



FortiOS - Cookbook

Version 6.0.0

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



June 24, 2020

FortiOS 6.0.0 Cookbook

01-600-000000-20200624

TABLE OF CONTENTS

| | |
|---|-----------|
| Change log | 9 |
| Getting started | 10 |
| Installing a FortiGate in NAT mode | 10 |
| Connecting network devices | 10 |
| Configuring interfaces | 11 |
| Adding a default route | 12 |
| Selecting DNS servers (optional) | 13 |
| Creating a policy | 13 |
| Results | 14 |
| Fortinet Security Fabric installation | 16 |
| Configuring Edge | 17 |
| Installing Accounting and Marketing | 22 |
| Installing Sales | 27 |
| Configuring the FortiAnalyzer | 32 |
| Adding security profiles (optional) | 35 |
| Results | 36 |
| VDOM configuration | 38 |
| Enabling and creating VDOMs | 39 |
| Configuring a management interface | 39 |
| Assigning interfaces | 40 |
| Creating per-VDOM administrators | 42 |
| Configuring the VDOMs | 43 |
| Configuring global security profiles | 44 |
| Results | 45 |
| FortiGate registration and basic settings | 47 |
| Registering your FortiGate | 47 |
| Setting system time | 50 |
| Creating administrators | 50 |
| Using a trusted host (optional) | 52 |
| Results | 53 |
| Verifying FortiGuard licenses and troubleshooting | 54 |
| Viewing your licenses | 54 |
| Troubleshooting | 56 |
| Results | 58 |
| Logging FortiGate traffic and using FortiView | 60 |
| Configuring log settings | 60 |
| Enabling logging | 61 |
| Results | 61 |
| Creating security policies for different users | 64 |
| Creating the Employee user and policy | 65 |
| Creating the Accounting user and policy | 67 |
| Creating the Admin user, device, and policy | 68 |
| Ordering the policy table | 70 |
| Results | 71 |
| Upgrading FortiGate firmware | 72 |

| | |
|--|------------|
| Checking the current FortiOS firmware | 73 |
| Upgrading to the latest version | 73 |
| Results | 75 |
| Tags in the Fortinet Security Fabric | 76 |
| Creating tag categories and tags | 76 |
| Applying tags | 78 |
| Results | 80 |
| Port forwarding | 82 |
| Creating virtual IP addresses | 82 |
| Creating a virtual IP group | 85 |
| Creating a security policy | 86 |
| Results | 87 |
| Security Rating | 90 |
| Checking the Security Rating widget | 91 |
| Checking your Security Rating | 91 |
| Results | 93 |
| Automation stitches | 95 |
| Creating the Automation stitches | 96 |
| Testing the Automation stitches | 97 |
| Results | 99 |
| FortiSandbox in the Fortinet Security Fabric | 100 |
| Checking your Security Rating | 101 |
| Connecting the FortiSandbox | 101 |
| Allowing VM Internet access | 103 |
| Adding FortiSandbox to the Security Fabric | 104 |
| Adding sandbox inspection to security profiles | 106 |
| Results | 109 |
| FortiManager in the Fortinet Security Fabric | 111 |
| Connecting the FortiManager | 111 |
| Allowing Internet access | 112 |
| Configuring central management | 113 |
| Results | 115 |
| Redundant Internet with SD-WAN | 116 |
| Blocking malicious domains using threat feeds | 119 |
| Authentication | 121 |
| Agent-based FSSO for Windows AD | 121 |
| Installing the FSSO agent | 121 |
| Configuring the FSSO agent | 126 |
| Setting up your FortiGate for FSSO | 126 |
| Results | 129 |
| FSSO in polling mode for Windows AD | 130 |
| Creating a Fabric Connector | 130 |
| Creating a user group | 131 |
| Creating a policy | 132 |
| Results | 132 |
| High availability | 133 |
| High availability with two FortiGates | 133 |

| | |
|--|-----|
| Setting up registration and licensing | 134 |
| Configuring the primary FortiGate for HA | 134 |
| Connecting the backup FortiGate | 135 |
| Configuring the backup FortiGate | 136 |
| Viewing the status of the HA cluster | 137 |
| Results | 139 |
| (Optional) Upgrading the firmware for the HA cluster | 140 |
| High Availability with FGCP (expert) | 141 |
| Configuring the primary FortiGate | 142 |
| Configuring the backup FortiGate | 145 |
| Connecting the primary and backup FortiGates | 146 |
| Checking cluster operation | 146 |
| Disabling override (recommended) | 147 |
| Results | 147 |
| Adding a third FortiGate to an FGCP cluster (expert) | 149 |
| Enabling override on the primary FortiGate (optional) | 150 |
| Configuring the new FortiGate | 150 |
| Connecting the new FortiGate to the cluster | 151 |
| Checking cluster operation | 152 |
| Disabling override (recommended) | 153 |
| Converting to an active-active cluster | 153 |
| Results | 154 |
| FGCP Virtual Clustering with two FortiGates (expert) | 155 |
| Preparing the FortiGates | 156 |
| Configuring clustering | 157 |
| Connecting and verifying cluster operation | 159 |
| Adding VDOMs and setting up virtual clustering | 160 |
| Checking virtual cluster operation | 161 |
| Results | 163 |
| FGCP Virtual Clustering with four FortiGates (expert) | 165 |
| Preparing the FortiGates | 166 |
| Configuring clustering | 167 |
| Connecting and verifying cluster operation | 169 |
| Adding VDOMs and setting up virtual clustering | 170 |
| Checking virtual cluster operation | 172 |
| Results | 174 |
| SD-WAN with FGCP HA (expert) | 177 |
| Connecting the FortiGate to your ISPs | 178 |
| Removing existing configuration references to interfaces | 178 |
| Creating the SD-WAN interface | 178 |
| Configuring SD-WAN load balancing | 179 |
| Creating a static route for the SD-WAN interface | 180 |
| Configuring a security policy for SD-WAN | 181 |
| Configuring the FortiGate for HA | 181 |
| Configuring the backup FortiGate | 183 |
| Connecting the primary and backup FortiGates | 184 |
| Checking cluster operation | 185 |
| Disabling override (recommended) | 186 |
| Results | 186 |

| | |
|---|------------|
| Testing HA failover | 187 |
| Testing ISP failover | 187 |
| Security profiles | 189 |
| Blocking Facebook while allowing Workplace by Facebook | 189 |
| Creating a web filter profile | 189 |
| Applying the security profiles | 191 |
| Results | 192 |
| Antivirus scanning using flow-based inspection | 193 |
| Verifying the inspection mode | 193 |
| Configuring the AntiVirus profile | 194 |
| Enabling antivirus in a policy | 194 |
| Results | 195 |
| FortiSandbox in the Fortinet Security Fabric | 196 |
| Checking the Security Rating | 197 |
| Connecting the FortiSandbox and Edge | 197 |
| Allowing VM Internet access | 200 |
| Adding the FortiSandbox to the Security Fabric | 201 |
| Adding sandbox inspection to security profiles | 203 |
| Results | 206 |
| DNS Filtering | 208 |
| Creating a DNS web filter profile | 208 |
| Enabling DNS filtering in a security policy | 209 |
| Results | 211 |
| (Optional) Changing the FortiDNS server and port | 211 |
| Troubleshooting | 212 |
| Content Disarm and Reconstruction (CDR) | 214 |
| Setting the system inspection mode | 214 |
| Testing FortiSandbox connectivity | 215 |
| Enabling Content Disarm and Reconstruction | 215 |
| Configuring the Internet access policy | 215 |
| Results | 216 |
| Troubleshooting | 217 |
| Preventing certificate warnings (CA-signed certificate) | 218 |
| Using a CA-signed certificate | 218 |
| Generating a CSR on a FortiGate | 219 |
| Getting the certificate signed by a CA | 220 |
| Importing the signed certificate to your FortiGate | 221 |
| Editing the SSL inspection profile | 221 |
| Importing the certificate into web browsers | 224 |
| Results | 226 |
| Preventing certificate warnings (default certificate) | 228 |
| Using the default certificate | 228 |
| Generating a unique certificate | 228 |
| Downloading the certificate | 229 |
| Applying SSL inspection to a policy | 229 |
| Importing the certificate into web browsers | 229 |
| Results | 232 |
| Preventing certificate warnings (self-signed) | 235 |

| | |
|--|------------|
| Creating a certificate with OpenSSL | 235 |
| Importing the self-signed certificate | 236 |
| Editing the SSL inspection profile | 236 |
| Applying SSL inspection to a policy | 237 |
| Importing the certificate into web browsers | 237 |
| Results | 240 |
| Why you should use SSL inspection | 243 |
| Full SSL inspection | 243 |
| SSL certificate inspection | 244 |
| Troubleshooting | 245 |
| Best practices | 245 |
| VPNs | 246 |
| SSL VPN quick start | 246 |
| SSL VPN split tunnel for remote user | 246 |
| Connecting from FortiClient VPN client | 249 |
| Set up FortiToken two-factor authentication | 251 |
| Connecting from FortiClient with FortiToken | 252 |
| SSL VPN using web and tunnel mode | 253 |
| Editing the SSL VPN portal | 253 |
| Configuring the SSL VPN tunnel | 255 |
| Adding security policies | 257 |
| Verifying remote user OS and software | 258 |
| Results | 259 |
| SSL VPN with RADIUS and FortiToken | 264 |
| Creating a user and a user group | 264 |
| Creating the RADIUS client | 266 |
| Connecting the FortiGate to FortiAuthenticator | 267 |
| Allowing users to connect to the VPN | 269 |
| Results | 270 |
| FortiToken Mobile Push for SSL VPN | 272 |
| Adding FortiToken to FortiAuthenticator | 273 |
| Adding user to FortiAuthenticator | 273 |
| Creating the RADIUS client on FortiAuthenticator | 277 |
| Connecting the FortiGate to the RADIUS server | 278 |
| Configuring the SSL VPN | 281 |
| Results | 283 |
| IPsec VPN with FortiClient | 285 |
| Adding a firewall address | 285 |
| Configuring the IPsec VPN | 286 |
| Creating a security policy | 288 |
| Add FortiToken two-factor authentication | 289 |
| Add LDAP user authentication | 290 |
| Configuring FortiClient | 291 |
| Results | 292 |
| One-Click VPN (OCVPN) | 294 |
| Enabling OCVPN | 294 |
| Confirming cloud membership | 296 |
| Results | 297 |

| | |
|--|------------|
| Troubleshooting | 299 |
| Site-to-site IPsec VPN with two FortiGate devices | 301 |
| Configuring IPsec VPN on HQ | 301 |
| Configuring IPsec VPN on Branch | 304 |
| Results | 305 |
| Fortinet Security Fabric over IPsec VPN | 306 |
| Configuring tunnel interfaces | 307 |
| Adding tunnel interfaces to the VPN | 308 |
| Authorizing Branch for the Security Fabric | 311 |
| Allowing Branch to access the FortiAnalyzer | 312 |
| Results | 315 |
| Desynchronizing settings for Branch (optional) | 315 |
| Site-to-site IPsec VPN with overlapping subnets | 316 |
| Planning the new addressing scheme | 316 |
| Configuring the IPsec VPN on HQ | 317 |
| Configuring static routes on HQ | 318 |
| Configuring address objects on HQ | 319 |
| Configuring firewall policies on HQ | 320 |
| Configuring IPsec VPN on Branch | 322 |
| Configuring static routes on Branch | 323 |
| Configuring address objects on Branch | 324 |
| Configuring firewall policies on Branch | 325 |
| Results | 327 |
| Explanation | 328 |
| IPsec VPN to Alibaba Cloud (AliCloud) | 329 |
| Configuring the Alibaba Cloud (AliCloud) VPN gateway | 330 |
| Configuring the FortiGate | 332 |
| SSL VPN for remote users with MFA and user sensitivity | 333 |
| Topology | 334 |
| Example configuration | 334 |
| Verification | 339 |
| WiFi | 342 |
| Setting up WiFi with FortiAP | 342 |
| Connecting FortiAP | 342 |
| Creating an SSID | 344 |
| Creating a custom FortiAP profile | 345 |
| Creating a security policy | 346 |
| Results | 347 |
| Replacing the Fortinet_Wifi certificate | 348 |
| Guest WiFi accounts | 350 |
| Creating a guest user group | 351 |
| Creating an SSID | 351 |
| Creating a security policy | 353 |
| Creating a guest user management account | 354 |
| Creating a guest user account | 355 |
| Results | 356 |

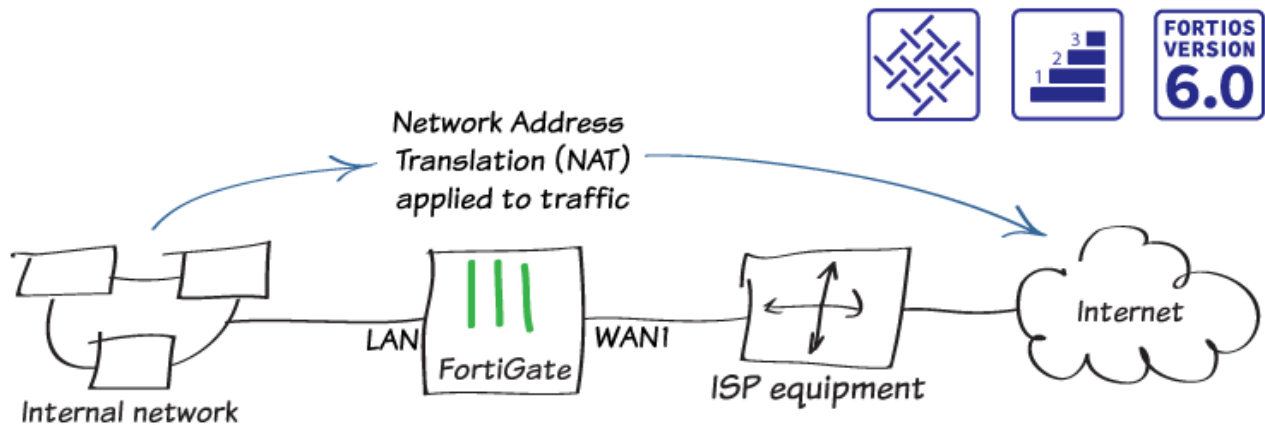
Change log

| Date | Change Description |
|------------|--|
| 2019-03-04 | Initial release. |
| 2019-05-09 | Added Blocking malicious domains using threat feeds on page 119 . |
| 2019-05-22 | Added Replacing the Fortinet_Wifi certificate on page 348 . |
| 2019-06-10 | Updated London FortiDNS server IP address in DNS Filtering on page 208 and related topics. |
| 2019-09-24 | Updated to remove outdated topic. |
| 2019-11-08 | Added video links. |
| 2020-03-24 | Added SSL VPN quick start on page 246 section. |
| 2020-06-24 | Added SSL VPN for remote users with MFA and user sensitivity on page 333 . |

Getting started

This section contains information about installing and setting up a FortiGate, as well common network configurations.

Installing a FortiGate in NAT mode



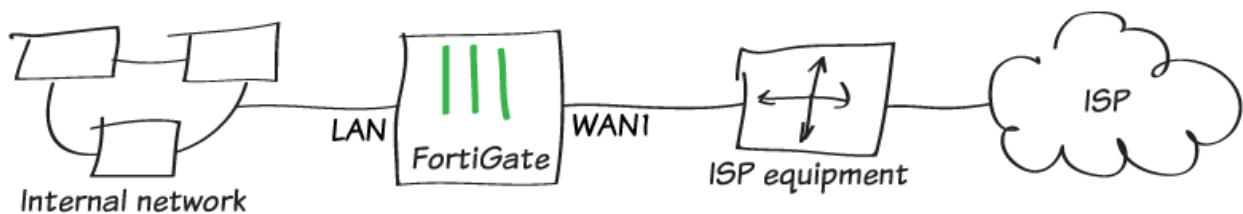
In this example, you connect and configure a new FortiGate in NAT mode, to securely connect a private network to the Internet.

In NAT mode, you install a FortiGate as a gateway, or router, between two networks. Typically, you set the FortiGate up between a private network and the Internet, which allows the FortiGate to hide the IP addresses of the private network using NAT.

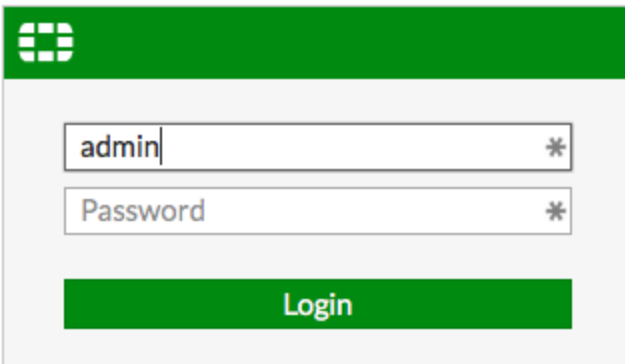
NAT mode is the most commonly used operating mode for a FortiGate.

Connecting network devices

1. Connect the FortiGate to your ISP-supplied equipment using the Internet-facing interface. This is typically WAN or WAN1, depending on your model.
2. Connect a PC to the FortiGate, using an internal port (in the example, port 3).





3. Power on the ISP equipment, the FortiGate, and the PC on the internal network.
4. Use the PC to connect to the FortiGate GUI using either FortiExplorer or an Internet browser. For more information about connecting to the GUI, see the QuickStart Guide for your FortiGate model.
5. Log in using an admin account. The default admin account has the username *admin* and no password.



The login screen features a green header with the FortiGate logo. Below it, there are two input fields: one for the username 'admin' and another for the password, both with asterisks indicating they are masked. A green 'Login' button is positioned at the bottom of the form.

Configuring interfaces

1. To edit the Internet-facing interface (in the example, wan1), go to **Network > Interfaces**.
2. Set the **Estimated Bandwidth** for the interface based on your Internet connection.
3. Set **Role** to **WAN**.

| | | | |
|---|--|---------------|--|
| Interface Name | wan1 (90:6C:AC:2A:14:5A) | | |
| Alias | <input type="text"/> | | |
| Link Status | Up  | | |
| Type | Physical Interface | | |
| Estimated Bandwidth  | <input type="text" value="10000"/> | Kbps Upstream | <input type="text" value="20000"/> Kbps Downstream |

Tags

| | |
|--|----------------------------------|
| Role  | <input type="text" value="WAN"/> |
| <input type="button" value="+ Add Tag Category"/> | |

Address

| | |
|-----------------|---|
| Addressing mode | <input type="button" value="Manual"/> <input type="button" value="DHCP"/> |
| IP/Network Mask | <input type="text" value="172.25.176.62/255.255.255.0"/> |

4. To determine which **Addressing mode** to use, check if your ISP provides an IP address for you to use or if the ISP equipment uses DHCP to assign IP addresses.
 - a. If your ISP provides an IP address, set **Addressing mode** to **Manual** and set the **IP/Network Mask** to that IP address.
 - b. If your ISP equipment uses DHCP, set **Addressing mode** to **DHCP** to allow the equipment to assign an IP address to WAN1.
5. Edit the **lan** interface, which is called **internal** on some FortiGate models.



If your FortiGate doesn't have a default LAN interface, for this step, you can use either an individual interface or create a software switch to combine the separate interfaces into a single virtual interface.

6. Set **Role** to **LAN**.
7. Set **Addressing mode** to **Manual** and set the **IP/Network Mask** to the private IP address that you want to use for the FortiGate.
8. If you need to assign IP addresses to devices on your internal network, enable **DHCP Server**.

Interface Name

Alias

Type

Interface Members

| | | |
|---------|----------|---------|
| port3 ✕ | port4 ✕ | port5 ✕ |
| port6 ✕ | port7 ✕ | port8 ✕ |
| port9 ✕ | port10 ✕ | |

+

Tags

Role

Add Tag Category

Address

Addressing mode ☒ Manual ☐ DHCP ☐ Dedicated to FortiSwitch

IP/Network Mask

Administrative Access

IPv4 ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access

☐ CAPWAP ☐ SSH ☐ SNMP ☐ FTM

☐ RADIUS Accounting ☐ FortiTelemetry

☒ DHCP Server

Address Range

Create New Edit Delete

| Starting IP | End IP |
|--------------|----------------|
| 192.168.65.2 | 192.168.65.254 |

Netmask

Default Gateway ☒ Same as Interface IP ☐ Specify


DNS Server ☒ Same as System DNS ☐ Same as Interface IP ☐ Specify

Advanced...

Adding a default route

1. To create a new default route, go to **Network > Static Routes**. Typically, you have only one default route. If the static route list already contains a default route, you can edit it, or delete the route and add a new one.
2. Set **Destination** to **Subnet** and leave the destination IP address set to 0.0.0.0/0.0.0.0.

3. Set **Gateway** to the IP address provided by your ISP and **Interface** to the Internet-facing interface.

| | |
|---------------------------|---|
| Destination ⓘ | <div>Subnet</div> <div>Named Address</div> <div>Internet Service</div> |
| | <input type="text" value="0.0.0.0/0.0.0.0"/> |
| Gateway | <input type="text" value="172.25.176.1"/> |
| Interface | <div> wan1 ▼</div> |
| Administrative Distance ⓘ | <input type="text" value="10"/> |
| Comments | <input type="text" value=""/> 0/255 |
| Status | <div>⬆ Enabled</div> <div>⬇ Disabled</div> |

+ Advanced Options

Selecting DNS servers (optional)

The FortiGate DNS settings are configured to use FortiGuard DNS servers by default, which is sufficient for most networks.

If you need to change the DNS servers, go to **Network > DNS**, select **Specify**, and add **Primary** and **Secondary** servers.

| | |
|----------------------|--|
| DNS Servers | <div>Use FortiGuard Servers</div> <div>Specify</div> |
| Primary DNS Server | <input type="text" value="208.91.112.53"/> |
| Secondary DNS Server | <input type="text" value="208.91.112.52"/> |
| Local Domain Name | <input type="text"/> |

Creating a policy



Some FortiGate models include an IPv4 security policy in the default configuration. If you have one of these models, edit it to include the logging options shown below, then proceed to the results section.

1. To create a new policy, go to **Policy & Objects > IPv4 Policy**. Give the policy a **Name** that indicates that the policy will be for traffic to the Internet (in the example, Internet).
2. Set the **Incoming Interface** to **lan** and the **Outgoing Interface** to **wan1**. Set **Source**, **Destination Address**, **Schedule**, and **Services**, as required.
3. Ensure the **Action** is set to **ACCEPT**.
4. Turn on **NAT** and select **Use Outgoing Interface Address**.

| | |
|--------------------|---|
| Name ⓘ | Internet |
| Incoming Interface | lan |
| Outgoing Interface | wan1 |
| Source | all |
| Destination | all |
| Schedule | always |
| Service | ALL |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

5. Scroll down to view the **Logging Options**. To view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options

Log Allowed Traffic ☒ Security Events ☒ All Sessions

Capture Packets ☐


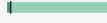
Results

1. Browse the Internet using the PC on the internal network.
2. If you can't connect to the Internet, see FortiGate installation troubleshooting.
3. To view information about FortiGate traffic, go to **FortiView > Traffic from LAN/DMZ > Sources**. The PC appears on the list of sources.





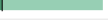
























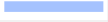
































| Source | Source Device | Bytes (Sent/Received) ▴ ▾ | Sessions ▴ ▾ | Bandwidth ▴ ▾ |
|--------------|----------------|---------------------------------|----------------------------|-------------------------------|
| 192.168.65.2 | jburkholder-pc | 19.92 MB <div><div></div></div> | 300 <div><div></div></div> | 3 Mbps <div><div></div></div> |

4. To view more detailed information about the traffic from the PC, right-click the entry for the PC and select **Drill Down to Details**.

Summary of 192.168.65.2

| | |
|-----------------------|---|
| Device | jburkholder-pc |
| Applications Detected | 3 |
| Bytes (Sent/Received) | 27.10 MB  |
| Bandwidth | 1.94 Mbps  |
| Sessions | 287 |
| Time Period | Realtime |
| FortiGate | FG800D3915800295 |

Destinations Applications Countries Policies Domains Categories Source Interfaces Destination Interfaces Sessions

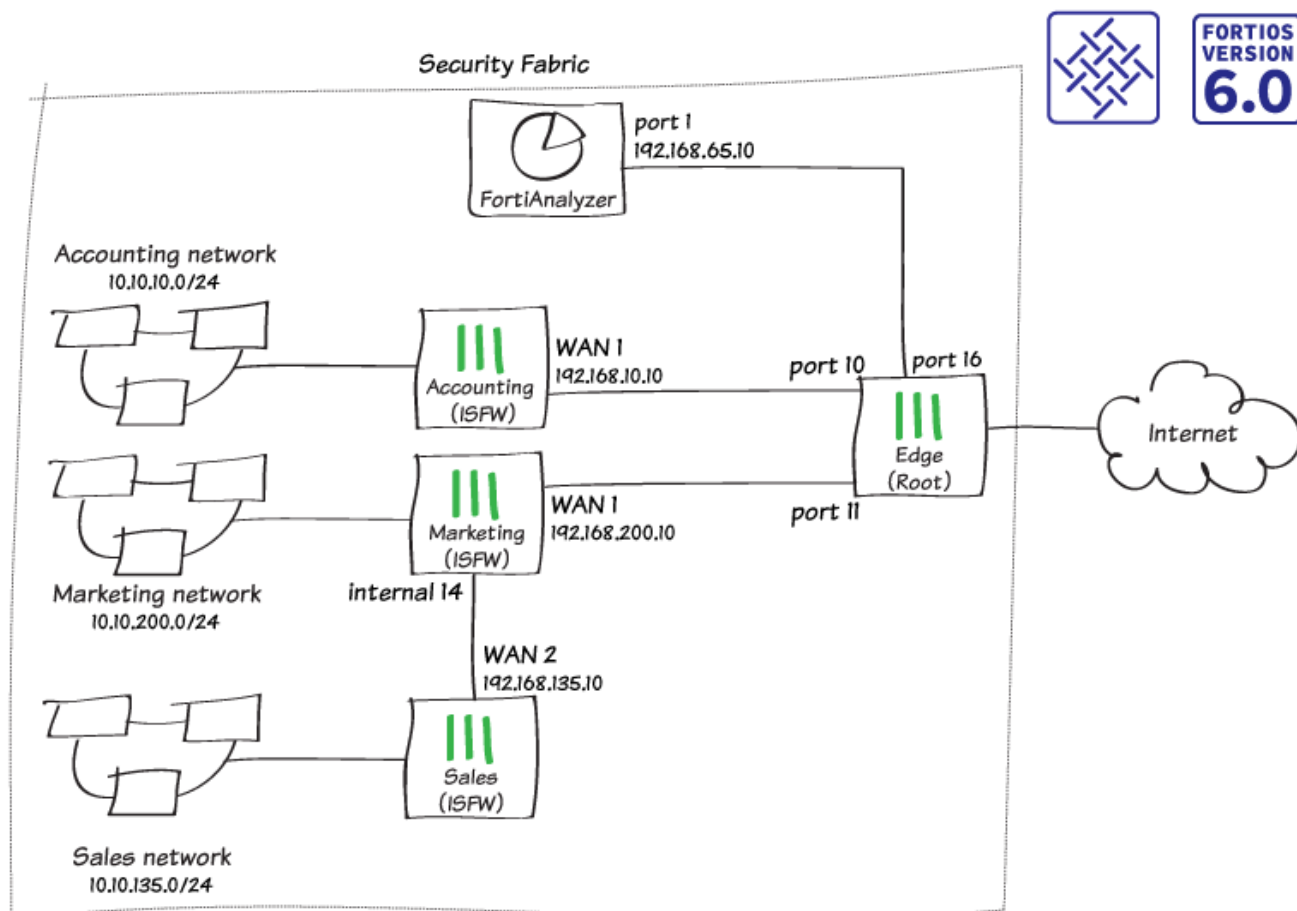
| Destination | Bytes (Sent/Received)  | Sessions  | Bandwidth  |
|---|---|--|---|
|  r1.sn-gvbxgn-tvve.googlevideo.com (209.148.198.204) | 19.06 MB  | 1 | 2 Mbps  |
|  googleapis.l.google.com (172.217.10.106) | 3.93 MB  | 3 | 48 bps  |
|  ytim.g.l.google.com (172.217.10.238) | 1.65 MB  | 1 | 256 bps  |
|  fcmatch.youtube.com (172.217.9.238) | 943.07 kB  | 2 | 40 bps  |
|  gstaticadssl.l.google.com (172.217.9.227) | 339.81 kB  | 2 | 88 bps  |
|  www.google.ca (216.58.193.67) | 317.69 kB  | 1 | 48 bps  |
|  pagead2.googleadsyndication.com (172.217.11.2) | 297.90 kB  | 1 | 48 bps  |
|  pagead-googlehosted.l.google.com (172.217.9.225) | 152.98 kB  | 1 | 48 bps  |
|  208.91.112.53 | 86.07 kB  | 222  | 288 bps  |
|  partnerad.l.doubleclick.net (172.217.10.98) | 83.45 kB  | 1 | 48 bps  |
|  redirector.gvt1.com (172.217.10.110) | 65.40 kB  | 2 | 40 bps  |
|  yt3.ggpht.com (172.217.10.97) | 63.22 kB  | 1 | 40 bps  |
|  www.google.com (172.217.3.164) | 27.01 kB  | 1 | 48 bps  |
|  adservice.google.com (172.217.12.194) | 21.46 kB  | 2 | 112 bps  |
|  cm.g.doubleclick.net (172.217.12.130) | 16.69 kB  | 2 | 88 bps  |
|  pipeline-edge-prod-25-561439127.us-west-2.elb.amazonaws.com (54.68.157.14) | 13.24 kB  | 1 | 3 kbps  |
|  208.91.112.52 | 12.10 kB  | 41  | 0 bps  |
|  cs9.wac.phicdn.net (72.21.91.29) | 8.34 kB  | 1 | 56 bps  |
|  static-doubleclick-net.l.google.com (172.217.9.230) | 6.43 kB  | 1 | 0 bps  |

5. If your FortiGate model has internal storage and disk logging enabled, a drop-down menu in the top corner allows you to view historical logging information for the previous **5 minutes**, **1 hour**, and **24 hours**.

6. If you're not sure whether your model supports disk logging, check the FortiGate [Feature/Platform Matrix](#).

For further reading, check out [NAT mode installation](#).

Fortinet Security Fabric installation



In this recipe, you configure a Fortinet Security Fabric that consists of four FortiGate devices and a FortiAnalyzer. One of the FortiGate devices acts as the network edge firewall and root FortiGate of the Security Fabric, while the other FortiGate devices function as Internal Segmentation Firewalls (ISFWs).

The example network uses the following FortiGate aliases:

- **Edge:** the root FortiGate in the Security Fabric. This FortiGate is named “Edge” because it’s the only FortiGate that directly connects to the Internet. This role is also known as the gateway FortiGate.



This FortiGate has already been installed in NAT mode using [Installing a FortiGate in NAT mode on page 10](#).

- **Accounting:** an ISFW FortiGate that connects to Edge.
- **Marketing:** an ISFW FortiGate that connects to Edge.
- **Sales:** an ISFW FortiGate that connects to Marketing.



Not all FortiGate models can run the FortiGuard Security Rating Service if they are the root FortiGate in a Security Fabric. For more information, see the [FortiOS 6.0 Release Notes](#).

Configuring Edge


In the Security Fabric, Edge is the root FortiGate. This FortiGate receives information from the other FortiGates in the Security Fabric.

In the example, the following interfaces on Edge connect to other network devices:

- Port 9 connects to the Internet (this interface was configured when Edge was installed)
 - Port 10 connects to Accounting (IP address: 192.168.10.2)
 - Port 11 connects to Marketing (IP address: 192.168.200.2)
 - Port 16 connects to the FortiAnalyzer (IP address: 192.168.55.2)
1. To edit port 10 on Edge, go to **Network > Interfaces**. Set an **IP/Network Mask** for the interface (in the example, 192.168.10.2/255.255.255.0).
 2. Set **Administrative Access** to allow **FortiTelemetry**, which is required so that FortiGate devices in the Security Fabric can communicate with each other.




Interface Name port10 (00:09:0F:09:19:03)

Alias Accounting

Link Status Up 

Type Physical Interface

Tags

Role  LAN 
 Add Tag Category

Address

Addressing mode **Manual** DHCP


IP/Network Mask 192.168.10.2/255.255.255.0


Administrative Access

IPv4 ☐ HTTPS ☐ HTTP  ☒ PING ☐ FMG-Access
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☒ FortiTelemetry
















☐ DHCP Server

Networked Devices

Device Detection 

Active Scanning 

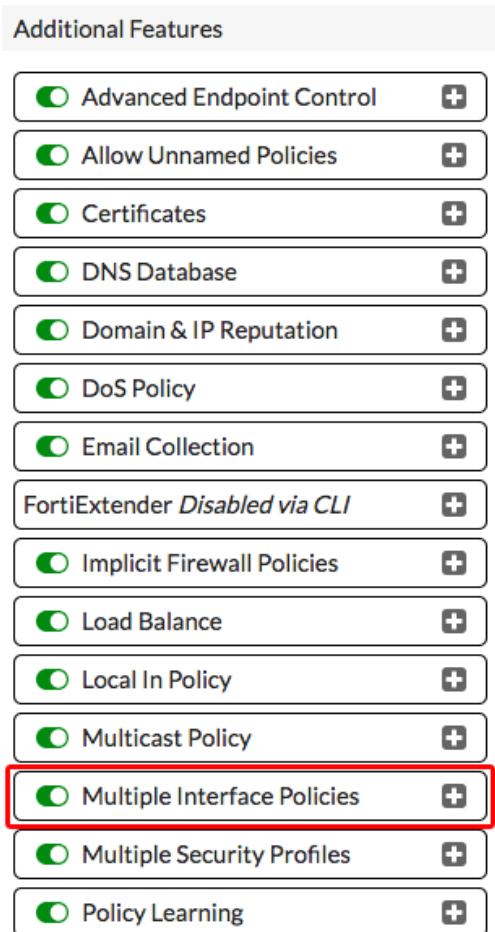
3. Repeat the previous steps to configure the other interfaces with the appropriate IP addresses, as listed above.
4. To create a policy for traffic from Accounting to the Internet, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
5. Set **Incoming Interface** to **port 10** and **Outgoing Interface** to **port 9**.
6. Enable **NAT**.

| | |
|--------------------|---|
| Name ⓘ | Accounting-Internet |
| Incoming Interface |  Accounting (port10)  + |
| Outgoing Interface |  Internet (port9)  + |
| Source |  all  + |
| Destination |  all  + |
| Schedule |  always  |
| Service |  ALL  + |
| Action |  ACCEPT  DENY  LEARN |









Firewall / Network Options

NAT ☒IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

7. Repeat the previous steps to create a similar policy for Marketing.
8. On Edge, go to **System > Feature Select**. Under **Additional Features**, enable **Multiple Interface Policies**.



9. To create a policy that allows Accounting and Marketing to access the FortiAnalyzer, go to **Policy & Objects > IPv4 Policy**.

| | | |
|--|--|---|
| Name  | Access-Resources | |
| Incoming Interface |  Accounting (port10) | ✕ |
| |  Marketing (port11) | ✕ |
| | + | |
| Outgoing Interface |  Network-Resources (port16) | ✕ |
| | | + |
| Source |  all | ✕ |
| | | + |
| Destination |  all | ✕ |
| | | + |
| Schedule |  always ▼ | |
| Service |  ALL | ✕ |
| | | + |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN | |

Firewall / Network Options

NAT ☒IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

10. To enable communication between the FortiGate devices in the Security Fabric, go to **Security Fabric > Settings** and enable **FortiGate Telemetry**. Set a **Group name** and **Group password** (the **Group password** option isn't available in FortiOS 6.0.3 and later).
11. **FortiAnalyzer Logging** is enabled by default. Set **IP address** to an internal address that will later be assigned to port 1 on the FortiAnalyzer (in the example, *192.168.65.10*). Set **Upload option** to **Real Time**.

☒ FortiGate Telemetry

Group name

Office-Security-Fabric


Group password


••••••••

Connect to upstream FortiGate

☐

FortiTelemetry enabled interfaces

 Accounting (port10)


 Marketing (port11)


+

×

×


☒ FortiAnalyzer Logging



FortiAnalyzer can also be installed on [Amazon Web Services \(AWS\)](#) . Please watch the setup [Video](#).

IP address

192.168.65.10



Test Connectivity


Upload option

Real Time

Every Minute

Every 5 Minutes



Encrypt log transmission

 ☒

12. Select **Test Connectivity**. An error appears because the FortiGate isn't yet authorized on the FortiAnalyzer. This authorization is configured in a later step.

Installing Accounting and Marketing

1. To edit **wan1** on **Accounting**, go to **Network > Interfaces**.
2. Set an **IP/Network Mask** for the interface that is on the same subnet as port 10 on Edge (in the example, *192.168.10.10/255.255.255.0*).
3. Under **Administrative Access**, select **HTTPS** and **SSH** to allow Edge to use this interface to manage the FortiGate.

| | | | |
|---|--|---------------|--|
| Interface Name | wan1 (70:4C:A5:28:05:52) | | |
| Alias | <input type="text"/> | | |
| Link Status | Up  | | |
| Type | Physical Interface | | |
| Estimated Bandwidth  | <input type="text" value="0"/> | Kbps Upstream | <input type="text" value="0"/> Kbps Downstream |

Tags

| | |
|--|----------------------------------|
| Role  | <input type="text" value="WAN"/> |
| <input type="button" value="+ Add Tag Category"/> | |

Address

| | |
|-----------------|---|
| Addressing mode | <input checked="" type="button" value="Manual"/> <input type="button" value="DHCP"/> <input type="button" value="PPPoE"/> |
| IP/Network Mask | <input type="text" value="192.168.10.10/255.255.255.0"/> |

Administrative Access

| | | | | |
|------|--|--|--|--|
| IPv4 | <input checked="" type="checkbox"/> HTTPS | <input checked="" type="checkbox"/> HTTP  | <input checked="" type="checkbox"/> PING | <input checked="" type="checkbox"/> FMG-Access |
| | <input type="checkbox"/> CAPWAP | <input checked="" type="checkbox"/> SSH | <input type="checkbox"/> SNMP | <input type="checkbox"/> FTM |
| | <input type="checkbox"/> RADIUS Accounting | <input type="checkbox"/> FortiTelemetry | | |

4. Edit the **lan** interface.
5. Set **Addressing mode** to **Manual** and set the **IP/Network Mask** to a private IP address (in the example, *10.10.10.1/255.255.255.0*).
6. Set **Administrative Access** to allow **FortiTelemetry**.
7. If you require the FortiGate to provide IP addresses using DHCP to devices that connect to this interface, enable **DHCP Server**.
8. Under **Networked Devices**, enable **Device Detection**.



It's a best practice to enable **Device Detection** on all interfaces classified as **LAN** or **DMZ**.

| | |
|-------------------|---|
| Interface Name | lan |
| Alias | <input type="text"/> |
| PoE Status | Up Not Connected |
| Type | Hardware Switch |
| Interface Members | <div><div>port1 ✕</div><div>port2 ✕</div><div>port3 ✕</div><div>port4 ✕</div><div>port5 ✕</div><div>port6 ✕</div><div>port7 ✕</div><div>port8 ✕</div><div>port9 ✕</div><div>port10 ✕</div><div>port11 ✕</div><div>port12 ✕</div><div>port13 ✕</div><div>port14 ✕</div><div>port15 ✕</div><div>port16 ✕</div><div>port17 ✕</div><div>+</div></div> |

Tags

Role

LAN

+ Add Tag Category

Address

Addressing mode

Manual DHCP PPPoE Dedicated to FortiSwitch

IP/Network Mask

10.10.10.1/255.255.255.0

Administrative Access

IPv4

☒ HTTPS

☒ HTTP

☒ PING

☒ FMG-Access

☒ CAPWAP

☐ SSH

☐ SNMP

☐ FTM

☐ RADIUS Accounting

☒ FortiTelemetry

DHCP Server

Address Range

+ Create New

Edit

Delete

| Starting IP | End IP |
|-------------|--------------|
| 10.10.10.2 | 10.10.10.254 |

Netmask

255.255.255.0

Default Gateway

Same as Interface IP Specify

DNS Server

Same as System DNS Same as Interface IP Specify

+ Advanced...

Networked Devices

Device Detection

9. To add a static route, go to **Network > Static Routes**. Set **Gateway** to the IP address of port 10 on Edge.

| | | |
|-------------------------|---|-----------------------------|
| Destination | <div>Subnet Named Address Internet Service</div> <input type="text" value="0.0.0.0/0.0.0.0"/> | |
| Gateway | <input type="text" value="192.168.10.2"/> | |
| Interface | wan1 | Detected via routing lookup |
| Administrative Distance | <input type="text" value="10"/> | |
| Comments | <input type="text"/> | 0/255 |
| Status | <div> Enabled Disabled </div> | |

10. To create a policy to allow users on the Accounting network to access Edge, go to **Policy & Objects > IPv4 Policy**.

| | |
|--------------------|---|
| Name | <input type="text" value="Internet"/> |
| Incoming Interface | lan |
| Outgoing Interface | wan1 |
| Source | <input type="text" value="all"/> <div>+</div> |
| Destination | <input type="text" value="all"/> <div>+</div> |
| Schedule | always |
| Service | <input type="text" value="ALL"/> <div>+</div> |
| Action | <div> ACCEPT DENY LEARN </div> |

Firewall / Network Options






NAT

IP Pool Configuration


Use Outgoing Interface Address | Use Dynamic IP Pool



- To add Accounting to the Security Fabric, go to **Security Fabric > Settings**. Enable **FortiGate Telemetry**, then enter the same **Group name** and **Group password** that you set previously on Edge (the **Group password** option isn't available in FortiOS 6.0.3 and later).
- Enable **Connect to upstream FortiGate** and enter the IP address of port 10 on Edge.
- FortiAnalyzer Logging** is enabled by default. Settings for the FortiAnalyzer are retrieved when Accounting connects to Edge.



FortiGate Telemetry

| | |
|---|--|
| Group name | <input type="text" value="Office-Security-Fabric"/> |
| Group password | <input type="password" value="••••••••"/> |
| Topology |  Accounting |
| Connect to upstream FortiGate |  |
| FortiGate IP | <input type="text" value="192.168.10.2"/> |
| Management IP  | Use WAN IP Specify |
| Status |  Connecting |
| FortiTelemetry enabled interfaces |  lan + × |

FortiAnalyzer Logging

 FortiAnalyzer settings will be retrieved from the root FortiGate in the Security Fabric.

 FortiAnalyzer can also be installed on [Amazon Web Services \(AWS\)](#) . Please watch the setup [Video](#).

| | | |
|--|---|--------------------------------|
| IP address | <input type="text"/> | Test Connectivity |
| Upload option | Real Time Every Minute Every 5 Minutes | |
| Encrypt log transmission  |  | |

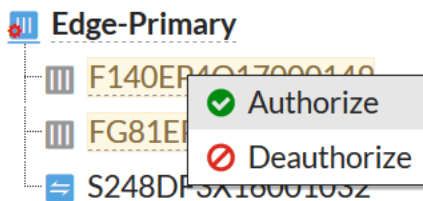
14. Connect WAN 1 on Accounting to port 10 on Edge.
15. Connect and configure Marketing, using the same method that you used to configure Accounting. Make sure you complete the following steps:
 - Configure WAN 1 to connect to Edge (IP address: 192.168.200.10/255.255.255.0) and allow HTTPS and SSH access.
 - Configure the LAN interface for the Marketing network (IP address: 10.10.200.2/255.255.255.0).
 - a. Create a static route pointing traffic to port 11 on Edge.
 - b. Create a policy to allow users on the Marketing network to access Edge.
 - c. Add Marketing to the Security Fabric.

16. If you're using FortiOS 6.0.3 and later, connect to Edge and go to **Security Fabric > Settings**. Authorize both Accounting and Marketing to join the Security Fabric.

Group name

Office-Security-Fabric

Topology



Installing Sales

1. To edit the interface on Marketing that connects to Sales (in the example, port12), go to **Network > Interfaces**.
2. Set an **IP/Network Mask** for the interface (in the example, 192.168.135.2/255.255.255.0).
3. Set **Administrative Access** to allow **FortiTelemetry**.

Interface Name port12 (90:6C:AC:D8:91:1D)

Alias

Link Status

Up

PoE Status

Up Not Connected

Type

Physical Interface

Tags

Role

LAN

Add Tag Category

Address

Addressing mode

Manual

DHCP

PPPoE

Dedicated to FortiSwitch

IP/Network Mask








192.168.135.2/255.255.255.0

Administrative Access

IPv4

☐ HTTPS☐ HTTP ☐ PING☐ FMG-Access☒ CAPWAP☐ SSH☐ SNMP☐ FTM☐ RADIUS Accounting☒ FortiTelemetry

4. To create a policy for traffic from Sales to Edge, go to **Policy & Objects > IPv4 Policy**.
5. Enable **NAT**.

| | |
|--|---|
| Name  | Sales-Internet |
| Incoming Interface |  port12 ▼ |
| Outgoing Interface |  wan1 ▼ |
| Source |  all ✕ + |
| Destination |  all ✕ + |
| Schedule |  always ▼ |
| Service |  ALL ✕ + |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

6. To edit wan2 on Sales, go to **Network > Interfaces**.
7. Set an **IP/Network Mask** for the interface that's on the same subnet as the internal 14 interface on Marketing (in the example, *192.168.135.10/255.255.255.0*).
8. Under **Administrative Access**, select **HTTPS** and **SSH**.

| | | | |
|---------------------|--------------------------------|---------------|--|
| Interface Name | wan2 (90:6C:AC:5B:CB:6A) | | |
| Alias | <input type="text"/> | | |
| Link Status | Up | | |
| Type | Physical Interface | | |
| Estimated Bandwidth | <input type="text" value="0"/> | Kbps Upstream | <input type="text" value="0"/> Kbps Downstream |

Tags

| | |
|---|----------------------------------|
| Role | <input type="text" value="WAN"/> |
| <input type="button" value="+ Add Tag Category"/> | |

Address

| | |
|-----------------|---|
| Addressing mode | <input checked="" type="button" value="Manual"/> <input type="button" value="DHCP"/> <input type="button" value="PPPoE"/> |
| IP/Network Mask | <input type="text" value="192.168.135.10/255.255.255.0"/> |

Administrative Access

| | | | | |
|------|--|--|--|--|
| IPv4 | <input checked="" type="checkbox"/> HTTPS | <input checked="" type="checkbox"/> HTTP | <input checked="" type="checkbox"/> PING | <input checked="" type="checkbox"/> FMG-Access |
| | <input type="checkbox"/> CAPWAP | <input checked="" type="checkbox"/> SSH | <input type="checkbox"/> SNMP | <input type="checkbox"/> FTM |
| | <input type="checkbox"/> RADIUS Accounting | | <input type="checkbox"/> FortiTelemetry | |

9. Edit the **lan** interface.
10. Set **Addressing Mode** to **Manual**, and set the **IP/Network Mask** to a private IP address (in the example, *10.10.135.1/255.255.255.0*).
11. Set **Administrative Access** to allow **FortiTelemetry**.
12. If you require the FortiGate to provide IP addresses, using DHCP, to devices that connect to this interface, enable **DHCP Server**.
13. Under **Networked Devices**, enable **Device Detection**.

Interface Name

Alias

Type **Hardware Switch**

Interface Members

lan1 ✕

lan2 ✕

lan3 ✕

lan4 ✕

lan5 ✕

+

Tags

Role LAN

+ Add Tag Category

Address

Addressing mode **Manual** DHCP PPPoE Dedicated to FortiSwitch

IP/Network Mask

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP ☒ PING ☒ FMG-Access
☒ CAPWAP ☒ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry

☒ DHCP Server

Address Range

| | | |
|---------------------------|---------------------|-----------------------|
| + Create New | ✎ Edit | 🗑 Delete |
| Starting IP | End IP | |
| 10.10.135.2 | 10.10.135.254 | |

Netmask

Default Gateway **Same as Interface IP** Specify

DNS Server **Same as System DNS** Same as Interface IP Specify

+ Advanced...

Networked Devices

Device Detection ☒

14. To add a default route, go to **Network > Static Routes** and select **Create New**. Set **Gateway** to the IP address of the internal 14 interface on Marketing.

| | |
|-------------------------|---|
| Destination | <div>Subnet Named Address Internet Service</div> <div>0.0.0.0/0.0.0.0</div> |
| Gateway | 192.168.135.2 |
| Interface | wan2 ▼ |
| Administrative Distance | 10 |
| Comments | <div></div> 0/255 |
| Status | <div> Enabled Disabled </div> |

15. To create a policy that allow users on the Sales network to access Marketing, go to **Policy & Objects > IPv4 Policy**.

| | |
|--------------------|---|
| Name | Internet |
| Incoming Interface | lan ▼ |
| Outgoing Interface | wan2 ▼ |
| Source | <div> all ✕</div> <div>+</div> |
| Destination | <div> all ✕</div> <div>+</div> |
| Schedule | always ▼ |
| Service | <div> ALL ✕</div> <div>+</div> |
| Action | <div> ACCEPT DENY LEARN </div> |

Firewall / Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address Use Dynamic IP Pool

16. To add Sales to the Security Fabric, go to **Security Fabric > Settings**. Enable **FortiGate Telemetry**, then enter the same **Group name** and **Group password** that you set previously..
17. Enable **Connect to upstream FortiGate** and enter the IP address of the internal 14 interface on Marketing.
18. **FortiAnalyzer Logging** is enabled by default. Settings for the FortiAnalyzer are retrieved when Sales connects to Edge.

☒ FortiGate Telemetry

Group name

Group password

Connect to upstream FortiGate ☒

FortiGate IP

Management IP [i](#) Use WAN IP Specify

FortiTelemetry enabled interfaces lan + ×

☒ FortiAnalyzer Logging

[i](#) FortiAnalyzer settings will be retrieved from the root FortiGate in the Security Fabric.

[i](#) FortiAnalyzer can also be installed on [Amazon Web Services \(AWS\)](#). Please watch the setup [Video](#).

IP address Test Connectivity

Upload option Real Time Every Minute Every 5 Minutes

Encrypt log transmission [i](#) ☒

19. Connect WAN 2 on Sales to internal 14 on Marketing.
20. If you're using FortiOS 6.0.3 and later, connect to Edge and go to **Security Fabric > Settings**. Authorize Sales to join the Security Fabric.

Group name

Topology

```

graph TD
    Edge-Primary[Edge-Primary] --- S248DF3X16001032[S248DF3X16001032]
    S248DF3X16001032 --- Accounting[Accounting]
    Accounting --- Marketing[Marketing]
    Marketing --- FGT51F2H146001055[FGT51F2H146001055]
  
```

Connect to upstream FortiGate ☐

FortiTelemetry enabled interfaces Accounting (not up) ×

✓ Authorize

✗ Deauthorize

Configuring the FortiAnalyzer

To use the FortiAnalyzer in the Security Fabric, make sure that the firmware is compatible with the version of FortiOS on the FortiGates. To check for compatibility, see the [FortiAnalyzer Release Notes](#).

1. To edit the port on FortiAnalyzer that connects to Edge (in the example, port4), go to **System Settings > Network** and select **All Interfaces**.

- Set **IP Address/Netmask** to the IP address that you use to configure the Security Fabric settings on Edge (192.168.65.10/255.255.255.0).
- Add a **Default Gateway**, using the IP address of port 16 on Edge.



The **Default Gateway** setting may not appear until you save the settings with the new IP address.

| | |
|----------------------------|---|
| Name | port4 |
| IP Address/Netmask | 192.168.65.10/255.255.255.0 |
| IPv6 Address | ::/0 |
| Administrative Access | <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service <input type="checkbox"/> FortiManager |
| IPv6 Administrative Access | <input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service <input type="checkbox"/> FortiManager |
| Default Gateway | 192.168.65.2 |
| Primary DNS Server | 208.91.112.53 |
| Secondary DNS Server | 208.91.112.63 |

- Go to **Device Manager**. The FortiGate devices are listed as **Unregistered**.

| <input type="checkbox"/> | Device Name | Model | Serial Number | Connecting IP |
|--------------------------|-------------|--------------------|------------------|---------------|
| <input type="checkbox"/> | Edge | FortiGate-600D | FGT6HD3916806070 | 192.168.65.2 |
| <input type="checkbox"/> | Accounting | FortiGate-140E-POE | F140EP4Q17000089 | 192.168.65.2 |
| <input type="checkbox"/> | Sales | FortiGate-51E | FGT51E3U16002482 | 192.168.65.2 |
| <input type="checkbox"/> | Marketing | FortiGate-81E-POE | FG81EP4Q16002749 | 192.168.65.2 |

- Select the FortiGate devices, then select **+Add**.

Add Device

| Device Name | Assign New Device Name |
|------------------|------------------------|
| FGT6HD3916806070 | Edge |
| F140EP4Q17000089 | Accounting |
| FGT51E3U16002482 | Sales |
| FG81EP4Q16002749 | Marketing |

OK
Cancel

- The FortiGate devices now appear as **Registered**.

4 Devices
Total

?

0 Devices
Unregistered

4 Devices
Log Status Down

56% Storage Used
Total 1000.0 MB

+ Add Device

Edit

Delete

More

Column Settings

Device Name

IP Address

Platform

Logs

Average Log Rate(Logs/Sec)

Device Storage

Description

Accounting

192.168.65.2

FortiGate-140E-POE

Real Time

N/A

(1.31%)

Edge

192.168.65.2

FortiGate-600D

Real Time

N/A

(37.56%)

Marketing

192.168.65.2

FortiGate-81E-POE

Real Time

N/A

(2.35%)

Sales

192.168.65.2

FortiGate-51E

Real Time

N/A

(2.24%)

- After a moment, a warning icon appears beside Edge because the FortiAnalyzer needs administrative access to the root FortiGate in the Security Fabric.



You may need to refresh the page before the icon appears.

8. Double-click on the FortiGate to enter the **Authentication** information.

Authentication

Please enter admin user name and password for the device.

| | | |
|------------|--|--|
| Admin User | <input type="text" value="admin"/> | |
| Password | <input type="password" value="....."/> | |

OK

Cancel

9. On Edge, go to **Security Fabric > Settings**. **FortiAnalyzer Logging** now shows **Storage usage** information.

☒ FortiAnalyzer Logging

FortiAnalyzer can also be installed on [Amazon Web Services \(AWS\)](#) . Please watch the setup [Video](#).

| | | |
|--------------------------|--|--|
| IP address | <input type="text" value="192.168.65.10"/> | <input type="button" value="Test Connectivity"/> |
| Logging to ADOM | root | |
| Storage usage | <div><div>68%</div></div> 678.23 MiB / 1000.00 MiB | |
| Analytics usage | <div><div>81%</div></div> 565.91 MiB / 700.00 MiB (Number of days stored: 60/60) | |
| Archive usage | <div><div>37%</div></div> 112.32 MiB / 300.00 MiB (Number of days stored: 365/365) | |
| Upload option | <input checked="" type="button" value="Real Time"/> <input type="button" value="Every Minute"/> <input type="button" value="Every 5 Minutes"/> | |
| Encrypt log transmission | <input checked="" type="checkbox"/> | |

Adding security profiles (optional)

The Security Fabric allows you to distribute security profiles to different FortiGates in your network, which can lessen the workload of each device and avoid creating bottlenecks. For example, you can implement antivirus scanning on Edge while the ISFW FortiGates apply application control and web filtering.

This results in distributed processing between the FortiGates in the Security Fabric, which reduces the load on each one. It also allows you to customize the web filtering and application control for the specific needs of the Accounting network since other internal networks may have different application control and web filtering requirements.

This configuration may result in threats getting through Edge, which means you should very closely limit access to the network connections between the FortiGates in the network.

1. To edit the policy that allows traffic from Accounting to the Internet, connect to Edge and go to **Policy & Objects > IPv4 Policy**.
2. Under **Security Profiles**, enable **AntiVirus** and select the **default** profile.
3. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.



Using the **deep-inspection** profile may cause certificate errors.

| Security Profiles | | | |
|---------------------|-------------------------------------|---------------------|--|
| AntiVirus | <input checked="" type="checkbox"/> | AV default | |
| Web Filter | <input type="checkbox"/> | | |
| DNS Filter | <input type="checkbox"/> | | |
| Application Control | <input type="checkbox"/> | | |
| IPS | <input type="checkbox"/> | | |
| Proxy Options | <input checked="" type="checkbox"/> | PRX default | |
| SSL Inspection | <input checked="" type="checkbox"/> | SSL deep-inspection | |

4. Do the same for the policy that allows traffic from Marketing to the Internet.
5. To edit the policy that allows traffic from the Accounting network to Edge, connect to Accounting and go to **Policy & Objects > IPv4 Policy**.
6. Under **Security Profiles**, enable **Web Filter** and **Application Control**. Select the **default** profile for both.
7. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.

| Security Profiles | | | |
|---------------------|-------------------------------------|---------------------|--|
| AntiVirus | <input type="checkbox"/> | | |
| Web Filter | <input checked="" type="checkbox"/> | WEB default | |
| DNS Filter | <input type="checkbox"/> | | |
| Application Control | <input checked="" type="checkbox"/> | APP default | |
| Proxy Options | <input type="checkbox"/> | PRX default | |
| SSL Inspection | <input type="checkbox"/> | SSL deep-inspection | |

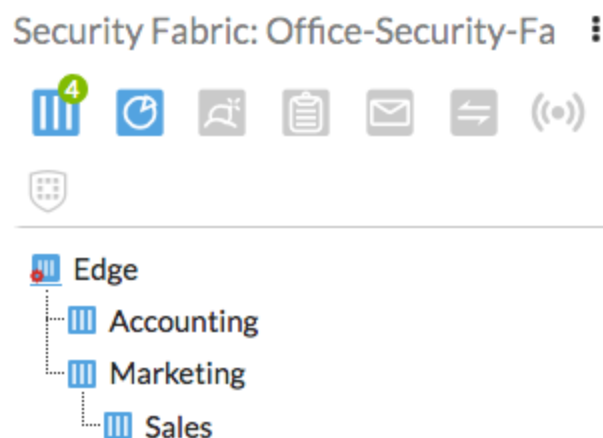
- Repeat this step for both Marketing and Sales.

Results

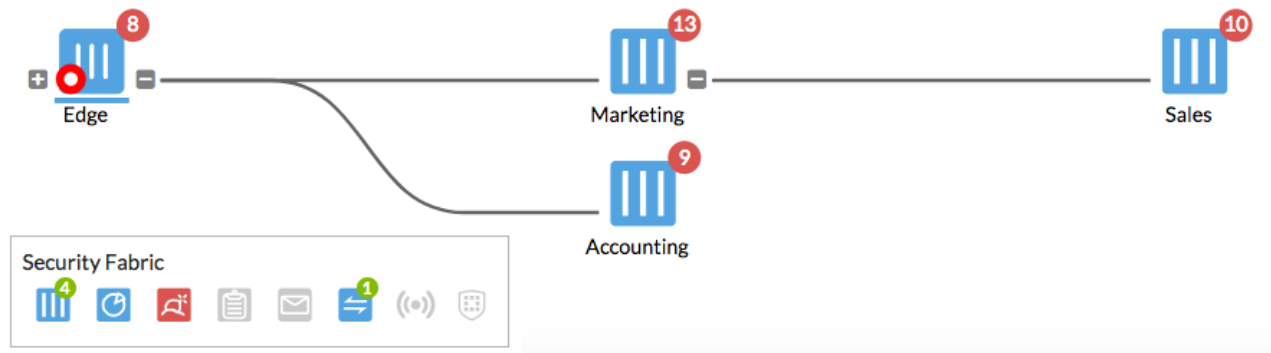
- On Edge, go to **Dashboard > Main**. The Security Fabric widget displays the names of the FortiGates in the Security Fabric.

The icons on the top of the widget indicate the other Fortinet devices that can be used in a Security Fabric. Devices in blue are detected in your network, devices in gray aren't detected in your network, and devices in red are also not detected in your network but are recommended for a Security Fabric.

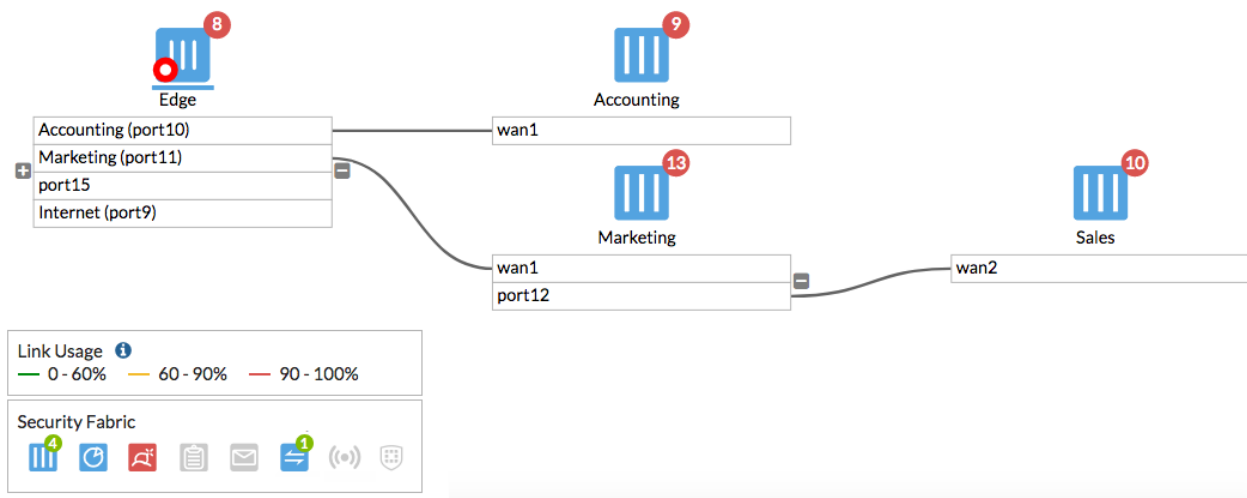
If either of this widgets doesn't appear on your dashboard, you can add them using the settings button in the bottom right corner.



- Go to **Security Fabric > Physical Topology**. This page shows a visualization of access layer devices in the Security Fabric.



- Go to **Security Fabric > Logical Topology**. This dashboard displays information about the interface (logical or physical) that each device in the Security Fabric connects.

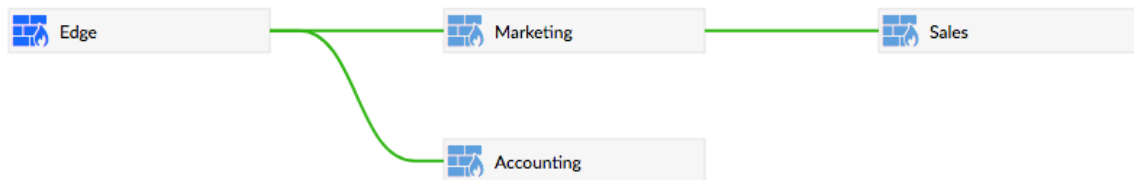


- On the FortiAnalyzer, go to **Device Manager**. The FortiGates are now shown as part of a Security Fabric group. The * beside Edge indicates that it's the root FortiGate in the Security Fabric.

| <input type="checkbox"/> | ▲ Device Name | IP Address | Platform | Logs | Average Log Rate(Logs/Sec) | Device Storage |
|--------------------------|--------------------------|--------------|--------------------|-------------|----------------------------|----------------|
| <input type="checkbox"/> | ✖ Office-Security-Fabric | | | | | |
| <input type="checkbox"/> | Accounting | 192.168.65.2 | FortiGate-140E-POE | ● Real Time | 0 | (1.34%) |
| <input type="checkbox"/> | Edge* | 192.168.65.2 | FortiGate-600D | ● Real Time | 0 | (47.73%) |
| <input type="checkbox"/> | Marketing | 192.168.65.2 | FortiGate-81E-POE | ● Real Time | 0 | (2.43%) |
| <input type="checkbox"/> | Sales | 192.168.65.2 | FortiGate-51E | ● Real Time | 0 | (2.31%) |

- Right-click on the Security Fabric group and select **Fabric Topology**. The topology of the Security Fabric is displayed.

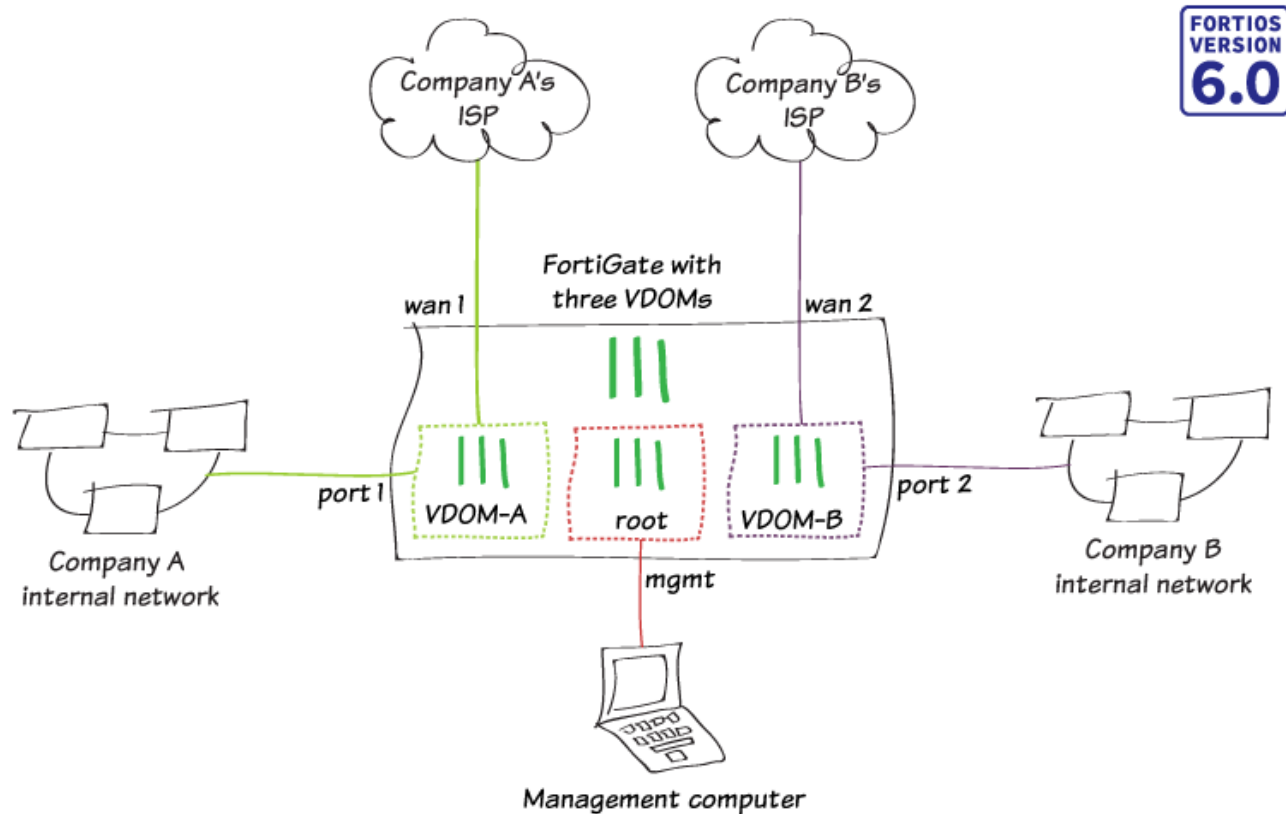
Topology for Office-Security-Fabric



Close

For further reading, check out [Configuring the Security Fabric](#) in the [FortiOS 6.0 Online Help](#).

VDOM configuration



In this recipe, you use virtual domains (VDOMs) to provide Internet access for two different companies (called Company A and Company B) using a single FortiGate.

Enabling and creating VDOMs

1. To enable VDOMs, go to **System > Settings**. Under **System Operation Settings**, enable **Virtual Domains**.
2. Select **OK** to confirm the VDOM mode change. When the change is applied, you are logged out of the FortiGate.

System Operation Settings

| | | |
|-----------------|-------------------------------------|--------------|
| Inspection Mode | Flow-based | Proxy |
| NGFW Mode | Profile-based | Policy-based |
| Virtual Domains | <input checked="" type="checkbox"/> | |

3. Log back in. To edit global settings, select **Global** from the dropdown menu located in the top-left corner.
4. To create a new VDOM, go to **System > VDOM** and select **Create New**. Enter a name (*VDOM-A*).

| | |
|-----------------|-------------------------------------|
| Virtual Domain | <input type="text" value="VDOM-A"/> |
| Inspection Mode | Flow-based Proxy |
| NGFW Mode | Profile-based Policy-based |
| Comments | <div></div> |

5. Create a second VDOM, called *VDOM-B*.

| | |
|-----------------|-------------------------------------|
| Virtual Domain | <input type="text" value="VDOM-B"/> |
| Inspection Mode | Flow-based Proxy |
| NGFW Mode | Profile-based Policy-based |
| Comments | <div></div> |

Configuring a management interface

By default, **root** is the management VDOM. You use the management VDOM to access the global settings for the FortiGate as well as the settings for each VDOM.

1. To configure an interface to connect to the management VDOM, go to **Global > Network > Interfaces** and edit an interface (in the example, **mgmt**).
2. Enable **Dedicated Management Port** and add the management computers as **Trusted Host**.

3. Set **Administrative Access** to **HTTPS**, **PING**, and **SSH**.

Interface Name mgmt (70:4C:A5:23:40:C1)

Alias

Link Status Up

Type Physical Interface

Virtual Domain root

Dedicated Management Port

Trusted Hosts

Tags

Role

Add Tag Category

Address

IP/Network Mask

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP ☒ PING ☒ FMG-Access

☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM

☐ RADIUS Accounting ☐ FortiTelemetry

Assigning interfaces

In this example, you assign two interfaces each to VDOM-A and VDOM-B: one for Internet access and one for use by the local network.

You can't change the VDOM assignment if an interface is used in an existing FortiGate configuration. You may need to delete existing policies and routes in order to add a particular interface, as some FortiGate models have default configurations.

1. To assign an interface that provides VDOM-A with Internet access, go to **Network > Interfaces** and edit an interface (in the example, **wan 1**).
2. Set **Virtual Domain** to **VDOM-A** and **Role** to **WAN**.
3. Check if your ISP provides an IP address for you to use or if the ISP equipment uses DHCP to assign IP addresses.
 - If your ISP provides an IP address, set **Addressing mode** to **Manual** and set the **IP/Network Mask** to that IP address.
 - If your ISP equipment uses DHCP, set **Addressing mode** to **DHCP** to allow the equipment to assign an IP address to WAN1.

| | | | |
|---------------------|--------------------------------|---------------|--|
| Interface Name | wan1 (70:4C:A5:23:40:C2) | | |
| Alias | <input type="text"/> | | |
| Link Status | Up | | |
| Type | Physical Interface | | |
| Virtual Domain | VDOM-A | | |
| Estimated Bandwidth | <input type="text" value="0"/> | kbps Upstream | <input type="text" value="0"/> kbps Downstream |

Tags

| | |
|------------------|----------------------------------|
| Role | <input type="text" value="WAN"/> |
| Add Tag Category | |

Address

| | |
|-----------------|--|
| Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE |
| IP/Network Mask | <input type="text" value="172.25.177.46/255.255.255.0"/> |

4. To assign an interface for the VDOM-A internal network, go to **Network > Interfaces** and edit the interface (in the example, **port 1**).
5. Set **Virtual Domain** to **VDOM-A** and **Role** to **LAN**.
6. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.46.1/255.255.255.0*), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**.
7. If you need to assign IP addresses to devices on your internal network, enable **DHCP Server**.

Interface Name port1 (None)

Alias

Link Status Up

Type Physical Interface

Virtual Domain VDOM-A

Tags

Role LAN

Add Tag Category

Address

Addressing mode **Manual** DHCP PPPoE One-Arm Sniffer Dedicated to FortiSwitch

IP/Network Mask

Administrative Access

IPv4 ☒ HTTPS ☒ HTTP ☐ PING ☐ FMG-Access
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry

DHCP Server

Address Range

Create New Edit Delete

| Starting IP | End IP |
|--------------|----------------|
| 192.168.46.2 | 192.168.46.254 |

Netmask

Default Gateway **Same as Interface IP** Specify

DNS Server **Same as System DNS** Same as Interface IP Specify

- Repeat the above steps to assign interfaces to VDOM-B.

Creating per-VDOM administrators

Per-VDOM administrator accounts only allow administrative access to specific VDOMs. By creating per-VDOM administrators, you allow both Company A and Company B to manage their respective VDOMs without allowing access to settings for other VDOMs or the global settings.

- To create a per-VDOM administrator for VDOM-A, go to **System > Administrators** and select **Create New > Administrator**.
- Enter a **Username** and set **Type** to **Local User**. Enter and confirm a **Password**. Set **Administrator Profile** to **prof_admin**.



You must use either the **prof_admin** or a custom profile for per-VDOM administrators.

3. Remove the **root** VDOM from the **Virtual Domains** list and add **VDOM-A**.

| | |
|-----------------------|---|
| Username | <input type="text" value="admin-a"/> |
| Type | <div>Local User</div> <div>Match a user on a remote server group</div> <div>Match all users in a remote server group</div> <div>Use public key infrastructure (PKI) group</div> |
| Password | <input type="password" value="••••••••"/> |
| Confirm Password | <input type="password" value="••••••••"/> |
| Comments | <input type="text" value="Write a comment..."/> 0/255 |
| Administrator Profile | <input type="text" value="prof_admin"/> ▼ |
| Virtual Domains | <div>VDOM-A</div> <div>+</div> <div>×</div> |
| Email Address | <input type="text"/> |








4. Repeat the above steps to create a per-VDOM administrator for VDOM-B.

Configuring the VDOMs

1. Access VDOM-A using the dropdown menu located in the top-left corner.
2. To add a static route, go to **Network > Static Routes** and select **Create New**.
3. Set **Destination** to **Subnet** and leave the destination IP address set to 0.0.0.0/0.0.0.0.
4. Set **Gateway** to the IP address provided by your ISP and **Interface** to the Internet-facing interface.

| | |
|---------------------------|--|
| Destination ⓘ | <div>Subnet</div> <div>Named Address</div> <div>Internet Service</div> |
| | <input type="text" value="0.0.0.0/0.0.0.0"/> |
| Gateway | <input type="text" value="172.25.177.1"/> |
| Interface | <div>wan1</div> <div>▼</div> |
| | Detected via routing lookup |
| Administrative Distance ⓘ | <input type="text" value="10"/> |
| Comments | <input type="text"/> 0/255 |
| Status | <div>↑ Enabled</div> <div>↓ Disabled</div> |

5. To create a new policy, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
6. Set the **Incoming Interface** to **port 1** and set the **Outgoing Interface** to **wan 1**.

| | | | |
|--|---|--|--|
| Name  | Internet-VDOM-A | | |
| Incoming Interface |  port1 ▼ | | |
| Outgoing Interface |  wan1 ▼ | | |
| Source |  all ✕ + | | |
| Destination |  all ✕ + | | |
| Schedule |  always ▼ | | |
| Service |  ALL ✕ + | | |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN | | |

Firewall / Network Options

NAT ☒

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

7. Repeat the above steps to configure VDOM-B.

Configuring global security profiles

You can create two types of security profiles for VDOMs: per-VDOM profiles that are only available to a specific VDOM, and global security profiles which are available for use by multiple VDOMs. You can use both types of profiles for your configuration.

Global profiles are available for the following security features:

- Antivirus
- Application control
- Data leak prevention
- Intrusion prevention
- Web filtering

Each security feature has at least one default global profile. Global profiles are identified by the “g-” at the beginning of the profile name.

Some security profile features, such as URL filters, are not available for use in a global profile.

1. To edit the default global web filter, go to **Global > Security Profiles > Web Filter** and edit **g-default**.
2. Right-click the **Bandwidth Consuming** category and select **Block**.

| | |
|-----------------|--|
| Name | <input type="text" value="g-default"/> |
| Comments | <input type="text" value="Default web filtering."/> 22/255 |
| Inspection Mode | Flow-based |

☒ FortiGuard category based filter

| | |
|---|--|
| Show <input type="radio"/> All | |
| <input checked="" type="checkbox"/> Local Categories | |
| <input type="checkbox"/> Potentially Liable | |
| <input type="checkbox"/> Adult/Mature Content | |
| <input type="checkbox"/> Bandwidth Consuming | |
| <input type="checkbox"/> Security Risk | |
| <input checked="" type="checkbox"/> General Interest - Personal | |
| <input checked="" type="checkbox"/> General Interest - Business | |
| <input type="checkbox"/> Unrated | |

Results

1. Connect to VDOM-A and log in using the VDOM-A administrator account. Only the per-VDOM options are shown.
2. To view the default global web filter, go to **Security Profiles > Web Filter** and select **g-default**. The VDOM-A administrator can't edit the profile.

Name


Comments 22/255

☒ FortiGuard category based filter


Show ☐ All

- ☐ Potentially Liable
- ☒ Adult/Mature Content
- ☒ Bandwidth Consuming
- ☒ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business
- ☒ Unrated

☐ Static URL Filter

URL Filter  ☐

Block malicious URLs discovered by FortiSandbox ☐

Web Content Filter  ☐

☐ Rating Options

Allow websites when a rating error occurs ☐

Rate URLs by domain and IP Address ☐

3. To view a summary of the VDOM configuration, connect to the management VDOM and go to **Global > System > VDOM**.

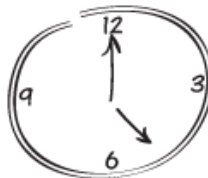
| Name | Operation Mode | Inspection Mode | NGFW Mode | Security Preset | Enable | CPU | Memory | Interfaces | Comments | Ref. |
|--------|----------------|-----------------|---------------|-----------------|-------------------------------------|--|---|---|----------|------|
| VDOM-A | NAT | Flow-based | Profile-based | Custom | <input checked="" type="checkbox"/> | <div><div></div></div> 0% | <div><div></div></div> 2% | port1 sslVDOM-A(SSL VPN interface) wan1 | | 5 |
| VDOM-B | NAT | Flow-based | Profile-based | Custom | <input checked="" type="checkbox"/> | <div><div></div></div> 0% | <div><div></div></div> 2% | port2 sslVDOM-B(SSL VPN interface) wan2 | | 4 |
| root | NAT | Flow-based | Profile-based | Custom | <input checked="" type="checkbox"/> | <div><div></div></div> 1% | <div><div></div></div> 16% | dmz ha1 ha2 mgmt modem npu0_vlink0 npu0_vlink1 port3 port4 port5 port6 port7 port8 port9 port10 port11 port12 port13 port14 port15 Display More (2 hidden, 22 total) | | 29 |
| | | | | | | Total Usage <div><div></div></div> 1% | Total Usage <div><div></div></div> 20% | | | |

For further reading, check out [Virtual domains overview](#) in the [FortiOS 6.0 Online Help](#).

FortiGate registration and basic settings



*Register your
FortiGate*



*Set the
system time*



*Configure the
admin account*

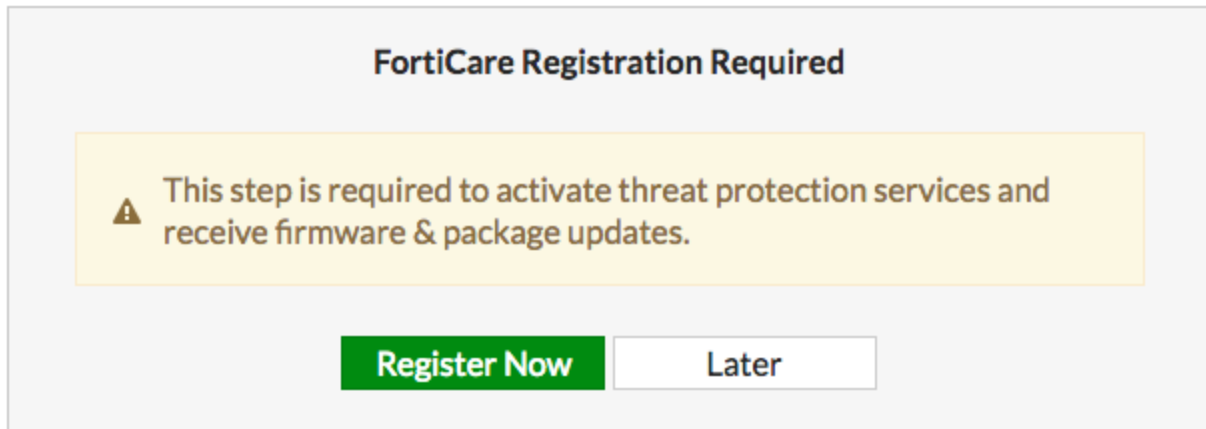
In this recipe, you will complete these following basic administrative tasks to get a newly installed FortiGate ready for use:

- Register your FortiGate with a Fortinet Support account.
- Set the system time.
- Create a new administrator and edit the default account.
- Restrict administrative access to a trusted host (optional).

Registering your FortiGate

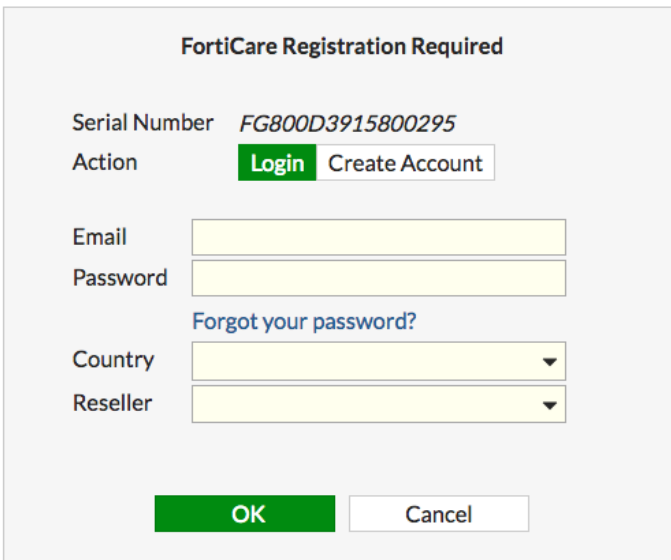
You must register your FortiGate to receive firmware upgrades, FortiGuard updates, and access to [Fortinet Support](#). Before you register your FortiGate, it must be connected to the Internet.

1. Connect to your FortiGate. A message appears that states that FortiCare registration is required. Select **Register Now**.



2. To allow Fortinet Support to keep a complete list of your devices, you should use one account to register all of your Fortinet products.

If you have a Fortinet Support account, set **Action** to **Login**.

A form titled "FortiCare Registration Required". It contains the following fields and options:

- Serial Number: *FG800D3915800295*
- Action: Two buttons, "Login" (green) and "Create Account" (white with a grey border).
- Email: A text input field.
- Password: A text input field.
- Forgot your password?: A blue link.
- Country: A dropdown menu.
- Reseller: A dropdown menu.
- At the bottom, there are two buttons: "OK" (green) and "Cancel" (white with a grey border).

If you need to create an account, set **Action** to **Create Account**.

FortiCare Registration Required

Serial Number *FG800D3915800295*

Action

About You

First Name

Last Name

Title

Sign-In

Email

Password

Confirm Password

Contact

Company

Phone Number

Fax Number

Address

Address

City

Postal / Zip Code

Country

State / Province

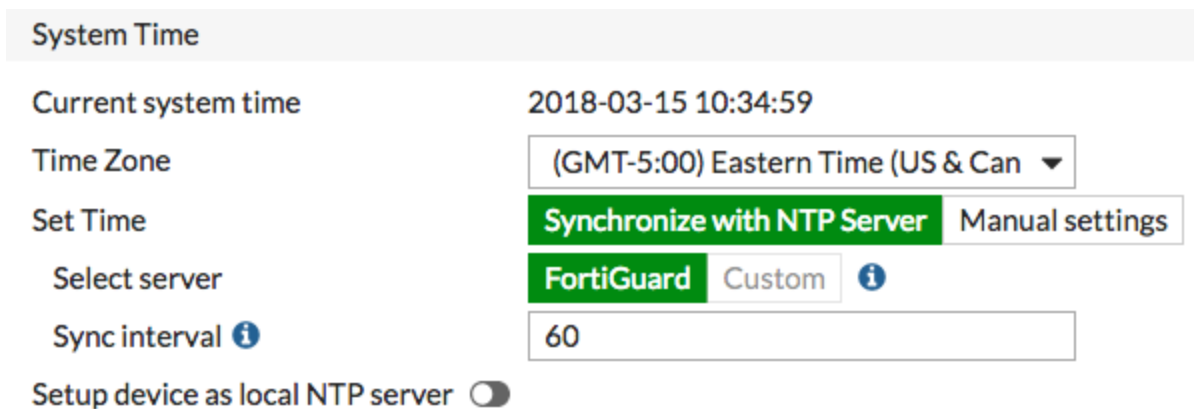
3. Go to **System > FortiGuard**. In **License Information**, **FortiCare Support** appears as **Registered**.

| Contract | Status |
|-------------------|--|
| FortiCare Support |  Registered - XXXXXXXXXX <input type="button" value="Launch Portal"/> |

4. Your other FortiGuard licenses now show as licensed. There may be a delay before all of them appear as licensed.

Setting system time

1. Go to **System > Settings**. Under **System Time**, select your **Time Zone** and either set the time manually or select **Synchronize with NTP Server**.



System Time

Current system time 2018-03-15 10:34:59

Time Zone (GMT-5:00) Eastern Time (US & Can ▼)

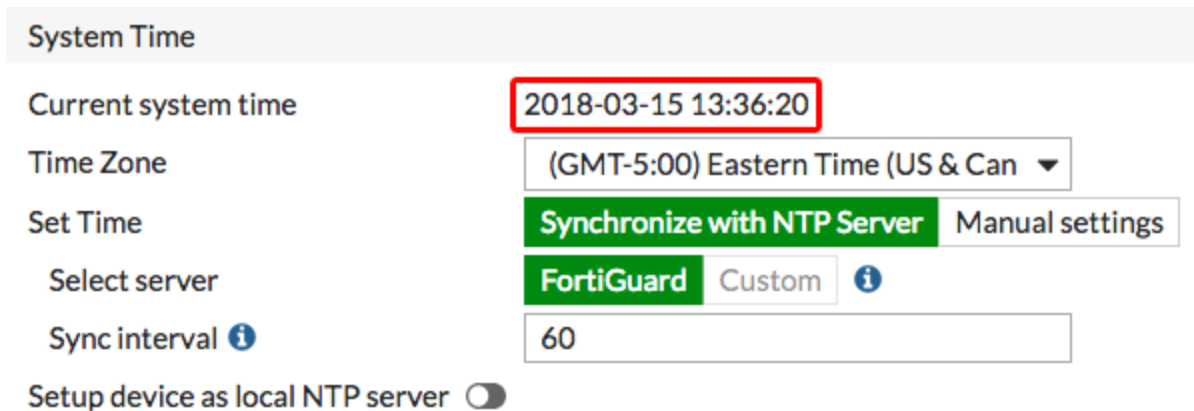
Set Time **Synchronize with NTP Server** Manual settings

Select server **FortiGuard** Custom ⓘ

Sync interval ⓘ 60

Setup device as local NTP server ☐

2. **Current system time** displays the correct time.



System Time

Current system time 2018-03-15 13:36:20

Time Zone (GMT-5:00) Eastern Time (US & Can ▼)

Set Time **Synchronize with NTP Server** Manual settings

Select server **FortiGuard** Custom ⓘ

Sync interval ⓘ 60


Setup device as local NTP server ☐

Creating administrators

1. Go to **System > Administrators** and create a new account. Set **User Name** and **Password**.
2. Set **Administrator Profile** to **super_admin**. This profile allows the administrator full access to configure the FortiGate.


| | |
|-----------------------|---|
| User Name | <input type="text" value="mwatney"/> |
| Type | <div>Local User Match a user on a remote server group Match all users in a remote server group Use public key infrastructure (PKI) group</div> |
| Password | <input type="password" value="••••••"/> |
| Confirm Password | <input type="password" value="••••••"/> |
| Comments | <input type="text" value="Write a comment..."/> 0/255 |
| Administrator Profile | <input type="text" value="super_admin"/> |
| Email Address | <input type="text"/> |

3. Log out of the FortiGate and log in using your new account.



Login

4. To secure your FortiGate, it's recommended that you change the name and password of the default admin account. Go to **System > Administrators** and edit the default account. Change the **User Name**.

| | | |
|-----------------------|---|--|
| User Name | <input type="text" value="rpurnell"/> |  Change Password |
| Type | <div>Local User Match a user on a remote server group Match all users in a remote server group Use public key infrastructure (PKI) group</div> | |
| Comments | <input type="text" value="Write a comment..."/> 0/255 | |
| Administrator Profile | <input type="text" value="super_admin"/> | |
| Email Address | <input type="text"/> | |



5. Select **Change Password** to add a password to this account.

| | |
|------------------|---|
| User Name | <input type="text" value="admin"/> |
| New Password | <input type="password" value="••••••••"/> |
| Confirm Password | <input type="password" value="••••••••"/> |

Using a trusted host (optional)

You can configure an administrative account to be accessible only to someone who is using a trusted host. You can set a specific IP address for the trusted host or use a subnet.

1. Go to **System > Administrators** and edit the default admin account.
2. Enable **Restrict login to trusted hosts**. Set **Trusted Host 1** to the static IP address of the computer you use to administer the FortiGate.
3. If required, set additional trusted hosts.


| | | |
|---|--|---|
| User Name  | <input type="text" value="admin"/> |  Change Password |
| Type | <div>Local User</div> <div>Match a user on a remote server group</div> <div>Match all users in a remote server group</div> <div>Use public key infrastructure (PKI) group</div> | |
| Comments | <input type="text" value="Write a comment..."/> 0/255 | |
| Email Address | <input type="text"/> | |

☐ SMS

☐ Two-factor Authentication

☒ Restrict login to trusted hosts

| | |
|----------------|--|
| Trusted Host 1 | <input type="text" value="192.168.13.2/32"/> |
| Trusted Host 2 | <input type="text"/> |
| Trusted Host 3 | <input type="text"/> |



Results

- 1. Attempt to log in using the original credentials for the default account. Access is denied.

Authentication failure. Please try again...

User Name

Password

Login

- 2. Log in using the new credentials for the default account. Access is granted.

rpurnell

●●●●●●●●

Login

- 3. Go to **Log & Report > System Events**. You can see the successful and failed login attempts in the events list.

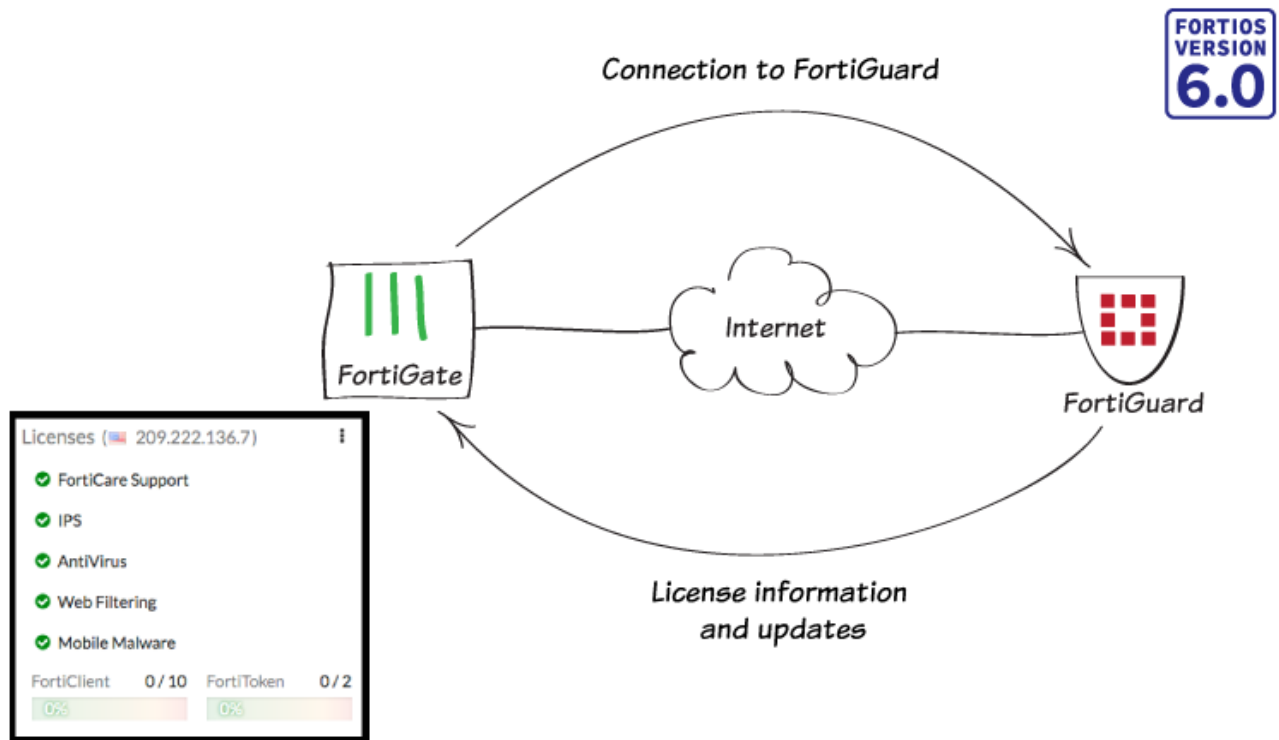


For system events to appear in the GUI, you must configure disk logging in the log settings on the FortiGate. This option is only available on FortiGate models that have an internal hard drive.

| # | Date/Time | Level | User | Message |
|---------|-----------|-------------|----------|---|
| Refresh | | | | |
| 1 | 14:54:41 | <div></div> | rpurnell | Administrator rpurnell logged in successfully from https(172.25.177.46) |
| 2 | 14:54:33 | <div></div> | admin | Administrator admin login failed from https(172.25.177.46) because of invalid user name |

For further reading, check out [Basic Administration](#) in the [FortiOS 6.0 Online Help](#).

Verifying FortiGuard licenses and troubleshooting



In this recipe, you verify that your FortiGate displays the correct FortiGuard licenses and troubleshoot any errors. You must [register your FortiGate](#) before it can show your FortiGuard licenses.

Viewing your licenses

1. To view your licenses, go to the **Dashboard** and find the **Licenses** widget. The FortiGuard licenses are listed, with their status indicated:
 - A green check mark indicates an active license.
 - A gray question mark indicates an unavailable license.
 - A license highlighted in orange is either unlicensed or expires soon.
 - A license highlighted in red is expired.

Licenses



✓ FortiCare Support

✓ IPS

❗ AntiVirus

? Web Filtering

? Mobile Malware



2. The widget only displays licenses for features you enabled in feature visibility. To enable more features, go to **System > Feature Visibility**.
3. The **Web Filtering** license only appears as active when a web filter profile is applied to a firewall policy.



When you apply the profile, a warning will appear stating that web filtering doesn't have a valid license. You can ignore this for the moment.

-
4. You can also view FortiGuard license information by going to **System > FortiGuard**.

License Information

| Contract | Status | |
|--------------------------------|---|------------------------------------|
| FortiCare Support | ✓ Registered | Launch Portal |
| Hardware Version | ✓ Advanced hardware - expires on 2019/03/17 | |
| Firmware | ✓ Web/online - expires on 2019/03/17 | |
| Enhanced Support | ✓ 24x7 support - expires on 2019/03/17 | |
| Comprehensive Support | ✓ 24x7 support - expires on 2019/03/17 | |
| Application Control Signatures | ⊙ Version 6.00741 | + Upgrade Database |
| IPS | ✓ Licensed - expires on 2019/03/17 | + Upgrade Database |
| IPS Definitions | ⊙ Version 6.00741 | |
| IPS Engine | ⊙ Version 3.00510 | |
| Malicious URLs | ⊙ Version 1.00930 | |
| AntiVirus | ❗ Expired - expired on 2017/07/27 | + Upgrade Database |
| AV Definitions | ⊙ Version 1.00000 | View List |
| AV Engine | ⊙ Version 5.00350 | |
| Botnet IPs | ⊙ Version 3.00300 | |
| Botnet Domains | ⊙ Version 1.00946 | |
| Mobile Malware | ❓ Unavailable | |
| Mobile Malware Definitions | ⊙ Version 56.00524 | |
| Web Filtering | ❓ Unavailable | |
| FortiClient | ✓ Free License | 0% 0 / 10 |

Troubleshooting

If you need to add or renew a subscription, go to [Fortinet Support](#).

If a license that should be active isn't currently available, you can use the following steps to troubleshoot your connection. After each troubleshooting step, go to **System > FortiGuard** to check if the licenses are now showing as available.

Connecting to FortiGuard

1. To prompt your FortiGate to connect to FortiGuard, connect to the CLI and use the following command:

```
diagnose debug application update -1
diagnose debug enable
execute update-now
```
2. If your FortiGate has multiple VDOMs, make sure that you use the management VDOM and that the VDOM has Internet access. To set the proper VDOM as the management VDOM, use the following command:

```
config system global
    set management-vdom
end
```

Checking FortiGuard filtering

1. To test if FortiGuard is reachable, go to **System > FortiGuard**.
2. Under **Filtering**, check **Filtering Services Availability**. If you don't see a green check mark, select **Check Again**.
3. If you still don't see a green check mark, change the **FortiGuard Filtering Port** to the alternate port (8888). Select **Apply** and see if the services become available.



If you're updating FortiGuard using a FortiManager, the **FortiGuard Filtering Port** can also be 80.

Filtering

Web Filter Cache ☒

Clear cache after Minutes

Clear Web Filter Cache

Anti-Spam Cache ☒

Clear cache after Minutes

FortiGuard Filtering Port

Filtering Services Availability ☒

Available Check Again

Request re-evaluation of a URL's category

Testing the DNS

1. To test if your DNS can reach FortiGuard, use the following CLI command:

```
execute ping guard.fortinet.net
```
2. If you can reach the address, run the following command:

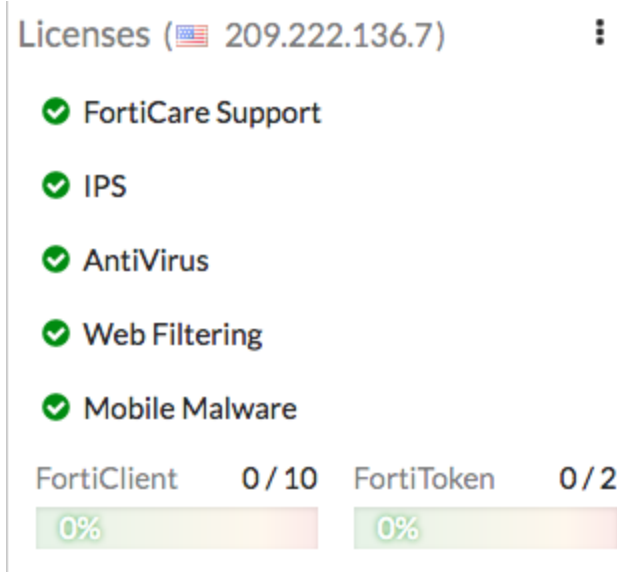
```
diagnose debug application update -1
diagnose debug enable
execute update-now
```
3. If you can't reach the address, go to **System > DNS** and verify that the settings are correct. Then run the PING test again.

Contacting Support

If you still can't connect, contact [Fortinet Support](#).

Results

1. Go to the **Dashboard** and view the **Licenses** widget. Any subscribed services should have a green check mark beside it.



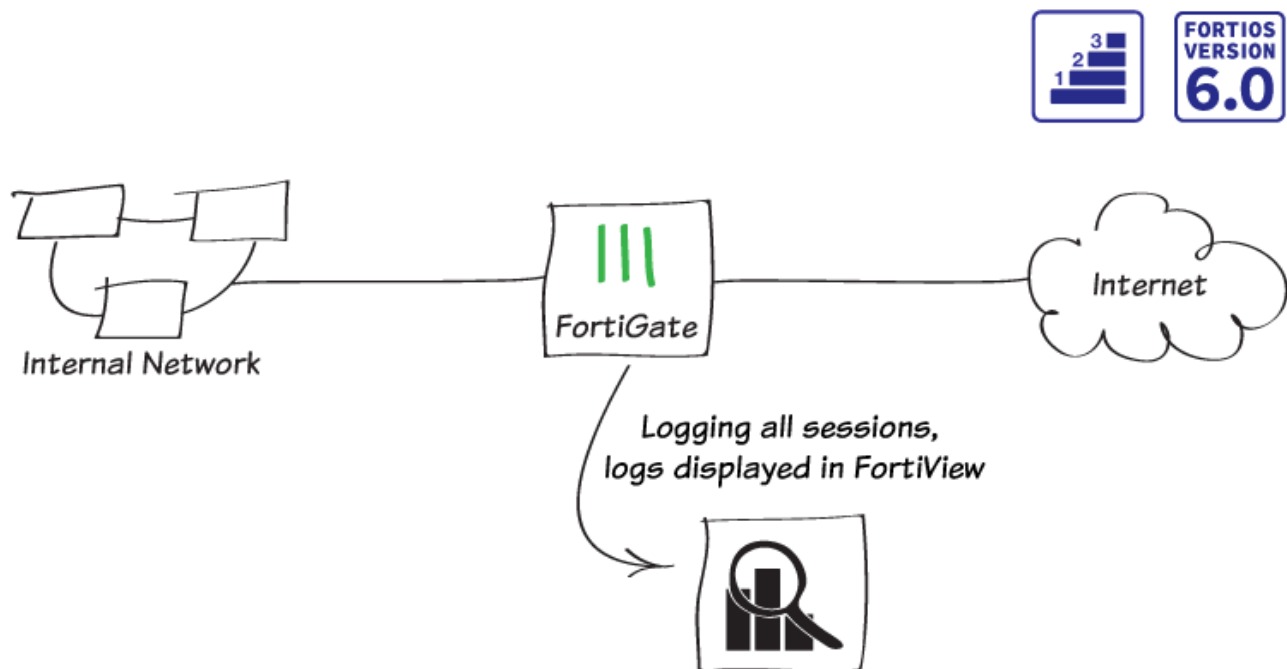
2. Go to **System > FortiGuard**. Features and services you're subscribed to should have a green check mark beside

them.

| License Information | | |
|--------------------------------|---|--|
| Contract | Status | |
| FortiCare Support | ✓ Registered | Launch Portal |
| Hardware Version | ✓ Advanced hardware - expires on 2019/03/17 | |
| Firmware | ✓ Web/online - expires on 2019/03/17 | |
| Enhanced Support | ✓ 24x7 support - expires on 2019/03/17 | |
| Comprehensive Support | ✓ 24x7 support - expires on 2019/03/17 | |
| Application Control Signatures | ⦿ Version 6.00741 | Upgrade Database |
| IPS | ✓ Licensed - expires on 2019/03/17 | Upgrade Database |
| IPS Definitions | ⦿ Version 6.00741 | |
| IPS Engine | ⦿ Version 3.00510 | |
| Malicious URLs | ⦿ Version 1.00930 | |
| AntiVirus | ✓ Licensed - expires on 2019/03/17 | Upgrade Database |
| AV Definitions | ⦿ Version 1.00000 | View List View List |
| AV Engine | ⦿ Version 5.00350 | |
| Botnet IPs | ⦿ Version 3.00300 | |
| Botnet Domains | ⦿ Version 1.00946 | |
| Mobile Malware | ✓ Licensed | |
| Mobile Malware Definitions | ⦿ Version 56.00524 | |
| Web Filtering | ✓ Licensed - expires on 2019/03/17 | <div>0% <div></div></div> 0 / 10 |
| FortiClient | ✓ Free License | |

For further reading, check out [FortiGuard](#) in the [FortiOS 6.0 Handbook](#).

Logging FortiGate traffic and using FortiView



In this example, you will configure logging to record information about sessions processed by your FortiGate. You will then use FortiView to look at the traffic logs and see how your network is being used.

FortiView is a logging tool that contains dashboards that show real time and historical logs. You can filter the dashboards to show specific results and also drill down for more information about a particular session. Each dashboard focuses on a different aspect of your network traffic, such as traffic sources of WiFi clients.

Some FortiView dashboards, such as applications and web sites, require you to apply security profiles to traffic before you can view results.

Configuring log settings

1. To configure log settings, go to **Log & Report > Log Settings**.
2. Select where you want to record log messages. This example uses **Local Log**, because it is required by FortiView. You can also use **Remote Logging and Archiving** to send logs to either a FortiAnalyzer/FortiManager, FortiCloud, or a syslog server.
3. Enable **Disk**, **Local Reports**, and **Historical FortiView**.

Local Log

- Disk ☒
- Enable Local Reports ☒
- Enable Historical FortiView ☒

- Under **Log Settings**, set both **Event Logging** and **Local Traffic Log** to **All**.

Log Settings

- Event Logging **All** [Customize](#)
- Local Traffic Log **All** [Customize](#)

Enabling logging

Because logging all sessions uses more system resources, it is typically recommended to log only security events. However, for the purpose of this recipe, all sessions will be logged to ensure that logging has been configured correctly.

- To edit the Internet policy, go to **Policy & Objects > IPv4 Policy**.
- Under **Logging Options**, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options

- Log Allowed Traffic ☒ [Security Events](#) **All Sessions**
- Capture Packets ☐

Results

- Browse the Internet to generate traffic through the FortiGate.
- To view a realtime display of all active sessions, go to **FortiView > All Segments > All Sessions**.

| Source | Source Device | Source Interface | Destination | Destination Device | Destination Interface | Application | Bytes (Sent/Received) | Policy |
|--------------|---------------|------------------|---------------|--------------------|-----------------------|-------------|-----------------------|------------------------------|
| 192.168.65.2 | AdminPC | lan | 172.217.6.227 | | wan1 | TCP/443 | 166.03 kB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 172.217.10.2 | | wan1 | TCP/443 | 6.98 kB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 432 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 8.253.151.248 | | wan1 | TCP/80 | 73.28 kB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 8.253.151.248 | | wan1 | TCP/80 | 1.31 MB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 249 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 408 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 197 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.53 | | wan1 | UDP/53 | 410 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 410 B | Internet (1) |

- If you right-click a session in the list, you can choose to end the session, end all sessions, ban the source IP, or filter logs by the source device.

4. Select the **24 hours view**. You can see a historical view of your traffic. To see more information, doubleclick a session.



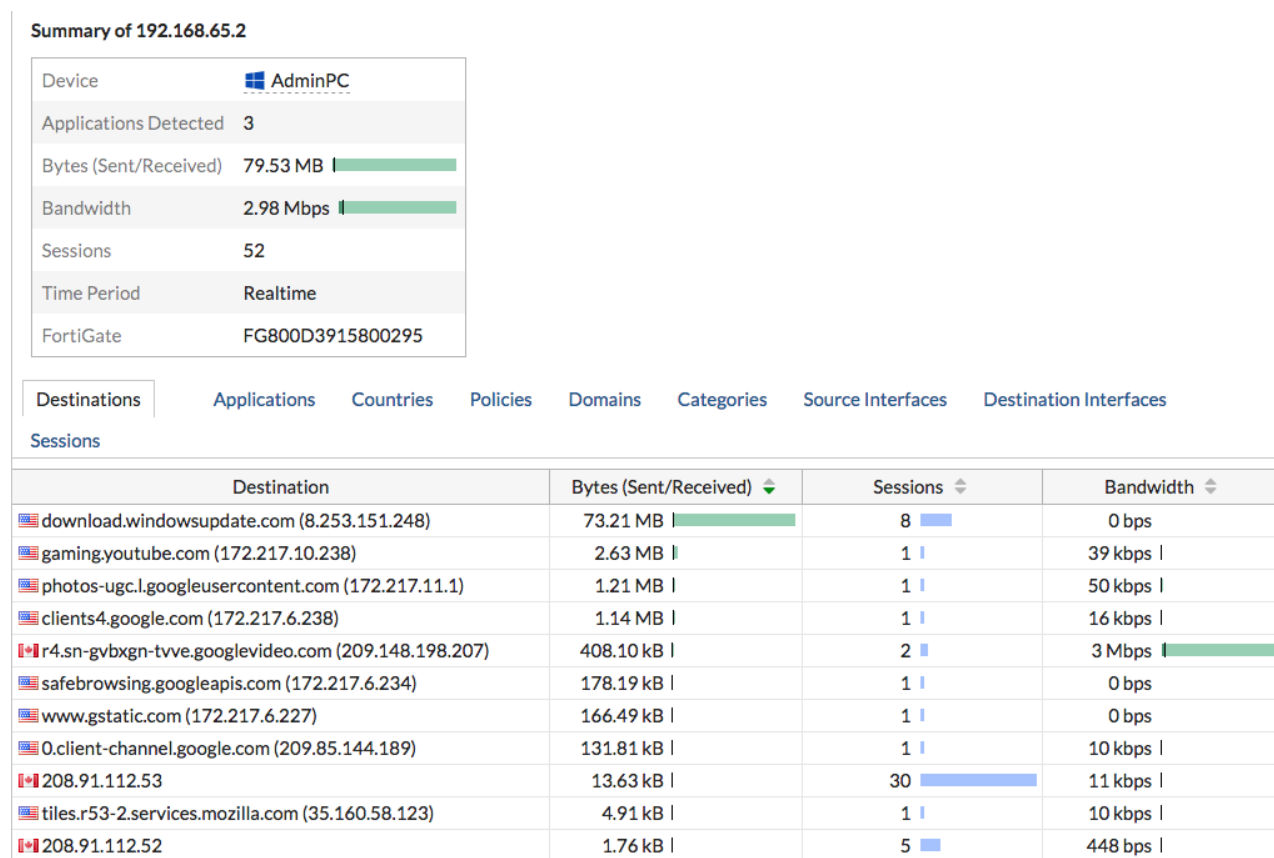
Historical views are only available on FortiGate models with internal hard drives.

| # | Date/Time | Source | Destination | Application Name | Secu | Log Details |
|----|-----------|---------|---|------------------|------|--|
| 1 | 07:58:27 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | General Date 02/09/2018 Time 07:58:27 Duration 5s Session ID 252603 Virtual Domain root NAT Translation Source Source IP 192.168.65.2 NAT IP 172.25.176.62 Source Port 57308 Country Reserved Primary MAC 24:b6:fd:40:0c:81 Source Interface lan Device Type Windows PC Destination IP 209.148.198.207 Host Name r4.sn-gvbxgn-tvve.googlevideo.com Port 443 Country Canada Destination Interface wan1 |
| 2 | 07:58:27 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 3 | 07:58:21 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 4 | 07:58:21 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 5 | 07:58:17 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 6 | 07:58:17 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 7 | 07:58:11 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 8 | 07:58:11 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 9 | 07:58:07 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 10 | 07:58:06 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 11 | 07:58:01 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 12 | 07:58:01 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 13 | 07:57:57 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 14 | 07:57:56 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 15 | 07:57:56 | AdminPC | 54.148.143.136 (tiles.r53-2.services.mozilla.com) | HTTPS | | |
| 16 | 07:57:55 | AdminPC | 54.148.143.136 (tiles.r53-2.services.mozilla.com) | HTTPS | | |
| 17 | 07:57:53 | AdminPC | 54.148.143.136 (tiles.r53-2.services.mozilla.com) | HTTPS | | |
| 18 | 07:57:51 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 19 | 07:57:51 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | | |
| 20 | 07:57:48 | AdminPC | 35.165.158.113 (shavar.prod.mozaws.net) | HTTPS | | |

5. To view a list of the sources in your network traffic, go to **FortiView > Traffic from LAN/DMZ > Sources**.

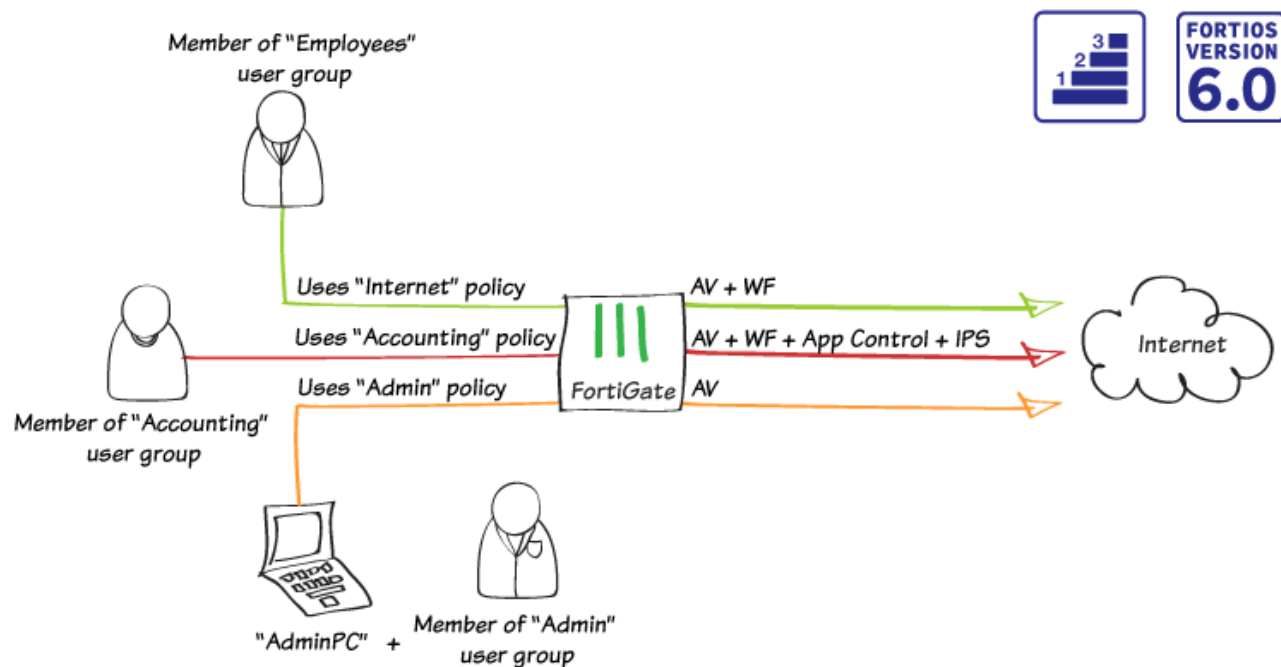
| Source | Source Device | Bytes (Sent/Received) | Sessions | Bandwidth |
|--------------|---------------|-----------------------|----------|-----------|
| 192.168.65.2 | AdminPC | 79.95 MB | 79 | 4 Mbps |

6. Right-click on any source listed and select Drill Down to Details. You can view a variety of information about the source address, including traffic destinations, security policies used, and if any threats are linked to traffic from this address.



For further reading, check out [FortiView](#) in the [FortiOS 6.0 Online Help](#).

Creating security policies for different users



In this recipe, you will create multiple security policies, which will apply security inspection to different users based on which user group they belong to.

This example contains three IPv4 policies:

- *Internet*: The policy that the *Employee* user group uses to access the Internet. You use the FortiGate to apply some security inspection to traffic.
- *Accounting*: The policy that the *Accounting* user group uses to access the Internet. You use the FortiGate to apply increased security inspection to protect sensitive information.
- *Admin*: The policy that the *Admin* user group uses, connecting from a specific computer, to access the Internet. You use the FortiGate to apply limited security inspection.



For information about creating the Internet policy, see [Installing a FortiGate in NAT mode on page 10](#).

Creating the Employee user and policy

1. To create a new user, go to **User & Device > User Definition** (in the example, this account is called *jpearson*).
2. In the **User Type** section, select **Local User**.

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

3. In the **Login Credentials** section, set **Username** and set a **Password**.

✓ User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Username

Password

4. In the **Contact info** section, set the user's **Email Address**.

✓ User Type > ✓ Login Credentials > 3 Contact Info > 4 Extra Info

Email Address

☐ SMS

☐ Two-factor Authentication

5. In the **Extra Info** section, verify that **User Account Status** is **Enabled**.

✓ User Type > ✓ Login Credentials > ✓ Contact Info > 4 Extra Info

User Account Status ⬆ Enabled ⬇ Disabled

User Group ☐

6. Your FortiGate now lists the new user.

| ⌵ User Name ⌵ | ⌵ Type ⌵ | ⌵ Two-factor Authentication ⌵ | ⌵ Ref. ⌵ |
|---------------|----------|-------------------------------|----------|
| guest | 👤 LOCAL | ✖ | 1 |
| jpearson | 👤 LOCAL | ✖ | 0 |

7. To create a new user group, go to **User & Device > User Groups** (in the example, this group is called *Employees*). Add user **jpearson** to the **Members** list.

| | |
|---------|--------------------------------|
| Name | Employees |
| Type | Firewall |
| | Fortinet Single Sign-On (FSSO) |
| | RADIUS Single-Sign-On (RSSO) |
| | Guest |
| Members | jpearson |
| | + |

8. The FortiGate now lists the new user group.

| Group Name | Group Type | Members | Ref. |
|-----------------------------|--------------------------------|----------|------|
| Employees (1 Members) | Firewall | jpearson | 0 |
| Guest-group (1 Members) | Firewall | guest | 0 |
| SSO_Guest_Users (0 Members) | Fortinet Single Sign-On (FSSO) | | 1 |

9. To edit the Internet policy, go to **Policy & Objects > IPv4 Policy**.
10. For **Source**, set **Address** to **all** and **User** to the **Employees** group.
11. Under **Security Profiles**, enable **AntiVirus** and **Web Filter**. Set both to use the default profile.
12. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.



Using the **deep-inspection** profile may cause certificate errors.

Name ⓘ Internet
 Incoming Interface ↕ lan
 Outgoing Interface 🏠 wan1
 Source
 all
 Employees
 +
 Destination
 all
 +
 Schedule always
 Service ALL
 +
 Action
 ✓ ACCEPT ✗ DENY 📖 LEARN

Firewall / Network Options

NAT ☒

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Security Profiles

AntiVirus ☒ AV default
 Web Filter ☒ WEB default
 DNS Filter ☐
 Application Control ☐
 IPS ☐
 Proxy Options ☒ PRX default
 SSL Inspection ⚠ ☒ SSL deep-inspection

Creating the Accounting user and policy

1. To create another user, go to **User & Device > User Definition** and select **Create New** (in the example, *akeating*).

| 🔽 User Name 🔼 | 🔽 Type 🔼 | 🔽 Two-factor Authentication 🔼 | 🔽 Ref. 🔼 |
|---------------|----------|-------------------------------|----------|
| akeating | 👤 LOCAL | ✗ | 0 |
| guest | 👤 LOCAL | ✗ | 1 |
| jpearson | 👤 LOCAL | ✗ | 2 |

2. To create another user group, go to **User & Device > User Groups** and select **Create New** (in the example, *Accounting*). Add user **akeating** to the **Members** list.

| 🔽 Group Name 🔼 | 🔽 Group Type 🔼 | 🔽 Members 🔼 | 🔽 Ref. 🔼 |
|-----------------------------|----------------------------------|-------------|----------|
| Accounting (1 Members) | 🏠 Firewall | 👤 akeating | 0 |
| Employees (1 Members) | 🏠 Firewall | 👤 jpearson | 1 |
| Guest-group (1 Members) | 🏠 Firewall | 👤 guest | 0 |
| SSO_Guest_Users (0 Members) | 🔑 Fortinet Single Sign-On (FSSO) | | 1 |

3. To create a new *Accounting* policy, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
4. For **Source**, set **Address** to **all** and **User** to the **Accounting** group.

- Under **Security Profiles**, enable **AntiVirus**, **Web Filter**, **Application Control**, and **IPS**. Set all of these to use the **default** profile.
- SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.

Name ⓘ Accounting
 Incoming Interface ↕ lan
 Outgoing Interface 📶 wan1
 Source
 all
 Accounting
 +
 Destination
 all
 +
 Schedule ⌚ always
 Service 🖨 ALL
 +
 Action
 ✓ ACCEPT ✗ DENY 🎓 LEARN

Firewall / Network Options

NAT ☒

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Security Profiles

AntiVirus ☒ AV default
 Web Filter ☒ WEB default
 DNS Filter ☐
 Application Control ☒ APP default
 IPS ☐
 Proxy Options ☒ PRX default
 SSL Inspection ⚠ ☒ SSL deep-inspection

Creating the Admin user, device, and policy

- To create another user, go to **User & Device > User Definition** and select **Create New** (in the example, *tal-jamil*).

| ⌵ User Name ⌵ | ⌵ Type ⌵ | ⌵ Two-factor Authentication ⌵ | ⌵ Ref. ⌵ |
|---------------|----------|-------------------------------|----------|
| akeating | 👤 LOCAL | ✗ | 1 |
| guest | 👤 LOCAL | ✗ | 1 |
| jpearson | 👤 LOCAL | ✗ | 1 |
| tal-jamil | 👤 LOCAL | ✗ | 0 |

- To create another user group, go to **User & Device > User Groups** and select **Create New** (in the example, *Admin*). Add user **tal-jamil** to the Members list.

| Group Name | Group Type | Members | Ref. |
|-----------------------------|--------------------------------|-----------|------|
| Accounting (1 Members) | Firewall | akeating | 1 |
| Admin (1 Members) | Firewall | tal-jamil | 0 |
| Employees (1 Members) | Firewall | jpearson | 1 |
| Guest-group (1 Members) | Firewall | guest | 0 |
| SSO_Guest_Users (0 Members) | Fortinet Single Sign-On (FSSO) | | 1 |

- To add a new device, go to **User & Device > Custom Devices & Groups** and select **Create New**.
- Set **Alias** to *AdminPC* and enter the **MAC Address** of the PC. Select the appropriate **Device Type**.

| | |
|-----------------|--|
| Alias | AdminPC |
| MAC Address | 24:b6:fd:40:0c:81 |
| Additional MACs | + |
| Device Type | Windows PC |
| Custom Groups | + |
| Avatar | <input type="button" value="Upload Image"/> <input type="button" value="Capture Image"/> |
| Comments | 0/255 |

- The PC is now listed under **Custom Devices**.

| Custom Devices (1) | | |
|------------------------------|---|------------------------------------|
| AdminPC | 192.168.65.2 | |
| Custom Device Groups (3) | | |
| Mobile Devices 8 Members | Android Phone Android Tablet BlackBerry Phone BlackBerry PlayBook iPad iPhone Windows Phone Windows Tablet | Phones, tablets, etc. |
| Network Devices 3 Members | Fortinet Device Other Network Device Router/NAT Device | Routers, firewalls, gateways, e... |
| Others 2 Members | Gaming Console Media Streaming | Other devices. |

- To create a new *Admin* policy, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
- For **Source**, set **Address** to **all**, **User** to the **Admin** group, and **Device** to the **AdminPC**.
- Under **Security Profiles**, enable **AntiVirus** and set it to use the **default** profile.
- SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.

| | |
|--------------------|---|
| Name | Admin |
| Incoming Interface | lan |
| Outgoing Interface | wan1 |
| Source | <div>all</div> <div>Admin</div> <div>AdminPC</div> <div>+</div> |
| Destination | <div>all</div> <div>+</div> |
| Schedule | always |
| Service | ALL |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Security Profiles

| | | | |
|---------------------|-------------------------------------|---------------------|--|
| AntiVirus | <input checked="" type="checkbox"/> | AV default | |
| Web Filter | <input type="checkbox"/> | | |
| DNS Filter | <input type="checkbox"/> | | |
| Application Control | <input type="checkbox"/> | | |
| IPS | <input type="checkbox"/> | | |
| Proxy Options | <input checked="" type="checkbox"/> | PRX default | |
| SSL Inspection | <input checked="" type="checkbox"/> | SSL deep-inspection | |

Ordering the policy table

- To view the policy table, go to **Policy & Objects > IPv4 Policy**. Select the **By Sequence** view, which shows the policies in the order that they are used by your FortiGate.

Currently, the policies are arranged in the order you created them, with the oldest policy at the top of the list.

| ID | Name | From | To | Source | Destination | Schedule | Service | Action | NAT | Security Profiles | Log | Bytes |
|----|---------------|------|------|-------------------------|-------------|----------|---------|--------|---------|---|----------|-----------|
| 1 | Internet | lan | wan1 | all Employees | all | always | ALL | ACCEPT | Enabled | AV default WEB default SSL deep-inspection | UTM | 478.00 MB |
| 2 | Accounting | lan | wan1 | all Accounting | all | always | ALL | ACCEPT | Enabled | AV default WEB default APP default SSL deep-inspection | UTM | 0 B |
| 3 | Admin | lan | wan1 | all Admin AdminPC | all | always | ALL | ACCEPT | Enabled | AV default SSL deep-inspection | UTM | |
| 0 | Implicit Deny | any | any | all | all | always | ALL | DENY | | | Disabled | 467.88 kB |

- To have the correct traffic flowing through each policy, you must arrange them so that the more specific policies are located at the top.

To rearrange the policies, select the column on the far left (in the example, ID) and drag the policy to the required

position, as shown on the right.

| ID | Name | From | To | Source | Destination | Schedule | Service | Action | NAT | Security Profiles | Log | Bytes |
|----|---------------|------|------|-------------------------|-------------|----------|---------|--------|---------|---|----------|-----------|
| 3 | Admin | lan | wan1 | all Admin AdminPC | all | always | ALL | ACCEPT | Enabled | AV default SSL deep-inspection | UTM | 0 B |
| 2 | Accounting | lan | wan1 | all Accounting | all | always | ALL | ACCEPT | Enabled | AV default WEB default APP default SSL deep-inspection | UTM | 0 B |
| 1 | Internet | lan | wan1 | all Employees | all | always | ALL | ACCEPT | Enabled | AV default WEB default SSL deep-inspection | UTM | 478.00 MB |
| 0 | Implicit Deny | any | any | all | all | always | ALL | DENY | | | Disabled | 529.54 kB |

Results

- From any PC in the internal network, attempt to browse the Internet. A log in screen will appear. Use the **jpearson** account to log in. After authentication, you can connect to the Internet.



If a certificate error occurs during the authentication process, browse to a different site and re-attempt user authentication.



Authentication Required

Please enter your username and password to continue.

Username:

Password:

- Go to **Monitor > Firewall User Monitor**. The list shows **jpearson** is online.

| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|-----------|------------|---------------------|--------------|----------------|----------|
| jpearson | Employees | 1 minute 39 seconds | 192.168.65.3 | 3.52 MB | Firewall |

- Right-click the account and select **Deauthenticate**.
- On the same PC, attempt to browse the Internet again. This time, log in using the **akeating** account.

5. The **Firewall User Monitor** now shows **akeating** is online and you can access the Internet.

| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|-----------|------------|------------|--------------|----------------|----------|
| akeating | Accounting | 51 seconds | 192.168.65.3 | 291.08 kB | Firewall |

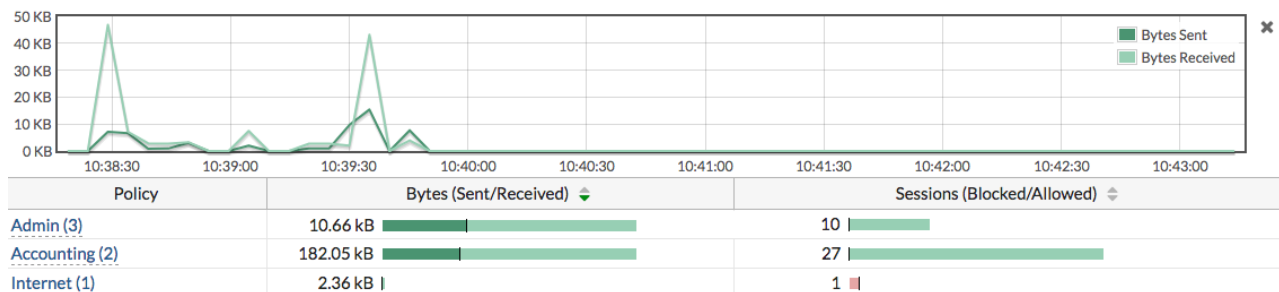
6. From the **AdminPC**, attempt to browse the Internet. Log in using the **tal-jamil** account.

7. The **Firewall User Monitor** now shows **tal-jamil** is online and you can access the Internet.

| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|-----------|------------|---------------------|--------------|----------------|----------|
| tal-jamil | Admin | 1 minute 32 seconds | 192.168.65.2 | 334.73 kB | Firewall |

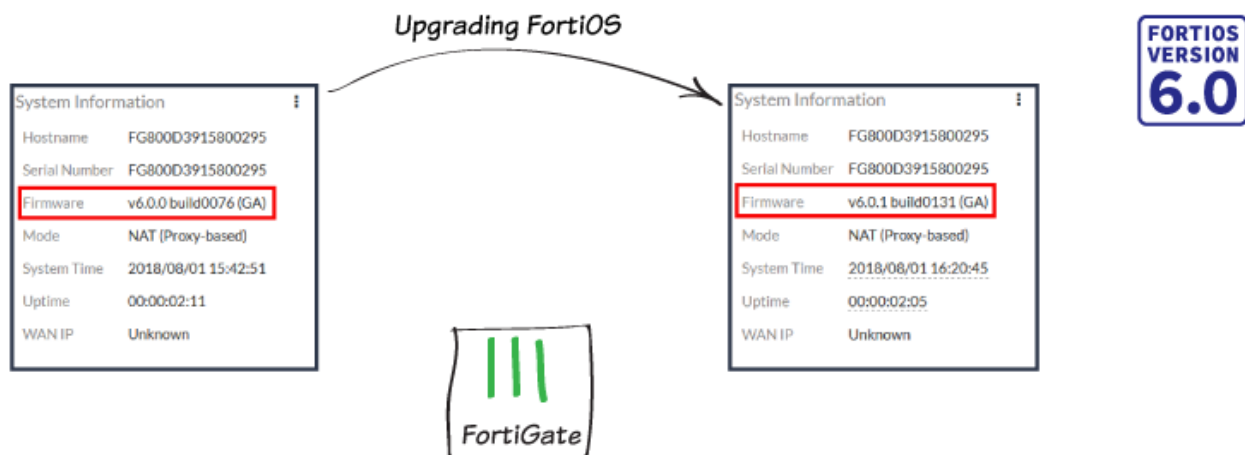
8. If you attempt to log in from any other device using the **tal-jamil** account, the account will authenticate; however, you will not have Internet access.

9. Go to **FortiView > All Segments > Policies** and select the **5 minutes** view. You can see traffic hitting all three policies and that each user's traffic is flowing through the correct policy.



For further reading, check out [Firewall policies](#) in the [FortiOS 6.0 Online Help](#).

Upgrading FortiGate firmware



In this example, you upgrade your FortiGate firmware from FortiOS 6.0.0 to 6.0.1.

Checking the current FortiOS firmware

1. To check which firmware version you're using, go to the **Dashboard** and view the **System Information** widget, which shows the current **Firmware**.


| System Information | |
|--------------------|-----------------------|
| Hostname | FG800D3915800295 |
| Serial Number | FG800D3915800295 |
| Firmware | v6.0.0 build0076 (GA) |
| Mode | NAT (Proxy-based) |
| System Time | 2018/08/01 15:42:51 |
| Uptime | 00:00:02:11 |
| WAN IP | Unknown |

2. To find out if a new FortiOS version is available, go to **System > Firmware**. If new firmware is available, a notice appears under **Current version**.



When a new FortiOS version is released, it may not be listed on your FortiGate right away. If this occurs, download the firmware from [Fortinet Support](#), then use **Upload Firmware** to upgrade your FortiGate.

Current version FortiOS v6.0.0 build0076 (GA)

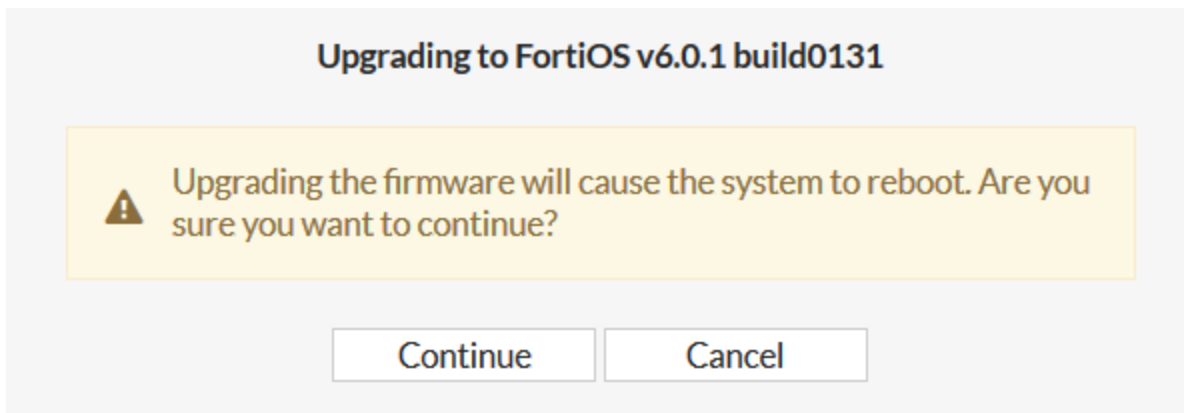
 FortiOS v6.0.1 available

Upgrading to the latest version

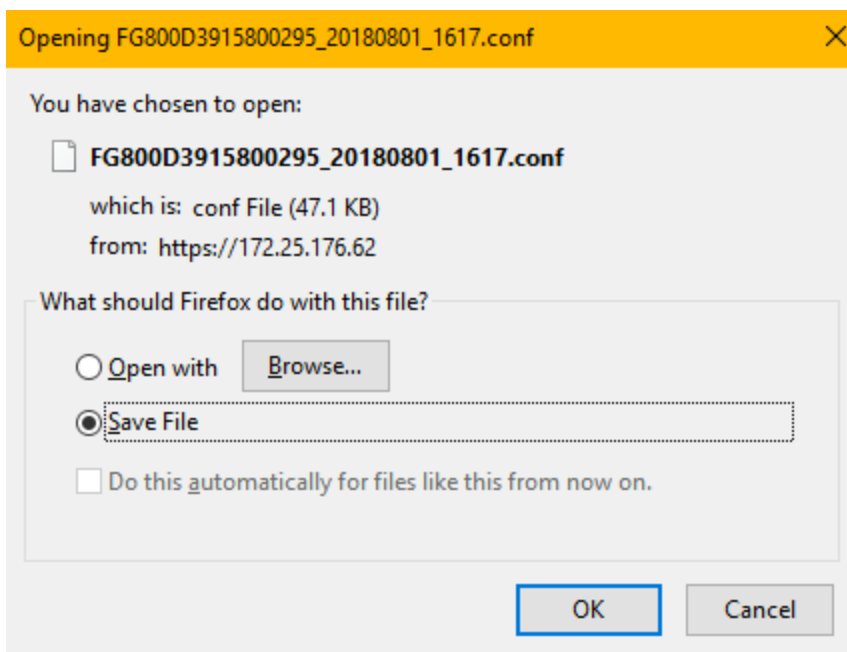
1. Under **FortiGuard Firmware**, select **Latest**. A notice may appear stating that there is no valid upgrade path for this firmware version. If this is the case, select **All available** instead and find a suitable firmware version for your FortiGate.
For more information about the upgrade path, go to [Fortinet Support](#).
2. If no warning appears, select **Release notes** to learn more about the firmware build. Release notes are also available at the [Fortinet Documentation Library](#).



3. To upgrade your FortiGate, select **Backup config and upgrade**. When prompted, select **Continue**.



4. Save the backup of your current FortiGate configuration, in case you need to restore it after the upgrade process.

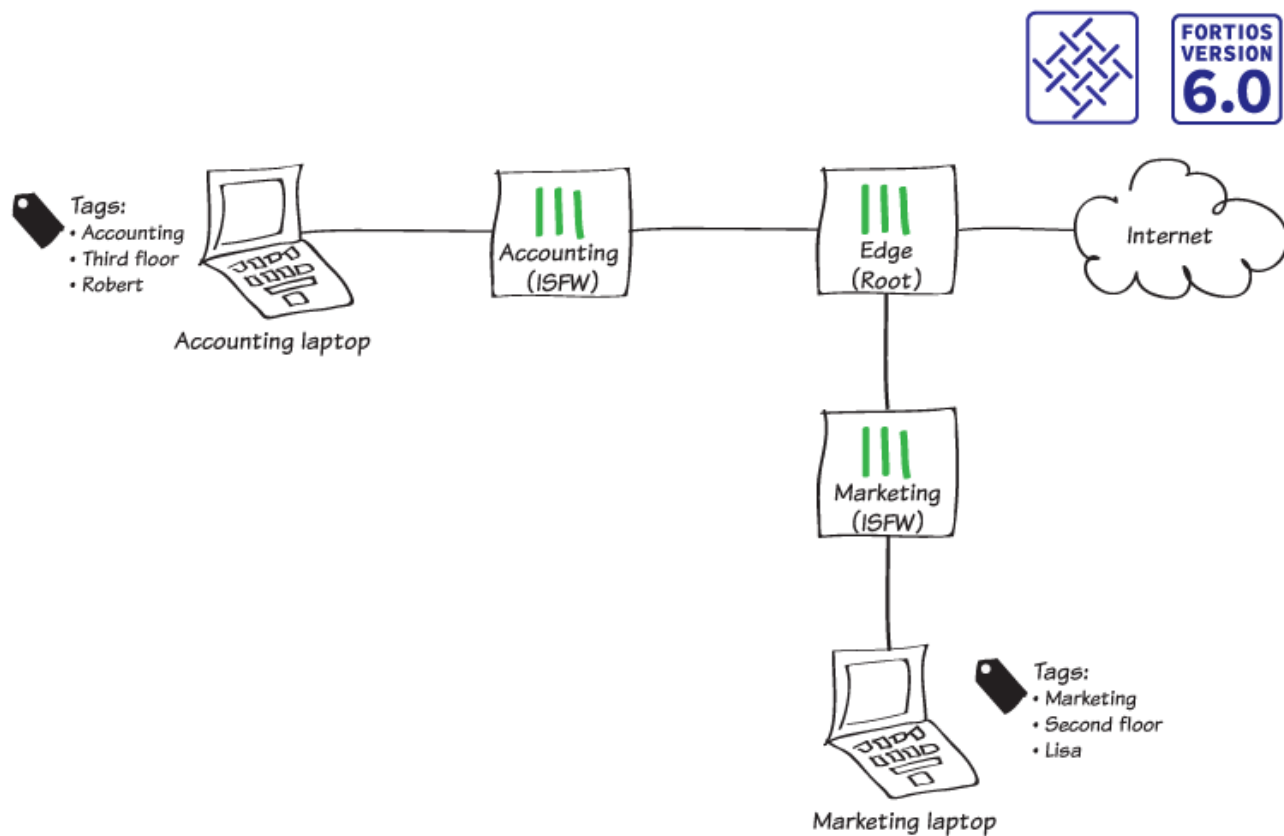


Results

1. The FortiGate uploads and installs the firmware, then restarts. This process takes a few minutes. When the firmware is installed, the FortiGate login appears.
2. Go to the **Dashboard**. The **System Information** widget shows the new **Firmware** version.

| System Information | | ⋮ |
|--------------------|-----------------------|---|
| Hostname | FG800D3915800295 | |
| Serial Number | FG800D3915800295 | |
| Firmware | v6.0.1 build0131 (GA) | |
| Mode | NAT (Proxy-based) | |
| System Time | 2018/08/01 16:20:45 | |
| Uptime | 00:00:02:05 | |
| WAN IP | Unknown | |

Tags in the Fortinet Security Fabric



In this recipe, you create tag categories and tags for your network. By applying these tags to different devices, interfaces, and addresses, you identify the location and function of each part of your Security Fabric and increase network visibility.


Creating tag categories and tags

In this example, you use tags to identify the following things about devices in the Security Fabric:

- Physical location
 - Department
 - Network administrators
1. To create the tag category for physical location, connect to Edge and go to **System > Tags**.
 2. Set **Tag Category** to **Location**. Because each device in the network can only have one location, disable **Allow multiple tag selection**.
 3. Add **Tags** for the first floor, second floor, and third floor.
 4. Under **Tag Scope**, set **Device** to **Mandatory**.

Tag Category

Allow multiple tag selection ☒

Color 

Tags

| | | |
|----------------------------------|----------------------------------|----------------------------------|
| First floor | <input type="button" value="x"/> | <input type="button" value="0"/> |
| Second floor | <input type="button" value="x"/> | <input type="button" value="0"/> |
| Third floor | <input type="button" value="x"/> | <input type="button" value="0"/> |
| <input type="button" value="+"/> | | |


Tag Scope

| | | | |
|-----------|---|---|---|
| Interface | <input checked="" type="button" value="Disable"/> | <input type="button" value="Mandatory"/> | <input type="button" value="Optional"/> |
| Device | <input type="button" value="Disable"/> | <input checked="" type="button" value="Mandatory"/> | <input type="button" value="Optional"/> |
| Address | <input checked="" type="button" value="Disable"/> | <input type="button" value="Mandatory"/> | <input type="button" value="Optional"/> |

5. For the department tag, enable **Allow multiple tag selection**.
6. Add **Tags** for the following departments: *Accounting*, *Marketing*, *Sales*, and *Admin*.
7. Under **Tag Scope**, set **Interface** to **Mandatory** and set **Device** to **Mandatory**. Because the FortiGate configuration includes default addresses, set **Address** to **Optional**.

Tag Category

Allow multiple tag selection ☒

Color 

Tags

| | | |
|----------------------------------|----------------------------------|----------------------------------|
| Accounting | <input type="button" value="x"/> | <input type="button" value="0"/> |
| Marketing | <input type="button" value="x"/> | <input type="button" value="0"/> |
| Sales | <input type="button" value="x"/> | <input type="button" value="0"/> |
| Admin | <input type="button" value="x"/> | <input type="button" value="0"/> |
| <input type="button" value="+"/> | | |

Tag Scope


| | | | |
|-----------|--|---|--|
| Interface | <input type="button" value="Disable"/> | <input checked="" type="button" value="Mandatory"/> | <input type="button" value="Optional"/> |
| Device | <input type="button" value="Disable"/> | <input checked="" type="button" value="Mandatory"/> | <input type="button" value="Optional"/> |
| Address | <input type="button" value="Disable"/> | <input type="button" value="Mandatory"/> | <input checked="" type="button" value="Optional"/> |

8. For the network administrators tag, enable **Allow multiple tag selection**.






9. Add **Tags** for *Robert* and *Lisa*.
10. Under **Tag Scope**, set **Device** to **Mandatory**.

Tag Category

Allow multiple tag selection ☒

Color 

Tags











| | | |
|---|---|---|
| Robert |  |  |
| Lisa |  |  |
|  | | |

Tag Scope

| | | | |
|-----------|----------------|------------------|----------|
| Interface | Disable | Mandatory | Optional |
| Device | Disable | Mandatory | Optional |
| Address | Disable | Mandatory | Optional |




11. Because the configuration of tag categories and tags isn't synchronized across the Security Fabric, you must connect to each FortiGate device separately and add the appropriate tags for the part of your network that uses that FortiGate.











Connect to Accounting and repeat the previous steps to create the tags that are shown.

| Tag Category  | Allow Multiple Tag Selection  | Interface  | Address  | Device  | Tags  |
|--|--|---|---|--|--|
| default | Enable | Optional | Optional | Optional | |
| Department | Enable | Mandatory | Optional | Mandatory |  Accounting |
| Location | Disable | Disable | Disable | Mandatory |  Third floor |
| Network administrators | Enable | Disable | Disable | Mandatory |  Lisa  Robert |


Applying tags






1. To apply tags to devices in your network, go to **User & Device > Device Inventory**.
2. Edit the Accounting FortiGate.
3. Under **Tags**, add the following tags:
 - For **Department**, add the **Accounting** tag
 - For **Location**, add the **Third floor** tag
 - For **Network administrators**, add the **Robert** and **Lisa** tags

| | |
|-----------------|--|
| Alias | <input type="text" value="Accounting-FortiGate"/> |
| MAC Address | 70:4c:a5:22:cf:0b |
| Additional MACs | <input type="text" value=""/> |
| Device Type |  Fortinet Device ▼ |
| Custom Groups | <input type="text" value=""/> |
| Avatar |  Upload Image  Capture Image |
| Comments | <input type="text" value=""/> 0/255 |


| | |
|---|--|
| Tags | |
| Department | <div> Accounting  </div> <div><input type="text" value=""/></div> |
| Location | <div> Third floor ▼ </div> |
| Network administrators | <div> Lisa </div> <div> Robert </div> <div><input type="text" value=""/></div> |
| <div> Add Tag Category</div> | |

4. Edit all other devices listed and apply the appropriate tags for department, location, and administrators.
5. To apply tags to interfaces in your network, go to **Network > Interfaces**. Edit the interface that connects Edge and Accounting (in the example, **port 10**).
6. Under **Tags**, set **Department** to **Accounting**.








| | |
|----------------|--|
| Interface Name | port10 (00:09:0F:09:19:03) |
| Alias | <input type="text" value="Accounting"/> |
| Link Status | Up  |
| Type | Physical Interface |

| | |
|---|--|
| Tags | |
| Role  | <div><input type="text" value="LAN"/> ▼</div> |
| Department | <div> Accounting  </div> <div><input type="text" value=""/></div> |
| <div> Add Tag Category</div> | |

7. Edit all other interfaces and apply the appropriate tag for department.
8. To apply tags to addresses in your network, go to **Policy & Objects > Addresses**. Edit the address for the Accounting subnet.
9. Under **Tags**, set **Department** to **Accounting**.

| | | |
|----------------|--|--|
| Interface Name | port10 (00:09:0F:09:19:03) | |
| Alias | <input type="text" value="Accounting"/> | |
| Link Status | Up  | |
| Type | Physical Interface | |

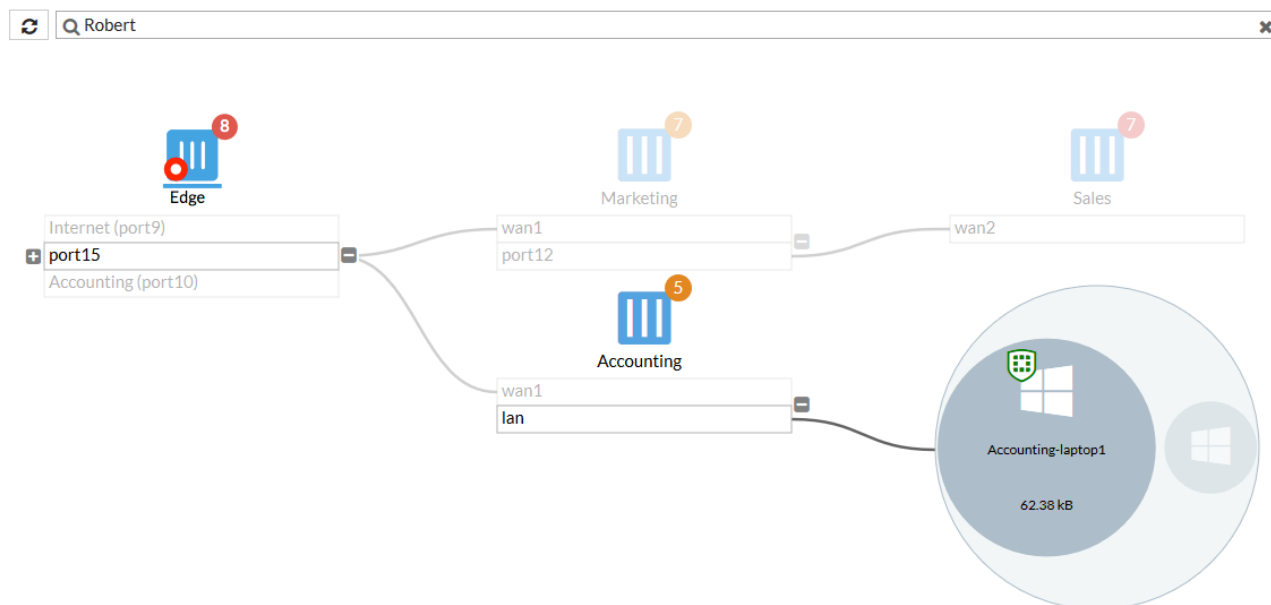
Tags

| | | |
|---|--|--|
| Role  | <input type="text" value="LAN"/> |  |
| Department | <div> Accounting </div> <div></div> | <div></div> |
| <div> Add Tag Category</div> | | |

10. Edit all other addresses and apply the appropriate tag for department.
11. To apply tags to devices in on the accounting network, connect to Accounting and go to **User & Device > Device Inventory**.
12. Edit a computer on this network.
13. Under **Tags**, add the following tags:
 - For **Department**, add the **Accounting** tag
 - For **Location**, add the **Third floor** tag
 - For **Network administrators**, add the **Robert** tag
14. Apply the appropriate tags to other devices, interfaces, and addresses on this network.

Results

1. To sort devices and interfaces by tags, connect to Edge and go to **Security Fabric > Logical Topology**.
2. In the **Search** field, enter *Robert*. The devices that have the **Robert** tag are highlighted.

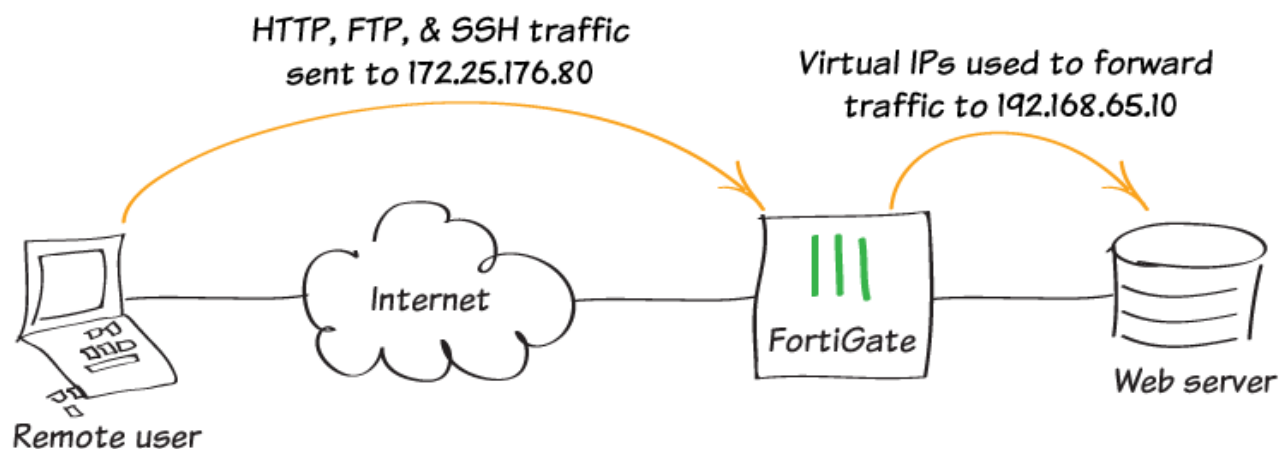


3. To view more information about a highlighted device, including tags, hover over that device in the topology. The **Robert** tag is highlighted.

The panel displays detailed information for the device 'Accounting-laptop1' (vmartin, 10.10.10.2). It includes a list of vulnerabilities (1), hostname, MAC address, last seen time, and tags: Accounting, Third floor, and **Robert** (highlighted in yellow). The topology section shows the device's position within the network hierarchy: Edge2-Primary > Accounting2 > Accounting-laptop1. Performance metrics are also shown: 69 sessions, 15.23 kB bytes sent/received, 536 bps bandwidth, and 168 B packets sent/received.

| Field | Value |
|-------------------------|--|
| Device | Accounting-laptop1 |
| Vulnerabilities | 1 |
| Hostname | Accounting-laptop1 |
| MAC Address | 50:7b:9d:37:42:02 |
| Last Seen | 2018/05/04 14:30:14 |
| Tags | Accounting, Third floor, Robert |
| Topology | Edge2-Primary > Accounting2 > Accounting-laptop1 |
| Sessions | 69 |
| Bytes (Sent/Received) | 15.23 kB |
| Bandwidth | 536 bps |
| Packets (Sent/Received) | 168 B |

Port forwarding



In this recipe, you configure port forwarding to open specific ports and allow connections from the Internet to reach a server located behind the FortiGate. This allows Internet users to reach the server through the FortiGate without knowing the server's internal IP address. Users can also connect using only the ports that you choose.


Creating virtual IP addresses

In this example, you open TCP ports 8096 (HTTP), 21 (FTP), and 22 (SSH) for remote users to communicate with the server behind the firewall. The external IP address of the server is 172.25.176.60, which is mapped to the internal IP address 192.168.70.10.

1. To create a virtual IP (VIP) address for port 8096, go to **Policy & Objects > Virtual IPs** and create a new virtual IP address.
2. Set **External IP Address/Range** to 172.25.176.60 and set **Mapped IP Address/Range** to 192.168.65.10.
3. Enable **Port Forwarding**. Set **Protocol** to **TCP**, set **External Service Port** to **8096**, and set **Map to Port** to 8096.

Name 

Comments 0/255

Color 

Network

Interface

Type Static NAT

External IP Address/Range -

Mapped IP Address/Range -

Optional Filters ☐Port Forwarding ☒

Protocol

External Service Port -

Map to Port -

4. Create a second VIP address for port 21. Set both **External Service Port** and **Map to Port** to 21.

Name 

Comments 0/255

Color 

Network

Interface

Type Static NAT

External IP Address/Range -

Mapped IP Address/Range -

Optional Filters ☐Port Forwarding ☒

Protocol


External Service Port -

Map to Port -

5. Create a third VIP address for port 22. Set both **External Service Port** and **Map to Port** to 22.

Name 

Comments 0/255

Color 

Network

Interface

Type Static NAT

External IP Address/Range -

Mapped IP Address/Range -

Optional Filters ☐

Port Forwarding ☒

Protocol

External Service Port -


Map to Port -

Creating a virtual IP group

1. To add the new virtual IP addresses to a virtual IP group, go to **Policy & Objects > Virtual IPs** and create a new group.
2. Set the new virtual IP addresses as **Members** of the group.








Name 0/255

Comments

Color 

Interface

Members

| | |
|---|---|
|  server-FTP |  |
|  server-HTTP |  |
|  server-SSH |  |
|  | |

Creating a security policy

1. To allow Internet users to reach the server, go to **Policy & Objects > IPv4 Policy** and create a new policy.
2. Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to the interface connected to the server, and **Destination Address** to the VIP group.

NAT is disabled for this policy so that the server sees the original source addresses of the packets it receives. This is the preferred setting for a number of reasons. For example, the server logs are more meaningful if they record the actual source addresses of your users.



If the FortiGate has Central NAT enabled, the VIP objects won't be available for selection in the policy editing window.

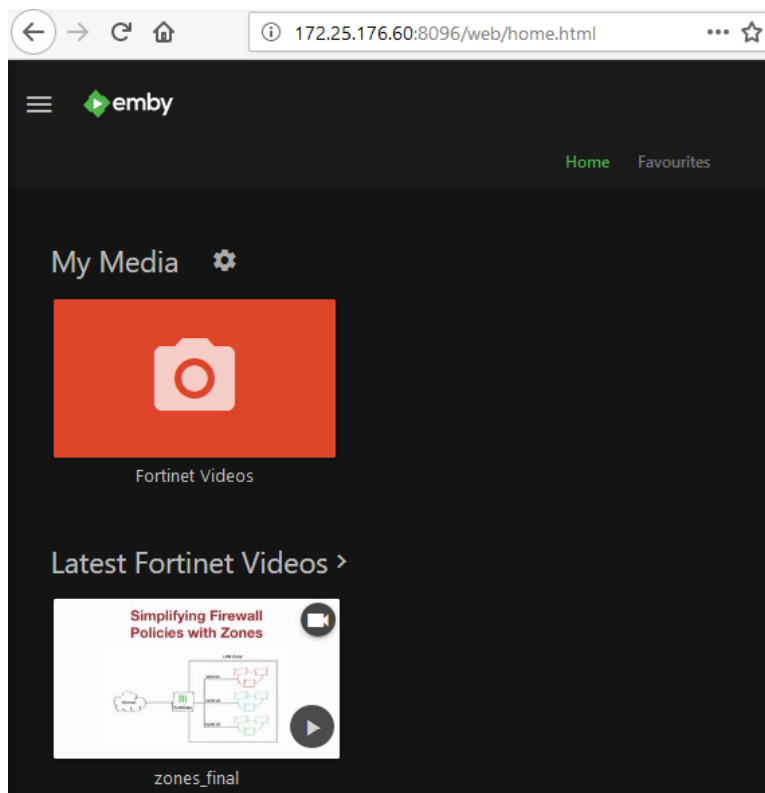
| | |
|--------------------|---|
| Name | Server-access |
| Incoming Interface | wan1 |
| Outgoing Interface | port11 |
| Source | all |
| Destination | server-ports |
| Schedule | always |
| Service | ALL |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

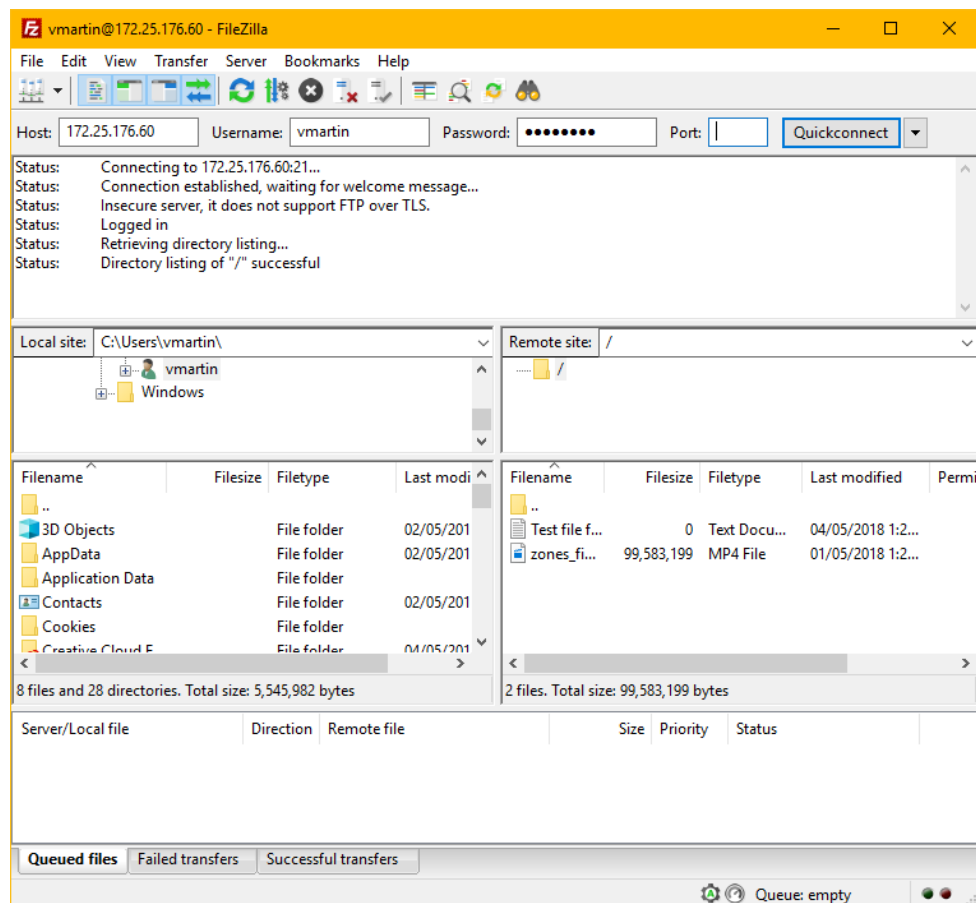
NAT ☐

Results

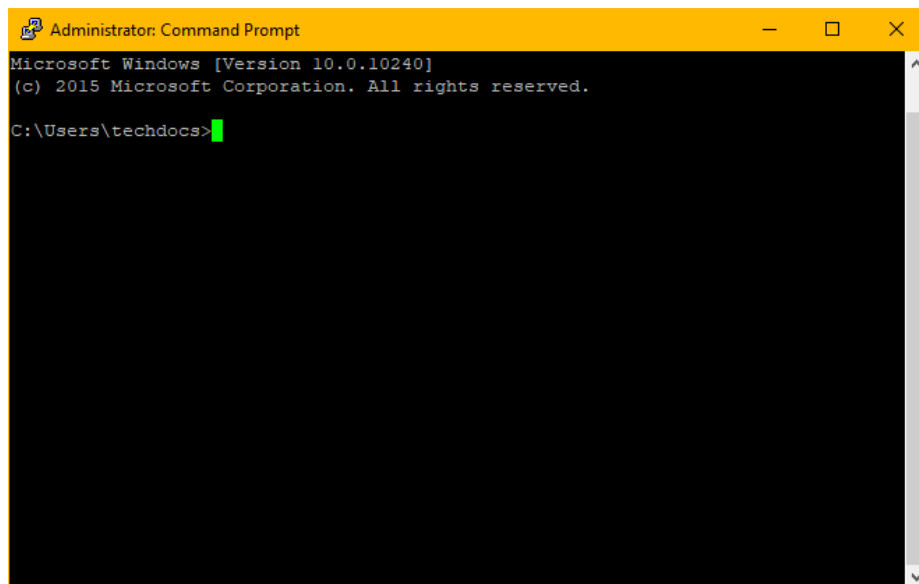
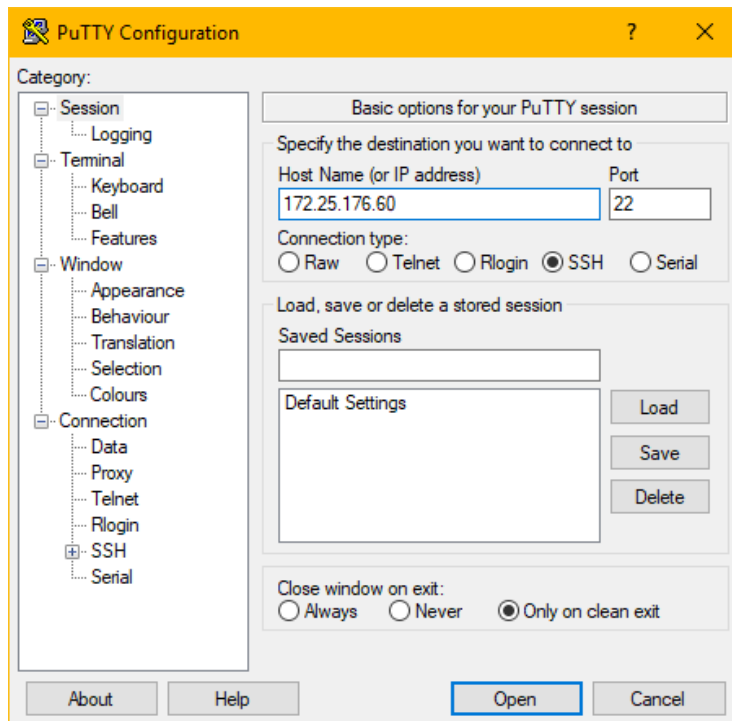
1. To ensure that TCP port 8096 is open, browse to <http://172.25.176.60:8096>.



2. Next, ensure that TCP port 21 is open by using an FTP client to connect to the FTP server from a remote connection on the other side of the firewall.

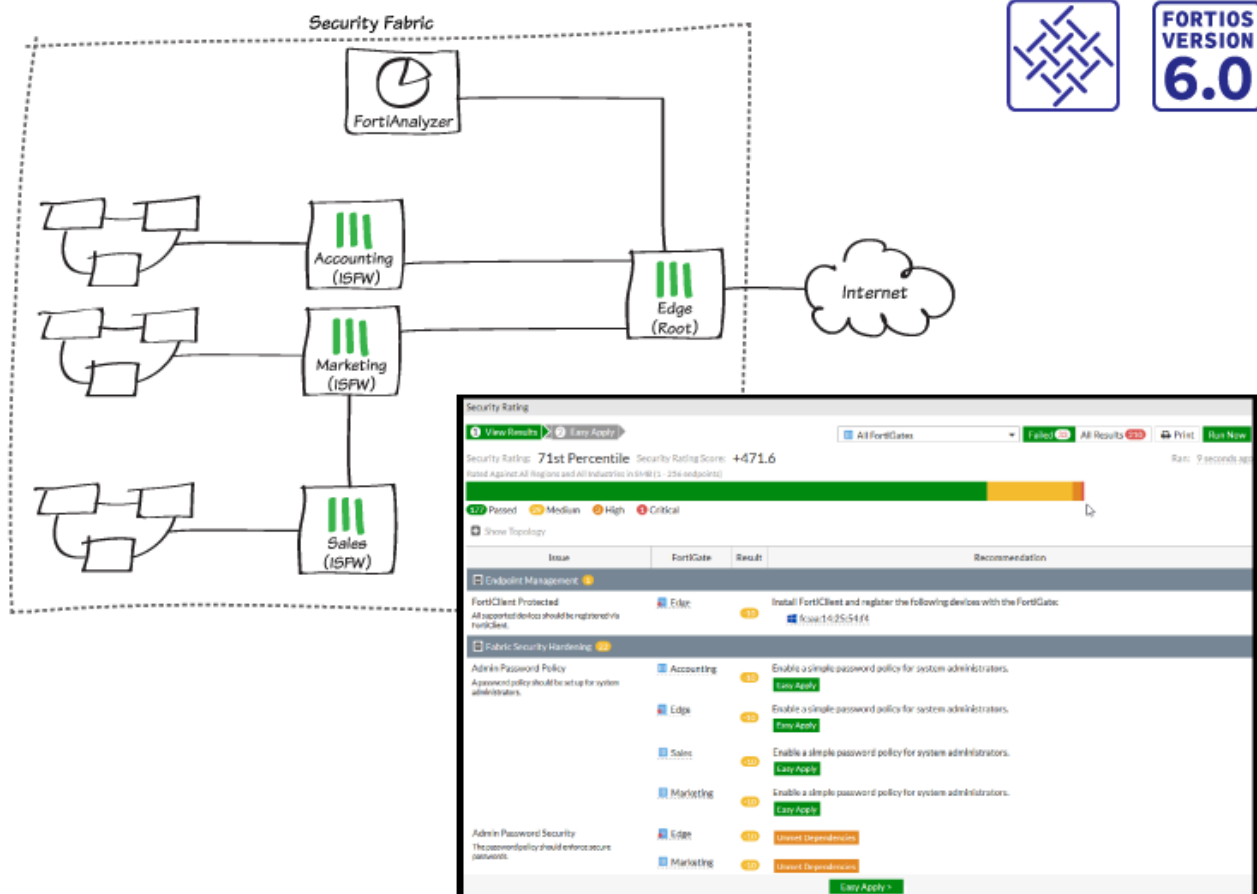


3. Finally, ensure that TCP port 22 is open by connecting to the SSH server from a remote connection on the other side of the firewall.



For further reading, check out [Virtual IPs](#) in the [FortiOS 6.0 Online Help](#).

Security Rating



In this recipe, you run a Security Rating check, which analyzes the Fortinet Security Fabric deployment to identify potential vulnerabilities and highlight best practices.

Using the Security Rating can help you improve your network configuration, deploy new hardware and software, and gain more visibility and control over your network. By regularly checking your Security Rating and your Security Rating Score, and making the recommended improvements, you can have confidence that your network is getting more secure over time.

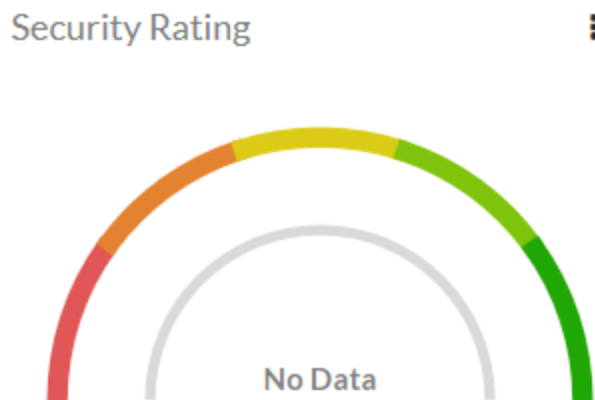
To run all available checks, you must have a valid Security Rating license from FortiGuard. If you don't have a license, only certain checks are available. For more information about these checks, see [Security Best Practices & Security Rating Feature](#).



Not all FortiGate models can run the FortiGuard Security Rating Service if they are the root FortiGate in a Security Fabric. For more information, see the [FortiOS 6.0 Release Notes](#).

Checking the Security Rating widget

1. Go to the **Dashboard** and locate the **Security Rating** widget. In the example, the widget doesn't display any information because it's not properly configured.



2. Once you configure the widget, it displays a comparison between your Security Rating and the ratings of other organizations. You can compare your rating to the ratings of organizations that belong to all industries or the same industry as your organization. You can also compare your rating with organizations in your region or all regions.



Your FortiCare account settings determine your industry categorization.

3. To change which organizations your score is compared to, select the options menu in the top right corner, then select **Settings**.

| | | |
|----------|----------------|-------------|
| Industry | All Industries | My Industry |
| Region | All Regions | CA |

OK

Cancel

Checking your Security Rating

1. On Edge, go to **Security Fabric > Security Rating**. The Security Rating runs automatically on the root FortiGate. However, if you want more recent results, select **Run Now** to run another Security Rating.
2. You can also select whether to run the Security Rating on **All FortiGates** or on specific FortiGate devices in the Security Fabric.

Security Rating

1 View Results 2 Easy Apply

All FortiGates Failed 33 All Results 210 Print Run Now

Security Rating: **71st Percentile** Security Rating Score: **+471.6** Ran: 9 seconds ago
 Rated Against All Regions and All Industries in SMB (1 - 256 endpoints)

177 Passed 29 Medium 3 High 1 Critical

Show Topology

| Issue | FortiGate | Result | Recommendation |
|--|------------|--------|---|
| Endpoint Management 1 | | | |
| FortiClient Protected All supported devices should be registered via FortiClient. | Edge | -10 | Install FortiClient and register the following devices with the FortiGate: fc:aa:14:25:54:f4 |
| Fabric Security Hardening 22 | | | |
| Admin Password Policy A password policy should be set up for system administrators. | Accounting | -10 | Enable a simple password policy for system administrators. Easy Apply |
| | Edge | -10 | Enable a simple password policy for system administrators. Easy Apply |
| | Sales | -10 | Enable a simple password policy for system administrators. Easy Apply |
| | Marketing | -10 | Enable a simple password policy for system administrators. Easy Apply |
| Admin Password Security The password policy should enforce secure passwords. | Edge | -10 | Unmet Dependencies |
| | Marketing | -10 | Unmet Dependencies |

Easy Apply >

- At the top of the page, you can see your network's **Security Rating**, which shows which percentile your network is in compared to other organizations. You can also see your **Security Rating Score**, which is based on how many checks your Security Fabric passed or failed, and how many FortiGate units are in your network.
- Further down the page, you can see information about each failed check, including which FortiGate failed the check, the effect on your Security Rating Score, and recommendations for how you can the issue.
- In the next step of the Security Rating, you can apply recommendations marked as **Easy Apply** to any FortiGate in the Security Fabric. However, if the Security Rating results are older than 30 minutes, you must first run it again to make sure all information is current and accurate.
- By using **Easy Apply**, you can change the configuration of any FortiGate in the Security Fabric from the root FortiGate.
- Select all the changes that you want to make, then select **Apply Recommendations**.

[View Results](#) [2 Easy Apply](#)
All FortiGates
Failed 33
All Results 210
[Print](#)
[Run Now](#)

Backup configuration before applying any recommendations ☒

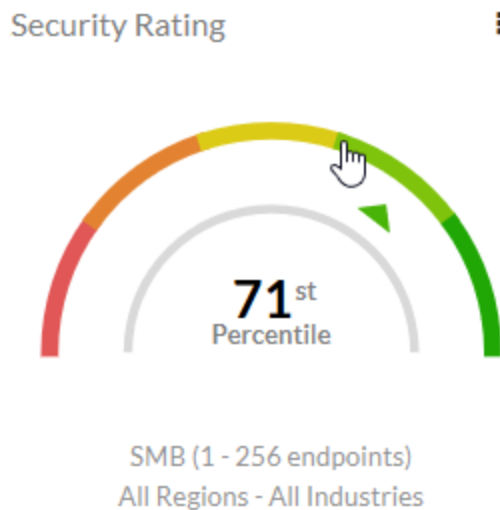
Recommendations are applied based on Security Rating results generated at 2018/04/17 12:58:01

| Issue | FortiGate | Result | Recommendation |
|--|------------|--------|--|
| Fabric Security Hardening | | | |
| Admin Password Policy A password policy should be set up for system administrators. | Accounting | -10 | Enable a simple password policy for system administrators. |
| | Edge | -10 | Enable a simple password policy for system administrators. |
| | Sales | -10 | Enable a simple password policy for system administrators. |
| | Marketing | -10 | Enable a simple password policy for system administrators. |
| Admin Idle Timeout The timeout for idle administrators should be at most 10 minutes. | Edge | -10 | Modify the timeout for idle administrators to be at most 10 minutes. |
| | Sales | -10 | Modify the timeout for idle administrators to be at most 10 minutes. |
| Failed Login Attempts The administrator lockout threshold should be at most 3 attempts, and the lockout duration at least 15 minutes. | Edge | -10 | Apply the following requirement(s): • Lockout duration should be at least 15 minutes. |
| | Marketing | -10 | Apply the following requirement(s): • Lockout duration should be at least 15 minutes. |
| | Accounting | -10 | Apply the following requirement(s): • Lockout duration should be at least 15 minutes. |
| | Sales | -10 | Apply the following requirement(s): • Lockout duration should be at least 15 minutes. |

[< Back](#)
[Apply Recommendations](#)

Results

1. Go to the **Dashboard**. The **Security Rating** widget displays information from the most recent Security Rating check.



2. Go to **Security Fabric > Physical Topology**. Each FortiGate has a Security Rating indicator, which is circle that contains a number. The number shows how many checks the FortiGate failed and the color shows the severity of failed checks (red for critical, orange for high, yellow for medium, and blue for low).



- To view the failed checks on a specific FortiGate device, select the Security Rating indicator on the FortiGate in the topology.
- A screen appears, showing the Security Rating recommendations for that unit. You can also apply **Easy Apply** recommendations from here.

1 View Results 2 Easy Apply

Sales Failed 6 All Results 42 Run Now

Ran: 17 minutes 28 seconds ago

36 Passed 6 Medium

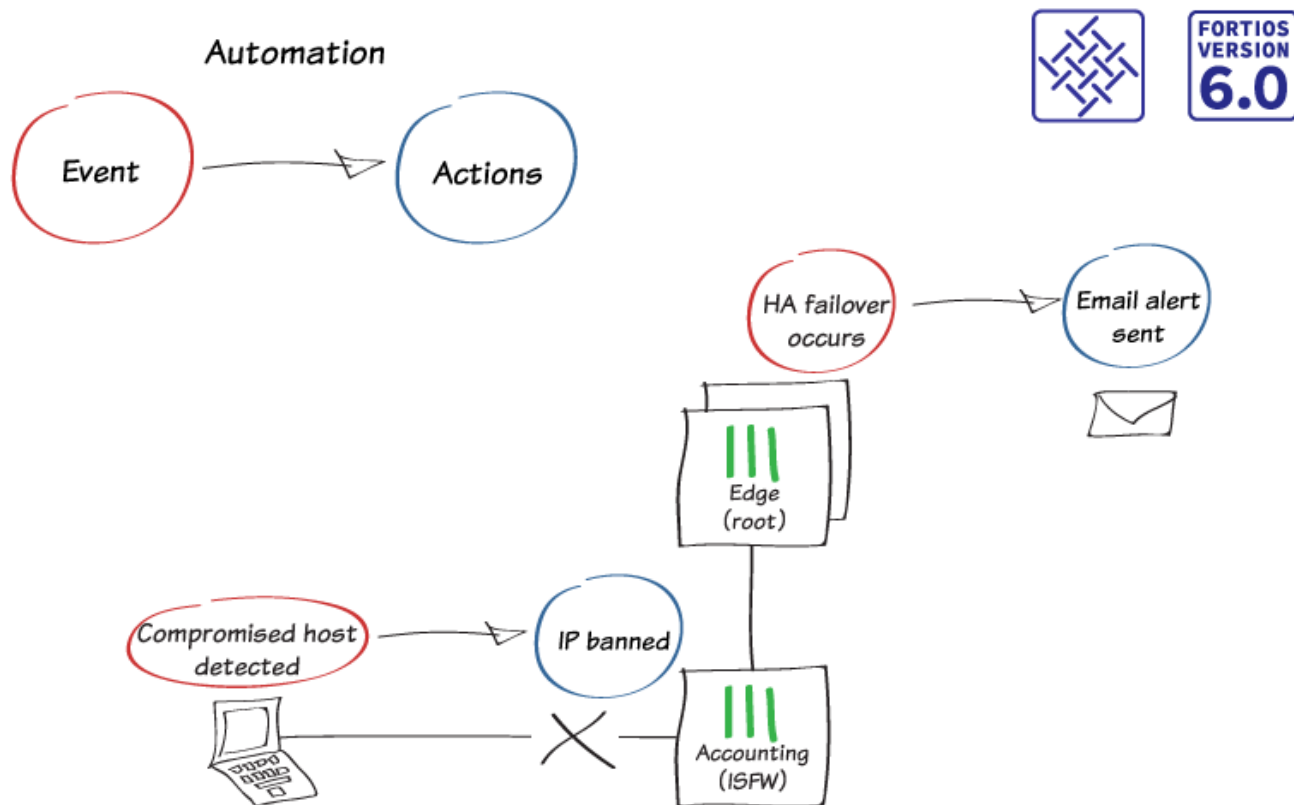
Show Topology

| Issue | Result | Recommendation | | | | |
|--|-----------|--|--------|-----------|---|-------|
| Fabric Security Hardening 5 | | | | | | |
| Admin Password Policy A password policy should be set up for system administrators. | -10 | Enable a simple password policy for system administrators. Easy Apply | | | | |
| Admin Password Security The password policy should enforce secure passwords. | -10 | Unmet Dependencies | | | | |
| Admin Idle Timeout The timeout for idle administrators should be at most 10 minutes. | -10 | Modify the timeout for idle administrators to be at most 10 minutes. Easy Apply | | | | |
| Failed Login Attempts The administrator lockout threshold should be at most 3 attempts, and the lockout duration at least 15 minutes. | -10 | Apply the following requirement(s): • Lockout duration should be at least 15 minutes. Easy Apply | | | | |
| Valid HTTPS Certificate - Administrative GUI The administrative GUI should be using a valid and secure certificate. | -10 | Configure a valid certificate. The current certificate "Fortinet_Factory" does not meet the following requirements: • Must not be a built-in default certificate. Acquire a certificate for your domain, upload it, and use it. | | | | |
| Network Design & Policies 1 | | | | | | |
| Unused Policies All IPv4 policies should be used. | -10 | Review the following IPv4 policies that haven't been used in the last 90 days: | | | | |
| | | <table border="1"> <thead> <tr> <th>Policy</th> <th>Last Used</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Never</td> </tr> </tbody> </table> | Policy | Last Used | 1 | Never |
| Policy | Last Used | | | | | |
| 1 | Never | | | | | |

Close Easy Apply >

For further reading, check out [Running a Security Fabric Rating](#) in the [FortiOS 6.0 Online Help](#).

Automation stitches



In this recipe, you configure Automation stitches for your Fortinet Security Fabric. Each Automation pairs an event trigger and one or more actions, which allows you to monitor your network and take appropriate action when the Security Fabric detects a threat. You can use Automation stitches to detect events from any source in the Security Fabric and apply actions to any destination.

In this example, you create the following Automation stitches:

- Ban a compromised host's IP address.
- Send an email alert when HA failover occurs.

In this example, the Security Fabric consists of Edge, an HA cluster that is the root FortiGate of the Security Fabric, and three ISFW FortiGate devices (Accounting, Marketing, and Sales). You configure the Automation stitches on the root FortiGate and the settings are synchronized with the other FortiGate devices in the Security Fabric.

Creating the Automation stitches

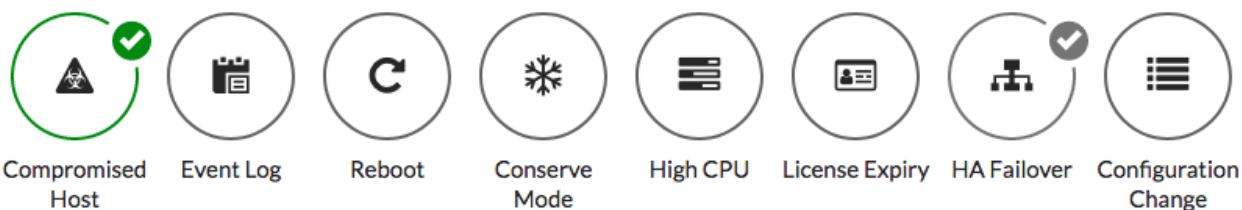
1. To create a new Automation that bans the IP address of a compromised host, go to **Security Fabric > Automation** and select **Create New**.
2. Set **FortiGate** to **All FortiGates**.
3. Set **Trigger** to **Compromised Host**. Set **IOC level threshold** to **High**.
4. Set **Action** to **IP Ban**.

Name

Status Enabled Disabled

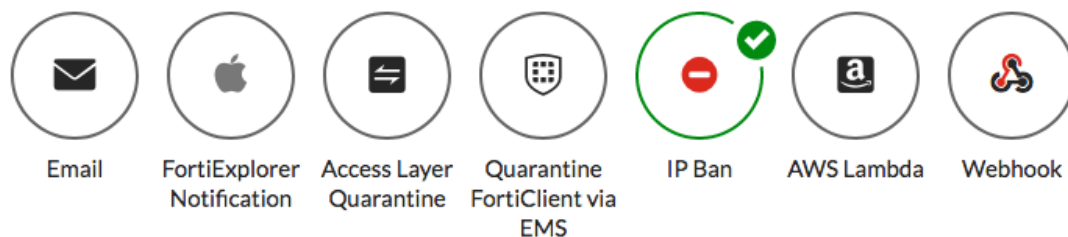
FortiGate All FortiGates ×

Trigger



IOC level threshold Medium High

Action



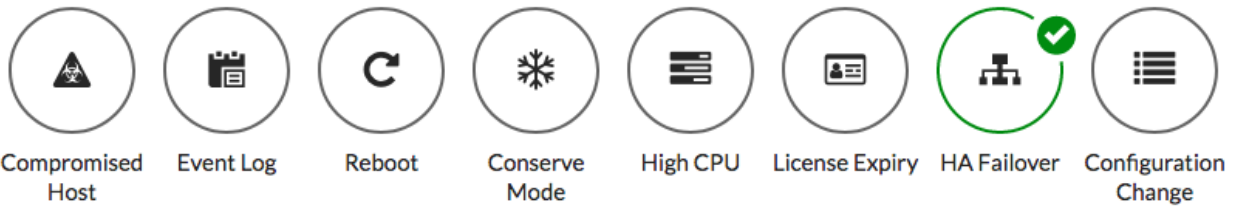
Minimum interval (seconds)

5. Create a second Automation that sends an email alert when HA failover occurs.
6. Set **FortiGate** to **Edge-Primary**, which is part of the only HA cluster in the Security Fabric.
7. Set **Trigger** to **HA Failover**. Set **Action** to **Email**.

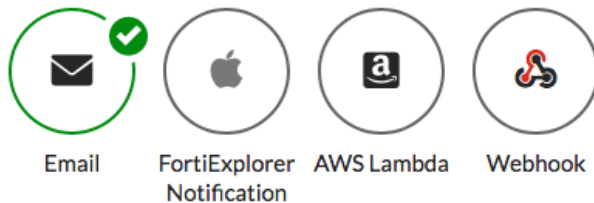
8. Set the Email subject and email address.

| | |
|-----------|--|
| Name | <input type="text" value="HA-failover"/> |
| Status | Enabled Disabled |
| FortiGate | <div>Edge-Primary</div> <div>+</div> |

Trigger



Action



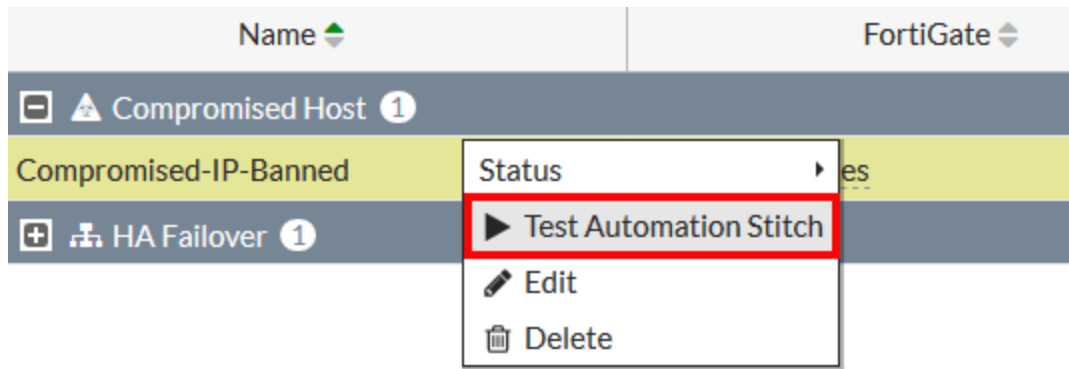
Minimum interval (seconds)

Email

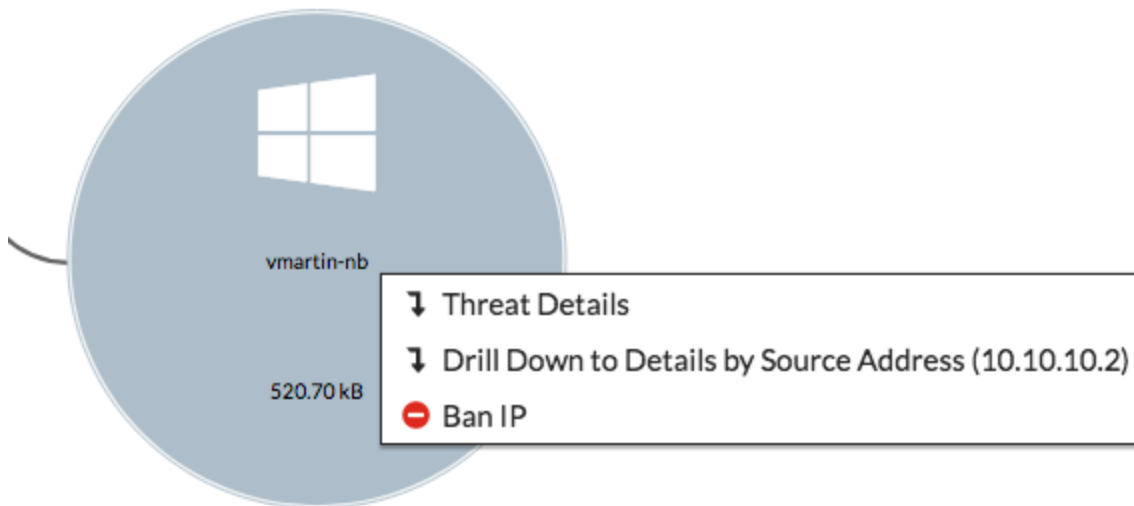
| | |
|---------------|---|
| Email subject | <input type="text" value="HA Failover"/> |
| To | <div>admin@example.com</div> <div>+</div> |

Testing the Automation stitches

1. If your FortiOS version is 6.0.2 or higher, to test the Automation stitches go to **Security Fabric > Automation**, right-click the Automation, and select **Test Automation Stitch**.



- If your FortiOS version is 6.0.0 or 6.0.1, use the following instructions to test the automation stitches. Instead of testing the Automation that blocks compromised hosts, the following steps simulate its effects by manually blocking the IP address of a PC on your network. Go to **Security Fabric > Physical Topology** and locate a PC on your network. Right-click the PC and select **Ban IP**.



- Set **Ban Type** to **Temporary**. Set **Duration** to **30 minutes**.

i An IP ban will be created on FortiGate F140EP4Q17000089. It can be removed in Monitor » Quarantine

Ban Type

☒ Temporary
 ☐ Permanent

Duration

Minutes

▼

- To test the Automation for HA failover, go to Edge-Primary. In the administrative drop-down menu, select **System > Reboot**.

5. Set an **Event log message**.

 Are you sure you want to reboot the device?

Event log message

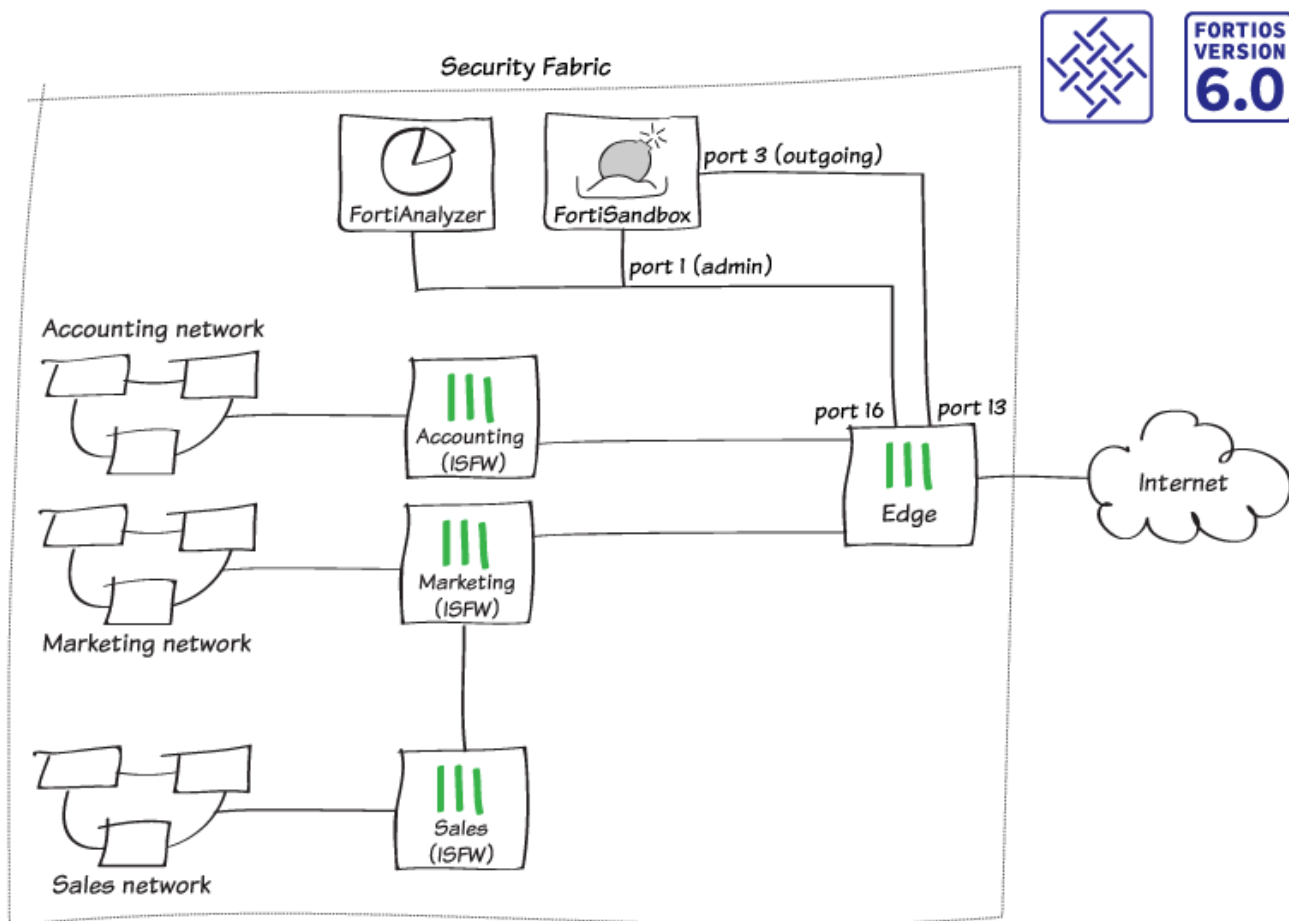
Testing automation.

Results

1. If you have simulated the the Automation that blocks compromised hosts, the banned device can no longer access the Internet.
2. When HA failover occurs or when the Automation is tested, an email similar to the one shown is sent to the email that you configured in the Automation.

```
FGT[FGT6HD3916806098] Automation Stitch:HA-failover is triggered.  
log: logid="0108037892" type="event" subtype="ha" level="notice" vd="root"  
eventtime=1522173378 logdesc="Virtual cluster member state moved"  
msg="Virtual cluster's member state moved" ha_role="master" vcluster=1  
vcluster_state="work" vcluster_member=0 hostname="Edge-Backup"  
sn="FGT6HD3916806098"
```

FortiSandbox in the Fortinet Security Fabric



In this recipe, you will add a FortiSandbox to the Fortinet Security Fabric and configure each FortiGate in the network to send suspicious files to FortiSandbox for sandbox inspection. The FortiSandbox scans and tests these files in isolation from your network.

This example uses the Security Fabric configuration created in [Fortinet Security Fabric installation on page 16](#). The FortiSandbox connects to the root FortiGate in the Security Fabric, known as Edge. There are two connections between the devices:

- FortiSandbox port 1 (administration port) connects to Edge port 16
- FortiSandbox port 3 (VM outgoing port) connects to Edge port 13

If possible, you can also use a separate Internet connection for FortiSandbox port 3, rather than connecting through the Edge FortiGate to use your main Internet connection. This configuration avoids having IP addresses from your main network blacklisted if malware that's tested on the FortiSandbox generates an attack. If you use this configuration, you can skip the steps listed for FortiSandbox port 3.



Checking your Security Rating

1. On Edge (the root FortiGate in the Security Fabric), go to **Security Fabric > Security Rating**.
2. Since you haven't yet installed a FortiSandbox in your network, the Security Fabric fails the **Advanced Threat Protection** check. In the example, the **Security Rating Score** decreases by 30 points for each of the four FortiGates in the Security Fabric.

| Threat and Vulnerability Management 4 | | | |
|---|------------|-----|---|
| Advanced Threat Protection Suspicious files should be submitted to FortiSandbox Appliance/FortiSandbox Cloud for inspection. | Edge | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |
| | Sales | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |
| | Marketing | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |
| | Accounting | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |

Connecting the FortiSandbox



1. Connect to the FortiSandbox.
2. To edit **port 1**, which is used for communication between the FortiSandbox and the rest of the Security Fabric, go to **Network > Interfaces**.
3. Set **IP Address/Netmask** to an internal IP address. In this example, the FortiSandbox connects to the same subnet as the FortiAnalyzer that you installed previously, using the IP address *192.168.65.20*.

| Interface Status | |
|-------------------|---|
| Interface: | port1 (administration port) |
| Interface Status: |  |
| Link Status: |  |

| IP Address / Netmask | |
|----------------------|-----------------------------|
| IPv4: | 192.168.65.20/255.255.255.0 |
| IPv6: | |

| Access Rights |
|--|
| <input checked="" type="checkbox"/> HTTP |
| <input checked="" type="checkbox"/> SSH |
| <input checked="" type="checkbox"/> Telnet |

4. Edit **port 3**. This port is used for outgoing communication by the virtual machines (VMs) running on the FortiSandbox. It's recommended that you connect this port to a dedicated interface on your FortiGate to protect the rest of the network from threats that the FortiSandbox is currently investigating.
5. Set **IP Address/Netmask** to an internal IP address (in the example, *192.168.179.10/255.255.255.0*).







| Interface Status | |
|----------------------|---|
| Interface: | port3 (VM outgoing port) |
| Interface Status: |  |
| Link Status: |  |
| IP Address / Netmask | |
| IPv4: | 192.168.179.10/255.255.255.0 |
| IPv6: | |

6. To add a static route, go to **Network > System Routing**. Set **Gateway** to the IP address of the FortiGate interface that port 1 connects to (in the example, 192.168.65.2).

| | |
|----------------------|-----------------|
| Destination IP/Mask: | 0.0.0.0/0.0.0.0 |
| Gateway: | 192.168.65.2 |
| Device: | port1 |

7. Connect to Edge.

8. To configure the port that connects to port3 on the FortiSandbox (in the example, port13), go to **Network > Interfaces**. Set **IP/Network Mask** to an address on the same subnet as port 3 on the FortiSandbox (in the example, 192.168.179.2/255.255.255.0)

| | | | |
|--|---|---|--|
| Interface Name | port13 (00:09:0F:09:19:06) | | |
| Alias | FortiSandbox-Internet | | |
| Link Status | Down  | | |
| Type | Physical Interface | | |
| Tags | | | |
| Role | LAN | | |
|  Add Tag Category | | | |
| Address | | | |
| Addressing mode | Manual  DHCP | | |
| IP/Network Mask | 192.168.179.2/255.255.255.0 | | |
| Administrative Access | | | |
| IPv4 | <input type="checkbox"/> HTTPS | <input type="checkbox"/> HTTP  | <input checked="" type="checkbox"/> PING |
| | <input type="checkbox"/> CAPWAP | <input checked="" type="checkbox"/> SSH | <input type="checkbox"/> SNMP |
| | <input type="checkbox"/> RADIUS Accounting | <input type="checkbox"/> FortiTelemetry | <input type="checkbox"/> FMG-Access |
| | | <input type="checkbox"/> FTM | |
| <input type="radio"/> DHCP Server | | | |
| Networked Devices | | | |
| Device Detection  | | | |
| Active Scanning  | | | |

9. Connect the FortiSandbox to the Security Fabric.

Allowing VM Internet access

1. Connect to Edge.
2. To create a policy that allows connections from the FortiSandbox to the Internet, go to **Policy & Objects > IPv4 Policy**.

| | |
|--------------------|---|
| Name | FortiSandbox-Internet |
| Incoming Interface | FortiSandbox-Internet (port13) |
| | + |
| Outgoing Interface | Internet (port9) |
| | + |
| Source | all |
| | + |
| Destination | all |
| | + |
| Schedule | always |
| Service | ALL |
| | + |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

3. Connect to FortiSandbox.
4. Go to **Scan Policy > General** and select **Allow Virtual Machines** to access external network through outgoing port3. Set **Gateway** to the IP address of port 13 on the FortiGate.

☒ Allow Virtual Machines to access external network through outgoing port3

| | |
|--|------------------------------|
| Status: | |
| Port3 IP: | 192.168.179.10/255.255.255.0 |
| Gateway: | 192.168.179.2 |
| <input type="checkbox"/> Disable SIMNET if Virtual Machines are not able to access external network through outgoing port3 | |
| DNS: | 208.91.112.53 |
| <input type="checkbox"/> Use Proxy | |

- Go to the **Dashboard** and locate the **System Information** widget. Verify that **VM Internet Access** has a green check mark beside it.

— System Information

| | |
|-----------------------|--|
| Unit Type | Standalone |
| Host Name | FSA1KD3A14000118 [Change] |
| Serial Number | FSA1KD3A14000118 |
| System Time | Fri Mar 2 16:11:25 2018 EST [Change] |
| Firmware Version | v2.4.1,build0261 (GA) [Update] |
| System Configuration | Last Backup: 2017-11-01 16:38 [Backup/Restore] |
| Current Administrator | admin |
| Uptime | 0 day(s) 1 hour(s) 20 minute(s) |
| Windows VM | ✓ [Upload License] |
| Microsoft Office | ⚠ [Upload License] |
| VM Internet Access | ✓ |

Adding FortiSandbox to the Security Fabric

- Connect to Edge.
- To add FortiSandbox to the Security Fabric, go to **Security Fabric > Settings**. Enable **Sandbox Inspection**.
- Make sure **FortiSandbox Appliance** is selected and set **Server** to the IP address of port 1 on the FortiSandbox.

☒ Sandbox Inspection

⚠ [No AntiVirus profile has enabled FortiSandbox inspection. Click to Check.](#)

| | | | |
|-------------------|-------------------------------|--------------------------|----------------------------|
| FortiSandbox type | FortiSandbox Appliance | FortiSandbox Cloud | Activate FortiCloud |
| Server | 192.168.65.20 | Test connectivity | |
| Notifier email | | | |

- Select **Test Connectivity**. An error message appears because Edge hasn't been authorized on the FortiSandbox.

FortiSandbox Server 192.168.65.20


Status Unreachable or not authorized

5. Edge, as the root FortiGate, pushes FortiSandbox settings to the other FortiGates in the Security Fabric. To verify this, connect to Accounting and go to **Security Fabric > Settings**.

Sandbox Inspection







No AntiVirus profile has enabled FortiSandbox inspection. [Click to Check.](#)

FortiSandbox type **FortiSandbox Appliance** FortiSandbox Cloud  **Activate FortiCloud**


Server

Notifier email

6. On the FortiSandbox, go to **Scan Input > Device**. The FortiGates in the Security Fabric (Edge, Accounting, Marketing, and Sales) are listed but the **Auth** column indicates that the devices are unauthorized.

| Device Name | Serial | Malicious | High | Medium | Low | Clean | Others | Malware Pkg | URL Pkg | Auth |
|--|------------------|-----------|------|--------|-----|-------|--------|-------------|---------|------|
|  Marketing | FG81EP4Q16002706 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | \$\$ |
|  Sales | FGT51E3U16001255 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | \$\$ |
|  Edge | FGT6HD3916806070 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | \$\$ |
|  Accounting | F140EP4Q17000149 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | \$\$ |

7. Select and edit **Edge**. Under **Permissions & Policies**, select **Authorized**.

| Device Status | |
|----------------------------------|---|
| Serial Number: | FGT6HD3916806070 |
| Alias: | Edge |
| IP: | 192.168.55.2 |
| Status: |  |
| Last Modified: | 2018-03-02 14:55:01 |
| Last Seen: | 2018-03-02 16:19:33 |
| Permissions & Policy | |
| Authorized: | <input checked="" type="checkbox"/> Last Changed 2018-03-02 14:55:01 |
| New VDOMs Inherit Authorization: | <input checked="" type="checkbox"/> |
| Email Settings | |
| Administrator Email: | |
| Send Notifications: | <input checked="" type="checkbox"/> |
| Send PDF Reports: | <input checked="" type="checkbox"/> |

- Repeat this for the other FortiGate devices.
- On Edge, go to **Security Fabric > Settings** and test the **Sandbox Inspection** connectivity again. Edge is now connected to the FortiSandbox.

| | |
|---------------------|--------------------|
| FortiSandbox Server | 192.168.65.20 |
| Status | Service is online. |

Adding sandbox inspection to security profiles

You can apply sandbox inspection with three types of security inspection: antivirus, web filter, and FortiClient compliance profiles. In this step, you add sandbox to all FortiGate devices in the Security Fabric individually, using the profiles that each FortiGate applies to network traffic.




In order to pass the **Advanced Threat Protection** check, you must add sandbox inspection to antivirus profiles for all FortiGate devices in the Security Fabric.

- Go to **Security Profiles > AntiVirus** and edit the **default** profile.
- Under **Inspection Options**, set **Send Files to FortiSandbox Appliance for Inspection** to **All Supported Files**.

3. Enable **Use FortiSandbox Database**, so that if the FortiSandbox discovers a threat, it adds a signature for that file to the antivirus signature database on the FortiGate.

| | |
|----------------|--|
| Name | <input type="text" value="default"/> |
| Comments | <input type="text" value="Scan files and block viruses."/> 29/255 |
| Scan Mode | <input type="button" value="Quick"/> <input checked="" type="button" value="Full"/> |
| Detect Viruses | <input checked="" type="button" value="Block"/> <input type="button" value="Monitor"/> |

APT Protection Options

| | |
|--|---|
| Treat Windows Executables in Email Attachments as Viruses | <input checked="" type="checkbox"/> |
| Send Files to FortiSandbox Appliance for Inspection | <input type="button" value="None"/> <input checked="" type="button" value="All Supported Files"/> |
| Do not submit files matching types | <input type="text" value="+"/> |
| Do not submit files matching file name patterns | <input type="text" value="+"/> |
| Use Virus Outbreak Prevention Database   | <input type="checkbox"/> |
| Use FortiSandbox Database  | <input checked="" type="checkbox"/> |
| Include Mobile Malware Protection | <input checked="" type="checkbox"/> |

4. Go to **Security Profiles > Web Filter** and edit the **default** profile.
5. Under **Static URL Filter**, enable **Block malicious URLs discovered by FortiSandbox**. If the FortiSandbox discovers a threat, the URL that threat came from is added to the list of URLs that are blocked by the FortiGate.

Name

Comments 22/255

☒ FortiGuard category based filter

Show ☐ All

- ☒ Local Categories
- ☐ Potentially Liable
- ☐ Adult/Mature Content
- ☒ Bandwidth Consuming
- ☐ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business
- ☐ Unrated

☐ Static URL Filter

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☒

Web Content Filter ☐



- Go to **Security Profiles > FortiClient Compliance Profiles** and edit the **default** profile. Enable **Security Posture Check**.
- Enable **Realtime Protection** and **Scan with FortiSandbox**.

☒ Security Posture Check

Realtime Protection ☒

Up-to-date signatures ☐

Scan with FortiSandbox ☒

Third party AntiVirus on Windows   ☐

Web Filter ☐

Application Firewall ☐

Non-compliance action

Results

1. If a FortiGate in the Security Fabric discovers a suspicious file, it sends the file to the FortiSandbox. You can view information about scanned files on either the FortiGate that sent the file or the FortiSandbox. On one of the FortiGate devices, go to the **Dashboard** and locate the **Advanced Threat Protection Statistics** widget. This widget shows files that both the FortiGate and FortiSandbox scan.

Advanced Threat Protection Statistics



| | |
|---------------------------|-------|
| FortiGate Scanned Files | 1,887 |
| Malicious | 1 |
| Zero-Day Malware Variants | 0 |
| Suspicious | 0 |
| Clean | 1,886 |

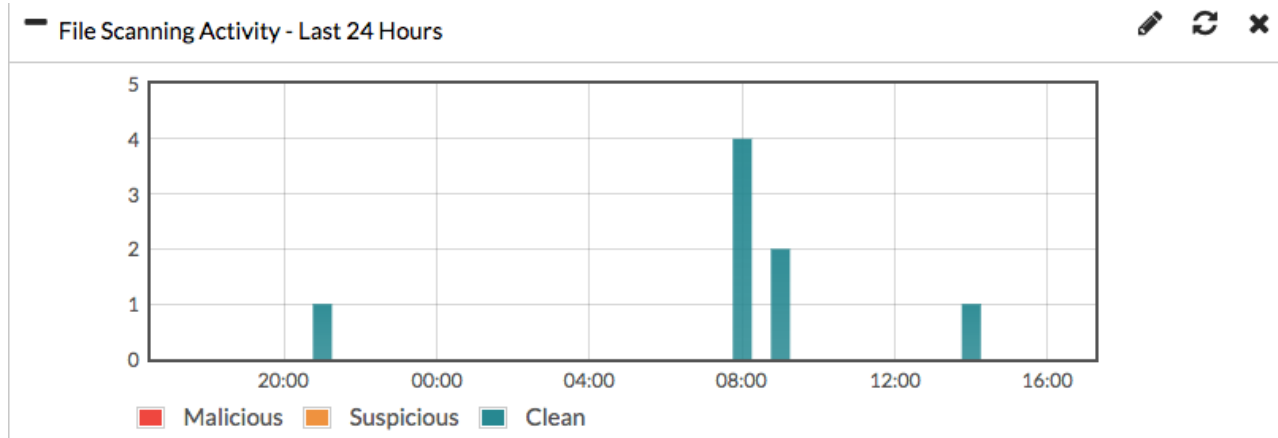


| | |
|----------------------------|---|
| FortiSandbox Scanned Files | 8 |
| Malicious | 0 |
| Suspicious - High Risk | 0 |
| Suspicious - Med/Low Risk | 0 |
| Clean | 8 |

2. On the FortiSandbox, go to **System > Status** and view the **Scanning Statistics** widget for a summary of scanned files.

| Scanning Statistics - Last 24 Hours | | | | | | | |
|-------------------------------------|---------|-----------|-----------|---------|---------|-----|-----|
| Rating | Sniffer | Device(s) | On Demand | Network | Adapter | URL | All |
| Malicious | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - High Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - Medium Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - Low Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clean | 0 | 8 | 0 | 0 | 0 | 0 | 8 |
| Other | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Processed | 0 | 8 | 0 | 0 | 0 | 0 | 8 |
| Pending | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Processing | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 0 | 8 | 0 | 0 | 0 | 0 | 8 |

3. You can also view a timeline of scanning in the **File Scanning Activity** widget.



4. On Edge, go to **Security Fabric > Security Rating** and run a rating. When it is finished, select the **All Results** view.

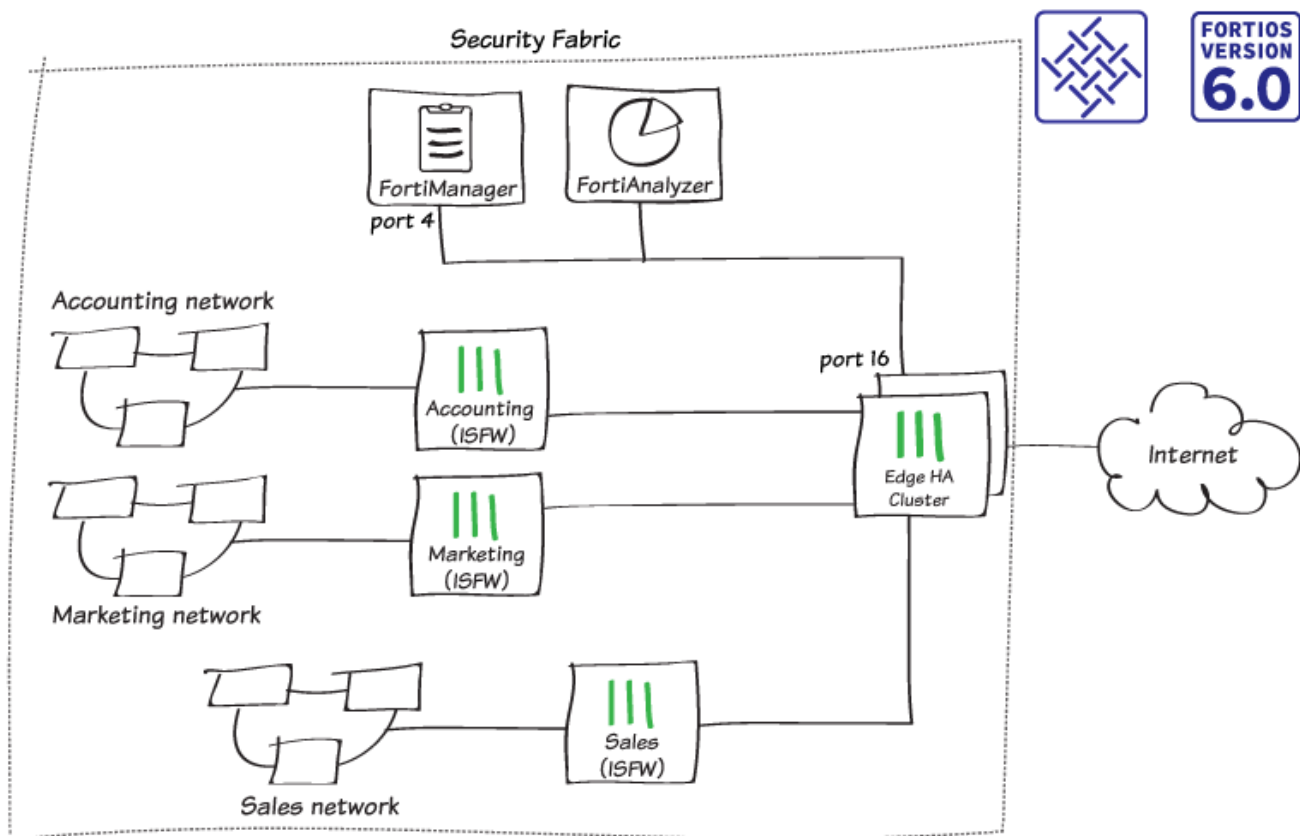
In the example, all four FortiGate devices in the Security Fabric pass the **Advanced Threat Protection** check and the **Security Rating Score** increases by 9.7 points for each FortiGate.

Advanced Threat Protection

Suspicious files should be submitted to FortiSandbox Appliance/FortiSandbox Cloud for inspection.

| | |
|---------------|------|
| Edge2-Primary | +9.7 |
| Accounting2 | +9.7 |
| Marketing2 | +9.7 |
| Sales2 | +9.7 |

FortiManager in the Fortinet Security Fabric



In this recipe, you add a FortiManager to the Security Fabric. This simplifies network administration because you manage all of the FortiGate devices in your network from the FortiManager.

In this example, you add the FortiManager to an existing Security Fabric, with an HA cluster called Edge as the root FortiGate and three internal FortiGates: Accounting, Marketing, and Sales. Network resources, such as a FortiManager, are located on the subnet 192.168.65.x.

Connecting the FortiManager


In this example, port 16 on Edge connects to port 4 on the FortiManager.

1. To configure the interface on the root FortiGate, connect to Edge, go to **Network > Interfaces**, and edit **port 16**.
2. Configure **Administrative Access** to allow **FMG-Access** and **FortiTelemetry**.


Administrative Access

| | | | | |
|------|--|---|--|--|
| IPv4 | <input type="checkbox"/> HTTPS | <input type="checkbox"/> HTTP ⓘ | <input checked="" type="checkbox"/> PING | <input checked="" type="checkbox"/> FMG-Access |
| | <input type="checkbox"/> CAPWAP | <input checked="" type="checkbox"/> SSH | <input type="checkbox"/> SNMP | <input type="checkbox"/> FTM |
| | <input type="checkbox"/> RADIUS Accounting | | <input checked="" type="checkbox"/> FortiTelemetry | |

3. To configure the interface on the FortiManager, connect to the FortiManager, go to **System Settings > Network**, select **All Interfaces**, and edit **port 4**.
4. Set **IP Address/Netmask** to an internal IP address (in the example, *192.168.65.30/255.255.255.0*).

| | |
|----------------------------|--|
| Name | port4 |
| Alias | 192.168.65.30  |
| IP Address/Netmask | 192.168.65.30/255.255.255.0 |
| IPv6 Address | ::/0 |
| Administrative Access | <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service |
| IPv6 Administrative Access | <input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service |
| Service Access | <input checked="" type="checkbox"/> FortiGate Updates <input type="checkbox"/> Web Filtering |
| Status | Enable Disable |

5. Select **Routing Table** and add a default route for port 4. Set **Gateway** to the IP address of port 16 on Edge.


| | |
|---------------------|---|
| ID | 1 |
| Destination IP/Mask | 0.0.0.0/0.0.0.0  |
| Gateway | 192.168.65.2 |
| Interface | port4 ▼ |

6. If you haven't already done so, connect the FortiManager and Edge.

















Allowing Internet access

In order to communicate with FortiGuard, the FortiManager requires Internet access.

1. To create an address for the FortiManager, connect to Edge, go to **Policy & Objects > Addresses**, and create a new address.


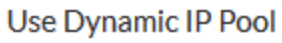
| | |
|----------------------------|---|
| Category | Address Multicast Address |
| Name | FortiManager-address |
| Color |  Change |
| Type | Subnet ▼ |
| Subnet / IP Range | 192.168.65.30 |
| Interface | <input type="checkbox"/> any ▼ |
| Show in Address List | <input checked="" type="checkbox"/> |
| Static Route Configuration | <input type="checkbox"/> |
| Comments | <input type="text"/> 0/255 |

2. To allow the FortiManager to access the Internet, go to **Policy & Objects > IPv4 Policy**, and create a new policy.

| | |
|--|---|
| Name  | FortiManager-Internet |
| Incoming Interface |  Network-Resources (port16)  + |
| Outgoing Interface |  Internet (port9)  + |
| Source |  FortiManager-address  + |
| Destination |  all  + |
| Schedule |  always  |
| Service |  ALL  + |
| Action |  ACCEPT  DENY  LEARN |



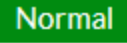
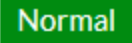



Firewall / Network Options

NAT 

IP Pool Configuration  

Configuring central management

1. To enable central management, connect to Edge, go to **Security Fabric > Settings**, and enable **Central Management**.
2. Set **Type** to **FortiManager**, **Mode** to **Normal**, and set **IP/Domain Name** to the IP address of port 4 on the FortiManager.

| | |
|--|---|
|  Central Management | |
| Type |   |
| Mode |   |
| IP/Domain Name | 192.168.65.30  |
| Status |  Not Managed |

- After you select **Apply**, a message appears stating that the FortiManager received the message and Edge is waiting for management confirmation.

Awaiting management confirmation from FortiManager administrator. Once confirmed full control of this FortiGate will be granted to FMG3HE3R17000019 at "192.168.65.30".

OK

- Edge, as the root FortiGate, pushes FortiManager settings to the other FortiGate devices in the Security Fabric. To verify this, connect to Accounting and go to **Security Fabric > Settings**.

☐ Central Management

Central management settings will be retrieved from the root FortiGate in the Security Fabric.

Type

FortiManager FortiCloud

Mode

Normal Backup

IP/Domain Name

192.168.65.30



Status

Waiting for FortiManager to process registration.

- To confirm the management connection, connect to the FortiManager and go to **Device Manager > Unregistered Devices**. Select the FortiGate devices and select **+ Add**.

| <input type="checkbox"/> | ▲ Device Name | Model | Management Mode | Serial Number | Connecting IP | Firmware Version |
|--------------------------|---------------|--------------------|-------------------------|------------------|---------------|--------------------------------|
| <input type="checkbox"/> | Accounting2 | FortiGate-140E-POE | Configuration & Logging | F140EP4Q17000089 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |
| <input type="checkbox"/> | Edge2-Primary | FortiGate-600D | Configuration & Logging | FGT6HD3916806070 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |
| <input type="checkbox"/> | Marketing2 | FortiGate-81E-POE | Configuration & Logging | FG81EP4Q16002749 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |
| <input type="checkbox"/> | Sales2 | FortiGate-51E | Configuration & Logging | FGT51E3U16002482 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |


- Add the FortiGate devices to the FortiManager.

Add Device

| Device Name | Credential | Assign New Device Name |
|------------------|--|--|
| FGT6HD3916806070 | <input type="text" value="admin"/> | <input type="text" value="Edge2-Primary"/> |
| FG81EP4Q16002749 | <input type="text" value="admin"/> ... | <input type="text" value="Marketing2"/> |
| FGT51E3U16002482 | <input type="text" value="admin"/> ... | <input type="text" value="Sales2"/> |
| F140EP4Q17000089 | <input type="text" value="admin"/> ... | <input type="text" value="Accounting2"/> |

7. Connect to Edge. A warning message appears stating that the FortiGate is now managed by a FortiManager. Select **Login Read-Only**.

This FortiGate is currently managed by a FortiManager device


 All changes should be performed from a FortiManager to avoid conflict. How would you like to proceed?

8. Go to **Security Fabric > Settings**. Under **Central Management**, the **Status** is now **Registered on FortiManager**.

☒ **Central Management**

Type FortiManager FortiCloud

Mode Normal Backup

IP/Domain Name

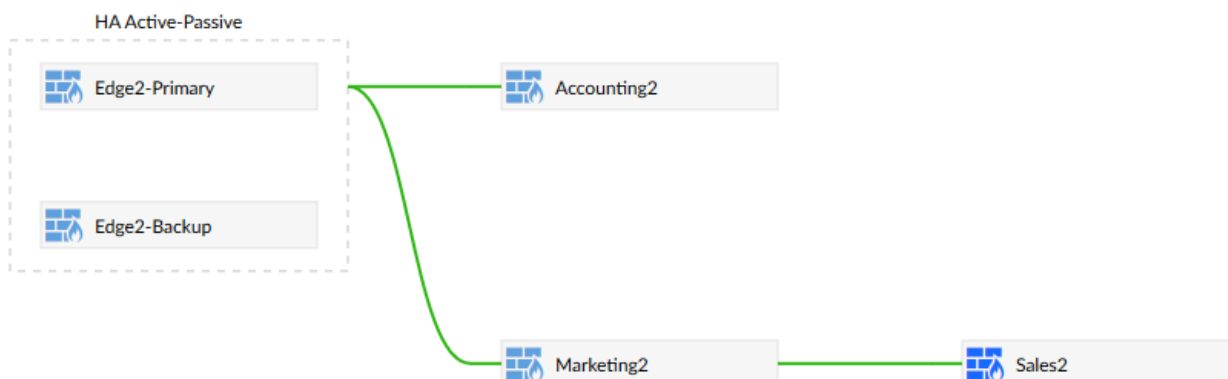
Status ↑ **Registered on FortiManager.**

Results

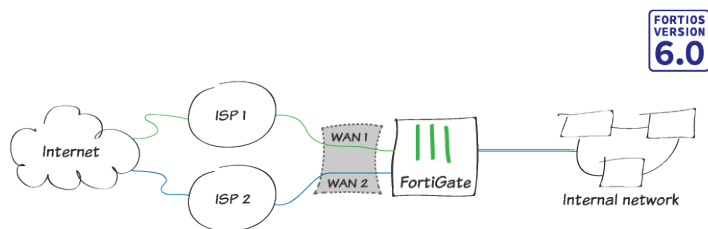
1. The FortiGate devices are on the **Managed FortiGate** list and appear as part of a Security Fabric group. The * beside Edge indicates that it's the root FortiGate in the Security Fabric.

| <input type="checkbox"/> ▲ Device Name | Config Status | Policy Package Status | Host Name | IP Address | Platform |
|---|----------------|-----------------------|---------------|--------------|--------------------|
| <input type="checkbox"/> FGT6HD3916806070 | | | | | |
| <input type="checkbox"/> ▲ Accounting2 | ✓ Synchronized | ▲ Never installed | Accounting2 | 192.168.65.2 | FortiGate-140E-POE |
| <input type="checkbox"/> ▲ Edge2-Primary* | ✓ Auto-update | ▲ Never installed | Edge2-Primary | 192.168.65.2 | FortiGate-600D |
| <input type="checkbox"/> ▲ Marketing2 | ✓ Synchronized | ▲ Never installed | Marketing2 | 192.168.65.2 | FortiGate-81E-POE |
| <input type="checkbox"/> ▲ Sales2 | ✓ Synchronized | ▲ Never installed | Sales2 | 192.168.65.2 | FortiGate-51E |

- Right-click on any of the FortiGate devices and select **Fabric Topology**. The topology of the Security Fabric is displayed.

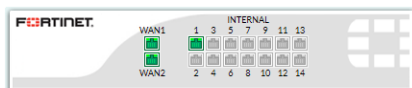


Redundant Internet with SD-WAN



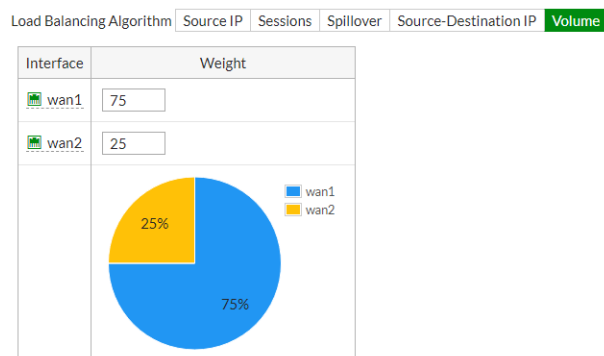
This recipe provides an example of how you can configure redundant Internet connectivity for your network using SD-WAN. This allows you to load balance your Internet traffic between multiple ISP links and provides redundancy for your network's Internet connection if your primary ISP is unavailable.

- Connect the FortiGate to your ISP devices by connecting the Internet-facing (WAN) ports on the FortiGate to your ISP devices. Connect WAN1 to the ISP that you want to use for most traffic, and connect WAN2 to the other ISP.



- Before you can configure FortiGate interfaces as SD-WAN members, you must remove or redirect existing configuration references to those interfaces in routes and security policies. This includes the default Internet access policy that's included with many FortiGate models. Note that after you remove the routes and security policies, traffic can't reach the WAN ports through the FortiGate. Redirecting the routes and policies to reference other interfaces avoids your having to create them again later. After you configure SD-WAN, you can reconfigure the routes and policies to reference the SD-WAN interface. Remove existing configuration references to interfaces:

- a. Go to *Network > Static Routes* and delete any routes that use WAN1 or WAN2.
- b. Go to *Policy & Objects > IPv4 Policy* and delete any policies that use WAN1 or WAN2.
3. Create the SD-WAN interface:
 - a. Go to *Network > SD-WAN* and set *Status* to *Enable*.
 - b. Under *SD-WAN Interface Members*, select + and select *wan1*. Set the *Gateway* to the default gateway for this interface. This is usually the default gateway IP address of the ISP that this interface is connected to. Repeat these steps to add *wan2*.
 - c. Go to *Network > Interfaces* and verify that the virtual interface for *SD-WAN* appears in the interface list. You can expand SD-WAN to view the ports that are included in the SD-WAN interface.
4. Configure SD-WAN load balancing:
 - a. Go to *Network > SD-WAN Rules* and edit the rule named *sd-wan*.
 - b. In the *Load Balancing Algorithm* field, select *Volume*, and prioritize WAN1 to serve more traffic. In the example, the ISP connected to WAN1 is a 40Mb link, and the ISP connected to WAN2 is a 10Mb link, so we balance the weight 75% to 25% in favor of WAN1.



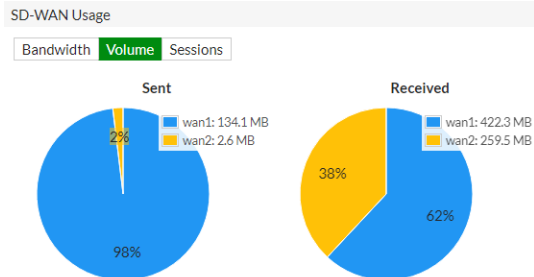
5. Create a static route for the SD-WAN interface:
 - a. Go to *Network > Static Routes* and create a new route.
 - b. In the *Destination* field, select *Subnet*, and leave the destination IP address and subnet mask as 0.0.0.0/0.0.0.0.
 - c. In the *Interface* field, select the SD-WAN interface from the dropdown list.
 - d. Ensure that *Status* is set to *Enable*. If you previously removed or redirected existing references in routes to interfaces that you wanted to add as SD-WAN interface members, you can now reconfigure those routes to reference the SD-WAN interface.
6. Configure a security policy that allows traffic from your organization's internal network to the SD-WAN interface.
 - a. Go to *Policy & Objects > IPv4 Policy* and create a new policy.
 - b. Set *Incoming Interface* to the interface that connects to your organization's internal network and set *Outgoing Interface* to the SD-WAN interface.
 - c. Enable *NAT* and apply *Security Profiles* as required.
 - d. Enable *Log Allowed Traffic for All Sessions* to allow you to verify the results later. If you previously removed or redirected existing references in security policies to interfaces that you wanted to add as SD-WAN interface members, you can now reconfigure those policies to reference the SD-WAN interface.
7. You can configure link health monitoring to verify the health and status of the links that make up the SD-WAN link:
 - a. Go to *Network > Performance SLA* and create a new performance SLA.
 - b. Set the *Protocol* for the health checks. In the *Server* fields, enter the IP addresses of up to two servers that you want to use to test the health of each SD-WAN member interface.* In the *Participants* field, select the SD-WAN interface members that you want the health check to apply to.
 - c. You can view link quality measurements on the *Performance SLA* page. The table displays information about configured health checks. The values in the *Packet Loss*, *Latency*, and *Jitter* columns apply to the server that

the FortiGate is using to test the health of the SD-WAN member interfaces. The green (up) arrows indicate only that the server is responding to the health checks, regardless of the packet loss, latency, and jitter values, and do not indicate that the health checks are being met.

| <div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> </div> | | | | | | |
|--|--------------------|------------------------------|----------------------------------|--------------------------------|-------------------|--------------------|
| Name | Detect Server | Packet Loss | Latency | Jitter | Failure Threshold | Recovery Threshold |
| WAN_Ping_SLA | 8.8.8.8 8.8.4.4 | wan1: 0.00 % wan2: 0.00 % | wan1: 10.67 ms wan2: 10.67 ms | wan1: 0.38 ms wan2: 0.38 ms | 5 | 5 |

8. View the results:

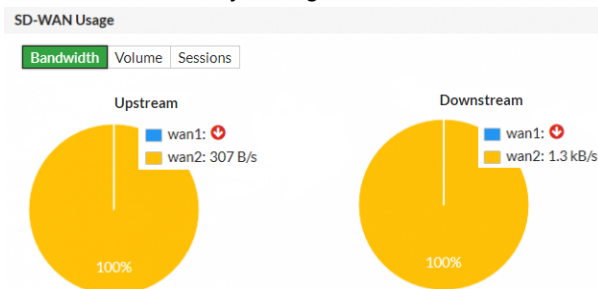
- Browse the Internet using a computer on your internal network and then go to *Network > SD-WAN*.
- In the *SD-WAN Usage* section, you can see the bandwidth, volume, and sessions for traffic on the SD-WAN interfaces.



- Go to *Monitor > SD-WAN Monitor* to view the number of sessions, bit rate, and more information for each interface.
9. To test failover of the redundant Internet configuration, you must simulate a failed Internet connection to one of the ports. Do so by physically disconnecting the Ethernet cable connected to WAN1:
- Verify that users still have Internet access by navigating to *Monitor > SD-WAN Monitor*. The *Upload* and *Download* values for WAN1 show that traffic is not going through that interface.

| Interface | Status | Sessions | Upload | Download |
|-----------|--------|----------|---------|-----------|
| sd-wan | | | | |
| wan1 | | 16 | 0 B/s | 0 B/s |
| wan2 | | 103 | 242 B/s | 1.24 kB/s |

- Go to *Network > SD-WAN*. In the *SD-WAN Usage* section, you can see that bandwidth, volume, and sessions have diverted entirely through WAN2.



- Users on the internal network should not notice the WAN1 failure. Likewise, if you are using the WAN1 gateway IP address to connect to the admin dashboard, nothing should change from your perspective. It appears as though you are still connecting through WAN1. After you verify successful failover, reconnect the WAN1 Ethernet cable.

Blocking malicious domains using threat feeds

This example uses a domain name threat feed and FortiGate DNS filtering to block malicious domains. The text file in this example is a list of gambling site domain names.

Threat feeds allow you to dynamically import external block lists in the form of a text file into your FortiGate. These text files, stored on an HTTP server, can contain a list of web addresses or domains. You can use threat feeds to deny access to a source or destination IP address in Web Filter and DNS Filter profiles, SSL inspection exemptions, and as a source/destination in proxy policies. You can use Fabric connectors for FortiGates that do not belong to a Fortinet Security Fabric.

1. Create an external block list. The external block list should be a plain text file with one domain name per line. The use of simple wildcards is supported. You can create your own text file or download it from an external service. Upload the text file to the HTTP file server.

```
100casinopicks.com
100kcasino.com
100pour100-gratuit.com
1010casino.com
123gambling.com
123onlinecasino.com
```

2. Configure the threat feed:
 - a. In FortiOS, go to *Security Fabric > Fabric Connectors*. Click *Create New*.
 - b. Under *Threat Feeds*, select *Domain Name*.
 - c. Configure the *Name*, *URI of external resource*, and *Refresh Rate* fields. In the *URI of external resource* field, enter the location of the text file on the HTTP file server. By default, the FortiGate rereads the file and uploads any changes every five minutes.

Threat Feeds

Domain Name

Connector Settings

Name: gambling-domains

URI of external resource: http://172.25.175.222/external-resour

Refresh Rate: 5

Comments: o2ss

Last Update: 2018/08/07 09:19:47 View Entries

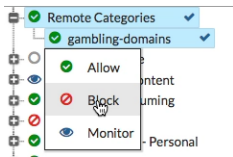
Status: OK Cancel

- d. Click *View Entries* to see the text file's domain list.

| Domain Name Threat Feed "gambling-domains" | |
|--|-----------------------|
| Search | 2,004 Valid 0 Invalid |
| Entry | Validity |
| 100casinopicks.com | Valid |
| 100kcasino.com | Valid |
| 100pour100-gratuit.com | Valid |
| 1010casino.com | Valid |
| 123gambling.com | Valid |
| 123onlinecasino.com | Valid |

- e. Click *OK*.
3. Add the threat feed to the DNS filter:
 - a. Go to *Security Profiles > DNS Filter*.
 - b. Scroll to the list of preconfigured FortiGuard filters.

- c. The resource file uploaded earlier is listed under *Remote Categories*. Set the action for this category to *Block*.



4. Configure the outgoing Internet policy:

- a. Go to *Policy & Objects > IPv4 Policy*.
- b. Under *Security Profiles*, enable *DNS Filter*.
- c. From the *SSL Inspection* dropdown list, select an SSL inspection profile.

5. View the results:

- a. Visit a domain on the external resource file. This example visits 123gambling.com. A *Web Page Blocked!* message appears.



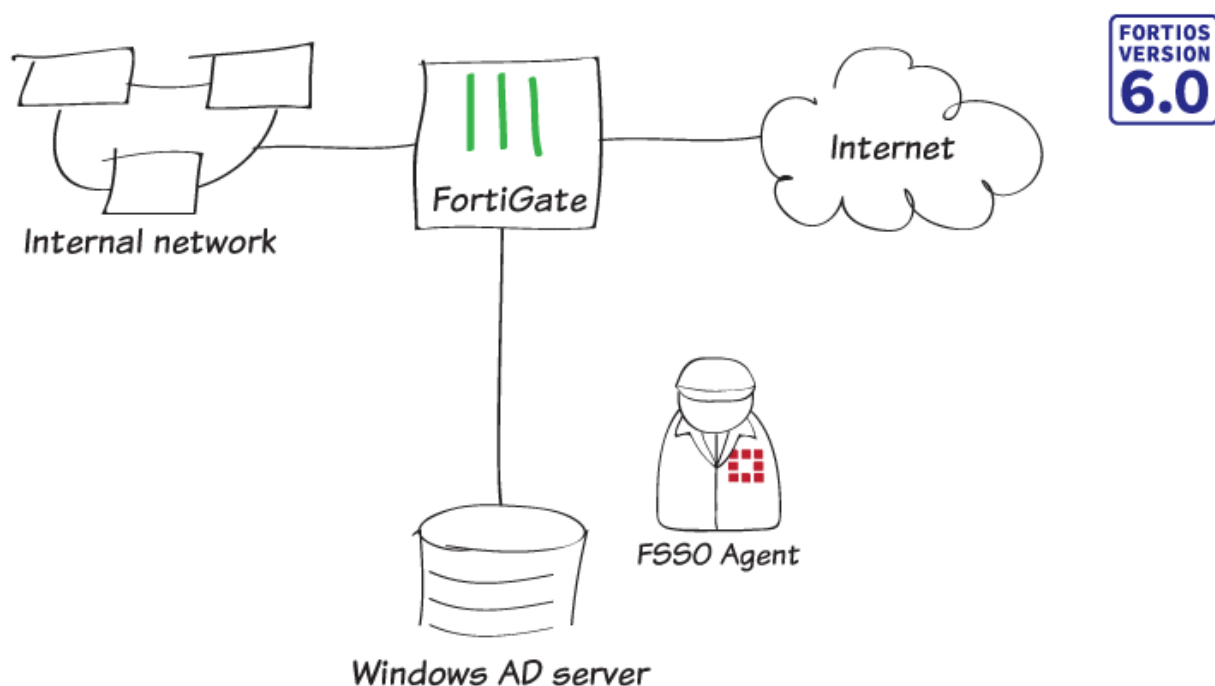
- b. In FortiOS, go to *Log & Report > DNS Query*. The logs show that the 123gambling.com domain belongs to a blocked category.

| # | Date/Time | DNS Type | Source | Domain Name | Query Type | Policy | Message |
|---|-----------|--------------|--------------------------|--------------------|------------|--------|---|
| 1 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | 123gambling.com | A | 1 | Domain belongs to a denied category in policy |
| 2 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | 123gambling.com | A | 1 | Domain belongs to a denied category in policy |
| 3 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | www.richcasino.com | A | 1 | Domain belongs to a denied category in policy |
| 4 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | www.richcasino.com | A | 1 | Domain belongs to a denied category in policy |

Authentication

This section contains information about authenticating users and devices.

Agent-based FSSO for Windows AD



In this recipe, you use agent-based Fortinet single sign-on (FSSO) to allow users to login to the network once with their Windows AD credentials and seamlessly access all appropriate network resources.

This example uses the FSSO agent in advanced mode. The main difference between advanced and standard mode is the naming convention used when referring to username information. Standard mode uses Windows convention: Domain\Username. Advanced mode uses LDAP convention: CN=User, OU=Name, DC=Domain.

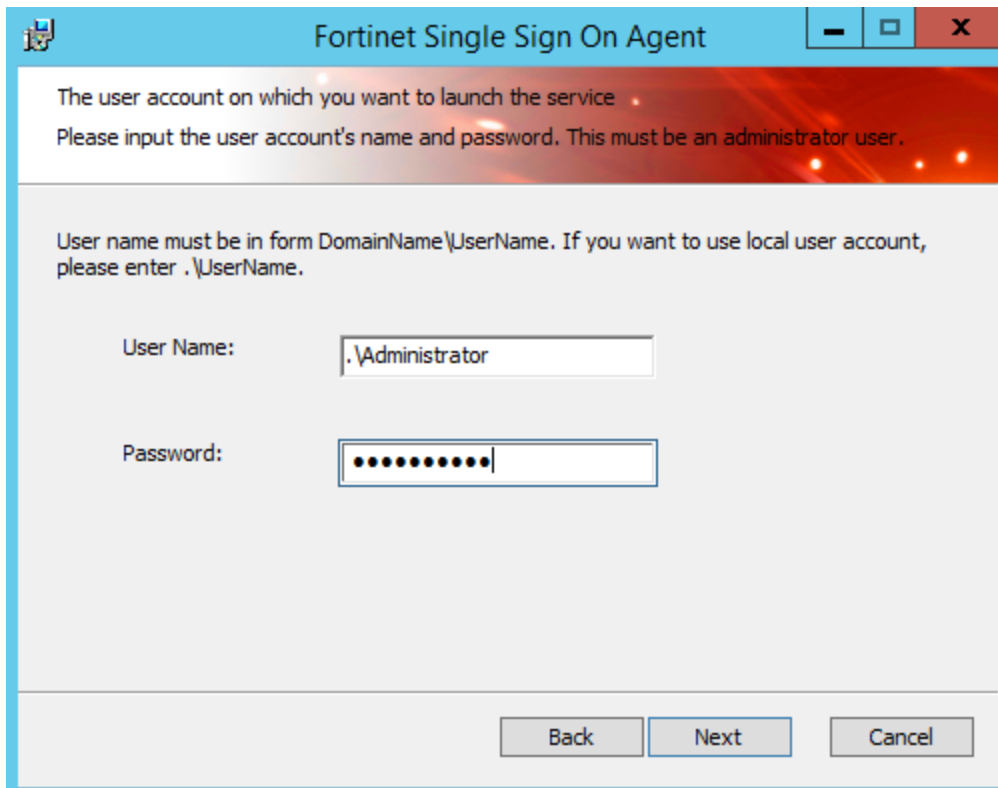
Standard mode supports device names up to 15 characters long. Advanced mode supports device names longer than 15 characters.

Advanced mode is required for multi-domains environments.

Installing the FSSO agent

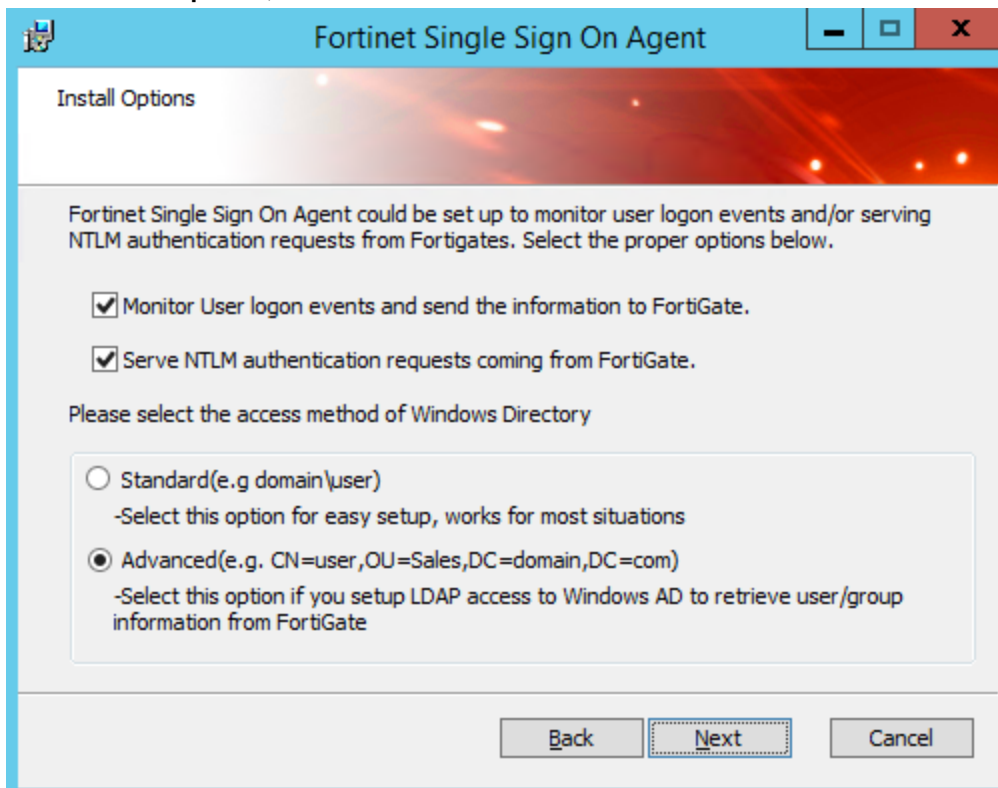
Connect to the Windows AD server and download the FSSO agent from [Fortinet Support](#).

1. To install the agent, open the installer file and use the installation wizard.
2. Set a **User Name** and **Password** for the FSSO domain administrator.



The screenshot shows the 'Fortinet Single Sign On Agent' installation window. The title bar is blue with the Fortinet logo and window controls. The main area has a red header with the text: 'The user account on which you want to launch the service' and 'Please input the user account's name and password. This must be an administrator user.' Below this, a grey box contains instructions: 'User name must be in form DomainName\UserName. If you want to use local user account, please enter .\UserName.' There are two input fields: 'User Name:' with the text '.\Administrator' and 'Password:' with masked characters. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

3. For the **Install Options**, select **Advanced** to use advanced mode instead of standard.



The screenshot shows the 'Fortinet Single Sign On Agent' installation window at the 'Install Options' step. The title bar is blue with the Fortinet logo and window controls. The main area has a red header with the text: 'Install Options'. Below this, a grey box contains the text: 'Fortinet Single Sign On Agent could be set up to monitor user logon events and/or serving NTLM authentication requests from Fortigates. Select the proper options below.' There are two checked checkboxes: 'Monitor User logon events and send the information to FortiGate.' and 'Serve NTLM authentication requests coming from FortiGate.' Below these is the text: 'Please select the access method of Windows Directory'. There are two radio button options: 'Standard(e.g domain\user)' with the description '-Select this option for easy setup, works for most situations' and 'Advanced(e.g. CN=user,OU=Sales,DC=domain,DC=com)' with the description '-Select this option if you setup LDAP access to Windows AD to retrieve user/group information from FortiGate'. The 'Advanced' option is selected. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

4. After installing the FSSO agent, run **Install DC Agent**.
5. Set the **Collector Agent IP address** and the **Collector Agent listening port**.

Fortinet Single Sign On Agent - Install DC Agent

Welcome to the DC Agent installation wizard. This wizard will install DC Agent on the Domain Controllers in your domain.

First please confirm the Collector Agent address and listening port.

Collector Agent

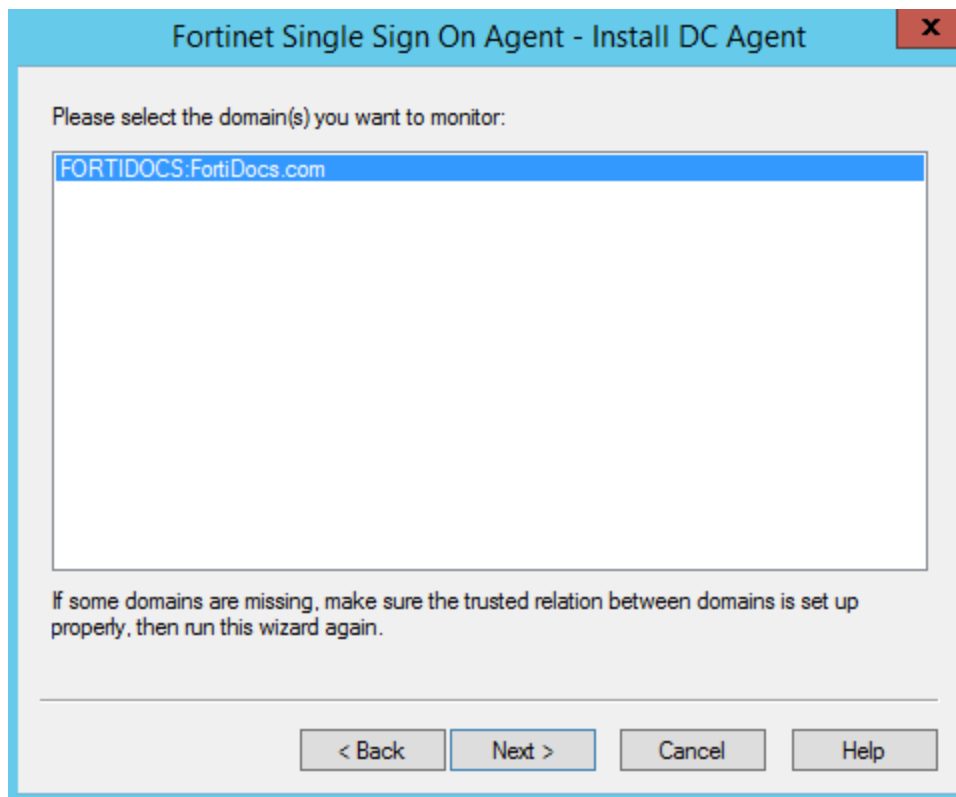
Collector Agent IP address: 172.25.176.140

Collector Agent listening port: 8002

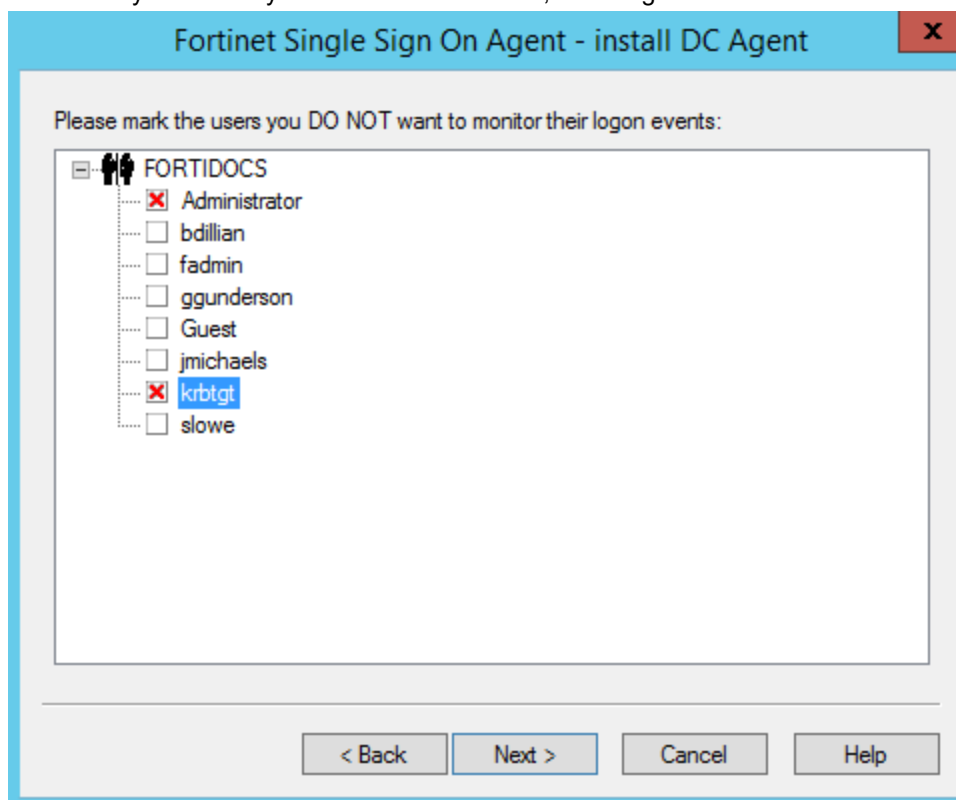
Note: You need to have administrator access to the domain controller in order to install the DC Agent!

< Back Next > Cancel Help

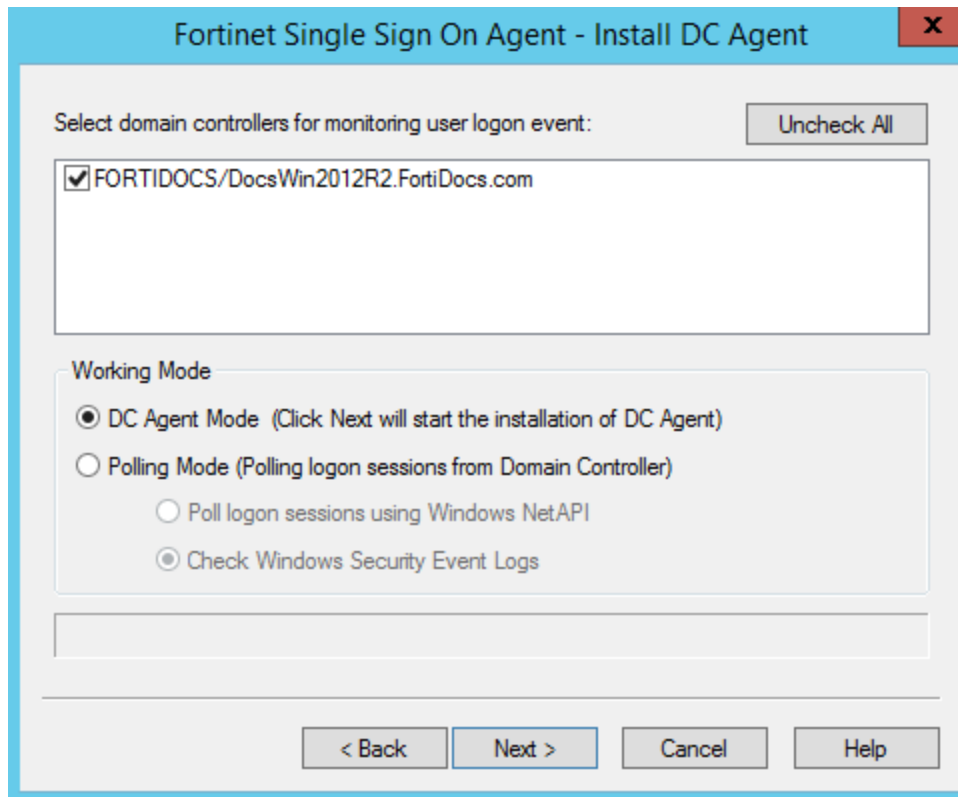
6. Select the domain you wish to monitor.



7. Exclude any users that you don't want to monitor, including the administrator.



8. Set **Working Mode** to **DC Agent Mode**



9. Restart your server to apply all changes.

Configuring the FSSO agent

1. To configure the settings for your network, open the FSSO agent. You can use the default for most settings.

2. Select **Set Directory Access Information**. Set **AD access mode** to **Advanced**.

Setting up your FortiGate for FSSO

Because you have installed FSSO in advanced mode, you need to configure LDAP to use with FSSO.

1. To configure the LDAP service, go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter all information about your LDAP server. Select **Test Connectivity**. If your information is correct, **Connection status** is **Successful**.

| | | | |
|--|---|-----------|---------|
| Name | FortiDocs | | |
| Server IP/Name | 172.25.176.140 | | |
| Server Port | 389 | | |
| Common Name Identifier | cn | | |
| Distinguished Name | DC=FortiDocs,DC=com | Browse | |
| Bind Type | Simple | Anonymous | Regular |
| Username | ator,CN=Users,DC=FortiDocs,DC=com | | |
| Password | <input type="password"/> <input type="button" value="eye"/> | | |
| Secure Connection | <input type="checkbox"/> | | |
| <input type="button" value="Test Connectivity"/> | | | |
| <input type="button" value="Test User Credentials"/> | | | |

3. Create a Fabric Connector to the FSSO agent by going to **Security Fabric > Fabric Connectors** and select **+ Create New**.
4. Under **SSO/Identity**, select **Fortinet Single Sign-On Agent**.
5. Set the **Name** and enter the IP address and password for the **Primary FSSO Agent**.
6. Set **Collector Agent AD access mode** to **Advanced** and set **LDAP Server** to the new LDAP service.

SSO/Identity



Fortinet Single
Sign-On Agent

Connector Settings

| | | | |
|--------------------------------|----------------|----------|---|
| Name | FortiDocs | | |
| Primary FSSO Agent | 172.25.176.140 | - | <input type="password"/> <input type="button" value="+"/> |
| Collector Agent AD access mode | Standard | Advanced | |
| LDAP Server | FortiDocs ▼ | | |








7. Your FortiGate displays information retrieved from the AD server. Select **Groups**, then right-click the FSSO group and select **+ Add Selected**.
8. Select **Selected**.
The FSSO group is shown.

| Users | Groups | Organizational Units | Selected |
|---|---|----------------------------|----------|
| Search | | Q | |
| ID | Name | | |
| Domain Controllers | Domain Controllers | | |
| Domain Guests | Domain Guests | | |
| Domain Users | Domain Users | | |
| Enterprise Admins | Enterprise Admins | | |
| Enterprise Read-only Domain Controllers | Enterprise Read-only Domain Controllers | | |
| FortiDocs | FortiDocs | | |
| Group Policy Creator Owners | Group Policy Creator Owners | + Add Selected | |
| Protected Users | Protected Users | | |
| RAS and IAS Servers | RAS and IAS Servers | | |
| Read-only Domain Controllers | Read-only Domain Controllers | | |
| Schema Admins | Schema Admins | | |
| WinRMRemoteWMIUsers_ | WinRMRemoteWMIUsers_ | | |
| | | << < 1 /1 > >> [Total: 20] | |

- To create a user group for FSSO users, go to **User & Device > User Groups** and select **Create New**.
- Enter a group **Name** and set **Type** to **Fortinet Single Sign-On (FSSO)**. Add the FSSO users to **Members**.

| | |
|---------|--|
| Name | FortiDocs_FSSO |
| Type | Firewall Fortinet Single Sign-On (FSSO) RADIUS Single Sign-On (RSSO) Guest |
| Members | CN=FortiDocs,CN=Users,DC=FortiDocs + |

- To create a policy for FSSO users, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
- For **Source**, set **User** to the FSSO user group.

| | | | |
|--------------------|---|---|---|
| Name ⓘ | Internet-FSSO | | |
| Incoming Interface |  port1 | + | ✕ |
| Outgoing Interface |  wan1 | + | ✕ |
| Source |  all  FortiDocs_FSSO | + | ✕ |
| Destination |  all | + | ✕ |
| Schedule |  always ▼ | | |
| Service |  ALL | + | ✕ |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN <input type="checkbox"/> IPsec | | |

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Results

Log into a computer on the domain and access the Internet. The FortiGate uses FSSO for authentication and doesn't require your credentials to be entered again.



On the FortiGate, go to **Monitor > Firewall User Monitor** and select **Show all FSSO Logons**.

Refresh

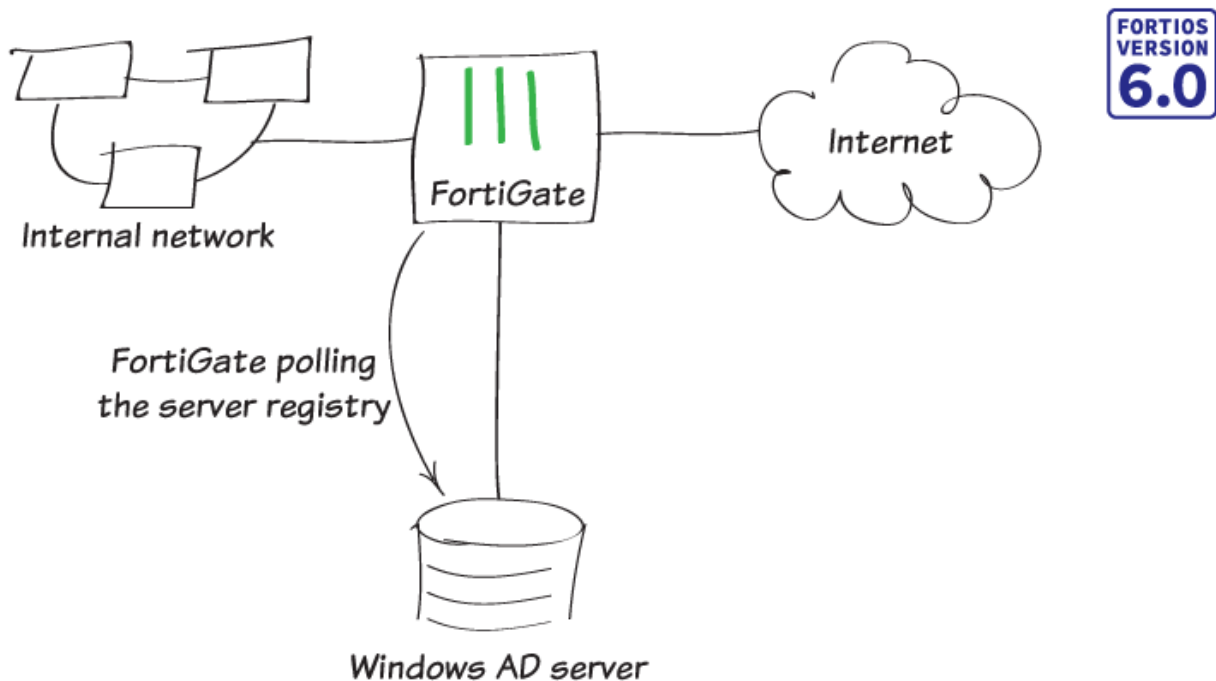
Deauthenticate

Show all FSSO Logons

Search

| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|-----------|--|-----------------------------|--------------|---------------------------------|---|
| SLOWE |  FortiDocs_FSSO | 4 minute(s) and 9 second(s) | 192.168.10.2 | 34.35 MB <div><div></div></div> |  Fortinet Single Sign-On |

FSSO in polling mode for Windows AD



In this recipe, you use Fortinet single sign-on (FSSO) in polling mode to allow users to log in to the network once with their Windows Active Directory (AD) credentials and seamlessly access all appropriate network resources.

Creating a Fabric Connector

1. To configure the LDAP service, go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter all information about your LDAP server. Select **Test Connectivity**. If your information is correct, **Connection status** is **Successful**.

| | |
|------------------------------------|--|
| Name | FortiDocs |
| Server IP/Name | 172.25.176.140 |
| Server Port | 389 |
| Common Name Identifier | cn |
| Distinguished Name | DC=FortiDocs,DC=com Browse |
| Bind Type | Simple <input type="radio"/> Anonymous <input type="radio"/> Regular <input checked="" type="radio"/> |
| Username | ator,CN=Users,DC=FortiDocs,DC=com |
| Password | •••••••• 👁 |
| Secure Connection | <input type="checkbox"/> |
| Test Connectivity | |
| Test User Credentials | |

3. To create a Fabric Connector, go to **Security Fabric > Fabric Connectors** and select **Create New**.

- Under **SSO/Identity**, select **Poll Active Directory Server**.
- Set the **Server IP/Name** and enter the credentials for the administrator account. Set **LDAP Server** to the new LDAP service.

SSO/Identity

Poll Active
Directory
Server

Connector Settings

Server IP/Name

User

Password

LDAP Server

Enable Polling ☒

Users/Groups

- Your FortiGate displays information retrieved from the AD server. Select **Groups**, then right-click the FSSO group and select **+ Add Selected**.
- Select **Selected**. The list includes the FSSO group.

| Users Groups Organizational Units Selected | |
|--|---|
| Search <input type="text" value=""/> | |
| ID | Name |
| Domain Users | Domain Users |
| Enterprise Admins | Enterprise Admins |
| Enterprise Read-only Domain Controllers | Enterprise Read-only Domain Controllers |
| Event Log Readers | Event Log Readers |
| FortiDocs | FortiDocs |
| Group Policy Creator Owners | Group Policy Creator Owners |
| Guests | Guests |
| Hyper-V Administrators | Hyper-V Administrators |
| IIS_IUSRS | IIS_IUSRS |
| Incoming Forest Trust Builders | Incoming Forest Trust Builders |
| Network Configuration Operators | Network Configuration Operators |
| Performance Log Users | Performance Log Users |

+ Add Selected

Creating a user group

- To create a user group for FSSO users, go to **User & Device > User Groups** and select **Create New**.
- Enter a group **Name** and set **Type** to **Fortinet Single Sign-On (FSSO)**. Add the FSSO users to **Members**.

| | |
|---------|--|
| Name | FortiDocs |
| Type | <div>Firewall</div> <div>Fortinet Single Sign-On (FSSO)</div> <div>RADIUS Single Sign-On (RSSO)</div> <div>Guest</div> |
| Members | <div> CN=Fortinet FSSO,CN=Users,DC </div> <div>+</div> |

Creating a policy

1. To create a policy for FSSO users, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. For **Source**, set **User** to the FSSO user group.

| | |
|--------------------|--|
| Name | FortiDocs-Internet |
| Incoming Interface | <div> port1 </div> <div>+</div> |
| Outgoing Interface | <div> wan1 </div> <div>+</div> |
| Source | <div> all </div> <div> FortiDocs </div> <div>+</div> |
| Destination | <div> all </div> <div>+</div> |
| Schedule | <div> always </div> |
| Service | <div> ALL </div> <div>+</div> |
| Action | <div> <input checked="" type="checkbox"/> ACCEPT </div> <div> <input type="checkbox"/> DENY </div> <div> <input type="checkbox"/> LEARN </div> <div> <input type="checkbox"/> IPsec </div> |

Firewall / Network Options

| | |
|-----------------------|---|
| NAT | <input checked="" type="checkbox"/> |
| IP Pool Configuration | <div> <input checked="" type="checkbox"/> Use Outgoing Interface Address </div> <div> <input type="checkbox"/> Use Dynamic IP Pool </div> |

Results

1. Log in to a computer on the domain and access the Internet. The FortiGate uses FSSO for authentication and doesn't require your credentials to be entered again.
2. On the FortiGate, go to **Monitor > Firewall User Monitor** and select **Show all FSSO Logons**.

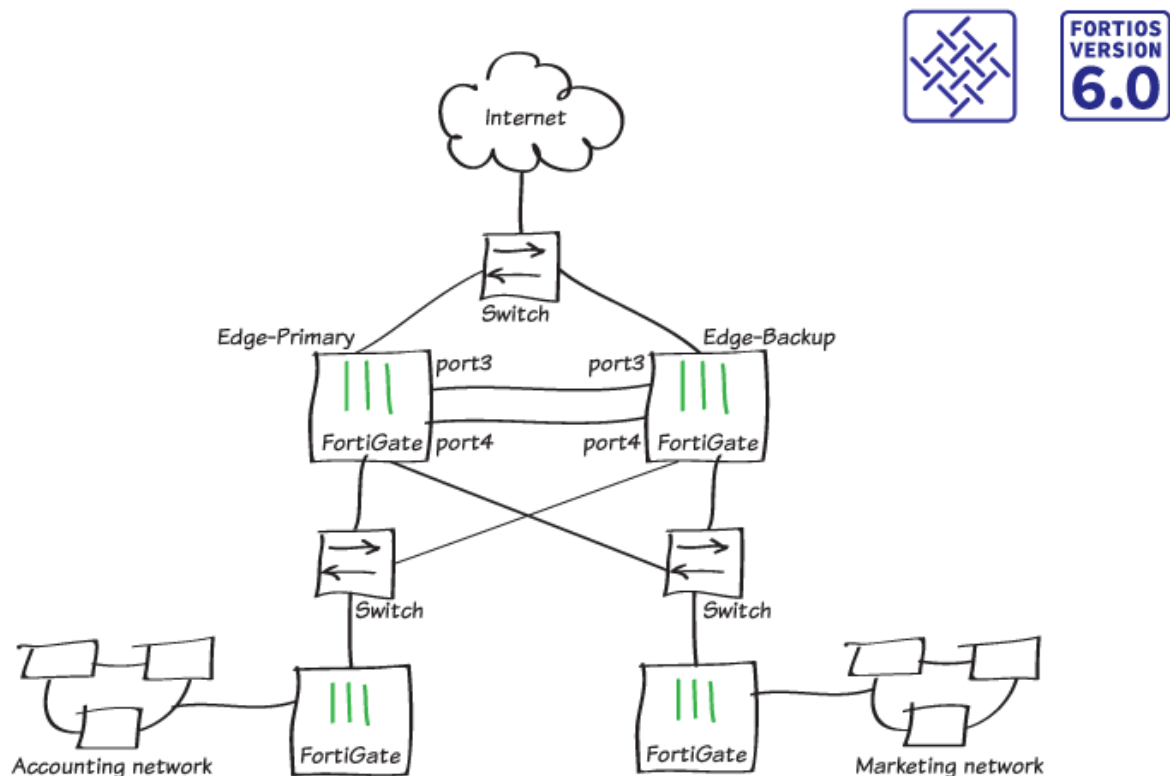
| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|-----------|------------|------------------------------|----------------|----------------|-------------------------|
| slowe | | 2 minute(s) and 30 second(s) | 172.25.176.124 | 0 B | Fortinet Single Sign-On |

For further reading, check out [Single sign-on to Windows AD](#) in the [FortiOS 6.0 Online Help](#).

High availability

This section includes recipes about how you can use high availability (HA) with your FortiGate.

High availability with two FortiGates



This recipe describes how to add a backup FortiGate to a previously installed FortiGate, to form a high availability (HA) cluster to improve network reliability.

Before you begin, make sure that the FortiGates are running the same FortiOS firmware version and interfaces are not configured to get their addresses from DHCP or PPPoE. Also, you can't use a switch port as an HA heartbeat interface. If necessary, convert the switch port to individual interfaces.

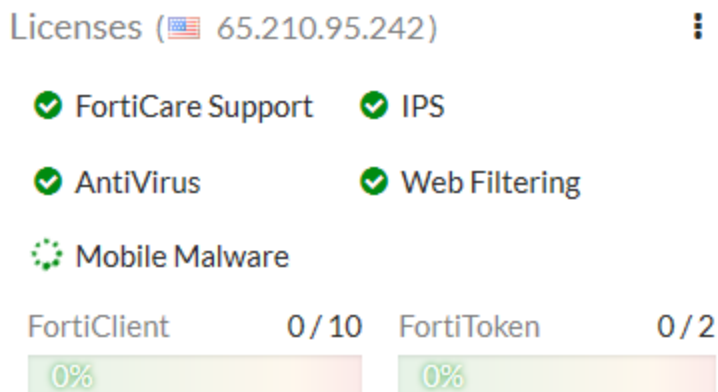
This recipe is in the Fortinet Security Fabric collection. It can also be used as a standalone recipe.

This recipe uses the FortiGate Clustering Protocol (FGCP) for HA. After you complete this recipe, the original FortiGate continues to operate as the primary FortiGate and the new FortiGate operates as the backup FortiGate.

For a more advanced HA recipe that includes CLI steps and involves using advanced options such as override to maintain the same primary FortiGate, see [High Availability with FGCP \(expert\) on page 141](#).

Setting up registration and licensing

1. Make sure both FortiGates are running the same FortiOS firmware version. Register and apply licenses to the new FortiGate unit before you add it to the HA cluster.



This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, and additional **virtual domains** (VDOMs).

All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add **FortiToken** licenses at any time because they're synchronized to all cluster members.



If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before you apply other licenses). When you apply the FortiOS Carrier license, the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.

2. You can also install any third-party certificates on the primary FortiGate before you form the cluster. Once the cluster is running, the FGCP synchronizes third-party certificates to the backup FortiGate.

Configuring the primary FortiGate for HA

1. On the primary FortiGate, go to **System > Settings** and change the **Host name** to identify this as the primary FortiGate in the HA cluster.

Host name

2. Go to **System > HA** and set the **Mode** to **Active-Passive**. Set the **Device priority** to a higher value than the default (in the example, 250) to make sure this FortiGate will always be the primary FortiGate. Also, set a **Group name** and **Password**.

Make sure you select **Heartbeat interfaces** (in the example, port3 and port4). Set the **Heartbeat Interface Priority** for each interface to 50.

Mode Active-Passive

Device priority ⓘ 250

Cluster Settings



Group name Edge-HA-Cluster

Password •••••••• Change



Session pickup ☐

Monitor interfaces +

Heartbeat interfaces

| | |
|---|----------------|
|  port3 | × |
|  port4 | × |
| + | |

Heartbeat Interface Priority ⓘ

| | | |
|-------|--|----|
| port3 |  | 50 |
| port4 |  | 50 |

Since the backup FortiGate isn't available, when you save the HA configuration, the primary FortiGate forms a cluster of one FortiGate but keeps operating normally.



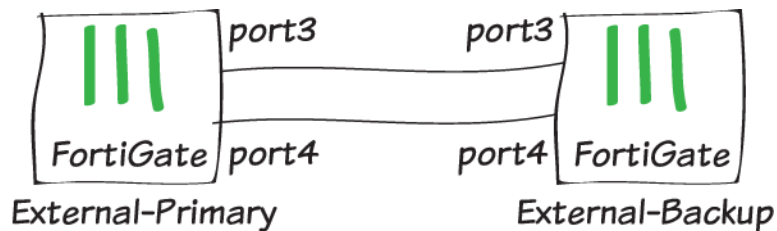
If these steps don't start HA mode, make sure that none of the FortiGate interfaces use DHCP or PPPoE addressing.

If there are other FortiOS HA clusters on your network, you may need to change the cluster group ID, using this CLI command:

```
config system ha
  set group-id 25
end
```

Connecting the backup FortiGate

Connect the backup FortiGate to the primary FortiGate and to the network, as shown in the network diagram at the start of this use case.



Since these connections disrupt traffic, you should make the connections when the network isn't processing a lot of traffic. If possible, make direct Ethernet connections between the heartbeat interfaces of the two FortiGate units.



This example uses two FortiGate-600Ds and the default heartbeat interfaces (port3 and port4). You can use any interfaces for HA heartbeat interfaces. A best practice is to use interfaces that don't process traffic, but this is not a requirement. If you are setting up HA between two FortiGates in a VM environment (for example, VMware or Hyper-V) you must enable promiscuous mode and allow mac address changes for heartbeat communication to work. Since the HA heartbeat interfaces must be on the same broadcast domain, for HA between remote data centers (called distributed clustering) you must support layer 2 extensions between the remote data centers, using technology such as MPLS or virtual extensible LAN (VXLAN).

You must use switches between the cluster and the Internet, and between the cluster and the internal networks, as shown in the network diagram. You can use any good quality switches to make these connections. You can also use one switch for all of these connections, as long as you configure the switch to separate traffic from the different networks.

Configuring the backup FortiGate

1. If required, change the firmware running on the new FortiGate to be the same version as is running on the primary FortiGate.
2. Enter the following command to reset the new backup FortiGate to factory default settings.
`execute factoryreset`
You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all, it's a best practice to reset your FortiGate to factory defaults to reduce the chance of synchronization problems.
3. Register and apply licenses to the backup FortiGate before configuring it for HA operation. This includes licensing for **FortiCare Support, IPS, AntiVirus, Web Filtering, Mobile Malware, FortiClient, FortiCloud, Security Rating, Outbreak Prevention**, and additional **virtual domains (VDOMs)**. All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add **FortiToken** licenses at any time because they're synchronized to all cluster members.



If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before applying other licenses). When you applying the FortiOS Carrier license the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.

Licenses (🇨🇦 173.243.138.78) ⋮

✔ FortiCare Support

✔ AntiVirus

✔ Web Filtering

⚠ Security Rating

| | | | |
|--------------------------|--------|--------------------------|-------|
| FortiClient | 0 / 10 | FortiToken | 0 / 2 |
| <div><div>0%</div></div> | | <div><div>0%</div></div> | |

4. Click on the **System Information** dashboard widget and select **Configure settings in System > Settings**. Change the FortiGate's **Host name** to identify it as the backup FortiGate.

Host name

You can also enter this CLI command:

```
config system global
  set hostname Backup
end
```

Duplicate the primary FortiGate HA settings, except set the Device Priority to a lower value (for example, 50) and do not enable override.

```
config system ha
  set mode a-p
  set group-id 100
  set group-name My-cluster
  set password <password>
  set priority 50
  set hbdev lan4 200 lan5 100
end
```

Similar to when configuring the primary FortiGate, once you enter the CLI command the backup FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed to HA virtual MAC addresses.



If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

Viewing the status of the HA cluster

Connect to the GUI of the primary FortiGate. The **HA Status** widget shows the cluster mode (**Mode**) and group name (**Group**).

HA Status

Mode

Active-Passive

Group

Edge-HA-Cluster

Master

Edge-Primary

Slave

Edge-Backup

Uptime

142:00:44:58

State Changed

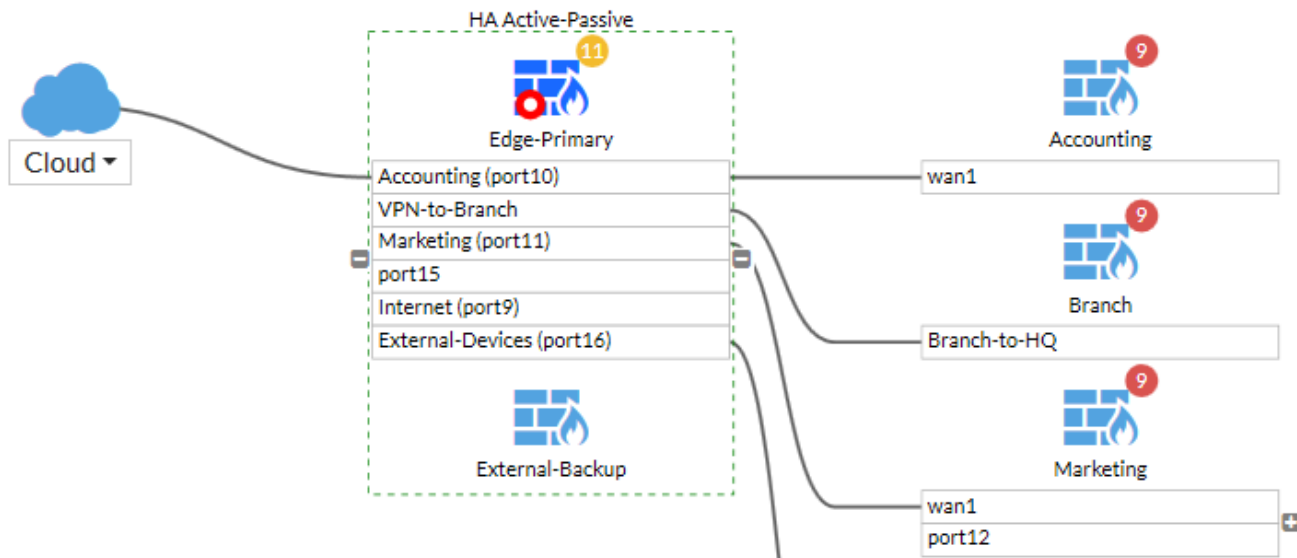
09:00:47:32

It also shows the host name of the primary FortiGate, which you can hover over to verify that the cluster is synchronized and operating normally. You can click on the widget to change the HA configuration or view a list of recently recorded cluster events, such as members joining or leaving the cluster.

To view the cluster status, click on the **HA Status** widget and select **Configure settings in System > HA** (or go to **System > HA**).

| Synchronized | Priority | Hostname | Serial No. | Role | Uptime | Sessions | Throughput |
|--|----------|--------------|------------------|--------|------------|----------|-------------|
| <div><div><div><div><div></div></div><div>FortiGate 600D</div></div><div><div>MGMT1</div><div>1</div><div>3</div><div>5</div><div>7</div><div>9</div><div>11</div><div>13</div><div>15</div><div>17</div><div>18</div><div>MGMT2</div><div>2</div><div>4</div><div>6</div><div>8</div><div>10</div><div>12</div><div>14</div><div>16</div></div></div></div> | | | | | | | |
| <div></div> | 250 | Edge-Primary | FGT6HD3916800525 | Master | 9d 22m 33s | 167 | 381.00 kbps |
| <div><div><div><div><div></div></div><div>FortiGate 600D</div></div><div><div>MGMT1</div><div>1</div><div>3</div><div>5</div><div>7</div><div>9</div><div>11</div><div>13</div><div>15</div><div>17</div><div>18</div><div>MGMT2</div><div>2</div><div>4</div><div>6</div><div>8</div><div>10</div><div>12</div><div>14</div><div>16</div></div></div></div> | | | | | | | |
| <div></div> | 50 | Edge-Backup | FGT6HD3916801195 | Slave | 9d 26m 14s | 47 | 72.00 kbps |

If the cluster is part of a Security Fabric, the FortiView Physical and Logical Topology views show information about the cluster status.



Results

All traffic should now be flowing through the primary FortiGate. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue operating as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.



If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover

You will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\
Request timeout for icmp_seq 75\
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to log into the primary FortiGate. If the primary FortiGate is powered off you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into. The FortiGate continues to operate in HA mode and if you restart the primary FortiGate, after a few minutes it should rejoin the cluster and operate as the backup FortiGate. Traffic should not be disrupted when the restarted primary unit rejoins the cluster.

(Optional) Upgrading the firmware for the HA cluster

Upgrading the firmware on the primary FortiGate automatically upgrades the firmware on the backup FortiGate. Both FortiGates are updated with minimal traffic disruption. Always review the Release Notes before you install new firmware.

1. Click the **System Information** widget and select **Update firmware in System > Firmware**. Back up the configuration and update the firmware from FortiGuard or upload a firmware image file. The firmware installs onto both the primary and backup FortiGates.

Current Version FortiOS v5.6.0,
Build 1449 [View Release Notes](#)

✔ System software is up to date

Upload Firmware

Update the current firmware manually using a file from your PC

[+ Upload Firmware](#)

Available Firmware


New Firmware

[All Available](#)

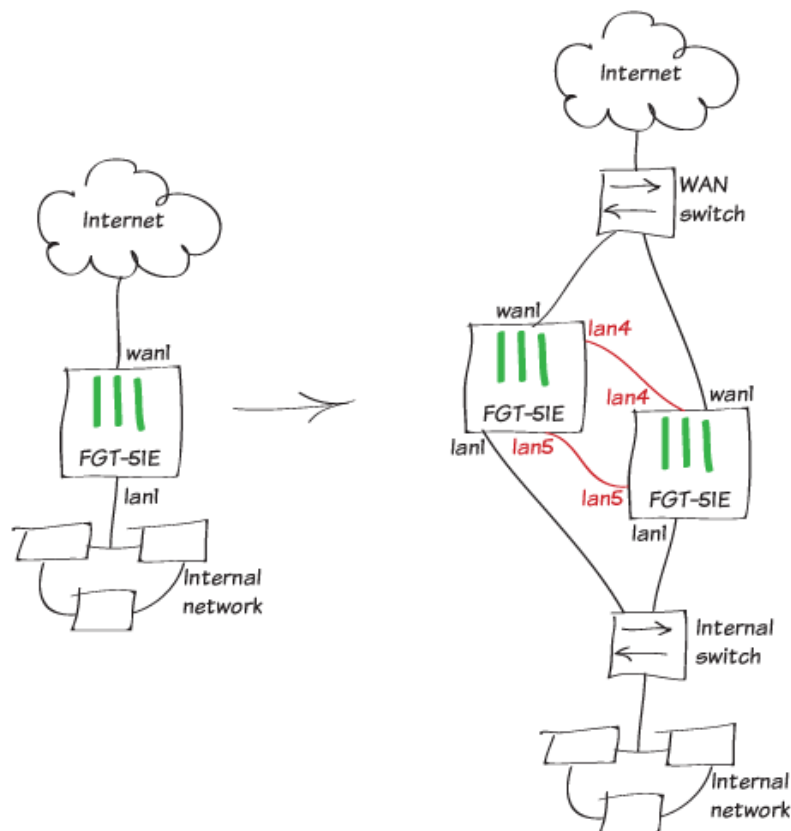
No new firmware versions are available

After the upgrade completes, verify that the **System Information** widget shows the new firmware version.

System Information

| | |
|---------------|---|
| Hostname | External-Primary |
| Serial Number | FGT6HD3916800525 |
| Firmware | v6.0.0 build0014 (Beta 2) |
| Mode | NAT (Flow-based) |
| System Time | 2018/03/02 12:11:56 |
| Uptime | 08:20:29:51 |
| WAN IP |  24.114.222.34 |

High Availability with FGCP (expert)

FORTIOS
VERSION
6.0

This recipe describes how to enhance the reliability of a network protected by a FortiGate by adding a second FortiGate and setting up a FortiGate Clustering Protocol (FGCP) High Availability cluster.

You will configure the FortiGate already on the network to become the primary FortiGate by:

1. Licensing it (if required)
2. Enabling HA
3. Increasing its device priority
4. Enabling override

You will prepare the new FortiGate by:

1. Setting it to factory defaults to wipe any configuration changes
2. Licensing it (if required)
3. Enabling HA without changing the device priority and without enabling override
4. Connecting it to the FortiGate already on the network

The new FortiGate becomes the backup FortiGate and its configuration is overwritten by the primary FortiGate.

This recipe describes best practices for configuring HA and involves extra steps that are not required for a basic HA setup. If you are looking for a basic HA recipe see [High availability with two FortiGates on page 133](#).

Before you start, the FortiGates should be running the same FortiOS firmware version and their interfaces should not be configured to get addresses from DHCP or PPPoE.

This recipe features two FortiGate-51Es. FortiGate-51Es have a 5-port switch lan interface. Before configuring HA, the lan interface was converted to 5 separate interfaces (lan1 to lan5). The lan1 interface connects to the internal network and the wan1 interface connects to the Internet. The lan4 and lan5 interfaces will become the HA heartbeat interfaces.



The FGCP does not support using a switch interface for the HA heartbeat. As an alternative to using the lan4 and lan5 interfaces as described in this recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

Configuring the primary FortiGate

1. Connect to the primary FortiGate, click on the **System Information** dashboard widget and select **Configure settings in System > Settings**.
2. Change the **Host name** to identify this FortiGate as the primary FortiGate.

Host name

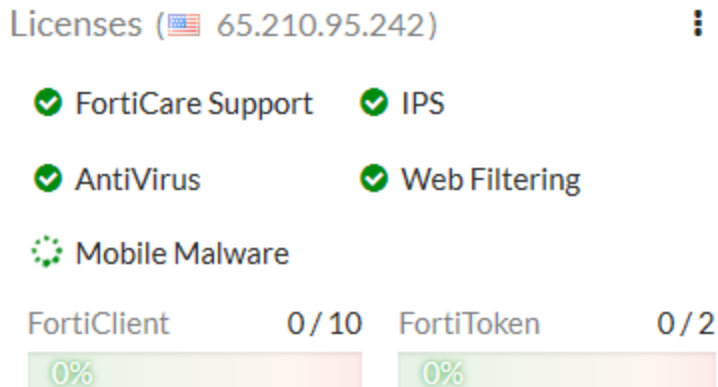
You can also enter this CLI command:

```
config system global
    set hostname Primary
end
```

3. Register and apply licenses to the primary FortiGate before configuring it for HA operation. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, and additional **virtual domains** (VDOMs). All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add **FortiToken** licenses at any time because they're synchronized to all cluster members.



If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before applying other licenses). When you applying the FortiOS Carrier license the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.



You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to the backup FortiGate(s).

4. Enter this CLI command to set the HA mode to active-passive, set a group id, group name and password, increase the device priority to a higher value (for example, 250) and enable override.

```
config system ha
    set mode a-p
    set group-id 100
    set group-name My-cluster
    set password <password>
    set priority 250
    set override enable
    set hbdev lan4 200 lan5 100
end
```

Enabling override and increasing the device priority means this FortiGate always becomes the primary unit.

This configuration also selects lan4 and lan5 to be the heartbeat interfaces and sets their priorities to 200 and 100 respectively. Its a best practice to set different priorities for the heartbeat interfaces (but not a requirement).

If you have more than one cluster on the same network, each cluster should have a different group id. Changing the group id changes the cluster interface virtual MAC addresses. If your group id causes a MAC address conflict on your network, you can select a different group id.

You can also configure most of these settings from the GUI (go to **System > HA**).

Mode Active-Passive

Device priority ⓘ 250

Cluster Settings



Group name My-cluster

Password •••••••• Change



Session pickup ☐

Monitor interfaces +

Heartbeat interfaces

| | |
|--|----------------|
|  lan4 | × |
|  lan5 | × |
| + | |

Heartbeat Interface Priority ⓘ

| | | |
|------|--|-----|
| lan4 |  | 200 |
| lan5 |  | 100 |

Override and the group id can only be configured from the CLI.

```
config system ha
  set group-id 100
  set override enable
end
```

After you enter the CLI command or make the GUI changes, the FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed to HA virtual MAC addresses.



If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

The FGCP uses virtual MAC addresses for failover. The virtual MAC address assigned to each FortiGate interface depends on the HA group ID. A group ID of 100 sets FortiGate interfaces to the following MAC addresses: 00:09:0f:09:64:00, 00:09:0f:09:64:01, 00:09:0f:09:64:02 and so on.

You can verify that the FGCP has set the virtual MAC addresses by viewing the configuration of each FortiGate interface from the GUI (go to **Network > Interfaces**) or by entering the following CLI command (shown below for lan2 on a FortiGate-51E):

```
get hardware nic lan2
...
Current_HWaddr 00:09:0f:09:64:01
Permanent_HWaddr 70:4c:a5:98:11:54
...
```

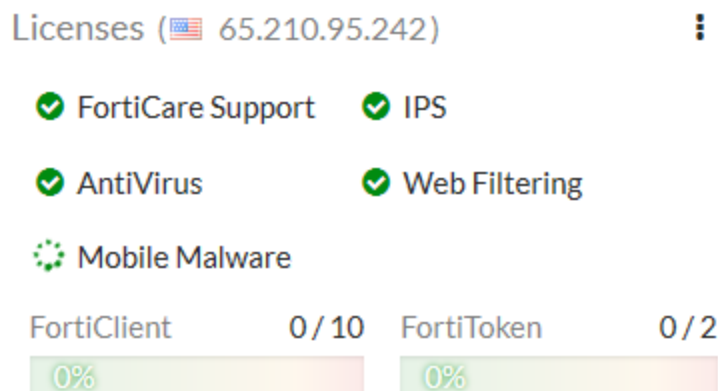
You can also use the `diagnose hardware deviceinfo nic lan2` command to display this information. The output shows the current hardware (MAC) address (the virtual MAC set by the FGCP) and the permanent hardware (MAC) address for the interface.

Configuring the backup FortiGate

1. If required, change the firmware running on the new FortiGate to be the same version as is running on the primary FortiGate.
2. Enter the following command to reset the new backup FortiGate to factory default settings.
`execute factoryreset`
You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all, it's a best practice to reset your FortiGate to factory defaults to reduce the chance of synchronization problems.
3. Register and apply licenses to the backup FortiGate before configuring it for HA operation. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, and additional **virtual domains** (VDOMs). All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add **FortiToken** licenses at any time because they're synchronized to all cluster members.



If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before applying other licenses). When you applying the FortiOS Carrier license the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.



4. Click on the **System Information** dashboard widget and select **Configure settings in System > Settings**. Change the FortiGate's **Host name** to identify it as the backup FortiGate.

Host name

You can also enter this CLI command:

```
config system global
set hostname Backup
```

end

1. Duplicate the primary FortiGate HA settings, except set the Device Priority to a lower value (for example, 50) and do not enable override.

```
config system ha
    set mode a-p
    set group-id 100
    set group-name My-cluster
    set password <password>
    set priority 50
    set hbdev lan4 200 lan5 100
end
```

Similar to when configuring the primary FortiGate, once you enter the CLI command the backup FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed to HA virtual MAC addresses.



If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

If the group ID is the same, the backup FortiGate interfaces get the same virtual MAC addresses as the primary FortiGate. You can check **Network > Interfaces** on the GUI or use the `get hardware nic` command to verify.

Connecting the primary and backup FortiGates

Connect the primary and backup FortiGates together and to your network as shown in the network diagram at the start of the use case. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the Internet and between the cluster and the internal network as shown in the network diagram. You can use any good quality switches to make these connections. You can also use one switch for all of these connections as long as you configure the switch to separate traffic from the different networks.

The example shows the recommended configuration of direct connections between the lan4 heartbeat interfaces and between the lan5 heartbeat interfaces.

When the heartbeat interfaces are connected, the FortiGates find each other and negotiate to form a cluster. The primary FortiGate synchronizes its configuration to the backup FortiGate. The cluster forms automatically with minimal or no additional disruption to network traffic.

The cluster will have the same IP addresses as the primary FortiGate had. You can log into the cluster by logging into the primary FortiGate CLI or GUI using one of the original IP addresses of the primary FortiGate.

Checking cluster operation

Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.

1. Log into the primary FortiGate CLI and enter this command:

```
diagnose sys ha checksum cluster
```

The command output lists all cluster members' configuration checksums. If both cluster members have identical checksums you can be sure that their configurations are synchronized. If the checksums are different, wait a short

while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized.

If the checksums never become identical visit the [Fortinet Support](#) website for assistance.

2. The **HA Status** dashboard widget also shows synchronization status. Mouse over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.

HA Status

Mode Active-Active

Group My-cluster

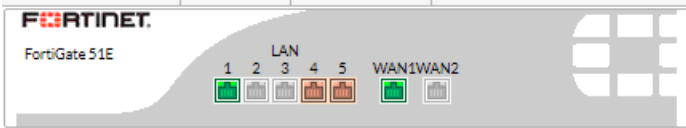
Master Primary

Slave Backup

Uptime 10:03:44:12

State Changed

3. To view more information about the cluster status, click on the **HA Status** widget and select **Configure Settings in System > HA** (or go to **System > HA**).

| Synchronized | Priority | Hostname | Serial No. | Role | Uptime | Sessions | Throughput |
|--|----------|----------|------------------|--------|----------------|----------|------------|
|  | | | | | | | |
| | 250 | Primary | FGT51E5618000206 | Master | 3d 37m 48s | 63 | 92.00 kbps |
| | 50 | Backup | FGT51E5618000259 | Slave | 2d 23h 46m 27s | 31 | 33.00 kbps |

Disabling override (recommended)

When the checksums are identical, disable override on the primary FortiGate by entering the following command:

```
config system ha
  set override disable
end
```

Results

All traffic should now be flowing through the primary FortiGate. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue operating as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.



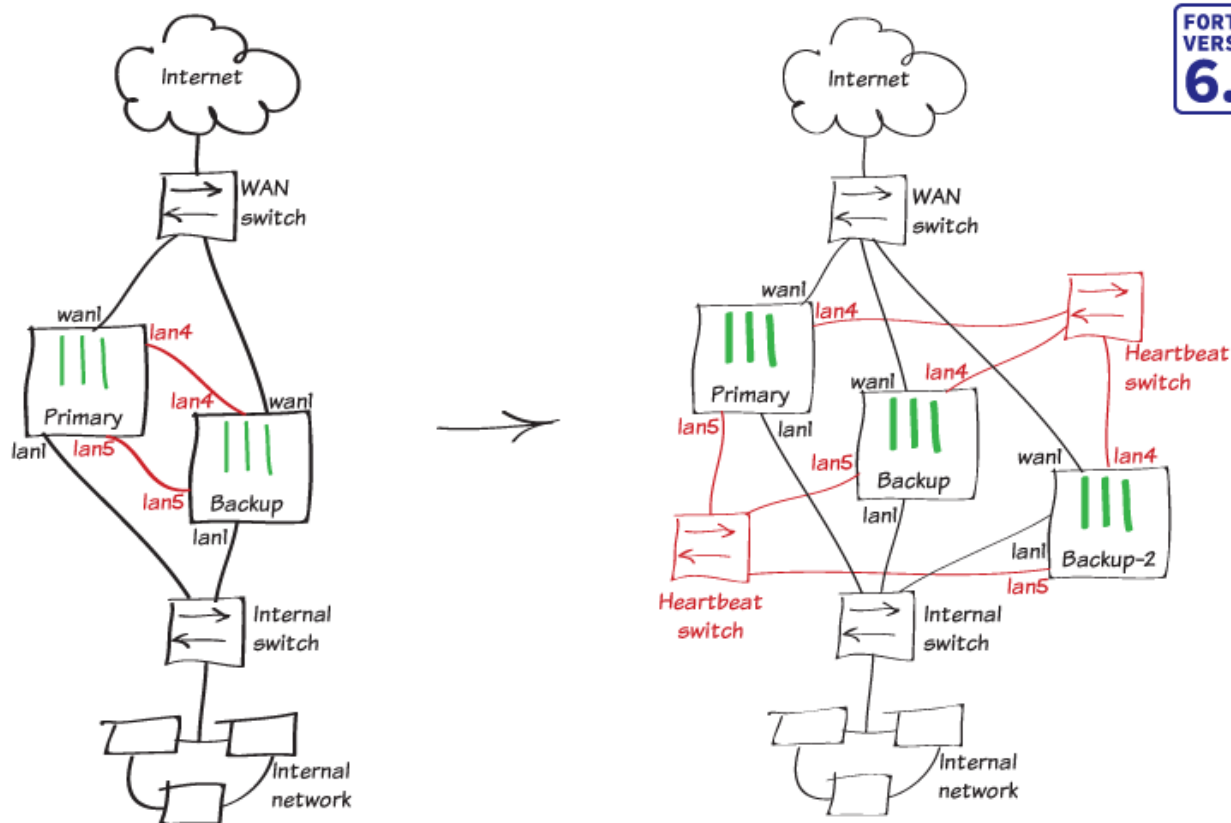
If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover

You will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\  
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\  
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\  
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\  
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\  
Request timeout for icmp_seq 75\  
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\  
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\  
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\  
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\  
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\  
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\  
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to log into the primary FortiGate. If the primary FortiGate is powered off you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into. The FortiGate continues to operate in HA mode and if you restart the primary FortiGate, after a few minutes it should rejoin the cluster and operate as the backup FortiGate. Traffic should not be disrupted when the restarted primary unit rejoins the cluster.

Adding a third FortiGate to an FGCP cluster (expert)



This use case describes how to add a third FortiGate to an already established FGCP cluster (the cluster from [High Availability with FGCP \(expert\) on page 141](#)) and configure active-active HA.

You prepare the new FortiGate by:

1. Setting it to factory defaults to wipe any configuration changes.
2. Licensing it (if required).
3. Enabling HA without changing the device priority and without enabling override.
4. Connecting it to the FGCP cluster already on the network.

The new FortiGate becomes a second backup FortiGate; its configuration synchronized to match the configuration of the cluster.

Before you start, the new FortiGate should be running the same FortiOS firmware version as the cluster and its interfaces should not be configured to get addresses from DHCP or PPPoE.

After the third FortiGate joins the cluster, this recipe also describes how to switch the cluster to operate in active-active (or a-a) mode. Active-active HA enables proxy-based NGFW/UTM load-balancing to allow the three FortiGates to share proxy-based NGFW/UTM processing. If the cluster handles a large amount of NGFW/UTM traffic, active-active HA with three FortiGates may enhance performance.

This use case features three FortiGate-51Es. These FortiGate models include a 5-port switch lan interface. Before configuring HA, the lan interface was converted to five separate interfaces (lan1 to lan5). The lan1 interface connects to

the internal network and the wan1 interface connects to the Internet. The lan4 and lan5 interfaces become the HA heartbeat interfaces.



The FGCP does not support using a switch interface for the HA heartbeat. As an alternative to using the lan4 and lan5 interfaces as described in this recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

Enabling override on the primary FortiGate (optional)

Before adding the third FortiGate to the cluster, enable override on the primary FortiGate. In most cases this step would not be necessary but it is a best practice because enabling override makes sure the configuration of the primary FortiGate is not overwritten by the configuration of the new backup FortiGate.

To enable override, log into the primary FortiGate CLI and enter this command:

```
config system ha
    set override enable
end
```

Configuring the new FortiGate

1. Enter this command to reset the new FortiGate to factory default settings:

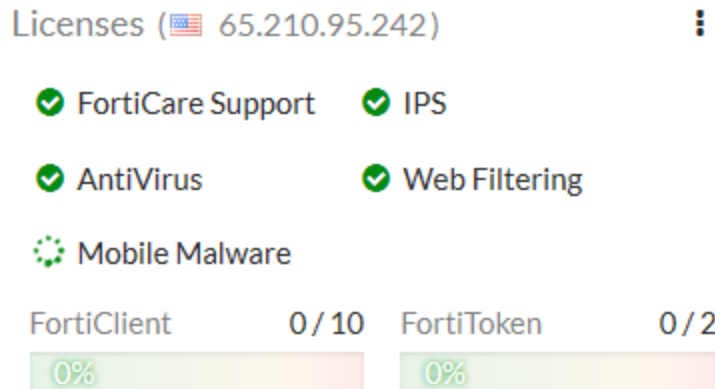
```
execute factoryreset
```

You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all it's recommended to set it back to factory defaults to reduce the chance of synchronization problems.

2. If required, change the firmware running on the new FortiGate to match the cluster firmware version.
3. Register and apply licenses to the new FortiGate before configuring it for HA operation. This includes licensing for **FortiCare Support, IPS, AntiVirus, Web Filtering, Mobile Malware, FortiClient, FortiCloud, Security Rating, Outbreak Prevention**, and additional **virtual domains (VDOMs)**. All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add **FortiToken** licenses at any time because they're synchronized to all cluster members.



If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before applying other licenses). When you applying the FortiOS Carrier license the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.



- Change the host name of the new FortiGate to identify it as **Backup-2** by clicking on the **System Information** dashboard widget and selecting **Configure settings in System > Settings** and changing the **Host name**.

Host name

You can also enter this CLI command:

```
config system global
  set hostname Backup-2
end
```

- Duplicate the primary FortiGate HA settings, except set the Device Priority to a lower value (for example, 50) and do not enable override.

```
config system ha
  set mode a-p
  set group-id 100
  set group-name My-cluster
  set password <password>
  set priority 50
  set hbdev lan4 200 lan5 100
end
```

Once you enter the CLI command the new FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate while FGCP negotiation takes place and the FortiGate interface MAC addresses change to HA virtual MAC addresses.



If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

If the group ID is the same, the backup FortiGate interfaces get the same virtual MAC addresses as the primary FortiGate. You can check **Network > Interfaces** on the GUI or use the `get hardware nic` command.

Connecting the new FortiGate to the cluster

Connect the new FortiGate to the cluster and your network as shown in the network diagram at the start of this use case. Making these connections disrupts network traffic as you disconnect and re-connect the heartbeat interfaces. If you have already added switches to connect the heartbeat interfaces, you can connect the new FortiGate without disrupting network traffic.

When you add a third FortiGate to a cluster you need to connect the heartbeat interfaces together using switches. You can use separate switches for each heartbeat interface (recommended for redundancy) or you can use the same switch for both heartbeat interfaces as long as you separate the traffic from each heartbeat interface.

When you connect the heartbeat interfaces of the new FortiGate, the cluster re-negotiates. If you have enabled override on the primary FortiGate and set its priority highest, the primary FortiGate synchronizes its configuration to the new FortiGate. The cluster automatically forms with minimal or no additional disruption to network traffic.

The new cluster will have the same IP addresses as the primary FortiGate. You can log into the cluster by logging into the primary FortiGate CLI or GUI.

Checking cluster operation

Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.

1. Log into the primary FortiGate CLI and enter this command:

```
diagnose sys ha checksum cluster
```

The command output lists all cluster members' configuration checksums. If they all have identical checksums, you can be sure that the configurations are synchronized. If the checksums are different, wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized.

If the checksums never become identical visit the [Fortinet Support](#) website for assistance.

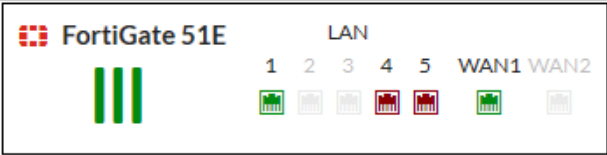
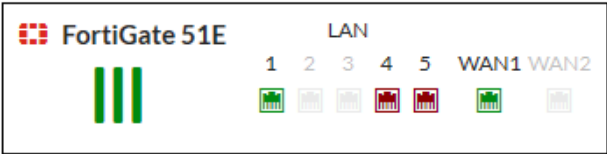
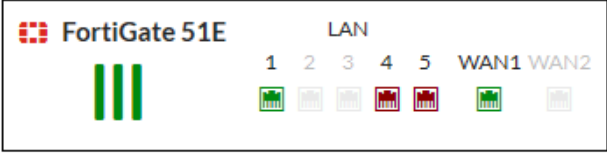
2. The **HA Status** dashboard widget also shows synchronization status. Mouse over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.

HA Status

| | |
|--------|----------------|
| Mode | Active-Passive |
| Group | My-cluster |
| Master | ✓ Primary |
| Slave | ✓ Backup |
| Slave | ✓ Backup-2 |
| Uptime | 02:00:17:22 |

3. To view more information about the cluster status, click on the **HA Status** widget and select **Configure Settings in**

System > HA (or go to **System > HA**).

| Synchronized | Priority | Hostname | Serial No. | Role | Uptime | Sessions | Throughput |
|---|----------|----------|------------------|--------|---------------|----------|------------|
|  | | | | | | | |
| ✓ | 250 | Primary | FGT51E5618000086 | Master | 2d 1h 39m 32s | 62 | 49.00 kbps |
|  | | | | | | | |
| ✓ | 50 | Backup | FGT51E5618000259 | Slave | 2d 24m 56s | 25 | 32.00 kbps |
|  | | | | | | | |
| ✓ | 50 | Backup-2 | FGT51E5618000206 | Slave | 2d 1m 36s | 25 | 31.00 kbps |

Disabling override (recommended)

When the checksums are identical, disable override on the primary FortiGate by entering the following command:

```
config system ha
  set override disable
end
```

FGCP clusters dynamically respond to network conditions. If you keep override enabled, the same FortiGate always becomes the primary FortiGate. With override enabled; however, the cluster may negotiate more often to keep the same FortiGate as the primary FortiGate, potentially increasing traffic disruptions.

If you disable override it is more likely that the backup FortiGate could become the primary FortiGate. Disabling override is recommended unless its important that the same FortiGate remains the primary FortiGate



To see how enabling override can cause minor traffic disruptions, with override enabled set up a continuous ping through the cluster. Then disconnect power to the backup unit. You will most likely notice a brief disruption in the ping traffic. Try the same thing with override disabled and you shouldn't see this traffic disruption.

With override enabled, the disruption is minor and shouldn't be noticed by most users. For smoother operation, the best practice is to disable override.

Converting to an active-active cluster

Log into the primary FortiGate CLI and enter this command to convert the cluster from an active-passive to an active-active cluster. The cluster changes modes without any traffic interruption.

```
config system ha
  set mode a-a
```

end



Active-active HA load-balancing distributes proxy-based NGFW/UTM processing to all cluster members. Proxy-based NGFW/UTM processing is CPU and memory-intensive. Distributing NGFW/UTM processing in this way may result in higher throughput.

Results

Most traffic should now be flowing through the primary FortiGate with proxy-based NGFW/UTM sessions distributed to all three FortiGates in the cluster. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue operating as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.



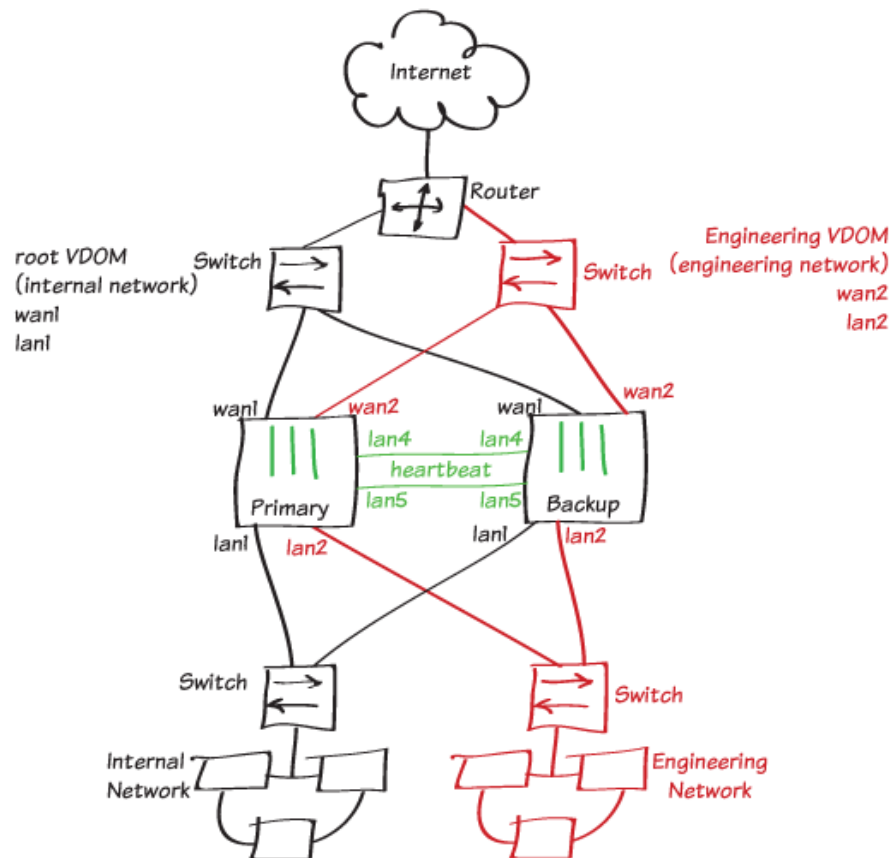
If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

You will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\  
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\  
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\  
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\  
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\  
Request timeout for icmp_seq 75\  
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\  
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\  
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\  
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\  
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\  
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\  
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to log into the primary FortiGate. If the primary FortiGate is powered off you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into. The FortiGate continues to operate in HA mode and if you restart the primary FortiGate, after a few minutes it should rejoin the cluster and operate as the backup FortiGate. Traffic should not be disrupted when the restarted primary unit rejoins the cluster.

FGCP Virtual Clustering with two FortiGates (expert)



FORTIOS
VERSION
6.0

In this use case you set up a FortiGate Clustering Protocol (FGCP) virtual clustering configuration with two FortiGates to provide redundancy and failover protection for two networks. The FortiGate configuration includes two VDOMs. The root VDOM handles internal network traffic and the Engineering VDOM handles Engineering network traffic. This use case describes a very simple two-VDOM configuration. However, the same principles described in this example apply to a virtual cluster with more VDOMs.

In this virtual cluster configuration the primary FortiGate processes all internal network traffic and the backup FortiGate processes all Engineering network traffic. Virtual clustering enables override and uses device priorities to distribute traffic between the primary and backup FortiGates in the virtual cluster.

This use case describes the recommended steps for setting up a virtual cluster of two FortiGates. You can follow the procedure described in [High Availability with FGCP \(expert\) on page 141](#) to configure virtual clustering by converting a FortiGate with VDOMs to HA mode and then adding another FortiGate to form a cluster. However, taking this approach with virtual clustering is not as foolproof as a normal HA configuration. If you accidentally add the management VDOM to virtual cluster 2 before adding the backup FortiGate, the configuration of the primary FortiGate can be overwritten by the backup FortiGate. If want to experiment with this approach, make sure you don't add the management VDOM to virtual cluster 2 until all of the FortiGates have joined the cluster.

Before you start, the FortiGates should be running the same FortiOS firmware version and their interfaces should not be configured to get addresses from DHCP or PPPoE.

This user case features two FortiGate-51Es. FortiGate-51Es have a 5-port switch lan interface. Before configuring HA, the lan interface was converted to 5 separate interfaces (lan1 to lan5).



The FGCP does not support using a switch interface for the HA heartbeat. As an alternative to using the lan4 and lan5 interfaces as described in this recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

Preparing the FortiGates

1. If required, upgrade the firmware running on the FortiGates. Both FortiGates should be running the same version of FortiOS.

2. On each FortiGate, enter the following command to reset them factory default settings.

```
execute factoryreset
```

You can skip this step if the FortiGates are fresh from the factory. But if their configurations have changed at all, it's a best practice to reset them to factory defaults to reduce the chance of synchronization problems.

In some cases, after resetting to factory defaults you may want to make some initial configuration changes to connect the FortiGates to the network or for other reasons. To write this recipe, the lan switch on the FortiGate-51Es was converted to separate lan1 to lan5 interfaces.

3. Change the primary FortiGate **Host name** to identify it as the primary FortiGate by going to **System > Settings**.

Host name

4. Change the backup FortiGate **Host name** to identify it as the backup FortiGate by going to **System > Settings**.

Host name

You can also use the CLI to change the host name. From the Primary FortiGate:

```
config system global
  set hostname Primary
end
```

From the Backup-1 FortiGate:

```
config system global
  set hostname Backup
end
```

5. Register and apply licenses to the FortiGates before configuring the cluster. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, and additional **virtual domains** (VDOMs).

Licenses (🇺🇸 65.210.95.242) ⋮

✅ FortiCare Support
✅ IPS

✅ AntiVirus
✅ Web Filtering

🔄 Mobile Malware

FortiClient 0 / 10

FortiToken 0 / 2

0%

0%

Both FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add **FortiToken** licenses at any time because they're synchronized to all cluster members.



If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before applying other licenses). When you applying the FortiOS Carrier license the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.

Configuring clustering

1. On the primary FortiGate, enter the following CLI command to set the HA mode to active-passive, set a group-id, group name, and password, increase the device priority to 200, enable override, and configure the heartbeat interfaces (lan4 and lan5 in this example).

```
config system ha
    set mode a-p
    set group-id 88
    set group-name My-vcluster
    set password <password>
    set priority 200
    set override enable
    set hbdev lan4 200 lan5 100
end
```



If you have more than one cluster on the same network, each cluster should have a different group id. Changing the group id changes the cluster interface virtual MAC addresses. If your group id causes a MAC address conflict on your network, you can select a different group id.

Enabling override is optional; but it makes sure the FortiGate with the highest device priority becomes the primary unit.

You can also configure most of these settings from the GUI (go to **Global > System > HA**). The group-id and override can only be configured from the CLI.

Mode Active-Passive

Device priority ⓘ 200

Cluster Settings



Group name My-vcluster

Password ●●●●●●●● Change



Session pickup ☐

Monitor interfaces +

Heartbeat interfaces

| | |
|--|----------------|
|  lan4 | × |
|  lan5 | × |
| + | |

Heartbeat Interface Priority ⓘ

| | | |
|------|--|-----|
| lan4 |  | 200 |
| lan5 |  | 100 |

- On the backup FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 50.

```
config system ha
  set mode a-p
  set group-id 88
  set group-name My-vcluster
  set password <password>
  set priority 50
  set override enable
  set hbdev lan4 200 lan5 100
end
```

After you enable HA, each FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces change to HA virtual MAC addresses.



If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate (or just deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

The FGCP uses virtual MAC addresses for failover. The virtual MAC address assigned to each FortiGate interface depends on the HA group ID. A group ID of 88 sets FortiGate interfaces to the following MAC addresses:

00:09:0f:09:58:00, 00:09:0f:09:58:01, 00:09:0f:09:58:02 and so on. For details, see Cluster virtual MAC addresses. You can verify that the FGCP has set the virtual MAC addresses by viewing the configuration of each FortiGate interface from the GUI (go to Network > Interfaces) or by entering the following CLI command (shown below for lan2 on a FortiGate-51E):

```
get hardware nic lan2
...
Current_HWaddr 00:09:0f:09:58:01
Permanent_HWaddr 70:4c:a5:98:11:54
...
```

You can also use the `diagnose hardware deviceinfo nic lan2` command to display this information. The output shows the current hardware (MAC) address (the virtual MAC set by the FGCP) and the permanent hardware (MAC) address for the interface.

Connecting and verifying cluster operation

Connect the FortiGates together and to your networks as shown in the network diagram at the start of the use case. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the Internet, between the cluster and the internal network, and between the cluster and the Engineering network as shown in the diagram. You can use any good quality switches to make these connections.

To make HA heartbeat connections, connect all of the lan4 interfaces to the same switch and all of the lan5 interfaces to another switch.

You can also use fewer switches for all of these connections as long as you configure the switches to separate traffic from the different networks.

When you connect the heartbeat interfaces and power on the FortiGates, they find each other and negotiate to form a cluster. The cluster will have the same IP addresses as the primary FortiGate. You can log into the cluster by logging into the primary FortiGate GUI or CLI using one of the original IP addresses of the primary FortiGate.

Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration. Log into the primary FortiGate CLI and enter this command:

```
diagnose sys ha checksum cluster
```

The command output lists all cluster members' configuration checksums. If both cluster members have identical checksums you can be sure that their configurations are synchronized. If the checksums are different, wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized. If the checksums never become identical you can use the information in Synchronizing the configuration to troubleshoot the problem or visit the Fortinet Support website for assistance.

You can also use the `get system ha status` command to display detailed information about the cluster. .

The **HA Status** dashboard widget also shows synchronization status. Hover over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.

HA Status

| | |
|---------------|----------------|
| Mode | Active-Passive |
| Group | My-vcluster |
| Master | ✓ Primary |
| Slave | ✓ Backup |
| Uptime | 03:02:01:56 |
| State Changed | |

Adding VDOMs and setting up virtual clustering

1. Enable VDOMs by going to **System > Settings > System Operation Settings** and enabling **Virtual Domains**. Or enter the following CLI command.

```
config system global
    set vdom-admin enable
end
```

2. Add VDOMs as required. Go to **Global > System > VDOM** and select **Create New**. Or enter the following CLI command to add the Engineering VDOM.

```
config global
    edit Engineering
end
```


3. Configure virtual clustering and VDOM partitioning on the primary FortiGate. The following command enables virtual cluster 2, adds the Engineering VDOM to virtual cluster 2, and sets the virtual cluster 2 device priority of the primary FortiGate to 50.

```
config global
    config system ha
        set vcluster2 enable
        config secondary-vcluster
            set vdom Engineering
            set priority 50
        end
    end
end
```

You can also configure virtual clustering and VDOM partitioning from the GUI by going to **Global > System > HA**.


VDOM Partitioning

Virtual cluster 1

 root

+


Virtual cluster 2

 Engineering

✕

+

Secondary Cluster Settings

Device priority 

50

Monitor interfaces

+

- Set the virtual cluster 2 priority of the backup FortiGate to a relatively high value (in this example, 200) so that this FortiGate processes traffic for the VDOMs in virtual cluster 2. The FGCP synchronizes all other HA settings from the primary FortiGate.

You can only configure the virtual cluster 2 priority of the backup FortiGate from the CLI. Use `execute ha manage` to access the backup FortiGate CLI.

```
config global
  config system ha
    config secondary-vcluster
      set priority 200
    end
  end
end
```



The root VDOM can only be associated with virtual cluster 1.





The VDOM that is assigned as the management VDOM can also only be associated with virtual cluster 1.

Checking virtual cluster operation

- Once again use the `diagnose sys ha checksum cluster` command and the `get system ha status` command to check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.





The **HA Status** dashboard widget shows the VDOMs in the virtual clusters. You can hover over the VDOM names to see status information for the VDOMs. You can hover over the host names of each FortiGate to verify that they are synchronized and both have the same checksum.

HA Status

| | |
|-------------------|---|
| Mode | Active-Passive |
| Group | My-vcluster |
| Virtual cluster 1 |  root |
| Virtual cluster 2 |  Engineering |
| Master |  Primary |
| Slave |  Backup |
| Uptime | 03:03:00:43 |

2. To view more information about the cluster status, click on the **HA Status** widget and select **Configure Settings in System > HA** (or go to **System > HA**).

The HA status page shows both FortiGates in the cluster. It also shows that Primary is the primary FortiGate for the root VDOM (so the primary FortiGate processes all root VDOM traffic). The page also shows that Backup is the primary FortiGate for the Engineering VDOM (so the backup FortiGate processes all Engineering VDOM traffic).

| Synchronized | Priority | Hostname | Virtual Domains | Serial No. | Role |
|--|----------|----------|-----------------|------------------|--------|
| Virtual cluster 1 (2) | | | | | |
|  | | | | | |
| ✓ | 200 | Primary | • root | FGT51E5618000206 | Master |
|  | | | | | |
| ✓ | 50 | Backup | • root | FGT51E5618000259 | Slave |
| Virtual cluster 2 (2) | | | | | |
|  | | | | | |
| | 50 | Primary | • Engineering | FGT51E5618000206 | Slave |
|  | | | | | |
| | 200 | Backup | • Engineering | FGT51E5618000259 | Master |

Results

All traffic should now be flowing through the primary FortiGate. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue operating as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.



If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover

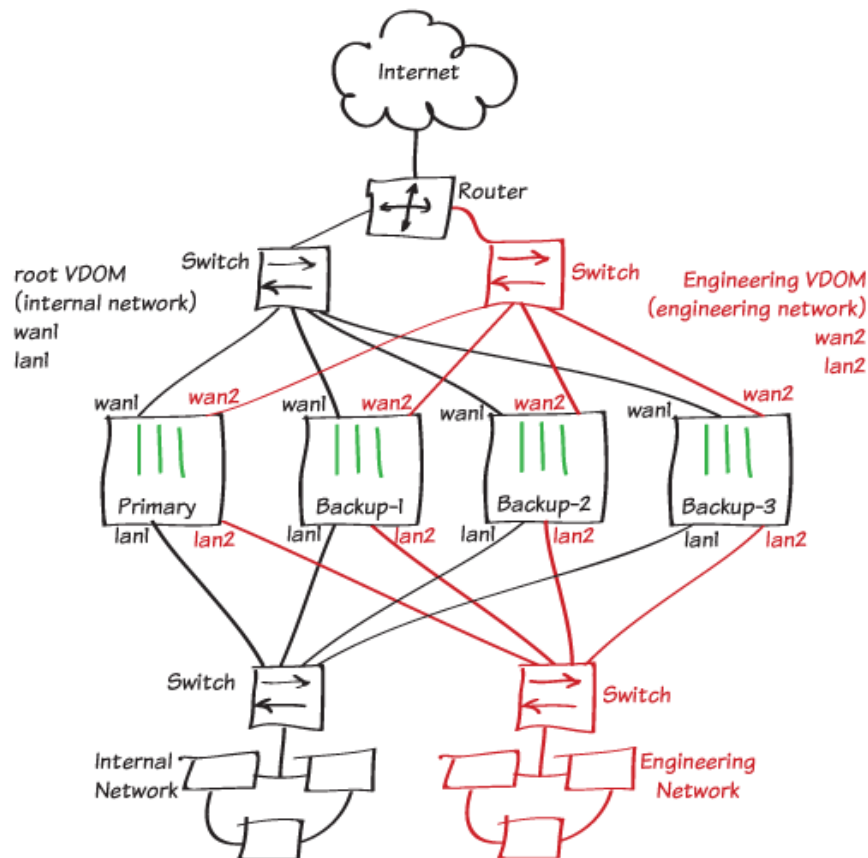
You will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\  
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\  
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\  
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\  
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\  
Request timeout for icmp_seq 75\  
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\  
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\  
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\  
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\  
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\  
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\  
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to log into the primary FortiGate. If the primary FortiGate is powered off you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into.

When you restart the primary FortiGate, after a few minutes it should rejoin the cluster and because override is enabled, the original virtual cluster configuration should be re-established. Traffic may be temporarily disrupted when the restarted primary FortiGate rejoins the cluster.

FGCP Virtual Clustering with four FortiGates (expert)



In this use case you set up a FortiGate Clustering Protocol (FGCP) virtual clustering configuration with four FortiGates to provide redundancy and failover protection for two networks. The FortiGate configuration includes two VDOMs. The root VDOM handles internal network traffic and the Engineering VDOM handles Engineering network traffic. This recipe describes a very simple two-VDOM configuration. However, the same principles described in this example apply to a virtual cluster with more VDOMs.

In this virtual cluster configuration the primary FortiGate processes all internal network traffic and the backup FortiGate processes all Engineering network traffic. Virtual clustering enables override and uses device priorities to distribute traffic between the primary and backup FortiGates in the virtual cluster.

The third FortiGate (the recipe names it Backup-2) acts as a backup to the primary FortiGate; if the primary FortiGate fails, all primary FortiGate network traffic transfers to the Backup-2 FortiGate, which becomes the new primary FortiGate.

The fourth FortiGate (Backup-3) acts as a backup to the backup FortiGate; if the backup FortiGate fails, all backup FortiGate network traffic transfers to the Backup-3 FortiGate, which becomes the new backup FortiGate.

This recipe describes the recommended steps for setting up a virtual cluster of four FortiGates. You can follow the procedure described in [High Availability with FGCP \(expert\) on page 141](#) to configure virtual clustering by converting a FortiGate with VDOMs to HA mode and then adding another FortiGate to form a cluster. However, taking this approach with virtual clustering is not as foolproof as a normal HA configuration. If you accidentally add the management VDOM to virtual cluster 2 before adding the backup FortiGate, the configuration of the primary FortiGate can be overwritten by the

backup FortiGate. If want to experiment with this approach, make sure you don't add the management VDOM to virtual cluster 2 until all of the FortiGates have joined the cluster.

Before you start, the FortiGates should be running the same FortiOS firmware version and their interfaces should not be configured to get addresses from DHCP or PPPoE.

This recipe features four FortiGate-51Es. FortiGate-51Es have a 5-port switch lan interface. Before configuring HA, the lan interface was converted to 5 separate interfaces (lan1 to lan5).



The FGCP does not support using a switch interface for the HA heartbeat. As an alternative to using the lan4 and lan5 interfaces as described in this recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

Preparing the FortiGates

1. If required, upgrade the firmware running on the FortiGates. All of the FortiGates should be running the same version of FortiOS.

2. On each FortiGate, enter the following command to reset them factory default settings.

```
execute factoryreset
```

You can skip this step if the FortiGates are fresh from the factory. But if their configurations have changed at all, it's a best practice to reset them to factory defaults to reduce the chance of synchronization problems.

In some cases, after resetting to factory defaults you may want to make some initial configuration changes to connect the FortiGates to the network or for other reasons. To write this recipe, the lan switch on the FortiGate-51Es was converted to separate lan1 to lan5 interfaces.

3. Change the primary FortiGate **Host name** to identify it as the primary FortiGate by going to **System > Settings**.

Host name

4. Change the backup FortiGate **Host name** to identify it as Backup-1 by going to **System > Settings**.

Host name

5. Change the third FortiGate **Host name** to identify it as Backup-2 by going to **System > Settings**.

Host name

6. Change the fourth FortiGate **Host name** to identify it as Backup-3 by going to **System > Settings**.

Host name

You can also use the CLI to change the host name. From the Primary FortiGate:

```
config system global
    set hostname Primary
end
```

From the Backup-1 FortiGate:

```
config system global
    set hostname Backup-1
end
```

From the Backup-2 FortiGate:

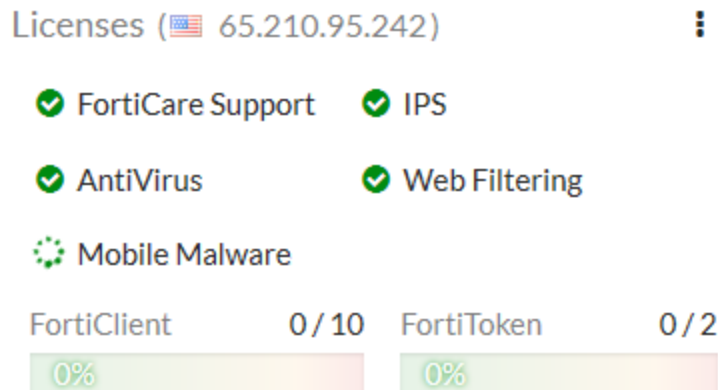
```
config system global
```

```
set hostname Backup-2
end
```

From the Backup-3 FortiGate:

```
config system global
set hostname Backup-3
end
```

7. Register and apply licenses to the FortiGates before configuring the cluster. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, and additional **virtual domains** (VDOMs).



All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add **FortiToken** licenses at any time because they're synchronized to all cluster members.



If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before applying other licenses). When you applying the FortiOS Carrier license the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.

Configuring clustering

1. On the primary FortiGate, enter the following CLI command to set the HA mode to active-passive, set a group-id, group name, and password, increase the device priority to 200, enable override, and configure the heartbeat interfaces (lan4 and lan5 in this example).

```
config system ha
set mode a-p
set group-id 88
set group-name My-vcluster
set password <password>
set priority 200
set override enable
set hbdev lan4 200 lan5 100
end
```



If you have more than one cluster on the same network, each cluster should have a different group id. Changing the group id changes the cluster interface virtual MAC addresses. If your group id causes a MAC address conflict on your network, you can select a different group id.

Enabling override is optional; but it makes sure the FortiGate with the highest device priority becomes the primary unit.

You can also configure most of these settings from the GUI (go to **Global > System > HA**). The group-id and override can only be configured from the CLI.

Mode Active-Passive

Device priority ⓘ 200

Cluster Settings



Group name My-vcluster

Password ●●●●●●●● Change

Session pickup ☐

Monitor interfaces +

Heartbeat interfaces

| | |
|--|----------------|
|  lan4 | × |
|  lan5 | × |
| + | |

Heartbeat Interface Priority ⓘ

lan4 —————|————— 200

lan5 —————|————— 100

- On the Backup-1 FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 50. Setting the device priority to a relatively low value means the Backup-1 FortiGate will most likely always become the backup FortiGate.

```
config system ha
  set mode a-p
  set group-id 88
  set group-name My-vcluster
  set password <password>
  set priority 50
  set override enable
  set hbdev lan4 200 lan5 100
end
```

- On the Backup-2 FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 150. A device priority of 150 is almost as high as the device priority of the primary FortiGate. So if the primary FortiGate fails, the Backup-2 FortiGate should become the new primary FortiGate.

```
config system ha
  set mode a-p
  set group-id 88
```

```

set group-name My-vcluster
set password <password>
set priority 150
set override enable
set hbdev lan4 200 lan5 100
end

```

4. On the Backup-3 FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 100. A device priority of 100 means that if the backup FortiGate fails, the Backup-3 FortiGate will have the lowest device priority so will become the new backup FortiGate.

```

config system ha
set mode a-p
set group-id 88
set group-name My-vcluster
set password <password>
set priority 100
set override enable
set hbdev lan4 200 lan5 100
end

```

After you enable HA, each FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces change to HA virtual MAC addresses.



If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate (or just deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

The FGCP uses virtual MAC addresses for failover. The virtual MAC address assigned to each FortiGate interface depends on the HA group ID. A group ID of 88 sets FortiGate interfaces to the following MAC addresses: 00:09:0f:09:58:00, 00:09:0f:09:58:01, 00:09:0f:09:58:02 and so on. For details, see [Cluster virtual MAC addresses](#).

You can verify that the FGCP has set the virtual MAC addresses by viewing the configuration of each FortiGate interface from the GUI (go to **Network > Interfaces**) or by entering the following CLI command (shown below for `lan2` on a FortiGate-51E):

```

get hardware nic lan2
...
Current_HWaddr 00:09:0f:09:58:01
Permanent_HWaddr 70:4c:a5:98:11:54
...

```

You can also use the `diagnose hardware deviceinfo nic lan2` command to display this information.

The output shows the current hardware (MAC) address (the virtual MAC set by the FGCP) and the permanent hardware (MAC) address for the interface.

Connecting and verifying cluster operation

Connect the FortiGates together and to your networks as shown in the network diagram at the start of the use case. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the Internet, between the cluster and the internal network, and between the cluster and the Engineering network as shown in the diagram. You can use any good quality switches to make these connections.

To make HA heartbeat connections, connect all of the lan4 interfaces to the same switch and all of the lan5 interfaces to another switch.

You can also use fewer switches for all of these connections as long as you configure the switches to separate traffic from the different networks.

When you connect the heartbeat interfaces and power on the FortiGates, they find each other and negotiate to form a cluster. The cluster will have the same IP addresses as the primary FortiGate. You can log into the cluster by logging into the primary FortiGate GUI or CLI using one of the original IP addresses of the primary FortiGate.

Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration. Log into the primary FortiGate CLI and enter this command:

```
diagnose sys ha checksum cluster
```

The command output lists all cluster members' configuration checksums. If both cluster members have identical checksums you can be sure that their configurations are synchronized. If the checksums are different, wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized. If the checksums never become identical you can use the information in Synchronizing the configuration to troubleshoot the problem or visit the Fortinet Support website for assistance.

You can also use the `get system ha status` command to display detailed information about the cluster. .

The **HA Status** dashboard widget also shows synchronization status. Hover over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.

HA Status

| | |
|--------|----------------|
| Mode | Active-Passive |
| Group | My-vcluster |
| Master | ✓ Primary |
| Slave | ✓ Backup-1 |
| Slave | ✓ Backup-2 |
| Slave | ✓ Backup-3 |

Adding VDOMs and setting up virtual clustering

1. Enable VDOMs by going to **System > Settings > System Operation Settings** and enabling **Virtual Domains**. Or enter the following CLI command.

```
config system global
    set vdom-admin enable
end
```

2. Add VDOMs as required. Go to **Global > System > VDOM** and select **Create New**. Or enter the following CLI command to add the Engineering VDOM.




```
config global
  edit Engineering
end
```

3. Configure virtual clustering and VDOM partitioning on the primary FortiGate. The following command enables virtual cluster 2, adds the Engineering VDOM to virtual cluster 2, and sets the virtual cluster 2 device priority of the primary FortiGate to 50.

```
config global
  config system ha
    set vcluster2 enable
    config secondary-vcluster
      set vdom Engineering
      set priority 50
    end
```

You can also configure virtual clustering and VDOM partitioning from the GUI by going to **Global > System > HA**.

VDOM Partitioning

| | |
|-------------------|---|
| Virtual cluster 1 |  root <div style="text-align: center;">+</div> |
| Virtual cluster 2 |  Engineering  <div style="text-align: center;">+</div> |

Secondary Cluster Settings

| | |
|---|----|
| Device priority  | 50 |
| Monitor interfaces | + |

4. Set the virtual cluster 2 priority of the Backup-1 FortiGate to a relatively high value (in this example, 200) so that this FortiGate processes traffic for the VDOMs in virtual cluster 2. The FGCP synchronizes all other HA settings from the primary FortiGate.

You can only configure the virtual cluster 2 priority of the backup FortiGate from the CLI. Use `execute ha manage` to access the backup FortiGate CLI.

```
config global
  config system ha
    config secondary-vcluster
      set priority 200
    end
```

5. Set the virtual cluster 2 priority of the Backup-2 FortiGate to 100 so that if the primary FortiGate fails, Backup-2 will become the primary FortiGate but will have the lowest virtual cluster 2 priority. The FGCP synchronizes all other HA settings from the primary FortiGate.

You can only configure the virtual cluster 2 priority of the Backup-2 FortiGate from the CLI. Use `execute ha manage` to access the backup FortiGate CLI.

```
config global
  config system ha
    config secondary-vcluster
      set priority 100
    end
```

6. Set the virtual cluster 2 priority of the Backup-3 FortiGate to 150 so that if the backup FortiGate fails, Backup-3 will have the highest virtual cluster 2 device priority. The FGCP synchronizes all other HA settings from the primary

FortiGate.

You can only configure the virtual cluster 2 priority of the backup FortiGate from the CLI. Use `execute ha manage` to access the backup FortiGate CLI.



```
config global
  config system ha
    config secondary-vcluster
      set priority 150
    end
```

Checking virtual cluster operation

1. Once again use the `diagnose sys ha checksum cluster` command and the `get system ha status` command to check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.





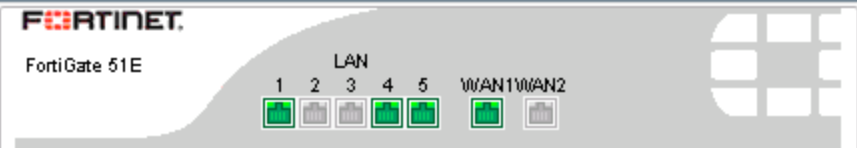


The **HA Status** dashboard widget shows the VDOMs in the virtual clusters. You can hover over the VDOM names to see status information for the VDOMs. You can hover over the host names of each FortiGate to verify that they are synchronized and both have the same checksum.

HA Status

| | |
|-------------------|---|
| Mode | Active-Passive |
| Group | My-vcluster |
| Virtual cluster 1 |  root |
| Virtual cluster 2 |  Engineering |
| Master | ✓ Primary |
| Slave | ✓ Backup-1 |
| Slave | ✓ Backup-2 |
| Slave | ✓ Backup-3 |
| Uptime | 00:09:27:05 |

2. To view more information about the cluster status, click on the **HA Status** widget and select **Configure Settings in System > HA** (or go to **System > HA**).

The HA status page shows all four FortiGates in the cluster. It also shows that Primary is the primary FortiGate for the root VDOM (so the primary FortiGate processes all root VDOM traffic). The page also shows that Backup-1 is the primary FortiGate for the Engineering VDOM (so the backup FortiGate processes all Engineering VDOM traffic).

| Synchronized | Priority | Hostname | Virtual Domains | Serial No. | Role |
|--|----------|----------|-----------------|------------------|--------|
| Virtual cluster 1 (4) | | | | | |
|  | | | | | |
| ✓ | 200 | Primary | • root | FGT51E5618000206 | Master |
|  | | | | | |
| ✓ | 50 | Backup-1 | • root | FGT51E5618000259 | Slave |
|  | | | | | |
| ✓ | 150 | Backup-2 | • root | FGT51E5618000086 | Slave |
|  | | | | | |
| ✓ | 100 | Backup-3 | • root | FGT51E3U17002027 | Slave |
| Virtual cluster 2 (4) | | | | | |
|  | | | | | |
| | 50 | Primary | • Engineering | FGT51E5618000206 | Slave |
|  | | | | | |
| | 200 | Backup-1 | • Engineering | FGT51E5618000259 | Master |
|  | | | | | |

Results

All root VDOM traffic should now be flowing through the primary FortiGate and Engineering VDOM traffic should be flowing through the backup FortiGate. If the primary FortiGate becomes unavailable, the cluster negotiates and traffic fails over and all traffic would be processed by the backup FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.



If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.






You will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\  
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\  
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\  
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\  
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\  
Request timeout for icmp_seq 75\  
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\  
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\  
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\  
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\  
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\  
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\  
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\  
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```



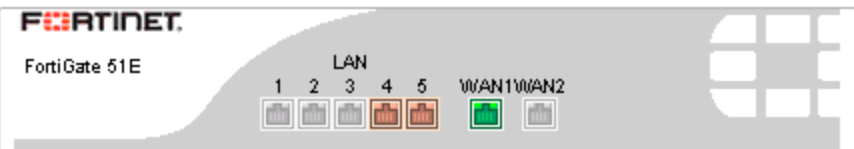



You can log into the cluster GUI or CLI using the same IP address as you had been using to log into the primary FortiGate. If the primary FortiGate is powered off you will be logging into the Backup-1 FortiGate. Check the host name to verify the FortiGate that you have logged into.

After the primary FortiGate fails the **HA Status** dashboard widget shows that the Backup-2 has become the primary FortiGate.

HA Status

| | |
|-------------------|---|
| Mode | Active-Passive |
| Group | My-vcluster |
| Virtual cluster 1 |  root |
| Virtual cluster 2 |  Engineering |
| Master |  Backup-2 |
| Slave |  Backup-1 |
| Slave |  Backup-3 |
| Uptime | 00:10:19:01 |

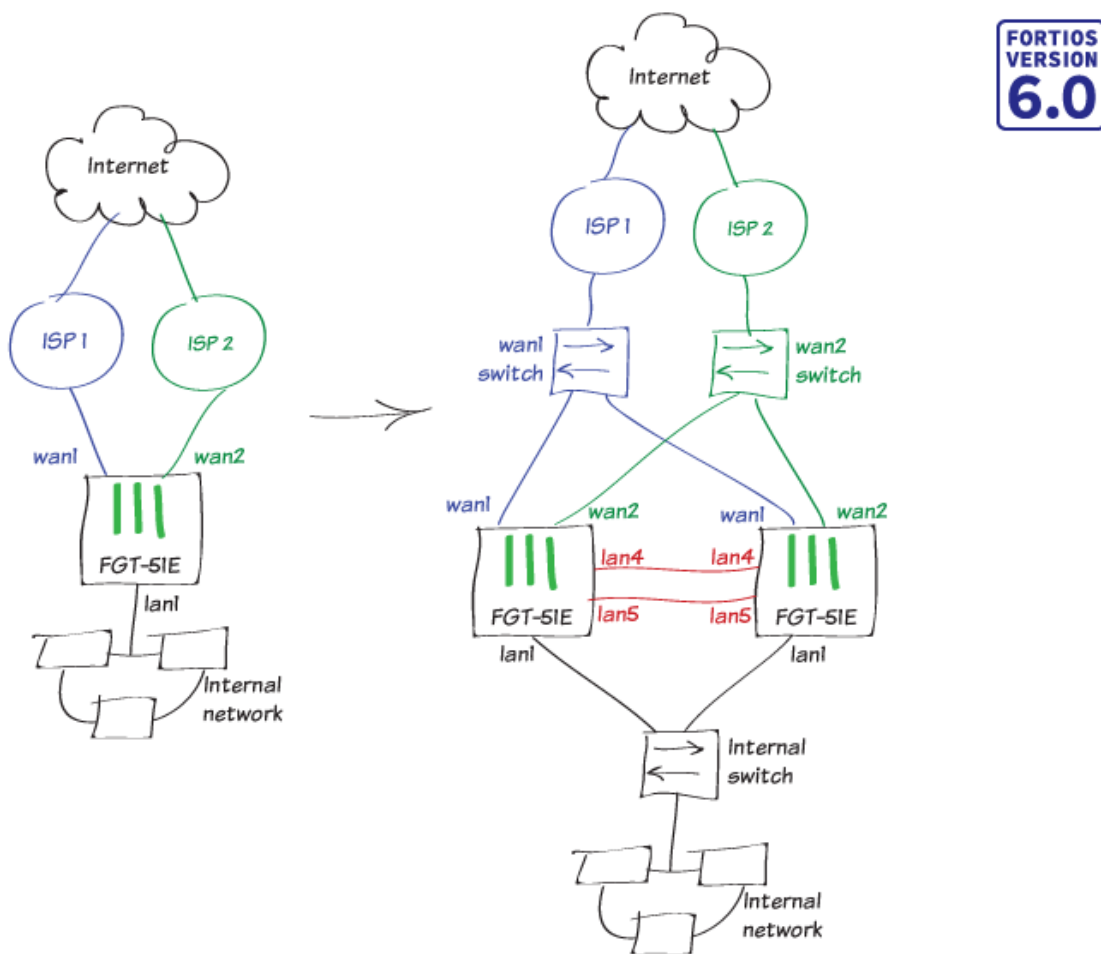
The **System > HA** page shows that the Backup-2 FortiGate has become the primary FortiGate for virtual cluster 1. This page also shows that the Backup-1 FortiGate continues to process virtual cluster 2 traffic.

| Synchronized | Priority | Hostname | Virtual Domains | Serial No. | Role |
|---|----------|----------|-----------------|------------------|--------|
| Virtual cluster 1 (3) | | | | | |
|  | | | | | |
| ✓ | 150 | Backup-2 | • root | FGT51E5618000086 | Master |
|  | | | | | |
| ✓ | 50 | Backup-1 | • root | FGT51E5618000259 | Slave |
|  | | | | | |
| ✓ | 100 | Backup-3 | • root | FGT51E3U17002027 | Slave |
| Virtual cluster 2 (3) | | | | | |
|  | | | | | |
| | 100 | Backup-2 | • Engineering | FGT51E5618000086 | Slave |
|  | | | | | |
| | 200 | Backup-1 | • Engineering | FGT51E5618000259 | Master |
|  | | | | | |
| | 128 | Backup-3 | • Engineering | FGT51E3U17002027 | Slave |

If you restart the primary FortiGate, after a few minutes it should rejoin the cluster and because override is enabled, the original virtual cluster configuration should be re-established. Traffic may be temporarily disrupted when the restarted primary FortiGate rejoins the cluster.

You can also try powering off other FortiGates in the virtual cluster to see how the cluster adapts to the failover. Because of the device priority configuration, if two FortiGates are operating, virtual cluster 1 and virtual cluster 2 traffic will be distributed between them.

SD-WAN with FGCP HA (expert)

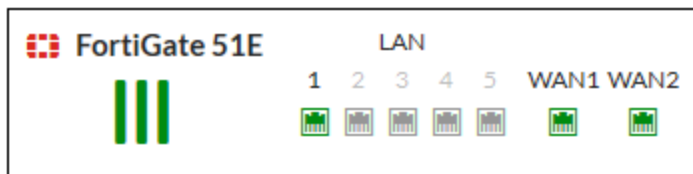


This use case provides an example of how to set up a FortiGate for redundant Internet connectivity using SD-WAN and then convert this single FortiGate into an FGCP HA cluster of two FortiGates. This SD-WAN HA configuration allows you to load balance your Internet traffic between multiple ISP links and provides redundancy for your network's Internet connection if your primary ISP is unavailable or if one of the FortiGates in the HA cluster fails.

This use case features two FortiGate-51Es, which have a 5-port switch lan interface. Before starting the steps in this recipe, we converted the lan interface to 5 separate interfaces (lan1 to lan5). The lan1 interface connects to the internal network, the wan1 interface connects to one Internet service provider (ISP) and the wan2 to a second ISP. For the FGCP HA configuration, the lan4 and lan5 interfaces become HA heartbeat interfaces.

Connecting the FortiGate to your ISPs

Connect the Internet-facing ports (WAN ports) on the FortiGate to your ISP devices. Connect WAN1 to the ISP that you want to use for most traffic. Connect WAN2 to the other ISP.



Removing existing configuration references to interfaces


Before you can configure FortiGate interfaces as SD-WAN members, you must remove or redirect existing configuration references to those interfaces in routes and security policies. This includes the default Internet access policy that's included with many FortiGate models. Note that after you remove the routes and security policies, traffic can't reach the WAN ports through the FortiGate.

Redirecting the routes and policies to reference other interfaces avoids your having to create them again later. After you configure SD-WAN, you can reconfigure the routes and policies to reference the SD-WAN interface.





1. Go to **Network > Static Routes** and delete any routes that use WAN1 or WAN2.
2. Go to **Policy & Objects > IPv4 Policy** and delete any policies that use WAN1 or WAN2.

Creating the SD-WAN interface







1. Go to **Network > SD-WAN** and set **Status** to **Enable**.
Under SD-WAN Interface Members, select + and select wan1. Set the Gateway to the default gateway for this interface. This is usually the default gateway IP address of the ISP that this interface is connected to. Repeat these steps to add wan2.

Name SD-WAN
 Type SD-WAN Interface
 Status  Enable Disable

SD-WAN Interface Members

Interface  wan1 
 Gateway 172.25.176.1
 Status Enable Disable
 Interface  wan2 
 Gateway 172.25.177.1
 Status Enable Disable

- Go to **Network > Interfaces** and verify that the virtual interface for SD-WAN appears in the interface list. You can expand SD-WAN to view the ports that are included in the SD-WAN interface.

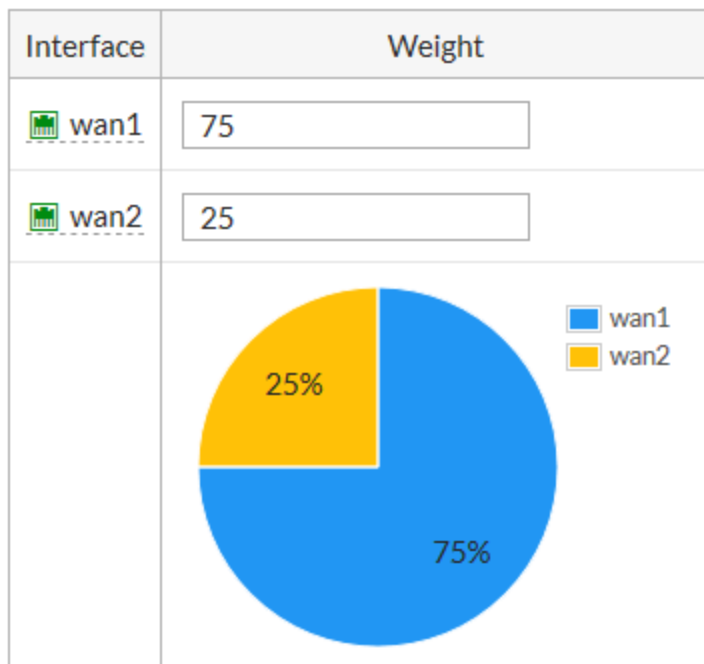
| SD-WAN Interface (3) | | | | | |
|---|---|------|--|-----------------------------|--|
| SD-WAN | | | | SD-WAN Interface | |
|  |  | wan1 | | 172.25.176.33 255.255.255.0 |  Physical Interface |
|  |  | wan2 | | 172.25.177.33 255.255.255.0 |  Physical Interface |

Configuring SD-WAN load balancing

- Go to **Network > SD-WAN Rules** and edit the rule named **sd-wan**.
- In the **Load Balancing Algorithm** field, select **Volume**, and prioritize WAN1 to serve more traffic.
 In the example, the ISP connected to WAN1 is a 40Mb link, and the ISP connected to WAN2 is a 10Mb link, so we balance the weight 75% to 25% in favor of WAN1.

Load Balancing Algorithm


| Source IP | Sessions | Spillover | Source-Destination IP | Volume |
|-----------|----------|-----------|-----------------------|--------|
|-----------|----------|-----------|-----------------------|--------|



Creating a static route for the SD-WAN interface



1. Go to **Network > Static Routes** and create a route.
2. In the **Destination** field, select **Subnet**, and leave the destination IP address and subnet mask as 0.0.0.0/0.0.0.0.
3. In the Interface field, select the SD-WAN interface from the drop-down menu.
4. Ensure that **Status** is set to **Enable**.

Destination ⓘ Subnet Internet Service

Interface  SD-WAN ▼

Administrative Distance ⓘ








Comments 0/255

Status  Enabled  Disabled

5. If you previously removed or redirected existing references in routes to interfaces that you wanted to add as SD-WAN interface members, you can now reconfigure those routes to reference the SD-WAN interface.

Configuring a security policy for SD-WAN

1. Configure a security policy that allows traffic from your organization's internal network to the SD-WAN interface.
2. Go to **Policy & Objects > IPv4 Policy** and create a policy.
3. Set **Incoming Interface** to the interface that connects to your organization's internal network, and set **Outgoing Interface** to the SD-WAN interface.
4. Enable **NAT** and apply **Security Profiles** as required.
5. Configure other policy options as required.

| | |
|--|---|
| Name  | Internet Access |
| Incoming Interface |  lan1 ▼ |
| Outgoing Interface |  SD-WAN ▼ |
| Source |  all ✕ + |
| Destination |  all ✕ + |
| Schedule |  always ▼ |
| Service |  ALL ✕ + |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒

Configuring the FortiGate for HA

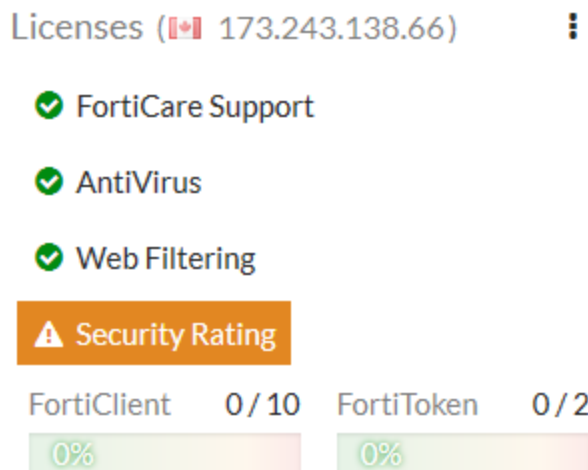
1. Change the **Host name** to identify this FortiGate as the primary FortiGate. From the **System Information** dashboard widget, select **Configure settings in System > Settings**.

Host name

You can also enter this CLI command:

```
config system global
    set hostname Primary
end
```

2. Register and apply licenses to the primary FortiGate before configuring it for HA operation.



3. Enter this CLI command to set the HA mode to active-passive; set a group ID, group name and password; increase the device priority to a higher value (for example, 250); and enable override.

```
config system ha
set mode a-p
set group-id 100
set group-name My-cluster
set password <password>
set priority 250
set override enable
set hbdev lan4 200 lan5 100
end
```

Enabling override and increasing the device priority means this FortiGate always becomes the primary unit.

This configuration also selects lan4 and lan5 to be the heartbeat interfaces and sets their priorities to 200 and 100 respectively. It's a best practice to set different priorities for the heartbeat interfaces (but not a requirement).

If you have more than one cluster on the same network, each cluster should have a different group ID. Changing the group id changes the cluster interface virtual MAC addresses. If your group ID causes a MAC address conflict on your network, you can select a different group ID.

Override and the group ID can only be configured from the CLI.

```
config system ha
set group-id 100
set override enable
end
```

4. You can also configure most of these settings from the GUI (go to **System > HA**).

Mode Active-Passive

Device priority ⓘ 250

Cluster Settings





Group name My-cluster

Password •••••••• Change



Session pickup ☐

Monitor interfaces +

Heartbeat interfaces

| | |
|--|---|
|  lan4 |  |
|  lan5 |  |
| + | |

Heartbeat Interface Priority ⓘ

| | | |
|------|---|-----|
| lan4 |  | 200 |
| lan5 |  | 100 |

After you enter the CLI command or make changes from the GUI, the FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed to HA virtual MAC addresses.



If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

Configuring the backup FortiGate

If required, change the firmware running on the new FortiGate to the same version as is running on the primary FortiGate.

Enter the following command to reset the new backup FortiGate to factory default settings.

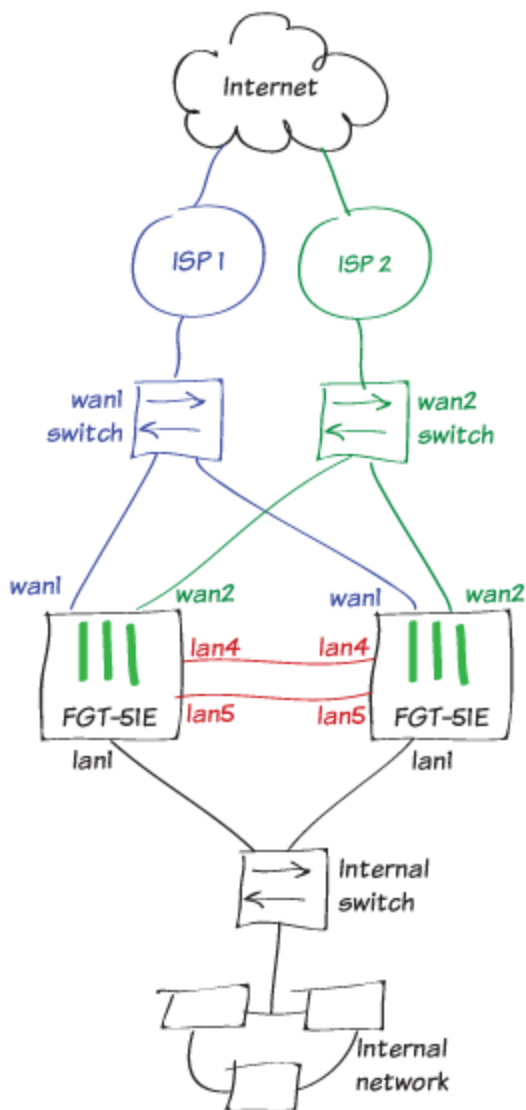
```
execute factoryreset
```

You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all, it's a best practice to reset your FortiGate to factory defaults to reduce the chance of synchronization problems.

Connecting the primary and backup FortiGates

Connect the primary and backup FortiGates to each other and to your network as shown. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the ISPs and between the cluster and the internal network as shown in the network diagram. You can use any good quality switches to make these connections. You can also use one switch for all of these connections as long as you configure the switch to separate traffic from the different networks.



The example shows the recommended configuration of direct connections between the lan4 heartbeat interfaces and between the lan5 heartbeat interfaces.

When the heartbeat interfaces are connected, the FortiGates find each other and negotiate to form a cluster. The primary FortiGate synchronizes its configuration to the backup FortiGate. The cluster forms automatically with minimal or no additional disruption to network traffic.

The cluster will have the same IP addresses as the primary FortiGate had. You can log into the cluster by logging into the primary FortiGate CLI or GUI using one of the original IP addresses of the primary FortiGate.

Checking cluster operation

Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.

1. Log into the primary FortiGate CLI and enter this command:

```
diagnose sys ha checksum cluster
```

The command output lists all cluster members' configuration checksums. If both cluster members have identical checksums you can be sure that their configurations are synchronized. If the checksums are different, wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized.

If the checksums never become identical visit the [Fortinet Support](#) website for assistance.

2. The **HA Status** dashboard widget also shows synchronization status. Mouse over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.

HA Status

Mode **Active-Active**

Group **My-cluster**


Master **✓ Primary**

Slave **✓ Backup**

Uptime **10:03:44:12**

State Changed

3. To view more information about the cluster status, click on the **HA Status** widget and select **Configure Settings in System > HA** (or go to **System > HA**).

| Synchronized | Priority | Hostname | Serial No. | Role | Uptime | Sessions | Throughput |
|---|----------|----------|------------------|--------|----------------|----------|------------|
|  | | | | | | | |
| ✓ | 250 | Primary | FGT51E5618000206 | Master | 3d 37m 48s | 63 | 92.00 kbps |
| ✓ | 50 | Backup | FGT51E5618000259 | Slave | 2d 23h 46m 27s | 31 | 33.00 kbps |

Disabling override (recommended)

When the checksums are identical, disable override on the primary FortiGate by entering the following command:

```
config system ha
  set override disable
end
```

FGCP clusters dynamically respond to network conditions. If you keep override enabled, the same FortiGate always becomes the primary FortiGate. With override enabled; however, the cluster may negotiate more often to keep the same FortiGate as the primary FortiGate, potentially increasing traffic disruptions.

If you disable override it is more likely that the backup FortiGate could become the primary FortiGate. Disabling override is recommended unless its important that the same FortiGate remains the primary FortiGate



To see how enabling override can cause minor traffic disruptions, with override enabled set up a continuous ping through the cluster. Then disconnect power to the backup unit. You will most likely notice a brief disruption in the ping traffic. Try the same thing with override disabled and you shouldn't see this traffic disruption.

With override enabled, the disruption is minor and shouldn't be noticed by most users. For smoother operation, the best practice is to disable override.

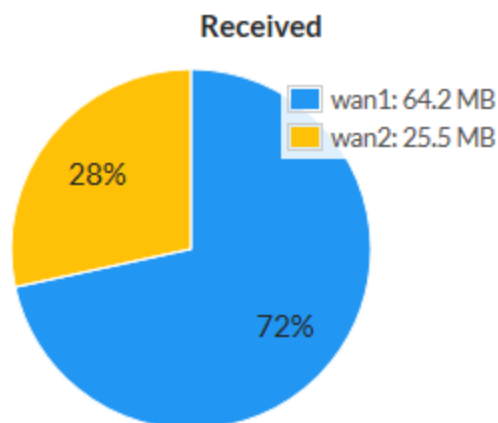
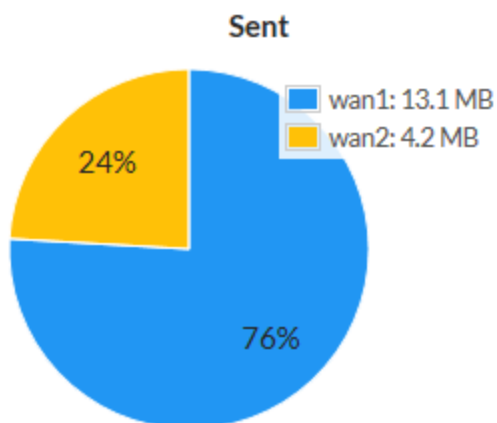
Results

1. Browse the Internet using a computer on your internal network.
2. Go to **Network > SD-WAN**.

In the **SD-WAN Usage** section, you can see the bandwidth, volume, and sessions for traffic on the SD-WAN interfaces.

SD-WAN Usage

Bandwidth Volume Sessions



3. Go to **Monitor > SD-WAN Monitor** to view the number of sessions, bit rate, and more information for each

interface.

| + | Interface | Status | Sessions | Upload | Download |
|---|-----------|--------|---------------------------|--------------------------------|----------------------------------|
| | sd-wan | | | | |
| → | wan1 | | 68 <div><div></div></div> | 255 B/s <div><div></div></div> | 4.03 kB/s <div><div></div></div> |
| → | wan2 | | 30 <div><div></div></div> | 174 B/s <div><div></div></div> | 715 B/s <div><div></div></div> |

Testing HA failover

All traffic should now be flowing through the primary FortiGate. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue operating as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.



If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover

You will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\
Request timeout for icmp_seq 75\
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to log into the primary FortiGate. If the primary FortiGate is powered off you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into. The FortiGate continues to operate in HA mode and if you restart the primary FortiGate, after a few minutes it should rejoin the cluster and operate as the backup FortiGate. Traffic should not be disrupted when the restarted primary unit rejoins the cluster.

Testing ISP failover

1. To test failover of the redundant Internet configuration, you must simulate a failed Internet connection to one of the ports. You can do so by disconnecting power from the wan1 switch or otherwise disconnecting the wan1 interfaces of both FortiGates from ISP 1.

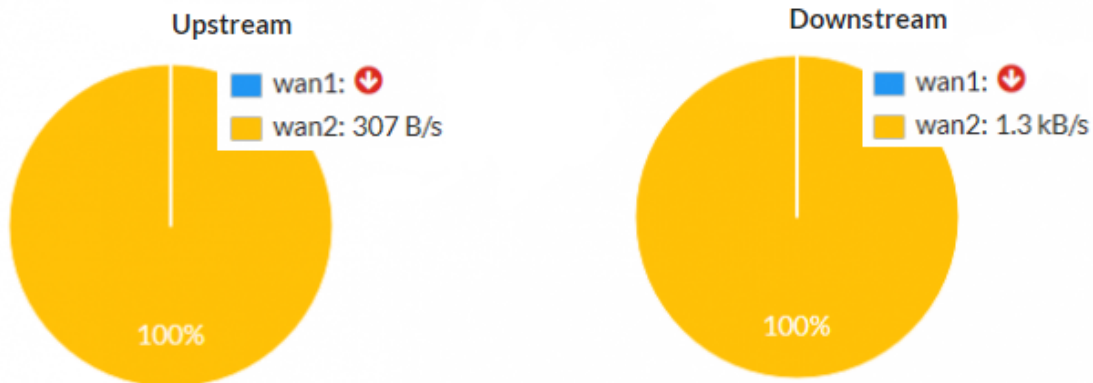
2. Verify that users still have Internet access by navigating to **Monitor > SD-WAN Monitor**. The **Upload** and **Download** values for WAN1 show that traffic isn't going through that interface.

| + | Interface | Status | Sessions | Upload | Download |
|---|-----------|--------|----------|---------|-----------|
| | sd-wan | | | | |
| | wan1 | | 16 | 0 B/s | 0 B/s |
| | wan2 | | 103 | 242 B/s | 1.24 kB/s |

3. Go to **Network > SD-WAN**. In the **SD-WAN Usage** section, you can see that bandwidth, volume, and sessions have diverted entirely through WAN2.

SD-WAN Usage

Bandwidth Volume Sessions



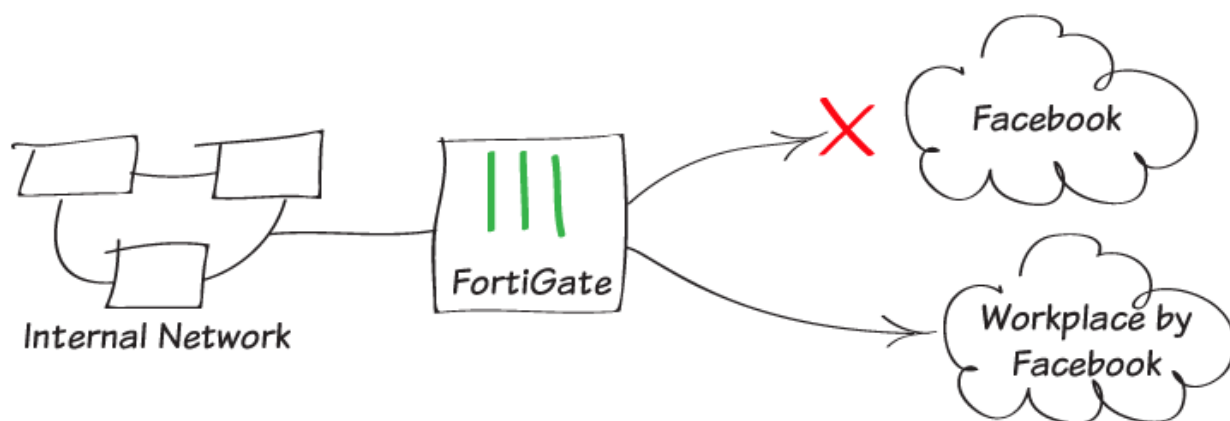
Users on the internal network shouldn't notice the WAN1 failure. Likewise, if you're using the WAN1 gateway IP address to connect to the admin dashboard, nothing should change from your perspective. It appears as though you're still connecting through WAN1.

4. After you verify successful failover, re-establish the connection to ISP 1.

Security profiles

This section contains information about using FortiOS security features to protect your network.

Blocking Facebook while allowing Workplace by Facebook



In this recipe, you block access to Facebook using web filtering, while making an exception to allow access to Workplace by Facebook.

Creating a web filter profile

1. To make sure the features you need are available in the GUI, go to **System > Feature Visibility**. Under **Security Features**, enable **Web Filter**. Under **Additional Features**, enable **Multiple Security Profiles**.

| Security Features | Additional Features |
|---|--|
| Feature Set: Custom | <input type="checkbox"/> Advanced Endpoint Control |
| <input checked="" type="checkbox"/> AntiVirus | <input type="checkbox"/> Allow Unnamed Policies |
| <input checked="" type="checkbox"/> Application Control | <input type="checkbox"/> DNS Database |
| <input checked="" type="checkbox"/> DLP | <input type="checkbox"/> Domain & IP Reputation |
| <input checked="" type="checkbox"/> Endpoint Control | <input type="checkbox"/> DoS Policy |
| <input type="checkbox"/> Intrusion Prevention | <input type="checkbox"/> Email Collection |
| <input checked="" type="checkbox"/> Web Filter | <input checked="" type="checkbox"/> Implicit Firewall Policies |
| | <input type="checkbox"/> Load Balance |
| | <input type="checkbox"/> Local In Policy |
| | <input type="checkbox"/> Local Reports |
| | <input type="checkbox"/> Multicast Policy |
| | <input type="checkbox"/> Multiple Interface Policies |
| | <input checked="" type="checkbox"/> Multiple Security Profiles |

- To create a web filter profile, go to **Security Profiles > Web Filter** and select .
- Enter a **Name** for the profile. Under **Static URL Filter**, enable **URL Filter**. Create a new URL filter to block Facebook. Set **URL** to *facebook.com*, **Type** to **Wildcard**, and **Action** to **Block**.

| | |
|--------|---|
| URL | <input type="text" value="facebook.com"/> |
| Type | <input type="button" value="Simple"/> <input type="button" value="Reg. Expression"/> <input checked="" type="button" value="Wildcard"/> |
| Action | <input type="button" value="Exempt"/> <input checked="" type="button" value="Block"/> <input type="button" value="Allow"/> <input type="button" value="Monitor"/> |
| Status | <input checked="" type="checkbox"/> |

- Create a **URL** filter to allow Workplace by Facebook. Set URL to your Workplace by Facebook site (in the example, *fortinet.facebook.com*), **Type** to **Simple**, and **Action** to **Allow**.

URL

Type Simple Reg. Expression Wildcard

Action Exempt Block Allow Monitor

Status ☒

URL filters are applied in the order that they are listed. Make sure the filter allowing Workplace by Facebook is located above the filter blocking Facebook.

Name

Comments 0/255

☐ FortiGuard category based filter

☒ Static URL Filter

URL Filter ☒

| + Create | Edit | Delete | <input type="text" value="Search"/> | Q |
|--------------------------|----------------------|---|--|-------------------|
| URL | Type | Action | Status | |
| fortinet.facebook.com | Simple | <input checked="" type="checkbox"/> Allow | <input checked="" type="checkbox"/> Enable | |
| facebook.com | Wildcard | <input type="checkbox"/> Block | <input checked="" type="checkbox"/> Enable | |

Applying the security profiles

1. To apply the security profiles to traffic, go to **Policy > IPv4 Policy** and edit the policy allowing Internet access.
2. Under **Security Profiles**, enable **Web Filter** and set it to use the new profiles.
3. Set **SSL Inspection** to **certificate-inspection**.

AntiVirus ☐

Web Filter ☒ WEB block-facebook [Edit](#)

DNS Filter ☐

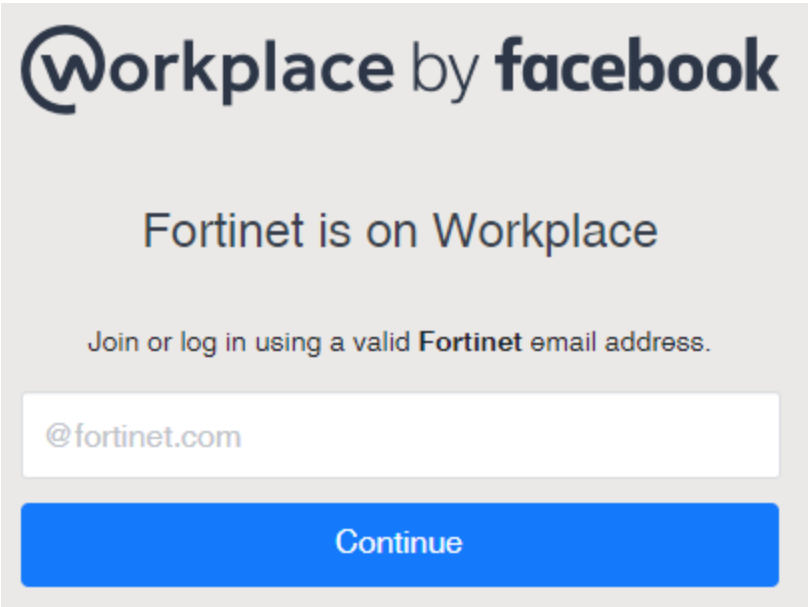
Application Control ☐

SSL Inspection ☒ SSL certificate-inspection [Edit](#)

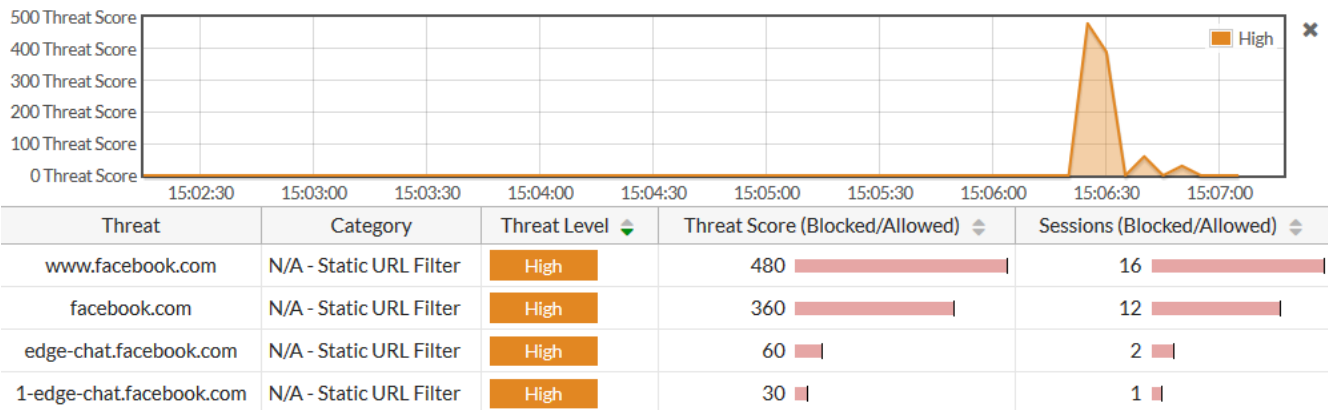
Results

Attempt to access www.facebook.com. Access is blocked. Access is also blocked for the Facebook app.

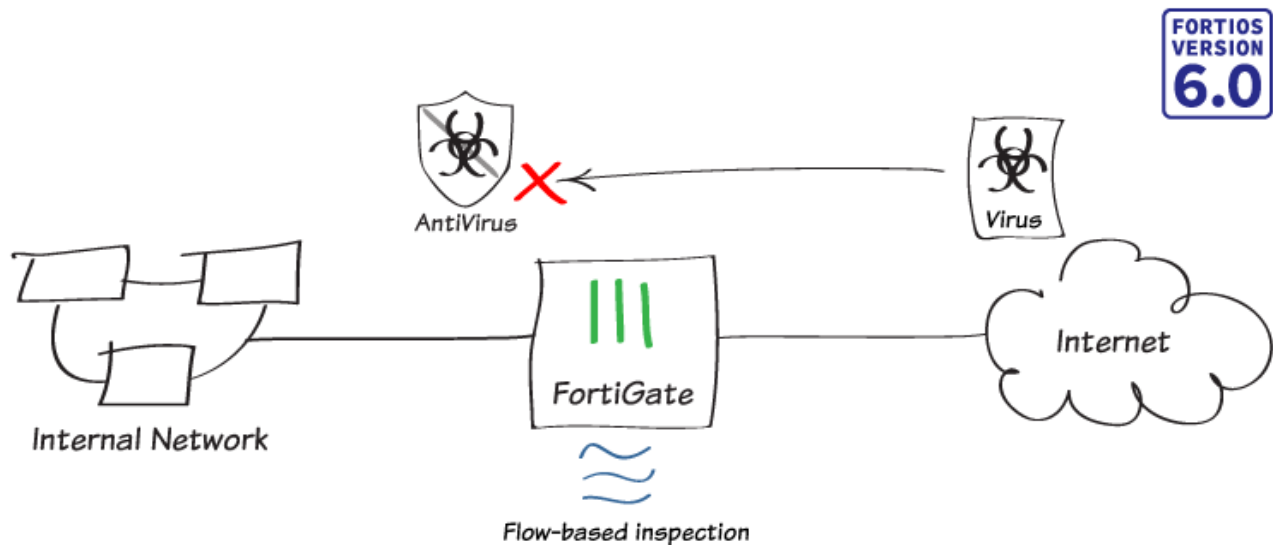
Browse to your Workplace by Facebook site. Access is allowed.



To view information about the blocked traffic, go to **FortiView > Threats**. The page shows the blocked attempts to access Facebook.



Antivirus scanning using flow-based inspection



In this recipe, you will turn on flow-based inspection on your FortiGate and apply flow-based antivirus scanning to network traffic.

For more information about the different antivirus inspection modes available in FortiOS, see FortiOS antivirus inspection modes.

Verifying the inspection mode

1. Flow-based is the default inspection mode for FortiOS. To verify that your FortiGate is in this mode, go to **System > Settings** and locate **System Operations Settings**.
2. Verify that **Inspection Mode** is set to **Flow-based** and **NGFW Mode** is set to **Profile-based**.

System Operation Settings

Inspection Mode **Flow-based** Proxy

NGFW Mode **Profile-based** Policy-based

Virtual Domains ☐

Configuring the AntiVirus profile

1. Go to **System > Feature Visibility** and verify that **AntiVirus** is enabled under **Security Features**.

Security Features

Feature Set: Custom

- ☒ AntiVirus +
- ☒ Application Control +
- ☒ DNS Filter +
- ☒ Endpoint Control +
- ☒ Intrusion Prevention +
- ☒ Web Filter +

2. To edit the default antivirus profile, go to **Security > Profiles AntiVirus**.
3. Set **Scan Mode** to **Full** and **Detect Viruses** to **Block**.
4. Under **APT Protection Options**, enable **Use Virus Outbreak Prevention Database** to provide an additional layer of protection from early stage virus outbreaks.

Name default

Comments Scan files and block viruses. 29/255

Scan Mode Quick **Full**

Detect Viruses **Block** Monitor

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Send Files to FortiSandbox Cloud for Inspection **None** All Supported Files

Use Virus Outbreak Prevention Database i ☒

Use FortiSandbox Database i ☐

Include Mobile Malware Protection ☒

Enabling antivirus in a policy

Delete this text and replace it with your own content.

1. To edit your Internet access policy, go to **Policy & Objects > IPv4 Policy**.
2. Under **Security Profiles**, enable **AntiVirus** and select the **default** profile.
3. **SSL Inspection** is enabled by default. Select **deep-inspection**.

Security Profiles

| | | | |
|----------------------------------|-------------------------------------|--------------------------------|--|
| AntiVirus | <input checked="" type="checkbox"/> | <div>AV default</div> | |
| Web Filter | <input type="checkbox"/> | | |
| DNS Filter | <input type="checkbox"/> | | |
| Application Control | <input type="checkbox"/> | | |
| IPS | <input type="checkbox"/> | | |
| Proxy Options | <input checked="" type="checkbox"/> | <div>PRX default</div> | |
| SSL Inspection | <input checked="" type="checkbox"/> | <div>SSL deep-inspection</div> | |
| Mirror SSL Traffic to Interfaces | <input type="checkbox"/> | | |



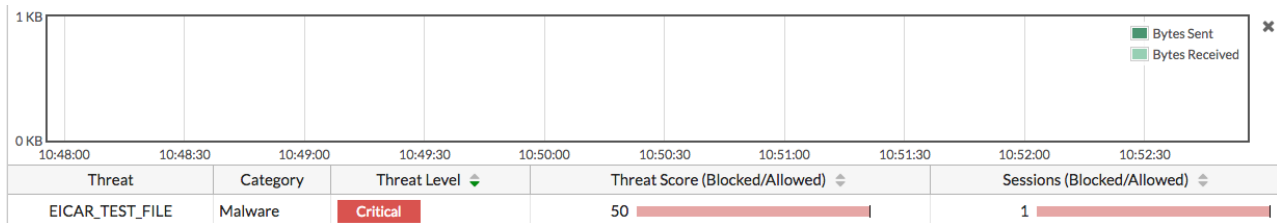
Using the deep-inspection profile may cause certificate errors. See **Preventing certification warnings** for more information.

Results

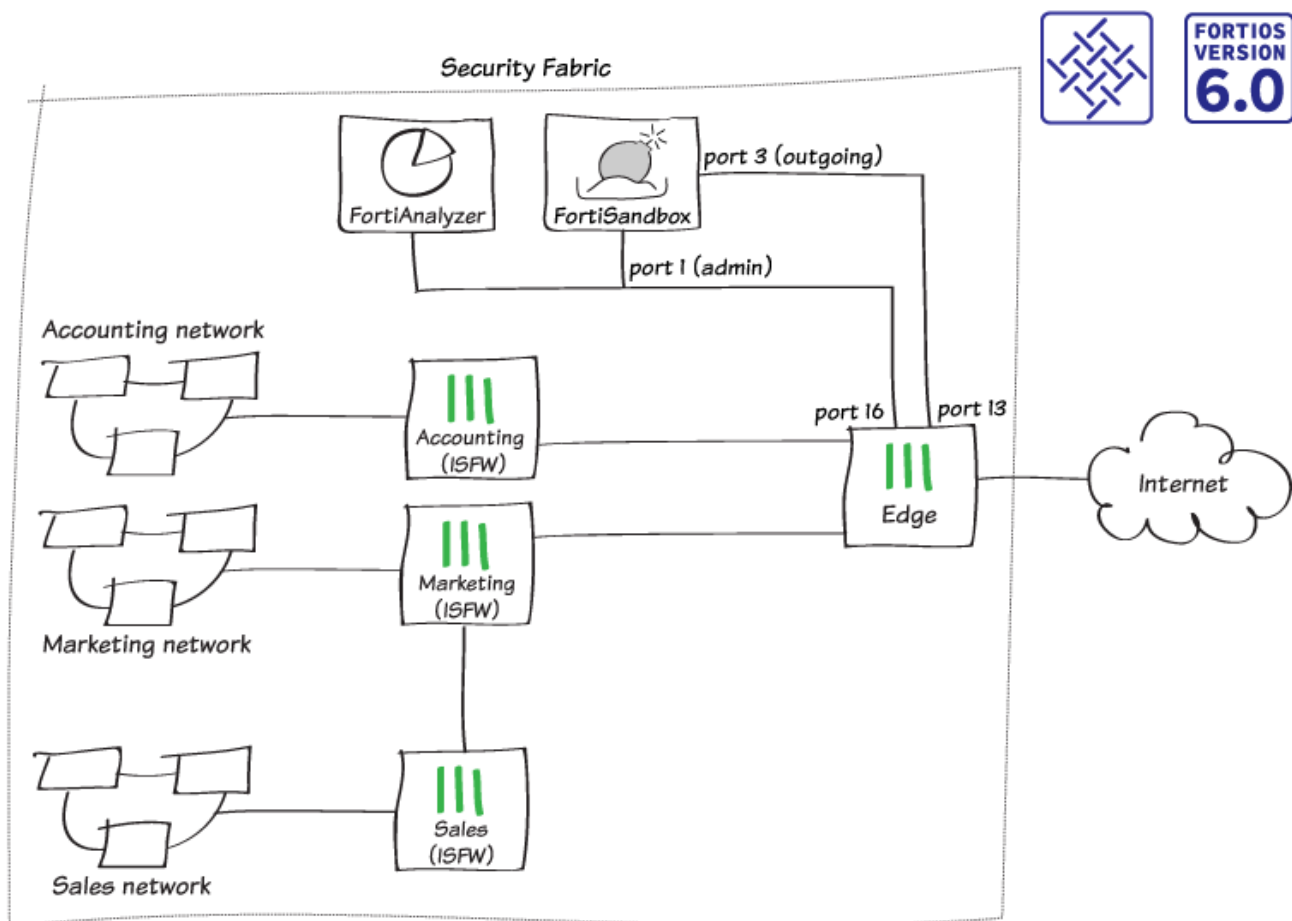
1. To test the antivirus scanning, go to www.eicar.org and attempt to download a test file. The browser will display a message denying permission to download the file.



2. To view information about the blocked file, go to **FortiView > Traffic from LAN/DMZ > Threats**.



FortiSandbox in the Fortinet Security Fabric



In this recipe, you will add a FortiSandbox to the Fortinet Security Fabric and configure each FortiGate in the network to send suspicious files to FortiSandbox for sandbox inspection. The FortiSandbox scans and tests these files in isolation from your network.

This example uses the Security Fabric configuration created in the Fortinet Security Fabric collection recipe. The FortiSandbox connects to the root FortiGate in the Security Fabric, known as External. There are two connections between the devices:

- FortiSandbox port 1 (administration port) connects to Edge port 16
- FortiSandbox port 3 (VM outgoing port) connects to Edge port 13

If possible, you can also use a separate Internet connection for FortiSandbox port 3, rather than connecting through the Edge FortiGate to use your main Internet connection. This configuration avoids having IP addresses from your main network blacklisted if malware that's tested on the FortiSandbox generates an attack. If you use this configuration, you can skip the steps listed for FortiSandbox port 3.

Checking the Security Rating

On Edge (the root FortiGate in the Security Fabric), go to **Security Fabric > Security Rating**.

Since you haven't yet installed a FortiSandbox in your network, the Security Fabric fails the **Advanced Threat Protection** check.



In the example, the **Security Rating Score** decreases by 30 points for each of the four FortiGates in the Security Fabric.

| Threat and Vulnerability Management 4 | | | |
|---|------------|-----|---|
| Advanced Threat Protection Suspicious files should be submitted to FortiSandbox Appliance/FortiSandbox Cloud for inspection. | Edge | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |
| | Sales | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |
| | Marketing | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |
| | Accounting | -30 | Configure AntiVirus profiles to send files to FortiSandbox Appliance/FortiSandbox Cloud for inspection. |

Connecting the FortiSandbox and Edge

1. Connect to the FortiSandbox.
2. To edit **port1**, which is used for communication between the FortiSandbox and the rest of the Security Fabric, go to **Network > Interfaces**.
3. Set **IP Address/Netmask** to an internal IP address.

In this example, the FortiSandbox connects to the same subnet as the FortiAnalyzer that you installed previously, using the IP address 192.168.65.20.

| Interface Status | |
|-------------------|---|
| Interface: | port1 (administration port) |
| Interface Status: |  |
| Link Status: |  |



| IP Address / Netmask | |
|----------------------|-----------------------------|
| IPv4: | 192.168.65.20/255.255.255.0 |
| IPv6: | |

| Access Rights | |
|-------------------------------------|--------|
| <input checked="" type="checkbox"/> | HTTP |
| <input checked="" type="checkbox"/> | SSH |
| <input checked="" type="checkbox"/> | Telnet |

4. Edit **port3**.

This port is used for outgoing communication by the virtual machines (VMs) running on the FortiSandbox. It's recommended that you connect this port to a dedicated interface on your FortiGate to protect the rest of the network from threats that the FortiSandbox is currently investigating.

5. Set **IP Address/Netmask** to an internal IP address (in the example, 192.168.179.10/255.255.255.0).

| Interface Status | |
|-------------------|---|
| Interface: | port3 (VM outgoing port) |
| Interface Status: |  |
| Link Status: |  |

| IP Address / Netmask | |
|----------------------|------------------------------|
| IPv4: | 192.168.179.10/255.255.255.0 |
| IPv6: | |

6. To add a static route, go to **Network > System Routing**. Set **Gateway** to the IP address of the FortiGate interface that port 1 connects to (in the example, 192.168.65.2).

| | |
|----------------------|-----------------|
| Destination IP/Mask: | 0.0.0.0/0.0.0.0 |
| Gateway: | 192.168.65.2 |
| Device: | port1 |

7. Connect to Edge.
8. To configure the port that connects to port3 on the FortiSandbox (in the example, **port13**), go to **Network > Interfaces**. Set **IP/Network Mask** to an address on the same subnet as port 3 on the FortiSandbox (in the example, 192.168.179.2/255.255.255.0)


Interface Name port13 (00:09:0F:09:19:06)

Alias FortiSandbox-Internet

Link Status Down 

Type Physical Interface

Tags

Role 

LAN

 Add Tag Category

Address

Addressing mode **Manual** DHCP


IP/Network Mask 192.168.179.2/255.255.255.0


Administrative Access

IPv4 ☐ HTTPS ☐ HTTP  ☒ PING ☐ FMG-Access
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry

☐ DHCP Server

Networked Devices

Device Detection 

Active Scanning 

9. Connect the FortiSandbox to the Security Fabric.

Allowing VM Internet access

1. Connect to Edge.
2. To create a policy that allows connections from the FortiSandbox to the Internet, go to **Policy & Objects > IPv4 Policy**.

| | |
|--------------------|--|
| Name ⓘ | FortiSandbox-Internet |
| Incoming Interface | <div> FortiSandbox-Internet (port13) </div> <div>+</div> |
| Outgoing Interface | <div> Internet (port9) </div> <div>+</div> |
| Source | <div> all </div> <div>+</div> |
| Destination | <div> all </div> <div>+</div> |
| Schedule | <div> always </div> <div>▼</div> |
| Service | <div> ALL </div> <div>+</div> |
| Action | <div> <input checked="" type="checkbox"/> ACCEPT </div> <div> <input type="checkbox"/> DENY </div> <div> <input type="checkbox"/> LEARN </div> |

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

3. Connect to FortiSandbox.
4. Go to **Scan Policy > General** and select **Allow Virtual Machines to access external network through outgoing port3**. Set **Gateway** to the IP address of port 13 on the FortiGate.

☒ Allow Virtual Machines to access external network through outgoing port3

| | |
|--|------------------------------|
| Status: | |
| Port3 IP: | 192.168.179.10/255.255.255.0 |
| Gateway: | 192.168.179.2 |
| <input type="checkbox"/> Disable SIMNET if Virtual Machines are not able to access external network through outgoing port3 | |
| DNS: | 208.91.112.53 |
| <input type="checkbox"/> Use Proxy | |

- Go to the **Dashboard** and locate the **System Information** widget. Verify that **VM Internet Access** has a green checkmark beside it.

— System Information

| | |
|-----------------------|--|
| Unit Type | Standalone |
| Host Name | FSA1KD3A14000118 [Change] |
| Serial Number | FSA1KD3A14000118 |
| System Time | Fri Mar 2 16:11:25 2018 EST [Change] |
| Firmware Version | v2.4.1,build0261 (GA) [Update] |
| System Configuration | Last Backup: 2017-11-01 16:38 [Backup/Restore] |
| Current Administrator | admin |
| Uptime | 0 day(s) 1 hour(s) 20 minute(s) |
| Windows VM | ✓ [Upload License] |
| Microsoft Office | ⚠ [Upload License] |
| VM Internet Access | ✓ |

Adding the FortiSandbox to the Security Fabric

- Connect to Edge.
- To add FortiSandbox to the Security Fabric, go to **Security Fabric > Settings**. Enable **Sandbox Inspection**.
- Make sure **FortiSandbox Appliance** is selected and set **Server** to the IP address of port 1 on the FortiSandbox.

☒ Sandbox Inspection

⚠ [No AntiVirus profile has enabled FortiSandbox inspection. Click to Check.](#)


| | | | |
|-------------------|--|--|---------------------|
| FortiSandbox type | FortiSandbox Appliance | FortiSandbox Cloud | Activate FortiCloud |
| Server | <input type="text" value="192.168.65.20"/> | <input type="button" value="Test connectivity"/> | |
| Notifier email | <input type="text"/> | | |

4. Select **Test Connectivity**. An error message appears because Edge hasn't been authorized on the FortiSandbox.

FortiSandbox Server 192.168.65.20


Status Unreachable or not authorized

5. Edge, as the root FortiGate, pushes FortiSandbox settings to the other FortiGates in the Security Fabric. To verify this, connect to Accounting and go to **Security Fabric > Settings**.

 **Sandbox Inspection**







No AntiVirus profile has enabled FortiSandbox inspection. [Click to Check.](#)

FortiSandbox type **FortiSandbox Appliance** FortiSandbox Cloud  **Activate FortiCloud**

Server


Notifier email

6. On the FortiSandbox, go to **Scan Input > Device**. The FortiGates in the Security Fabric (Edge, Accounting, Marketing, and Sales) are listed but the **Auth** column indicates that the devices are unauthorized.

| Device Name | Serial | Malicious | High | Medium | Low | Clean | Others | Malware Pkg | URL Pkg | Auth |
|--|------------------|-----------|------|--------|-----|-------|--------|-------------|---------|------|
|  Marketing | FG81EP4Q16002706 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | 🔒 |
|  Sales | FGT51E3U16001255 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | 🔒 |
|  Edge | FGT6HD3916806070 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | 🔒 |
|  Accounting | F140EP4Q17000149 | 0 | 0 | 0 | 0 | 0 | 0 | N/A | N/A | 🔒 |

7. Select and edit Edge. Under **Permissions & Policies**, select **Authorized**.

8. Repeat this for the other FortiGates.

| Device Status | |
|----------------|---|
| Serial Number: | FGT6HD3916806070 |
| Alias: | Edge |
| IP: | 192.168.55.2 |
| Status: |  |
| Last Modified: | 2018-03-02 14:55:01 |
| Last Seen: | 2018-03-02 16:19:33 |

| Permissions & Policy | |
|----------------------------------|--|
| Authorized: | <input checked="" type="checkbox"/> Last Changed 2018-03-02 14:55:01 |
| New VDOMs Inherit Authorization: | <input checked="" type="checkbox"/> |

| Email Settings | |
|----------------------|-------------------------------------|
| Administrator Email: | |
| Send Notifications: | <input checked="" type="checkbox"/> |
| Send PDF Reports: | <input checked="" type="checkbox"/> |

9. On Edge, go to **Security Fabric > Settings** and test the **Sandbox Inspection** connectivity again. External is now connected to the FortiSandbox.

| | |
|---------------------|--------------------|
| FortiSandbox Server | 192.168.65.20 |
| Status | Service is online. |

Adding sandbox inspection to security profiles

You can apply sandbox inspection with three types of security inspection: antivirus, web filter, and FortiClient compliance profiles. In this step, you add sandbox to all FortiGate devices in the Security Fabric individually, using the profiles that each FortiGate applies to network traffic.

In order to pass the **Advanced Threat Protection** check, you must add sandbox inspection to antivirus profiles for all FortiGate devices in the Security Fabric.

1. Go to **Security Profiles > AntiVirus** and edit the **default** profile.
2. Under **Inspection Options**, set **Send Files to FortiSandbox Appliance for Inspection** to **All Supported Files**.

| | |
|----------------|--|
| Name | <input type="text" value="default"/> |
| Comments | <input type="text" value="Scan files and block viruses."/> 29/255 |
| Scan Mode | <input type="radio"/> Quick <input checked="" type="radio"/> Full |
| Detect Viruses | <input checked="" type="radio"/> Block <input type="radio"/> Monitor |

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Send Files to FortiSandbox Appliance for Inspection



☐ None ☒ All Supported Files

Do not submit files matching types

+

Do not submit files matching file name patterns

+

Use Virus Outbreak Prevention Database  

☐

Use FortiSandbox Database 

☒

Include Mobile Malware Protection

☒

Enable **Use FortiSandbox Database**, so that if the FortiSandbox discovers a threat, it adds a signature for that file to the antivirus signature database on the FortiGate.

3. Go to **Security Profiles > Web Filter** and edit the **default** profile.
4. Under **Static URL Filter**, enable **Block malicious URLs discovered by FortiSandbox**.

Name

Comments 22/255

☒ FortiGuard category based filter

Show ☐ All

- ☒ Local Categories
- ☐ Potentially Liable
- ☐ Adult/Mature Content
- ☒ Bandwidth Consuming
- ☐ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business
- ☐ Unrated

☐ Static URL Filter

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☒

Web Content Filter ☐

If the FortiSandbox discovers a threat, the URL that threat came from is added to the list of URLs that are blocked by the FortiGate.

5. Go to **Security Profiles > FortiClient Compliance Profiles** and edit the default profile. Enable **Security Posture Check**.
6. Enable **Realtime Protection** and **Scan with FortiSandbox**.

☒ Security Posture Check

Realtime Protection ☒

Up-to-date signatures ☐

Scan with FortiSandbox ☒

Third party AntiVirus on Windows ☐

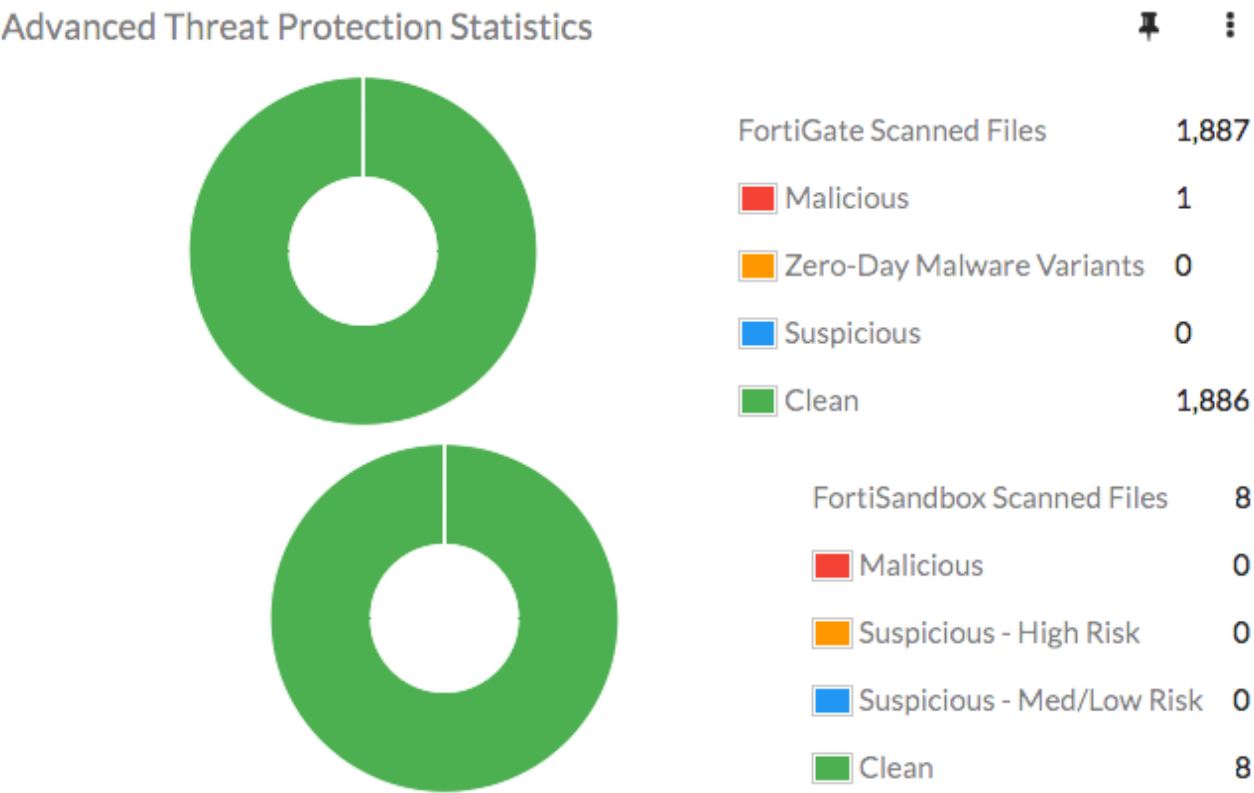
Web Filter ☐

Application Firewall ☐

Non-compliance action

Results

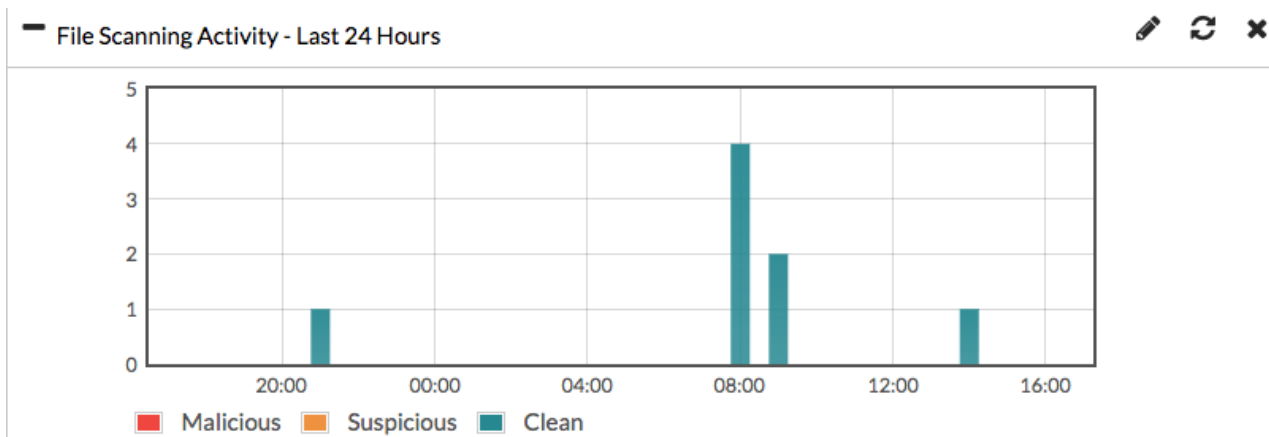
- If a FortiGate in the Security Fabric discovers a suspicious file, it sends the file to the FortiSandbox.
- You can view information about scanned files on either the FortiGate that sent the file or the FortiSandbox.
1. On one of the FortiGate devices, go to the Dashboard and locate the Advanced Threat Protection Statistics widget. This widget shows files that both the FortiGate and FortiSandbox scan.



2. On the FortiSandbox, go to System > Status and view the Scanning Statistics widget for a summary of scanned files.

Scanning Statistics - Last 24 Hours

| Rating | Sniffer | Device(s) | On Demand | Network | Adapter | URL | All |
|--------------------------|---------|-----------|-----------|---------|---------|-----|-----|
| Malicious | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - High Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - Medium Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - Low Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clean | 0 | 8 | 0 | 0 | 0 | 0 | 8 |
| Other | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Processed | 0 | 8 | 0 | 0 | 0 | 0 | 8 |
| Pending | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Processing | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 0 | 8 | 0 | 0 | 0 | 0 | 8 |



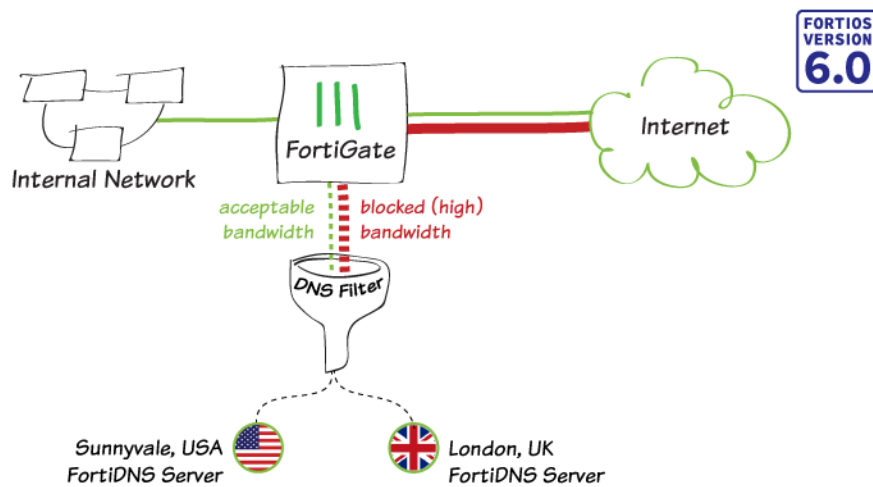
You can also view a timeline of scanning in the File Scanning Activity widget.

- On Edge, go to Security Fabric > Security Rating and run a rating. When it is finished, select the All Results view.

In the example, all four FortiGate devices in the Security Fabric pass the Advanced Threat Protection check and the Security Rating Score increases by 9.7 points for each FortiGate.

| | | |
|--|---------------|------|
| Advanced Threat Protection Suspicious files should be submitted to FortiSandbox Appliance/FortiSandbox Cloud for inspection. | Edge2-Primary | +9.7 |
| | Accounting2 | +9.7 |
| | Marketing2 | +9.7 |
| | Sales2 | +9.7 |

DNS Filtering



In this recipe you will set up DNS filtering to block access to bandwidth consuming websites.

Following the results section, you will find instructions for changing the FortiDNS server that your FortiGate will use to verify domains, as well as troubleshooting information.

If DNS Filter is not listed under **Security Profiles**, go to **System > Feature Visibility**, and enable **DNS Filter** under **Security Features**.



Creating a DNS web filter profile

1. Go to **Security Profiles > DNS Filter**, and edit the default profile.
2. Enable **FortiGuard category based filter**, right-click **Bandwidth Consuming**, and set it to **Block**.

Edit DNS Filter Profile

Name

Comments 22/255

Block DNS requests to known botnet C&C ☒

Enforce 'Safe search' on Google, Bing, YouTube ☐

60631 domains in [botnet package](#).

☒ FortiGuard category based filterPre-configured filters **Custom** G PG-13 R

Show ☐ All

☐ Potentially Liable

☒ Adult/Mature Content

☒ Bandwidth Consuming ✓

☒ Allow

☒ Block

☐ Monitor

Static Domain Filter

Domain Filter ☐

















Enabling DNS filtering in a security policy

All traffic that matches this policy will be redirected to the FortiDNS server.

1. Go to **Policy & Objects > IPv4 Policy**, and edit the outgoing policy that allows Internet access.
2. Under **Security Profiles**, enable **DNS Filter** and set it to **default**.

Proxy Options and **SSL Inspection** profiles are automatically enabled.

Edit Policy

| | |
|--|---|
| Name  | internal-to-wan1 |
| Incoming Interface |  internal  + |
| Outgoing Interface |  wan1  + |
| Source |  all  + |
| Destination |  all  + |
| Schedule |  always ▼ |
| Service |  ALL  + |
| Action |  ACCEPT  DENY  LEARN  IPsec |


Firewall / Network Options

NAT 

IP Pool Configuration  

Security Profiles




AntiVirus 



Web Filter 

DNS Filter   

Application Control 

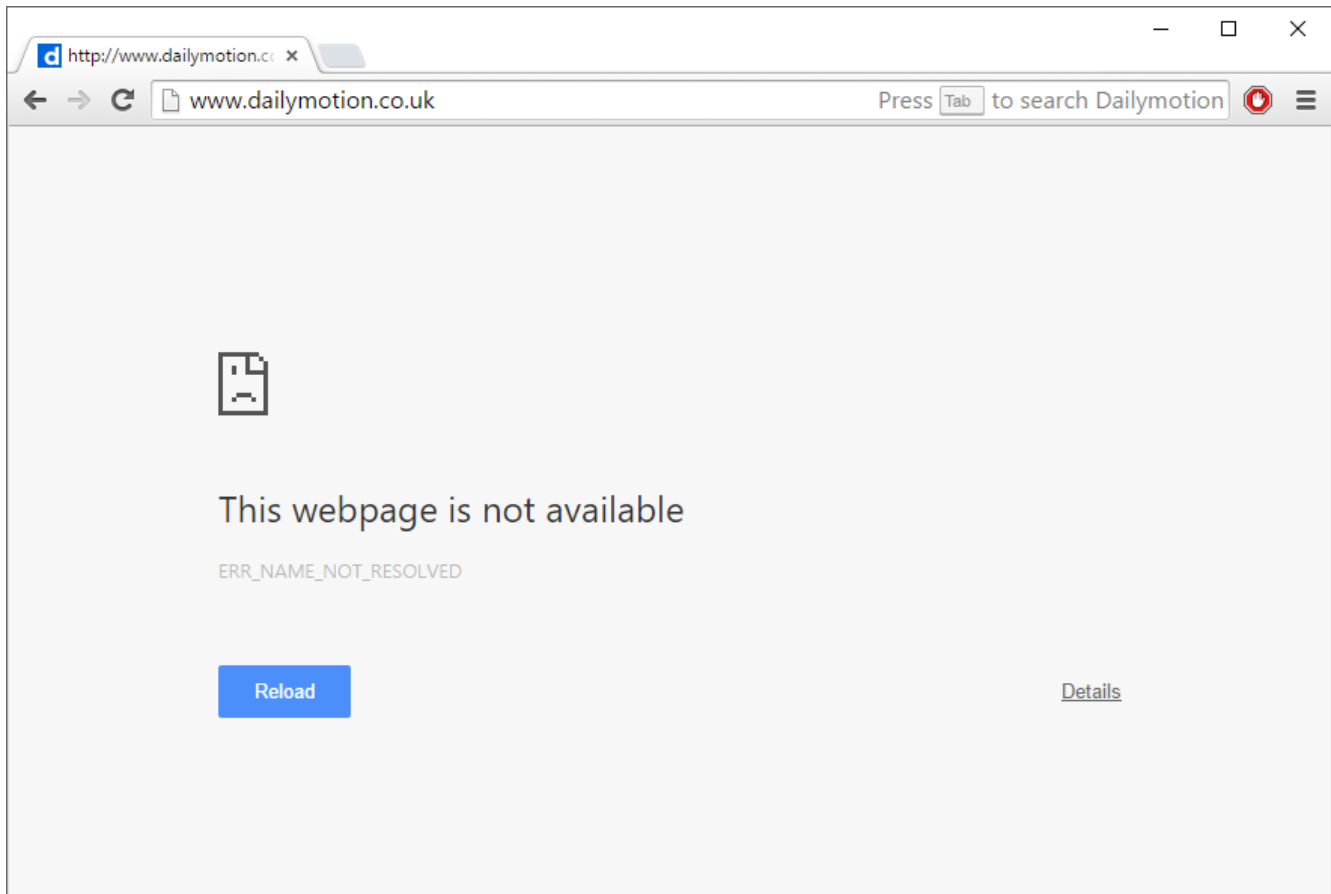
IPS 

Proxy Options   

SSL Inspection   

Results

Open a browser using a computer on the internal network and navigate to [dailymotion.co.uk](http://www.dailymotion.co.uk). The page will be blocked.



Enter the following CLI command to sniff packets with a destination URL that does not belong to the bandwidth consuming category:

```
diagnose sniffer packet any 'port 53 and host 194.153.110.160' 4
```

The resulting output should indicate that the IP (in this example, paris.fr) was allowed by FortiGuard:

```
interfaces=[any]
filters=[port 53]
2.851628 172.20.121.56.59046 -> 208.91.112.52.53: udp 43
2.916281 208.91.112.52.53 -> 172.20.121.56.59046: udp 436
3.336945 10.1.2.102.51755 -> 208.91.112.53.53: udp 37
3.338611 208.91.112.53.53 -> 10.1.2.102.51755: udp 37
```

(Optional) Changing the FortiDNS server and port

You can use the default FortiDNS server located in Sunnyvale, USA (IP address: 208.91.112.220), or you can switch to the server in London, UK (IP address: 194.69.172.53).

Communication between your FortiGate and the FortiDNS server uses Fortinet's proprietary DNS communication protocol.

```
config system fortiguard
  set sdns-server-ip 208.91.112.220
end
```

The North American server should work in most cases, however you can switch to the European server to see if it improves latency.

You can also change the port used to communicate with the FortiDNS server using the following command:

```
config system fortiguard
  set sdns-server-port <value>
end
```

Troubleshooting

The Security Profiles > DNS Filter menu is missing

Go to **System > Feature Visibility** and enable **DNS Filter**.

You Configured DNS Filtering, but it is not working

Verify that **DNS Filter** is enabled in a policy and **SSL Inspection** has been applied as needed (SSL inspection is required in order to block traffic to sites that use HTTPS).

If both settings are enabled, verify that the policy is being used for the correct traffic and that traffic is flowing by going to the policy list and viewing the **Sessions** column.

If the above settings are correct, verify that DNS requests are going through the policy, rather than to an internal DNS server. Also verify that proxy options and SSL/SSH inspection settings have both HTTP and HTTPS enabled and use the correct ports.

Communication with the FortiDNS server fails

Verify that the correct FortiDNS server is configured using the following diagnose command:

```
diag test application dnsproxy 3
```

The resulting output should indicate that communication with the correct FortiDNS server was established. For example:

```
FWF60D4615016384 # diag test application dnsproxy 3
vdom: root, index=0, is master, vdom dns is enabled, mip-169.254.0.1 dns_log=1
dns64 is disabled
dns-server:208.91.112.53:53 tz=0 req=919160 to=545900 res=117880 rt=1800 secure=0
ready=1
dns-server:208.91.112.52:53 tz=0 req=913029 to=520111 res=134810 rt=6 secure=0 ready=1
dns-server:208.91.112.220:53 tz=-480 req=0 to=0 res=0 rt=0 secure=1 ready=1
dns-server:45.75.200.89:53 tz=0 req=0 to=0 res=0 rt=0 secure=1 ready=1
vfid=0, interface=wan1, ifindex=6, recursive, dns
DNS_CACHE: hash-size=2048, ttl=1800, min-ttl=60, max-num=5000
```



```
DNS_FD: udp_s=12 udp_c=14:15 ha_c=18 unix_s=19, unix_nb_s=20, unix_nc_s=21, v6_udp_s=11, v6_udp_c=16:17
```

```
DNS_FD: tcp_s=24, tcp_s6=23
```

```
FQDN: hash_size=1024, current_query=1024
```

```
DNS_DB: response_buf_sz=131072
```

```
LICENSE: expiry=2016-08-15, expired=0, type=2
```

```
FDG_SERVER:208.91.112.220:53
```

```
SERVER_LDB: gid=6d61, tz=-480
```

```
FGD_REDIR:208.91.112.55
```

This CLI result shows that the DNS server IP is set to the North American server, and is being accessed through port 53 (208.91.112.220:53).

Next, verify that bandwidth consuming sites are blocked, while other URLs are allowed.

Go to the CLI Console and enter the following:

```
diagnose sniffer packet any 'port 53' and 'host 195.8.215.138' 4
```

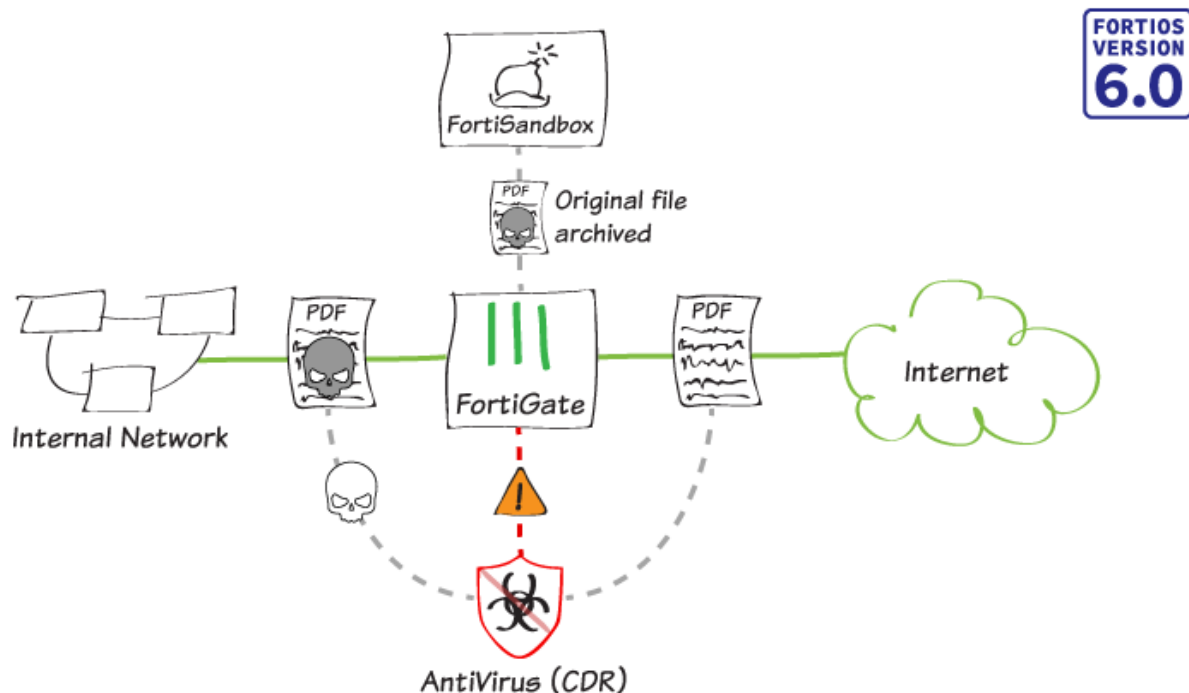
The resulting output should indicate that the IP (in this example, dailymotion.co.uk) was blocked by the FortiDNS server:

```
interfaces=[any]
filters=[port 53]
2.026733 172.20.121.56.59046 -> 208.91.112.220.53: udp 117
2.027316 172.20.121.56.59046 -> 45.75.200.89.53: udp 112
2.028480 172.20.121.56.59046 -> 208.91.112.220.53: udp 116
2.029591 172.20.121.56.59046 -> 208.91.112.220.53: udp 117
```

FortiGuard has the wrong categorization for a website

If you believe a website has been placed in the wrong category by FortiGuard, you can submit the URL for re-classification by going to the [FortiGuard website](#).

Content Disarm and Reconstruction (CDR)



In this recipe you will configure the default AntiVirus security profile to include a new FortiOS 6.0 feature: Content Disarm and Reconstruction (CDR). You will apply this security profile to the Internet access policy so that exploitable content leaving the network is stripped from documents and replaced with content that is known to be safe.

In the example, we will use FortiSandbox as the original file destination, where the original file is archived and can be retrieved if necessary. The CDR feature works without FortiSandbox configured, but only if you wish to discard the original file.

Content that can be scanned includes PDF and Microsoft Office files leaving the network on CDR-supported protocols* (for more information, refer to the Security Profiles handbook).

Note that the FortiGate must be in Proxy inspection mode for CDR to function.

Setting the system inspection mode

Go to **System > Settings** and set **System Operation Settings > Inspection Mode** to **Proxy**.

System Operation Settings

Inspection Mode

Flow-based

Proxy

Testing FortiSandbox connectivity

1. On the FortiGate, go to **Security Fabric > Settings** and enable **Sandbox Inspection**.
2. Select your **FortiSandbox type** and **Server** address.
3. Confirm that the service is available by selecting **Test connectivity**.
The Status should read "Service is online."

Test FortiSandbox Connectivity

| | |
|---------------------|--------------------|
| FortiSandbox Server | 172.25.176.128 |
| Status | Service is online. |

Enabling Content Disarm and Reconstruction

1. Go to **Security Profiles > AntiVirus**.
2. Under **APT Protection Options**, enable **Content Disarm and Reconstruction** and select the **Original File Destination**.

APT Protection Options

| | |
|---|---|
| Content Disarm and Reconstruction | <input checked="" type="checkbox"/> |
| Original File Destination | <div>FortiSandbox</div> <div>File Quarantine</div> <div>Discard</div> |
| Treat Windows Executables in Email Attachments as Viruses | <input checked="" type="checkbox"/> |
| Send Files to FortiSandbox Appliance for Inspection | <div>None</div> <div>All Supported Files</div> |
| Do not submit files matching types | <div>+</div> |
| Do not submit files matching file name patterns | <div>+</div> |
| Use Virus Outbreak Prevention Database ⓘ | <input type="checkbox"/> |
| Use FortiSandbox Database ⓘ | <input type="checkbox"/> |




If you enable **FortiSandbox** as the file destination, original files caught by the AntiVirus profile are archived on the FortiSandbox. The FortiSandbox administrator can retrieve the original files, but only for a short time.

If you enable either **File Quarantine** or **Discard** as the file destination, original files caught by the AntiVirus profile are lost. Only the disarmed content is made available.

Configuring the Internet access policy

1. Go to **Policy & Objects > IPv4 Policy** and **Edit** the Internet access policy.
2. Under **Security Profiles**, enable the default **AntiVirus** profile. **Proxy Options** and **SSL Inspection** are

automatically enabled.

| Security Profiles | | | |
|--------------------------|-------------------------------------|----------------------------|---|
| AntiVirus | <input checked="" type="checkbox"/> | AV default |  |
| Web Filter | <input type="checkbox"/> | | |
| DNS Filter | <input type="checkbox"/> | | |
| Application Control | <input type="checkbox"/> | | |
| IPS | <input type="checkbox"/> | | |
| Anti-Spam | <input type="checkbox"/> | | |
| DLP Sensor | <input type="checkbox"/> | | |
| VoIP | <input type="checkbox"/> | | |
| ICAP | <input type="checkbox"/> | | |
| Web Application Firewall | <input type="checkbox"/> | | |
| Proxy Options | <input checked="" type="checkbox"/> | PRX default |  |
| SSL Inspection | <input checked="" type="checkbox"/> | SSL certificate-inspection |  |

Results

As the AntiVirus profile scans files using CDR, it replaces content that is deemed malicious or unsafe with content that will allow the traffic to continue but not put the recipient at risk.

CDR appends a new cover page to the malicious/unsafe content that includes a replacement message.

This file has been cleaned of potential threats.

If you wish to disable the cover page, enter the following commands in the CLI Console:

```
config antivirus profile
edit default
config content-disarm
set cover-page disable
end
end
```

Troubleshooting

The feature is not visible in the GUI

Confirm that the **Inspection Mode** is set to **Proxy** under **System > Settings**.

Also check that the AntiVirus profile inspection mode is set to proxy using the **CLI Console**:

```
config antivirus profile
edit default
set inspection-mode proxy
next
end
```

Error messages and/or conflicts

If you receive an error message when attempting to enable Content Disarm and Reconstruction on the AntiVirus profile, check the Proxy Options settings in the **CLI Console** and disable `splice` and `clientcomfort` on CDR-supported protocols:

```
>config firewall profile-protocol-options
>edit default
>config smtp
>unset options splice
>next
>config http
>unset options clientcomfort
>next
>end
>end
```

You should also confirm the AntiVirus profile's protocol settings under `config antivirus profile`:

- ensure that `set options scan` is enabled on CDR-supported protocols
- if `set options av-monitor` is configured on a CDR-supported protocol, it overrides the `config content-disarm detect-only` setting (and CDR will not occur)

The FortiSandbox service is unreachable

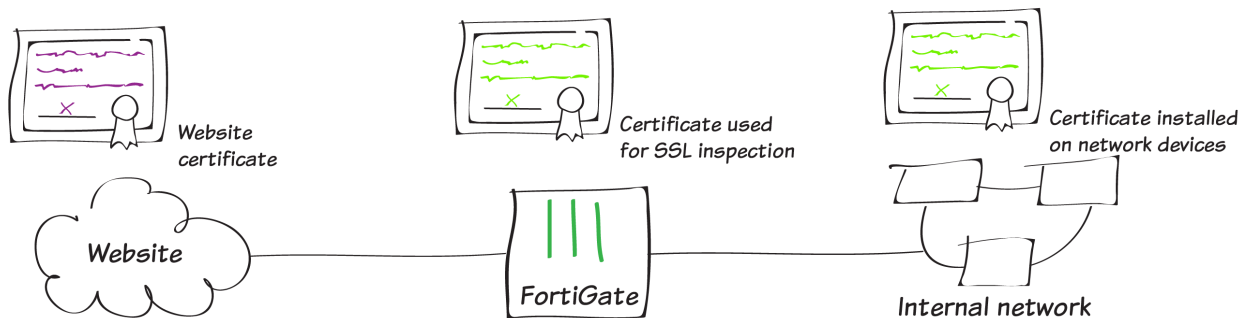
If testing the FortiSandbox connectivity returns a “*Service is unreachable*” error message, then you may need to authorize the FortiGate on the FortiSandbox.

On the FortiSandbox, go to **Scan Input > Device** and edit the entry for the FortiGate.

Under **Permissions & Policy**, enable **Authorized**.

| Permissions & Policy | | |
|--|-------------------------------------|----------------------------------|
| Authorized: | <input checked="" type="checkbox"/> | Last Changed 2018-03-07 12:40:36 |
| New VDOMs/Domains Inherit Authorization: | <input checked="" type="checkbox"/> | |

Preventing certificate warnings (CA-signed certificate)



In this recipe, you prevent users from receiving a security certificate warning when your FortiGate performs full SSL inspection on incoming traffic. There are several methods for doing this, depending on whether you're using a CA-signed certificate, as presented here, your FortiGate default certificate (see [Preventing certificate warnings \(default certificate\) on page 228](#), or a self-signed certification (see [Preventing certificate warnings \(self-signed\) on page 235](#)).

When you enable full SSL inspection, your FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the end user. This is the same process used in "man-in-the-middle" attacks, which is why a user's device may show a security certificate warning.

For more information about SSL inspection, see [Why you should use SSL inspection on page 243](#).

Often, when users receive security certificate warnings, they simply select **Continue** without understanding why the error is occurring. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

Using a CA-signed certificate

In this method, you obtain a CA-signed certificate and install this certificate on your FortiGate to use with SSL inspection. In order to implement SSL inspection, you also need to add another security profile to your policy controlling Internet traffic. You can use either FortiAuthenticator as your CA or a trusted private CA.

If you use FortiAuthenticator as a CA, you generate a certificate signing request (CSR) on your FortiGate, have it signed on the FortiAuthenticator, import the certificate into your FortiGate, and configure your FortiGate to use the certificate for SSL deep inspection of HTTPS traffic.

If you use a trusted private CA, you generate a CSR on your FortiGate, apply for an SSL certificate from the trusted private CA, import the certificate into your FortiGate, and configure your FortiGate so the certificate can be used for SSL deep inspection of HTTPS traffic.

Generating a CSR on a FortiGate

1. On your FortiGate, create a new CSR by going to **System > Certificates** and select **Generate**.
2. Enter a **Certificate Name**, the external IP of your FortiGate, and a valid email address.
3. To ensure the certificate is securely encrypted, set **Key Type** to **RSA** and **Key Size** to **2048 Bit** (the industry standard).

Generate Certificate Signing Request

Certificate Name

Subject Information

ID Type **Host IP** Domain Name E-Mail
IP

Optional Information

Organization Unit

Organization
Locality(City)
State / Province
Country / Region ☐
E-Mail
Subject Alternative Name
Password for private key

Key Type **RSA** Elliptic Curve
Key Size

Enrollment Method **File Based** Online SCEP

Once generated, the certificate shows a Status of Pending. To save the .csr file to your local drive, highlight the certificate and select Download.

| ▼ Name | ▼ Subject | ▼ Comments | ▼ Issuer | ▼ Expires | ▼ Status | ▼ Source |
|------------------------|--|------------------------------------|----------|-------------------------|----------------|----------|
| Certificates (11) | | | | | | |
| RV example-cert | | | | | Pending | User |
| RV Fortinet_Factory | C = US, CN = FG100D3G15818864, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate | This certificate is embedded in... | Fortinet | 2038-01-19 03:14:07 GMT | OK | Factory |
| RV Fortinet_SSL | C = US, CN = FG100D3G15818864, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate | This certificate is embedded in... | Fortinet | 2027-11-09 18:36:56 GMT | OK | Factory |

Getting the certificate signed by a CA

Trusted private CA:

If you want to use a trusted private CA to sign the certificate, use the CSR to apply for an SSL certificate with your trusted private CA.

FortiAuthenticator:

1. If you want to use a FortiAuthenticator as a CA to sign the certificate, on the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and select **Import**.
2. Set **Type** to **CSR to sign**, enter a **Certificate ID**, and import the **example-cert.csr** file. Make sure to select the **Certificate authority** from the drop-down menu and set the **Hash algorithm** to **SHA-256**.

Import Signing Request or Local CA Certificate

Type:

☐ PKCS12 Certificate

☐ Certificate and Private Key

☒ CSR to sign

☐ Local certificate

Certificate ID:

example_cert

CSR file (.csr, .req):

Browse...

example-cert.csr

Certificate Signing Options

Certificate authority:

FGT90D_RootCA | ST=Ontario, O=Fortinet, CN=FGT90DRootCA, emailAddress=jhaney@fortinet.com

Validity period:

☒ Set length of time

☐ Set an expiry date

3650

days

Hash algorithm:

SHA-256

Subject Alternative Name☐ Email:☐ User Principal Name (UPN):**Advanced Options: Key Usages**

OK

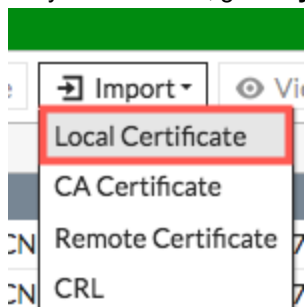
Cancel

3. Once imported, you should see that **example_cert** has been signed by the FortiAuthenticator, showing a **Status** of **Active**, and with the **CA Type** of **Intermediate (non-signing) CA**. Highlight the certificate and select **Export**. This will save the **example_cert.crt** file to your local drive.

| Name | Subject | Comments | Issuer | Expires | Status | Source |
|-------------------|--|------------------------------------|----------|-------------------------|---------|---------|
| Certificates (11) | | | | | | |
| example-cert | | | | | Pending | User |
| Fortinet_Factory | C = US, CN = FG100D3G15818864, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate | This certificate is embedded in... | Fortinet | 2038-01-19 03:14:07 GMT | OK | Factory |
| Fortinet_SSL | C = US, CN = FG100D3G15818864, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate | This certificate is embedded in... | Fortinet | 2027-11-09 18:36:56 GMT | OK | Factory |

Importing the signed certificate to your FortiGate

1. On your FortiGate, go to **System > Certificates** and select **Local Certificate** from the Import drop-down menu.



2. Browse to the certificate file and select **OK**.

Import Certificate

Type: **Local Certificate** PKCS #12 Certificate Certificate

Certificate file:

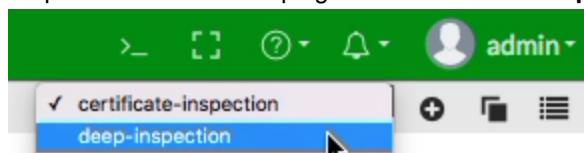
OK Cancel

You should now see that the certificate has a Status of **OK**.

| Name | Subject | Comments | Issuer | Expires | Status | Source |
|-------------------|--|----------|----------|-------------------------|--------|--------|
| Certificates (12) | | | | | | |
| example-cert | CN = FG100D3G15818864, emailAddress = support@fortinet.com, L = Sunnyvale, O = Fortinet, ST = California | | Fortinet | 2038-01-19 03:14:07 GMT | OK | User |

Editing the SSL inspection profile

1. To use your certificate in an SSL inspection profile go to **Security Profiles > SSL/SSH Inspection**. Use the dropdown menu in the top right corner to select **deep-inspection**.



2. The **deep-inspection** profile is read-only. To use the CA-signed certificate for SSL inspection, you must clone the deep-inspection profile and configure the new profile to use your certificate. To clone an existing profile, select the Clone icon (one page behind another) and enter a new name when prompted. In this example, the name of the profile is *custom-deep-inspection*.


Clone "deep-inspection"


Please enter the desired name for the clone:

Name

3. Set **CA Certificate** to use the new certificate.

Edit SSL/SSH Inspection Profile custom-deep-inspection ▼


Name 

Comments 37/255 

SSL Inspection Options

Enable SSL Inspection of Multiple Clients Connecting to Multiple Servers
Protecting SSL Server

Inspection Method SSL Certificate Inspection Full SSL Inspection

CA Certificate  example-cert ▼

4. Verify that SSL inspection is applied to your policy that controls traffic to the Internet. You must also apply at least one other security profile to that policy in order to implement SSL inspection. In this example, we apply antivirus.

| | |
|--------------------|---------------------|
| Name ⓘ | outgoing |
| Incoming Interface | internal |
| Outgoing Interface | wan1 |
| Source | all |
| Destination | all |
| Schedule | always |
| Service | ALL |
| Action | ACCEPT DENY LEARN |

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Proxy Options default

Security Profiles

| | | |
|--------------------------|-------------------------------------|------------------------|
| AntiVirus | <input checked="" type="checkbox"/> | default |
| Web Filter | <input type="checkbox"/> | |
| DNS Filter | <input type="checkbox"/> | |
| Application Control | <input type="checkbox"/> | |
| IPS | <input type="checkbox"/> | |
| Anti-Spam | <input type="checkbox"/> | |
| DLP Sensor | <input type="checkbox"/> | |
| VoIP | <input type="checkbox"/> | |
| ICAP | <input type="checkbox"/> | |
| Web Application Firewall | <input type="checkbox"/> | |
| SSL Inspection ⚠ | <input checked="" type="checkbox"/> | custom-deep-inspection |

Importing the certificate into web browsers

Once your certificate is signed by FortiAuthenticator, you need to import the certificate into users' browsers.



If you have the right environment, such as the Windows Group Policy Management Console, you can push the certificate to users' browsers using the Windows Group Policy Editor. In this case, you do not have to import the certificate into users' browsers.

The method you use for importing the certificate varies depending on the type of browser.

Internet Explorer, Chrome, and Safari (on Windows and macOS):

Internet Explorer, Chrome, and Safari use the operating system's certificate store for Internet browsing. If users will be using these browsers, you must install the certificate into the certificate store for the OS.

1. If you are using Windows 7/8/10, double-click the certificate file and select **Open**. Select **Install Certificate** to launch the **Certificate Import Wizard**.
2. Use the wizard to install the certificate into the **Trusted Root Certificate Authorities** store. If a security warning appears, select **Yes** to install the certificate.

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

| | |
|------------------------------------|--|
| Certificate Store Selected by User | Trusted Root Certification Authorities |
| Content | Certificate |

3. If you are using macOS, double-click the certificate file to launch **Keychain Access**.
4. Locate the certificate in the **Certificates** list and select it. Expand **Trust** and select **Always Trust**. If necessary,

enter the administrative password for your computer to make this change.



172.25.176.51

Intermediate certificate authority

Expires: Monday, July 17, 2028 at 4:12:23 PM GMT-04:00

✖ This certificate was signed by an unknown authority

▼ Trust

When using this certificate: Always Trust 

Secure Sockets Layer (SSL) Always Trust

Secure Mail (S/MIME) Always Trust

Extensible Authentication (EAP) Always Trust

IP Security (IPsec) Always Trust

iChat Security Always Trust

Kerberos Client Always Trust

Kerberos Server Always Trust

Code Signing Always Trust

Time Stamping Always Trust

X.509 Basic Policy Always Trust

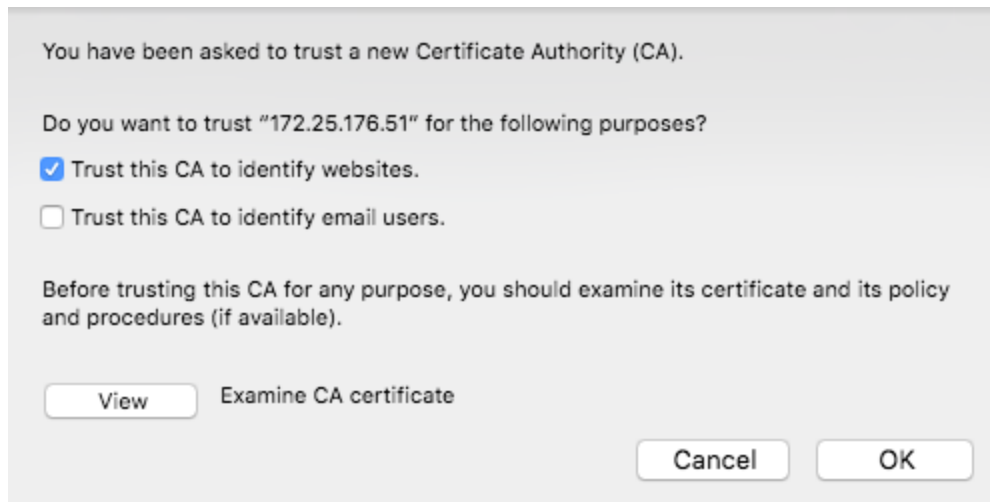
Firefox (on Windows and macOS)

Firefox has its own certificate store. To avoid errors in Firefox, the certificate must be installed in this store, rather than in the OS.

If users are using Firefox, instead of being pushed to all of their devices, the certificate must be installed on each device.

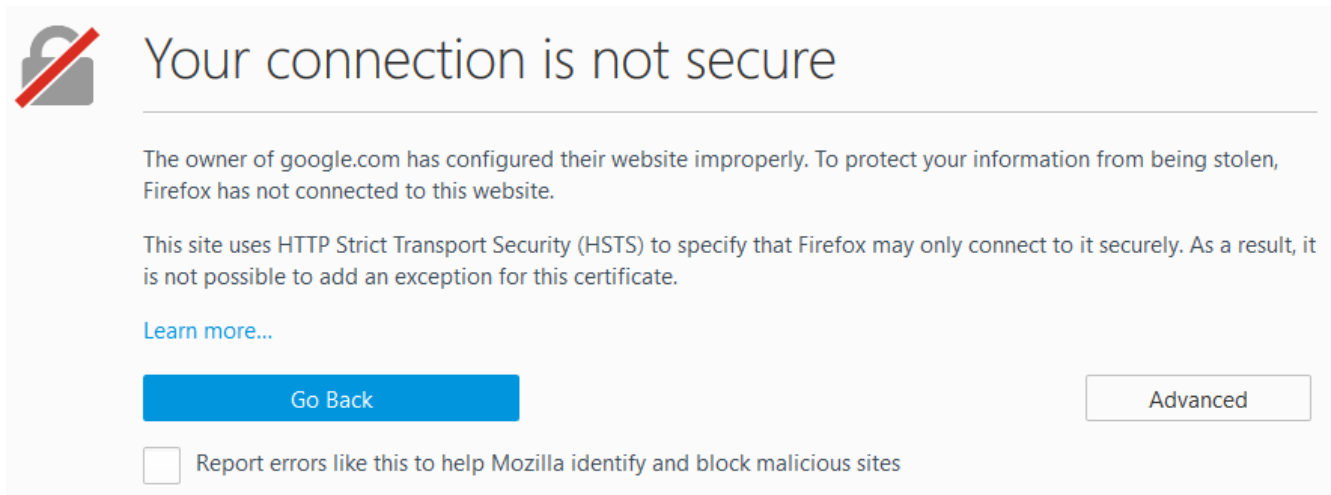
1. In Firefox, go to **Options > Privacy & Security** (Windows) or **Preferences > Privacy & Security** (macOS).
2. Scroll down to the **Certificates** section. Select **View Certificates**, select the **Authorities** list. **Import** the certificate

and set it to be trusted for website identification.



Results

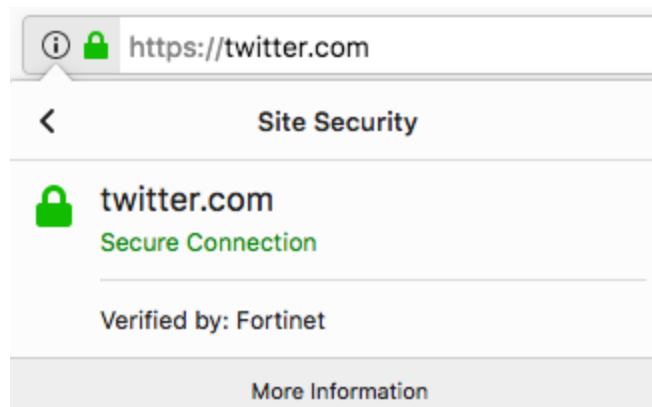
Before you install the certificate, an error message appears in users' browsers when they access a site that uses HTTPS (this example shows an error message in Firefox).



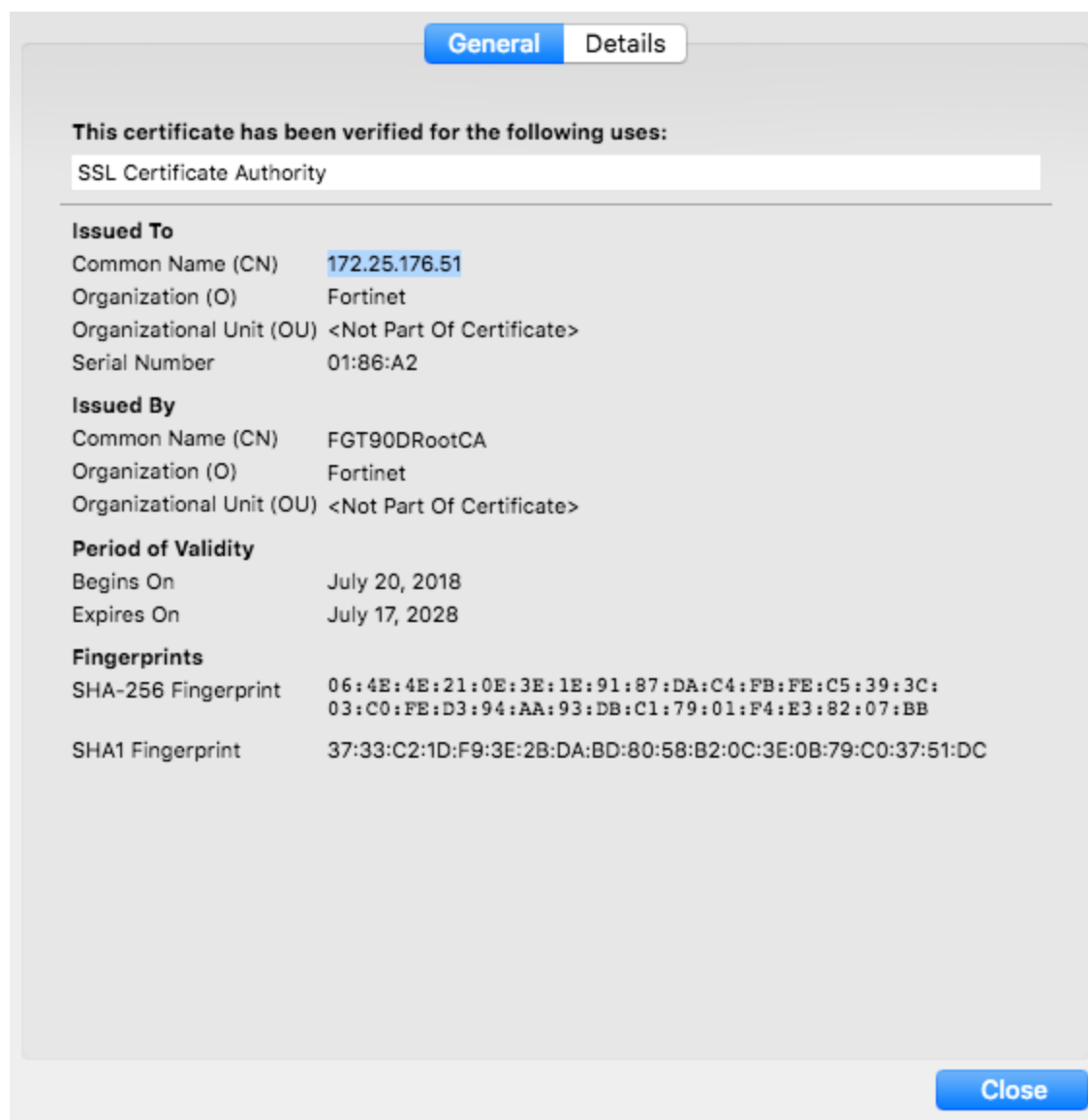
After you install the certificate, users shouldn't experience a certificate security issue when they browse to sites that the FortiGate performs SSL content inspection on.

Users can view information about the connection and the certificate that's used.

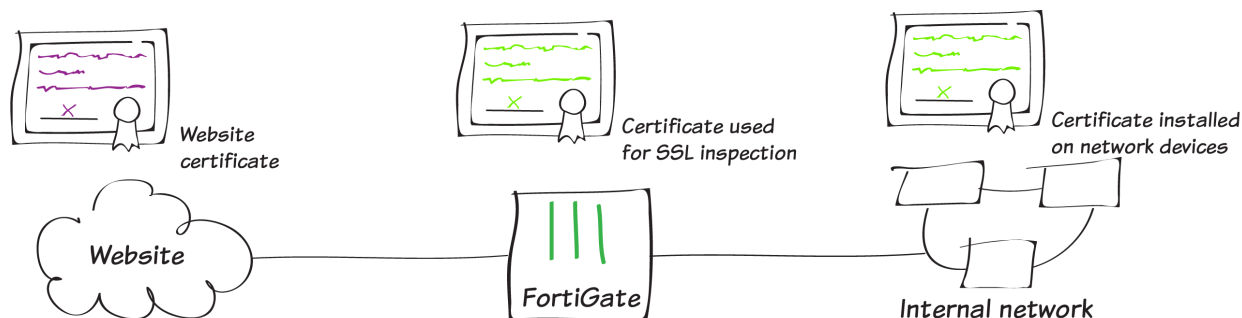
When users view information about the connection, they'll see that it's verified by Fortinet.



When users view the certificate in the browser, they will see which certificate is used and information about that certificate.



Preventing certificate warnings (default certificate)



In this recipe, you prevent users from receiving a security certificate warning when your FortiGate performs full SSL inspection on incoming traffic. There are several methods for doing this, depending on whether you're using your FortiGate default certificate, as presented here, your a CA-signed certificate (see [Preventing certificate warnings \(CA-signed certificate\) on page 218](#)), or a self-signed certification (see [Preventing certificate warnings \(self-signed\) on page 235](#)).

When you enable full SSL inspection, your FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the end user. This is the same process used in "man-in-the-middle" attacks, which is why a user's device may show a security certificate warning.

For more information about SSL inspection, see [Why you should use SSL inspection on page 243](#).

Often, when users receive security certificate warnings, they simply select **Continue** without understanding why the error is occurring. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

Using the default certificate

All FortiGate devices have a default certificate that's used for full SSL inspection. This certificate is also used in the default **deep-inspection** profile. To prevent users from seeing certificate warnings, you can install this certificate on users' devices.

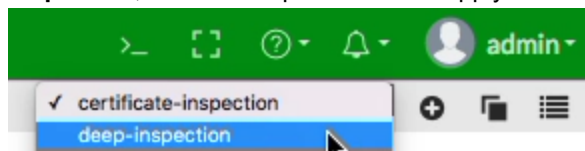
Generating a unique certificate

Run the following CLI command to generate an SSL certificate that's unique to your FortiGate:

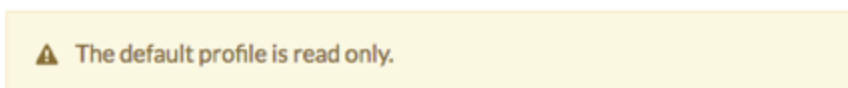
```
exec vpn certificate local generate default-ssl-ca
```


Downloading the certificate

1. Go to **Security Profiles > SSL/SSH Inspection**. Use the drop-down menu in the top right corner to select **deep-inspection**, which is the profile used to apply full SSL inspection.



2. The default FortiGate certificate is listed as the **CA Certificate**. Select **Download Certificate**.



| | | |
|----------|---|--------|
| Name | <input type="text" value="deep-inspection"/> | |
| Comments | <input type="text" value="Read-only deep inspection profile."/> | 34/255 |

SSL Inspection Options

| | | |
|----------------------------|---|---|
| Enable SSL Inspection of | <input type="button" value="Multiple Clients Connecting to Multiple Servers"/> <input type="button" value="Protecting SSL Server"/> | |
| Inspection Method | <input type="button" value="SSL Certificate Inspection"/> <input checked="" type="button" value="Full SSL Inspection"/> | |
| CA Certificate ⚠ | <input type="text" value="Fortinet_CA_SSL"/> | <input type="button" value="Download Certificate"/> |
| Untrusted SSL Certificates | <input checked="" type="button" value="Allow"/> <input type="button" value="Block"/> <input type="button" value="View Trusted CAs List"/> | |
| RPC over HTTPS | <input type="checkbox"/> | |

Applying SSL inspection to a policy

Before you import the certificate, verify that SSL inspection is applied to your policy that controls traffic to the Internet. You must also apply at least one other security profile to that policy in order to implement SSL inspection

Importing the certificate into web browsers

Once you have your FortiGate device's default certificate, you need to import the certificate into users' browsers.



If you have the right environment, such as the Windows Group Policy Management Console, you can push the certificate to users' browsers using the Windows Group Policy Editor. In this case, you do not have to import the certificate into users' browsers.

The method you use for importing the certificate varies depending on the type of browser.

Internet Explorer, Chrome, and Safari (on Windows and macOS):

Internet Explorer, Chrome, and Safari use the operating system's certificate store for Internet browsing. If users will be using these browsers, you must install the certificate into the certificate store for the OS.

1. If you are using Windows 7/8/10, double-click the certificate file and select **Open**. Select **Install Certificate** to launch the **Certificate Import Wizard**.
2. Use the wizard to install the certificate into the **Trusted Root Certificate Authorities** store. If a security warning appears, select **Yes** to install the certificate.

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

| | |
|------------------------------------|--|
| Certificate Store Selected by User | Trusted Root Certification Authorities |
| Content | Certificate |
| | |

3. If you are using macOS, double-click the certificate file to launch **Keychain Access**.
4. Locate the certificate in the **Certificates** list and select it. Expand **Trust** and select **Always Trust**. If necessary,

enter the administrative password for your computer to make this change.



172.25.176.51

Intermediate certificate authority

Expires: Monday, July 17, 2028 at 4:12:23 PM GMT-04:00

✖ This certificate was signed by an unknown authority

▼ Trust

When using this certificate: Always Trust ?

Secure Sockets Layer (SSL) Always Trust

Secure Mail (S/MIME) Always Trust

Extensible Authentication (EAP) Always Trust

IP Security (IPsec) Always Trust

iChat Security Always Trust

Kerberos Client Always Trust

Kerberos Server Always Trust

Code Signing Always Trust

Time Stamping Always Trust

X.509 Basic Policy Always Trust

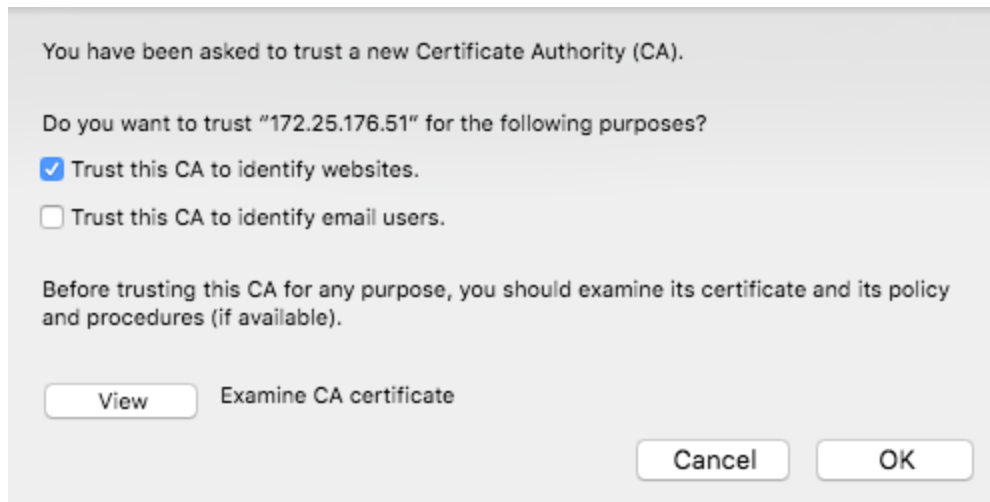
Firefox (on Windows and macOS)

Firefox has its own certificate store. To avoid errors in Firefox, the certificate must be installed in this store, rather than in the OS.

If users are using Firefox, instead of being pushed to all of their devices, the certificate must be installed on each device.

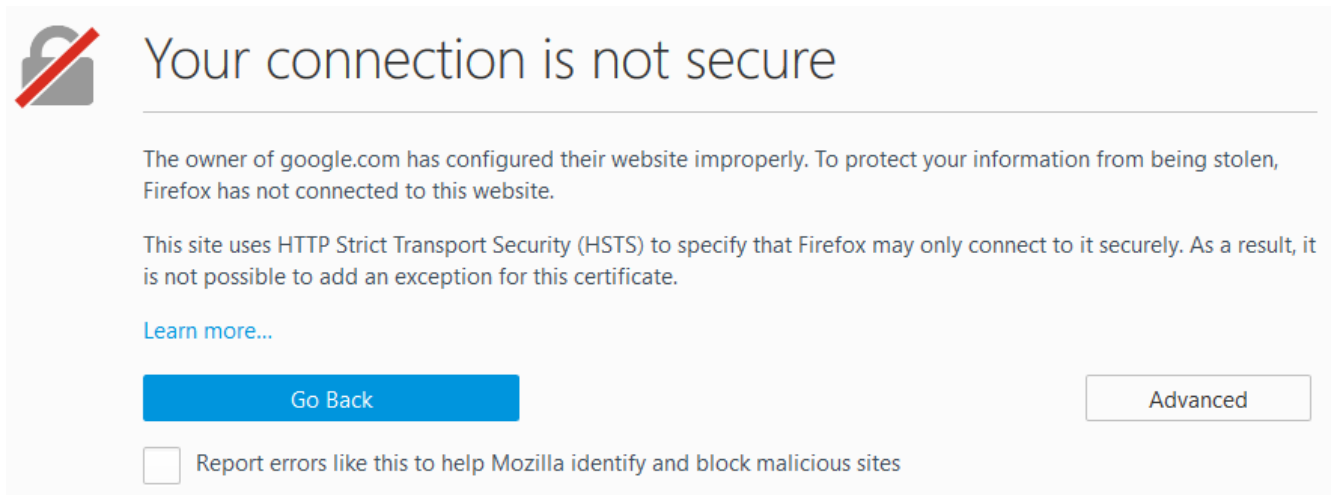
1. In Firefox, go to **Options > Privacy & Security** (Windows) or **Preferences > Privacy & Security** (macOS).
2. Scroll down to the **Certificates** section. Select **View Certificates**, select the **Authorities** list. **Import** the certificate

and set it to be trusted for website identification.



Results

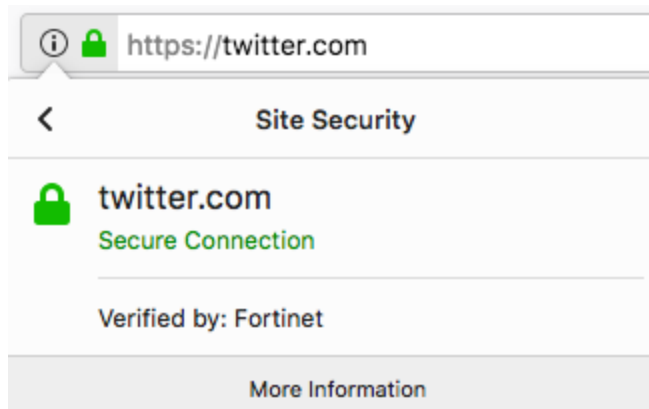
Before you install the certificate, an error message appears in users' browsers when they access a site that uses HTTPS (this example shows an error message in Firefox).



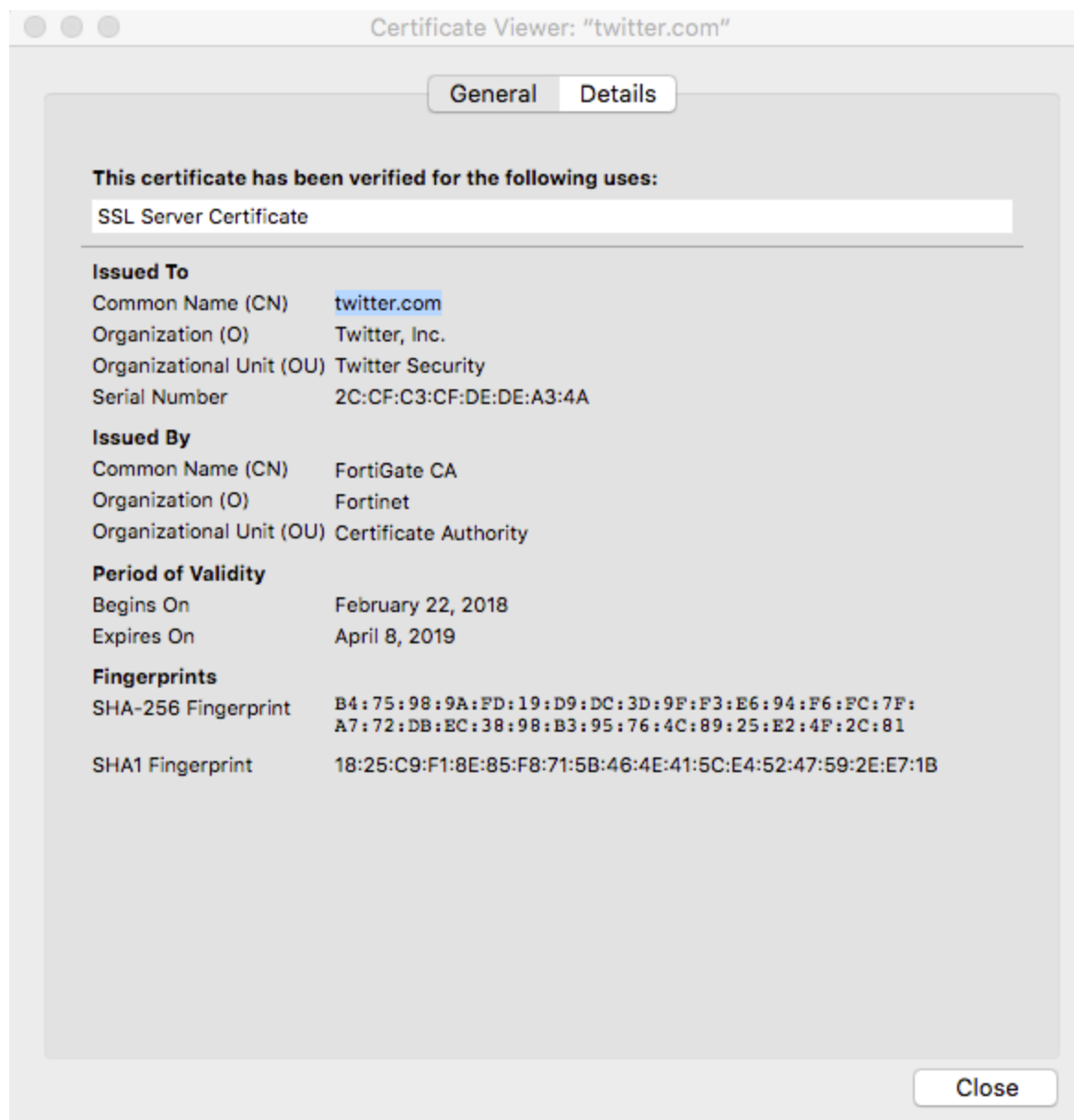
After you install the certificate, users shouldn't experience a certificate security issue when they browse to sites that the FortiGate performs SSL content inspection on.

Users can view information about the connection and the certificate that's used.

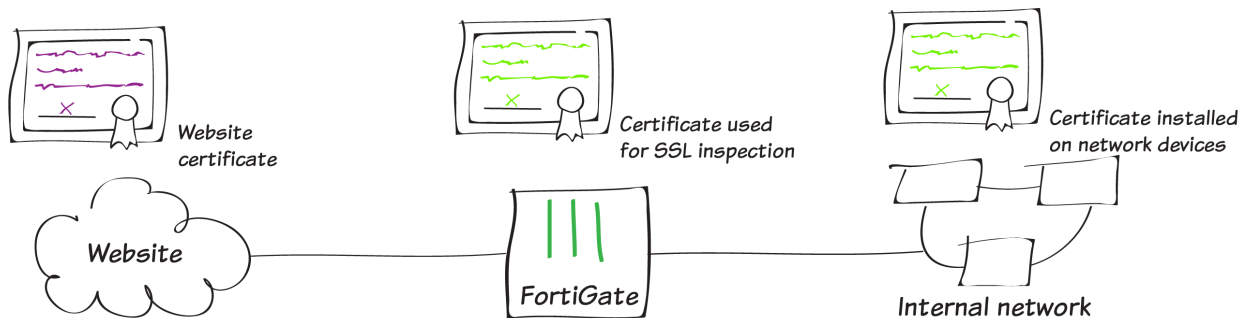
When users view information about the connection, they'll see that it's verified by Fortinet.



When users view the certificate in the browser, they will see which certificate is used and information about that certificate.



Preventing certificate warnings (self-signed)



In this recipe, you prevent users from receiving a security certificate warning when your FortiGate performs full SSL inspection on incoming traffic. There are several methods for doing this, depending on whether you're using a self-signed certificate, as presented here, your FortiGate default certificate (see [Preventing certificate warnings \(default certificate\) on page 228](#), or a CA-signed certification (see [Preventing certificate warnings \(CA-signed certificate\) on page 218](#)).

When you enable full SSL inspection, your FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the end user. This is the same process used in "man-in-the-middle" attacks, which is why a user's device may show a security certificate warning.

For more information about SSL inspection, see [Why you should use SSL inspection on page 243](#).

Often, when users receive security certificate warnings, they simply select **Continue** without understanding why the error is occurring. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

Creating a certificate with OpenSSL

1. If necessary, download and install Open SSL. Make sure that the *openssl.cnf* file is located in the BIN folder for OpenSSL.
2. Using a command prompt (CMD), navigate to the BIN folder.
In this example, the command is:

```
cd c:\OpenSSL\bin
```
3. Generate an RSA key with the following command:

```
openssl genrsa -aes256 -out fgcaprivkey.pem 2048 -config openssl.cnf
```


This RSA key uses AES-256 encryption and a 2048-bit key.
4. When prompted, enter a passphrase for encrypting the private key.
Use the following command to launch OpenSSL, submit a new certificate request, and sign the request:

```
openssl req -new -x509 -days 3650 -extensions v3_ca -key fgcaprivkey.pem -out fgcert.pem -config openssl.cnf
```


The result is a standard x509 binary certificate that's valid for 3650 days (approximately 10 years).

- When prompted, re-enter the passphrase for encryption, then enter the details required for the certificate request, such as location and organization name.

Two new files are created: a public certificate (*fgcacert.pem*) and a private key (*fgcaprivkey.pem*).

Importing the self-signed certificate

- Go to **System > Certificates** and select **Import > Local Certificate**.
- Set **Type** to **Certificate**, then select your **Certificate file** and Key file. Enter the **Password** that you set when you created the certificate.

Import Certificate

Type: Local Certificate, PKCS #12 Certificate, **Certificate**

Certificate file: + fgcacert.pem

Key file: + fgcaprivkey.pem

Password: [masked]

Certificate Name: fgcacert

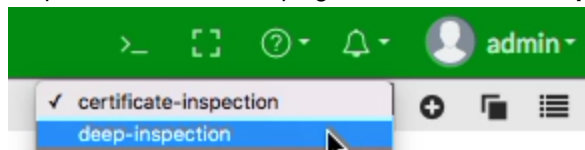
OK Cancel

The certificate now appears in the **Local CA Certificates** list.

| Local CA Certificates (3) | |
|---------------------------|---|
| Fortinet_CA_Untrusted | C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority |
| Fortinet_CA_SSL | C = US, CN = FGT51E3U15000097, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority |
| fgcacert | C = CA, CN = KJ, L = Ottawa, O = Fortinet, ST = ON, emailAddress = kjacobs@fortinet.com |

Editing the SSL inspection profile

- To use your certificate in an SSL inspection profile go to **Security Profiles > SSL/SSH Inspection**. Use the dropdown menu in the top right corner to select **deep-inspection**.



- The **deep-inspection** profile is read-only. To use the CA-signed certificate for SSL inspection, you must clone the deep-inspection profile and configure the new profile to use your certificate. To clone an existing profile, select the Clone icon (one page behind another) and enter a new name when prompted. In this example, the name of the profile is *custom-deep-inspection*.

Clone "deep-inspection"

Please enter the desired name for the clone:

Name

OK

Cancel

3. Set **CA Certificate** to use the new certificate.
4. Select **Download Certificate**, to download the certificate file.

Edit SSL/SSH Inspection Profile

custom-deep-inspection ▼

Name Comments

37/255

SSL Inspection Options

Enable SSL Inspection of

Multiple Clients Connecting to Multiple Servers

Protecting SSL Server

Inspection Method

SSL Certificate Inspection

Full SSL Inspection

CA Certificate ⚠

fgccert ▼

Download Certificate

Untrusted SSL Certificates

Allow

Block

View Trusted CAs List

RPC over HTTPS



Applying SSL inspection to a policy

Before you import the certificate, verify that SSL inspection is applied to your policy that controls traffic to the Internet. You must also apply at least one other security profile to that policy in order to implement SSL inspection.

Importing the certificate into web browsers

Once you have your self-signed certificate, you need to import the certificate into users' browsers.



If you have the right environment, such as the Windows Group Policy Management Console, you can push the certificate to users' browsers using the Windows Group Policy Editor. In this case, you do not have to import the certificate into users' browsers.

The method you use for importing the certificate varies depending on the type of browser.

Internet Explorer, Chrome, and Safari (on Windows and macOS):

Internet Explorer, Chrome, and Safari use the operating system's certificate store for Internet browsing. If users will be using these browsers, you must install the certificate into the certificate store for the OS.

1. If you are using Windows 7/8/10, double-click the certificate file and select **Open**. Select **Install Certificate** to launch the **Certificate Import Wizard**.
2. Use the wizard to install the certificate into the **Trusted Root Certificate Authorities** store. If a security warning appears, select **Yes** to install the certificate.

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

| | |
|------------------------------------|--|
| Certificate Store Selected by User | Trusted Root Certification Authorities |
| Content | Certificate |
| | |

3. If you are using macOS, double-click the certificate file to launch **Keychain Access**.
4. Locate the certificate in the **Certificates** list and select it. Expand **Trust** and select **Always Trust**. If necessary,

enter the administrative password for your computer to make this change.



172.25.176.51

Intermediate certificate authority

Expires: Monday, July 17, 2028 at 4:12:23 PM GMT-04:00

✖ This certificate was signed by an unknown authority

▼ Trust

When using this certificate: Always Trust 

Secure Sockets Layer (SSL) Always Trust

Secure Mail (S/MIME) Always Trust

Extensible Authentication (EAP) Always Trust

IP Security (IPsec) Always Trust

iChat Security Always Trust

Kerberos Client Always Trust

Kerberos Server Always Trust

Code Signing Always Trust

Time Stamping Always Trust

X.509 Basic Policy Always Trust

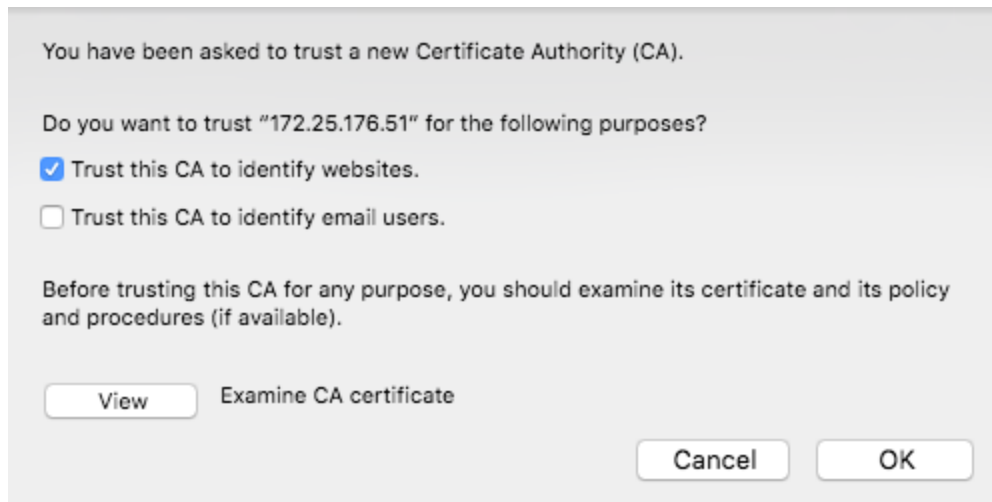
Firefox (on Windows and macOS)

Firefox has its own certificate store. To avoid errors in Firefox, the certificate must be installed in this store, rather than in the OS.

If users are using Firefox, instead of being pushed to all of their devices, the certificate must be installed on each device.

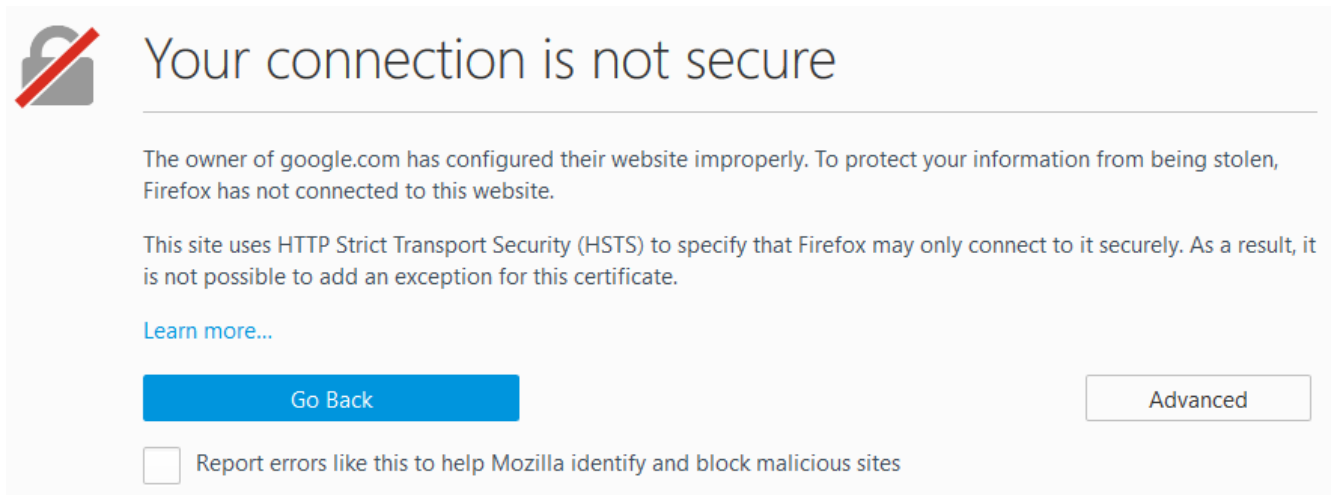
1. In Firefox, go to **Options > Privacy & Security** (Windows) or **Preferences > Privacy & Security** (macOS).
2. Scroll down to the **Certificates** section. Select **View Certificates**, select the **Authorities** list. **Import** the certificate

and set it to be trusted for website identification.



Results

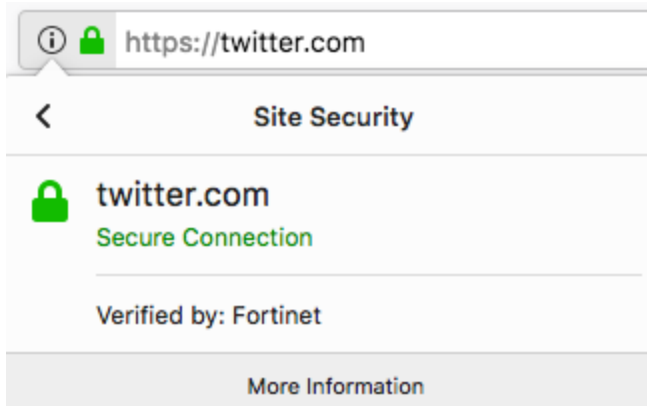
Before you install the certificate, an error message appears in users' browsers when they access a site that uses HTTPS (this example shows an error message in Firefox).



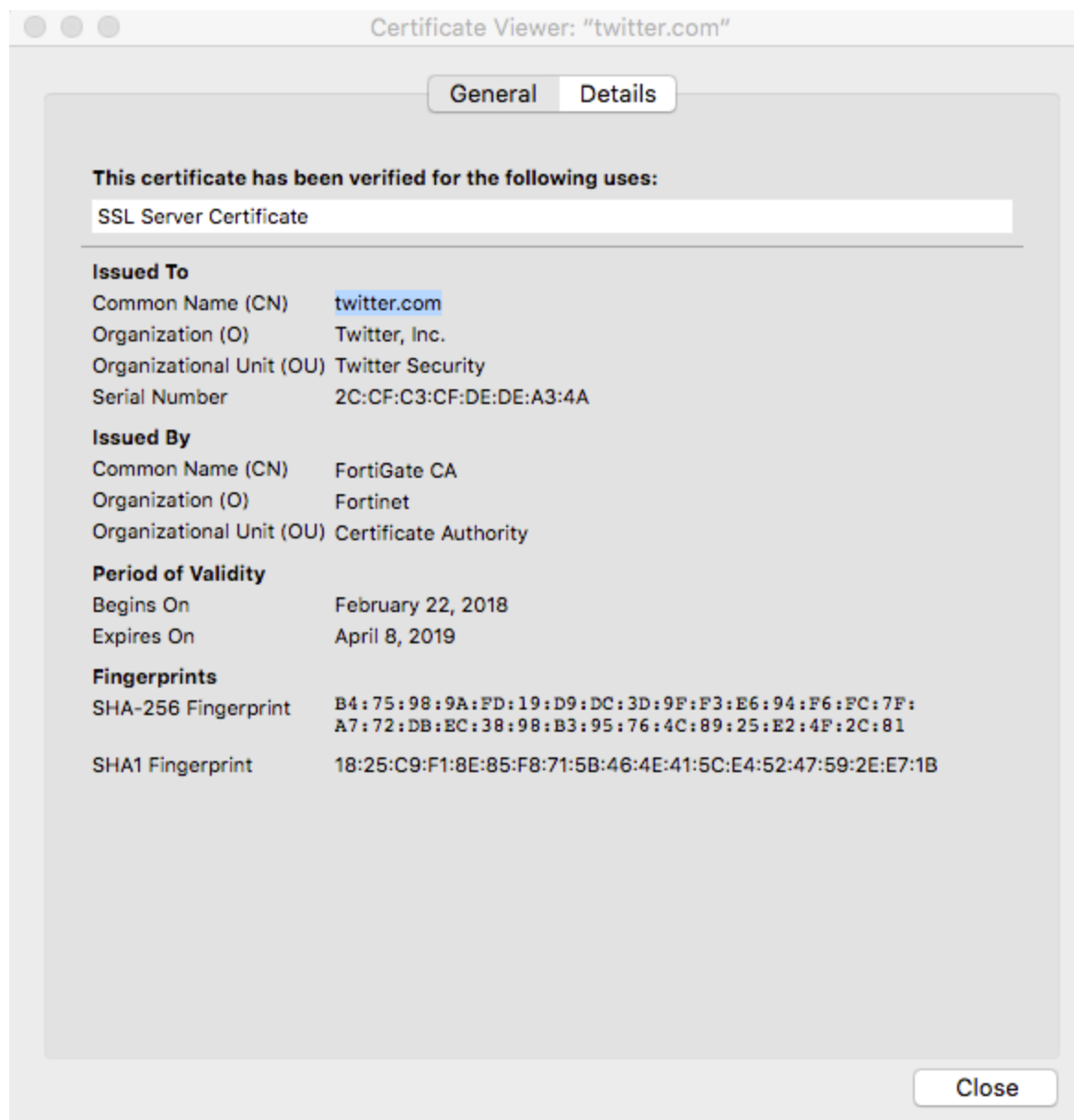
After you install the certificate, users shouldn't experience a certificate security issue when they browse to sites that the FortiGate performs SSL content inspection on.

Users can view information about the connection and the certificate that's used.

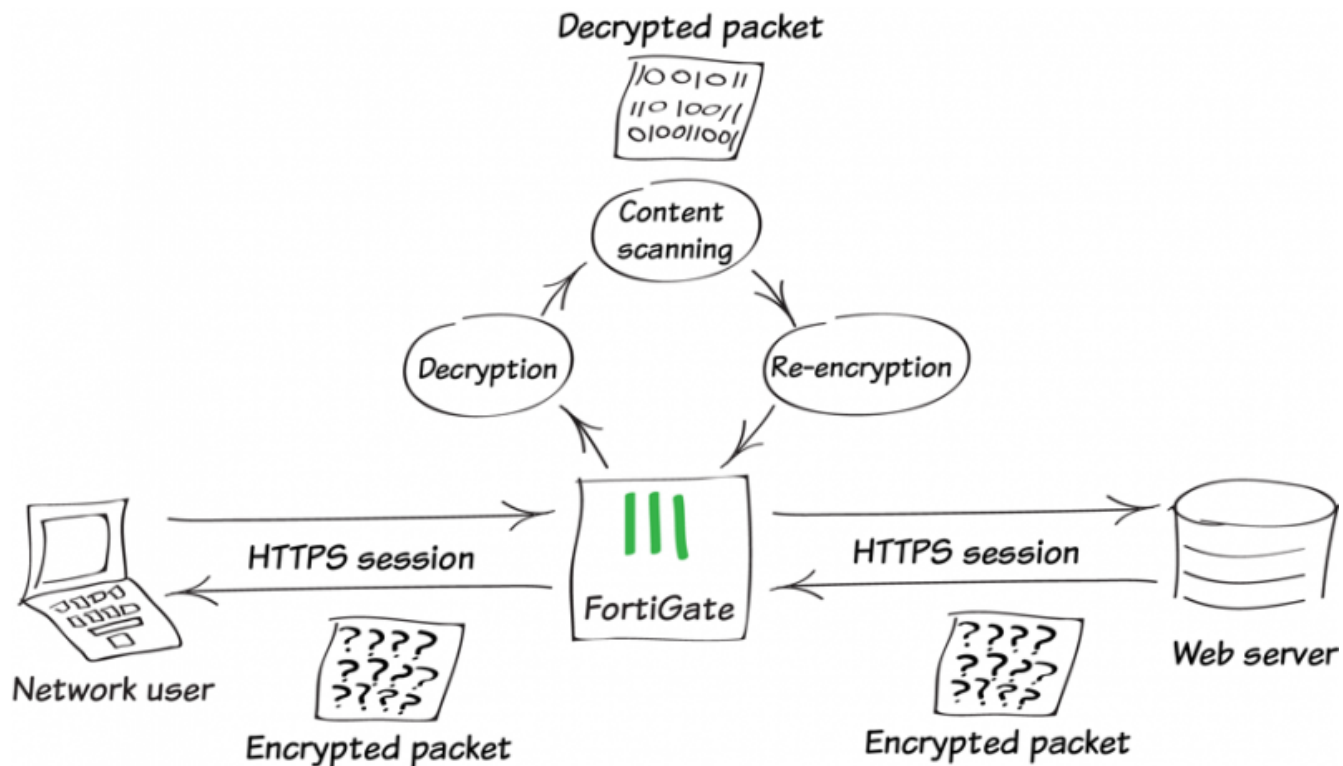
When users view information about the connection, they'll see that it's verified by Fortinet.



When users view the certificate in the browser, they will see which certificate is used and information about that certificate.



Why you should use SSL inspection



Most of us are familiar with HTTPS and how it protects a variety of activities on the Internet by applying SSL encryption to the web traffic.

Using HTTPS provides the benefit of using encryption keeps your private data safe from prying eyes. However, there are risks associated with its use, since encrypted traffic can be used to get around your normal defenses.

For example, you might download a file containing a virus during an e-commerce session. Or you could receive a phishing email containing a seemingly harmless downloader file that, when launched, creates an encrypted session to a C&C server and downloads malware onto your computer. Because the sessions in these attacks are encrypted, they might get past your network's security measures.

To protect your network from these threats, SSL inspection is the key your FortiGate uses to unlock encrypted sessions, see into encrypted packets, find threats, and block them. SSL inspection not only protects you from attacks that use HTTPS, but also from other commonly used encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.

Full SSL inspection

To make sure that all encrypted content is inspected, you must use full SSL inspection (also known as deep inspection). When full SSL inspection is used, the FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the sender.

When the FortiGate re-encrypts the content it uses a certificate stored on the FortiGate. The client must trust this certificate to avoid certificate errors. Whether or not this trust exists depends on the client, which can be the computer's OS, a browser, or another application, which will likely maintain its own certificate repository.

There are two deployment methods for full SSL inspection:

1. Multiple Clients Connecting to Multiple Servers:

- Uses a CA certificate (which can be uploaded using the Certificates menu)
- Typically applied to outbound policies where destinations are unknown (i.e. normal web traffic)
- Address and web category whitelists can be configured to bypass SSL inspection

2. Protecting SSL Server

- Uses a server certificate (which can be uploaded using the Certificates menu) to protect a single server
- Typically used on inbound policies to protect servers available externally through Virtual IPs
- Since this is typically deployed "outside-in" (clients on the Internet accessing server(s) on the internal side of the FortiGate), server certificates using the public FQDN of the server are often purchased from a commercial Certificate Authority and uploaded to the FortiGate. This avoids client applications generating SSL certificate errors due to certificate mismatch.

More detail is available in the [FortiOS Online Help](#). Also, check the Fortinet Knowledge Base for these technical notes:

- [How to Enable SSL inspection from the CLI and Apply it to a Policy](#)
- [How to block web-based chat on Gmail webmail using App Sensor + SSL inspection](#)

SSL certificate inspection

The FortiGate also supports a second type of SSL inspection, called SSL certificate inspection. When certificate inspection is used, the FortiGate inspects only the headers up to the SSL/TLS layer.

Certificate inspection is used to verify the identity of web servers and can be used to make sure that HTTPS protocol is not used as a workaround to access sites you have blocked using web filtering.

The only security feature that can be applied using SSL certificate inspection mode is web filtering. However, since only the packet header is inspected, this method does not introduce certificate errors and can be a useful alternative to full SSL inspection when web filtering is used.

When using SSL certificate inspection, you may get certificate errors for blocked websites, due to your FortiGate attempting to display a replacement message for that site using HTTPS. To prevent these errors, you must install the certificate that the FortiGate uses for encryption in your browser. By default, this is the same certificate used for SSL inspection.

For more information, see:

- [Preventing certificate warnings \(CA-signed certificate\) on page 218.](#)
- [Preventing certificate warnings \(default certificate\) on page 228.](#)
- [Preventing certificate warnings \(self-signed\) on page 235](#)

Troubleshooting

The most common problem with SSL inspection is users receiving SSL errors when the certificate is not trusted. This is because, by default, the FortiGate uses a certificate that is not trusted by the client. There are several methods to fix this, depending on whether you are using your FortiGate's default certificate, a self-signed certificate, or a CA-signed certificate.

Best practices

Because all traffic needs to be decrypted, inspected, and re-encrypted, using SSL inspection can reduce the overall performance of your FortiGate. To avoid using too many resources for SSL inspection, do the following:

- **Know your traffic** – Know how much traffic is expected and what percentage of the traffic is encrypted. You can also limit the number of policies that allow encrypted traffic.
- **Be selective** – Use whitelists or trim your policy to apply SSL inspection only where it is needed.
- **Use hardware acceleration** – FortiGate models with either the CP6 or CPU processor have an SSL/TLS protocol processor for SSL content scanning and SSL acceleration. For more information about this, see the Hardware Acceleration handbook.
- **Test real-world SSL inspection performance yourself** – Use the flexibility of FortiGate's security policy to gradually deploy SSL inspection, rather than enabling it all at once.

VPNs

This section contains information about creating and using a virtual private network (VPN).

SSL VPN quick start

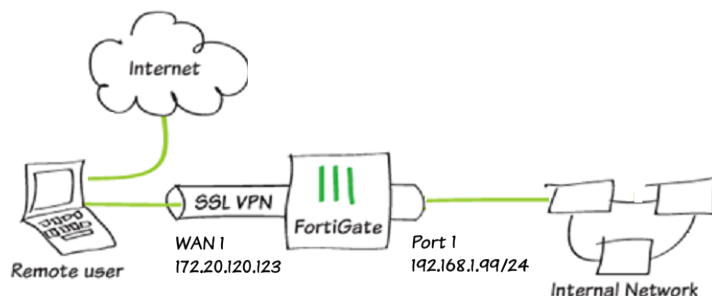
The following topics provide introductory instructions on configuring SSL VPN:

- [SSL VPN split tunnel for remote user on page 246](#)
- [Connecting from FortiClient VPN client on page 249](#)
- [Set up FortiToken two-factor authentication on page 251](#)
- [Connecting from FortiClient with FortiToken on page 252](#)

SSL VPN split tunnel for remote user

This is a sample configuration of remote users accessing the corporate network and internet through an SSL VPN by tunnel mode using FortiClient but accessing the Internet without going through the SSL VPN tunnel.

Sample topology



Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
 - a. Go to *Network > Interfaces* and edit the *wan1* interface.
 - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
 - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.

- d. Click OK.
 - e. Go to *Policy & Objects > Address* and create an address for internal subnet *192.168.1.0*.
2. Configure user and user group.
 - a. Go to *User & Device > User Definition* to create a local user *sslvpnuser1*.
 - b. Go to *User & Device > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.
3. Configure SSL VPN web portal.
 - a. Go to *VPN > SSL-VPN Portals* to create a tunnel mode only portal *my-split-tunnel-portal*.
 - b. Enable *Split Tunneling*.
 - c. Select *Routing Address* to define the destination network that will be routed through the tunnel. Leave undefined to use the destination in the respective firewall policies.
4. Configure SSL VPN settings.
 - a. Go to *VPN > SSL-VPN Settings*.
 - b. For *Listen on Interface(s)*, select *wan1*.
 - c. Set *Listen on Port* to *10443*.
 - d. Optionally, set *Restrict Access* to *Limit access to specific hosts*, and specify the addresses of the hosts that are allowed to connect to this VPN.
 - e. Choose a certificate for *Server Certificate*. The default is *Fortinet_Factory*.
 - f. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *tunnel-access*.
 - g. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-split-tunnel-portal*.
5. Configure SSL VPN firewall policy.
 - a. Go to *Policy & Objects > IPv4 Policy*.
 - b. Fill in the firewall policy name. In this example, *sslvpn split tunnel access*.
 - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
 - d. Choose an *Outgoing Interface*. In this example, *port1*.
 - e. Set the *Source* to *SSLVPN_TUNNEL_ADDR1* and group to *sslvpngroup*. The source address references the tunnel IP addresses that the remote clients are using.
 - f. In this example, the *Destination* is *192.168.1.0*.
 - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
 - h. Click OK.

To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
    edit "wan1"
        set vdom "root"
        set ip 172.20.120.123 255.255.255.0
    next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
    next
end
```

```
config firewall address
  edit "192.168.1.0"
    set subnet 192.168.1.0 255.255.255.0
  next
end
```

3. Configure user and user group.

```
config user local
  edit "sslvpnuser1"
    set type password
    set passwd your-password
  next
end

config user group
  edit "sslvpngroup"
    set member "sslvpnuser1"
  next
end
```

4. Configure SSL VPN web portal.

```
config vpn ssl web portal
  edit "my-split-tunnel-portal"
    set tunnel-mode enable
    set split-tunneling enable
    set split-tunneling-routing-address "192.168.1.0"
    set ip-pools "SSLVPN_TUNNEL_ADDR1"
  next
end
```

5. Configure SSL VPN settings.

```
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 "wan1"
  set source-address "all"
  set source-address6 "all"
  set default-portal "full-access"
  config authentication-rule
    edit 1
      set groups "sslvpngroup"
      set portal "my-split-tunnel-portal"
    next
  next
end
```

Optionally, to restrict access to specific hosts:

```
config vpn ssl settings
  set source-address <address> <address> ... <address>
  set source-address6 <address> <address> ... <address>
end
```

6. Configure one SSL VPN firewall policy to allow remote user to access the internal network. Traffic is dropped from internal to remote client.

```
config firewall policy
  edit 1
    set name "sslvpn split tunnel access"
    set srcintf "ssl.root"
    set dstintf "port1"
    set srcaddr "SSLVPN_TUNNEL_ADDR1"
    set dstaddr "192.168.1.0"
    set groups "sslvpngroup"
    set action accept
    set schedule "always"
    set service "ALL"
  next
end
```

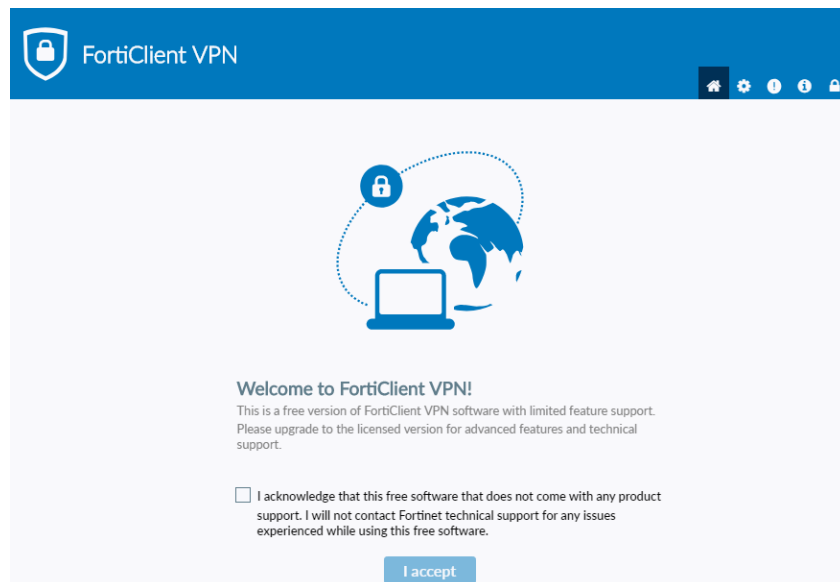
Connecting from FortiClient VPN client

For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS. This version does not include central management, technical support, or some advanced features.

Downloading and installing the standalone FortiClient VPN client

You can download the free VPN client from [FNDN](#) or [FortiClient.com](#).

When the free VPN client is run for the first time, it displays a disclaimer. You cannot configure or create a VPN connection until you accept the disclaimer and click *I accept*:



Configuring an SSL VPN connection

To configure an SSL VPN connection:

1. On the *Remote Access* tab, click on the settings icon and then *Add a New Connection*.

2. Select *SSL-VPN*, then configure the following settings:

| | |
|---------------------------|--|
| Connection Name | SSLVPNtoHQ |
| Description | (Optional) |
| Remote Gateway | 172.20.120.123 |
| Customize port | 10443 |
| Client Certificate | Select <i>Prompt on connect</i> or the certificate from the dropdown list. |
| Authentication | Select <i>Prompt on login</i> for a prompt on the connection screen |

3. Click *Save* to save the VPN connection.

Connecting to SSL VPN

To connect to SSL VPN:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.
2. Enter your username and password.
3. Click the *Connect* button.
4. After connecting, you can now browse your remote network. Traffic to 192.168.1.0 goes through the tunnel, while other traffic goes through the local gateway. FortiClient displays the connection status, duration, and other relevant information.
5. Click the *Disconnect* button when you are ready to terminate the VPN session.

Checking the SSL VPN connection

To check the SSL VPN connection using the GUI:

1. On the FortiGate, go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
2. On the FortiGate, go to *Log & Report > Forward Traffic* to view the details of the SSL entry.

To check the tunnel log in using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
  Index   User           Auth Type   Timeout   From           HTTP in/out  HTTPS in/out
  0       sslvpuser1     1 (1)      291       10.1.100.254   0/0          0/0

SSL VPN sessions:
  Index   User           Source IP   Duration   I/O Bytes      Tunnel/Dest IP
  0       sslvpuser1     10.1.100.254  9          22099/43228    10.212.134.200
```

Set up FortiToken two-factor authentication

This configuration adds two-factor authentication (2FA) to the split tunnel configuration ([SSL VPN split tunnel for remote user on page 246](#)). It uses one of the two free mobile FortiTokens that is already installed on the FortiGate.

To configure 2FA using the GUI:

1. Configure a user and user group.
 - a. Go to *User & Device > User Definition* and edit local user *sslvpuser1*.
 - b. Enter the user's *Email Address*.
 - c. Enable *Two-factor Authentication* and select one mobile *Token* from the list,
 - d. Enable *Send Activation Code* and select *Email*.
 - e. Click *Next* and click *Submit*.
2. Activate the mobile token.
 When a FortiToken is added to user *sslvpuser1*, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

To configure 2FA using the CLI:

1. Configure a user and user group.

```
config user local
  edit "sslvpuser1"
    set type password
    set two-factor fortitoken
    set fortitoken <select mobile token for the option list>
    set email-to <user's email address>
    set passwd <user's password>
  next
end
config user group
  edit "sslvpngroup"
    set member "sslvpuser1"
```

```

    next
end

```

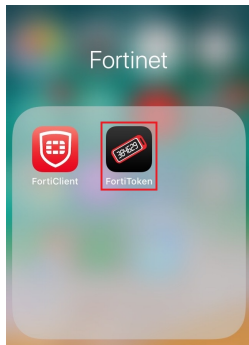
2. Activate the mobile token.

When a FortiToken is added to user *sslvpnuser1*, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

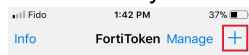
Connecting from FortiClient with FortiToken

To activate your FortiToken:

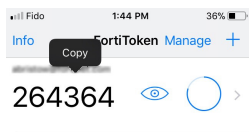
1. On your device, open FortiToken Mobile. If this is your first time opening the application, it may prompt you to create a PIN for secure access to the application and tokens.



2. You should have received your notification via email, select + and use the device camera to scan the token QR code in your email.



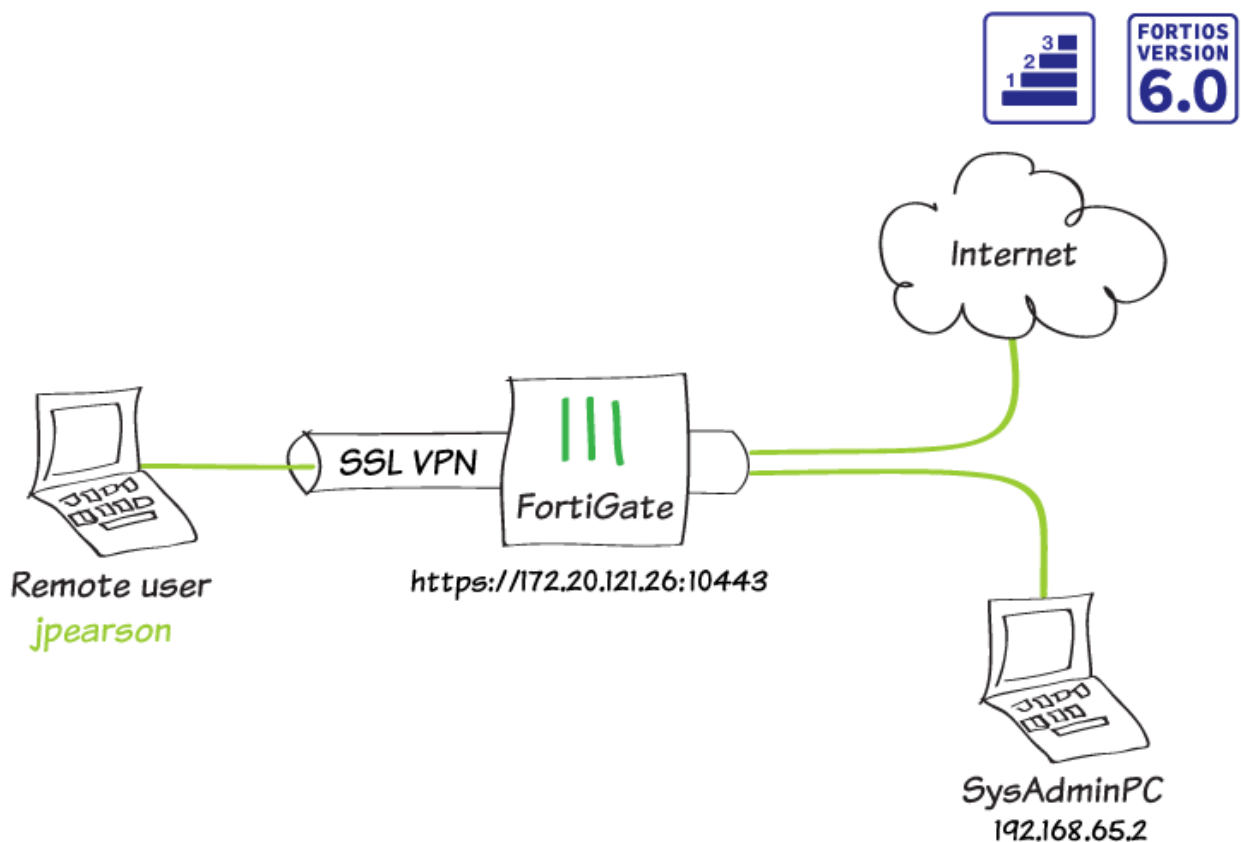
3. FortiToken Mobile provisions and activates your token and generates token codes immediately. To view the OTP's digits, select the eye icon. After you open the application, FortiToken Mobile generates a new six-digit OTP every 30 seconds.



To connect to SSL VPN:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list. Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.
2. Enter your username and password.
3. Click the *Connect* button.
4. A Token field will appear, prompting you for the FortiToken code. Enter the FortiToken code from your Mobile device.
5. After connecting, you can now browse your remote network. Traffic to 192.168.1.0 goes through the tunnel, while other traffic goes through the local gateway. FortiClient displays the connection status, duration, and other relevant information.
6. Click the *Disconnect* button when you are ready to terminate the VPN session.

SSL VPN using web and tunnel mode



In this example, you will allow remote users to access the corporate network using an SSL VPN, connecting either by web mode using a web browser or tunnel mode using FortiClient.

Web mode allows users to access network resources, such as the the AdminPC used in this example.

For users connecting via tunnel mode, traffic to the Internet will also flow through the FortiGate, to apply security scanning to this traffic. During the connecting phase, the FortiGate will also verify that the remote user's antivirus software is installed and up-to-date.

This recipe is in the Basic FortiGate network collection. You can also use it as a standalone recipe.

Editing the SSL VPN portal

1. To edit the **full-access** SSL VPN portal, go to **VPN > SSL-VPN Portals**. The **full-access** portal allows the use of tunnel mode and web mode.
2. Under **Tunnel Mode**, disable **Enable Split Tunneling** for both IPv4 and IPv6 traffic to ensure all Internet traffic will go through the FortiGate.
3. Set **Source IP Pools** to use the default IP range **SSLVPN_TUNNEL_ADDR1**.

Name

Limit Users to One SSL-VPN Connection at a Time ☐

☒ Tunnel Mode

Enable Split Tunneling ⓘ ☐

Source IP Pools

 SSLVPN_TUNNEL_ADDR1 
+

Enable Split Tunneling ⓘ ☐

Routing Address

+

Source IPv6 Pools

 SSLVPN_TUNNEL_IPv6_ADDR1 
+

Tunnel Mode Client Options

Allow client to save password ☐

Allow client to connect automatically ☐

Allow client to keep connections alive ☐

DNS Split Tunneling ☐

4. Under **Enable Web Mode**, create **Predefined Bookmarks** for any internal resources that the SSL VPN users need to access. In the example, the bookmark allows the remote user RDP access to a computer on the internal network.

| | |
|-----------------|------------------------------|
| Name | AdminPC |
| Type | RDP ▼ |
| Host | 192.168.65.2 |
| Port | 3389 |
| Description | |
| Single Sign-On | Disable SSL-VPN Login |
| Username | |
| Password | |
| Keyboard Layout | English (US) keyboard ▼ |
| Security | Standard RDP encryption. ▼ |

Configuring the SSL VPN tunnel

1. To configure the SSL VPN tunnel, go to **VPN > SSL-VPN** Settings.
2. Set **Listen on Interface(s)** to **wan1**. To avoid port conflicts, set **Listen on Port** to **10443**.
3. Set **Restrict Access** to **Allow access from any host**
Optionally, set **Restrict Access** to **Limit access to specific hosts** and specify the addresses of the hosts that are allowed to connect to this VPN.
4. In the example, the **Fortinet_Factory** certificate is used as the **Server Certificate**. To ensure that traffic is secure, you should use your own CA-signed certificate. For more information about using certificates, see Preventing certificate warnings (CA-signed certificates).

5. Under **Tunnel Mode Client Settings**, set **IP Ranges** to use the default IP range **SSLVPN_TUNNEL-ADDR1**.

Connection Settings ⓘ

Listen on Interface(s)

wan1

+

×

Listen on Port

10443

ⓘ Web mode access will be listening at <https://172.25.176.62:10443>

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

Fortinet_Factory

ⓘ You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.

Click here to learn more

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addresses
 Specify custom IP ranges

IP Ranges

SSLVPN_TUNNEL-ADDR1

+

×

DNS Server

Same as client system DNS
 Specify

Specify WINS Servers ☐

Allow Endpoint Registration ☐

6. Under **Authentication/Portal Mapping**, click **Create New** to add the *Employee* user group and map it to the **full-access** portal.
7. If necessary, map a portal for **All Other Users/Groups**.

Users/Groups

Employees

+

×

Portal

full-access

Adding security policies

1. To add an address for the local network, go to **Policy & Objects > Addresses**.
2. Set **Type** to **Subnet**, **Subnet/IP Range** to the local subnet, and **Interface** to **lan**.

| | |
|----------------------------|---|
| Name | <input type="text" value="Internal-network"/> |
| Color | <input type="button" value="Change"/> |
| Type | <input type="text" value="Subnet"/> |
| Subnet / IP Range | <input type="text" value="192.168.65.0/255.255.255.0"/> |
| Interface | <input type="text" value="lan"/> |
| Show in Address List | <input checked="" type="checkbox"/> |
| Static Route Configuration | <input type="checkbox"/> |
| Comments | <input type="text" value=""/> 0/255 |

3. To create a security policy allowing access to the internal network through the VPN tunnel interface, go to **Policy & Objects > IPv4 Policy**.
4. Set **Incoming Interface** to **ssl.root** and **Outgoing Interface** to **lan**. Select **Source** and set **Address** to **all** and **User** to the *Employee* user group. Set **Destination** to the local network address, **Service** to **ALL**, and enable **NAT**.

| | |
|----------------------|---|
| Name ⓘ | <input type="text" value="SSL-access-internal-network"/> |
| Incoming Interface ⚠ | <input type="text" value="SSL-VPN tunnel interface (ssl.root)"/> |
| Outgoing Interface | <input type="text" value="lan"/> |
| Source | <div> all Employees </div> <div>+</div> |
| Destination | <div> Internal-network </div> <div>+</div> |
| Schedule | <input type="text" value="always"/> |
| Service | <div> ALL </div> <div>+</div> |
| Action | <input checked="" type="button" value="ACCEPT"/> <input type="button" value="DENY"/> <input type="button" value="LEARN"/> |

Firewall / Network Options

NAT ☒

IP Pool Configuration

5. Add a second security policy allowing SSL VPN access to the Internet.



If you are allowing split tunneling, this policy is not required.

6. For this policy, set **Incoming Interface** to **ssl.root** and **Outgoing Interface** to **wan1**. Select **Source** and set **Address** to **all** and **User** to the *Employee* user group.

| | |
|--------------------|---|
| Name | SSL-Internet-access |
| Incoming Interface | SSL-VPN tunnel interface (ssl.root ▼) |
| Outgoing Interface | wan1 ▼ |
| Source | <div> all ✕ </div> <div> Employees ✕ </div> <div>+</div> |
| Destination | <div> all ✕ </div> <div>+</div> |
| Schedule | always ▼ |
| Service | <div> ALL ✕ </div> <div>+</div> |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Verifying remote user OS and software

To verify that remote users are using up-to-date devices to connect to your network, you can configure a host check for both operating system (supported for Windows and Mac OS) and software.

You can configure an OS host check for specific OS versions. This check includes the following options: allow the device to connect, block the device, or check that the OS is up-to-date. The default action for all OS versions is allow.

The software host can verify whether the device has AntiVirus software recognized by Windows Security Center, firewall software recognized by Windows Security Center, both, or a custom setting.

Configure both checks using the CLI:

```
config vpn ssl web portal
edit full-access
set os-check enable
```

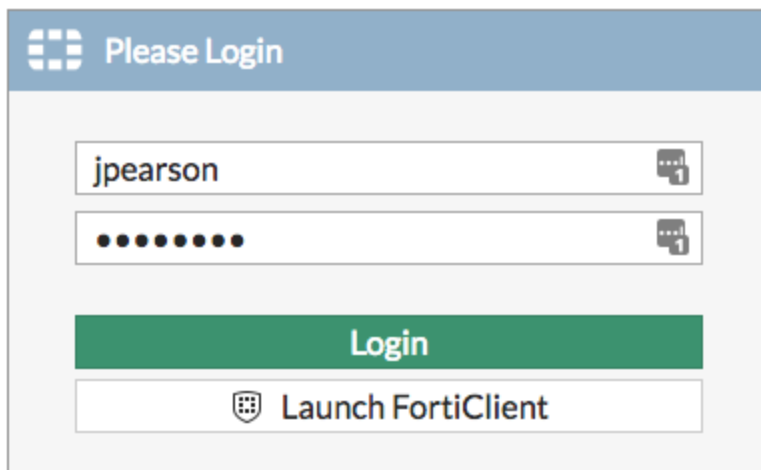
```
config os-check-list {macos-high-sierra-10.13 | macos-sierra-10.12 | os-x-el-  
    capitan-10.11 | os-x-mavericks-10.9 | os-x-yosemite-10.10 | windows-7 |  
    windows-8 | windows-8.1 | windows-10 | windows-2000 | windows-vista | windows-  
    xp}  
    set action {deny | allow | check-up-to-date}  
end  
set host-check {av | fw | av-fw| custom}  
end
```

Results

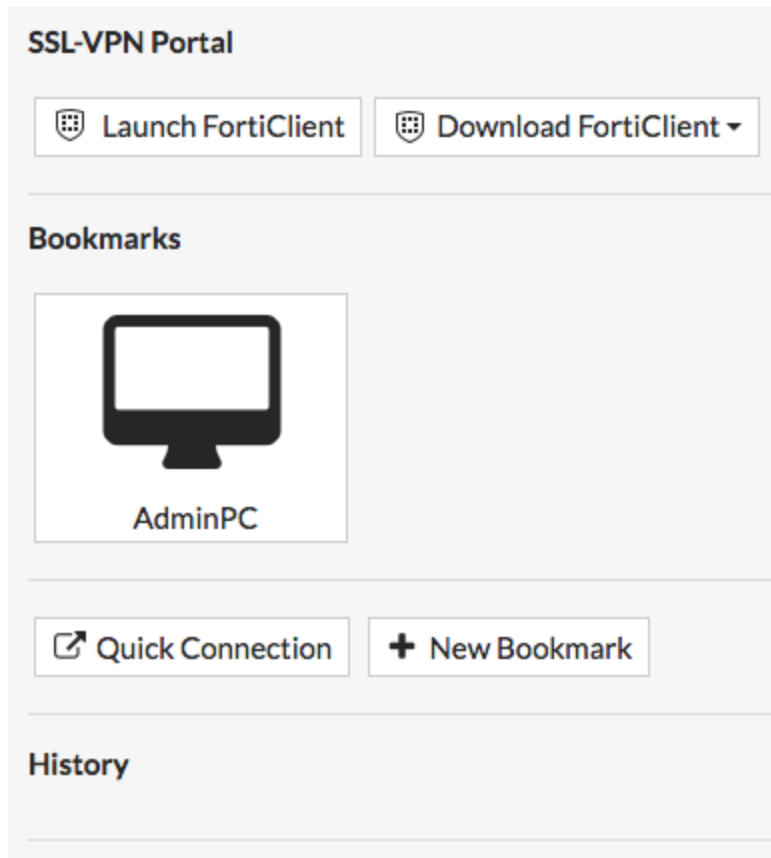
The steps for connecting to the SSL VPN differ depending on whether you are using a web browser or FortiClient.

Web browsers

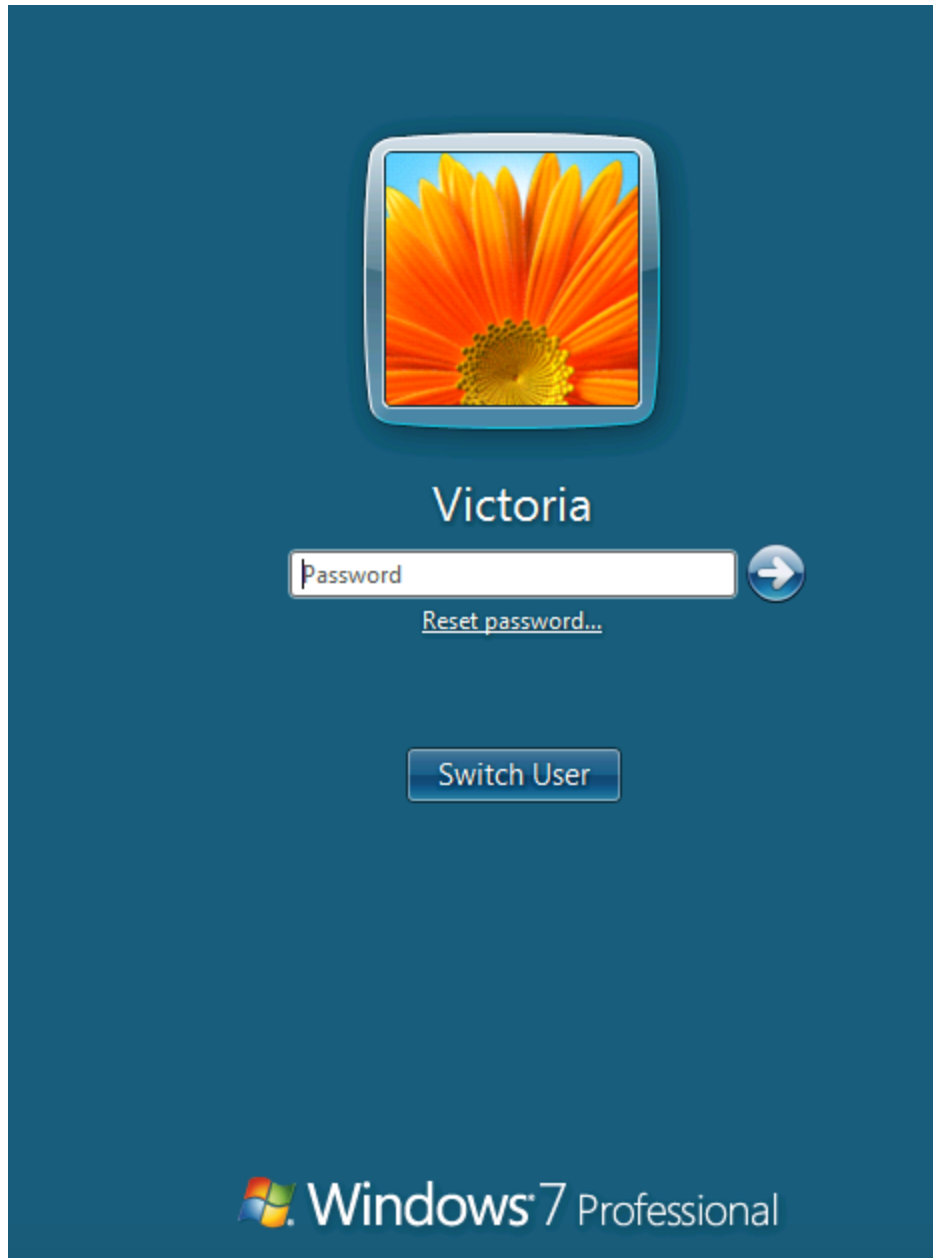
1. Using a supported Internet browser, connect to the SSL VPN web portal using the remote gateway configured in the SSL VPN settings (in the example, <https://172.25.176.62:10443>).
2. Log in to the SSL VPN.



3. After authenticating, you can access the **SSL-VPN Portal**. From this portal, you can launch or download FortiClient, access **Bookmarks**, or connect to other resources using the **Quick Connection** tool.



In this example, selecting the bookmark enables you to connect to the AdminPC.



4. To connect to the Internet, select **Quick Connection**. Select **HTTP/HTTPS**, then enter the **URL** and select **Launch**.

Quick Connection

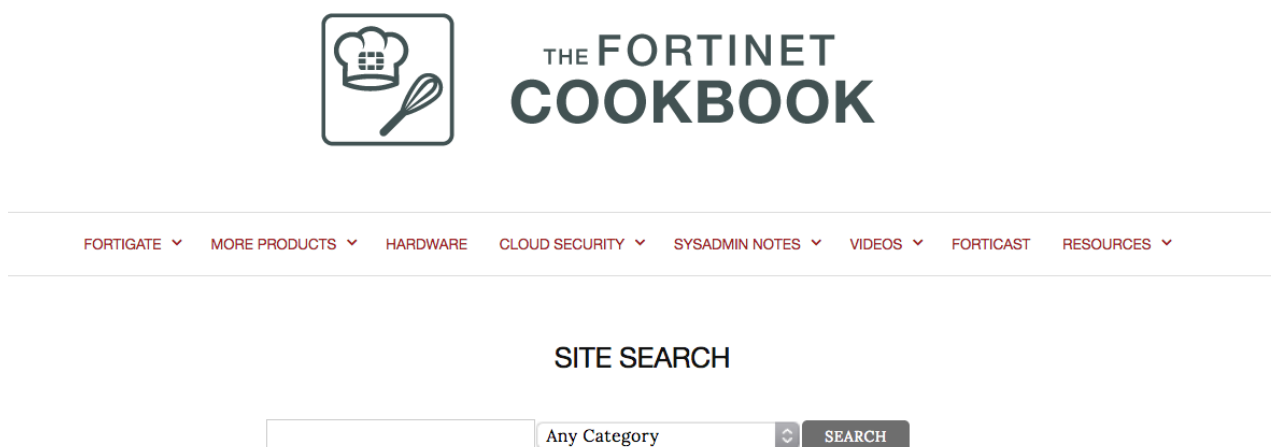
HTTP/HTTPS FTP SMB/CIFS RDP VNC Citrix SSH Telnet Port Forward Ping

URL:

SSO Credentials ☐

Launch Cancel

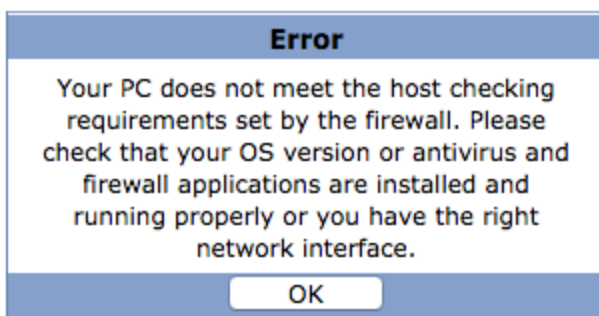
The website loads.



5. To view the list of users currently connected to the SSL VPN, go to **Monitor > SSL-VPN Monitor**. The user is connected to the VPN.

| Username | Last Login | Remote Host | Active Connections |
|----------|--------------------------|---------------|--------------------|
| jpearson | Wed Feb 14 13:14:30 2018 | 172.25.177.46 | SSH: 192.168.62.2 |

6. If a remote device fails the OS or host check, a warning message appears after authentication instead of the portal.



FortiClient

1. If you have not done so already, download FortiClient from www.forticlient.com.
2. Open the FortiClient Console and go to **Remote Access**. Add a new connection.
3. Set **VPN Type** to **SSL VPN**, set **Remote Gateway** to the IP of the listening FortiGate interface (in the example, 172.25.176.62). Select **Customize Port** and set it to **10443**.
4. Select **Add**.

The screenshot shows the 'VPN >> Add Connection' window. Under 'VPN Type', 'SSL VPN' is selected. The 'Connection Name' is 'Office-VPN'. The 'Remote Gateway' is '172.25.176.62'. The 'Customize Port' checkbox is checked, and the port is set to '10443'. The 'Client Certificate' is set to 'None'. Under 'Authentication', 'Save Login' is unchecked. The 'Username' field contains 'username or login name'.

5. Log in to the SSL VPN.

The screenshot shows the login interface. The 'VPN Name' dropdown is set to 'Office-VPN'. The 'Username' field contains 'jpearson'. The 'Password' field is masked with dots.

You are able to connect to the VPN tunnel.

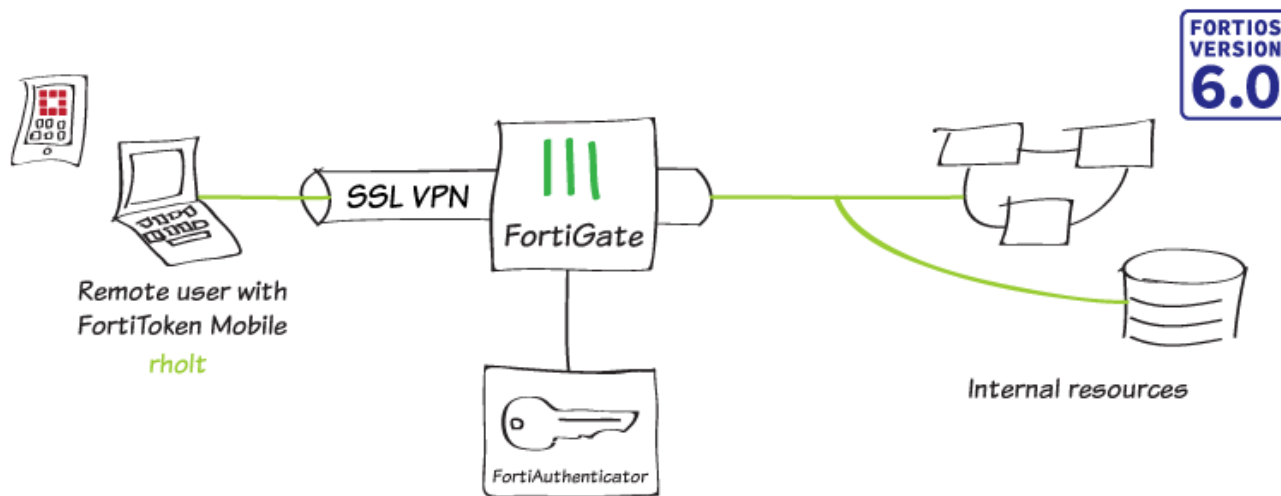


| | |
|----------------|----------|
| Duration | 00:00:07 |
| Bytes Received | 56.866 K |
| Bytes Sent | 29.817 K |

6. To view the list of users currently connected to the SSL VPN, go to **Monitor > SSL-VPN Monitor**. The user is connected to the VPN.

| ▼ Username ▼ | ▼ Last Login ▼ | ▼ Remote Host ▼ | ▼ Active Connections ▼ |
|--------------|--------------------------|-----------------|--------------------------|
| jpearson | Wed Feb 14 13:18:06 2018 | 172.25.177.46 | 🔒 Tunnel: 10.212.134.200 |

SSL VPN with RADIUS and FortiToken



In this recipe, you configure a FortiAuthenticator as a RADIUS server to use with a FortiGate SSL VPN. Remote users connect to the SSL VPN using FortiClient and use FortiToken for two-factor authentication.

If you do not already have an SSL VPN tunnel configured, see [SSL VPN using web and tunnel mode](#).

Creating a user and a user group

1. To create a user account, connect to the FortiAuthenticator, go to **Authentication > User Management > Local Users**, and select **Create New**.

Username:

Password creation:

Password:

Password confirmation:

☒ **Allow RADIUS authentication**

Role

Role:
☐ Administrator
☐ Sponsor
☒ **User**

2. Enter a **Username** and set **Password creation** to **Specify a password**. Enter and confirm the password. Enable **Allow RADIUS authentication** and set **Role** to **User**.
3. After you create the user, more options are available. Edit the account and enable **Token-based authentication**.

Username:

☐ Disabled

☒ Password-based authentication [\[Change Password\]](#)

☒ Token-based authentication

Deliver token code by:
 ☒ FortiToken
 ☐ Email
 ☐ SMS
 ☐ Dual (Email & SMS)
 [Test Token](#)

FortiToken Hardware:
 FortiToken Mobile:
 Delivery method:
 ☒ Email
 ☐ SMS

[Configure a temporary e-mail/SMS token.](#)

☒ Allow RADIUS authentication

☐ Enable account expiration

User Role

Role:
☐ Administrator
☐ Sponsor
☒ **User**

☐ Allow LDAP browsing

User Information

First name: Last name:

Email: Phone number:

4. Set **Deliver token code by** to **FortiToken**. Set **FortiToken Mobile** to an available FortiToken. Set **Delivery method** to **Email**.
5. Under **User Information**, set **Email** to the user's email address.
6. To create a user group, go to **Authentication > User Management > User Groups** and select **Create New**. Add the new user to the group.

Name:

Type: ☒ Local ☐ Remote LDAP ☐ Remote RADIUS ☐ MAC

Users:

Available users ?

admin
leela

Selected users

rholt

Choose all visible
Remove all

7. After you create the user group, more options are available. Edit the group and create a new RADIUS attribute. Set **Vendor** to **Fortinet**, set **Attribute ID** to **Fortinet-Group-Name**, and set **Value** to the name of the group (in the example, `SSL_VPN_RADIUS`).

Create New User Group RADIUS Attribute

Vendor:

Attribute ID:

Type:

Value:

Creating the RADIUS client

1. To create a RADIUS client, go to **Authentication > RADIUS Service > Clients**, and select **Create New**.
2. Enter a **Name** for the client. Set **Client address** to **IP/Hostname** and enter the IP address of the FortiGate (in the example, 172.25.176.62). Set a **Secret** for the client.

Name:

Client address: ☒ IP/Hostname ☐ Subnet ☐ Range

Secret:

First profile name:

Description:

☐ Apply this profile based on RADIUS attributes .

EAP types:

☐ EAP-GTC

☐ EAP-TLS

☐ PEAP

☐ EAP-TTLS

3. Under **User Authentication**, set **Authentication method** to **Apply two-factor authentication if available**. Select **Enable FortiToken Mobile push notifications authentication**.

User Authentication

Authentication method:

☐ Enforce two-factor authentication

☒ Apply two-factor authentication if available (authenticate any user)

☐ Password-only authentication (exclude users without a password)

☐ FortiToken-only authentication (exclude users without a FortiToken)

☒ Enable FortiToken Mobile push notifications authentication

Username input format:

☒ username@realm

☐ realmusername

☐ realm/username

Realms:

| Default | Realm | Allow local users to override remote users | Use Windows AD domain authentication | Groups | Delete |
|----------------------------------|---------------------|--|--------------------------------------|---|----------------------------------|
| <input checked="" type="radio"/> | local Local users | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> Filter: SSL_VPN_RADIUS [Edit] <input type="checkbox"/> Filter local users: [Edit] | <input type="button" value="X"/> |
| + Add a realm | | | | | |

4. For **Realms**, set the default realm to **local | Local users**. Under **Groups**, enable **Filter** and set it to the user group.

Connecting the FortiGate to FortiAuthenticator

1. To add the FortiAuthenticator as a RADIUS server for FortiGate, connect to the FortiGate, go to **User & Device > RADIUS Servers** and select **Create New**.

2. Set a **Name** for the server and set **Authentication method** to **Default**.

Name

Authentication method Default Specify

NAS IP

Include in every user group ☐

Primary Server

IP/Name

Secret

Connection status ✓ Successful

Test Connectivity

Test User Credentials


3. Under **Primary Server**, set **IP/Name** to the IP address of the FortiAuthenticator (in this example, 172.25.176.141) and set **Secret** to the same secret you configured on the FortiAuthenticator.
4. Select **Test Connectivity** to make sure you used the proper settings.
5. To import the user group, go to **User & Device > User Groups** and create a new group.

Name

Type

Members

Remote Groups

| + Add Edit Delete | |
|--|----------------|
| Remote Server | Group Name |
|  RADIUS-FAC | SSL_VPN_RADIUS |

6. Set a **Name** for the group. Under **Remote Groups**, select **+Add** and select the RADIUS server. Set **Groups** to the RADIUS attribute you assigned to the group (in the example, *SSL_VPN_RADIUS*).


















Allowing users to connect to the VPN

1. To configure SSL VPN authentication, go to **VPN > SSL-VPN Settings**.

Authentication/Portal Mapping

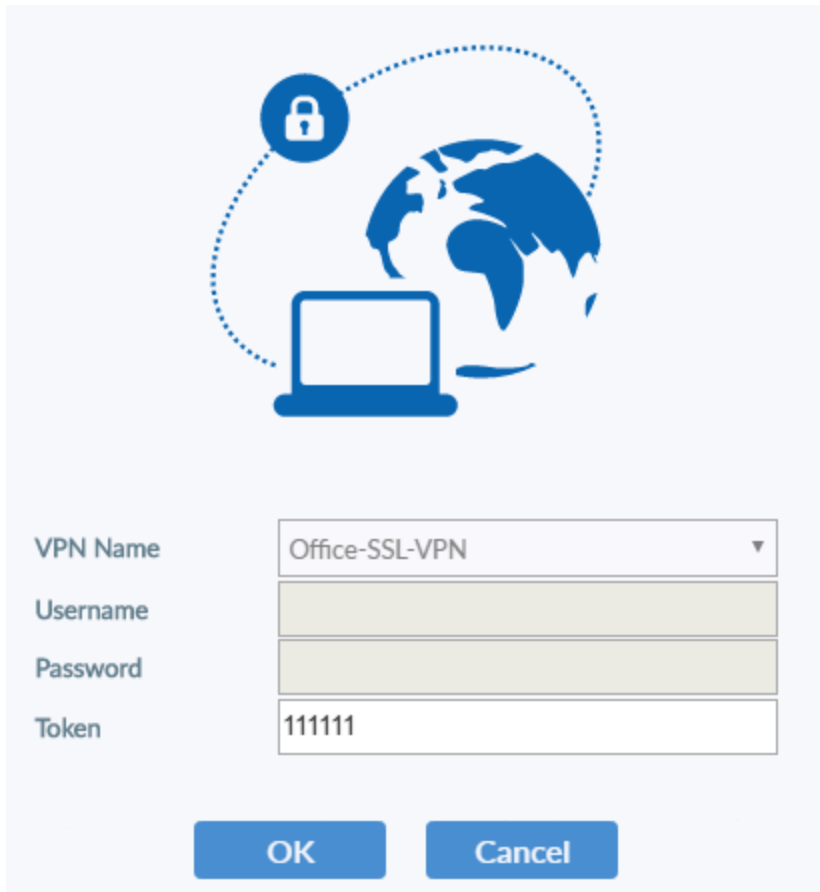
| <div>  Create New  Edit  Delete </div> | |
|---|---------------|
| Users/Groups | Portal |
|  Employees | full-access |
|  RADIUS-VPN | tunnel-access |
| All Other Users/Groups | web-access |

2. Under **Authentication/Portal Mapping**, create a new entry for the RADIUS group. Set **Portal** to **tunnel-access**, which allows users to connect using FortiClient.
3. To allow the new group access to the VPN, go to **Policy & Objects > IPv4 Policy** and edit the policy for the SSL VPN. Select **Source** and set **User** to include the RADIUS group.

| | |
|--|--|
| Name  | SSL-access-internal-network |
| Incoming Interface |  SSL-VPN tunnel interface (ssl.root) ▼ |
| Outgoing Interface |  lan ▼ |
| Source | <div>  all   Employees   SSL_VPN_RADIUS  </div> <div>+</div> |
| Destination | <div>  Internal-network  </div> <div>+</div> |
| Schedule |  always ▼ |
| Service | <div>  ALL  </div> <div>+</div> |
| Action | <div>  ACCEPT  DENY  LEARN </div> |

Results

1. Log in to the SSL VPN.
2. Enter the FortiToken code when it is requested.

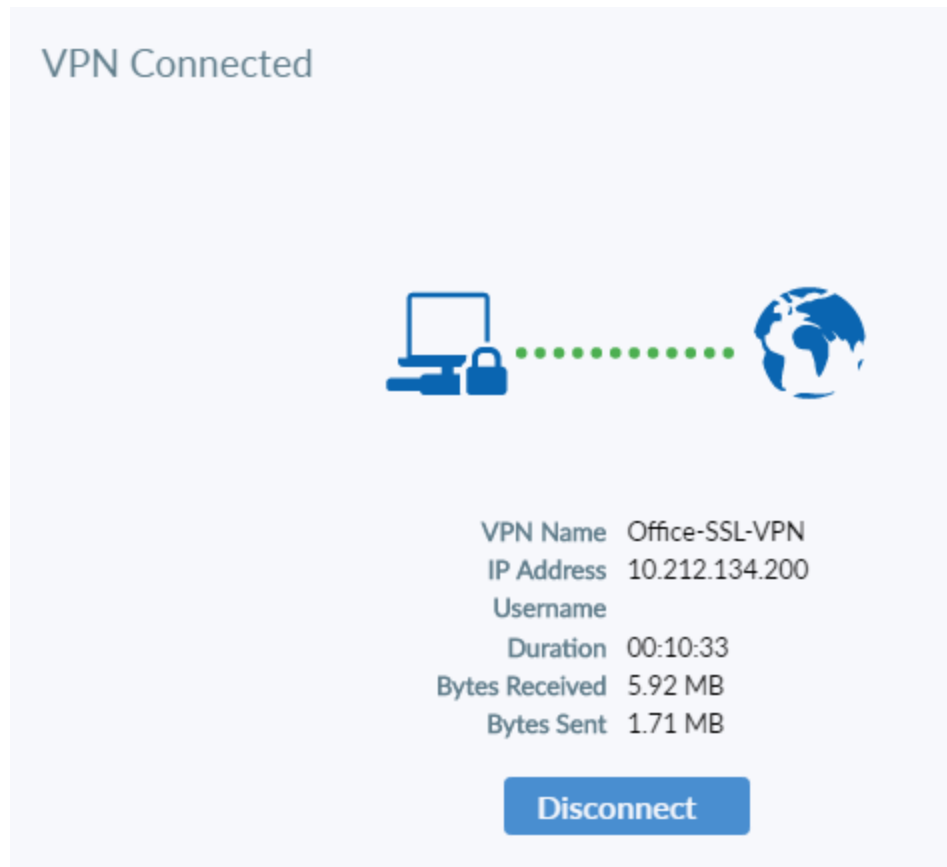


The image shows a login interface for an SSL VPN. At the top, there is a blue icon depicting a globe with a laptop in front of it and a padlock icon above the laptop, connected by dotted lines, symbolizing a secure connection. Below the icon, there are four input fields labeled 'VPN Name', 'Username', 'Password', and 'Token'. The 'VPN Name' field is a dropdown menu currently showing 'Office-SSL-VPN'. The 'Username' and 'Password' fields are empty. The 'Token' field contains the text '111111'. At the bottom of the form, there are two blue buttons: 'OK' and 'Cancel'.

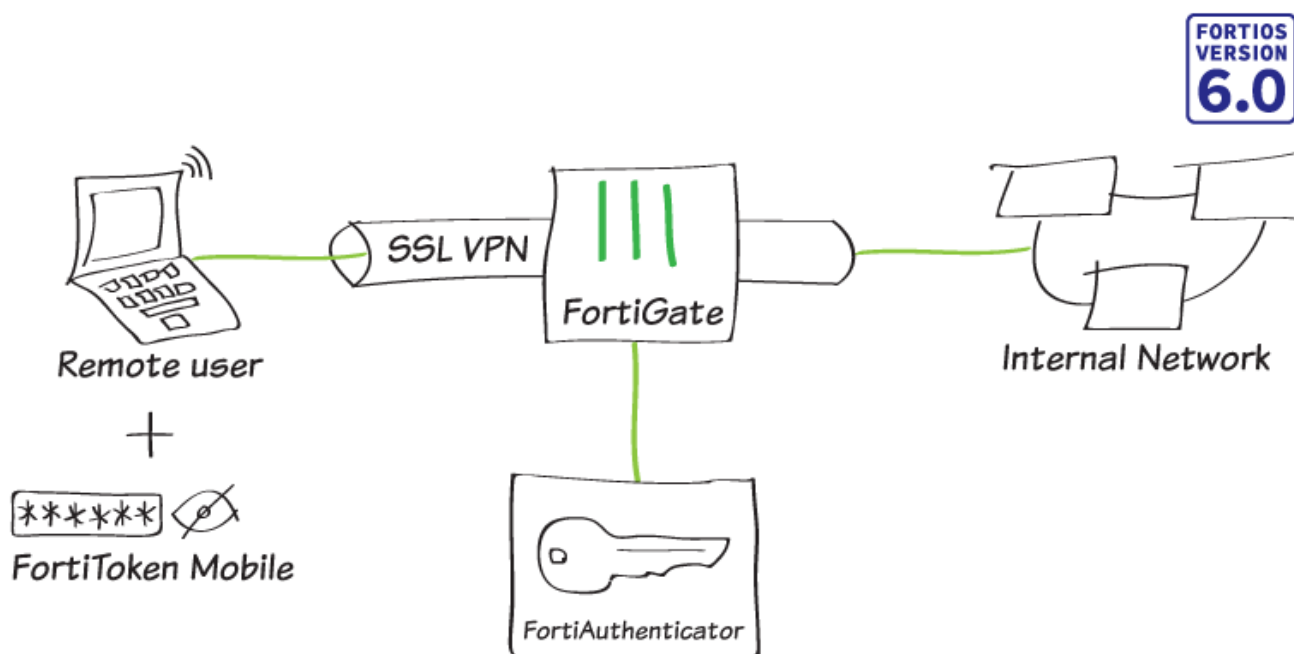
| | |
|----------|------------------|
| VPN Name | Office-SSL-VPN ▼ |
| Username | |
| Password | |
| Token | 111111 |

OK Cancel

3. You are connected to the VPN tunnel.



FortiToken Mobile Push for SSL VPN



In this recipe, you set up FortiAuthenticator to function as a RADIUS server to authenticate SSL VPN users using FortiToken Mobile Push two-factor authentication. With Push notifications enabled, the user can easily accept or deny the authentication request.

For this configuration, you:

- Create a user on the FortiAuthenticator.
- Assign a FortiToken Mobile license to the user.
- Create the RADIUS client (FortiGate) on the FortiAuthenticator, and enable FortiToken Mobile Push notifications.
- Connect the FortiGate to the RADIUS server (FortiAuthenticator).
- Create an SSL VPN on the FortiGate, allowing internal access for remote users.

The following names and IP addresses are used:

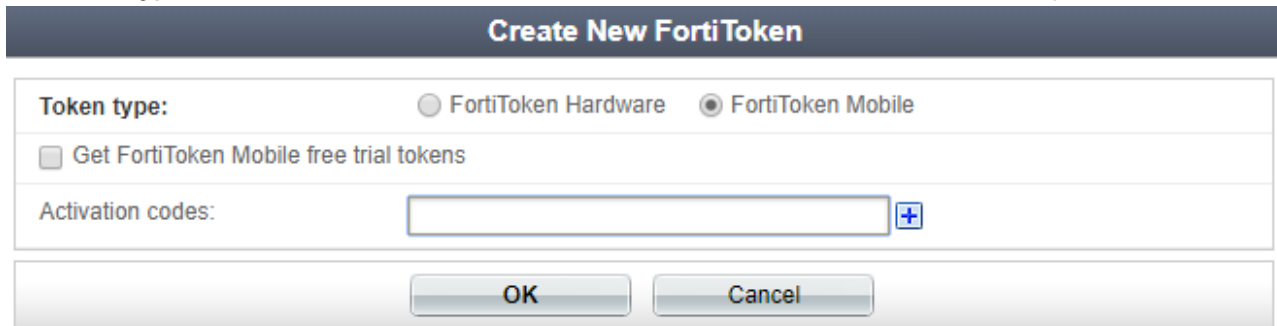
- Username: gthreepwood
- User group: RemoteFTMGroup
- RADIUS server: OfficeRADIUS
- RADIUS client: OfficeServer
- SSL VPN user group: SSLVPNGroup
- FortiAuthenticator: 172.25.176.141
- FortiGate: 172.25.176.92

For the purposes of this recipe, a FortiToken Mobile free trial token is used. This recipe also assumes that the user has already installed the FortiToken Mobile application on their smartphone. You can install the application for Android and iOS. For details, see:

- FortiToken Mobile for Android
- FortiToken Mobile for iOS

Adding FortiToken to FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > User Management > FortiTokens**, and select **Create New**.
2. Set **Token type** to **FortiToken Mobile**, and enter the FortiToken **Activation codes** in the field provided.



Create New FortiToken

Token type: ☐ FortiToken Hardware ☒ FortiToken Mobile

☐ Get FortiToken Mobile free trial tokens

Activation codes: +

OK Cancel

Adding user to FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > User Management > Local Users**, and select **Create New**.
2. Enter a **Username** (*gthreepwood*) and enter and confirm the user password.

3. Enable **Allow RADIUS authentication**, and select **OK** to access additional settings.

Create New Local User

Username:

Password creation:

Password:

Password confirmation:

☒ Allow RADIUS authentication

☐ Force password change on next logon

Role

Role: ☐ Administrator
☐ Sponsor
☒ User

Account Expiration

☐ Enable account expiration

4. Enable **Token-based authentication** and select to deliver the token code by **FortiToken**. Select the FortiToken added earlier from the **FortiToken Mobile** drop-down menu.
5. Set **Delivery method** to **Email**. This will automatically open the **User Information** section where you can enter the user email address in the field provided.

Change local user

✓ Successfully added local user "gthreepwood". You may edit it again below.

| | |
|---|--|
| Username: gthreepwood | |
| <input type="checkbox"/> Disabled | |
| <input checked="" type="checkbox"/> Password-based authentication [Change Password] | |
| <input checked="" type="checkbox"/> Token-based authentication | |
| Deliver token code by: <input checked="" type="radio"/> FortiToken <input type="radio"/> Email <input type="radio"/> SMS <input type="radio"/> Dual (Email & SMS) <button style="float: right;">Test Token</button> | |
| FortiToken Hardware: | <input type="text" value="[Please Select]"/> <div style="float: right;"> FortiToken Mobile: <input type="text" value="XXXXXXXXXXXX"/> x </div> |
| Delivery method: <input checked="" type="radio"/> Email <input type="radio"/> SMS | |
| Configure a temporary e-mail/SMS token. | |
| <input checked="" type="checkbox"/> Allow RADIUS authentication | |
| <input type="checkbox"/> Enable account expiration | |
| <input type="checkbox"/> Force password change on next logon | |

User Role

| |
|---|
| Role: <input type="radio"/> Administrator <input type="radio"/> Sponsor <input checked="" type="radio"/> User |
| <input type="checkbox"/> Allow LDAP browsing |

User Information

| | | | |
|--------------------------------------|---|--------------------------------------|--|
| First name: | <input type="text"/> | Last name: | <input type="text"/> |
| Email: | <input type="text" value="admin@fortinet.com"/> | Phone number: | <input type="text"/> |
| Mobile number: | <input type="text"/> | SMS gateway: | <input type="text" value="Use default"/> <div style="float: right;">Test SMS</div> |
| Street address: <input type="text"/> | | | |
| City: <input type="text"/> | | State/Province: <input type="text"/> | |

6. Next, go to **Authentication > User Management > User Groups**, and select **Create New**.
7. Enter a **Name** (*RemoteFTMUsers*) and add **gthreepwood** to the group by moving the user from **Available users** to **Selected users**.

Create New User Group

Name: RemoteFTMUsers

Type: ☒ Local ☐ Remote LDAP ☐ Remote RADIUS ☐ MAC

Users:

Available users ⓘ

adam
admin
efuufuas
leela
pacman
rholt

Selected users

gthreepwood

Choose all visible

Remove all

Password policy: Default ▼

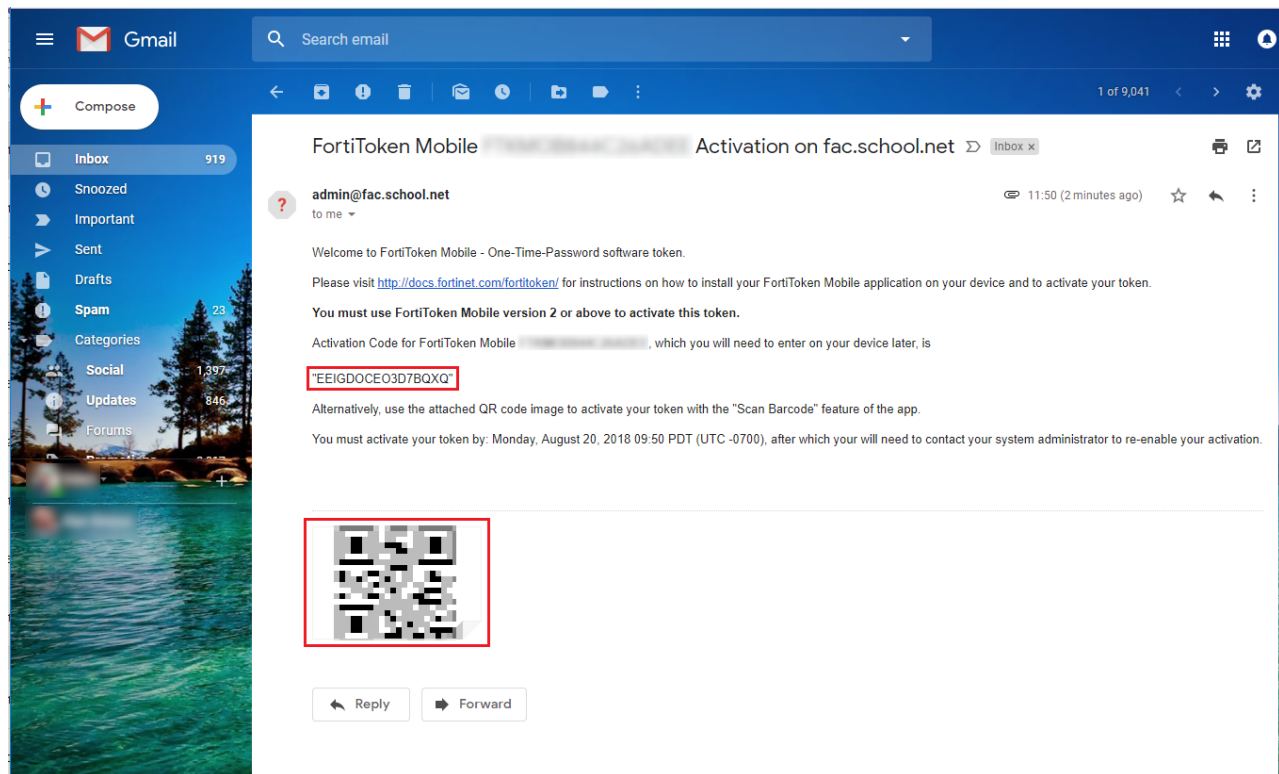
☐ Usage Profile [Please Select] ▼

☐ Allow token self-provisioning

OK

Cancel

8. The FortiAuthenticator sends the FortiToken Mobile activation to the user's email address. If the email does not appear in the inbox, check the spam folder.
9. The user activates their FortiToken Mobile through the FortiToken Mobile application by either entering the activation code provided or by scanning the QR code attached.



Creating the RADIUS client on FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients**, and select **Create New** to add the FortiGate as a RADIUS client.
2. Enter a **Name** (*OfficeServer*), the IP address of the FortiGate, and set a **Secret**. The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.
3. Set **Authentication method** to **Enforce two-factor authentication** and check the **Enable FortiToken Mobile push notifications authentication** checkbox.



Note the **Username input format**. This is the format that the user must use to enter their username in the web portal, made up of their username and realm. In this example, the full username for gthreepwood is **"gthreepwood@local"**.

4. Set **Realms** to **local | Local users**, and add **RemoteFTMUsers** to the **Groups** filter.

Add RADIUS client

| Name: | <input type="text" value="OfficeServer"/> | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--------------------------------------|--|--------|---------|-------|--|--------------------------------------|--------|--------|----------------------------------|---------------------|--------------------------|--------------------------|--|---|---------------|--|--|--|--|--|
| Client address: | <input checked="" type="radio"/> IP/Hostname <input type="radio"/> Subnet <input type="radio"/> Range | | | | | | | | | | | | | | | | | | | | | | |
| | <input type="text" value="172.25.176.92"/> | | | | | | | | | | | | | | | | | | | | | | |
| Secret: | <input type="password" value="*****"/> | | | | | | | | | | | | | | | | | | | | | | |
| First profile name: | <input type="text" value="Default"/> | | | | | | | | | | | | | | | | | | | | | | |
| Description: | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Apply this profile based on RADIUS attributes. | | | | | | | | | | | | | | | | | | | | | | | |
| EAP types: | <input type="checkbox"/> EAP-GTC <input type="checkbox"/> EAP-TLS <input type="checkbox"/> PEAP <input type="checkbox"/> EAP-TTLS | | | | | | | | | | | | | | | | | | | | | | |
| Device Authentication | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> MAC Authentication Bypass(MAB) | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> AD machine authentication | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> MAC device filtering | | | | | | | | | | | | | | | | | | | | | | | |
| User Authentication | | | | | | | | | | | | | | | | | | | | | | | |
| Authentication method: | <input checked="" type="radio"/> Enforce two-factor authentication <input type="radio"/> Apply two-factor authentication if available (authenticate any user) <input type="radio"/> Password-only authentication (exclude users without a password) <input type="radio"/> FortiToken-only authentication (exclude users without a FortiToken) | | | | | | | | | | | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> Enable FortiToken Mobile push notifications authentication | | | | | | | | | | | | | | | | | | | | | | | |
| Username input format: | <input checked="" type="radio"/> username@realm <input type="radio"/> realm/username <input type="radio"/> realm/username | | | | | | | | | | | | | | | | | | | | | | |
| Realms: | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Default</th> <th style="width: 30%;">Realm</th> <th style="width: 20%;">Allow local users to override remote users</th> <th style="width: 20%;">Use Windows AD domain authentication</th> <th style="width: 15%;">Groups</th> <th style="width: 5%;">Delete</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="radio"/></td> <td>local Local users</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> <td> <input checked="" type="checkbox"/> Filter: RemoteFTMUsers [Edit] <input type="checkbox"/> Filter local users: [Edit] </td> <td style="text-align: center;">✕</td> </tr> <tr> <td colspan="6" style="text-align: center;">+ Add a realm</td> </tr> </tbody> </table> | | | | | Default | Realm | Allow local users to override remote users | Use Windows AD domain authentication | Groups | Delete | <input checked="" type="radio"/> | local Local users | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> Filter: RemoteFTMUsers [Edit] <input type="checkbox"/> Filter local users: [Edit] | ✕ | + Add a realm | | | | | |
| Default | Realm | Allow local users to override remote users | Use Windows AD domain authentication | Groups | Delete | | | | | | | | | | | | | | | | | | |
| <input checked="" type="radio"/> | local Local users | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> Filter: RemoteFTMUsers [Edit] <input type="checkbox"/> Filter local users: [Edit] | ✕ | | | | | | | | | | | | | | | | | | |
| + Add a realm | | | | | | | | | | | | | | | | | | | | | | | |
| Enable captive portal: | <input type="checkbox"/> Credentials based portals (Captive URL: /caplogin/, Guest URL: /guests/) <input type="checkbox"/> Social based captive portal (URL: /social_login/) <input type="checkbox"/> MAC address based captive portal (URL: /malogin/) | | | | | | | | | | | | | | | | | | | | | | |

Connecting the FortiGate to the RADIUS server

1. On the FortiGate, go to **User & Device > RADIUS Servers**, and select **Create New** to connect to the RADIUS server (FortiAuthenticator).
2. Enter a **Name** (*OfficeRADIUS*), the IP address of the FortiAuthenticator, and enter the **Secret** created before.
3. Select **Test Connectivity** to be sure you can connect to the RADIUS server. Then select **Test User Credentials** and enter the credentials for **gthreepwood**.

New RADIUS Server

Name

OfficeRADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.25.176.141

Secret

••••••••

Connection status

☒ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

- Because the user has been assigned a FortiToken, the test should come stating that **More validation is required**.
- The FortiGate can now connect to the FortiAuthenticator as the RADIUS client configured earlier.

New RADIUS Test User Credentials ✕

Name Username

Authentication Password

NAS IP

Include in e Connection status ✓ Successful

Primary Ser User credentials ✗ More validation is required

IP/Name Server message

Secret

Connection

Test Conn

Test User

Secondary S

AVP: l=79 t=Reply-Message(18) Value: '+Enter token code or no code to send a notification to your FortiToken Mobile'; AVP: l=11 t=Vendor-Specific(26) v=Fortinet(12356) VSA: l=5 t=Fortinet-Token-Challenge(15) Value: '001'; AVP: l=3 t=State(24) Value: 31

Test Close

- Then go to **User & Device > User Groups**, and select **Create New** to map authenticated remote users to a user group on the FortiGate.
- Enter a **Name** (*SSLVPNGroup*) and select **Add** under **Remote Groups**.

Edit User Group

Name

Type **Firewall**

Fortinet Single Sign-On (FSSO)

RADIUS Single Sign-On (RSSO)

Guest

Members +

Remote Groups

+ Add Edit Delete

| Remote Server | Group Name |
|---------------------------|------------|
| No matching entries found | |

OK Cancel

- Select **OfficeRADIUS** under the **Remote Server** drop-down menu, and leave the **Groups** field blank.

| Edit User | | Add Group Match | |
|-----------|---------------|-----------------|---|
| Name | Remote Server | OfficeRADIUS | |
| Type | Groups | | + |

Configuring the SSL VPN

1. On the FortiGate, go to **VPN > SSL-VPN Portals**, and edit the **full-access** portal.
2. Toggle **Enable Split Tunneling** so that it is disabled.

| Edit SSL-VPN Portal | |
|---|--|
| Name | full-access |
| Limit Users to One SSL-VPN Connection at a Time <input type="checkbox"/> | |
| <input checked="" type="checkbox"/> Tunnel Mode | |
| <div> <div>Enable Split Tunneling</div> <div> <i>i</i> <input type="checkbox"/> </div> </div> | |
| Source IP Pools | <div> <div>SSLVPN_TUNNEL_ADDR1</div> <div>+</div> </div> |

3. Then go to **VPN > SSL-VPN Settings**.
4. Under **Connection Settings** set **Listen on Interface(s)** to **wan1** and **Listen on Port** to **10443**.
5. Under **Tunnel Mode Client Settings**, select **Specify custom IP ranges**. The **IP Ranges** should be set to **SSLVPN_TUNNEL_ADDR1** and the IPv6 version by default.
6. Under **Authentication/Portal Mapping**, select **Create New**.
7. Set the **SSLVPNGroup** user group to the **full-access** portal, and assign **All Other Users/Groups** to **web-access**

— this will grant all other users access to the web portal *only*.

8. Go to **Policy & Objects > IPv4 Policy** and create a new SSL VPN policy.
9. Set **Incoming Interface** to the **SSL-VPN tunnel interface** and set **Outgoing Interface** to the Internet-facing interface (in this case, **wan1**).
10. Set **Source** to the **SSLVPNGroup** user group and the **all** address.
11. Set **Destination Address** to **all**, **Schedule** to **always**, **Service** to **ALL**, and enable **NAT**.

New Policy

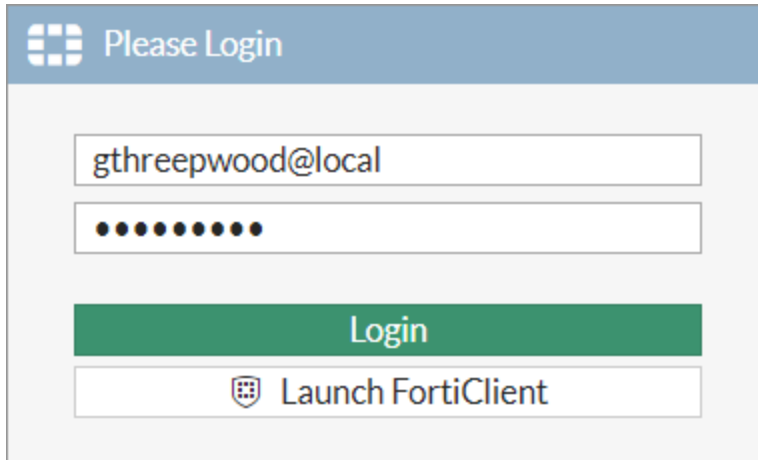
| | |
|--------------------|---|
| Name | SSL-VPN |
| Incoming Interface | SSL-VPN tunnel interface (ssl.root |
| Outgoing Interface | wan1 |
| Source | all SSLVPNGroup |
| Destination | all |
| Schedule | always |
| Service | ALL |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒

Results

1. From a remote device, open a web browser and navigate to the SSL VPN web portal (*https://<fortigate-ip>:10443*).
2. Enter **gthreepwood**'s credentials and select **Login**. Use the correct format (in this case, username@realm), as per the client configuration on the FortiAuthenticator.

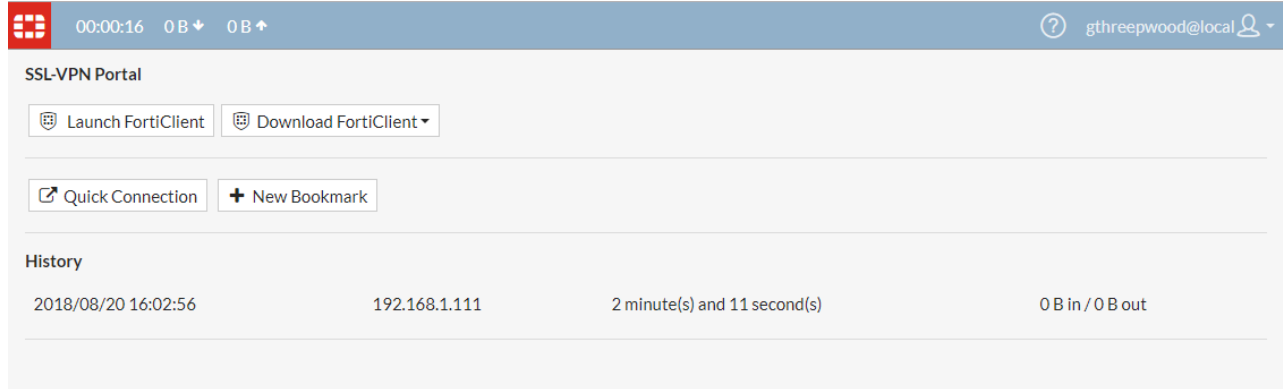


The screenshot shows the FortiAuthenticator SSL VPN web portal login interface. At the top, there is a blue header with the FortiAuthenticator logo and the text "Please Login". Below the header, there are two input fields. The first field contains the username "gthreepwood@local". The second field is a password field with ten dots representing the masked password. Below the password field, there is a green button labeled "Login". At the bottom, there is a white button with a shield icon and the text "Launch FortiClient".

3. The FortiAuthenticator will then push a login request notification through the FortiToken Mobile application. Select

Approve.

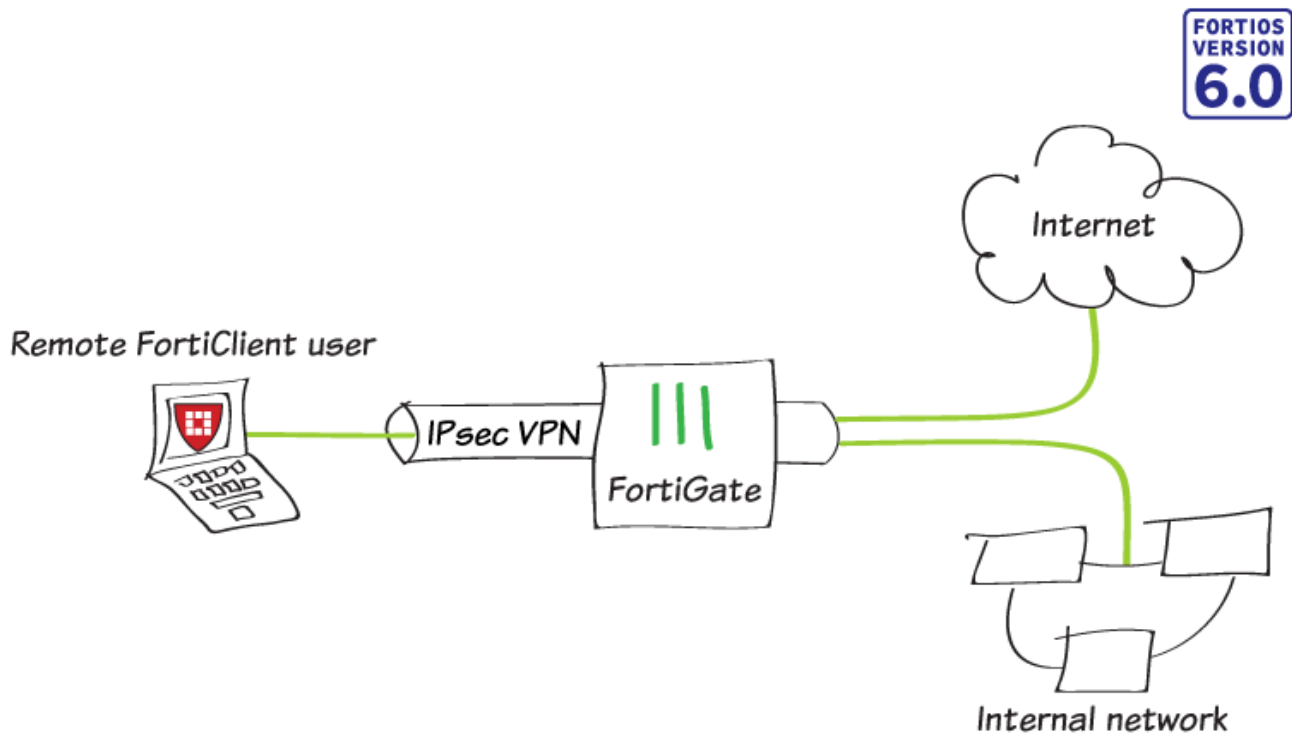
4. Upon approving the authentication, **gthreepwood** is successfully logged into the SSL VPN portal.



5. On the FortiGate, go to **Monitor > SSL-VPN Monitor** to confirm the user's connection.

| Refresh | | | |
|-------------------|---------------------|---------------|--------------------|
| Username | Last Login | Remote Host | Active Connections |
| gthreepwood@local | 2018/08/20 16:32:02 | 192.168.1.111 | |

IPsec VPN with FortiClient





In this example, you allow remote users to access the corporate network using an IPsec VPN that they connect to using FortiClient. The remote user Internet traffic is also routed through the FortiGate (split tunneling will not be enabled).

Optionally, you can create a user that uses two factor authentication, and an user LDAP user.

Adding a firewall address



1. To create a new firewall address, go to **Policy & Objects > Addresses** and select **Create New > Address**.
2. Set **Category** to **Address** and enter a **Name**. Set **Type** to **Subnet**, **Subnet/IP Range** to the local subnet, and

Interface to lan.




| | |
|----------------------------|--|
| Category | Address Proxy Address |
| Name | Internal-network |
| Color |  Change |
| Type | Subnet ▼ |
| Subnet / IP Range | 192.168.65.0/255.255.255.0 |
| Interface |  lan ▼ |
| Show in Address List | <input checked="" type="checkbox"/> |
| Static Route Configuration | <input type="checkbox"/> |
| Comments | <input type="text"/> 0/255 |

Configuring the IPsec VPN

1. To create the VPN, go to **VPN > IPsec Wizard** and create a new tunnel using a pre-existing template.
2. Name the VPN. The tunnel name cannot include any spaces or exceed 13 characters. Set **Template** to **Remote Access**, and set **Remote Device Type** to **FortiClient VPN for OS X, Windows, and Android**.

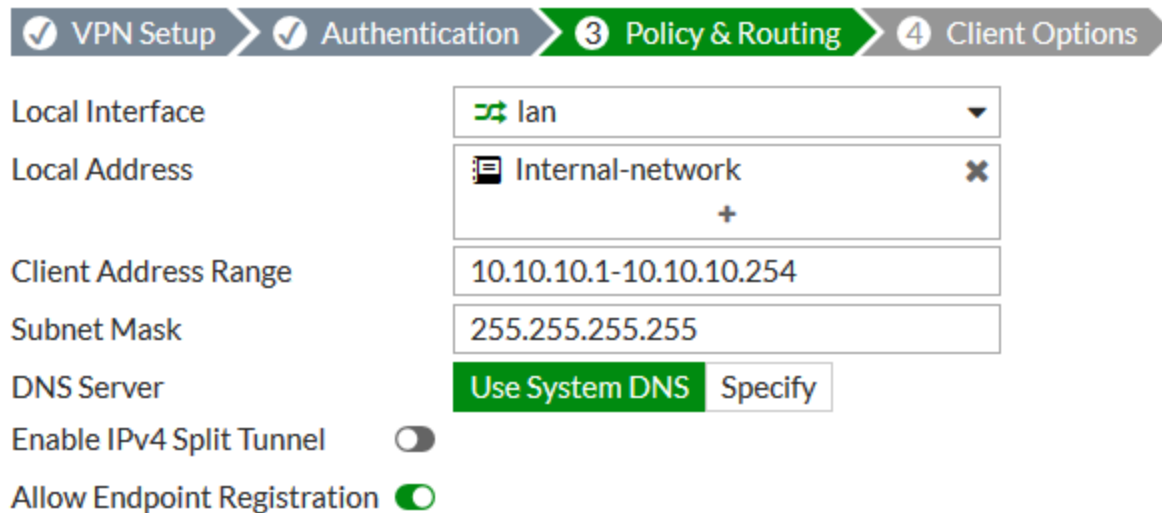
| | | | |
|--------------------|---|--------------------|------------------|
| 1 VPN Setup | 2 Authentication | 3 Policy & Routing | 4 Client Options |
| Name | FCT-VPN | | |
| Template Type | Site to Site Remote Access Custom | | |
| Remote Device Type | Client-based Native | | |
| |  FortiClient  Cisco | | |

3. Set the **Incoming Interface** to **wan1** and **Authentication Method** to **Pre-shared Key**.
4. Enter a pre-shared key. This pre-shared key is a credential for the VPN and should differ from the user password. Select the **Employees** group.

| | | | |
|-----------------------|--|--------------------|------------------|
| ✓ VPN Setup | 2 Authentication | 3 Policy & Routing | 4 Client Options |
| Incoming Interface |  wan1 ▼ | | |
| Authentication Method | Pre-shared Key Signature | | |
| Pre-shared Key | <input type="password"/>  | | |
| User Group |  Employees ▼ | | |

5. Set **Local Interface** to **lan** and set **Local Address** to the local network address.

6. Enter a **Client Address Range** for VPN users. The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the `_range` suffix (in the example, `IPsec-FCT_range`).
7. Make sure **Enable IPv4 Split Tunnel** is *not* selected, so that all Internet traffic will go through the FortiGate. If you do select **Enable Split Tunneling**, traffic not intended for the corporate network will not flow through the FortiGate or be subject to the corporate security profiles.



VPN Setup > Authentication > **3 Policy & Routing** > 4 Client Options

Local Interface: lan

Local Address: Internal-network

Client Address Range: 10.10.10.1-10.10.10.254

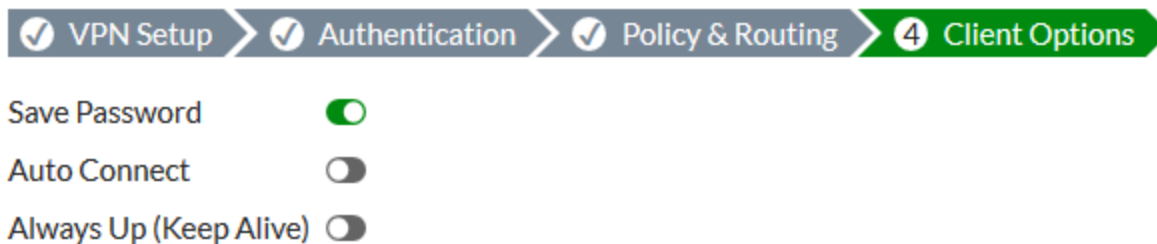
Subnet Mask: 255.255.255.255

DNS Server: Use System DNS Specify

Enable IPv4 Split Tunnel: ☐

Allow Endpoint Registration: ☒

8. Select **Client Options** as desired.



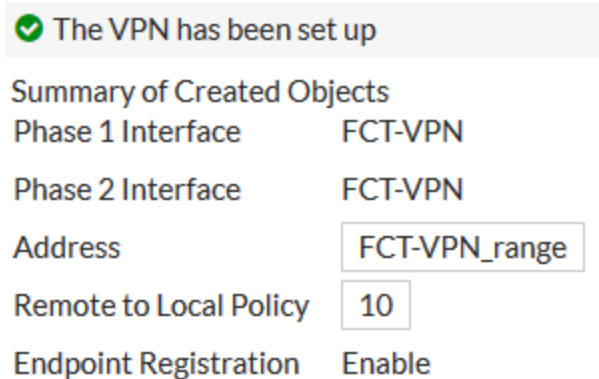
VPN Setup > Authentication > Policy & Routing > **4 Client Options**

Save Password: ☒

Auto Connect: ☐

Always Up (Keep Alive): ☐

9. After you create the tunnel, a summary page appears listing the objects which have been added to the FortiGate's configuration by the wizard.



✓ The VPN has been set up

Summary of Created Objects

| | |
|------------------------|---------------|
| Phase 1 Interface | FCT-VPN |
| Phase 2 Interface | FCT-VPN |
| Address | FCT-VPN_range |
| Remote to Local Policy | 10 |
| Endpoint Registration | Enable |

10. If multiple dialup IPsec VPNs are defined for the same dialup server interface, each phase1 configuration must define a unique peer ID to distinguish the tunnel that the remote client is connecting to:
 - a. Go to **VPN > IPsec Tunnels** and edit the just created tunnel.
 - b. Click **Convert To Custom Tunnel**.
 - c. In the **Authentication** section, click **Edit**.

- d. Under **Peer Options**, set **Accept Types** to **Specific peer ID**.
- e. In the **Peer ID** field, enter a unique ID, such as **dialup1**.
- f. Click **OK**.

11. To view the VPN interface created by the wizard, go to **Network > Interfaces**.

| Status | Name | Members | IP/Netmask | Type |
|--------|---------|---------|-----------------------------|--------------------|
| | wan1 | | 172.25.176.62 255.255.255.0 | Physical Interface |
| | FCT-VPN | | 169.254.1.1 255.255.255.255 | Tunnel Interface |

12. To view the firewall address created by the wizard, go to **Policy & Objects > Addresses**.

| Name | Type | Details |
|---------------|----------|---------------------------|
| Address 16 | | |
| FCT-VPN_range | IP Range | 10.10.10.1 - 10.10.10.254 |

13. To view the security policy created by the wizard, go to **Policy & Objects > IPv4 Policy**.








| ID | Name | Source | Destination | Schedule | Service | Action | NAT |
|-----------------|--------------|---------|---------------|----------|---------|--------|---------|
| FCT-VPN → lan 1 | | | | | | | |
| 10 | vpn_FCT-V... | FCT-VPN | Internal-netw | always | ALL | ACCEPT | Enabled |

Creating a security policy

The IPsec wizard automatically created a security policy allowing IPsec VPN users to access the internal network. However, since split tunneling is disabled, another policy must be created to allow users to access the Internet through the FortiGate.

1. To create a new policy, go to **Policy & Objects > IPv4 Policies** and select **Create New**. Set a policy name that will identify what this policy is used for (in the example, *IPsec-VPN-Internet*).
2. Set **Incoming Interface** to the tunnel interface and **Outgoing Interface** to **wan1**. Set **Source** to the IPsec client address range, **Destination Address** to **all**, **Service** to **ALL**, and enable **NAT**.

3. Configure any remaining firewall and security options as desired.

| | | |
|--|---|--|
| Name  | IPsec-VPN-Internet | |
| Incoming Interface |  FCT-VPN ▼ | |
| Outgoing Interface |  wan1 ▼ | |
| Source |  FCT-VPN_range ✕ + | |
| Destination |  all ✕ + | |
| Schedule |  always ▼ | |
| Service |  ALL ✕ + | |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN | |

Firewall / Network Options

NAT ☒

Add FortiToken two-factor authentication

This configuration adds two-factor authentication (2FA) to the FortiClient dialup VPN configuration ([Configuring the IPsec VPN on page 286](#)). It uses one of the two free mobile FortiTokens that is already installed on the FortiGate.

To configure 2FA using the GUI:

1. Configure a user:
 - a. Go to **User & Device > User Definition** and create or edit local user **twoFAuser1**.
 - b. Enter the user's **Email Address**.
 - c. Enable **Two-factor Authentication** and select one mobile **Token** from the list,
 - d. Enable **Send Activation Code** and select **Email**.
 - e. Click **Next** and click **Submit**.
2. Add the user to the group:
 - a. Go to **User & Device > User Groups** and edit the **Employees**.
 - b. Add **twoFAuser1** to the **Members** list.
 - c. Click **OK**.
3. Activate the mobile token.
 - a. When a FortiToken is added to user **twoFAuser1**, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

To configure 2FA using the CLI:

1. Configure a user and user group.

```
config user local
    edit "twoFAuser1"
        set type password
        set two-factor fortitoken
        set fortitoken <select mobile token for the option list>
        set email-to <user's email address>
        set passwd <user's password>
    next
end
config user group
    edit "Employees"
        append member "twoFAuser1"
    next
end
```

2. Activate the mobile token.

- a. When a FortiToken is added to user **twoFAuser1**, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

Add LDAP user authentication

This configuration adds LDAP user authentication to the FortiClient dialup VPN configuration ([Configuring the IPsec VPN on page 286](#)). You must have already generated and exported a CA certificate from your AD server.

To configure LDAP user authentication using the GUI:

1. Import the CA certificate into FortiGate:

- a. Go to **System > Certificates**.
If the **Certificates** option is not visible, enable it in **Feature Visibility**.
- b. Click **Import > CA Certificate**.
- c. Set **Type** to **File**.
- d. Click **Upload** then find and select the certificate file.
- e. Click **OK**.
The CA certificate now appears in the list of **External CA Certificates**. In this example, it is called **CA_Cert_1**.
- f. Optionally, rename the system generated **CA_Cert_1** to something more descriptive:

```
config vpn certificate ca
    rename CA_Cert_1 to LDAPS-CA
end
```

2. Configure the LDAP user:

- a. Go to **User & Device > LDAP Servers** and click **Create New**.
- b. Set **Name** to **ldaps-server** and specify **Server IP/Name**.
- c. Specify **Common Name Identifier** and **Distinguished Name**.
- d. Set **Bind Type** to **Regular**.
- e. Specify **Username** and **Password**.
- f. Enable **Secure Connection** and set **Protocol** to **LDAPS**.

- g. For **Certificate**, select **LDAP server CA LDAPS-CA** from the list.
 - h. Click **OK**.
- 3. Add the LDAP user to the user group:
 - a. Go to **User & Device > User Groups** and edit the **Employees** group.
 - b. In **Remote Groups**, click **Add** to add the **ldaps-server** remote server.
 - c. Click **OK**.

To configure LDAP user authentication using the CLI:

1. Import the CA certificate using the GUI.
2. Configure the LDAP user:

```
config user ldap
  edit "ldaps-server"
    set server "172.20.120.161"
    set cnid "cn"
    set dn "cn=Users,dc=qa,dc=fortinet,dc=com"
    set type regular
    set username "CN=Administrator,cn=users,DC=qa,DC=fortinet,DC=com"
    set password *****
    set group-member-check group-object
    set secure ldaps
    set ca-cert "LDAPS-CA"
    set port 636
  next
end
```

3. Add the LDAP user to the user group:

```
config user group
  edit "Employees"
    append member "ldaps-server"
  next
end
```

Configuring FortiClient

1. To add the VPN connection, open FortiClient, go to **Remote Access** and click **Add a new connection**.
2. Set the **VPN** to **IPsec VPN** and **Remote Gateway** to the FortiGate IP address.

3. Set **Authentication Method** to **Pre-Shared Key** and enter the key below.

New VPN Connection

VPN SSL-VPN **IPsec VPN**

Connection Name

Description

Remote Gateway ✕
✚Add Remote Gateway

Authentication Method Pre-shared key ▼

Authentication (XAuth) ☒ Prompt on login ☐ Save login ☐ Disable

4. Expand **Advanced Settings > Phase 1** and in the **Local ID** field, enter **dialup1**.
5. Configure remaining settings as needed, then click **Save**.

Results

1. On FortiClient, select the VPN, enter the username and password, and select **Connect**.



The image shows the FortiClient VPN connection window. At the top, there is a graphic of a globe with a padlock icon and a laptop, connected by dotted lines. Below the graphic, there are three input fields: 'VPN Name' with a dropdown menu showing 'Office-VPN', 'Username' with the text 'jpearson', and 'Password' with masked characters '.....'. At the bottom, there is a blue 'Connect' button.

VPN Name Office-VPN ▼

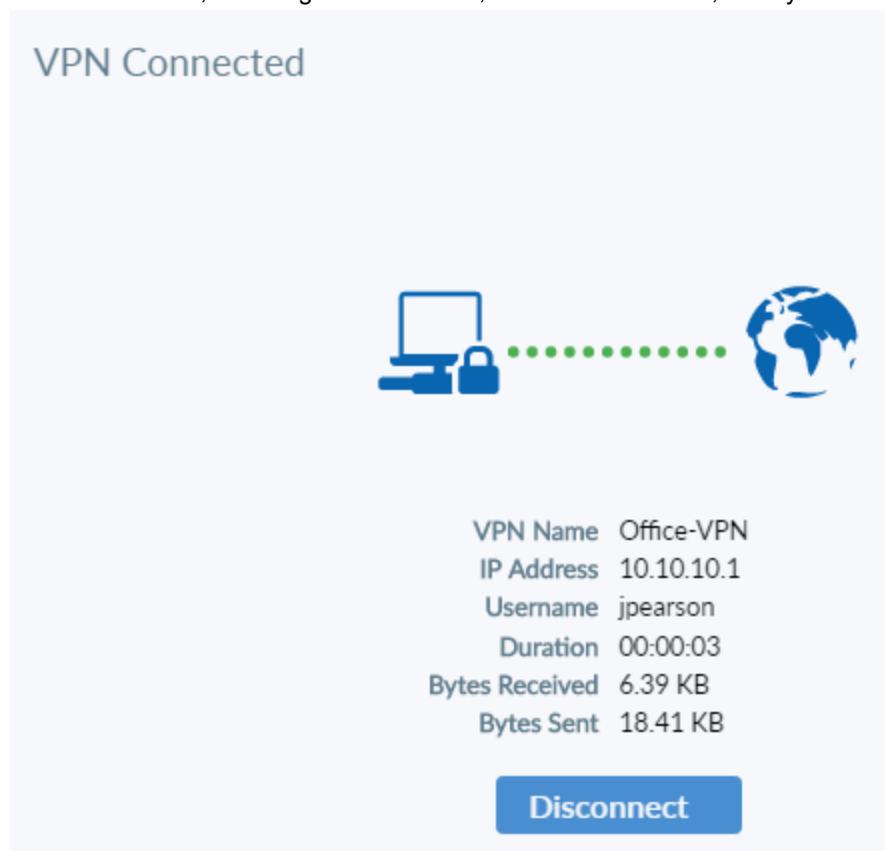
Username

Password



Connect

2. If 2FA is configured, a **Token** field will appear, prompting you for the FortiToken code. Enter the FortiToken code from your mobile device.

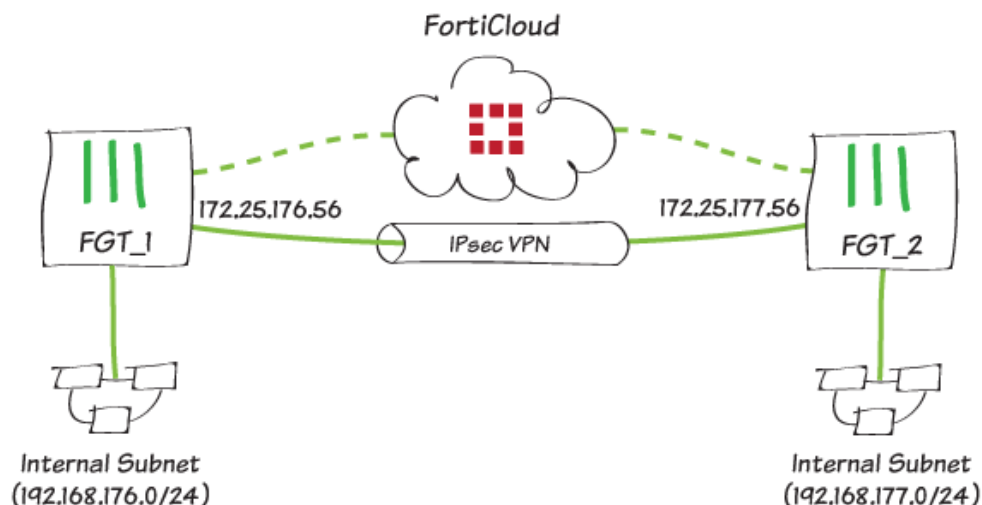
- Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



- On the FortiGate, go to **Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**.
- Under **Remote Gateway**, the monitor shows the FortiClient user's assigned gateway IP address.

| Name ▾ | Type ▾ | Remote Gateway ▾ |
|--|---|------------------|
|  FCT-VPN2_0 |  Dialup - FortiClient (Windows, Mac OS, Android) | 172.25.177.46 |

One-Click VPN (OCVPN)



In this recipe, you use the cloud-assisted OCVPN solution to greatly simplify the provisioning and configuration of IPsec VPN.

Note the following limitations:

- The FortiGate must be registered with a valid FortiCare Support license. You can verify the status of your FortiCare Support contract under **System > FortiGuard**.
- Only full-mesh VPN configurations using PSK cryptography are supported.
- Public IPs must be used (FortiGates behind NAT cannot participate).
- Non-root VDOMs and FortiGate VMs are not supported.
- Up to 16 nodes can be added to the OCVPN cloud, each with a maximum of 16 subnets.
- OCVPN with SD-WAN is not currently supported.


You can repeat the "Enabling OCVPN" section to add up to 16 nodes to the OCVPN cloud (barring the above limitations), but you will configure only two nodes in this example.

Enabling OCVPN


1. On FGT_1, go to **VPN > One-Click VPN Settings**.
2. Set **Status** to **Enabled** and confirm **Cloud Status**. This may take a minute or two.
3. As indicated, a green checkmark appears along with the message **Connected to the cloud service**.


4. Finally, add the required **Subnets** from FGT_1.

One-Click VPN Settings






FortiCare Support  Registered

Status  Enabled  Disabled

Cloud Status  Connected to the cloud service

Subnets


Cloud Members


| | | |
|---|--|--|
|  Refresh | <input type="text" value="Search"/> |  |
| Device Name  | Remote Gateway  | Subnets  |
| No results | | |


5. On FGT_2, repeat steps 1 to 4.
6. Enable and confirm connection to the cloud service, and then add the required subnets from FGT_2.

One-Click VPN Settings






FortiCare Support  Registered

Status  Enabled  Disabled

Cloud Status  Connected to the cloud service

Subnets



Cloud Members

| | | |
|---|--|--|
|  Refresh | <input type="text" value="Search"/> |  |
| Device Name  | Remote Gateway  | Subnets  |
| No results | | |


Confirming cloud membership

1. In the Cloud Members table on FGT_1, click **Refresh** and confirm the entries.
The remote gateway and corresponding subnets for each device should populate the list.

One-Click VPN Settings






FortiCare Support  Registered

Status  Enabled  Disabled

Cloud Status  Connected to the cloud service



Subnets


Cloud Members

| <div> Refresh</div> <div><input type="text" value="Search"/></div> <div></div> | | |
|--|--|---|
| Device Name  | Remote Gateway  | Subnets  |
| FGT_1 | 172.25.176.56 | 192.168.176.0/24 |
| FGT_2 | 172.25.177.56 | 192.168.177.0/24 |






2. You can perform step 1 on any FortiGate that is a member of the OCVPN cloud.
FGT_2 should return the same results as in step 1.

One-Click VPN Settings

FortiCare Support  RegisteredStatus  Enabled  DisabledCloud Status  Connected to the cloud serviceSubnets



Cloud Members













| <div>  Refresh </div> <div> <input type="text" value="Search"/>  </div> | | |
|---|--|---|
| Device Name  | Remote Gateway  | Subnets  |
| FGT_1 | 172.25.176.56 | 192.168.176.0/24 |
| FGT_2 | 172.25.177.56 | 192.168.177.0/24 |

Results













As the Cloud Members table populates, the OCVPN cloud updates each member automatically.

You can now verify that the remainder of the configuration has also been created, and proceed to test the tunnel.

- On either FortiGate, go to **VPN > IPsec Tunnels** and confirm the entry of a new tunnel with the prefix **_OCVPN**.

| <div>  Create New  Edit  Delete  Print Instructions </div> | | | | |
|--|---|--|--|--|
| Tunnel  | Interface Binding  | Template  | Status  | Ref.  |
| _OCVPN0-1 |  wan1 |  Custom |  Up | 4 |

- Go to **Network > Static Routes** and confirm the new static routes.

| <div>  Create New  Edit  Clone  Delete </div> | | | |
|---|---|---|---|
| Destination  | Gateway  | Interface  | Comment  |
| IPv4 (3) | | | |
| 0.0.0.0/0 | 172.25.176.1 |  wan1 | |
|  _OCVPN0-1_remote_networks | |  _OCVPN0-1 | Generated by OCVPN Cloud Servic... |
|  _OCVPN0-1_remote_networks | | Blackhole | Generated by OCVPN Cloud Servic... |

3. Go to **Policy & Objects > IPv4 Policy** and confirm the new policies.

| + Create New | | Edit | Delete | Policy Lookup | Search | Q | Interface Pair View | By Sequence |
|--------------|------------------------|------------------------|-----------|---------------------------|---------------------------|---|---------------------|-------------|
| ID | Name | From | To | Source | Destination | | | |
| 1 | internal-to-wan1 | internal | wan1 | all | all | | | |
| 2 | wifi-to-wan1 | TheLostJedi (FAP-221C) | wan1 | all | all | | | |
| 3 | _OCVPN0-1_internal_in | _OCVPN0-1 | internal | _OCVPN0-1_remote_networks | _OCVPN0-1_local_networks | | | |
| 4 | _OCVPN0-1_internal_out | internal | _OCVPN0-1 | _OCVPN0-1_local_networks | _OCVPN0-1_remote_networks | | | |
| 0 | Implicit Deny | any | any | all | all | | | |

4. Go to **Monitor > IPsec Monitor** and verify that the tunnel status is **Up**.

Refresh

Reset Statistics

Bring Up

Bring Down

FGT_1

| Name | Type | Remote Gateway | User Name | Status | Incoming Data | Outgoing Data | Phase 1 |
|-----------|--------|----------------|-----------|--------|---------------|---------------|-----------|
| _OCVPN0-1 | Custom | 172.25.177.56 | | Up | | | _OCVPN0-1 |

5. Go to **Log & Report > VPN Events** and view the tunnel statistics.

<

6. Using **Command Prompt/Terminal**, attempt a ping from one internal network to the other. Ping should be successful:

```
ping 192.168.177.99
```

```
Pinging 192.168.177.99 with 32 bytes of data:
```

```
Reply from 192.168.177.99: bytes=32 time=5ms TTL=254
```

```
Reply from 192.168.177.99: bytes=32 time=1ms TTL=254
```

```
Reply from 192.168.177.99: bytes=32 time<1ms TTL=254
```

```
Reply from 192.168.177.99: bytes=32 time<1ms TTL=254
```

```
Ping statistics for 192.168.177.99:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 5ms, Average = 1ms
```

7. Now, disable OCVPN (**VPN > One-Click VPN Settings**) and repeat the ping attempt to confirm that OCVPN was indeed responsible for the successful ping above:

```
ping 192.168.177.99
```

```
Pinging 192.168.177.99 with 32 bytes of data:  
Reply from 192.168.176.99: Destination net unreachable.  
Reply from 192.168.176.99: Destination net unreachable.  
Reply from 192.168.176.99: Destination net unreachable.  
Reply from 192.168.176.99: Destination net unreachable.  
  
Ping statistics for 192.168.177.99:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

8. Re-enable OCVPN.

Troubleshooting

The following diagnose commands can be useful.

To verify OCVPN status, use the following command:

```
FGT_1 # diag vpn ocvpn status  
Current State : registered  
OCVPN Status : OK (200)
```

To view device states, use the following command:

```
FGT_1 # diag vpn ocvpn device-state  
FGT_1 wan1 172.25.176.56 0 6 0 2 200 2 0x3 0x3
```



The log report example is truncated.

To print a log report, use the following command:

```

FGT_1 # diag vpn ocvpn log
OCVPN Polling: state = undefined
cvpn_save_state: FGT_1 <null> 0.0.0.0 -1 0 0 0 0 0 0x0 0x0
OCVPN Polling: state = undefined
cvpn_save_state: FGT_1 <null> 0.0.0.0 -1 0 0 0 0 0 0x0 0x0
OCVPN Polling: state = undefined
cvpn_save_state: FGT_1 <null> 0.0.0.0 -1 0 0 0 0 0 0x0 0x0

=====

Thurs Mar 29 09:00:00 2018

=====

cvpn_load_state: FGT_1 <null> 0.0.0.0 -1 0 0 0 0 0 0x0 0x0
OCVPN Register: sn=x, num_subnets=0
Current State: undefined -> registering
cvpn_save_state: FGT_1 <null> 0.0.0.0 -1 2 0 0 0 0 0x0 0x0
WAN intf wan1, IP 172.25.176.56/255.255.255.0
WAN intf changed from <null> to wan1
WAN IP changed from 0.0.0.0 to 172.25.176.56

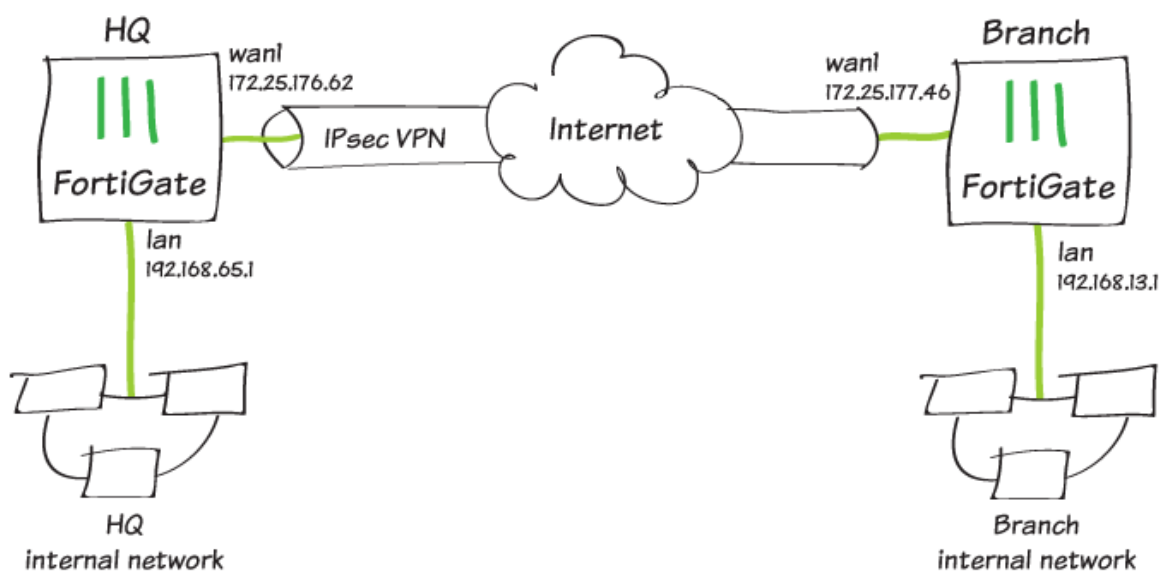
Local Subnets:
192.168.176.0/255.255.255.0
JSON Update request = '{ "SN": "x", "IPv4": "172.25.176.56",
Sending OCVPN request: method=Update, data='{ "SN": "x", "IPv
Received OCVPN response: method=Update, res=0, http_resp=200
JSON Response: '{"key":"","rev":1,"members":[{"IPv4":"172.25.
Member table size = 1
Member: { "IPv4": "172.25.176.56", "port": "500", "slot": 0,
Subnet 192.168.176.0/255.255.255.0
cvpn_config_install: prev mask 0x1, new mask 0x1
Update response code = 200
Current State: updating -> registered
cvpn_save_state: FGT_1 wan1 172.25.176.56 0 6 0 1 200 1 0x1 0
JSON Response: '{"key":"8TVdIwG2xS400jMOxyNN9WK0YWZEsaJDIV8JU
"rev":1,"members":[{"IPv4":"172.25.176.56","port":"500","slot
Member table size = 1
Member: { "IPv4": "172.25.176.56", "port": "500", "slot": 0,
Subnet 192.168.176.0/255.255.255.0
cvpn_config_install: prev mask 0x0, new mask 0x1
New members table, revision = 1
Register response code = 200
Current State: registering -> registered
cvpn_save_state: FGT_1 wan1 172.25.176.56 0 6 0 1 200 1 0x1 0
Current State: registered -> acknowledging

```

To view a list of OCVPN cloud members, use the following command:


```
FGT_1 # diag vpn ocvpn print-members
Member: { "IPv4": "172.25.176.56", "port": "500", "slot": 0,
Member: { "IPv4": "172.25.177.56", "port": "500", "slot": 1,
```

Site-to-site IPsec VPN with two FortiGate devices



In this recipe, you create a site-to-site IPsec VPN tunnel to allow communication between two networks that are located behind different FortiGate devices. You use the VPN Wizard's **Site to Site – FortiGate** template to create the VPN tunnel on both FortiGate devices.

In this example, one FortiGate is called HQ and the other is called Branch.

Configuring IPsec VPN on HQ

1. To create a new IPsec VPN tunnel, connect to HQ, go to **VPN > IPsec Wizard**, and create a new tunnel.
2. In the **VPN Setup** step, set **Template Type** to **Site to Site**, set **Remote Device Type** to **FortiGate**, and set **NAT Configuration** to **No NAT between sites**.

1 VPN Setup > 2 Authentication > 3 Policy & Routing

Name

Template Type **Site to Site** Remote Access Custom

Remote Device Type **FortiGate**
Cisco


NAT Configuration **No NAT between sites**
This site is behind NAT
The remote site is behind NAT

3. In the **Authentication** step, set **IP Address** to the public IP address of the Branch FortiGate (in the example, 172.25.177.46).
4. After you enter the IP address, the wizard automatically assigns an interface as the **Outgoing Interface**. If you want to use a different interface, select it from the drop-down menu.
5. Set a secure **Pre-shared Key**.

✓ VPN Setup > 2 Authentication > 3 Policy & Routing

Remote Device **IP Address** Dynamic DNS

IP Address


Outgoing Interface  wan1 ▼
Detected via routing lookup

Authentication Method **Pre-shared Key** Signature

Pre-shared Key

6. In the **Policy & Routing** step, set **Local Interface** to **lan**. The wizard adds the local subnet automatically. Set **Remote Subnets** to the Branch network's subnet (in the example, 192.168.13.0/24).
7. Set **Internet Access** to **None**.

✓ VPN Setup > ✓ Authentication > 3 Policy & Routing

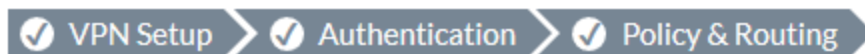
Local Interface  lan ▼

Local Subnets

Remote Subnets

Internet Access **None** Share WAN Force to use remote WAN

8. A summary page shows the configuration created by the wizard, including interfaces, firewall addresses, routes, and policies.



✓ The VPN has been set up

Summary of Created Objects

| | |
|------------------------|---------------------|
| Phase 1 Interface | HQ-to-Branch |
| Local Address Group | HQ-to-Branch_local |
| Remote Address Group | HQ-to-Branch_remote |
| Phase 2 Interface | HQ-to-Branch |
| Static Route | 2 |
| Blackhole Route | 3 |
| Local to Remote Policy | 7 |
| Remote to Local Policy | 8 |

9. To view the VPN interface created by the wizard, go to **Network > Interfaces**.

| Status | Name | IP/Netmask | Ref. |
|--------|--------------|-----------------------------|------|
| | wan1 | 172.25.176.62 255.255.255.0 | 10 |
| | HQ-to-Branch | 0.0.0.0 0.0.0.0 | 4 |

10. To view the firewall addresses created by the wizard, go to **Policy & Objects > Addresses**.

| Name | Type | Details | Interface | Visibility | Ref. |
|-----------------------|--------|-----------------|-----------|------------|------|
| Address 13 | | | | | |
| FIREWALL_AUTH_... | Subnet | 0.0.0.0/0 | | Hidden | 0 |
| HQ-to-Branch_local... | Subnet | 192.168.65.0/24 | | Visible | 1 |
| HQ-to-Branch_rem... | Subnet | 192.168.13.0/24 | | Visible | 1 |

11. To view the routes created by the wizard, go to **Network > Static Routes**.

| Destination | Gateway | Interface | Comment |
|---------------------|--------------|--------------|------------------------------------|
| 0.0.0.0/0 | 172.25.176.1 | wan1 | |
| HQ-to-Branch_remote | | HQ-to-Branch | VPN: HQ-to-Branch (Created by V... |
| HQ-to-Branch remote | | Blackhole | VPN: HQ-to-Branch (Created by V... |

12. To view the policies created by the wizard, go to **Policy & Objects > IPv4 Policy**.

| Name | From | To | Source | Destination |
|-------------------------|--------------|--------------|---------------------|---------------------|
| Internet | lan | wan1 | all | all |
| vpn_HQ-to-Branch_local | lan | HQ-to-Branch | HQ-to-Branch_local | HQ-to-Branch_remote |
| vpn_HQ-to-Branch_remote | HQ-to-Branch | lan | HQ-to-Branch_remote | HQ-to-Branch_local |

Configuring IPsec VPN on Branch

1. To create a new IPsec VPN tunnel, connect to Branch, go to **VPN > IPsec Wizard**, and create a new tunnel.
2. In the **VPN Setup** step, set **Template Type** to **Site to Site**, set **Remote Device Type** to **FortiGate**, and set **NAT Configuration** to **No NAT between sites**.

1 VPN Setup > 2 Authentication > 3 Policy & Routing

| | |
|--------------------|--|
| Name | Branch-to-HQ |
| Template Type | Site to Site Remote Access Custom |
| Remote Device Type | FortiGate Cisco |
| NAT Configuration | No NAT between sites This site is behind NAT The remote site is behind NAT |

3. In the **Authentication** step, set **IP Address** to the public IP address of the HQ FortiGate (in the example, 172.25.176.62).
4. After you enter the IP address, the wizard automatically assigns an interface as the **Outgoing Interface**. If you want to use a different interface, select it from the drop-down menu.
5. Set the secure **Pre-shared Key** that was used for the VPN on HQ.

1 VPN Setup > 2 Authentication > 3 Policy & Routing

| | |
|-----------------------|---|
| Remote Device | IP Address Dynamic DNS |
| IP Address | 172.25.176.62 |
| Outgoing Interface | wan1 |
| Authentication Method | Detected via routing lookup Pre-shared Key Signature |
| Pre-shared Key | ●●●●●●●● |

6. In the **Policy & Routing** step, set **Local Interface** to **lan**. The wizard adds the local subnet automatically. Set **Remote Subnets** to the HQ network's subnet (in the example, 192.168.65.0/24).

7. Set **Internet Access** to **None**.

VPN Setup > Authentication > **3 Policy & Routing**

Local Interface: LAN-A (lan)

Local Subnets: 192.168.13.0/24

Remote Subnets: 192.168.65.0/24

Internet Access: **None** | Share WAN | Force to use remote WAN

8. A summary page shows the configuration created by the wizard, including interfaces, firewall addresses, routes, and policies.

VPN Setup > Authentication > **Policy & Routing**

✓ The VPN has been set up

Summary of Created Objects

| | |
|------------------------|---------------------|
| Phase 1 Interface | Branch-to-HQ |
| Local Address Group | Branch-to-HQ_local |
| Remote Address Group | Branch-to-HQ_remote |
| Phase 2 Interface | Branch-to-HQ |
| Static Route | 2 |
| Blackhole Route | 3 |
| Local to Remote Policy | 2 |
| Remote to Local Policy | 3 |

9. To bring the VPN tunnel up, go to **Monitor > IPsec Monitor**. Right-click under **Status** and select **Bring Up**.

| Name | Type | Remote Gateway | User Name | Status | Incoming Data |
|--------------|--------------------------|----------------|-----------|--------|---------------|
| HQ-to-Branch | Site to Site - FortiGate | 172.25.177.46 | | Down | |

Reset Statistics
Bring Up
Bring Down

Results

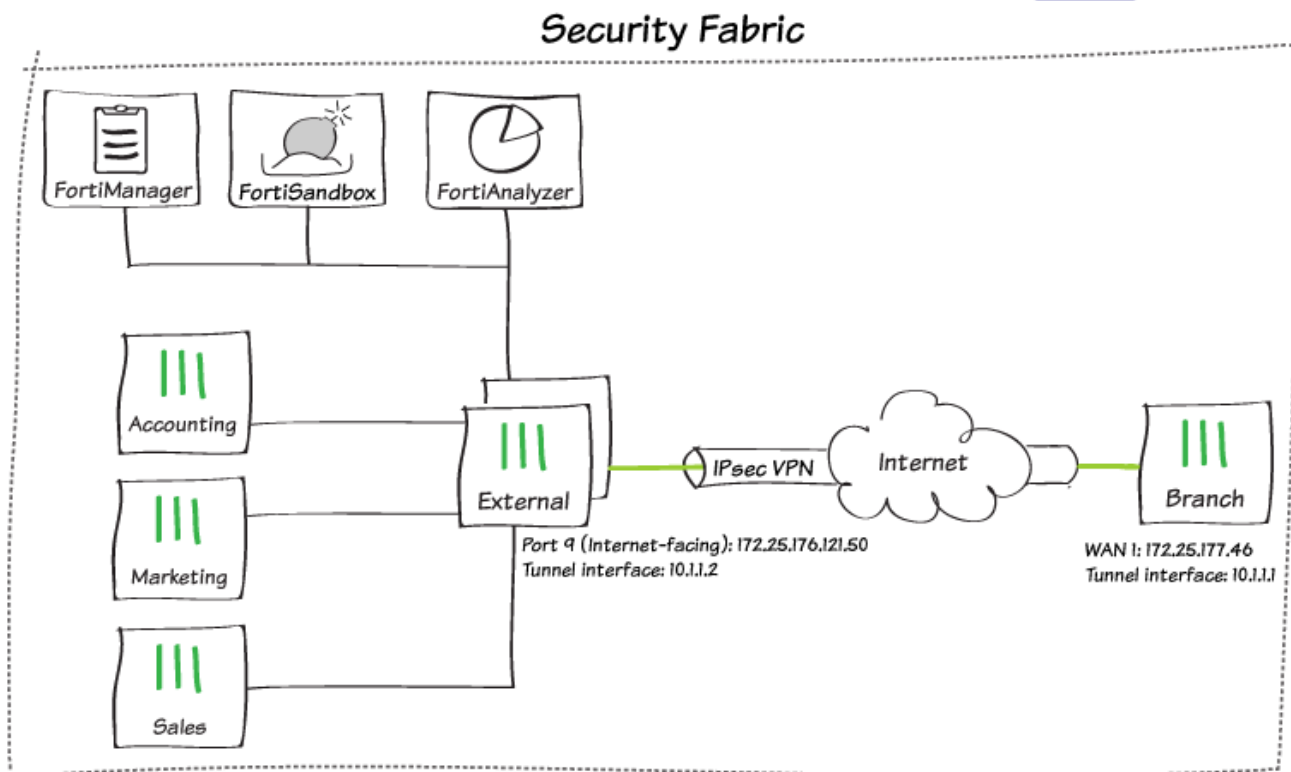
Users on the HQ internal network can access resources on the Branch internal network and vice versa.

To test the connection, ping HQ's LAN interface from a device on the Branch internal network.

```
Pinging 192.168.65.1 with 32 bytes of data:
Reply from 192.168.65.1: bytes=32 time=1ms TTL=254
Reply from 192.168.65.1: bytes=32 time=1ms TTL=254
Reply from 192.168.65.1: bytes=32 time<1ms TTL=254
Reply from 192.168.65.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.65.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fortinet Security Fabric over IPsec VPN



In this recipe, you add FortiTelemetry traffic to an existing IPsec VPN site-to-site tunnel between two FortiGate devices, in order to add a remote FortiGate to the Security Fabric. You also allow the remote FortiGate to access the FortiAnalyzer for logging.

If you do not already have a site-to-site VPN created, see [Site-to-site IPsec VPN with two FortiGate devices on page 301](#)






In this example, an HA cluster called Edge is the root FortiGate in the Security Fabric and a FortiGate called Branch is the remote FortiGate.

Configuring tunnel interfaces

1. To configure Edge to listen for FortiTelemetry traffic over the VPN, connect to Edge, go to **Network > Interfaces**, and edit the tunnel interface.
2. Set **IP** to the local IP address for this interface (10.10.10.1) and **Remote IP/Network mask** to the IP address for the Branch tunnel interface (10.10.10.2/32).
3. Under **Administrative Access**, enable **FortiTelemetry**.

| | |
|----------------|----------------------|
| Interface Name | Edge-to-Branch |
| Alias | <input type="text"/> |
| Type | Tunnel Interface |
| Interface | port9 |

Tags

| | |
|---|--|
| Role  | Undefined |
| Department  | <div>Admin </div> <div></div> <div> Add Tag Category</div> |

Address

| | |
|------------------------|--|
| Addressing mode | Manual |
| IP | <input type="text" value="10.10.10.1"/> |
| Remote IP/Network Mask | <input type="text" value="10.10.10.2/32"/> |

Administrative Access

| | | | | |
|------|--|---|-------------------------------|-------------------------------------|
| IPv4 | <input type="checkbox"/> HTTPS | <input type="checkbox"/> HTTP  | <input type="checkbox"/> PING | <input type="checkbox"/> FMG-Access |
| | <input type="checkbox"/> CAPWAP | <input type="checkbox"/> SSH | <input type="checkbox"/> SNMP | <input type="checkbox"/> FTM |
| | <input type="checkbox"/> RADIUS Accounting | <input checked="" type="checkbox"/> FortiTelemetry | | |

4. Connect to Branch, go to **Network > Interfaces**, and edit the tunnel interface.
5. Set **IP** to the local IP address for this interface (10.10.10.2) and **Remote IP/Network mask** to the IP address for the

Edge tunnel interface (10.10.10.1/32).


Interface Name Edge-to-Branch

Alias

Type Tunnel Interface

Interface wan1

Tags

Role 

Undefined

 Add Tag Category

Address

Addressing mode Manual

IP

10.10.10.2

Remote IP/Network Mask

10.10.10.1/32

Adding tunnel interfaces to the VPN

1. To create an address for the Edge tunnel interface, connect to Edge, go to **Policy & Objects > Addresses**, and create a new address.
2. Set **Category** to **Address** and set **Subnet/IP Range** to the IP address for the Edge tunnel interface (10.10.10.1/32).

Category

Address Multicast Address

Name

Edge-tunnel-interface

Color



Change

Type

Subnet

Subnet / IP Range

10.10.10.1/32

Interface

☐ any

Show in Address List




Static Route Configuration



Comments

0/255

3. Create a second address for the Branch tunnel interface. For this address, enable **Static Route Configuration**.

| | |
|----------------------------|---|
| Category | Address Multicast Address |
| Name | Branch-tunnel-interface |
| Color |  <input type="button" value="Change"/> |
| Type | Subnet ▼ |
| Subnet / IP Range | 10.10.10.2/32 |
| Interface | <input type="checkbox"/> any ▼ |
| Show in Address List | <input checked="" type="checkbox"/> |
| Static Route Configuration | <input checked="" type="checkbox"/> |
| Comments | <input type="text"/> 0/255 |

4. To allow VPN traffic between the Edge tunnel interface and the Branch tunnel interface, go to **VPN > IPsec Tunnels**, and edit the VPN tunnel. Select **Convert To Custom Tunnel**.
5. Under **Phase 2 Selectors**, create a new Phase 2. Set **Local Address** to use a **Named Address** and select the address for the Edge tunnel interface. Set **Remote Address** to use a **Named Address**, and select the address for the Branch tunnel interface.

| Phase 2 Selectors | | |
|---|------------------------------|---|
| Name | Local Address | Remote Address |
| Edge-tunnel-to-Branch-tunnel | Edge-to-Branch_local | Edge-to-Branch_remote  |
| <div> <div>New Phase 2</div> <div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div> </div> | | |
| Name | Edge-tunnel-to-Branch-tunnel | |
| Comments | <input type="text"/> | |
| Local Address | Named Addr ▼ | Edge-tunnel-interfac ▼ |
| Remote Address | Named Addr ▼ | Branch-tunnel-interf ▼ |
|  Advanced... | | |

6. To route traffic to the Branch tunnel interface, go to **Network > Static Routes**, and create a new route.
7. Set **Destination** to **Named Address**, and select the address for the Branch tunnel interface. Set **Device** to the tunnel interface.

| | |
|-------------------------|--|
| Destination | <div>Subnet Named Address Internet Service</div> <div>Branch-tunnel-interface</div> |
| Interface | Edge-to-Branch |
| Administrative Distance | 10 |
| Comments | <div></div> 0/255 |
| Status | <div>Enabled</div> <div>Disabled</div> |

- To allow traffic between the tunnel interfaces, go to **Policy & Objects > IPv4 Policy** and edit the policy allowing local VPN traffic.
- Set **Source** to include the Edge tunnel interface and **Destination** to include the Branch tunnel interface. To configure this, you must have Multiple Interface Policies enabled. If you have not done this already, go to **System > Feature Visibility**.

| | | |
|--------------------|--|--|
| Name | vpn_Edge-to-Branch_local | |
| Incoming Interface | <div>LAN (port1)</div> <div>+</div> | |
| Outgoing Interface | <div>Edge-to-Branch</div> <div>+</div> | |
| Source | <div>Edge-tunnel-interface</div> <div>Edge-to-Branch_local</div> <div>+</div> | |
| Destination | <div>Branch-tunnel-interface</div> <div>Edge-to-Branch_remote</div> <div>+</div> | |
| Schedule | always | |
| Service | ALL | |
| Action | <div>ACCEPT</div> <div>DENY</div> <div>LEARN</div> | |

10. Edit the policy allowing remote VPN traffic to include the tunnel interfaces.

| | | |
|--------------------|---|--------|
| Name | vpn_Edge-to-Branch_remote | |
| Incoming Interface | Edge-to-Branch | X |
| Outgoing Interface | LAN (port1) | X |
| Source | Branch-tunnel-interface Edge-to-Branch_remote | X X |
| Destination | Edge-tunnel-interface Edge-to-Branch_local | X X |
| Schedule | always | |
| Service | ALL | X |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN | |

11. On Branch, repeat steps 1 to 10 to include the following:
- Addresses for both tunnel interfaces (enable **Static Route Configuration** for the Edge tunnel interface address)
 - A Phase 2 that allows traffic between the Branch tunnel interface and the Edge tunnel interface
 - A static route to the Edge tunnel interface
 - Edited policies that allow traffic to flow between the tunnel interfaces
12. To allow the new phase 2 to take effect, go to **Monitor > IPsec Monitor**, and restart the VPN tunnel.

Authorizing Branch for the Security Fabric

1. You can authorize a FortiGate, FortiAP, or FortiSwitch to join the Security Fabric by using the device's serial number, rather than sharing the password for the Security Fabric (the **Group password** option is not available FortiOS 6.0.3 and later). To authorize Branch, connect to Edge, and enter the following CLI command:

```
config system csf
  config trusted-list
    edit <serial_number>
  end
end
```

2. To add Branch to the Security Fabric, connect to Branch, and go to **Security Fabric > Settings**.
3. Enable **FortiGate Telemetry**. Set the **Group name**. Leave **Group password** blank (the **Group password** option is not available in FortiOS 6.0.3 and later). Enable **Connect to upstream FortiGate**. Set **FortiGate IP** to the IP

address of the Edge tunnel interface.

☒ FortiGate Telemetry

Group name

Office-Security-Fabric

Group password ⓘ

Connect to upstream FortiGate ☒

FortiGate IP

10.10.10.1

Management IP ⓘ

Use WAN IP

Specify

4. To verify that Branch is now part of the Security Fabric, connect to Edge, and go to **Security Fabric > Settings**. Branch appears in the **Topology**.

☒ FortiGate Telemetry

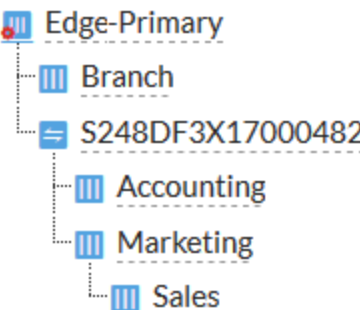
Group name

Office-Security-Fabric

Group password


●●●●●●●●

Topology



Allowing Branch to access the FortiAnalyzer




1. To create an address for the FortiAnalyzer, connect to Branch, go to **Policy & Objects > Addresses**, and create a new address. Enable **Static Route Configuration**.

| | |
|----------------------------|---|
| Name | FortiAnalyzer |
| Color |  <input type="button" value="Change"/> |
| Type | Subnet ▼ |
| Subnet / IP Range | 192.168.65.10 |
| Interface | <input type="checkbox"/> any ▼ |
| Show in Address List | <input checked="" type="checkbox"/> |
| Static Route Configuration | <input checked="" type="checkbox"/> |
| Comments | <input type="text"/> 0/255 |

- To allow VPN traffic between the FortiAnalyzer and the Branch tunnel interface, go to **VPN > IPsec Tunnels**, and create a new Phase 2.

| | | |
|--------------------|---|--|
| New Phase 2 | | <input checked="" type="checkbox"/> <input type="button" value="Refresh"/> |
| Name | Branch-to-FortiAnalyzer | |
| Comments | <input type="text"/> | |
| Local Address | <input type="button" value="Named Addr"/> ▼ | <input type="button" value="Branch-tunnel-interf"/> ▼ |
| Remote Address | <input type="button" value="Named Addr"/> ▼ | <input type="button" value="FortiAnalyzer"/> ▼ |

- To route traffic to the FortiAnalyzer, go to **Network > Static Routes**, and create a new route.

| | |
|---|---|
| Destination | <input type="button" value="Subnet"/> <input checked="" type="button" value="Named Address"/> <input type="button" value="Internet Service"/> |
| |  FortiAnalyzer ▼ |
| Interface |  Edge-to-Branch ▼ |
| Administrative Distance  | 10 |
| Comments | <input type="text"/> 0/255 |
| Status | <input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/> |

- On Edge, repeat this step to create an address for FortiAnalyzer and a new Phase 2 that allows traffic between the FortiAnalyzer and the Branch tunnel interface. Edge doesn't require a new static route.
- To allow traffic between Branch and the FortiAnalyzer, go to **Policy & Objects > IPv4 Policy**, and create a new policy.
- Set **Incoming Interface** to the VPN interface, and set **Outgoing Interface** to the interface that connects to the FortiAnalyzer (in the example, **port16**). Set **Source** to the Branch tunnel interface, and set **Destination** to the FortiAnalyzer.

7. Enable **NAT** for this policy.

| | | |
|--------------------|---|---|
| Name ⓘ | Branch-access-FortiAnalyzer | |
| Incoming Interface | Edge-to-Branch | × |
| | + | |
| Outgoing Interface | Network-Resources (port16) | × |
| | + | |
| Source | Branch-tunnel-interface | × |
| | + | |
| Destination | FortiAnalyzer | × |
| | + | |
| Schedule | always ▼ | |
| Service | ALL | × |
| | + | |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN | |

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

8. To authorize the Branch FortiGate on the FortiAnalyzer, connect to the FortiAnalyzer, and go to **Device Manager > Unregistered**.
9. Select Branch, then select **+Add** to register Branch.

Add Device

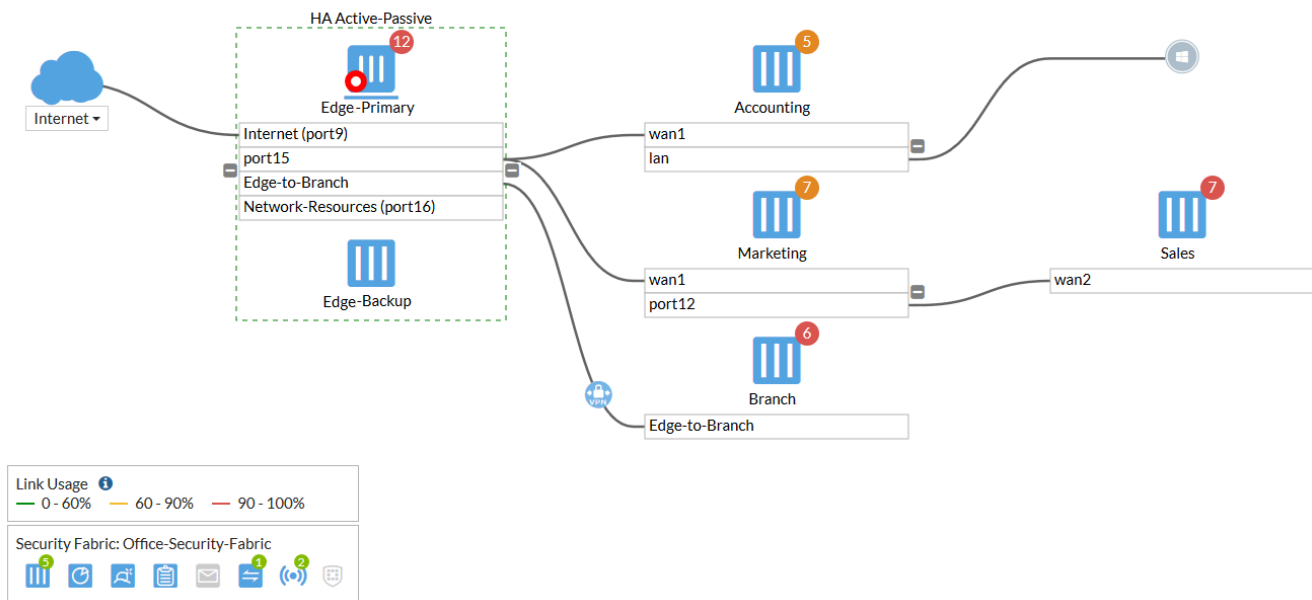
| Device Name | Assign New Device Name |
|------------------|------------------------|
| FG101E4Q17000263 | Branch |

10. Branch now appears as **Registered**.

| <input type="checkbox"/> | ▲ Device Name | IP Address | Platform | Logs |
|--------------------------|--------------------------|--------------|--------------------|-------------|
| <input type="checkbox"/> | Branch | 192.168.65.2 | FortiGate-101E | ● Real Time |
| <input type="checkbox"/> | ✖ Office-Security-Fabric | | | |
| <input type="checkbox"/> | Accounting | 192.168.65.2 | FortiGate-140E-POE | ● Real Time |
| <input type="checkbox"/> | Edge* | 192.168.65.2 | FortiGate-600D | ● Real Time |
| <input type="checkbox"/> | Marketing | 192.168.65.2 | FortiGate-81E-POE | ● Real Time |
| <input type="checkbox"/> | Sales | 192.168.65.2 | FortiGate-51E | ● Real Time |

Results

To view Branch as part of the Security Fabric topology, connect to Edge and go to **Security Fabric > Logical Topology**. Branch is shown as part of the Security Fabric, connecting over the IPsec VPN tunnel.



Desynchronizing settings for Branch (optional)

1. If you don't want Branch to automatically use the settings that Edge pushes for the FortiAnalyzer, FortiSandbox, and FortiManager, use the following CLI command to configure these settings locally:

```
config system csf
  set configuration-sync local
end
```

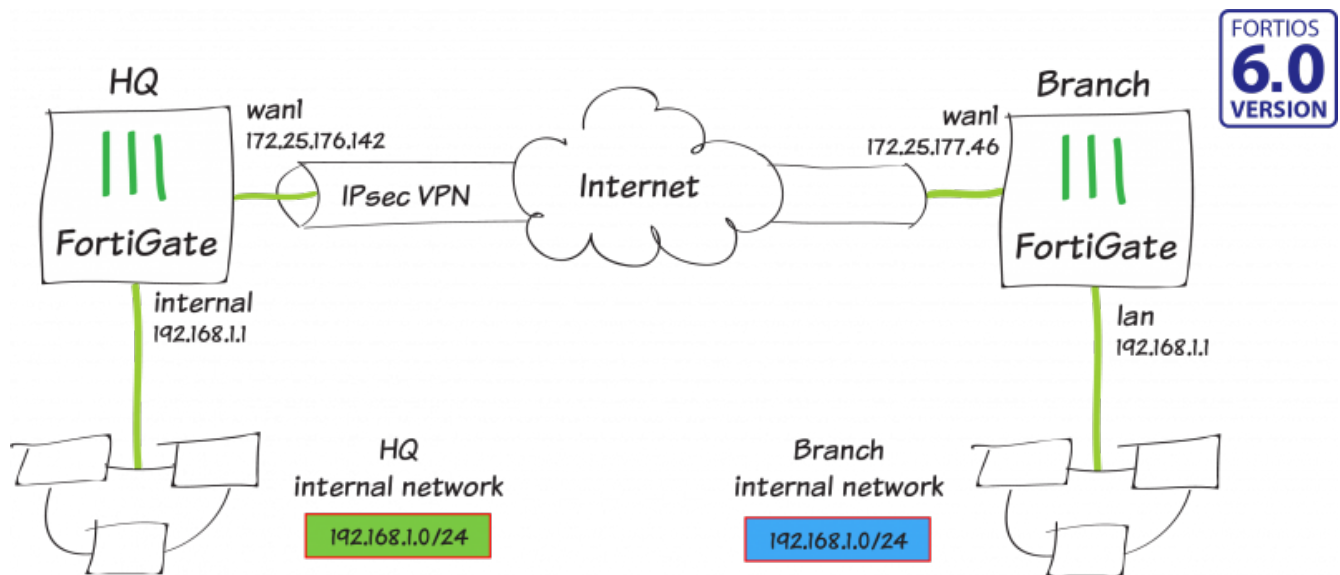
2. Go to **Security Fabric > Settings**. You can now configure the settings for **FortiAnalyzer logging, Central**

Management, and **Sandbox Inspection**. You can also choose to use local logging rather than sending logs to a FortiAnalyzer.



This option is available for all FortiGate devices in the Security Fabric, except for the root FortiGate.

Site-to-site IPsec VPN with overlapping subnets



In this recipe, you create a route-based IPsec VPN tunnel, as well as configure both source and destination NAT, to allow transparent communication between two overlapping networks that are located behind different FortiGates.

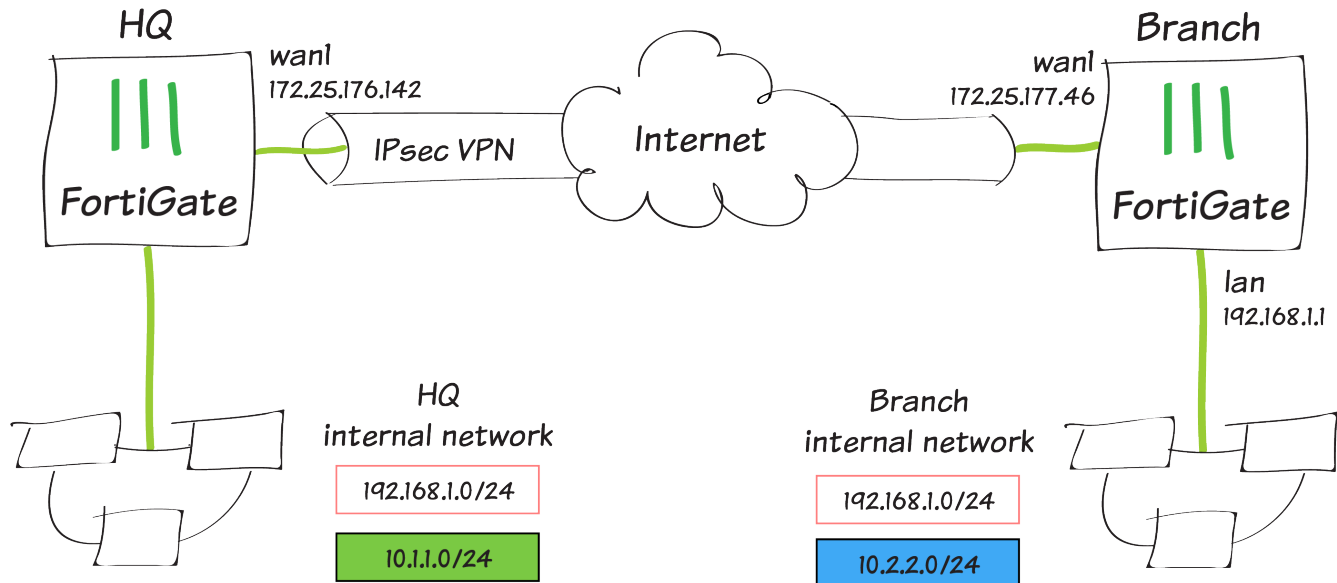
In this example, one FortiGate will be referred to as HQ and the other as Branch. They both have 192.168.1.0/24 in use as their internal network (LAN), but both LANs need to be able to communicate to each other through the IPsec tunnel.

Planning the new addressing scheme

In order for overlapping subnets to be able to communicate over a route-based IPsec tunnel, new virtual subnets of equal size must be decided upon and used for all communication between the two overlapping subnets.



Devices on both local networks DO NOT need their IP addresses changed. However, the devices/users will need to be sure to use the new subnet range of the remote network when communicating across the tunnel.



In this example, you perform a one-to-one mapping of HQ's 192.168.1.0/24 network to 10.1.1.0/24, and Branch's 192.168.1.0/24 network to 10.2.2.0/24. This will allow HQ clients to use Branch's new subnet to communicate to Branch clients, and vice-versa.

Configuring the IPsec VPN on HQ

1. To create the tunnel on HQ, connect to HQ and go to **VPN > IPsec Tunnels**.
2. In the **VPN Setup** step, set **Template Type** to **Custom** and enter VPN-to-Branch for the **Name**.


1 VPN Setup

| | |
|---------------|--|
| Name | VPN-to-Branch |
| Template Type | <input type="radio"/> Site to Site <input type="radio"/> Remote Access <input checked="" type="radio"/> Custom |





3. Enter Branch's public IP address (in the example, 172.25.177.46) for the **IP Address**, and select HQ's WAN interface for **Interface** (in the example, wan1).

| | |
|----------------|--|
| Network | |
| IP Version | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| Remote Gateway | Static IP Address |
| IP Address | 172.25.177.46 |
| Interface | <input checked="" type="radio"/> wan1 |

4. Enter a secure key for the **Pre-shared Key**. Later, you will enter the same key in the "Configuring the IPsec VPN on Branch" section.

| | |
|-----------------------|--|
| Authentication | |
| Method | Pre-shared Key ▼ |
| Pre-shared Key | ••••••••  |

5. Type the new address ranges selected in the "Planning the new addressing scheme" section for HQ and Branch's LAN in the **Local Address** and **Remote Address** fields (in the example, 10.1.1.0/24 and 10.2.2.0/24, respectively).



| | | |
|--|----------------------|---|
| Phase 2 Selectors | | |
| Name | Local Address | Remote Address |
| VPN-to-Branch | 10.1.1.0/24 | 10.2.2.0/24  |
| New Phase 2   | | |
| Name | VPN-to-Branch | |
| Comments | Comments | |
| Local Address | Subnet ▼ | 10.1.1.0/24 |
| Remote Address | Subnet ▼ | 10.2.2.0/24 |
|  Advanced... | | |

6. Optionally, expand **Advanced** and enable **Auto-negotiate**.

| | |
|--------------------|-------------------------------------|
| Auto-negotiate | <input checked="" type="checkbox"/> |
| Autokey Keep Alive | <input checked="" type="checkbox"/> |


Configuring static routes on HQ

- To create the necessary routes on HQ, go to **Network > Static Routes** and select **Create New**.
- Enter the new subnet created in the "Planning the new addressing scheme" section for Branch's LAN in the **Destination** field, and select the VPN tunnel created in the "Configuring the IPsec VPN on HQ" section as the **Interface** (in the example, this is 10.2.2.0/24 and VPN-to-Branch).

| | |
|---|---|
| Destination | Subnet Named Address Internet Service |
| | 10.2.2.0/24 |
| Interface |  VPN-to-Branch ▼ |
| Administrative Distance  | 10 |



- Create an additional route with the same **Destination** as the previous route, but this time change the **Administrative Distance** to 200 and select **Blackhole** as the **Interface**. This is the best practice for route-based IPsec VPN tunnels, as it ensures traffic for the remote FortiGate's subnet is not sent using the default route in the

event that the IPsec tunnel goes down.



| Destination | Subnet | Named Address | Internet Service |
|---|---------------------------------|---------------|------------------|
| | 10.2.2.0/24 | | |
| Interface | <input type="radio"/> Blackhole | | |
| Administrative Distance  | 200 | | |

Configuring address objects on HQ

1. To create address objects you will utilize in a later step, navigate to **Policy & Objects > Addresses** and select **Create New > Address**.
2. Enter *HQ-original* for the **Name**, the original LAN subnet of HQ for **Subnet** (in the example, 192.168.1.0/24), and select the LAN-side interface for **Interface** (in the example, internal).

| | |
|-------------------|---|
| Name | HQ-original |
| Color |  Change |
| Type | Subnet |
| Subnet / IP Range | 192.168.1.0/24 |
| Interface |  internal |


3. Repeat the process to create an additional new address object.
4. Enter *Branch-new* for the **Name**, the new LAN subnet of Branch for **Subnet** (in the example, 10.2.2.0/24), and select the VPN interface for **Interface** (in the example, VPN-to-Branch).

| | |
|-------------------|---|
| Name | Branch-new |
| Color |  Change |
| Type | Subnet |
| Subnet / IP Range | 10.2.2.0/24 |
| Interface |  VPN-to-Branch |

5. To create an IP Pool, navigate to **Policy & Objects > IP Pools** and select **Create New**.
6. Enter *HQ-new* for the **Name** and select **Fixed Port Range** for **Type**. For the **External IP Range** enter the new subnet for HQ (in the example, 10.1.1.1 – 10.1.1.254). You do not need to include the network address or the broadcast address for the subnet in the External IP Range of the IP Pool. For the **Internal IP Range**, enter the original subnet for HQ (in the example, 192.168.1.1 – 192.168.1.254).

| | | | |
|-------------------|--|---|---|
| Name | <input type="text" value="HQ-new"/> | | |
| Comments | <input type="text"/> 0/255 | | |
| Type | <input type="button" value="Overload"/> <input type="button" value="One-to-One"/> <input type="button" value="Fixed Port Range"/> <input type="button" value="Port Block Allocation"/> | | |
| External IP Range | <input type="text" value="10.1.1.1"/> | - | <input type="text" value="10.1.1.254"/> |
| Internal IP Range | <input type="text" value="192.168.1.1"/> - <input type="text" value="192.168.1.254"/> | | |
| ARP Reply | <input checked="" type="checkbox"/> | | |













- Finally, to create a Virtual IP, navigate to **Policy & Objects > Virtual IPs** and select **Create New > Virtual IP**.
- Enter *HQ-new-to-original* for the **Name** and select the VPN interface for **Interface** (in the example, VPN-to-Branch). For the **External IP Address/Range** enter the new subnet for HQ (in the example, 10.1.1.1 – 10.1.1.254). You do not need to include the network address or the broadcast address for the subnet in the External IP Range of the Virtual IP. For the **Mapped IP Address/Range**, enter the original subnet (in the example, 192.168.1.1 – 192.168.1.254).

| | |
|----------|---|
| Name | <input type="text" value="HQ-new-to-original"/> |
| Comments | <input type="text"/> 0/255 |
| Color |  <input type="button" value="Change"/> |

| | |
|---------------------------|---|
| Network | |
| Interface | <input type="button" value="VPN-to-Branch"/> |
| Type | Static NAT |
| External IP Address/Range | <input type="text" value="10.1.1.1"/> - <input type="text" value="10.1.1.254"/> |
| Mapped IP Address/Range | <input type="text" value="192.168.1.1"/> - <input type="text" value="192.168.1.254"/> |


Configuring firewall policies on HQ

- To create firewall policies on HQ, go to **Policy & Objects > IPv4 Policies** and select **Create New**.
- Enter *From-HQ-to-Branch* for the **Name**, the LAN-side interface on HQ for **Incoming Interface** (in the example, internal), and the VPN tunnel interface for **Outgoing Interface** (in the example, VPN-to-Branch).

| | |
|--|---|
| Name  | From-HQ-to-Branch |
| Incoming Interface |  internal |
| Outgoing Interface |  VPN-to-Branch |
| Source |  HQ-original  + |
| Destination |  Branch-new  + |
| Schedule |  always |
| Service |  ALL  + |
| Action |  ACCEPT  DENY |

Firewall / Network Options

NAT 

| | | |
|-----------------------|---|---------------------|
| IP Pool Configuration | Use Outgoing Interface Address | Use Dynamic IP Pool |
| |  HQ-new  + | |

3. For the **Source**, select HQ-original, for the **Destination** select Branch-new, and for the **Service** select ALL.
4. Finally, enable **NAT**, select **Use Dynamic IP Pool**, and select the HQ-new IP Pool.
5. Repeat the process to create an additional new IPv4 Policy.
6. Enter *From-Branch-to-HQ* for the **Name**, the VPN interface for **Incoming Interface** (in the example, VPN-to-Branch), and the LAN-side interface for **Outgoing Interface** (in the example, internal).

| | |
|--------------------|--|
| Name ⓘ | From-Branch-to-HQ |
| Incoming Interface | VPN-to-Branch ▼ |
| Outgoing Interface | internal ▼ |
| Source | Branch-new ✕ + |
| Destination | HQ-new-to-original ✕ + |
| Schedule | always ▼ |
| Service | ALL ✕ + |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY |

Firewall / Network Options

NAT ☐

- For the **Source**, select Branch-new, for the **Destination** select HQ-new-to-original (the Virtual IP object you created in the "Configuring static routes on HQ" section), and for the **Service** select ALL.
- Note for this policy, you **do not** need to enable NAT.

Configuring IPsec VPN on Branch

- To create the tunnel on Branch, connect to Branch, and go to **VPN > IPsec Tunnels** and create a new tunnel.
- In the **VPN Setup** step, set **Template Type** to **Custom** and enter *VPN-to-HQ* for the **Name**.

1 VPN Setup

| | |
|---------------|--|
| Name | VPN-to-HQ |
| Template Type | <input type="radio"/> Site to Site <input type="radio"/> Remote Access <input checked="" type="radio"/> Custom |


- Enter HQ's public IP address (in the example, 172.25.176.142) for the **IP Address**, and select Branch's WAN interface for **Interface** (in the example, wan1).

| | |
|----------------|--|
| Network | |
| IP Version | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| Remote Gateway | Static IP Address ▼ |
| IP Address | 172.25.176.142 |
| Interface | wan1 ▼ |

4. Enter a matching secure key for the **Pre-shared Key**.


Authentication



Method Pre-shared Key

Pre-shared Key •••••••• 

5. Type the new address ranges selected in the "Planning the new addressing scheme" section for Branch and HQ's LAN in the **Local Address** and **Remote Address** fields (in the example, 10.2.2.0/24 and 10.1.1.0/24, respectively). The Local and Remote Address fields are the reverse of what you created in the "Configuring the IPsec VPN on HQ" section.

Phase 2 Selectors

| Name | Local Address | Remote Address |
|-----------|---------------|---|
| VPN-to-HQ | 10.2.2.0/24 | 10.1.1.0/24  |

New Phase 2  

Name VPN-to-HQ

Comments

Local Address Subnet 10.2.2.0/24

Remote Address Subnet 10.1.1.0/24


6. Optionally, expand **Advanced** and enable **Auto-negotiate**.

Auto-negotiate ☒


Autokey Keep Alive ☒


Configuring static routes on Branch

- To create the necessary routes on Branch, go to **Network > Static Routes** and select **Create New**.
- Enter the new subnet created in the "Planning the new addressing scheme" section for HQ's LAN in the **Destination** field, and select the VPN tunnel created in the "Configuring the IPsec VPN on Branch" section as the **Interface** (in the example, this is 10.1.1.0/24 and VPN-to-HQ).

Destination  Subnet Named Address Internet Service

10.1.1.0/24

Interface  VPN-to-HQ

Administrative Distance  10



- Create an additional route with the same **Destination** as the previous route, but this time change the

Administrative Distance to 200 and select Blackhole as the **Interface**.



| Destination | Subnet | Named Address | Internet Service |
|-------------------------|---------------|---------------|------------------|
| | 10.1.1.0/24 | | |
| Interface | ○ Blackhole ▼ | | |
| Administrative Distance | 200 | | |

Configuring address objects on Branch

1. To create address objects you will utilize in a later step, navigate to **Policy & Objects > Addresses** and select **Create New > Address**.
2. Enter *Branch-original* for the **Name**, the original LAN subnet of Branch for **Subnet** (in the example, 192.168.1.0/24), and select the LAN-side interface for **Interface** (in the example, lan).

| | |
|-------------------|---|
| Name | Branch-original |
| Color |  <input type="button" value="Change"/> |
| Type | Subnet ▼ |
| Subnet / IP Range | 192.168.1.0/24 |
| Interface |  lan ▼ |


3. Repeat the process to create an additional new address object.
4. Enter *HQ-new* for the **Name**, the new LAN subnet of HQ for **Subnet** (in the example, 10.1.1.0/24), and select the VPN interface for **Interface** (in the example, VPN-to-HQ).

| | |
|-------------------|---|
| Name | HQ-new |
| Color |  <input type="button" value="Change"/> |
| Type | Subnet ▼ |
| Subnet / IP Range | 10.1.1.0/24 |
| Interface |  VPN-to-HQ ▼ |

5. To create an IP Pool, navigate to **Policy & Objects > IP Pools** and select **Create New**.
6. Enter *Branch-new* for the **Name** and select **Fixed Port Range** for **Type**. For the **External IP Range** enter the new subnet for Branch (in the example, 10.2.2.1 – 10.2.2.254), and enter the original subnet for Branch in the **Internal IP Range** (in the example, 192.168.1.1 – 192.168.1.254).

| | | | |
|-------------------|--|---|--|
| Name | <input type="text" value="Branch-new"/> | | |
| Comments | <input type="text"/> 0/255 | | |
| Type | <input type="button" value="Overload"/> <input type="button" value="One-to-One"/> <input type="button" value="Fixed Port Range"/> <input type="button" value="Port Block Allocation"/> | | |
| External IP Range | <input type="text" value="10.2.2.1"/> | - | <input type="text" value="10.2.2.254"/> |
| Internal IP Range | <input type="text" value="192.168.1.1"/> | - | <input type="text" value="192.168.1.254"/> |
| ARP Reply | <input checked="" type="checkbox"/> | | |

- Finally, to create a Virtual IP, navigate to **Policy & Objects > Virtual IPs** and select **Create New > Virtual IP**.
- Enter *Branch-new-to-original* for the **Name** and select the VPN interface for **Interface** (in the example, VPN-to-HQ). For the **External IP Range** enter the new subnet for Branch (in the example, 10.2.2.1 – 10.2.2.254), and enter the original subnet for Branch in the **Internal IP Range** (in the example, 192.168.1.1 – 192.168.1.254).













| | |
|----------|---|
| Name | <input type="text" value="Branch-new-to-original"/> |
| Comments | <input type="text"/> 0/255 |
| Color |  <input type="button" value="Change"/> |

Network

| | | | |
|---------------------------|--|---|--|
| Interface | <input type="text" value="VPN-to-HQ"/> | | |
| Type | Static NAT | | |
| External IP Address/Range | <input type="text" value="10.2.2.1"/> | - | <input type="text" value="10.2.2.254"/> |
| Mapped IP Address/Range | <input type="text" value="192.168.1.1"/> | - | <input type="text" value="192.168.1.254"/> |



Configuring firewall policies on Branch

- To create firewall policies on Branch, navigate to **Policy & Objects > IPv4 Policies** and select **Create New**.
- Enter *From-Branch-to-HQ* for the **Name**, the LAN-side interface on Branch for **Incoming Interface** (in the example, lan), and the VPN tunnel interface for **Outgoing Interface** (in the example, VPN-to-HQ).









| | |
|--|---|
| Name  | From-Branch-to-HQ |
| Incoming Interface |  lan |
| Outgoing Interface |  VPN-to-HQ |
| Source |  Branch-original  + |
| Destination |  HQ-new  + |
| Schedule |  always |
| Service |  ALL  + |
| Action |  ACCEPT  DENY |

Firewall / Network Options

NAT 

| | | |
|-----------------------|---|---------------------|
| IP Pool Configuration | Use Outgoing Interface Address | Use Dynamic IP Pool |
| |  Branch-new  + | |

3. For the **Source**, select Branch-original, for the **Destination** select HQ-new, and for the **Service** select ALL.
4. Finally, enable **NAT**, select **Use Dynamic IP Pool**, and select the Branch-new IP Pool.
5. Repeat the process to create an additional new IPv4 Policy.
6. Enter *From-HQ-to-Branch* for the **Name**, the VPN interface for **Incoming Interface** (in the example, VPN-to-HQ), and the LAN-side interface for **Outgoing Interface** (in the example, lan).

| | |
|--------------------|---|
| Name ⓘ | From-HQ-to-Branch |
| Incoming Interface |  VPN-to-HQ ▼ |
| Outgoing Interface |  lan ▼ |
| Source |  HQ-new ✕ + |
| Destination |  Branch-new-to-original ✕ + |
| Schedule |  always ▼ |
| Service |  ALL ✕ + |
| Action |  ACCEPT  DENY |

Firewall / Network Options

NAT ☐

- For the **Source**, select HQ-new, for the **Destination** select Branch-new-to-original (the Virtual IP object you created in the "Configuring address objects, Virtual IPs, and IP Pools on Branch" section), and for the **Service** select ALL.
- Note for this policy, you **do not** need to enable NAT.

Results

- The IPsec tunnels should now be up on both sides, which you can verify under **Monitor > IPsec Monitor**. If you did not enable auto-negotiate in the "Configuring the IPsec VPN on HQ" section or "Configuring the IPsec VPN on Branch" section earlier, then you may have to highlight the tunnel and select **Bring Up**.

Refresh

Reset Statistics

Bring Up

Bring Down

| Name | Type | Remote Gateway | User Name | Inco |
|---------------|--------|----------------|-----------|------|
| VPN-to-Branch | Custom | 172.25.177.46 | | |

Refresh

Reset Statistics

Bring Up

Bring Down

| Name | Type | Remote Gateway | User Name | Incor |
|-----------|--------|----------------|-----------|-------|
| VPN-to-HQ | Custom | 172.25.176.142 | | |

- From a PC on the HQ network, try to ping a PC on the Branch network using the new IP for the Branch PC. The ping should be successful.

```

C:\Users\jheadley>ping 10.2.2.98

Pinging 10.2.2.98 with 32 bytes of data:
Reply from 10.2.2.98: bytes=32 time=7ms TTL=62
Reply from 10.2.2.98: bytes=32 time=1ms TTL=62
Reply from 10.2.2.98: bytes=32 time=1ms TTL=62
Reply from 10.2.2.98: bytes=32 time=1ms TTL=62

Ping statistics for 10.2.2.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 2ms

```

3. From a PC on the Branch network, try to ping a PC on the HQ network using the new IP for the HQ PC. The ping should be successful.

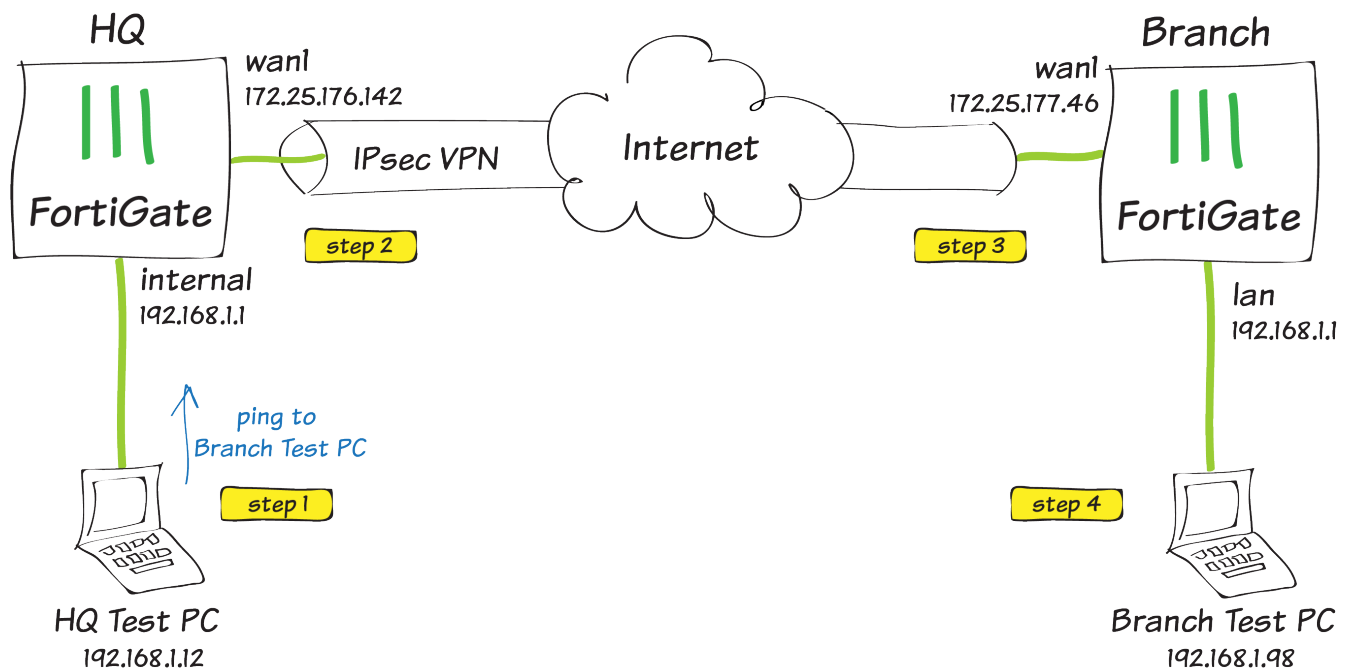
```

[Johns-MacBook-Air:~ John$ ping 10.1.1.12
PING 10.1.1.12 (10.1.1.12): 56 data bytes
64 bytes from 10.1.1.12: icmp_seq=0 ttl=126 time=1.912 ms
64 bytes from 10.1.1.12: icmp_seq=1 ttl=126 time=1.743 ms
64 bytes from 10.1.1.12: icmp_seq=2 ttl=126 time=1.403 ms
64 bytes from 10.1.1.12: icmp_seq=3 ttl=126 time=1.425 ms
^C
--- 10.1.1.12 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.403/1.621/1.912/0.215 ms

```

Explanation

Using the two example PCs below, the source and destination NAT that is performed in order to allow these two PCs in overlapping subnets to communicate is explained.



Step 1 – Ping Request: HQ Test PC sends a ping destined for Branch Test PC's new IP address of 10.2.2.98.

Src IP: 192.168.1.12

Dst IP: 10.2.2.98

Step 2 – Source NAT: The HQ FortiGate receives the ping, and after a route lookup, matches the traffic to firewall policy From-HQ-to-Branch that you created in the "Configuring firewall policies on HQ" section of the recipe.

Since the policy has NAT enabled and the HQ-new IP Pool selected, the HQ FortiGate will perform source NAT on HQ Test PC's IP address before sending into the IPsec tunnel.

Src IP: 10.1.1.12

Dst IP: 10.2.2.98



When you created an IP Pool with Type of Fixed Port Range, and then selected an External IP Range and Internal IP Range of equal size, the last octet of the IP addresses after SNAT will not change. This means 192.168.1.12 will be changed to 10.1.1.12, which makes using the new address range as simple as possible.

Step 3 – Destination NAT: Branch FortiGate receives the traffic on the IPsec tunnel, and before a policy is matched, the Virtual IP (VIP) you created called Branch-new-to-original performs destination NAT (DNAT).



Similar to our Fixed Port Range IP Pool, a VIP will exactly map the External IP Range to the Mapped IP Range. This means that 10.2.2.98 will DNAT to 192.168.1.98.

After DNAT, a route lookup is performed, and the traffic will match the From-HQ-to-Branch policy that you created in the "Configuring firewall policies on Branch" section of the recipe.

Src IP: 10.1.1.12

Dst IP: 192.168.1.98

Step 4 – Ping Reply: Branch Test PC receives the ping request from HQ Test PC and sends the ping reply back to 10.1.1.12.

The FortiGate is a stateful firewall, and the same firewall policy that was used when the session was initiated will be used on the way back (the From-HQ-to-Branch policy on both FortiGates).

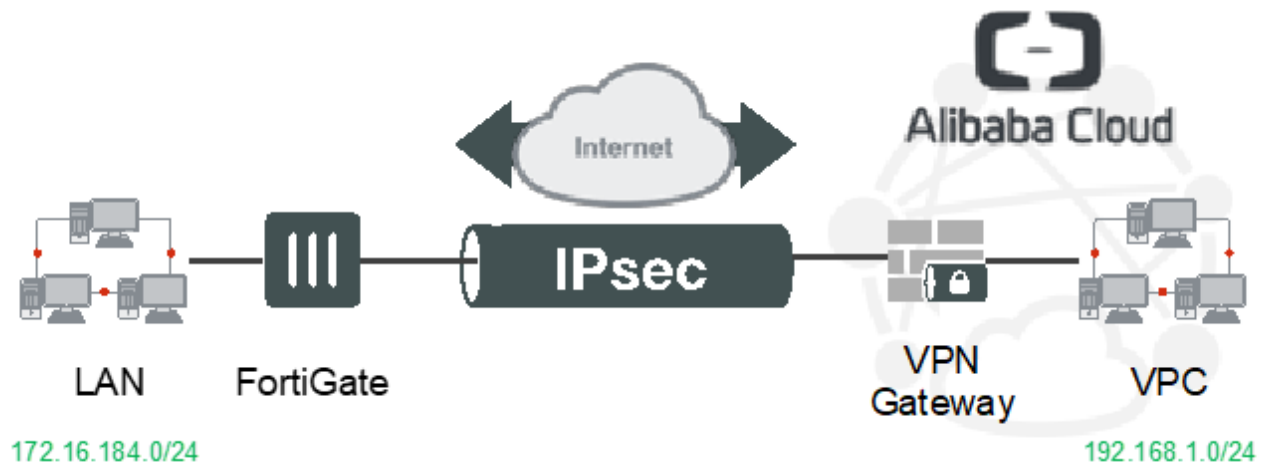
The session table on each FortiGate remembers the SNAT or DNAT that was performed in the "Configuring the IPsec VPN on HQ" section and "Configuring static routes on HQ" section, and will perform the reverse operation on the reply traffic.

Src IP: 192.168.1.98

Dst IP: 10.1.1.12

IPsec VPN to Alibaba Cloud (AliCloud)

The following recipe demonstrates how to configure a site-to-site IPsec VPN tunnel to Alibaba Cloud (AliCloud).



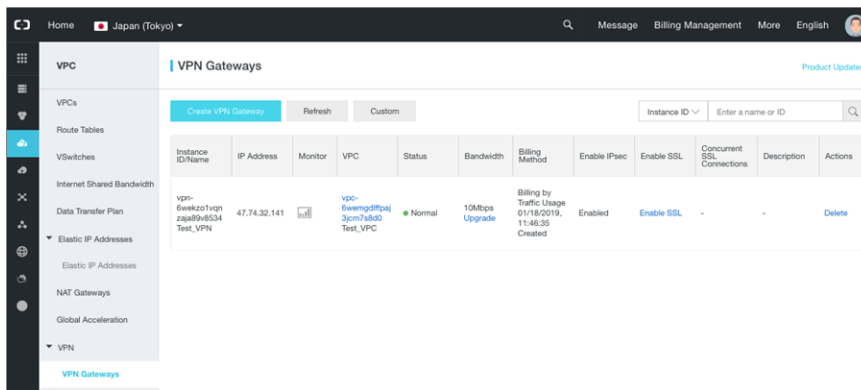
Using FortiOS 6.0.0, the example describes how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established.

The following is required for this recipe:

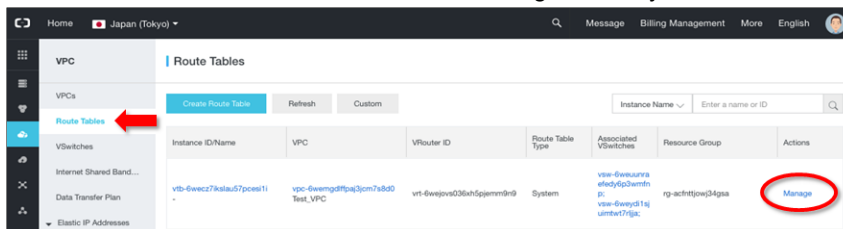
- One FortiGate (physical or virtual) with an Internet-facing IP address
- One valid Alibaba Cloud (AliCloud) account
- One VPC that has already been created

Configuring the Alibaba Cloud (AliCloud) VPN gateway

1. Log into Alibaba Cloud (AliCloud) and go to *Products & Services > VPN Gateway*.
2. Ensure that the correct region is selected in the top left corner. Otherwise, you cannot see your VPC. Verify that the VPC has already been configured.
3. Create the VPN gateway:
 - a. Click *Create VPN Gateway*.
 - b. In the *Name* field, enter the desired name.
 - c. From the *VPC* dropdown list, select the desired *VPC*.
 - d. For *IPsec VPN*, select *Enable*.
 - e. Click *Buy Now*.
 - f. Select *VPN Gateway Agreement of Service*.
 - g. Click *Activate*.
4. Return to the Alibaba Cloud (AliCloud) management console and verify that the VPN gateway has been created under *VPNs > VPN Gateways*.



5. An IP address has been assigned to the VPN gateway. Note down this IP address, as you will need it later in the process.
6. Register the FortiGate on your site as the customer gateway:
 - a. Go to *VPN > Customer Gateways*, then click *Create Customer Gateway*.
 - b. In the *Name* field, enter the FortiGate name.
 - c. In the *IP Address* field, enter the FortiGate's Internet-facing interface.
 - d. Click *OK*.
7. Set parameters for the IPsec tunnel:
 - a. Go to *VPN > IPsec Connections*, then click *Create IPsec Connection*.
 - b. In the *Name* field, enter the IPsec connection name.
 - c. For *VPN Gateway* and *Customer Gateway*, select those created in steps 3 and 6.
 - d. In the *Local Network* field, enter the VPC subnet address.
 - e. In the *Remote Network* field, enter the subnet address of the LAN on your site.
 - f. Set *Effective Immediately* to *Yes*. If this option is set to *No*, the VPN gateway attempts to establish IPsec tunnel connection only when traffic occurs and may cause delays in sending traffic.
 - g. Configure advanced settings:
 - i. Click *Advanced Configuration*.
 - ii. Enter the *Pre-Shared Key* for authentication purposes. Your FortiGate will require this keyword in a later step.
 - iii. From the *Version* dropdown list, select *ikev2*.
 - iv. Leave the other parameters as-is.
 - v. Under *IPsec Configurations*, modify *SA Life Cycle (seconds)* to 43200 so that it matches the FortiGate default value. *Advanced Configuration* contains two *SA Life Cycle (seconds)* fields: one for IKE configuration and one for IPsec configuration. Ensure that you are modifying the one under IPsec configuration.
 - vi. Click *OK*.
8. Configure a static route that will route traffic to the IPsec tunnel:
 - a. Go to *VPC > Route Tables*. You will see a routing table for your VPC. Click *Manage*.



- b. Click *Add Route Entry*.

- c. In the *Destination CIDR Block* field, enter the subnet address of the LAN on your site.
- d. From the *Next Hop Type* dropdown list, select *VPN Gateway*.
- e. From the *VPN Gateway* dropdown list, select the VPN gateway created in step 3.
- f. Click *OK*.

Configuring the FortiGate

1. Log into FortiOS.
2. Create the IPsec tunnel:
 - a. Go to *VPN > IPsec Tunnels*, then click *Create New*.
 - b. Configure the basic settings:
 - i. In the *Name* field, enter the desired name.
 - ii. For *Template Type*, select *Custom*.
 - iii. Click *Next*.
 - c. Configure the network settings:
 - i. In the *IP Address* field, enter the VPN gateway's IP address as provided by Alibaba Cloud (AliCloud) in step 5 of [Configuring the Alibaba Cloud \(AliCloud\) VPN gateway on page 330](#).
 - ii. From the *Interface* dropdown list, select an Internet-facing interface, such as *wan1*.
 - iii. If you want to automatically check the available of the remote VPN gateway, set *Dead Peer Detection* to *On Idle*.
 - d. Configure authentication:
 - i. *Authentication*, from the *Method* dropdown list, select *Pre-shared Key*.
 - ii. In the *Pre-Shared Key* field, enter the pre-shared key entered for the Alibaba Cloud (AliCloud) VPN gateway in step 7 of [Configuring the Alibaba Cloud \(AliCloud\) VPN gateway on page 330](#).
 - iii. For *IKE Version*, select 2.
 - e. Under *Diffie-Hellman Groups*, select 2. The Alibaba Cloud (AliCloud) VPN gateway's default DH group is 2. Leave the other parameters as-is.
 - f. For *Local Address*, select *Subnet* from the dropdown list, then enter the LAN subnet address.
 - g. For *Remote Address*, select *Subnet*, then enter the VPC subnet address on Alibaba Cloud (AliCloud).
 - h. Under *Advanced*, also select 2 under *Diffie-Hellman Groups*. Leave the other parameters as-is, then click *OK*.
3. To pass traffic to and from the IPsec tunnel, you must create a policy that allow transaction between the FortiGate and Alibaba Cloud (AliCloud). You must first create an address object which represents the subnet on your VPC:
 - a. Go to *Policy & Objects > Addresses*, then click *Create New > Address*.
 - b. In the *Name* field, enter the address object's name.
 - c. From the *Type* dropdown list, select *Subnet*.
 - d. In the *Subnet/IP Range* field, enter the VPC subnet address.
 - e. Enable *Static Route Configuration*. This allows you to use this address object as a static route destination in a later step.
4. Create a policy that permits outgoing sessions to the IPsec tunnel.
 - a. Go to *Policy & Objects > IPv4 Policy*, then click *Create New*.
 - b. In the *Name* field, enter the desired policy name.
 - c. In the *Incoming Interface* field, select your local LAN interface.
 - d. In the *Outgoing Interface* field, select the IPsec tunnel created in step 2.
 - e. For *Source*, select *all*, or specify any address objects if you want to allow access only from specific addresses.
 - f. For *Destination*, select the address object created for your VPC subnet in step 3.

- g. For *Service*, select all or specify any services you want to allow.
- h. Ensure that NAT is not enabled.
- i. Click *OK*.
5. Create a policy for incoming sessions from the VPC. Repeat the steps above, except for the following:
 - a. In the *Incoming Interface* field, select the IPsec tunnel created in step 2.
 - b. In the *Outgoing Interface* field, select your local LAN interface.
 - c. For *Source*, select subnets on your VPC.
6. To avoid packet drops and fragmentation, it is recommended to limit the TCP maximum segment size (MSS) being sent and received. For both firewall policies, configure the following in the CLI console:


```
config firewall policy
  edit <policy-id>
    set tcp-mss-sender 1350
    set tcp-mss-receiver 1350
  next
end
```
7. Go to *Monitor > IPsec Monitor*. If all configuration is complete as desired, the IP tunnel displays as being up. Otherwise, you must review and correct your settings.

| Name | Type | Remote Gateway | Peer ID | Incoming Data | Outgoing Data | Phase 1 | Phase 2 Selectors |
|---------------|--------|----------------|---------|---------------|---------------|---------------|-------------------|
| Alibaba Cloud | Custom | 47.74.32.141 | | 0 B | 0 B | Alibaba Cloud | Alibaba Cloud |

8. Create a static route to forward traffic from the LAN to Alibaba Cloud (AliCloud):
 - a. Go to *Network > Static Routes*, then select *Create New*.
 - b. For *Destination*, select *Named Address*. From the list, select your remote subnet.
 - c. From the *Interface* dropdown list, select the IPsec tunnel created in step 2.
 - d. Click *OK*.
9. FortiOS is now connected to Alibaba Cloud (AliCloud) via IPsec. You should see the traffic counter in *Monitor > IPsec Monitor*.

| Name | Type | Remote Gateway | Peer ID | Incoming Data | Outgoing Data | Phase 1 | Phase 2 Selectors |
|---------------|--------|----------------|---------|---------------|---------------|---------------|-------------------|
| Alibaba Cloud | Custom | | | 16.52 kB | 16.87 kB | Alibaba Cloud | Alibaba Cloud |

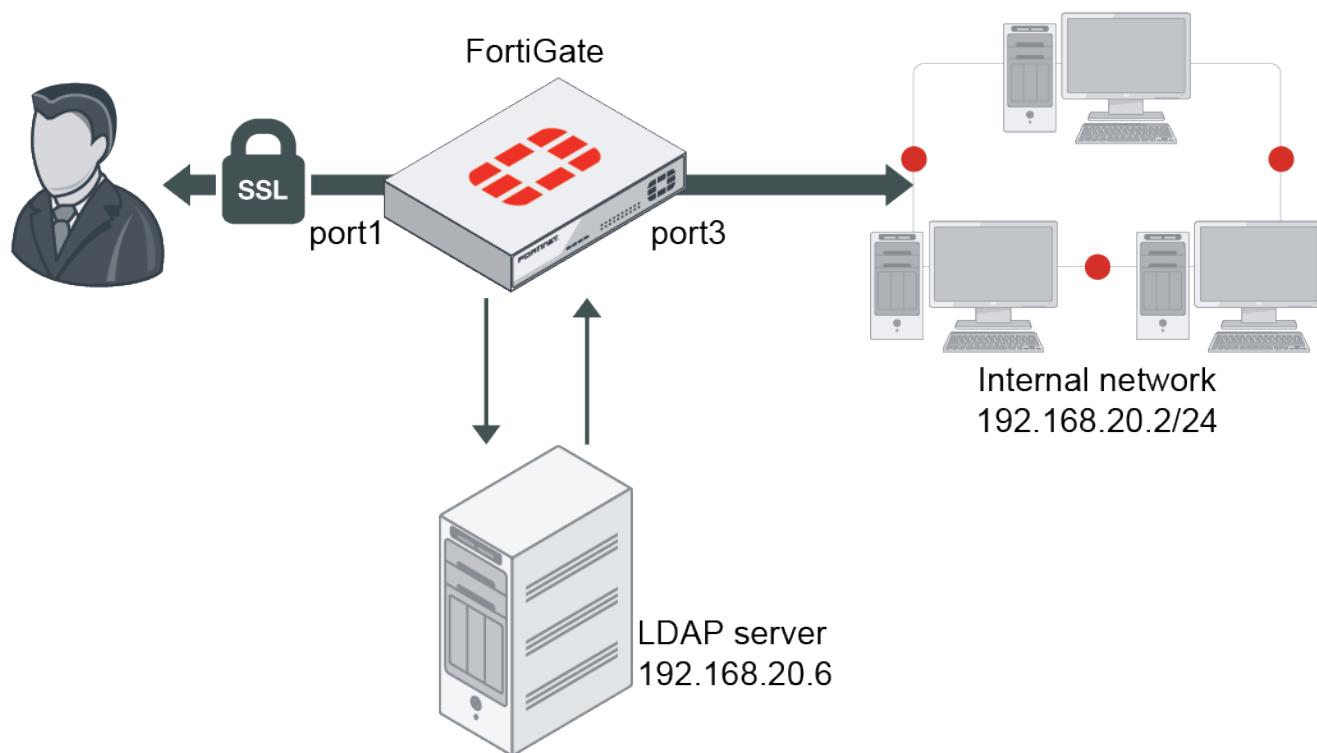
SSL VPN for remote users with MFA and user sensitivity

By default, remote LDAP and RADIUS user names are case sensitive. When a remote user object is applied to SSL VPN authentication, the user must type the exact case that is used in the user definition on the FortiGate.

Case sensitivity can be disabled by disabling the `username-sensitivity` CLI command, allowing the remote user object to match any case that the end user types in.

In this example, a remote user is configured with multi-factor authentication (MFA). The user group includes the LDAP user and server, and is applied to SSL VPN authentication and the policy.

Topology



Example configuration

To configure the LDAP server:

1. Generate and export a CA certificate from the AD server .
2. Import the CA certificate into FortiGate:
 - a. Go to *System > Features Visibility* and ensure *Certificates* is enabled.
 - b. Go to *System > Certificates* and select *Import > CA Certificate*.
 - c. Select *Local PC* and then select the certificate file.
The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA_Cert_1*.
 - d. If you want, you can use CLI commands to rename the system-generated *CA_Cert_1* to be more descriptive:

```
config vpn certificate ca
    rename CA_Cert_1 to LDAPS-CA
end
```

3. Configure the LDAP user:
 - a. Go to *User & Device > LDAP Servers* and click *Create New*.
 - b. Configure the following options for this example:

| | |
|-----------------------|----------------|
| Name | WIN2K16-KLHOME |
| Server IP/Name | 192.168.20.6 |

| | |
|-------------------------------|--|
| Server Port | 636 |
| Common Name Identifier | sAMAccountName |
| Distinguished Name | dc=KLHOME,dc=local |
| Bind Type | Regular |
| Username | KLHOME\Administrator |
| Password | ***** |
| Secure Connection | Enable |
| Protocol | LDAPS |
| Certificate | CA_Cert_1 This is the CA certificate that you imported in step 2. |

Edit LDAP Server

| | |
|------------------------------------|--|
| Name | WIN2K16-KLHOME |
| Server IP/Name | 192.168.20.6 |
| Server Port | 636 |
| Common Name Identifier | sAMAccountName |
| Distinguished Name | dc=KLHOME,dc=local Browse |
| Bind Type | Simple Anonymous Regular |
| Username | KLHOME\Administrator |
| Password | ***** 🔑 |
| Secure Connection | <input checked="" type="checkbox"/> |
| Protocol | STARTTLS LDAPS |
| Certificate | CA_Cert_1 |
| Test Connectivity | |
| Test User Credentials | |

OK Cancel

c. Click OK.

To configure an LDAP user with MFA:

1. Go to *User & Device > User Definition* and click *Create New*.
2. Select *Remote LDAP User*, then click *Next*.
3. Select the just created LDAP server, then click *Next*.

Users/Groups Creation Wizard

User Type **LDAP Server** Remote Users

LDAP Server WIN2K16-KLHOME

< Back **Next** Cancel

4. Right click to add the selected user, then click *Submit*.
5. Edit the user that you just created.
The username will be pulled from the LDAP server with the same case as it has on the server.
6. Set the *Email Address* to the address that FortiGate will send the FortiToken to.
7. Enable *Two-factor Authentication*.
8. Set *Authentication Type* to *FortiToken*.

9. Set *Token* to a FortiToken device. See [FortiToken Mobile Push for SSL VPN on page 272](#) for more information.

10. Click **OK**.

To disable case sensitivity on the remote user:

This can only be configured in the CLI.

```
config user local
  edit "fgdocs"
    set type ldap
    set two-factor fortitoken
    set fortitoken "FTKMOBxxxxxxxx"
    set email-to "fgdocs@fortinet.com"
    set username-sensitivity disable
    set ldap-server "WIN2K16-KLHOME"
  next
end
```

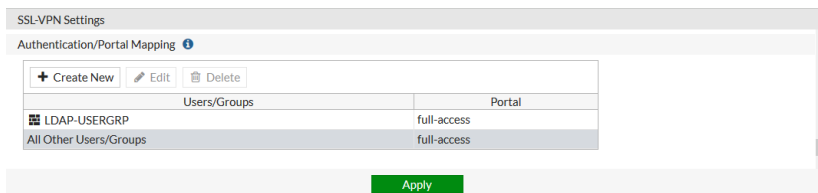
To configure a user group with the remote user and the LDAP server:

1. Go to *User & Device > User Groups* and click *Create New*.
2. Set the *Name* to *LDAP-USERGRP*.
3. Set *Members* to the just created remote user.
4. In the *Remote Groups* table, click *Add*:
 - a. Set *Remote Server* to the LDAP server.
 - b. Set the group or groups that apply, and right click to add them.
 - c. Click **OK**.

5. Click **OK**.

To apply the user group to the SSL VPN portal:

1. Go to *VPN > SSL-VPN Settings*.
2. In the *Authentication/Portal Mapping* table, click *Create New*.
 - a. Set *Users/Groups* to the just created user group.
 - b. Configure the remaining settings as required.
 - c. Click *OK*.

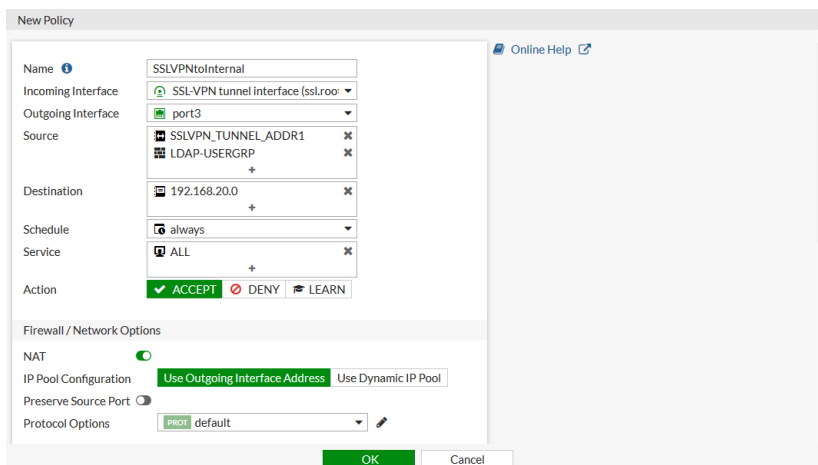


3. Click *Apply*.

To apply the user group to a firewall policy:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Configure the following:

| | |
|---------------------------|---|
| Name | SSLVPNtoInternal |
| Incoming Interface | SSL-VPN tunnel interface (ssl.root) |
| Outgoing Interface | port3 |
| Source | Address - SSLVPN_TUNNEL_ADDR1 User - LDAP-USERGRP |
| Destination | The address of the internal network. In this case: 192.168.20.0. |
| Schedule | always |
| Service | ALL |
| Action | ACCEPT |
| NAT | Enabled |



3. Configuring the remaining settings as required.
4. Click OK.

To configure this example in the CLI:

1. Configure the LDAP server:

```
config user ldap
  edit "WIN2K16-KLHOME"
    set server "192.168.20.6"
    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
```

2. Configure an LDAP user with MFA and disable sensitivity on the remote user:

```
config user local
  edit "fgdocs"
    set type ldap
    set two-factor fortitoken
    set fortitoken "FTKMOBxxxxxxxxxx"
    set email-to "fgdocs@fortinet.com"
    set username-sensitivity disable
    set ldap-server "WIN2K16-KLHOME"
  next
end
```

3. Configure a user group with the remote user and the LDAP server:

```
config user group
  edit "LDAP-USERGRP"
    set member "fgdocs" "WIN2K16-KLHOME"
  next
end
```

4. Apply the user group to the SSL VPN portal:

```
config vpn ssl settings
  set servercert <server certificate>
  set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
  set source-interface "port1"
  set source-address "all"
  set default-portal "web-access"
  config authentication-rule
    edit 1
      set groups "LDAP-USERGRP"
      set portal "full-access"
    next
  end
end
```

5. Apply the user group to a firewall policy:

```
config firewall policy
  edit 5
    set name "SSLVPNtoInternal"
    set srcintf "ssl.root"
    set dstintf "port3"
    set srcaddr "SSLVPN_TUNNEL_ADDR1"
    set dstaddr "192.168.20.0"
    set action accept
    set schedule "always"
    set service "ALL"
    set groups "LDAP-USERGRP"
    set nat enable
  next
end
```

Verification

To setup the VPN connection:

1. Download FortiClient from www.forticlient.com.
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection:
 - a. Set the connection name.
 - b. Set *Remote Gateway* to the IP of the listening FortiGate interface.
 - c. If required, set the *Customize Port*.
4. Save your settings.

To test the connection with case sensitivity disabled:

1. Connect to the VPN:
 - a. Log in to the tunnel with the username, using the same case that it is on the FortiGate.
 - b. When prompted, enter your FortiToken code.
You should now be connected.
2. Check the web portal log in using the CLI:

```
# get vpn ssl monitor
SSL VPN Login Users:
  Index   User      Group    Auth Type    Timeout    From    HTTP in/out    HTTPS
in/out
  0       fgdocs    LDAP-USERGRP  16(1)      289      192.168.2.202  0/0
0/0

SSL VPN sessions:
  Index   User      Group    Source IP    Duration    I/O Bytes    Tunnel/Dest IP
  0       fgdocs    LDAP-USERGRP  192.168.2.202  45      99883/5572
10.212.134.200
```

3. Disconnect from the VPN connection.

4. Reconnect to the VPN:

- a. Log in to the tunnel with the username, using a different case than on the FortiGate.
- b. When prompted, enter your FortiToken code.
You should now be connected.

5. Check the web portal log in using the CLI:

```
# get vpn ssl monitor
SSL VPN Login Users:
  Index   User      Group   Auth Type   Timeout   From   HTTP in/out   HTTPS
in/out
  0       FGDOCS      LDAP-USERGRP   16(1)     289      192.168.2.202 0/0
0/0

SSL VPN sessions:
  Index   User      Group   Source IP   Duration   I/O Bytes   Tunnel/Dest IP
0       FGDOCS      LDAP-USERGRP   192.168.2.202 45        99883/5572
10.212.134.200
```

In both cases, the remote user is matched against the remote LDAP user object and prompted for multi-factor authentication.

To test the connection with case sensitivity enabled:**1. Enable case sensitivity for the user:**

```
config user local
  edit "fgdocs"
    set username-sensitivity enable
  next
end
```

2. Connect to the VPN

- a. Log in to the tunnel with the username, using the same case that it is on the FortiGate.
- b. When prompted, enter your FortiToken code.
You should now be connected.

3. Check the web portal log in using the CLI:

```
# get vpn ssl monitor
SSL VPN Login Users:
  Index   User      Group   Auth Type   Timeout   From   HTTP in/out   HTTPS
in/out
  0       fgdocs      LDAP-USERGRP   16(1)     289      192.168.2.202 0/0
0/0

SSL VPN sessions:
  Index   User      Group   Source IP   Duration   I/O Bytes   Tunnel/Dest IP
0       fgdocs      LDAP-USERGRP   192.168.2.202 45        99883/5572
10.212.134.200
```

1. Disconnect from the VPN connection.**2. Reconnect to the VPN:**

- a. Log in to the tunnel with the username, using a different case than on the FortiGate.
You will not be prompted for your FortiToken code. You should now be connected.

3. Check the web portal log in using the CLI:

```
# get vpn ssl monitor
```

```
SSL VPN Login Users:
```

| Index | User | Group | Auth Type | Timeout | From | HTTP in/out | HTTPS |
|--------|---------------|-------|--------------|---------|------|---------------|-------|
| in/out | | | | | | | |
| 0 | FGdocs | | LDAP-USERGRP | 16(1) | 289 | 192.168.2.202 | 0/0 |
| 0/0 | | | | | | | |

```
SSL VPN sessions:
```

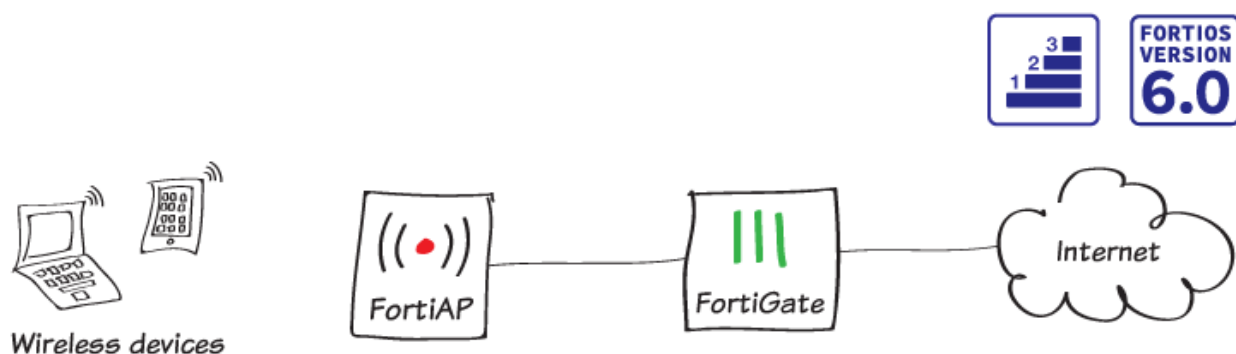
| Index | User | Group | Source IP | Duration | I/O Bytes | Tunnel/Dest IP |
|----------------|---------------|-------|--------------|---------------|-----------|----------------|
| 0 | FGdocs | | LDAP-USERGRP | 192.168.2.202 | 45 | 99883/5572 |
| 10.212.134.200 | | | | | | |

In this case, the user is allowed to log in without a FortiToken code because the entered user name did not match the name defined on the remote LDAP user object. Authentication continues to be evaluated against the LDAP server though, which is not case sensitive.

WiFi

This section contains information about creating and configuring WiFi networks.

Setting up WiFi with FortiAP



In this recipe, you will set up a WiFi network with by adding a FortiAP in Tunnel mode to your network.

You can configure a FortiAP in either Tunnel mode (default) or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet.

Connecting FortiAP

1. To edit the interface that will connect to the FortiAP (in the example, **port 22**), go to **Network > Interfaces**.
2. Set **Role** to **LAN** and **Addressing Mode** to **Manual**. Set **IP/Network Mask** to a private IP address (in the example **10.10.200.1/255.255.255.0**).
3. Under **Administrative Access**, enable **CAPWAP**.
4. Enable **DHCP Server**.
5. Under **Networked Devices**, enable **Device Detection**.

Interface Name port22 (90:6C:AC:2A:14:59)

Alias

Link Status Up

Type Physical Interface

Tags

Role LAN

Add Tag Category

Address

Addressing mode **Manual** DHCP Dedicated to FortiSwitch

IP/Network Mask

Administrative Access

IPv4 ☐ HTTPS ☐ HTTP ☒ PING ☐ FMG-Access

☒ CAPWAP ☒ SSH ☐ SNMP ☐ FTM

☐ RADIUS Accounting ☐ FortiTelemetry

DHCP Server

Address Range

Create New Edit Delete

| Starting IP | End IP |
|-------------|---------------|
| 10.10.200.2 | 10.10.200.254 |

Netmask

Default Gateway **Same as Interface IP** Specify

DNS Server **Same as System DNS** Same as Interface IP Specify

Advanced...

Networked Devices

Device Detection

- Connect the FortiAP unit to the interface.
- To view the list of managed FortiAPs, go to **WiFi & Switch Controller > Managed FortiAPs**. The new FortiAP appears in the list but it is grayed out because it is not authorized. If the FortiAP does not appear, wait a few minutes, then refresh the page.

Select the FortiAP, and select **Authorize**.

| Access Point | State | Connected Via | SSIDs | Channel | Clients | OS Version | FortiAP Profile |
|------------------|-------|-----------------------|------------------------------|------------------------|--------------------------|------------|-----------------|
| FP221C3X16004328 | | 10.10.200.2 - port22 | Radio 1: All Radio 2: All | Radio1: 0 Radio2: 0 | Radio 1: 0 Radio 2: 0 | | FAP221C-default |

- After a few minutes, select **Refresh**. The FortiGate shows the FortiAP as authorized.

| Access Point | State | Connected Via | SSIDs | Channel | Clients | OS Version | FortiAP Profile |
|------------------|-------|-----------------------|------------------------------|------------------------|--------------------------|-----------------------|-----------------|
| FP221C3X16004328 | | 10.10.200.2 - port22 | Radio 1: All Radio 2: All | Radio1: 0 Radio2: 0 | Radio 1: 0 Radio 2: 0 | FP221C-v5.6-build0476 | FAP221C-default |

Creating an SSID

1. To create a new SSID to be broadcast for WiFi users, go to **WiFi & Switch Controller > SSID**.
2. Set **Traffic Mode** to **Tunnel** and set **IP/Network Mask** to a private IP address (in the example *10.10.201.1/255.255.255.0*).
3. Enable **DHCP Server** and **Device Detection**.

| | |
|----------------|---|
| Interface Name | wireless |
| Alias | |
| Type | WiFi SSID |
| Traffic Mode | 🔌 Tunnel 📶 Bridge 🌐 Mesh |

Tags

+ Add Tag Category

Address

IP/Network Mask 10.10.201.1/255.255.255.0

Administrative Access

IPv4 ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access
☐ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry

☒ DHCP Server

Address Range

| + Create New Edit Delete | |
|--------------------------|---------------|
| Starting IP | End IP |
| 10.10.201.2 | 10.10.201.254 |

Netmask 255.255.255.0

Default Gateway Same as Interface IP Specify

DNS Server Same as System DNS Same as Interface IP Specify

+ Advanced...

Networked Devices

Device Detection ☒

4. Under **WiFi Settings**, name the **SSID** (in the example, *Office-WiFi*) and set a secure **Pre-shared Key**.

5. Enable **Broadcast SSID**.

WiFi Settings

| | |
|--------------------------|-------------------------------------|
| SSID | Office-WiFi |
| Security Mode | WPA2 Personal ▼ |
| Pre-shared Key ⓘ | •••••••••• ⓘ 👁 |
| Client Limit | <input type="checkbox"/> |
| Multiple Pre-shared Keys | <input type="checkbox"/> |
| Broadcast SSID | <input checked="" type="checkbox"/> |

Creating a custom FortiAP profile

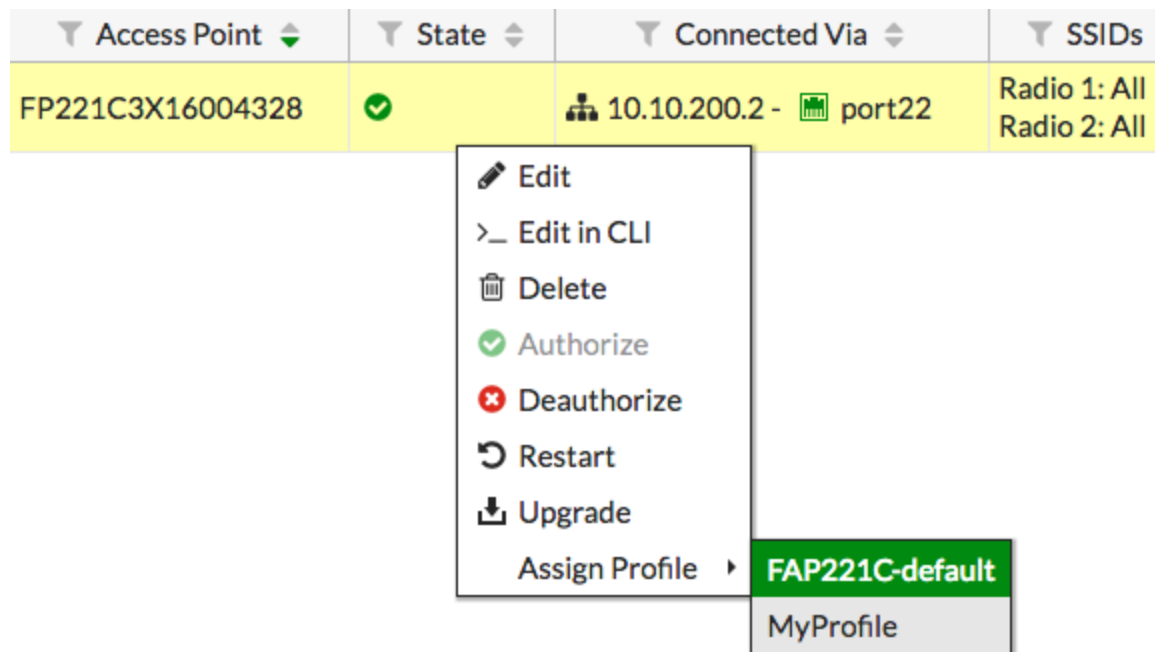
1. To create a new FortiAP profile, go to **WiFi & Switch Controller > FortiAP Profiles**.
2. Set Platform to the FortiAP model you are using (in the example, **FAP221C**) and **Country/Region** to the appropriate location.
3. Set an **AP Login Password** to secure the FortiAP.
4. Under **Radio 1**, set **Mode** to **Access Point** and **SSIDs** to **Manual**. Add your new SSID.

| | |
|---------------------|---|
| Name | MyProfile ⓘ |
| Comments | Write a comment... 0/255 |
| Platform | FAP221C ▼ |
| Country / Region | Canada ▼ |
| AP Login Password ⓘ | <input checked="" type="button" value="Set"/> <input type="button" value="Leave Unchanged"/> <input type="button" value="Set Empty"/> •••••••• ⓘ |

Radio 1

| | |
|-----------------------------|---|
| Mode | <input type="button" value="Disabled"/> <input checked="" type="button" value="Access Point"/> <input type="button" value="Dedicated Monitor"/> |
| WIDS Profile | <input type="checkbox"/> |
| Radio Resource Provision | <input type="checkbox"/> |
| Client Load Balancing | <input type="checkbox"/> Frequency Handoff <input type="checkbox"/> AP Handoff |
| Band | 2.4 GHz 802.11n/g ▼ |
| Channel Width | 20MHz |
| Short Guard Interval | <input type="checkbox"/> |
| Channels | <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 11 |
| TX Power Control | <input type="button" value="Auto"/> <input checked="" type="button" value="Manual"/> |
| TX Power | <input type="range"/> 100% |
| SSIDs ⓘ | <input type="button" value="Auto"/> <input checked="" type="button" value="Manual"/> (••) Office-WiFi (wireless) ✕ <div>+</div> |
| Monitor Channel Utilization | <input type="checkbox"/> |

5. To assign the new profile, go to **WiFi & Switch Controller > Managed FortiAPs** and right-click the FortiAP. Select **Assign Profile** and set the FortiAP to use the new profile.



Creating a security policy

1. To create a new policy for wireless Internet access, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Set **Incoming Interface** to the SSID and **Outgoing Interface** to your Internet-facing interface.

3. Enable **NAT**.

| | |
|--------------------|---|
| Name ⓘ | WiFi-Internet |
| Incoming Interface | Office-WiFi (wireless) ▼ |
| Outgoing Interface | wan1 ▼ |
| Source | all + ✕ |
| Destination | all + ✕ |
| Schedule | always ▼ |
| Service | ALL + ✕ |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |

Firewall / Network Options

NAT ☒IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Results

1. Connect to the SSID with a wireless device. After a connection is established, browse the Internet to generate traffic.
2. To view the traffic using the wireless Internet access policy, go to **FortiView > All Segments > Policies**.

| Policy | Bytes (Sent/Received) ▾ | Sessions ▾ | Bandwidth ▾ |
|-------------------|-------------------------|------------|-------------|
| WiFi-Internet (2) | 110.52 kB | 41 | 2 kbps |
| Internet (1) | 197 B | 1 | 0 bps |

3. To view more information about this traffic, right-click the policy and select **Drill Down to Details**.

Summary of WiFi-Internet

| | |
|-----------------------|------------------|
| Policy Name | WiFi-Internet |
| Policy ID | 2 |
| Bytes (Sent/Received) | 107.30 kB |
| Bandwidth | 2.58 kbps |
| Sessions | 33 |
| Time Period | Realtime |
| FortiGate | FG800D3915800295 |

Sources Destinations Applications Countries Sessions

| Source | Source Device | Source Interface | Bytes (Sent/Received) ▾ | Sessions ▾ | Bandwidth ▾ |
|-------------|---------------|------------------------|-------------------------|------------|-------------|
| 10.10.201.2 | vmartin-mac | Office-WiFi (wireless) | 106.60 kB | 33 | 3 kbps |

For further reading, check out [Configuring a WiFi LAN](#) in the [FortiOS 6.0 Online Help](#).

Replacing the Fortinet_Wifi certificate



These instructions apply to FortiWiFi devices using internal WiFi radios and FortiGate/FortiWiFi devices configured as WiFi Controllers that are managing FortiAP devices, and have WiFi clients that are connected to WPA2-Enterprise SSID and authenticated with local user groups.

On FortiOS, the built-in *Fortinet_Wifi* certificate is a publicly signed certificate that is only used in WPA2-Enterprise SSIDs with local user-group authentication. The default WiFi certificate configuration is:

```
config system global
    set wifi-ca-certificate "Fortinet_Wifi_CA"
    set wifi-certificate "Fortinet_Wifi"
end
```

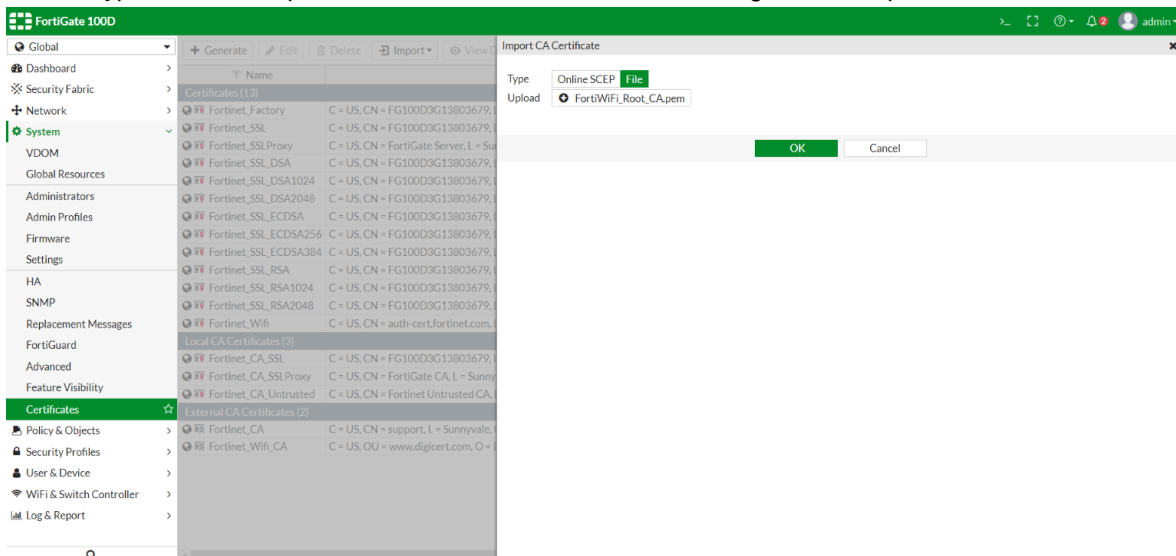
WiFi administrators must consider the following factors:

- The *Fortinet_Wifi* certificate is issued to *Fortinet Inc.* with common name (CN) *auth-cert.fortinet.com*. If a company or organization requires their own CN in their WiFi deployment, they must replace it with their own certificate.
- The *Fortinet_Wifi* certificate has an expire date. When it is expiring, it must be renewed or replaced with a new certificate.

To replace the Fortinet_Wifi certificate:

1. Get new certificate files, including a root CA certificate, a certificate signed by the CA, and the corresponding private key file:
Purchase a publicly signed certificate from a commercial certificate service provider, or generate a self-signed certificate.
2. Import the new certificate files into FortiOS:
 - a. On the FortiGate, go to *System > Certificates*.
If VDOMs are enable, got to *Global > System > Certificates*.
 - b. Click *Import > CA Certificate*.

- c. Set the *Type* to *File* and upload the CA certificate file from the management computer.

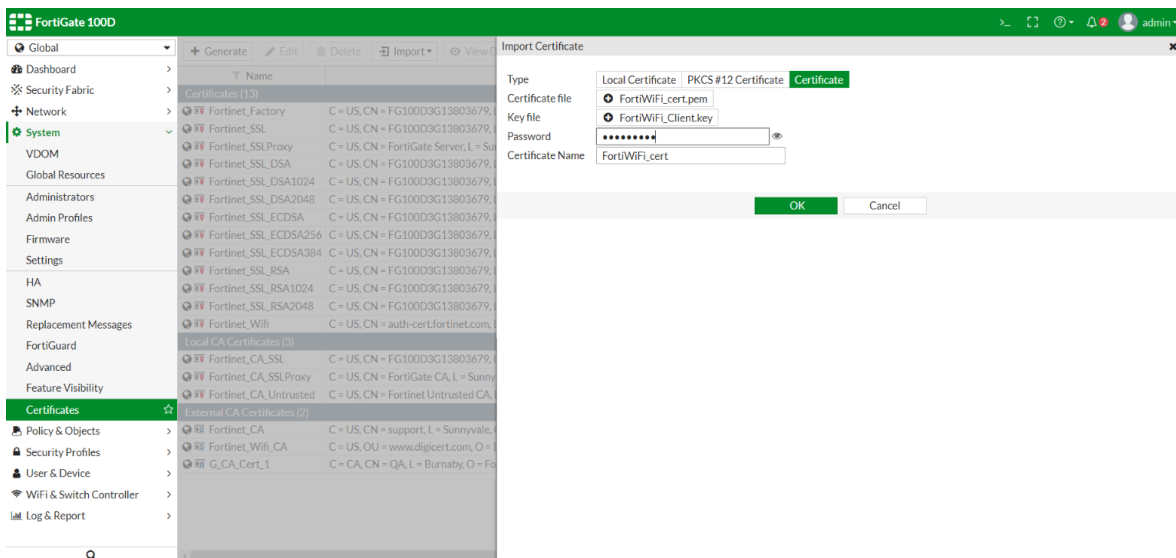


- d. Click **OK**.

The imported CA certificate is named *CA_Cert_N*, or *G_CA_Cert_N* when VDOMs are enabled, where *N* starts from 1 and increments for each imported certificate, and *G* stands for global range.

- e. Click *Import > Local Certificate*.

- f. Set the *Type* to *Certificate*, upload the certificate file and key file, enter the password, and enter the certificate name.



- g. Click **OK**.

The imported certificates are listed on the *Certificates* page.

3. Change the WiFi certificate settings:

```
config system global
    set wifi-ca-certificate <name of the imported CA certificate>
    set wifi-certificate <name of the imported certificate signed by the CA>
end
```

Notes



If necessary, the factory default certificates can also be used to replace the certificates:

```
config system global
  set wifi-ca-certificate "Fortinet_CA"
  set wifi-certificate "Fortinet_Factory"
end
```

As the factory default certificates are self-signed, WiFi clients will need to accept it at the connection prompt, or import the *Fortinet_CA* certificate to validate it.

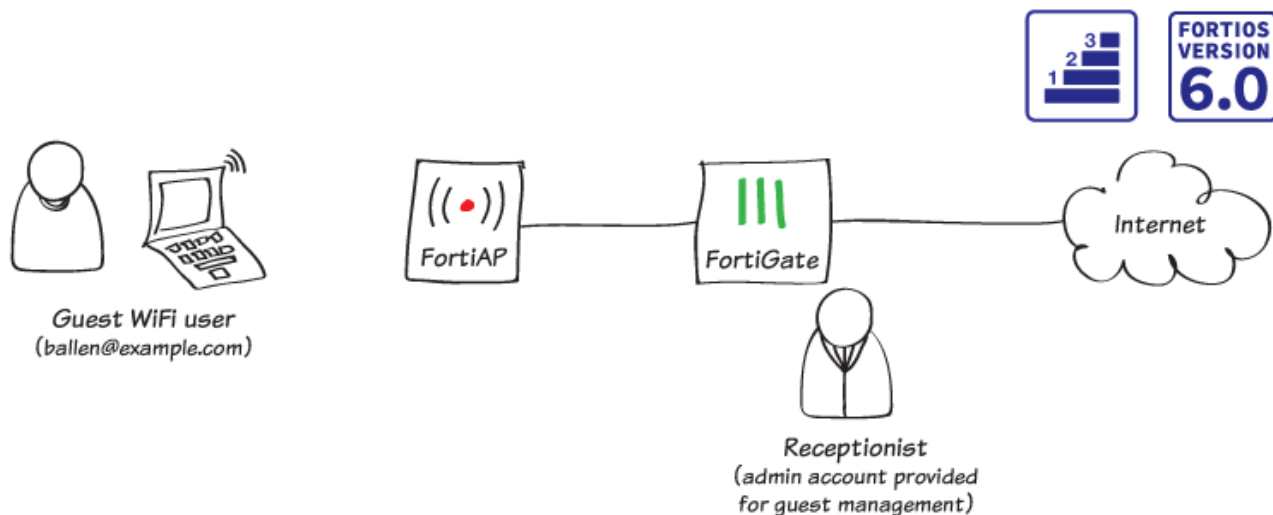


If the built-in *Fortinet_Wifi* certificate has expired and not been renewed or replaced, WiFi clients can still connect to the WPA2-Enterprise SSID with local user-group authentication by ignoring any prompted warning messages or bypassing *Validate server certificate* (or similar) options.



With FortiOS 6.0.1 and later, the *Fortinet_Wifi* certificate can be updated automatically through the FortiGuard service certificate bundle update.

Guest WiFi accounts



In this recipe, you create temporary guest accounts that can connect to your WiFi network after authenticating using a captive portal. To make management easier, you also create a separate administrative account that can only be used to manage guest accounts.

This example uses a FortiAP in Tunnel mode to provide WiFi access to guests. For information about configuring the FortiAP, see [Setting up WiFi with FortiAP on page 342](#).

Creating a guest user group

1. To create a guest user group, go to **User & Device > User Groups** and create a new group.
2. Set **Type** to **Guest** and set **User ID** to **Email**.
3. Under **Guest Details**, enable **Require Email**, enable **Password**, and set the password to **Auto Generated**.
4. Under **Expiration**, set **Start Countdown** to **After First Login** and set **Time** to 5 minutes for testing purposes.

Name

Type **Guest**

Batch Guest Account Creation ☐

User ID **Email** Auto Generated Specify

Maximum Accounts ☐

Guest Details

Require Name ☐

Require Email ☒

Require SMS ☐

Password ☒ **Auto Generated** Specify

Sponsor ☐

Company ☐

Expiration

Start Countdown ☐ On Account Creation ☒ After First Login

Time Days Hours Minutes Seconds

Creating an SSID

1. To create an SSID for guest users, go to **WiFi & Switch Controller > SSID** and create a new SSID.
2. Set **Traffic Mode** to **Tunnel**. Assign an **IP/Network Mask** to the interface and enable **DHCP Server**.

Interface Name

Alias

Type

Traffic Mode ☒ Tunnel ☐ Bridge ☐ Mesh

Tags

[+ Add Tag Category](#)

Address

IP/Network Mask

Administrative Access

IPv4 ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access
☐ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry

☒ DHCP Server

Address Range

| Starting IP | End IP |
|-------------|---------------|
| 10.10.100.2 | 10.10.100.254 |

Netmask

Default Gateway ☒ Same as Interface IP ☐ Specify

DNS Server ☒ Same as System DNS ☐ Same as Interface IP ☐ Specify

[+ Advanced...](#)

3. Under WiFi Settings, set the following:

- **Security Mode** to **Captive Portal**
- **Portal Type** to **Authentication**
- **User Groups** to the guest user group

WiFi Settings

SSID

Security Mode

Client Limit ☐

Portal Type ☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only

Authentication Portal ☒ Local ☐ External

User Groups

4. To broadcast the new SSID, go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile used by the FortiAP.
5. Under **Radio 1** set **SSIDs** to include the new SSID.

Radio 1

Mode

Disabled Access Point Dedicated Monitor

WIDS Profile

☐

Radio Resource Provision

☐

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

2.4 GHz 802.11n/g ▼

Channel Width

20MHz

Short Guard Interval

☐

Channels

☒ 1 ☒ 6 ☒ 11

TX Power Control

Auto Manual

TX Power

0%

SSIDs ⓘ

Auto Manual

⌵ Guest-WiFi (Guest-WiFi) ✕












⌵ Office-WiFi (wireless) ✕

+

Creating a security policy

1. To allow WiFi guest users to access the Internet, go to **Policy & Objects > IPv4 Policy** and create a new policy.
2. Set **Incoming Interface** to the guest SSID and set **Outgoing Interface** to your Internet-facing interface. Select **Source** and set **Address** to **all** and **User** to the guest user group.

3. Enable **NAT**.

| | | |
|--|---|--|
| Name  | Guest-Internet | |
| Incoming Interface |  Guest-WiFi (Guest-WiFi) ▼ | |
| Outgoing Interface |  wan1 ▼ | |
| Source | <div>  all  </div> <div>  Guest-WiFi  </div> <div>+</div> | |
| Destination | <div>  all  </div> <div>+</div> | |
| Schedule | always ▼ | |
| Service | <div>  ALL  </div> <div>+</div> | |
| Action | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN | |

Firewall / Network Options

NAT ☒IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Creating a guest user management account

To simplify guest account creation, you can create an admin account that is only used for guest user management. This allows new accounts to be made as needed without requiring full administrative access to the FortiGate. In this example, the account is made for use by receptionist.

1. To create the guest management account, go to **System > Administrators** and create a new account.
2. Set a **User Name** and set **Type** to **Local User**. Set and confirm a **Password**.

3. Enable **Restrict admin to guest account provisioning only** and set **Guest Group** to the WiFi guest user group.

| | |
|------------------|---|
| User Name | <input type="text" value="reception"/> |
| Type | <div><div>Local User</div><div>Match a user on a remote server group</div><div>Match all users in a remote server group</div><div>Use public key infrastructure (PKI) group</div></div> |
| Password | <input type="password" value="••••••••"/> |
| Confirm Password | <input type="password" value="••••••••"/> |
| Comments | <input type="text" value="Write a comment..."/> 0/255 |
| Email Address | <input type="text"/> |

☐ SMS

☐ Two-factor Authentication

☐ Restrict login to trusted hosts

☒ Restrict admin to guest account provisioning only

| | |
|-------------|---|
| Guest Group | <div><div> Guest-WiFi</div><div>+</div><div>×</div></div> |
|-------------|---|

Creating a guest user account

1. Using the receptionist account, create a guest account.
2. Set **Email** to the user's email address (in the example, `ballen@example.com`). To test the account, set **Expiration** to **5 Minutes**.

| | | |
|------------|---|-----------|
| User ID | Use Email Address | |
| Password | Auto Generated | |
| Email | <input type="text" value="ballen@example.com"/> | |
| Expiration | <input type="text" value="5"/> | Minutes ▼ |
| Comments | <input type="text"/> Optional | |

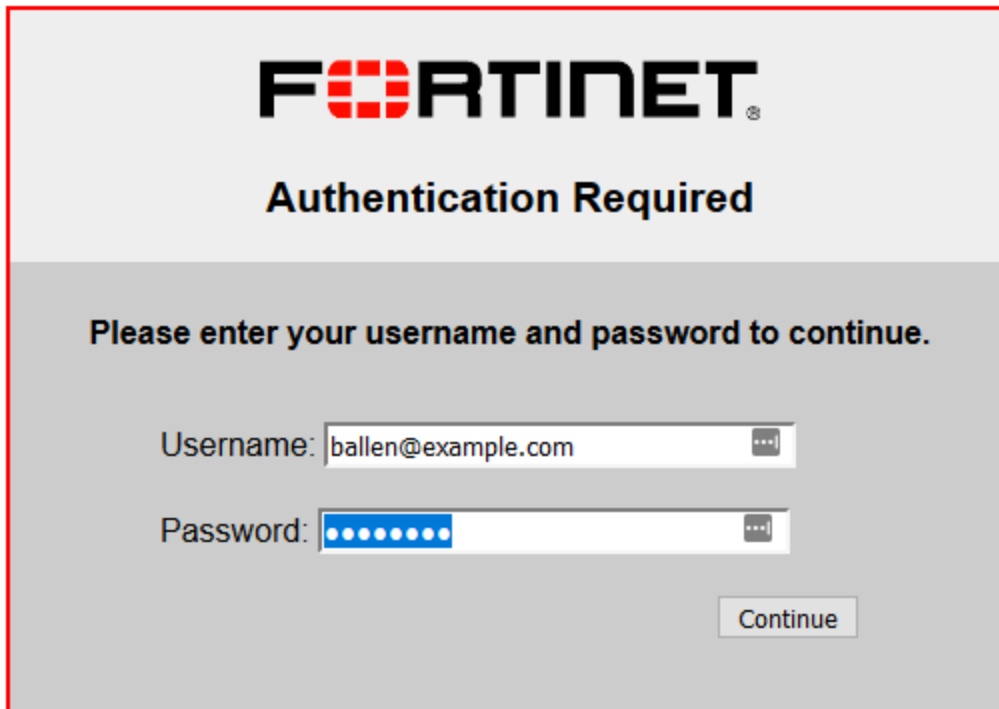
- After you select **OK**, a **User Created Successfully** notice appears that shows the new account's **Password**. This password can then be printed or emailed to the guest user. You can also view the password by editing the user account.

✓ User Created Successfully

| | |
|------------|---|
| User ID | ballen@example.com |
| Password | 8zck4zja |
| Email | ballen@example.com |
| Expiration | 5 Minutes |
| Send | <input type="button" value="Print"/> <input type="button" value="Email"/> |

Results

- On a PC, connect to the guest SSID and attempt to browse the Internet. When the authentication screen appears, log in using the guest user's credentials.



The image shows a Fortinet authentication interface. At the top is the Fortinet logo. Below it, the text "Authentication Required" is displayed. A message asks the user to enter their username and password. There are two input fields: "Username:" with the value "ballen@example.com" and "Password:" with masked characters. A "Continue" button is at the bottom right.

FORTINET

Authentication Required

Please enter your username and password to continue.

Username:

Password:

2. After the account is authenticated, you can connect to the Internet.
3. Five minutes after the initial login, the guest user account will expire and you will no longer be able to log in using those credentials.
4. Use the reception account to log on to the FortiGate. The guest account is listed as **Expired**.

| User ID | Expires |
|--------------------|---------|
| ballen@example.com | Expired |



FORTINET®



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.