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=13326

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 February 2013</td>
<td>Corrected the URL for cpvpc.zip archive in the Quick Start section (&quot;Quick Start&quot; on page 7)</td>
</tr>
<tr>
<td>02 February 2012</td>
<td>Added Check Point Security Gateway Virtual Appliance Configuration Tool (&quot;Quick Start&quot; on page 7)</td>
</tr>
<tr>
<td>04 January 2012</td>
<td>Added AMI for Sao Paulo</td>
</tr>
<tr>
<td>05 November 2011</td>
<td>Added configuration steps to protect Web applications that face the Internet (&quot;Inspecting Traffic Between VPC Networks&quot; on page 19)</td>
</tr>
<tr>
<td>07 November 2011</td>
<td>Added available AMI names (&quot;Launching the Security Gateway Instance&quot; on page 12)</td>
</tr>
<tr>
<td>14 June 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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 Security Gateway Virtual Appliance R75 for Amazon Web Services VPC Getting Started Guide).
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Glossary</td>
<td>5</td>
</tr>
<tr>
<td>Overview</td>
<td>6</td>
</tr>
<tr>
<td>Deployment Components</td>
<td>6</td>
</tr>
<tr>
<td>Security Gateway Deployment</td>
<td>7</td>
</tr>
<tr>
<td>Quick Start</td>
<td>7</td>
</tr>
<tr>
<td>Setting Up the VPC Environment</td>
<td>9</td>
</tr>
<tr>
<td>Planning the Network Topology</td>
<td>9</td>
</tr>
<tr>
<td>Preparing the VPC</td>
<td>9</td>
</tr>
<tr>
<td>Creating the SSH Key Pair</td>
<td>9</td>
</tr>
<tr>
<td>Creating the Amazon VPC Internet Gateway</td>
<td>10</td>
</tr>
<tr>
<td>Creating the Check Point Security Gateway Subnet</td>
<td>10</td>
</tr>
<tr>
<td>Preparing the Routing Table</td>
<td>10</td>
</tr>
<tr>
<td>Creating Security Groups</td>
<td>11</td>
</tr>
<tr>
<td>Installing and Configuring Check Point Security Gateway Virtual Appliance</td>
<td>12</td>
</tr>
<tr>
<td>Launching the Security Gateway Instance</td>
<td>12</td>
</tr>
<tr>
<td>Routing Traffic Through the Security Gateway</td>
<td>13</td>
</tr>
<tr>
<td>Assigning an Elastic IP Address</td>
<td>13</td>
</tr>
<tr>
<td>Securely Accessing the Security Gateway</td>
<td>13</td>
</tr>
<tr>
<td>Installing Check Point Software Blades</td>
<td>14</td>
</tr>
<tr>
<td>Finalizing the VPC Environment Setup</td>
<td>15</td>
</tr>
<tr>
<td>Creating Private Subnets</td>
<td>15</td>
</tr>
<tr>
<td>Preparing Private Subnet Routing Tables</td>
<td>15</td>
</tr>
<tr>
<td>Configuring Check Point Objects</td>
<td>16</td>
</tr>
<tr>
<td>Stand-Alone Deployment</td>
<td>16</td>
</tr>
<tr>
<td>Distributed Security Gateway Deployment</td>
<td>16</td>
</tr>
<tr>
<td>Setting Up a VPN Tunnel</td>
<td>17</td>
</tr>
<tr>
<td>Tunnel between Centrally Managed Gateways</td>
<td>17</td>
</tr>
<tr>
<td>VPN Tunnel with Externally Managed Gateway</td>
<td>18</td>
</tr>
<tr>
<td>Inspecting Traffic Between VPC Networks</td>
<td>19</td>
</tr>
<tr>
<td>Environment Requirements</td>
<td>19</td>
</tr>
<tr>
<td>Workflow</td>
<td>20</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

In This Chapter
- Glossary 5
- Overview 6
- Deployment Components 6
- Security Gateway Deployment 7
- Quick Start 7

Note - This document explains how to deploy the Check Point Security Gateway virtual appliance 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/.

This document assumes that you have basic expertise with:
- Check Point Security Gateway and Security Management Server
- Amazon Web Services VPC and EC2

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EC2</td>
<td>A service provided by Amazon.com that lets users use virtual computers (<a href="http://aws.amazon.com/ec2/">http://aws.amazon.com/ec2/</a>).</td>
</tr>
<tr>
<td>Amazon VPC</td>
<td>Virtual Private Cloud (<a href="http://aws.amazon.com/vpc/">http://aws.amazon.com/vpc/</a>). A private cloud that exists within the public cloud of Amazon. You can run EC2 instances within a VPC.</td>
</tr>
<tr>
<td>Customer VPC network</td>
<td>The address range of the customer VPC.</td>
</tr>
<tr>
<td>Private subnet</td>
<td>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.</td>
</tr>
<tr>
<td>Security Gateway subnet</td>
<td>A network subnet that connects the private subnet with the VPC Internet gateway. The R75 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.</td>
</tr>
</tbody>
</table>
Overview

The cloud technology lets a company use computing resources from professional IT vendors. It takes advantage of externally managed IT resources with a flexible capacity using a pay-as-you-go model. Amazon Web Services (AWS) provides cloud computing services which let companies launch a wide range of servers and services. The Virtual Private Network (VPC) lets companies keep their cloud IT resources in a private network, in the AWS public cloud.

Having part of your IT resources in a public cloud can introduce security issues. Check Point Security Gateway Virtual Appliance for Amazon Web Services VPC helps you meet the security challenges of the public cloud. With this solution, you can:

- Establish and maintain multiple VPN tunnels between your VPC and your corporate networks.
- 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

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Example IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Your AWS instances in private subnets, separated from the rest of the Amazon cloud by the VPC, and protected by the Security Gateway.</td>
<td>10.0.1.0/24</td>
</tr>
<tr>
<td>2</td>
<td>Check Point Security Gateway Virtual Appliance for VPC, in the Security Gateway Subnet, optionally apply NAT-hide on internal private subnets (1).</td>
<td>10.0.0.10 - instance of Security Gateway Subnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.0.0.0/28 - Security Gateway Subnet</td>
</tr>
<tr>
<td>3</td>
<td>VPC routes outgoing traffic from the Security Gateway Subnet to the VPC Internet gateway.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>The Amazon VPC Internet Gateway.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Internet. Traffic to and from the Internet is routed through the Amazon VPC Internet Gateway.</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Security Gateway Deployment

A company using Amazon Web Services VPC can run servers at the virtual environment and on the local premises. An administrator uses a local Security Management Server to manage the Security Gateways running in the company site and in the AWS virtual environment. This gives you one policy protecting on-site and cloud computing resources.

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

Limitations

There are currently routing limitations in the Amazon VPC environment. A host in a private subnet with a public IP address cannot have its traffic routed through the Check Point Security Gateway.

Centrally Managed or Stand-Alone Deployments:

The Check Point Security Gateway Virtual Appliance running in the Amazon Web Services VPC can be deployed in stand-alone configuration (Security Gateway and Security Management Server) or be centrally managed from an on-premises Check Point Security Management Server.

Quick Start

The Check Point Security Gateway Virtual Appliance for AWS Configuration Tool creates a VPC with a private subnet and a Virtual Appliance with an elastic IP address in the new environment. It also creates an Internet gateway, a security group for the Virtual Appliance, and a route table associated with the private subnet. Then it starts the Virtual Appliance.

You cannot use this tool if you want to add a Check Point Security Gateway Virtual Appliance to an existing VPC. If you already have a VPC, do the steps of this guide, starting with preparation of the environment ("Setting Up the VPC Environment" on page 9).

Prerequisites:

- Make sure you have your AWS Access Key and Secret Key. You can find them on the AWS web console > AWS Security Credentials page > Access Keys tab.
- This tool is for Windows only.

To use this tool:

1. Download and extract the tool: cpvpc.zip (http://supportcontent.checkpoint.com/file_download?id=13375)
2. Run: cpvpc.exe
3. Enter your AWS Access Key and Secret Key (http://aws.amazon.com/iam/).
4. See the default settings that will be used to create the environment.
   - To accept these settings, enter: A
   - To change these settings, enter: M
     If you choose M, configure the settings (see the next procedure) and then return to this procedure.
      The tool starts to create the VPC. It shows a notification of success, with the configuration details. It shows how to access your new Check Point Security Gateway Virtual Appliance.
5. Access the Virtual Appliance and configure Check Point objects ("Configuring Check Point Objects" on page 16).

If you choose M when you start the tool, configure the changed settings.

To use the tool with modified settings:

1. Select an AWS region for the VPC.
2. Enter the VPC CIDR ("Preparing the VPC" on page 9).
5. Select an address range for the Private subnet ("Creating Private Subnets" on page 15).
7. Select an SSH key pair from the key pairs you have in your region, or type 0, to create a new one ("Launching the Security Gateway Instance" on page 12).
   If you create a new key, the private key shows on-screen. Copy it to a file and save it.
8. Configure the Elastic IP address for the Security Gateway instance. Do one of these:
   • Select an Elastic IP addresses in your region.
   • Enter 0 to create a new one ("Assigning an Elastic IP Address" on page 13).
Chapter 2

Setting Up the VPC Environment

In This Chapter

- Planning the Network Topology 9
- Preparing the VPC 9
- Creating the SSH Key Pair 9
- Creating the Amazon VPC Internet Gateway 10
- Creating the Check Point Security Gateway Subnet 10
- Preparing the Routing Table 10
- Creating Security Groups 11

Planning the Network Topology

Plan the VPC network topology before you start configurations.

<table>
<thead>
<tr>
<th>Decision</th>
<th>Example IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Select a contiguous private address range for your VPC.</td>
<td>10.0.0.0/16</td>
</tr>
<tr>
<td>✓ Allocate a subset of the VPC address range. This will be the Security Gateway Subnet. This can be as small as a /28 subnet block.</td>
<td>10.0.0.0/28</td>
</tr>
<tr>
<td>✓ Allocate one IP address in the subnet above, for the Security Gateway.</td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>✓ Decide how many VPC private subnets to create. For each, allocate an IP address range from your VPC address range.</td>
<td>10.0.1.0/24 10.0.2.0/24</td>
</tr>
</tbody>
</table>

Preparing the VPC

This first procedure creates your VPC and a secure connection to your VPC instances with SSH key pairs.

To prepare the VPC:
1. Open the AWS Management Console > Amazon VPC tab.
2. Click Your VPC > Create VPC.
3. In the CIDR Block window, enter the prefix of the VPC IP address range.

Alternative CLI:

PROMPT> ec2-create-vpc 10.0.0.0/16
VPC vpc-1a2b3c4d pending 10.0.0.0/16 default

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. If you already have an SSH key pair, import the public key to the Security Gateway through the Amazon VPC dashboard.
• To create the SSH Key Pair, click **Key Pairs > Create Key Pair**.

**Alternative CLI:**

```bash
PROMPT> ec2-create-keypair MyKey
```

---

**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 configure a new Internet Gateway in the VPC:**
1. Open the AWS Management Console > **Amazon VPC** tab.
2. Click **Your VPC**.
3. In the **VPC** area, click **Internet Gateway**.
4. Attach the newly created Internet Gateway to your VPC.

**Alternative CLI:**

```bash
PROMPT> ec2-create-internet-gateway
INTERNETGATEWAY igw-c0a643a9
```

---

**Creating the Check Point Security Gateway Subnet**

Create a subnet in the VPC to be the Security Gateway Subnet, containing only the Security Gateway.

**To create the Security Gateway subnet:**
1. Open the AWS Management Console > **Amazon VPC** tab.
2. Select the **Subnets** menu.
3. Click **Create Subnet**.
4. Enter the subnet prefix (for example, 10.0.0.0/28) and create the Security Gateway Subnet.

**Alternative CLI:**

```bash
PROMPT> ec2-create-subnet -c vpc-1a2b3c4d -i 10.0.0.0/28
SUBNET subnet-9c4a7b6c pending vpc-1a2b3c4d 10.0.0.0/28 250 us-east-1a
```

---

**Preparing the Routing Table**

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

Configure the VPC routing tables.

**To configure the Security Gateway Subnet routing table:**
1. In the **VPC** section, click **Route Tables**.
2. Click **Create Route Table**.
3. Select the current VPC.
4. 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
```

5. Open the **Associations** tab.
6. 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. This procedure explains how to 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 Security Groups menu.
2. Click Create Security Group.
3. Name the new group PermissiveSecGrp, and select the VPC.
4. In the Security Groups list, select PermissiveSecGrp and open the Inbound tab.
5. Create a new rule that accepts all traffic from any source address.
6. Add the rule to the security group.

Alternative CLI:

PROMPT> ec2-create-route-table vpc-1a2b3c4d
ROUTETABLE rtb-6aa34603 vpc-1a2b3c4d
ROUTE local active 10.0.0.0/16

PROMPT> ec2-create-route rtb-6aa34603 -r 0.0.0.0/0 -g igw-c0a643a9
ROUTE igw-c0a643a9 0.0.0.0/0

PROMPT> ec2-associate-route-table rtb-6aa34603 -s subnet-9d4a7b6c
ASSOCIATION rtbassoc-61a34608 rtb-6aa34603 subnet-9d4a7b6c

PROMPT> ec2-create-group security -d 'PermissiveSecGrp' -c vpc-1a2b3c4d
GROUP sg-4def22a5 security PermissiveSecGrp

PROMPT> ec2-authorize sg-4def22a5 -P all -s 0.0.0.0/0
GROUP sg-4def22a5
PERMISSION ALLOWS All FROM CIDR 0.0.0.0/0 ingress
Chapter 3

Installing and Configuring Check Point Security Gateway Virtual Appliance

In This Chapter

- Launching the Security Gateway Instance 12
- Routing Traffic Through the Security Gateway 13
- Assigning an Elastic IP Address 13
- Securely Accessing the Security Gateway 13
- Installing Check Point Software Blades 14

Launching the Security Gateway Instance

Currently, the available AMI names for Check Point Security Gateway Virtual Appliance are:

<table>
<thead>
<tr>
<th>Region</th>
<th>AMI Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>US-East (Virginia)</td>
<td>ami-5e39c737</td>
<td>Check Point Virtual Appliance R75</td>
</tr>
<tr>
<td>US-West (Oregon)</td>
<td>ami-acf17c9c</td>
<td>Check Point Virtual Appliance R75</td>
</tr>
<tr>
<td>US-West (N. California)</td>
<td>ami-9de2b1d8</td>
<td>Check Point Virtual Appliance R75</td>
</tr>
<tr>
<td>EU-West (Ireland)</td>
<td>ami-a692a2d2</td>
<td>Check Point Virtual Appliance R75</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ami-246e1476</td>
<td>Check Point Virtual Appliance R75</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ami-8c0bbf8d</td>
<td>Check Point Virtual Appliance R75</td>
</tr>
<tr>
<td>South America (Sao Paulo)</td>
<td>ami-a424fbb9</td>
<td>Check Point Virtual Appliance R75</td>
</tr>
</tbody>
</table>

To launch a new instance of Check Point Security Gateway Virtual Appliance:

1. Select the Amazon EC2 tab.
2. Click Launch Instance.
3. Select the Check Point AMI from the above table, according to our VPC region.
4. Select the instance type: Small for 1 core, or High-CPU Medium for 2 cores.
   **Note** - the "Micro" instance type is not supported.
5. Select Launch Instances Into Your Virtual Private Cloud.
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).
10. Launch the instance.
Routing Traffic Through the Security Gateway

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

**To route traffic through the Security Gateway:**
1. Open EC2 > instance list.
2. Right-click the Check Point Security Gateway Virtual Appliance instance.

**Alternative CLI:**

```
PROMPT> ec2-modify-instance-attribute i-770af21c --source-dest-check false
```

Assigning an Elastic IP Address

An Amazon VPC elastic IP address is a public IP address. The 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 Check Point Security Gateway Virtual Appliance instance:**
1. On the Amazon VPC tab, open Elastic IPs.
2. Click Allocate New Address.
3. From EIP used in, select VPC and then click Yes, Allocate.
4. Select the IP address in the list and click Associate Address.
5. Select the Security Gateway instance and click Yes, Associate.

**Alternative CLI:**

```
PROMPT> ec2-allocate-address -d vpc
ADDRESS 198.51.100.1 vpc eipalloc-5723d13e
```
```
PROMPT> ec2-associate-address -a eipalloc-5723d13e -i i-770af21c
ADDRESS i-770af21c eipalloc-5723d13e eipassoc-fc5ca095
```

Securely Accessing the Security Gateway

In this section, you access the Security Gateway instance. Before you can install Software Blades, you must 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.

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

**Note** - 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 EC2 Instances.
2. Right-click the Check Point Security Gateway Virtual Appliance instance and select Get System Log.
3. Take note of the fingerprint string.
To connect to the Security Gateway:

1. Open an SSH client.
2. In the SSH client, connect using the SSH Private Key ("Creating the SSH Key Pair" on page 9), as admin, to the elastic IP address of the Security Gateway.
   - For example, in Linux: `ssh -i MyKey.pem admin@<elasticIP>
3. Compare the public key fingerprint with the string sent by the Security Gateway.

Installing Check Point Software Blades

- **Note** - The host IP address and the default route are set automatically and should not be changed.

1. Run: `sysconfig`
2. Set the network configurations. For example: DNS servers, NTP servers, and so on.
3. At the **Products List**, select the products to install (for example, the Security Gateway).
4. Reboot.
Chapter 4

Finalizing the VPC Environment Setup

In This Chapter

Creating Private Subnets 15
Preparing Private Subnet Routing Tables 15
Configuring Check Point Objects 16

Creating Private Subnets

After you set up the Security Gateway, your VPC is protected. At this time, you can securely define and populate the private subnets.

⚠️ Important - Make sure that you do not assign an elastic IP address to an instance in these private subnets. If you do, you will bypass the Check Point protection.

To create a private subnet:
1. In the Amazon VPC tab, select Subnets menu > Create New Subnet.
2. Enter the subnet prefix (for example, 10.0.1.0/24).

Alternative CLI:
PROMPT> ec2-create-subnet -c vpc-1a2b3c4d -i 10.0.1.0/24
SUBNET subnet-9d4a7615 pending vpc-1a2b3c4d 10.0.1.0/24 250 us-east-1a

Preparing Private Subnet Routing Tables

If you have multiple private subnets, configure the routing tables to let traffic move between them.

⚠️ Note - The Security Gateway can only inspect traffic going to the Internet or through VPN.

To configure private subnet routing tables:
1. In the VPC section, open the Route Tables menu.
2. Create a new routing table.
3. Select the current VPC.
4. Add a default routing entry in the new table.
   - Destination = 0.0.0.0/0
   - Target = the Security Gateway instance

The routing table is then:

```
<VPC network CIDR>   <Default route>  
local               Check Point Security Gateway Virtual Appliance instance ID
```
5. Open the **Associations** tab.
6. Associate this routing table with the private subnets.
7. Launch host instances in the private subnets.

**Alternative CLI:**

```bash
PROMPT> ec2-create-route-table vpc-1a2b3c4d
ROUTETABLE  rtb-6aa34615  vpc-1a2b3c4d
ROUTE          local  active  10.0.0.0/16
```

```bash
PROMPT> ec2-create-route rtb-6aa34615 -r 0.0.0.0/0 -g i-770af21c
ROUTE  i-770af21c  0.0.0.0/0
```

```bash
PROMPT> ec2-associate-route-table rtb-6aa34603 -s subnet-9d4a7b6c
ASSOCIATION rtbassoc-61a34608  rtb-6aa34615  subnet-9d4a7b6c
```

### Configuring Check Point Objects

Use these guidelines to make sure that Check Point objects operate correctly in the VPC:

- Instances in the VPC private subnets can only use private IP addresses. To access the Internet, you must NAT-hid them behind the IP address of the Security Gateway.
- The Security Gateway IP address is static-NATted by the Amazon infrastructure to the elastic IP address. In SmartDashboard, use the elastic IP address as the primary address of the Security Gateway.
- The Security Gateway has only one network interface. You cannot use Anti-Spoofing. Ignore the warning about this when you install the security policy, or edit the gateway object. Anti-Spoofing is handled at the perimeter by Amazon VPC.

#### Stand-Alone Deployment

If you installed a Security Gateway and a Security Management Server in the VPC, use these steps to configure the gateway.

1. Open SmartDashboard.
2. Connect to the Security Gateway, by its elastic IP address, as the server address.
3. In the **Network Objects** tree, right-click the gateway object and select **Convert to Gateway**.
4. Create a network object for each of the private subnets:
   a) Define the VPC private subnet range.
   b) Use NAT to hide the range behind the Security Gateway and select the Security Gateway.

#### Distributed Security Gateway Deployment

If the VPC Security Gateway is managed by a Security Management Server in a distributed environment, use these steps to configure the Security Gateway.

1. Open SmartDashboard.
2. Connect to the local Security Management Server.
3. Create a new gateway object.
4. Set the IP address of the new gateway object to the elastic IP address of the Security Gateway in the VPC.
5. Initialize secure internal communications (SIC) and get the interfaces.
6. Create a network object for each private subnet:
   a) Define the VPC private subnet range.
   b) Click the **NAT** tab and select **Hide behind the gateway** and select the Security Gateway.
Chapter 5

Setting Up a VPN Tunnel

In This Chapter

| Tunnel between Centrally Managed Gateways | 17 |
| VPN Tunnel with Externally Managed Gateway | 18 |

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

These procedures 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 R75 Virtual Private Network Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11675).

Tunnel between Centrally Managed Gateways

In this deployment, the company’s local site Security Management Server centrally manages the Security Gateway at the company 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 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:**

2. Define the encryption domains for each of the VPN peers ("Tunnel between Centrally Managed Gateways" on page 17).
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.

**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. Define the encryption domains for each of the VPN peers ("Tunnel between Centrally Managed Gateways" on page 17).
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.
Chapter 6

Inspecting Traffic Between VPC Networks

In This Chapter

Environment Requirements 19
Workflow 20

You can configure Check Point Security Gateway Virtual Appliance 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  Check Point Security Gateway Virtual Appliance 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 to reflect your environment when you do the steps.

<table>
<thead>
<tr>
<th>Component / Range</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC CIDR address range</td>
<td>10.0.0.0/16</td>
</tr>
<tr>
<td>Check Point Security Gateway subnet</td>
<td>10.0.0.0/24</td>
</tr>
<tr>
<td>Check Point Security Gateway private address</td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>Back-end subnet</td>
<td>10.0.1.0/24</td>
</tr>
<tr>
<td>Web servers subnet</td>
<td>10.0.2.0/24</td>
</tr>
<tr>
<td>Corporate network</td>
<td>200.0.0.0/24</td>
</tr>
</tbody>
</table>

**NAT Components**

**Masking Addresses**

<table>
<thead>
<tr>
<th>NAT Components</th>
<th>Masking Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back-end NAT</td>
<td>172.16.1.0/24</td>
</tr>
<tr>
<td>Web servers subnet</td>
<td>172.16.2.0/24</td>
</tr>
</tbody>
</table>

* 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:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>Internet-GW</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>Check Point Security Gateway private address (10.0.0.10)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>172.16.1.0/24</td>
<td>Check Point Security Gateway private address (10.0.0.10)</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td></td>
</tr>
</tbody>
</table>

6. In the Firewall NAT policy add these rules:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Translated Source</th>
<th>Translated Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.2.0/24</td>
<td>172.16.1.0/24</td>
<td>172.16.2.0/24</td>
<td>10.0.1.0/24</td>
</tr>
</tbody>
</table>

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:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Allow/Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
<td>10.0.2.0/24</td>
<td>Deny</td>
</tr>
<tr>
<td>All</td>
<td>All</td>
<td>0.0.0.0/0</td>
<td>Allow</td>
</tr>
</tbody>
</table>

   **Outbound:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Destination</th>
<th>Allow/Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
<td>10.0.2.0/24</td>
<td>Deny</td>
</tr>
<tr>
<td>All</td>
<td>All</td>
<td>0.0.0.0/0</td>
<td>Allow</td>
</tr>
</tbody>
</table>
9. Create these network ACLs and associate them to the Web servers subnet:

**Inbound:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Allow/Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
<td>10.0.1.0/24</td>
<td>Deny</td>
</tr>
<tr>
<td>All</td>
<td>All</td>
<td>0.0.0.0/0</td>
<td>Allow</td>
</tr>
</tbody>
</table>

**Outbound:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Destination</th>
<th>Allow/Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
<td>10.0.1.0/24</td>
<td>Deny</td>
</tr>
<tr>
<td>All</td>
<td>All</td>
<td>0.0.0.0/0</td>
<td>Allow</td>
</tr>
</tbody>
</table>