Integration Guide

VeloCloud SD-WAN
Netskope SSE

Services

Arista.com

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: VeloCloud SD-WAN and Netskope SSE Integration Guide....1

Chapter 2: Overview of VeloCloud SD-WAN and Netskope SSE Integration....2

Chapter 3: System Requirements....4

Chapter 4: Configure IPsec from VeloCloud Gateway to Netskope POP....5

4.1 Configure VPN Credentials on the Netskope Portal....5

Chapter 5: Configure Non SD-WAN Destination via Gateway....8

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

Chapter 6: Test and Verify Security Policies....17

Appendix A: References....20

A.1 Related Documents....20

Chapter 1

VeloCloud SD-WAN and Netskope SSE Integration Guide

The VeloCloud SD-WAN™ and Netskope Integration Security Service Edge (SSE) Guide describes the configurations required to integrate Netskope Next Gen Secure Web Gateway with the VeloCloud Edge Cloud Orchestrator.

Chapter 2

Overview of VeloCloud SD-WAN and Netskope SSE Integration

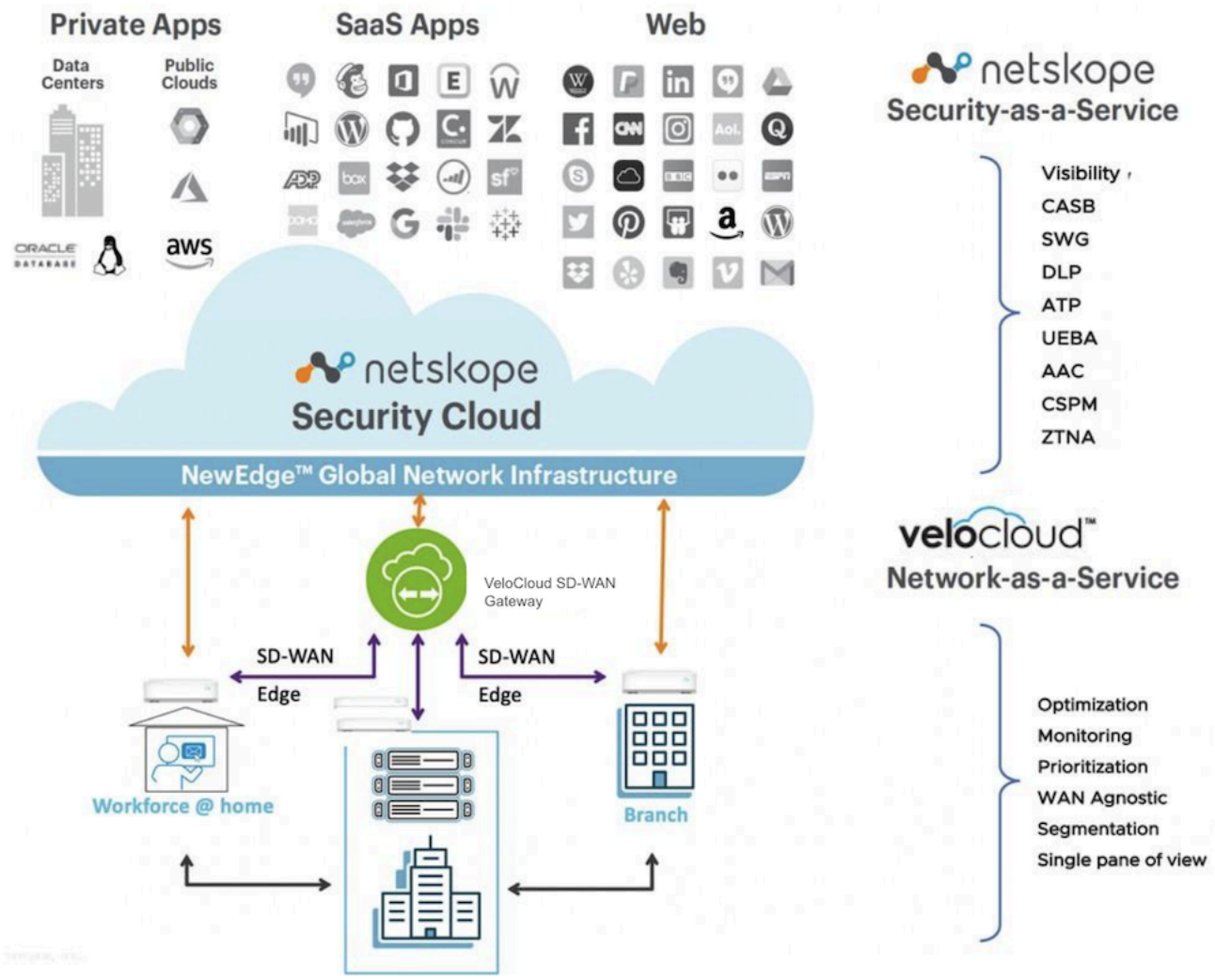
VeloCloud SD-WAN integrates with Netskope Next Gen Secure Web Gateway (SWG) to enable organizations with comprehensive cloud-enabled security in addition to optimized connectivity.

VeloCloud SD-WAN provides networking services by delivering high-performance, reliable access to cloud services, private data centers, and SaaS-based enterprise applications, while Netskope Security Service Edge (SSE) provides the complementary security services such as a Next Gen SWG, a Cloud Access Security Broker (CASB) with both API-enabled and inline protections. Together they provide advanced data and threat protection for users, applications, and data. VeloCloud Edge can be deployed as a physical appliance or as a virtual machine at the customer site. The Edges communicate through secure IPsec to the Netskope Security Cloud.

When accessing public clouds such as AWS or Azure, or SaaS applications such as Office 365 and Workday, the VeloCloud Gateways send traffic to the Netskope Security Cloud to apply granular activity and security controls, with advanced data and threat protection. More specifically, this extends virtual access of the users to the New Edge global network infrastructure which serves as the network foundation for the Netskope

Security Cloud and provides high-capacity, and low-latency access to cloud apps, infrastructure, and websites for a high performance user experience.

Figure 2-1: Example Topology for VeloCloud SD-WAN and Netskope SWG



Together, Netskope and VeloCloud tightly integrate security and SD-WAN features delivering network optimization services like acceleration, QoS, and de-jitter, along with cloud-native, converged single-pass security controls like CASB, SWG, DLP, and ZTNA, to offer organizations with a highly-scalable, fast, and secure environment that protects users and data inside and outside the traditional corporate perimeter.

Chapter 3

System Requirements

Netskope Next Generation Secure Web Gateway

- Active Netskope tenant
- Administrator login credentials
- Ability to configure varying policies in the SWG service

VeloCloud Edge Cloud Orchestrator

- Enterprise account access to VeloCloud Edge Cloud Orchestrator
- Administrator login credentials

VeloCloud and Netskope have tested the following scenarios:

- IKEv2-based NSD Tunnel from Gateway- Netskope POP for Single tenant.
- IKEv2-based NSD Tunnels from Gateway- Multiple tunnels for Multiple Tenants using the same Source, VeloCloud Gateway IP address, and Destination, Netskope POP based on strongSwan 5.71, using FQDN.
- Pass traffic from multiple tenants using the above IPSEC tunnels and apply different Netskope Policies to each Tenant. Bring up the Tunnels in a redundant fashion both from VeloCloud and Netskope POP perspective and test failover scenarios.
- IKEv2-based NSD Tunnel from Edge to Netskope POP.

Chapter 4

Configure IPsec from VeloCloud Gateway to Netskope POP

To integrate VeloCloud SD-WAN and Netskope, configure the IPsec from the Gateway to Netskope POP.

4.1 Configure VPN Credentials on the Netskope Portal

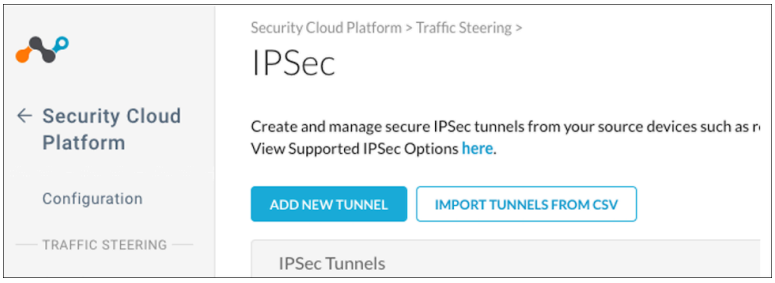
Ensure that you have valid login credentials to access Netskope.

To configure the VPN credentials:

Navigate to the Netskope NG SWG Portal- `https://<customer-tenant>.goskope.com/`

1. Configure the Netskope tunnel to connect with VeloCloud SD-WAN. In the Netskope portal, select **Settings** > **Security Cloud Platform** > **Traffic Steering** > **IPSec**.
2. Select **Add New Tunnel**.

Figure 4-1: Adding a New Tunnel



3. In the **Add New IPsec Tunnel** window, configure the following:

Figure 4-2: Adding New IPsec Tunnel

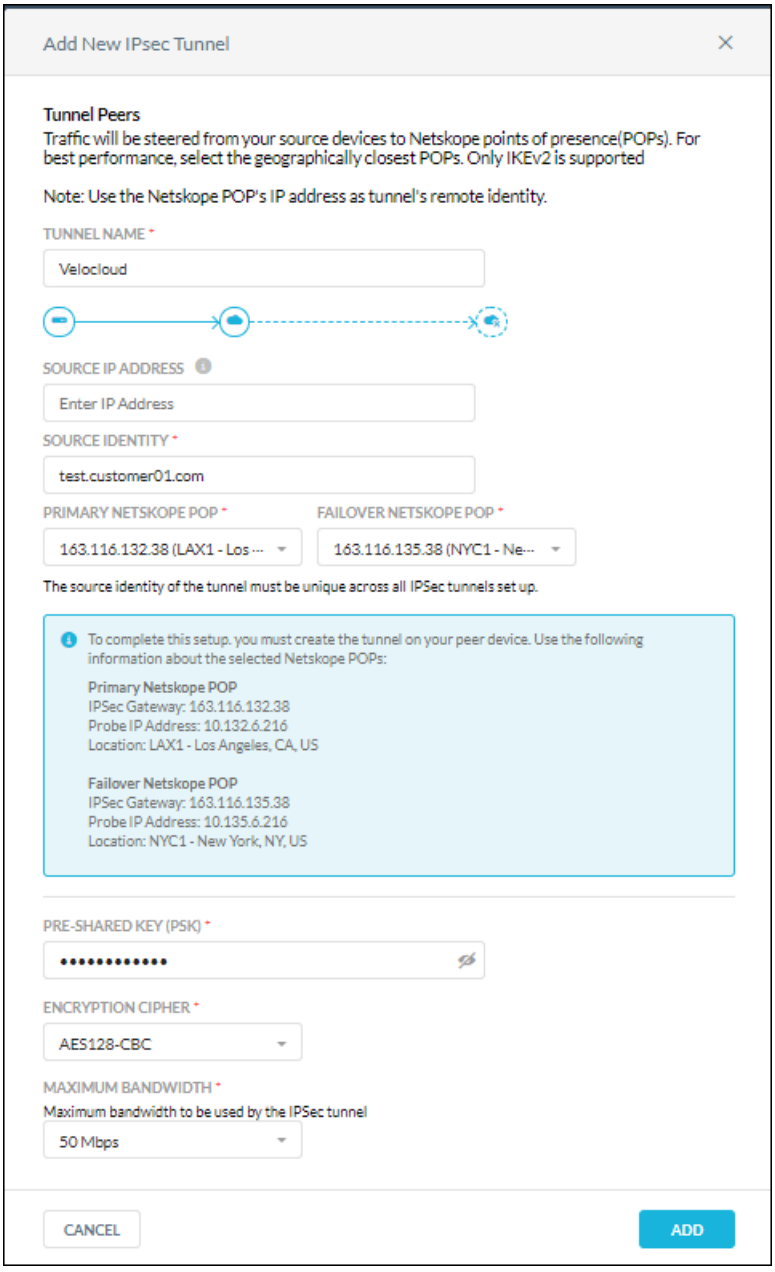
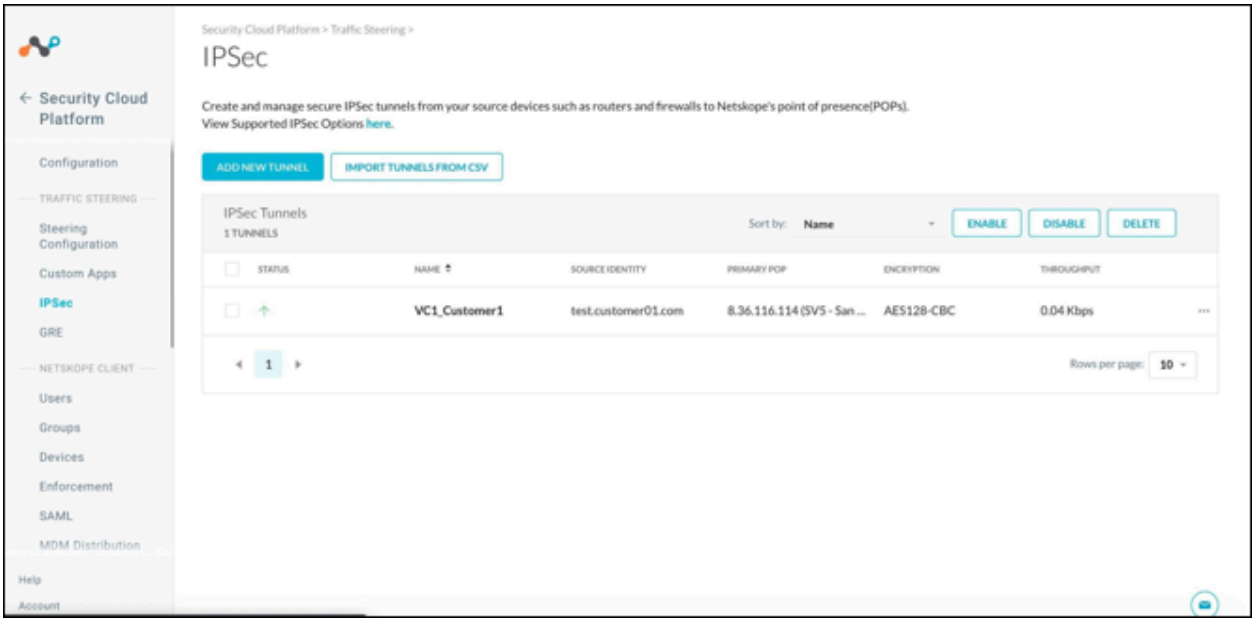


Table 1: New IPsec Tunnel Option Descriptions

Option	Description
Tunnel Name	Enter a name for the new IPsec tunnel
Source IP Address	Enter the source IP address
Source Identity	Enter the FQDN.
Primary Netskope POP	Select the primary Netskope POP
Failover Netskope POP	Select the secondary Netskope POP
Pre-Shared Key (PSK)	Enter the pre-shared key
Encryption Cipher	Select the encryption as **AES128-CBC** from the drop-down list.
Maximum Bandwidth	Select the maximum bandwidth to be used by the IPsec tunnel, from the list.

4. Select **Add**.
5. The configured tunnel displays in the **IPsec** window.

Figure 4-3: Displaying the Configured Tunnel



6. Choose the tunnel and select **Enable** to bring up the tunnel. The status arrow displays green when the tunnel successfully authenticates and establishes between Netskope and VeloCloud SD-WAN.

Configure the Tunnel in VeloCloud Edge Cloud Orchestrator. See Configure Non SD-WAN Destination via Gateway.

Chapter 5

Configure Non SD-WAN Destination via Gateway

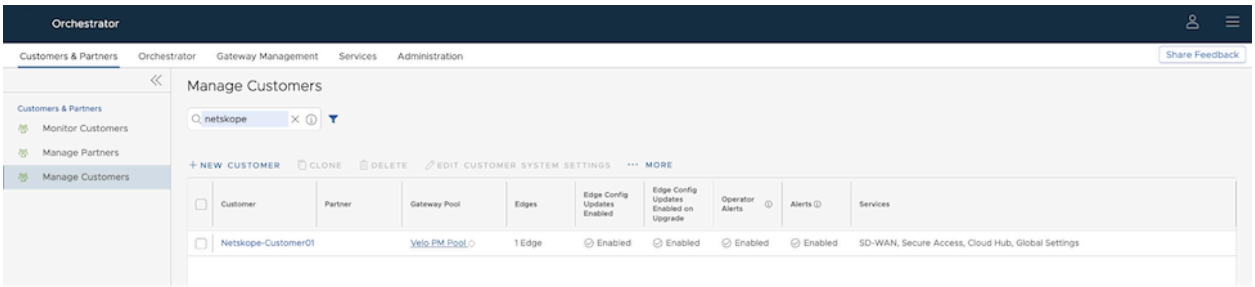
Configure a Non SD-WAN Destination via Gateway in Orchestrator to establish a secure IPSec tunnel to the Netskope portal through Gateway.

Ensure you have configured an IPsec tunnel in the Netskope NG SWG Portal. See Configure VPN Credentials on the Netskope Portal.

To configure a Non SD-WAN Destination via Gateway:

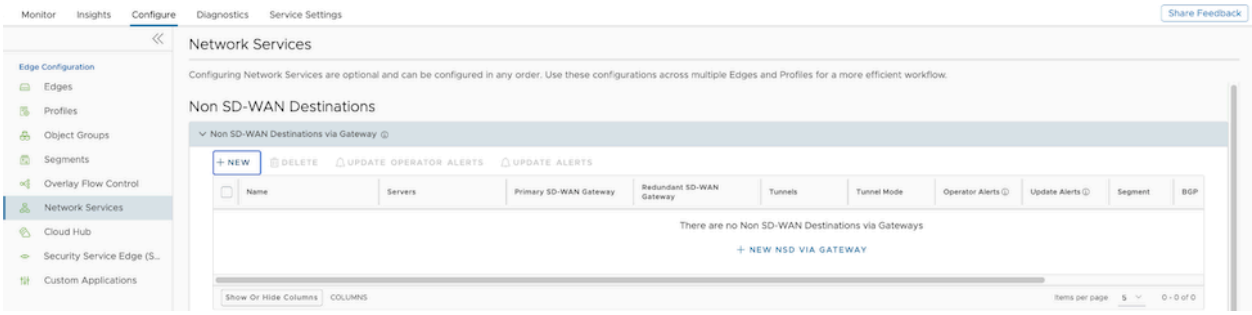
1. Login to Orchestrator to verify the presence of customers instances and you have active Edges.

   Figure 5-1: Verifying the Customer Instance



2. Select the link to a customer name to navigate to the Enterprise portal.
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: Configuring a New Non SD-WAN Destination via Gateway



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

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

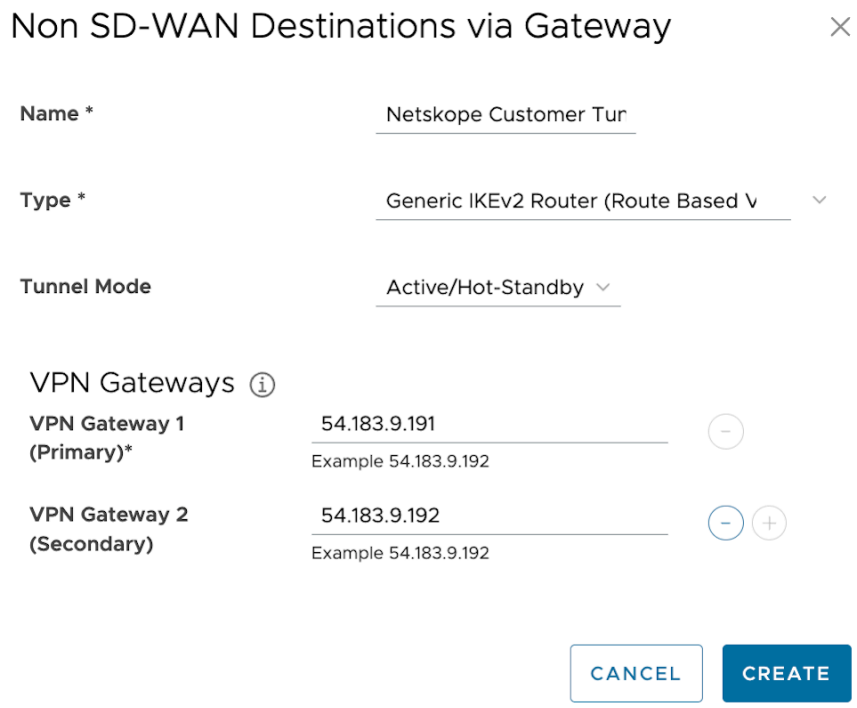


Table 2: New Non SD-WAN Destination via Gateway Option Descriptions

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 Primary POP used to setup the VPN tunnel in the Netskope portal.
Secondary VPN Gateway	Enter the IP address of the Secondary POP used to setup the VPN tunnel in the Netskope portal.

6. Select **Next**.

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

Figure 5-4: Netskope Customer Tunnel

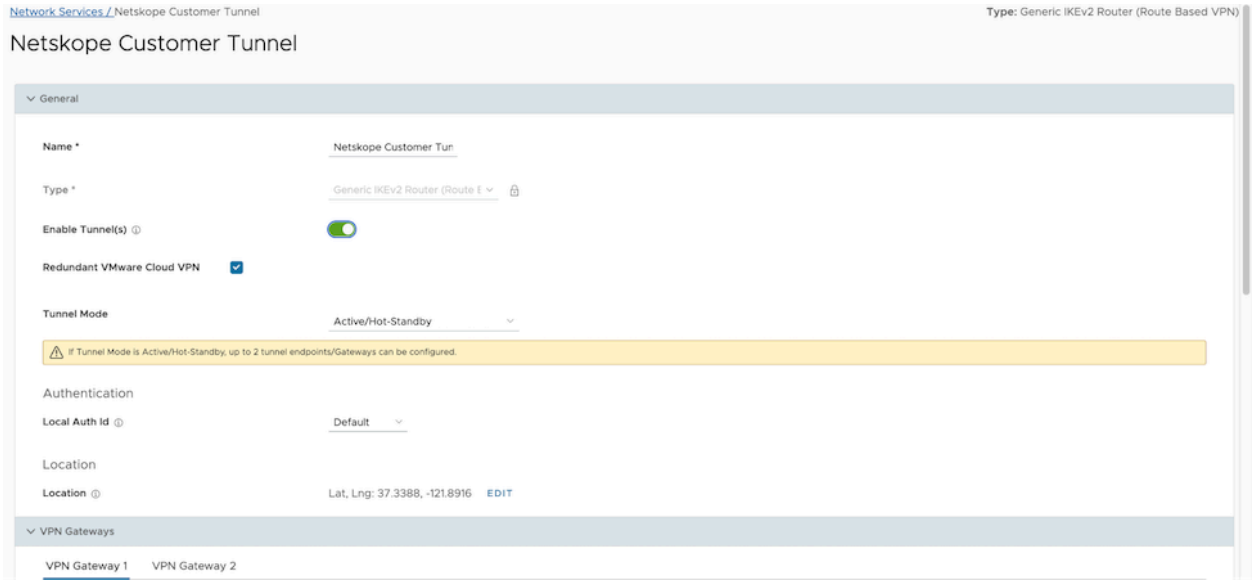


Figure 5-5: Netskope Customer Tunnel - VPN Gateway 1

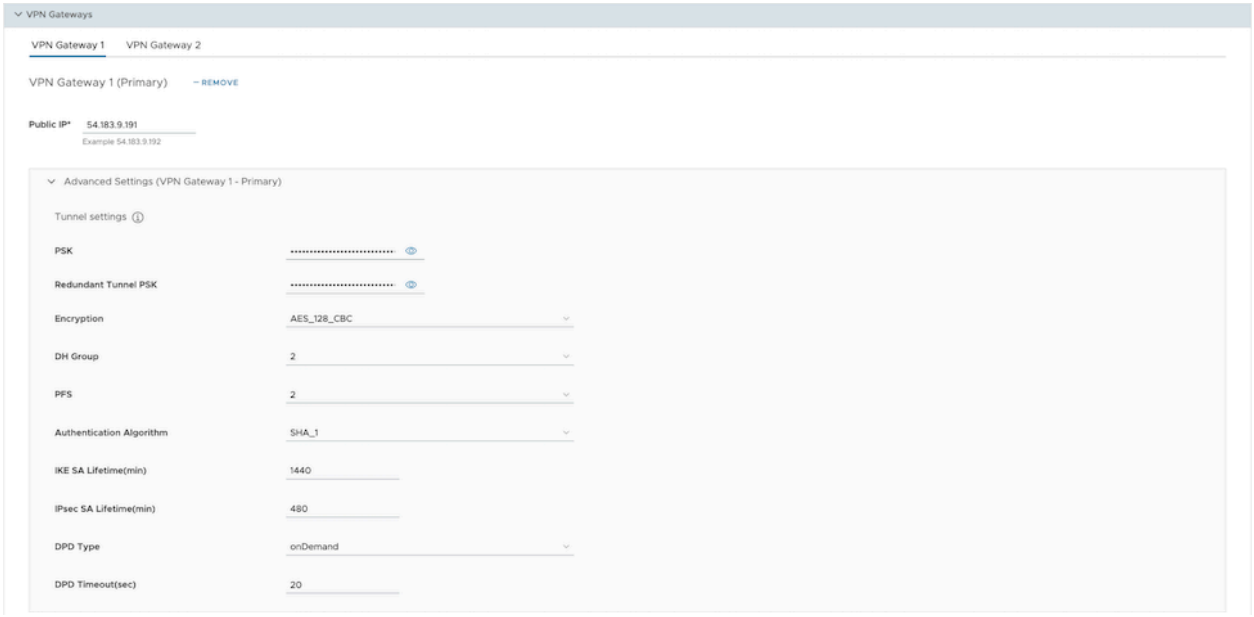
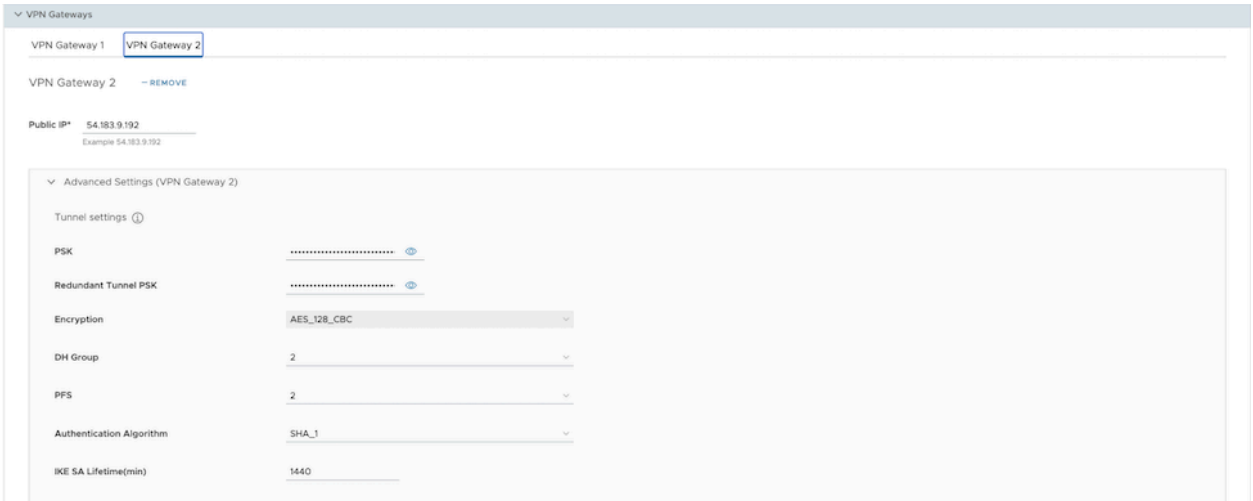


Figure 5-6: Netskope Customer Tunnel - VPN Gateway 2



8. The **Name** and **Type** of the Non SD-WAN Destination displays. Select **Enable Tunnel(s)** to activate the tunnel.
9. Select **Advanced** to configure the other IPsec tunnel parameters for the Primary and Secondary VPN Gateways as follows:

Table 3: IPsec Tunnel Option Descriptions

Option	Description
Encryption	Select the AES algorithms key from the drop-down list, to encrypt data. If you do not want to encrypt the data, select **Null**. The default value is AES 128.
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. The supported DH Groups are 2, 5, 14, 15, and 16. It is recommended to use DH Group 14.
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are 2, 5, 14, 15, and 16. The default value is deactivated.
Hash	Select the authentication algorithm for the VPN header from the drop-down list. The following Secure Hash Algorithm (SHA) options are available: • SHA 1 • SHA 256 • SHA 384 • SHA 512 The default value is SHA 256.
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 maximum time that the device should wait to receive a response to a DPD message before considering the peer as dead. The default value is 20 seconds. You can deactivate the DPD by configuring the DPD timeout timer as Zero (0).

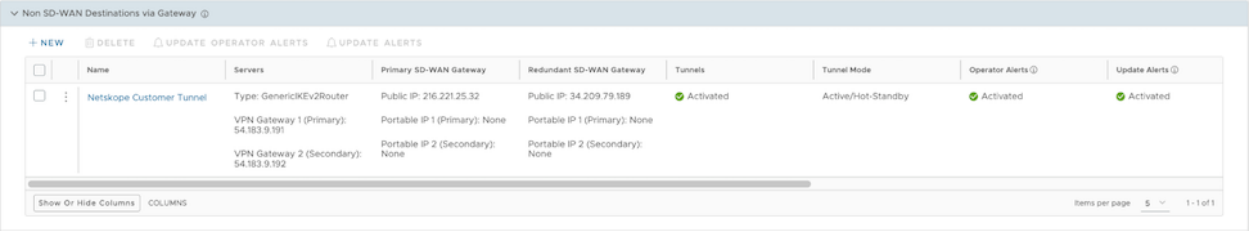
10. Configure a **Redundant VeloCloud Cloud VPN**:
    a. Select the checkbox to establish the IPSEC tunnels from the Primary and Secondary Gateways.
11. Configure **Site Subnets**:
    a. Add subnets for the Non SD-WAN Destination using the **+** icon. If you do not need subnets for the site, select **Deactivate Site Subnets**.
12. Configure the **Local Auth Id** by selecting the local authentication from the list and define the format and identification of the local gateway.

    Select one of the following options:

    - **Default** – By default, the Interface Public IP address of the Gateway is used as the local authentication ID.
    - **FQDN**- The Fully Qualified Domain Name or hostname. For example, company.com.
    - **User FQDN**- The User Fully Qualified Domain Name in the form of email address. For example, user@company.com.
    - **IPv4**- The IP address used to communicate with the local gateway.
13. 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 SD-WAN Destination



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

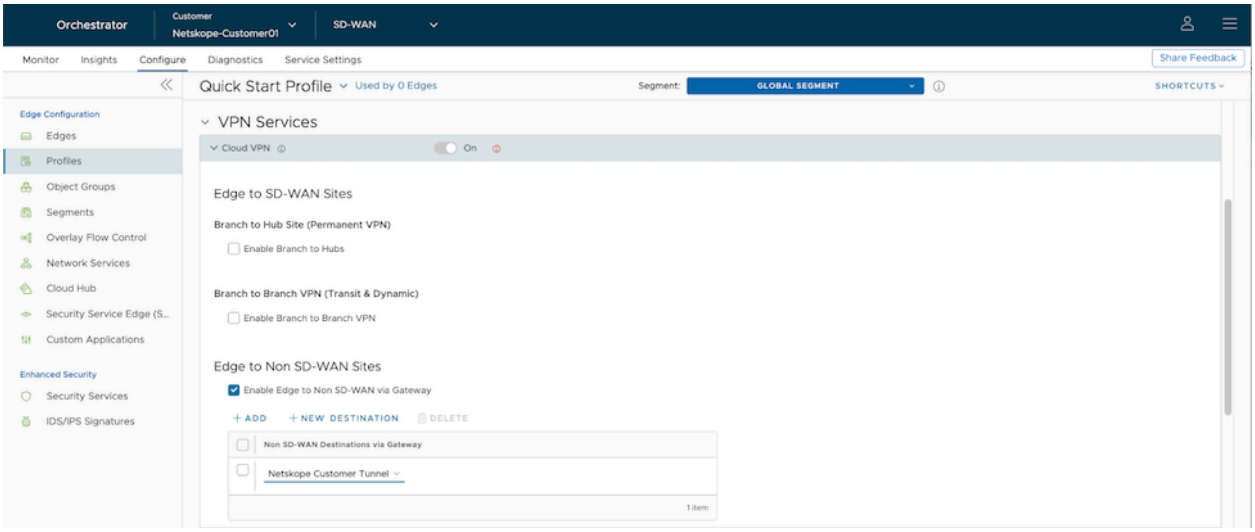
5.1 Configure Profile with Non SD-WAN Destination via Gateway

Configure the 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. 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 **Device** 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 **Enable** under **Branch to Non SD-WAN Destinations via Gateway**.

Figure 5-8: Enabling the VPN Connection



5. Select a **Non SD-WAN Destination via Gateway** from the menu to establish VPN connection. Select the **+** to add more.
6. Select **Save Changes**.

Create a Business Policy to route the traffic from the Non SD-WAN Destination tunnel to Netskope portal. See Create Business Policy for Non SD-WAN Destination.

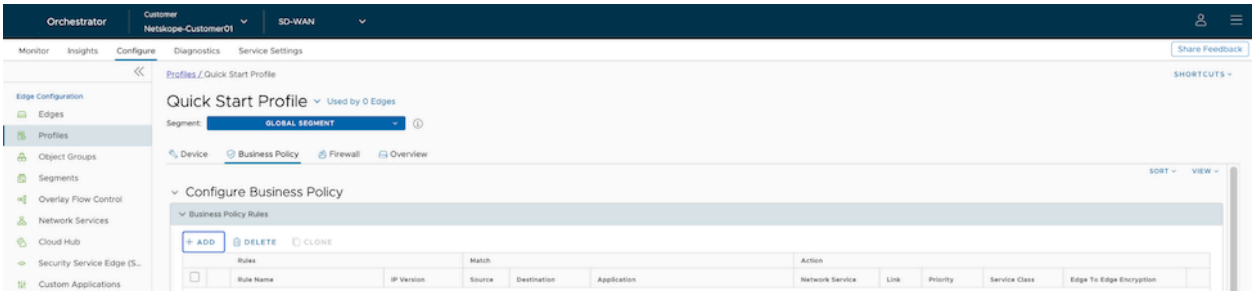
5.2 Create Business Policy for Non SD-WAN Destination

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.

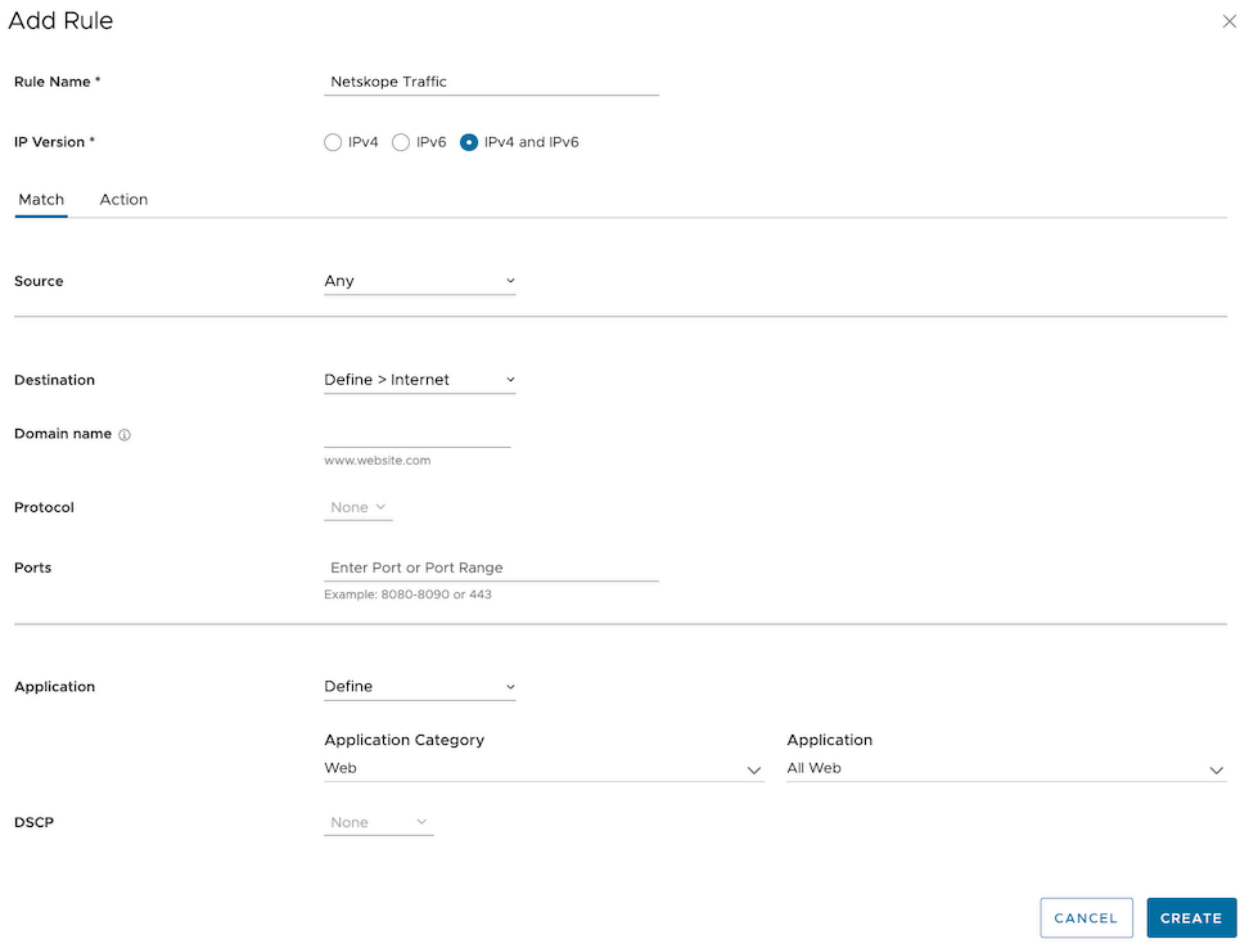
1. In the **Enterprise** portal, select **Configure** > **Profiles**.
2. Select a profile from the list and select the **Business Policy** tab.
3. Select **New Rule** or **Actions** > **New Rule**.
4. Enter a name for the business rule.

Figure 5-9: Business Rule Name



5. In the **Match** area, select **Define** and choose **Internet** as the Destination.

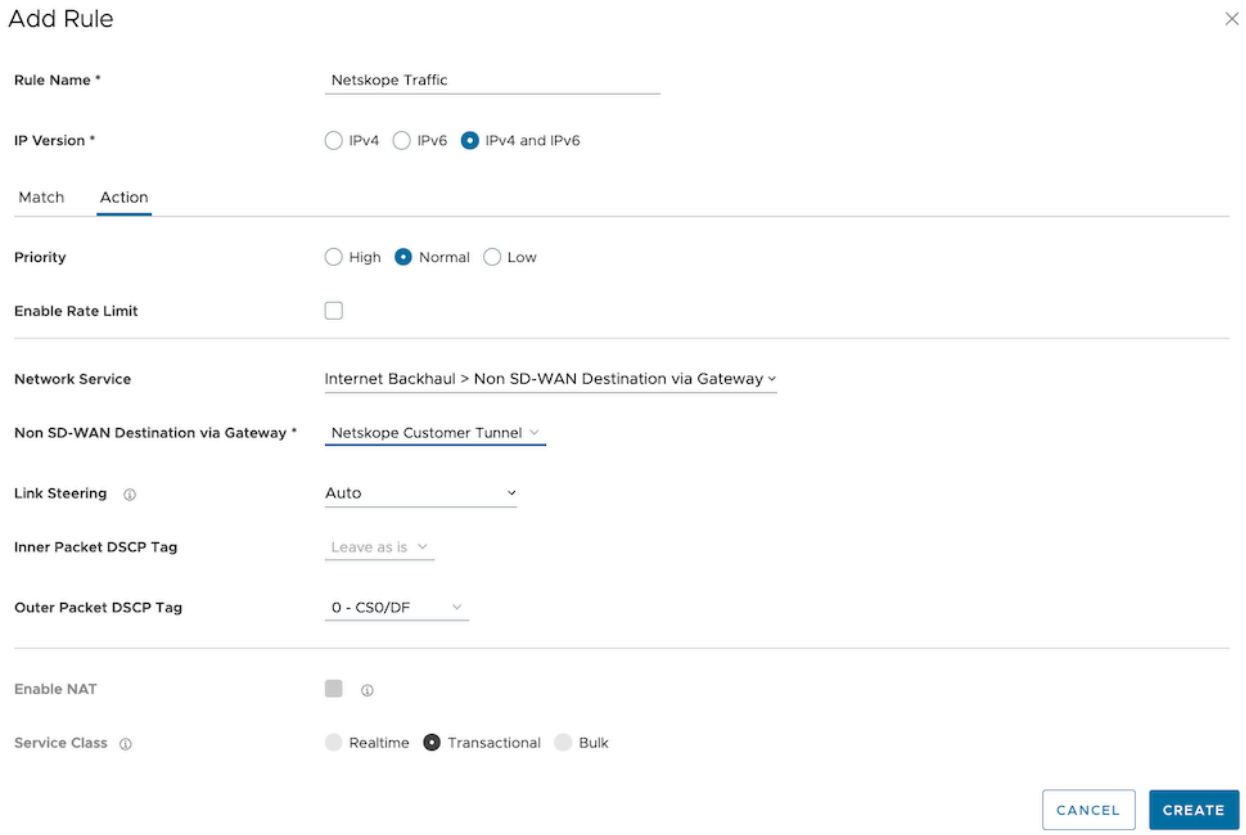
Figure 5-10: Destination > Internet



6. Select the **Application** as **Web**.

7. In the **Action** area, select **Internet Backhaul** as the Network Service and choose **Non SD-WAN Destination via Gateway** and select the Non SD-WAN Destination service created with the Netskope tunnel parameters..

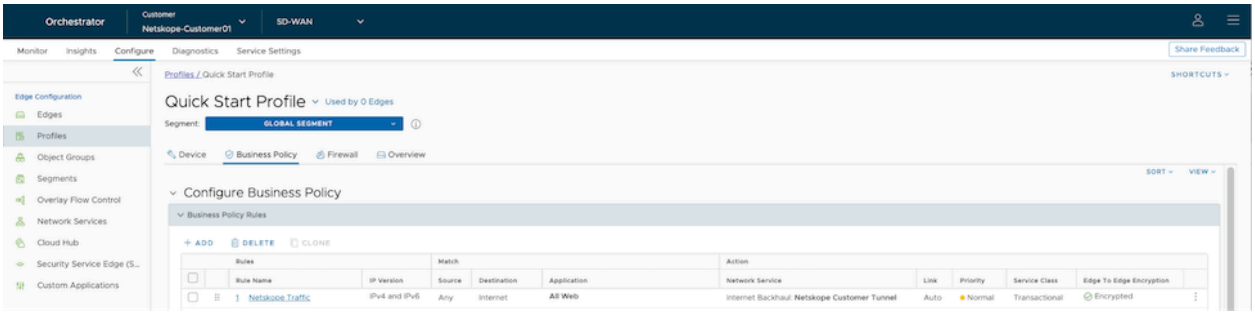
Figure 5-11: Internet Backhaul



8. Choose the other actions as required and select **Create**.

The Business Policy redirects the Internet destined HTTP/HTTPS traffic to Netskope POP using the IPSEC tunnel. The newly created policy installed at the top and inspected first.

Figure 5-12: Displaying the Business Rule



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

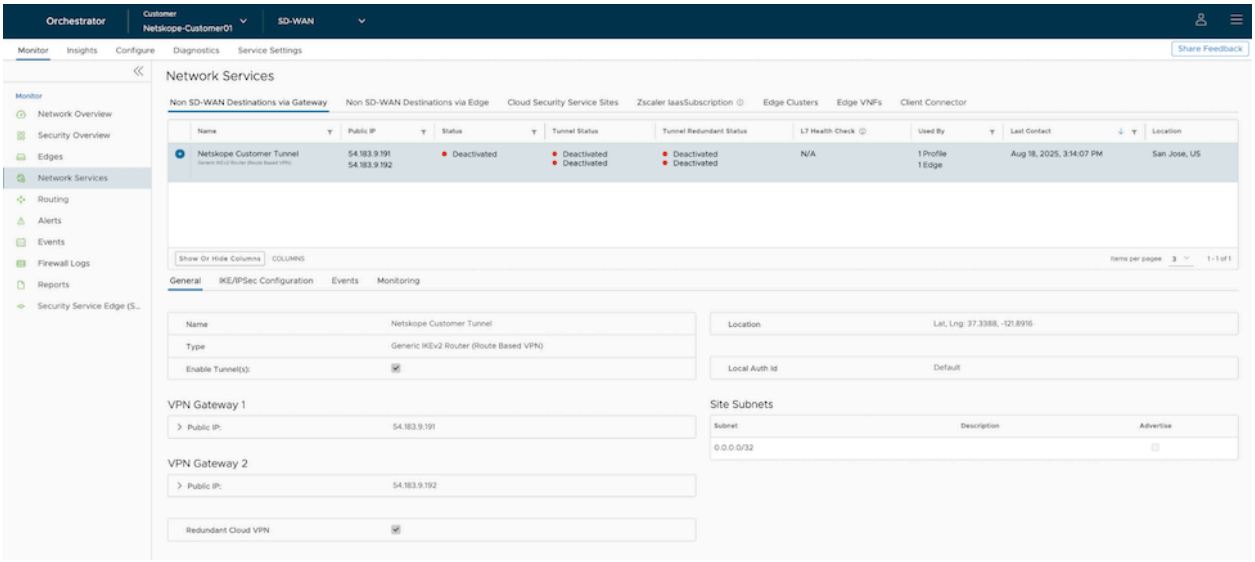
5.3 Monitor Non SD-WAN Destination via Gateway

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.

Figure 5-13: Monitoring the Non SD-WAN Destination via Gateway



Test and Verify Security Policies

Configure security policies in the Netskope security cloud to validate connectivity between the Netskope and VeloCloud SD-WAN traffic.

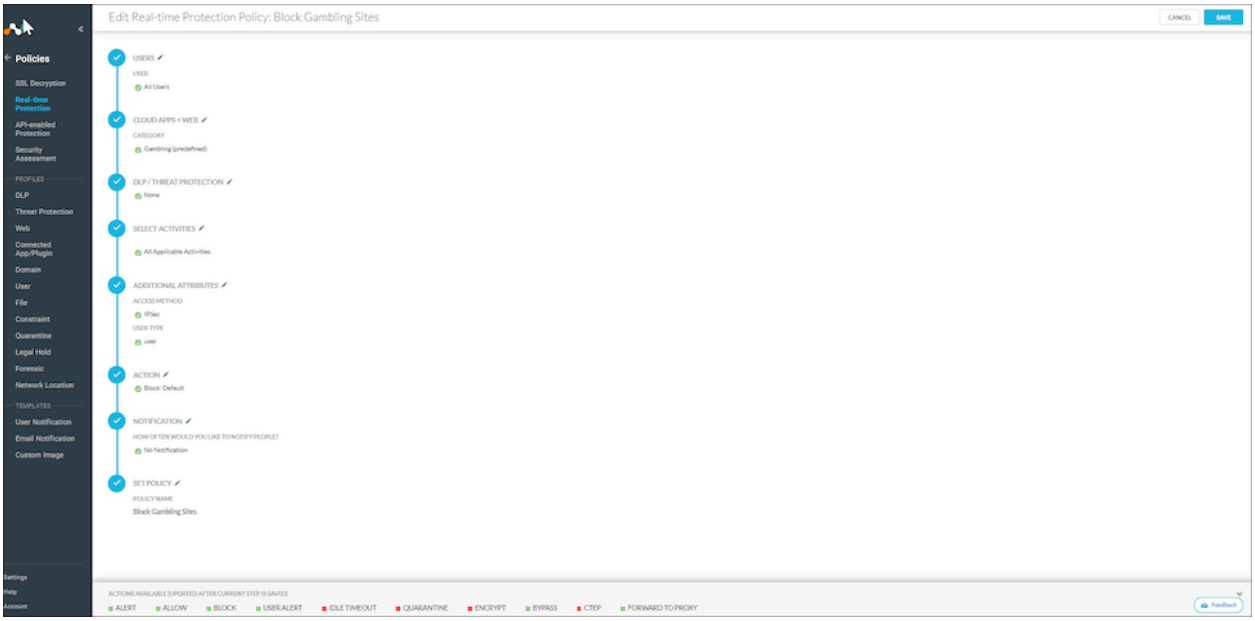
Ensure that the IPSEC tunnels to both the Primary and Secondary Netskope POPs connected successfully.

The following steps provide an example of blocking gambling-related websites by configuring the security policies.

Note: You can skip this procedure if you already have active production traffic through the portals.

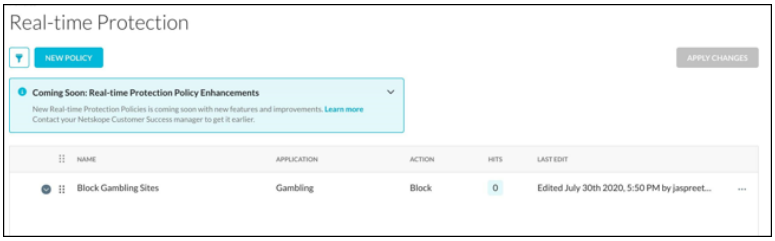
1. Login to the Netskope Next-generation Secure Web Gateway and navigate to **Policies** > **Real-time Protection**. Configure a policy to block all gambling-related web sites.

   Figure 6-1: Configuring a Policy



2. Confirm that the policy applied and note the number of current hits or matches against the policy. In the following example, there are 0 Hits.

Figure 6-2: Real-time Protection



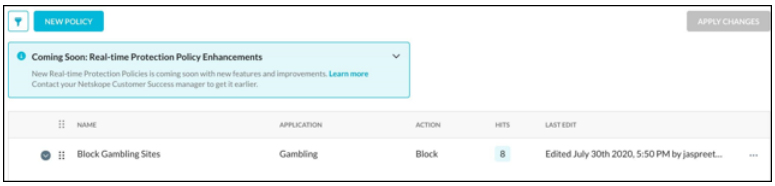
3. In the Edge, login to any Windows-based client on the LAN and try to browse any gambling-related website.

Figure 6-3: Displaying a Non-Compliant Action

Notice that the Netskope portal blocks the action as per the policy configured in the Netskope portal.

4. In the Netskope Next-Generation Secure Web Gateway, navigate to **Policies** > **Real-time Protection** and check the hit count for the **Block Gambling Sites** policy.

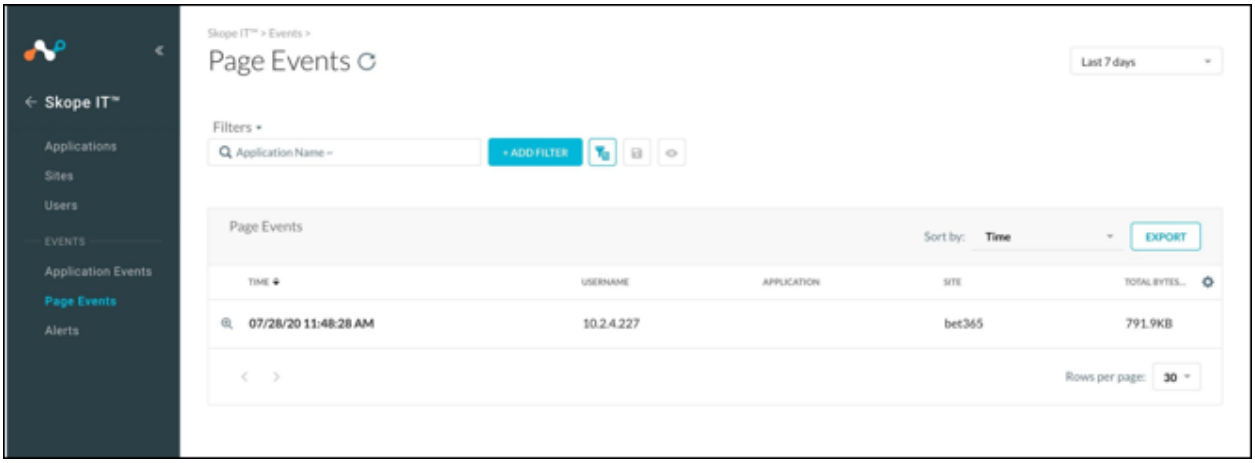
Figure 6-4: Monitoring the Activity



Notice that the hit count has incremented, which indicates active traffic passing through the Netskope Cloud Security platform.

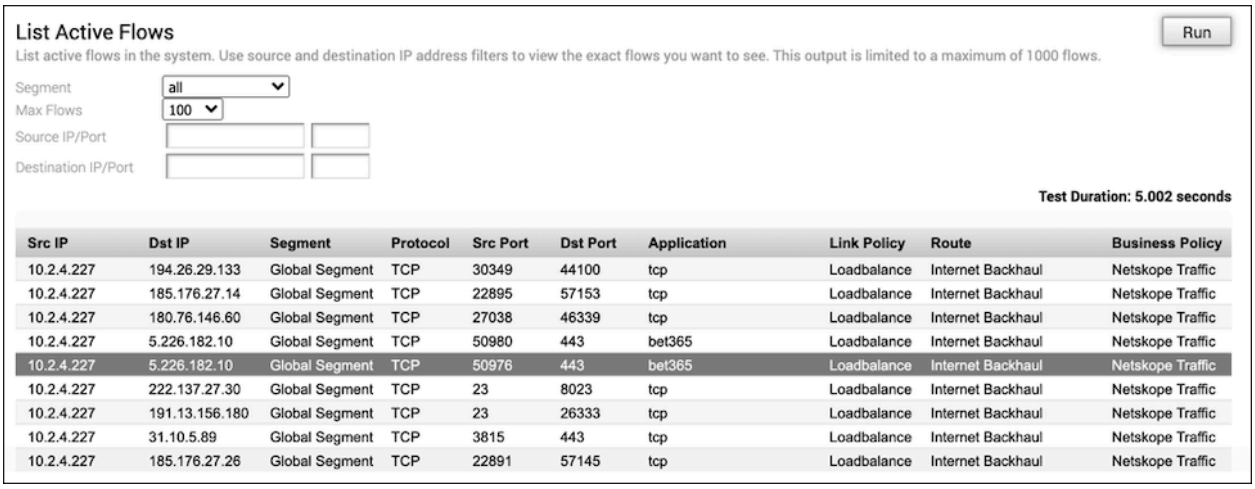
5. Navigate to the Skope IT portal and confirm the matches in the **Page Events** screen.

Figure 6-5: Displaying Page Events



6. Check the active flow in VeloCloud Edge Cloud Orchestrator portal to verify that the traffic hit the Non SD-WAN Destination via Gateway, for ultimate delivery to the Netskope security cloud.
7. In the **Enterprise** portal, select **Test & Troubleshoot** > **Remote Diagnostics**.
8. The **Remote Diagnostics** page displays all the active Edges.
9. Select the Edge configured with Non SD-WAN Destination via Gateway. The Edge enters live mode and displays all the possible Remote Diagnostics tests than you can run on the Edge.
10. Scroll down to the **List Active Flows** section and select **Run** to view the traffic flow.

Figure 6-6: List Active Flows



Src IP	Dst IP	Segment	Protocol	Src Port	Dst Port	Application	Link Policy	Route	Business Policy
10.2.4.227	194.26.29.133	Global Segment	TCP	30349	44100	tcp	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	185.176.27.14	Global Segment	TCP	22895	57153	tcp	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	180.76.146.60	Global Segment	TCP	27038	46339	tcp	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	5.226.182.10	Global Segment	TCP	50980	443	bet365	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	5.226.182.10	Global Segment	TCP	50976	443	bet365	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	222.137.27.30	Global Segment	TCP	23	8023	tcp	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	191.13.156.180	Global Segment	TCP	23	26333	tcp	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	31.10.5.89	Global Segment	TCP	3815	443	tcp	Loadbalance	Internet Backhaul	Netskope Traffic
10.2.4.227	185.176.27.26	Global Segment	TCP	22891	57145	tcp	Loadbalance	Internet Backhaul	Netskope Traffic

Notice that the traffic destined to the URL **`http://www.bet365.com`** has transited through the Internet Backhaul route and then to the Netskope security cloud.

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*