HPE Aruba Networking
EdgeConnect SD-WAN
Integration with HPE Aruba Networking SSE – Secure Web Gateway
Integration Guide
Important Notice

© Copyright 2023 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 C, September 2023
Contents

1. Overview ....................................................................................................................................................................... 3
2. Topology ....................................................................................................................................................................... 3
3. Before You Start – Configure Loopback Interface ........................................................................................................ 5
4. Orchestrator Configuration ............................................................................................................................................ 6
   4.1. Finding the Closest Axis 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 Appliances ................................................................................................ 14
5. Axis Cloud Configuration ............................................................................................................................................ 16
   5.1. Configure Branches as Locations ........................................................................................................................ 17
   5.2. Configure IPsec Tunnel ........................................................................................................................................ 18
   5.3. Policy to Permit Internet Traffic ............................................................................................................................ 19
6. Redirect Traffic to the Axis Service Using Business Intent Overlay ........................................................................... 20
7. Verify Service Orchestration Configuration Push to Devices ......................................................................................................................... 22
8. Verify Tunnel Status and IP SLA Status ............................................................................................................................ 23
   8.1. Passthrough Tunnel Status .................................................................................................................................. 23
   8.2. IP SLA Status ....................................................................................................................................................... 24
9. Verify Active Flows on the EdgeConnect SD-WAN .................................................................................................... 25
10. Verify Traffic Flows on the Axis Console .................................................................................................................... 25
1. Overview

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

2. Topology

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

IPsec tunnels to Axis SWG endpoints can be deployed in a single appliance site or sites with Aruba EdgeHA deployment, which involves two appliances and multiple uplinks. If configured, Service Orchestration pushes the IPsec tunnel configuration to the appliances to build tunnels using all available uplinks.
The following figure shows a simple topology: a single EdgeConnect SD-WAN appliance with one ISP connection.

![Single Appliance Topology](image1)

Figure 2: Single Appliance Topology

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

![Dual EdgeConnect in EdgeHA Deployment](image2)

Figure 3: Dual EdgeConnect in EdgeHA Deployment
3. Before You Start – Configure Loopback Interface

Before you set up Service Orchestration configuration, it is important to ensure that each EdgeConnect appliance has at least one valid loopback interface with IP address. The EdgeConnect appliance 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 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 appliance in the network. Complete the following steps to set up loopback orchestration:


2. Click New Label, select LAN, and then enter a name (for example, Loopback).

3. Click Save.


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 appliance.

9. Click Add.

![Loopback Orchestration](image)

Figure 4: Loopback Orchestration
4. Orchestrator Configuration

The Service Orchestration feature orchestrates tunnel configuration for all appliances 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 “Axis” in the Name field and “AXS” in the Prefix field, and then click Save.

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

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

4.1. Finding the Closest Axis Remote Endpoints – Geo DNS Lookup

To build tunnels from SD-WAN appliances to Axis SWG, use the primary and secondary DNS names below. When an individual appliance resolves these fully qualified domain names (FQDNs), it resolves to the nearest Axis POP (point-of-presence) endpoints based on the geolocation from where the DNS query was made. This results in SD-WAN appliances 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 Axis POP endpoints using the FQDN identified in Section 4.1 and a pre-shared key. First you 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Secondary</td>
</tr>
<tr>
<td>IP Address</td>
<td>ipsec-proxy-secondary-geo.axisapps.io</td>
</tr>
<tr>
<td>Interface Label</td>
<td>any</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>Enter a pre-shared key.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Primary</td>
</tr>
<tr>
<td>IP Address</td>
<td>ipsec-proxy-geo.axisapps.io</td>
</tr>
<tr>
<td>Interface Label</td>
<td>any</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>Enter the same pre-shared key that was set for secondary.</td>
</tr>
<tr>
<td>Backup Remote Endpoint</td>
<td>Secondary</td>
</tr>
</tbody>
</table>

**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 Axis 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.

   **NOTE:** You must add each of the WAN IPs (public IP address) on the Axis Cloud (under Locations). For example, if one branch has two WAN uplinks, then both WAN public IP addresses must be added in the Axis Cloud portal.

2. Click **Save**.

4.4. Tunnel Settings

This section explains how to configure the IKE-Phase1 and Phase-2 settings that the SD-WAN appliance uses to build tunnels to the Axis 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.

![IKE Identifier variables available to use](image)

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 appliance 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 Axis dialog box, as shown in the following figure. Take special care to ensure that the settings in the following table are configured correctly.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IP SLA rule orchestration</td>
<td>Enabled</td>
</tr>
<tr>
<td>Monitor</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>Address</td>
<td>ip-sla.silverpeak.cloud</td>
</tr>
<tr>
<td>Source interface</td>
<td>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 the probe destination address. Note that for the IP SLA profile to be</td>
</tr>
</tbody>
</table>
3. Click **Save**.

### 4.6. BIO Breakout

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP request timeout</td>
<td>2</td>
</tr>
</tbody>
</table>

- Click **BIO Breakout**.
- Ensure that the **BIO Breakout** check box is selected.
- (Optional) If an icon must be visible on the BIO, upload a service icon (image size must be less than 20 KB).
- Click **Save**.

- **Pushed to the SD-WAN appliances, there must be at least one interface on the appliance with the matching label.**
4.7. Remote Endpoint Association

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

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

2. Click Remote Endpoint Association.

3. Click the Add check box next to Primary. This associates both the primary and secondary Axis endpoints with the selected EdgeConnect SD-WAN appliances.

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 appliances.

After a few minutes, the Service Orchestration page auto populates the Tunnel Local Identifier field for each of the EdgeConnect appliances. Record the identifier details for each appliance because you will use those details in Section 5 to configure the "IKE Identifier" on the Axis Management portal under Settings > Connector > Tunnels > New IPsec Tunnel.

4.9. Change Default MSS settings for the Appliances

By default, the TCP MSS setting for the appliance is set at 9000. This may cause web traffic to be dropped at the Axis Secure Web Gateway. HPE Aruba Networking recommends modifying the TCP MSS value for the appliance either per appliance 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.

4.9.1. Per Appliance Level TCP - MSS Change

1. Select the appliances 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:
2. Click the edit icon next to each appliance and modify the Maximum TCP MSS setting to “1350” (from the default of 9000).

4.9.2. 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. Modify the Maximum TCP MSS value to “1350” from the default of 9000, as shown in the following figure.
5. Axis Cloud Configuration

This section explains how to complete configuration on the Axis Management portal to provision tunnel and IP settings for each EdgeConnect appliance. You need the WAN IP Address and Tunnel Local Identifier information for each EdgeConnect appliance to proceed further in this section.

To obtain the WAN IP addresses of the EdgeConnect WAN interfaces from Orchestrator, navigate to Configuration > Networking > Interfaces.

<table>
<thead>
<tr>
<th>Edit</th>
<th>Appliance</th>
<th>Name</th>
<th>LACP Status</th>
<th>IP Address/Mask</th>
<th>Public IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chelmsford...</td>
<td>wan0</td>
<td>up</td>
<td>172.17.50.1/24</td>
<td>70.20.26.82</td>
</tr>
<tr>
<td></td>
<td>DAS-N2-EC...</td>
<td>wan0.60</td>
<td>up</td>
<td>172.16.60.103/24</td>
<td>16.143.16.40</td>
</tr>
<tr>
<td></td>
<td>DAS-N2-Sx</td>
<td>wan0</td>
<td>up</td>
<td>172.16.0.109/24</td>
<td>16.143.16.40</td>
</tr>
</tbody>
</table>

To obtain the IKE Identifier for each EdgeConnect from Orchestrator, navigate to Configuration > Cloud Services > Service Orchestration and refer to Section 4.8.
5.1. Configure Branches as Locations

In this section, you add the WAN IP address for each branch as a location. You can add a single IP address or an IP address range.

1. Log in to the Axis Management portal.
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 click Sub Location to add IP address detail for a sub-location under that location. You can enter one branch IP address or an IP address range for a given geographical area.

5. Click Submit.

6. To commit the changes, click Apply Changes.

7. 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.

4. Click Submit.

5. To commit the changes, click Apply Changes.
5.3. Policy to Permit Internet Traffic

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.


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.
6. Redirect Traffic to the Axis Service Using Business Intent Overlay

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

1. In Orchestration, 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 "InternetBreakOut."

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 the Port check box and enter “80|443” in the Port field to match on TCP ports 80 (HTTP) and 443 (HTTPS).
   Now this overlay will attract any traffic matching ports 80 and 443 for internet bound destinations.
6. Click the **Breakout Traffic to Internet & Cloud Services** tab.

7. Drag the **Axis** policy from the Available Policies column to the Preferred Policy Order column.

**NOTE:** It is important to put the Axis policy at the top of the Preferred Policy Order. This enables all internet-bound traffic (http/https) to be redirected to Axis service tunnels.

If you select Backhaul Via Overlay, Break Out Locally, or both to use as backup options and the Axis 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 drops if the Axis tunnel service is down.

8. Under **Break Out Locally Using These Interfaces**, drag and drop all primary WAN interfaces to the Primary section and all backup interfaces to the Backup section.

9. To complete the setting changes, click **OK**.

10. To complete Business Intent Overlay configurations, click **Save and Apply Changes to Overlays**.
7. Verify Service Orchestration Configuration Push to Devices

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

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

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

![Audit Logs](image)

**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 appliance.

**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 SD-WAN appliance 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 Axis service tunnel in the Preferred Policy Order section (see Section 6).
8. 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.

8.1. Passthrough Tunnel Status

On the Axis tab, click Tunnels. The Tunnels tab opens, allowing you to view the IPsec tunnel status for each of the appliances.
8.2. IP SLA Status

On the Axis 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.
9. Verify Active Flows on the EdgeConnect SD-WAN

This section explains how to validate whether internet traffic is being redirected on the Axis service tunnels by checking the flows on the EdgeConnect SD-WAN appliances.

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.

The example above has filtered traffic for the LAN subnet 172.23.25.0/24. The traffic matches the InternetBreakOut overlay, and inbound and outbound tunnels show as "ThirdParty_AXS_Primary_INET1_Primary_1" This confirms that the traffic is being redirected to the Axis service tunnel properly and the user has successful inbound and outbound connections through the Axis Secure Web Gateway.

Verify Traffic Flows on the Axis Console Gateway.

10. Verify Traffic Flows on the Axis Console

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

On the Axis Management Portal, navigate to Insights > Exploration and then filter for Integration type IPSEC or match for private IP address of the user on the LAN side.
You will see the detailed view of the flows including source IP, destination application, web category and the policy match rule, etc.

<table>
<thead>
<tr>
<th>Date</th>
<th>Integration</th>
<th>Source</th>
<th>Protocol</th>
<th>Host</th>
<th>Status</th>
<th>Matched Rule</th>
<th>Branch Name</th>
<th>Port</th>
<th>Web Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 07 2022 10:56:15</td>
<td>IPSEC</td>
<td>172.21.24.60</td>
<td>HTTPS</td>
<td><a href="mailto:m3-as-offname@googlevido.com">m3-as-offname@googlevido.com</a></td>
<td>Success</td>
<td>Web Traffic Default</td>
<td>2 Branch Names</td>
<td>443</td>
<td>Streaming Media</td>
</tr>
<tr>
<td>Jul 07 2022 10:56:15</td>
<td>IPSEC</td>
<td>172.21.24.60</td>
<td>HTTPS</td>
<td>mail.google.com</td>
<td>Success</td>
<td>Web Traffic Default</td>
<td>2 Branch Names</td>
<td>443</td>
<td>Web-based Email</td>
</tr>
</tbody>
</table>