Guide Cisco public IIIIII CISCO The bridge to possible

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.

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 <u>guide</u>.

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.

4	Manage	Manag	e > Remote Ne	itworks											Push Config ~
? গ্র	Service Setup ^ Overview Shared Mobile Users	Conboa automa Remote	note Net rd geographically- ate the whole onb e Networks	WORKS SETUP distributed sites – branch of oarding experience with our Bandwidth Management	ffices, retail stores, and SD-WAN APIs Advanced Settings	l deployments — to Prisma Acc	ess. You can								
*	Remote Networks Service Connections	Re	mote Networ	ks (2)				Group By 🗸	Routing Information	Q, Search			0	Delete Add	Remote Networks
	Configuration +	0	Site	Subnets	Status	Config	Prisma Access	Loopt	ack IP	Service IP	EBGP Rou	iter	1	ECMP	BGP IPv4
		D	CISCO-SITE-1		0 ок	In sync	US Northwest	192.1	68.255.1	134.238.191.117	192.168.2	55.1	r	Disabled	Disabled
B		0	CISCO-SITE-2		Ок	In sync	US West	192.1	68.255.2	130.41.55.94	192.168.2	55.2	C	Disabled	Disabled
٩															

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.

4	Manage	Manage > Remote Networks > Remote Networks		
		Add Remote Networks		
୧ ଶ୍ର 🍄 🗄 🖷 📰 ସ	Service Setup ^ Overview Shared Mobile Users Remote Networks Service Cennections Configuration ~	General * Site Name Prisma Access Location * IPSec Termination Node ECMP Load balancing * Primary Tunnel	SAMPLE-NETWORK US Northwest X * us-northwest-violet * disabled * None * Enabled * Set up IPSec VPN humels between your site and Prisma Access and turn on tunnel monitoring to check connectivity to a destinution of the set of the	@ SetUp
48		Routing Enable Prisma Access to route traffic to your corporate	Ser Up	Caref Son

4	Manage	Manage 🗲 Remote Networks 🗲 Remote Networks		Create IPSec Tunnel			
		Add Remote Networks		< Back			
• 6 0 0 0 0 0 0 0 0 0 0		General * Site Name Priona Access Location * If Sic: Termination Node CCMP Load balancing * Primary Tunnel	SAMPLE NETWORK US Northwest is mothwest-skilet Nore	Tunnel Name # IPSEC1 Branch Device Type Cisco-ISR Authentication Pre-Shared Key © Certif Pre-Shared Key # Confirm Pre-Shared Key # RCE Local Identification FQCN (hostname)	fcate X v]	NGC 1	*
			IP address across the turnel.	IKE Peer Identification FQDN (hostname)	Value is required	I	
		Routing	C Set Up	Branch Device IP Address Static IP Ø Dynamic		î	
			0	IKE Passive Mode			
			resources. Nois can use studic moting or INGP (or both).	Turn on Tunnel Monitoring Proxy ID			
		* Required Field		Items (0)			Delete Add
4.				Proxy ID	Local Proxy ID	Remote Praxy	Y X Remote ProxyProtocol Cancel Ser
?							
0							Cancel Sove

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.

4	Manage	Manage > Remote Networks > Remote Networks	IKE Advanced Options
		Add Remote Networks	C Back
• G & E a II		General # Stire Name SAMPLE NETWORK Prisma Access Location US Northwest # IPSec Terminution Node us northwest-violet ECMP Lead bulancing None	IKE Protocol Version IKEV2 cryste Perfile CiscoPatoFunctiKE × CiscoPatoFunctKE × CiscoPatoFunctKE × CiscoPatoFunctKE × CiscoPatoFun
a d		* Primary Tunnel	IKE NAT Travenal Cancel Save
		Routing Set Up Enable Priama Access to multi-traffic to your corporate resources. You can use static multing or BGP for boths * Required Field	
A			

Similarly, create new for IPSec as shown below.

4	Manage > Remote Networks > Remote Networks		IPSec Advanced Options
	Add Remote Networks		< Back
9	General		IPSec Crypto Profile CiscoPaloIPsed × v
62.6	* Site Name	SAMPLE NETWORK	Create New Manage
-	Prisma Access Location	US Northwest	Anti Replay
	* IPSec Termination Node	us-northwest-violet	Copy ToS
	ECMP Load balancing	None	Enable GRE Encapsulation
18	* Primary Tunnel		Cancel Save
Q			
		0.00	
		Set up (PSec VPN tunnels between your size and Prisma Arcess and turn on tunnel monitor	
		IP address across the tunnel	

Save the above configuration to create the active tunnel. Similarly, create a secondary tunnel. Both tunnel configurations are shown below.

4	Manage	Manage > Remote Networks > Remote Networks			
€ 62a 42 10 10 10 10 10 10 10 10 10 10 10 10 10	Overview Shared Mobile Users Remote Networks Service Connections Configuration	Amage * Render Networks * Render Networks CSCO-SITE-1 ************************************	X ¥ ¥		
∎ ∎ α		* Primary Tunnel IPsec Tunnel S Branch Device IP Address Authentication P Tunnel Monitoring IP N	E-14PSEC-1		© tet
		Secondary Tunnel IPsec Tannel S Branch Device IP Address D Authensistation P Tunnel Monitoring IP N	E-14PSEC-2 ananic -Shared Key t configured		🛞 sat
		Routing	0	i Set Up	

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

4	Manage	Manag	e 🕨 Remote Ne	etworks										Push Config 🛩
	ÿ	Ren	note Net	works Setup									Push	
	Service Setup	Onboa	rd geographically-	distributed sites - branch of	fices, retail stores, and SD-WAN	I deployments — to Prisma Acces	s. You can						Revert to	Last Push
	Overview	automa	ite the whole onb	oarding experience with our	APIs								lobs	
Ð	Shared	Remote	P Networks	Bandwidth Management	Advanced Settings								2005	
	Mobile Users	-											Errors	
•	Remote Networks	Rei	mote Networ	ks (2)				Group By ~ Routing Informat	ion Q Search			0	Config V	ersion Snapshots
8	Service Connections		Site		Status		Prisma Access							Links
	Configuration 👻	0	Name	Suboate	Tunnel	Config	Location	Loopback ID	Sendre ID	EBCD Par	tar	5/	MD	PCD ID-4
-				Jubilets	Totales	Conng	Location	LOOPDACK IF	361VICE IP	EDGP ROO	iter			BGF IF V4
		- L.J.	CISCO-SHE-1		OK	U Out of Sync	US Northwest	192.168.255.1	134.238.191.117	192.168.2	55.1	De	labled	Disabled
			CISCO-SITE-2		📀 ок	Out of Sync	US West	192.168.255.2	130.41.55.94	192.168.2	155.2	Di	sabled	Disabled
۹														

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.



≡ Cisco SD-WAN	Select Resource Group+	Templates	
		Configuration Groups Feature Profiles Device Templates Feature Templates	
Q			
Add Template			
Template Type 🗸 🗸			

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.

Cisco SD-WAN	⊘ Select Resource Group +	Tem	blates		\bigcirc =
		Configuration Groups Feature Profiles	evice Templates Feature Templates		
ture Templete > Cisco Secure In	sternet Gateway (SIG) > CLOUDFLARE-GRE-SIG				
ce Type ISR	4451-X				
olate Name C					
ription	LOUDFLARE-GRE-SIG				
Provider	Umbrella 💮 Zscaler 🚫 Generic				
Tracker (BETA)					
Source IP Address	172.21.255.55/32				
	Variable name is required; must not in	clude special characters; maximum 256 characters			
New Tracker					
Name	Endpoint DNS URL	Threshold	interval	Multiplier	Action
[tassiser_name]	[track/gscgnd.point - nci - urt]	[gggcker_threshold]	[gacker_interval]	[tracker_multiplier]	/ 0
Variable name is required; must not i	nclude special characters; multimist/d/bline.audquirvd; must not include spec	al characters; maldmidth@56noiaiaadeeinod; must not include i	pecial characters; ma klariabi/256rob.isaekeeir ed; must not include i	pecial characters; maklarisbl@56reb.aowtesired; must not include	ipecial character
Configuration					
Configuration					

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.

		Configu	ration Groups Feature Profiles	Device Templates Feature Templates		
Feature Template > Cisr	Update Tunnel					×
Source IP Address	IKE ID for local End point	⊕ ▼ ciscolpsec 1				
New Tracker	IKE ID for Remote End point	patolpsec1				
Name	IPSec					Action
tracker1	IPsec Rekey Interval (seconds)	⊘ ▼ 3600				/ 0
	IPsec Replay Window	⊘ ▼ 512				
Configuration	IPsec Cipher Suite	⊕ - AES 256 CBC SHA1	•			
Add Tunnel	Perfect Forward Secrecy	⊘ ▼ Group-16 4096-bit modulus				
Tunnel Name	.4				Save Changes Cancel	Action
e lpsec2			⊘ No		0 1400	10
			Cancel	Update		
VNC config	root@SYSTEMBED1-U	Configuration - Templ				0

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.

≡ Cisco SD-WAN	⊘ Select Resource Group+	т	emplates		
		Configuration Groups Feature Profiles	Device Templates Feature Templates		
Feature Template > Cisco Secure	Internet Gateway (SIG) > CLOUDFLARE-GRE-SIG				
✓ Configuration					
Add Turned					
Add Tunnel					
Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
Gre 1		⊘ No		I400	/ 0
⊕ gre2		⊘ No		I400	/ 0
	_	_	_	_	
Active	Active Weight	Backup	Backup Weight		
Pair-1		🕀 gre2 👻	1) 🕀	
		Cancel	Update		

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.

≡ Cisco SD-WAN	Templates	
	Configuration Groups Feature Profiles Device Templates Feature Templates	
Feature Template > Cisco VPN > VPN_1_SIG_TEMPLATE	20	

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.

≡ Cisco SD-WAN	♦ Select Resource Group •	Templates	
		Configuration Groups Feature Profiles Device Templates Feature Templates	
Feature Template > Cisco VPN >	VPN_1_SIG_TEMPLATE		
✓ SERVICE ROUTE	Update	e Service Route	_
New Service Route	Prefix	⊕ • 0.0.0.0j0	
Brothy	Service	⊕ • 533 •	Antine
· 0.0.0.0/0	I SIG		/ 0
· 2.2.2.2/32	SIG		10
① 1.1.1.1/32	o sia		/ 0
✓ GRE ROUTE	_	Save Changes Cancel	
New GRE Route			
Optional Prefix	VPN ID	GRE Interface Nrs rista sualilable	Action
		Cancel Update	

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA