

Skyhigh[®] Security Service Edge (SSE)

IPSec Silver Peak Edge Connect



Page 1 of 12

Table of Contents

HUB AND SPOKE ARCHITECTURE 3 DIRECT TO CLOUD 4 CONFIGURING IPSEC SITE-TO-SITE WITH SILVER PEAK 4 IPSEC SITE-TO-SITE OVERVIEW 4 ENVIRONMENT. 4 SETUP INCLUDES. 4 CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE 5 FINDING THE BEST AVAILABLE POINTS OF PRESENCE 5 CONFIGURING AN IPSEC VPN TUNNEL WITH SILVER PEAK EDGECONNECT 6 CLIENT ADDRESS 9 FULLY QUALIFIED DOMAIN NAME 10 USER FQDN 11	INTRODUCTION TO SD-WAN ARCHITECTURE
DIRECT TO CLOUD 4 CONFIGURING IPSEC SITE-TO-SITE WITH SILVER PEAK 4 IPSEC SITE-TO-SITE OVERVIEW 4 ENVIRONMENT 4 SETUP INCLUDES 4 CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE 5 FINDING THE BEST AVAILABLE POINTS OF PRESENCE 5 CONFIGURING AN IPSEC VPN TUNNEL WITH SILVER PEAK EDGECONNECT 6 CLIENT ADDRESS 8 SPECIFIC IPV4 ADDRESS 9 FULLY QUALIFIED DOMAIN NAME 10 USER FQDN 11	HUB AND SPOKE ARCHITECTURE
CONFIGURING IPSEC SITE-TO-SITE WITH SILVER PEAK 4 IPSEC SITE-TO-SITE OVERVIEW 4 ENVIRONMENT 4 SETUP INCLUDES 4 CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE 5 FINDING THE BEST AVAILABLE POINTS OF PRESENCE 5 CONFIGURING AN IPSEC VPN TUNNEL WITH SILVER PEAK EDGECONNECT 6 CLIENT ADDRESS 8 SPECIFIC IPV4 ADDRESS 9 FULLY QUALIFIED DOMAIN NAME 10 USER FQDN 11	DIRECT TO CLOUD
IPSEC SITE-TO-SITE OVERVIEW 4 ENVIRONMENT. 4 SETUP INCLUDES 4 CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE 5 FINDING THE BEST AVAILABLE POINTS OF PRESENCE 5 CONFIGURING AN IPSEC VPN TUNNEL WITH SILVER PEAK EDGECONNECT 6 CLIENT ADDRESS 8 SPECIFIC IPV4 ADDRESS 9 FULLY QUALIFIED DOMAIN NAME 10 USER FQDN 11	CONFIGURING IPSEC SITE-TO-SITE WITH SILVER PEAK4
ENVIRONMENT. 4 SETUP INCLUDES. 4 CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE 5 FINDING THE BEST AVAILABLE POINTS OF PRESENCE 5 CONFIGURING AN IPSEC VPN TUNNEL WITH SILVER PEAK EDGECONNECT 6 CLIENT ADDRESS 9 FULLY QUALIFIED DOMAIN NAME 10 USER FQDN 11	IPsec site-to-site overview
SETUP INCLUDES	ENVIRONMENT
CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE	SETUP INCLUDES
FINDING THE BEST AVAILABLE POINTS OF PRESENCE	CONSIDERATIONS FOR CONFIGURING IPSEC SITE-TO-SITE
CONFIGURING AN IPSEC VPN TUNNEL WITH SILVER PEAK EDGECONNECT	FINDING THE BEST AVAILABLE POINTS OF PRESENCE
CLIENT ADDRESS	CONFIGURING AN IPSEC VPN TUNNEL WITH SILVER PEAK EDGECONNECT6
SPECIFIC IPV4 ADDRESS	CLIENT ADDRESS
FULLY QUALIFIED DOMAIN NAME	SPECIFIC IPv4 Address
User FQDN11	FULLY QUALIFIED DOMAIN NAME
	User FQDN11



Page 2 of 12

Introduction to SD-WAN Architecture

A Software-Defined Wide Area Network (SD-WAN) is a virtual WAN architecture that simplifies the connectivity, management, and operation of a traditional WAN.

As more companies shift to cloud applications, the result is a higher demand for bandwidth and direct internet connections to remote locations. Traditional MPLS networks are secure and stable, but expensive, and often fall victim to backhauling via the traditional hub and spoke architecture, where data is routed back through a central data center and out again to remote offices and users.



Hub and Spoke Architecture

SD-WAN combines traditional WAN technologies, such as MPLS and broadband connections, because it is abstracted from the hardware. Organizations leverage SD-WAN solutions because they provide enhanced capabilities for connectivity, monitoring, and managing network traffic while reducing cost.

Skyhigh Security Service Edge leverages SD-WAN technologies that allow remote offices to securely redirect web traffic to the Skyhigh Secure Web Gateway Cloud Service, where it is filtered according to your organization's web policy.



Page 3 of 12

Direct to Cloud



This guide explains how to set up IPsec tunnels from Silver Peak EdgeConnect to Skyhigh Secure Web Gateway Cloud Service to apply policies and enable advanced security inspection.

Configuring IPsec site-to-site with Silver Peak

If your organization uses one of the supported third-party devices to secure your network, you can use the IPsec protocol to secure communications between your network and Skyhigh Cloud Service.

IPsec site-to-site overview

To secure communications between a remote site and Skyhigh WGCS using IPsec siteto-site authentication, you create an IPsec VPN tunnel between the supported SD-WAN device and the cloud service.

Environment

- Skyhigh Security Service Edge (SSE)
- Silver Peak EdgeConnect

Setup includes

- Configuration of Skyhigh WGCS using the Skyhigh Security Service Edge management console.
- Configuration of the supported device.



Page 4 of 12

For information about configuring Skyhigh WGCS for IPsec site-to-site, see the Skyhigh Secure Web Gateway Cloud Service Guide.

Considerations for configuring IPsec site-to-site

Before configuring IPsec site-to-site authentication, review the following considerations.

- Routing only HTTP and HTTPS traffic Skyhigh WGCS only handles IPsec traffic directed to ports 80 and 443 (HTTP and HTTPS traffic, respectively) through the VPN tunnel. Configure your device to route only HTTP and HTTPS traffic through the VPN tunnel.
- **Configuring two IPsec VPN tunnels** Best practice is to configure a primary and secondary VPN tunnel. The primary tunnel is connected to the best available point of presence (POP), while the secondary tunnel is connected to the second-best point of presence. This practice ensures continuous IPsec support in case one point of presence is not available.
- Using an IPsec VPN tunnel to connect remote sites If you have one or more remote sites that are connected to your network by VPN, you can protect traffic and improve network latency by creating a VPN tunnel between each site and Skyhigh WGCS.
- Adding SAML authentication You can add a SAML configuration to an IPsec location. Skyhigh WGCS uses SAML to authenticate requests received from the location through the IPsec tunnel.
- Using a NAT device If your IPsec device is located behind a NAT device and the outgoing interface has a private IP address, set the Local ID attribute to your public IP address.

Finding the best available points of presence

To find the point of presence closest to the device that you are configuring for IPsec authentication, you query the Global Routing Manager (GRM). The GRM is a DNS service that routes traffic to the best available point of presence.

From the network where your device is installed, run the nslookup command-line tool, as follows:

- nslook-up l.network.wgcs.Skyhigh.cloud
- nslook-up 2.network.wgcs.Skyhigh.cloud

In response to these commands, the GRM returns the IP addresses of the best and second-best points of presence, respectively, based on the network location of your device. You need these values when configuring the primary and secondary IPsec VPN tunnels in your device and in Skyhigh WGCS.



Page 5 of 12

Configuring an IPsec VPN tunnel with Silver Peak EdgeConnect

Configure the IPsec VPN tunnel in the Silver Peak EdgeConnect web interface.

- 1. Log on to the web interface that you use to configure the EdgeConnect device on your remote network.
- 2. Select Configuration | Tunnels | Tunnels to open the Tunnels page.
- 3. Select Passthrough to open the Passthrough page.
- 4. Click the pencil icon to edit the tunnel, then click Add Tunnel.
- 5. Select the **General** tab, then configure these settings:
 - Alias Specify a name for the configuration.
 - Mode Select IPsec.
 - Admin Select Up.
 - Local IP Provide the public IP address of the EdgeConnect appliance installed on your network.
 - Remote IP Specify the IP address that Skyhigh WGCS uses for IPsec communications. To find the IP address of the point of presence closest to your device, you can use the nsLook-up command-line tool to query the Global Routing Manager.
 - NAT Select None.
 - **Peer/Service** Leave this field blank.
 - Auto Max BW Enabled Select this setting.
 - Max BW Kbps Leave this field blank.
- 6. Click **Save** to save the general settings.
- 7. Select the IKE tab, then configure these settings:
 - Pre-Shared Key Provide the same pre-shared key value that you provide when configuring the IPsec location in the Skyhigh SSE
 - Authentication Algorithm Select SHA2 or higher.
 - Encryption Algorithm Select SHA2-256 or AES-256.
 - Diffie-Hellman Group Select 2 or higher.
 - Lifetime Specify 360 for Mins.
 - Dead Peer Detection Specify 300 for the Delay Time and 5 for the Retry Count.
 - Local IKE Identifier This value must match the Client ID that you specify when configuring IPsec in the Skyhigh SSE. If the Client ID Type selected in the Skyhigh SSE is the Client Address, provide the client address for the client ID.
 - **Remote IKE Identifier** This value must match the value that you provided for the **Remote IP** on the **General** tab.
 - Phase 1 Mode Select Aggressive, then select IKE v2 for the IKE Version.



Page 6 of 12

Note: The selected algorithms and the value of the pre-shared key must match the IPsec configuration in the Skyhigh SSE. For example, if you select SHA1 for IKE in EdgeConnect, you must also select SHA1 as the authentication algorithm in Skyhigh SSE.

- 8. Click **Save** to save the IKE settings.
- 9. Select the IPsec tab, then configure these settings:
 - Authentication Algorithm Select SHA2 or higher.
 - Encryption Algorithm Select SHA2-256 or AES-256.
 - Enable IPsec Anti-replay Window Select this setting.
 - Lifetime Specify 360 for Mins and 0 for MegaBytes.
 - Perfect Forward Secrecy Group Select 2 or higher.

10. Click **Save.**

The IPsec VPN tunnel is configured on the Silver Peak EdgeConnect side.

IPsec VPN configuration options

You use one of the following options when configuring IPsec site-to-site authentication in the EdgeConnect web interface. Then you select the same option from the Child ID Type drop-down list when configuring IPsec site-to-site in the Skyhigh SSE.

- Client Address
- Specific IPv4 Address
- Fully qualified Domain Name
- User FQDN



Page 7 of 12

Client Address

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **Client Address** as the **Client ID Type** in the Skyhigh SSE.

人	silver	rpeak~						///	///
Netwo	rk View	Monitoring	Configuration	Administration	Maintenance	Support			
Tun	nels 🕜	Ċ	Config	uration Monitoring	l i	Modify Passthrough Tunnel		×]
Use sh Und 4 Ro	iared subnet lerlay Pa	information ssthrough	Add Tunnel R			General IKE IPsec IKE Preshared Key	•••••		
Edit	Passthro	ugh Tunnel	Admin State	Status	L	Authentication Algorithm Encryption Algorithm	SHA2-256 💌 AES-256 💌		NAT
1	Jay-ipv4		down	down	n 192.168.	Diffie-Hellman Group	14		
1	UserFQDN-	×	down	down	n 192.168.	Lifetime	360	Mins	
1	ClientAddre	SS	down	down	n 192.168.	. Dead Peer Detection		-	
1	FQDN		up	up - act	tive 192.168.	Delay time	10	Secs	
						Retry Count	3 DPD effective timeout 34 Se	cs.	
						Local IKE Identifier	1		
						Remote IKE Identifier	185.xxx.xxx.xxx		
						Phase 1 Mode	Aggressive 👻		
						IKE Version	IKE v2		
							Save	incel	

To configure IPsec site-to-site authentication in the Skyhigh SSE, select **Settings** | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping.

IP Range Mapping	IPSec Mapping					
Provide your identity settings						
Client ID Type	Use Client Address 🛛 🗸					
Client Address	106.201.35.24					
Pre-Shared Key	mic_1234					



Page 8 of 12

Specific IPv4 Address

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **Specific IPv4 Address** as the **Client ID Type** in the Skyhigh SSE.

two	rk View Monitoring	Configuration	Administration	Maintenance	Support			
lunr	nels 🕜 💽	Config	uration Monitoring		Modify Passthrough Tunnel		×	1
se sh	ared subnet information	V			General DE IPsec	+t+		
Und	erlay Passthrough	Add Tunnel R	ediscover MTU		IKE	12		
4 Ro	ws. 1 Selected				Preshared Key			
	Department Transl	A data	Chaba		Authentication Algorithm	SHA2-256		
Car	Passtnrough Tunnel	State	Scatus		Encryption Algorithm	AES-256		NAT.
/	Jay-ipv4	down	down	192.168	Diffie-Helman Group	14		
1	UserFQDN-x	down	down	192.168.	Lifetime	360	Mins	
1	ClientAddress	down	down	192.168.	Dead Peer Detection			
1	FQDN	up	up - act	ive 192.168.	Delay time	10	Secs	
					Retry Count	3		
						DPD effective timeout 345	ecs.	
					Local IXE Identifier	147	4	
					Remote IKE Identifier	185.XXX.XXX.XXX	_	
					Phase 1 Mode	ME v2		
					IAE Version	1NC Y2		

To configure IPsec site-to-site authentication in the Skyhigh SSE, select **Settings** | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping.

IP Range Mapping	IPSec Mapping						
Provide your identity settings							
Client ID Type	Use specific IPv4 Address 🛛 🗸						
Client ID	192.168.145.132						
Client Address	106.201.35.24						
Pre-Shared Key	mic_1234						
	li li						



Page 9 of 12

Fully Qualified Domain Name

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **Fully Qualified Domain Name** as the **Client ID Type** in the Skyhigh SSE.

Modify Passthrough Tunnel Add Tunnel Rows, 1 Selected Edit Passthrough Tunnel Admin State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State	×		lodify Passthrough Tunnel					
Jase shared subnet information Underlay Passtbrough Add Tunnel Rediscover MTU 4Rows, 1 Selected Edit Passtbrough Tunnel Admin State Londerlay Passtbrough Tunnel Admin State Londown 192.168. Lifetime Jay-ipv4 down down down down 192.168. Delay time Lifetime Jay-ipv4 down down 192.168. Delay time Lifetime Delay time Lifetime Delay time	1				<i>iration</i> Monitoring	Config	2	unne
Underlay Passtbrough Add Tunnel Rediscover MTU IKE 4 Rows, 1 Selected]		General IKE IPsec				onet information	se shar
ARows, 1 Selected Preshared Key Edit Passthrough Tunnel Admin State Status Lo 4 Jay-ipv4 down down 192.168.1 Ver CDN-x down down 192.168.1 CientAddress down 192.168.1 Dead Peer Detection Dead Peer Detection	J		IKE		ediscover MTU	Add Tunnel R	Passthrough	Under
Edit Passthrough Tunnel Admin State Status Lo Authentication Algorithm SHA2-256 / Jay-ipv4 down down 192.168.1 Diffe-Hellman Group 14 / UserFQDN-x down down 192.168.1 Lifetime 360 10 / ClientAddress down 192.168.1 Dead Peer Detection Dead Year Delay time 10 10		•••••	Preshared Key				elected	4 Rows
East Admin Status Encryption Algorithm AES-256 * Jay-ipv4 down down 192.168.1 Diffie-Hellman Group 14 * UserFQDN-x down down 192.168.1 Lifetime 360 14 * ClientAddress down 192.168.1 Dead Peer Detection 10 10		SHA2-256 💌	Authentication Algorithm		Chabus	8 desire	there are Transal	- dia
Jay-ipv4 down down 192.168. Diffie-Hellman Group 14 UserFQDN-x down down 192.168. Lifetime 360 ClientAddress down down 192.168. Dead Peer Detection ECDN up up up 102.168. Delay time		AES-256	Encryption Algorithm	LO	Status	State	surrougn runner	Edit
UserFQDN-x down down 192.168.: Lifetime 360 ClientAddress down down 192.168.: Dead Peer Detection Image: ClientAddress umage: ClientAddress 192.168.: Dead Peer Detection		14	Diffie-Hellman Group	192.168.1	down	down	4	/ J.
ClientAddress down down 192.168.; Dead Peer Detection Dead y time 10	Mins	360	Lifetime	192.168.1	down	down	DN-x	/ U
FORM ID DELTING 102 158 Delay time 10			Dead Peer Detection	192.168.1	down	down	ddress	/ c
up up active 192.106.1	Secs	10	Delay time	ive 192.168.1	up - act	up		/ F
Retry Count 3		3	Retry Count					
DPD effective timeout 34 Secs	.s.	DPD effective timeout 34 Secs	a contrato a contra					
Local IKE Identifier	j		Local IKE Identifier					
Remote IKE Identifier 185.xxx.xxx	J	185.xxx.xxx.xxx	Remote IKE Identifier					
Phase 1 Mode Aggressive 👻		Aggressive v	Phase 1 Mode					
IKE Version IKE v2		IKE V2	IKE Version					

To configure IPsec site-to-site authentication in the Skyhigh SSE, select **Settings** | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping.

IP Range Mapping	IPSec Mapping
Provide your iden	tity settings
Client ID Type	Use Fully Qualified Domain Name 🛛 🗸
Client ID	Juliniau Taul.com
Client Address	223.235.221.102
Pre-Shared Key	mic_123
	<i>h</i>



Page 10 of 12

User FQDN

This screenshot shows how to configure IPsec site-to-site authentication in the EdgeConnect web interface when you select **User FQDN** as the **Client ID Type** in the Skyhigh SSE.

etwo	rk View Monitoring	Configuration	Administration	Maintenance	Support	t		
F un se sh Und	nels () () 3 mins	Config	uration Monitoring	1		Modify Passthrough Tunnel General IKE IPsec IKE Preshared Key	•••••	×
4Rd	ows, 1 Selected			~		Authentication Algorithm	SHA2-256	
Edit	Passthrough Tunnel	Admin State	Status		Local IP	Encryption Algorithm Diffie-Hellman Group	AES-256	
1	Jay-ipv4	down	dow	n 192.16	8.145.132	Lifetime	360	Mins
1	FQDN	down	dow	n 192.16	8.145.132	Dead Peer Detection		
1	ClientAddress	down	dow	n 192.16	8.145.132	Delay time	10	Secs
1	UserFQDN-x	up	up - ac	tive 192.16	8.145.132	Retry Count	3	
						Local IKE Identifier Remote IKE Identifier Phase 1 Mode IKE Version	DPD effective timeout : jai@min.mosfie.com 185.xxx.xxx.xxx Aggressive + IKE v2 +	34 Secs.

To configure IPsec site-to-site authentication in the Skyhigh SSE, select **Settings** | Infrastructure | Web Gateway Setup | New Location | IPsec Mapping.

IP Range Mapping	IPSec Mapping
Provide your iden	tity settings
Client ID Type	Use a User FQDN 🗸
Client ID	
Client Address	106.201.35.24
Pre-Shared Key	mic_1234



Page 11 of 12

Configure Business Intent Overlay policies for Silver Peak

To use the IPsec VPN tunnels in a business intent overlay, complete the following steps.

- 1. From the Silver Peak Orchestrator, select **Configuration: Business Intent Overlay**.
- 2. Select Create New.
- 3. Select ACL Policies, then click Add Rule.
- 4. Click Edit Match Criteria, then select Add port 80, 443.
- 5. Click **Save** to return to the previous page.
- 6. On the Business Intent Overlay page, move the services to the Preferred Policy Order section, then move the primary service above the secondary service. The primary and secondary services correspond to the primary and secondary IPsec VPN tunnels that you configure. If the primary tunnel is not available, the system sends the web traffic through the secondary tunnel to Skyhigh WGCS for filtering. If neither tunnel is available, the system drops the web traffic.
- 7. Click Save all to apply the changes.

The business intent overlay policies point to the primary and secondary IPsec VPN tunnels.

Trellix, FireEye, and Mcafee Security are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC and their affiliates in the US and /or other countries. Mcafee is the trademark or registered trademark of Mcafee LLC or its subsidiaries in the US and /or other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

Copyright © 2022 Musarubra US LLC.



Page 12 of 12