Deploying EdgeConnect SDWAN-Virtual (EC-V) in Amazon Web Service (AWS) Cloud

Deployment and Integration with AWS
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 A, March 2023
Click any Green icon in the following figure to take you to the relevant section of this guide.

NOTE: Because several sections in this guide are used by multiple use cases, there are specific instructions and hyperlinks provided after each section, which guide you to the next relevant section for the use case that you are configuring. Do not assume, after completing an instruction set, that the next process to be configured is on the next page in the guide.
Overview

Aruba EdgeConnect can be deployed as a hardware appliance or as a virtual appliance in a hypervisor or in the public cloud using a cloud service provider, such as AWS, Azure, etc. Virtual appliances offer the same benefits as hardware appliances. Figure 1 shows various deployment models that are supported by Aruba EdgeConnect in combination with public cloud providers.

In an on-prem deployment model, Aruba EdgeConnect can be used as a VPN gateway to extend connectivity to the public cloud. When EdgeConnect is deployed in the cloud, it extends the SDWAN fabric to the cloud and provides an end-to-end SDWAN fabric experience, and it offers the full benefits of SDWAN in the cloud. Finally, EdgeConnect can be deployed in a multi-cloud environment with service providers offering network as a service (NaaS).

This document focuses on deploying an Aruba EdgeConnect-Virtual (EC-V) appliance 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.

This guide provides configuration steps required to achieve Single EC-V and high availability (HA) EC-V deployment in an AWS Virtual Private Cloud (VPC) and redirect traffic to it using either static routes or Border Gateway Protocol (BGP).

There are two main ways to deploy EC-V in AWS. Users can deploy one or more EC-Vs into a VPC directly from Aruba Orchestrator (Managed Deployment), or they can be deployed from the AWS Management Console (Unmanaged Deployment).

NOTE: Deploying EC-V through Aruba Orchestrator is the recommended and most common method of deploying EC-V in AWS. It deploys EC-V as per AWS best practices and reduces the number of manual tasks on the AWS Console. Deploying EC-V from Orchestrator is also supported for Azure and Google Cloud EC-V deployments.
1 Deploying EC-V through Orchestrator (Managed Deployment)

This section of the document describes how to deploy a single EC-V or HA EC-Vs through Orchestrator with few clicks and minimal configuration on the AWS side.

1.1 AWS Account Configuration

Before configuring anything in Orchestrator, make sure that you have all the AWS credentials and account details that are required to deploy EC-V through Orchestrator. Complete the following steps (1.1.1 and 1.1.2) to create an AWS Identity and Access Management (IAM) user account with the required permissions for creating EC-V instances in AWS and add it to Orchestrator (1.1.3).

1.1.1 Create a Policy with Required Permissions

On the AWS Management Console, create a new AWS Access Management policy with all the required permissions that you will attach later to an IAM user account.

**NOTE:** You can access the following instructions in Orchestrator by going to Configuration > IaaS > Cloud Hubs in AWS and clicking the help icon.

1. Log in to the AWS Dashboard.
2. On the Find Services search menu, enter IAM to open the Identity and Access Management (IAM) page.
4. Click Create policy and click the JSON tab. Delete the existing text, as shown in the following figure.
5. Go to this [web page](#), click the link for your version of Orchestrator, and then copy and paste the JSON policy text into the editor.

6. Click **Next: Tags** to proceed to the next page.

7. (Optional) add metadata to the policy by attaching tags as key-value pairs.

8. Click **Next: Review**.

9. On the Review policy page, enter a name and optional description for the new policy.

10. Review the policy summary to see the permissions granted by your policy, and then click **Create policy** to save your work.
1.1.2 Add Orchestrator IAM User Account and Attach Policy

1. Click **Users > Add user**. The Add user page opens.
2. Enter a username in the User name field (for example, ArubaOrchestrator).
3. Under Access type, select **Programmatic access**, and clear the AWS Management Console access check box.
4. Click **Next: Permissions**.
5. Under Set Permissions, click **Attach existing policies**.
6. Select the Policy that you created in previous steps from the list, and then click **Next: Tags**.
7. Click **Next: Review**.
8. Under Permissions summary, review and make sure the correct policy is attached. Click **Create user**.

Add user

<table>
<thead>
<tr>
<th>User name</th>
<th>Aruba-Orchestrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS access type</td>
<td>Programmatic access - with an access key</td>
</tr>
<tr>
<td>Permissions boundary</td>
<td>Permissions boundary is not set</td>
</tr>
</tbody>
</table>

Permissions summary

The following policies will be attached to the user shown above.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed policy</td>
<td>ArubaOrchestrator-Policy</td>
</tr>
</tbody>
</table>

Tags

No tags were added.

9. After you successfully create the user, download or copy and paste the Access key ID and Secret access key to a secure place for later use in Orchestrator.

**IMPORTANT:** The only time you can copy or download the Secret access key is right after the user is created. You cannot access the key again unless you create a new key.
1.1.3 Add AWS Account in Orchestrator

1. Log in to Orchestrator and navigate to Configuration > Cloud Services > Cloud Hubs in AWS.
2. Click AWS Accounts.
3. Click Add AWS Account and enter a name, Access key ID, and Secret access key, which was collected in the previous step. Click Save.

This completes the account creation in AWS and adding it to Orchestrator.

NEXT: Deploy EC-V through Orchestrator

- To deploy a Single EC-V through Orchestrator, proceed to Section 1.2
- To deploy HA EC-V through Orchestrator, proceed to Section 1.3
1.2 Deploying a Single EC-V

1.2.1 Prerequisites

- Access to Orchestrator with the required licenses to deploy EC-V.
- Access to the AWS Management Console.
- New IAM user account (in AWS) with required permission for Orchestrator to deploy resources. Refer to Section 1.1 to create a new user account with required permissions.
- Identify the AWS region on which the EC-V will be deployed (e.g., us-east-2).
- EC-V cannot be deployed on an existing VPC. For each new deployment, Orchestrator prompts the user to enter a Classless Inter-Domain Routing (CIDR) block that it will use for deploying one or many EC-Vs into a VPC.

**NOTE:** A single deployment can contain one or more EC-Vs. The smallest VPC CIDR block supported by the Orchestrator is /24 and the largest is /16. Identify a CIDR block, such as 192.168.1.0/24, for your deployment.

- Key pair. Refer to Section 2.1.3h to create a new key pair.

1.2.2 Topology

The following example (Figure 2), shows how to deploy an EC-V on a new VPC CIDR \textbf{172.20.32.0/22} in US-East-2 region. Orchestrator automatically creates this VPC using the configured CIDR block.

![Diagram of Single EC-V Deployment](image-url)
1.2.3 Single EC-V Deployment Procedure

Follow these steps to complete the deployment of a single EC-V:

1. Log in to Orchestrator and navigate to Configuration > Cloud Services > Cloud Hubs in AWS.
2. Add an AWS account. Refer to Section 1.1 to create an IAM user account and add an AWS account to Orchestrator. Skip this step if you already have the AWS account added to Orchestrator.
3. Click New Deployment.
4. AWS Deployment Configuration page opens

This is the only differentiator for Single EC-V vs HA EC-V deployment.
5. Fill in the details on the AWS Deployment Configuration page:

a. **Name**: Enter a name for the deployment. This name is used only for identifying the deployment. A deployment consists of one or more EC-Vs that an Orchestrator creates in an AWS VPC. Only alphanumerical letters and hyphens are allowed in the deployment name. The maximum allowed length is 20 characters.

b. **AWS account**: Select an AWS account for deploying the EC-V.

c. **Region**: Select an AWS region in which this EC-V instance will be deployed.

d. **VPC CIDR**: Enter a VPC CIDR block. The smallest supported CIDR block is /24 and the largest supported CIDR block is /16. Orchestrator creates all AWS resources required for the EC-V deployment within this VPC. For each EC-V you deploy, Orchestrator creates three subnets that are /28 in size. In other words, if you deploy two EC-Vs, Orchestrator creates six subnets in total. This is true even if both EC-Vs are created in a single Availability Zone.

e. **SSH key**: Enter the SSH key pair you created in the previous section.

f. **Boost**: Enable Boost if needed. To enable Boost, you must have a valid Boost license in your account. Boost requires additional resources on the AWS EC2 instance. After Boost is selected and an appropriate WAN Bandwidth value is selected, Orchestrator displays the appropriate AWS instance types for the deployment on the Instance Type drop-down menu.

**NOTE**: Selecting the Boost check box does not enable Boost on the EC-V. It only allows Orchestrator to display appropriate AWS instance types that can support Boost for the selected WAN bandwidth tier. To enable Boost on the EC-V, go to the Deployment page and the Business Intent Overlay (BIO) page after the deployment is complete.

g. **WAN bandwidth**: Select WAN Bandwidth. After you select a WAN Bandwidth value, Orchestrator displays the appropriate AWS instance types for the deployment on the Instance Type drop-down menu.

h. **Instance type**: Select the instance type. Based on your selection of Boost and WAN Bandwidth values, Orchestrator displays the appropriate AWS instance types on this drop-down menu.

i. **AWS tags (Optional)**: Any comma-separated tags entered here are applied to all AWS resources that Orchestrator creates while deploying the EC-V. If you do not enter any tags, Orchestrator automatically creates a unique tag for each AWS resource that it creates while deploying the EC-V. This AWS tag is created to identify each resource created by Orchestrator. The tag is formatted as follows: sp-automated-deployment name-instance-index-resource name.

j. **Comment (Optional)**: Enter an optional comment if you want to attach any additional details for the deployment.

k. **Advanced Settings**: Custom AMI ID: If you want to deploy the EC-V with a specific public or private image, provide the AMI ID. You can obtain the AMI ID from the AWS console. Leave this field blank to allow Orchestrator to deploy the EC-V with the base AMI obtained from the AWS Marketplace.

l. **Select Number of instances**: You can deploy multiple EC-Vs by clicking + and selecting the Availability Zone for each EC-V. If the selected region supports multiple Availability Zones, each Availability Zone is shown on the drop-down menu. When deploying multiple EC-Vs, it is a best practice to deploy each EC-V in a unique Availability Zone.

m. **Appliance Tag (Optional)**: Enter an Appliance Tag on this field if you want to assign a pre-configuration file to the deployment. If this field is left blank, Orchestrator will automatically assign an Appliance Tag for its own configuration purposes.
6. Click **Review and Deploy** to complete the deployment. After a few minutes, the Cloud Hubs in AWS page should display status as “Deployed”.

7. Click the info icon on the Cloud Hubs in AWS page to view the instance details, such as IP addresses assigned to WAN0, MGMT0, and LAN0 interfaces, and their MAC addresses.

This completes the Managed Deployment of a single EC-V from the Aruba Orchestrator.

**NEXT: Provision EC-V on Aruba Orchestrator**
- Provision the newly deployed EC-V and add it to the SD-WAN fabric, refer to section 3.2
1.3 Deploying HA EC-Vs

When deploying a pair of EC-Vs in AWS for HA purpose, Aruba recommends that EC-Vs be deployed on a Transit VPC (also known as Edge VPC). Transit VPC is an alternate name for a VPC dedicated for deploying network virtual appliances such as SD-WAN instances.

Deploying EC-Vs in an HA configuration on a cloud platform is different to an On-Prem EdgeConnect HA deployment. Cloud environments do not allow Layer 2 access to users. Currently, achieving EC-V HA in AWS is only possible by establishing BGP sessions from each EC-V with an AWS-native service that supports BGP such as the AWS Virtual Private Gateway (VGW) or AWS Transit Gateway (TGW).

In Section 5 and Section 6 of this document, has configuration steps required to establish BGP with the AWS Transit Gateway to set up EC-V in HA configuration.

NOTE: This deployment guide does not cover how to establish BGP with the AWS VPN Gateway (Virtual Private Network Gateway).

1.3.1 Prerequisites

- Access to Orchestrator with the required licenses to deploy EC-Vs.
- Access to the AWS Management Console.
- New IAM user account (on AWS) with required permission for Orchestrator to deploy resources. Refer to Section 1.1 to create a new user account with required permission.
- Determine the region where the EC-V will be hosted.
- EC-V cannot be deployed on an existing VPC. For each new deployment, Orchestrator prompts the user to enter a Classless Inter-Domain Routing (CIDR) block that it will use for deploying one or many EC-Vs into a VPC.
  NOTE: A single deployment can contain one or more EC-Vs. The smallest VPC CIDR block supported by the Orchestrator is /24 and the largest is /16. Identify a CIDR block, such as 192.168.1.0/24, for your deployment.
- Key pair. Refer to Section 2.1.3h to create a new key pair.
1.3.2 Topology

The following example (Figure 3), shows how to deploy a pair EC-Vs on a new VPC CIDR `172.20.36.0/22` in US-East-2 region. Orchestrator automatically creates this VPC using the configured CIDR block.

![HA EC-V Deployment Diagram](image-url)
1.3.3 HA EC-V Deployment Procedure

Follow these steps to deploy the HA EC-V:

1. Log in to Orchestrator and navigate to **Configuration > Cloud Services > Cloud Hubs in AWS**.
2. Add an AWS account. Refer to **Section 1.1** to create an IAM user account and add an AWS account to Orchestrator. Skip this step if you already have the AWS account added to Orchestrator.
3. Click **New Deployment**.

4. **AWS Deployment Configuration** page opens.
5. Fill in the details on the **AWS Deployment Configuration** page:

   a. **Name**: Enter a name for the deployment. This name is used only for identifying the deployment. A deployment consists of one or more EC-Vs that an Orchestrator creates in an AWS VPC. Only alphanumerical letters and hyphens are allowed in the deployment name. The maximum allowed length is 20 characters.

   b. **AWS account**: Select an AWS account to use for deploying the EC-V.

   c. **Region**: Select the region in which this EC-V instance will be deployed.

   d. **VPC CIDR**: Enter a VPC CIDR block. The smallest supported CIDR block is /24 and the largest supported CIDR block is /16. Orchestrator creates all AWS resources required for the EC-V deployment within this VPC. For each EC-V you deploy, Orchestrator creates three subnets that are /28 in size. In other words, if you deploy two EC-Vs, Orchestrator creates six subnets in total. This is true even if both EC-Vs are created in a single Availability Zone.

   e. **SSH key**: Enter the SSH key pair you created for the EC-V in the previous section.

   f. **Boost**: Enable Boost if needed. To enable Boost, you must already have a valid Boost license in your account. Boost requires additional resources on the AWS EC2 instance. After Boost is selected and an appropriate WAN Bandwidth value is selected, Orchestrator displays the appropriate AWS instance types for the deployment on the Instance Type drop-down menu.

   **NOTE:** Selecting the Boost check box does not enable Boost on the EC-V. It only allows Orchestrator to display appropriate AWS instance types that can support Boost for the selected WAN bandwidth tier. To enable Boost on the EC-V, go to the Deployment page and the Business Intent Overlay (BIO) page after the deployment is complete.

   g. **WAN bandwidth**: Select a WAN Bandwidth value. After you select a WAN Bandwidth value, Orchestrator displays the appropriate AWS instance types for the deployment on the Instance Type drop-down menu.

   h. **Instance type**: Select the AWS instance type. Based on your selection of Boost and WAN Bandwidth values, Orchestrator displays the appropriate AWS instance types on this drop-down menu.

   i. **AWS Tags (Optional)**: Any comma-separated tags entered here are applied to all AWS resources that Orchestrator creates while deploying the EC-V. If you do not enter any tags, Orchestrator automatically creates a unique tag for each AWS resource created by Orchestrator. The tag is formatted as follows: sp-automated-deployment name-instance-index-resource name.

   j. **Comment (Optional)**: Enter an optional comment if you want to attach any additional details for the deployment.

   k. **Advanced Settings**: Custom AMI ID: If you want to deploy the EC-V with a specific public or private image, provide the AMI ID. You can obtain the AMI ID from the AWS console. Leave this field blank to allow Orchestrator to deploy the EC-V with the base AMI obtained from the AWS Marketplace.

   l. **Select Number of instances**: You can deploy multiple EC-Vs by clicking + and selecting the Availability Zone for each EC-V. If the selected region supports multiple Availability Zones, each Availability Zone is shown on the drop-down menu. When deploying multiple EC-Vs, it is a best practice to deploy each EC-V in a unique Availability Zone.

   m. **Appliance Tag (Optional)**: Enter an Appliance Tag on this field if you want to assign a pre-configuration file to the deployment. If this field is left blank, Orchestrator will automatically assign an Appliance Tag for its own configuration purposes.
6. Click **Review and Deploy** to complete the deployment. After a few minutes, the Cloud Hubs in AWS page should display status as “Deployed”.

```
6. Click Review and Deploy to complete the deployment. After a few minutes, the Cloud Hubs in AWS page should display status as “Deployed”.
```

7. Click the info icon on the Cloud Hubs in AWS page to view the instance details such as IP addresses assigned to WAN0, MGMT0, and LAN0 interfaces, and their MAC addresses.

```
7. Click the info icon on the Cloud Hubs in AWS page to view the instance details such as IP addresses assigned to WAN0, MGMT0, and LAN0 interfaces, and their MAC addresses.
```

This completes the Managed Deployment of HA EC-Vs from Orchestrator.

**NEXT: Provision EC-Vs on Aruba Orchestrator**
- Provision the newly deployed EC-Vs and add them to the SD-WAN fabric, refer to **Section 3.2**
2 Deploying EC-V through AWS Console (Unmanaged Deployment)

Deploying an EC-V in AWS cloud from the AWS Management Console will be detailed in this section. The deployment procedure is similar for both Single EC-V and HA EC-V, however, when deploying HA EC-V you must place each EC-V into a unique AWS Availability Zone for redundancy purposes.

2.1 Single EC-V Deployment through AWS Management Console

The following configuration steps guide you to deploy a single EC-V instance through the AWS Management Console. Section 2.1.3 contains information for preparing AWS resources that are required to deploy an EC-V instance, such as VPC, subnets, security groups, Internet Gateway, network interfaces and Elastic IP (EIP) address, and key pair. Section 2.1.4 contains the procedure for deploying the EC-V.

2.1.1 Prerequisites

- Operational Orchestrator and EdgeConnect licenses for the EC-Vs.
- Determine the type of EC2 instance needed based on the WAN bandwidth requirements. For more information on the recommended AWS instance types, refer to the Aruba EdgeConnect Virtual Appliance Host System Requirements.
- An AWS account and credentials to use the AWS Management Console.
- A virtual private cloud (VPC) in AWS with separate subnets for the WAN0, LAN0, and MGMT0 interfaces.
- Aruba recommends that you deploy the EC-V only in Router Mode.
2.1.2 Topology

In the following example (Figure 4), you will deploy an EC-V on a new VPC **172.20.32.0/22** in US-East-2 region.

![Figure 4: Single EC-V Deployment](image)
2.1.3 Create AWS Resources Prior to Deploying the EC-V Instance

This section describes all AWS resources that you must create prior to deploying an EC-V. It is important that you create these resources prior to launching the EC-V.

2.1.3.a Create New VPC

1. Log in to the AWS Management Console for your account and select the Region (e.g., Ohio) in which the EC-V will be deployed.

2. Navigate to Services > Networking & Content Delivery > VPC > Your VPCs or use the search bar to search for “VPC.”

3. Click Create VPC and complete the VPC settings:

4. The following VPCs are used in this deployment example:

<table>
<thead>
<tr>
<th>Name</th>
<th>VPC ID</th>
<th>State</th>
<th>IPv4 CIDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>RKAWS-E2-VPC1</td>
<td>vpc-0a025fa5e5148ba3</td>
<td>Available</td>
<td>172.20.32.0/22</td>
</tr>
<tr>
<td>RKAWS-E2-VPC2</td>
<td>vpc-016dc264163fe5cb7</td>
<td>Available</td>
<td>172.20.36.0/22</td>
</tr>
</tbody>
</table>

We will be using this VPC with CIDR 172.20.32.0/22 in this example.
2.1.3.b Create Subnets

1. Each EC-V instance requires three subnets, one for each interface (LAN0, MGMT0, and WAN0).

   **IMPORTANT**: Do not place multiple interfaces into one subnet!

2. Navigate to **VPC > Virtual private cloud > Subnets** or use the search bar to search for “Subnets” and select **Subnets** from the search results.

3. Click **Create subnet** to create 3 new subnets (LAN0, WAN0, and MGMT0).

   Enter the Subnet settings, such as VPC, Subnet name, Subnet block, and Availability Zone.

4. Enter the Subnet settings for each subnet that is required for LAN/WAN/MGMT interface mapping. The following figure lists subnets that are used in this deployment example:

   It helps to name each subnet with its interface details, which will be useful when creating and attaching it to the interfaces.

If HA EC-Vs are being deployed, make sure that you map them to two different Availability Zones for redundancy purposes. Example:

- EC-V1-WAN0-Subnet – us-east-2a
- EC-V2-WAN0-Subnet – us-east-2c
2.1.3.c Create an Internet Gateway

In this step, you are creating an Internet Gateway (IGW) and attaching it to the VPC that you created earlier, and then updating the route table for the IGW. This is required for the EC-V appliance to reach the Aruba Cloud Portal over the internet, as well as to establish SD-WAN tunnels to remote EdgeConnect appliances.

1. Navigate to **VPC > Virtual Private Cloud** and click **Internet gateways**. The following figure shows that the IGW is attached to the VPC that was created earlier.
   ![Internet Gateway Attached](image)

2. If your VPC is not attached to the Internet Gateway, click **Create internet gateway** and attach it to the VPC.
   ![Create Internet Gateway](image)

3. Ensure that the route table that is attached to the subnets has a default route added that points to the Internet Gateway.
   To locate the route table, navigate to **VPC > Subnets > Select the Route Table attached to WAN subnet**.
   ![Route Table](image)

4. Click **Edit Routes** to add a new route.
   ![Edit Routes](image)

5. Add a 0.0.0.0/0 route pointing to IGW. Click **Save changes** to complete the route table changes.
2.1.3.d Create Security Groups

Aruba recommends using a unique security group for LAN, WAN, and MGMT interfaces. This gives flexibility to configure allow/deny policies based on the requirements of a given interface.

Adding the suffixes "-mgmt0SecurityGroup", "-wan0SecurityGroup", and "-lan0SecurityGroup" when naming the security groups is useful because when the EC-V boots for the first time, it will be able to identify and map MAC addresses to interfaces automatically using those suffixes. This eliminates manually mapping MAC addresses to interfaces.

1. Navigate to VPC > Security > Security groups or use the search bar to search for “Security Groups” and select Security Groups from the search results.

2. If needed, click Create security group to create new policies. Complete the details for each policy.

3. Add Inbound and Outbound rules like the rules shown in the following figure for LAN Security Group.

![Create security group](image)

This policy is for the LAN interface to allow communication between the SD-WAN network and VPC networks. For simplicity, the whole Class B range is added for this deployment example. It is a common practice to allow inbound traffic on all RFC1918 addresses on the LAN0 Security Group.
4. Add Inbound rules for other MGMT Security Group like those shown in the following figure.

```
<table>
<thead>
<tr>
<th>Inbound rules (4)</th>
<th>RKAWS-mgmt0SecurityGroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group rule ID</td>
<td>IPv4</td>
</tr>
<tr>
<td>Type</td>
<td>HTTPS/TCP</td>
</tr>
<tr>
<td>Protocol</td>
<td>x.x.x.x/32</td>
</tr>
<tr>
<td>Source</td>
<td>(Temp Rule to allow inbound HTTPS)</td>
</tr>
<tr>
<td>Description</td>
<td>Temp Rule to allow inbound SSH)</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
```

The first two lines indicate a custom rule that allows inbound https/ssh traffic for the local IP from where the EC-V will be accessed for initial configuration. E.g., Add the public IP address of your PC (or local router/modem).

```
<table>
<thead>
<tr>
<th>RKAWS-mgmt0SecurityGroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group rule ID</td>
</tr>
<tr>
<td>Security group rule ID</td>
</tr>
<tr>
<td>Source</td>
</tr>
</tbody>
</table>
```

5. Add an Inbound rule for other WAN Security Group like the rule shown in the following figure.

```
<table>
<thead>
<tr>
<th>Inbound rules (1/1)</th>
<th>RKAWS-wan0SecurityGroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group rule ID</td>
<td>IPv4</td>
</tr>
<tr>
<td>Source</td>
<td>All</td>
</tr>
</tbody>
</table>
```

6. Also make sure you ALLOW ALL Outbound traffic (default configured) on each of the security groups. This is needed for bidirectional communication.

```
<table>
<thead>
<tr>
<th>Outbound rules (1/1)</th>
<th>　　　　　　　　　　　　</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group rule ID</td>
<td>IPv4</td>
</tr>
<tr>
<td>Source</td>
<td>All</td>
</tr>
</tbody>
</table>
```
2.1.3.e Create Network Interfaces

The number of interfaces supported on a given EC-V depends on the type of instance selected. Refer to the Aruba EdgeConnect Virtual Cloud Host System Requirements to find the number of interfaces supported on each instance type. In AWS, an EC-V can be deployed with multiple WAN and LAN interfaces.

An EC-V appliance can be deployed without a management (MGMT0) interface if needed. However, it is recommended to create a separate elastic network interface (ENI) and assign it to the MGMT0 interface.

1. To create an elastic network interface (ENI), navigate to EC2 Dashboard > Network & Security > Network Interfaces and open the ENI page, or use the search bar to search for “Network Interfaces” and select Network Interfaces from the search results.

2. Click Create network interface to create a new interface and fill in the details. From the Security groups section, select the security group that was created in Step 2.1.3d.

3. Repeat steps 1 through 2 for LAN0 and MGMT0 interfaces. In total, you should create three network interfaces with corresponding subnet mapping and security group mapping.
4. The following figure shows interfaces that are used in this example deployment:

![Network Interfaces Table]

2.1.3.f Elastic IP Address Mapping

When an EC-V appliance boots for the first time, it needs to establish connectivity with Aruba Cloud Portal, so an elastic IP address is required on MGMT0 interface. Another elastic IP address is needed on the WAN0 interface as it needs to establish SD-WAN tunnels over the internet with remote EdgeConnect appliances.

For LAN0 interface: If you plan to integrate EC-V with AWS Transit Gateway using BGP over IPsec then you also need to create an Elastic IP address and attach it to the LAN0 interface. If you plan to integrate EC-V with AWS Transit Gateway using BGP over GRE, an Elastic IP address is not required on the LAN0 interface.

1. Navigate to VPC > Elastic IP Addresses or use the search bar to search for “Elastic IP” and select Elastic IP addresses from the search results.
2. To create a new Elastic IP address, click Allocate Elastic IP address then click Allocate.
3. Associate the Elastic IP address to the network interface. In this example WAN0 interface is attached with this Elastic IP address.
4. Repeat steps 2 and 3 to create an Elastic IP and associate it to the MGMT0 interface.

The private IP address automatically pops up when the cursor is placed in this field. In this case it’s the WAN0 interface private IP address.

Make sure to select the correct interface that was created in Step 2.2.1e by using the interface name or the interface ID.
2.1.3.g Gathering Interface Details

Record the interface IP address, MAC address, subnet, and Elastic IP address for the WAN0, MGMT0, and LAN interfaces that you have created so far. You will need these details when provisioning the EC-V from Orchestrator.

1. To locate the network interfaces, navigate to EC2 > Network & Security > Network Interfaces or use the search bar to search for “Network Interfaces” and select Network Interfaces. Then look for the LAN0, WAN0 and MGMT0 interfaces created in Step 2.1.3e.

2. The following figure shows an example of the interface details for the WAN0 interface:

3. Repeat steps 1 through 2 for each interface and document the details. The following table is an example of the details that you need to gather. This information is required when provisioning the EC-V.

Table 1: Example – Summary of Network Interface Details

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>Interface IP</th>
<th>SUBNET</th>
<th>Next Hop</th>
<th>Mac Address</th>
<th>Elastic IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT0</td>
<td>172.20.32.9</td>
<td>172.20.32.0/28</td>
<td>172.20.32.1</td>
<td>02:91:88:E9:8A:B8</td>
<td>3.137.112.152</td>
</tr>
<tr>
<td>WAN0</td>
<td>172.20.32.25</td>
<td>172.20.32.16/28</td>
<td>172.20.32.17</td>
<td>02:BC:AF:8B:61:A4</td>
<td>3.128.241.141</td>
</tr>
<tr>
<td>LAN0</td>
<td>172.20.32.36</td>
<td>172.20.32.32/28</td>
<td>172.20.32.33</td>
<td>02:A2:5D:D2:70:A8</td>
<td>NA</td>
</tr>
</tbody>
</table>
2.1.3.h Creating a Key Pair

To deploy an EC2 instance on AWS Cloud, you need a key pair. Use an existing key pair if you have already created one or create a new one.

1. To create a new key pair, navigate to EC2 > Network & Security > Key Pairs.

2. Click **Create key pair** and complete the steps to create a key pair.

3. Provide a name for the key pair and leave the .pem or .ppk for the file format. Click **Create key pair** to complete the generation of a new key pair.

4. The .pem/.ppk file is saved to your desktop.

**NOTE:** Save the .pem/.ppk file to your computer. You will need it to SSH into the EC-V appliance to perform the initial configuration.

This completes all the tasks for creating resources on the AWS Management Console.

**NEXT:** Launch EC-V from AWS Management Console

- Proceed to **Section 2.1.4** to launch the EdgeConnect EC-V from the AWS Management Console.
2.1.4 Launching a Single EC-V Instance From the AWS Management Console

Deploy a single EC-V instance through the AWS Management Console using the resources created in Section 2.1.3.

1. Log in to the AWS Management console and open the EC2 dashboard (Navigate to Services > Compute > EC2).
2. Click Launch instance from the EC2 dashboard.
4. Select Silver Peak Unity EdgeConnect for AWS and click Continue.
5. Enter a name for the EC-V instance under the Name and tags section.

Name and tags

Name: RKAWS-EC01

Add additional tags

Application and OS images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don’t see what you are looking for below.

- AMI from catalog
- Recents
- My AMIs
- Quick Start

AWS Marketplace AMIs

Catalog: 2021-12-20
Architecture: x86_64
Root device type: ebs

If you have an existing license entitlement to use this software, you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement.

6. Depending on the WAN bandwidth requirements, select an appropriate EC2 instance type. For more information on the recommended instance types, refer to EdgeConnect Virtual System Requirements.

7. Select the key pair that was created in Step 2.1.3h or use an existing key pair.
8. Edit Network settings to map the VPC and interfaces.

9. Modify the VPC and subnet to match the ones created in earlier steps. The following example uses the VPC created in Step 2.1.3a and the subnet created in Step 2.1.3b. Click Add network interface to progress through the steps.

![Network settings](image)

- VPC: Select the VPC from the drop-down list.
- Subnet: Map the corresponding subnet that was created in step 2.2.1b. Because MGMT0 has an Elastic IP attached, it is preferable to add the MGMT in this first step.
- Firewall: Select the existing security group, BUT do not map any security groups. Because the interfaces are already mapped, you do not have to assign a security group in this step.

Click Advanced network configuration to add the three interfaces (MGMT, WAN and LAN).

10. Map the MGMT interface and click Add network interface twice to map the LAN and WAN interfaces.

![Advanced network configuration](image)

11. Map the LAN and WAN interfaces.
12. Leave the rest of the settings as is. Check the Summary section to ensure that only a single instance is being deployed and that the required instance type is being used. Then, click **Launch instance**.

You should see the following screen that indicates the launched instance was successful.

13. After few minutes, navigate to **EC2 > Instances** and search for the name of the EC-V or the instance id. You should see the new EC-V instance up and running.

This completes the Unmanaged Deployment of a Single EC-V from the AWS Management Console.

**NEXT: Provision EC-V on Aruba Orchestrator**
- Provision the newly deployed EC-V and add it to the SD-WAN fabric, proceed to **Section 3**.
2.2 HA EC-V Deployment through AWS Management Console

When deploying a pair of EC-Vs in a single virtual private cloud (VPC) for High Availability purpose, Aruba recommends that the EC-Vs be deployed on a Transit VPC (also known as Edge VPC). High Availability on EC-Vs deployed on cloud is not achieved in the same way that it is achieved for an on-prem EdgeConnect device. Because these EC-Vs are deployed on cloud, there is no Layer 2 redundancy possible. Currently, achieving EC-V HA in AWS is only possible by establishing BGP sessions from each EC-V with an AWS-native service that supports BGP, such as the AWS Transit Gateway (TGW).

Deploying an HA EC-V through the AWS Management console is almost identical to deploying a Single EC-V except that you must ensure that you deploy each EC-V into a unique Availability Zone. When creating the subnets required for each EC-V, make sure that you create them in appropriate Availability Zones on which you are planning to deploy the EC-Vs. Subnets created for each EC-V must be in different Availability Zones. For example, LAN0/MGMT0/WAN0 subnets for EC-V1 would be on availability zone us-east-2a. But for EC-V2, the availability zone for those subnets would be us-east-2c.

2.2.1 Topology

In the following example (Figure 5), you will deploy a pair EC-Vs on a new VPC 172.20.36.0/22 in US-East-2 region.
2.2.2 Prerequisites

- An operational Orchestrator and EdgeConnect license for the EC-V before it can be deployed in AWS Cloud.
- Determine the type of EC2 instance needed based on the WAN bandwidth requirements. For more information on the recommended AWS instance types, refer to the Aruba EdgeConnect Virtual Cloud Host System Requirements.
- An AWS account and credentials to use AWS Management console.
- A virtual private cloud (VPC) in AWS with separate subnets for the WAN0, LAN0, and MGMT0 interfaces.
- Aruba recommends that the EC-V be deployed only in Router Mode.

2.2.3 HA-ECV Deployment procedure

To deploy HA-ECVs, complete the following steps:

1. Deploy the first EC-V by following the instructions in Section 2.1.3 and Section 2.1.4.
2. When creating subnets (Section 2.1.3b) for the second EC-V, ensure that you map the subnets of the second EC-V to a different zone than the one mapped on the first EC-V. This ensures redundancy on the AWS Cloud.
3. Repeat the instructions in Section 2.1.3 and Section 2.1.4 to deploy the second EC-V instance. You may choose to exclude some instructions, which may duplicate steps. The instructions in the subsections of Section 2.1.3 listed below can be excluded for the second EC-V instance deployment.
   1. Section 2.1.3a – Because both the EC-Vs are going to be on the same VPC, you don’t have to create a new VPC for the second ECV deployment.
   2. Section 2.1.3c – Because the VPC is already attached to an Internet Gateway, this step can be excluded.
   3. Section 2.1.3d – You can use the same security group for the second EC-V interface.
   4. Section 2.1.3h – You can use the same key pair to deploy the second EC-V.
4. Provision each EC-V as described in Section 3.

This completes the Unmanaged Deployment of HA EC-Vs from the AWS Management Console.

NEXT: Provisioning EC-Vs on Aruba Orchestrator

- Provision the newly deployed EC-Vs and add them to the SD-WAN fabric, proceed to Section 3.
3 Provisioning EC-Vs On Aruba Orchestrator

3.1 Prepare EC-V Instance Using the Initial Configuration Wizard

In this section, you prepare the EC-V instance that enables it to reach Orchestrator. You need the account name and account key to license and register the EC-V with Aruba Cloud Portal. You will perform some initial configuration from the EC-V CLI and WebUI before provisioning the EC-V in Orchestrator.

3.1.1 SSH to EC-V Instance from a Local Computer

Using the key pair .pem file that was used to deploy the EC-V, log in to the EC-V appliance CLI from a local computer to configure passwords for admin and to monitor users. By default, there is no password set.

- SSH to your instance using its public IP. *(This is the Elastic IP address of EC-V’s MGMT0 interface.)*
  
  Guide example: 3.22.72.73

- Configure a secure password for admin using the following commands:
  
  ```
  enable
  config t
  username admin password <password>
  ```

The following figure shows an example of how to log in to AWS Cloud EC-V from a MacBook machine using the public IP and key pair:

![Putty Configuration](image)

The following figure shows an example of how to log in to AWS Cloud EC-V from a Windows PC using the public IP and key pair:
In the following step, configure passwords for admin usernames using the commands highlighted in the figure below.

3.1.2 Access the WebUI of EC-V Instance to Configure Provisioning Parameters

1. Using the password created in Step 3.1.1, log in to the WebUI of the EC-V instance, e.g., https://3.22.72.73

   ![WebUI Login]

   ![Configuration Wizard]

2. Navigate to **Configuration tab > Initial Configuration Wizard**, and note that the three interfaces are pre-populated with MAC addresses. Under Registration, enter **Account Name** and **Account Key**, and click **Save**.

   - If you have configured the EC-Vs through AWS Marketplace (Unmanaged Deployment), then notice that the MAC address is pre-populated next to respective interface name. This is only possible when you configure security groups with correct suffix such as “-wan0SecurityGroup”, “-lan0SecurityGroup” and “-mgmt0SecurityGroup”.

   For Deployment through Aruba Orchestrator – this is automatically done.
3.2 Provisioning the EC-V Instance in Orchestrator

1. Log in to Orchestrator. Note the **Appliance Discovered** button that appears.

2. Click **Appliances Discovered**. Click the **Approve** button for the EC-V to continue.

3. When you click **Approve**, the **Upgrade Appliance** screen appears, as shown in the following figure. You can click **Skip** for now and proceed, or perform the upgrade to the required software version. In this example, click **Skip** and proceed.

   ![Upgrade Appliance](image)

   If you click **Upgrade & Reboot Appliance**, you will have to wait for the upgrade process to complete and the EC-V to be rediscovered by Orchestrator before you can proceed.

4. Appliance Wizard appears as shown in the following figure. Enter a name for the appliance in the Appliance field, select a **Group** in which the EC-V will be placed and enter a new **Admin Password**. Note in this example that the **Hub Site** option is enabled because this is being deployed as a Hub in AWS Cloud and you can choose to enable or disable it based on your topology.

   You can fill in other details such as **Location** and **Site Name** if needed.

   **IMPORTANT**: When deploying EC-V HA in AWS, you must enter the same Site Name on both EC-Vs. This will prevent the AWS EC-Vs from establishing SD-WAN tunnels between them.

5. Click **Next** to proceed to the second page of the wizard.
6. Select **Router** on this deployment page to deploy the EC-V in Router Mode. If you deployed the EC-V from Orchestrator, you do NOT need to fill in any of the following details. You need to enter the following details only if you deployed the EC-V from the AWS Management Console.

- Fill in the IP address and **Next Hop** details for the LAN and WAN interfaces.
- Assign **Bandwidth** for inbound and outbound (as needed and based on available license).
- Enable **NAT**, apply an interface label (e.g., **INET1**) and select **Stateful + NAT** FW mode on WAN interfaces.
- Select **License** for EC-V appliance.
- Click **Next** to EC-V appliance.

7. Loopback interface can be added here if needed, in this example skip this and click **Next** to proceed to the fourth page of the wizard.
8. Select the **Automatically advertise local subnets** check box to advertise local LAN subnets to the SD-WAN fabric. Click **Next** to proceed to the final page of the wizard.

9. Apply any Business Intent Overlays and Template Groups if needed, and click **Apply** to complete the provisioning of the EC-V appliance in Orchestrator.

10. A final status on the wizard should appear indicating all the provisioning parameters successfully applied on the EC-V.

This completes the provisioning of EC-Vs to the SDWAN Fabric.

**NEXT: Traffic Redirection**

- To redirect traffic to the EC-V from VPCs using static routes, refer to **Section 4**.
- To redirect traffic to the EC-V from VPCs using BGP over GRE method, refer to **Section 5**.
- To redirect traffic to the EC-V from VPCs using BGP over IPsec method, refer to **Section 6**.
4 Static Route Integration with AWS VPC

The following section describes the steps required to redirect traffic from user workloads deployed in a VPC to AWS EC-V appliance. The static route method of integration is only recommended for single EC-V deployments where the AWS VPC configuration or the on-prem routes do not change often. With every change, you must manually update routes both on the VPC route table as well as the route table for the AWS EC-V. If you have multiple EC-Vs (HA) deployed in AWS cloud, static route integration is not recommended as static routes do not get updated when the primary EC-V fails.

4.1 Topology

In the following topology (Figure 6), a single EC-V is deployed in a VPC with an Ubuntu Linux instance as a workload on the same VPC.

![Figure 6: Single EC-V Deployment]
4.2 Enable IP Forwarding on EC-V LAN0 Interface

By default, AWS EC2 instances have a source/destination check enabled on each interface. You must disable this on the LAN0 ENI (enable IP forwarding) for traffic to traverse through the EC-V instance.

1. Navigate to the EC-V instance and click the LAN0 interface eni ID in the Interface ID field.

2. On the interface page, select Change source/dest. check from the Actions drop down.

3. Clear the Enable check box and click Save.
4.3 Modify Route Table on AWS

Because the AWS VPC internal route table does not have a route to reach the remote branch network (e.g., SD-WAN networks), you need to add a route table entry with next hop as LAN0 interface of EC-V to reach the remote branch network.

NOTE: Because this deployment example is on a single VPC environment, there is only one route table used for both EC-V and other workloads within the VPC. If you have a different route table attached to EC-V interfaces and other workloads in the cloud, then you would have to repeat this section for both of the route tables.

1. Identify the route table. Navigate to **Instances** and select your instance then click **Networking**. On the Subnets page, click **Subnet ID**, and then click the Route table “rtb-xxxxxxxxxxxxx”.

2. Click **Routes** to display existing routes. As shown below, only two routes are displayed, one is a default route and the other is a local VPC network route.

3. Add an entry for SD-WAN network. In the Target field enter “Network Interface → LAN0 interface of EC-V”, in this example CIDR 172.16.0.0/12 is added, so any traffic destined for 172.16.0.0/12 is redirected to LAN0 interface of the EC-V.

4. Click **Save changes**.
4.4 Add Static Route Entry on EC-V to Reach the Workload Subnet

You need to add static route entry to reach AWS VPC CIDR (e.g., 172.20.32.0/22) via the LAN0 default gateway.

1. Log in to Orchestrator and select the EC-V from the appliance tree.
2. Navigate to Configuration > Routing > Route and click the edit icon next to the EC-V.
3. Enter the Subnet/Mask, enter Next Hop, and click Add then click Save to complete the static route addition on EC-V.
4.5 **Security Group Policies Check**

Once IP Forwarding is enabled on the LAN0 interface and route table entry is added to reach the remote network, ensure the security group associated with your instance and EC-V LAN0 allows traffic originating from the remote network.

In this example, you will test connectivity between an Ubuntu client on AWS cloud and a host in the branch network. The Ubuntu instance and the EC-V LAN0 interface have their own security groups.

The following figure shows the security group policy associated with the Ubuntu client instance, which has an inbound rule to allow traffic from the 172.16.0.0/12 network.

![Image of Ubuntu client instance security group policy]

The following figure shows the security group policy associated with LAN0, which has an inbound rule to allow traffic from the 172.16.0.0/12 network.

![Image of LAN0 security group policy]
4.6 Testing Connectivity

From the client instance on AWS cloud, initiate a ping/traceroute test:

Make sure that the flows on the EC-V appliance show up properly.

Single EC-V Deployment. You have successfully completed all the required steps to deploy EC-V in AWS Cloud and configuring traffic redirection using Static Route method.
5 GRE Method of Integrating with AWS Transit Gateway

Integrating with AWS Transit Gateway (TGW) offers the benefit of connecting the SD-WAN Fabric with VPCs that are attached to the AWS Transit Gateway. It also provides the flexibility of using BGP to exchange routes between EC-V and TGW. This section details the configuration steps necessary to integrate EC-V with TGW.

The following subsections detail the configuration tasks that are required to be completed in the AWS Management Console and Orchestrator to integrate the EC-V with TGW.

1. AWS Transit Gateway Configuration
2. EC-V Configuration for GRE Integration with TGW

5.1 AWS Transit Gateway Configuration

To prepare for AWS TGW integration with EC-V, the following tasks must be completed on the AWS Management Console before configuring EC-V appliances:

1. Create Transit Gateway
2. Create Transit Gateway Attachment for VPCs
3. Create Transit Gateway Attachment for Connect
4. Creating Connect Peers
5. Verifying Security Group for GRE Communication
6. Verifying Route Table to Reach GRE Endpoints
7. Enable IP Forwarding

HA EC-V Deployment: Most of the tasks in this section detail the procedure for a Single EC-V, so some of the tasks must be repeated for both the EC-Vs in HA deployment. When additional configuration is needed in HA EC-V deployment, refer to specific instructions provided on each task.
5.1.1 Create Transit Gateway

**NOTE:** You can skip this step if you already have a Transit Gateway (TGW) running in the **same region** as that of EC-V.

1. To create a new TGW, Navigate to **VPC > Transit Gateways**.
2. Click **Create transit gateway** and fill in the details such as **Name** and **ASN** (Autonomous System Number based on your design or you can pick a new ASN between the ranges 64512-65534 or 4200000000-4294967294).
3. Leave the rest of the default settings and click **Create transit gateway** to complete the Transit Gateway creation.

This completes the step of creating a new Transit Gateway.

**NEXT:** **VPC attachment with Transit Gateway**

- Proceed to **Section 5.1.2** to create Transit Gateway Attachment.
5.1.2 Create Transit Gateway Attachments for VPCs

In this step, attach all VPCs in the region that need to forward traffic to the SD-WAN fabric including the Transit VPC (where the EC-Vs are deployed) to the Transit Gateway. Table 2 provides a list of VPCs that are in the AWS cloud region that you will attach to the Transit Gateway. This step is important. Failing to add VPCs results in the TGW not propagating the VPC CIDR to the EC-V and on-prem sites being unable to reach workloads in VPCs that are not attached.

<table>
<thead>
<tr>
<th>VPC Detail</th>
<th>CIDR</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit VPC</td>
<td>172.20.36.0/22</td>
<td>2 x EC-Vs are deployed in this VPC.</td>
</tr>
<tr>
<td>Spoke VPC – A</td>
<td>172.20.40.0/22</td>
<td>Web server instances in this VPC.</td>
</tr>
<tr>
<td>Spoke VPC – B</td>
<td>172.20.44.0/22</td>
<td>Email server instances in this VPC.</td>
</tr>
</tbody>
</table>

1. Navigate to VPC > Transit Gateways > Transit gateway attachments.
2. Click Create transit gateway attachment. The Create transit gateway attachment page opens.
3. Enter a name in the Name tag field, select the Transit Gateway ID, select VPC in the Attachment type drop down, and select the VPC ID that will be attached to the TGW.
4. After you have entered all the details, click Create transit gateway attachment.

5. Repeat steps 1 to 4 for each VPC in the region that needs to send traffic to the SD-WAN fabric.

This completes the step of creating new Transit Gateway Attachment.

NEXT: Connect Attachment with Transit Gateway

Proceed to Section 5.1.3 to Create Transit Gateway Connect Attachment.
5.1.3 Create Transit Gateway Connect Attachment

**IMPORTANT:** Complete Section 5.1.2 for Transit VPC attachment before stating this step. You need the Transit VPC attachment ID to create the Connect attachment.

1. Navigate to VPC > Transit gateways > Transit gateway attachment.
2. Click Create transit gateway attachment. The Create transit gateway attachment page opens.
3. Enter a name in the Name tag field, select the Transit Gateway ID, and select Connect in the Attachment type field.
4. Under the Connect attachment section, select your Transit VPC attachment ID from the Transport attachment ID drop down.
5. After you have entered all the details, click Create transit gateway attachment.

This completes the step of creating new Transit Gateway Attachment.

**NEXT: Connect Peers**

- Proceed to Section 5.1.4 to Create Connect Peers.
5.1.4 Creating Connect Peers

Before starting this step, gather the following details from the EC-V that you will use for creating the Connect Peer with Transit Gateway.

**Peer GRE address**: LAN0 IP address of the EC-V.

**Peer ASN**: AS Number that will be used on the EC-V for peering with TGW.

**BGP Inside CIDR IPV4**: Identify a /29 subnet within the range of 169.254.0.0/16 that is needed for the BGP endpoints on the Transit Gateway and the EC-V.

An example of details you would need to proceed further in this section:

<table>
<thead>
<tr>
<th>Peer GRE address</th>
<th>172.20.36.36</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer ASN</td>
<td>65120</td>
</tr>
<tr>
<td>BGP inside CIDR IPV4</td>
<td>169.254.36.0/29</td>
</tr>
</tbody>
</table>

**HA Deployment:**

Repeat the task of collecting the peer details from the second EC-V.

Repeat the following steps 1 through 8 for the second EC-V.

**On step 5**: Ensure that you add the same AS Number for both of the EC-Vs in the HA Deployment.

1. Navigate to VPC > Transit gateways > Transit gateway attachment.
2. Locate the Transit VPC attachment in the available list. You can also search by name to locate the attachment.
3. When you locate the attachment, do not click any of the IDs only click the check box on the left.
4. Click the Connect Peers tab and then click Create connect peer.
5. On the Create connect peer page, enter a name in the Name Tag field, enter the Peer GRE address, enter the BGP Inside CIDR blocks IPv4, and enter the Peer ASN.

6. Click Create connect peer to complete the connect peer creation.

7. After creating the Connect Peer, the Connect Peers tab should show something like the following graphic with details of the GRE IP address and the BGP address.
8. The following is a summary of information gathered from this section. You will use this information in later steps for creating a GRE tunnel and creating BGP neighbors on the EC-V appliance.

<table>
<thead>
<tr>
<th>Transit Gateway ASN</th>
<th>65100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit Gateway GRE address</td>
<td>172.20.252.115</td>
</tr>
<tr>
<td>Transit Gateway BGP1 address</td>
<td>169.254.36.34</td>
</tr>
<tr>
<td>Transit Gateway BGP2 address</td>
<td>169.254.36.35</td>
</tr>
<tr>
<td>EC-V ASN</td>
<td>65120</td>
</tr>
<tr>
<td>EC-V GRE address (EC-V LAN0 IP)</td>
<td>172.20.36.36</td>
</tr>
<tr>
<td>EC-V BGP address (EC-V VTI IP)</td>
<td>169.254.36.33</td>
</tr>
</tbody>
</table>

5.1.5 Verifying Security Group for GRE communication

This section describes how to validate security group settings attached to the LAN0 interface subnet. It is important to ensure that the LAN0 interface can receive incoming traffic that is coming from the GRE endpoints.

**HA Deployment:** Repeat the following steps 1 to 6 for each EC-V instance that you will integrate with the AWS Connect GRE endpoint.

1. Locate your EC-V instance. Navigate to **EC2 Dashboard > Instances** and then search for your EC-V instance name or ID or the IP address for your EC-V instance.
2. At the bottom multiple tabs appear providing various details about your instance, click the **Networking** tab.
3. Identify your LAN0 interface ENI. Do not click the ENI but scroll to the right to view the security group.
4. Click the Security Group for the LAN0 interface to view the inbound rules.

5. **Verifying Security Group for GRE communication**

   **HA Deployment:** Repeat the following steps 1 to 6 for each EC-V instance that you will integrate with the AWS Connect GRE endpoint.

1. Locate your EC-V instance. Navigate to **EC2 Dashboard > Instances** and then search for your EC-V instance name or ID or the IP address for your EC-V instance.
2. At the bottom multiple tabs appear providing various details about your instance, click the **Networking** tab.
3. Identify your LAN0 interface ENI. Do not click the ENI but scroll to the right to view the security group.
4. Click the Security Group for the LAN0 interface to view the inbound rules.
5. In the following example, the security group policy associated with LAN0 has an inbound rule to **allow all** traffic from 172.16.0.0/12 network. Because the GRE endpoint in this example is within the range of 172.20.252.0/24, this rule is sufficient. Add an inbound rule specific to your GRE endpoint subnets if your GRE endpoint subnet is not already part of the inbound rules.

6. Similarly, check the outbound rules to ensure outbound communication (most of the time the default outbound rule is set to allow all outbound traffic). If there is no explicit permit entry, then add one to allow all outbound traffic to reach GRE endpoints.

This completes the step of creating new Transit Gateway Attachment.

**NEXT: Verify Route Table**

- Proceed to **Section 5.1.6** to Verify Route Table to reach GRE endpoints.
5.1.6 Verifying Route Table to Reach GRE Endpoints

Ensure that there is a route table entry to reach the GRE endpoints (in this example: 172.20.252.0/24 is the network for the GRE endpoints) with Transit Gateway as next hop. This is required for the EC-V to be able to reach the AWS Connect GRE endpoints to build a GRE tunnel. To check the routing, locate your instance LAN0 subnet and check the routing table entry on the route table associated with the subnet.

HA Deployment: Repeat the following steps 1 to 6 for each EC-V instance that you will integrate with the AWS Connect GRE endpoint.

1. Locate your EC-V instance. Navigate to EC2 Dashboard > Instances and then search for your EC-V instance name or ID or the IP address for your EC-V instance.
2. At the bottom multiple tabs appear providing various details about your instance, click the Networking tab.
3. Identify your LAN0 ENI. Do not click the ENI but scroll to the right of the screen to view the subnet ID.
4. The Subnets page opens with the specific LAN0 subnet filtered. Click the ID in the Route table field.
5. View existing routes under the Routes tab. Click Edit routes to add a route table entry to reach the GRE endpoint (172.20.252.0/24) via the Transit Gateway.
In the following example, 172.16.0.0/12 includes the GRE endpoint subnet 172.20.252.0/24 route entry added pointing to TGW.

This completes the Route Table verification for LAN0 interface.

**NEXT: Enable IP Forwarding on LAN0 interface**

- Proceed to Section 5.1.7 to enable IP Forwarding on LAN0 interface.
5.1.7 Enable IP Forwarding on EC-V LAN0 Interface

By default, AWS EC2 instances have a source/destination check enabled on each interface. You must disable this on the LAN0 ENI (enable IP forwarding) for traffic to traverse through the EC-V instance.

1. Navigate to the EC-V instance and click the LAN0 interface eni ID in the Interface ID field.

2. On the interface page, select the Change source/dest. check from the Actions drop down.

3. Clear the Enable check box and click Save.

This completes Transit Gateway configuration on AWS Management console for GRE integration.

**NEXT: EC-V Configuration for GRE Integration**

- Proceed to Section 5.2 to complete EC-V side configuration for GRE integration through Aruba Orchestrator.
5.2 EC-V Configuration for GRE Integration with TGW Connect

Figure 7 provides a logical representation of an EC-V integration with AWS TGW using the TGW Connect method, which works on a GRE tunnel. In this GRE method of integration, we do not need a public IP address on the LAN0 interface. A single GRE tunnel is formed between the LAN0 interface private IP and the TGW GRE endpoint private IP. Then BGP sessions are established over the GRE tunnel between the EC-V Virtual Tunnel Interface (VTI) and TGW to exchange routes dynamically between them.

The following diagram only shows the LAN0 interface and the VTI interface required for establishing connectivity with the Transit Gateway. The WAN0 interface and MGMT0 interface details are omitted for brevity.
Section 5.1 details all the required tasks that you must complete from the AWS management console before configuring the EC-V via Orchestrator, such as, creating a Transit Gateway attachment and creating Connect Peers, Security Groups, and Route Table to establish BGP over GRE connectivity with the Transit Gateway.

The following section details configuration tasks that you must complete in Orchestrator to integrate the EC-V with AWS TGW.

1. Create a Static Route on the EC-V to reach TGW Connect GRE Endpoints
2. Create a GRE Passthrough Tunnel
3. Create a VTI interface
4. Establish a BGP Peer Neighborship with TGW Connect BGP Endpoints
5. Redistributing Routes and Enabling ECMP
6. Check Routes on EC-V
7. Check Routes on TGW

Configuration Tasks on the EC-V are common for both Single and HA EC-V deployments. For HA EC-V deployments, refer to specific instructions provided in each task.
5.2.1 Create Static Route to Reach TGW Connect GRE Endpoints via LAN0 Interface

Adding a static route to reach GRE endpoints is essential to form GRE tunnels between the EC-V and TGW GRE endpoints.

HA Deployment: You must complete this task (steps 1 to 5) on each EC-V that will connect to the AWS Transit Gateway.

To complete this step, you need the GRE endpoint IP address or subnet and LAN0 interface next hop address. In this example, the GRE endpoints are part of subnet 172.20.252.0/24. You will add a static route to reach this subnet via the LAN0 interface next hop (172.20.36.33).

1. Log in to Orchestrator.
2. Select the EC-V from the appliance tree.
4. Click the edit icon next to the EdgeConnect appliance. In this example, for Segment select Default because the LAN0 interface is on that segment.

5. Click Add Route.
6. Add a static route to reach the GRE subnet using the LAN0 next hop (you can choose to add a specific host IP route as well).

The following example shows the route table after adding the static route.

```
<table>
<thead>
<tr>
<th>Subnet/Mask</th>
<th>172.20.252.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Hop</td>
<td>172.20.36.33</td>
</tr>
<tr>
<td>Interface</td>
<td>lan0</td>
</tr>
<tr>
<td>Metric</td>
<td>50</td>
</tr>
<tr>
<td>Tag</td>
<td>ANY</td>
</tr>
<tr>
<td>Comments</td>
<td>Static Route to reach TELV Connect GRE endpoints</td>
</tr>
</tbody>
</table>
```

7. This completes the task of adding static route on EC-V to reach GRE peer IP addresses.

**NEXT: Configure GRE Passthrough Tunnel**

- Proceed to Section 5.2.2 to create GRE Passthrough tunnel.
5.2.2 Create GRE Pass Through Tunnel

After the static route to reach the GRE endpoints is added, the GRE tunnel can be built from the LAN0 interface. You will need to create a single passthrough tunnel from each EC-V.

HA Deployment: You must repeat this task (steps 1 to 6) for each EC-V appliance that will build a tunnel with the AWS Transit Gateway.

1. In Orchestrator, select the EC-V from the appliance tree.
3. Click the edit icon next to the EdgeConnect appliance.
4. On the Tunnels page, click Passthrough then click Add Tunnel.
5. Enter information in the Alias, Mode, Admin, Local IP, and Remote IP fields. Click Save.

6. The tunnel should show status as “up-active” on the Passthrough section.

This completes the task of creating GRE Passthrough tunnel on EC-V.

NEXT: Create VTI Interface

- Proceed to Section 5.2.3 to create VTI interface.
5.2.3 Create VTI Interface

To create BGP neighborship with TGW Connect peers, you need a VTI interface on the EC-V, which will be mapped to the GRE passthrough tunnel that was created in the previous step.

HA Deployment: You must repeat this task (steps 1 to 5) for each EC-V appliance that will build a tunnel with the AWS Transit Gateway.

1. In Orchestrator, select the EC-V from the appliance tree.
3. Click the edit icon next to the EdgeConnect appliance.
4. On the Virtual Tunnel Interfaces (VTI) page, click Add to add a new VTI interface and enter the required details.
   - Segment: Select Default (in this example BGP will be using the default VRF segment) from the drop down.
   - Interface vti: Enter a valid number (e.g., 1).
   - IP/Mask: Enter the BGP address for the EC-V that was obtained when creating a Connect Peer in Section 5.1.4. It is important to add the correct subnet mask here along with the IP address. Because this ensures that BGP will find a proper route in the route table to reach the TGW Connect BGP peers via the VTI interface.
   - Passthrough Tunnel: From the drop down, select the GRE tunnel name that was added in Section 5.2.2.
   - Interface Type: Select lan from the drop down.
   - Label/Zone: Leave the default selection for both.
5. Click Add to save the new VTI interface.
6. After the VTI interface is added, it should appear on the Virtual Tunnel Interfaces (VTI) page with a status of “up.”

This completes the task of creating VTI interface on EC-V.

NEXT: Configure BGP Peering

- Proceed to Section 5.2.4 to configure and establish BGP peer neighborship with Transit Gateway.
5.2.4 Establish BGP Peer Neighborship with TGW Connect Endpoints

The GRE tunnel and VTI interface created in the previous steps helps to complete the final task of establishing BGP neighborship with the TGW. After the BGP neighborship is established, EC-V and TGW Connect are able to exchange routes dynamically.

HA Deployment: You must complete this task (steps 1 to 10) for each EC-V appliance that will establish a BGP neighborship with the AWS Transit Gateway.

1. In Orchestrator, select the EC-V from the appliance tree.
2. Navigate to Configuration > Networking > Routing > BGP.
3. Click the edit icon next to the EdgeConnect appliance. In this example, for Segment select Default because it is the intended segment. The VTI interface is also created on the same default segment.
4. On the BGP page, move the toggle to Enable BGP.
5. Refer to the summary table created in Step 5.1.4 as this information is needed to complete the rest of the steps in this task. The following example table is provided for reference:

<table>
<thead>
<tr>
<th>Transit Gateway ASN</th>
<th>65100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit Gateway GRE address</td>
<td>172.20.252.115</td>
</tr>
<tr>
<td>Transit Gateway BGP1 address</td>
<td>169.254.36.34</td>
</tr>
<tr>
<td>Transit Gateway BGP1 address</td>
<td>169.254.36.35</td>
</tr>
<tr>
<td>EC-V ASN</td>
<td>65120</td>
</tr>
<tr>
<td>EC-V GRE address</td>
<td>172.20.36.36</td>
</tr>
<tr>
<td>EC-V BGP address</td>
<td>169.254.36.33</td>
</tr>
</tbody>
</table>
6. Enter the details in the Autonomous System Number field, the Router ID field (could be IP address of VTI or LAN0 interface), and optionally select the Graceful restart check box.
7. After the BGP information is added, click Add to add BGP peers.
8. Enter the information on the BGP peer page to complete BGP peer configuration and click **Add**.

![BGP Peer Information](image)

- **Peer IP**: Enter the TGW Connect BGP1 address.
- **Peer Adjacency**: Click Multi-Hop.
- **Local Interface**: Select vti1 from the drop down.
- **Peer ASN**: Enter 65100.
- **Override ASN**: Select the check box.
- **Peer Type**: Select Branch from the drop down.

9. Repeat **Step 8** for the second TGW Connect BGP address and the second BGP2 endpoint.

![BGP Peer Information](image)

- **Peer IP**: Enter the TGW Connect BGP2 address.
- **Peer Adjacency**: Click Multi-Hop.
- **Local Interface**: Select vti1 from the drop down.
- **Peer ASN**: Enter 65100.
- **Override ASN**: Select the check box.
- **Peer Type**: Select Branch from the drop down.

10. This completes the BGP configuration on the EC-V. Navigate to **Configuration > Networking > Routing > BGP** and click **Peers**.

   If the GRE tunnel is established and the VTI interface is mapped to the correct passthrough GRE tunnel, you should see a status of “Established” in the Peer State column for the BGP session.

This completes the task of configuring and establishing BGP neighborship with TGW.

**NEXT: Route Redistribution and ECMP**

- Proceed to **Section 5.2.5** to configure Route Redistribution and ECMP.
5.2.5 Redistributing Routes and Enabling ECMP

Now that BGP is established between TGW and the EC-V, you can see how the SD-WAN fabric routes are redistributed to TGW and how the TGW BGP routes are getting redistributed to the SD-WAN fabric.

**HA Deployment:** Repeat sections 5.2.5a to 5.2.5d for each EC-V appliance that has established a BGP session with the AWS Transit Gateways.

5.2.5.a Redistributing SD-WAN Fabric Routes to TGW

By default, EdgeConnect appliances send all Local/Static, OSPF, BGP and other SD-WAN fabric routes to TGW. This is controlled by the BGP Outbound route map that is attached to the BGP neighbor under the BGP peer configuration. You can customize the route maps according to your requirements, either by creating a new route map or by modifying an existing route map to allow or deny specific routes based on protocol or subnet prefix.

Navigate to Configuration > Routing > BGP and click the edit icon next to the EC-V appliance. Then edit the BGP peer by clicking the edit icon for the Outbound route map.

5.2.5.b Receiving BGP Routes from TGW

Similarly, the BGP Inbound route map controls what routes are accepted by the EdgeConnect. By default, all BGP routes coming from TGW BGP neighbors are accepted by EdgeConnect appliances. You can further customize by adding rules on the existing route map or attaching a new route map to permit/deny specific subnet prefixes.
5.2.5.c Redistributing TGW BGP Routes to SD-WAN fabric

By default, all BGP routes from TGW are sent to the SD-WAN fabric using subnet sharing (an internal route sharing protocol used by EdgeConnect devices). You can customize the subnet share route map to control which routes can be shared with the rest of the SD-WAN fabric including the TGW BGP routes.

1. To view the current route map that controls the subnet sharing with the SD-WAN fabric, navigate to Configuration > Networking > Routing > Routes, then click the edit icon next to the hostname and the Route page opens. This example is on the default segment.

2. For REDistribute route to SD-WAN fabric, click the edit icon to view the rules and ensure that the Match Criteria shows “Source Protocol BGP” and Permit shows “Allow.”

The following figure shows the “default_rtnmap_to_subsh” route map, which allows BGP routes to be redistributed to the SD-WAN fabric.
5.2.5.d Enabling ECMP

Equal Cost Multi Path (ECMP) allows the traffic to be carried on multiple paths simultaneously when more than one equal cost route to a destination exists on the appliance. ECMP is disabled on the EdgeConnect appliance by default. You can enable ECMP under the Routes tab of the configuration.

**NOTE:** This setting is common for all VRF segments when enabled ECMP is applied to all the VRF segments (if VRF is configured in your environment).

Navigate to Configuration > Networking > Routing > Routes and click the edit icon next to the hostname. This example is on the default segment.

This completes the task of configuring Route Redistribution and ECMP. **NEXT: Verify Routes on EC-V**

- Proceed to Section 5.2.6 to verify BGP routes coming from TGW to ECV.
### 5.2.6 Checking Routes from TGW to EC-V

When the BGP session shows “Established” on the BGP page (Peers), you can validate if both the TGW BGP endpoints are sending routes to EC-V or not.

**HA Deployment:** Repeat steps 1 to 6 for each EC-V appliance that has established a BGP session with the AWS Transit Gateways.

1. Navigate to Configuration > Networking > Routing > Routes and click BGP to view BGP routes only.

   The route table in **Figure 8** shows the routes for both BGP peers 169.254.36.34 and 169.254.36.35, which are the two TGW BGP neighbors configured in Section 5.2.4.

   Note that each route is learned twice because ECMP is enabled on the EC-V. For example, in **Figure 8**, subnet 172.20.44.0/22 is learned from **169.254.36.34** TGW BGP neighbor and as well from **169.254.36.35** TGW BGP neighbor.

2. You must enable ECMP under the Routes tab to see multiple route paths. Refer to Section 5.1.7 to enable ECMP. With ECMP enabled, EdgeConnect is able to send traffic across both BGP peers.

3. Navigate to Configuration > Networking > Routing > Routes and click BGP to view BGP routes only.

4. Check your inbound route map attached to the BGP neighbor if you don’t see all the routes that are expected to come from TGW (refer to Section 5.2.5b). The following figure shows an inbound route map that allows all the BGP routes coming from TGW BGP peers.

   ![Figure 8: Route Table of a EC-V](image)

   **This completes the task of verifying routes on EC-V coming from TGW.**

   **NEXT: Verify Routes on TGW**

   - Proceed to **Section 5.2.7** to verify BGP routes coming from EC-V to TGW.
5.2.7 Checking Routes from EC-V to TGW

To ensure end-to-end communication from AWS VPCs to the EdgeConnect SD-WAN fabric, you will validate that the EdgeConnect SD-WAN fabric routes are making it to the TGW route table.

1. On the AWS Management Console, navigate to VPC > Transit gateways and locate your TGW on the right panel. You can also search for your TGW using the TGW name or ID.
2. Under the Details section, click the Association route table ID to display the route table for your TGW.

3. On the Routes tab, you will see all the incoming routes from EdgeConnect BGP peers.

   If it is a single EC-V deployment, you must see 2 Attachments under the Attachment ID column to indicate that routes are received on both of the BGP connections from the single EC-V.

   In this example, two EdgeConnect appliances have been integrated with TGW, so you see 4 Attachments for each route entry because both of the EC-Vs are sending the routes to TGW (each EC-V has 2 BGP neighborships with TGW).
4. If you do not see your intended SD-WAN fabric routes, check the Outbound route map that is attached to each TGW BGP peer on your EdgeConnect. The following figure shows a route map that allows all the SD-WAN fabric routes by default.

![Route Map Example](image)

This completes the task of verifying routes on TGW coming from EC-V.

**NEXT:** Only for HA EC-V Deployment - Proceed to Section 7 to configure Redundancy.

**Single EC-V Deployment** - You have successfully completed all the required steps to deploy EC-V in AWS Cloud and integrated it with AWS TGW using GRE Connect method.
6 IPsec Method of Integrating with AWS Transit Gateway

Integrating with AWS Transit Gateway (TGW) offers the benefit of connecting the SD-WAN Fabric with VPCs that are attached to the Transit Gateway. It also provides the flexibility of using BGP to exchange routes between EC-V and TGW. In this section, we will detail the configuration steps necessary to integrate EC-V with TGW using IPSEC method.

The following subsections outline the configuration tasks in both the AWS Management Console and Orchestrator to complete the integration between the EC-V and TGW.

1. AWS Transit Gateway configuration
2. EC-V configuration for IPsec integration with TGW

These instructions establish BGP with Transit Gateway using a VPN attachment feature on AWS. To establish a VPN attachment with the Transit Gateway, the remote VPN endpoint must be a public IP address. You will use the LAN0 interface of an AWS EC-V instance when establishing a VPN attachment with the Transit Gateway. Because the LAN0 interface does not have a public IP address assigned to it, you must assign an Elastic IP to it before you attempt to create a VPN attachment with the Transit Gateway.

6.1 AWS Transit Gateway Configuration

To prepare for AWS TGW integration with EC-V, complete the following tasks on the AWS Management Console before configuring EC-V appliances:

1. Create Transit Gateway
2. Create Transit Gateway Attachment for VPCs
3. Create Elastic IP Address and Attach it to LAN0 Interface
4. Create Customer Gateway
5. Create Transit Gateway Attachment for Customer Gateway
6. Download VPN Configuration
7. Verifying Security Group for IPsec Communication
8. Verify Route table to Reach VPN Gateway Endpoints
9. Enable IP Forwarding

HA EC-V Deployment: Most of the tasks in this section detail the procedure for a Single EC-V, so some of the tasks must be repeated for both the EC-Vs in HA deployment. When additional configuration is needed in HA EC-V deployment, refer to specific instructions provided on each task.
6.1.1 Create Transit Gateway

You can skip this step if you already have a Transit Gateway (TGW) running in the same region as that of EC-V.

1. To create a new TGW, Navigate to VPC > Transit Gateways.
2. Select Create transit gateway and fill in the details such as Name, ASN (Autonomous System Number based on your design or you can pick a new ASN between 64512-65534 or 4200000000-4294967294 ranges).
3. Leave the rest of the default settings and click Create transit gateway to complete the Transit Gateway creation.
4. Leave the rest of the default settings and click Create transit gateway to complete the Transit Gateway creation.

AS Number for the Transit Gateway. Note: this is not the AS number of the EC-V appliance.

Providing a /24 CIDR here is required when using GRE integration. AWS Connect will use this IP subnet for GRE tunnel termination.
6.1.2 Create Transit Gateway Attachments for VPCs

In this step, attach all VPCs in the region that need to forward traffic to the SD-WAN fabric including the Transit VPC (where the EC-Vs are deployed) to the Transit Gateway. Table 3 provides a list of VPCs that are in the AWS cloud region that you will be attach to the Transit Gateway. This step is important. Failing to add VPCs results in the TGW not propagating the VPC CIDR to the EC-V and on-prem sites being unable to reach workloads in VPCs that are not attached.

<table>
<thead>
<tr>
<th>VPC Detail</th>
<th>CIDR</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit VPC</td>
<td>172.20.36.0/22</td>
<td>2 x EC-Vs are deployed in this VPC</td>
</tr>
<tr>
<td>Spoke VPC – A</td>
<td>172.20.40.0/22</td>
<td>Web server instances in this VPC</td>
</tr>
<tr>
<td>Spoke VPC – B</td>
<td>172.20.44.0/22</td>
<td>Email server instances in this VPC</td>
</tr>
</tbody>
</table>

1. Navigate to **VPC > Transit Gateways > Transit gateway attachment**.
2. Click **Create transit gateway attachment**. The Create transit gateway attachment page opens.
3. Enter a name in the Name tag field, select the Transit Gateway ID, select **VPC** in the attachment type drop down, and select the VPC ID that will be attached to the TGW.
4. After you have entered all the details, click **Create transit gateway attachment**.

5. Repeat steps 1 to 4 for each VPC in the region that needs to send traffic to the SD-WAN fabric.
6.1.3 Create Elastic IP Address and Attach it to LAN0 Interface

Skip this task if the LAN0 interface already has an Elastic IP address attached to it.

HA Deployment: Repeat steps 1 to 3 for each EC-V instance that will be integrated with the AWS TGW.

1. Navigate to VPC > Elastic IP Addresses or use the search bar to search for “Elastic IP” and select Elastic IP addresses from the search results.

2. To create a new Elastic IP address, click Allocate Elastic IP address then click Allocate.

3. From the Actions drop down, click Associate Elastic IP address to associate the Elastic IP address to the LAN0 interface. Enter the appropriate information and click Associate.

- **Resource type:** Click the Network interface radio button.
- **Network interface:** Make sure you select the LAN0 interface ID. You can find this ID on the Networking tab under your EC-V instance.
- **Private IP address:** The Private IP address automatically pops up when the cursor is placed in this field. In this case it’s the LAN0 interface private IP address.
6.1.4 Create Customer Gateway

You will add the EC-V as a customer gateway in this section. This task allows you to add the EC-V as a VPN attachment to the TGW.

HA Deployment: Repeat steps 1 and 2 for each EC-V instance that will be integrated with the AWS TGW.

2. Select Create customer gateways and enter the details as required. Leave the optional fields as is. Click Create customer gateway.

Name tag: Enter a name for your attachment.
BGP ASN: Enter the ASN Number that is configured on the EC-V appliance.
IP Address: Enter the LAN0 Elastic IP address.
6.1.5 Create Transit Gateway Attachment for Customer Gateway

In this section, select each customer gateway (EC-V) and attach it to the transit gateway to create site-to-site VPN configuration.

HA Deployment: Repeat the steps 1 to 8 for each EC-V instance that will be integrated with the AWS TGW.

1. Navigate to VPC > Transit Gateways > Transit gateway attachment.
2. Click Create transit gateway attachment. The Create transit gateway attachment page opens.
3. Select the Transit gateway ID from the drop-down list.
4. Select VPN from the Attachment type drop down.

5. Under the VPN Attachment section, for Customer Gateway click Existing and select the Customer Gateway ID that you created in Step 6.1.4.
6. Leave the default selections for the other items, and click Create transit gateway attachment.
7. After the customer gateway attachment is completed successfully, the Site-to-Site VPN Connections page is automatically created and lists the tunnel detail for each customer gateway attachment.

8. Navigate to **VPC > Virtual Private Networks (VPN) > Site-to-Site Connections** and locate your customer gateway using either the name or public IP. When you have located your customer gateway, click the **Tunnel Details** tab.

```
<table>
<thead>
<tr>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down</td>
<td>Status</td>
</tr>
</tbody>
</table>
```

Status will show Down as we have not completed the setup on the EC-V.
6.1.6 Download VPN Configuration

In this section, you will download the VPN configuration file, which contains the IPsec tunnel endpoint IP address, IKE/IPsec auth parameters, and BGP peering details that are necessary to complete the EC-V configuration.

HA Deployment: Repeat above steps 1 to 5 for each EC-V customer gateway as it is single file per customer gateway VPN connections.

1. Navigate to VPC > Virtual Private Networks (VPN) > Site-to-Site VPN Connections and locate your customer gateway using either the name or the public IP.

2. When you locate your customer gateway, highlight it, as shown in the following figure, but do not click any IDs. Click Download configuration to download the VPN configuration for that specific EC-V.

3. The Download Configuration menu appears, as shown in the following figure. Click Download to download the VPN configuration file for the customer gateway (EC-V).

NOTE: Make sure you save the configuration file to your desktop because you will need the information from the file to configure the EC-V IPsec Tunnel and BGP peering.
6.1.7 Verifying Security Group for IPsec Communication

Validate security group settings attached to the LAN0 interface subnet. This is important to make sure that the LAN0 interface can receive incoming traffic coming from TGW VPN endpoints.

**HA Deployment:** Repeat the steps 1 to 6 for each EC-V instance that will be integrated with the AWS Transit Gateway for IPsec integration.

1. Locate your EC-V instance. Navigate to **EC2 Dashboard > Instances** and then search for your EC-V instance name or ID or the IP address for your EC-V instance.
2. At the bottom multiple tabs appear providing various details about your instance, click the **Networking** tab.
3. Identify your LAN0 ENI. Do not click the ENI but scroll to the right of the screen to view the security group.

4. Click the security group for the LAN0 interface to view the inbound rules.

   In the following example, the security group policy associated with LAN0 interface has Inbound rules to allow traffic from specific VPN endpoints for IPSEC communication (UDP port 4500 and UDP 500).

5. Also check the Outbound rules to ensure outbound communication (most of the time the default outbound rule is set to allow all outbound traffic). If there is no explicit permit entry, then add one to reach IPSEC endpoints.
6.1.8 Verifying Route Table to Reach VPN Gateway Endpoints

Ensure that there is a route table entry to reach IPSEC VPN endpoints (in this example 3.18.28.220 and 18.188.142.5 are the two VPN endpoints) with Internet Gateway as next hop. This is required for the EC-V to reach the TGW VPN Gateway endpoints to build the IPsec tunnel. To check the routing, locate your instance LAN0 subnet and check the routing table entry on the route table associated with the subnet.

HA Deployment: Repeat steps 1 to 8 for each EC-V instance that will be integrated with the AWS Transit Gateway for IPsec integration.

1. Locate your EC-V instance. Navigate to **EC2 Dashboard > Instances** and then search for your EC-V instance name or ID or the IP address for your EC-V instance.

2. At the bottom multiple tabs appear providing various details about your instance, click the **Networking** tab.

3. Identify your LAN0 interface ENI. Do not click the ENI but scroll to the right to view the subnet ID.

4. Click the Subnet ID for the LAN0 interface.

5. The Subnets page opens with the specific LAN0 subnet filtered. Click the ID in the Route table field.

6. On the Route table page, click the check box for the row that displays the route table ID.
7. **Click the Routes tab to view existing routes.**

Add specific routes to reach TGW VPN endpoints from LAN0 subnet via Internet Gateway, click the **Edit routes** icon and add entries. Although the next hop is Internet Gateway, this traffic never leaves the AWS network. This is because the LAN0 interface has a public IP address owned by AWS and whenever AWS sees traffic originating from an IP address it owns, it keeps that traffic within its network as much as possible. Gather the VPN Gateway IP addresses from the Downloaded VPN configuration file (refer to **Section 6.1.6**).

The following figure shows a view of the Route table after adding route entries.
6.1.9 Enable IP Forwarding on EC-V LAN0 Interface

By default, AWS EC2 instances have a source/destination check enabled on each interface. You must disable this on the LAN0 ENI (enable IP forwarding) for traffic to traverse through the EC-V instance.

1. Navigate to the EC-V instance and click the LAN0 interface eni ID in the Interface ID field.

   ![Image of EC2 instance interface](image)

2. On the interface page, select Change source/dest. check from the Actions drop down.

   ![Image of Actions dropdown](image)

3. Clear the Enable check box and click Save.

   ![Image of Save button](image)

This completes all tasks at AWS Management Console side for Transit Gateway integration with EC-V.

NEXT: EC-V Configuration for IPSec integration

- Proceed to Section 6.2 to complete EC-V side configuration for IPsec integration.
6.2 EC-V Configuration for IPsec Integration with AWS TGW

Figure 9 provides a logical view of Transit Gateway integration with the EC-V when using IPsec method. It is important to note that the IPsec tunnel can be formed either on the WAN0 interface or on the LAN0 interface, but the use case specified here focuses on using the LAN0 interface because this avoids consuming WAN bandwidth on the EC-V appliance. When an EC-V is deployed in a VPC, it is recommended to use the LAN0 interface of that EC-V to establish connectivity with the Transit Gateway rather than a WAN interface.

Note that Figure 9 only shows the LAN0 interface and the VTI required for establishing connectivity with the Transit Gateway. The WAN0 interface and MGMT0 interface are omitted for brevity.

When integrated using the IPsec method, TGW creates an IPsec tunnel with two different VPN endpoints using public IP addresses. Hence, the LAN0 interface must have a public IP address mapped to it to be able to reach the VPN endpoint (on the Transit Gateway side). Finally, eBGP is established between the EC-V Virtual Tunnel Interface (VTI) and the Transit Gateway BGP endpoint IP addresses to exchange routes between them.
Section 6.1 details all the tasks that you must complete from the AWS management console before configuring the EC-V via Orchestrator, such as, creating an Elastic IP for the LAN0 interface, creating Transit Gateway attachments and a customer gateway, and ensuring security groups permit the required traffic and route entries to reach VPN endpoints through the LAN interface.

The following subsections outline the configuration tasks in Orchestrator to integrate EC-V with AWS TGW.

1. Create Two IPsec Passthrough Tunnels
2. Create Two VTI Interfaces
3. Establish BGP Neighborship with TGW BGP Endpoints
4. Redistributing Routes and Enabling ECMP
5. Check Routes on EC-V
6. Check Routes on TGW

Configuration tasks on the EC-V are common for both Single and HA EC-V deployments. For HA EC-V deployments, refer to specific instructions provided in each task.
6.2.1 Creating Passthrough IPsec Tunnels

Using the information from the downloaded VPN configuration file (refer to Section 6.1.6), you will build two IPsec passthrough tunnels on each EC-V. These IPsec tunnels terminate at two different VPN endpoints at TGW.

HA Deployment: This task steps 1 to 11 must be completed on each EC-V that needs to be connected to the Transit Gateway.

1. To complete this step, refer to the following sections on the downloaded VPN configuration file:

<table>
<thead>
<tr>
<th>Information from VPN config file – Tunnel 1</th>
<th>Information from VPN config file – Tunnel 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside IP Addresses:</td>
<td>Outside IP Addresses:</td>
</tr>
<tr>
<td>- Customer Gateway:</td>
<td>- Customer Gateway:</td>
</tr>
<tr>
<td>3.132.50.104</td>
<td>3.132.50.104</td>
</tr>
<tr>
<td>- Virtual Private Gateway</td>
<td>- Virtual Private Gateway</td>
</tr>
<tr>
<td>3.18.167.62</td>
<td>3.18.167.62</td>
</tr>
<tr>
<td>- IKE version:</td>
<td>- IKE version:</td>
</tr>
<tr>
<td>IKEv2</td>
<td>IKEv2</td>
</tr>
<tr>
<td>- Authentication Method:</td>
<td>- Authentication Method:</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>- Authentication Algorithm:</td>
<td>- Authentication Algorithm:</td>
</tr>
<tr>
<td>sha1</td>
<td>sha1</td>
</tr>
<tr>
<td>- Encryption Algorithm:</td>
<td>- Encryption Algorithm:</td>
</tr>
<tr>
<td>aes-128-cbc</td>
<td>aes-128-cbc</td>
</tr>
<tr>
<td>- Phase 1 Negotiation Mode:</td>
<td>- Phase 1 Negotiation Mode:</td>
</tr>
<tr>
<td>main</td>
<td>main</td>
</tr>
<tr>
<td>- Diffie-Hellman:</td>
<td>- Diffie-Hellman:</td>
</tr>
<tr>
<td>Group 2</td>
<td>Group 2</td>
</tr>
</tbody>
</table>

2. In Orchestrator, select the EC-V from the appliance tree.
4. Click the edit icon next to the EdgeConnect appliance.
5. On the Tunnels page, click Passthrough and click Add Tunnel.
6. Enter the details on the General tab.

Alias: Enter a name for the passthrough tunnel.
Mode: Select IPsec from the drop down.
Admin: Select up from the drop down.
Local IP: Begin typing and select the LAN0 interface IP from the drop down.
Remote IP: Enter the VPN endpoint outside IP address.
7. Click **IKE** and enter the details on the IKE tab.

8. Click **IPSec** and on the IPSec tab ensure that **SHA1** is selected from the Authentication algorithm drop down.

9. Click **Save** to complete the passthrough tunnel creation.

10. Repeat steps 4 through 8 for the second VPN endpoint.

11. Check the IPsec Passthrough Tunnel status. It should show a status of “up-active”, as shown in the following figure. If the tunnel doesn’t come up, check your VPN configurations for accuracy and correct any errors.
6.2.2 Create VTI Interfaces

Using the information from the downloaded VPN configuration file from Section 6.1.6, you will build two Virtual Tunnel Interfaces (VTI) that will be mapped to the two passthrough IPsec tunnels created in the previous step.

HA Deployment: You must complete steps 1 to 10 of this task on each EC-V that will connect to the Transit Gateway.

1. To complete this step, refer to the following sections on the downloaded VPN configuration file:

   **Information from VPN config file – Tunnel 1**

   **Information from VPN config file – Tunnel 2**

2. In Orchestrator, select the EC-V from the appliance tree.
3. Navigate to Configuration > Networking > Virtual Tunnel Interfaces (VTI).
4. Click the edit icon next to the EdgeConnect appliance.
5. On the Virtual Tunnel Interfaces (VTI) page, click Add to add a new VTI interface and enter the required details.

   - **Segment:** Select Default from the drop down.
   - **Interface vti:** Enter a valid number (e.g., 1).
   - **IP/Mask:** Tunnel 1 – Enter the Customer Gateway IP address from the VPN configuration file.
   - **Admin:** Select up from the drop down.
   - **Passthrough Tunnel:** Select the Passthrough tunnel 1 for this VTI interface.
   - **Interface Type:** Select lan from the drop down.

6. Click Add to save the new VTI interface.
7. On the Virtual Tunnel Interfaces (VTI) page, click **Add** to add another new VTI interface and enter the required details.

8. Click **Add** to save the new VTI interface.

This completes creation of two VTI interfaces on the EC-V that will be used in the next task to establish BGP neighborship with the TGW BGP endpoint.
6.2.3 Establish BGP Peer Neighborship with TGW Connect Endpoints

VTI interfaces created in previous step will help to complete the final task of establishing eBGP neighborship with TGW. Once the BGP neighborship is established, EC-V and TGW will be able to exchange routes dynamically.

**HA Deployment:** You must complete this task steps 1 to 7 on each EC-V that will connect to the AWS Transit Gateway.

You will need the following information from the VPN configuration file (refer Section 6.1.6).

### Information from VPN config file – BGP 1
- **BGP Configuration Options:**
  - Customer Gateway ASN: 65120
  - Virtual Private Gateway ASN: 65100
  - Neighbor IP Address: 169.254.10.1

### Information from VPN config file – BGP 2
- **BGP Configuration Options:**
  - Customer Gateway ASN: 65120
  - Virtual Private Gateway ASN: 65100
  - Neighbor IP Address: 169.254.20.1

1. Select the EC-V from the appliance tree.
2. Navigate to **Configuration > Networking > Routing > BGP.**
3. Click the edit icon next to the EdgeConnect appliance. In this example, for Segment select Default because it is the intended segment.

**Note:** The VTI interface is created on the same default segment.

- **Edit**
  - Appliance: ITX2000
  - Segment: Default
  - Peer IP: 169.254.10.1
  - Local Interface: PEER1
  - Peer ASN: 65100
  - Peer State: Up
  - Soft Reset: Checked

4. On the BGP page move the toggle to **enable BGP,** and enter the required details, such as Autonomous System Number, Router ID, and Graceful Restart. Then click **Add** to add BGP Peers.

**Autonomous System Number:** Enter the ASN number for the EC-V.

**Router ID:** Enter the LAN0 or Loopback interface IP.

**Graceful Restart:** Optional, select check box to activate.
5. Enter the information on the BGP peer page to complete BGP peer configuration and click Add.

4. Repeat Step 5 to add another BGP peer by clicking "Add" icon on the BGP page.

When the BGP configuration on one EC-V is complete, you should see the BGP neighborship with a status of "Established" on the BGP page.
6.2.4 Redistributing Routes and ECMP

Now that BGP is established between TGW and the EC-V, you can see how the SD-WAN fabric routes are redistributed to TGW and how the TGW BGP routes are getting redistributed to the SD-WAN fabric.

HA Deployment: Repeat sections 6.2.4a to 6.2.4d for each EC-V appliance that has established BGP sessions with the Transit Gateways.

6.2.4.a Redistributing SD-WAN Fabric Routes to TGW

By default, EdgeConnect appliances send all Local/Static, OSPF, BGP and other SD-WAN fabric routes to TGW. This is controlled by the BGP Outbound route map that is attached to the BGP neighbor under the BGP peer configuration. You can customize the route maps according to your requirements, either by creating a new route map or by modifying an existing route map to allow or deny specific routes based on protocol or subnet prefix.

Navigate to Configuration > Routing > BGP and click the edit icon next to the EC-V appliance. Then edit the BGP peer by clicking the edit icon for the Outbound route map.
6.2.4.b Receiving BGP Routes from TGW

Similarly, the BGP Inbound route map controls what routes are accepted by the EdgeConnect. By default, all BGP routes coming from TGW BGP neighbors are accepted by EdgeConnect appliances. You can further customize by adding rules on the existing route map or attaching a new route map to permit/deny specific subnet prefix or multiple prefixes.

6.2.4.c Redistributing TGW BGP Routes to SD-WAN Fabric

By default, all BGP routes from TGW are sent to the SD-WAN fabric using subnet sharing (an internal route sharing protocol used by EdgeConnect devices). You can customize the subnet share route map to control which routes can be shared with the rest of the SD-WAN fabric including the TGW BGP routes.

1. To view the current route map that controls the subnet sharing with the SD-WAN fabric, navigate to Configuration > Networking > Routing > Routes, then click the edit icon next to the hostname and the Route page opens. This example is on the default segment.

2. For Redistribute route to SD-WAN fabric, click the edit icon to review the rules and ensure that the Match Criteria shows “Source Protocol BGP” and Permit shows “Allow.”

The following figure shows the “default_rmap_to_subsh” route map, which allows BGP routes to be redistributed to the SD-WAN fabric.
6.2.4.d Enabling ECMP

Equal Cost Multi Path (ECMP) allows the traffic to be carried on multiple paths simultaneously when more than one equal cost route to a destination exists on the appliance. ECMP is disabled on the EdgeConnect appliance by default. You can enable ECMP under the Routes tab of the configuration.

**NOTE:** This setting is common for all VRF segments when enabled ECMP is applied to all the VRF segments (if VRF is configured in your environment).

Navigate to **Configuration > Networking > Routing > Routes** and click the edit icon next to the hostname. This example is on the default segment.

![Routes configuration](image-url)
6.2.5 Checking Routes Learned from TGW on EC-V

When the BGP session shows Established on the BGP page (Peers), we can validate if both TGW BGP endpoints are sending routes to EC-V or not.

**HA Deployment:** Repeat steps 1 to 6 for each EC-V appliance that has established a BGP session with the AWS Transit Gateway.

1. Navigate to Configuration > Networking > Routing > Routes and click BGP to view BGP routes only. The following figure shows a route table with routes for both BGP peers (169.254.10.1 and 169.254.20.1), which are the two TGW BGP neighbors configured in Section 6.2.3.

   Note that each route is learned twice because EMCP is enabled on the EC-V. For example, in the following figure, subnet 172.20.44.0/22 is learned from 169.254.10.1 TGW BGP neighbor and as well from 169.254.20.1 TGW BGP neighbor.

2. You must enable ECMP under the Routes tab to see multiple route paths. Refer to Section 6.2.4d to enable ECMP. With ECMP enabled, EdgeConnect is able to send traffic across both the passthrough tunnels.

3. Navigate to Configuration > Networking > Routing > Routes and click BGP to view BGP routes only.

4. Check your inbound route map attached to the BGP neighbor if you don’t see all the routes that are expected to come from TGW. The following figure shows an inbound route map that allows all the BGP routes coming from TGW BGP peers.
6.2.6 Checking Routes from EC-V to TGW

To ensure end-to-end communication from AWS VPCs to the EdgeConnect SD-WAN fabric, you will validate whether the EdgeConnect SD-WAN fabric routes are making it to the TGW route table.

1. On AWS Management Console, navigate to **VPC > Transit gateways** and locate your TGW on the right panel. You can also search for your TGW using the TGW name or ID.

2. Under the Details section, click the **Association route table ID** to display the route table for your TGW.

3. On the Routes tab, you will see all the incoming routes from EdgeConnect BGP peers.

If it is a single EC-V deployment, you must see **2 Attachments** under the Attachment ID column to indicate that routes are received on both of the BGP connections from the single EC-V.

In this example, two EdgeConnect appliances have been integrated with TGW, so you see **4 Attachments** for each route entry because both of the EC-Vs are sending the routes to TGW (each EC-V has 2 BGP neighbourships with TGW).
4. If you do not see your intended SD-WAN fabric routes, check Outbound route map that is attached to each TGW BGP peer on your EdgeConnect. The following figure shows a route map that allows all the SD-WAN fabric routes by default.

This completes the task of verifying routes on TGW coming from EC-V.

**NEXT:** Only for HA EC-V Deployment – Proceed to **Section 7** to configure Redundancy.

**Single EC-V Deployment** - You have successfully completed all the required steps to deploy EC-V in AWS Cloud and integrated it with AWS TGW using GRE Connect method.
7 Redundancy in HA Deployment

When two EC-Vs are deployed in the AWS Cloud, there are two possible solutions to achieve redundancy.

1. Active-Standby Redundancy
2. Active-Active Redundancy

7.1 Active-Standby Redundancy

In Active-Standby failover mode, traffic between the on-premises network and the AWS workloads traverses only through one EC-V. When active EC-V fails and the TGW BGP neighborship goes down, traffic will traverse through the standby EC-V. Active-Standby failover mode is supported on both IPsec integration and on the GRE integration. You can make use of the peer priority feature on the branch side configuration to prefer EC-V-1 as the active and EC-V-2 as the backup. You will also use the well-known BGP AS_PATH attribute on the EC-V configuration to influence routes on TGW to prefer the EC-V-1 with the least AS_PATH count.

7.1.1 Topology:

![Figure 10: Active-Standby HA Deployment with EC-V-1 as Active]
7.1.2 Configure Peer Priority on Remote Appliances

This configuration must be done on the remote branch appliances that will be sending traffic to the AWS region (not on the AWS EC-V itself).

By entering a lower peer priority value for EC-V-1 than for EC-V-2, EC-V-1 will become the active appliance for receiving traffic from a remote EdgeConnect appliance and EC-V-2 will become the standby.

Because peer priority must be configured on the remote branch appliances, you must configure this on more than one appliance in a typical SD-WAN fabric. Aruba recommends using the Template Group Configuration in Orchestrator to push the peer priority to all intended appliances to avoid configuring each individual appliance.

Configuring Peer Priority on Branch appliances using Template Groups:

1. In Orchestrator, navigate to Configuration > Templates & Policies > Templates.
2. If you are already using templates for your branch appliances, you can modify a template to add peer priority to it. Otherwise create a new template and include peer priority during configuration.
3. Click Show All.
4. Drag the Peer Priority template from the Available Templates section to the Active Templates section.
5. Configure EC-V-1 with a lower value (e.g., 10) and EC-V-2 with a higher value (e.g., 20).
6. Click Save to save the template configuration.
7. Select Remote Appliances from the appliance tree and click **Apply Template Groups** (if configured new template group).
7.1.3 Configure AS Path Prepend Count

AS Path attribute is a well-known mandatory attribute in BGP that is present in all prefixes (route-paths) exchanged between BGP neighbors. When any BGP router receives a route path for a single destination with varying AS Path counts, the route path with the least number of AS path count will be preferred.

Figure 11 shows two route paths for the destination 172.16.0.0/24 via next hop 172.16.39 and 172.16.5.20. But the BGP router will prefer the next hop 172.16.1.39 because the AS Path count is 1 compared to 3 AS Path count for the other peer.

![Figure 11: BGP Route path table on a Router](image)

You will use the ASN Prepend Count feature in EdgeConnect to artificially increase the AS Path count only on the standby EC-V, which causes the TGW to prefer the active EC-V. ASN prepend count is configured through the Outbound Redistribution maps. The following section outlines the steps to create a new Outbound Redistribution map and assign it to the BGP peers of the standby EC-V.

**NOTE:** You will NOT modify the ASN prepend count on the active EC-V because you want it to use the default settings.

Before configuring AS path prepend on EC-V-2, check your AWS Transit Gateway route table to see the routes from both the EC-Vs (you should see 4 attachments for each route). Refer to Section 6.2.6.

1. In Orchestrator, select the Standby EC-V from the appliance tree.
2. Navigate to Configuration > Routing > BGP and click the edit icon next to the EC-V. The BGP configuration page opens.

![BGP Configuration](image)

3. Click the edit icon of the first AWS Transit Gateway BGP Peer to modify the peer configuration.
4. On the Update Peer configuration page, click the edit icon next to the Outbound route map.

5. Click **Clone Map** to clone the existing map configuration. Enter a name for the cloned Outbound route map.

6. Modify each row. Click the **ASN Prepend Count** check box and enter 1 in the field.
7. The new Outbound route map with AS path prepend count configured should look like the following figure.

8. Click **Apply** to save the Route map and close the page.

9. On the BGP Peer configuration page, select the newly configured route map under the Outbound route map dropdown.

10. Click **Update** and then click **Save** to complete configuration of the first AWS Transit Gateway BGP peer.

11. Repeat steps 4 through 10 to modify the configuration for the second AWS Transit Gateway peer, and ensure both BGP peers have the same Outbound route map configured.
7.1.4 Checking Routes on TGW

Now that the BGP AS path prepend is modified on the standby EC-V (EC-V-2), you can check the AWS Transit Gateway route table to ensure that it has preferred the routes towards the active EC-V (EC-V-1).

1. On the AWS Management Console navigate to **VPC > Transit gateways** and locate your TGW on the right panel. You can also search for your TGW using the TGW name or ID.

2. Under the Details section, click the **Association route table ID** to display the route table for your TGW.

3. On the Routes tab, you will see all the incoming routes from EdgeConnect BGP peers.

In the following example, the SD-WAN fabric route **172.23.0.5/32** is showing as **2 Attachments**. If you click those either of those two attachments, you will see both are referring to the same Attachment ID (2 x BGP peer towards EC-V1). If you see "4 Attachments" that means the BGP AS path prepend is not configured correctly and you should review **Section 7.1.3**.

---

You have successfully completed all the required steps to deploy HA EC-V in an Active-Standby topology.
7.2 Active-Active Redundancy

Active-Active redundancy mode is appropriate for users who want to use both AWS EC-Vs simultaneously to increase bandwidth for workloads in AWS. Similar to Active-Standby failover mode, Active-Active failover mode is supported on EC-V integration with AWS Transit Gateway either with IPsec integration or with GRE integration.

In the IPsec integration, an IPsec VPN tunnel from the EC-V to the TGW supports up to 1.25 Gbps. As a result, each EC-V can support up to 2.5 Gbps for a total throughput of 5 Gbps to and from the TGW (ECMP must be enabled under the Routes configuration to achieve this throughput).

7.2.1 Topology:

![Figure 12: Active-Active HA Deployment](image-url)
Configuring EC-Vs in Active-Active failover mode is straightforward. Because it requires all BGP path attributes to be identical on each BGP route paths, you will not modify any BGP attributes on the EC-Vs. When a remote EdgeConnect appliance can reach a destination via two separate EdgeConnect tunnels, it randomly selects one tunnel to forward traffic.

Because ECMP (Equal Cost Multi Path) is enabled by default on AWS Transit Gateway, it will send traffic towards both EC-Vs randomly. This may cause asymmetric flows where SD-WAN inbound traffic from remote branch ingresses through EC-V-1, but the return traffic (outbound) may get egressed through EC-V-2 if the TGW chooses to send traffic to EC-V-2 due to the nature of ECMP routing.

Asymmetric flows do not affect a majority of the applications. However, if you have firewalls deployed on the LAN-side of the EC-Vs, asymmetric flows will cause the firewall to drop traffic unless you have specifically allowed such traffic in the firewall. Also, enabling Flow Redirection is mandatory if you enable Boost on the AWS EC-Vs. The Flow Redirection feature helps in scenarios with asymmetric flows by redirecting the flow to a peer EdgeConnect appliance when an appliance only sees one-way traffic.

7.2.2 Enable Flow Redirection

Flow Redirection is configured from the EdgeConnect Appliance Manager. Flow Redirection is not configurable in Orchestrator.

7.2.2.a Configuring Flow Redirection on EC-V-1

1. Open the Appliance Manager Web UI for EC-V-1. From Orchestrator, select the appliance in the appliance tree, right click, and then click Appliance Manager in the drop down.

2. Navigate to Configuration > Flow Redirection and enter these settings on the Flow Redirection page.

   - Enable: Click the check box.
   - Wait time: Enter 50.
   - Interface: Select lan0 from the drop down.

3. Click Add Peer and enter the LAN0 interface IP address for EC-V-2.

4. Click Apply to save the settings. The state will appear as "UNKNOWN" initially until EC-V-2 configuration is complete.
7.2.2.b Configuring Flow Redirection on EC-V-2

1. Open the Appliance Manager Web UI for EC-V-2. From Orchestrator, select the appliance in the appliance tree, right click, and then click Appliance Manager in the drop down.

2. Navigate to Configuration > Flow Redirection and enter these settings on the Flow Redirection page.

   Enable: Click the check box.
   Wait time: Enter 50.
   Interface: Select lan0 from the drop down.

3. Click Add Peer and the LAN0 interface IP address for EC-V-1.

4. Click Apply to save the settings. The state may appear as “UNKNOWN” momentarily before it changes to “OK.”

You have successfully completed all the required steps to deploy HA EC-V in an Active-Active topology.