

CloudGuard on Huawei Cloud Deployment Guide





Table of Contents

CloudGuard on Huawei Cloud Deployment Guide	1
1. Start configuration of Check Point GW	3
2. Start configuration of Check Point Management	5
3. Unified management gateway	13
4. Policy configuration.....	16

CHECK POINT INTERNAL



1. Start configuration of Check Point GW

Select already created instance, remote connection

Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Operation
hw-gw-1 324f3c2e-44fa-4157-a2ec-022809e855a		AZ2	Stopped	2 vCPUs 4 GB c3.large.2 R8030GW	119.3.247.67 (EIP) 5 Mbit/s 192.168.1.101 (Private IP)	Pay-per-use	Remote Login More
windows-2016 0a8b7d66-7983-4c16-94e1-7652e1689e67		AZ2	Stopped	2 vCPUs 4 GB c3.large.2 Windows Server 2016 Standard 64bit English	49.4.64.111 (EIP) 5 Mbit/s 192.168.2.187 (Private IP)	Pay-per-use	Remote Login More
edge-vpn 9fa48a29-6fa7-43f9-b488-79567c429af3		AZ2	Stopped	2 vCPUs 4 GB c3.large.2 r77208wedge	49.4.111.163 (EIP) 5 Mbit/s 192.168.1.186 (Private IP)	Pay-per-use	Remote Login More
gw-1 33f2d07f42fe-4674-e944-24b1b4fb72ae		AZ2	Stopped	2 vCPUs 8 GB c3.large.4 R8030GW	49.4.71.7 (EIP) 5 Mbit/s 192.168.2.75 (Private IP)	Pay-per-use	Remote Login More
gw-2 e5a7efb8-ee11-4892-b8d0-037747c6506f		AZ2	Stopped	2 vCPUs 8 GB c3.large.4 R8030GW	192.168.2.139 (Private IP)	Pay-per-use	Remote Login More
mgmt 140243e35cd-46da-aad1-3007c5a67b20		AZ2	Stopped	4 vCPUs 8 GB c3.xlarge.2 R8030-mgmt	49.4.51.5 (EIP) 5 Mbit/s 192.168.2.174 (Private IP)	Pay-per-use	Remote Login More

Use public IP of ECS to login the GW with SSH tool, then enter the user name as admin, the password is as admin,

Change password command : set user admin password

```
This system is for authorized use only.  
login: admin  
Password:  
You have logged into the system.  
By using this product you agree to the terms and conditions  
as specified in https://www.checkpoint.com/download_agreement.html  
In order to configure your system, please access the Web UI and finish the First Time Wizard.  
gw-1f5cb7?
```

Login to the web portal with public IP of GW ECS (EIP) through the public network :

<https://EIP>

then enter the user name as admin, the password is as admin. The new password can be set at blow page.

Check Point
SOFTWARE TECHNOLOGIES LTD.
Gaia Portal R80.30

This system is for authorized use only.

Username:

Password:

LOGIN →



Blink Check Point
SOFTWARE TECHNOLOGIES LTD.

Authentication
Configure the Gaia OS password for user "admin"

New Password:

Confirm Password:

Network Configuration

Host Name:

IPv4 Addr (eth0):

Subnet mask:

Default Gateway:

SIC

Activation Key:

Confirm Activation Key:

Configurations

Enable cluster membership for this gateway

Automatically download Blade Contracts and other important data (highly recommended) i

Improve product experience by sending data to Check Point i

Go!

SIC one-time password for managing server connections to gateway devices

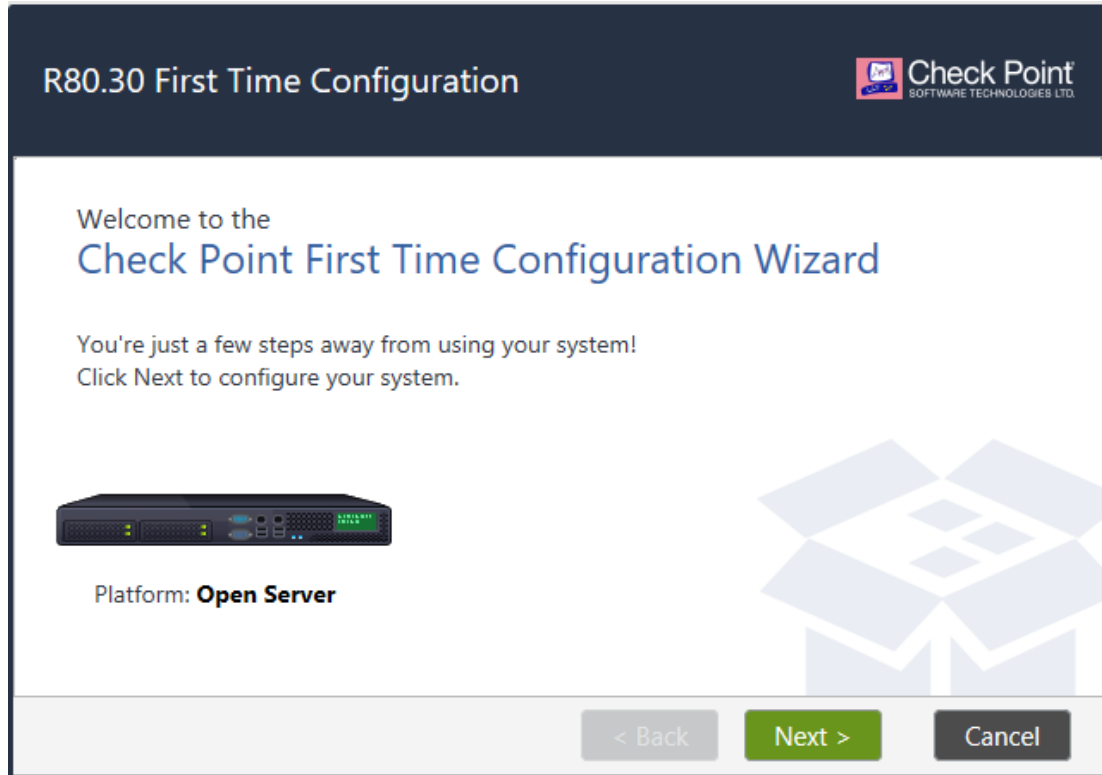


2. Start configuration of Check Point Management

For the management server, the initialization process need to be done at the first time. Login to the web portal with public IP of management ECS (EIP) through the public network :


<https://EIP>

then enter the user name as admin, the password is as admin. According to the blow screenshots to finish the initialization.





Deployment Options



Setup


Continue with R80.30 configuration

Installation

Install from Check Point cloud


Install from USB device

Recovery


Import existing snapshot 

< Back Next > Cancel

Authentication Details



Change the default administrator password:

Password:  Good


Confirm Password:

It is strongly recommended to use both uppercase and lowercase characters as well as one of the following characters in the password: !@#\$%^&*()-_+=+;

< Back Next > Cancel



Management Connection



Interface: eth0

Configure IPv4:

IPv4 address:

Subnet mask:

Default Gateway:


Configure IPv6:

IPv6 Address:

Mask Length:

Default Gateway:

Device Information



Host Name:

Domain Name:

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings


Use a Proxy server

Address:

Port:



Date and Time Settings



Set time manually:

Date:

Time: :

Time Zone:


Use Network Time Protocol (NTP):

Primary NTP server: Version:

Secondary NTP server: Version:

Time Zone:

Installation Type




Security Gateway and/or Security Management

Multi-Domain Server



Products



Products

Security Gateway
 Security Management

Clustering


Unit is a part of a cluster, type:

Define Security Management as:

Automatically download Blade Contracts and other important data (highly recommended)
i For more information click [here](#)

< Back Next > Cancel

Security Management Administrator



Use Gaia administrator: admin
 Define a new administrator


Administrator Name:

New Password:

Confirm Password:

< Back Next > Cancel

Security Management GUI Clients




GUI clients can log into the Security Management from:

- Any IP Address
- This machine
IP address:
- Network
IP Address:
Subnet:
- Range of IPv4 addresses:
 -


< Back Next > Cancel

First Time Configuration Wizard Summary

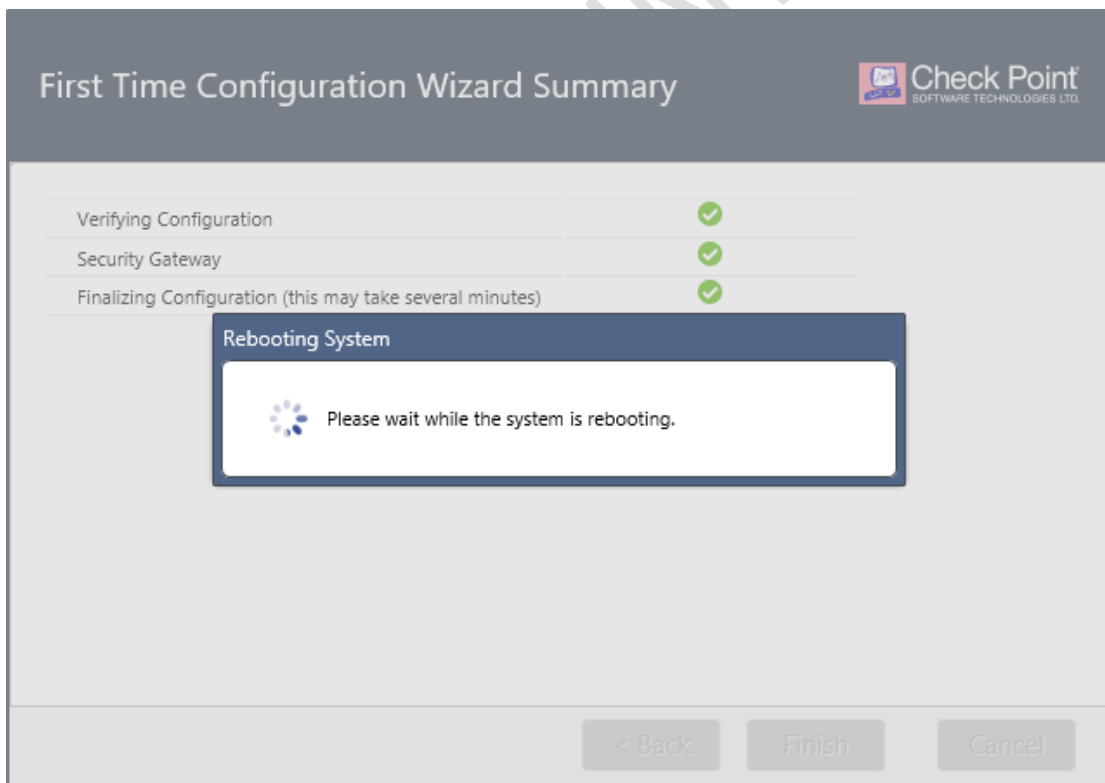
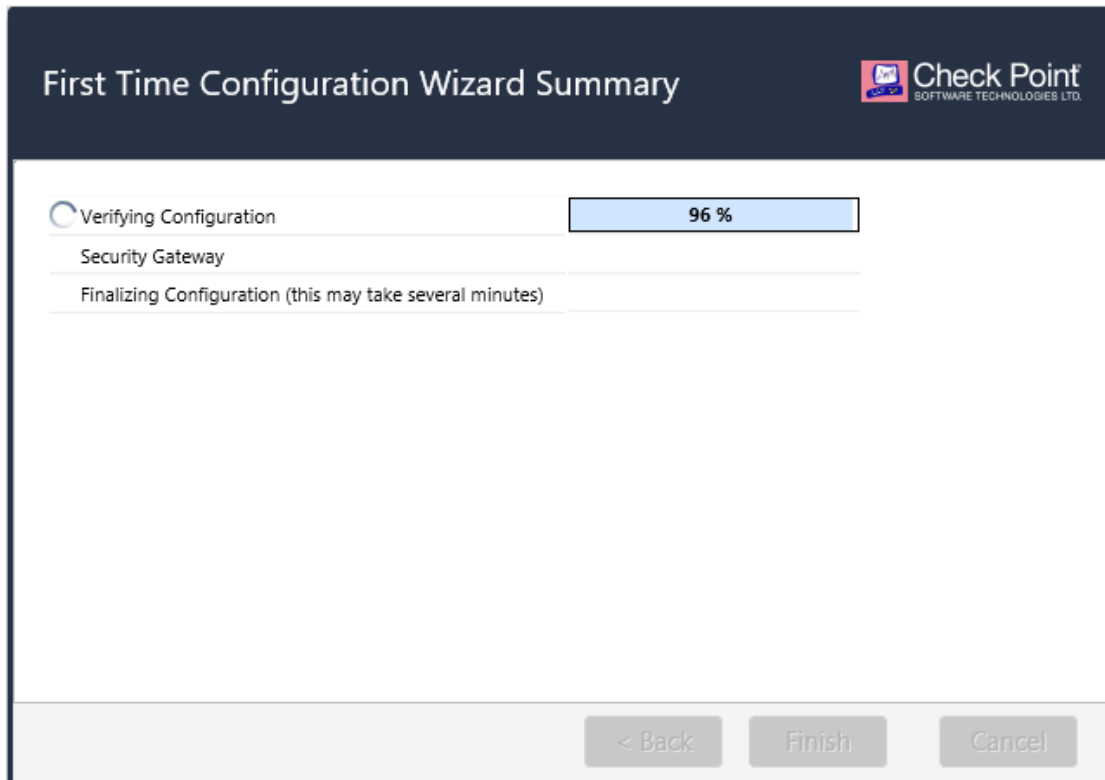


Your device will be configured with the following products:

- Security Gateway

Improve product experience by sending data to Check Point
 For more information click [here](#)


< Back Finish Cancel



Uninstall the default policy (deny all) from the login command line after restart: `fw unloadlocal`



```
This system is for authorized use only.  
login: admin  
Password:  
Last login: Thu Nov 22 07:59:08 on tty1  
You have logged into the system.  
By using this product you agree to the terms and conditions  
as specified in https://www.checkpoint.com/download\_agreement.html  
gw2> fw unloadlocal
```

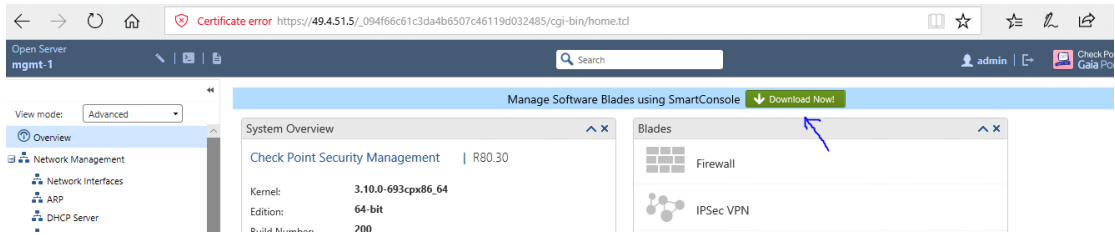


CHECK POINT INTERNAL

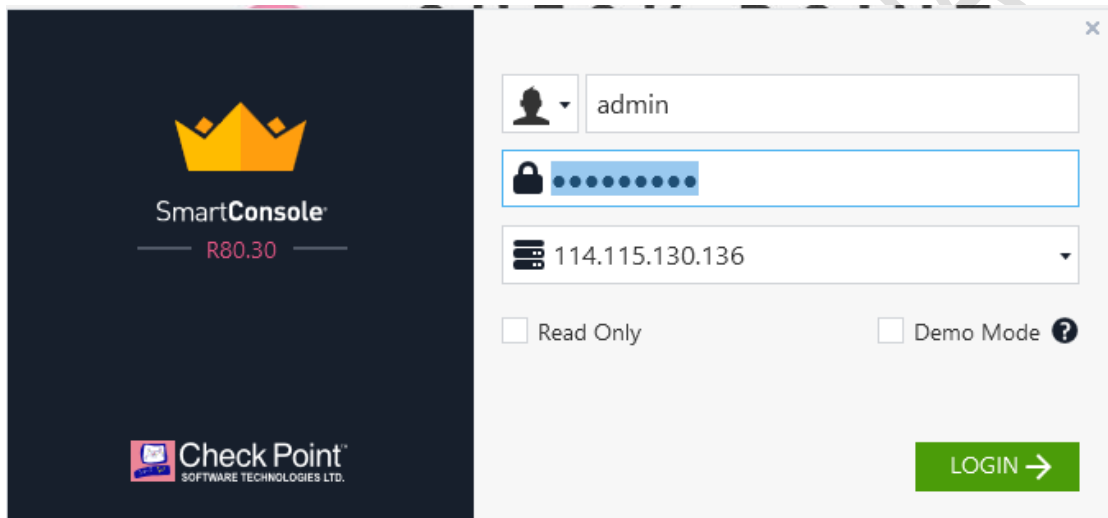


3. Unified management gateway

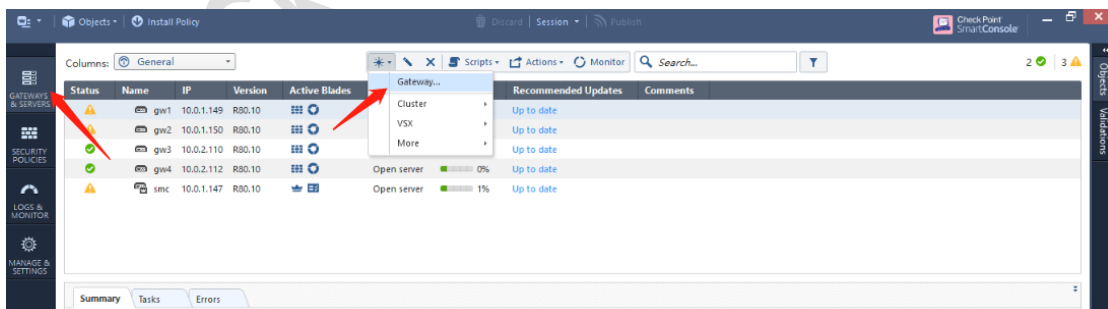
Download the Smart Console from the Check Point website or web UI and install it.



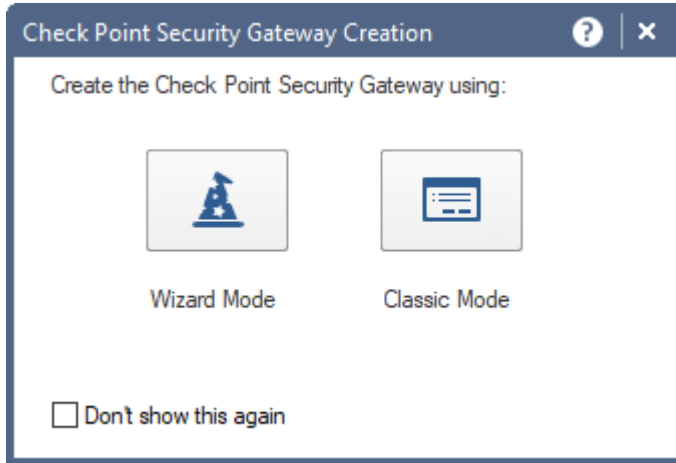
After installation, open it and login Smart Console with username, password and IP of management gateway.



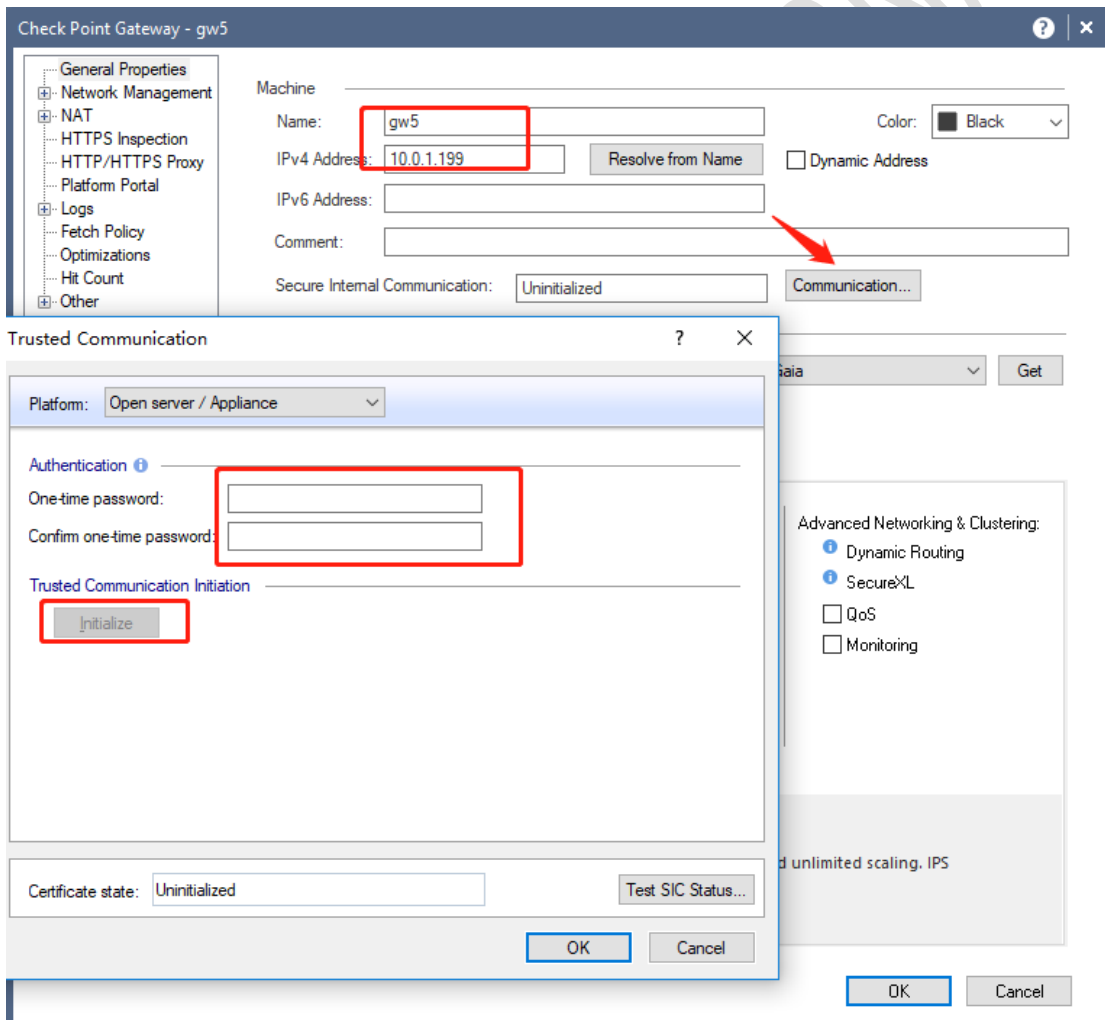
Add Gateway object



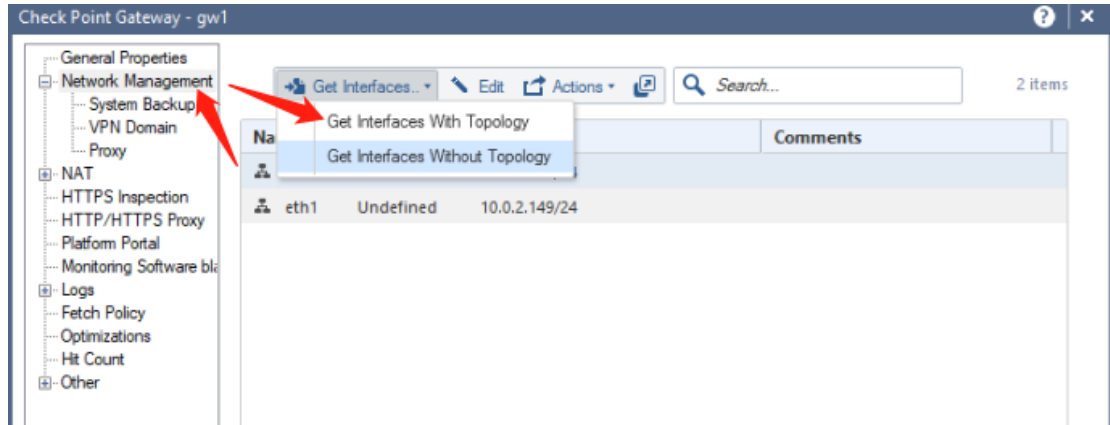
Classic mode is usually chosen



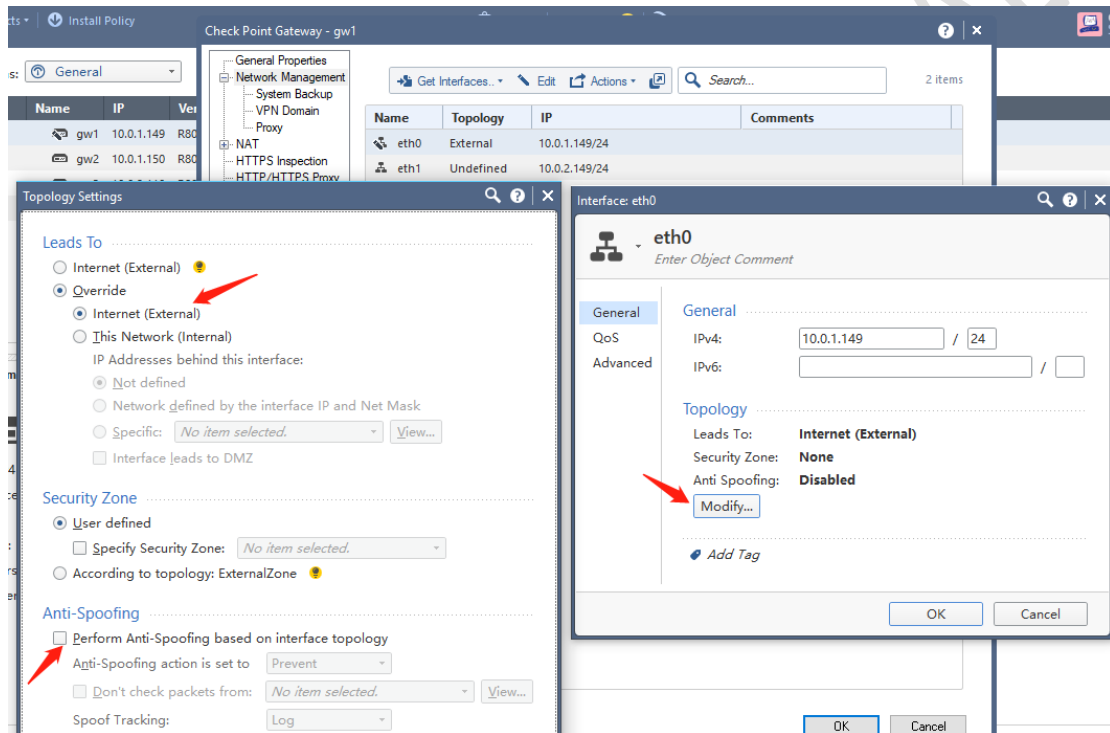
Enter the hostname and IP of the instance without error, select communication, enter the one-time secret key created when initializing the gateway and click initialize, then click ok



Then get interface with topology

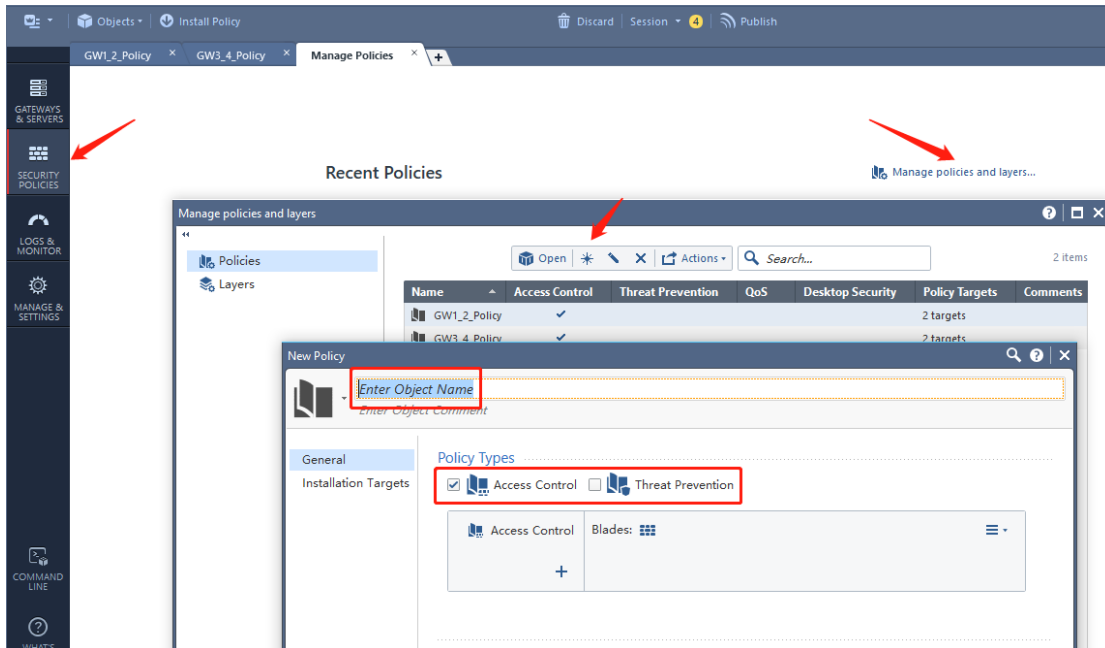


Disable anti spoofing

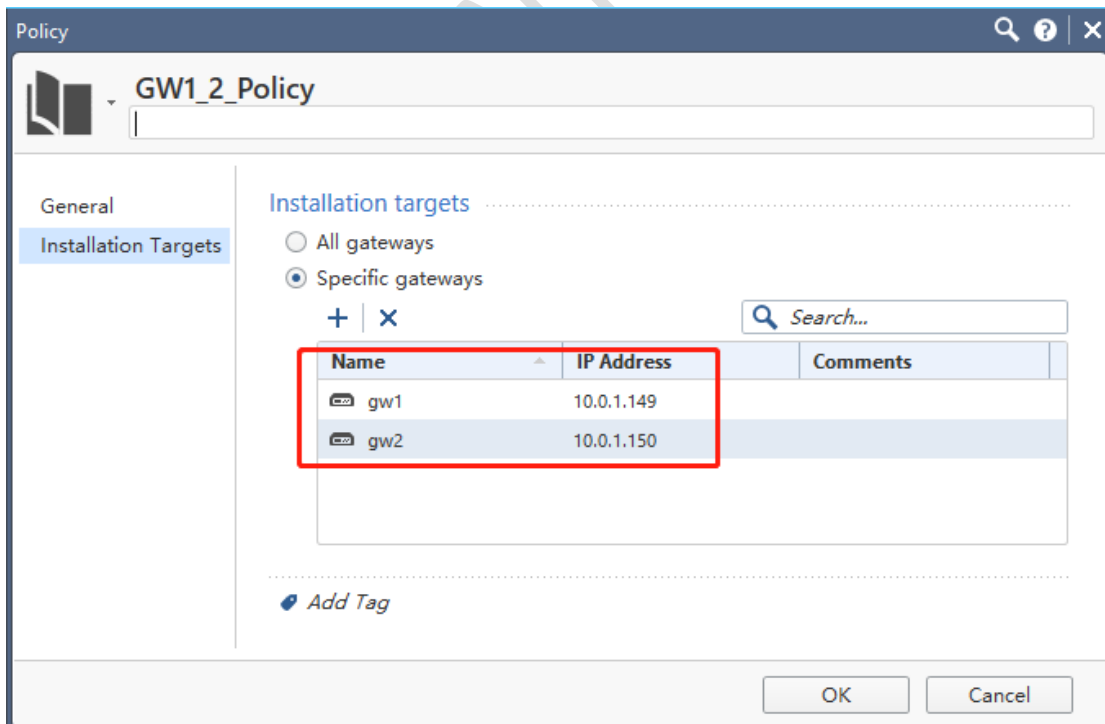


4. Policy configuration

You can create a policy package for the gateway, such as the name GW1_2_Policy



Select GW1 and GW2 (please carefully select gateway objects managed by the policy package)



The same method creates the policy packages for GW3 and GW4, which are currently permit any

Recent Policies

[Manage policies and layers...](#)

Name	Policies	Gateways
GW3_4_Policy		2 targets
GW1_2_Policy		2 targets

Create NAT Policy

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
1	All_Internet	H_10.0.1.149	TCP_8088	H_10.0.2.149	H_10.0.2.1	TCP_8088	gw1	
2	All_Internet	H_10.0.1.150	TCP_8088	H_10.0.2.111	H_10.0.2.1	TCP_8088	gw2	

Automatic Generated Rules : Machine Static NAT (No Rules)
 Automatic Generated Rules : Machine Hide NAT (No Rules)
 Automatic Generated Rules : Address Range Static NAT (No Rules)
 Automatic Generated Rules : Network Static NAT (No Rules)
 Automatic Generated Rules : Address Range Hide NAT (No Rules)
 Automatic Generated Rules : Network Hide NAT (No Rules)
 Manual Lower Rules (No Rules)

Instructions :

- The original source, destination and service are the source IP (in this case, All_Internet, please do not write any, otherwise the policy will fail), destination IP (the upper IP of GW1 and GW2), and the published application port
- Translated source, destination and service are converted source IP (in this case, GW1 and GW2), destination IP (Nginx listening IP), port (Nginx listening port)
- Select the appropriate install object

The NAT entries for GW3 and GW4 are as follows, with the policy permit any

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
1	All_Internet	H_10.0.2.110	TCP_8080	H_10.0.3.125	H_10.0.3.11	Original	gw3	
2	All_Internet	H_10.0.2.112	TCP_8080	H_10.0.3.126	H_10.0.3.11	Original	gw4	

Automatic Generated Rules : Machine Static NAT (No Rules)
 Automatic Generated Rules : Machine Hide NAT (No Rules)
 Automatic Generated Rules : Address Range Static NAT (No Rules)
 Automatic Generated Rules : Network Static NAT (No Rules)
 Automatic Generated Rules : Address Range Hide NAT (No Rules)
 Automatic Generated Rules : Network Hide NAT (No Rules)
 Manual Lower Rules (No Rules)

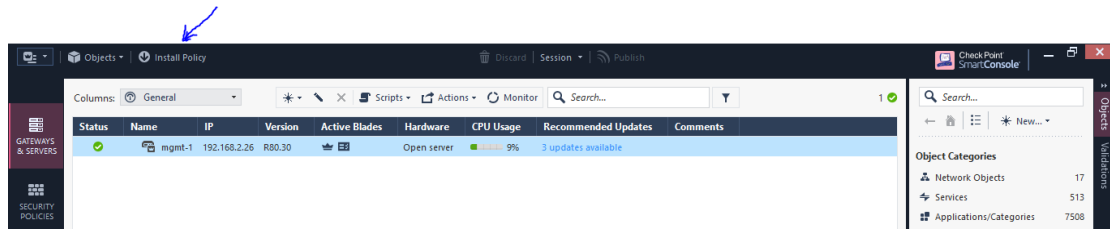
Instructions :

- The original source, destination and service are the source IP (in this case, All_Internet, please do not write any, otherwise the policy will fail), destination IP (the upper IP of GW3 and GW4), and the published application port
- Translated source, destination and service are translated source IP (in this case, GW3 and GW4), destination IP (web server), service (application port)
- Select the appropriate install object



CloudGuard on Huawei Cloud Deployment Guide

Configuration completed, the policy can be published :



CHECK POINT INTERNAL



Copyright

Any text description, document format, illustrations, photos, methods, codes and other contents appearing in this document shall be copyrighted by Check Point and protected by relevant property rights and copyright laws, unless otherwise specified. No individual or institution may copy or reference any fragment of this document in any way without the written permission of Check Point.

CHECK POINT INTERNAL