Silver Peak

EdgeConnect

Deployment Guide for Partners

A step-by-step guide to managing successful EdgeConnect 8.1.x deployments

2017

Contents

Before You Begin

This document means to help Silver Peak resell partners understand the deployment process for Silver Peak Unity EdgeConnect appliances. The four aspects of deployment are:

- Unity EdgeConnect CPO or POC request
- Unity Orchestrator for management and control of the EdgeConnect appliances
- Unity EdgeConnect Headend/Data Center appliance(s)
- Unity EdgeConnect branch appliance(s)

This document will guide you through the necessary steps to first deploy the Orchestrator and then the EdgeConnect appliances. Where appropriate, links to online documentation are provided to offer additional detail, as required.

Prior to beginning deployment, you must acquire the following information from Silver Peak:

- an Account Name
- an Account Key
- a valid license for Orchestrator and all EdgeConnect appliances

As long as a valid request has been submitted by your Silver Peak account representative, all of this information will be provided in an email to the customer. Silver Peak partners are unable to obtain this information directly.

Unity Orchestrator Considerations

The Silver Peak Unity Orchestrator provides a single pane of glass for manageability of all Silver Peak appliances in the WAN. From Orchestrator you are able to provision, deploy, configure, monitor and troubleshoot your Silver Peak SD-WAN regardless of the make, model or deployment type. Orchestrator will manage physical, virtual and cloud-based EdgeConnect appliances seamlessly from a single console.

Orchestrator is only offered as a virtual appliance and, therefore, requires a suitable host to run on. It will be required to identify an appropriate host machine with adequate resources to host the Orchestrator. Typical deployment locations for Orchestrator would be in a Network Operations Center (NOC) or Data Center, though any location with efficient access to the WAN devices could be suitable. For more

information on Orchestrator requirements, refer to the *Orchestrator Host System Requirements* on Silver Peak's User Documentation site.

For licensing, the Orchestrator (IP address) must be able to reach the Silver Peak Cloud Portal via the Internet. Allocate an appropriate IP address for the Orchestrator appliance and allow it access through any security components in the environment to the "silver-peak.com" domain. (Orchestrator requires port 443 access.)

Prerequisites

Before you begin your deployment:

- Read this entire guide before your first EdgeConnect deployment.
- Silver Peak recommends that all new EdgeConnect and Orchestrator deployments run VXOA version 8.1.4.0 or above.
- Prior to making any network changes, it's good idea to print and work with the customer to complete the deployment worksheet in Site Deployment Worksheet.
- This guide assumes a bridge mode deployment where the MPLS and INTERNET are in separate layer 3 subnets.
- Each EdgeConnect appliance requires one IP address in the subnet being bridged
- During installation, you should be online to facilitate access to latest documentation and support information, should they be needed.
- Be sure to confirm access to the customer virtual environment.Check logins and access permissions prior to deployment.
- This guide assumes a bridge mode deployment, which means the network will be down for a brief time. Please plan accordingly.
- Prior to deploying any EdgeConnect physical appliance, you must have a detailed understanding of the customer's network as it relates to the wide area network (WAN), including a detailed diagram showing IP addressing and physical connections. If you are planning to deploy EdgeConnect virtual appliances, download the quick start guide for virtual appliances, which outlines the detailed steps for your deployment type.
- The deployment in this document assumes you have a single MPLS router and a single Internet firewall at the site—each device is deployed in its own subnet. If your customer's network does not match this criteria, please reach out to the Silver Peak Deployment Engineer for your region for additional deployment options and guidance.

Setting Up

Step 1: Download the Orchestrator Virtual Appliance Package

1. Using your preferred browser, go to: *https://www.silver-peak.com.*
2. Go to *Partners* > *Partner Login*, then click **Login**.
3. Enter your Silver Peak partner login information.

   If you do not have a partner login, click **Request Login**.

   Once you submit the online registration form, you will receive an email with your partner login information. If you don't see the email, check your spam or junk folder.

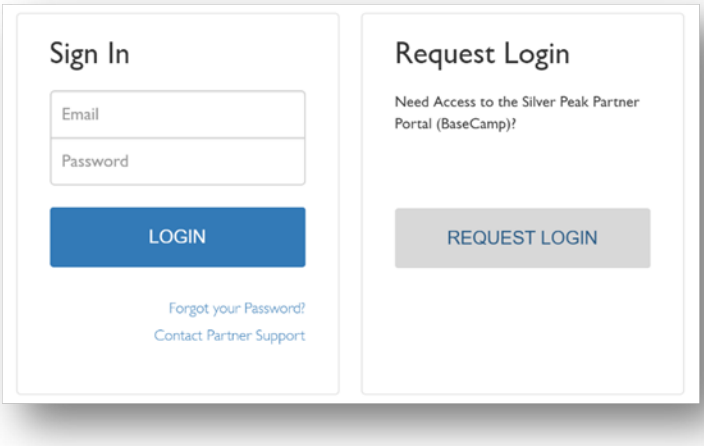


Figure 1. Partner login screen.

4. Once you are logged in, select **Download Software**.

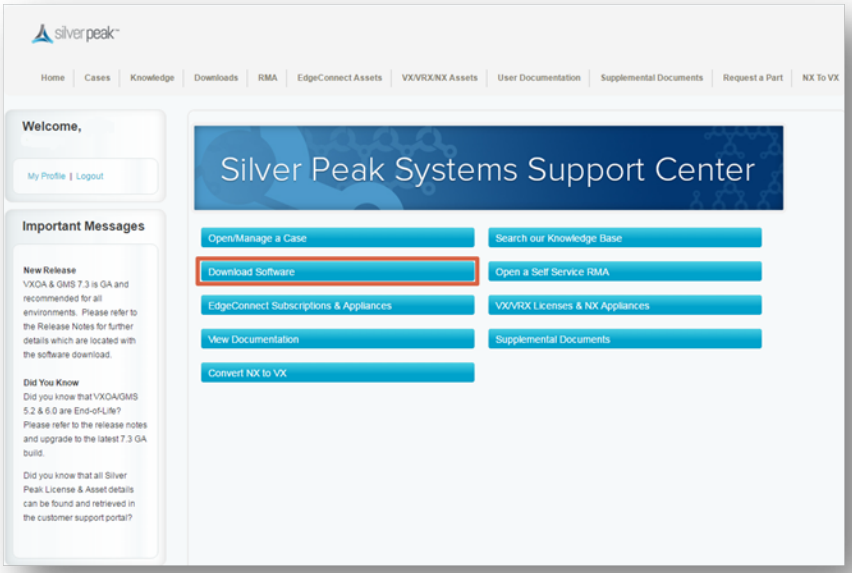


Figure 2. Silver Peak Systems Support Center Download section

5. Select the Unity Orchestrator file for your appropriate hypervisor.

> **NOTE:** For this deployment, we are using VMware for our hypervisor. Be sure to select the appropriate hypervisor download file for your target environment.

6. Select **Initial Installation Packages**.
7. Select **Orchestrator (GMS)**.
8. Select **GA** (General Availability).
9. Select the recommended release number to download your OVA file.
10. Save the OVA file in a location where you can import it into your VMware vSphere environment.

Once the OVA file for Unity Orchestrator has been downloaded, it is ready to be deployed via the hypervisor.

The next step shows how to deploy Orchestrator in a VMWare environment. However, Silver Peak supports the following hypervisors:

- VMware
- Microsoft Hyper-V
- Citrix XenServer
- KVM

Step 2: Deploy the Orchestrator Virtual Appliance

Now you can deploy the Unity Orchestrator appliance VMware vSphere. The Quick Start Guides in the *documentation* section of our website can help with this process. For this example, see *Silver Peak Unity Orchestrator Quick Start for VMware.*

Step 3: Configure the Orchestrator

After you have deployed and configured Orchestrator, verify that the Orchestrator instance can connect to Silver Peak's Cloud Portal.

1. Log into Orchestrator, then go to *Orchestrator Administration* > *Silver Peak Cloud Portal*.

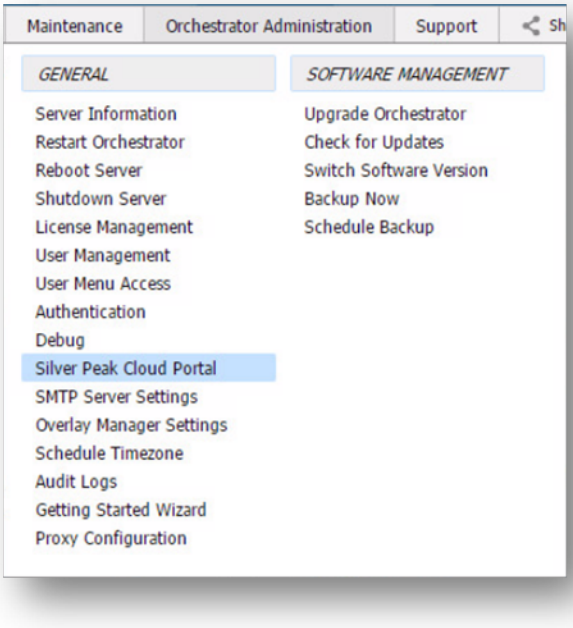


Figure 3. Access the cloud portal configuration from the Orchestrator.

2. Configure the Cloud Portal Host and Port fields:
   - Host: cloudportal.silver-peak.com
   - Port:443
3. Under the **Registration** section, enter the **Account Name** and **Account Key**.

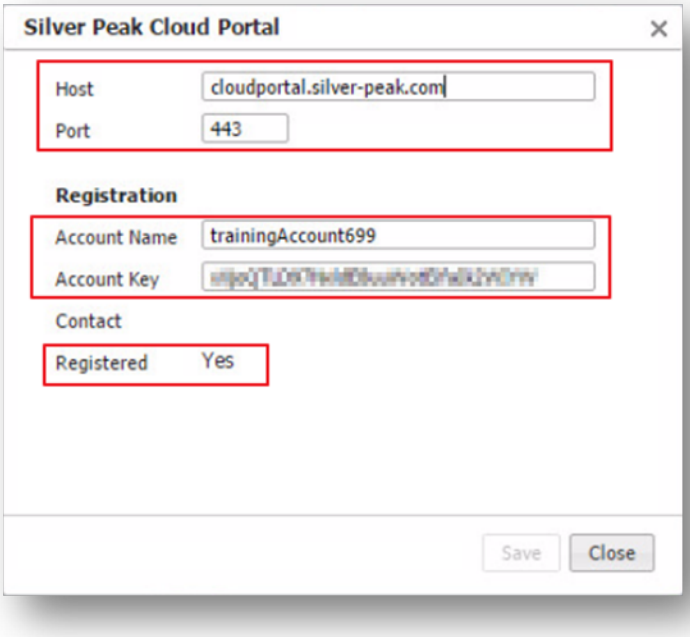


Figure 4. Configure the cloud portal access from the Orchestrator.

Your customer received an email with the registration information. Be sure to use the correct Account Name, Key and Licenses for each installation.

Without proper licensing the appliances will BLOCK traffic.

The **Registered** field should show **Yes**, as displayed in Figure 4. This confirms the registration information is correct and the Orchestrator can connect to the Silver Peak Cloud Portal.

If you are unable to successfully validate registration or connectivity, verify the account information and check that the Orchestrator has appropriate security permissions enabled.

If further support is needed, contact Silver Peak support.

Step 4: Confirm the Default Business Intent Overlays

1. From your preferred browser, browse to your Orchestrator instance, and log in using your admin credentials.

   The default username/password is admin/admin.

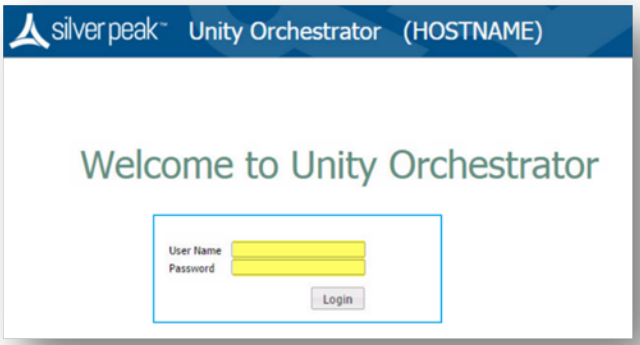


Figure 5. The Unity Orchestrator login screen.

2. Click **Login**.

Step 5: Verify WAN labels

Interface labels are used to identify common transports and aid in configuring tunnels.

1. To create your labels, go to *Configuration* > *Interface Labels*.

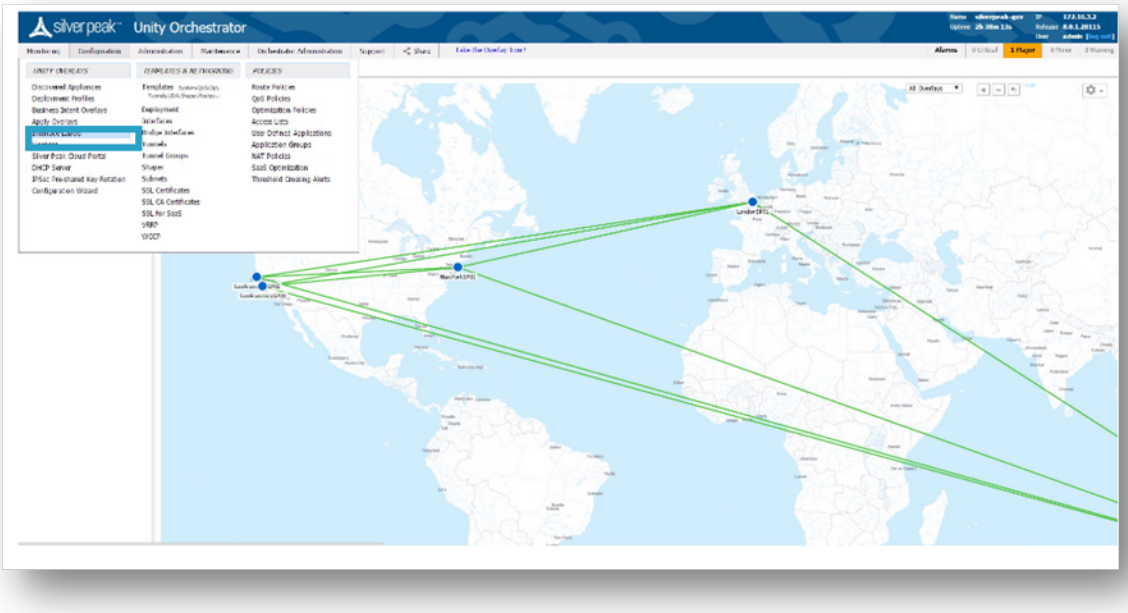


Figure 6. Choose Interface Labels

2. Choose WAN and input the label name.

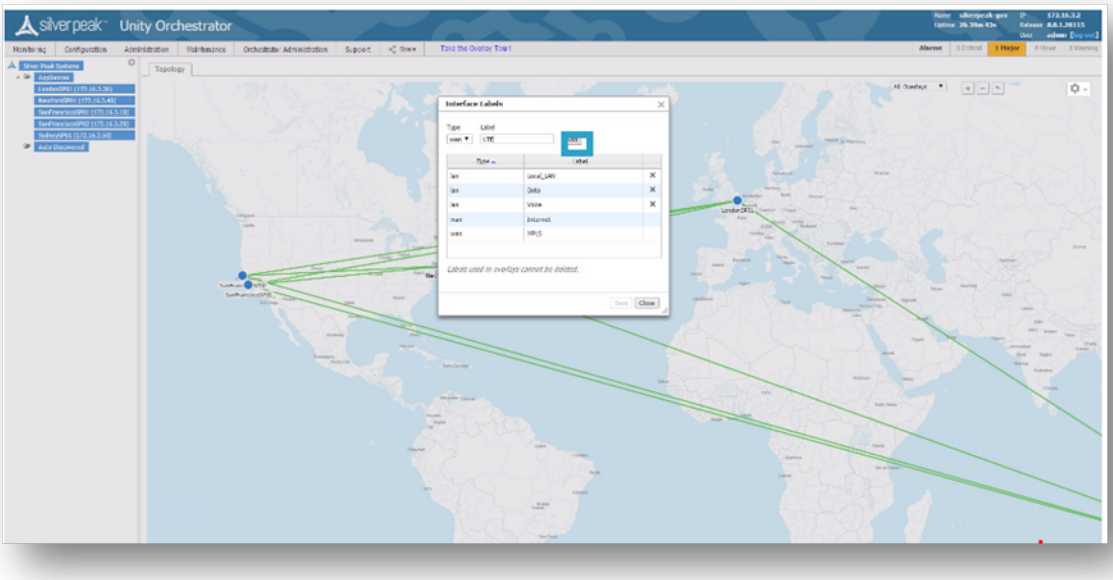


Figure 7. Example: The interface label is LTE.

Step 6: Verify an Access List

Access lists are used to match traffic for processing by a specific overlay.

Best practice is to:

- Create an ACL for real-time traffic to map onto the real-time overlay.
- Create a default ACL to catch all other traffic.

To create an access list:

1. Go to *Configuration* > *Access Control Lists*.

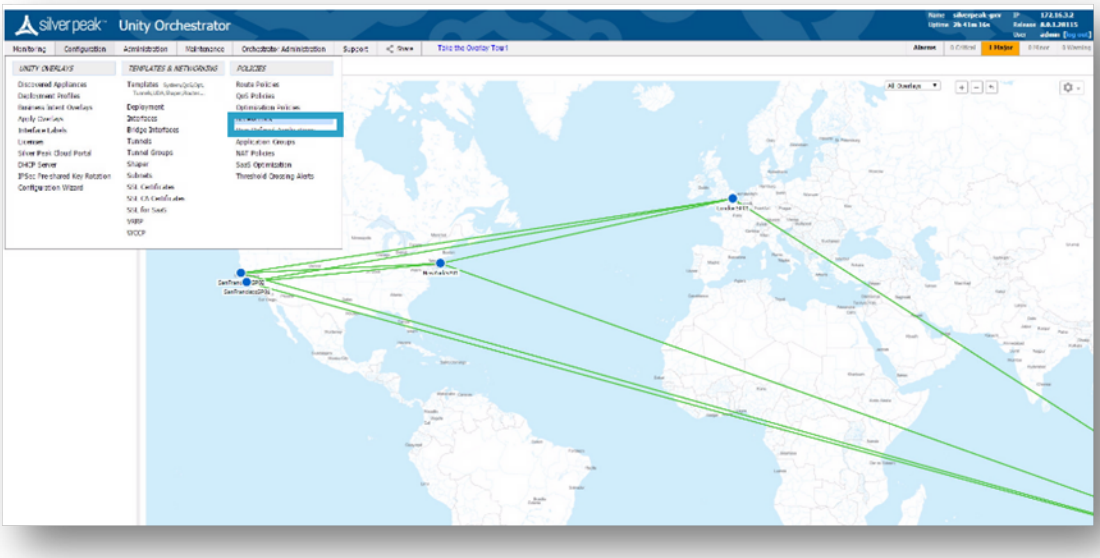


Figure 8. Access Control List

2. Click **Manage Access Lists with templates**.

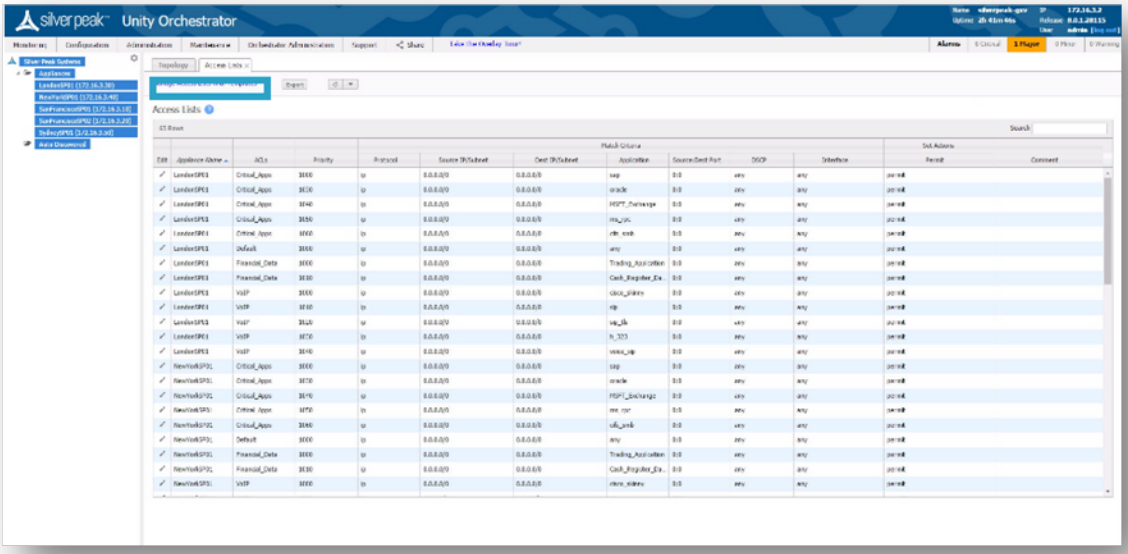


Figure 9. Manage Access Lists with Templates

3. Several Default Access-Lists are already created:
   - **Realtime** – voice and video protocols.
   - **Interactive** – citrix, terminal services, RDP etc.
   - **AnyTraffic** – default permit ip any any.

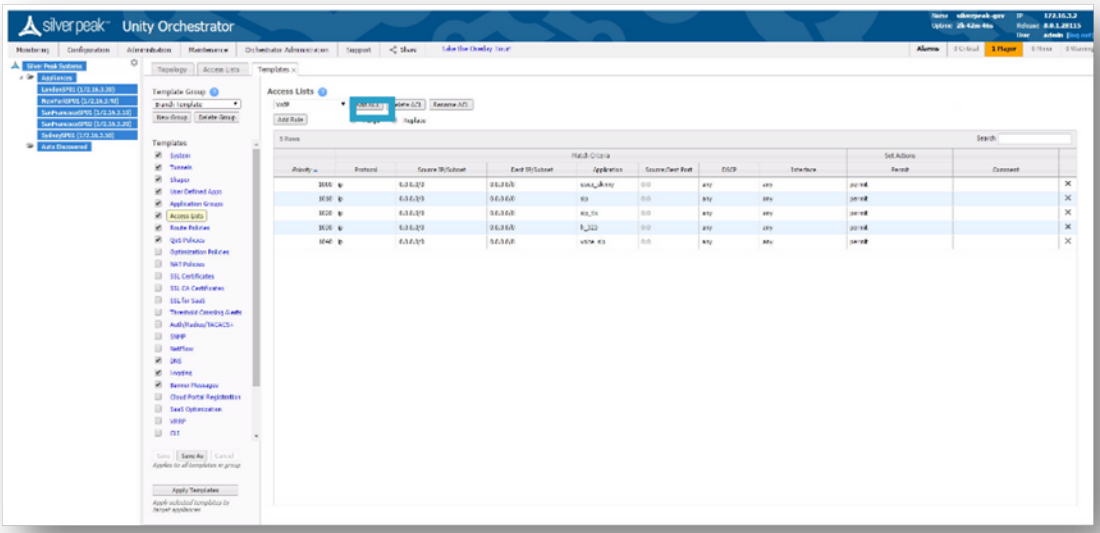


Figure 10. Access Control List Template

4. Make your changes, then click **Save**.

Step 7: Verify a Deployment Profile

Deployment Profiles are used during the deployment wizard to help streamline the installation process by requesting all the locally significant config items per site.

1. Go to *Configuration* > *Deployment*.

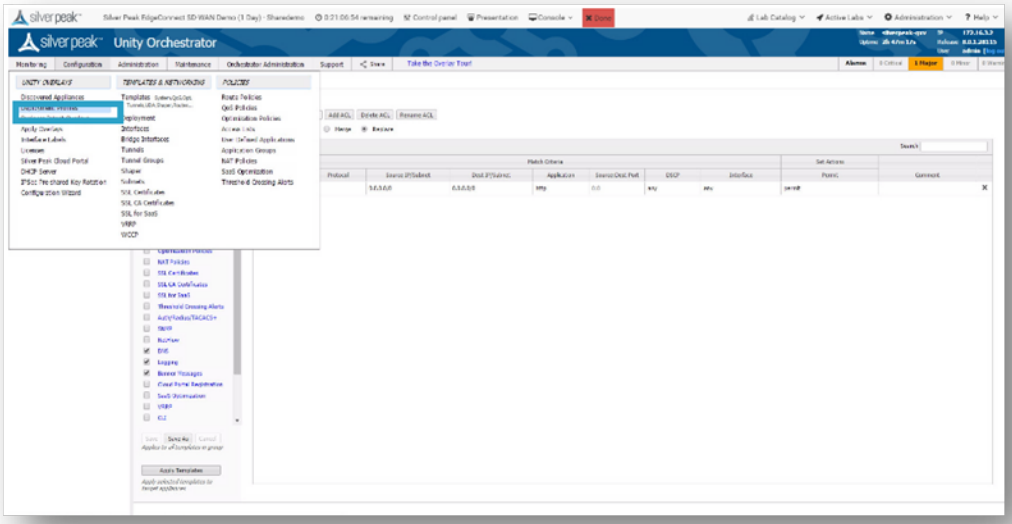
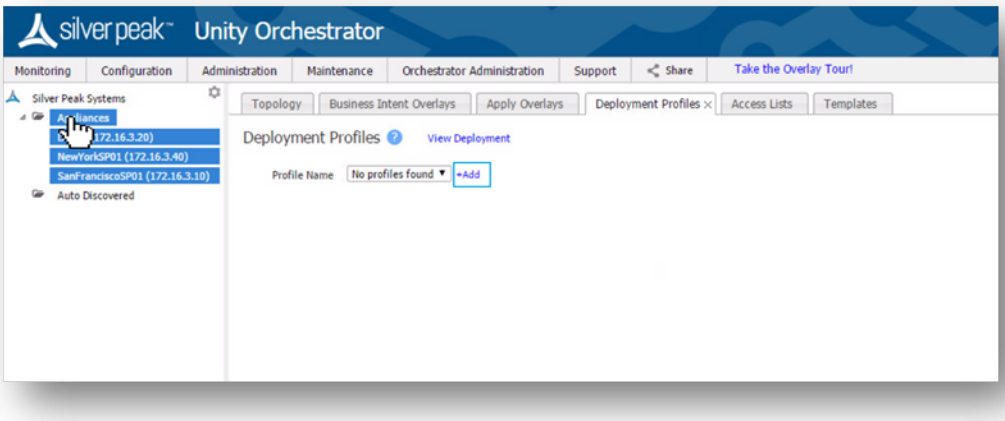
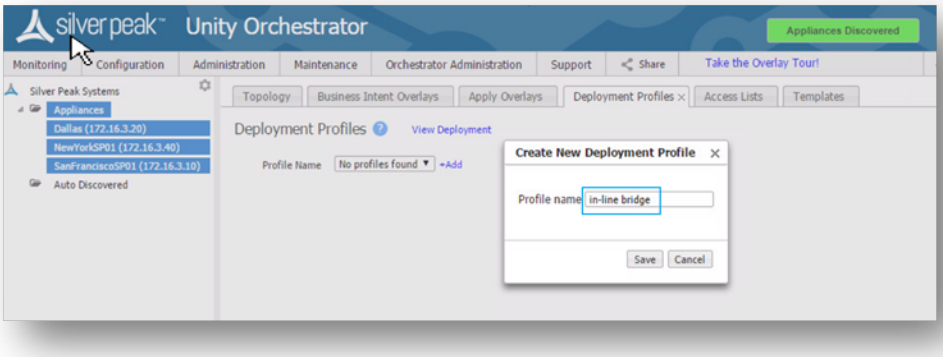


Figure 11. Configuration > Deployment

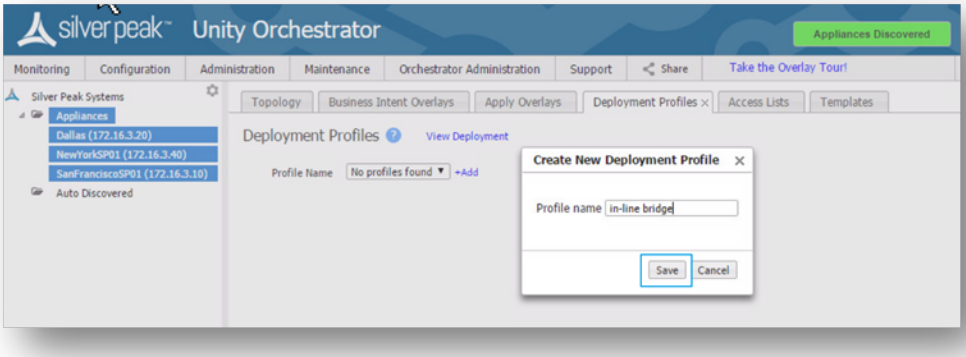
2. A default inline router mode profile exists for routed installations. To implement the inline bridge deployment method, click **Add**.



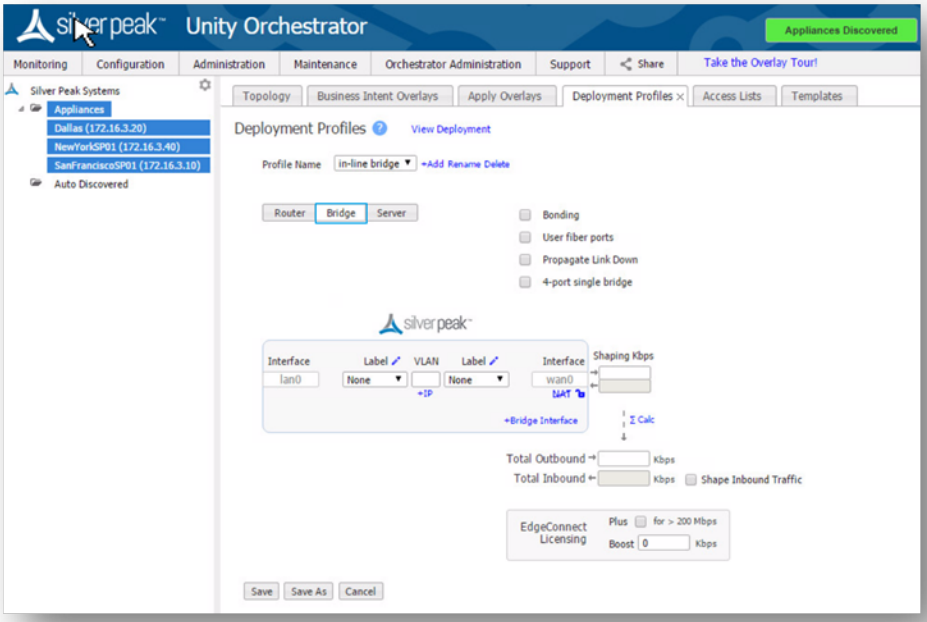
3. Type **in-line bridge**.



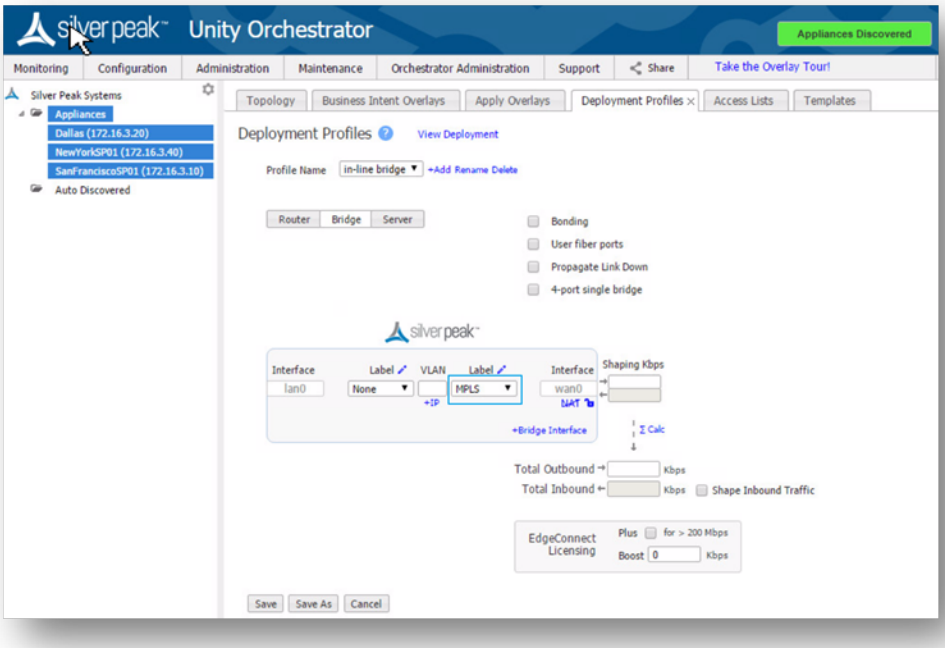
4. Click **Save**.



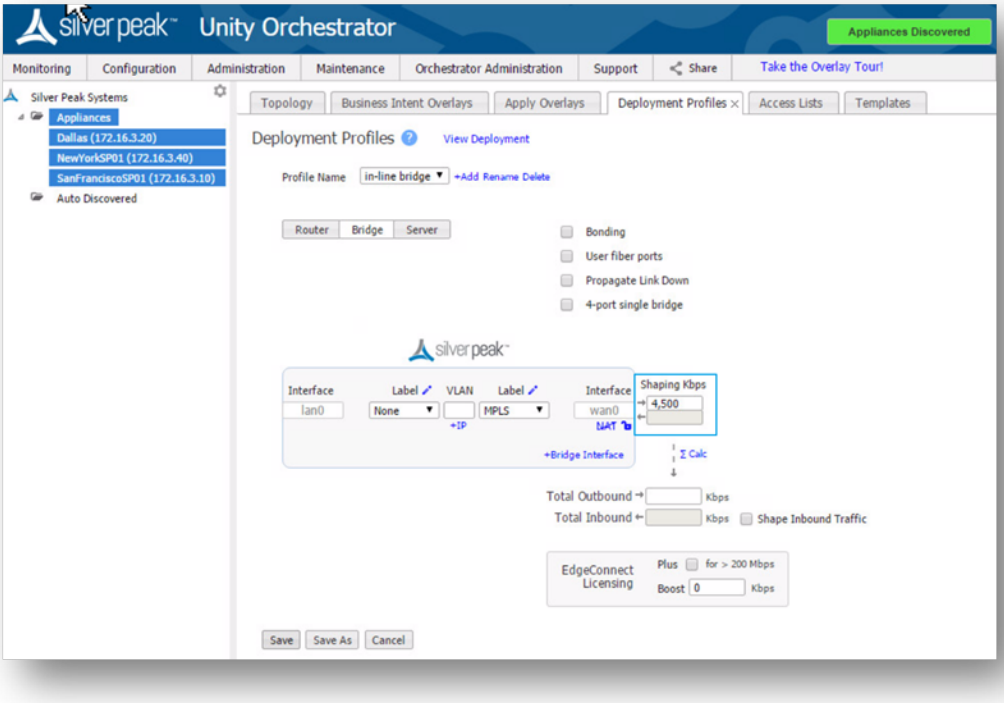
5. Click **Bridge Mode**.



6. Map the WAN label to the MPLS interface.



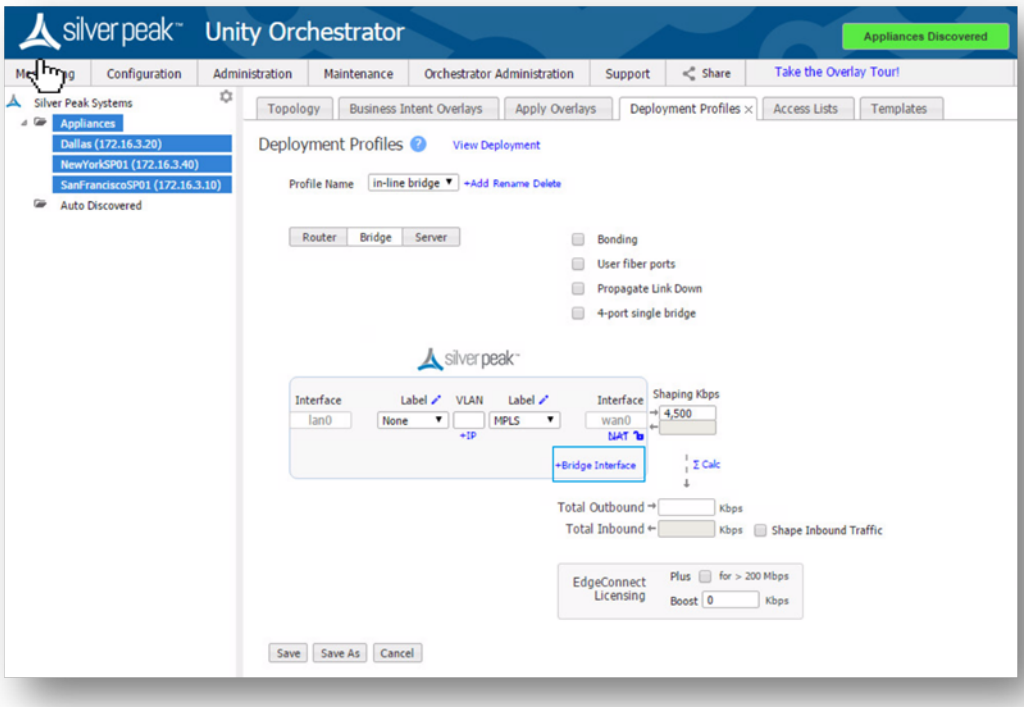
a. Add shaping Kbps to the MPLS interface.



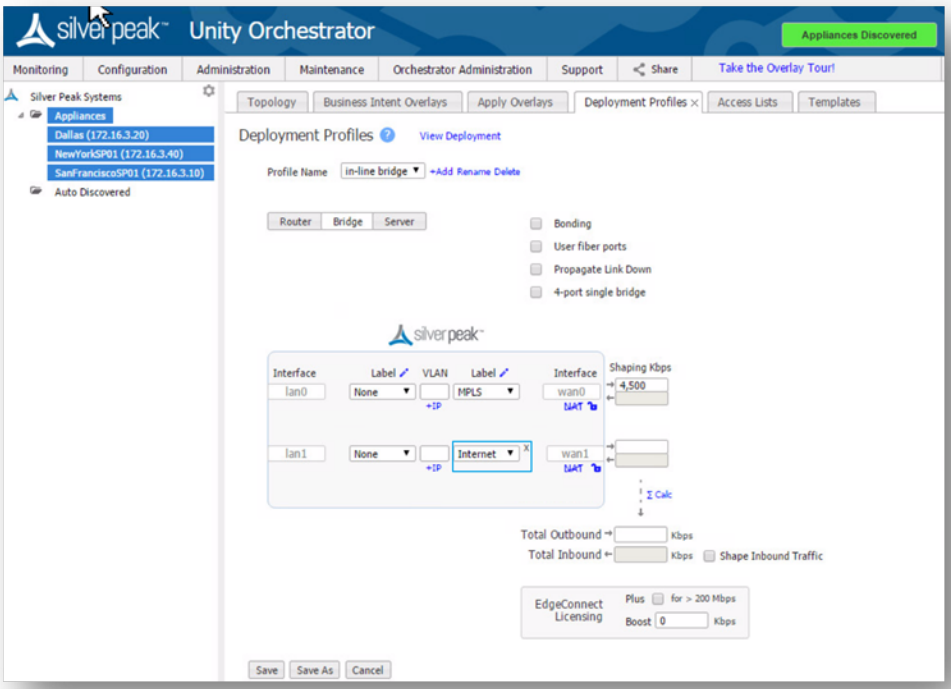
NOTE: It is important to set the actual WAN bandwidth. If you are unsure, use the lower number.

If asymmetric bandwidths, click **shape inbound traffic** to unshadow inbound.

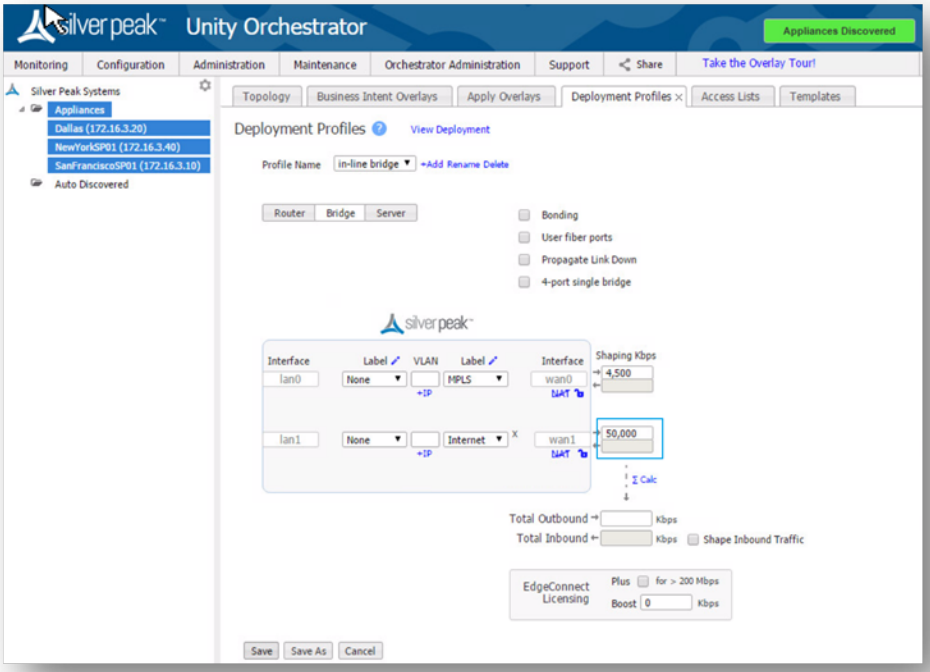
b. ADD the bridge interface for INTERNET.



7. Map the WAN label to the INTERNET interface.



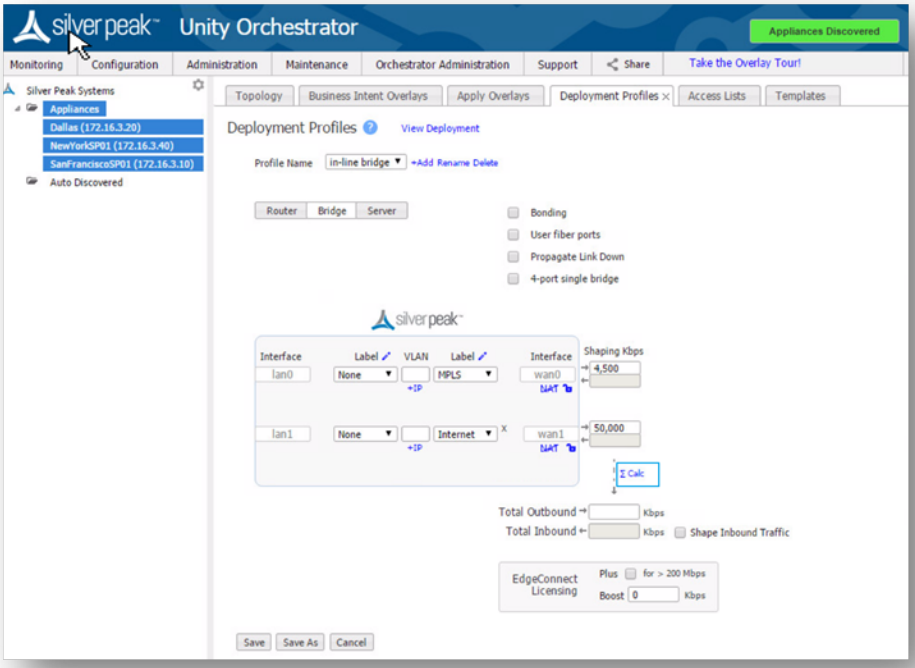
a. Add shaping Kbps to INTERNET interface.



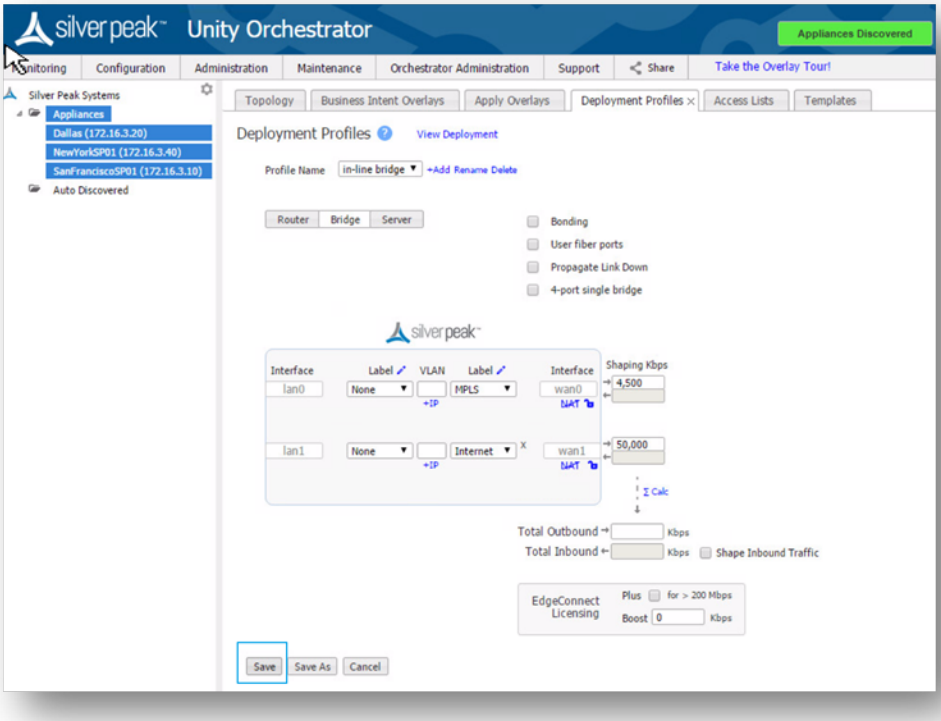
NOTE: You must set the actual WAN bandwidth. If you are unsure, use the lower number.

If asymmetric bandwidths, click **shape inbound traffic** to unshadow inbound.

8. Sum the shaping Kbps.

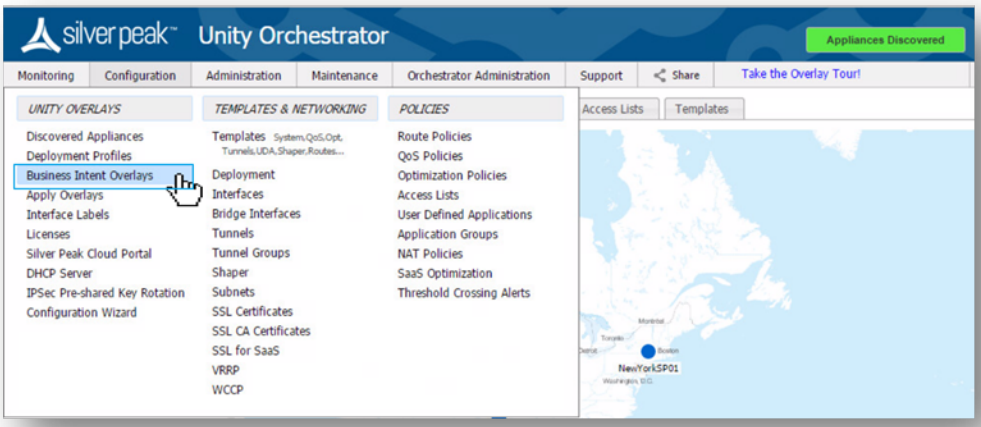


9. Save the Deployment Profile.



Step 8: Verify an Overlay

1. Go to *Configuration* > *Business Intent Overlays*.



Three default overlays are automatically created:

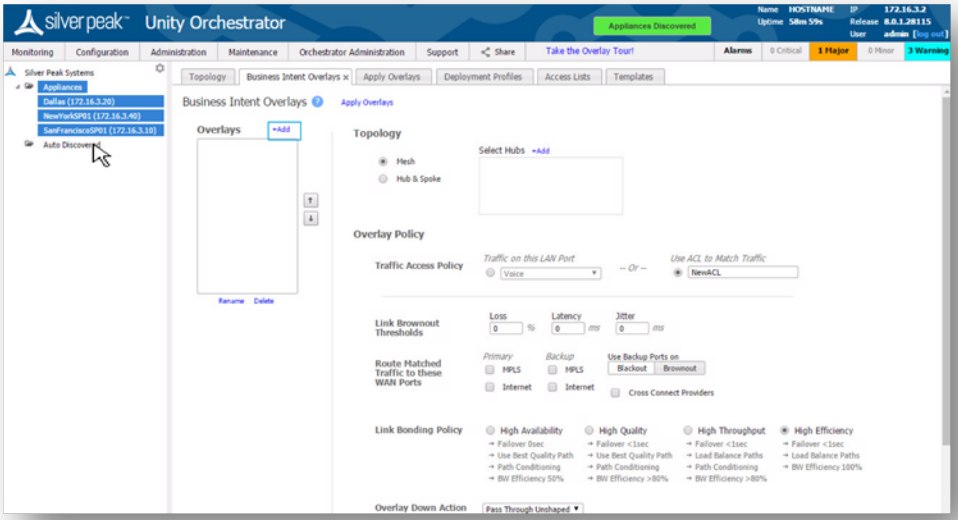
- Realtime – voice and video applications.
- Interactive – Citrix, terminal services, RDP, etc.
- AnyTraffic – default permit ip any any.

> **Note**: You don't need to apply every overlay to every site. If, say, a branch does not have voice, you are not required to apply the realtime overlay to that site.

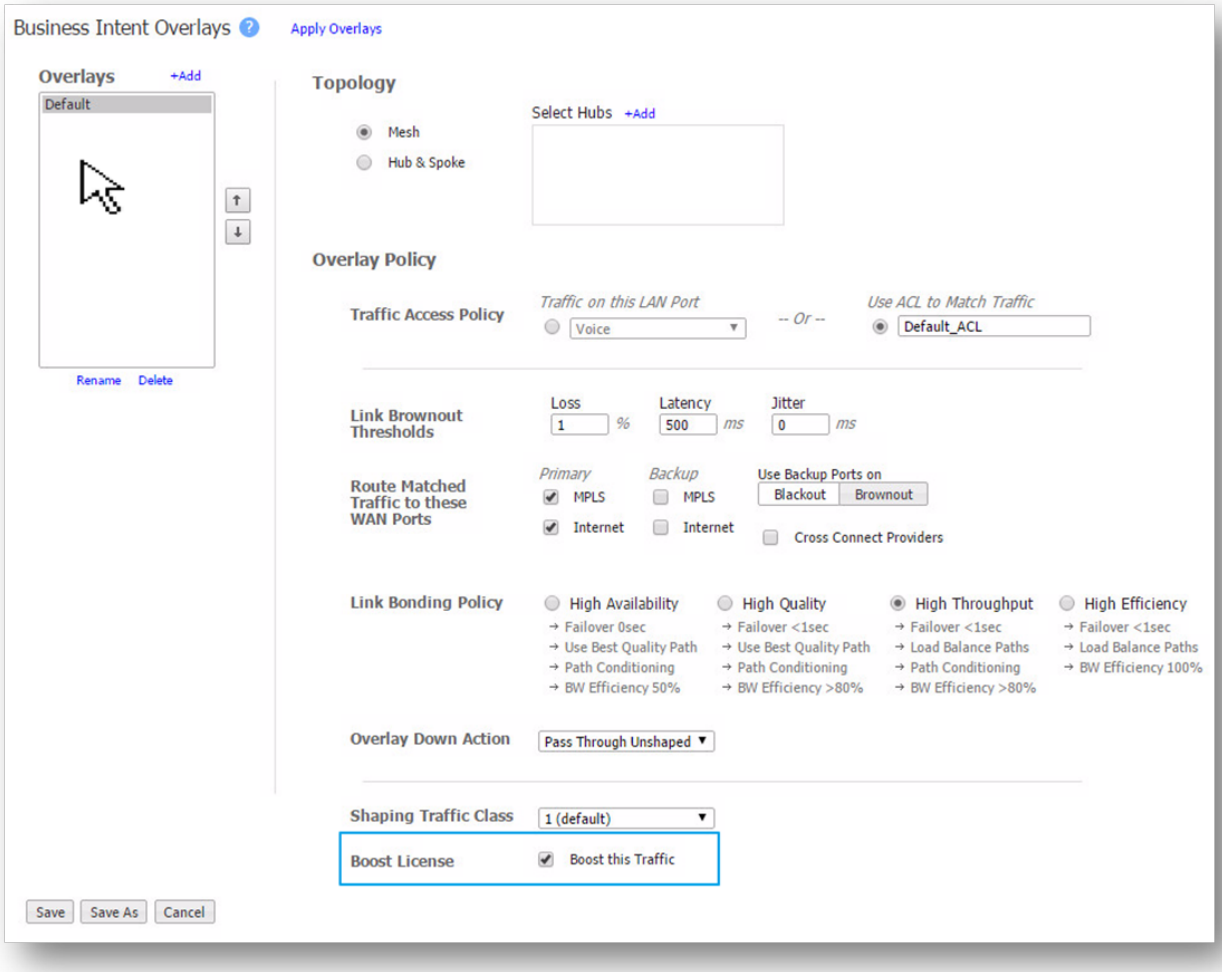
While we recommend using the default settings, you can rename or add additional overlays.

> **Note**: VXOA 8.1 is limited to seven overlays total.

2. Click **ADD**.



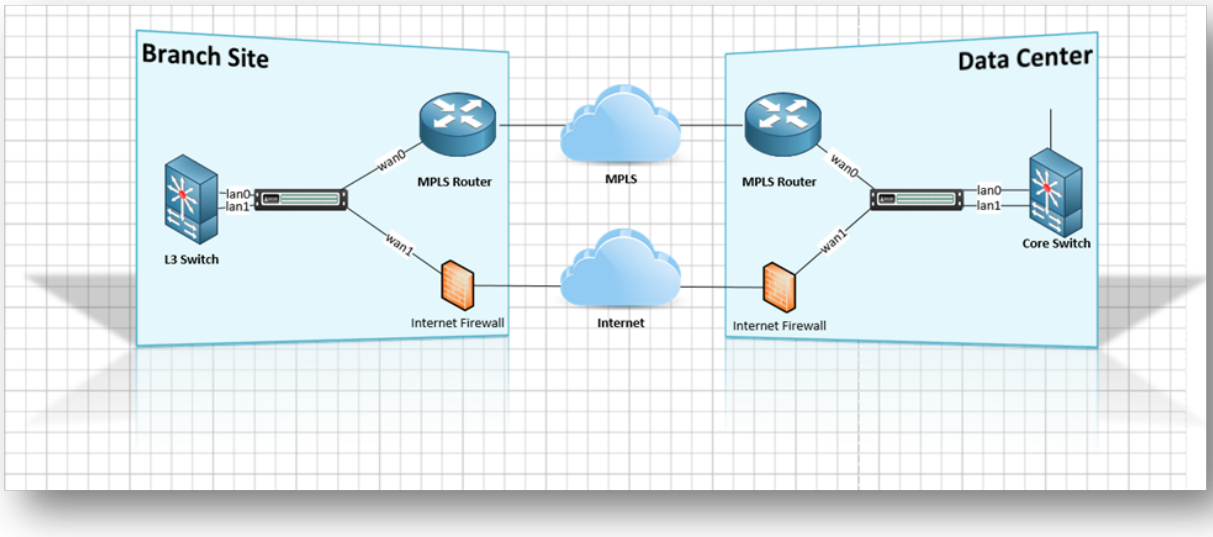
3. Click to enable BOOST if POC or if the CPO included the license



4. **Save**.

   Scroll down to see the Save button or change your web browser zoom.

Sample Customer Network



Deployment

While several deployment scenarios are available to you when deploying an EdgeConnect appliance, this document focuses on the simplest configuration.

- The Data Center headend device as in-line bridge
- The Branch device installed in-line as a bridge

Once you're comfortable with the environment and the deployment plan, keep the following tips in mind:

- Orchestrator must be configured and deployed before any EdgeConnect appliance is installed.
- You must have the license, account keys and account names from Silver Peak.
- The Silver Peak Cloud Portal can act as the rendezvous between appliance and Orchestrator for discovery. It also acts as a secondary channel for the appliance to remain connected with Orchestrator in case the appliance loses direct connection to Orchestrator.
- Check to make sure Orchestrator has access to the Silver Peak Cloud portal.
- OVA files for Orchestrator and EdgeConnect Virtual appliances are available from *www.silver-peak.com*.
- The quick start guides provide a step-by-step process EdgeConnect appliance.
- The deployment of both the Orchestrator and EdgeConnect appliances is easy—simply following the steps in this document.
- Review the Prerequisites.

Installing a Physical EdgeConnect Appliance

Use the same procedure to install and configure a **Data Center** or **Branch** physical EdgeConnect appliance:

1. Download the *Quick Start Guide (QSG) for the Unity EdgeConnect.*
2. Unbox the appliance and place it in the rack using the included rails or ears.
3. Follow the steps provided in the Quick Start Guide.
4. Connect the **mgmt0** port to a DHCP capable switch port and power the unit on.
5. DO NOT connect any LAN or WAN ports until approved, licensed, and configured.
6. Log into Orchestrator. Orchestrator and the physical appliance will both contact the Silver Peak cloud portal and when successful, will illuminate the green **Appliances Discovered** button.
7. Click **Appliances Discovered** 

in the TOP right banner.
8. Click **Approve** to select the appliance you want to manage and bring into your network.
9. Follow the **Appliance Setup Wizard** to configure the appliance.
    - The IP address was identified in the *deployment worksheet*.
10. Once the appliance is licensed, approved and configured, you can schedule the downtime to wire up the Silver Peak to your customers' MPLS and FIREWALL.
11. The following steps affect service:
    a. Remove the LAN side network cable from the MPLS router (make a note of which Ethernet port) connect it to the **LAN0** port of the EC device. Take a new red cross-over cable (included in the packagingz0 and connect it from the **WAN0** port on the EC device to the original MPLS router Ethernet port.
    b. Remove the LAN side network cable from the FIREWALL router (make a note of which Ethernet port) connect it to the **LAN1** port of the EC device. Take a new red cross-over cable (included in the packaging) and connect it from the **WAN1** port on the EC device to the original FIREWALL Ethernet port.
    c. The Alarms regarding link and next-hop should clear.

All IP addresses for LAN & WAN interfaces need to be configured statically for in-line bridge mode.

In-Line Bridge Mode is supported with or without a firewall

For deployments in the branch, one of the simplest options for EdgeConnect appliances is inline bridge mode, when there are two devices involved (MPLS + Firewall). Other deployments are available. For example, a broadband connection can be terminated directly on the EC device. See the appendix for more details.

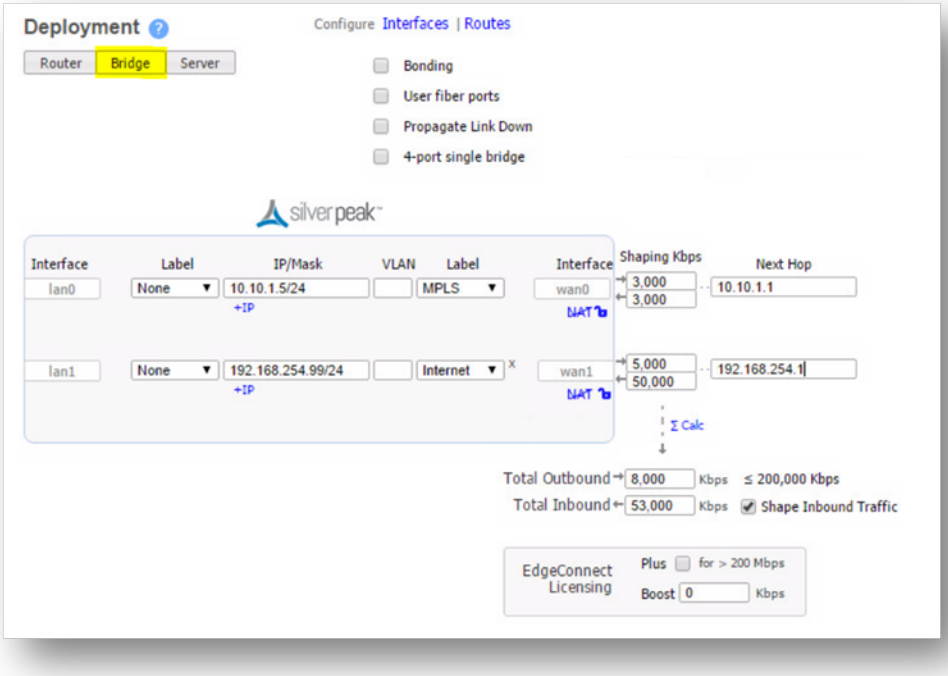
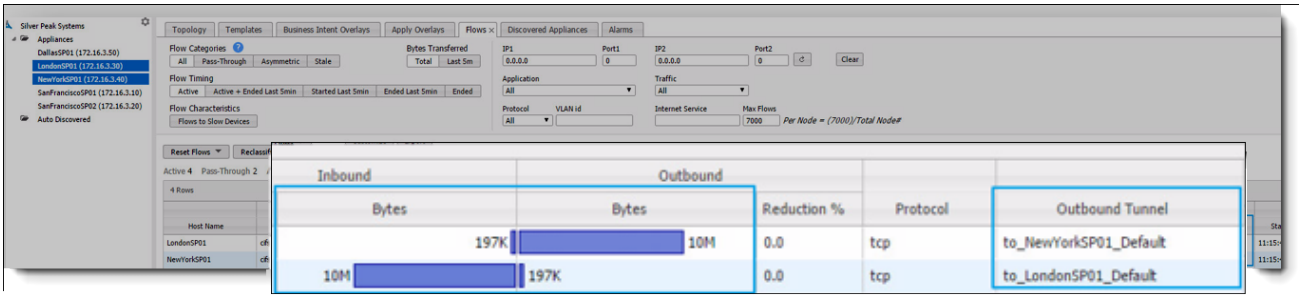


Figure 12. In-Line Bridge Mode Deployment

Validating Traffic

Within Orchestrator, go to *Monitoring* > *Flows*.

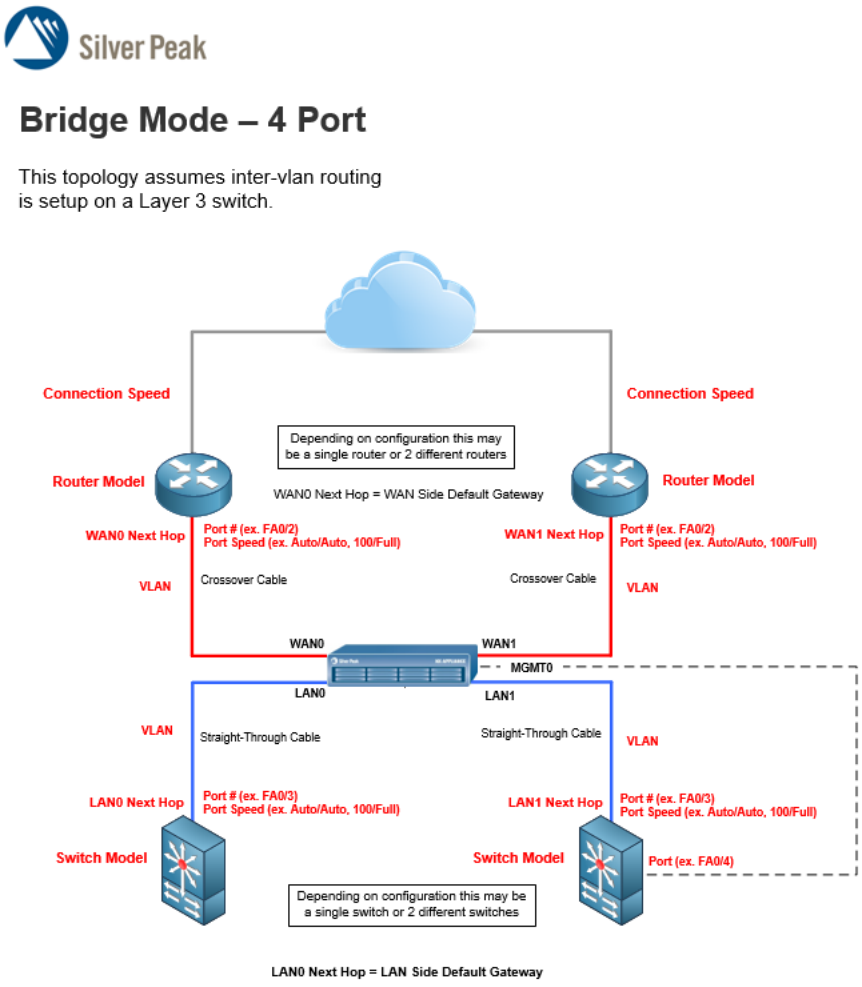
- The flows appear on both the branch and the data center.
- You should see both INBOUND & OUTBOUND bytes; a value of 0 indicates an issue.
- You should see the Default Overlay in use for the outbound tunnel (or Realtime if VOIP).



Appendixes

Appendix A - Site Deployment Worksheet

All IP addresses for LAN & WAN interfaces must be configured statically for in-line bridge mode.



Replace the following example with your specific information:

Site Name	Example
Silver Peak Hostname	HOSTNAME
Deployment Mode	4-Port, Bridge
Management IP (mgmt0)	MGMT0_IP
mgmt0 Default GW	MGMT0_DEFAULT_GW
Appliance IP (wan0)	WAN0_IP
wan0 Next Hop	WAN0_IP_DEFAULT_GW
lan0 Next Hop	LAN0_IP_DEFAULT_GW
Appliance IP (wan1)	WAN1_IP
wan1 Next Hop	WAN1_IP_DEFAULT_GW
lan1 Next Hop	LAN1_IP_DEFAULT_GW

Define VLAN/SUBNETS to Optimize at Local Site

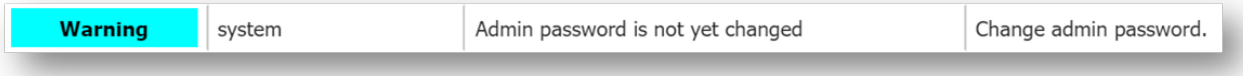
VLAN#	SUBNET/XX	Description
VLAN_#	xx.xx.xx.xx/yy	A description here

Appendix B - Alarms

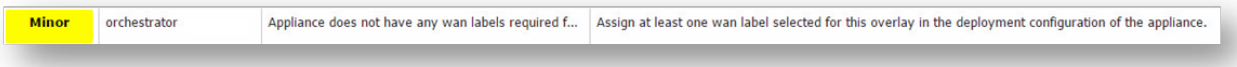
ALWAYS check both the appliance and the orchestrator for alarms, as these provide valuable information in isolating any lingering issues.

The *SD-WAN Deployment Guide* has a detailed section on alarms. This document simply discusses the most common alarms related to deployment of Edge Connect devices and Business Intent Overlays.

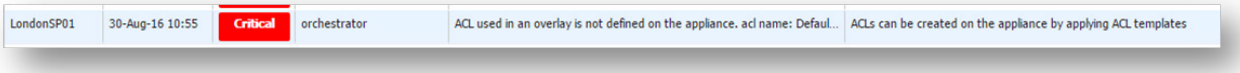
Admin password left as default



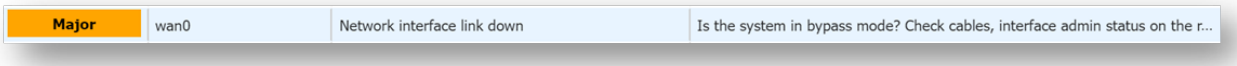
WAN labels not applied, Overlay manager will not build tunnels to appliance



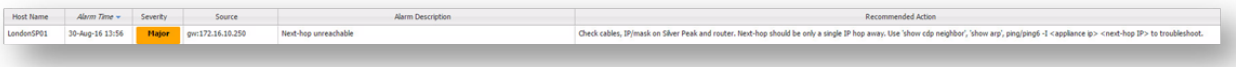
Overlay references an ACL, but no ACL is applied



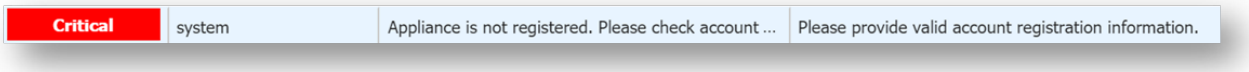
Interface is not connected



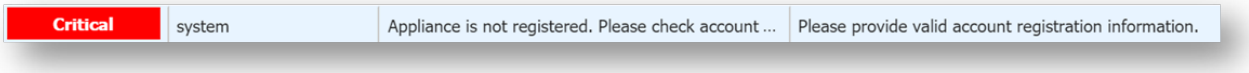
Next hop is not reachable



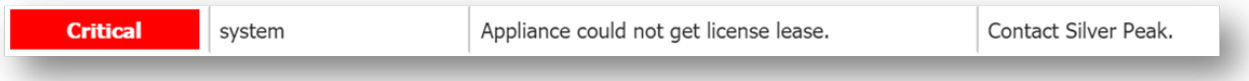
Tunnel DOWN alarms



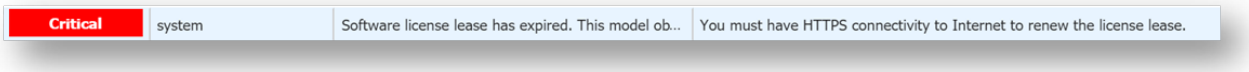
Appliance is not registered



License not granted



License has expired



Appendix C - Tunnel Troubleshooting

Debugging consists of 4 parts:

1. Check the Obvious Stuff
2. Are the Appliances Talking?
3. Debugging IPSec Tunneling
4. Tunneling Alternatives

Check the Obvious Stuff

1. Do you have any Alarms on the appliance or orchestrator?
2. Can you ping the IP address of the next hop?
3. Can you ping an IP address on the internet?
4. Have you verified that you're using the correct public IP address?
    - Does the NAT switch need to be on or off?
5. If the appliance is directly connected to broadband, turn off wan hardening.
    - Can you access the appliance via https and ssh?
    - If so, you know you are on the public internet.
    - **Turn WAN hardening back on immediately.**

Are the Appliances Talking?

1. Verify Bi directional traffic flow
   - Use `tcpdump` to verify traffic is coming/going from the data center
   - ssh to the data center appliance
   - `tcpdump -i bvi0 host 97.174.110.10` (example remote appliance IP)
   - You should see traffic coming and going to that IP
2. If bidirectional conversations are occurring, try changing to GRE or UDP. This is perhaps an IPsec issue, see Debugging IPSec Tunneling.

Debugging IPSec Tunneling

IPSec Troubleshooting - Basic

When debugging IPSec tunneling, look out for:

1. If you have bi-directional traffic via ESP or NAT-T then the appliances are trying to establish an IPSec tunnel.
   - Silver Peak Recommendation: Set the MTU size to 1400 to account for IPSec overhead.
2. Another common scenario occurs when another device appliance responds to IPSec requests, rather than the Silver Peak. If you encounter tunnel connectivity issues, it may be necessary to validate the IPSec response is coming from the correct Silver Peak appliance. If this is found to be happening, most firewalls have an IPSec pass-through feature that can be enabled to get around this.
3. A third scenario to be aware of is the case where no IPSec devices are responding to IPSec requests from the Silver Peak appliance. This scenario could be caused by a misconfiguration of the pre-shared key or IPSec setup. It could also be caused when the IPSec requests are blocked by a firewall or other device somewhere between the Silver Peak appliances.

IMPORTANT: If you're not familiar with IPSec or comfortable troubleshooting using a CLI , we recommend that you involve your network or firewall administrator for assistance in troubleshooting connectivity issues. Making changes to routers, firewalls, and other devices in production environments can cause disruptions in service.

IPSec Troubleshooting – Advanced

Broadcast CLI

Silver Peak Orchestrator provides the Broadcast CLI (BCLI) tool that enables administrators to issue CLI commands centrally from the Orchestrator interface. The BCLI can be used to issue commands to one or many appliances at a time. As long as the Orchestrator can communicate with remote appliances, Broadcast CLI can be used to issue commands for troubleshooting IPSec.

Broadcast CLI can be accessed on the Orchestrator by choosing *Maintenance* > *[Tools] Broadcast CLI*

To identify if another device is responding to *IPSec requests*:

1. Use the BCLI to issue the following command on the remote silver peak:

   (Tunnel name in this example is *tun1*. Replace *tun1* with appropriate tunnel name in your environment.)

```
BRSUPP86 (config) # show int tunnel tun1 ipsec status
Tunnel tun1 ipsec state
  Tunnel Oper:          Down

IPSec Enabled:        yes
  IPSec Oper:           Healthy
  Total IPSec SAs:      in:1 out:1**
  IPSec Key Size:       256 bits
  Replay Window(bits): 1024
```

   NOTE: 1 SA (security association) sent (out) and 1 SA received (in), but we can't validate which device responded to our SA.

2. Issue the following command from the BCLI:

```
BRSUPP86 (config) # show int tunnel tun1 ipsec debug


IPSec stats for tid 2
-----Key-management---
Current state: 2
Req key by dp: 1
Rekey dp: 0
Rekey TO: 0
Rekey # in pkts: 0
```

```
Rekey # out pkts: 0
Key wait TO: 0
Passive key TO: 0

-----In-bound---
Total packets: 0**

Aligment: 0
No sa: 0
Verify fail: 0
Replay check: 0
Decryption fail: 0
Other reason: 0

-----Out-bound---
Total packets: 453
No sa: 6
Encryption fail: 0
Authentication fail: 0
Other reason: 0
```

NOTE: "Total packets" should not be 0. This indicates the firewall in front of us responded, and the Silver Peak appliance never got the request. (Scenario 2, above) In this situation, it is necessary to enable "ipsec passthrough" on the firewall. Alternatively, you could elect to connect the Silver Peak appliance directly to the public internet. (Make sure WAN hardening is enabled and proper security precautions are in place.)

To validate a deeper issue with IPSec packets traversing the network:

1. If the tunnel debug command shows no SAs at all, you could have an issue with the IKE exchange. This scenario could be caused by a misconfiguration of the pre-shared key or IPSec setup. It could also be caused when the IPSec requests are blocked by a firewall or other device somewhere between the Silver Peak appliances.
2. Issue the following command from the BCLI:

   (Replace *tun1* with appropriate tunnel name in your environment.)

```
BRSUPP86 (config) # show int tunnel tun1 ipsec debug

IPSec stats for tid 2
-----Key-management---
Current state: 2
Req key by dp: 1
```

```
Rekey dp: 0
Rekey TO: 0
Rekey # in pkts: 0
Rekey # out pkts: 0
Key wait TO: 0
Passive key TO: 0

-----In-bound---
Total packets: 435
Alignment: 0
No sa: 0
Verify fail: 0
Replay check: 0
Decryption fail: 0
Other reason: 0

-----Out-bound---
Total packets: 453
No sa: 6
Encryption fail: 0
Authentication fail: 0
Other reason: 0
```

The *Current State* output indicates the ISAKMP key exchange state. For reference, here's a table of ISAKMP key exchange states as they map to the *Current State* value:

ISAKMP Key Exchange State	Current State ID
ST_INIT	1
ST_ACTIVE_KEY_WAIT	2
ST_ACTIVE_READY	3
ST_PASSIVE_READY	4

- If you are stuck in ST_ACTIVE_KEY_WAIT (Current State = 2), then you might have an IKE connectivity problem or a pre-shared-key issue.
  - Check firewall config
  - Check pre-shared key entered correctly
- If no IKE exchange is happening at all - the SPs (Security Policies) which packets hit to trigger the IKE session may be wrong or missing, due to misconfiguration
  - Check IP address configuration
- If tunnels come up but we are seeing bad performance
  - Revisit the MTU configuration. MTU may need to be adjusted lower.

Tunneling Alternatives

As an alternative to IPSec encapsulation, you can try setting tunnel encapsulation to **GRE** or **UDP**. Remember, using GRE or UDP encapsulation is useful for troubleshooting, but these encapsulation methods do not provide as much protection as IPSec with encryption.

Using GRE or UDP means that data will be sent in the clear and is NOT recommended for production use across insecure links.

Appendix D - Appliance Interfaces

Unity EdgeConnect Hardware Platforms

silverpeak	EdgeConnect XS	EdgeConnect S	EdgeConnect M	EdgeConnect L	EdgeConnect XL
					
Part Identifier	EC-XS	EC-S	EC-M	EC-L	EC-XL
Typical Deployment	Small Branch	Large Branch	Head Office Small Hub	Data Center Large Hub	Data Center Large Hub
Typical WAN Bandwidth	2 - 200 Mbps	10 - 1000 Mbps	50 - 2000 Mbps	1 - 5 Gbps	2 - 10 Gbps
Recommended Boost up to	50 Mbps	200 Mbps	500 Mbps	1 Gbps	5 Gbps
Redundancy / FRUs	No	No	Power and SSD	Power and SSD	Power and SSD
Datapath Interfaces	4 x RJ45 10 / 100 / 1000	6 x RJ45 1/10G Option	4 x RJ45 2 x 1/10G Fiber	4 x RJ45 2 x 1/10G Fiber	4 x 1/10G Fiber

Appendix E - Alternate Deployment Modes

For more information on deployment modes, see the *Appliance Managers Operation Guide*.

IN-LINE BRIDGE at the Branch with NO FIREWALL

If your branch does not have a firewall, you can plug the broadband directly into the silver peak

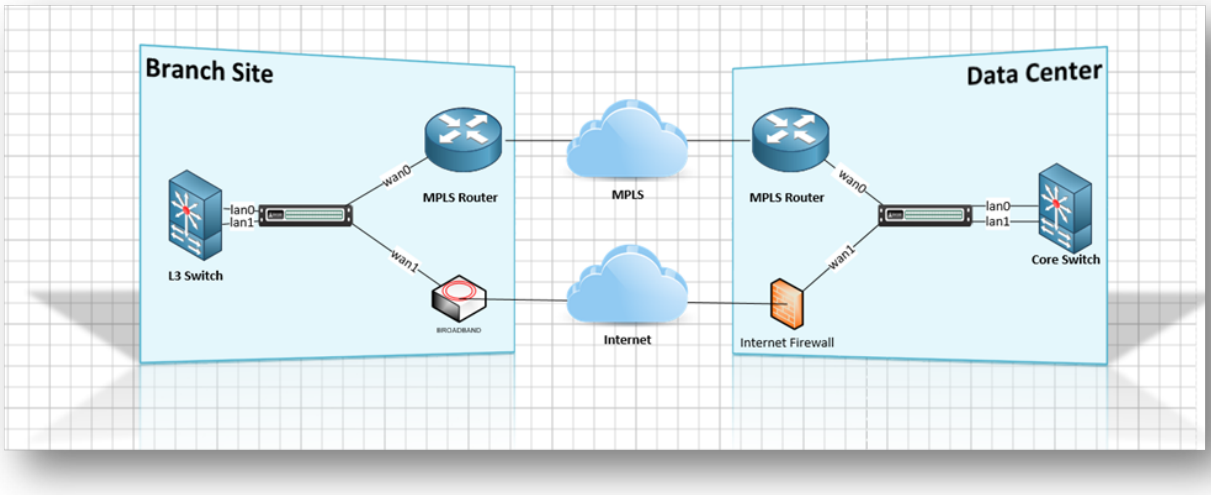


Figure 13. In-Line Bridge – Direct to broadband

For large deployments, the ideal mode in the datacenter is router mode.

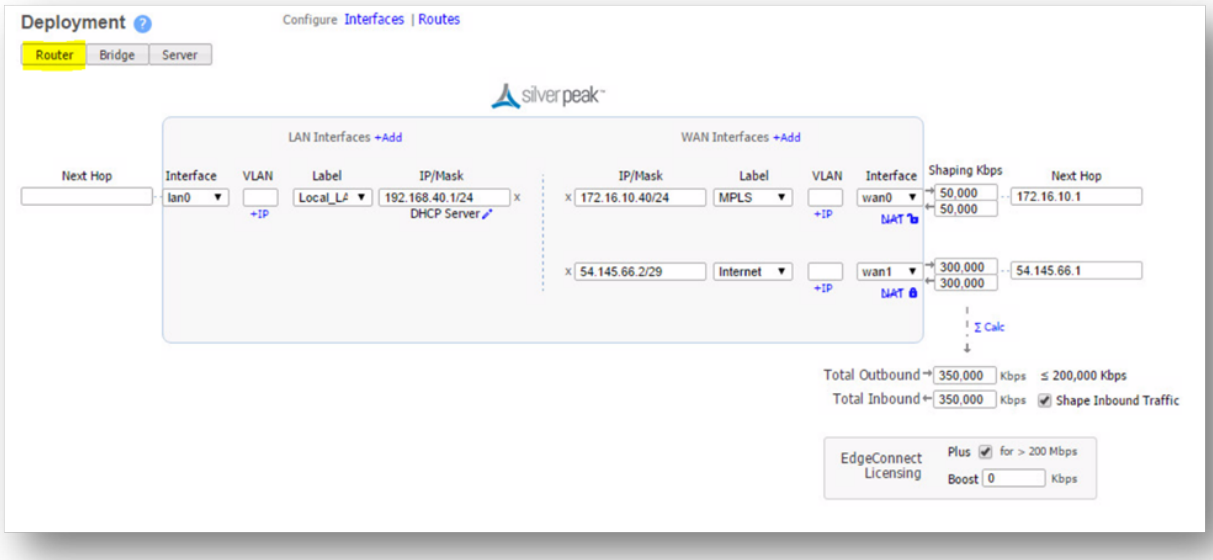


Figure 14. In-Line Router Mode Deployment

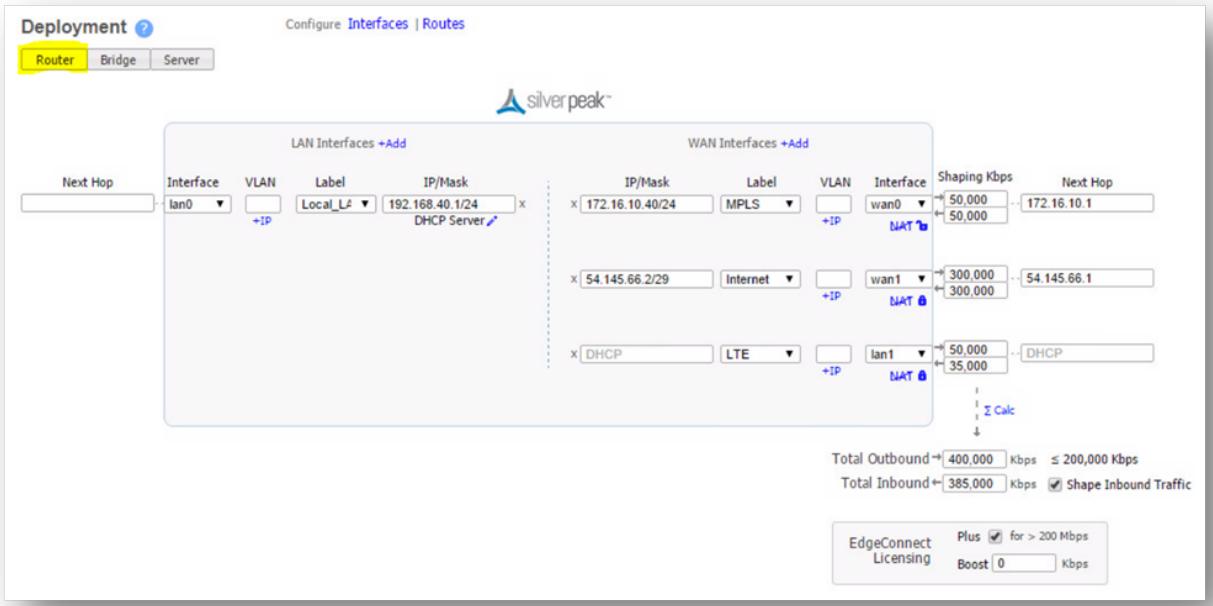


Figure 15. Quad In-Line Router Mode Deployment

Note the use of **lan1** as a wan port. Only the EC-S model ships with an actual **WAN2** port. The other appliances in the EdgeConnect family can utilize any port for LAN or WAN depending on the required configuration.