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 ...................................................................... 12
4. Policy configuration ...................................................................................... 15
1. Start configuration of Check Point GW

Select already created instance, remote connection

Enter the user name admin, the password is admin,
Change password command: set user admin password

Login to the web portal through the public network:
SIC one-time password for managing server connections to gateway devices
2. Start configuration of Check Point Management
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: !@#$%^&*()_+=~.

Management Connection

Interface: eth0
Configure IPv4: Manually
IPv4 address: 192.168.2.25
Subnet mask: 255.255.255.0
Default Gateway: 192.160.2.1
Configure IPv6: Off
IPv6 Address:
Mask Length:
Default Gateway:
Device Information

- **Host Name:** mgmt-1
- **Domain Name:** Optional
- **Primary DNS Server:** 100.125.1.250
- **Secondary DNS Server:** 100.125.21.250
- **Tertiary DNS Server:**

Proxy Settings

- **Use a Proxy server**
  - **Address:**
  - **Port:** 8080

Date and Time Settings

- **Set time manually:**
  - **Date:** Wednesday, November 21, 2018
  - **Time:** 20:19
  - **Time Zone:** Shanghai, Asia (GMT +8:00)

- **Use Network Time Protocol (NTP):**
  - **Primary NTP server:** http://cloud.aliyun.com
    - **Version:** 4
  - **Secondary NTP server:** http://1.cloud.aliyun.com
    - **Version:** 4
  - **Time Zone:** Taipei, Asia (GMT +8:00)
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: ClusterXL
- Define Security Management as: Primary

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

<br>

First Time Configuration Wizard Summary

- Verifying Configuration
  - Security Gateway: 96%
  - Finalizing Configuration (this may take several minutes)

<br>

< Back  Finish  Cancel

< Back  Finish  Cancel
Uninstall the default policy (deny all) from the login command line after restart: `fw unloadlocal`
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
Create NAT Policy

**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.

**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.
Configuration completed, the policy can be published:
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.