Silver Peak Systems

EdgeConnect for Amazon Web Services (AWS)

Dinesh Fernando

2-22-2018

Contents

Overview

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

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

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

Deploying EC-V Router Mode

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

Topology

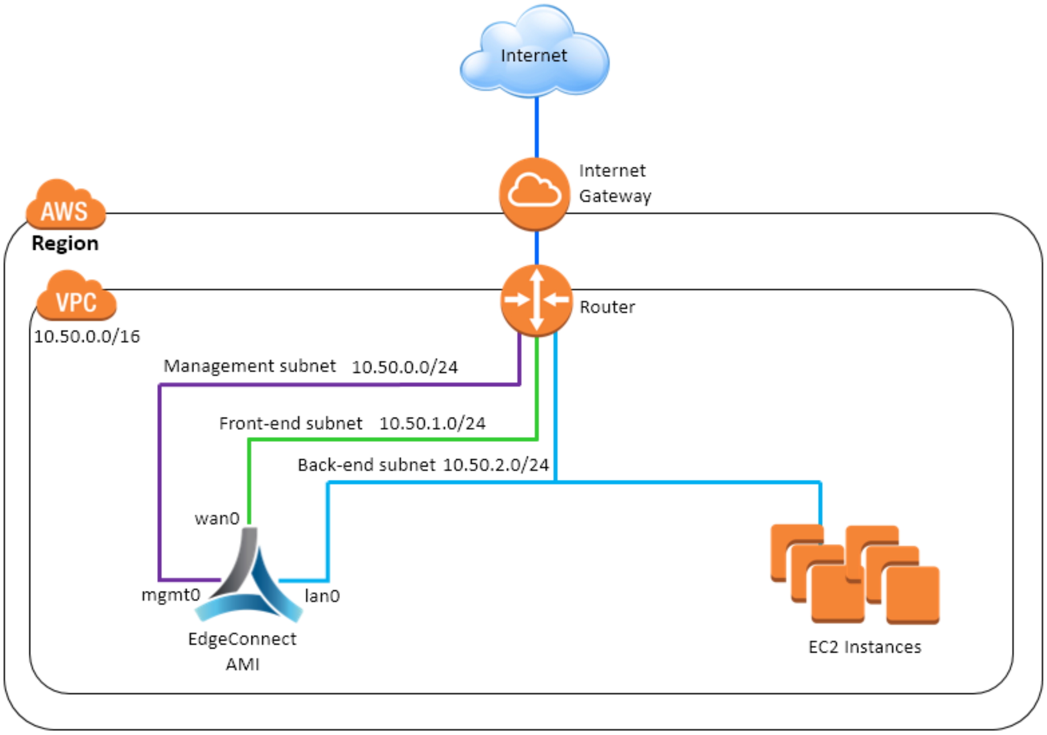


Figure 1: Topology of an EC-V deployment with one WAN interface, one LAN interface, and one management interface.

Assumptions and Prerequisites

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

  Note: In AWS, an EC-V can be deployed with multiple WAN interfaces and LAN interfaces. As shown in Figure 1, this deployment assumes that there is no site-to-site VPN or Direct Connect link between the VPC and the on-premises network. Therefore, the WAN0 and MGMT0 interfaces must have Public IPs that are accessible over the Internet.

To learn more about configuring a VPC, please refer to the AWS documentation: https://aws.amazon.com/documentation/vpc/

Best Practices

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

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

Procedure

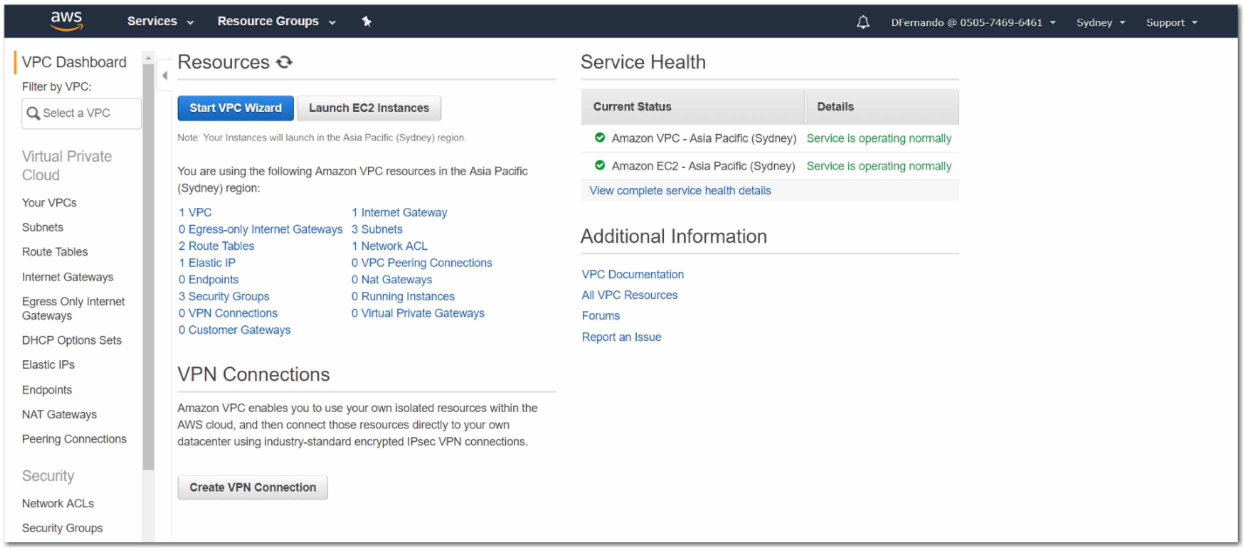
Deploying an EC-V from the AWS Marketplace takes only a few minutes.

Evaluate the VPC in preparation for the EC-V deployment

In this section, you'll verify that you have all the necessary AWS components.

1. First, **login to your AWS account** and **select the region** in which you want to deploy the EC-V.

   Under **Networking & Content Delivery**, click **VPC.** The VPC Dashboard appears.



Note: Your Instances will launch in the Asia Pacific (Sydney) region.

You are using the following Amazon VPC resources in the Asia Pacific (Sydney) region:

1 VPC	1 Internet Gateway
0 Egress-only Internet Gateways	3 Subnets
2 Route Tables	1 Network ACL
1 Elastic IP	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
3 Security Groups	0 Running Instances
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	

VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

Service Health

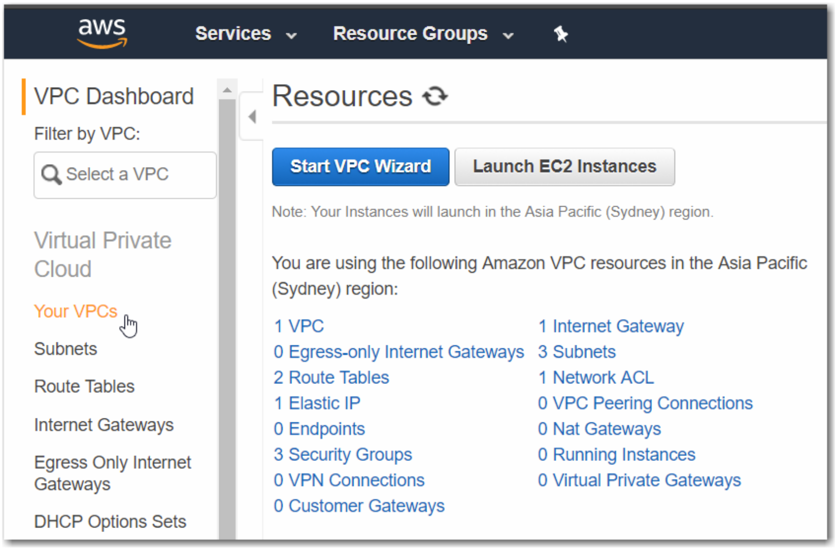
Current Status	Details
Amazon VPC - Asia Pacific (Sydney)	Service is operating normally
Amazon EC2 - Asia Pacific (Sydney)	Service is operating normally

View complete service health details

Additional Information

VPC Documentation
All VPC Resources
Forums
Report an Issue

2. Under **Virtual Private Cloud**, select **Your VPCs**.

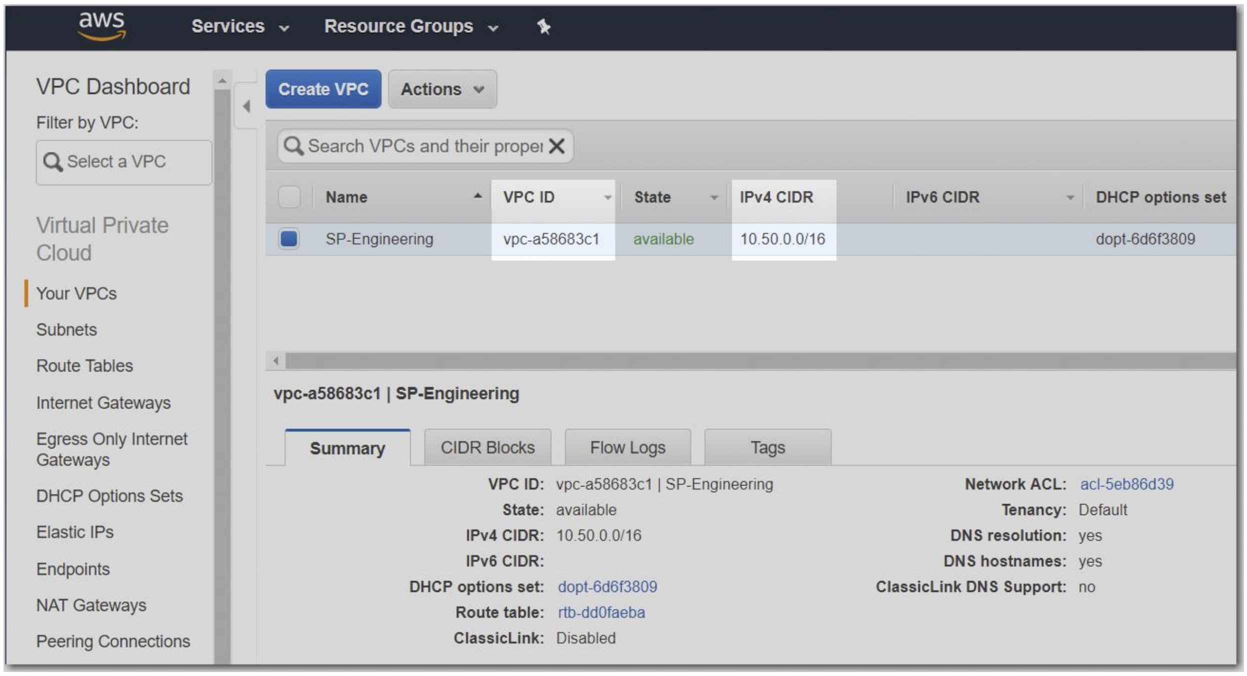


Note: Your Instances will launch in the Asia Pacific (Sydney) region.

You are using the following Amazon VPC resources in the Asia Pacific (Sydney) region:

1 VPC	1 Internet Gateway
0 Egress-only Internet Gateways	3 Subnets
2 Route Tables	1 Network ACL
1 Elastic IP	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
3 Security Groups	0 Running Instances
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	

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



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
SP-Engineering	vpc-a58683c1	available	10.50.0.0/16		dopt-6d6f3809

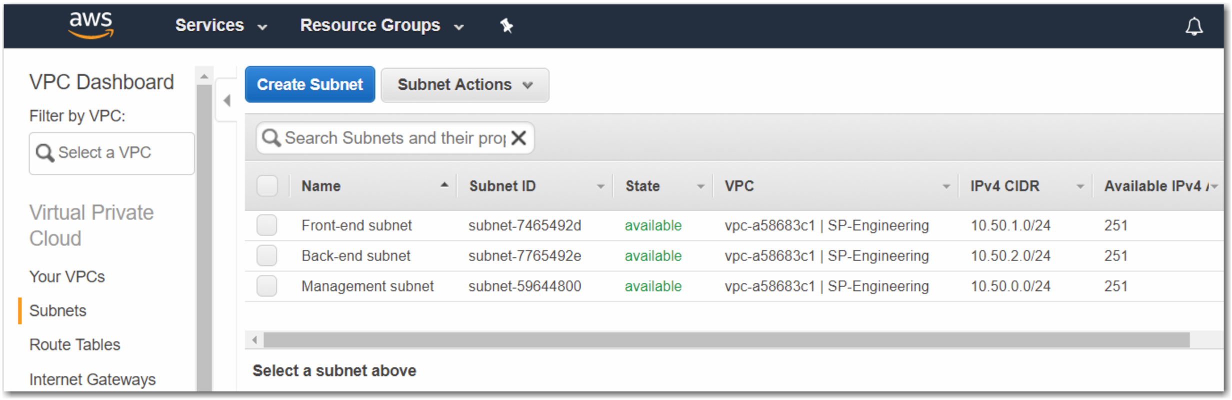
vpc-a58683c1 | SP-Engineering

VPC ID: vpc-a58683c1 | SP-Engineering
State: available
IPv4 CIDR: 10.50.0.0/16
IPv6 CIDR:
DHCP options set: dopt-6d6f3809
Route table: rtb-dd0faeba
ClassicLink: Disabled

Network ACL: acl-5eb86d39
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

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

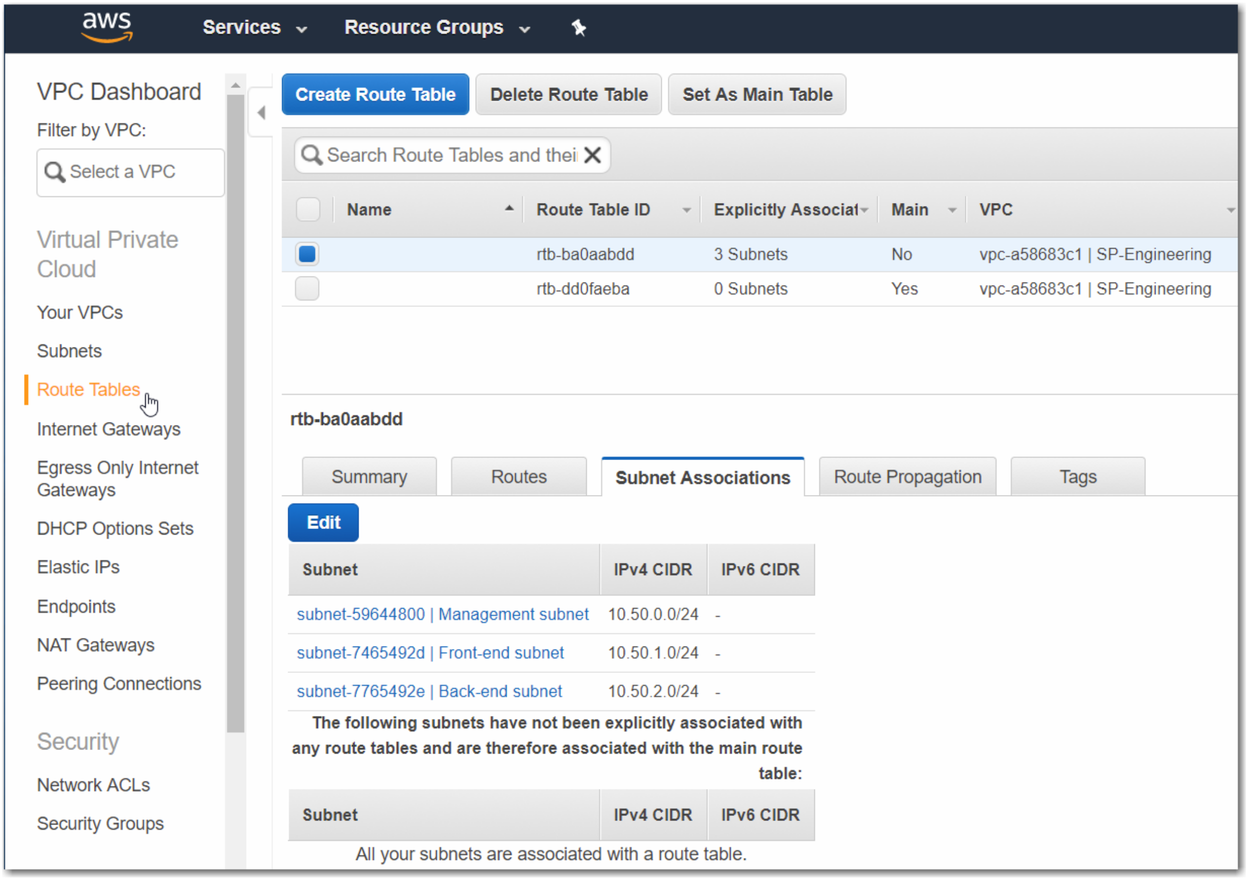
   The SP-Engineering VPC has the three necessary subnets: Management subnet (10.50.0.0/24), Front-end subnet (10.50.1.0/24), and Back-end subnet (10.50.2.0/24). Soon, we'll pair them with MGMT0, WAN0, and LAN0, respectively.



Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4
Front-end subnet	subnet-7465492d	available	vpc-a58683c1 | SP-Engineering	10.50.1.0/24	251
Back-end subnet	subnet-7765492e	available	vpc-a58683c1 | SP-Engineering	10.50.2.0/24	251
Management subnet	subnet-59644800	available	vpc-a58683c1 | SP-Engineering	10.50.0.0/24	251

Select a subnet above

4. From the left side menu, click **Route Tables**, and select the route table that is associated with your subnets.
5. Click the **Subnet Associations** tab. Verify that all subnets are associated with the selected route table.



	Name	Route Table ID	Explicitly Associat	Main	VPC
☑		rtb-ba0aabdd	3 Subnets	No	vpc-a58683c1 | SP-Engineering
□		rtb-dd0faeba	0 Subnets	Yes	vpc-a58683c1 | SP-Engineering

rtb-ba0aabdd

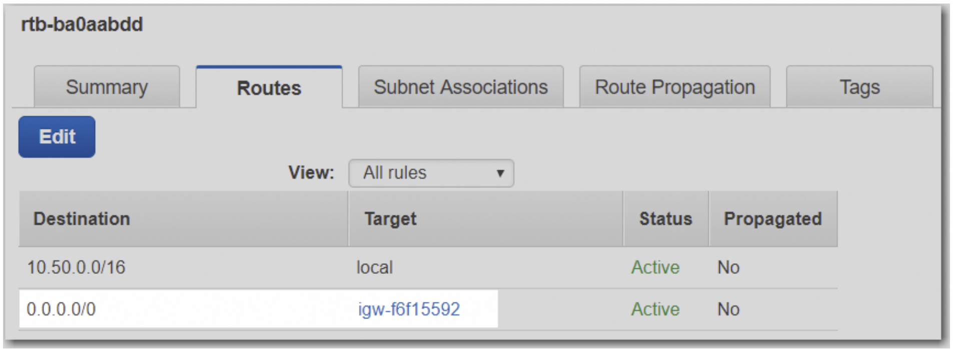
Subnet	IPv4 CIDR	IPv6 CIDR
subnet-59644800 | Management subnet	10.50.0.0/24	-
subnet-7465492d | Front-end subnet	10.50.1.0/24	-
subnet-7765492e | Back-end subnet	10.50.2.0/24	-

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	IPv4 CIDR	IPv6 CIDR

All your subnets are associated with a route table.

6. Select the **Routes** tab. Verify that an Internet Gateway is the target for any Internet-bound (0.0.0.0/0) traffic.



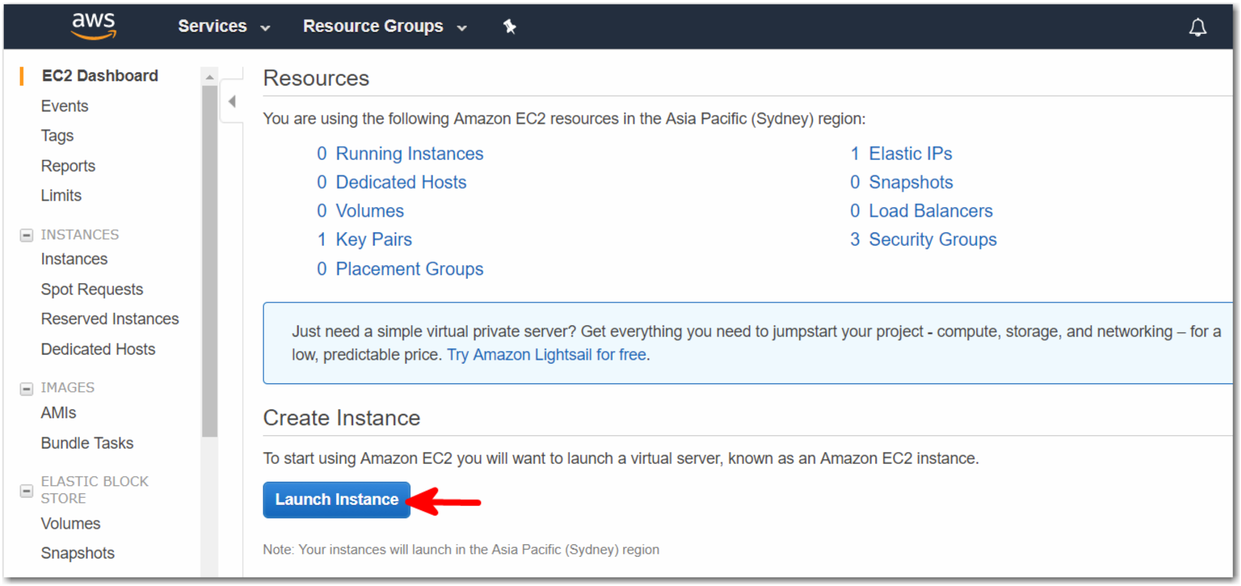
rtb-ba0aabdd

View: All rules

Destination	Target	Status	Propagated
10.50.0.0/16	local	Active	No
0.0.0.0/0	igw-f6f15592	Active	No

Deploy the EC-V

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



Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Sydney) region:

0 Running Instances	1 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
1 Key Pairs	3 Security Groups
0 Placement Groups	

Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free.

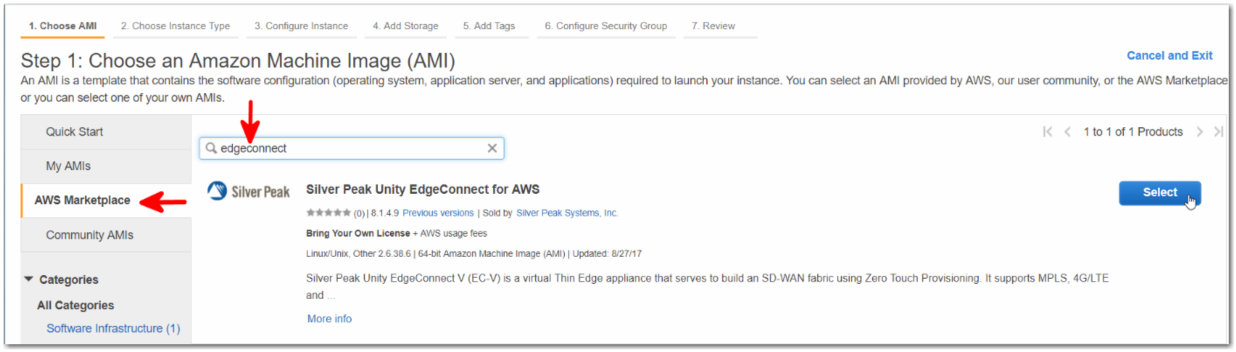
Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the Asia Pacific (Sydney) region

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

3. Click the **AWS Marketplace** link, and enter **`edgeconnect`**.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace or you can select one of your own AMIs.

Silver Peak Unity EdgeConnect for AWS

★★★★★ (0) | 8.1.4.9 Previous versions | Sold by Silver Peak Systems, Inc.

Bring Your Own License + AWS usage fees

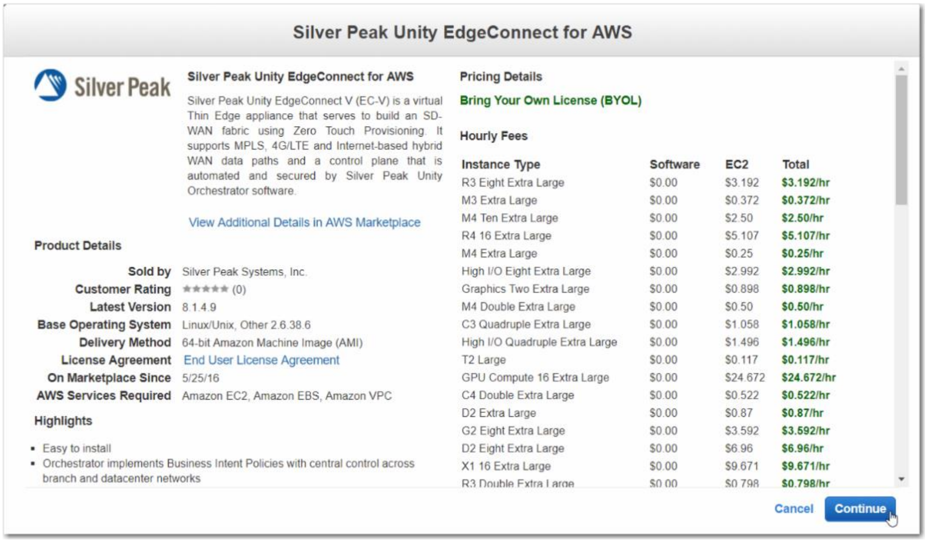
Linux/Unix, Other 2.6.38.6 | 64-bit Amazon Machine Image (AMI) | Updated: 8/27/17

Silver Peak Unity EdgeConnect V (EC-V) is a virtual Thin Edge appliance that serves to build an SD-WAN fabric using Zero Touch Provisioning. It supports MPLS, 4G/LTE and ...

The latest version of the **Silver Peak Unity EdgeConnect for AWS** AMI appears.
NOTE: You must have an EdgeConnect license before you can continue deploying the EC-V.

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

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



Silver Peak Unity EdgeConnect for AWS

Silver Peak Unity EdgeConnect for AWS

Silver Peak Unity EdgeConnect V (EC-V) is a virtual Thin Edge appliance that serves to build an SD-WAN fabric using Zero Touch Provisioning. It supports MPLS, 4G/LTE and Internet-based hybrid WAN data paths and a control plane that is automated and secured by Silver Peak Unity Orchestrator software.

Product Details

Sold by	Silver Peak Systems, Inc.
Customer Rating	★★★★★ (0)
Latest Version	8.1.4.9
Base Operating System	Linux/Unix, Other 2.6.38.6
Delivery Method	64-bit Amazon Machine Image (AMI)
License Agreement	End User License Agreement
On Marketplace Since	5/25/16
AWS Services Required	Amazon EC2, Amazon EBS, Amazon VPC

Highlights

- Easy to install
- Orchestrator implements Business Intent Policies with central control across branch and datacenter networks

Pricing Details

Bring Your Own License (BYOL)

Hourly Fees

Instance Type	Software	EC2	Total
R3 Eight Extra Large	$0.00	$3.192	$3.192/hr
M3 Extra Large	$0.00	$0.372	$0.372/hr
M4 Ten Extra Large	$0.00	$2.50	$2.50/hr
R4 16 Extra Large	$0.00	$5.107	$5.107/hr
M4 Extra Large	$0.00	$0.25	$0.25/hr
High I/O Eight Extra Large	$0.00	$2.992	$2.992/hr
Graphics Two Extra Large	$0.00	$0.898	$0.898/hr
M4 Double Extra Large	$0.00	$0.50	$0.50/hr
C3 Quadruple Extra Large	$0.00	$1.058	$1.058/hr
High I/O Quadruple Extra Large	$0.00	$1.496	$1.496/hr
T2 Large	$0.00	$0.117	$0.117/hr
GPU Compute 16 Extra Large	$0.00	$24.672	$24.672/hr
C4 Double Extra Large	$0.00	$0.522	$0.522/hr
D2 Extra Large	$0.00	$0.87	$0.87/hr
G2 Eight Extra Large	$0.00	$3.592	$3.592/hr
D2 Eight Extra Large	$0.00	$6.96	$6.96/hr
X1 16 Extra Large	$0.00	$9.671	$9.671/hr
R3 Double Extra Large	$0.00	$0.798	$0.798/hr

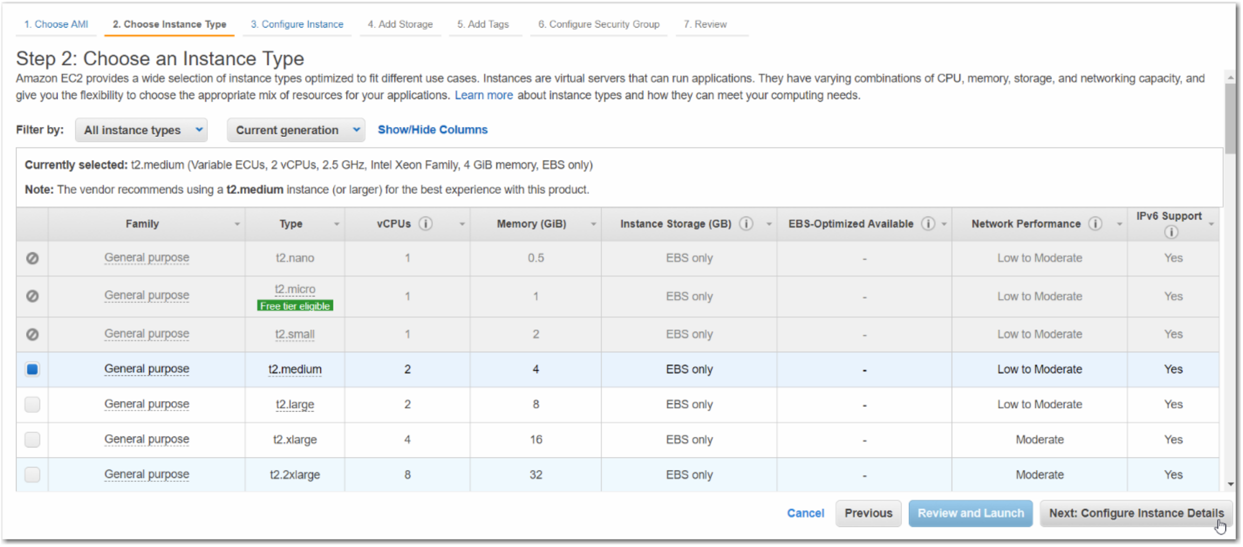
The **Step 2: Choose an Instance Type** page appears.

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

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

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

6. Click **Next: Configure Instance Details**.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation | **Show/Hide Columns**

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.5 GHz, Intel Xeon Family, 4 GiB memory, EBS only)

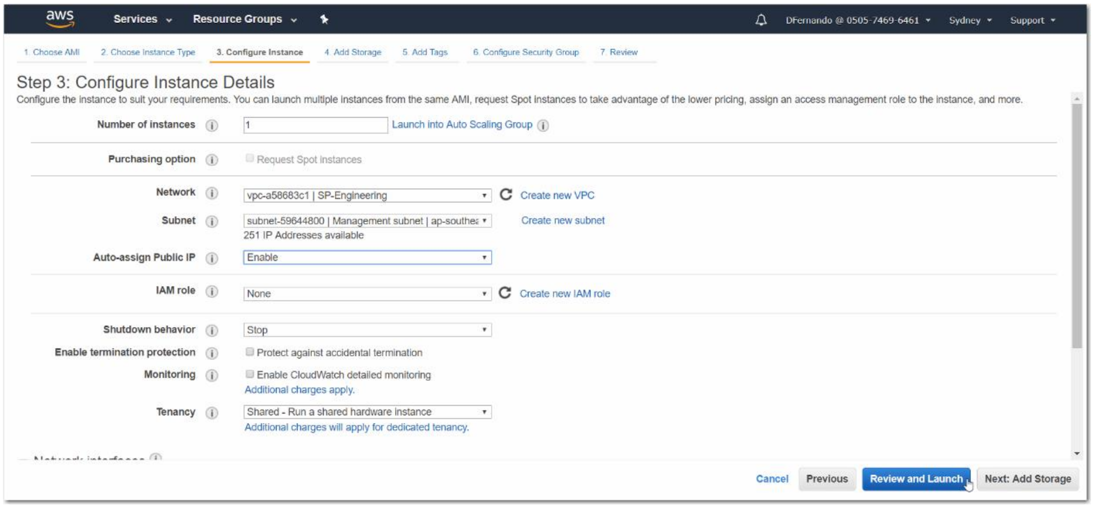
Note: The vendor recommends using a **t2.medium** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
⊘	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
⊘	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
⊘	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes

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

Number of instances	1
Purchasing option	Keep the default setting.
Network	Select the VPC into which you want to deploy the EC-V.
Subnet	Select the Management subnet.
Auto-assign Public IP	**Enable** (Enable means a dynamic public IP will be assigned to the interface.) If you've already established a VPN or Direct Connect link, you can choose **Disable**.
IAM role	Select an appropriate IAM role. If no IAM roles are created, select **None**.
Shutdown behavior	**Stop**

Enable termination protection	Deselect **Protect against accidental termination**
Monitoring	Deselect **Enable CloudWatch detailed monitoring**
Tenancy	**Shared – Run a shared hardware instance**



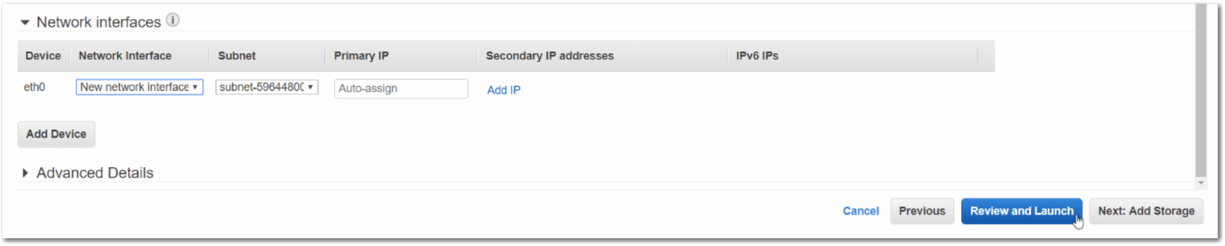
Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-a58683c1 | SP-Engineering · Create new VPC
Subnet	subnet-59644800 | Management subnet | ap-southea · Create new subnet 251 IP Addresses available
Auto-assign Public IP	Enable
IAM role	None · Create new IAM role
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

To assign the MGMT0 IP automatically (from the AWS DHCP server), leave **Primary IP** blank. Otherwise, enter a static Private IP for the MGMT0 interface.

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

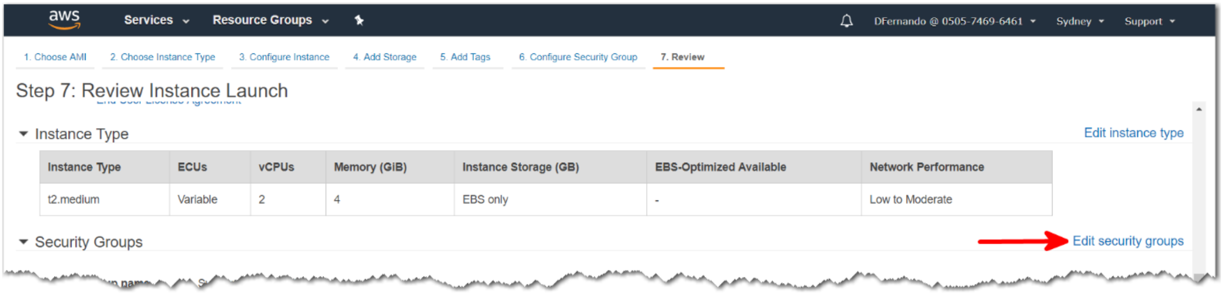


Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-5964480C	Auto-assign	Add IP	

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

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



Step 7: Review Instance Launch

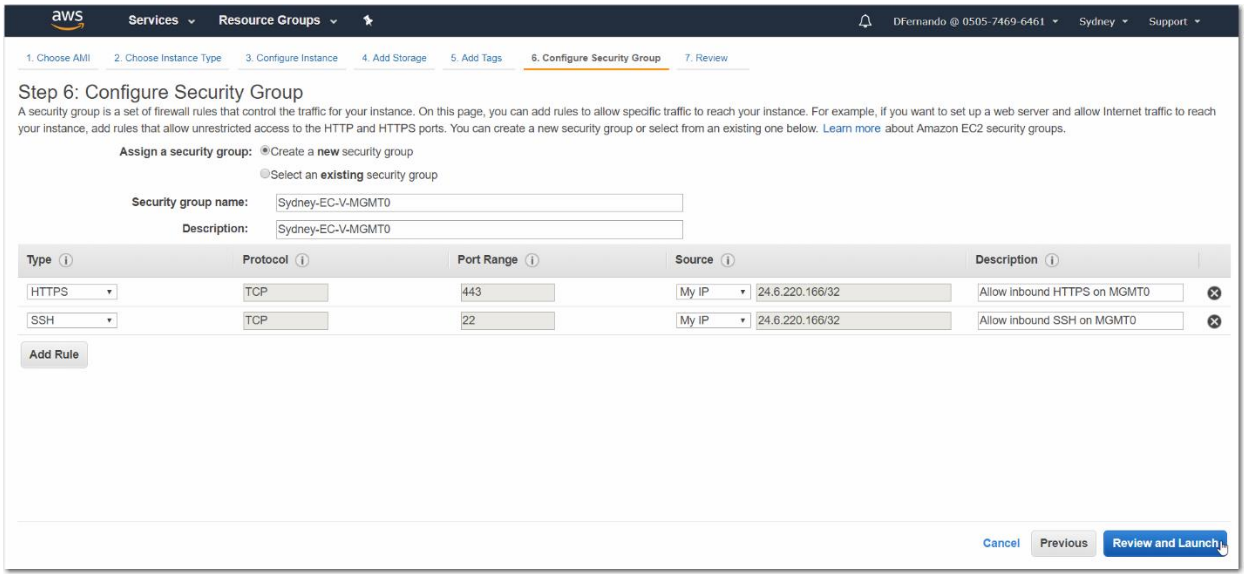
Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

Security Groups

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

10. Create a **new** Security Group or select an **existing** Security Group for the MGMT0 interface. (If you choose an existing Security Group, verify that it allows inbound HTTPS and SSH.)



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: Sydney-EC-V-MGMT0

Description: Sydney-EC-V-MGMT0

Type	Protocol	Port Range	Source		Description
HTTPS	TCP	443	My IP	24.6.220.166/32	Allow inbound HTTPS on MGMT0
SSH	TCP	22	My IP	24.6.220.166/32	Allow inbound SSH on MGMT0

a. In our example, we select **Create a new security group** and change the default security group name to **Sydney-EC-V-MGMT0**.

b. Enter a meaningful description for the security group.

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

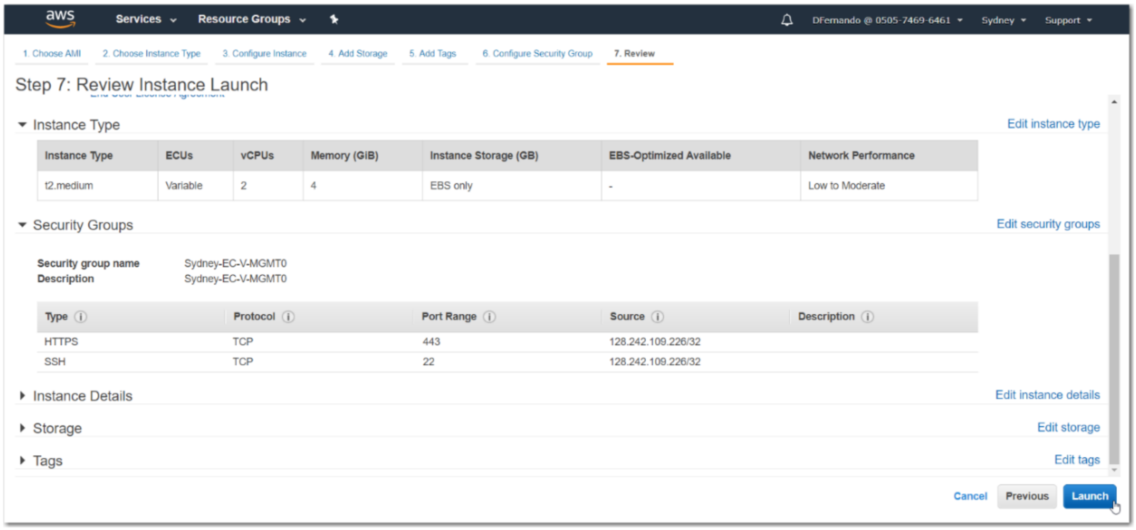
For **Source**, select either **Custom** or **My IP**. This ensures that the MGMT0 interface only allows inbound HTTPS traffic from your current location. When selecting **My IP**, AWS auto-populates your current Public IP in the text box.

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

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

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

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



Step 7: Review Instance Launch

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

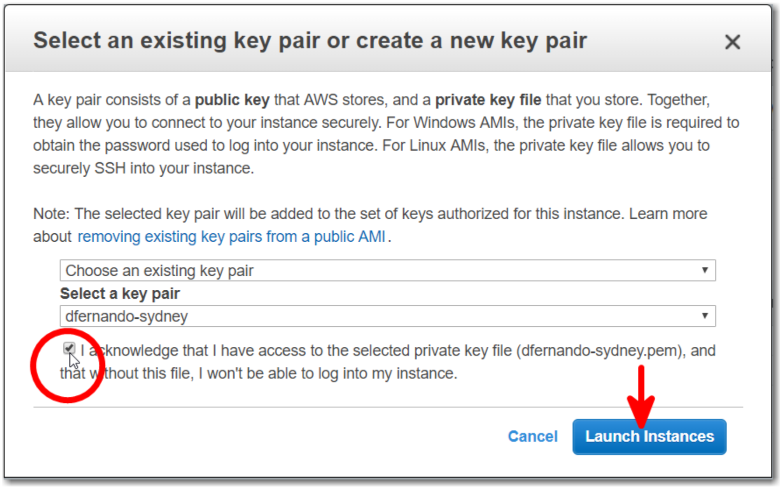
Security Groups

Security group name Sydney-EC-V-MGMT0
Description Sydney-EC-V-MGMT0

Type	Protocol	Port Range	Source	Description
HTTPS	TCP	443	128.242.109.226/32	
SSH	TCP	22	128.242.109.226/32	

The **Select an existing key pair or create a new key pair** page appears.

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



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

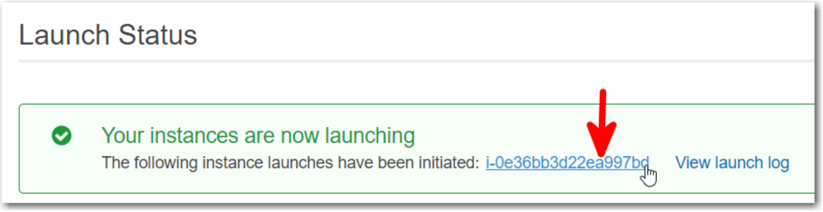
Select a key pair

dfernando-sydney

☑ I acknowledge that I have access to the selected private key file (dfernando-sydney.pem), and that without this file, I won't be able to log into my instance.

The **Launch Status** page appears.

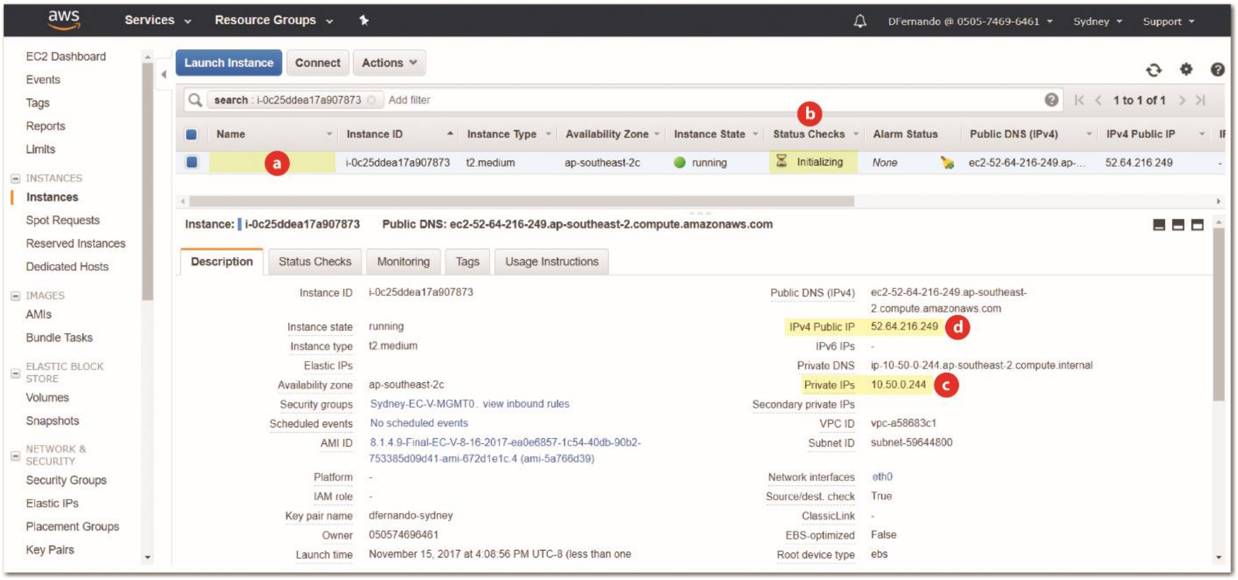
14. To view the instance launch on the EC2 Dashboard, click the instance ID link.



Launch Status

Your instances are now launching

The following instance launches have been initiated: i-0e36bb3d22ea997bd



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IF
	i-0c25ddea17a907873	t2.medium	ap-southeast-2c	running	Initializing	None	ec2-52-64-216-249.ap-...	52.64.216.249	-

Instance: i-0c25ddea17a907873 Public DNS: ec2-52-64-216-249.ap-southeast-2.compute.amazonaws.com

Instance ID	i-0c25ddea17a907873	Public DNS (IPv4)	ec2-52-64-216-249.ap-southeast-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	52.64.216.249
Instance type	t2.medium	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-50-0-244.ap-southeast-2.compute.internal
Availability zone	ap-southeast-2c	Private IPs	10.50.0.244
Security groups	Sydney-EC-V-MGMT0 . view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-a58683c1
AMI ID	8.1.4.9-Final-EC-V-8-16-2017-ea0e6857-1c54-40db-90b2-753385d09d41-ami-672d1e1c.4 (ami-5a766d39)	Subnet ID	subnet-59644800
Platform	-	Network interfaces	eth0
IAM role	-	Source/dest. check	True
Key pair name	dfernando-sydney	ClassicLink	-
Owner	050574696461	EBS-optimized	False
Launch time	November 15, 2017 at 4:08:56 PM UTC-8 (less than one	Root device type	ebs

a. Enter a **Name**.

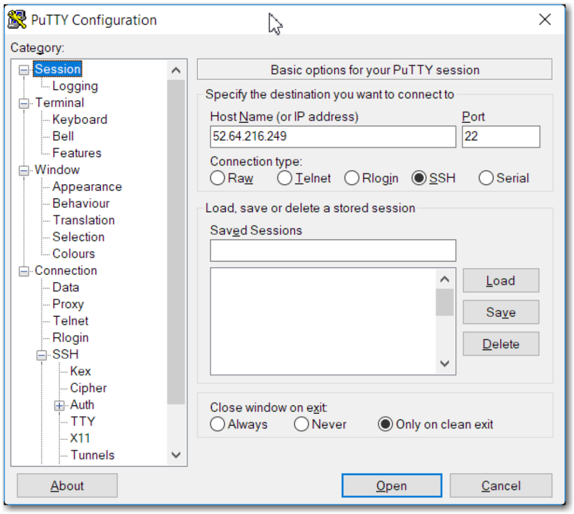
b. Wait until **Status Checks** changes from **Initializing** to **2/2 checks**.

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

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

Create a new password for EC-V

1. Login to the EC-V via SSH.
2. Open PuTTY, and enter the EC-V's Public IP in the **Host Name (or IP Address)** field.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 52.64.216.249

Port: 22

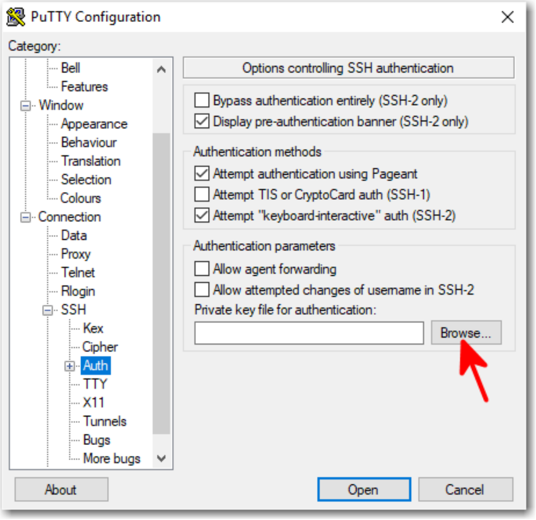
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Close window on exit: ○ Always ○ Never ● Only on clean exit

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



PuTTY Configuration

Options controlling SSH authentication

☐ Bypass authentication entirely (SSH-2 only)
☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

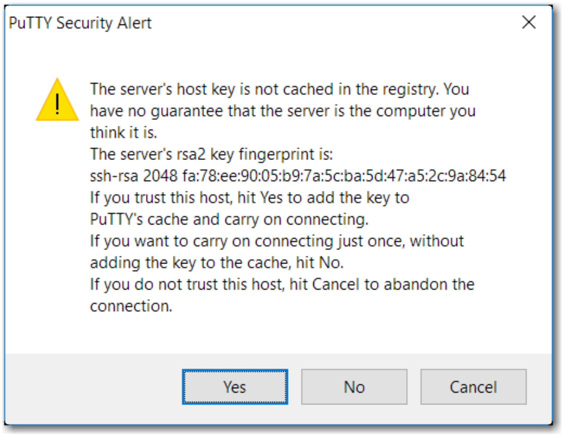
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

4. Select the appropriate .ppk file.
5. Click **Open** to initiate the session. The PuTTY Security Alert appears.
6. Click **Yes** to add the key to the PuTTY's cache.



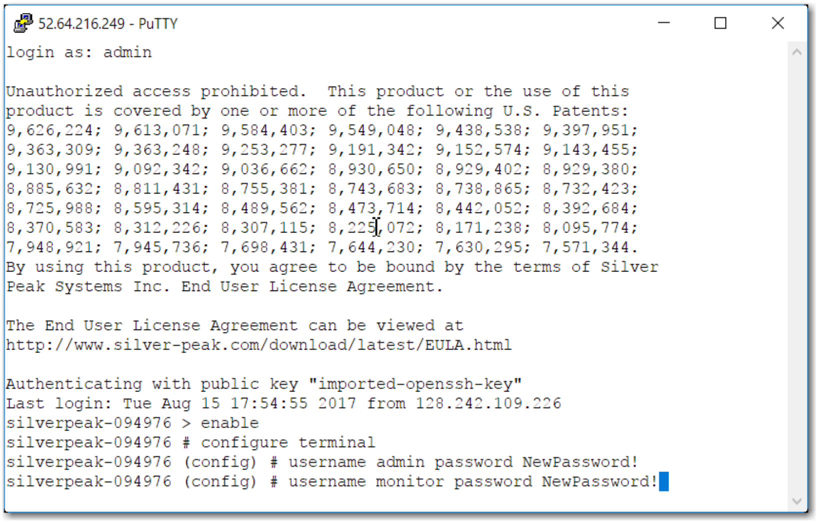
PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 fa:78:ee:90:05:b9:7a:5c:ba:5d:47:a5:2c:9a:84:54
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

7. Login as **admin**.

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

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



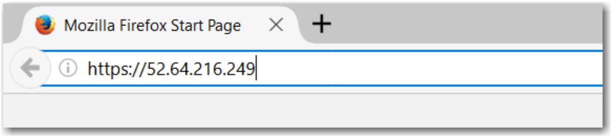
52.64.216.249 - PuTTY

```
login as: admin

Unauthorized access prohibited.  This product or the use of this
product is covered by one or more of the following U.S. Patents:
9,626,224; 9,613,071; 9,584,403; 9,549,048; 9,438,538; 9,397,951;
9,363,309; 9,363,248; 9,253,277; 9,191,342; 9,152,574; 9,143,455;
9,130,991; 9,092,342; 9,036,662; 8,930,650; 8,929,402; 8,929,380;
8,885,632; 8,811,431; 8,755,381; 8,743,683; 8,738,865; 8,732,423;
8,725,988; 8,595,314; 8,489,562; 8,473,714; 8,442,052; 8,392,684;
8,370,583; 8,312,226; 8,307,115; 8,225,072; 8,171,238; 8,095,774;
7,948,921; 7,945,736; 7,698,431; 7,644,230; 7,630,295; 7,571,344.
By using this product, you agree to be bound by the terms of Silver
Peak Systems Inc. End User License Agreement.

The End User License Agreement can be viewed at
http://www.silver-peak.com/download/latest/EULA.html

Authenticating with public key "imported-openssh-key"
Last login: Tue Aug 15 17:54:55 2017 from 128.242.109.226
silverpeak-094976 > enable
silverpeak-094976 # configure terminal
silverpeak-094976 (config) # username admin password NewPassword!
silverpeak-094976 (config) # username monitor password NewPassword!
```

Configure the EC-V with Appliance Manager

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

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



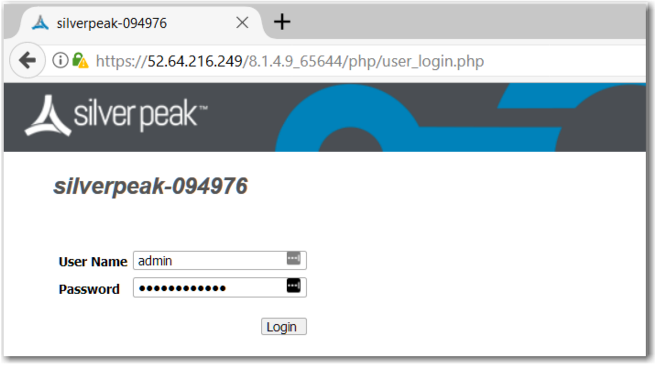
https://52.64.216.249

NOTE: If there's a preconfigured site-to-site VPN or a Direct Connect link established between your current location and the VPC, you should be able to access the MGMT0 interface using its Private IP.

2. To login to the WebUI, enter the following:

   User Name: admin

   Password: <The_Newly_Created_Password>



silverpeak-094976

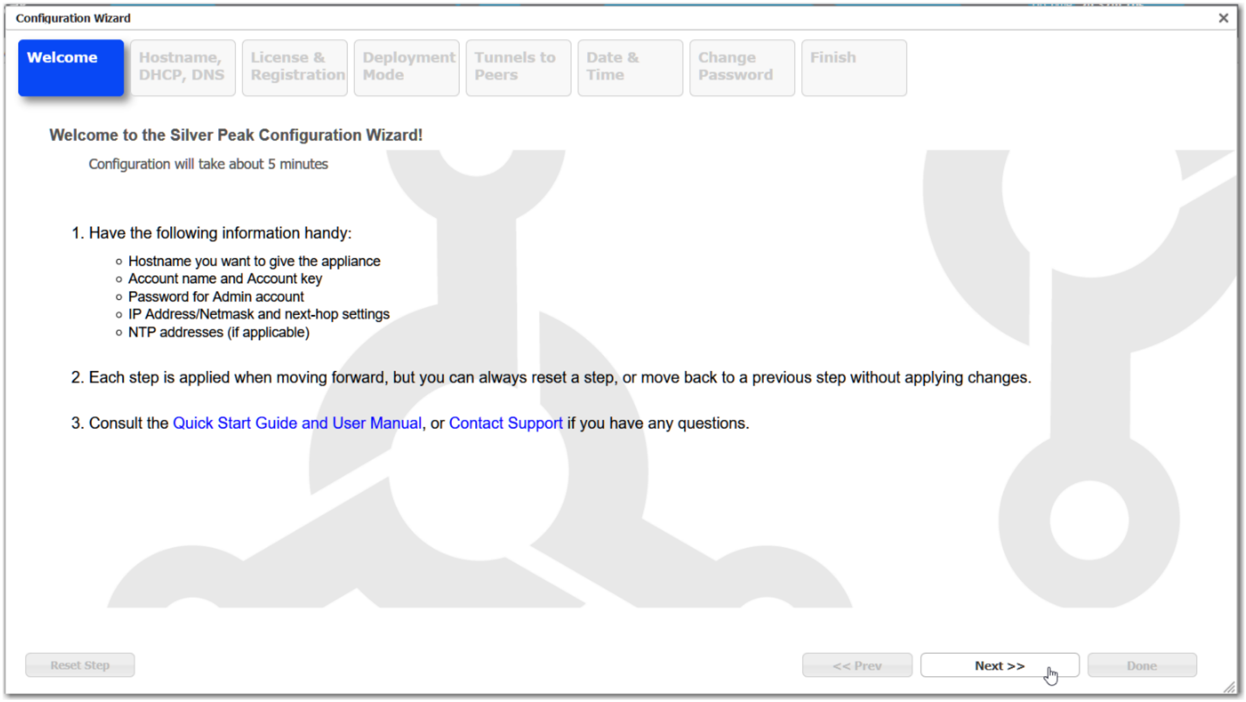
https://52.64.216.249/8.1.4.9_65644/php/user_login.php

silverpeak-094976

User Name: admin

Password: ••••••••••••

The Configuration Wizard opens.



Configuration Wizard

Welcome to the Silver Peak Configuration Wizard!

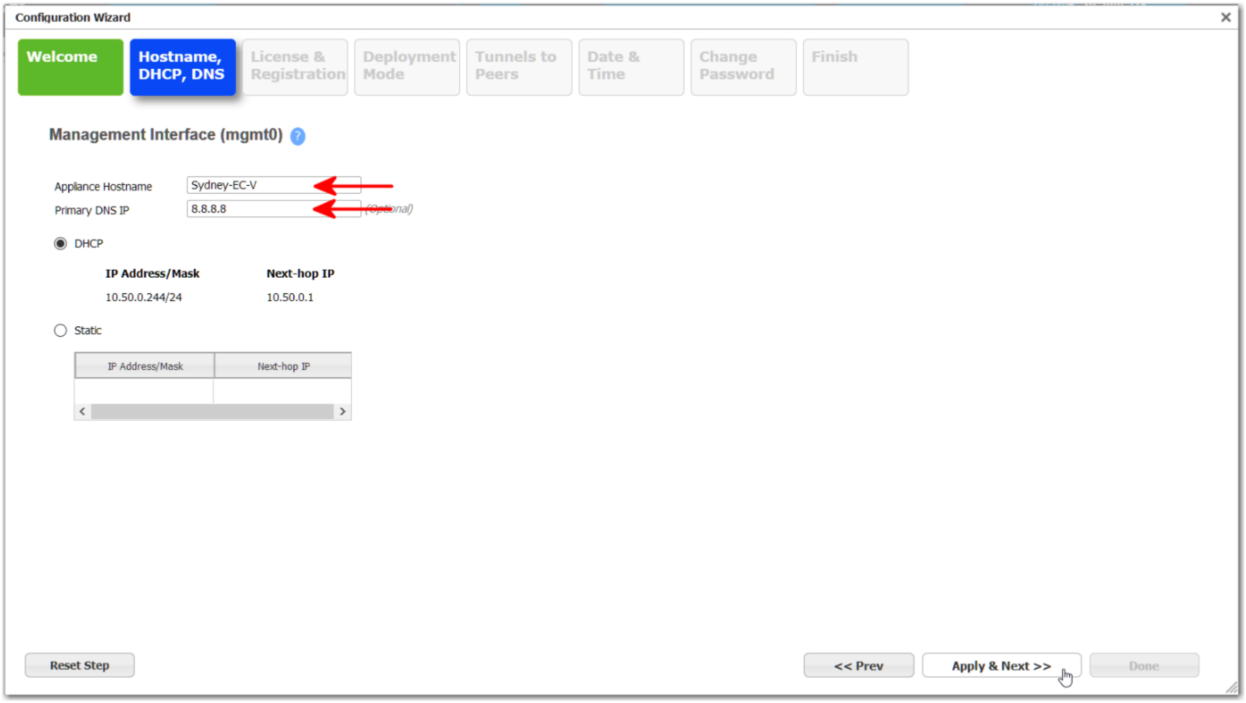
Configuration will take about 5 minutes

1. Have the following information handy:
   - Hostname you want to give the appliance
   - Account name and Account key
   - Password for Admin account
   - IP Address/Netmask and next-hop settings
   - NTP addresses (if applicable)
2. Each step is applied when moving forward, but you can always reset a step, or move back to a previous step without applying changes.
3. Consult the Quick Start Guide and User Manual, or Contact Support if you have any questions.

Click **Next**.

3. In the **Hostname, DHCP, DNS** page, enter the following information:

   - Appliance Hostname
   - Primary DNS IP



Management Interface (mgmt0)

Appliance Hostname: Sydney-EC-V

Primary DNS IP: 8.8.8.8 (Optional)

● DHCP

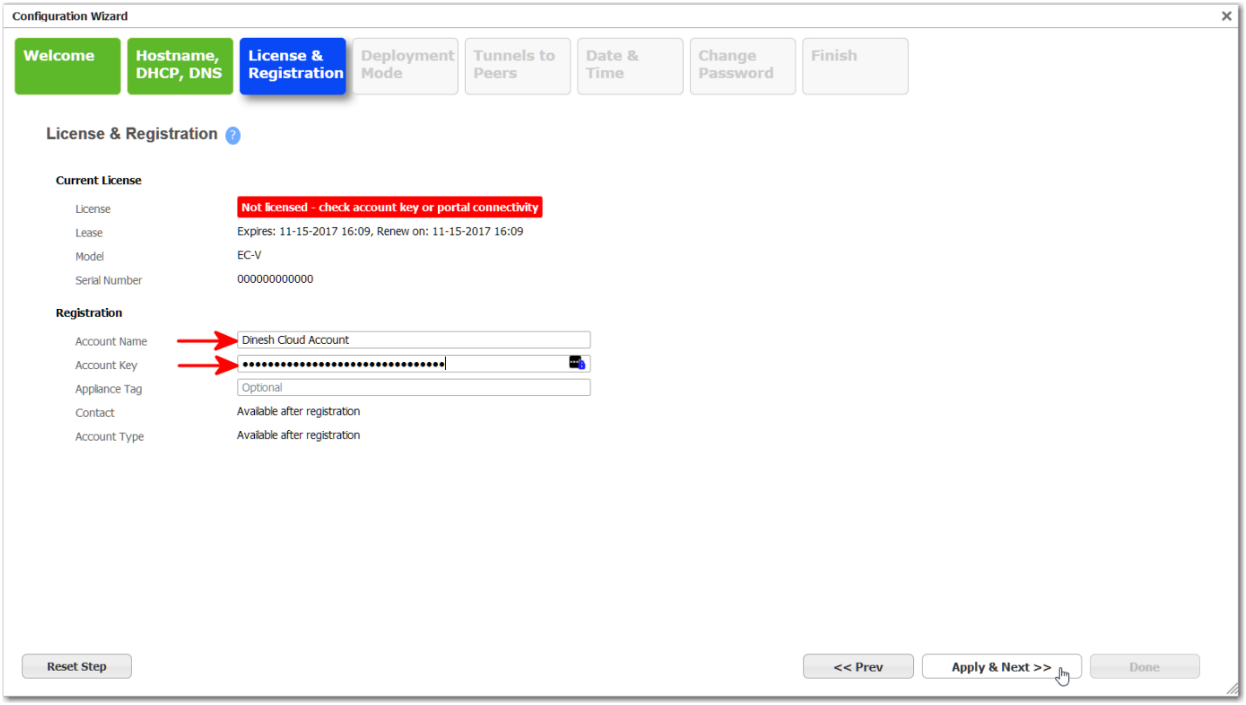
IP Address/Mask	Next-hop IP
10.50.0.244/24	10.50.0.1

○ Static

IP Address/Mask	Next-hop IP

Click **Apply & Next**.

4. In the **License & Registration** page, enter the **Account Name** and **Account Key**.



License & Registration

Current License

License	Not licensed - check account key or portal connectivity
Lease	Expires: 11-15-2017 16:09, Renew on: 11-15-2017 16:09
Model	EC-V
Serial Number	000000000000

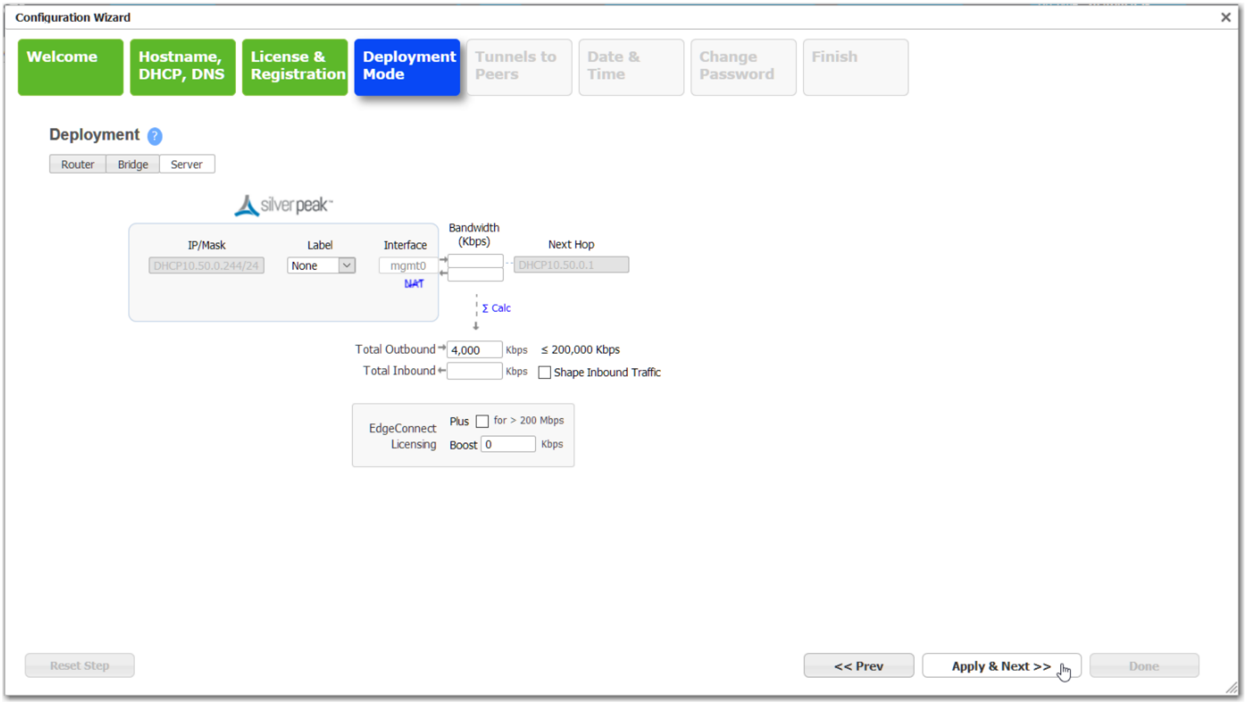
Registration

Account Name	Dinesh Cloud Account
Account Key	••••••••••••••••••••••••••••••••
Appliance Tag	Optional
Contact	Available after registration
Account Type	Available after registration

Click **Apply & Next**.

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

NOTE: Later, after adding the Elastic Network Interfaces (ENI) for WAN0 and LAN0 in AWS, we'll change the deployment mode from Server to Router.



Deployment

Router | Bridge | Server

IP/Mask	Label	Interface	Bandwidth (Kbps)	Next Hop
DHCP10.50.0.244/24	None	mgmt0 NAT		DHCP10.50.0.1

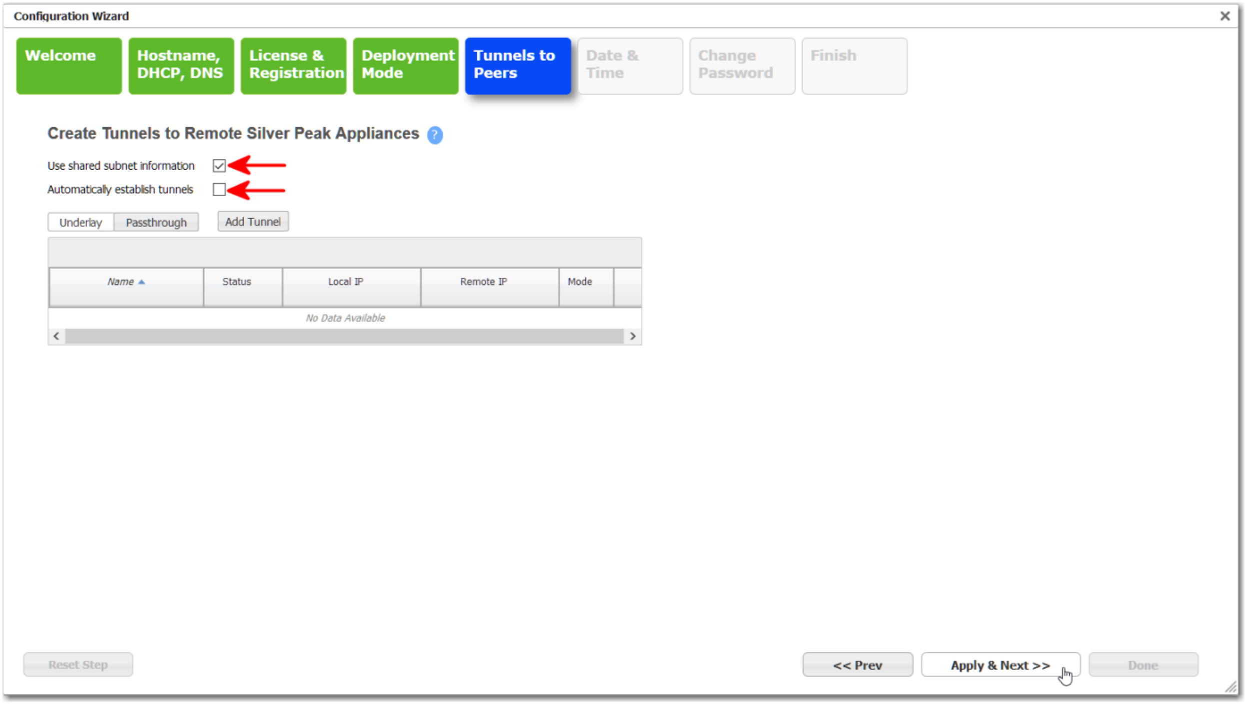
Total Outbound 4,000 Kbps ≤ 200,000 Kbps

Total Inbound Kbps □ Shape Inbound Traffic

EdgeConnect Licensing: Plus □ for > 200 Mbps; Boost 0 Kbps

Click **Apply & Next**.

6. In the **Tunnels to Peers** page, do the following:



Create Tunnels to Remote Silver Peak Appliances

Use shared subnet information ☑

Automatically establish tunnels □

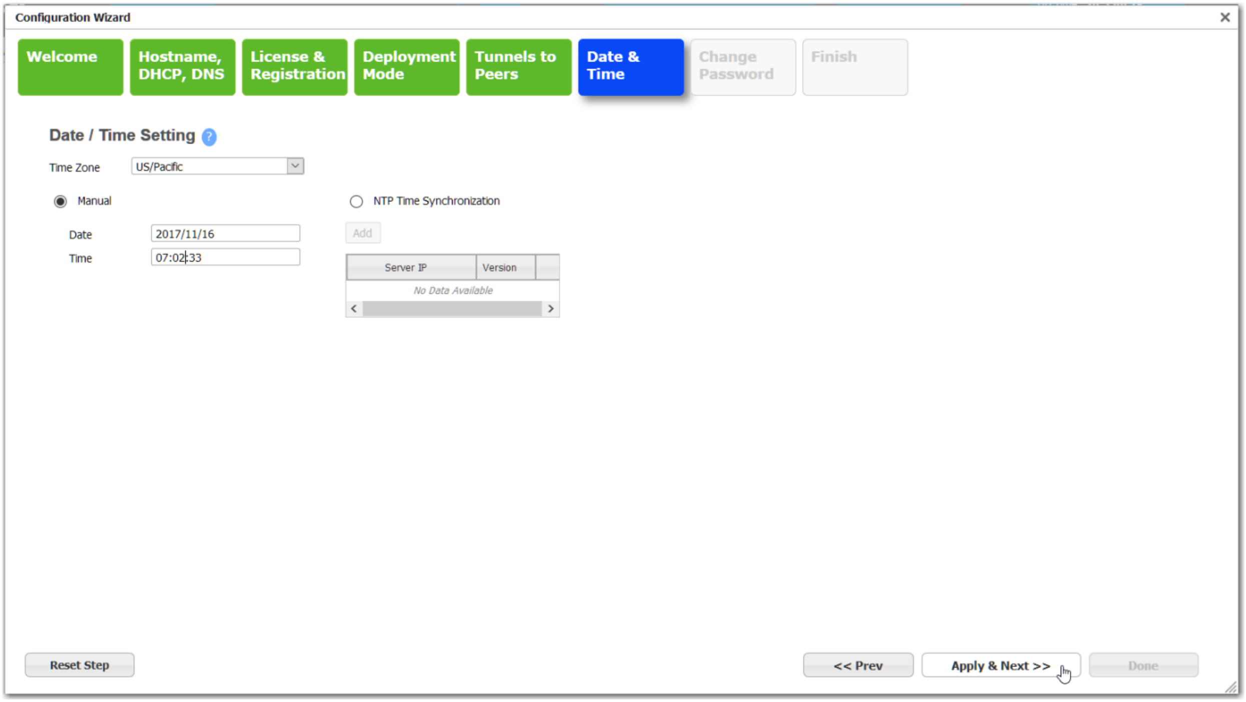
Name ▲	Status	Local IP	Remote IP	Mode
No Data Available				

   a. Select **Use shared subnet information**.

   b. Deselect **Automatically establish tunnels**. (This item only displays in versions prior to 8.1.7.)

   c. Click **Apply & Next**.

7. In the **Date & Time** page, set the time zone and click **Apply & Next**.



Date / Time Setting

Time Zone: US/Pacific

● Manual

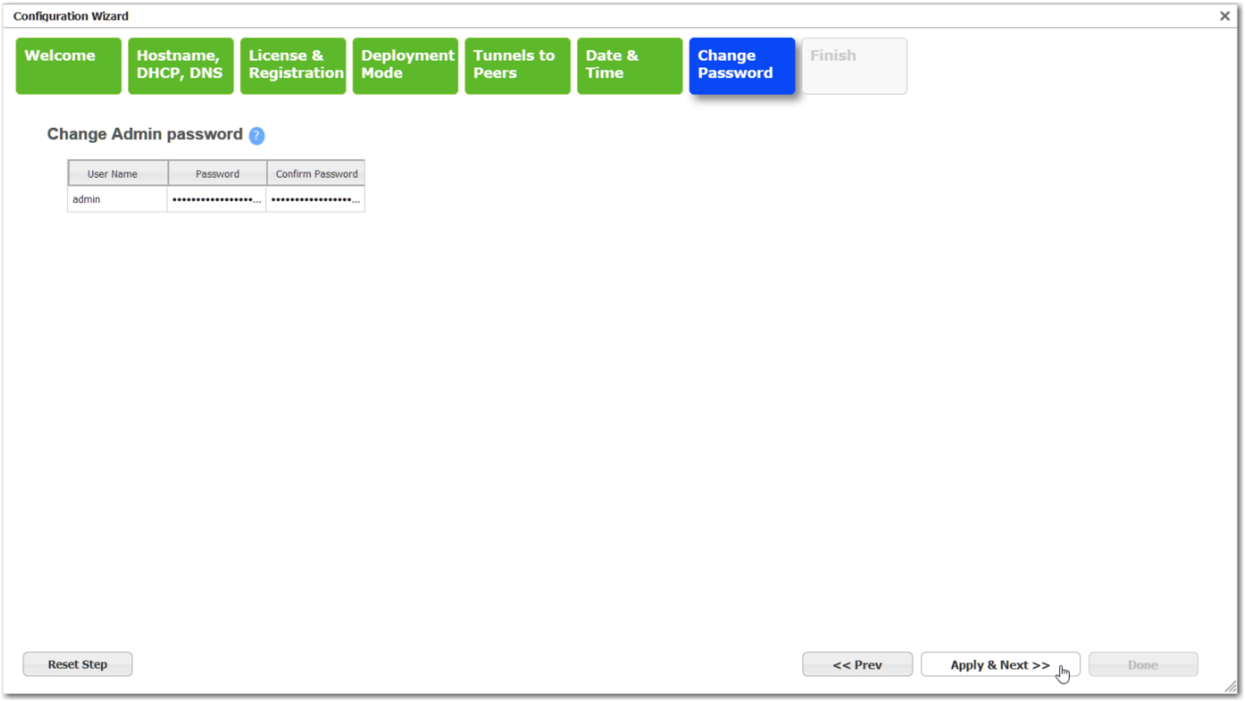
○ NTP Time Synchronization

Date: 2017/11/16

Time: 07:02:33

Server IP	Version
No Data Available	

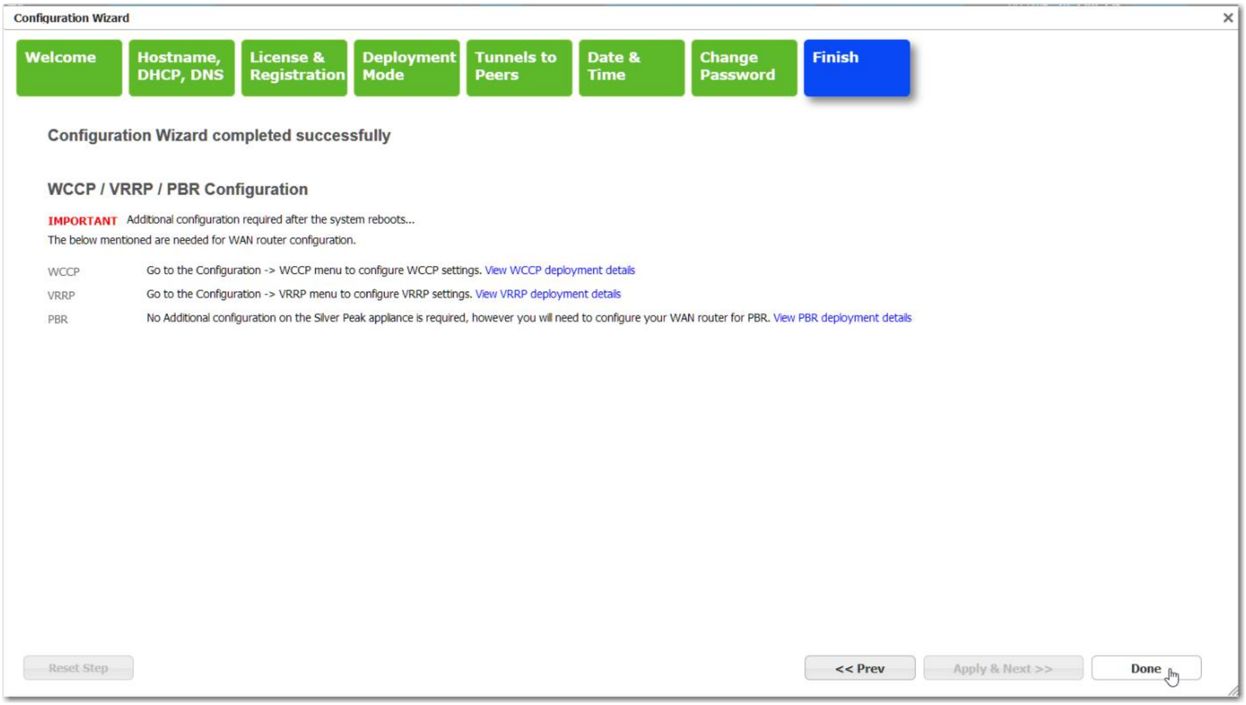
8. The **Change Password** page needs no changes. Since the password was setup earlier, simply click **Apply & Next** to proceed to the next page.



Change Admin password

User Name	Password	Confirm Password
admin	••••••••••••••••...	••••••••••••••••...

9. When the **Finish** page appears, click **Done** to complete the configuration wizard.



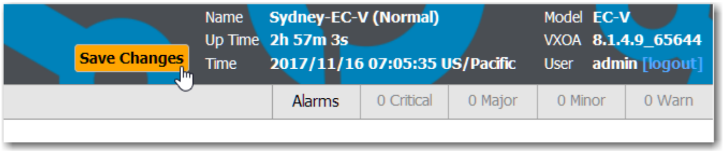
Configuration Wizard completed successfully

WCCP / VRRP / PBR Configuration

IMPORTANT Additional configuration required after the system reboots...
The below mentioned are needed for WAN router configuration.

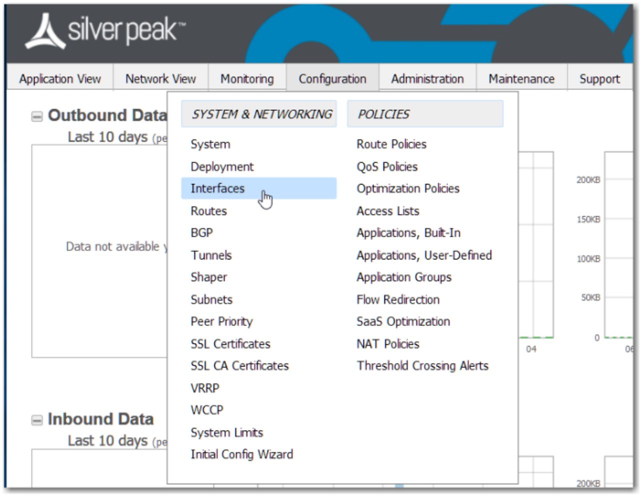
WCCP	Go to the Configuration -> WCCP menu to configure WCCP settings. View WCCP deployment details
VRRP	Go to the Configuration -> VRRP menu to configure VRRP settings. View VRRP deployment details
PBR	No Additional configuration on the Silver Peak appliance is required, however you will need to configure your WAN router for PBR. View PBR deployment details

10. Click **Save Changes**.

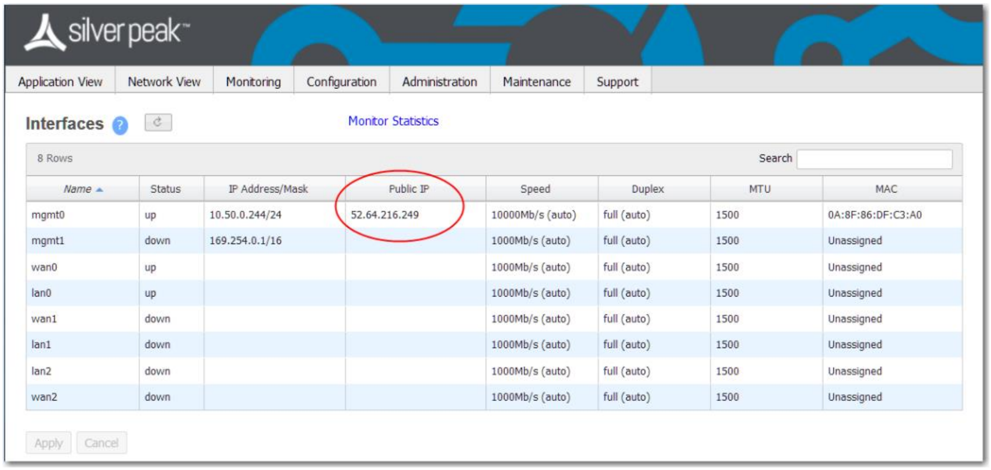


Name	Sydney-EC-V (Normal)	Model	EC-V
Up Time	2h 57m 3s	VXOA	8.1.4.9_65644
Time	2017/11/16 07:05:35 US/Pacific	User	admin [logout]

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



Verify that the MAC address, the Private IP, and the Public IP (assigned by Amazon) are properly assigned on the MGMT0 interface.



Interfaces

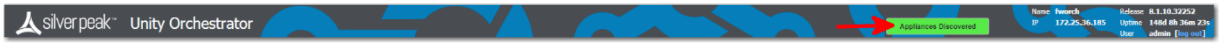
8 Rows

Name	Status	IP Address/Mask	Public IP	Speed	Duplex	MTU	MAC
mgmt0	up	10.50.0.244/24	52.64.216.249	10000Mb/s (auto)	full (auto)	1500	0A:8F:86:DF:C3:A0
mgmt1	down	169.254.0.1/16		1000Mb/s (auto)	full (auto)	1500	Unassigned
wan0	up			1000Mb/s (auto)	full (auto)	1500	Unassigned
lan0	up			1000Mb/s (auto)	full (auto)	1500	Unassigned
wan1	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
lan1	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
lan2	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
wan2	down			1000Mb/s (auto)	full (auto)	1500	Unassigned

Add the EC-V to the Orchestrator.

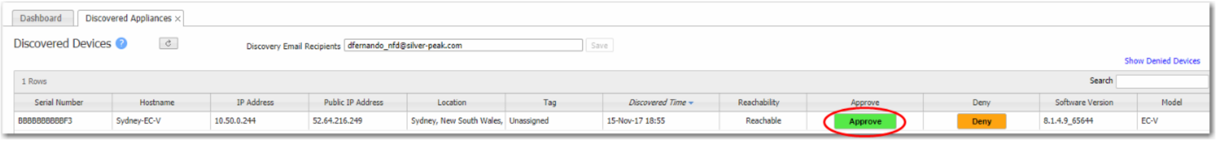
By now, the EC-V has communicated with the Silver Peak Cloud Portal. As a result, it appears on the Silver Peak Orchestrator as a new appliance that is ready to be added to the SD-WAN fabric.

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



Name fworch
IP 172.25.36.185
Release 8.1.10.32252
Uptime 148d 8h 36m 23s
User admin [log out]

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



Discovered Devices

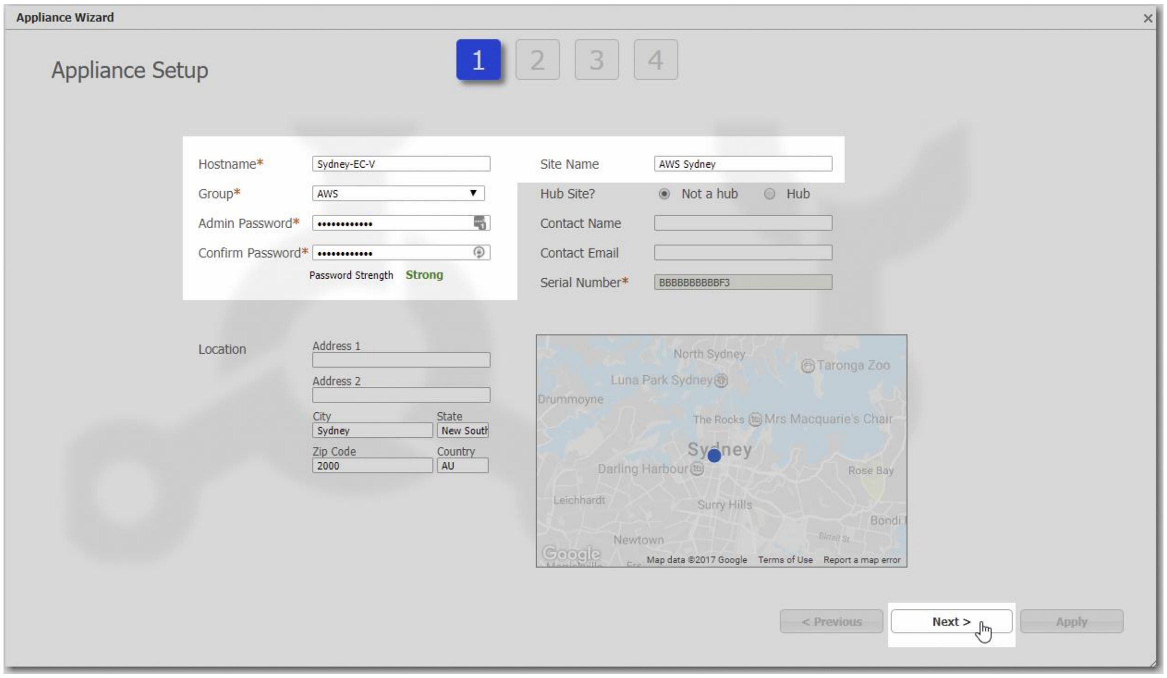
Discovery Email Recipients dfernando_nfd@silver-peak.com

1 Rows

Serial Number	Hostname	IP Address	Public IP Address	Location	Tag	Discovered Time	Reachability	Approve	Deny	Software Version	Model
BBBBBBBBBBF3	Sydney-EC-V	10.50.0.244	52.64.216.249	Sydney, New South Wales,	Unassigned	15-Nov-17 18:55	Reachable	Approve	Deny	8.1.4.9_65644	EC-V

The Appliance Wizard appears.

3. Enter the **admin password** that you previously configured and the **Site Name** (an existing region in your AWS account). Then click **Next**.



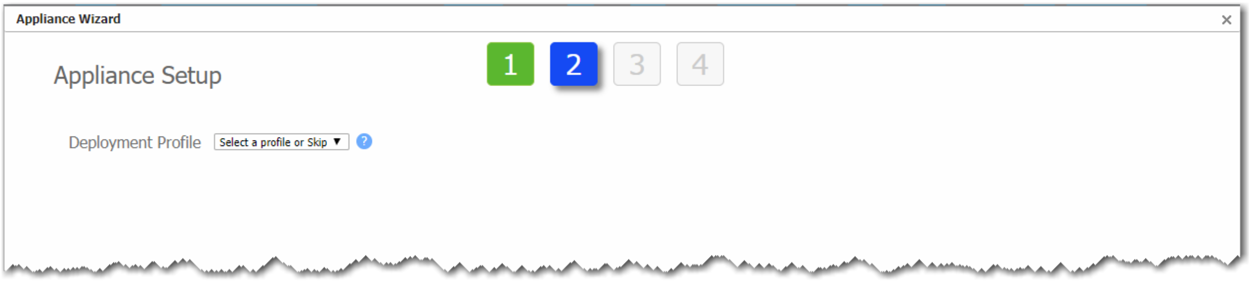
Appliance Setup

Hostname* Sydney-EC-V
Group* AWS
Admin Password* ••••••••••••
Confirm Password* ••••••••••••
Password Strength Strong

Site Name AWS Sydney
Hub Site? ● Not a hub ○ Hub
Contact Name
Contact Email
Serial Number* BBBBBBBBBBF3

Location
Address 1
Address 2
City Sydney
State New South
Zip Code 2000
Country AU

4. Leave the **Deployment Profile** field unchanged, and click **Next**.



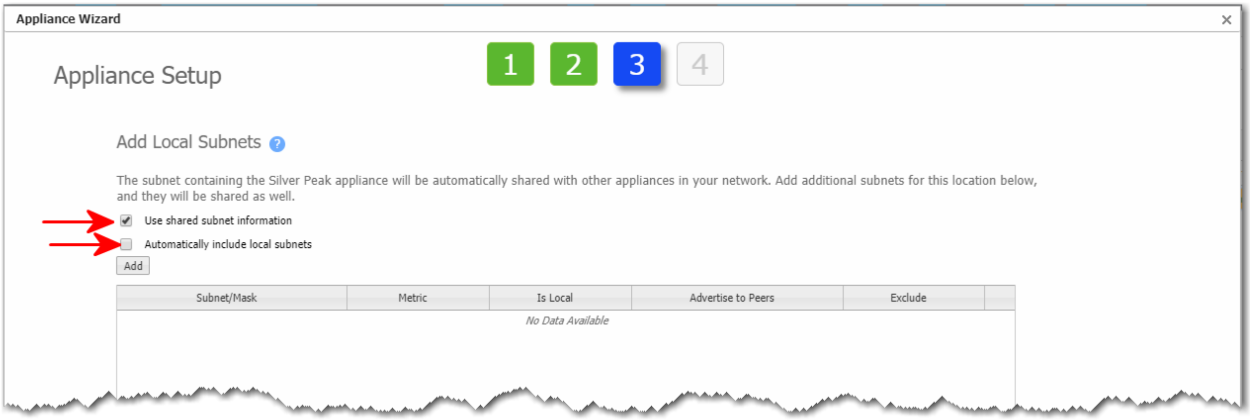
Appliance Wizard ×

Appliance Setup

1 2 3 4

Deployment Profile: Select a profile or Skip ▼

5. On the Add Local Subnets page, do the following:



Appliance Wizard ×

Appliance Setup

1 2 3 4

Add Local Subnets

The subnet containing the Silver Peak appliance will be automatically shared with other appliances in your network. Add additional subnets for this location below, and they will be shared as well.

☑ Use shared subnet information

□ Automatically include local subnets

Add

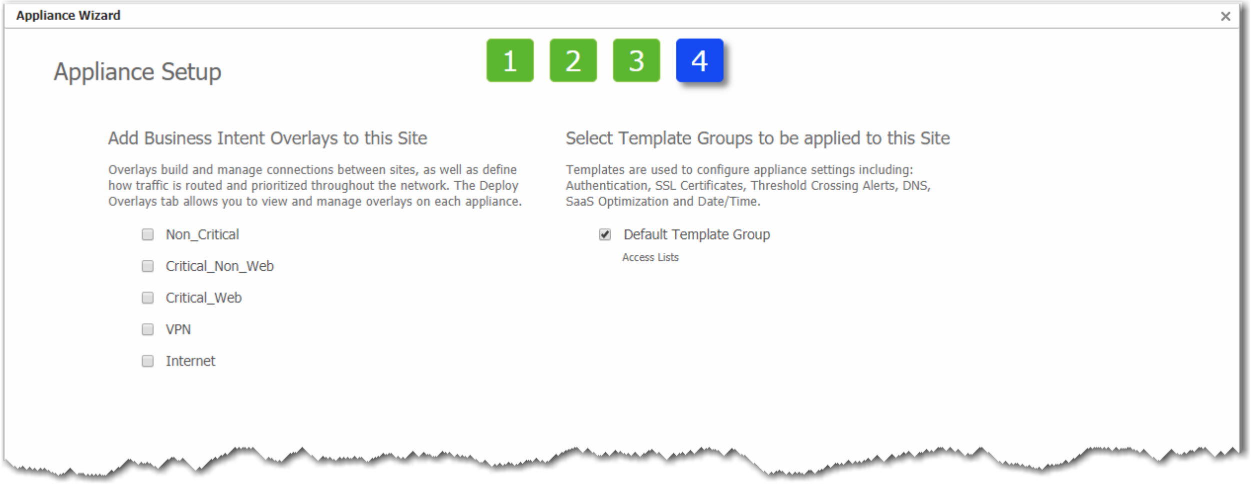
Subnet/Mask	Metric	Is Local	Advertise to Peers	Exclude
		No Data Available		

   a. Select **Use shared subnet information**.

   b. Deselect **Automatically include local subnets**.

   c. Click **Next**.

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



Appliance Wizard ×

Appliance Setup

1 2 3 4

Add Business Intent Overlays to this Site

Overlays build and manage connections between sites, as well as define how traffic is routed and prioritized throughout the network. The Deploy Overlays tab allows you to view and manage overlays on each appliance.

□ Non_Critical

□ Critical_Non_Web

□ Critical_Web

□ VPN

□ Internet

Select Template Groups to be applied to this Site

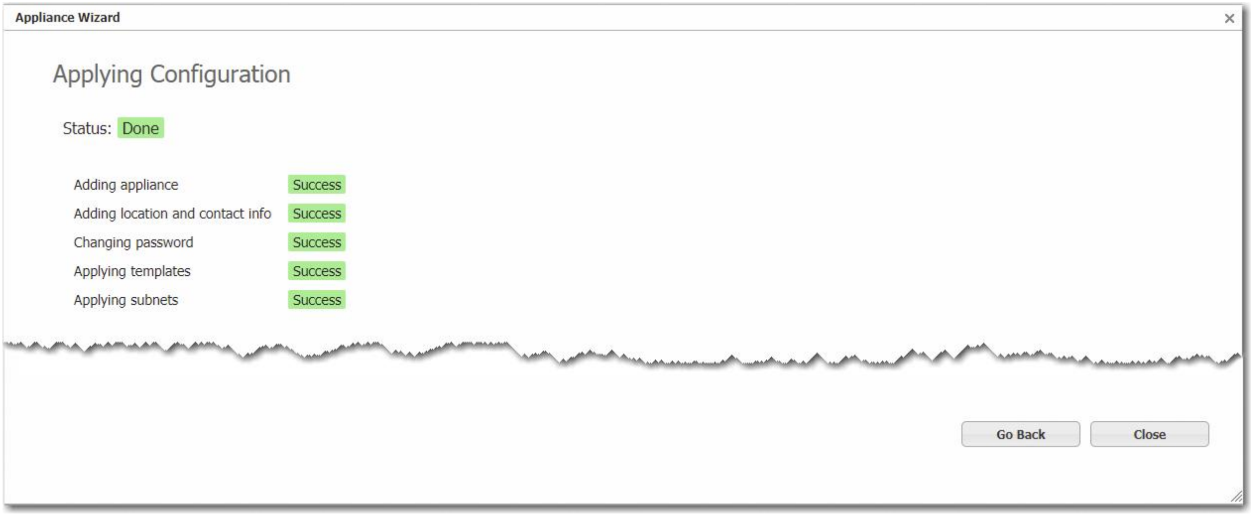
Templates are used to configure appliance settings including: Authentication, SSL Certificates, Threshold Crossing Alerts, DNS, SaaS Optimization and Date/Time.

☑ Default Template Group

Access Lists

Click **Apply**.

7. After the wizard has finished applying the configuration, click **Close**.



Appliance Wizard

Applying Configuration

Status: Done

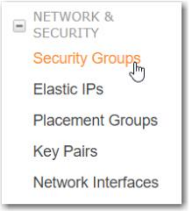
Adding appliance	Success
Adding location and contact info	Success
Changing password	Success
Applying templates	Success
Applying subnets	Success

You have now successfully added the EC-V into the SD-WAN fabric.

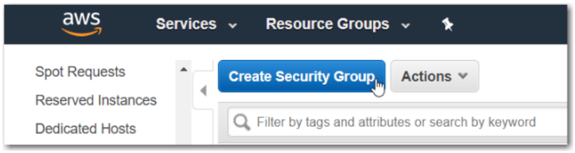
Create Security Groups for the LAN0 and WAN0 interfaces

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

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

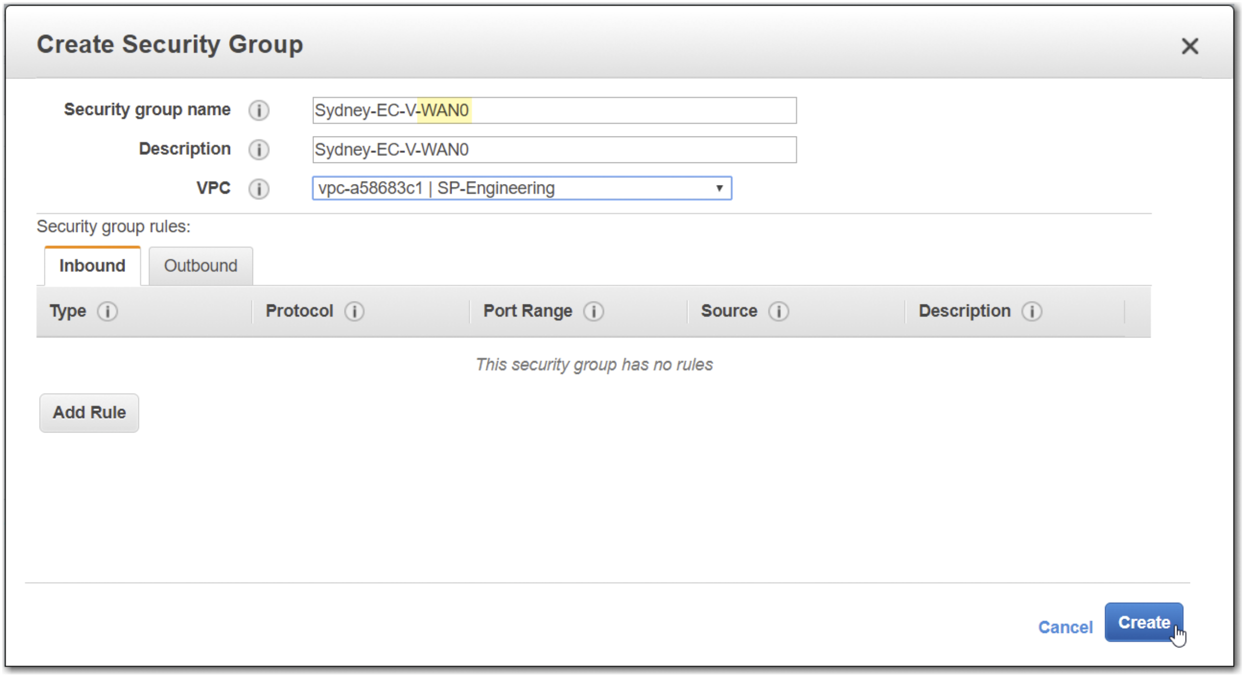


2. Click Create Security Group



The **Create Security Group** page appears.

3. First, let’s create a Security Group for the WAN0 interface. Enter a **Security group name, Description,** and select the **VPC** where you want the Security Group to reside.



Create Security Group

Security group name: Sydney-EC-V-WAN0

Description: Sydney-EC-V-WAN0

VPC: vpc-a58683c1 | SP-Engineering

Security group rules:

Type	Protocol	Port Range	Source	Description

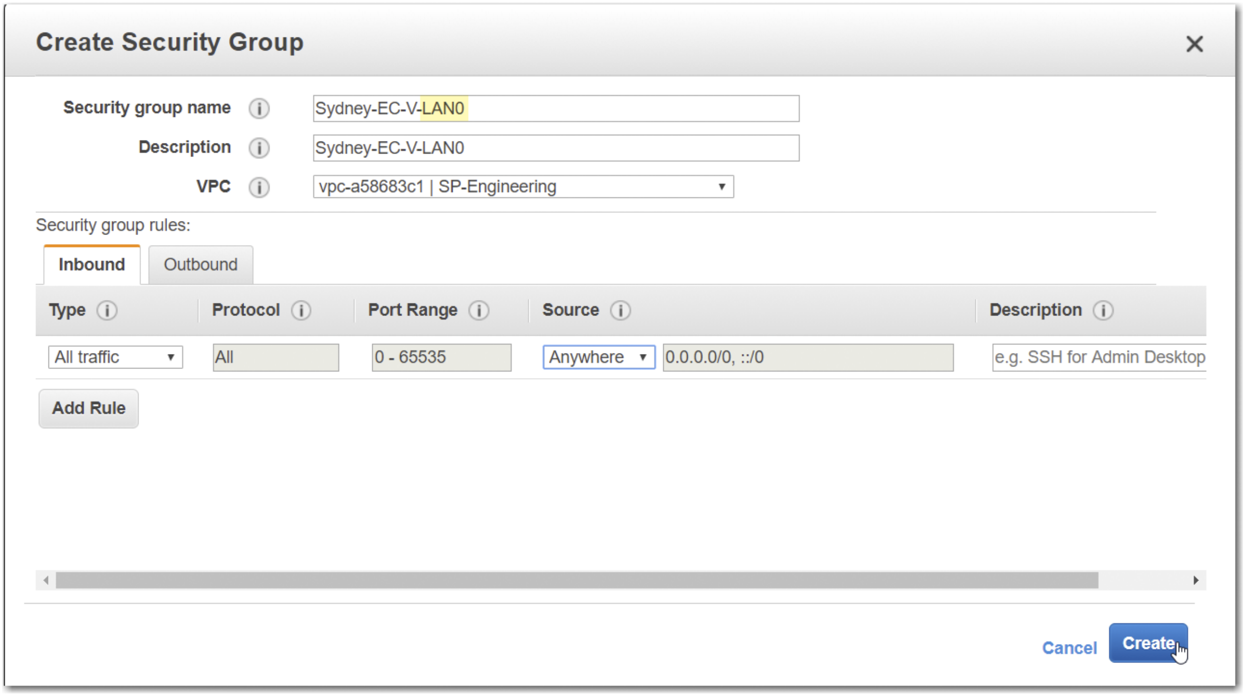
This security group has no rules

Accept the default settings and click **Create.**
By default, no traffic is allowed inbound. Conversely, by default, all outbound traffic is allowed.

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

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

5. Select the **Inbound** tab and click **Add Rule**. Under Source, select **Anywhere**. Next, click **Create**.



Create Security Group

Security group name: Sydney-EC-V-LAN0

Description: Sydney-EC-V-LAN0

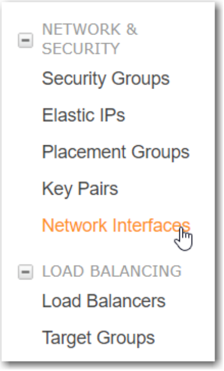
VPC: vpc-a58683c1 | SP-Engineering

Security group rules:

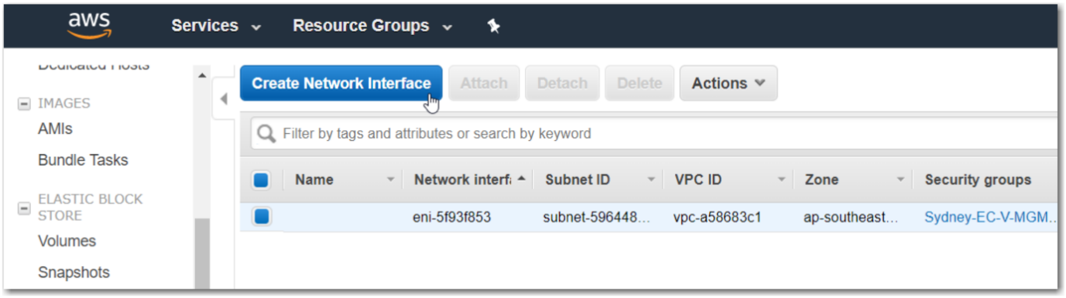
Type	Protocol	Port Range	Source		Description
All traffic	All	0 - 65535	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Create LAN0 and WAN0 Elastic Network Interfaces (ENIs)

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



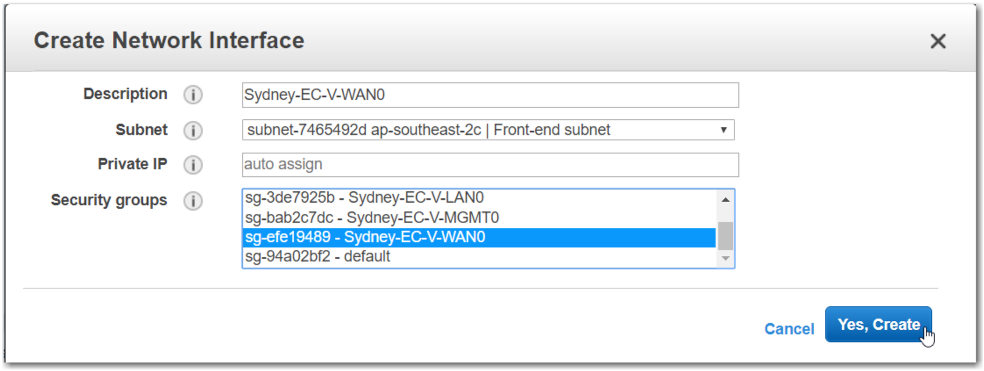
2. Click **Create Network Interface**.



Name	Network interf	Subnet ID	VPC ID	Zone	Security groups
	eni-5f93f853	subnet-596448...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-MGM...

The **Create Network Interface** page appears.

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

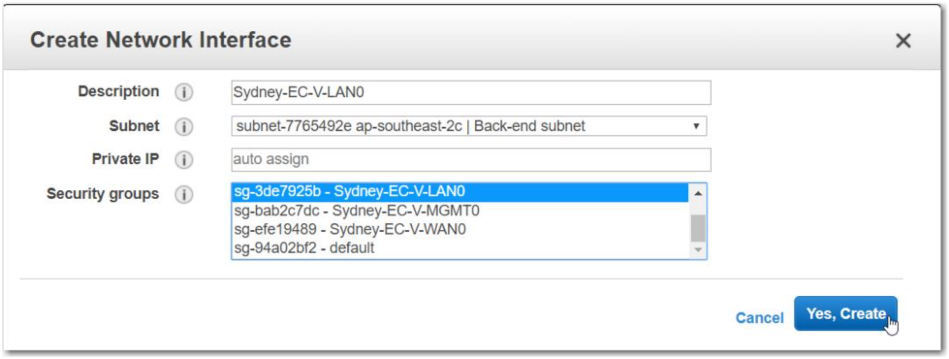


Create Network Interface

Description	Sydney-EC-V-WAN0
Subnet	subnet-7465492d ap-southeast-2c | Front-end subnet
Private IP	auto assign
Security groups	sg-3de7925b - Sydney-EC-V-LAN0 sg-bab2c7dc - Sydney-EC-V-MGMT0 sg-efe19489 - Sydney-EC-V-WAN0 sg-94a02bf2 - default

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

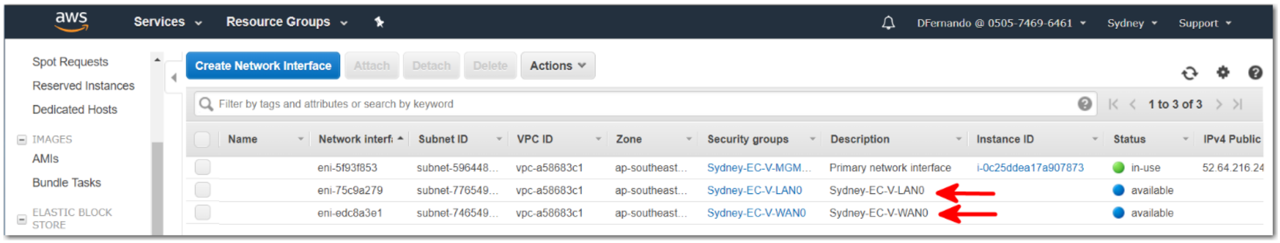
4. Next, create the LAN0 ENI. As you did with the WAN0 ENI, enter a **Description**, **Subnet**, **Private IP**, and select the **LAN0 Security Group**. Leave the **Private IP** blank if you want AWS to automatically assign an IP address for the LAN0 interface.



Description	Sydney-EC-V-LAN0
Subnet	subnet-7765492e ap-southeast-2c | Back-end subnet
Private IP	auto assign
Security groups	sg-3de7925b - Sydney-EC-V-LAN0 sg-bab2c7dc - Sydney-EC-V-MGMT0 sg-efe19489 - Sydney-EC-V-WAN0 sg-94a02bf2 - default

Click **Yes, Create** to create the LAN0 ENI.

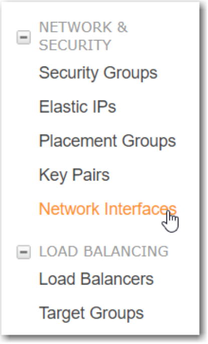
Note that the WAN0 and LAN0 ENIs have been added to the list of available interfaces.



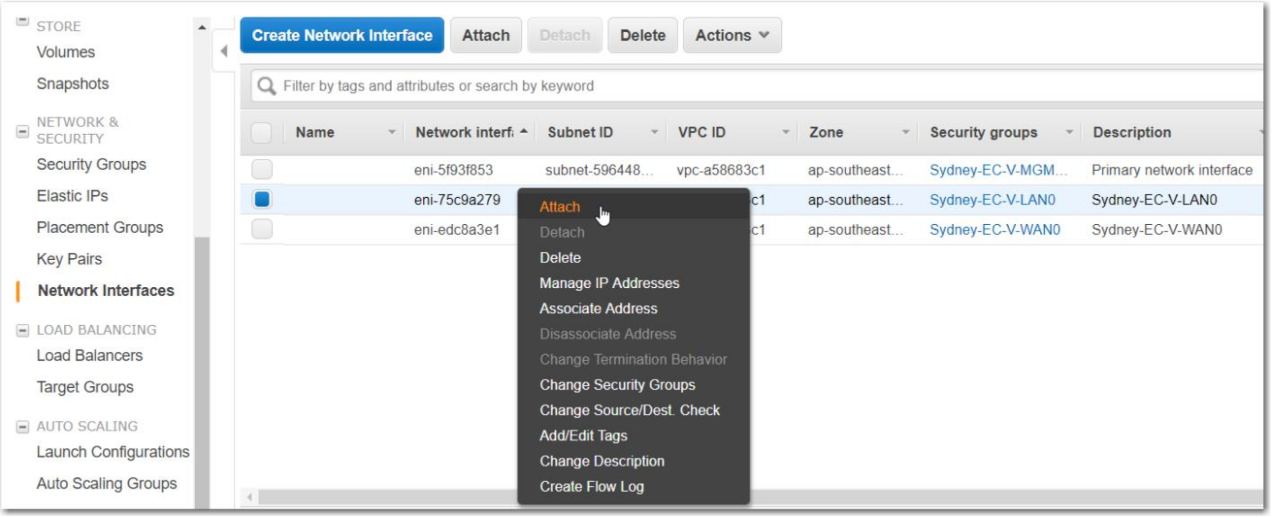
Name	Network interf	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID	Status	IPv4 Public
	eni-5f93f853	subnet-596448...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-MGM...	Primary network interface	i-0c25ddea17a907873	in-use	52.64.216.24
	eni-75c9a279	subnet-776549...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-LAN0	Sydney-EC-V-LAN0		available	
	eni-edc8a3e1	subnet-746549...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-WAN0	Sydney-EC-V-WAN0		available	

Attach the ENIs to the EC-V

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



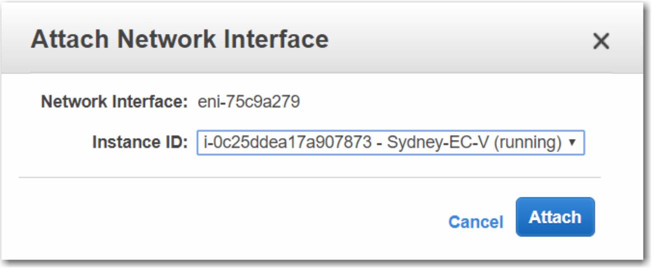
2. Select the LAN0 ENI, right-click, and click **Attach**.



Name	Network interf	Subnet ID	VPC ID	Zone	Security groups	Description
	eni-5f93f853	subnet-596448...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-MGM...	Primary network interface
	eni-75c9a279		c1	ap-southeast...	Sydney-EC-V-LAN0	Sydney-EC-V-LAN0
	eni-edc8a3e1		c1	ap-southeast...	Sydney-EC-V-WAN0	Sydney-EC-V-WAN0

The **Attach Network Interface** page appears.

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



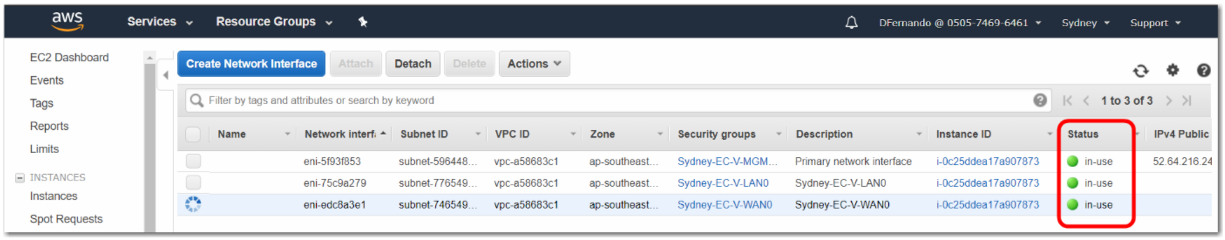
Attach Network Interface

Network Interface: eni-75c9a279

Instance ID: i-0c25ddea17a907873 - Sydney-EC-V (running)

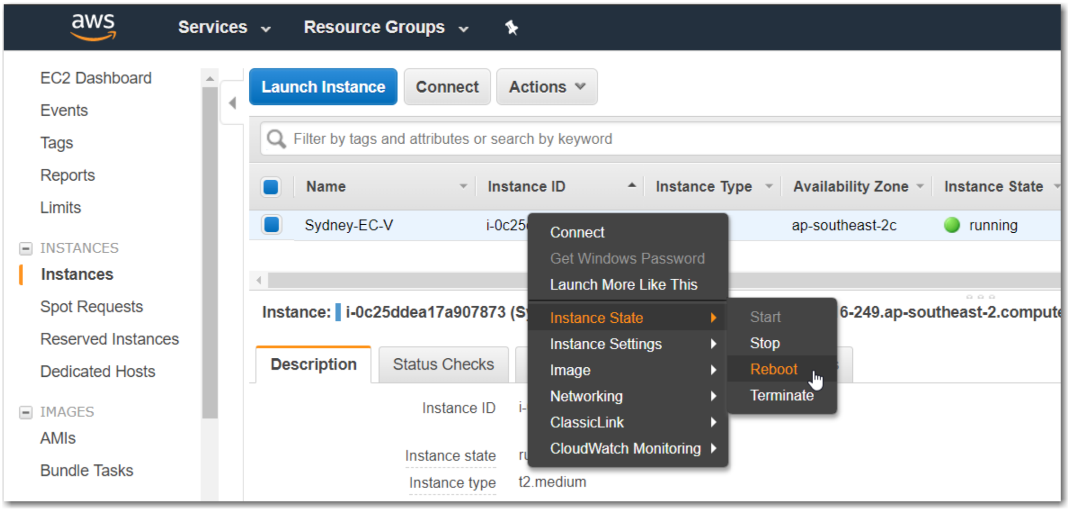
4. Similarly, attach the WAN0 ENI to the EC-V.

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



Name	Network interf.	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID	Status	IPv4 Public
	eni-5f93f853	subnet-596448...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-MGM...	Primary network interface	i-0c25ddea17a907873	● in-use	52.64.216.24
	eni-75c9a279	subnet-776549...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-LAN0	Sydney-EC-V-LAN0	i-0c25ddea17a907873	● in-use	
	eni-edc8a3e1	subnet-746549...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-WAN0	Sydney-EC-V-WAN0	i-0c25ddea17a907873	● in-use	

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



Name	Instance ID	Instance Type	Availability Zone	Instance State
Sydney-EC-V	i-0c25		ap-southeast-2c	● running

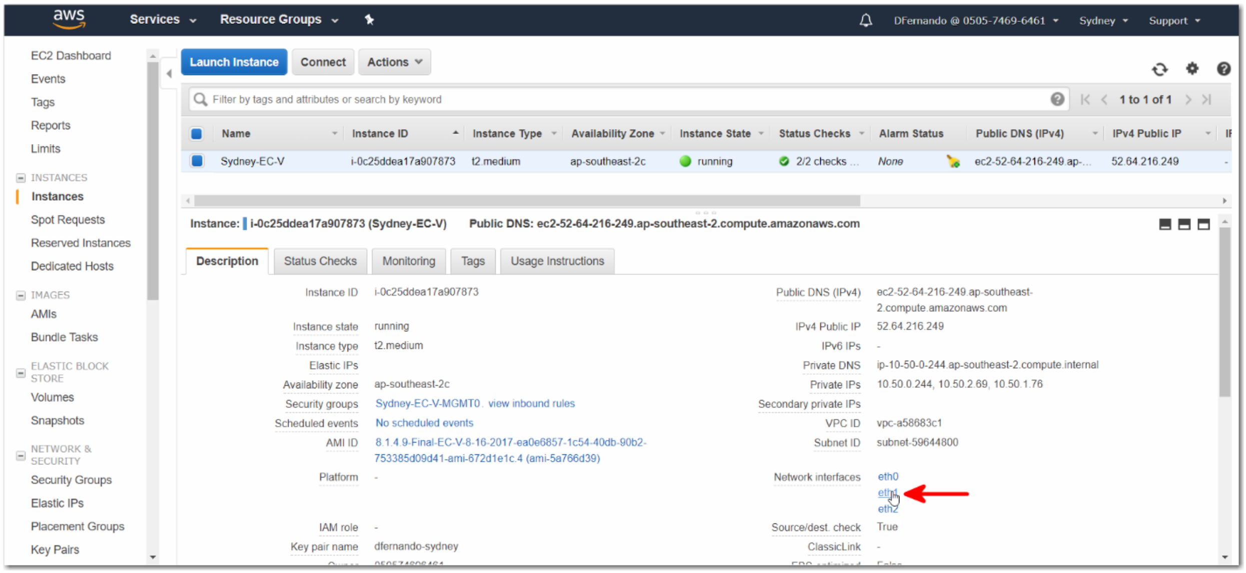
Instance: i-0c25ddea17a907873 (S... 6-249.ap-southeast-2.compute

Instance ID i-

Instance state ru

Instance type t2.medium

6. After the VM reboots, verify the MAC addresses of the newly-attached ENIs.
   a. In the **Description** tab, select the **EC-V** and click **eth1**.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
Sydney-EC-V	i-0c25ddea17a907873	t2.medium	ap-southeast-2c	running	2/2 checks ...	None	ec2-52-64-216-249.ap-...	52.64.216.249

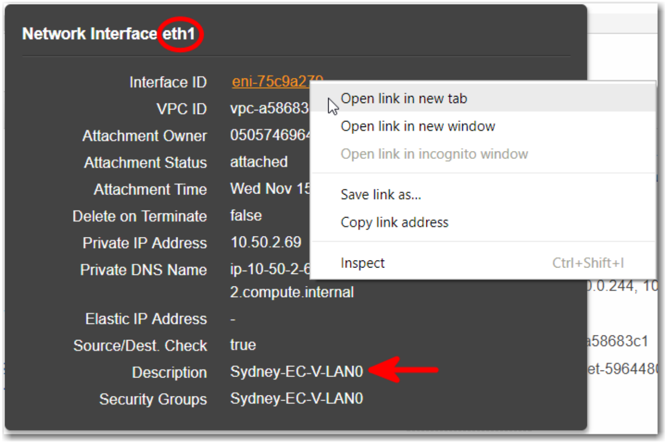
Instance: i-0c25ddea17a907873 (Sydney-EC-V)   Public DNS: ec2-52-64-216-249.ap-southeast-2.compute.amazonaws.com

Instance ID i-0c25ddea17a907873
Instance state running
Instance type t2.medium
Elastic IPs
Availability zone ap-southeast-2c
Security groups Sydney-EC-V-MGMT0 . view inbound rules
Scheduled events No scheduled events
AMI ID 8.1.4.9-Final-EC-V-8-16-2017-ea0e6857-1c54-40db-90b2-753385d09d41-ami-672d1e1c.4 (ami-5a766d39)
Platform -
IAM role -
Key pair name dfernando-sydney

Public DNS (IPv4) ec2-52-64-216-249.ap-southeast-2.compute.amazonaws.com
IPv4 Public IP 52.64.216.249
IPv6 IPs -
Private DNS ip-10-50-0-244.ap-southeast-2.compute.internal
Private IPs 10.50.0.244, 10.50.2.69, 10.50.1.76
Secondary private IPs
VPC ID vpc-a58683c1
Subnet ID subnet-59644800
Network interfaces eth0
eth1
eth2
Source/dest. check True
ClassicLink -

The **Network Interface eth1** page appears. As the Description suggests, **eth1** is the **LAN0** interface of the EC-V.

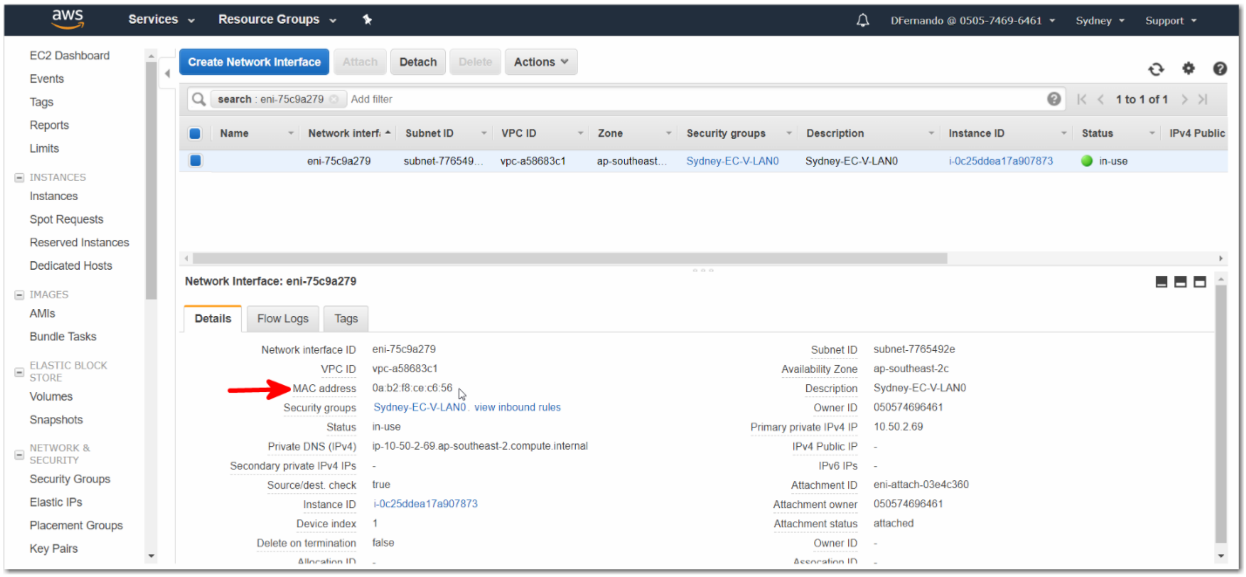
b. Right-click on the **Interface ID link** and open it in a new tab.



Network Interface eth1

Interface ID eni-75c9a279
VPC ID vpc-a58683
Attachment Owner 0505746964
Attachment Status attached
Attachment Time Wed Nov 15
Delete on Terminate false
Private IP Address 10.50.2.69
Private DNS Name ip-10-50-2-6
2.compute.internal
Elastic IP Address -
Source/Dest. Check true
Description Sydney-EC-V-LAN0
Security Groups Sydney-EC-V-LAN0

The **Network interface** page appears. Note the **MAC address** in the **Details** tab.



Name	Network interf.	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID	Status	IPv4 Public
	eni-75c9a279	subnet-776549...	vpc-a58683c1	ap-southeast...	Sydney-EC-V-LAN0	Sydney-EC-V-LAN0	i-0c25ddea17a907873	in-use	

Network Interface: eni-75c9a279

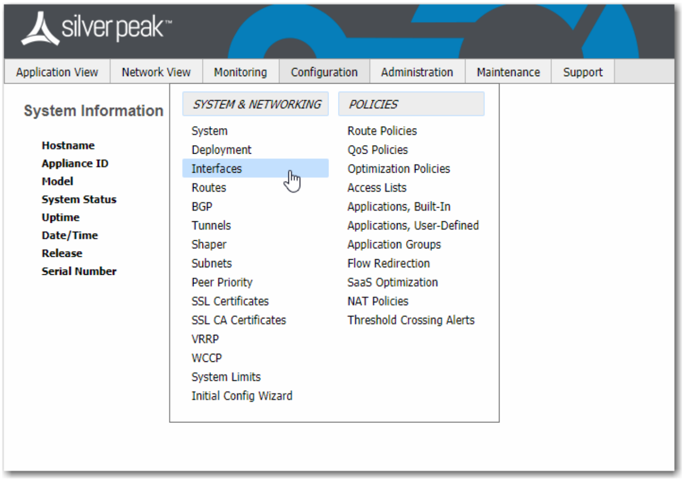
Network interface ID eni-75c9a279
VPC ID vpc-a58683c1
MAC address 0a:b2:f8:ce:c6:56
Security groups Sydney-EC-V-LAN0 . view inbound rules
Status in-use
Private DNS (IPv4) ip-10-50-2-69.ap-southeast-2.compute.internal
Secondary private IPv4 IPs -
Source/dest. check true
Instance ID i-0c25ddea17a907873
Device index 1
Delete on termination false

Subnet ID subnet-7765492e
Availability Zone ap-southeast-2c
Description Sydney-EC-V-LAN0
Owner ID 050574696461
Primary private IPv4 IP 10.50.2.69
IPv4 Public IP -
IPv6 IPs -
Attachment ID eni-attach-03e4c360
Attachment owner 050574696461
Attachment status attached
Owner ID -

c. Similarly, click **eth2** and note the MAC address of the **WAN0** interface.

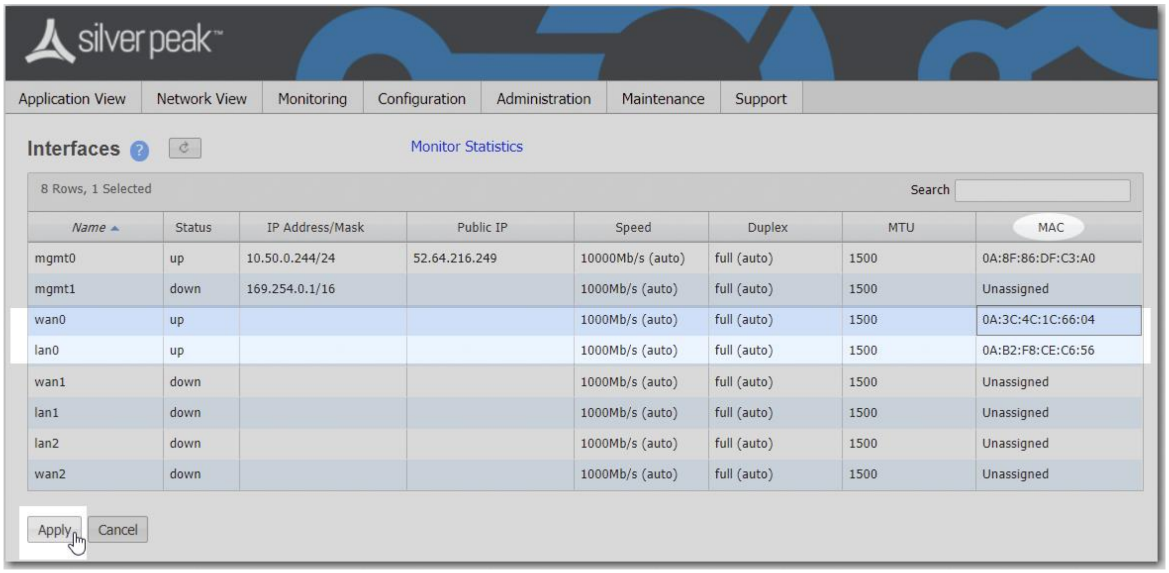
Assign the LAN0 and WAN0 MAC addresses

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



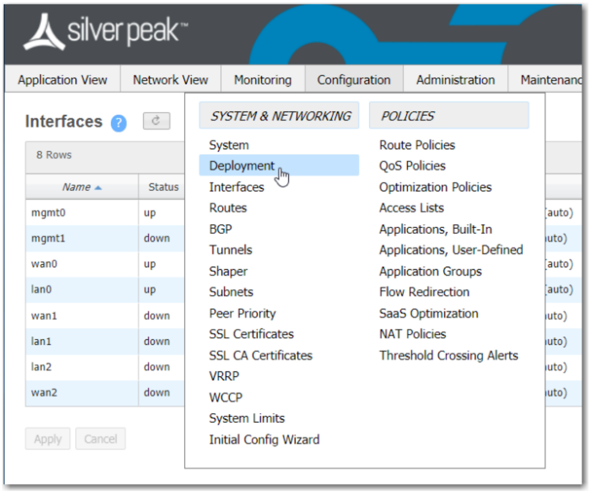
The **Interfaces** page appears.

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



Name	Status	IP Address/Mask	Public IP	Speed	Duplex	MTU	MAC
mgmt0	up	10.50.0.244/24	52.64.216.249	10000Mb/s (auto)	full (auto)	1500	0A:8F:86:DF:C3:A0
mgmt1	down	169.254.0.1/16		1000Mb/s (auto)	full (auto)	1500	Unassigned
wan0	up			1000Mb/s (auto)	full (auto)	1500	0A:3C:4C:1C:66:04
lan0	up			1000Mb/s (auto)	full (auto)	1500	0A:B2:F8:CE:C6:56
wan1	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
lan1	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
lan2	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
wan2	down			1000Mb/s (auto)	full (auto)	1500	Unassigned

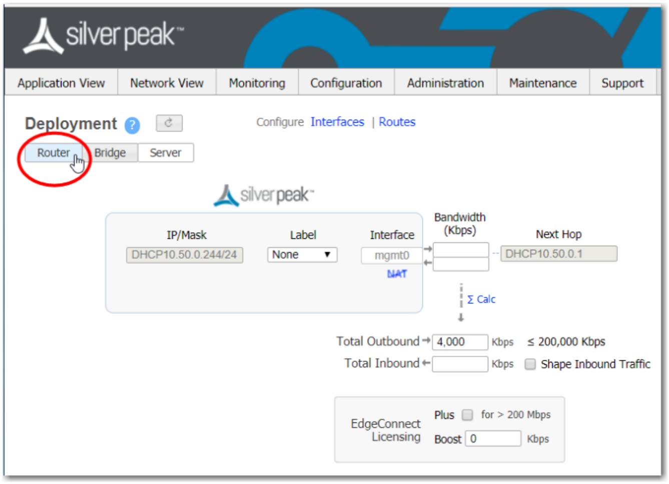
3. Click **Save Changes**, but **DO NOT** click **Reboot Required**.
Instead, select **Configuration > Deployment**.



Name	Status
mgmt0	up
mgmt1	down
wan0	up
lan0	up
wan1	down
lan1	down
lan2	down
wan2	down

Change the Deployment Mode from Server to Router

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



IP/Mask: DHCP10.50.0.244/24 Label: None Interface: mgmt0 Next Hop: DHCP10.50.0.1

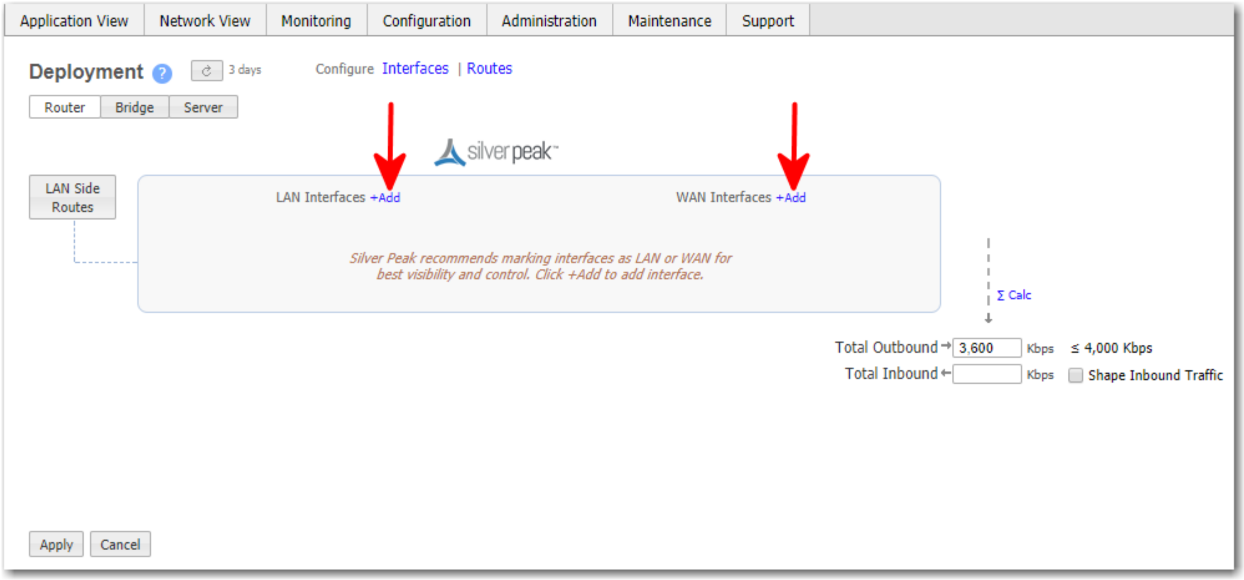
Total Outbound 4,000 Kbps ≤ 200,000 Kbps

Total Inbound Kbps □ Shape Inbound Traffic

Plus □ for > 200 Mbps

Boost 0 Kbps

2. To create a LAN0 interface and the WAN0 interface, click **+Add** for each.



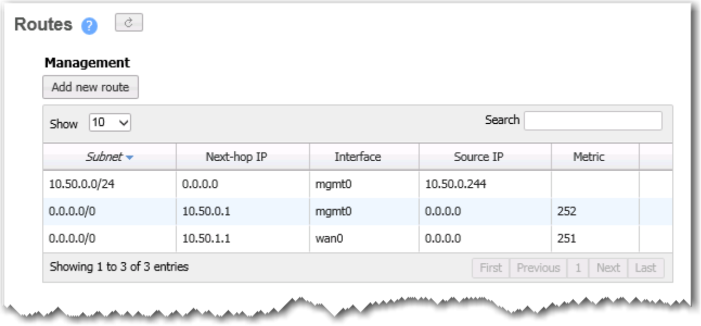
Silver Peak recommends marking interfaces as LAN or WAN for best visibility and control. Click +Add to add interface.

Total Outbound 3,600 Kbps ≤ 4,000 Kbps

Total Inbound Kbps □ Shape Inbound Traffic

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

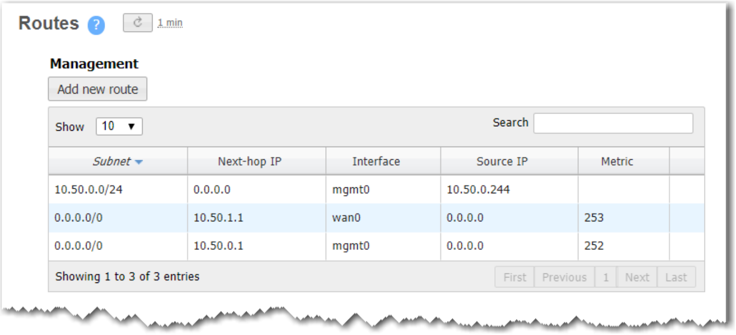
    Important: If you leave WAN0 IP/Mask blank, the EC-V automatically obtains the WAN0 IP address that AWS assigned on the WAN0 ENI. However, this would also change the management default route metric (**Configuration > Routes** page) and make WAN0 the preferred interface for management traffic. As shown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



Subnet	Next-hop IP	Interface	Source IP	Metric
10.50.0.0/24	0.0.0.0	mgmt0	10.50.0.244	
0.0.0.0/0	10.50.0.1	mgmt0	0.0.0.0	252
0.0.0.0/0	10.50.1.1	wan0	0.0.0.0	251

Showing 1 to 3 of 3 entries

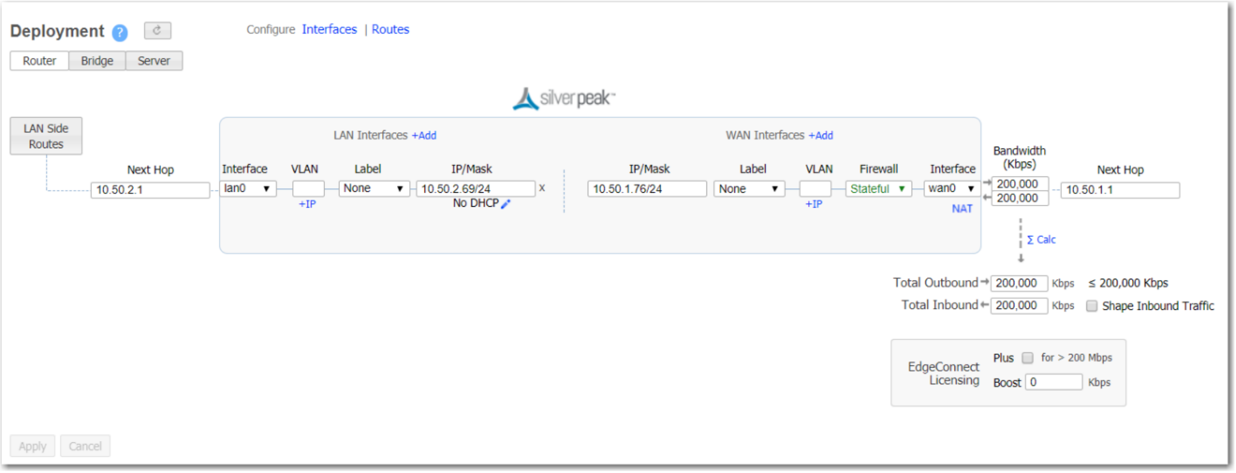
Instead of enabling DHCP client, when you enter a **static IP** on the WAN0 interface, the management interface becomes the preferred interface for management traffic and receives a lower metric than the WAN0 interface, as shown below.



Subnet	Next-hop IP	Interface	Source IP	Metric
10.50.0.0/24	0.0.0.0	mgmt0	10.50.0.244	
0.0.0.0/0	10.50.1.1	wan0	0.0.0.0	253
0.0.0.0/0	10.50.0.1	mgmt0	0.0.0.0	252

Showing 1 to 3 of 3 entries

5. Enter the inbound and outbound **bandwidth** (Kbps) for the WAN0 interface, and click **∑Calc**.
6. Set WAN0 Firewall to **Stateful**.
7. Enable **NAT**. (We'll assign a static Public IP for the WAN0 interface in the next step. After it's assigned, the Orchestrator will use that public IP as the tunnel endpoint when establishing tunnels for the EC-V.)
8. Click **Apply**. You will be prompted to reboot the VM.



Next Hop	Interface	VLAN	Label	IP/Mask
10.50.2.1	lan0		None	10.50.2.69/24 No DHCP

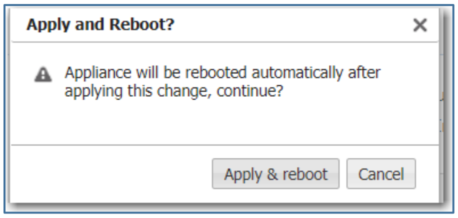
IP/Mask	Label	VLAN	Firewall	Interface	Bandwidth (Kbps)	Next Hop
10.50.1.76/24	None		Stateful	wan0	200,000 200,000	10.50.1.1

Total Outbound 200,000 Kbps ≤ 200,000 Kbps

Total Inbound 200,000 Kbps □ Shape Inbound Traffic

EdgeConnect Licensing: Plus □ for > 200 Mbps; Boost 0 Kbps

9. Click **Apply & reboot**.

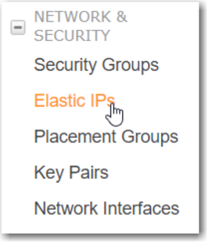


Apply and Reboot?

Appliance will be rebooted automatically after applying this change, continue?

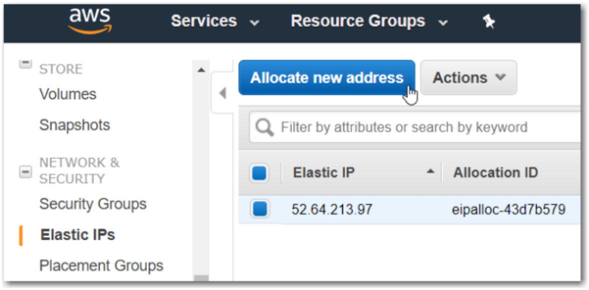
Attach an Elastic IP to the WAN0 interface

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



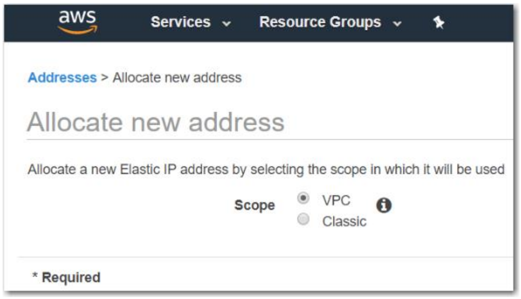
An **Elastic IP address** is a public IPv4 address that is reachable from the Internet. It is possible to assign a dynamic public IP address for WAN0 interface of the EC-V; however, the best practice is to assign an Elastic IP. This ensures that the public IP address persists, even after a reboot or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

2. Click **Allocate new address**.



Elastic IP	Allocation ID
52.64.213.97	eipalloc-43d7b579

3. Select **VPC** and click **Allocate**.



Addresses > Allocate new address

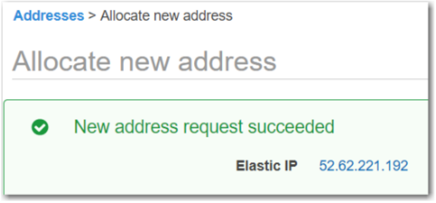
Allocate new address

Allocate a new Elastic IP address by selecting the scope in which it will be used

Scope ● VPC ○ Classic

* Required

4. Click **Close**



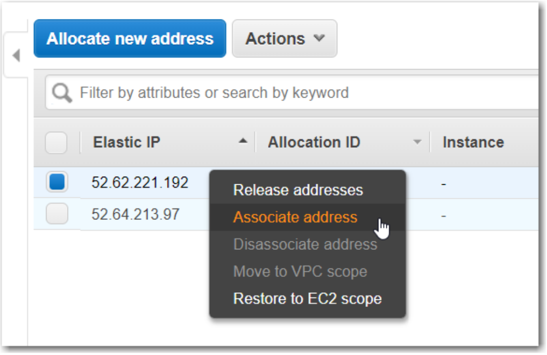
Addresses > Allocate new address

Allocate new address

New address request succeeded

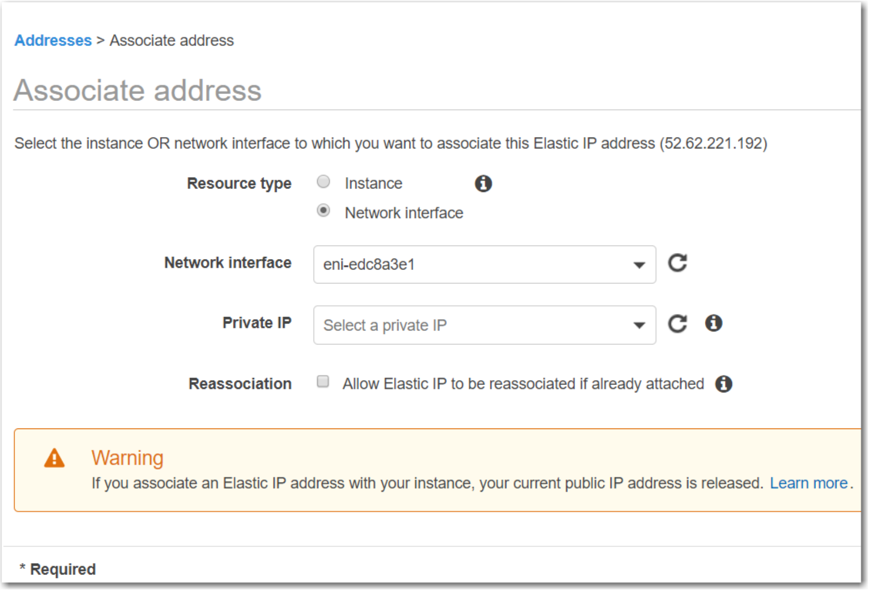
Elastic IP 52.62.221.192

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



	Elastic IP	Allocation ID	Instance
☑	52.62.221.192		-
□	52.64.213.97		-

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



Addresses > Associate address

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (52.62.221.192)

Resource type ○ Instance ● Network interface

Network interface eni-edc8a3e1

Private IP Select a private IP

Reassociation □ Allow Elastic IP to be reassociated if already attached

Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.

* Required

Resource type: Network interface

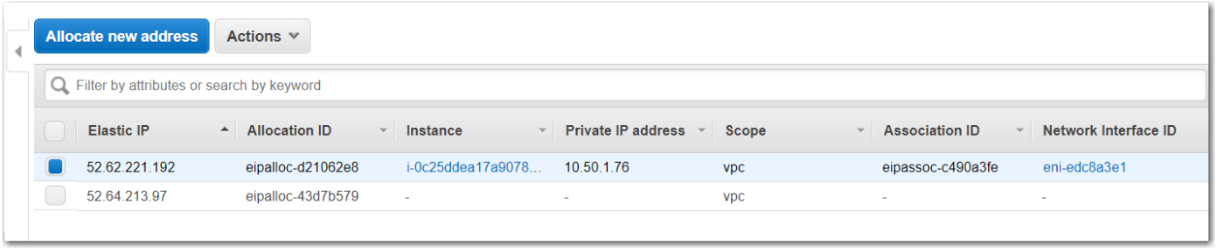
Network interface: [Enter the WAN0 interface ID]

Private IP: [optional]

Reassociation: [optional]

7. Click **Associate**.

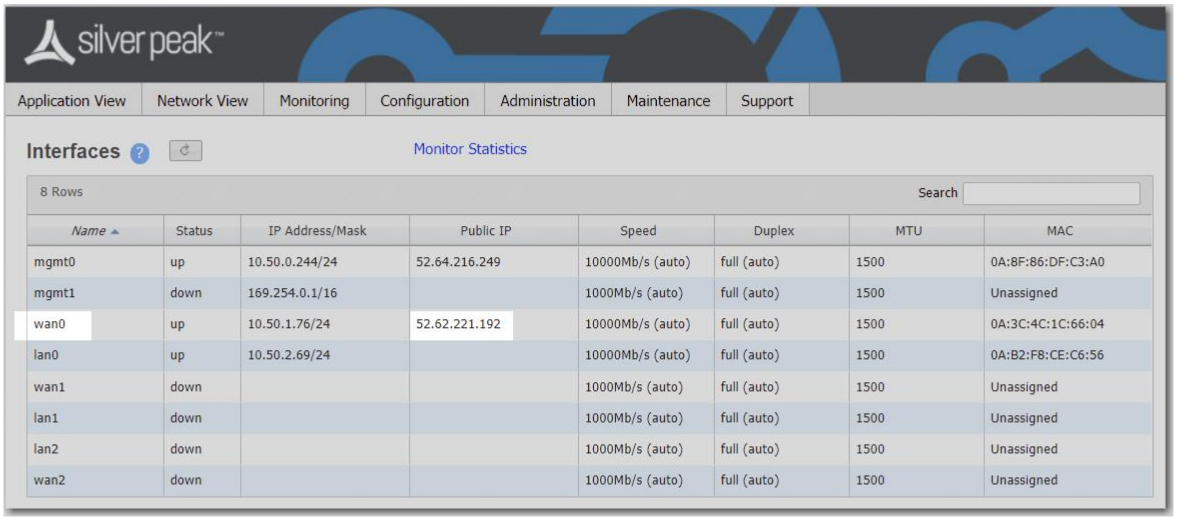
   The public IP is now attached to the WAN0 interface.



	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID	Network Interface ID
■	52.62.221.192	eipalloc-d21062e8	i-0c25ddea17a9078...	10.50.1.76	vpc	eipassoc-c490a3fe	eni-edc8a3e1
□	52.64.213.97	eipalloc-43d7b579	-	-	vpc	-	-

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

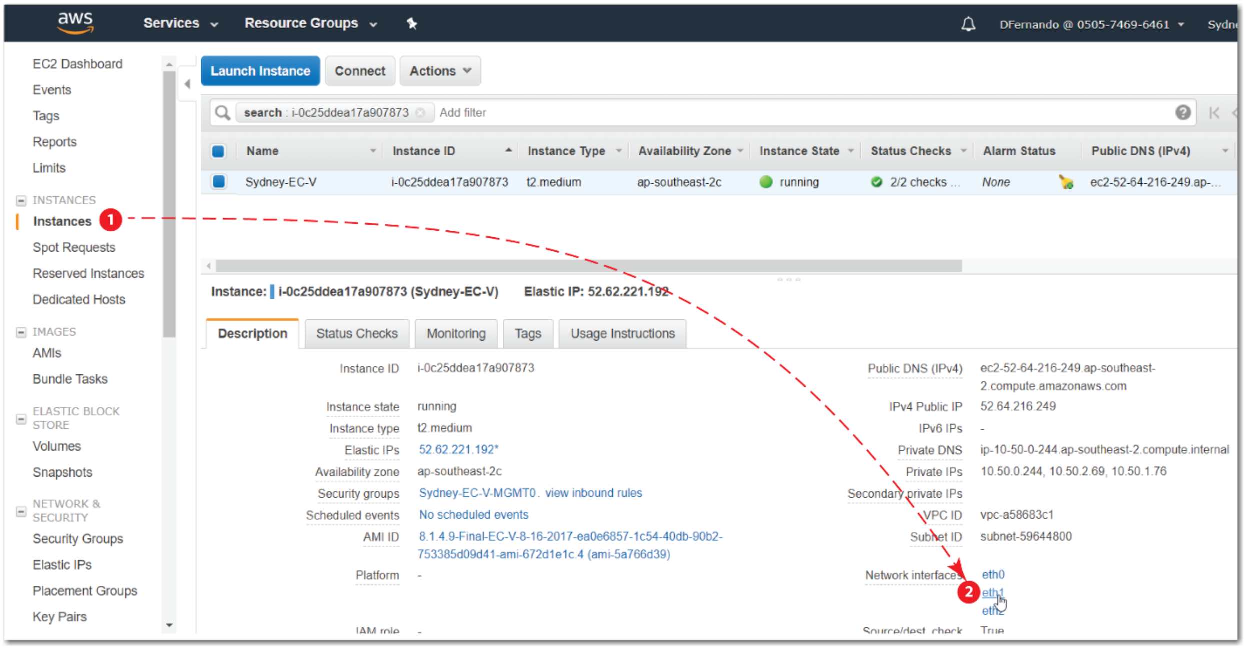
To view the public IP WAN0, go to the EC-V Appliance Manager and select **Configuration > Interfaces**.



Name	Status	IP Address/Mask	Public IP	Speed	Duplex	MTU	MAC
mgmt0	up	10.50.0.244/24	52.64.216.249	10000Mb/s (auto)	full (auto)	1500	0A:8F:86:DF:C3:A0
mgmt1	down	169.254.0.1/16		1000Mb/s (auto)	full (auto)	1500	Unassigned
wan0	up	10.50.1.76/24	52.62.221.192	10000Mb/s (auto)	full (auto)	1500	0A:3C:4C:1C:66:04
lan0	up	10.50.2.69/24		10000Mb/s (auto)	full (auto)	1500	0A:B2:F8:CE:C6:56
wan1	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
lan1	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
lan2	down			1000Mb/s (auto)	full (auto)	1500	Unassigned
wan2	down			1000Mb/s (auto)	full (auto)	1500	Unassigned

Enable IP forwarding on the LAN0 interface

1. Click **Instances**, and select the LAN0 interface (**eth1**, in our example).

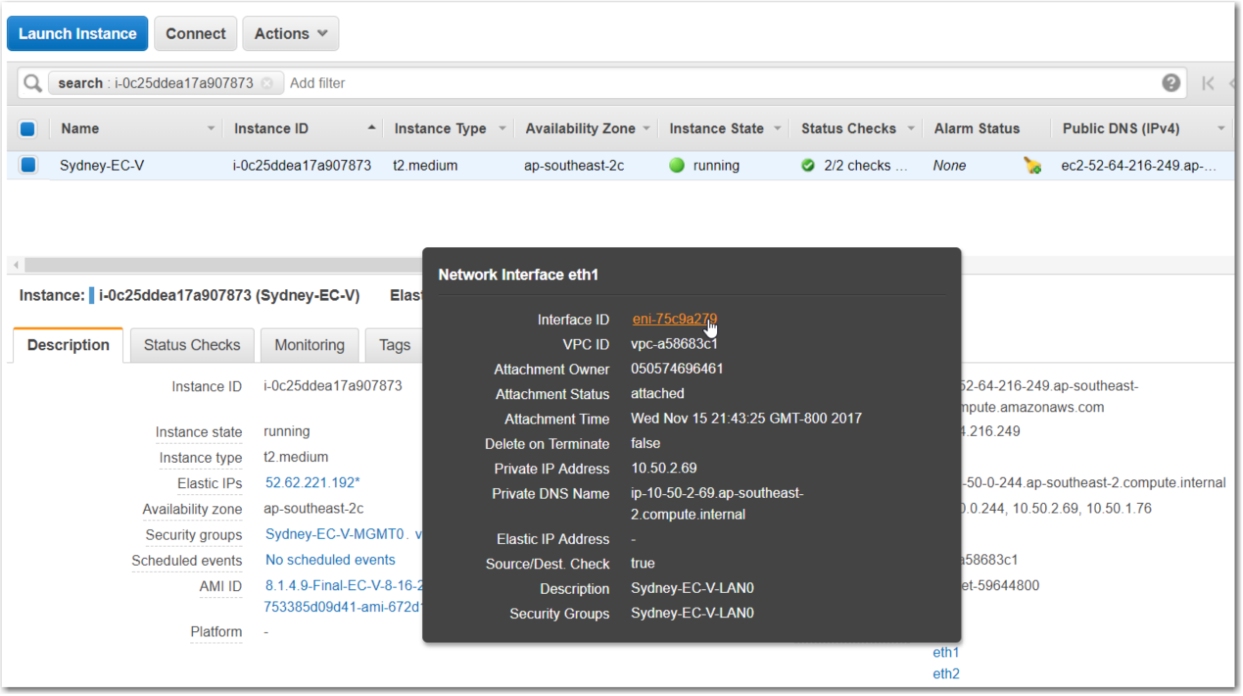


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Sydney-EC-V	i-0c25ddea17a907873	t2.medium	ap-southeast-2c	running	2/2 checks ...	None	ec2-52-64-216-249.ap-...

Instance: i-0c25ddea17a907873 (Sydney-EC-V) Elastic IP: 52.62.221.192

Instance ID	i-0c25ddea17a907873	Public DNS (IPv4)	ec2-52-64-216-249.ap-southeast-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	52.64.216.249
Instance type	t2.medium	IPv6 IPs	-
Elastic IPs	52.62.221.192*	Private DNS	ip-10-50-0-244.ap-southeast-2.compute.internal
Availability zone	ap-southeast-2c	Private IPs	10.50.0.244, 10.50.2.69, 10.50.1.76
Security groups	Sydney-EC-V-MGMT0. view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-a58683c1
AMI ID	8.1.4.9-Final-EC-V-8-16-2017-ea0e6857-1c54-40db-90b2-753385d09d41-ami-672d1e1c.4 (ami-5a766d39)	Subnet ID	subnet-59644800
Platform	-	Network interfaces	eth0 eth1 eth2
IAM role	-	Source/dest. check	True

2. When the **eth1** (LAN0) interface details appear, click the **Interface ID**.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Sydney-EC-V	i-0c25ddea17a907873	t2.medium	ap-southeast-2c	running	2/2 checks ...	None	ec2-52-64-216-249.ap-...

Instance: i-0c25ddea17a907873 (Sydney-EC-V)

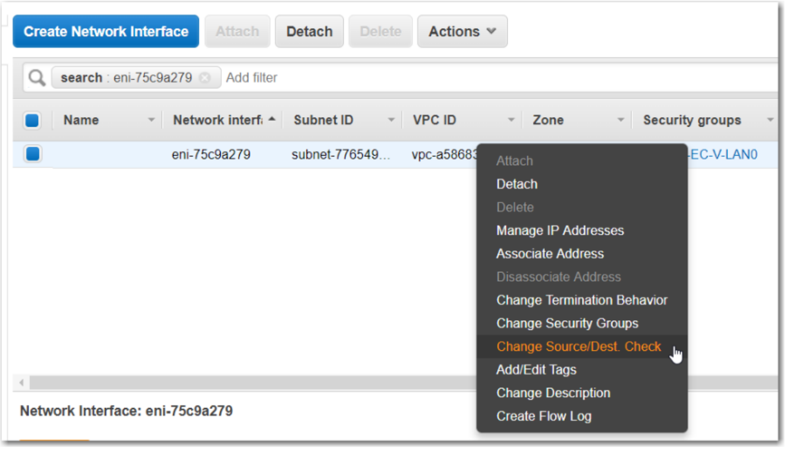
Instance ID	i-0c25ddea17a907873
Instance state	running
Instance type	t2.medium
Elastic IPs	52.62.221.192*
Availability zone	ap-southeast-2c
Security groups	Sydney-EC-V-MGMT0. v
Scheduled events	No scheduled events
AMI ID	8.1.4.9-Final-EC-V-8-16-2 753385d09d41-ami-672d
Platform	-

Network Interface eth1

Interface ID	eni-75c9a279
VPC ID	vpc-a58683c1
Attachment Owner	050574696461
Attachment Status	attached
Attachment Time	Wed Nov 15 21:43:25 GMT-800 2017
Delete on Terminate	false
Private IP Address	10.50.2.69
Private DNS Name	ip-10-50-2-69.ap-southeast-2.compute.internal
Elastic IP Address	-
Source/Dest. Check	true
Description	Sydney-EC-V-LAN0
Security Groups	Sydney-EC-V-LAN0

2-64-216-249.ap-southeast-
npute.amazonaws.com
.216.249
-50-0-244.ap-southeast-2.compute.internal
0.244, 10.50.2.69, 10.50.1.76
58683c1
et-59644800
eth1
eth2

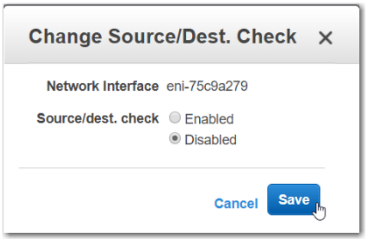
3. On the resulting page, right-click the row and select **Change Source/Dest. Check**.



Name	Network interf	Subnet ID	VPC ID	Zone	Security groups
	eni-75c9a279	subnet-776549...	vpc-a58683		EC-V-LAN0

Network Interface: eni-75c9a279

4. Click **Disabled**, and click **Save**.
   NOTE: It is not necessary to disable **Source/Dest. Check** on the WAN interfaces.


Change Source/Dest. Check

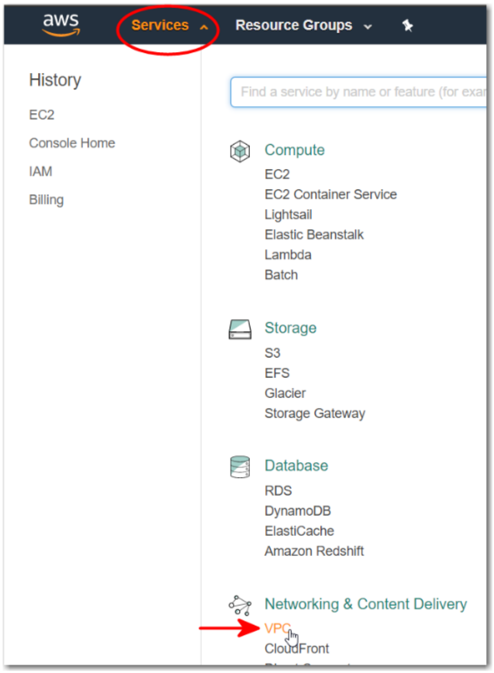
Network Interface eni-75c9a279

Source/dest. check ○ Enabled ● Disabled

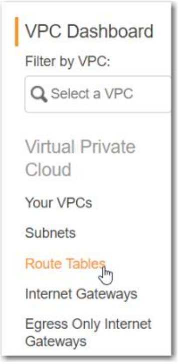
Redirect outbound traffic to EC-V

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

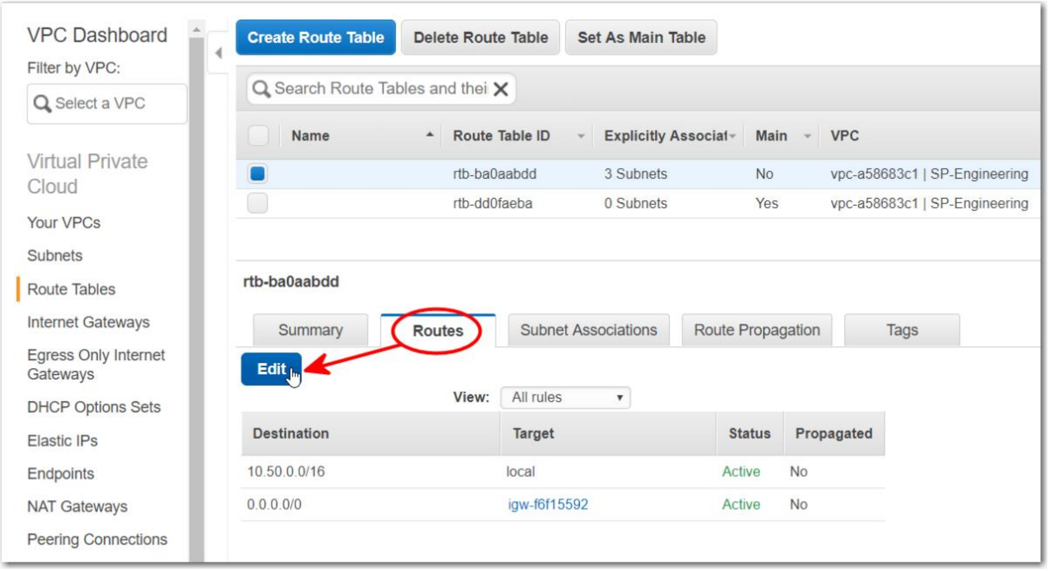
1. Click **Services > VPC**.



2. Under **Virtual Private Cloud**, click **Route Tables**.



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

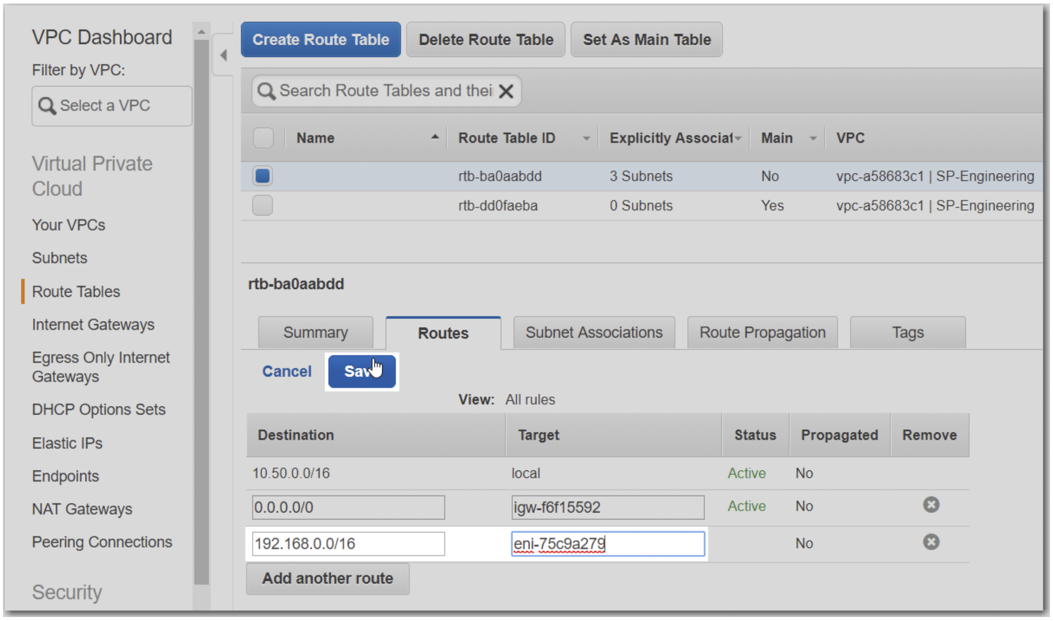


	Name	Route Table ID	Explicitly Associat	Main	VPC
☑		rtb-ba0aabdd	3 Subnets	No	vpc-a58683c1 | SP-Engineering
□		rtb-dd0faeba	0 Subnets	Yes	vpc-a58683c1 | SP-Engineering

rtb-ba0aabdd

Destination	Target	Status	Propagated
10.50.0.0/16	local	Active	No
0.0.0.0/0	igw-f6f15592	Active	No

4. Click **Add another route**, and then enter the **destination subnet**, and the **LAN0 ENI ID** under Target.



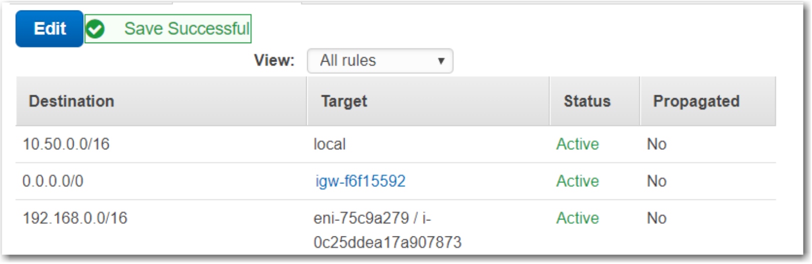
	Name	Route Table ID	Explicitly Associat	Main	VPC
☑		rtb-ba0aabdd	3 Subnets	No	vpc-a58683c1 | SP-Engineering
□		rtb-dd0faeba	0 Subnets	Yes	vpc-a58683c1 | SP-Engineering

rtb-ba0aabdd

Destination	Target	Status	Propagated	Remove
10.50.0.0/16	local	Active	No	
0.0.0.0/0	igw-f6f15592	Active	No	⊗
192.168.0.0/16	eni-75c9a279		No	⊗

Click **Save**. Any outbound traffic destined for the 192.168.0.0/16 network is now sent to the EC-V. This enables the Silver Peak to perform Application Visibility Control, QoS, WAN Optimization, and other operations on this traffic.

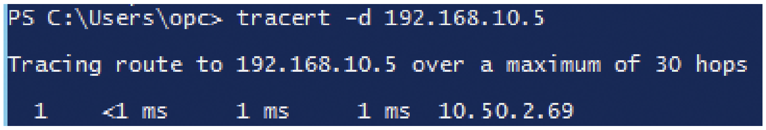
As shown below, the EC-V LAN0 interface (eni-75c9a279) is now the target (next-hop) for any traffic that's destined for the 192.168.0.0/16 network.



Destination	Target	Status	Propagated
10.50.0.0/16	local	Active	No
0.0.0.0/0	igw-f6f15592	Active	No
192.168.0.0/16	eni-75c9a279 / i-0c25ddea17a907873	Active	No

5. To verify that outbound traffic directed to the 192.168.0.0/16 network hits the Silver Peak LAN0 interface first, do one of the following:

   - [Linux] Run **traceroute -n <an IP address in your remote network>**
   - [Windows] Run **tracert -d <an IP address in your remote network>** from a Windows device in your VPC.



```
PS C:\Users\opc> tracert -d 192.168.10.5

Tracing route to 192.168.10.5 over a maximum of 30 hops

  1    <1 ms     1 ms     1 ms  10.50.2.69
```

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

Now that the outbound traffic redirection is set up correctly in VPC, you may create the necessary Business Internet Overlays (BIO) and other traffic policies in the Silver Peak Orchestrator.

For more information about creating BIOs, click here: https://www.silver-peak.com/sites/default/files/UserDocuments/WAN-OP-HTML/content/building_an_overlay.htm?TocPath=Configuration%7CBusiness%20Intent%20Overlays%20(BIO)%7C_____2

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