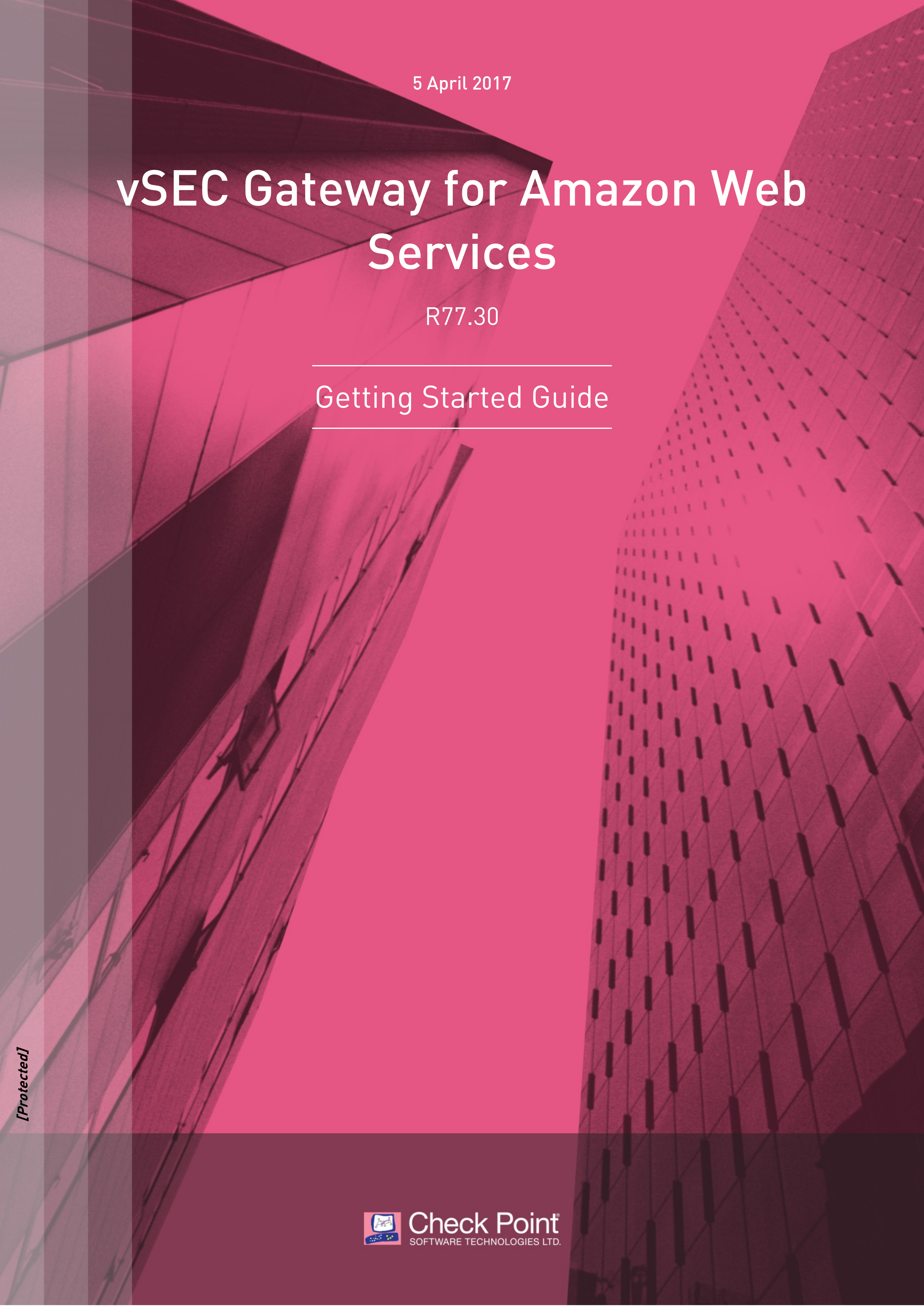


5 April 2017

vSEC Gateway for Amazon Web Services

R77.30

Getting Started Guide

Check Point
SOFTWARE TECHNOLOGIES LTD.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=45816

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Revision History

Date	Description
05 April 2017	Product name change from Security Gateway Virtual Edition to vSEC Gateway for Amazon Web Services. Added sk111013 http://supportcontent.checkpoint.com/solutions?id=sk111013. Updated instructions ("Routing Traffic through the Security Gateway" on page 12). Updated instructions ("Assigning an Elastic IP Address" on page 13). Updated instructions ("Installing Check Point Software Blades" on page 14).
11 April 2016	Updated Protecting a Web Server (on page 15)
29 February 2016	Updated Routing Traffic Through the Security Gateway (on page 12) and Securely Accessing the Security Gateway (on page 13)
24 November 2015	Updated for R77.30
8 February 2015	Added Pay As You Go (on page 12)
10 November 2014	First release of this document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on vSEC Gateway for Amazon Web Services R77.30 Getting Started Guide.

Contents

Introduction

This document explains how to deploy the Check Point vSEC Gateway in the Amazon Web Services VPC environment. All names and trademarks of Amazon.com and AWS services and technologies belong to Amazon. For more about Amazon names, see http://aws.amazon.com/trademark-guidelines/.

For this document you need basic expertise with:

- Check Point Security Gateway and Security Management Server
- Amazon Web Services VPC and EC2

Glossary

Term	Definition
Amazon EC2	A service provided by Amazon.com that lets users use virtual computers (http://aws.amazon.com/ec2/).
Amazon VPC	Virtual Private Cloud (http://aws.amazon.com/vpc/). A private cloud that exists within the public cloud of Amazon. You can run EC2 instances within a VPC.
Customer VPC network	The address range of the customer VPC.
Private subnet	The part of the customer VPC network that is protected by the Security Gateway and separated by it from the rest of the cloud services and traffic.
Security Gateway subnet	A network subnet that connects the private subnet with the VPC Internet gateway. The R77.30 Security Gateway is the only gateway connected to this subnet. Traffic that leaves the private subnet (Outbound Traffic) is routed to the Security Gateway. Traffic destined for the private subnet (Inbound Traffic) must go through the Security Gateway.

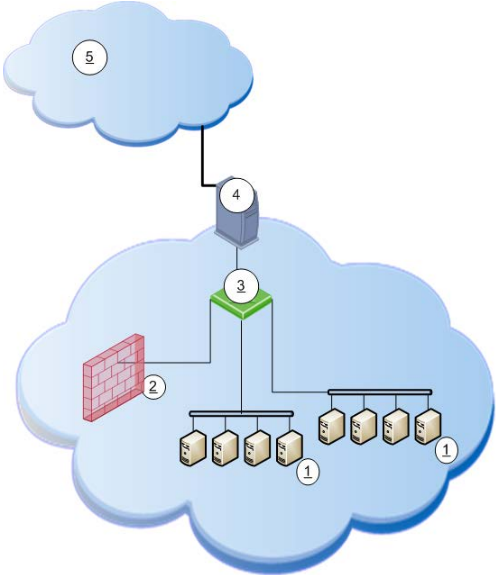
Overview

Use a Virtual Private Cloud (VPC) to keep your cloud IT resources in a private network in the AWS public cloud. The vSEC Gateway secures your information and addresses the security issues you care about.

With this solution, you can:

- Open and maintain multiple VPN tunnels
- Inspect data entering and leaving the VPC private subnet
- Segregate networks in the VPC
- Protect your VPC resources with Check Point Software Blades
- Centrally manage this solution from your existing Check Point management server deployment

Deployment Components



Key		Example IP Address
1	Your AWS instances in private subnets, separated from the rest of the Amazon cloud by the VPC, and protected by the Security Gateway.	10.0.1.0/24
2	vSEC Gateway for VPC, in the Security Gateway Subnet, optionally apply NAT-hide on internal private subnets (1).	10.0.0.10 - instance of Security Gateway 10.0.0.0/28 - Security Gateway Subnet
3	VPC routes outgoing traffic from the Security Gateway Subnet to the VPC Internet gateway.	
4	The Amazon VPC Internet Gateway.	
5	Internet. Traffic to and from the Internet is routed through the Amazon VPC Internet Gateway.	

With the Amazon Web Services VPC you can deploy your gateways to protect your servers and manage them from your Security Management Server. The vSEC Gateway can be set up in a stand-alone configuration as both your gateways and Security Management Server, or be centrally managed from the Check Point Security Management Server. Your gateways can be deployed on-premises or on the AWS VPC. This gives you one policy protecting on-site and cloud computing resources.

If you have a VPC, you can use the vSEC Gateway to secure your assets. If you have a Check Point secured environment, you can meet the unique security challenges of cloud computing while enjoying its advantages.

For quick deployment of your system, use the pre-configured AWS Cloud Formation templates, see sk111013 http://supportcontent.checkpoint.com/solutions?id=sk111013.

For manual configuration of your environment, see ("Setting Up the VPC Environment" on page 8).

Setting Up the VPC Environment

In This Section:

Planning the Network Topology

Plan the VPC network topology before you start configurations.

	Decision	Example IP Address
☑	Select a contiguous private address range for your VPC.	10.0.0.0/16
☑	Allocate a subset of the VPC address range. This will be the Security Gateway subnet.	10.0.0.0/24
☑	Allocate one IP address in the subnet above for the Security Gateway.	10.0.0.10
☑	Decide how many VPC private subnets to create. For each, allocate an IP address range from your VPC address range.	10.0.1.0/24 10.0.2.0/24

Preparing the VPC

This procedure creates your VPC.

To prepare the VPC:

1. Open the AWS Management Console.
2. Select **Services** > **Networking & Content Delivery** > **VPC**.
3. Click **Your VPCs**.
4. Click **Create VPC**.
5. Add a **Name tag**.
6. Add a **CIDR Block**.

   Enter the prefix of the VPC IP address range.
7. Select a **Tenancy**.
8. Click **Yes, Create**.

Creating the SSH Key Pair

To set up the Security Gateway and connect to it remotely, you must have an SSH key pair to make this connection secure.

To create the SSH Key Pair:

1. Open the AWS Management Console.
2. Select **Services** > **EC2**.
3. Select **Key Pairs** > **Create Key Pair**.

   Note - If you already have an SSH key pair, import the public key to the Security Gateway through the Amazon VPC dashboard.

Creating the Amazon VPC Internet Gateway

The Amazon VPC Internet Gateway is the only connection point between the VPC components and the Internet. You must configure an Internet Gateway in your VPC.

To create the Amazon VPC Internet Gateway:

1. Open the AWS Management Console.
2. Select **Services** > **Networking & Content Delivery** > **VPC**.
3. Select **Internet Gateways**.
4. Click **Create Internet Gateway**.

   Note - Use a **Tag** to name the new Internet Gateway.
5. Click **Yes**, **Create**.
6. Right click the newly created Internet Gateway and attach it to your VPC.

Creating the Check Point Security Gateway Subnet

Create a Security Gateway subnet to connect your VPC to the Internet gateway.

To create the Security Gateway subnet:

1. Open the AWS Management Console.
2. Select **Services** > **Networking & Content Delivery** > **VPC**.
3. Select **Subnets**.
4. Click **Create Subnet**.
5. Enter the subnet prefix (for example, 10.0.0.0/24) and create the Security Gateway subnet.

Preparing the Routing Table

The Check Point Security Gateway must be able to route outbound Internet traffic through the Amazon VPC Internet gateway.

To configure the Security Gateway subnet routing table:

1. Open the AWS Management Console.
2. Select **Services** > **Networking & Content Delivery** > **VPC**.

3. Select **Route Tables**.
4. Click **Create Route Table**.
5. Select the VPC. Click **Yes, Create**.
6. Select the **Routes** tab at the bottom of the screen. Click **Edit**.
7. Add a default routing entry:
   - Destination = 0.0.0.0/0
   - Target = the Internet Gateway

   The routing table is then:

   <*VPC* | *network CIDR*> `local`

   <*Default route*> `Internet Gateway`
8. Select the **Subnet Associations** tab. Click **Edit** to associate this routing table with the Security Gateway subnet.

Creating Security Groups

The Check Point Security Gateway can enforce a more sophisticated security policy making the Amazon VPC security groups redundant. Create a permissive VPC security group to make sure that the Amazon VPC security groups do not conflict with the Check Point security policy.

To create a new security group:

1. Open the AWS Management Console.
2. Select **Services** > **Networking & Content Delivery** > **VPC**.
3. Select **Security Groups**.
4. Click **Create Security Group**.
5. Name the new group **PermissiveSecGrp** and select the VPC.
6. In the **Security Groups** list, select **PermissiveSecGrp** and open the **Inbound** tab.
7. Create a new rule that **accepts** all traffic from **any** source address.
8. Add the rule to the security group.

Installing and Configuring the vSEC Gateway

In This Section:

Launching the Security Gateway Instance

The type of instance you launch depends on the license you want to use.

For non GovCloud regions, launch the instance from the AWS Marketplace:

- **Bring Your Own License**

  If you have a Check Point Security Gateway license in the AWS cloud.

- **Pay As You Go**

  If you want to pay for a Check Point Security Gateway only when you need it.

For GovCloud users, use the Amazon Machine Image (AMI).

Bring Your Own License

If you have a license for a Check Point Security Gateway, you can launch an Amazon BYOL image and use your existing Check Point license.

To launch the Security Gateway with BYOL:

1. Go to the **Check Point vSEC Gateway (BYOL)** page https://aws.amazon.com/marketplace/pp/B01CEYZMB6.
2. Click **Continue**.
3. On the **Launch on EC2** page, choose the parameters for your Security Gateway.
4. Click **Launch with 1-click**.

   Note - Immediately after you click, a gateway is created in AWS.
5. Click **Services** > **Compute** > **EC2**.

   Note - You can check the instance and parameters of your Security Gateway from here.

Pay As You Go

Use PAYG if you want to pay for the Check Point vSEC Gateway only when you need it.

To launch the Security Gateway with PAYG:

1. Go to the **Check Point vSEC Gateway (PAYG)** page https://aws.amazon.com/marketplace/pp/B017V7FVDA.
2. Click **Continue**.
3. On the **Launch on EC2** page, the instance has default parameters.

   Note - You can configure your own parameters here.
4. Click **Launch with EC2 Console**.
5. Proceed with the next steps.
6. Click **Launch Instance** to continue with the Instance deployment.

GovCloud Users

To launch an instance of the vSEC Gateway in GovCloud:

1. Select the **Amazon EC2** tab.
2. Click **Launch Instance**.
3. Select the AMI image as listed in sk103403 http://supportcontent.checkpoint.com/solutions?id=sk103403.
4. Select the instance type.
5. Select **Launch Instances Into Your Virtual Private Cloud**.
6. Select the Check Point Security Gateway Subnet ("Deployment Components" on page 7).
7. In **IP Address**, enter the private IP address of the Security Gateway (for example, 10.0.0.10).
8. In **Key Pair**, select the SSH key pair ("Creating the SSH Key Pair" on page 9).
9. Select the security group ("Creating Security Groups" on page 10).
10. Launch the instance.

Routing Traffic through the Security Gateway

To let the Security Gateway route the traffic of your private subnets, make this change.

To route traffic through the Security Gateway:

1. Open the AWS Management Console.
2. Select **Services** > **EC2** > **Instances**.
3. Right-click the vSEC Gateway instance.
4. Select **Networking** > **Change Source/Destination Check**.
5. Click **Yes/Disable**.

Assigning an Elastic IP Address

An Amazon VPC elastic IP address is a public IP address. Every Security Gateway has a private IP address and must also have an elastic IP address. The Amazon VPC Internet Gateway translates the elastic IP address of the Security Gateway to its private IP address.

To assign an elastic IP address to the vSEC Gateway instance:

1. Open the AWS Management Console.
2. Select **Services** > **Networking & Content Delivery** > **VPC** > **Elastic IPs**.
3. Click **Allocate New Address**.
4. Select **VPC** > **Allocate**.
5. Right click the **Elastic IP** > **Associate Address**.
6. Select the Security Gateway instance and click **Yes/Associate**.

Securely Accessing the Security Gateway

In this section, you can access the Security Gateway Instance. Before you install any Software Blades, first connect to the instance using SSH. Connect as the admin user. Compare the public fingerprint from the Security Gateway Instance to the public key from the AWS Console.

Notes:

If you do not compare the fingerprints, you are vulnerable to a man-in-the-middle attack on your SSH session.

It can take up to three minutes after the launch of an instance before the system log is available on the AWS Console.

To get the SSH public key fingerprint of the Security Gateway from the AWS Console:

1. Open the AWS Management Console.
2. Select **Services** > **Compute** > **EC2** > **Instances**.
3. Select the **Instance**.
4. Click **Actions** > **Instance Settings** > **Get System Log**.
5. Search for the list of Host key fingerprints in the log that opens.

To connect to the Security Gateway:

1. Open an SSH client.
2. In the SSH client, connect as admin to the elastic IP address of the Security Gateway using the SSH Private Key ("Creating the SSH Key Pair" on page 9).

   For example, in Linux: `ssh -i MyKey.pem -o FingerprintHash=md5 admin@<`*Your Instance IP*`>`
3. Compare the public key fingerprint with the fingerprint found in the System Log.

   Note - If your SSH client is on Linux or OS X, make sure that the private key is only readable to the current user (`chmod 400`).

Installing Check Point Software Blades

The Host IP address and the default route are set automatically and should not be changed.

To install the Check Point Software Blades:

1. Set the administrator password. Run: `set user admin password`

   At the prompt, enter the administrator password.
2. Run: `save config`
3. Exit the gateway shell. Run: `exit`

   The gateway is now ready for configuration.
4. Using a browser, connect to https://<*elasticIP*>
5. In the Gaia Portal window, log in using the administrator name (admin) and password that you defined earlier.
6. The WebUI shows the **First Time Configuration Wizard**. Click **Next**.
7. In the **Deployment Options** window, click **Next**.
8. In the **Management Connection** window, click **Next**.
9. In **Connection to UserCenter**, manually configure the IPv4 address to: 10.0.1.10, and the subnet mask to: 255.255.255.0. Click **Next**.
10. In **Device Information**, set the Host name. Click **Next**.

    Optional - Set the Domain name and IPv4 addresses for the DNS servers.
11. In **Date and Time Settings**, set the date and time manually. Click **Next**.

    You can also enter the Hostname or IP address of the NTP server.
12. In **Installation Type**, select **Security Gateway** or **Security Management**. Click **Next**.
13. In **Products**, select **Security Gateway** or **Security Management**, or both. Click **Next**.

    a) If you checked **Security Management**, in the Security Management Administrator, set the administrator name and password.

       In the Security Management GUI clients, list the GUI clients that can log into the Security Management Server. Click **Next**.

    b) If you checked **Security Gateway** in **Dynamically Assigned IP**, make sure that **No** is selected. Click **Next**.

       If you selected **Security Gateway**, in Secure Internal Communication (SIC), enter the Activation key. Click **Next**.
14. Click **Finish** > **Yes**.
15. If the **Help Check Point Improve Software Updates window** opens, click **Yes** or **No**.
16. In a few minutes, you can use the WebUI to configure your stand-alone server.

Protecting a Web Server

You can configure the vSEC Gateway to protect servers located in the VPC, in particular to protect web servers from malicious users on the Internet.

Environment requirements

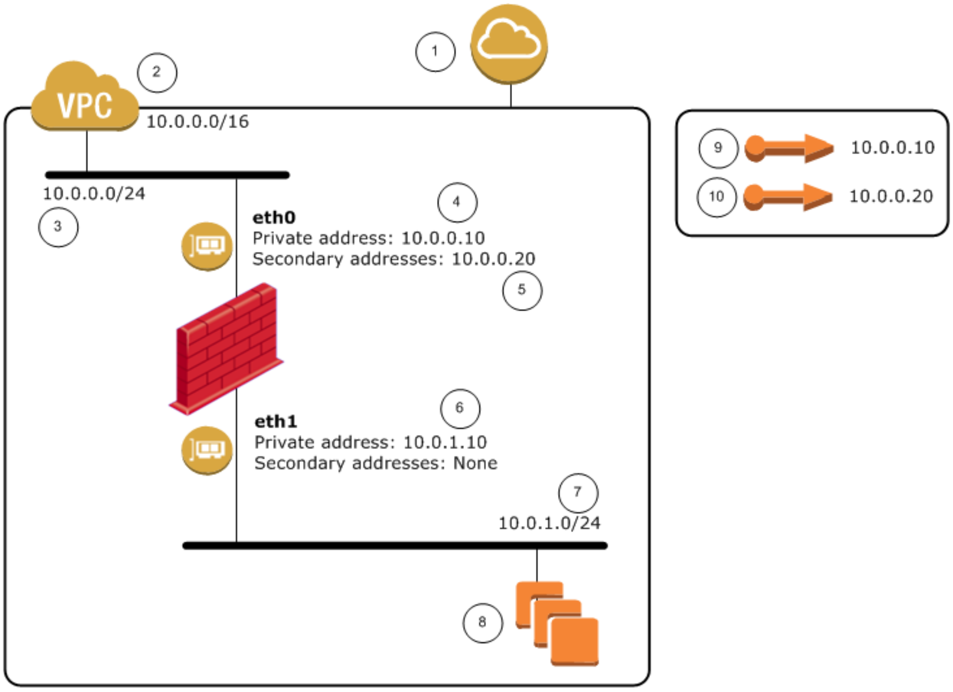
Connectivity - Clients on the Internet can access web servers inside the VPC

Security - Traffic to the web servers passes through the vSEC Gateway

In this configuration, the vSEC Gateway does load balancing of traffic between multiple web servers. Alternatively, you can deploy an internal AWS Elastic Load Balancer (ELB) behind your Check Point Security Gateway. See sk104249 http://supportcontent.checkpoint.com/solutions?id=sk104249.

Example environment

To explain the configuration steps, below is an example environment. Replace the addresses for your environment when you do the steps.


1
2
VPC
10.0.0.0/16
10.0.0.0/24
3
4
eth0
Private address: 10.0.0.10
Secondary addresses: 10.0.0.20
5
6
eth1
Private address: 10.0.1.10
Secondary addresses: None
7
10.0.1.0/24
8
9
10.0.0.10
10
10.0.0.20

Key	Component	Example IP Address
1	Internet Gateway	
2	Amazon Virtual Private Cloud (VPC) CIDR	10.0.0.0/16
3	External subnet	10.0.0.0/24
4	External private address	10.0.0.10
5	Secondary external private address	10.0.0.20

Key	Component	Example IP Address
6	Internal private address	10.0.1.10
7	Internal subnet	10.0.1.0/24
8	Web server instances	
9	Gateway elastic IP address	Allocated by AWS
10	Web servers elastic IP address	Allocated by AWS

To configure the vSEC Gateway:

1. Create a VPC using the VPC CIDR (10.0.0.0/16).
2. Create these subnets inside the VPC:
   - External subnet (10.0.0.0/24)
   - Internal subnet (10.0.1.0/24)

   Note - These subnets must be in the same Availability Zone.
3. Create this routing table and associate it with the external subnet:
   ```
   10.0.0.0/16   Local
   0.0.0.0/0     Internet-GW
   ```
4. Run a vSEC Gateway instance with these interfaces and IP addresses:

Network interface	eth0	eth1
Subnet	10.0.0.0/24 (external subnet)	10.0.1.0/24 (internal subnet)
Private IP address	10.0.0.10	10.0.1.10
Source/Dest check	false	false
Security Group	permissive	permissive

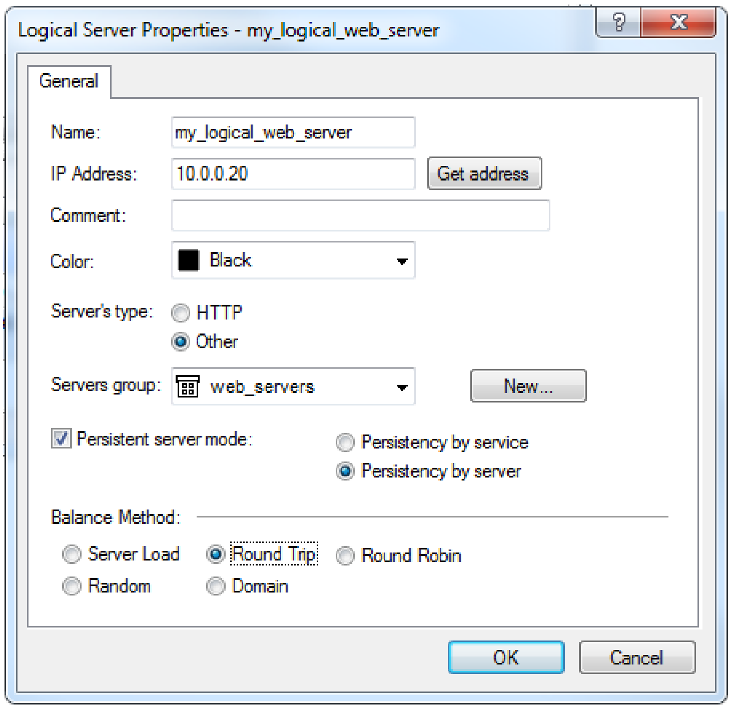
5. Allocate an elastic IP address. Associate it with the vSEC Gateway external private address.

   Use this address to manage the vSEC Gateway.
6. Create this routing table and associate it with the internal subnet:

   `10.0.0.0/16`   `Local`

   `0.0.0.0/0`   The Internal interface (ENI) of the vSEC Gateway
7. Add to `eth0` a secondary IP address: `10.0.0.20`
8. Allocate a different elastic IP address. Associate it with the secondary external private IP address of the vSEC Gateway.

   Use this address to connect to the web servers.
9. Launch multiple web servers in the internal subnet.
10. For each web server, create a network object in SmartDashboard.
11. Create a simple group object with all web servers.
12. Create a logical server object with these properties:
    - **IP Address** = `10.0.0.20`
    - **Server's Type** = **Other** (Make sure the HTTP server type is not supported)
    - **Servers group** = The simple group object you created above



Logical Server Properties - my_logical_web_server

General

Name: my_logical_web_server

IP Address: 10.0.0.20

Comment:

Color: Black

Server's type: ○ HTTP ● Other

Servers group: web_servers

☑ Persistent server mode: ○ Persistency by service ● Persistency by server

Balance Method: ○ Server Load ● Round Trip ○ Round Robin ○ Random ○ Domain

Source	Destination	VPN	Service	Action	Track
Any	`my_logical_web_server`	Any Traffic	http https	Accept	Log

13. Install the policy.

The web servers are accessible from the Internet using the elastic IP address associated with the secondary IP address.

Setting Up a VPN Tunnel

In This Section:

Setting up a VPN Tunnel is optional. You can create a tunnel of encrypted traffic between the Security Gateway in the VPC and a Security Gateway in your local company site.

The procedures in this guide explain how to configure the VPN for these deployments only. For more about defining VPN tunnels with gateways on different sites and different servers, see the *R77.30 Virtual Private Network Administration Guide* http://supportcontent.checkpoint.com/solutions?id=sk104859.

Tunnel between Centrally Managed Gateways

In this deployment, the company's local site Security Management Server centrally manages the Security Gateway at the local site and the Security Gateway protecting the company's private subnets in the Amazon VPC. You can encrypt the data going between the company's local site and the company's private subnets in the Amazon VPC. Create a VPN tunnel between the two Security Gateways.

To create the VPN tunnel:

1. Open SmartDashboard.
2. Create a group network object for the encryption domain behind the VPC Security Gateway. Add the VPC private subnets to the group.
3. Edit the VPC gateway object:
   a) In **General Properties**, click **VPN**.
   b) In **Topology**, in the **VPN Domain** section, click **Manually defined**. Set the encryption domain to the object you created in step 2.
   c) Open **IPSec VPN** > **Link Selection**.
   d) Select **Always Use this IP Address**.
   e) Select **Statically NATed IP**.
   f) Enter the elastic IP address.
4. Create a group network object for the encryption domain behind the company local site gateway. Add the local site internal networks to this object.
5. Edit the company local site Security Gateway object:
   a) In **General Properties**, click **VPN**.
   b) In **Topology**, in the **VPN Domain** section, click **Manually defined** and set the encryption domain to the object you created in step 4.
6. Add the VPC peer gateway object and the VPC gateway object to the **My Intranet** community.
7. Install the policy on the two Security Gateways.

VPN Tunnel with Externally Managed Gateway

In this deployment, two Security Management Servers manage the Security Gateways. There is one Security Management Server at the company's local site, and the other Security Management Server is in the Amazon VPC network. The VPN tunnel must be configured on each of the two Security Management Servers. In each Security Management Server, define the other peer gateway (the other Security Gateway) as an **externally managed gateway**.

Do these steps in the local site Security Management Server:

1. Open SmartDashboard, connecting to the Security Management Server.
2. Create two group network objects for the encryption domain of each of the VPC peers ("Tunnel between Centrally Managed Gateways" on page 18).

3. Edit the Security Gateway object of the company local site:
   a) In **General Properties**, click **VPN**.
   b) In **Topology**, make sure the topology is set.
4. Create an externally managed VPN gateway object for the VPC gateway.
   a) In **General Properties** > **Gateway IP**, enter the elastic IP address of the VPC Security Gateway.
   b) In **Topology**, set the encryption domain of the VPC object.
   c) In **Topology** > **Interface**, set the interface IP address to the private IP address of the VPC Security Gateway.
   d) Open **IPSec VPN** > **Link Selection**.
   e) Select **Always Use this IP Address**.
   f) Select **Statically NATed IP**.
   g) Enter the elastic IP address.
5. Add the VPC peer gateway object and the VPC gateway object to the **My Intranet** community.
6. Install the policy on the two Security Gateways.

Connect to the Security Management Server of the VPC Security Gateway and do the symmetrical settings:

1. Open SmartDashboard, connecting to the Security Management Server at the VPC.
2. Create two group network objects for the encryption domain of each of the VPC peers ("Tunnel between Centrally Managed Gateways" on page 18).
3. Edit the VPC site Security Gateway object:
   a) In **General Properties**, click **VPN**.
   b) In **Topology**, in the **VPN Domain** section, click **Manually defined** and set the encryption domain.
4. Create an externally managed VPN gateway object for the local site gateway.
   a) In **General Properties** > **Gateway IP**, enter the IP address of the local site gateway.
   b) In **Topology**, set the encryption domain of the local site gateway.
5. Add the VPC peer gateway object and the VPC gateway object to the **My Intranet** community.
6. Install the policy on the two Security Gateways.

Inspecting Traffic Between VPC Networks

In This Section:

You can configure the vSEC Gateway to inspect traffic between networks in the VPC, in particular, to protect web applications in the VPC.

The web application environment in the VPC is assumed to have:

- Internet facing web servers in the VPC
- Back-end servers in the VPC (such as Tomcat or database servers)
- Servers inside the corporate network
- Clients inside the corporate network that manage this environment

Environment Requirements

This environment will give you the required connectivity and security.

Connectivity:

- The web servers must have access to the back-end servers.
- The back-end servers must have access to servers inside the corporate network.

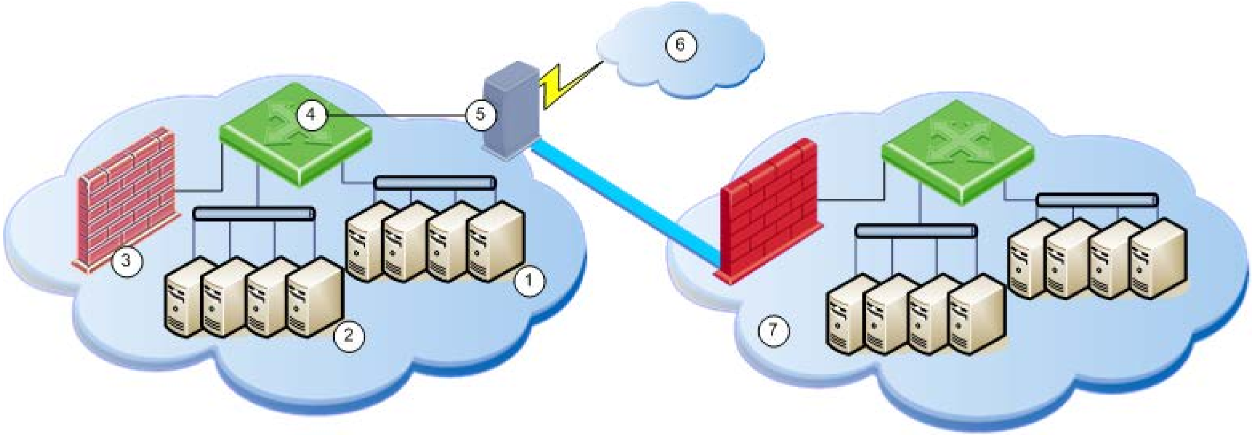
Security:

- Traffic from the web servers to the back-end servers must be inspected and logged by the Check Point gateway.
- Traffic between the VPC and the corporate network must be carried over a VPN.

To make this true, create these subnets in the VPC:

- A public subnet that hosts the web servers
- A private subnet that hosts the back-end servers
- A dedicated subnet that hosts the Check Point Security Gateway

Because routing inside the VPC is direct, use NAT to force traffic between these subnets to pass through the gateway.



Key	
1	Web server subnet
2	Back-end subnet
3	vSEC Gateway subnet
4	VPC routes outgoing traffic from the Security Gateway Subnet to VPC Internet gateway
5	Amazon VPC Internet Gateway
6	Internet
7	Corporate network

Workflow

To best explain the configuration steps, we use this example environment. Make sure to replace the addresses for your environment when you do the steps.

Component / Range	Address
VPC CIDR address range	10.0.0.0/16
Check Point Security Gateway subnet	10.0.0.0/24
Check Point Security Gateway private address	10.0.0.10
Back-end subnet	10.0.1.0/24
Web servers subnet	10.0.2.0/24
Corporate network	200.0.0.0/24
NAT Components	Masking Addresses*
Back-end NAT	172.16.1.0/24
Web servers subnet	172.16.2.0/24

* NAT masking addresses must be outside the VPC CIDR address range.

To protect your Internet facing web applications:

1. Create a VPC using the VPC CIDR address range (10.0.0.0/16).
2. Create these subnets inside the VPC:
   - Check Point Security Gateway subnet (10.0.0.0/24)
   - Back-end subnet (10.0.1.0/24)
   - Web servers subnet (10.0.2.0/24)
3. Create this routing table and associate it with the Check Point Security Gateway subnet:

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Your Internet Gateway

4. Create this routing table and associate it with the back-end subnet:

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Check Point Security Gateway private address (10.0.0.10)

5. Create this routing table and associate it with the web servers subnet:

Destination	Target
10.0.0.0/16	Local
172.16.1.0/24	Check Point Security Gateway private address (10.0.0.10)
0.0.0.0/0	

6. In the Firewall NAT policy add these rules:

Source	Destination	Translated Source	Translated Destination
10.0.2.0/24	172.16.1.0/24	172.16.2.0/24	10.0.1.0/24

   The next steps protect the back-end subnet from direct access from the web servers subnet.

7. Configure the web servers to reach the back-end servers through the Back-end NAT subnet (172.16.1.0/24).
8. Create these network ACLs and associate them to the back-end subnet:

   Inbound:

Port	Protocol	Source	Allow/Deny
All	All	10.0.2.0/24	Deny
All	All	0.0.0.0/0	Allow

Outbound:

Port	Protocol	Destination	Allow/Deny
All	All	10.0.2.0/24	Deny
All	All	0.0.0.0/0	Allow

9. Create these network ACLs and associate them to the web servers subnet:

Inbound:

Port	Protocol	Source	Allow/Deny
All	All	10.0.1.0/24	Deny
All	All	0.0.0.0/0	Allow

Outbound:

Port	Protocol	Destination	Allow/Deny
All	All	10.0.1.0/24	Deny
All	All	0.0.0.0/0	Allow