



HPE Aruba Networking

EdgeConnect and Zscaler Internet Access IPSec Integration Guide



Hewlett Packard
Enterprise

May 2024
Rev D

Contents

Copyright and Trademarks	3
Support	4
Related Documentation	5
About Zscaler Integration with EdgeConnect	6
Zscaler Prerequisites	7
Find the IP Address of Primary and Secondary ZENS	7
Create a VPN Credential in Zscaler	9
Create a Location in Zscaler	11
Tunnel Capacity Limits	12
Deployment Scenarios with EdgeConnect	13
Internet Breakout with One Internet Service Provider (ISP)	13
Configure Business Intent Overlay Policies	13
Configure IPsec Tunnels	15
Verify Client Traffic is Sent to ZIA	18
Internet Breakout with Two ISPs	18
Failure Scenarios	19
Configure Two Locations in Zscaler Cloud Service	20
Configure Business Intent Overlay Policies	21
Configure IPsec Tunnels	23
Verify Client Traffic is Sent to ZIA	27



Copyright and Trademarks

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to [Aruba Eula](#).

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America



Support

For product and technical support, contact Support using any of the following methods:

1.877.210.7325 (toll-free in USA)

+1.408.935.1850

www.silver-peak.com/support

We're dedicated to continually improving the usability of our products and documentation.

If you have suggestions or feedback for our documentation, send an e-mail to sp-techpubs@hpe.com.



Related Documentation

- **Release Notes** provide information on new software features, system bugs, and software compatibility.
- All HPE Aruba Networking EdgeConnect SD-WAN user documentation is available at <https://www.arubanetworks.com/website/techdocs/sdwan/>.
- Visit the following websites for more information about Zscaler.
 - Zscaler documentation and knowledge base: <https://help.zscaler.com/zia?filter=documentation>
 - ZIA test page: <http://ip.zscaler.com/>



About Zscaler Integration with EdgeConnect

This guide explains how to service chain traffic from HPE Aruba Networking EdgeConnect in a branch to Zscaler Internet Access (ZIA) to enable advanced security inspection.

You can service chain EdgeConnect with ZIA by setting up interoperable site-to-site IPSec tunnels between EdgeConnect and ZIA.

ZIA uses Zscaler Endpoint Nodes (ZENs) to inspect web traffic and enforce security policies.

CAUTION This guide represents the **manual** configuration of IPsec tunnels from EdgeConnect to the Zscaler cloud. Refer to the [Zscaler Internet Access](#) section on the HPE Aruba Networking EdgeConnect SD-WAN Documentation site if you want to automate this process.



Zscaler Prerequisites

Before you can service chain traffic from EdgeConnect to Zscaler Internet Access, complete the following prerequisites.

- Create a Zscaler Internet Access account.
- For FQDN-based authentication, provision your organization domain and user names in Zscaler.

Find the IP Address of Primary and Secondary ZENs

To establish IPsec tunnels from an EdgeConnect appliance to your primary and secondary ZENs, first identify the public IP address of your ZENs.

1. In your browser address bar, enter `ips.<Your Zscaler cloud name>.net`.

TIP Find the name of your cloud portal in the URL that your administrator uses to sign in to the Zscaler service. For example, if your administrator signs in to **admin.zscalertwo.net**, your organization's cloud name is **zscalertwo**. In this case, enter `ips.zscalertwo.net`.

NOTE Refer to the "What is my cloud name"? page on the [Zscaler website](#).

2. From the left pane, select **Cloud Enforcement Node Ranges**.
3. From the **VPN Host Name** column, find the two ZENs that are the closest to your EdgeConnect application's location.



4. Choose one of the two Zscaler locations as your primary ZEN and the other as your secondary ZEN.

Cloud Enforcement Node Ranges

Looking for the latest changes? [Changelog](#)

Customers that have implemented private Cloud Enforcement Nodes in their environment; you may need to take into account additional address ranges not represented here. Customers should ensure that access is permitted to data center IP ranges. Allowing access to only specific IP addresses may result in a loss of service.

Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	VPN Host Name	Notes
Europe Copy IP Addresses					
Frankfurt IV	165.225.72.0/22	fra4.sme.zscalerbeta.net	165.225.72.38	fra4-vpn.zscalerbeta.net	
US & Canada Copy IP Addresses					
San Francisco IV	199.168.148.0/23	sunnyvale1.sme.zscalerbeta.net	199.168.148.131	sunnyvale1-vpn.zscalerbeta.net	
Washington DC	104.129.194.0/23	was1.sme.zscalerbeta.net	104.129.194.38	was1-vpn.zscalerbeta.net	

5. After you identify your location and the VPN host name, use `nslookup` or `ping` to find the public IP address of the primary and secondary ZENs.




```
Command Prompt
Microsoft Windows [Version 10.0.17134.48]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\> nslookup sunnyvale1-vpn.zscalerbeta.net
Server: UnKnown
Address: 172.23.40.18

Non-authoritative answer:
Name: sunnyvale1-vpn.zscalerbeta.net
Address: 199.168.148.132

C:\Users\> nslookup was1-vpn.zscalerbeta.net
Server: UnKnown
Address: 172.23.40.18

Non-authoritative answer:
Name: was1-vpn.zscalerbeta.net
Address: 104.129.194.39

C:\Users\>
```

Create a VPN Credential in Zscaler

Follow these steps to create a VPN credential in Zscaler. Add your VPN credentials and link the VPN credentials to a location.

1. Sign in to the Zscaler cloud portal.
The Dashboard screen opens.
2. Select **Administration**, and under Resources, select **VPN Credentials**.
The VPN Credentials screen opens.
3. Select **+Add VPN Credential**.
The Add VPN Credential screen opens.
4. For **Authentication Type**, select FQDN to identify your peer, and specify the following menu items based on your selection.

NOTE Do not use **Xauth** as an authentication type.



FQDN-based authentication	Task
User ID	Enter a user name and select the FQDN from the list.
New Pre-Shared Key	Enter a pre-shared key.
Confirm New Pre-Shared Key	Re-enter the pre-shared key.
Comments	Any additional information about the credential.

IP address-based authentication	Task
IP Address	Select the EdgeConnect static public IP address from the list. First ask Zscaler support to provide the EdgeConnect's static public IP address so it displays in the list.
New Pre-Shared Key	Enter a pre-shared key.
Confirm New Pre-Shared Key	Re-enter the pre-shared key.
Comments	Any additional information about the credential.

5. Select **Save**.



Add VPN Credential
✕

VPN CREDENTIAL

Authentication Type

FQDN
XAUTH
IP

User ID

@

silverpeak-demo.com
▾

New Pre-Shared Key

.....

Confirm New Pre-Shared Key

.....

Comments

zscaler PSK

Save
Cancel

Create a Location in Zscaler

Follow the steps to create a location.

1. Select **Administration**.
2. Under **Resources**, select **Locations**.
The **Locations** screen opens.
3. Select **+Add Location**.
The Add Location screen opens.
4. Configure the **Location** settings.

Location Settings	Task
Name	Enter a name for your location setting.
State/Province	Enter your state or province.



Group	Select the default group.
Country	Select your country.
TimeZone	Select your time zone.

LOCATION

Name Test driving the new Python SDK	Country NONE
State/Province	Time Zone NONE
Group None	Managed By Silver Peak

ADDRESSING

VPN Credentials
test@demo-silver-peak.com

GATEWAY OPTIONS

Enable XFF Forwarding <input type="checkbox"/>	Enforce Authentication <input type="checkbox"/>
Enable AUP <input type="checkbox"/>	
Enable SSL Scanning <input type="checkbox"/>	Enforce Firewall Control <input type="checkbox"/>

BANDWIDTH CONTROL

Enforce Bandwidth Control

TIP If you select **FQDN** as the authentication method, instead of selecting the EdgeConnect's public IP address as the VPN Credential, select the **user_FQDN** IKE identifier.

5. Select **Save**.

Tunnel Capacity Limits

Zscaler supports a soft limit of 200 Mbps per tunnel. If you require more bandwidth, create multiple tunnels in Zscaler. For example, two tunnels to a single ZEN provide 400 Mbps. Three tunnels provide 600 Mbps. On the EdgeConnect appliance, the tunnel capacity depends on the appliance model and the available WAN bandwidth. If you configure parallel tunnels, each IPsec tunnel must source from a unique IP address.



Deployment Scenarios with EdgeConnect

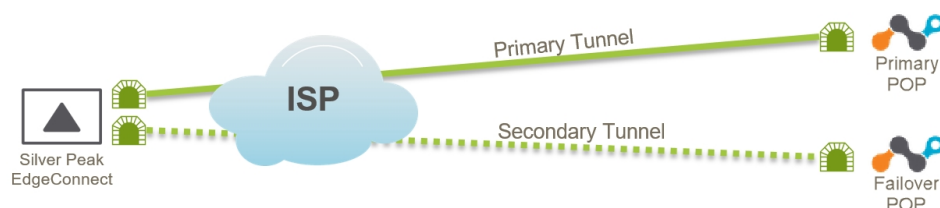
HPE Aruba Networking supports two ways to configure and deploy an EdgeConnect appliance with Zscaler Internet Access.

- [Internet Breakout with One Internet Service Provider \(ISP\) below](#)
- [Internet Breakout with Two ISPs on page 18](#)

NOTE Use ECOS version 8.1.8.0 or later and Orchestrator version 8.4.0 or later.

Internet Breakout with One Internet Service Provider (ISP)

When an EdgeConnect appliance has access to the Internet using a single internet service provider (ISP), the appliance can create two IPsec VPN tunnels to a primary ZEN and secondary ZEN as shown in the following figure. Only the primary tunnel carries traffic to the primary ZEN. If the primary tunnel is inactive, EdgeConnect automatically routes the traffic to the secondary ZEN.



Configure Business Intent Overlay Policies

Complete the following steps to configure BIO policies to associate with Zscaler.

Before creating the IPsec tunnels from the EdgeConnect appliance to the primary and secondary ZENs, create a business intent overlay (BIO) on the Orchestrator system that points to the IPsec tunnels. Using access control lists (ACL), specify the applications that you want to forward to Zscaler on the BIO screen.

TIP Before creating a BIO, create ACLs on the **Configuration > Template** screen and apply them on the EdgeConnect appliance.

NOTE Refer to the BIO and ACL online help for more information.

1. From the Orchestrator home screen, select **Configuration > Business Intent Overlays**.

The **Business Intent Overlays** tab opens.



Business Intent Overlays ? [Apply Overlays](#) [Regions](#) [Hubs](#) [View Overlay Stats](#) [Interface Labels](#)

Priority	Overlay	SD-WAN Traffic to Internal Subnets ↗				Breakout Traffic to Internet & Cloud Services ↗			
		Topology	Hubs	Primary Interfaces	Backup Interfaces	QoS & Security	Policy Order	Primary Interfaces	Backup Interfaces
1	RealTime Match Traffic Overlay ACL	Mesh		MPLS1 INET2 INET1 MPLS2 High Availability Waterfall: Overall Quality	LTE If Pri & Sec Down		1 Zscaler Cloud 2 Check Point Clou... 3 Break out 4 Backhaul	INET2 INET1 Waterfall: Auto	LTE
2	CriticalApps Match Traffic Overlay ACL	Mesh		INET2 INET1 MPLS1 MPLS2 High Quality Waterfall: Overall Quality	LTE If Pri & Sec Down		1 Break out 2 Backhaul	INET2 INET1 Waterfall: Auto	LTE
3	BulkApps Match Traffic Overlay ACL	Mesh		INET2 INET1 MPLS1 MPLS2 High Quality Waterfall: Overall Quality	LTE If Pri & Sec Down		1 Break out 2 Backhaul	INET2 INET1 Waterfall: Auto	LTE
4	DefaultOverlay Match Traffic Overlay ACL	Mesh		INET2 INET1 MPLS1 MPLS2 High Quality Waterfall: Overall Quality	LTE If Pri & Sec Down		1 Break out 2 Backhaul	INET2 INET1 Waterfall: Auto	LTE
5	voice Match Traffic lan	Mesh		MPLS1 High Quality Waterfall: Overall Quality			1 Check Point Clou... 2 Backhaul	Waterfall: Auto	

[+New](#)

NOTE In this example, the BIO references a **CriticalApps** ACL that already exists on the EdgeConnect appliance.

- Click any cell in the column **SD-WAN Traffic to Internal Subnets**. This opens the BIO edit dialog.
- Select the **Link Bonding Policy** you want to apply to your ACL.
- Navigate to the tab to the right, **Breakout Traffic to Internet & Cloud Services**.
- Select the pencil icon next to **Available Policies**.

The Services screen opens.

- For **Service Name**, enter a name for the first ZEN, such as **Primary_ZEN**.
- NOTE** This service references the traffic sent to the primary ZEN.
- Select **Add**.
- For **Service Name**, enter a name for the second ZEN, such as **Secondary_ZEN**.
- Select **Add**.
- Select **Save**.

The two services display in the **Available Policies** section.

- Drag the services to the **Preferred Policy Order** section.
- In the **Preferred Policy Order** section, move the primary ZEN service above the secondary ZEN service.

NOTE By moving the primary ZEN to the top of the list, traffic is automatically forwarded to the primary ZEN.

- Select **OK**. Your changes are highlighted in the BIO table, but have not been applied.
- Select **Save and Apply changes to Overlay**.

You configured a business intent overlay that points to the IPsec VPN tunnels.



Configure IPsec Tunnels

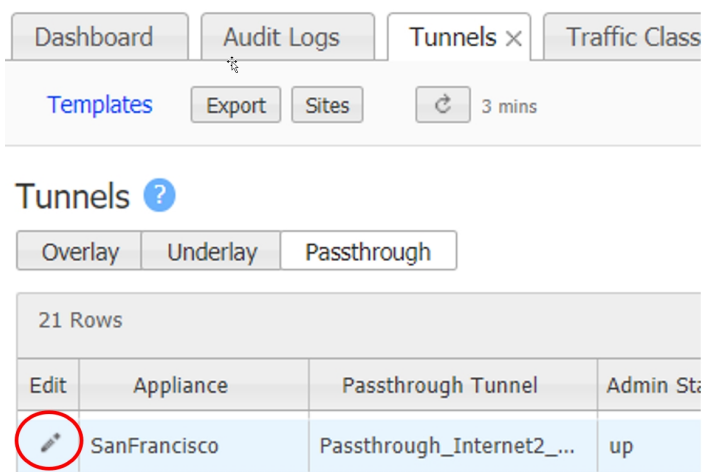
Follow the steps below to configure IPsec tunnels. You will need to create an IPsec VPN tunnel to the primary Zscaler Endpoint Node (ZEN) and an IPsec VPN tunnel to the secondary ZEN.

Create Tunnel to Primary ZEN

1. Sign in to Orchestrator.
2. From the home screen, select **Configuration > Networking > Tunnels > Tunnels**.

The Tunnels screen opens.

3. Click the pencil icon to edit the tunnel.



4. Select the **Passthrough** tab, then select **Add Tunnel**.

The Add Passthrough Tunnel screen opens.

5. Select the **General** tab.
6. Fill in the following fields.

General	Task
Alias	Enter a name for the tunnel.
Mode	Select IPsec .
Admin	Select up .
Local IP	Enter the EdgeConnect internet WAN interface IP address.
Remote IP	Enter the ZEN IP address that you discovered using an nslookup command.



NAT	Keep the default option, none . NAT is always none because no source NAT is performed. Zscaler inspects the private branch addresses. If the source NAT is used, all the source addresses have the EdgeConnect's WAN interface IP address. This isn't useful when performing advanced security inspection.
Peer/Service	Enter the service name that you assigned to you tunnel on the BIO screen.
Auto Max BW Enabled	Select the check box.
Max BW Kbps	Leave this field blank.

- Select the **IKE** tab.
- Fill in the following fields for IKE.

IKE	Task
Preshared Key	Enter the same pre-shared key that you entered when creating the VPN credential on the Zscaler website.
Authentication Algorithm	Select SHA1 .
Encryption Algorithm	Select auto .
Diffie-Hellman Group	Select 2 .
Rekey Interval/Lifetime	Enter 480 .
Dead Peer Detection	Delay time: the amount of time, in seconds, to wait for traffic from the destination IKE peer. This should be set to 300 . Retry Count: the number of times to retry the connection before determining that the connection is dead. This should be set to 3 . NOTE: Dead Peer Detection is only supported on EdgeConnect appliances running VXOA software version 8.2.1 and higher.
IKE Identifier	From the list, select FQDN . Select USER_FQDN as the IKE identifier.
Phase 1 Mode	Select Aggressive as the phase 1 mode.
IKE Version	Select IKEv1.

TIP Make sure the algorithms and pre-shared key match the ones in Zscaler Internet Access.

- Select the **IPsec** tab.



10. Fill in the following fields.

IPsec	Task
Authentication Algorithm	Select SHA1 .
Encryption Algorithm	Select NULL . For the IPsec tunnels, use null encryption because internet bound traffic is encrypted by the applications themselves using HTTPS protocol. This removes an extra layer of encryption using IPsec null encryption. You can set the IKE encryption to the default auto selection.
Enable IPsec Anti-Replay Window	Select the check box.
Rekey Interval/Lifetime	In the Mins field, enter 60 . In the Megabytes field, enter 0 .
Perfect Forward Secrecy Group	Select disable .

On the Tunnels screen, the IPsec tunnel to the primary ZEN displays.

11. Select **Save**.

You created an IPsec VPN tunnel to the primary ZEN.

Create Tunnel to Secondary ZEN

1. Select the **Passthrough** tab.
2. Select **Add Tunnels**.
3. Create the tunnel to the secondary ZEN by entering the same values that you used for the first tunnel. However, make sure the public IP address and service name of the secondary ZEN are different from the ones you used for the primary ZEN.

Tunnels ?

Overlay Underlay Passthrough

3 Rows Search

Edit	Applican...	Passthrough Tunnel	Admin...	Status	Local IP	Remote IP	Mode	NAT	Peer/Service	Max BW Kbps	Advance...	...
✓	SanFra...	Passthrough_Internet1_Bus...	up	up - active	10.4.139.20		No Encap	none	Overlay_Busines...	25000(Auto)		⌵
✓	SanFra...	Active_tun_to_Primary_ZEN	up	up - active	10.4.139.20	199.168.148.132	IPsec	none	Primary_ZEN	25000(Auto)		⌵
✓	SanFra...	Backup_tun_to_Secondary_...	up	up - active	10.4.139.20	104.129.194.39	IPsec	none	Backup_ZEN	25000(Auto)		⌵



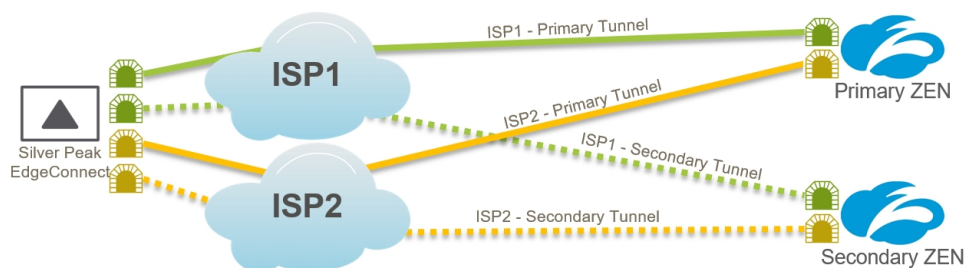
Verify Client Traffic is Sent to ZIA

1. In your web browser address bar, enter <http://ip.zscaler.com/>.
2. Use the Zscaler Internet Access test page to verify access to the ZIA.

Internet Breakout with Two ISPs

When an EdgeConnect appliance has access to the Internet using two internet service providers, **ISP1** and **ISP2**, the appliance can create four IPsec VPN tunnels to the primary and secondary ZENs as shown in the following figure. Only the primary tunnels from both **ISP1** and **ISP2** carry the traffic to the primary ZEN.

When you create the IPsec tunnels on the Business Intent Overlay screen, you allow the EdgeConnect appliance to load balance traffic to the primary ZEN using **ISP1** and **ISP2** by providing the same service name for the primary tunnels from both ISPs. This is a “flow-based” load balancing mechanism. The IPsec tunnel’s dead peer detection is used to monitor the health of the primary tunnels. If one of the primary tunnels becomes inactive, Orchestrator sends the new sessions from the client devices in your LAN to the Zscaler Cloud Security Service using the remaining primary tunnel.



Failure Scenarios

The following is a table of failure scenarios that can be secured using an EdgeConnect appliance.

ZEN Availability	ISP Availability	Outcome
Primary ZEN is unavailable. Secondary ZEN is available.	Both ISPs are available.	ISP1-Primary-Tunnel and ISP2-Primary-Tunnel goes down. New sessions from the clients are moved to the secondary ZEN using ISP1-Secondary-Tunnel and ISP2-Secondary-Tunnel.
Primary ZEN is available. Secondary ZEN is available.	ISP1 is unavailable. ISP2 is available.	ISP1-Primary-Tunnel and ISP1-Secondary-Tunnel goes down. New sessions from the clients are served by the remaining ISP2-Primary-Tunnel.
Primary ZEN is available. Secondary ZEN is unavailable.	Both ISPs are available.	No action is performed. The client traffic flows as usual to the primary ZEN from ISP1-Primary-Tunnel and ISP2-Primary-Tunnel.
Primary ZEN is available. Secondary ZEN is available.	ISP1 is available. ISP2 is unavailable.	ISP2-Primary-Tunnel and ISP2-Secondary-Tunnel goes down. New sessions from the clients are served by the remaining ISP1-Primary-Tunnel.
Both ZENs are unavailable	Both ISPs are available.	Traffic follows the sequence of the preferred policy order configured on the Business Intent Overlay screen on Orchestrator. If local breakout is listed as one of the policies, traffic is forwarded directly to the internet by passing the ZEN.



Configure Two Locations in Zscaler Cloud Service

Follow the steps to configure the locations.

Give the Zscaler support team the EdgeConnect appliance's static public IP addresses for **ISP2**. This allows the Zscaler Cloud Security Service to initiate the IPsec tunnel to the appliance's **ISP2** public IP address from Zscaler.

Refer to [setting up the location in the Zscaler website](#) to create a new location for **ISP2**, and link it to your existing VPN Credential. After you create the new location, it appears as below.

Locations

The screenshot shows the Zscaler Locations management interface. At the top, there are tabs for 'LOCATIONS (6)' and 'LOCATION GROUPS (0)'. Below the tabs is a toolbar with various actions: 'Add ...', 'Impo...', 'Dow...', 'Sam...', and 'Enter...'. There is also a search bar and a 'Search...' label. The main content is a table with the following columns: No., Name, IP Address..., X-..., Authe..., SSL, Firew..., Band..., Virtual Z..., Group, and a final column with three dots. The table contains two rows: '1' with 'ISP-1' and '2' with 'ISP-2'. Each row has a blue pencil icon and a blue link icon in the final column.

No.	Name	IP Address...	X-...	Authe...	SSL	Firew...	Band...	Virtual Z...	Group	
1	ISP-1	...	---	---	---	---	---	---	---	
2	ISP-2	...	---	---	---	---	---	---	---	



Configure Business Intent Overlay Policies

Before creating the IPsec tunnels from the EdgeConnect appliance to the primary and secondary ZENs using **ISP1** and **ISP2**, create a business intent overlay (BIO) on the Orchestrator system that points to the IPsec tunnels. Using access control lists (ACL), specify the applications that you forward to Zscaler on the BIO screen.

TIP Before creating a BIO, create ACLs on the **Configuration > Template** screen and apply them on the EdgeConnect appliance.

NOTE Refer to the BIO and ACL online help for more information.

1. From the Orchestrator home screen, select **Configuration > Business Intent Overlays**.

The **Business Intent Overlays** tab opens.

Priority	Overlay	Topology	Hubs	Primary Interfaces	Backup Interfaces	QoS & Security	Policy Order	Primary Interfaces	Backup Interfaces
1	RealTime Match Traffic Overlay ACL	Mesh		MPLS1 INET2 INET1 MPLS2	LTE If Pri & Sec Down	High Availability Waterfall: Overall Quality	1 Zscaler Cloud 2 Check Point Clou... 3 Break out 4 Backhaul	INET2 INET1	LTE
2	CriticalApps Match Traffic Overlay ACL	Mesh		INET2 INET1 MPLS1 MPLS2	LTE If Pri & Sec Down	High Quality Waterfall: Overall Quality	1 Break out 2 Backhaul	INET2 INET1	LTE
3	BulkApps Match Traffic Overlay ACL	Mesh		INET2 INET1 MPLS1 MPLS2	LTE If Pri & Sec Down	High Quality Waterfall: Overall Quality	1 Break out 2 Backhaul	INET2 INET1	LTE
4	DefaultOverlay Match Traffic Overlay ACL	Mesh		INET2 INET1 MPLS1 MPLS2	LTE If Pri & Sec Down	High Quality Waterfall: Overall Quality	1 Break out 2 Backhaul	INET2 INET1	LTE
5	voice Match Traffic lan	Mesh		MPLS1		High Quality Waterfall: Overall Quality	1 Check Point Clou 2 Backhaul	Waterfall: Auto	

NOTE In this example, the BIO references a **CriticalApps** ACL that already exists on the EdgeConnect appliance.

2. Click any cell in the **SD-WAN Traffic to Internal Subnets** column. This opens the BIO edit dialog.
3. Select the **Link Bonding Policy** you want to apply to your ACL.
4. Navigate to the tab to the right, **Breakout Traffic to Internet & Cloud Services**.
5. Select the pencil icon next to **Available Policies**.

The Services screen opens.

6. For **Service Name**, enter a name for the first ZEN, such as **Primary_ZEN**.

NOTE This service references the traffic sent to the primary ZEN.



7. Select **Add**.
8. For **Service Name**, enter a name for the second ZEN, such as **Secondary_ZEN**.
9. Select **Add**.
10. Select **Save**.

The two services should display in the **Available Policies** section.

11. Drag the services to the **Preferred Policy Order** section.
12. In the **Preferred Policy Order** section, move the primary ZEN service above the secondary ZEN service.

NOTE By moving the primary ZEN to the top of the list, traffic is automatically forwarded to the primary ZEN.

13. Select **OK**. Your changes are highlighted in the BIO table, but have not been applied.
14. Select **Save and Apply changes to Overlay**.

You configured a business intent overlay that points to the IPsec VPN tunnels.



Configure IPsec Tunnels

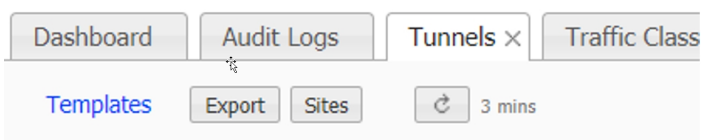
Follow the steps to configure IPsec tunnels. You will create IPsec VPN tunnels to the primary Zscaler Endpoint Node (ZEN) and secondary ZEN.

Create Tunnel to Primary ZEN

1. Sign in to Orchestrator.
2. From the home screen, select **Configuration > Networking > Tunnels > Tunnels**.


The Tunnels screen opens.

3. Click the pencil icon to edit the tunnel.



Tunnels ?



21 Rows			
Edit	Appliance	Passthrough Tunnel	Admin Sta
	SanFrancisco	Passthrough_Internet2_...	up

4. Select the **Passthrough** tab, then select **Add Tunnel**.

The **Add Passthrough Tunnel** screen opens.

Tunnels - SanFrancisco

Tunnels ?

Use shared subnet information



21 Rows, 1 Selected

5. Select the **General** tab.



6. Fill in the following fields.

General	Task
Alias	Enter a name for the tunnel.
Mode	Select IPsec .
Admin	Select up .
Local IP	Enter the EdgeConnect internet WAN interface IP address.
Remote IP	Enter the ZEN IP address that you discovered using an nslookup command.
NAT	Keep the default option, none . NAT is always none because no source NAT is performed. Zscaler inspects the private branch addresses. If the source NAT is used, all the source addresses have the EdgeConnect's WAN interface IP address. This isn't useful when performing advanced security inspection.
Peer/Service	Enter the service name that you assigned to you tunnel on the BIO screen.
Auto Max BW Enabled	Select the check box.
Max BW Kbps	Leave this field blank.

7. Select the **IKE** tab.

8. Fill in the following fields for IKEv2.

IKE	Task
Preshared Key	Enter the same preshared key that you entered when creating the VPN credential on the Zscaler website.
Authentication Algorithm	Select SHA1 .
Encryption Algorithm	Select auto .
Diffie-Hellman Group	Select 2 .
Rekey Interval/Lifetime	Enter 480 .
Dead Peer Detection	Delay time: the amount of time, in seconds, to wait for traffic from the destination IKE peer. This should be set to 300 . Retry Count: the number of times to retry the connection before determining that the connection is dead. This should be set to 3 . NOTE: Dead Peer Detection is only supported on EdgeConnect appliances running VXOA software version 8.2.1 and higher.



IKE IdentifierFrom the list, select **FQDN**.Select **USER_FQDN** as the IKE identifier.**Phase 1 Mode**Select **Aggressive** as the phase 1 mode.**IKE Version**

Select IKEv1.

TIP Make sure the algorithms and pre-shared key match the ones in Zscaler Internet Access.

9. Select the **IPsec** tab.
10. Fill in the following fields.

IPsec	Task
Authentication Algorithm	Select SHA1 .
Encryption Algorithm	Select NULL .
	For the IPsec tunnels, use null encryption because internet bound traffic is encrypted by the applications themselves using HTTPS protocol. This removes an extra layer of encryption using IPsec null encryption. You can set the IKE encryption to the default auto selection.
Enable IPsec Anti-Replay Window	Select the check box.
Rekey Interval/Lifetime	In the Mins field, enter 60 .
	In the Megabytes field, enter 0 .
Perfect Forward Secrecy Group	Select disable .

11. Select **Save**.

On the **Tunnels** screen, the IPsec tunnel to the primary ZEN displays.

Create Remaining Tunnels

1. Select the **Passthrough** tab.
2. Select **Add Tunnels**.
3. Create the remaining IPsec VPN tunnels by entering the same values that you used for the first tunnel. However, make sure the public IP addresses and service names are different from the ones you used for the primary ZEN.



Tunnels ?

Overlay Underlay Passthrough

4/6 Rows											Search <input type="text" value="ISP"/>	
Edit	Appli...	Passthrough Tunnel ▲	Admin Sta...	Status	Local IP	Remote IP	Mode	NAT	Peer/Service	Max BW Kbps	Adva...	...
	SanF...	ISP1_Active_Primary_ZEN	up	up - active	10.4.139.20	199.168.148.132	IPSec	none	Primary_ZEN	25000(Auto)		✓
	SanF...	ISP1_Backup_Secondary_Z...	up	up - active	10.4.139.20	104.129.194.39	IPSec	none	Backup_ZEN	25000(Auto)		✓
	SanF...	ISP2_Active_Primary_ZEN	up	up - active	10.4.141.20	199.168.148.132	IPSec	none	Primary_ZEN	25000(Auto)		✓
	SanF...	ISP2_Backup_Secondary_Z...	up	up - active	10.4.141.20	104.129.194.39	IPSec	none	Backup_ZEN	25000(Auto)		✓

NOTE Because of the preferred policy order, an EdgeConnect appliance does not need a separate IP SLA rule to handle the failure of an IPsec tunnel to a primary ZEN. If both IPsec tunnels to the primary ZEN are down, new sessions from the client devices are moved to the secondary ZEN by using the secondary tunnels on **ISP1** and **ISP2**.



Verify Client Traffic is Sent to ZIA

1. In your web browser address bar, enter <http://ip.zscaler.com/>.
2. Use the Zscaler Internet Access test page to verify access to the ZIA.

