EdgeConnect and Akamai IPsec Tunnel Integration Using Service Orchestration

INTEGRATION GUIDE
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>3</td>
</tr>
<tr>
<td>TOPOLOGY</td>
<td>3</td>
</tr>
<tr>
<td>AKAMAI CONTROL CENTER CONFIGURATION</td>
<td>3</td>
</tr>
<tr>
<td>Configure Branches as Locations in SLA</td>
<td>4</td>
</tr>
<tr>
<td>Configure IPsec Credentials in SLA</td>
<td>5</td>
</tr>
<tr>
<td>Akamai POP FQDNs</td>
<td>5</td>
</tr>
<tr>
<td>ARUBA ORCHESTRATOR TUNNEL CONFIGURATION</td>
<td>6</td>
</tr>
<tr>
<td>Remote Endpoint Configuration</td>
<td>6</td>
</tr>
<tr>
<td>Interface Labels</td>
<td>8</td>
</tr>
<tr>
<td>Tunnel Settings</td>
<td>9</td>
</tr>
<tr>
<td>IP SLA</td>
<td>10</td>
</tr>
<tr>
<td>BIO Breakout</td>
<td>11</td>
</tr>
<tr>
<td>Remote Endpoint Association</td>
<td>11</td>
</tr>
<tr>
<td>REDIRECT TRAFFIC TO THE AKAMAI SERVICE USING BUSINESS INTENT OVERLAY</td>
<td>12</td>
</tr>
<tr>
<td>VERIFY SERVICE ORCHESTRATION CONFIG PUSH TO DEVICES</td>
<td>15</td>
</tr>
<tr>
<td>VERIFY TUNNEL STATUS AND IP SLA STATUS</td>
<td>16</td>
</tr>
<tr>
<td>Passthrough Tunnel Status</td>
<td>17</td>
</tr>
<tr>
<td>IP SLA Status</td>
<td>17</td>
</tr>
<tr>
<td>VERIFY ACTIVE FLOWS ON THE EDGECONNECT SD-WAN</td>
<td>18</td>
</tr>
</tbody>
</table>
OVERVIEW

This document details the configurations required on the Aruba Orchestrator and Akamai Control Center portal to provision IPsec tunnels between an EdgeConnect SD-WAN appliance and Akamai VPN 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.

TOPOLOGY

IPsec tunnels to Akamai endpoints can be deployed in a single appliance site or sites with Aruba Edge-HA 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 image below shows a simple topology: a single EdgeConnect SD-WAN appliance with one ISP connection.

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

AKAMAI CONTROL CENTER CONFIGURATION

Prior to configuring Aruba Orchestrator, complete following steps on Akamai Control Center.
Configure Branches as Locations in SLA

**NOTE:** For reference, see [https://techdocs.akamai.com/etp/docs/create-location](https://techdocs.akamai.com/etp/docs/create-location).

1. Log in to the Akamai Control Center.
2. Using the top-left menu, navigate to **Your services > Enterprise Security > Enterprise Center**.
3. From the left sidebar, navigate to **Threat Protection > Locations**.
4. Click the + icon at the top-left of the screen to add new location.
5. Add the branch details, such as name and public IP address, and then associate an existing location policy.
6. Click **Save**.
7. To commit the changes, click **Save and Deploy**.
8. Repeat the steps in this procedure for each branch location.

**Configure IPsec Credentials in SLA**

**NOTE:** For reference, see [https://techdocs.akamai.com/etp/docs/prepare-sdwan-setup](https://techdocs.akamai.com/etp/docs/prepare-sdwan-setup).

1. From the left sidebar in the Akamai Control Center, navigate to Threat Protection > Clients & Connectors > Connection Credentials.

2. To add new IPsec credentials associated with an IKE identifier, click the + icon.

3. Enter the IKE identifier name for your SD-WAN fabric and pre-shared key used for IPsec negotiation.

**Akamai POP FQDNs**

To build tunnels from SD-WAN appliances to Akamai, use the primary and secondary DNS names below. When an individual appliance resolves these FQDNs, the nearest Akamai POP IPv4 address resolves as well, with resulting SD-WAN appliances automatically picking up the nearest POP location to build tunnels.
• primary.ipsec.akaetp.net
• secondary.ipsec.akaetp.net

These will be used for the configuration steps in the next section.

**ARUBA ORCHESTRATOR TUNNEL CONFIGURATION**

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

1. Log in to your Aruba Orchestrator.

2. Navigate to *Configuration > Cloud Services > Service Orchestration*, and then click *Add Service*.

   The Add Service window opens.

3. Enter a name and prefix—in this example, *Akamai* and *AKA*, respectively—and then click *Save*.

   This should create a new service on the Service Orchestration tab called *Akamai*.

The sections that follow explain how to configure each of the tabs under the Akamai service.

**Remote Endpoint Configuration**

This section explains how to configure the primary and secondary Akamai POP endpoints using the FQDN identified previously, along with the pre-shared key configured in the Akamai Enterprise Center.
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-POP</td>
</tr>
<tr>
<td>IP Address</td>
<td>secondary.ipsec.akaetp.net</td>
</tr>
<tr>
<td>Interface Label</td>
<td>any</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>Enter the key configured in the Akamai Enterprise Center.</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-POP</td>
</tr>
<tr>
<td>IP Address</td>
<td>primary.ipsec.akaetp.net</td>
</tr>
<tr>
<td>Interface Label</td>
<td>any</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>Enter the key configured in the Akamai Enterprise Center.</td>
</tr>
<tr>
<td>Backup Remote Endpoint</td>
<td>Secondary-POP</td>
</tr>
</tbody>
</table>
Interface Labels

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

1. Click **Interface Labels**.

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

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

3. Click **Save**.
Tunnel Settings

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

Akamai-supported cipher suites for IKE and ESP are listed here: https://techdocs.akamai.com/etp/docs/ipsec-cipher-suites. This serves as a reference when configuring the tunnel settings.

1. Click Tunnel Settings.
2. Configure the General tab as follows:

3. Configure the IKE and IPsec tabs as follows.

**NOTE:** The IKE identifier is configured based on the IPsec credential settings in the Akamai Control Center. It is important to enter the same string copied from Akamai Control Center > Enterprise Center > Threat Protection > IPsec Credentials.
4. Click **Save**.

**IP SLA**

This section illustrates how to enable IP SLA settings so the appliance can monitor tunnel health using HTTPS probe to sp-ipsla.silverpeak.cloud. The probe destination URL in this setting can be customized.

1. Click **IP SLA**.

2. Configure the IP SLA Settings for Akami window as follows:
NOTE: Take special care to ensure that the following settings are configured correctly:

- **Enable IP SLA rule orchestration**: Enabled
- **Monitor**: HTTP/HTTPS
- **Source interface**: Select the interface label from the drop-down list. In this example, Loopback is selected. IP SLA uses this value to source probe traffic to the probe destination address. Note that for the IP SLA profile to be pushed to the SD-WAN appliances, there must be at least one interface on the appliance with the matching label.
- **HTTP request timeout**: 2

3. Click **Save**.

**BIO Breakout**

This section explains how to ensure that the tunnels created for the Akamai 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 BIO, upload a Service Icon.
4. Click **Save**.

**Remote Endpoint Association**

This section explains how to associate the Akamai endpoints to the EdgeConnect SD-WAN appliances. When association is completed, Aruba Orchestrator pushes the required IPsec tunnel configuration and IP SLA configurations to the EdgeConnect appliances.
1. In Orchestrator, select the appliances from the left-side Appliance Tree. This example will associate all appliances with the Akamai endpoints.

2. Click Remote Endpoint Association.

3. Select the Add check box next to Primary-POP. This associates both the primary and secondary Akamai endpoints with the EdgeConnect SD-WAN appliance.

4. Click Save.

REDIRECT TRAFFIC TO THE AKAMAI SERVICE USING BUSINESS INTENT OVERLAY

This section explains how to configure the Business Intent Overlay for which internet traffic is directed to the Akamai service.

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 will reconfigure an existing overlay called CASB.
3. In the Match field, click the **Edit** icon.

4. Modify the Overlay ACL to match **TCP port 80 (HTTP)** and **443 (HTTPS)**.

5. Click the **Breakout Traffic to Internet & Cloud Services** tab.

6. Drag the **Akamai** policy from the Available Policies column to the Preferred Policy Order column.
NOTE: It is important to put the Akamai policy at the top of the Preferred Policy Order. This enables all internet-bound traffic to be redirected to Akamai tunnels.

7. If you select **Backhaul Via Overlay, Break Out Locally**, or both to use as backup options, then if the Akamai tunnel service goes down, traffic is redirected using these policies. If you do not want a backup option, remove them from Preferred Policy Order. In that case, internet-bound traffic drops if the Akamai 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. If more than one interface is added to the Primary section, then the traffic is load-balanced on the Akamai IPsec tunnel built on those WAN interfaces.
9. To complete the setting changes, click **OK**.

10. To complete Business Intent Overlay configurations, click **Save and Apply Changes to Overlays**.

**VERIFY SERVICE ORCHESTRATION CONFIG PUSH TO DEVICES**

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

1. Navigate to **Orchestrator > Tools > Audit Logs**.
2. Search for **AKA** (or the prefix entered when configuring the Akamai service).
   a. The image below shows that the passthrough tunnel configuration has been pushed to the device successfully.
NOTE: Passthrough tunnel configuration will only be pushed if at least one matching WAN label (as configured under Interface Labels) exists on the EdgeConnect SD-WAN appliance.

b. The image below shows that the FQDNs for NSLOOKUP have been applied successfully. Because FQDNs are used for the primary and secondary POP, the EdgeConnect SD-WAN appliance must be able to resolve those FQDNs before tunnel can be built.

c. The image below shows that IP SLA rules have been pushed to the device successfully. IP SLA rules are pushed to the device only if the following two conditions are met:

i. 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 IP SLA).

ii. There is at least one overlay (under Business Intent Overlay) using the Akamai service tunnel in the Preferred Policy Order section. (see Redirecting Traffic to Akamai).

VERIFY TUNNEL STATUS AND IP SLA STATUS

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 IP SLA probes are working through the tunnel.
Passthrough Tunnel Status

On the Akamai Service Orchestration tab, click Tunnels. The Tunnels tab of the Orchestrator opens, allowing you to view the IPsec tunnel status of the appliances:

![Tunnels Tab]

IP SLA Status

On the Akamai Service Orchestration tab, click IP SLA. The IP SLA tab of the Orchestrator opens, allowing you to verify tunnel health using IP SLA probes:

![IP SLA Tab]
VERIFY ACTIVE FLOWS ON THE EDGECONNECT SD-WAN

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

2. Filter based on IP or port number.

The example below has filtered traffic for a PC with an IP address 172.23.21.30. The traffic matches the CASB overlay, and inbound and outbound tunnels show as "AKA_Primary-POP_INET1." This confirms that the traffic is being redirected to the Akamai service tunnel properly and the user has successful inbound and outbound connections through the Akamai service tunnels.