



HPE Aruba Networking EdgeConnect and HPE Aruba Networking SSE Secure Web Gateway

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 D, March 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



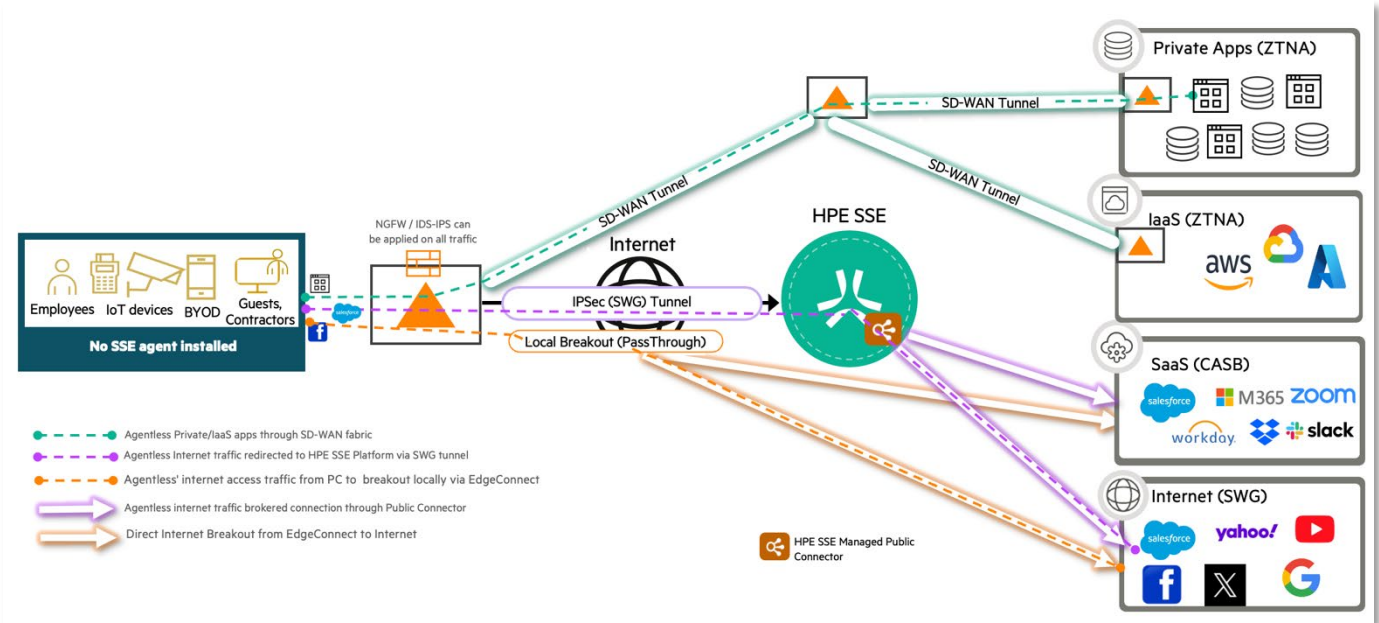
Contents

1.	Overview	3
2.	Topology	3
3.	Before You Begin – Configure Loopback Interface	5
4.	Orchestrator Configuration.....	6
4.1.	Finding the Closest HPE SSE Remote Endpoints – Geo DNS Lookup.....	6
4.2.	Remote Endpoint Configuration	7
4.3.	Interface Labels.....	9
4.4.	Tunnel Settings	9
4.5.	IP SLA	11
4.6.	BIO Breakout.....	12
4.7.	Remote Endpoint Association	13
4.8.	Collect IKE Identifier Details from Orchestrator	14
4.9.	Change Default MSS Settings for the EdgeConnect Gateways	14
5.	HPE SSE Management Console Configuration.....	16
5.1.	Configure Branches as Locations	16
5.2.	Configure IPsec Tunnel.....	18
6.	Verify Service Orchestration Configuration Push to Devices	19
7.	Verify Tunnel Status and IP SLA Status	20
7.1.	Passthrough Tunnel Status.....	20
7.2.	IP SLA Status	21
8.	Traffic Redirection to HPE SSE Using Business Intent Overlay.....	22
8.1.	Send HPE-SSE Application traffic via Local Break Out.....	22
8.2.	Send Internet Traffic to HPE SSE Cloud	23
9.	Inspecting Branch Traffic at the HPE SSE Cloud	25
9.1.	External Web Profiles.....	27
9.2.	File Security Profile	28
9.3.	Example 1 – Policy to Redirect Traffic to Permit Internet Access.....	28
9.4.	Example 2 - Web Filtering / URL Filtering Based on Web Categories	29
9.5.	Example 3 – Prevent Download/Upload of Files.....	30
9.6.	Example 4 – “Break out” Private Apps Traffic via EdgeConnect Instead of Agent Tunnel.....	32
10.	Verify Active Flows on the Orchestrator	34
11.	Verify Traffic Flows on the HPE SSE Management Console	34



1. Overview

This document details the configurations required on the HPE Aruba Networking Orchestrator and HPE SSE Management Console portal to provision IPsec tunnels between an EdgeConnect SD-WAN gateway and HPE SSE Secure Web Gateway (SWG) endpoints. The Service Orchestration feature on Orchestrator can be used to orchestrate IPsec tunnel configuration for the SD-WAN fabric, which comprises multiple EdgeConnect gateways.



2. Topology

The Service Orchestration feature in Orchestrator builds a configuration for each EdgeConnect gateway in the fabric and pushes it to the EdgeConnect gateways.

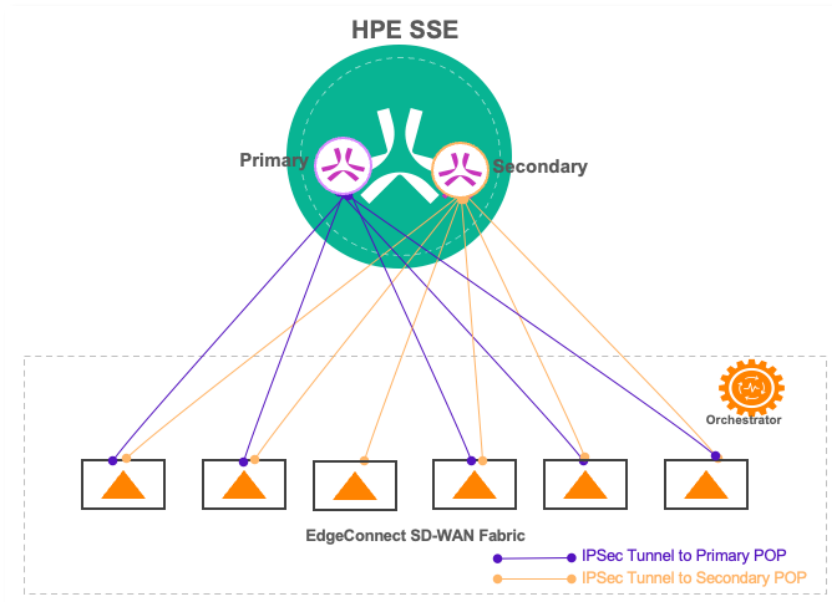


Figure 1: Orchestrated Tunnels to HPE SSE SWG



IPsec tunnels to SWG endpoints can be deployed in a single gateway site or sites with EdgeHA deployment, which involves two gateways and multiple uplinks. If configured, Service Orchestration pushes the IPsec tunnel configuration to the gateways to build tunnels using all available uplinks.

The following figure shows a simple topology: a single EdgeConnect SD-WAN gateways with one ISP connection.

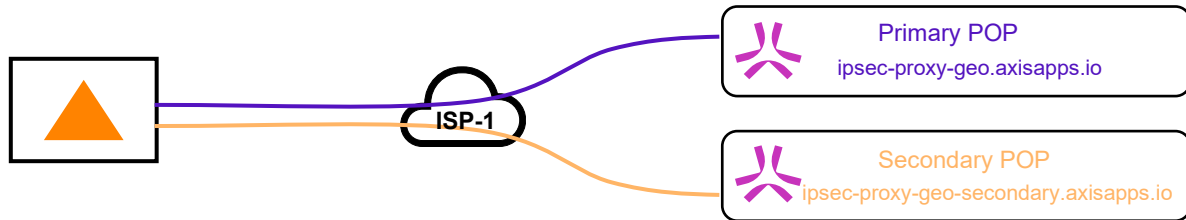


Figure 2: Single Gateway Topology

The following figure shows EdgeHA topology: two EdgeConnect SD-WAN gateways sharing their uplink connection. In this case, Service Orchestration builds tunnels using the uplink from each gateway.

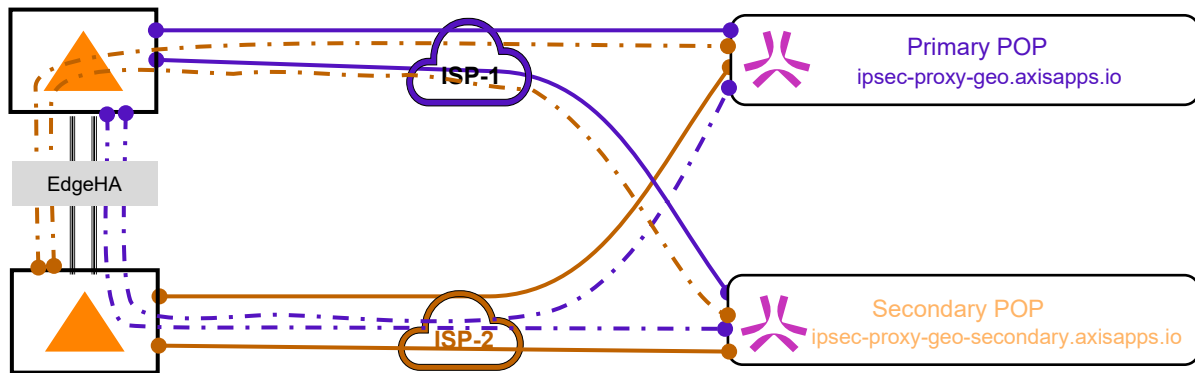


Figure 3: Dual EdgeConnect in EdgeHA Deployment



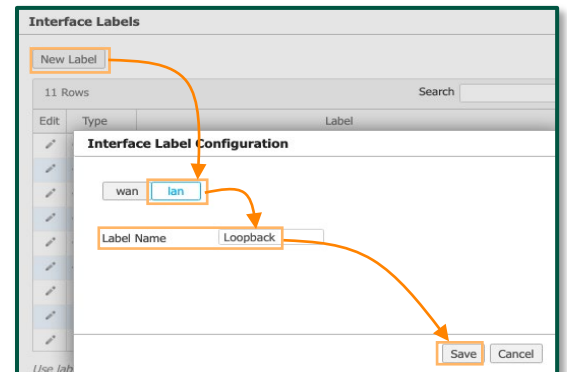
3. Before You Begin – Configure Loopback Interface

Before you set up Service Orchestration configuration, it is important to ensure that each EdgeConnect gateway has at least one valid loopback interface with IP address. The EdgeConnect gateway uses the loopback interface (label) as the source interface when it sends IP SLA probes to the destination.

If you have a loopback interface configured on the EdgeConnect, you do not need to create a new one. Proceed to the next section.

HPE Aruba Networking recommends using the Loopback Orchestration feature to automatically assign a loopback address to each EdgeConnect managed by the Orchestrator from a group of address pools. You can create a pool of loopback addresses for Orchestrator to automatically create one or more loopback interfaces. You can also assign IP addresses from the pool to each gateway in the network. Complete the following steps to set up loopback orchestration:

1. Navigate to **Configuration > Overlay & Security > Interface Labels**.
2. Click **New Label**, select **LAN**, and then enter a name (for example, Loopback).
3. Click **Save**.



4. Navigate to **Configuration > Networking > Loopback Orchestration**.
5. Select **+Add Loopback Interface**.

The **Loopback Interface** dialog box opens.

6. Select the **Label** you configured in step 2 from the drop-down list.
7. Specify the firewall zone if you want the loopback interface to be part of a specific firewall zone.
8. Select the **Management** check box if you want the interface to be used by management applications running on the gateway.
9. Click **Add**.

Loopback Orchestration NOTE: Management					
+Add Loopback Interface Segment <input type="text" value="All"/>					
1 Rows					
Segment	Label ▲	Zone	Management IP	Loopback Pool	Allocated / Total
Default	Loopback	Management	Yes	172.23.1.0/27	5 / 32

Figure 4: Loopback Orchestration



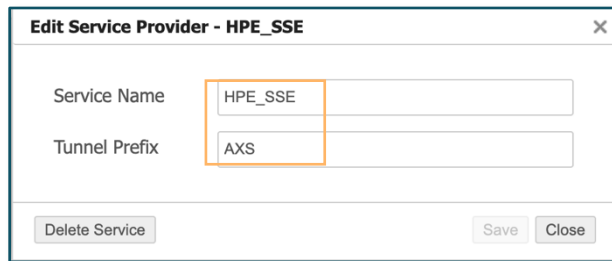
4. Orchestrator Configuration

The Service Orchestration feature orchestrates tunnel configuration for all gateways managed by Orchestrator.

1. Log in to your Orchestrator.
2. Navigate to **Configuration > Cloud Services > Service Orchestration**, and then click **+Add Service**.

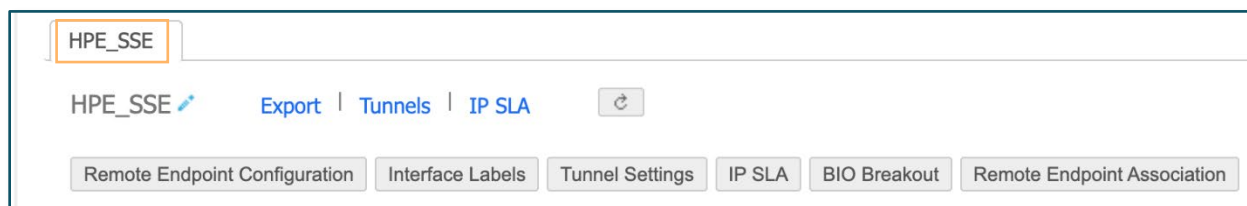
The Add Service dialog box opens.

3. Enter "HPE_SSE" in the Name field and "AXS" in the Prefix field, and then click **Save**.



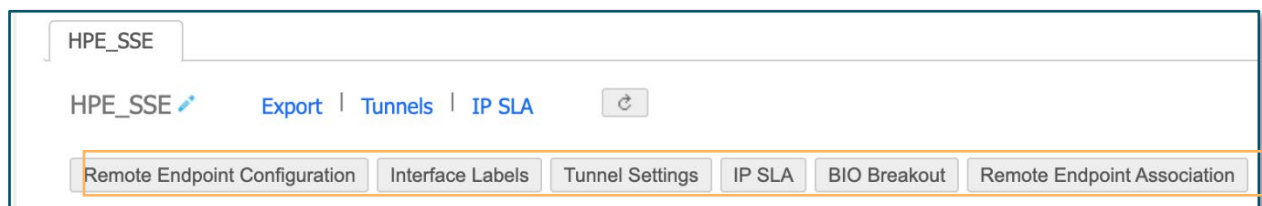
The screenshot shows a dialog box titled "Edit Service Provider - HPE_SSE". It has two input fields: "Service Name" with the value "HPE_SSE" and "Tunnel Prefix" with the value "AXS". Below the fields are three buttons: "Delete Service", "Save", and "Close".

A new tab called HPE_SSE is created on the Service Orchestration page.



The screenshot shows the Service Orchestration page with a tab labeled "HPE_SSE" selected. Below the tab, there are several configuration options: "Remote Endpoint Configuration", "Interface Labels", "Tunnel Settings", "IP SLA", "BIO Breakout", and "Remote Endpoint Association".

The following sections explain how to configure each of the tabs for the HPE_SSE service.



The screenshot shows the Service Orchestration page with the "HPE_SSE" tab selected. The "Remote Endpoint Configuration" tab is highlighted with an orange box.

4.1. Finding the Closest HPE SSE Remote Endpoints – Geo DNS Lookup

To build tunnels from EdgeConnect to HPE SSE SWG endpoints, use the primary and secondary DNS names below. When an individual EdgeConnect resolves these fully qualified domain names (FQDNs), it resolves to the nearest SSE POP (point-of-presence) endpoints based on the geolocation from where the DNS query was made. This results in EdgeConnect automatically picking up the nearest POP location to build tunnels.

ipsec-proxy-geo.axisapps.io

ipsec-proxy-secondary-geo.axisapps.io



4.2. Remote Endpoint Configuration

This section explains how to configure the primary and secondary SSE POP endpoints using the FQDN identified in [Section 4.1](#) and a pre-shared key. First, add the Secondary POP endpoint, then configure the Primary POP endpoint, and finally map the Secondary POP endpoint as a backup.

1. Click **Remote Endpoint Configuration**.
2. To add a row, click **+Remote Endpoint**.
3. Enter the following:

The screenshot shows the 'Add Remote Endpoints for HPE_SSE' interface. At the top, there are buttons for '+Remote Endpoint', 'Interface Label Default', 'PSK Default', 'Import', and 'Export'. Below these is a search bar and a table with 2 rows. The table has columns for Name, IP Address, Interface Label, Pre-shared Key, Probe Address, and Backup Remote Endp... The first row is highlighted and has the following values: Name: Secondary, IP Address: ipsec-proxy-secondary-geo.axisapps.io, Interface Label: any, Pre-shared Key: *****.

Field	Value
Name	Secondary
IP Address	ipsec-proxy-secondary-geo.axisapps.io
Interface Label	any
Pre-shared Key	Enter a pre-shared key.

4. To add an additional row, click **+Remote Endpoint again**.
5. Enter the following:

The screenshot shows the 'Add Remote Endpoints for HPE_SSE' interface with 4 rows, 1 selected. The table has columns for Name, IP Address, Interface Label, Pre-shared Key, Probe Address, and Backup Remote En... The first row is highlighted and has the following values: Name: Primary, IP Address: ipsec-proxy-secondar..., Interface Label: any, Pre-shared Key: *****. The second row has the following values: Name: Secondary, IP Address: ipsec-proxy-geo.axisa..., Interface Label: any, Pre-shared Key: *****.

Field	Value
Name	Primary
IP Address	ipsec-proxy-geo.axisapps.io
Interface Label	any



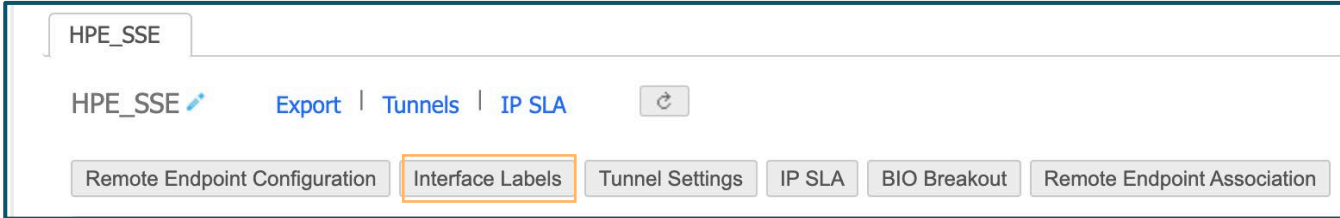
Field	Value
Pre-shared Key	Enter the same pre-shared key that was set for secondary.
Backup Remote Endpoint	Secondary

NOTE: In steps 3 and 5, the interface label is configured as “any.” This means the Orchestrator will use all available WAN interfaces configured under Interface Labels to build the tunnel configuration.



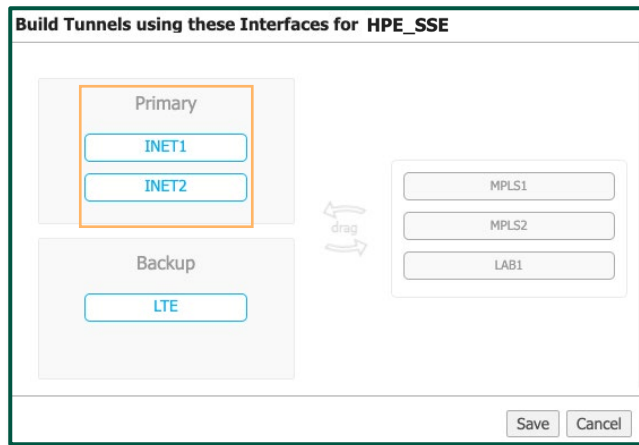
4.3. Interface Labels

This section explains how to select the uplink interfaces (labels) used to build tunnels to SSE primary and secondary POP endpoints.



1. Click **Interface Labels**.

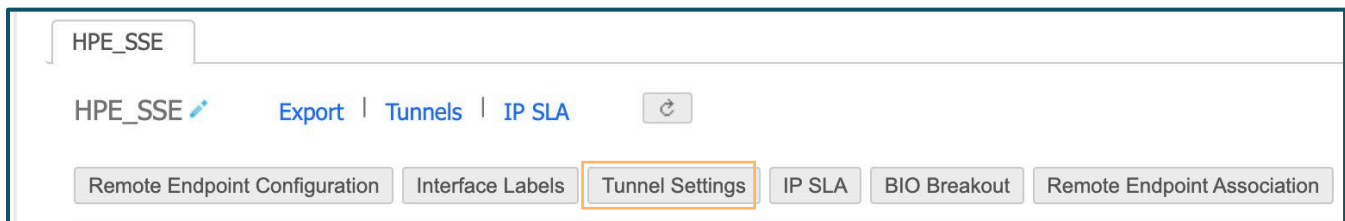
Select all WAN Interface labels that your SD-WAN fabric is using. Service Orchestration prepares IPsec tunnel configuration for each WAN interface selected.



2. Click **Save**.

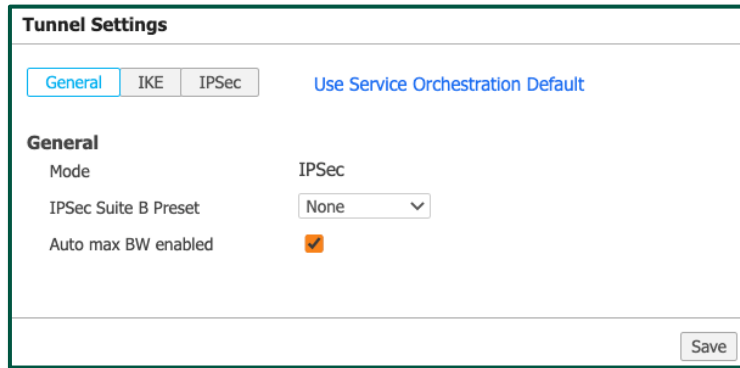
4.4. Tunnel Settings

This section explains how to configure the IKE-Phase1 and Phase-2 settings that the EdgeConnect gateway uses to build tunnels to the SSE POP endpoints.



1. Click **Tunnel Settings**.
2. Configure the General tab, as shown in the following figure:





3. Configure the IKE and IPSec tabs, as shown in the following figures.

NOTE: You can dynamically configure the IKE identifier field using one of the variables shown in [Figure 5](#). This example uses `%hostname%_%label%@RKLAB.COM`. The domain name can be anything that uniquely identifies your SD-WAN fabric.

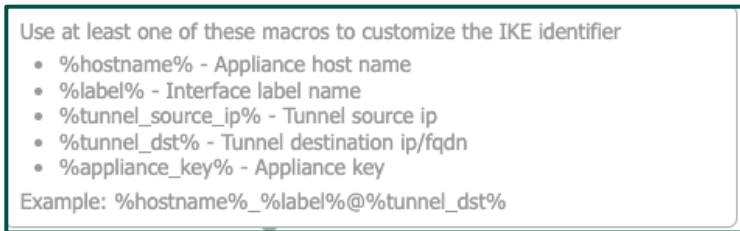
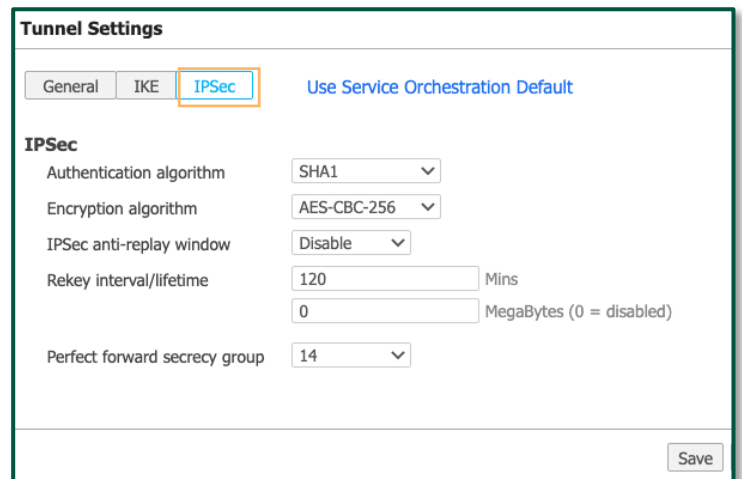
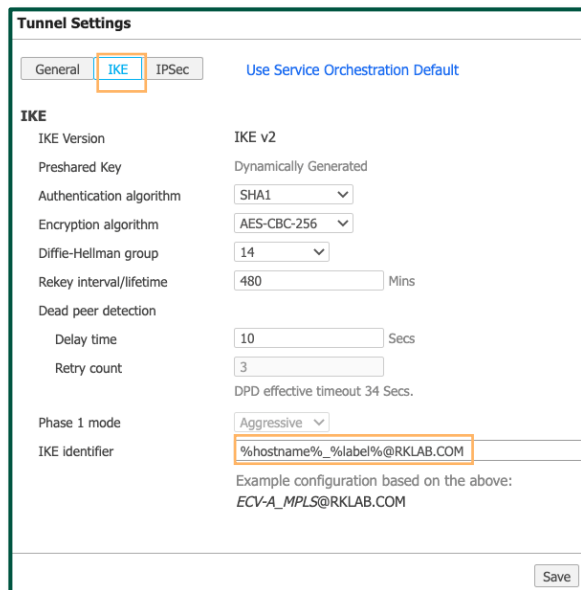


Figure 5: IKE Identifier Variables Available to Use

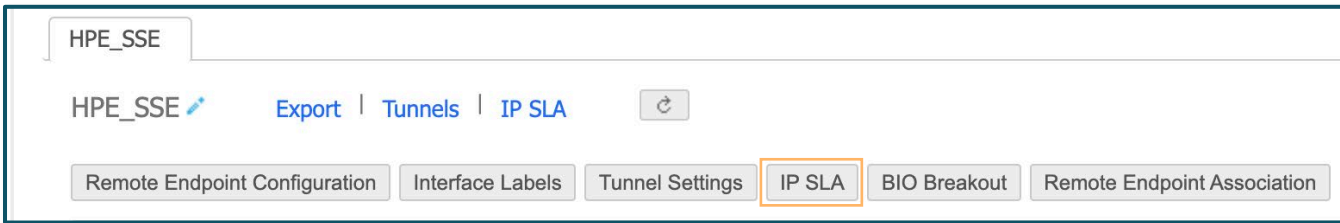


4. Click **Save**.

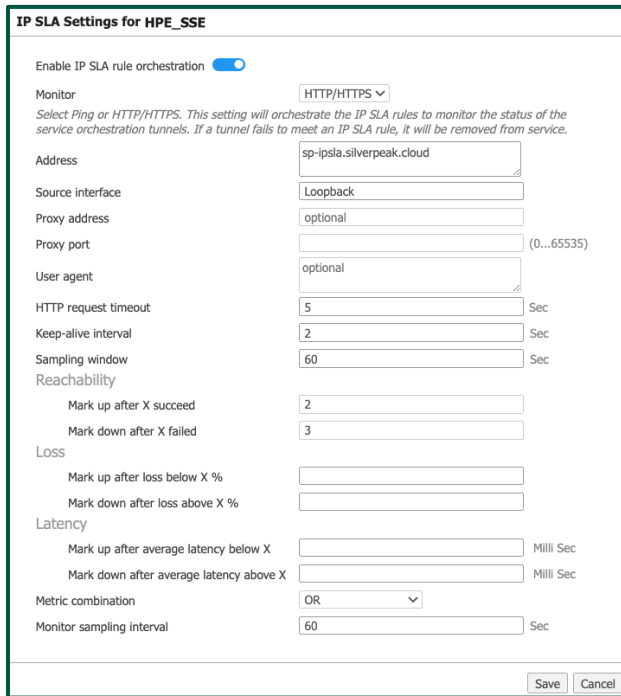


4.5. IP SLA

This section explains how to enable IP SLA settings so the EdgeConnect can monitor tunnel health using an HTTPS probe to sp-ipsla.silverpeak.cloud. You can customize the probe destination URL in this setting.



1. Click **IP SLA**.
2. Configure the settings on the IP SLA Settings for HPE_SSE dialog box, as shown in the following figure. Take special care to ensure that the settings in the following table are configured correctly.



Field	Value
Enable IP SLA rule orchestration	Enabled
Monitor	HTTP/HTTPS
Address	ip-sla.silverpeak.cloud
Source interface	Select the interface label from the drop-down list. In this example, Loopback is selected. IP SLA uses this label to source probe traffic to

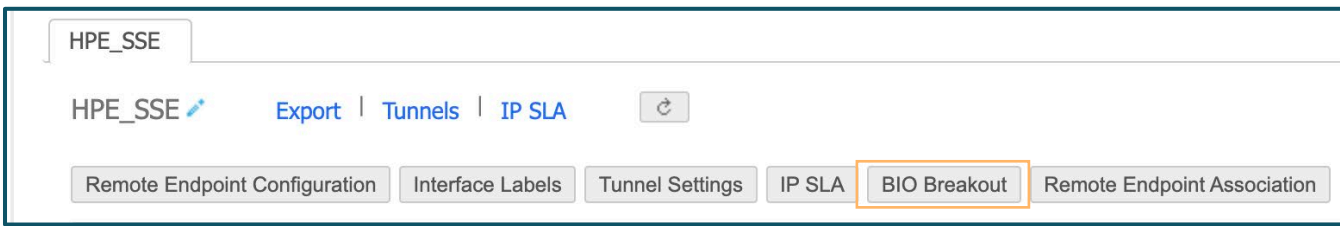


Field	Value
	the probe destination address. Note that for the IP SLA profile to be pushed to the SD-WAN gateways, there must be at least one interface on the gateway with the matching label.
HTTP request timeout	2

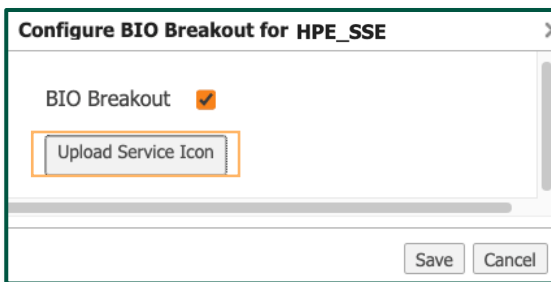
3. Click **Save**.

4.6. BIO Breakout

This section explains how to ensure that the tunnels created for the SSE endpoints are added to the Business Intent Overlay (BIO) as a service.



1. Click **BIO Breakout**.
2. Ensure that the **BIO Breakout** check box is selected.

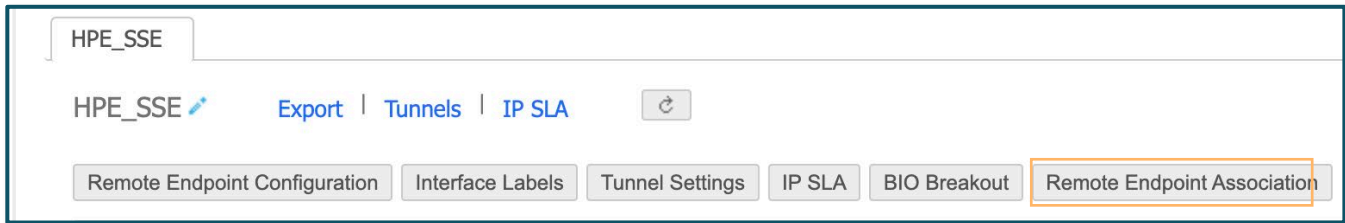


3. (Optional) If an icon must be visible on the BIO, upload a service icon (image size must be less than 20 KB).
4. Click **Save**.

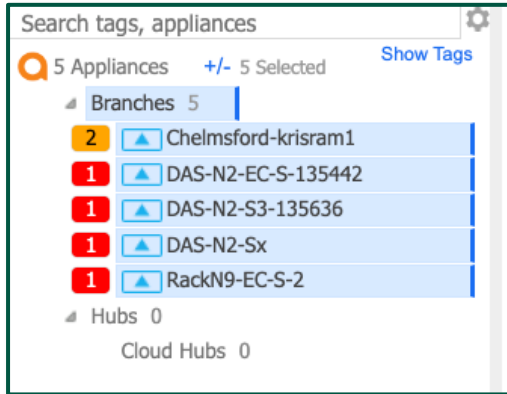


4.7. Remote Endpoint Association

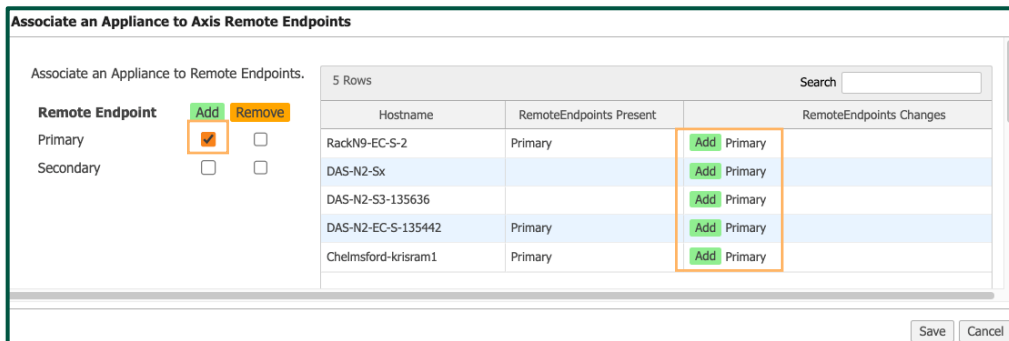
This section explains how to associate the HPE SSE endpoints to the EdgeConnect SD-WAN gateways. When association is completed, Orchestrator pushes the required IPsec tunnel configuration and IP SLA configurations to the EdgeConnect gateways.



1. In Orchestrator, select the gateways from the appliance tree. This example associates all gateways with the SSE endpoints.



2. Click **Remote Endpoint Association**.
3. Select the **Add** check box next to Primary. This associates both the primary and secondary SSE endpoints with the selected EdgeConnect SD-WAN gateways.

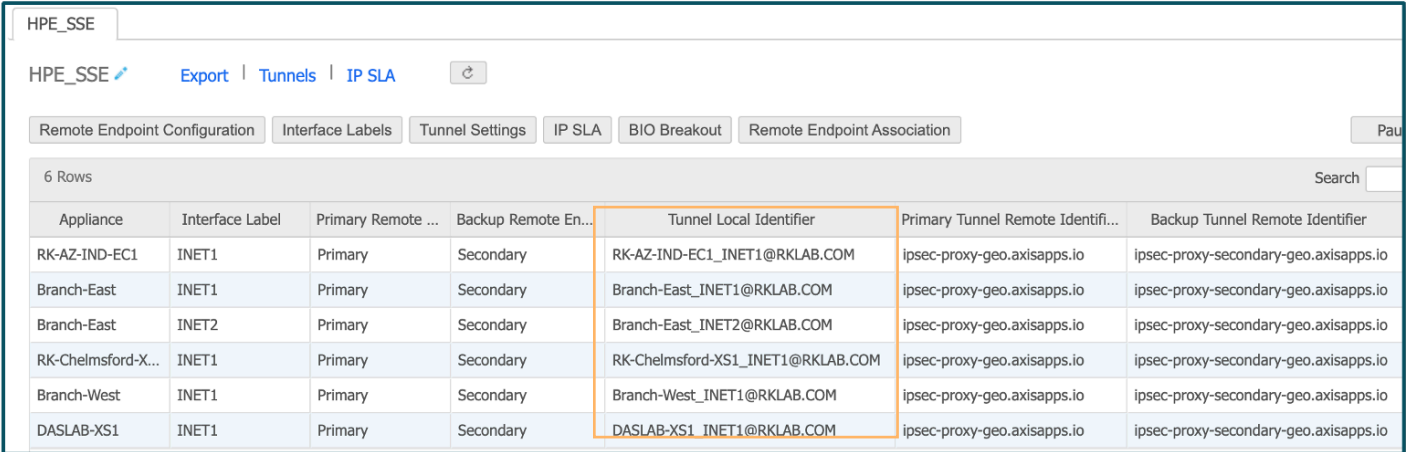


4. Click **Save**.



4.8. Collect IKE Identifier Details from Orchestrator

When the Remote Endpoint Association is completed, Orchestrator pushes the tunnel configurations to each of the EdgeConnect gateways.



Appliance	Interface Label	Primary Remote ...	Backup Remote En...	Tunnel Local Identifier	Primary Tunnel Remote Identifi...	Backup Tunnel Remote Identifier
RK-AZ-IND-EC1	INET1	Primary	Secondary	RK-AZ-IND-EC1_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
Branch-East	INET1	Primary	Secondary	Branch-East_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
Branch-East	INET2	Primary	Secondary	Branch-East_INET2@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
RK-Chelmsford-X...	INET1	Primary	Secondary	RK-Chelmsford-XS1_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
Branch-West	INET1	Primary	Secondary	Branch-West_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
DASLAB-XS1	INET1	Primary	Secondary	DASLAB-XS1_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io

After a few minutes, the Service Orchestration page auto populates the Tunnel Local Identifier field for each of the EdgeConnect gateways. Record the identifier details for each gateway because you will use those details in [Section 5](#) to configure the “IKE Identifier” on the SSE Management Console under **Settings > Connector > Tunnels > New IPsec Tunnel**.

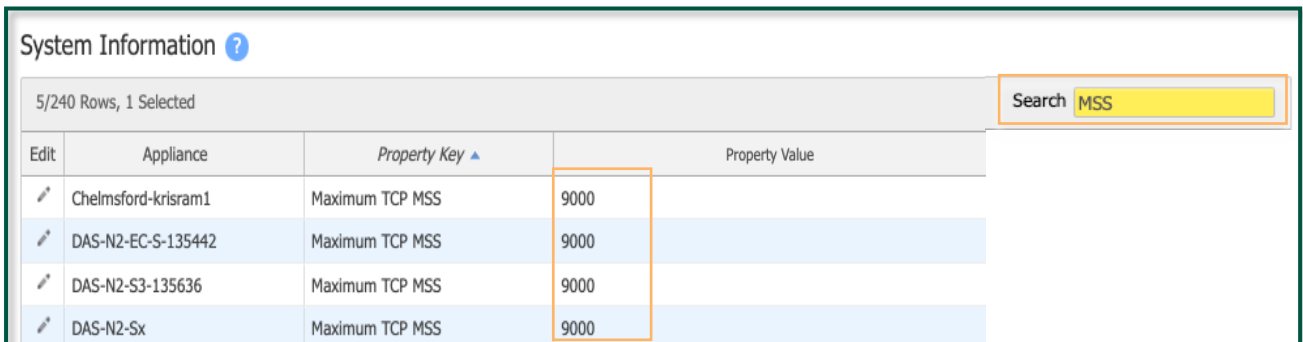
4.9. Change Default MSS Settings for the EdgeConnect Gateways

By default, the TCP MSS setting for the gateway is set at 9000. This may cause web traffic to be dropped at the Secure Web Gateway. HPE Aruba Networking recommends modifying the TCP MSS value for the gateway either per gateway level or using template-based configuration.

You can follow one of the two methods to change the TCP MSS value. HPE Aruba Networking always recommends using template-based configuration.

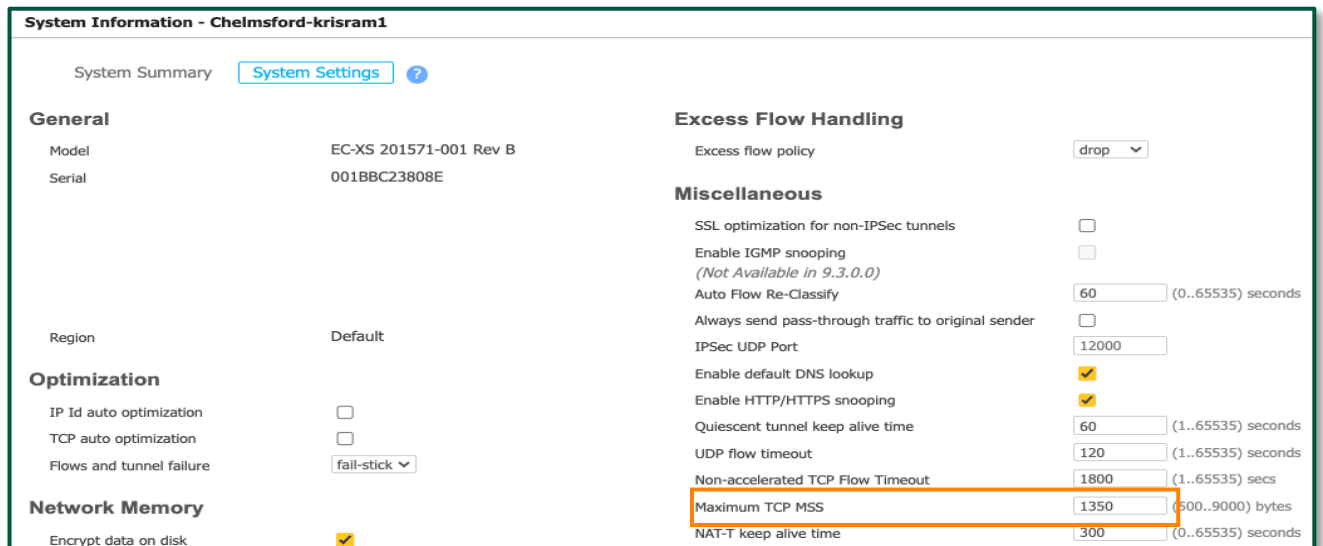
Per Gateway Level TCP - MSS Change

1. Select the gateways from the appliance tree. In Orchestrator, navigate to **Administration > Software > Upgrade > System Information** and use the search box to search for the keyword “MSS” to view the current MSS setting:



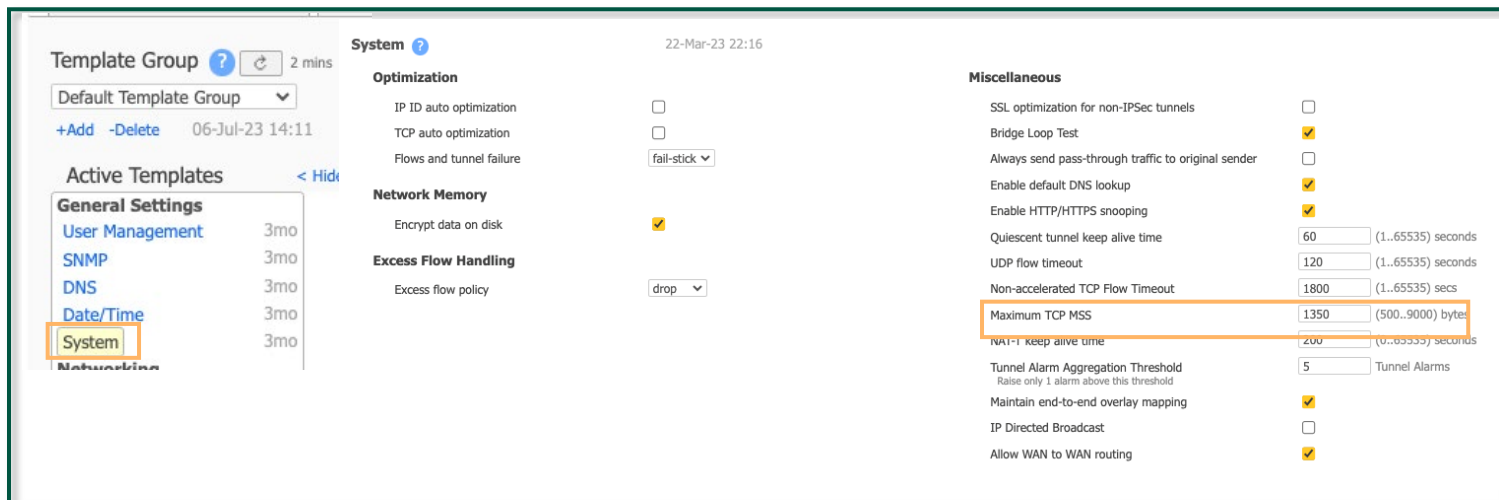
Edit	Appliance	Property Key ▲	Property Value
	Chelmsford-krisram1	Maximum TCP MSS	9000
	DAS-N2-EC-S-135442	Maximum TCP MSS	9000
	DAS-N2-S3-135636	Maximum TCP MSS	9000
	DAS-N2-Sx	Maximum TCP MSS	9000

2. Click the edit icon next to each gateway and set Maximum TCP MSS to “1350” (from the default of 9000).



Template Based TCP - MSS Change

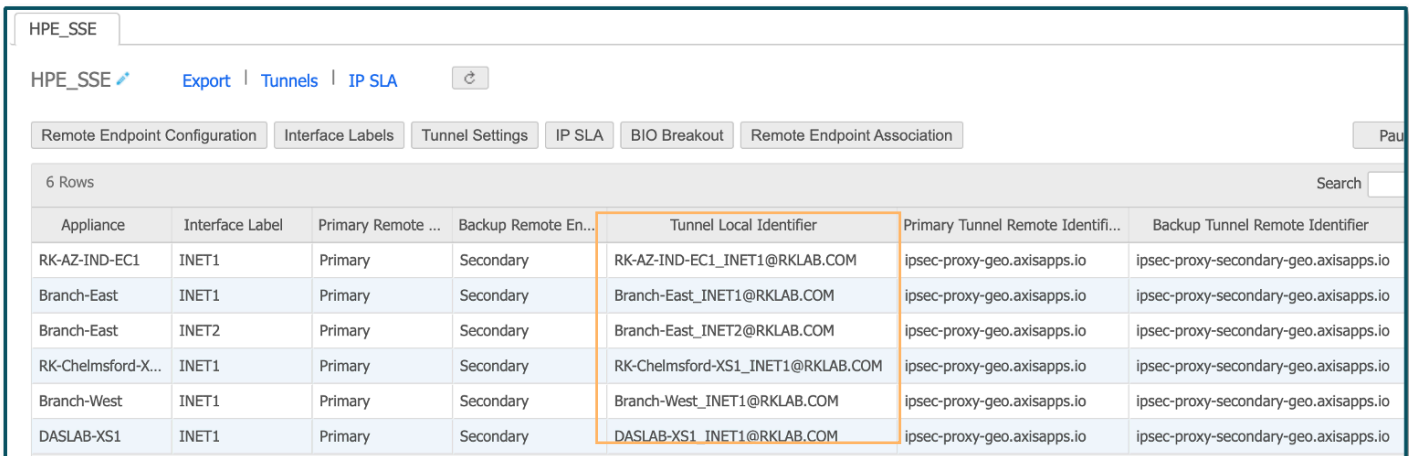
1. In Orchestrator, navigate to **Configuration > Templates & Policies > Templates > New / Existing Template groups**.
2. Use either an existing template group that has the System template already mapped to it or add the System template to the existing or new template group. In the following example, Default Template Group is used and it already has the System template mapped.
3. Set the Maximum TCP MSS value to “1350” (from the default of 9000), as shown in the following figure.



5. HPE SSE Management Console Configuration

This section explains how to complete configuration on the SSE Management console to provision tunnel and IP settings for each EdgeConnect gateway. You need the Tunnel Local Identifier information for each EdgeConnect gateway to proceed further in this section.

To obtain the IKE Identifier for each EdgeConnect from Orchestrator, navigate to **Configuration > Cloud Services > Service Orchestration** and refer to [Section 4.8](#).

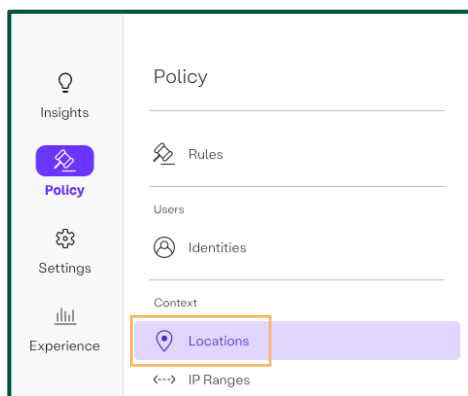


Appliance	Interface Label	Primary Remote ...	Backup Remote En...	Tunnel Local Identifier	Primary Tunnel Remote Identifi...	Backup Tunnel Remote Identifier
RK-AZ-IND-EC1	INET1	Primary	Secondary	RK-AZ-IND-EC1_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
Branch-East	INET1	Primary	Secondary	Branch-East_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
Branch-East	INET2	Primary	Secondary	Branch-East_INET2@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
RK-Chelmsford-X...	INET1	Primary	Secondary	RK-Chelmsford-XS1_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
Branch-West	INET1	Primary	Secondary	Branch-West_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io
DASLAB-XS1	INET1	Primary	Secondary	DASLAB-XS1_INET1@RKLAB.COM	ipsec-proxy-geo.axisapps.io	ipsec-proxy-secondary-geo.axisapps.io

5.1. Configure Branches as Locations

In this section, you will create one entry per site (Branch Location) irrespective of whether you have a single EdgeConnect or HA Pair at a given site/branch/location.

1. Log in to the SSE Management Console.
2. From the left sidebar of the Dashboard, navigate to **Policy > Locations**.

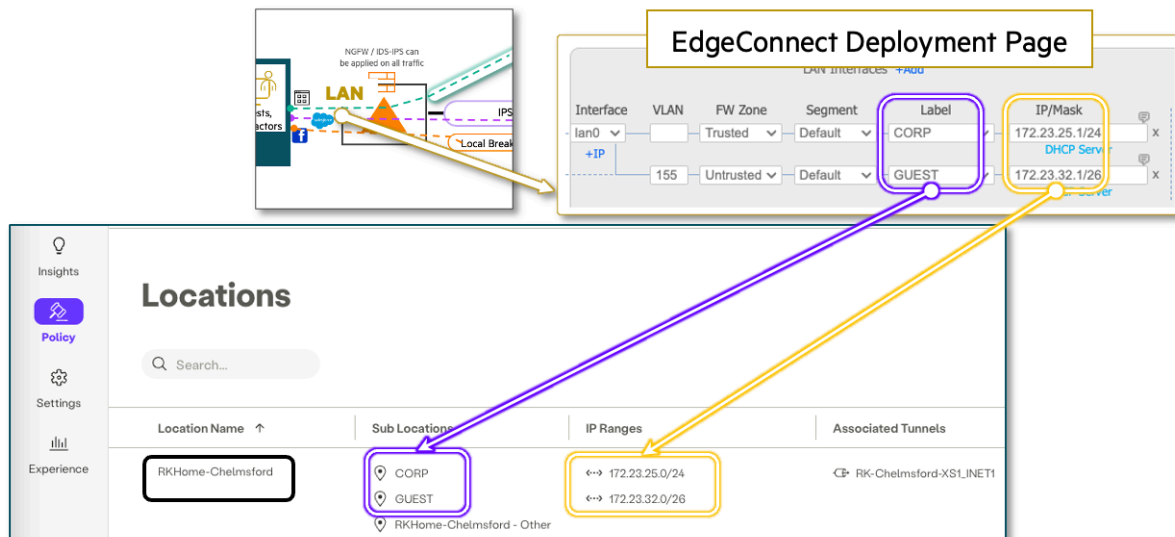


3. Click **New Location** to add a new location.



4. Add the Location Name and optionally add **Sublocations**. Sublocation provides a way to identify traffic coming from a specific subnet/network of the Branch (EdgeConnect) and the SSE policy can be applied specifically to those sublocations. This could be compared to “interface Label” on the EdgeConnect deployment page.
5. Click **Sub Location** to add the IP address detail for a sub-location under that location. You can enter a whole subnet or IP-range. In the following example, a location is added along with sub-location matching the interface labels CORP and GUEST.

NOTE: There is no direct relation between an EdgeConnect interface label and a sub-location. Label names are merely referred in this example for convenience and consistency.



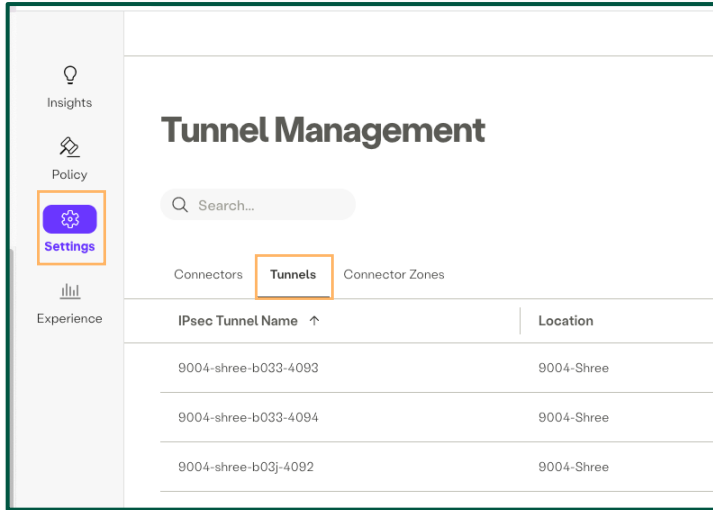
6. Click **Submit**.
7. To commit the changes, click **Apply Changes**.
8. Repeat the steps in this procedure for each branch location.



5.2. Configure IPsec Tunnel

In this section, you configure IPsec credentials (IKE ID and Pre-Shared Key) and map the tunnel credentials to the location that you added in the previous step.

1. From the left sidebar of the Dashboard, navigate to **Settings > Connectors > Tunnels**.



2. To add new IPsec tunnel settings, click **New IPsec Tunnel**.
3. Enter the IPsec Tunnel Name, IKE ID, PSK, and the pre-shared key used for IPsec negotiation.

The screenshot shows the 'New Tunnel' configuration form. It has a title bar with a close button. The form contains several fields: 'IPsec Tunnel Name' with the value 'DAS-N2-EC-S-135442_INET1@RKLAB.COM'; 'IPsec Tunnel Authentication' section with 'ID' and 'PSK' fields, both containing the same value as the tunnel name; and 'Associated Location' section with a 'Location' dropdown menu set to 'Andover-Site'. At the bottom, there are 'Cancel' and 'Submit' buttons.

4. Click **Submit**.
5. To commit the changes, click **Apply Changes**.



6. Verify Service Orchestration Configuration Push to Devices

This section explains how to check a passthrough tunnel configuration push to verify Service Orchestration on EdgeConnect SD-WAN gateways.

1. In Orchestrator, navigate to **Orchestrator > Tools > Audit Logs**.
2. Search for “AXS” or use the prefix entered when configuring HPE_SSE Service.

The image below shows that the IP SLA and passthrough tunnel configurations have been pushed to the device successfully.

Audit Logs ?							
10/147 Rows							Search <input type="text" value="axs"/>
User Name	IP Address	Appliance	Action ▲	Task Status	Results	Start Time	End Time
OverlayMana...		Chelmsford-krisr...	Add Ipsla Rules	COMPLETED	Ipsla rules added {"MGR_http-monitor_om_passThroug...	03-May-23 13:05	03-May-23 13:05
OverlayMana...		DAS-N2-EC-S-13...	Add Ipsla Rules	COMPLETED	Ipsla rules added {"MGR_http-monitor_om_passThroug...	03-May-23 12:11	03-May-23 12:11
OverlayMana...		RackN9-EC-S-2	Add Ipsla Rules	COMPLETED	Ipsla rules added {"MGR_http-monitor_om_passThroug...	03-May-23 11:22	03-May-23 11:22
OverlayMana...		Chelmsford-krisr...	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ...	03-May-23 13:05	03-May-23 13:05
OverlayMana...		RackN9-EC-S-2	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ...	03-May-23 11:22	03-May-23 11:22
OverlayMana...		DAS-N2-EC-S-13...	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ...	03-May-23 11:21	03-May-23 11:21

NOTE: Passthrough tunnel configuration is only pushed if at least one matching WAN label, as configured under Interface Labels, exists on the EdgeConnect SD-WAN gateway.

NOTE: IP SLA rules are pushed to the device only if the following two conditions are met:

1. The interface must exist on the EdgeConnect gateway with a matching label that is configured as a Source Interface for IP SLA probes (see [Section 4.5](#)).
2. There is at least one overlay (under Business Intent Overlay) using the HPE_SSE service tunnel in the Preferred Policy Order section (see [Section 8](#)).



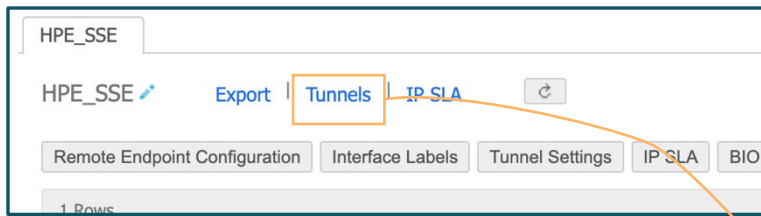
7. Verify Tunnel Status and IP SLA Status

In Orchestrator, on the Service Orchestration tab (**Configuration > Cloud Services > Service Orchestration**), the Connection Status should be “Up.” This indicates that the IPsec tunnel is functional, and the IP SLA probes are working through the tunnel.

Appliance	Interface Label	Primary Remote ...	Backup Remote ...	Tunnel Local Identifier	Primary Tunnel Rem...	Backup Tunnel Remote ...	Connection Statu...
DAS-N2-EC-S-1354...	INET1	Primary	Secondary	DAS-N2-EC-S-135442_INET1@RKLAB.COM	ipsec-geo.axisapps.io	ipsec-geo-secondary.ax...	Up
RackN9-EC-S-2	INET1	Primary	Secondary	RackN9-EC-S-2_INET1@RKLAB.COM	ipsec-geo.axisapps.io	ipsec-geo-secondary.ax...	Up
Chelmsford-krisram1	INET1	Primary	Secondary	Chelmsford-krisram1_INET1@RKLAB.COM	ipsec-geo.axisapps.io	ipsec-geo-secondary.ax...	Up

7.1. Passthrough Tunnel Status

On the HPE_SSE tab, click **Tunnels**. The Tunnels tab opens, allowing you to view the IPsec tunnel status for each of the gateways.



Edit	Applian...	Segment	Passthrough Tunnel	Admin...	Ch...	Status ▲	Local IP	Remote IP
	Branch-...	Default	ThirdParty_AXS_Primary_INET2_Primar...	up	≡	up - active	172.16.60.103	104.43.163.146
	Branch-...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	16.143.16.47	104.43.163.68
	Branch-...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	16.143.16.47	104.43.163.146
	Branch-...	Default	ThirdParty_AXS_Primary_INET2_Primar...	up	≡	up - active	172.16.60.103	104.43.163.68
	Branch-...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	16.143.16.15	104.43.163.68
	Branch-...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	16.143.16.15	104.43.163.146
	DASLA...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	16.143.16.14	104.43.163.68
	DASLA...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	16.143.16.14	104.43.163.146
	RK-Che...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	172.17.50.1	44.214.114.70
	RK-Che...	Default	ThirdParty_AXS_Primary_INET1_Primar...	up	≡	up - active	172.17.50.1	44.213.222.153



7.2. IP SLA Status

On the HPE_SSE tab, click **IP SLA**. The IP SLA tab opens, allowing you to verify tunnel health using IP SLA probes. If “Up” appears in the State column, that indicates that the tunnel is in good health.



IP SLA ?

10/36 Rows

Search ThirdParty_AXS

Edit	Applianc...	Active...	State	Monitor	Down Action	Up Action	Charts	Com...	Up Stats	Down Sta...
	Branch-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:1d 1...	Total :0, L...
	Branch-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:1d 1...	Total :0, L...
	Branch-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:1d 1...	Total :0, L...
	Branch-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:1d 1...	Total :0, L...
	Branch-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:1d 1...	Total :1, L...
	Branch-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:1d 1...	Total :1, L...
	DASLAB-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:1d 1...	Total :1, L...
	DASLAB-...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:20h ...	Total :2, L...
	RK-Chel...	Yes	Up	HTTP/HTTPS: Keep Alive Tim	Tunnel Down: Tunnel = T	Tunnel Up: Tu		generate	Last:2d 1...	Total :1, L...



8. Traffic Redirection to HPE SSE Using Business Intent Overlay

When the traffic is received on the EdgeConnect gateway's LAN side (from the employees/guests/IoT devices), it will be subject to Overlay ACL to identify the Business Intent Overlay. It is important to identify what traffic or what "internet bound" application you want to redirect to the HPE-SSE cloud.

Note that the traffic received at the EdgeConnect LAN side, is still subject to any Zone Based Firewall policy, IDS-IPS inspection, DDoS, and other firewall features if it is configured. You can choose to apply security policies at the Local EdgeConnect and/or you can send the traffic over to the HPE SSE cloud for further inspection.

8.1. Send HPE-SSE Application traffic via Local Break Out

EdgeConnect uses First Packet iQ to identify the application type based on ip/domain/address-range. There is a pre-defined list of IP address/domain names that are classified as **HPE-SSE application** on the EdgeConnect application database. Use the match criteria of application for HPE-SSE to break out locally.

While configuring Overlay ACL policies, HPE Aruba Networking recommends that any internet traffic for the "HPE SSE application" destinations be sent as Local Breakout only. This is a key step to ensure when a user/device has an SSE Agent installed, then the SSE Agent tunnel traffic will break out locally instead of going over the IPsec tunnel between EdgeConnect and SSE.

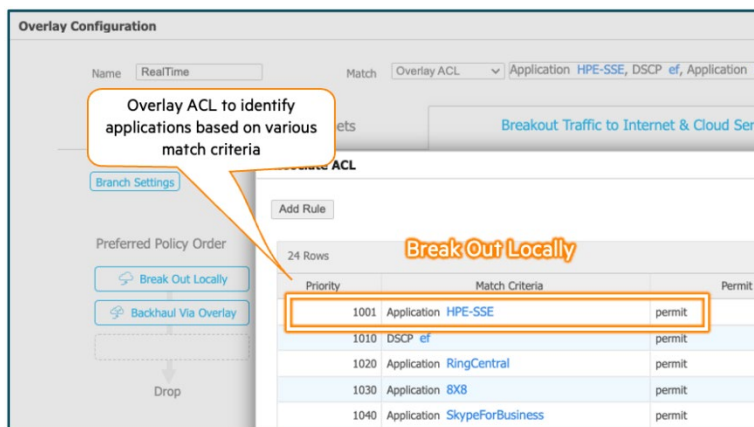
In this example of Overlay ACL configuration shows, ACL matching HPE-SSE traffic breaks out locally. This section explains how to configure the Business Intent Overlay to redirect HPE-SSE Application traffic via local breakout. Modify an existing Overlay which is at the TOP of the BIO Priority

1. In Orchestrator, navigate to **Configuration > Overlays & Security > Business Intent Overlay**.

This example uses an existing overlay called "RealTime".

2. Click **Overlay ACL**.
3. In the Match field, click the edit icon.
4. Click in the Match Criteria field to modify the overlay ACL.

The Match Criteria dialog box opens.



5. Click **Add Rule** to add a new entry with match criteria for application, such as "HPE-SSE".
6. Click the **Breakout Traffic to Internet & Cloud Services** tab and ensure Break Out Locally is at the top of the Preferred Policy Order.
7. To complete the setting changes, click **OK**.
8. To complete Business Intent Overlay configurations, click **Save and Apply Changes to Overlays**.

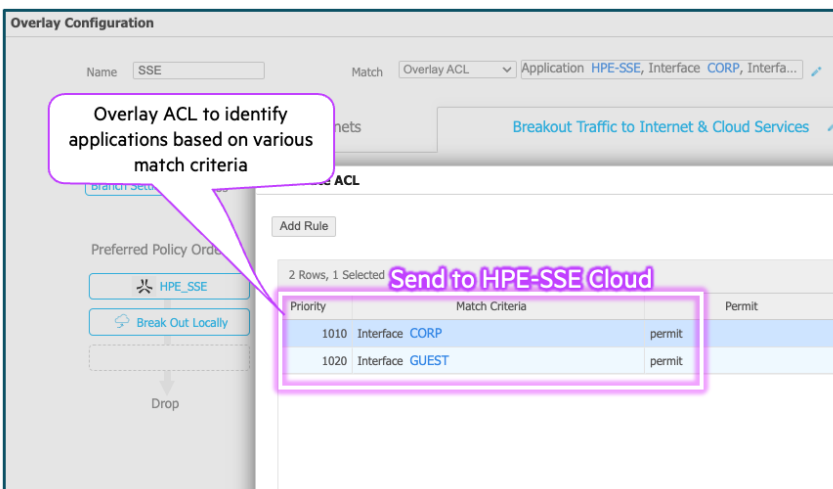
8.2. Send Internet Traffic to HPE SSE Cloud

This section explains how to configure the Business Intent Overlay to determine which internet traffic is directed to the HPE SSE Secure Web Gateway service.

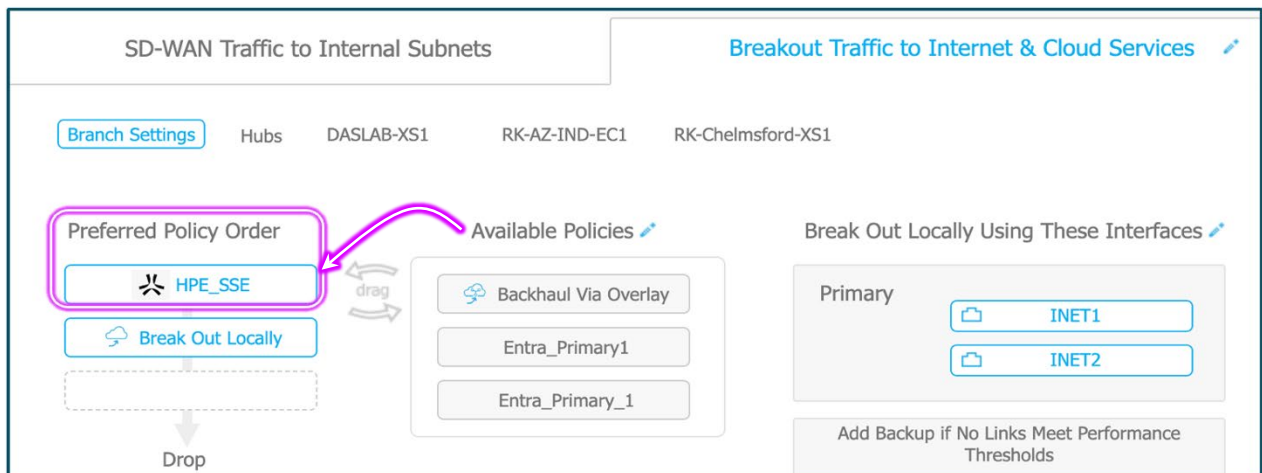
The following example shows an Overlay ACL configuration matching interface labels “CORP” and “GUEST”. Any traffic coming from the interface with labels (CORP or GUEST) will be sent over to HPE SSE Cloud for further policy inspection.

1. In Orchestrator, navigate to **Configuration > Overlays & Security > Business Intent Overlay**.
2. Either select any existing Overlay that is currently matching the internet traffic or create a new overlay for redirecting internet traffic. This example modifies an existing overlay called “SSE.”
3. Click **Overlay ACL**.
4. In the Match field, click the edit icon.

The Match Criteria dialog box opens. In this example, traffic is identified using “Interface Label” match criteria. You can choose your own criteria to match traffic that you want to send to the HPE SSE Cloud. Now this overlay will attract any traffic from GUEST and CORP interfaces, for internet bound destinations.

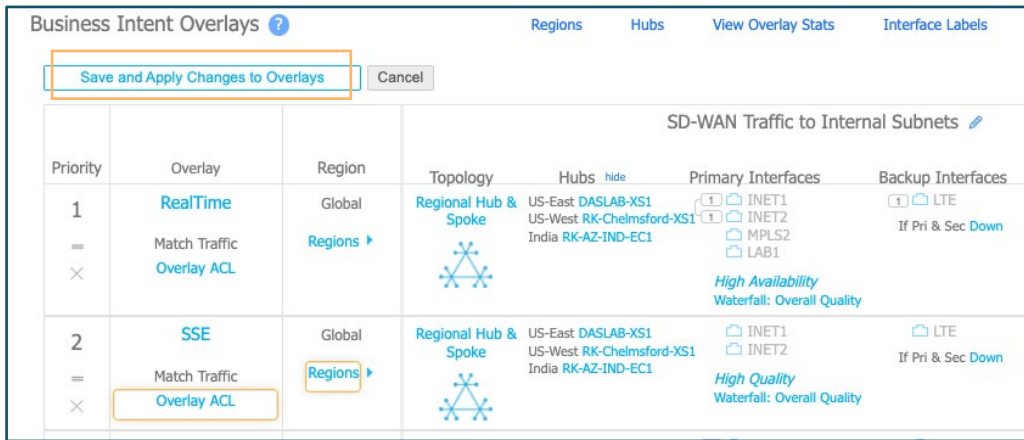


5. Click the **Breakout Traffic to Internet & Cloud Services** tab.
6. Drag the **HPE_SSE** policy from the Available Policies column to the Preferred Policy Order column.

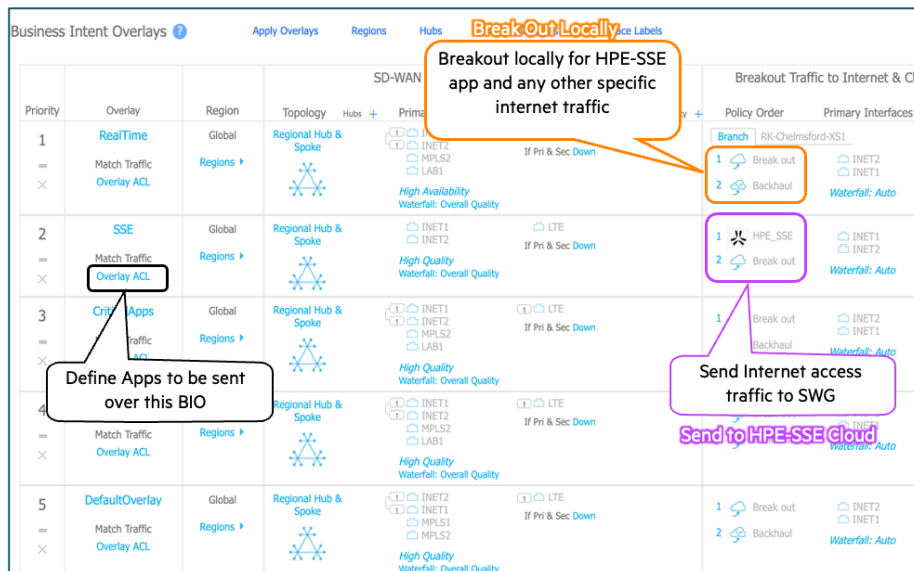


If you select Backhaul Via Overlay, Break Out Locally, or both to use as backup options under the Preferred Policy Order and the SSE tunnel service goes down, traffic is redirected using these policies. If you do not want a backup option, remove them from the Preferred Policy Order column, and then internet-bound traffic will drop when the SSE tunnel service is down.

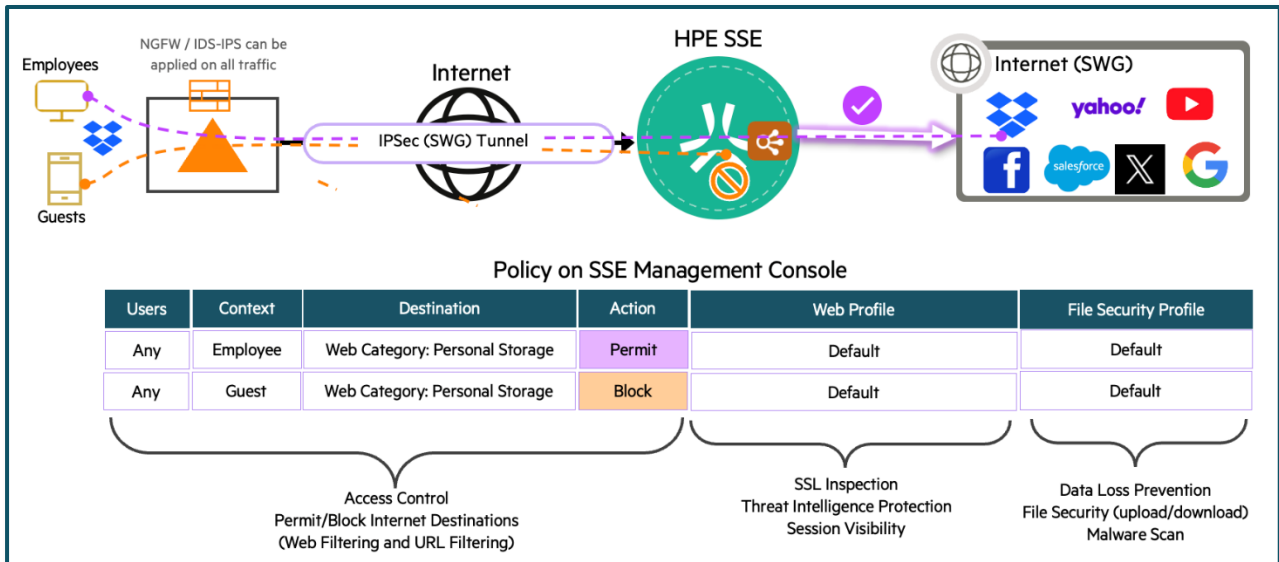
7. Under Break Out Locally Using These Interfaces, drag all primary WAN interfaces to the Primary section and all backup interfaces to the Backup section.
8. To complete the setting changes, click **OK**.
9. To complete Business Intent Overlay configurations, click **Save and Apply Changes to Overlays**.



The following figure shows the Business Intent Overlay page with “RealTime” overlay at the TOP of the BIO list Breaks Out locally. “HPE_SSE” overlay, which is 2nd in the BIO list, sends the traffic over to the SSE cloud. Priority of the BIO plays a role in correctly identifying the application and sending traffic over the intended path (either local breakout, the HPE-SSE cloud, or backhaul to SD-WAN peer).



9. Inspecting Branch Traffic at the HPE SSE Cloud



HPE SSE Secure Web Gateway (SWG) offers the following features for internet traffic coming from branches (EdgeConnect gateway) through the IPsec tunnel.

Feature	Description	Notes
Web Filtering and URL Filtering	<p>The primary function of SWG is to provide access to the internet based on the categories of web domains. Policies are created to allow or block access to web domains based on the categories. Web filtering is achieved through SNI inspection and does not require SSL inspection.</p> <p>URL filtering function offers the function of blocking the entire URL and not just the domain name. URL filtering requires SSL inspection to be enabled. Learn more at https://docs.axissecurity.com/docs/dns-and-url-filtering</p>	SSL Inspection Required for URL filtering function
Threat Intelligence Protection	Prevent access to “high risk” internet websites based on site/domain reputation. This function is part of the web profile that is associated with a policy. Each policy has either a default web profile or you can assign a custom web profile. On the Profile, you will need to enable “Threat Intelligence Protection”. Once enabled, this function either “blocks” or “warns” the user that they are accessing a “high risk” website based on the reputation (for example, a website domain that was only registered a week ago).	None
DLP (Data Loss Prevention)	Prevent data leakage with File Security Profiles for more control and less risk. This functionality of	SSL Inspection Required



Feature	Description	Notes
	preventing upload/download of files/data is only available if you enable “SSL Inspection” on the web profile that is attached to a policy.	
Malware Protection	Protection against malware through repeatable hash and anti-virus scanning. Malware protection is a functionality of scanning the files from the internet for any known malware (known hashes) before the user is allowed to download the file. This feature is also an SSL inspection-based feature. This means SSL Inspection must be enabled on the web profile that is attached to a policy.	SSL Inspection Required
Sandboxing	Protection for Day-0 malware threats. In the Security world, sandboxing refers to the concept of inspecting (deep scanning) files for “unknown” malware hashes at a secure location and making the decision to permit/block the traffic.	SSL Inspection Required Sandboxing is an add-on feature. It is not part of Foundation+/Advanced or SASE-SWG-BW.

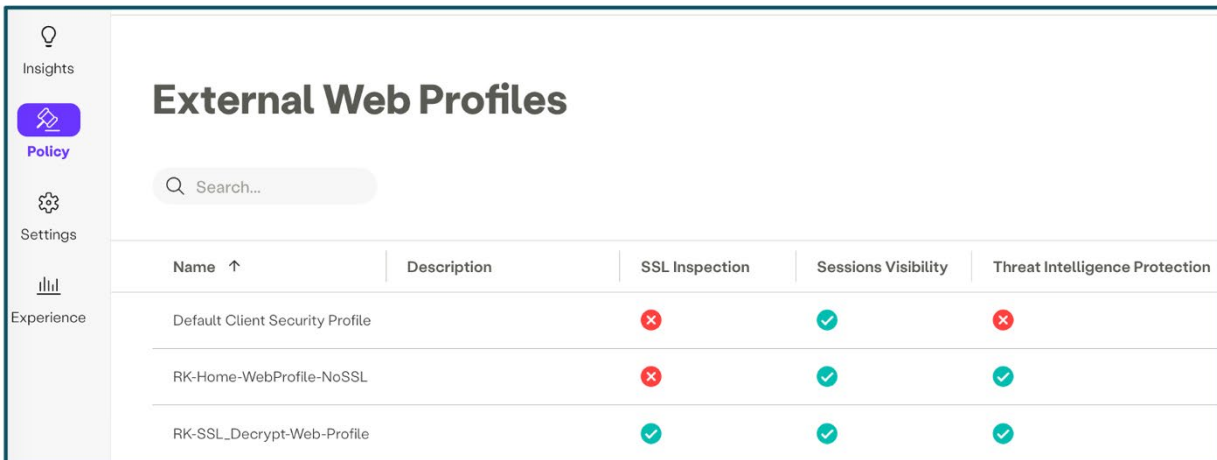


9.1. External Web Profiles

A web profile must be attached to every policy. Web profiles control:

- SSL Inspection
- Session Visibility
- Threat Intelligence Protection

To select a web profile, navigate to the SSE Management Console, and then click **Management Console > Policy > External Web Profiles**.



Name ↑	Description	SSL Inspection	Sessions Visibility	Threat Intelligence Protection
Default Client Security Profile		✘	✔	✘
RK-Home-WebProfile-NoSSL		✘	✔	✔
RK-SSL_Decrypt-Web-Profile		✔	✔	✔

SSL Inspection

SSL inspection refers to a process in which SSL-encrypted internet communication between a client and a server is intercepted and reviewed. Most internet communications are encrypted using SSL, therefore enabling SSL inspection is crucial for using the Web Gateway advanced URL filtering solution.

For SSL inspection to work, you will either need to upload your CA certificate, which is installed on your laptops (or any device that is trying to access internet) to the HPE SSE Management console; or you can use the default CA certificate from HPE SSE Management Console, which need to be distributed to your laptops (or any device that is trying to access internet).

For more information, see <https://docs.axissecurity.com/docs/enabling-ssl-inspection>.

Session Visibility

This enables visibility for user sessions to administrators' access to the users' DNS and SWG activities by sending logs to SIEM.

Threat Intelligence Protection

The detection of high-risk websites is accomplished by analyzing various factors, including web content, domain registration information, and reputation data. By leveraging advanced algorithms and techniques, the threat intelligence protection system can accurately identify websites that pose a significant risk to users and organizations.

For more information, see <https://docs.axissecurity.com/docs/threat-intelligence-protection>.



9.2. File Security Profile

The File Security Profile (FSP) defines a policy object that matches file data in a user's session for further action such as Allow, Block, Scan (static scan against known hashes), or Deep Scan (Dynamic Scanning / Sandboxing). The File Security Profile is a key Data Loss Prevention (DLP) and Security feature, controlling the transport of session file data by allowing approved data, blocking risky data, or directing suspicious data to be scanned further. A FSP consists of a list of Data Matcher objects along with the action each matched data object should be subject to.

For more information, see <https://docs.axissecurity.com/docs/data-security-profile>.

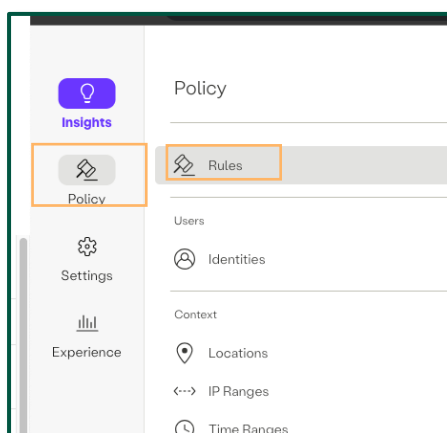
9.3. Example 1 – Policy to Redirect Traffic to Permit Internet Access

In most cases, there will be policies to permit or deny user internet traffic. But for cases when you don't have an existing policy configured, then you must configure a policy to permit internet traffic (including the IP SLA probes coming from EdgeConnect appliances) as part of the Service Orchestration.

Keep the following in mind when constructing policies on the HPE SSE Management Console with respect to Branch traffic coming through the IPSec tunnel.

- **Users** – IPSec traffic from the EdgeConnect to the SSE cloud does not carry any “user” identity with it. For example, radius-snooped or VXLAN-learned user role is not carried with IPSec traffic to the SSE cloud. When internet traffic reaches the SSE cloud for policy inspection, it only contains the “source IP” and “destination IP”.
NOTE: The source IP of the traffic is the LAN side IP address of the device. Use “Any” as the value for the “Users” attribute.
- **Context** – When creating policies for IPSec traffic from EdgeConnect to SSE, either use ANY or select a specific location or sub-location name from the drop-down list. More than one location/sub-location can be added to a single policy context.
- **Destinations** – Select either “Any Web Traffic” or a specific category. You can add one or more web categories to a single policy.
- **Profiles** – Each policy has default profiles attached. The two profiles that are relevant for IPSec traffic are Web Profile and File Security Profile. For more information, see [Inspecting Branch Traffic at the HPE SSE Cloud](#).

1. Navigate to **Policy > Rules**.



2. Click **New Rule** and add a rule to permit traffic. The rule shown in the following figure permits all traffic.

NOTE: This is a sample rule that permits all traffic. Modify the rules according to your requirements. Refer to other examples below for other variations.

9.4. Example 2 - Web Filtering / URL Filtering Based on Web Categories

The following figure shows some examples of policy constructs.

Policies are processed from the top to bottom order

Enabled	Name	Users	Context	Destinations	Action	Profiles
<input checked="" type="checkbox"/>	RestrictedSites-Policy	Any	Any	<ul style="list-style-type: none"> Cheating Spyware and Adware Phishing IP Addresses SPAM URLs Low-THC Cannabis Pro... And 23 more... 	Block	Default Profiles
<input checked="" type="checkbox"/>	RK-Demo-SWG-External-Storage	Any	GUEST	<ul style="list-style-type: none"> Personal Storage And 5 Default Profiles 	Block	<ul style="list-style-type: none"> RK-SSL_Decrypt-Web... RK-FileSecurity-Strict And 5 Default Profiles
<input checked="" type="checkbox"/>	Branch-Default-Policy	Any	Any	<ul style="list-style-type: none"> Any Web Traffic 	Allow	Default Profiles

This policy restricts access to some common block categories (Spyware/Spam/Phishing...)

This policy restricts access to Personal Storage websites (Google Drive, Box....) from GUEST sub-location

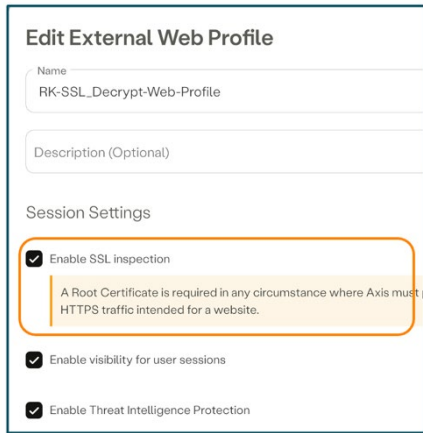
This policy will allow access to ALL internet websites



9.5. Example 3 – Prevent Download/Upload of Files

Download/Upload of file prevention can only be achieved with SSL inspection turned on. Also, you must use either a custom CA Certificate on HPE SSE or install the default CA Certificate downloaded from SSE Management Console on your PC.

1. Create a web profile and ensure “SSL Inspection is enabled” (**Policy > External Web > Create new or modify an existing profile**).

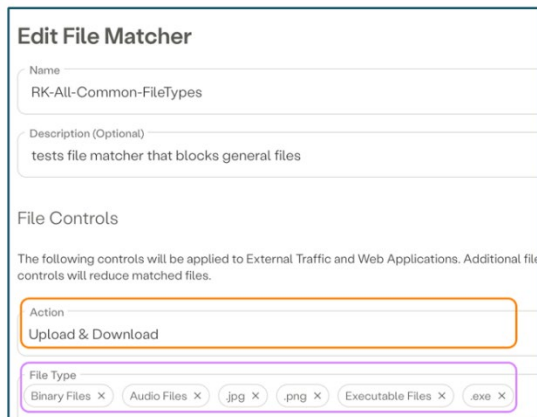


2. Ensure HPE SSE Management Console uses the same Root certificate (either custom or the default certificate from the SSE Console) (**Settings > Certificates > CA Certificates**).



3. Create a File Matcher to match the list of files that you want to upload and/or download (**Policy > File Security > File Matcher**).

The following File Matcher has an action of Upload & Download for certain file types (for example, .jpeg, .png, .exe, executable.)



4. Create a File Security Profile to define the action for files that are identified in the “File Matcher” - **Policy > File Security > Profiles**. Action can be:

- **Allow** – Allows the identified file types to be uploaded/downloaded
- **Block** – Prevents the user from Download and/or Upload identified file types
- **Fast Scan** – Scans the files for Malware/Antivirus hash matches (a.k.a Static Scanning)
- **Deep Scan** – Sandboxing (This is an add-on feature. An additional subscription is required.)

The following Security Profile blocks the file types identified in the file matcher that was created in Step 3.

5. Create a policy to allow access to the web destination that you want to apply file security and associate the web-profile and file security profile to the policy:

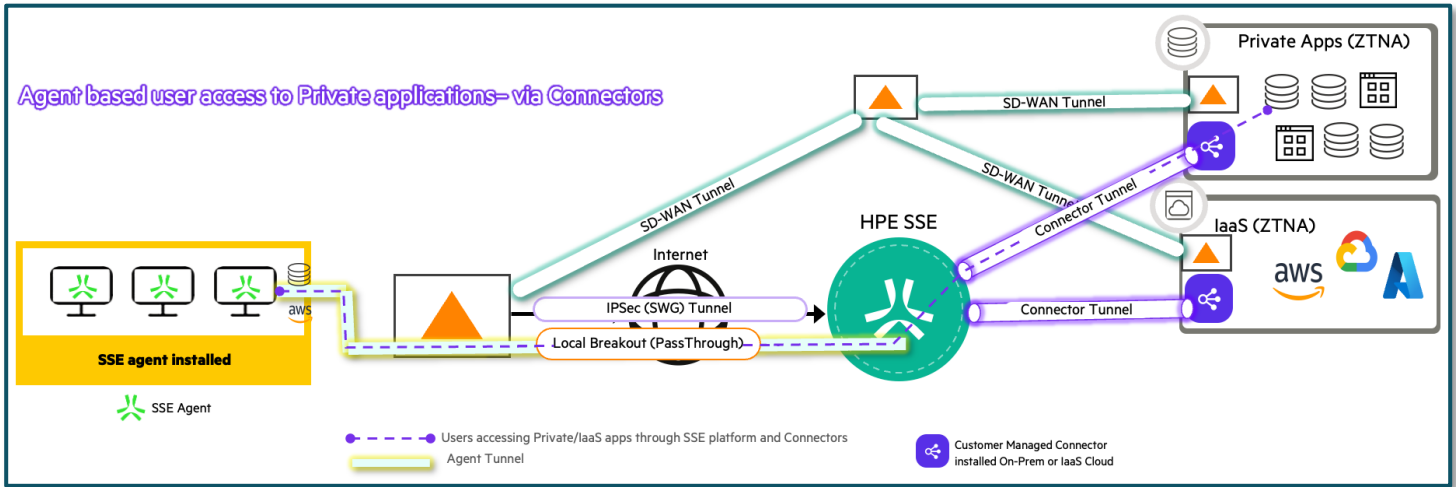
The following policy example shows users from sub-location CORP are allowed access to “Any Web Traffic” and subject to SSL inspection and file security profile attached to the policy to enforce Upload/Download of certain type of data.

Name	Users	Context	Destinations	Action	Profiles
RKOffice-WebPolicy-Location-CORP	Any	CORP	Any Web Traffic	Allow	<ul style="list-style-type: none"> RK-SSL_Decrypt-Web-Profile RK-FileSecurity-Strict



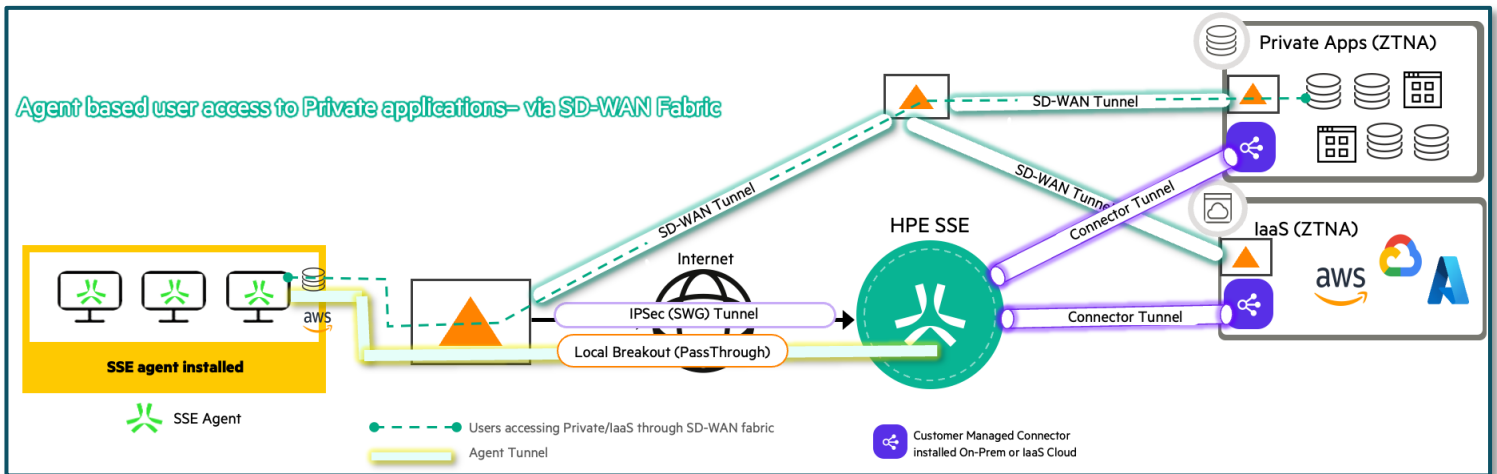
9.6. Example 4 – “Break out” Private Apps Traffic via EdgeConnect Instead of Agent Tunnel

When using an SSE Agent on your user machines, the Agent running on the machine will automatically build an Agent Tunnel to the closest SSE endpoints.



The previous figure shows that users running the SSE Agent on their device access the enterprises’ “Private applications” through the **Connectors** via a brokered SSE cloud connection. This may not be ideal when the Agent running the machines is connected behind an EdgeConnect SD-WAN gateway. Because the EdgeConnect is part of the SD-WAN fabric, the traffic will have the best possible path to reach the private app destinations.

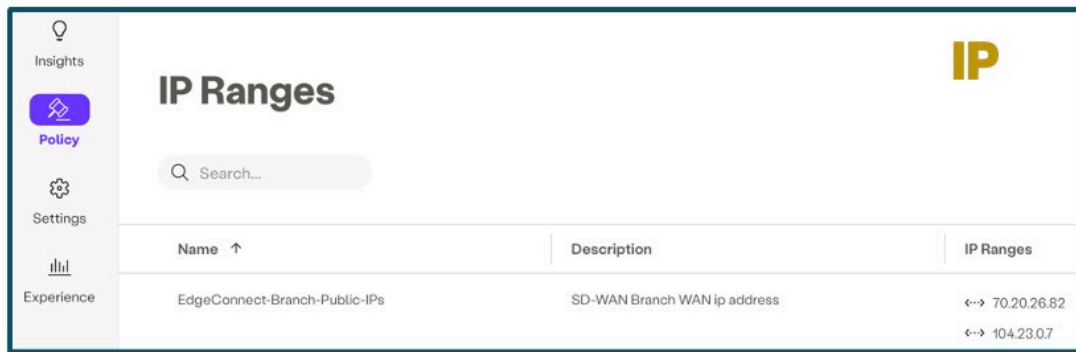
HPE Aruba Networking advises configuring the SSE policy in a way that allows the users who are behind an EdgeConnect to “bypass” the “Agent Tunnel” running on their machine to access private app destinations. The following figure shows an Agent PC accessing private apps in the data center via the **SD-WAN fabric** tunnel.



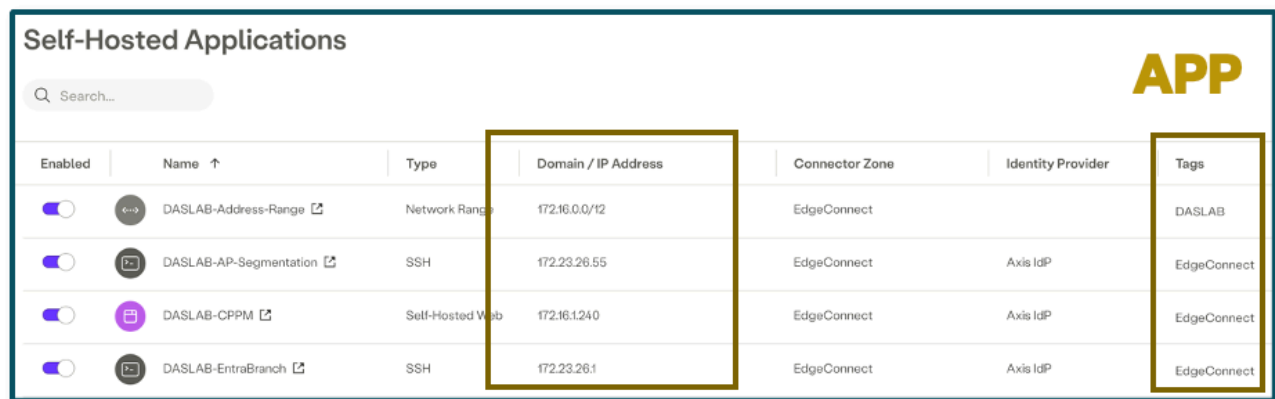
1. Create an IP-Ranges object that contains all your SD-WAN Fabric WAN IP addresses (**Policy > Context > IP Ranges > New IP Range**).

You will use this IP range later in creating a policy to identify traffic originating from a user behind an EdgeConnect branch that has an IPSec tunnel with HPE SSE.

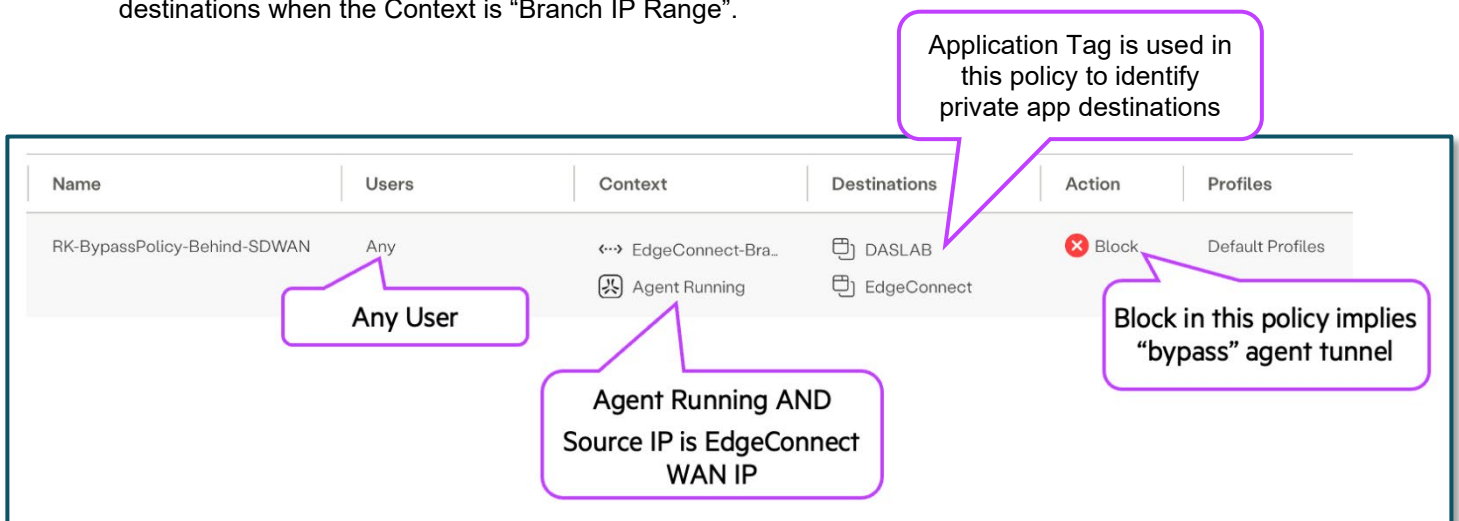




2. Identify the Application that you want to Bypass when behind Branch (for example, Application Name or Tag).



3. Create a Policy (**Policy > Rules > New Rule**) similar to the below one which blocks access to “Private Apps” destinations when the Context is “Branch IP Range”.



The assumption of this example is that “Private Apps” destination subnets/IPs are reachable via EdgeConnect SD-WAN fabric, so the user machine is able to find the best path for the private app destinations via EdgeConnect.



10. Verify Active Flows on the Orchestrator

This section explains how to validate whether internet traffic is being redirected on the HPE_SSE service tunnels by checking the flows on the Orchestrator.

1. In Orchestrator, navigate to **Monitoring > Flows > Active & Recent Flows**.
2. Filter for internet bound traffic using either the IP address or the port number to view the flows on the EdgeConnect.

Applica...	Detail	Start Tim...	Uptime...	Overlay	Application...	IP1	Po...	IP2	Por...	Inbound ...	Outbound ...	Inbound Tunnel	Outbound Tunnel
RK-Ch...	ⓘ	08:14:32	1m 53s	SSE	Office365C...	172.23.25.153	60...	mobile.events.data.m...	443	9K	6K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...
RK-Ch...	ⓘ	08:14:30	1m 55s	SSE	Office365C...	172.23.25.153	60...	self.events.data.micro...	443	9K	6K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...
RK-Ch...	ⓘ	08:16:08	17s	SSE	Office365C...	172.23.25.153	60...	mobile.events.data.m...	443	8K	7K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...
RK-Ch...	ⓘ	08:15:54	31s	SSE	Https	172.23.25.153	54...	dns.google (8.8.4.4)	443	10K	5K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...
RK-Ch...	ⓘ	08:16:20	5s	SSE	Icloud	172.23.25.153	60...	p57-fmfmobile.icloud...	443	10K	5K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...
RK-Ch...	ⓘ	07:49:55	26m 30s	SSE	Intercom	172.23.25.153	51...	nexus-websocket-a.in...	443	7K	7K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...
RK-Ch...	ⓘ	07:54:02	22m 23s	SSE	Office365C...	172.23.25.153	54...	pus5-collabhubrtc.offi...	443	5K	8K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...
RK-Ch...	ⓘ	08:15:35	50s	SSE	Office365C...	172.23.25.153	60...	teams.events.data.mi...	443	8K	4K	ThirdParty_AXS_Primary_INET1...	ThirdParty_AXS_Primary_INET1...

The example above has filtered traffic for the LAN subnet 172.23.25.153. The traffic matches the SSE overlay, and inbound and outbound tunnels show as “ThirdParty_AXS_Primary_INET1_Primary_1”. This confirms that the traffic is being redirected to the HPE_SSE service tunnel properly and the user has successful inbound and outbound connections through the SSE Secure Web Gateway.

11. Verify Traffic Flows on the HPE SSE Management Console

This section explains how to validate whether internet traffic is received on HPE SSE and how to check the status of the incoming internet traffic from gateways through the IPSEC tunnel.

On the SSE Management Console, navigate to **Insights > Exploration** and then filter for Integration type **IPSEC** or match for private IP address of the user on the LAN side.

The screenshot shows the 'Exploration' view in the HPE SSE Management Console. A filter menu is open, with 'Source IP' and 'Integration Type' selected. The background table shows traffic logs with columns for Host, Status, and Integration Type.

Host	Status	Integration Type
Jul 07, 2023 10:45:30	IPSEC	IPSEC
Jul 07, 2023 10:45:04	IPSEC	IPSEC
Jul 07, 2023 10:44:59	IPSEC	IPSEC
Jul 07, 2023 10:44:52	IPSEC	IPSEC
Jul 07, 2023 10:44:51	IPSEC	IPSEC
Jul 07, 2023 10:44:51	IPSEC	IPSEC
Jul 07, 2023 10:44:49	IPSEC	IPSEC
Jul 07, 2023 10:44:47	IPSEC	IPSEC
Jul 07, 2023 10:44:46	IPSEC	IPSEC

You will see the detailed view of the flows including source IP, destination application, web category and the policy match rule, and so on.

Exploration Last 1 hour ▾ Filters ▾ ☰ Total Rows: 1,504 Last updated on July 07, 2023 10:59:08										
Date	Integration	Source	Protocol	Host	Status	Matched Rule	Branch Name	Port	Web Category	
Jul 07, 2023 10:56:55	IPSEC	172.23.24.60	HTTPS	rr3--sn-q4fzene7.googlevideo.com	Success	Web Traffic Default	2 Branch Names	443	Streaming Media	
Jul 07, 2023 10:56:55	IPSEC	172.23.24.53	HTTPS	www.adobe.com	Success	Web Traffic Default	2 Branch Names	443	2 Web Categories	
Jul 07, 2023 10:56:52	IPSEC	172.23.24.53	HTTPS	www.adobe.com	Success	Web Traffic Default	2 Branch Names	443	2 Web Categories	
Jul 07, 2023 10:56:50	IPSEC	172.23.24.53	HTTPS	www.adobe.com	Success	Web Traffic Default	2 Branch Names	443	2 Web Categories	
Jul 07, 2023 10:56:50	IPSEC	172.23.24.60	HTTPS	rr3--sn-q4fzene7.googlevideo.com	Success	Web Traffic Default	2 Branch Names	443	Streaming Media	
Jul 07, 2023 10:56:47	IPSEC	172.23.24.60	HTTPS	rr3--sn-q4fzene7.googlevideo.com	Success	Web Traffic Default	2 Branch Names	443	Streaming Media	
Jul 07, 2023 10:56:46	IPSEC	172.23.24.60	HTTPS	accounts.google.com	Success	Web Traffic Default	2 Branch Names	443	Internet Portals	
Jul 07, 2023 10:56:46	IPSEC	172.23.24.60	HTTPS	accounts.google.com	Success	Web Traffic Default	2 Branch Names	443	Internet Portals	
Jul 07, 2023 10:56:45	IPSEC	172.23.24.60	HTTPS	accounts.google.com	Success	Web Traffic Default	2 Branch Names	443	Internet Portals	
Jul 07, 2023 10:56:45	IPSEC	172.23.24.60	HTTPS	mail.google.com	Success	Web Traffic Default	2 Branch Names	443	Web-based Email	
Jul 07, 2023 10:56:44	IPSEC	172.23.24.60	HTTPS	www.gmail.com	Success	Web Traffic Default	2 Branch Names	443	Web-based Email	
Jul 07, 2023 10:56:42	IPSEC	172.23.24.53	HTTPS	www.adobe.com	Success	Web Traffic Default	2 Branch Names	443	2 Web Categories	
Jul 07, 2023 10:56:41	IPSEC	172.23.24.53	HTTPS	www.adobe.com	Success	Web Traffic Default	2 Branch Names	443	2 Web Categories	

