GUIDE

McAfee® Unified Cloud Edge

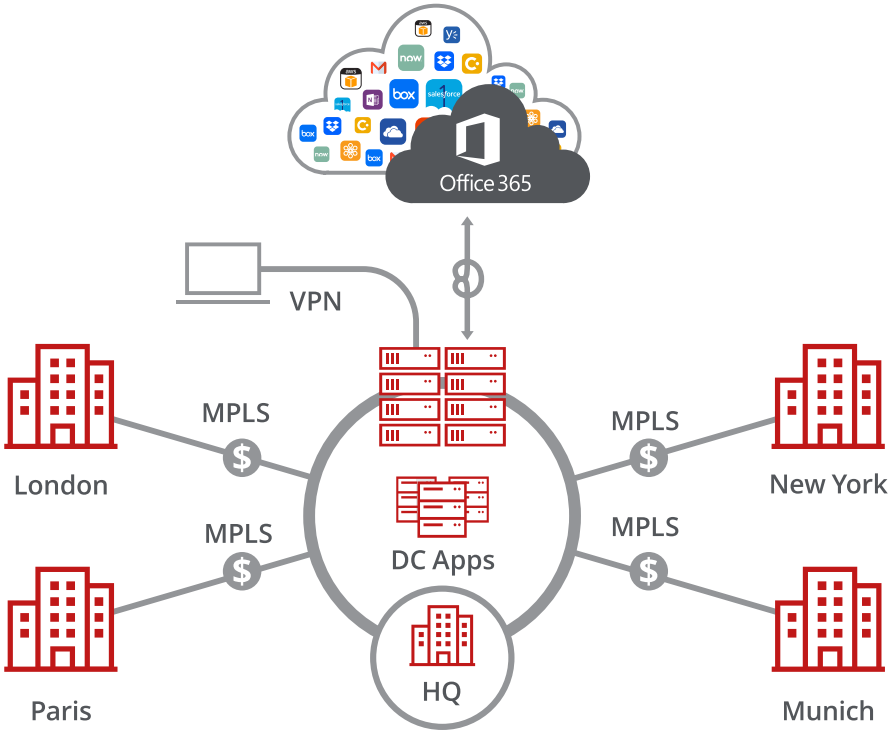
IPSec Configuration Fortinet FortiGate

Introduction to SD-WAN Architecture

A Software-Defined Wide Area Network (SD-WAN) is a virtual WAN architecture that simplifies the connectivity, management, and operation of a traditional WAN.

As more companies shift to cloud applications, the result is higher demand for bandwidth and direct internet connections to remote locations. Traditional MPLS networks are secure and stable, but expensive, and often fall victim to backhauling via the traditional hub and spoke architecture, where data is routed back through a central data center and out again to remote offices and users.

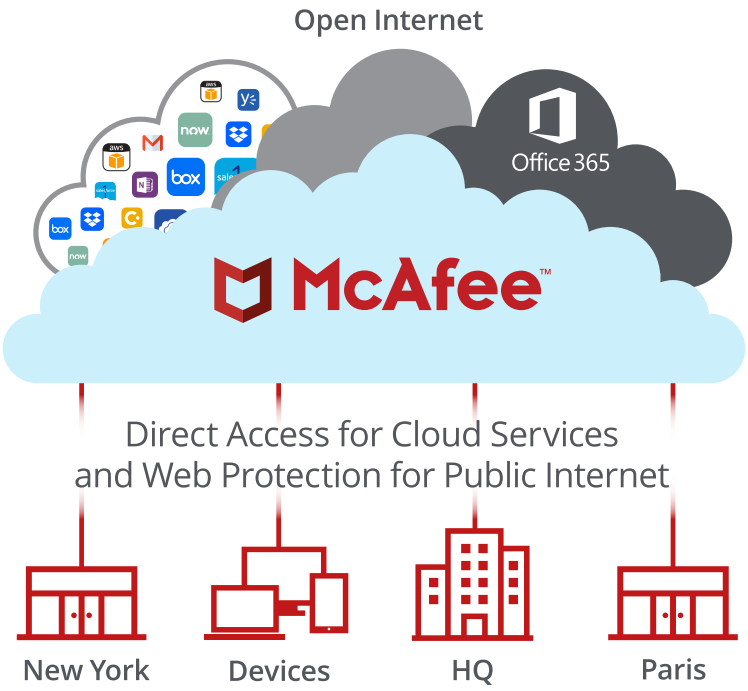
Hub and Spoke Architecture



SD-WAN combines traditional WAN technologies, such as MPLS and broadband connections, because it is abstracted from hardware. Organizations leverage SD-WAN solutions, because they provide enhanced capabilities for connectivity, monitoring, and managing network traffic while reducing cost.

McAfee® Unified Cloud Edge leverages SD-WAN technologies that allow remote offices to securely redirect web traffic to the McAfee® Web Gateway Cloud Service, where it is filtered according to your organization's web policy.

Direct to Cloud



This guide explains how to set up IPSec tunnels from Fortinet FortiGate to McAfee Web Gateway Cloud Service to apply policies and enable advanced security inspection.

Configuring IPsec site-to-site with Fortinet FortiGate

If your organization uses a supported third-party SD-WAN device to secure a remote office, you can use the IPsec protocol to secure communications between this site and McAfee® Web Gateway Cloud Service (McAfee® WGCS).

IPsec site-to-site overview

To secure communications between a remote site and McAfee WGCS using IPsec site-to-site authentication, you create an IPsec VPN tunnel between the supported SD-WAN device and the cloud service.

Environment

- McAfee® MVISION Unified Cloud Edge
- Fortinet FortiGate

Setup includes:

- Configuration of McAfee WGCS using the MVISION Unified Cloud Edge management console
- Configuration of the supported device

For information about configuring McAfee WGCS for IPsec site-to-site, see the McAfee Web Gateway Cloud Service Installation Guide for MVISION Unified Cloud Edge.

Considerations for configuring IPsec site-to-site

Before configuring IPsec site-to-site authentication, review the following considerations.

- **Routing only HTTP and HTTPS traffic** – McAfee WGCS only handles IPsec traffic directed through the VPN tunnel to ports 80 and 443 (HTTP and HTTPS traffic, respectively). Configure your device to route only HTTP and HTTPS traffic through the VPN tunnel.
- **Configuring two IPsec VPN tunnels** – Best practice is to configure a primary and secondary VPN tunnel. The primary tunnel is connected to the best available point of presence (PoP), while the secondary tunnel is connected to the second-best point of presence. This practice ensures continuous IPsec support in case one point of presence is not available.
- **Using an IPsec VPN tunnel to connect remote sites** – If you have multiple remote offices connected to your main office by VPN, you can protect traffic and improve network latency by creating a VPN tunnel between each site and McAfee WGCS.
- **Adding SAML authentication** – You can add a SAML configuration to an IPsec site. McAfee WGCS uses SAML to authenticate requests received from the site through the IPsec tunnel.
- **Using a NAT device** – If your IPsec device is located behind a NAT device and the outgoing interface has a private IP address, set the **Local ID** attribute to your public IP address.

Finding the best available points of presence

To find the point of presence closest to the device that you are configuring for IPsec authentication, you query the Global Routing Manager (GRM). The GRM is a DNS service that routes traffic to the best available point of presence.

From the network where your device is installed, run the nslookup command-line tool, as follows:

```
nslookup 1.network.wgcs.mcafee-cloud.com
```

```
nslookup 2.network.wgcs.mcafee-cloud.com
```

In response to these commands, the GRM returns the IP addresses of the best and second-best points of presence, respectively, based on the network location of your device. You need these values when configuring the primary and secondary IPsec VPN tunnels in your device and in McAfee WGCS.

Configure an IPsec VPN tunnel with Fortinet FortiGate

Configure the IPsec VPN tunnel in the Fortinet FortiGate web interface.

1. Create a VPN tunnel.
2. Configure the VPN tunnel.
3. View the status of the VPN tunnel.

Create an IPsec VPN tunnel with FortiGate

Create an IPsec VPN tunnel between the FortiGate device on the remote network and McAfee WGCS.

1. Log on to the web interface that you use to configure the FortiGate device on your remote network.
2. From the menu, select **VPN I IPsec I Tunnels**, then click **Create New**. The **VPN Creation Wizard** opens to the **VPN Setup** step.
3. In the **Name** field, specify a name for the VPN tunnel that you are configuring.
4. From the **Template** options, select **Site to Site • FortiGate**, then click **Next**.
5. Configure the Authentication settings:
   - **Remote Gateway** – Specify the IP address that McAfee WGCS uses for IPsec communications. IPsec communications are sent from the remote network to this address.
   - **Note:** To find the IP address of the point of presence closest to your device, use the nsLook-up command-line tool to query the Global Routing Manager.
   - **Outgoing Interface** – From this drop-down list, select the outgoing interface of the FortiGate device. **Example:** Port1
   - **Authentication Method** – Select **Pre-shared Key**.
   - **Pre-shared Key** – Specify the value of the key that you define and share with McAfee WGCS. This setting matches the Pre-Shared Key value that you specify when configuring the VPN tunnel in MVISION Cloud.
   - **Local ID** – Specify the IP address that matches the Client ID.
6. Click Next.
7. Configure the **Policy & Routing** settings:
   - Local Interface – From the drop-down list, select the local interface of the FortiGate device.
   - **Local Subnets** – Specify the internal IP address of the remote network in IPv4 format using CIDR notation with a network size range of 16-32 bits. IPsec communications are sent from McAfee WGCS to this address. This setting matches the Local Network value that you specify when configuring the VPN tunnel in McAfee WGCS.
   - **Remote Subnets** – Specify the range of requested IP addresses that are sent through the VPN tunnel to McAfee WGCS. To make sure that all traffic is sent to McAfee WGCS through the tunnel, specify this value: 0.0.0.0/0.
8. Choose **Remote** as internet.
9. Click **Create**.

The VPN Creation Wizard displays this message: The VPN has been set up.

Configure the IPsec VPN tunnel for FortiGate

Configure the IPsec VPN tunnel using the values that MVISION Cloud supports.

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **VPN I IPsec I Tunnels**.
3. Select the tunnel you created, then click **Edit**.
4. Click **Convert to Custom Tunnel**.
5. Under the **Authentication** heading, set the **IKE Version** to 2.
6. Under the **Phase 1 Proposal** heading:
   a. Remove the two 3DES entries from the list.
   b. Verify that Group 5 is selected.
7. Under the Phase 2 Selectors heading, verify that the **Local Address** and **Remote Address** settings are correct.
8. To open the **Phase 2 Proposal** settings, click Advanced, then:
   a. Remove the two **3DES** entries from the list.
   b. Verify that **Group 5** is selected.
9. Click **OK**.

IPsec VPN configuration options

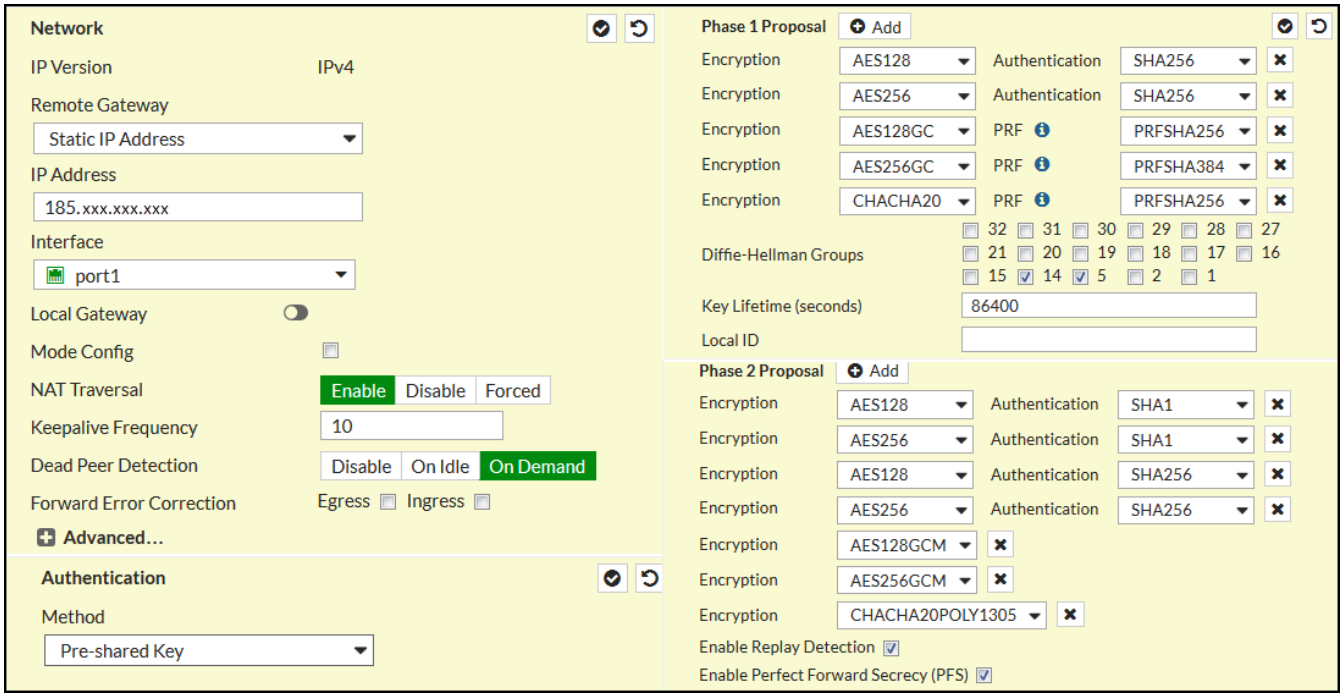
You use one of the following options when configuring IPsec site-to-site authentication in the FortiGate web interface. Then you select the same option from the Client ID Type drop-down list when configuring IPsec site-to-site in the MVISION Cloud UI.

- Specific IPv4 Address
- Fully Qualified Domain Name
- User FQDN

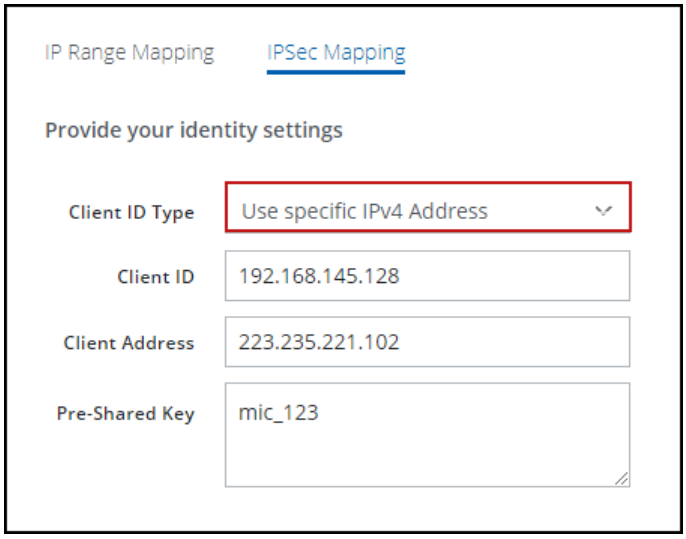
Specific IPv4 Address

This screenshot shows how to configure IPsec site-to-site authentication in the FortiGate web interface when you select **Specific IPv4 Address** as the **Client ID Type** in the MVISION Cloud UI.

Note: When using this option to configure FortiGate, make sure to leave the **Local ID** field empty.

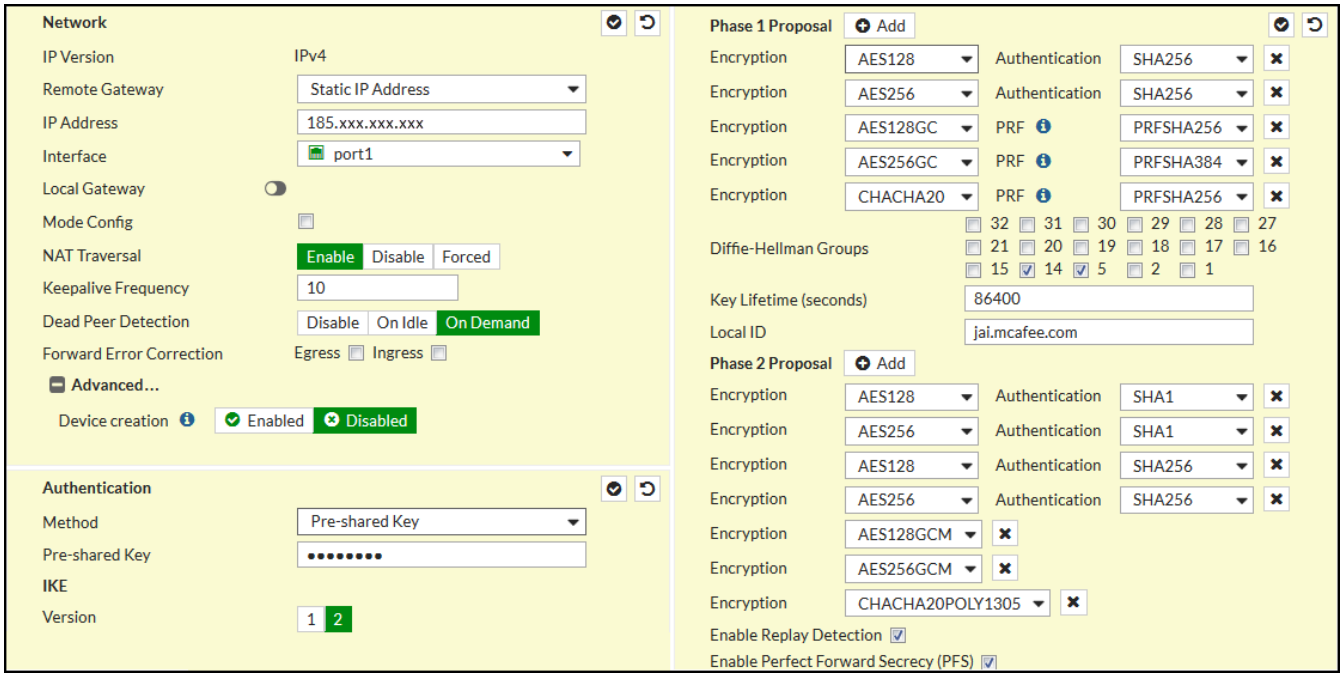


To configure IPsec site-to-site authentication in the MVISION Cloud UI, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

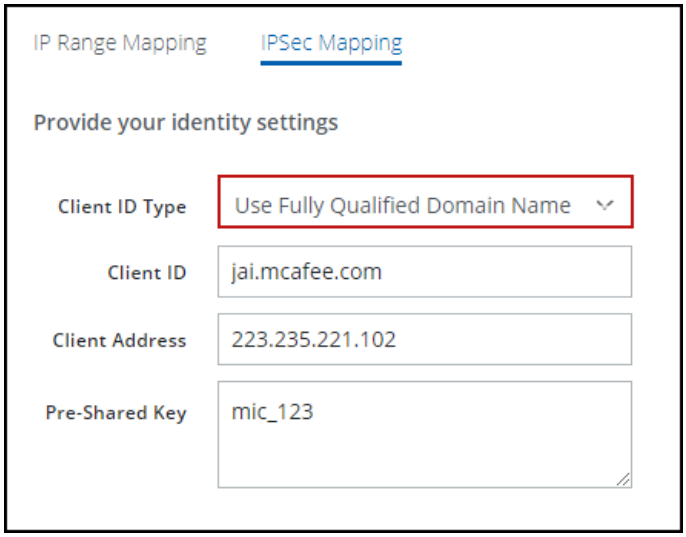


Fully Qualified Domain Name

This screenshot shows how to configure IPsec site-to-site authentication in the FortiGate web interface when you select **Fully Qualified Domain Name** as the **Client ID Type** in the MVISION Cloud UI.

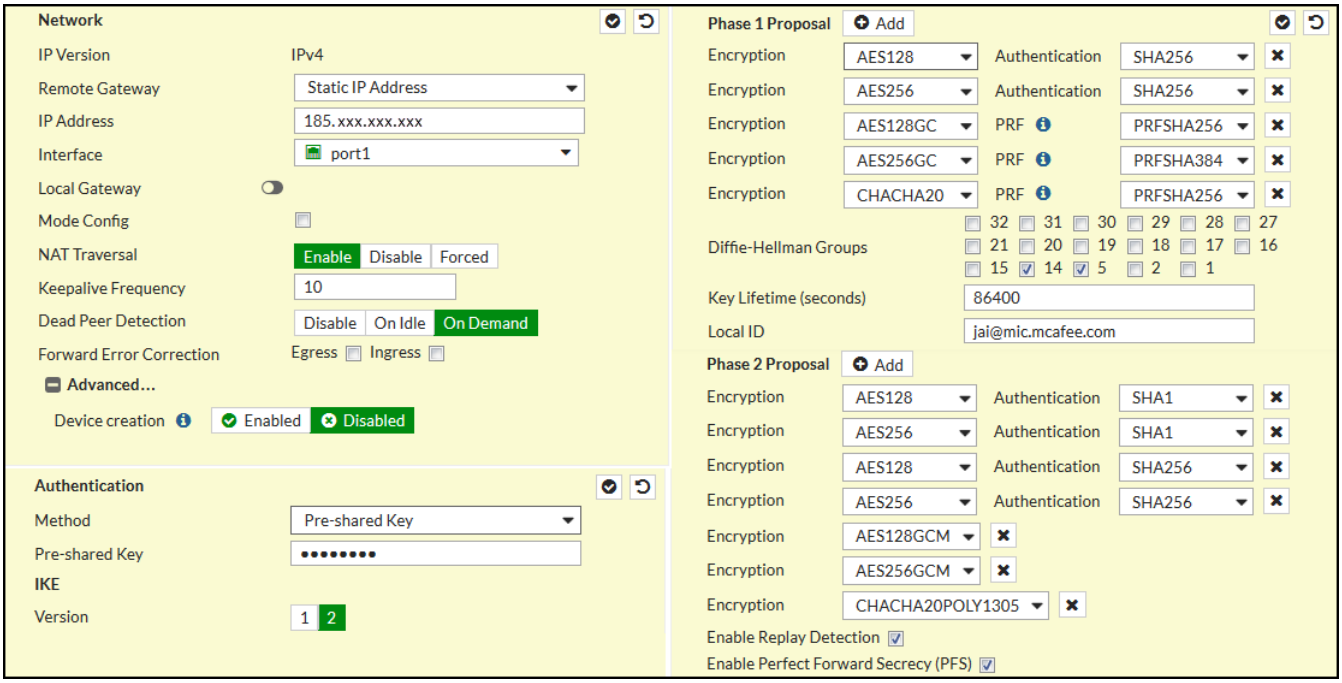


To configure IPsec site-to-site authentication in the MVISION Cloud UI, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.

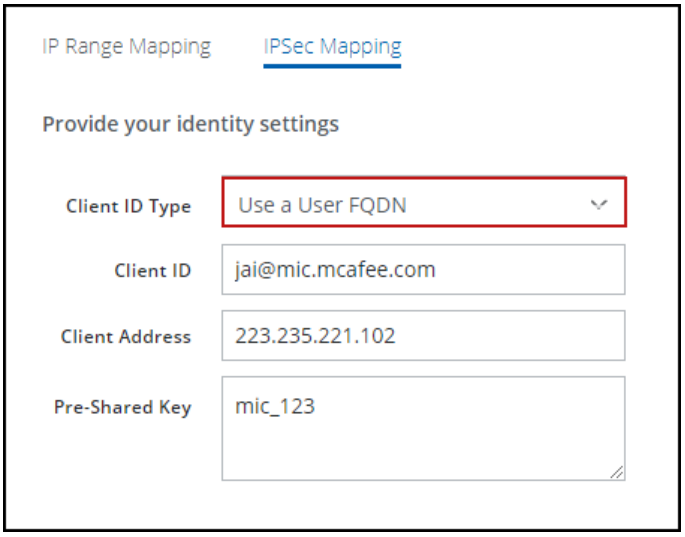


User FQDN

This screenshot shows how to configure IPsec site-to-site authentication in the FortiGate web interface when you select **User FQDN** as the **Client ID Type** in the MVISION Cloud UI.



To configure IPsec site-to-site authentication in the MVISION Cloud UI, select **Settings | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping**.



View the status of the tunnel configured with FortiGate

To verify that the IPsec VPN tunnel with FortiGate is correctly configured, view the status of the tunnel.

Task

1. Open the web interface that you use to configure the FortiGate device on your network.
2. Select **VPN I Monitor I IPsec Monitor**.
3. In the table, locate the VPN tunnel in the **Name** column.

In the **Status** column, a green icon and up arrow show that the VPN tunnel is configured correctly.

FortiGate 64D static and policy routes

Complete these tasks to create and configure the static and policy routes for FortiGate.

1. Create a static route for FortiGate
2. Create a policy route for FortiGate
3. Configure the policy route for FortiGate

Create a static route for FortiGate 64D

The FortiGate device uses the static route to direct IPsec packets through the VPN tunnel that you create and configure.

Task

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **Network I Static Routes**, then click **Create New**.
3. Configure these settings:
   - **Destination** – Specify the IP address that McAfee WGCS uses for IPsec communications. This setting matches the Remote Gateway value that you configure when creating the VPN tunnel in the FortiGate interface.
     To find the IP address of the point of presence closest to your device, use the nslookup command-line tool to query the Global Routing Manager.
   - **Gateway** – Specify the FortiGate outbound IP address. This setting matches the External IP value that you specify when configuring the VPN tunnel in McAfee WGCS.
4. Expand the **Advanced Options**, then specify a value for the **Priority** setting. Review these considerations:
   - The static route with the lowest priority value has the highest priority.
   - Specify a value that is greater than the priority configured for the default static route, so that the default static route always has a higher priority.
   - When configuring static routes for multiple VPN tunnels, the routes can have the same priority value.
5. Click **OK**.

Create a policy route for FortiGate

The FortiGate device uses the policy route to determine whether TCP packets are directed through the VPN tunnel or to the Internet.

- **TCP packets going to ports 80 and 443** – Using the static route, the device directs these packets through the VPN tunnel.
- **All other packets** – Using the default static route, the device directs these packets to the Internet.

Task

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **Network I Policy Routes**, then click **Create New**.
3. Under **If incoming traffic matches**, configure these settings:
   - **Protocol** – Select TCP.
   - **Incoming interface** – From the drop-down list, select **internal**.
   - **Source address | mask** – Specify the internal IP address of your network in IPv4 format using CIDR notation with a network size range of 16-32 bits. IPsec communications are sent from McAfee WGCS to this address. This setting matches the Local Network value that you specify when configuring the VPN tunnel in McAfee WGCS.
   - **Destination address | mask** – Specify the range of requested IP addresses that are sent through the policy route to McAfee WGCS. To ensure that all traffic is sent to McAfee WGCS through this route, specify this value: 0.0.0.0/0.
4. Under **Then**, configure these settings:
   - **Action** – Select **Enable Forward Traffic**.
   - **Gateway address** – Specify the outgoing interface of the FortiGate device.
5. Click **OK**.

Configure the policy route for FortiGate

Configure the policy route so that the FortiGate device only routes TCP packets going to ports 80 and 443 (HTTP and HTTPS traffic, respectively) through the IPsec VPN tunnel.

Task

1. Open the web interface that you use to configure the FortiGate device on your network.
2. From the menu, select **Policy & Objects | IPv4 Policy**.
3. Select the policy route that you created, then click **Edit**.
4. From the **Service** drop-down list: Under **Web Access**, select **HTTP**.
5. Click the **Add** icon, then under **Web Access**, select **HTTPS**.
6. Click **OK**.

McAfee™
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com