GUIDE

McAfee® Unified Cloud Edge

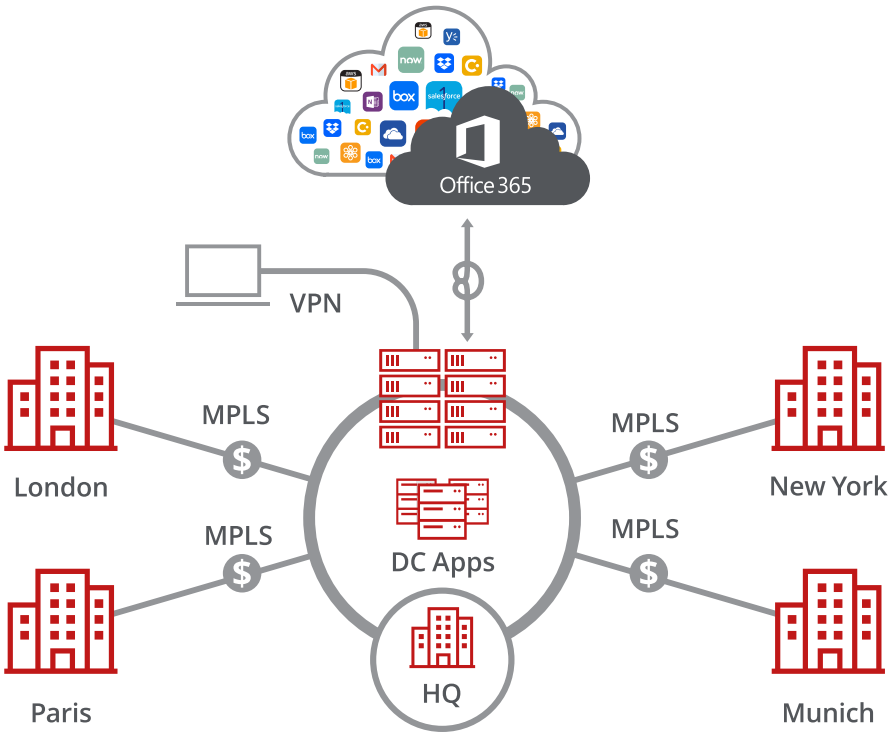
IPSec Configuration VeloCloud

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.

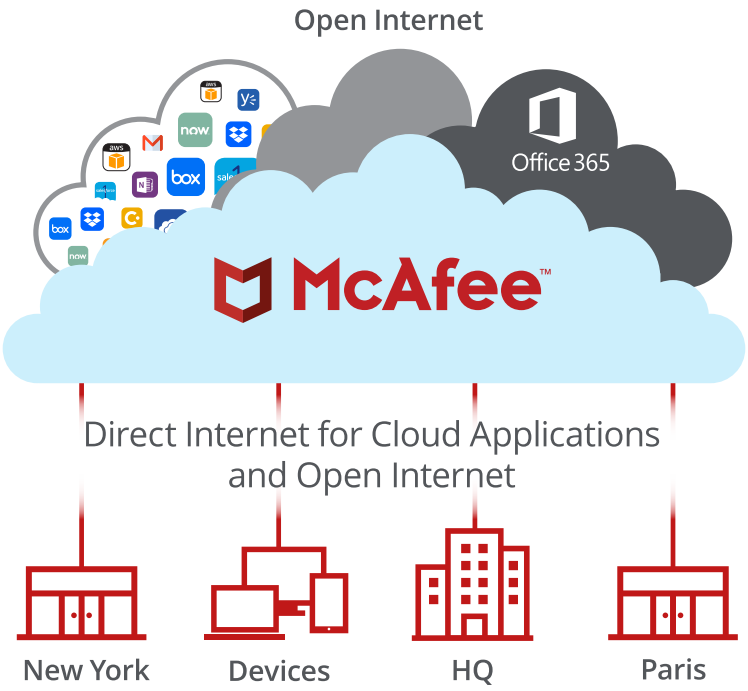
Hub and Spoke Architecture



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 VMware VeloCloud version 4.0 to McAfee Web Gateway Cloud Service to apply policies and enable advanced security inspection.

Configure IPsec site-to-site with VeloCloud 4.0

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
- VMware VeloCloud Orchestrator

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 PoP. 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:

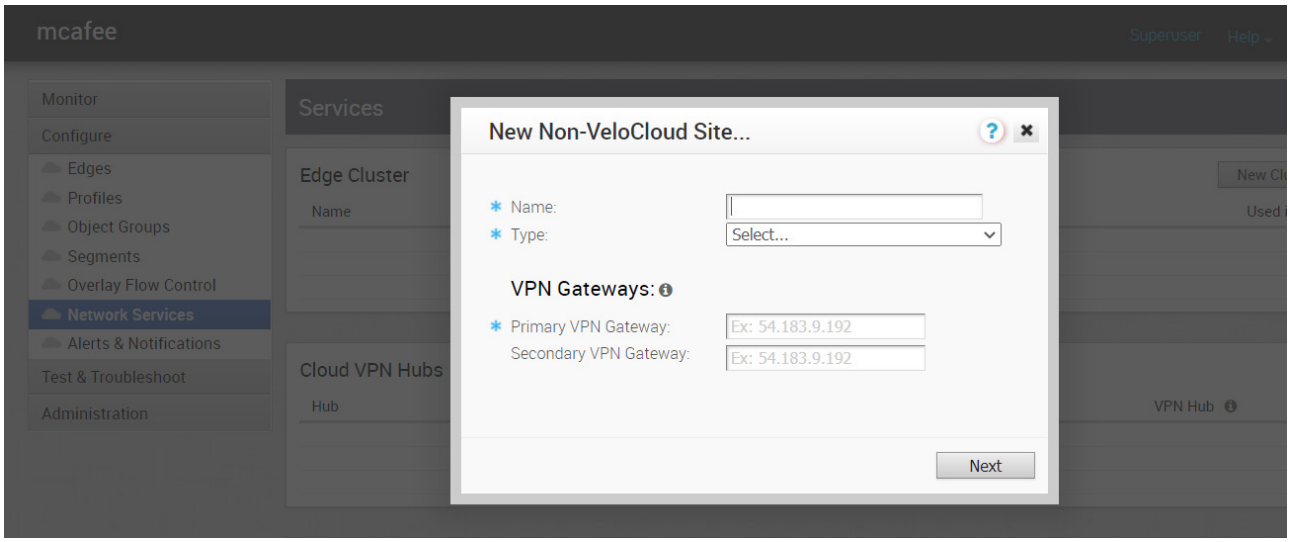
```
nslookup 1.network.wgcs.mcafee-cloud.com
```

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

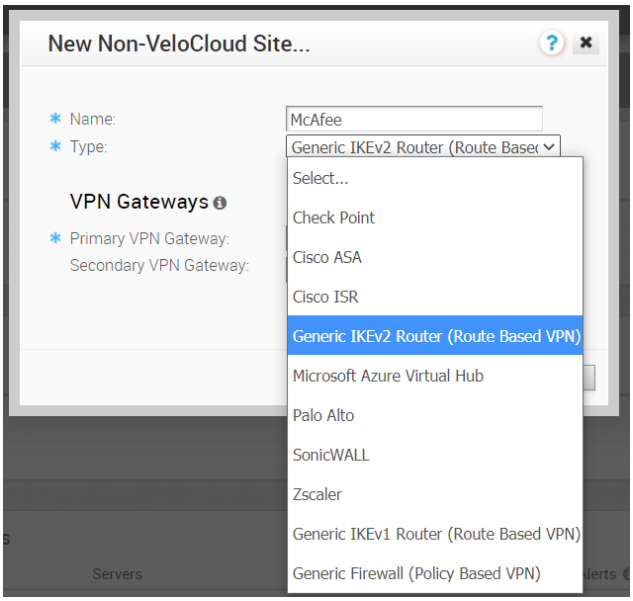
In response to these commands, the GRM returns the IP addresses of the best and second-best PoP, respectively, based on the network location of your device. You need these values when configuring the primary and secondary IPsec VPN tunnels in your device and in McAfee WGCS.

Configure an IPsec VPN tunnel with VMware VeloCloud Orchestrator

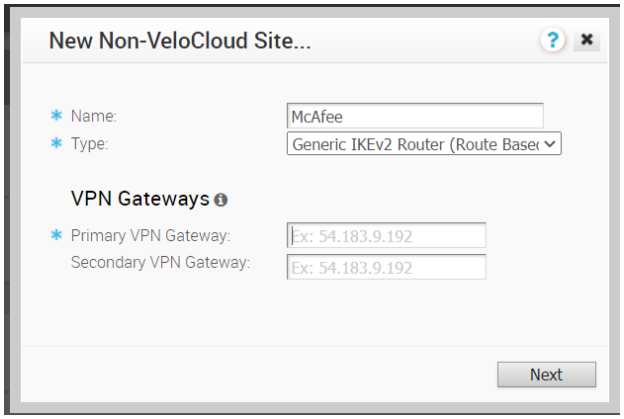
1. In SD-WAN VeloCloud Orchestrator, click **Configure | Network Services**.
2. Click **New** in Non-VeloCloud Sites to create a new site.



3. Enter the name of the site in the **Name** field.
4. Select **Generic IKEv2 Router** from the **Type** drop-down list.



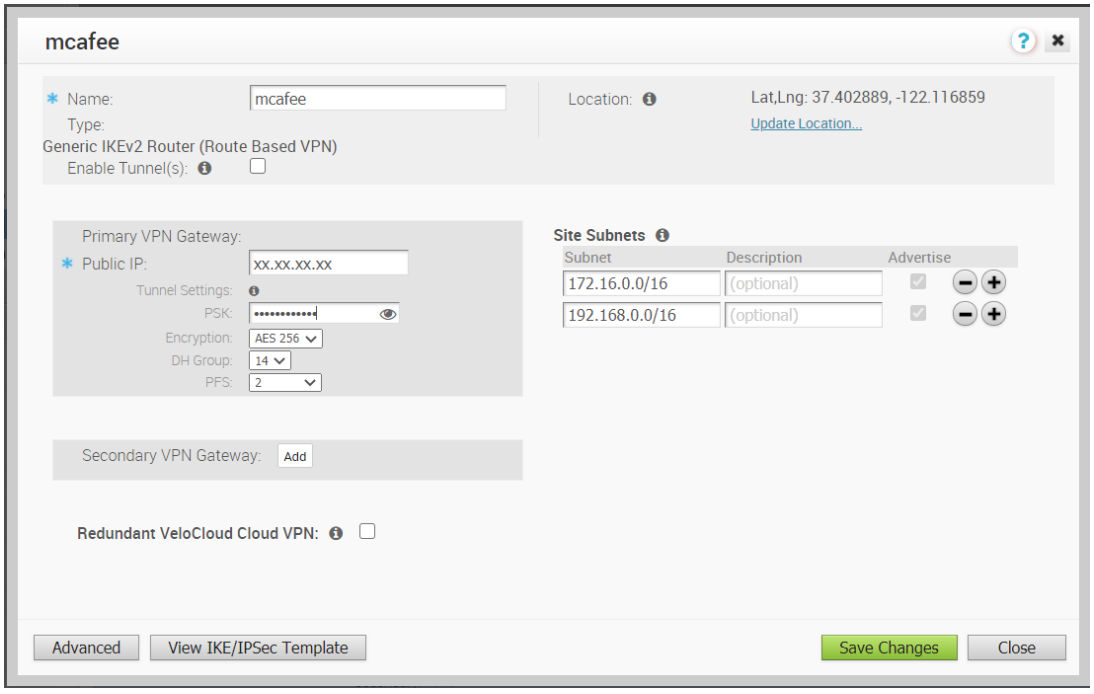
5. Enter an IPv4 address in the **Primary VPN Gateway** field.



6. Click **Next**.
   VeloCloud creates the site and generates the IKE and IPsec configuration (including pre-shared key) for the site.
7. Click **Advanced**.
8. Update the IKE and IPsec parameters and add the Site Subnets that you will protect.

   PSK: Configure shared Secret
   Encryption: AES 256
   DH Group: 14
   PFS: 2

9. Select the **Enable Tunnel(s)** check box.
10. Click **Save Changes**.

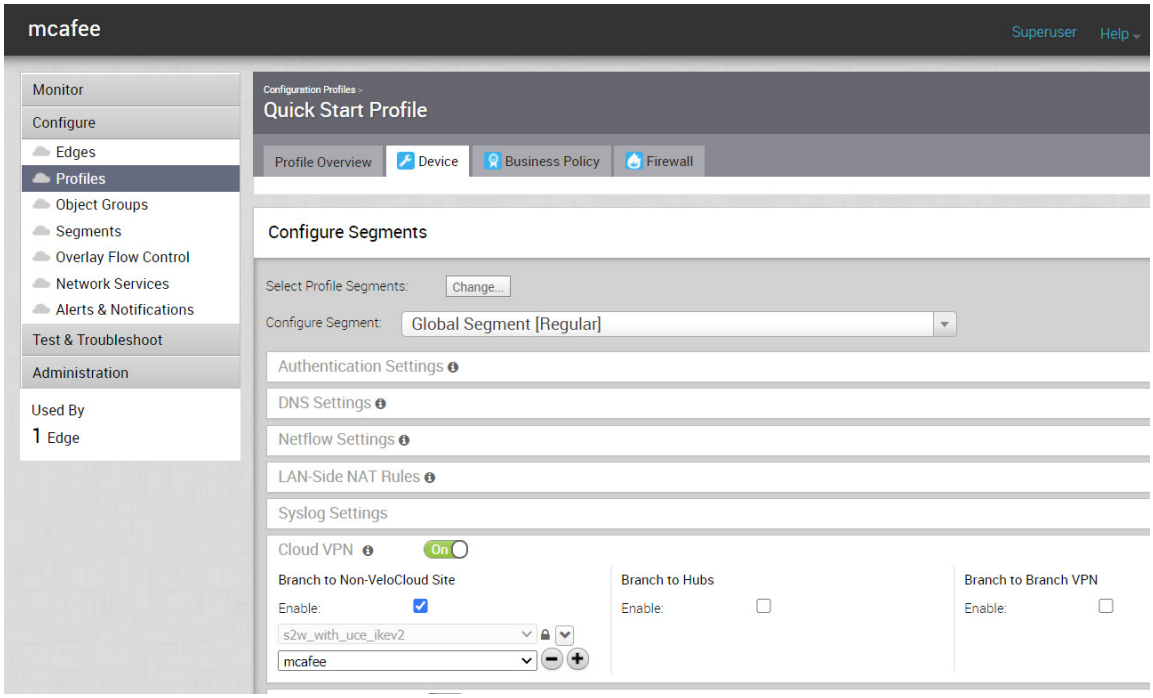


To view the detailed IKE, IPsec parameters, and the public IP address used by the VeloCloud gateway, click **View IKE/IPSec Template**.

Configure the customer profile

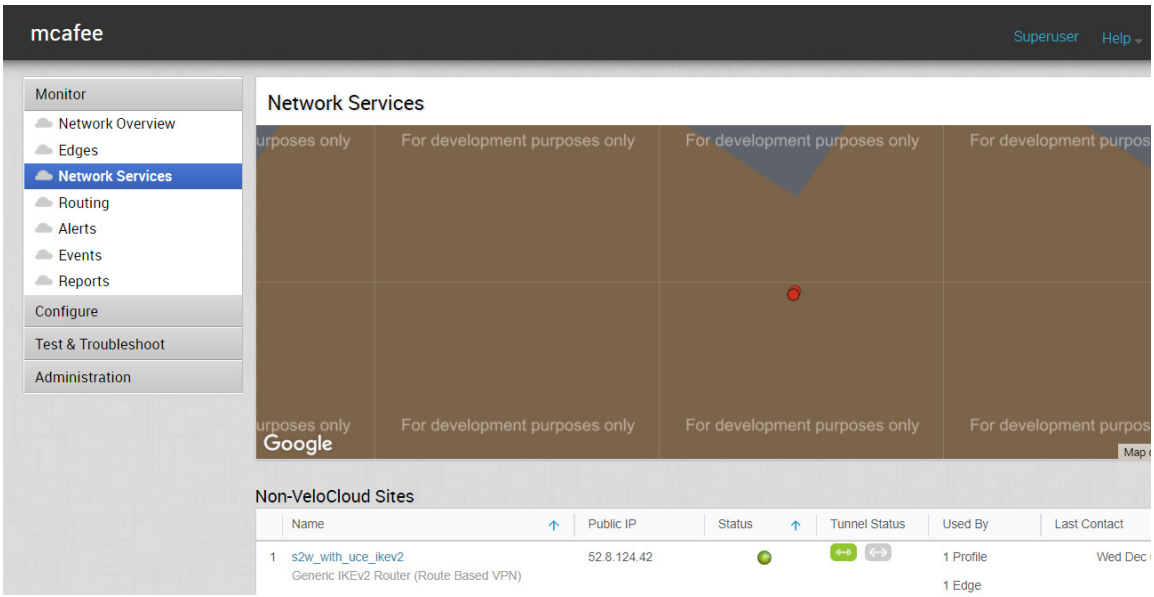
You can configure the customer profile to service-chain the Non-VeloCloud site to the customer's SD-WAN.

1. Select **Configure | Profiles | Profile-Name**, where Profile-Name is the customer's profile.
2. Click the **Device** tab.
3. Enable the **Cloud VPN** feature to turn on VPN connectivity from the Branch and Data Center sites.
4. In the **Branch to Non-VeloCloud Site** section, click **Enable** and then select **Non-VeloCloud Site**.
5. **Save** your changes.



6. **Verify** the status of the remote network tunnel.

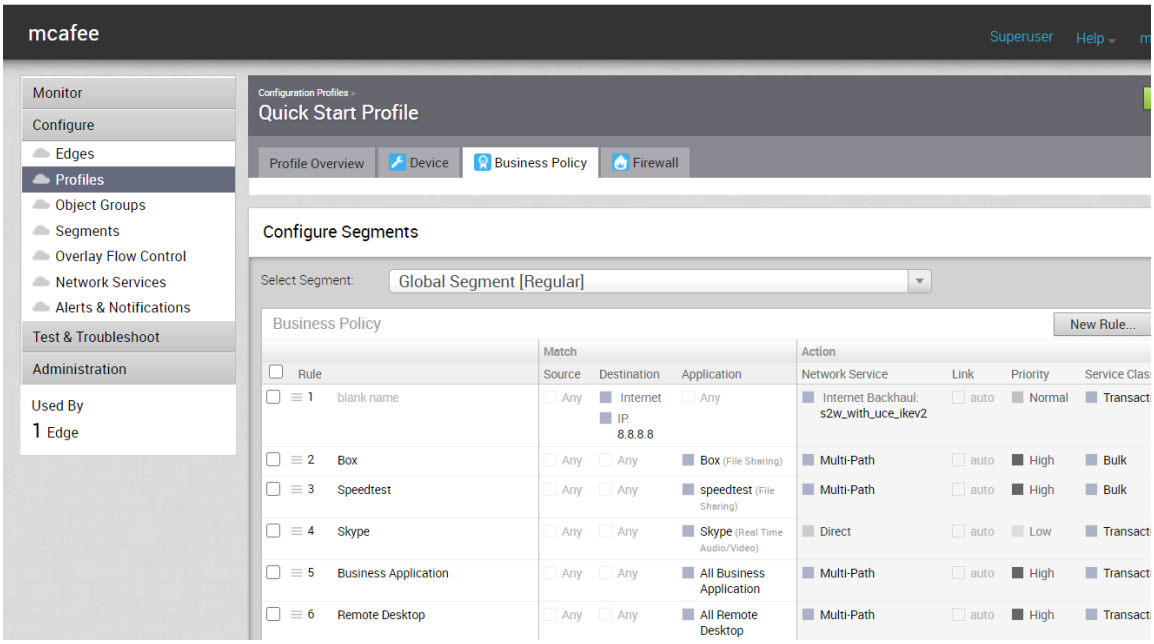
To view tunnel status in the VMware SD-WAN Orchestrator, select **Monitor Edge** in the VMware SD-WAN Orchestrator.



Route the traffic

To define routes from your branch office IPsec tunnels to McAfee server for the traffic:

1. In **Profiles | Business Policy**, click **New Rule**.



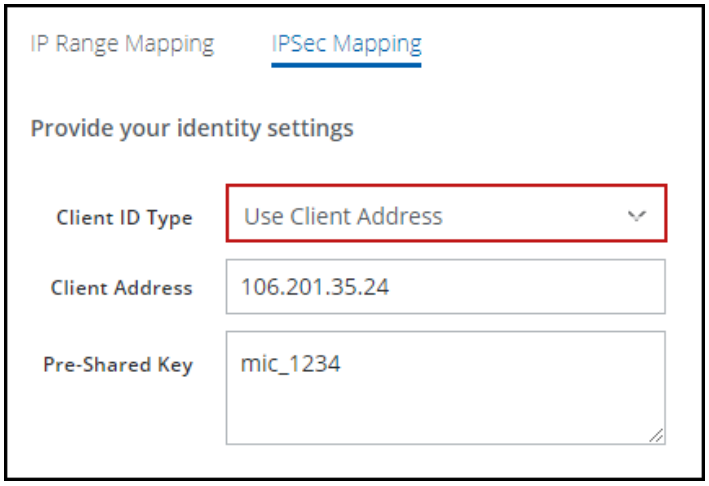
2. Enter the relevant information to configure the new rule
3. To add two sites that represent tunnels, navigate to **Edges | Device** and click **Add**.
4. Click **Save Changes**.

IPsec VPN configuration options

You use one of the following options when configuring IPsec site-to-site authentication in the EdgeConnect 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.

Client Address

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



6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com