Integration Guide

VeloCloud SD-WAN Forcepoint SSE

Services

Arista.com

Arista Networks

DOC-08381-01

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

© Copyright 2025 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

Chapter 1: Arista VeloCloud SD-WAN and Forcepoint SSE Integration Guide.....1

Chapter 2: Overview.....2

Chapter 3: System Requirements.....3

Chapter 4: Configure Forcepoint Cloud Security Gateway..... 4

Chapter 5: Configure Tunnels on VeloCloud Gateway..... 7

5.1 Configure Non SD-WAN Destination via Gateway.....7
5.2 Configure Profile with Non SD-WAN Destination via Gateway.....12
5.3 Create Business Policy for Non SD-WAN Destination via Gateway.....13
5.4 Monitor Non SD-WAN Destination via Gateway.....15

Chapter 6: Configure Tunnels on VeloCloud Edge..... 16

6.1 Configure Non SD-WAN Destination via Edge.....16
6.2 Configure Profile with Non SD-WAN Destination via Edge.....19
6.3 Create Business Policy for Non SD-WAN Destination via Edge.....19
6.4 Configure Edge with Tunnel Parameters.....21
6.5 Monitor Non SD-WAN Destination via Edge.....23

Chapter 7: Verify the Status of IPsec Tunnels.....24

Chapter 8: Validate End to End Integration..... 25

Appendix A: References.....26

A.1 Related Documents.....26

Chapter 1

Arista VeloCloud SD-WAN and Forcepoint SSE Integration Guide

The Arista VeloCloud SD-WAN™ and Forcepoint SSE (Security Service Edge) Integration Guide describes the configurations required to integrate Forcepoint Cloud Security Gateway with the VeloCloud Edge Cloud Orchestrator.

Chapter 2

Overview

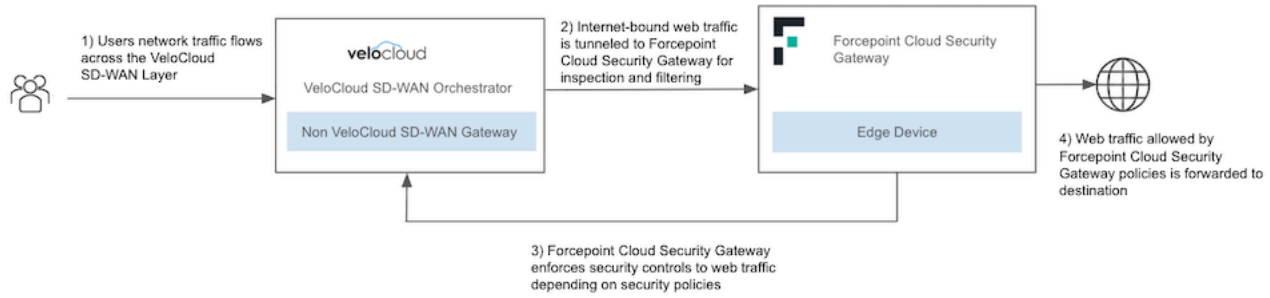
You can integrate Forcepoint Cloud Security Gateway with VeloCloud SD-WAN so that Internet-bound web traffic flowing over the SD-WAN layer is filtered by Forcepoint Cloud Security Gateway according to customizable security policies.

The integration of Forcepoint Cloud Security Gateway with VeloCloud SD-WAN enables system administrators to perform the following:

- Configure VeloCloud Edge Cloud Orchestrator to connect and route web traffic to Forcepoint Cloud Security Gateway using either a Gateway or an Edge device.
- Configure Forcepoint Cloud Security Gateway to connect to VeloCloud SD-WAN and apply web security policies to traffic received from VeloCloud SD-WAN.

The following image shows the workflow between the components involved in the integration.

Figure 2-1: Example Workflow



Chapter 3

System Requirements

Ensure you have the following products installed and configured:

- Forcepoint Cloud Security Gateway
- VeloCloud SD-WAN 4.0 or later.

The configuration does not require other software or physical devices to integrate Forcepoint Cloud Security Gateway with VeloCloud SD-WAN. For additional information on installing and configuring the products, refer to the following documentation:

- Forcepoint Cloud Security Gateway
- *VeloCloud SD-WAN*

Chapter 4

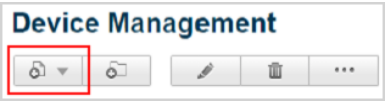
Configure Forcepoint Cloud Security Gateway

The configuration requires a configured **Edge Device** to route traffic from VeloCloud SD-WAN to Forcepoint Cloud Security Gateway for inspection and filtering.

To create a new **Edge Device** in Forcepoint Cloud Security Gateway:

1. Login to **Forcepoint Cloud Security Gateway** using an account with administrative privileges.
2. Navigate to **Web** > **Device Management**, select the drop-down Icon under the headline, and select **Add Edge Device**.

   Figure 4-1: Adding an Edge Device



3. In the **Tunneling Type** window, select **IPsec Advanced** and configure the following settings:

Figure 4-2: Selecting the Tunneling Type

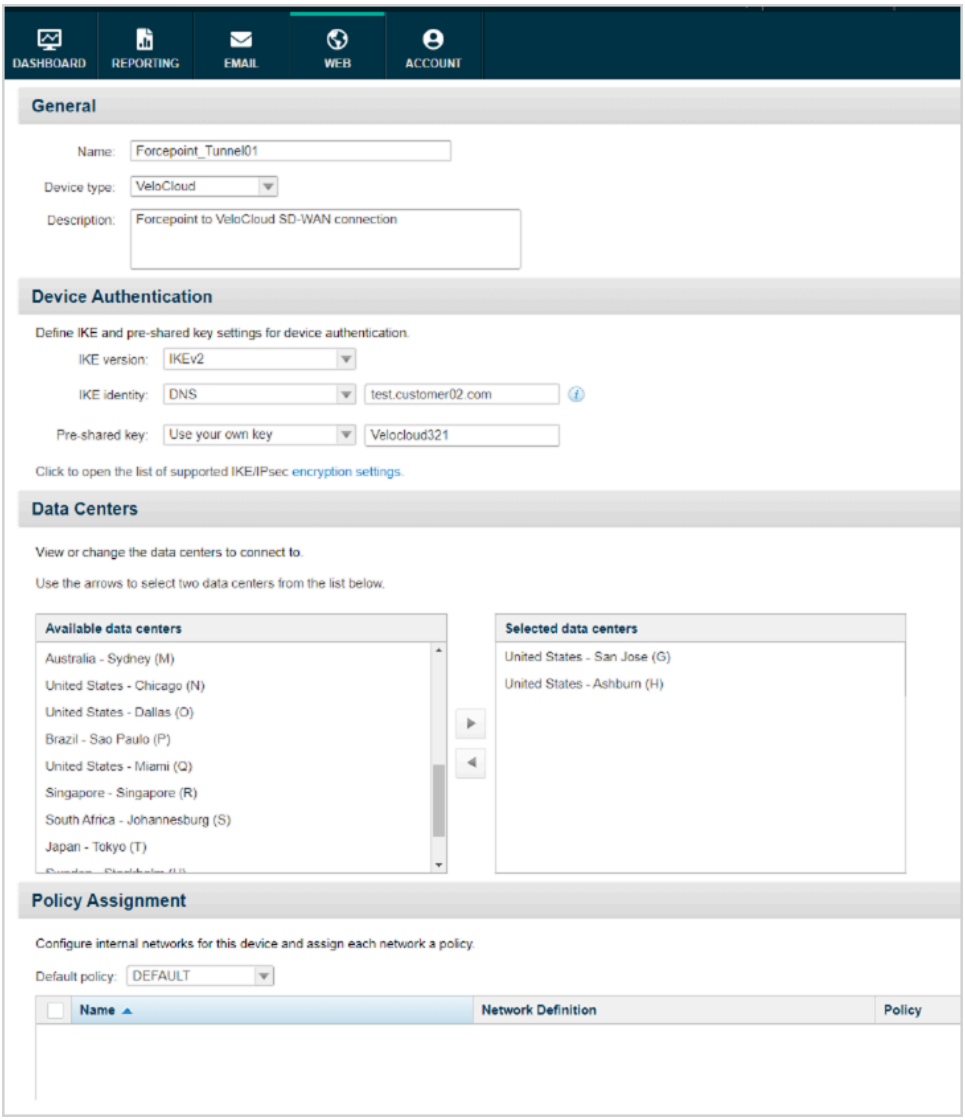
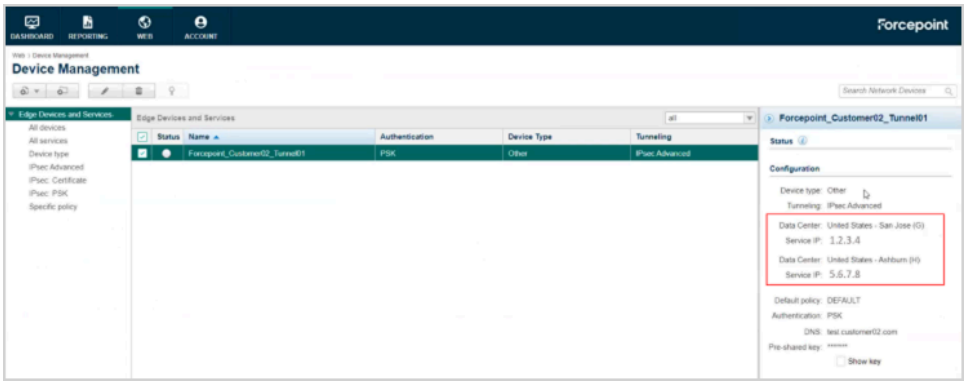


Table 1: Tunnel option Descriptions

Option	Description
Name	Enter a descriptive name to identify the connection of the Edge.
Device type	Select **VeloCloud** from the list.
Description	You can enter more details describing the connection.
IKE version	Select **IKEv2** from the list.
IKE identity	Select **DNS** and enter a DNS name within your namespace to configure on the VeloCloud SD-WAN as well.
Pre-shared key	Select **Use your own key** and enter the same key to use on the VeloCloud SD-WAN.
Data Centers	Select any two data centers close to the location of VeloCloud Edges, from **Available data centers** and move them to the **Selected data centers** pane. The latency is minimal when you choose the data centers close to the VeloCloud Edges.
Policy Assignment	Select a default policy from the list, that applies to all traffic coming from the VeloCloud Edges.

4. After configuring the settings, select **Save**.
5. In the **Device Management** page, select the newly created **Edge Device** and note the **Service IP** of both the Data Centers from the **Status** menu. The VeloCloud SD-WAN configuration requires these details.

   Figure 4-3: Device Management



   The **Edge Device** on Forcepoint Cloud Security Gateway waits for connections initiated by the VeloCloud Gateway.

Configure the components of the VeloCloud Edge Cloud Orchestrator to connect the Forcepoint Cloud Security Gateway to one of the following:

- Gateway – See Configure Tunnels on VeloCloud Gateway
- Edge – See Configure Tunnels on VeloCloud Edge

Chapter 5

Configure Tunnels on VeloCloud Gateway

Configure the SD-WAN layer of Orchestrator using a Gateway as the endpoint for the tunnels between VeloCloud SD-WAN and Forcepoint Cloud Security Gateway. Ensure that you have configured the customer.

5.1 Configure Non SD-WAN Destination via Gateway

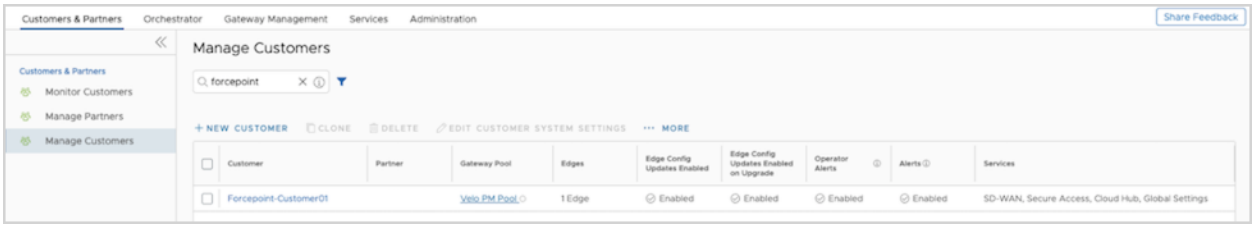
You can define and configure a Non SD-WAN Destination instance as Forcepoint Cloud Security Gateway and establish a secure IPsec tunnel to the Forcepoint Cloud Security Gateway through a VeloCloud Gateway.

Ensure that you have Administrator privileges to login to VeloCloud Edge Cloud Orchestrator.

To configure a Non SD-WAN Destination via Gateway:

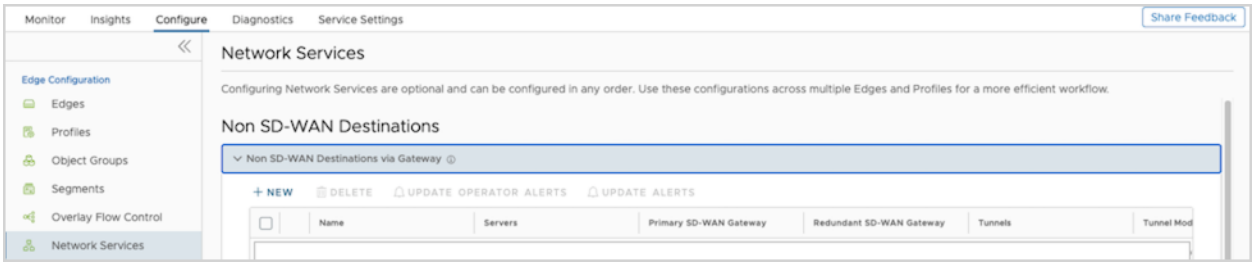
1. Login to Orchestrator and navigate to **Manage Customers**.

   Figure 5-1: Managing Customers



2. Select the link to a customer whose traffic would be routed to Forcepoint Cloud Security Gateway.
3. In the Enterprise portal, select **Configure** > **Network Services**.
4. In the **Non SD-WAN Destinations via Gateway** pane, select **New** to create a new Non SD-WAN Destination.

   Figure 5-2: Creating a New Non SD-WAN Destination



5. In the **New Non SD-WAN Destination via Gateway** window, configure the following:

Figure 5-3: Adding New Non SD-WAN Destination Parameters

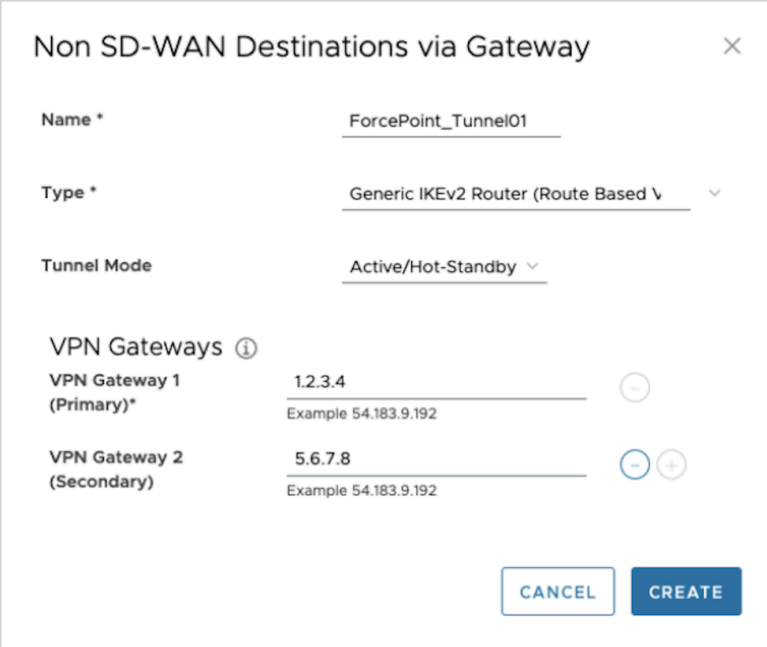


Table 2: New Non SD-WAN Destination Parameters Option Descriptions

Option	Description
Name	Enter a descriptive name for the Non SD-WAN Destination.
Type	Select the type as **Generic IKEv2 Router (Route Based VPN)**.
Primary VPN Gateway	Enter the IP address of the first data center from the Forcepoint Cloud Security Gateway **Edge Device** configuration.
Secondary VPN Gateway	Enter the IP address of the second data center from the Forcepoint Cloud Security Gateway **Edge Device** configuration.

6. Select **Next**.

7. In the next window, configure the following settings:

Figure 5-4: Configuring ForcePoint Tunnels - Example 1

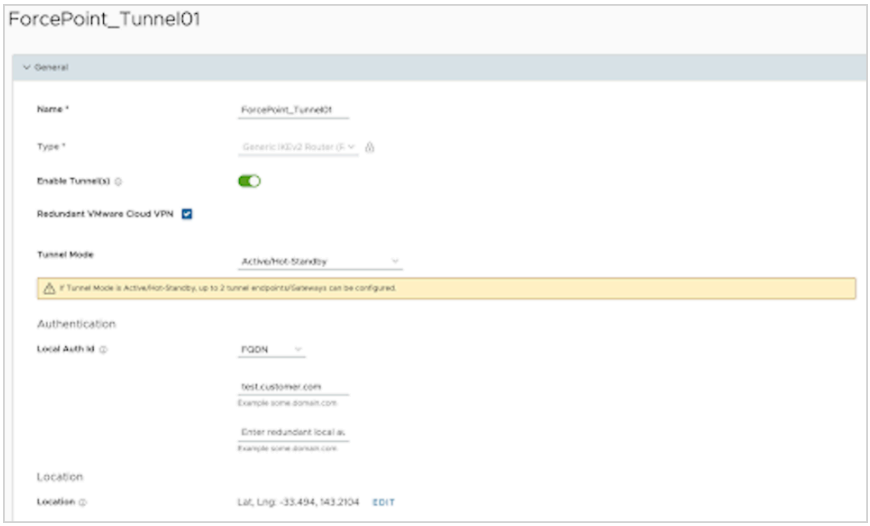


Figure 5-5: Configuring ForcePoint Tunnels - Example 2

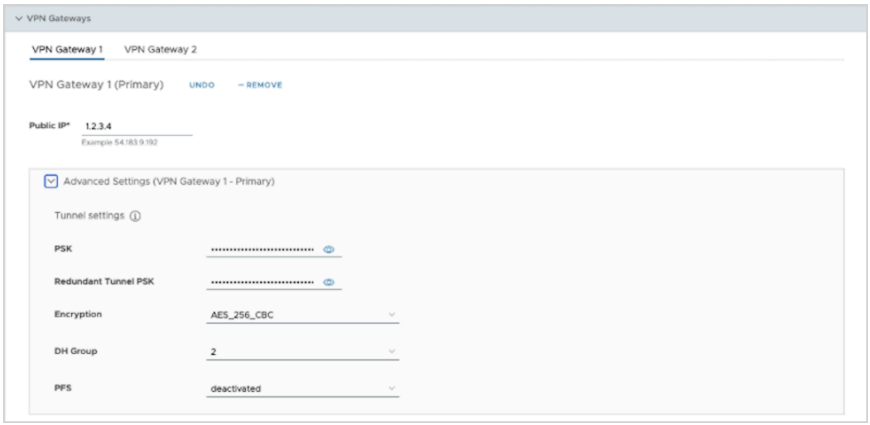
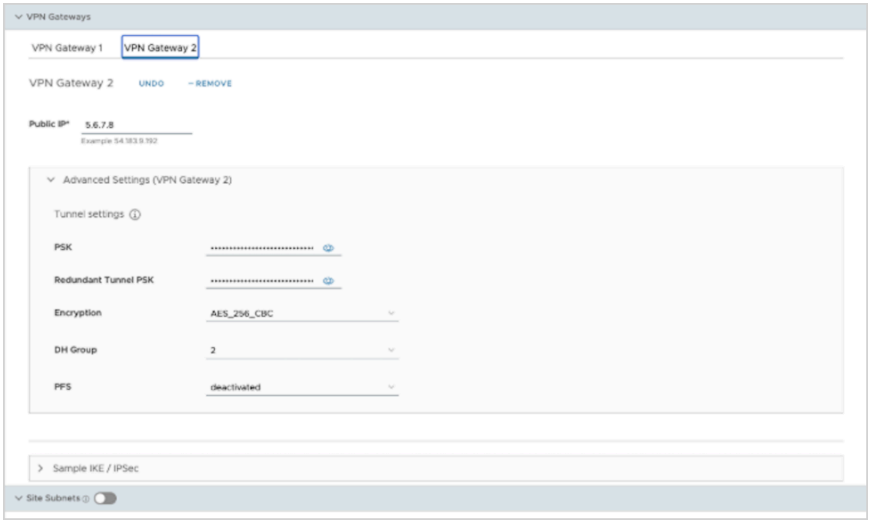


Figure 5-6: Configuring ForcePoint Tunnels - Example 3



The **Name** and **Type** of the Non SD-WAN Destination are displayed. Select the **Enable Tunnel(s)** checkbox to enable the tunnel.

Select **Advanced** to configure the other IPsec tunnel parameters for the Primary and Secondary VPN Gateways as follows:

Table 3: Additional IPsec Tunnel Option Descriptions

Option	Description
PSK	Enter the pre-shared key used in configuring the **Edge Device** in the Forcepoint Cloud Security Gateway.
Redundant Tunnel PSK	Repeat entering the pre-shared key.
Encryption	Select **AES-256** as the AES algorithms key from the drop-down list, to encrypt data.
DH Group	Select the Diffie-Hellman (DH) Group algorithm to be used when exchanging the pre-shared key. The DH Group sets the strength of the algorithm in bits.
PFS	Select the Perfect Forward Secrecy (PFS) level as **deactivated**.
Hash	Select the authentication algorithm for the VPN header as **SHA 256** from the drop-down list.
IKE SA Lifetime(min)	Enter the IKE SA lifetime in minutes. The rekeying should be initiated for Edges before the time expires. The range is from 10 to 1440 minutes. The default value is 1440 minutes.
IPsec SA Lifetime(min)	Enter the IPsec SA lifetime in minutes. The rekeying should be initiated for Edges before the time expires. The range is from 3 to 480 minutes. The default value is 480 minutes.
DPD Timeout Timer(sec)	Enter the DPD timeout value. The DPD timeout value to add to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection). Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value. • Library Name: Quicksec • Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec) • Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, 0.5+1+2+4+8+16+16 = 47.5). • Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec **Note:** Prior to the 5.1.0 release, you can deactivate DPD by configuring the DPD timeout timer to 0 seconds. However, for the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds will get added onto the default minimum value of 47.5 seconds).

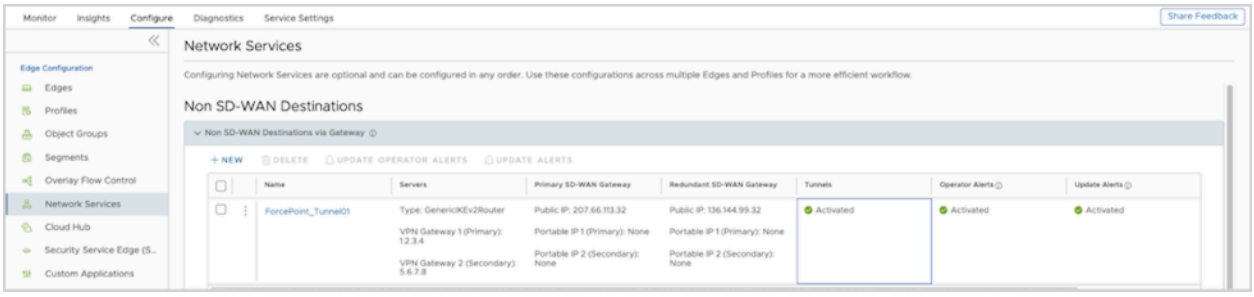
8. Select **Redundant VeloCloud Cloud VPN** to establish the IPSEC tunnels from the Primary and Secondary Gateways.
9. Configure **Site Subnets**:

   Add subnets for the Non SD-WAN Destination using the **+**. If you do not need subnets for the site, select **Deactivate Site Subnets**.
10. Configure **Local Auth Id**:

    Select the Local authentication ID as **FQDN** from the list and enter the DNS name used while configuring the **Edge Device** in the Forcepoint Cloud Security Gateway.
11. Select **Save Changes** and close the window.

The new Non SD-WAN Destination via Gateway displays in the **Network Services** window:

Figure 5-7: Displaying the New Non SD-WAN Destination via Gateway



Configure Profile to use the new Non SD-WAN Destination via Gateway. See Configure Profile with Non SD-WAN Destination via Gateway.

5.2 Configure Profile with Non SD-WAN Destination via Gateway

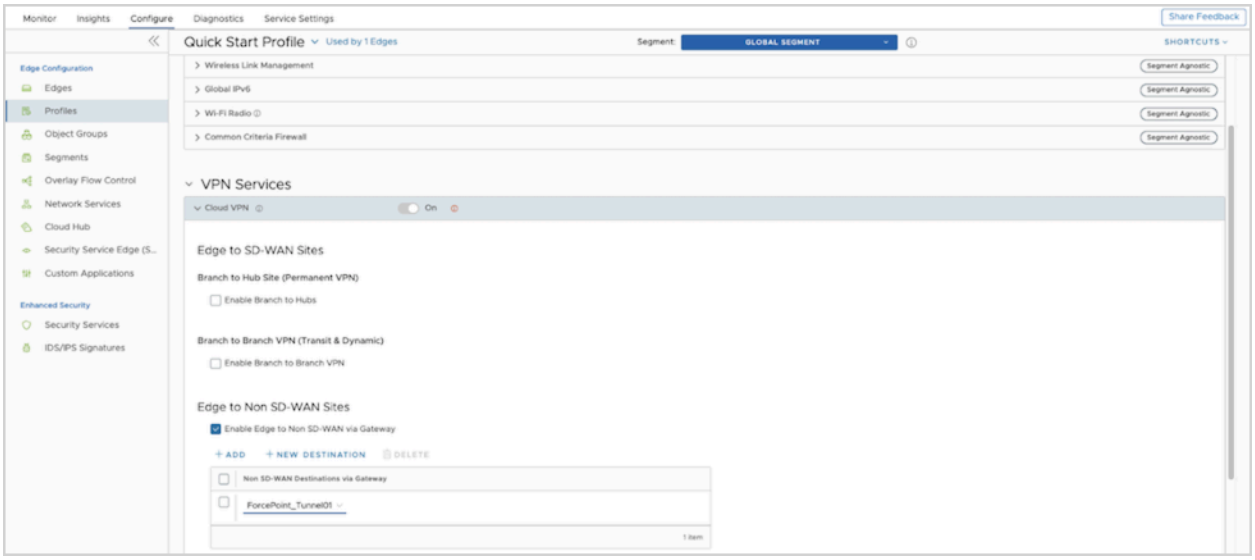
You can configure a profile to establish a VPN connection between a branch and a Non SD-WAN Destination via Gateway.

Ensure that you have created a Non SD-WAN Destination via Gateway with the required IPsec tunnel parameters relevant to Forcepoint Cloud Security Gateway. To create a Non SD-WAN Destination via Gateway, see Configure Non SD-WAN Destination via Gateway.

1. In the **Enterprise** portal, select **Configure** > **Profiles**.
2. Select the **Device** Icon for a profile, or select a profile and select the **Device** tab.
3. In the **Device** tab, scroll down to the **Cloud VPN** section and select the slider to **ON** position.

4. To establish a VPN connection between a Branch and Non SD-WAN Destination via Gateway, select the **Enable** checkbox under **Branch to Non SD-WAN Destinations via Gateway**.

   Figure 5-8: Configuring a VPN Connection



5. Select **Forcepoint Tunnel** as the Non SD-WAN Destination via Gateway option from the list to establish a VPN connection.
6. Select **Save Changes**.

Create a Business Policy to route the traffic from the Non SD-WAN Destination tunnel to the Forcepoint Cloud Security Gateway. See Create Business Policy for Non SD-WAN Destination via Gateway.

5.3 Create Business Policy for Non SD-WAN Destination via Gateway

After you establish a VPN connection between a branch and a Non SD-WAN Destination via Gateway, create a Business Policy to route the traffic from the Non SD-WAN Destination tunnel.

Ensure that you have established the VPN connection between branch and Non SD-WAN Destination via Gateway. See Configure Profile with Non SD-WAN Destination via Gateway.

1. In the **Enterprise** portal, select **Configure** > **Profiles.**
2. Select a profile from the list and select the **Business Policy** tab.
3. Select **New Rule** or **Actions** > **New Rule**.
4. Enter a name for the business rule.
5. In the **Match** area, select **Define** and choose **Internet** as the Destination.
6. Select the **Application** as **Any** to steer all the Internet traffic or select **Web** to steer only the HTTP/HTTPS traffic.
7. In the **Action** area, select **Internet Backhaul** as the Network Service.

8. Choose **Non SD-WAN Destination via Gateway** and select the Non SD-WAN Destination service created with the Forcepoint tunnel parameters.

Figure 5-9: Configuring a Rule - Example 1

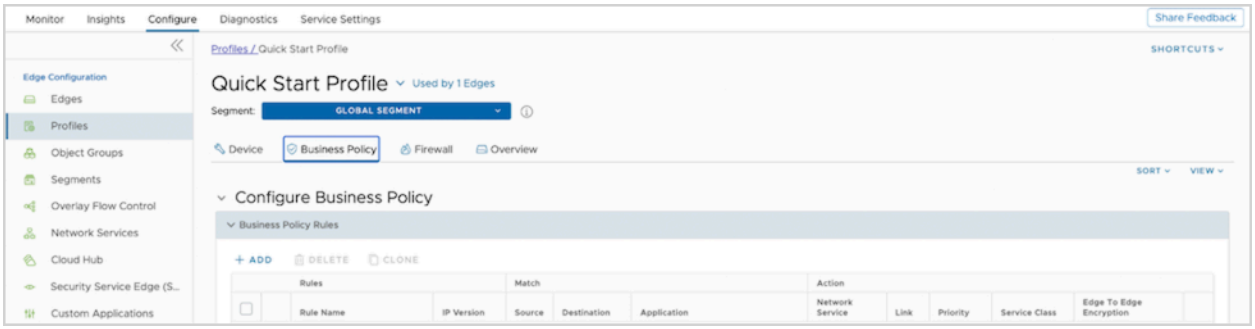


Figure 5-10: Configuring a Rule - Example 2

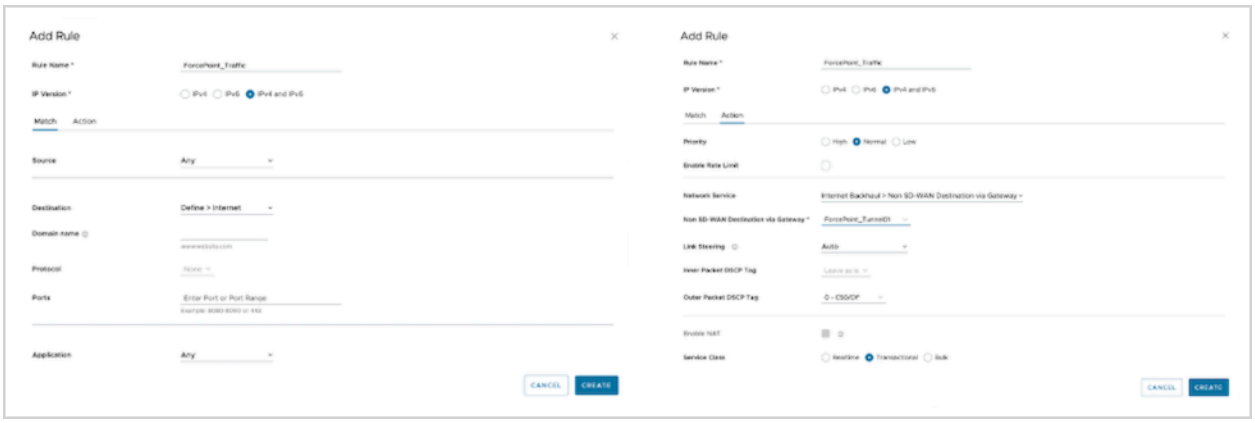


Figure 5-11: Configuring a Rule - Example 3

9. Choose the other actions as required and select **OK**.

   The Business Policy redirects the Internet destined traffic to Forcepoint Cloud Security Gateway using the IPSEC tunnel.

You can verify that the tunnel is online by monitoring the Network Services. See Monitor Non SD-WAN Destination via Gateway.

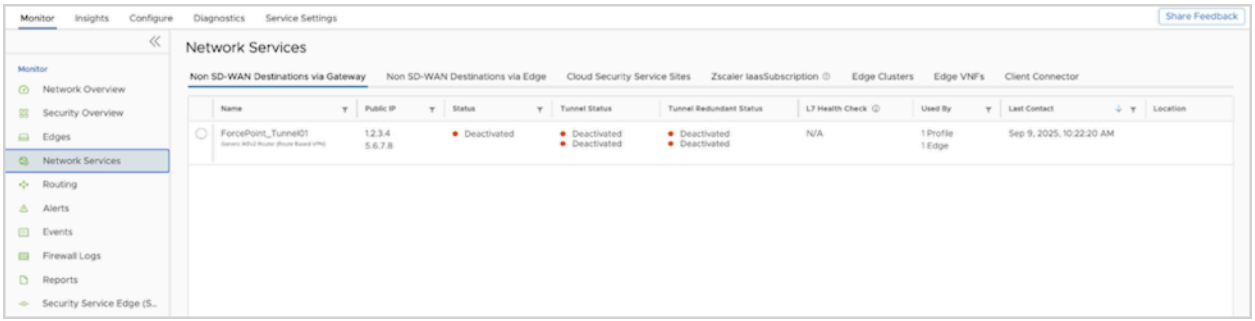
5.4 Monitor Non SD-WAN Destination via Gateway

You can monitor and verify the Non SD-WAN Destination Tunnel configuration using the **Monitoring** tab.

To monitor the Non SD-WAN Destination Tunnel configuration:

1. In the **Enterprise** portal, select **Monitor** > **Network Services**.
2. The **Non SD-WAN Destination via Gateway** section displays the configured Non SD-WAN Destination along with the status. The Forcepoint data center acts as the endpoint of redundant IPsec tunnels.

Figure 5-12: Monitoring the Non SD-WAN Destination via Gateway



Chapter 6

Configure Tunnels on VeloCloud Edge

Configure the SD-WAN layer of Orchestrator using an Edge as the endpoint for the tunnels between VeloCloud SD-WAN and Forcepoint Cloud Security Gateway. Ensure that you have configured the customer.

6.1 Configure Non SD-WAN Destination via Edge

You can define and configure a Non SD-WAN Destination instance as Forcepoint Cloud Security Gateway and establish a secure IPsec tunnel to the Forcepoint Cloud Security Gateway through a VeloCloud Edge.

Ensure that you have Administrator privileges to login to VeloCloud Edge Cloud Orchestrator.

To configure a Non SD-WAN Destination via Edge:

1. Login to **Orchestrator** and navigate to **Manage Customers**.
2. Select the link to a customer whose traffic would be routed to Forcepoint Cloud Security Gateway.
3. In the Enterprise portal, select **Configure** > **Network Services**.
4. In the **Non SD-WAN Destinations via Edge** pane, select **New** to create a new Non SD-WAN Destination.
5. In the **New Non SD-WAN Destination via Edge** window, configure the following:

   Figure 6-1: Configuring Non SD-WAN Destinations via Edge

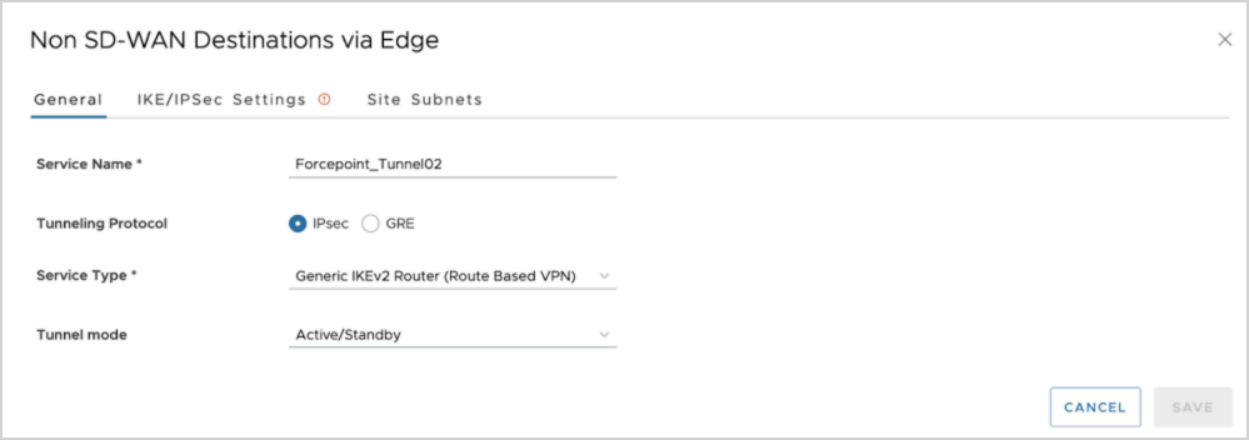


   Table 4: Non SD-WAN Destinations via Edge Option Descriptions

Option	Description
Service Name	Enter a descriptive name for the Non SD-WAN Destination.
Service Type	Select the type as **Generic IKEv2 Router (Route Based VPN)**.

6. Select **Next**.

7. In the next window, configure the following settings:

Figure 6-2: Configuring Parameters

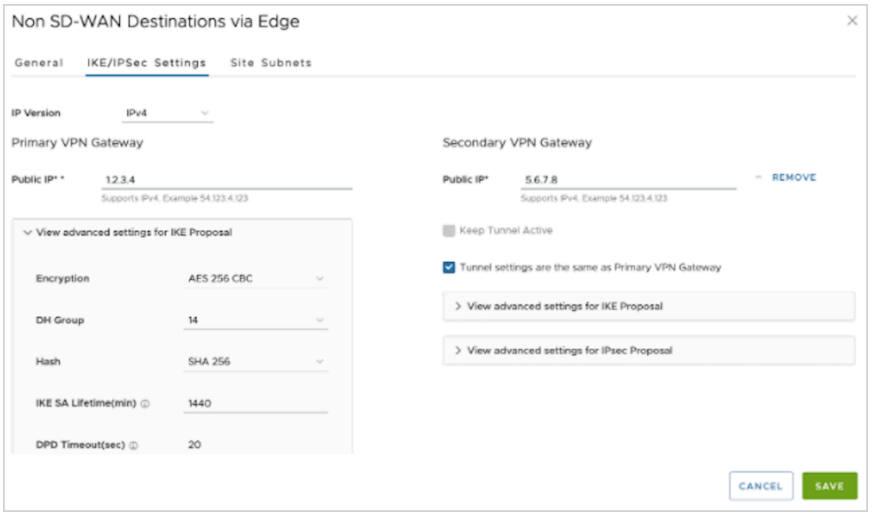
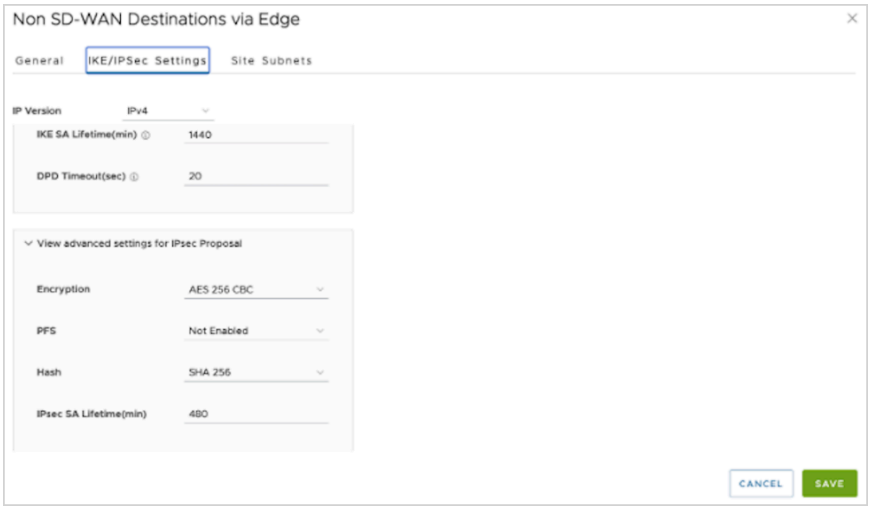


Figure 6-3: Configuring Parameters



8. Select **Advanced** to configure the other IPsec tunnel parameters for the Primary and Secondary VPN Gateways as follows:

Table 5: Advanced option Descriptions

Option	Description
Encryption	Select **AES-256** as the AES algorithms key from the list, to encrypt data.
DH Group	Select the Diffie-Hellman (DH) Group algorithm as **14** used when exchanging the pre-shared key. The DH Group sets the strength of the algorithm in bits.
PFS	Select the Perfect Forward Secrecy (PFS) level as **Deactivated**.
Hash	Select the authentication algorithm for the VPN header as **SHA 256** from the list.
IKE SA Lifetime(min)	Enter the IKE SA lifetime in minutes. The rekeying should be initiated for Edges before the time expires. The range is from 10 to 1440 minutes. The default value is 1440 minutes.
IPsec SA Lifetime(min)	Enter the IPsec SA lifetime in minutes. The rekeying should be initiated for Edges before the time expires. The range is from 3 to 480 minutes. The default value is 480 minutes.
DPD Timeout Timer(sec)	Enter the DPD timeout value. The DPD timeout value will be added to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection). Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value. • Library Name: Quicksec • Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec) • Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, 0.5+1+2+4+8+16+16 = 47.5). • Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec **Note:** Prior to the 5.1.0 release, you can deactivate DPD by configuring the DPD timeout timer to 0 seconds. However, for the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds adds onto the default minimum value of 47.5 seconds).

9. For the Secondary VPN Gateway, select **Tunnel settings are same as Primary VPN** to configure the tunnel settings similar to the Primary VPN Gateway. The Edge sets up two tunnels.
10. Select the default values for other settings.
11. Select **Save Changes** and close the window.

    The new Non SD-WAN Destination via Edge is displayed in the **Network Services** window:

Figure 6-4: Network Services

Configure a profile to use the new Non SD-WAN Destination via Edge. See Configure Profile with Non SD-WAN Destination via Edge.

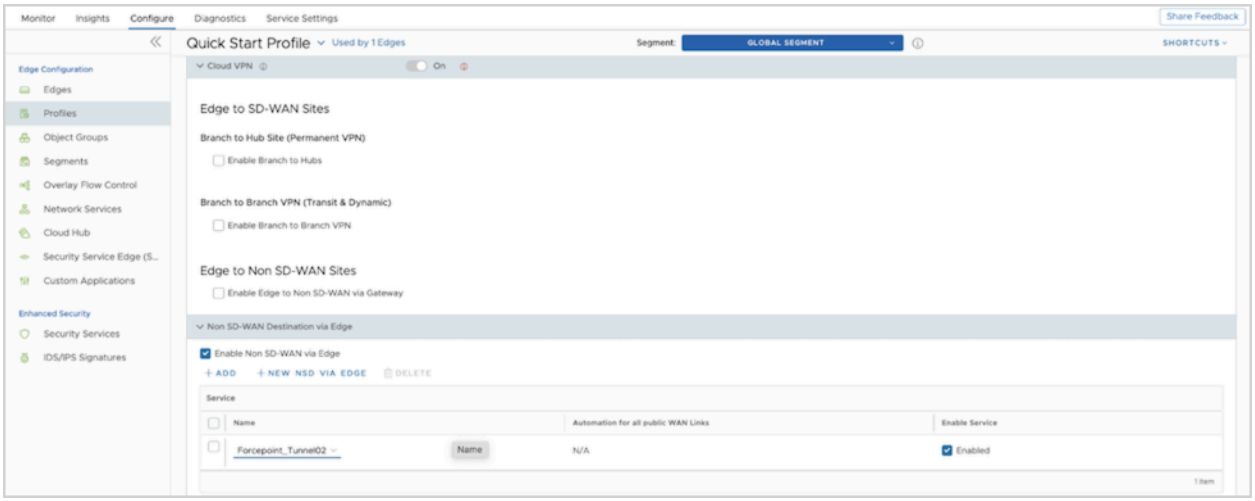
6.2 Configure Profile with Non SD-WAN Destination via Edge

You can configure a profile to establish a VPN connection between a branch and a Non SD-WAN Destination via Edge.

Ensure that you have created a Non SD-WAN Destination via Edge with the required IPsec tunnel parameters relevant to Forcepoint Cloud Security Gateway. To create a Non SD-WAN Destination via Edge, see Configure Non SD-WAN Destination via Edge.

1. In the **Enterprise** portal, select **Configure** > **Profiles**.
2. Select the **Device** Icon for a profile, or select a profile and select the **Device** tab.
3. In the **Device** tab, navigate to the **Cloud VPN** section and select the slider to **ON** position.
4. To establish a VPN connection between a Branch and Non SD-WAN Destination via Edge, select **Enable** under **Branch to Non SD-WAN Destinations via Edge**.

   Figure 6-5: Enabling the VPN Connection



5. Select **Forcepoint Tunnel** as the Non SD-WAN Destination via Edge to establish VPN connection.
6. Select **Save Changes**.

Create a Business Policy to route the traffic from the Non SD-WAN Destination tunnel to the **Forcepoint Cloud Security Gateway**. See Create Business Policy for Non SD-WAN Destination via Edge.

6.3 Create Business Policy for Non SD-WAN Destination via Edge

After you establish a VPN connection between a branch and a Non SD-WAN Destination via Edge, create a Business Policy to route the traffic from the Non SD-WAN Destination tunnel.

Ensure that you have established the VPN connection between branch and Non SD-WAN Destination via Edge. See Configure Profile with Non SD-WAN Destination via Edge.

1. In the **Enterprise** portal, select **Configure** > **Profiles**.

2. Select a profile from the list and select the **Business Policy** tab.
3. Select **New Rule** or **Actions** > **New Rule**.
4. Enter a name for the business rule.
5. In the **Match** area, select **Define** and choose **Internet** as the Destination.
6. Select the **Application** as **Any** to steer all the Internet traffic or select **Web** to steer only the HTTP/HTTPS traffic.
7. In the **Action** area, select **High** as Priority and select **Internet Backhaul** as the Network Service.
8. Choose **Non SD-WAN Destination via Edge** and select the Non SD-WAN Destination service created with the Forcepoint tunnel parameters.

Figure 6-6: Configuring a Rule - Example 1

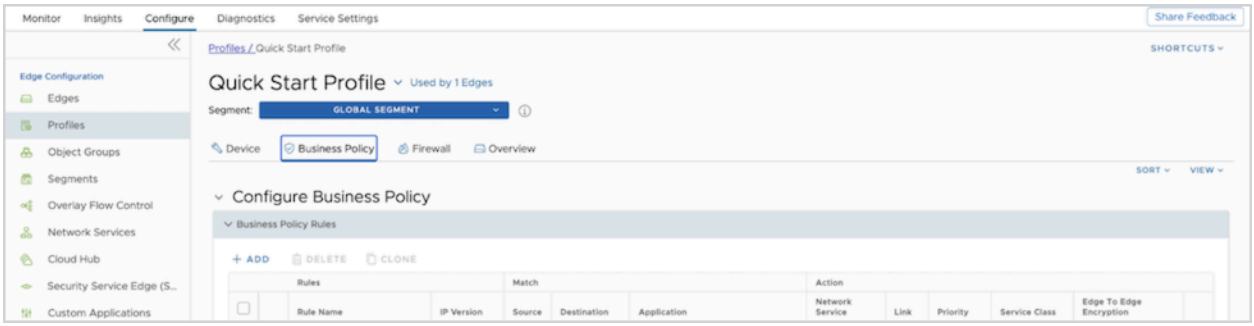


Figure 6-7: Configuring a Rule - Example 2

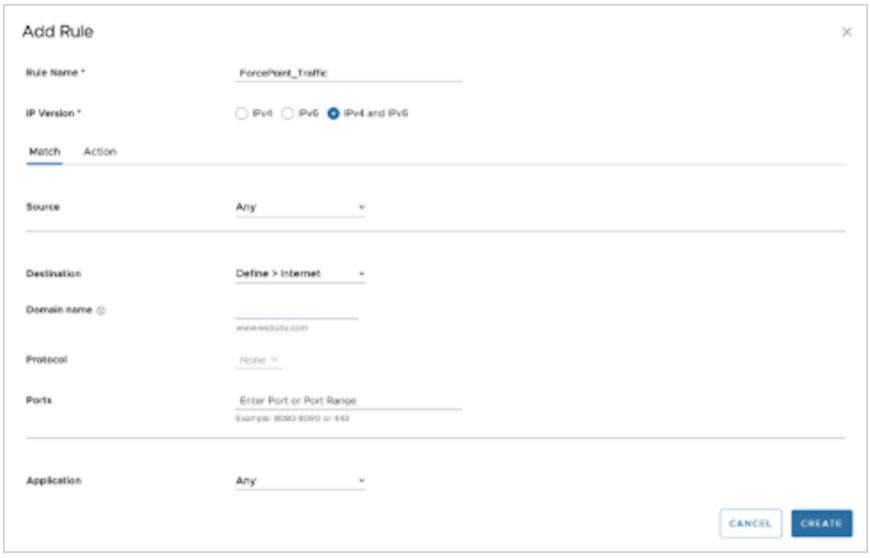


Figure 6-8: Configuring a Rule - Example 3

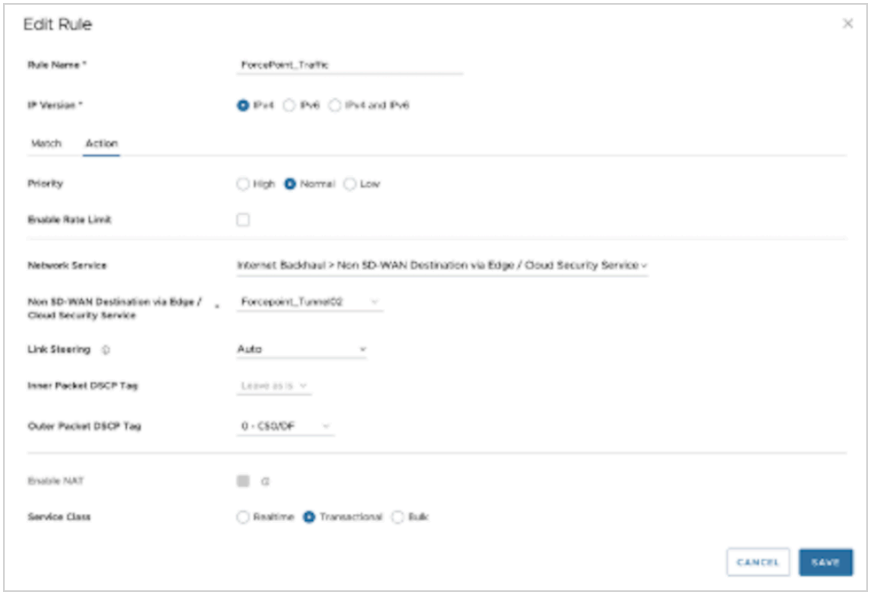
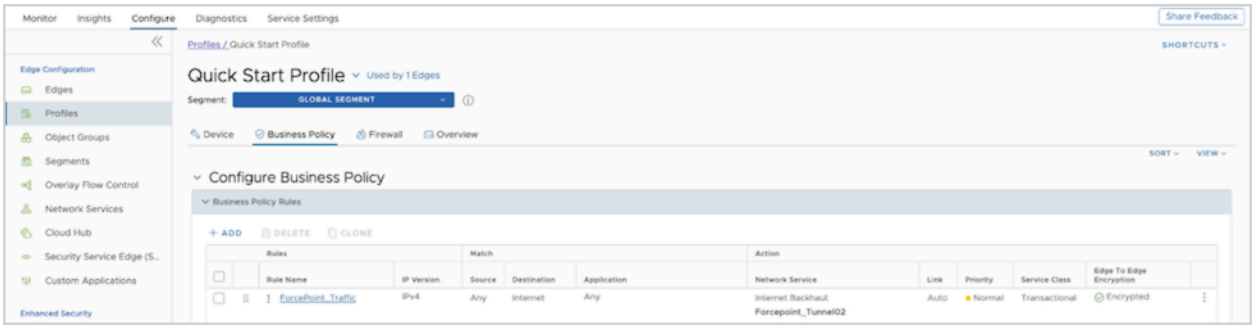


Figure 6-9: Configuring a Rule - Example 4



9. Choose the other actions as required and select **OK**.

   The Business Policy redirects the Internet-destined HTTP/HTTPS traffic to the **Forcepoint Cloud Security Gateway** using the IPSEC tunnel.

Configure the Tunnel parameters for a selected Edge. See Configure Edge with Tunnel Parameters.

6.4 Configure Edge with Tunnel Parameters

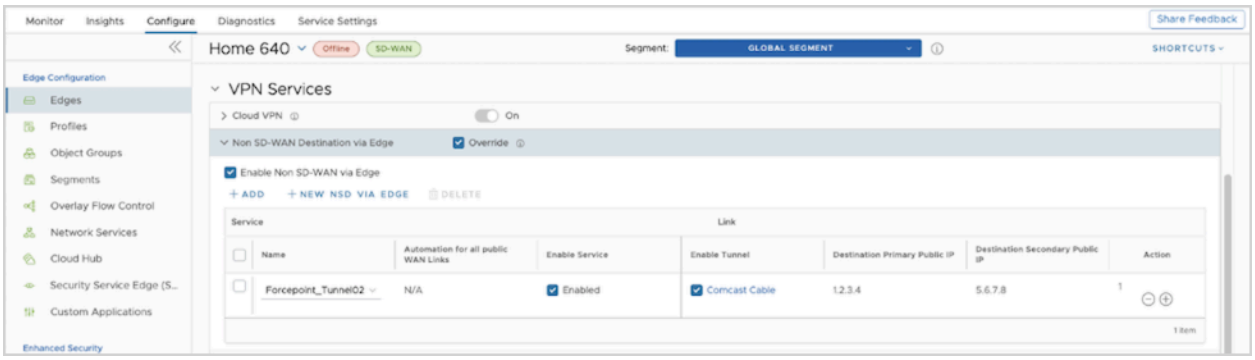
When you configure a profile to establish a VPN connection between a branch and a Non SD-WAN Destination via Edge, the settings are automatically applied to all the Edges that are associated with the profile. You can configure the Tunnel parameters for an individual Edge and choose the source of the Tunnel as the WAN IP address.

Ensure that you have established the VPN connection between branch and Non SD-WAN Destination via Edge. See Configure Profile with Non SD-WAN Destination via Edge.

To configure the tunnel parameters for an Edge:

1. In the **Enterprise** portal, select **Configure** > **Edges**.
2. Select **Device** for an Edge, or select an Edge and select the **Device** tab.
3. In the **Device** tab, scroll down to the **Cloud VPN** section.
4. Select **Enable Edge Override** and select **Add** in the **Action** column.

   Figure 6-10: Displaying Cloud VPN



5. In the **Add Tunnel** window, configure the following parameters:

   Figure 6-11: Adding a Tunnel

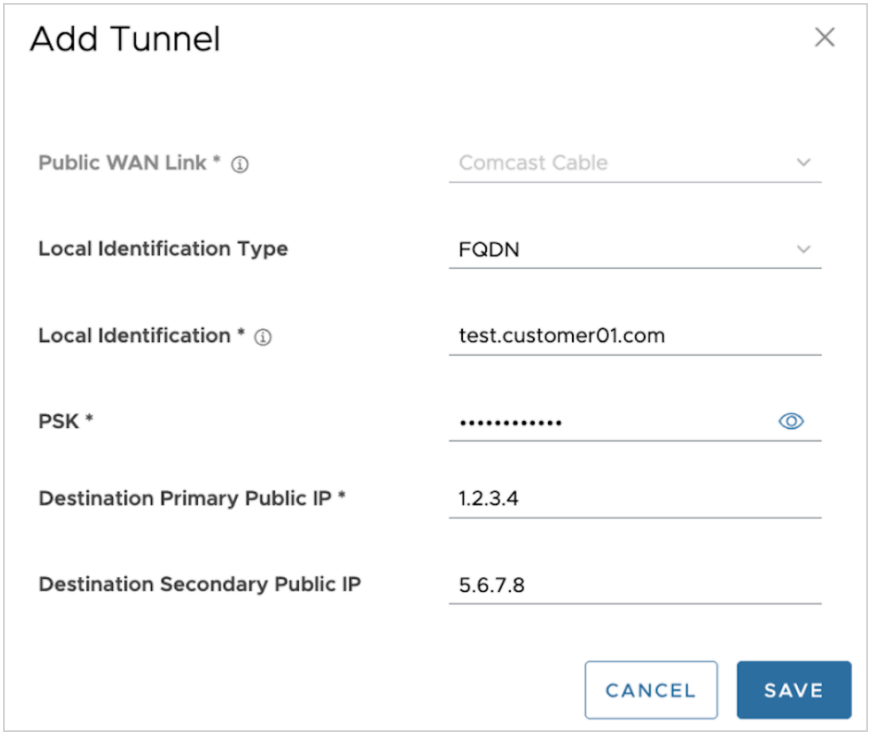


Table 6: Add tunnel Option Descriptions

Option	Description
Public WAN Link	Select the IP address of the Edge hosting the Tunnel endpoint connecting to Forcepoint Cloud Security Gateway.
Local Identification Type	Select the type as **FQDN/Hostname** from the list.
PSK	Enter the same Pre-Shared Key configured in the Forcepoint Cloud Security Gateway.
Destination Primary Public IP	Enter the Service IP address of the primary data center obtained from the Forcepoint Cloud Security Gateway configuration.
Destination Secondary Public IP	Enter the Service IP address of the secondary data center obtained from the Forcepoint Cloud Security Gateway configuration.

6. Select **Save Changes**.

Verify that the tunnel is online by monitoring the Edges. See Monitor Non SD-WAN Destination via Edge.

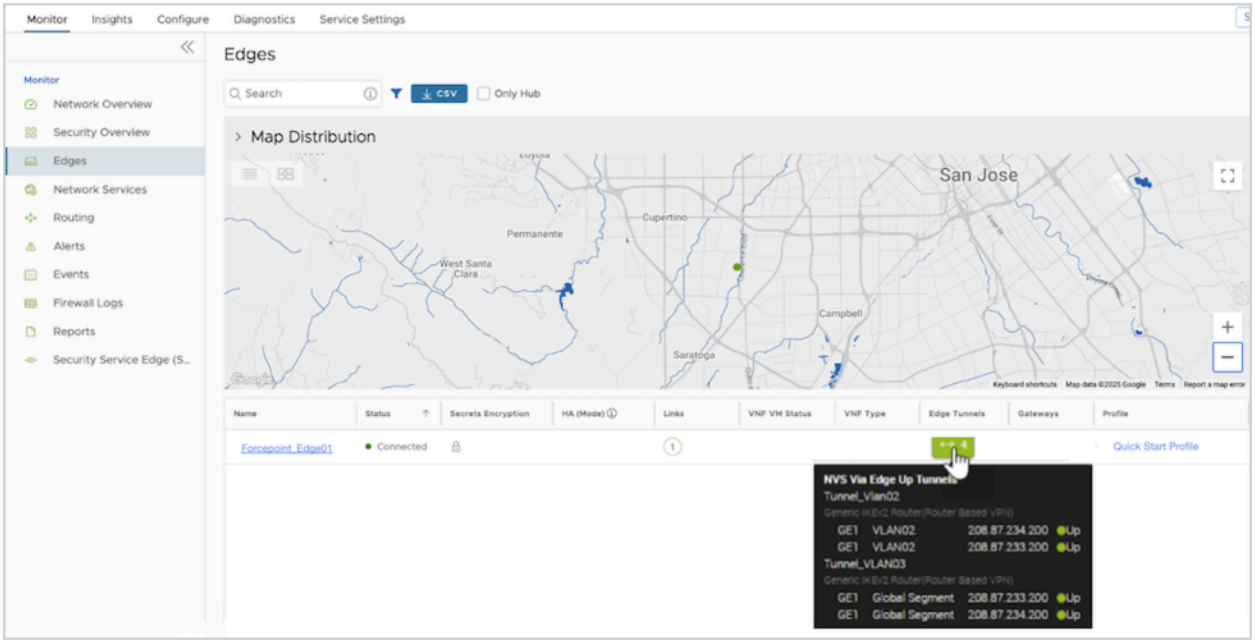
6.5 Monitor Non SD-WAN Destination via Edge

You can monitor and verify the Non SD-WAN Destination Tunnel configuration using the Monitoring tab.

To monitor the Non SD-WAN Destination Tunnel configuration:

1. In the **Enterprise** portal, select **Monitor** > **Edges**.
2. The **Edges** page displays the configured Non SD-WAN Destination along with the status. The Forcepoint data center becomes the endpoint of redundant IPsec tunnels.

Figure 6-12: Monitoring the Non SD-WAN Destination via Edge



Chapter 7

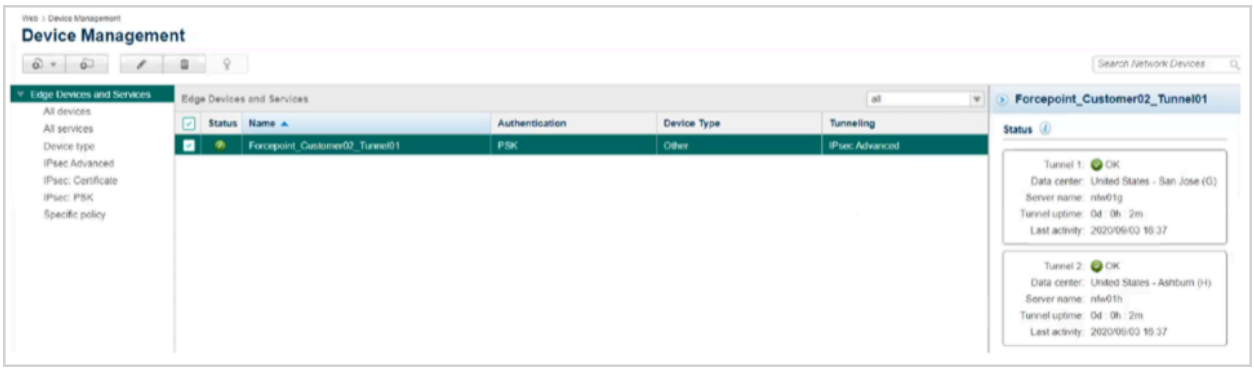
Verify the Status of IPsec Tunnels

After configuring the IPsec tunnels in both VeloCloud SD-WAN and Forcepoint Cloud Security Gateway, it takes a few minutes for the IPsec tunnels to establish. You can check the status of the established IPsec tunnels in both products.

To check the status of the IPsec tunnels in **Forcepoint Cloud Security Gateway**:

1. In the **Forcepoint Cloud Security Gateway**, navigate to **Device Management** > **Edge Devices and Services**.
2. Select the Edge Device configured for the integration.

   Figure 7-1: Displaying the Edge Device



3. If you set up the IPsec tunnels correctly, both the Tunnels display a green icon and display details of the connections. Note that each tunnel displays green if at least one of the redundant connections from VeloCloud SD-WAN becomes active.

   To view the status of the IPsec tunnels in the Orchestrator, refer to the following:

   - Monitor Non SD-WAN Destination via Gateway
   - Monitor Non SD-WAN Destination via Edge

Chapter 8

Validate End to End Integration

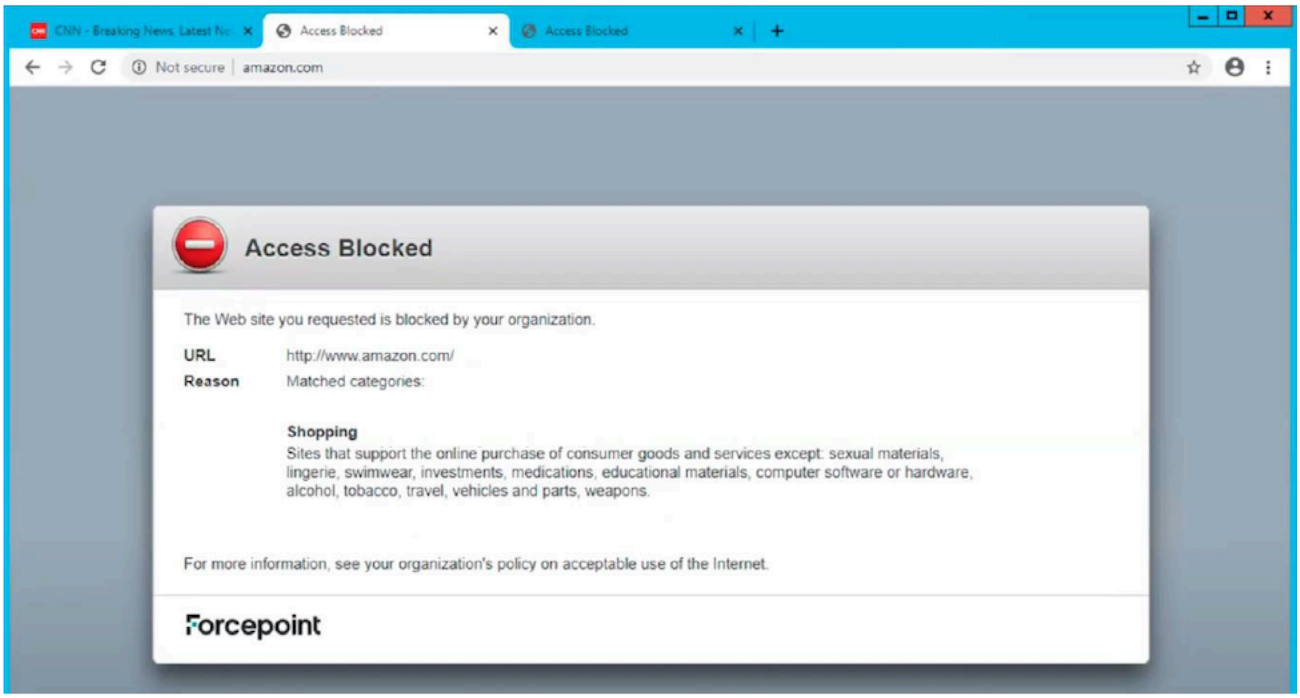
You can validate the integration of VeloCloud SD-WAN and Forcepoint Cloud Security Gateway by testing the security policies.

After configuring both VeloCloud SD-WAN and Forcepoint Cloud Security Gateway, you can do end to end validation. Try to browse a website not allowed by the security policy configured in Forcepoint Cloud Security Gateway from a system connected to VeloCloud SD-WAN.

Open a browser in the system connected to VeloCloud SD-WAN and navigate to a website that belongs to a category blocked by security policy assigned to the Edge Device used for the integration with VeloCloud SD-WAN.

If configured correctly and the security policy displays a block notification, the browser displays a message similar to the following:

Figure 8-1: Blocking Access



The above example shows that the user traffic correctly tunneled to Forcepoint Cloud Security Gateway and web security policies enforced successfully.

Appendix A

References

A.1 Related Documents

The following documentation is available for ***Arista VeloCloud SD-WAN***:

- *Arista VeloCloud SD-WAN Operator Guide*
- *Arista VeloCloud SD-WAN Administration Guide*
- *Arista VeloCloud SD-WAN Gateway Monitoring Guide*
- *Arista VeloCloud SD-WAN Orchestrator Deployment and Monitoring Guide*
- *Arista VeloCloud SD-WAN Partner Guide*
- *Arista VeloCloud SASE Global Settings Guide*
- *Arista VeloCloud SD-WAN Troubleshooting Guide*
- *Arista VeloCloud SD-WAN Design Guide for Enhanced Firewall Services*
- *Arista VeloCloud SD-WAN 6.4 API*
- *Arista VeloCloud Portal API 6.4*
- *Arista AliCloud Virtual Edge Deployment Guide*
- *Arista AWD Virtual Edge Deployment Guide*
- *Arista Azure Virtual Edge Deployment Guide*
- *Arista Google Cloud Platform Virtual Edge Deployment Guide*
- *Arista VeloCloud SASE and QRadar SIEM Integration Guide*
- *Arista VeloCloud SD-WAN and Cloud on AWS Deployment Guide*
- *Arista VeloCloud SD-WAN and Forcepoint SSE Integration Guide*
- *Arista VeloCloud SD-WAN and Google Network Connectivity Center Integration Guide*
- *Arista VeloCloud SD-WAN and Microsoft Route Server Integration Guide*
- *Arista VeloCloud SD-WAN and Netskope SSE Integration Guide*
- *Arista VeloCloud SD-WAN Azure Private Multi-Access Edge Compute Deployment Guide*
- *Arista VeloCloud SD-WAN License Management Guide*