



Hewlett Packard
Enterprise

HPE Aruba Networking SD-WAN and SSE solution by Microsoft: Branch Connectivity and IPSec Configuration

Integration Guide

Important Notice

© 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](#).

Revision A, February 2024

Open Source Code:

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



Contents

Contents	2
1 Overview	3
2 Prerequisites	3
3 EdgeConnect SD-WAN IPSec with SSE solution by Microsoft	4
4 Planning and Topologies.....	5
4.1 Branch with a Single Gateway - NO Zone Redundancy at SSE solution by Microsoft	5
4.2 Branch with a Single Gateway - With Zone Redundancy at SSE solution by Microsoft.....	6
4.3 Branch with HA Pair - Tunnels Over Directly Connected WAN - With Zone Redundancy at SSE solution by Microsoft	6
4.4 Branch with HA Pair - Tunnels Over Direct and Shared WAN - With Zone Redundancy at SSE solution by Microsoft	7
4.5 Branch with HA Pair - Tunnels Over Direct and Shared WAN - NO Zone Redundancy at SSE solution by Microsoft	7
5 Remote Network Configuration on Microsoft Entra Admin Center	8
6 Passthrough Tunnel Configuration on the EdgeConnect Gateway	11
6.1 Creating a Passthrough Tunnel.....	11
6.2 Tunnel Monitoring Using IP SLA Probes	13
7 Policy Based Traffic Redirection to the SSE solution by Microsoft.....	15
7.1 Verify the Flows on the EdgeConnect Gateway	19
8 Route Based Traffic Redirection to the SSE solution by Microsoft.....	20
8.1 Add Loopback Interfaces.....	22
8.2 Add VTI Interfaces.....	23
8.3 Add a Static Route to Reach the BGP Peer Via VTI.....	25
8.4 Create BGP Neighborhood	27
8.5 Enable the “Consider Non-default routes as internal subnets” Option.....	29
8.6 Change the Business Internet Overlay to Use Best Route	29
8.7 Configure Active-Active or Active-Backup Load Balancing.....	30
8.8 Verify Traffic flows on the EdgeConnect Gateway.....	31



1 Overview

This document details the configurations required on the HPE Aruba Networking Orchestrator and Microsoft Entra admin center to provision IPSec tunnels between an EdgeConnect SD-WAN gateway and the Security Service Edge (SSE) solution by Microsoft, which includes [Microsoft Entra Internet Access](#) and [Microsoft Entra Private Access](#) products. [Global Secure Access \(preview\)](#) is the unified location in the [Microsoft Entra admin center](#) where you can configure these two products.

For the remainder of this document, the reader shall assume that "SSE" refers to the SSE solution by Microsoft and that "SD-WAN" refers to the EdgeConnect solution by HPE Aruba Networking.

2 Prerequisites

1. Access to an HPE Aruba Networking Orchestrator to configure IPSec and routing configurations.
2. An operational EdgeConnect SD-WAN gateway (virtual or hardware).
3. Access to Microsoft Entra admin center > Global Secure Access.
4. The WAN IP addresses of the EdgeConnect SD-WAN gateway.

NOTE: This documentation is based on ECOS release 9.4 and Orchestrator OS release 9.4. This integration with the SSE solution by Microsoft is supported on earlier ECOS and Orchestrator versions, but some of the IKE/IPSec parameters may not be supported in older versions.



3 EdgeConnect SD-WAN IPsec with SSE solution by Microsoft

This document uses the topology shown in *Figure 1 EdgeConnect SDWAN Gateway – Single Gateway Topology* to demonstrate how an EdgeConnect SD-WAN gateway is establishing a site-to-site IPsec connection with the SSE gateway by Microsoft. The **SSE gateway** is Microsoft's endpoint with which the HPE EdgeConnect gateway sets up IPsec tunnel. Configuration details also include traffic redirection from the EdgeConnect gateway to SSE gateways by Microsoft using either policy based routing or BGP routing.

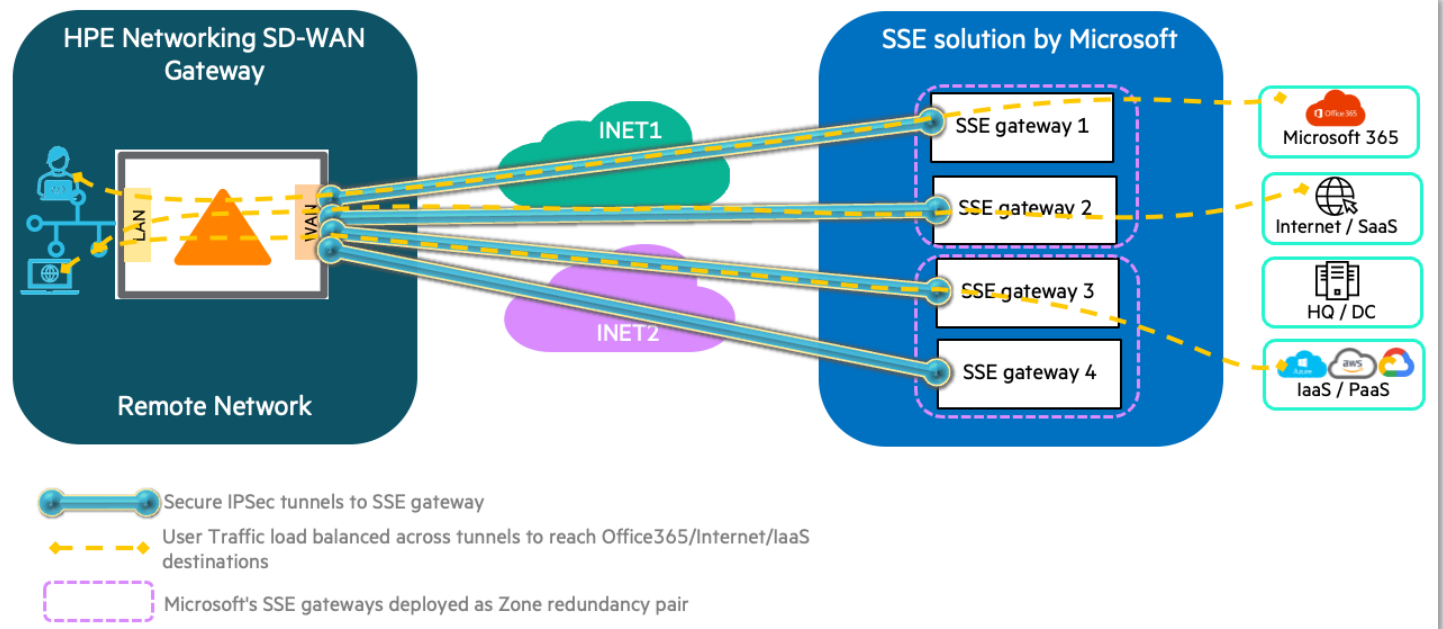


Figure 1: EdgeConnect SDWAN Gateway – Single Gateway Topology

The topology above depicts a deployment of a remote site (or branch or location) with a single EdgeConnect gateway and two WAN services (INET1 and INET2). EdgeConnect can be configured to load balance traffic on both the WAN underlays or to use one of the WAN underlays as a primary and the other as a backup.

To configure an IPsec connection between an EdgeConnect SD-WAN gateway and SSE gateways, you must complete the following tasks:

High-Level Configuration Tasks on Microsoft Entra Admin Center

- Complete remote network configuration on the Microsoft Entra admin center.

High-Level Configuration Tasks on HPE Aruba Networking Orchestrator

- Passthrough tunnel configuration (IPsec tunnel).
- Traffic redirection to the SSE gateways.
 - a. Policy based (BIO policy configuration)

OR

 - b. Route based (BGP configuration)



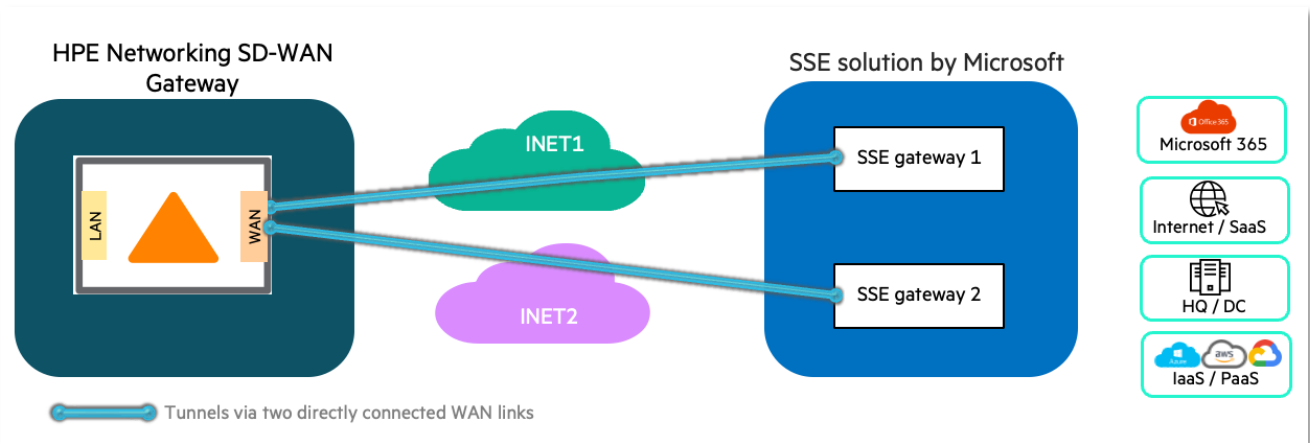
4 Planning and Topologies

Before configuration on Microsoft Entra admin center or HPE Aruba Networking Orchestrator, identify the following details for each site.

- The number of WAN links terminating on the EdgeConnect gateway, and the public IP address of each WAN link.
- A /29 subnet that you will use for loopback interface and VTI interfaces; the loopback interface address will be used as BGP peer address.
- A BGP Autonomous System Number (ASN) for the EdgeConnect gateway. Even if you don't plan to use BGP integration, you still need this detail when setting up the site in the Microsoft Entra admin center > Global Secure Access.
- Although the SSE solution by Microsoft doesn't require a unique subnet for BGP, it is a best practice to identify a /30 subnet for local BGP addresses. This subnet must be different from that of the local BGP address. Even if you don't plan to use BGP integration, you still need this detail when setting up the site in Microsoft Entra admin center > Global Secure Access.
- Identify the bandwidth capacity for the SSE gateway (Microsoft offers 250/500/750/1000 Mbps).
- Determine if the SSE gateway with Zone Redundancy is required. When you select Zone Redundancy, two SSE gateways are deployed per WAN link.
- Determine if you want to use Policy based traffic redirection (BIO – Overlay policy) or Route based (BGP) traffic redirection to the SSE solution by Microsoft.
- Determine if you need Active/Active load balancing for traffic on all available uplinks. The SSE solution by Microsoft doesn't distinguish gateways as active or backup, so you must choose whether all tunnels will share the traffic load or some tunnels will be backup.

Sections 4.1 through 4.5 show some of the possible topologies of a site with a dual-WAN uplink network:

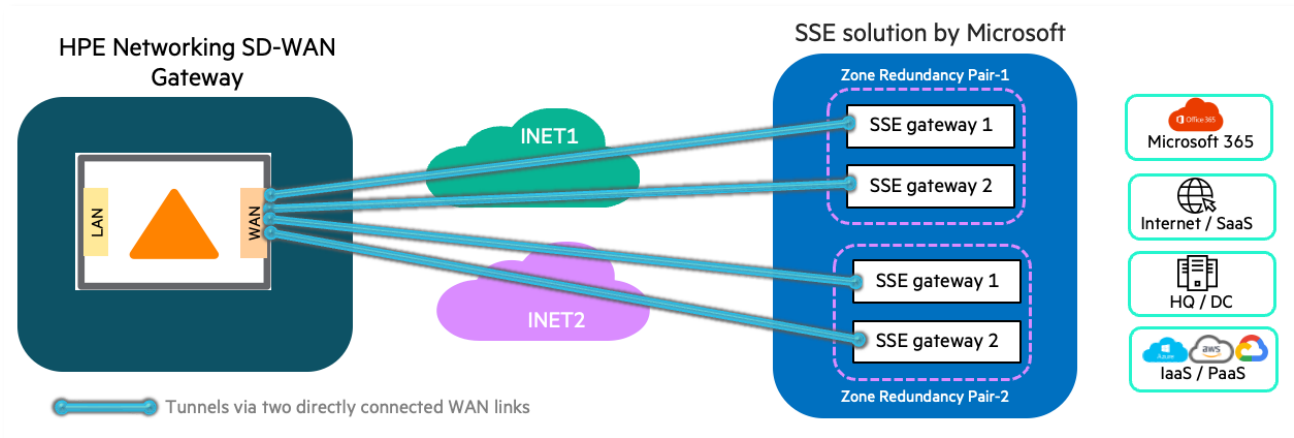
4.1 Branch with a Single Gateway - NO Zone Redundancy at SSE solution by Microsoft



1. Configure two WAN links when configuring the Remote Network on Microsoft Entra admin center > Global Secure Access.
2. This results in **two** passthrough tunnel configurations.
3. Set Redundancy as “No Redundancy” when configuring the Remote Network. See Figure 2.
4. Traffic can be active-active (load balanced on both tunnels) OR active-backup.

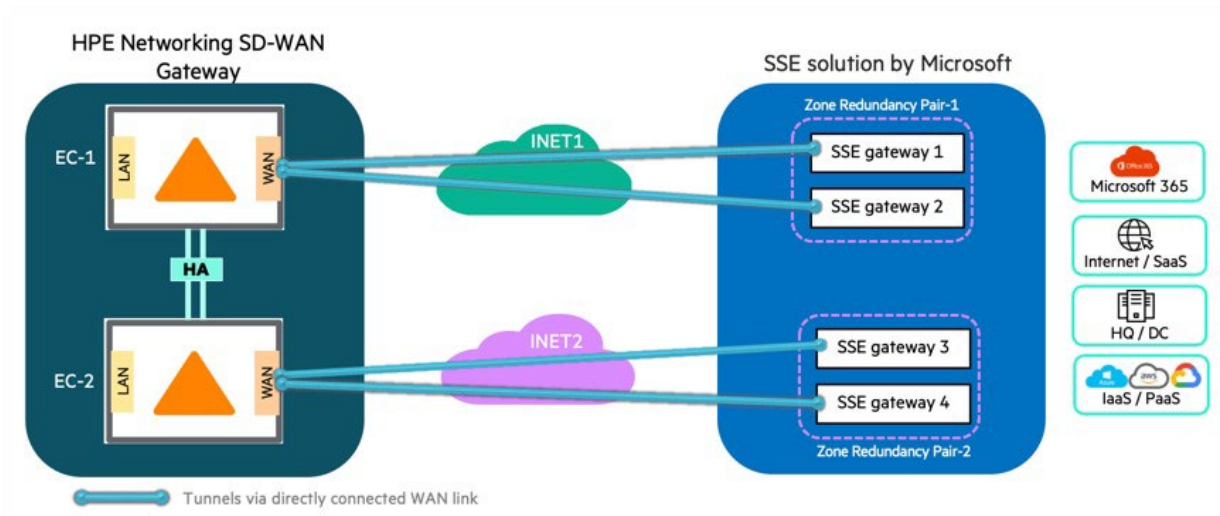


4.2 Branch with a Single Gateway - With Zone Redundancy at SSE solution by Microsoft



1. Configure two WAN links when configuring the Remote Network on Microsoft Entra admin center > Global Secure Access.
2. This results in **four** passthrough tunnel configurations.
3. Set Redundancy as “Zone Redundancy” when configuring the Remote Network.
4. Traffic can be active-active (load balanced on both tunnels) OR active-backup.

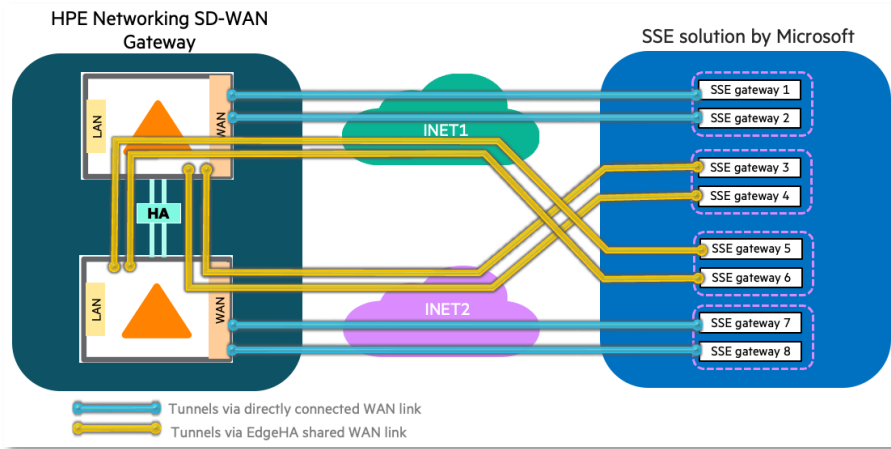
4.3 Branch with HA Pair - Tunnels Over Directly Connected WAN - With Zone Redundancy at SSE solution by Microsoft



1. Configure one WAN link per EdgeConnect gateway when configuring the Remote Network on Microsoft Entra Admin Center > Global Secure Access. A total of two WAN links per site is required.
2. This results in **two** passthrough tunnel configurations per EdgeConnect gateway, and a total of **four** passthrough tunnel configurations per site.
3. Set Redundancy as “Zone Redundancy” when configuring the Remote Network.
4. Traffic can be active-active (load balanced on both tunnels) OR active-backup.

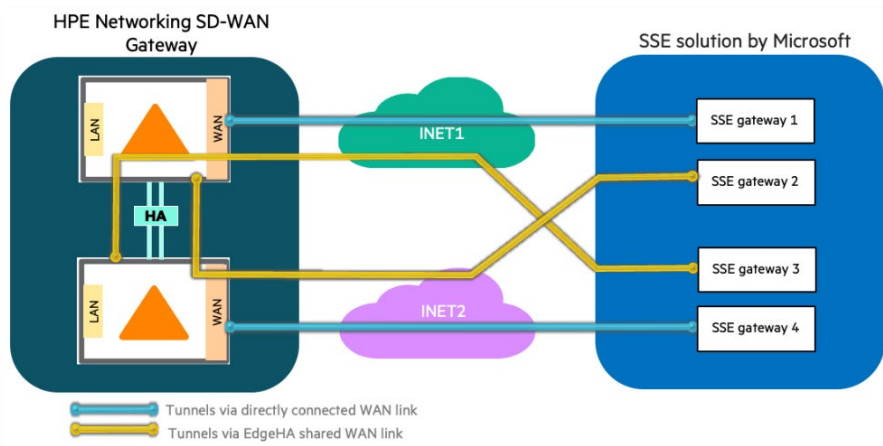


4.4 Branch with HA Pair - Tunnels Over Direct and Shared WAN - With Zone Redundancy at SSE solution by Microsoft



1. Configure two WAN links per EdgeConnect gateway when configuring the Remote Network on Microsoft Entra Admin Center > Global Secure Access. A total of four WAN links per site is required.
2. This results in **four** passthrough tunnel configurations per EdgeConnect gateway, and a total of eight passthrough tunnel configurations per site.
3. Set Redundancy as “Zone Redundancy” when configuring the Remote Network.
4. Traffic can be active-active (load balanced on both tunnels) OR active-backup.

4.5 Branch with HA Pair - Tunnels Over Direct and Shared WAN - NO Zone Redundancy at SSE solution by Microsoft



1. Configure two WAN links per EdgeConnect gateway when configuring the Remote Network on Microsoft Entra Admin Center > Global Secure Access. A total of four WAN links per site is required.
2. This results in **two** passthrough tunnel configurations per EdgeConnect gateway, and a total of four passthrough tunnel configurations per site.
3. Set Redundancy as “No Zone Redundancy” when configuring the Remote Network.
4. Traffic can be active-active (load balanced on both tunnels) OR active-backup.

After you have carefully reviewed your design and topology, proceed to [Remote Network Configuration on Microsoft Entra Admin Center \(Section 5\)](#).

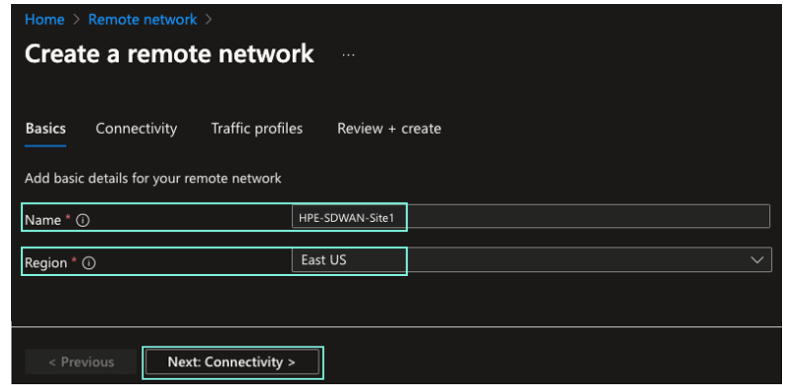


5 Remote Network Configuration on Microsoft Entra Admin Center

For more information on Remote Network configuration on Microsoft Entra admin center, see this [article](#) on the Microsoft documentation site.

1. Log in to Microsoft Entra admin center and navigate to **Global Secure Access (preview) > Connect > Remote networks**.
2. Click **Create remote network** and enter the following details:

- **Name:** Enter a name that represents your physical location. It is recommended to have one remote network per site.
- **Region:** Select the closest to your physical location. In this example, the closest region for the Andover site is "East US".



3. Click **Next: Connectivity >** and then click **+ Add Link** to add your device links. In this section, add a link for each WAN link per site to establish IPSec tunnels over each of those WAN links.

Link name: Enter a name for the link.

Device type: Enter "HPE Aruba".

IP address: Enter the public IP address of your WAN link.

Local BGP address: Enter an IP address for the local BGP peer. Choose a unique subnet because it cannot overlap with Peer BGP address.

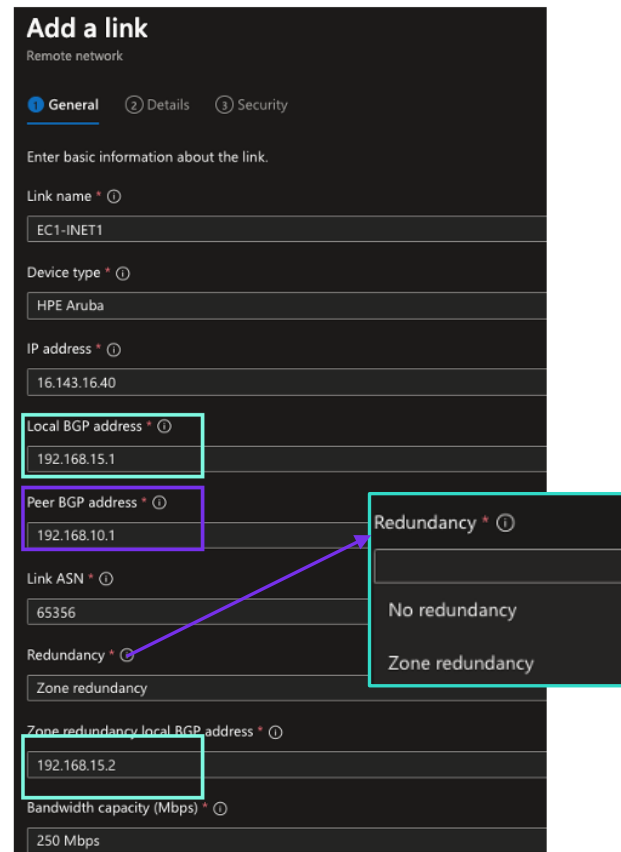
Peer BGP address: Enter an IP address for EdgeConnect gateway BGP peer (loopback interface). Choose a unique subnet because it cannot overlap with Local BGP address.

Link ASN: BGP AS number for your EdgeConnect Gateway.

Redundancy: (Only if you want to terminate tunnels on two redundant gateways.) Select **Zone redundancy** if you need to deploy redundant tunnels on this link.

Zone redundancy local BGP address: Provide an IP address for redundancy BGP peer. Use the same subnet you used for Local BGP address.

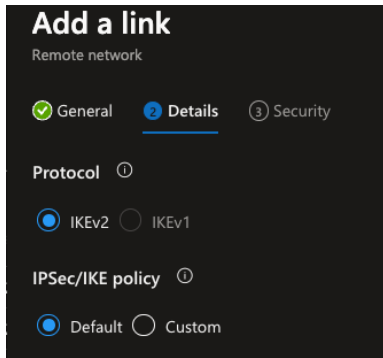
Bandwidth capacity (Mbps): Select the appropriate bandwidth for your network (250/500/750/1000).



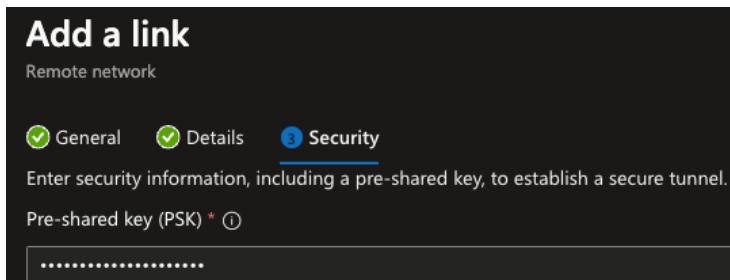
4. Click **Next**.
5. Leave the default IKE/IPSec setting as is.

Figure 2 - Adding a Link on Microsoft Entra Admin Center

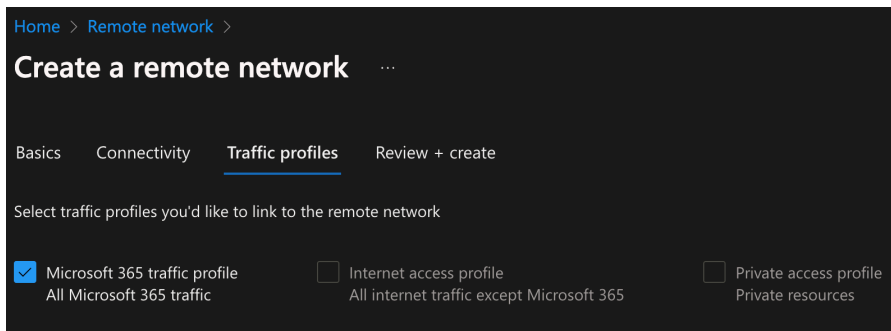




6. Click **Next**.
7. Enter a pre-shared key for your IPSec tunnel.



8. To complete adding the link, click **Save**.
9. Repeat steps 3 to 8 for each WAN uplink per gateway. For example, if you have two WAN links and two EdgeConnect gateways connected through EdgeHA then you must complete the process of adding a link four times (2 uplinks × 2 EdgeConnect gateways = 4 links).
10. Click **Traffic profiles**.
11. Under Traffic profiles, select the profile that matches your requirements.



12. Click **Review + create** to complete the Remote Network configuration.

NOTE: If there are any links you failed to add, you can go back to the Remote Networks section > Select your Site and click **Add Link +** to add additional links for that site.

13. After you complete remote network configuration for the site, you can view/download the configuration file for that site. Navigate to **Global Secure Access (preview) > Connect > Remote networks** and click the corresponding **View configuration** for your site.



Remote network n...	Region	Links	Device type	Forwarding profiles	Last modified	Object Id	Connectivity details
HPE-Aruba	East US	> 2 links		1 profile	01/22/2024, 12:42 ...	4d3d0ad2-b936-4e12-8de6-ee530715d2e2	View configuration
HPE-SDWAN-Site1	East US	> 4 links		1 profile	01/24/2024, 11:28 ...	341c01f2-b8a2-405a-91cb-a6032316ac27	View configuration
Seattle branch	West US 2	> 1 link		1 profile	09/28/2023, 06:04 ...	009de9e7-ae3e-48af-864e-319e8abf4b21	View configuration
to-eric	West US 2	> 1 link			11/06/2023, 01:49 ...	e921a56d-6351-4b17-94bd-07aca337b5a1	View configuration
VMware-google	West US 2	> 1 link		1 profile	10/12/2023, 12:53 ...	1bae25c5-b852-478a-b9f6-076561574242	View configuration

The following graphic shows how to identify tunnel details from the configuration file.

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#networks",
  "branchId": "341c01f2-b8a2-405a-91cb-a6032316ac27",
  "branchName": "HPE-SDWAN-Site1",
  "links@odata.context": "https://graph.microsoft.com/beta/$metadata#networks('341c01f2-b8a2-405a-91cb-a6032316ac27')/links",
  "links": [
    {
      "id": "d2021ca6-8e25-4acf-81fd-313e5c6d8d6c",
      "displayName": "EC1-INET1",
      "localConfigurations": [
        {
          "endpoint": "40.76.245.144",
          "asn": 65136,
          "bgpAddress": "192.168.15.1",
          "region": "eastUS"
        },
        {
          "endpoint": "20.163.176.193",
          "asn": 65136,
          "bgpAddress": "192.168.15.2",
          "region": "eastUS"
        }
      ],
      "peerConfiguration": {
        "endpoint": "16.143.16.43",
        "asn": 65356,
        "bgpAddress": "192.168.10.1"
      }
    },
    {
      "id": "a3429d77-5a1e-4d68-97aa-8aa7f4a5d763",
      "displayName": "EC1-INET2",
      "localConfigurations": [
        {
          "endpoint": "40.76.245.144",
          "asn": 65136,
          "bgpAddress": "192.168.25.1",
          "region": "eastUS"
        },
        {
          "endpoint": "20.163.176.193",
          "asn": 65136,
          "bgpAddress": "192.168.25.2",
          "region": "eastUS"
        }
      ],
      "peerConfiguration": {
        "endpoint": "16.143.16.40",
        "asn": 65356,
        "bgpAddress": "192.168.20.1"
      }
    }
  ]
}
```

EC1-INET1 relevant configuration

Tunnel Endpoint#1 for INET1 Tunnel

Tunnel Endpoint#2 for INET1 Tunnel

EC1-INET2 relevant configuration

Tunnel Endpoint#1 for INET2 Tunnel

Tunnel Endpoint#2 for INET2 Tunnel



Creating Remote Network configuration on the Microsoft Entra Admin Center is complete. Proceed to [Passthrough Tunnel Configuration on the EdgeConnect Gateway \(Section 6\)](#).



6 Passthrough Tunnel Configuration on the EdgeConnect Gateway

6.1 Creating a Passthrough Tunnel

1. Log in to HPE Aruba Networking Orchestrator and select your EdgeConnect gateway from the appliance tree.
2. Navigate to **Configuration > Networking > Tunnels > Tunnels**.

The Tunnels tab opens.

3. Click the edit icon on any of the existing tunnels. The Tunnels dialog box opens.
4. On the Tunnels dialog box for the gateway, click **Passthrough** and then click **Add Tunnel**.

The Add Passthrough Tunnel dialog box opens.

Before configuring anything on the General tab, read the following considerations if you are intending to use Policy Based Traffic Redirection (Business Intent Overlay based redirection). Otherwise proceed to [Step 5](#) directly.

Consideration for Active-Active Traffic on Tunnels for Policy Based Traffic Redirection

On the General tab, enter a **common** "Peer/Service" name for all the passthrough tunnels that you create. Doing this associates all tunnels to one service name and EdgeConnect automatically load balances traffic among all the tunnels that share the common service name.

Consideration for Active-Backup Traffic on Tunnels for Policy Based Traffic Redirection

On the General tab, enter a **unique** "Peer/Service" name for primary tunnels and backup tunnels. EdgeConnect load balances traffic only on the tunnels with the common Peer/Service name. Backup tunnels are used only when primary tunnels fail (this setting is on the BIO – Preferred Policy Order).

5. Configure the settings on the General, IKE, and IPSec tabs, as shown in the following example.

For all the supported IKE and IPSec parameters including other combinations of IKE and IPSec parameters, refer to the [Add or Modify a Manually Created Passthrough Tunnel](#) section of the Orchestrator User Guide.

NOTE: The IKE and IPSec tabs appear after you select **IPSec** from the Mode drop-down menu.

The screenshot shows the 'Modify Passthrough Tunnel' dialog box with the 'General' tab selected. The settings are as follows:

Field	Value
Alias	Entra_Primary_INET1_POP1
Mode	IPSec
IPSec Suite B Preset	None
Admin	up
Local IP	16.143.16.43 - Default
Remote IP	40.76.245.144
NAT	none
Peer/Service	Entra_Primary
Auto max BW enabled	<input checked="" type="checkbox"/>
Max BW Kbps	250000

Mode: Select **IPSec**.

Alias: Enter a unique name for the tunnel.

Local IP: Select your WAN interface.

Remote IP: Enter the IP address for the SSE Remote Gateway from the configuration file you downloaded in Section 5.

Peer/Service: Enter a service name. This service name is used by the Business Intent Overlay to forward traffic.

Auto max BW enabled: Click the check box.



Pre-shared key: Enter the pre-shared key that was set during configuration of the SSE Remote Networks.

Authentication Algorithm: Select **SHA2-256**.

Encryption Algorithm: Select **AES-CBC-256**.

Diffie-Hellman Group: Select **2**.

Local IKE identifier: Enter a unique name for the Local IKE identifier. In this example, the IP address of the WAN uplink is used as the identifier.

Remote IKE identifier: Enter the IP address for the SSE gateway.

IKE Version: Select **IKE V2**.

NOTE: On the IPsec tab, select “Encryption Algorithm” first, which automatically sets Authentication algorithm to “NA”.

Authentication algorithm: Select **Encryption Algorithm**. This automatically sets it to “NA”.

Encryption algorithm: Select **AES-GCM-256**.

Perfect forward secrecy group: Select **disable**.

- Click **Save** and then click **Close** to complete the tunnel configuration.
- Repeat Steps 5 and 6 for as many tunnels that are configured on the Microsoft Entra admin center > Remote Networks for a given site.
- The IPsec tunnel between the EdgeConnect and the SSE gateways are established. After a few minutes, the tunnels should appear on the Tunnels tab with a Status of “up - active”. The figure below shows four IPsec tunnels established between the EdgeConnect and SSE gateways.

Edit	Appliance	Segment...	Passthrough Tunnel	Admin Status	Charts	Status	Local IP	Remote IP	Mode	NAT	Peer/Service
	Store101-EC1	Default	Entra_Primary_INET1_POP1	up		up - active	16.143.16.43	40.76.245.144	IPsec	none	Entra_Primary
	Store101-EC1	Default	Entra_Primary_INET1_POP2	up		up - active	16.143.16.43	20.163.176.193	IPsec	none	Entra_Primary
	Store101-EC1	Default	Entra_Primary_INET2_POP3	up		up - active	172.16.8.43	40.76.245.144	IPsec	none	Entra_Primary
	Store101-EC1	Default	Entra_Primary_INET2_POP4	up		up - active	172.16.8.43	20.163.176.193	IPsec	none	Entra_Primary



Creating an IPsec tunnel from the EdgeConnect gateway to Microsoft Entra SSE endpoints is now completed. Proceed to Tunnel Monitoring Using IP SLA Probes (Section 6.2).



6.2 Tunnel Monitoring Using IP SLA Probes

After the passthrough tunnels are established, HPE Aruba Networking recommends that you configure IP SLA monitoring for each tunnel to ensure availability of the tunnel for data traffic. IP SLA monitoring actively sends probes (either HTTP or ICMP) to configured destinations to ensure tunnel availability.

1. Log in to HPE Aruba Networking Orchestrator and select your EdgeConnect gateway from the appliance tree.
2. Navigate to **Configuration > Templates & Policies > TCAs > IP SLA**.
 The IP SLA tab opens.
3. Click the edit icon on any of the existing IP SLA rules.
4. On the IP SLA dialog box for the gateway, click **Add**.
 The IP SLA Rule dialog box opens.
5. Configure the settings in the Monitor and Actions sections, as shown in the following example.

Monitor

Monitor: Select **Ping**.

Address: Enter the IP address or FQDN of a known destination that can respond to ICMP packets. In this example, the following were entered as ping destinations: sp-ipsla.silverpeak.cloud,8.8.8, 8.8.4.4

Source: Select **Interface**.

Interface: Select the VTI interface that corresponds to the tunnel that will be monitored by this IP SLA rule. In this example, the tunnel to INET1_POP1 is monitored, which is also attached to the VTI1 interface. Hence **vti1** is selected as the interface.

Ping Interval: Enter **1**. This determines how frequently probe packets are sent.

Action

Down action: Select **Disable Tunnel**.

Tunnel: Select the tunnel that is being monitored. In this example, the tunnel to INET1_POP1 is selected.

Up action: Select **Enable Tunnel**.

Tunnel: Select the tunnel that is being monitored. In this example, the tunnel to INET1_POP1 is selected.



- 6. Click **Add** to complete the IP SLA rule configuration.
- 7. Repeat Steps 4 and 6 for as many tunnels that were configured as part of Section 6.1. In this example, four passthrough tunnels were added in Section 6.1, so four IP SLA rules are added to monitor each of those tunnels.

After a few moments, IP SLA probes start and the status appears on the IP SLA tab.

IP SLA ?								
14 Rows								
Search <input type="text"/>								
Edit	Appliance	Active	State	Monitor	Down Action	Up Action	Up Stats	Down Stats
	Store101-EC1	Yes	Up	Ping: Force DNS = false, Down Thresh	Tunnel Down: Tunnel = Entra_Primary_INET1_POP1	Tunnel Up: Tunnel = Entra_Primary_INET1_POP1	Last:2h 18m 32s	Total :11, Last:6h 12m 32s
	Store101-EC1	Yes	Up	Ping: Force DNS = false, Down Thresh	Tunnel Down: Tunnel = Entra_Primary_INET1_POP2	Tunnel Up: Tunnel = Entra_Primary_INET1_POP2	Last:2h 18m 32s	Total :11, Last:6h 12m 32s
	Store101-EC1	Yes	Up	Ping: Force DNS = false, Down Thresh	Tunnel Down: Tunnel = Entra_Primary_INET2_POP3	Tunnel Up: Tunnel = Entra_Primary_INET2_POP3	Last:2h 18m 32s	Total :11, Last:6h 12m 32s
	Store101-EC1	Yes	Up	Ping: Force DNS = false, Down Thresh	Tunnel Down: Tunnel = Entra_Primary_INET2_POP4	Tunnel Up: Tunnel = Entra_Primary_INET2_POP4	Last:2h 18m 32s	Total :11, Last:6h 12m 32s



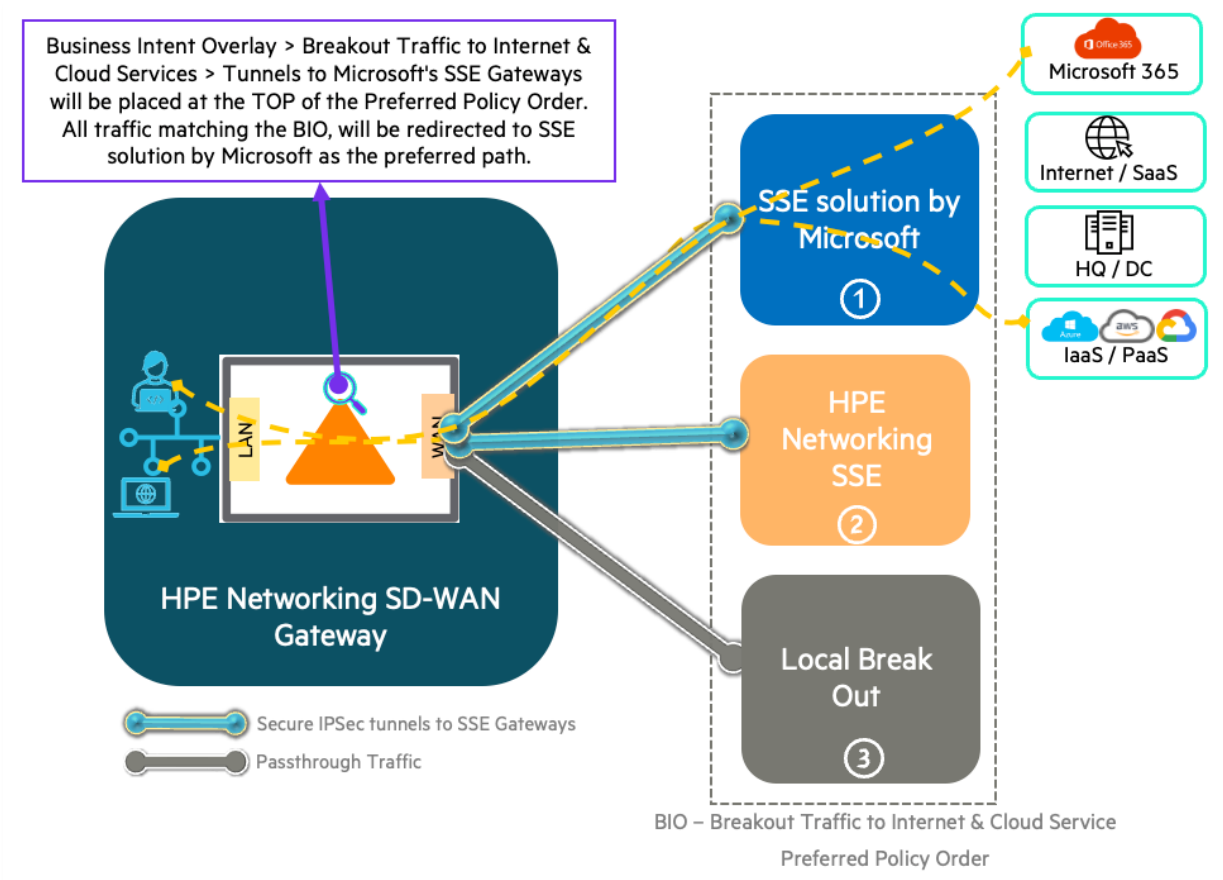
Creating IPsec tunnels and creating IP SLA rules to monitor tunnel health is now completed on the EdgeConnect. Proceed to configure traffic redirection:

- a. [Policy Based Traffic Redirection to the SSE Gateway \(Section 7\)](#).
- b. [Route Based Traffic Redirection to the SSE Gateway \(Section 8\)](#).



7 Policy Based Traffic Redirection to the SSE solution by Microsoft

You must identify application traffic that needs to be redirected to the SSE solution by Microsoft. The Business Intent Overlay framework in HPE Aruba Networking Orchestrator supports configuration of granular policies to steer application traffic based on application name, application group, domains, IP address/subnets/address group, interface, etc.



In the topology above, the “SSE solution by Microsoft” tunnel is placed at the top of the Preferred Policy Order, which forces all the traffic matching a given BIO to take the SSE tunnel path. Optionally, you can add other policies as a backup in case the primary path to the “SSE solution by Microsoft” is unavailable.

1. Log in to Orchestrator and select your EdgeConnect gateway from the appliance tree.
2. Navigate to **Configuration > Overlays & Security > Business Intent Overlay**.
 The Business Intent Overlay tab opens.
3. Click an existing overlay or click **+New** to create a new overlay. If you are creating a new overlay, enter a name for the overlay in the Create Overlay dialog box and click **Add**.
 The Overlay Configuration dialog box opens.
4. Click the edit icon next to Match section to modify the Overlay ACL.

Overlay Configuration

Name: Match: Application: Region:

The Association ACL dialog box opens.

5. Click **Add Rule** to add new rules to this overlay ACL.



In the following example, the CASB Overlay policy was modified to permit any HTTP/HTTPS or user traffic from the lan0.1300 interface to use the CASB overlay.

Associate ACL

Add Rule

3 Rows

Priority	Match Criteria	Permit
1060	Application http https , Fabric/Internet Internet	permit
1070	Protocol tcp , Port 80 443 , Fabric/Internet Interne	permit
1080	Interface lan0.1300	permit

- Click **Save** to add the rule and then click **Close**.

The Associate ACL dialog box closes. After you are done modifying the Overlay ACL, you must configure the SSE tunnels in Available Policies.

- Click **Breakout Traffic to Internet & Cloud Services**.
- Click the edit icon next to **Available Policies**, as shown in the following figure.

Overlay Configuration

Name: Match:

SD-WAN Traffic to Internal Subnets Breakout Traffic to Internet & Cloud Services

Preferred Policy Order Available Policies Break Out Locally Using These Interfaces

The Services dialog box opens.

- From the drop down, select the name that you entered for Peer/Service during passthrough tunnel configuration. In the following example, "Entra_Primary" was the service name configured, so it is selected from the menu.

Services

Service Name

Modify Passthrough Tunnel

General | IKE | IPSec

General

Alias:

Mode:

IPSec Suite B Preset:

Admin:

Local IP:

Remote IP:

NAT:

Peer/Service:

Auto max BW enabled:

Max BW Kbps:

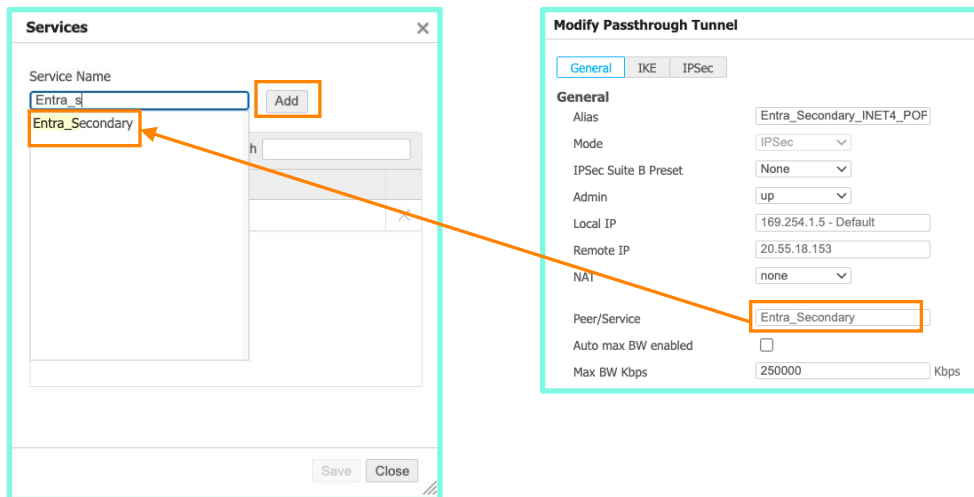
- Click **Add**, then click **Save** and **Close**.



11. Drag the `Entra_Primary` policy to the top of the Preferred Policy Order column. This routes the traffic identified by the Business Intent Overlay to the SSE gateways using the IPSec tunnels.

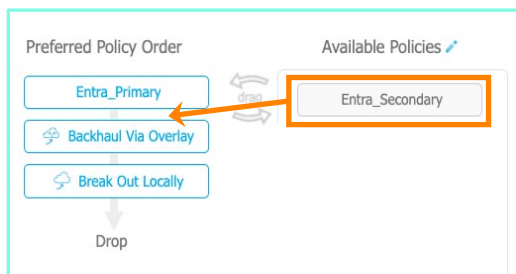


12. Applicable only for Active-Backup Tunnels: If you have configured two different Peer/Services for your tunnels towards the SSE gateways then you need to add the backup tunnels as the next preferred policy. In the following example, "Entra_Secondary" was the service name configured for backup tunnels, so it is selected from the menu.

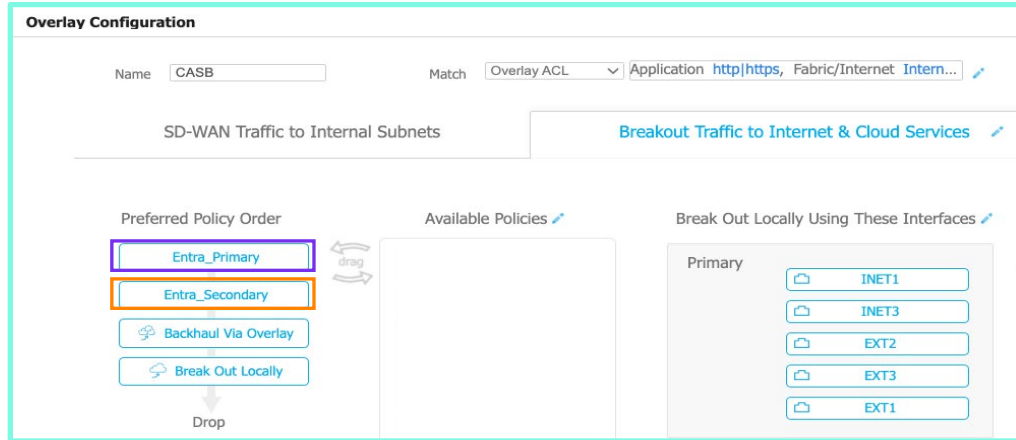


13. Click **Add**, then click **Save** and **Close**.

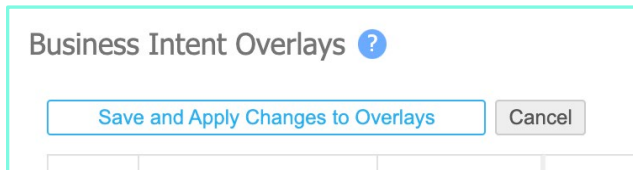
Drag the `Entra_Secondary` policy directly below `Entra_Primary`. This enables the EdgeConnect gateway to redirect traffic to backup tunnels automatically when the primary tunnels go down.




When you are done, the Overlay configuration should look similar to the following figure:



14. Click **OK** to exit the Overlay Configuration and return to Business Intent Overlay dialog box.
15. Click **Save and Apply Changes to Overlays** to save the changes.



 Traffic redirection from the EdgeConnect gateway to the SSE gateways is now completed. Validate traffic redirection to the “SSE solution by Microsoft” by sending traffic that is identified in the Overlay ACL (in this example any HTTP/HTTPS). Proceed to [Verify the Flows on the EdgeConnect Gateway \(Section 7.1\)](#) to see the flow details.



7.1 Verify the Flows on the EdgeConnect Gateway

In Orchestrator, navigate to **Monitoring > Bandwidth > Flows > Active & Recent Flows**. Check your user traffic flows by filtering based on the user IP address or the application. The following figure shows an example of a flow that is filtered based on IP address:

Inbound/Outbound Tunnel shows “Entra_Primary” tunnel that was mapped on the Business Intent Overlay.

Appliance	Detail	Start Time	Uptime	Overlay	Application	IP1	Port1	IP2	Port2	Inbound Bytes	Outbound Bytes	Inbound Tunnel	Outbound Tunnel
Hub-West		09:58:30	30s	EntraSSE	Office365Common	172.23.25.153	60502	mobile.events.data.microsoft.com (52.168.117.169)	443	8K	4K	Entra_Primary	Entra_Primary
Hub-West		09:57:49	1m 11s	EntraSSE	Office365Common	172.23.25.153	51663	mobile.events.data.microsoft.com (52.168.117.169)	443	8K	4K	Entra_Primary	Entra_Primary
Hub-West		09:56:57	2m 3s	EntraSSE	Office365Common	172.23.25.153	51303	mobile.events.data.microsoft.com (52.168.117.169)	443	8K	4K	Entra_Primary	Entra_Primary
Hub-West		09:57:28	1m 32s	EntraSSE	Office365Common	172.23.25.153	51439	mobile.events.data.microsoft.com (52.168.117.169)	443	8K	4K	Entra_Primary	Entra_Primary

Click the info icon to view additional flow details.

Flow details for IP1: 172.23.25.153 Port1: 60502 IP2: 52.168.117.169 and Port2: 443

General Optimization TCP NAT AVC/DNS Internet Performance User Details Identity

Route		Stats	
Map Name	map1	Outbound Ratio	1.00
Priority in Map (ACL)	20006 (ACL: 1000)	Inbound Ratio	1.00
Overlay	EntraSSE	Outbound LAN bytes	4,779
Configured Tx Action	Entra_Primary	Outbound WAN bytes	4,779
Tx Action	Entra_Primary	Inbound LAN bytes	8,341
Rx Action	Entra_Primary	Inbound WAN bytes	8,341
Tx Reason	primary	Outbound LAN pkts	20
Application First Pkt	Office365Common (http-domain)	Outbound WAN pkts	20
Application	Office365Common (http-domain)	Inbound LAN pkts	20
Application Group	Microsoft,Encrypted,Network_Services	Inbound WAN pkts	20
Traffic Category	Undetermined	Inbound WAN lost	0
Protocol	tcp	Inbound WAN average jitter	0.00 milli sec
Using Stale Map Entry	No	Flow Up Time	2m 12s
Flow Direction	Outbound	Flow ID	239795
Ingress interface	lan0	Active	No
Egress interface	wan0	TCP Flow Context	239795
Flow Redirected From		Is Flow Queued For Reset	No
Auto-opt Transit Node		Web Proxy Detected	No
LAN-side VLAN	None	Source IP	172.23.25.153
Subnet	0.0.0.0/0 (50) (Non-Local) mid 2074573	Dest IP	52.168.117.169
Internet flow	Yes	Last Policy Change	547051304
WAN routing	Entra_INET1_Primary1	Last Policy Lookup	570508328
LAN routing	lan0		

OnS Security

Refresh Close

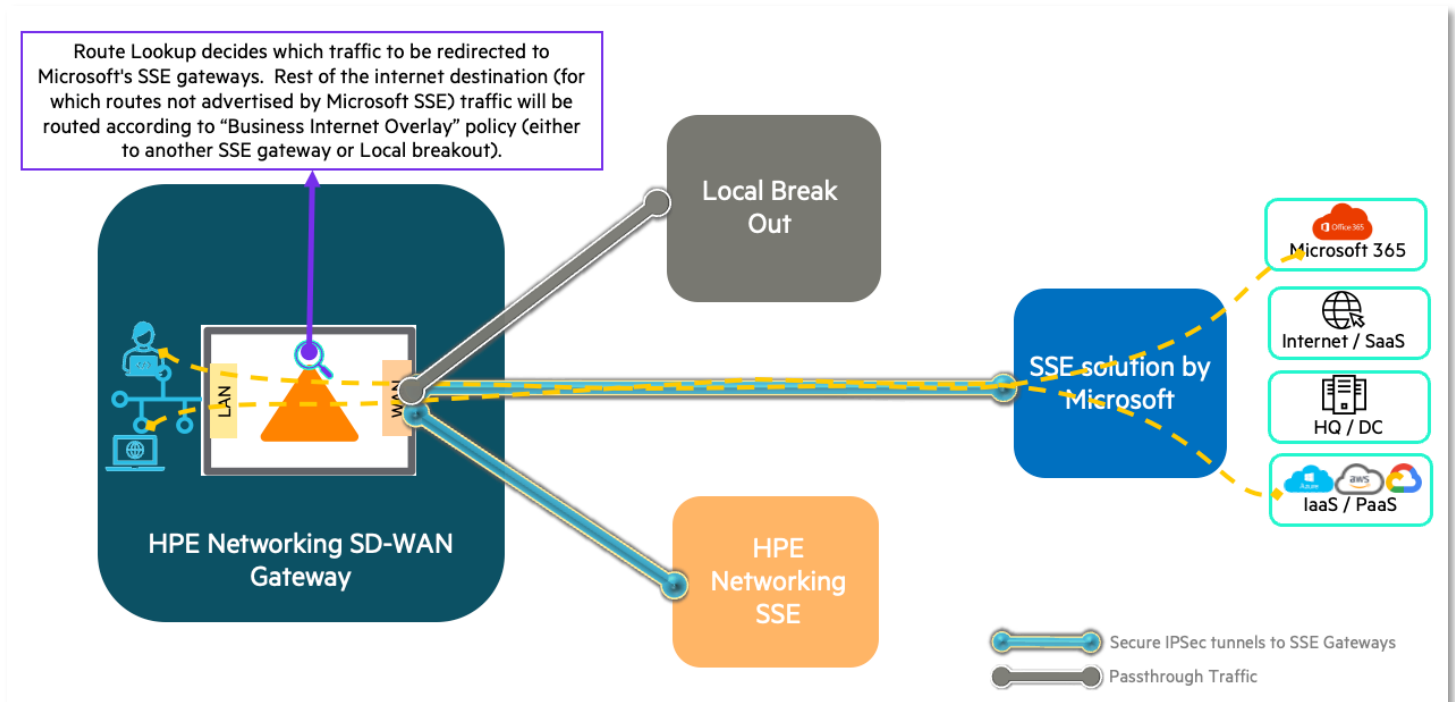


You have completed all the tasks required for establishing an IPsec tunnel with the SSE gateway and traffic redirection to SSE gateway using the policy-based method.



8 Route Based Traffic Redirection to the SSE solution by Microsoft

Route based traffic redirection to the SSE gateway is achieved by establishing eBGP peering between EdgeConnect gateways and the SSE gateway. Received BGP routes from the SSE gateway are treated as internal subnets and the Use Best Route option on the Business Intent Overlay redirects the traffic to use the passthrough tunnels. ECMP is used to achieve load balancing across all available tunnels if active-active load balancing is required.



The following configuration steps detail how to establish eBGP peering, enabling ECMP, enabling internal subnet, and modifying the BIO to use the Use Best Route option to redirect traffic to the SSE gateway.

High-level Configuration Tasks:

1. Add Loopback interfaces.
2. Add VTI interfaces.
3. Add a static route to reach the BGP peer via VTI.
4. Create a BGP neighborhood with the SSE gateway.
5. Enable the "Consider Non-default routes as internal subnets" option.
6. Change the Business Intent Overlay to Use Best Route instead of Drop.
7. Configure Active-Active or Active-Backup load balancing.
8. Verify traffic flows on the EdgeConnect gateway.

Before configuring BGP peering, make sure you download the Remote network configuration from the Microsoft Entra admin center > Global Secure Access. This configuration contains important details for BGP configuration.

Relevant sections on the Remote network configuration are highlighted in the following figure. Note that the `bgpAddress` under `peerConfiguration` represents the BGP source address on the EdgeConnect gateway. This document uses that address for configuring loopback and VTI interfaces with IP addresses within the /29 subnet range.



Remote network configuration

HPE-SDWAN-Site1

To complete the process of IPsec tunnel creation, configure your CPE (customer premise equipment) with following connectivity details. [Learn more](#)

```

{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#networks",
  "branchId": "341c01f2-b8a2-405a-91cb-a6032316ac27",
  "branchName": "HPE-SDWAN-Site1",
  "Links@odata.context": "https://graph.microsoft.com/beta/$metadata#networks/links",
  "Links": [
    {
      "id": "d2021ca6-8e25-4acf-81fd-313e5c6d8d6c",
      "displayName": "EC1-INET1",
      "LocalConfigurations": [
        {
          "endpoint": "40.76.245.144",
          "asn": 65476,
          "bgpAddress": "192.168.15.1",
          "region": "EastUS"
        },
        {
          "endpoint": "20.163.176.193",
          "asn": 65476,
          "bgpAddress": "192.168.15.2",
          "region": "EastUS"
        }
      ],
      "peerConfiguration": {
        "endpoint": "192.143.16.40",
        "asn": 65356,
        "bgpAddress": "192.168.10.1"
      }
    },
    {
      "id": "a3429d77-5a1e-4d68-97aa-8aa7f4a5d763",
      "displayName": "EC1-INET2",
      "LocalConfigurations": [
        {
          "endpoint": "40.76.245.144",
          "asn": 65476,
          "bgpAddress": "192.168.25.1",
          "region": "EastUS"
        },
        {
          "endpoint": "20.163.176.193",
          "asn": 65476,
          "bgpAddress": "192.168.25.2",
          "region": "EastUS"
        }
      ],
      "peerConfiguration": {
        "endpoint": "192.143.16.40",
        "asn": 65356,
        "bgpAddress": "192.168.20.1"
      }
    }
  ]
}
    
```

Annotations:

- BGP ASN / Peer address of Endpoint#1 on INET1_POP1 Tunnel
- BGP ASN / Peer address of Endpoint#2 on INET1_POP2 Tunnel
- BGP ASN / EdgeConnect Loopback address (BGP source) of EdgeConnect
- BGP ASN / Peer address of Endpoint#3 on INET2_POP1 Tunnel
- BGP ASN / Peer address of Endpoint#4 on INET2_POP2 Tunnel
- BGP ASN / Loopback address (BGP source) of EdgeConnect

Figure 3 - Remote network configuration downloaded from Microsoft Entra admin center > Global Secure Access

BGP details from the Remote network configuration are shown in the following topology of a single EdgeConnect gateway to two pair of redundant SSE gateways via two WAN links (INET1 and INET2).

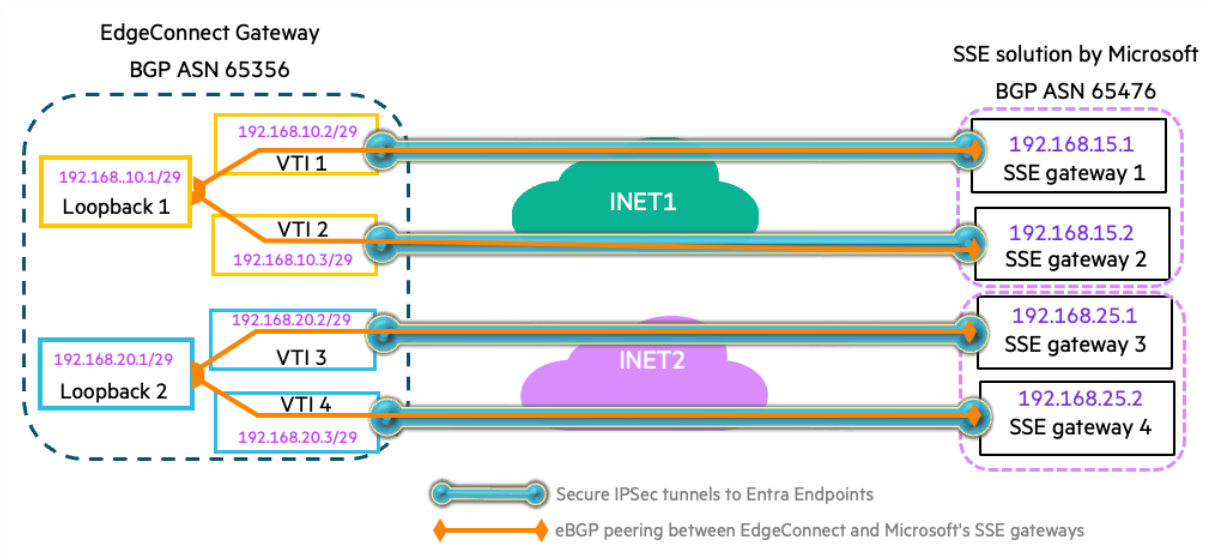


Figure 4 – Topology with Loopback/VTI interface IP address and peer BGP address



8.1 Add Loopback Interfaces

1. Log in to Orchestrator and select your EdgeConnect gateway from the appliance tree.
2. Navigate to **Configuration > Networking > Loopback Interfaces**.

The Loopback Interfaces tab opens.

3. Click the edit icon next to the gateway name.

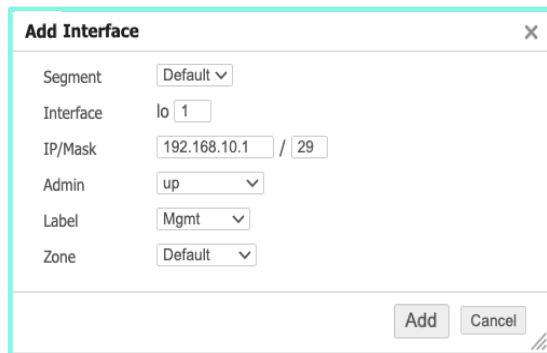
The Loopback Interfaces dialog box for the gateway opens.

NOTE: One loopback interface per zone redundancy at the SSE gateway pair is required with a dedicated IP address. The example shown in Figure 4 needs two loopback interfaces because there is a zone redundancy at each point where an SSE gateway pair is deployed.

4. Click **Add**.

The Add Interface dialog box opens.

5. Enter the required details, as shown in the following example.



Segment: Select your VRF segment if you have any, otherwise select **Default**.

Interface lo: Enter a number for the VTI interface.

IP/Mask: Enter the IP address with /29 mask. This IP address comes from the Remote network configuration file you downloaded from Microsoft Entra admin center > Global Secure Access.

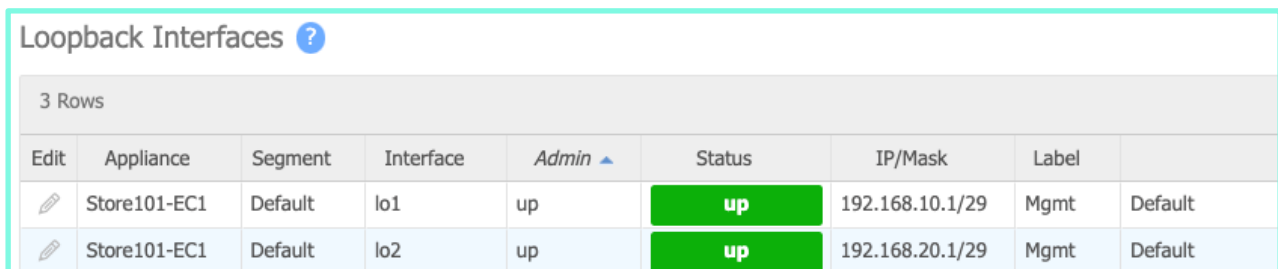
Admin: Select **up**.

Label: (optional)

Zone: Select a specific zone if any, otherwise select **Default**.

6. Click **Add** and then click **Save**.

The loopback interface you added appears in the Loopback Interfaces for the EdgeConnect gateway.



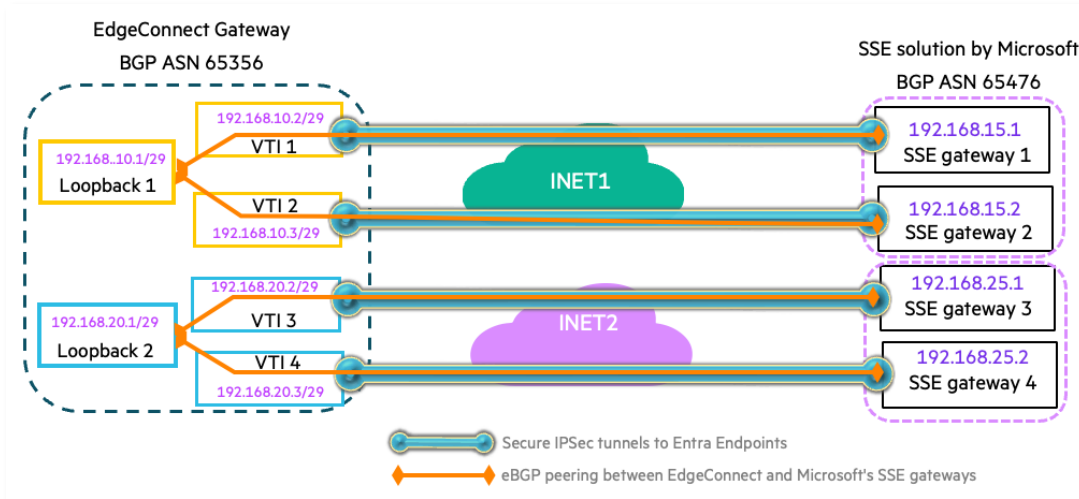
Edit	Appliance	Segment	Interface	Admin ▲	Status	IP/Mask	Label	
	Store101-EC1	Default	lo1	up	up	192.168.10.1/29	Mgmt	Default
	Store101-EC1	Default	lo2	up	up	192.168.20.1/29	Mgmt	Default

7. Repeat Steps 4 to 6 for any additional loopback interfaces.



8.2 Add VTI Interfaces

NOTE: One VTI interface per tunnel is required with a dedicated IP address. The following example needs four VTI interfaces because there are four tunnels.



1. In Orchestrator, select your EdgeConnect gateway from the appliance tree.
2. Navigate to **Configuration > Networking > Virtual Tunnel Interfaces (VTI)**.
The Virtual Tunnel Interfaces (VTI) tab opens.
3. Click the edit icon next to the gateway name.
The VTI dialog box for the gateway opens.
4. Click **Add**.
The Add VTI Interface dialog box opens.
5. Enter the required details, as shown in the following example.

Add VTI Interface ✕

Segment	Default ▾
Interface	vti 1
IP/Mask	192.168.10.2 / 29
Admin	up ▾
Passthrough Tunnel	Entra_Primary_INET1_POP1
Interface Type	lan ▾
Label	Mgmt ▾
Zone	Default ▾

Add Cancel

Segment: If you have a specific segment, select it, otherwise select **Default**.

Interface vti: Enter a number for the VTI interface.

IP/Mask: Enter the IP address for the VTI interface with /29 mask.

Passthrough Tunnel: Select the newly configured passthrough tunnel from the drop-down menu.

Interface Type: Select **lan** as the interface type.

Label: (optional)

Zone: If you have a specific zone, select it, otherwise select **Default**.



- 6. Click **Add** and then click **Save**.

The VTI interface you added appears in the VTI dialog box for the EdgeConnect gateway.

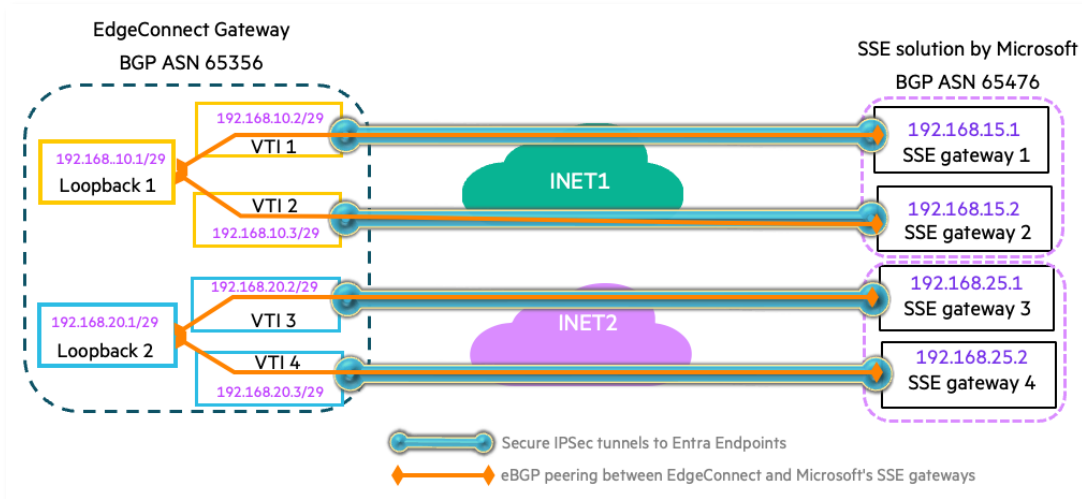
Virtual Tunnel Interfaces (VTI) ?										
4 Rows										
Edit	Appliance	Segment	Interface ▲	Admin	Status	IP/Mask	Passthrough Tunnel	Interface Type	Label	Zone
	Store101-EC1	Default	vti1	up	up	192.168.10.2/32	Entra_Primary_INET1_P...	lan	Mgmt	Default
	Store101-EC1	Default	vti2	up	up	192.168.10.3/32	Entra_Primary_INET1_P...	lan	Mgmt	Default
	Store101-EC1	Default	vti3	up	up	192.168.20.2/32	Entra_Primary_INET2_P...	lan	Mgmt	Default
	Store101-EC1	Default	vti4	up	up	192.168.20.3/32	Entra_Primary_INET2_P...	lan	Mgmt	Default

- 7. Repeat Steps 4 to 6 for additional VTI interfaces.



8.3 Add a Static Route to Reach the BGP Peer Via VTI

NOTE: One static route per BGP peer address is required. In this example, you need four static routes to the respective BGP peers via VTI interface.



1. In Orchestrator, navigate to **Configuration > Networking > Routing > Routes**.
2. Click the edit icon next to the gateway name. (If you have a VRF segment, click the edit icon next to your segment.)
The Routes dialog box for the gateway opens.
3. Click **Add Route**.
The Add Route dialog box opens.
4. Enter the details, as shown in the following example, to add a static route for the SSE gateway #1 IP address (e.g., 192.168.15.1) with the VTI interface as the next hop.

Add Route - Segment : Default	
Subnet/Mask	192.168.15.1/32
Next Hop	192.168.10.2
Interface	vti1 (Optional) Zone None
Metric	50
Tag	FROM_LAN
Comments	Route-to-Endpoint1-via-INET1_Tunnel

Subnet/Mask: Enter the BGP peer address of the SSE gateway.

Next Hop: Enter the IP address of the VTI interface.

Interface: Select the VTI interface from the menu.





Metric: Enter **50**.

Tag: Select **FROM_LAN**.



- 5. Click **Add** and then click **Save**.

The static route you added appears in the Routes dialog box for the gateway.

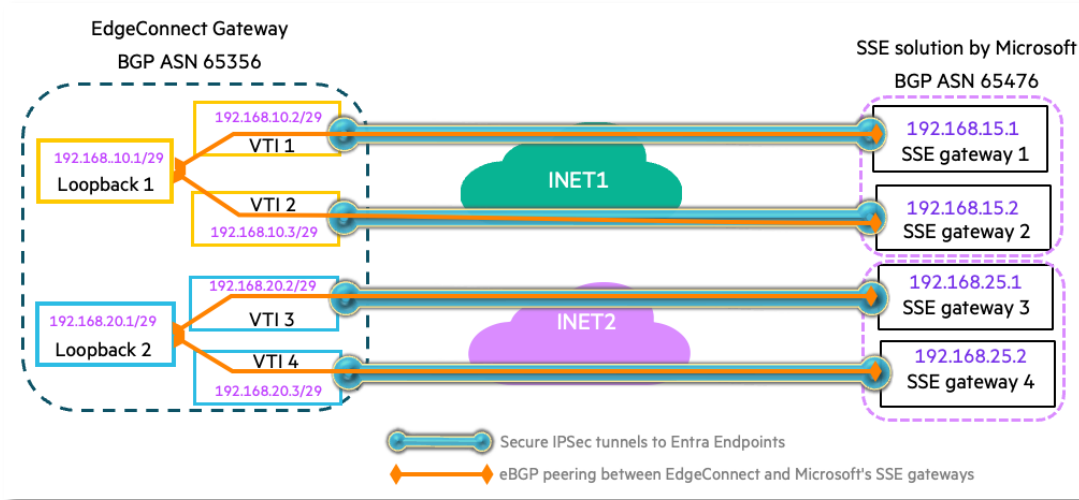
4 Rows							
Edit	Subnet/Mask	Next Hop ▲	Interfac...	State	Additional Info	Comment	Metric
	192.168.15.1/32	192.168.10.2	vti1	UP	Tag FROM_LAN	INET1_POP1-BPG Peer	50
	192.168.15.2/32	192.168.10.3	vti2	UP	Tag FROM_LAN	INET1_POP2-BPG Peer	50
	192.168.25.1/32	192.168.20.2	vti3	UP	Tag FROM_LAN	INET2_POP3-BPG Peer	50
	192.168.25.2/32	192.168.20.3	vti4	UP	Tag FROM_LAN	INET2_POP4-BPG Peer	50

- 6. Repeat Steps 3 to 5 for additional static route entries.



8.4 Create BGP Neighborhood

NOTE: One BGP neighbor configuration per gateway is required. In this example, four BGP neighbor configurations are required.



1. In Orchestrator, select your EdgeConnect gateway from the appliance tree.
2. Navigate to **Configuration > Networking > Routing > BGP**.
The BGP tab opens.
3. Click the edit icon next to the gateway name.
The BGP dialog box for the gateway opens.
4. Enable BGP, and then set the Autonomous System Number and the Router ID, as shown in the following example. Leave the rest of the settings as is.

BGP - Store101-EC1 - Segment : Default

BGP Information ?

Enable BGP

Autonomous system number

Router ID
(Router ID is common for BGP and OSPF; changing it here will update it for OSPF)

Graceful restart

Max restart time (1..3600) Sec

Stale path time (1..3600) Sec

AS path propagate

Log BGP update messages

Enable BGP: Move the toggle to enable this setting.

Autonomous system number: Enter the ASN number that you have configured. Refer to the Remote network configuration downloaded from Microsoft Entra.

Router ID: Enter your loopback address. In this example a unique Router ID is provided.

NOTE: Leave the rest of the settings as is.

5. To add the SSE gateways as a BGP neighbor, In the BGP Peers section, click **Add**.
The Add Peer dialog box opens.



- Enter the settings in the Add Peer dialog box using the information in the [Remote network configuration](#) file that you downloaded and as shown in the following example.

Add Peer - Segment : Default X

BGP Peer Information ?

Peer IP:

Peer Adjacency:

Local Interface:

Peer ASN:

Override ASN:

Peer Type:

Routes learned from PE-router peer will not be advertised to SD-WAN Fabric.

Admin Status:

Soft Reconfiguration:

Next-Hop-Self:

Inbound route map:

Outbound route map:

Peer IP: Enter the BGP peer IP address of the SSE gateway.

Peer Adjacency: Click **Single-Hop**.

Local Interface: Select the loopback interface that corresponds to this SSE gateway peer.

Peer ASN: Enter the ASN number of the SSE gateway.

NOTE: Leave the rest of the settings as is.

- Click **Add**.
- The BGP peer you added appears in the BGP dialog box for the gateway.
- Repeat Steps 5 to 7 for the other SSE gateway peers.
- When you are done adding peers to the gateway, click **Save** to close the BGP dialog box for the gateway.

If the passthrough tunnel, VTI interface, and static route for the SSE gateways are configured correctly then the EdgeConnect gateway should appear on the BGP tab with a Peer State status of “Established,” as shown in the following figure.

BGP ?

7 Rows

Edit	Appliance	Segment	Peer IP	Local Interface	Peer ASN	Peer State	Soft Reset	Establishe...	Inbound Route Map	Outbound Route Map
	Store101-EC1	Default	192.168.15.1	lo1	65476	Established	<input type="button" value="Soft Reset"/>	45m 41s	default_rtmap_bgp_inbound_br	default_rtmap_bgp_outbound_br
	Store101-EC1	Default	192.168.15.2	lo1	65476	Established	<input type="button" value="Soft Reset"/>	45m 16s	default_rtmap_bgp_inbound_br	default_rtmap_bgp_outbound_br
	Store101-EC1	Default	192.168.25.1	lo2	65476	Established	<input type="button" value="Soft Reset"/>	45m 17s	default_rtmap_bgp_inbound_br	default_rtmap_bgp_outbound_br
	Store101-EC1	Default	192.168.25.2	lo2	65476	Established	<input type="button" value="Soft Reset"/>	45m 19s	default_rtmap_bgp_inbound_br	default_rtmap_bgp_outbound_br

- Verify the routes coming from the SSE gateway by navigating to **Configuration > Networking > Routing > Routes**. Enter the ASN number of the SSE gateway in the Search field to filter the list, as shown in the following figure.

Routes ?

27/31 Rows

Search 65476

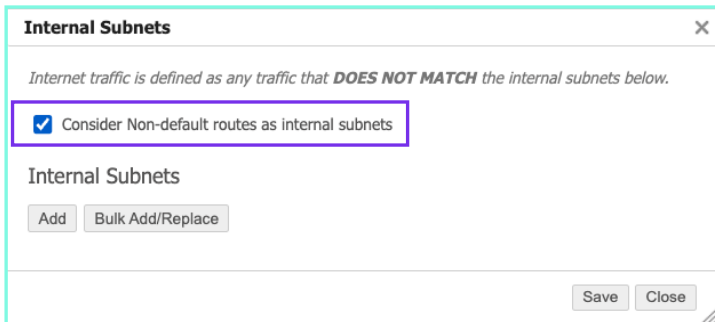
Edit	Appliance	Segment	Subnet/Mask	Next Hop	Interface	Type	State	Additional Info
	Store101-EC1	Default	204.79.197.215/32	192.168.10.2 (Original nexthop 192.168.15.1)	vti1(vti1)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	131.253.33.215/32	192.168.10.2 (Original nexthop 192.168.15.1)	vti1(vti1)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	52.244.160.207/32	192.168.10.2 (Original nexthop 192.168.15.1)	vti1(vti1)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	52.244.37.168/32	192.168.10.2 (Original nexthop 192.168.15.1)	vti1(vti1)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	52.238.119.141/32	192.168.10.2 (Original nexthop 192.168.15.1)	vti1(vti1)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	13.107.140.6/32	192.168.10.2 (Original nexthop 192.168.15.1)	vti1(vti1)	EBGP:192.168.15.1	UP	AS Path 65476



8.5 Enable the “Consider Non-default routes as internal subnets” Option

To use the routes shared by SSE gateways to redirect traffic via tunnels, you need to configure the SSE gateway routes as internal subnets from an EdgeConnect gateway perspective.

1. In Orchestrator, navigate to **Configuration > Overlays & Security > Business Intent Overlays**.
The Business Intent Overlays tab opens.
2. Click the edit icon next SD-WAN Traffic to Internal Subnets.
The Internal Subnets dialog box opens.
3. Click the **Consider Non-default routes as internal subnets** check box.

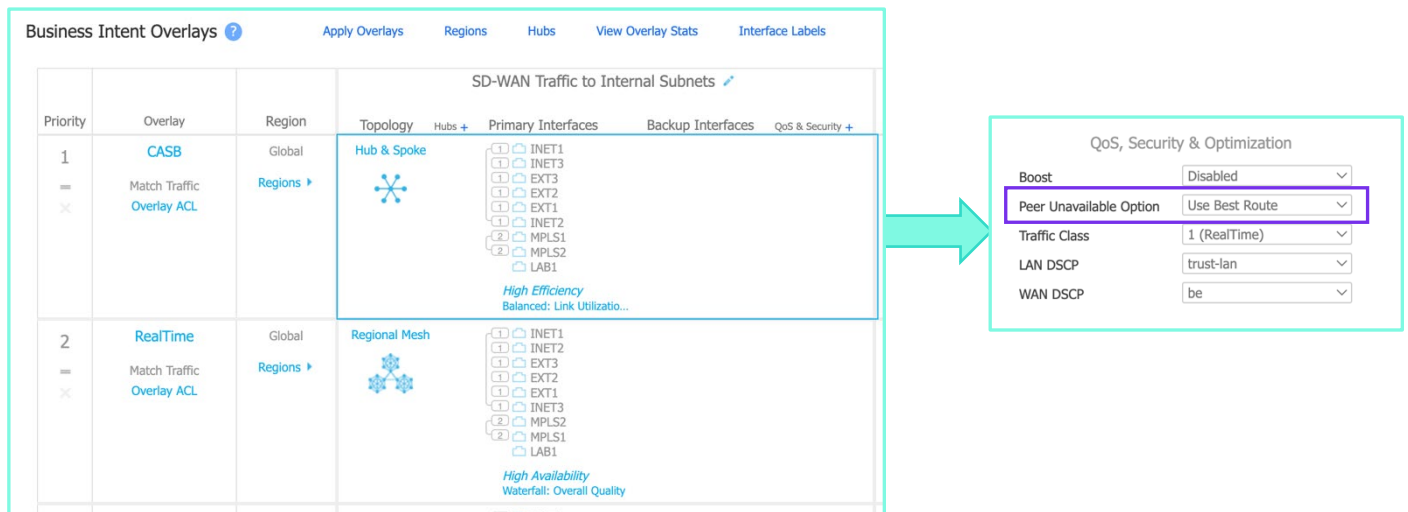


4. Click **Save** and then click **OK**.

8.6 Change the Business Internet Overlay to Use Best Route

Business Intent Overlays on the EdgeConnect gateways default to Drop for the Peer Unavailable Option setting. In this section, you modify this setting for the existing Business Intent Overlays to use the best available routes (Use Best Route) on the EdgeConnect, so traffic gets redirected to the SSE gateways.

1. Navigate to **Configuration > Overlays & Security > Business Intent Overlays**.
The Business Intent Overlays tab opens.
2. Click a Business Intent Overlay and select **Use Best Route** from the Peer Unavailable Option menu (SD-WAN Traffic to Internal Subnets > QoS, Security & Optimization).
[Repeat this step for ALL overlays.](#)



8.7 Configure Active-Active or Active-Backup Load Balancing

By default, an EdgeConnect gateway prefers a single route as the best route in its route table. So, traffic is always placed on a single path (e.g., a tunnel towards the SSE gateways). To achieve active-backup load balancing on tunnels, no additional configuration is required except to make sure ECMP is disabled on the EdgeConnect gateway.

Equal Cost Multi Path (ECMP) allows traffic to be carried on multiple paths simultaneously when more than one equal cost route to a destination exists on the EdgeConnect gateway. ECMP is disabled on the EdgeConnect gateway by default. You can enable ECMP on the Routes tab to achieve active-active load balancing.

NOTE: This setting is common for all VRF segments when enabled ECMP is applied to all the VRF segments (if VRF is configured in your environment).

1. In Orchestrator, navigate to **Configuration > Networking > Routing > Routes** and click the edit icon next to the hostname. The following example is on the default segment.

Routes - RKAWS-East-EC01 - Segment : Default

Routes ?

Automatically advertise local LAN subnets

Automatically advertise local WAN subnets

Metric for automatically added routes

Redistribute routes to SD-WAN fabric

Filter routes from SD-WAN fabric with matching local ASN

Include BGP local ASN to routes sent to SD-WAN fabric

Tag BGP communities to routes

Common settings for all segments

Use SD-WAN fabric learned routes

Enable Equal Cost Multi Path (ECMP)

2. Navigate to **Configuration > Networking > Routing > Routes** and verify that multiple paths for the same destination are installed on the route table. Enter the ASN number of the SSE gateway in the Search field to filter the list, as shown in the following figure.

Routes ?

108/115 Rows Search 65476

Edit	Appliance	Segment	Subnet/Mask ▲	Next Hop	Interface	Type	State	Additional Info
	Store101-EC1	Default	204.79.197.215/32	192.168.10.2 (Original nexthop 192.168.15.1)	vti1(vti1)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	204.79.197.215/32	192.168.20.2 (Original nexthop 192.168.25.1)	vti3(vti3)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	204.79.197.215/32	192.168.20.3 (Original nexthop 192.168.25.2)	vti4(vti4)	EBGP:192.168.15.1	UP	AS Path 65476
	Store101-EC1	Default	204.79.197.215/32	192.168.10.3 (Original nexthop 192.168.15.2)	vti2(vti2)	EBGP:192.168.15.1	UP	AS Path 65476

In this example, route 204.79.197.215/32 is learned from four different eBGP peers. This confirms that ECMP is working.



8.8 Verify Traffic flows on the EdgeConnect Gateway

In Orchestrator, navigate to **Monitoring > Bandwidth > Flows > Active & Recent Flows**. Check your user traffic flows by filtering based on the user IP address or the application. The following figure shows an example of a flow that is filtered based on IP address:

Inbound/Outbound Tunnel shows "Entra_Primary_INET1_POP1" as the traffic path.

Click the info icon to view additional flow details.



You have completed all the tasks required for establishing an IPsec tunnel with the SSE solution and traffic redirection to SSE gateways using BGP integration.

