



# Hybrid Mesh Network Security

16 April 2026

## CLOUD FIREWALL FOR OCI AUTO-SCALING INSTANCE POOL DEPLOYMENT GUIDE

Deployment Guide



# 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.



## Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



## Check Point Cloud Firewall for OCI Auto-Scaling Instance Pool Deployment Guide



## Latest Version of this Document in English

Open the latest version of this [document in a Web browser](#).  
Download the latest version of this [document in PDF format](#).



## Feedback

Check Point is engaged in a continuous effort to improve its documentation.  
[Please help us by sending your comments](#).

## Revision History

Date	Description
09 Mar 2025	First release of this document

# Table of Contents

---

<b>Overview of Cloud Firewall for OCI Instance Pools</b> .....	<b>5</b>
Licensing .....	5
Introduction to OCI Instance Pools .....	5
Prerequisites .....	6
Components of the Check Point Deployed Solution .....	6
<b>Scale-In and Scale-Out Events in Cloud Firewall for OCI Instance Pools</b> .....	<b>8</b>
Scale Out .....	8
Scale In .....	9
Testing Scale-In and Scale-Out Processes .....	9
<b>Configure Load Balancers in Cloud Firewall for OCI Instance Pools</b> .....	<b>11</b>
Network Diagram .....	11
Load Balancers Overview .....	11
Routing Tables .....	11
<b>Traffic Flows in Cloud Firewall for OCI Instance Pools</b> .....	<b>14</b>
Inbound Traffic - Request .....	14
Inbound Traffic - Reply .....	14
Outbound Traffic - Request .....	14
Outbound Traffic - Reply .....	15
East-West Outbound Traffic - Request .....	15
East-West Outbound Traffic - Reply .....	15
Intra-Subnet Traffic .....	16
<b>Configure Cloud Firewall for OCI Instance Pools</b> .....	<b>17</b>
Step 1: Prepare your OCI Account .....	17
Step 2: Install the Check Point Security Management Server .....	18
Step 3: Configure the Check Point Security Management Server .....	19
Step 4: Deploy the Check Point Instance Pool .....	19
Step 5: Set Up the Load Balancers .....	21

---

Creating Dynamic Objects 'LocalGatewayExternal' and 'LocalGatewayInternal' .....	22
Step 6: Configure Inbound Protection .....	23
Step 7: Configure Outbound and East-West Protection .....	25
Configuring Outbound Protection .....	25
Configuring East-West Protection Between Internal Subnets. ....	27
<b>Cloud Firewall Instance Pool Solution Upgrade .....</b>	<b>30</b>
<b>Configure Cloud Management Extension (CME) .....</b>	<b>32</b>
Downloading and Installing the Latest CME Version .....	32
Configuring the CME on the Security Management Server .....	32
<b>Configure HTTPS Inspection .....</b>	<b>39</b>
Creating an Outbound Certificate .....	39
Creating an HTTPS Inspection Rule to Inspect SSL Traffic .....	39
<b>IPS Geo Protection Based on X-Forwarded-For HTTP Header .....</b>	<b>41</b>
Use Case 1 .....	41
Use Case 2 .....	41
<b>Limitations of Cloud Firewall for OCI Instance Pools .....</b>	<b>43</b>

# Overview of Cloud Firewall for OCI Instance Pools

Use this guide to deploy a Check Point Cloud Firewall for OCI Instance Pools solution.

 **Note** - For the list of supported versions, refer to the [Support Life Cycle Policy](#).

## Licensing

Check Point Cloud Firewall Gateways and Check Point Security Management Server must have a license.

The Cloud Firewall for OCI Instance Pools solution uses the BYOL licensing model.

 **Important** - All Cloud Firewall Gateways in the Instance Pool must use BYOL.

To buy BYOL licenses, contact [Check Point Sales](#).

For more information about licensing, see the [Cloud Firewall Central License Management Utility](#) guide.

## Introduction to OCI Instance Pools

OCI Instance Pools let you deploy and manage groups of identical virtual machines (VMs) in Oracle Cloud. They automatically adjust VM numbers based on your needs. Each OCI Instance Pool spreads VMs across different Availability Zones for reliability. A Load Balancer sends network traffic to these VMs.

Check Point Cloud Firewall protects OCI Instance Pools from cyber attacks, and it must be as scalable, as the resources it protects.

The system uses these key parts:

- Cloud Firewall Gateways shield your resources (VMs).
- A Security Management Server manages all Cloud Firewall Gateways.
- Oracle Autoscale monitors your Instance Pool size and adds or removes Cloud Firewall Gateways as needed.

### **Notes:**

- Cloud Firewall Gateway count must match your Instance Pool size.
- The Security Management Server can run in Oracle Cloud or on-premises.

# Prerequisites

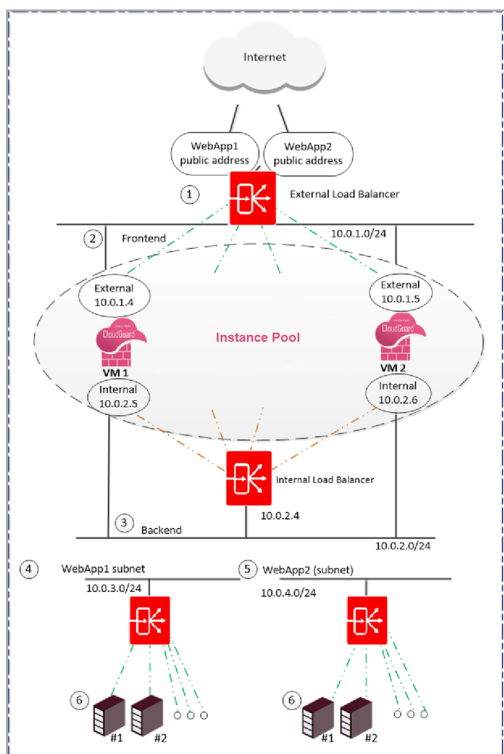
Make sure you are familiar with these topics:

Vendor	Topics
Oracle Cloud Infrastructure	<ul style="list-style-type: none"> <li>Instance Pool</li> <li>Auto-Scaling</li> <li>Load Balancers</li> </ul>
Check Point	<ul style="list-style-type: none"> <li>Cloud Firewall Gateway</li> <li>Cloud Firewall for OCI</li> </ul>

# Components of the Check Point Deployed Solution

The diagram below depicts an OCI Virtual Cloud Network (VCN) with the deployed Check Point solution.

## Network Diagram



There are two backend subnets - WebApp1 and WebApp2.


WebApp1 and WebApp2 are each a user-deployed backend subnet. Each has its own load-balanced web server.

**The Check Point deployed solution has these components:**

- Frontend subnet
- Instance Pool

The number of instances that you can deploy in the Cloud is dynamic.

- Internal Load Balancer
- Backend subnet
- External Load Balancer

 **Note** - Instance Pool cannot host different VM types.

# Scale-In and Scale-Out Events in Cloud Firewall for OCI Instance Pools

Oracle Autoscale adjusts the number of Cloud Firewall Gateways in the Instance pool based on the traffic load.


It uses two main events:

- **Scale Out:** Adds Cloud Firewall Gateways to the Instance pool when the traffic load increases.
- **Scale In:** Removes Cloud Firewall Gateways from the Instance pool when the traffic load decreases.

To view or edit Oracle Autoscale settings, go to **OCI Portal > Compute > Autoscaling Configurations**.

Default Cloud Firewall Gateway CPU thresholds to trigger autoscaling events:

- **Scale Out:** Triggers at 80% CPU use (5-minute average).
- **Scale In:** Triggers at 60% CPU use (5-minute average).

 **Note** - To use Cloud Firewall Metrics as triggers for scale-in and scale-out events, you need special permissions. For more information, see [Adding proper permissions for metrics](#).

## Scale Out

When a scale-out event triggers:

1. Oracle Autoscale launches new Cloud Firewall Gateways.
2. New Cloud Firewall Gateways automatically run the First Time Configuration Wizard and reboot.
3. The Security Management Server:
  - a. Detects new Cloud Firewall Gateway instances.
  - b. Creates a Secure Internal Communication (SIC) channel with these Cloud Firewall Gateway instances.
  - c. Installs a Security Policy on each new Cloud Firewall Gateway.
4. The External Load Balancer starts sending traffic to these new Cloud Firewall Gateways.

- Note** - New Cloud Firewall Gateways report their status and send logs to the Security Management Server.

## Scale In

When a scale-in event triggers:

1. Oracle Autoscale marks one or more Cloud Firewall Gateways as candidates for termination.
2. The External Load Balancer stops sending traffic to marked Cloud Firewall Gateways.
3. Oracle Autoscale terminates marked Cloud Firewall Gateways.
4. The Security Management Server removes terminated Cloud Firewall Gateways from its database.

- Important** - : Keep at least two Cloud Firewall Gateways (one in each Availability Zone) running for redundancy and availability.

## Testing Scale-In and Scale-Out Processes

The initial solution deployment process includes these steps:

1. When the Check Point Cloud Firewall for OCI Instance Pools solution is deployed, it creates Cloud Firewall Gateways.
2. Each new Cloud Firewall Gateway automatically runs the First Time Configuration Wizard. This usually takes 10 minutes to complete. Large Virtual Machines may require additional time.
3. After configuration completes, the Security Management Server automatically installs the Security Policy on these Cloud Firewall Gateways.
4. To verify deployment success, use SmartConsole to:
  - Confirm the Security Policy installation.
  - Verify log generation and transmission by Cloud Firewall Gateways.

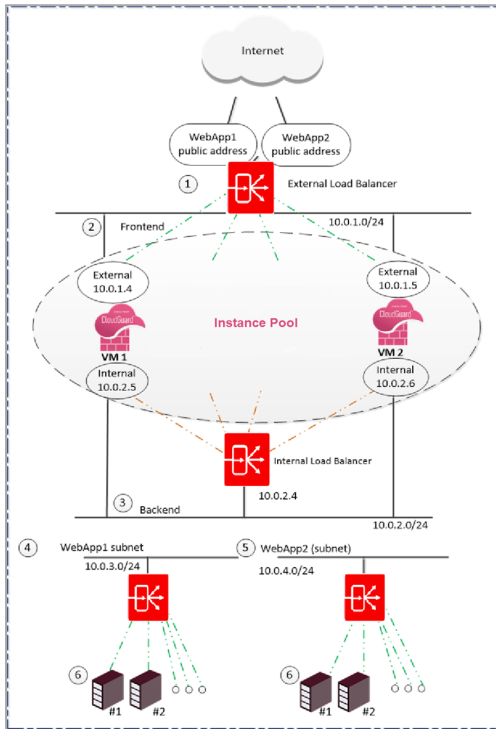
To test scale-in and scale-out processes, simulate high CPU load on Cloud Firewall Gateways

Step	Description
1	Connect to the Cloud Firewall Gateway command line interface (CLI) over SSH.
2	Enter Expert mode.

Step	Description
3	Download the CPU load simulation script ( <code>simulate_cpu_load.sh</code> ) from this link: <a href="https://raw.githubusercontent.com/CheckPointSW/CloudGuardIaaS/master/common/simulate_cpu_load.sh">https://raw.githubusercontent.com/CheckPointSW/CloudGuardIaaS/master/common/simulate_cpu_load.sh</a>
4	Place the script in the correct directory of the Cloud Firewall Gateway: <pre>/var/tmp/simulate_cpu_load.sh</pre>
5	Set execute permissions to the script: <pre>chmod u+x /var/tmp/simulate_cpu_load.sh</pre>
6	Validate script syntax: <pre>sh -n /var/tmp/simulate_cpu_load.sh</pre>
7	Execute the script to simulate high CPU load: <pre>./var/tmp/simulate_cpu_load.sh</pre>
8	In a separate terminal, monitor CPU load (it must be at a high level): <pre>top</pre>
<p><b>Note</b> - After 10 minutes of high CPU load, a scale-out event triggers. Oracle Autoscale provisions a new Cloud Firewall Gateway.</p>	
9	After the new Cloud Firewall Gateway is provisioned, press any key to stop the simulation script on the original Cloud Firewall Gateway.
10	In a separate terminal, monitor CPU load (it must return to normal levels): <pre>top</pre>
<p><b>Note</b> - After 10 minutes of normal CPU load, a scale-in event triggers. Security Management Server automatically removes the newly provisioned Cloud Firewall Gateway.</p>	

# Configure Load Balancers in Cloud Firewall for OCI Instance Pools

## Network Diagram



## Load Balancers Overview

In the diagram above, you can see Load Balancers at three levels.

These routes describe the flow of traffic through the Load Balancers

- Level 1: External Load Balancer (handles Internet traffic)
- Level 2: Internal Load Balancer (of the deployed Check Point solution)
- Level 3: Web Server Load Balancers



**Note** - Subnets with load-balanced hosts (Web Servers) use Level 3 Load Balancers.

## Routing Tables



**Note** - *WebApp1* and *WebApp2* routing tables have the same VNET address, but different subnet addresses.

**Load Balancing Rules of the External Load Balancer**

1	<b>Example 1</b>	<b>Frontend</b> WebApp1:80	<b>Backend port</b> 8081
	<b>Example 2</b>	<b>Frontend</b> WebApp2:80	<b>Backend port</b> 8083

**Frontend Routing Table - User Defined Routes (UDR)**

2	<b>Destination</b> 10.0.0.0/16	<b>Nexthop</b> None (Drop)
	10.0.1.0/24	Virtual Network

**Backend Routing Table - User Defined Routes (UDR)**

3	<b>Destination</b> 0.0.0.0/0	<b>Nexthop</b> None (Drop)
---	---------------------------------	-------------------------------

**WebApp1 - User Defined Routes (UDR)**

4	<b>Frontend</b>	<b>Nexthop</b>
	10.0.0.0/16 - <i>VNET address</i>	10.0.2.4 - <i>IP address of the Internal Load Balancer</i>
	0.0.0.0/0	10.0.2.4 - <i>IP address of the Internal Load Balancer</i>
	10.0.2.0/24	<i>Virtual Network</i>
	10.0.3.0/24 (WebApp1) - <i>Subnet address</i>	<i>Virtual Network</i>

**WebApp2 - User Defined Routes (UDR)**

5	<b>Frontend</b>	<b>Nexthop</b>
---	-----------------	----------------

	<b>10.0.0.0/16 -VNET address</b>	<b>10.0.2.4 -IP address of the Internal Load Balancer</b>
	<b>0.0.0.0/0</b>	<b>10.0.2.4 -IP address of the Internal Load Balancer</b>
	<b>10.0.2.0/24</b>	<i>Virtual Network</i>
	<b>10.0.4.0/24 (WebApp2) - Subnet address</b>	<i>Virtual Network</i>

**Hosts**

6	WebApp1 (subnet) load balanced Instance Pool WebApp2 (subnet) load balanced Instance Pool
---	--

# Traffic Flows in Cloud Firewall for OCI Instance Pools

## Inbound Traffic - Request

Inbound traffic - request flow:

1. The request traffic from the Internet reaches the External Load Balancer in the deployed Check Point solution.
2. The External Load Balancer receives the request traffic on port 80 and sends it to the Cloud Firewall Gateway of the Instance Pool.
3. The Cloud Firewall Gateway:
  - a. Inspects the request traffic.
  - b. Performs Source NAT and Destination NAT on the request traffic.
  - c. Forwards the request traffic to the Web Server Host.

## Inbound Traffic - Reply

Inbound traffic - reply flow:

1. The Web Server host sends its reply to the Cloud Firewall Gateway that processed the connection.
2. The Cloud Firewall Gateway:
  - a. Inspects the reply traffic.
  - b. Reverses NAT and restores the original destination.
  - c. Forwards the reply traffic to the destination on the Internet.

## Outbound Traffic - Request

Outbound traffic - request flow:

1. The request traffic from the Web Server host reaches the Internal Load Balancer in the deployed Check Point solution.
2. The Internal Load Balancer sends the request traffic to the Cloud Firewall Gateway of the Instance Pool.
3. The Cloud Firewall Gateway:

- a. Inspects the request traffic.
- b. Performs Hide NAT on the request traffic.
- c. Forwards the request traffic to the destination on the Internet.

## Outbound Traffic - Reply

Outbound traffic - reply flow:

1. The reply traffic from the Internet reaches the Cloud Firewall Gateway of the Instance Pool.
2. The Cloud Firewall Gateway:
  - a. Inspects the reply traffic.
  - b. Reverses Hide NAT.
  - c. Forwards the reply traffic to the Web Server host.

## East-West Outbound Traffic - Request

East-West outbound traffic - request flow:

1. The request traffic from the Web Server host reaches the Internal Load Balancer in the deployed Check Point solution.
2. The Internal Load Balancer sends the request traffic to the Cloud Firewall Gateway of the Instance Pool.
3. The Cloud Firewall Gateway:
  - a. Inspects the request traffic.
  - b. Forwards the request traffic to the Application's Internal Load Balancer.
4. The Application's Internal Load Balancer forwards the request traffic to the App Server host.

## East-West Outbound Traffic - Reply

East-West outbound traffic - reply flow:

1. The reply traffic from the App Server host reaches the Internal Load Balancer in the deployed Check Point solution.
2. The Internal Load Balancer sends the reply traffic to the same Cloud Firewall Gateway that processed the request traffic from the Web Server host.
3. The Cloud Firewall Gateway:

- a. Inspects the reply traffic.
- b. Forwards the reply traffic to the Web Server host.

## Intra-Subnet Traffic

Traffic within the same subnet flows directly. No inspection or routing are required.

# Configure Cloud Firewall for OCI Instance Pools

## Step 1: Prepare your OCI Account

The Check Point Security Management Server uses an API signing key to monitor Instance Pools and Cloud Firewall Gateway provisioning.

To set up user permissions:

1. Create a permission group:

- In your OCI account, navigate to **Identity & Security**.
- Under **Identity**, click **Domains**.
- Select the target user domain.
- On the left pane, click **Groups**.
- Click **Create Group** to create a new group for autoscale permissions.

2. Configure Security Policies:

- Navigate to **Identity & Security > Policies**.
- Create a new policy for the previously created group (use the group name for `<group_name>`) with these permissions:

```
Allow group <domain>/<group_name> to manage instance-family in
compartment <compartment_name>
Allow group <domain>/<group_name> to inspect vnic-attachments
in compartment <compartment_name>
Allow group <domain>/<group_name> to manage virtual-network-
family in compartment <compartment_name>
Allow group <domain>/<group_name> to inspect instance-pools in
compartment <compartment_name>
```

3. Assign target users to the created permission group. For that, go to the group and click **Assign user to groups**.

To generate an API Signing Key pair, refer to the [OCI documentation](#) for the most up-to-date instructions. After generating an API signing key, write down these values for the "Configure the Check Point Security Management Server" step:

- User OCID
- Tenancy OCID
- Private API key.

To allow the Cloud Firewall Gateway to publish metrics to the Monitoring service, you must set up necessary permissions:

1. Create a Dynamic Group.

- In your OCI Account, navigate to **Identity & Security**.
- Under **Identity**, click **Domains**.
- Click **Create domain**. For **Domain type**, select **Free**.
- Click on the created domain. Under **Identity domain**, select **Dynamic groups**.
- Click **Create dynamic group**. For the matching rules, select **Match any rules defined below** and add the following:

```
Any {instance.compartment.id = '<compartment_name>'}
```

2. Configure Security Policies:

- Navigate to **Identity & Security/ > Policies**.
- Click **Create Policy**. For **Policy Builder**, press **Show manual editor** and add these permissions:

```
allow dynamic-group <domain>/<dynamic_group> to use metrics in
compartment <compartment_name>
```

## Step 2: Install the Check Point Security Management Server

These steps are required only if you do not have an installed Check Point Security Management Server.

If you already have the Security Management Server installed, skip to **Step 3**.

### Requirements for the Check Point Security Management Server

Must start connections to the Cloud Firewall Gateways.

### Requirements for Cloud Firewall Gateways

Must start connections to the Security Management Server. For example, to send logs.

## Deploying a Security Management Server in OCI

From the OCI Marketplace, deploy the solution "Cloud Firewall Security Management".


## Deploying a Security Management Server on-premises

Follow the instructions in the *Check Point Installation and Upgrade Guide* for your Security Management Server version.

# Step 3: Configure the Check Point Security Management Server

Do these steps to manage Instance Pools with the Check Point Security Management Server:

1. In SmartConsole, change the IP address of the Security Management Server object to be its public IP address.
2. ["Downloading and Installing the Latest CME Version" on page 32](#) of CME.
3. ["Configuring the CME on the Security Management Server" on page 32](#)
4. Configure the Security Policy in SmartConsole.

 **Note** - By default, each Cloud Firewall Gateway and Security Management Server's Gaia Portal is accessible from the internet by browsing to `http://<virtual-machine-public-ip>`. Restriction of access to the Gaia Portal is possible by configuring a Security List, or by configuring the Cloud Firewall Gateway and Security Management Server settings.

# Step 4: Deploy the Check Point Instance Pool

To deploy the Check Point Instance Pool, do these steps:


1. Find the stack by searching for "Cloud Firewall AutoScale - BYOL Stack" in the OCI marketplace, agree to the licensing terms, and click **Launch Stack**.
2. Name your stack and add a description. Use the default Terraform version.
3. Use these parameters in the **Compute Configuration** section:

Parameter	Description
Compartment	The OCI compartment where the Instance Pool is deployed.

Parameter	Description
<b>Minimum Instance Count in Pool</b>	The minimum number of Cloud Firewall Gateway instances in the Instance Pool. We recommend a minimum of two.
<b>Maximum Instance Count in Pool</b>	The maximum number of Cloud Firewall Gateway instances in the Instance Pool.
<b>Scale In CPU Threshold</b>	The CPU utilization threshold percentage to scale in.
<b>Scale Out CPU Threshold</b>	The CPU utilization threshold percentage to scale out.

- For the **Network Configuration** section, choose to either create a new VCN and subnets or use an existing one.
- Use these parameters in the **Additional Configuration** section:

Parameter	Description
<b>Name of the Existing Management with CME</b>	Must exactly match the management name configured in CME on the Security Management Server.
<b>Name of the Template for this stack.</b>	Must exactly match the configuration template name configured in CME on the Security Management Server.
<b>Management interface to use.</b>	Select which interface to use as the management interface for the Instance Pool: <ul style="list-style-type: none"> <li>▪ eth0: frontend VNIC</li> <li>▪ eth1: backend VNIC</li> </ul>
<b>Indicates if the management interface is using its public IP address or private IP address to connect.</b>	<p><b>Public:</b> Manage the Cloud Firewall Gateway Instance Pool with the public IP addresses of the instance.</p> <p><b>Private:</b> Manage the Cloud Firewall Gateway Instance Pool with the private IP address of the instance. The Security Management Server must have access to the private IP addresses.</p>

Parameter	Description
<b>Enable Cloud Firewall metrics</b>	<p>Enable Cloud Firewall metrics to send statuses and statistics collected from instances to the OCI Monitor service.</p> <p>If the Cloud Firewall metrics are enabled:</p> <ul style="list-style-type: none"> <li>▪ The Cloud Firewall metrics agent starts to send metrics each minute.</li> <li>▪ The Cloud Firewall metrics are sent to the OCI Monitor resource immediately after the instance pool deployment is completed.</li> </ul> <p> <b>Note</b> - <i>"To allow the Cloud Firewall Gateway to publish metrics to the Monitoring service, you must set up necessary permissions:" on page 18</i></p>

6. After reviewing that everything is correct, click **Create**.
7. The **Stack Details** page opens. Click **Apply** to start creation of the autoscale resources.
8. The next screen shows the status updates as the deployment proceeds, allowing you to troubleshoot any problems if necessary.

The deployment includes a VCN and two subnets (if you decided not to use the existing subnets), two network Load Balancers, and an Instance Pool with the configured minimum number of Cloud Firewall Gateways.

After the deployment finishes successfully, it takes 1-3 minutes until the Security Management Server finishes the configuration. Autoscaling is ready when the health check of the Load Balancer passes (find it at **OCI console > Compute > Instance Pools > Your Instance Pool Stack > Load Balancers > Health Check**).

All resources can be deleted by clicking **Destroy** on the **Stack Details** page.

## Step 5: Set Up the Load Balancers

By default, the stack you deploy creates an external and internal Load Balancer.

### The External Load Balancer:

- Listens on TCP port 80 on the static public IP address of the External Load Balancer.
- Forwards the traffic it receives to the pool of Cloud Firewall Gateways on TCP port 8081.
- Uses TCP health probes on port 8117 to know the health of the Cloud Firewall Gateways.

### The Internal Load Balancer:

- Listens and forwards all TCP or UDP traffic on all ports.
- Uses TCP health probes on port 8117 to know the health of the Cloud Firewall Gateways.

### Notes:

- You cannot use ports 80, 443, 444, 8082, 8117, and 8880 for forwarded traffic.
- In addition, you cannot use the ports defined in [sk52421](#) (used by Check Point software), and 32768 - 65535 as defined in [sk162619](#) (FWD daemon listening on multiple random high ports).
- Do not change the health probes.
- The Instance Pool deployment includes a default security list that allows all outbound and inbound traffic.

## Creating Dynamic Objects 'LocalGatewayExternal' and 'LocalGatewayInternal'

You must also create these Dynamic Objects in SmartConsole:

- **LocalGatewayExternal**
- **LocalGatewayInternal**



### Procedure:

1. Click **Objects** menu > **More object types** > **Network Object** > **Dynamic Object** > **New Dynamic Object**.
2. Enter this exact name (case-sensitive, no spaces):  
**LocalGatewayExternal**
3. Click **OK**.
4. Click **Objects** menu > **More object types** > **Network Object** > **Dynamic Object** > **New Dynamic Object**.
5. Enter this exact name (case-sensitive, no spaces):  
**LocalGatewayInternal**
6. Click **OK**.
7. Publish the SmartConsole session

## Step 6: Configure Inbound Protection

Configure Access Control and NAT rules for Northbound-Southbound inbound traffic

Step	Description
1	Connect with SmartConsole to your Security Management Server or Multi-Domain Server.
2	<p>Create a host object to represent one of these:</p> <ul style="list-style-type: none"> <li>▪ The Application Load Balancer that is related to your backend Instance Pools.</li> <li>▪ The specific Application Host you want to access through the Internet.</li> </ul> <p>You must do this for each Application Load Balancer you use to balance your servers.</p> <p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Click <b>Objects</b> menu &gt; <b>New Host</b>.</li> <li>b. Enter a descriptive name. For example, <code>application-load-balancer-app-1</code></li> <li>c. Enter the private IP address of the Application Load Balancer.</li> <li>d. Click <b>OK</b>.</li> </ol>
3	<p>Create a new TCP service to represent the internal port of the External Load Balancer or External Application Gateway configuration.</p> <p>You must do this for each backend port, such as port 8081.</p> <p>Do these steps:</p> <ol style="list-style-type: none"> <li>a. Click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Service</b> &gt; <b>New TCP</b>.</li> <li>b. Enter a descriptive name. For example, <code>http-8081</code>.</li> <li>c. In the <b>Protocol</b> field, select the applicable protocol (such as HTTP or HTTPS).</li> <li>d. In the <b>Port</b> field, select <b>Customize</b> and enter the port number. For example, <code>8081</code>.</li> <li>e. Click <b>OK</b>.</li> </ol>

Step	Description																		
4	<p>Create a corresponding Access Control rule for each External Load Balancer with these values:</p> <table border="1" data-bbox="300 353 1458 741"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Descriptive name</td> <td>Any</td> <td>LocalGatewayExternal</td> <td>Any</td> <td>The service object that represents the internal port of the External Load Balancer</td> <td>Accept</td> <td>Log</td> <td>Policy Targets</td> </tr> </tbody> </table> <p> <b>Note</b> - Create only one <b>LocalGatewayExternal</b> object for each Security Management Server. See <a href="#">"Creating Dynamic Objects 'LocalGatewayExternal' and 'LocalGatewayInternal'" on page 22.</a></p>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On	1	Descriptive name	Any	LocalGatewayExternal	Any	The service object that represents the internal port of the External Load Balancer	Accept	Log	Policy Targets
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On											
1	Descriptive name	Any	LocalGatewayExternal	Any	The service object that represents the internal port of the External Load Balancer	Accept	Log	Policy Targets											
5	<p>Create a NAT rule with these values for each Application Host or Application Load Balancer.</p> <p>In the <b>Translated Source</b> column:</p> <ol style="list-style-type: none"> <li>1. Add the <b>LocalGatewayInternal</b> object.</li> <li>2. Right-click on the <b>LocalGatewayInternal</b> object &gt; select <b>NAT Method</b> &gt; click <b>Hide</b>.</li> </ol> <table border="1" data-bbox="300 1196 1458 1765"> <thead> <tr> <th>No</th> <th>Original Source</th> <th>Original Destination</th> <th>Original Services</th> <th>Translated Source</th> <th>Translated Destination</th> <th>Translated Services</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>All_Internet</td> <td>LocalGatewayExternal</td> <td>The service object that represents the internal port of the External Load Balancer</td> <td>LocalGatewayInternal</td> <td>The Host object that represents the internal Application Host or Application Load Balancer</td> <td>The service object that represents the port, on which the Internal Load Balancer or Application Host listens (for example, http)</td> <td>Policy Targets</td> </tr> </tbody> </table> <p> <b>Note</b> - Do not use *Any in the <b>Original Source</b> column.</p>	No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	1	All_Internet	LocalGatewayExternal	The service object that represents the internal port of the External Load Balancer	LocalGatewayInternal	The Host object that represents the internal Application Host or Application Load Balancer	The service object that represents the port, on which the Internal Load Balancer or Application Host listens (for example, http)	Policy Targets		
No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On												
1	All_Internet	LocalGatewayExternal	The service object that represents the internal port of the External Load Balancer	LocalGatewayInternal	The Host object that represents the internal Application Host or Application Load Balancer	The service object that represents the port, on which the Internal Load Balancer or Application Host listens (for example, http)	Policy Targets												

Step	Description
	<p>This NAT rule:</p> <ul style="list-style-type: none"> <li>Matches any traffic that arrives at the Cloud Firewall Gateway on the applicable backend port.</li> <li>Translates the Source IP address to match the IP address of the Cloud Firewall Gateway that handles the connection ("eth1"). When you use this, the packets that return are routed to the correct Cloud Firewall Gateway.</li> <li>Translates the destination IP address to the IP address of the Application Load Balancer or Application Host associated with the Web Servers.</li> </ul>
6	Publish the session.
7	Install the Access Control Policy on the Cloud Firewall Gateways.

## Step 7: Configure Outbound and East-West Protection

Configure UDR tables and NAT rules for Outbound and East-West traffic protection.

You can configure the Check Point Instance Pool to examine Outbound and East-West traffic across internal subnets.

To configure the traffic inspection from servers in internal private subnets, you must route traffic through the Check Point Instance Pool. Use the Check Point Internal Load Balancer as the *Next hop* in the private subnet UDR. The Internal Load Balancer then forwards all the traffic to one of the Cloud Firewall Gateways.

### Configuring Outbound Protection

To configure Outbound Protection

Step	Description
1	Connect with SmartConsole to your Security Management Server or Multi-Domain Server.

Step	Description																								
2	<p>Create a Network object that represents the OCI VCN:</p> <ol style="list-style-type: none"> <li>Click <b>Objects</b> menu &gt; <b>New Network</b>.</li> <li>Enter a descriptive name.</li> <li>From the left tree, click <b>General</b>. Enter the applicable information.</li> <li>From the left tree, click <b>NAT</b>. Select <b>Add automatic address translation rules</b>. This performs Static NAT for all outbound rules.</li> <li>Click <b>OK</b>.</li> </ol>																								
3	In SmartConsole, from the left navigation panel, click <b>Security Policies</b> .																								
4	In the <b>Access Control</b> section, click <b>NAT</b> .																								
5	<p>Make sure these Automatic NAT rules exist:</p> <table border="1"> <thead> <tr> <th>No</th> <th>Original Source</th> <th>Original Destination</th> <th>Original Services</th> <th>Translated Source</th> <th>Translated Destination</th> <th>Translated Services</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>AllVnet</td> <td>AllVnet</td> <td>Any</td> <td>=Original</td> <td>=Original</td> <td>=Original</td> <td>Policy Targets</td> </tr> <tr> <td>3</td> <td>AllVnet</td> <td>Any</td> <td>Any</td> <td>≠AllVnet</td> <td>=Original</td> <td>=Original</td> <td>Policy Targets</td> </tr> </tbody> </table>	No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	2	AllVnet	AllVnet	Any	=Original	=Original	=Original	Policy Targets	3	AllVnet	Any	Any	≠AllVnet	=Original	=Original	Policy Targets
No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On																		
2	AllVnet	AllVnet	Any	=Original	=Original	=Original	Policy Targets																		
3	AllVnet	Any	Any	≠AllVnet	=Original	=Original	Policy Targets																		
6	In the <b>Access Control</b> section, click <b>Policy</b> .																								
7	<p>Add this explicit Access Control rule:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>To Internet</td> <td>AllVnet</td> <td>All_Internet</td> <td>Any</td> <td>Any</td> <td>Accept</td> <td>Log</td> <td>Policy Targets</td> </tr> </tbody> </table>	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On	To Internet	AllVnet	All_Internet	Any	Any	Accept	Log	Policy Targets								
Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On																		
To Internet	AllVnet	All_Internet	Any	Any	Accept	Log	Policy Targets																		
8	In SmartConsole, install the Access Control Policy.																								
9	Connect to the OCI portal.																								
10	Add UDR rules with the Internal Load Balancer's private IP address as next hop.																								

Example - UDR rules with the Internal Load Balancer's private IP address as the next hop

NAME	ADDRESS PREFIX	NEXT HOP
to-internet	0.0.0.0/0	Private IP address of the Internal Load Balancer.

## Configuring East-West Protection Between Internal Subnets.

Solution:

Do these steps for each subnet:

Step	Description
1	Connect with SmartConsole to your Security Management Server or Multi-Domain Server.
2	<p>Create a Network object:</p> <ol style="list-style-type: none"> <li>Click <b>Objects</b> menu &gt; <b>New Network</b>.</li> <li>Enter a descriptive name (for example, "NetworkA").</li> <li>From the left tree, click <b>General</b>. Enter the applicable information.</li> <li>From the left tree, click <b>NAT</b>. Select <b>Add automatic address translation rules</b>. This performs Static NAT for all outbound rules.</li> <li>Click <b>OK</b>.</li> </ol>
3	In SmartConsole, from the left navigation panel, click <b>Security Policies</b> .
4	In the <b>Access Control</b> section, click <b>NAT</b> .

Step	Description																								
5	<p>Make sure these Automatic NAT rules exist:</p> <table border="1" data-bbox="304 320 1460 739"> <thead> <tr> <th data-bbox="304 320 384 512">No</th> <th data-bbox="384 320 521 512">Original Source</th> <th data-bbox="521 320 695 512">Original Destination</th> <th data-bbox="695 320 839 512">Original Services</th> <th data-bbox="839 320 1003 512">Translated Source</th> <th data-bbox="1003 320 1177 512">Translated Destination</th> <th data-bbox="1177 320 1345 512">Translated Services</th> <th data-bbox="1345 320 1460 512">Install On</th> </tr> </thead> <tbody> <tr> <td data-bbox="304 512 384 624">2</td> <td data-bbox="384 512 521 624">Network A</td> <td data-bbox="521 512 695 624">NetworkA</td> <td data-bbox="695 512 839 624">Any</td> <td data-bbox="839 512 1003 624">= Original</td> <td data-bbox="1003 512 1177 624">= Original</td> <td data-bbox="1177 512 1345 624">= Original</td> <td data-bbox="1345 512 1460 624">Policy Targets</td> </tr> <tr> <td data-bbox="304 624 384 739">3</td> <td data-bbox="384 624 521 739">Network A</td> <td data-bbox="521 624 695 739">Any</td> <td data-bbox="695 624 839 739">Any</td> <td data-bbox="839 624 1003 739">NetworkA</td> <td data-bbox="1003 624 1177 739">= Original</td> <td data-bbox="1177 624 1345 739">= Original</td> <td data-bbox="1345 624 1460 739">Policy Targets</td> </tr> </tbody> </table>	No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	2	Network A	NetworkA	Any	= Original	= Original	= Original	Policy Targets	3	Network A	Any	Any	NetworkA	= Original	= Original	Policy Targets
No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On																		
2	Network A	NetworkA	Any	= Original	= Original	= Original	Policy Targets																		
3	Network A	Any	Any	NetworkA	= Original	= Original	Policy Targets																		
6	<p>Create a Network Group object to represent the full internal address space:</p> <ol style="list-style-type: none"> <li>Click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Group</b> &gt; <b>New Network Group</b>.</li> <li>Enter a descriptive name. For example, <code>AllInternalAddressSpace</code>.</li> <li>Add the VCN's <b>Network</b> objects you created in Step 2.</li> <li>Click <b>OK</b>.</li> </ol>																								
7	<p>In the <b>Access Control</b> section, click <b>NAT</b>.</p>																								
8	<p>Add a Manual NAT rule to skip NAT for internal traffic between VCNs:</p> <table border="1" data-bbox="304 1196 1460 1610"> <thead> <tr> <th data-bbox="304 1196 515 1388">Original Source</th> <th data-bbox="515 1196 727 1388">Original Destination</th> <th data-bbox="727 1196 866 1388">Original Services</th> <th data-bbox="866 1196 1026 1388">Translated Source</th> <th data-bbox="1026 1196 1190 1388">Translated Destination</th> <th data-bbox="1190 1196 1350 1388">Translated Services</th> <th data-bbox="1350 1196 1460 1388">Install On</th> </tr> </thead> <tbody> <tr> <td data-bbox="304 1388 515 1610"> <b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)                 </td> <td data-bbox="515 1388 727 1610"> <b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)                 </td> <td data-bbox="727 1388 866 1610">Any</td> <td data-bbox="866 1388 1026 1610">= Original</td> <td data-bbox="1026 1388 1190 1610">= Original</td> <td data-bbox="1190 1388 1350 1610">= Original</td> <td data-bbox="1350 1388 1460 1610">Policy Targets</td> </tr> </tbody> </table>	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	<b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)	<b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)	Any	= Original	= Original	= Original	Policy Targets										
Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On																			
<b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)	<b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)	Any	= Original	= Original	= Original	Policy Targets																			
9	<p>In the <b>Access Control</b> section, click <b>Policy</b>.</p>																								

Step	Description																
10	<p>Add this explicit Access Control rule to allow outbound access from the full internal address space to the Internet:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>To Internet</td> <td><b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)</td> <td>All_Internet</td> <td>Any</td> <td>Any</td> <td>Accept</td> <td>Log</td> <td>Policy Targets</td> </tr> </tbody> </table>	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On	To Internet	<b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)	All_Internet	Any	Any	Accept	Log	Policy Targets
Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On										
To Internet	<b>Network Group</b> object that represents the full internal address space (AllInternalAddressSpace)	All_Internet	Any	Any	Accept	Log	Policy Targets										
11	In SmartConsole, install the Access Control Policy.																
12	Connect to the OCI portal.																
13	<p>Add UDR rules for each internal private subnet:</p> <ol style="list-style-type: none"> <li>Create the rule to 0.0.0.0/0, use the Internal Load Balancer’s private IP address as the next hop to monitor outbound traffic.</li> <li>Create the rule to a different internal private subnet, use the Internal Load Balancer’s private IP address as the next hop to monitor outbound traffic.</li> </ol>																

**Example - UDR rules for each internal private subnet**

NAME	ADDRESS PREFIX	NEXT HOP
to-Internet	0.0.0.0/0	Private IP address of the Internal Load Balancer
to-internal-subnet	10.0.2.0/0	Private IP address of the Internal Load Balancer

# Cloud Firewall Instance Pool Solution Upgrade

This section provides instructions for upgrading an already deployed Cloud Firewall Instance Pool solution.

The upgrade procedure includes these steps:




1. Deploying a new version of the Cloud Firewall Instance Pool solution alongside the older version (a side-by-side upgrade).
2. Reconfiguring OCI resources and Check Point configuration to use this new version of the Cloud Firewall Instance Pool solution.
3. Deleting the older version of the Cloud Firewall Instance Pool solution.

## Terms:

- **Source** - The original template and solution (with the lower version)
- **Target** - The new template and solution (with the higher version)

## To upgrade the Cloud Firewall Instance Pool solution

Step	Description
1	Log in to the OCI portal.
2	Deploy a target Cloud Firewall Instance Pool solution from the OCI Marketplace. To do this: <ol style="list-style-type: none"> <li>a. Select the desired image version.</li> <li>b. Use the same Security Management Server name as for the source Cloud Firewall Instance Pool solution.</li> <li>c. Use a different configuration template name than in the source Cloud Firewall Instance Pool solution.</li> <li>d. Use the same VCN and subnets as the source solution.</li> <li>e. Deploy the stack.</li> </ol>
3	Configure the <a href="#">CME template</a> . For this, run: <pre style="border: 1px solid black; padding: 5px;">           autoprov_cfg add template -tn "&lt;Template-Name&gt;" -           otp "&lt;SIC-key&gt;" -ver &lt;Version&gt; -po "&lt;Policy-Name&gt;"           </pre>

Step	Description
4	Reconfigure the network load balancers in SmartConsole of the Security Management Server to use the IP addresses of the load balancers created by the target template.
5	Wait for provisioning to complete and for the policy to install on the new Cloud Firewall Instance Pool instances.
6	<p> <b>Note</b> - In this step, all open connections on the source Cloud Firewall Instance Pool become closed.</p> <p>Shut down the source Cloud Firewall Instance Pool and make sure that traffic flows correctly.</p>
7	<p> <b>Note</b> - Before proceeding, make sure the target Instance Pool handles all traffic (inbound, outbound, East-West) as expected.</p> <p>Delete the CME template of the source Cloud Firewall Instance Pool. For this, run:</p> <pre data-bbox="352 884 1364 945">autoprov_cfg delete template -tn "&lt;Template-Name&gt;"</pre>
8	<p>Delete the corresponding Instance Pool resource.</p> <p> <b>Important</b> - Do <b>NOT</b> delete the stack of the source Cloud Firewall Instance Pool, as it can contain the VCN resources currently in use.</p>


# Configure Cloud Management Extension (CME)

## Downloading and Installing the Latest CME Version

To download and install the CME (Cloud Management Extension) on the Security Management Server or Multi-Domain Server, see [sk157492](#).

## Configuring the CME on the Security Management Server

The instructions below contain information about how to configure an Instance Pool environment in CME. For more information about CME configurations, see the "Overview" section in the [Cloud Management Extension Administration Guide](#).

 **Note** - Configuring CME in the Smart-1 Cloud GUI is not supported for the Cloud Firewall for OCI Instance Pools solution.

### Configure the CME on the Security Management Server with CME API (recommended)

With CME Management API you can configure the CME tool.

#### API Documentation:

- SwaggerHub: [CME API](#)
- Postman Collection: [CME API Postman collection](#)

#### Prerequisites:

- CME Take 139 or higher installed on the Security Management Server.
- Management API version 1.8 or higher installed on the Security Management Server (see the [Check Point Management API Reference](#) (at the top, select the correct version)).

1. To configure Security Management Server during the Cloud Firewall Gateway for Oracle Instance Pool deployment:

**Send a PUT request:**

```
PUT https://<Management_IP_address>/web_api/v1.8/cme-
api/v1.3/management
```

**Request body parameters:**

Parameter Name	Description
name	Your OCI account name (for example, "my-management").

This operation returns "status-code": 200.

## 2. To configure CME on the Security Management Server:

**Send a POST request:**

```
POST https://<Management_IP_address>/web_api/v1.8/cme-
api/v1.3/accounts/oci
```

**Request body parameters:**

Parameter Name	Description
name	Your OCI account name.
compartment	Compartment OCID
region	OCI region
realm_domain	The domain of the realm

Parameter Name	Description
credentials_data	<p>Base64-encoded string of the following JSON:</p> <pre>{ "user": "&lt;USER OCID&gt;", "tenancy": "&lt;TENANCY OCID&gt;", "key": "&lt;CONTENTS OF PRIVATE KEY FILE&gt;" }</pre> <p><b>Note</b> - The value of "key" parameter should begin with "-----BEGIN PRIVATE KEY-----" and end with "-----END PRIVATE KEY-----". To ensure correct parsing, preserve the exact line breaks and spacing. This can be achieved by either copying the key as-is or explicitly appending newline characters (\n) at the end of each line within the key.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li> <p>Directly copying and pasting the API key:</p> <pre>echo -n '{ "user": "ocid1.user.oc1..aaaaa", "tenancy": "ocid1.tenancy.oc1..aaaaa", "key": "-----BEGIN PRIVATE KEY-----&lt;br&gt;&lt;PRIVATE&gt;&lt;br&gt;&lt;KEY&gt;&lt;br&gt;&lt;CONTENT&gt;&lt;br&gt;-----END PRIVATE KEY-----"}'   base64 -w 0</pre> </li> <li> <p>Adding newline characters (\n) to the API key:</p> <pre>echo -n '{ "user": "ocid1.user.oc1..aaaaa", "tenancy": "ocid1.tenancy.oc1..aaaaa", "key": "-----BEGIN PRIVATE KEY-----&lt;br&gt;\n&lt;PRIVATE&gt;&lt;br&gt;\n&lt;KEY&gt;&lt;br&gt;\n&lt;CONTENT&gt;&lt;br&gt;\n-----END PRIVATE KEY-----"}'   base64 -w 0</pre> </li> </ul>

This operation returns "status-code": 200.

### 3. To configure gw\_conf:

#### Send a POST request:

```
POST https://<Management_IP_address>/web_api/v1.8/cme-api/v1.3/gwConfigurations/oci
```

#### Request body parameters:

Parameter Name	Description
name	The name of the relevant set of Instance Pool configurations to apply (for example, "my-configuration-template-for-x").
base64_sic_key	A random value that has at least 8 alphanumeric characters (for example, "MySICkey123").
version	The Cloud Firewall Gateway version.
policy	The name of the policy to install (for example, "Standard").
related_account	Your OCI account to associate with this configuration.

This operation returns "status-code": 200.

**To configure the CME on the Security Management Server with autoprov-cfg**

Step	Description
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	<p>Execute this command (see the explanation of parameters below):</p> <p>Run:</p> <pre>autoprov_cfg init OCI -mn "&lt;Management-Name&gt;" -tn "&lt;Configuration-Template-Name&gt;" -otp "&lt;SIC-key&gt;" -ver &lt;Version&gt; -po "&lt;Policy-Name&gt;" -cn "&lt;Controller-Name&gt;" -co "&lt;Compartment&gt;" -rg "&lt;Region&gt;" -rd "&lt;Realm-Domain&gt;" -cred "&lt;Credentials-File-Data&gt;"</pre> <p>Example:</p> <pre>autoprov_cfg init OCI -mn "my-management" -tn "my-configuration-template" -otp "MySICkey123" -ver R81.20 -po "Standard" -cn "my-oci-controller" -co "ocidl.compartment.oc1..12345" -rg "eu-frankfurt-1" -rd "oraclecloud.com" -cred "eyJ1c..."</pre>
4	<p>When this message shows, type <b>yes</b> and press Enter to apply the modifications:</p> <pre>Would you like to restart the service now?</pre>

Step	Description
5	<p>Confirm the configuration:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>service cme test</pre> </div> <p>Every controller in the configuration must have unique credentials.</p>
6	<p>Follow the instructions in the <i>Enabling and Disabling Software Blades</i> section in the <a href="#">Cloud Management Extension Administration Guide</a>.</p>

**Parameters**

**i Important** - The exact values that you select, must be typed exactly when you deploy the Instance Pool. Make sure to write them down and enter them correctly. Otherwise, the components cannot communicate with each other.

Parameter	Description	Example
"<Management-Name>"	<p>Select a descriptive name.</p> <p>When you deploy the Check Point Instance Pool with this name, the Check Point Security Management Server identifies and automatically provisions it.</p>	"my-management"
"<Configuration-Template-Name>"	<p>Configurations that automatically provision the Cloud Firewall Gateways in the Instance Pool are found in this template.</p> <p>When you deploy the Check Point Instance Pool with this template name, it references the relevant set of configurations to apply to it.</p> <p>Therefore, you can maintain multiple sets of configurations and associate them with different Instance Pools that are managed by the Security Management Server.</p>	"my-configuration-template-for-x"
"<SIC-key>"	<p>Select a random key that has at least 8 alphanumeric characters.</p>	"MySICkey123"
<Version>	<p>The Cloud Firewall Gateway version.</p>	R8X.XX
"<Policy-Name>"	<p>The name of the policy to install.</p> <p>The name of this policy has to be the exact same name of the policy in SmartConsole.</p>	"Standard"

Parameter	Description	Example
"<Controller-Name>"	Select a name that represents the controller. The controller name includes configurations for your OCI environment, such as the compartment OCID and region. You can maintain different controllers to automatically provision different Cloud environments, with the Security Management Server.	"OCI-Production"
"<Compartment>"	The compartment OCID.	"ocid1.compartment.Oc1..abcdefghijklmnopklm"
"<Region>"	An OCI region.	"eu-frankfurt-1"
"<Realm-Domain>"	The domain for the realm.	"oraclecloud.com"

Parameter	Description	Example
<p>"&lt;Credentials-File-Data&gt;"</p>	<p><b>Base64-encoded string of the following JSON:</b></p> <pre>{ "user": "&lt;USER OCID&gt;", "tenancy": "&lt;TENANCY OCID&gt;", "key": "&lt;CONTENTS OF PRIVATE KEY FILE&gt;" }</pre> <p><b>Note</b> - The value of "key" parameter should begin with "-----BEGIN PRIVATE KEY-----" and end with "-----END PRIVATE KEY-----". To ensure correct parsing, preserve the exact line breaks and spacing. This can be achieved by either copying the key as-is or explicitly appending newline characters (\n) at the end of each line within the key.</p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li> <p>Directly copying and pasting the API key:</p> <pre>echo -n '{ "user": "ocid1.user.oc1..aaaaa", "tenancy": "ocid1.tenancy.oc1..aaaaa", "key": "-----BEGIN PRIVATE KEY-----&lt;br&gt;&lt;PRIVATE&gt;&lt;br&gt;&lt;KEY&gt;&lt;br&gt;&lt;CONTENT&gt;&lt;br&gt;-----END PRIVATE KEY-----"}'   base64 -w 0</pre> </li> <li> <p>Adding newline characters (\n) to the API key:</p> <pre>echo -n '{ "user": "ocid1.user.oc1..aaaaa", "tenancy": "ocid1.tenancy.oc1..aaaaa", "key": "-----BEGIN PRIVATE KEY-----&lt;br&gt;\n&lt;PRIVATE&gt;\n&lt;KEY&gt;\n&lt;CONTENT&gt;\n-----END PRIVATE KEY-----"}'   base64 -w 0</pre> </li> </ul>	<p>"eyJ1c..."</p>

# Configure HTTPS Inspection

Follow the steps below to enable HTTPS Inspection.

## Notes:

- If you have an outbound CA certificate you can skip these steps. Otherwise, create one in "Creating an Outbound Certificate."
- Only want inbound SSL inspection.

## Creating an Outbound Certificate

To create an Outbound Certificate

Step	Description
1	In SmartConsole, go to <b>Policy &gt; HTTPs policy</b> .
2	Go to the <b>Destination</b> column, and edit the default rule to be <b>Any</b> .
3	Go to the <b>Track</b> column, and edit to <b>Log</b> .
4	Go to <b>Gateways and Servers</b> . Open one of the VMSS instances you have.
5	Open HTTPs Inspection and click <b>Create Certificate</b> .
6	Enter the information and click <b>OK</b> .
7	Click <b>Enable HTTPs Inspection</b> .
8	Publish the SmartConsole session.
9	Install policy.

## Creating an HTTPS Inspection Rule to Inspect SSL Traffic

This procedure creates an HTTPS Inspection rule to inspect SSL traffic that belongs to a web application

Step	Description
1	In SmartConsole, from the left navigation panel, click <b>Manage &amp; Settings</b> .
2	From the left tree, click <b>Blades</b> .
3	In the <b>HTTPS Inspection</b> section, click <b>Configure in SmartConsole</b> .

Step	Description
4	From the left tree, click <b>Gateways</b> .
5	At the bottom of the page, click <b>Create Certificate</b> .
6	Enter the information and click <b>OK</b> .
7	From the left tree, click <b>Server Certificates</b> .
8	Enter the information and click <b>OK</b> .
9	From the left tree, click <b>Policy</b> .
10	Add this rule: <ul style="list-style-type: none"><li>▪ <b>Source</b> - <i>Any</i></li><li>▪ <b>Destination</b> - <i>Any</i> (do not use the <b>Internet</b> object)</li><li>▪ <b>Service</b> - The HTTPS service you created</li><li>▪ <b>Action</b> - <i>Inspect</i></li><li>▪ <b>Certificate</b> - The certificate you created</li></ul>
11	Save the changes: Click <b>Menu &gt; File &gt; Save</b> .
12	Close the SmartConsole.
13	Publish the SmartConsole session

# IPS Geo Protection Based on X-Forwarded-For HTTP Header

The IPS Geo protection filters and logs traffic based on the country, from each it arrives. This protection is applied to both the source address of the connection, as well as to any IPv4 address present in an '*X-Forwarded-For*' HTTP header.

## Notes:

- The External Load Balancer does not hide the client's original IP address.
- If an HTTP request goes through multiple proxies or Load Balancers, the *X-Forwarded-For* HTTP header is expected to contain multiple IP addresses.
- All IPv4 addresses contained in the *X-Forwarded-For* HTTP header, are inspected by the IPS Geo protection.
- Any IPv6 address in the *X-Forwarded-For* HTTP header is ignored.

For more information, see [sk115532](#) on IPS Geo protection based on *X-Forwarded-For* HTTP header.

## Use Case 1

### Single user

1. A user is located in Dallas (USA), and the client opens a direct connection to the External Load Balancer.
2. The Load Balancer forwards the connection to one of the Check Point Cloud Firewall Gateways and leaves the source IP address unchanged.
3. The IPS Geo protection on the Cloud Firewall Gateway identifies the country of origin as the United States.
4. The Cloud Firewall Gateway allows or drops the connection based on the policy.

## Use Case 2

### Multiple users

1. A user is located in Dallas (USA), and the client opens a direct connection to the External Load Balancer.

The Load Balancer forwards the UserA's connection to one of the Check Point Cloud Firewall Gateways and leaves the UserA's source IP address unchanged.

The IPS Geo protection on the Cloud Firewall Gateway identifies the country of origin as the United States for the UserA's connection.

2. UserB is also located in Dallas (USA), and the client uses a proxy server to connect to the External Load Balancer.

The proxy adds an *X-Forwarded-For* HTTP header to the UserB's connection with the IP address of the UserB's client in Dallas.

The Load Balancer forwards the connection to one of the Cloud Firewall Gateways.

The IPS Geo protection on the Cloud Firewall Gateways identifies the country of origin as the United States for the UserB's connection.

3. The Cloud Firewall Gateway allows or drops the connections based on the policy.

# Limitations of Cloud Firewall for OCI Instance Pools

- Anti-Spoofing is disabled by default on the Instance Pool instances eth0 and eth1 and must not be enabled.
- Configuring CME in the Smart-1 Cloud GUI is not supported for Cloud Firewall for OCI Instance Pools.