



R80.40 Tutorial

For beginners, an exercise for those who wish to practice their appliance capabilities.

By: Eido Epstein

Mar
2021

Glossary

Requirements	4
Topology	5
Network Setup.....	5
Features & IPS	7
Instructions.....	9
Network Setup.....	9
Features & IPS	9
Installation & Setup.....	10
Setting a VMnet.....	10
Setting Network Information	12
Installing Gaia	13
Installing Security Management Server	16
Enabling Interface Connections.....	23
Smart Console	25
Initial Setup.....	25
Enabling Internet Connection	27
Basic Policy Rules	29
Creating Objects	29
Basic Rules	30
Security Gateway	33
Installation & Configuration	33
Enabling SG in SMS	37
Creating a New Policy	40
DC Server.....	42
Configuration.....	42
Adding Clients to a Domain.....	43
Enabling Connection to Web Server.....	44

HTTPS Inspection	46
Enabling HTTPS Inspection	46
Creating HTTPS Rules	50
Identity Awareness.....	51
Initial Setup.....	51
Creating an LDAP Object	55
Creating an LDAP Group & Access Roles	58
LDAP Group.....	58
Access Roles	59
URL Filtering	60
Filtering Rules	60
Testing the Rules	65
IPS	67
Enabling IPS	67
Setting A Rule	68
Checking the Max Ping Size Rule	70
Conclusion	70

Requirements

In order to manually follow-up with this article, there are some prerequisites that needs be made;

- Basic familiarity with networks.
- One Windows Server 2019 OS installed.
- Two Windows 10 OS installed.
- Two Check Point R80.40 GAIA .iso ([Link to download](#)).
- A Virtual Machine (VM) System, preferably VMware.

This guide can only serve as an additional exercise for Check Point's CCSA exam. It cannot replace other studying tools or documentations, only enriching them.

- ❖ R80.40 is a system that consists of multiple features called blades that are mainly focusing on security aspects for organizations. The system's main functionality is its firewall capabilities but the blades enable to expand the system capabilities, given you the advantage of managing different security aspects from one resource.

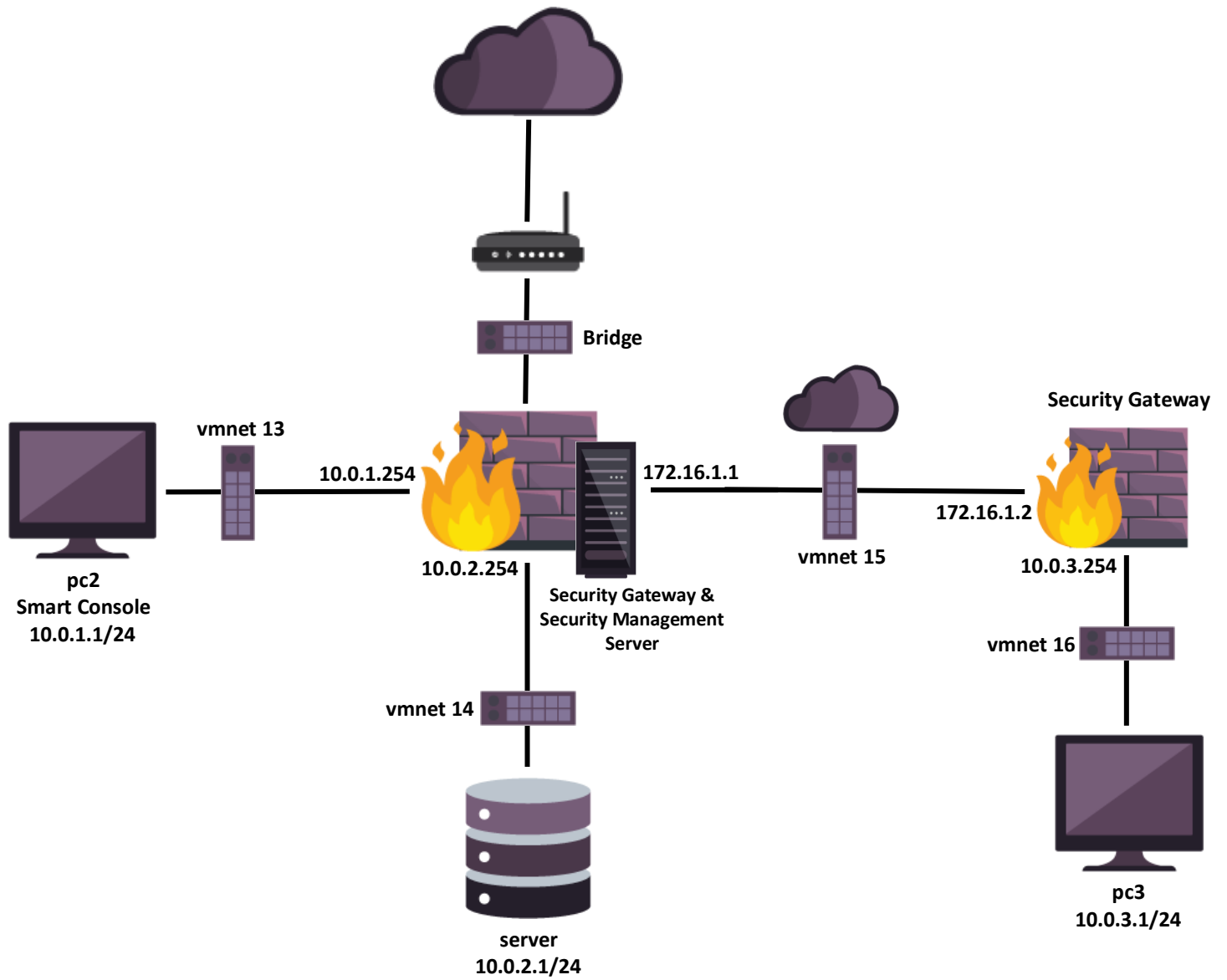
For this article and in order to make sure some of the R80.40 basic functionalities are covered. We'll practice on two topologies.

It is also important to mention that this exercise will not cover some of the basic setup that needs to be done, the main focus of it is the enablement process of R80.40 and some of its basic features.

Should you require any assistance with the initial topology setup please refer to my-[MCSA Tutorial](#).

Topology

Network Setup



- Network Data;

Name	IP Address	Subnet Mask	Default Gateway	DNS Address	Functionality
pc2	10.0.1.1	255.255.255.0	10.0.1.254	8.8.8.8	Smart Console
pc3	10.0.3.1	255.255.255.0	10.0.3.254	10.0.2.1	Endpoint
server	10.0.2.1	255.255.255.0	10.0.2.254	10.0.2.1	DC, DNS, Web
Security Gateway (SG)	172.16.1.2	255.255.255.0	172.16.1.1	8.8.8.8	Security Gateway
Security Management Server (SMS)	---	---	---	8.8.8.8	Security Management Server, Security Gateway

- Interfaces;

From	To	IP Address	Subnet Mask
pc2	SMS	10.0.1.254	255.255.255.0
server	SMS	10.0.2.254	255.255.255.0
pc3	SG	10.0.3.254	255.255.255.0
SG	SMS	172.16.1.2	255.255.255.0
SMS	Internet	Bridge	---
SMS	SG	172.16.1.1	255.255.255.0

- VMnet;

Network	VMnet
10.0.1.0/24	VMnet13
10.0.2.0/24	VMnet14
172.16.1.0/24	VMnet15
10.0.3.0/24	Vmnet16
Router	Bridge

- Credentials;

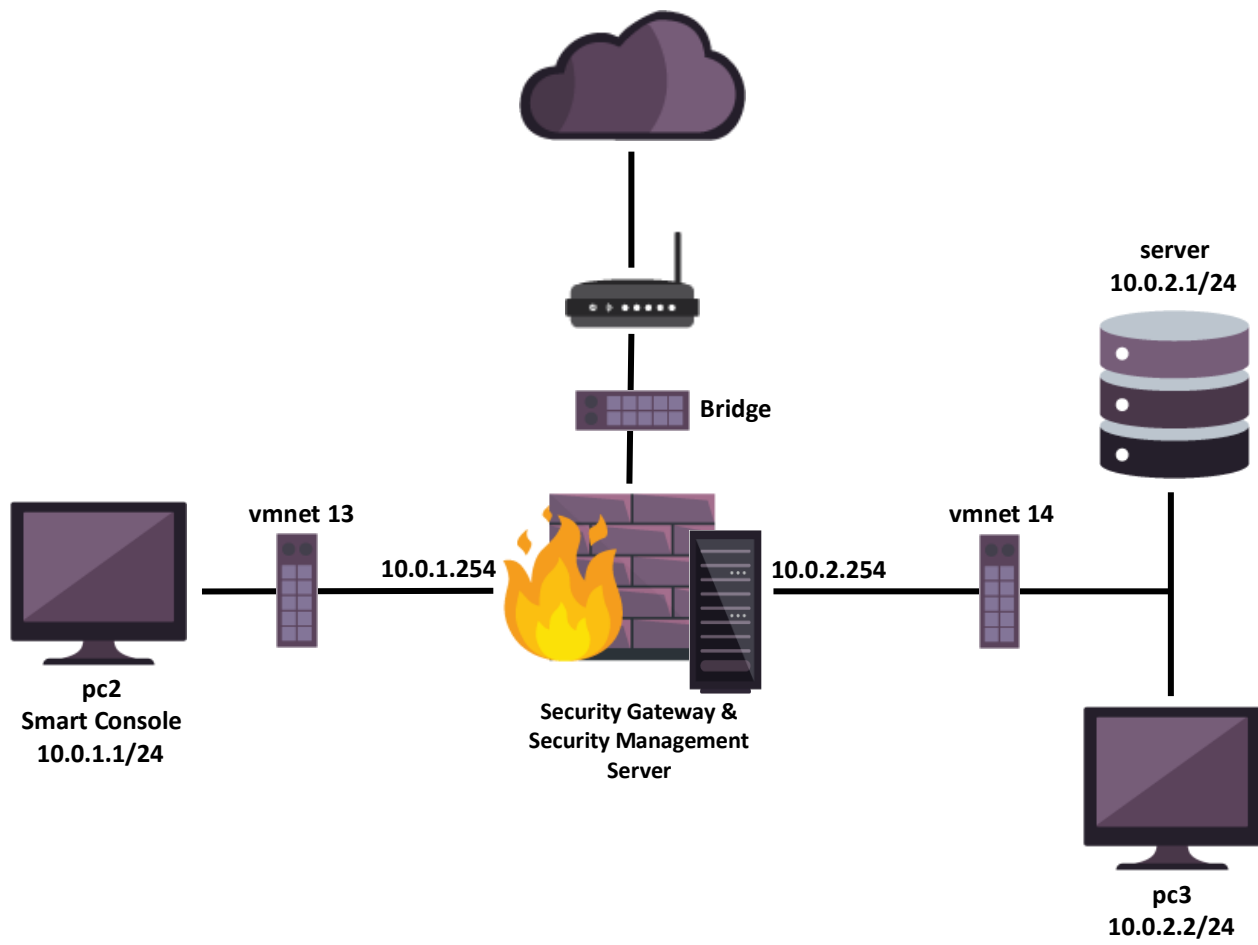
System	User Name	Password
Gaia (SMS)	admin	vpn123
Smart Console	eido	vpn123
Gaia (SG)	admin	vpn123
Secure Communication	---	vpn123

- Objects;

Name	Type	Value
pc2	Host	10.0.1.1/24
pc3	Host	10.0.3.1/24
dc	Host	10.0.2.1/24
	NAT (Static)	IP Bridge Range
VMnet13	Network	10.0.1.0/24
	NAT	Hide
VMnet14	Network	10.0.2.0/24

Name	Type	Value
VMnet15	Network	172.16.1.0/24
	NAT	Hide
Vmnet16	Network	10.0.3.0/24
	NAT	Hide
Network Setup	Network Group	All VMnets
sg	Gateway	172.16.1.2/24

Features & IPS



- Network Data;

Name	IP Address	Subnet Mask	Default Gateway	Functionality
pc2	10.0.1.1	255.255.255.0	10.0.1.254	Smart Console
pc3	10.0.2.2	255.255.255.0	10.0.2.254	Endpoint
server	10.0.2.1	255.255.255.0	10.0.2.254	DC, DNS
Security Management Server (SMS)	---	---	---	Security Management Server, Security Gateway

- Interfaces;

From	To	IP Address	Subnet Mask
pc2	SMS	10.0.1.254	255.255.255.0
server	SMS	10.0.2.254	255.255.255.0
pc3	SMS	10.0.2.254	255.255.255.0
SMS	Internet	Bridge	---

- VMnet;

Network	VMnet
10.0.1.0/24	VMnet13
10.0.2.0/24	VMnet14
Router	Bridge

- Credentials;

System	User Name	Password
Gaia (SMS)	admin	vpn123
Smart Console	eido	vpn123
SSL Certificate	server.local (Domain)	vpn123
server	User1	Welcome1!

- Objects;

Name	Type	Value
pc2	Host	10.0.1.1/24
pc3	Host	10.0.2.2/24
dc	Host	10.0.2.1/24
VMnet13	Network	10.0.1.0/24
VMnet14	Network	10.0.2.0/24
Features&IPS	Network Group	All VMnets
LDAP_Connection	LDAP Account Unit	Server.local
LDAP_Group	LDAP Group	LDAP_Connection
Users	Access Role	VMnet13, VMnet14
		Any Users
VMnet14 AR	Access Role	VMnet14
		LDAP_Group
Domains Filtering	Inline Layer	Policy Layer

Instructions

Network Setup

- Set the network topology with the following information;
 - Some configurations can only be applied after some progress with enabling certain device features.
- Install R80.40 and set its initial configurations.
- ◊ Make sure the server is set with DC, DNS and Web services ([MCSA Tutorial](#)).
- Set the basic rules that should be on a Firewall.
- Make sure all the devices inside the Intranet are able to communicate with each other.
- Allow external users to access your Intranet only via HTTP.

Features & IPS

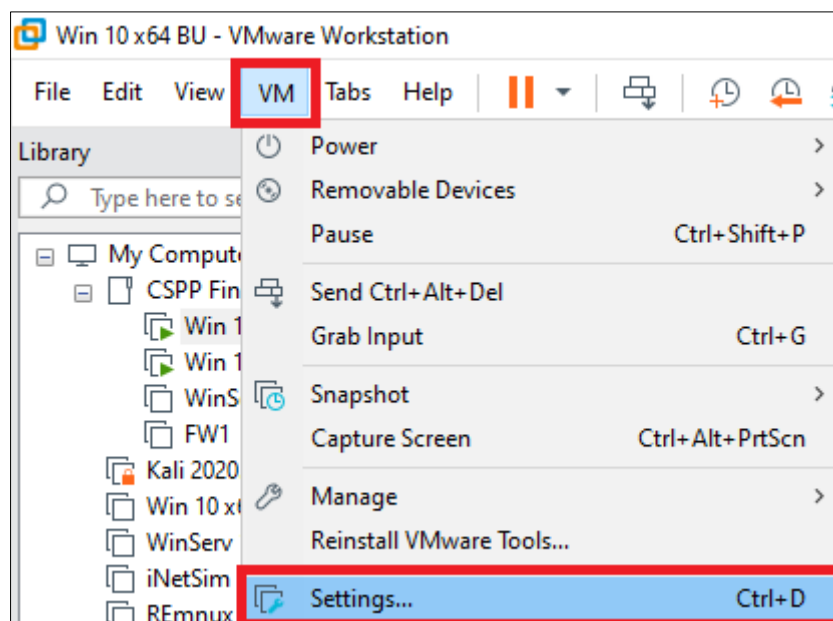
- Set the network topology with the following information;
 - Some configurations can only be applied after some progress with enabling certain device features.
- Install R80.40 and set its initial configurations.
- ◊ Make sure the server is set with DC and DNS services ([MCSA Tutorial](#)).
- Set the basic rules that should be on a Firewall.
- Make sure all the devices inside the Intranet are able to communicate with each other.
- Enable HTTPS Inspection and make sure any traffic to Financial Services will not be inspected.
- Enable Identity Awareness and URL Filtering;
 - Allow only users from VMnet14 access to YouTube.
 - Block Media Streaming and Media Sharing for your network.
 - Enable users to access Social Networking only after they receive a notification.
 - Block any traffic containing CC credentials (PCI).
- Enable IPS and set Max Ping Size rule of 200 bytes for each request.

Installation & Setup

In this section we will focus on how to setup some of the basic configurations for the endpoint devices and how to install R80.40

Setting a VMnet

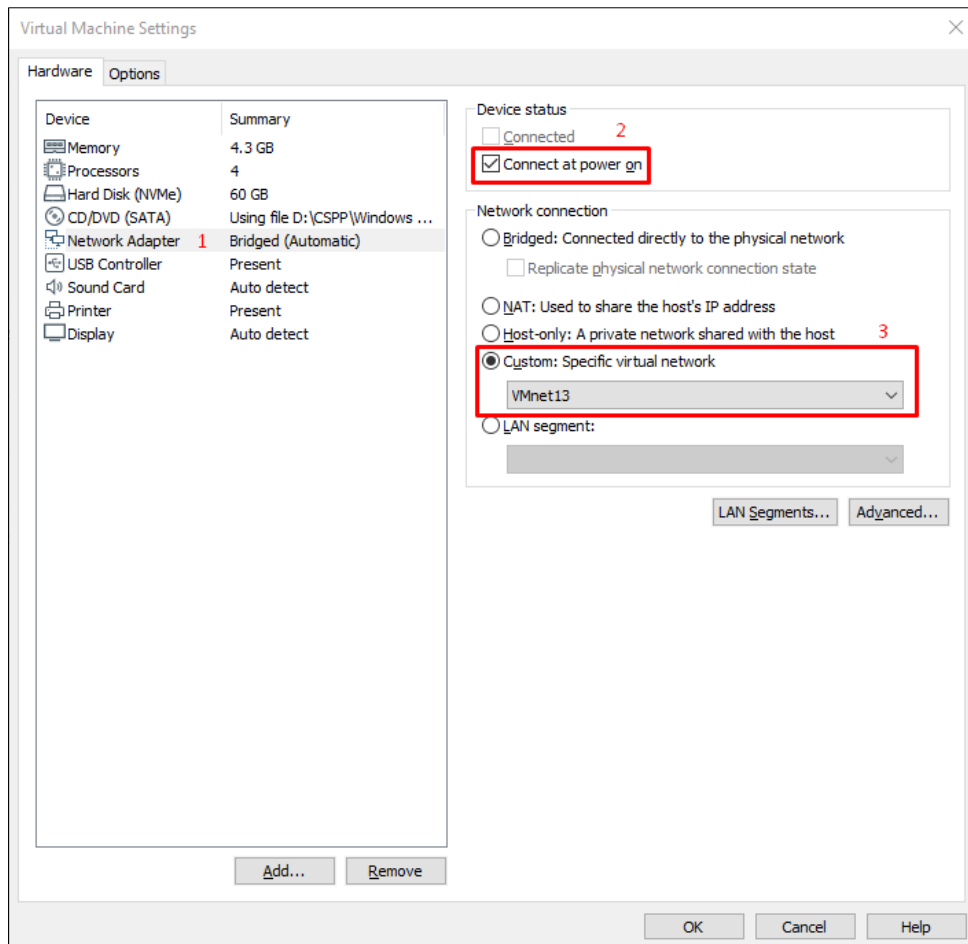
- ❖ VMnet- A service in VMware, its purpose is to connect between network interfaces and enabling them to communicate with each other.
 - In this guide we'll be using VMware Workstation. If you are using another VM, please use any relevant documentation in order to make sure the network connections are being properly set.
- 1) Open VMware and choose the relevant device.
 - 2) At the top-left corner, press on "**VM**" and then click on "**Settings**".



- 3) At the left bar, choose "**Network Adapter**".

[Next Page]

- 4) Make sure the checkbox for "**connect at power on**" is marked.
- 5) At the "**Network connection**" section, choose "**Custom...**" and pick the relevant VMnet according to the topology you are working on.



- Press on "**OK**" when you are done.

Setting Network Information

- 1) On the relevant device, go to-
Control Panel\Network and Internet\Network Connections
- 2) Right click on the relevant network icon and choose "**Properties**"
- 3) Double click on "**Internet Protocol Version 4 (TCP/IPv4)**"

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 0 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 1 . 254

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: . . .

☐ Validate settings upon exit

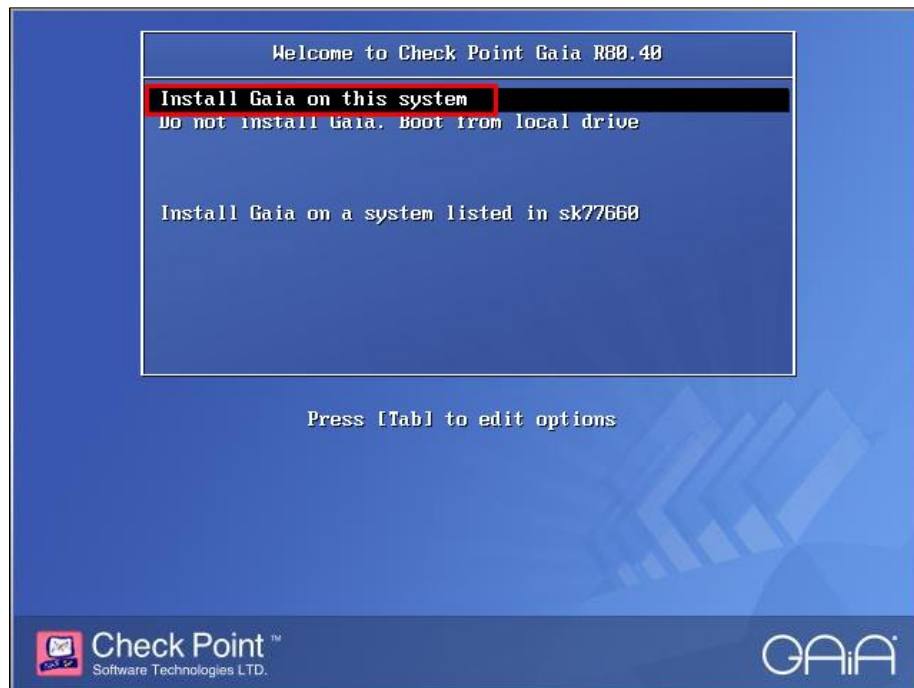
Advanced...

OK Cancel

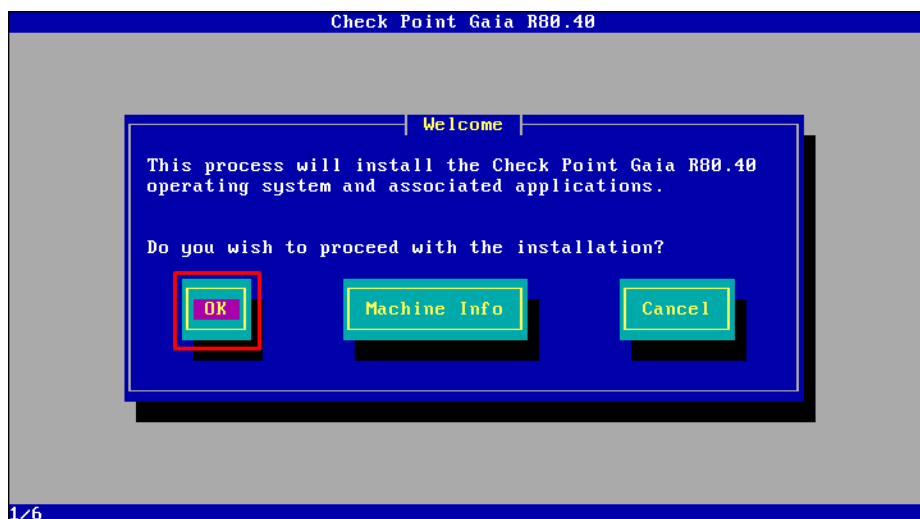
- Press on "**OK**" when you are done.
- On how to change your devices names please follow this- [Link](#)
- Make sure that Windows Firewall is turned off.

Installing Gaia

- ❖ Gaia- Check Point's Operating System for security applications. This OS supports the full portfolio of Check Point's security features and products.
- 1) Create a VM image with Gaia's .iso and set hardware data.
 - 2) Set the device VMnet to "**VMnet13**"
 - 3) Activate the OS and choose "**Install Gaia on this system**"

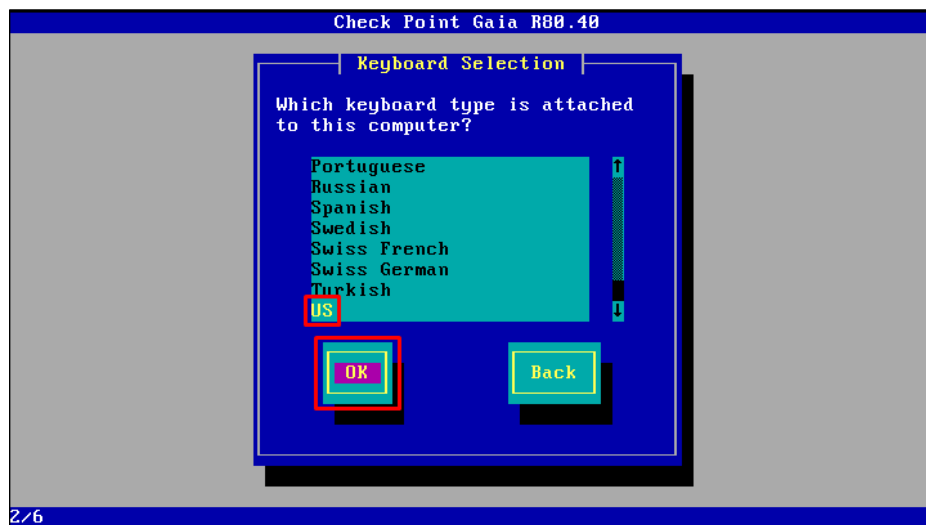


- 4) Wait until the OS finish loading and press on "**OK**"

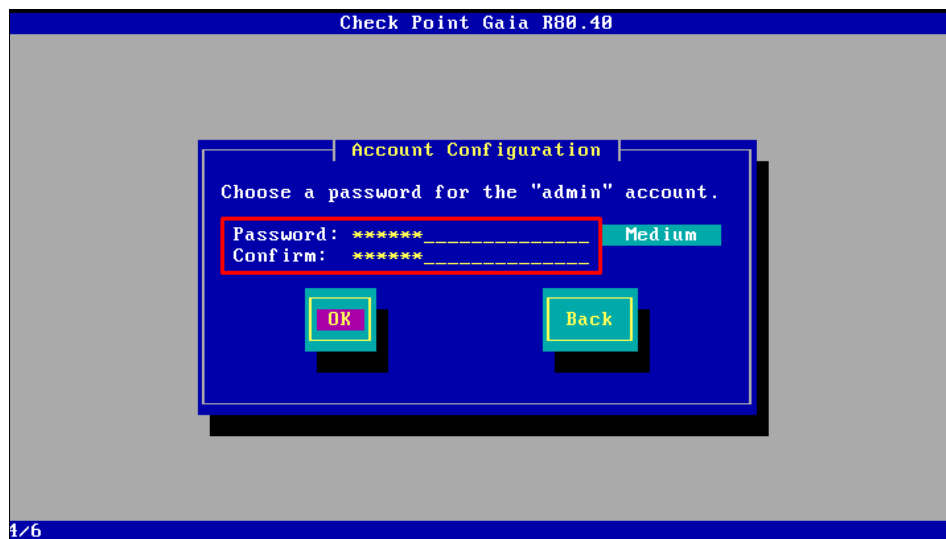


[Next Page]

- 5) Choose the relevant keyboard language and press on "OK"



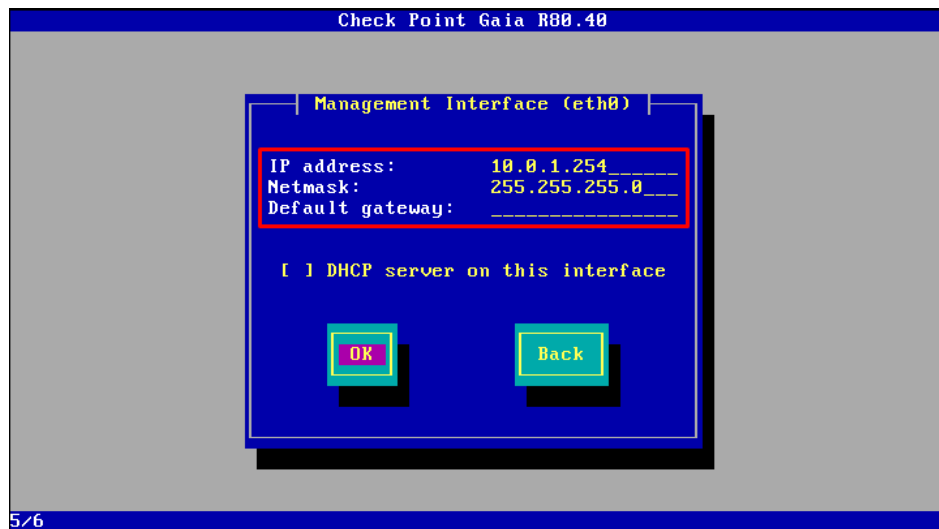
- 6) Press on "OK" until you reach the "Account Configuration" window.
- 7) Create a password for the admin account according to the Topology section.



- Press on "OK" when you are done.

[Next Page]

- 8) At the "**Management Interface**" section, input the credentials according to the Topology section.

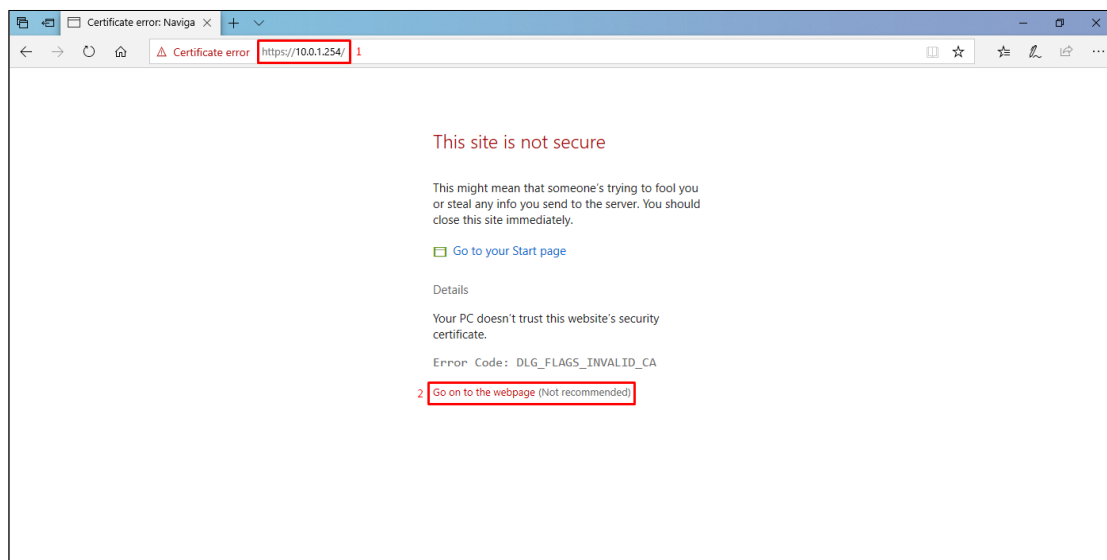


- Make sure the "**Default gateway**" field is empty.
 - Press on "**OK**" when you are done.
- 9) Press on "**OK**" to begin the installation process.

Installing Security Management Server

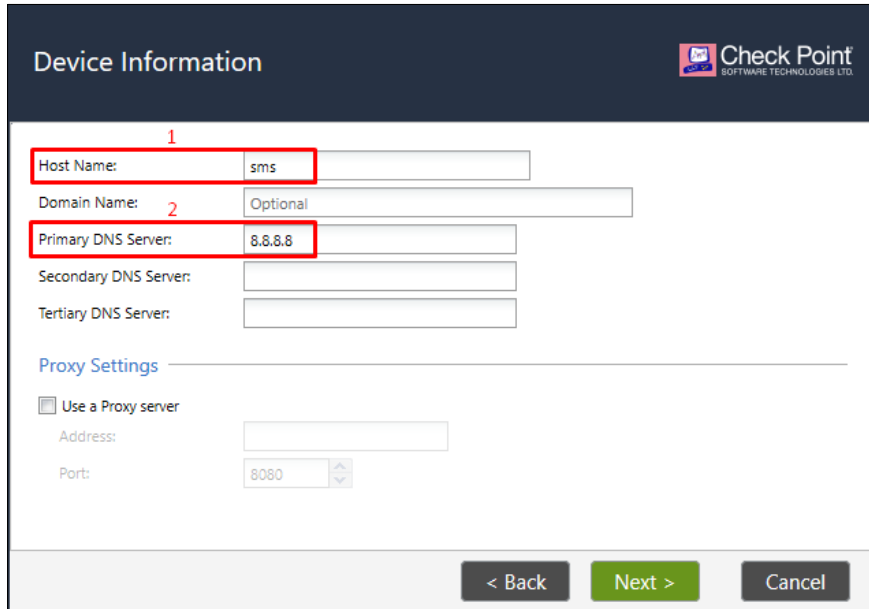
- ❖ Security Management Server- An interface that enables you to control a network/s configuration and features from one source, some of the options include; Network management, user management, routing and more.

- 1) Add a VMnet Bridge connection to pc2.
 - We will use this connection only for updating the R80.40 system.
- 2) Open pc2.
- 3) Disable Windows Firewall for pc2.
 - For the sake of this tutorial, we are disabling the device firewall in order to prevent any unnecessary errors.
- 4) Open the browser and type "**https://10.0.1.254**"
At the warning page, press on "**Go on to the webpage**"



[Next Page]

- 5) Input your Gaia's admin credentials.
- 6) At the configuration window, click on "**Next**" until you reach the "**Device Information**" window.
- 7) Change the Host Name according to the Topology section.
- 8) For the "**Primary DNS Server**" field, input "**8.8.8.8**".
 - This is a temporary measure that we'll be using for the installation process. Later on, we will change it.



Device Information

Check Point
SOFTWARE TECHNOLOGIES LTD.

1
Host Name: sms

2
Domain Name: Optional

Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings

☐ Use a Proxy server

Address:

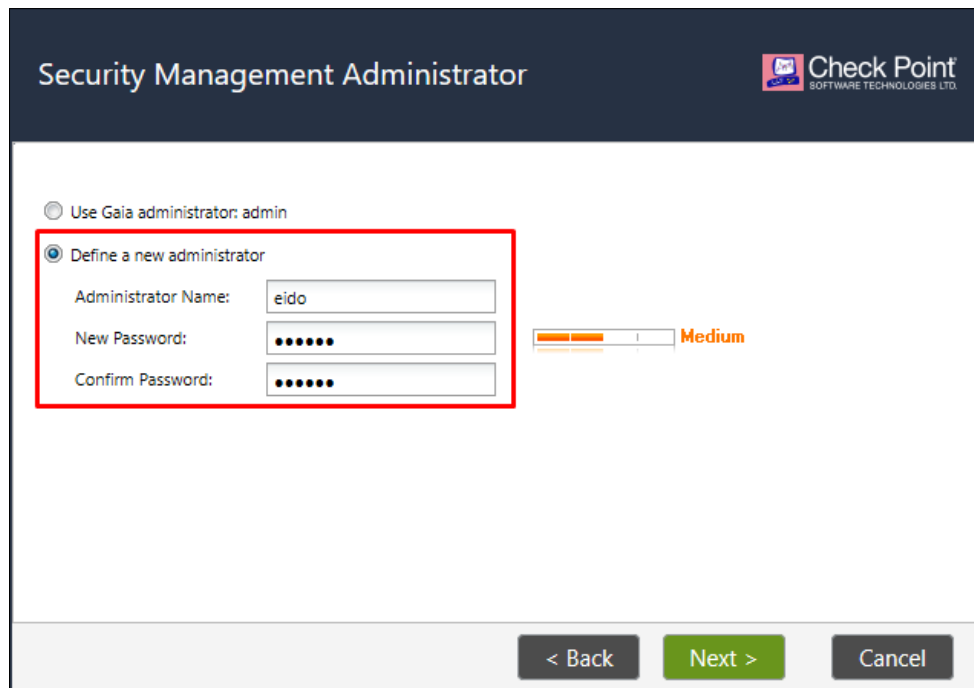
Port: 8080

< Back Next > Cancel

- Press on "**Next**" when you are done.
- 9) Click on "**Next**" until you reach the "**Security Management Administrator**".

[Next Page]

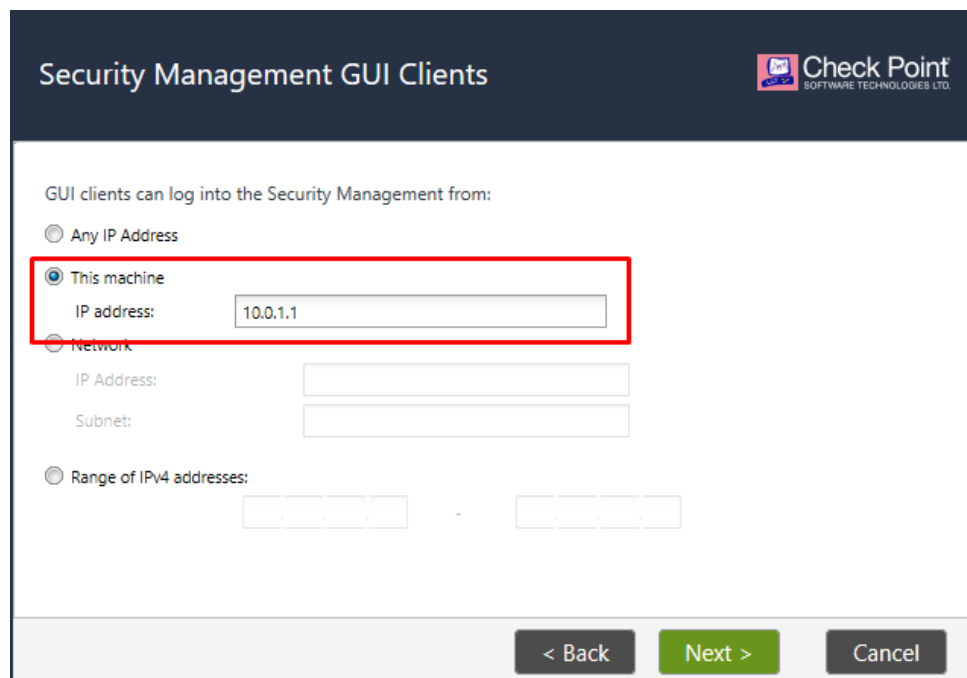
- 10) Check the "**Define a new administrator**" and input the credentials according to the Topology section.



The screenshot shows the "Security Management Administrator" window. At the top, there is a header with the "Security Management Administrator" title and the Check Point logo. Below the header, there are two radio button options: "Use Gaia administrator: admin" and "Define a new administrator". The "Define a new administrator" option is selected and highlighted with a red rectangle. Below this option, there are three input fields: "Administrator Name:" with the value "eido", "New Password:" with masked characters, and "Confirm Password:" with masked characters. To the right of these fields, there is a password strength indicator showing a bar with the word "Medium" in orange. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

- Press on "**Next**" when you are done.

- 11) At the "**Security Management GUI Clients**" window, check the "**This machine**" option.



The screenshot shows the "Security Management GUI Clients" window. At the top, there is a header with the "Security Management GUI Clients" title and the Check Point logo. Below the header, there is a section titled "GUI clients can log into the Security Management from:". There are three radio button options: "Any IP Address", "This machine", and "Network". The "This machine" option is selected and highlighted with a red rectangle. Below this option, there is an input field for "IP address:" with the value "10.0.1.1". Below the "Network" option, there are input fields for "IP Address:" and "Subnet:". Below the "Range of IPv4 addresses:" option, there are two input fields for IP address ranges. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

- Press on "**Next**" when you are done.

[Next Page]

- 12) Remove the "Send data to Check Point" checkbox.
- 13) Press on "Finish".
 - Once the installation is complete, reboot the system.
- 14) After the installation is complete, turn off the Gaia OS.
- 15) Add the remaining VMnet to Gaia according to the Topology section.
- 16) Open the web interface at "**https://10.0.1.254**" again and input the relevant credentials.
- 17) At the left bar, under "**Network Management**", press on "**Network Interfaces**"
- 18) Configure each Ethernet interface to its respective VMnet or Bridge.

Network Adapter	Custom (VMnet13)
Network Adapter 2	Bridged (Automatic)
Network Adapter 3	Custom (VMnet14)
Network Adapter 4	Custom (VMnet15)

Name	Type
eth0	Ethernet
eth1	Ethernet
eth2	Ethernet
eth3	Ethernet
lo	Loopback

- The order of interfaces displayed in Gaia is in partial correlation with the order your VMnets and bridge connections are set on your SMS.
- In some cases, a little troubleshooting with the command-
show interfaces all may be required.
- The following are examples on how you are setting these connections;

Edit eth2

Link Status: Up

Type: ethernet

Enable: ☒

Comment: VMnet14

IPv4 | IPv6 | Ethernet

☐ Obtain IPv4 address automatically

☒ Use the following IPv4 address:

IPv4 address: 10 . 0 . 2 . 254

Subnet mask: 255 . 255 . 255 . 0

OK Cancel

Edit eth1

Link Status: Down

Type: ethernet

Enable: ☒

Comment: Bridge

IPv4 | IPv6 | Ethernet

☒ Obtain IPv4 address automatically

☐ Use the following IPv4 address:

IPv4 address:

Subnet mask:

OK Cancel

[Next Page]

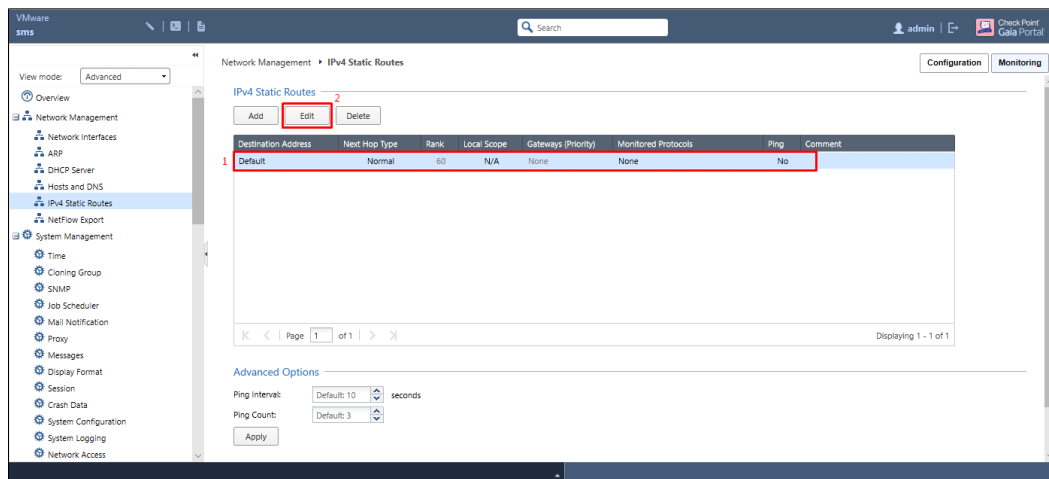
19) Enter Gaia via its server environment and send a ping to 8.8.8.8

- If you didn't receive the message "**connect: Network is unreachable**" and you have an internet connection; You can skip steps 18 - 23.
- You weren't able to get a reply, continue to the next step.

20) Open Gaia's web interface.

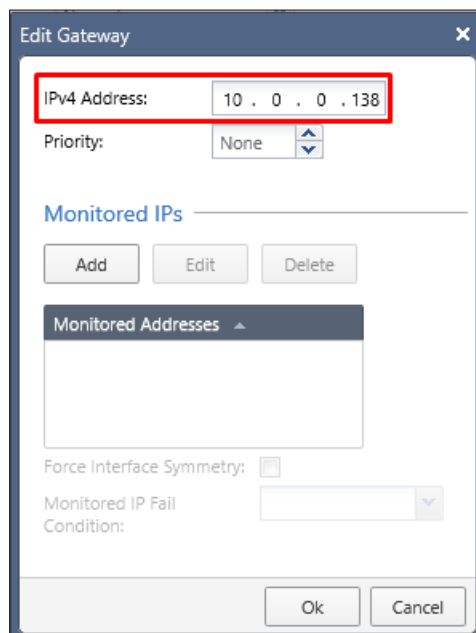
21) At the left bar, under "**Network Management**", press on "**IPv4 Static Routes**"

22) At the main page, mark the "**default**" row and press on "**Edit**"



23) At the edit page press on "**Add Gateway**" and then press on "**IP Address**"

24) Add the relevant Gateway IP address.



- For this tutorial, it will be the Gateway IP address of the device on which our VMware system is installed on.
- Press on "**Ok**" and then on "**Save**" when you are done.

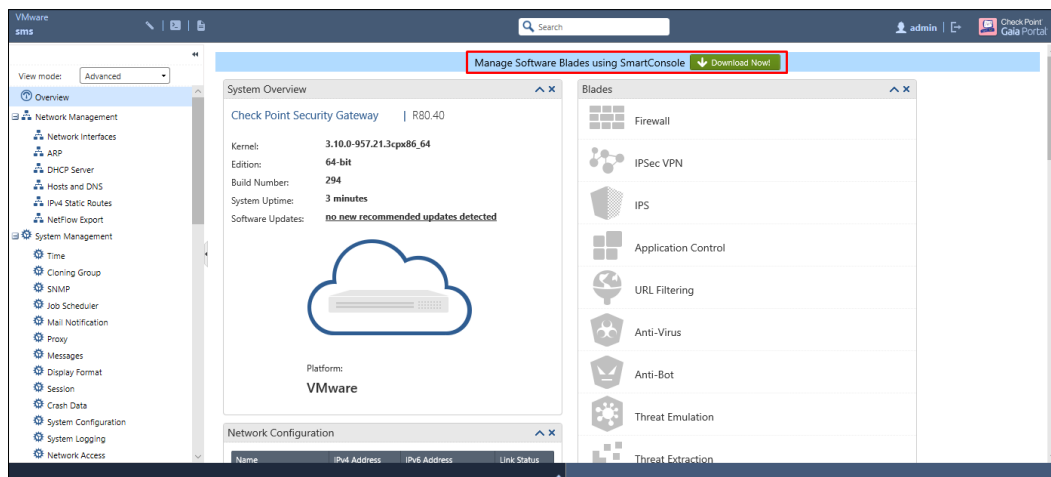
[Next Page]

- 25) If you correctly followed the instructions, you should be able to receive replies for pings being sent from the Gaia's server environment to 8.8.8.8

```
sms> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=75.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=75.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=75.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=75.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=110 time=75.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=110 time=74.9 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 74.985/75.139/75.324/0.295 ms
```

- Type **Ctrl + C** in order to stop the server from sending pings.

- 26) At the main page, right to "**Manage Software Blades using SmartConsole**"-
Press on "**Download Now**"

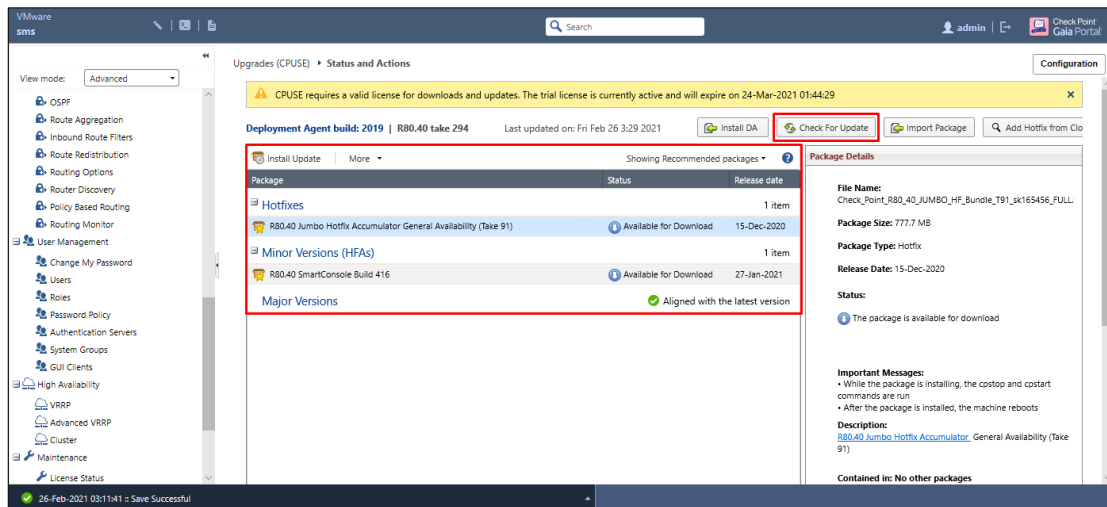


- 27) Run the installation software, check the License Agreement box and press on "**Install**"



[Next Page]

- 28) Open Gaia's web interface.
- 29) At the left bar, under "**Upgrades (CPUSE)**" at the bottom-press on "**Status and Actions**"
- 30) Press on "**Check For Updates**" and then install all the available packages.



- After you finish with all the updates, you can remove/disable the Bridge connection on pc2.

Enabling Interface Connections

- 1) Open pc2.
- 2) Open the browser and type "**https://10.0.1.254**"
- 3) At the left bar, under the "**Network Management**" section-
Click on "**IPv4 Static Routes**"
- 4) Click on the "**Add**" button, at the "**Add Destination Route**" window;
 - i. Set the relevant IP network and Subnet Mask.
 - ii. Click on "**Add Gateway**" and choose "**Network Interface**".

Add Destination Route

Destination: 10 . 0 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send *unreachable* messages.
Black Hole: Drop packets, but don't send *unreachable* messages.

Rank: Default: 60

Local Scope: ☐

Comment: VMnet13

Add Gateway

Ping: ☐

Add Gateway ▼ Edit Delete

IP Address

Network Interface

Priority ▲ Monitored Addresses

Save Cancel

[Next Page]

- iii. At the opened window, choose the relevant interface and assign it with a priority

Add Logical Interface Gateway

Logical Interface: eth3

Priority: 1

Monitored IPs

Add Edit Delete

Monitored Addresses

Force Interface Symmetry: ☐

Monitored IP Fail Condition:

Ok Cancel

- If you correctly followed the instruction the configuration should look similar to the following;

Network Management > IPv4 Static Routes

Configuration Monitoring

IPv4 Static Routes

Add Edit Delete

Destination Address	Next Hop Type	Rank	Local Scope	Gateways (Priority)	Monitored Protocols	Ping	Comment
Default	Normal	60	N/A	10.0.0.138 (None)	None	No	
10.0.2.0/24	Normal	60	On	eth2 (1)	None	No	
172.16.1.0/24	Normal	60	On	eth3 (1)	None	No	

Page 1 of 1

Displaying 1 - 3 of 3

Advanced Options

Ping Interval: Default: 10 seconds

Ping Count: Default: 3


Apply

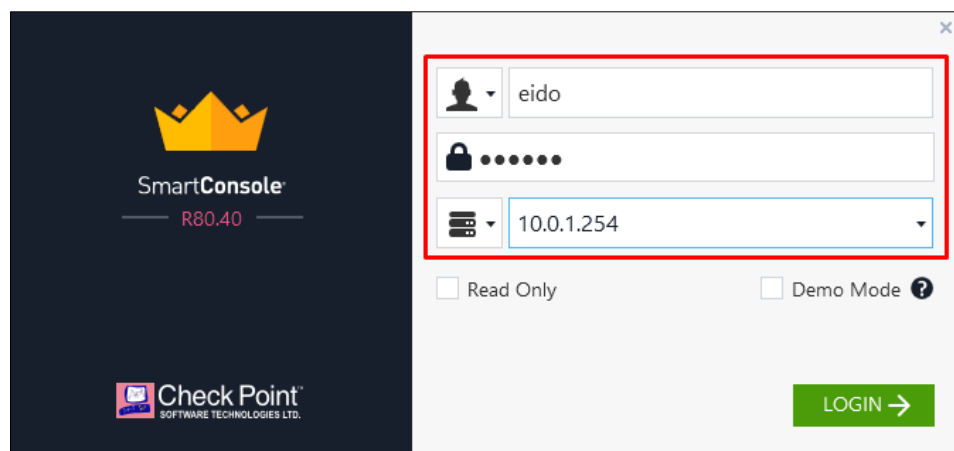
Smart Console

In this section we'll focus on some of the initial setups we need to do for the Smart Console.

- ❖ Smart Console- The actual User Interface (UI) on which we are actually managing all of our security settings and features, Smart Console can only work when you have an SMS installed on a Gaia OS.

Initial Setup

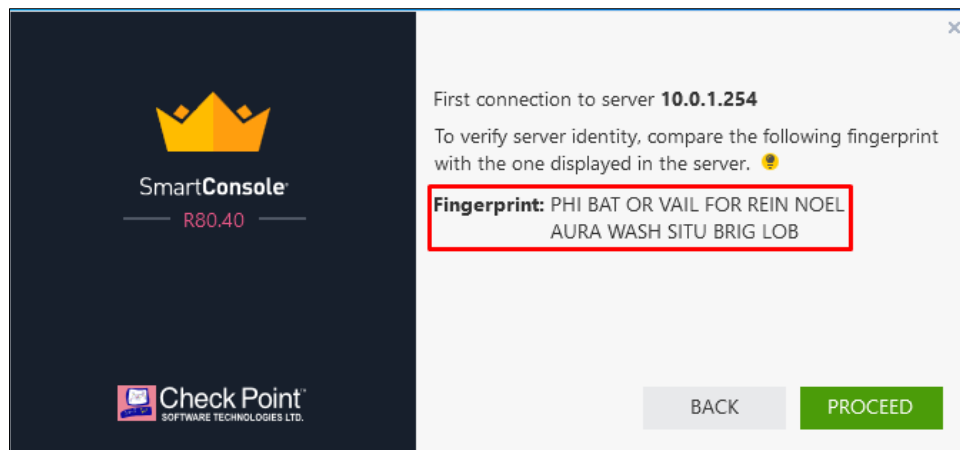
- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application - 
- 3) Input the credentials you set when installing the SMS



- Press on "**LOGIN**" when you are done.

[Next Page]

4) On your first connection, save the fingerprint displayed.



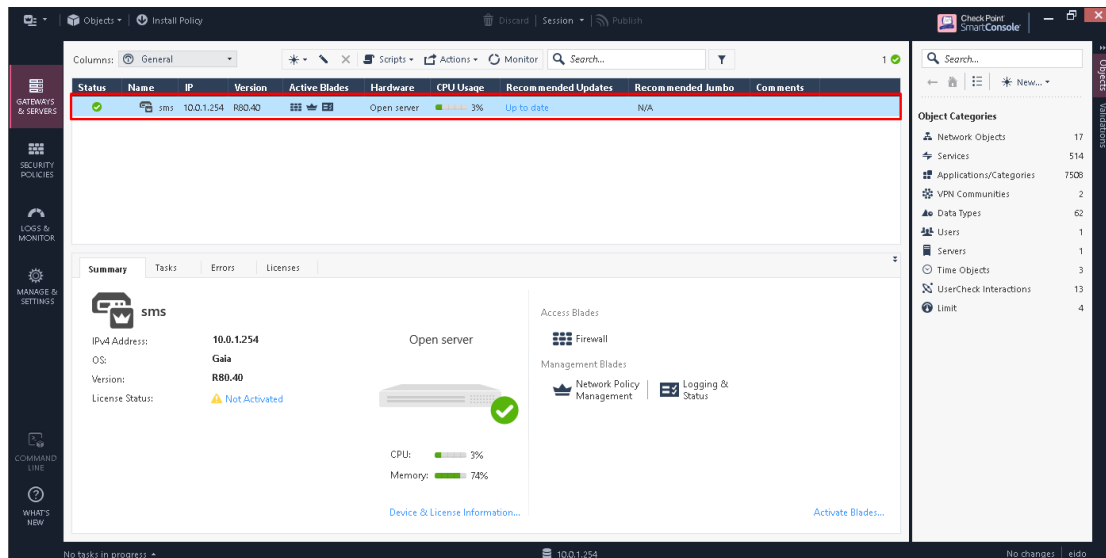
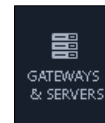
- This fingerprint is used to prevent [Phishing](#) attempts.
- In order to verify it;
 - i. Login to Gaia via its Server environment.
 - ii. Type "**cpconfig**" and choose option "**8**".
 - iii. Cross-reference the fingerprint from the server and UI to verify its valid.

```
Configuring Certificate's Fingerprint...
=====
The following text is the fingerprint of this Security Management Server:
PHI BAT OR VAIL FOR REIN NOEL AURA WASH SITU BRIG LOB
```

- Press on "**PROCEED**" once you are done.

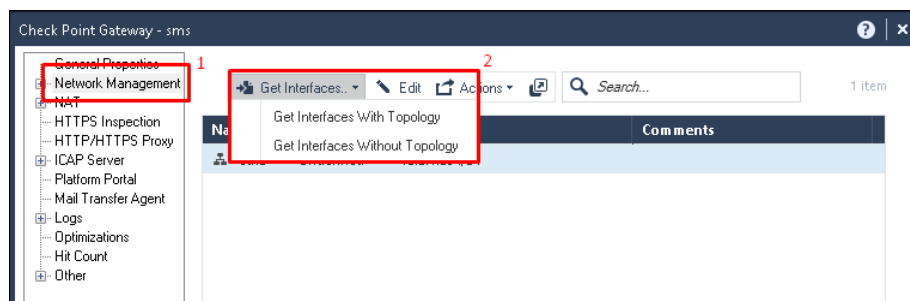
Enabling Internet Connection

- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application.
- 3) At the main window, under the **"GATEWAYS & SERVERS"** tab -
- 4) Double click on the existing Gateway.

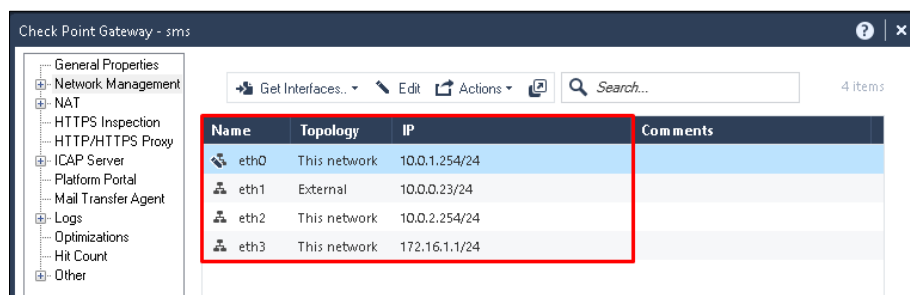


- If you correctly followed this tutorial, the name of the device should be 'sms' and the IP associated with him should be '10.0.1.254'.

- 5) At the left bar, click on **"Network Management"**
- 6) Press on **"Get Interfaces"** and then choose **"Get Interfaces With Topology"**

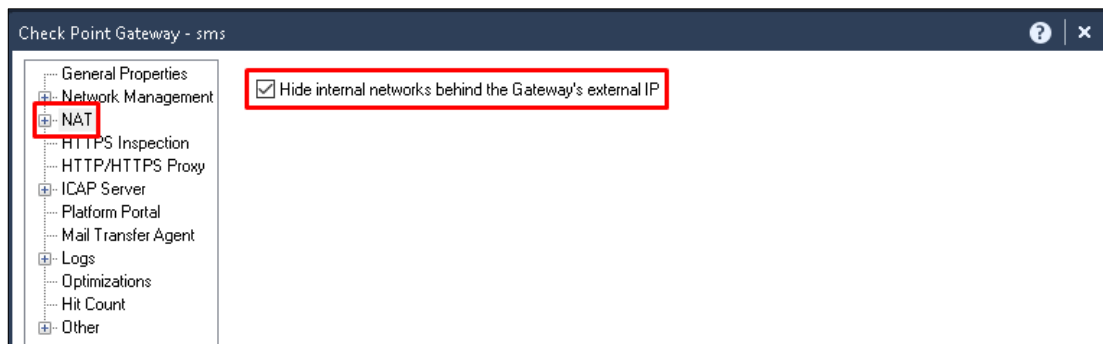


- Press on **"Yes"** and at the opened window, click on **"Accept"**.
- If you correctly followed the instructions, you'll see the following;



[Next Page]

7) At the left bar, click on "**NAT**" and check the box for-



8) When you are done, exit the window and press on "**Publish**" -



- This command informs other users on the changes you made in the system. The changes do not take effect, they are only shared.

9) Next, at the window top-left corner, press on "**Install Policy**" -



- After clicking on "**Install**" at the opened window, the user applies the published changes he made on the relevant device/s.

Basic Policy Rules

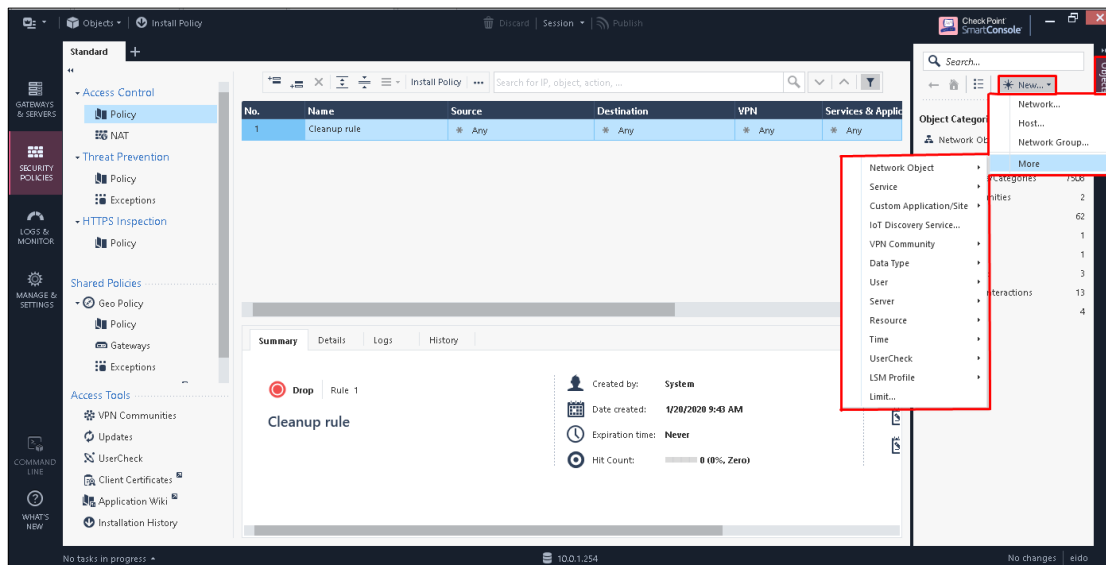
In this section we'll focus on some of the basic available options for creating a policy, how to manage our policy settings and what are the basic rules that should be applied for a policy.

- ❖ **Security Policy**- Identifies the rules and features for all individuals accessing and using an organization's assets and resources. The objective of a Security Policy is to preserve the confidentiality, integrity and availability of systems and information being used by an organization's members.

Creating Objects

- ❖ **Objects**- Individual or groups of data that are being assigned with an adjective that usually has the same name. We use them in order to represent parts of our network topology and to apply rules on them.

- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application.
- 3) At the main window, click on the **"SECURITY POLICIES"** tab -
- 4) At the right bar, make sure you are on the **"Objects"** tab.
- 5) Click on **"New"** and choose the new object you would like to create.



- The full list of objects is quite extensive and will not be fully mentioned in this tutorial, we suggest you to Check Point's [Data Base](#) for this matter.
- In order to correctly follow this tutorial, you can check the objects we applied in the Topology section.

- 6) Configure the relevant object according to your needs.

Basic Rules

In this section we'll be presenting some of the basic rules that should be applied on a firewall before adding additional rules according to your topology and organization's needs.

This tutorial will not cover all of the features; Therefore, we highly recommend the reader to further enrich himself from additional sources regarding this matter.

- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application.
- 3) At the main window, click on the **"SECURITY POLICIES"** tab.
- 4) Make sure you are at the **"Access Control"** section, under **"Policy"** at the left bar.
- 5) Use the options bar at the top in order to adjust your policy.



- The entire usage options will not be covered in this tutorial.
For further documentation please refer to other resources.

- 6) Create the following basic rules for your policy;







Clean-Up Rule

This rule purpose is to log dropped packets that did not apply with any rule in the policy. This rule will always be the last in a policy.

Name	Source	Destination	Services & Applications	Action	Track
Cleanup rule	* Any	* Any	* Any	 Drop	 Log

Internet Access

This rule purpose is to enable all of our networks to have access to the internet via HTTP, HTTPS and QUIC connections. This rule will always be between the Clean-Up and Stealth rules.

Name	Source	Destination	Services & Applications	Action	Track
Internet Access	 Network Setup	* Any	 http  https  quic	 Accept	 Log

DNS Queries

This rule purpose is to enable devices in our network to send DNS queries. This rule will always be between the Clean-Up and Stealth rules.

Name	Source	Destination	Services & Applications	Action	Track
DNS Queries	 Network Setup	* Any	 domain-udp	 Accept	 Log

ICMP Requests

This rule purpose is to help us make sure all of the devices in our network are able to communicate with each other. This rule will always be between the Clean-Up and Stealth rules.

Name	Source	Destination	Services & Applications	Action	Track
ICMP Requests	 Network Setup	* Any	 icmp-requests	 Accept	 Log

Stealth Rule








This rule purpose is to make sure any unauthorized requests to the SMS will

Name	Source	Destination	Services & Applications	Action	Track
Stealth Rule	* Any	 sms	* Any	 Drop	 Log

Management Rule

This rule purpose is to enable a device to have access to the SMS.

This rule will always be above the Stealth Rule.

Name	Source	Destination	Services & Applications	Action	Track
Management Rule	 pc2	 sms	 https  icmp-requests  ssh_version_2	 Accept	 Log

Filter Rule

This rule purpose is to drop any unnecessary traffic without any log in order to save memory and processing power. In addition, it also helps in having a much clearer capability to inspect the logs. This rule will always be placed first in the policy.

Name	Source	Destination	Services & Applications	Action	Track
Filter Rule	* Any	* Any	 nbdatalogram	 Drop	 None

[Next Page]

- The majority of other rules you can add, will be added between the Clean-Up and Stealth rules.
- If you correctly applied the above basic rules, the following should be presented to you;

No.	Name	Source	Destination	Services & Applications	Action	Track
1	Filter Rule	* Any	* Any	UDP nbdatagram	Drop	None
2	Management Rule	pc2	sms	https icmp-requests ssh_version_2	Accept	Log
3	Stealth Rule	* Any	sms	* Any	Drop	Log
4	ICMP Requests	Network Setup	* Any	icmp-requests	Accept	Log
5	DNS Queries	Network Setup	* Any	domain-udp	Accept	Log
6	Internet Access	Network Setup	* Any	http https UDP quic	Accept	Log
7	Cleanup rule	* Any	* Any	* Any	Drop	Log

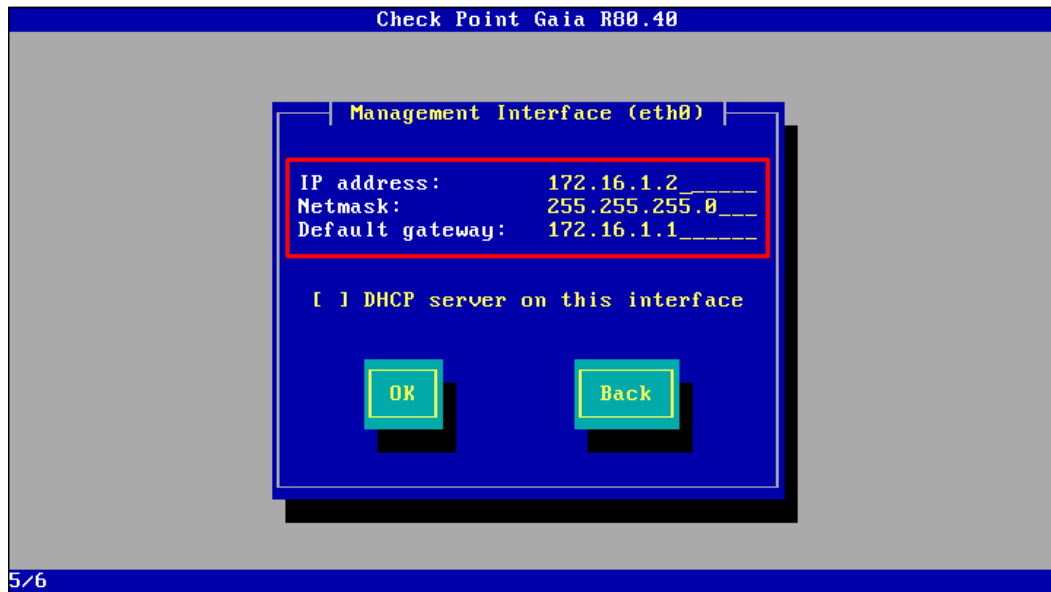
- Press on "**Publish**" and then "**Install Policy**" when you are done.

Security Gateway

In this section we'll present the main steps that are needed to be preformed in order to install another Security Gateway (Firewall) in our network.

Installation & Configuration

- 1) Repeat the "**Installing Gaia**" section in this document.
 - In this installation, set the Default Gateway according to the Topology section.



[Next Page]

- 2) Repeat the **"Installing Security Management Server"** section in this document, with the following exceptions;
- At the **"Device Information"** window-
Change the **"Host Name"** according to the Topology section.

Device Information

Check Point
SOFTWARE TECHNOLOGIES LTD.

Host Name: sg

Domain Name: Optional

Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings

☐ Use a Proxy server

Address:

Port: 8080

< Back Next > Cancel

- At the **"Products"** window-
Under the **"Products"** section, unmark the **"Security Management"** box.

Products

Check Point
SOFTWARE TECHNOLOGIES LTD.

Products

☒ Security Gateway

☐ Security Management

Clustering

☐ Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

☒ Automatically download Blade Contracts, new software, and other important data (highly recommended)

For more information click [here](#)

< Back Next > Cancel

- At the **"Dynamically Assigned IP"** window, press on **"Next"**.

[Next Page]

- iv. At the "**Secure Communication to Management Server**" window-
Input credentials according to the Topology section.

Secure Communication to Management Server

Check Point
SOFTWARE TECHNOLOGIES LTD.

Activation Key: [masked]

Confirm Activation Key: [masked]

[Learn more about SIC here](#)

☐ Connect to your Management as a Service

Authentication token: [input field]

Don't have an account? Click [here](#)

< Back Next > Cancel

- v. Uncheck the "**Send data to Check Point**" box and press on "**Finish**".
- vi. Set a new interface on SG for VMnet16 according to the Topology section.
- vii. Set a new Interface on SG according to the Topology section.

[Next Page]

- 3) Repeat the "**Enabling Interface Connections**" in this document, according to the Topology section.
- 4) At the SMS's Gaia web interface, configure an IPv4 Static Route for VMnet16.

Add Destination Route

Destination:10 . 0 . 3 . 0

Subnet mask:255 . 255 . 255 . 0

Next Hop Type:Normal

Normal: Accept and forward packets.

Reject: Drop packets, and send *unreachable* messages.

Black Hole: Drop packets, but don't send *unreachable* messages.

Rank:Default: 60

Local Scope:☐

Comment:VMnet16

Add Gateway

Ping:☐

Add Gateway

Edit

Delete

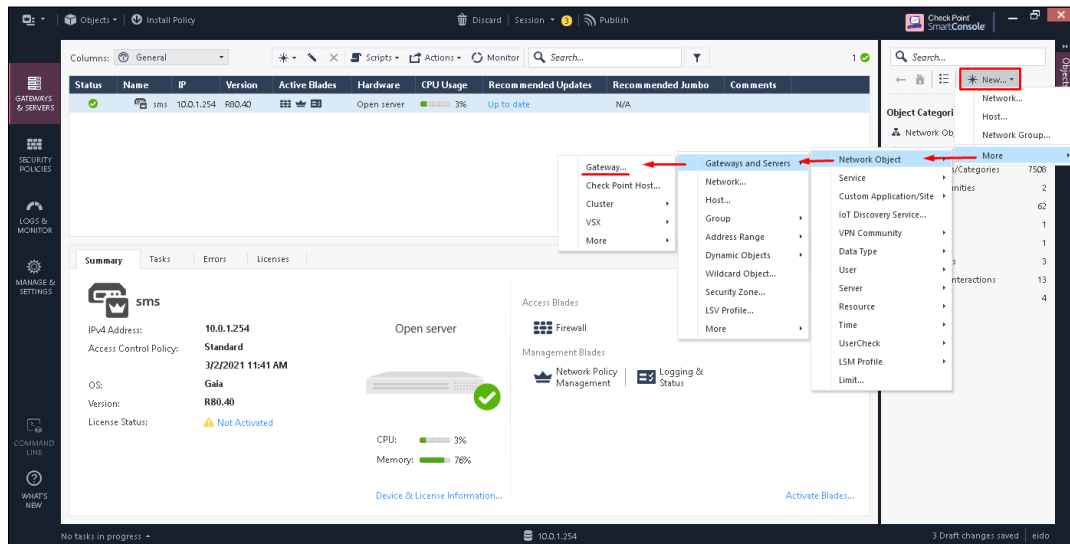
Gateway	Priority	Monitored Addresses
172.16.1.2	1	None

Save

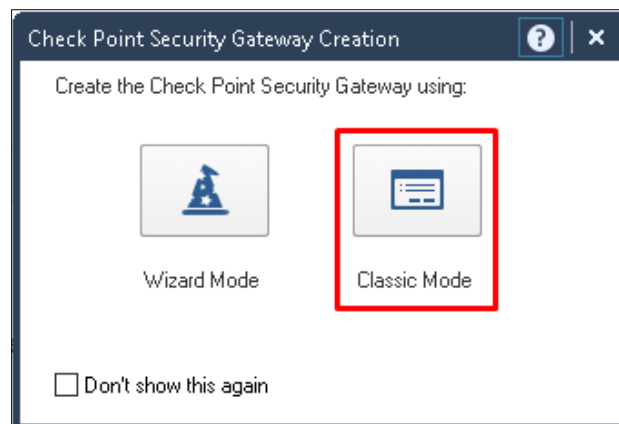
Cancel

Enabling SG in SMS

- 1) Open pc2 and click on the Smart Console.
- 2) At the right tab, create a new Gateway object.



- 3) Choose "**Classic Mode**".



[Next Page]

- 4) Input the SG IP address and then press on the **"Communication"** button.

Check Point Gateway - sg

Machine

Name: sg

IPv4 Address: 172.16.1.2

Resolve from Name

Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Uninitialized

Communication...

Platform

Hardware: Open server

Version: R80.40

OS: Gaia

Get

Network Security (1) Threat Prevention (0) Management (0)

Access Control:

☒ Firewall

☐ IPSec VPN

☐ Policy Server

☐ Mobile Access

☐ Application Control

☐ URL Filtering

☐ Identity Awareness

☐ Content Awareness

Advanced Networking & Clustering:

☒ Dynamic Routing

☒ SecureXL

☐ QoS

☐ Monitoring

Other:

☐ Data Loss Prevention

☐ Anti-Spam & Email Security

Anti-Spam & Email Security

Comprehensive and multidimensional protection for organizations' email infrastructure. Updates are included.

File Explorer

OK

Cancel

- 5) Input the Secure Communication password according to the Topology section and press on **"Initialize"**.

Trusted Communication

Platform: Open server / Appliance

Authentication

One-time password:

Confirm one-time password:

Trusted Communication Initiation

Initialize

Certificate state: Uninitialized

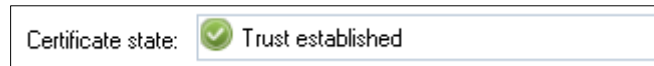
Test SIC Status...

OK

Cancel

[Next Page]

- If the connection was performed successfully, you'll see the following message at the bottom of the window;




6) Press on the "OK" button to finish the process.

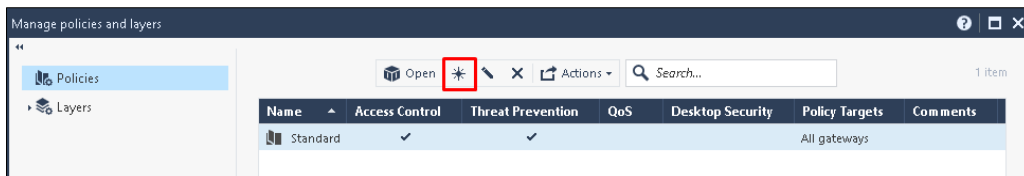
- If you followed this process correctly, the SG Will be shown in the Smart Console.

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo	Comments
—	sg	172.16.1.2	R80.40		Open server				
	sms	10.0.1.254	R80.40		Open server	3%	Up to date	N/A	

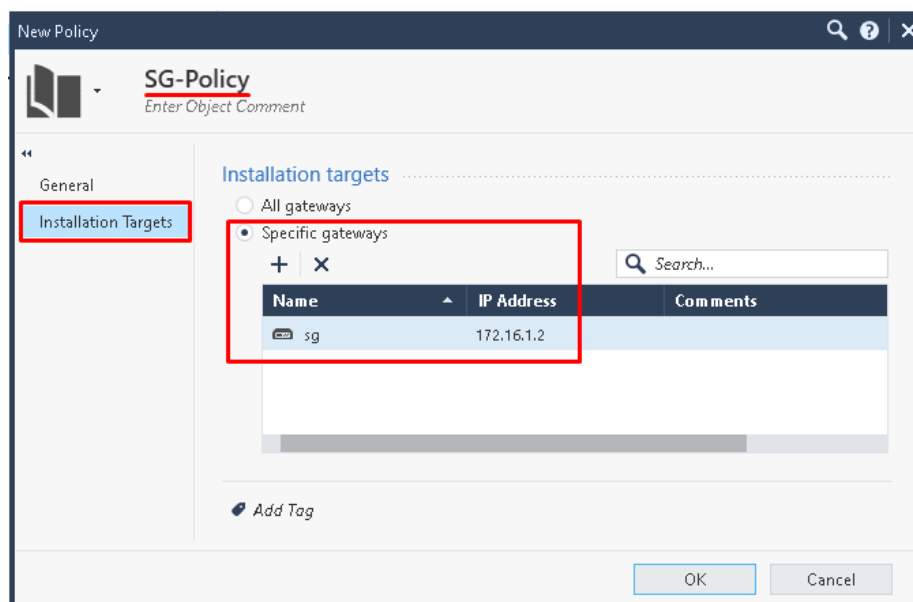
- 7) Repeat the " **Enabling Internet Connection** " process in this document for SMS.
- 8) Repeat the " **Enabling Internet Connection** " process in this document for SG.

Creating a New Policy

- 1) Open pc2 and access the Smart Console.
- 2) At the "SECURITY POLICIES" tab, press on the plus button **+** at the top left corner or type **ctrl + T** in order to access the "Manage Policies section".
- 3) Click on the "Manage policies and layers" button  Manage policies and layers...
- 4) At the opened window, press on the "New" button.













- 5) Name the new policy and press on "Installation Targets" at the left bar.
- 6) Choose the "Specific Gateway" option and add the SG firewall.



- Edit the Standard policy in the same manner- Make sure that it is only applied on the SMS firewall

[Next Page]

- 7) Repeat the "**Basic Rules**" section, under "**Security Policies**" in this document, for the SG policy.
- The only major difference is in the Management Rule, we are including the SMS and SG together in the rule (With pc2).
 - Make sure you are updating the Management Rule for the SMS policy as well.

No.	Name	Source	Destination	Services & Applications	Action	Track
1	Management Rule	 pc2  sms  sg	 sg  sms	 https  icmp-requests  ssh_version_2	 Accept	 Log

DC Server

In this section we'll present how to install a DC server and note only specific adjustments that were made according to our topologies.

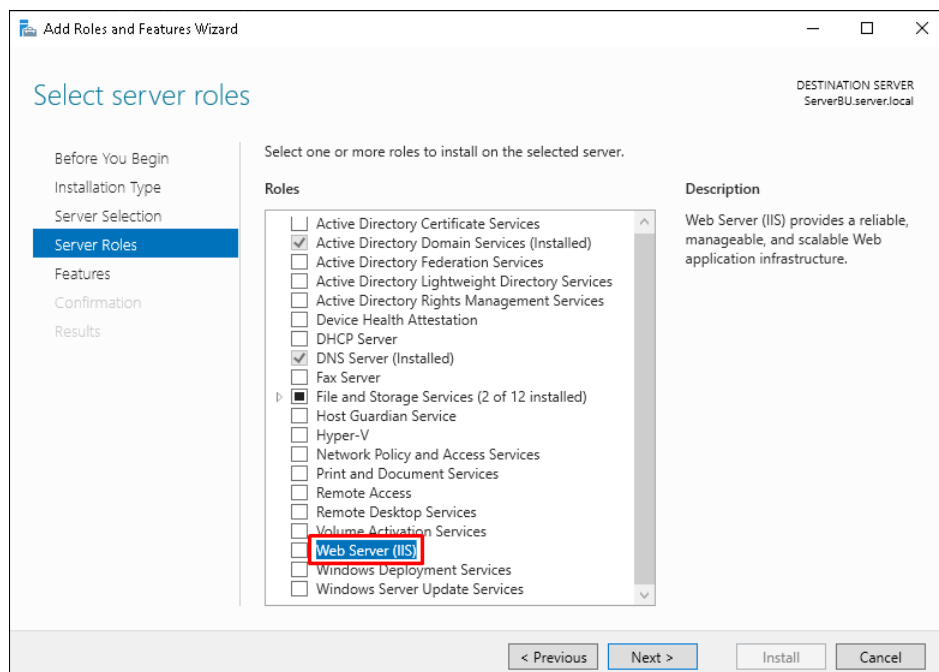
Configuration

Because our focus in this tutorial is on Check Point's R80.40 configurations and features, we will not display the entire process for setting our server. Instead, we suggest the reader to use the [MCSA Tutorial](#) for further guidance;

- ◇ Active Directory section.
 - In this this tutorial, we named our domain ***server.local***
- ◇ DNS section.
 - Set a DNS request forwarder to **8.8.8.8**
- ◇ Web Server;

Because the MCSA Tutorial doesn't explain how to add a Web Server, we'll explain how to do it.

- 1) Open the DC's Server Manager.
- 2) Press on **"Manage"** at the top-right corner and choose-
"Add Roles and Features"
- 3) Press on **"Next"** until you reach the **"Server Roles"** section.
- 4) Choose **"Web Server (IIS)"** and then press on **"Add Features"**.









- 5) Press on **"Next"** until you reach the **"Confirmation"** section-
Finally, press on **"Install"**.

Adding Clients to a Domain

In order to add our endpoints to the domain- **server.local** and enabling a proper connection with the server, we'll need to make some additions to the firewall rules.

- For understanding how the following mentioned rules were chosen, you can view the logs in SMS for the device you are currently configuring.
- 1) Change the "**Preferred DNS server**" for all the clients network configuration to- **10.0.2.1**
- 2) Disable the **Filter Rule** for the SMS and SG policies;













No.	Name	Source	Destination	Services & Applications	Action	Track
1	 Filter Rule	 Any	 Any	 nbdatagram	 Drop	 None

- We disabled the rule because currently we don't wish to filter something in particular.

- 3) Add the Following rule below the **Stealth Rule**, for the SMS and SG policies;

DC Domain Connection

This rule purpose is to enable all the services required for connecting endpoints to a Domain and log the actions.

No.	Name	Source	Destination	Services & Applications	Action	Track
1	DC Domain Connection	 Network Setup	 dc	 ldap  ldap_udp  Kerberos_v5_TCP  nbname  nbdatagram  microsoft-ds  ntp  tcp-high-ports	 Accept	 Log

- 4) Add the Following rule above the **Cleanup Rule**, for the SMS and SG policies;

Web Server Access

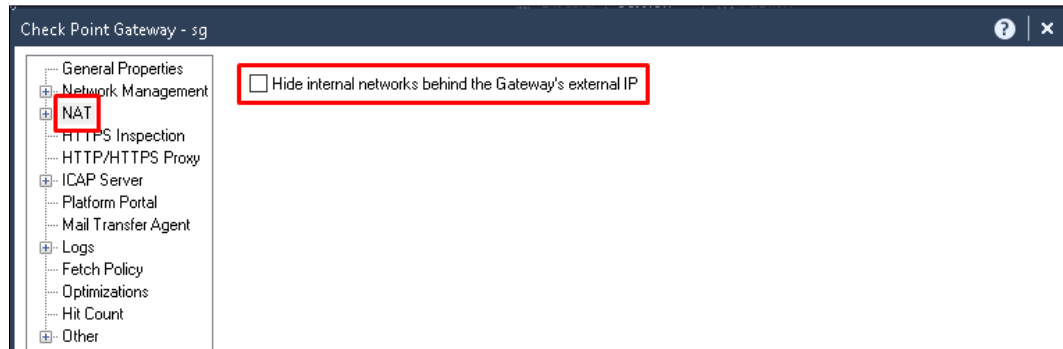
This rule purpose is to enable clients to have access to the Web Server and log their actions.

No.	Name	Source	Destination	Services & Applications	Action	Track
1	Web Server Access	 Any	 dc	 http	 Accept	 Log

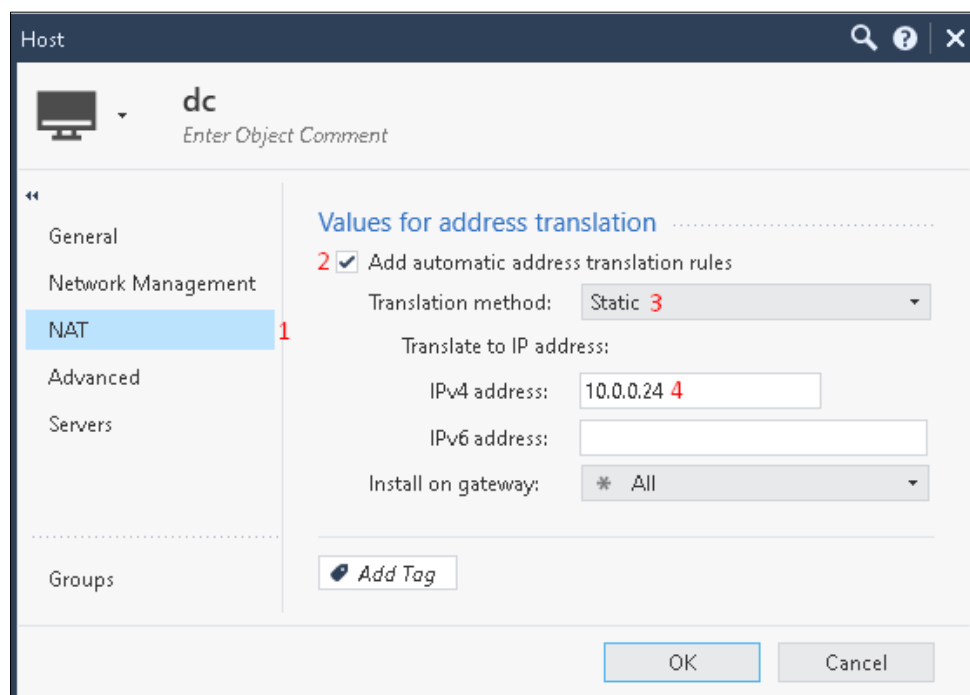
- 5) Add the domain to all the clients in your network.
 - If you are not familiar with how to do this step- Check the [MCSA Tutorial](#)'s "**Adding Devices to a Domain**" section.

Enabling Connection to Web Server

- 1) Open pc2, access the Smart Console.
- 2) Disable the NAT configuration for the SG and SMS gateways;
 - i. Go to the "**GATEWAYS & SERVERS**" tab.
 - ii. Click on the gateway you wish to configure.
 - iii. At the left bar, click on "**NAT**" and remove the checked boxed.

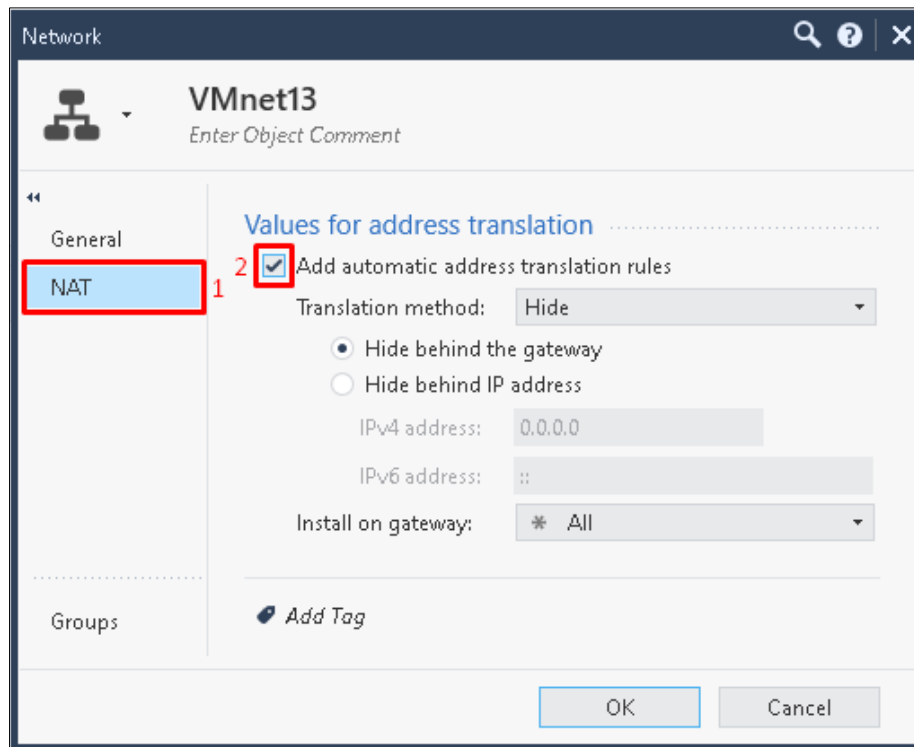


- 3) Configure a Static NAT for the dc host object;
 - i. Choose the relevant object.
 - ii. At the left panel, click on "**NAT**".
 - iii. Check the box of "**Add automatic address translation rules**".
 - iv. In "**Translation method**", choose "**Static**" and input the relevant IP address.

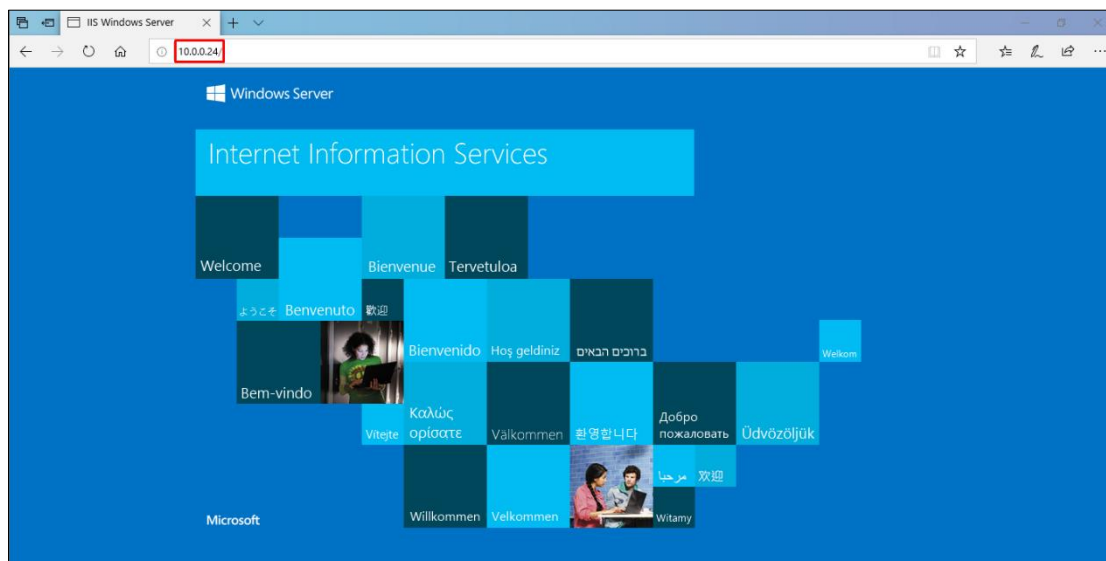


[Next Page]

- 4) Set all the networks that dc is not a part of them to be hidden behind NAT;
 - i. Choose the relevant object.
 - ii. At the left panel, click on "NAT".
 - iii. Check the box of "Add automatic address translation rules".
 - iv. In "Translation method", choose "Hide".



- If you correctly followed the instructions, you should be able to access the Web Server from a browser on a client;



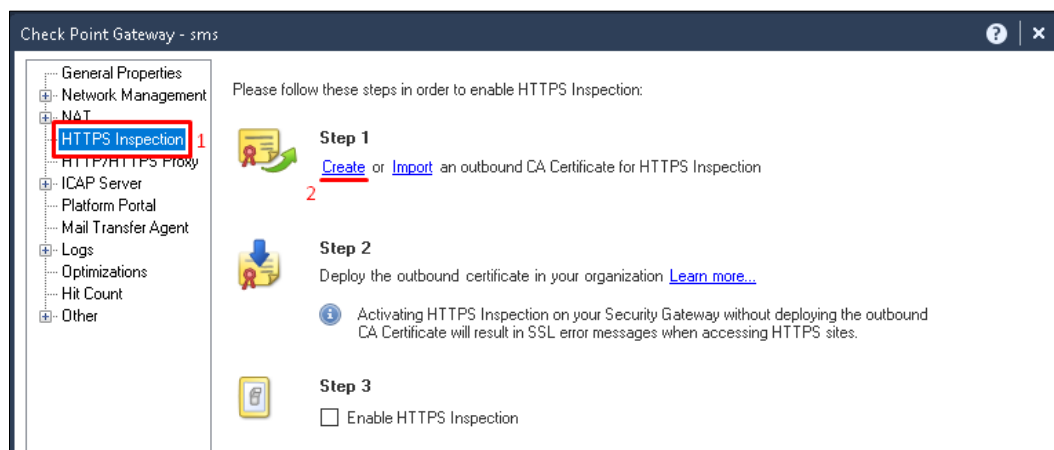
HTTPS Inspection

In this section we'll display how to set the HTTPS Inspection feature for a network.

- ❖ HTTPS- Hypertext Transfer Protocol Secure, is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL).
- ❖ HTTPS Inspection- HTTPS Internet traffic uses the SSL protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. With HTTPS Inspection, the Security Gateway can inspect the traffic that is encrypted by HTTPS.

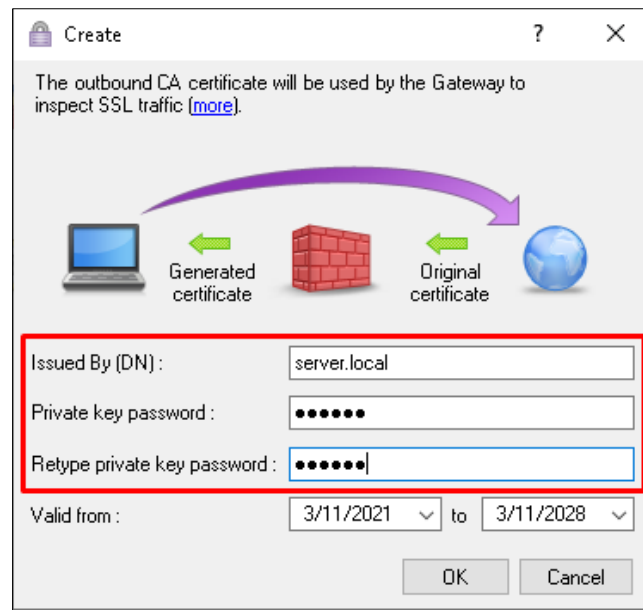
Enabling HTTPS Inspection

- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application.
- 3) At the main window, under the "**GATEWAYS & SERVERS**" tab- Double click on the existing Gateway.
- 4) At the left bar, press on "**HTTPS Inspection**" and click on the "**Create**" link.



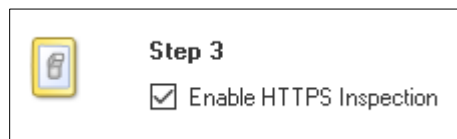
[Next Page]

- 5) At the opened window, input the credentials according to the Topology section.



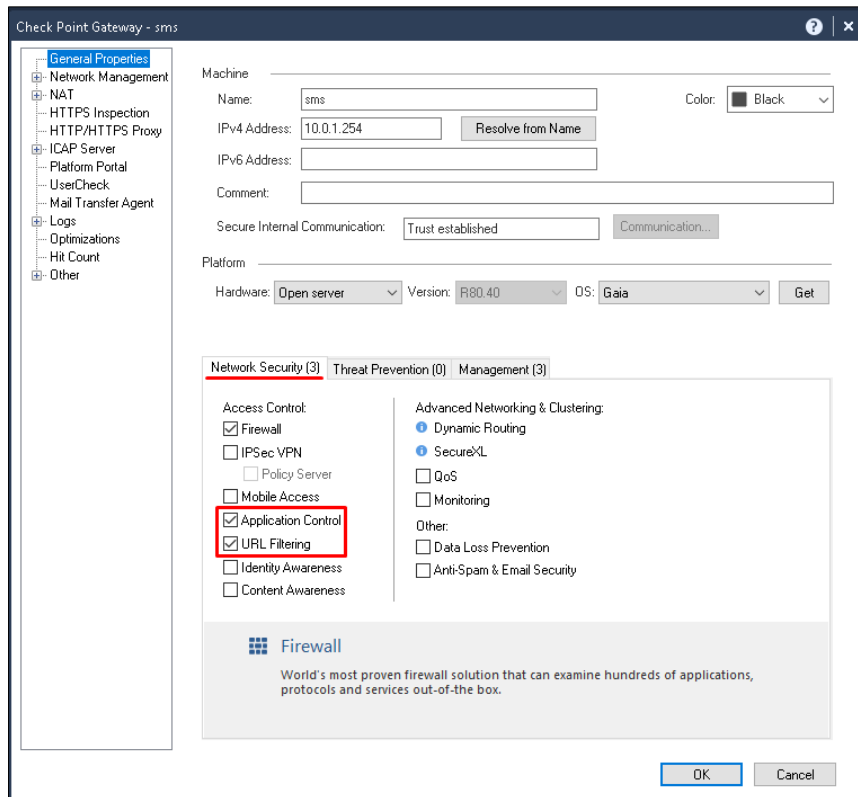
- Press on "OK" when you are done.

- 6) Check the "Enable HTTPS Inspection" box at Step 3.



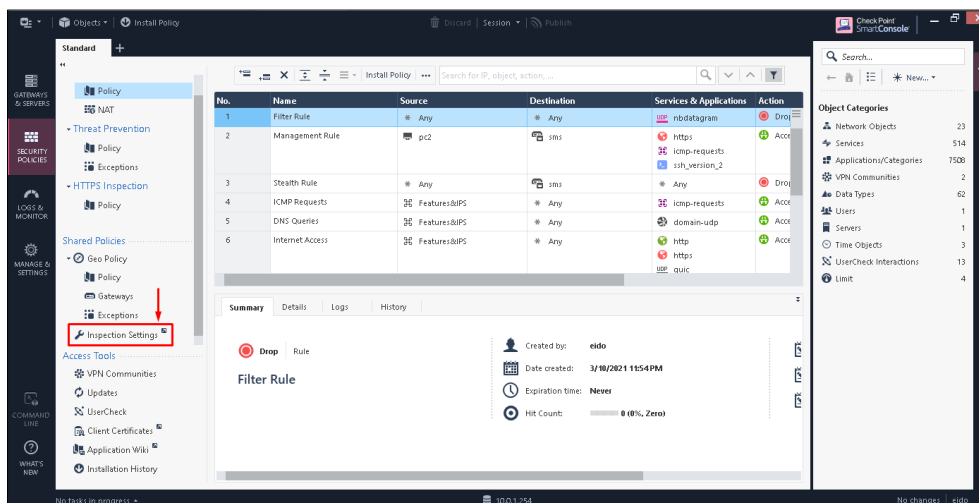
[Next Page]

- 7) At the left options bar, click on **"General Properties"**.
- 8) At the **"Network Security"** tab, mark the-
"Application Control" and **"URL Filtering"** check boxes.



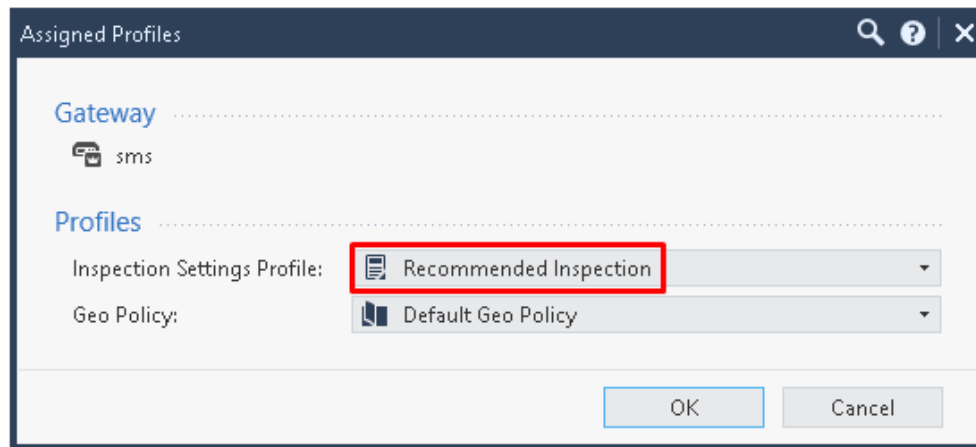
- Press on **"OK"** when you are done.

- 9) At the left main panel, choose **"SECURITY POLICIES"**.
- 10) At the policy options panel, click on **"Inspection Settings"**.



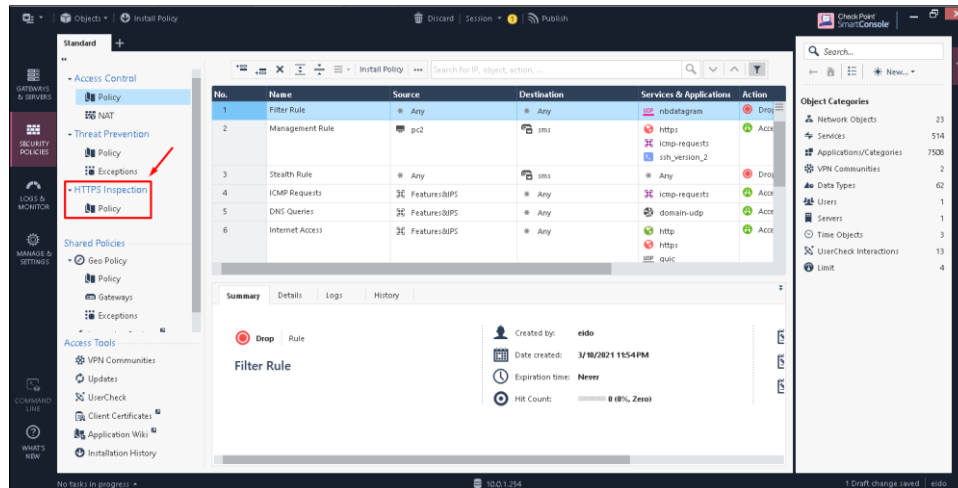
[Next Page]

- 11) At the left panel, choose "**Gateways**" and double click on the SMS configuration.
- 12) At the "**Inspection Settings Profile**" field change its value to- "**Recommended Inspection**".



Creating HTTPS Rules

- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application.
- 3) At the left main panel, choose **"SECURITY POLICIES"**.
- 4) At the policy options panel, under **"HTTPS Inspection"** click on **"Policy"**.



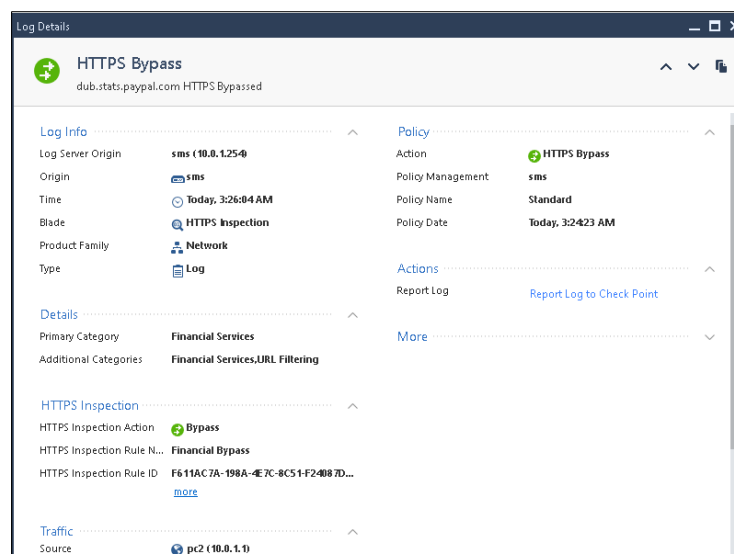
- 5) Add Rules according to your needs, similar to adding ordinary rules in your main Access Control policy.
 - In order to correctly follow this tutorial, add a rule according to the Instructions section;

Financial Bypass

This rule purpose is to ignore HTTPS connections made to Financial Institutes by clients in our network and to log each time the rule is triggered.

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track
1	Financial Bypass	* Any	Internet	HTTPS default s...	Financial Services	Bypass	Log

- If you correctly followed this guide you should see in the log an indication that the bypass rule worked;



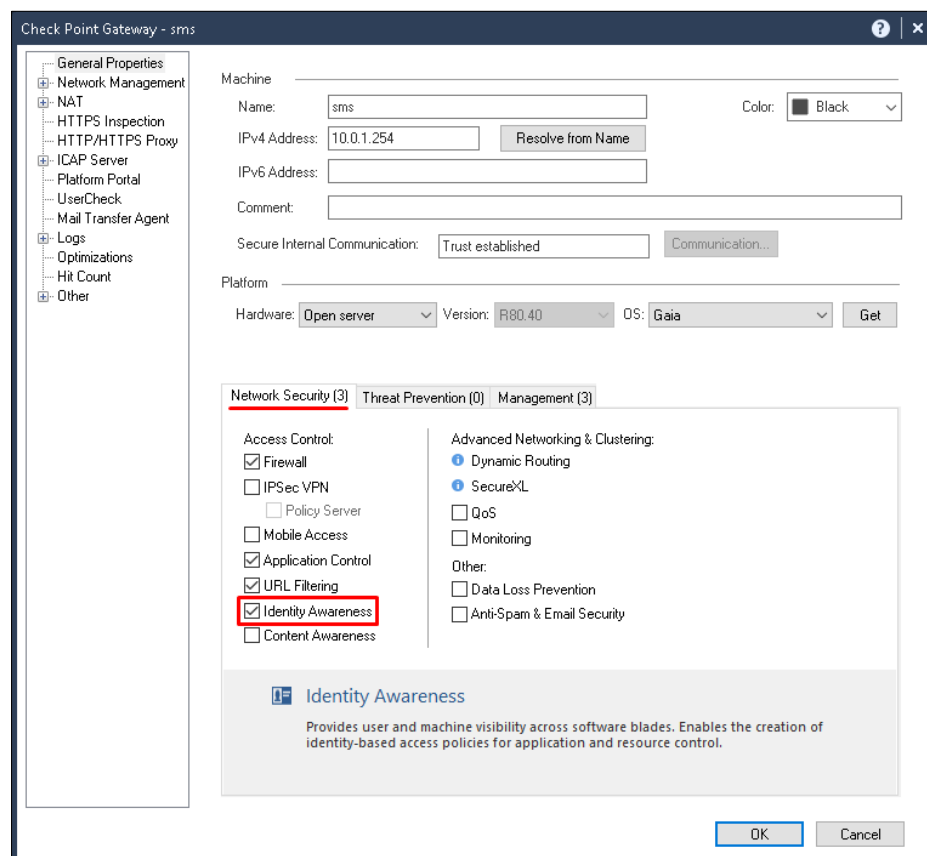
Identity Awareness

In this section we'll display how to apply the Identity Awareness feature for a network. We'll also present how to connect and sync our user management features with the DC.

- ❖ Identity Awareness- In most environments, a Check Point Gateway will not directly handle the access request to join a network. The Identity Awareness feature import identity elements from other sources (AD Domain access, Wi-Fi Access point, connecting multiple clients to a network etc.) in order to enforce user-based policy decisions.

Initial Setup

- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application.
 - Make sure you have the "DC Domain Connection" policy rule enabled before you begin the setup.
- 3) At the main window, under the "GATEWAYS & SERVERS" tab- Double click on the existing Gateway.
- 4) At the "Network Security", mark the "Identity Awareness" checkbox.



[Next Page]

- 5) At the opened window-
Mark the "AD Query" and "Browser-Based Authentication" check boxes.

The screenshot shows the 'Methods For Acquiring Identity' window. It has a blue header with a gear icon and the title 'Methods For Acquiring Identity'. Below the header, it says 'Select how users will be identified by your security gateway.' There are three options, each with an icon and a checkbox:

- ☒ **AD Query**
The gateway seamlessly identifies Active Directory users and computers.
- ☒ **Browser-Based Authentication**
Transparent Kerberos authentication or Captive Portal.
- ☐ **Terminal Servers**
Identify individual users traffic coming from terminal servers (e.g. Citrix).
An [agent](#) is required on the terminal server.

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- 6) Input your DC credentials in order to connect it with the SMS.

The screenshot shows the 'Integration With Active Directory' window. It has a blue header with a gear icon and the title 'Integration With Active Directory'. Below the header, it says 'Select an Active Directory:'. There is a dropdown menu with 'Create new domain...' selected. Below this, there are four input fields, all of which are highlighted with a red border:

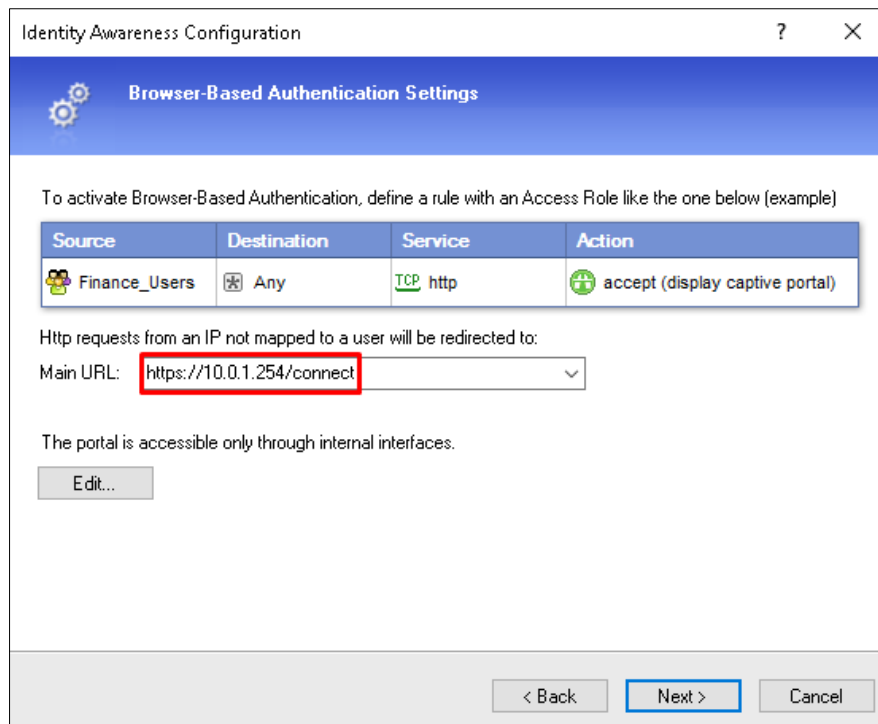
- Domain Name: server.local
- Username: Administrator
- Password: ••••••••
- Domain Controller: 10.0.2.1

Below the input fields, there is an information icon and the text 'Domain Administrator credentials are required.' At the bottom left, there is a 'Connect' button. To its right, the text 'Successfully connected!' is displayed in green and underlined. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- For assistance with the DC server, use the [MCSA Tutorial](#).
- Connect the other endpoints in your network with the Domain.

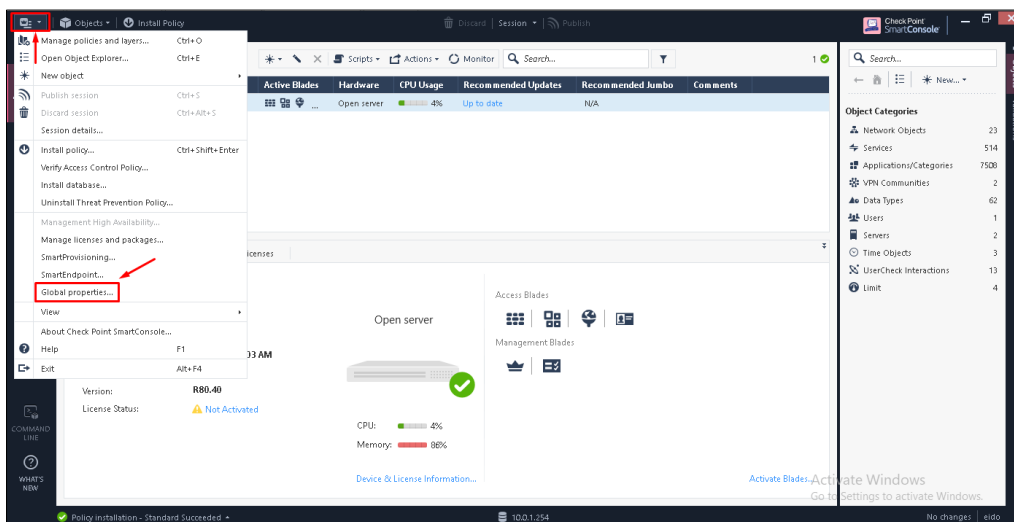
[Next Page]

- 7) Make sure to remember the address the users will be able to connect from.



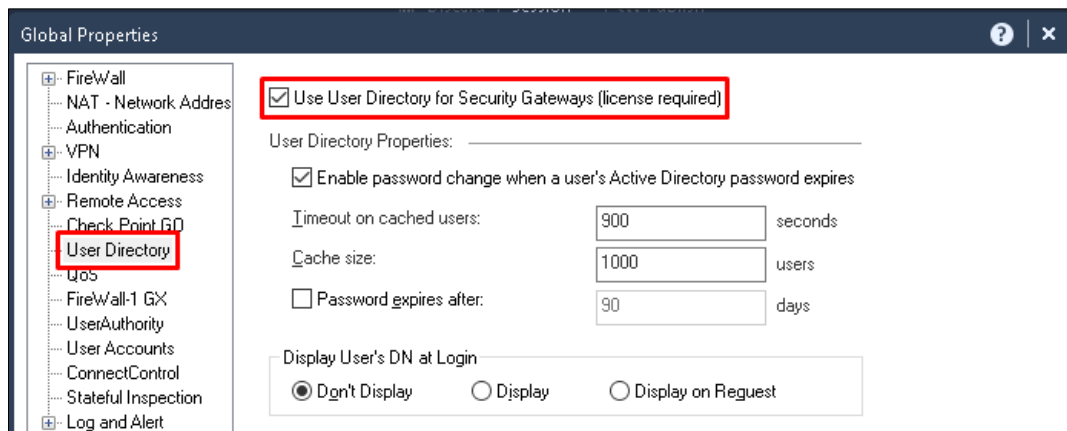
- Click on "Next" and then "Finish" when you are done.

- 8) At the main window, top-left corner, open the main options list and choose "Global properties".



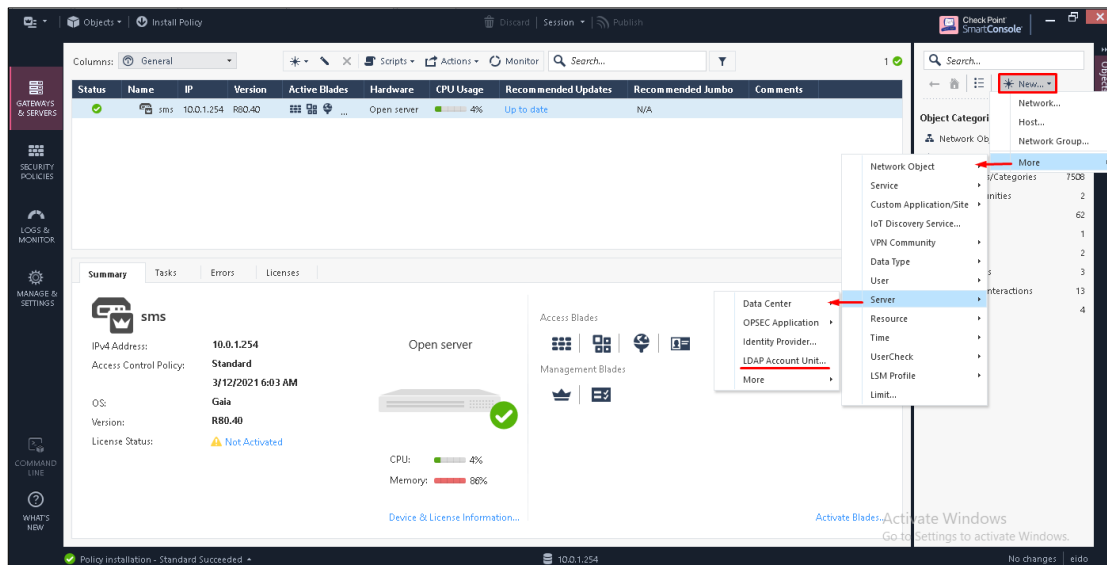
[Next Page]

- 9) At the left options panel, click on User Directory.
- 10) Mark the checkbox with the following text-
"Use User Directory for Security Gateways (license required)"

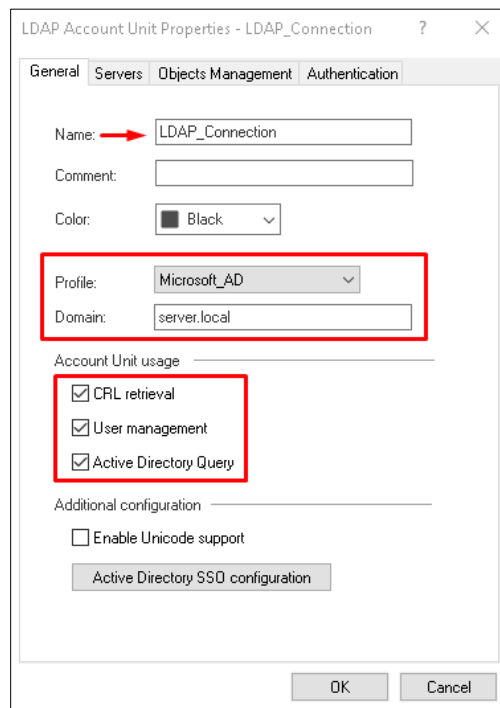


Creating an LDAP Object

- 1) At the right panel, press on **"New"**.
- 2) Next, click on **"More"**, then **"Server"** and choose **"LDAP Account Unit"**.

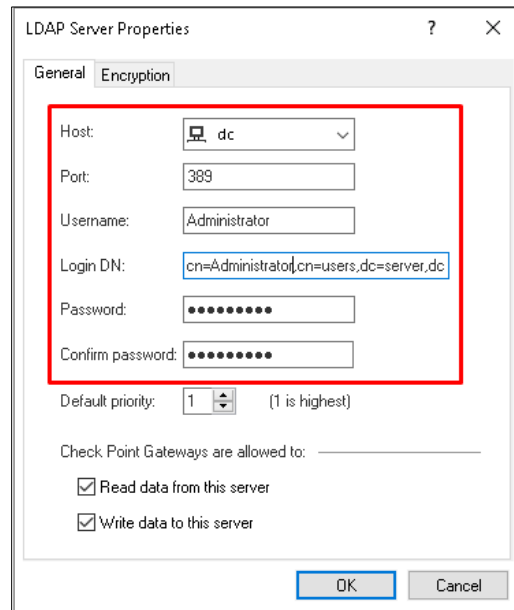


- 3) At the opened window, under the **"General"** tab;
 - i. Name the object according to the Topology section.
 - ii. Change the Profile value to **"Microsoft_AD"**.
 - iii. Input the name of your Domain.
 - iv. Make sure all the checkboxes are marks.



[Next Page]

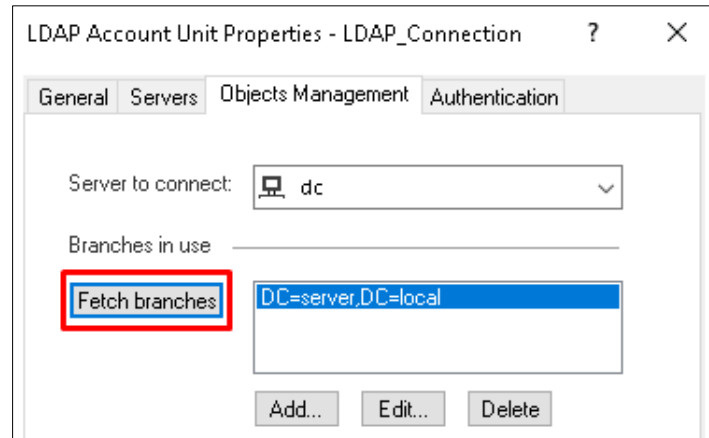
- 4) Under the "**Servers**" tab, click on "**Add**".
- 5) At the opened window, input the credentials you applied for the DC server.



The image shows the "LDAP Server Properties" dialog box with the "General" tab selected. A red rectangle highlights the "Host", "Port", "Username", "Login DN", "Password", and "Confirm password" fields. The "Host" is set to "dc", "Port" to "389", "Username" to "Administrator", and "Login DN" to "cn=Administrator,cn=users,dc=server,dc". The "Password" and "Confirm password" fields are filled with dots. Below these fields, the "Default priority" is set to "1" and "Check Point Gateways are allowed to:" is checked for "Read data from this server" and "Write data to this server". "OK" and "Cancel" buttons are at the bottom right.

- For this tutorial, input in the "Login DN" field-
"cn=<ADMIN-USER>,cn=users,dc=server,dc=local"

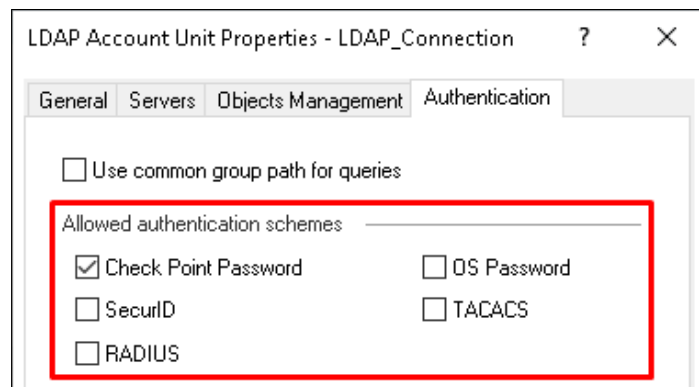
- 6) Under the "**Objects Management**" tab, press on "**Fetch Branches**".



The image shows the "LDAP Account Unit Properties - LDAP_Connection" dialog box with the "Objects Management" tab selected. A red rectangle highlights the "Fetch branches" button. The "Server to connect" is set to "dc". The "Branches in use" list contains "DC=server,DC=local". Below the list are "Add...", "Edit...", and "Delete" buttons.

[Next Page]

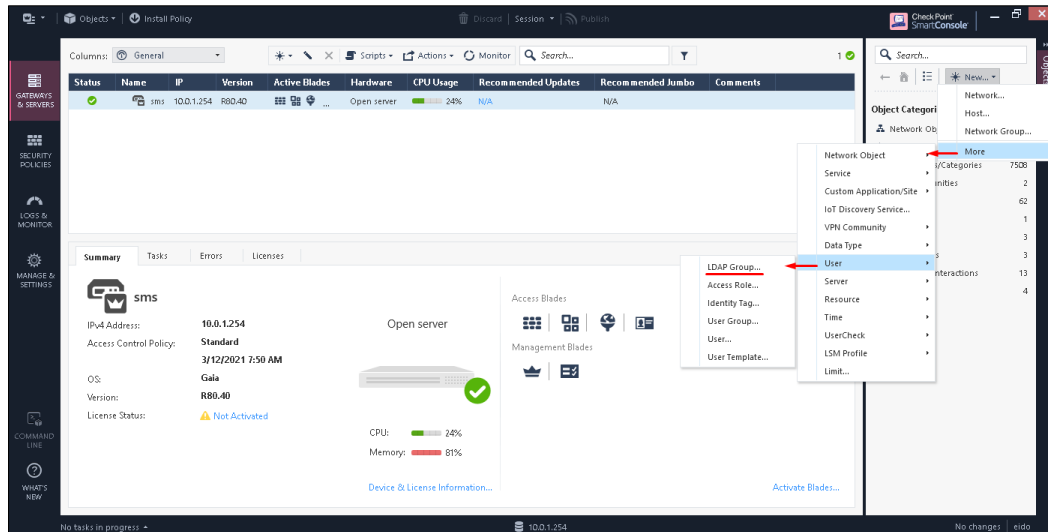
- 7) Under the "**Authentication**" tab, unmark all the checkboxes. Except of "**Check Point Password**".



Creating an LDAP Group & Access Roles

LDAP Group

- 1) At the right panel, press on **"New"**.
- 2) Next, click on **"More"**, then **"User"** and choose **"LDAP Group"**.



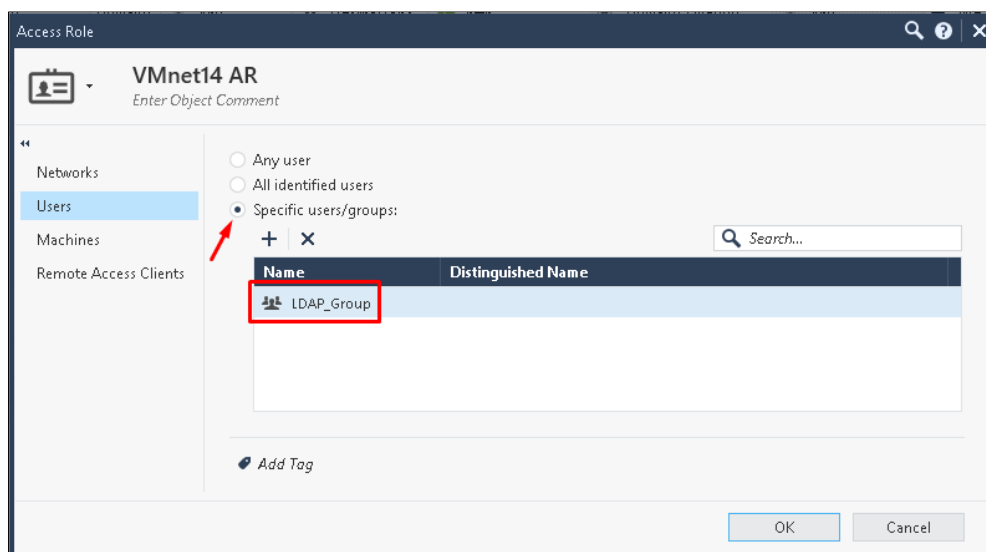
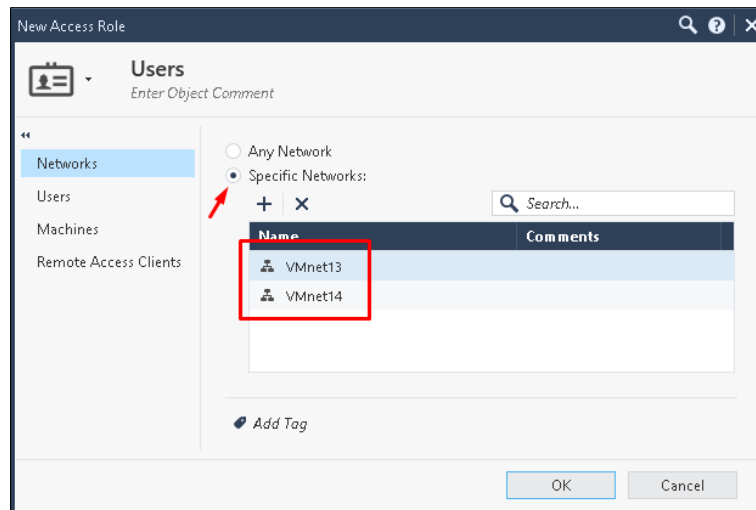
- 3) At the **"Account Unit"** field, input **"LDAP_Connection"**.

A screenshot of the 'New LDAP Group' dialog box. The title bar says 'New LDAP Group'. Below the title, there's a group icon and the text 'LDAP_Group' with a subtext 'Enter Object Comment'. The 'Account Unit' field is a dropdown menu showing 'LDAP_Connection', which is highlighted with a red rectangle. Below this, there's a section 'Group's Scope' with three radio button options: 'All Account-Unit's Users' (selected), 'Only Sub Tree ([optional prefix] . branch):', and 'Only Group in branch (DN prefix)'. The 'Only Sub Tree' option has a text field containing 'DC=server,DC=local'. The 'Only Group in branch' option also has a text field containing ',DC=server,DC=local'. Below the scope section is an 'LDAP Filter' section with a checkbox 'Apply filter for dynamic group' and an empty text field. At the bottom, there's an 'Add Tag' button and 'OK' and 'Cancel' buttons.

- Press on **"OK"** when you are done.

Access Roles

- 1) At the right panel, press on **"New"**.
- 2) Next, click on **"More"**, then **"User"** and choose **"Access Role"**.
- 3) At the opened window, input the credentials according to the Topology section;



- Press on **"OK"** when you are done.
- The Policy Rule for enabling users to connect will be presented in the URL Filtering section.

URL Filtering

In this section we'll present some of the basic capabilities the URL filtering feature is able to provide through a Gateway policy.

- ❖ URL Filtering- This feature enables Admins to apply rules for restricting or permitting access to URLs on the web, thus, reducing the chance that users will be exposed or be a part of a malicious activity.
 - We'll put more focus on the rules that need to be applied, based on the Instructions and Identity Awareness section.

Filtering Rules

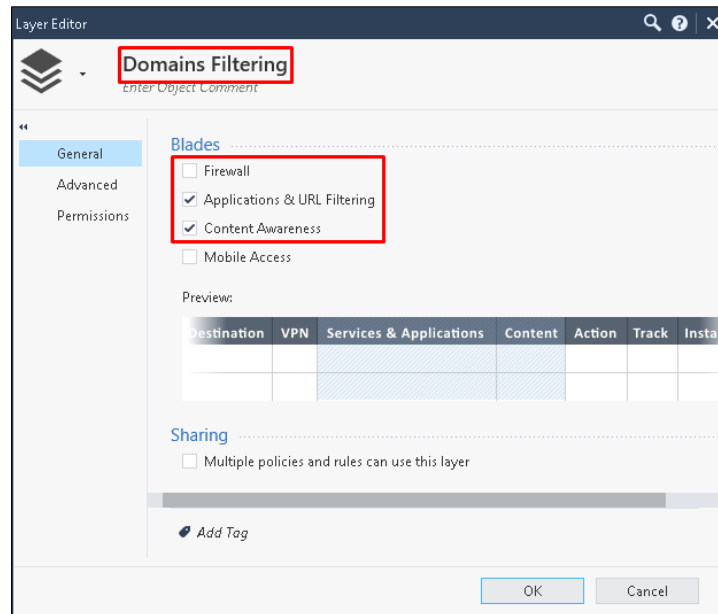
- 1) Open pc2.
- 2) At the desktop, enter the Smart Console application.
- 3) At the main window, go to "**SECURITY POLICIES**".
- 4) Create an Inline Layer;
 - i. Create an ordinary rule.
 - ii. At the "**Action**" column, right click on the new rule.
 - iii. Choose "**Inline Layer**" and click on "**New Layer**".

No.	Destination	Services & Applications	Action	Track	Install On
		UDP nbname UDP nbdatagram microsoft-ds ntp tcp-high-ports			
5	* Any	* Any	<div> <div>Accept</div> <div>Drop</div> <div>More ...</div> <div>Inline Layer</div> </div>	one	* Policy...
6	* Any	icmp-requests		g	* Policy...
7	* Any	domain-udp		g	* Policy...
8	* Any	http		g	* Policy...
		https			

- iv. Name the Inline Layer according to the Topology section.

[Next Page]

- v. Mark the checkbox of **"Applications & URL Filtering"**.
- vi. Remove the checkbox of **"Firewall"**.



- vii. At the left options bar, go to **"Advanced"**.
- viii. Under **"Implicit Cleanup Action"** choose **"Accept"**.
- ix. Press on **"OK"** when you are done.

5) Add the following rules for the Inline Layer group;

Main Layer Rule

In this rule we'll configure the first rules that will be applied for the users who belong to the Access Role we created.

► 4	Domains Filtering	* Any	ExternalZone	http https UDP quic	Domains Filtering	* Any	N/A
-----	-------------------	-------	--------------	---------------------------	-------------------	-------	-----

- You can disable the **"Internet Access"** rule.
- On how to set an External Zone;
 - ❖ External Zone- A predefined object in the Smart Console that when set by the Admin, it will represent network that are not in the intranet.
 - i. Open the Smart Console.
 - ii. At the main window, go to **"GATEWAYS & SERVERS"**.
 - iii. At the left options bar, press **"Network Management"**.
 - iv. Double click on the interface that's connected to external networks.
 - v. At the opened window, press on **"Modify"**.
 - vi. At the Security Zone area, check the **"Specify Security Zone"**.
 - vii. Choose the **"ExternalZone"** value and press **"OK"** when you are done.

YouTube Access

This rule will only allow the specified network to have access to YouTube.

4.1	YouTube Access	VMnet14 AR	ExternalZone	YouTube Allowed	Accept (display capti	* Any	Log	Acco
-----	----------------	------------	--------------	-----------------	-----------------------	-------	-----	------

- Make sure to mark the **"Enable Identity Captive Portal"** checkbox for the Accept Action.

Media Access

This rule will block any networks that try to access media related websites.

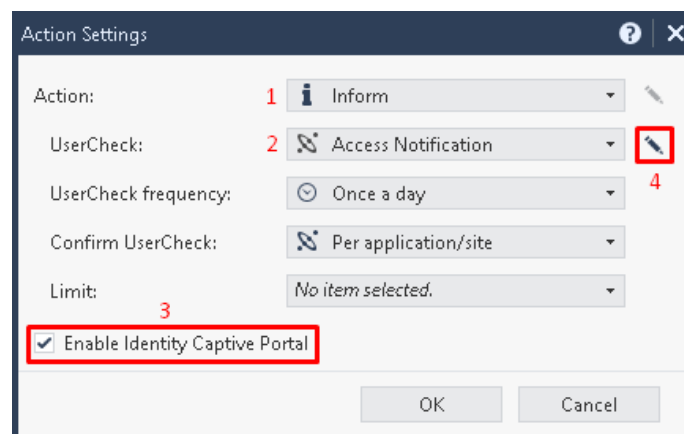
4.2	Media Access	* Any	ExternalZone	Media Sharing Media Streams	Drop	* Any	Log	Acco
-----	--------------	-------	--------------	--------------------------------	------	-------	-----	------

Social Media Access

This rule will present a notification to users before accessing Social Media websites.

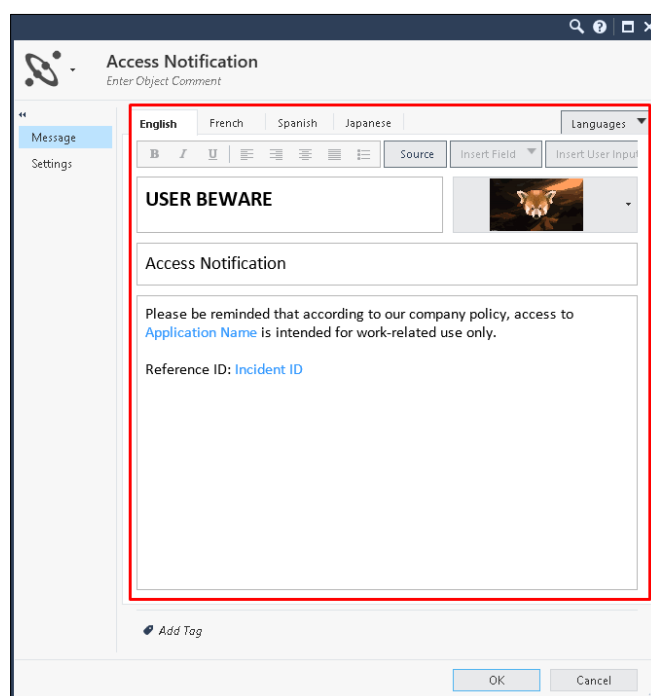
4.3	Social Media Access	Users	ExternalZone	Social Networking	Inform (display capti Access Notifica... Once a day Per applicatio...	* Any	Log	Acco
-----	---------------------	-------	--------------	-------------------	--	-------	-----	------

- How to create a notification;
 - Right click on the **"Action"** column.
 - Click on **"Inform"** and choose **"Access Notification"**.
 - Right click on the **"Action"** column and press on **"More"**.
 - Mark the **"Enable Identity Captive Portal"** checkbox.
 - At the **"User Check"** line click on the edit button.



[Next Page]

- vi. Edit the Access Notification message according to your needs.



CC Control

- 1) Open pc2 and click on the Smart Console.
- 2) Apply the Content Awareness feature;
 - i. At the main window, go to "**GATEWAYS & SERVERS**."
 - ii. Double click on the relevant Gateway.
 - iii. Under the "**Network Security**" tab, check the "**Content Awareness**" box.
- 3) Add the following rules for the Inline Layer group;

This rule will prevent from users to submit or receive CC data.

4.4	CC Control	* Any	ExternalZone	http	Drop	Any Direction PCI - Credit...	Log
-----	------------	-------	--------------	------	------	----------------------------------	-----




































[Next Page]

Cleanup Rule (Inline Layer)

Not like the original Cleanup Rule, if our traffic doesn't match the rules for the layer, we would like it to pass. Therefore, we'll set this rule with an Accept value.

No.	Name	Source	Destination	Services & Applications	Action	Track
5,4	Cleanup rule	* Any	* Any	* Any	 Accept	 None

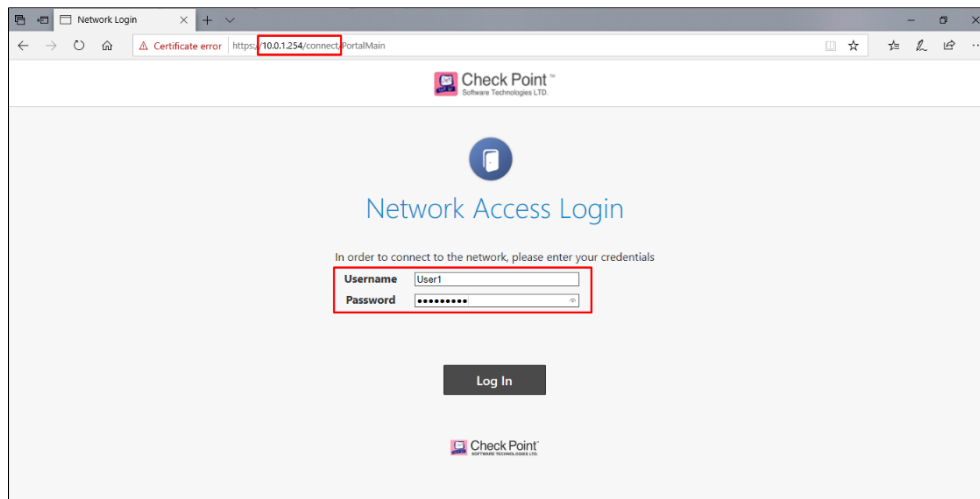
- If you correctly followed this process, the rules should look together as follow;

No.	Name	Source	Destination	Services & Applications	Action	Content	Track
▼ 4	Domains Filtering	* Any	 ExternalZone	 http  https  UDP quic	 Domains Filtering	* Any	 N/A
4.1	YouTube Access	 VMnet14 AR	 ExternalZone	 YouTube Allowed	 Accept (display capti	* Any	 Log  Acco
4.2	Media Access	* Any	 ExternalZone	 Media Sharing  Media Streams	 Drop	* Any	 Log  Acco
4.3	Social Media Access	 Users	 ExternalZone	 Social Networking	 Inform (display capti  Access Notifica...  Once a day  Per applicatio...	* Any	 Log  Acco
4.4	CC Control	* Any	 ExternalZone	 http	 Drop	 Any Direction  PCI - Credit...	 Log
4.5	Cleanup rule	* Any	* Any	* Any	 Accept	* Any	 Log

Testing the Rules

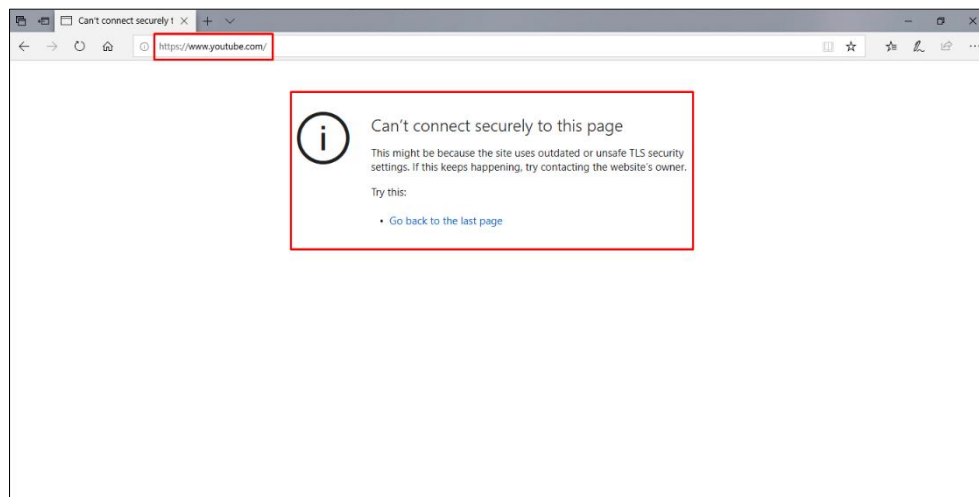
In order to verify all the rules are working as they should we'll need to create a user in our DC server. Should you require, we advise you to use [MCSA Tutorial](#) for additional guidance on how to do create users.

- 1) Create a user.
- 2) Choose a client, in the browser, type; "**https://10.0.1.254/connect**"
- 3) Input the user credentials according to the Topology section.



- 4) If you correctly enabled the rules the following will occur;

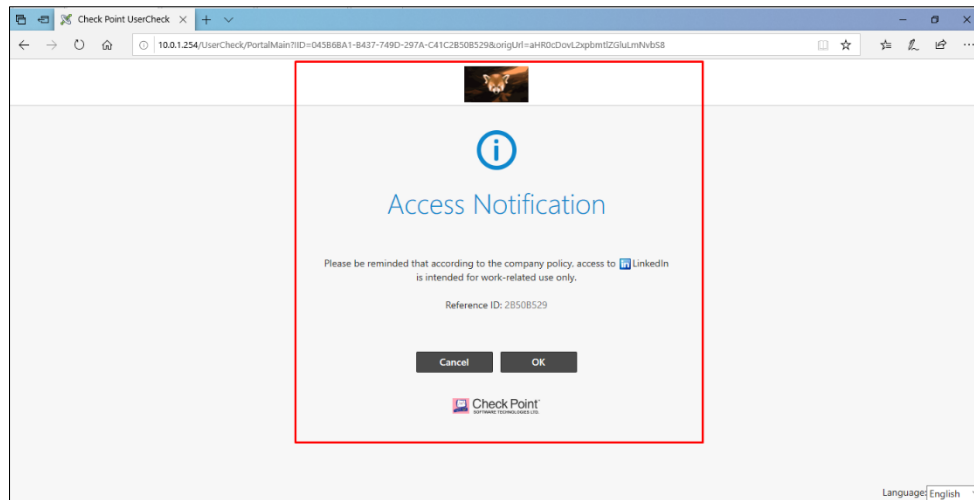
- i. You will not be able to access YouTube from pc2.



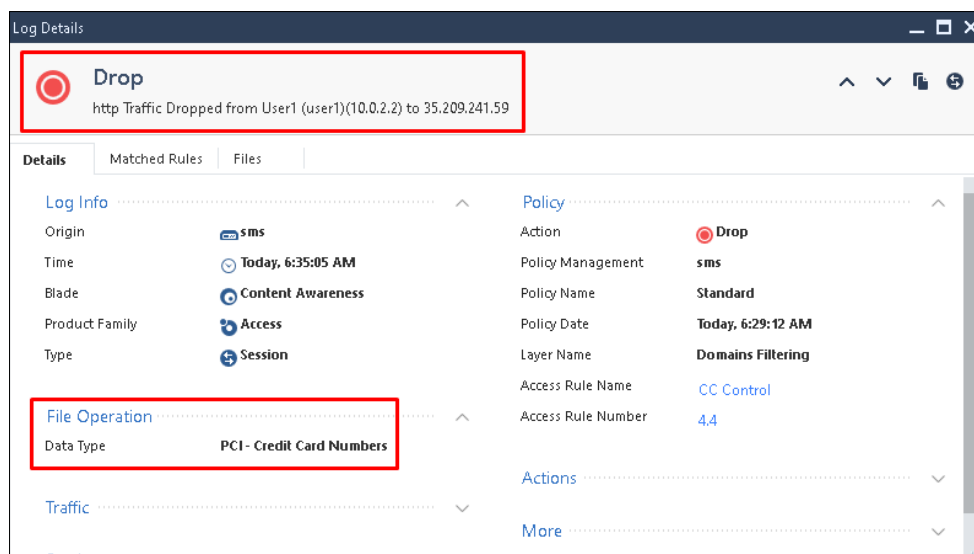
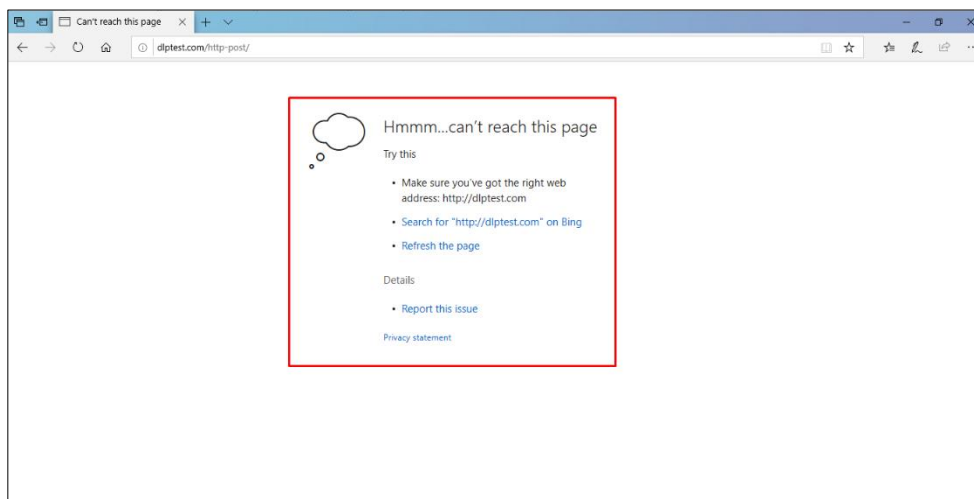
- On pc3 you suppose to have access to YouTube.

[Next Page]

- ii. When trying to access a Social Media website, you supposed to be presented with the following;



- iii. When trying to submit a fake CC number like 4580-0000-0000-0000 At <http://dlptest.com/http-post/> , you shouldn't be able to succeed;



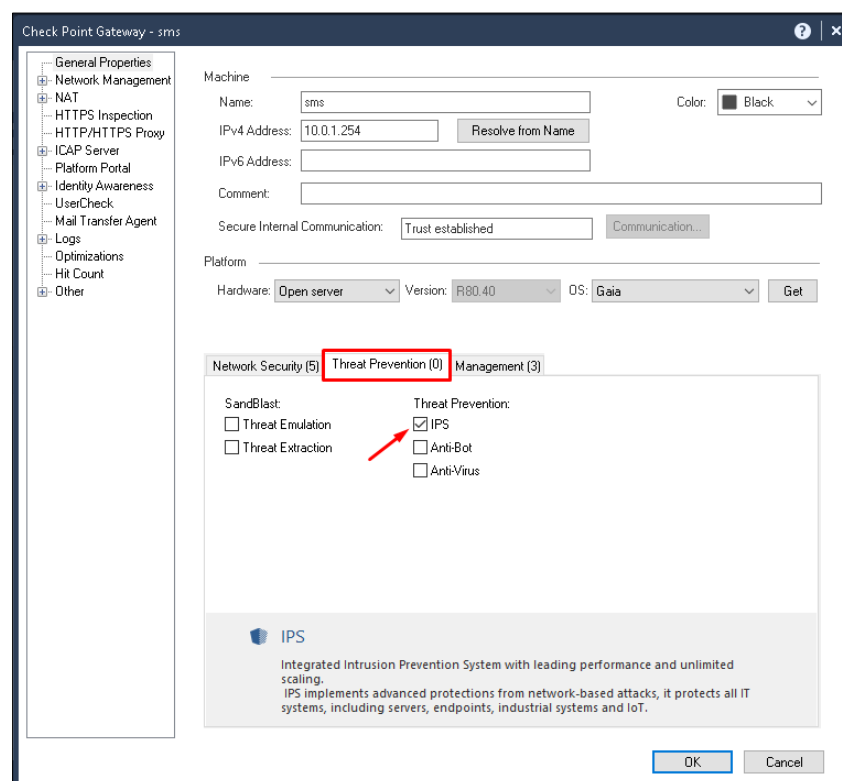
IPS

In this section we'll display how to enable the IPS Blade for our network and some of its basic capabilities.

- ❖ IPS- Intrusion Prevention System, is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
- ❖ Blade- A Software Blade is a Check Point's security application or module that's independent, modular and centrally managed. Using Blades allows organizations to customize their security configuration with the right mix of protection and investment, according to their needs.

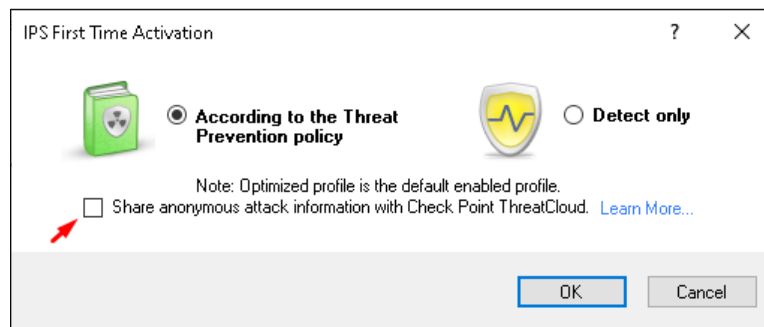
Enabling IPS

- 1) Open pc2 and click on the Smart Console.
- 2) At the main window, go to "**GATEWAYS & SERVERS**".
- 3) Double click on the relevant Gateway.
- 4) Press on the "**Threat Prevention**" tab and mark the "**IPS**" checkbox.



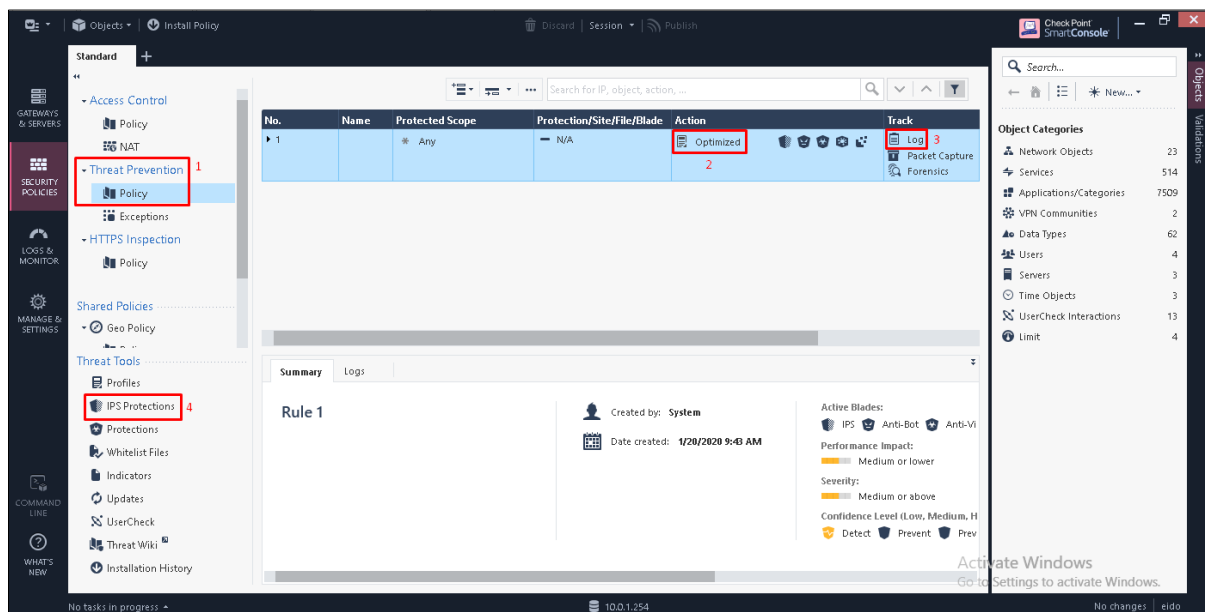
[Next Page]

- At the opened window, remove the checkbox and press on "OK".



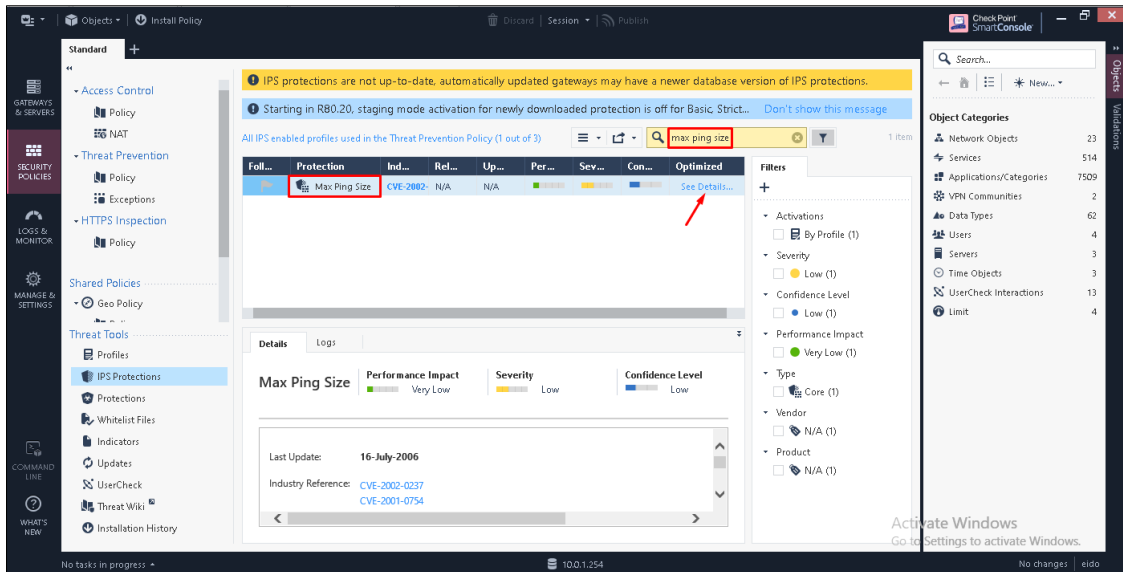
Setting A Rule

- Open pc2 and click on the Smart Console.
- At the main window, go to "SECURITY POLICIES".
- Press on the "Threat Prevention" Policy.
- Make sure that the Action column is set to "Optimized" and that the Track column is with a "Log" value.
- After validating the previous step, press on "IPS Protections" at the left options bar.

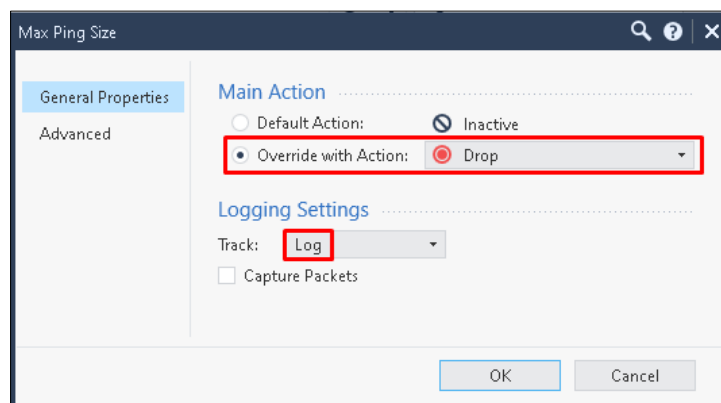


[Next Page]

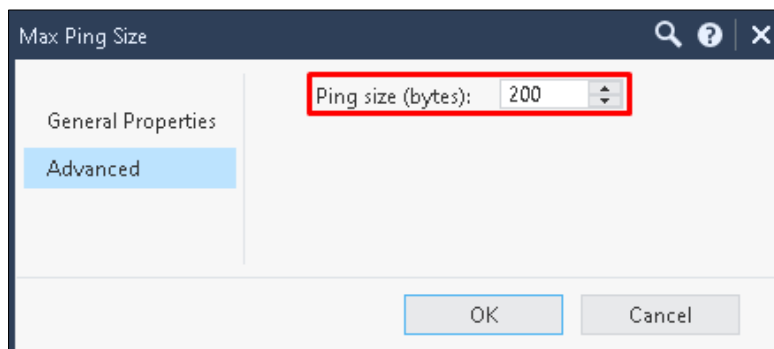
- 6) At the search bar, type **max ping size**.
- 7) Under the "**Optimized**" column, press on "**See Details**".



- 8) At the opened window, double click on the "**Optimized**" Profile.
- 9) At the "**General Properties**" section;
 - i. Mark the "**Override with Action**" option and choose the "**Drop**" value.
 - ii. Make sure the rule will be Logged.



- 10) At the "Advanced" section, set the "**Ping size (bytes)**" value according to your needs.



- For this tutorial, we set the value to 200.

Checking the Max Ping Size Rule

- 1) On pc2, open a terminal.
- 2) Type: **ping 10.0.1.254 -l 200**

```
C:\Users\pc2>ping 10.0.1.254 -l 200

Pinging 10.0.1.254 with 200 bytes of data:
Reply from 10.0.1.254: bytes=200 time<1ms TTL=64
Reply from 10.0.1.254: bytes=200 time=1ms TTL=64
Reply from 10.0.1.254: bytes=200 time<1ms TTL=64
Reply from 10.0.1.254: bytes=200 time<1ms TTL=64

Ping statistics for 10.0.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- The maximum size of allowed ping request is 200, therefore, the requests were able to be sent.

- 3) Type: **ping 10.0.1.254 -l 201**

```
C:\Users\pc2>ping 10.0.1.254 -l 201

Pinging 10.0.1.254 with 201 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- The above requests were blocked because they exceeded the maximum allowed bytes size of 200.

Conclusion

R80.40 is a comprehensive tool that I enjoyed practicing and using, the broad set of tools and the fact you are able to manage them from one source are something that I believe many security practitioners can enjoy. Although there are some products that might prove to be better at their field than a specific blade, I am highly recommending to use this tool for training and gaining knowledge in the cyber security industry.

This tutorial, doesn't cover the full capabilities of the system, for the full documentation and more. I suggest the reader to review the [R80.40 documentation](#) at Check Point's website.