

# Cisco Catalyst SD-WAN Integration with Netskope Configuration Guide

## Overview

Cisco and Netskope have collaborated to offer customers a leading Secure Access Service Edge (SASE) solution. This solution provides a simple and effortless way to set up tunnels and direct traffic to Netskope. It has been tested and validated for use with Cisco IOS XE SD-WAN routers that run on software versions 17.9 or 20.9 (August – 2022), as well as the Netskope cloud dashboard. The most significant advantage for customers is the easy implementation of a complete end-to-end solution for SD-WAN and security.

Cisco Catalyst SD-WAN integration with Netskope is used for north-south traffic that is leaving the SD-WAN branch and destined for the internet or a Software-as-a-Service (SaaS) application and needs to be inspected at Netskope.

## Features

### Connectivity

- **Connection Types:** IPsec & GRE
- **Bandwidth (BW):** 2Gbps for IPsec and GRE

### Foundational Features

- Configuration simplification using reusable SIG templates
- Tunnel health check using L7 probes
- Redundancy: Active – Backup tunnel
- Redirection for internet-bound traffic
- Customized tunnel naming for easy monitoring and troubleshooting

### Advanced Feature Set

- **Granular traffic redirection:** Traffic policies based on IP/user/applications
- **Enhanced throughput:** 4 active and 4 backup tunnels

- **Traffic Load Balancing:** Equal Cost Multipath (ECMP) and weighted load balancing
- **CoR for SaaS applications:** Ability to select the best tunnel for a given application

### Monitoring/Visibility

- Tunnel Status, Application health, Tunnel and Application Statistics

## Prerequisites

- Netskope SSE cloud platform.
- We have tested this on version 17.9 software on the Cisco Catalyst™ 8000 platform.

**Step 1:** Set up tunnels on the Netskope SSE cloud platform. Generic Routing Encapsulation (GRE) and IPsec configurations are shown.

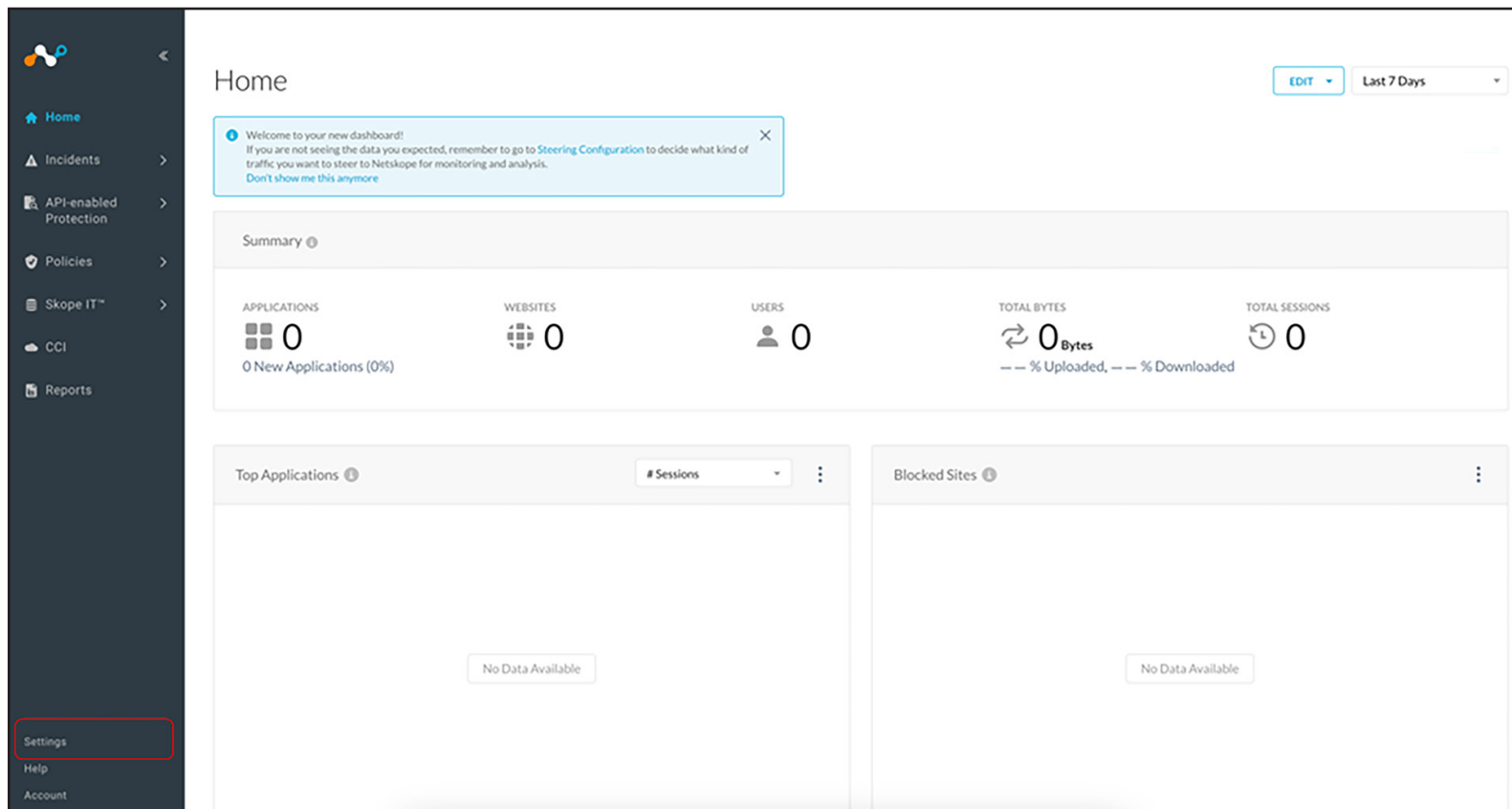
**Step 2:** Set up tunnels on the Catalyst SD-WAN Manager (formerly vManage) platform using Secure Internet Gateway (SIG) templates.

**Step 3:** Set up policy to route traffic to Netskope.

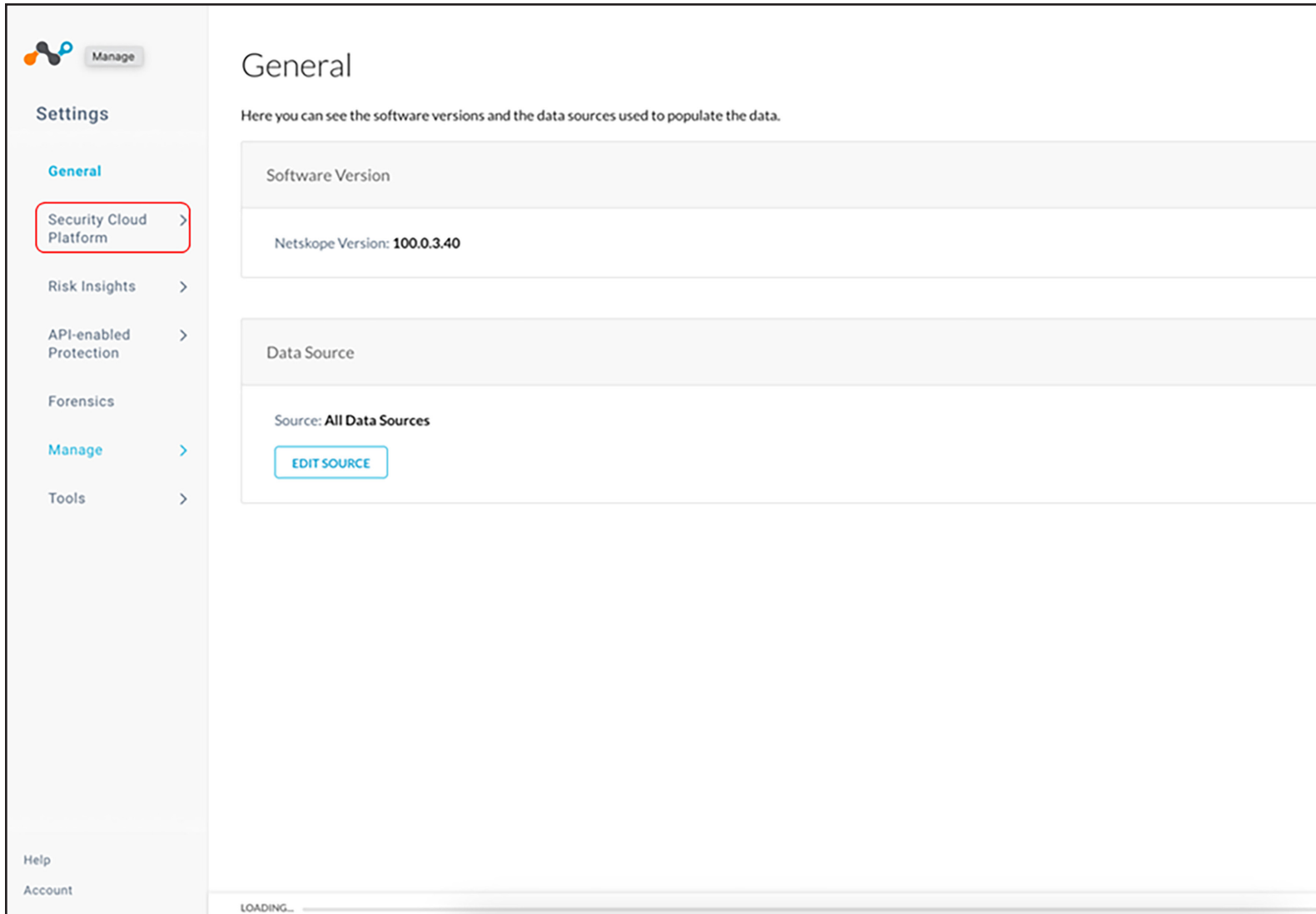
## Step 1: Logging into SD-WAN manager

Open the SD-WAN manager and the SIG templates. All the configuration for setting up a connection to Netskope has to be done on this SIG template. Within a few minutes, this template can be configured and pushed out to hundreds or even thousands of your devices.

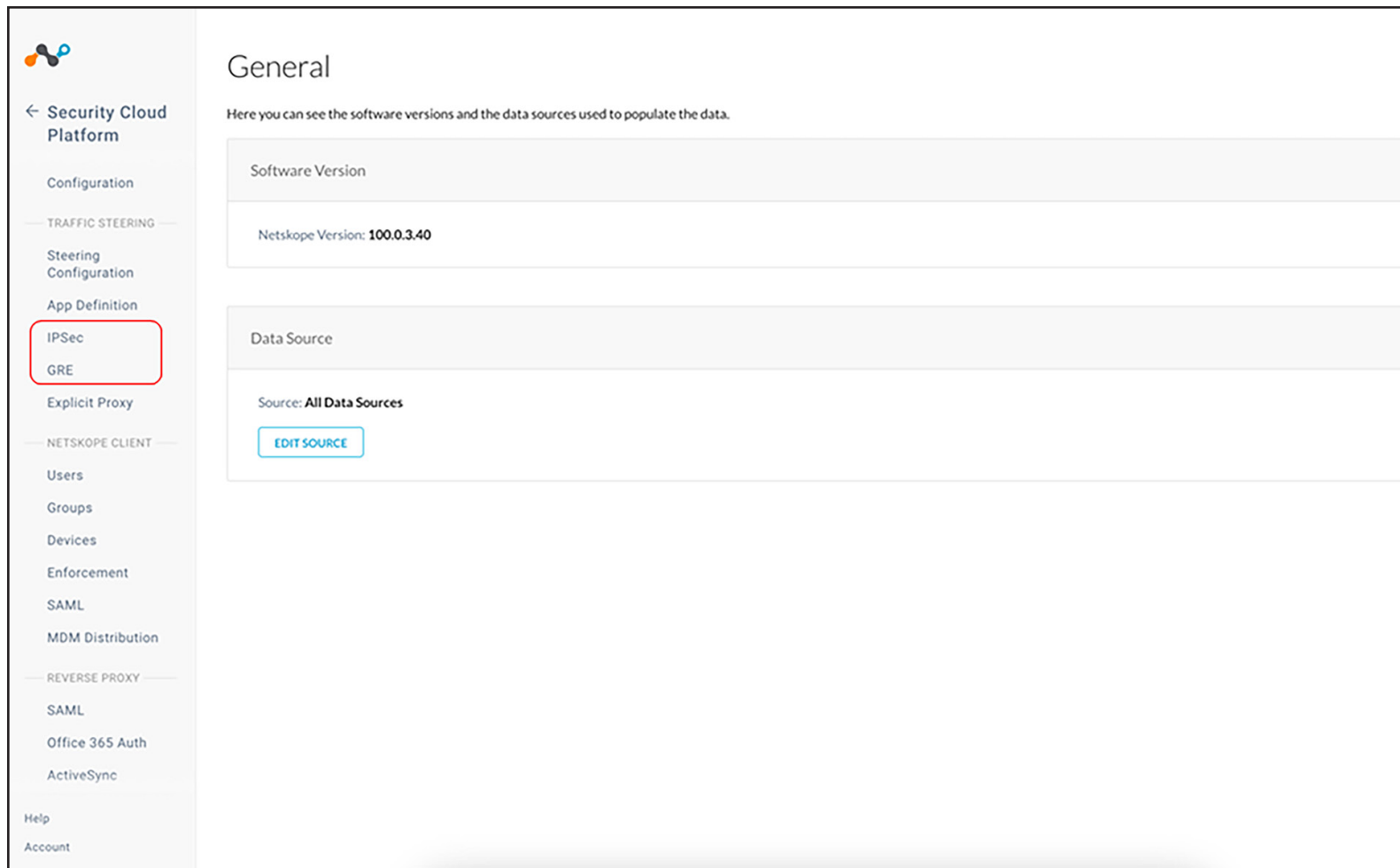
**GRE tunnel setup:** On the Netskope dashboard, go to Settings -> Security Cloud Platform and choose IPsec or GRE tunnels.



The screenshot displays the Netskope Home dashboard. On the left is a dark sidebar with navigation items: Home, Incidents, API-enabled Protection, Policies, Skope IT™, CCI, Reports, Settings (highlighted with a red box), Help, and Account. The main content area is titled "Home" and includes an "EDIT" button and a "Last 7 Days" filter. A blue notification box at the top states: "Welcome to your new dashboard! If you are not seeing the data you expected, remember to go to Steering Configuration to decide what kind of traffic you want to steer to Netskope for monitoring and analysis. Don't show me this anymore". Below this is a "Summary" section with five metrics: APPLICATIONS (0 New Applications (0%)), WEBSITES (0), USERS (0), TOTAL BYTES (0 Bytes, -- % Uploaded, -- % Downloaded), and TOTAL SESSIONS (0). At the bottom are two panels: "Top Applications" (with a "# Sessions" dropdown) and "Blocked Sites", both showing "No Data Available".



The screenshot shows the 'General' settings page for the Cisco Security Cloud Platform. On the left is a navigation sidebar with a 'Manage' button at the top. Below it are menu items: 'Settings', 'General' (highlighted in blue), 'Security Cloud Platform' (highlighted with a red box), 'Risk Insights', 'API-enabled Protection', 'Forensics', 'Manage', and 'Tools'. At the bottom of the sidebar are 'Help' and 'Account' links. The main content area is titled 'General' and contains the text: 'Here you can see the software versions and the data sources used to populate the data.' There are two main sections: 'Software Version' and 'Data Source'. The 'Software Version' section shows 'Netskope Version: 100.0.3.40'. The 'Data Source' section shows 'Source: All Data Sources' and an 'EDIT SOURCE' button. A 'LOADING...' indicator is visible at the bottom of the main content area.



The screenshot shows the Cisco Security Cloud Platform configuration interface. On the left is a navigation menu with the following items: Security Cloud Platform, Configuration, TRAFFIC STEERING, Steering Configuration, App Definition, IPsec (highlighted with a red box), GRE, Explicit Proxy, NETSKOPE CLIENT, Users, Groups, Devices, Enforcement, SAML, MDM Distribution, REVERSE PROXY, SAML, Office 365 Auth, ActiveSync, Help, and Account. The main content area is titled "General" and contains the following information:

- Software Version: Netskope Version: **100.0.3.40**
- Data Source: Source: **All Data Sources** with an **EDIT SOURCE** button.

To create the tunnel, you need to obtain the IPs of the Netskope Points of Presence (POPs), which are shown below. You can choose the PoP based on the geographical location. This IP will be used to configure the SD-WAN Manager SIG templates later.

Then click “New GRE configuration” and enter the name of the tunnel and the source IP of the Cisco Catalyst SD-WAN router from which the tunnel is originating, as shown below.

GRE

Last Updated: 10-5-2022 5:55:32 PM

Security Cloud Platform > Traffic Steering >

GRE tunneling is one of the several methods to steer traffic. Using existing network infrastructure, you can quickly and easily send web traffic to Netskope. See [help documentation](#) for the prerequisites then create and manage GRE tunnels from your source devices such as routers and firewalls to Netskope's point of presence (POPs).

+ ADD FILTER

NEW GRE CONFIGURATION

NETSKOPE POPS

GRE Configurations Sort by: **Name** ▾ ENABLE DISABLE DELETE

1 CREATED

NAME	SOURCE IDENTITY	NETSKOPE POP	USER TRAFFI...	USER TRAFFIC LAST UPDATED	KEEPALIVE LAST UPDATED	KEEPALL...	THROUGHPUT
<input type="checkbox"/> Cisco-GRE-Gowri	128.107.85.120	NYC1 - New York, NY, US	● Not Seen	10-3-2022 10:44:32 AM	10-5-2022 5:55:32 PM	● Not Seen	0.00 Kbps
		LAX1 - Los Angeles, CA, US	● Not Seen	10-3-2022 7:56:03 PM	9-27-2022 8:04:03 PM	● Not Seen	0.00 Kbps

◀ 1 ▶
Rows per page: 10 ▾

Netskope POPs
✕

Use the information of Netskope POPs to configure the tunnel on your peer device. For best performance, select the geographically closest POPs and configure at least two tunnels for each egress location.

- + LAX1 - Los Angeles, CA, US
 

Gateway: 163.116.132.36

Probe IP Address: 10.132.6.209

Location: Los Angeles, CA, US
- + NYC1 - New York, NY, US
- + PAR1 - Paris, FR
- + STO1 - Stockholm, SE
- + ATL1 - Atlanta, GA, US
- + SEA1 - Seattle, WA, US
- + LON1 - London, GB
- + ORD1 - Chicago, IL, US
- + MEL1 - Melbourne, AU
- + MIA1 - Miami, FL, US
- + FRA1 - Frankfurt, DE
- + HKG1 - Hong Kong, HK
- + JNB1 - Johannesburg, ZA

CANCEL

New GRE Configuration
✕

Traffic will be steered from your source devices (e.g. router, firewall) to Netskope points of presence (POPs).

CONFIGURATION NAME \*

✖ Please Specify the configuration name

TUNNEL TYPE \*

Default

SOURCE PEER \*

i Remember to configure the tunnel on your peer device using the Netskope POPs information to complete the tunnel configuration.

**▶ Advanced Settings**

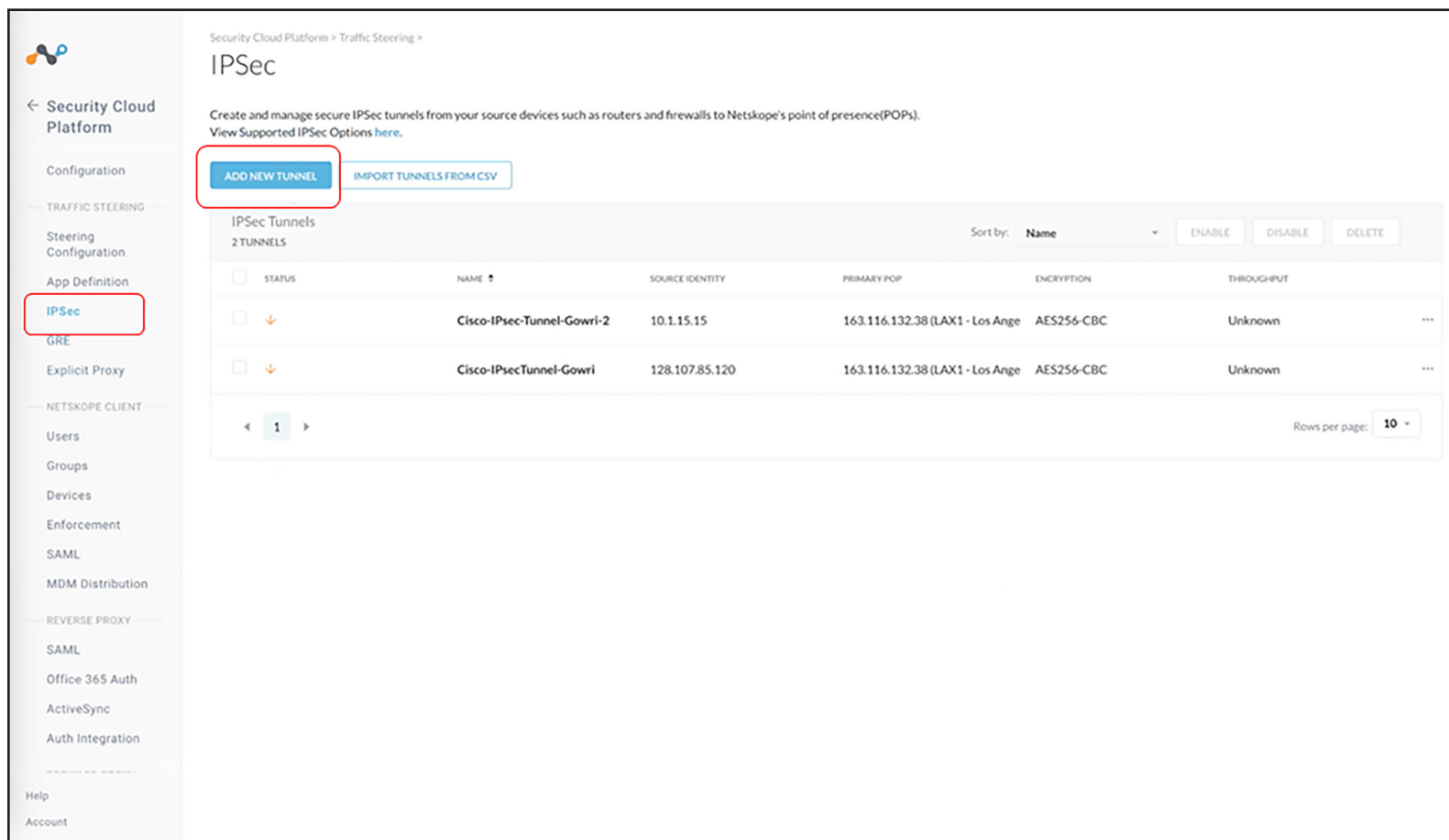
CANCEL

SAVE AND VIEW POPs

SAVE

You can have multiple tunnels (up to four) for redundancy purposes, originating from the same source IP but terminating at different Netskope POPs.

**IPsec tunnel setup:** Go to the IPsec section and click “Add new tunnel” as shown below.



Security Cloud Platform > Traffic Steering > IPsec

Create and manage secure IPsec tunnels from your source devices such as routers and firewalls to Netskope's point of presence (POPs).  
View Supported IPsec Options [here](#).

**ADD NEW TUNNEL** IMPORT TUNNELS FROM CSV

IPsec Tunnels  
2 TUNNELS

Sort by: Name

STATUS	NAME	SOURCE IDENTITY	PRIMARY POP	ENCRYPTION	THROUGHPUT
<input type="checkbox"/>	Cisco-IPsec-Tunnel-Gowri-2	10.1.15.15	163.116.132.38 (LAX1 - Los Ange	AES256-CBC	Unknown
<input type="checkbox"/>	Cisco-IPsecTunnel-Gowri	128.107.85.120	163.116.132.38 (LAX1 - Los Ange	AES256-CBC	Unknown

Rows per page: 10


Enter the tunnel name and source IP address or Fully Qualified Domain Name (FQDN). Select the IPsec POPs from the drop-down. Use both primary and secondary tunnel POP IPs for redundancy. The preshared keys and cipher for encryption of the IPsec tunnel will be shown on the screen and can be matched on the SD-WAN Manager side. You can also choose the maximum bandwidth required.

### Add New IPsec Tunnel

**Tunnel Peers**  
Traffic will be steered from your source devices to Netskope points of presence(POPs). For best performance, select the geographically closest POPs. Only IKEv2 is supported

**Note:** Use the Netskope POP's IP address as tunnel's remote identity.

TUNNEL NAME \*  
Enter a name to remember the tunnel by



SOURCE IP ADDRESS ⓘ  
Enter IP Address

SOURCE IDENTITY \*  
Enter IP Address or FQDN

⊗ Specify the Source Identity

PRIMARY NETSKOPE POP \*  
163.116.132.38 (LAX1 - Los Ar ▾)

FAILOVER NETSKOPE POP \*  
163.116.135.38 (NYC1 - New \ ▾)

The source identity of the tunnel must be unique across all IPsec tunnels set up.

PRE-SHARED KEY (PSK) \*  
.....

ENCRYPTION CIPHER \*  
AES128-CBC ▾


MAXIMUM BANDWIDTH \*  
Maximum bandwidth to be used by the IPsec tunnel  
50 Mbps ▾

▶ Advanced Settings

CANCEL SAVE CANCEL SAVE

### Add New IPsec Tunnel

Enter a name to remember the tunnel by



SOURCE IP ADDRESS ⓘ  
Enter IP Address

SOURCE IDENTITY \*  
Enter IP Address or FQDN

⊗ Specify the Source Identity

PRIMARY NETSKOPE POP \*  
163.116.132.38 (LAX1 - Los Ar ▾)

FAILOVER NETSKOPE POP \*  
163.116.135.38 (NYC1 - New \ ▾)

The source identity of the tunnel must be unique across all IPsec tunnels set up.

PRE-SHARED KEY (PSK) \*  
.....

ENCRYPTION CIPHER \*  
AES128-CBC ▾

MAXIMUM BANDWIDTH \*  
Maximum bandwidth to be used by the IPsec tunnel  
50 Mbps ▾

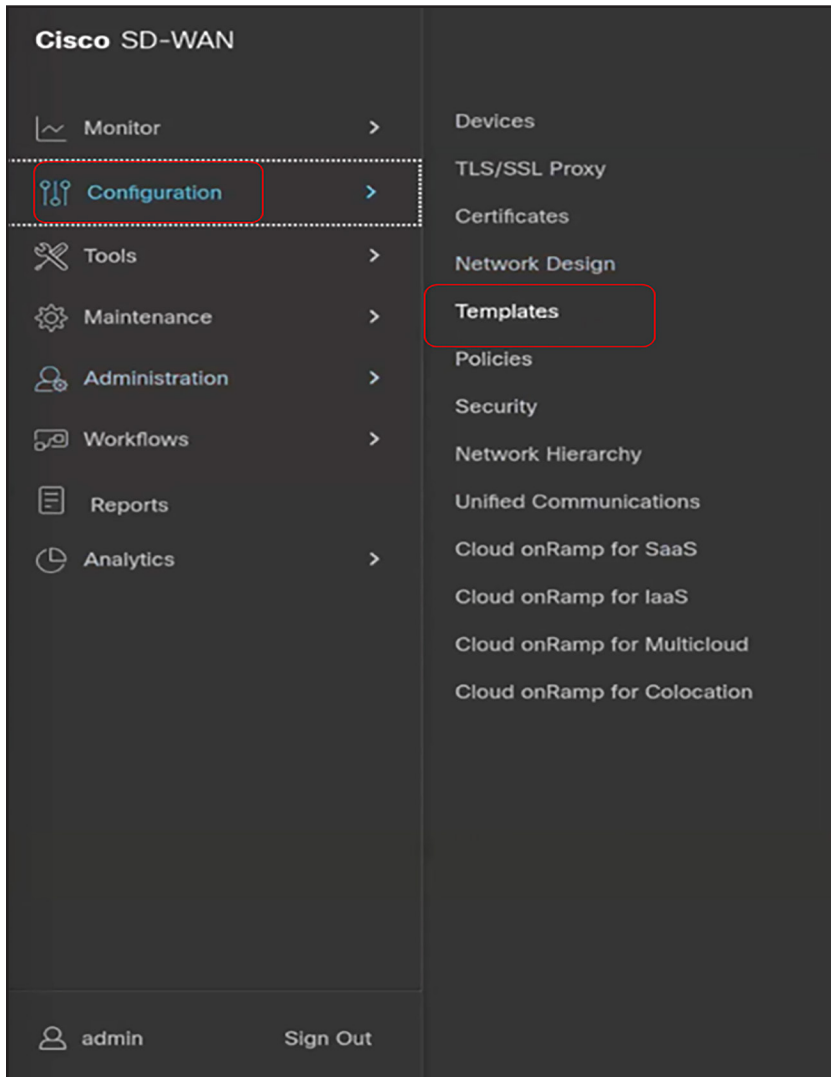
▶ Advanced Settings

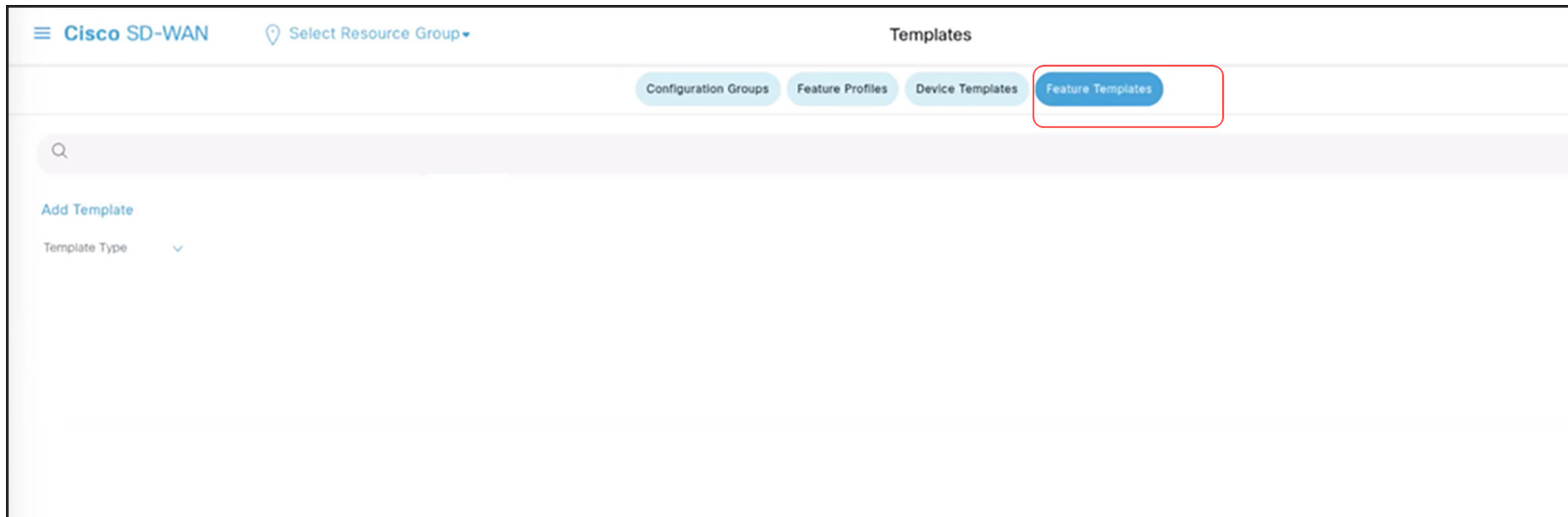
CANCEL SAVE



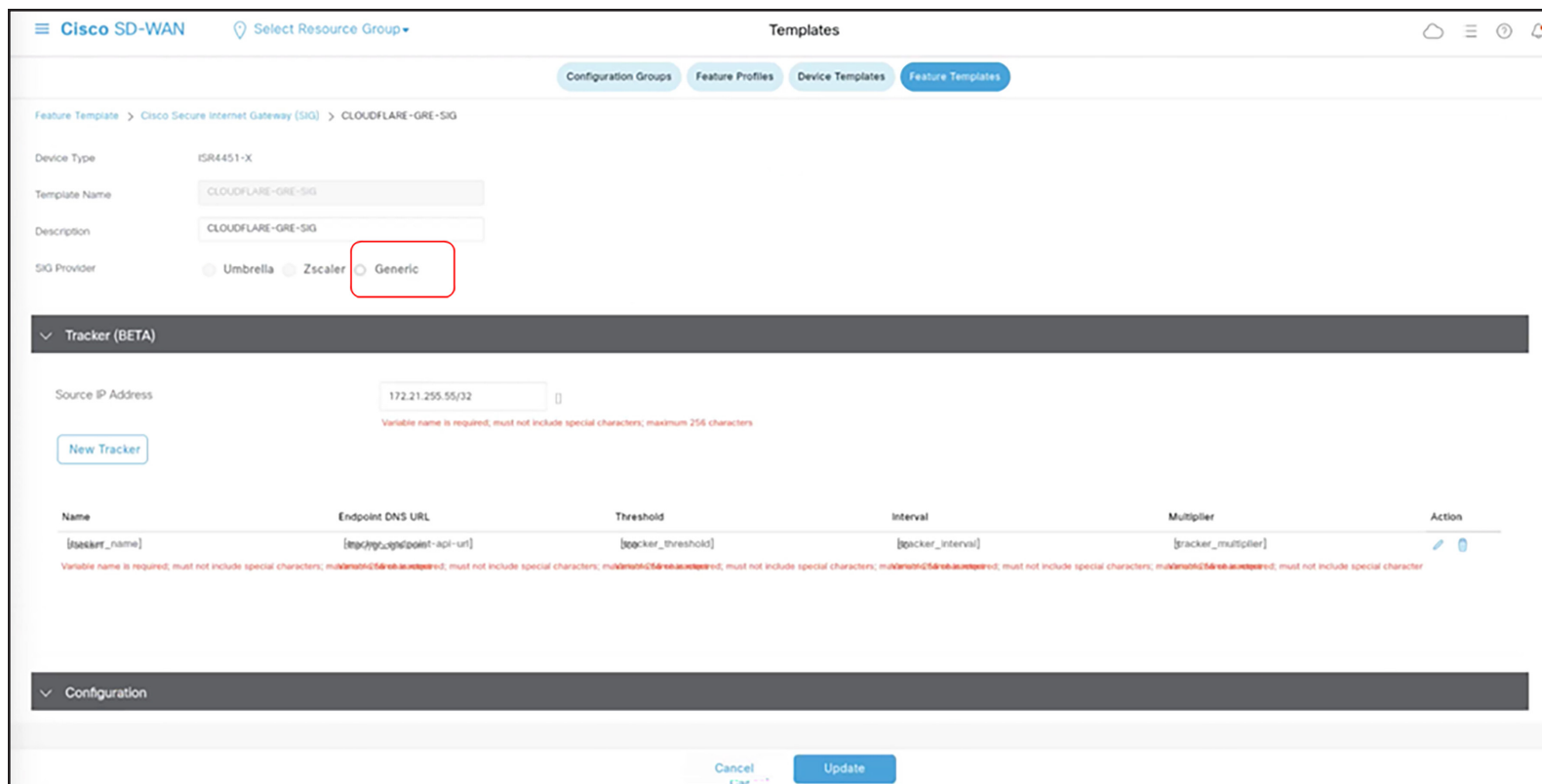
**Step 2:**

To set up tunnels in SD-WAN Manager using SIG templates, navigate to the SD-WAN Manager, select Configuration -> Templates -> Feature Template -> Create a SIG template. This will allow for easy and efficient configuration of tunnels on the Cisco Catalyst SD-WAN platform.





- In the SIG template, select the Generic tunnel option.
- Create a tracker to ensure the health of the tunnel. For this, you can use any stable IP address. In the given example, google.com has been used as the endpoint address.



The screenshot shows the Cisco SD-WAN configuration interface for a Feature Template. The breadcrumb trail is: Feature Template > Cisco Secure Internet Gateway (SIG) > CLOUDFLARE-GRE-SIG. The configuration fields are as follows:

- Device Type: ISR4451-X
- Template Name: CLOUDFLARE-GRE-SIG
- Description: CLOUDFLARE-GRE-SIG
- SIG Provider: Umbrella, Zscaler, **Generic** (highlighted with a red box)

Below the provider selection is a section for "Tracker (BETA)". The "Source IP Address" field contains "172.21.255.55/32" and has a red error message: "Variable name is required, must not include special characters; maximum 256 characters". A "New Tracker" button is located below this field.

A table lists the configured trackers:

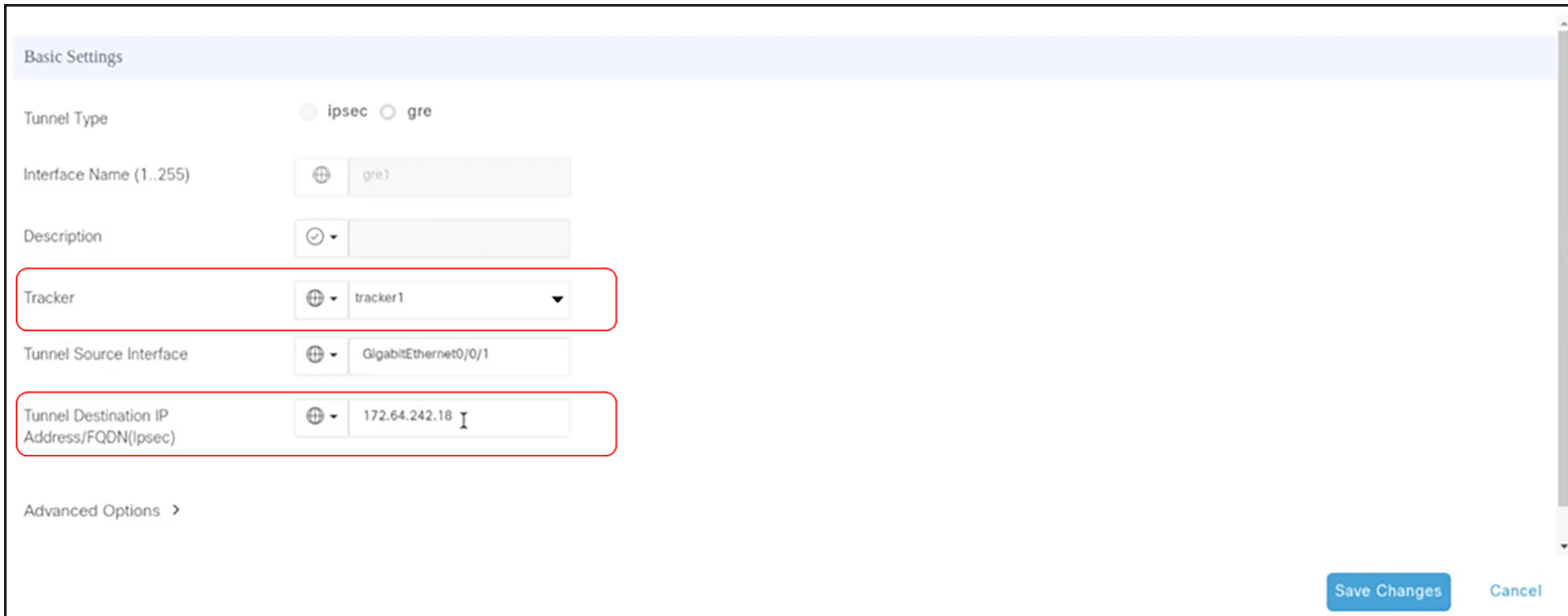
Name	Endpoint DNS URL	Threshold	Interval	Multiplier	Action
[tracker_name]	[tracker_endpoint-api-url]	[tracker_threshold]	[tracker_interval]	[tracker_multiplier]	[edit] [delete]

Below the table is a red error message: "Variable name is required, must not include special characters; maximum 256 characters; must not include special characters; maximum 256 characters; must not include special characters; maximum 256 characters; must not include special characters; maximum 256 characters; must not include special characters".

At the bottom of the form are "Cancel" and "Update" buttons.

As part of the tunnel creation, select the tracker you created in the previous step from the drop-down.

Enter the IP of the Netskope POP endpoint for tunnel destination IP.



Basic Settings

Tunnel Type  ipsec  gre

Interface Name (1..255)

Description

Tracker

Tunnel Source Interface

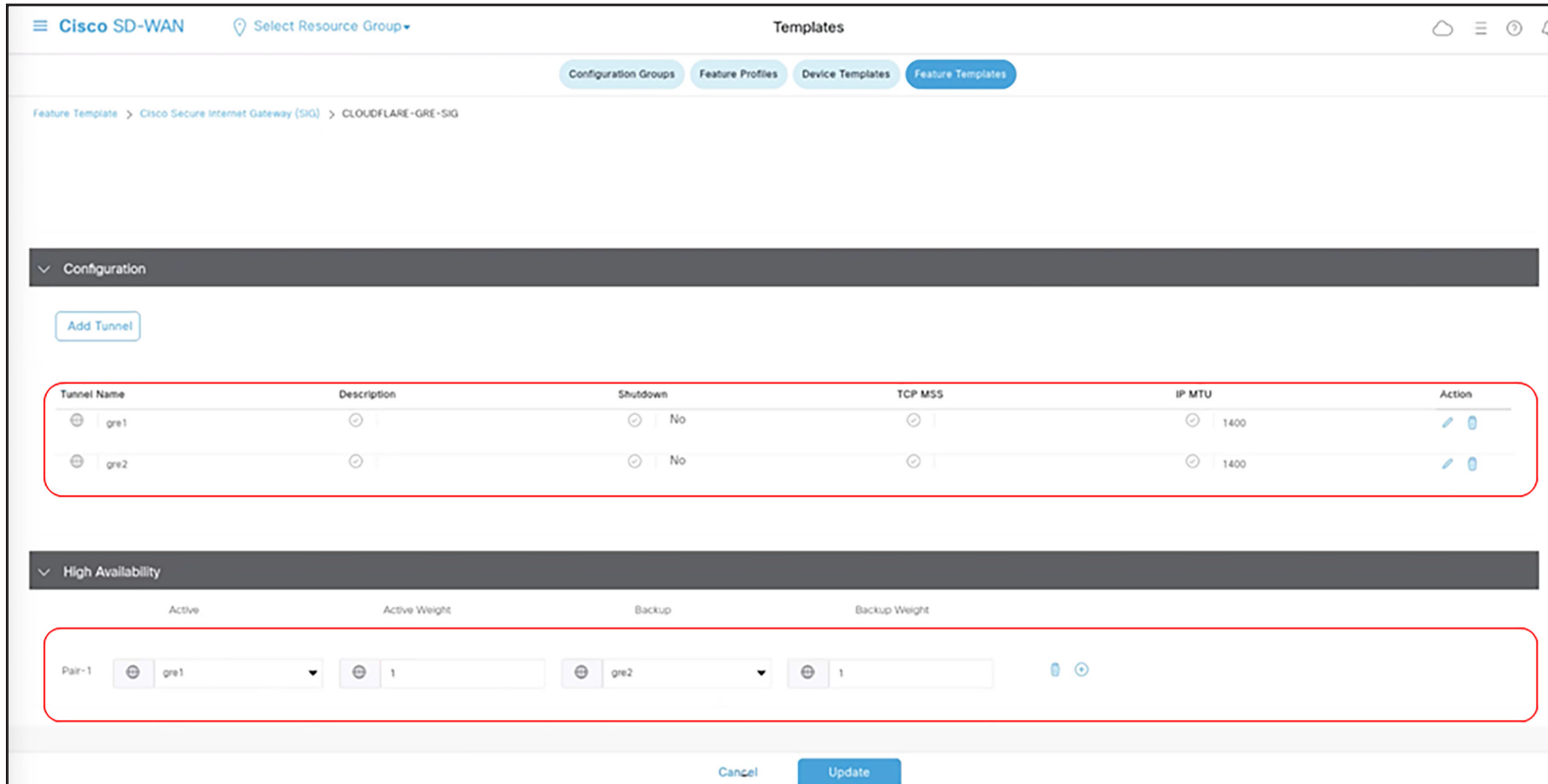
Tunnel Destination IP Address/FQDN(ipsec)

Advanced Options >

Save Changes Cancel





Standby tunnel: In a similar manner, create the standby tunnel and use the other Netskope POP IP.

Once the two tunnels are created, as seen below, add a High Availability (HA) configuration using these two tunnels. This helps ensure that traffic fails over to the secondary tunnel in case the primary one goes down.



**Configuration**

Add Tunnel

Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
gre1		No		1400	 
gre2		No		1400	 

**High Availability**

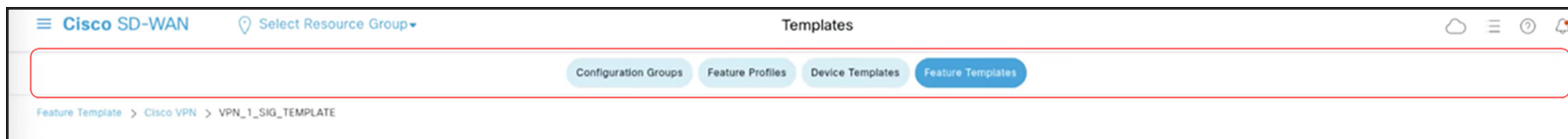
Active	Active Weight	Backup	Backup Weight	
Pair-1	gre1	1	gre2	1

Cancel Update

### Step 3: Setting up a route-based service route

To set up the route-based service route for sending traffic through the tunnels for inspection in Netskope before it reaches the destination, follow these steps:

1. Use a service route and select SIG from the drop-down. The tunnels will automatically be picked up.
2. Add the subnets of the specific traffic that needs to be inspected at Netskope.

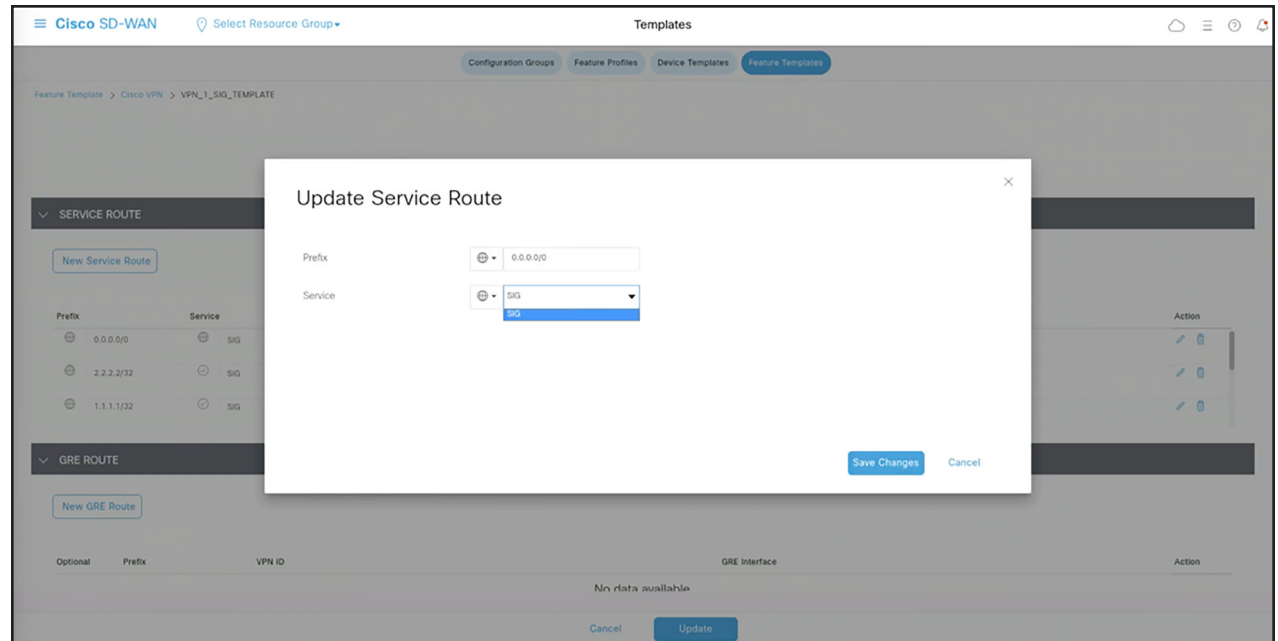


Feature Template > Cisco VPN > VPN\_1\_SIG\_TEMPLATE

## Try it now

Take the first step in modernizing your WAN architecture. Contact us for a free consultation on integrating your Cisco Catalyst SD-WAN with Netskope.

- [SDWAN@cisco.com](mailto:SDWAN@cisco.com).



## For more information

Learn more about Cisco Catalyst SD-WAN Security - <https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/sd-wan-security.html>