Silver Peak VX for Amazon Web Services

© 2013 Silver Peak Systems, Inc

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). Silver Peak recommends launching the VX AMI in environments where your VPC already has a configured virtual private network (VPN). On the Amazon side, your VPN needs to be anchored by either an Amazon Virtual Private Gateway (VPG) or a third-party VPN tunnel. If you don't have a VPN, please contact Silver Peak Support for assistance.

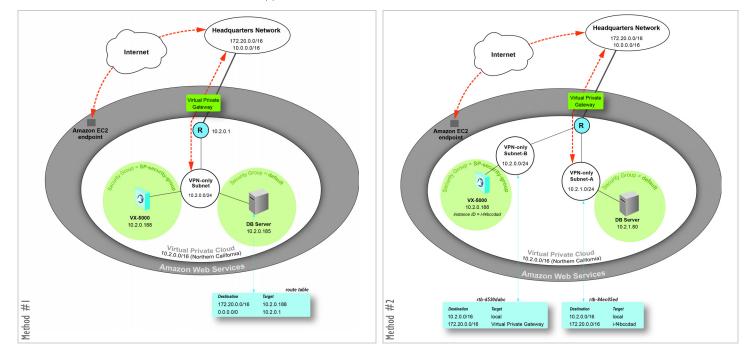
This guide explains how to deploy a Silver Peak VX AMI in the VPC environment, using the VX-5000 (WAN bandwidth = 50 Mbps) as an example. By following simple steps in the example, you can install a VX virtual appliance and start working with it within minutes of deployment.

SUMMARY OF TASKS

- Obtain and launch a VX AMI from the AWS Marketplace
- Install a VX AMI into the Virtual Private Cloud (VPC)
- **5** If you created a key pair at launch, change the Silver Peak password
- **4** In a browser, configure the Silver Peak VX Appliance

5 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 Systems, Inc. | 2860 De La Cruz Blvd. Suite 100. Santa Clara, CA 95050 | www.silver-peak.com/support I.877.210.7325 (toll-free in USA) | +1.408.935.1850

Silver Peak

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

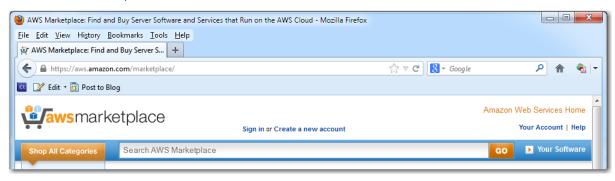
Before You Begin

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



When you arrive on the Silver Peak page, click the product title. This takes you to a new page.

- b. To begin, select the appropriate response:
 - If you bring your own license (BYOL), scroll down to **Resources**, click on the link for getting a free trial license, and follow the instructions. After getting your license, resume with these instructions by clicking **Continue**.
 - If you are using an hourly license, then click **Continue**.

The Launch on EC2 page appears.

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



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

Region	ID	
US East (Virginia)	ami-6689370f	Launch with EC2 Console
US West (Oregon)	ami-c2e56cf2	Launch with EC2 Console
US West (Northern California)	ami-31b89f74	Launch with EC2 Console
EU West (Ireland)	ami-dbe4e4af	Launch with EC2 Consule

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

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

2 Install a VX 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:

Request Insta	ances Wizard			Cancel 🗙
CHOOSE AN AMI		CREATE KEY PAIR CONFIGURE F	IREWALL REVIEW	
Provide the det "spot" instance		(s). You may also decide whethe	r you want to launch your instances as "on-demand" o	or
Number of Inst	tances: 1	Instance Type:	M1 Extra Large (m1.xlarge, 15 GiB)	•
Launch as an E	BS-Optimized instar	ce (additional charges apply):		
Launch In	istances			
		pute capacity by the hour with Ich smaller variable costs.	n no long term commitments. This transforms what a	are
Launch into:	© EC2-Cla	assic EC2-VPC		
	Subnet:	subnet-d3ec05ba (10.2.0.0/24)	us-west-1c 🚽 246 available IP addresses	
© Request S	pot Instances	subnet-d3ec05ba (10.2.0.0/24) subnet-a027ccc8 (10.2.3.0/24) subnet-d021cab8 (10.2.2.0/24) subnet-289e7741 (10.2.1.0/24)	us-west-1c us-west-1c	

Number of instances: 1 Instance Type: M1 Extra Large (m1.xlarge, 15 GiB) Launch as an EBS-Optimized instance (additional charges apply): [select] [Select Launch Instances] Launch into: EC2-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 VX instance has a 30GB volume attached to it. Silver Peak recommends adding a second, 200GB volume so that the VX AMI can support a larger dataset of cached data (if needed).

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

Request	Instances Wi	zard				Cancel 🗙
CHOOSE AN A) DETAILS CREATE KE	EY PAIR	CONFIGURE FIREWALL	REVIEW	
Number (of Instances: 1					
Availabili	ity Zone: N	lo Preference				
Storage	Device Confi	guration				
		ched with the follow ngs of the root volur		ge device settings. Edit th	nese settings to ac	d EBS volumes, instance store
Туре	Device	Snapshot ID	Size	Volume Type IOPS	Delete on Terr	nination
EBS	/dev/sda	snap-0ce4ee20	30GiB	standard	true	🔀 Remove 🔷
Í						
						Edit.

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

Volume Size:	200 [GB]
Volume Type:	Standard
Device:	/dev/sdf

	nces Wiza					Cancel
CHOOSE AN AMI		AILS CREATE KI	EY PAIR	CONFIGURE FIREWALL	REVIEW	
Number of Insta	ances: 1					
Availability Zon	e: No	Preference				
Storage Devi	ce Configu	iration				
		ed with the follow of the root volur		ge device settings. Edit t	hese settings to add EB	S volumes, instance store
🔊 Root Volum	• EBS Vol	umes 🔎 Instanc	e Store	Volumes		
Create and map	an EBS vol	ume to the spec	ified dev	ice. Increasing EBS Perfo	ormance.	
Create and map Snapshot:		ume to the spec	ified dev	ice. Increasing EBS Perfo	Termination:	
	None	ume to the spec		ice. Increasing EBS Perfo	Delete on	
Snapshot: Volume Size:	None				 Delete on Termination: 	
Snapshot: Volume Size: Device:	None 200 G /dev/ sdf	iB Volume			 Delete on Termination: 	
Snapshot: Volume Size: Device: Type De	None 200 G /dev/ sdf	iB Volume	Type: 🤇	Standard -	 Delete on Termination: IOPS: 	
Snapshot: Volume Size: Device: Type De	None 200 G /dev/ sdf	iB Volume	Type:	Standard Volume Type IOPS	Delete on Termination: IOPS: Delete on Termina	100

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

© Root V	olume 💿 EBS 🔪	/olumes 🔘 Instan	ce Store	Volumes			
Create a	nd map an EBS	volume to the spe	cified dev	rice. Increasing EBS Perf			
Sna	pshot: None					ete on 🛛 📝 nation:	
Volume	e Size: 200	GiB Volume	Type:	Standard 🗸		IOPS: 100	
, D	evice: /dev/ so	lg 🗸					C Add
Туре	Device	Snapshot ID	Size	Volume Type IOPS	Delete on T	ermination	
EBS	/dev/sda	snap-0ce4ee20	30GiB	standard	true		Kemove ^
EBS	/dev/sdf		200GiB	standard	true		🔰 Delete
							Ψ.
< Back				Continue			

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.

roup Name roup Descri	ption	SP-security-group Northern CA VX	
Inbound Rule	5		
Create a new rule:	Custor	n TCP rule	•
Port range:		30 or 49152-65535)	
Source:	0.0.0.0	/0	
		192.168.2.0/24, sg-47 57890/default)	7ad482e, or

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:

roup Name roup Descri 1bound Rule		SP-security-group Northern CA VX-5000			
Create a new rule:	Custom	n TCP rule	▼ ICMP Port (Service)	Source	Action
Port range:	(e.g., 8	0 or 49152-65535)	ALL	172.20.0.0/16	Delete
Source:	0.0.0.0/0 (e.g., 192.168.2.0/24, sg-47ad482e, or		TCP Port (Service)	Source	Action
	123456	7890/default)	22 (SSH)	172.20.0.0/16 172.20.0.0/16	Delete Delete
			80 (HTTP) 443 (HTTPS)	172.20.0.0/16	Delete
			GRE (47) Port (Service)	Source	Action
			ALL	10.0.100.102/32	Delete

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.

https://console.aws.amazor Zedit • Rest to Blog	n.com/e	c2/home?region=us-wes	t-1#s=Instances			☆ ⊽ C	<mark>∛]</mark> ▼ Google		_
	idit 🗸	,					Silver Peak	IT 👻 N. Californi	a 🕶 Help 🕶
lavigation	My I	instances							
EC2 Dashboard	🐻 L	aunch Instance Instan	ce Actions 🔻				U	Show/Hide 🛛 🍣 Ret	resh 🕜 Help
Events	View	ing: All Instances	✓ All In	stance Types	 Search 		≪ →	🕻 1 to 11 of 11 Inst	ances 🔉 🔌
INSTANCES		Name 🚿	Instance	AMI ID	Root Device	Туре	State	Status Checks	Alarm Status
Instances Spot Requests		perf_testbed_tg2	河 i-49a9710e	ami-592d7f1c	ebs	m1.large	running	🥝 2/2 checks p	none
Reserved Instances		Windows Server	🚮 i-45d30b02	ami-f1cc91b4	ebs	m1.small	running	2/2 checks participation	none
- IMAGES		perf_testbed_vx2	🅃 i-23077a64	ami-55f1ae10	ebs	m1.large	running	2/2 checks participation	none
AMIs Bundle Tasks		DB server	🥃 i-01aceb46	ami-ddf0ad98	ebs	m1.large	running	2/2 checks participation	none
		ami_tools	i-cfe4a988	ami-1bd68a5e	ebs	m1.large	running	2/2 checks participation	none
ELASTIC BLOCK STORE Volumes		VX-Cyrus	i-bb7384e2	ami-9388acd6	ebs	m1.xlarge	running	2/2 checks p	none
Snapshots		bootstrap-30GB	i-10148d49	ami-c783a782	instance store	m1.large	running	2/2 checks p	none
NETWORK & SECURITY		vx_pubkey_test	🥃 i-f887e2a1	ami-827051c7	ebs	m1.large	running	2/2 checks p	none
Security Groups Elastic IPs	:	perf_test_vx1 30/70	i-da0c6283	ami-36290873	ebs	m1.large	running	2/2 checks p	none
Placement Groups		perf_test_vx2 30/70	🥃 i-f21f71ab	ami-36290873	ebs	m1.large	running	2/2 checks p	none
Load Balancers Kev Pairs		empty	i-f4bccdad	ami-36290873	ebs	m1.large	running	📓 initializing	none

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, $\sqrt{x} - 5000$, and save it.



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

EC2 Instance selected.				
EC2 Instance: V 10.2.0.188	X-5000 (i-f4bccdad)			•
Description Status AMI: VX-UNLICENSED (ami-36	5 5	Alarm Status:	none	-
Zone:	us-west-1c	Security Groups:	SP-security-group. view rules	
Туре:	m1.large	State:	running	
Scheduled Events:	No scheduled events	Owner:	050574696461	

m. 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.

I 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.

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**.

11.00

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.

- n. In the **VPC Management Console's Navigation** pane, on the left, click **Security Groups**.
- o. From the table, select the VX subnet's security group, and select the **Inbound** tab below.

					Silver Peak IT 🕶	N. California 👻 🛛 Help	•
Navigation	Security	Groups					
VPC:		e Security Group 🛛 💥 Delete			🎲 Show/	Hide ಿ Refresh 🛛 🕝 H	Help
All VPCs	Viewing	VPC Security Groups -			I< <	1 to 3 of 3 Items	×
> VPC Dashboard		me	VPC	Description	18 8	10001010000	~1
> VPC Dashboard				Northern CA VX-5000			
VIRTUAL PRIVATE CLOUDS		SP-security-group	vpc-889f76e1 (10.2.0.0/16)				
> Your VPCs	-	Calif_All_Traffic	vpc-889f76e1 (10.2.0.0/16)	all traffic			
 Subnets Route Tables 		▶ default	vpc-889f76e1 (10.2.0.0/16)	default VPC security group			
 Internet Gateways 							
 DHCP Options Sets 							
> Elastic IPs							
Flasue IPS							
SECURITY							
Network ACLs							
 Network ACES 							
Security Groups							
Security Groups VPN CONNECTIONS	1 Securi	ity Group selected					•
 Security Groups VPN CONNECTIONS Customer Gateways 			security-group				-
Security Groups VPN CONNECTIONS		curity Group: SP-s					^
 Security Groups VPN CONNECTIONS Customer Gateways 		curity Group: SP-s					•
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys Se Details	curity Group: SP-s		ІСМР			•
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys i Se	curity Group: SP-s	und	ICMP Port (Service)	Source	Action	•
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Details Creat new r	Curity Group: SP-s	und		Source 172.20.0.0/16	Action Delete	•
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Details Creat new r	curity Group: SP-s	und -	Port (Service)			A III
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Details Creat new r	curity Group: SP-s Inbound Outboo e a Custom TCP rule ule: ange: (e.g., 80 or 49152- ce: 0.0.0.00	und -	Port (Service) ALL			A H
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Detaile Creat new r Port r	Currity. Group: SP-S Inbound Outboo Custom TCP rule Custom TCP rule (e.g., 80 or 49152- (e.g., 192.168.2.0) Custom 7.9	und •	Port (Service) ALL TCP	172.20.0.0/16	Delete	E E
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Detaile Creat new r Port r	curity Group: SP-s Inbound Outboo e a Custom TCP rule ule: ange: (e.g., 80 or 49152- ce: 0.0.0.00	und 65535) 24, sg-47ad482e, or It)	Port (Service) ALL TCP Port (Service)	172.20.0.0/16 Source	Delete Action	E
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Detaile Creat new r Port r	Currity. Group: SP-S Inbound Outboo Custom TCP rule Custom TCP rule (e.g., 80 or 49152- (e.g., 192.168.2.0) Custom 7.9	und •	Port (Service) ALL TCP Port (Service) 22 (SSH)	172.20.0.0/16 Source 172.20.0.0/16	Delete Action Delete	E
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Detaile Creat new r Port r	Currity. Group: SP-S Inbound Outboo Custom TCP rule Custom TCP rule (e.g., 80 or 49152- (e.g., 192.168.2.0) Custom 7.9	und 65535) 24, sg-47ad482e, or It)	Port (Service) ALL TCP Port (Service) 22 (SSH) 80 (HTTP)	172.20.0.0/16 Source 172.20.0.0/16 172.20.0.0/16	Delete Action Delete Delete	E
 > Security Groups > VPN CONNECTIONS > Customer Gateways > Virtual Private Gateway 	ys > Se Detaile Creat new r Port r	Currity. Group: SP-S Inbound Outboo Custom TCP rule Custom TCP rule (e.g., 80 or 49152- (e.g., 192.168.2.0) Custom 7.9	und 65535) 24, sg-47ad482e, or R) 4 Add Rule	Port (Service) ALL TCP Port (Service) 22 (SSH) 80 (HTTP) 443 (HTTPS)	172.20.0.0/16 Source 172.20.0.0/16 172.20.0.0/16	Delete Action Delete Delete	E

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

p. 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.

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

etails In	bound Outbound			
Create a	Custom TCP rule	✓ ALL		
new rule:		Port (Service)	Source	Actio
Port range:		ALL	sg-1314077f	Delete
5	(e.g., 80 or 49152-65535)	ІСМР		
Source:	0.0.0/0	Port (Service)	Source	Actio
	(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)	ALL	172.20.20.0/24	Delete
		тср		
	🕂 Add Ru	Port (Service)		Actio
		22 (SSH)	172.20.20.0/24	Delete
	Apply Rule Changes	80 (HTTP)	172.20.20.0/24	Delete
	· · · · · · · · · · · · · · · · · · ·	443 (HTTPS)	172.20.20.0/24	Delete

NOTE: If you don't want to use GRE as your tunnel encapsulation mode, be sure to add a rule for UDP or IPsec.

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 If you created a key pair at launch, 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:

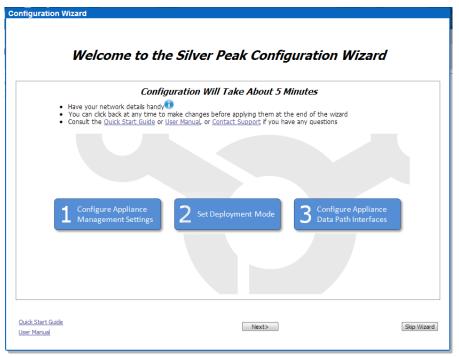
[vx-appliance] > enable	[ENTER]
[vx-appliance] # configure terminal	[ENTER]
<pre>[vx-appliance] (config) # username admin password <new-password></new-password></pre>	[ENTER]
Dr.	
[vx-appliance] (config) # username monitor password <new-password></new-password>	[ENTER]
	<pre>[vx-appliance] # configure terminal [vx-appliance] (config) # username admin password <new-password> or</new-password></pre>

4 In a browser, configure the Silver Peak VX Appliance

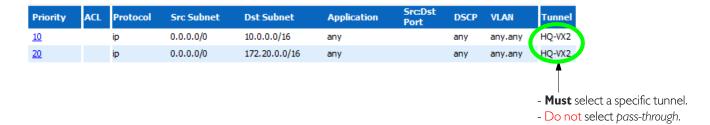
To finish the initialization process, you need to complete the initial configuration wizard and manually create a tunnel and route policy.

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.

- If you didn't specify a key pair at VX launch time, use the username and password, admin / admin.
- If you have a key pair for the VX, 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 route policy so that traffic destined to the Headquarters Network goes through the tunnel you just created. For example:



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.

5 Redirect traffic to the Silver Peak VX Appliance

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

• **METHOD #I**: 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.

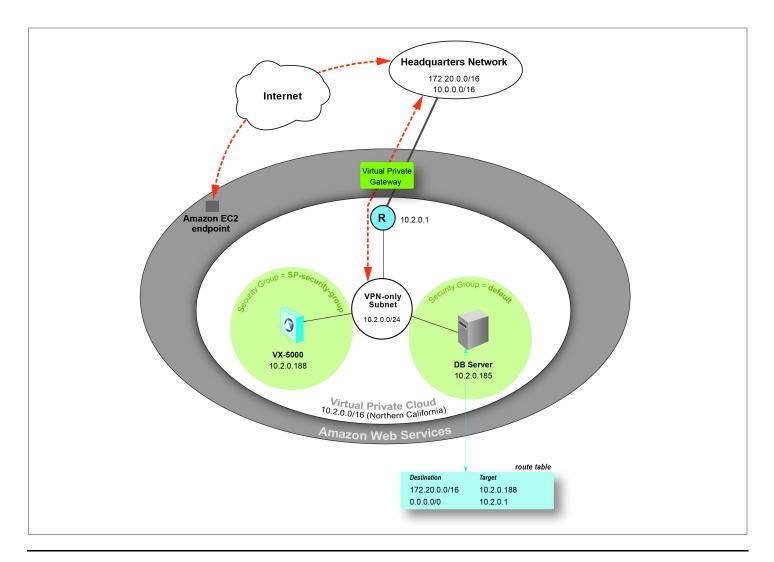
Be aware that the Amazon VPC environment has some inherent limitations that could affect your deployment choices:

- 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



a. In the **Instances** table, select **DB Server** and make note of its IP address.

۱	aunch Instance Instand	ce Actions 🔻								🍃 Show/Hide	Refresh 🥝 Help
ew	ng: Running Instances	✓ All In	stance Types	 Search 						≪ ≪ 1 to 11 c	of 11 Instances 📎 📎
	Name 🤝	Instance	AMI ID	Root Device	Туре	State	Status Checks	Alarm Status	Monitoring	Security Groups	Key Pair Name
1	perf_testbed_tg2	🏹 i-49a9710e	ami-592d7f1c	ebs	m1.large	running	2/2 checks page	none	basic	default	vpc-keypair-secret
]	Windows Server	🚮 i-45d30b02	ami-f1cc91b4	ebs	m1.small	running	2/2 checks p;	none	basic	default	SPIT-TEST
1	perf_testbed_vx2	🥃 i-23077a64	ami-55f1ae10	ebs	m1.large	running	2/2 checks page	none	basic	default	
	DB Server	🥃 i-01aceb46	ami-ddf0ad98	ebs "Im	m1.large	running	2/2 checks p	none	basic	default	vpc-keypair-secret
1	ami_tools	🅃 i-cfe4a988	ami-1bd68a5e	ebs	m1.large	running	2/2 checks page	none	basic	default	ami_tools_key
1	VX-Cyrus	🍯 i-bb7384e2	ami-9388acd6	ebs	m1.xlarge	running	2/2 checks page	none	basic	Calif_All_Traffic	vpc-keypair-secret
	bootstrap-30GB	🥃 i-10148d49	ami-c783a782	instance store	m1.large	running	2/2 checks page	none	basic	default	
1	vx_pubkey_test	🥃 i-f887e2a1	ami-827051c7	ebs	m1.large	running	2/2 checks page	none	basic	default	ami_tools_key
]	perf_test_vx1 30/70	🅃 i-da0c6283	ami-36290873	ebs	m1.large	running	2/2 checks p;	none	basic	default	
1	perf_test_vx2 30/70	🥃 i-f21f71ab	ami-36290873	ebs	m1.large	running	2/2 checks page	none	basic	default	
1	VX-5000	i-f4bccdad	ami-36290873	ebs	m1.large	running	2/2 checks p:	none	basic	SP-security-group	silver-peak-key 🔫
1	EC2 Instance: 0.2.0.185 escription Statu		01aceb46)								
	AMI: RHEL-6.1-Starter-EBS-x86_64-7-Hourly2 (ami-ddf0ad98)				ddf0ad98)	Alarn	n Status:	none			
1	Zone:	us-west-1c				Secu	Security Groups: default. view rules				
	ype:	m1.large				State	State: running				
		Scheduled Events: No scheduled events				Own	Owner: 050574696461				
		No schedu vpc-889f76					et ID:	subnet-d3ec			

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

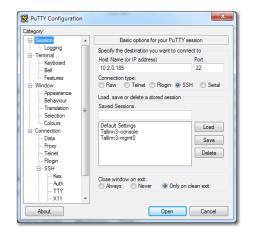
Your **DB Server** could be either a Linux machine or a Windows machine. The means for accessing each is slightly different:

- If it's Linux, see steps **b** through **d**.
- If it's Windows, see steps **e** through **f**.

How to add the route for a Linux machine:

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.

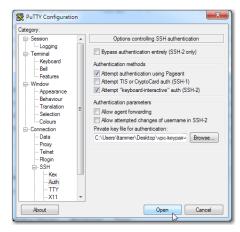
b. Open a terminal emulator and enter the EC2 instance's IP address and click **Open**. For **DB Server**, it's 10.2.0.185.



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. Use the Load and Save buttons only.

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

To make the route persistent, use Linux instructions that pertain to your environment to add a permanent route.

This concludes **Method #I** for redirecting traffic from a Linux machine to the VX.

How to add a route for a Windows machine:

- e. Using a Remote Desktop connection, login to **DB Server**.
- f. Log in and create a specific route policy which tells **DB Server** (the EC2 instance) to redirect its traffic to the VX. To make the route persistent, use -p. For example:

root@ip-10-2-0-185 ~] # route ADD [-p] <destination IP address or subnet> MASK <subnet
mask> <VX-5000 gateway IP address>

Specifically:

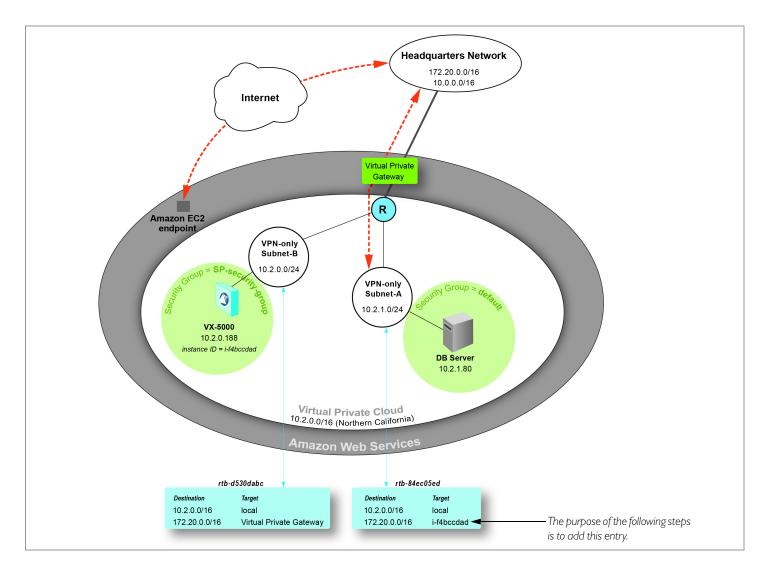
root@ip-10-2-0-185 ~] # route ADD -p 172.20.0.0 mask 255.255.0.0 10.2.0.188

This concludes **Method #I** for redirecting traffic from a Windows machine to the VX.

g. 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.

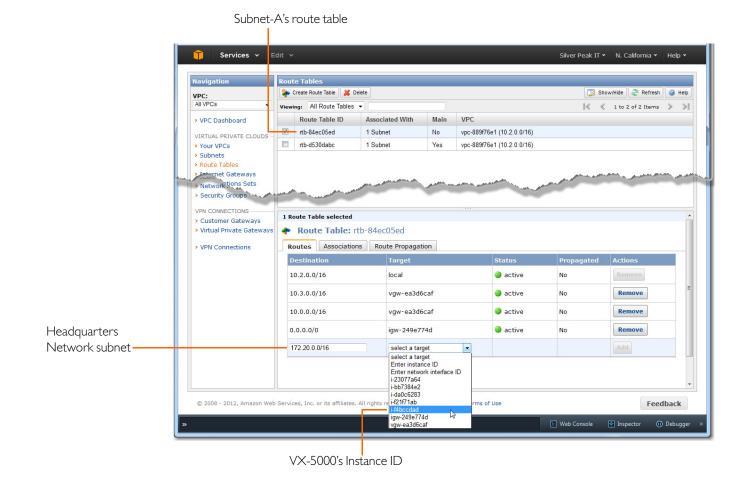
lavigation	My Instances									
EC2 Dashboard	🙀 Launch Instance Actions 🔻 😨 Refresh 🔮 Help									
Events	View	ing: Running Instances	✓ All In:	stance Types	▼ Search 🛛 🕹 🐇 search					
INSTANCES		Name 🐄	Instance	AMI ID	Root Device	Туре	State	Status Checks	Alarm Statu	
Instances Spot Requests		perf_testbed_tg2	🅃 i-49a9710e	ami-592d7f1c	ebs	m1.large	running	2/2 checks pa	none	
Reserved Instances		Windows Server	🚮 i-45d30b02	ami-f1cc91b4	ebs	m1.small	running	🔮 2/2 checks p	none	
IMAGES AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes		perf_testbed_vx2	🅃 i-23077a64	ami-55f1ae10	ebs	m1.large	running	2/2 checks page	none	
		DB server	竇 i-01aceb46	ami-ddf0ad98	ebs	m1.large	running	📀 2/2 checks p	none	
		ami_tools	i-cfe4a988	ami-1bd68a5e	ebs	m1.large	running	2/2 checks page	none	
		VX-Cyrus	🍯 i-bb7384e2	ami-9388acd6	ebs	m1.xlarge	running	📀 2/2 checks p	none	
Snapshots		bootstrap-30GB	🥃 i-10148d49	ami-c783a782	instance store	m1.large	running	2/2 checks page	none	
 NETWORK & SECURITY Security Groups Elastic IPs Placement Groups Load Balancers Key Pairs 		vx_pubkey_test	藚 i-f887e2a1	ami-827051c7	ebs	m1.large	running	2/2 checks page	none	
		perf_test_vx1 30/70	🥃 i-da0c6283	ami-36290873	ebs	m1.large	running	2/2 checks page	none	
		perf_test_vx2 30/70	Contrates	ami-36290873	ebs	m1.large	running	2/2 checks page	none	
		VX-5000	i-f4bccdad	ami-36290873	ebs	m1.large	running	2/2 checks page	none	

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.

1 Route Table selected				
Route Table: rtb-	-84ec05ed			
Routes Associations	Route Propagation			
Destination	Target	Status	Propagated	Actions
172.20.0.0/16	eni-1b8cca72 / i-f4bccdad	active	No	Remove

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

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 <u>BYOL license</u>.