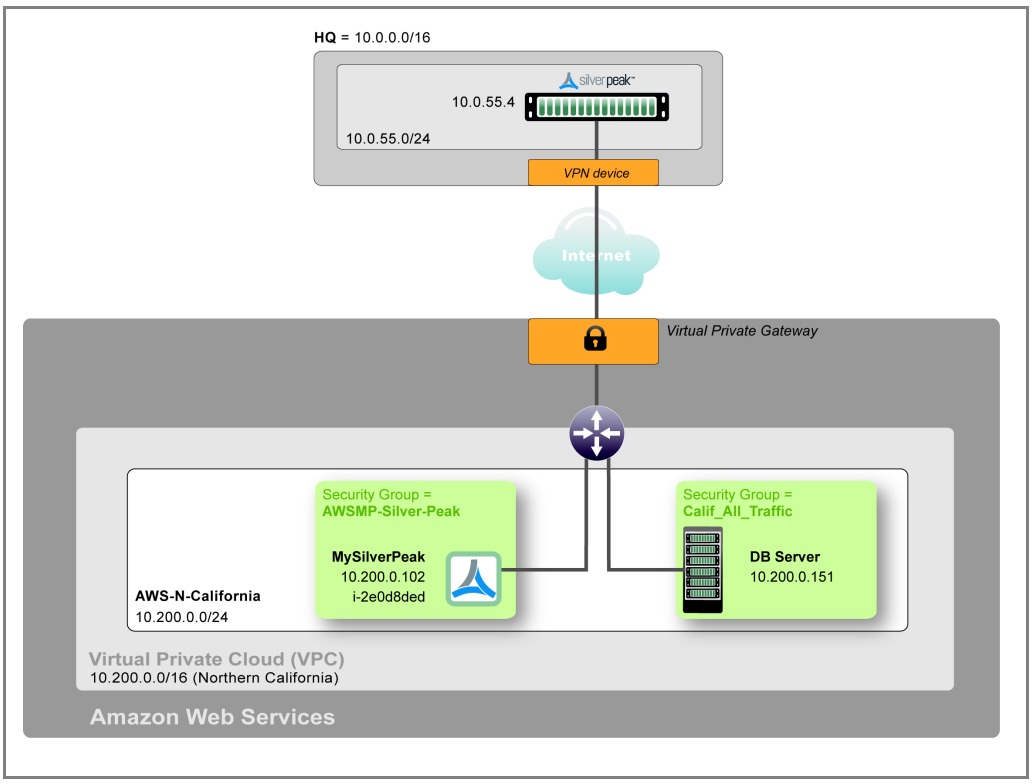
Silver Peak VX for Amazon Web Services

A Silver Peak VX virtual appliance can be deployed within an Amazon Web Services (AWS) cloud environment to accelerate the migration of data to the cloud, and accelerate access to that data from anywhere.

Specifically, the Silver Peak VX is available as an Amazon Machine Image (AMI), created and launched from the Amazon Marketplace.

This guide explains how to deploy a Silver Peak VX AMI in the Virtual Private Cloud (VPC) environment. The steps assume that you've already configured a virtual private network (VPN) between your site (HQ) and the AWS network. Without a VPN, the Silver Peak AMI would require a public IP address.

By following simple steps in the example, you can install a VX virtual appliance and start working with it within minutes of deployment.



Prerequisites

- ☑ **An AWS account**
- ☑ **A virtual private cloud (VPC)**
- ☑ **Security Groups**
  (create new or use existing)
- ☑ **Key Pair**
  (create new or use existing)
- ☑ **Enabled ports:**

80	HTTP
22	SSH
4163	UDP
443	HTTPS

- ☑ **An SSH client, such as PuTTY, installed on your PC**

SUMMARY OF TASKS

1. **Obtain and launch a VX AMI from the AWS Marketplace**
2. **Edit the VX's Security Group to allow inbound application traffic**
3. **Change the Silver Peak password**
4. **Configure the Silver Peak VX Appliance from browser wizard**
5. **Redirect traffic to the Silver Peak VX Appliance for optimization**

Before you begin . . . *review the Silver Peak VX for AWS datasheet*

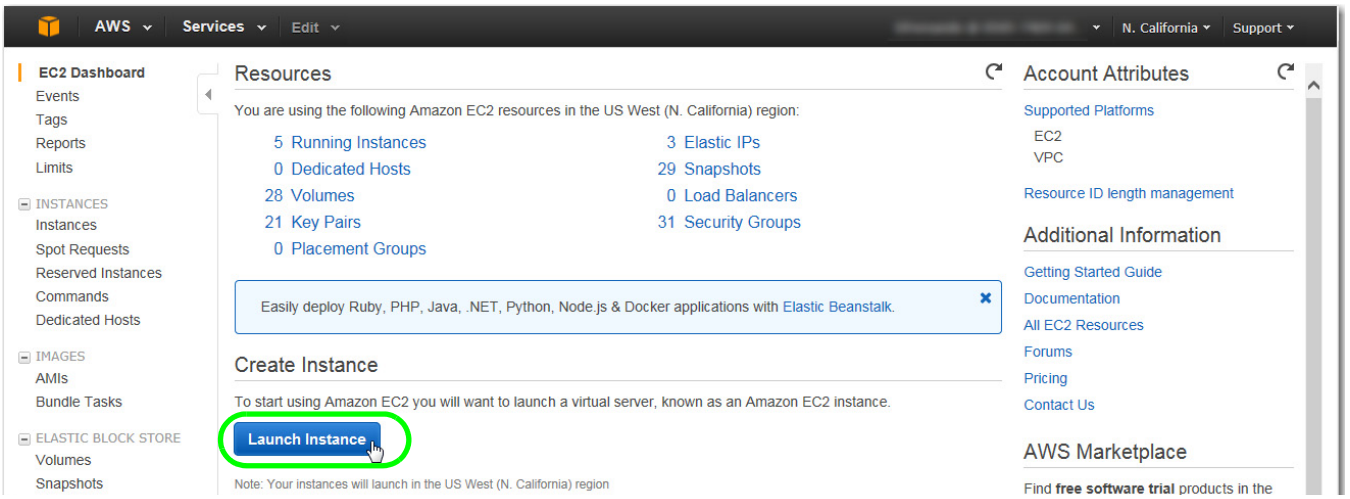
- It describes the resource requirements for each VX AMI and maps them to Amazon instance types.
- It gives an example that compares the hourly license against a subscription-based BYOL (Bring Your Own License).

Obtain and launch a VX AMI from the AWS Marketplace

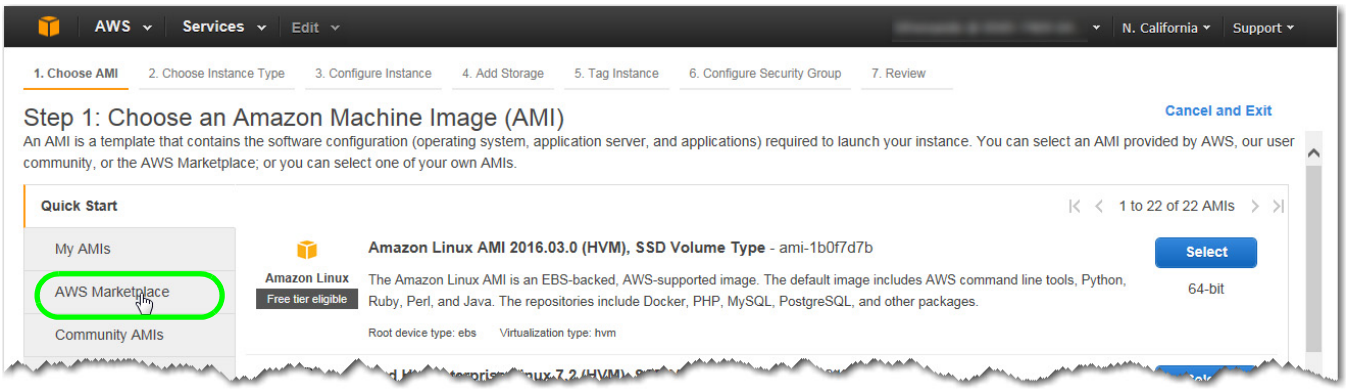
a. After signing in to you AWS account, go to the **Amazon Web Services** page, and select the region in which you want to deploy.

b. Click **EC2**.

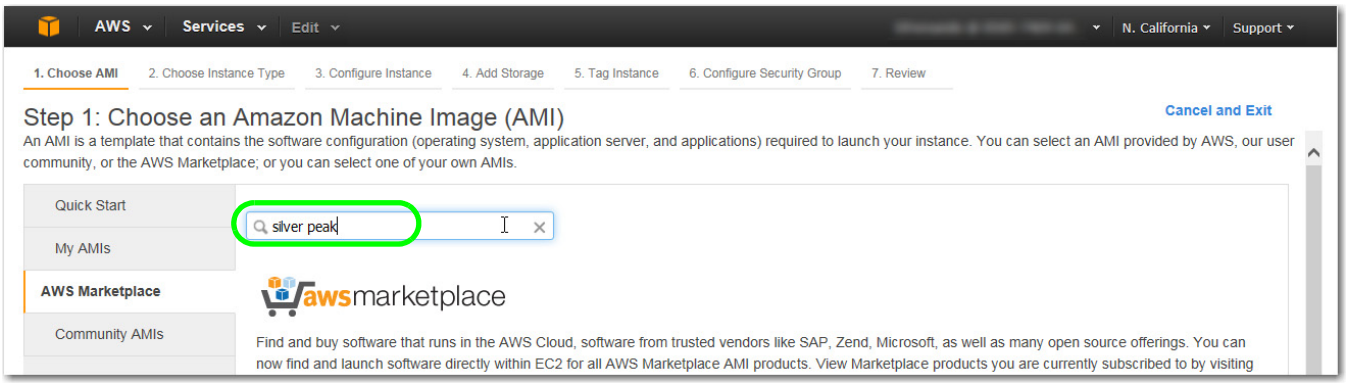
c. When the **EC2 Dashboard** appears, click **Launch Instance**.



When **Step 1** appears, select **AWS Marketplace**.



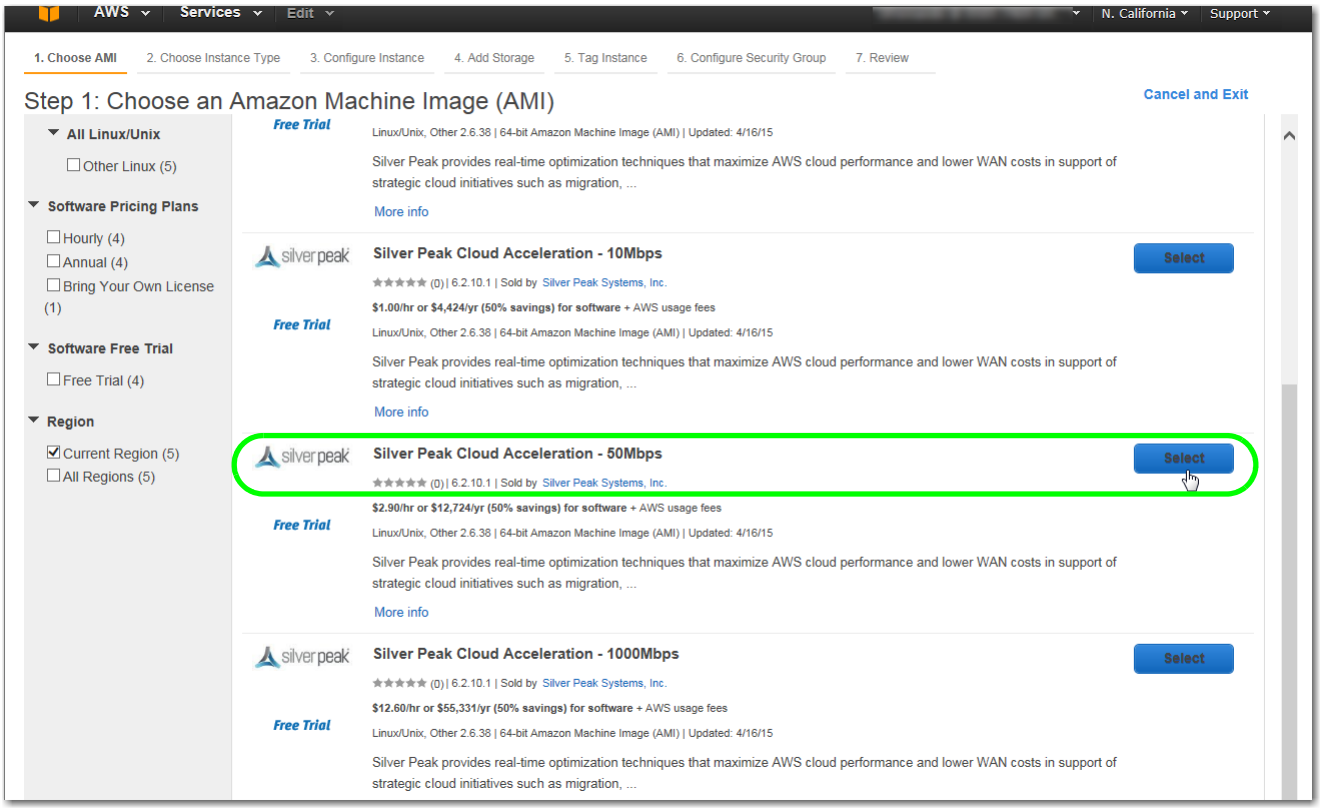
d. In the Amazon Marketplace, search for **`Silver Peak`**.



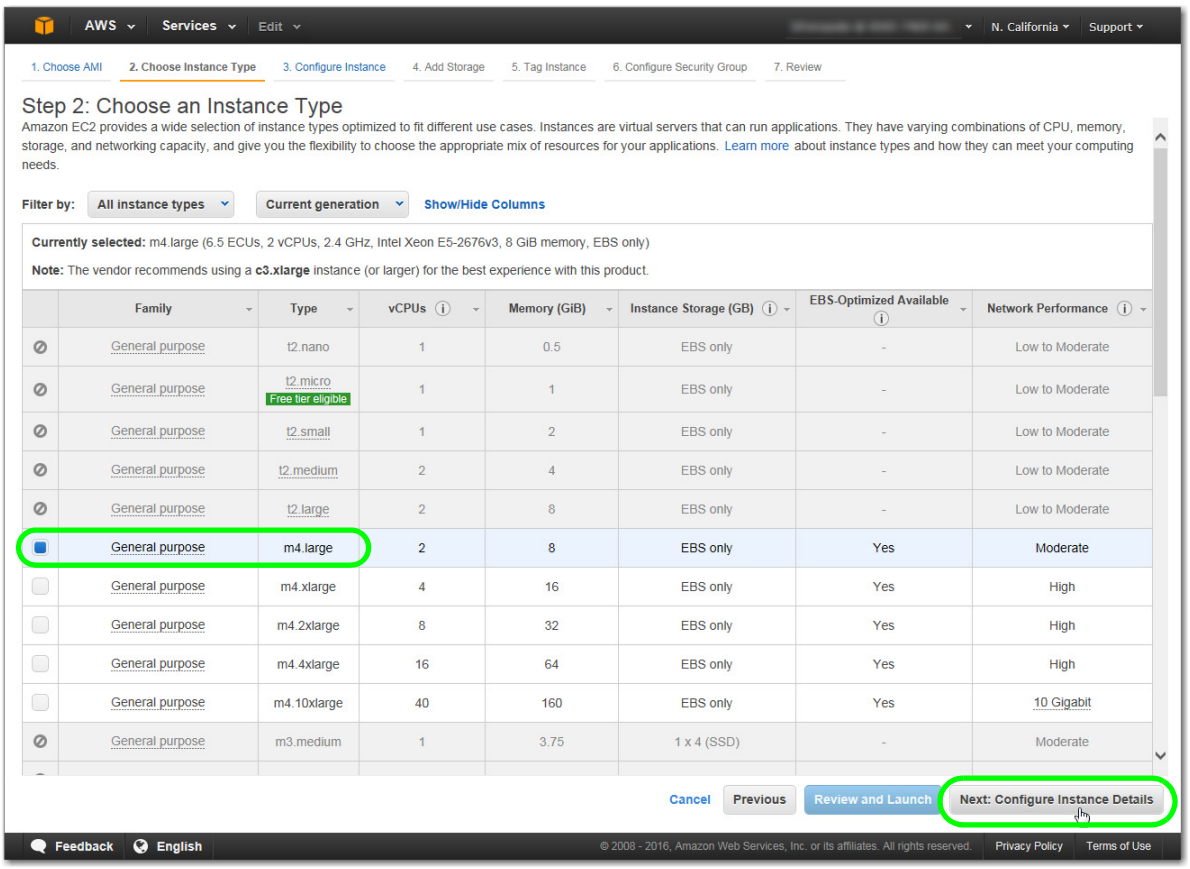
e. When you arrive on the Silver Peak results page, you have a choice of products:

- The BYOL (Bring Your Own License) option requires you to receive a separate license key from Silver Peak before deploying.
- The remaining options are different models of hourly licenses, which already contain an embedded license.

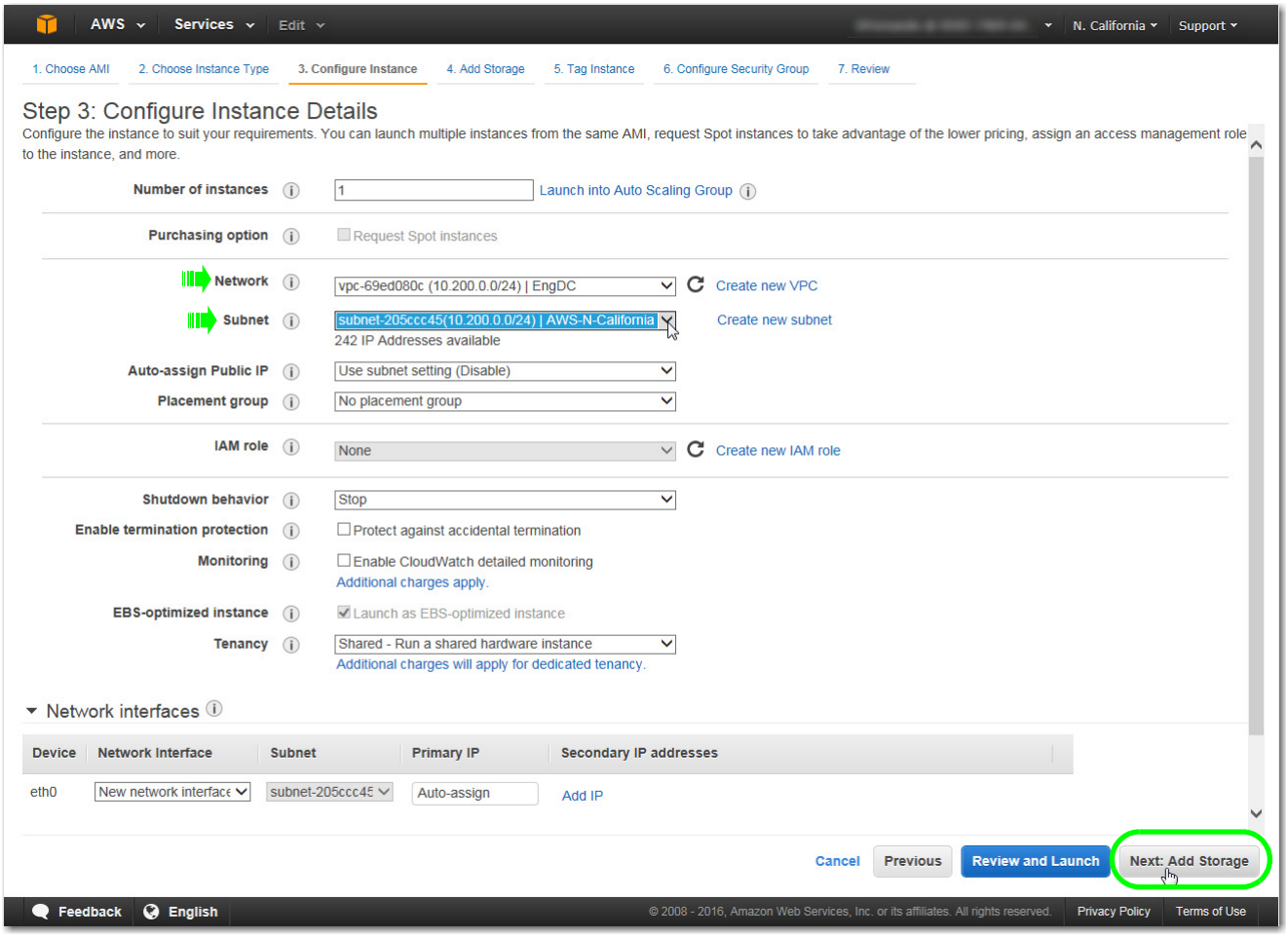
f. In this example, we'll select the option, **Silver Peak Cloud Acceleration – 50 Mbps**. (A license key is embedded in this appliance.).



g. When it asks you to choose an instance type, select one and click **Next: Configure Instance Details**. Here, we'll use **m4.large**.



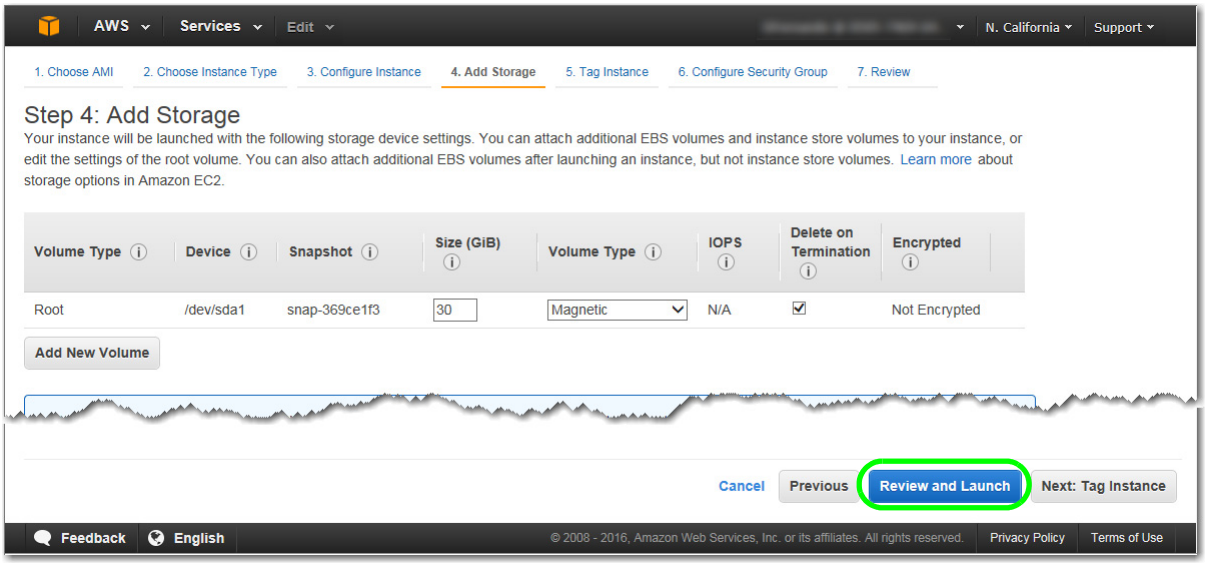
h. Select the **Network** and **Subnet** in which you want to deploy the Silver Peak instance.



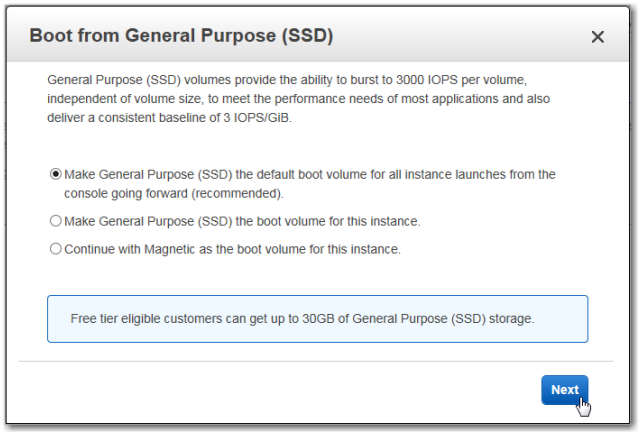
NOTE: If you don't have a VPN connection to Amazon Web Services, then go to **Auto-assign Public IP** and enable an appropriate option. Alternatively, you can assign an **Elastic IP** to your instance after the appliance is running.

Click **Next: Add Storage**.

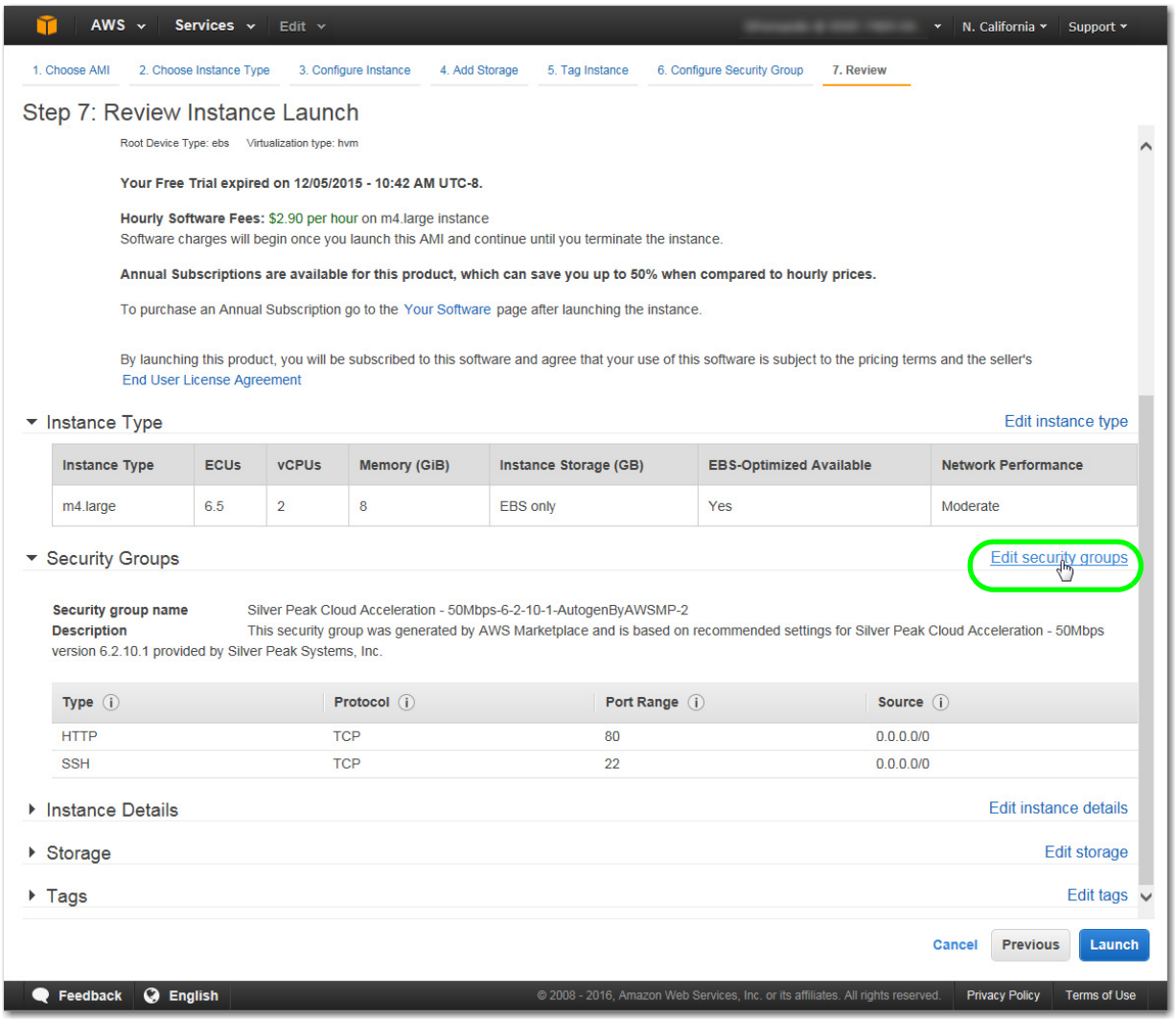
i. After evaluating your storage options, click **Review and Launch**. Here, we accepted the defaults.



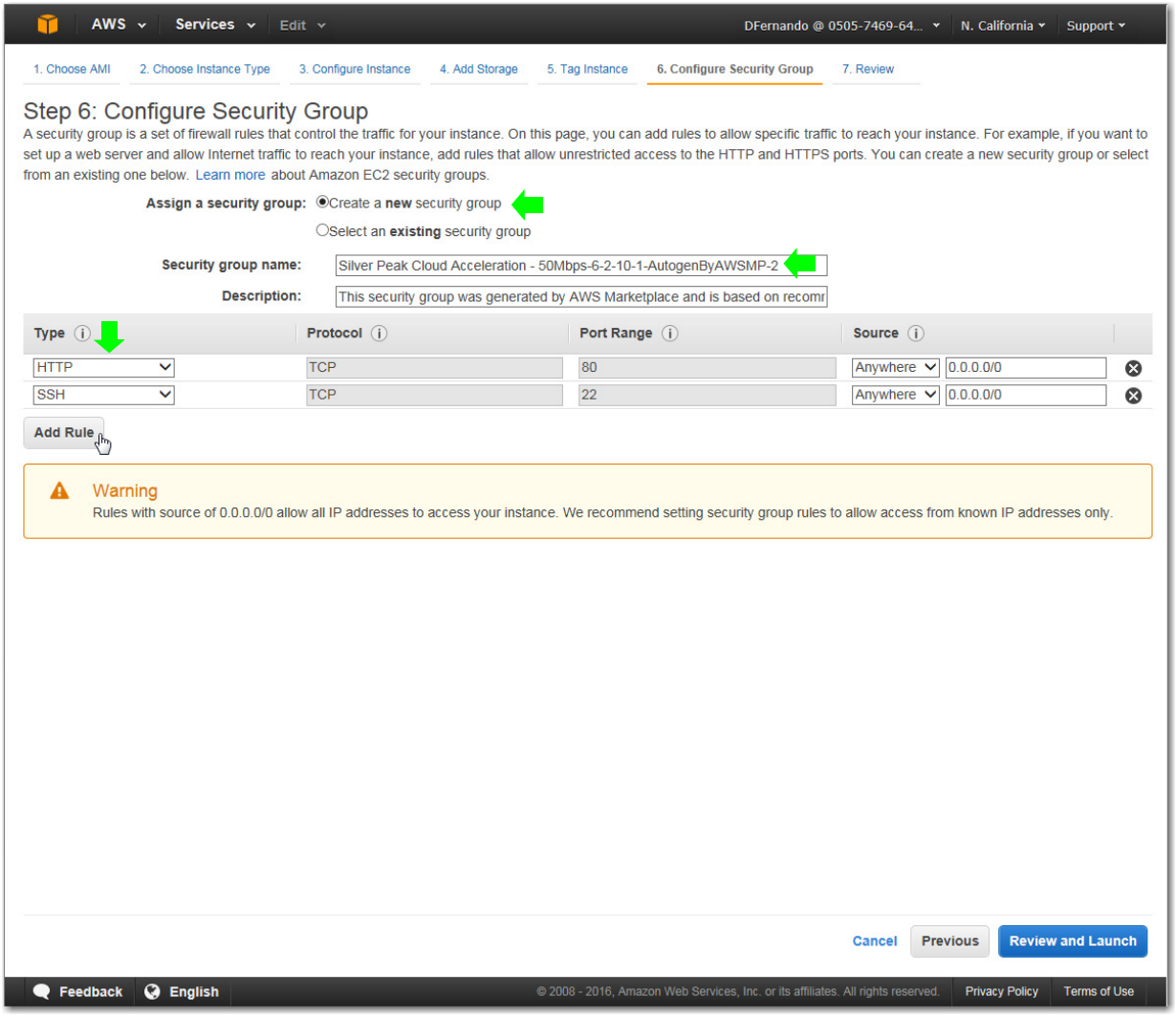
j. When the Boot from General Purpose (SSD) window dialog box appears, accept the recommended option.



k. If you don't have a security group for the appliance you'll be deploying, you'll need to create one. When asked to review the instance launch, scroll down to **Security Groups** and click **Edit security groups**.



l. When the security group configuration page appears, you'll observe a new group with a default, auto-generated name, containing rules for HTTP and SSH.



You'll need to add rules for HTTPS and UDP.

m. Click **Add Rule**, and complete the following:

Type: [Select] `HTTPS`

Source: [Enter the address(es) to your network]

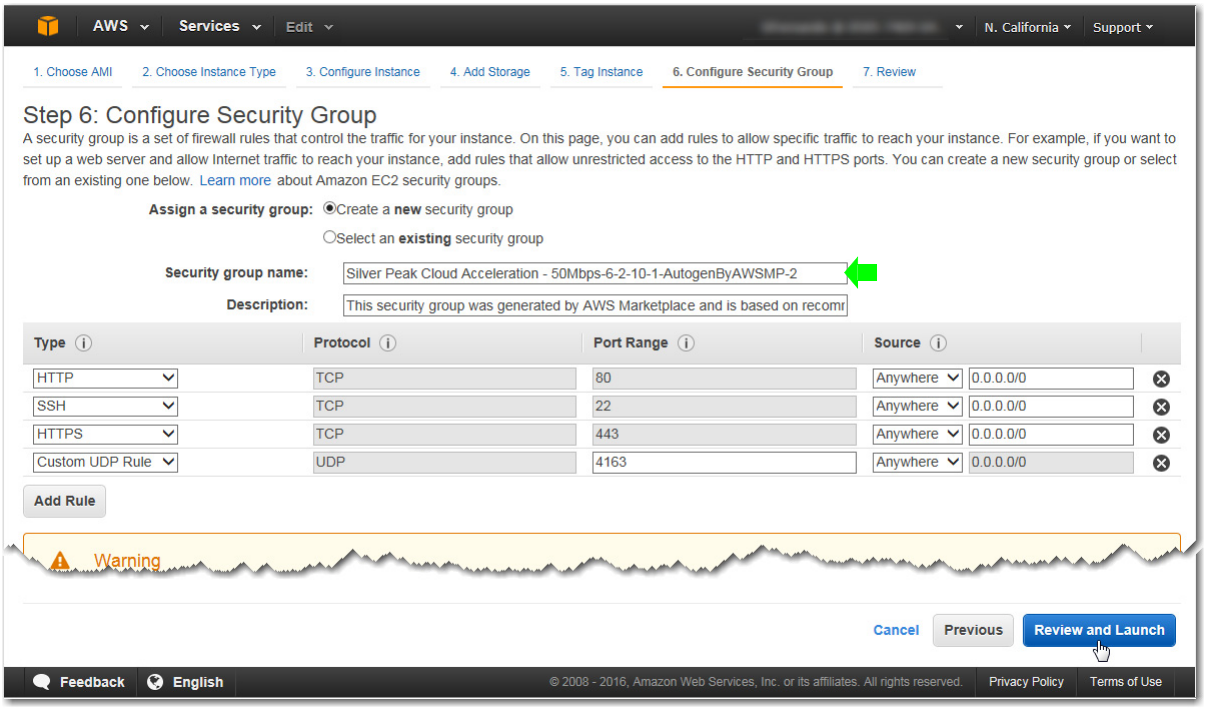
n. Click **Add Rule**, and complete the following:

Type: [Select] `Custom UDP Rule`

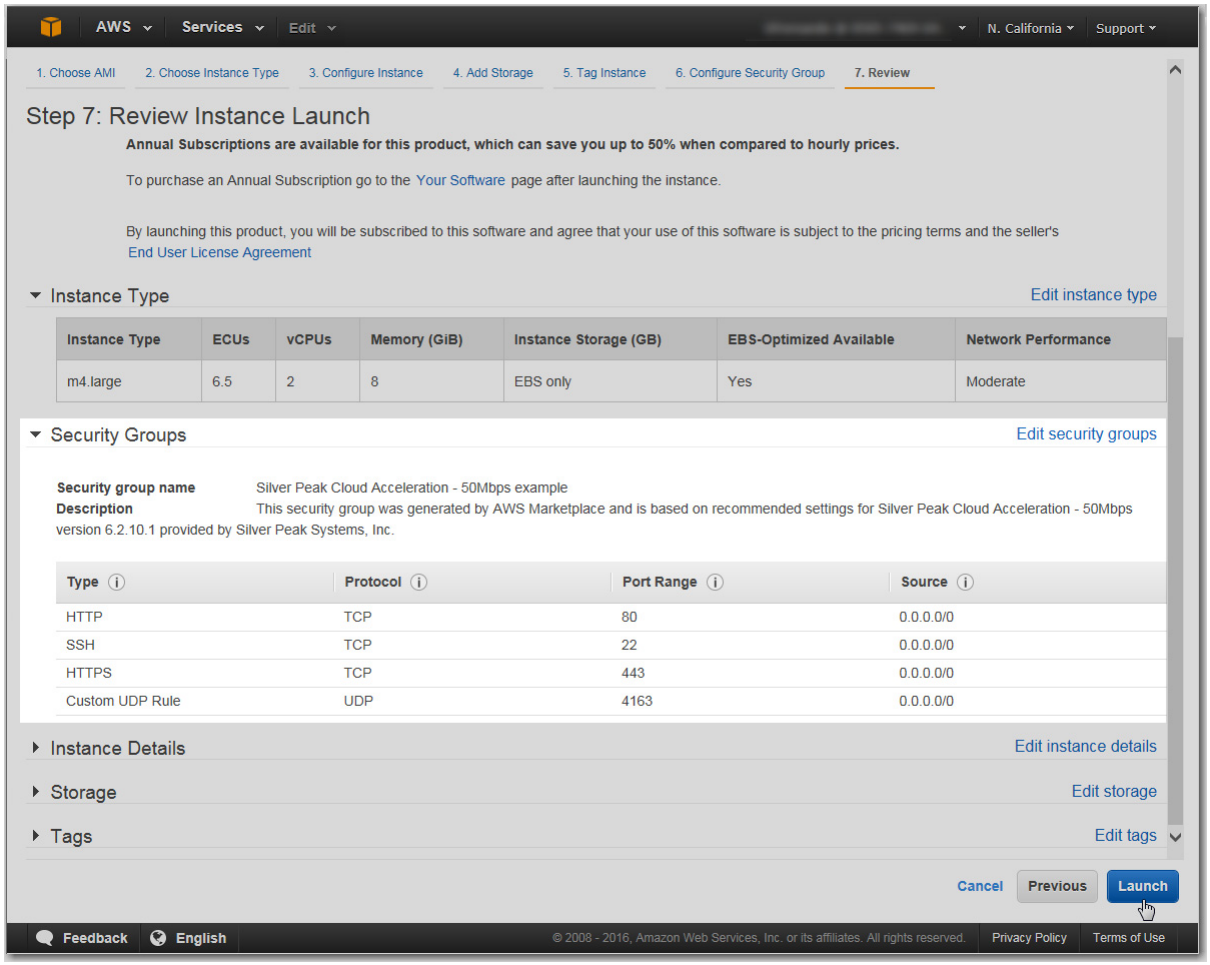
Port Range: `4163`

Source: [Enter the address(es) to your network]

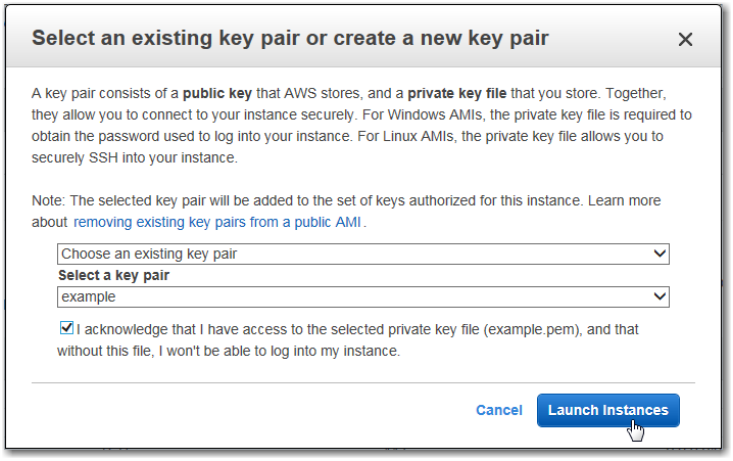
o. After renaming the security group (optional), click **Review and Launch**.



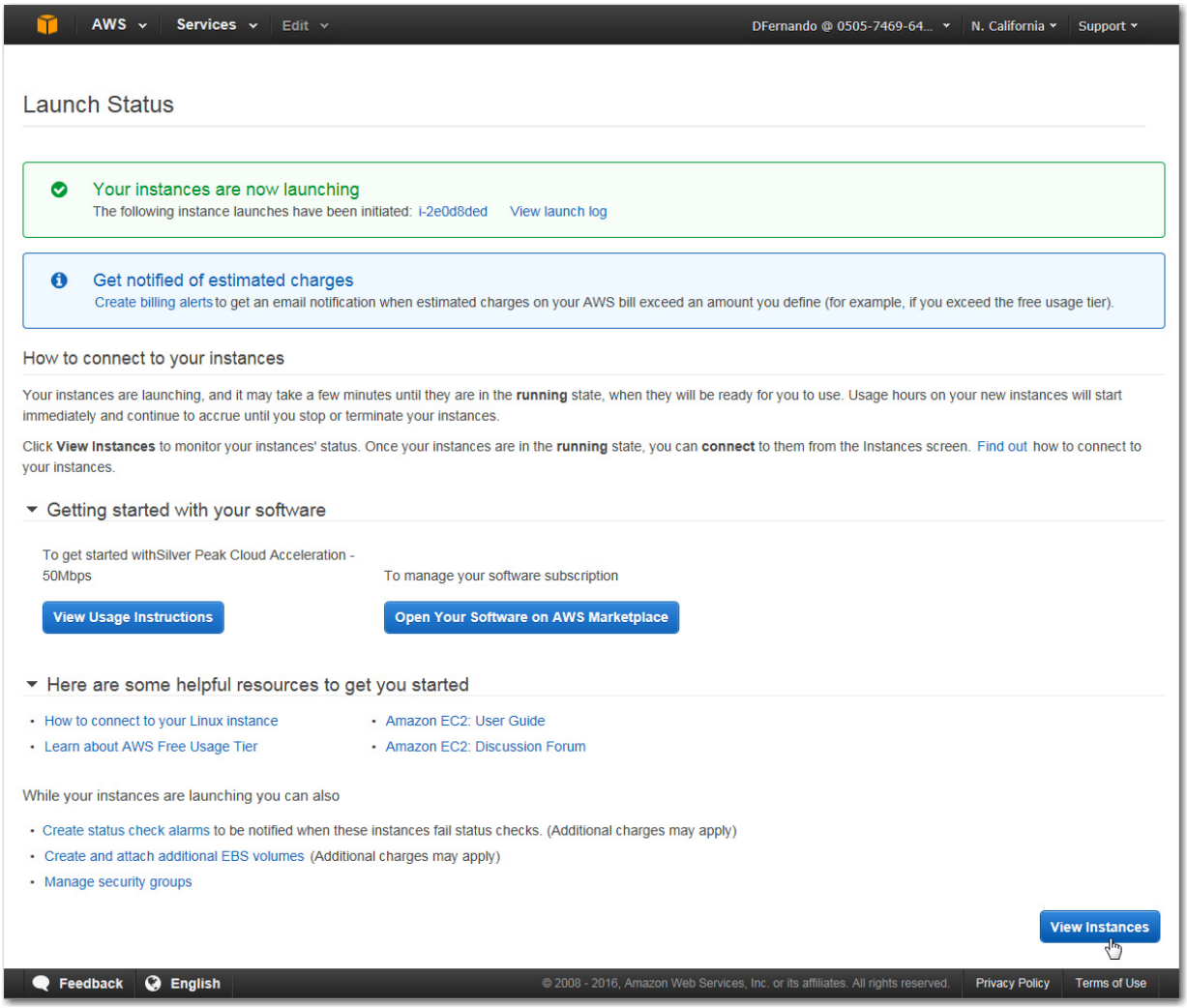
p. When the review page appears, scroll down to **Security Groups**, verify the data, and click **Launch**.



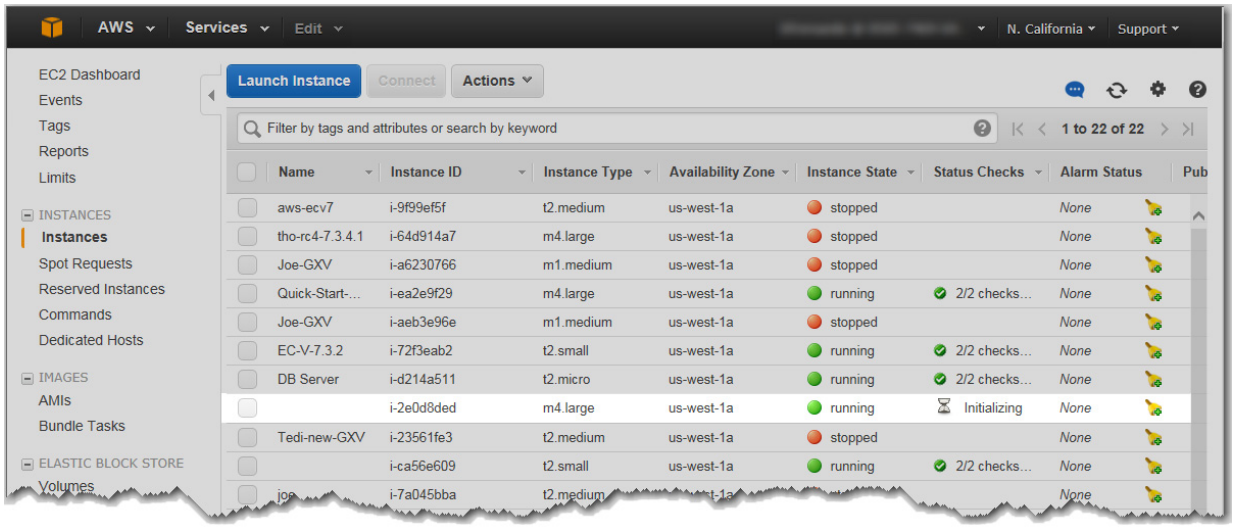
When the pop-up window appears, asking you to create or select a key pair, make the choice that fits your circumstances and click **Launch Instances**.



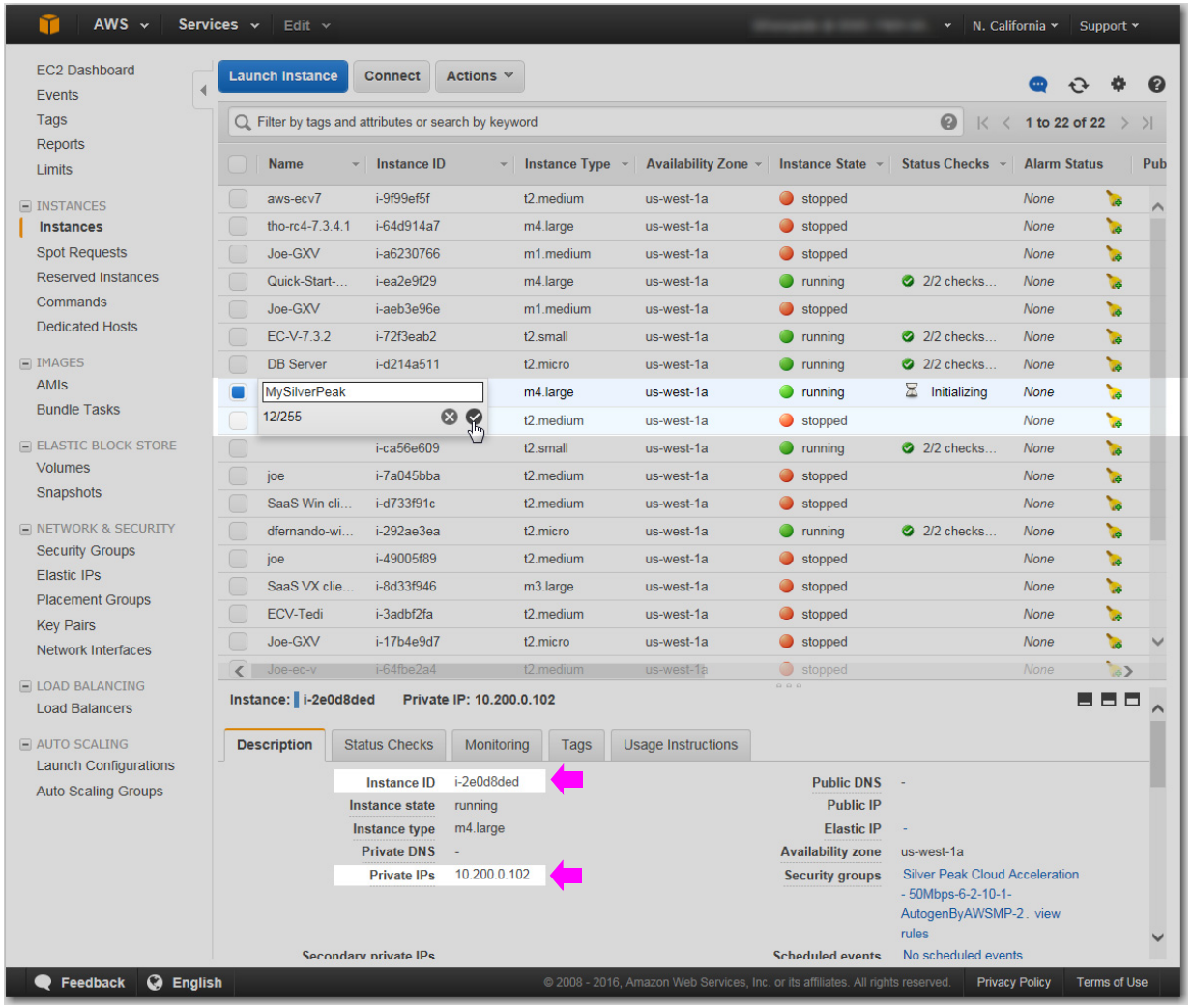
q. After the **Launch Status** window appears, select **View Instances**.



r. An instance table appears. The instance you just launched is initializing and appears with the **Name** field blank.

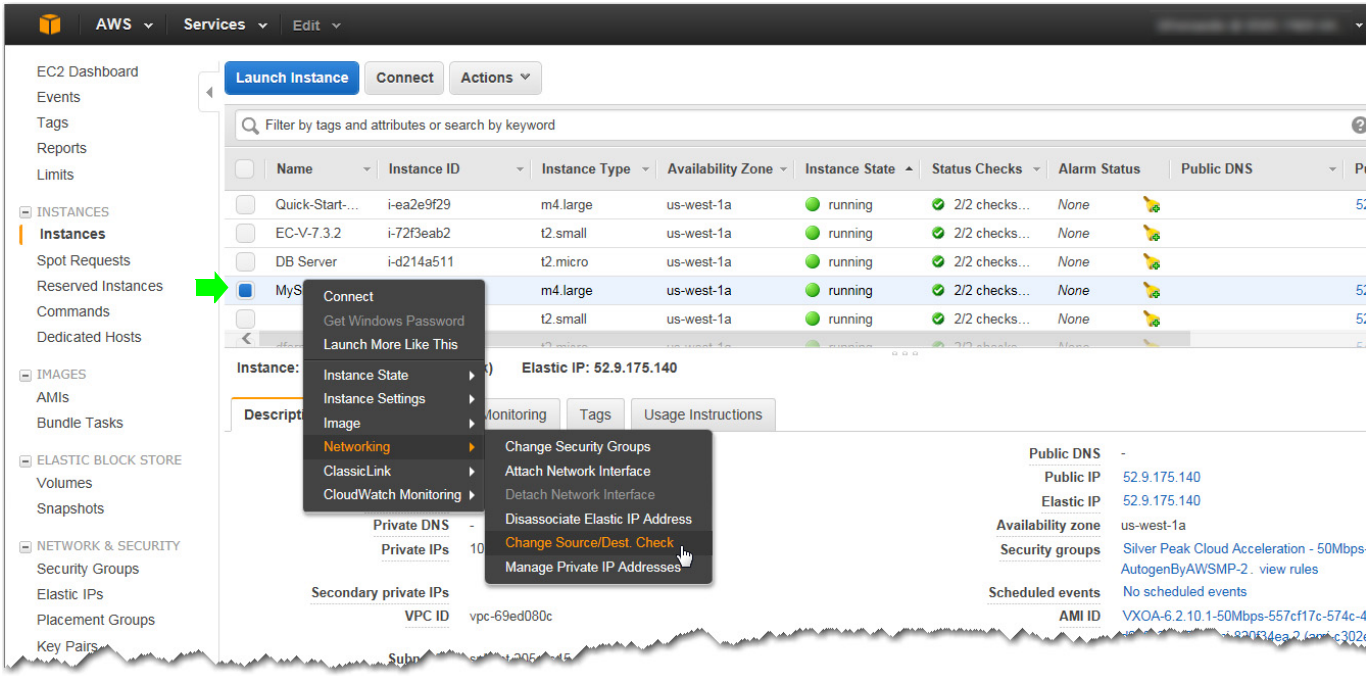


s. Select the instance, assign a name, and click the checkmark to apply it.



Jot down the **Private IP** address. You'll need it later to access Appliance Manager and also to create a UDP tunnel to **HQ**. Later, you'll also need the **Instance ID** to set up traffic redirection in the route table.

t. To enable the VX to forward redirected traffic, you must disable the VX AMI's **Source / Dest Check**.



☑ To do this, right-click over the VX instance in the EC2 Console's **Instances** page.

☑ From the drop-down list, select **Change Source / Dest Check**.

☑ When prompted, click **Yes, Disable**.

If you don't do this, then MySilverPeak drops de-tunneled datapath packets because the reconstituted packets reference the destination IP address of the remote host, as opposed to MySilverPeak's IP address.

u.

2 Edit the VX's Security Group to allow inbound application traffic

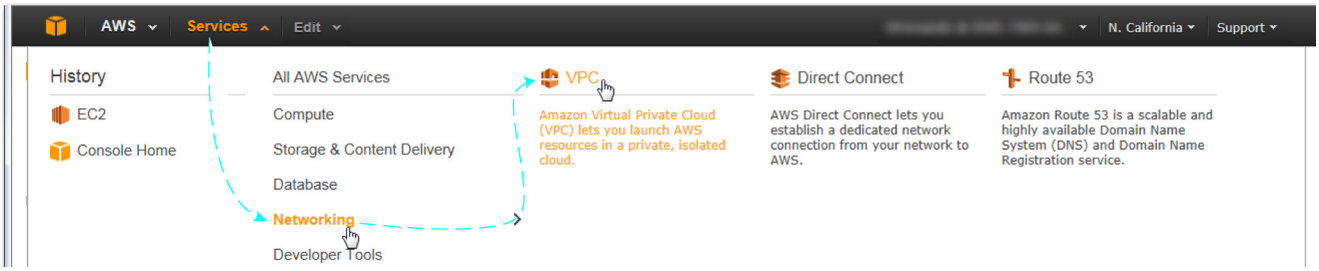
For the VX to optimize traffic, you must add rule(s) to the VX's Security Group that:

- allow application traffic to and from the VX.
- open ports to allow application traffic your AWS application's security group.

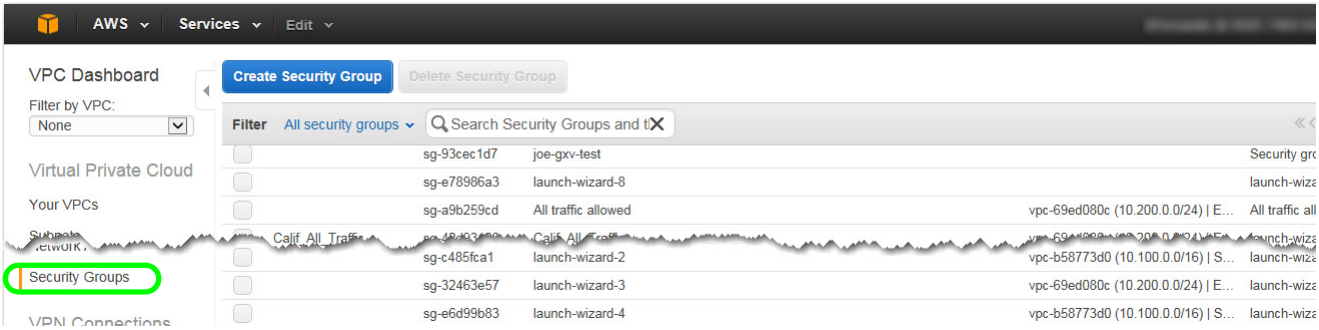
Here, we'll configure **MySilverPeak**'s Security Group to open for application traffic from **DB Server**'s Security Group.

a. First, access **Security Groups**:

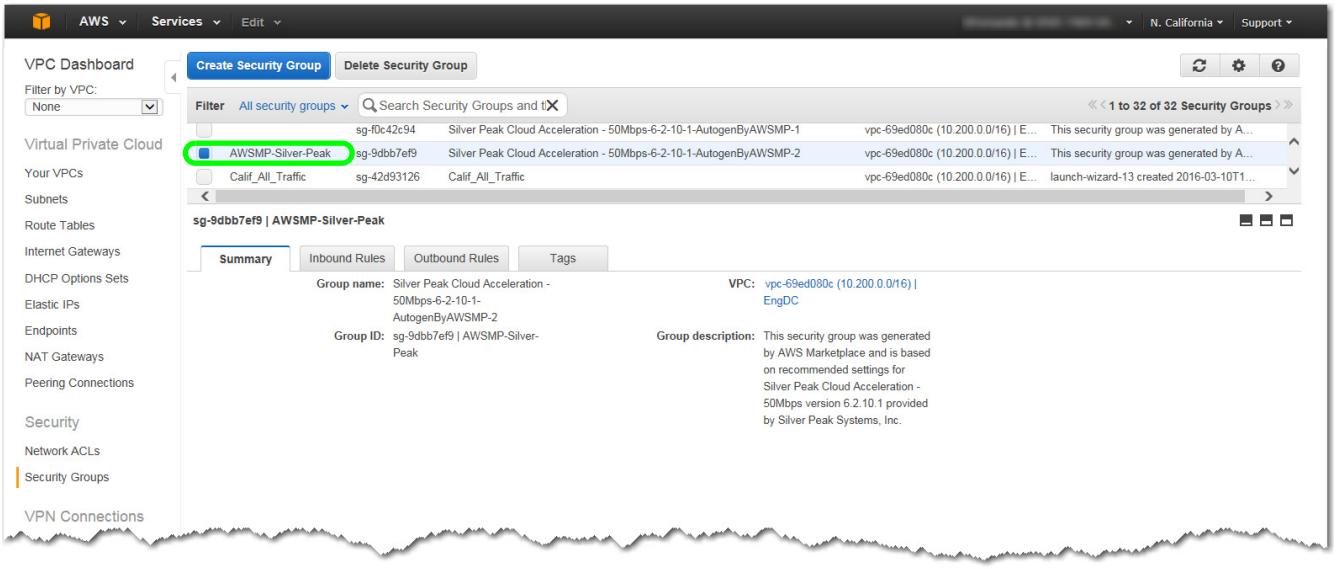
☑ Point to the **Services** menu, pass over Networking, and click **VPC**.



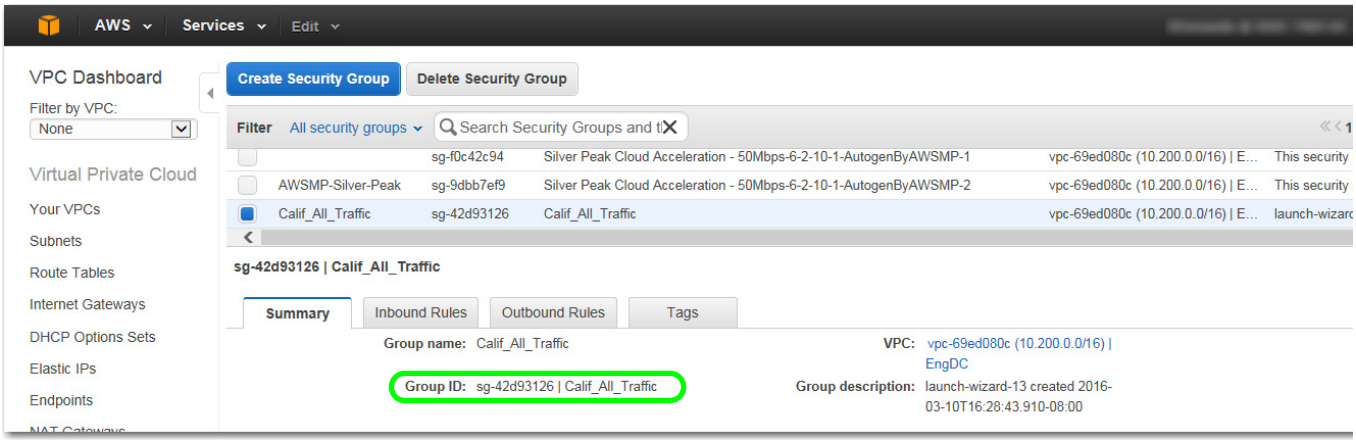
☑ On the left side of the resulting page, click **Security Groups**.



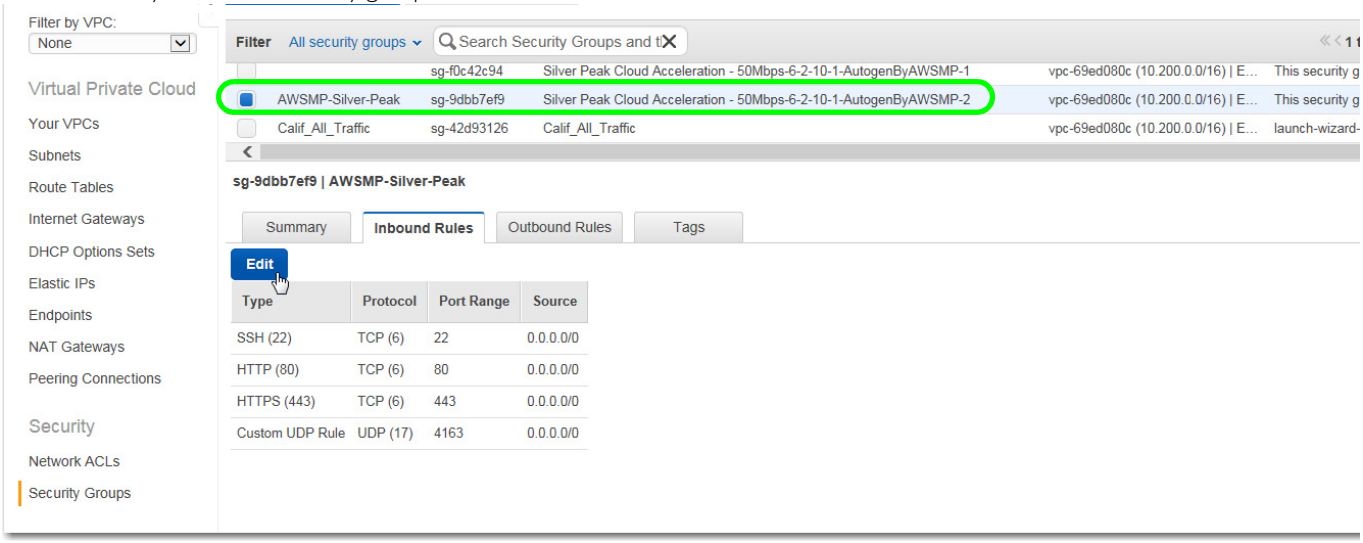
b. [*Optional*] To make identification easier, you can sort to find **MySilverPeak's** Security Group, and give it a recognizable name. Here, we entered **`AWSMP-Silver-Peak`** in the blank first column.



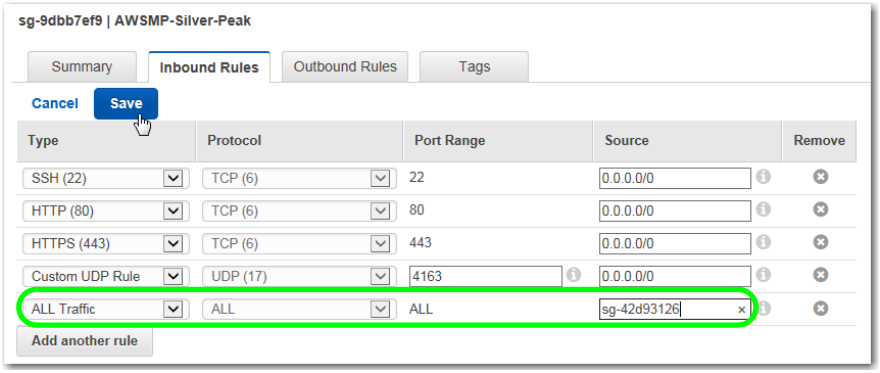
c. Select **DB Server's** security group, **Calif_All_Traffic**, and view the **Details** tab to see the **Group ID**.



d. Now select MySilverPeak's security group, **`AWSMP-Silver-Peak`**, select the **Inbound Rules** tab, and click **Edit**.



Make the following entries:



☑ In the **Type** field, select **ALL Traffic** from the list.

☑ In the **Protocol** field, select **ALL**.

☑ In the **Source** field, enter **Calif_All_Traffic**'s Group ID, **`sg-42d93126`**.

☑ Click **Save**.

NOTE: For all WAN traffic that you intend to optimize, you must add the application server's security group ID to the VX's security group. This is true even if your application server's security group has the same name as the VX's security group.

TIP: If you want to set up a second network path to the appliance, you can attach an associated elastic IP address to the VX AMI, so that the appliance is reachable through an alternative path.

3 Change the Silver Peak password

In this example, we'll use PuTTY to change the Silver Peak VX's password.

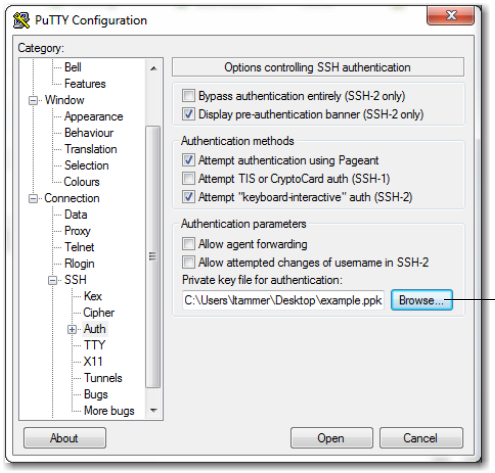
There are three password-related steps to consider in order to successfully use a key-pair with a VX:

a. If you created a new key pair for the VX, make sure to protect your VX private key file so that only you can read it.

For example, on Linux and OS X, use `chmod 400 <private-key-name>.pem` to change key file permissions.
In this example, the command is `chmod 400 example.pem`.

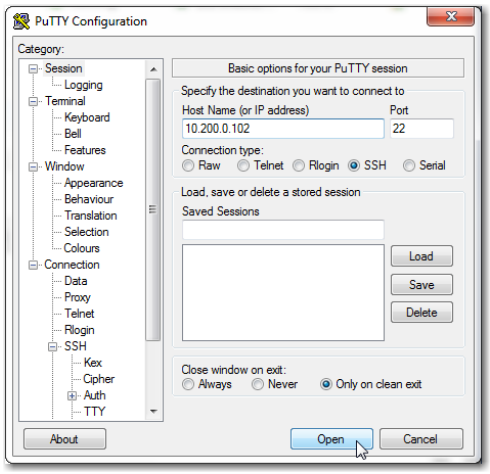
If you don't do this, AWS will ignore your private key and ask you for a password. However, providing a password will not work.

b. Before accessing Appliance Manager, open PuTTY and in the Category window, navigate to **Connection > SSH > Auth**, click **Browse**, and select the appropriate **.ppk** file.



Verify that the file type you select is **.ppk**.

c. Then, in the Category window, scroll upwards and click **Session**.



☑ In the **Host Name (or IP address)** field, enter MySilverPeak's **Private IP** (jotted down in an earlier step): `10.200.0.102`

☑ For **Connection type**, select **SSH**.

☑ Click **Open**.

d. Create secure passwords for the VX admin and/or monitor users. To do this, enter the following commands:

[vx-appliance] > `enable` [ENTER]

[vx-appliance] # `configure terminal` [ENTER]

[vx-appliance] (config) # `username admin password <new-password>` [ENTER]

and/or

[vx-appliance] (config) # `username monitor password <new-password>` [ENTER]

e. Exit the session.

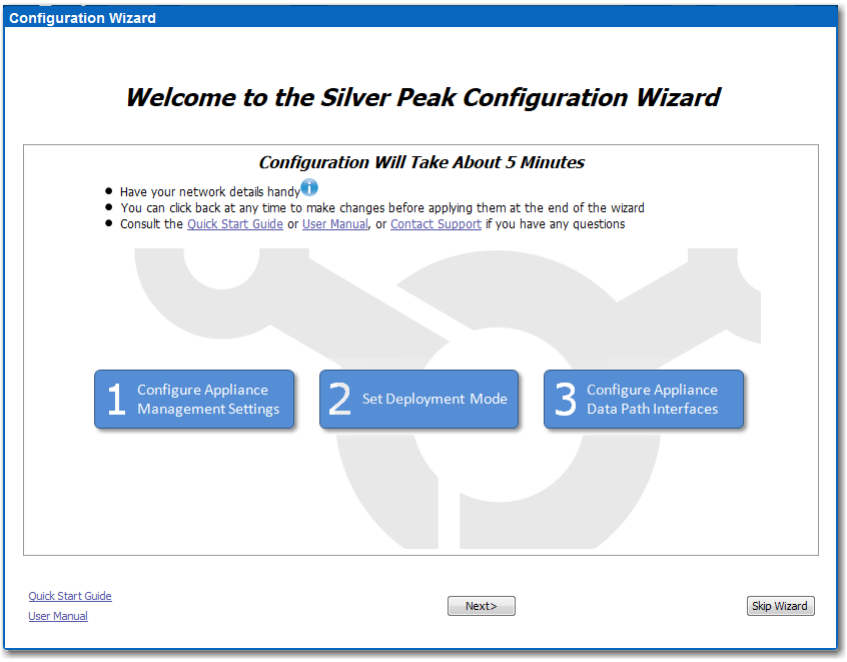
Now your VX virtual appliance is accessible via a browser.

4 Configure the Silver Peak VX Appliance from browser wizard

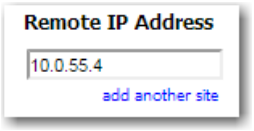
- When you bring your own license, you'll need to have it available for entry. If you're using an hourly license, it's already embedded in the appliance.
- Make sure to use your user name with the new password you created in Task 3.

a. In a browser, enter the VX's IP address in the browser's address bar. The login page loads.

When prompted, enter the user name and password.
The initial configuration wizard appears.



- On the **Configure Appliance Management Settings** page, keep the default, **DHCP**.
  [**Static** is not supported.]
- On the **Configure Appliance for Server/Out-of-Path** page, deselect **Auto-Tunnel**. **Auto-Tunnel** is not supported in AWS.
- On the **Add Remote Silver Peak** page, enter the remote appliance IP address of the VX's peer at the HQ site.



- Click **Apply**.

You have finished configuring the VX.

5 Redirect traffic to the Silver Peak VX Appliance for optimization

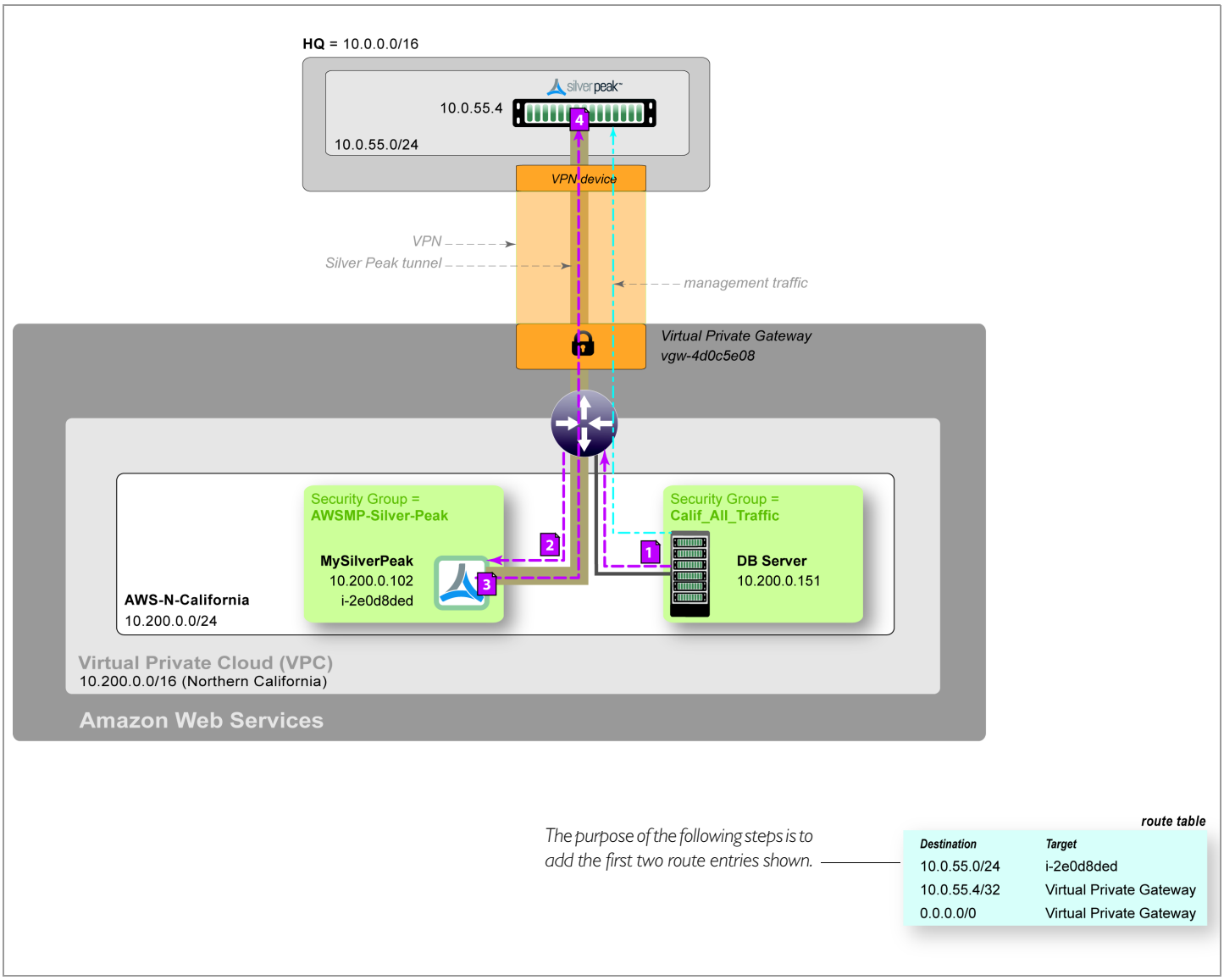
Be aware that the Amazon Virtual Private Cloud (VPC) environment has some inherent limitations that could affect your deployment choices:

- No WCCP or policy-based routing (PBR) support by Amazon VPC routers
- No broadcast or multicast support. Therefore, no VRRP support.

This diagram shows how we'll modify **AWS-N-California**'s route table to redirect **DB Server**'s traffic destined for **HQ** (at 10.0.0.0/16) to the **MySilverPeak** instance id, **i-e0d8ded**, for WAN optimization.

DB Server's traffic is routed through the VPC to **HQ** as follows:

- When DB Server sends traffic to HQ's subnet, 10.0.55.0/24, it's routed to the target, MySilverPeak. 1 2 Then, MySilverPeak optimizes the application traffic before tunnelizing it and sending it to HQ's appliance for forwarding. 3 4
- Management traffic destined from the subnet, AWS-N-California, to HQ's Silver Peak is not sent to MySilverPeak. Instead, it's routed to HQ via the Virtual Private Gateway.

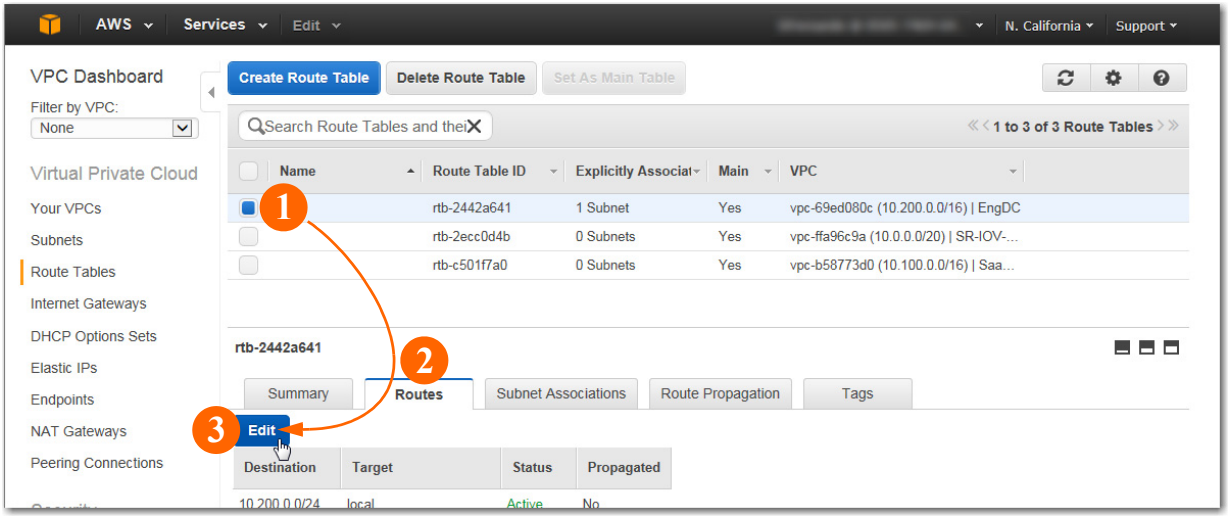


a. You must add two entries to the VPC route table — one to redirect application traffic to MySilverPeak for optimization, and the other to route management traffic without optimization.

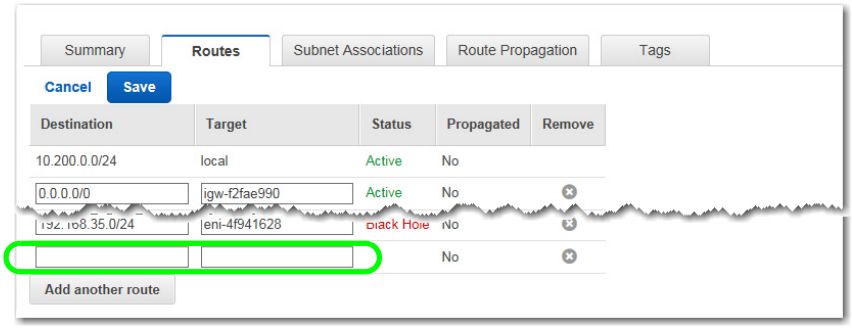
On the **AWS Management Console** tab, click **Services** and select **Navigation > VPC** from the drop-down lists.

The **VPC Dashboard** appears. From the **Navigation** pane on the left, select **Route Tables**.

b. Select the route table belonging to your subnet (or VPC), select the **Routes** tab, and click **Edit**.



The route table provides a new entry row.



c. To optimize *application traffic* going from DB server to HQ's target subnet, you need to redirect it to MySilverPeak. Complete the following:

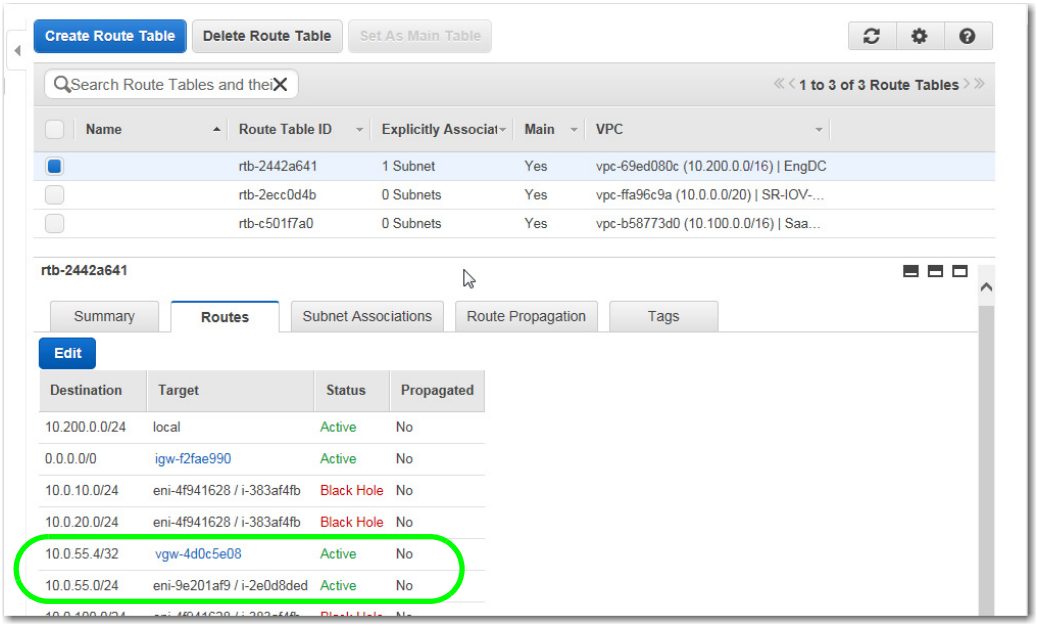
Destination:	`10.0.55.0/24`	[**HQ**'s Silver Peak appliance]
Target:	`i-2e0d8ded`	[Silver Peak instance in **AWS-N-California** subnet]

d. Click **Add another route**.

e. To route *management traffic* directly from DB Server to HQ's Silver Peak appliance, complete the following:

Destination:	`10.0.55.0/24`	[**HQ**'s Silver Peak appliance]
Target:	`vgw-4d0c5e08`	[Virtual Private Gateway]

f. Click **Save**. Both entries appear



You can now log out of Amazon.

You're now ready to begin optimizing traffic.

Following is a description of how an AWS–based virtual appliance is different from a regular virtual appliance.

How an AWS–based virtual appliance differs from a regular virtual appliance ...

An AWS–based virtual appliance has the following limitations/characteristics:

- DHCP-only
- Single-interface support. Traffic must be redirected to a VX.
- No serial port access
- No WCCP or policy-based routing (PBR) support by Amazon VPC routers.
- No broadcast or multicast support. Therefore, no VRRP support.
- No VX auto-tunnel or auto-opt support. All traffic to be optimized must be assigned to a Silver Peak tunnel.
- Traffic cannot be optimized between two **utility licensed** (that is, billed by the hour) VX appliances. To support WAN optimization between two VXs within AWS (could be in the same or different availability zones and/or regions), please make sure at least one of the VXs has a BYOL license.