CloudGuard on Huawei Cloud Deployment Guide





Table of Contents

Clou	dGuard on Huawei Cloud Deployment Guide	1
	Start configuration of Check Point GW	
	Start configuration of Check Point Management	
	Unified management gateway	
	Policy configuration	



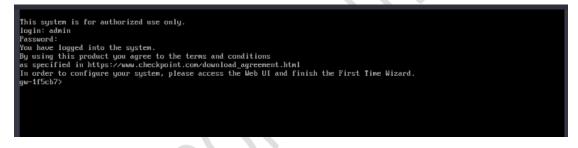
1. Start configuration of Check Point GW

Select already created instance, remote connection

The	Tab View is now available to experience on the ECS	console. Provide feedba	ck on the new view.						
Star	t Stop Reset Password M	lore 🔻						C	00
Searc	hed by name by default.								
	Name/ID	Monitoring	AZ 7	Status 🖓	Specifications/Image	IP Address	Billing Mode 7	Operation	
~	HW-gw-1 324f3c2e-44fb-4157-a2ec-022b809e855a	B	AZ2	Stopped Stopped	2 vCPUs 4 GB c3.large.2 R8030GW	119.3.247.67 (EP) 5 Mbit/s 192.168.1.101 (Private IP)	Pay-per-use	Remote Login	More -
	windows-2016 0a8b7d66-7983-4c16-94e1-7b52e1689e67	四	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 9fa48a20-6fa7-43f9-b488-70567c429a93	Ø	AZ2	Stopped	2 vCPUs 14 GB 1 c3.large 2 v772089edge	49.4.11.163 (EIP) 5 Mbit/s 192.168.1.186 (Private IP)	Pay-per-use	Bemote Login	More •
	gw-1 3372d07142fe-4674-a944-24b1b4fb72ae	國	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 65a7efbb-ee11-4f82-bbf0-037747c6506f	Ø	AZ2	Stopped	2 vCPUs 8 GB c3.large.4 R8030GW	192.168.2.139 (Private IP)	Pay-per-use	Remote Login	More •
	mgmt 14024#3e-35cd-4dda-aa81-3007c5a57b20	8	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



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.

	1 This system is for authorized use only.
Gaia Portal R80.30	Username: admin Password: ••••• LOGIN →



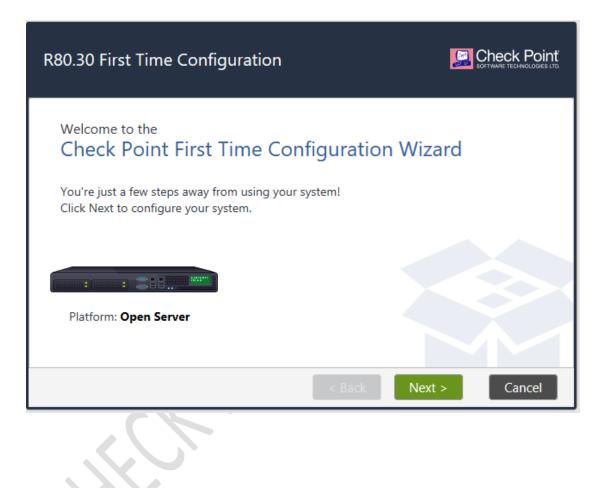
‡ Blink	
Authentication Configure the Gaia OS password for user "admin" New Password: Confirm Password: SIC	Network ConfigurationHost Name:gw-1IPv4 Addr (eth0):192.168.2.212Subnet mask:255.255.255.0Default Gateway:192.168.2.1Configurations
Activation Key: Confirm Activation Key:	Enable cluster membership for this gateway
 Automatically download Blade Contracts and other im Improve product experience by sending data to Check 	

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



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			Check Point SOFTWARE TECHNOLOGIES LTD.
Setup Continue with R80.30 Installation Install from Check Po Install from USB device Recovery Import existing snaps	int cloud e			
		< Back	Next >	Cancel
			-	
Authentication	n Details			Check Point
Authentication				Check Point SOFTWARE TECHNOLOGIES LTD.
			Good	Check Point SOFTWARE TECHNOLOGIES LTD
Change the default admi Password: Confirm Password: It is strongly recommence	inistrator password:	ase characters as we	Good	Check Point Software technologies LTD
Change the default admi Password: Confirm Password: It is strongly recommence	inistrator password:	ase characters as we	Good	Check Point Software technologies LTD
Change the default admi Password: Confirm Password: It is strongly recommence	inistrator password:	ase characters as we	Good	Check Point Software technologies LTD



Management	t Connection			Poinť ologies lta
Interface:	eth0			
Configure IPv4:	Manually 🗸			
IPv4 address:	192,168,2,26			
Subnet mask:	255, 255, 255, 0			
Default Gateway:	192,168, 2, 1			
Configure IPv6:	Off 👻			
IPv6 Address:				
Mask Length:				
Default Gateway:				
		Deale		
		< Back	Next > Can	icel
Device Inforn	nation			Poinť
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			
		< Back	Next > Can	cel



Date and Time S	Settings			
 Set time manually: Date: Time: Time Zone: 	Wednesday, November 21, 2018 20 : 19 Shanghai, Asia (GMT +8:00)	3	•	
Use Network Time Protoc Primary NTP server: Secondary NTP server: Time Zone:		Version: Version:	4 ~	
		< Back	Next >	Cancel
Installation Type	e			
Installation Type Security Gateway and/or Multi-Domain Server				Check Point SOFTWARE TECHNOLOGIES LTD
Security Gateway and/or				



Products		
Products		
Security Management		
Clustering		
Unit is a part of a cluster, type:	ClusterXL	
Define Security Management as:	Primary 👻	
 Automatically download Blade Contr For more information click <u>her</u> 	racts and other important data (highly recommer r <u>e</u>	nded)
	< Back	Next > Cancel
		-
Security Management	t Administrator	
Security Management	t Administrator	BOFTWARE TECHNOLOGIES LTD
 Use Gaia administrator: admin Define a new administrator 	t Administrator	BOFTWARE TECHNOLOGIES LTD
 Use Gaia administrator: admin Define a new administrator Administrator Name: 	t Administrator	BOFTWARE TECHNOLOGIES LTD
Use Gaia administrator: admin Define a new administrator Administrator Name: New Password:	t Administrator	BOFTWARE TECHNOLOGIES LTD.
 Use Gaia administrator: admin Define a new administrator Administrator Name: 	Administrator	Check Point oftware technologies ltd
 Use Gaia administrator: admin Define a new administrator Administrator Name: New Password: 	Administrator	Check Point Software technologies ltd
 Use Gaia administrator: admin Define a new administrator Administrator Name: New Password: 	Administrator	CRECK POINT OFTWARE TECHNOLOGIES LTD
Use Gaia administrator: admin Define a new administrator Administrator Name: New Password:	Administrator	CONTRACTOR
Use Gaia administrator: admin Define a new administrator Administrator Name: New Password:	Administrator	



Security Man	agement GUI Clients	
GUI clients can log ir	nto the Security Management from:	
Any IP Address		
This machine		
IP address:	221.221.146.189	
Network		
IP Address:		
Subnet:		
Range of IPv4 addre	esses:	
	< Back	Next > Cancel
	- firm the Mirrord Commence	Check Point
First Time Co	onfiguration Wizard Summary	Check Point BOFTWARE TECHNOLOGIES LTD.
First Time Co	onfiguration Wizard Summary	Check Point BOFTWARE TECHNOLOGIES LTD.
	onfiguration Wizard Summary	Check Point BOFTWARE TECHNOLOGIES LTD.
Your device will be cor		Check Point BOFTWARE TECHNOLOGIES LTD.
Your device will be cor		Check Point BOFTWARE TECHNOLOGIES LTD
Your device will be cor		Check Point BOFTWARE TECHNOLOGIES LTD.
Your device will be cor		Check Point Software technologies ltd
Your device will be cor		Check Point Bottware technologies ltd
Your device will be cor		CHECK POINT OTTWARE TECHNOLOGIES LTD
Your device will be cor		
Your device will be con Security Gateway	nfigured with the following products:	CORCEA POINT DETURARE TECHNOLOGIES LTD
Your device will be con Security Gateway	nfigured with the following products: xperience by sending data to Check Point	

< Back

Cancel



First Time Configuration Wizard Su	ımmary		Check Point Software technologies ltd.
Verifying Configuration Security Gateway Finalizing Configuration (this may take several minutes)	96 %		
First Time Configuration Wizard Su	< Back	Finish	Cancel Check Point
Verifying Configuration Security Gateway Finalizing Configuration (this may take several minutes) Rebooting System	© ©		
Please wait while the system	is rebooting.		

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



3. Unified management gateway

Download the Smart Console from the Check Point website or web UI and install it $_{\circ}$

$\leftarrow \ \rightarrow $	0	8	Certificat	te error https://49.4.51.5/_094f66c61c3da4b65	07c46119d032485/cgi-bin/home.tc			□☆ ⊈	LE
Open Server mgmt-1		N 2			Search			👤 admin [-	 Check Po Gaia Poi
View mode:	Advanced	•	44		Manage Software Blade	es using Sma	rtConsole 🔸 Download Now!		
Overview			^	System Overview	^×	Blades	~	~ × ~	
Network M Network				Check Point Security Management	R80.30		Firewall		
ARP				Kernel: 3.10.0-693cpx86_64 Edition: 64-bit Puild Number 200		100	IPSec VPN		

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

Smart Console R80.30		×
	Read Only	Demo Mode 🛿
		LOGIN ->

Add Gateway object

© <u>:</u> - ∣	🎓 Objects • 🛛 🕙 Install Policy							Û	j Dis	icard Session 🔹 🏐 Publi	sh		Check Point Smart Console			
800	Columns: Status	General Name	IP	• Version	Active Blades	*•	Sateway		ots ≠	Actions - O Monitor Recommended Updates	Q Search	T		2 🕗	3 🔺	Object
GATEWAYS & SERVERS SECURITY POLICIES LOGS & MONITOR	313005 A O O A	ම gw1 ම gw2 ම gw3 ම gw4	10.0.1.149 10.0.1.150 10.0.2.110 10.0.2.112 10.0.1.147	R80.10 R80.10 R80.10 R80.10			Cluster VSX More n server		, %	Up to date Up to date Up to date Up to date Up to date Up to date	Commens					s Validations
	Summa	ry Tasks	Errors												2	

Classic mode is usually chosen



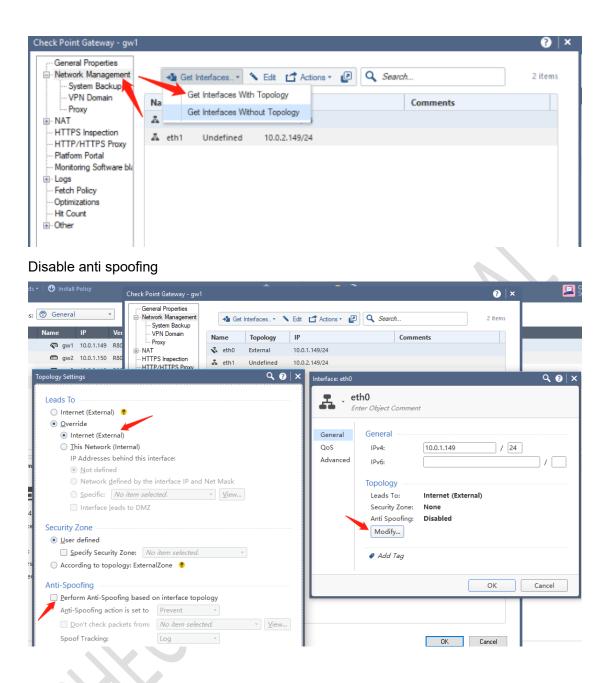


Enter the hostname and IP of the instance without error, select communication, enter the one-time secret key created when initializing the gateway and click initialize, then click ok

Check Point Gateway - gw	j	
General Properties → Network Management → NAT HTTPS Inspection HTTP/HTTPS Proxy → Platform Portal → Logs → Fetch Policy → Optimizations	Machine Name: gw5 IPv4 Address: 10.0.1.199 Resolve from Name IPv6 Address: Comment:	Color: Black ~
Hit Count ⊕ Other	Secure Internal Communication: Uninitialized	Communication
Trusted Communication Platfom: Open server / Appendix Authentication One-time password: Confirm one-time password: Trusted Communication Initia Initialize		Advanced Networking & Clustering:
Certificate state: Uninitialize	d Test SIC Status OK Cancel	d unlimited scaling. IPS
		OK Cancel

Then get interface with topology







4. Policy configuration

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

≌: *	🎁 Objects • 🕻	Install Policy		童 D	iscard Session 🝷 👍 🏹	Publish	
_	GW1_2_Policy	× GW3_4_Policy	× Manage Policies × +				
GATEWAYS & SERVERS							
SECURITY POLICIES			Recent Policies			06 м	anage policies and layers
LOGS & MONITOR		Manage policies an	d layers			Search	
MANAGE & SETTINGS		💦 Policies	Name	 Access Control 	K X C Actions • ol Threat Prevention	QoS Desktop Security	Policy Targets Comments 2 targets
			New Policy Enter Object Nau Emer Object Com	ne			2 tarnets
					Blades: :::]	=.
				🛄 Access Control 🕂	Blades:		=-
⑦ WHAT'S				****			

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

Policy				♀
GW1_2_	Policy			
General Installation Targets	 Installation targets All gateways ● Specific gateways + × 		🔍 Search	
	Name	 IP Address 	Comments	
	inanie gw1	10.0.1.149	connents	
	₪ gw2	10.0.1.150		
	Add Tag			
			ОК	Cancel

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_Po	licy 🗰	📼 2 targets
GW1_2_Po	licy 🔛	📼 2 targets

Create NAT Policy

- Access Control		+=	• × <u>∓</u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u>	Actions • Search for	or IP, object, action,		٩, ٧	^ T			
Policy	No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin	Translated Services	Install On	Comments		
NAT NAT	1	 All_Internet 	₩ H_10.0.1.149	← TCP_8088			← TCP_8088	📾 gw1			
	2	 All_Internet 	₩ H_10.0.1.150					📾 gw2			
hared Policies	Autom	Automatic Generated Rules : Machine Static NAT (No Rules)									
🖉 Geo Policy	Autom	atic Generated Rules : Mad	hine Hide NAT (No Rul	es)							
	Autom	Automatic Generated Rules : Address Range Static NAT (No Rules)									
	Autom	atic Generated Rules : Net	work Static NAT (No Ru	les)							
	Autom	atic Generated Rules : Add	ress Range Hide NAT (N	No Rules)							
	Autom	atic Generated Rules : Net	work Hide NAT (No Rule	es)							
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

GW3_4_Policy × Manage Policies × +												
	Later X I → Lat Actions - Search for IP, object, action,											
N	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		🖶 _s H_10.0.3.11	= Original	📾 gw3				
	2	All_Internet	₩ H_10.0.2.112	┿ TCP_8080		🖶 _s H_10.0.3.11	= Original	📼 gw4				
	Automatic	Generated Rules : Macl	nine Static NAT (No Rul	es)								
	Automatic	Generated Rules : Macl	hine Hide NAT (No Rule	is)								
ettings 🖻	Automatic Generated Rules : Address Range Static NAT (No Rules)											
-	Automatic	Generated Rules : Netw	ork Static NAT (No Rul	es)								
	Automatic	Generated Rules : Addr	ess Range Hide NAT (N	o Rules)								
	Automatic	Generated Rules : Netw	ork Hide NAT (No Rule	s)								
	Manual Lo	wer 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



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.