VXOA AMI on Amazon Web Services

A Silver Peak Virtual Appliance (VX) 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.

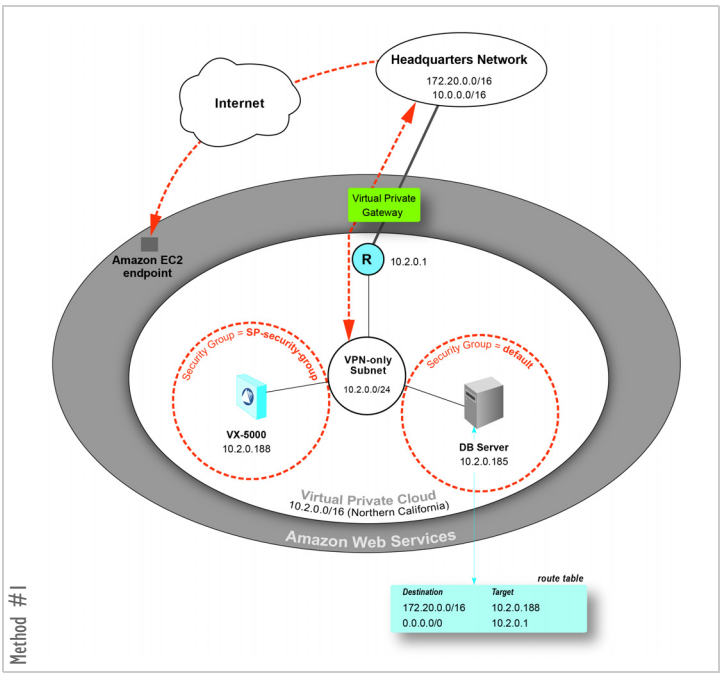
Specifically, the Silver Peak VX is available as an Amazon Machine Image (AMI), created using the Amazon Elastic Computing Cloud (EC2) management dashboard in your account, within an Amazon Virtual Private Cloud (VPC).

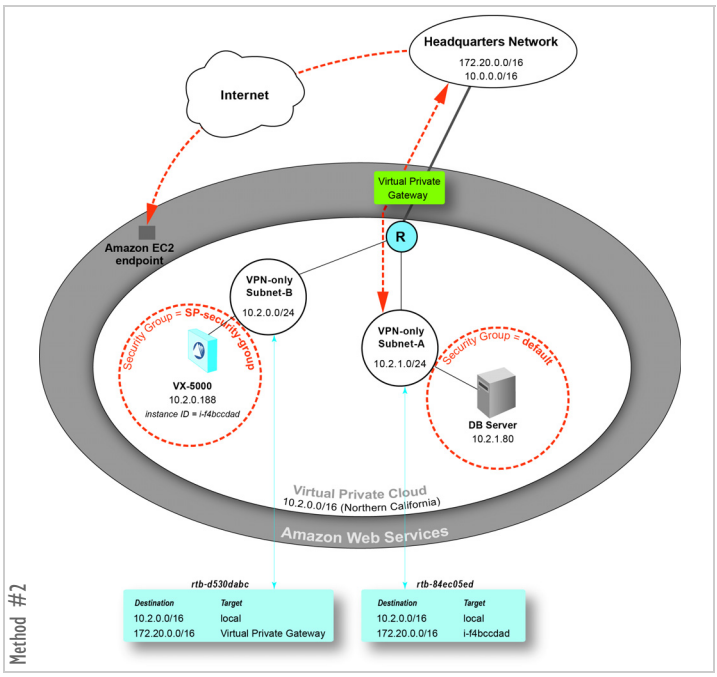
This guide explains how to deploy a Silver Peak VXOA AMI in the VPC environment, using the VX-5000 as an example. By following simple steps in the example, you can install a VX virtual appliance and start working with it within minutes of deployment.

SUMMARY OF TASKS

1. **Within Amazon Web Services (AWS), create a Virtual Private Cloud (VPC)**
2. **Obtain and launch a VXOA AMI from the AWS Marketplace**
3. **Install a VXOA AMI into the Virtual Private Cloud (VPC)**
4. **If you're using a private key, change the Silver Peak password**
5. **In a browser, configure the Silver Peak VX Appliance**
6. **Redirect traffic to the Silver Peak VX Appliance**

   Method #1 – Redirect an application server's traffic to a VX
   Method #2 – Redirect all application server traffic on a subnet to a VX





Silver Peak | Silver Peak Systems, Inc. | 4500 Great America Parkway. Suite 100. Santa Clara, CA 95054 | www.silver-peak.com/support
1.877.210.7325 (toll-free in USA) | +1.408.935.1850

For deployment within an Amazon WEB Services (AWS) cloud environment, the VX is available as an Amazon Machine Image (AMI) created using the Amazon Elastic Computing Cloud (EC2) Management console, within an Amazon Virtual Private Cloud (VPC).

Prerequisites

☑ **A virtual private cloud (VPC)**

For optimizing a VPC's inbound and outbound traffic, you must deploy a Silver Peak VX within that same VPC.

☑ **An AWS account**

☑ **Visit either the Silver Peak Marketplace or the Amazon Marketplace to register.**

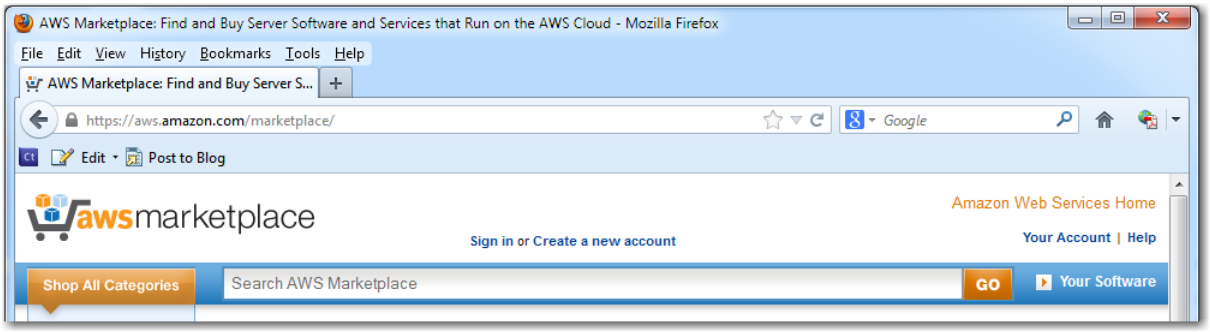
From there, you can access both the Silver Peak VXOA AMI and the VX License Key.

Within Amazon Web Services (AWS), create a Virtual Private Cloud (VPC)

To create a Virtual Private Cloud, follow the steps outlined in the *Amazon VPC Getting Started Guid*e, at http://docs.amazonwebservices.com/AmazonVPC/latest/GettingStartedGuide.

2 Obtain and launch a VXOA AMI from the AWS Marketplace

a. In the Amazon Marketplace, search for "Silver Peak".

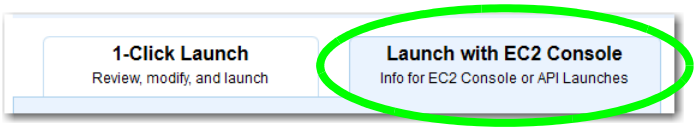


When you arrive on the Silver Peak page, click the product title.

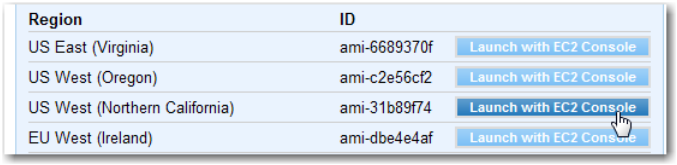
b. On the page that appears, scroll down to **Resources**, click on the link for getting a free trial license, and follow the instructions.

c. To place your order, click **Continue**. The **Launch on EC2** page appears.

d. Make sure to click the **Launch with EC2 Console** tab on the right.



e. Select a region and click **Launch with EC2 Console**.



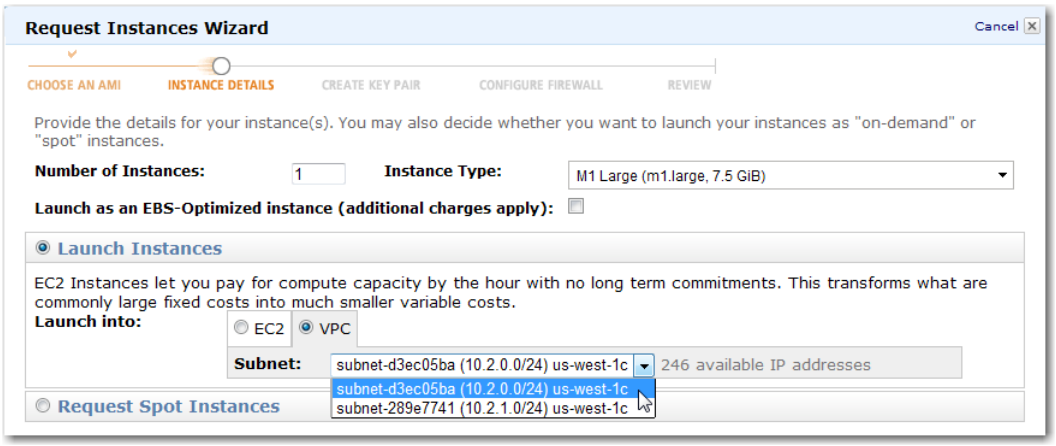
The **Request Instances Wizard** appears, and its **Choose an AMI** page displays the summarized **AMI Details**.

f. Click **Continue**. The wizard's **Instance Details** page appears, and you're now ready to launch an instance of the VXOA AMI.

3 Install a VXOA AMI into the Virtual Private Cloud (VPC)

Launching the Amazon Machine Image creates an instance in a region and in a subnet, with a specific instance type.

a. On the **Instance Details** page, complete the following fields:



Number of instances: `1`

Instance Type: `M1 Large (m1.large, 7.5 GiB)`

[Select **Launch Instances**]

Launch into: `VPC`

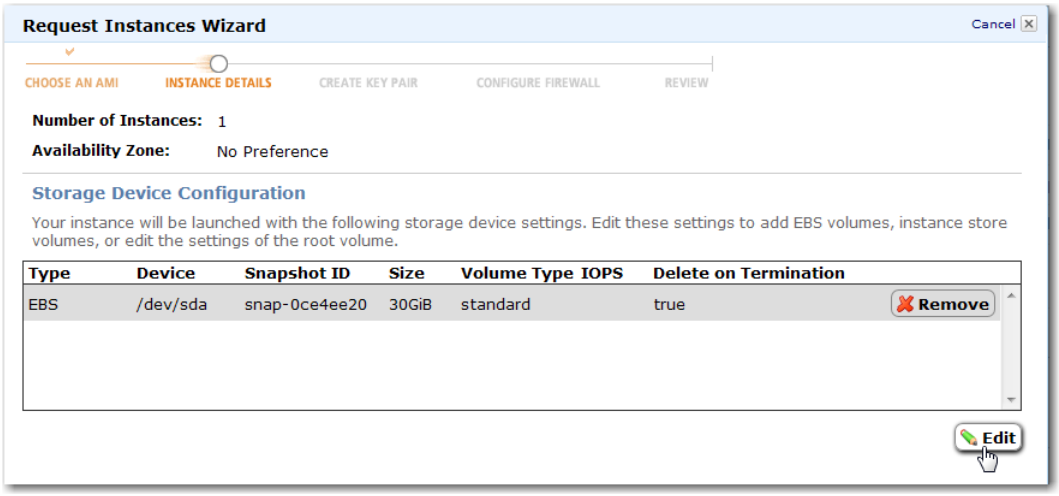
Subnet: `subnet-d3ec05ba (10.2.0.0/24)us-west-1c`
[select the subnet where you're launching the VX-5000]

At the bottom of the page, click **Continue**.

b. When the **Advanced Instance Options** page appears, just click **Continue**.
The **Storage Device Configuration** page appears.

By default, the VXOA instance has a 30GB volume attached to it. Silver Peak recommends adding a second, 70GB volume so that the VXOA AMI can support a larger dataset of cached data (if needed).

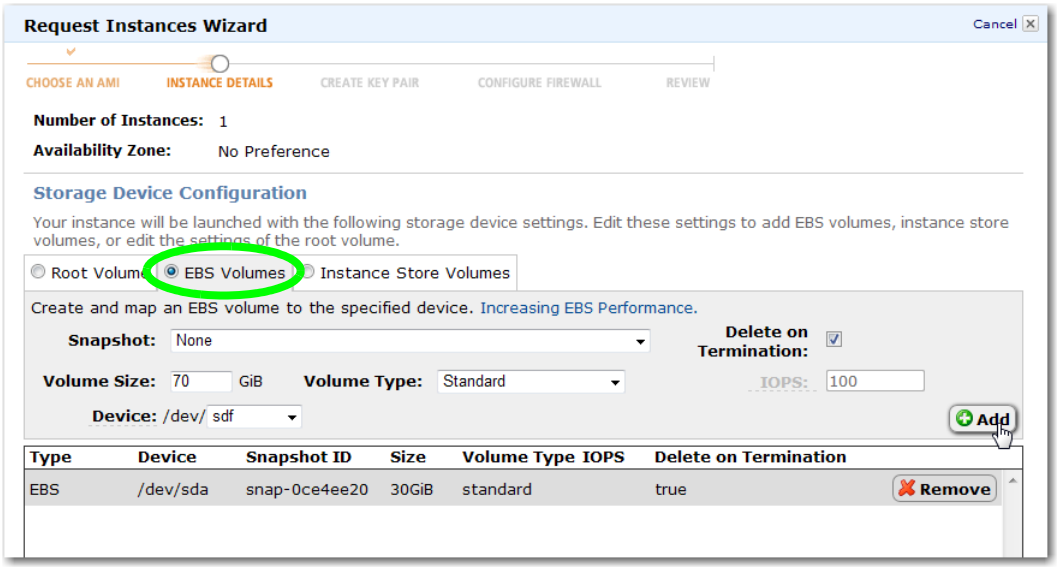
c. To begin adding a second EBS volume, click **Edit**.



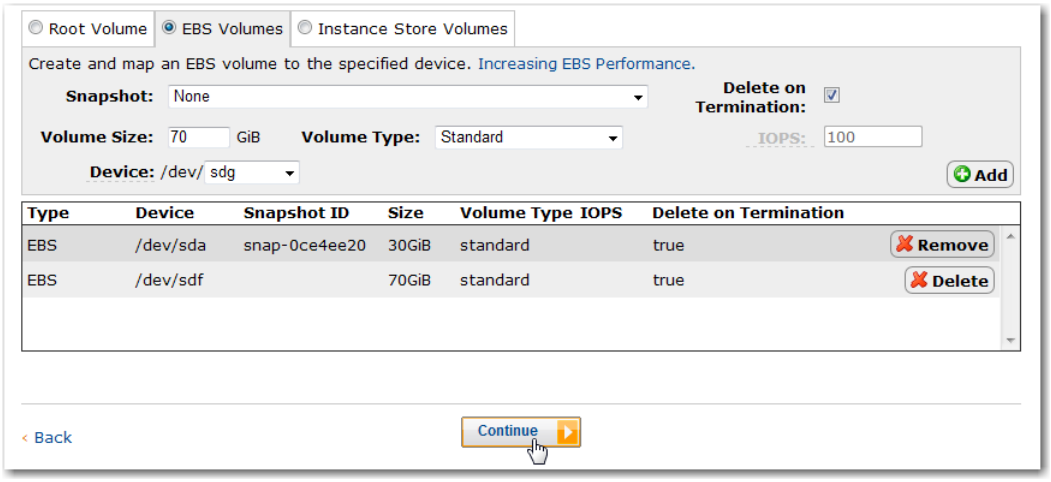
d. On the expanded **Storage Device Configuration** page, select the **EBS Volumes** tab and complete the following fields:

Volume Size: `70` [GB]

Volume Type: `Standard`



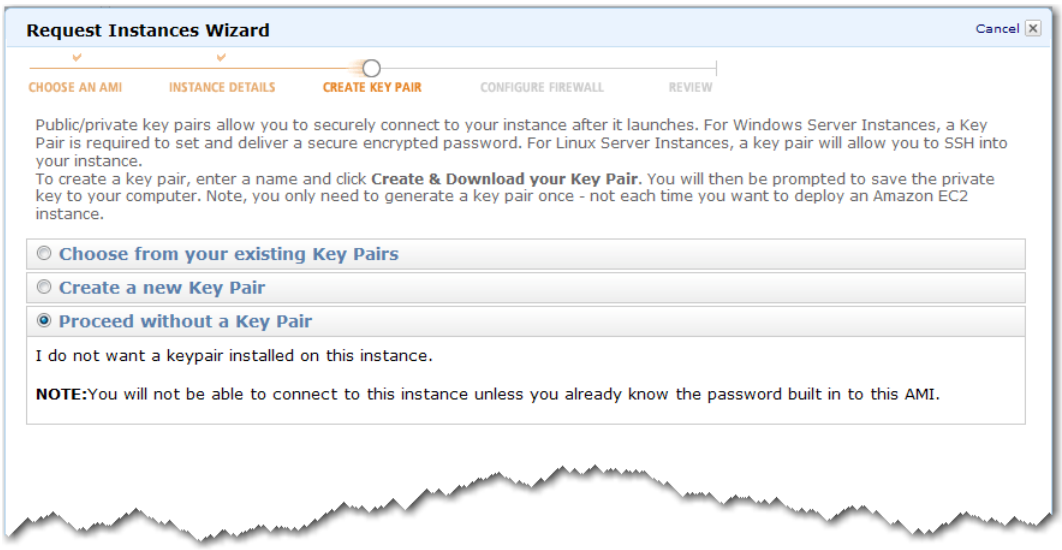
Click **Add**. The new volume appears.



Click **Continue**.

e. On the next page, you can add **optional** Key/Value tags, which are an Amazon feature available for filtering searches in your VPC. For example, you could enter a key, `VX-5000`, and a value, `Silver Peak`.

f. Click **Continue** until you arrive at the **Create Key Pair** page.



You have the following options:

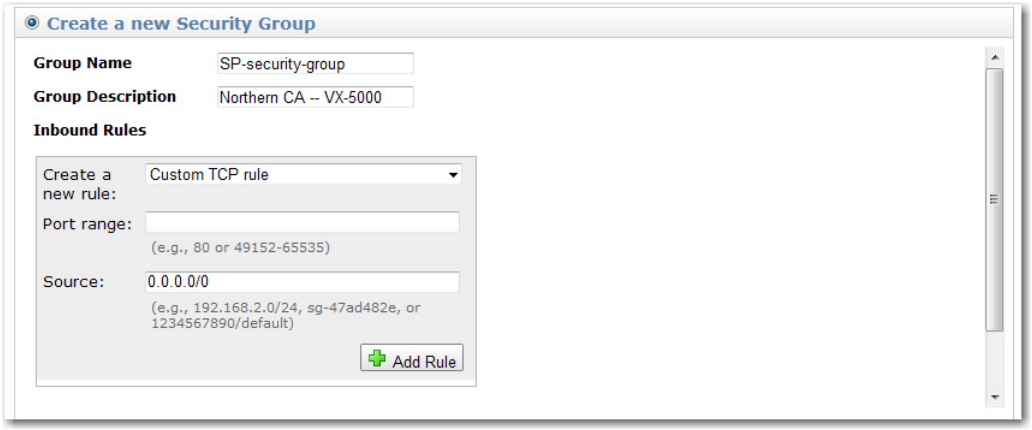
- You can either use a key pair for the VX or proceed without one. The VX works either way.
- If you create a new key pair, the wizard saves the private key to a user-specified directory on your client machine.
- If you want to use an existing key pair, the wizard prompts you to select it from the VPC's drop-down list of generated key pairs.

NOTE: If you create a key pair, or use an existing one, you'll have an additional password-related task later, in Step 4.

g. After making and following through with your key pair selection, click **Continue**. The wizard's first **Configure Firewall** page appears.

Although you can use an existing Security Group, for this example, we'll create a Security Group for the VX-5000 and we'll name it, *SP-security-group*.

h. Select **Create a new Security Group**, and enter a **Group Name** and **Group Description**.
In this example, we entered `SP-security-group` and `Northern CA -- VX-5000`, respectively.

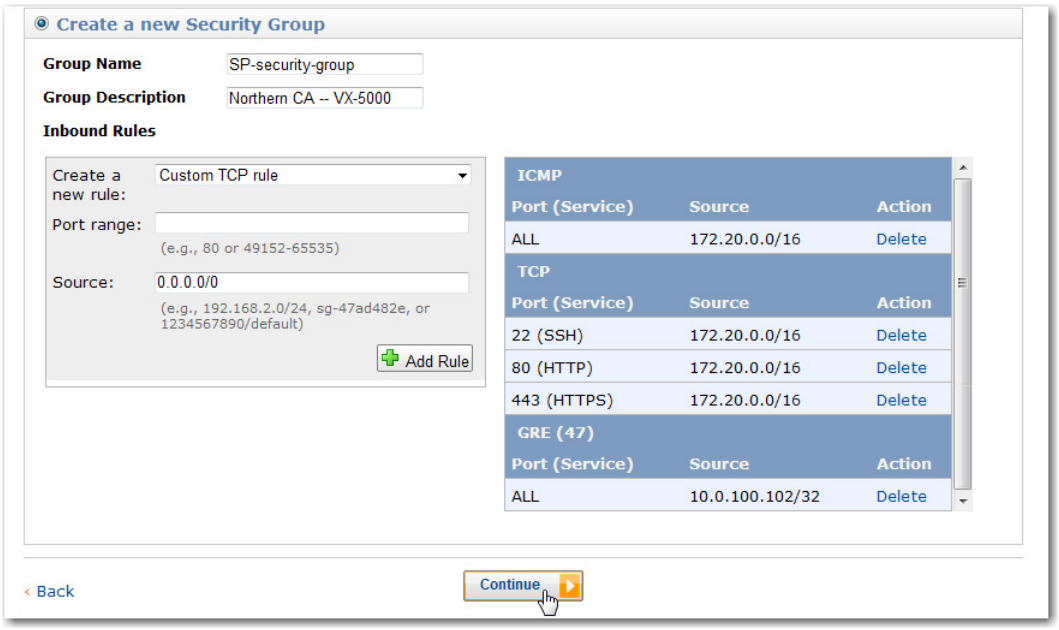


Now we need to create the inbound rules for traffic coming from the Headquarters Network to the VX-5000.

i. Select or enter the following, one line at a time:

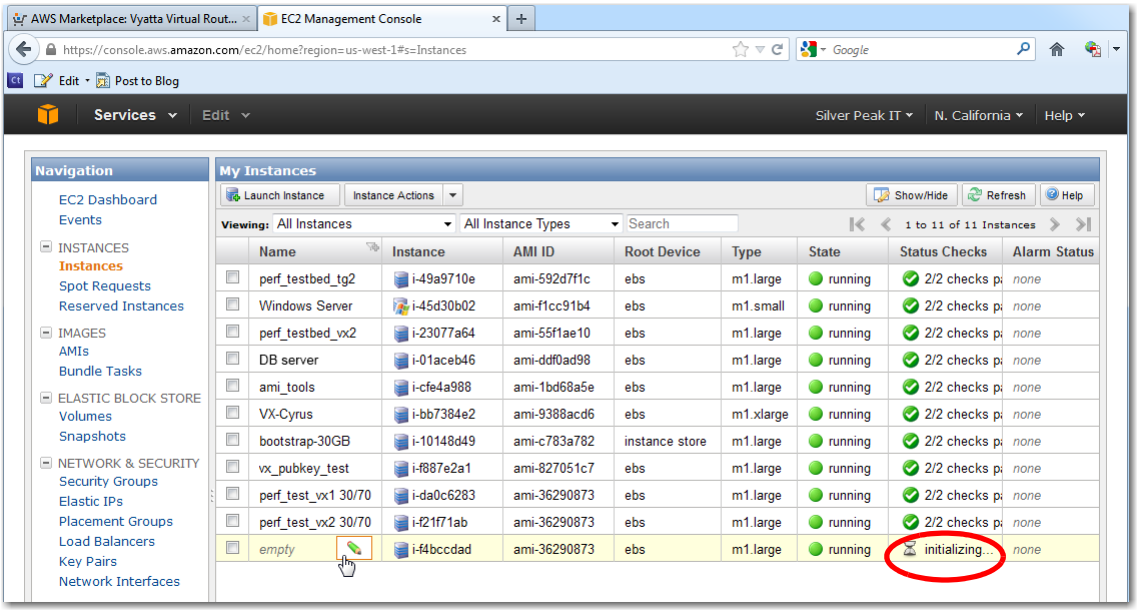
Create a new rule:	**Port range:**	**Source**:		
Custom TCP Rule	22	172.20.0.0/16	[Headquarters Network]	Click **Add Rule**
Custom TCP Rule	80	172.20.0.0/16	[Headquarters Network]	Click **Add Rule**
Custom TCP Rule	443	172.20.0.0/16	[Headquarters Network]	Click **Add Rule**
All ICMP	-	172.20.0.0/16	[Headquarters Network]	Click **Add Rule**
Custom protocol rule	47	10.0.100.102/32	[VX peer IP address]	Click **Add Rule**

The VX peer IP address is also the remote tunnel endpoint.
This is a composite view of the result:

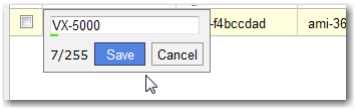


j. Click **Continue**. The wizard displays a summary of instance details.

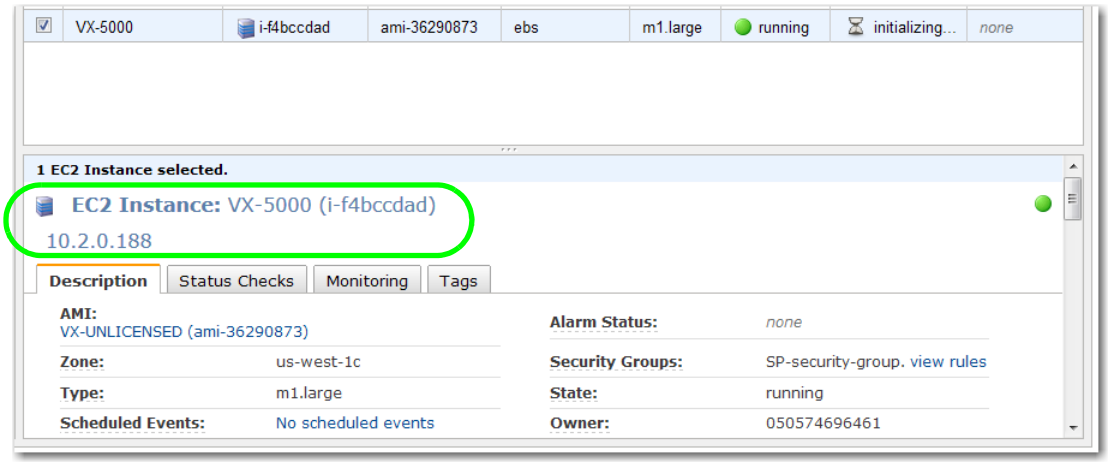
k. Click **Launch**, and when the VX launch is complete, click **Close**. The **My Instances** page of the **EC2 Console** is visible. The VX should still be initializing.



To name the VX, expose the editing icon by hovering at the right side of the *empty* **Name** field. For easy identification, in this example we name it, `VX-5000`, and save it.



l. To be able to access the WebUI (a.k.a., Access Manager) later, write down the VXOA AMI's IP address. Note that this AMI has an IP address of 10.2.0.188.



m. To enable the VX to forward redirected traffic, you must disable the VXOA AMI's **Source / Dest Check**.

☑ To do this, right-click over the VXOA 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, AWS drops de-tunneled datapath packets because the reconstituted packets have an original source IP address of source host, not the VX's source IP address.

4 If you're using a private key, change the Silver Peak password

NOTE: This section describes tasks ***as if*** you had created or used (an existing) key pair in Step 3f.

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

a. 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 silver-peak-key.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. If you're using a key pair, then the VX has no default administrative password. Therefore, you must log into the VX using the **`ssh`** command (with private key specified) before accessing Appliance Manager.

For example, **`ssh -i silver-peak-key.pem admin@10.2.0.188`**,
where the .pem file contains the private key and the VX has IP address, 10.2.0.188.

c. 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]

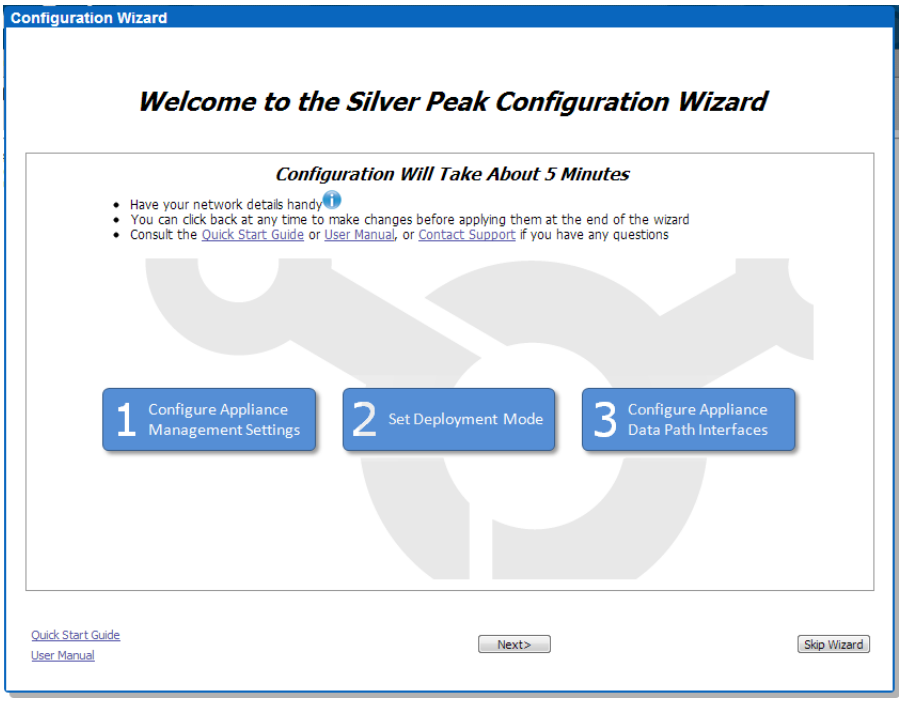
5 In a browser, configure the Silver Peak VX Appliance

To finish the initialization process, you need to complete the initial configuration wizard and manually create a tunnel and route policy.

You will need to have your VX License Key available for entry:

- If you didn't specify a key pair at VX launch time, your user name and password default to **`admin`** / **`admin`**.
- If the VX has a key pair, make sure to use your user name with the new password you created in Task 4.

a. In a browser, enter the IP address of the VX. 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 Mode** page, **Auto-Tunnel** is not supported.

b. Create a tunnel to the VX peer at the Headquarters Network, making sure to either select **Auto Discover MTU** or set the value to **1400**.

c. Create a route policy so that traffic destined to the Headquarters Network goes through the tunnel you just created. For example:

Priority	ACL	Protocol	Src Subnet	Dst Subnet	Application	Src:Dst Port	DSCP	VLAN	Tunnel
10		ip	0.0.0.0/0	10.0.0.0/16	any		any	any.any	HQ-VX2
20		ip	0.0.0.0/0	172.20.0.0/16	any		any	any.any	HQ-VX2

- **Must** select a specific tunnel.
- Do not select *pass-through*.

You must also create a route policy at the remote appliance to tunnel traffic to this VX, if destined to addresses that reside in the VPC.

You have now finished configuring your VX for optimization.

6 Redirect traffic to the Silver Peak VX Appliance

There are two approaches to redirecting traffic to the Silver Peak VX:

- **METHOD #1**: Redirect instance traffic to a VX

  This involves changing each instance's individual route table to add a route to HQ or to a branch office site.

- **METHOD #2**: Redirect all traffic within a subnet to a VX

  This involves putting the VX instance in its own subnet and adding a route entry to the VPC route table (the "middleman") to redirect all traffic in a subnet to the VX. The advantage of this approach is that all applications within a subnet can be redirected to a VX without modifying every instance's route table.

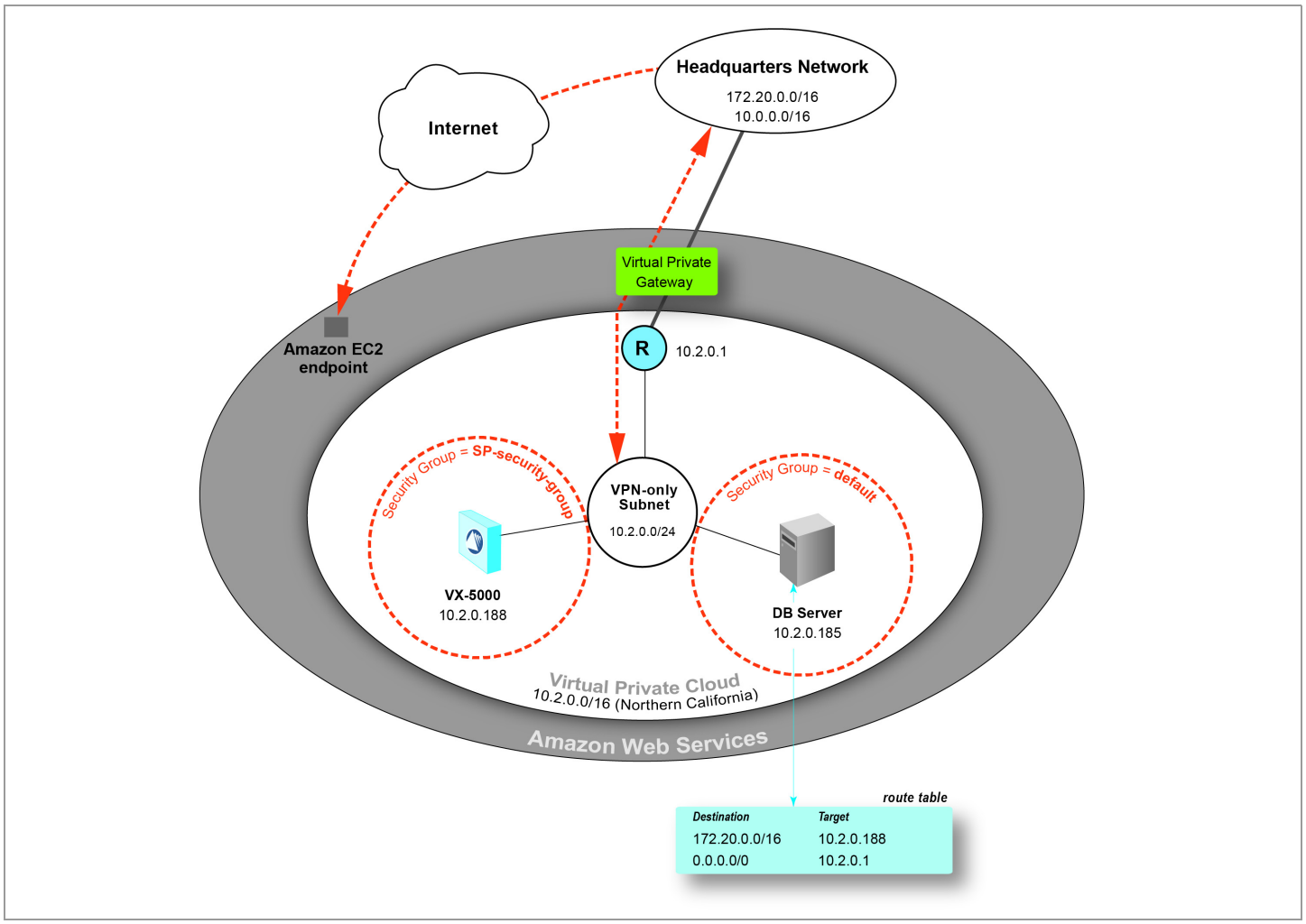
Be aware that the Amazon VPC environment has some inherent limitations that could affect your deployment choices:

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

Following are the steps for each method.

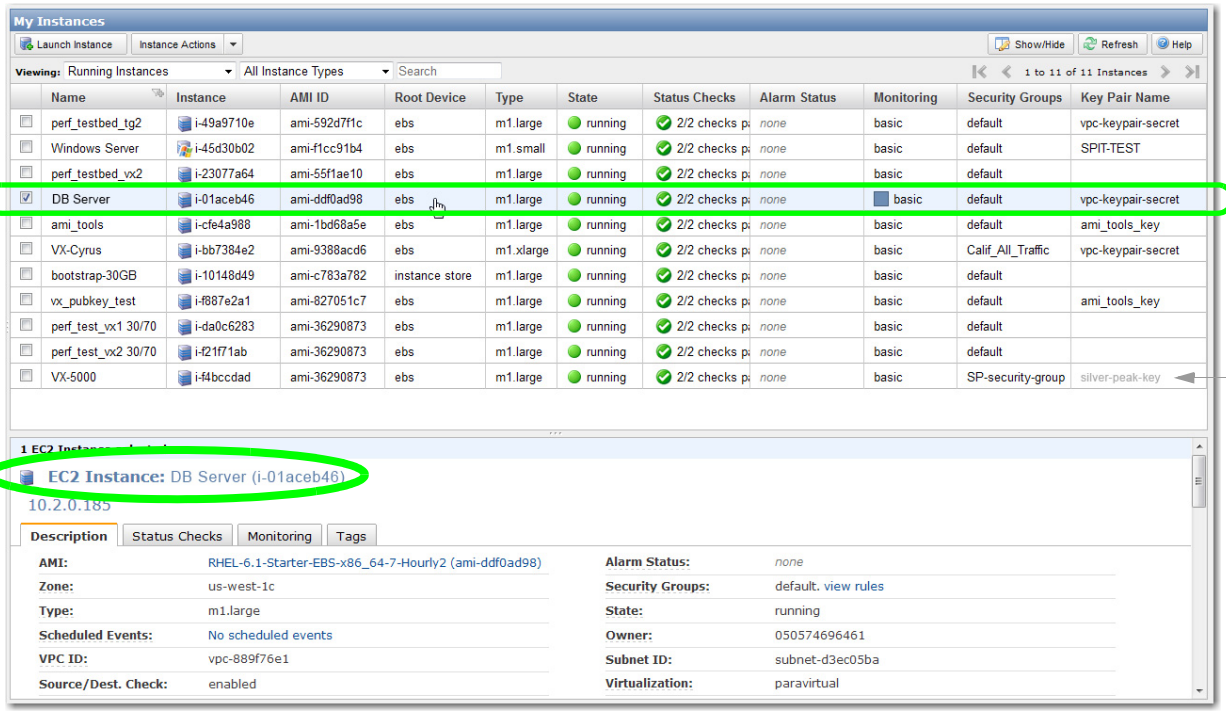
METHOD #1: Redirect instance traffic to a VX

This diagram shows how DB Server's route table is modified to redirect its traffic to the VX appliance for WAN optimization



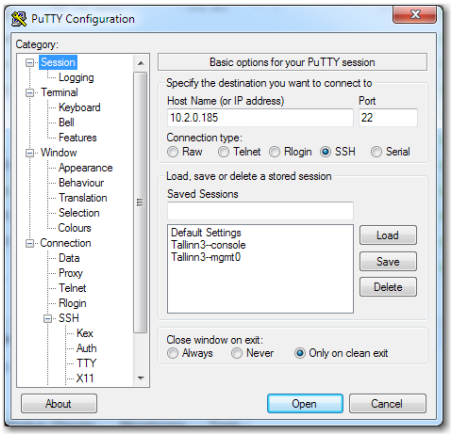
If your EC2 instance has a key, then you'll need to use a terminal emulator to access the instance and retrieve the key. In this example, we'll use *putty* to access the DB server.

a. In the **Instances** table, select **DB Server** and make note of its IP address. You'll redirect its traffic to the Silver Peak VX.



If you don't use a key pair, this is blank.

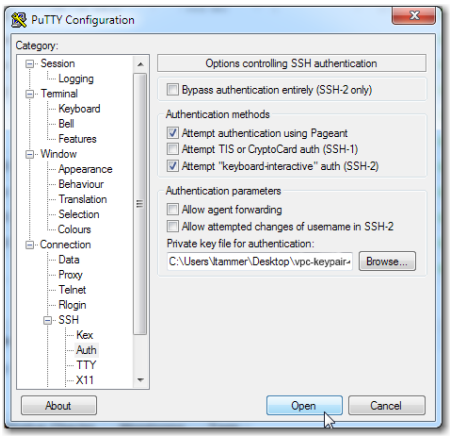
b. Open a terminal emulator and enter the EC2 instance's IP address and click **Open**. For **DB Server**, it's `10.2.0.185`.



TIP: Verify which key format your terminal emulator application requires.

- Amazon (along with many others, including SecureCRT) generates keys in **.pem** format.
- Putty only accepts keys in the **.ppk** format.
- You can use the app, PuTTYgen, to convert a **.pem** key to a **.ppk** key.

c. In the navigation tree, select **SSH** > **Auth**, click **Browse** to locate your key file, and click **Open**.



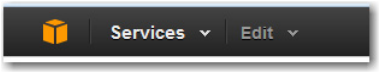
d. When the console window opens, login with your username.

Log in and create a specific route policy which tells **DB Server** (the EC2 instance) to redirect its traffic to the VX.
For example:

```
root@ip-10-2-0-185 ~]# ip route add 172.20.0.0/16 via 10.2.0.188
```

This concludes **Method #1** for redirecting traffic to the VX.

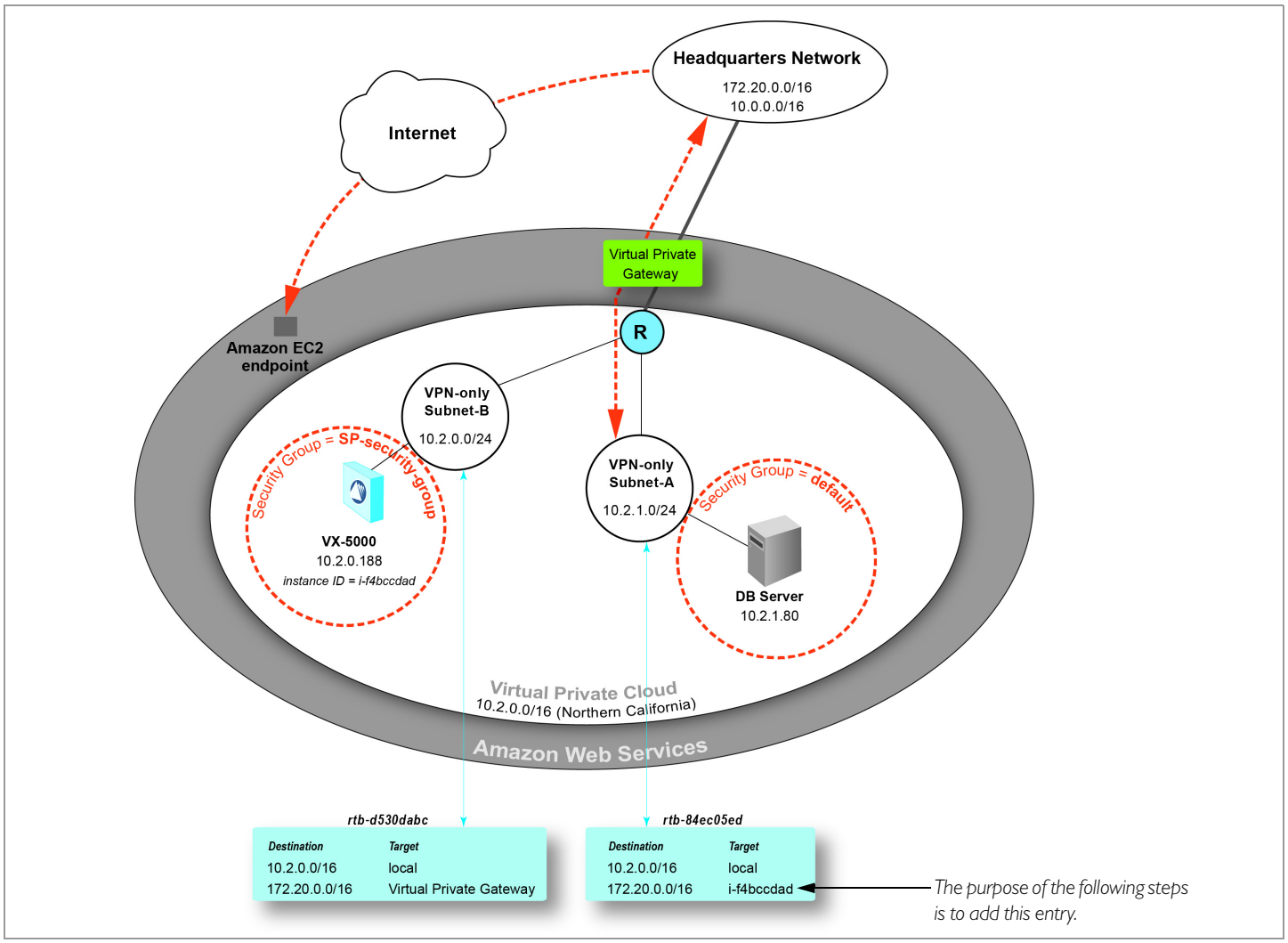
NOTE: Depending on the tunnel type, you need to verify that the tunnel port is open in the VX's security group. To do that, go to **Services > VPC > Security Group** list. **Services** is located in the left upper quadrant.



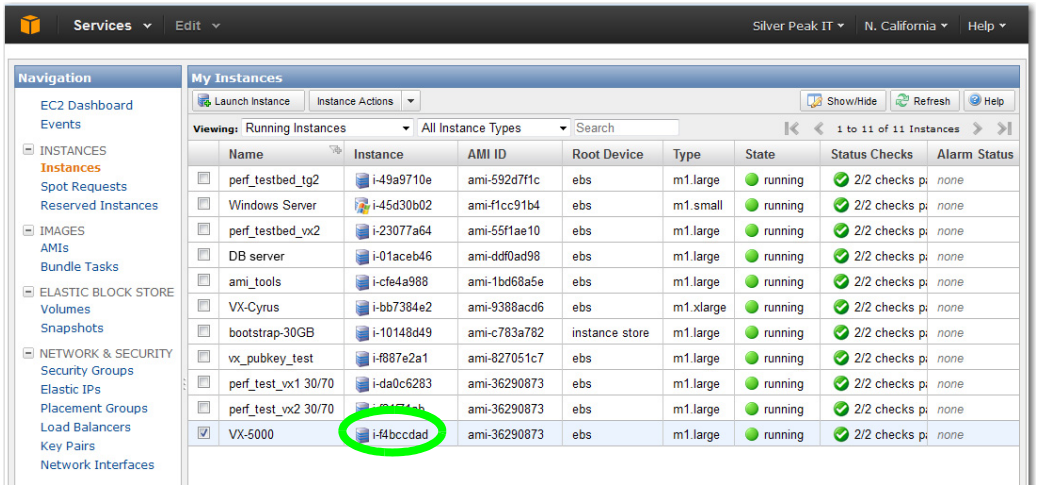
You can now log out of Amazon.

METHOD #2: Redirect all applications within a subnet to a VX

This diagram shows how Subnet-A's route table is modified to redirect traffic destined for HQ (at 172.20.0.0/16) to the VX-5000 instance id, i-f4bccdad, in subnet 10.2.0.0/24. After the VX appliance optimizes traffic, Subnet-B's route table forwards it to the VPC.



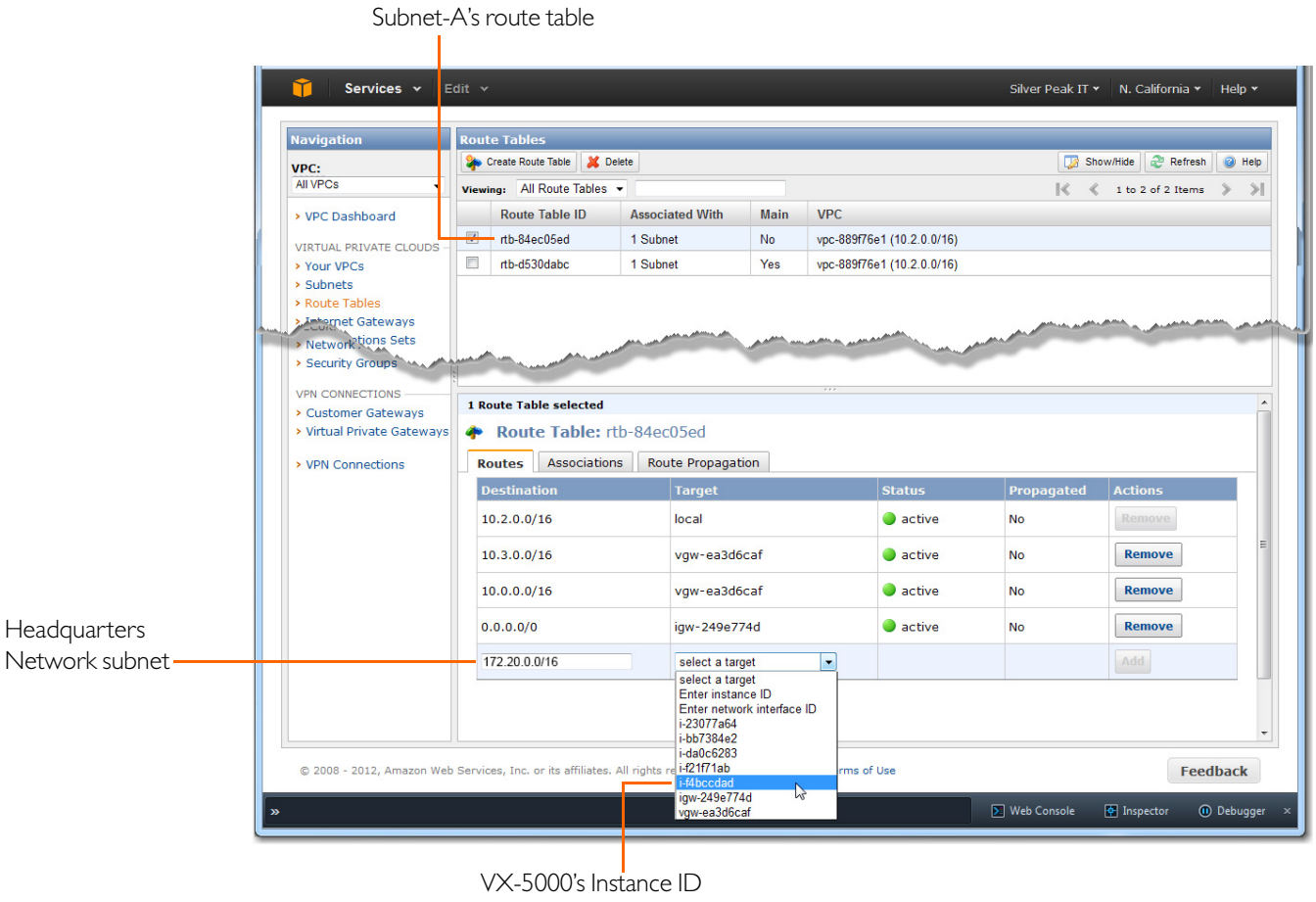
a. In the **Instances** table, select **VX-5000** and make note of its Instance value. You'll need it for the route table later.



b. At the top of the page, click **Services** and select **VPC** from the drop-down list.

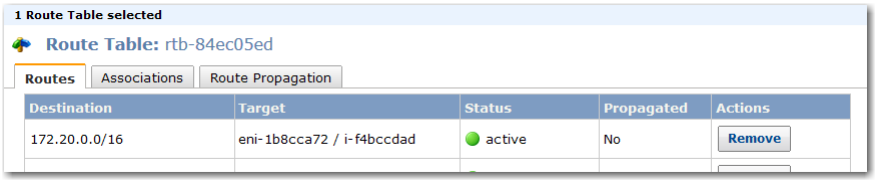
The **Amazon VPC Console Dashboard** appears. From the **Navigation** pane on the left, select **Route Tables**.

c. After selecting Subnet-A's route table, add an entry that redirects the datapath traffic you want to optimize to Subnet-B and then to the Headquarters Network (172.20.0.0/16).



d. Click **Add**, and when asked if you want to create the route, click **Yes, Create**.

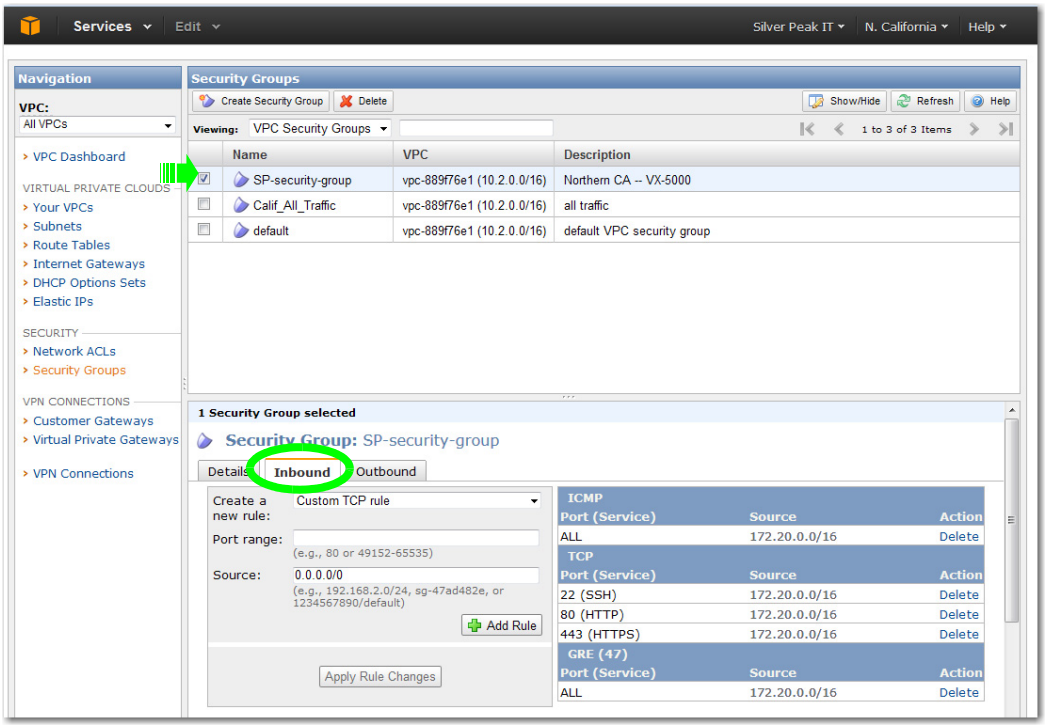
The new entry appears at the top of the route table.



Now, you need to add a rule to the VX's security group to allow traffic between applications using the `default` security group and the VX, which is using `SP-security-group`.

e. In the **VPC Management Console's Navigation** pane, on the left, click **Security Groups**.

f. From the table, select the VX subnet's security group, and select the **Inbound** tab below.



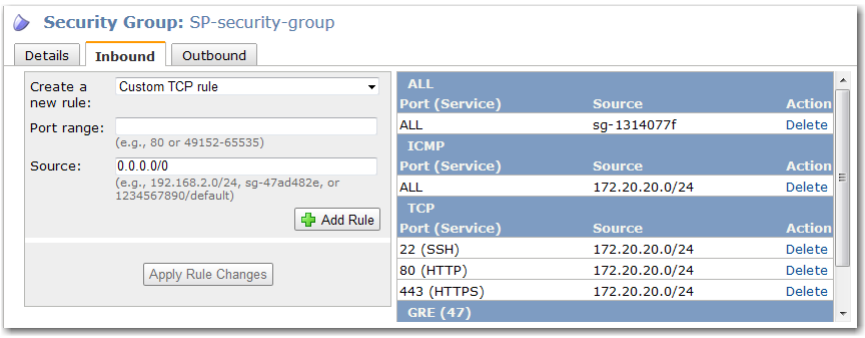
In this example, the VX is in **Subnet-B**, and it's security group is **SP-security-group**.

g. Complete the following fields:

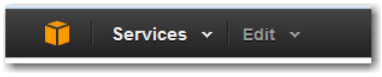
Create a new rule: [Select] **All Traffic**

Source: [Select the source application server's security group]
Here, that application server's security group is **Default**, and from its **Details** tab we can find its Group ID, `sg-1314077f`.

h. Click **Add Rule**, and verify the result.



NOTE: Depending on the tunnel type, you need to verify that the tunnel port is open in the VX's security group. To do that, go to **Services > VPC > Security Group** list. Services is located in the left upper quadrant.



This concludes **Method #2** for redirecting traffic to the VX.
You can now log out of Amazon.

Following as 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.