Guide
Cisco public

Cisco Catalyst SD-WAN Palo Alto Prisma SSE Cloud Integration User Guide

Contents

Overview 3

Cisco Catalyst SD-WAN SASE Integration with Palo Alto for Secure Internet Access 3

Features 3

Sample topology diagram 4

Redundancy connectivity matrix 5

Overview of configuration steps 6

For more information 13

Overview

The integration of Cisco® Catalyst® Software-Defined Wide Area Network (SD-WAN) with Palo Alto Prisma SSE cloud enables customers to enhance the security of their branch internet traffic through effective redirection. Leveraging Cisco Catalyst SD-WAN Secure Internet Gateway (SIG) templates, the implementation process becomes efficient and straightforward. These templates offer a simplified workflow for end-to-end configuration, encompassing vital features such as POP availability, application health checks, weighted load balancing, and data policy. With this integration, users can seamlessly specify the desired redirection of branch traffic to the Palo Alto Prisma cloud endpoint. It is important to note that the integration has undergone testing and validation within Cisco, ensuring seamless compatibility and reliable performance. Specifically, the testing and validation were conducted using the 17.9/20.9 (August 2022) SD-WAN software version on the cEdge device.

Cisco Catalyst SD-WAN SASE Integration with Palo Alto for Secure Internet Access

Use Case

This integration guide can be used as a reference for customers who run the Palo Alto Prisma Cloud–based Secure Service Edge (SSE) solution along with the Cisco Catalyst SD-WAN solution. It is designed for scenarios where the branch users' internet or SAAS application access needs to be inspected and secured by the Palo Alto Prisma SASE solution.

The Cisco Catalyst SD-WAN solution provides capability to integrate automatically with the Cisco SASE solution and other third-party solutions using automated or manual tunnel integrations (subject to the SASE provider). The flexibility allows users to select a unified SASE solution or a SASE provider of their choice.

Features

Connectivity

- **Connection Types:** IPsec
- **Bandwidth (BW):** 1Gbps for IPSec

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 & Application Statistics

Pre-requisites and validated environment

- Palo Alto Prisma Access Cloud platform.
- Cisco Catalyst SD-WAN Manager (formerly called vManage) 20.9, Cisco IOS-XE Release 17.9 for SD-WAN edge. We have tested this on 17.9 software on the Cisco Catalyst 8000 platform.
- A working knowledge of Cisco Catalyst SD-WAN configuration and features.

Sample topology diagram

The following tests have been conducted with redundancy in mind. In the example below, dual routers have been connected to redundant Prisma DC location

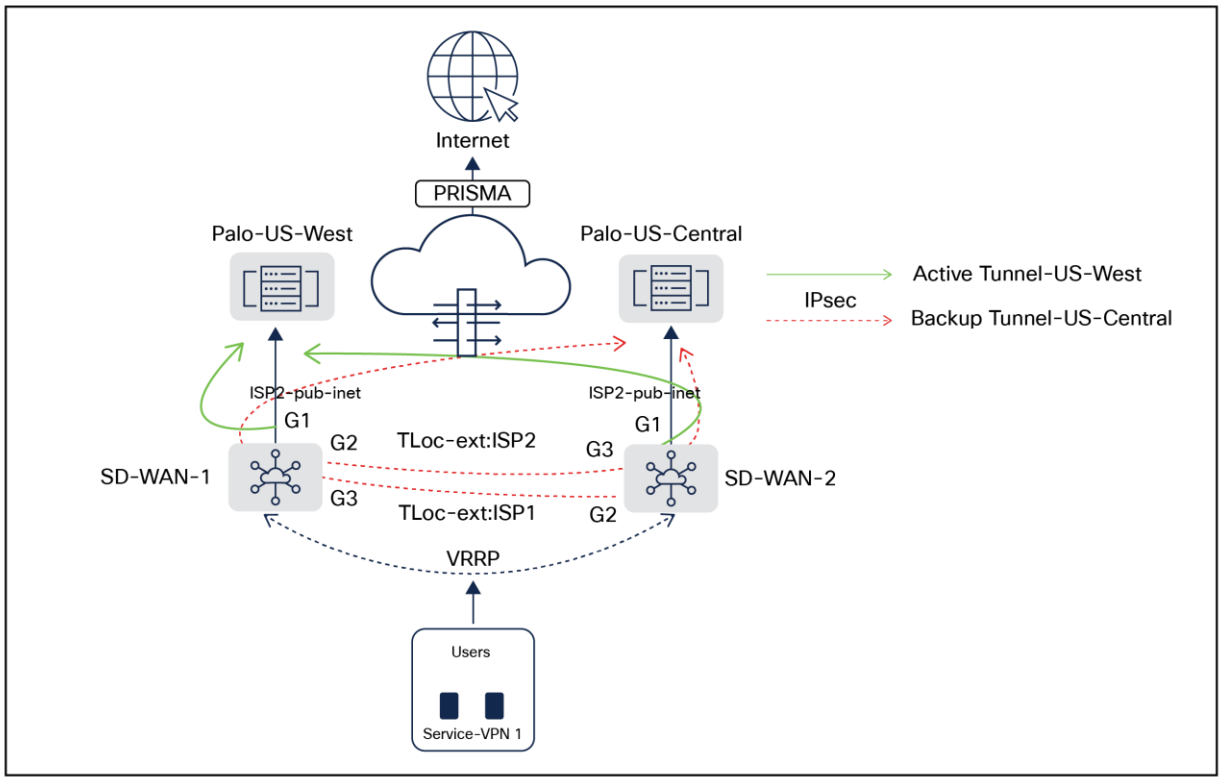


Figure 1.
Cisco Catalyst SD-WAN dual-homed branch connectivity to multi-region Palo Alto Datacenters using redundant ISP Links

In the above topology, two branch routers SD-WAN-1 and SD-WAN-2 are connected to redundant Palo Alto SASE Datacenter locations (West and Central) using redundant ISPs (Biz-internet and public-internet colors). The Tloc-extension feature has been used to provide cross- ISP connectivity from both routers. The service VPN can be redundantly configured using Layer 2 protocol such as Virtual Router Redundancy Protocol (VRRP) or Layer 3 routing protocols like Border Gateway Protocol (BGP) or other supported protocols. The architecture provides redundancy at tunnels, data center, ISP, and router levels. For higher throughput, customers are advised to use loopback-based Equal Cost Multi-Path (ECMP) tunnels under the SIG template and to configure a pair of additional HA sites on the Prisma Access side. SIG templates are used for connectivity, providing multiplexing capability to carry multiple service VPN (Virtual Routing and Forwarding [VRF]) traffic into the same set of tunnels, and are recommended by Cisco for any SIG connectivity.

Redundancy connectivity matrix

Router	ISP-Color	Prisma DC
SDWAN-1	Biz-internet (Gig1)	US-West (Primary Tunnel)
SDWAN-1	Public-internet (Gig2) using tloc-extension from SDWAN2	US-Central (Primary Tunnel)
SDWAN-2	Pub-internet (Gig1)	US-West (Secondary Tunnel)
SDWAN-2	Biz-internet (Gig2) using tloc-extension from SDWAN1	US-Central (Secondary Tunnel)

Note:

- BGP is not supported using the SIG template. For use cases requiring BGP support, configure IPsec tunnels using IPsec templates in Cisco Catalyst SD-WAN Manager. These tunnels are initiated per service VPN (VRF).
- Currently, IPsec tunnels along with the SIG-template are not supported from the same SD-WAN edges. It is recommended to choose a hub location for the IPsec template for any private application access use cases, and use the SIG-template at branch locations for secure internet access use cases.
- Inbound trackers from SIG providers are not supported using the SIG template. The SIG template already utilizes outbound trackers and enables failover traffic based on brownout conditions.

Traffic to SIG

The traffic from the service VPN can be redirected to SIG tunnels using either the default route to the service SIG, or using data policy redirect to service SIG, in case specific applications or traffic need to be redirected for secure internet/SAAS access. For further information on the SIG Template and Redirection policy, refer to the following guide.

Overview of configuration steps

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.

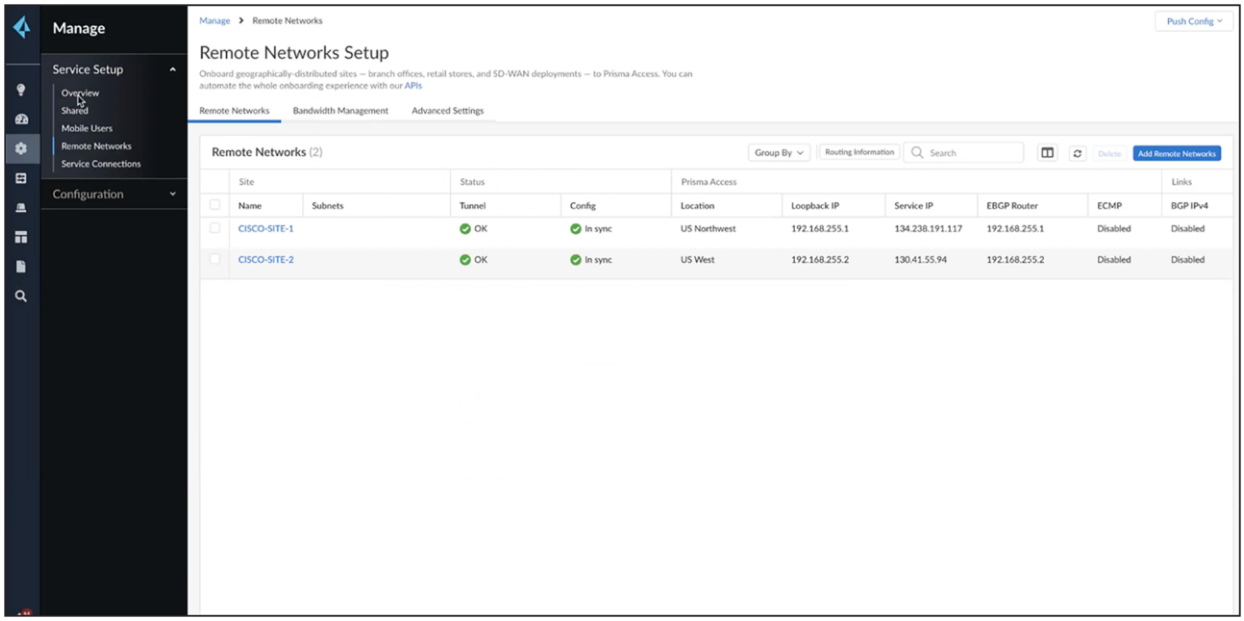
Note: Only IPSec is supported for Palo Alto Prisma; Generic Routing Encapsulation (GRE) is not supported.

Step 2. Set up tunnels on the Cisco Catalyst SD-WAN Manager platform using SIG templates

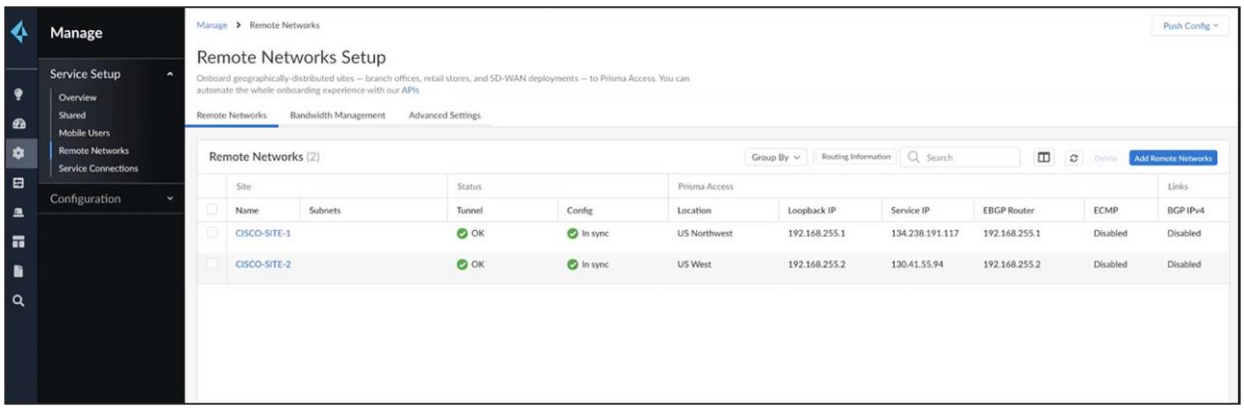
Step 3. Set up policy to route traffic to Palo Alto

Step 1. Palo Alto setup

IPSec Tunnel Setup:



Go to overview -> Manage -> Remote networks. Create the IPSec endpoints as shown below.

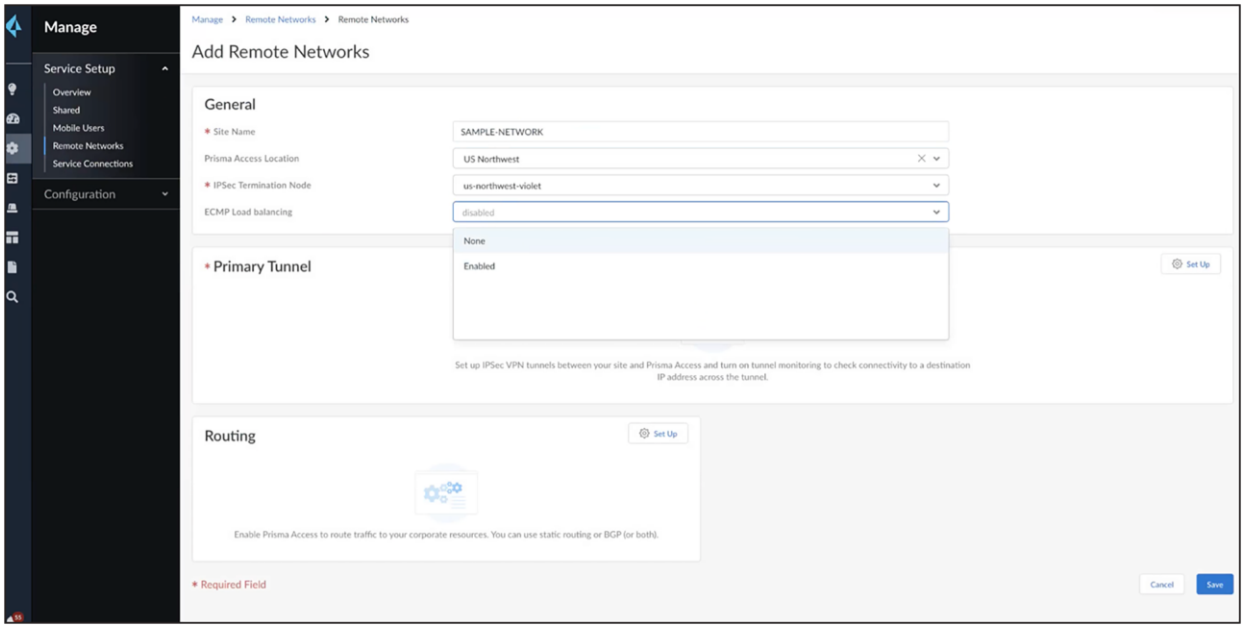


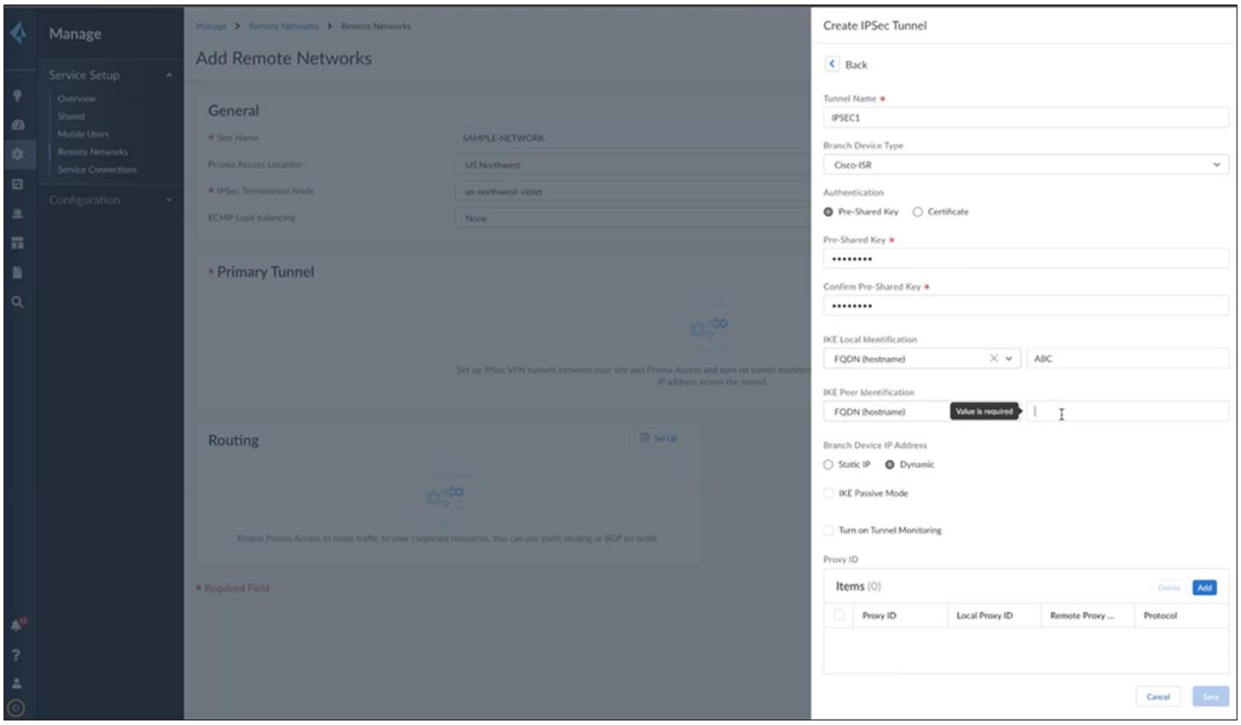
Add the name of the tunnel, select the data center endpoint, and enable/disable load balancing as shown below. If load balancing is not enabled, you can create primary/backup tunnels.

If load balancing is enabled, you will be allowed to create four tunnels, and adding BGP routes becomes mandatory (which is not supported with SIG-template).

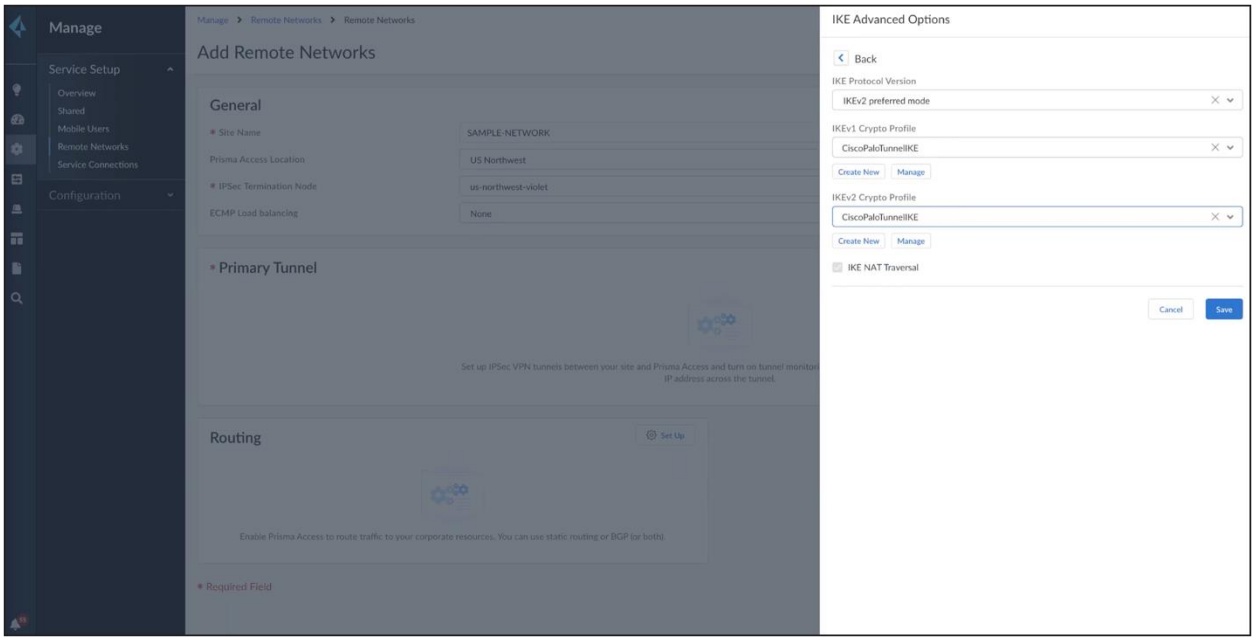
For the above example configuration, do not configure load balancing and leave it as “None.”

Enter the IPSec tunnel as shown in the screenshot.

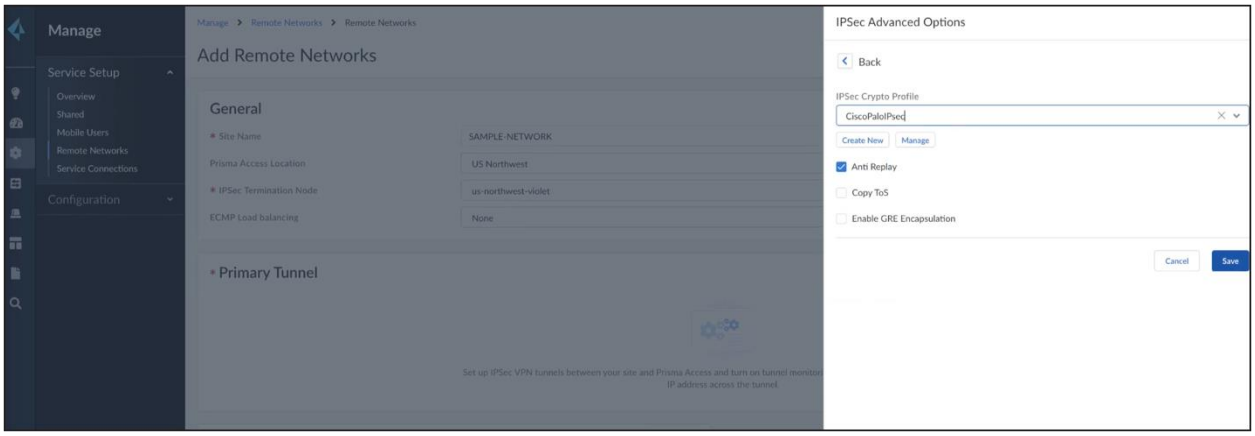




You can choose Cisco ISR as an option, but do not use the preloaded options for IKE and IPSec. Instead, create new options as shown below. Under the IKE advanced options, use IKEv2 as the preferred mode.

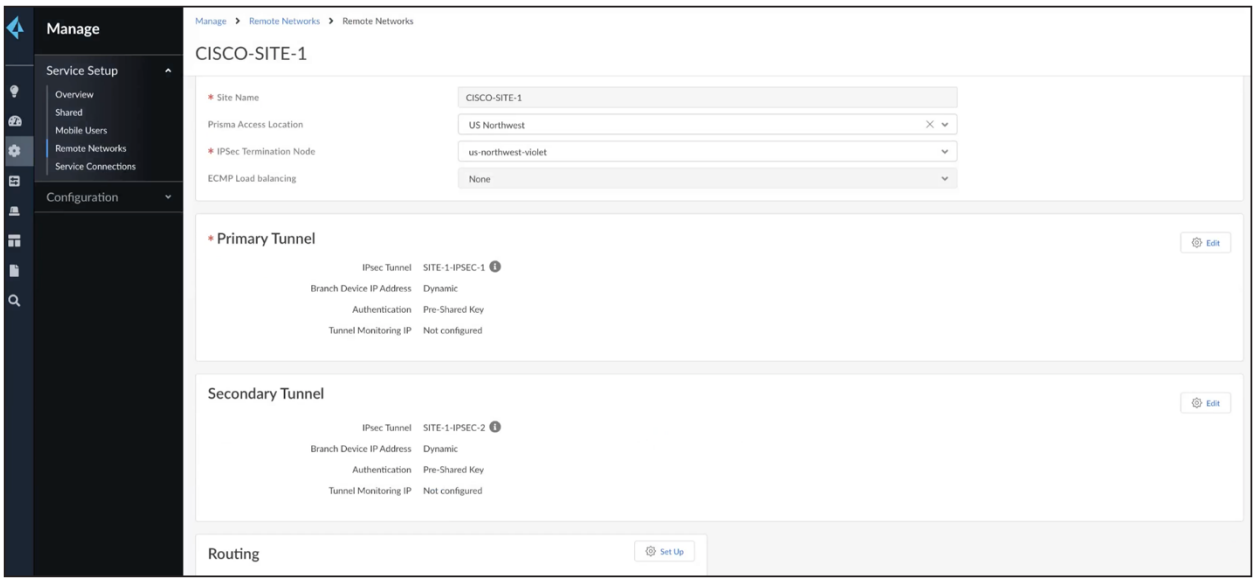


Similarly, create new for IPSec as shown below.

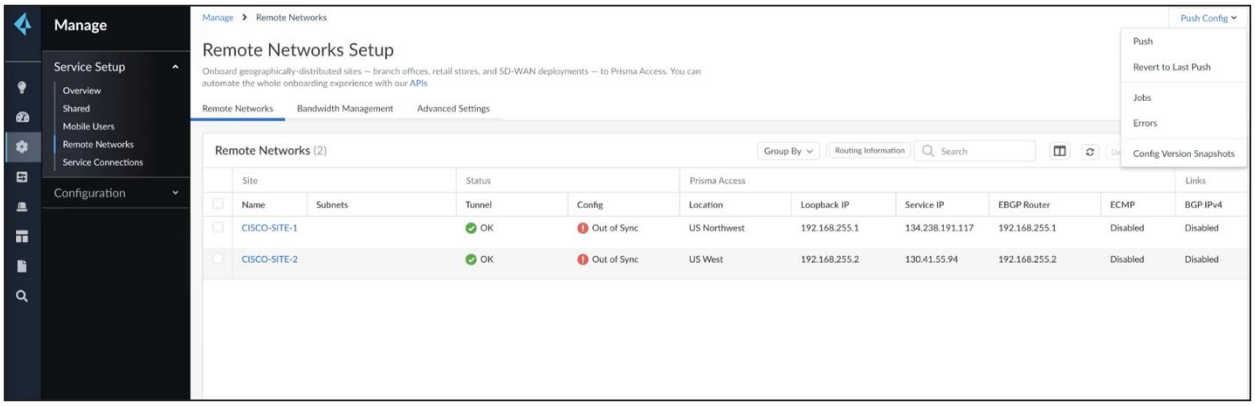


Save the above configuration to create the active tunnel. Similarly, create a secondary tunnel.

Both tunnel configurations are shown below.



After the tunnels are created, push the configuration. Collect the service IP (as shown below) for the remote site's tunnel destination configuration.

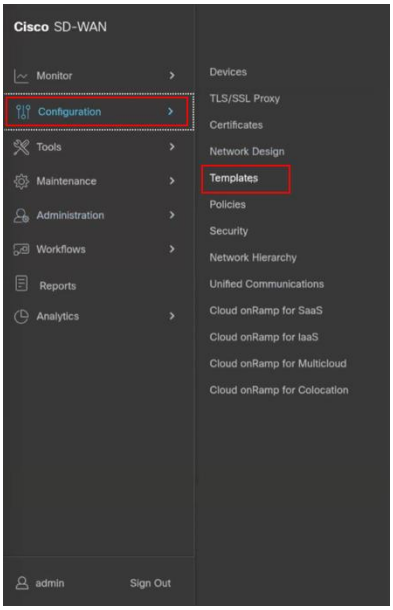


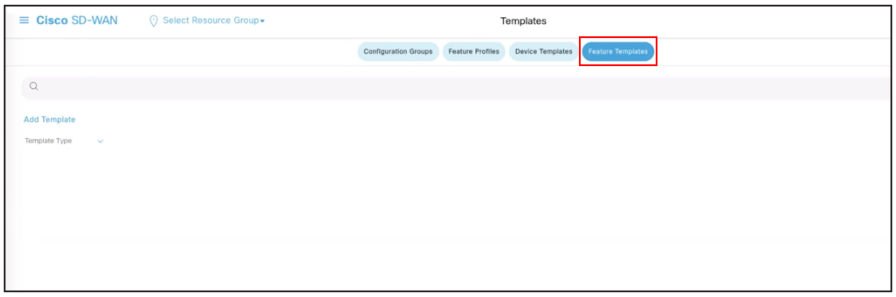
Note: To create additional tunnels, you can create another HA pair. The Cisco router supports up to four active and four backup tunnels. From the Palo Alto Prisma side, each HA pair will appear as part of a different network, but they will all be part of the same Cisco router.

We are using HA pairs because the other option, with ECMP enabled, would require BGP routes which are not supported.

Step 2. Cisco Catalyst SD-WAN Manager setup. As mentioned earlier, set up IPsec tunnels only.

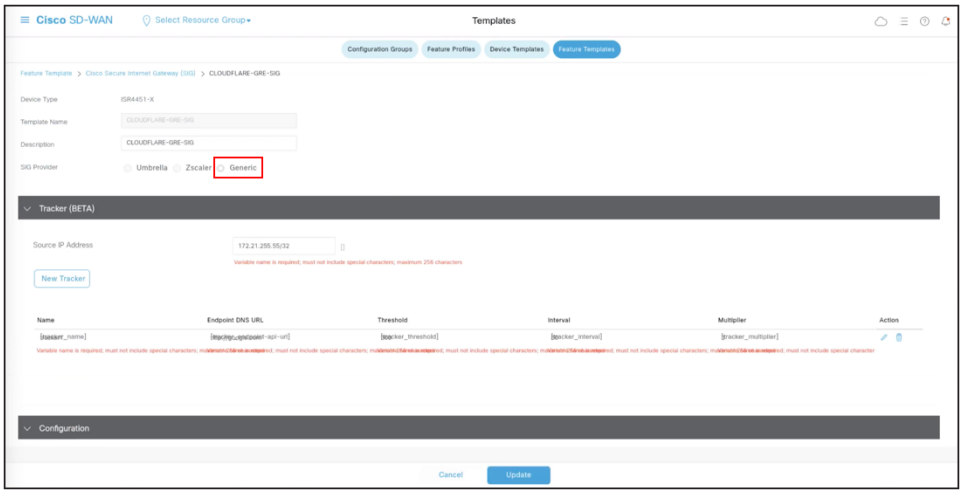
To set up tunnels using SIG templates, navigate to the Cisco Catalyst SD-WAN Manager dashboard, select Configuration -> Templates -> Feature Template, and create a SIG template.





In the SIG Template, select the **Generic Tunnel option**.

Create a Tracker to ensure the health of the tunnel. In this example, we have used “google.com” as the endpoint address, but you can use any internet HTTP destination. Please note that HTTPS destinations are not supported. RFC 1918 IP is supported as tracker source.

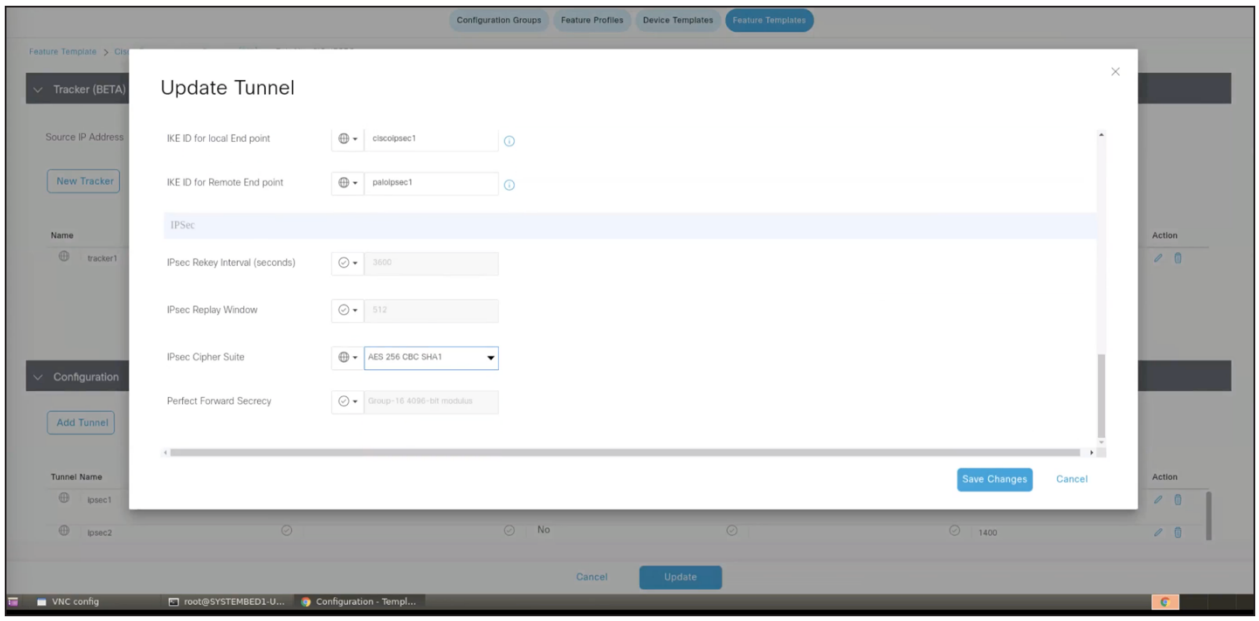


During the tunnel creation, select the tracker you created in the previous step from the drop-down menu.

Enter the IP of the Palo Alto Prisma POP endpoint as the tunnel destination IP.

Note: In the advanced options for tunnel creation, the default is NULL SHA1. Change it to AES 256, as that is the configuration on the Palo Alto Prisma side as well. Please refer to the screenshot shown below.

Ensure that the IKE and IPSec cipher suites match on both ends.

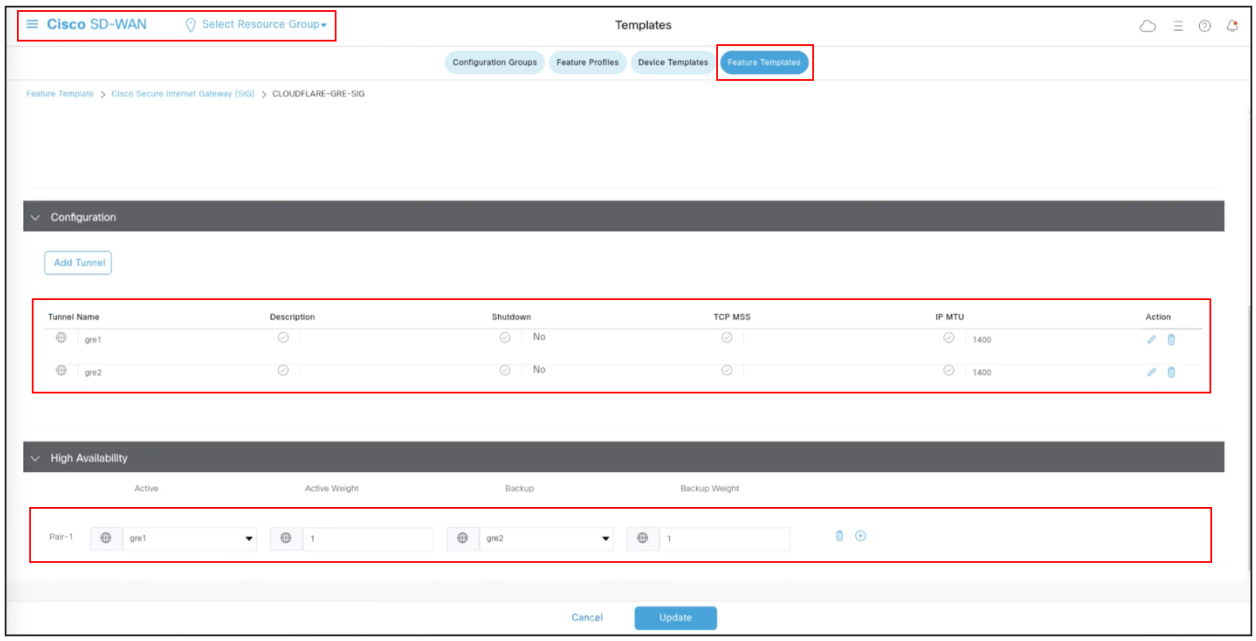


Standby Tunnel:

Similar to the above steps, create the standby tunnel and use the other Palo Alto Prisma POP IP.

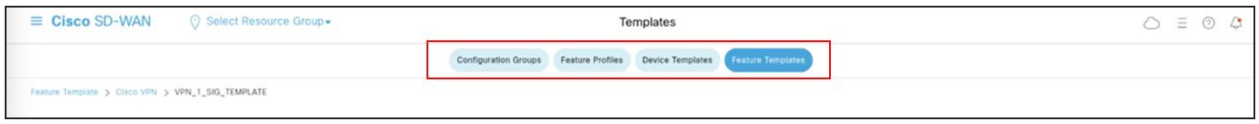
HA Configuration:

Once the two tunnels are created as shown below, add an HA configuration using these two tunnels. This ensures that traffic fails over to the secondary tunnel in case the primary tunnel goes down.



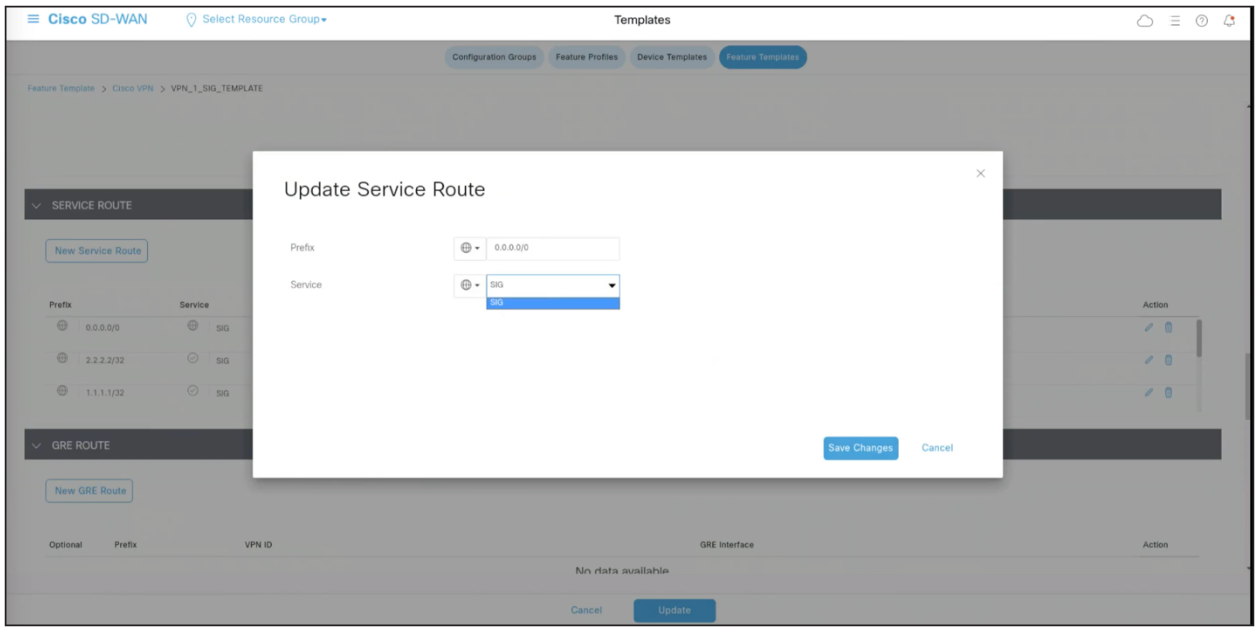
Step 3. Set up route-based service route

To set up a route-based service route, you can direct traffic through the tunnels for inspection in Palo Alto Prisma before it reaches the destination.



To configure a service route, select the SIG option from the dropdown menu. The tunnels will be automatically assigned. Then, add the subnets of the specific traffic that needs to be inspected at Palo Alto Prisma.

Note: Central Traffic data policy can also be used to re-direct traffic to tunnels based on specific match criteria and setting next-hop to service the SIG.



In conclusion, the integration of Cisco Catalyst SD-WAN with Palo Alto Prisma SSE cloud offers an efficient and secure solution for branch internet traffic. The seamless redirection and comprehensive features enhance network performance while ensuring robust cybersecurity measures. This validated guide serves as a valuable reference for customer simplementing the Palo Alto Prisma Cloud-based Secure Service Edge solution along side Cisco Catalyst SD-WAN, providing flexibility and reliable performance.

For more information

Learn more about [Cisco Catalyst SD-WAN Security].

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-3773673-00 11/23