Contents

Copyright and Trademarks .............................................................................................................. 4
Support ............................................................................................................................................. 5
Related Documentation .................................................................................................................... 6

EdgeConnect Virtual (EC-V) in Microsoft Azure .............................................................................. 7

Single EC-V Deployment with Static Routes .................................................................................. 9
  Prerequisites to Deploying EC-V in Azure ...................................................................................... 10
  Topology – Single EC-V Deployment .............................................................................................. 11
  Create an EC-V Appliance in the Azure Portal ................................................................................ 12
    Prepare the Resource Group ......................................................................................................... 13
      Create a Virtual Network ........................................................................................................... 13
      Create the Subnets ..................................................................................................................... 14
      Create Network Security Groups ............................................................................................... 15
      Create an SSH Private-Public Key Pair ...................................................................................... 18
      Create an EC-V Virtual Machine in Azure .................................................................................. 19
  Configure the EC-V ....................................................................................................................... 24
    Create an EC-V Password ............................................................................................................ 25
    Apply the EC-V Configuration Wizard ....................................................................................... 26
    Verify MGMT0 Interface MAC Address ....................................................................................... 28
    Add the EC-V to the SD-WAN Fabric .......................................................................................... 29
  Create Data Path Interfaces ........................................................................................................... 31
    Create the WAN0 Network Interface on the Azure Portal .............................................................. 32
    Create the LAN0 Network Interface on the Azure Portal .............................................................. 33
    Enable Accelerated Networking on WAN0 and LAN0 Interfaces ............................................... 35
    Assign a Public IP Address to the WAN0 Interface ........................................................................ 38
    Enable IP Forwarding on the LAN0 Network Interface ............................................................... 39
    Attach WAN0 and LAN0 Network Interfaces to the EC-V ............................................................ 40
    Configure the EC-V for In-line Router Mode ................................................................................ 41
  Configure Traffic Redirection Using Static Routes ........................................................................ 43
    Create a Static Route on the Azure Route Table ......................................................................... 44
    Add a Route on the EC-V to Advertise the Workload’s Subnet ...................................................... 46
    Verify end-to-end connectivity ................................................................................................... 47

Single EC-V Deployment with BGP Routing ................................................................................... 48
  Azure Virtual Hub Overview and an EC-V Appliance ................................................................. 49
  Prerequisites to Deploying a Single EC-V Appliance with Azure Virtual Hub from the Azure Portal ............................................................................................................................. 51
  Topology – EC-V Deployment (BGP Routing) .............................................................................. 52
EC-V HA Deployment: Azure Virtual Hub

Azure Virtual Hub Overview and the EC-V HA Architecture .............................................. 54
Prerequisites to Deploying EC-V HA with Azure Virtual Hub from the Azure Portal ........... 57
Topology – EC-V HA Deployment (Azure Virtual Hub) .................................................. 58
  Assign a Public IP Address to the LAN0 Interface ......................................................... 59
  Creating an Azure Virtual Hub in an EC-V HA Architecture ........................................... 61
  Create an Azure Virtual WAN (VWAN) Hub ................................................................. 62
    Create the VWAN .......................................................................................................... 62
    Create the Virtual Hub ................................................................................................... 62
  Create the VPN Sites ........................................................................................................ 64
  Create the Virtual Network Connections ....................................................................... 67
  Download the Virtual Hub’s VPN Configuration File ..................................................... 68
Traffic Redirection in the HA Deployment (Azure Virtual Hub) ............................................. 70
  Create IPsec Tunnels from the EC-Vs to the Azure Virtual Hub ........................................ 71
  Create a Loopback Interface on an EC-V ......................................................................... 74
  Create VTls on the EC-Vs .................................................................................................. 75
  Create Static Routes on the EC-Vs .................................................................................... 77
  Configure BGP Sessions on EC-V ..................................................................................... 80
  Configure EC-V Failover mode ......................................................................................... 84
    Configure EC-V in Active-Standby failover mode ......................................................... 84
    Configure EC-Vs in Active-Active failover mode ............................................................ 89
  Enable Flow Redirection .................................................................................................. 90

EC-V HA Deployment: Azure Internal Load Balancer .......................................................... 92

Azure Load Balancer and the EC-V Architecture ................................................................ 93
Prerequisites to Deploying EC-V with Azure Standard Internal Load Balancer .................. 95
Topology – EC-V Deployment (Azure ILB) ......................................................................... 96
Create an Azure Standard ILB in an EC-V Architecture .................................................... 98
  Create an Azure Standard Internal Load Balancer ......................................................... 99
  Create a Backend Pool ..................................................................................................... 101
  Create a Health Probe ...................................................................................................... 102
  Create a Load Balancing Rule ......................................................................................... 103
  Verify the IP address of the Internal Load Balancer ....................................................... 105
Health Probe Traffic in the HA Deployment (Azure ILB) .................................................... 106
  Create a Static Route on the EC-V for Health Probe Traffic ............................................ 107
  Verify Health Probe Responses using tcpdump (Optional) ............................................. 109
Traffic Redirection in the HA Deployment (Azure ILB) ....................................................... 110
  Create a Virtual Network Peering Session ...................................................................... 111
  Create an Azure Route Table ......................................................................................... 112
  Associate the Workloads Subnet to the Route Table ...................................................... 113
  Create a Static Route to Forward Traffic to the ILB ....................................................... 114
  Create Static Routes to Advertise Azure Subnets to Remote EdgeConnect Devices ....... 115
  Enable Flow Redirection on the EC-V ............................................................................ 117
Copyright and Trademarks

Silver Peak EdgeConnect Virtual (EC-V) in Microsoft Azure Deployment Guide

Date: September 2022

Copyright © 2021 Silver Peak Systems, Inc. All rights reserved. Information in this document is subject to change at any time. Use of this documentation is restricted as specified in the End User License Agreement. No part of this documentation can be reproduced, except as noted in the End User License Agreement, in whole or in part, without the written consent of Silver Peak Systems, Inc.

Trademark Notification

Silver Peak, the Silver Peak logo, and all Silver Peak product names, logos, and brands are trademarks or registered trademarks of Silver Peak Systems, Inc. in the United States and/or other countries. All other product names, logos, and brands are property of their respective owners.

Warranties and Disclaimers

THIS DOCUMENTATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SILVER PEAK SYSTEMS, INC. ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THIS DOCUMENTATION OR OTHER DOCUMENTS WHICH ARE REFERENCED BY OR LINKED TO THIS DOCUMENTATION. REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL SILVER PEAK SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENTATION. THIS DOCUMENTATION MAY INCLUDE TECHNICAL OR OTHER INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE DOCUMENTATION. SILVER PEAK SYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENTATION AT ANY TIME.

Silver Peak Systems, Inc.
2860 De La Cruz Boulevard
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support
Support

For product and technical support, contact Silver Peak Systems at either of the following:

1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com/support

We’re dedicated to continually improving the usability of our products and documentation.

- If you have suggestions or feedback for our documentation, send an e-mail to techpubs@silver-peak.com.
- If you have comments or feedback about the interface, send an e-mail to usability@silver-peak.com.
Related Documentation

- **Release Notes** provide information on new software features, system bugs, and software compatibility.

- All user documentation is available at [https://www.silver-peak.com/support/user-documentation](https://www.silver-peak.com/support/user-documentation).
EdgeConnect Virtual (EC-V) in Microsoft Azure

A Silver Peak EdgeConnect Virtual (EC-V) appliance can be deployed in Microsoft Azure to establish and enhance WAN connectivity as well as accelerate data migration from branch offices and data centers to Azure. Your EC-V appliance can be created and launched from the Azure Marketplace using a Bring Your Own License (BYOL) model. An EC-V can be deployed as a single Virtual Machine (VM) or in a High Availability configuration.

Single Appliance Deployments
The following EC-V single appliance deployment instructions are provided:

- Deployment of a single appliance, using static routes on the Azure virtual network route table:
  
  **Use case:** Single appliance deployment using static routing
  
  **Deployment Guide link:** Single EC-V Deployment with Static Routes

- Single EC-V Deployment with BGP Routing
  
  **Use case:** Single appliance deployment using BGP to redirect traffic to the EC-V
  
  **Deployment Guide link:** Single EC-V Deployment with BGP Routing

HA Appliance Deployments
Microsoft offers two distinct Azure-native services for deploying EC-Vs horizontally to increase availability of cloud-based workloads:

- Azure Virtual WAN Hub (referenced in this guide as *Azure Virtual Hub*)
- Azure Standard Internal Load Balancer (ILB)

Each Azure-native service has advantages and disadvantages that are discussed in their respective chapters. Before implementing an HA appliance deployment, we recommend reading both deployment models and selecting the model most appropriate for your environment.

The following HA appliance deployment instructions are provided:

- High Availability Deployment of two appliances using BGP and the Azure Virtual Hub:
  
  **Use case:** HA deployment of two appliances using BGP routing
  
  **Deployment Guide link:** EC-V HA Deployment: Azure Virtual Hub

- High Availability Deployment of two appliances using static routes and the Azure Standard ILB:
  
  **Use case:** HA deployment of multiple appliances using static routing
  
  **Deployment Guide link:** EC-V HA Deployment: Azure Internal Load Balancer

The deployment procedures in this guide can be modified to create custom EC-V Azure deployments.
Guide Structure

Because several procedures in this guide are used by multiple use cases, instructions and hyperlinks are provided after each procedure to guide you to the next procedure 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.
Single EC-V Deployment with Static Routes

Background Topics
The following topics provide information about implementing a single EC-V appliance in Azure.
- Prerequisites to Deploying EC-V in Azure on the next page

Configuration Topics
The following procedures implement the EC-V deployment depicted in Figure 1. These procedures can be modified to deploy any single EC-V appliance architecture with static routes.

1. Review your topology and assemble the required information. (Topology – Single EC-V Deployment on page 11).

2. Repeat Steps A through C for each EC-V appliance to be deployed:
   A. Create an EC-V Appliance in the Azure Portal on page 12
   B. Configure the EC-V on page 24
   C. Create Data Path Interfaces on page 31

3. Configure traffic redirection (Configure Traffic Redirection Using Static Routes on page 43)

Use the following list to determine your next topic:
- To review background information first: Prerequisites to Deploying EC-V in Azure on the next page
- To begin configuration immediately: Topology – Single EC-V Deployment on page 11

First Step: Proceed to your selected section
Prerequisites to Deploying EC-V in Azure

- A current Azure account
- Silver Peak Orchestrator
- Silver Peak EdgeConnect-Virtual appliance licenses
  The Azure Marketplace may offer various EdgeConnect OS versions when you create a virtual machine that implements an EC-V appliance. However, the available option may be lower than your desired version.
  Upon deploying and accessing an EC-V, Orchestrator provides an upgrade option that accesses the most recent OS versions. The upgrade takes only a few minutes. You are also provided an upgrade option upon initially accessing the EC-V through the Appliance Manager.
- Ensure you have an existing Virtual Network in Azure
- EC-V deployments illustrated in this guide assume there are no pre-existing site-to-site VPN or ExpressRoute links between the Azure virtual network and the on-premises network. In this case, assign a public IP address on **WAN0** and **MGMT0** interfaces to access the EC-V remotely.
  If you have a previously configured site-to-site VPN or an ExpressRoute link between your virtual network and the on-premises network, it is not required to assign a public IP address on the MGMT0 interface of the EC-V to access the EC-V via one of those links.
- If you do not want to assign a separate public IP for MGMT0 interface, you may deploy the Azure Bastion service to connect to the EC-V from the MGMT0 interface when it is first deployed.
  Visit the following page to learn more about the Azure Bastion service:
  
  https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

  This guide does not use Azure Bastion. Instead, a public IP is assigned to the MGMT0 interface to access EdgeConnect appliances via SSH and HTTPS when they are deployed for the first time.

**First Step: Proceed to Topology – Single EC-V Deployment on the next page**
Topology – Single EC-V Deployment

Figure 1 shows a logical topology of a basic EC-V deployment in Azure. The Azure workloads in the topology are deployed in the same virtual network as the EC-V appliance.

Figure 1. Logical topology of a Single EC-V deployment in Azure

The instructions in this section of the guide assume that your Azure workloads are deployed on the same virtual network as the EC-V appliance.

You can deploy the EC-V appliance in a different virtual network from the Azure workloads. Deploying an EC-V appliance in this manner, requires a Virtual Network Peering session between your workloads virtual network and the EC-V appliance virtual network. To learn about how to set up virtual network peering, access https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview.

Before starting the deployment process, assemble the following information:

- **Azure account**: Username and password that accesses your Azure account
- **Azure Resource Group**: Name of the resource group
- **EdgeConnect license details**: Account name and Account key – received from Silver Peak

First Step: Proceed to Prepare the Resource Group on page 13
Create an EC-V Appliance in the Azure Portal

The following tasks configure an existing resource group that meets the requirements for an EC-V deployment and configures a virtual machine as an EC-V appliance.

The following sections provide the required configuration steps:

- Prepare the Resource Group on the next page
- Create an EC-V Virtual Machine in Azure on page 19
Prepare the Resource Group

The following instructions prepare the resource group to create the EC-V virtual machine. Tasks include:

- Create a Virtual Network
- Create the Subnets
- Create Network Security Groups
- Create an SSH Private-Public Key Pair

Prerequisites include an Azure Network Security Group, to which you have creation rights, and access to a program that creates an SSH Key pair. The example in this section uses PuTTygen to create the keys.

*You may use any existing virtual network (including its subnets and Network Security Groups) and SSH key pair that meet EC-V deployment requirements. This guide provides instruction to create all resources required for the EC-V.*

Create a Virtual Network

These steps create a virtual network. If your desired virtual network exists, proceed to Create the Subnets.

1. Log on to the Azure Portal and navigate to your Resource Group.
2. Click +Create in the menu bar.
3. Begin entering Virtual Network in the search field, then select Virtual Network in the drop-down menu to open the Virtual Network page.
4. Click Create to open the Create virtual network page.
5. Verify that Basics is selected in the menu bar and enter settings from the following list:
   - Subscription: (drop-down) Depends on your Azure account. Guide example is Pay-As-You-Go
   - Resource Group: (drop-down) Select your Resource Group. Guide example is SP-Tech
   - Name: Enter the label for the new virtual network. Guide example is vn_ECV
   - Region: (drop-down) Select the region that you want to deploy the EC-V. Guide example is (US) West US
6. Click Next: IP Addresses (bottom of page) and proceed to Create the Subnets.
Create the Subnets

These steps assign an address space to the virtual network and create four subnets that correspond to MGMT0, LAN0, WAN0, and Workloads subnets in Figure 1.

The virtual network selected for an EC-V deployment requires at least two subnets for WAN0 and LAN0 interfaces. Although optional, we recommend creating a separate MGMT0 interface and deploying it on a separate subnet from the WAN and LAN subnets. The guide implementation uses three subnets.

1. Select **IP Addresses** in the Create virtual network menu bar.
2. In the IPv4 address space field, enter an IP address space (CIDR notation) that will include the address spaces of the four subnets.
   - If a CIDR range already appears in the IPv4 address space field, remove the field contents and enter your preferred CIDR range.
   - Guide example is **10.6.0.0/16**
3. For each subnet, perform the following:
   - Click +Add subnet to open the Add Subnet dialog
   - In the Subnet name field, enter a descriptive name for the subnet
   - In the Subnet address range, enter an address space (CIDR notation)
   - In the NAT Gateway, select None
   - In the Service Endpoints, select 0 Selected
   - Click the Add button
   - Guide examples include:
     ```
     sub_MGMT0 - 10.6.1.0/24  
     sub_WAN0 - 10.6.2.0/24  
     sub_LAN0 - 10.6.3.0/24  
     sub_WKLD - 10.6.4.0/24  
     ```
4. Click Review + create at the bottom of the page.
   - Azure displays the Create virtual network page. Proceed when the green Validation passed bar appears at the top of the page.
5. Click the Create button at the bottom of the page.
   - When the Overview page displays Your Deployment is complete, proceed.
Create Network Security Groups

Network security groups (NSG) are required when creating the WAN and LAN interfaces on the Azure portal. The MGMT0 interface's NSG is created automatically when deploying the EC-V. Therefore, it is not created in this procedure.

These instructions create the WAN0 Network Security Group:

1. Navigate to your Resource group and click the **Create** button in the menu bar.
2. Use the search field to select **Network Security Group** in the drop-down menu to open the **Network Security Group** page.
3. Click the **Create** button to open the **Create Network Security Group** page.
4. Verify that **Basics** is selected in the menu bar and enter settings from the following list:
   - **Subscription**: (drop-down) Depends on your Azure account. Guide example is **Pay-As-You-Go**
   - **Resource Group**: (drop-down) Select your Resource Group. Guide example is **SP-Tech**
   - **Name**: Enter the label for the new WAN0 NSG. Guide example is **nsg_WAN0**
   - **Region**: (drop-down) Select the region where your EC-V will be created. Guide example is **(US) West US**
5. Click **Review + create** at the bottom of the page. Proceed when the **Create network security group** page displays a green **Validation passed** bar at the top of the page.
6. Click **Create** at the bottom of the page. Proceed when the **Overview** page displays **Your Deployment is complete**.
7. Click **Go to resource**.
   The **nsg_WAN0** page opens
8. Click **Inbound security rules** in the **Settings** menu list.
9. Click **Add** in the button bar to open the **Add inbound security rule** dialog.
10. In the **Add inbound security rule** panel (right side of page), enter the following settings:
    - **Source**: (drop-down) Select **Any**
    - **Source port ranges**: Enter *
    - **Destination**: (drop-down) Select **Any**
    - **Service**: Select **Custom**
    - **Destination port ranges**: Enter *
    - **Protocol**: Select **Any**
- **Action:** Select *Allow*
- **Priority:** Enter *100*
- **Name:** Enter descriptive name. Guide example is *Allow_All_Inbound*
  
  This example allows all inbound traffic because Firewall Mode is set to Stateful+SNAT when the WAN interface of the EC-V is configured through Silver Peak software later in this guide.
  
  Do not allow all inbound traffic on the NSG if you plan to set the EC-V's WAN interface firewall mode (on the Deployment page) to *Allow All*.

11. Click *Add* at the bottom of the dialog.

12. Click *Outbound security rules* in the *Settings* menu list.

13. Click *+Add* in the button bar.

14. In the *Add outbound security rule* panel (right side of page), enter the following settings:
   - **Source:** (drop-down) Select *Any*
   - **Source port ranges:** Enter *
   - **Destination:** (drop-down) Select *Any*
   - **Service:** Select *Custom*
   - **Destination port ranges:** Enter *
   - **Protocol:** Select *Any*
   - **Action:** Select *Allow*
   - **Priority:** Enter *100*
   - **Name:** Enter descriptive name. Guide example is *Allow_All_Outbound*

15. Click *Add* at the bottom of the dialog.

These instructions create the LAN0 Network Security Group:

1. Navigate to your Resource group and click the *+Create* button in the menu bar.
2. Use the search field to select *Network Security Group* in the drop-down menu to open the *Network Security Group* page.
3. Click the *Create* button to open the *Create Network Security Group* page.
4. Verify that *Basics* is selected in the menu bar and enter settings from the following list:
   - **Subscription:** (drop-down) Depends on your Azure account. Guide example is *Pay-As-You-Go*
   - **Resource Group:** (drop-down) Select your Resource Group. Guide example is *SP-Tech*
   - **Name:** Enter the label for the new LAN0 NSG. Guide example is *nsg_LAN0*
- **Region**: (drop-down) Select the region where your EC-V will be created. Guide example is *(US) West US*

5. Click **Review + create** at the bottom of the page. Proceed when the **Create network security group** page displays a green **Validation passed** bar at the top of the page.

6. Click **Create** at the bottom of the page. Proceed when the **Overview** page displays **Your Deployment is complete**.

7. Click **Go to resource**. The **nsg_LAN0** page opens.

8. Click **Inbound security rules** in the **Settings** menu list.

9. Click **+Add** in the button bar.

10. In the **Add inbound security rule** panel (right side of page), enter the following settings:
   - **Source**: (drop-down) Select **IP Addresses**
   - **Source IP Addresses/CIDR ranges**: Enter **10.6.0.0/16**
   - **Source port ranges**: Enter *
   - **Destination**: (drop-down) Select **Any**
   - **Service**: Select **Custom**
   - **Destination port ranges**: Enter *
   - **Protocol**: Select **Any**
   - **Action**: Select **Allow**
   - **Priority**: Enter **100**
   - **Name**: Enter descriptive name. Guide example is **Allow All Inbound**

Only allow inbound traffic from Azure virtual network CIDR address ranges. We strongly recommend not allowing all inbound traffic (0.0.0.0/0) on the LAN0 NSG whether or not a public IP address is assigned to the LAN0 interface.

For the single EC-V deployment with static routes, a public IP address is not assigned to the LAN0 interface.

For EC-V deployments with an Azure Virtual Hub, the LAN0 interface requires a public IP address to be assigned.

11. Click **Add** at the bottom of the page.

12. Click **Outbound security rules** in the **Settings** menu list.

13. Click **+Add** in the button bar.

14. In the **Add outbound security rule** panel (right side of page), enter the following settings:
   - **Source**: (drop-down) Select **Any**
   - **Source port ranges**: Enter *
- **Destination**: (drop-down) Select *Any*
- **Service**: Select *Custom*
- **Destination port ranges**: Enter *
- **Protocol**: Select *Any*
- **Action**: Select *Allow*
- **Priority**: Enter 100
- **Name**: Enter descriptive name. Guide example is *Allow_All_Outbound*

It is safe to allow inbound traffic on the LAN interface. It is not assigned a public IP address, resulting in only workloads in your Azure environment sending traffic to the LAN0 interface.

15. Click **Add** at the bottom of the page.

**Create an SSH Private-Public Key Pair**

PuTTyGen can be used to create the Private-Public key pair. To create a key pair, click the **Generate** button, follow the instructions on the app, then save the private key to an accessible location.

**Next Step: Proceed to Create an EC-V Virtual Machine in Azure on the next page**
Create an EC-V Virtual Machine in Azure

The following procedure utilizes an Azure Virtual Machine wizard to configure an EC-V appliance.

1. From the Azure portal, navigate to your Resource group and click +Create in the menu bar.
2. Use the search field to select *Silver Peak Unity EdgeConnect* in the drop-down menu to open the *Silver Peak Unity EdgeConnect* page.
3. In the *Select a software plan* drop-down, select an EdgeConnect version, then click *Create*. Unless otherwise instructed, select the most recent software version.

The *Create Virtual Machine* page displays configuration options. The menu bar at the top of the page accesses the multiple pages that configures the virtual machine.

*Figure 2. Create virtual machine page - Basics*

4. Select **Basics** in the menu bar and enter the settings from the following list.
   - **Subscription**: (drop-down) Depends on your Azure account. Guide example is *Pay-As-You-Go*
   - **Resource group**: (drop-down) Select your resource group.
   - **Virtual machine name**: Enter a descriptive name for your EC-V. Guide example is *vm-ECV*
   - **Region**: Select the Azure region to deploy your EC-V.
   - **Availability options**: Selection depends on whether your deployment is a single EC-V deployment or an HA EC-V deployment.
     - **Single EC-V Deployment**: Select *No infrastructure redundancy required.*
     - **HA EC-V Deployment**: Select *Availability Zone* and select unique availability zones (AZ) for each EC-V.
       Use a different AZ for each EC-V to ensure that EC-Vs in other AZs continue, when one EC-V fails due to an AZ failure. When deploying multiple EC-Vs in a region that does not support AZs, place all EC-Vs in a single Availability Set. An Availability Set ensures that deployed EC-Vs are distributed in a cluster across multiple, isolated hardware nodes to protect against Azure hardware failures.
   - **Security**: Select *Standard*
- **Image**: Select the latest EdgeConnect image.
- **Run with Azure Spot discount**: (Selection Box) **Clear** (default value).
- **Size**: The size should match the WAN bandwidth and number of interfaces required on the EC-V. Guide example is **Standard DS3_v2**.

The list of recommended instance types for EC-V is available at the following linked location: **EC-V Host Requirements Guide**.

- **Authentication type**: Select **SSH public key**.

The private key associated with the public key entered here is required to log in to the appliance from your SSH client.

**IMPORTANT** EC-V does not support password-based authentication in Azure.

- **Username**: Enter any valid username except **admin**.

The username entered here is used only on Azure to complete the **Basic** page. The username **admin** is used to log into the EC-V via SSH or HTTPS.

Guide example is **azureuser**

- **SSH public key source**: (drop-down) Select [**Use existing public key**]

EdgeConnect does not support **Generate new key pair or Use existing key stored in Azure** options.

- **SSH public key**: Enter a single-line SSH public key.

**IMPORTANT** Best practice for entering a public key is to open the application that created the key pair, use the private key to re-generate public key, then copy it directly from the application into Azure. Saving the private key to a text file and then copying that file into Azure may introduce another text line, causing the appliance to reject the key.

As shown in **Figure 3**, use a single-line public key. Do Not use a multi-line public key.

**Figure 3. Retrieving the Public Key**
5. Select **Disks** in the menu bar and enter the following setting.

- **OS disk type**: Select **Standard SSD** or **Premium SSD**.
- **Encryption type**: Select *(Default) Encryption at-rest with a platform-managed key.*
- **Enable Ultra Disk Compatibility**: Select *(Default) Clear.*

6. Select **Networking** in the menu bar and enter the settings from the following list.

- **Virtual Network**: (drop-down) Select the virtual network created in **Prepare the Resource Group**.
  Guide example is *vn_ECV*
- **Subnet**: Select a subnet to deploy the **MGMT0** interface.
  We add WAN0 and LAN0 interfaces on the EC-V after the appliance is created and discovered in the Orchestrator.
  Guide example is *sub_MGMT0 (10.6.1.0/24)*
- **Public IP**: Click **Create New** (below the drop-down field) and enter the following in the **Create public IP address** dialog on the right side of the page:
  - **Name**: Enter a descriptive name. Guide example is *ip_PUBLIC*
  - **SKU**: (radio button) Select **Standard**.
  - **Assignment**: Options not available when SKU is set to **Standard**
    Microsoft recommends using Standard SKU public IP addresses. They are zone-redundant by default and work with the Standard SKU Load Balancer.
  - **Routing preference**: Select your preferred routing option.
  - **Availability zone**: Select **Zone-redundant**.
- **NIC network security group**: Select **Advanced**
- **Configure network security group**: We strongly recommend tightening security rules to allow incoming traffic from only your network. After approving the EC-V on Orchestrator, you can block inbound access to the **MGMT0** interface.
  **IMPORTANT** DO NOT USE the NSGs created in **Prepare the Resource Group**– they are created specifically for the WAN0 and LAN0 interfaces.
  Guide example is *(new) vm-ECV-nsg*
- **Accelerated networking**: (Selection box) **Mark**
  This parameter is locked *(cleared)* for instance types that do not support Accelerated Networking.
- Place this virtual machine behind an existing load balancing solution?: (Selection box) Clear

7. Select Management in the menu bar and enter the settings in the following list.
   - Boot Diagnostics: Select Enable with managed storage account (recommended)
   - Enable OS guest diagnostics (Selection box): Clear (off)
   - System assigned managed identity: Clear (off)
   - Login with Azure AD (Preview): Clear (off)
   - Enable auto-shutdown: Clear (off)
   - Patch Orchestration options: Select image default

8. Select Advanced in the menu bar. All default settings on this page are acceptable.

9. Select Tags in the menu bar. All default settings on this page are acceptable.

10. Click Review+create at the bottom of the page.
    Proceed when the Create a virtual machine displays a green Validation passed bar.

11. Enter a Preferred e-mail address, a Preferred phone number, and click Create.
    The Azure Dashboard appears as the EC-V begins to deploy.

12. To view the progress of the VM deployment:
    - Monitor the Resource Group you created earlier by clicking Resource Groups.
    - Select the name of the Resource Group selected for the EC-V
    - Allow a couple of minutes for the virtual machine (EC-V) to appear.

Figure 4 displays the resources in your Resource Group after the VM is created successfully.

Figure 4. Displayed resources related to the EC-V
Next Step: Proceed to Create an EC-V Password on page 25
Configure the EC-V

The following sections provide the required login and configuration steps:

- Create an EC-V Password
- Apply the EC-V Configuration Wizard
- Verify MGMT0 Interface MAC Address
- Add the EC-V to the SD-WAN Fabric
Create an EC-V Password

This section creates the admin password for logging into the EC-V’s Appliance Manager. The EC-V does not have a default password, which is required to access the Appliance Manager.

The following steps create a password for the EC-V by logging into its Command Line Interface (CLI).

1. Locate the public IP address of the MGMT0 interface from the Virtual Machine page (Figure 5).

   Figure 5. Locate the EC-V’s public IP address

   ![Figure 5](image)

2. Open your preferred SSH client. (PuTTY is used throughout this guide to illustrate examples).

3. Enter the EC-V public IP address as the Host Name (or IP Address).

4. Navigate to **Connection: SSH: Auth**, and click **Browse**.

5. Select the private (.ppk) key file associated with the public key you entered on the Azure console.
   (If you use a Linux-based operating system, use the .pem file to log in via SSH.)

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

7. If prompted, click **Yes** to add the key to the PuTTY's cache.

8. When you connect to the CLI of the EC-V, login as username **admin**.

9. Create a secure password for the admin user on the EC-V by entering the following:
   - `enable [Enter]`
   - `configure terminal [Enter]`
   - `username admin password <enter_a_new_password> [Enter]`

**Next Step: Proceed to Apply the EC-V Configuration Wizard on the next page**
Apply the EC-V Configuration Wizard

These steps log into the EC-V Appliance Manager and configure the EC-V with the Configuration Wizard.

The initial access into the Appliance Manager opens the Configuration Wizard. To access the Configuration Wizard after the initial configuration, click **Configuration: Initial Config Wizard**.

1. Enter `https://<MGMT0_public_IP>` in a web browser, using the address noted in Step 1 of Create an EC-V Password as the MGMT Public IP. Guide example is **137.135.44.198**. The **Appliance Manager** Login page opens.

2. Enter the following to login into the Appliance Manager:

   **Username**: admin. Do not enter the username created in the Azure Portal.

   **Password**: Enter the new password.

   The Appliance Manager opens to the **Configuration Wizard**. The menu bar of the Configuration Wizard is shown in **Figure 6**.

   **Figure 6. Configuration Wizard**

3. Click **Next** on the Welcome page.

   The **Hostname, DHCP, DNS** page opens.

4. Enter an **Appliance Hostname** and **Primary DNS IP**. Click **Apply & Next**.

   The **License and Registration** page opens.

5. Enter the **Account Name** and **Account Key**. Click **Apply & Next**.

   The **Deployment Mode** page opens.

6. Leave the default settings unchanged. Click **Apply & Next**.

   Deployment mode is changed from **Server** to **Router** when network interfaces are added later from the Azure Portal. Until then, keep the deployment mode as **Server**.

   The **Tunnels to Peer** page opens.

7. Select the **Use Shared subnet information** check box. Click **Apply & Next**.

   The **Date & Time** page opens.
8. Set the Time Zone. Click **Apply & Next**.
   The **Change Password** page opens.

9. As you already created a password via SSH, click **Apply & Next**.
   The **Finish** page opens.

10. Click **Done**.

11. Click the **Save Changes** button in the top banner, if it is visible.

**Next Step: Proceed to Verify MGMT0 Interface MAC Address on the next page**
Verify MGMT0 Interface MAC Address

Complete the following steps in the EC-V Appliance Manager to verify MGMT0 interface settings.

1. Open the **Interface** page by selecting **Configuration > System and Networking > Interfaces** from the menu bar (Figure 7).

   **Figure 7. Navigating to the Interfaces page**

   ![Navigation to Interfaces Page](image)

2. When the **Interfaces** page opens, note that the MAC address and IP addresses are properly assigned on the MGMT0 interface (Figure 8).

   **Figure 8. Verify MAC and IP Addresses**

   ![Verify MAC and IP Addresses](image)

   Next Step: Proceed to **Add the EC-V to the SD-WAN Fabric on the next page**
Add the EC-V to the SD-WAN Fabric

After an EC-V device is configured (Apply the EC-V Configuration Wizard), it communicates with the Silver Peak Cloud Portal to coordinate it with your network. Orchestrator then displays the EC-V as a new appliance that is ready for addition to the SD-WAN fabric. Add an EC-V device to the SD-WAN fabric by using the Appliance Setup wizard to approve the device on Orchestrator.

Complete the following steps to add the EC-V to your SD-WAN fabric.

1. Log on to Orchestrator.
2. Click Appliances Discovered (Figure 9).

   Figure 9. Orchestrator page – Appliances Discovered button

3. From the Discovered Devices screen, click Approve for the EC-V device being configured. The device’s Appliance Setup wizard's page 1 opens. Figure 10 displays the wizard's menu bar.

   Figure 10. Appliance Setup Wizard Menu Bar

4. From the Appliance Setup [1] wizard screen (Figure 10):
   - Complete the Appliance Setup details to select the upgrade version.
     (HA EC-V Deployment) – To deploy multiple EC-Vs in a single region for redundancy, enter an identical Site Name on each EC-V. Orchestrator does not create underlays between EC-Vs with identical Site Names. Multiple EC-Vs deployed for redundancy in the same Azure region should not be connected by underlays.
   - Click Next to open Page 2, which includes an option to select a Deployment profile.

5. From the Appliance Setup [2] wizard screen:
Select a deployment profile or skip.
Click Next to open Page 3, which includes an option to add Loopback Interfaces.

6. From the Appliance Setup [3] wizard screen:
Click Next to open Page 4, which includes an option to add Local Routes.

7. From the Appliance Setup [4] wizard screen:
- Check the Use shared subnet information check box.
- Clear the Automatically include local subnets check box.
- Click Next to open Page 5, which provides an option to add Business Intent Overlays.

8. From the Appliance Setup [5] wizard screen:
Click Apply.
Business Intent Overlays and Template Groups are typically configured after the EC-V is fully provisioned.

After the configuration is applied successfully, the Appliance Wizard displays status similar to that shown in Figure 11.

**Figure 11. Applying Configuration**

9. Click Close after you review the status panel.

**Next Step:** Proceed to Create the WAN0 Network Interface on the Azure Portal on page 32
Create Data Path Interfaces

After creating the EC-V and accessing it through Orchestrator, the next task is configuring data path interfaces. The following tasks create the data path interfaces:

- Create the WAN0 Network Interface on the Azure Portal
- Create the LAN0 Network Interface on the Azure Portal
- Enable Accelerated Networking on WAN0 and LAN0 Interfaces
- Assign a Public IP Address to the WAN0 Interface
- Enable IP Forwarding on the LAN0 Network Interface
- Attach WAN0 and LAN0 Network Interfaces to the EC-V
- Configure the EC-V for In-line Router Mode
Create the WAN0 Network Interface on the Azure Portal

The following steps create and assign a **WAN0** network interface on the Azure portal.

1. From the Azure portal, navigate to your Resource group and click **+Create** in the menu bar.

2. Use the search field to select **network interface** in the drop-down menu, then click **Create** to open the **Create Network Interface** page.

3. Enter **Create Network Interface** field settings, using the following list:
   - **Subscription**: (drop-down) Depends on your Azure account. Guide example is **Pay-As-You-Go**
   - **Resource group**: (drop-down) Select your resource group.
   - **Name**: Enter a descriptive name for the WAN0 interface. Guide example is **ni_WAN0**
   - **Region**: Select the region where you deployed the EC-V. Guide example is **(US) West US**
   - **Virtual Network**: (drop-down) Select the virtual network where you deployed the EC-V. Guide example is **vn_ECV**
   - **Subnet**: (drop-down) Select the WAN0 subnet. Guide example is **vn_ECV/sub_wan0 (10.6.2.0/24)**
   - **Private IP address assignment**: Select **Static**
   - **Private IP address**: Enter an IP address belonging to the WAN0 subnet address space. In HA deployments, each appliance must have a different IP address. Guide example (single appliance deployment) is **10.6.2.10** Guide example (HA deployment – ECV-A) is **10.6.2.10** Guide example (HA deployment – ECV-B) is **10.6.2.11**
   - **Network security group**: (drop-down) Select the WAN0 NSG created in **Prepare the Resource Group**. Guide example is **nsg_WAN0**
   - **Private IP address (IPv6)**: (selection box): **Clear** (default value).

4. Click **Review + Create**. Azure displays the **Create network interface** page. Proceed when the green **Validation passed** bar appears at the top of the page.

5. Click the **Create** button at the bottom of the page. Proceed when the **Overview** page displays **Your Deployment is complete**.

**Next Step**: Proceed to **Create the LAN0 Network Interface on the Azure Portal on the next page**
Create the LAN0 Network Interface on the Azure Portal

The following steps create and assign a LAN0 network interface on the Azure Portal.

1. From the Azure portal, navigate to your Resource group and click +Create in the menu bar.

2. Use the search field to select network interface in the drop-down menu, then click Create to open the Create Network Interface page.

3. Enter Create Network Interface field settings, using the following list:
   - **Subscription**: (drop-down) Depends on your Azure account.
     Guide example is Pay-As-You-Go
   - **Resource group**: (drop-down) Select your resource group.
   - **Name**: Enter a descriptive name for the LAN0 interface.
     Guide example is ni_LAN0
   - **Virtual Network**: (drop-down) Select the virtual network where you deployed the EC-V.
     Guide example is vn_ECV-1A
   - **Subnet**: (drop-down) Select the LAN0 subnet.
     Guide example is vn_ECV/sub_lan0 (10.6.3.0/24)
   - **Private IP address assignment**: Select Static
   - **Private IP address**: Enter an IP address belonging to the LAN0 subnet address space.
     In HA deployments, each appliance must have a different IP address.
     Guide example (single appliance deployment) is 10.6.3.10
     Guide example (HA deployment – ECV-A) is 10.6.3.10
     Guide example (HA deployment – ECV-B) is 10.6.3.11
   - **Network security group**: (drop-down) Select the LAN0 NSG created in Prepare the Resource Group.
     Guide example is nsg_LAN0
   - **Private IP address (IPv6)**: (selection box): Clear (default value).

4. Click Review + Create.

   Azure displays the Create network interface page. Proceed when the green Validation passed bar appears at the top of the page.

5. Click the Create button at the bottom of the page.

   Proceed when the Overview page displays Your Deployment is complete.
6. Open the **Resource Group** page to review your resources (Figure 12). Verify the Network Interfaces and Network Security Groups are added successfully.

**Figure 12. Verify Network Interfaces and Network Security Groups**

![Network Interfaces and Network Security Groups Table]

Next Step: Proceed to **Enable Accelerated Networking on WAN0 and LAN0 Interfaces on the next page**
Enable Accelerated Networking on WAN0 and LAN0 Interfaces

Accelerated Networking, also known as Single Root I/O Virtualization (SR-IOV), improves networking performance on an EC-V appliance. When a network interface is created from the Azure Portal, Accelerated Networking is disabled by default on the new network interface. As of February 2020, Accelerated Networking-enabled network interfaces cannot be created from the Azure Portal.

This procedure enables Accelerated Networking through CLI commands on the Azure Portal Cloud Shell.

Opening the Azure Cloud Shell

1. Click the Cloud Shell icon on the right side of the menu bar to open the Cloud Shell (Figure 13).

   *Figure 13. Cloud Shell icon*

2. Verify that Bash is selected on the Cloud Shell dropdown menu (Figure 14).

   *Figure 14. Selecting Bash*

Enabling Accelerated Networking on WAN0

1. Run this command to display current WAN0 NIC settings.

   ```
   az network nic show --name <WAN0 NIC name> --resource-group <Resource Group name>
   ```

   replace `<WAN0 NIC name>` with the name that was assigned to the WAN0 NIC.

   replace `<Resource Group name>` with the name of the resource group.

   Guide Example: az network nic show --name ni_WAN0 --resource-group SP-Tech
2. Verify that Accelerated Networking is disabled on the WAN0 NIC (Figure 15).

*Figure 15. Accelerated Networking disabled*

```plaintext
dinosh@Azure:~$ az network nic show --name ni_WAN0 --resource-group SP-Tech
{
  "dnsSettings": {
    "appliedDnsServers": [],
    "dnsServers": [],
    "internalDnsNameLabel": null,
    "internalDomainNameSuffix": "wvnn0banayzudmikor4cdti0kc.bx.internal.cloudapp.net",
    "internalFqdn": null
  },
  "dscpConfiguration": null,
  "enableAcceleratedNetworking": false,
  "enableIpForwarding": false,
  "etag": "W/\"d1cf67bf-bf4d-4743-94a9-24cf4919763b\"",
  "extendedLocation": null,
  "hostedWorkloads": []
}
```

3. Run this command to enable Accelerated Networking on the WAN0 NIC (Figure 16).

```plaintext
az network nic update --accelerated-networking true --name <WAN0 NIC name> --resource-group <Resource Group name>
```

   replace `<WAN0 NIC name>` with the name assigned to the WAN0 NIC.

   replace `<Resource Group name>` with the name of the resource group.

   Guide Example: `az network nic update --accelerated-networking true --name ni_WAN0 --resource-group SP-Tech`

4. Verify that Accelerated Networking is enabled on the WAN0 NIC.

*Figure 16. Accelerated Networking enabled*

```plaintext
dinosh@Azure:~$ az network nic update --accelerated-networking true --name ni_WAN0 --resource-group SP-Tech
{
  "dnsSettings": {
    "appliedDnsServers": [],
    "dnsServers": [],
    "internalDnsNameLabel": null,
    "internalDomainNameSuffix": "wvnn0banayzudmikor4cdti0kc.bx.internal.cloudapp.net",
    "internalFqdn": null
  },
  "dscpConfiguration": null,
  "enableAcceleratedNetworking": true,
  "enableIpForwarding": false,
  "etag": "W/\"c9f8952f-26ce-4fa5-a08c-fc1c0a6506cd\"",
  "extendedLocation": null,
```
Enabling Accelerated Networking on LAN0

1. Run this command to display current LAN0 NIC settings.
   
   ```bash
   az network nic show --name <LAN0 NIC name> --resource-group <Resource Group name>
   
   replace <LAN0 NIC name> with the name assigned to the LAN0 NIC.
   replace <Resource Group name> with the name of the resource group.
   
   Guide Example: az network nic show --name ni_LAN0 --resource-group SP-Tech
   ```

2. Verify that Accelerated Networking is disabled on the LAN0 NIC.

3. Run this command to enable Accelerated Networking on the WAN0 NIC.
   
   ```bash
   az network nic update --accelerated-networking true --name <LAN0 NIC name> --resource-group <Resource Group name>
   
   replace <LAN0 NIC name> with the name assigned to the LAN0 NIC.
   replace <Resource Group name> with the name of the resource group.
   
   Guide Example: az network nic update --accelerated-networking true --name ni_LAN0 --resource-group SP-Tech
   ```

4. Verify that Accelerated Networking is enabled on the LAN0 NIC.

Next Step: Proceed to Assign a Public IP Address to the WAN0 Interface on the next page
Assign a Public IP Address to the WAN0 Interface

A public IP address is required on the WAN0 interface because the Orchestrator will establish an Underlay over the Internet.

The following steps assign a public IP address to the WAN network interface in the Azure Portal.

1. Open the WAN Network Interface page by clicking its name on the Resource group page. Guide example: click ni_WAN0
2. In the Settings menu, click IP configurations.
3. Click ipconfig1. The ipconfig1 edit panel opens.
4. Select the Public IP Address option of Associate.
5. Click Create New below the Public IP address field. The Add a public IP address dialog opens.
6. Select the public IP address parameters:
   - **Name**: Enter a descriptive name of the IP Address. Guide example: ip_WAN0
   - **SKU**: Selection depends on deployment type:
     - Single EC-V Deployment: Select Basic
     - Multiple EC-V Deployment: Select Standard
       Microsoft recommends Standard SKU public IP addresses; they are zone-redundant by default and work with the Standard SKU Load Balancer.
   - **Assignment**: Select Static
     This parameter is available only when Basic is the selected SKU.
   - Click OK
7. Enter the following parameter settings:
   - **Assignment**: Select Static
   - **IP address**: Select the IP address assigned to WAN0.
     Guide example (single appliance deployment) is 10.6.2.10
     Guide example (HA deployment – ECV-A) is 10.6.2.10
     Guide example (HA deployment – ECV-B) is 10.6.2.11

8. Click Save in the menu bar to return to the Resource Group page.

Next Step: Proceed to Enable IP Forwarding on the LAN0 Network Interface on the next page
Enable IP Forwarding on the LAN0 Network Interface

The following steps enable IP forwarding on the LAN0 network interface.

1. Open the Network Interface page for the LAN interface by clicking its name from the Azure Portal Resource group page.
   Guide example: click *ni_LAN0*

2. In the **Settings** menu, click **IP configurations**.

3. For IP forwarding, select **Enabled**.

4. Click **Save** in the menu bar.
   The Resource Group page returns.

**Next Step: Proceed to Attach WAN0 and LAN0 Network Interfaces to the EC-V on the next page**
Attach WAN0 and LAN0 Network Interfaces to the EC-V

An EC-V must be powered off before attaching additional interfaces to the appliance.

The following steps attach **WAN0** and **LAN0** network interfaces to the EC-V and record the MAC addresses of the attached interfaces.

**Attaching the Interfaces**

1. Open the **Virtual machine** page for the EC-V (from the Azure Portal Resource group page).
   Guide example: click *vm-ECV*

2. Power OFF the EC-V by clicking **Stop** in the menu bar.
   Reserve the Public IP address, if prompted. Do not proceed until the VM has stopped.

3. Select **Networking** from the **Settings** menu (left-side column).
   The **Networking** page opens for the virtual machine.

4. Click **Attach network interface** from the menu bar at the top of the page.

5. Select the WAN0 network interface (drop-down menu) and click **OK**.
   Guide example: *ni_WAN0*

6. Click **Attach network interface** from the menu bar at the top of the page.

7. Select the LAN0 network interface (drop-down menu) and click **OK**.
   Guide example: *ni_LAN0*

8. Return to the **Virtual machine** page and click **Start** to power up the EC-V.
   Do not proceed until the status is **Running**.

**Recording the MAC Addresses of the Interfaces**

The MAC Addresses are required when configuring the EC-V appliances.

1. Open the WAN0 network interface page (from the **Resource group** page).

2. Click **Properties** from the **Settings** menu.

3. Record the MAC address of the WAN interface.

4. Open the LAN0 network interface page (from the **Resource group** page).

5. Click **Properties** from the **Settings** menu.

6. Record the MAC address of the LAN interface.

**Next Step:** Proceed to **Configure the EC-V for In-line Router Mode on the next page**
Configure the EC-V for In-line Router Mode

The following steps configure an EC-V for In-line Router Mode.

1. Log on to Orchestrator.

2. Select the EC-V in the appliance menu and open the Interfaces page (Configuration > Networking > Interfaces).

3. Assign the WAN0 and LAN0 MAC addresses:
   A. Click the Edit icon on one of the Interface rows to open the Interface edit popup.
   B. Click the MAC field for the wan0 interface. Select its MAC address (drop-down).
   C. Click the MAC field for the lan0 interface. Select its MAC address (drop-down).
   D. Click Apply in the bottom right corner of the popup.

4. Select the EC-V in the appliance menu and open the Deployment page (Configuration > Networking > Deployment).

5. Configure deployment parameters for the EC-V:
   A. Click the edit icon of a deployment row to open the Deployment edit popup.
   B. Click Router (upper left corner).
   C. Under LAN0 IP/Mask, enter the LAN0 interface private IP address / subnet mask.
      Guide example (single appliance deployment) is 10.6.3.10/24
      Guide example (HA deployment – ECV-A) is 10.6.3.10/24
      Guide example (HA deployment – ECV-B) is 10.6.3.11/24
   D. Under WAN0 IP/Mask, enter the WAN0 interface private IP address and subnet mask.
      Guide example (single appliance deployment) is 10.6.2.10/24
      Guide example (HA deployment – ECV-A) is 10.6.2.10/24
      Guide example (HA deployment – ECV-B) is 10.6.2.11/24
      Guide example: 10.6.2.10/24
   E. Under LAN0 Next Hop, enter the first IP address of the LAN0 subnet address space. Azure sets the subnet’s first IP address as its gateway.
      Guide example is 10.6.3.1
   F. Under WAN0 Next Hop, enter the first IP address of the WAN0 subnet address space.
      Guide example is 10.6.2.1
   G. Enter the Total Outbound and Total Inbound bandwidth (Kbps) for the WAN0 interface and click ∑Calc.
   H. Set WAN0 Firewall Mode to Stateful+SNAT.
   I. Click Not behind NAT (under WAN Next Hop) and select NAT in the NAT Settings popup.
This allows Orchestrator to use the \texttt{WAN0} public IP address as the tunnel endpoint when establishing underlays to the \texttt{WAN0} interface.

J. Click \textbf{Apply}.

K. Click \textbf{Apply & Reboot} when prompted.

6. After the VM reboots, go to the \textit{Configuration > Networking > Interfaces} page and verify that the \texttt{WAN0} public IP address appears in the table.

7. (Optional) Upgrade the EC-V appliance to the desired software version (\textit{Administration > Software > Upgrade > Upgrade Appliances}).

Refer to the Release Notes for information about available software versions. Implementing the deployment of the depicted topology does not require an appliance upgrade.

\textbf{IMPORTANT} The next step in the configuration process depends on your deployment type and progress.

- When deploying a single EC-V appliance, the next step is configuring traffic redirection.

- When deploying two appliances in an HA configuration, the next step depends on 1) if both appliances are configured, and 2) the type of HA deployment being configured. In either HA deployment case, \textbf{DO NOT proceed} to the \textit{Single EC-V Deployment: Configure Traffic Redirection Using Static Routes} topic.

Use the following list to determine your next topic:

- Single EC-V Deployment with static routes: \textit{Create a Static Route on the Azure Route Table} on page \pageref{page:44}

- Single EC-V Deployment with BGP routing: \textit{Create an Azure Virtual WAN (VWAN) Hub} on page \pageref{page:62}

The \textit{Single EC-V Appliance with BGP Routing} and \textit{HA EC-V Virtual Hub} use cases utilize the same processes to create the VWAN Hub. The \textit{Create an Azure Virtual WAN Hub} topic that the link accesses is in the HA configuration section. Disregard instructions that reference a second EC-V appliance when implementing the \textit{Single EC-V Appliance with BGP Routing} use case.

- HA Deployment using Azure Virtual Hub:
  - To configure the second EC-V: \textit{Create an EC-V Virtual Machine in Azure} on page \pageref{page:19}
  - All appliances are configured: \textit{Creating an Azure Virtual Hub in an EC-V HA Architecture} on page \pageref{page:61}

- HA Deployment using Azure Internal Load Balancer:
  - To configure the second EC-V: \textit{Create an EC-V Virtual Machine in Azure} on page \pageref{page:19}
  - All appliances are configured: \textit{Create an Azure Standard Internal Load Balancer} on page \pageref{page:99}

\textbf{Next Step: Proceed to the section specified by your deployment selection and status}
Configure Traffic Redirection Using Static Routes

To redirect outbound traffic from workloads in Azure to the EC-V with static routes (also known as User Defined Routes), perform the following tasks:

Tasks include:
- Create a Static Route on the Azure Route Table
- Add a Route on the EC-V to Advertise the Workload's Subnet
- Verify end-to-end connectivity
Create a Static Route on the Azure Route Table

The following steps create an Azure route table, adds a route to the table, then associates the route to the Workloads subnet.

Create the Route Table

1. From the Azure portal, navigate to your Resource group and click +Create in the menu bar.
2. Use the search field to select Route Table in the drop-down menu, then click Create to open the Create Route Table page.
3. Enter the following values in the Create Route Table fields:
   - **Name**: Enter a descriptive name for the route. Guide example is rt_ECV
   - **Subscription**: (drop-down) Depends on your Azure account. Guide example is Pay-As-You-Go
   - **Resource Group**: (drop-down) Select your Resource Group. Guide example is SP-Tech
   - **Location**: Select the region where you deployed the EC-V.
   - **Propagate Gateway Routes**: Enabling this option is optional because the topology does not include a VPN gateway. Guide example is Disabled
4. Click Review + Create. Azure displays the Create Route table page. Proceed when the green Validation passed bar appears at the top of the page.
5. Click the Create button at the bottom of the page.
6. When the Overview page displays Your Deployment is complete, open the Route Table page by clicking Go to Resource.

Create a Route

These steps are performed from the Route Table page.

1. Select Routes from the Settings menu (left-side column). The Route Table page opens.
2. Click +Add in the menu bar. The Add Route panel opens.
3. Enter the following values in the Add route fields:
   - **Route name**: Enter a descriptive name for the route. Guide example is `rte_REMOTE`
   - **Address Prefix**: Enter the IP address of the workload. Guide example is `10.3.2.0/24`
   - **Next-hop type**: (drop-down) Select **Virtual Appliance**
   - **Next-hop address**: Enter the local EC-V’s LAN0 IP address. Guide example is `10.6.3.10`

4. Click **OK** at the bottom of the panel.
The Route Table page opens.

**Associate the Route to a Subnet**

1. Select **Subnets** from the **Settings** menu (left-side column).
The Route Table | Subnets page opens.

2. Click +**Associate** on the menu bar.
The Associate subnet dialog opens (Right side of page).

3. Enter the following values in the Associate subnet fields:
   - **Virtual Network**: (drop-down) Select the virtual network used for the deployment. Guide example is `vn_ECV`
   - **Subnet**: (drop-down) Select the Workloads subnet. Guide example is `sub_WKLD`

4. Click **OK** at the bottom of the dialog.

Next Step: Proceed to **Add a Route on the EC-V to Advertise the Workload's Subnet on the next page**
Add a Route on the EC-V to Advertise the Workload's Subnet

You can advertise Azure subnets to remote EdgeConnect devices by adding them on the Azure EC-V's route table. After a route is added, it is advertised to remote EdgeConnect devices.

The following steps add a **local** route to the Azure EC-V **Routes** page.

1. Open Orchestrator, select the EC-V (in the Appliance menu) and open the **Routes** tab (**Configuration > Networking > Routing > Routes**).
2. Click an icon in the **Edit** column.
   The **Routes** dialog opens.
3. Click **Add Route**, located above the table.
   The **Add Route** dialog opens.
4. Enter the following values in the **Add Route** fields:
   - **Subnet/Mask**: Enter the Azure workload subnet.
     Guide example is **10.6.4.0/24**
   - **Next Hop**: Enter the LAN0 next-hop IP address.
     Guide example is **10.6.3.1**
   - **Interface**: Optional
   - **Metric**: Use the default metric value.
   - **Tag**: (drop-down) Select **FROM_WAN**
   - **Comments**: (Checkbox) Optional
5. Click **Add** (bottom of popup).
6. Click the edit icon right of the **Redistribute routes to SD-WAN Fabric** data field.
   The **SD-WAN Fabric Route Distribution Maps** dialog opens.
7. Verify the dialog includes a rule with the following settings:
   - **Match Criteria**: Source Protocol **Local/Static**
     - **Prefix**: Enter the Route address
     Guide example is **10.6.4.0/24**
   - **Permit** (Selection box): **Mark**
     This ensures the static routes are advertised to the SD-WAN fabric.
8. Modify or add a rule if necessary, then click **Apply**.
    If no modification is required, click **Cancel**.
9. Click **Apply** to close the Routes dialog.

**Next Step**: Proceed to **Verify end-to-end connectivity on the next page**
Verify end-to-end connectivity

To verify that outbound traffic from the Azure workloads is received by the Azure EC-V:

1. Log into a workload deployed on the *workloads* subnet.
2. Run `traceroute` to any IP address on the remote network.
   Guide example – the remote network’s address space is 10.3.2.0/24.

As shown in the `traceroute` command output in Figure 17, traffic successfully reaches the remote workload via IP address 10.6.3.4 – the LAN0 interface of the local Azure EC-V instance. This confirms the Azure EC-V receives outbound traffic sent from the Azure workload.

**Figure 17. Verify end-to-end connectivity**

```
$ traceroute 10.3.2.5
traceroute to 10.6.3.4 (10.6.3.4), 30 hops max, 60 byte packets
1 10.6.3.4 2.673 ms 2.655 ms 2.645 ms
2 10.3.2.4 6.000 ms 5.977 ms 5.979 ms
3
4
5
6 10.3.2.5 4.615 ms 4.570 ms
```

The Monitoring: Flow page can also confirm end-to-end connectivity of the traffic.

**Figure 18. Flows page**

Now that the outbound traffic redirection is set up correctly in Azure and you can send traffic end-to-end, you may create the necessary Business Internet Overlays (BIO) and other traffic policies in the Silver Peak Orchestrator. For more information about creating BIOs, refer to Building Business Overlays.

For a general overview of BIOs, refer to About Business Overlays.

Next Step: The Single EC-V Deployment is completed.
Single EC-V Deployment with BGP Routing

The following sections describe the implementation of a single EC-V Deployment with BGP routes on the Azure Route Table to redirect traffic to the EC-V.

Background Topics

The following topics provide information about implementing EC-V appliances with an Azure Virtual Hub:

- Azure Virtual Hub Overview and an EC-V Appliance on the next page
- Prerequisites to Deploying a Single EC-V Appliance with Azure Virtual Hub from the Azure Portal on page 51

Configuration Topics

The following procedures implement the EC-V HA deployment depicted in Figure 19. These procedures can be modified to deploy any EC-V architecture with an Azure Virtual Hub.

1. Review your topology and assemble the required information. (Topology – EC-V Deployment (BGP Routing) on page 52).

2. Repeat Steps A through C for the EC-V appliance:
   A. Create an EC-V Appliance in the Azure Portal on page 12
   B. Configure the EC-V on page 24
   C. Create Data Path Interfaces on page 31

   **IMPORTANT** Data Path Interfaces are configured after configuring the Virtual Hub. Do Not perform the Single Deployment Data Path Interfaces procedures.

3. Configure the Azure Virtual Hub (Creating an Azure Virtual Hub in an EC-V HA Architecture on page 61):

4. Create the BGP over IPsec tunnels from the appliance to the Virtual Hub (Traffic Redirection in the HA Deployment (Azure Virtual Hub) on page 70):

Use the following list to determine your next topic:

- To review background information first: Azure Virtual Hub Overview and an EC-V Appliance
- To begin configuration immediately: Topology – EC-V Deployment (BGP Routing)

**First Step: Proceed to your selected section**
Azure Virtual Hub Overview and an EC-V Appliance

Azure Virtual Hub Overview

An Azure Virtual Hub is a Microsoft-managed service that is part of the Azure Virtual WAN (VWAN) solution. With an Azure subscription, you can deploy one Azure Virtual Hub per Azure region. An Azure Virtual Hub can connect to virtual networks without using IPsec tunnels, learning the virtual networks' address ranges. This allows the Virtual Hub to forward inbound traffic destined to a connected Spoke virtual network without using static routes in its route table.

The Azure Virtual Hub comes in different sizes (scale units), supporting a maximum throughput of 20 Gbps. The Azure Virtual Hub can terminate an IPsec tunnel from a VPN device. It is also capable of establishing a BGP session with a third-party BGP peer. When a BGP peer establishes a BGP session with the Azure Virtual Hub, it advertises the address range of the virtual networks to which it is connected.

Azure Virtual Hub pricing details are available at: https://azure.microsoft.com/en-us/pricing/details/virtual-wan/

Azure Virtual Hub Functionality With an EC-V Appliance

Silver Peak software supports VRRP, WCCP, BGP, and OSPF protocols. Silver Peak use these protocols to eliminate single points of failure on EdgeConnect devices. Of these protocols, Azure supports only BGP, which is available on the Azure Virtual Hub. With an Azure EC-V appliance, the Azure Virtual Hub acts as the BGP peer of the EC-V deployed in Azure.

Using BGP to Learn and Advertise routes Dynamically with the Azure Virtual Hub

BGP can be used to advertise routes that the Azure EC-V learns (from other EdgeConnect devices via Subnet Sharing) to the Azure Virtual Hub. With routes advertised in this manner, the Virtual Hub does not require static routes in its route table to forward outbound (Azure to on-prem bound) traffic to the EC-V. Similarly, static routes are not required on the EC-V to advertise Azure virtual network subnets with other (remote) EdgeConnect devices. When an Azure EC-V establish BGP sessions with Azure Virtual Hub, it learns subnets of each virtual network connected to the Azure Virtual Hub.

Using IPsec Tunnels for BGP Sessions from an EC-V to an Azure Virtual Hub

Because Azure is a multi-tenant environment, BGP peers (such as the EC-V appliances) must encapsulate BGP sessions over IPsec tunnels to establish their sessions with the Azure Virtual Hub. This is true even when the EC-V appliance runs on the same region as the Virtual Hub.
Inter-Virtual Network Communication Through an Azure Virtual Hub

There are two types of Azure Virtual WANs: Basic and Standard. In a "Basic" Virtual WAN resource, the workloads in your spoke virtual networks cannot communicate with workloads in other spoke virtual networks through the Azure Virtual Hub. To allow this communication, you must create virtual network Peering between the two spoke virtual networks. Similarly, the Azure Virtual Hubs in your Virtual WAN resource cannot communicate with other Azure Virtual Hubs in different Azure regions.

In a "Standard" Virtual WAN resource, workloads in your spoke virtual networks CAN communicate with workloads in other spoke virtual networks through the Azure Virtual Hub. The Azure Virtual Hubs in your Virtual WAN resource can also communicate with other Azure Virtual Hubs in different Azure regions to allow branch-to-branch communication through the Azure backbone.

We recommend deploying a "Standard" Virtual WAN resource for this deployment.

BGP over IPsec tunnels from WAN and LAN interfaces

EdgeConnect supports BGP over IPsec tunnels to the Virtual Hum from both WAN-side and LAN-side interfaces on Azure EC-V appliances. Figure 19 displays BGP over IPsec tunnels over LAN-side tunnels.

Traffic between IPsec Tunnels on the EC-V Appliance and the Azure Virtual Hub stays in the Azure network

IPsec tunnel traffic from EC-V to the Azure Virtual Hub is matched by the default route (0.0.0.0/0) on the Azure virtual network route table whose next-hop is set as Internet. However, traffic never leaves Azure's backbone network because Microsoft owns public IP address assigned to the EC-V appliance (that terminates the IPsec tunnel on the EC-V side) and the public IP address on the Azure Virtual Hub.

Design Limitations

Even though Azure Virtual Hub supports Equal-cost multi-path routing (ECMP), BGP over IPsec tunnels from one EC-V to the Virtual Hub utilize only one path for sending and receiving traffic through the Azure Virtual Hub. This is because EC-V does not support BGP ECMP. As a result, a single EC-V can only send (and receive) up to 1 Gbps from the Azure Virtual Hub because Azure only supports 1 Gbps per IPsec VPN tunnel to their Virtual Hub.
Prerequisites to Deploying a Single EC-V Appliance with Azure Virtual Hub from the Azure Portal

- All Single EC-V Deployment prerequisites, as listed on Prerequisites to Deploying EC-V in Azure.
- An EC-V deployment with Azure Virtual Hub requires Unity EdgeConnect version 8.3.0.5 and above, and Unity Orchestrator version 8.9.0 or 8.10.0 and above.
- Azure Virtual Hub's virtual network must differ from that of the EC-Vs, as shown in Figure 19. The Virtual Hub virtual network should also not overlap with any of on-premises networks or other Azure virtual networks.

Next Step: Proceed to Topology – EC-V Deployment (BGP Routing)
**Topology – EC-V Deployment (BGP Routing)**

*Figure 19* shows a logical topology of an EC-V deployment with the Azure Virtual Hub.

*Figure 19. Logical topology of an EC-V appliance with the Azure Virtual Hub*

Deployment considerations for implementing an EC-V for use an Azure Virtual Hub includes:

- Use Standard public IP addresses when assigning public IP addresses to EC-V interfaces.
  
  **IMPORTANT** Do not assign basic public IP addresses to any interface.

Before starting the deployment process, assemble the following information:

- **Azure account**: Username and password that accesses your Azure account
- **Azure Resource Group**: Name of the resource group
- **EdgeConnect credentials**: Account name and Account key – received from Silver Peak

**IMPORTANT** Starting with versions 8.3.0.5 and 8.3.1.0, EdgeConnect supports BGP over IPsec tunnels over both WAN interfaces and LAN interfaces. When you establish the BGP over an IPsec tunnel from a LAN interface, you must assign a public IP address to the LAN0 interface.

**First Step: Proceed to Prepare the Resource Group on page 13**
EC-V HA Deployment: Azure Virtual Hub

This section describes the deployment of two EC-V appliances to provide high availability for your workloads. The topology uses an Azure Virtual Hub and implements BGP over IPsec tunnels on the EC-V to exchange traffic through the Virtual Hub.

Background Topics

The following topics provide information about implementing EC-V appliances with an Azure Virtual Hub:

- Azure Virtual Hub Overview and the EC-V HA Architecture
- Prerequisites to Deploying EC-V HA with Azure Virtual Hub from the Azure Portal

Configuration Topics

The following procedures implement the EC-V HA deployment depicted in Figure 21. These procedures can be modified to deploy any EC-V architecture with an Azure Virtual Hub.

1. Review your topology and assemble the required information. (Topology – EC-V HA Deployment (Azure Virtual Hub) on page 58).

2. Repeat Steps A through C for each EC-V appliance to be deployed:
   A. Create an EC-V Appliance in the Azure Portal on page 12
   B. Configure the EC-V on page 24
   C. Create Data Path Interfaces on page 31

   **IMPORTANT** Traffic Redirection is configured after configuring the Virtual Hub. Do Not perform the Single Deployment Traffic Redirection procedures.

3. Configure the Virtual Hub (Creating an Azure Virtual Hub in an EC-V HA Architecture on page 61).

4. Create BGP over IPsec tunnels from the appliances to the Virtual Hub (Traffic Redirection in the HA Deployment (Azure Virtual Hub) on page 70).
   After BGP over IPsec tunnels are established from each EC-V to the Virtual Hub, you can set up either active-standby failover mode or active-active failover mode.

Use the following list to determine your next topic:

- To review background information first: Azure Virtual Hub Overview and the EC-V HA Architecture
- To begin configuration immediately: Topology – EC-V HA Deployment (Azure Virtual Hub)

**First Step: Proceed to your selected section**
Azure Virtual Hub Overview and the EC-V HA Architecture

Azure Virtual Hub Overview

An Azure Virtual Hub is a Microsoft-managed service that is part of the Azure Virtual WAN (VWAN) solution. With an Azure subscription, you can deploy one Azure Virtual Hub per Azure region. An Azure Virtual Hub can connect to virtual networks without using IPsec tunnels, learning the virtual networks’ address ranges. This allows the Virtual Hub to forward inbound traffic destined to a connected Spoke virtual network without using static routes in its route table.

The Azure Virtual Hub comes in different sizes (scale units), supporting a maximum throughput of 20 Gbps. The Azure Virtual Hub can terminate an IPsec tunnel from a VPN device. It is also capable of establishing a BGP session with a third-party BGP peer. When a BGP peer establishes a BGP session with the Azure Virtual Hub, it advertises the address range of the virtual networks to which it is connected.

Azure Virtual Hub pricing details are available at: https://azure.microsoft.com/en-us/pricing/details/virtual-wan/

Azure Virtual Hub Functionality Within an EC-V HA Architecture

Silver Peak software supports VRRP, WCCP, BGP, and OSPF protocols. Silver Peak use these protocols to eliminate single points of failure on EdgeConnect devices. Of these protocols, Azure supports only BGP, which is available on the Azure Virtual Hub. In an Azure EC-V HA architecture, the Azure Virtual Hub acts as the BGP peer of the EC-Vs deployed in Azure.

Using BGP to Deploy EC-Vs in a Scale-out Architecture

When deploying multiple EC-Vs in Azure in a scale-out architecture to achieve high throughput and redundancy, each EC-V establishes two BGP sessions with the Azure Virtual Hub. When one EC-V fails, BGP sessions from the failed EC-V to the Azure Virtual Hub cease and the Virtual Hub stops forwarding traffic to that EC-V. It forwards traffic to the other EC-V with which it has active BGP sessions.

To place the device in active-standby failover mode, configure the Metric field on the BGP Inbound Route Redistribution Map and the ASN Prepend Count value on the BGP Outbound Route Redistribution Map. If you require active-active failover mode, leave all BGP path attributes the same across all BGP sessions on each Azure EC-V.

BGP can be used to advertise routes that the Azure EC-V learns (from other EdgeConnect devices via Subnet Sharing) to the Azure Virtual Hub. With routes advertised in this manner, the Virtual Hub does not require static routes in its route table to forward outbound (Azure to on-prem bound) traffic to the EC-V. Similarly, static routes are not required on the EC-V to advertise Azure virtual network subnets with other (remote) EdgeConnect devices. When Azure EC-Vs establish BGP
sessions with Azure Virtual Hub, they learn subnets of each virtual network connected to the Azure Virtual Hub.

**Using IPsec Tunnels for BGP Sessions from EC-Vs to an Azure Virtual Hub**

Because Azure is a multi-tenant environment, BGP peers (such as the EC-V appliances) must encapsulate BGP sessions over IPsec tunnels to establish their sessions with the Azure Virtual Hub. This is true even when the EC-V appliance runs on the same region as the Virtual Virtual Hub.

**Inter-Virtual Network Communication Through an Azure Virtual Hub**

There are two types of Azure Virtual WANs: Basic and Standard. In a "Basic" Virtual WAN resource, the workloads in your spoke virtual networks cannot communicate with workloads in other spoke virtual networks through the Azure Virtual Hub. To allow this communication, you must create virtual network Peering between the two spoke virtual networks. Similarly, the Azure Virtual Hubs in your Virtual WAN resource cannot communicate with other Azure Virtual Hubs in different Azure regions.

In a "Standard" Virtual WAN resource, workloads in your spoke virtual networks CAN communicate with workloads in other spoke virtual networks through the Azure Virtual Hub. The Azure Virtual Hubs in your Virtual WAN resource can also communicate with other Azure Virtual Hubs in different Azure regions to allow branch-to-branch communication through the Azure backbone.

We recommend deploying a "Standard" Virtual WAN resource for this deployment.

**BGP over IPsec tunnels from WAN and LAN interfaces**

EdgeConnect supports BGP over IPsec tunnels to the Virtual Hum from both WAN-side and LAN-side interfaces on Azure EC-V appliances. **Figure 21** displays BGP over IPsec tunnels over LAN-side tunnels.

**Traffic between IPsec Tunnels on EC-V Appliances and the Azure Virtual Hub stays in the Azure network**

IPsec tunnel traffic from EC-V to the Azure Virtual Hub is matched by the default route (0.0.0.0/0) on the Azure virtual network route table whose next-hop is set as Internet. However, traffic never leaves Azure's backbone network because Microsoft owns public IP address assigned to the EC-V appliance (that terminates the IPsec tunnel on the EC-V side) and the public IP address on the Azure Virtual Hub.

**Design Limitations**

Even though Azure Virtual Hub supports Equal-cost multi-path routing (ECMP), BGP over IPsec tunnels from one EC-V to the Virtual Hub utilize only one path for sending and receiving traffic through the Azure Virtual Hub. This is because EC-V does not support BGP ECMP. As a result, a single EC-V can only send (and receive) up to 1 Gbps from the Azure Virtual Hub because Azure only supports 1 Gbps per IPsec VPN tunnel to their Virtual Hub.
Deploying EC-Vs in an active-active configuration increases available bandwidth for workloads deployed in Azure. However, this results in asymmetric flows because the Azure Virtual Hub has two paths (via the two EC-Vs) to forward traffic to the remote site. Asymmetric flows do not affect most applications. However, if you have firewalls deployed on the LAN-side of the EC-Vs in Azure as shown in Figure 20, asymmetric flows cause the firewall to drop traffic unless you specifically allow such traffic in the firewall. This is because the firewall did not receive the initial incoming packet from the remote network.

Firewalls deployed on the LAN-side of the EC-Vs in Azure drop asymmetric flows. This is avoided by deploying the EC-Vs in active-standby configuration.

Figure 20. EC-V deployment with the Azure Virtual Hub and Firewall

Next Step: Proceed to Prerequisites to Deploying EC-V HA with Azure Virtual Hub from the Azure Portal on the next page
Prerequisites to Deploying EC-V HA with Azure Virtual Hub from the Azure Portal

- All Single EC-V Deployment prerequisites, as listed on Prerequisites to Deploying EC-V in Azure.
- An EC-V deployment with Azure Virtual Hub requires Unity EdgeConnect version 8.3.0.5 and above, and Unity Orchestration version 8.9.0 or 8.10.0 and above.
- A public IP address is required on the LAN0 interface to establish an IPsec tunnel from the LAN0 interface to the Virtual Hub.
- When deploying EC-Vs in a region that supports Availability Zones (AZ), place each EC-V in unique AZs as shown in Figure 21.
  As of June 2020, several Azure regions do not support AZs.
- When deploying EC-Vs in a region that does not support AZs, place all EC-Vs in a single Availability Set to protect against Azure hardware failures.
  An Availability Set ensures that the deployed EC-Vs are distributed across multiple, isolated hardware nodes, in a cluster. If you are deploying EC-Vs in a region that supports AZs, instead of placing EC-Vs in an Availability Set, you must deploy them in unique AZs.
- Both EC-Vs must be deployed on the same virtual network.
  Azure Virtual Networks (VNets), subnets, and load balancers are regional resources – not zonal. Therefore, only one MGMT0, WAN0, and LAN0 subnet is required for both EC-Vs as shown in Figure 21.
- Azure (user) workloads must exist on a different virtual network(s) than the virtual network where the EC-Vs are deployed.
- Azure Virtual Hub’s virtual network must differ from that of the EC-Vs, as shown in Figure 21.
  The Virtual Hub virtual network should also not overlap with any of on-premises networks or other Azure virtual networks.
- Instead of creating a Network Security Group (NSG) for each vNIC on each EC-V, you may create one NSG for both MGMT0 interfaces, one NSG for both WAN0 interfaces, and one NSG for both LAN0 interfaces. This will simplify the management of firewall rules applied on each vNIC.

Next Step: Proceed to Topology – EC-V HA Deployment (Azure Virtual Hub) on the next page
# Topology – EC-V HA Deployment (Azure Virtual Hub)

Figure 21 displays EC-V – Azure Virtual Hub deployment topology implemented by this chapter.

**Figure 21. Logical topology of an EC-V deployment with the Azure Virtual Hub**

Deployment considerations for implementing each EC-V with an Azure Virtual Hub includes:

- If the selected Azure region supports Availability Zones (AZ), place each EC-V in different AZs.
- If the selected region does not support AZs, place each EC-V in the same Availability Set. Placing all EC-Vs in one availability set ensures that at least one EC-V continues running when a hardware or software failure incapacitates one rack in the selected Azure data center.
- Use Standard public IP addresses when assigning public IP addresses to EC-V interfaces.

**IMPORTANT**  Do not assign basic public IP addresses to any interface.

Before starting the deployment process, assemble the following information:
Assign a Public IP Address to the LAN0 Interface

The following steps assign a public IP address to the LAN network interface in the Azure Portal.

1. Open the Virtual machine page for the EC-V (from the Azure Portal Resource group page).
   Guide example: click vm-ECV

2. Power OFF the EC-V by clicking Stop in the menu bar.
   Reserve the Public IP address, if prompted. Do not proceed until the VM has stopped.

3. Open the LAN Network Interface page by clicking its name on the Resource group page.
   Guide example: click ni_LAN0

4. In the Settings menu, click IP configurations.

5. Click ipconfig1.
   The ipconfig1 edit panel opens

6. Click Create New, located below the Public IP address field.
   The Add a public IP address dialog opens.

7. Select the public IP address parameters.
   - Name: Enter a descriptive name of the IP Address. Guide example: ip_LAN0
   - SKU: Selection depends on deployment type
     - Single EC-V Deployment: Select Basic
     - Multiple EC-V Deployment: Select Standard
       Microsoft recommends Standard SKU public IP addresses; they are zone-redundant by default and work with the Standard SKU Load Balancer.
   - Assignment: Select Static
     This parameter is available only when Basic is the selected SKU.

8. Enter the following parameter settings:
   - Public IP address: Select Associate
   - Assignment: Select Static
   - IP address: Select the IP address assigned to LAN0.
     Guide example (single appliance deployment) is 10.6.3.10
     Guide example (HA deployment – ECV-A) is 10.6.3.10
     Guide example (HA deployment – ECV-B) is 10.6.3.11
9. Click the **IP address - Configure required settings** box (below the Public IP address parameter).
   The **Choose public IP address** panel opens right of the ipconfig1 edit panel.

10. Click **OK** at the bottom of the page to return to the **ipconfig1** panel.

11. Click **Save** in the menu bar to return to the **Resource Group** page.

12. Return to the **Virtual machine** page and click **Start** to power up the EC-V. Do not proceed until the status is **Running**.

**Next Step: Proceed to Prepare the Resource Group on page 13**
Creating an Azure Virtual Hub in an EC-V HA Architecture

The following instructions configure the Azure Virtual Hub.

**Configuration Tasks include:**

- Create an Azure Virtual WAN (VWAN) Hub
- Create the VPN Sites
- Create the Virtual Network Connections
- Download the Virtual Hub's VPN Configuration File
Create an Azure Virtual WAN (VWAN) Hub

The following instructions create an Azure Virtual WAN (VWAN) and a Hub within the VWAN.

Create the VWAN

1. From the Azure portal, navigate to your Resource group and click +Create in the menu bar.

2. Use the search field to select Virtual WAN in the drop-down menu, then click Create to open the Virtual WAN page.

3. Verify that Basics is selected in the menu bar and enter settings from the following list:
   - **Subscription**: (drop-down) Depends on your Azure account.
     Guide example is Pay-As-You-Go
     Guide example is SP-Tech
   - **Resource Group Location**: (drop-down) Select the region where the Resource Group was deployed.
     Guide example is (US) West US
   - **Name**: Enter the label for the new VWAN.
     Guide example is vw_NET
   - **Type**: (drop-down) Select Standard

4. Click Review + create at the bottom of the page.
   Azure displays the Create WAN page. Proceed when the green Validation passed bar appears at the top of the page.

5. Click Create at the bottom of the page.
   The Deployment is Underway page is displayed.

6. When the page displays Your Deployment is complete, click Go to Resource.
   The Virtual WAN page is displayed for the new VWAN.

Create the Virtual Hub

1. Select Hubs from the Connectivity menu (left-side column).
   The Hub page opens for the Virtual WAN.

2. Click + New Hub in the button bar at the top of the page.
   The Create virtual hub page opens for the Virtual WAN.
3. Select **Basics** in the menu bar and enter the settings from the following list.
   - **Region**: (drop-down) Select the region where the Resource Group was deployed.
     Guide example is *(US) West US*
   - **Name**: Enter the label for the new hub.
     Guide example is vh_HUB-1
   - **Hub private address space**: Enter the hub IP address space (CIDR notation). This space cannot share any common addresses with the virtual network where the EC-Vs are deployed or any of your on-premises networks.
     Guide example is 10.7.0.0/16

4. Select **Site to site** in the menu bar and enter the settings from the following list.
   - **Do you want to create a site to site VPN**: Select *Yes*
   - **AS**: 65515 (not editable).
   - **Gateway scale units**: Select an option appropriate to your network requirements.
     Guide example is 1 scale unit - 500 Mbps x 2
   - **Routing Preference**: Select your preferred routing option.
     Guide example is *Internet*

5. Click the **Review + create** button at the bottom of the page.
   Azure displays the **Create virtual hub page** page. Verify that **Point to site** and **ExpressRoute** are disabled.
   Proceed when the green **Validation passed** bar appears at the top of the page.

6. Click **Create** at the bottom of the page.
   The **Deployment is Underway** page is displayed.
   Creating a hub with a gateway typically takes 30 minutes. Tasks in the next section can be performed while the hub is being deployed.

   **IMPORTANT** After the hub is created, you are charged for it even if you don't attach any sites to it.

Next Step: Proceed to **Create the VPN Sites on the next page**
Create the VPN Sites

While the virtual hub is deploying, create a VPN site for each EC-V that you deployed in Azure.

In a typical Azure VWAN deployment, details of your on-premises VPN device are entered when creating an Azure VPN Site. In this deployment, because we establish BGP over IPsec tunnels from the Azure EC-Vs to the VWAN Hub, details of the Azure EC-Vs are entered when creating the VPN Sites in Azure.

Create the First VPN Site (Using EC-V-A Details)

1. Open the Virtual WAN page for the VWAN that you created.
2. Select VPN (Sites) from the Connectivity menu (left-side column). The VPN (Sites) page opens for the Virtual WAN.
3. Click + Create site in the button bar at the top of the page. The Create VPN site panel opens.
4. Select Basics at the top of the panel and enter following values:
   - **Region**: (drop-down) Select the region where the Resource Group was deployed. Guide example is *(US) West US*
   - **Name**: Enter the label for the new VPN site. Guide example is *vpn_SITE-A*
   - **Device Vendor**: Enter *Silver Peak*
   - **Private Address Space**: None required because BGP is enabled.
5. Select Links at the bottom of the panel and enter following values:
   - **Link name**: (drop-down) Enter a descriptive name for the link. Guide example is *Link-1*
   - **Link speed**: Enter the Link speed (Mbps) of your ISP connection. Guide example is *50*
   - **Link provider name**: Enter the name of your Internet Service Provider (IPS). Guide example is *ISP Vendor A*
   - **Link IP address / FQDN**: Enter the public IP address of the EC-V interface connecting to the hub. The Network Interface page provides this information *(Figure 22).* Guide example: The LAN0 Interface connects to the Hub using *52.254.56.87*
- **Link BGP address**: Enter the IP address of Loopback interface (l0) that you plan to create on the EC-V (*Create a Loopback Interface on an EC-V*).
  
  Choose an IP address that does not overlap with any IP address range in your on-premises networks as well as Azure virtual networks. The IP address cannot be in the same address range as the Hub virtual network.
  
  While you can use any 169.254.x.x IP address as the loopback IP address (BGP endpoint) on the EC-V, it is not recommended due to additional configurations required on the Virtual Hub side and Azure’s handling of APIPA addresses. Visit this link for more information: [https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview)
  
  Guide example: **10.254.10.1**

- **Link ASN** Enter a private ASN number in the range between 64512 and 65535.
  
  **IMPORTANT** Do not use ASNs 65515, 65517-65520 (reserved by Azure services) or any private ASN that configured in your network.
  
  Guide example: **65500**

*Figure 22. LAN0 Public Address*

6. Click **Next : Review + Create** at the bottom of the page.
   Proceed when the page displays **Validation passed**.

7. Click **Create** at the bottom of the page.
   Proceed when the page displays **Deployment is Underway**.

8. Verify the status of the new VPN site is **Provisioned**.

9. Open the page for the previously created Virtual Hub by opening the **Virtual WAN** page and selecting the **Virtual Hub** on that page.

10. Open the VPN Site to Site page by selecting VPN (Site to Site) under Connectivity in the left side menu.
11. In the middle of the page, click the X next to the Hub Association: Connected to this Hub text.

12. In the table on the bottom of the page, select the new VPN site and click Connect VPN sites in the menu of the bottom table.

   The Connect Sites dialog appears.

13. Retain the settings in the Connect Sites dialog and click Connect at the bottom of the dialog.

Create the Second VPN Site (Using EC-V-B Details)

Follow the steps in the previous section for each VPN site in your configuration.

When entering the public IP address and the peering address, enter values relevant for the subject EC-V.

**IMPORTANT** Each EC-V must have a different Loopback interface IP address (BGP address).

**Next Step:** Proceed to Create the Virtual Network Connections on the next page
Create the Virtual Network Connections

This procedure creates a virtual network connection from Azure Virtual Hub to the Spoke virtual networks. As shown in Figure 21, the architecture has two Spoke virtual networks: Spoke-VNet-A (10.8.0.0/16) and Spoke-VNet-B (10.9.0.0/16).

This procedure assumes the two virtual networks were previously created. The names and address spaces used by the guide example are vn_SPOKE-1 (10.8.0.0/16) and vn_SPOKE-2 (10.9.0.0/16).

Connect the First Spoke Virtual Network

1. From the Virtual WAN page, select **Virtual network connections** from the Connectivity menu (left-side column).
   The Virtual network connections page opens for the Virtual WAN.

2. Click + Add Connection in the button bar at the top of the page.
   The Add Connection panel opens on the right side of the page.

3. Enter values to connect the first spoke virtual network to the virtual hub:
   - **Connection name**: Enter a name for the connection.
     Guide example is **hub_SPOKE-A**
   - **Hubs**: Select the hub previously created.
     Guide example is **vh_HUB-1**
   - **Subscription**: (drop-down) Depends on your Azure account.
     Guide example is **Pay-As-You-Go**
     Guide example is **SP-Tech**
   - **Virtual Network**: (drop-down) Select the virtual network for the first spoke network.
     Guide example is **vn_SPOKE-1**

4. Click OK at the bottom of the panel.

   The Add Connection panel disappears and the Virtual network connections page updates to display the new connection.

Connect the Second Spoke Virtual Network

Repeat steps in the previous section to connect the Spoke-B network to the virtual hub.

Next Step: Proceed to [Download the Virtual Hub's VPN Configuration File on the next page](#)
Download the Virtual Hub's VPN Configuration File

The virtual hub's VPN configuration file is a text file that contains the virtual hub's IP addresses (public and private), IPsec parameters, and other information required to establish BGP over IPsec tunnels from the EC-V. This information is used in the Create IPsec Tunnels from the EC-Vs to the Azure Virtual Hub procedure.

Complete the following steps to download the virtual hub's VPN configuration file.

1. On the Virtual WAN page, select VPN sites from the Connectivity menu (left-side column). The VPN sites page opens.

2. Click Download Site-to-Site VPN configuration in the button bar at the top of the page.

   The Download Site-to-Site VPN configuration panel opens on the right side of the page.

3. Click Click here to download the link.

   A configuration file starts downloading. This file contains the details to create IPsec tunnels and BGP sessions from each EC-V to the Azure Virtual Hub. The VPN configuration text file is stored in an Azure Storage Account on the same region where the Azure Virtual Hub is deployed.

   **IMPORTANT** If you are unable to download the VPN configuration file due to a permission error, ask your organization's Cloud Administrator to download the file on your behalf. Currently, when you deploy a Virtual WAN, Azure selects a Resource Group and a Storage Account for this operation instead of prompting you for a Storage Account. If you do not have access to the selected Resource Group or Storage Account, you will be unable to download the VPN configuration file.

4. After the VPN configuration is downloaded, open it on a text editor.

5. Convert the text using a JSON formatter.

   If your text editor does not convert to JSON, use an online JSON formatter such as https://jsonformatter.org/. The configuration file contains two sections – one for each EC-V (or site).

The VPN Configuration file shown in Figure 23 provides tunnel parameter settings for a single EC-V appliance. The file that you download replicates this information for each EC-V in your configuration:

In each section, the gatewayConfiguration > IpAddresses code lists two public IP addresses, labeled instance0 and instance1. The Create IPsec Tunnels from the EC-Vs to the Azure Virtual Hub section uses these addresses as the Azure Virtual Hub's IPsec tunnel endpoints.
Figure 23. VPN Configuration text file

```json
{
    "configurationVersion": {
        "LastUpdatedTime": "2019-07-31T07:41:31.4132645Z",
        "Version": "c7beac21-648e-491e-a341-6f80a4053fe6"
    },

    "vpnSiteConfiguration": {
        "Name": "US-East-2-EC-V-A",
        "IPAddress": "52.254.56.97",
        "BgpSetting": {
            "Asn": 64520,
            "BgpPeeringAddress": "10.254.10.1",
            "PeerWeight": 32768
        },
        "LinkName": "US-East-2-EC-V-A"
    },

    "vpnSiteConnections": [
        "hubConfiguration": {
            "AddressSpace": "10.7.0.0/16",
            "Region": "East US 2",
            "ConnectedSubnets": ["10.8.0.0/16", "10.9.0.0/16"]
        },

        "gatewayConfiguration": {
            "IpAddress": {
                "Instance0": "20.44.80.170",
                "Instance1": "20.44.81.51"
            },

            "BgpSetting": {
                "Asn": 65515,
                "BgpPeeringAddresses": {
                    "Instance0": "10.7.0.6",
                    "Instance1": "10.7.0.7"
                },
                "PeerWeight": 0
            }
        },

        "connectionConfiguration": {
            "IsBgpEnabled": true,
            "PsK": "ec-v-a-psk18",
            "IPsecParameters": {
                "SADatasetSizeInKilobytes": 102400000,
                "SALifeTimeInSeconds": 3600
            }
        }
    ]
}
```

Next Step: Proceed to Create IPsec Tunnels from the EC-Vs to the Azure Virtual Hub on page 71
Traffic Redirection in the HA Deployment (Azure Virtual Hub)

Creating BGP over IPsec tunnels from EC-V appliances to the Azure Virtual Hub redirect traffic consists of the following steps:

- Create IPsec Tunnels from the EC-Vs to the Azure Virtual Hub
- Create a Loopback Interface on an EC-V
- Create VTIs on the EC-Vs
- Create Static Routes on the EC-Vs
- Configure BGP Sessions on EC-V
- Configure EC-V Failover mode

Figure 24 displays the logical resources that are required to redirect traffic through the Azure Virtual Hub.

Figure 24. Traffic Redirection Through the Azure Virtual Hub
Create IPsec Tunnels from the EC-Vs to the Azure Virtual Hub

This section creates two IPsec tunnels from the EC-V appliances to the Azure Virtual Hub.

Configuring the Tunnels on ECV-A

Configuring the First Tunnel on ECV-A

1. Select **ECV-A** in the Orchestrator appliance menu and open the **Tunnels** tab (*Configuration > Network > Tunnels > Tunnels*).
2. Click **Passthrough** (located above the table).
3. Open the **Tunnels** dialog by clicking an **edit icon**.
4. Click **Passthrough** (located above the table).
5. Open the **Add Passthrough Tunnel** by clicking **Add Tunnel** and enter these values:
   - **Alias**: Enter a name for your IPsec tunnel. Guide Example: *tun_ECV-A1*
   - **Mode**: (drop-down) Select **IPSec**
   - **Admin**: (drop-down) Select **up**
   - **Local IP**: (drop-down) Select the ECV-A LAN0 interface's private IP address. Guide Example: *10.6.3.10*
   - **Remote IP**: Enter the **Azure Hub Instance0 public IP address**
     VPN Configuration file (Figure 23) – Letter “A” Guide Example: *20.44.80.170*
   - **NAT**: Select **none**
   - **Peer/Service**: Optional
   - **Auto Max BW Enabled**: (Selection box) **Checked**
   - **Max BW Kbps**: Locked when **Auto Max BW Enabled** is selected.

Selecting **IPSec** as the **Mode** provides access to **IKE** and **IPsec** edit popups.

6. Select **IKE** at the top of the popup and enter the following values:
   - **IKE Version**: (drop-down) Select **IKE v2**
   - **Preshared Key**: Enter the PSK. VPN Configuration file (Figure 23) – Letter “B”
   - **Authentication Algorithm**: (drop-down) Select **SHA1**
   - **Encryption Algorithm**: (drop-down) Select **AES-256**
【Diffie-Hellman Group】: (drop-down) Select 2
【Rekey Interval/Lifetime】: (minutes) Enter 1440
【Delay time (Dead Peer Detection)】: (seconds) Enter 10
【Retry Count (Dead Peer Detection)】: Value locked at 3
Retry count field is not editable by user.

【Local IKE Identifier (Data field)】: Enter EC-V LAN0 interface public IP address.
VPN Configuration file: Figure 23 – Letter “C”
Guide Example: 52.254.56.87

【Remote IKE Identifier (Data field)】: Enter Azure Hub Instance0 public IP address.
VPN Configuration file: Figure 23 – Letter “A”
Guide Example: 20.44.80.170

【Phase 1 Mode】: (drop-down) Select Aggressive

7. Select IPsec at the top of the popup and enter these values:
   - 【Authentication Algorithm】: (drop-down) Select SHA1
   - 【Encryption Algorithm】: (drop-down) Select AES-256
   - 【Enable IPsec Anti-replay Window】: (checkbox) Check
   - 【Rekey Interval】: (minutes) Enter 60
     VPN Configuration file (Figure 23) – Letter “D”) lists this value in seconds.
   - 【Rekey Lifetime】: (megabytes) Enter 102400
     VPN Configuration file (Figure 23) – Letter “E”) lists this value in Kilobytes.
   - 【Perfect Forward Secrecy Group】: Enter 2

8. Close the Add Passthrough Tunnel popup by clicking Save at the bottom of the popup.
9. Close the Tunnels popup by clicking Close at the bottom of the popup.
10. Click the Refresh icon after a few seconds.
    The IPsec tunnels appear with an Up-active status.

### Configuring the Second Tunnel on ECV-A

Establish the second tunnel using Configuring the First ECV-A Tunnel steps. Data differences:

- Step 5: 【Remote IP】: Use the Azure Hub instance1 public IP address.
- Step 6: 【Remote IKE Identifier】: Use the Azure Hub instance1 public IP address.
Configuring the Tunnels on ECV-B

Create two tunnels on EC-V-B by following the instructions in the Configuring the Tunnels on ECV-A and Configuring the First Tunnel on ECV-A sections.

Verifying the Tunnels

Verify the tunnel configuration from the Tunnels page (Configuration > Tunnels > Tunnels). Figure 25 displays the four IPSec tunnels on both EC-Vs.

Figure 25. Tunnels Table – Orchestrator Tunnels Page

Next Step: Proceed to Create a Loopback Interface on an EC-V on the next page
Create a Loopback Interface on an EC-V

This section creates Loopback interfaces on each EC-V appliance.

Previously, when creating VPN Sites in the Azure Portal (Create the VPN Sites), the Loopback interface IP address entered in the BGP address field as the Guide example was 10.254.10.1. This address is used in the following procedure.

**Configure the EC-V-A Loopback Interface**

1. Select ECV-A in the Orchestrator appliance menu and open the Loopback Interfaces page (Configuration > Networking > Loopback Interfaces).
2. Click an edit icon in the Tunnels table to open the Loopback Interfaces panel.
3. Click Add on the upper left corner of the panel to open the Add Interface popup and enter these values.
   - **Interface lo**: Enter an Interface number. Guide example is 1
   - **IP/Mask**: Enter the IP address/mask used on the Azure Portal under BGP address. Guide example: 10.254.10.1 / 24
   - **Admin**: Select up
   - **Label**: Optional
   - **Zone**: Optional
4. Click Apply in the bottom right corner of the popup.

**Configuring the EC-V-B Loopback Interface**

Create a Loopback interface on EC-V-B by following steps in the preceding section. EC-V appliances cannot use identical Loopback interface IP addresses.

Next Step: Proceed to Create VTIs on the EC-Vs on the next page
Create VTIs on the EC-Vs

After creating the Loopback interfaces on the EC-Vs, create two VTIs on each EC-V and associate the IPsec tunnels to them.

Configuring the First VTI on ECV-A

1. Select ECV-A in the Orchestrator appliance menu and open the Virtual Tunnel Interfaces (VTI) tab (Configuration > Networking > Virtual Tunnels Interfaces (VTI)).
2. Click an edit column icon in the Tunnels table to open the Virtual Tunnel Interfaces (VTI) popup.
3. Click Add (upper left corner) to open the Add VTI Interface dialog and enter these values.
   - **Interface**: Select vti0
   - **IP/Mask**: Enter an IP address that does not overlap with 1) any IP address range in your on-premises networks, 2) your Azure virtual networks, and 3) the Hub virtual network. Guide example: 10.254.10.2/32
   - **Admin**: Select up
   - **Passthrough Tunnel**: (drop-down) Select the first IPsec tunnel (to Azure instance0 public IP address) created on the EC-V. Guide Example: tun_ECV-A1
   - **Direction**: Specifies the direction for establishing the IPsec tunnel to the Virtual Hub. Select wan when creating an IPsec tunnel from the WAN0 interface. Select lan when creating an IPsec tunnel from the LAN0 interface. Guide Example: Select lan – The IPsec tunnel is created on the LAN0 interface.
   - **Label**: Select NONE
   - **Zone**: Use the Default setting.
4. Click Add (bottom of dialog) to save the values and close the Add VTI Interface dialog.
5. Click Apply (bottom right corner) to close the Virtual Tunnel Interfaces (VTI) panel.

Configuring the Second VTI on ECV-A

Create the second VTI interface on ECV-A. Step 3 differences:

- **IP/Mask** use a different IP address than VTI0 address. Guide Example: 10.254.10.3/32
- **Passthrough tunnel** use the second IPsec tunnel name. Guide Example: tun_ECV-A2

Configuring VTI on ECV-B

Follow the previous instructions to create two VTIs on EC-V-B.
Verify VTI Configurations

Verify tunnel configuration parameters from the Virtual Tunnel Interfaces (VTI) page.

Next Step: Proceed to Create Static Routes on the EC-Vs on the next page
Create Static Routes on the EC-Vs

The EC-Vs require static routes to establish BGP sessions to the Azure Virtual Hub because the IP address of the EC-V loopback interface is in a different subnet from the Azure Virtual Hub's private IP addresses.

Configuring the First Static Route on ECV-A

1. Select ECV-A in the Orchestrator appliance menu and open the Routes page (Configuration > Networking > Routing > Routes).
2. Open the Routes panel by clicking an edit icon and enter these values.
   - **Automatically advertise local LAN subnets**: (selection box) Check
   - **Automatically advertise local WAN subnets**: (selection box) Uncheck
   - **Metric for automatically added subnets**: Enter 50
   - **Redistribute routes to SD-WAN Fabric**: (drop-down) Select an available route map. The selected route map is modified in a subsequent step.
     - Guide Example: default_rtmp_to_subsh
   - **Filter Routes From SD-WAN Fabric With Matching Local ASN**: (selection box) Uncheck
   - **Include BGP Local ASN to routes sent to SD-WAN Fabric**: (selection box) Check
   - **Communities**: (data field): Content is optional
3. Open the SD-WAN Fabric Route Redistribution Maps popup by clicking the Redistribute routes to SD-WAN Fabric edit icon.
   - Add rules to allow traffic from Local/Static and BGP source protocols (Figure 26).
   - Click **Apply** (lower right corner) to close the popup and return to the Routes popup.

*Figure 26. SD-WAN Fabric Route Redistribution Maps popup*
4. Click **Add Route** (top of the popup) to open the **Add Route** popup and enter these values:
   - **Subnet/Mask**: Enter the Azure Hub’s instance0 BGP Peering Address.
     VPN Configuration file: **Figure 23** – Letter “F”
     Guide example: Enter **10.7.0.6/32**.
   - **Next Hop**: Enter the Azure Hub Instance0 public IP Address.
     VPN Configuration file: **Figure 23** – Letter “A”
     Guide example: Enter **20.44.80.170/32**.
   - **Interface**: Enter **vti0**
   - **Metric**: Enter **50**
   - **Tag**: Select the opposite tag from where the BGP sessions are being built.
     Guide example: Select **FROM_LAN**
   - **Comments**: Optional

5. Click **Add** to close the **Add Route** popup and return to the **Routes** panel.

6. Click **Apply** to close the **Routes** panel and return to the **Routes** page.

### Configuring the Second Static Route on ECV-A

Create the second static route by using steps in the preceding section. This route establishes the second BGP session with the Azure Virtual Hub via the second IPsec tunnel.

Note the following step 3 differences:
   - **Subnet/Mask**: use the instance1 private IP address. Guide example: **10.7.0.7/32**
   - **Next Hop**: use the instance1 public IP address. Guide example: **22.44.81.51/32**
   - **Interface**: Select **vti1**

### Configuring Static Routes on ECV-B

Create two static routes on EC-V-B by following steps in the preceding sections.
Verify the Static Routes

Verify the tunnel configuration from the Orchestrator Routes page.

**Figure 27** displays the four static routes on ECV-A and ECV-B.

**Figure 27. Routes Table – Orchestrator Routes Page**

<table>
<thead>
<tr>
<th>Edit</th>
<th>Appliance Name</th>
<th>Subnet/Mask</th>
<th>Next Hop</th>
<th>Interface</th>
<th>State</th>
<th>Metric</th>
<th>Advertise T...</th>
<th>Type</th>
<th>Additional Info</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>ECV-A</td>
<td>10.7.0.7/32</td>
<td>10.4.1.33</td>
<td>v01</td>
<td>UP</td>
<td>50</td>
<td>50 (40.1)</td>
<td></td>
<td></td>
<td>Tag PROM_LAN</td>
</tr>
<tr>
<td>✓</td>
<td>ECV-A</td>
<td>10.7.0.7/32</td>
<td>10.4.0.279</td>
<td>v00</td>
<td>UP</td>
<td>50</td>
<td>50 (40.1)</td>
<td></td>
<td></td>
<td>Tag PROM_LAN</td>
</tr>
<tr>
<td>✓</td>
<td>ECV-B</td>
<td>10.7.0.7/32</td>
<td>10.4.1.33</td>
<td>v01</td>
<td>UP</td>
<td>50</td>
<td>50 (40.1)</td>
<td></td>
<td></td>
<td>Tag PROM_LAN</td>
</tr>
<tr>
<td>✓</td>
<td>ECV-B</td>
<td>10.7.0.7/32</td>
<td>10.4.0.279</td>
<td>v00</td>
<td>UP</td>
<td>50</td>
<td>50 (40.1)</td>
<td></td>
<td></td>
<td>Tag PROM_LAN</td>
</tr>
</tbody>
</table>

**Next Step: Proceed to Configure BGP Sessions on EC-V on the next page**
Configure BGP Sessions on EC-V

This section creates BGP sessions from the EC-Vs to the Azure Virtual Hub using previously configured loopback interfaces, IPsec tunnels, VTIs, and static routes.

Configure the First BGP Session on ECV-A

1. Select ECV-A in the Orchestrator appliance menu and open the BGP page (Configuration > Networking > Routing > BGP).
2. Open the BGP panel by clicking an edit icon and enter these values.
   - **Enable BGP**: Select *Enable*
   - **Autonomous System Number**: Enter the EC-Vs BGP ASN.  
     VPN Configuration file: Figure 23 – Letter “G”  
     Guide example: Enter 64520.
   - **Router ID**: The IPv4 address Azure Virtual Hub uses to identify the EC-V for BGP purposes.  
     VPN Configuration file: Figure 23 – Letter “C”  
     Guide example: Enter 52.254.56.87 (LAN0 public IP address).
   - **Graceful Restart**: Optional
   - **AS Path Propagate**: Select *Enable*
3. Click **Add** above the BGP Peers table to open the Add Peer popup and enter these values:
   - **Peer IP**: Enter the Azure Virtual Hub's instance0 BGP Peering Address.  
     VPN Configuration file: Figure 23 – Letter “F”  
     Guide example: Enter 10.7.0.6/32.
   - **Local Interface**: Select the loopback interface.  
     Guide example: Enter lo1.
   - **Peer ASN**: Enter the Virtual Hub's BGP ASN.  
     VPN Configuration file: Figure 23 – Letter “H”  
     Guide example: Enter 65515.
   - **Peer Type**: (drop-down) Select *Branch*
   - **Admin Status**: Select *UP*
   - **Next-Hop-Self**: (Selection box) *Uncheck*
   - **Inbound route map**: (drop-down) Select an available route map.  
     Guide example: Enter default_rmap_bgp_inbound_br
   - **Outbound route map**: (drop-down) Select an available route map.  
     Guide example: Enter default_rmap_bgp_oubound_br
- **Keep Alive Timer**: Enter 30
- **Hold Timer**: Enter 90

4. Modify the `default_rtmag_bgp_oubound_br` Route Map to disable advertising the previously created static route.

By default, the `default_rtmag_bgp_oubound_br` Route Map advertises static routes created locally on the EdgeConnect appliance to the Virtual Hub (EdgeConnect's BGP peer). Disabling previously created static routes from advertising to the Virtual Hub is important because failing to do so can prevent the Virtual Hub from establishing a BGP session with the appliance.

- Click the *Edit* button of the `default_rtmag_bgp_oubound_br` link to open the **BGP Outbound Route Redistribution Maps** popup.
  - The **Source Protocol Local/Static** is set to *Allow*, which advertises all local static routes created on the EdgeConnect to the Virtual Hub.
- Click the *edit* button on the **Source Protocol Local/Static** row to open the **Update Rule** popup.
- Uncheck the *Permit* button (*Figure 28*).
- Click *Update* to save the change and close the **Update Rule** popup.
- Click *Apply* to close the **BGP Outbound Route Redistribution Maps** popup.

*Figure 28. Selecting Bash*

5. Click *Add* to close the **Add Peer** popup and return to the **BGP** panel.
6. Click *Apply* to close the **BGP** panel and return to the **BGP** page.
7. Click refresh after a few seconds.

Remaining BGP parameters are modified when Failover Mode (active-standy or active-active) is configured (*Configure EC-V Failover mode*).
Configure the Second BGP Session on ECV-A

Create the second BGP session to the virtual hub by following the steps in the preceding section. Note the following step 3 differences:

- **Peer IP**: use the instance1 private IP address. Guide example: `10.7.0.7/32`
  
  When both BGP sessions use the same BGP Outbound Route Map (`default_rtm_bgp_outbound_br`) the Route Map does not need to be edited again. If you assign a different BGP Route Map to the second BGP session, that Route Map must be edited to prevent Source Protocol Local/Static routes from being advertised to the Virtual Hub via BGP.

Configure BGP Sessions on ECV-B

Establish two BGP sessions on ECV-B with the hub, by using instructions in the two preceding sections.

Disable Source Protocol Local/Static routes from being advertised to the Virtual Hub on EC-V-B in a manner similar to the method that they are disabled on EC-V-A.
Verify the BGP Sessions

Figure 29 displays the two BGP sessions created from EC-V-A’s Loopback interface to the Hub across the two IPsec tunnels. The Peer State of both BGP sessions appear as “Established” as shown in Figure 30.

Figure 29. BGP sessions on the Flows page on EC-V-A

![Image](image.png)

Figure 30. EC-V-A’s both BGP sessions to the Azure Virtual Hub

Navigate to Flows tab to confirm the BGP sessions are going over the created IPsec tunnels.

Click the Include Built-in checkbox and filter by BGP on the Application field.

Use the following list to determine your next topic:

- Single EC-V Deployment with BGP routing: The Virtual Hub Deployment is completed for the single appliance deployment.
- HA Deployment using Azure Virtual Hub: Configure EC-V Failover mode on the next page

Next Step: Proceed to the section specified by your deployment selection
Configure EC-V Failover mode

You can configure the EC-Vs in one of two failover modes:

- Active-Standby failover mode – Configure EC-V in Active-Standby failover mode
- Active-Active failover mode – Configure EC-Vs in Active-Active failover mode

Configure EC-V in Active-Standby failover mode

In Active-Standby failover mode, traffic between the on-premises network and the Azure workloads traverses only the active Azure EC-V. If that EC-V fail and both BGP sessions to the Azure Hub are down, traffic is sent across the standby EC-V.

To configure Active-Standby failover mode, configure the *Autonomous System (AS) Prepend Count* value and *Metric* value on each appliance such that ECV-A values are smaller than values on ECV-B.

- The *AS Prepend Count* is configured in the **BGP outbound Route Redistribution Map**.
- The *Metric* is configured in the **BGP inbound Route Redistribution Map**.

In Active-Standby failover mode, traffic between the on-premises network and the Azure workloads traverses only the active Azure EC-V. If that EC-V fail and both BGP sessions to the Azure Virtual Hub are down, traffic is sent across the standby EC-V.

**IMPORTANT** As of June 2020, EdgeConnect does not support BGP ECMP (Equal Cost Multi-Path or BGP multi-path load sharing). As a result, even if you enter identical BGP path attributes on both BGP sessions on a single EC-V, the EC-V picks only one path to send and receive traffic to and from the Azure Virtual Hub.

**Active-Standby Configuration Parameters**

The following instructions configure the EC-Vs in Active-Standby failover mode by configuring ECV-A's *AS Prepend Count* and *Metric* values such that the ECV-A values are smaller than the values on ECV-B. This makes ECV-A the preferred EdgeConnect for receiving and sending inbound and outbound traffic to and from Azure workloads.

These values are assigned to route maps that manage BGP route distribution:

- ECV-A BGP session 1: Metric = 1 and AS Prepend Count = 1
- ECV-A BGP session 2: Metric = 2 and AS Prepend Count = 2
- ECV-B BGP session 1: Metric = 3 and AS Prepend Count = 3
- ECV-B BGP session 2: Metric = 4 and AS Prepend Count = 4

You only need to modify the Metric value and the AS Prepend Count value on each BGP session to the Virtual Hub. All other BGP path attributes can remain the same (default values) on each BGP session.
Configuring the First BGP Session on ECV-A

These instructions configure the first BGP session on ECV-A:

1. Select ECV-A in the Orchestrator appliance menu and open the BGP page (Configuration > Networking > Routing > BGP).
2. Open the BGP popup by clicking an icon in the edit column.
3. Open the Update Peer popup for the first BGP session by clicking the icon in the edit column in the row for the peer corresponding to the first BGP session.
   Refer to Configure BGP Sessions on EC-V if you are unsure as to which peer corresponds to the first BGP session.
4. Select the Inbound route map for the specified route map (as configured in Configure BGP Sessions on EC-V) and click its edit icon to open the BGP inbound Route Redistribution Maps popup.
5. Click the icon in the edit column for the BGP source protocol to open the Update Rule popup.
6. Select the Metric checkbox and enter 1 in the data field.
7. Click the Update button in the Update Rule popup and the Apply button in the the BGP inbound Route Redistribution Maps popup.
8. Select the Outbound route map for the specified route map (as configured in Configure BGP Sessions on EC-V) and click its edit icon to open the BGP outbound Route Redistribution Maps popup.
9. Click the icon in the edit column for the BGP source protocol to open the Update Rule popup.
10. Select the ASN Prepend Count checkbox and enter 1 in the data field.
11. Click Update in the Update Rule popup, Apply in the the BGP inbound Route Redistribution Maps, and Update in the Update Peer popup.
Configuring the Second BGP Session on ECV-A

These instructions configure the second BGP session on ECV-A. The process is similar to configuring the first session. Parameters in Steps 4 and 8 configure different parameter values from the first session.

1. Open the **Update Peer** popup for the second BGP session by clicking the icon in the *edit* column in the row of the peer corresponding to the second BGP session.
   
   Refer to **Configure BGP Sessions on EC-V** if you are unsure as to which peer corresponds to the second BGP session.

2. Select the **Inbound route map** for the specified route map (as configured in **Configure BGP Sessions on EC-V**) and click its edit icon to open the **BGP inbound Route Redistribution Maps** popup.

3. Click the icon in the edit column for the **BGP** source protocol to open the **Update Rule** popup.

4. Select the **Metric** checkbox and enter 2 in the data field.

5. Click the Update button in the **Update Rule** popup and the Apply button in the **BGP inbound Route Redistribution Maps**.

6. Select the **Outbound route map** for the specified route map (as configured in **Configure BGP Sessions on EC-V**) and click its edit icon to open the **BGP outbound Route Redistribution Maps** popup.

7. Click the icon in the edit column for the **BGP** source protocol to open the **Update Rule** popup.

8. Select the **ASN Prepend Count** checkbox and enter 2 in the data field.

9. Click **Update** in the **Update Rule** popup, **Apply** in the **BGP inbound Route Redistribution Maps** popup, **Update** in the **Update Peer** popup, and **Apply** in the **BGP** popup.
Configuring the First BGP Session on ECV-B

These instructions configure the first BGP session on ECV-B. The process is similar to configuring the first session on ECV-A. Parameters in Steps 6 and 10 configure different parameter values from the first EC-V.

1. Select ECV-B in the Orchestrator appliance menu and open the BGP page (**Configuration > Networking > Routing > BGP**).
2. Open the BGP popup by clicking an icon in the *edit* column.
3. Open the **Update Peer** popup for the first BGP session by clicking the icon in the *edit* column in the row for the peer corresponding to the first BGP session.
   - Refer to **Configure BGP Sessions on EC-V** if you are unsure as to which peer corresponds to the first BGP session.
4. Select the **Inbound route map** for the specified route map (as configured in **Configure BGP Sessions on EC-V**) and click its edit icon to open the **BGP inbound Route Redistribution Maps** popup.
5. Click the icon in the *edit* column for the BGP source protocol to open the **Update Rule** popup.
6. Select the **Metric** checkbox and enter 3 in the data field.
7. Click the Update button in the **Update Rule** popup and the Apply button in the the **BGP inbound Route Redistribution Maps** popup.
8. Select the **Outbound route map** for the specified route map (as configured in **Configure BGP Sessions on EC-V**) and click its edit icon to open the **BGP outbound Route Redistribution Maps** popup.
9. Click the icon in the edit column for the BGP source protocol to open the **Update Rule** popup.
10. Select the **ASN Prepend Count** checkbox and enter 3 in the data field.
11. Click **Update** in the **Update Rule** popup, **Apply** in the the **BGP inbound Route Redistribution Maps**, and **Update** in the **Update Peer** popup.
Configuring the Second BGP Session on ECV-B

These instructions configure the second BGP session on ECV-B. The process is similar to configuring the second session on ECV-A. Parameters in Steps 4 and 8 configure different parameter values from ECV-A.

1. Open the Update Peer popup for the second BGP session by clicking the icon in the edit column in the row of the peer corresponding to the second BGP session.
   
   Refer to Configure BGP Sessions on EC-V if you are unsure as to which peer corresponds to the second BGP session.

2. Select the Inbound route map for the specified route map (as configured in Configure BGP Sessions on EC-V) and click its edit icon to open the BGP inbound Route Redistribution Maps popup.

3. Click the icon in the edit column for the BGP source protocol to open the Update Rule popup.

4. Select the Metric checkbox and enter 4 in the data field.

5. Click the Update button in the Update Rule popup and the Apply button in the the BGP inbound Route Redistribution Maps.

6. Select the Outbound route map for the specified route map (as configured in Configure BGP Sessions on EC-V) and click its edit icon to open the BGP outbound Route Redistribution Maps popup.

7. Click the icon in the edit column for the BGP source protocol to open the Update Rule popup.

8. Select the ASN Prepend Count checkbox and enter 4 in the data field.

9. Click Update in the Update Rule popup, Apply in the the BGP inbound Route Redistribution Maps popup, Update in the Update Peer popup, and Apply in the BGP popup.

Next Step: The Virtual Hub Deployment is completed for active-standby failover mode.
Configure EC-Vs in Active-Active failover mode

You can configure the EC-Vs in Active-Active failover mode to increase throughput between the on-premises network and the Azure workloads. An IPsec connection to the Azure Virtual Hub supports up to 1 Gbps. As a result, in an active-active configuration, each EC-V can support 1 Gbps of throughput to the Azure Virtual Hub.

Configuring EC-Vs in Active-Active failover mode requires that each BGP path attribute be the same on both inbound and outbound route redistribution maps.

When all BGP path attributes are identical on each EC-V, the Azure Virtual Hub uses Equal Cost Multi Path (ECMP) routing for outbound traffic from Azure. Similarly, inbound traffic to the Azure Virtual Hub from each EC-V will also use ECMP routing on the EC-V appliances.

Next Step: Proceed to Enable Flow Redirection on the next page
Enable Flow Redirection

Flow redirection is a method by merging the traffic of an asymmetric flow into a single appliance, thus removing the flow asymmetry. Figure 31 depicts the redirection of a traffic flow through ECV-A

**IMPORTANT** Flow Redirection works only for TCP traffic.

*Figure 31. Flow Redirection – Azure Hub Topology*

Deploying EC-Vs in an active-active configuration increases available bandwidth for workloads deployed in Azure. However, this results in asymmetric flows as the Azure Virtual Hub has two separate paths (via ECV-A and ECV-B) to forward traffic to the remote site. Asymmetric flows do not affect most applications. However, if firewalls are deployed on the LAN-side of the EC-Vs in Azure (see Figure 20) asymmetric flows will cause the firewall to drop traffic unless you specifically allowed such traffic in the firewall. This is because the firewall has not seen the (first) incoming packet from the remote network.

If you have firewalls in your Azure deployment as shown in Figure 20, you can avoid flow asymmetry by enabling Source Network Address Translation (SNAT) on the firewall. If firewalls are not deployed
in Azure (Figure 21) you can enable SNAT on the EC-Vs to avoid flow asymmetry. The following instructions assume that you do not have firewalls in your environment and that you have not enabled SNAT on the EC-Vs. In such situations, you can enable the Flow Redirection feature to avoid flow asymmetry.

In the deployment shown in Figure 21, the LAN0 interface of both EC-Vs are on the same subnet. As a result, you can configure Flow Redirection on the LAN0 interface on the EC-Vs.

Flow Redirection is configured from the EdgeConnect Appliance Manager. Flow Redirection is not configurable on Orchestrator (as of June 2020). Complete the following steps to enable flow redirection.

**IMPORTANT** Optimizing TCP flows requires that a client request and its server response use the same path through the EdgeConnect appliances. Therefore, configuring Flow Redirection is required to optimize TCP traffic using Silver Peak Boost (WAN optimization) technology.

**Configuring Flow Redirection on ECV-A**

1. Open EC-V-A’s Appliance Manager Web UI.
2. Open the Flow Redirection page *Configuration > Flow Redirection* and enter these settings:
   - **Enable**: (Selection box) check
   - **Wait Time**: Enter 50 ms
   - **Interface**: Select *lan0*
3. Click *Add Peer*.
4. Enter EC-V-B’s Lan0 IP address.
5. Click *Apply*.
   The state column will change to *Unreachable*.

**Configuring Flow Redirection on ECV-B**

Configure flow redirection on EC-V-B by following steps in the preceding section.

After flow redirection is configured on each EC-V, the state should appear as *OK*.

**Next Step: The Virtual Hub Deployment is completed.**
EC-V HA Deployment: Azure Internal Load Balancer

This section illustrates deploying EC-Vs with the Azure Standard Internal Load Balancer. EC-V appliances can be scaled horizontally to increase throughput and redundancy using the Azure Standard Internal Load Balancer (ILB).

Background Topics

The following topics provide information about implementing EC-V appliances with an Azure ILB:

- Azure Load Balancer and the EC-V Architecture
- Prerequisites to Deploying EC-V with Azure Standard Internal Load Balancer

Configuration Topics

The following procedures implement the EC-V HA deployment depicted in Figure 32 or Figure 33. These procedures can be used as a model for deploying any EC-V architecture with Azure ILB.


2. Repeat Steps A through C for each EC-V appliance to be deployed:
   A. Create an EC-V Appliance in the Azure Portal on page 12
   B. Configure the EC-V on page 24
   C. Create Data Path Interfaces on page 31

   IMPORTANT Data Path Interfaces are configured after configuring the Internal Load Balancer. Do Not perform the Single Deployment Data Path Interfaces procedures.

3. Create an Azure Standard Internal Load Balancer on page 99

4. Configure a Health Probe (Health Probe Traffic in the HA Deployment (Azure ILB) on page 106)

5. Configure traffic redirection (Traffic Redirection in the HA Deployment (Azure ILB) on page 110)

Use the following list to determine your next topic:

- To review background information first: Azure Load Balancer and the EC-V Architecture on the next page
- To begin configuration immediately: Topology – EC-V Deployment (Azure ILB) on page 96

First Step: Proceed to your selected section
Azure Load Balancer and the EC-V Architecture

Azure Load Balancer Overview

Azure Load Balancers distribute inbound flows that arrive at the load balancer’s frontend IP address to backend pool instances. Backend pool instances are the VMs to where the load balancer forwards traffic. In our design, the backend pool instances are the EC-Vs that are deployed in Azure.

Azure offers two load balancer SKUs: Basic and Standard. Although the Basic Load Balancer is free, we do not use it for the following reasons:

- It does not support TCP and UDP flows on all ports simultaneously.
- It cannot forward traffic to VMs in different Availability Zones.

We use the Azure Standard Internal Load Balancer to support EC-V HA. Azure guarantees that a Standard Load Balancer, serving two or more healthy Virtual Machine instances, is available 99.99% of the time.

Visit the following page for details about Azure Load Balancers:

Standard Internal Load Balancer Functions Within an EC-V HA Architecture

Azure Load Balancers operate at layer four of the Open Systems Interconnection (OSI) model. The Azure Load Balancer in our deployment is called an Internal or private load balancer because it is only exposed to Azure workloads. The Internal Load Balancer (ILB) distributes outbound (Azure-to-on-premises) flows it receives from Azure workloads to backend pool instances (EC-Vs). These flows are specified by configured load balancing rules and health probes.

Azure Standard ILBs support forwarding outbound traffic from Azure workloads to multiple, healthy EC-V instances deployed in Azure. Standard Internal Load Balancer can be used to horizontally scale EC-Vs to support high availability and increased throughput for Azure workloads and services.

Available Failover modes with the Azure Standard Internal Load Balancer

EC-V can only be deployed in active-active failover mode with Azure Standard Internal Load Balancer (as of June 2020). Active-standby is not a valid option because Azure load balancer session persistence algorithms do not support sending outbound (Azure to on-premises) traffic from all Azure workloads to a single back end pool VM (active EC-V) and failover traffic to another VM (standby EC-V) only when the active VM (active EC-V) fails.

Azure Standard Internal Load Balancer and Dynamic Routing

Azure Standard Internal Load Balancer does not support BGP. To advertise Azure virtual network address ranges (or subnets) to the SD-WAN fabric, you must create static routes in your Azure EC-Vs. Similarly, to forward outbound traffic from the Azure workloads to the Standard Internal Load Balancer, you must create static routes (UDRs) in the Azure Route Table.
Detection of EC-V Failures

TCP health probes that are configured on the Standard Internal Load Balancer to monitor an interface of an EC-V can detect a failure of an EC-V when it stops receiving responses to its health probes.

Azure Load Balancer pricing

Visit the following page for pricing details:

Next Step: Proceed to Prerequisites to Deploying EC-V with Azure Standard Internal Load Balancer on the next page
Prerequisites to Deploying EC-V with Azure Standard Internal Load Balancer

- All Single EC-V Deployment prerequisites, as listed on Prerequisites to Deploying EC-V in Azure.
- When deploying EC-Vs in a region that supports Availability Zones (AZs), place each EC-V in unique AZs.
  As of February 2020, several Azure regions do not support AZs.
- When deploying EC-Vs in a region that does not support AZs, place all EC-Vs in a single Availability Set to protect against Azure hardware failures.
  An Availability Set ensures that the deployed EC-Vs are distributed across multiple, isolated hardware nodes, in a cluster. If you are deploying EC-Vs in a region that supports AZs, instead of placing EC-Vs in an Availability Set, you must deploy them in unique AZs.
- Both EC-Vs must be deployed on the same virtual network.
  Azure Virtual Networks (VNets), subnets, and load balancers are regional resources – not zonal. Therefore, only one MGMT0, WAN0, and LAN0 subnet is required for both EC-Vs as shown in Figure 32.
- An Azure Standard Load Balancer requires Standard SKU Public IPs on the VMs deployed on the backend pool.
  In the sample deployment, VMs on the backend pool are the EC-Vs. As a result, when creating public IPs on the EC-V, assign Standard Public IPs to the appliances instead of Basic Public IPs.
- Azure workloads can exist either on the same virtual network where your EC-Vs and the ILB are deployed or on a different virtual network.
  When deploying EC-Vs on an existing virtual network where your workloads already reside, deploy the ILB on the same virtual network as the EC-Vs.
  When deploying EC-Vs and the ILB on a different virtual network than the workloads, a virtual network Peering session between the two virtual networks is required is because the virtual networks do not communicate with each other by default, as shown in Figure 32.
- Whether you deploy the EC-V and the ILB on the same virtual network as the workloads or on a different virtual network, static routes on the Azure Route Table are required to forward outbound traffic from the workload subnets to the private (frontend) IP address of the ILB.
- Instead of creating a Network Security Group (NSG) for each vNIC on each EC-V, you can create one NSG for both MGMT0 interfaces, one NSG for both WAN0 interfaces, and one NSG for both LAN0 interfaces. This simplifies the management of firewall rules applied on each vNIC.

Next Step: Proceed to Topology – EC-V Deployment (Azure ILB) on the next page
Topography – EC-V Deployment (Azure ILB)

The deployment of an EC-V with Azure Internal Load Balancer depends on the location of the workloads:

- **Workloads in the same virtual network as the EC-Vs and ILB**: Static routes are required on the virtual network route table. Figure 32 displays the topology of an active-active EC-V deployment using an Azure Standard Internal Load Balancer with EC-Vs, ILB, and workload deployed in the same virtual network.

  Figure 32. Logical topology of an HA EC-V deployment with an Azure Standard Internal Load Balancer: EC-Vs and workloads are deployed in the same virtual network.

- **Workloads deployed in a different virtual network than the EC-Vs and the ILB**: A virtual network Peering session between the workload’s virtual network and the virtual network where the EC-Vs are deployed is required, in addition to static routes on the virtual network’s route table. Figure 33 displays the topology of an active-active EC-V deployment using an Azure Standard Internal Load Balancer that includes a peering session to the workloads.
Figure 33. Logical topology of an HA EC-V deployment with an Azure Standard Internal Load Balancer: EC-Vs and workloads are deployed in different virtual networks.

Deployment considerations for implementing each EC-V with an Azure ILB includes:

- If the selected Azure region supports Availability Zones (AZ), place each EC-V in different AZs.
- If the selected region does not support AZs, place each EC-V in the same Availability Set. Placing all EC-Vs in one availability set ensures that at least one EC-V continues running when a hardware or software failure incapacitates one rack in the selected Azure data center.
- Use Standard public IP addresses when assigning public IP addresses to EC-V interfaces.

**IMPORTANT** Do not assign basic public IP addresses to any interface.

Before starting the deployment process, assemble the following information:

- **Azure account**: Username and password that accesses your Azure account
- **Azure Resource Group**: Name of the resource group
- **EdgeConnect credentials**: Account name and Account key – received from Silver Peak

**First Step**: Proceed to **Prepare the Resource Group on page 13**
Create an Azure Standard ILB in an EC-V Architecture

Configuration Tasks include:

- Create an Azure Standard Internal Load Balancer
- Create a Backend Pool
- Create a Health Probe
- Create a Load Balancing Rule
- Verify the IP address of the Internal Load Balancer
Create an Azure Standard Internal Load Balancer

1. From the Azure portal, navigate to your Resource group and click +Add in the menu bar.
2. Use the search field to select Load Balancer in the drop-down menu, then click Create to open the Load Balancer page.
3. Verify that Basics is selected in the menu bar and enter settings from the following list:
   - **Project Details**
     - **Subscription**: (drop-down) Depends on your Azure account. Guide example is Pay-As-You-Go
     - **Resource Group**: (drop-down) Select your Resource Group. Guide example is SP-Tech
   - **Instance Details**
     - **Name**: Enter the label for the new Load Balancer. Guide example is 1b_ECV
     - **Region**: (drop-down) Select the region where the EC-V was deployed. Guide example is (US) West US
     - **SKU**: Select Standard
     - **Type**: Select Internal
     - **Tier**: Select Regional (Selection locked when Type is Internal)
4. Click Next: Frontend IP Configuration enter settings from the following list:
   - **Name**: Enter a name for the Frontend IP. Guide example is fe_ECV
   - **Virtual network**: Select the virtual network where you deployed the EC-Vs. Guide example is vn_ECV
   - **Subnet**: Select the LAN0 subnet of the EC-Vs. Guide example is LAN0 (10.6.3.0/24)
   - **IP address assignment**: Select Static or Dynamic Guide example is Static
   - **Private IP address**: If static is selected, enter an available private IP of the LAN0 subnet. Guide example: 10.6.3.13
   - **Availability zone**: Select Zone-redundant
     This parameter is not available in regions that do not support availability zones.
5. Click Next: Backend pools.
   Backend pools are created in the next section.
6. Click Next: Review + create.
Azure displays the **Create load balancer** page. Proceed when the green **Validation passed** bar appears at the top of the page.

7. Click **Create** at the bottom of the page.
   The **Deployment is Underway** page is displayed.

8. When the page displays **Your Deployment is complete**, click **Go to Resource**.
   The **Load Balancer** page is displayed for the new load balancer.

9. Click **Frontend IP configuration** in the Settings menu (left side column) to open the **Frontend IP Configuration** page (Figure 34).

   This page lists the load balancer's frontend IP appears. When creating a static route later, use this private IP as the next hop for outbound traffic from Azure workloads.

**Figure 34. Front-end IP address of the load balancer**

Next Step: Proceed to **Create a Backend Pool on the next page**
Create a Backend Pool

1. Open the **Load Balancer** page (accessible from the **Resource Group** page).
2. Select **Backend pools** from the **Setting** menu to open the **Backend pools** page.
3. Click + **Add** at the top of the page to open the **Add backend pool** page.
4. Select **Basics** at the top of the panel and enter following values:
   - **Name**: Enter a backend pool name.
     Guide example is *bep_ECV*
   - **IP Backend Pool Configuration**: Select **NIC**
   - **IP IP Version**: Select **IPv4**
   - **Virtual Machines**: Click +Add to open the **Add Virtual machines to backend pool** dialog. Select the Virtual Machine – LAN0 IP address for each appliance in your configuration, then click **Add** at the bottom of the dialog.
     Guide example (1): **Virtual Machine** = *vm-ECV-A*; **IP Configuration** = *10.6.3.11/24*
     Guide example (2): **Virtual Machine** = *vm-ECV-B*; **IP Configuration** = *10.6.3.12/24*
5. Click **OK** at the bottom of the panel to close the panel.

   The two EC-Vs appear in the **Backend Pool** page (**Figure 35**).

**Figure 35. Viewing EC-Vs in the Backend Pool**

Next Step: Proceed to Create a Health Probe on the next page
Create a Health Probe

After creating the backend pool, create a health probe to monitor an interface on the EC-V.

2. Click Health probes on the Setting menu (left-side column) to open the Health probes page.
3. Click + Add at the top of the page to open the Add health probe page and enter the following settings:
   - **Name**: Enter a name for the health probe. 
     Guide example: hp_ECV
   - **Protocol**: (drop-down) Select TCP
     **IMPORTANT** Do not use HTTPS.
   - **Port**: Enter a port number.
     Guide example: 443
   - **Interval**: Period (seconds) between probe attempts. Shortest supported interval is five seconds.
     Guide example: Enter 5
   - **Unhealthy threshold**: Number of consecutive probe failures that define a virtual machine as unhealthy.
     Guide example: Enter 2
4. Click Add at the bottom of the panel to close the page.

The Health probe appears in the Health probes page (Figure 36).

**Figure 36. Viewing Health Probes**

Next Step: Proceed to Create a Load Balancing Rule on the next page
Create a Load Balancing Rule

After creating a health probe, create a load balancing rule.

2. Select Load balancing rules from the Setting menu to open the Load balancing rules page.
3. Click + Add in the button bar at the top of the page to open the Add load balancing rule page and enter the following settings:
   - **Name**: Enter a name for the load balancing rule
     Guide example: lbr_ECV-1
   - **IP Version**: Select IPv4
   - **Frontend IP address**: Select the load balancer's frontend private IP address
     Guide example: 10.6.3.254
   - **HA Ports**: (Selection box) Check
     This enables load balancing on all ports for TCP and UDP protocols.
   - **Backend pool**: (drop-down) Select the backend pool that consists of the EC-Vs. This backend pool is the target of the rule's load balanced traffic.
     Guide example: bep_ECV
   - **Health Probe**: (drop-down) Select the health probe that you created.
     This health probe is used by this rule to determine the healthy EC-Vs in the backend pool that can receive load balanced traffic.
     Guide example: hp_ECV
   - **Session Persistence**: (drop-down) Select a session persistence policy. Persistence policies specify traffic handling processes from a client by the same virtual machine in the backend pool for the duration of a session. Options include:
     - **None** – successive requests from the same client may be handled by any virtual machine in the backend pool.
     - **Client IP** – successive requests from the same client IP address are handled by the same virtual machine in the backend pool.
     - **Client IP and protocol** – successive requests from the same client IP address and protocol combination are handled by the same backend pool virtual machine.
     Guide example: Client IP and protocol
   - **Idle timeouts (minutes)**: This is the setting that decides to keep a TCP or HTTP connection open without relying on clients to send keep-alive messages.
     Guide example: Enter 4.
   - **TCP Reset**: (Selection box) Enabled
   - **Floating IP**: (Selection box) Disabled
   - **Create Implicit Outbound Rules**: Select No
4. Click Add at the bottom of the panel to close the page.
The load balancing rule appears in the **Load balancing rules** page (Figure 37).

**Figure 37. Viewing Load Balancing Rules**

<table>
<thead>
<tr>
<th>Name</th>
<th>Load balancing rule</th>
<th>Backend pool</th>
<th>Health probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>lb_ECV-1</td>
<td>lb_ECV-1 (All/0)</td>
<td>bps_ECV</td>
<td>hp_ECV</td>
</tr>
</tbody>
</table>

Next Step: Proceed to **Verify the IP address of the Internal Load Balancer on the next page**
Verify the IP address of the Internal Load Balancer

After creating the load balancing rule, verify the IP address of the ILB by viewing incoming health probe traffic on the EC-V.

1. In Orchestrator, select the EC-Vs in the appliance menu and open the Flows page. \((\text{Monitoring} > \text{Bandwidth} > \text{Flows} > \text{Active and Recent Flows})\).
2. Enter the LAN0 IP address on the IP/Subnet textbox and the TCP port on the Port textbox. This filters traffic the LAN0 interface is receiving that is destined to port 443.
   Guide example: Enter 443
3. Select Include Built-in (selection box).
4. Click Apply to apply the filter. Note the health probes that are received from the ILB.
   The IP address of the ILB is a virtual IP address that Azure reserves for load balancers. In this deployment, the address is 168.63.129.16. This panel indicates the health probes are going pass-through on WAN0 interface on the EC-V as shown on Figure 38.
   The WAN0 next-hop IP address on the Outbound Tunnel column confirms this.

Create a Static Route on the EC-V for Health Probe Traffic creates a static route on the EC-V that replies to the health probes from the ILB instead of forwarding them on its WAN interface. This allows the ILB to detect the health of the EC-V.

Figure 38. Health probe traffic leaving WAN0 interface

Next Step: Proceed to Create a Static Route on the EC-V for Health Probe Traffic on page 107
Health Probe Traffic in the HA Deployment (Azure ILB)

Tasks include:

- Create a Static Route on the EC-V for Health Probe Traffic
- Verify Health Probe Responses using tcpdump (Optional)
Create a Static Route on the EC-V for Health Probe Traffic

Complete the following steps to create a static route that responds to health probes from the ILB.

1. In Orchestrator, select ECV-A in the appliance menu and open the Routes page (Configuration > Networking > Routing > Routes).

2. Open the Routes panel by clicking an edit icon and enter these values.
   - Use shared subnet information: (selection box) Check
   - Automatically advertise local LAN subnets: (selection box) Uncheck
   - Automatically advertise local WAN subnets: (selection box) Uncheck
   - Metric for automatically added subnets: Enter 50
   - Redistribute routes to SD-WAN Fabric: (drop-down) Select an available route map. Guide Example: default_rtmap_to_subsh
   - Include BGP Local ASN to routes sent to SD-WAN Fabric: (selection box) Uncheck
   - Tag BGP communities to routes: (Selection box) Uncheck

3. Click the edit icon right of the Redistribute routes to SD-WAN Fabric data field. The SD-WAN Fabric Route Distribution Maps popup opens.

4. Verify the popup includes a rule with the following settings:
   - Match Criteria: Source Protocol Local/Static
     Guide example is 10.6.0.0/24
   - Permit: Allow
     Guide example is 10.6.3.1

   This ensures the static routes are advertised to the SD-WAN fabric.

5. Modify or add a rule if necessary, then click Apply. If no modification is required, click Cancel.

6. Open the Add Route by clicking Add Route at the top of the panel and enter these values:
   - Subnet/Mask: Enter the Load Balancer IP Address, as displayed on the Flows page. Guide example: Enter 168.63.129.16/32
   - Next Hop: Enter the LAN0 next hop address. Guide example: Enter 10.6.3.1
   - Interface: (drop-down) Enter lan0
   - Metric: Enter 50
   - Tag: (drop-down) Select ALL
   - Comments: Optional

7. Click Add to close the Add Route popup and return to the Routes panel.
8. The following steps prevent routes that you add from being advertised to the SD-WAN fabric via Subnet Sharing by creating a rule on the SD-WAN Fabric Route Redistribution Maps table.

- Click the edit icon that is located right of the Redistribute routes to SD-WAN Fabric dropdown menu. The SD-WAN Fabric Route Distribution Maps popup opens.

- Open the Add Rule popup by clicking Add rule and enter these values:
  - Select Match Criteria – Source Protocol (dropdown): Local/Static
  - Select Match Criteria – Prefix (check box): Select and enter 168.63.129.16/32
  - Set Actions – Permit (check box): De-select

- Click Add to close the Add Rule popup, then click Apply to close the SD-WAN Fabric Route Redistribution Maps popup.

9. Click Apply to close the Routes panel and return to the Routes page.

10. Open the Flows page (Monitoring > Bandwidth > Flows > Active and Recent Flows)

11. Click the refresh icon until the Outbound Tunnel column of a new flow indicates a passthrough tunnel with a LAN0 next hop (Figure 39). This will require a few seconds.

   This confirms the EC-V responds to health probes on the LAN interface instead of forwarding the probes through its WAN interface. This allows the load balancer to forward traffic to the EC-V when probes indicate the EC-V is healthy.

   **Figure 39. Responding to health probe traffic on lan0**

Next Step: Proceed to Verify Health Probe Responses using tcpdump (Optional) on the next page
Verify Health Probe Responses using tcpdump (Optional)

You can further verify health probe responses by running a quick packet capture. Complete the following steps to run a packet capture on the Web CLI.

1. In Orchestrator, right-click a selected EC-V in the appliance menu and select *CLI Session*. A CLI session opens on a new tab.
2. Type the following commands to capture the traffic received on the LAN0 interface:
   ```
   enable
tcpdump -i lan0 port 443 -nn
   ```

Create the same static route on EC-V-B and confirm that it responds to the health probes from the ILB.

**Next Step:** Proceed to *Traffic Redirection in the HA Deployment (Azure ILB) on the next page*
Traffic Redirection in the HA Deployment (Azure ILB)

The next task is to configure traffic redirection to forward outbound traffic from the Azure workloads to the ILB. The configuration depends on the location of your workloads with Azure:

- If your workloads are deployed within the same virtual network as the EC-Vs and the ILB, you only need to create a static route on the virtual network's route table. Figure 32 displays the topology of this configuration.

  To create the static routes, perform the following:
  - Create an Azure Route Table
  - Associate the Workloads Subnet to the Route Table
  - Create a Static Route to Forward Traffic to the ILB
  - Create Static Routes to Advertise Azure Subnets to Remote EdgeConnect Devices
  - Enable Flow Redirection on the EC-V

- Workloads deployed in a different virtual network than the EC-Vs and the ILB require a virtual network Peering session between the workload virtual network and the virtual network where the EC-Vs are deployed. Figure 33 displays the topology of this configuration.

  To create the virtual network Peering session and the static routes, perform the following:
  - Create a Virtual Network Peering Session
  - Create an Azure Route Table
  - Associate the Workloads Subnet to the Route Table
  - Create a Static Route to Forward Traffic to the ILB
  - Create Static Routes to Advertise Azure Subnets to Remote EdgeConnect Devices
  - Enable Flow Redirection on the EC-V
Create a Virtual Network Peering Session

The following steps create a virtual network peering session.

1. From Azure portal, open the deployment virtual network page (accessible from the Resource Group page).
   Guide example: *vn_ECV*

2. Select *Peerings* in the Settings menu (left side of page) to open the *Peerings* page.

3. Click + *Add* in the button bar to open the *Add peering* page and enter the following values.
   - **Name of the peering from vn_ECV to remote virtual network**: Enter a name
     Guide example: *peer_ECV-1A*

   **Peer Details**
   - **Virtual network deployment model**: Select *Resource Manager*
   - **I know my resource**: (Selection box) *Unchecked*
   - **Subscription**: (drop-down) Select the subscription that you used to deploy the EC-Vs.
     Guide example: *Pay-As-You-Go*
   - **Virtual Network**: Select the virtual network where the workloads are deployed.
     Guide example: *(drop-down) vn_WKLOAD*
   - **Name of the peering from vn_WKLOAD to vn_ECV**: Enter a name.
     Guide example: Enter *peer_ECV-1B*

   **Configuration**
   - **Allow virtual network access from vn_ECV to vn_WKLOAD**: (Selection box) *Enabled*
   - **Allow virtual network access from vn_WKLOAD to vn_ECV**: (Selection box) *Enabled*
   - **Allow forwarded traffic from vn_WKLOAD to vn_ECV**: (Selection box) *Disabled*
   - **Allow forwarded traffic from vn_ECV to vn_WKLOAD**: (Selection box) *Enabled*
   - **Allow gateway transit**: (Selection box) *Disabled*

4. Click *OK* at the bottom of the panel to close the panel.

   One new peering appears in the *Peerings* page. The other peering is added to the *Peerings* page of the Workload virtual network.

**Next Step**: Proceed to Create an Azure Route Table on the next page
Create an Azure Route Table

If your Azure workload subnet is associated to a Route Table, you may use that Route Table instead of creating a new one. In that case, proceed to Associate the Workloads Subnet to the Route Table. Otherwise, create a route table to associate with your Azure workload subnet.

The following steps create a route table for your Azure workload.

1. From the Azure portal, navigate to your Resource group and click +Add in the menu bar.
2. Use the search field to select Route Table in the drop-down menu.
   The Route table window opens.
3. Click the Create button.
   The Create Route Table screen opens.
4. Enter the following values in the Create Route Table fields:
   - **Name**: Enter a descriptive name for the route.
     Guide example is rt_ECV
   - **Subscription**: (drop-down) Depends on your Azure account.
     Guide example is Pay-As-You-Go
     Guide example is SP-Tech
   - **Location**: Select an Azure region where you want to create the route table.
     Guide example is (US) West US
   - **Virtual Network Gateway Route Propagation**: Select Enabled
5. Click Create at the bottom of the Create Route Table panel.
   The Resource Group page opens.

Next Step: Proceed to Associate the Workloads Subnet to the Route Table on the next page
Associate the Workloads Subnet to the Route Table

Associating the Workloads subnet to the route table allows VMs in the workloads subnet to use the static route that is created in the next step.

The following steps associate the subnet where your workloads are deployed to the route table.

1. Open the Route Table page for the previously created route table (accessible from the Resource Group page).

2. Select Subnets from the Settings menu (left-side column) to open the Subnets page.

3. Click + Associate in the button bar at the top of the page to open the Associate subnet panel on the right side of the page and enter the following values.
   - **Virtual network deployment model**: (drop-down) Select the deployment virtual network.
     Guide example: vn_ECV
   - **Subnet**: (drop-down) Select the virtual network that accesses the workload.
     Guide example: WKLOAD

4. Click OK at the bottom of the panel to close the panel.
   The specified subnet appears on the Subnets page, indicating that it is associated to the Route Table.

**Next Step:** Proceed to Create a Static Route to Forward Traffic to the ILB on the next page
Create a Static Route to Forward Traffic to the ILB

The following steps create a static route on the Azure portal to forward outbound traffic from the workloads to the ILB.

1. Open the Route Table page for the previously created route table (accessible from the Resource Group page).
2. Click Routes from the Settings menu (left-side column) to open the Routes page.
3. Click + Add in the button bar at the top of the page to open the Add route page and enter the following values:
   - Route name: Enter a name for the route.
     Guide example: rt_TO-REMOTE
   - Address prefix: The destination IP address range (CIDR notation) to which this applies. Packets match this route when their destination IP address falls in this range.
     Guide example: 10.3.2.0/24
   - Next hop type: Select Virtual appliance
   - Next hop address: Enter the ILB's frontend private IP address.
     For traffic that you prefer not to forward to the SD-WAN fabric or perform application classification in the EC-V, such as Internet-bound (SaaS) traffic from Azure workloads, enter the Azure Internet Gateway IP address as the next-hop.
     Guide example: 10.6.3.254
4. Click OK to create the route and close the page.
   The new route subnet appears on the Routes page.

Next Step: Proceed to Create Static Routes to Advertise Azure Subnets to Remote EdgeConnect Devices on the next page
Create Static Routes to Advertise Azure Subnets to Remote EdgeConnect Devices

This topic create static routes to advertise Azure subnets to remote EdgeConnect Devices.

Create a Static Route
Repeat these steps to create the necessary static routes on each EC-V in the deployment:

1. In Orchestrator, select ECV-A in the appliance menu and open the Routes page (Configuration > Networking > Routing > Routes).
2. Open the Routes panel by clicking an edit icon and enter these values.
   - Automatically advertise local LAN subnets: (Selection box) Check
   - Automatically advertise local WAN subnets: (Selection box) Uncheck
   - Metric for automatically added subnets: Enter 50
   - Redistribute routes to SD-WAN Fabric: (drop-down) Select an available route map. Guide Example: default_rtmap_to_subsh
   - Filter Routes From SD-WAN Fabric With Matching Local ASN: (selection box) Uncheck
   - Include BGP Local ASN to routes sent to SD-WAN Fabric: (selection box) Uncheck
   - Tag BGP communities to routes: (Selection box) Uncheck
3. Click the edit icon right of the Redistribute routes to SD-WAN Fabric data field. The SD-WAN Fabric Route Distribution Maps popup opens.
4. Verify the popup includes a rule with the following settings:
   - Match Criteria: Source Protocol Local/Static
     Guide example is 10.6.4.0/24
   - Permit: Allow
     Guide example is 10.6.3.1
   This ensures the static routes are advertised to the SD-WAN fabric.
5. Modify or add a rule if necessary, then click Apply.
   If no modification is required, click Cancel.
6. Click Add route above the Routes table to open the Add Route popup and enter the following values:
   - Subnet/Mask: Enter an IP address space to the Workload subnet. Guide example: 10.6.4.0/24
   - Next Hop (Optional): Enter the LAN0 next hop IP address. Guide example: 10.6.3.1
   - Interface: (drop-down) Enter the interface that connects to the Load Balancer.
Guide example: Enter **LAN0**
- **Metric**: Enter **50**
- **Tag**: Select **FROM_WAN**
- **Comments**: Optional

7. Click **Add** to close the popup and return to the **Routes** panel. Verify the new route is listed in the routes table.

8. Click **Apply** in the bottom left corner to close the panel and return to the **Routes** page. Verify the new route is listed in the routes table.

**Create Additional Static Routes on ECV-A**

Static routes are required for all Azure subnets that need to be reachable by remote EdgeConnect devices. Repeat steps in the previous section to create the required static routes on the ECV.

**Create Static Routes on EC-V-B**

Repeat steps in the previous section to create static routes on EC-V-B. Static routes are identical in each EC-V.

**Verify the Static Routes**

Verify the static routes in each EC-V by viewing the Routes page. It should look similar to **Figure 40**.

**Figure 40. Static routes on each EC-V.**

Next Step: Proceed to **Enable Flow Redirection on the EC-V** on the next page
Enable Flow Redirection on the EC-V

Flow redirection is a method by merging the traffic of an asymmetric flow into a single appliance, thus removing the flow asymmetry. Figure 41 depicts the redirection of a traffic flow through ECV-A.

**IMPORTANT** Flow Redirection works only for TCP traffic.

*Figure 41. Flow Redirection – Azure ILB Topology*

Enable Flow Redirection on each appliance when flow symmetry is required or to enable Boost on the EC-Vs. Flow Redirection prevents asymmetric flows on the EC-Vs regardless of the ILB session persistence algorithm. Enabling flow redirection is optional when Boost is not enabled on the appliances. Traffic flow continues even when flows are asymmetric. This is not an issue for most applications.

Flow Redirection is configured on the LAN0 interface of the EC-Vs. To configure Flow Redirection, log into the EdgeConnect Appliance Manager Web UI. (It is not available on the Orchestrator Web UI.)

**Configure Flow Redirection on an EC-V**

Use the LAN0 interface instead of creating a separate MGMT1 interface on the EC-V. Flow Redirection requires that the LAN0 interface of each EC-V is on the same subnet.
1. Open Orchestrator, right click the ECV-A in the Appliance menu, and select Appliance Manager.
2. Open the Flow Redirection page (Configuration > Policies > Flow Redirection) and enter the following values:
   - **Enable**: (Selection box) Check
   - **Wait Time**: Select 50
   - **Interface**: Select lan0
3. Click Add Peer and enter EC-V-B's LAN0 IP address.
4. Click Apply. The State column will change to Unreachable.

**Configure Flow Redirection on EC-V-B**

Enable Flow Redirection on EC-V-B by following the instructions above. Once you enable Flow Redirection on both EC-Vs, the State column on the Flow Redirection page will indicate OK.

Enabling flow redirection on both EC-Vs eliminates asymmetric flows on the appliances. The inbound and outbound tunnel show the same tunnel name for all flows.

This concludes the EC-V HA deployment using the Azure Standard Internal Load Balancer. To increase throughput and redundancy for your cloud-based workloads, continue adding EC-Vs to the Standard Internal Load Balancer and build tunnels to the remote EdgeConnect devices.

**Next Step: The Internal Load Balancer Deployment is completed.**