



Overview

You can discover Checkpoint Firewall R80 to your NetBrain domains and visualize the device data and topology on dynamic maps. This guide introduces the way of discovering Checkpoint Firewall R80 to your NetBrain domain.

Supported Firewall Modes

The system can discover Checkpoint Firewall R80 in the following deployment modes:

- Physical Mode
- Cluster Mode
- VSX
- VSX Cluster

Note: NetBrain does not support the firewalls in the Bridge mode.

Discovery Flow

The pseudo-code below describes a high-level flow to discover Checkpoint Firewall R80, including configurations at both <u>Checkpoint Manager</u> side and <u>NetBrain</u> side.

1. Checkpoint Manager Side:

- 1.1 Set account permission.
- 1.2 Enable and set API access permission.
- 2. NetBrain Side:
 - 2.1 Configure API Server Manager for Checkpoint Firewall R80.
- 3. Discover Checkpoint Firewall R80
- 4. Run a benchmark for Checkpoint Firewall R80

1. Configurations at Checkpoint Manager Side

Before discovering Checkpoint Firewall R80, you need to set up an account and API access permission in your Checkpoint Manager so that your NetBrain system has access to the Checkpoint Management Domain. The configurations for a single domain and multi-domain are somewhat different. Select the configuration steps based on your actual domain scenario.

- <u>Single Domain Configurations</u>
- <u>Multi-domain Configurations</u>

Single Domain Configurations

Assign permissions to the account that you will use for your NetBrain system to access the Checkpoint data.
 You can select any of the three permissions shown in the figure below.

	object comment				
ieneral	Authentication				
Additional Info	Authentication Method:	Check Point Passwo	rd *]	
	Password is defined	Set New Password	.]		
	Certificate Information:				
	O Certificate is not defined	Create			
	Permissions				
	Permission Profile:	Read Write All		*	0
		Q		New	
	Never Expire At: 12/31/2030	Read Only All Read Write All			
		to a second to second the second to be			

2. Enable API access to accept API calls from your NetBrain Front Server. Select the **All IP addresses** or **All IP** addresses that can be used for **GUI clients** option.

TEWAYS SERVERS		Application Control & URL Filtering Advanced Settings	
	 Q View Sessions Q Advanced Q Revisions Tags 	Content Awareness Advanced Settings	
OGS & ONITOR	 Preferences Sync with UserCenter 	O Threat Prevention Advanced Settings	
		Data Loss Prevention	Q 0 X
		Configure in SmartDashboard	Automatic start Access Settings Accept API calls from:
		Settings	Management server only All IP addresses that can be used for GUI clients All IP addresses
		Management API Advanced Settings	OK Cancel

Note: If you select the All IP address that can be used for GUI clients option, add the IP address of NetBrain Front Server to the Trusted Clients so that it has the GUI permission.

- 🎯 Permissions & Administrators	Trusted Clients			* `	× Q Search
Administrators	Client Name Client Type	Value	Comment		
Rermission Profiles	Netbrain_FS IPv4 Address	10.10.4.41			
Trusted Clients	📮 any 🛛 Any	Any			
Advanced					
III Blades					
• 🔂 Sessions					
C View Sessions		Trusted Cl	ient		۹. 🤋
Advanced			-80V-11		
			NI di CC		
G Revisions			• Netbrain_FS	vent	
 Revisions Tags 			• Netbrain_FS Enter Object Comm	ient	
 Revisions Tags Preferences 		Gene	• Netbrain_FS Enter Object Comm	nent	
 Revisions Tags Preferences Sync with UserCenter 		Gene	Netbrain_FS Enter Object Comm ral	ient	
 Revisions Tags Preferences Sync with UserCenter 		Gene Type	Netbrain_FS Enter Object Comm ral IPv4 Addre	ess •	
 Revisions Tags Preferences Sync with UserCenter 		Gene Type IPv4	Netbrain_FS Enter Object Comm ral IPv4 Addre Address: 10.10.4.41	ess *	Resolve from name
 Revisions Tags Preferences Sync with UserCenter 		Gene Type IPv4	Netbrain_FS Enter Object Comm ral :: IPv4 Addres: 10.10.4.41 dd Tag	ess •	Resolve from nam

3. Log into Smart Dashboard via SSH with an SSH/Telnet tool and execute the api restart command to make

API access permission take effect.



Multi-Domain Configurations

1. Assign permissions to the account that you will use for your NetBrain system to access the Checkpoint data.

One of the following permissions is required:

- Domain Manager
- Global Manager
- Domain Super User
- Multi-Domain Super User

c	Authoptication			
General Additional Info	Authentication Method:	Check Point Password	-	
	Password is defined	Set New Password		
	Certificate Information:			
	O Certificate is not defined	Create		
	Permissions			
	Multi-Domain Permission Profile:	🔒 Multi-Domain Super	User 🔹	0
	Full permissions on the entire	Q	New	
	full permissions on the entir Expiration	A Multi-Domain Super U	New Jser]
	 Full permissions on the entir Expiration Never 	Q Multi-Domain Super U	New Jser	
	 Full permissions on the entir Expiration Never Expire At: 9/17/2021 	Q Image: Super User Image: Domain Super User Image: Global Manager	New	
	 Full permissions on the entir Expiration Never Expire At: 9/17/2021 9/17/2021 	Multi-Domain Super U Domain Super User Global Manager Domain Manager	New	

Note: If you cannot discover the devices or retrieve data with a permission, promote the permission to give a try.

2. Enable API access to accept API calls from your NetBrain Front Server. Select the **All IP addresses** or **All IP** addresses that can be used for **GUI clients** option.

Q: •		
	Compliance Settings Inactive Objects Management API	<u>୧</u> ଡ଼ା×
Advanced Advanced MI Blades Controor Contr	Advanced Settings	Startup Settings Automatic start Access Settings Accept API calls from: Management server only All IP addresses that can be used for GUI clients All IP addresses OK Cancel

Note: If you select the **All IP address that can be used for GUI clients** option, add the IP address of NetBrain Front Server to the Trusted Clients so that it has the GUI permission.

S Domains	Trusted Clients					*	1)	< Q Se	arch
R Global Assignments	Client Name	Client Type	Value		Comment				
- 🌣 Permissions & Administrators	😋 AnyHost	Any	Any						
2 Administrators	Netbrain_FS	IPv4 Address	10.10.4.41						
Permission Profiles									
R Trusted Clients			Tr	usted Client					٩
Advanced									
Blades				Net	Drain_FS				
→ C Sessions				-V Linter	object comment				
View Sessions				General					
Advanced				Tan	ID-A Address				
O Revisions				type:	IPV4 Address				1
Tags				IPv4 Address:	10.10.4.41		R	esolve from	name
O Preferences				Domains Ass	ianment				
Sync with UserCenter				+ ×	and the second		Q Sec	arch	
				Name		4	Comm	ents	
				📉 All Doma	ins		Catego	ry includes	all Domains,
				S Domain1					
				S Domain2					
				Additional Se	ttings				
				Multi-Dom	ain Server Trustee	Clien	ıt		
							-		

3. Log into Smart Dashboard via SSH with an SSH/Telnet tool and execute the api restart command to make

API access permission take effect.

疴 10.10.32.151 - SecureCRT

File Edit View Options Transfer Script Tools Window Help This system is for authorized use only. Last login: Thu Aug 29 10:44:56 2019 from 10.10.4.41 CPR80_MDS_Test> CPR80_MDS_Test> CPR80_MDS_Test> api restart 2019-Aug-29 16:12:02 - Stopping API... 2019-Aug-29 16:12:06 - API stopped successfully. 2019-Aug-29 16:13:15 - API started successfully. CPR80_MDS_Test>

2. Configurations at NetBrain Side

NetBrain discovers Checkpoint Firewall R80 using both Checkpoint Manager APIs and CLI/SNMP. After completing configurations at Checkpoint Manager side, you need to configure Network Settings and an API Server Manager for Checkpoint Firewall R80 in NetBrain.

Configure Network Settings

Configure network settings, such as SSH/Telnet Login, Privilege Login, and SNMP String credentials, for Checkpoint Firewall R80.



Configure API Server Manager

The API Server Manager contains the endpoints and credentials to access Checkpoint Management Domain during

the discovery.

Follow the steps below to configure the API Server Manager:

 In the Domain Management page, select **Operations > Discover Settings >API Server Manager** from the quick access toolbar.

Domain Management		Ten	ant: Initial Tenant	Domain: L2_mimic	Operations
Start Page				Start Page	
5				Discover	
Domain: L2_mimic	Maximum Nodes: 1000 Description:		Network Settings	Discover Settings	>
			Do-Not-Scan	Fine Tune	
			Network Definition	n Topology Manage	r >
Discover	S Fine Tune	Site	API Server Manage	er Site Manager	
				Schedule Task	
• 0	9 267	• 0		Benchmark Tools	>
U	3 07	•• 0		Advanced Tools	>
Last discovered	Fully Accessed Devices	Sites		Domain Settings	>
Result Not Executed	Yet Discovered by SNMP Only 21	Container Sites 0	Discover	y Ta Share Policy	

2. Click Add on the API Server Manager tab. The Add External API Server dialog opens.

Add External API Server				×			
Server Name:	Checkpoint R80						
Description:	Discover checkpoint firewa	over checkpoint firewall R80 to a domain.					
API Source Type:	CheckPoint R80 API	heckPoint R80 API					
Endpoints:	https://10.10.32.157	:ps://10.10.32.157					
Username:	admin	Password:					
Front Server/Front Server Group:	WIN-BHURUGCTRE6(10).10.17.77)		\sim			
──── Advanced ∨ Managed Devices: 0							
Test			Cancel	ОК			

- 1) Enter a unique name in the **Server Name** field.
- 2) Enter a description of the API server.
- 3) Select **CheckPoint R80 API** from the **API Source Type** drop-down menu.

In the **Endpoints** field, enter the address of the Checkpoint Management Domain. The format is https://IP.
 Note that use the multi-domain server IP address upon checkpoint multiple domains.

o <u>:</u> -				🌐 Discard Session 🝷 🎲 Publish
	** Domains	Domains		*• 🔪 🗶 🗖 Connect 🔍 Search
MULTI	 Global Assignments OP Permissions & Administrators 	Servers (1) Domains (3)	CPR80_MDS_Test 10.10.32.151	use this IP
888	Administrators	Na Domain1	Domain1_Server 10.10.33.87	
ATEWAYS SERVERS	Trusted Clients	Na Domain2	Commain2_Server	
OGS &	Advanced Ill Blades	B* Global	8	

- 5) In the **Username** and **Password** fields, enter the username and password of the account that you have configured in the Checkpoint Manager.
- 6) Select a Front Server that can connect to the Checkpoint Manager from the **Front Server** drop-down menu.
- 7) Click **Test** to check connectivity between your NetBrain Front Server and Checkpoint Management

Domain.

	Edit External API Ser	Test External API Server	×	×
		Start Time: 2019-08-29 16:26:06		
		Connecting to Front Server(WIN-3946J1V3AIQ)		
		Successful		
1		Connecting to end points (https://10.10.32.157) via Front		
		Server(WIN-3946J1V3AIQ)		\sim
		Successful		
		End Time:2019-08-29 16:26:21		
	Front Server/Fro	ОК		~
	Advanced	s/		
	Managed Devices:	20		
	Test		Cance	ОК

8) Click **OK**.

3. Discovering Checkpoint Firewall R80 in NetBrain

After finishing configurations at Checkpoint Manager side and NetBrain side, you can get started to discover Checkpoint Firewall R80 to one of your NetBrain domains.

Note: To ensure that all CheckPoint Firewall R80 can be correctly discovered to your NetBrain domain, execute the discovery via CLI/SNMP first and then re-run a discovery via API after the CLI/SNMP discovery is complete.

- 1. Discover Checkpoint Firewall R80 via SNMP/CLI in NetBrain:
 - 1) In the **Domain Management** page, select **Operations > Discover** from the quick access toolbar.
 - 2) On the **Discover** tab, select **Scan IP Range.**
 - 3) Enter all management IP addresses of your Checkpoint Firewall R80 devices and separate each IP address with a semicolon. You can also enter all IP address by importing an IP list in CSV format.

Ca) 🖬 🤊 -	ء (م الم	L3 Se	ed Router List.	csv - Micro	osoft Excel				x
r e	Home	Insert	Page Layout	Formulas	Data	Review	View	Add-Ins	0 -	a x
	A1	- ()	f _x	192.168.0.1						×
		A	В	C		D	E	F	G	
1	192.168.0.1									
2	192.168.10.1	1								
3	192.168.20.3	1								
4	10.10.0.1									
5	10.10.10.1									
C 14 4	► N L3 See	ed Router List	. 2				111			F
Read	У						100%	Θ		+ .::

4) Keep other options as default and click **Start Discovery**.

D	omain Mar	nagement								
	Start Page	Network Settings $~ imes~$	Discover $ imes$	Schedule Task	×	Change Managem	ent Settings $ imes$	Advar	iced Settings	\times
	Discover via Seed Routers Scan IP Range					twork Settings	👁 View Last Res	sult		
	10.10.10.9;19	2.168.1.1;10.10.10.7			Se	elect Devices	Import IP	List		
	Access Mode:	SNMP and SSH/Telnet	- I Discovery	Depth: 0	Advan	ced Select Plugin	Start Discov	very		

- 2. Re-discover Checkpoint Firewall R80 via API after the SNMP/CLI discovery is completed.
 - Enter the IP address of the Endpoint (excluding the https://IP) that you have configured in the <u>API Server</u> <u>Manager</u>.

2) Keep other options as default and click **Start Discovery**.

tart Page	Ansible Agent Manage	er × Discover	× API Ser	rver Manager 🛛 🗙		
Discover vi	a Seed Routers 💿 Scan I	P Range		Network Settings	O View Last Result	
10.10.32.157				Select Devices	Import IP List	
ccess Mode:	SNMP and SSH/Teinet	Discovery I	Depth: 0	Advanced Select Plugin	Start Discovery	
Discovery	is completed. but there a	re some issues need to	o be resolved i	n Domain Manager. For troub	leshooting, please Contac	t Net
biscovered 1 li	P addresses, found 20 device Report 🛛 🗶 Execution L	ces within 00:00:52. Fini Log 🔂 Plugin Log	ished additiona	l operations within 00:02:45.		
Discovery Su	mmary License Details					
	-					
Chec	kpoint Fire Che	eckpoint Fire				

Note: The discovery adds Checkpoint Firewall R80 to your NetBrain domain and only retrieves very basic information via Checkpoint APIs. After the discovery, you need to <u>run a benchmark</u> to retrieve more data of the devices, such as configuration files, routing table and NCT data (Policy Table/NAT Table/IPsec VPN Table).

4. Run a benchmark to Update Data and Build Topology

After the discovery is done, you need to run a benchmark task to update the data of the Checkpoint Firewall R80 devices and build topology in your NetBrain system.

Edit Benchmark Task						
Task Name: Basic System Benchmark Description: Default system b						
Frequency Device Scope Retrieve Live Data	CLI Commands Additional Operations after Benchmark	Plugins Summary				
Select Device	$\ensuremath{\mathscr{C}}$ Select external API servers to retrieve data of SDN nodes					
All Devices Device Group Site	API Source Type Server Name Endpoint	Description				
 WLC(2) LAN Switch(1) Firewall(3) L3 Switch(54) Router(18) 						
 End System(56) Unclassified Device(5) 						
W AP(3)						
Exclude Device Groups: <please select=""></please>						
		Cancel Submit				