Deployment guide Cisco public IIIIII CISCO The bridge to possible

Cisco Catalyst SD-WAN and Skyhigh Security Service Edge Integration User Guide

April 2024

Contents

Overview	3
Cisco Catalyst SD-WAN SSE Integration with Skyhigh for Secure Internet Access	4
Sample topology diagram with SD-WAN and Skyhigh network	4
Overview of Configuration Steps	5
Deployment models	19
Skyhigh Web Gateway Configuration Modification Procedure	22
Cisco Catalyst SD-WAN Manager Configuration Modification Procedure	23
For more information	26

Overview

The integration of Cisco Catalyst[™] SD-WAN with Skyhigh Security Service Edge (SSE) cloud empowers customers to bolster the security of their branch internet traffic through seamless redirection. By harnessing Cisco[®] Catalyst SD-WAN Secure Internet Gateway (SIG) templates, the implementation process becomes efficient and straightforward. These templates offer an intuitive workflow for comprehensive end-to-end configuration, encompassing critical features such as Point of Presence (POP) availability, application health checks, weighted load balancing, and data policy enforcement. With this integration, users can effortlessly specify the desired redirection of branch traffic to the Skyhigh SSE. It's worth noting that the integration has undergone rigorous testing and validation within Cisco, ensuring seamless compatibility and reliable performance.

This document serves as a technical and configuration guide for successfully integrating Skyhigh SSE and Cisco Catalyst SD-WAN, utilizing the capabilities provided by Cisco Catalyst SD-WAN Manager Release 20.9 and Cisco IOS® XE SD-WAN WAN Edge Release 17.9. It includes practical examples demonstrating how to provision a new service to integrate Skyhigh SSE and Cisco Catalyst SD-WAN IPsec tunnel using the SIG feature template implementation. IPsec primary and secondary tunnels are established to Skyhigh SSE for Direct Internet Traffic (DIA).

The following Cisco Catalyst SD-WAN and Skyhigh SSE use cases are covered within this document:

- Dual WAN Edge design with one active tunnel per WAN Edge
- Dual WAN Edge design with one active/standby tunnel per WAN Edge
- Dual WAN Edge design with two active/active Equal-Cost Multi-Path Routing (ECMP) tunnel deployment per WAN Edge
- Utilization of centralized data policy for traffic redirection



Figure 1.

Cisco Catalyst SD-WAN - Skyhigh network topology with active backup tunnels to Skyhigh POPs

Cisco Catalyst SD-WAN SSE Integration with Skyhigh for Secure Internet Access

Use case

This integration guide serves as a reference for customers who run the Skyhigh SSE solution alongside the Cisco Catalyst SD-WAN solution. It is designed for scenarios where branch users require internet or SaaS application access that needs to be inspected and secured by the Skyhigh SSE solution.

Pre-requisites and Validated Environment

- Skyhigh Security Cloud Version 6.4.2
- Cisco Catalyst SD-WAN Manager Release 20.9, Cisco Catalyst SD-WAN Validator Release 20.9, Cisco Catalyst SD-WAN Controller Release 20.9, Cisco Catalyst SD-WAN C8kv Edge Release 17.9
- Knowledge of Cisco Catalyst SD-WAN configuration and features

Supported Hardware

- ISR 4461, 4451, 4431, 4351, 4331, 4321, 4221X, 4221, CSR, ISRv, and ISR 1K
- Catalyst® 8500L, 8300, 8200, and 8000V

Sample topology diagram with SD-WAN and Skyhigh network

The following tests have been conducted with an emphasis on ensuring redundancy.



Figure 2.

SD-WAN - Skyhigh network topology with active backup tunnels to Skyhigh POPs

In the above topology, two branch routers, SD-WAN-1 and SD-WAN-2, are connected to Skyhigh SSE Datacenter locations (Los Angeles and Singapore) using redundant ISPs (Biz-internet and public-internet colors). The Transport Locator (TLOC) extension feature has been used to provide cross-ISP connectivity from both routers. The Service VPN can be redundantly configured using Layer 2 protocols including Virtual Router Redundancy Protocol (VRRP) or Layer 3 routing protocols such as Border Gateway Protocol (BGP) or any other supported protocols. The architecture provides redundancy at the tunnel, data center, ISP, and router levels.

Redundancy Connectivity Matrix

In the above diagram, ISP1 is tied with the LA location, and ISP2 is tied with the Singapore location.

Router	ISP-Color	Skyhigh SSE POP
SD-WAN-1	Biz-internet (Gig1)	LA (Active Tunnel)
SD-WAN-1	Public-internet (Gig2) using TLOC extension from SDWAN2	LA (Backup Tunnel)
SD-WAN-2	Pub-internet (Gig1)	Singapore (Backup Tunnel)
SD-WAN-2	Biz-internet (Gig2) using TLOC extension from SD-WAN1	Singapore (Active Tunnel)

Note: The TLOC extension feature enables a WAN Edge router to communicate over the WAN transport connected to the adjacent WAN Edge router through a TLOC extension interface, allowing for redundancy on the transport side.

Overview of Configuration Steps

Step 1: Set up locations on the Skyhigh SSE cloud platform under web-gateway

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

Step 3: On SD-WAN Manager, set up policy to route traffic to Skyhigh SSE

Step 4: Verify tunnel operation on Cisco Catalyst SD-WAN Manager and CLI

Step 5: Verify web traffic on the Skyhigh SSE cloud platform

Configuration Process in Detail

Step 1: Skyhigh location setup

Navigate to Setup > Infrastructure > Web Gateway setup.

Skyhigh Security	Dashboards Governance Analyt	ics Incidents Policy	Reports		•	• • • ± =
My Dashboard						Service Management PoP Management < User Management
Top AI Services by Users Number of users by Service Name and Risk type for 0 Services - Month	Last Top AI Services by Dat Total data volume by Service Month OB	a Volume • Name and Risk type for 0 Serv	vices - Last	Data Volu ^{Total data ve}	Tokenization Data Feed Info Proxy Management Client Proxy Management	 Infrastructure Integrations Global Notification Settings Audit Log
No Article During the Topo During	No Activity	During this Time Pariod			Cloud Connector Web Gateway Setup Private Access Configuration	
to Activity bulling this interreliou					NO ACTIVITY DUTING THIS TIME F	

Figure 3. Skyhigh Dashboard

IPsec Tunnel Setup:

Under Secure Web Gateway Setup, go to Configure Locations > New Location.

🚺 si	kyhigh Security	Dashboards	Governance	Analytics	Incidents	Policy	Reports		¢ 0	1:
Seci	ure Web Gateway Setup									
	Configure SCP 1 of 4 steps completed. Skyhigh Client Proxy (SCP) is client softwa the gateways defined in its policy settings. SCP also authenticates forwarded traffic.	re that is installed o users and endpoint	on your endpoints ts when it forward	using standar Is traffic. Skyhij	d software dep gh Security's ga	oyment too eways can	Js. SCP forwards internet traffic from the endpoints to use this information when applying the policy to the		Get Starter Get SCP	I
	Skyhigh Mobile Cloud Security Skyhigh Mobile Cloud Security (MCS) extends protection to mobile information, test device certificates, and use the specified steps to	endpoints by redir configure MDM so	recting cloud traffi lutions to enable	c through Skyh traffic redirecti	nigh Secure We ion to Skyhigh S	o Gateway f ecure Web	or Cloud for policy enforcement. Update root CA Gateway for Cloud.		Configure	
\oslash	Managing Certificate Authorities for HTTPS Scanning Skyhigh provides a default certificate authority for SAML authenti endpoints. We also recommend that you replace the custom CA w	ation and a custom ith a CA of your ow	n certificate autho m. You can manag	rity for HTTPS : ge the custom (scanning. We re	commend 5 Scanning	that you download the default CA here and deploy it on your leature configuration page.			
	Setup SAML Configure SAML authentication to use your own Identity Provider	(IdP) service to auth	nenticate users.						New SAMI	
	Enable Active Directory User Group Lookup Enable a lookup of your user group or groups in an Active Directo appropriate web policy when you are logging on to Secure Web G	ኅ (AD) when this in ateway (SWG).	formation cannot	be provided b	y Secure Client	Proxy (SCP)	. User group information is required to select the		Configure	
\oslash	Configure Locations Configure locations to use a different authentication method for e tme-cisco-br tme-cisco-b	ach region.						1	Vew Locatio	'n

Figure 4. Skyhigh Web Gateway Setup

Configure Location attributes:

Configure Location Name me-disco-branch1-1 Settings To configure advanced SAML settings, such as adding exceptions, use the configuration in Web Policy. Learn more Select SAML Configuration None Log Data Residency Define at least one location mapping. Provide your identity settings Client ID time@cisco.com Client ID time@cisco.com Client ID time@cisco.com Client Address 20.157.25.81 Pre-Shared Key C1 10						
Name tme-disco-branch1-1 Settings To configure advanced SAML settings, such as adding exceptions, use the configuration in Web Policy. Learn more Select SAML Configuration None Log Data Residency Default Default Define at least one location mapping. Provide your identity settings Client 10 Type Use a User FQDN Client Address 20.157.25.81 Pre-Shared Key C1 10 Define subnets to protett O Define subnets to protett	Configure Location					
Impercises Settings To configure advanced SAML settings, such as adding exceptions, use the configuration in Web Policy, Learn more Select SAML Configuration None Log Data Residency Define at least one location mapping. Provide your identity settings Glient ID Type Use a User FQDN Client ID Type Use a User FQDN Client Address 20.157.25.81 Pre-Shared Key Client Address Provide yours I Optime subnets to protet	Name					
Settings To configure advanced SAML settings, such as adding exceptions, use the configuration in Web Policy. Learn more Select SAML Configuration None Log Data Residency Define at least one location mapping. PSec Mapping PSec Mapping Client at least one location Client ID Time@cisco.com Client Address 20.157.25.81 Pre-Shared Key Cl 10	tme-cisco-branch	11-1				
Settings To configure advanced SAML settings, such as adding exceptions, use the configuration in Web Policy. Learn more Select SAML Configuration None Log Data Residency Default Define at least one location mapping. IP Range Mapping IPSec Mapping GRE Tunnel Mapping Provide your identity settings Client ID Type Use a User FQDN Client Address 20.157.25.81 Pre-Shared Key C1 10						
To configure advanced SAML settings, such as adding exceptions, use the configuration in Web Policy. Learn more Select SAML Configuration None Log Data Residency Default Define at least one location mapping. IP Range Mapping IPSec Mapping Glient ID Type Use a User FQDN Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C1 10	Settings					
Select SAML Configuration Log Data Residency Define at least one location mapping. IP Range Mapping IPSec Mapping GRE Tunnel Mapping Client ID Type Use a User FQDN Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C1 10	To configure adva	nced SAML setti	ngs, such as adding excep	ptions, use the configuration in Web Policy. Learn more		
Log Data Residency Default Define at least one location mapping. IP Range Mapping IPSec Mapping Glient ID Type User FQDN Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C1 10	Select SAML C	onfiguration	None	~		
Define at least one location mapping. IP Range Mapping IPSec Mapping Great Variable GRE Tunnel Mapping Client ID Type Use a User FQDN Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C1 10 Ø Define subnets to protett Image Angelen	Log Da	ta Residency	Default	\checkmark		
Define at least one location mapping. IP Range Mapping IPSec Mapping GRE Tunnel Mapping Grient ID Type Use a User FQDN Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C110						
IP Range Mapping IPSec Mapping GRE Tunnel Mapping Provide your identity settings Client ID Type Use a User FQDN Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C110 O Define subnets to protect Image: Any subnet	Define at least on	e location ma	oping.			
Provide your identity settings Client ID Type Use a User FQDN Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C110 Define subnets to protect Q Ary subnet	IP Range Mapping	IPSec Map	ping GRE Tunnel N	Mapping		
Client ID Type Use a User FQDN Client ID tme@clisco.com Client Address 20.157.25.81 Pre-Shared Key C110 Ø Define subnets to protect O Define subnets to protect O Any subnet	Provide vour iden	tity settings				
Client ID Use a User FQDN Client ID tme@clsco.com Client Address 20.157.25.81 Pre-Shared Key C110	r toviac your lacit	any seconds				
Client ID tme@cisco.com Client Address 20.157.25.81 Pre-Shared Key C10 Ø Any subnet	Client ID Type	Use a User F	QDN	~		
Client Address 20.157.25.81 Pre-Shared Key C110 Ø Define subnets to protect	Client ID	tme@cisco.co	om			
Pre-Shared Key C110 O Define subnets to protect Image: Any subnet	Client Address	20.157.25.81				
Define subnets to protect O Any subnet	Pre-Shared Key C110					
O Define subnets to protect O Any subnet						
O Define subnets to protect O Any subnet						
Define subnets to protect O Any subnet						
Cancel Save	Cancel	Save				

Figure 5.

Skyhigh location configuration

Location Mapping: IPsec Mapping (in this phase, only IPsec is validated)

Note: Skyhigh supports both IPsec and Generic Routing Encapsulation (GRE).

Client ID Type: Can be based on IPs, Fully Qualified Domain Names (FQDNs) or emails and can be behind Network Address Translation (NAT)

The Client ID should be provided with the corresponding Client ID type. Follow the article for reference.

Client ID = email (in this case)

Client address = ISP outgoing IP used to build tunnels

Note: Each Skyhigh location requires a unique client address to create location, meaning each location is tied to the ISP's outgoing IP.

Pre-shared key= Use any secure key

Choose Any subnet or Define protected subnets that need to be secured on the branch side.

Define subnets to protect O Any subnet	
Subnet	Comment
192.168.100.1/32	Tracker
172.16.0.0/16	LAN

Using a similar process, add the Second Skyhigh location:

Configure I	Location			
Name				
tme-cisco-branc	h1-2			
Settings				
To configure adv	anced SAML setti	ngs, such as adding exceptions, use	the configuration in Web Policy. Learn more	
Select SAML (Configuration	None 🗸		
Log Da	ata Residency	Default 🗸		
Provide your ider Client ID Type	ntity settings Use a User F	QDN ~		
Client Address	20.47.120.69			
Pre-Shared Key	C:	0		
Define subne	ets to protect	Any subnet		
Cancel	Save			

Figure 6. Skyhigh location configuration

Configure the rules on Skyhigh as required for Web policy:

Refer to the Skyhigh web policy page for further details.

Skyhigh Security Dashboar	ds Governance Analytics Incidents	Policy Reports	●☆@⊥።
1y Dashboard	I	Web Policy > Malware Policies >	Policy Actions ~
Top AI Services by Users Number of users by Service Name and Risk type for 0 Services - Last Month	Top AI Services by Data Volume Total data volume by Service Name and Risk type f Month OB	Access Control > Configuration Audit Vulnerabilities Application Control Workload Hardening	Feature Configuration End User Notification Pages vices - Last Month
No Activity During this Time Period	No Activity During this Time Peric	Connected Apps Policies Encryption Policy On-Demand Scan Policy Templates User Lists	No Activity During this Time Period
New Services Number of services by Service Category for 21 Services - Last 7 Days	Unassigned Services Number of services by Service Category for 25 Serv	Policy Settings) Risk Services ad data volume by Service Name for 0 Services - Last 7 Days

Figure 7.

Skyhigh Web Policy setup

Step 2: Catalyst SD-WAN Manager IPsec tunnel setup

SIG Templates are used for connectivity, providing multiplexing capability to carry multiple Service VPN (VRF) traffic within the same set of tunnels. They are recommended by Cisco for any SIG connectivity.

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



Figure 8. Cisco SD-WAN Manager Dashboard



Figure 9.

Cisco SD-WAN SIG Feature Template configuration

SIG Provider:

In the SIG Template, select the Generic Tunnel option.

(Only template-based tunnel is supported at this point)

Configuring Layer 7 Health Checks to Monitor Tunnels:

Create a tracker to ensure the health of the tunnel. In this example, "cisco.com" is used as the endpoint address, but any internet HTTP destination can be used. Please note that HTTPS destinations are not supported. RFC 1918 IP is supported as a tracker source.

Note: Layer 7 Health Checks are used to monitor the health of tunnels toward the SIG using trackers attached to the tunnels. These trackers facilitate automatic failover to back up tunnels based on tunnel health. Failover occurs when SLA parameters are not met or when the SIG tunnel is down.

≡ Cisco SD-WAN	♦ Select Resource Group •	Configuration	Templates		
		Configuration Groups Feature Profiles	evice Templates Feature Templates		
Feature Template > Cisco Sec	ure Internet Gateway (SIG) > skyhigh-sig-templat	3			
Device Type	C8000v				
Template Name	skyhigh-sig-template				
Description	skyhigh-sig-template				
SIG Provider	🔵 Umbrella 🔵 Zscaler 🗿 Generic				
Y Tracker (BETA)					
Source IP Address	⊕ ▼ 172	16.2.1/32			
New Tracker					
Name	Endpoint DNS URL	Threshold	Interval	Multiplier	Action
Cisco-tracker	http://www.cisco.com	⊕ 300	۵۵	3	/

Figure 10.

Cisco SD-WAN tracker configuration in SIG template

Add IPsec Tunnel:

During the tunnel creation, select tunnel type IPsec. Then from the dropdown menu, select the tracker created in the previous step from the dropdown menu.

Select IPsec source interface.

Tunnel destinations can be found using nslookup. Refer to this article by Skyhigh.

≡ Cisco SD-W	AN 💮 Select Resource G	oup• Con	figuration · Templates		△ ≡ ⊘ ¢
		Configuration Groups Feature	Profiles Device Templates Feature Templates		
Feature Template >	Update Tunnel				×
✓ Configuratic	Basic Settings				
Add Tunnel	Tunnel Type	ipsec gre			
	Interface Name (1255)	ipsec101			
Tunnel Name	Description	Primary Tunnel			Action
ipsec1	Tracker	Cisco-tracker			
() ipsecz	Tunnel Source Interface	GigabitEthernet1			V (j
	Tunnel Destination IP Address/FQDN(Ipsec)		Skyhigh PoP		
✓ High Availat	Preshared Key	• •			
Pair-1				Save Changes Cancel	

Figure 11. Cisco SD-WAN IPsec tunnel configuration in SIG template

Advanced options:

In the IKE ID for the local end point, use the Client ID specified in step 1 during the Skyhigh location creation.

Ensure that the IKE and IPsec cipher suites are part of supported ciphers by Skyhigh.

Please refer to this Skyhigh article for Skyhigh IKE/IPsec settings.

Note: In the advanced options for tunnel creation, the default is NULL SHA1. Change it to AES 256.

≡ Cisco SD-W	AN 🗘 Select Resource G	oup • Configuration · Templates	\bigcirc) 🗘
		Configuration Groups Feature Profiles Device Templates Feature Templates			
Feature Template > Cisc	o Secure Internet Gateway (SIG) > skyhigi	-sig-template	-		
⊕ cisco-tr	Update Tunnel		×	0	
	IKE Cipher Suite	Ø• AES 256 CBC SHA1	- 1		
✓ Configuration	IKE Diffie-Hellman Group	T4 2049-bit modulus	- 1		
Add Tunnel	IKE ID for local End point	tme@cisca.com	- 1		
Tunnel Name	IKE ID for Remote End point	©• 0		Action	
⊕ ipsec10	IPSec			0	
ipsec20	IPsec Rekey Interval (seconds)	Ø • 3600		0	
	IPsec Replay Window	©• 512	- 4		
✓ High Availabi	IPsec Cipher Suite	⊕ ► AES 256 CBC SHA1 ▼	- 1		
Pair-1		Save Changes Cancel			

Figure 12.

Cisco SD-WAN IPsec tunnel advanced options configuration

Secondary Tunnel:

Following the same steps as above, create the secondary tunnel and utilize the IP address of the other Skyhigh POP.

≡ Cisco SD-W/	AN 💮 Select Resource Gro	vup Configuration · Templates	
		Configuration Groups Feature Profiles Device Templates Feature Templates	
Feature Template >	Update Tunnel		×
✓ Configuratic	Basic Settings		
Add Tunnel	Tunnel Type	◯ ipsec ◯ gre	
	Interface Name (1255)	e ipsec201	
Tunnel Name	Description	Secondary Tunnel	Action
Upsec 1	Tracker	G v cisco-tracker v	
U ipsecz	Tunnel Source Interface	GigabitEthernet2	<i>~</i> U
	Tunnel Destination IP Address/FQDN(Ipsec)	⊕ ▼ 161.69.122.2	
✓ High Availat	Preshared Key	⊕ ▼	
Pair-1		Save Changes Car	ncel

Figure 13. Cisco SD-WAN IPsec tunnel configuration for backup tunnel

HA Configuration:

Once the two tunnels are created as shown below, proceed to HA configuration using these two tunnels. This step ensures that traffic automatically fails over to the secondary tunnel if the primary tunnel goes down.

Cisco SD-WAN	Select Resource Group•	Configuration •	Templates		$\bigcirc \equiv \odot$ 4
		Configuration Groups Feature Profiles	Device Templates Feature Templates		
ture Template > Cisco Secur Name	e Internet Gateway (SIG) > skyhigh-sig-template Endpoint DNS URL	Threshold	Interval	Multiplier	Action
cisco-tracker	http://www.cisco.com	300	۵۵	۵	/ 1
Configuration					
Add Tunnel					
Add Tunnel	Description	Shutdown	TCP MSS	IP MTU	Action
Add Tunnel Tunnel Name tipsec101	Description	Shutdown	TCP MSS	IP MTU 🔿 1400	Action
Add Tunnel Tunnel Name tipsec101 tipsec201	Description Primary Tunnel Geodary Tunnel	Shutdown	TCP MSS	IP MTU O 1400 O 1400	Action
Add Tunnel Tunnel Name	Description Primary Tunnel Secondary Tunnel	Shutdown No No	CP MSS	IP MTU	Action 0 1 1 0
Add Tunnel Tunnel Name	Description Primary Tunnel Secondary Tunnel	Shutdown No No No	CP MSS	IP MTU 2 1400 2 1400	Action
Add Tunnel Tunnel Name	Description Primary Tunnel Secondary Tunnel	Shutdown No No	TCP MSS	IP MTU O 1400 O 1400	Action
Add Tunnel Tunnel Name Bipsec101 Bipsec201 High Availability Active	Description Primary Tunnel Secondary Tunnel Active Weight	Shutdown No No Backup	TCP MSS	IP MTU O 1400 O 1400	Action C I I I I I I I I I I I I I
Add Tunnel Tunnel Name	Description Primary Tunnel Secondary Tunnel Active Weight	Shutdown No Mo Backup	TCP MSS	IP MTU 2 1400 2 1400	Action
Add Tunnel Tunnel Name	Description Pérmary Tunnel	Shutdown No No Backup Backup	TCP MSS	IP MTU ○ 1400 ○ 1400	Action

Figure 14.

Cisco SD-WAN active/backup high-availability configuration

ECMP Tunnels:

To configure ECMP tunnels, choose "None" under the backup of Pair-1, and configure Pair-2 with secondary tunnel as the active tunnel, as shown in figure 14 below.

✓ High A	wailability				
	Active	Active Weight	Backup	Backup Weight	
Pair-1	ipsec101	• 1	None	▼ 1	(
Pair-2	ipsec201	▼ ⊕ 1	None	▼ ■ 1	† •

Figure 15.

Cisco SD-WAN IPsec ECMP configuration

Note: The Cisco solution offers a capability of four ECMP active and four backup tunnels, which can be configured using loopbacks with same outgoing ISP IP and location combination. However, to have multiple ECMP tunnels, multiple locations must be configured using unique public IP on the Skyhigh portal. So, four unique public IP addresses are required for configuring four ECMP active tunnels.

Add SIG Feature Template to the Device Template:

Navigate to the Catalyst SD-WAN Manager Dashboard, select Configuration > Templates > Device Templates, and edit the device template.

Add Cisco Secure Internet Gateway template from right end, as shown in figure 15.

≡ Cisco SD-WAN	⑦ Select Resource Group▼	Configuration · Templates	\bigcirc	=	0	4
		Configuration Groups Feature Profiles Device Templates Feature Templates				
Transport & Management V	/PN					
Cisco VPN 0 *	VPN_0_20-04-2023_02-18-53	Additional Cisco VPN 0 Templates				
Cisco Secure Internet Gateway	skyhigh-sig-template	③ Cisco BGP ④ Cisco OSPF				
Cisco VPN Interface Ethernet	interface_GigabitEthernet1_20-04-202	Cisco OSPFv3 Cisco Secure Internet Gateway				
Cisco VPN Interface Ethernet	interface_GigabitEthernet2_20-04-202	Cisco VPN Interface Ethernet Cisco VPN Interface GRE				
Cisco VPN Interface Ethernet	interface_GigabitEthernet3_20-04-202	Gisco VPN Interface IPsec VPN Interface Cellular VPN Interface Autibility Constraints				
Cisco VPN Interface Ethernet	Loopback-1	VPN Interface United PPPOE OPPN Interface DSL (PoE				
Cisco VPN Interface Ethernet	Loopback-2	VPN Interface DSL PPPoA VPN Interface DSL PPPoE VPN Interface DSL PPPoE				
Cisco VPN Interface Ethernet	Loopback-3	VPN Interface SVI VPN Interface TI-E1-Serial VPN Interface T1-E1-Serial				
Cisco VPN Interface Ethernet	Loopback-4	0				

Figure 16.

Cisco SD-WAN device template configuration

No variables need to be defined, so click Update>"Next" after this step, then proceed to "Configure Devices."

Catalyst SD-WAN Manager should return a success message once the configuration process is complete.

=	Cisco SD-WA	٨N	Select Resource Gr	roup∙						0 4
Push	Feature Template Co	onfiguratio	n 🥝 Validation Success					Initiated By:	srsaredd From: 73.3	231.130.88
Total	Task: 1 Success : 1									
Q	Search									∇
									Total Rows: 1	C 🕸
\sim	Status		Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP	
	Success		Template successfully attac	C8K-D976AF4A-D471-B13	C8000v	CSRSD-WAN-2	1.1.101.2	101	1.1.1.1	
	[25-Sep-2023 11:1] [25-Sep-2023 11:1] [25-Sep-2023 11:1] [25-Sep-2023 11:1] [25-Sep-2023 11:1]	7:10 PDT] 7:11 PDT] 7:16 PDT] 7:18 PDT] 7:21 PDT] 7:21 PDT]	Updating device configurat Sending configuration to o Successfully notified dev Device has pulled the con Device: Config applied su Template successfully atta	cion in vManage levice ice to pull configuration figuration cressfully iched to device					•	2

Figure 17. Cisco SD-WAN configuration status

Step 3: Setup policy-based traffic redirection

Traffic to SIG

The traffic from the service VPN can be redirected to SIG tunnels in two ways.

- Using a static default route to the service SIG
- Using centralized data policy to redirect to the 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 this guide.

Note: Skyhigh SSE (web gateway) can only process secure web (http(s)) traffic. Therefore, Internet Control Message Protocol (ICMP), and Domain Name System (DNS) traffic should not be sent through the tunnels toward Skyhigh SSE. In this case, data policy can be used to redirect web traffic to Skyhigh.

Navigate to the Catalyst SD-WAN Manager Dashboard, select Configuration > Policies > Centralized Policy.

Cisco SD-WAN			Configurat	ion · Policies		
🗠 Monitor ၂၂၀ Configuration		Devices TLS/SSL Proxy	Centralized Policy	Localized Policy		ମୁଙ୍ଗୁ Custom Options 🗸
💥 Tools		Network Design		•		∇
{ộ}} Maintenance		Templates				
administration		Policies Security				Total Rows: 1 🛛 🔗 🔅
🖓 Workflows		Network Hierarchy	Activated	Updated By	Policy Version	Last Updated
() Analytics	>	Network Riferatory Unified Communications Cloud onRamp for SaaS Cloud onRamp for laaS Cloud onRamp for Multicloud Cloud onRamp for Colocation	true	admin	07062023T133946732	06 Jul 2023 1:39:48 PM PDT •••

Figure 18.

Cisco SD-WAN policy configuration

Navigate to Centralized Policy and configure a traffic data policy to match on ports 80 and 443. Redirect all web to Skyhigh SSE using the tunnels configured above. Apply the policy to the Service VPN and to sites configured with tunnels.

View Data Policy Name* St0-redirect Description* StG-redirect Image: Custom Image: Custom Image: Custom Image: Custom Default Action Actions Description*: Port 80 443 Image: Custom Accept Secure Internet Gateway Enabled Secure Internet Gateway Enabled	≡ Cisco SD-	WAN	Ċ	Select Resource Group+		Configuration · Policies		\bigcirc	Ξ	04
Custom Actions Default Action Image: Custom in the image: Custom	View Data Policy Name* Description*	SIG-redire	t t							
Default Action Match Conditions Actions Default Action Destination: Port 80.443 Accept Secure Internet Gateway Fallback to Routing	Custom		(?	Custom						Data
	Default Action	efault Action		Match Conditions Destination: Port	80 443		Actions Accept Secure Internet Gateway Enabled Fallback to Routing			

Figure 19.

Cisco SD-WAN custom data policy configuration

Note: The default action is drop for traffic data policy, so change that to Accept.

≡ Cisco SD-	-WAN	Select Resource Group•	Configuration - Policies	
View Data Policy				
Name*	SIG-redirect			
Description*	SIG-redirect			
: Custom		Default Action		
Default Action		Accept	Enabled	

Figure 20.

Cisco SD-WAN default data policy configuration

Step 4: Verify Tunnel operation on Cisco Catalyst SD-WAN Manager and CLI

In the SD-WAN Manager GUI:

Under Monitor navigate to	Devices -> WAN Edg	e router ellipsis	-> Real Time

=	Cisco	SD-W	AN 🛇	Select Resourc	ce Group•		Moni	itor · Devices				C		9 (\$
						Overview	Devices Tunnels	Security VPN	Logs	Multicloud				
De	evices	Coloca	ation Cluster	Certificates	Licensing									
	Device Gr	oup All	~											
	Devices	(2/6)											① Expo	rt 🚳
	Q WAI	N												∇
												As of: Sep 25, 2023	03:21 PM	S
	Hostname		Device Model	Site ID	System IP	Health 🕕	Reachability	vSmart Control	BFD	Up Since	CPU Load	Memory Utilization	Act	ion
	CSRSD-WAN	N-1	C8000v	101	1.1.101.1	\oslash	\uparrow	1/1	1/1	Aug 22, 2023 07:27 PM	8.77%	43.1%		
	CSRSD-WAM	N-2	C8000v	101	1.1.101.2	\oslash	\uparrow	1/1	1/1	Sep 22, 2023 05:57 PM	9.09%	- 43.29 R	eal Time	
>											Items per page: 25 👻	1 - 2 of 2	SH Termina	

Figure 21. Cisco SD-WAN device monitoring Under Applications > Interface, click Real Time at the top right of the chart.

Then, select the interface on the right-hand side of the chart to view specific interface activity.



Figure 22.

Cisco SD-WAN device 360 Real Time Monitor

If the interface is missing from the graph, scroll down past the chart to see the complete list of interfaces. Click the checkbox on the left for the interface to display on the chart. You can view the state and statistics of all device interfaces from this list.

≡ Cisco SD-WAN	Select Resource (Group+	Monitor · Devices · Devic	e 360				
Network > Interface Select Device	CSRSD-WAN-1 1.1.101.1	Site ID: 101 Device Model: C8000v	0					
APPLICATIONS	8 Rows Selected	The interface details shown in th	e table is not historical but current status	from the device and do	esn't change when differe	nt time range is selec	ted. Total Rov	vs: 23 📿 🍪
SAIE Applications	Oper \downarrow (4) Oper 个	(19) Admin 🔶 (0) Admin 个 (23)						
Tracker	VPN (VRF)	Interface Name 👻 Interface de	scription Physical Address	IPv4 Address	IPv4 Subnet Mask	Admin Status	Oper Status	Interface Typ
QoS	0	Tunnel100201 Secondary	Tunnel 00:00:00:00:00:00	192.168.1.1	255.255.255.252	۲	^	iana-iftype-
ON-DEMAND TROUBLESHOOTING	0	Tunnel100101 Primary Tun	nel 00:00:00:00:00	10.2.1.5	255.255.255.0	\uparrow	\uparrow	iana-iftype-

Figure 23.

Cisco SD-WAN Real Time device interface monitoring

Verify Tunnel Operation Using CLI:

Use the show sdwan secure-internet-gateway tunnels command to view SIG tunnel status to Skyhigh SSE

Device# show TUNNEL IF	sdwan secu TUNNEL	re-internet-gateway tunnels	HA	DEVICE	SIG	TRACKE
NAME	ID	TUNNEL NAME	PAIR	STATE	STATE	STATE
Tunnel100001 Tunnel100002	52615809 52615814	site1820851800sys172x16x255x15ifTunnel100001 site1820851800sys172x16x255x15ifTunnel100002	Active Backup	Up Up	NA NA	Enable

Figure 24.

Cisco Edge device CLI output

Step 5: Verify web traffic on Skyhigh SSE cloud platform

Navigate to Analytics > Web > Web Traffic on the Skyhigh dashboard.

🚺 Skyhigh Security			Dashboard	ls Governanc	e	Analytics	Incidents	Policy	Reports				* 0 1	000 000 000
Web Traffic Overview >					-	Services								
Web Users						Users						Last 7 D	ays Sep 19 - Sep	26 UTC
						Web	>	Web Traffi	c					
< Filters Views	L	og Source: North A	merica			Unmatch	ned Uploads	Web Users					Save V	iew
						Infrastru	cture (laaS)	Web Malw	are					
1	4	Users 目				Vulnerat	le Storage	Isolated Si	Sites				Actions	~
Log Source						Connect	ed Apps	Isolated Fil	e Transfers					
Australia	U	ser Name 🔸	Site	Reputation	App Nan	Resource	es >	Requests	Requests	Isolated Requests	Time spent on Isolated Sites	Total Bytes	Downloaded Bytes	Uplc
Undia	4.	.155.16.89	1	Minimal Risk	Un	Devices		19.2 к	0	0	Os	28.2 мв	21.6 мв	E
North America	20	0.47.120.69	61	2	13	Private A	ccess >	33.6 к	1	0	Os	1.5 дв	1.5 дв	
United Arab Emirates	20	0.3.178.43	19	2	4		28.6 к	- 28.6 κ	3	0	Os	1.7 дв	1.7 дв	16
O United Kingdom	20	0 157 25 81	1	Minimal Risk	Uni	nown	4	A	0	0	0s	7.2 кв	5.8 KB	
				initia rask	011	alowin	-		0	0	05	7.2.10	5.0 10	
Reputation														
Minimal Risk 4														
Unverified 2														
Application Category														
Unknown 4														
Social media 2														
Collaboration 2														
Security 2														
Content Sharing 1														
IT Services 1														

Figure 25.

Skyhigh Web Traffic analytics

The Web Traffic page offers an overview of organization's traffic data, which can be used for analysis or reporting. It includes aggregated data on visits, website and application names, requests (hits), access status (allowed or denied), and data transfer (bytes uploaded and downloaded). For more details on filtering and sorting web traffic refer to this <u>article</u>.

Deployment models

Below are a few deployment models in the case of two SD-WAN edge devices, two ISPs, and two Skyhigh locations.



Deployment model 1: One active IPsec tunnel per WAN Edge

Figure 26.

SD-WAN and Skyhigh topology diagram with one active IPsec tunnel per Edge

- SD-WAN-1 is connected to the Skyhigh SSE Datacenter location LA using ISP1
- SD-WAN-2 is connected to the Skyhigh SSE Datacenter location SIN using ISP2
- Active IPsec tunnels are established from SD-WAN-1 and SD-WAN-2 to LA and SIN, respectively
- Service VPN is redundantly configured with VRRP





Figure 27.

SD-WAN and Skyhigh topology diagram with one active - one backup IPsec tunnel per Edge

- SD-WAN-1 is connected to the Skyhigh SSE Datacenter location LA using ISP1 and ISP2 (TLOC extension)
- SD-WAN-2 is connected to the Skyhigh SSE Datacenter location SIN using ISP1 (TLOC extension) and ISP2
- Active/Backup IPsec tunnels are established from SD-WAN1 router to LA and from SD-WAN-2 to SIN
- Service VPN is redundantly configured with VRRP



Deployment model 3: Two active/active ECMP IPsec tunnels per WAN Edge

Figure 28.

SD-WAN and Skyhigh topology diagram with two active ECMP IPsec tunnels per Edge

- SD-WAN-1 is connected to the Skyhigh SSE Datacenter location LA using ISP1 and ISP2 (TLOC extension)
- SD-WAN-2 is connected to the Skyhigh SSE Datacenter location SIN using ISP1 and ISP2 (TLOC extension)
- Active/Active ECMP IPsec tunnels are established from SD-WAN 1 to LA and from SD-WAN 2 to Singapore
- Service VPN is redundantly configured with VRRP

Skyhigh Web Gateway Configuration Modification Procedure

Once changes are made on the web gateway, save, and publish the changes.

Note: To make changes to configurations on Skyhigh UI, it is recommended to first shut down tunnels on the SD-WAN edge device and then perform the changes. Once changes are completed on the Skyhigh UI, enable the tunnels on the SD-WAN Edge. This will provide immediate implementation of any changes.

Configure L	ocation		
lame			
tme-cisco-branch	11-1		
ettings			
To configure adva	nced SAML settir	s, such as adding exceptions, use the configuration in Web Policy. Lear	rn more
Select SAML C	onfiguration	None Y	
Log Dat	ta Residency	Default 🗸	
P Range Mapping Provide your iden Client ID Type Client ID	IPSec Map tity settings Use a User Fi tme2@cisco.o	mg GRE Tunnel Mapping	
Client Address	20.157.25.81		
Pre-Shared Key	C1sco123456	890	
Cancel	Save		

() s	Skyhigh Security Dashboards Governance Analytics Incidents Policy Reports	- * 0 ± ∷
\bigcirc	Managing Certificate Authorities for HTTPS Scanning Changes to the polisy need to be published. Skyhigh provides a default certificate authority for SAML authentication and a custom certificate authority for HTTPS scanning. We recommide ploy it on your endpoints. We also recommend that you replace the custom CA with a CA of your own. You can manage the custom CA or the HTTPS Scanning feature configuration page	rking
	Setup SAML Configure SAML authentication to use your own Identity Provider (IdP) service to authenticate users.	New SAML
	Enable Active Directory User Group Lookup Enable a lookup of your user group or groups in an Active Directory (AD) when this information cannot be provided by Secure Client Proxy (SCP). User group information is required to select the appropriate web policy when you are logging on to Secure Web Gateway (SWG).	Configure

Figure 29.

Skyhigh location configuration changes

Cisco Catalyst SD-WAN Manager Configuration Modification Procedure

Example: To change IKE ID on IPsec tunnel101

Go to Configuration > Templates > Feature Template. Click on the ellipsis icon to edit the template.

≡ Cisco SD-W	IAN 💮 Select F	Resource Group -		Configuration • Te	emplates			△ ≡ ⊘ 4
			Configuration Groups	Feature Profiles Device	ce Templates Feature Te	emplates		
Q skyhigh × S	iearch							∇
Add Template								
Template Type Non-E	Default 🗸							Total Rows: 4 of 55 🛛 🖓
Name	Description	Туре	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
skyhigh-sig-template	skyhigh-sig-template	Cisco SIG - Secure Inte	C8000v	1	global	1	srsaredd	21 Sep 2023 1:24:08 •••
skyhigh-sig-template	. skyhigh-sig-template	Cisco SIG - Secure Inte	C8000v	1	global	1	srsaredd	25 Sep 2023 11:22:11
skyhigh-sig-template	. skyhigh-sig-template	Cisco SIG - Secure Inte	C8000v	0	global	0	admin	18 Jul View Edit
skyhigh-sig-template	. skyhigh-sig-template2	Cisco SIG - Secure Inte	C8000v	0	global	0	admin	18 Jul Change Device Models Change Resource Group Delete Copy

Edit the tunnel configuration, and save it as shown in figures 29 and 30 below by clicking Update and Save Changes.

≡ Cisco SD-WAN	⑦ Select Resource Group▼	Configuration	n · Templates		△ ≡ ⊘ \$
	Confi	guration Groups Feature Profiles	Device Templates Feature Templates		
Feature Template > Cisco Secure I	nternet Gateway (SIG) > skyhigh-sig-template-br2	-	-	~	-
		_		_	_
✓ Configuration					
Add Tunnel					
Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec101	Primary Tunnel	No	\odot	 ⊘ 1400 	
ipsec201	Secondary Tunnel	⊘ No	\odot	I400	
✓ High Availability					
Active	Active Weight	Backup	Backup Weight	t	
	-				
Pair-1 ipsec101	▼ ⊕ 1	ipsec201	• 1		
		Cancel	Update		

Figure 30.

Cisco SD-WAN device template configuration changes

Update Tunnel			
IKE			
IKE Rekey Interval (seconds)	€ • 86400		
IKE Cipher Suite	AES 256 CBC SHA1	•	
IKE Diffie-Hellman Group	14 2048-bit modulus	•	
IKE ID for local End point	● ▼ 10.10.10.10	\odot	
IKE ID for Remote End point	\odot -	\odot	
IPSec			
(Dear-Davan Internet (corrunte)			Save Changes Cancel

Figure 31. Cisco SD-WAN IPsec tunnel advanced configuration changes

Update and click Next.

Ξ	E Cisco SD-WAN	ct Resource (Group v	Configuration · Templa	tes		○ ≡	0 4
Devi	e Template 5d02cae9-5d71-43f3-	90e5-db565	0dabca6					
	Q Search							∇
							Total Rows: 1	<u>∓</u> <u>↓</u>
	S Chassis Number	System IP	Hostname	Interface Name(GigabitEthernet4)	IPv4 Address/ prefix-length(172.101.1.2/24)	Prefix(0.0.0.0/0)	Address(1	
	C8K-D976AF4A-D471-B137-C8E9-F0E6	1.1.101.2	CSRSD-WAN-2	GigabitEthermet4	172.16.1.2/24	0.0.0.0/0	192.168.1ť •	••
				Next Cancel				

Figure 32.

Cisco SD-WAN device provisioning with changes

Config preview and config differences can be viewed on this page.



Figure 33.

Cisco SD-WAN config preview

Config difference can be viewed in two ways: side by side or inline.

This is an inline view with changes highlighted in red and green. Once validated, click Configure Devices.

≡ Cisco SD-WAN		⊙ s	elect	Reso	urce Group • Configuration • Templates						
Device Template	Total		204	294	crypto revez keyring in-apseczor-ikevz-keyring						
5d02cae9-5d71-43f3-9	1		295	295	peer lf-lpsec201-lkev2-keyring-peer						
			386	386	auguruss 103.221.07.2						
Device list (Total: 1 devices)			387	387	pre-snareu-key Ciscoizz4567650						
Filter/Search			388	388							
			389	389	crypto ikey2 policy_policyl-global						
			390	390	proposal pl-global						
F0E66BF69433			391	391							
			392	392	crypto ikev2 profile if-ipsec101-ikev2-profile						
			393	393	authentication local pre-share						
			394	394	authentication remote pre-share						
395 395				395	no config-exchange request						
396			396	396	dpd 10 3 on-demand						
			397		identity local email tme@cisco.com						
				397	identity local address 10.10.10.10						
398			398	398	keyring local if-ipsec101-ikev2-keyring						
399 3			399	399	lifetime 86400						
400				400	match identity remote address 185.221.69.2						
401 4				401	1						
			402	402	crypto ikev2 profile if-ipsec201-ikev2-profile						
			403	403	authentication local pre-share						
			404	404	authentication remote pre-share						
			405	405	no config-exchange request						
			406	406	dpd 10 3 on-demand						
			407	407	identity local email tme2@cisco.com						
			408	408	keyring local if-ipsec201-ikev2-keyring						
			409	409	lifetime 86400						
			410	410	match identity remote address 185.221.69.2						
			411	411	1						
			412	412	crypto ikev2 proposal p1-global						
			413	413	encryption aes-cbc-128 aes-cbc-256						
Configure Device Rollback Time	er										
					Back Configure Devices Cancel						

Figure 34.

Cisco SD-WAN config difference

Once the Configuration is deployed to SD-WAN Edge, the status returns as Success.

≡	Cisco SD-WAN	O Select Resource G	roup•						0 4				
Push	Jush Feature Template Configuration 🖉 Validation Success Initiated By: srsaredd From: 73.231.130.88												
Total	Task: 1 Success : 1												
Q	Search								∇				
								Total Rows: 1	C 🕸				
~	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP					
	Success	Template successfully attac	C8K-D976AF4A-D471-B13	C8000v	CSRSD-WAN-2	1.1.101.2	101	1.1.1.1					
	[25-Sep-2023 11:17:10 PDT] [25-Sep-2023 11:17:11 PDT] [25-Sep-2023 11:17:16 PDT] [25-Sep-2023 11:17:16 PDT] [25-Sep-2023 11:17:21 PDT] [25-Sep-2023 11:17:21 PDT]	Updating device configura Sending configuration to Successfully notified dev Device has pulled the con Device: Config applied su Template successfully att	tion in vManage device ice to pull configuration figuration ccessfully ached to device										

Figure 35.

Cisco SD-WAN configuration status

In conclusion, the integration of Cisco Catalyst SD-WAN with Skyhigh SSE 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 customers implementing the Skyhigh Secure Service Edge solution alongside Cisco Catalyst SD-WAN, providing flexibility and reliable performance.

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.

• <u>SDWAN@cisco.com</u>

For more information

Please visit:

- <u>Cisco SD-WAN Security</u>
- <u>Cisco SASE</u>

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