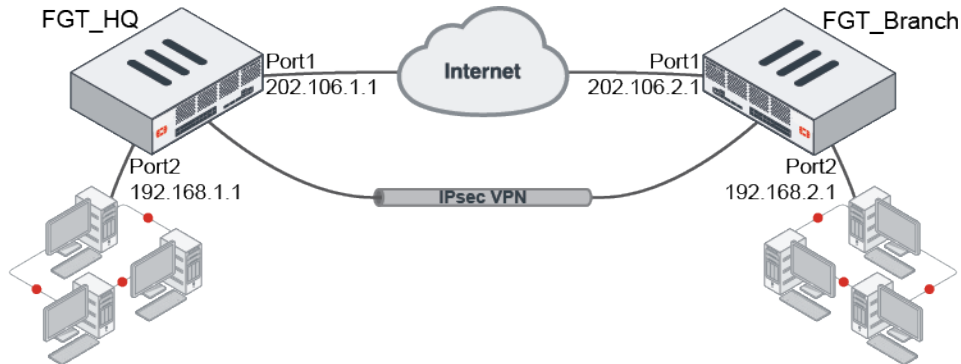
In general, tunnel IDs are assigned the IP address of the remote gateway. If multiple tunnels use the same gateway IP address, then a random IP address from the subnet 10.0.0.0/8 is assigned.

The IPsec kernel design change has also changed the routing table output, as seen in the following examples:

- [Example 1: Static site to site VPN with static routing on page 488](#)
- [Example 2: Static site to site VPN with dynamic routing on page 491](#)
- [Example 3: Dynamic dial-up VPN with mode-cfg on page 496](#)

Example 1: Static site to site VPN with static routing

In this example, two sites are connected by a site-to-site IPsec VPN.



To configure IPsec on the FGT_HQ:

```
config vpn ipsec phase1-interface
  edit "hq-vpn"
    set interface "port1"
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set dpd on-idle
    set remote-gw 202.106.2.1
    set psksecret <secret>
  next
end

config vpn ipsec phase2-interface
  edit "hq-vpn"
    set phase1name "hq-vpn"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
    chacha20poly1305
    set auto-negotiate enable
  next
end

config router static
  edit 2
    set dst 192.168.2.0 255.255.255.0
    set device "hq-vpn"
  next
end
```

To configure IPsec on the FGT_Branch:

```
config vpn ipsec phase1-interface
  edit "branch-vpn"
```

```

        set interface "port1"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 202.106.1.1
        set psksecret <secret>
    next
end

config vpn ipsec phase2-interface
    edit "branch-vpn"
        set phasename "branch-vpn"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
        set auto-negotiate enable
    next
end

config router static
    edit 2
        set dst 192.168.1.0 255.255.255.0
        set device "branch-vpn"
    next
end

```

To compare the debug and routing table output between 7.0.1 and 6.4.7:

7.0.1	6.4.7
<pre> # diagnose vpn ike gateway list vd: root/0 name: hq-vpn version: 1 interface: port1 3 addr: 202.106.1.1:500 -> 202.106.2.1:500 tun_id: 202.106.2.1 remote_location: 0.0.0.0 created: 740s ago IKE SA: created 1/1 established 1/1 time 0/0/0 ms IPsec SA: created 1/1 established 1/1 time 0/0/0 ms id/spi: 0 d2c4a8cff4cb24ac/5344ca7ec529dbcd direction: initiator status: established 740-740s ago = 0ms proposal: aes128-sha256 key: c0a6eb7bdae7fd4a-a86ff7a09b8216b0 lifetime/rekey: 86400/85359 DPD sent/recv: 0000000c/0000005a </pre>	<pre> # diagnose vpn ike gateway list vd: root/0 name: hq-vpn version: 1 interface: port1 3 addr: 202.106.1.1:500 -> 202.106.2.1:500 created: 1026s ago IKE SA: created 1/2 established 1/1 time 10/10/10 ms IPsec SA: created 2/2 established 1/1 time 0/0/0 ms id/spi: 3 abf61a9364796569/e4f7a35227b039bd direction: responder status: established 1001-1001s ago = 10ms proposal: aes128-sha256 key: 85b316cc2242f0ae-95eaf5d3d38ab83c lifetime/rekey: 86400/85128 DPD sent/recv: 00000000/00000031 No tunnel ID is listed. </pre>

7.0.1

The output lists the tunnel ID that is associated with the remote gateway in the site-to-site IPsec tunnel.

```
# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=hq-vpn ver=1 serial=1 202.106.1.1:0-
>202.106.2.1:0 tun_id=202.106.2.1 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0
weight=1
bound_if=3 lgwy=static/1 tun=intf/0
mode=auto/1 encap=none/512 options
[0200]=frag-rfc run_state=0 accept_
traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=3
olast=3 ad=/0
stat: rxb=0 txp=0 rxp=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3
count=0 seqno=13
natt: mode=none draft=0 interval=0 remote_
port=0
proxyid=hq-vpn proto=0 sa=1 ref=2 serial=1
auto-negotiate
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=38203 type=00 soft=0
mtu=1438 expire=42185/0B replaywin=2048
  seqno=1 esn=0 replaywin_
lastseq=00000000 itn=0 qat=0 hash_search_
len=1
  life: type=01 bytes=0/0
timeout=42930/43200
  dec: spi=83fc537f esp=aes key=16
be77c39ca8255d551d51a0c2207c40ff
  ah=sha1 key=20
6734e315495cd2399a3eb3b1bf2cbb7fd086b777
  enc: spi=5a32b74b esp=aes key=16
94bd1250fdfdbd32bd4f52f491671f4f
  ah=sha1 key=20
7edc2b28b9b4cb48f2b6e74212bed74a67efb4fb
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
run_tally=0
```

```
# get router info routing-table all
Codes: K - kernel, C - connected, S -
static, R - RIP, B - BGP
```

6.4.7

```
# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=hq-vpn ver=1 serial=2 202.106.1.1:0-
>202.106.2.1:0 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0
mode=auto/1 encap=none/512 options
[0200]=frag-rfc run_state=0 accept_
traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=12 ilast=6
olast=6 ad=/0
stat: rxb=0 txp=0 rxp=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3
count=0 seqno=50
natt: mode=none draft=0 interval=0 remote_
port=0
proxyid=hq-vpn proto=0 sa=1 ref=2 serial=1
auto-negotiate
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=38203 type=00 soft=0
mtu=1438 expire=41889/0B replaywin=2048
  seqno=1 esn=0 replaywin_
lastseq=00000000 itn=0 qat=0 hash_search_
len=1
  life: type=01 bytes=0/0
timeout=42897/43200
  dec: spi=13721bed esp=aes key=16
2fbf85f8c19ee1699196e2a05fd8dfbf
  ah=sha1 key=20
6910afbf9bea9e72cc0647af9e2f78dfe0312db4
  enc: spi=5a32b74a esp=aes key=16
b52e9ac4ccdf4998d1a7f3c6e4bc7368
  ah=sha1 key=20
6bda8e5e442ddce0214f418e56b2eab5b3517c49
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
run_tally=1
```

```
# get router info routing-table all
Codes: K - kernel, C - connected, S -
static, R - RIP, B - BGP
```


7.0.1

O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default

Routing table for VRF=0

```
S* 0.0.0.0/0 [10/0] via 202.106.1.254, port1
C 192.168.1.0/24 is directly connected, port2
S 192.168.2.0/24 [10/0] via hq-vpn tunnel 202.106.2.1
C 202.106.1.0/24 is directly connected, port1
```

The remote network is routable through the next hop corresponding to the hq-vpn tunnel with tunnel ID 202.106.2.1.

6.4.7

O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default

Routing table for VRF=0

```
S* 0.0.0.0/0 [10/0] via 202.106.1.254, port1
C 192.168.1.0/24 is directly connected, port2
S 192.168.2.0/24 [10/0] is directly connected, hq-vpn
C 202.106.1.0/24 is directly connected, port1
```

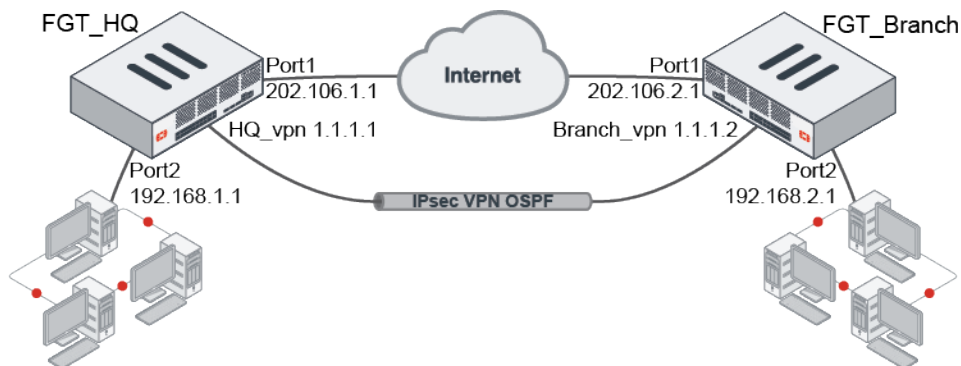
The remote network is shown as directly connected.



Although the remote gateway can be used as the tunnel ID, it does not equate to the actual IP of the next hop when it appears in the routing table.

Example 2: Static site to site VPN with dynamic routing

In this example, two sites are connected by a site-to-site IPsec VPN and routing is implemented using OSPF.



To configure IPsec on the FGT_HQ:

```
config vpn ipsec phase1-interface
edit "hq-vpn"
```

```
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 202.106.2.1
        set psksecret <secret>
    next
end

config vpn ipsec phase2-interface
    edit "hq-vpn"
        set phaselname "hq-vpn"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
        set auto-negotiate enable
    next
end

config system interface
    edit "hq-vpn"
        set vdom "root"
        set ip 1.1.1.1 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 1.1.1.2 255.255.255.0
        set interface "port1"
    next
end

config router ospf
    set router-id 1.1.1.1
    config area
        edit 0.0.0.0
    next
end

config ospf-interface
    edit "hq-vpn"
        set interface "hq-vpn"
        set mtu-ignore enable
        set network-type point-to-point
    next
end

config network
    edit 1
        set prefix 1.1.1.0 255.255.255.0
    next
    edit 2
        set prefix 192.168.1.0 255.255.255.0
    next
end
end
```

To configure IPsec on the FGT_Branch:

```
config vpn ipsec phase1-interface
    edit "branch-vpn"
```

```
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 202.106.1.1
        set psksecret <secret>
    next
end

config vpn ipsec phase2-interface
    edit "branch-vpn"
        set phasename "branch-vpn"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
        set auto-negotiate enable
    next
end

config system interface
    edit "branch-vpn"
        set vdom "root"
        set ip 1.1.1.2 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 1.1.1.1 255.255.255.0
        set interface "port1"
    next
end

config router ospf
    set router-id 1.1.1.2
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "branch-vpn"
            set interface "branch-vpn"
            set mtu-ignore enable
            set network-type point-to-point
        next
    end
    config network
        edit 1
            set prefix 1.1.1.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```

To compare the debug and routing table output between 7.0.1 and 6.4.7:

7.0.1	6.4.7
<pre># diagnose vpn ike gateway list vd: root/0 name: hq-vpn version: 1 interface: port1 3 addr: 202.106.1.1:500 -> 202.106.2.1:500 tun_id: 202.106.2.1 remote_location: 0.0.0.0 virtual-interface-addr: 1.1.1.1 -> 1.1.1.2 created: 119s ago IKE SA: created 1/1 established 1/1 time 0/0/0 ms IPsec SA: created 1/1 established 1/1 time 0/0/0 ms id/spi: 0 3ff498dd0a456fc9/9278ce9982a2e19a direction: initiator status: established 119-119s ago = 0ms proposal: aes128-sha256 key: fafdecf0c15fee4d-0c03b09f437517bd lifetime/rekey: 86400/85980 DPD sent/recv: 00000000/00000000</pre> <p>The output lists the tunnel ID that is associated with the remote gateway in the site-to-site IPsec tunnel.</p>	<pre># diagnose vpn ike gateway list vd: root/0 name: hq-vpn version: 1 interface: port1 3 addr: 202.106.1.1:500 -> 202.106.2.1:500 virtual-interface-addr: 1.1.1.1 -> 1.1.1.2 created: 800s ago IKE SA: created 1/1 established 1/1 time 0/0/0 ms IPsec SA: created 1/1 established 1/1 time 0/0/0 ms id/spi: 0 3758c158569e3d79/47b6c55c18b72213 direction: initiator status: established 800-800s ago = 0ms proposal: aes128-sha256 key: 01d2e21717f05a84-434ab868d0ff37db lifetime/rekey: 86400/85299 DPD sent/recv: 00000000/00000000</pre> <p>No tunnel ID is listed.</p>
<pre># diagnose vpn tunnel list list all ipsec tunnel in vd 0 ----- name=hq-vpn ver=1 serial=1 202.106.1.1:0- >202.106.2.1:0 tun_id=202.106.2.1 dst_ mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1 bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/512 options [0200]=frag-rfc run_state=0 accept_ traffic=1 overlay_id=0 proxyid_num=1 child_num=0 refcnt=6 ilast=4 olast=4 ad=/0 stat: rxp=24 txp=28 rxb=3328 txb=1934 dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=0</pre>	<pre># diagnose vpn tunnel list list all ipsec tunnel in vd 0 ----- name=hq-vpn ver=1 serial=1 202.106.1.1:0- >202.106.2.1:0 dst_mtu=1500 bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/512 options [0200]=frag-rfc run_state=0 accept_ traffic=1 overlay_id=0 proxyid_num=1 child_num=0 refcnt=17 ilast=5 olast=4 ad=/0 stat: rxp=124 txp=125 rxb=16672 txb=8343 dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=0 natt: mode=none draft=0 interval=0 remote_</pre>

7.0.1

```
natt: mode=none draft=0 interval=0 remote_
port=0
proxyid=hq-vpn proto=0 sa=1 ref=6 serial=1
auto-negotiate
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=38203 type=00 soft=0
mtu=1438 expire=42808/0B replaywin=2048
  seqno=1d esn=0 replaywin_
lastseq=00000019 itn=0 qat=0 hash_search_
len=1
  life: type=01 bytes=0/0
timeout=42932/43200
  dec: spi=ffdf028f esp=aes key=16
c7008f0d5592bf0e3471e68d930fe12c
  ah=sha1 key=20
c65b1d158a69c5735ea68e257d4b792aa92c3669
  enc: spi=5a32b750 esp=aes key=16
4c3fb9452d7a7d7c15e139b0327f23ad
  ah=sha1 key=20
clad92d290c96393c43e8db9f56b5b35e5835c2b
  dec:pkts/bytes=24/1708,
enc:pkts/bytes=28/3808
run_tally=0
```

```
# get router info routing-table all
Codes: K - kernel, C - connected, S -
static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF
external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 -
IS-IS level-2, ia - IS-IS inter area
      * - candidate default
```

```
Routing table for VRF=0
S*    0.0.0.0/0 [10/0] via 202.106.1.254,
port1
S    1.1.1.0/24 [5/0] via hq-vpn tunnel
202.106.2.1
C    1.1.1.1/32 is directly connected,
hq-vpn
C     192.168.1.0/24 is directly
connected, port2
O    192.168.2.0/24 [110/101] via hq-vpn
```

6.4.7

```
port=0
proxyid=hq-vpn proto=0 sa=1 ref=5 serial=1
auto-negotiate
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=38203 type=00 soft=0
mtu=1438 expire=42128/0B replaywin=2048
  seqno=7e esn=0 replaywin_
lastseq=0000007d itn=0 qat=0 hash_search_
len=1
  life: type=01 bytes=0/0
timeout=42932/43200
  dec: spi=1374fc07 esp=aes key=16
33634bc564af960d809be9e78962dc30
  ah=sha1 key=20
7342c18b7aad274f81c4773bbd8065eb77adf064
  enc: spi=5a32b74f esp=aes key=16
1a6c88078b3efab4e33bala421d1cc4
  ah=sha1 key=20
31621fa9cd466d23ef5a04ec20d896d4b746b2ed
  dec:pkts/bytes=124/8289,
enc:pkts/bytes=125/16760
run_tally=1
```

```
# get router info routing-table all
Codes: K - kernel, C - connected, S -
static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF
external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 -
IS-IS level-2, ia - IS-IS inter area
      * - candidate default
```

```
Routing table for VRF=0
S*    0.0.0.0/0 [10/0] via 202.106.1.254,
port1
C    1.1.1.0/24 is directly connected,
hq-vpn
C    1.1.1.1/32 is directly connected,
hq-vpn
C     192.168.1.0/24 is directly
connected, port2
O    192.168.2.0/24 [110/101] via
```

7.0.1

tunnel 202.106.2.1, 00:01:23

C 202.106.1.0/24 is directly connected, port1

The remote virtual tunnel interface is one hop away.
The OSPF route has the next hop of the hq-vpn tunnel with tunnel ID 202.106.2.1.

6.4.7

1.1.1.2, hq-vpn, 00:09:28

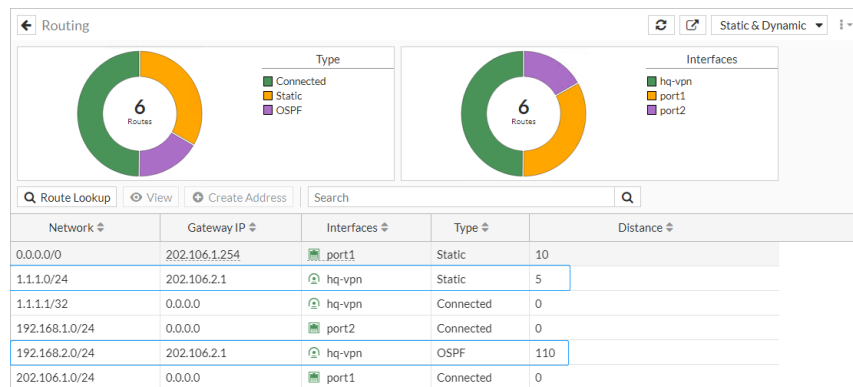
C 202.106.1.0/24 is directly connected, port1

Both the local and remote virtual tunnel interface IP addresses and subnets are directly connected.
The route learned from OSPF has a next hop through the remote virtual tunnel interface IP address, over the hq-vpn tunnel.

In the GUI, go to *Dashboard > Network* and expand the Routing widget to see the routing table:

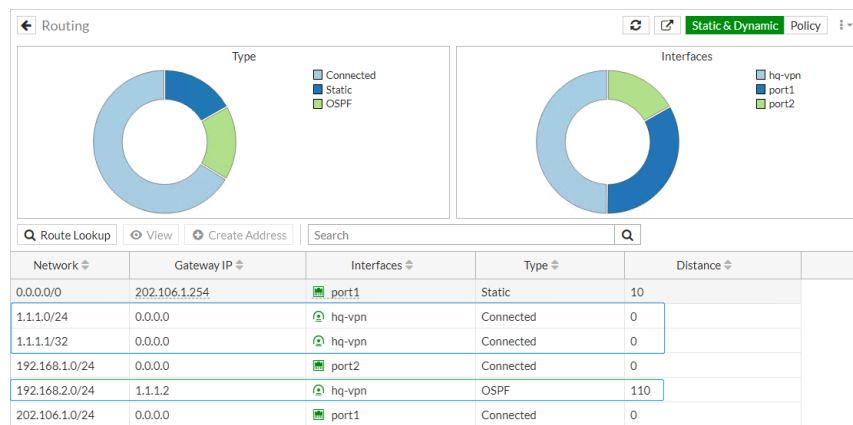
7.0.1:

The gateway IP address shows the tunnel ID.



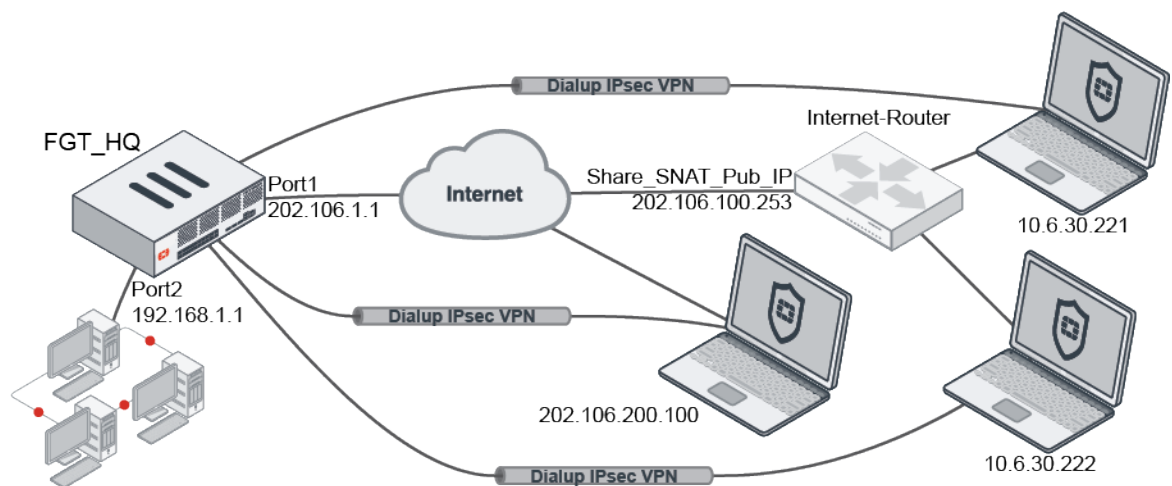
6.4.7:

The next hop is the hq-vpn, and the gateway IP address is the remote IP address 1.1.1.2.



Example 3: Dynamic dial-up VPN with mode-cfg

In this example, the HQ-FGT is the dial-up tunnel server. The remote clients include an endpoint with a public IP address, and two endpoints that are behind NAT.



The clients are connected through FortiClient VPN:

- 7.0.1

Client	Tunnel name	Assigned IP Address
user1 - 10.6.30.221 (NAT'd to 202.106.100.253)	Dia_0	10.212.1.100
user3 - 202.106.200.100	Dia_1	10.212.1.102
user2 - 10.6.30.222 (NAT'd to 202.106.100.253)	Dia_2	10.212.1.101

- 6.4.7

Client	Tunnel name	Assigned IP Address
user1 - 10.6.30.221 (NAT'd to 202.106.100.253)	Dia_0	10.212.1.100
user2 - 10.6.30.222 (NAT'd to 202.106.100.253)	Dia_1	10.212.1.101
user3 - 202.106.200.100	Dia_2	10.212.1.102

To configure IPsec on the FGT_HQ:

```
config vpn ipsec phase1-interface
edit "Dia"
    set type dynamic
    set interface "port1"
    set mode aggressive
    set peertype any
    set net-device disable
    set mode-cfg enable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set comments "VPN: Dia (Created by VPN wizard)"
    set wizard-type dialup-forticlient
    set xauthtype auto
```

```

        set authusrgrp "Guest-group"
        set ipv4-start-ip 10.212.1.100
        set ipv4-end-ip 10.212.1.200
        set ipv4-netmask 255.255.255.0
        set dns-mode auto
        set ipv4-split-include "Dia_split"
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret <secret>
    next
end

config vpn ipsec phase2-interface
    edit "Dia"
        set phaselname "Dia"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
        set comments "VPN: Dia (Created by VPN wizard)"
    next
end

```

To compare the debug and routing table output between 7.0.1 and 6.4.7:

7.0.1	6.4.7
<pre> # diagnose vpn ike gateway list vd: root/0 name: Dia_0 version: 1 interface: port1 3 addr: 202.106.1.1:4500 -> 202.106.100.253:4500 tun_id: 202.106.100.253 remote_location: 0.0.0.0 created: 373s ago xauth-user: user1 2FA: no FortiClient UID: D09AAEEE825945DBA3D41F89D1016AA3 assigned IPv4 address: 10.212.1.100/255.255.255.0 nat: peer IKE SA: created 1/1 established 1/1 time 110/110/110 ms IPsec SA: created 1/1 established 1/1 time 0/0/0 ms ... </pre>	<pre> # diagnose vpn ike gateway list vd: root/0 name: Dia_1 version: 1 interface: port1 3 addr: 202.106.1.1:4500 -> 202.106.100.253:1024 created: 247s ago xauth-user: user2 FortiClient UID: 288E34633A3C4716A55C32C42EEF1E0D assigned IPv4 address: 10.212.1.101/255.255.255.0 nat: peer IKE SA: created 1/1 established 1/1 time 10/10/10 ms IPsec SA: created 1/1 established 1/1 time 0/0/0 ms ... vd: root/0 name: Dia_0 version: 1 </pre>

7.0.1

```

vd: root/0
name: Dia_1
version: 1
interface: port1 3
addr: 202.106.1.1:500 -> 202.106.200.100:500
tun_id: 202.106.200.100
remote_location: 0.0.0.0
created: 342s ago
xauth-user: user3
2FA: no
FortiClient UID:
5911723955D74B86879F4F0EBB254082
assigned IPv4 address:
10.212.1.101/255.255.255.0
IKE SA: created 1/1 established 1/1 time
1220/1220/1220 ms
IPsec SA: created 1/1 established 1/1 time
1700/1700/1700 ms
...
vd: root/0
name: Dia_2
version: 1
interface: port1 3
addr: 202.106.1.1:4500 ->
202.106.100.253:1025
tun_id: 10.0.0.2
remote_location: 0.0.0.0
created: 78s ago
xauth-user: user2
2FA: no
FortiClient UID:
288E34633A3C4716A55C32C42EEF1E0D
assigned IPv4 address:
10.212.1.102/255.255.255.0
nat: peer
IKE SA: created 1/1 established 1/1 time
0/0/0 ms
IPsec SA: created 1/1 established 1/1 time
0/0/0 ms
...

```

The output lists the tunnel ID that is associated with each dial-up tunnel. When there is a conflict, the FortiGate uses an address from the 10.0.0.0/8 subnet as the `tun_id`.

6.4.7

```

interface: port1 3
addr: 202.106.1.1:4500 ->
202.106.100.253:4500
created: 237s ago
xauth-user: user1
FortiClient UID:
D09AAEEE825945DBA3D41F89D1016AA3
assigned IPv4 address:
10.212.1.100/255.255.255.0
nat: peer
IKE SA: created 1/1 established 1/1 time
120/120/120 ms
IPsec SA: created 1/1 established 1/1 time
0/0/0 ms
...
vd: root/0
name: Dia_2
version: 1
interface: port1 3
addr: 202.106.1.1:500 -> 202.106.200.100:500
created: 214s ago
xauth-user: user3
FortiClient UID:
5911723955D74B86879F4F0EBB254082
assigned IPv4 address:
10.212.1.102/255.255.255.0
IKE SA: created 1/1 established 1/1 time
1230/1230/1230 ms
IPsec SA: created 1/1 established 1/1 time
1710/1710/1710 ms
...

```

No tunnel ID is listed. The route tree is used to look up the tunnel for routing.

7.0.1

```
# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
-----
name=Dia_0 ver=1 serial=2 202.106.1.1:4500-
>202.106.100.253:4500 tun_id=202.106.100.253
dst_mtu=1500 dpd-link=on remote_
location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0
mode=dial_inst/3 encap=none/896 options
[0380]=rgwy-chg rport-chg frag-rfc run_
state=0 accept_traffic=1 overlay_id=0
parent=Dia index=0
...
-----
-----
name=Dia_1 ver=1 serial=3 202.106.1.1:0-
>202.106.200.100:0 tun_id=202.106.200.100
dst_mtu=0 dpd-link=on remote_
location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0
mode=dial_inst/3 encap=none/640 options
[0280]=rgwy-chg frag-rfc run_state=0
accept_traffic=1 overlay_id=0
parent=Dia index=1
...
-----
-----
name=Dia_2 ver=1 serial=4 202.106.1.1:4500-
>202.106.100.253:1025 tun_id=10.0.0.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0
weight=1
bound_if=3 lgwy=static/1 tun=intf/0
mode=dial_inst/3 encap=none/896 options
[0380]=rgwy-chg rport-chg frag-rfc run_
state=0 accept_traffic=1 overlay_id=0
parent=Dia index=2
...
-----
-----
name=Dia ver=1 serial=1 202.106.1.1:0-
>0.0.0.0:0 tun_id=10.0.0.1 dst_mtu=0 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0
mode=dialup/2 encap=none/512 options
[0200]=frag-rfc accept_traffic=1 overlay_
```

6.4.7

```
# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
-----
name=Dia ver=1 serial=1 202.106.1.1:0-
>0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0
mode=dialup/2 encap=none/512 options
[0200]=frag-rfc accept_traffic=1 overlay_
id=0

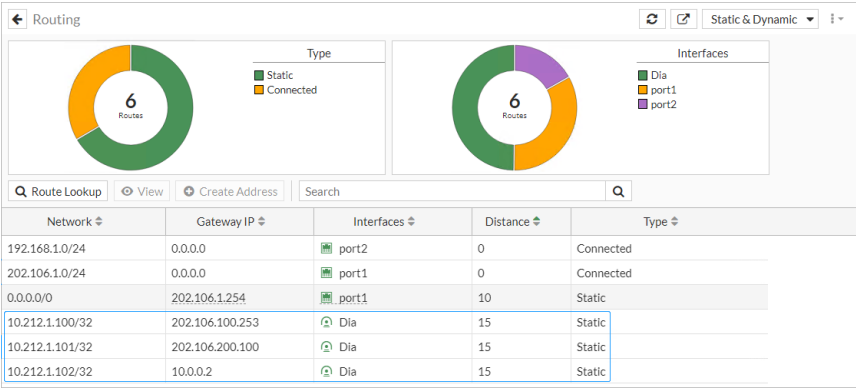
proxyid_num=0 child_num=3 refcnt=18
ilast=981 olast=981 ad=/0
stat: rxp=2639 txp=353 rxb=3378568
txb=3147348
dpd: mode=on-demand on=0 idle=20000ms
retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_
port=0
run_tally=3
ipv4 route tree:
10.212.1.100->10.212.1.100 0
10.212.1.101->10.212.1.101 1
10.212.1.102->10.212.1.102 2
-----
-----
name=Dia_0 ver=1 serial=5 202.106.1.1:4500-
>202.106.100.253:4500 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0
mode=dial_inst/3 encap=none/896 options
[0380]=rgwy-chg rport-chg frag-rfc run_
state=1 accept_traffic=1 overlay_id=0
parent=Dia index=0
...
-----
-----
name=Dia_1 ver=1 serial=4 202.106.1.1:4500-
>202.106.100.253:1024 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0
mode=dial_inst/3 encap=none/896 options
[0380]=rgwy-chg rport-chg frag-rfc run_
state=1 accept_traffic=1 overlay_id=0
parent=Dia index=1
...
```

7.0.1	6.4.7
<pre>id=0 proxyid_num=0 child_num=3 refcnt=5 ilast=560 olast=560 ad=/0 stat: rxp=667 txp=88 rxb=804272 txb=740428 dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0 natt: mode=none draft=0 interval=0 remote_ port=0 run_tally=0 # get router info routing-table all Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default Routing table for VRF=0 S* 0.0.0.0/0 [10/0] via 202.106.1.254, port1 S 10.212.1.100/32 [15/0] via Dia tunnel 202.106.100.253 S 10.212.1.101/32 [15/0] via Dia tunnel 202.106.200.100 S 10.212.1.102/32 [15/0] via Dia tunnel 10.0.0.2 C 192.168.1.0/24 is directly connected, port2 C 202.106.1.0/24 is directly connected, port1 The parent tunnel and tunnel ID are shown as the next hop, which uniquely identifies the tunnel that is being referenced.</pre>	<pre>----- ----- name=Dia_2 ver=1 serial=6 202.106.1.1:0- >202.106.200.100:0 dst_mtu=0 bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/640 options [0280]=rgwy-chg frag-rfc run_state=1 accept_traffic=1 overlay_id=0 parent=Dia index=2 # get router info routing-table all Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default Routing table for VRF=0 S* 0.0.0.0/0 [10/0] via 202.106.1.254, port1 S 10.212.1.100/32 [15/0] via 202.106.100.253, Dia S 10.212.1.101/32 [15/0] via 202.106.100.253, Dia S 10.212.1.102/32 [15/0] via 202.106.200.100, Dia C 192.168.1.0/24 is directly connected, port2 C 202.106.1.0/24 is directly connected, port1 The remote IP address and parent tunnel are shown as the next hop, but when two devices are behind NAT, the actual tunnel must be matched by looking up the route tree.</pre>

In the GUI, go to *Dashboard > Network* and expand the Routing widget to see the routing table:

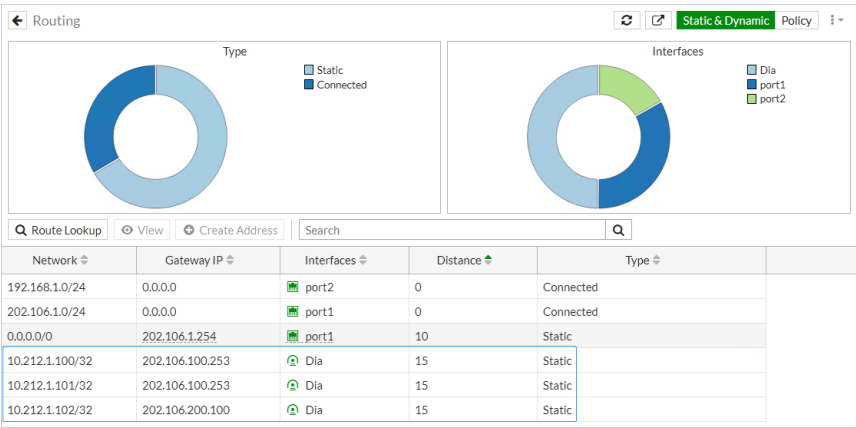
7.0.1:

The gateway IP address shows the tunnel ID.



6.4.7:

The next hop is Dia, and the gateway IP address is the remote IP address.



User and authentication

This section includes information about user and authentication related new features:

- [Authentication on page 503](#)

Authentication

This section includes information about authentication related new features:

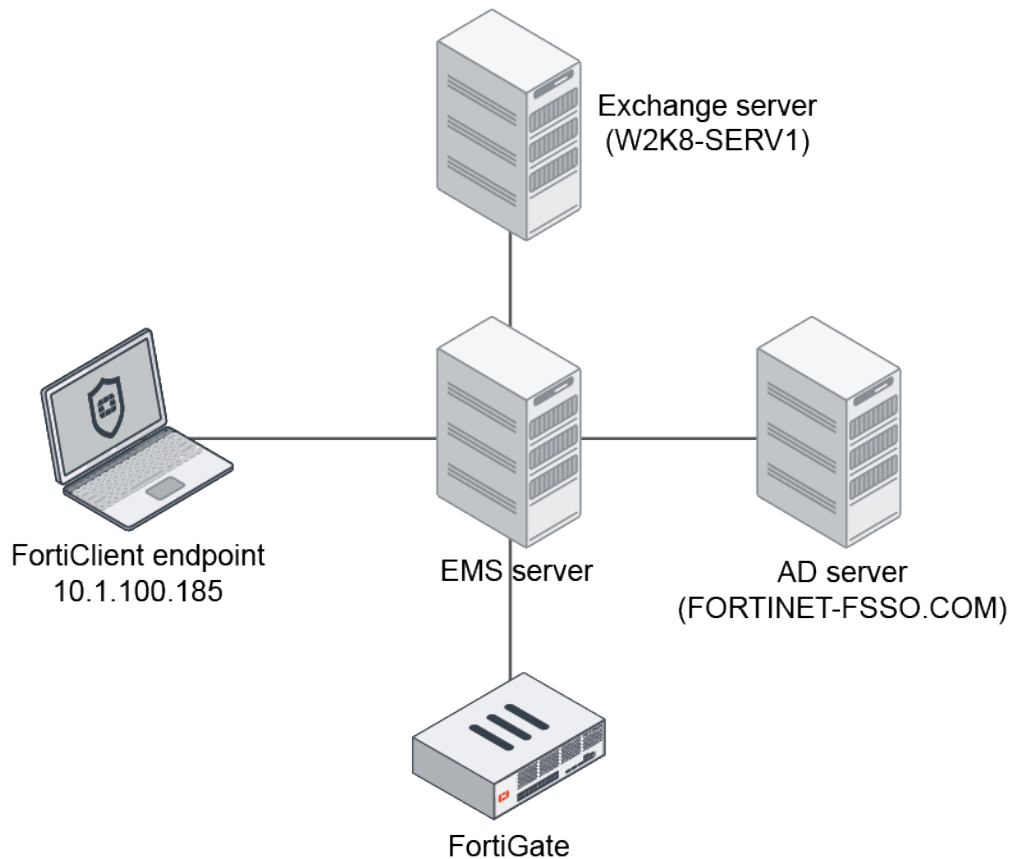
- [Integrate user information from EMS connector and Exchange connector in the user store on page 503](#)
- [SAML authentication in a proxy policy on page 506](#)
- [Improve FortiToken Cloud visibility 7.0.1 on page 510](#)
- [Use a browser as an external user-agent for SAML authentication in an SSL VPN connection 7.0.1 on page 511](#)
- [Add configurable FSSO timeout when connection to collector agent fails 7.0.1 on page 515](#)
- [Track users in each Active Directory LDAP group 7.0.2 on page 517](#)
- [Configuring SAML SSO in the GUI 7.0.2 on page 520](#)

Integrate user information from EMS connector and Exchange connector in the user store

When a FortiClient endpoint is managed by EMS, logged in user and domain information is shared with FortiOS through the EMS connector. This information can be joined with the Exchange connector to produce more complete user information in the user store.

The `diagnose user-device-store device memory list` command displays detailed device information.

Sample topology



In this example, the FortiClient PC user (test1) logs on to the AD domain (FORTINET-FSSO.COM), which is also the same domain as the Exchange server. The user information is pushed to the EMS server that the user is registered to. The FortiGate synchronizes the information from EMS, and at the same time looks up the user on the Exchange server under the Exchange connector. If the user exists on the Exchange server, additional information is fetched. These details are combined in the user store, which is visible in the *FortiClient* widget in the *Status* dashboard.

To configure the Exchange server:

```
config user exchange
  edit "exchange-140"
    set server-name "W2K8-SERV1"
    set domain-name "FORTINET-FSSO.COM"
    set username "Administrator"
    set password "*****"
  next
end
```

To configure the EMS server:

```
config endpoint-control fctems
  edit "ems133"
    set server "172.18.62.12"
    set certificate-fingerprint "4F:A6:76:E2:00:4F:A6:76:E2:00:4F:A6:76:E2:00:E0"
```

```
    next
end
```

To view the user information in the GUI:

1. Go to *Dashboard > Status*.
2. In the *FortiClient* widget, hover over a device or user name to view the information.

To view the user information in the CLI:

```
# diagnose user-device-store device memory list
...
Record #13:
    device_info
        'ipv4_address' = '10.1.100.185'
        'mac' = '00:0c:29:11:5b:6b'
        'hardware_vendor' = 'VMware'
        'vdom' = 'root'
        'os_name' = 'Microsoft'
        'os_version' = 'Windows 7 Professional Edition, 32-bit Service Pack 1
(build 7601)'
        'hostname' = 'win7-5'
        'unauth_user' = 'Administrator'
        'last_seen' = '1611356490'
        'host_src' = 'forticlient'
        'user_info_src' = 'forticlient'
        'is_forticlient_endpoint' = 'true'
        'unjoined_forticlient_endpoint' = 'false'
        'is_forticlient_unauth_user' = 'true'
        'avatar_source' = 'OS'
        'domain' = 'Fortinet-FSSO.COM'
        'forticlient_id' = '*****'
        'forticlient_username' = 'Administrator'
        'forticlient_version' = '6.4.2'
        'on_net' = 'true'
        'quarantined_on_forticlient' = 'false'
        'vuln_count' = '0'
        'vuln_count_critical' = '0'
        'vuln_count_high' = '0'
        'vuln_count_info' = '0'
        'vuln_count_low' = '0'
        'vuln_count_medium' = '0'
        'is_online' = 'true'
    interface_info
        'ipv4_address' = '10.1.100.185'
        'mac' = '00:0c:29:11:5b:6b'
        'master_mac' = '00:0c:29:11:5b:6b'
        'detected_interface' = 'port10'
        'last_seen' = '1611356490'
        'is_master_device' = 'true'
        'is_detected_interface_role_wan' = 'false'
        'detected_interface_fortitelemetry' = 'true'
        'forticlient_gateway_interface' = 'port10'
        'on_net' = 'true'
        'is_online' = 'true'
```

SAML authentication in a proxy policy

SAML user authentication is supported for explicit web proxies and transparent web proxies with the FortiGate acting as a SAML SP. SAML is supported as a new authentication method for an authentication scheme that requires using a captive portal.

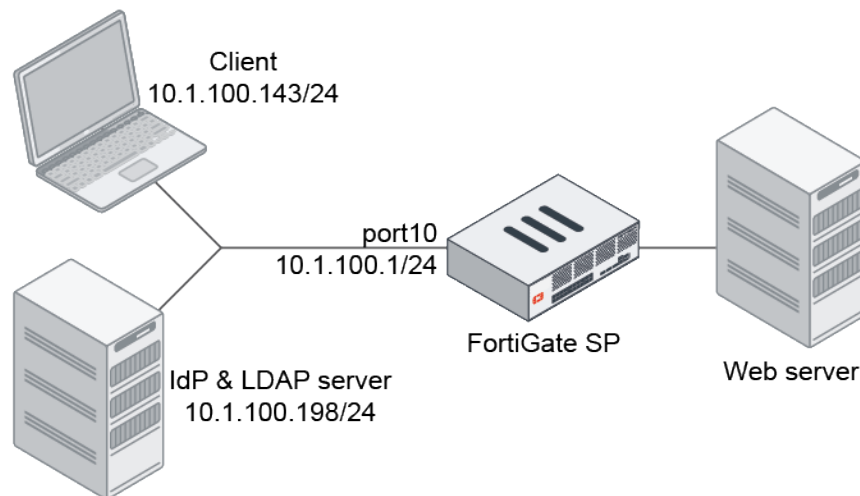
```
config authentication scheme
  edit <name>
    set method saml
    set saml-server <server>
    set saml-timeout <seconds>
    set user-database <database>
  next
end
```

In the SAML user settings, two digest methods are supported for its certificate signing algorithms.

```
config user saml
  edit <name>
    set digest-method {sha1 | sha256}
  next
end
```

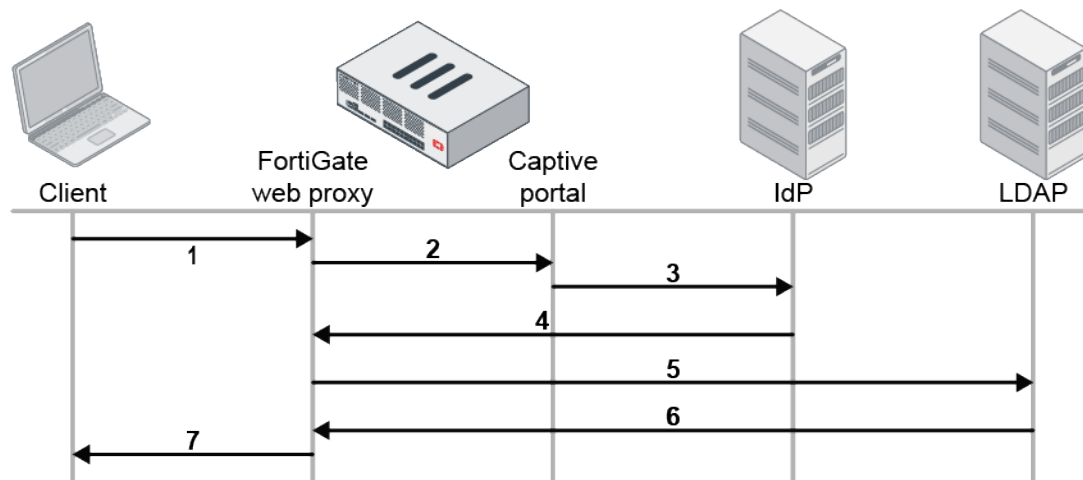
By default, the `digest-method` is set to `sha1`. For applications requiring SHA256, set the `digest-method` to `sha256`.

Topology



In this configuration, SAML authentication is used with an explicit web proxy. The IdP is a Windows 2016 server configured with ADFS. The LDAP and IdP servers are on the same server. The LDAP server is used as the user backend for the IdP to perform authentication; however, they are not required to be on the same server.

The authentication and authorization flow is as follows:



1. The client opens a browser and visits <https://www.google.com>.
2. The browser is redirected by the web proxy the captive portal.
3. The request is redirected to the IdP's sign-in page.
4. If the user signs in, the IdP authenticates the user and sends back a SAML assertion message to the FortiGate with the user group information.
5. If the FortiGate authentication scheme has a user database configured, the FortiGate will query the LDAP server for the user group information and ignore the user group information from the SAML message.
6. The user group information is returned. The FortiGate matches the user group information against the LDAP group in the proxy policy group settings. If there is a match, the request is authorized and the proxy policy is matched.
7. If all policy criteria match successfully, then the webpage is returned to the client.

To configure SAML authentication with an explicit web proxy:

1. Enable the web proxy:

```
config web-proxy explicit
    set status enable
    set http-incoming-port 8080
end
```

2. Enable the proxy captive portal:

```
config system interface
    edit "port10"
        set vdom "vdom1"
        set ip 10.1.100.1 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
        set type physical
        set explicit-web-proxy enable
        set explicit-ftp-proxy enable
        set proxy-captive-portal enable
        set snmp-index 12
    next
end
```

3. Configure the LDAP server:

```
config user ldap
    edit "ldap-10.1.100.198"
```

```
        set server "10.1.100.198"
        set cnid "cn"
        set dn "dc=myqalab,dc=local"
        set type regular
        set username "cn=fosqal,cn=users,dc=myqalab,dc=local"
        set password *****
        set group-search-base "dc=myqalab,dc=local"
    next
end
```

4. Configure the user group:

```
config user group
    edit "ldap-group-saml"
        set member "ldap-10.1.100.198"
    next
end
```

5. Configure SAML:

```
config user saml
    edit "saml_user"
        set cert "Fortinet_CA_SSL"
        set entity-id "https://fgt9.myqalab.local:7831/XX/YY/ZZ/saml/metadata/"
        set single-sign-on-url "https://fgt9.myqalab.local:7831/XX/YY/ZZ/saml/login/"
        set single-logout-url "https://fgt9.myqalab.local:7831/XX/YY/ZZ/saml/logout/"
        set idp-entity-id "http://MYQALAB.LOCAL/adfs/services/trust"
        set idp-single-sign-on-url "https://myqalab.local/adfs/ls"
        set idp-single-logout-url "https://myqalab.local/adfs/ls"
        set idp-cert "REMOTE_Cert_4"
        set digest-method sha256
        set adfs-claim enable
        set user-claim-type name
        set group-claim-type group
    next
end
```

6. Configure the authentication scheme, rule, and setting:

```
config authentication scheme
    edit "saml"
        set method saml
        set saml-server "saml_user"
        set user-database "ldap-10.1.100.198"
    next
end

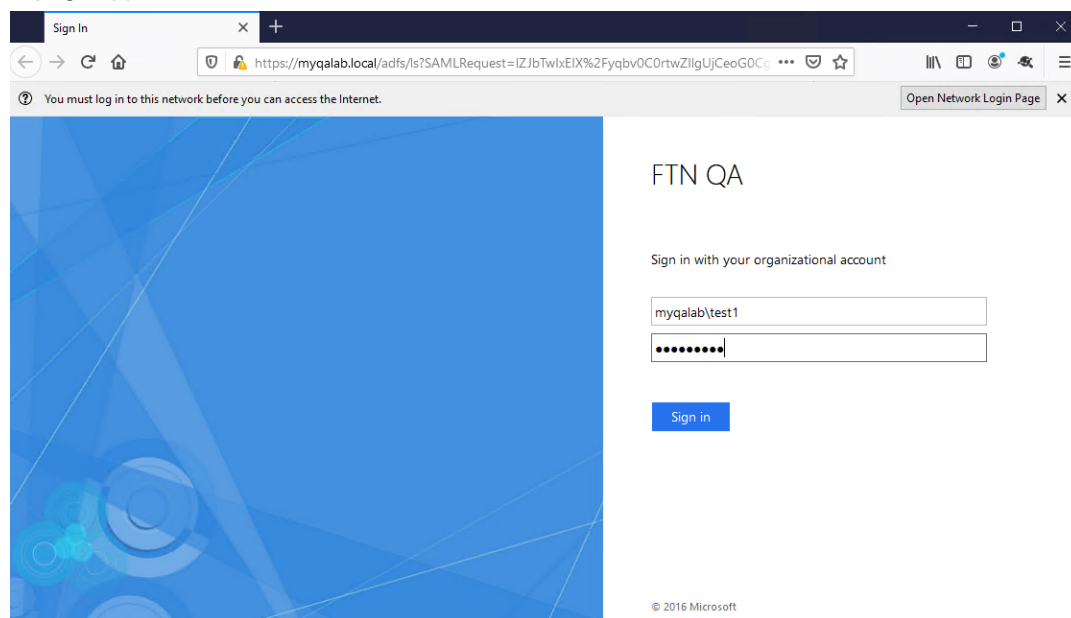
config authentication rule
    edit "saml"
        set srcaddr "all"
        set active-auth-method "saml"
    next
end

config authentication setting
    set captive-portal "fgt9.myqalab.local"
end
```

7. Configure the proxy policy:

```
config firewall proxy-policy
  edit 3
    set proxy explicit-web
    set dstintf "port9"
    set srcaddr "all"
    set dstaddr "all"
    set service "webproxy"
    set action accept
    set schedule "always"
    set logtraffic all
    set groups "ldap-group-saml"
    set utm-status enable
    set profile-protocol-options "protocol"
    set ssl-ssh-profile "deep-custom"
    set av-profile "av"
  next
end
```

When a user goes to www.google.com in a browser that is configured to use the FortiGate as a proxy, the IdP sign-in page appears.



Sample log

```
7: date=2021-03-16 time=21:11:19 eventtime=1615954279072391030 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="vdom1" srcip=10.1.100.143 srcport=53544
srcintf="port10" srcintfrole="undefined" dstcountry="United States" srccountry="Reserved"
dstip=173.194.219.99 dstport=443 dstintf="port9" dstintfrole="undefined"
sessionid=1751272387 service="HTTPS" wanoptapptype="web-proxy" proto=6 action="accept"
policyid=3 policytype="proxy-policy" poluuid="052ae158-7d40-51eb-c1d8-19235c4500c2"
trandisp="snat" transip=172.16.200.1 transport=14844 duration=268 user="test1@MYQALAB.local"
group="ldap-group-saml" authserver="ldap-10.1.100.198" wanin=345633 rcvdbyte=345633
wanout=13013 lanin=5098 sentbyte=5098 lanout=340778 appcat="unscanned"
```

Improve FortiToken Cloud visibility - 7.0.1

A FortiToken Cloud license can now be purchased through FortiExplorer. Customers can download FortiExplorer to acquire or renew a FortiToken Cloud license. The FortiOS GUI has been enhanced to help customers easily download the FortiExplorer app. Clear warning messages indicate if there is no FortiToken Cloud subscription, or if the subscription is expired. The default token type when enabling two-factor authentication is now FortiToken Cloud.

To download FortiExplorer through the FortiOS GUI:

1. Go to *User & Authentication > User Definition* or *System > Administrators*.
2. Create a new user or administrator, or edit an existing entry.
3. In the right-side gutter *FortiExplorer* section, click *Get the app* or hover over the link to scan the QR code.

You are redirected to a page where you can download FortiExplorer.

Sample warning messages

If the user does not have a FortiToken Cloud license, the message includes a link to download a trial subscription:

If the FortiToken Cloud license is expired, the message includes a link to download FortiExplorer to renew the FortiToken Cloud subscription:

The screenshot shows the 'Users/Groups Creation Wizard' with the 'Contact Info' step selected. Under 'Two-factor Authentication', 'FortiToken Cloud' is chosen. A yellow warning box states: 'No active FortiToken Cloud subscription. Please renew from our partners, or directly through the FortiExplorer app.' A QR code is displayed next to the warning. Below the warning, there is an 'Email Address' input field and an 'SMS' toggle switch. On the right side, there is a sidebar with links for 'FortiExplorer', 'Documentation', 'Online Help', and 'Video Tutorials'. At the bottom, there are '< Back', 'Next', and 'Cancel' buttons.

If the maximum number of FortiToken Cloud users is reached, a warning is displayed:

The screenshot shows the 'Users/Groups Creation Wizard' with the 'Contact Info' step selected. Under 'Two-factor Authentication', 'FortiToken Cloud' is chosen. A yellow warning box states: 'The maximum number of FortiToken Cloud users has been reached.' Below the warning, there is an 'Email Address' input field and an 'SMS' toggle switch. On the right side, there is a sidebar with links for 'FortiExplorer', 'Documentation', 'Online Help', and 'Video Tutorials'. At the bottom, there are '< Back', 'Next', and 'Cancel' buttons.

Use a browser as an external user-agent for SAML authentication in an SSL VPN connection - 7.0.1

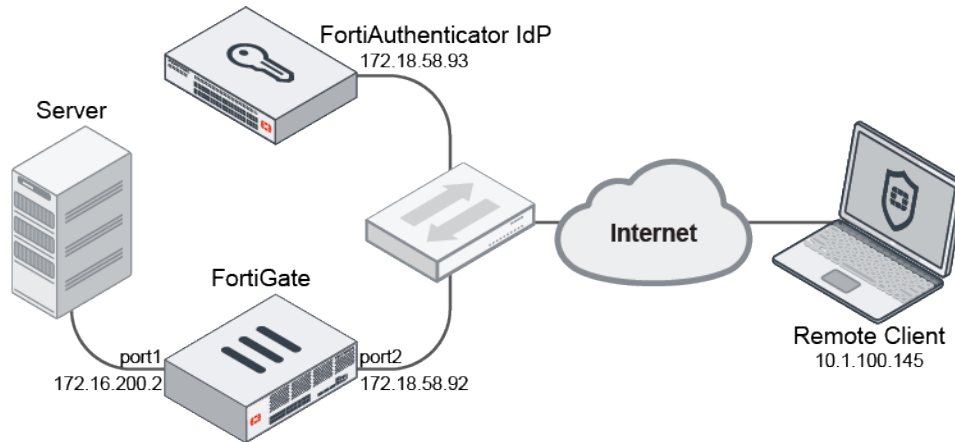
FortiClient can use a browser as an external user-agent to perform SAML authentication for SSL VPN tunnel mode, instead of the FortiClient embedded log in window. If a user has already done SAML authentication in the default browser, they do not need to authenticate again in the FortiClient built-in browser. FortiClient 7.0.1 is required.

The following CLI is used to set the SAML local redirect port on the FortiClient endpoint after successful SAML authentication:

```
config vpn ssl settings
    set saml-redirect-port <port>
end
```

Example

In this example, a user wants to use their default browser to connect to IdP for SAML authentication, without needing to separately authenticate in the FortiClient built-in browser. After authenticating in the browser, FortiClient obtains the authentication cookie directly from the browser.



The authentication process proceeds as follows:

1. The remote client uses FortiClient to connect to the FortiGate SSL VPN on 172.16.58.92:1443 with the *Use external browser as user-agent for saml user authentication* option enabled.
2. The SSL VPN redirects FortiClient to complete SAML authentication using the Identity Provider (IdP).
3. FortiClient opens the default browser to authenticate the IdP server.
4. After a successful authentication, the browser redirects to localhost:<port>, where the port is defined by the `saml-redirect-port` variable on the FortiGate.
5. FortiClient reads the authentication ID passed by the successful authentication, then requests that the SAML authentication process continues on the FortiGate with this ID.
6. The FortiGate continues with the remaining SSL-VPN host-check and other steps until it receives the authentication cookie. It then allow the SSL VPN user to connect using tunnel mode.

To configure the VPN:

1. Configure a SAML user:

```

config user saml
  edit "sul"
    set cert "fgt_gui_automation"
    set entity-id "http://172.18.58.92:1443/remote/saml/metadata/"
    set single-sign-on-url "https://172.18.58.92:1443/remote/saml/login/"
    set single-logout-url "https://172.18.58.92:1443/remote/saml/logout/"
    set idp-entity-id "http://172.18.58.93:443/saml-idp/222222/metadata/"
    set idp-single-sign-on-url "https://172.18.58.93:443/saml-idp/222222/login/"
    set idp-single-logout-url "https://172.18.58.93:443/saml-idp/222222/logout/"
    set idp-cert "REMOTE_Cert_1"
    set user-name "Username"
    set group-name "Groupname"
    set digest-method sha1
  next
end

```

2. Add the SAML user to a user group:

```
config user group
    edit "saml_grp"
        set member "sul"
    next
end
```

3. Create an SSL VPN web portal:

```
config vpn ssl web portal
    edit "testportal1"
        set tunnel-mode enable
        set ipv6-tunnel-mode enable
        set web-mode enable
        ...
    next
end
```

4. Configure the SSL VPN:

```
config vpn ssl settings
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 1443
    set source-interface "port2"
    set source-address "all"
    set source-address6 "all"
    set default-portal "testportal1"
    ...
end
```

5. Configure a firewall policy for the SSL VPN and assign the SAML group and a local user to it:

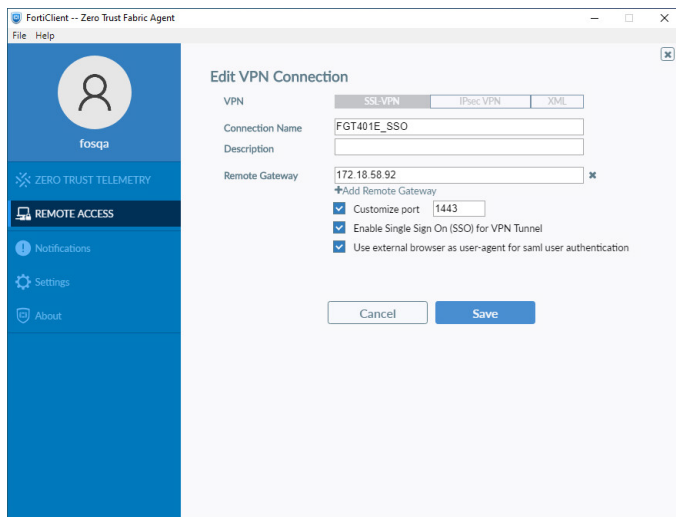
```
config firewall policy
    edit 1
        set name "policy_to_sslvpn_tunnel"
        set srcintf "ssl.root"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set groups "saml_grp"
        set users "u1"
    next
end
```

6. Enable the SAML redirect port:

```
config vpn ssl settings
    set saml-redirect-port 8020
end
```

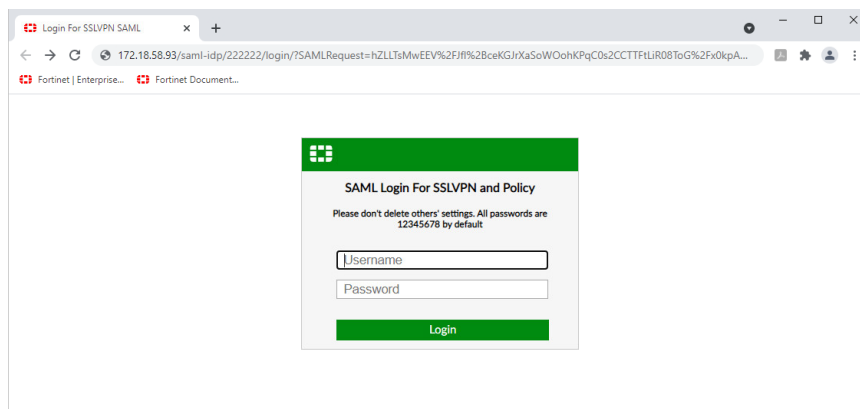
To connect to the VPN using FortiClient:

1. Configure the SSL VPN connection:
 - a. Open FortiClient and go to the *Remote Access* tab and click *Configure VPN*.
 - b. Enter a name for the connection.
 - c. Set the *Remote Gateway* to the FortiGate port 172.18.58.92.
 - d. Enable *Customize port* and set the port to 1443.
 - e. Enable *Enable Single Sign On (SSO) for VPN Tunnel* and *Use external browser as user-agent for saml user authentication*.



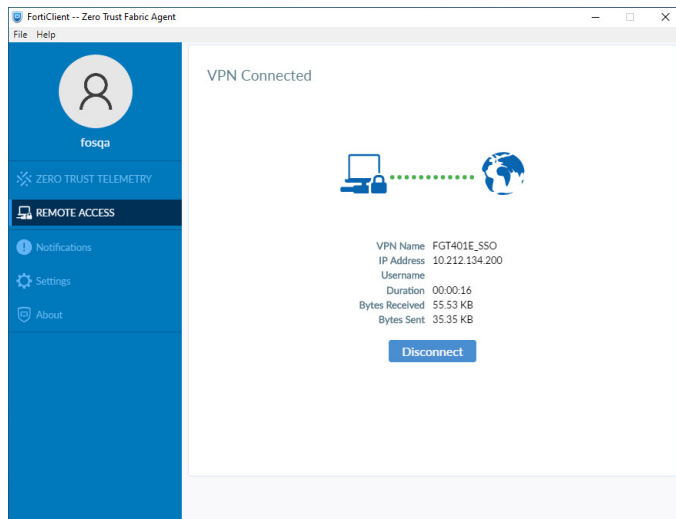
- f. Click *Save*.
2. On the *Remote Access* tab select the *FGT401E_SSO* VPN connection from the dropdown list.
3. Click *SAML Login*.

The default browser opens to the IdP authentication page.



4. Enter the username and password, then click *Login*.

The authenticated result is sent back to FortiClient and the connection is established.



To check the connection on the FortiGate:

```
# get vpn ssl monitor
```

SSL-VPN Login Users:

Index	User	Group	Auth Type	Timeout	Auth-Timeout	From	HTTP in/out
	HTTPS in/out	Two-factor	Auth				
1	fac3	saml_grp	256(1)	N/A	10.1.100.254	0/0	0/0 0

SSL-VPN sessions:

Index	User	Group	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	fac3	saml_grp	10.1.100.254	5	9990/8449	
10.212.134.200, fdff:ffff::1						

```
# diagnose firewall auth list
```

```
10.212.134.200, fac3
  type: fw, id: 0, duration: 6, idled: 0
  expire: 259199, allow-idle: 259200
  flag(80): sslvpn
  server: sul
  packets: in 28 out 28, bytes: in 23042 out 8561
  group_id: 5
  group_name: saml_grp
```

Add configurable FSSO timeout when connection to collector agent fails - 7.0.1

The `logon-timeout` option is used to manage how long authenticated FSSO users on the FortiGate will remain on the list of authenticated FSSO users when a network connection to the collector agent is lost.

```
config user fsso
  edit <name>
    set server <string>
    set password <string>
    set logon-timeout <integer>
```

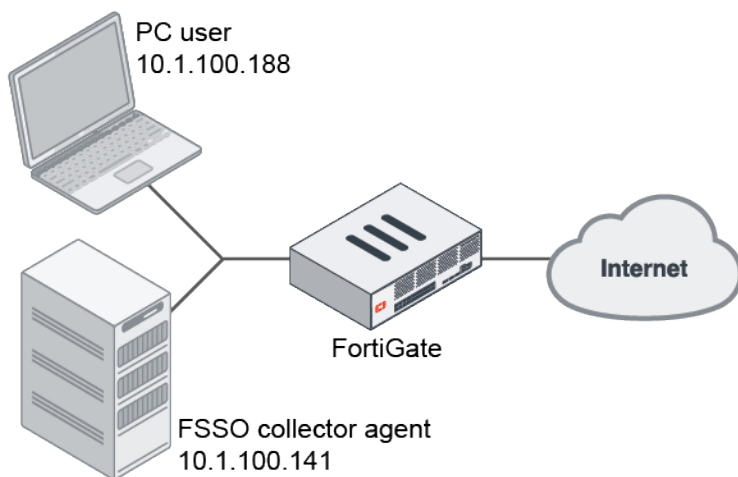
```

next
end

```

<code>logon-timeout <integer></code>	Enter the interval to keep logons after the FSSO server is down, in minutes (1 - 2880, default = 5).
--	--

Example



In this example, the logon timeout is set for four minutes.

To configure the FSSO logon timeout:

1. Set the timeout value:

```

config user fsso
  edit "ad"
    set server "10.1.100.141"
    set password *****
    set logon-timeout 4
  next
end

```

2. Log on to a PC with a valid FSSO user account.

3. Enable real-time debugging and check for authd polling collector agent information. During this time, the connection to the collector agent is lost:

```

# diagnose debug enable
# diagnose debug application authd -1
# diagnose debug application fssod -1
2021-06-10 16:20:41 authd_timer_run: 2 expired
2021-06-10 16:20:41 authd_epoll_work: timeout 39970
2021-06-10 16:20:46 fsae_io_ctx_process_msg[ad]: received heartbeat 100031
2021-06-10 16:20:46 authd_epoll_work: timeout 1690
2021-06-10 16:20:47 authd_timer_run: 1 expired
2021-06-10 16:20:47 authd_epoll_work: timeout 39990
2021-06-10 16:20:56 fsae_io_ctx_process_msg[ad]: received heartbeat 100032
2021-06-10 16:20:56 authd_epoll_work: timeout 31550
2021-06-10 16:21:00 _event_error[ad]: error occurred in epoll_in: Success
2021-06-10 16:21:00 disconnect_server_only[ad]: disconnecting

```

```
2021-06-10 16:21:00 authd_timer_run: 1 expired
2021-06-10 16:21:00 authd_epoll_work: timeout 9620
```

4. After about three minutes, check that the FSSO user is still in the list of authenticated users and can connect to the internet:

```
# diagnose firewall auth 1
10.1.100.188, TEST1
    type: fssso, id: 0, duration: 229, idled: 229
    server: ad
    packets: in 0 out 0, bytes: in 0 out 0
    user_id: 16777219
    group_id: 3 33554433
    group_name: ad CN=GROUP1,OU=TESTING,DC=FORTINET-FSSO,DC=COM

----- 1 listed, 0 filtered -----
```

5. After four minutes, check the debugs again. Note that the FSSO users are cleared:

```
...
2021-06-10 16:24:57 authd_timer_run: 3 expired
2021-06-10 16:24:57 authd_epoll_work: timeout 60000
2021-06-10 16:24:59 [fsae_db_logoff:248]: vfid 0, ip 10.1.100.188, id(0), port_range_sz
(0)
2021-06-10 16:24:59 [authd_fp_notify_logoff:444]: vfid 0, ip 10.1.100.188, id 0
2021-06-10 16:24:59 [authd_fp_on_user_logoff:412]: vfid 0, ip 10.1.100.188
2021-06-10 16:24:59 [authd_fp_on_user_logoff:412]: vfid 0, ip 10.1.100.188
2021-06-10 16:24:59 [authd_fp_on_user_logoff:412]: vfid 0, ip 10.1.100.188
2021-06-10 16:24:59 [authd_fpc_on_msg:545]: code 0, type 132, len 28 seq 0
2021-06-10 16:24:59 [authd_fp_on_user_logoff:412]: vfid 0, ip 10.1.100.188
2021-06-10 16:24:59 authd_epoll_work: timeout 21990

# diagnose firewall auth 1

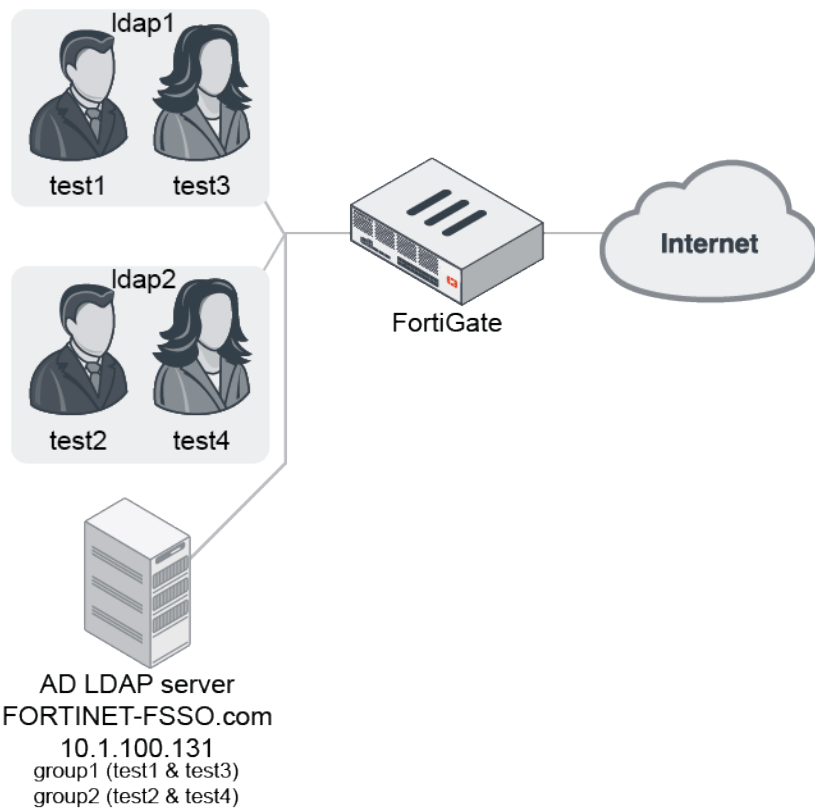
----- 0 listed, 0 filtered -----
```

After the connection to the collector agent is restored, all users remain in the list of authenticated users and are synchronized to the FortiGate. The users do not need to log in again for authentication.

Track users in each Active Directory LDAP group - 7.0.2

When LDAP users log on through firewall authentication, the active users per Active Directory LDAP group is counted and displayed in the *Firewall Users* widget and the CLI.

Example



The Active Directory LDAP server, FORTINET-FSSO.com, is configured with two groups that contain two users each: group1 consists of users test1 and test3; group2 consists of users test2 and test4.

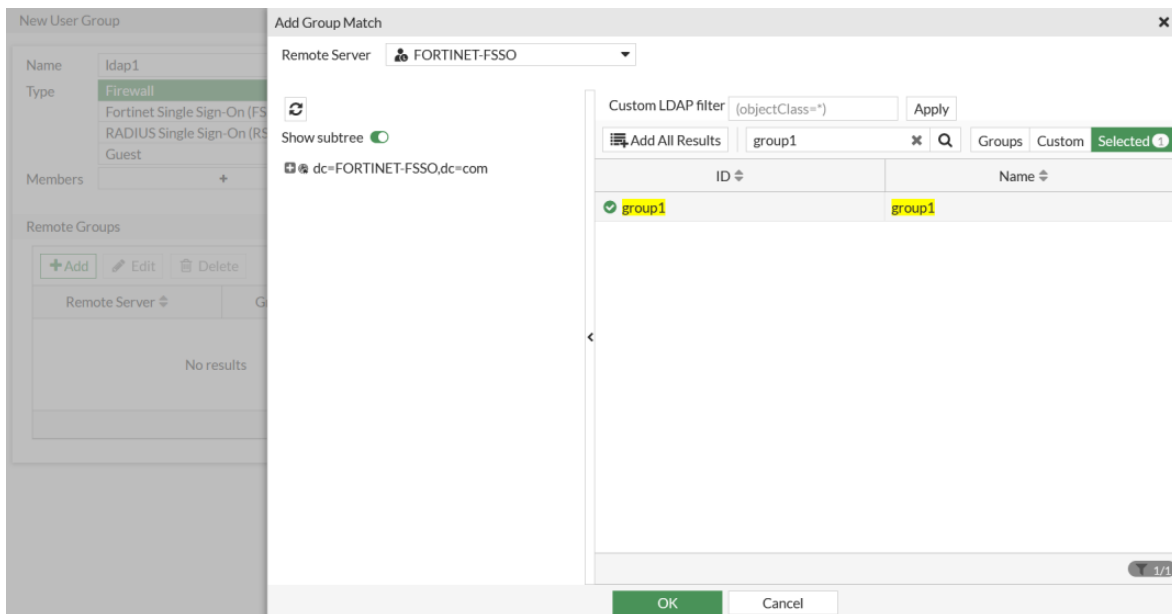
To configure AD LDAP user groups in the GUI:

1. Configure the Active Directory LDAP server, FORTINET-FSSO:
 - a. Go to *User & Authentication > LDAP Servers* and click *Create New*.
 - b. Enter the following:

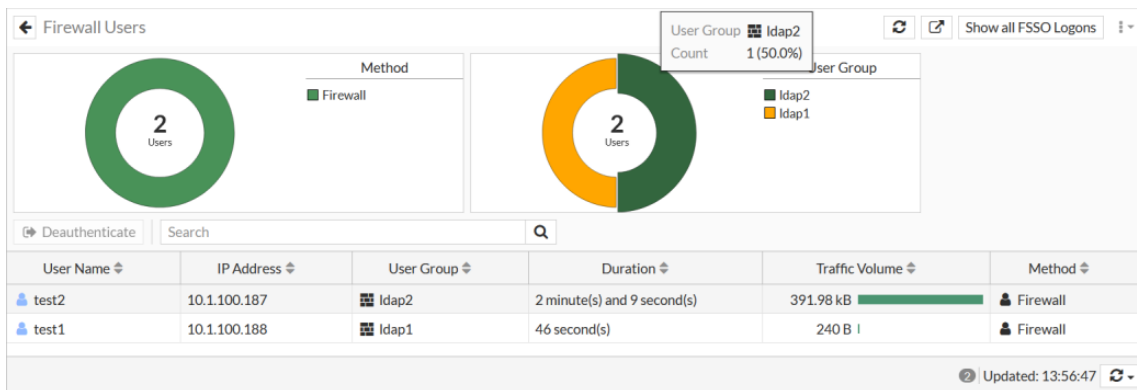
Name	<i>FORTINET-FSSO</i>
Server IP/Name	<i>10.1.100.131</i>
Distinguished Name	<i>dc=FORTINET-FSSO,dc=com</i>
Bind Type	<i>Regular</i>
Username	<i>cn=administrator,cn=users,dc=FORTINET-FSSO,dc=com</i>
Password	Enter the password.

- c. Click *OK*.
2. Configure the LDAP user groups:
 - a. Go to *User & Authentication > User Groups* and click *Create New*.
 - b. Enter the name, *ldap1*.

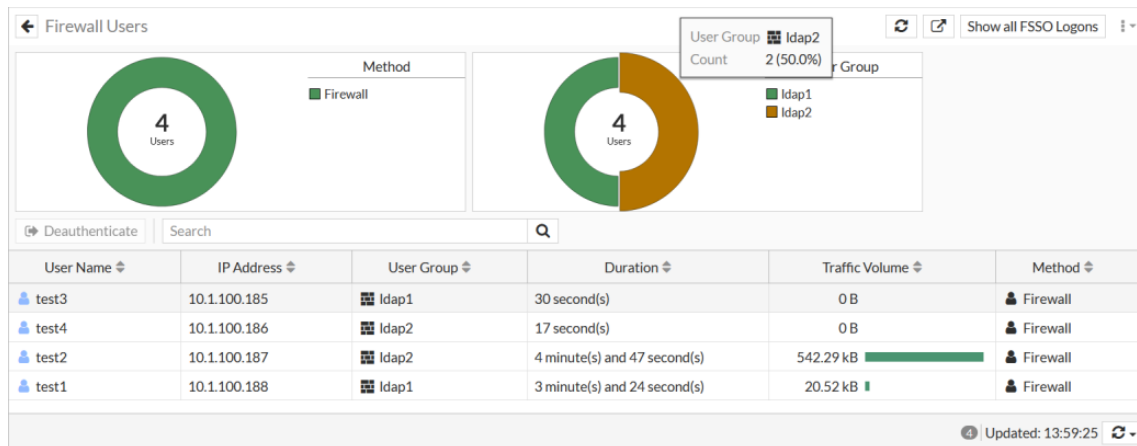
- c. In the *Remote Groups* table, click *Add*. The *Add Group Match* pane opens.
- d. For *Remote Server*, select *FORTINET-FSSO*.
- e. In the search box, enter *group1*, and select the result in the table.
- f. Click *OK*.



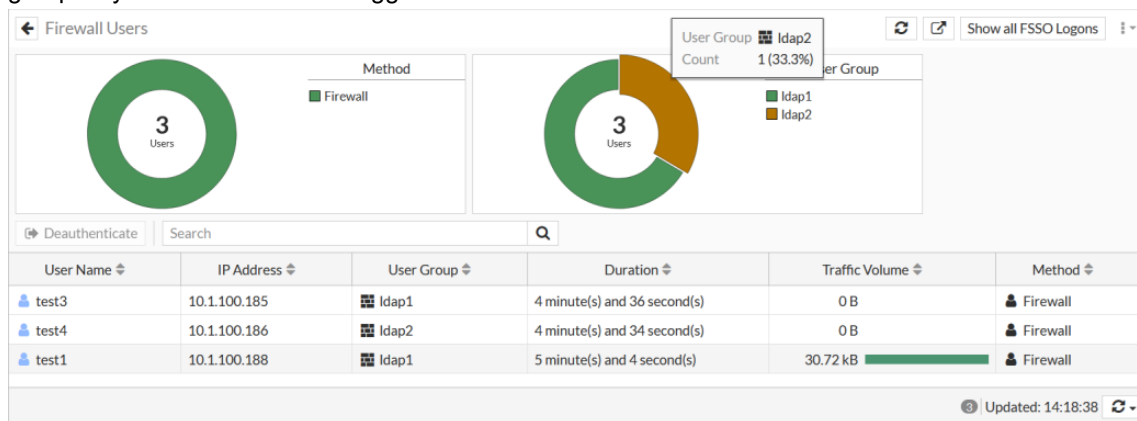
- g. Repeat these steps to configure *ldap2* with the *FORTINET-FSSO group2*.
- h. Click *OK*.
3. Configure a firewall policy with both LDAP groups:
 - a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
 - b. For *Source*, select *ldap1* and *ldap2*.
 - c. Configure the other settings as needed.
 - d. Click *OK*.
4. Get users *test1* and *test2* to log in.
5. In FortiOS, go to *Dashboard > Users & Devices* and click the *Firewall Users* widget to expand to full screen view. Hover over a group in the *User Group* donut chart to view how many users are logged on from that group, and the number of users as a percentage of all logged on users. The chart shows that two users are logged in.



6. Get users *test3* and *test4* to log in, and refresh the *Firewall Users* widget. Each LDAP group has two users logged in, with a total of four active users.



7. Get user test2 to log out, and refresh the *Firewall Users* widget. There is a total of three active users, and the Idap2 group only has one user that is logged in.

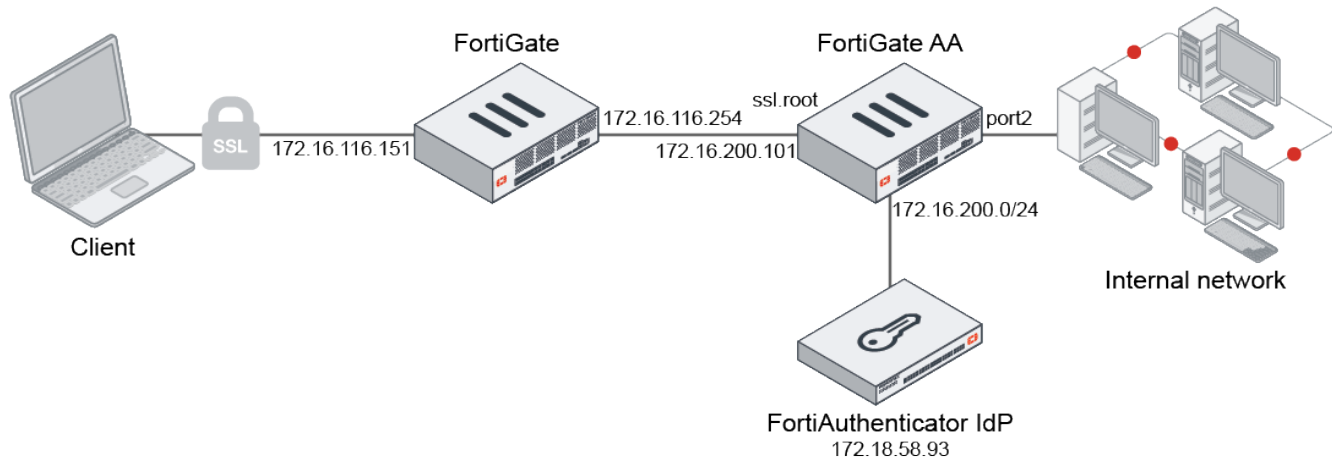


To verify the user group count in the CLI:

```
# diagnose user-device-store user-count list <integer>
# diagnose user-device-store user-count query <FQDN of AD group>
```

Configuring SAML SSO in the GUI - 7.0.2

SAML single sign-on configurations can now be done from the GUI under *User & Authentication > User Groups*. The new GUI wizard helps generate the service provider (SP) URLs based on the supplied SP address. The SAML object that is created can be selected when defining new user groups.



In this example, FortiGate AA is the inside firewall (172.16.200.101). The other FortiGate is the outside firewall that only does port forwarding from 172.16.116.151:55443 to 172.16.200.101:443. FortiGate AA is configured to allow full SSL VPN access to the network in port2. This SSL VPN portal allows users from the user group *saml_grp* and SAML server *saml_test* to log in. In this topology, a FortiAuthenticator acts as the SAML identity provider (IdP), while the FortiGate is the SAML SP. External users are directed to the FortiAuthenticator IdP login URL to authenticate. For more information about configuring a FortiAuthenticator as an IdP, see [Service providers](#).

The FortiAuthenticator in this example has the following configuration:

The screenshot displays the FortiAuthenticator VM configuration interface for a SAML Service Provider. The left sidebar shows the navigation menu with categories like System, Authentication, and SAML IdP. The main panel is titled 'Edit SAML Service Provider' and contains the following sections:

- General:**
 - IdP address: 172.18.58.93:443
 - SP name: FGT501E-kw
 - IdP prefix: 43211234
 - IdP entity id: http://172.18.58.93:443/saml-idp/43211234/metadata/
 - IdP single sign-on URL: https://172.18.58.93:443/saml-idp/43211234/login/
 - IdP single logout URL: https://172.18.58.93:443/saml-idp/43211234/logout/
 - Server certificate: Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-35728DCE
 - IdP signing algorithm: http://www.w3.org/2000/09/xmldsig#rsa-sha1
 - ☐ Support IdP-initiated assertion response
 - ☐ Participate in single logout
- SP Metadata:**
 - SP entity ID: http://172.16.116.151:55443/remote/saml/metadata/
 - SP ACS (login) URL: https://172.16.116.151:55443/remote/saml/login/
 - SP SLS (logout) URL: https://172.16.116.151:55443/remote/saml/logout/
 - ☐ SAML request must be signed by SP
- Authentication:**
 - Authentication method:
 - ☐ Mandatory password and OTP
 - ☒ Every configured password and OTP factors
 - ☐ Password-only
 - ☐ OTP-only
 - ☐ FIDO-only
 - ☐ Password and FIDO
 - ☐ Adaptive Authentication (with 'Configure subnets' button)
 - Application name for FTM push notification: (empty field)
 - ☐ Use FIDO-only authentication if requested by the SP
- Assertion Attribute Configuration:**
 - Subject NameID: Username
 - Format: urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified
 - ☐ Include realm name in subject NameID
- Assertion Attributes:**
 - Assertion attribute: (red X icon)
 - SAML attribute: users
 - User attribute: Username
 - Assertion attribute: (red X icon)
 - SAML attribute: Groupname
 - User attribute: Group
 - + Add Assertion Attribute
- Debugging Options:** (expandable section)

To configure FortiGate AA as an SP:


1. Create a new SAML server entry:
 - a. Go to *User & Authentication > Single Sign-On* and click *Create New*. The single-sign on wizard opens.
 - b. Enter a name (*saml_test*). The other fields will automatically populate based on the FortiGate's WAN IP and port.


New Single Sign-On


1 ————— 2


Name

SP address

SP address 

SP entity ID 

SP single sign-on URL 

SP single logout URL 

SP certificate ☐



Click the icon beside the *SP entity ID*, *SP single sign-on URL*, and *SP single logout URL* fields to copy the text.

- c. Click *Next*.
- d. Enter the FortiAuthenticator IdP details:

IdP address	172.18.58.93:443
Prefix	43211234
IdP certificate	REMOTE_Cert_1

- e. Enter the additional SAML attributes that will be used to verify authentication attempts:

Attribute used to identify users	Username
Attribute used to identify groups	Group

The IdP must be configured to include these attributes in the SAML attribute statement. In FortiAuthenticator, this is configured in the *Assertion Attributes* section.

New Single Sign-On

✓ ————— 2

IdP Details

Log into your Identity Provider platform to find the following information.

IdP type: **Fortinet Product** Custom

IdP address: 172.18.58.93:443

Prefix: 43211234

IdP certificate: REMOTE_Cert_1

Additional SAML Attributes

The FortiGate will look for these attributes to verify authentication attempts. Configure your Identity Provider to include them in the SAML Attribute Statement.

Attribute used to identify users: Username

Attribute used to identify groups: Group

Back Submit Cancel

f. Click **Submit**.

The following is created in the backend:

```
config user saml
  edit "saml_test"
    set cert "fgt_gui_automation"
    set entity-id "http://172.16.116.151:55443/remote/saml/metadata/"
    set single-sign-on-url "https://172.16.116.151:55443/remote/saml/login/"
    set single-logout-url "https://172.16.116.151:55443/remote/saml/logout/"
    set idp-entity-id "http://172.18.58.93:443/saml-idp/43211234/metadata/"
    set idp-single-sign-on-url "https://172.18.58.93:443/saml-idp/43211234/login/"
    set idp-single-logout-url "https://172.18.58.93:443/saml-idp/43211234/logout/"
    set idp-cert "REMOTE_Cert_1"
    set user-name "Username"
    set group-name "Group"
    set digest-method sha1
  next
end
```

2. Create the SAML group:

- a. Go to *User & Authentication > User Groups* and click *Create New*.
- b. Enter a name, *saml_grp*.
- c. In the *Remote Groups* table, click *Add*.

- d. In the *Remote Server* dropdown, select *saml_test* and click *OK*.

- e. Click *OK*.

The following is created in the backend:

```
config user group
  edit "saml_grp"
    set member "saml_test"
  next
end
```

3. Add the SAML group in the SSL VPN settings:
- Go to *VPN > SSL-VPN Settings*.
 - In the *Authentication/Portal Mapping* table, click *Create New*.
 - For *Users/Groups*, click the + and select *saml_grp*.
 - Select the *Portal* (*testportal1*).
 - Click *OK*.

- f. Click *Apply*.
- 4. Configure the firewall policy:
 - a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
 - b. Enter the following:

Incoming Interface	ssl.root
Outgoing Interface	port2
Source	all, saml_grp, saml_test

- c. Configure the other settings as needed.
 - d. Click *OK*.
- 5. On the client, log in with SAML using the SSL VPN web portal.



If you are using FortiClient for tunnel mode access, enable *Enable Single Sign On (SSO) for VPN Tunnel* in the *SSL-VPN* connection settings to use the SAML log in. See [Configuring an SSL VPN](#) connection for more information.

- 6. In FortiOS, go to *Dashboard > Network* and click the *SSL-VPN* widget to expand to full view and verify the connection information.

Secure access

This section includes information about secure access related new features:

- [Wireless on page 527](#)
- [Switch controller on page 571](#)
- [NAC on page 588](#)
- [FortiExtender on page 614](#)

Wireless

This section includes information about wireless related new features:

- [Configure Agile Multiband Operation on page 527](#)
- [Captive portal authentication when bridged via software switch on page 532](#)
- [DHCP address enforcement on page 534](#)
- [Increase maximum number of supported VLANs on page 535](#)
- [Add RADIUS MAC delimiter options on page 536](#)
- [Radio transmit power range in dBm on page 538](#)
- [Wireless NAC support on page 593](#)
- [Station mode on FortiAP radios to initiate tests against other APs on page 540](#)
- [AP operating temperature 7.0.1 on page 542](#)
- [Allow indoor and outdoor flags to be overridden 7.0.1 on page 542](#)
- [DNS configuration for local standalone NAT VAPs 7.0.1 on page 544](#)
- [Backward compatibility with FortiAP models that uses weaker ciphers 7.0.1 on page 546](#)
- [Disable console access on managed FortiAP devices 7.0.1 on page 548](#)
- [Captive portal authentication in service assurance management \(SAM\) mode 7.0.1 on page 550](#)
- [Provide LBS station information with REST API 7.0.2 on page 553](#)
- [Allow users to select individual security profiles in bridged SSID 7.0.2 on page 557](#)
- [Wireless client MAC authentication and MPSK returned through RADIUS 7.0.2 on page 561](#)
- [FQDN for FortiPresence server IP address in FortiAP profiles 7.0.2 on page 565](#)
- [Wi-Fi Alliance Hotspot 2.0 Release 3 support 7.0.2 on page 566](#)
- [Automatic BSS coloring 7.0.2 on page 568](#)
- [Configure 802.11ax MCS rates 7.0.2 on page 570](#)

Configure Agile Multiband Operation

The Wi-Fi Alliance Agile Multiband Operation (MBO) feature enables better use of Wi-Fi network resources in roaming decisions and improves overall performance. This enhancement allows the FortiGate to push the MBO configuration to managed APs, which adds the MBO information element to the beacon and probe response for 802.11ax.

```
config wireless-controller vap
  edit <name>
```

```

        set mbo {enable | disable}
        set gas-comeback-delay <integer>
        set gas-fragmentation-limit <integer>
        set mbo-cell-data-conn-pref {excluded | prefer-not | prefer-use}
    next
end

```

mbo {enable disable}	Enable/disable Multiband Operation (default = disable).
gas-comeback-delay <integer>	GAS comeback delay in milliseconds (100 - 10000, default = 500, 0 = special).
gas-fragmentation-limit <integer>	GAS fragmentation limit (512 - 4096, default = 1024).
mbo-cell-data-conn-pref {excluded prefer-not prefer-use}	<p>MBO cell data connection preference:</p> <ul style="list-style-type: none"> excluded: Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection. prefer-not: Wi-Fi Agile Multiband AP prefers that the Wi-Fi Agile Multiband STA should not use cellular data connection. prefer-use: Wi-Fi Agile Multiband AP prefers that the Wi-Fi Agile Multiband STA should use cellular data connection.

To configure MBO for an 802.11ax FortiAP:

1. Configure MBO on the VAP:

```

config wireless-controller vap
    edit "FOS-QA"
        set max-clients 15
        set ssid "FOS-QAehta-01"
        set pmf enable
        set pmf-assoc-comeback-timeout 8
        set mbo enable
        set gas-comeback-delay 0
        set gas-fragmentation-limit 2048
        set mbo-cell-data-conn-pref prefer-use
        set passphrase <somepassword>
        set schedule "always"
        set target-wake-time disable
        set igmp-snooping enable
        unset broadcast-suppression
        set mu-mimo disable
        set quarantine disable
        set dhcp-option82-insertion enable
        set qos-profile "test"
    next
end

```

2. Enable the VAP on a WTP profile:

```

config wireless-controller wtp-profile
    edit "FAP234F-default"
        config platform
            set type 234F
            set ddscan enable
        end
    end
end

```

```

set ble-profile "new"
set wan-port-mode wan-lan
config lan
    set port-mode bridge-to-ssid
    set port-ssid "16sep"
end
set handoff-sta-thresh 55
set ip-fragment-preventing tcp-mss-adjust icmp-unreachable
set allowaccess https ssh snmp
set poe-mode high
set frequency-handoff enable
set ap-handoff enable
config radio-1
    set band 802.11ax
    set short-guard-interval enable
    set auto-power-level enable
    set auto-power-high 21
    set auto-power-low 1
    set darrp enable
    set vap-all manual
    set vaps "FOS-QA"
    set channel "1" "6" "11"
end
config radio-2
    set band 802.11ax-5G
    set short-guard-interval enable
    set auto-power-level enable
    set auto-power-low 1
    set darrp enable
    set vap-all manual
    set vaps "FOS-QA"
    set channel "36" "40" "44" "48" "149" "153" "157" "161" "165"
end
config radio-3
    set mode monitor
    set wids-profile "default"
end
config lbs
    set station-locate enable
end
next
end

```

3. Verify the MBO settings are pushed to the FortiAP:

```

# diagnose debug application wpa2 255
21176.239 Received data - hexdump(len=153):
 13 02 00 00 00 00 00 00 00 00 00 00 B0 01 A5 C0 .....
 7E 14 01 00 04 D5 90 E9 F4 E0 46 50 34 33 31 46 ~.....FP431F
 54 46 32 30 30 30 30 30 31 35 00 00 00 00 00 00 TF20000015.....
 80 18 39 91 FF 7F 00 00 00 E2 C2 90 07 E0 32 AC ..9.....2.
 FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00 .....
 00 00 00 00 00 00 00 00 78 BF E1 15 00 00 00 00 .....x.....
 00 00 01 00 31 00 00 00 D0 00 3C 00 04 D5 90 E9 ....1.....<.....
 F4 E0 A0 51 0B 4A 84 F4 FF FF FF FF FF FF A0 03 ...Q.J.....
 04 0A 00 6C 02 00 00 10 00 00 01 02 00 10 01 DD ...l.....
 DD 06 00 50 6F 9A 12 01 02 ...Po....
21176.239 HOSTAPD: <0>192.165.1.176:5246<1-0> entering state RUN

```

```

mgmt::action
: GAS: GAS Initial Request from a0:51:0b:4a:84:f4 (dialog token 0)
ANQP: 1 Info IDs requested in Query list
ANQP: Unsupported WFA vendor type 18
ANQP: Locally generated ANQP responses - hexdump(len=0):
ANQP: Initial response (no comeback)
21176.239 Sending data - hexdump(len=141):
  0C 03 00 00 00 00 00 00 00 00 00 00 00 B0 01 A5 C0 .....
  7E 14 01 00 04 D5 90 E9 F4 D0 00 00 00 00 00 00 00 ~.....
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

4. On the FortiAP, verify the MBO settings are pushed from the FortiGate:

```

# vcfg
-----VAP Configuration      1-----
Radio Id  0 WLAN Id  0 FOS-QAehta-01 ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
    vlanid=0, intf=wlan00, vap=0x12b8018, bssid=e0:23:ff:b2:18:70
    llax high-efficiency=enabled target-wake-time=disabled bss-color=0
partial=enabled
    mesh backhaul=disabled
    local_auth=disabled standalone=disabled nat_mode=disabled
    local_bridging=disabled split_tunnel=disabled
    intra_ssid_priv=disabled
    mcast_enhance=disabled igmp_snooping=enabled
    mac_auth=disabled fail_through_mode=disabled sta_info=0/0
    mac=local, tunnel=8023, cap=8ce0, qos=disabled
    prob_resp_suppress=disabled
    rx sop=disabled
    sticky client remove=disabled
    mu mimo=disabled          ldpc_config=rxtx
    dhcp_option43_insertion=enabled          dhcp_option82_insertion=enabled,
dhcp_option82_circuit_id=disable, dhcp_option82_remote_id=disable
    access_control_list=disabled
    bc_suppression=
    auth=WPA2, PSK, AES WPA keyIdx=4, keyLen=16, keyStatus=1, gTsc=000000000000
    key=dee8be7d 3675eda2 7123f695 1d740319
    pmf=required
    okc=disabled, dynamic_vlan=disabled, extern_roaming=disabled
    voice_ent(802.11kv)=disabled, fast_bss_trans(802.11r)=disabled mbo=enabled
    airfairness weight: 20%
    schedules=SMTWTFS 00:00->00:00,
    ratelimit(Kbps): ul=100 dl=0 ul_user=0 dl_user=0 burst=disabled

-----VAP Configuration      2-----
Radio Id  1 WLAN Id  0 FOS-QAehta-01 ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
    vlanid=0, intf=wlan10, vap=0x12b8860, bssid=e0:23:ff:b2:18:78
    llax high-efficiency=enabled target-wake-time=disabled bss-color=0
partial=enabled
    mesh backhaul=disabled
    local_auth=disabled standalone=disabled nat_mode=disabled
    local_bridging=disabled split_tunnel=disabled
    intra_ssid_priv=disabled
    mcast_enhance=disabled igmp_snooping=enabled

```



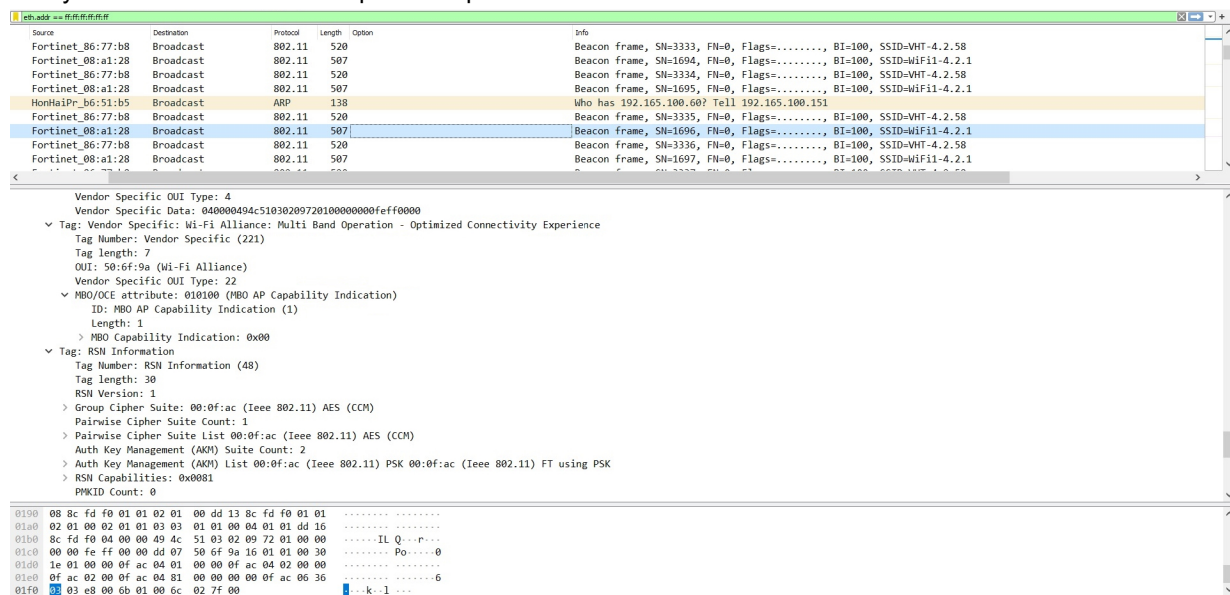
```

mac_auth=disabled fail_through_mode=disabled sta_info=0/0
mac=local, tunnel=8023, cap=8ce0, qos=disabled
prob_resp_suppress=disabled
rx sop=disabled
sticky client remove=disabled
mu mimo=disabled          ldpc_config=rxtx
dhcp_option43_insertion=enabled      dhcp_option82_insertion=enabled,
dhcp_option82_circuit_id=disable, dhcp_option82_remote_id=disable
access_control_list=disabled
bc_suppression=
auth=WPA2, PSK, AES WPA keyIdx=4, keyLen=16, keyStatus=1, gTsc=000000000000
key=6042ccb8 66c18743 18cdb5d0 12f9c0fc
pmf=required
okc=disabled, dynamic_vlan=disabled, extern_roaming=disabled
voice_ent(802.11kv)=disabled, fast_bss_trans(802.11r)=disabled mbo=enabled
airfairness weight: 20%
schedules=SMTWTFS 00:00->00:00,
ratelimit(Kbps): ul=100 dl=0 ul_user=0 dl_user=0 burst=disabled

```

-----Total 2 VAP Configurations-----

5. Verify the beacon frames in the packet captures:



The image shows a Wireshark packet capture of beacon frames. The top pane displays a list of packets with columns for Source, Destination, Protocol, Length, and Info. The bottom pane shows the detailed view of a selected beacon frame (SN=1696).

Source	Destination	Protocol	Length	Info
Fortinet_86:77:b8	Broadcast	802.11	520	Beacon frame, SN=3333, FH=0, Flags=....., BI=100, SSID=WHT-4.2.58
Fortinet_08:a1:28	Broadcast	802.11	507	Beacon frame, SN=1694, FH=0, Flags=....., BI=100, SSID=Wifi1-4.2.1
Fortinet_86:77:b8	Broadcast	802.11	520	Beacon frame, SN=3334, FH=0, Flags=....., BI=100, SSID=WHT-4.2.58
Fortinet_08:a1:28	Broadcast	802.11	507	Beacon frame, SN=1695, FH=0, Flags=....., BI=100, SSID=Wifi1-4.2.1
HonHaiPr_b6:51:b5	Broadcast	ARP	138	Who has 192.165.100.60? Tell 192.165.100.151
Fortinet_86:77:b8	Broadcast	802.11	520	Beacon frame, SN=3335, FH=0, Flags=....., BI=100, SSID=WHT-4.2.58
Fortinet_08:a1:28	Broadcast	802.11	507	Beacon frame, SN=1696, FH=0, Flags=....., BI=100, SSID=Wifi1-4.2.1
Fortinet_86:77:b8	Broadcast	802.11	520	Beacon frame, SN=3336, FH=0, Flags=....., BI=100, SSID=WHT-4.2.58
Fortinet_08:a1:28	Broadcast	802.11	507	Beacon frame, SN=1697, FH=0, Flags=....., BI=100, SSID=Wifi1-4.2.1

Details of Beacon frame, SN=1696:

- Vendor Specific OUI Type: 4
- Vendor Specific Data: 040000494c51030209720100000000efff0000
- Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience
 - Tag Number: Vendor Specific (221)
 - Tag Length: 7
 - OUI: 50:6f:9a (Wi-Fi Alliance)
- Vendor Specific OUI Type: 22
- MBO/OCE attribute: 010100 (MBO AP Capability Indication)
 - ID: MBO AP Capability Indication (1)
 - Length: 1
 - MBO Capability Indication: 0x00
- Tag: RSN Information
 - Tag Number: RSN Information (48)
 - Tag Length: 30
 - RSN Version: 1
 - Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 - Pairwise Cipher Suite Count: 1
 - Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
 - Auth Key Management (AKM) Suite Count: 2
 - Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) FT using PSK
 - RSN Capabilities: 0x0001
 - PMKID Count: 0

Packet Bytes:

```

0190 08 8c fd f0 01 01 02 01 00 dd 13 8c fd f0 01 01 .....
01a0 02 01 00 02 01 01 03 03 01 01 00 04 01 01 dd 16 .....
01b0 8c fd f0 04 00 00 49 4c 51 03 02 09 72 01 00 00 ..... IL Q...
01c0 00 00 fe ff 00 00 dd 07 50 6f 9a 16 01 01 00 30 ..... Po....0
01d0 1e 01 00 00 0f ac 04 01 00 00 0f ac 04 02 00 00 .....
01e0 0f ac 02 00 0f ac 04 81 00 00 00 0f ac 06 36 .....-6
01f0 03 e8 00 0b 01 00 0c 02 7f 00 .....k...1...

```

The image displays two screenshots from the Wireshark network protocol analyzer. The top screenshot shows a list of captured packets, with several IEEE 802.11 Beacon frames from Fortinet_86:77:b8. The bottom screenshot shows the detailed view of a selected packet (Frame 132), which is an IEEE 802.11 Action frame. The details pane shows the frame structure, including the Radiotap header, 802.11 radio information, and the IEEE 802.11 Action frame. The Action frame is of type 'Public Action' and contains an 'Advertisement Protocol' element (ANQP).

Captive portal authentication when bridged via software switch

In a scenario where a tunnel mode SSID or a VLAN sub-interface of an SSID is bridged with other interfaces via a software switch, captive portal authentication on the SSID or VLAN sub-interface is now allowed. This requires the `intra-switch-policy` to be set to `explicit` when the switch interface is created. Users accessing the SSID will be redirected to the captive portal for authentication.

To configure captive portal authentication on an SSID or VLAN sub-interface:

1. Configure the local user:

```
config user local
  edit "user1"
    set passwd *****
  next
end
```

2. Configure the user group:

```
config user group
  edit "wifi-group"
```

```

        set member "user1"
    next
end

```

3. Configure the VAP:

```

config wireless-controller vap
    edit "test-captive"
        set ssid "test-captive"
        set security captive-portal
        set portal-type auth+disclaimer
        set selected-usergroups "wifi-group"
        set schedule "always"
    next
end

```

4. Create a software switch interface consisting of a tunnel VAP with captive portal security and a physical interface (port7):

```

config system switch-interface
    edit "test-ssw"
        set vdom "vdom1"
        set member "port7" "test-captive"
        set intra-switch-policy explicit
    next
end

```

5. Create the firewall policy:

```

config firewall policy
    edit 1
        set srcintf "test-captive" "port7"
        set dstintf "port7" "test-captive"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat disable
    next
end

```

6. Connect the external DHCP server to the physical interface.

7. Connect a WiFi client to the tunnel VAP. The client will get an IP assignment from the DHCP server and pass the captive portal authentication.

8. Verify the authenticated firewall users list:

```

# diagnose firewall auth list
10.100.250.250, u1
    src_mac: fc:d8:d0:9a:8b:85
    type: fw, id: 0, duration: 29, idled: 12
    expire: 288, allow-idle: 300
    flag(100): wssso
    packets: in 229 out 162, bytes: in 192440 out 22887
    user_id: 16777218
    group_id: 2
    group_name: wifi
----- 1 listed, 0 filtered -----

```

DHCP address enforcement

DHCP address enforcement ensures that clients who connect must complete the DHCP process to obtain an IP address; otherwise, they are disconnected from the SSID. This prevents users with static addresses that may conflict with the DHCP address scheme, or users that fail to obtain a DHCP IP assignment to connect to the SSID.

To configure DHCP address enforcement in FortiOS:

```
config wireless-controller vap
  edit "test-tunnel"
    set ssid "test-tunnel"
    set passphrase *****
    set schedule "always"
    set dhcp-address-enforcement enable
  next
end
```



The default setting for dhcp-address-enforcement is disable.

To view the diagnostics in FortiAP:

```
# cw_diag -c vap-cfg
-----VAP Configuration      1-----
Radio Id  1 WLAN Id  0 test-tunnel ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown (-1)
  vlanid=0, intf=wlan11, vap=0x1d481ae, bssid=90:6c:ac:4e:47:c1
  mesh backhaul=disabled
  local_auth=disabled standalone=disabled nat_mode=disabled
  local_bridging=disabled split_tunnel=disabled
  intra_ssid_priv=disabled
  mcast_enhance=disabled igmp_snooping=disabled
  mac_auth=disabled fail_through_mode=disabled sta_info=2/0
  mac=local, tunnel=8023, cap=8ce0, qos=disabled
  prob_resp_suppress=disabled
  rx sop=disabled
  sticky client remove=disabled
  mu mimo=enabled          ldpc_config=rxtx
  dhcp_option43_insertion=enabled      dhcp_option82_insertion=disabled
  dhcp_enforcement=enabled
  access_control_list=disabled
  bc_suppression=dhcp dhcp-ucast arp
  auth=WPA2, PSK, AES WPA keyIdx=1, keyLen=16, keyStatus=1, gTsc=000000000000
  key=3c0b3084 639b28d9 07448633 55e9adda
  pmf=disable
  okc=disabled, dynamic_vlan=disabled, extern_roaming=disabled
  voice_ent(802.11kv)=disabled, fast_bss_trans(802.11r)=disabled
  airfairness weight: 20%
  schedules=SMTWTFS 00:00->00:00,
  ratelimit(Kbps): ul=0 dl=0 ul_user=0 dl_user=0 burst=disabled
  rates control configuration: No data rate is configured
-----Total      1 VAP Configurations-----
```

Sample FortiOS WiFi events log:

```
1: date=2021-02-26 time=11:35:14 eventtime=1614368114443516023 tz="-0800" logid="0104043709"
type="event" subtype="wireless" level="warning" vd="vdom1" logdesc="Wireless client denied
by DHCP enforcement for using static IP address" sn="FP423E3X000000000" ap="TEST-FAP-423E"
vap="test-tunnel" ssid="test-tunnel" stamac="ac:1f:74:12:40:86" security="WPA2 Personal"
encryption="AES" action="DHCP-enforcement" reason="N/A" msg="Client ac:1f:74:12:40:86 denied
by DHCP enforcement for using static IP 10.8.0.5" remotewtptime="3314.349637"
```

In this example, a client configured with static IP address was rejected.

To view the diagnostics in FortiOS:

```
# execute dhcp lease-list
test-tunnel
  IP          MAC-Address      Hostname      VCI          SSID          AP
Expiry
  10.8.0.3    b2:4a:c0:37:9f:0b Testhost      test-tunnel  FP423E3X000000000 Sat Feb
27 17:40:15 2021

# diagnose wireless-controller wlac -d sta
  vf=1 wtp=1 rId=2 wlan=test-tunnel vlan_id=0 ip=10.8.0.3 ip6=fe80::1c3b:cefd:790b:20cc
mac=b2:4a:c0:37:9f:0b vci= host=Testhost user= group= signal=-55 noise=-95 idle=2 bw=0
use=6 chan=144 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_authed=no
online=yes mimo=1
      ip6=*fe80::1c3b:cefd:790b:20cc,12,
```

In this example, a client with a DHCP assigned IP address was able to join the SSID.

Increase maximum number of supported VLANs

VLAN pooling in SSIDs allow you to load-balance users into various VLANs. To service larger deployments, FortiGate 2U and high-end models support up to 64 VLANs.

To configure VLAN pooling in the GUI:

1. Go to *WiFi & Switch Controller > SSIDs* and click *Create New > SSID*.
2. Enable *VLAN pooling* and select a method (*Managed AP Group*, *Round Robin*, or *Hash*).
3. In the table, click *Create New*.
4. Enter an *ID*, and if using the *Managed AP Group* method, select a group from the dropdown.

5. Click **OK** and add more VLAN pool entries as needed.

6. Edit the remaining SSID settings as needed.
7. Click **OK**.

To configure VLAN pooling in the CLI:

```
config wireless-controller vap
  edit <name>
    ...
    set vlan-pooling {wtp-group | round-robin | hash | disable}
    config vlan-pool
      edit <id>
        set wtp-group <string>
      next
    end
  next
end
```

Add RADIUS MAC delimiter options

In the wireless controller settings, options have been added to specify the delimiter used for various RADIUS attributes for RADIUS MAC authentication and accounting. The options are hyphen, single-hyphen, colon, or none.

```
config wireless-controller vap
  edit <name>
    set mac-username-delimiter {hyphen | single-hyphen | colon | none}
    set mac-password-delimiter {hyphen | single-hyphen | colon | none}
    set mac-calling-station-delimiter {hyphen | single-hyphen | colon | none}
    set mac-called-station-delimiter {hyphen | single-hyphen | colon | none}
    set mac-case MAC {uppercase | lowercase}
  next
end
```

Example

In this example, a username (single-hyphen, lowercase) and password (colon, lowercase) are configured on a FreeRADIUS server.

To configure RADIUS MAC delimiter options:**1. Configure the VAP:**

```

config wireless-controller vap
    edit "wifi"
        set ssid "starr-fgt4-1"
        set security wpa2-only-enterprise
        set mac-username-delimiter single-hyphen
        set mac-password-delimiter colon
        set mac-calling-station-delimiter none
        set mac-called-station-delimiter single-hyphen
        set mac-case lowercase
        set radius-mac-auth enable
        set radius-mac-auth-server "peap"
        set auth radius
        set radius-server "peap"
    next
end

```

2. On the FreeRADIUS server, configure a username (such as 1c872c-b7f64c), and a cleartext password (such as 1c:87:2c:b7:f6:4c).**3. After the client passes RADIUS MAC authentication, verify the RADIUS server log. The FortiGate sent the username as 1c872c-b7f64c and the password as 1c:87:2c:b7:f6:4c:**

```

Fri Mar 12 10:28:52 2021 : Auth: (0) Login OK: [1c872c-b7f64c/1c:87:2c:b7:f6:4c] (from
client fwf port 0 cli 1c872cb7f64c)

```

4. Once the client is connected, verify the accounting log on the accounting server. The FortiGate sent the called station ID as 906cac-c127d8:starr-fgt4-1 and the calling station ID as 1c872cb7f64c:

```

Fri Mar 12 10:33:02 2021
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Name = "tester"
NAS-IP-Address = 0.0.0.0
NAS-Identifier = "127.0.0.1/15246-wifi"
Called-Station-Id = "906cac-c127d8:starr-fgt4-1"
NAS-Port-Type = Wireless-802.11
Service-Type = Framed-User
NAS-Port = 1
Fortinet-SSID = "starr-fgt4-1"
Fortinet-AP-Name = "FWF61E-WIFI0"
Calling-Station-Id = "1c872cb7f64c"
Connect-Info = "CONNECT 0/0Mbps(Tx/Rx) 11AC"
Acct-Session-Id = "6048FE9800000064"
Acct-Multi-Session-Id = "4AD14F4FCBDDDDFF"
WLAN-Pairwise-Cipher = 1027076
WLAN-Group-Cipher = 1027076
WLAN-AKM-Suite = 1027073
Framed-IP-Address = 10.10.80.106
Fortinet-WirelessController-Device-MAC = 0x1c872cb7f64c
Fortinet-WirelessController-WTP-ID = "FWF61E4Q00000000"
Fortinet-WirelessController-Assoc-Time = "Mar 12 2021 10:32:59 PST"
Event-Timestamp = "Mar 12 2021 10:33:02 PST"
Acct-Delay-Time = 0
Acct-Unique-Session-Id = "51c531ce7fd0e92cbf4f3cf06f7ce372"
Timestamp = 1615573982

```

Radio transmit power range in dBm

The radio transmit power can be configured in dBm or as a percentage in FortiAP profiles and override settings.

```
config wireless-controller wtp-profile
  edit <name>
    config radio-1
      set power-mode {dBm | percentage}
      set power-value <integer>
    end
  next
end
```

power-mode {dBm |
percentage}

Set the radio EIRP power in dBm or by percentage.

power-value <integer>

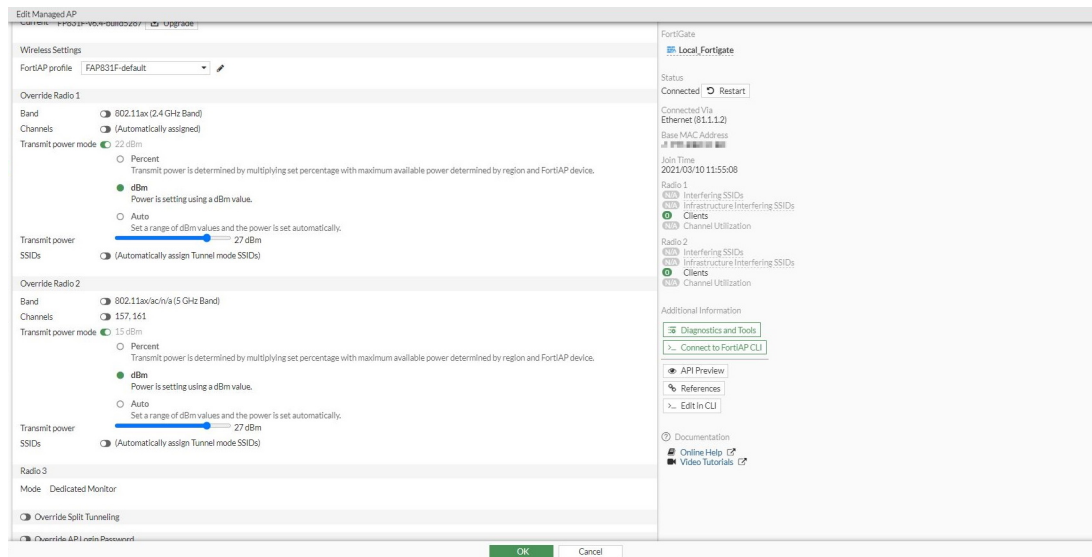
Set the power value for dBm (1 - 33, default = 27) or percentage (0 - 100, default = 100).

To configure the radio transmit power range in dBm in the GUI:

1. Go to *WiFi & Switch Controller > FortiAP Profiles*, or *WiFi & Switch Controller > Managed FortiAPs*.
2. Create a new profile or edit an existing one.
3. For *Transmit power mode*, select *dBm* and adjust the slider to the desired value.

Sample FortiAP Profile:

Sample override radio setting in managed FortiAP:



4. Configure the other settings as needed.
5. Click **OK**.

To configure the radio transmit power range in dBm in the CLI:

```
config wireless-controller wtp-profile
  edit "FAP831F-default"
    config platform
      set type 831F
    end
    set handoff-sta-thresh 55
    set allowaccess https ssh snmp
    config radio-1
      set band 802.11ax-only
      set power-mode dBm
      set power-value 22
      set channel-utilization disable
    end
    config radio-2
      set band 802.11ax-5G
      set power-mode dBm
      set power-value 15
      set channel-utilization disable
      set channel "157" "161"
    end
    config radio-3
      set mode monitor
      set channel-utilization disable
    end
  next
end
```

To verify the settings in FortiAP:

```
# rcfg
  Radio 0: AP
```

```
...
txpwr mode      : set by value (22 dBm)
txpwr cfg/oper  : 22/22 (EIRP +0)
...
```

Radio 1: AP

```
...
txpwr mode      : set by value (15 dBm)
txpwr cfg/oper  : 15/15 (EIRP +0)
...
```

Radio 2: Monitor

```
...
```

Station mode on FortiAP radios to initiate tests against other APs

This enhancement allows service assurance management (SAM) mode to be configured from the CLI where a radio is designated to operate as a client and perform tests against another AP. Ping and iPerf tests can run on an interval, and the results are captured in the Wi-Fi event logs. This allows the FortiGate to verify and assure an existing Wi-Fi network can provide acceptable services.

To configure station mode with a ping test on a managed FortiAP:

1. Enable the SAM ping test on the AP radio:

```
config wireless-controller wtp-profile
  edit "FAP231E-sam"
    ...
    config radio-2
      set mode sam
      set sam-ssid "test-sam"
      set sam-bssid 00:00:00:00:00:00
      set sam-security-type wpa-personal
      set sam-captive-portal disable
      set sam-password *****
      set sam-test ping
      set sam-server "iperf.he.net"
      set sam-report-intv 60
    end
  ...
next
end
```

2. On the AP, verify the configuration settings:

```
# rcfg
...
sam ssid          : test-sam
sam bssid         : 00:00:00:00:00:00
sam security type : Personal
sam captive portal : disabled
sam test          : Ping
sam server ip     : iperf.he.net
sam report interval: 60
sam iperf port    : 5001
```

```
    sam iperf protocol : TCP
...

```

Sample FortiOS WiFi event log:

```
1: date=2021-03-18 time=11:46:45 eventtime=1616006806043197750 tz="-0700" logid="0104043711"
type="event" subtype="wireless" level="notice" vd="vdom1" logdesc="SAM ping test result"
sn="FP231ETF20000449" ap="FP231ETF20000449" vap="test-sam" ssid="test-sam"
stamac="04:d5:90:bf:4b:57" radioid=2 channel=144 security="WPA2 Personal" encryption="AES"
action="sam-ping-result" msg="Connected to AP TEST-FAP-423E, 0.0% packet loss"
remotewtptime="3107.537428"

```

To configure station mode with an iPerf test on a managed FortiAP:**1. Enable the SAM iPerf test on the AP radio:**

```
config wireless-controller wtp-profile
  edit "FAP231E-sam"
    ...
    config radio-2
      set mode sam
      set sam-ssid "test-sam"
      set sam-bssid 00:00:00:00:00:00
      set sam-security-type wpa-personal
      set sam-captive-portal disable
      set sam-password *****
      set sam-test iperf
      set sam-server "iperf.he.net"
      set iperf-server-port 5001
      set iperf-protocol tcp
      set sam-report-intv 60
    end
    ...
  next
end

```

2. On the AP, verify the configuration settings:

```
# rcfg
...
sam ssid          : test-sam
sam bssid         : 00:00:00:00:00:00
sam security type : Personal
sam captive portal : disabled
sam test          : Iperf
sam server ip     : iperf.he.net
sam report interval: 60
sam iperf port    : 5001
sam iperf protocol : TCP
...

```

Sample FortiOS WiFi event log:

```
1: date=2021-03-19 time=10:41:35 eventtime=1616175695652094949 tz="-0700" logid="0104043710"
type="event" subtype="wireless" level="notice" vd="vdom1" logdesc="SAM iperf test result"
sn="FP231ETF20000449" ap="FP231ETF20000449" vap="test-sam" ssid="test-sam"
stamac="04:d5:90:bf:4b:57" radioid=2 channel=144 security="WPA2 Enterprise" encryption="AES"

```

```
action="sam-iperf-result" msg="Connected to AP TEST-FAP-423E, TCP, max rate 10.9 MB/s"
remotewtptime="4061.104484"
```

AP operating temperature - 7.0.1

This enhancement allows the wireless controller to obtain temperature values from FortiAP-F models that have built-in temperature sensors.

The following commands are available in FortiOS:

- `# get wireless-controller wtp-status <serial number> | grep Temp`
- `# diagnose wireless-controller wlac -c wtp <serial number> | grep Temp`

The following command is available in FortiAP:

- `# cw_diag -c temperature`

The temperature measured by the sensors is displayed in degrees Celsius.

Sample FortiOS diagnostics:

```
# get wireless-controller wtp-status FP231FTF20000000 | grep Temp
Temperature in Celsius: 1 (52)

# diagnose wireless-controller wlac -c wtp FP433FTF20000000 | grep Temp
Temperature in Celsius: 3 (55,57,54)
```

Sample FortiAP diagnostics:

```
# cw_diag -c temperature
Temperature in Celsius: 3 (52,52,52)
```

Allow indoor and outdoor flags to be overridden - 7.0.1

When indoor AP models are placed outdoors, or outdoor AP models are placed indoors, there is an option to override the indoor or outdoor flag. This enables the available channels list to reflect the region based on the AP placement.

To change the AP deployment type in the GUI:

1. Go to *WiFi & Switch Controller > FortiAP Profiles* and edit an existing profile. For *Indoor / Outdoor*, the default setting is displayed.
2. Click *Override* to change the setting, then click *Indoor* or *Outdoor*. The radio channel settings in the profile will change based on the deployment type.

The screenshot shows the 'Edit FortiAP Profile' window. The 'Radio 1' section is expanded, showing settings for Mode (Access Point), Band (2.4 GHz), Channel width (20MHz), and Transmit power mode (Percent). The 'Transmit power' slider is set to 100%. The 'SSIDs' section shows 'Tunnel' selected. The right sidebar contains links for Local Fortigate, API Preview, References, Edit in CLI, Documentation, Online Help, and Video Tutorials.

3. Configure the other settings as needed.
4. Click OK.

To change the AP deployment type in the CLI:

```
config wireless-controller wtp-profile
  edit <name>
    set ap-country <string>
    set indoor-outdoor-deployment {platform-determined | indoor | outdoor}
  next
end
```

To verify the deployment type used on an AP:

```
# diagnose wireless-controller wlac -c wtp <serial number> | grep deploy
```

Example

This example uses a sample deployment and available channels for a FAP-431F in Tunisia. The default platform-determined deployment mode for 431F models is indoors, but the user needs to change the deployment to outdoors.

Original configuration:

```
config wireless-controller wtp-profile
  edit FAP431-TN
    set ap-country TN
    set indoor-outdoor-deployment indoor
  config radio-1
    set channel {1 2 3 4 5 6 7 8 9 10 11 12 13}
  end
```

```
        config radio-2
            set channel {36 40 44 48 52* 56* 60* 64*}
        end
    next
end

# diagnose wireless-controller wlac -c wtp FP431FTF20000000 | grep deploy
deployment      : cfg indoor oper indoor
```

With the original FAP-431 indoor deployment, the available options in Tunisia for 2.4 GHz (radio 1) channels are from 1 to 13. The available options for 5 GHz (radio 2) channels are 36, 40, 44, 48, 52, 56, 60, and 64.

To change the AP to an outdoor deployment:

```
config wireless-controller wtp-profile
    edit FAP431-TN
        set ap-country TN
        set indoor-outdoor-deployment outdoor
        config radio-1
        end
        config radio-2
            set channel {100* 104* 108* 112* 116*}
        end
    next
end
```

With the FAP-431 outdoor deployment in Tunisia, there are no available options for 2.4 GHz (radio 1) channels. The available options for 5 GHz (radio 2) channels have changed to 100, 104, 108, 112, and 116.

To verify the AP deployment type changed to outdoor:

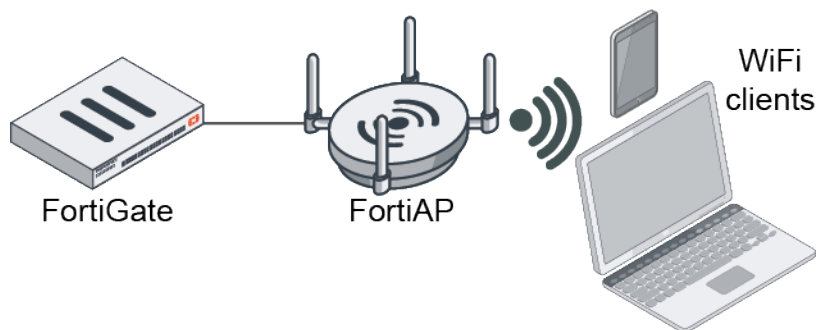
```
# diagnose wireless-controller wlac -c wtp FP431FTF20000000 | grep deploy
deployment      : cfg outdoor oper outdoor
```

DNS configuration for local standalone NAT VAPs - 7.0.1

For SSIDs in local standalone NAT mode, up to three DNS servers can be defined and assigned to wireless endpoints through DHCP.

Example

In this example, an SSID (wifi.fap.01) is configured in local standalone mode with local standalone NAT enabled. Two DNS servers are specified so that wireless endpoints receive the DNS server IP addresses through DHCP when the endpoints connect to the SSID.



To configure the DNS servers and confirm that they are propagated to the endpoints:

1. Configure a VAP:

```
config wireless-controller vap
  edit "wifi.fap.01"
    set ssid "wifi-ssid.fap.01"
    set passphrase *****
    set local-standalone enable
    set local-standalone-nat enable
    set local-standalone-dns enable
    set local-standalone-dns-ip 8.8.8.8 8.8.4.4
    set local-bridging enable
    set local-authentication enable
  next
end
```

2. Check the configured DNS server:

```
# diagnose wireless-controller wlac -c wlan wifi.fap.01
WLAN (001/002) vdom,name: vdom1, wifi.fap.01
  vlanid          : 0 (auto vlan intf disabled)
  ...
  mesh backhaul   : disabled
  local standalone : enabled (nat enabled 0.0.0.0/0.0.0.0 lease 2400 dns enabled
dns-ip 8.8.8.8 8.8.4.4)
  local bridging  : enabled
  ...
  ldpc config     : rxtx
  mf acl cfg      : disabled, allow, 0 entries
  WTP 0001        : 3, FP431FTF20013818
  ---- 3-10.100.100.230:5246 (13 - CWAS_RUN)
```

3. On the managed FortiAP, verify the configuration:

```
FortiAP-431F # vcfg
-----VAP Configuration      1-----
Radio Id 1 WLAN Id 0 wifi-ssid.fap.01 ADMIN_UP(INTF_UP) init_going 0.0.0.0/0.0.0.0
unknown (-1)
  vlanid=0, intf=wlan10, vap=0xb85018, bssid=e0:23:ff:b5:2a:40
  llax high-efficiency=enabled target-wake-time=enabled bss-color=0
partial=enabled
  mesh backhaul=disabled
  local_auth=enabled standalone=enabled nat_mode=enabled
  standalone_dns=enabled dns_ip=8.8.8.8,8.8.4.4
```

```

        bandsteering=disabled
        ...
        primary wag:
        secondary wag:
-----Total      1 VAP Configurations-----

FortiAP-431F # dhcpconf
# dhcpd.conf

default-lease-time 2400;
max-lease-time 8640000;
option domain-name-servers 172.17.254.148,208.91.112.53;
ddns-update-style none;
authoritative;

# intf br.nat.0
subnet 192.168.116.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.116.255;
    option routers 192.168.116.1;
    option domain-name-servers 8.8.8.8,8.8.4.4;
    range 192.168.116.20 192.168.116.249;
    default-lease-time 2400;
}

FortiAP-431F # acconf | grep dns
local_st_dns_1_0=1
sz_st_dns_ip_1_0=2
local_st_dns_ip_list[0]_1_0=8080808
local_st_dns_ip_list[1]_1_0=8080404

```

4. Check the SSID and DNS configuration on a Linux client connected to that SSID:

```

# iwconfig
wlan0 IEEE 802.11 ESSID:"wifi-ssid.fap.01"
      Mode:Managed Frequency:5.22 GHz Access Point: E0:23:FF:B5:2A:40
      Bit Rate=260 Mb/s   Tx-Power=200 dBm
      ...

# resolvectl status | grep -1 'DNS Server'
DNSSEC supported: no
Current DNS Server: 8.8.8.8
DNS Servers: 8.8.8.8
8.8.4.4

```

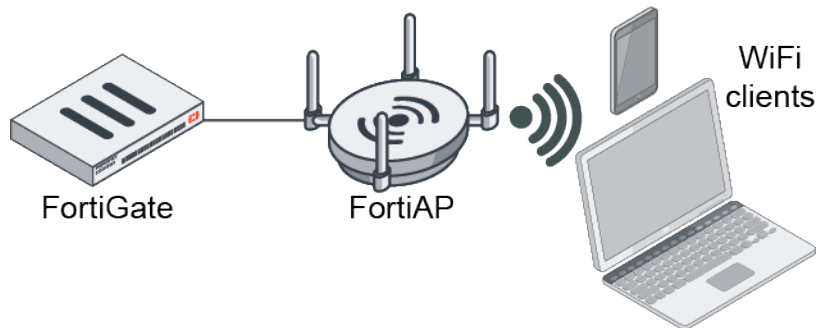
Backward compatibility with FortiAP models that uses weaker ciphers - 7.0.1

FortiAP connections with weak cipher encryption (legacy FortiAP models with names ending in B, C, CR, or D, and FortiAP devices that cannot be upgraded) can be managed by FortiGates that are running FortiOS 7.0.1 by using compatibility mode. This allows for backwards compatibility with 3DES, SHA1, and Strong list ciphers, and is the default tunnel mode.

Set the tunnel mode to `strict` to follow system level strong-crypto ciphers.

To configure the tunnel mode:

```
config wireless-controller global
    set tunnel-mode {compatible | strict}
end
```

**To check the available ciphers in the different tunnel modes:****1. Enable compatibility mode:**

```
config wireless-controller global
    set tunnel-mode compatible
end
```

2. Verify that the legacy FortiAP ciphers AES128-SHA and DES-CBC3-SHA are present:

```
# diagnose wireless-controller wlap -c ciphers
```

Supported cipher list:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384
DHE-RSA-AES128-SHA256
AES128-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES128-SHA256
AES128-SHA
DES-CBC3-SHA
```

Total: 18

3. Set the tunnel mode to strict and verify that the legacy ciphers are not present:

```
config wireless-controller global
    set tunnel-mode strict
end
```

```
# diagnose wireless-controller wlac -c ciphers
```

Supported cipher list:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384
DHE-RSA-AES128-SHA256
AES128-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES128-SHA256
```

Total: 16

Disable console access on managed FortiAP devices - 7.0.1

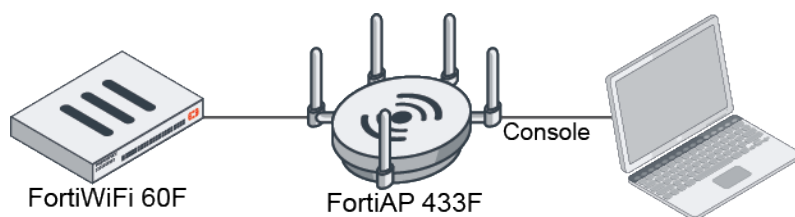
Serial console access on managed FortiAP devices can be disabled in FortiOS by disabling console login in the WTP profile that is applied to the FortiAP. By default, console login is enabled in WTP profiles.

```
config wireless-controller wtp-profile
  edit <profile>
    set console-login {enable | disable}
  next
end
```

When the console access is changed, the managed FortiAPs are rebooted.

Example

In this example, a FortiWiFi 60F is managing a [FortiAP 433F](#). A WTP profile with console login disabled is applied to the FortiAP.



To configure the WTP profile and apply it to the FortiAP:**1. Configure a WTP profile:**

```
config wireless-controller wtp-profile
  edit "FAP433F-default"
    config platform
      set type 433F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess https ssh snmp
    config radio-1
      set band 802.11ax,n,g-only
    end
    config radio-2
      set band 802.11ax-5G
    end
    config radio-3
      set mode monitor
    end
  next
end
```

2. Configure the FortiAP to use the profile:

```
config wireless-controller wtp
  edit "FP433FTF21000000"
    set admin enable
    set wtp-profile "FAP433F-default"
    config radio-1
    end
    config radio-2
    end
  next
end
```

3. On the FortiAP, confirm that console login is enabled:

```
FortiAP-433F # wcfg | grep console-login
console-login      : enabled
```

4. Disable console login in the WTP profile:

```
config wireless-controller wtp-profile
  edit FAP433F-default
    set console-login disable
  WARNING: changing console-login will reboot managed APs.
  next
end
```

The managed FortiAPs are rebooted.

5. Log in to the FortiAP with the SSH connection and confirm that console login is disabled:

```
FortiAP-433F # wcfg | grep console-login
console-login      : disabled
```

Captive portal authentication in service assurance management (SAM) mode - 7.0.1

When configuring a radio in service assurance management (SAM) mode, a client can be configured to authenticate with the captive portal. The captive portal match, success, and failure strings must be specified to automatically detect the authentication success or failure.

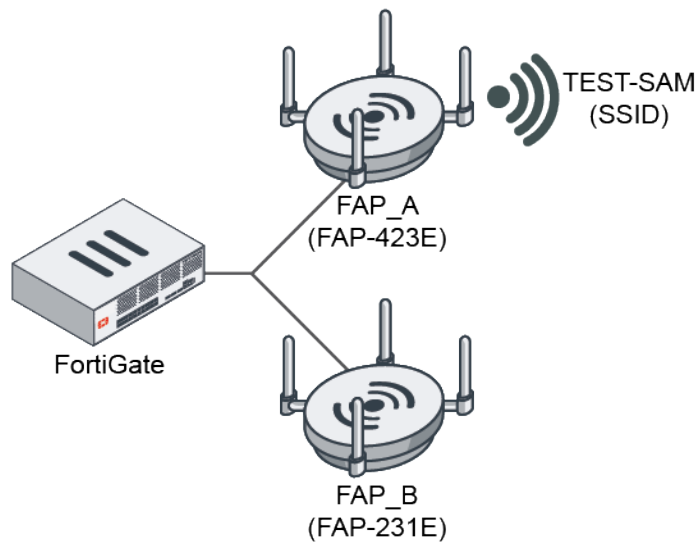
```
config wireless-controller wtp-profile
  edit <name>
    config radio-1
      set sam-cwp-username <string>
      set sam-cwp-password <string>
      set sam-cwp-test-url <string>
      set sam-cwp-match-string <string>
      set sam-cwp-success-string <string>
      set sam-cwp-failure-string <string>
    end
  next
end
```

sam-cwp-username <string>	Enter the username for captive portal authentication.
sam-cwp-password <string>	Enter the password for captive portal authentication.
sam-cwp-test-url <string>	Enter the website the client is trying to access.
sam-cwp-match-string <string>	Enter the identification string from the captive portal login form.
sam-cwp-success-string <string>	Enter the success identification text to appear on the page after a successful login.
sam-cwp-failure-string <string>	Enter the failure identification text on the page after an incorrect login.



Currently, FortiAP only supports bridge mode SSIDs configured with external portal authentication. Other captive portal authentication combinations are not supported.

Example



In this example, a FortiGate manages two FortiAPs (FAP_A and FAP_B). FAP_A serves the SSID, TEST-SAM, with captive portal authentication. FAP_B connects to the SSID and authenticates to the captive portal with the specified credentials.

To configure captive portal authentication in SAM mode:

1. Configure FAP_A to have an SSID with captive portal authentication so it can perform a SAM test.

- a. Configure the RADIUS server:

```
config user radius
  edit "172.18.56.161"
    set server "172.18.56.161"
    set secret *****
  next
end
```

- b. Configure the VAP:

```
config wireless-controller vap
  edit "test-sam"
    set ssid "TEST-SAM"
    set security captive-portal
    set external-web "http://172.18.56.163/portal/index.php"
    set radius-server "172.18.56.161"
    set local-bridging enable
    set portal-type external-auth
    set schedule "always"
  next
end
```

- c. Configure the FortiAP profile:

```
config wireless-controller wtp
  edit "FP423E3X16000020"
    set admin enable
    set wtp-profile "FAP423E-default"
```

```
        config radio-1
            set override-vaps enable
            set vap-all manual
            set vaps "test-sam"
        end
        config radio-2
            set override-vaps enable
            set vap-all manual
        end
    next
end
```

2. Configure the SAM and captive portal settings on FAP_B.

a. Configure the FortiAP profile:

```
config wireless-controller wtp-profile
    edit "FAP231E-default"
        config platform
            set type 231E
            set ddscan enable
        end
        set handoff-sta-thresh 55
        set allowaccess https ssh snmp
        config radio-1
            set mode sam
            set sam-ssid "TEST-SAM"
            set sam-captive-portal enable
            set sam-cwp-username "tester"
            set sam-cwp-password ENC
            set sam-cwp-test-url "https://www.fortinet.com"
            set sam-cwp-match-string "fgtauth"
            set sam-cwp-success-string "Fortinet"
            set sam-cwp-failure-string "failed"
            set sam-password ENC
            set sam-test ping
            set sam-server-type ip
            set sam-server-ip 8.8.8.8
            set sam-report-intv 60
        end
        config radio-2
            unset band
        end
        config radio-3
            set mode monitor
        end
    next
end
```

b. Configure the managed FortiAP settings:

```
config wireless-controller wtp
    edit "FP231ETF20000000"
        set admin enable
        set wtp-profile "FAP231E-default"
        config radio-2
        end
    end
```

```
    next
end
```

3. After a few minutes, check the FAP_B configuration in FortiAP:

```
FortiAP-231E # rcfg
Radio 0: AP
...
sam ssid          : TEST-SAM
sam bssid         : 00:00:00:00:00:00
sam security type : Open
sam captive portal : enabled
sam cwp test url  : https://www.fortinet.com
sam cwp match string : fgtauth
sam cwp success string : Fortinet
sam cwp failure string : failed
sam test         : Ping
sam server       : 8.8.8.8
sam report interval: 60
sam iperf port   : 5001
sam iperf protocol : UDP
...
```

Sample FortiOS WiFi event log:

```
1: date=2021-07-13 time=22:04:20 eventtime=1626239060874592177 tz="-0700" logid="0104043602"
type="event" subtype="wireless" level="warning" vd="root" logdesc="Wireless station sign on
success" sn="FP423E3X16000000" ap="FP423E3X16000000" vap="test-sam" ssid="TEST-SAM"
radioid=1 user="tester" group="N/A" stamac="04:d5:90:bf:4b:4f" srcip=10.1.99.165 channel=11
radioband="802.11ac-2G" signal=-19 snr=76 security="Captive Portal" encryption="N/A"
action="user-sign-on-success" reason="Reserved 0" mpsk="N/A" msg="Client 04:d5:90:bf:4b:4f
user login success."
```

```
2: date=2021-07-13 time=22:04:33 eventtime=1626239073413031350 tz="-0700" logid="0104043711"
type="event" subtype="wireless" level="notice" vd="root" logdesc="SAM ping test result"
sn="FP231ETF20000000" ap="FP231ETF20000000" vap="test-sam" ssid="TEST-SAM"
stamac="04:d5:90:bf:4b:4f" radioid=1 channel=11 security="Captive Portal" encryption="N/A"
action="sam-ping-result" msg="Connected to AP FP423E3X16000000, 0.0% packet loss"
remotewtptime="3566.658211"
```

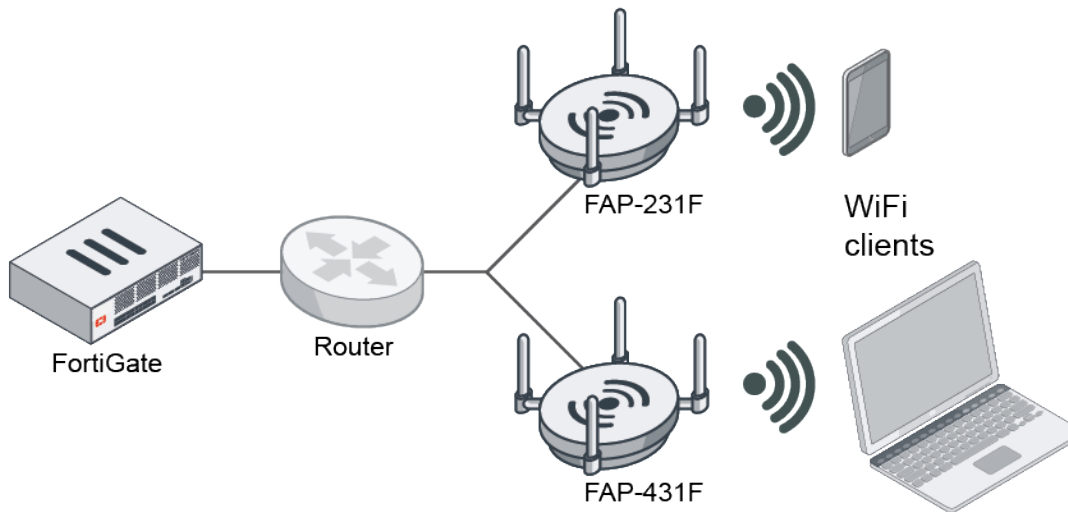
Provide LBS station information with REST API - 7.0.2

Location based services (LBS) information of associated and unassociated wireless stations can be retrieved through a REST API.



This feature requires FortiAP 7.0.2 or FortiAP-W2 7.0.2 and later.

Example



In this example, a FortiGate manages two FortiAPs (FAP-231F and FAP-431F).

To configure the FortiAPs:

1. Configure the region on the devices, for example on the FAP-431F:

```
config wireless-controller wtp
  edit "FP431FTF20012724"
    set admin enable
    set region "wifi"
    set region-x "0.2514256912442"
    set region-y "0.3601190476190"
    set wtp-profile "FAP431F-default"
    config radio-1
    end
    config radio-2
    end
  next
end
```

2. Enable station location in the corresponding WTP profiles, for example on the FAP-431F:

```
config wireless-controller wtp-profile
  edit FAP431F-default
    config lbs
      set station-locate enable
    end
  next
end
```

3. Enable BLE scanning on the devices:

```
config wireless-controller ble-profile
  edit fortiap-discovery
    set ble-scanning enable
  next
end
```


4. Add the BLE profile to the WTP profiles, for example on the FAP-431F:

```
config wireless-controller wtp-profile
  edit FAP431F-default
    set ble-profile fortiaap-discovery
  next
end
```

REST APIs**Associated wireless stations:**

https://<FortiGate IP>/api/v2/monitor/wifi/client?with_triangulation=true

```
{
  "http_method": "GET",
  "results": [
    {
      "ip": "10.10.80.2",
      "ip6": [
        ""
      ],
      "wtp_name": "FP431FTF20012724",
      "wtp_id": "FP431FTF20012724",
      "wtp_radio": 2,
      "wtp_ip": "10.100.100.234",
      "vap_name": "wifi.fap.01",
      "ssid": "wifi-ssid.fap.01",
      "mac": "f8:e4:e3:d8:5e:af",
      "11k_capable": false,
      "11v_capable": false,
      "11r_capable": false,
      "sta_maxrate": 286800,
      "sta_rxrate_mcs": 3,
      "sta_txrate": 48000,
      "sta_txrate_mcs": 0,
      "sta_txrate_score": 16,
      "os": "Debian",
      "hostname": "fosqa-PowerEdge-R210",
      "authentication": "pass",
      "captive_portal_authenticated": 0,
      "manufacturer": "Intel",
      "data_rate_bps": 48000000,
      "data_rxrate_bps": 0,
      "data_txrate_bps": 48000000,
      "snr": 0,
      "idle_time": 0,
      "association_time": 1628812700,
      "bandwidth_tx": 4048,
      "bandwidth_rx": 2314,
      "lan_authenticated": false,
      "channel": 140,
      "signal": 0,
      "vci": "",
      "host": "fosqa-PowerEdge-R210",
      "security": 1,
    }
  ]
}
```

```

    "security_str": "captive",
    "encrypt": 1,
    "noise": 0,
    "radio_type": "802.11ax-5G",
    "mimo": "2x2",
    "vlan_id": 0,
    "tx_discard_percentage": 0,
    "tx_retry_percentage": 0,
    "triangulation_regions": [
      {
        "wtp_id": "FP431FTF20012724",
        "rssi": 60,
        "last_seen": 1628781149
      },
      {
        "wtp_id": "FP231FTF20000041",
        "rssi": 66,
        "last_seen": 1628783914
      }
    ],
    "health": {
      "signal_strength": {
        "value": 0,
        "severity": "good"
      },
      "snr": {
        "value": 0,
        "severity": "poor"
      },
      "band": {
        "value": "5ghz",
        "severity": "good"
      },
      "transmission_retry": {
        "value": 0,
        "severity": "good"
      },
      "transmission_discard": {
        "value": 0,
        "severity": "good"
      }
    }
  },
  "vdom": "vdom1",
  "path": "wifi",
  "name": "client",
  "action": "",
  "status": "success",
  "serial": "FG101FTK20003465",
  "version": "v7.0.2",
  "build": 189
}

```

Unassociated wireless stations and BLE devices:

https://<FortiGate IP>/api/v2/monitor/wifi/unassociated-devices?with_triangulation=true

```
{
  ...
  "type": "unassociated device",
  "mac": "00:00:c7:6e:c5:e2",
  "manufacturer": "ARIX CORPORATION",
  "triangulation_regions": [
    {
      "wtp_id": "FP431FTF20012724",
      "rssi": 54,
      "last_seen": 1628813005
    },
    {
      "wtp_id": "FP231FTF20000041",
      "rssi": 50,
      "last_seen": 1628812378
    }
  ]
},
{
  "type": "BLE device",
  "mac": "78:bd:bc:cc:7e:3d",
  "manufacturer": "Samsung",
  "triangulation_regions": [
    {
      "wtp_id": "FP431FTF20012724",
      "rssi": 2,
      "last_seen": 1628810553
    }
  ]
},
}
```

Allow users to select individual security profiles in bridged SSID - 7.0.2

When configuring an SSID in bridge mode, users can select individual security profiles instead of a security profile group. This applies to models in the FAP-U series that can perform UTM on the FortiAP itself.



The security profile type must be enabled in *System > Feature Visibility* to make the option visible in the GUI.

In the following example, individual antivirus, web filter, application control, and intrusion prevention profiles are applied to a bridge mode SSID.

To apply security profiles to an SSID in the GUI:

1. Go to *WiFi & Switch Controller > SSIDs*, and click *Create New > SSID* or edit an existing SSID.
2. In the *WiFi Settings* section, enable *Security Profiles*.
3. Enable the desired security profile types and select a profile from the corresponding dropdown.

Edit Interface

Name: FOS_utm_bridge (utm_br1)
 Alias: b
 Type: WIFI SSID
 Traffic mode: Bridge

WiFi Settings
 SSID: FOS_utm_bridge
 Client limit: ☐
 Broadcast SSID: ☒

Security Mode Settings
 Security mode: WPA2 Personal

Pre-shared Key
 Mode: Single Multiple
 Passphrase:

Client MAC Address Filtering
 RADIUS server: ☐







Security Profiles
 AntiVirus: ☒ AV wifi-default
 Web filter: ☒ WEB wifi-default
 Application control: ☒ APP wifi-default
 Intrusion Prevention: ☒ IPS wifi-default
 Scan botnets: Disable Block Monitor
 Logging: ☒ Enabled ☐ Disabled

FortiGate
 FortiGate-80E-POE
 Status: Up
 MAC address:
 Additional Information:
 API Preview
 References
 Edit in CLI
 SSID
 Guides
 FortiAP-S Bridge Mode Security Profiles
 Documentation
 Online Help
 Video Tutorials

OK Cancel

4. Edit the other settings as needed.

5. Click OK. The list of applied security profiles is visible in the SSID table.

<div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Clone</div><div>Search</div><div>Q</div></div>						
Name	SSID	Traffic Mode	Security	Schedule	Status	Security Profiles
SSID 2						
ssid1	 FOS_ssid1 (ssid1)	Tunnel	WPA2 Personal	 always	 Up	
utm_br1	 FOS_utm_bridge (utm_br1)	Local Bridge	WPA2 Personal	 always	 Up	<div><div>IPS</div>wifi-default</div>
						<div><div>APP</div>wifi-default</div>
						<div><div>AV</div>wifi-default</div>
						<div><div>WEB</div>wifi-default</div>

To apply security profiles to an SSID in the CLI:

1. Configure the VAP:

```
config wireless-controller vap
  edit "utm_br1"
    set ssid "FOS_utm_bridge"
    set local-bridging enable
    set utm-status enable
    set ips-sensor "wifi-default"
    set application-list "wifi-default"
    set antivirus-profile "wifi-default"
    set webfilter-profile "wifi-default"
```

```
        set scan-botnet-connections block
    next
end
```

2. Assign the VAP to a managed FAP-U device.

a. Configure the FortiAP profile:

```
config wireless-controller wtp-profile
    edit "FAPU431F-default"
        config radio-1
            set band 802.11ax-5G
            set vap-all manual
            set vaps "utm_br1"
        end
        config radio-2
            set band 802.11ax,n,g-only
            set vap-all manual
            set vaps "utm_br1"
        end
    next
end
```

b. Configure the managed FortiAP settings:

```
config wireless-controller wtp
    edit "PU431F5E19000000"
        set admin enable
        set wtp-profile "FAPU431F-default"
        config radio-1
        end
        config radio-2
        end
    next
end
```

3. On the FortiAP, verify that the UTM profiles have been pushed from the FortiGate:

```
# utm_diag cfg show -v
LogServer: :0
UploadInterval: 60
-----
SSID: FOS_utm_bridge
IPS: enabled
    Name: wifi-default
    Sensor: 1
        RuleID:
        LocaFilter: all
        SeveFilter: medium high critical
        ProtFilter: all
        OSFilter: all
        AppFilter: all
        LogOption: enabled
        Action: default
    ApplicationControl: enabled
        Name: wifi-default
        AppBlkPageOption: enabled
        OtherAppActionOption: pass
        UnknownAppActionOption: pass
```

```
DeepAppCtrlOption: disabled
UnknownAppLogOption: disabled
OtherAppLogOption: disabled
SpecialOptions:
    AllowDNS: enabled
    AllowICMP: disabled
    AllowHTTP: disabled
    AllowSSL: disabled
Sensor: 1
    RuleID:
    CatNum:
    SubCatNum:
    Popularity: 1 2 3 4 5
    ProtocolFilter: all
    VendorFilter: all
    TechFilter: all
    BehaviorFilter: all
    RuleParams:
    SessionTTL: 0
    LogOption: disabled
    Action: pass
AntiVirus: enabled
    Name: wifi-default
    HTTP: scan
    SMTP: scan
    POP3: scan
    IMAP: scan
    FTP: scan
    LogOption: enabled
WebFilter: enabled
    Name: wifi-default
    FtgdOption: enabled
    InvalidURLOption: enabled
    PostAction: disabled
CategoryFilters:
    0 - Unrated: monitor
    2 - Alternative Beliefs: block
    7 - Abortion: block
    8 - Other Adult Materials: block
    9 - Advocacy Organizations: block
    11 - Gambling: block
    12 - Extremist Groups: block
    13 - Nudity and Risque: block
    14 - Pornography: block
    15 - Dating: block
    16 - Weapons (Sales): block
    26 - Malicious Websites: block
    57 - Marijuana: block
    61 - Phishing: block
    63 - Sex Education: block
    64 - Alcohol: block
    65 - Tobacco: block
    66 - Lingerie and Swimsuit: block
    67 - Sports Hunting and War Games: block
    86 - Spam URLs: block
    88 - Dynamic DNS: block
```

```

    90 - Unknown: block
    91 - Unknown: block
Botnet: enabled
  Name: utm_br1
  Mode: block
ScanProtOptions: enabled
  Name: FOS_utm_bridge
  MaxAVScanFileSize: 10
  CheckHttpsCert: enabled
GraywareOption: enabled
LogOption: enabled

```

Wireless client MAC authentication and MPSK returned through RADIUS - 7.0.2

Wireless clients can be authenticated using MAC authentication and Multiphase Shift Keying (MPSK) against a RADIUS server. The MPSK passphrases can be dynamically passed from the RADIUS server when the client MAC is authenticated by the RADIUS server, instead of statically storing them on the FortiGate. The passphrases are cached on the FortiGate for future authentication, with a timeout period configured for each VAP.

The `radius-mac-mpsk-auth` and `radius-mac-mpsk-timeout` commands are added to the VAP configuration when the security mode is WPA-Personal:

```

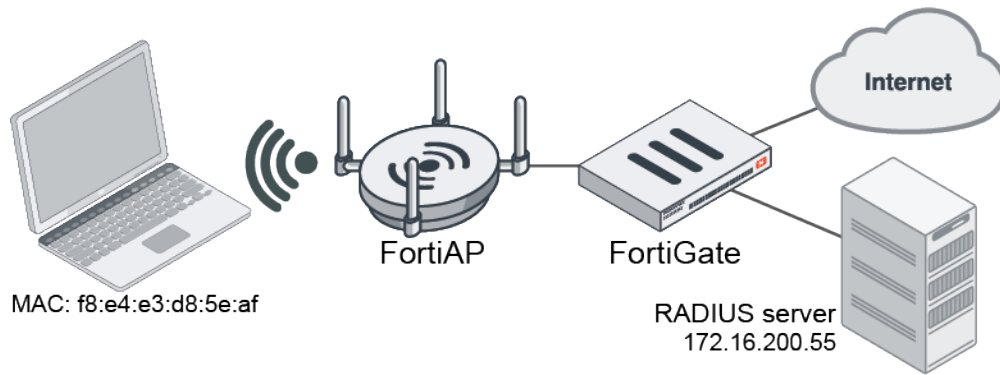
config wireless-controller vap
  edit <name>
    set radius-mac-auth enable
    set radius-mac-auth-server <server>
    set mpsk-profile <profile>
    set radius-mac-mpsk-auth enable
    set radius-mac-mpsk-timeout <timeout>
  next
end

```

<code>radius-mac-mpsk-auth</code> {enable disable}	Enable/disable RADIUS-based MAC authentication of clients for MPSK authentication (default = disable).
<code>radius-mac-mpsk-timeout</code> <timeout>	RADIUS MAC MPSK cache timeout interval, in seconds (1800 - 864000, default = 86400).

Authentication can happen dynamically, and be offloaded to the RADIUS server. Two pieces of information are needed for authentication: the client MAC address and the passphrase (PSK).

The user registers to the RADIUS server, where the client MAC is stored and a passphrase is generated for the user device or group. When the user connects to the FortiAP SSID using WPA-Personal, the FortiGate wireless controller dynamically authenticates the device with its client MAC address, using RADIUS based MAC authentication. The RADIUS server returns a Tunnel-Password for that user device or group. If the client provided a passphrase that matches the Tunnel-Password, the client will successfully authenticate to the SSID, and be placed into a VLAN if one was specified.



In these examples, the RADIUS server (172.16.200.55) has a record for device MAC F8-E4-E3-D8-5E-AF with Tunnel-Password 111111111111.

In the first example, the client connects to the SSID wifi-ssid.fap.01 in tunnel mode, so the MPSK key is cached on the FortiGate. In the second example, the client connects to the SSID wifi-ssid.fap.02 in bridging mode, so the MPSK key is cached on the FortiAP.

To configure the RADIUS server and MPSK profiles for the examples:

1. Configure the RADIUS server:

```
config user radius
  edit "peap"
    set server "172.16.200.55"
    set secret *****
  next
end
```

2. Configure the MPSK profiles:

```
config wireless-controller mpsk-profile
  edit "wifi.fap.01"
    set ssid "wifi-ssid.fap.01"
    config mpsk-group
      edit "g1"
        config mpsk-key
          edit "p1"
            set passphrase *****
            set mpsk-schedules "always"
          next
        end
      next
    end
  next
end
next
edit "wifi.fap.02"
  set ssid "wifi-ssid.fap.02"
  config mpsk-group
    edit "g1"
      config mpsk-key
        edit "p1"
          set passphrase *****
          set mpsk-schedules "always"
        next
      end
    next
  end
end
```



```

        end
      next
    end
  next
end

```

The static passphrase is a dummy passphrase that should have enough complexity that it cannot be guessed. It can be used by the wireless client connect, but is not required as this solution uses dynamic passphrases that are stored on the RADIUS server.

3. After a successful authentication, the PMK values from the RADIUS server are cached on the FortiGate:

```

show wireless-controller mpsk-profile
edit "wifi.fap.01"
  set ssid "wifi-ssid.fap.01"
  config mpsk-group
    edit "g1"
      config mpsk-key
        edit "p1"
          set passphrase ENC
CC7uRvXBDCe4...8hPjCk0IYu4GubkQ/DNzKrU8siLowIAvMZ9GasXkUAryFga5jsxA==
          set pmk ENC
ISI6o9moiCjkGN...43eeWB8KnaJcEwWBSrHbZauul5qPihVazE7MMjfwb8clh7RL5dzasQ==
          set mpsk-schedules "always"
        next
      end
    next
  end
next
edit "wifi.fap.02"
  set ssid "wifi-ssid.fap.02"
  config mpsk-group
    edit "g1"
      config mpsk-key
        edit "p1"
          set passphrase ENC
TIF73K91DV0MxC...6Ob5ZCjU81T/saK6QTjDJVGG8I8NbVcbthgxSq2GrMmrpOcio2Q==
          set pmk ENC
q7ep1EVvCS4WO+B2...xFUgpZzxpX+N2U0duCn1rHwpr52ooEnZ1r1/m5aotyENms56wrH6g==
          set mpsk-schedules "always"
        next
      end
    next
  end
next
end

```

To configure and test the first example, in tunnel mode:

1. Configure the wireless controller VAP:

```

config wireless-controller vap
edit "wifi.fap.01"
  set ssid "wifi-ssid.fap.01"
  set radius-mac-auth enable
  set radius-mac-auth-server "peap"
  set radius-mac-mpsk-auth enable

```

```

        set radius-mac-mpsk-timeout 1800
        set schedule "always"
        set mpsk-profile "wifi.fap.01"
    next
end

```

2. On the RADIUS server, set the Tunnel-Password attribute in the device's account:

```

F8-E4-E3-D8-5E-AF Cleartext-Password := "F8-E4-E3-D8-5E-AF"
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-Id = 100,
Tunnel-Password = "111111111111",
Fortinet-Group-Name = group_mac

```

3. On a wireless endpoint, connect to the wifi.fap.01 SSID using WPA2-personal with the same passphrase as the Tunnel-Password, then confirm that the client (MAC f8:e4:e3:d8:5e:af) can connect to the SSID in tunnel mode:

```

# diagnose wireless-controller wlaac -d sta online
vf=1 wtp=7 rId=2 wlan=wifi.fap.01 vlan_id=0 ip=10.10.80.2 ip6:::
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user=F8-E4-E3-D8-5E-AF group=group_
mac signal=-33 noise=-95 idle=3 bw=1 use=6 chan=149 radio_type=11AX_5G security=wpa2_
only_personal mpsk= encrypt=aes cp_authed=no online=yes mimo=2
rad_mac_auth=allow age=12

```

4. Verify that the RADIUS MPSK is cached on the FortiGate:

```

# diagnose wpa wpad radius-mac-mpsk wifi-ssid.fap.01
SSID config: SSID(wifi-ssid.fap.01) VAP(wifi.fap.01) refcnt(1)
Total RADIUS MPSK cache count: (1)
    mac-binding: f8:e4:e3:d8:5e:af
    vlan-id: 100
    expiration: 1785 seconds

```

To configure and test the second example, in bridge mode:

1. Configure the wireless controller VAP:

```

config wireless-controller vap
    edit "wifi.fap.02"
        set ssid "wifi-ssid.fap.02"
        set radius-mac-auth enable
        set radius-mac-auth-server "peap"
        set radius-mac-mpsk-auth enable
        set radius-mac-mpsk-timeout 1800
        set local-standalone enable
        set local-bridging enable
        set local-authentication enable
        set schedule "always"
        set mpsk-profile "wifi.fap.02"
    next
end

```

2. On a wireless endpoint, connect to the wifi.fap.02 SSID using WPA2-personal, then confirm that the client (MAC f8:e4:e3:d8:5e:af) can connect to the local-standalone SSID with the same passphrase as the Tunnel-Password:

```

FortiAP-231F # sta
wlan11 (wifi-ssid.fap.02) client count 1
MAC:f8:e4:e3:d8:5e:af ip:10.100.100.231 ip_proto:dhcp ip_age:74 host:fosqa-

```

```
PowerEdge-R210 vci:
  vlanid:0 Auth:Yes channel:149 rate:48Mbps rssi:65dB idle:11s
  Rx bytes:6095 Tx bytes:1719 Rx rate:87Mbps Tx rate:48Mbps Rx last:11s Tx
last:68s
  AssocID:1 Mode: Normal Flags:1000000b PauseCnt:0
```

3. Verify that the RADIUS MPSK is cached on the FortiAP:

```
FortiAP-231F # h_diag radius-mac-mpsk wifi-ssid.fap.02
SSID config: SSID(wifi-ssid.fap.02) VAP(wlan11) refcnt(1)
Total RADIUS MPSK cache count: (1)
  mac-binding: f8:e4:e3:d8:5e:af
  vlan-id: 100
  expiration: 1660 seconds
```



Dynamic VLAN is not configured on either of the VAPs, so the FortiGate does not use the VLAN passed by the RADIUS server, but still caches it. Consequently, the cache and station statistics show different VLAN IDs.

FQDN for FortiPresence server IP address in FortiAP profiles - 7.0.2

When defining the FortiPresence server for location based services, the server address can be configured as an FQDN. This means that the wireless controller configuration does not need to be changed when the FortiPresence server IP address changes but it keeps the same domain name.

To configure a wireless controller profile with a FortiPresence server FQDN:

```
config wireless-controller wtp-profile
  edit "FAP431F-default"
    config lbs
      set fortipresence foreign
      set fortipresence-server-addr-type fqdn
      set fortipresence-server-fqdn "test.fortipresence.com"
      set fortipresence-port 10443
    end
  next
end
```

To verify that FortiAP receives the FortiPresence server domain name and resolves the IP address:

```
FortiAP-431F # wcfg
WTP Configuration
  name          : FortiAP-431F
  ...
  fsm-state     : RUN 75
  wtp-ip-addr   : 10.19.20.20:5246 - 10.19.20.20:53582
  ac-ip-addr    : 172.18.56.42:5246 - 172.18.56.42:5247      STATIC
  ...
  fortipresence : foreign, ble enabled, rogue disabled, unassoc_sta enabled, freq
30
                  server 0172.16.200.133(test.fortipresence.com):10443 secret csum
[0xc6a7] project [fortipresence]
```

```
LAN mode           : WAN LAN, ESL
...
```

Wi-Fi Alliance Hotspot 2.0 Release 3 support - 7.0.2

FortiOS supports Wi-Fi Alliance Hotspot 2.0 Release 3. The release version can be configured in the wireless control hotspot profile.

Six new hotspot profile options are available:

release	Hotspot 2.0 Release number (1, 2, 3, default = 2).
venue-url	Venue name.
oper-icon	Operator icon.
advice-of-charge	Advice of charge.
osu-provider-nai	Online sign up (OSU) provider network access identifier (NAI).
terms-and-conditions	Terms and conditions.

To configure wireless controller hotspot 2.0 hs-profile related settings:

```
config wireless-controller hotspot20 hs-profile
  edit "profile1"
    set release 3
    set venue-url "venue-ubr-config1"
    set oper-icon "icon-orange"
    set advice-of-charge "aoc1"
    set osu-provider-nai "osu_nai1"
    set terms-and-conditions "tc-1"
  next
end

config wireless-controller hotspot20 anqp-venue-url
  edit "venue-ubr-config1"
    config value-list
      edit 1
        set number 1
        set value "https://venue-server.r2m-testbed.wi-fi.org/floorplans/index.html"
      next
    end
  next
end

config wireless-controller hotspot20 icon
  edit "icon-orange"
    config icon-list
      edit "icon_orange_zxx.png"
        set lang "zxx"
        set file "icon_orange_zxx.png"
        set width 128
        set height 61
      next
    end
  end
```

```
        next
    end

    config wireless-controller hotspot20 h2qp-advice-of-charge
        edit "aoc1"
            config aoc-list
                edit "list1"
                    config plan-info
                        edit "plan1"
                            set lang "ENG"
                            set currency "USD"
                            set info-file "time_plan1"
                        next
                    end
                next
            end
        end
    next
end

config wireless-controller hotspot20 h2qp-osu-provider-nai
    edit "osu_nai"
        config nai-list
            edit "nai1"
                set osu-nai "anonymous@hotspot.net"
            next
        end
    next
end

config wireless-controller hotspot20 h2qp-terms-and-conditions
    edit "tc-1"
        set filename "tandc-id1-content.txt"
        set timestamp 13578042
        set url "https://tandc-server.r2m-testbed.wi-fi.org"
    next
end
```

To verify the hotspot profile:

```
# diagnose wireless-controller wlac -c hsprof
```

```
HSPROF (003/004) vdom,name: root, profile1
venue url      : venue-ulr-config1
operator icon   : icon-orange
advice of charge : aoc1
osu provider nai : osu_nai
terms and conditions : tc-1
wlan cnt       : 2
vap 001 : 0     ssid_wpa3_en
vap 002 : 0     ssid_ent
```

To enable OSEN as part of key management in a WPA2/WPA3 enterprise radius authentication SSID:

```
config wireless-controller vap
    edit "ssid_ent"
        set ssid "ssid_ent"
        set security wpa2-only-enterprise
```

```

        set auth radius
        set radius-server "wifi-radius"
        set schedule "always"
        set hotspot20-profile "profile1"
        set osen enable
    next
end

```

To verify the SSID options:

```

# diagnose wireless-controller wlac -c wlan

WLAN (002/003) vdom,name: root, ssid_ent
vlanid          : 0 (auto vlan intf disabled)
hotspot20-profile : profile1
osen            : 1
ssid             : ssid_ent
radius_server    : wifi-radius

```

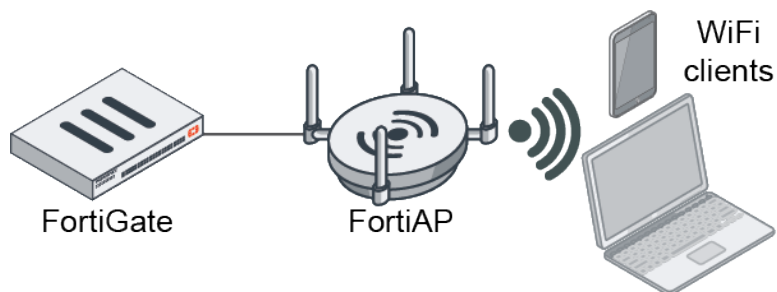
Automatic BSS coloring - 7.0.2

BSS coloring is a mechanism in 802.11ax that enables spatial reuse when overlapping BSS occurs. This can happen when adjacent APs use the same channels and, in the case of BSS coloring, the same color. Automatic Basic Service Set (BSS) coloring can be configured in the FortiGate wireless controller for the FortiAP radios to automatically change colors when BSS coloring conflicts are detected. Automatic BSS coloring is enable by default.

```

config wireless-controller wtp-profile
    edit <profile>
        config <radio>
            set bss-color-mode {auto | static}
        end
    next
end

```



The following configurations show the WTP profiles for a FortiAP U431F that has three radios. The two examples demonstrate using automatic and static BSS coloring to separate the BSS color on the two radios to prevent coloring conflicts.

To configure the FortiAP profile with automatic BSS coloring:

```

config wireless-controller wtp-profile
    edit "FAPU431F-BSS-auto"
        config platform
            set type U431F
        end
    end
end

```

```
end
set handoff-sta-thresh 30
set allowaccess https ssh
config radio-1
    set band 802.11ax-5G
    set vap-all manual
end
config radio-2
    set band 802.11ax,n,g-only
    set vap-all manual
end
config radio-3
    set mode monitor
end
next
end

# diagnose wireless-controller wlac -c wtp PU431F5E19000105 | grep "bss color"
bss color mode      : Auto
bss color mode      : Auto
```

To configure the FortiAP profile with static BSS coloring:

```
config wireless-controller wtp-profile
    edit "FAPU431F-BSS-static"
        config platform
            set type U431F
        end
        set handoff-sta-thresh 30
        set allowaccess https ssh snmp
        config radio-1
            set band 802.11ax-5G
            set bss-color 60
            set bss-color-mode static
            set vap-all manual
        end
        config radio-2
            set band 802.11ax,n,g-only
            set bss-color 50
            set bss-color-mode static
            set vap-all manual
        end
        config radio-3
            set mode monitor
        end
    next
end

# diagnose wireless-controller wlac -c wtp PU431F5E19000105 | grep "bss color"
bss color mode      : Static
bss color           : 60
bss color mode      : Static
bss color           : 50
```

Configure 802.11ax MCS rates - 7.0.2

You can configure 802.11ax specified VAP data rates from the FortiGate wireless controller to cover 802.11ax data rates and modulation schemes that 802.11ac does not support. This feature is currently supported on 802.11ax-capable FAP-U models.

```
config wireless-controller vap
    edit rate-test
        set rates-11ax-ss12 <option_1>, ... <option_n>
        set rates-11ax-ss34 <option_1>, ... <option_n>
    next
end
```

rates-11ax-ss12	<p>Set allowed data rates for 802.11ax with one or two spatial streams.</p> <p>The following options are available: mcs0/1, mcs1/1, mcs2/1, mcs3/1, mcs4/1, mcs5/1, mcs6/1, mcs7/1, mcs8/1, mcs9/1, mcs10/1, mcs11/1, mcs0/2, mcs1/2, mcs2/2, mcs3/2, mcs4/2, mcs5/2, mcs6/2, mcs7/2, mcs8/2, mcs9/2, mcs10/2, and mcs11/2.</p>
rates-11ax-ss34	<p>Set allowed data rates for 802.11ax with three or four spatial streams.</p> <p>The following options are available: mcs0/3, mcs1/3, mcs2/3, mcs3/3, mcs4/3, mcs5/3, mcs6/3, mcs7/3, mcs8/3, mcs9/3, mcs10/3, mcs11/3, mcs0/4, mcs1/4, mcs2/4, mcs3/4, mcs4/4, mcs5/4, mcs6/4, mcs7/4, mcs8/4, mcs9/4, mcs10/4, and mcs11/4.</p>

In the following example, a FAP-U431F is configured with 802.11ax data rates.

To configure the data rates:

1. Configure the VAP:

```
config wireless-controller vap
    edit rate-test
        set rates-11ax-ss12 mcs1/1 mcs3/1 mcs5/1 mcs6/2 mcs8/2 mcs10/2
        set rates-11ax-ss34 mcs1/3 mcs5/3 mcs7/3 mcs2/4 mcs8/4 mcs10/4
    next
end
```

2. Verify the configuration in FortiAP:

```
# vcfg
-----VAP Configuration      1-----
...
Rates Configuration:
    11a_rate_set=No_data_rate_is_configured
    11n_rate_set=No_data_rate_is_configured
    11ac_rate_set=No_data_rate_is_configured

    11ax_rate_set=mcs1/1,mcs3/1,mcs5/1,
                  mcs6/2,mcs8/2,mcs10/2,
                  mcs1/3,mcs5/3,mcs7/3,
                  mcs2/4,mcs8/4,mcs10/4,
    ...
```


Switch controller

This section includes information about switch controller related new features:

- [FortiSwitch NAC VLANs widget on page 588](#)
- [Forward error correction settings on switch ports on page 571](#)
- [Cancel pending or downloading FortiSwitch upgrades on page 572](#)
- [Automatic provisioning of FortiSwitch firmware upon authorization on page 574](#)
- [Use wildcards in a MAC address in a NAC policy on page 590](#)
- [Additional FortiSwitch recommendations in Security Rating on page 576](#)
- [FortiGate NAC engine optimization on page 592](#)
- [PoE pre-standard detection disabled by default on page 577](#)
- [Cloud icon indicates that the FortiSwitch unit is managed over layer 3 on page 577](#)
- [GUI support for viewing and configuring shared FortiSwitch ports on page 578](#)
- [Dynamic port profiles for FortiSwitch ports on page 598](#)
- [GUI updates for the switch controller on page 601](#)
- [Ability to re-order FortiSwitch units in the Topology view 7.0.1 on page 579](#)
- [Support of the DHCP server access list 7.0.1 on page 581](#)
- [SNMP OIDs added for switch statistics and port status 7.0.1 on page 583](#)
- [Display port properties of managed FortiSwitch units 7.0.1 on page 584](#)
- [IGMP-snooping querier and per-VLAN IGMP-snooping proxy configuration 7.0.2 on page 584](#)
- [Managing DSL transceivers \(FN-TRAN-DSL\) 7.0.2 on page 586](#)

Forward error correction settings on switch ports

Supported managed-switch ports can be configured with a forward error correction (FEC) state of Clause 74 FC-FEC for 25-Gbps ports and Clause 91 RS-FEC for 100-Gbps ports.

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    config ports
      edit <port_name>
        set fec-capable {0 | 1}
        set fec-state {disabled | c174 | c191}
      next
    end
  next
end
```

```
fec-capable {0 | 1}
```

Set whether the port is FEC capable.

- 0: The port is not FEC capable.
- 1: The port is FEC capable.

```
fec-state {disabled |
  c174 | c191}
```

Set the FEC state:

- disabled: Disable FEC on the port.
- c174: Enable Clause 74 FC-FEC. This option is only available for 25Gbps ports.

- **c191:** Enable Clause 91 RS-FEC. This option is only available for 100Gbps ports.

In this example, a FortiSwitch 3032E that is managed by the FortiGate device is configured with Clause 74 FC-FEC on port 16.1 and Clause 91 RS-FEC on port 8.

To configure FEC on the switch ports:

```
config switch-controller managed-switch
  edit FS3E32T419000000
    config ports
      edit port16.1
        set fec-state cl74
      next
      edit port8
        set fec-state cl91
      next
    end
  next
end
```

Cancel pending or downloading FortiSwitch upgrades

A FortiSwitch device in FortiLink mode can be upgrade using the FortiGate device.

If a connectivity issue occurs during the upgrade process and the FortiSwitch unit loses contact with the FortiGate device, the FortiSwitch upgrade status can get stuck at Upgrading. Use the following CLI command to cancel the process:

```
execute switch-controller switch-software cancel {all | sn <FortiSwitch_serial_number> |
switch-group <switch_group_ID>}
```

To test canceling a failed FortiSwitch upgrade process:

1. Check that there is at least one FortiSwitch unit in FortiLink mode on the FortiGate device:

```
# execute switch-controller get-conn-status
Managed-devices in current vdom vdom1:
```

```
FortiLink interface : flink
```

SWITCH-ID	NAME	VERSION	STATUS	FLAG	ADDRESS	JOIN-TIME
FS1D243Z170000XX	13:51:11 2020	v6.4.0 (456)	Authorized/Up	E	169.254.1.3	Fri Nov 27
S248DN3X170002XX	13:50:56 2020	v6.4.0 (456)	Authorized/Up	E	169.254.1.6	Fri Nov 27
S248EPTF180018XX	13:51:05 2020	v6.4.0 (456)	Authorized/Up	E	169.254.1.5	Fri Nov 27

```
Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config
sync error, 3=L3
```

```
Managed-Switches: 5 (UP: 4 DOWN: 1)
```

2. Confirm that the upgrade status of the FortiSwitch units is normal:

```
# execute switch-controller get-upgrade-status
Device      Running-version      Status
Next-boot

=====
=====
VDOM : vdom1
      FS1D243Z170000XX  FS1D24-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248DN3X170002XX  S248DN-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248EPTF180018XX  S248EP-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
```

3. Upload the FortiSwitch image to the FortiGate device and confirm that it was uploaded successfully:

```
# execute switch-controller switch-software upload tftp FSW-248E-POE-454.out
172.18.60.160

Downloading file FSW-248E-POE-454.out from tftp server 172.18.60.160...
#####
Image checking ...
Image MD5 calculating ...
Image Saving S248EP-IMG.swtp ...
Successful!

File Syncing...

# execute switch-controller switch-software list-available

ImageName      ImageSize(B)  ImageInfo      Uploaded Time
S248EP-IMG.swtp 28579517      S248EP-v6.4-build454  Fri Nov 27 14:01:24 2020
```

4. Start the FortiSwitch upgrade process:

```
# execute switch-controller switch-software upgrade S248EPTF180018XX S248EP-IMG.swtp
Image download process: 11 %
```

5. Check the FortiSwitch upgrade process:

```
# execute switch-controller get-upgrade-status
Device      Running-version      Status
Next-boot

=====
=====
VDOM : vdom1
      FS1D243Z170000XX  FS1D24-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248DN3X170002XX  S248DN-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248EPTF180018XX  S248EP-v6.4.0-build456,201121 (Interim)      (14/0/0)  N/A
(Upgrading)
```

6. On the FortiSwitch unit, shut down the physical port that is used by FortiLink, in this case port 17:

```
config switch physical-port
  edit port17
    set status down
```

```

    next
end

```

7. On the FortiGate device, recheck the FortiSwitch upgrade process:

```

# execute switch-controller get-upgrade-status
Device      Running-version      Status
Next-boot

=====
=====
VDM : vdom1
      FS1D243Z170000XX  FS1D24-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248DN3X170002XX  S248DN-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248EPTF180018XX  S248EP-v6.4.0-build456,201121 (Interim)      (14/0/0)  N/A
(Upgrading)

```

Note that the process is stuck on Upgrading.

8. Cancel the upgrade process:

```
execute switch-controller switch-software cancel sn S248EPTF180018XX
```

9. Confirm that the upgrade status of the FortiSwitch units is back to normal:

```

# execute switch-controller get-upgrade-status
Device      Running-version      Status
Next-boot

=====
=====
VDM : vdom1
      FS1D243Z170000XX  FS1D24-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248DN3X170002XX  S248DN-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)
      S248EPTF180018XX  S248EP-v6.4.0-build456,201121 (Interim)      (0/0/0)  N/A
(Idler)

```

Automatic provisioning of FortiSwitch firmware upon authorization

FortiSwitch firmware images can be automatically provisioned after authorization. After a FortiSwitch unit is authorized by FortiLink, its firmware is upgraded to the version provisioned by the administrator.

On FortiGate models that have a hard disk, up to four images for the same FortiSwitch model can be uploaded. For FortiGate models without a hard disk, only one image can be uploaded for each FortiSwitch model.

To configure the automatic provisioning:

```

config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    set firmware-provision {enable | disable}
    set firmware-provision-version <version>
  next
end

```

firmware-provision {enable disable}	Enable or disable provisioning firmware to the FortiSwitch unit after authorization (the default is disable).
firmware-provision-version <version>	The firmware version to provision the FortiSwitch unit with on bootup. The format is major_version.minor_version.build_number, for example, 6.4.0454.

Example

In this example, a FortiSwitch 248E-POE is upgraded from FortiSwitchOS 6.4.3 to 6.4.4.

To configure automatic provisioning and upgrade the FortiSwitch firmware after authorization:

1. Upload the FortiSwitch image to the FortiGate device and confirm that it was uploaded successfully:

```
# execute switch-controller switch-software upload tftp 248-454.out 172.18.60.160

Downloading file 248-454.out from tftp server 172.18.60.160...
#####
Image checking ...
Image MD5 calculating ...
Image Saving S248EP-IMG.swtp ...
Successful!

File Syncing...

# execute switch-controller switch-software list-available

ImageName                      ImageSize(B)  ImageInfo                      Uploaded Time
S248EP-v6.4-build454-IMG.swtp  28579517     S248EP-v6.4-build454          Mon Nov 30
15:06:07 2020
```

2. On the FortiSwitch unit, check the current version:

```
# get system status
Version: FortiSwitch-248E-POE v6.4.3,build0452,201029 (GA)
Serial-Number: S248EPTF18001842
BIOS version: 04000004
System Part-Number: P22169-02
Burn in MAC: 70:4c:a5:e1:53:f6
Hostname: S248EPTF18001842
Distribution: International
Branch point: 452
System time: Wed Dec 31 16:11:17 1969
```

3. On the FortiSwitch unit, change the management mode to FortiLink:

```
config system global
    set switch-mgmt-mode fortilink
end
```

4. On the FortiGate device, enable firmware provisioning and specify the version:

```
config switch-controller managed-switch
    edit S248EPTF18000000
        set firmware-provision enable
        set firmware-provision-version 6.4.0454
```

```

    next
end

```

5. On the FortiGate device, authorize the FortiSwitch unit:

```

config switch-controller managed-switch
    edit S248EPTF18000000
        set fsw-wan1-peer flink
        set fsw-wan1-admin enable
    next
end

```

6. When the authorized FortiSwitch unit is in FortiLink mode, it automatically starts upgrading to the provisioned firmware:

```

# execute switch-controller get-upgrade-status

```

Device	Running-version	Status
Next-boot		
=====		
=====		
VDOM : vdom1		
FS1D243Z170000XX	FS1D24-v6.4.0-build456,201121 (Interim)	(0/0/0) N/A
(Idle)		
S248DN3X170002XX	S248DN-v6.4.0-build456,201121 (Interim)	(0/0/0) N/A
(Idle)		
S248EPTF18000000	S248EP-v6.4.3-build452,201029 (GA)	(14/0/0) N/A
(Upgrading)		

7. Check the version when the upgrade is complete:

```

# execute switch-controller get-conn-status
Managed-devices in current vdom vdom1:

```

FortiLink interface : flink	SWITCH-ID	VERSION	STATUS	FLAG	ADDRESS	JOIN-TIME
	NAME					
	FS1D243Z17000032	v6.4.0 (456)	Authorized/Up	-	169.254.1.3	Mon Nov 30
	11:08:10 2020	-				
	S248DN3X170002XX	v6.4.0 (456)	Authorized/Up	-	169.254.1.4	Mon Nov 30
	11:08:32 2020	-				
	S248EPTF18000000	v6.4.4 (454)	Authorized/Up	C	169.254.1.6	Mon Nov 30
	15:20:53 2020	-				

Additional FortiSwitch recommendations in Security Rating

Three new tests have been added to the FortiSwitch recommendations in the *Security Fabric > Security Rating* page to help optimize your network:

- Check if the quarantine bounce port option is enabled.
- Check if the PoE status of the switch controller auto-config default policy is enabled.
- Check if PoE pre-standard detection for all user ports is enabled.

PoE pre-standard detection disabled by default

Starting with this version, the factory default setting for power over Ethernet (PoE) pre-standard detection is `disable` for both managed and standalone FortiSwitch units.

Depending on the FortiSwitch model, you can manually change the `poe-pre-standard-detection` setting on the global level or on the port level.



PoE pre-standard detection is a global setting for the following FortiSwitch models: FSR-112D-POE, FS-548DFPOE, FS-524D-FPOE, FS-108D-POE, FS-224D-POE, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, and FS-124EFPOE. For the other FortiSwitch PoE models, PoE pre-standard detection is set on each port.

On the global level, set `poe-pre-standard-detection` with the following commands:

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    set poe-pre-standard-detection {enable | disable}
  next
end
```

On the port level, set `poe-pre-standard-detection` with the following commands:

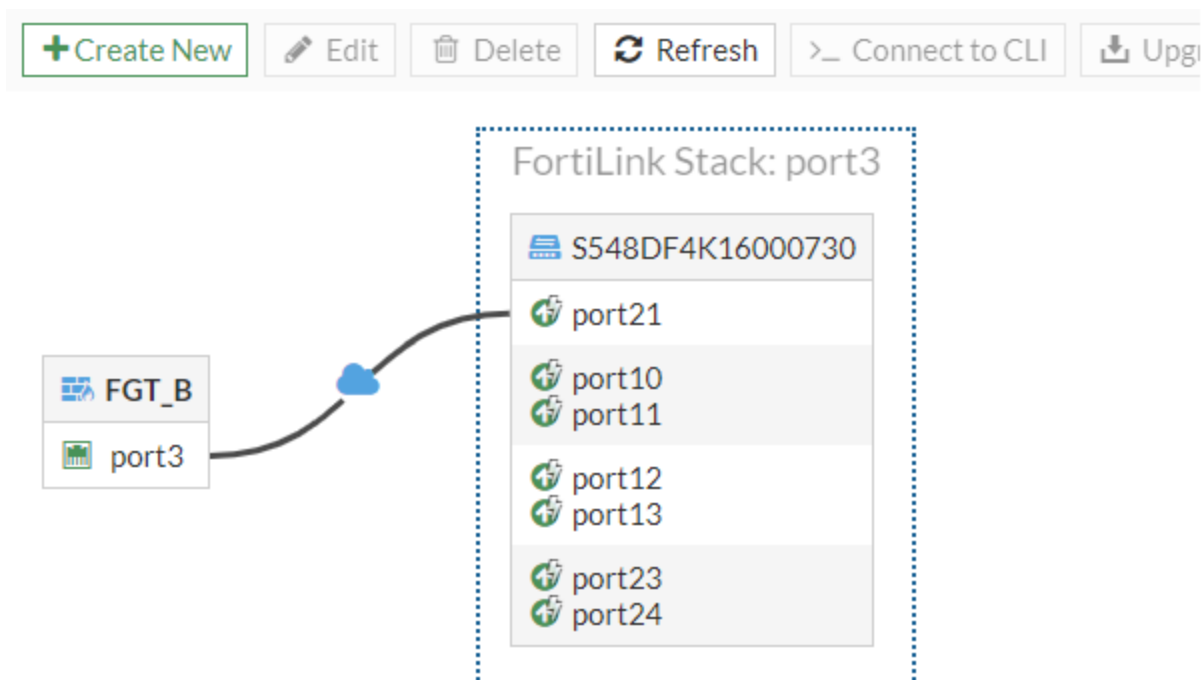
```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    config ports
      edit <port_name>
        set poe-pre-standard-detection {enable | disable}
      next
    end
  next
end
```

When you upgrade FortiOS, the setting of `poe-pre-standard-detection` stays the same. When you downgrade from FortiOS 6.4 to FortiOS 6.2, the setting of `poe-pre-standard-detection` stays the same. The setting of `poe-pre-standard-detection` might change during a downgrade from FortiOS 7.0 to FortiOS 6.4.

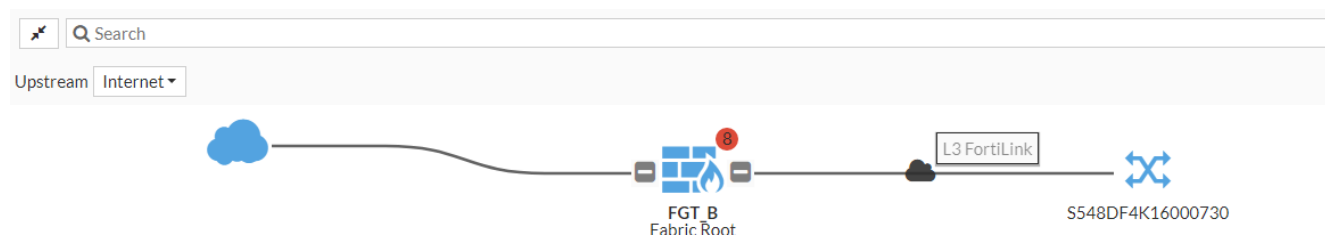
Cloud icon indicates that the FortiSwitch unit is managed over layer 3

A new cloud icon indicates when the FortiSwitch unit is being managed over layer 3. The cloud icon is displayed in two places in the GUI.

Go to *WiFi & Switch Controller > Managed FortiSwitch* and select *Topology*. In the following figure, the cloud icon over the connection line indicates that S548DF4K16000730 is being managed over layer 3.



Go to *Security Fabric > Physical Topology*. In the following figure, the cloud icon over the connection line indicates that S548DF4K16000730 is being managed over layer 3.



GUI support for viewing and configuring shared FortiSwitch ports

You can now use the GUI to view and configure FortiSwitch ports that are shared between VDOMs. To share FortiSwitch ports between VDOMs, you must use the CLI.

One use case for this feature is to have each VDOM dedicated to a separate tenant with a single administrator managing all VDOMs.

Go to *WiFi & Switch Controller > FortiSwitch Ports* to view the shared FortiSwitch ports and edit them.

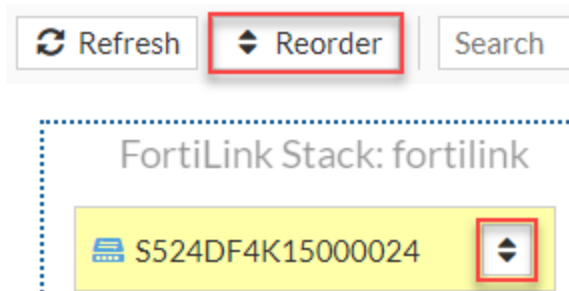
Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information
port6				vlan_tenant		Powered	00:0c:29:a9:12:74
port7				vlan_tenant	vlan_lab	Powered	
port8				vlan_voice		Powered	
port11				vlan_voice		Powered 6.10W	Android
port25				vlan_tenant			

Ability to re-order FortiSwitch units in the Topology view - 7.0.1

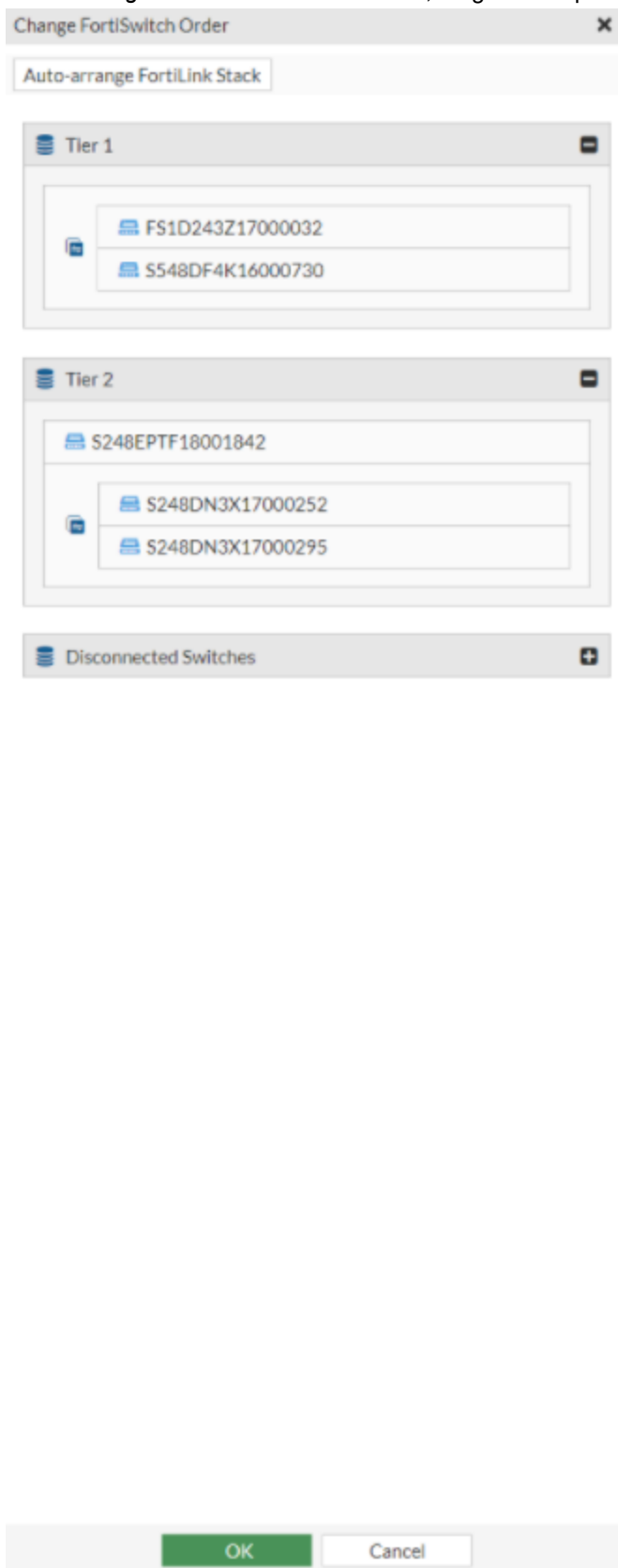
You can now change the order in which FortiSwitch units are displayed in the Topology view.

To rearrange the FortiSwitch units in the GUI:

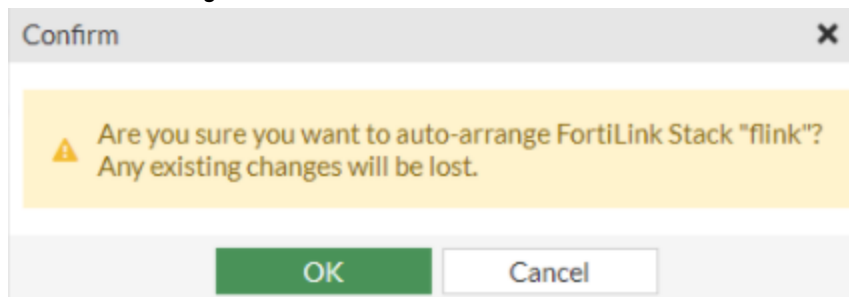
1. Go to *WiFi & Switch Controller > Managed FortiSwitches*.
2. In the *View* dropdown list, select *Topology*.
3. Click *Reorder* or the double-arrow button next to the FortiSwitch serial number.



4. In the *Change FortiSwitch Order* window, drag-and-drop each FortiSwitch unit to change the order.



5. If you want FortiOS to determine the arrangement with the fewest edge crossings, click *Auto-arrange FortiLink Stack* in the *Change FortiSwitch Order* window and then click *OK* in the *Confirm* window.



To rearrange the FortiSwitch units in the FortiOS CLI:

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    move <FortiSwitch_serial_number1> before <FortiSwitch_serial_number2>
  next
end
```

FortiSwitch_serial_number1 is now listed above FortiSwitch_serial_number2.

Support of the DHCP server access list - 7.0.1

You can now configure in FortiOS which DHCP servers that DHCP snooping includes in the server access list. These servers on the list are allowed to respond to DHCP requests.

NOTE: You can add 255 servers per table. The maximum number of DHCP servers that can be added to all instances of the table is 2,048. This maximum is a global limit and applies across all VLANs.

Configuring the DHCP server access list consists of the following steps:

1. Enable the DHCP server access list on a VDOM level or switch-wide level.
By default, the server access list is disabled, which means that all DHCP servers are allowed. When the server access list is enabled, only the DHCP servers in the server access list are allowed.
2. Configure the VLAN settings for the managed switch port.
You can set the DHCP server access list to `global` to use the VDOM or system-wide setting, or you can set the DHCP server access list to `enable` to override the global settings and enable the DHCP server access list.
In the managed FortiSwitch unit, all ports are untrusted by default, and DHCP snooping is disabled on all untrusted ports. You must set the managed switch port to be trusted to allow DHCP snooping.
3. Configure DHCP snooping and the DHCP access list for the managed FortiSwitch interface.
By default, DHCP snooping is disabled on the managed FortiSwitch interface.

To enable the DHCP sever access list on a global level:

```
config switch-controller global
  set dhcp-server-access-list enable
end
```

For example:

```
FGT_A (vdom1) # config switch-controller global
FGT_A (global) # set dhcp-server-access-list enable
FGT_A (global) # end
```

To configure the VLAN settings:

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    set dhcp-server-access-list {global | enable | disable}
  config ports
    edit <port_name>
      set vlan <VLAN_name>
      set dhcp-snooping trusted
    next
  end
next
end
```

For example:

```
config switch-controller managed-switch
  edit "S524DN4K16000116"
    set fsw-wan1-peer "port11"
    set fsw-wan1-admin enable
    set dhcp-server-access-list enable
  config ports
    edit "port19"
      set vlan "_default.13"
      set allowed-vlans "quarantine.13"
      set untagged-vlans "quarantine.13"
      set dhcp-snooping trusted
      set export-to "vdom1"
    next
  end
next
end
```

To configure the interface settings:

```
config system interface
  edit <VLAN_name>
    set switch-controller-dhcp-snooping enable
  config dhcp-snooping-server-list
    edit <DHCP_server_name>
      set server-ip <IPv4_address_of_DHCP_server>
    next
  end
next
end
```

For example:

```
config system interface
  edit "_default.13"
    set vdom "vdom1"
    set ip 5.4.4.1 255.255.255.0
    set allowaccess ping https ssh http fabric
    set alias "_default.port11"
    set snmp-index 30
    set switch-controller-dhcp-snooping enable
  config dhcp-snooping-server-list
    edit "server1"
      set server-ip 10.20.20.1
```

```

        next
    end
    set switch-controller-feature default-vlan
    set interface "port11"
    set vlanid 1
next
end

```

SNMP OIDs added for switch statistics and port status - 7.0.1

Three SNMP OIDs have been added to the FortiOS enterprise MIB 2 tables. They report the FortiSwitch port status and FortiSwitch CPU and memory statistics.

SNMP OID	Description
fgSwDeviceInfo.fgSwDeviceTable.fgSwDeviceEntry.fgSwDeviceEntry.fgSwCpu 1.3.6.1.4.1.12356.101.24.1.1.1.11	Percentage of the CPU being used.
fgSwDeviceInfo.fgSwDeviceTable.fgSwDeviceEntry.fgSwDeviceEntry.fgSwMemory 1.3.6.1.4.1.12356.101.24.1.1.1.12	Percentage of memory being used.
fgSwPortInfo.fgSwPortTable.fgSwPortEntry.fgSwPortStatus 1.3.6.1.4.1.12356.101.24.2.1.1.6	Whether a managed FortiSwitch port is up or down.

These OIDs require FortiSwitchOS 7.0.0 or higher. FortiLink and SNMP must be configured on the FortiGate device.

FortiSwitch units update the CPU and memory statistics every 30 seconds. This interval cannot be changed.

FortiOS versions 6.4.2 through 7.0.0 show the port status in the configuration management database (CMDB) for managed ports; FortiOS 7.0.1 and higher show the link status that has been retrieved from the switch port as the port status for managed ports.

Sample queries

To find out how much CPU is being used on a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```

root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
1.3.6.1.4.1.12356.101.24.1.1.1.11.2.8.17000032

```

To find out how much memory is being used on a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```

root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
1.3.6.1.4.1.12356.101.24.1.1.1.12.2.8.17000032

```

To find out the status of port1 of a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```

root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
1.3.6.1.4.1.12356.101.24.2.1.1.6.2.8.17000032.1

```

Display port properties of managed FortiSwitch units - 7.0.1

Use the new `diagnose switch-controller switch-info port-properties [<FortiSwitch_serial_number>] [<port_name>]` command to check the port properties of managed FortiSwitch units.

To check the port properties:

```
diagnose switch-controller switch-info port-properties [<FortiSwitch_serial_number>] [<port_name>]
```

If the FortiSwitch serial number is not specified, results for all FortiSwitch units are returned. If the port name is not specified, results for all ports are returned.

For example:

```
FortiGate-100F # diagnose switch-controller switch-info port-properties S524DF4K15000024 port18

Vdom: root
Switch: S524DF4K15000024
Port: port18
    PoE           : 802.3af/at,30.0W
    Connector     : RJ45
    Speed         : 10Mhalf/10Mfull/100Mhalf/100Mfull/1Gauto/auto
```

IGMP-snooping querier and per-VLAN IGMP-snooping proxy configuration - 7.0.2

Before FortiOS 7.0.2, you could use the CLI to enable IGMP proxy on a system-wide basis. Starting in FortiOS 7.0.2, you can use the CLI to enable IGMP proxy per FortiSwitch unit.

Starting in FortiOS 7.0.2, you can configure the IGMP-snooping querier version 2 or 3. When the IGMP querier version 2 is configured, the managed FortiSwitch unit will send IGMP version-2 queries when no external querier is present. When the IGMP querier version 3 is configured, the managed FortiSwitch unit will send IGMP version-3 queries when no external querier is present.

Follow these steps to configure the IGMP-snooping proxy and IGMP-snooping querier:

1. Enabling IGMP snooping and the IGMP-snooping proxy.
2. Configuring the IGMP-snooping querier.

Enabling IGMP snooping and the IGMP-snooping proxy

By default, IGMP snooping is disabled. You need to enable IGMP snooping on the FortiGate device before you can enable the IGMP-snooping proxy.

To enable IGMP snooping and the IGMP-snooping proxy:

```
config system interface
    edit <VLAN_interface>
        set switch-controller-igmp-snooping enable
        set switch-controller-igmp-snooping-proxy enable
    next
end
```

For example, you can enable IGMP snooping and the IGMP-snooping proxy on VLAN 100:

```
config system interface
  edit vlan100
    set switch-controller-igmp-snooping enable
    set switch-controller-igmp-snooping-proxy enable
  next
end
```

Configuring the IGMP-snooping querier

If you have IGMP snooping and the IGMP-snooping proxy enabled on a VLAN, you can then configure the IGMP-snooping querier on the same VLAN on a managed switch. By default, the IGMP-snooping querier is disabled.

You must enable the overriding of the global IGMP-snooping configuration with the `set local-override enable` command.

By default, the maximum time (`aging-time`) that multicast snooping entries without any packets are kept is for 300 seconds. This value can be in the range of 15-3,600 seconds.

By default, `flood-unknown-multicast` is disabled, and unregistered multicast packets are forwarded only to mRouter ports. If you enable `flood-unknown-multicast`, unregistered multicast packets are forwarded to all ports in the VLAN.

The IGMP-snooping proxy uses the global IGMP-snooping configuration by default. You can enable or disable the IGMP-snooping on the VLAN.

You can optionally specify the IPv4 address that IGMP reports are sent to. You can also set the IGMP-snooping querier version. The default IGMP querier version is 2.

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
  config igmp-snooping
    set local-override enable
    set aging-time <15-3600>
    set flood-unknown-multicast {enable | disable}
  config vlans
    edit <VLAN_interface>
      set proxy {disable | enable | global}
      set querier enable
      set querier-addr <IPv4_address>
      set version {2 | 3}
    next
  end
end
end
```

For example:

```
config switch-controller managed-switch
  edit S524DF4K15000024
  config igmp-snooping
    set local-override enable
    set aging-time 1000
    set flood-unknown-multicast enable
  config vlans
    edit vlan100
      set proxy disable
```

```

        set querier enable
        set querier-addr 1.2.3.4
        set version 3
    next
end
end
end

```

Managing DSL transceivers (FN-TRAN-DSL) - 7.0.2

A Procend 180-T DSL transceiver (FN-TRAN-DSL) that is plugged in to a FortiGate-managed FortiSwitch port can now be managed by a FortiGate unit. The management of the DSL transceiver and the FortiSwitch port includes the ability to program the physical-layer attributes on the DSL module, retrieve the status and statistics from the module, upgrade the module's firmware, and reset the module.

You can use the following FortiGate models to manage FN-TRAN-DSL: FG-80F, FG-81F, FG-80F-BP, FGR-60F, FGR-60F-3G4G, FG-60F, and FG-40F-3G4G. The FortiSwitch unit must be running FortiSwitchOS 7.0.1, build 0038 or later. A FortiSwitch unit running in standalone mode cannot program the physical-layer attributes on the DSL module.

To create a DSL policy:

```

config switch-controller dsl policy
  edit <DSL_policy_name>
    set type Procend
    set us-bitswap {enable | disable}
    set ds-bitswap {enable | disable}
    set profile {auto-30a | auto-17a | auto-12ab}
    set cs {A43, B43, A43C, V43}
    set pause-frame {enable | disable}
    set cpe_aele {enable | disable}
    set cpe_aele-mode {ELE_M0 | ELE_DS | ELE_PB | ELE_MIN}
    set append_padding {enable | disable}
  next
end

```

Option	Description	Default value
<DSL_policy_name>	Enter a name for the DSL policy.	No default
type Procend	You can only select the <code>Procend</code> type.	Procend
us-bitswap {enable disable}	Enable or disable whether the upstream bits are exchanged.	enable
ds-bitswap {enable disable}	Enable or disable whether the downstream bits are exchanged.	enable
profile {auto-30a auto-17a auto-12ab}	Select which very-high-bit-rate digital subscriber line (VDSL) customer premises equipment (CPE) profile to use.	auto-30a
cs {A43, B43, A43C, V43}	Select which CPE carrier set to use.	A43 B43 A43C

Option	Description	Default value
pause-frame {enable disable}	Enable or disable device pause frames.	enable
cpe_aele {enable disable}	Enable or disable CPE alternative electrical length estimation (AELE) mode.	enable
cpe_aele-mode {ELE_M0 ELE_DS ELE_PB ELE_MIN}	Select the CPE AELE mode to use.	ELE_MIN
append_padding {enable disable}	Enable or disable whether to append padding.	enable

To specify the DSL policy to use:

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    config ports
      edit <port>
        set dsl-profile <DSL_policy_name>
      next
    end
  next
end
```

To display DSL statistics:

```
get switch-controller dsl link-time <FortiSwitch_serial_number> <port_name>
get switch-controller dsl pkt-count <FortiSwitch_serial_number> <port_name>
get switch-controller dsl pm-line-curr <FortiSwitch_serial_number> <port_name>
get switch-controller dsl policy
get switch-controller dsl rate <FortiSwitch_serial_number> <port_name>
get switch-controller dsl status <FortiSwitch_serial_number> <port_name>
get switch-controller dsl summary <FortiSwitch_serial_number> <port_name>
get switch-controller dsl version <FortiSwitch_serial_number> <port_name>
```

Option	Description
link-time <FortiSwitch_serial_number> <port_name>	Display the link time for the DSL module plugged in to the specified FortiSwitch port.
pkt-count <FortiSwitch_serial_number> <port_name>	Display the packet count for the DSL module plugged in to the specified FortiSwitch port.
pm-line-curr <FortiSwitch_serial_number> <port_name>	Display the line current for the DSL module plugged in to the specified FortiSwitch port.
policy	List the available DSL policies and their settings.
rate <FortiSwitch_serial_number> <port_name>	Display the rate for the DSL module plugged in to the specified FortiSwitch port.

Option	Description
status <FortiSwitch_serial_number> <port_name>	Display the status of the DSL module plugged in to the specified FortiSwitch port.
summary <FortiSwitch_serial_number> <port_name>	Display a summary for the DSL module plugged in to the specified FortiSwitch port.
version <FortiSwitch_serial_number> <port_name>	Display the version of the DSL module plugged in to the specified FortiSwitch port.

To reset the DSL module on a FortiSwitch port:

```
execute switch-controller dsl reset <FortiSwitch_serial_number> <port_name>
```

To upload a FortiSwitch image to the FortiGate local storage:

```
execute switch-controller dsl update ftp <DSL_image_name_on_FTP_server> <FTP_server>[:<FTP_port>] <FTP_user_name> <FTP_password> <FortiSwitch_serial_number> <port_name>
execute switch-controller dsl update tftp <DSL_image_name_on_TFTP_server> <TFTP_server> <FortiSwitch_serial_number> <port_name>
```

NAC

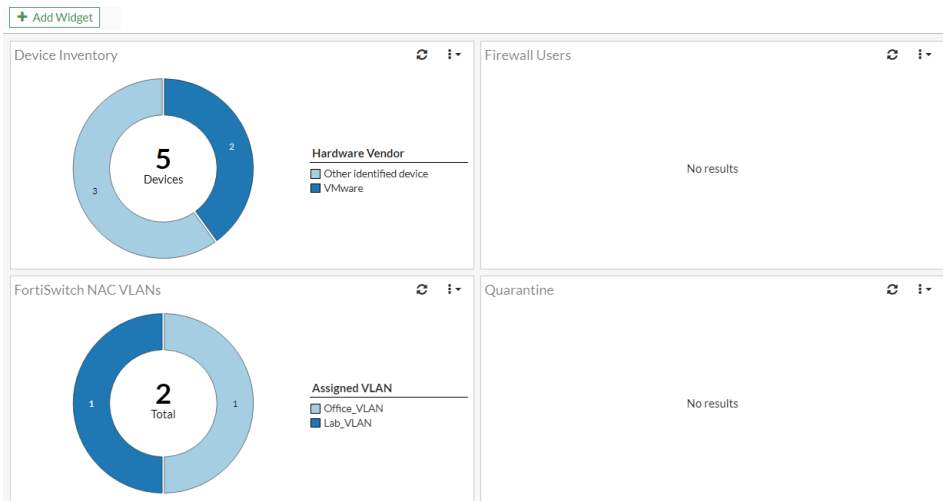
This section includes information about NAC related new features:

- [FortiSwitch NAC VLANs widget on page 588](#)
- [Use wildcards in a MAC address in a NAC policy on page 590](#)
- [FortiGate NAC engine optimization on page 592](#)
- [Wireless NAC support on page 593](#)
- [Dynamic port profiles for FortiSwitch ports on page 598](#)
- [GUI updates for the switch controller on page 601](#)
- [Support dynamic firewall addresses in NAC policies 7.0.1 on page 602](#)
- [NAC LAN segments 7.0.1 on page 605](#)
- [Specify FortiSwitch groups in NAC policies 7.0.2 on page 612](#)

FortiSwitch NAC VLANs widget

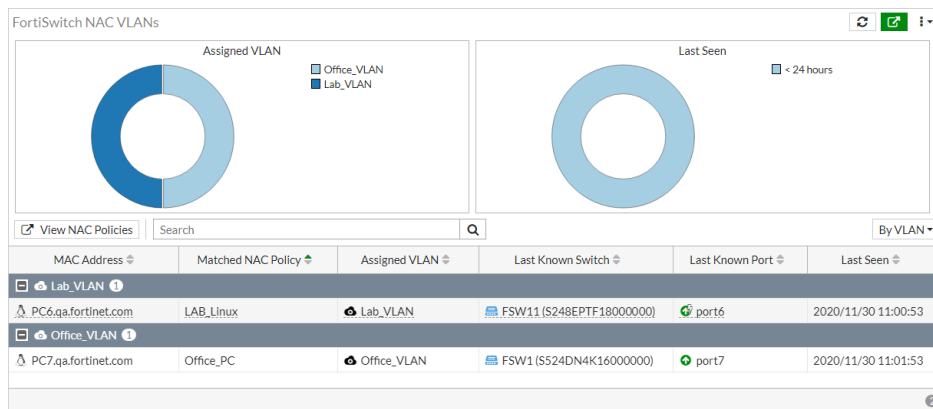
The widget shows a pie chart of the assigned FortiSwitch NAC VLANs. When expanded to the full screen, the widget shows a full list of devices grouped by VLAN, NAC policy, or last seen.

The widget is added to the *Users & Devices* dashboard after a dashboard reset or can be manually added to a dashboard. It can also be accessed by going to *WiFi & Switch Controller > NAC Policies* and clicking *View Matched Devices*.



The expanded view of the widget shows Assigned VLAN and Last Seen pie charts and a full device list. The list can be organized *By VLAN*, *By NAC Policy*, or *By Policy Type*.

Click [View NAC Policies](#) to go to *WiFi & Switch Controller > NAC Policies*.



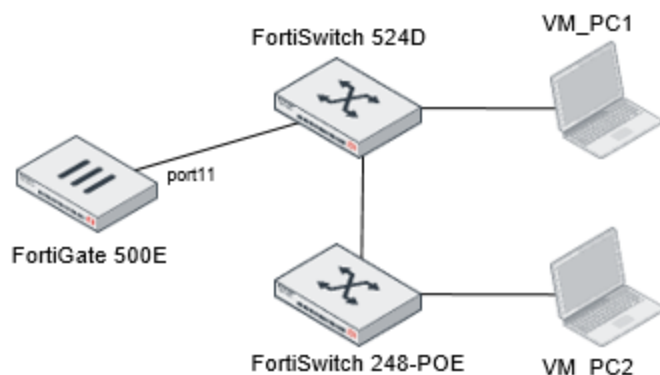
When a NAC device is matched to a NAC policy and assigned to a VLAN, an event log is created.

Date/Time	Level	Message	Log Description	Serial Number	Log Details
2020/11/30 11:20:30	Level 5	Edit switch.acl.ingress:action 3	FortiSwitch system	S248EPTF18000000	<div>FortiSwitch Events</div> <div>Details</div> <div>General</div> <div>Date</div> 2020/11/30 <div>Time</div> 11:20:28 <div>Virtual Domain</div> vdom1 <div>Log Description</div> NAC device addition <div>Source</div> <div>User</div> Switch-Controller <div>Data</div> <div>Message</div> New NAC device added with MAC=00:0c:29:d4:4f:... <div>Action</div> <div>Security</div> <div>Level</div> <div>Cellular</div> <div>Serial Number</div> S248EPTF18000000 <div>Other</div> <div>Log event original timestamp</div> 1606764028195609300 <div>Timezone</div> -0800 <div>Log ID</div> 0115022897 <div>Type</div> event <div>Sub Type</div> switch-controller <div>User Interface</div> flcfd <div>Name</div> FSW11
2020/11/30 11:20:30	Level 5	Edit switch.acl.ingress:classifier 3	FortiSwitch system	S248EPTF18000000	
2020/11/30 11:20:30	Level 5	Add switch.acl.ingress 3	FortiSwitch system	S248EPTF18000000	
2020/11/30 11:20:30	Level 5	Add switch.vlan.member-by-mac 2001:3	FortiSwitch system	S248EPTF18000000	
2020/11/30 11:20:30	Level 5	Edit switch.interface port6	FortiSwitch system	S248EPTF18000000	
2020/11/30 11:20:30	Level 5	Edit switch.physical-port port6	FortiSwitch system	S248EPTF18000000	
2020/11/30 11:20:28	Level 5	New NAC device added with MAC=00:0c:29:d4:4f:...	NAC device addition	S248EPTF18000000	
2020/11/30 11:20:15	Level 5	primary port port6 instance 0 changed state from dl...	FortiSwitch spanning Tree	S248EPTF18000000	
2020/11/30 11:20:13	Level 5	primary port port6 instance 0 changed role from dis...	FortiSwitch spanning Tree	S248EPTF18000000	
2020/11/30 11:20:13	Level 5	primary switch port port6 has come up	FortiSwitch link	S248EPTF18000000	
2020/11/30 11:20:09	Level 5	primary port port6 instance 0 changed role from de...	FortiSwitch spanning Tree	S248EPTF18000000	
2020/11/30 11:20:09	Level 5	primary switch port port6 has gone down	FortiSwitch link	S248EPTF18000000	
2020/11/30 11:20:09	Level 5	primary port port6 instance 0 changed role from dis...	FortiSwitch spanning Tree	S248EPTF18000000	
2020/11/30 11:20:09	Level 5	primary switch port port6 has come up	FortiSwitch link	S248EPTF18000000	
2020/11/30 11:20:05	Level 5	Bounce port: putting switch port port6 as up	FortiSwitch switch	S248EPTF18000000	
2020/11/30 11:20:01	Level 5	primary port port6 instance 0 changed role from de...	FortiSwitch spanning Tree	S248EPTF18000000	
2020/11/30 11:20:01	Level 5	primary switch port port6 has gone down	FortiSwitch link	S248EPTF18000000	
2020/11/30 11:20:00	Level 5	Bounce port: putting switch port port6 as down	FortiSwitch switch	S248EPTF18000000	
2020/11/30 11:20:00	Level 5	Config download successful	Switch-Controller Switch Sync Complete	S248EPTF18000000	
2020/11/30 11:20:00	Level 5	Delete switch.acl.ingress 3	FortiSwitch system	S248EPTF18000000	

Use wildcards in a MAC address in a NAC policy

When configuring a NAC policy, you can use the wildcard * character when manually specifying a MAC address to match the device.

```
config user nac-policy
  edit <policy>
    set mac "xx:xx:xx:*:*:*"
  next
end
```



In this example, VM_PC1 and VM_PC2 both have MAC addresses that start with 00:0c:29. A NAC policy is created on the FortiGate 500E to match both PCs. After the PCs are connected to the FortiSwitch units, they are detected by the NAC policy and assigned to Lab_VLAN.

To configure a MAC address with wildcards in a NAC policy using the CLI:

1. Configure a MAC policy to be applied on the managed FortiSwitch units through the NAC device:

```
config switch-controller mac-policy
    edit "LAB_Linux"
        set fortilink "port11"
        set vlan "Lab_VLAN"
    next
end
```

2. Configure the NAC policy matching pattern to identify matching NAC devices:

```
config user nac-policy
    edit "VM-Policy"
        set mac "00:0c:29:**:**:**"
        set switch-fortilink "port11"
        set switch-mac-policy "LAB_Linux"
    next
end
```

3. Check that the NAC devices are added:

```
# show switch-controller nac-device
config switch-controller nac-device
    edit 2
        set description "auto detected @ 2020-11-30 14:13:45"
        set mac 00:0c:29:d4:4f:3c
        set last-known-switch "S248EPTF18001384"
        set last-known-port "port6"
        set matched-nac-policy "VM-Policy"
        set mac-policy "LAB_Linux"
    next
    edit 3
        set description "auto detected @ 2020-11-30 14:16:07"
        set mac 00:0c:29:a8:0a:1c
        set last-known-switch "S524DN4K16000116"
        set last-known-port "port7"
        set matched-nac-policy "VM-Policy"
        set mac-policy "LAB_Linux"
    next
end
```

To configure a MAC address with wildcards in a NAC policy using the GUI:

1. Go to *WiFi & Switch Controller > NAC Policies*.
2. Click *Create New*.
3. In the *Name* field, enter a name for the NAC policy.
4. Make certain that the status is set to *Enabled*.
5. Click *Specify* to select which FortiSwitch units to apply the NAC policy to or click *All* to select all FortiSwitch units.
6. Click *Device*.
7. Enable *MAC address* and enter the MAC address with wildcards.
8. If you want to assign a specific VLAN to a device assigned to the specified user group, click *Assign VLAN* and enter the VLAN identifier.

9. If you want to assign port-level settings for devices assigned to the specific user group, click *Apply Port Specific Settings*. You can specify the LLDP profile, QoS profile, 802.1x policy, and VLAN policy.
10. Click *OK*.

FortiGate NAC engine optimization

The FortiGate NAC engine is responsible for assigning the device to the right VLAN based on the NAC policy when a device first connects to a switch port or when a device goes from offline to online. This process has been optimized to shorten the amount of time it takes for a new device to be recognized and assigned to the VLAN.

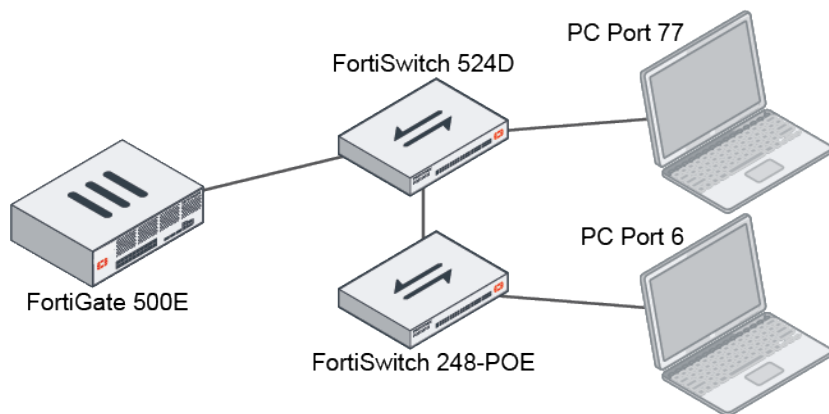
These optimizations include:

- A new event-based approach.
- A new NAC MAC cache table that populates MAC addresses from the FortiSwitch unit immediately after an event.
- NAC inactive timers are now applied to the `nac-mac-cache` table.
- Added `nac-periodic-interval` to run the NAC engine at intervals in case any events are missed. The range is 5 to 60 seconds, and the default setting is 15 seconds.

Before these optimizations, the process took approximately 65 seconds from the time the device links to a switch port to matching the device to a NAC policy. After optimization, the process takes a maximum of 16 seconds with a minimum `nac-periodic-interval` of 5 seconds.

Example

In the following example, you configure the NAC engine to run every five seconds.



To configure the NAC engine to run every five seconds:

```

config switch-controller system
    set nac-periodic-interval 5
end
  
```

To view the NAC clients:

```

# diagnose switch-controller nac-mac-cache show
VFID      SWITCH      MAC-ADDRESS      VLAN CREATION(secs ago)  LAST-SEEN(secs ago)
INTERFACE
  
```

```

1      S524DN4K16000116    00:0c:29:a8:0a:1c 4089 24      0
port7
1      S248EPTF18001384    00:0c:29:d4:4f:3c 4089 44      0
port6

```

Wireless NAC support

The wireless controller supports NAC profiles that onboard wireless clients into the default VLAN. NAC policies match clients based on device properties, user groups, or EMS tags, and then assign the clients to specific VLANs. VLAN subinterfaces are based on the VAP interfaces that are used for the VLAN assignment.

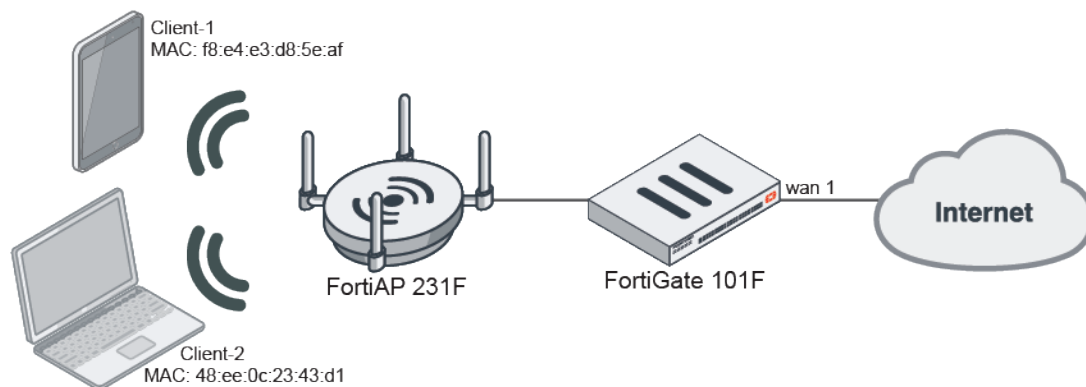
When a wireless client first connects, it is assigned to the default VLAN per the NAC profile. After the client information is captured, if it matches a NAC policy, the client is disconnected and, when it reconnects, assigned to the VLAN that is specified by the SSID policy.

The device properties that can be matched include: MAC address, hardware vendor, type, family, operating system, hardware version, software version, host, user, and source.

Example

When both clients first connect, they are onboarded into the *vap_v100* VLAN. The client information is captured after up to two minutes and, if it matches the NAC policy, the wireless controller disconnects the client. When the client reconnects, it is assigned to the VLAN specified by the policy.

In this example, NAC profiles are configured to onboard wireless Client-1 into default VLANs based on the device's MAC address, user group, or EMS tag.



To configure the VAP, interfaces, profiles, and SSID policy in the CLI:

1. Create the VAP SSID:

```

config wireless-controller vap
    edit "wifi.fap.01"
        set ssid "wifi-ssid.fap.01"
        set passphrase *****
        set schedule "always"
    next
end

```

2. Create two VLAN interfaces under the VAP:

```
config system interface
  edit "vap_v100"
    set vdom "vdom1"
    set ip 10.100.1.1 255.255.255.0
    set allowaccess ping
    set device-identification enable
    set role lan
    set snmp-index 37
    set interface "wifi.fap.01"
    set vlanid 100
  next
  edit "vap_v200"
    set vdom "vdom1"
    set ip 10.101.1.1 255.255.255.0
    set allowaccess ping
    set device-identification enable
    set role lan
    set snmp-index 40
    set interface "wifi.fap.01"
    set vlanid 200
  next
end
```

3. Create the wireless NAC profile:

```
config wireless-controller nac-profile
  edit "wifi-nac-profile-1"
    set onboarding-vlan "vap_v100"
  next
end
```

4. Select the wireless NAC profile in the VAP:

```
config wireless-controller vap
  edit "wifi.fap.01"
    set nac enable
    set nac-profile "wifi-nac-profile-1"
  next
end
```

5. Create the SSID policy:

```
config wireless-controller ssid-policy
  edit "wifi-ssid-policy-1"
    set vlan "vap_v200"
  next
end
```

6. Create NAC policies to match clients based on [Device properties](#), [User groups](#), or [EMS tags](#).

Device properties

This policy matches clients with the MAC address `f8:e4:e3:d8:5e:af`.

To match a wireless client based on its MAC address:

1. Create a NAC policy that matches wireless clients with a specific MAC address:

```
config user nac-policy
  edit "wifi-nac-policy-1"
    set category device
    set mac "f8:e4:e3:d8:5e:af"
    set ssid-policy "wifi-ssid-policy-1"
  next
end
```

When both clients first connect, they are onboarded into the *vap_v100* VLAN:

```
# diagnose wireless-controller wlac -d sta online
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.10 ip6=:
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user= group= signal=-45 noise=-95
idle=1 bw=2 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_personal mpsk=
encrypt=aes cp_authed=no online=yes mimo=2
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=:
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user= group= signal=-25 noise=-95 idle=14
bw=0 use=6 chan=157 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no online=yes mimo=2
```

After the client information is collected, Client-1 matches the policy. It is disconnected, then reconnects and is assigned to the *vap_v200* VLAN in accordance with the NAC policy:

```
# diagnose wireless-controller wlac -d sta online
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=200 ip=10.101.1.10 ip6=:
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user= group= signal=-24 noise=-95
idle=0 bw=7 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_personal mpsk=
encrypt=aes cp_authed=no online=yes mimo=2
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=:
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user= group= signal=-25 noise=-95 idle=0 bw=4
use=6 chan=157 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no online=yes mimo=2
```

2. Verify that Client-1 matched the policy, and Client-2 did not:

```
# diagnose wireless-controller wlac_hlp -c sta-nac

STA (001/002) vfid,mac: 1, 48:ee:0c:23:43:d1
ip                : 10.100.1.11
wlan              : wifi.fap.01(tunnel)
vlan-id(oper/dflt) : 100/100
matched nac-policy : N/A
STA (002/002) vfid,mac: 1, f8:e4:e3:d8:5e:af
ip                : 10.101.1.10
wlan              : wifi.fap.01(tunnel)
vlan-id(oper/dflt) : 200/100
matched nac-policy : wifi-nac-policy-1
```

User groups

This policy matches clients that are authenticated in the *group_local* user group.

To match a wireless client based on its user group:

1. Change the security mode to WPA2 enterprise only and add a user group in the VAP:

```
config wireless-controller vap
    edit "wifi.fap.01"
        set security wpa2-only-enterprise
        set auth usergroup
        set usergroup "group_local" "group_radius"
        set schedule "always"
    next
end
```

2. Create a NAC policy that matches wireless clients that are authenticated in a specific user group:

```
config user nac-policy
    edit "wifi-nac-policy-2"
        set category firewall-user
        set user-group "group_local"
        set ssid-policy "wifi-ssid-policy-1"
    next
end
```

When both clients first connect, they are onboarded into the *vap_v100* VLAN:

```
# diagnose wireless-controller wlacl -d sta online
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.10 ip6=:
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user=local group=group_local
signal=-45 noise=-95 idle=1 bw=2 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_
enterprise mpsk= encrypt=aes cp_authed=no online=yes mimo=2
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=:
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user=tester group=group_radius signal=-24
noise=-95 idle=27 bw=0 use=6 chan=157 radio_type=11AC security=wpa2_only_enterprise
mpsk= encrypt=aes cp_authed=no online=yes mimo=2
```

After the client information is collected, Client-1 matches the policy. It is disconnected, then reconnects and is assigned to the *vap_v200* VLAN in accordance with the NAC policy:

```
# diagnose wireless-controller wlacl -d sta online
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=200 ip=10.101.1.10 ip6=:
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user=local group=group_local
signal=-20 noise=-95 idle=1 bw=9 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_
enterprise mpsk= encrypt=aes cp_authed=no online=yes mimo=2
vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=:
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user=tester group=group_radius signal=-24
noise=-95 idle=35 bw=0 use=6 chan=157 radio_type=11AC security=wpa2_only_enterprise
mpsk= encrypt=aes cp_authed=no online=yes mimo=2
```

3. Verify that Client-1 matched the policy, and Client-2 did not:

```
# diagnose wireless-controller wlacl_hlp -c sta-nac

STA (001/002) vfid,mac: 1, 48:ee:0c:23:43:d1
ip                : 10.100.1.11
wlan              : wifi.fap.01(tunnel)
vlan-id(oper/dflt) : 100/100
matched nac-policy : N/A
STA (002/002) vfid,mac: 1, f8:e4:e3:d8:5e:af
ip                : 10.101.1.10
```

```
wlan                : wifi.fap.01(tunnel)
vlan-id(oper/dflt)  : 200/100
matched nac-policy : wifi-nac-policy-2
```

EMS tags

This policy matches clients that have the specified EMS tag. EMS control must already be configured, see [Synchronizing FortiClient EMS tags and configurations](#) for details.

To match a wireless client based on its EMS tag:

1. Find the EMS tag:

```
# diagnose firewall dynamic list
MAC_FCTEMSTA20002318_ems135_winOS_tag(total-addr: 2): ID(62)
    MAC(F0:B4:D2:AB:E0:09)
    MAC(10:C3:7B:9C:46:AA)
```

2. Create a NAC policy that matches a wireless client with that tag:

```
config user nac-policy
    edit "wifi-nac-policy-3"
        set category ems-tag
        set ems-tag "MAC_FCTEMSTA20002318_ems135_winOS_tag"
        set ssid-policy "wifi-ssid-policy-1"
    next
end
```

When both clients first connect, they are onboarded into the *vap_v100* VLAN. After the client information is collected, Client-1 matches the policy. It is disconnected, then reconnects and is assigned to the *vap_v200* VLAN in accordance with the NAC policy:

```
# diagnose wireless-controller wlac -d sta online
wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=200 ip=10.101.1.11 ip6=fe80::add7:9b4a:cd39:e65c
mac=f0:b4:d2:ab:e0:09 vci=MSFT 5.0 host=DESKTOP-05HBKE1 user= group= signal=-52 noise=-
95 idle=6 bw=0 use=6 chan=40 radio_type=11AC(wave2) security=wpa2_only_personal mpsk=
encrypt=aes cp_authed=no online=yes mimo=2
    ip6=*fe80::add7:9b4a:cd39:e65c,256,
```

3. Verify that Client-1 matched the policy, and Client-2 did not:

```
# diagnose wireless-controller wlac_hlp -c sta-nac

STA (001/002) vfid,mac: 1, 48:ee:0c:23:43:d1
    ip                : 10.100.1.11
    wlan              : wifi.fap.01(tunnel)
    vlan-id(oper/dflt) : 100/100
    matched nac-policy : N/A
STA (002/002) vfid,mac: 1, f8:e4:e3:d8:5e:af
    ip                : 10.101.1.10
    wlan              : wifi.fap.01(tunnel)
    vlan-id(oper/dflt) : 200/100
    matched nac-policy : wifi-nac-policy-3
```

Dynamic port profiles for FortiSwitch ports

Dynamic port policies allow you to specify rules that dynamically determine port policies. After you create the FortiLink policy settings, you define the dynamic port policy rules. When a rule matches the specified device patterns, the switch-controller actions control the port's properties.

When you add dynamic port policy rules to the FortiLink policy settings, the rules are processed sequentially, from the first rule to the last rule. The last rule in the FortiLink policy settings should indicate the default properties for any port that has been assigned these FortiLink policy settings.

To configure dynamic port policy rules:

1. [Set the access mode and port policy for the port on page 598](#)
2. [Set the FortiLink policy settings to the FortiLink interface on page 598](#)
3. [Create the FortiLink policy settings on page 598](#)
4. [Create the dynamic port policy rule on page 599](#)
5. [Set how often the dynamic port policy engine runs on page 601](#)

Set the access mode and port policy for the port

```
config switch-controller managed-switch
    edit <FortiSwitch_serial_number>
        config ports
            edit <port_name>
                set access-mode dynamic
                set port-policy <dynamic_port_policy>
            next
        end
    next
end
```

Set the FortiLink policy settings to the FortiLink interface

Enable the dynamic port policy on the FortiLink interface by specifying the FortiLink policy settings on the FortiLink interface.

```
config system interface
    edit fortilink
        set switch-controller-dynamic <FortiLink_policy_settings>
    next
end
```

Create the FortiLink policy settings

Using the GUI

1. Go to *WiFi & Switch Controller > FortiSwitch Port Policies*.
2. Click *Dynamic Port Policies*.
3. Click *Configure Dynamic Port Settings*.

4. Select the onboarding VLAN from the *Onboarding VLAN* dropdown list. The default onboarding VLAN is *onboarding*.
5. Move the *Bounce port* slider to enable it if you want the link to go down and then up when the NAC mode is configured on the port.
6. If you are using the dynamic port policy with FortiSwitch network access control, move the *Apply rule to NAC policies* slider to enable it.
7. Click *Next*.
8. When devices are matched by a dynamic port policy, you can assign those devices to a dynamic port VLAN. By default, there are six VLAN templates:
 - *default*—This VLAN is assigned to all switch ports when the FortiSwitch unit is first discovered.
 - *onboarding*—This VLAN is for NAC onboarding devices.
 - *quarantine*—This VLAN contains quarantined traffic.
 - *rspan*—This VLAN contains RSPAN and ERSPAN mirrored traffic.
 - *video*—This VLAN is dedicated for video devices.
 - *voice*—This VLAN is dedicated for voice devices.

You can select one of the default VLAN templates, edit one of the default VLAN templates, or create a dynamic port VLAN.
9. Click *Submit*.

Using the CLI

```
config switch-controller fortilink-settings
  edit <name_of_this_FortiLink_configuration>
    set inactive-timer <integer>
    set link-down-flush {enable | disable}
    config nac-ports
      set onboarding-vlan <string>
      set bounce-nac-port {enable | disable}
    end
  next
end
```

Create the dynamic port policy rule

Using the GUI

1. On the *Dynamic Port Policies* page, select the dynamic port policy that you want to add dynamic port policy rules to.
2. Click *Edit*.
3. Click *Create New*.
4. In the *Name* field, enter a name for the dynamic port policy rule.
5. Make certain that the status is set to *Enabled*.
6. In the *Description* field, enter a description of the dynamic port policy rule.
7. If you want the device to match a MAC address, move the *MAC Address* slider and enter the MAC address to match.
8. If you want the device to match a host name or IP address, move the *Host* slider and enter the host name or IP address to match.
9. If you want the device to match a device family, move the *Device Family* slider and enter the name of the device family to match.
10. If you want the device to match a device type, move the *Type* slider and enter the device type to match.

11. If you want to assign an LLDP profile to the device that matches the specified criteria, move the *LLDP profile* slider and enter the name of the LLDP profile.
12. If you want to assign a QoS policy to the device that matches the specified criteria, move the *QoS policy* slider and enter the name of the QoS policy.
13. If you want to assign an 802.1x policy to the device that matches the specified criteria, move the *802.1X policy* slider and enter the name of the 802.1x policy.
14. If you want to assign a VLAN policy to the device that matches the specified criteria, move the *VLAN policy* slider and enter the name of the VLAN policy.
15. Click **OK**.

Using the CLI

```
config switch-controller dynamic-port-policy
edit <dynamic_port_policy_name>
set description <string>
set fortilink <FortiLink_interface_name>
config policy
edit <policy_name>
set description <string>
set status {enable | disable}
set category {device | interface-tag}
set mac <MAC_address>
set type <device_type>
set family <device_family_name>
set host <host_name_or_IP_address>
set lldp-profile <LLDP_profile_name>
set qos-policy <QoS_policy_name>
set 802-1x <802.1x_policy_name>
set vlan-policy <VLAN_policy_name>
set bounce-port-link {disable | enable}
next
end
next
end
```

Creating a VLAN policy

You can specify a VLAN policy to be used in the port policy. In the VLAN policy, you can specify the native VLAN to be applied, the allowed VLANs, and the untagged VLANs. You can enable or disable all defined VLANs and select whether to discard untagged or tagged frames or to not discard any frames.

```
config switch-controller vlan-policy
edit <VLAN_policy_name>
set description <policy_description>
set fortilink <FortiLink_interface>
set vlan <VLAN_name>
set allowed-vlans <lists_of_VLAN_names>
set untagged-vlans <lists_of_VLAN_names>
set allowed-vlans-all {enable | disable}
set discard-mode {none | all-untagged | all-tagged}
next
end
```

For example:

```
config switch-controller vlan-policy
  edit vlan_policy_1
    set fortilink fortilink1
    set vlan default
  next
end
```

Set how often the dynamic port policy engine runs

In the FortiOS CLI, you can change how often the dynamic port policy engine runs. By default, it runs every 15 seconds. The range of values is 5-60 seconds.

```
config switch-controller system
  set dynamic-periodic-interval <5-60 seconds>
end
```

GUI updates for the switch controller

There have been GUI updates to the *FortiSwitch Ports*, *FortiLink Interface*, and *FortiSwitch NAC Policies* pages to simplify the configuration of NAC policies.

Previously, dynamic port policies had to be configured in the *FortiSwitch Ports*, *FortiLink Interface*, and *FortiSwitch NAC Policies* pages. Now, configuring dynamic port policies is under the *Dynamic Port Policies* tab on the *FortiSwitch Port Policies* page. For more information about dynamic port policies, see [Dynamic port profiles for FortiSwitch ports on page 598](#).

Name	Ref.	Description
port11	1	

The *FortiSwitch NAC Policies* page is now the *NAC Policies* page.

The access mode of each FortiSwitch port is listed in the *Mode* column in the FortiSwitch Ports page. Right-click in the *Mode* column to select the access mode of the port:

- *Static*—The port does not use a dynamic port policy or FortiSwitch NAC policy.
- *Assign Port Policy*—The port uses a dynamic port policy.
- *NAC*—The port uses a FortiSwitch NAC policy.

<div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> <div>Search</div> <div>Q</div> </div> <div>Port Trunk Faceplates</div>								
Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information
S524DF4K15000024 33								
port1		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port2		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port3		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port4		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port5		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port6		NAC		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	onboarding.fortilink (onboarding)	quarantine.fortilink (quarantine)	Powered	
port7		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port8		Static		<div> <div>Edge Port</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port9		Static		<div> <div>Edge Port</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port10		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port11		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	
port12		Static		<div> <div>Edge Port</div> <div>Spanning Tree Protocol</div> </div>	default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	

Support dynamic firewall addresses in NAC policies - 7.0.1

You can configure a dynamic firewall address for devices and use it in a NAC policy. When a device matches the NAC policy, the MAC address for that device is automatically assigned to the dynamic firewall address, which can be used in firewall policies to control traffic from/to these devices.

Configuring a dynamic firewall address requires setting the address type to `dynamic` and the address subtype to `swc-tag`. Using the dynamic firewall address in a NAC policy requires specifying the conditions that a device must match and setting the firewall address to the name of the dynamic firewall address.

To configure a dynamic firewall address and use it in a NAC policy in the CLI:

```
config firewall address
  edit <name_of_dynamic_firewall_address>
    set type dynamic
    set sub-type swc-tag
  next
end

config user nac-policy
  edit <policy_name>
    set description <description_of_policy>
    set category device
    set status enable
    set mac <MAC_address>
    set hw-vendor <hardware_vendor>
    set type <device_type>
    set family <device_family>
    set os <operating_system>
```



```
set hw-version <hardware_version>
set sw-version <software_version>
set host <host_name>
set user <user_name>.
set src <source>
set switch-fortilink <FortiLink_interface>
set switch-scope <list_of_managed_FortiSwitch_serial_numbers>
set switch-auto-auth {enable | disable}
set switch-mac-policy <switch_mac_policy>
set firewall-address <name_of_dynamic_firewall_address>
next
end
```

For example:

```
config firewall address
  edit "lab_vm_device"
    set type dynamic
    set sub-type swc-tag
  next
end

config user nac-policy
  edit "LAB_VM"
    set hw-vendor "VMware"
    set switch-fortilink "port11"
    set switch-mac-policy "LAB_VM"
    set firewall-address "lab_vm_device"
  next
end
```

To view the dynamic MAC addresses attached to the firewall:

```
diagnose firewall dynamic list
```

To configure a dynamic firewall address and use it in a NAC policy in the GUI:

1. Go to *WiFi & Switch Controller > NAC Policies*.
2. Click *Create New*.
3. In the *Name* field, enter a name for the NAC policy.
4. Make certain that the status is set to *Enabled*.
5. Click *Specify* to select which FortiSwitch units to apply the NAC policy to or click *All*.
6. Select *Device* for the category.
7. If you want the device to match a MAC address, enable *MAC Address* and enter the MAC address to match.
8. If you want the device to match a hardware vendor, enable *Hardware Vendor* and enter the name of the hardware vendor to match.
9. If you want the device to match a device family, enable *Device Family* and enter the name of the device family to match.
10. If you want the device to match a device type, enable *Type* and enter the device type to match.
11. If you want the device to match an operating system, enable *Operating System* and enter the operating system to match.
12. If you want the device to match a user, enable *User* slider and enter the user name to match.
13. If you want to assign a specific VLAN to the device that matches the specified criteria, enable *Assign VLAN* and enter the VLAN identifier.

14. If you do not want to bounce the switch port (administratively bringing the link down and then up) when NAC mode is configured, disable *Bounce port*.
15. To use a dynamic firewall address for matching a device, enable *Assign device to dynamic address* and, from the dropdown list, click *Create*.

Create NAC Policy

Name

Status

Enabled

Disabled

FortiSwitches

All

Specify

Description

0/63

Device Patterns

Category

Device

User

EMS Tag

MAC address

Hardware vendor

Device family

Type

Operating system

User

Switch Controller Action

Assign VLAN

Bounce port

Assign device to dynamic address

dynamicaddress1

Search

+ Create

dynamicaddress1

Wireless Controller Action

Assign VLAN

OK

Cancel

- a. In the *Name* field, enter the name of the dynamic firewall address.

New Address

Name	
Color	<div style="display: flex; align-items: center;"> <div style="width: 20px; height: 20px; background-color: #ccc; border: 1px solid #ccc; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; padding: 2px 5px;">Change</div> </div>
Type	<div style="border: 1px solid #ccc; padding: 2px;">Dynamic ▼</div>
Sub Type i	<div style="border: 1px solid #ccc; padding: 2px;">Switch Controller NAC Policy Tag ▼</div>
Interface	<div style="display: flex; align-items: center;"> <input type="checkbox"/> any ▼ </div>
Comments	<div style="border: 1px solid #ccc; padding: 2px;">Write a comment... 0/255</div>

OK

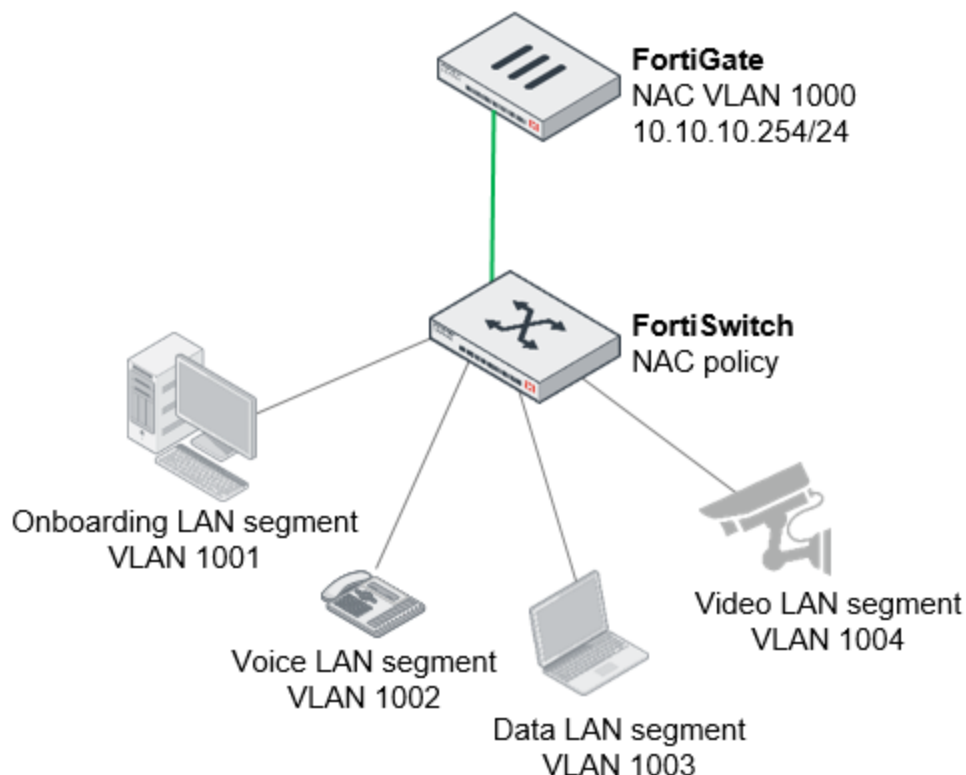
Cancel

- b. To change the color, click *Change* and select the color used for the corresponding icon in the GUI.
- c. The address type is set to *Dynamic* by default and the subtype is set to *Switch Controller NAC Policy Tag* by default.
- d. For the interface, select the interface whose IP address is to be used.
- e. In the *Comments* field, enter a description of the dynamic firewall address.
- f. Click *OK* to save the dynamic firewall address.
16. Click *OK* to create the new NAC policy.

NAC LAN segments - 7.0.1

When NAC mode is configured on a port, the link of a switch port goes down and then up by default, which restarts the DHCP process for that device. When a link goes down, the NAC devices are cleared from all switch ports by default. Bouncing the switch port and restarting DHCP changes the IP addresses of hosts and invalidates firewall sessions. Starting in FortiOS 7.0.1, you can avoid these problems by assigning each VLAN to a separate LAN segment.

LAN segments prevent the IP addresses of hosts from changing but still provide physical isolation. For example, the following figure shows how four LAN segments have been assigned to four separate VLANs:



The switch controls traffic between LAN segments. Enable *Block Intra-VLAN Traffic* in the GUI or use the `set switch-controller-access-vlan` command to allow or prevent traffic between hosts in a LAN segment.



- An RSPAN VLAN interface cannot be a member of a LAN segment group.
- IGMP snooping is not supported with LAN segments.

LAN segments require the following:

- FortiGate devices running FortiOS 7.0.1 or higher with managed FortiSwitch units running FortiSwitchOS 7.0.1 or higher.
- To see which FortiSwitch models support this feature, refer to the [FortiSwitch feature matrix](#).

To use LAN segments:

- Configure FortiSwitch VLANs without layer-3 properties (unset the IP address, set the access mode to `static`, unset `allowaccess`, and disable the DHCP server).
- Optionally, enable *Block Intra-VLAN Traffic*.
- Enable LAN segments.
- Specify the NAC LAN interface.
- Specify which VLANs belong to that LAN segment.



Do not make changes after assigning a VLAN to a LAN segment. Changing VLANs assigned to LAN segments might have unexpected results.

To configure LAN segments on a global level:

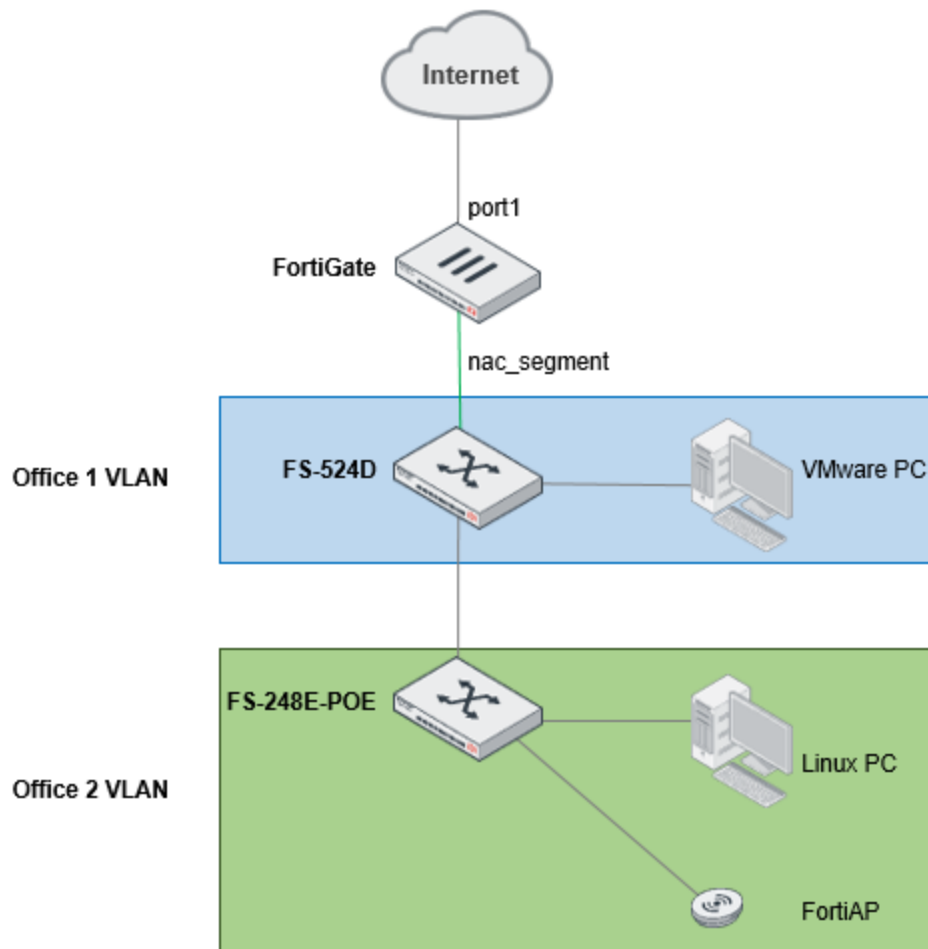
```
config switch-controller fortilink-settings
  edit <name_of_this_FortiLink_configuration>
    config nac-ports
      set lan-segment {enabled | disabled}
      set nac-lan-interfaces <string>
      set nac-segment-vlans <VLAN_interface_name>
    end
  next
end
```

For example:

```
config switch-controller fortilink-settings
  edit "port20"
    config nac-ports
      set onboarding-vlan "onboarding"
      set lan-segment enabled
      set nac-lan-interface "nac_segment"
      set nac-segment-vlans "voice" "video"
    end
  next
end
```

Example of using LAN segments with NAC

In this example, devices are initially placed in the onboarding VLAN and receive IP addresses from the nac_segment DHCP server. Ports connected to the devices are configured with the NAC access mode. NAC policies are used to identify devices by OS and place them into the appropriate VLAN segment and dynamic firewall address. Firewall policies match traffic from the nac_segment interface by the dynamic firewall address and apply the appropriate security profiles to each.



1. Configure the FortiSwitch VLANs for Office 1 and Office 2.

```
config system interface
  edit "Office2"
    set vdom "root"
    set device-identification enable
    set role lan
    set snmp-index 33
    set color 10
    set interface "fortilink"
    set vlanid 2000
  next
  edit "Office1"
    set vdom "root"
    set device-identification enable
    set role lan
    set snmp-index 34
    set color 5
    set interface "fortilink"
    set vlanid 2001
  next
end
```

2. The following is the configuration for the `nac_segment` interface and its corresponding DHCP server settings. These settings are the default.

```
config system interface
    edit "nac_segment"
        set vdom "root"
        set ip 10.255.13.1 255.255.255.0
        set description "NAC Segment VLAN"
        set alias "nac_segment.fortilink"
        set device-identification enable
        set snmp-index 32
        set switch-controller-feature nac-segment
        set interface "fortilink"
        set vlanid 4088
    next
end
config system dhcp server
    edit 5
        set lease-time 300
        set dns-service default
        set default-gateway 10.255.13.1
        set netmask 255.255.255.0
        set interface "nac_segment"
        config ip-range
            edit 1
                set start-ip 10.255.13.2
                set end-ip 10.255.13.254
            next
        end
        set timezone-option default
    next
end
```

3. Add the Office 1 VLAN and Office 2 VLAN to the LAN segment VLANs.

```
config switch-controller fortilink-settings
    edit "fortilink"
        config nac-ports
            set onboarding-vlan "onboarding"
            set lan-segment enabled
            set nac-lan-interface "nac_segment"
            set nac-segment-vlans "voice" "video" "Office2" "Office1"
        end
    next
end
```

4. Configure the NAC policy for devices in Office 1 and Office 2.

If you configure the NAC policy from the GUI, you can create the `office2_device` and `office1_device` dynamic firewall addresses inline. However, if you create the NAC policy from the CLI, first create the firewall addresses and then create the MAC policy and NAC policies.

```
config firewall address
    edit "office2_device"
        set type dynamic
```

```
        set sub-type swc-tag
        set color 19
    next
    edit "office1_device"
        set type dynamic
        set sub-type swc-tag
        set color 10
    next
end

config switch-controller mac-policy
    edit "Office2_FAP"
        set fortilink "fortilink"
        set vlan "Office2"
    next
    edit "Office2_PC"
        set fortilink "fortilink"
        set vlan "Office2"
    next
    edit "Office1_PC"
        set fortilink "fortilink"
        set vlan "Office1"
    next
end

config user nac-policy
    edit "OFFICE2_FAP"
        set hw-vendor "Fortinet"
        set family "FortiAP"
        set os "FortiAP OS"
        set switch-fortilink "fortilink"
        set switch-scope "S248EPTF18001384"
        set switch-mac-policy "Office2_FAP"
        set firewall-address "office2_device"
    next
    edit "OFFICE2_PC"
        set os "Linux"
        set switch-fortilink "fortilink"
        set switch-scope "S248EPTF18001384"
        set switch-mac-policy "Office2_PC"
        set firewall-address "office2_device"
    next
    edit "OFFICE1_PC"
        set hw-vendor "VMware"
        set switch-fortilink "fortilink"
        set switch-scope "S524DN4K16000116"
        set switch-mac-policy "Office1_PC"
        set firewall-address "office1_device"
    next
end
```

5. Configure the firewall policy for devices in Office 1 or Office 2.

The source of all traffic is `nac_segment`, but the traffic is filtered on the `srcaddr` by the dynamic firewall address previously assigned by the NAC policies.


```
config firewall policy
  edit 5
    set name "Office1_Device"
    set uuid d3e2bbdc-d9c1-51eb-dbd3-cb534366b58d
    set srcintf "nac_segment"
    set dstintf "port1"
    set action accept
    set srcaddr "office1_device"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set ssl-ssh-profile "certificate-inspection"
    set logtraffic all
    set nat enable
  next
  edit 4
    set name "Office2_Device"
    set uuid a724c2fc-d9c1-51eb-e8d8-a501419308b3
    set srcintf "nac_segment"
    set dstintf "port1"
    set action accept
    set srcaddr "office2_device"
    set dstaddr "all"
    set schedule "always"
    set service "ALL_ICMP" "FTP" "FTP_GET" "FTP_PUT" "HTTP" "HTTPS" "TFTP"
    set ssl-ssh-profile "certificate-inspection"
    set logtraffic all
    set nat enable
  next
  edit 3
    set name "All_devices"
    set uuid 0accfbae-d9c1-51eb-b0bf-2ba0b00647c0
    set srcintf "nac_segment"
    set dstintf "port1"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set ssl-ssh-profile "certificate-inspection"
    set av-profile "default"
    set webfilter-profile "default"
    set dnsfilter-profile "default"
    set ips-sensor "default"
    set application-list "default"
    set logtraffic all
    set nat enable
  next
end
```

6. Place the ports in NAC mode.

```
config switch-controller managed-switch
  edit "S524DN4K16000116"
    config ports
      edit "port7"
```

```
        set vlan "onboarding"
        set allowed-vlans "quarantine" "nac_segment"
        set untagged-vlans "quarantine" "nac_segment"
        set access-mode nac
    next
end
next
edit "S248EPTF18001384"
    config ports
        edit "port1"
            set vlan "onboarding"
            set allowed-vlans "quarantine" "nac_segment"
            set untagged-vlans "quarantine" "nac_segment"
            set access-mode nac
        next
        edit "port6"
            set vlan "onboarding"
            set allowed-vlans "quarantine" "nac_segment"
            set untagged-vlans "quarantine" "nac_segment"
            set access-mode nac
        next
    end
next
end
```

Specify FortiSwitch groups in NAC policies - 7.0.2

You can now specify FortiSwitch groups in NAC policies using the GUI and CLI. In previous FortiOS versions, you specified individual managed FortiSwitch units when creating a NAC policy using the `set switch-scope` command or selecting the FortiSwitch units in the *Create NAC Policy* window.

In FortiOS 7.0.2, the `set switch-scope` command has been replaced with the `set switch-group` command, and the *Create NAC Policy* window allows you to specify FortiSwitch groups. You can select more than one FortiSwitch group in the CLI and GUI, and the same FortiSwitch unit can be included in more than one FortiSwitch group. If no FortiSwitch group is specified in the `set switch-group` command, all FortiSwitch groups are used for the NAC policy.

When you upgrade to FortiOS 7.0.2, the individual FortiSwitch units selected for the NAC policy are assigned to a new FortiSwitch group, and the new FortiSwitch group replaces the individual FortiSwitch units in the NAC policy. If you downgrade from FortiOS 7.0.2, the individual FortiSwitch units in the FortiSwitch group are listed in the `set switch-scope` command in the NAC policy, and the `set switch-group` command is removed from the NAC policy.

To create a FortiSwitch group in the CLI:

```
config switch-controller switch-group
    edit <name>
        set description <string>
        set fortilink <name_of_FortiLink_interface>
        set members <serial-number-1> <serial-number-2> ...
    next
end
```

For example:

```
config switch-controller switch-group
    edit NACswitchgroup1
```

```
set description "FortiSwitch group for NAC policy"
set fortilink "fortilink"
set members S524DF4K15000024 S548DF5018000776
next
end
```

To create a FortiSwitch group in the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitches*.
2. Click *Create New > FortiSwitch Group*.
3. In the *Name* field, enter a name for the FortiSwitch group.
4. In the *Members* field, click + to select which switches to include in the FortiSwitch group.
5. In the *Description* field, enter a description of the FortiSwitch group.
6. Click *OK*.

To specify FortiSwitch groups in the NAC policy in the CLI:

```
config user nac-policy
edit <NAC_policy_name>
set description <description_of_NAC_policy>
set category {user | device | ems-tag}
set status enable
set switch-group <FortiSwitch_group_1> <FortiSwitch_group_2> ...
...
next
end
```

For example:

```
config user nac-policy
edit "OFFICE_VM"
set hw-vendor "VMware"
set switch-fortilink "fortilink"
set switch-mac-policy "OFFICE_VM"
set firewall-address "office_vm_device"
set switch-group NACswitchgroup1 NACswitchgroup2 NACswitchgroup3
next
end
```

To specify FortiSwitch groups in the NAC policy in the GUI:

1. Go to *WiFi & Switch Controller > NAC Policies*.
2. Click *Create New*.
3. In the *Name* field, enter a name for the NAC policy.
4. Make certain that the status is set to *Enabled*.
5. Click *Specify*.
6. Click + in the *FortiSwitch groups* field to select which FortiSwitch groups to apply the NAC policy to.
7. Configure the remaining settings as needed.
8. Select *OK* to create the new NAC policy.

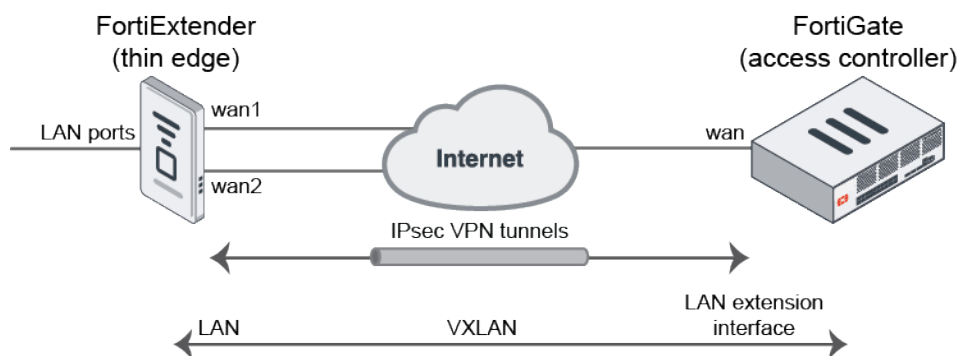
FortiExtender

This section includes information about FortiExtender related new features:

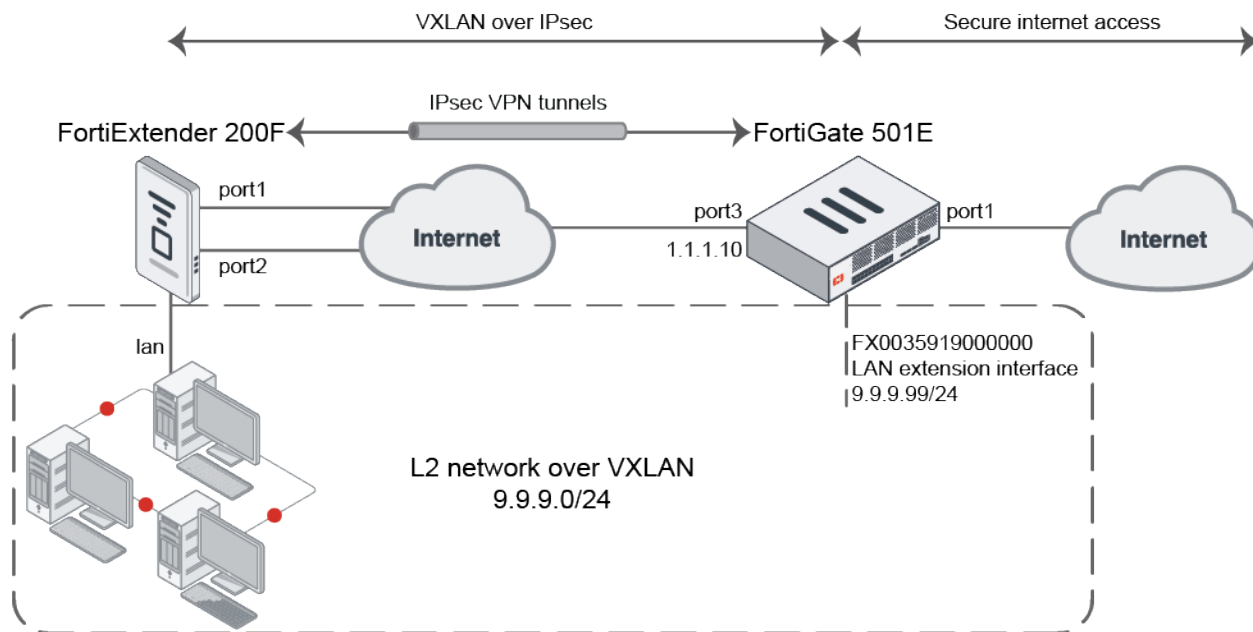
- [Introduce LAN extension mode for FortiExtender 7.0.2 on page 614](#)
- [Using the backhaul IP when the FortiGate access controller is behind NAT 7.0.2 on page 622](#)
- [Bandwidth limits on the FortiExtender Thin Edge 7.0.2 on page 629](#)

Introduce LAN extension mode for FortiExtender - 7.0.2

LAN extension is a new configuration mode on the FortiGate that allows FortiExtender to provide remote thin edge connectivity back to the FortiGate over a backhaul connection. A FortiExtender deployed at a remote location will discover the FortiGate access controller (AC) and form an IPsec tunnel (or multiple tunnels when multiple links exist on the FortiExtender) back to the FortiGate. A VXLAN is established over the IPsec tunnels to create an L2 network between the FortiGate and the network behind the remote FortiExtender.



In the following example, a FortiGate 501E is the FortiExtender AC that provides secure internet access to the remote network behind the FortiExtender 200F thin edge. The FortiGate 501E has two WAN connections; one is used as an inbound backhaul connection and the other for outbound internet access. The FortiExtender 200F has two wired WAN/uplink ports connected to the internet. Once the FortiExtender discovers the FortiGate AC and is authorized by the FortiGate, the FortiGate pushes an extender profile to the FortiExtender. From the profile, the extender uses the configurations to form two IPsec tunnels back to the FortiGate. Additional VXLAN aggregate interfaces are automatically configured to create an L2 network between the FortiExtender LAN port and a virtual LAN extension interface on the FortiGate. Clients behind the FortiExtender can now connect to the internet through the FortiGate that secures the internet connection.



Authorizing the devices

To discover and authorize the FortiExtender in the GUI:

- On the FortiGate, enable the Security Fabric connection on port3 to allow the FortiExtender to connect over CAPWAP:
 - Go to *Network > Interfaces* and edit port3.
 - In the *Administrative Access* section, select *PING* and *Security Fabric Connection*.
 - Click OK.
- On the FortiExtender, connect to the CLI via SSH and set the AC server address to the FortiGate:

```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
        set server 1.1.1.10
      next
    end
  set ac-ctl-port 5246
  set ac-data-port 25246
  set discovery-intf port1 port2
  set ingress-intf
end
end
```

Once the FortiExtender's discovery packet reaches port3 on the FortiGate, the FortiExtender will appear under *Network > FortiExtenders* as unauthorized.

Managed FortiExtenders			
+ Create New Edit Delete Deauthorize Search			
Name	Serial Number	Status	Mode
FX0035919000000	FX200F5919000000	Unauthorized	LAN extension

The FortiGate automatically creates a VPN profile for this FortiExtender, which appears on the *VPN > IPsec Tunnels* page.

+ Create New Edit Delete Search			
Tunnel	Interface Binding	Status	Ref.
Custom 1			
fxext-ipsec-ksKS	port3	Inactive	3

The FortiGate also creates an extender profile for that model of FortiExtender, which appears on the *Network > FortiExtenders > Profiles* tab.

Managed FortiExtenders			
+ Create New Edit Delete Search			
Name	Model	Mode	Ref.
FX200F-lanext-default	FX200F	LAN extension	1

The FortiExtender profile is configured based on the FortiExtender model. It automatically selects *Load Balance* (as the *Link load balance* setting), the IPsec interface, and the pre-configured tunnel.

Edit FortiExtender Profile

Name

FX200F-lanext-default

Model

FX200F

Mode

LAN extension

LAN extension

Link load balance

Active backup **Load Balance**

IPsec interface

port3

IPsec interface IP/FQDN

IPsec tunnel

fxext-ipsec-ksKS

FortiExtender uplink port

[+ Create New](#)
[Edit](#)
[Delete](#)

Name	Uplink port	Weight
1	port1	1
2	port2	1

Additional Information

API Preview

References

Edit in CLI

Documentation

[Online Help](#)
[Video Tutorials](#)

3. Authorize the FortiExtender:

- Go to *Network > FortiExtenders*, select the *Managed FortiExtenders* tab, and edit the discovered FortiExtender.

- b. In the *Status* section, enable *Authorized*.

Serial number: FX200F5919000000

Alias:

Mode: LAN extension

Profile: FX200F-lanext-default

State

Authorized: ☒

FortiGate

FortiGate-501E

Additional Information

API Preview

Edit in CLI

Documentation

Online Help

Video Tutorials

OK Cancel

- c. Click OK. The device now displays as authorized.

Managed FortiExtenders			
Profiles Data Plans			
+ Create New Edit Delete Deauthorize <input type="text" value="Search"/>			
Name	Serial Number	Status	Mode
FX0035919000000	FX200F5919000000	Authorized	LAN extension

To discover and authorize the FortiExtender in the CLI:

- On the FortiGate, enable the Security Fabric connection on port3 to allow the FortiExtender to connect over CAPWAP:

```
config system interface
  edit "port3"
    set vdom "root"
    set ip 1.1.1.10 255.255.255.0
    set allowaccess ping fabric
  next
end
```

- On the FortiExtender, connect to the CLI via SSH and set the AC server address to the FortiGate:

```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
        set server 1.1.1.10
      next
    end
    set ac-ctl-port 5246
    set ac-data-port 25246
    set discovery-intf port1 port2
    set ingress-intf
  end
end
```

3. The FortiGate discovers the FortiExtender and some basic configurations are automatically initialized in FortiOS:

```
config extender-controller extender
    edit "FX0035919000000"
        set id "FX200F5919000000"
        set device-id 0
        set extension-type lan-extension
        set profile "FX200F-lanext-default"
    next
end
```

4. An IPsec tunnel is automatically created for the detected FortiExtender:

```
config vpn ipsec phase1-interface
    edit "fext-ipsec-ksKS"
        set type dynamic
        set interface "port3"
        set ike-version 2
        set peertype one
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set localid "localid-5bzuqs54dGni2TT0x2NePg0HexHW2piQ44aZ4NiGe8SVxxBnFuiqZqo"
        set dpd on-idle
        set comments "[FX200F-lanext-default] Do NOT edit. Automatically generated by
extender controller."
        set peerid "peerid-svxVy5bZbPxZdfoIQBNA7YrkSKBA9UilvZsvYcVrgplUy0aFMCVZzGzh"
        set psksecret ENC <secret>
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit "fext-ipsec-ksKS"
        set phasename "fext-ipsec-ksKS"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set comments "[FX200F-lanext-default] Do NOT edit. Automatically generated by
extender controller."
    next
end
```

5. A FortiExtender profile is created for the model of the detected FortiExtender:

```
config extender-controller extender-profile
    edit "FX200F-lanext-default"
        set id 0
        set model FX200F
        set extension lan-extension
        config lan-extension
            set link-loadbalance loadbalance
            set ipsec-tunnel "fext-ipsec-ksKS"
            set backhaul-interface "port3"
            config backhaul
                edit "1"
                    set port port1
                next
                edit "2"
                    set port port2
            next
        next
    next
end
```



```

end
end

```

6. Authorize the FortiExtender:

```

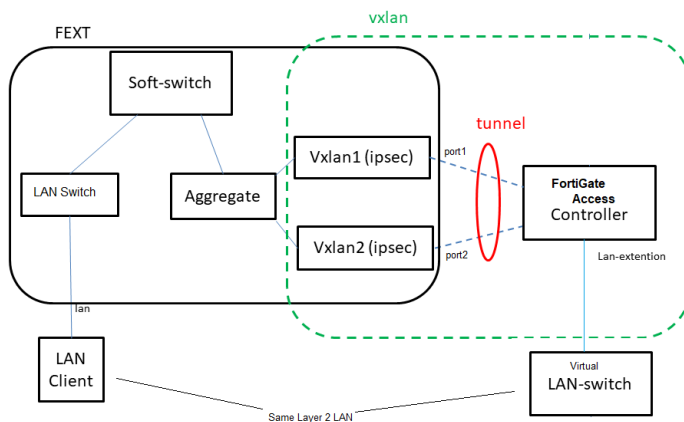
config extender-controller extender
  edit "FX0035919000000"
    set authorized enable
  next
end

```

Backhaul tunnel and VXLAN auto-deployment

Once the FortiExtender is authorized, the FortiGate immediately pushes the IPsec tunnel configuration to the extender. This forces the FortiExtender to establish the tunnel and form the VXLAN mechanism.

In the following diagram, the VXLANs are built on the IPsec tunnels between the FortiExtender and FortiGate. The two VXLAN interfaces are aggregated to provide load balancing and redundancy. A softswitch is also used to combine the aggregate interface with the local LAN ports, which allows the LAN ports to be part of the VXLAN. This ultimately combines the local LAN ports with the virtual LAN extension interface on the FortiGate AC.



Underlying configurations that are automatically configured:

1. The FortiExtender receives the IPsec configurations from the FortiGate and creates the corresponding tunnels for each uplink:

```

config vpn ipsec phase1-interface
  edit le-uplink-port1
    set ike-version 2
    set keylife 86400
    set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
  3des-sha1
    set dhgrp 14 5
    set interface port1
    set type static
    set remote-gw 1.1.1.10
    set authmethod psk
    set psksecret *****
    set localid peerid-svxVy5bZbPxZdfoIQBNA7YrkSKBA9UilvZsvYcVrgplUy0aFMCVZzGzh
    set peerid localid-5bzuqs54dGni2TT0x2NePg0HexHW2piQ44aZ4NiGe8SVxxBnFuiqZqo
  
```

```
        set add-gw-route enable
        set dev-id-notification disable
    next
    edit le-uplink-port2
        set ike-version 2
        set keylife 86400
        set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
3des-sha1
        set dhgrp 14 5
        set interface port2
        set type static
        set remote-gw 1.1.1.10
        set authmethod psk
        set psksecret *****
        set localid peerid-svxVy5bZbPxZdfoIQBNA7YrkSKBA9UilvZsvYcVrgplUy0aFMCVZzGzh
        set peerid localid-5bzuqs54dGni2TT0x2NePg0HexHW2piQ44aZ4NiGe8SVxxBnFuiqZqo
        set add-gw-route enable
        set dev-id-notification disable
    next
end
```

2. VXLAN interfaces are formed over each tunnel:

```
config system vxlan
    edit le-vxlan-port1
        set vni 0
        set remote-ip 10.252.0.1
        set local-ip 10.252.0.2
        set dstport 9999
    next
    edit le-vxlan-port2
        set vni 0
        set remote-ip 10.252.0.1
        set local-ip 10.252.0.3
        set dstport 9999
    next
end
```

3. An aggregate interface is configured to load balance between the two VXLAN interfaces:

```
config system aggregate-interface
    edit le-agg-link
        set mode loadbalance
        set mapping-timeout 60
        config members
            edit le-vxlan-port1
                set interface le-vxlan-port1
                set weight 1
                set health-check-event le-agg-port1
                set health-check-fail-cnt 5
                set health-check-recovery-cnt 5
            next
            edit le-vxlan-port2
                set interface le-vxlan-port2
                set weight 1
                set health-check-event le-agg-port2
                set health-check-fail-cnt 5
```

```

        set health-check-recovery-cnt 5
    next
end
next
end

```

4. The softswitch bridges the aggregate interface and the local LAN to connect the LAN to the VXLAN bridged L2 network, which spans across to the FortiGate LAN extension interface:

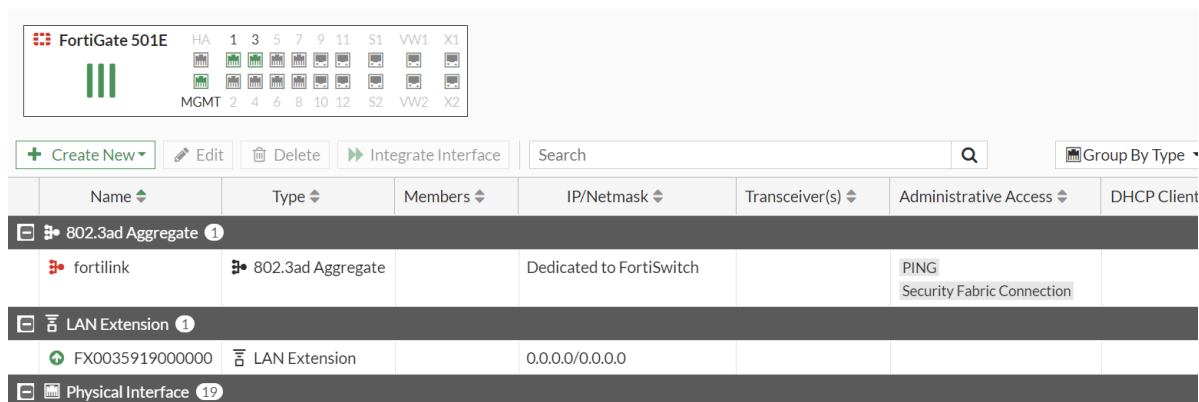
```

config system switch-interface
    edit le-switch
        set members le-agg-link lan
        set stp disable
    next
end

```

Configuring the LAN extension and firewall policy

Once the IPsec tunnel is set up and the VXLAN is created over the IPsec tunnel, the new LAN extension interface appears on the FortiGate.



To configure the LAN extension interface and firewall policy:

1. Edit the LAN extension interface:
 - a. Go to **Network > Interfaces** and edit the LAN extension interface.
 - b. Configure the **IP/Netmask** (9.9.9.99/255.255.255.0). Other devices on the remote LAN network will configure this as their gateway.
 - c. Optionally, enable **DHCP Server** to assign IPs to the remote devices using DHCP.
 - d. Click **OK**.
2. Configure the firewall policy to allow traffic from the LAN extension interface to the WAN (port1):
 - a. Go to **Policy & Objects > Firewall Policy** and click **Create New**.
 - b. Enter the following:

Incoming Interface	FX0035919000000
Outgoing Interface	port1
Source	all

Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable (NAT)

- c. Configure the other settings as needed, such as security profiles.
- d. Click OK.

This policy allows the remote LAN clients to access the internet through the backhaul channel. Clients in the remote LAN behind the FortiExtender will now be able to receive an IP over DHCP and reach the internet securely through the FortiGate.

Using the backhaul IP when the FortiGate access controller is behind NAT - 7.0.2

When the FortiGate LAN extension controller is behind a NAT device, remote thin edge FortiExtenders must connect to the FortiGate through a backhaul address. This is an address on the upstream NAT device that forwards traffic to the FortiGate. It can be configured as an IP or FQDN on the FortiGate extender profile.

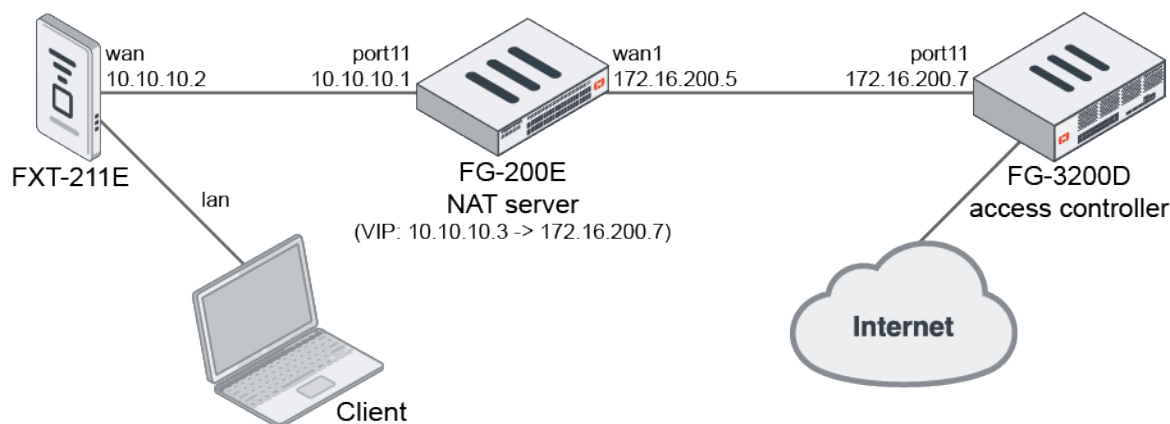
When the default IKE port 500 is not accessible, it is possible to configure a custom IKE port on the FortiExtender and FortiGate.

This topic contains four configuration examples:

- [Configuring an IP as a backhaul address in the FortiGate extender profile](#)
- [Configuring an FQDN as a backhaul address in the FortiGate extender profile](#)
- [Configuring the IKE port on FortiExtender when NAT traversal is enabled in the FortiGate IPsec tunnel settings](#)
- [Configuring the IKE port on FortiExtender when NAT traversal is disabled in the FortiGate IPsec tunnel settings](#)

Examples

The following topology is used for the first three examples and assumes the FortiExtender has already been discovered (see [Introduce LAN extension mode for FortiExtender 7.0.2 on page 614](#) for more information).



Configuring an IP as a backhaul address in the FortiGate extender profile

To configure an IP as a backhaul address in the GUI:

1. Edit the LAN extension profile:
 - a. Go to *Network > FortiExtenders*, select the *Profiles* tab, and edit the default LAN extension profile (*FX211E-lanext-default*).
 - b. In the *LAN extension* section, set the *IPsec interface IP/FQDN* to *10.10.10.3*.

Edit FortiExtender Profile

Name: FX211E-lanext-default
 Model: FX211E
 Mode: LAN extension
 Data plan: +

LAN extension

Link load balance: **Active backup** Load Balance
 IPsec interface: port1
 IPsec interface IP/FQDN: 10.10.10.3
 IPsec tunnel: fext-ipsec-bwyt

FortiExtender uplink port

Name	Uplink port	Role
1	wan	Primary
2	lte1	Secondary

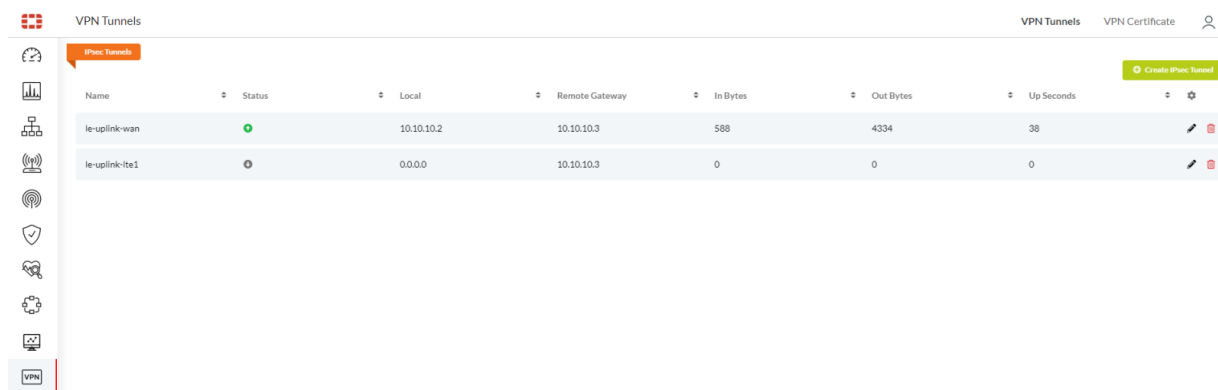
Modem 1

Default SIM: **SIM1** SIM2 Carrier Lowest cost
 SIM1 PIN: ☐
 SIM2 PIN: ☐
 GPS: ☒
 Auto SIM switch: ☐
 By disconnecting: ☐
 By signal: ☐

Additional Information: API Preview, References, Edit in CLI, Documentation, Online Help, Video Tutorials

OK Cancel

- c. Click **OK**.
2. Authorize the FortiExtender:
 - a. Go to *Network > FortiExtenders*, select the *Managed FortiExtenders* tab, and edit the discovered FortiExtender.
 - b. In the *Status* section, enable *Authorized*.
 - c. Click **OK**.
 In FortiExtender, the *VPN Tunnels* page displays the IPsec tunnel *le-uplink-wan* as up. The *Remote Gateway* is set to *10.10.10.3*.



Name	Status	Local	Remote Gateway	In Bytes	Out Bytes	Up Seconds	Actions
le-uplink-wan	●	10.10.10.2	10.10.10.3	588	4334	38	
le-uplink-lte1	●	0.0.0.0	10.10.10.3	0	0	0	

To configure an IP as a backhaul address in the CLI:

1. Configure the backhaul IP address:

```
config extender-controller extender-profile
  edit "FX211E-lanext-default"
    set id 1
    set model FX211E
    set extension lan-extension
    config cellular
      config sms-notification
      end
      config modem1
      end
    end
    config lan-extension
      set ipsec-tunnel "fext-ipsec-bwyt"
      set backhaul-interface "port1"
      set backhaul-ip "10.10.10.3"
      config backhaul
        edit "1"
          set port wan
          set role primary
        next
        edit "2"
          set port lte1
          set role secondary
        next
      end
    end
  next
end
```

2. Verify the configuration in FortiExtender:

```
config vpn ipsec phase1-interface
  edit le-uplink-wan
    set ike-version 2
    set keylife 86400
    set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
    3des-sha1
    set dhgrp 14 5
    set interface wan
```

```

set type static
set remote-gw 10.10.10.3
set authmethod psk
set psksecret *****
set localid peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRTeXnb4mUi6MmXX
set peerid localid-33rR5UQbwq705X95TyKfQ0h7GtDbMfAjX4jz6Vsm0Au8gibcCsZk09t
set add-gw-route enable
set dev-id-notification disable
next
end

```

Configuring an FQDN as a backhaul address in the FortiGate extender profile

To configure an FQDN as a backhaul address in the GUI:

1. Edit the LAN extension profile:
 - a. Go to **Network > FortiExtenders**, select the *Profiles* tab, and edit the default LAN extension profile (*FX211E-lanext-default*).
 - b. In the *LAN extension* section, set the *IPsec interface IP/FQDN* to *fgt3200d.qatest.com*.

Edit FortiExtender Profile

Name: FX211E-lanext-default
 Model: FX211E
 Mode: LAN extension
 Data plan: +

LAN extension

Link load balance: **Active backup** Load Balance
 IPsec interface: port1
 IPsec interface IP/FQDN: fgt3200d.qatest.com
 IPsec tunnel: fext-ipsec-bwyt

FortiExtender uplink port

Name	Uplink port	Role
1	wan	Primary
2	lte1	Secondary

Modem 1

Default SIM: **SIM1** SIM2 Carrier Lowest cost
 SIM1 PIN: ☐
 SIM2 PIN: ☐
 GPS: ☒
 Auto SIM switch: ☐
 By disconnecting: ☐
 By signal: ☐

OK Cancel

Additional Information

API Preview
 References
 Edit in CLI
 Documentation
 Online Help
 Video Tutorials

- c. Click OK.
2. Authorize the FortiExtender:
 - a. Go to **Network > FortiExtenders**, select the *Managed FortiExtenders* tab, and edit the discovered FortiExtender.
 - b. In the *Status* section, enable *Authorized*.
 - c. Click OK.

In FortiExtender, the *VPN Tunnels* page displays the IPsec tunnel *le-uplink-wan* as up. The *Remote Gateway* is set to *fgt3200d.qatest.com*.

Name	Status	Local	Remote Gateway	In Bytes	Out Bytes	Up Seconds	
le-uplink-wan	●	10.10.10.2	fgt3200d.qatest.com	906	4070	36	
le-uplink-lte1	●	0.0.0.0	fgt3200d.qatest.com	0	0	0	

To configure an FQDN as a backhaul address in the CLI:

1. Configure the backhaul IP address:

```
config extender-controller extender-profile
  edit "FX211E-lanext-default"
    set id 1
    set model FX211E
    set extension lan-extension
    config cellular
      config sms-notification
      end
      config modem1
      end
    end
    config lan-extension
      set ipsec-tunnel "fext-ipsec-bwyt"
      set backhaul-interface "port1"
      set backhaul-ip "fgt3200d.qatest.com"
      config backhaul
        edit "1"
          set port wan
          set role primary
        next
        edit "2"
          set port lte1
          set role secondary
        next
      end
    end
  next
end
```

2. Verify the configuration in FortiExtender:

```
config vpn ipsec phase1-interface
  edit le-uplink-wan
    set ike-version 2
    set keylife 86400
    set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
    3des-sha1
    set dhgrp 14 5
    set interface wan
```



```

set type ddns
set remotegw-ddns fgt3200d.qatest.com
set authmethod psk
set psksecret *****
set localid peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRteXnb4mUi6MmXX
set peerid localid-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZkO9t
set add-gw-route enable
set dev-id-notification disable
next
end

```

Configuring the IKE port on FortiExtender when NAT traversal is enabled in the FortiGate IPsec tunnel settings

To configure the IKE port on FortiExtender when NAT traversal is enabled:

1. Set the IKE port on the FortiGate:

```

config system settings
    set ike-port 6000
end

```

2. Set the IKE port on the FortiExtender:

```

config system settings
    set ike-port 6000
end

```

3. Start a packet capture on the FG-200E's port11 with the filter set to UDP protocol and port 4500 or 6000.
4. Terminate the IPsec VPN tunnel in FortiExtender:

```

~ # swanctl -t -i le-uplink-wan
[IKE] deleting IKE_SA le-uplink-wan[5] between 10.10.10.2[peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRteXnb4mUi6MmXX]...10.10.10.3[localid-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZkO9t]
[IKE] sending DELETE for IKE_SA le-uplink-wan[5]
[ENC] generating INFORMATIONAL request 2 [ D ]
[NET] sending packet: from 10.10.10.2[4500] to 10.10.10.3[6000] (80 bytes)
[NET] received packet: from 10.10.10.3[6000] to 10.10.10.2[4500] (80 bytes)
[ENC] parsed INFORMATIONAL response 2 [ ]
[IKE] IKE_SA deleted
terminate completed successfully

```

5. Verify the packet capture on the FG-200E. During the tunnel setup, the first packet from the FortiExtender has source port set to 6000, but it changes to 4500 since NAT traversal is enabled. FortiExtender only supports port 4500 when NAT traversal is enabled:

```

# diagnose sniffer packet port11 'udp and port 4500 or port 6000' 4
interfaces=[port11]
filters=[udp and port 4500 or port 6000]
...
24.064847 port11 -- 10.10.10.2.6000 -> 10.10.10.3.6000: udp 936
24.065929 port11 -- 10.10.10.3.6000 -> 10.10.10.2.6000: udp 428

24.119178 port11 -- 10.10.10.2.4500 -> 10.10.10.3.6000: udp 612
24.120272 port11 -- 10.10.10.3.6000 -> 10.10.10.2.4500: udp 276

```

6. Verify the IPsec tunnel status in FortiExtender to confirm port 4500 is used:

```

~ # swanctl -l
le-uplink-wan: #3, ESTABLISHED, IKEv2, 1fbb2997d6a5afc7_i* 5d500758882339f4_r
  local 'peerid-SIbiT5AnbTo2tk0pZttfxzh1CFihu9tP7EBsKniCpRTeXnb4mUi6MmXX' @ 10.10.10.2
[4500]
  remote 'localid-33rR5UQbwq705X95TyKfQOh7GtDbMfAjX4jz6Vsm0Au8gibcCsZkO9t' @ 10.10.10.3
[6000]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  established 90s ago, rekeying in 85289s
le-uplink-wan: #3, reqid 3, INSTALLED, TUNNEL-in-UDP, ESP:AES_CBC-128/HMAC_SHA1_96
  installed 90s ago, rekeying in 38952s, expires in 47430s
  in c3406a5a (0x00000005), 1512 bytes, 18 packets, 2s ago
  out 7d17257c (0x00000005), 8000 bytes, 52 packets, 2s ago
  local 10.252.8.2/32
  remote 10.252.8.1/32

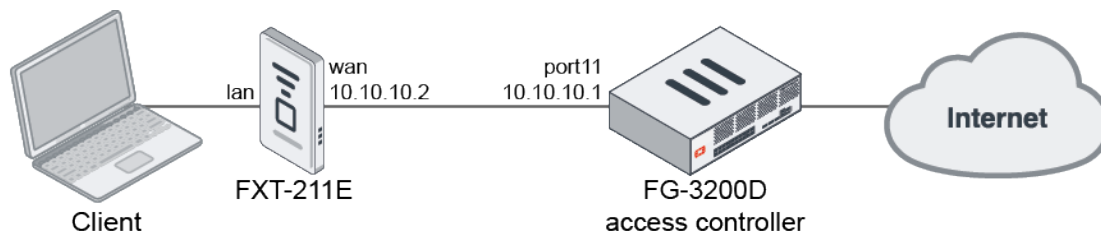
```



NAT traversal has default value enabled in the FortiGate IPsec tunnel settings, and it is not recommended to change any IPsec tunnel configurations, even if there is a NAT server between the FortiExtender and FortiGate access controller. The IPsec tunnel will always use port 4500 for NAT traversal.

Configuring the IKE port on FortiExtender when NAT traversal is disabled in the FortiGate IPsec tunnel settings

NAT traversal is enabled by default in the FortiGate IPsec tunnel setting and it cannot be changed in the GUI. If NAT traversal is disabled, the IPsec tunnel can use a custom IKE port (port 6300 in this example).



To configure the IKE port on FortiExtender when NAT traversal is disabled:

1. Set the IKE port on the FortiGate:

```

config system settings
  set ike-port 6300
end

```

2. Set the IKE port on the FortiExtender:

```

config system settings
  set ike-port 6300
end

```

3. Verify the IPsec tunnel status in FortiExtender to confirm port 6300 is used:

```

~ # swanctl -l
le-uplink-wan: #2, ESTABLISHED, IKEv2, 14a9fe5800b9d0b9_i* 9dd465f634ed9abd_r
  local 'peerid-aRuaScJBVVJ1DWKrrKcY8VcHF8Vg6cgLQkpEtdzDRpRTVvapxdeeJoiO' @ 10.10.10.2

```

```
[6300]
remote 'localid-dCcVF2kc5PWVuKbNvWEoBlm332ik5dz1jtRqxfaxxiH4G7y5wLDAPcN' @ 10.10.10.1
[6300]
AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
established 3606s ago, rekeying in 82066s
le-uplink-wan: #1, reqid 1, INSTALLED, TUNNEL, ESP:AES_CBC-128/HMAC_SHA1_96
  installed 3606s ago, rekeying in 37205s, expires in 43914s
  in  c3ae8beb (0x00000003),  60564 bytes,   721 packets,    1s ago
  out d0d92a63 (0x00000003), 343410 bytes, 2365 packets,    1s ago
  local 10.252.8.2/32
  remote 10.252.8.1/32
```

Bandwidth limits on the FortiExtender Thin Edge - 7.0.2

The FortiGate LAN extension controller can push a bandwidth limit to the FortiExtender Thin Edge. The limit is enforced on the FortiExtender using traffic shaping.

To configure a bandwidth limit:

1. On the FortiGate, create a LAN extension profile with bandwidth control enabled and a bandwidth limit configured (in Mbps):

```
config extender-controller extender-profile
  edit "FX200F-lanext-default"
    set model FX200F
    set extension lan-extension
    set enforce-bandwidth enable
    set bandwidth-limit 20
  next
end
```

2. Add a FortiExtender in LAN extension mode and apply the profile to it:

```
config extender-controller extender
  edit "FX0035919000000"
    set id "FX200F5919000000"
    set authorized enable
    set extension-type lan-extension
    set profile "FX200F-lanext-default"
  next
end
```

3. On the FortiExtender, confirm that the bandwidth configuration has been pushed to it:

```
config firewall shaper
  config traffic-shaper
    edit le-traffic-shaper
      set max-bandwidth 20
      set bandwidth-unit mbps
    next
  end
end
config firewall shaping-policy
  edit le-shaping-policy
    set status enable
```

```
        set dstintf le-agg-link
        set traffic-shaper le-traffic-shaper
    next
end
```

If bandwidth enforcement is disabled on the FortiGate, the configuration that was pushed to the FortiExtender will be removed.

Log and report

This section includes information about logging and reporting related new features:

- [Logging on page 631](#)

Logging

This section includes information about logging related new features:

- [Add logs for the execution of CLI commands on page 631](#)
- [Logging IP address threat feeds in sniffer mode on page 632](#)
- [Enhance TLS logging 7.0.1 on page 633](#)
- [Generate unique user name for anonymized logs 7.0.2 on page 635](#)
- [Support TACACS+ accounting 7.0.2 on page 639](#)
- [Add dstuser field to UTM logs 7.0.2 on page 641](#)

Add logs for the execution of CLI commands

The `cli-audit-log` option records the execution of CLI commands in system event logs (log ID 44548). In addition to `execute` and `config` commands, `show`, `get`, and `diagnose` commands are recorded in the system event logs.

The `cli-audit-log` data can be recorded on memory or disk, and can be uploaded to FortiAnalyzer, FortiGate Cloud, or a syslog server.

To enable the CLI audit log option:

```
config system global
    set cli-audit-log enable
end
```

To view system event logs in the GUI:

1. Run the command in the CLI (`# show log fortianalyzer setting`).
2. Go to *Log & Report > Events > System Events*.
3. In the log location dropdown, select *Memory*.

4. Select the log entry and click *Details*.

Date/Time	Level	User	Message	Log Description	Log Details
40 seconds ago	Information		Delete 60 old report files	Outdated report files deleted	
Minute ago	Information	admin	show log fortianalyzer setting	Action performed	General Date 2021/03/03 Time 12:12:11 Virtual Domain root Log Description Action performed
Minute ago	Information	admin	Edit system.global	Attribute configured	
2 minutes ago	Information		stitch:Test is triggered.	Automation stitch triggered	
2 minutes ago	Information	admin	Administrator admin logged in successfully from jsconsole	Admin login successful	Source User admin
5 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	Action Action Show
5 minutes ago	Information		Delete 35 old report files	Outdated report files deleted	
10 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	Security Level Information
10 minutes ago	Information		Delete 36 old report files	Outdated report files deleted	
14 minutes ago	Information		DHCP statistics	DHCP statistics	Event User Interface jsconsole(2.0.248.28) Message show log fortianalyzer setting
14 minutes ago	Information		DHCP statistics	DHCP statistics	
14 minutes ago	Information		DHCP statistics	DHCP statistics	
14 minutes ago	Information		DHCP statistics	DHCP statistics	
14 minutes ago	Information		DHCP statistics	DHCP statistics	
14 minutes ago	Information		Fortigate scheduled update fcni=yes fdni=yes fsci=yes from 173.243.140...	FortiGate update succeeded	Other Log event original timestamp 1614902331006465000 Timezone -0800 Log ID 0100044548 Type event Sub Type system
15 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	
15 minutes ago	Information		Delete 38 old report files	Outdated report files deleted	
20 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	
20 minutes ago	Information		Delete 35 old report files	Outdated report files deleted	
25 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	
25 minutes ago	Information		Delete 36 old report files	Outdated report files deleted	
30 minutes ago	Information		Fortigate scheduled update fcni=yes fdni=yes fsci=yes from 173.243.140...	FortiGate update succeeded	
30 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	
30 minutes ago	Information		Delete 36 old report files	Outdated report files deleted	
35 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	
35 minutes ago	Information		Delete 35 old report files	Outdated report files deleted	
40 minutes ago	Information		Performance statistics: average CPU: 0, memory: 49, concurrent sessions: ...	System performance statistics	

To display the logs:

```
# execute log filter device disk
# execute log filter category event
# execute log filter field subtype system
# execute log filter field logid 0100044548
# execute log display
```

Sample log:

```
1: date=2020-11-16 time=10:43:00 eventtime=1605552179970875703 tz="-0800" logid="0100044548"
type="event" subtype="system" level="information" vd="root" logdesc="Action performed"
user="admin" ui="jsconsole(2.0.225.112)" action="Show" msg="show log fortianalyzer setting"

2: date=2020-11-16 time=10:42:43 eventtime=1605552163502003054 tz="-0800" logid="0100044548"
type="event" subtype="system" level="information" vd="root" logdesc="Action performed"
user="admin" ui="jsconsole(2.0.225.112)" action="Get" msg="get sys status"

3: date=2020-11-16 time=09:47:04 eventtime=1605548824762387718 tz="-0800" logid="0100044548"
type="event" subtype="system" level="information" vd="root" logdesc="Action performed"
user="admin" ui="jsconsole(2.0.228.202)" action="Diagnose" msg="diagnose log test"
```

Logging IP address threat feeds in sniffer mode

In sniffer mode, you can record traffic logs each time a source or destination address matches an IP address on an external threat feed.

```
config firewall sniffer
edit <id>
set logtraffic all
```

```

        set interface <interface>
        set ip-threatfeed-status {enable | disable}
        set ip-threatfeed <threat feed> ...
    next
end

```

ip-threatfeed-status {enable disable}	Enable/disable the IP threat feed.
ip-threatfeed <threat feed> ...	The name of an existing IP threat feed.

When the IP matches multiple threat feeds, the sniffer log will use the last external connector in the configuration, which is different from the normal firewall policy log that uses the first external connector in the configuration.

When the threat feed is enabled and configured in a sniffer policy, as long as the traffic IP matches threat feed, there will be a traffic log for it (even if `logtraffic` is set to `all` or `utm`).

To configure a sniffer policy to log the threat feed:

1. Enable inserting address UUIDs in traffic logs:

```

config system global
    set log-uuid-address enable
end

```

2. Configure the sniffer policy:

```

config firewall sniffer
    edit 1
        set logtraffic all
        set ipv6 enable
        set interface "port3"
        set ip-threatfeed-status enable
        set ip-threatfeed "g-source"
    next
end

```

Sample log

```

1: date=2021-01-26 time=15:51:37 eventtime=1611705097880421908 tz="-0800" logid="0004000017"
type="traffic" subtype="sniffer" level="notice" vd="vd1" srcip=10.1.100.12 srcport=34604
srcintf="port3" srcintfrole="undefined" dstip=172.16.200.55 dstport=80 dstintf="port3"
dstintfrole="undefined" srcthreadfeed="g-source" srccountry="Reserved" dstcountry="Reserved"
sessionid=30384 proto=6 action="accept" policyid=1 policytype="sniffer" service="HTTP"
trandisp="snat" transip=0.0.0.0 transport=0 duration=0 sentbyte=0 rcvbyte=0 sentpkt=0
rcvpkt=0 appcat="unscanned"

```

Enhance TLS logging - 7.0.1

New options have been added to the SSL/SSH profile to log server certificate information and TLS handshakes. New fields are added to the UTM SSL logs when these options are enabled.

```

config firewall ssl-ssh-profile
    edit <name>
        set ssl-server-cert-log {enable | disable}

```

```

        set ssl-handshake-log {enable | disable}
    next
end

```

To enable logging of server certificate information and TLS handshakes:

1. Configure the SSL/SSH protocol options:

```

config firewall ssl-ssh-profile
    edit "deep-inspection-clone"
        set comment "Read-only deep inspection profile."
        config https
            set ports 443
            set status deep-inspection
        end
        ...
        set ssl-exemptions-log enable
        set ssl-negotiation-log enable
        set ssl-server-cert-log enable
        set ssl-handshake-log enable
    next
end

```

2. Configure the firewall policy:

```

config firewall policy
    edit 1
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "deep-inspection-clone"
        set av-profile "av"
        set logtraffic all
        set nat enable
    next
end

```

Sample SSL server certificate log

```

1: date=2021-06-17 time=16:55:26 eventtime=1623974126384215772 tz="-0700" logid="1702062103"
type="utm" subtype="ssl" eventtype="ssl-negotiation" level="information" vd="vdom1"
action="info" policyid=1 sessionid=6361 service="HTTPS" profile="deep-inspection-clone"
srcip=10.1.100.11 srcport=48892 dstip=18.140.21.233 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" srcuid="8666f70e-cfb9-51eb-
4991-9012417d69da" dstuid="8666f70e-cfb9-51eb-4991-9012417d69da" proto=6
sni="www.fortinet.com" eventssubtype="server-cert-info" hostname="www.fortinet.com"
notbefore="2021-03-13T00:00:00Z" notafter="2022-04-13T23:59:59Z" issuer="DigiCert TLS RSA
SHA256 2020 CA1" cn="*.fortinet.com" san="*.fortinet.com;www.fortinet.com;fortinet.com"
sn="000aa00a00000a00000a00a00aa00a0" ski="df9152b605cc18b346efb34de6907275dbdb2b3c"
certhash="1d55cd34a1ed5d3f69bd825a45e04fbd2efba937" keyalgo="rsa" keysize=2048

```

Sample SSL handshake log

```

2: date=2021-06-17 time=16:55:26 eventtime=1623974126411127210 tz="-0700" logid="1702062103"
type="utm" subtype="ssl" eventtype="ssl-negotiation" level="information" vd="vdom1"
action="info" policyid=1 sessionid=6361 service="HTTPS" profile="deep-inspection-clone"
srcip=10.1.100.11 srcport=48892 dstip=18.140.21.233 dstport=443 srcintf="port2"
srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" srcuid="8666f70e-cfb9-51eb-

```



```
4991-9012417d69da" dstuuid="8666f70e-cfb9-51eb-4991-9012417d69da" proto=6 tlsver="tls1.3"
sni="www.fortinet.com" cipher="0x1302" authalgo="rsa" kxproto="ecdhe" kxcurve="secp256r1"
eventssubtype="handshake-done" hostname="www.fortinet.com" handshake="full" mitm="yes"
```

To view the logs in the GUI:

1. Go to *Log & Report > SSL*.

Service	Destination	Common Na...	Event Subtype	Event Type	Man-in-the-middle	TLS Version	Hostname	Issuer
HTTPS	18.140.21.233 (www.fortinet.com)		handshake-done	ssl-negotiation	yes	tls1.3	www.fortinet.com	
HTTPS	18.140.21.233 (www.fortinet.com)	*.fortinet.com	server-cert-info	ssl-negotiation			www.fortinet.com	DigiCert TLS RSA SHA2

Generate unique user name for anonymized logs - 7.0.2

With the `anonymization-hash` option, user fields in logs can be anonymized by generating a hash based on the user name and salt value. The hash for the same user will generate the same hash value, allowing the anonymized user to be correlated between logs.

```
config log setting
    set user-anonymize enable
    set anonymization-hash <salt string>
end
```

Example

In this example, user names are encrypted in traffic and event logs using the `anonymization-hash` option.

To encrypt the user name for logs in the GUI:

1. Configure the hash anonymization in the CLI:

```
config log setting
    set user-anonymize enable
    set anonymization-hash "random"
end
```

2. Configure a firewall policy with a user as a source:

- a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
- b. For *Source*, select a user.
- c. In the *Security Profiles* section, enable *AntiVirus* and select a profile.
- d. Configure the other settings as needed.
- e. Click *OK*.

3. Verify the forward traffic log:

- Go to *Log & Report > Forward Traffic*.
- Select an entry and double-click to view the log details.

Date/Time	Source	Device	Destination	Application Name	Security Events	Result	Policy ID	Log Details
29 seconds ago	e8557d12f6551b2d (10.1.100.72)		172.16.200.75		AV 1	Deny: UTM Blocked	WAN_out (1	Details Security
32 seconds ago	172.16.200.75		10.1.100.72			Deny: policy violation	WAN_in (3)	General
3 hours ago	anonymous (10.1.100.72)		172.16.200.75		AV 1	Deny: UTM Blocked	WAN_out (1	Absolute Date/Time 2021/09/09 15:24:52
3 hours ago	172.16.200.75		10.1.100.72			Deny: policy violation	WAN_in (3)	Time 15:24:52
5 hours ago	e8557d12f6551b2d (10.1.100.72)		172.16.200.75		AV 1	Deny: UTM Blocked	WAN_out (1	Duration 1s
5 hours ago	172.16.200.75		10.1.100.72			Deny: policy violation	WAN_in (3)	Session ID 383
								Virtual Domain vdom1
								NAT Translation Source
<div> <div>Source</div> <div>IP 10.1.100.72</div> <div>NAT IP 172.16.200.7</div> <div>Source Port 33250</div> <div>Country/Region Reserved</div> <div>Primary MAC</div> <div>Source Interface VLAN20 (dmz)</div> <div>OS Name Linux</div> <div>User e8557d12f6551b2d</div> </div> <div> <div>Destination</div> <div>IP 172.16.200.75</div> <div>Port 80</div> <div>Destination MAC</div> <div>Country/Region Reserved</div> <div>Destination Interface VLAN30 (wan1)</div> </div> <div> <div>Application Control</div> <div>Application Name</div> <div>Category unscanned</div> <div>Risk undefined</div> <div>Protocol 6</div> <div>Service HTTP</div> </div> <div> <div>Data</div> <div>Received Bytes 6 kB</div> <div>Received Packets 8</div> <div>Sent Bytes 469 B</div> <div>Sent Packets 6</div> <div>LAN In 149 B</div> <div>LAN Out 149 B</div> </div>								

The user name has a hashed value of e8557d12f6551b2d.

4. Verify the antivirus traffic log:

- Go to *Log & Report > AntiVirus*.
- Select an entry and double-click to view the log details.

#	Date/Time	Service	Source	File Name	Virus/Botnet	Details	Action	Log Details
1	4 minutes ago	HTTP	e8557d12f6551b2d (10.1.100.72)	eicar.com	EICAR_TEST_FILE	No user information	blocked	General
<div> <div>General</div> <div>Absolute Date/Time 2021/09/09 15:24:51</div> <div>Time 15:24:51</div> <div>Session ID 383</div> <div>Virtual Domain vdom1</div> <div>Agent Wget/1.17.1</div> </div> <div> <div>Source</div> <div>IP 10.1.100.72</div> <div>Source Port 33250</div> <div>Source Interface VLAN20 (dmz)</div> <div>Source UUID 877d43a4-c2f9-51eb-f78f-e09794924d8a</div> <div>User e8557d12f6551b2d</div> </div> <div> <div>Destination</div> <div>IP 172.16.200.75</div> <div>Port 80</div> <div>Destination Interface VLAN30 (wan1)</div> <div>Destination UUID 877d43a4-c2f9-51eb-f78f-e09794924d8a</div> <div>URL http://172.16.200.75/eicar.com</div> </div> <div> <div>Application Control</div> <div>Protocol 6</div> <div>Service HTTP</div> </div> <div> <div>Data</div> <div>File Name eicar.com</div> </div> <div> <div>Action</div> <div>Action blocked</div> <div>Threat 2</div> <div>Policy ID 1</div> </div> <div> <div>Security</div> <div>Level</div> <div>Threat Level Critical</div> <div>Threat Score 60</div> </div>								

The user name has the same hashed value. Hovering over the user name displays a *No user information* tooltip.

5. Verify the event log:
 - a. Go to *Log & Report > Events > System Events*.
 - b. Select an entry and double-click to view the log details.

Add Filter							System Events	Details
#	Date/Time	Absolute Date/Time	Level	User	Message	Log Description	Log Details	
1	10 seconds ago	2021-09-09 10:00:33	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable	<div>General</div> <div>Absolute Date/Time 2021/09/09 09:59:09</div> <div>Time 09:59:09</div> <div>Virtual Domain vdom1</div> <div>Log Description Admin login successful</div> <div>Source</div> <div>IP 10.6.30.254</div> <div>User 6a4d668735f5517a</div> <div>Destination</div> <div>IP 10.6.30.107</div> <div>Action</div> <div>Action login</div> <div>Status success</div> <div>Reason none</div> <div>Security</div> <div>Level</div> <div>Cellular</div> <div>Serial Number</div> <div>Event</div> <div>Profile Name super_admin</div> <div>User Interface https(10.6.30.254)</div> <div>Message Administrator 6a4d668735f5517a logged in successfully from https(10.6.30.254)</div> <div>Other</div> <div>Log event original timestamp 1631206750109938400</div> <div>Timezone -0700</div> <div>Log ID 0100032001</div> <div>Type event</div> <div>Sub Type system</div> <div>Method https</div>	
2	20 seconds ago	2021-09-09 10:00:23	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
3	30 seconds ago	2021-09-09 10:00:13	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
4	40 seconds ago	2021-09-09 10:00:03	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
5	50 seconds ago	2021-09-09 09:59:53	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
6	Minute ago	2021-09-09 09:59:43	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
7	Minute ago	2021-09-09 09:59:33	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
8	Minute ago	2021-09-09 09:59:23	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
9	Minute ago	2021-09-09 09:59:13	No user information		FortiGuard hostname	FortiGuard hostname unresolvable		
10	Minute ago	2021-09-09 09:59:09	Administrator 6a4d668735f5517a	6a4d668735f5517a	Administrator 6a4d668735f5517a logged in successfully	Admin login successful		
11	Minute ago	2021-09-09 09:59:03	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
12	Minute ago	2021-09-09 09:58:52	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
13	2 minutes ago	2021-09-09 09:58:42	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
14	2 minutes ago	2021-09-09 09:58:33	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
15	2 minutes ago	2021-09-09 09:58:23	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
16	2 minutes ago	2021-09-09 09:58:13	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
17	2 minutes ago	2021-09-09 09:58:03	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
18	2 minutes ago	2021-09-09 09:57:53	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
19	3 minutes ago	2021-09-09 09:57:43	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
20	3 minutes ago	2021-09-09 09:57:33	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
21	3 minutes ago	2021-09-09 09:57:23	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
22	3 minutes ago	2021-09-09 09:57:13	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
23	3 minutes ago	2021-09-09 09:57:03	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
24	3 minutes ago	2021-09-09 09:56:53	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
25	4 minutes ago	2021-09-09 09:56:43	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		
26	4 minutes ago	2021-09-09 09:56:32	unable to resolve FortiGuard hostname		unable to resolve FortiGuard hostname	FortiGuard hostname unresolvable		

The administrative user has a hashed value of 6a4d668735f5517a.

To encrypt the user name for logs in the CLI:

1. Configure the hash anonymization:

```
config log setting
    set user-anonymize enable
    set anonymization-hash "random"
end
```

2. Configure a firewall policy with a user as a source:

```
config firewall policy
    edit 1
        set name "WAN_out"
        set srcintf "dmz"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
    end
```

```

        set ssl-ssh-profile "deep-inspection"
        set av-profile "g-default"
        set nat enable
        set users "bob"
    next
end

```

3. Verify the forward traffic log. The user name has a hashed value of e8557d12f6551b2d:

```

date=2021-09-09 time=15:24:52 eventtime=1631226292981803646 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1"
srcip=10.1.100.72 srcport=33250 srcintf="dmz" srcintfrole="undefined"
dstip=172.16.200.75 dstport=80 dstintf="wan1" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=383 proto=6 action="client-rst"
policyid=1 policytype="policy" poluid="12f6f924-c2fb-51eb-6e06-3b997d55d5f4"
policyname="WAN_out" user="e8557d12f6551b2d" dstuser="e8557d12f6551b2d" service="HTTP"
trandisp="snat" transip=172.16.200.7 transport=33250 duration=1 sentbyte=469
rcvdbyte=6331 sentpkt=6 rcvdpkt=8 appcat="unscanned" wanin=369 wanout=149 lanin=149
lanout=149 utmaction="block" countav=1 crscore=50 craction=2 srchwvndor="VMware"
osname="Linux" mastersrcmac="*:~*:~*:~*:~*:~*" srcmac="*:~*:~*:~*:~*" srcserver=0
dsthwvndor="VMware" dstosname="Linux" masterdstmac="*:~*:~*:~*:~*"
dstmac="*:~*:~*:~*:~*" dstserver=0 utmref=0-28

```

4. Verify the antivirus traffic log. The user name has the same hashed value:

```

date=2021-09-09 time=15:24:51 eventtime=1631226291945007723 tz="-0700"
logid="0211008192" type="utm" subtype="virus" eventtype="infected" level="warning"
vd="vdom1" policyid=1 msg="File is infected." action="blocked" service="HTTP"
sessionid=383 srcip=10.1.100.72 dstip=172.16.200.75 srcport=33250 dstport=80
srcintf="dmz" srcintfrole="undefined" dstintf="wan1" dstintfrole="undefined"
srcuuid="877d43a4-c2f9-51eb-f78f-e09794924d8a" dstuuid="877d43a4-c2f9-51eb-f78f-
e09794924d8a" proto=6 direction="incoming" filename="eicar.com" quarskip="File-was-not-
quarantined" virus="EICAR_TEST_FILE" viruscat="Virus" dtype="av-engine"
ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172
url="http://172.16.200.75/eicar.com" profile="g-default" user="e8557d12f6551b2d"
dstuser="e8557d12f6551b2d" agent="Wget/1.17.1" analyticssubmit="false" crscore=50
craction=2 crlevel="critical"

```

5. Verify the event log. The administrative user has a hashed value of 6a4d668735f5517a:

```

date=2021-09-09 time=09:59:09 eventtime=1631206750109938510 tz="-0700"
logid="0100032001" type="event" subtype="system" level="information" vd="vdom1"
logdesc="Admin login successful" sn="*****" user="6a4d668735f5517a" ui="https
(10.6.30.254)" method="https" srcip=10.6.30.254 dstip=10.6.30.107 action="login"
status="success" reason="none" profile="super_admin" msg="Administrator 6a4d668735f5517a
logged in successfully from https(10.6.30.254)"

```

If user-anonymize is enabled in the log settings and anonymization-hash is left blank, the user name is displayed as anonymous in the logs.

Sample traffic log:

```

date=2021-09-09 time=11:27:44 eventtime=1631212064444723180 tz="-0700" logid="0000000013"
type="traffic" subtype="forward" level="notice" vd="vdom1" srcip=10.1.100.72 srcport=33246
srcintf="dmz" srcintfrole="undefined" dstip=172.16.200.75 dstport=80 dstintf="wan1"
dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=1337 proto=6
action="client-rst" policyid=1 policytype="policy" poluid="12f6f924-c2fb-51eb-6e06-
3b997d55d5f4" policyname="WAN_out" user="anonymous" dstuser="anonymous" service="HTTP"
trandisp="snat" transip=172.16.200.7 transport=33246 duration=1 sentbyte=469 rcvdbyte=6331

```

```
sentpkt=6 rcvdpkt=8 appcat="unscanned" wanin=369 wanout=149 lanin=149 lanout=149
utmaction="block" countav=1 crscore=50 craction=2 srchvwvendor="VMware" osname="Linux"
mastersrcmac="*:*:*:*:*:*" srcmac="*:*:*:*:*:*" srcserver=0 dsthwvendor="VMware"
dstosname="Linux" masterdstmac="*:*:*:*:*:*" dstmac="*:*:*:*:*:*" dstserver=0
utmref=0-14
```

Sample UTM log:

```
date=2021-09-09 time=11:27:43 eventtime=1631212063400129220 tz="-0700" logid="0211008192"
type="utm" subtype="virus" eventtype="infected" level="warning" vd="vdom1" policyid=1
msg="File is infected." action="blocked" service="HTTP" sessionid=1337 srcip=10.1.100.72
dstip=172.16.200.75 srcport=33246 dstport=80 srcintf="dmz" srcintfrole="undefined"
dstintf="wan1" dstintfrole="undefined" srcuuid="877d43a4-c2f9-51eb-f78f-e09794924d8a"
dstuuid="877d43a4-c2f9-51eb-f78f-e09794924d8a" proto=6 direction="incoming"
filename="eicar.com" quarskip="File-was-not-quarantined" virus="EICAR_TEST_FILE"
viruscat="Virus" dtype="av-engine" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE"
virusid=2172 url="http://172.16.200.75/eicar.com" profile="g-default" user="anonymous"
dstuser="anonymous" agent="Wget/1.17.1" analyticssubmit="false" crscore=50 craction=2
crlevel="critical"
```

Sample event log:

```
date=2021-09-09 time=11:27:26 eventtime=1631212046861637260 tz="-0700" logid="0100032102"
type="event" subtype="system" level="alert" vd="vdom1" logdesc="Configuration changed"
user="anonymous" ui="jsconsole" msg="Configuration is changed in the anonymous session"
```

Support TACACS+ accounting - 7.0.2

Customers can send system log entries to external TACACS+ accounting servers. Up to three external TACACS+ servers can be configured with different filters for log events. These filters include TACACS+ accounting for login events, configuration change events, and CLI command audits.

In the following example, one remote TACACS+ accounting server is configured and administrators log in to the FortiGate with SSH and HTTPS sessions to modify existing configurations. All events are sent to the TACACS+ accounting server.

To configure remote TACACS+ accounting:

1. Enable TACACS+ accounting and enter the server access information:

```
config log tacacs+accounting setting
    set status enable
    set server "10.1.100.34"
    set server-key *****
end
```

2. Configure the log message filters:

```
config log tacacs+accounting filter
    set login-audit enable
    set config-change-audit enable
    set cli-cmd-audit enable
end
```

3. Log in to the FortiGate with SSH and HTTPS sessions, and rename a local user.

4. Log off from the FortiGate and check the logs on the remote TACACS+ server:

- System events logs for SSH administrator session:

```
<102> 2021-09-10 08:35:52 [10.1.100.9:20537] 09/10/2021 08:35:52 NAS_IP=10.1.100.9
Port=ssh rem_addr=172.16.200.254 User=test1 Flags=Start service=fortigate event=sys_
acct start_time=1631288152644311549 reason="Administrator test1 logged in
successfully from ssh(172.16.200.254)" task_id=1631288152
<102> 2021-09-10 08:36:27 [10.1.100.9:20573] 09/10/2021 08:36:27 NAS_IP=10.1.100.9
Port= User=test1 Flags=Stop service=fortigate event=sys_acct stop_
time=1631288186895709341 reason="Rename user.local local-101 to local-102"
<102> 2021-09-10 08:37:09 [10.1.100.9:20625] 09/10/2021 08:37:09 NAS_IP=10.1.100.9
Port=ssh rem_addr=172.16.200.254 User=test1 Flags=Stop service=fortigate event=sys_
acct stop_time=1631288229650641602 reason="Administrator test1 logged out from ssh
(172.16.200.254)" task_id=1631288152
```

- System events logs for HTTPS administrator session:

```
<102> 2021-09-10 08:43:54 [10.1.100.9:20871] 09/10/2021 08:43:54 NAS_IP=10.1.100.9
Port=https rem_addr=172.16.200.254 User=admin Flags=Start service=fortigate
event=sys_acct start_time=1631288634531042178 reason="Administrator admin logged in
successfully from https(172.16.200.254)" task_id=1631288634
<102> 2021-09-10 08:44:21 [10.1.100.9:21020] 09/10/2021 08:44:21 NAS_IP=10.1.100.9
Port= User=admin Flags=Stop service=fortigate event=sys_acct stop_
time=1631288661938560301 reason="Rename user.local local-new to local-new-1"
<102> 2021-09-10 08:45:49 [10.1.100.9:21093] 09/10/2021 08:45:49 NAS_IP=10.1.100.9
Port=https rem_addr=172.16.200.254 User=admin Flags=Stop service=fortigate event=sys_
acct stop_time=1631288749504281964 reason="Administrator admin logged out from https
(172.16.200.254)" task_id=1631288634
```

By default, the system event logs sent to the TACACS+ server contain configuration modifications. To include `execute`, `show`, `get`, and `diagnose` commands in the system event logs, enable `cli-audit-log`.

To enable the CLI audit log option:

```
config system global
    set cli-audit-log enable
end
```

Sample TACACS+ server logs for diagnose and execute commands:

```
<102> 2021-09-27 14:19:11 [10.1.100.5:5568] 09/27/2021 14:19:11 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777550865151332
reason="dia sniffer packet any icmp" cmd=Diagnose
<102> 2021-09-27 14:19:33 [10.1.100.5:5583] 09/27/2021 14:19:33 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777572609260119
reason="dia test authserver ldap FORTINET-FSSO test2 test2" cmd=Diagnose
<102> 2021-09-27 14:19:38 [10.1.100.5:5587] 09/27/2021 14:19:38 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777577591769970
reason="exec log display" cmd=Execute
<102> 2021-09-27 14:20:22 [10.1.100.5:5615] 09/27/2021 14:20:22 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777621524026363
reason="exec log delete-all" cmd=Execute
<102> 2021-09-27 14:20:38 [10.1.100.5:5627] 09/27/2021 14:20:38 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777637777273617
reason="exec log filter category event" cmd=Execute
<102> 2021-09-27 14:20:42 [10.1.100.5:5633] 09/27/2021 14:20:42 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777641616751047
```

```

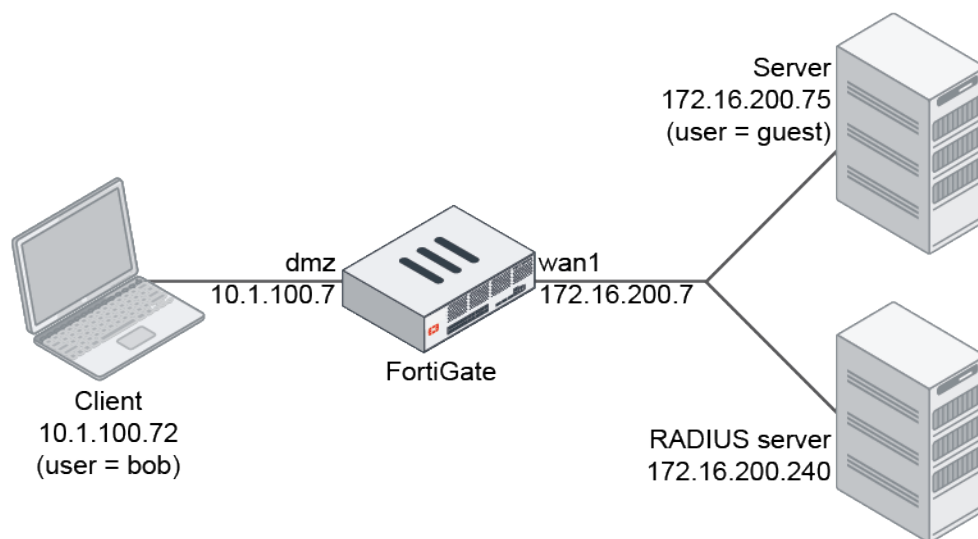
reason="exec log display" cmd=Execute
<102> 2021-09-27 14:20:53 [10.1.100.5:5639] 09/27/2021 14:20:53 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777652516689886
reason="dia test authserver ldap FORTINET-FSSO test2 test2" cmd=Diagnose
<102> 2021-09-27 14:20:56 [10.1.100.5:5642] 09/27/2021 14:20:56 NAS_IP=10.1.100.5 Port=
User=admin Flags=Stop service=fortigate event=cmd_acct stop_time=1632777656330649349
reason="exec log display" cmd=Execute

```

Add dstuser field to UTM logs - 7.0.2

The dstuser field in UTM logs records the username of a destination device when that user has been authenticated on the FortiGate.

Examples



In the following topology, the user, bob, is authenticated on a client computer. The user, guest, is authenticated on the server. Log are collected for AV and IPS in flow inspection mode. Logs are collected for application control and web filter in proxy mode.

To configure the RADIUS user and user groups:

1. Configure the RADIUS server:

```

config user radius
    edit "Ubuntu_docker"
        set server "172.16.200.240"
        set secret *****
    next
end

```

2. Configure the local user:

```

config user local
    edit "guest"
        set type password
    next
end

```

```
        set passwd *****
    next
end
```

3. Configure the RADIUS user groups:

```
config user group
    edit "RADIUS_User_Group"
        set member "Ubuntu_docker"
    next
    edit "Local_User"
        set member "guest"
    next
end
```

Flow inspection mode

To verify AV and IPS logs in flow mode:

1. Configure the firewall policies:

```
config firewall policy
    edit 1
        set name "WAN_out"
        set srcintf "dmz"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "g-default"
        set ips-sensor "sensor-11"
        set nat enable
        set groups "RADIUS_User_Group" "Local_User"
    next
    edit 3
        set name "WAN_in"
        set srcintf "wan1"
        set dstintf "dmz"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set groups "RADIUS_User_Group" "Local_User"
    next
end
```

2. Verify the AV log:

```
date=2021-09-14 time=16:37:25 eventtime=1631662646131356720 tz="-0700"
logid="0211008192" type="utm" subtype="virus" eventtype="infected" level="warning"
```



```
vd="vdom1" policyid=1 msg="File is infected." action="blocked" service="HTTP"
sessionid=4613 srcip=10.1.100.72 dstip=172.16.200.75 srcport=60086 dstport=80
srcintf="dmz" srcintfrole="undefined" dstintf="wan1" dstintfrole="undefined"
srcuuid="877d43a4-c2f9-51eb-f78f-e09794924d8a" dstuuid="877d43a4-c2f9-51eb-f78f-
e09794924d8a" proto=6 direction="incoming" filename="eicar.com" quarskip="Quarantine-
disabled" virus="EICAR_TEST_FILE" viruscat="Virus" dtype="av-engine"
ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172
url="http://172.16.200.75/eicar.com" profile="g-default" user="bob" group="RADIUS_User_
Group" authserver="Ubuntu_docker" dstuser="guest" agent="Wget/1.17.1"
analyticsscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"
analyticsssubmit="false" crscore=50 craction=2 crlevel="critical"
```

3. Verify the IPS log:

```
date=2021-09-14 time=16:56:06 eventtime=1631663765992499880 tz="-0700"
logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert"
vd="vdom1" severity="info" srcip=10.1.100.72 srccountry="Reserved" dstip=172.16.200.75
srcintf="dmz" srcintfrole="undefined" dstintf="wan1" dstintfrole="undefined"
sessionid=7881 action="dropped" proto=6 service="HTTP" policyid=1
attack="Eicar.Virus.Test.File" srcport=60092 dstport=80 direction="incoming"
attackid=29844 profile="sensor-11" ref="http://www.fortinet.com/ids/VID29844" user="bob"
group="RADIUS_User_Group" authserver="Ubuntu_docker" dstuser="guest"
incidentserialno=17825794 attackcontextid="2/2"
attackcontext="dGVudC1MZW5ndGg6IDY4DQpLZWVwLUFsaXZlOiB0aW1lb3V0PTUsIG1heD0xMDANCkNvbM5lY
3Rpb246IEt1ZXAtQWxpdmUNCkNvbRlbnQtVHlwZTogYXBwG1jYXRpb24veC1tc2Rvcylwcm9ncmFtDQoNC1g1T
yFQJUBBUFs0XFBaWDU0KFBBeKtdDQyk3fSRFSUNBUi1TVEFOREFSRC1BTlRJVklSVVMtVEVTVVC1GSUxFIGRIR0gqP
C9QQUNLRVQ+"

```

Proxy inspection mode

To verify application control and web filter logs in proxy mode:

1. Configure the firewall policies:

```
config firewall policy
edit 1
set name "WAN_out"
set srcintf "dmz"
set dstintf "wan1"
set action accept
set srcaddr "all"
set dstaddr "all"
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set ssl-ssh-profile "deep-inspection"
set av-profile "g-default"
set application-list "g-default"
set webfilter-profile "1"
set nat enable
set groups "RADIUS_User_Group" "Local_User"
next
edit 3
set name "WAN_in"
set srcintf "wan1"
set dstintf "dmz"
```

```
set action accept
set srcaddr "all"
set dstaddr "all"
set schedule "always"
set service "ALL"
set inspection-mode proxy
set logtraffic all
set nat enable
set groups "RADIUS_User_Group" "Local_User"
next
end
```

2. Verify the application control log:

```
date=2021-09-14 time=17:05:45 eventtime=1631664345570951500 tz="-0700"
logid="1059028704" type="utm" subtype="app-ctrl" eventtype="signature"
level="information" vd="vdom1" appid=38783 user="bob" group="RADIUS_User_Group"
authserver="Ubuntu_docker" dstuser="guest" srcip=10.1.100.72 dstip=172.16.200.75
srcport=60098 dstport=80 srcintf="dmz" srcintfrole="undefined" dstintf="wan1"
dstintfrole="undefined" proto=6 service="HTTP" direction="outgoing" policyid=1
sessionid=10871 applist="g-default" action="pass" appcat="General.Interest" app="Wget"
hostname="172.16.200.75" incidentserialno=17825796 url="/eicar.com"
msg="General.Interest: Wget," apprisk="low"
```

3. Verify the web filter log:

```
date=2021-09-14 time=17:14:46 eventtime=1631664886585770420 tz="-0700"
logid="0315012546" type="utm" subtype="webfilter" eventtype="urlfilter"
level="information" vd="vdom1" urlfilteridx=1 urlfilterlist="Auto-webfilter-urlfilter_
caex00jl5" policyid=1 sessionid=15251 user="bob" group="RADIUS_User_Group"
authserver="Ubuntu_docker" dstuser="guest" srcip=10.1.100.72 srcport=60106 srcintf="dmz"
srcintfrole="undefined" srcuuid="877d43a4-c2f9-51eb-f78f-e09794924d8a"
dstip=172.16.200.75 dstport=80 dstintf="wan1" dstintfrole="undefined" dstuuid="877d43a4-
c2f9-51eb-f78f-e09794924d8a" proto=6 service="HTTP" hostname="172.16.200.75" profile="1"
action="passthrough" reqtype="direct" url="http://172.16.200.75/eicar.com" sentbyte=149
rcvdbyte=0 direction="outgoing" msg="URL was allowed because it is in the URL filter
list"
```

Cloud

This section includes information about cloud related new features:

- [Public and private cloud on page 645](#)

Public and private cloud

This section includes information about public and private cloud related new features:

- [Collect only node IP addresses with Kubernetes SDN connectors on page 645](#)
- [Unicast HA on IBM VPC Cloud on page 649](#)
- [Update AliCloud SDN connector to support Kubernetes filters on page 656](#)
- [Synchronize wildcard FQDN resolved addresses to autoscale peers on page 659](#)
- [Obtain FortiCare-generated license and certificates for GCP PAYG instances on page 661](#)
- [FortiGate VM on KVM running ARM processors 7.0.1 on page 663](#)
- [Support MIME multipart bootstrapping on KVM with config drive 7.0.1 on page 667](#)
- [Support GCP gVNIC interface 7.0.1 on page 670](#)
- [FIPS cipher mode for OCI and GCP FortiGate VMs 7.0.1 on page 671](#)
- [SD-WAN transit routing with Google Network Connectivity Center 7.0.1 on page 672](#)
- [FGSP session sync on FortiGate-VMs on Azure with autoscaling enabled 7.0.1 on page 673](#)
- [Support C5d instance type for AWS Outposts 7.0.1 on page 672](#)
- [Flex-VM token and bootstrap configuration file fields in custom OVF template 7.0.2 on page 688](#)
- [Subscription-based VDOM license for FortiGate-VM S-series 7.0.2 on page 690](#)

Collect only node IP addresses with Kubernetes SDN connectors

By default, Kubernetes SDN connectors return both pod and node IP addresses. Peer Kubernetes SDN connectors can be configured to resolve dynamic firewall IP addresses to only node IP addresses. Results can also be filtered by specific IP addresses.

Example

In this example, a Kubernetes SDN connector and two dynamic firewall addresses are created. One of the addresses is configured to resolve only node IP addresses, while the other resolves both the pod and node IP addresses.

GUI configuration

To configure a Kubernetes SDN connector in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *Kubernetes*, then configure the connector settings:

Name	kuber_cloud
IP	35.236.76.254
Port	Specify - 443
Secret token	*****

3. Click **OK**.

To create the two dynamic firewall addresses in the GUI:

1. Go to **Policy & Objects > Addresses** and click **Create New > Address**.

Name	k8s_node_only
Type	Dynamic
Sub Type	Fabric Connector Address
SDN Connector	kuber_cloud
SDN address type	Private
Collect node addresses only	Enabled
Filter	K8S_NodeName=gke-zhmkc-hzhong-pool-3cb2c973-5mhw

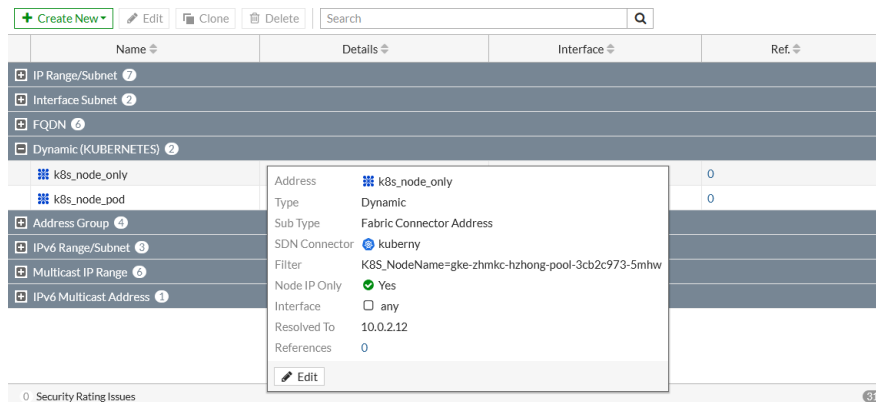
2. Click **OK**.

3. Click **Create New > Address** again to create the second address.

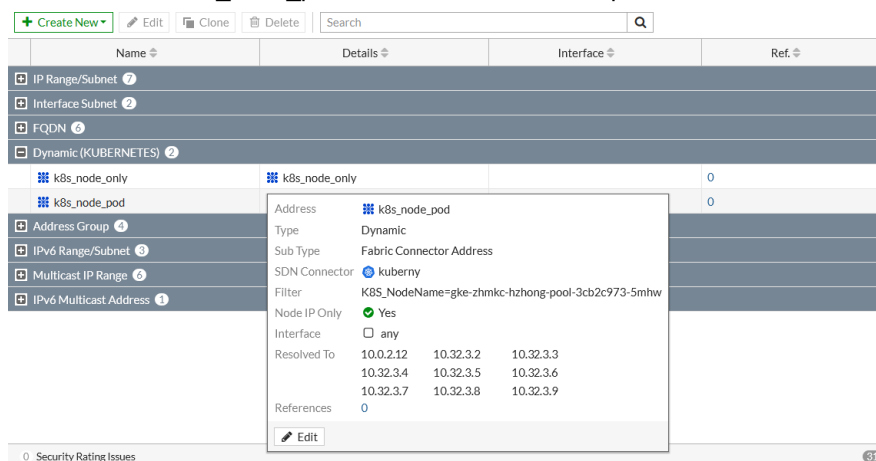
4. Configure the same settings as the first address, except set *Name* to *k8s_node_pod* and disable *Collect node addresses only*.
5. Click *OK*.

To check the resolved IP addresses of the two dynamic addresses in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. In the address list, hover the cursor over the *k8s_node_only* address. Only the node IP address is resolved.



3. Hover over the *k8s_node_pod* address. The node and pod IP addresses are all resolved.



The resolved IP addresses can be verified by accessing the Kubernetes cluster directly, see [Verify the resolved IP addresses on page 649](#).

CLI configuration

To configure a Kubernetes SDN connector in the CLI:

```
config system sdn-connector
  edit "kuber_cloud"
    set type kubernetees
    set server "35.236.76.254"
    set server-port 443
    set secret-token *****
  next
end
```

To create the two dynamic firewall addresses in the CLI:

```

config firewall address
    edit "k8s_node_only"
        set type dynamic
        set sdn "kuber_cloud"
        set color 19
        set filter "K8S_NodeName=gke-zhmkc-hzhong-pool-3cb2c973-5mhw"
        set node-ip-only enable
    next
    edit "k8s_node_pod"
        set type dynamic
        set sdn "kuber_cloud"
        set color 19
        set filter "K8S_NodeName=gke-zhmkc-hzhong-pool-3cb2c973-5mhw"
        set node-ip-only disable
    next
end

```

To check the resolved IP addresses of the two dynamic addresses in the CLI:

```

#show firewall address
config firewall address
    ...
    edit "k8s_node_only"
        ...
        config list
            edit "10.0.2.12"
            next
        end
    next
    edit "k8s_node_pod"
        ...
        config list
            edit "10.0.2.12"
            next
            edit "10.32.3.2"
            next
            edit "10.32.3.3"
            next
            edit "10.32.3.4"
            next
            edit "10.32.3.5"
            next
            edit "10.32.3.6"
            next
            edit "10.32.3.7"
            next
            edit "10.32.3.8"
            next
            edit "10.32.3.9"
            next
        end
    next
end

```

The resolved IP addresses can be verified by accessing the Kubernetes cluster directly.

Verify the resolved IP addresses

To confirm the node IP address:

```
fosqa@pc56:~$ kubectl get nodes gke-zhmkc-hzhong-pool-3cb2c973-5mhw -o wide
```

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP
EXTERNAL-IP	OS-IMAGE		KERNEL-VERSION	CONTAINER-RUNTIME	
gke-zhmkc-hzhong-pool-3cb2c973-5mhw	Ready	<none>	532d	v1.12.7-gke.10	10.0.2.12
35.236.118.65	Container-Optimized OS from Google		4.14.106+	docker://17.3.2	

To confirm the node and pods IP addresses:

```
fosqa@pc56:~$ kubectl get pods --all-namespaces -o wide | grep gke-zhmkc-hzhong-pool-3cb2c973-5mhw
```

default	guestbook-qcg7j	1/1	Running	0
186d	10.32.3.9	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
default	redis-master-mstb4	1/1	Running	0
186d	10.32.3.8	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
default	redis-slave-7tgcx	1/1	Running	0
186d	10.32.3.5	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	fluentd-gcp-scaler-6965bb45c9-2lpp2	1/1	Running	0
239d	10.32.3.4	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	fluentd-gcp-v3.2.0-nlnlp	2/2	Running	0
239d	10.0.2.12	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	heapster-gke-7858846d4d-vqc4d	3/3	Running	0
186d	10.32.3.6	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	kube-dns-5995c95f64-rqn4b	4/4	Running	0
186d	10.32.3.7	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	kube-dns-autoscaler-8687c64fc-dq9fn	1/1	Running	0
239d	10.32.3.2	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	kube-proxy-gke-zhmkc-hzhong-pool-3cb2c973-5mhw	1/1	Running	0
532d	10.0.2.12	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	metrics-server-v0.3.1-5c6fbf777-7bchg	2/2	Running	0
239d	10.32.3.3	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>
kube-system	prometheus-to-sd-xndgs	2/2	Running	0
186d	10.0.2.12	gke-zhmkc-hzhong-pool-3cb2c973-5mhw	<none>	<none>

Unicast HA on IBM VPC Cloud

IBM VPC Cloud users can deploy their BYOL FortiGate VMs in unicast HA. The HA failover will automatically trigger routing changes and floating IP reassignment on the IBM Cloud via the API.

Example

In this example, an administrator has an Ubuntu client protected by an IBM FortiGate in HA A-P mode. The administrator uses a VIP to access Ubuntu, the web, and has traffic inspected for EICAR.

When the primary device is shut down to simulate a failover event, the floating IP (FIP) and route fail over. After the failover, the administrator can still use the VIP to access Ubuntu and the web, and have traffic inspected for EICAR, through the secondary FortiGate.

In this example you will configure the IBM VPC device and the primary and secondary FortiGates.

To configure the IBM VPC:

1. Configure the subnets and attach the public gateway (see [Using the IBM Cloud console to create VPC resources](#)).

a. Configure four subnets:

- Public
- Internal
- Management
- Heartbeat

b. Make sure a public gateway is attached to the public subnet.

Subnets in this VPC

Status	Name	Location	IP range	Public gateway
Available	public	Washington DC 3	10.241.128.0/24	
Available	management	Washington DC 3	10.241.130.0/24	
Available	internal	Washington DC 3	10.241.129.0/24	—
Available	heartbeat	Washington DC 3	10.241.131.0/24	—

Routing table details

Name: default-route-table

Created: November 20, 2020 3:10:05 PM

Virtual private cloud: havpc

ID:

Attached subnets: 1

Traffic type: Egress

Routes: 1

Routes

State	Destination	Action	Type	Next hop	Location
Stable	0.0.0.0/0	Deliver	IP address	10.241.129.4	Washington DC 3

2. Configure the two route tables (see [Creating a routing table](#)).

a. Configure the internal route table as follows:

- It needs to be the IBM default route table for the VPC.
- It has a route for all traffic to the internal subnet IP of the primary FortiGate.
- It applies to the internal subnet.

b. Configure the open (non-default) route table as follows:

- This route table can have no routes.
- It applies to the public, management, and heartbeat subnets.



Non-default route tables cannot be used for the internal subnet's route table failover in IBM VPCs at this time.

Routing tables for VPC

VPC: havpc

Name	Default	Traffic type	Routes	Attached subnets
default-route-table		Egress	1	1
non-default		Egress	0	3

Items per page: 10 1-2 items

Page 1

3. Configure the floating IP (see [Managing network interfaces](#)).



IBM Cloud does not currently support multiple FIPs for a single instance. Even though the management ports can be configured, you will not be able to access them using a FIP in the final configuration.

If you want to access the instances for configuration purposes, you can attach a FIP to the public subnet's IP on the primary and secondary devices until the FortiOS configuration is finished. Also, you can connect directly to the local IPs through a VPN or another proxy instance.

In this example, the final configuration only needs one FIP attached to the primary public subnet IP.

Network interfaces ⓘ

[New interface ⓘ](#)

Interface	Subnet name	Private IP	Floating IP	Security groups	Allow IP Spoofing	
eth0	public	10.241.128.4		turkey-unaware-harmonize-versus	Enabled	
eth1	internal	10.241.129.4	—	turkey-unaware-harmonize-versus	Enabled	
eth2	heartbeat	10.241.131.4	—	turkey-unaware-harmonize-versus	Enabled	
eth3	management	10.241.130.4	—	turkey-unaware-harmonize-versus	Enabled	

To configure the primary FortiGate:

1. Configure the static IP addresses:

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.241.128.4 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 10.241.129.4 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set ip 10.241.131.4 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set ip 10.241.130.4 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 4
```

```

    next
end

```

2. Configure the HA settings:

```

config system ha
    set group-name "Test"
    set mode a-p
    set password *****
    set hbdev "port3" 100
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.241.130.1
        next
    end
    set override enable
    set priority 255
    set unicast-hb enable
    set unicast-hb-peerip 10.241.131.5
end

```

3. Verify that the primary and secondary FortiGates see each other and are synchronized:

```

# get system ha status
HA Health Status: OK
Model: FortiGate-VM64-IBM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 1 days 3:15:48
Cluster state change time: 2020-11-24 15:35:01
Primary selected using:
    <2020/11/24 15:35:01> FGVM08TM20000007 is selected as the primary because it has the
largest value of override priority.
ses_pickup: disable
override: enable
unicast_hb: peerip=10.241.131.5, myip=10.241.131.4, hasync_port='port3'
Configuration Status:
    FGVM08TM20000007(updated 1 seconds ago): in-sync
    FGVM08TM20000006(updated 2 seconds ago): in-sync
System Usage stats:
    FGVM08TM20000007(updated 1 seconds ago):
        sessions=4, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=4%
    FGVM08TM20000006(updated 2 seconds ago):
        sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=4%
HBDEV stats:
    FGVM08TM20000007(updated 1 seconds ago):
        port3: physical/10000full, up, rx-
bytes/packets/dropped/errors=15646281/45910/0/0, tx=21807567/45445/0/0
    FGVM08TM20000006(updated 2 seconds ago):
        port3: physical/10000full, up, rx-
bytes/packets/dropped/errors=25485511/54398/0/0, tx=22502231/143827/0/0
Primary      : FGVM08TM20000007, FGVM08TM20000007, HA cluster index = 0
Secondary    : FGVM08TM20000006, FGVM08TM20000006, HA cluster index = 1
number of vcluster: 1

```

```
vcluster 1: work 10.241.131.4
Primary: FGVM08TM20000007, HA operating index = 0
Secondary: FGVM08TM20000006, HA operating index = 1
```

4. Configure the static route. The gateway is the public subnet's first address:

```
config router static
  edit 1
    set gateway 10.241.128.1
    set device "port1"
  next
end
```

5. Configure the VDOM exception:

```
config system vdom-exception
  edit 1
    set object firewall.vip
  next
end
```

6. Configure the VIP:

```
config firewall vip
  edit "to internal ubuntu"
    set extip 10.241.128.4
    set mappedip "10.241.129.6"
    set extintf "port1"
    set portforward enable
    set extport 8822
    set mappedport 22
  next
end
```

7. Configure the firewall policies for the Ubuntu client and internal subnet:

```
config firewall policy
  edit 1
    set name "toVIP"
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "to internal ubuntu"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set nat enable
  next
  edit 2
    set name "main"
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
```

```
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set logtraffic all
        set nat enable
    next
end
```

8. Configure the SDN connector:

```
config system sdn-connector
    edit "1"
        set type ibm
        set ha-status enable
        set api-key *****
        set ibm-region us-east
    next
end
```

To configure the secondary FortiGate:

1. Configure the static IP addresses:

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.241.128.5 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 10.241.129.5 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set ip 10.241.131.5 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set ip 10.241.130.5 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set snmp-index 4
    next
end
```

2. Configure the HA settings:

```
config system ha
    set group-name "Test"
    set mode a-p
    set password *****
    set hbdev "port3" 100
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.241.130.1
        next
    end
    set override enable
    set priority 0
    set unicast-hb enable
    set unicast-hb-peerip 10.241.131.4
end
```

3. Configure the VIP:

```
config firewall vip
    edit "to internal ubuntu"
        set extip 10.241.128.5
        set mappedip "10.241.129.6"
        set extintf "port1"
        set portforward enable
        set extport 8822
        set mappedport 22
    next
end
```

To test the configuration:

1. Access the Ubuntu client via the public FIP and custom port 8822, then use cURL to get the EICAR file from HTTP. The FortiGate should block the file:

```
root@mail:/home/kvm/scripts# ssh ubuntu@xx.xxx.xxx.xxx -p 8822
ubuntu@xx.xxx.xxx.xxx's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1026-kvm x86_64)
... omitted ...
ubuntu@xxxxxxx-ha-ubuntu:~$ curl http://www.eicar.org/download/eicar.com
<!DOCTYPE html>
... omitted ...
<p>You are not permitted to download the file "eicar.com" because it is infected
with the virus "EICAR_TEST_FILE".</p>
```

2. Trigger the failover by shutting down the primary FortiGate. Verify that the FIP and route tables have moved, then try to access the Ubuntu client and get the EICAR file again:

```
root@mail:/home/kvm/scripts# ssh ubuntu@xx.xxx.xxx.xxx -p 8822
ubuntu@xx.xxx.xxx.xxx's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1026-kvm x86_64)
... omitted ...
ubuntu@xxxxxxx-ha-ubuntu:~$ curl http://www.eicar.org/download/eicar.com
<!DOCTYPE html>
... omitted ...
```

<p>You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".</p>

3. If the failover is unsuccessful, you can debug the secondary FortiGate in the IBM VPC. Note that even though there are some reported fails, the failover is successful:

```
HA event
HA state: primary
ibmd sdn connector is getting token
token size: 1163
token expiration: 1606264324
parsing instance 0777_e8e111aa-1aa1-11aa-a111-1111a1aa1a1a
ibmd HA successfully got fip for hb peer
parsing instance 0777_2b22bbbb-bb22-2b22-bb22-b222bbb22b2b
ibmd HA found hb host/peer info
in collect rtbl
ibmd HA found rtbl on hb peer ip
ibmd http request response: 204

ibmd HA deleted rtbl r014-167a1aaa-12ab-1111-bb2a-2ababbb22222
ibmd HA deleted rtbl r014-167a1aaa-12ab-1111-bb2a-2ababbb22222
ibmd http request response: 201
{"id":"r014-b8771aa1-1111-22aa-22bb-1aa22bb222ab","href":"https://us-
east.iaas.cloud.ibm.com/v1/vpcs/r014-ab1b121a-21ba-21ab-11ab-aabalabaabba/routes/r014-
b8771aa1-1111-22aa-22bb-1aa22bb222ab","name":"glancing-handprint-shakable-
gotten","action":"deliver","destination":"0.0.0.0/0","next_hop":
{"address":"10.241.129.5"},"lifecycle_state":"stable","created_at":"2020-11-
24T23:32:12Z","zone":{"name":"us-east-3","href":"https://us-
east.iaas.cloud.ibm.com/v1/regions/us-east/zones/us-east-3"}}

ibmd HA created rtbl
ibmd HA created rtbl
HA state: primary
ibmd sdn connector is getting token
token size: 1163
token expiration: 1606264337
parsing instance 0777_e8e111aa-1aa1-11aa-a111-1111a1aa1a1a
ibmd HA failed to parse fip list
ibmd HA failed to get fip for hb peer
parsing instance 0777_2b22bbbb-bb22-2b22-bb22-b222bbb22b2b
ibmd HA found hb host/peer info
in collect rtbl
ibmd HA failed to find hb fip
ibmd HA failed to move fip
```

Update AliCloud SDN connector to support Kubernetes filters

When an AliCloud SDN connector is configured, dynamic address objects can support Kubernetes filters based on cluster, service, node, pod, and more.

The following address filters can be applied:

- K8S_Cluster
- K8S_Namespace
- K8S_ServiceName
- K8S_NodeName

- K8S_PodName
- K8S_Region
- K8S_Zone
- K8S_Label

To configure an AliCloud SDN connector with a Kubernetes filter in the GUI:

1. Configure the AliCloud SDN connector:
 - a. Go to *Security Fabric > External Connectors*.
 - b. Click *Create New*, and select *AliCloud*.
 - c. Configure the settings as needed and click *OK*.

The screenshot shows the 'New External Connector' dialog box. The 'Public SDN' tab is active, displaying the AliCloud logo. Under 'Connector Settings', the Name is 'ali1', Status is 'Enabled', and Update Interval is 'Use Default'. The AliCloud Connector section shows AccessKey ID, AccessKey Secret, and Region ID (us-west-1). The right pane, 'Additional Information', contains links for API Preview, Public SDN Connector Setup Guides (Amazon Web Services, Google Cloud Platform, Microsoft Azure, Oracle Cloud Infrastructure), Private SDN Connector Setup Guides (Cisco Application Centric Infrastructure, Nuage Virtualized Services Platform, OpenStack Connector, VMware NSX), and Documentation (Online Help, Video Tutorials). At the bottom are 'OK' and 'Cancel' buttons.

2. Create a dynamic firewall address with the supported Kubernetes filter:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New > Address* and enter a name.
 - c. Configure the following settings:
 - i. For *Type*, select *Dynamic*.
 - ii. For *Sub Type*, select *Fabric Connector Address*.
 - iii. For *SDN Connector*, select the connector created in step 1.
 - iv. For *SDN address type*, select *Private*.
 - v. For *Filter*, select *K8S_Cluster=zhmcluster*.
 - d. Click *OK*.

The corresponding IP addresses are dynamically updated and resolved after applying the Kubernetes filter.

3. Confirm that the AliCloud SDN connector resolves dynamic firewall IP addresses using the configured filter:

- Go to **Policy & Objects > Addresses**.
- In the address table, hover over the address created in step 2 to view which IPs it resolves to:

+ Create New

IP Range/Sub

FABRIC_

FIREWALL

SSLVPN

all

none

FortiClient E

FCTEMS

2

ali_add1

aws_add1

FQDN 6

gmail.com

login.mic

login.mic

0 Security Ratin

Address

ali_add1

Type

Dynamic

Sub Type

Fabric Connector Address

SDN Connector

ali1

Filter

K8S_Cluster=zhmcluster1

Interface

any

Resolved To

10.0.0.28 10.0.0.29 10.0.0.30

10.0.1.129 10.0.104.237 10.0.104.238

10.0.2.65 10.0.50.166 172.16.0.20

172.16.1.10 172.16.1.30 172.16.1.50

172.16.2.30 172.16.3.30 172.16.4.30

172.16.5.30 172.16.6.30 172.16.7.30

172.16.8.30 172.20.0.130 172.20.0.131

172.20.0.132 172.20.0.133 172.20.0.2

172.20.0.3 172.20.0.4 172.20.0.5

172.20.0.66 172.20.0.67 172.20.0.68

172.20.0.69 172.20.0.70 172.20.0.71

172.20.0.72 172.20.0.73 172.20.0.74

172.20.0.75 172.21.0.1 172.21.0.10

172.21.1.159 172.21.11.21 172.21.12.245

172.21.12.35 172.21.13.2 172.21.14.62

172.21.2.138 172.21.2.254 172.21.3.135

172.21.9.67 192.168.0.202 192.168.0.203

192.168.0.204 192.168.0.94 192.168.0.95

Q

Interface	Type	Ref.
	Address	0
	Address	0
10	SSL-VPN tunnel interface (ssl.root)	2
	Address	2
	Address	0
	Address	0
	Address	0
	Address	0
	Address	0
	Address	1
	Address	1
	Address	1

0% 16 Updated: 11:58:46

To configure an AliCloud SDN connector with a Kubernetes filter in the CLI:

1. Configure the AliCloud SDN connector:

```
config system sdn-connector
  edit "ali1"
    set type alicloud
    set access-key "*****"
    set secret-key xxxxxxxx
    set region "us-west-1"
  next
end
```

2. Create a dynamic firewall address with the supported Kubernetes filter:

```
config firewall address
  edit "ali_add1"
    set type dynamic
    set sdn "ali1"
    set color 10
    set filter "K8S_Cluster=zhmcluster1"
  next
end
```

3. Confirm that the AliCloud SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
  edit "ali_add1"
    show
  config firewall address
    edit "ali_add1"
      set uuid c48e4f00-5435-51eb-0547-aced5cf80f1f
      set type dynamic
      set sdn "ali1"
```



```

        set color 10
        set filter "K8S_Cluster=zhmcluster1"
        config list
            edit "10.0.0.28"
            next
            edit "10.0.0.29"
            next
            edit "10.0.0.30"
            next
            ...
        end
    next
end
next
end

```

Synchronize wildcard FQDN resolved addresses to autoscale peers

This enhancement synchronizes wildcard FQDN IPs to other autoscale members whenever a peer learns of a wildcard FQDN address.

The following example uses an AWS deployment.

To synchronize wildcard FQDN resolved addresses to autoscale peers:

1. Configure an FG-AWS autoscale group with one primary and two secondary FortiGates (see [Deploying autoscaling on AWS](#) in the AWS Administration Guide).
2. On the primary FortiGate, configure a wildcard FQDN firewall address for *.cnn.com (see [Using wildcard FQDN addresses in firewall policies](#) in the FortiOS Administration Guide). The configuration will be synchronized between all autoscale peers.

To verify the wildcard FQDN resolved address synchronization:

1. On the primary FortiGate, ping `www.cnn.com`:

```

# execute ping www.cnn.com
PING turner-tls.map.fastly.net (***.232.65.67): 56 data bytes
64 bytes from ***.232.65.67: icmp_seq=0 ttl=52 time=0.4 ms
64 bytes from ***.232.65.67: icmp_seq=1 ttl=52 time=0.4 ms

```

2. View the list of resolved IP addresses of wildcard FQDN objects:

```

# diagnose firewall fqdn list
List all FQDN:
*.cnn.com: ID(4) ADDR(***.232.65.67)

```

3. On the secondary-1 FortiGate, view the list of resolved IP addresses of wildcard FQDN objects:

```

# diagnose firewall fqdn list
List all FQDN:
*.cnn.com: ID(4) ADDR(***.232.65.67)

```

4. On the secondary-2 FortiGate, view the list of resolved IP addresses of wildcard FQDN objects:

```
# diagnose firewall fqdn list
List all FQDN:
*.cnn.com: ID(4) ADDR(***.232.65.67)
```

5. On each FortiGate, go to **Policy & Object > Addresses** and hover over the FQDN address to view the resolved IP.

a. Primary:

Name		Details
IP Range/Subnet 6		
FABRIC_D	Address	demo-fqdn-1 0.0.0/0
FIREWALL	Type	FQDN 0.0.0/0
SSLVPN_TU	FQDN	*.cnn.com 212.134.200 - 10.212.134.210
all	Interface	any 0.0.0/0
metadata-s	Collected Resolved IPs	.101.201.67 254.169.254/32
none	References	0 0.0.0/32
FQDN 6		
demo-fqdn-1		*.cnn.com
gmail.com		gmail.com
internal-elb-web		service-elb- elb.us-east-1.amazonaws.com
test-eforceft.com		test-eforceft.com
0 Security Rating Issues 0% 16 Updated: 11:18:54		

b. Secondary-1:

Name		Details	Interface	Type
IP Range/Subnet 6				
FABRIC_D	Address	demo-fqdn-1		Address
FIREWALL	Type	FQDN		Address
SSLVPN_TU	FQDN	*.cnn.com 4.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Address
all	Interface	any		Address
metadata-s	Collected Resolved IPs	.101.201.67 9.254/32		Address
none	References	0		Address
FQDN 6				
demo-fqdn-1		*.cnn.com		Address
gmail.com		gmail.com		Address
internal-elb-web		service-elb- ...	port1	Address
test-eforceft.com		test-eforceft.com		Address
0 Security Rating Issues 0% 16 Updated: 11:26:00				

c. Secondary-2:

<div> <div>Create New</div> <div>Edit</div> <div>Clone</div> <div>Delete</div> <div>Search</div> <div>Q</div> </div>			
Name	Details	Interface	Type
IP Range/Subnet 6			
FABRIC	Address	demo-fqdn-1	Address
FIREWALL	Type	FQDN	Address
SSLVPN	FQDN	*.cnn.com	Address
all	Interface	any	Address
metadata	Collected Resolved IPs	.101.201.67	Address
none	References	0	Address
FQDN 8			
demo-fqdn-1	*.cnn.com		Address
gmail.com	gmail.com		Address
internal-elb-web	internal-elb-...	port1	Address
test-internal-elb-web	test-internal-elb-web		Address
<div>0 Security Rating Issues</div> <div>0% 16 Updated: 11:26:38</div>			

Obtain FortiCare-generated license and certificates for GCP PAYG instances

GCP PAYG instances can obtain FortiCare-generated licenses upon a new deployment, or in the CLI (`execute vm-license`) when upgrading from previous firmware. The process generates Fortinet_Factory and Fortinet_Factory_Backup certificates that contain the common name (CN) of the FortiGate serial number to uniquely identify this FortiGate.

Installing a new deployment

A newly deployed instance will automatically retrieve the signed certificate from FortiCare. Appropriately 30 seconds after booting the instance, it will get the certificate and reboot once to install the new certificate.

To verify the installation in a new deployment:

1. Enable debugging and check the update status:

```
# diagnose debug enable
# diagnose debug update -1
Debug messages will be on for 30 minutes.
VM license install succeeded. Rebooting firewall.
```

2. After the reboot, verify the license information:

```
# diagnose debug vm-print-license
SerialNumber: FGVM04TM*****
CreateDate: Tue Jun 8 02:30:19 2021
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: PG (22)
CPU: 2147483647
MEM: 2147483647
```

3. Verify the Fortinet_Factory certificate information (the CN is the serial number):

```
config vpn certificate local
# get Fortinet_Factory
name          : Fortinet_Factory
password      : *
private-key   : *
certificate    :
    Subject:    C = US, ST = California, L = Sunnyvale, O = Fortinet, OU =
FortiGate, CN = FGVM04TM*****, emailAddress = support@fortinet.com
    Issuer:     C = US, ST = California, L = Sunnyvale, O = Fortinet, OU =
Certificate Authority, CN = fortinet-subca2001, emailAddress = support@fortinet.com
    Valid from: 2021-06-08 02:30:19 GMT
    Valid to:   2056-01-19 03:14:07 GMT
    ...
```

Upgrading the firmware

To obtain a FortiCare-generated license during an upgrade:

1. Before upgrading, verify the Fortinet_Factory certificate information (the CN is FortiGate):

```
config vpn certificate local
# get Fortinet_Factory
name          : Fortinet_Factory
password      : *
private-key   : *
certificate    :
    Subject:    C = US, ST = California, L = Sunnyvale, O = Fortinet, OU =
FortiGate, CN = FortiGate, emailAddress = support@fortinet.com
    Issuer:     C = US, ST = California, L = Sunnyvale, O = Fortinet, OU =
Certificate Authority, CN = fortinet-subca2001, emailAddress = support@fortinet.com
    Valid from: 2016-11-30 19:58:17 GMT
    Valid to:   2056-11-20 19:58:07 GMT
    ...
```

2. Verify the license information:

```
# diagnose debug vm-print-license
SerialNumber: FGTMCGPH*****
CreateDate: 1623112103
Model: PG (22)
CPU: 2147483647
MEM: 2147483647
```

Since there is no unique certificate from FortiCare, there are no Key, Cert, Key2, or Cert2 fields.

3. Upgrade the firmware and update the license:

```
# execute vm-license
This operation will reboot the system !
Do you want to continue? (y/n)y

Get instance JWT token
Requesting FortiCare license: FGTMCGPH*****
VM license install succeeded. Rebooting firewall.
```

4. Verify the new Fortinet_Factory certificate information (the CN is the serial number):

```
config vpn certificate local
# get Fortinet_Factory
name          : Fortinet_Factory
password      : *
private-key   : *
certificate    :
    Subject:    C = US, ST = California, L = Sunnyvale, O = Fortinet, OU =
FortiGate, CN = FGTMCGPH*****, emailAddress = support@fortinet.com
    Issuer:     C = US, ST = California, L = Sunnyvale, O = Fortinet, OU =
Certificate Authority, CN = fortinet-subca2001, emailAddress = support@fortinet.com
    Valid from: 2021-06-08 02:30:19 GMT
    Valid to:   2056-01-19 03:14:07 GMT
    ...
```

5. Verify the license information (Key, Cert, Key2, or Cert2 fields are now available):

```
# diagnose debug vm-print-license
SerialNumber: FGTMCGPH*****
CreateDate: Tue Jun 8 02:30:19 2021
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: PG (22)
CPU: 2147483647
MEM: 2147483647
```

FortiGate VM on KVM running ARM processors - 7.0.1

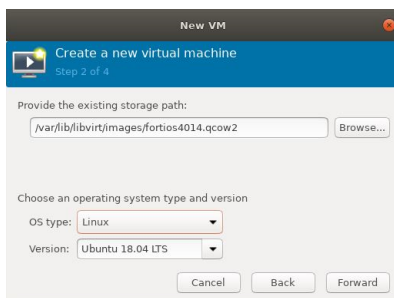
FortiGate VMs can be deployed on KVM hypervisors running ARM64 processors.

To deploy the FortiGate VM:

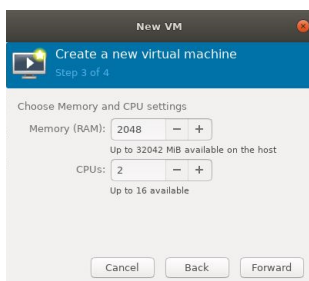
1. Upload the qcow2 file to the hypervisor host.
2. Open the *Virtual Machine Manager* and create a new virtual machine.
3. Select *Import existing disk image*.
4. Set the following in the *Architecture options*:
 - *Virt Type: KVM*
 - *Architecture: aarch64*
 - *Machine Type: virt*



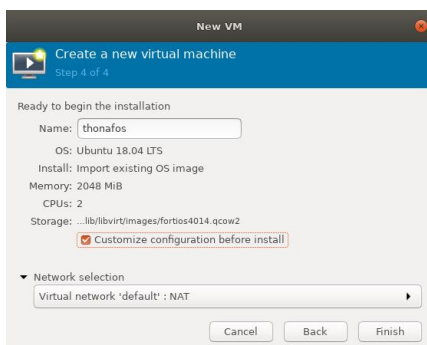
5. Click *Forward*.
6. Enter the storage path, pointing to the uploaded qcow2 file.
7. Set the OS type to *Linux* and Version to *Ubuntu 18.04 LTS*.



8. Click *Forward*.
9. Set the amount of memory and number of CPUs.

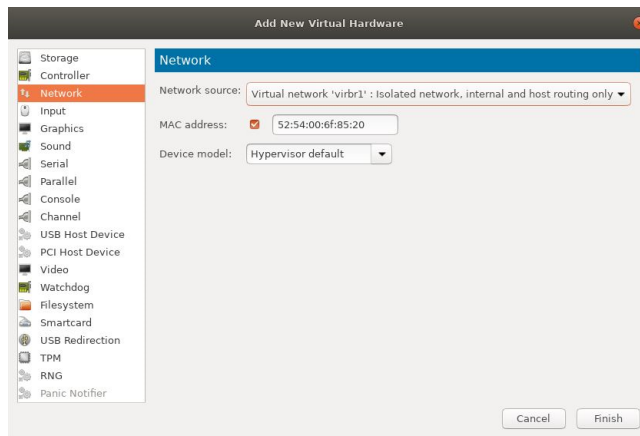


10. Click *Forward*.
11. Enter a name for the VM, select *Customize configuration before install*, and select a network.

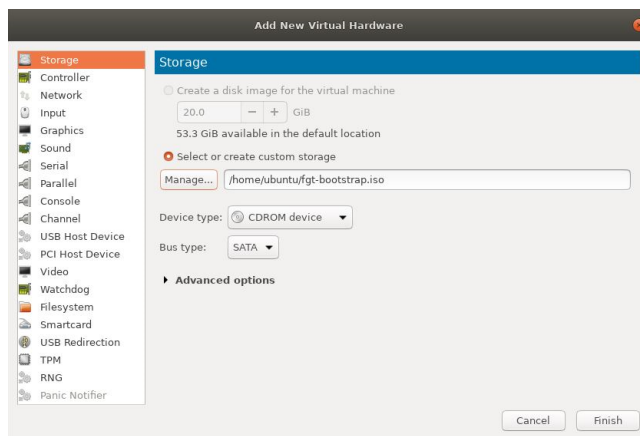


12. Click *Finish*.

13. Click *Add Hardware* and add another NIC to connect to an internal, private network.



14. Click *Add Hardware* again and add bootstrap CDROM device with a VM license.



15. Click *Begin Installation* to install the VM.
16. Confirm that CPU and memory allocation, and the platform:

```
# get system status
Version: FortiGate-ARM64-KVM v7.0.0,buid2292,201201 (interim)
...
License Status: Valid
License Expiration Date: 2021-11-07
VM Resources: 2 CPU/32 allowed, 1997 MB RAM
Log hard disk: Available
Hostname: cloud-init-test
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 2292
Release Version Information: interim
System time: Fri Dec 4 09:59:38 2020
```

17. Confirm that the FortiCloud debug shows the correct platform flag:

```
# diagnose test application forticldd 1
System=FGT Platform=ARM64-KVM
Management vdom: root, id=0, ha=primary.
acct_id=
acct_st=Logged Out

FortiGuard interface selection: method=auto specify=FortiGuard log: status=disabled,
full=overwrite, ssl_opt=1, source-ip=0.0.0.0

Centra Management: type=NONE, flags=000000bf.

active-tasks=0

rpdb_ver=00000001 rpdb6_ver=00000001
```

To configure the VM:

1. Configure the port1 and port2 interfaces:

```
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh fgfm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 10.1.100.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm radius-acct fabric ftm
        set type physical
        set snmp-index 2
    next
end
```

Port1 uses DHCP, as it is connected to the internet and has a DHCP gateway. Port2 is configured with a static IP.

2. Configure a basic firewall policy with an antivirus profile and certification:

```
config firewall policy
    edit 1
        set name "main"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set logtraffic all
        set nat enable
    next
end
```


To test the FortiGate antivirus:

1. Set the default route gateway on the client to the internal interface of the FortiGate:

```
qa@ubuntu-arm64:~$ sudo ip link set dev enp2s0 up

qa@ubuntu-arm64:~$ sudo ifconfig enp2s0 10.1.100.5 netmask 255.255.255.0
qa@ubuntu-arm64:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.100.5 netmask 255.255.255.0 broadcast 10.1.100.255
    inet6 fe80::5054:ff:febb:153b prefixlen 64 scopeid 0x20<link>
    ether 52:54:00:bb:15:3b txqueuelen 1000 (Ethernet)
    RX packets 1008 bytes 54119 (54.1 KB)
    RX errors 0 dropped 982 overruns 0 frame 0
    TX packets 32 bytes 4351 (4.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3471721 bytes 246592197 (246.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3471721 bytes 246592197 (246.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

qa@ubuntu-arm64:~$ sudo ip route add default via 10.1.100.1
qa@ubuntu-arm64:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=97 time=9.02 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.022/9.022/9.022/0.000 ms
```

2. Attempt to download the EICAR test file to confirm that it is blocked:

```
qa@ubuntu-arm64:~$ curl http://www.eicar.org/download/eicar.com
<!DOCTYPE html>
... omitted ...
<p>You are not permitted to download the file "eicar.com" because it is infected
with the virus "EICAR_TEST_FILE".</p>
```

Support MIME multipart bootstrapping on KVM with config drive - 7.0.1

On KVMs, FortiOS supports bootstrapping using a MIME file with config drive.

Sample MIME file

```
Content-Type: multipart/mixed; boundary="=====0740947994048919689=="
MIME-Version: 1.0

=====0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
```

```

Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"

config sys glo
set hostname mimecheck
set admintimeout 480
end
config sys admin
edit admin
set password 12345678
end

=====0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"

-----BEGIN FGT VM LICENSE-----
*****/*****
...
-----END FGT VM LICENSE-----

=====0740947994048919689===

```

To bootstrap a KVM using a MIME file with config drive:

1. Create a config drive ISO with a MIME file. See for [Cloud-init using config drive](#) for more information.

```

cd /home/kvm/bootstrap
cp mimefile.txt /home/kvm/bootstrap/kvm-cloudinit/openstack/latest/user_data
#optional, since license file is also in the mime file
cp /home/kvm/bootstrap/licenses/UL_license.txt
/home/kvm/bootstrap/kvm-cloudinit/openstack/content/0000
mkisofs -R -r -o fgt-bootstrap.iso kvm-cloudinit

```

2. Attach the ISO config drive at boot time. See [Cloud-init](#) for more information.

```

virt-install --connect qemu:///system \
    --name ${DOMAIN} \
    --virt-type kvm \
    --arch=${ARCH} \
    --hvm \
    --os-type=linux \
    --os-variant=generic \
    --graphics vnc,listen=0.0.0.0 --noautoconsole \
    --vcpus=${CPU} \
    --ram ${RAM} \
    --cpu host-passthrough \
    --sysinfo host \
    --disk ${DOMAIN}.qcow2,device=disk,bus=${DISKMODE},format=qcow2,cache=none \
    --disk ${DOMAIN}-log.qcow2,device=disk,bus=${DISKMODE},format=qcow2,cache=none \
    --disk ${DOMAIN}-
wanopt.qcow2,device=disk,bus=${DISKMODE},format=qcow2,cache=none \
    --disk ${DOMAIN}-
bootstrap.iso,device=cdrom,bus=${DISKMODE},format=raw,cache=none \
    --network bridge=br0,model=${NICMODE},mac=**:**:**:**:**:11 \

```

```
--network bridge=br1,model=${NICMODE},mac=**:**:**:**:22 \
--network bridge=br2,model=${NICMODE},mac=**:**:**:**:33 \
--import
```

3. Boot up the VM and verify the FortiGate bootstrap:

```
# diagnose debug cloudinit show
>> Checking metadata source config drive
>> Found config drive /dev/vdd
>> Successfully mount config drive
>> MIME parsed config script
>> MIME parsed VM license
>> Found metadata source: config drive
>> Trying to install vmlicense ...
>> Checking metadata source config drive
>> Found config drive /dev/vdd
>> Successfully mount config drive
>> MIME parsed config script
>> MIME parsed VM license
>> Found metadata source: config drive
>> Config drive parse metadata json failed
>> Run config script
>> Finish running script
>> FGVM01TM21000000 $ config sys glo
>> FGVM01TM21000000 (global) $ set hostname mimecheck
>> FGVM01TM21000000 (global) $ set admintimeout 480
>> FGVM01TM21000000 (global) $ end
>> mimecheck $ config sys admin
>> mimecheck (admin) $ edit admin
>> mimecheck (admin) $ set password *****
>> mimecheck (admin) $ end
>> mimecheck $ config sys glo
>> mimecheck (global) $ set hostname mimecheck
>> mimecheck (global) $ set admintimeout 480
>> mimecheck (global) $ end
>> mimecheck $ config sys admin
>> mimecheck (admin) $ edit admin
>> mimecheck (admin) $ set password *****
>> mimecheck (admin) $ end
```

4. Verify that the VM license is valid:

```
# get system status
Version: FortiGate-VM64-KVM v7.0.1,build0125,210517 (interim)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Serial-Number: FGVM01TM21000000
License Status: Valid
License Expiration Date: 2022-05-06
VM Resources: 1 CPU/1 allowed, 3962 MB RAM
```

```

Log hard disk: Available
Hostname: mimecheck
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0125
Release Version Information: interim
FortiOS x86-64: Yes
System time: Wed May 19 21:48:12 2021
Last reboot reason: warm reboot

```

Support GCP gVNIC interface - 7.0.1

The new GCP gVNIC interface is supported, which offers improved performance and bandwidth and is required on some VM shapes tuned for optimal performance.



A VM with gVNIC must be deployed with the CLI or API. Refer to the [Using Google Virtual NIC](#) documentation for other limitations. If you are upgrading from prior images that support virtIO, the images will remain that way.

Refer to [Creating a VM that uses gVNIC](#) for detailed instructions. The following example shows sample commands used to create an instance.

To deploy a gVNIC with the gcloud CLI:

1. Create a gVNIC enabled image using the FortiGate marketplace image.

```

gcloud compute --project=dev-project-000-000000 images create gcp-ond-700-gvnic --
source-image=fortinet-fgtdemand-700-20210407-000-w-license --source-image-
project=fortigcp-project-000 --guest-os-features=GVNIC

```

2. Deploy the instance with the gVNIC image and gVNIC specification in the parameter:

```

gcloud compute --project=dev-project-000-000000 instances create xxxxxx-script-ond-0128-
gvnic --zone=us-centrall1-c --machine-type=n1-standard-1 --network-interface nic-
type=GVNIC,subnet=xxxxxx-hapvc-port1external,private-network-
ip=10.0.0.15,address=**.**.*.* --network-interface nic-type=GVNIC,subnet=xxxxxx-
hapvc-port2internal,private-network-ip=10.0.1.15,no-address --can-ip-forward --
maintenance-policy=MIGRATE --service-account=*****-
compute@developer.gserviceaccount.com --scopes=https://www.googleapis.com/auth/cloud-
platform --image=gcp-ond-0128-gvnic --image-project=dev-project-000-000000 --boot-disk-
type=pd-standard --boot-disk-device-name=xxxxxx-script-ond-0128
Created [https://www.googleapis.com/compute/beta/projects/dev-project-000-
000000/zones/us-centrall1-c/instances/xxxxxx-script-ond-0128-gvnic].
NAME                                ZONE                MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP
EXTERNAL_IP  STATUS
xxxxxx-script-ond-0128-gvnic  us-centrall1-c  n1-standard-1                10.6.30.5
**.**.*.*.*  RUNNING

```

3. Verify that gVNIC is enabled for the NIC:

```
gcloud compute instances describe xxxxxx-script-ond-0128-gvnic --zone=us-central1-c
...
guestOsFeatures:
- type: GVNIC
...
name: xxxxxx-script-ond-0128-gvnic
networkInterfaces:
- accessConfigs:
- kind: compute#accessConfig
name: external-nat
natIP: **.***.***.***
networkTier: PREMIUM
type: ONE_TO_ONE_NAT
fingerprint: OiB_2ejfR-g=
kind: compute#networkInterface
name: nic0
network: https://www.googleapis.com/compute/v1/projects/xxx-xxxxxxx-000-000000/global/networks/xxxxxxx
networkIP: 10.6.30.5
nicType: GVNIC
...
```

4. Log in to the FortiGate using SSH and verify that the drivers are correct:

```
# diagnose hardware lspci -v
00:04.0 Class 0200: Device 1ae0:0042
    Subsystem: Device 1ae0:0058
    Flags: bus master, fast devsel, latency 0, IRQ 11
    Memory at feb01000 (32-bit, non-prefetchable) [size=4K]
    Memory at feb02000 (32-bit, non-prefetchable) [size=64]
    Memory at fea00000 (32-bit, non-prefetchable) [size=1M]
    Capabilities: [80] MSI-X: Enable+ Count=3 Masked-
    Kernel driver in use: gvnic

# diagnose hardware deviceinfo nic port1
Name:                port1
Driver:              gve
Version:             1.2.0
Bus:                 0000:00:04.0
Hwaddr:              **:**:**:**:**:**
Permanent Hwaddr:   **:**:**:**:**:**
State:               up
Link:                up
Mtu:                 1460
Supported:
Advertised:
Auto:                disabled
```

FIPS cipher mode for OCI and GCP FortiGate VMs - 7.0.1

FIPS cipher mode is supported on OCI and GCP FortiGate VMs. All VPN configurations must be removed before FIPS CC mode can be enabled.

In `fips-ciphers` mode, only a restricted set of ciphers are allowed for features that require encryption, such as SSH, IPsec, SSL VPN, and HTTPS. Insecure protocols, such as Telnet, TFTP, and HTTP, cannot be used to access the FortiGate VM. For details, see [FIPS cipher mode for AWS and Azure FortiGate VMs](#)

A factory reset is required to disable `fips-ciphers` mode.

To enable fips-cipher mode:

```
config system fips-cc
    set status fips-ciphers
end
Warning: entering fips-ciphers mode. To exit this mode, factory reset is required.
Do you want to continue? (y/n) y
```

SD-WAN transit routing with Google Network Connectivity Center - 7.0.1

With an SD-WAN transit routing setup with Google Network Connectivity Center (NCC), you can route data and exchange border gateway protocol (BGP) routing information between two or more remote sites via GCP.

You can do this by configuring the NCC hub and an endpoint (spoke) for each remote site. To reduce network latency, deploy a spoke in the GCP region that is located geographically closest to the remote site that you are creating the spoke for. The NCC hub itself is VPC-specific.

For a detailed example, see [SD-WAN transit routing with Google Network Connectivity Center](#).

Support C5d instance type for AWS Outposts - 7.0.1

Different sizes of the C5d instance type are supported (FortiGate BYOL and PAYG listings), which are currently the only C5 class instance available for AWS Outposts.

To configure a C5d instance for an AWS VM:

1. Deploy a new instance with FortiOS 7.0.1 or later (see [Deploying FortiGate-VM on AWS](#)).
2. Select the *c5d.large* instance type.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

<input type="checkbox"/>	c5ad	c5ad.16xlarge	64	128	2 x 1200 (SSD)	Yes	20 Gigabit	Yes
<input type="checkbox"/>	c5ad	c5ad.24xlarge	96	192	2 x 1900 (SSD)	Yes	20 Gigabit	Yes
<input checked="" type="checkbox"/>	c5d	c5d.large	2	4	1 x 50 (SSD)	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.xlarge	4	8	1 x 100 (SSD)	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.2xlarge	8	16	1 x 200 (SSD)	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.4xlarge	16	32	1 x 400 (SSD)	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.9xlarge	36	72	1 x 900 (SSD)	Yes	10 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.12xlarge	48	96	2 x 900 (SSD)	Yes	12 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.18xlarge	72	144	2 x 900 (SSD)	Yes	25 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.24xlarge	96	192	4 x 900 (SSD)	Yes	25 Gigabit	Yes
<input type="checkbox"/>	c5d	c5d.metal	96	192	4 x 900 (SSD)	Yes	25 Gigabit	Yes
<input type="checkbox"/>	c5n	c5n.large	2	5.3	EBS only	Yes	Up to 25 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

3. Configure the instance settings, such as VPC and network (see [Deploying from BYOL AMI](#)).
4. Review the setup and launch the instance (see [Deploying from BYOL AMI](#)).
5. On the *Instances* page, ensure that the C5d type FortiGate AWS instance is running.

New EC2 Experience Tell us what you think

EC2 Dashboard New

Events

Tags

Limits

▼ Instances

Instances New

Instances (1) Info

Filter instances

search: demo Clear filters

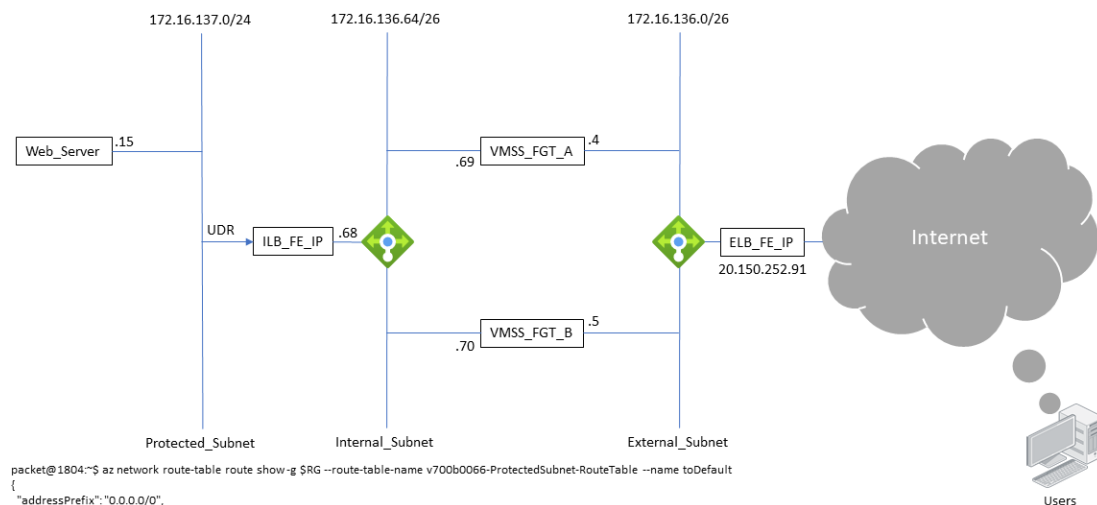
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	fgt-aws-c5d-demo-1	i-...	Running	c5d.large	2/2 checks passed	No alarms

You can now log in to the FortiGate AWS GUI.

FGSP session sync on FortiGate-VMs on Azure with autoscaling enabled - 7.0.1

FortiGate session life support protocol (FGSP) `cluster-sync` and `session-pickup` is automatically enabled on FortiGate-VM instances deployed on Azure with autoscaling enabled.

You can achieve the setup in this example by deploying the [template available on GitHub](#).



```
packet@1804:~$ az network route-table route show -g $RG --route-table-name v700b0066-ProtectedSubnet-RouteTable --name toDefault
{
  "addressPrefix": "0.0.0.0/0",
  "etag": "W/\"dc7d3637-fbcd-4461-b6dc-ef8062eab2b\"",
  "hasBgpOverride": false,
  "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/6899-VMSS-v700b0066/providers/Microsoft.Network/routeTables/v700b0066-ProtectedSubnet-RouteTable/routes/toDefault",
  "name": "toDefault",
  "nextHopIpAddress": "172.16.136.68",
  "nextHopType": "VirtualAppliance",
  "provisioningState": "Succeeded",
  "resourceGroup": "6899-VMSS-v700b0066",
  "type": "Microsoft.Network/routeTables/routes"
}
packet@1804:~$
```

The following describes the example configuration:

- The load balancing (LB) rules of both the external load balancer (ELB) and internal load balancer (ILB) have a floating IP address enabled and session persistence set to the client IP address.
- Outbound rules are configured to the ELB so that PC15 has Internet access.
- The FortiGate-VMs have firewall virtual IP address rules configured with the ELB performing destination network address translation so that client access from the Internet to PC15 keeps the original IP address.
- Client access from the Internet to PC15 has symmetric flow.

To configure FGSP session sync on FortiGate-VMs on Azure with autoscaling enabled:

1. In Azure, configure the ELB load balancing rules. Ensure that *Session persistence* is configured to the client IP address and that *Floating IP* is enabled:

Dashboard > Resource groups > 6899-VMSS-v700b0066 > v700b0066-ExternalLoadBalancer >

ExternalLBRule-FE-SSH

v700b0066-ExternalLoadBalancer

Name: ExternalLBRule-FE-SSH

IP Version: ☒ IPv4 ☐ IPv6

Frontend IP address: v700b0066-ELB-ExternalSubnet-FrontEnd (20.150.252.91)

Protocol: ☒ TCP ☐ UDP

Port: 65022

Backend port: 65022

Backend pool: v700b0066-ELB-ExternalSubnet-BackEnd

Health probe: lbprobe (TCP:8008) [Create new](#)

Session persistence: Client IP

Idle timeout (minutes): 4

TCP reset: ☒ Disabled ☐ Enabled

Floating IP: ☐ Disabled ☒ Enabled

Outbound source network address translation (SNAT): ☒ (Recommended) Use outbound rules to provide backend pool members access to the internet. [Learn more](#) ☐ Use implicit outbound rule. This is not recommended because it can cause SNAT port exhaustion. [Learn more](#)

2. Configure the ELB outbound rules:

Dashboard > Resource groups > 6899-VMSS-v700b0066 > v700b0066-ExternalLoadBalancer >

to_Internet

v700b0066-ExternalLoadBalancer

Name: to_Internet

Frontend IP address: 1 selected

Protocol: ☒ All ☐ TCP ☐ UDP

Idle timeout (minutes): 4 (Max: 100)

TCP Reset: ☒ Enabled ☐ Disabled

Backend pool: v700b0066-ELB-ExternalSubnet-BackEnd (2 instances)

Port allocation

Azure automatically assigns the number of outbound ports to use for source network address translation (SNAT) based on the number of frontend IP addresses and backend pool instances. [Learn more about outbound connectivity](#)

Port allocation: Manually choose number of outbound ports

Outbound ports

Choose by: Maximum number of backend instances

Ports per instance: 31976

Available Frontend Ports: 63960

Maximum number of backend instances: 2

3. Configure the ILB load balancing rules. Ensure that *Session persistence* is configured to the client IP address and that *Floating IP* is enabled:

Dashboard > Resource groups > 6899-VMSS-v700b0066 > v700b0066-InternalLoadBalancer >

lbruleFEall

v700b0066-InternalLoadBalancer

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name: lbruleFEall

IP Version: ☒ IPv4 ☐ IPv6

Frontend IP address: v700b0066-ILB-InternalSubnet-FrontEnd (172.16.136.68) ☐ HA Ports

Backend pool: v700b0066-ILB-InternalSubnet-BackEnd

Health probe: lbrule (TCP:8008) [Create new](#)

Session persistence: Client IP

Idle timeout (minutes): 5

TCP reset: ☒ Disabled ☐ Enabled

Floating IP: ☐ Disabled ☒ Enabled

4. Confirm the configuration in the FortiGate A CLI. The following shows an example of possible output:

```
v700b0066-FGT-A # diagnose ip address list
IP=172.16.136.4->172.16.136.4/255.255.255.192 index=3 devname=port1
IP=172.16.136.69->172.16.136.69/255.255.255.192 index=4 devname=port2
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=7 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=11 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=14 devname=vsys_fgfm

v700b0066-FGT-A #
v700b0066-FGT-A # show system vdom-exception
config system vdom-exception
  edit 10
    set object system.cluster-sync
  next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show system auto-scale
config system auto-scale
  set status enable
  set role primary
  set sync-interface "port2"
  set psksecret ENC
TJSGPV1J2oxb7+ePiw8Sd42y6fHGYfHm84LeKa2wGTkcMxDfLg94dpuNqB8ID53wke91tNs3lyl0rZ5xc8c
U6NGGLTws7U3pFkKd0vxCMF37fDVLcItPLDXN2EWXTiX5v2s02QpUTkqIWlAv/KedMpmRMuKdx6DDWmhWUoL
nw99CO3zUWQjtf5FAtxIupcL6yGtSAVw==
end
```

```
v700b0066-FGT-A #
v700b0066-FGT-A # show system cluster-sync
config system cluster-sync
    edit 1
        set peerip 172.16.136.70
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show system ha
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set session-pickup-nat enable
    set override disable
end

v700b0066-FGT-A #
v700b0066-FGT-A # show firewall vip 172.16.137.15:22
config firewall vip
    edit "172.16.137.15:22"
        set uuid a26b50cc-db75-51eb-7dd5-a313054c614a
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 65022
        set mappedport 22
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show firewall vip 172.16.137.15:80
config firewall vip
    edit "172.16.137.15:80"
        set uuid aba58d6a-db75-51eb-118b-b771bfbf59b4
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 80
        set mappedport 80
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show firewall vip 172.16.137.15:443
```

```
config firewall vip
    edit "172.16.137.15:443"
        set uuid b0e949d8-db75-51eb-fb60-f5537489a0bc
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 443
        set mappedport 443
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show firewall policy
config firewall policy
    edit 2
        set name "to_VIP"
        set uuid c9ff1fd8-db75-51eb-6b34-e17d224884b9
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "172.16.137.15:22" "172.16.137.15:443" "172.16.137.15:80"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "default"
        set logtraffic all
    next
    edit 3
        set name "to_Internet"
        set uuid d834ffb4-db75-51eb-e370-b6668f0fd24d
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set nat enable
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show router static
config router static
```

```
edit 1
    set gateway 172.16.136.1
    set device "port1"
next
edit 2
    set dst 172.16.136.0 255.255.252.0
    set gateway 172.16.136.65
    set device "port2"
next
edit 3
    set dst 168.63.129.16 255.255.255.255
    set gateway 172.16.136.65
    set device "port2"
next
edit 4
    set dst 168.63.129.16 255.255.255.255
    set gateway 172.16.136.1
    set device "port1"
next
edit 137
    set dst 172.16.137.0 255.255.255.0
    set gateway 172.16.136.65
    set device "port2"
next
end

v700b0066-FGT-A #
v700b0066-FGT-A # get system auto-scale
status           : enable
role             : primary
sync-interface   : port2
primary-ip       : 0.0.0.0
callback-url     :
hb-interval      : 10
psksecret        : *

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys ha autoscale-peers
Serial#: FGTAZRUPN-GQBR9B
VMID:    9b09d366-f5e2-490f-acab-3bbf2835bd7b
Role:    secondary
IP:      172.16.136.70

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys ha checksum autoscale-cluster

===== FGTAZRJ_NNBQZJD0 =====
```

```
is_autoscale_primary()=1
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e
```

```
checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e
```

```
===== FGTAZRUPN-GQBR9B =====
```

```
is_autoscale_primary()=0
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e
```

```
checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e
```

```
v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=115:0, update=505, delete=1:0, query=5
recv: create=7:0, update=22, delete=0:0, query=0
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=626, recv=28
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
    1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-
65535, dport=0:65535
```

5. Confirm the configuration in the FortiGate B CLI. The following shows an example of possible output:

```
v700b0066-FGT-B # diagnose ip address list
IP=172.16.136.5->172.16.136.5/255.255.255.192 index=3 devname=port1
IP=172.16.136.70->172.16.136.70/255.255.255.192 index=4 devname=port2
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=7 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=11 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=14 devname=vsys_fgfm
```

```
v700b0066-FGT-B #
v700b0066-FGT-B # show system vdom-exception
```

```
path=system, objname=vdom-exception, tablename=(null), size=88
config system vdom-exception
    edit 10
        set object system.cluster-sync
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show system auto-scale
path=system, objname=auto-scale, tablename=(null), size=184
config system auto-scale
    set status enable
    set sync-interface "port2"
    set primary-ip 172.16.136.69
    set psksecret ENC
eZcoPrBuiWb56WynxSJPLzPnxnD9SrMSRxHpb8uwW/jFi9tFl+66kj9atAtSlTfoWff/12hQJjp0nECYHWd
/RrUMN0AavBdDFzZM7u8COFk7MgkPmtW+DMJyIojlDS80VGTebNIUES+svJmlwkL7Km4FdNu3xKeZzEzv2V
UoyOlabrdWI50vz0MOOCesK7Xuxq/Kig==
end

v700b0066-FGT-B #
v700b0066-FGT-B # show system cluster-sync
path=system, objname=cluster-sync, tablename=(null), size=216
config system cluster-sync
    edit 1
        set peerip 172.16.136.70
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show system ha
path=system, objname=ha, tablename=(null), size=5960
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set session-pickup-nat enable
    set override disable
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall vip 172.16.137.15:22
path=firewall, objname=vip, tablename=172.16.137.15:22, size=840
config firewall vip
    edit "172.16.137.15:22"
        set uuid a26b50cc-db75-51eb-7dd5-a313054c614a
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
```

```
        set extintf "port1"
        set portforward enable
        set extport 65022
        set mappedport 22
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall vip 172.16.137.15:80
path=firewall, objname=vip, tablename=172.16.137.15:80, size=840
config firewall vip
    edit "172.16.137.15:80"
        set uuid aba58d6a-db75-51eb-118b-b771bfbf59b4
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 80
        set mappedport 80
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall vip 172.16.137.15:443
path=firewall, objname=vip, tablename=172.16.137.15:443, size=840
config firewall vip
    edit "172.16.137.15:443"
        set uuid b0e949d8-db75-51eb-fb60-f5537489a0bc
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 443
        set mappedport 443
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall policy
path=firewall, objname=policy, tablename=(null), size=2816
config firewall policy
    edit 2
        set name "to_VIP"
        set uuid c9ff1fd8-db75-51eb-6b34-e17d224884b9
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
```



```
        set dstaddr "172.16.137.15:22" "172.16.137.15:443" "172.16.137.15:80"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "default"
        set logtraffic all
    next
    edit 3
        set name "to_Internet"
        set uuid d834ffb4-db75-51eb-e370-b6668f0fd24d
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set nat enable
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show router static
path=router, objname=static, tablename=(null), size=296
config router static
    edit 1
        set gateway 172.16.136.1
        set device "port1"
    next
    edit 2
        set dst 172.16.136.0 255.255.252.0
        set gateway 172.16.136.65
        set device "port2"
    next
    edit 3
        set dst 168.63.129.16 255.255.255.255
        set gateway 172.16.136.65
        set device "port2"
    next
    edit 4
        set dst 168.63.129.16 255.255.255.255
        set gateway 172.16.136.1
        set device "port1"
    next
    edit 137
        set dst 172.16.137.0 255.255.255.0
```

```
        set gateway 172.16.136.65
        set device "port2"
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # get system auto-scale
path=system, objname=auto-scale, tablename=(null), size=184
status          : enable
role            : secondary
sync-interface  : port2
primary-ip      : 172.16.136.69
callback-url    :
hb-interval     : 10
psksecret       : *

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys ha autoscale-peers
Serial#: FGTAZRJ_NNBQZJD0
VMID:      d00cd4bc-2d8f-4fb5-a42f-0297d5e52db7
Role:      primary
IP:        172.16.136.69

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys ha checksum autoscale-cluster

===== FGTAZRUPN-GQBR9B =====

is_autoscale_primary()=0
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root:  21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all:   92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root:  21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all:   92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

===== FGTAZRJ_NNBQZJD0 =====

is_autoscale_primary()=1
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root:  21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all:   92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e
```

```

checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=59:0, update=219, delete=0:0, query=6
recv: create=11:0, update=45, delete=0:0, query=0
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=284, recv=51
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
    1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-
65535, dport=0:65535

v700b0066-FGT-B #

```

When autoscaling is enabled, the configuration syncs between the primary FortiGate to the secondary FortiGate in the virtual machine scale set (VMSS). With FGSP configured, sessions sync to all VMSS members. With the ELB performing DNAT and the firewall VIP policy configured on the FortiGate, original client IP addresses are kept.

```

fosqa@pc15:~$ w
 16:26:02 up 38 days,  1:29,  3 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
packet    pts/0    13.83.82.124     Wed15    23:45m 0.02s  0.00s tail -f /var/lo
fosqa     pts/1    207.102.138.19  Wed15    2:00s  0.03s  0.00s w
fosqa     pts/3    13.66.229.197   Wed15    23:45m 0.02s  0.00s tail -f /var/lo
fosqa@pc15:~$
fosqa@pc15:~$ tail /var/log/nginx/access.log
165.22.97.76 - - [12/Aug/2021:15:55:11 -0700] "GET /stalker_portal/c/version.js HTTP/1.1"
444 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/74.0.3729.169 Safari/537.36"
165.22.97.76 - - [12/Aug/2021:15:55:11 -0700] "GET /stream/live.php HTTP/1.1" 444 0 "-"
"Roku/DVP-9.10 (289.10E04111A)"
165.22.97.76 - - [12/Aug/2021:15:55:12 -0700] "GET /flu/403.html HTTP/1.1" 444 0 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/74.0.3729.169 Safari/537.36"
117.193.32.121 - - [12/Aug/2021:15:56:15 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
88.2.174.20 - - [12/Aug/2021:16:04:30 -0700] "GET / HTTP/1.1" 200 443 "-" "Mozilla/5.0
(Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2
Safari/601.7.7"
45.79.155.112 - - [12/Aug/2021:16:13:23 -0700] "GET / HTTP/1.1" 200 299 "-" "Mozilla/5.0
(Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0"
117.223.219.238 - - [12/Aug/2021:16:14:14 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
59.95.127.92 - - [12/Aug/2021:16:16:03 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
103.197.205.191 - - [12/Aug/2021:16:16:28 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
128.199.23.44 - - [12/Aug/2021:16:21:03 -0700] "GET / HTTP/1.1" 200 299 "-" "Mozilla/5.0
(Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.78
Safari/537.36 OPR/47.0.2631.39"
fosqa@pc15:~$

```

For example, when multiple users are connecting to PC15 via SSH from the Internet, DNAT sessions sync between the FortiGates:

```
v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session filter clear

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session filter proto 6

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session filter dport 65022

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session clear

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session list
total session 0

v700b0066-FGT-A #
v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session list

session info: proto=6 proto_state=11 duration=9 expire=3595 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty synced f00
statistic(bytes/packets/allow_err): org=4305/22/1 reply=4533/19/1 tuples=3
tx speed(Bps/kbps): 436/3 rx speed(Bps/kbps): 459/3
origin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=172.16.136.65/172.16.136.1
hook=pre dir=org act=dnat 207.102.138.19:57402->20.150.252.91:65022(172.16.137.15:22)
hook=post dir=reply act=snat 172.16.137.15:22->207.102.138.19:57402(20.150.252.91:65022)
hook=post dir=org act=noop 207.102.138.19:57402->172.16.137.15:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00001fd4 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008

session info: proto=6 proto_state=11 duration=10 expire=3589 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=dnat 13.83.82.124:55212->20.150.252.91:65022(172.16.137.15:22)
hook=post dir=reply act=snat 172.16.137.15:22->13.83.82.124:55212(20.150.252.91:65022)
hook=post dir=org act=noop 13.83.82.124:55212->172.16.137.15:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
```

```

misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00000591 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
np_u_state=0x001000
total session 2

v700b0066-FGT-A #
v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=213:0, update=899, delete=2:0, query=11
recv: create=32:0, update=119, delete=1:0, query=1
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=1125, recv=152
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
    1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-65535,
dport=0:65535

v700b0066-FGT-A #
v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session filter clear

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session filter proto 6

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session filter dport 65022

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session clear

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session list
total session 0

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session list

session info: proto=6 proto_state=11 duration=12 expire=3587 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=dnat 207.102.138.19:57402->20.150.252.91:65022(172.16.137.15:22)
hook=post dir=reply act=snat 172.16.137.15:22->207.102.138.19:57402(20.150.252.91:65022)
hook=post dir=org act=noop 207.102.138.19:57402->172.16.137.15:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0

```

```

serial=00001fd4 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x001000

session info: proto=6 proto_state=11 duration=13 expire=3598 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty synced f00
statistic(bytes/packets/allow_err): org=3861/27/1 reply=3965/21/1 tuples=3
tx speed(Bps/kbps): 277/2 rx speed(Bps/kbps): 284/2
origin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=172.16.136.65/172.16.136.1
hook=pre dir=org act=dnat 13.83.82.124:55212->20.150.252.91:65022 (172.16.137.15:22)
hook=post dir=reply act=snat 172.16.137.15:22->13.83.82.124:55212 (20.150.252.91:65022)
hook=post dir=org act=noop 13.83.82.124:55212->172.16.137.15:22 (0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00000591 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x001008
total session 2

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=23:0, update=89, delete=1:0, query=1
recv: create=43:0, update=146, delete=0:0, query=3
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=114, recv=187
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
    1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-65535,
dport=0:65535

v700b0066-FGT-B #

```

Flex-VM token and bootstrap configuration file fields in custom OVF template - 7.0.2

New *License Token* and *Configuration URL* fields have been added to custom Open Virtualization Format (OVF) templates to allow inputting a flex-VM token code and web URL where a bootstrap configuration file for the FortiGate are stored. This reduces the number of steps when provisioning and bootstrapping a FortiGate-VM.

Having FortiGate use a configuration file available on a web server dramatically reduces the deployment complexity:

- You can use a centralized web server to host all bootstrapping configuration files. You do not need to upload ISO files to multiple clouds and datastores.
- You do not need to attach a CD-ROM to the VM.
- You only need to create the configuration file on the web server and enter the file URL as an OVF custom property.

In the following example, the license token is 182C8C8143C841028572 and the configuration URL is <http://172.18.64.219/fgt-17491.txt>.

To provision a FortiGate-VM using the flex-VM token and bootstrap configuration file fields:

1. Create a new FGT-VM64 from the vCenter GUI with the `datadrive.vmdk`, `fortios.vmdk` and `FortiGate-VM64.vapp.ovf` files extracted from `FGT_VM64-v7-build0203-FORTINET.out.ovf.zip`. On the *Customize template* page, configure the *License Token* and *Configuration URL* fields with the flex-VM token and the URL where the bootstrap configuration file is stored.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Fortigate 6 settings	
License Token	182C8C8143C841028572
Configuration URL	http://172.18.64.219/fgt-17491.txt
Hostname	FortiGate-VM
Primary DNS	208.91.112.53
Secondary DNS	208.91.112.52
FortiManager	FQDN or IP address of FortiManager

Interface 01 4 settings	
Interface 1: Mode	IP/Netmask will be ignored if DHCP is chosen. Static
IP	10.6.30.66
Netmask	255.255.255.0
Gateway	10.6.30.254

CANCEL BACK NEXT

2. Configure the FortiGate as desired. This example configures the hostname and admin timeout:

```
root@CtrlPC-1:~# curl http://172.18.64.219/fgt-17491.txt
config sys global
    set hostname fgt-17491
    set admintimeout 480
end
```

After the FortiGate-VM boots up, it activates the VM license and automatically loads the configuration.

3. Verify the license and configuration data was populated to the FortiGate. Verify that the configuration you modified in step 2 was populated to the FortiGate:

```
fgt-17491 # get sys stat
Version: FortiGate-VM64 v7.0.2,buidl0203,210906 (interim)
Serial-Number: FGVMMMLTM20000045
License Status: Valid
License Expiration Date: 2022-10-31
```

```
fgt-17491 # diagnose debug cloudinit show
>> Checking metadata source ovf
>> Cloudinit downloading config:
>> Cloudinit download config successfully
```

```

>> Found metadata source: ovf
>> Trying to install vmlicense ...
>> License-token:182C8C8143C841028572
>> Run config script
>> Finish running script
>> FortiGate-VM $ config sys global
>> FortiGate-VM (global) $ set hostname fgt-17491
>> FortiGate-VM (global) $ set admintimeout 480
>> FortiGate-VM (global) $ end
>> fgt-17491 $

fgt-17491 # diagnose vmware ovfenv
<?xml version="1.0" encoding="UTF-8"?>
<Environment
...
  <PropertySection>
    <Property oe:key="config-url" oe:value="http://172.18.64.219/fgt-
17491.txt"/>
    <Property oe:key="license-token" oe:value="182C8C8143C841028572"/>
  ...

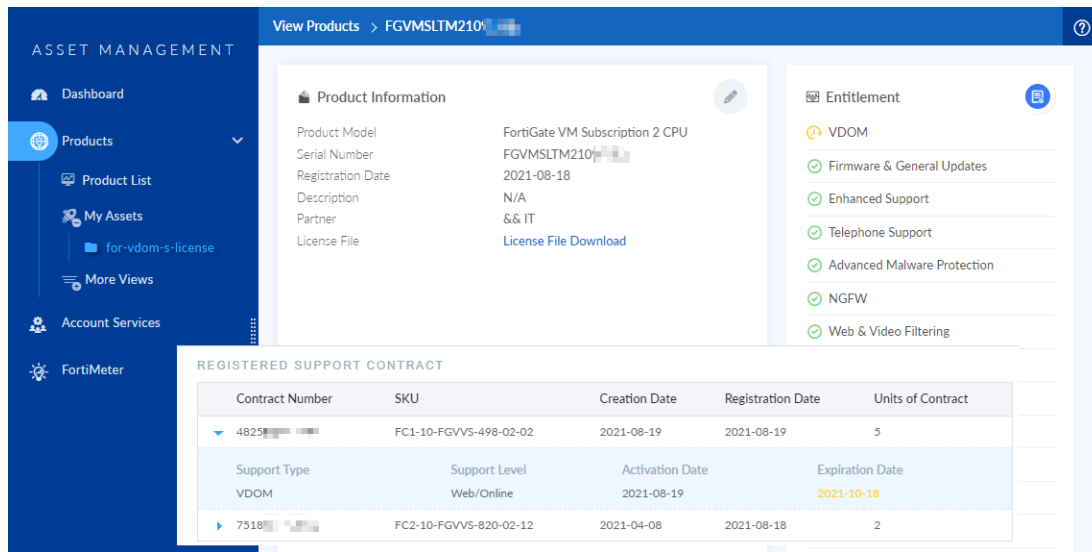
```

Subscription-based VDOM license for FortiGate-VM S-series - 7.0.2

The FortiGate-VM S-series licensing now supports subscription-based virtual domain (VDOM) licensing, using the new stackable subscription-based SKU.

The following describes the process for purchasing and applying the subscription-based VDOM license with FortiGate-VM S-series. The following assumes that the FortiGate-VM with the S-series license applied can connect to FortiGuard:

1. Purchase the VDOM subscription license (SKU FC1-10-FGVVS-498-02-DD). This license adds five VDOMs to a FortiGate-VM S-series running FortiOS 7.0.1 or a later version. You can stack this SKU to add more VDOMs.
2. Register the VDOM subscription license to the FortiGate-VM S-series license:
 - a. In FortiCloud Asset Management, go to *Products > Product List*.
 - b. View the desired FortiGate-VM.
 - c. In *Registration*, click *Add Licenses*.
 - d. Complete the steps to register the VDOM subscription license.



3. FortiGate-VM retrieves the VDOM subscription license from FortiGuard. This can take up to two hours. Confirm that the FortiGate-VM has retrieved the license using the `get system status` command. The following shows example output when FortiOS has successfully retrieved the license:

```
Version: FortiGate-VM64 v7.0.2,build0227,211006 (interim)
```

```
Virus-DB: 88.05870(2021-08-23 08:59)
```

```
Extended DB: 88.05870(2021-08-23 08:58)
```

```
Extreme DB: 1.00000(2018-04-09 18:07)
```

```
AV AI/ML Model: 2.00033(2021-07-29 11:18)
```

```
IPS-DB: 6.00741(2015-12-01 02:30)
```

```
IPS-ETDB: 6.00741(2015-12-01 02:30)
```

```
APP-DB: 6.00741(2015-12-01 02:30)
```

```
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
```

```
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
```

```
Serial-Number: FGVMSLTM210...
```

```
License Status: Valid
```

```
License Expiration Date: 2022-08-20
```

```
VM Resources: 1 CPU/2 allowed, 2007 MB RAM
```

```
Log hard disk: Available
```

```
Hostname: FortiGate-VM64
```

```
Private Encryption: Disable
```

```
Operation Mode: NAT
```

```
Current virtual domain: root
```

```
Max number of virtual domains: 6
```

```

Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0227
Release Version Information: interim
FortiOS x86-64: Yes
System time: Thu Oct  7 16:16:19 2021
Last reboot reason: warm reboot

```

You can also use the `diagnose debug vm-print-license`. The following shows example output for this command:

```

SerialNumber: FGVMSLTM210...
CreateDate: Thu Aug 19 06:27:38 2021
License expires: Sat Aug 20 17:00:00 2022
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: SL (18)
CPU: 2 (FDS:2)
MEM: 2147483647
VDOM license:
    permanent: 1
    subscription: 5
    expires: Wed Oct 20 17:00:00 2021

```

4. Enable multiple VDOMs:

```

config system global
    set vdom-mode multi-vdom
end

```

5. Use the following commands to debug the configuration:

```

diagnose debug application update -1
diagnose debug enable
execute update-now

```

The following shows the example output:

```

upd_status_extract_contract_info[1104]-Extracting contract...
  (SerialNumber=FGVMSLTM210...|Contract=AVDB-1-06-20220821:0:1:1:0*AVEN-1-06-
  20220821:0:1:1:0*NIDS-1-06-20220821:0:1:1:0*SPRT-1-20-20220821:0:1:1:0*ISSS-1-06-
  20220821:0:1:1:0*SPAM-1-06-20220821:0:1:1:0*SWNC-1-06-20220821:0:1:1:0*SWM-1-06-
  20220821:0:1:1:0*SWNO-1-06-20220821:0:1:1:0*VMLS-1-06-20220821:0:2:2:0*IPMC-1-06-
  20220821:0:1:1:0*IOTH-1-06-20220821:0:1:1:0*FAZC-1-06-20220821:0:1:1:0*FGSA-1-06-
  20220821:0:1:1:0*FMGC-1-06-20220821:0:1:1:0*FMWR-1-06-20220821:0:1:1:0*FRVS-1-06-
  20220821:0:1:1:0*FURL-1-06-20220821:0:1:1:0*ZHVO-1-06-20220821:0:1:1:0*VDOM-1-06-
20211021:0:5:5:0*

```

FortiOS Carrier

For changes to FortiOS Carrier, see the What's New sections in the [FortiOS Carrier Administration Guide](#).



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.