IBM Cloud - VPC

Single VPC Catalog Full Deployment
Contents

Overview ............................................................................................................................... 3
Single VPC Topology ......................................................................................................... 4
Installing Full Deployment of Check Point CloudGuard Gateway into Existing VPC ........... 5
Assign a Floating IP to eth0 of the Gateway .................................................................... 11
Configure the Check Point CloudGuard Gateway ............................................................. 13
Verify Gateway Configuration & Advanced Settings ....................................................... 16
Installing Full Deployment of Check Point CloudGuard Management Server ................ 18
Assign a Floating IP to eth0 of the Management Server ............................................... 24
Configure the Check Point CloudGuard Management Server ........................................ 26
Configure Routing .......................................................................................................... 42
Overview

This document provides instructions to install a full deployment of a Check Point CloudGuard Security Gateway and a Check Point CloudGuard Security Management Server within the IBM Cloud Virtual Private Cloud (VPC) infrastructure. This document will focus on deploying a Gateway into a previously created VPC consisting of three subnets (External, Internal and Management).
This document will cover creating Check Point Gateway and Management deployments.

**NOTE:** A VPC, as well as Internal, External and Management Subnets must exist in order to deploy Gateway. For the Management deployment, the VPC and Management Subnet must exist in order to deploy.

**NOTE:** Application and Database Subnets, as well as Route Tables and Check Point Gaia OS Routes are shown only as an example of one potential deployment architecture. Cascading subnets off the Internal Subnet or External Subnet allow for unlimited scalability.

**NOTE:** It is suggested that workloads i.e. Database subnet should NOT live in Internal, External and Management subnets only the Check Point vNic so the subnet masks can be very small.
Installing Full Deployment of Check Point CloudGuard Gateway into Existing VPC

1. Within the IBM Cloud portal, select **Catalog**.

2. Select **Check Point CloudGuard IaaS** in the catalogue drop-down menu.
3. Type **Check Point** in search field, and hit **Enter**.

4. Select the desired **Full Deployment** option. Example: *CloudGuard IaaS Security Gateway*
5. Review the information within the **Readme** tab to understand the various deployment parameters.

6. Enter the following initial information:

   a. **Name**: Give your workspace a unique name that you can easily recognize.
   b. **Resource Group**: Enter the desired Resource group for your workspace.
   c. **Tags**: Enter any tags, if required.

**NOTE:** It is recommended to acquire all of the deployment parameter values and enter them in notepad to easily cut and paste. See the **Readme** tab for specific commands to run within the IBM Cloud shell in order to acquire specific parameters.

Example: VPC\_Region = `ibmcloud is regions`

**NOTE:** “Subnets” are the only fields that require ID numbers.

**NOTE:** “VNF\_Security\_group” must be a unique name as it is created during deployment.

**NOTE:** To initiate the IBM Cloud shell select the following **icon**:
7. Enter values for the **Parameters** that do not have default values assigned. See examples below for additional information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>External_Subnet_ID</td>
<td>The ID of the subnet that exists in front of the Check Point Security Gateway that will be provisioned (the 'external' network).</td>
<td>Enter External_Subnet_ID</td>
</tr>
<tr>
<td>Internal_Subnet_ID</td>
<td>The ID of the subnet that exists behind the Check Point Security Gateway that will be provisioned (the 'internal' network).</td>
<td>Enter Internal_Subnet_ID</td>
</tr>
<tr>
<td>Management_Subnet_ID</td>
<td>The ID of the Check Point management subnet.</td>
<td>Enter Management_Subnet_ID</td>
</tr>
<tr>
<td>Resource_Group</td>
<td>The resource group that will be used when provisioning the Check Point VSI. If left unspecified, the account's default resource group will be used.</td>
<td>Enter Resource_Group</td>
</tr>
<tr>
<td>SSH_Key</td>
<td>The public SSH Key name that will be used when provisioning the Check Point VSI.</td>
<td>Enter SSH_Key</td>
</tr>
<tr>
<td>VNF_Security_Group</td>
<td>The name of the new security group assigned to the Check Point VSI.</td>
<td>Enter VNF_Security_Group</td>
</tr>
<tr>
<td>VPC_Name</td>
<td>The VPC where the Check Point VSI will be provisioned.</td>
<td>Enter VPC_Name</td>
</tr>
<tr>
<td>VPC_Raigon</td>
<td>The region where the VPC, networks, and Check Point VSI will be provisioned.</td>
<td>Enter VPC_Raigon</td>
</tr>
</tbody>
</table>

Information required: Set the required deployment values to install Check Point CloudGuard IaaS Security Gateway.
## Examples of Parameter Values

**Parameters without default values**
Enter the required value for each parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>External_Subnet_ID</code></td>
<td>The ID of the subnet that exists in front of the Check Point Security Gateway that will be provisioned (the 'external' network).</td>
<td><code>0737-18d49bb19-8d0a-4385-99ad</code></td>
</tr>
<tr>
<td><code>Internal_Subnet_ID</code></td>
<td>The ID of the subnet that exists behind the Check Point Security Gateway that will be provisioned (the 'internal' network).</td>
<td><code>0737-fb28be4d-89f8-4040-a650-7</code></td>
</tr>
<tr>
<td><code>Management_Subnet_ID</code></td>
<td>The ID of the Check Point management subnet.</td>
<td><code>0737-7d9a3bb2-6ecb-4a37-bd30</code></td>
</tr>
<tr>
<td><code>Resource_Group</code></td>
<td>The resource group that will be used when provisioning the Check Point VSI. If left unspecified, the account's default resource group will be used.</td>
<td>Default</td>
</tr>
<tr>
<td><code>SSH_Key</code></td>
<td>The public SSH Key name that will be used when provisioning the Check Point VSI.</td>
<td><code>development</code></td>
</tr>
<tr>
<td><code>VNF_Security_Group</code></td>
<td>The name of the new security group assigned to the Check Point VSI.</td>
<td><code>fd-sg-bn-2</code></td>
</tr>
<tr>
<td><code>VPC_Name</code></td>
<td>The VPC where the Check Point VSI will be provisioned.</td>
<td><code>full-deployment-vpc-bn</code></td>
</tr>
</tbody>
</table>
8. Enter Parameters with default values (pre-set but can be modified).
   a. **CP_Version** – Enter desired version.
   b. **VNF_Profile** – Value is set by default (Compute Profiles are recommended).
   c. **VNF_License** – Optional.

9. Click **Install**.
Assign a Floating IP to eth0 of the Gateway

**NOTE:** In our example, we are assigning a floating IP to eth0 as we will be managing the gateway remotely over the public Internet.

1. Select **Floating IP** within the **Network** sub-heading of the **VPC Infrastructure** main menu.

2. In the **Floating IPs for VPC** page, within the **Region** drop-down menu, ensure that the correct region that was entered earlier is selected.

3. Click **Create**.

4. Enter the following details with the **Reserve a Floating IP** page to assign a floating IP address to the VSI.

   a. **Floating IP Name** - Provide a name for the floating IP address.
   b. **Resource Group** - Select the appropriate group.
   c. **Location** - Select the location (region) of the gateway that was created in the previous step.
   d. **Instance to Bind** - Select the gateway that was created in the previous step.
   e. **Network Interface** - can only be assigned to eth0
   f. **Tags** - Add any tags if required.

5. Click **Reserve IP**.
Reserve a floating IP

Reserve a floating IP and bind it to the network interface of a virtual server instance to allow public traffic to the instance.

Floating IP name

- cp-gw-f-ip

Resource group

You can't change the resource group after the floating IP is created.

Learn about resource groups

- Default

View all resource groups

Location

- Dallas
  - Dallas 3

- Frankfurt
  - Frankfurt 3

Instance to bind

- checkpoint-gw

Network Interface

- eth0

Tags

Examples: env:dev, version-1

Get sample API call

Estimated monthly

- United States
  - $1.00

Cancel  Reserve IP
Configure the Check Point CloudGuard Gateway

1. Go to https://<<Floating IP Assigned to Gateway>>

2. Select Advanced.

3. Select Proceed To.
1. Enter username **admin**.

2. Enter password **admin**.

3. Click **Login**.

4. Enter the following information as part of the Check Point CloudGuard Gateway initial configuration:
   a. **Authentication** - Provide a new Gaia OS password for the **admin** account.
   b. **SIC** - Enter a SIC activation key.
   c. **Network Configuration** - Leave the default settings.
   d. **Configurations** - Check if this gateway will be part of a high-availability cluster.

5. Select **Go!**
NOTE: You have finished the Blink image configuration/initial gateway configuration.

6. Select **OK**.
Verify Gateway Configuration & Advanced Settings

1. Enter username **admin**.

2. Enter the new password for the **admin** account that was set in the previous step.

3. Click **Login**.
Installing Full Deployment of Check Point CloudGuard Management Server

1. Within the IBM Cloud Portal, select **Catalog**.

![IBM Cloud Portal Screenshot](image1)

2. Select **Check Point CloudGuard IaaS** in the catalogue drop-down menu.

![IBM Cloud Catalog Screenshot](image2)
3. Type **Check Point** in search field, and hit **Enter**.

4. Select the desired **Full Deployment** option. Example: *CloudGuard IaaS Security Management*

5. Review the information within the **Readme** tab to understand the various deployment parameters.

6. Enter the following initial information:
   a. Name: Give your workspace a unique name that you can easily recognize.
   b. Resource Group: Enter the desired Resource group for your workspace.
   c. Tags: Enter any tags, if required.
NOTE: It is recommended to acquire all of the deployment parameter values and enter them in notepad to easily cut and paste. See the Readme tab for specific commands to run within the IBM Cloud shell in order to acquire specific parameters.

Example: VPC_Region = `ibmcloud is regions`

NOTE: “Subnets” are the only fields that require ID numbers.

NOTE: “VNF_Security_group” must be a unique name as it is created during deployment.

NOTE: To initiate the IBM Cloud shell select the following icon:

7. Enter values for the Parameters that do not have default values assigned. See examples below for additional information
Set the deployment values

### Parameters without default values
Enter the required value for each parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Group</td>
<td>The resource group that will be used when provisioning the Check Point VSI.</td>
<td>7</td>
</tr>
<tr>
<td>SSH Key</td>
<td>The name of the public SSH Key that will be used when provisioning the Check Point VSI.</td>
<td></td>
</tr>
<tr>
<td>Subnet ID</td>
<td>The ID of the subnet where the Check Point VSI will be provisioned.</td>
<td></td>
</tr>
<tr>
<td>VNF Security Group</td>
<td>The name of the security group to be created for the VNF VPC.</td>
<td></td>
</tr>
<tr>
<td>VPC Name</td>
<td>The VPC where the Check Point VSI will be provisioned.</td>
<td></td>
</tr>
<tr>
<td>VPC Region</td>
<td>The region where the VPC, networks, and Check Point VSI will be provisioned.</td>
<td></td>
</tr>
</tbody>
</table>
8. Enter Parameters with default values (pre-set but can be modified).

   a. **CP_Version** – Enter desired version.
   b. **VNF_CP-MGMT_Instance** – Instance name.
   c. **VNF_Profile** - Value is set by default (Compute Profiles are recommended).
9. Click **Install**.
Assign a Floating IP to eth0 of the Management Server

**NOTE:** In our example, we are assigning a floating IP to eth0 as we will be managing the CloudGuard Management Server remotely over the public Internet.

1. Select **Floating IP** within the **Network** sub-heading of the **VPC Infrastructure** main menu.

2. In the **Floating IPs for VPC** page, within the **Region** drop-down menu, ensure that the correct region that was entered earlier is selected.

3. Click **Create**.

4. Enter the following details with the **Reserve a Floating IP** page to assign a floating IP address to the VSI.
   a. **Floating IP Name** - Provide a name for the floating IP address.
   b. **Resource Group** - Select the appropriate group.
   c. **Location** - Select the location (region) of the management server that was created in the previous step.
   d. **Instance to Bind** - Select the management server that was created in the previous step.
   e. **Network Interface** - Can only be assigned to eth0.
   f. **Tags** - Add any tags if required.

5. Click **Reserve IP**.
Reserve a floating IP

Reserve a floating IP and bind it to the network interface of a virtual server instance to allow public traffic to the instance.

Floating IP name

- cp-mgmt-fl-ip

Resource group

- Default

You can't change the resource group after the floating IP is created.

Learn about resource groups

Location

- Dallas
  - Dallas 1
- Frankfurt
  - Frankfurt 1

Instance to bind

- checkpoint-mgmt

Network interface

- eth0

Tags

- Examples: env:dev, version-1

Get sample API call

Estimated monthly

- United States
- $1.00

Cancel Reserve IP
Configure the Check Point CloudGuard Management Server

1. Go to https://<<Floating IP Assigned to Management Server>>
2. Select Advanced.
3. Select Proceed To.
7. Enter username **admin**.

8. Enter password **admin**.

9. Click **Login**.

10. Click **Next**.
11. In the **Deployment Options** page, select the option under **Setup**.
   
a. Click **Next**.
12. Provide the following information within the **Authentication Details** page:
   a. Enter Password
   b. Confirm Password

13. Click **Next**.
14. Review the information within the Management Connection page.
   a. Click Next.

   **NOTE:** All of the networking information will already be entered correctly and should not be changed within this page.
15. Enter the following information within the **Device Information** page:
   a. Hostname
   b. Domain Name (optional)
   c. DNS Servers

16. Click **Next**
17. Review (and edit, if required) settings within the **Date and Time Settings** page.

a. Click **Next**.
18. Within the **Installation Type**, select **Security Gateway and/or Security Management**.

   a. Click **Next**.
19. Within the **Products page**, uncheck **Security Gateway** (leaving only **Security Management** checked).

   a. Click **Next**.
20. With the **Security Management Administrator** page, select to use the built-in Gaia administrator user, **Admin**, or create a new user.

**NOTE:** This will be the administrator used from the SmartConsole application to access the management server.

a. Click **Next**.
21. Enter the desired settings within the Security Management GUI Clients page.

   a. Click Next.
22. Review the information within the **First Time Configuration Wizard Summary** page.

   a. Click **Finish**.
23. Click **Yes** in the **First Time Configuration Wizard** pop-up dialogue box.

24. The management server will begin the configuration:
25. Click **OK** on the **Configuration Completed Successfully** pop-up dialogue box.
26. Click **OK** in the *Message of the Day* pop-up dialogue box after you are automatically logged into the system.

![Image of Check Point Management Console]

27. Review settings make adjustments as needed.

28. Download and install SmartConsole, if you have not already done so.
Configure Routing

NOTE: This process will create the routing for the following for our sample topology.

- Anything from **Internal Subnet** going to **External Subnet** must go through the Check Point Gateway.
- Anything from **External Subnet** going to **Internal Subnet** must go through the Check Point Gateway.

NOTE: Additional routing may be required depending on your environment.

1. Select **Routing Tables** within the **Network** sub-heading of the **VPC Infrastructure** main menu.

2. In the **Routing Tables for VPC** page, within the **VPC** drop-down menu, ensure that the correct VPC is selected.

3. Select default route table was renamed earlier. Example: *single-vpc-rt*

4. Click **Create**.
5. Enter the following information to create two routes:
   a. Destination CIDR - Enter the destination network in CIDR notation.
   b. Location - Leave the default setting.
   c. Action - Choose Deliver.
   d. Type - Select IP Address.
   e. Next Hop - Enter the IP address of the next-hop interface.

6. Click Save.
<table>
<thead>
<tr>
<th>State</th>
<th>Destination</th>
<th>Action</th>
<th>Type</th>
<th>Next hop</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stable</td>
<td>10.240.128.64/27</td>
<td>Deliver</td>
<td>IP address</td>
<td>10.240.128.36</td>
<td>Dallas 3</td>
</tr>
<tr>
<td>Stable</td>
<td>10.240.128.32/27</td>
<td>Deliver</td>
<td>IP address</td>
<td>10.240.128.68</td>
<td>Dallas 3</td>
</tr>
</tbody>
</table>