EdgeConnect for Amazon Web Services (AWS)
Overview

A Silver Peak EdgeConnect Virtual (EC-V) appliance can be deployed in Amazon Web Services (AWS) cloud to establish and enhance the WAN connectivity as well as accelerate the migration of data from branch offices and data centers to AWS.

The Silver Peak EC-V is available as an Amazon Machine Image (AMI), created and launched from the Amazon Marketplace using a Bring Your Own License (BYOL) model.

This guide illustrates a simple, In-Line Router Mode deployment with one WAN interface, one LAN interface, and one management interface.
Deploying EC-V Router Mode

This section describes the deployment’s topology, assumptions and prerequisites, and best practices.

Topology

![Topology Diagram]

Figure 1: Topology of an EC-V deployment with one WAN interface, one LAN interface, and one management interface.

Assumptions and Prerequisites

- Orchestrator is up and running.
- To find out about the recommended AWS instance types, refer to the EdgeConnect Virtual Appliance Host System Requirements document: https://www.silver-peak.com/download/latest/sysrecsysreq_ecv_host.html.
- Since this is a BYOL (Bring Your Own License) AMI, you must have an EdgeConnect license for the EC-V before you can deploy it.
- You have an AWS account.
- You have a Virtual Private Cloud (VPC) with separate subnets for each of these three interfaces: WAN0, LAN0, and MGMT0.

**Note:** In AWS, an EC-V can be deployed with multiple WAN interfaces and LAN interfaces. As shown in Figure 1, this deployment assumes that there is no site-to-site VPN or Direct Connect link between the VPC and the on-premises network. Therefore, the WAN0 and MGMT0 interfaces must have Public IPs that are accessible over the Internet.
To learn more about configuring a VPC, please refer to the AWS documentation: https://aws.amazon.com/documentation/vpc/

Best Practices
An EC-V appliance can be deployed without a management (MGMT0) interface. However, the best practice is to create a separate Elastic Network Interface (ENI) and assign it to the MGMT0 interface.

The MGMT0 interface can be placed on the same subnet as the WAN0 subnet or the LAN0 subnet. Nevertheless, the best practice is to place the MGMT0 interface on a subnet of its own.

Procedure
Deploying an EC-V from the AWS Marketplace takes only a few minutes.

Evaluate the VPC in preparation for the EC-V deployment
In this section, you’ll verify that you have all the necessary AWS components.

1. First, login to your AWS account and select the region in which you want to deploy the EC-V. Under Networking & Content Delivery, click VPC. The VPC Dashboard appears.
2. Under **Virtual Private Cloud**, select **Your VPCs**.

![AWS VPC Dashboard](image1)

The current list of VPCs appears. Currently, only one VPC exists in this region. Take note of its **VPC ID** and **IPv4 CIDR**.

![AWS VPC Details](image2)

3. Click **Subnets**. A list of subnets appears with the corresponding VPC IDs and names.

The SP-Engineering VPC has the three necessary subnets: Management subnet (10.50.0.0/24), Front-end subnet (10.50.1.0/24), and Back-end subnet (10.50.2.0/24). All three subnets reside on the same Availability Zone and soon, we will pair them with MGMT0, WAN0, and LAN0 interfaces, respectively.
4. From the left side menu, click **Route Tables**, and select the route table that is associated with your subnets.

5. Click the **Subnet Associations** tab. Verify that all subnets are associated with the selected route table.
6. Select the Routes tab. Verify that an Internet Gateway is the target for any Internet-bound (0.0.0.0/0) traffic.

![Routes tab with Internet Gateway as target](image)

**Deploy the EC-V**

1. To begin deploying the EC-V, go the menu bar, click Services and select EC2 under Compute. The EC2 Dashboard appears.
2. Click Launch Instance.

![Launch Instance](image)

The page titled, Step 1: Choose an Amazon Machine Image (AMI), appears.

3. Click the AWS Marketplace link, and enter edgeconnect.
The latest version of the Silver Peak Unity EdgeConnect for AWS AMI appears.

**NOTE:** You must have an EdgeConnect license before you can continue deploying the EC-V.

4. Click **Select**. The AMI details appear.

5. Review the details and click **Continue**.

![EdgeConnect for AWS AMI](image)

The **Step 2: Choose an Instance Type** page appears.

When selecting an instance type for the EC-V, consider the vCPU, RAM, network interface, and storage needed to attain the required SD-WAN and BOOST bandwidths. The [EdgeConnect Virtual Appliance Host System Requirements](https://www.silver-peak.com/download/latest/sysreq_ecv_host.html) document specifies the recommended AWS instance types. You can find this document at [https://www.silver-peak.com/download/latest/sysreq_ecv_host.html](https://www.silver-peak.com/download/latest/sysreq_ecv_host.html).

Each AWS instance type has a fixed number of network interfaces that it supports. For instance, a **t2.medium** instance type supports up to three virtual interfaces, while an **m4.xlarge** instance type supports up to four virtual interfaces. The following AWS article specifies the maximum number of network interfaces supported by each instance type: [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html)

In our example, we select the **t2.medium** instance type. It supports 2 vCPUs, 4GB of RAM, and 3 network interfaces. A **t2.medium** instance type is sufficient for an EC-V that supports up to 1 Gbps SD-WAN bandwidth. If your AWS environment requires additional network interfaces on the EC-V, you can easily add them if your selected instance type supports it.

6. Click **Next: Configure Instance Details**.
7. When **Step 3: Configure Instance Details** appears, select the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of instances</td>
<td>1</td>
</tr>
<tr>
<td>Purchasing option</td>
<td>Keep the default setting.</td>
</tr>
<tr>
<td>Network</td>
<td>Select the VPC into which you want to deploy the EC-V.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Select the Management subnet.</td>
</tr>
<tr>
<td>Auto-assign Public IP</td>
<td>Enable (Enable means a dynamic public IP will be assigned to the interface.) If you’ve already established a VPN or Direct Connect link, you can choose Disable.</td>
</tr>
<tr>
<td>IAM role</td>
<td>Select an appropriate IAM role. If no IAM roles are created, select None.</td>
</tr>
<tr>
<td>Shutdown behavior</td>
<td>Stop</td>
</tr>
<tr>
<td>Enable termination protection</td>
<td>Deselect Protect against accidental termination</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Deselect Enable CloudWatch detailed monitoring</td>
</tr>
<tr>
<td>Tenancy</td>
<td>Shared – Run a shared hardware instance</td>
</tr>
</tbody>
</table>
To assign the MGMT0 IP automatically (from the AWS DHCP server), leave **Primary IP** blank. Otherwise, enter a static Private IP for the MGMT0 interface.

8. Scroll down and click **Review and Launch**.

The **Step 7: Review Instance Launch** page appears.

9. Scroll down to Security Groups, and click **Edit security groups**.

The **Step 6: Configure Security Group** page appears.

10. Create a **new** Security Group or select an **existing** Security Group for the MGMT0 interface. (If you choose an existing Security Group, verify that it allows inbound HTTPS and SSH.)
a. In our example, we select **Create a new security group** and change the default security group name to **Sydney-EC-V-MGMT0**.

b. Enter a meaningful description for the security group.

c. Change the application type from HTTP to **HTTPS**.

   For **Source**, select either **Custom** or **My IP**. This ensures that the MGMT0 interface only allows inbound HTTPS traffic from your current location. When selecting **My IP**, AWS auto-populates your current Public IP in the text box.

dl. Similarly, for SSH, select either **Custom** or **My IP**. This ensures that the MGMT0 interface only allows inbound SSH traffic from your current location.

   **Selecting Anywhere is not recommended** to select because it would allow traffic from any network into the MGMT0 interface.

11. Click **Review and Launch**. When the **Step 7: Review Instance Launch** page appears, verify your changes. You have now finished configuring the Security Group.

12. To begin provisioning the VM, click **Launch**.

The **Select an existing key pair or create a new key pair** page appears.
13. Select an existing key pair or create a new key pair, select the checkbox, and click Launch Instances.

The Launch Status page appears.

14. To view the instance launch on the EC2 Dashboard, click the instance ID link.

a. Enter a Name.

b. Wait until Status Checks changes from Initializing to 2/2 checks.

c. If you’re using a site-to-site VPN or a Direct Connect link between the VPC and the on-premises network, then you’ll log in using this Private IP.

d. Otherwise, jot down the Public IP address of the MGMT0 interface.
   In the following steps, you’ll use it to SSH to the VM to create a password for the EC-V.
Create a new password for EC-V

1. Login to the EC-V via SSH.

2. Open PuTTY, and enter the EC-V’s Public IP in the Host Name (or IP Address) field.

3. Navigate to Connection > SSH > Auth and click Browse.

4. Select the appropriate .ppk file.

5. Click Open to initiate the session. The PuTTY Security Alert appears.

6. Click Yes to add the key to the PuTTY’s cache.
7. Login as **admin**.

8. To create a secure password for both admin and monitor users on the EC-V, type:

   ```
   enable [Enter]
   configure terminal [Enter]
   username admin password <enter_a_new_password> [Enter]
   username monitor password <enter_a_new_password> [Enter]
   ```

---

**Configure the EC-V with Appliance Manager**

1. To login to the EC-V’s Appliance Manager WebUI, enter the following into a browser:

   ```
   https://<MGMT0 Public IP address>
   ```

   **NOTE:** If there’s a preconfigured site-to-site VPN or a Direct Connect link established between your current location and the VPC, you should be able to access the MGMT0 interface using its Private IP.
2. To login to the WebUI, enter the following:
   - **User Name:** admin
   - **Password:** `<The_Newly_Created_Password>`

   ![WebUI Login Screen](image)

   The Configuration Wizard opens.

   ![Configuration Wizard](image)

   Click **Next**.

3. In the **Hostname, DHCP, DNS** page, enter the following information:
   - Appliance Hostname
   - Primary DNS IP
4. In the **License & Registration** page, enter the **Account Name** and **Account Key**.

5. In the **Deployment Mode** page, leave the default settings unchanged.

   **NOTE:** Later, after adding the Elastic Network Interfaces (ENI) for WAN0 and LAN0 in AWS, we’ll change the deployment mode from Server to Router.
6. In the **Tunnels to Peers** page, do the following:
   
   a. Select **Use shared subnet information**.
   
   b. Deselect **Automatically establish tunnels**. (This item only displays in versions prior to 8.1.7.)
   
   c. Click **Apply & Next**.

7. In the **Date & Time** page, set the time zone and click **Apply & Next**.
8. The **Change Password** page needs no changes. Since the password was setup earlier, simply click **Apply & Next** to proceed to the next page.

9. When the **Finish** page appears, click **Done** to complete the configuration wizard.
10. Click **Save Changes**.

11. To view the current MAC address assignment, access the **Configuration > Interfaces** page.

Verify that the MAC address, the Private IP, and the Public IP (assigned by Amazon) are properly assigned on the MGMT0 interface.
Add the EC-V to the Orchestrator.

By now, the EC-V has communicated with the Silver Peak Cloud Portal. As a result, it appears on the Silver Peak Orchestrator as a new appliance that is ready to be added to the SD-WAN fabric.

1. Click **Appliance Discovered** to display the table of new devices.

2. Click **Approve** to add the EC-V to your Orchestrator.

The Appliance Wizard appears.

3. Enter the **admin password** that you previously configured and the **Site Name** (an existing region in your AWS account). Then click **Next**.
4. Leave the **Deployment Profile** field unchanged, and click **Next**.

5. On the Add Local Subnets page, do the following:
   
   a. Select **Use shared subnet information**.
   
   b. Deselect **Automatically include local subnets**.
   
   c. Click **Next**.

6. Select the necessary Business Intent Overlays and the Template Groups that need to be applied on the EC-V. If you don’t want to do this task now, you can do it in Orchestrator later.

   Click **Apply**.

7. After the wizard has finished applying the configuration, click **Close**.
You have now successfully added the EC-V into the SD-WAN fabric.

Create Security Groups for the LAN0 and WAN0 interfaces

Before creating LAN0 and WAN0 interfaces on the EC-V, you must create a separate Security Group for each of them. This enables you to assign the Security Groups to the network interfaces as you create them.

1. Navigate to the EC2 Dashboard and click Security Groups under NETWORK & SECURITY.

2. Click Create Security Group

The Create Security Group page appears.

3. First, let’s create a Security Group for the WAN0 interface. Enter a Security group name, Description, and select the VPC where you want the Security Group to reside.
Accept the default settings and click **Create**.
By default, no traffic is allowed inbound. Conversely, by default, all outbound traffic is allowed.

4. Next, follow the same procedure to create a Security Group for the LAN0 interface. Enter a **Security group name**, **Description**, and select the **VPC** where you want the Security Group to reside.

   Unlike the WAN0 interface, the LAN0 interface has no public IP address. The LAN0 interface allows all inbound traffic, enabling the EC-V to receive all traffic from your AWS resources.

5. Select the **Inbound** tab and click **Add Rule**. Under **Source**, select **Anywhere**. Next, click **Create**.
Create LAN0 and WAN0 Elastic Network Interfaces (ENIs)

1. Under NETWORK & SECURITY, click **Network Interface**.

![Network Interface](image)

2. Click **Create Network Interface**.

![Create Network Interface](image)

The Create Network Interface page appears.

3. Enter a **Description**, **Subnet**, **Private IP**, and select the **WAN0 Security Group**. Leave the **Private IP** blank if you want AWS to automatically assign an IP address for the WAN0 interface.

![Create Network Interface](image)

Click **Yes, Create** to create the WAN0 ENI.

4. Next, create the LAN0 ENI. As you did with the WAN0 ENI, enter a **Description**, **Subnet**, **Private IP**, and select the **LAN0 Security Group**. Leave the **Private IP** blank if you want AWS to automatically assign an IP address for the LAN0 interface.
Click **Yes, Create** to create the LAN0 ENI.

Note that the WAN0 and LAN0 ENIs have been added to the list of available interfaces.

Attach the ENIs to the EC-V

1. Under NETWORK & SECURITY, click **Network Interface**.

2. Select the LAN0 ENI, right-click, and click **Attach**.
The **Attach Network Interface** page appears.

3. Under Instance ID, select the EC-V and click **Attach**.

4. Similarly, attach the WAN0 ENI to the EC-V.

   Since all three interfaces (MGMT0, LAN0, and WAN0) are attached to the EC-V now, the **Status** column indicates that the ENI’s are **in-use**.

5. To enable the EC-V to identify the newly added interfaces, you must **reboot** the EC-V after adding the interfaces. To reboot the EC-V, select the **EC-V** on the EC2 Dashboard and right-click to access **Instance State > Reboot**.

6. After the VM reboots, verify the MAC addresses of the newly-attached ENIs.
   a. In the **Description** tab, select the **EC-V** and click **eth1**.
The **Network Interface eth1** page appears. As the Description suggests, **eth1** is the **LAN0** interface of the EC-V.

b. Right-click on the **Interface ID link** and open it in a new tab.

The **Network interface** page appears. Note the **MAC address** in the **Details** tab.
Similarly, click **eth2** and note the MAC address of the **WAN0** interface.

**Assign the LAN0 and WAN0 MAC addresses**

1. In a web browser, open the **EC-V Appliance Manager** and click **Configuration > Interface**.

![EC-V Appliance Manager](image)

The **Interfaces** page appears.

2. In the **MAC** column, assign the correct MAC addresses to the **WAN0** and **LAN0** interfaces, and click **Apply** to save the settings.

![Interfaces Page](image)

3. Click **Save Changes**, but **DO NOT** click **Reboot Required**. Instead, select **Configuration > Deployment**.
Change the Deployment Mode from Server to Router

1. On the Deployment page, select the **Router** mode.

2. To create a LAN0 interface and the WAN0 interface, click **Add** for each.
3. Check the LAN0 IP address from the AWS console.
   a. Under LAN0 IP/Mask textbox, type the private IP address and the subnet mask of the LAN0 interface.
   b. For Next Hop, enter the first IP address of the address prefix. Since our LAN0 subnet mask is 10.50.2.0/24, the first IP address of that range is 10.50.2.1. AWS sets the first IP address of a subnet as the subnet's gateway.

4. Similarly, for WAN0 IP/Mask textbox, type the private IP address and the subnet mask of the WAN0 interface. For Next Hop, enter the first IP address of the address prefix.
   **Important:** If you leave WAN0 IP/Mask blank, the EC-V automatically obtains the WAN0 IP address that AWS assigned on the WAN0 ENI. However, this would also change the management default route metric (Configuration > Routes page) and make WAN0 the preferred interface for management traffic. As shown on the following image, the WAN0 metric becomes lower than that of MGMT0 interface when WAN0 is set to DHCP.

   Instead of enabling DHCP client, when you enter a **static IP** on the WAN0 interface, the management interface becomes the preferred interface for management traffic and receives a lower metric than the WAN0 interface, as shown below.

5. Enter the inbound and outbound **bandwidth** (Kbps) for the WAN0 interface, and click **Calc**.

6. Set WAN0 Firewall to **Stateful**.

7. Enable **NAT**. (We’ll assign a static Public IP for the WAN0 interface in the next step. After it’s assigned, the Orchestrator will use that public IP as the tunnel endpoint when establishing tunnels for the EC-V.)

8. Click **Apply**. You will be prompted to reboot the VM.
9. Click **Apply & reboot**.

Attach an Elastic IP to the WAN0 interface

1. After the reboot, login to the EC2 Dashboard, and click **Elastic IPs** under NETWORK & SECURITY.

   ![Elastic IPs](image)

   An **Elastic IP address** is a public IPv4 address that is reachable from the Internet. It is possible to assign a dynamic public IP address for WAN0 interface of the EC-V; however, the best practice is to assign an Elastic IP. This ensures that the public IP address persists, even after a reboot or a shutdown of the EC-V.

2. Click **Allocate new address**.

   ![Allocate new address](image)

3. Select **VPC** and click **Allocate**.
4. Click Close

5. To associate the elastic IP to the WAN0 ENI, **right-click** on the newly-created Elastic IP and click **Associate address**.

6. When the pop-up opens, enter the following information:

   - **Resource type**: Network interface
Network interface: [Enter the WAN0 interface ID]
Private IP: [optional]
Reassociation: [optional]

7. Click Associate.

The public IP is now attached to the WAN0 interface.

The new public IP appears under WAN0 on the Interfaces page.

To view the public IP WAN0, go to the EC-V Appliance Manager and select **Configuration > Interfaces**.

Enable IP forwarding on the LAN0 interface

1. Click **Instances**, and select the LAN0 interface (eth1, in our example).
2. When the eth1 (LAN0) interface details appear, click the Interface ID.

3. On the resulting page, right-click the row and select Change Source/Dest. Check.
4. Click **Disabled**, and click **Save**.
   
   **NOTE:** It is not necessary to disable **Source/Dest. Check** on the WAN interfaces.

Redirect outbound traffic to EC-V

Next, to forward outbound traffic to the EC-V, add a route on the AWS route table.

1. Click **Services > VPC**.
2. Under Virtual Private Cloud, click Route Tables.

3. When the route table appears, select the Route tab, and click Edit.

4. Click Add another route, and then enter the destination subnet, and the LAN0 ENI ID under Target. As shown in Figure 1, the destination subnet of our example is 192.168.0.0/16.
Click **Save**. Any outbound traffic destined for the **192.168.0.0/16** subnet is now sent to the EC-V. This enables the Silver Peak to perform Application Visibility Control, QoS, WAN Optimization, and other operations on this traffic.

As shown below, the EC-V LAN0 interface (**eni-75c9a279**) is now the target (next-hop) for any traffic that’s destined for the **192.168.0.0/16** network.

5. To verify that outbound traffic directed to the **192.168.0.0/16** network hits the Silver Peak LAN0 interface first, do one of the following:
   - **[Linux]** Run `traceroute -n <an IP address in your remote network>` from a Linux device in your VPC.
   - **[Windows]** Run `tracert -d <an IP address in your remote network>` from a Windows device in your VPC.

   ![Traceroute Command Example]

   Then go to the EC-V Appliance Manager and look for the flow on the **Monitoring – Flows** page. If the flow appears on the Flows page, you have successfully redirected outbound traffic to the EdgeConnect LAN0 interface.

Now that the outbound traffic redirection is set up correctly in VPC, you may create the necessary Business Internet Overlays (BIO) and other traffic policies in the Silver Peak Orchestrator.
For more information about creating BIOS, click here: https://www.silver-peak.com/sites/default/files/UserDocuments/WAN-OP-HTML/content/building_an_overlay.htm?TocPath=Configuration%7CBusiness%20Intent%20Overlays%20(BIO)%7C2

For a general overview of BIOS, click here: https://www.silver-peak.com/sites/default/files/UserDocuments/WAN-OP-HTML/content/business_intent_overlays_bio.htm

Backing Up Appliance Configuration Files


Restoring a Backup to an Appliance

Please refer to the section "Restoring a Backup to an Appliance" on the Silver Peak Orchestrator Operator’s Guide to learn how to restore a backup to your EdgeConnect device. Link to the Unity Orchestrator Operator’s Guide: https://www.silver-peak.com/sites/default/files/userdocs/orchestrator_operators_guide.pdf

Support

Click the following link to learn about Silver Peak support programs: https://www.silver-peak.com/support

Click here to log into your Silver Peak Support Portal: https://www.silver-peak.com/support/customer-login