Integrations: Integrate Netskope IPSec with Silver Peak EdgeConnect

null

About Netskope IPSec and Silver Peak EdgeConnect

The Netskope Security Cloud provides distributed enterprises with unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private applications from anywhere, on any device. Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed required to secure their digital transformation journeys.

Silver Peak and Netskope have tested and verified product interoperability between the Unity EdgeConnect™ SD-WAN edge and the Security Cloud platforms, enabling enterprises to use EdgeConnect to connect branch and remote office locations to the full range of Netskope cloud security applications and services delivered over Netskope NewEdge network infrastructure. Learn more at www.netskope.com. This guide focuses on using Netskope IPSec tunnels.

Silver Peak EdgeConnect Use Cases

Silver Peak supports two ways to configure and deploy an EdgeConnect appliance with Netskope.

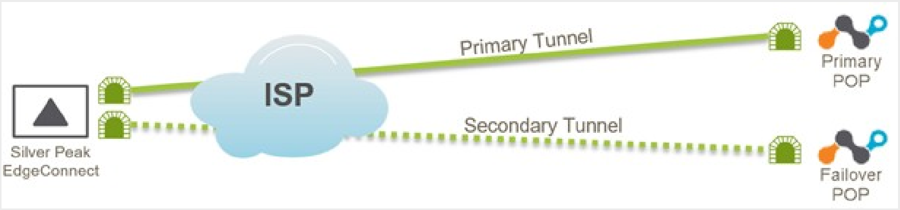
- Active - Backup Internet Breakout
- Active - Active Internet Breakout

Use Silver Peak Unity ECOS™ (ECOS) version 8.1.9.x or later and Silver Peak Unity Orchestrator version 8.8.5 or later.

Netskope Security Cloud accepts HTTP and HTTPS traffic on standard (80 and 443) or custom ports.

Active - Backup Internet Use Case

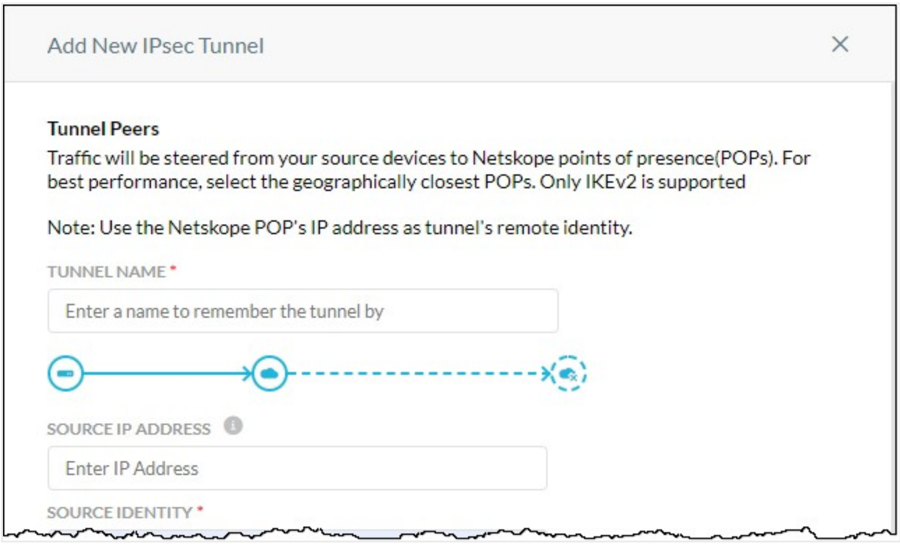
When an EdgeConnect appliance has access to the Internet using a single internet service provider (ISP), the appliance can create IPSec tunnels to a primary Netskope Point of Presence (POP) and a secondary Netskope POP, as shown in the following figure.



In this scenario, the tunnel to the primary POP carries all traffic unless the tunnel or POP become unavailable. In this case, traffic will automatically failover to the secondary POP.

Create a Tunnel on Netskope

1. Log in to your Netskope tenant.
2. On the Home page, click **Settings** in the bottom left.
3. Under Settings, click **Security Cloud Platform**.
4. Under Traffic Steering, click **IPSec**. The IPSec page lists all your configured IPSec tunnels.
5. Click **Add New Tunnel**. The Add New IPSec Tunnel page opens.



Add New IPsec Tunnel

Tunnel Peers

Traffic will be steered from your source devices to Netskope points of presence(POPs). For best performance, select the geographically closest POPs. Only IKEv2 is supported

Note: Use the Netskope POP's IP address as tunnel's remote identity.

TUNNEL NAME *

Enter a name to remember the tunnel by

SOURCE IP ADDRESS

Enter IP Address

SOURCE IDENTITY *

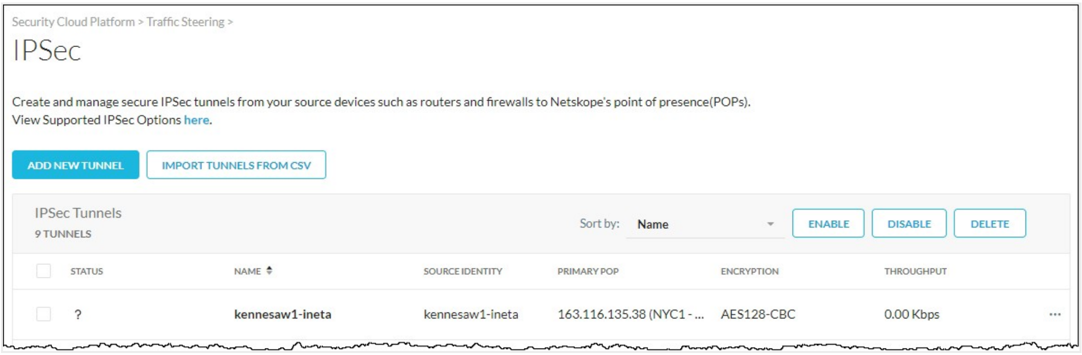
6. Enter or select the new tunnel parameters as follows:

Parameter	Description
Tunnel Name	Enter a descriptive name for the tunnel. For example, use some combination of the appliance name and interface name.
Source IP Address (optional)	The public IP address of the WAN interface on the EdgeConnect appliance that will originate the IPSec tunnel. In Unity Orchestrator, you can determine an interface’s public IP address on the Interfaces page (Configuration > Networking > Interfaces).
Source Identity	Enter a unique name that will identify the EdgeConnect source for this tunnel. You will use the source identity as the Local IKE Identifier when configuring the tunnel on the EdgeConnect appliance.

Parameter	Description
Primary Netskope POP	Select a primary Netskope POP that is geographically closest to the EdgeConnect appliance that will originate the tunnel.
Failover Netskope POP	Select a failover POP from the list of those available.
Pre-shared Key	Enter a complex pre-shared key that both sides of the tunnel will use to authenticate one another. You will need to use the same pre-shared key when configuring the tunnel on the EdgeConnect appliance.
Encryption Cipher	Select AES128-CBC or AES256-CBC for encrypting the connection.
Maximum Bandwidth	Select the maximum bandwidth to allow on the tunnel.

7. When the tunnel configuration is complete, click **Add**.

   You should see the new tunnel displayed on the Netskope IPSec page.



Create and manage secure IPSec tunnels from your source devices such as routers and firewalls to Netskope's point of presence(POPs).
View Supported IPSec Options here.

IPSec Tunnels
9 TUNNELS

	STATUS	NAME	SOURCE IDENTITY	PRIMARY POP	ENCRYPTION	THROUGHPUT	
□	?	kennesaw1-ineta	kennesaw1-ineta	163.116.135.38 (NYC1 - ...	AES128-CBC	0.00 Kbps	···

Configure Tunnels on EdgeConnect

Follow the steps below to configure IPsec tunnels. You will need to create an IPsec VPN tunnel to the primary POP and an IPsec VPN tunnel to the failover POP.

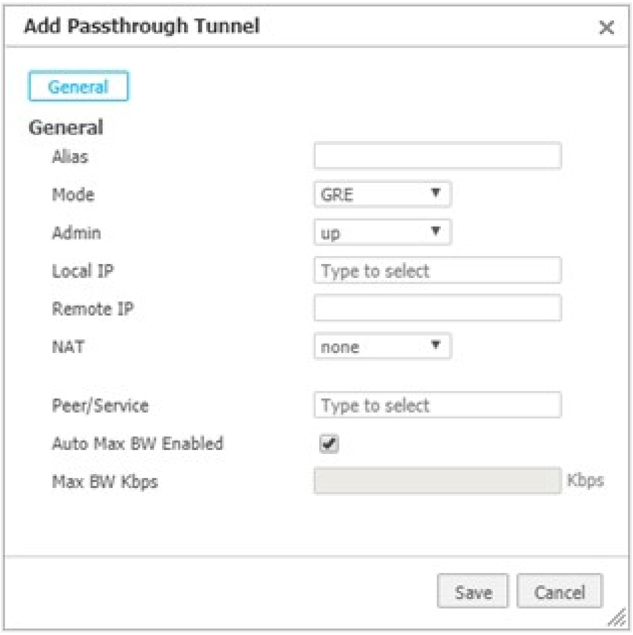
Create a Tunnel to a Primary POP

1. Log in to Silver Peak Unity Orchestrator.
2. In the device tree on the left, select the EdgeConnect appliance where you want to configure the tunnel to Netskope.
3. Open the Tunnels tab (click Configuration > Networking > Tunnels > Tunnels).

4. Click the edit icon ✎ on the left of any row in the table.

5. On the tunnels detail page, click **Passthrough** at the top of the table, and then click **Add Tunnel**.

   The Add Passthrough Tunnel dialog opens.



Add Passthrough Tunnel ×

General

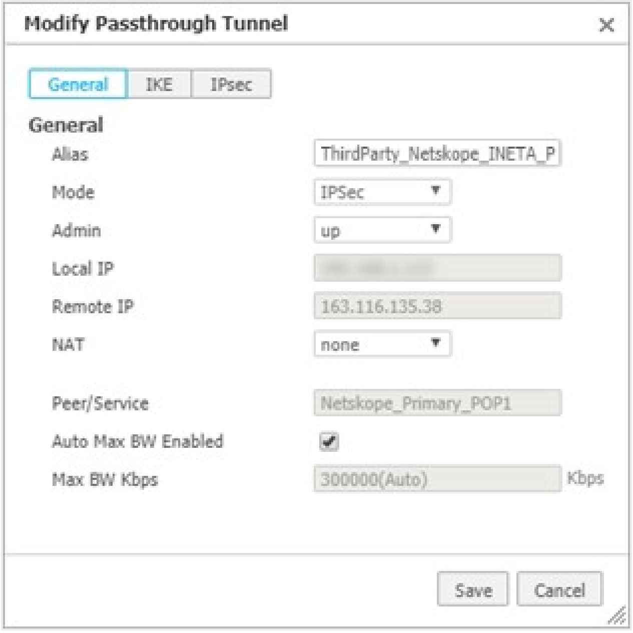
General

Alias	
Mode	GRE ▾
Admin	up ▾
Local IP	Type to select
Remote IP	
NAT	none ▾
Peer/Service	Type to select
Auto Max BW Enabled	☑
Max BW Kbps	Kbps

6. Enter or select the new tunnel parameters as follows:

Parameter	Description
Alias	Enter a descriptive name for the tunnel.
Mode	Select **IPSec**.
Admin	The administrative state of the tunnel. You can leave this at the default value of **up**.
Local IP	The IP address of the WAN interface that will originate the IPSec tunnel. Click into this field and select the IP address from those available.
Remote IP	Enter the IP address of the primary Netskope POP that you configured in Netskope.
NAT	This should be set to **none**.
Peer/Service	Enter the name of a new service that will use this tunnel. You will use this service for configuring breakout to Netskope under Business Intent Overlays.
Auto Max BW Enabled	Leave this checkbox selected to let the appliance auto-negotiate the maximum tunnel bandwidth.

Parameter	Description
Max BW Kbps	This field is not available when auto bandwidth is enabled.



Modify Passthrough Tunnel

General

Alias: ThirdParty_Netskope_INETA_P

Mode: IPSec

Admin: up

Local IP: [redacted]

Remote IP: 163.116.135.38

NAT: none

Peer/Service: Netskope_Primary_POP1

Auto Max BW Enabled: ☑

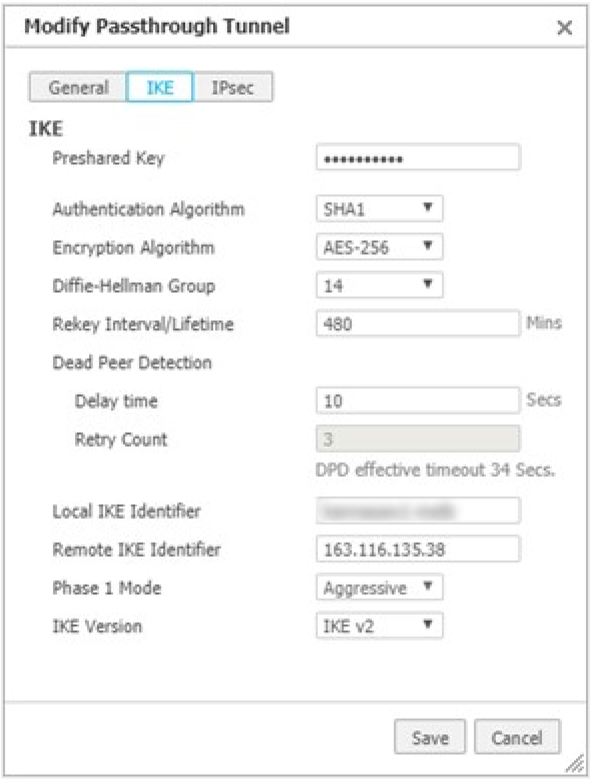
Max BW Kbps: 300000(Auto) Kbps

7. Click **IKE** in the Add Passthrough Tunnel dialog.

8. Enter or select the new tunnel parameters as follows:

   Set the IKE Version to IKE v2 first at the bottom because this will change some of the other fields availability.

Parameter	Description
IKE Version	Set to **IKE v2**.
Preshared Key	Enter the same preshared key that you created on Netskope.
Authentication Algorithm	Select **SHA1**.
Encryption Algorithm	Select the same algorithm as on Netskope (AES-128 or AES-256).
Diffie-Hellman Group	Select **14**.
Rekey Interval/Lifetime	Leave the default value of **480**.
Dead Peer Detection	Leave the delay time at its default value, and retry count cannot be changed.
Local IKE Identifier	Enter the Source Identity that you assigned to the tunnel on Netskope.
Remote IKE Identifier	Enter the IP address of the primary Netskope POP that you configured in Netskope.
Phase 1 Mode	This value cannot be changed.



Modify Passthrough Tunnel

IKE

Preshared Key: ••••••••••

Authentication Algorithm: SHA1

Encryption Algorithm: AES-256

Diffie-Hellman Group: 14

Rekey Interval/Lifetime: 480 Mins

Dead Peer Detection

Delay time: 10 Secs

Retry Count: 3

DPD effective timeout 34 Secs.

Local IKE Identifier: [redacted]

Remote IKE Identifier: 163.116.135.38

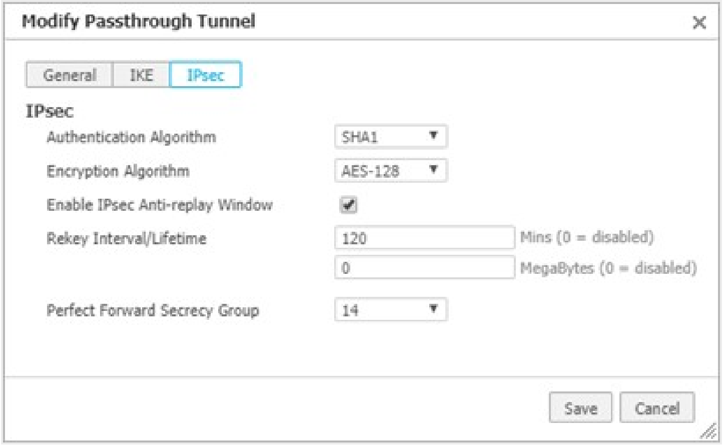
Phase 1 Mode: Aggressive

IKE Version: IKE v2

9. Click the **IPsec** button at the top of the Add Passthrough Tunnel dialog.

10. Enter or select the new tunnel parameters as follows:

Parameter	Description
Authentication Algorithm	Select **SHA1**.
Encryption Algorithm	Select **AES-128**.
Enable IPsec Anti-Replay Window	Leave this checkbox selected.
Rekey Interval/Lifetime	You can leave these values at their defaults.
Perfect Forward Secrecy Group	This can be left at the default value of **14**.



Modify Passthrough Tunnel

IPsec

Authentication Algorithm: SHA1

Encryption Algorithm: AES-128

Enable IPsec Anti-replay Window: ☑

Rekey Interval/Lifetime: 120 Mins (0 = disabled)

0 MegaBytes (0 = disabled)

Perfect Forward Secrecy Group: 14

11. When the settings for General, IKE, and IPSec are complete. Click **Save** to create the new tunnel.

Create a Tunnel to a Failover POP

1. Click **Add Tunnel** to create a second tunnel to the failover POP.
2. Use the same values that you used for the first tunnel except for the following:

   - Alias: Use a different name for the second Silver Peak tunnel.
   - Remote IP: Enter the IP address of the failover POP that you configured in Netskope.
   - Peer/Service: Create a new service name that will direct traffic to the failover POP.
   - Remote IKE Identifier: Use the IP address of the failover POP.

Configure Business Intent Overlay Policies

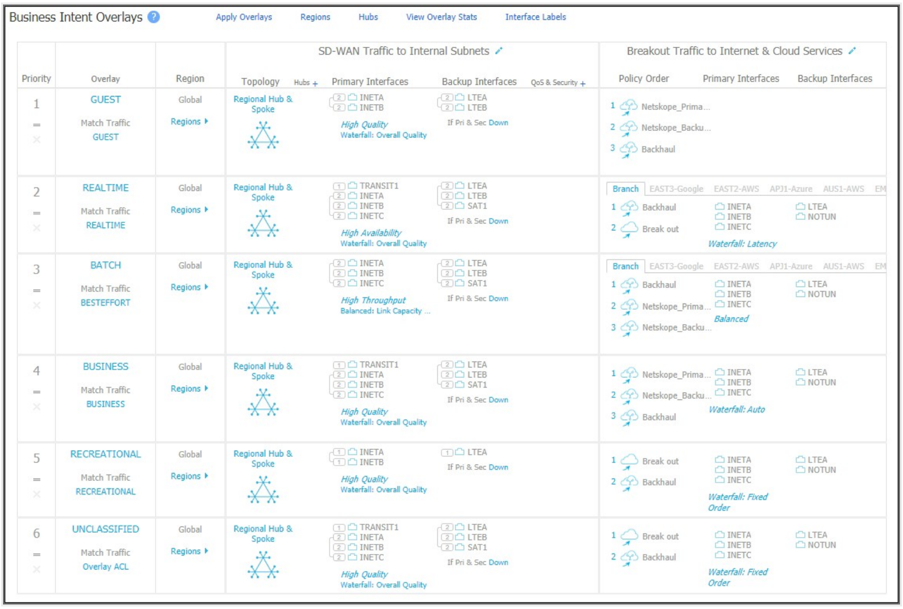
Complete the following steps to configure BIO policies to associate with Netskope.

After creating the IPsec tunnels from the EdgeConnect appliance to the primary and failover POPs, create a business intent overlay (BIO) that points to those IPsec tunnels. Using access control lists (ACL), specify the applications that you want to forward to Netskope on the BIO screen.

Before creating a BIO, create ACLs on the **Configuration** > **Template** screen and apply them on the EdgeConnect appliance. Refer to the BIO and ACL online help for more information.

1. On 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

			SD-WAN Traffic to Internal Subnets			Breakout Traffic to Internet & Cloud Services		
Priority	Overlay	Region	Topology Hubs +	Primary Interfaces	Backup Interfaces QoS & Security +	Policy Order	Primary Interfaces	Backup Interfaces
1	GUEST Match Traffic GUEST	Global Regions ▸	Regional Hub & Spoke	2 INETA 2 INETB *High Quality* Waterfall: Overall Quality	2 LTEA 2 LTEB If Pri & Sec Down	1 Netskope_Prima... 2 Netskope_Backu... 3 Backhaul		
2	REALTIME Match Traffic REALTIME	Global Regions ▸	Regional Hub & Spoke	1 TRANSIT1 2 INETA 2 INETB 2 INETC *High Availability* Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch EAST3-Google EAST2-AWS APJ1-Azure AUS1-AWS EM 1 Backhaul 2 Break out	INETA INETB INETC *Waterfall: Latency*	LTEA NOTUN
3	BATCH Match Traffic BESTEFFORT	Global Regions ▸	Regional Hub & Spoke	2 INETA 2 INETB 2 INETC *High Throughput* Balanced: Link Capacity ...	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch EAST3-Google EAST2-AWS APJ1-Azure AUS1-AWS EM 1 Backhaul 2 Netskope_Prima... 3 Netskope_Backu...	INETA INETB INETC *Balanced*	LTEA NOTUN
4	BUSINESS Match Traffic BUSINESS	Global Regions ▸	Regional Hub & Spoke	1 TRANSIT1 2 INETA 2 INETB 2 INETC *High Quality* Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	1 Netskope_Prima... 2 Netskope_Backu... 3 Backhaul	INETA INETB INETC *Waterfall: Auto*	LTEA NOTUN
5	RECREATIONAL Match Traffic RECREATIONAL	Global Regions ▸	Regional Hub & Spoke	1 INETA 1 INETB *High Quality* Waterfall: Overall Quality	1 LTEA If Pri & Sec Down	1 Break out 2 Backhaul	INETA INETB INETC *Waterfall: Fixed Order*	LTEA NOTUN
6	UNCLASSIFIED Match Traffic Overlay ACL	Global Regions ▸	Regional Hub & Spoke	1 TRANSIT1 2 INETA 2 INETB 2 INETC *High Quality* Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	1 Break out 2 Backhaul	INETA INETB INETC *Waterfall: Fixed Order*	LTEA NOTUN

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. Go to the, **Breakout Traffic to Internet & Cloud Services** tab.
5. Select the pencil icon next to **Available Policies.** The Services screen opens.
6. For **Service Name**, select the name assigned to the primary POP. This service references the traffic sent to the primary POP.
7. Click **Add.**
8. For **Service Name**, select the name assigned to the failover POP.
9. Click **Add**, and then click **Save.** The two services will be listed in the **Available Policies** section.

10. Drag the services to the **Preferred Policy Order** section.

11. In the **Preferred Policy Order** section, move the primary POP service above the failover POP service. By moving the primary POP to the top of the list, traffic is automatically forwarded to the primary POP.

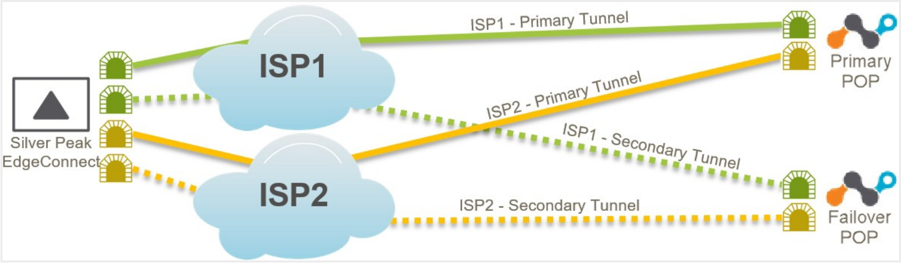
12. Click **OK**.

13. Click **Save** and **Apply changes to the Overlay**. You have now configured a business intent overlay that points to the new IPsec VPN tunnels.

Your changes will be highlighted in the BIO table, but they have not yet been applied.

Active - Active Internet Use Case

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 failover POPs as shown in the following figure. Only the primary tunnels from both **ISP1** and **ISP2** carry the traffic to the primary POP unless one of the primary tunnels or the primary POP is unavailable.



When you create the IPsec tunnels on the Business Intent Overlay screen, you allow the EdgeConnect appliance to load balance traffic to the primary POP using **ISP1** and **ISP2** by providing the same service name for the primary tunnels from both ISPs. This is a flow-based load balancing method.

Create a Second Tunnel on Netskope

1. Log in to the Netskope portal.

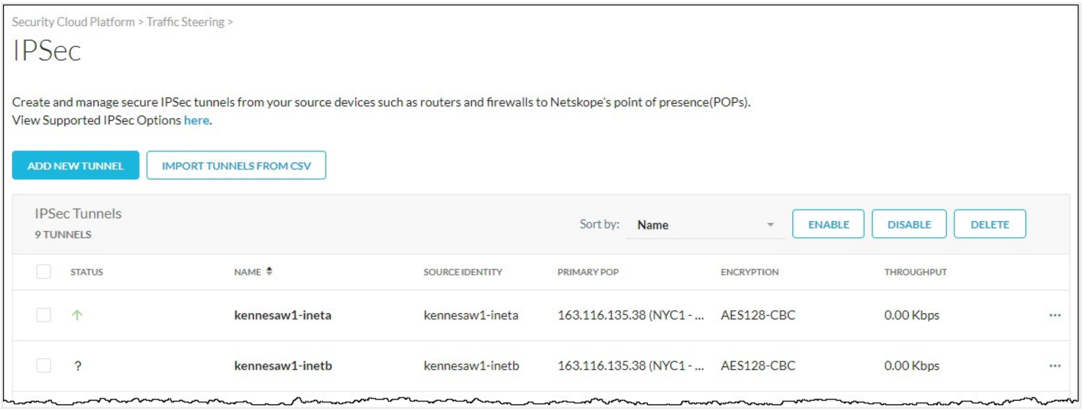
2. On the Home page, click **Settings** in the bottom left.

3. Under Settings, click **Security Cloud Platform**.
4. Under Traffic Steering, click **IPSec**. The IPSec page will list all your configured IPSec tunnels.
5. Click the **Add New Tunnel** button at the top of the page. The Add New IPSec Tunnel page opens.
6. Enter or select the new tunnel parameters as follows:

Parameter	Description
Tunnel Name	Enter a descriptive name for the tunnel. For example, use some combination of the appliance name and interface name.
Source IP Address	The public IP address of the WAN interface on the EdgeConnect appliance that will originate the IPSec tunnel. In Unity Orchestrator, you can determine an interface's public IP address on the Interfaces page (Configuration &gt; Networking &gt; Interfaces).
Source Identity	Enter a unique name that will identify the EdgeConnect source for this tunnel. Use the source identity as the Local IKE Identifier when configuring the tunnel on the EdgeConnect appliance.
Primary Netskope POP	Select the same primary Netskope POP that was used for the first tunnel.
Failover Netskope POP	Select the same failover POP that was used for the first tunnel.
Pre-shared Key	Enter a complex pre-shared key that both sides of the tunnel will use to authenticate one another. Use the same pre-shared key when configuring the tunnel on the EdgeConnect appliance.
Encryption Cipher	Select AES128-CBC or AES256-CBC for encrypting the connection.
Maximum Bandwidth	Select the maximum bandwidth to allow on the tunnel.

7. When the tunnel configuration is complete, click **Add**.

   You should see the new tunnel displayed on the Netskope IPSec page.



Security Cloud Platform > Traffic Steering >

IPSec

Create and manage secure IPSec tunnels from your source devices such as routers and firewalls to Netskope's point of presence(POPs).
View Supported IPSec Options here.

IPSec Tunnels
9 TUNNELS

Sort by: Name

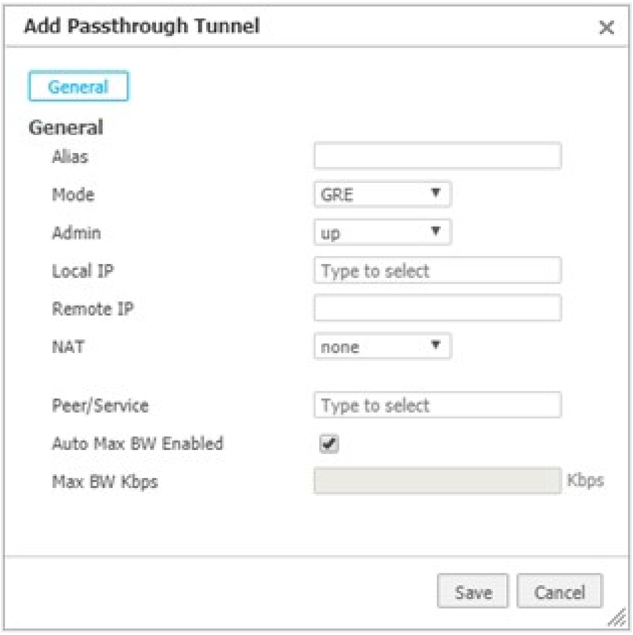
	STATUS	NAME	SOURCE IDENTITY	PRIMARY POP	ENCRYPTION	THROUGHPUT	
□	↑	kennesaw1-ineta	kennesaw1-ineta	163.116.135.38 (NYC1 - ...	AES128-CBC	0.00 Kbps	···
□	?	kennesaw1-inetb	kennesaw1-inetb	163.116.135.38 (NYC1 - ...	AES128-CBC	0.00 Kbps	···

Configure Additional Tunnels on EdgeConnect

To enable the active - active breakout scenario, you will create two additional IPSec tunnels to the same primary POP and the same failover POP from a secondary internet interface on your EdgeConnect appliance.

Create a Tunnel to a Primary POP

1. Log in to Silver Peak Unity Orchestrator.
2. In the device tree on the left, select the EdgeConnect appliance where you want to configure the tunnel to Netskope.
3. Open the Tunnels tab (click Configuration > Networking > Tunnels > Tunnels).
4. Click the edit icon to the left of any row in the table of tunnels.
5. On the tunnels detail page, click the **Passthrough** button at the top of the table, and then click the **Add Tunnel** button. The Add Passthrough Tunnel dialog appears.



Add Passthrough Tunnel

General

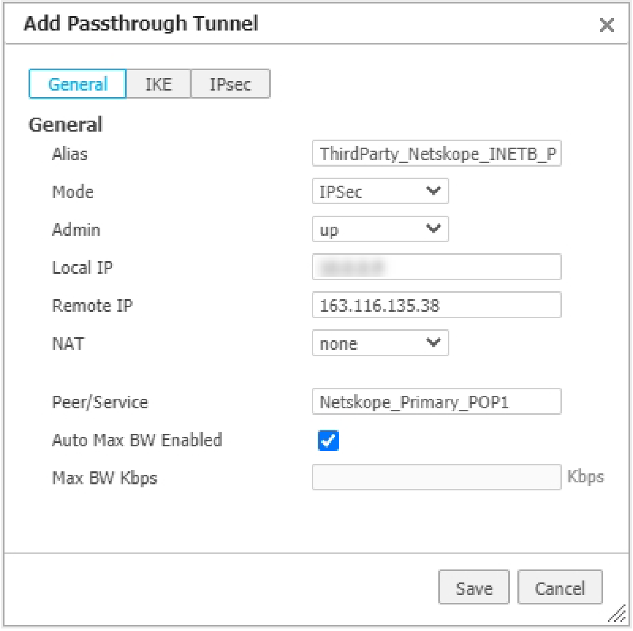
General

Alias	
Mode	GRE
Admin	up
Local IP	Type to select
Remote IP	
NAT	none
Peer/Service	Type to select
Auto Max BW Enabled	☑
Max BW Kbps	Kbps

6. Enter or select the new tunnel parameters as follows:

Parameter	Description
Alias	Enter a descriptive name for the tunnel.
Mode	Select **IPSec**.
Admin	The administrative state of the tunnel. You can leave this at the default value of **up**.
Local IP	The IP address of the WAN interface that will originate the IPSec tunnel. This should be the WAN interface associated with your second ISP.
Remote IP	Enter the IP address of the primary Netskope POP that you configured in Netskope.
NAT	This should be set to **none**.
Peer/Service	Enter the same service that was used for the first EdgeConnect tunnel.

Parameter	Description
Auto Max BW Enabled	Leave this checkbox selected to let the appliance auto-negotiate the maximum tunnel bandwidth.
Max BW Kbps	This field is not available when auto bandwidth is enabled.



Add Passthrough Tunnel ×

General

Alias	ThirdParty_Netskope_INETB_P
Mode	IPSec
Admin	up
Local IP	[redacted]
Remote IP	163.116.135.38
NAT	none
Peer/Service	Netskope_Primary_POP1
Auto Max BW Enabled	☑
Max BW Kbps	Kbps

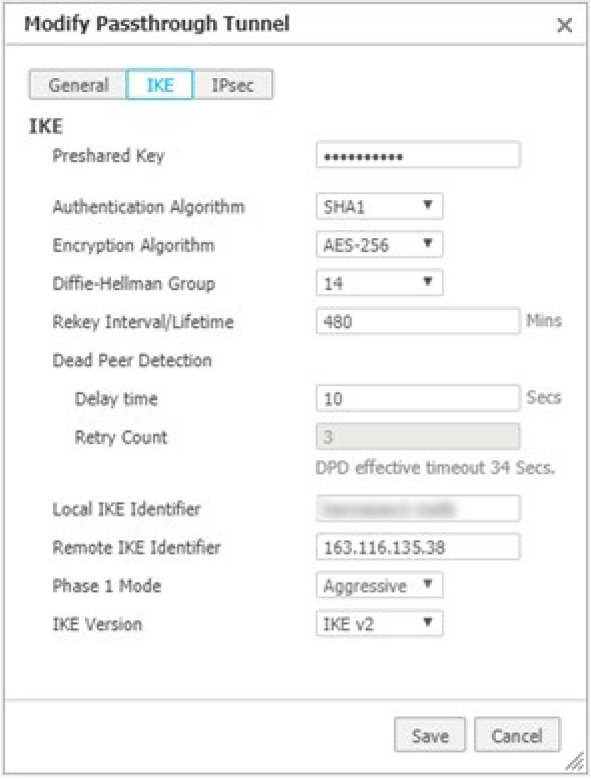
7. Click **IKE** in the Add Passthrough Tunnel dialog.

8. Enter or select the new tunnel parameters as follows:

   Set the IKE Version to IKE v2 first as it will change some of the other fields available.

Parameter	Description
IKE Version	Set this to **IKE v2**.
Preshared Key	Enter the same preshared key that you created on Netskope.
Authentication Algorithm	Select **SHA1**.
Encryption Algorithm	Select the same algorithm as on Netskope (AES-128 or AES-256).
Diffie-Hellman Group	Select **14**.
Rekey Interval/Lifetime	Leave this at the default value of**480**.
Dead Peer Detection	You can leave the delay time at its default value, and retry count cannot be changed.
Local IKE Identifier	Enter the Source Identity that you assigned to the second tunnel on Netskope.
Remote IKE Identifier	Enter the IP address of the primary Netskope POP that you configured in Netskope.

Parameter	Description
Phase 1 Mode	This value cannot be changed.



Modify Passthrough Tunnel

IKE

Preshared Key: ••••••••••

Authentication Algorithm: SHA1

Encryption Algorithm: AES-256

Diffie-Hellman Group: 14

Rekey Interval/Lifetime: 480 Mins

Dead Peer Detection

Delay time: 10 Secs

Retry Count: 3

DPD effective timeout 34 Secs.

Local IKE Identifier: [redacted]

Remote IKE Identifier: 163.116.135.38

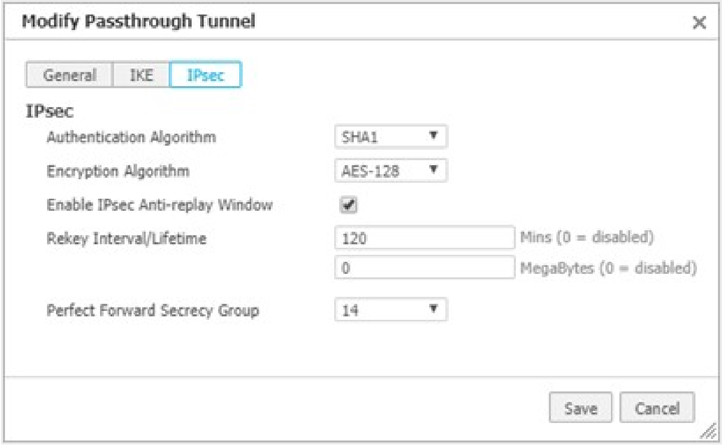
Phase 1 Mode: Aggressive

IKE Version: IKE v2

9. Click **IPSec** in the Add Passthrough Tunnel dialog.

10. Enter or select the new tunnel parameters as follows:

Parameter	Description
Authentication Algorithm	Select **SHA1**.
Encryption Algorithm	Select **AES-128**.
Enable IPsec Anti-Replay Window	Leave this checkbox selected.
Rekey Interval/Lifetime	You can leave these values at their defaults.
Perfect Forward Secrecy Group	This can be left at the default value of **14**.



Modify Passthrough Tunnel

IPsec

Authentication Algorithm: SHA1

Encryption Algorithm: AES-128

Enable IPsec Anti-replay Window: ☑

Rekey Interval/Lifetime: 120 Mins (0 = disabled)

0 MegaBytes (0 = disabled)

Perfect Forward Secrecy Group: 14

11. When the settings for General, IKE, and IPsec are complete, click **Save** to create the

new tunnel.

Create Tunnel to Failover POP

1. Click **Add Tunnel** to create a second tunnel to the failover POP.
2. Use the same values that you used for the first tunnel except for the following:
    - Alias: Use a different name for the second Silver Peak tunnel.
    - Remote IP: Enter the IP address of the failover POP that you configured in Netskope.
    - Peer/Service: Enter the same service name to direct traffic to the failover POP (same as the second EdgeConnect tunnel).
    - Remote IKE Identifier: Use the IP address of the failover POP.

After creating the IPsec tunnels from the EdgeConnect appliance to the primary and failover POPs using **ISP1** and **ISP2**, there are no additional changes to be made to the existing BIO. Proceed to, Configure Business Intent Overlay Policies if needed.

Configure Business Intent Overlay Policies

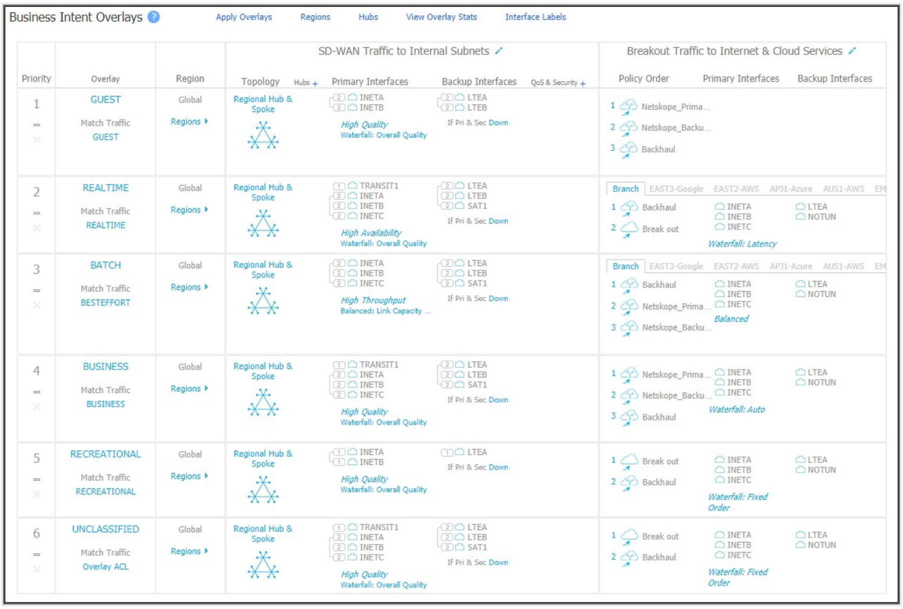
Complete the following steps to configure BIO policies to associate with Netskope.

After creating the IPsec tunnels from the EdgeConnect appliance to the primary and failover POPs, create a business intent overlay (BIO) that points to those IPsec tunnels. Using access control lists (ACL), specify the applications that you want to forward to Netskope on the BIO screen.

Before creating a BIO, create ACLs on the **Configuration** > **Template** screen and apply them on the EdgeConnect appliance. Refer to the BIO and ACL online help for more information.

1. On 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

			SD-WAN Traffic to Internal Subnets			Breakout Traffic to Internet & Cloud Services		
Priority	Overlay	Region	Topology Hubs +	Primary Interfaces	Backup Interfaces QoS & Security +	Policy Order	Primary Interfaces	Backup Interfaces
1	GUEST Match Traffic GUEST	Global Regions ▸	Regional Hub & Spoke	2 INETA 2 INETB *High Quality* Waterfall: Overall Quality	2 LTEA 2 LTEB If Pri & Sec Down	1 Netskope_Prima... 2 Netskope_Backu... 3 Backhaul		
2	REALTIME Match Traffic REALTIME	Global Regions ▸	Regional Hub & Spoke	1 TRANSIT1 2 INETA 2 INETB 2 INETC *High Availability* Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch EAST3-Google EAST2-AWS APJ1-Azure AUS1-AWS EM 1 Backhaul 2 Break out	INETA INETB INETC *Waterfall: Latency*	LTEA NOTUN
3	BATCH Match Traffic BESTEFFORT	Global Regions ▸	Regional Hub & Spoke	2 INETA 2 INETB 2 INETC *High Throughput* Balanced: Link Capacity ...	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch EAST3-Google EAST2-AWS APJ1-Azure AUS1-AWS EM 1 Backhaul 2 Netskope_Prima... 3 Netskope_Backu...	INETA INETB INETC *Balanced*	LTEA NOTUN
4	BUSINESS Match Traffic BUSINESS	Global Regions ▸	Regional Hub & Spoke	1 TRANSIT1 2 INETA 2 INETB 2 INETC *High Quality* Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	1 Netskope_Prima... 2 Netskope_Backu... 3 Backhaul	INETA INETB INETC *Waterfall: Auto*	LTEA NOTUN
5	RECREATIONAL Match Traffic RECREATIONAL	Global Regions ▸	Regional Hub & Spoke	1 INETA 1 INETB *High Quality* Waterfall: Overall Quality	1 LTEA If Pri & Sec Down	1 Break out 2 Backhaul	INETA INETB INETC *Waterfall: Fixed Order*	LTEA NOTUN
6	UNCLASSIFIED Match Traffic Overlay ACL	Global Regions ▸	Regional Hub & Spoke	1 TRANSIT1 2 INETA 2 INETB 2 INETC *High Quality* Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	1 Break out 2 Backhaul	INETA INETB INETC *Waterfall: Fixed Order*	LTEA NOTUN

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. Go to the, **Breakout Traffic to Internet & Cloud Services** tab.
5. Select the pencil icon next to **Available Policies**. The Services screen opens.
6. For **Service Name**, select the name assigned to the primary POP. This service references the traffic sent to the primary POP.
7. Click **Add**.
8. For **Service Name**, select the name assigned to the failover POP.
9. Click **Add**, and then click **Save**. The two services will be listed in the **Available Policies** section.
10. Drag the services to the **Preferred Policy Order** section.
11. In the **Preferred Policy Order** section, move the primary POP service above the

failover POP service. By moving the primary POP to the top of the list, traffic is automatically forwarded to the primary POP.

12. Click **OK**.

13. Click **Save** and **Apply changes to the Overlay**. You have now configured a business intent overlay that points to the new IPsec VPN tunnels.

Your changes will be highlighted in the BIO table, but they have not yet been applied.