Check Point®
SOFTWARE TECHNOLOGIES LTD.

Check Point Firewall R80.10 CCSA Complete Training Bootcamp

Lab Student Guide

v1.0

R80.10

Table of Contents

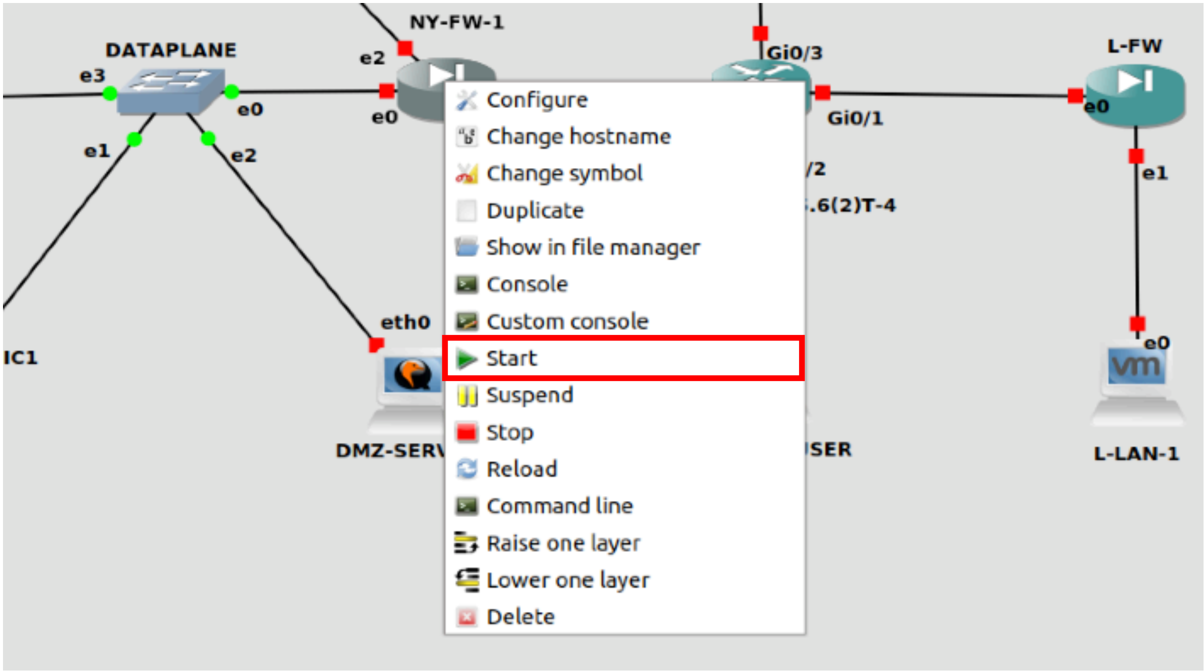
1.0 Lab: Install GAiA OS R80.10 on New York HQ Firewall

Lab Objectives

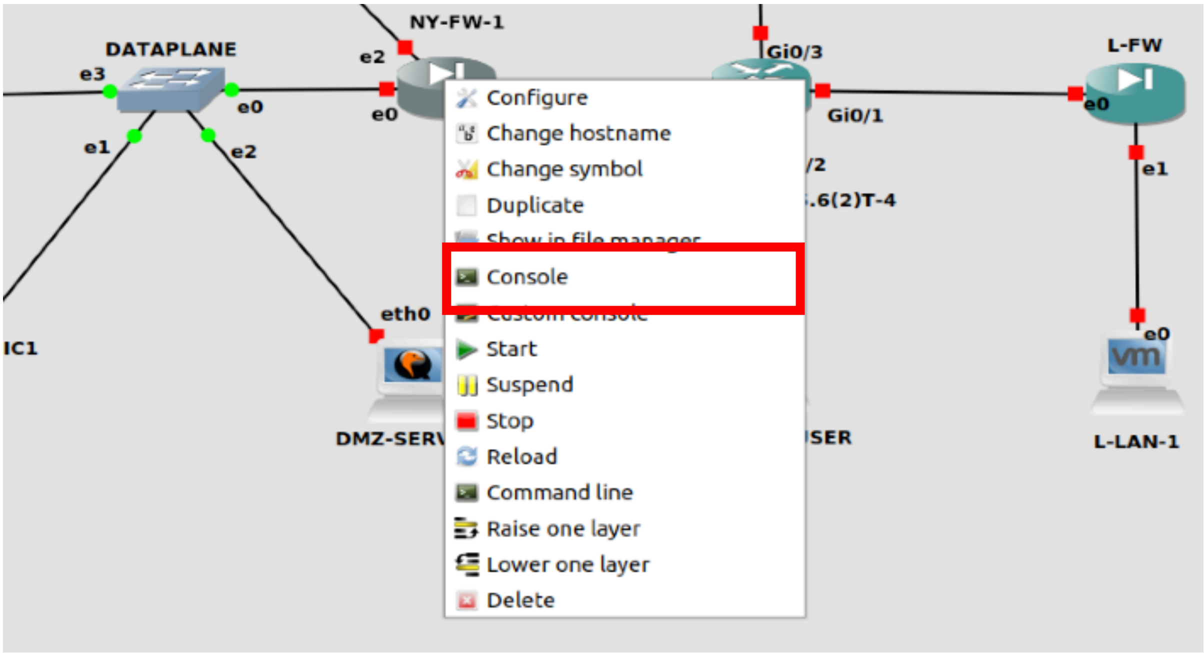
- Install GAiA OS on HQ Firewall – NY-FW-1

1.0 Start NY-FW-1 device and connect to the console

1. Right-click on NY-FW-1 and click **Start**

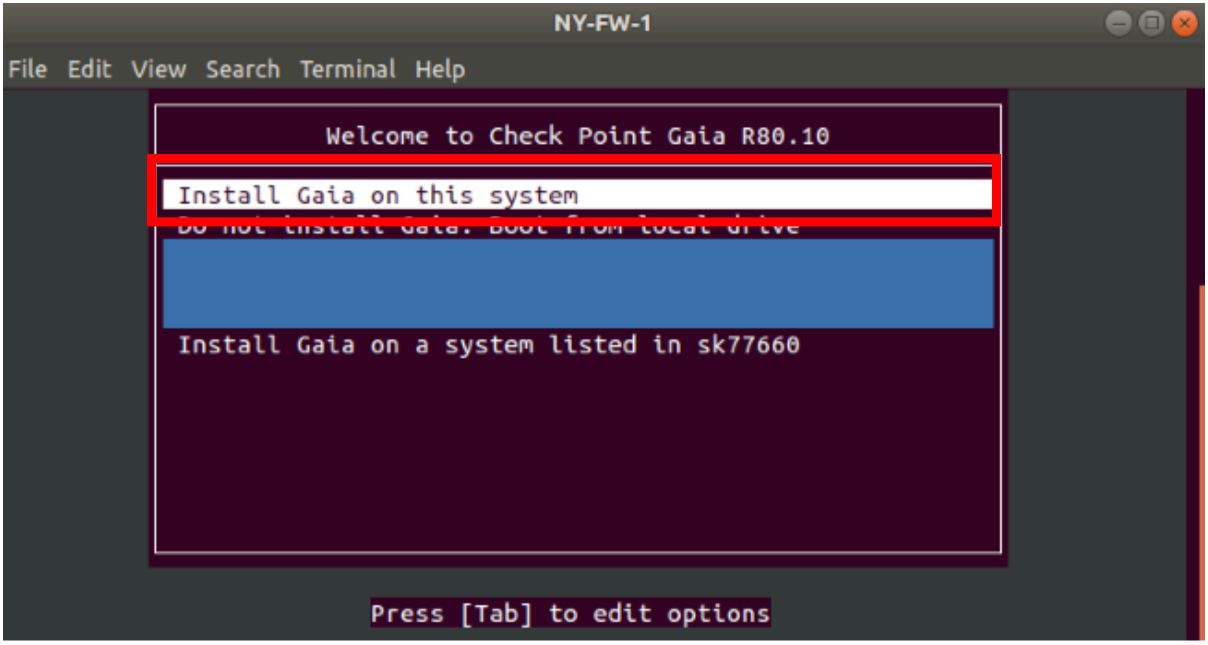


2. Right click on NY-FW-1 and click **Console**



2.0 Start GAiA OS installation process

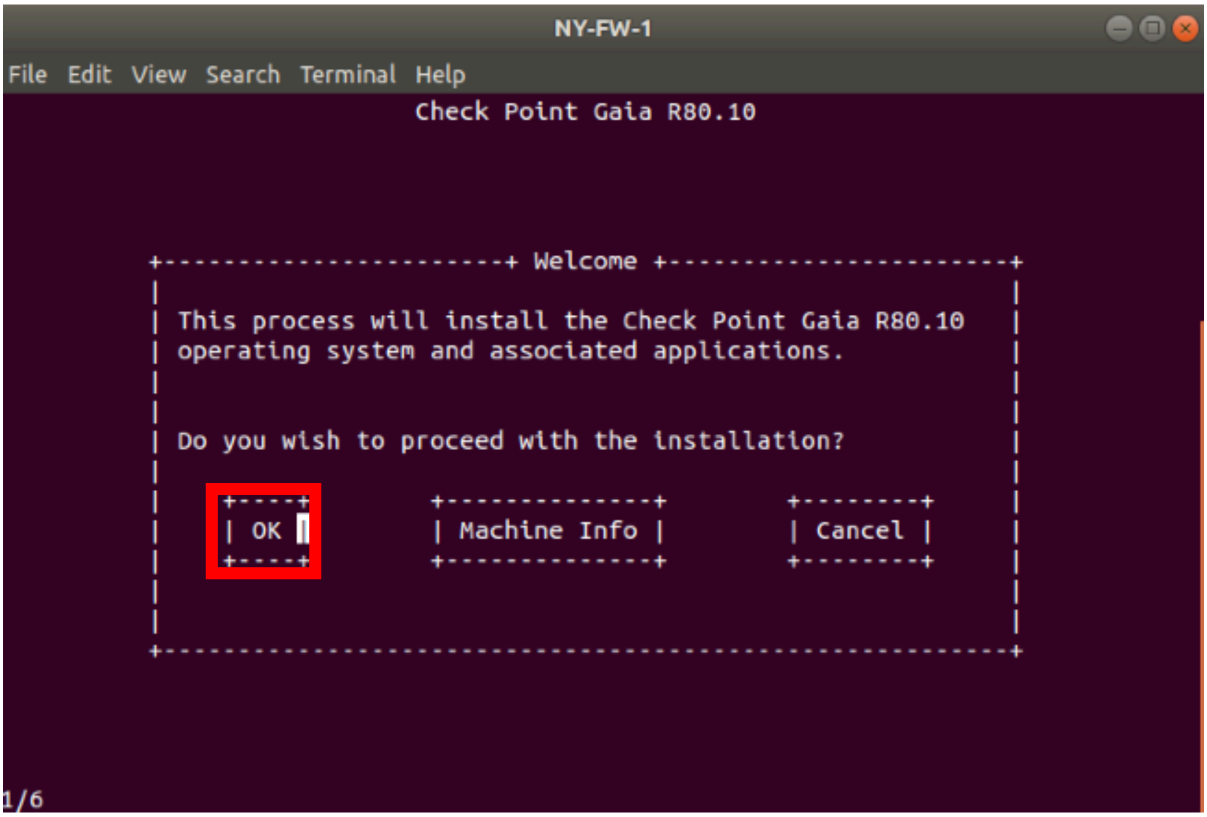
Select **Install Gaia on this system** and hit **Enter**



```
Welcome to Check Point Gaia R80.10

Install Gaia on this system
Do not install Gaia. Boot from local drive

Install Gaia on a system listed in sk77660

Press [Tab] to edit options
```

3.0 Confirm Check Point GAiA installation start

Select **OK** and hit **Enter.**



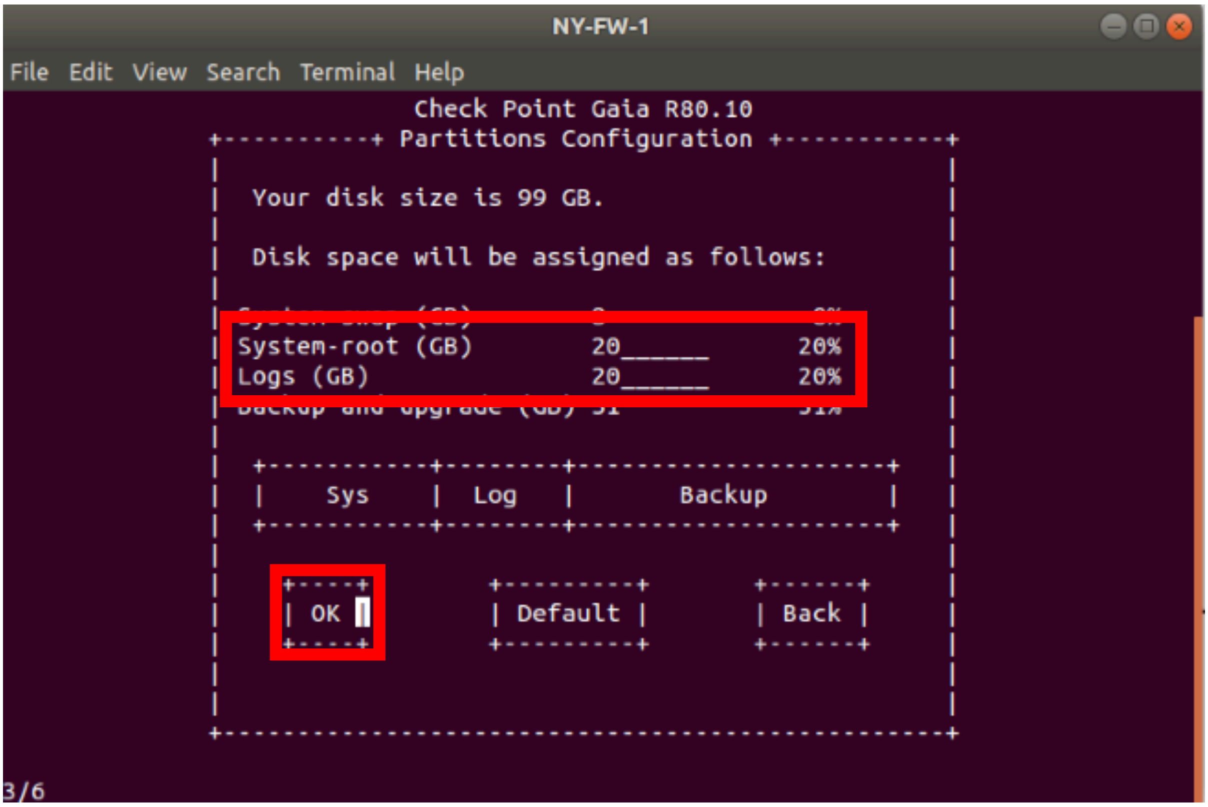
```
                         Check Point Gaia R80.10


+-----------------------+ Welcome +-----------------------+
|                                                          |
| This process will install the Check Point Gaia R80.10   |
| operating system and associated applications.            |
|                                                          |
|                                                          |
| Do you wish to proceed with the installation?            |
|                                                          |
|    +----+        +--------------+       +--------+       |
|    | OK |        | Machine Info |       | Cancel |       |
|    +----+        +--------------+       +--------+       |
|                                                          |
|                                                          |
+----------------------------------------------------------+

1/6
```

4.0 Let’s now increase **System-root** and **Logs** partitions’ size.

As a common practice, **Logs** partition can be increased in order to accommodate a larger amount of logs, which means visibility over a larger time window. Change the default values as follows:

Parameter	Value
System-root(GB)	20
Logs(GB)	20

Please note that **Backup and Upgrade(GB)** size adjusts automatically and is related to total disk size value and values configured for above partitions.



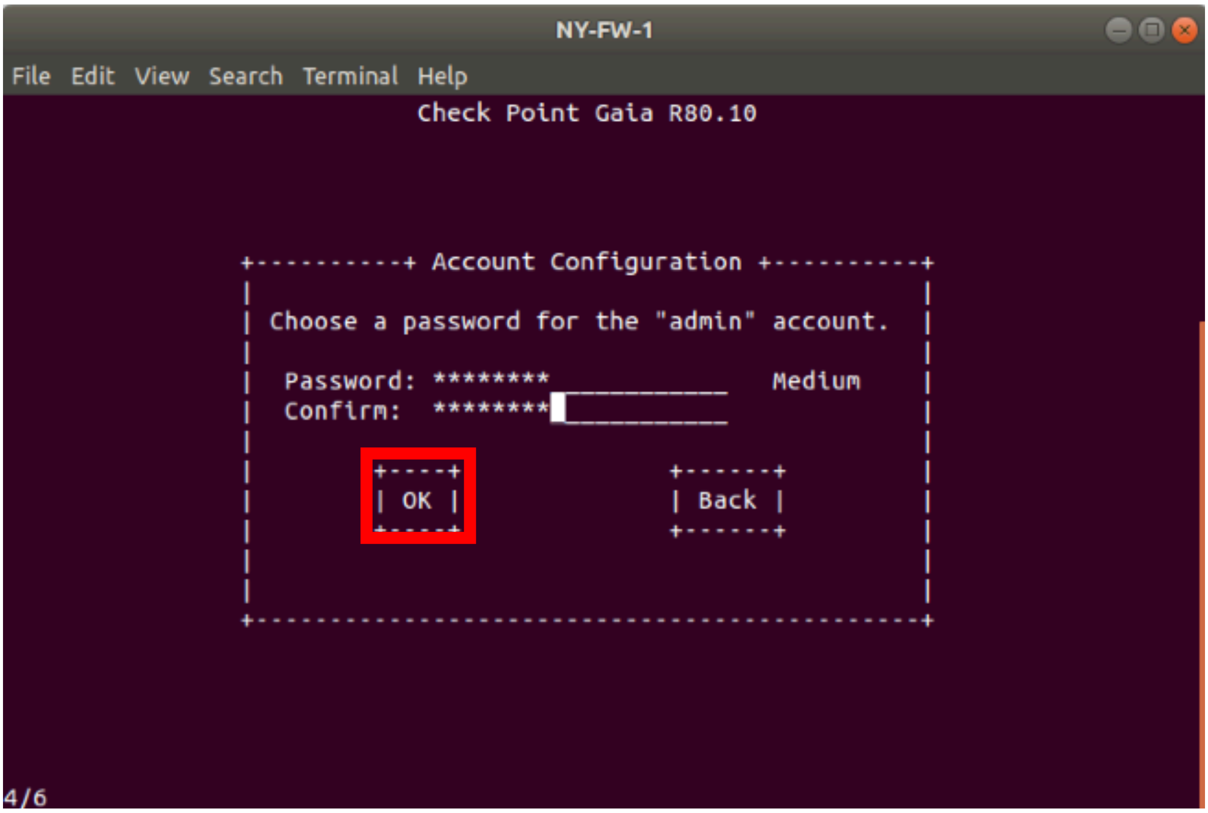
```
                    Check Point Gaia R80.10
         +----------+ Partitions Configuration +----------+
         |                                                 |
         |  Your disk size is 99 GB.                       |
         |                                                 |
         |  Disk space will be assigned as follows:        |
         |                                                 |
         | System-swap (GB)          8              8%     |
         | System-root (GB)          20______      20%     |
         | Logs (GB)                 20______      20%     |
         | Backup and upgrade (GB)   51            51%     |
         |                                                 |
         |  +-----------+--------+-------------------+    |
         |  |    Sys    |  Log   |       Backup      |    |
         |  +-----------+--------+-------------------+    |
         |                                                 |
         |  +----+        +---------+       +------+       |
         |  | OK |        | Default |       | Back |       |
         |  +----+        +---------+       +------+       |
         |                                                 |
         |                                                 |
         +-------------------------------------------------+
3/6
```

Select **OK** and hit **Enter** to continue.

5.0 Define password for the **admin** account

You will use this username and password pair in order to authenticate when connecting on the Check Point Gaia Firewall, either on Web UI or through an SSH session.

During the course I will use **admin/admin123** authentication credentials for Gaia OS devices, please define now the password for admin account at your own convenience.



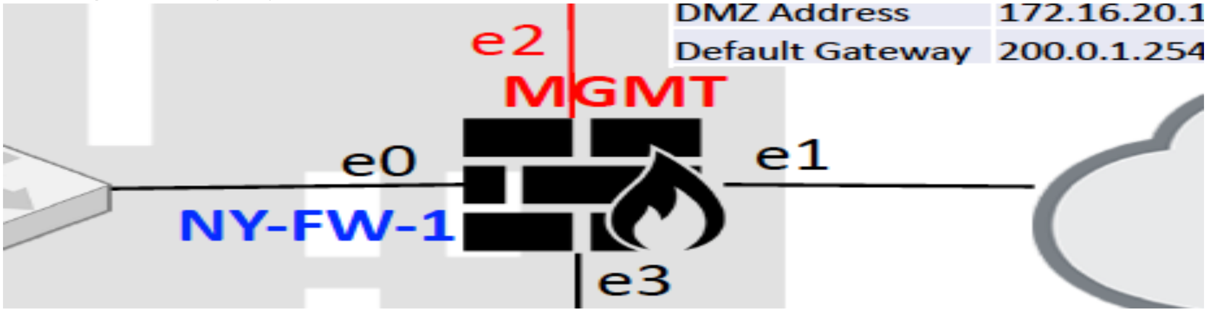
```
                        Check Point Gaia R80.10



          +----------+ Account Configuration +----------+
          |                                             |
          | Choose a password for the "admin" account.  |
          |                                             |
          |  Password: ********__________    Medium     |
          |  Confirm:  ********__________               |
          |                                             |
          |      +----+              +------+           |
          |      | OK |              | Back |           |
          |      +----+              +------+           |
          |                                             |
          |                                             |
          +---------------------------------------------+



4/6
```

Select **OK** and hit **Enter**.

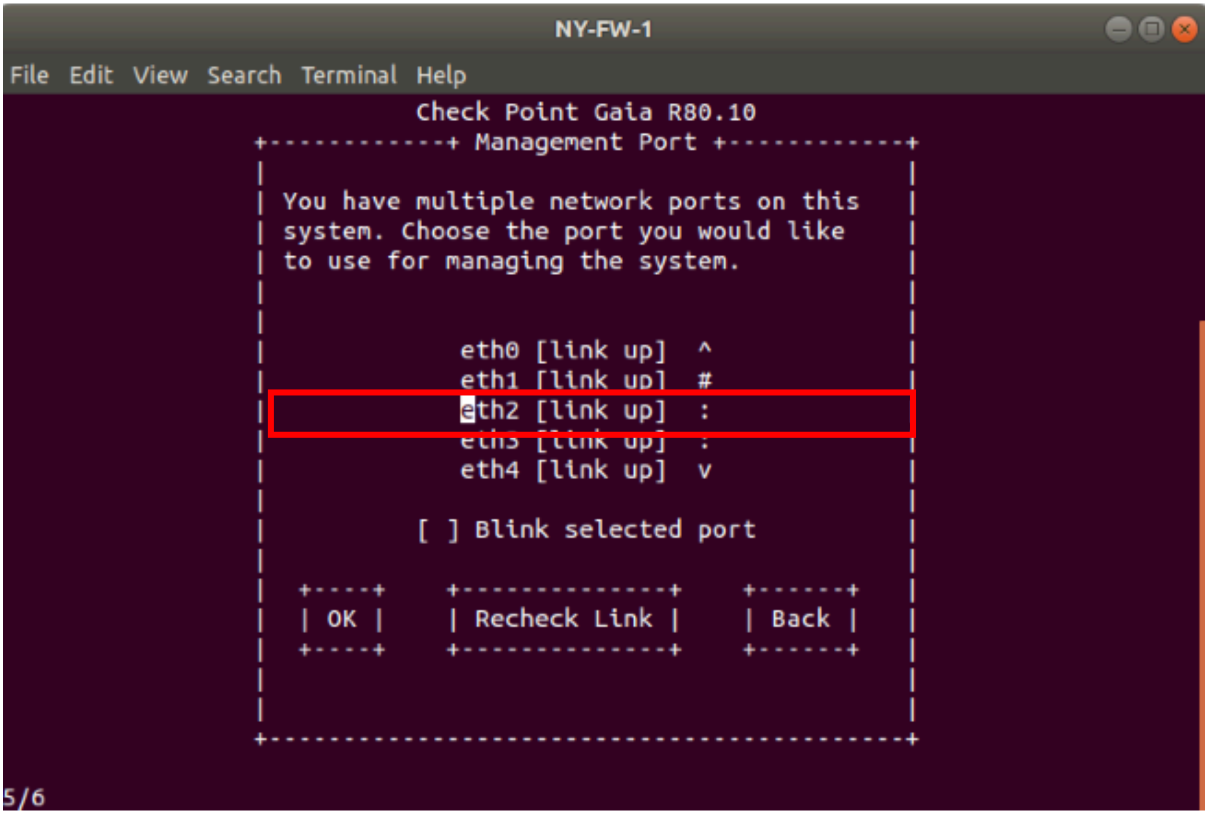
6.0 Define management port for NY-FW-1 Gaia Firewall

Please note that any port can be configured as the management port. The appliance will communicate through the management port with the Security Management Server, but first it establishes secure connectivity with the server (SIC – Secure Internal Communication).

Take a look on the Lab Diagram and note what is the port that will be used for management purposes.



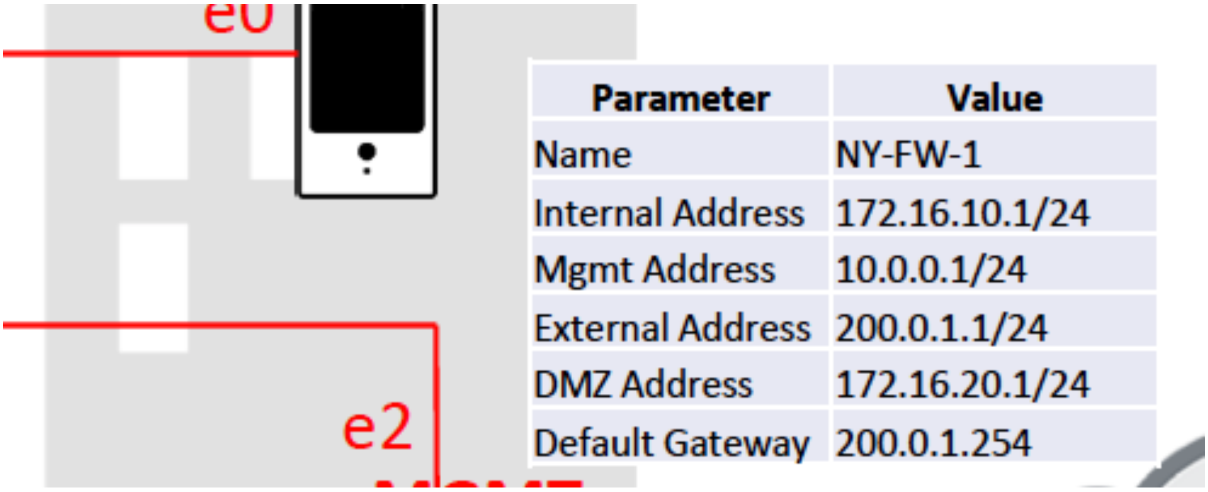
Navigate using the keyboard to **eth2** and hit **Enter** to continue.



```
                    Check Point Gaia R80.10
         +------------+ Management Port +------------+
         |                                           |
         | You have multiple network ports on this   |
         | system. Choose the port you would like    |
         | to use for managing the system.           |
         |                                           |
         |                                           |
         |             eth0 [link up]  ^             |
         |             eth1 [link up]  #             |
         |             eth2 [link up]  :             |
         |             eth3 [link up]  :             |
         |             eth4 [link up]  v             |
         |                                           |
         |          [ ] Blink selected port          |
         |                                           |
         |  +----+    +--------------+    +------+   |
         |  | OK |    | Recheck Link |    | Back |   |
         |  +----+    +--------------+    +------+   |
         |                                           |
         |                                           |
         +-------------------------------------------+
5/6
```

7.0 Define IP addressing configuration for management port.

Take a look on the Lab Diagram and note what is the IP addressing scheme that will be used for the management port.

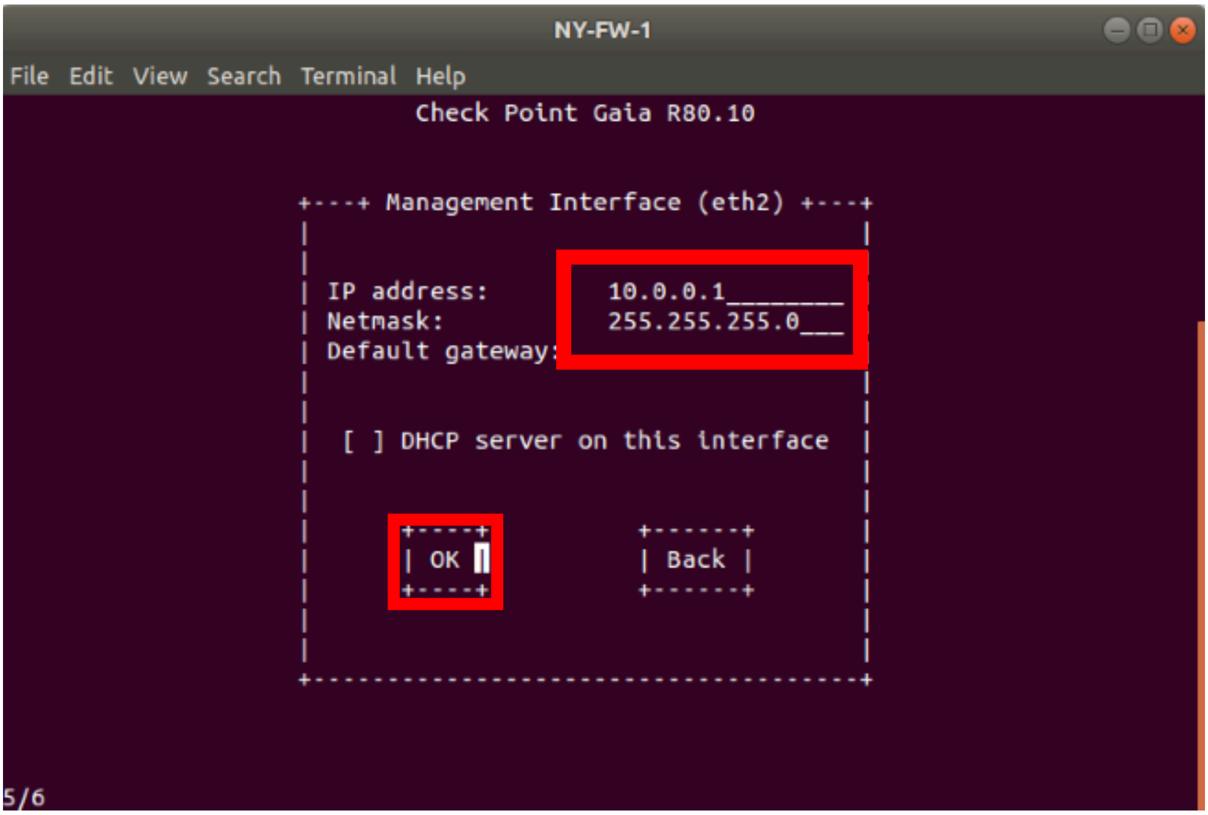


Parameter	Value
Name	NY-FW-1
Internal Address	172.16.10.1/24
Mgmt Address	10.0.0.1/24
External Address	200.0.1.1/24
DMZ Address	172.16.20.1/24
Default Gateway	200.0.1.254

Fill in the following details:

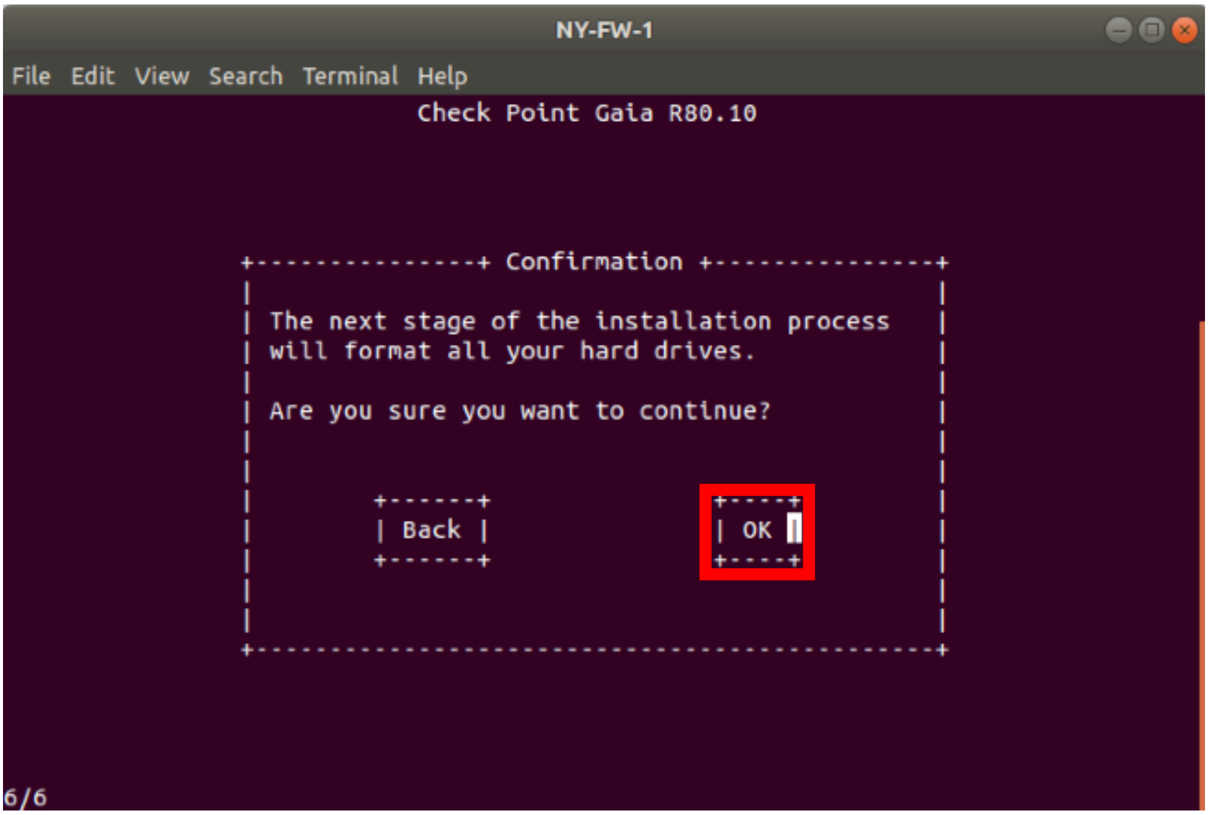
Parameter	Value
IP address	10.0.0.1
Netmask	255.255.255.0

Select **OK** and hit **Enter** to continue.



```
                         Check Point Gaia R80.10

          +---+ Management Interface (eth2) +---+
          |                                      |
          |                                      |
          | IP address:          10.0.0.1________|
          | Netmask:             255.255.255.0___|
          | Default gateway:                     |
          |                                      |
          |                                      |
          |   [ ] DHCP server on this interface  |
          |                                      |
          |                                      |
          |      +----+          +-------+       |
          |      | OK |          | Back  |       |
          |      +----+          +-------+       |
          |                                      |
          |                                      |
          +--------------------------------------+

5/6
```

8.0 Confirm the installation process start.

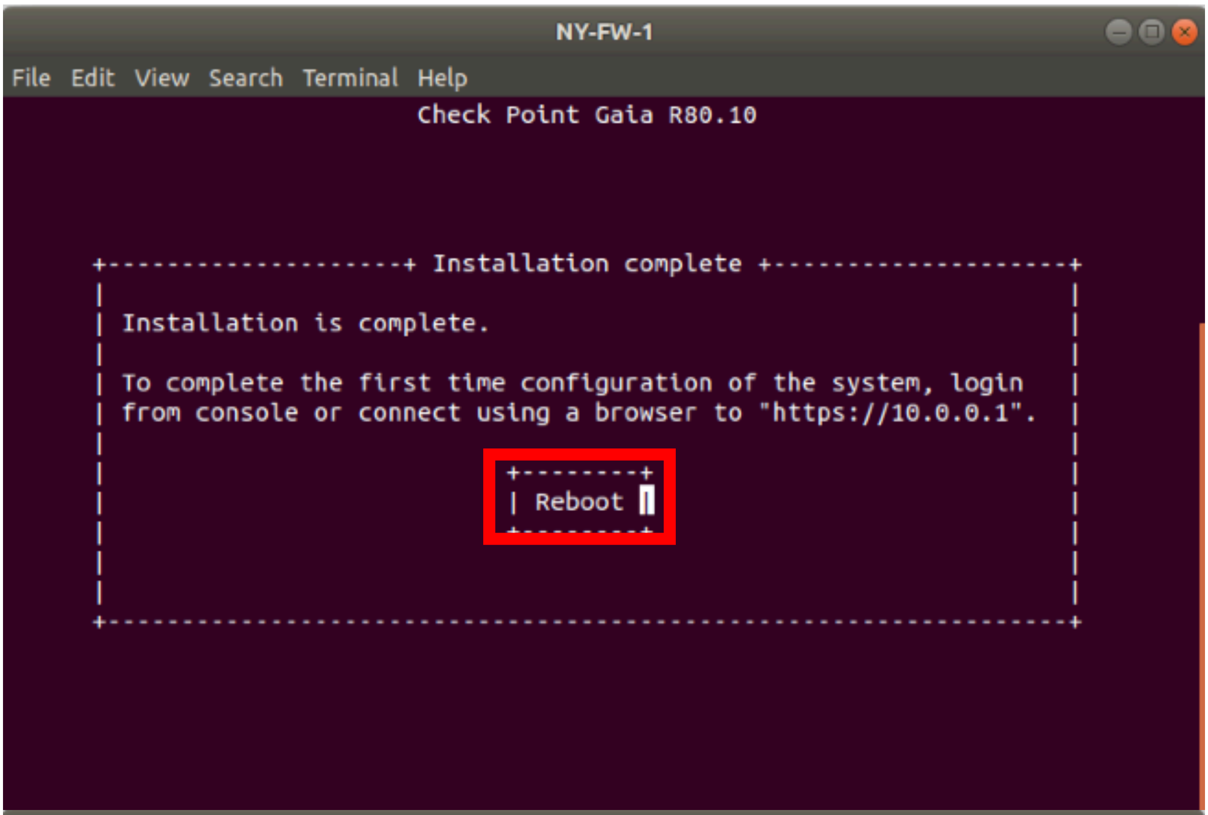


```
                         Check Point Gaia R80.10



      +---------------+ Confirmation +---------------+
      |                                               |
      | The next stage of the installation process    |
      | will format all your hard drives.             |
      |                                               |
      | Are you sure you want to continue?            |
      |                                               |
      |                                               |
      |       +-------+                +----+         |
      |       | Back  |                | OK |         |
      |       +-------+                +----+         |
      |                                               |
      |                                               |
      +-----------------------------------------------+

6/6
```

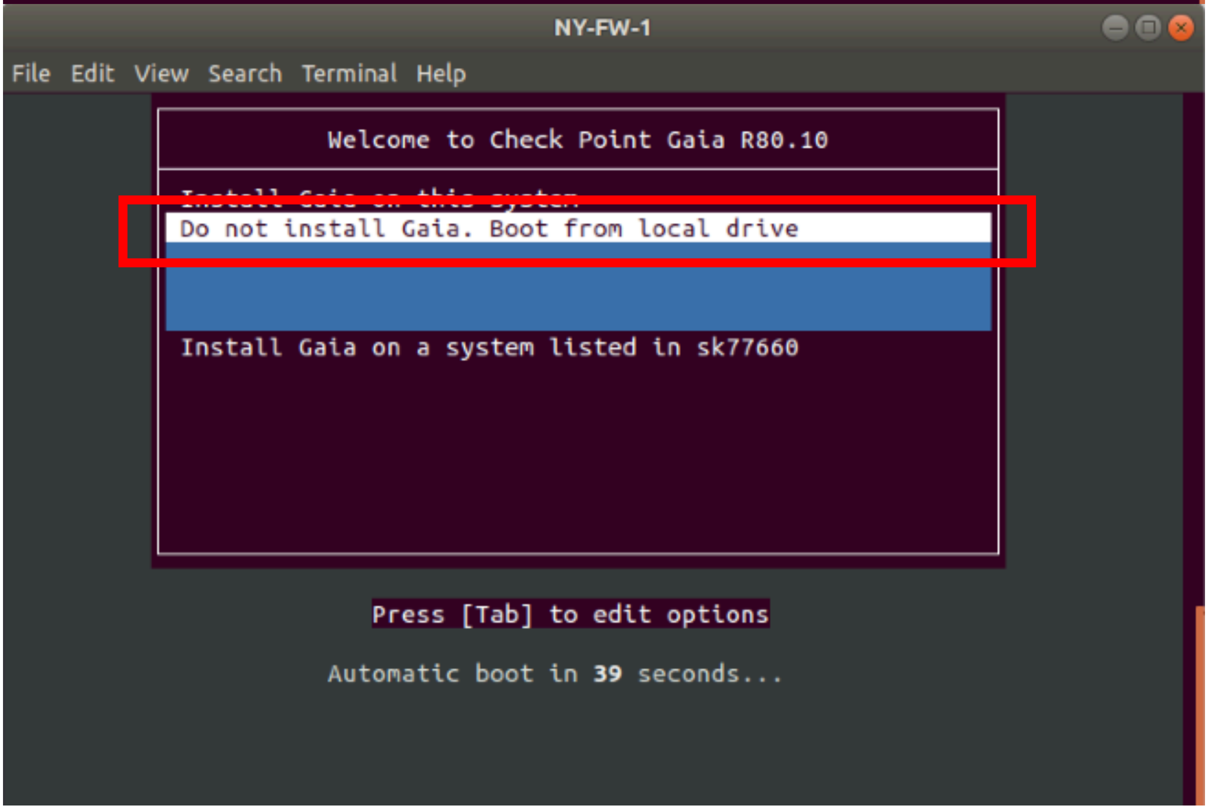
Select **OK** and hit **Enter** to start the installation process.

9.0 Installation is complete, **verify** login credentials

Hit **Enter** to **Reboot.** Select **Do not install Gaia. Boot from local drive**



```
                       Check Point Gaia R80.10


  +-------------------+ Installation complete +--------------------+
  |                                                                 |
  | Installation is complete.                                       |
  |                                                                 |
  | To complete the first time configuration of the system, login  |
  | from console or connect using a browser to "https://10.0.0.1". |
  |                                                                 |
  |                         +--------+                              |
  |                         | Reboot |                              |
  |                         +--------+                              |
  |                                                                 |
  |                                                                 |
  +-----------------------------------------------------------------+
```

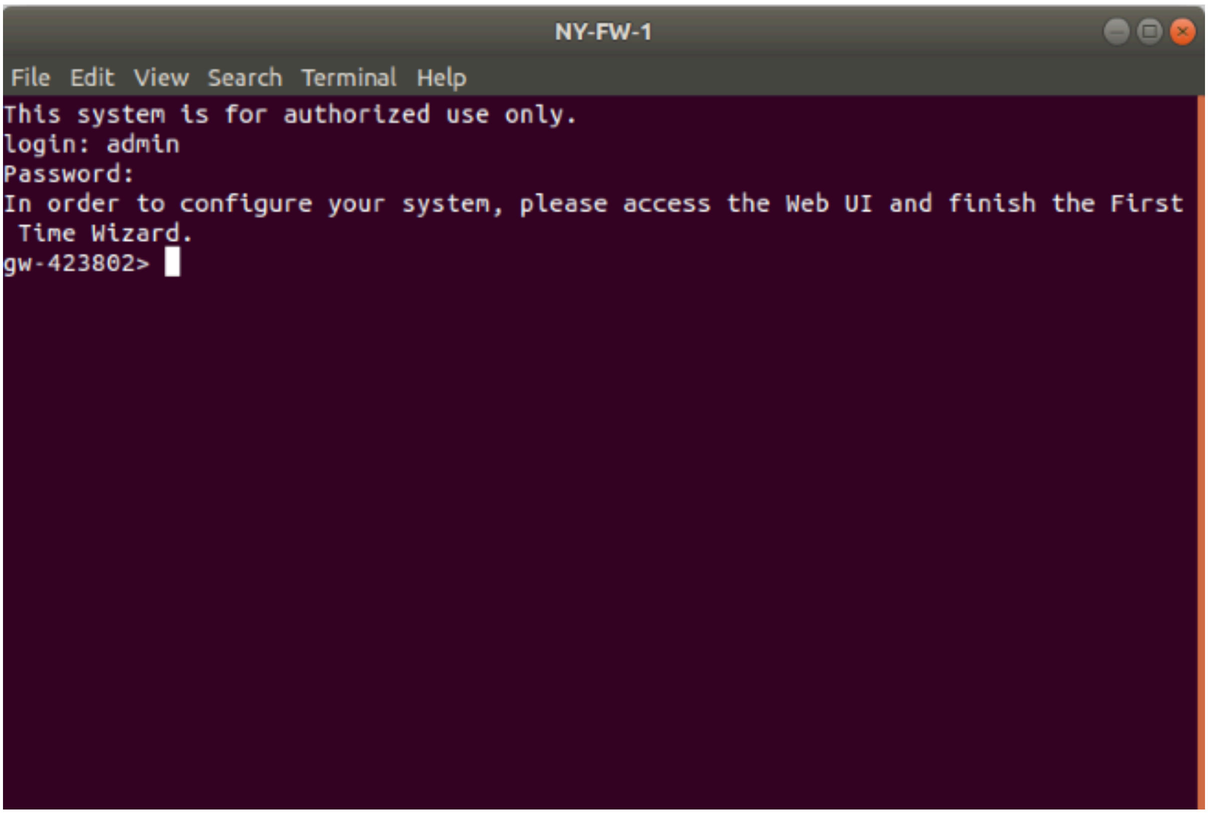


```
          Welcome to Check Point Gaia R80.10

   Install Gaia on this system
   Do not install Gaia. Boot from local drive

   Install Gaia on a system listed in sk77660


              Press [Tab] to edit options

           Automatic boot in 39 seconds...
```

Wait for 1-2 minutes, depending on hardware you are running the lab topology on and enter login credentials. Please type in the following parameters:

Parameter	Value
Login	admin
Password	admin123

Login is successful and this concludes Gaia R80.10 OS installation on NY-FW-1.



```
This system is for authorized use only.
login: admin
Password:
In order to configure your system, please access the Web UI and finish the First
 Time Wizard.
gw-423802>
```

NOTE: In this lab we have installed the Gaia OS on the HQ Firewall. Please note that installation is not finished yet, some parameters need to be configured from this point on.
Please note that when we were asked to **Reboot** the machine in order to finish installation, the following message was displayed:

To complete the first time configuration of the system, login from console or connect using a browser to "https://10.0.0.1"

In Module 4, we will connect to NY-FW-1 at https://10.0.0.1 using a browser and go through the First Time Configuration Wizard. A lab will be available on the topic and will provide you a complete walk-through.

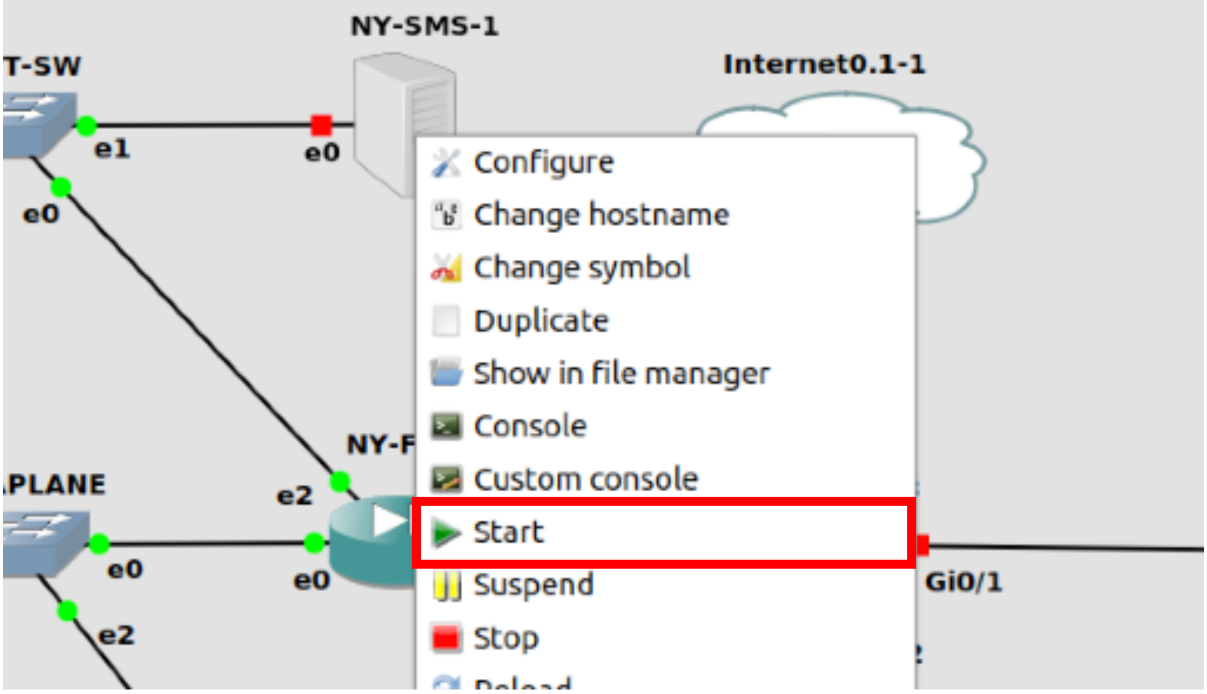
2.0 Lab: Install GAiA OS R80.10 on New York Security Management Server (SMS)

Lab Objectives

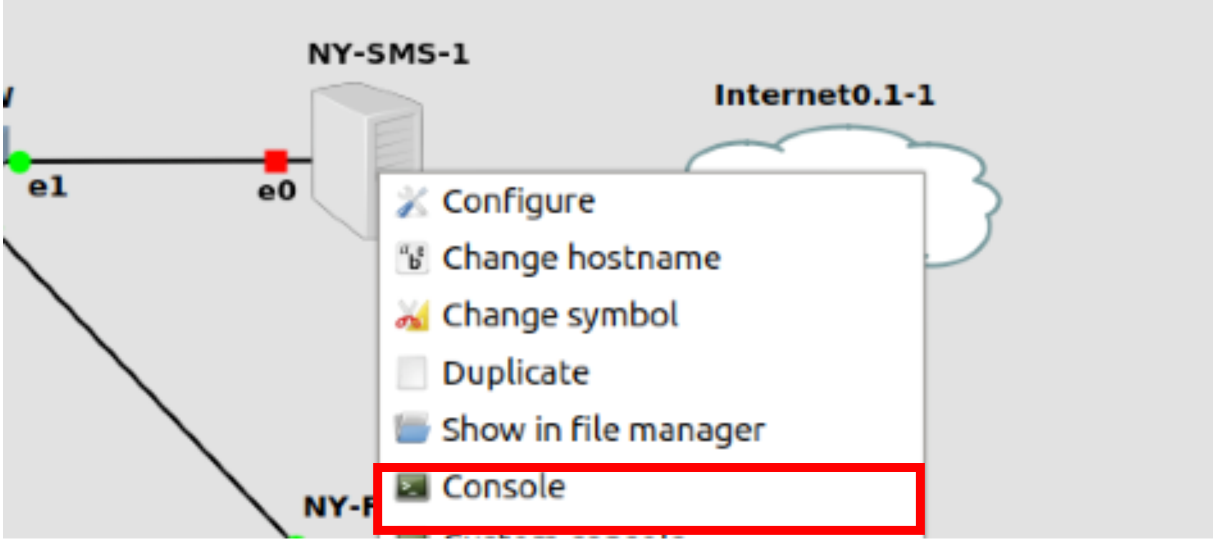
- Install GAiA OS on HQ SMS – NY-SMS-1

1.0 Start NY-FW-1 device and connect to the console

1. Right-click on NY-SMS-1 and click **Start**

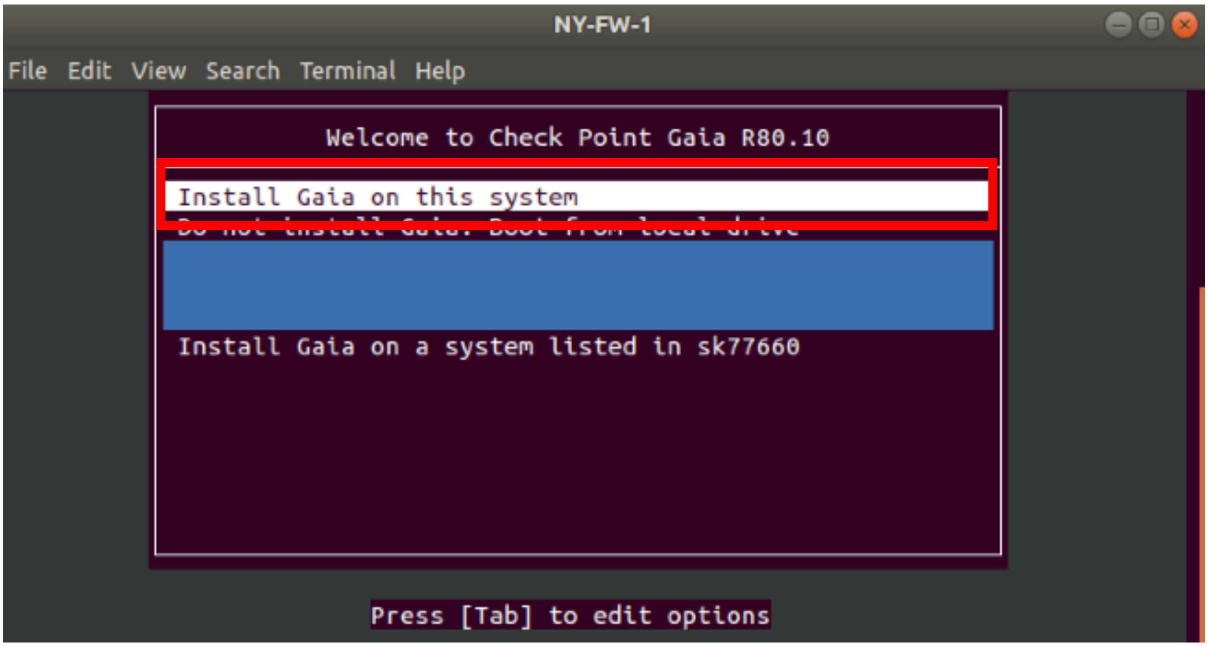


2. Right click on NY-SMS-1 and click **Console**



2.0 Start GAiA OS installation process

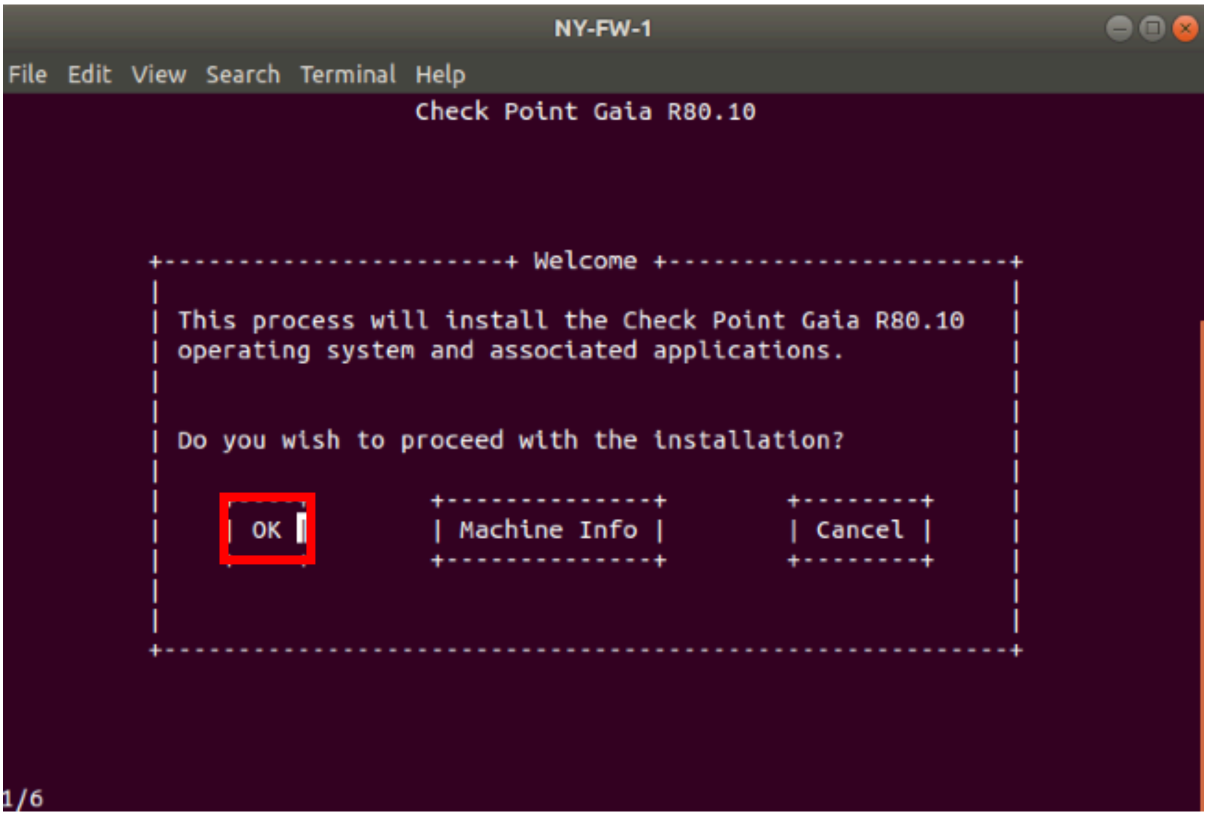
Select **Install Gaia on this system** and hit **Enter**



```
            Welcome to Check Point Gaia R80.10

 Install Gaia on this system
 Do not install Gaia. Boot from local drive


 Install Gaia on a system listed in sk77660



                  Press [Tab] to edit options
```

3.0 Confirm Check Point GAiA installation start

Select **OK** and hit **Enter.**



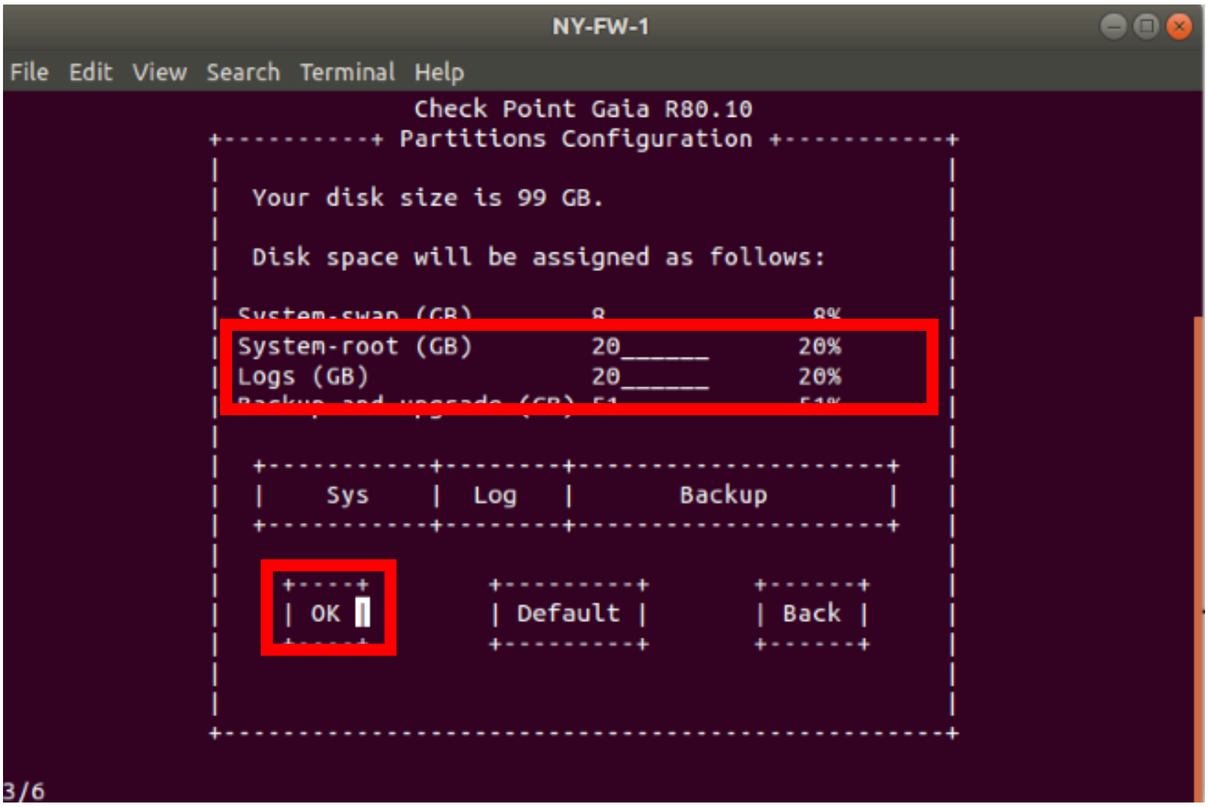
```
                          Check Point Gaia R80.10


          +-----------------------+ Welcome +-----------------------+
          |                                                         |
          | This process will install the Check Point Gaia R80.10   |
          | operating system and associated applications.           |
          |                                                         |
          |                                                         |
          | Do you wish to proceed with the installation?           |
          |                                                         |
          |   +----+         +---------------+       +--------+     |
          |   | OK |         | Machine Info  |       | Cancel |     |
          |   +----+         +---------------+       +--------+     |
          |                                                         |
          |                                                         |
          +---------------------------------------------------------+



1/6
```

4.0 Let’s increase **System-root** and **Logs** partitions’ size.

Same as we did when running the installation for NY-FW-1, change the default size values of the two partitions to the following new ones:

Parameter	Value
System-root(GB)	20
Logs(GB)	20

Again, please note that **Backup and Upgrade(GB)** size adjusts automatically and is related to total disk size value and values configured for above partitions.



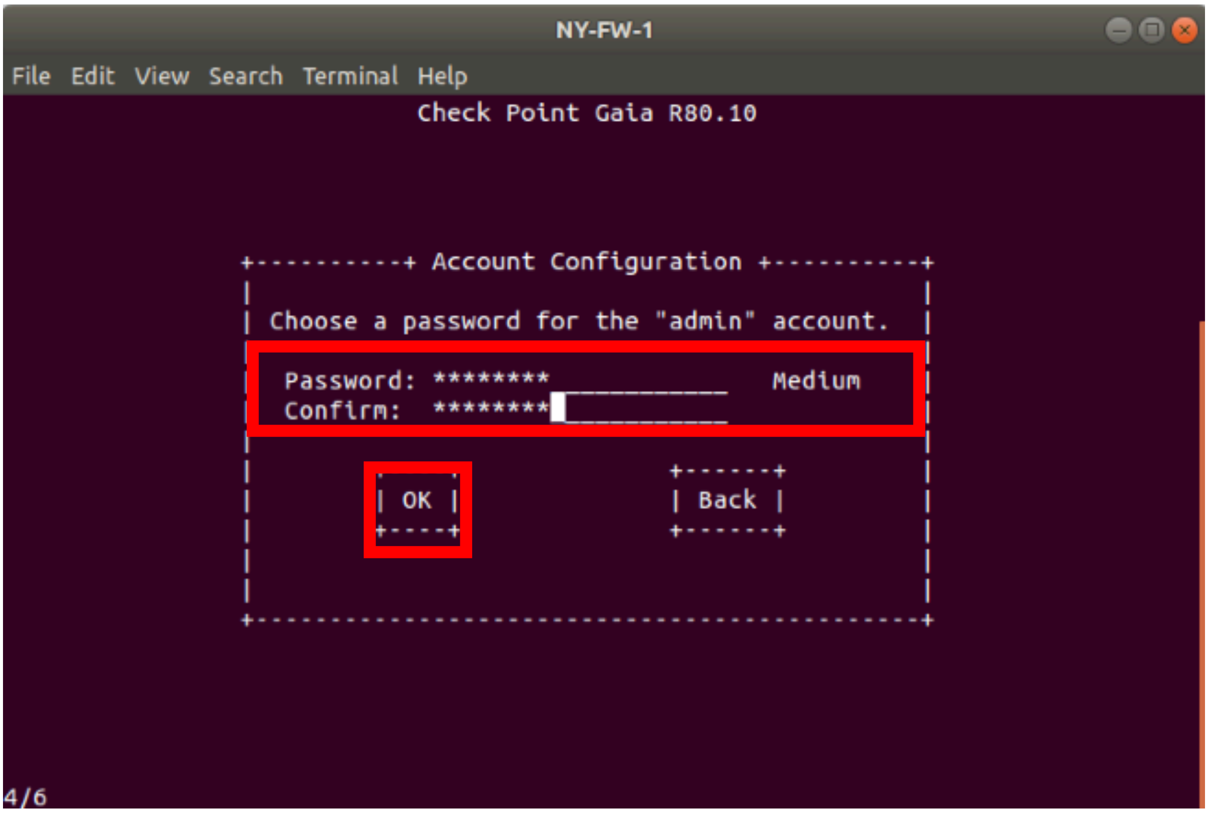
```
                  Check Point Gaia R80.10
 +----------+ Partitions Configuration +-----------+
 |                                                 |
 |  Your disk size is 99 GB.                       |
 |                                                 |
 |  Disk space will be assigned as follows:        |
 |                                                 |
 | System-swap (GB)       8             8%         |
 | System-root (GB)       20______      20%        |
 | Logs (GB)              20______      20%        |
 | Backup and upgrade (GB) 51           51%        |
 |                                                 |
 |  +-----------+--------+-------------------+     |
 |  |    Sys    |  Log   |       Backup      |     |
 |  +-----------+--------+-------------------+     |
 |                                                 |
 |  +----+        +---------+        +------+      |
 |  | OK |        | Default |        | Back |      |
 |  +----+        +---------+        +------+      |
 |                                                 |
 |                                                 |
 +-------------------------------------------------+
3/6
```

Select **OK** and hit **Enter** to continue.

5.0 Define password for the **admin** account

I will use the same username and password pair : **admin/admin123**

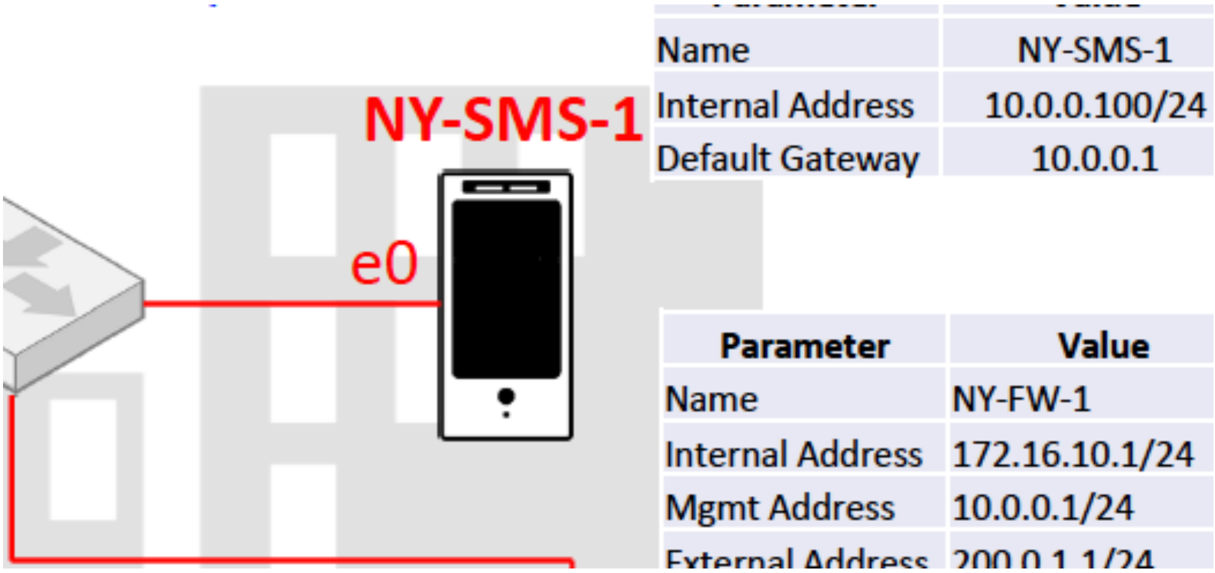
Please enter and confirm the password at your own convenience. Then select **OK** and hit **Enter** to continue.



```
                     Check Point Gaia R80.10



           +----------+ Account Configuration +----------+
           |                                             |
           | Choose a password for the "admin" account.  |
           |                                             |
           |  Password: ********__________     Medium    |
           |  Confirm:  ********__________               |
           |                                             |
           |      +----+              +------+           |
           |      | OK |              | Back |           |
           |      +----+              +------+           |
           |                                             |
           |                                             |
           +---------------------------------------------+




4/6
```

6.0 Define management port for NY-SMS-1 Gaia Firewall

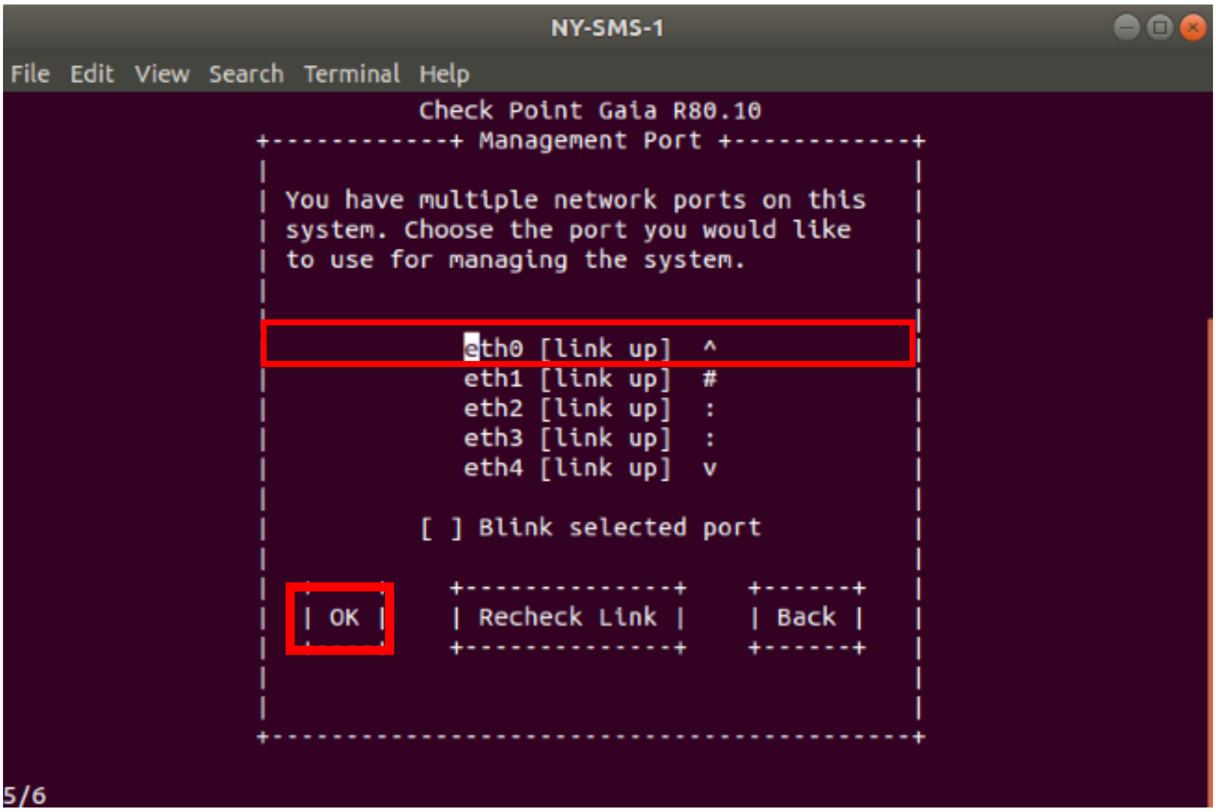
Take a look on the Lab Diagram and note what is the port that will be used for management purposes. Actually, as we can see on the Lab Diagram, this is the only port used on the SMS.



Parameter	Value
Name	NY-SMS-1
Internal Address	10.0.0.100/24
Default Gateway	10.0.0.1

Parameter	Value
Name	NY-FW-1
Internal Address	172.16.10.1/24
Mgmt Address	10.0.0.1/24
External Address	200.0.1.1/24

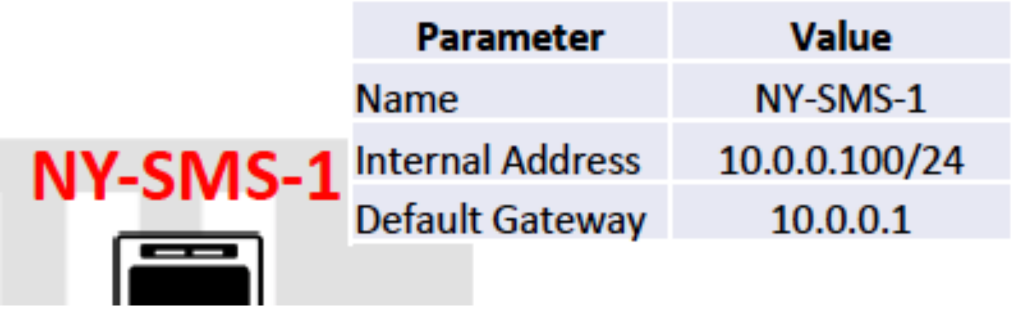
Navigate using the keyboard to **eth0** and hit **Enter** to continue.



```
                    Check Point Gaia R80.10
        +------------+ Management Port +------------+
        |                                           |
        | You have multiple network ports on this   |
        | system. Choose the port you would like    |
        | to use for managing the system.           |
        |                                           |
        |                                           |
        |             eth0 [link up]   ^            |
        |             eth1 [link up]   #            |
        |             eth2 [link up]   :            |
        |             eth3 [link up]   :            |
        |             eth4 [link up]   v            |
        |                                           |
        |          [ ] Blink selected port          |
        |                                           |
        |          +--------------+    +------+     |
        |  | OK |  | Recheck Link |    | Back |     |
        |          +--------------+    +------+     |
        |                                           |
        |                                           |
        +-------------------------------------------+
5/6
```

7.0 Define IP addressing configuration for management port.

Take a look on the Lab Diagram and note what is the port that will be used for management purposes.

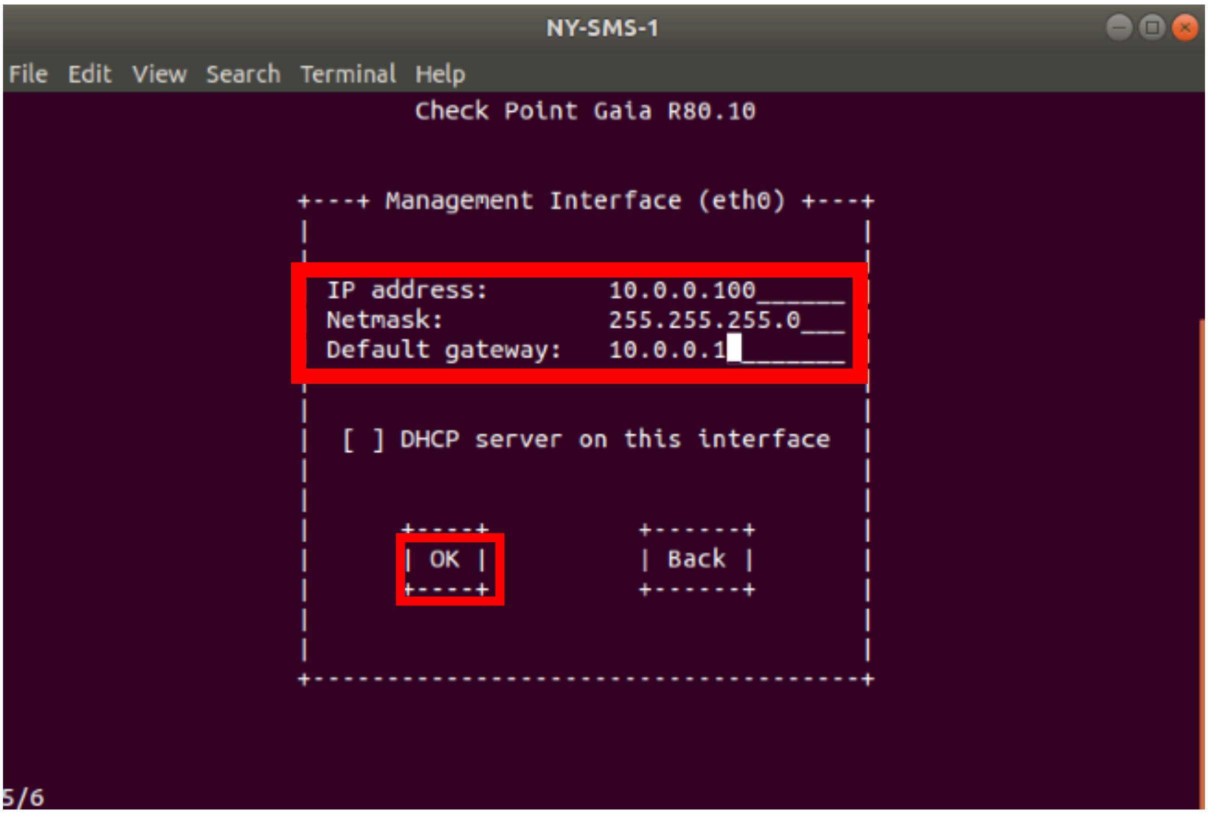


Parameter	Value
Name	NY-SMS-1
Internal Address	10.0.0.100/24
Default Gateway	10.0.0.1

Fill in the following details:

Parameter	Value
IP address	10.0.0.100
Netmask	255.255.255.0
Default gateway	10.0.0.1

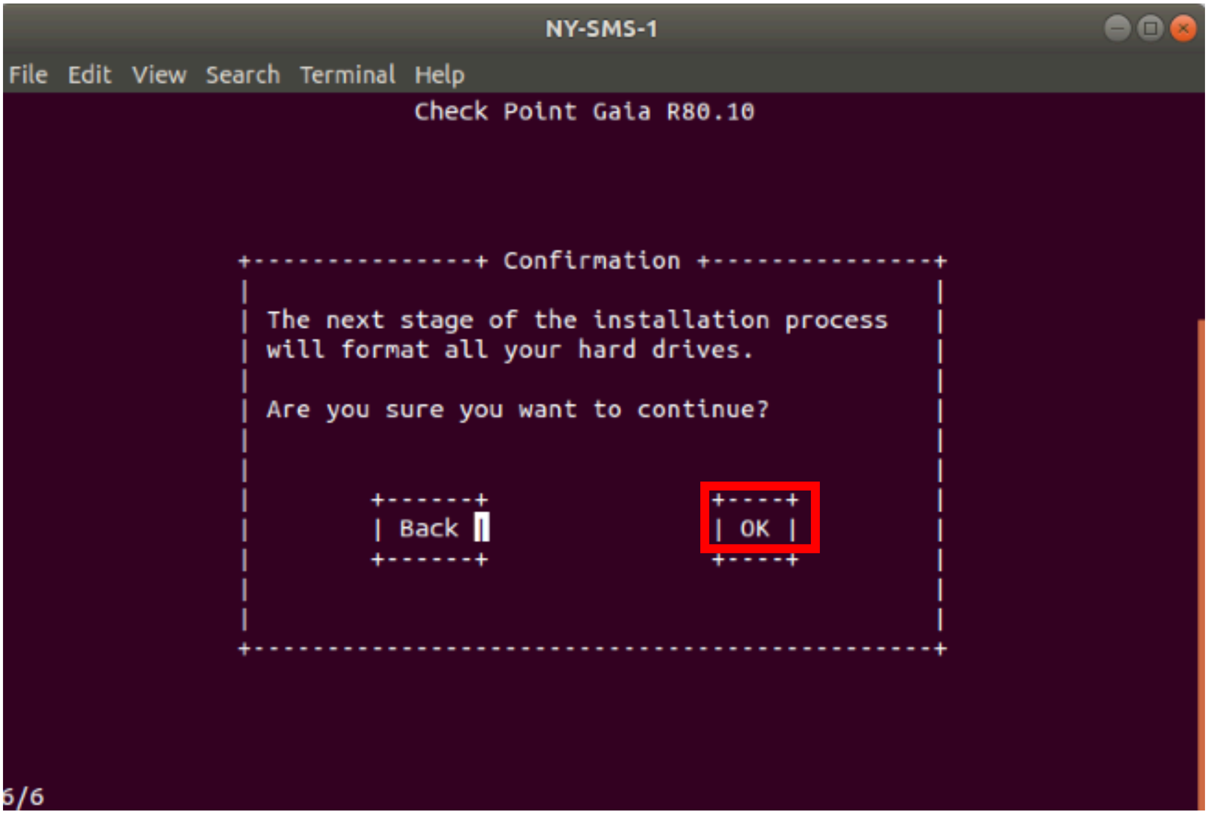
Select **OK** and hit **Enter** to continue.



```
                    Check Point Gaia R80.10


          +---+ Management Interface (eth0) +---+
          |                                      |
          |                                      |
          | IP address:         10.0.0.100______ |
          | Netmask:            255.255.255.0___ |
          | Default gateway:    10.0.0.1________ |
          |                                      |
          |  [ ] DHCP server on this interface   |
          |                                      |
          |                                      |
          |       +----+          +------+       |
          |       | OK |          | Back |       |
          |       +----+          +------+       |
          |                                      |
          |                                      |
          +--------------------------------------+


5/6
```

8.0 Confirm the installation process start.

Select **OK** and hit **Enter** to start the installation process.

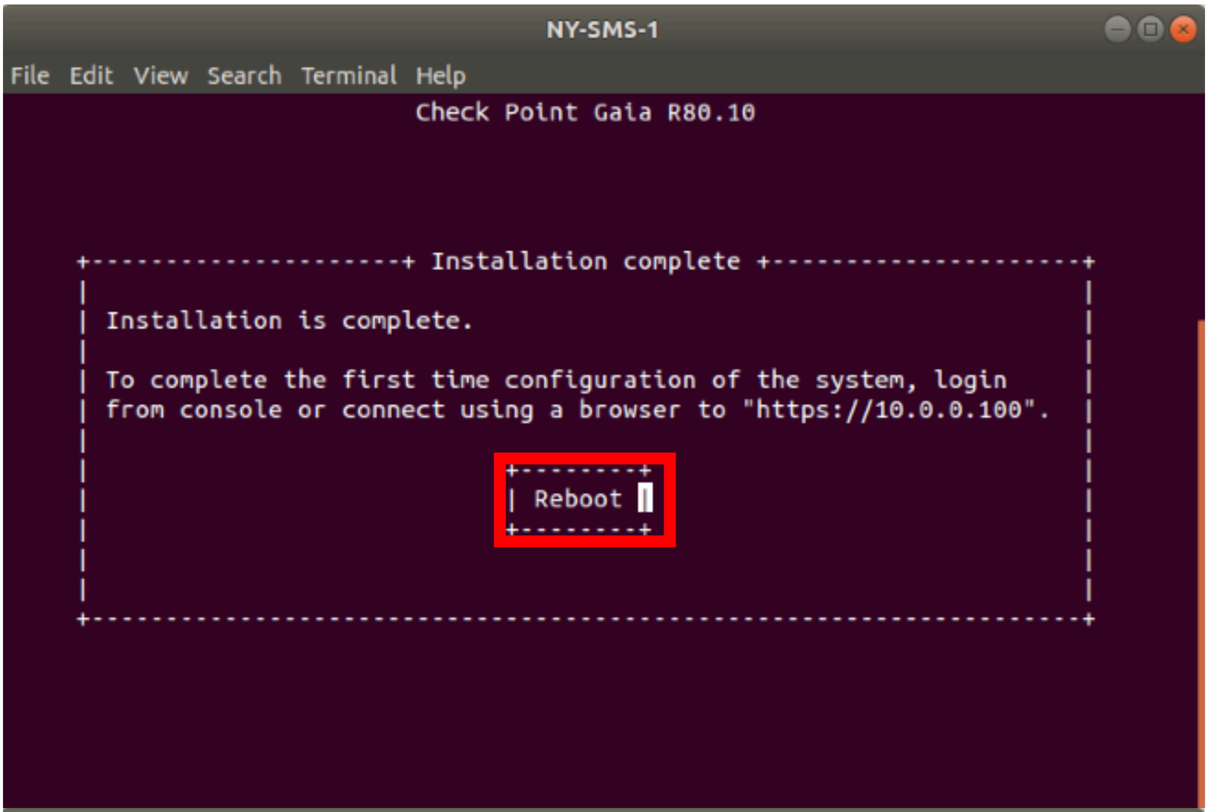


```
                    Check Point Gaia R80.10



      +---------------+ Confirmation +---------------+
      |                                              |
      | The next stage of the installation process   |
      | will format all your hard drives.            |
      |                                              |
      | Are you sure you want to continue?           |
      |                                              |
      |                                              |
      |         +------+               +----+        |
      |         | Back |               | OK |        |
      |         +------+               +----+        |
      |                                              |
      |                                              |
      +----------------------------------------------+


6/6
```

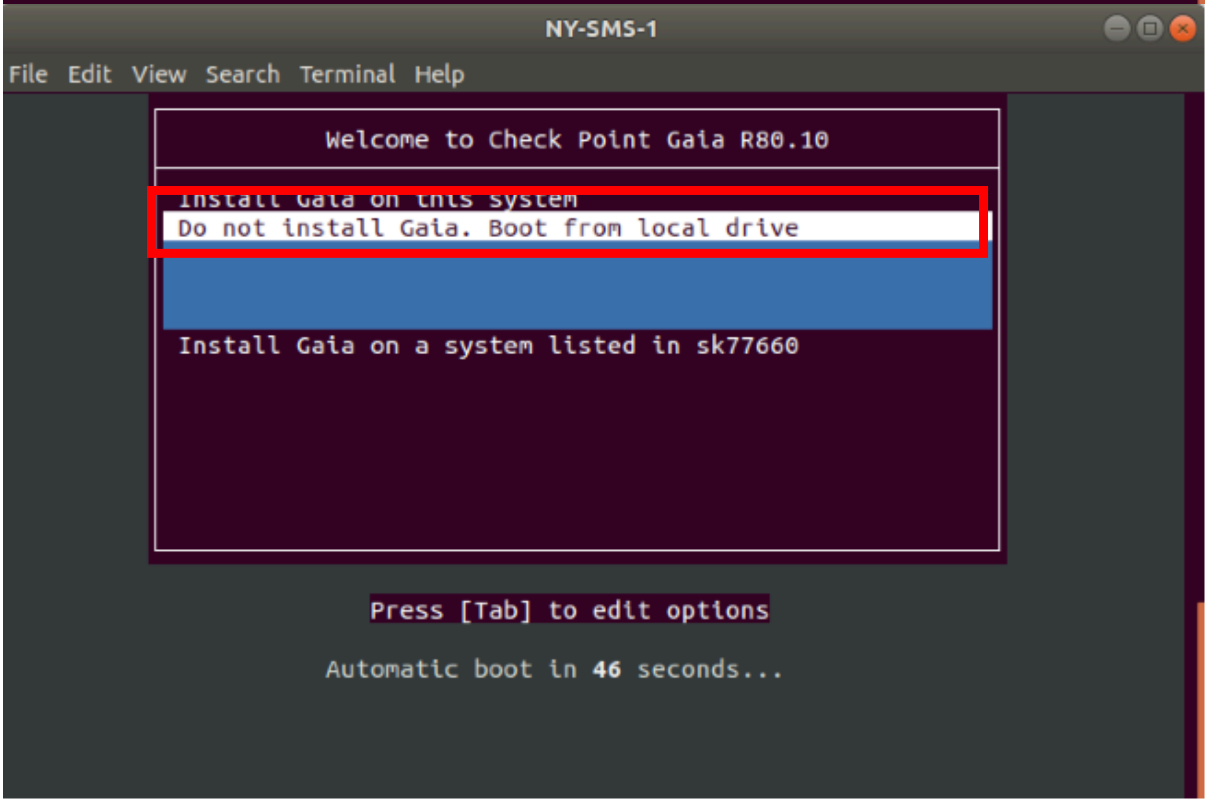
9.0 Installation is complete, **verify** login credentials

Installation is now complete, let’s verify login credentials and connectivity to NY-FW-1 through ICMP (ping).

Hit **Enter** to **Reboot.** Select **Do not install Gaia. Boot from local drive**



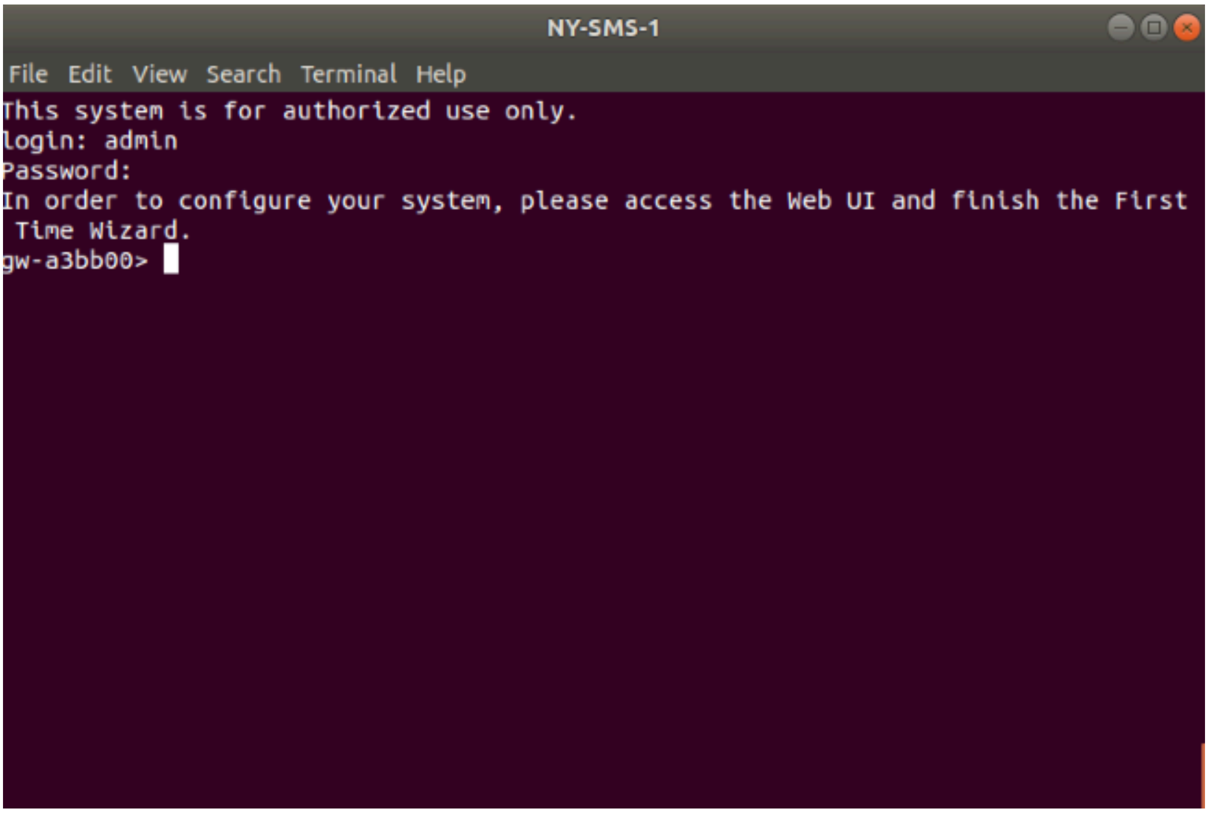
```
                        Check Point Gaia R80.10


  +--------------------+ Installation complete +--------------------+
  |                                                                  |
  | Installation is complete.                                        |
  |                                                                  |
  | To complete the first time configuration of the system, login   |
  | from console or connect using a browser to "https://10.0.0.100". |
  |                                                                  |
  |                          +--------+                              |
  |                          | Reboot |                              |
  |                          +--------+                              |
  |                                                                  |
  |                                                                  |
  +------------------------------------------------------------------+
```



```
            Welcome to Check Point Gaia R80.10

  Install Gaia on this system
  Do not install Gaia. Boot from local drive

  Install Gaia on a system listed in sk77660



                 Press [Tab] to edit options

               Automatic boot in 46 seconds...
```

Wait for 1-2 minutes, depending on hardware you are running the lab topology on and enter login credentials. Please type in the following parameters:

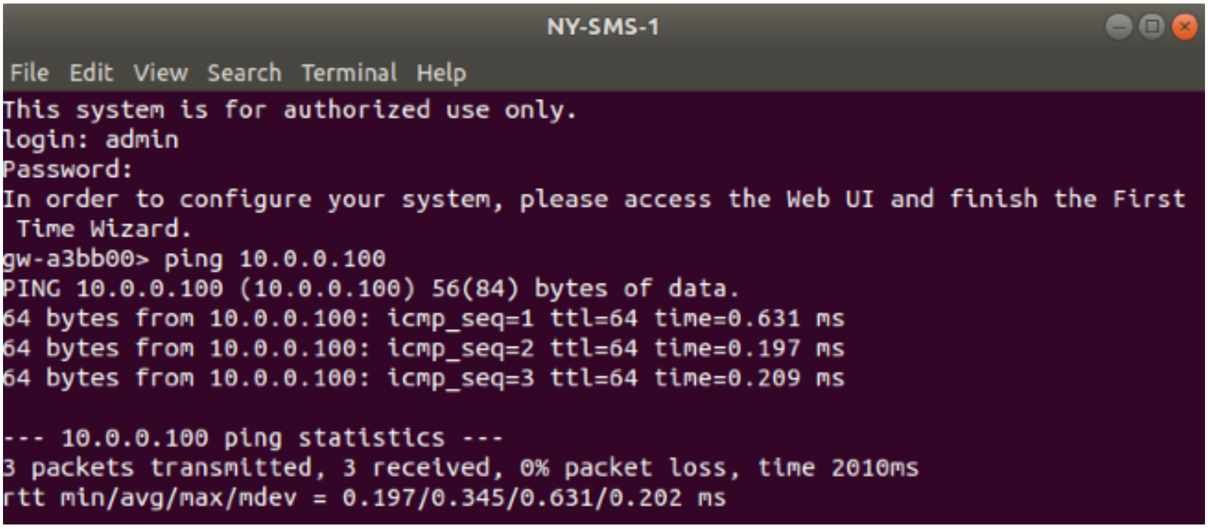
Parameter	Value
Login	admin
Password	admin123



```
This system is for authorized use only.
login: admin
Password:
In order to configure your system, please access the Web UI and finish the First
 Time Wizard.
gw-a3bb00>
```

Login is successful and this concludes Gaia R80.10 OS installation on NY-SMS-1.

Let's verify and confirm IP connectivity to NY-FW-1:



```
This system is for authorized use only.
login: admin
Password:
In order to configure your system, please access the Web UI and finish the First
 Time Wizard.
gw-a3bb00> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100) 56(84) bytes of data.
64 bytes from 10.0.0.100: icmp_seq=1 ttl=64 time=0.631 ms
64 bytes from 10.0.0.100: icmp_seq=2 ttl=64 time=0.197 ms
64 bytes from 10.0.0.100: icmp_seq=3 ttl=64 time=0.209 ms

--- 10.0.0.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.197/0.345/0.631/0.202 ms
```

Connectivity between NY-FW-1 and NY-SMS-1 is working as expected.

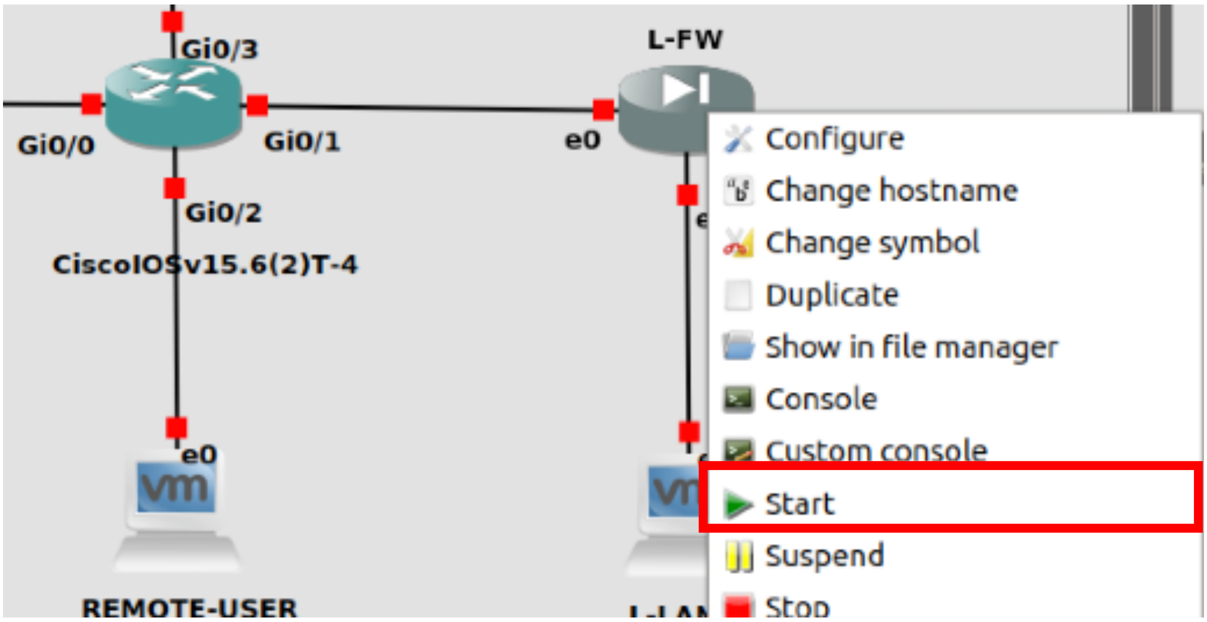
3.0 Lab: Install GAiA OS R80.10 on London Firewall

Lab Objectives

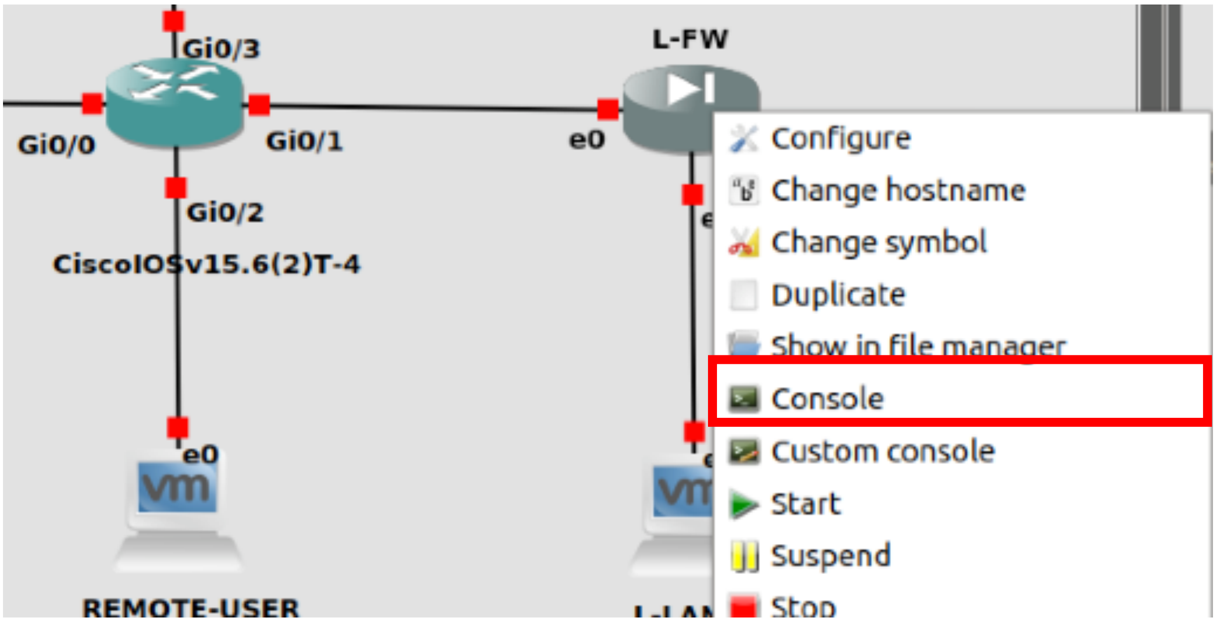
- Install GAiA OS on London FW – L-FW-1

1.0 Start NY-FW-1 device and connect to the console

1. Right-click on L-FW-1 and click **Start**

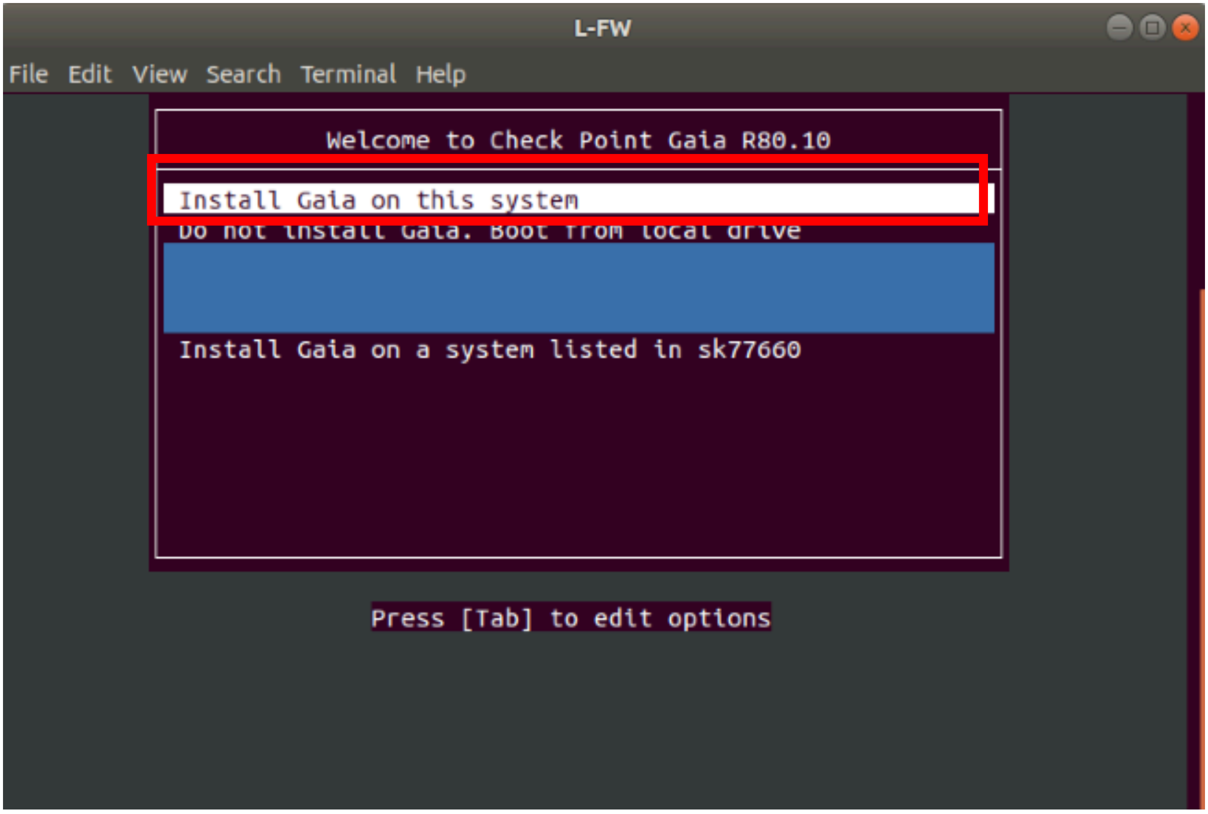


2. Right click on L-FW-1 click **Console**



2.0 Start GAiA OS installation process

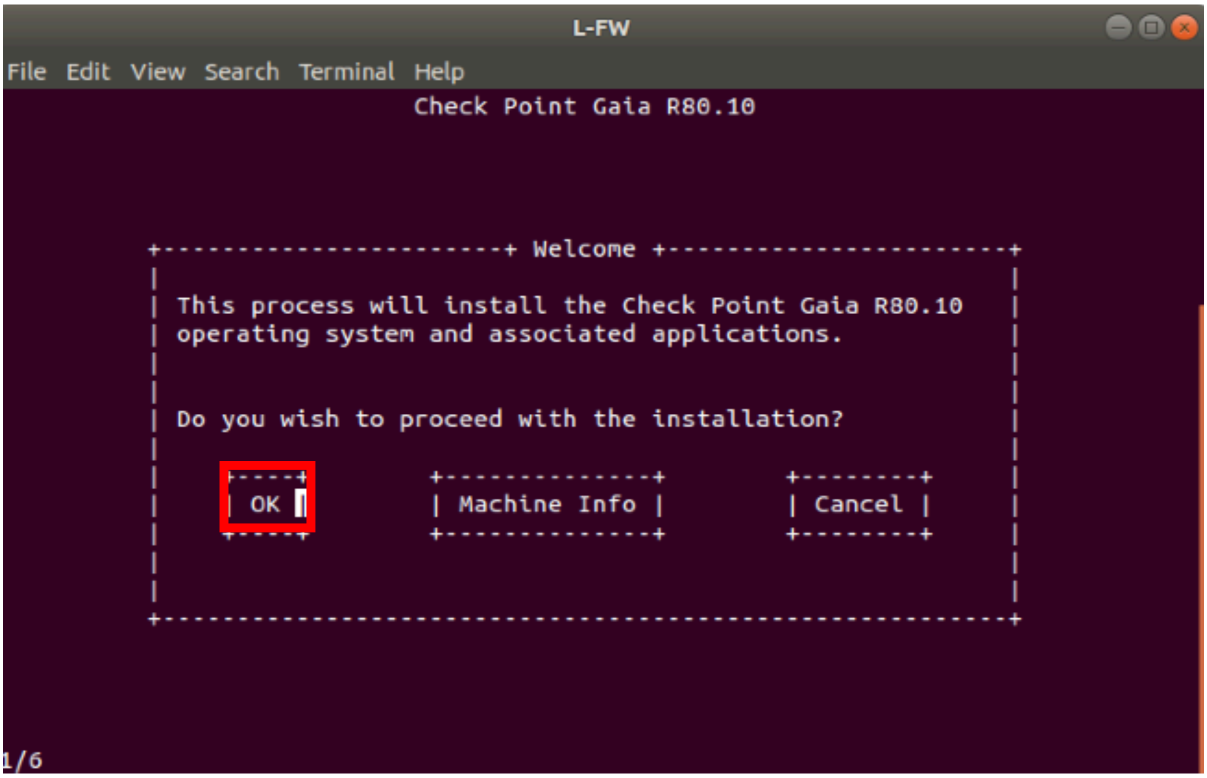
Select **Install Gaia on this system** and hit **Enter**



```
Welcome to Check Point Gaia R80.10

Install Gaia on this system
Do not install Gaia. Boot from local drive

Install Gaia on a system listed in sk77660

Press [Tab] to edit options
```

3.0 Confirm Check Point GAiA installation start

Select **OK** and hit **Enter.**

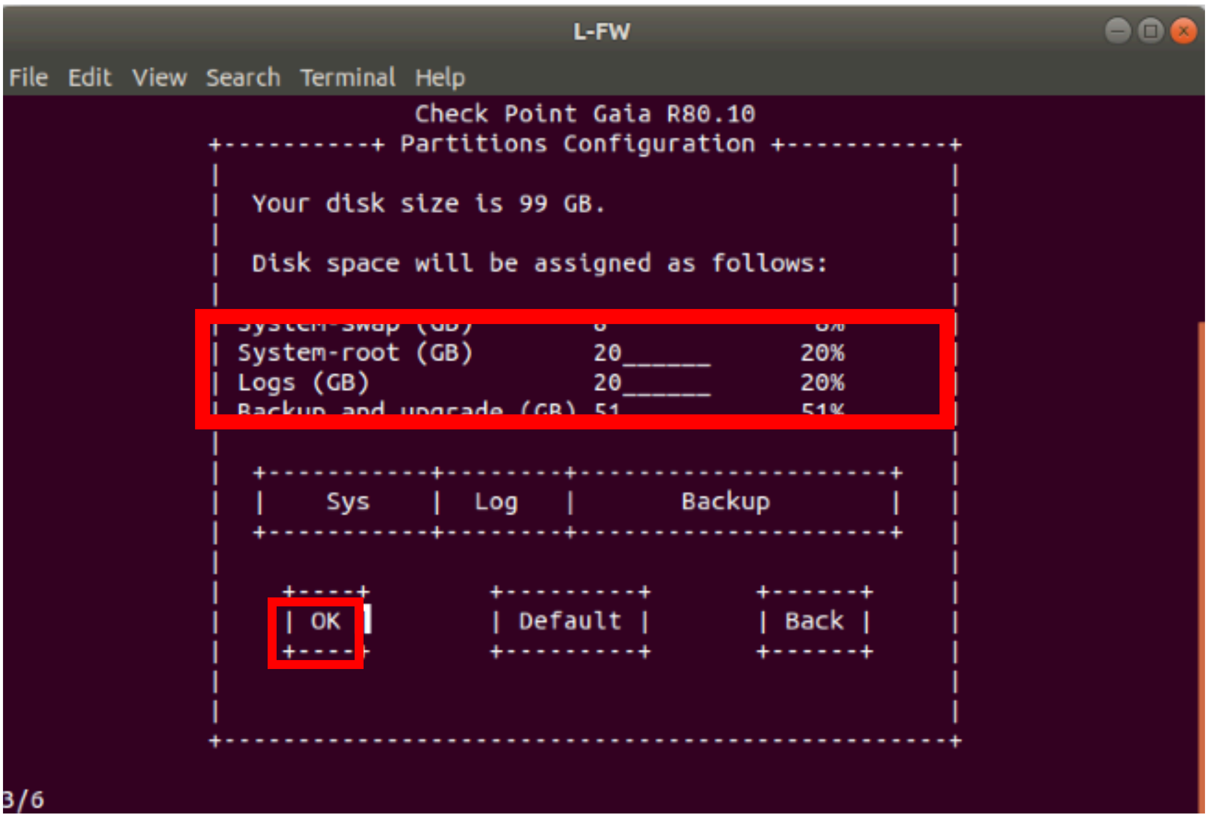


```
                     Check Point Gaia R80.10


+----------------------+ Welcome +----------------------+
|                                                       |
| This process will install the Check Point Gaia R80.10 |
| operating system and associated applications.         |
|                                                       |
|                                                       |
| Do you wish to proceed with the installation?         |
|                                                       |
|    +----+        +--------------+        +--------+   |
|    | OK |        | Machine Info |        | Cancel |   |
|    +----+        +--------------+        +--------+   |
|                                                       |
|                                                       |
+-------------------------------------------------------+

1/6
```

4.0 Let’s increase **System-root** and **Logs** partitions’ size.

Same as we did when running the installation for NY-FW-1 and NY-SMS-1, change the default size values of the two partitions to the following new ones:

Parameter	Value
System-root(GB)	20
Logs(GB)	20



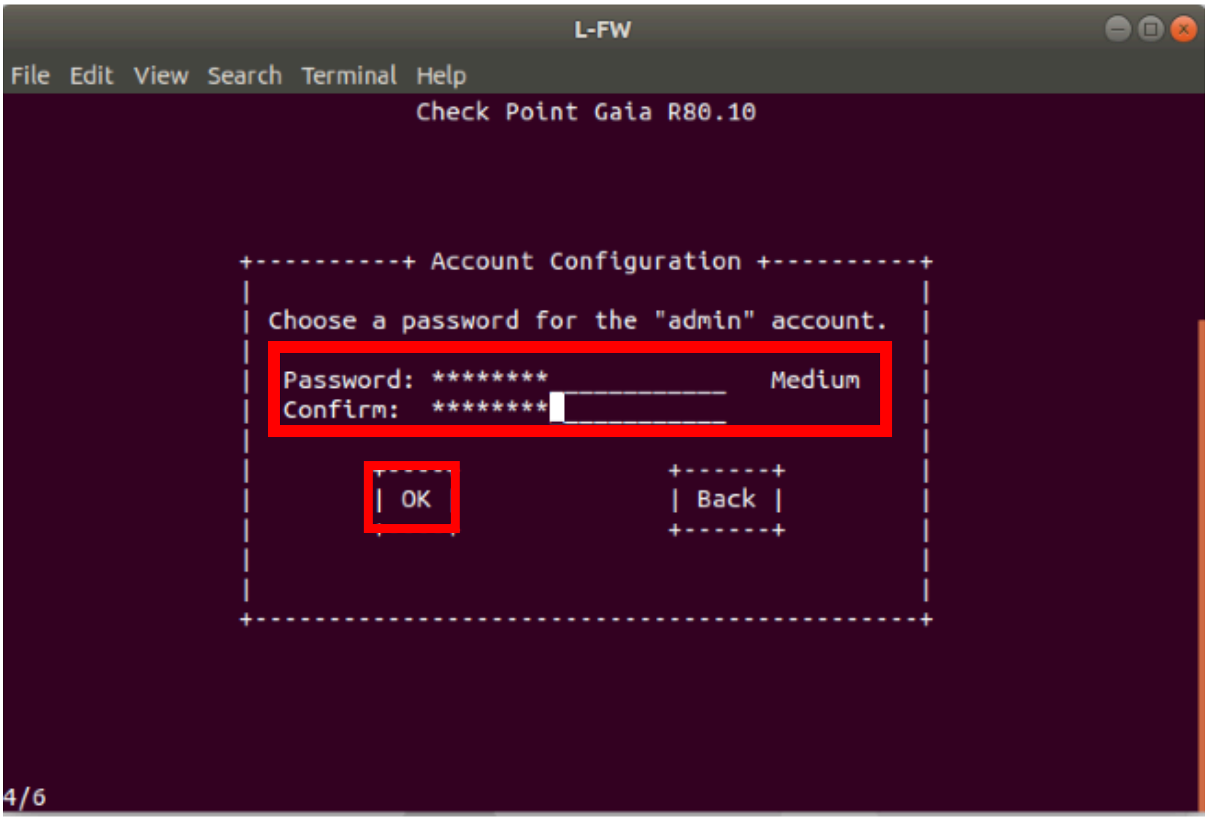
```
                    Check Point Gaia R80.10
      +----------+ Partitions Configuration +-----------+
      |                                                  |
      |  Your disk size is 99 GB.                        |
      |                                                  |
      |  Disk space will be assigned as follows:         |
      |                                                  |
      | System-swap (GB)        8              8%        |
      | System-root (GB)        20______       20%       |
      | Logs (GB)               20______       20%       |
      | Backup and upgrade (GB) 51             51%       |
      |                                                  |
      |  +-----------+--------+--------------------+    |
      |  |    Sys    |  Log   |       Backup       |    |
      |  +-----------+--------+--------------------+    |
      |                                                  |
      |   +----+        +---------+        +------+     |
      |   | OK |        | Default |        | Back |     |
      |   +----+        +---------+        +------+     |
      |                                                  |
      |                                                  |
      +--------------------------------------------------+
3/6
```

Select **OK** and hit **Enter** to continue.

5.0 Define password for the **admin** account

I will use the same username and password pair : **admin/admin123** as in the case of NY-FW-1 and NY-SMS-1 Gaia OS installation process.

Please enter and confirm the password at your own convenience. Then select **OK** and hit **Enter** to continue.

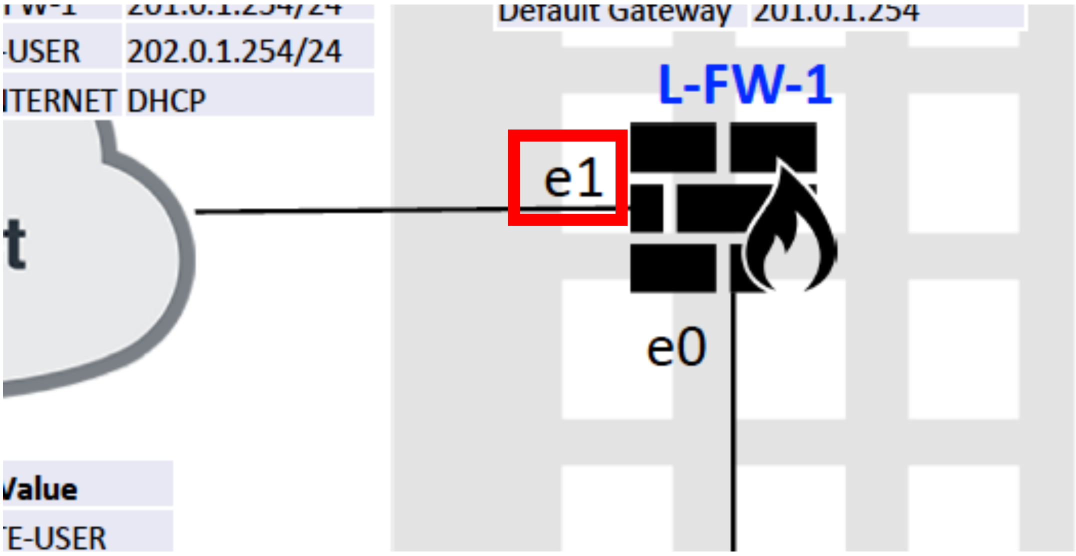


```
                    Check Point Gaia R80.10



     +----------+ Account Configuration +----------+
     |                                             |
     | Choose a password for the "admin" account.  |
     |                                             |
     | Password: ********____________    Medium    |
     | Confirm:  ********____________              |
     |                                             |
     |      +----+                +-------+        |
     |      | OK |                | Back  |        |
     |      +----+                +-------+        |
     |                                             |
     |                                             |
     +---------------------------------------------+



4/6
```

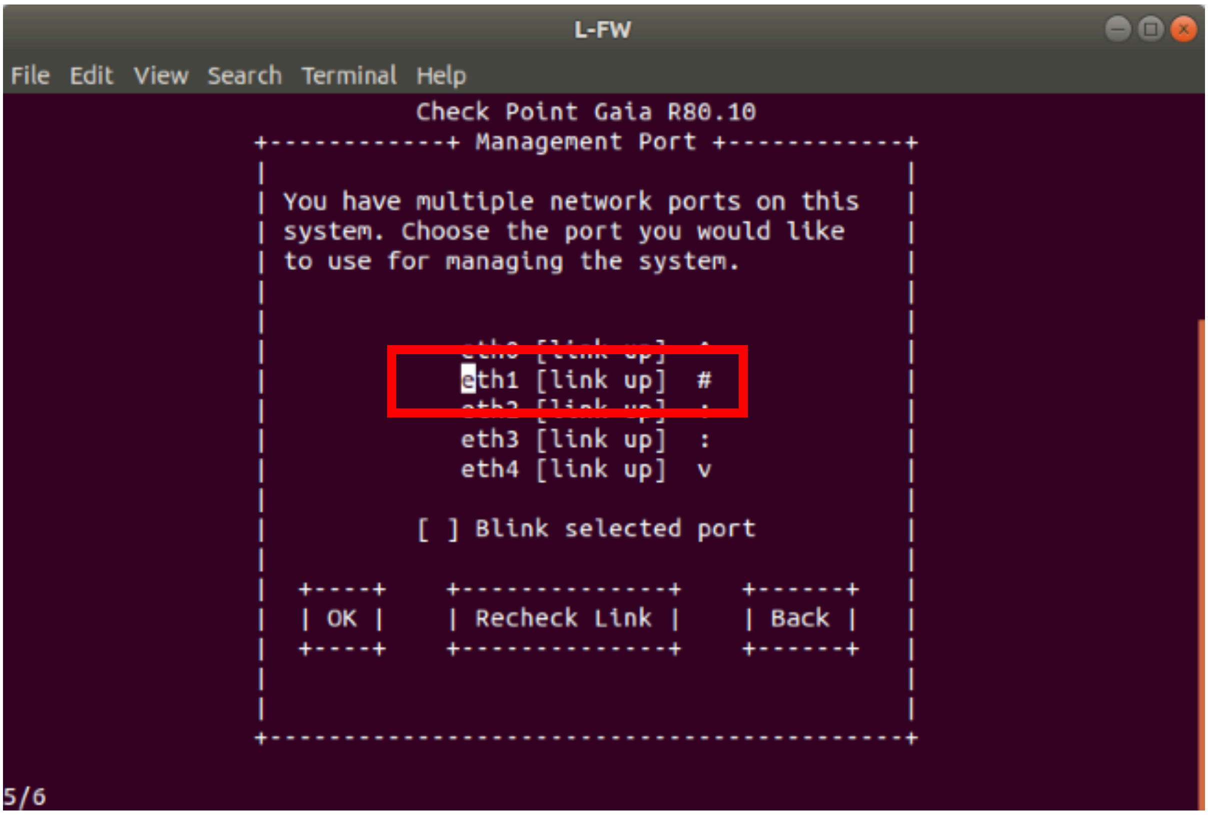
6.0 Define management port for L-FW-1 Gaia Firewall

The Remote Firewall in London Branch, L-FW-1, will be managed remotely by New York SMS. This means that the management interface must be the outside interface, connecting to internet cloud.

Take a look on the Lab Diagram and note what is the port that will be used for outside connectivity.



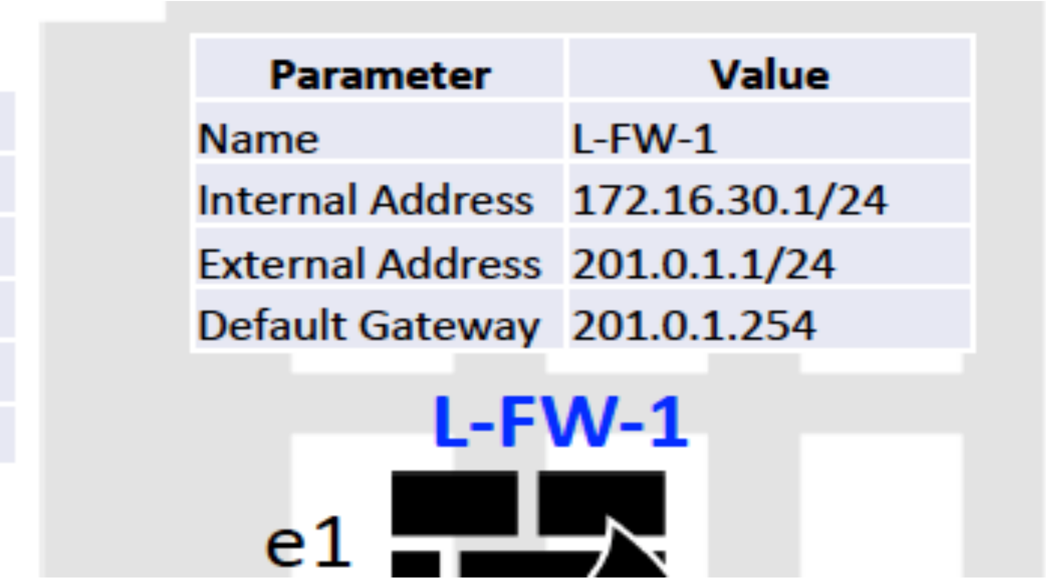
Navigate using the keyboard to **eth1** and hit **Enter** to continue.



```
                   Check Point Gaia R80.10
            +------------+ Management Port +------------+
            |                                           |
            | You have multiple network ports on this   |
            | system. Choose the port you would like    |
            | to use for managing the system.           |
            |                                           |
            |                                           |
            |               eth0 [link up]  ^           |
            |               eth1 [link up]  #           |
            |               eth2 [link up]  :           |
            |               eth3 [link up]  :           |
            |               eth4 [link up]  v           |
            |                                           |
            |          [ ] Blink selected port          |
            |                                           |
            |  +----+    +--------------+    +------+   |
            |  | OK |    | Recheck Link |    | Back |   |
            |  +----+    +--------------+    +------+   |
            |                                           |
            |                                           |
            +-------------------------------------------+
5/6
```

7.0 Define IP addressing configuration for management port.

Take a look on the Lab Diagram and note what is the IP addressing scheme that will be used for **eth1**.

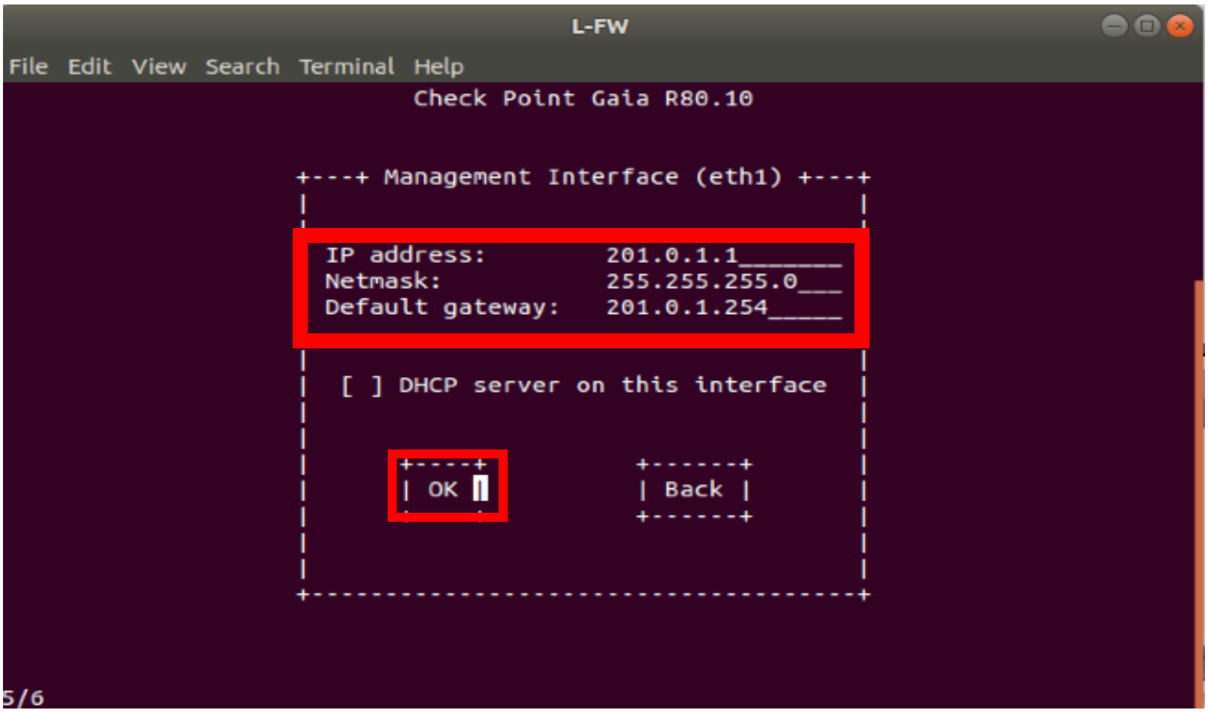


Parameter	Value
Name	L-FW-1
Internal Address	172.16.30.1/24
External Address	201.0.1.1/24
Default Gateway	201.0.1.254

Fill in the following details:

Parameter	Value
IP address	201.0.1.1
Netmask	255.255.255.0
Default gateway	201.0.1.254

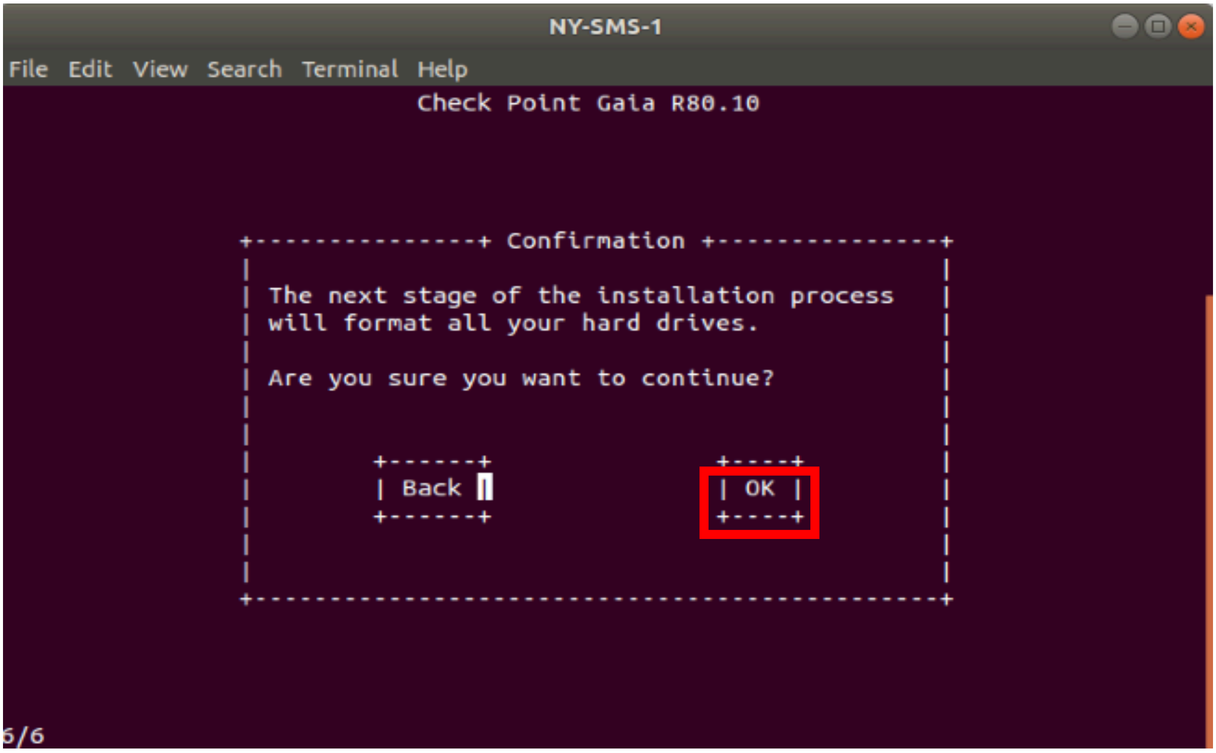
Select **OK** and hit **Enter** to continue.



```
                         Check Point Gaia R80.10

                +---+ Management Interface (eth1) +---+
                |                                     |
                |  IP address:         201.0.1.1________
                |  Netmask:            255.255.255.0___
                |  Default gateway:    201.0.1.254_____
                |                                     |
                |   [ ] DHCP server on this interface |
                |                                     |
                |      +----+          +-------+      |
                |      | OK |          | Back  |      |
                |      +----+          +-------+      |
                |                                     |
                +-------------------------------------+

5/6
```

8.0 Confirm the installation process start.

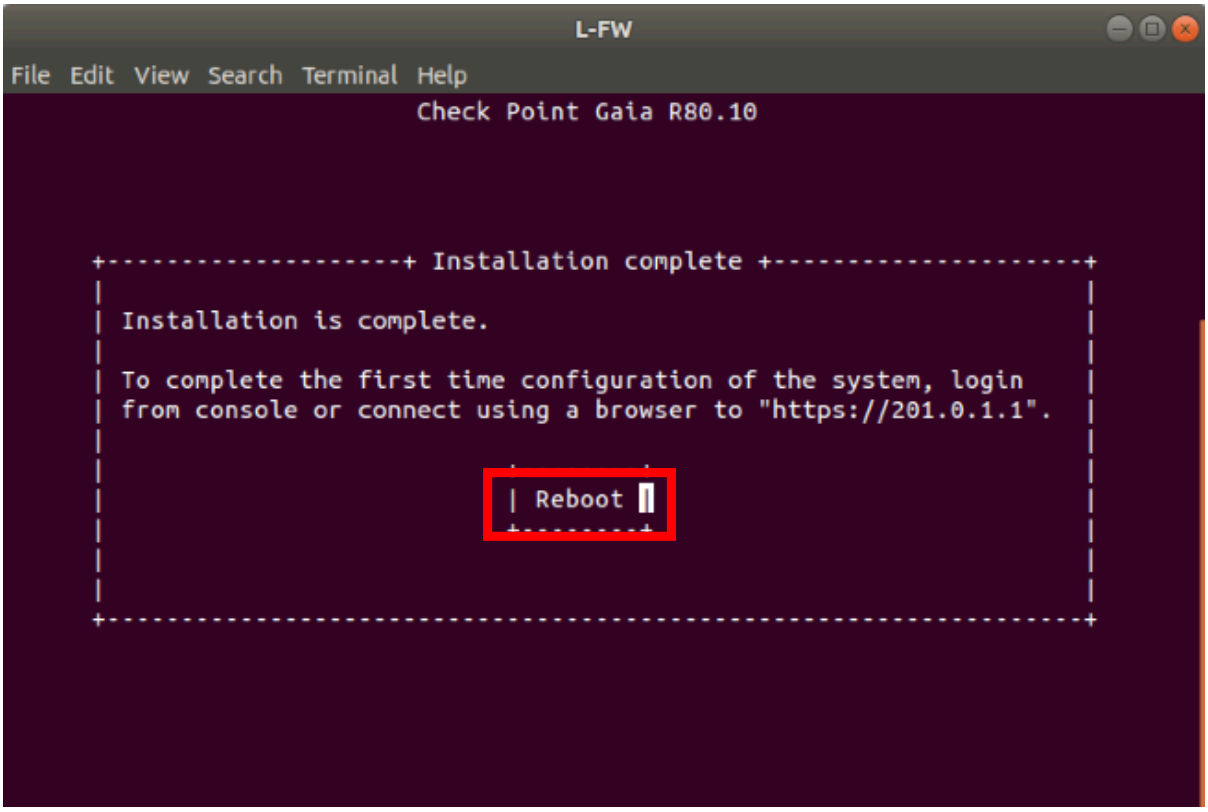
Select **OK** and hit **Enter** to start the installation process.



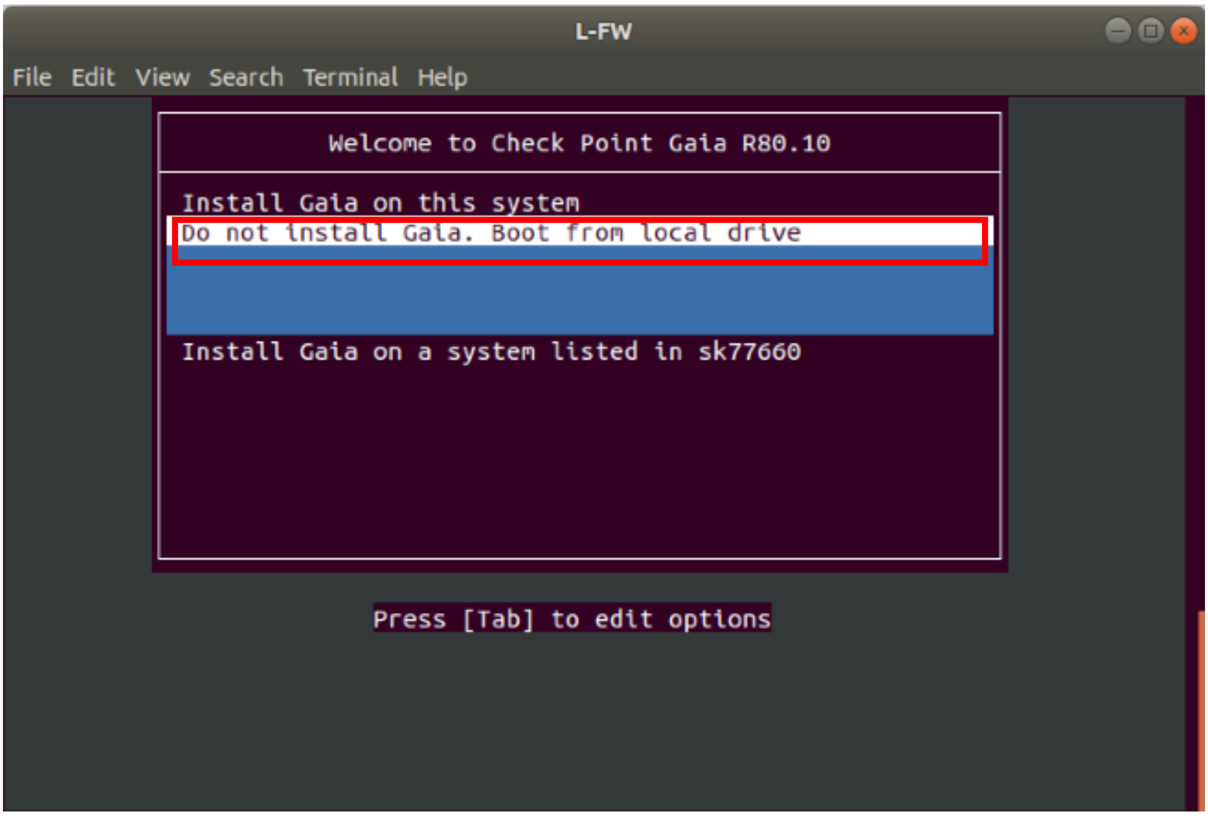
```
                         Check Point Gaia R80.10


            +---------------+ Confirmation +---------------+
            |                                              |
            | The next stage of the installation process   |
            | will format all your hard drives.            |
            |                                              |
            | Are you sure you want to continue?           |
            |                                              |
            |                                              |
            |       +-------+                 +----+       |
            |       | Back  |                 | OK |       |
            |       +-------+                 +----+       |
            |                                              |
            |                                              |
            +----------------------------------------------+

6/6
```

9.0 Installation is complete, **verify** login credentials

Hit **Enter** to **Reboot.** Select **Do not install Gaia. Boot from local drive**



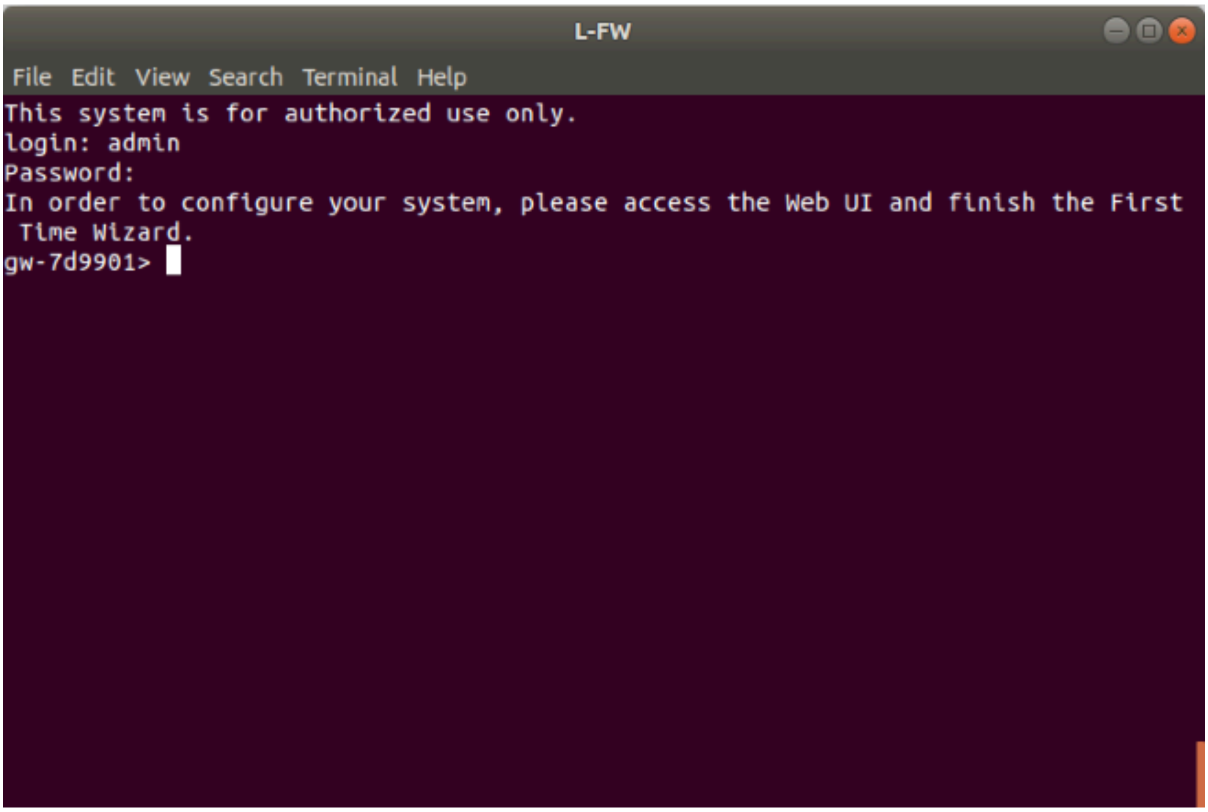
```
                     Check Point Gaia R80.10

+--------------------+ Installation complete +---------------------+
|                                                                  |
| Installation is complete.                                        |
|                                                                  |
| To complete the first time configuration of the system, login    |
| from console or connect using a browser to "https://201.0.1.1".  |
|                                                                  |
|                         +---------+                              |
|                         | Reboot  |                              |
|                         +---------+                              |
|                                                                  |
|                                                                  |
+------------------------------------------------------------------+
```



```
        Welcome to Check Point Gaia R80.10

 Install Gaia on this system
 Do not install Gaia. Boot from local drive

 Install Gaia on a system listed in sk77660



           Press [Tab] to edit options
```

Wait for 1-2 minutes, depending on hardware you are running the lab topology on and enter login credentials. Please type in the following parameters:

Parameter	Value
Login	admin
Password	admin123



```
This system is for authorized use only.
login: admin
Password:
In order to configure your system, please access the Web UI and finish the First
 Time Wizard.
gw-7d9901>
```

Login is successful and this concludes Gaia R80.10 OS installation on L-FW-1.

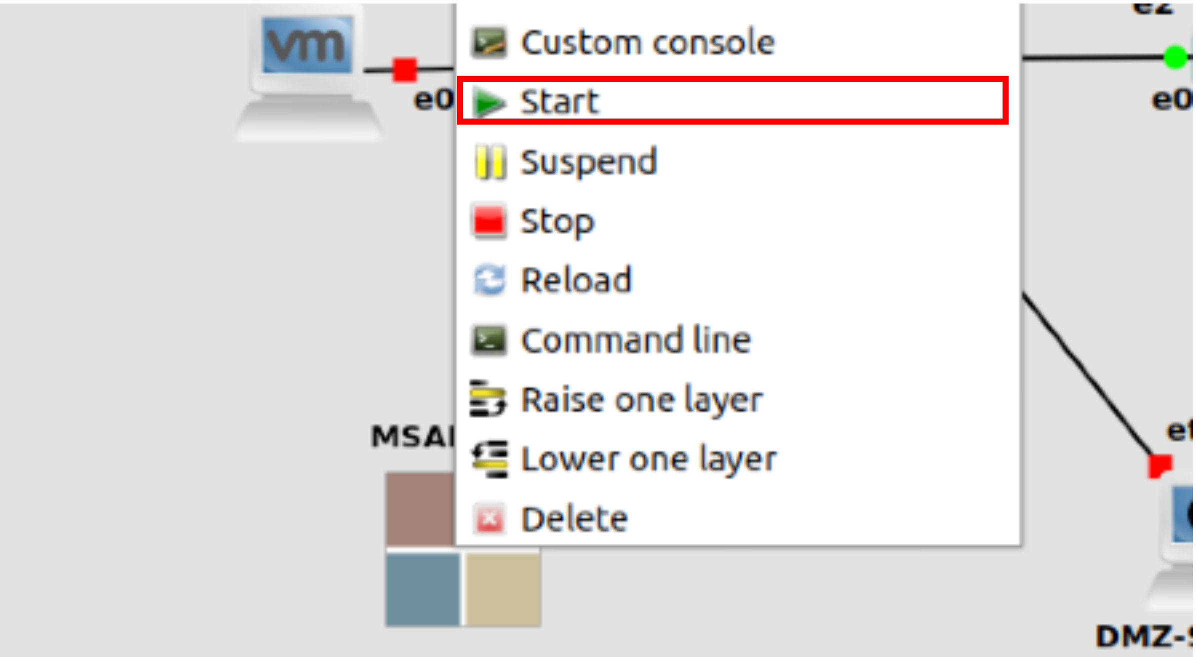
4.0 Lab: Install Microsoft Windows Server 2012 in NY HQ

Lab Objectives

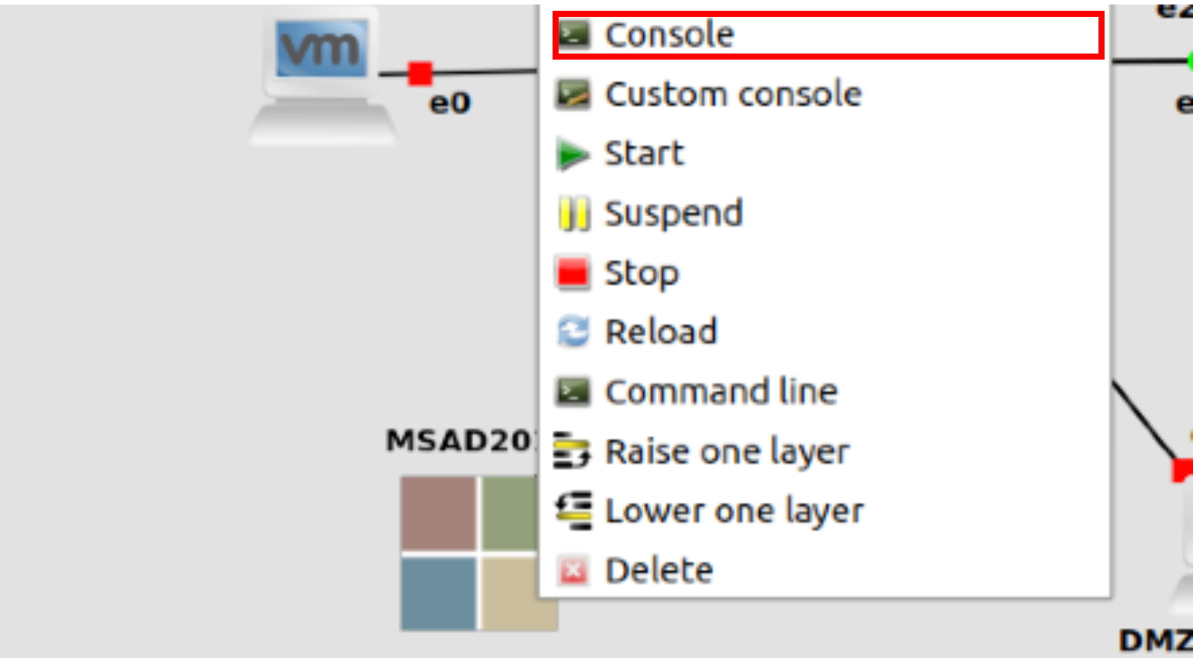
- Install Microsoft Windows Server 2012 located in New York HQ

1.0 Start NY-AD device and connect to the console

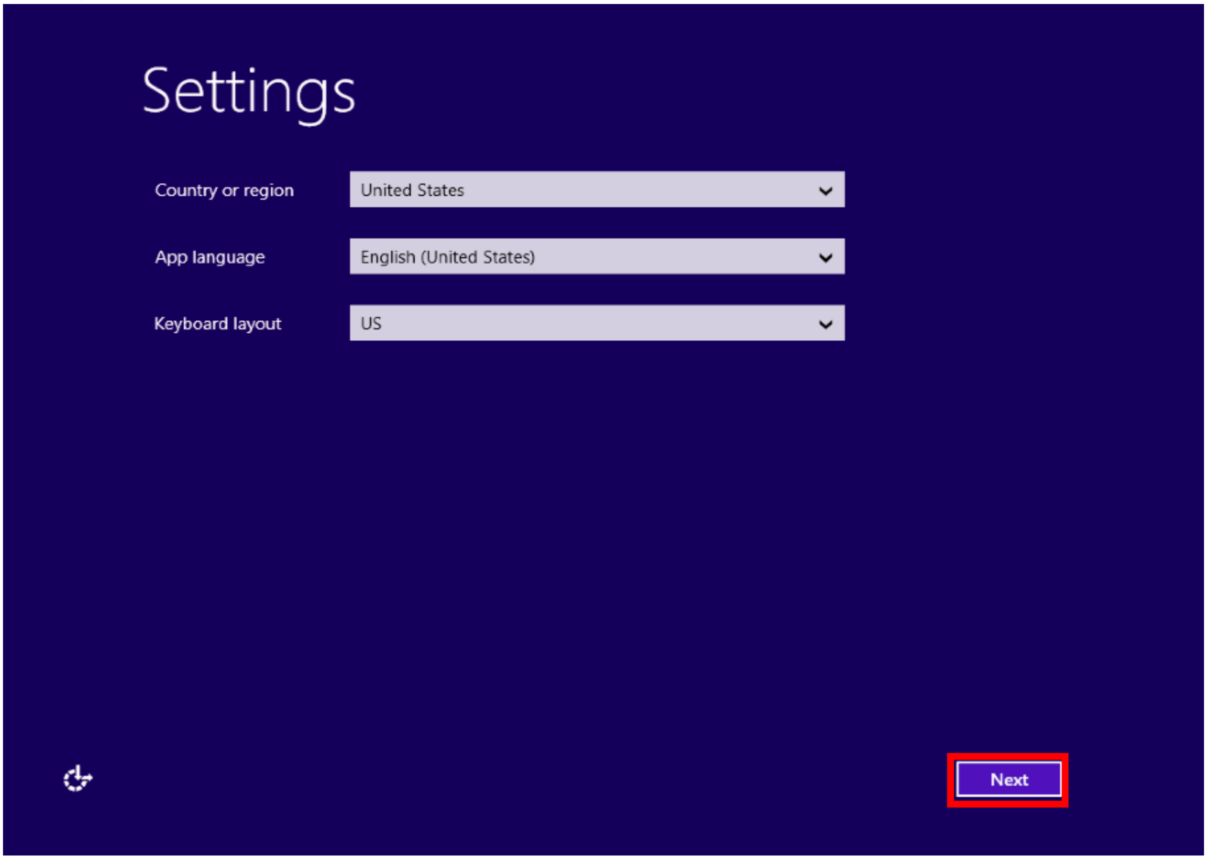
1. Right-click on NY-AD and click **Start**



2. Right click on NY-AD click **Console**



2.0 Choose Country or Region, Language and Keyboard layout that best suits you. Click **Next** to continue.



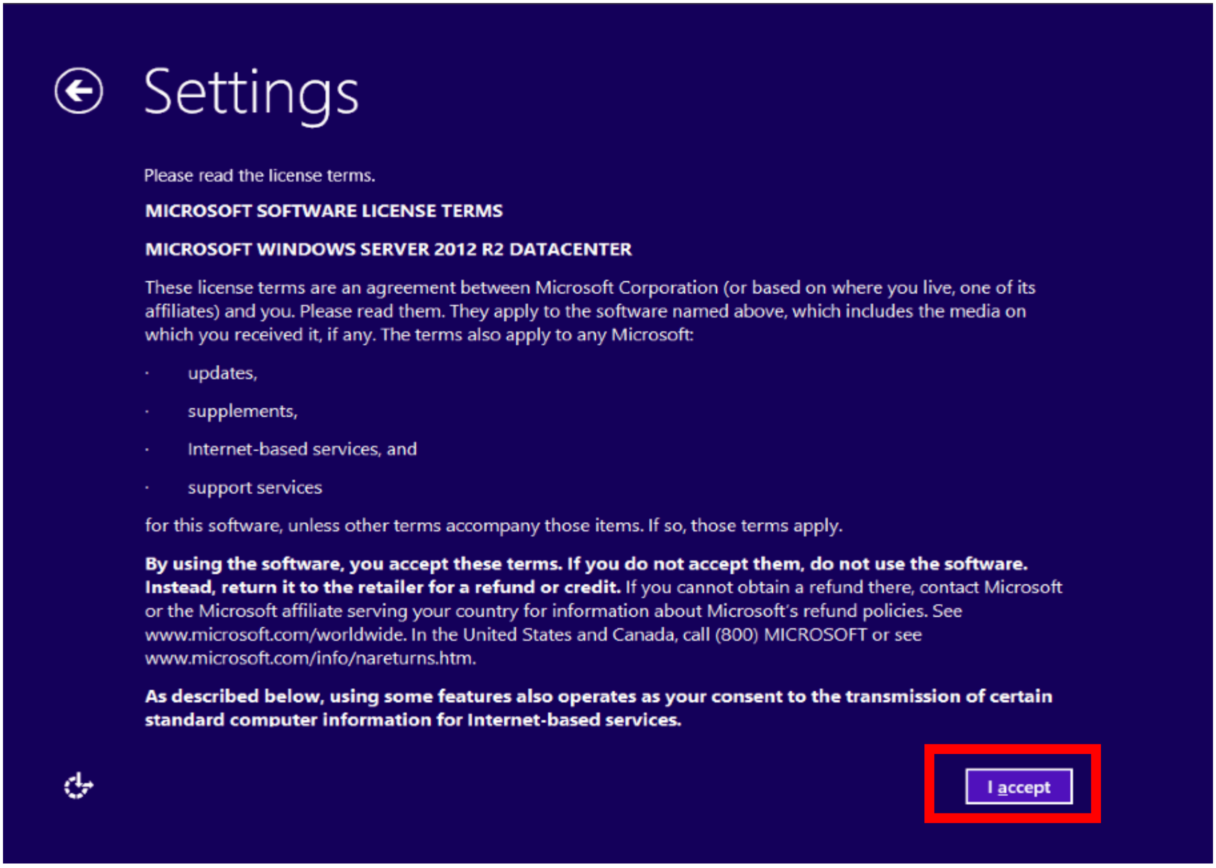
Settings

Country or region: United States

App language: English (United States)

Keyboard layout: US

3.0 Accept Microsoft Software License Terms. Click **I accept** to continue.



Settings

Please read the license terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT WINDOWS SERVER 2012 R2 DATACENTER

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

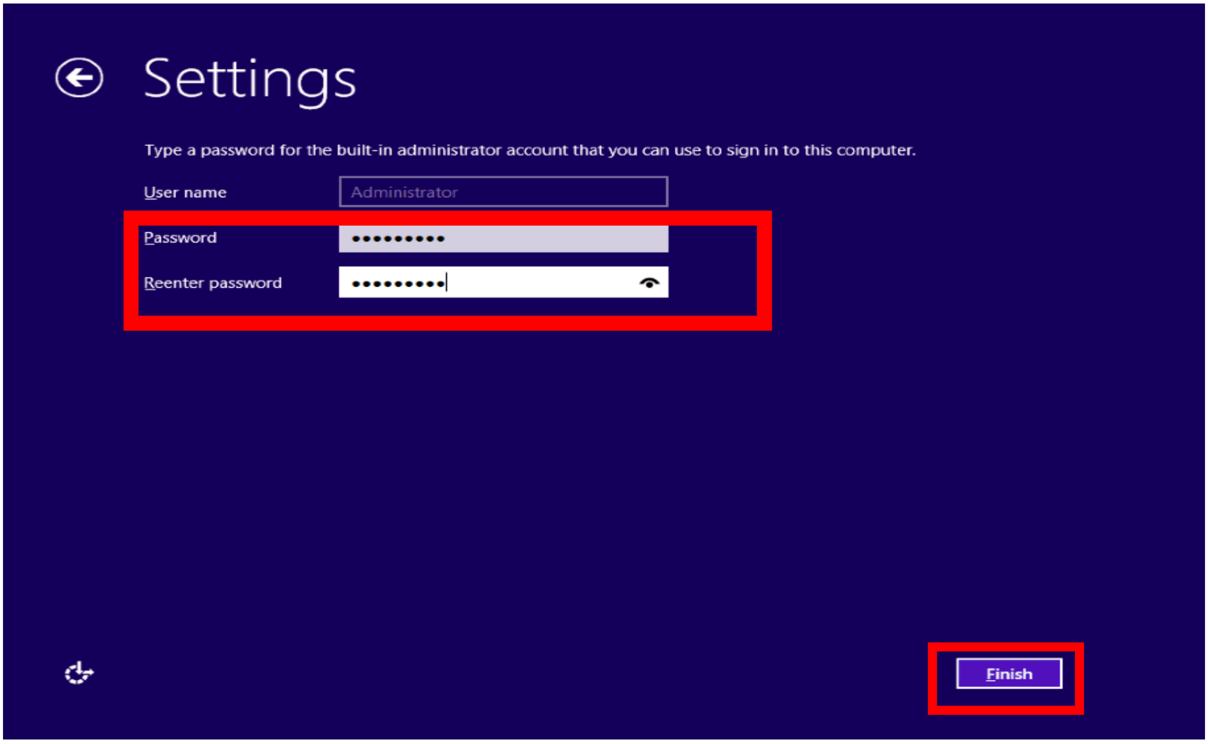
By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft's refund policies. See www.microsoft.com/worldwide. In the United States and Canada, call (800) MICROSOFT or see www.microsoft.com/info/nareturns.htm.

As described below, using some features also operates as your consent to the transmission of certain standard computer information for Internet-based services.

4.0 Define Administrator account password.

Please enter a password for the administrator account. For the Microsoft Server 2012 host, I will define the password “**admin123!”**.

Fill in the password in both fields and click **Finish**



Settings

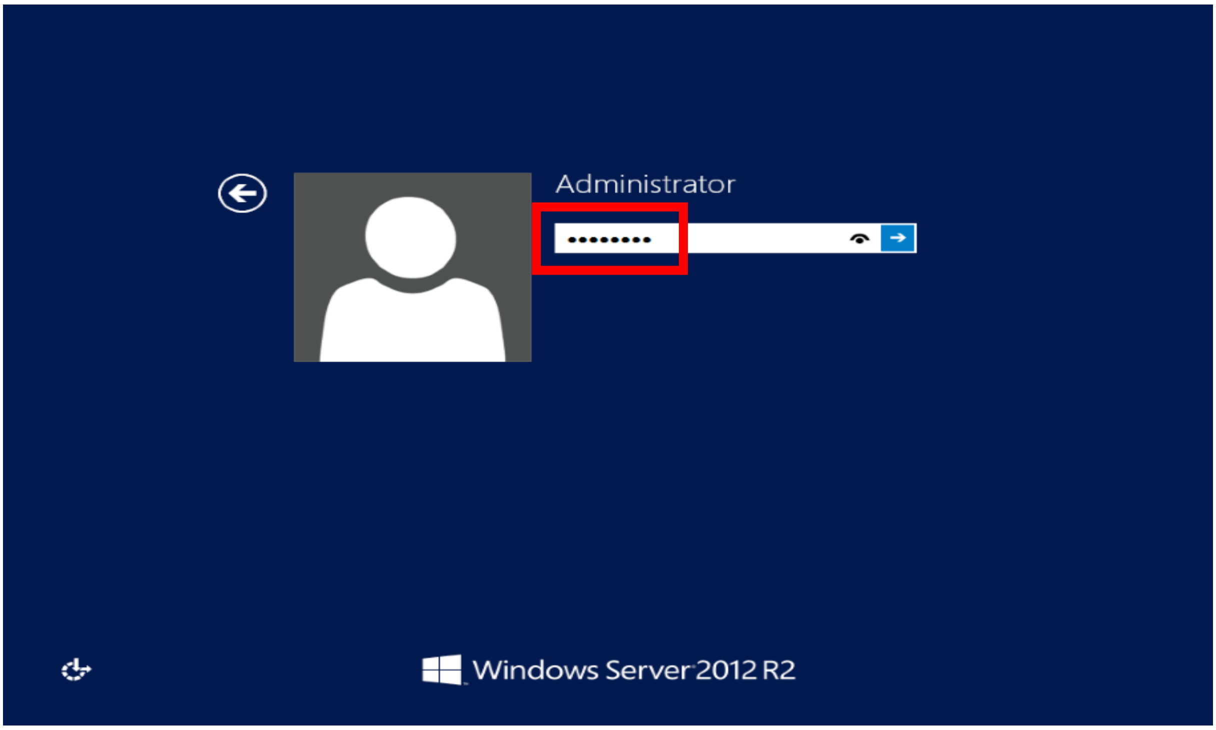
Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

Password: ••••••••••

Reenter password: ••••••••••

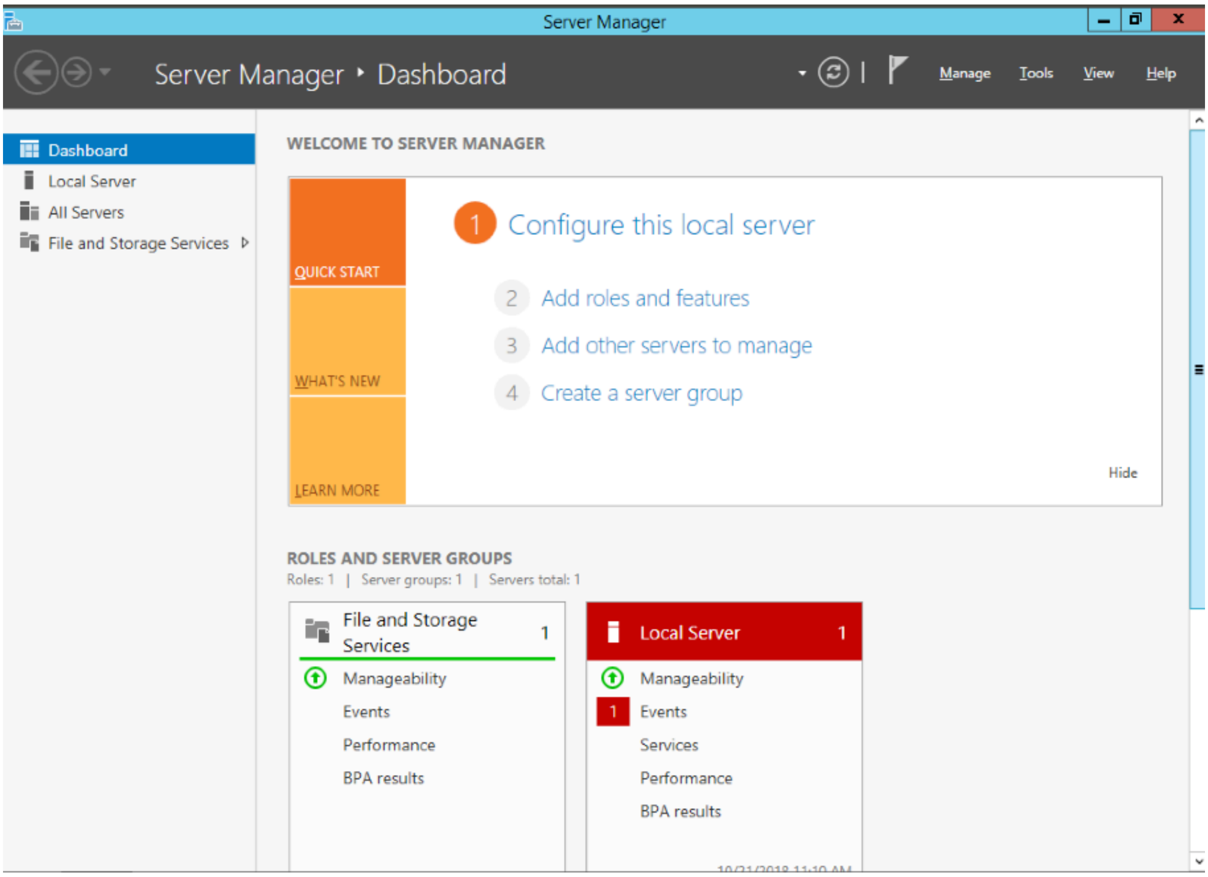
Installation is complete, let’s test the authentication credentials. Enter **admin123!** and hit **Enter** to log in.



Administrator

•••••••••

5.0 Installation is finished now. We now have the Microsoft Windows Server 2012 ready for adding roles. Please note that one of the roles that we will add to the server is, as the name implies (NY-AD), the **Active Directory** role.



5.0 Lab: Configure IP addressing on Lab hosts

Lab Objectives

- Configure IP addressing on Lab host machines
- Configure IP addressing on Cloud-Internet router

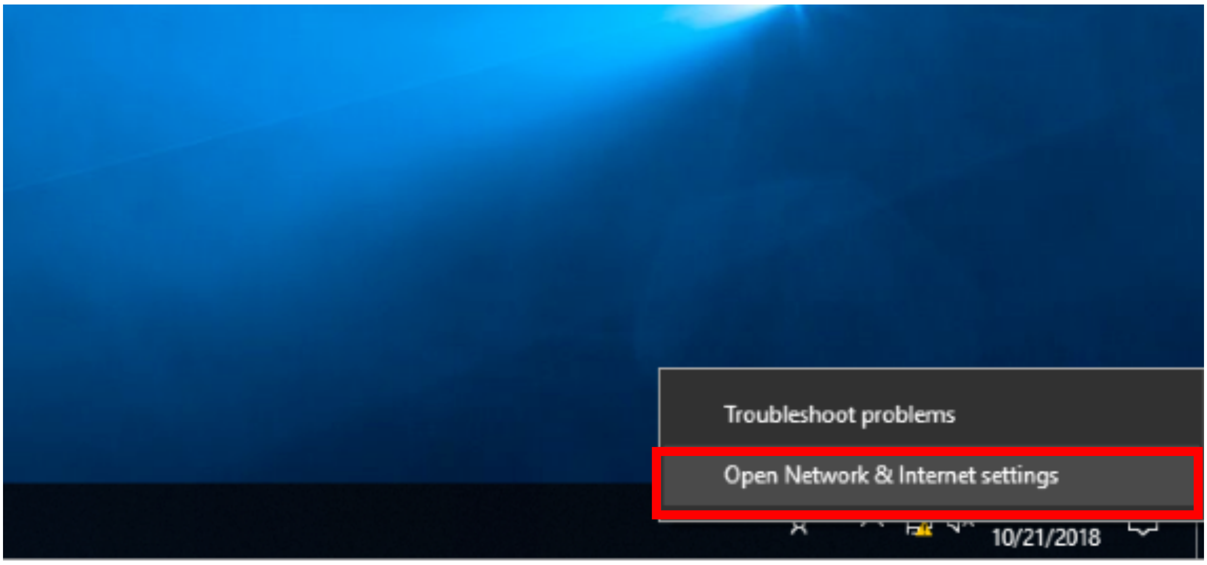
1.0 Start all Lab hosts and connect to console

Let's configure IP addressing on all of the hosts on the Lab topology, so that they are ready to use in the upcoming modules and associated labs. This section of Lab 5 refers to the following host machines:

- MGMT
- NY-LAN-1
- NY-AD
- NY-DMZ
- REMOTE-USER
- L-LAN-1

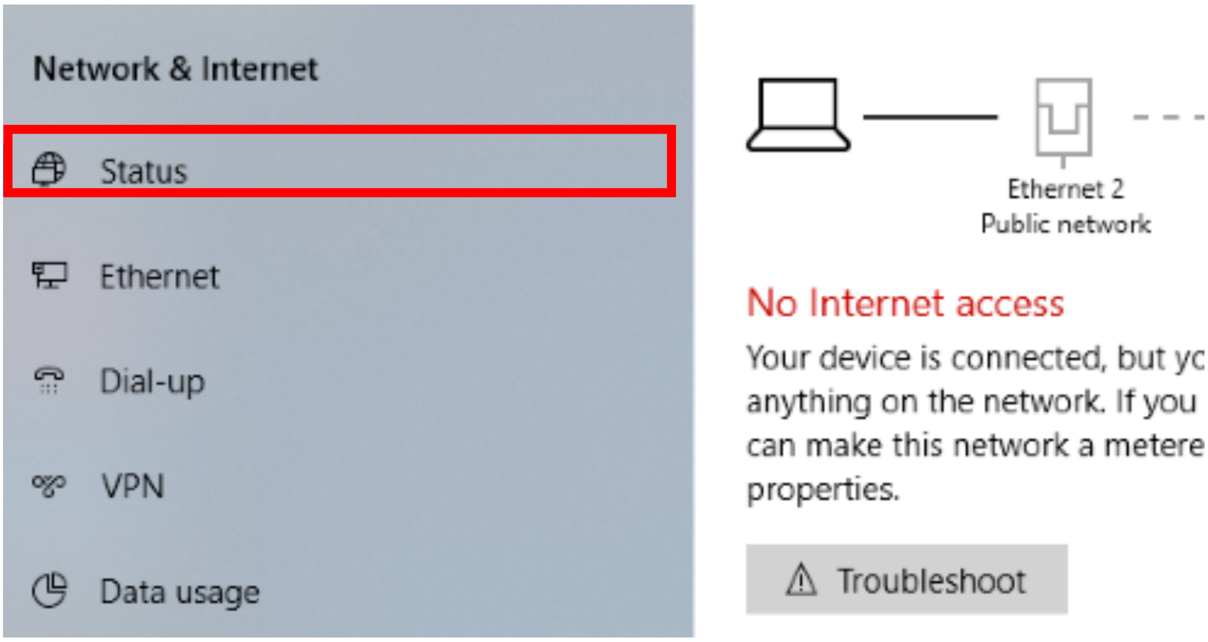
Right-click on device and click **Start.** Right-click on device and click **Console.**

Navigate with the cursor in the bottom-right of the screen, right-click on computer icon and click on **Open Network&Internet Settings.**



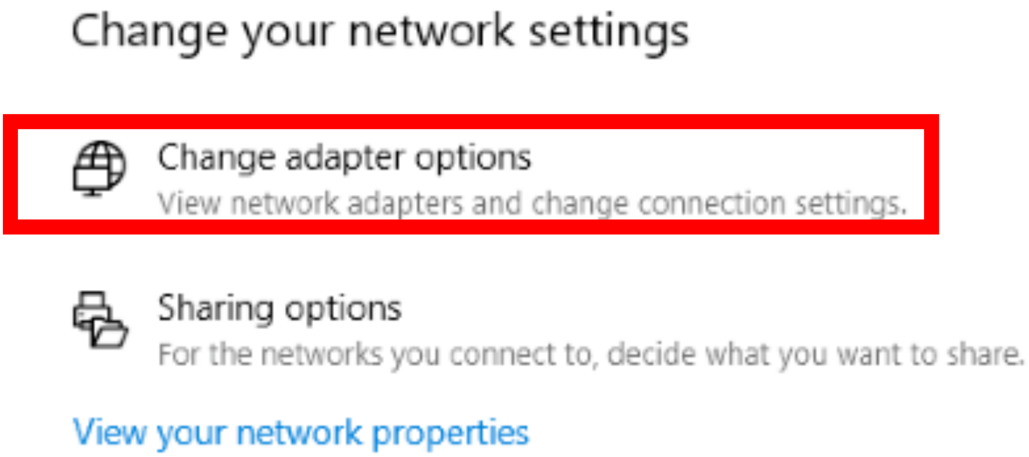
2.0 Navigate to Ethernet menu

On the left side, there is a menu **Network&Internet.** Navigate to **Status** category.



Your device is connected, but yc
anything on the network. If you
can make this network a metere
properties.

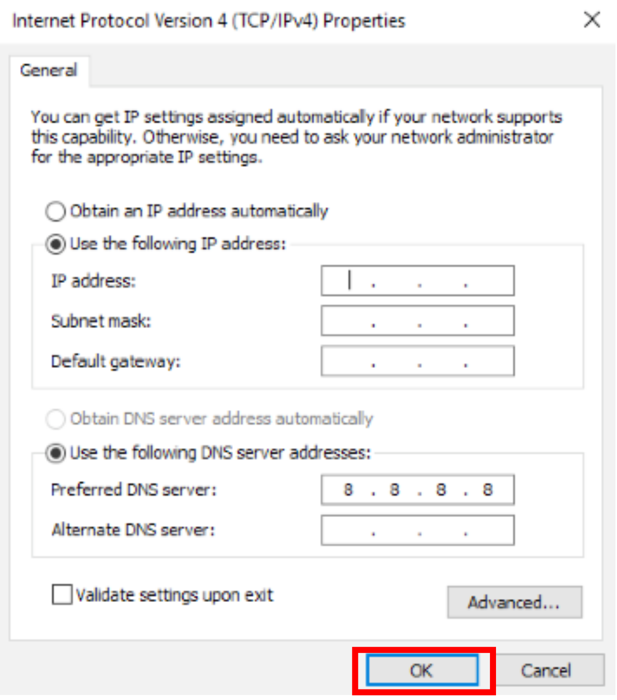
3.0 On the right side of the screen, under **Change your network settings** click on **Change adapter options**.


Change your network settings
Change adapter options
View network adapters and change connection settings.
Sharing options
For the networks you connect to, decide what you want to share.
View your network properties

4.0 Network connections window opens. You should see here at least one **Ethernet** card. Right-click on your Ethernet card and select **Properties.** Next, click on **Internet Protocol Version 4(TCP/IPv4)** and click on **Properties.**

Now, you can edit the IPv4 addressing for all your Windows host. Please take a look on the Lab diagram and note what is the IP addressing scheme used for the Windows hosts.

Fill in all the details and click **OK** to finish and apply configuration.



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: . . .

Subnet mask: . . .

Default gateway: . . .

○ 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

For simplicity, here is the complete list of IP addressing details that needs to be completed in this section of Lab 5 on Windows OS machines:

MGMT host machine

Parameter	Value
Name	MGMT
Internal Address	10.0.0.100/24
Default Gateway	10.0.0.1

NY-AD host machine

Parameter	Value
Name	NY-AD
Internal Address	172.16.10.200/24
Default Gateway	172.16.10.1

NY-LAN-1 host machine

Parameter	Value
Name	NY-LAN-1
Internal Address	172.16.10.100/24
Default Gateway	172.16.10.1

Remote-User host machine

Parameter	Value
Name	REMOTE-USER
IP Address	202.0.1.1/24
Default Gateway	202.0.1.254

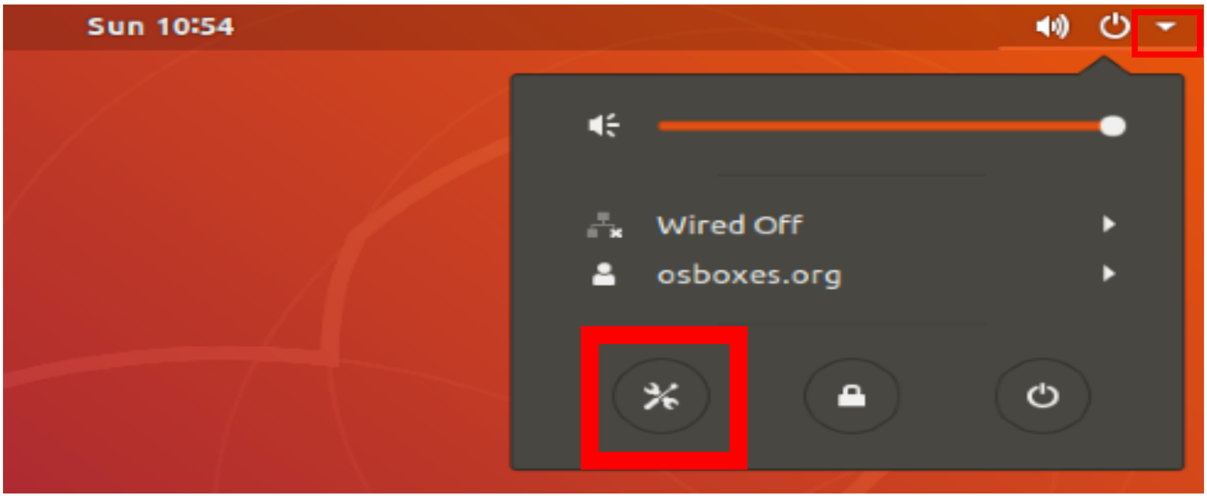
L-LAN-1 host machine

Parameter	Value
Name	L-LAN-1
Internal Address	172.16.30.100/24
Default Gateway	172.16.30.1

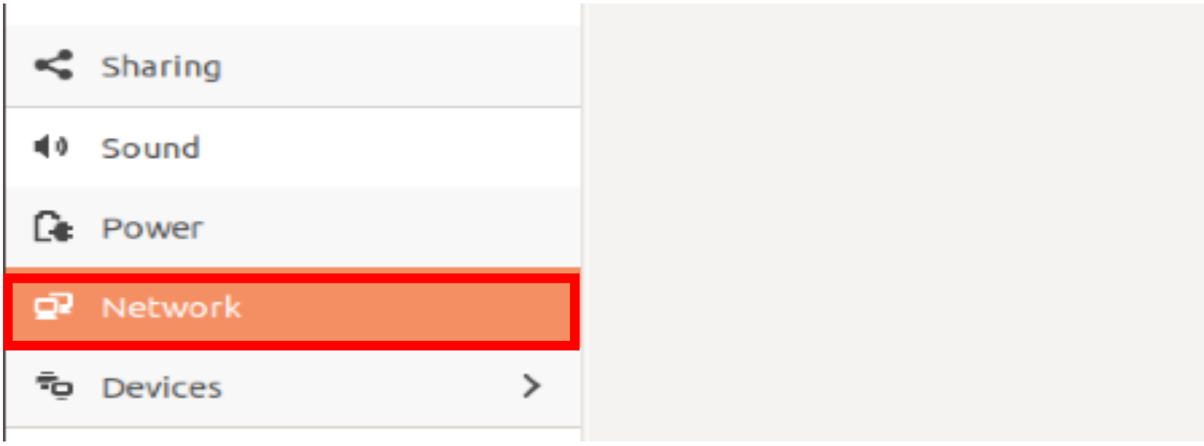
5.0 Configure IP addressing on NY-DMZ

Start NY-DMZ server and connect to console. Wait until the machine boots up and login. If you have installed the Ubuntu machine like it was presented in the video training, than the password is the same as username : **osboxes.org** Otherwise, enter your configured password.

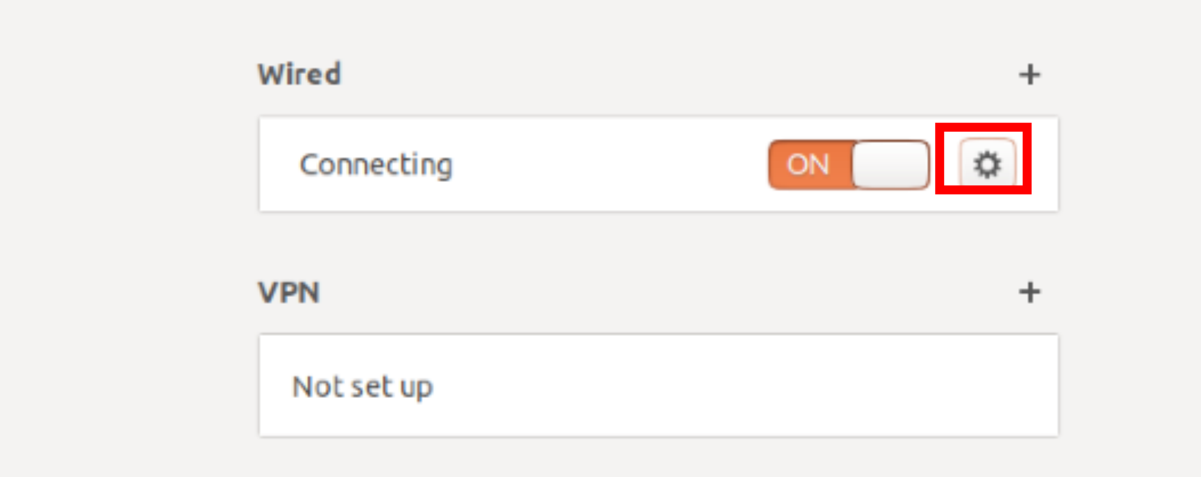
In the top-right part of the screen, click on the arrow and then click on Settings.



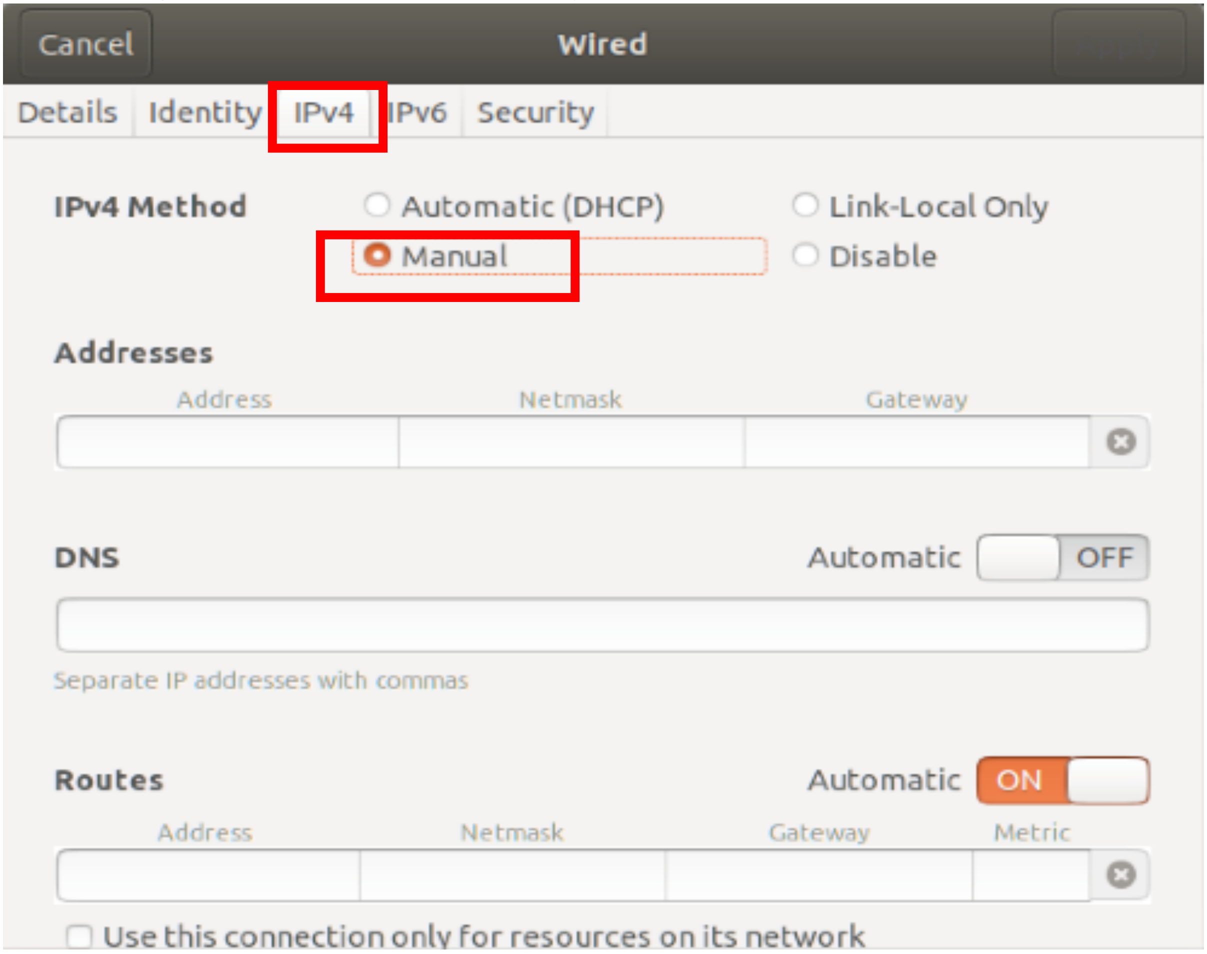
On the left-side of the Settings window, click on **Network.**



In the right-side of the window, click on **Settings** button.



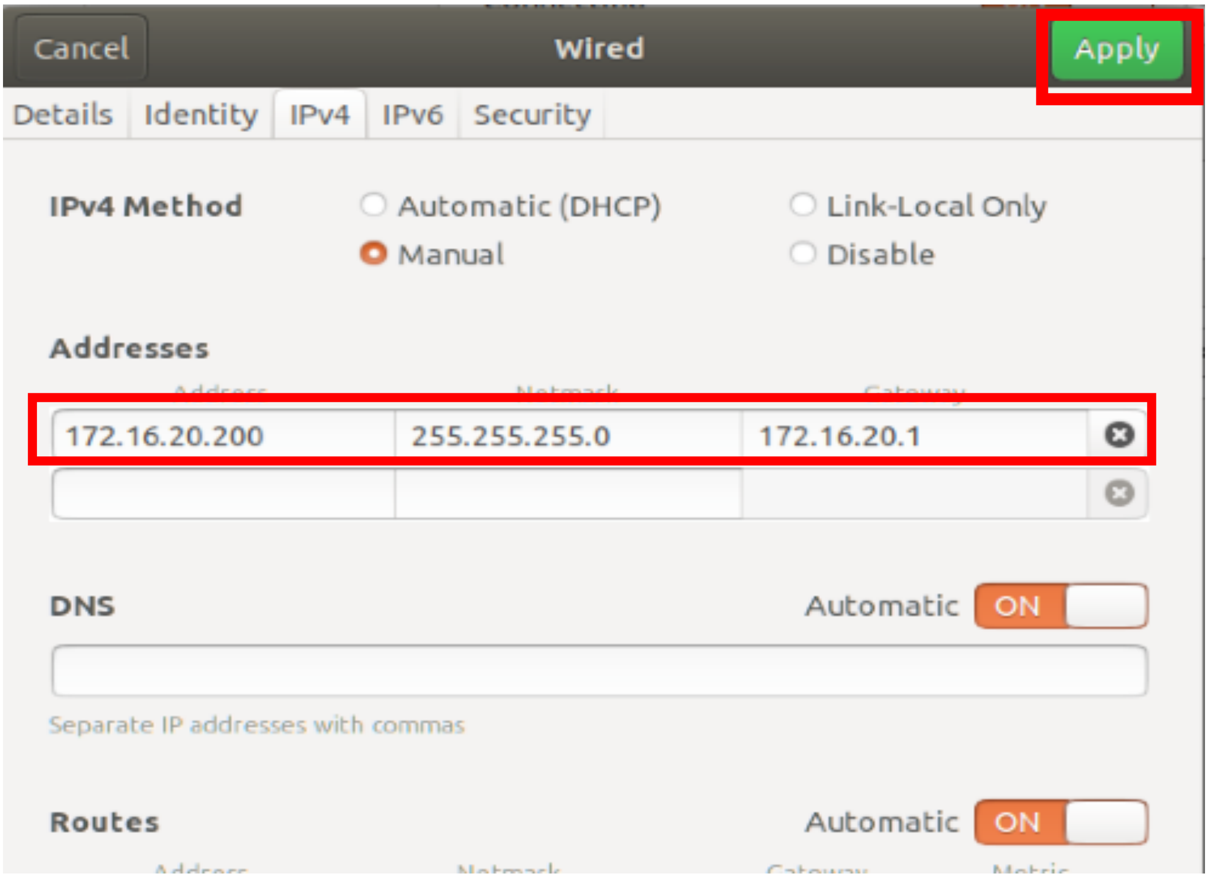
Now, navigate to **IPv4** menu at the top and click on **Manual.**



Fill in the following details, as outlined by the Lab Diagram:

Parameter	Value
Name	NY-DMZ
Internal Address	172.16.20.200/24
Default Gateway	172.16.20.1

When done, click **Apply** on top-right corner of the window.



IPv4 Method ○ Automatic (DHCP) ○ Link-Local Only ● Manual ○ Disable

Addresses

Address	Netmask	Gateway
172.16.20.200	255.255.255.0	172.16.20.1

DNS Automatic ON

Separate IP addresses with commas

Routes Automatic ON

Address Netmask Gateway Metric

6.0 Configure IP addressing on Cloud-Internet Router

Please take a look on the Lab diagram and note the IP addressing scheme.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CLOUD-ROUTER
CLOUD-ROUTER(config)#interface Gi1
CLOUD-ROUTER(config-if)#ip address 200.0.1.254 255.255.255.0
CLOUD-ROUTER(config-if)#description INTERFACE-TO-NY-FW-1
CLOUD-ROUTER(config-if)#interface Gi2
CLOUD-ROUTER(config-if)#ip address 201.0.1.254 255.255.255.0
CLOUD-ROUTER(config-if)#description INTERFACE-TO-L-FW-1
CLOUD-ROUTER(config-if)#interface Gi3
CLOUD-ROUTER(config-if)#ip address 202.0.1.254 255.255.255.0
CLOUD-ROUTER(config-if)#interface Gi4
CLOUD-ROUTER(config-if)#ip address dhcp
```

The CLOUD-ROUTER used in the Lab topology is a Cisco Router. Above configuration has been applied, but verifications need to be conducted. ALWAYS VERIFY YOUR CONFIGURATION !

Let's verify if interfaces got the IP addresses and also verify interfaces states:

```
CLOUD-ROUTER#show ip interface brief
Interface          IP-Address     OK? Method Status                Protocol
GigabitEthernet1   200.0.1.254    YES manual administratively down down
GigabitEthernet2   201.0.1.254    YES manual administratively down down
GigabitEthernet3   202.0.1.254    YES manual administratively down down
GigabitEthernet4   unassigned     YES DHCP   administratively down down
```

Technically speaking information related to IP addresses is not complete, because we don't see the subnet mask and we can't be sure if any typo is there or not. The next command should clarify the doubts:

```
CLOUD-ROUTER#show ip interface gi1
GigabitEthernet1 is administratively down, line protocol is down
  Internet address is 200.0.1.254/24
  Broadcast address is 255.255.255.255
  <output omitted>
```

Please note that all interfaces are not functional at the moment as they are in the **administratively down** state. Let's enable the interfaces:

```
CLOUD-ROUTER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CLOUD-ROUTER(config)#interface gi 1
CLOUD-ROUTER(config-if)#no shutdown
CLOUD-ROUTER(config-if)#interface gi 2
CLOUD-ROUTER(config-if)#no shut
CLOUD-ROUTER(config-if)#interface gi 3
CLOUD-ROUTER(config-if)#no shut
CLOUD-ROUTER(config-if)#interface gi 4
CLOUD-ROUTER(config-if)#no shut
CLOUD-ROUTER(config-if)#
CLOUD-ROUTER(config-if)#end
CLOUD-ROUTER#
CLOUD-ROUTER#
CLOUD-ROUTER#show ip interface brief
Interface          IP-Address     OK? Method Status                Protocol
GigabitEthernet1   200.0.1.254    YES manual up                    up
GigabitEthernet2   201.0.1.254    YES manual up                    up
GigabitEthernet3   202.0.1.254    YES manual up                    up
GigabitEthernet4   unassigned     YES DHCP   up                    up
```

Please note that interface Gi4 (or eth4) is connected to Internet Cloud and will receive the IP address through DHCP. A log like the following should appear in the CLOUD-ROUTER console, with different IP address/mask, depending on your environment.

%DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet4 assigned DHCP address 192.168.128.222, mask 255.255.255.0, hostname CLOUD-ROUTER

If everything went well, internet connectivity should be functional on CLOUD-ROUTER. Let’s verify:

```
CLOUD-ROUTER#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/17/18 ms
```

6.0 Lab: First Time Wizard on NY-FW-1

Lab Objectives

- Run the First Time Wizard on NY-FW-1 through WEB UI

After you finish the Gaia OS installation on NY-FW-1, when you connect to NY-FW-1 console, you will be provided the following message:

"In order to configure your system, please access the Web UI and finish the First Time Wizard."

What if you don't know what's the IP address of the FW you should be connecting to ? What is a quick way to find that ?

```
NY-FW-1> show management interface
eth2
NY-FW-1> show configuration interface
set interface eth0 link-speed 1000M/full
set interface eth0 state off
set interface eth0 auto-negotiation on
set interface eth1 state off
set interface eth2 link-speed 1000M/full
set interface eth2 state on
set interface eth2 ipv4-address 10.0.0.1 mask-length 24
set interface eth3 state off
set interface eth4 state off
set interface lo state on
set interface lo ipv4-address 127.0.0.1 mask-length 8
NY-FW-1>
```

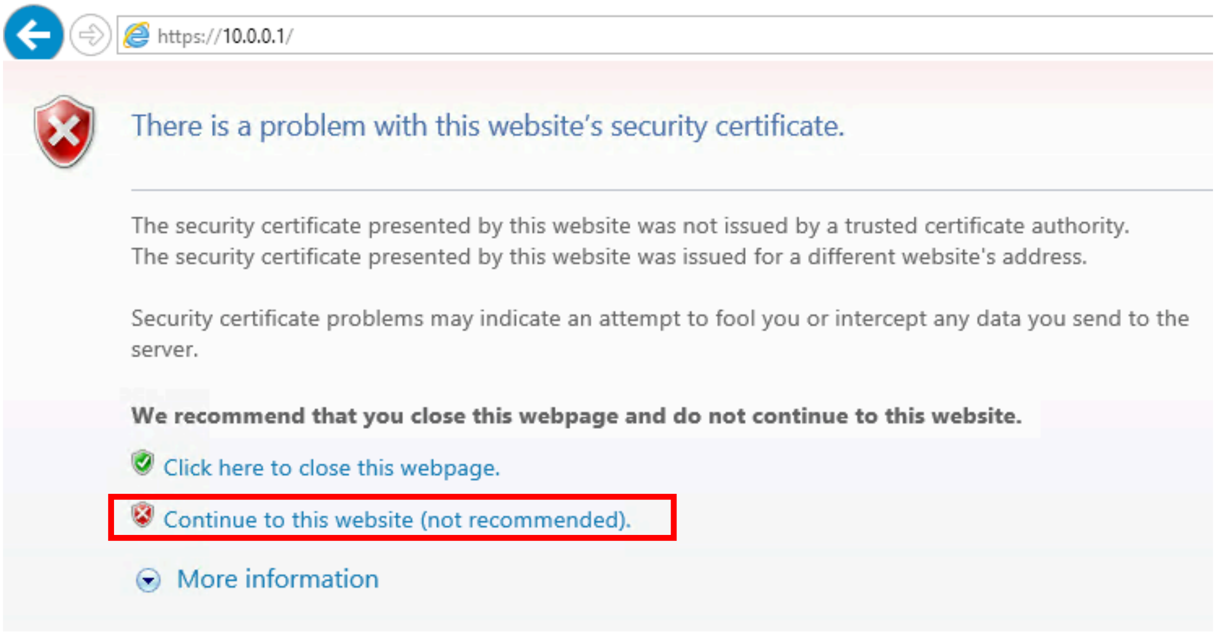
I know that we haven't discussed so far about CLI – Command Line Interface, I will be introducing this in this module, Module 4, with a detailed lab, but this is a good moment to learn something new.

So, if no information is available, no Lab diagram, etc … this is what you could do. The first command ***"show management interface"*** will show you what is the interface of the appliance that is being used as the management interface. If the appliance is not a physical one, any interface can be used as the management interface.

The second command ***"show configuration interface"*** will output the current configuration that is applied for all interfaces available. We can easily see that the Management IP address of NY-FW-1 is 10.0.0.1.

Open a browser, classic Internet Explorer (not Edge), on MGMT PC and navigate to : ***https://10.0.0.1.***

You will receive a warning related to the Digital Certificate the NY-FW-1 is presenting when connecting through secure HTTP (HTTPS).



https://10.0.0.1/

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

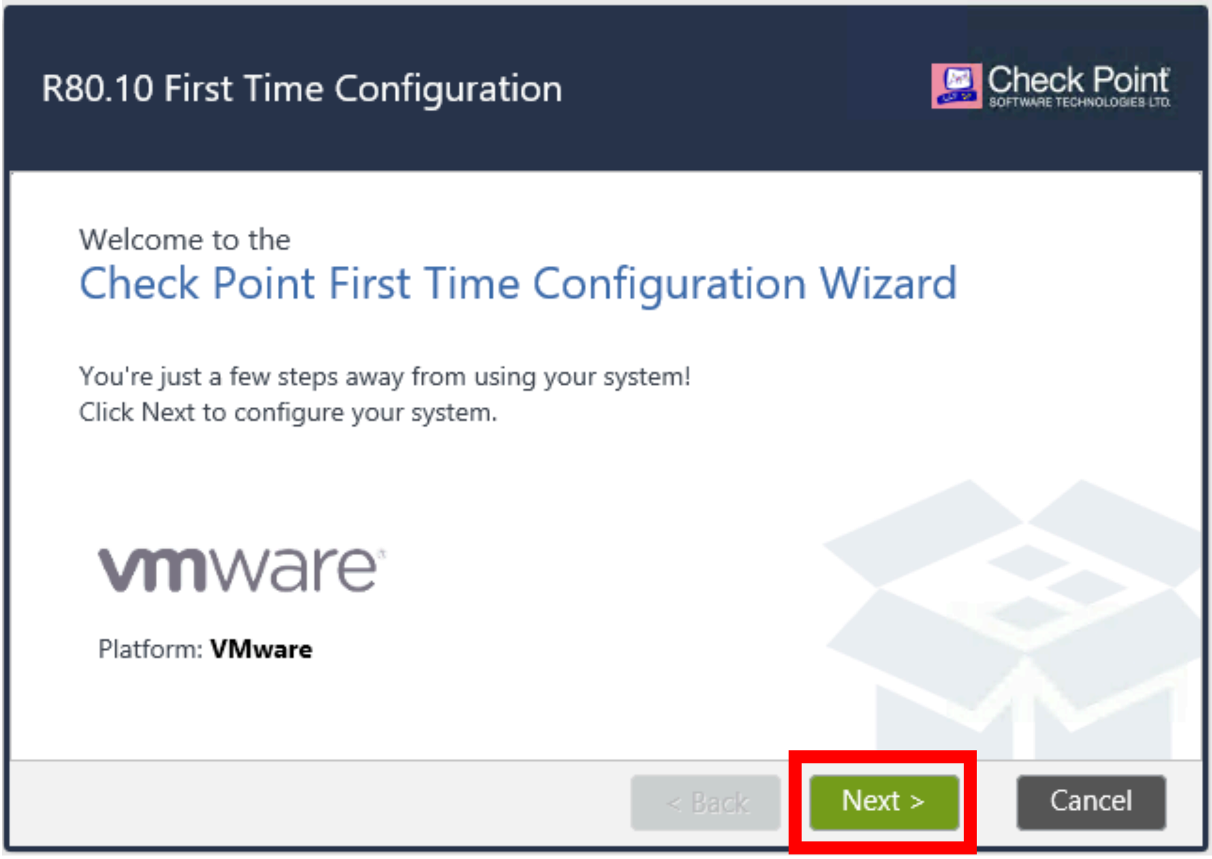
More information

Click on ***"Continue to this site (not recommended)"*** and you will be directed to Gaia Portal R80.10. Please enter login credentials as defined in the previous configuration steps. As mentioned previously, I am using ***admin/admin123*** as my username and password authentication pair.

Enter username and password and hit **Enter.**

Let's start the Check Point First Time Wizard for New York HQ Firewall.

Click **Next** to begin.



R80.10 First Time Configuration

Welcome to the
Check Point First Time Configuration Wizard

You're just a few steps away from using your system!
Click Next to configure your system.

Platform: **VMware**

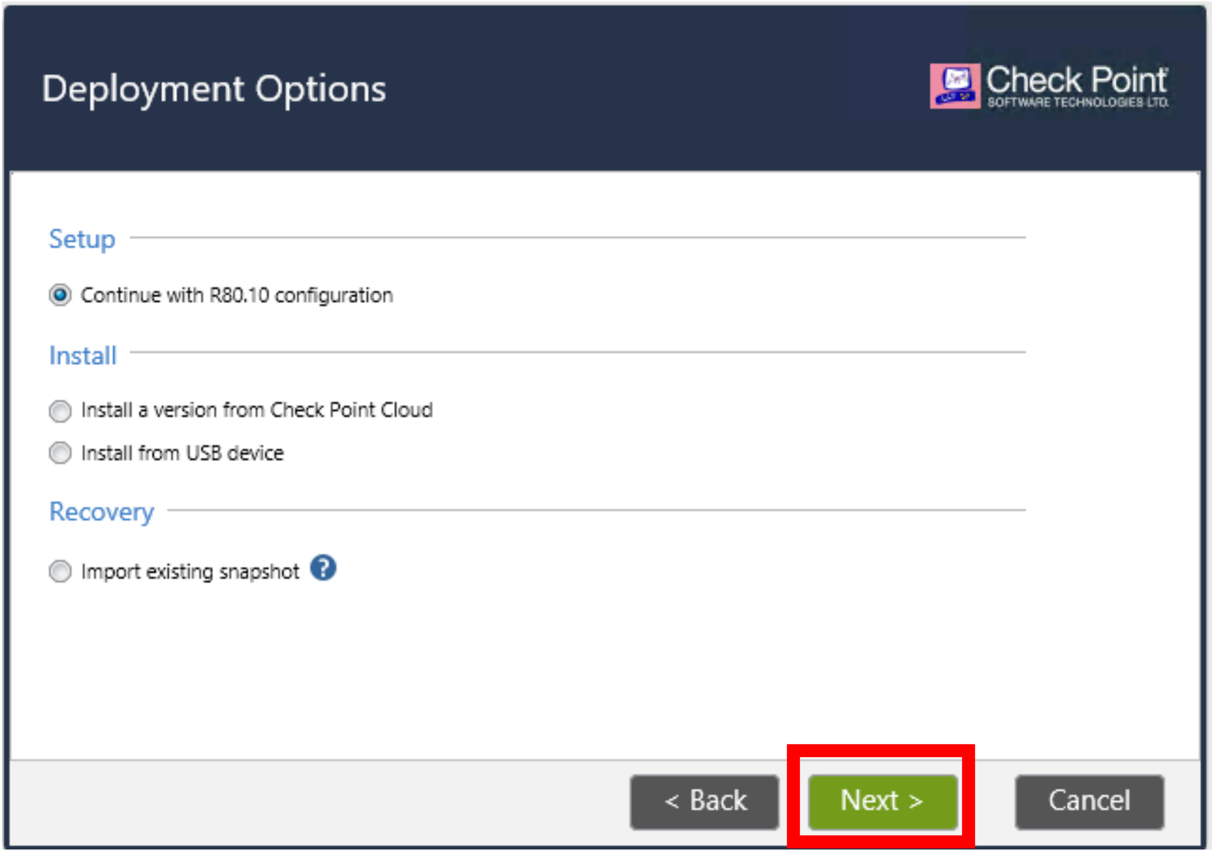
The next screen will provide you different options that you may want to choose when running the First Time Wizard (FTW).

The option ***Install a version from Check Point Cloud*** provides as the name implies installation of Gaia through the internet. In this case you would have to define IP address, Subnet Mask and Default Gateway on an interface that will connect to Check Point Cloud through Internet and will fetch configuration this way.

The option ***"Install from USB Device"*** will help you install fast the parameters included in FTW, from a previous install, that were saved on a USB stick.

The last option ***"Import existing snapshot"*** includes the most complete backup solution Check Point is offering for its appliances. This option includes OS and configuration parameters. You can think of this as a snapshot of a virtual machine that you are running in VMware Workstation on your PC.

1. Leave the first option selected ***"Continue with R80.10 configuration"*** and click **Next** to continue.



Deployment Options

Setup

● Continue with R80.10 configuration

Install

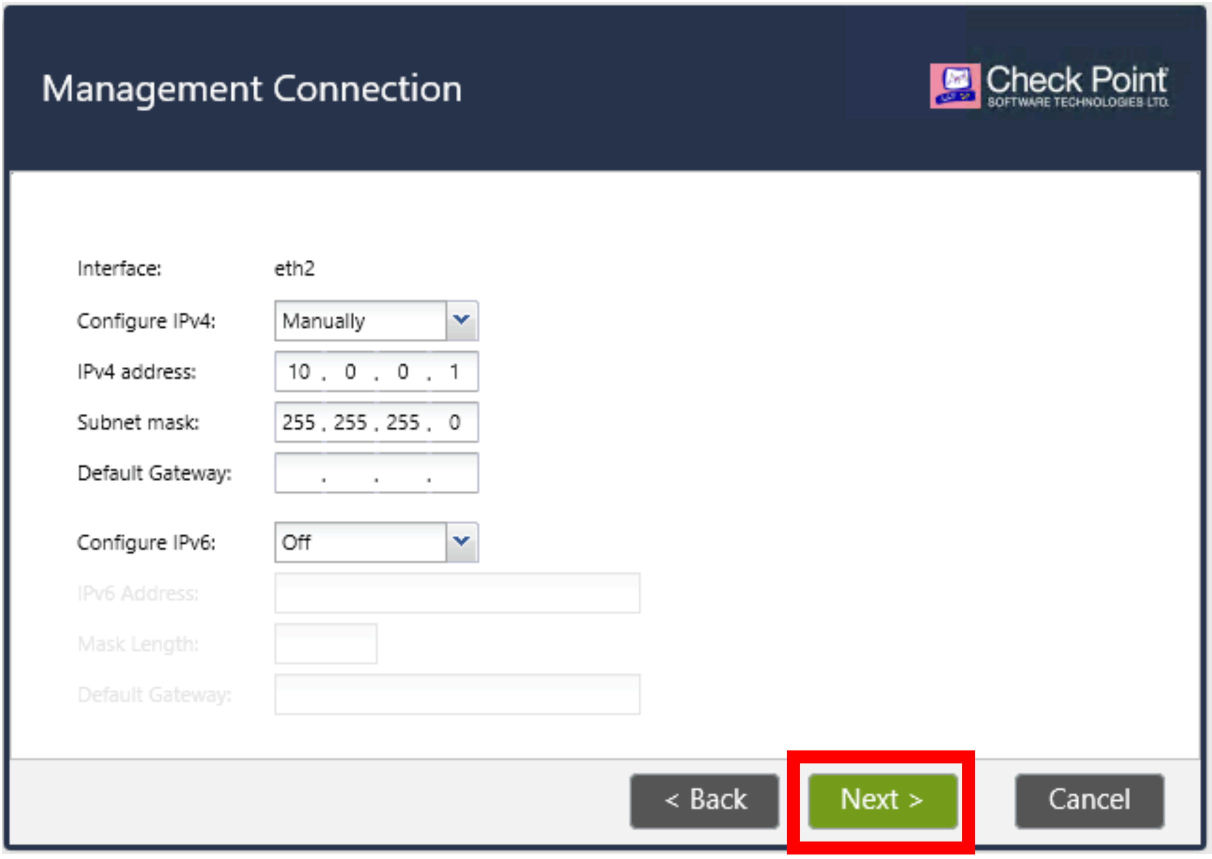
○ Install a version from Check Point Cloud

○ Install from USB device

Recovery

○ Import existing snapshot

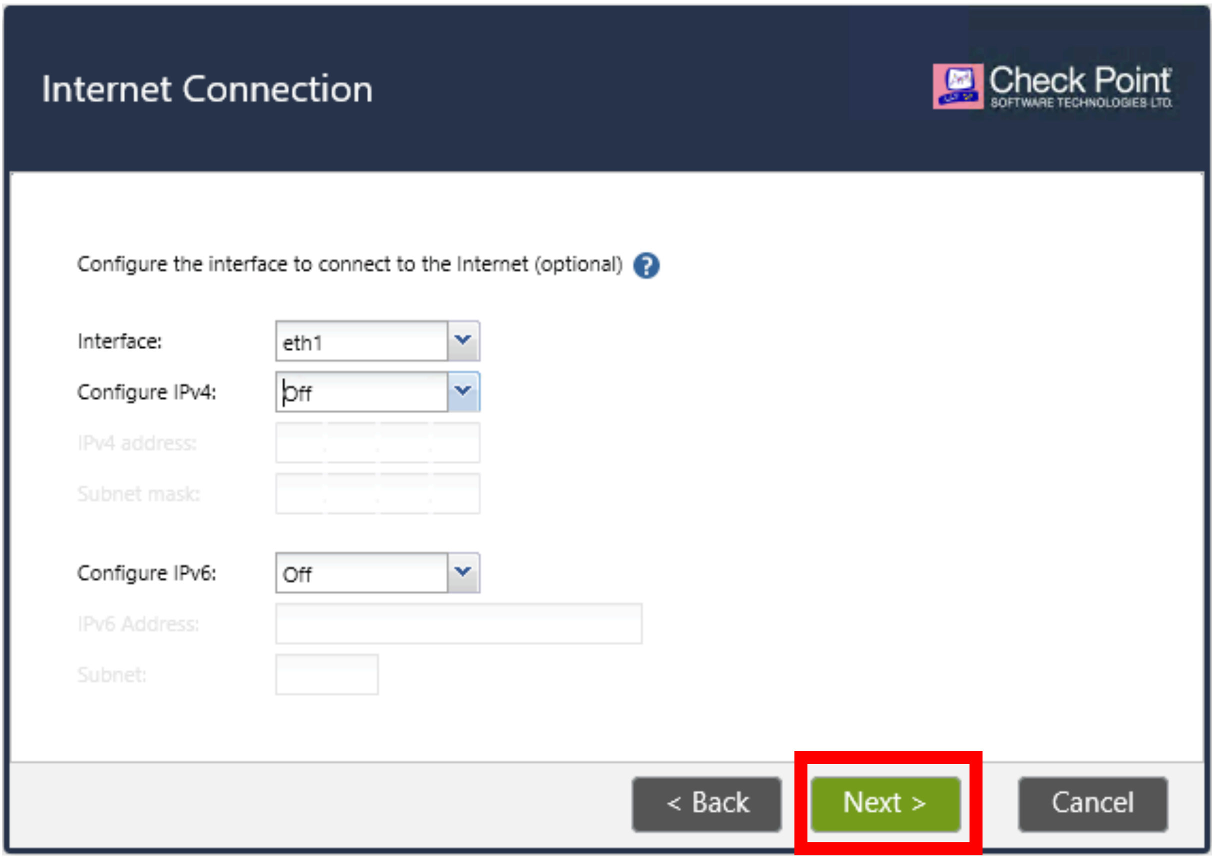
2. Confirm the IP addressing schema for your ETH2 management interface and click **Next** to continue.



Management Connection

Interface:	eth2
Configure IPv4:	Manually
IPv4 address:	10 . 0 . 0 . 1
Subnet mask:	255 . 255 . 255 . 0
Default Gateway:	. . .
Configure IPv6:	Off
IPv6 Address:	
Mask Length:	
Default Gateway:	

3. Optional, you can configure the IP address for NY-FW-1 internet connectivity in this step. This will be configured in a later module, when connection to the Web UI (user interface). For now, just click **Next** to continue.



Internet Connection

Configure the interface to connect to the Internet (optional)

Interface: eth1

Configure IPv4: Off

IPv4 address:

Subnet mask:

Configure IPv6: Off

IPv6 Address:

Subnet:

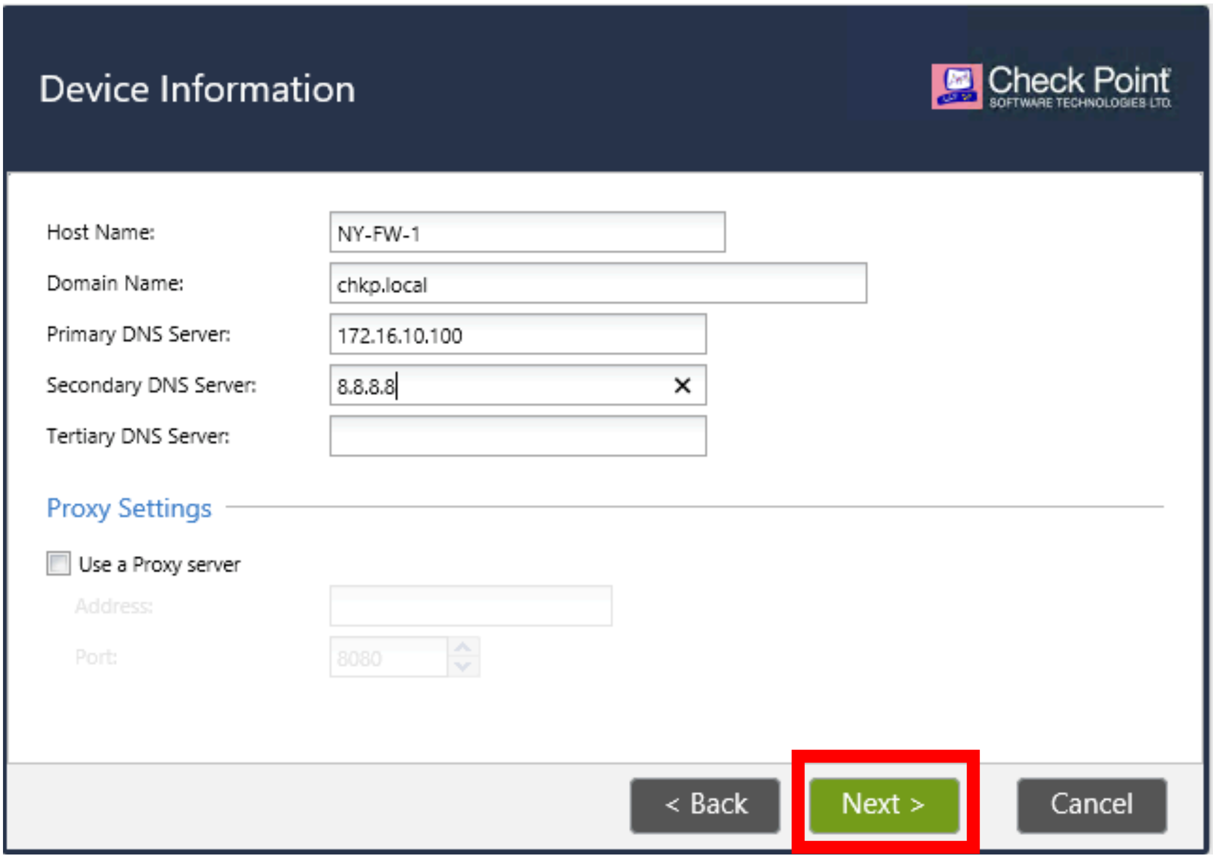
4. Configure device information.

Please fill in the necessary details as per below table.

Parameter	Value
Host Name	NY-FW-1
Domain Name	chkp.local
Primary DNS Server	172.16.10.100
Secondary DNS Server	8.8.8.8
Tertiary DNS	<Leave Blank>

Please note that the Primary DNS IP Address is actually the Microsoft 2012 AD Server. We will configure AD and DNS roles on the server at the later stage.

Click **Next** to continue.



Device Information

Host Name: NY-FW-1

Domain Name: chkp.local

Primary DNS Server: 172.16.10.100

Secondary DNS Server: 8.8.8.8

Tertiary DNS Server:

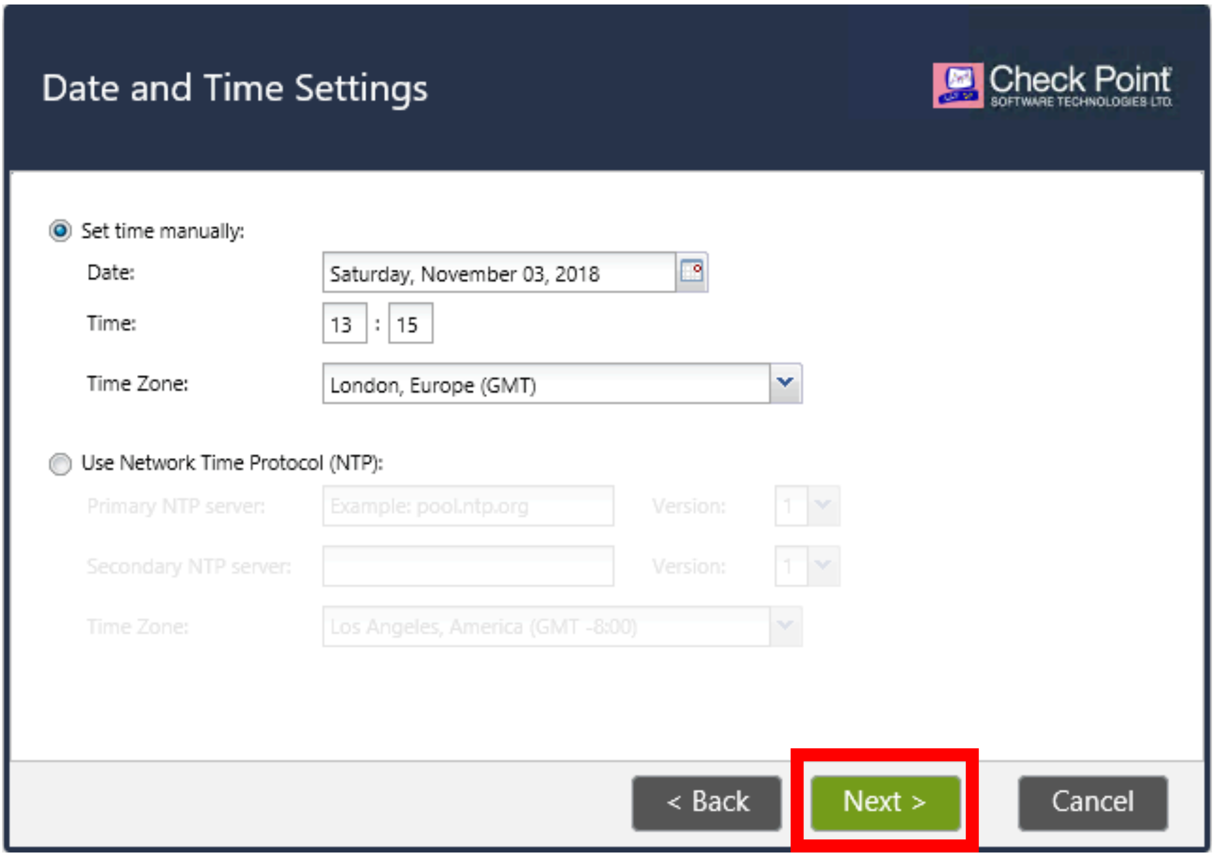
Proxy Settings

□ Use a Proxy server

Address:

Port: 8080

5. Date and Time settings.



Date and Time Settings

● Set time manually:

Date: Saturday, November 03, 2018

Time: 13 : 15

Time Zone: London, Europe (GMT)

○ Use Network Time Protocol (NTP):

Primary NTP server: Example: pool.ntp.org Version: 1

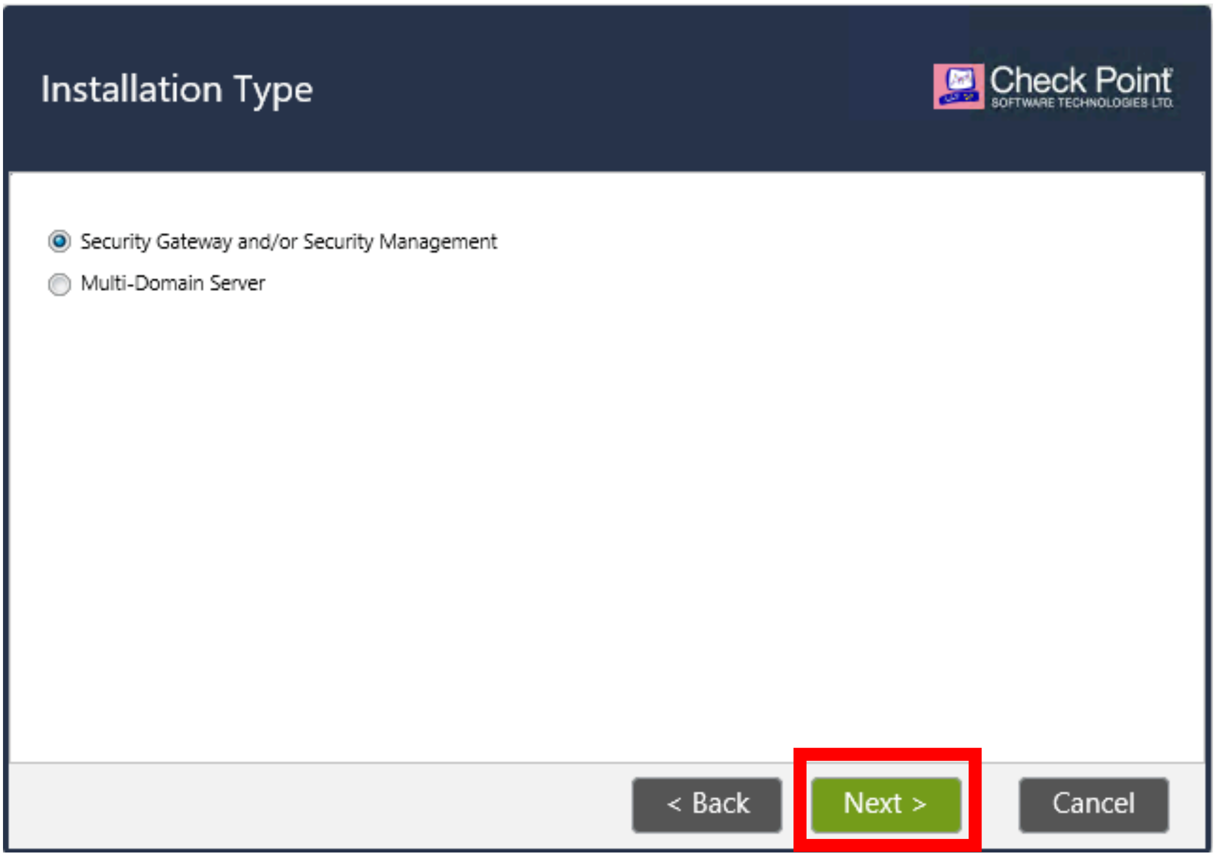
Secondary NTP server: Version: 1

Time Zone: Los Angeles, America (GMT -8:00)

6. Installation Type.

In this step, you will choose what is the machine going to be. Is it going to run as a Security Gateway ? Or a Security Management Server ? Either separate or on the same machine … or is this going to be a Multi-Domain server ?

For now, don’t worry about the second option, it will be explored later if needed. Our choice is the first one, please click **Next** to continue.



Installation Type

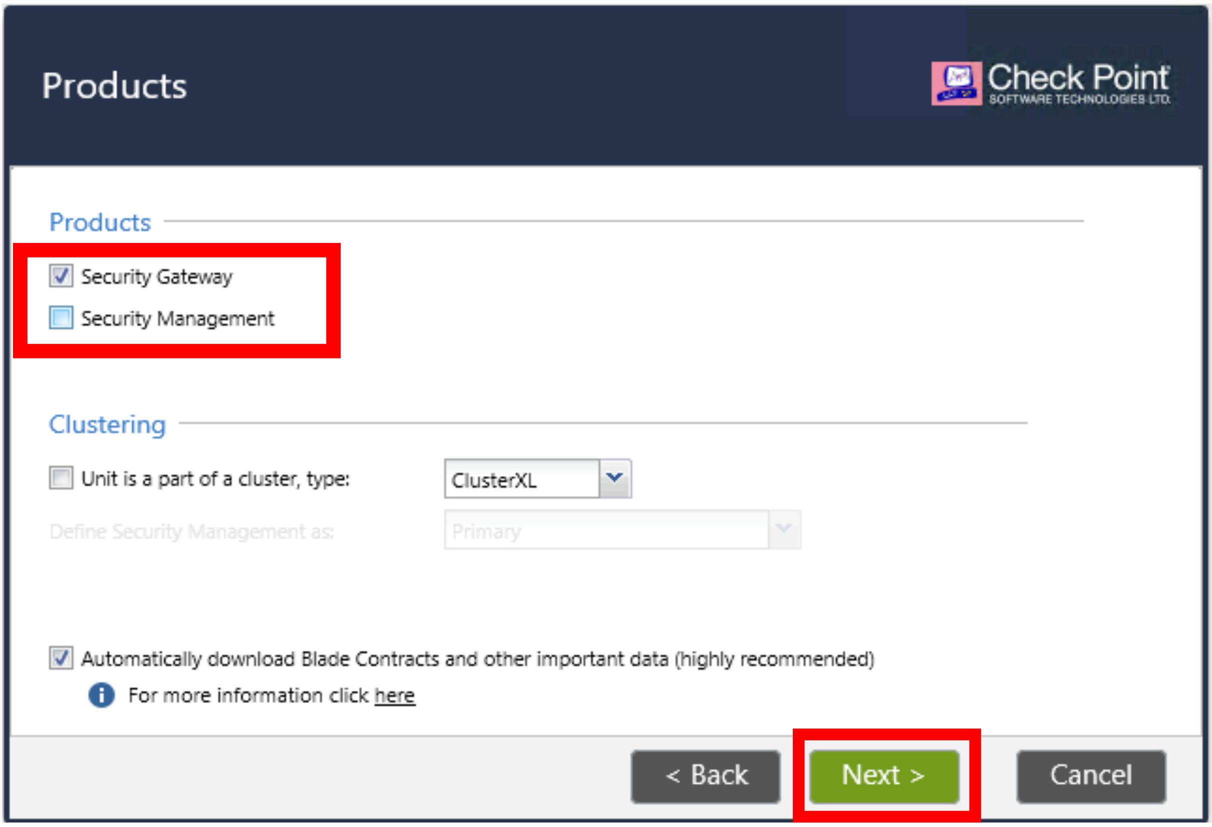
● Security Gateway and/or Security Management
○ Multi-Domain Server

7. Products.

This is a very important step in the configuration, please pay attention. Now you will define what kind of deployment will this be. Will you run the Security Gateway and the Security Management Server functionalities on the same machine or separately ?

This refers to what was explained in Module 1. You need to decide at this step if this is going to be a Standalone deployment or a Distributed deployment. In our lab, this is Distributed deployment, as we have a separate SMS machine.

Please **delesect** the **Security Management** option and then click **Next** to continue.



Products

Products

☑ Security Gateway

□ Security Management

Clustering

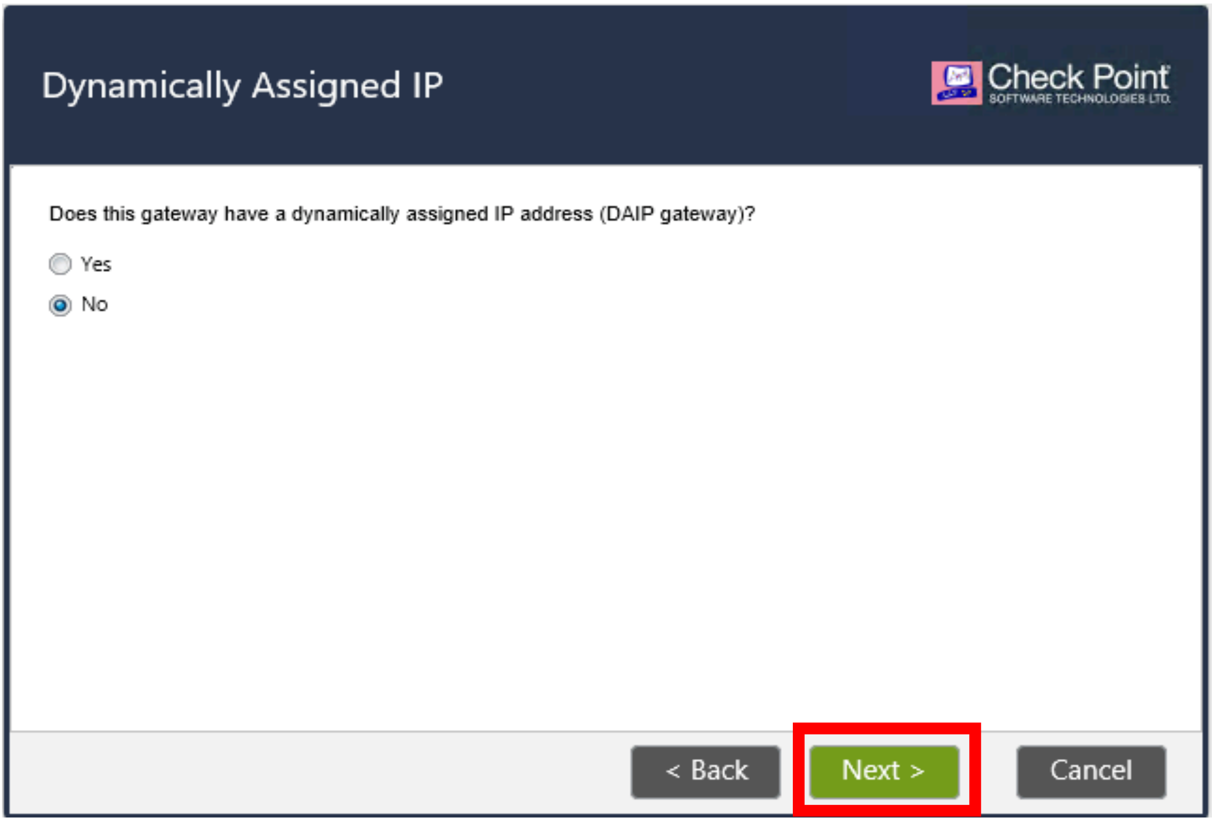
□ Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

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

For more information click here

8. Dynamically Assigned IP



Dynamically Assigned IP

Does this gateway have a dynamically assigned IP address (DAIP gateway)?

○ Yes

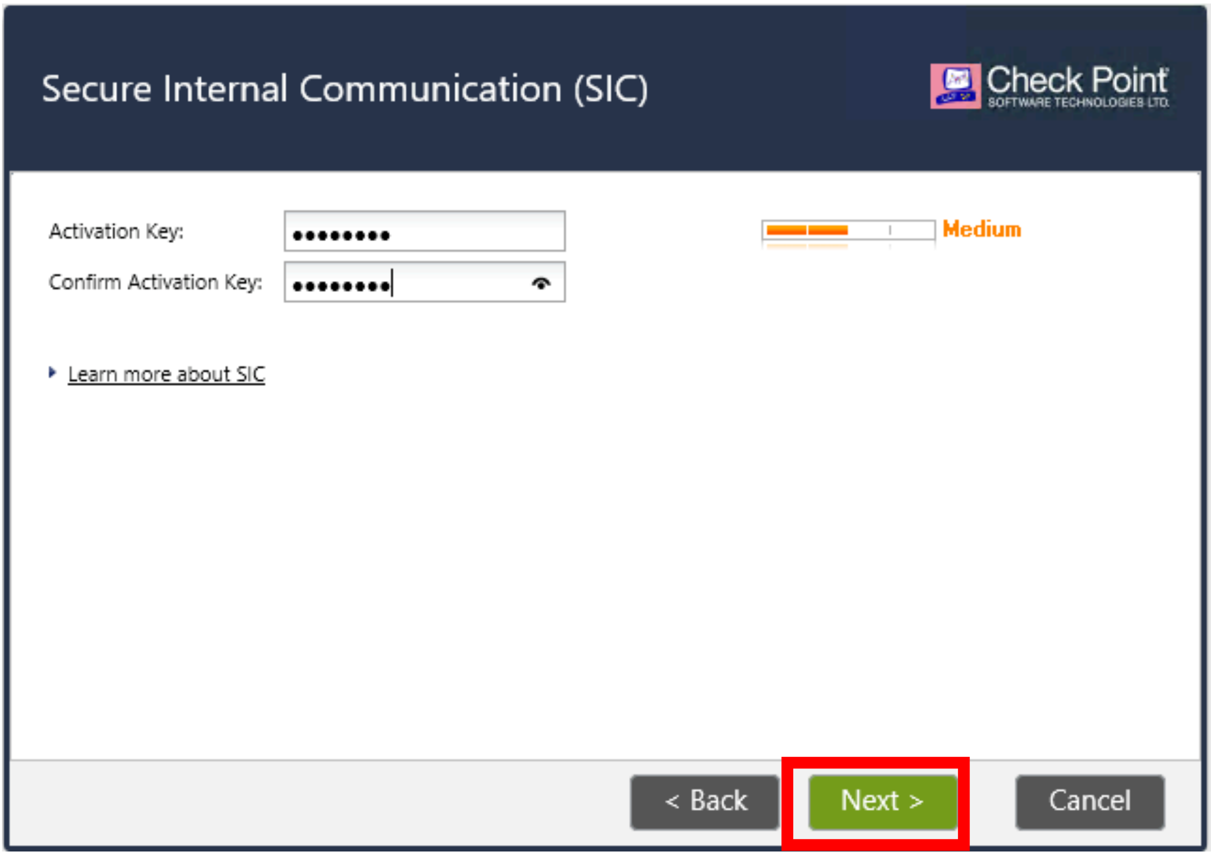
● No

NY-FW-1 Gateway will have all IP addresses statically defined, no dynamic DHCP in this case. Leave everything as it is and click **Next** to continue.

9. Secure Internal Communication (SIC)

When first contacting the Security Management Server, the connection between the GW and SMS is authenticated based on the password (or SIC key) that you define. After successful authentication, SMS will provide digital certificates to all GWs and the authentication will be based on certificates, just like in a typical PKI environment.

Please type **admin123** as the activation key and click **Next** to continue.



Secure Internal Communication (SIC)

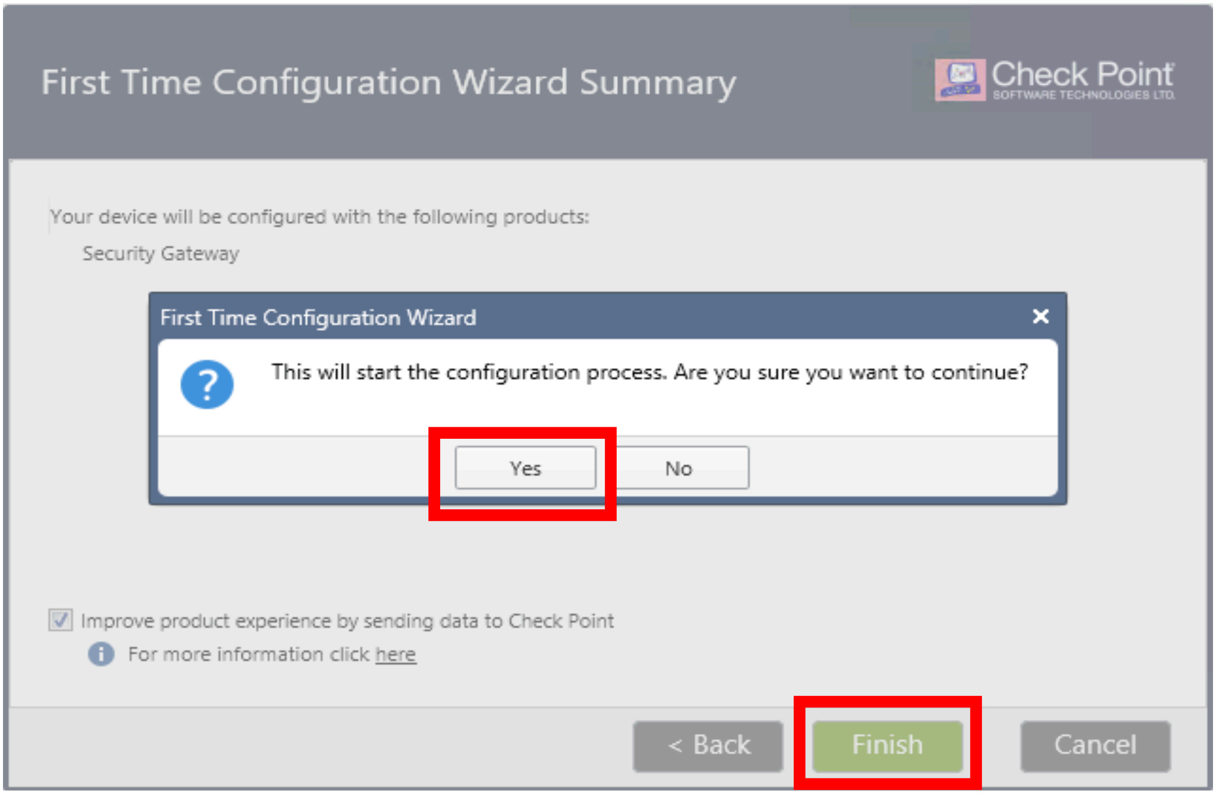
Activation Key: ••••••••

Confirm Activation Key: ••••••••

10. First Time Wizard Summary

This concludes the First Time Wizard installation steps. The wizard outlines the fact that this machine will be a Security Gateway after FTW installation will run.

Please click **Finish** and then **Yes** in order to start the FTW installation.


First Time Configuration Wizard Summary
Check Point
SOFTWARE TECHNOLOGIES LTD.
Yes
No
< Back
Finish
Cancel

Your device will be configured with the following products:

Security Gateway

First Time Configuration Wizard

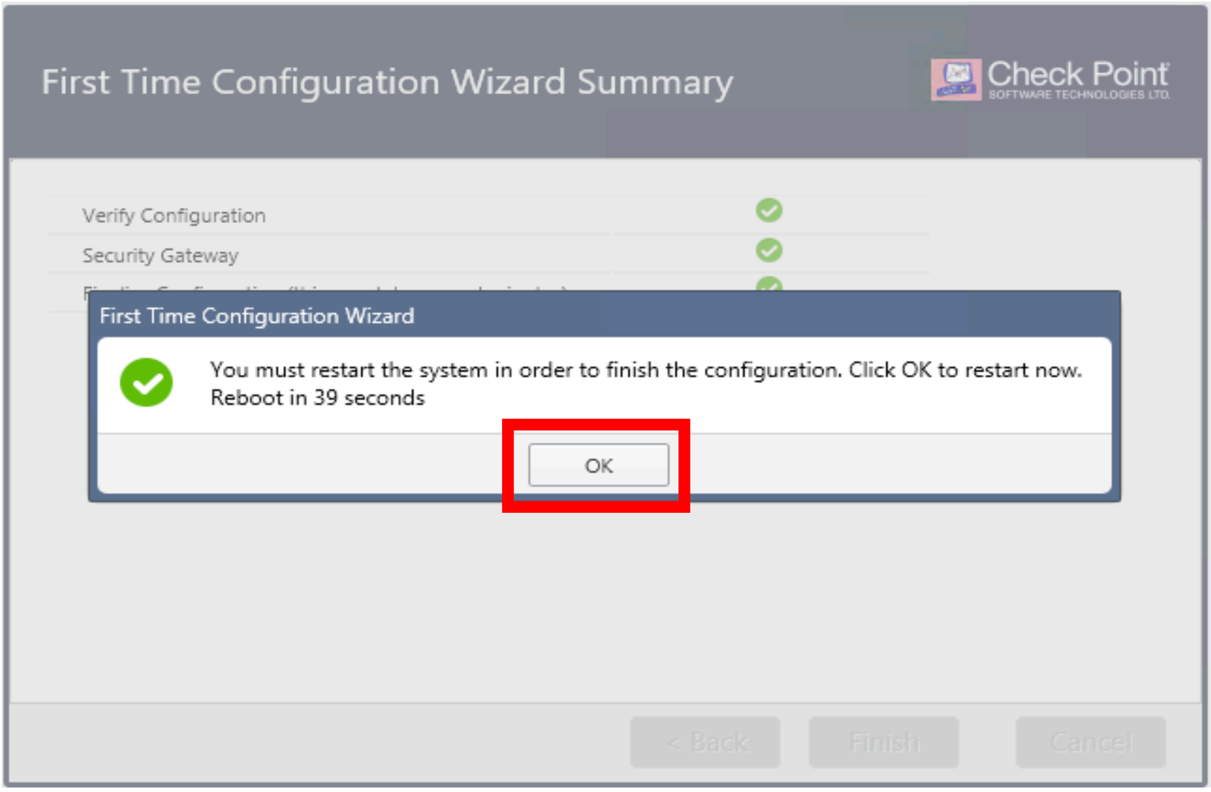
This will start the configuration process. Are you sure you want to continue?

☑ Improve product experience by sending data to Check Point

For more information click here

11. Restart the system.

Either wait or click **OK.**


First Time Configuration Wizard Summary
Check Point
SOFTWARE TECHNOLOGIES LTD.
OK
< Back
Finish
Cancel

Verify Configuration ✓

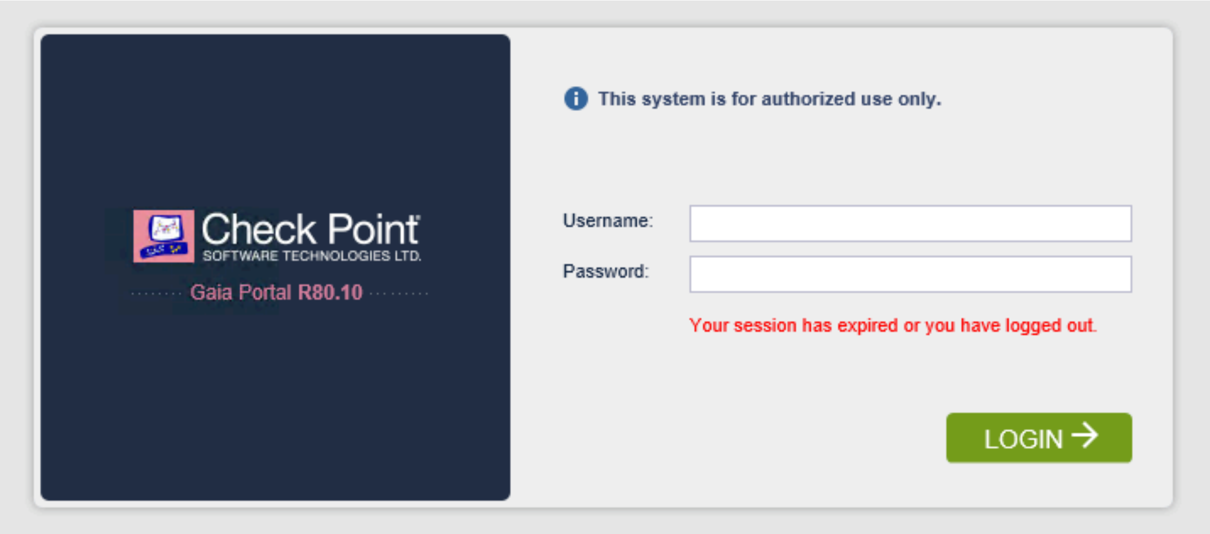
Security Gateway ✓

First Time Configuration Wizard

You must restart the system in order to finish the configuration. Click OK to restart now.
Reboot in 39 seconds

12.Verification

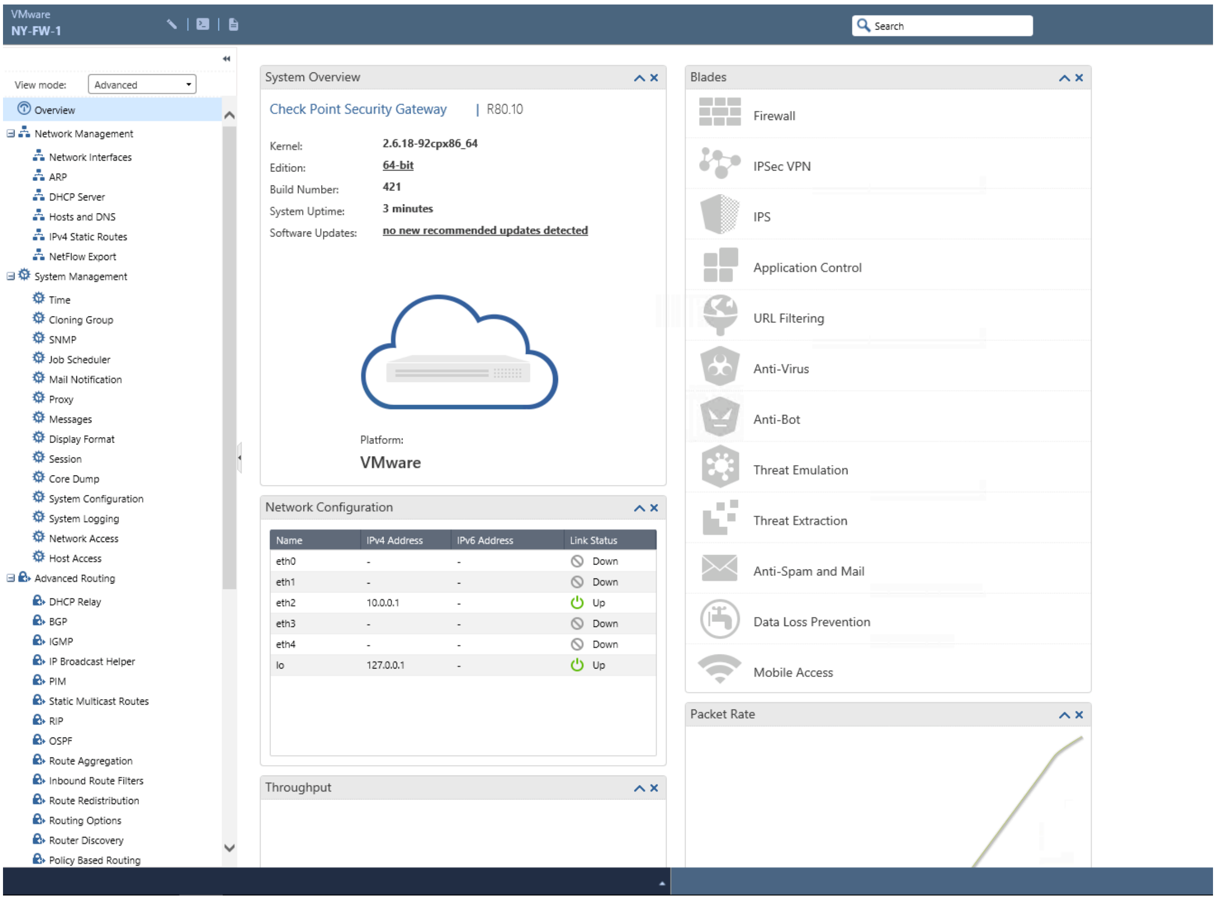
After the system restarts, you are being asked to login to the system:



This system is for authorized use only.

Your session has expired or you have logged out.

Enter your authentication username and password (admin/admin123) and you should successfully login into the Gaia Web UI.



Check Point Security Gateway | R80.10

Kernel: 2.6.18-92cpx86_64
Edition: 64-bit
Build Number: 421
System Uptime: 3 minutes
Software Updates: no new recommended updates detected

Platform: VMware

Name	IPv4 Address	IPv6 Address	Link Status
eth0	-	-	Down
eth1	-	-	Down
eth2	10.0.0.1	-	Up
eth3	-	-	Down
eth4	-	-	Down
lo	127.0.0.1	-	Up

7.0 Lab: Introduction to Gaia Web UI

Lab Objectives

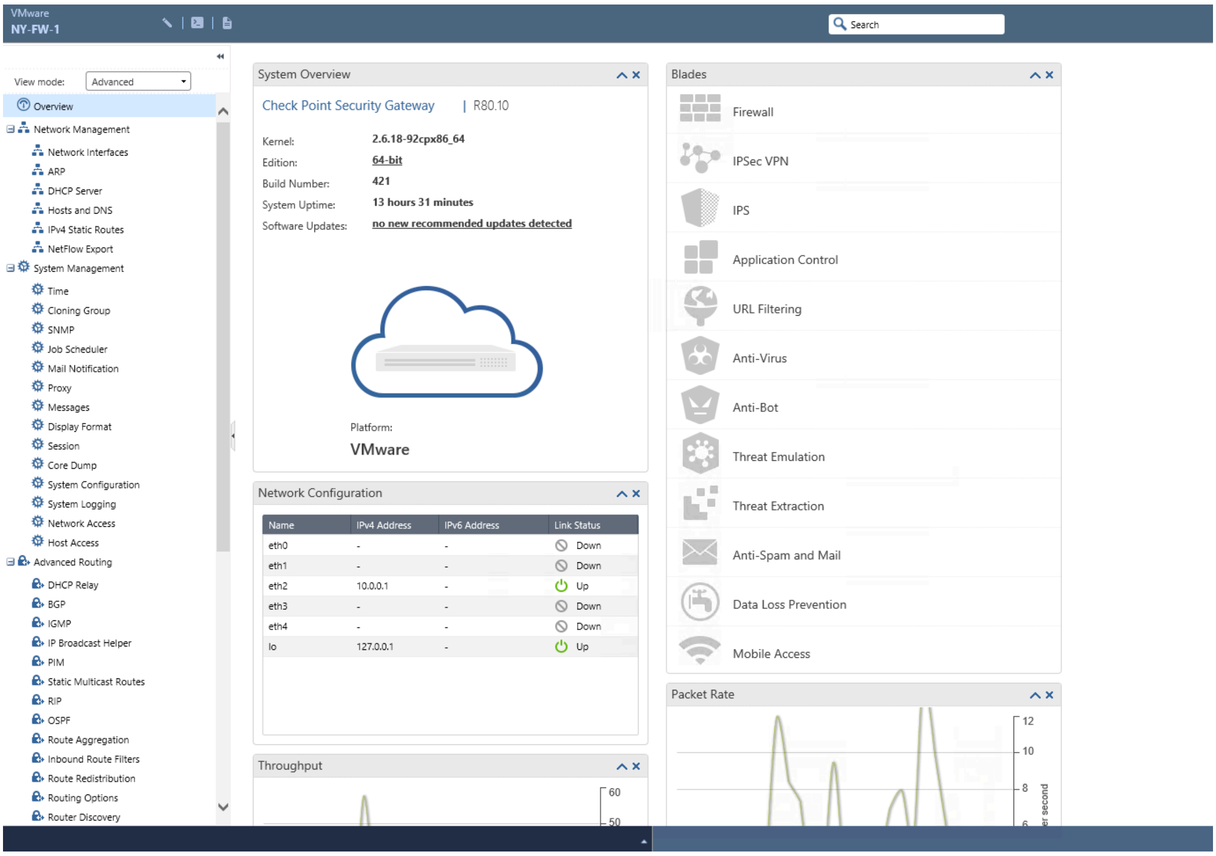
- Get familiar with Gaia Web UI

Gaia is the Check Point Operating System (OS), just like for Cisco Systems is the IOS, for Palo Alto Networks is the PAN-OS, for Fortinet is the Forti OS, etc.

Gaia can be configured through Command Line Interface (CLI) or via the Web User Interface through secure HTTP (HTTPS). The Web UI can be accessed through major browsers, like Safari, Internet Explorer, Google Chrome, etc.

In the previous Lab you have successfully run the First Time Wizard on the New York Firewall, which means that we can now access NY-FW-1 through Web UI. In this Lab we will go through a high level overview on Web UI on the NY-FW-1.

On the MGMT PC, open Internet Explorer (recommended browser for Windows users) and navigate to https://10.0.0.1. Enter the login credentials **admin/admin123** and you should be presented the NY-FW-1 Web UI.



Check Point Security Gateway | R80.10

Kernel: 2.6.18-92cpx86_64
Edition: 64-bit
Build Number: 421
System Uptime: 13 hours 31 minutes
Software Updates: no new recommended updates detected

Platform:
VMware

Network Configuration

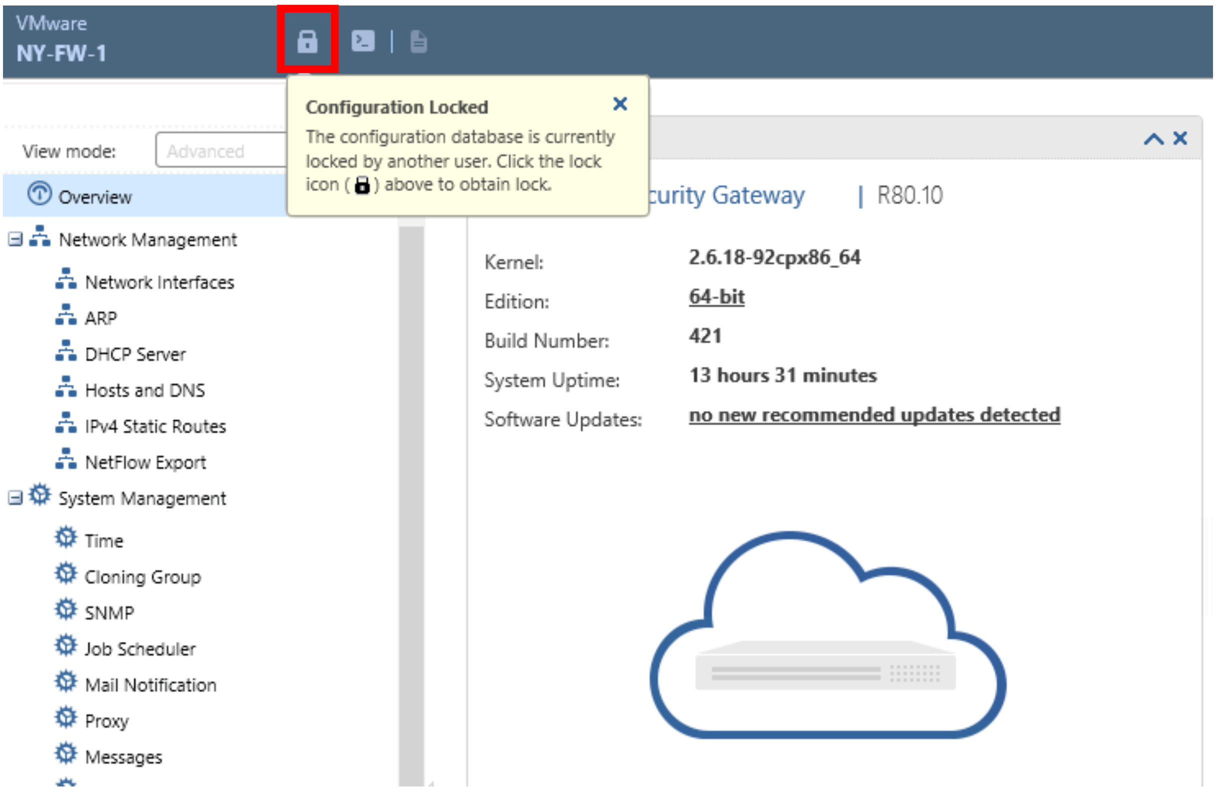
Name	IPv4 Address	IPv6 Address	Link Status
eth0	-	-	Down
eth1	-	-	Down
eth2	10.0.0.1	-	Up
eth3	-	-	Down
eth4	-	-	Down
lo	127.0.0.1	-	Up

First thing to note is that only one user has Read/Write permissions at any given time. Any other users, will have only Read Only rights, so will not be able to modify the Gaia OS configuration, but only view the configuration.

Let's take an example. User1 logs into Gaia and because no other user is logged in already, it will be granted Read/Write permissions. In Check Point world, this is called a **Configuration Lock**. When User2 logs into Gaia, because the Read/Write permissions have been granted to User1 (there is a user already logged in), it will be granted with only Read Only permissions. User2 has now two options, either continue the session with Read Only permissions or to **Override Configuration Lock**, which means User2 will be granted the Read/Write permissions (User2 will "take" the Read/Write permissions from User1). Please note that User1 will NOT be notified of this change and will continue to have Read Only (or view) permissions during this session.

How to obtain or **Override Configuration Lock** ?

If you are connecting to Gaia through Web UI, in the top-left corner of the page there is an icon button – Lock Icon that will help you override the configuration lock and obtain Read/Write permissions on the Gaia system.



Configuration Locked

The configuration database is currently locked by another user. Click the lock icon (🔒) above to obtain lock.

Kernel: 2.6.18-92cpx86_64

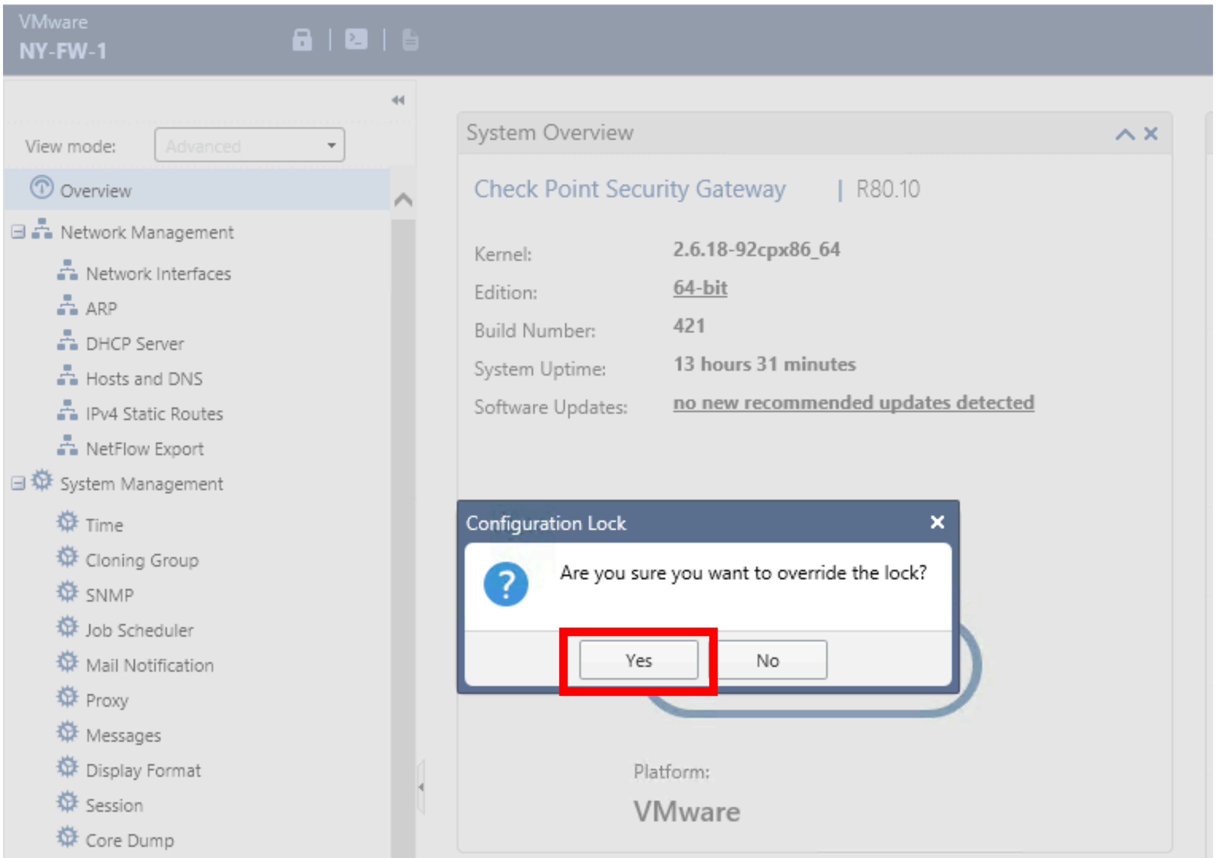
Edition: 64-bit

Build Number: 421

System Uptime: 13 hours 31 minutes

Software Updates: no new recommended updates detected

Click the **lock icon** and then confirm that you want to **override the lock.**

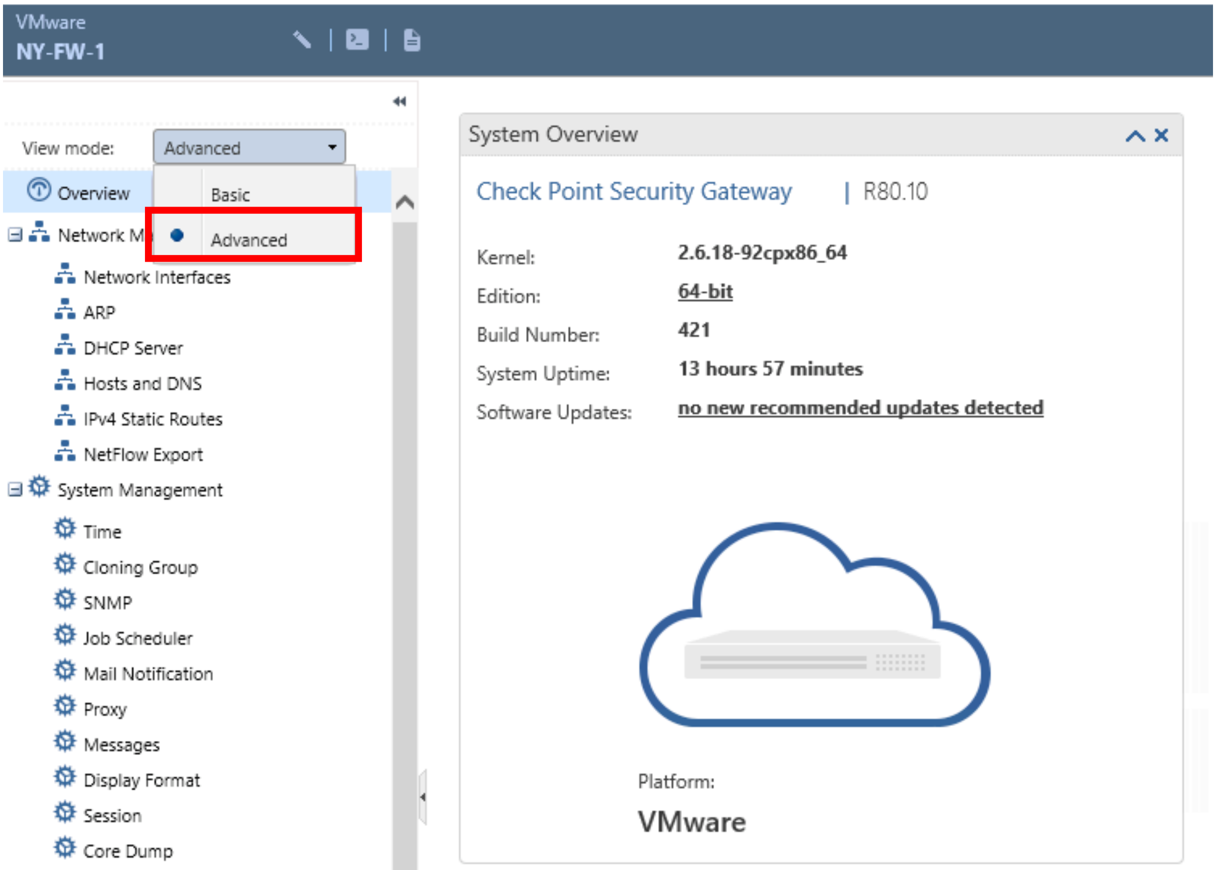


If you connected to Gaia through CLI, you will need to run a command, which will do the same thing, grant Read/Write permissions to the user. Please run **lock database override** if you need to override configuration lock and be granted with Read/Write permissions on the system.

```
This system is for authorized use only.
login: admin
Password:
CLINFR0771  Config lock is owned by admin. Use the command 'lock database override' to acquire the lock.
NY-FW-1> set user admin2 password
CLINFR0519  Configuration lock present. Can not execute this command. To acquire the lock use the command 'lock database override'.
NY-FW-1> lock database override
NY-FW-1> set user admin2 password
No existing User: Add user first using add user commands.
NY-FW-1>
```

I am try to create a new user, while I have Read Only rights. Other user has logged in before me and it has the Read Write(RW) rights. After I “request” the Read Write rights through **lock database override** command, I receive no error and I am able to run commands that need RW rights.

When you first log in the Web UI, you have the possibility to choose if you are going to see the complete page (Advanced) or a basic version with not all the options included (Basic). I advise you to choose the Advanced mode, as there are not so many options available and you should get comfortable, in time, with every option available in the GUI as well.



VMware
NY-FW-1

View mode: Advanced
- Basic
- ● Advanced

- Overview
- Network M
  - Network Interfaces
  - ARP
  - DHCP Server
  - Hosts and DNS
  - IPv4 Static Routes
  - NetFlow Export
- System Management
  - Time
  - Cloning Group
  - SNMP
  - Job Scheduler
  - Mail Notification
  - Proxy
  - Messages
  - Display Format
  - Session
  - Core Dump

System Overview

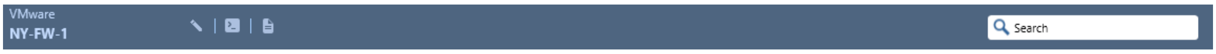
Check Point Security Gateway | R80.10

Kernel:	2.6.18-92cpx86_64
Edition:	64-bit
Build Number:	421
System Uptime:	13 hours 57 minutes
Software Updates:	no new recommended updates detected

Platform:
VMware

Top Toolbar

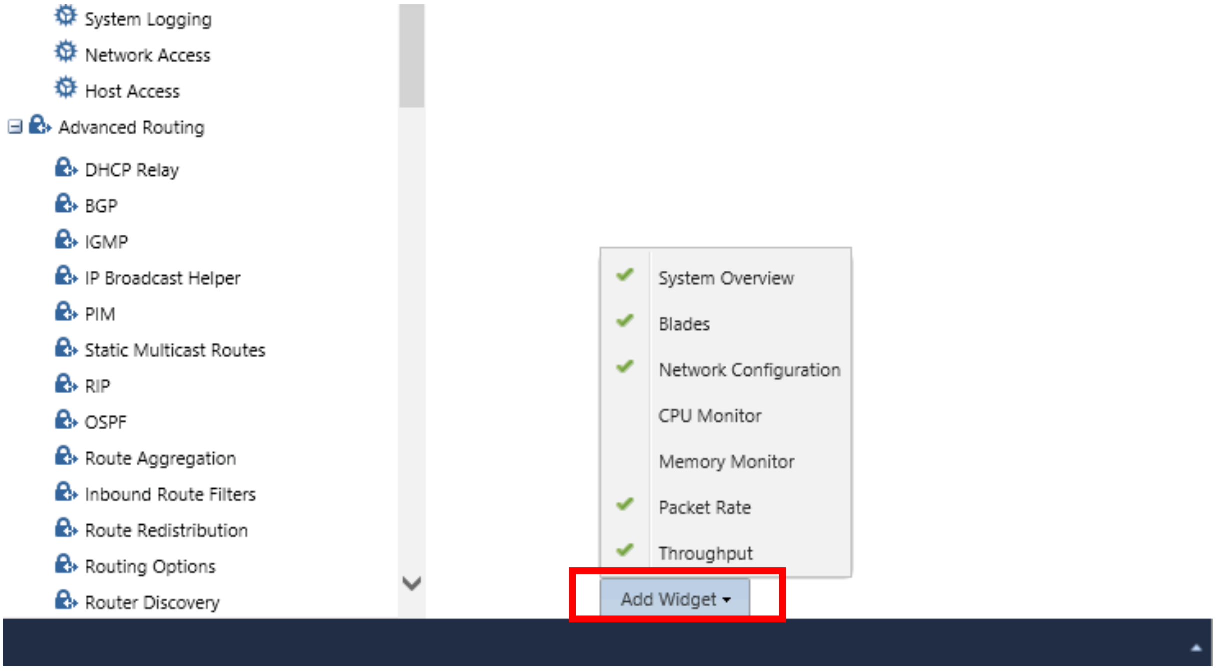
At the top of the page you can see a toolbar, that includes the following:
- Release/Override configuration lock icon
- Terminal icon – opens a shell for Gaia CLI configuration
- Open scratchpad – opens a Microsoft Word like scratchpad to take notes if you want to
- Search bar – search specific menus or options that are available on the Gaia OS



VMware
NY-FW-1

Overview page

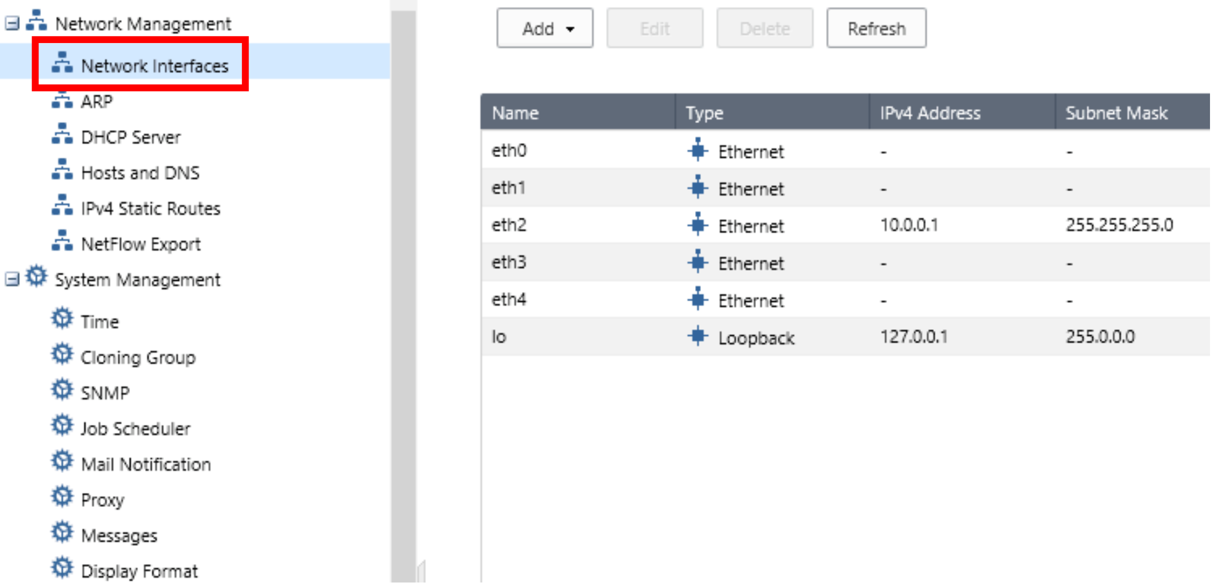
The **Overview** page provides general information about the system in a fast way through widgets. You can customize what widgets to be available on the page scrolling down the Overview page and click on **Add Widget** button. Once you decide what are the relevant widgets for you, you can rearrange them in the way you want, simply in a drag-and-drop manner.



1. **Network Management Menu**

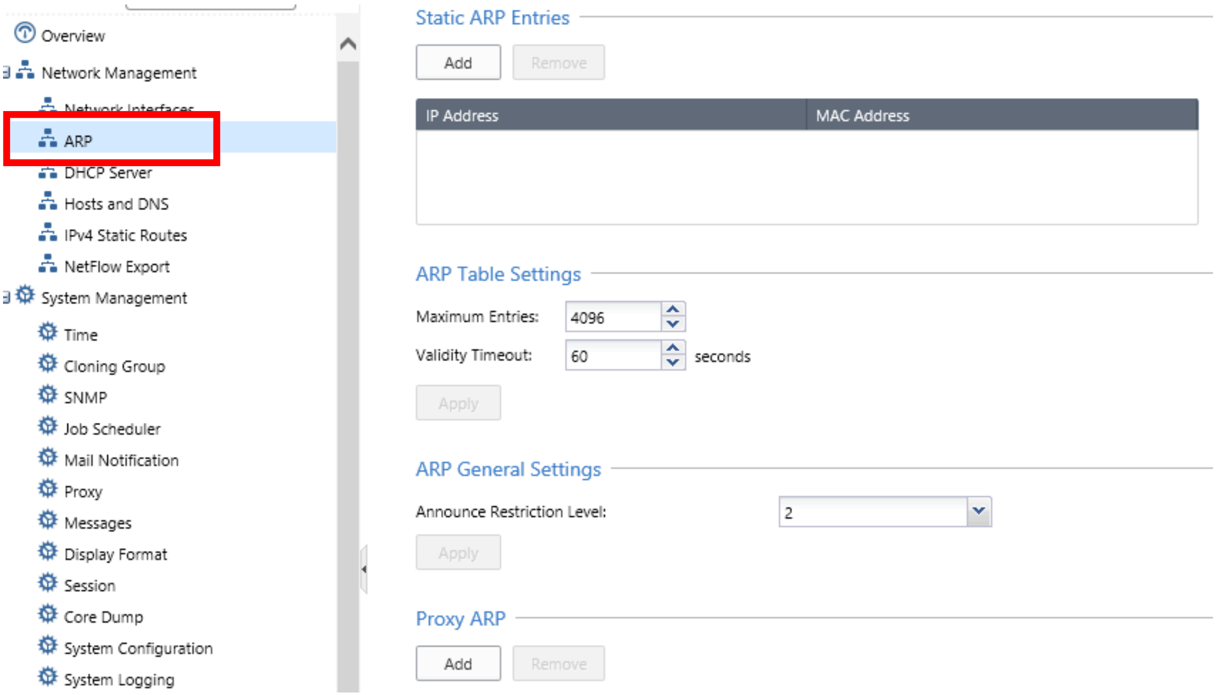
The Network Management menu contains very important configuration sub-menus that you must be aware of. As you ca see in the Web UI, the available sub-menus are:
- Network Interfaces
- ARP
- DHCP Server
- Hosts and DNS
- IPv4 Static Routes
- Netflow Export

In the **Network Interfaces** sub-menu, you configure the IP addresses of your Check Point appliance and also define what is the Management interface that you will be using.



Name	Type	IPv4 Address	Subnet Mask
eth0	Ethernet	-	-
eth1	Ethernet	-	-
eth2	Ethernet	10.0.0.1	255.255.255.0
eth3	Ethernet	-	-
eth4	Ethernet	-	-
lo	Loopback	127.0.0.1	255.0.0.0

In **ARP** sub-menu you can define static ARP entries, some general ARP settings and also define Proxy ARP.



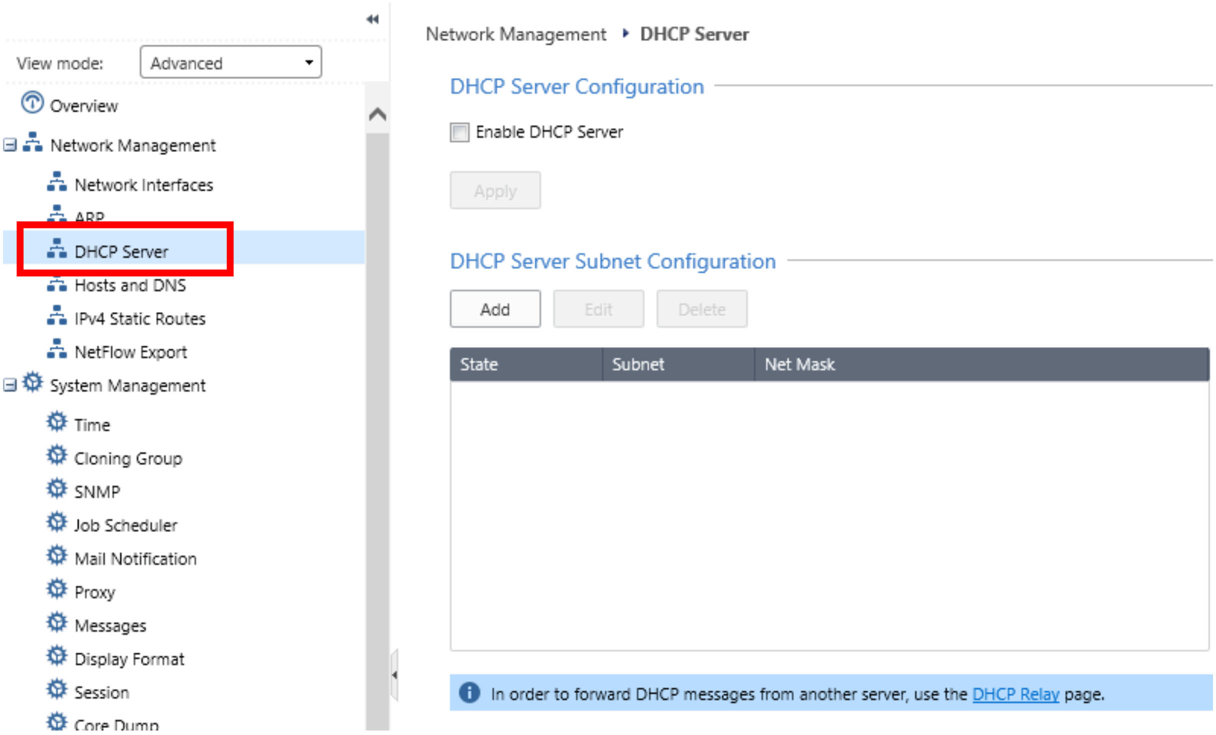
IP Address	MAC Address

Maximum Entries: 4096

Validity Timeout: 60 seconds

Announce Restriction Level: 2

In **DHCP Server** sub-menu you can enable your Gaia appliance in order to run as a DHCP server and also, obviously, define DHCP server subnets to be used.



Network Management ▸ DHCP Server

DHCP Server Configuration

□ Enable DHCP Server

Apply

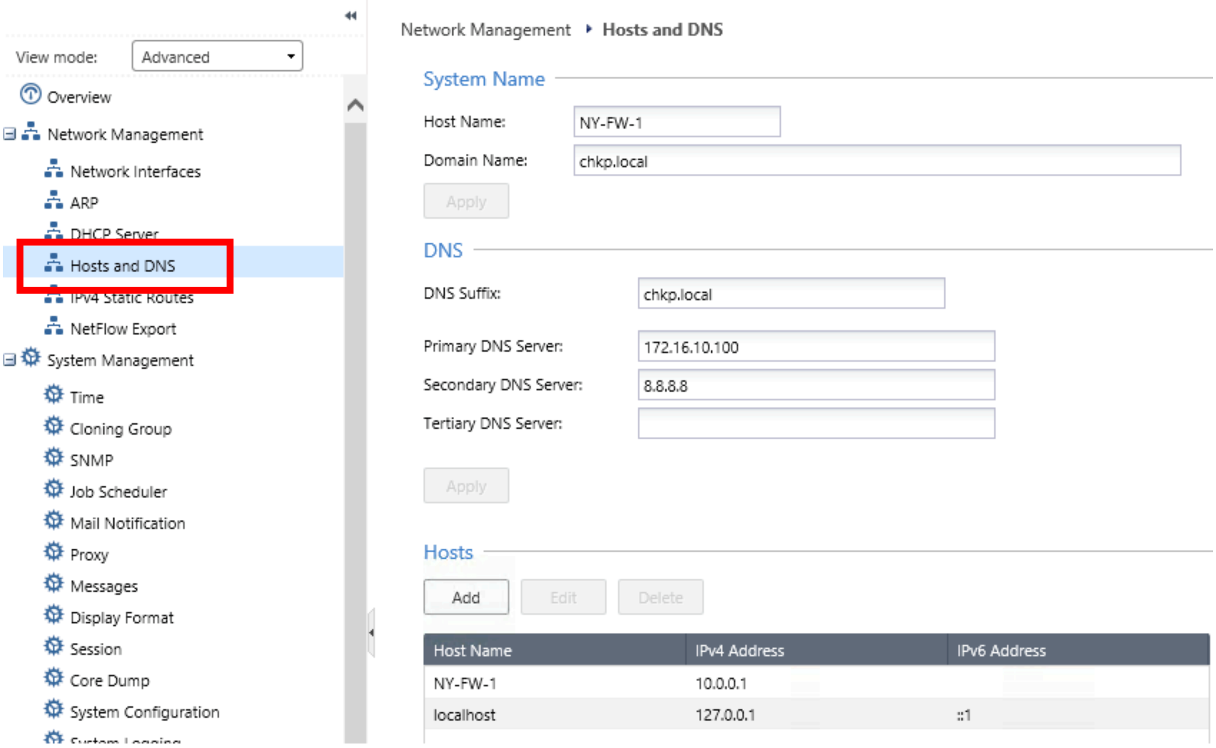
DHCP Server Subnet Configuration

Add | Edit | Delete

State	Subnet	Net Mask

In order to forward DHCP messages from another server, use the DHCP Relay page.

In **Hosts and DNS** sub-menu, you can define DNS settings and create static DNS mappings.



Network Management ▸ Hosts and DNS

System Name

Host Name: NY-FW-1

Domain Name: chkp.local

Apply

DNS

DNS Suffix: chkp.local

Primary DNS Server: 172.16.10.100

Secondary DNS Server: 8.8.8.8

Tertiary DNS Server:

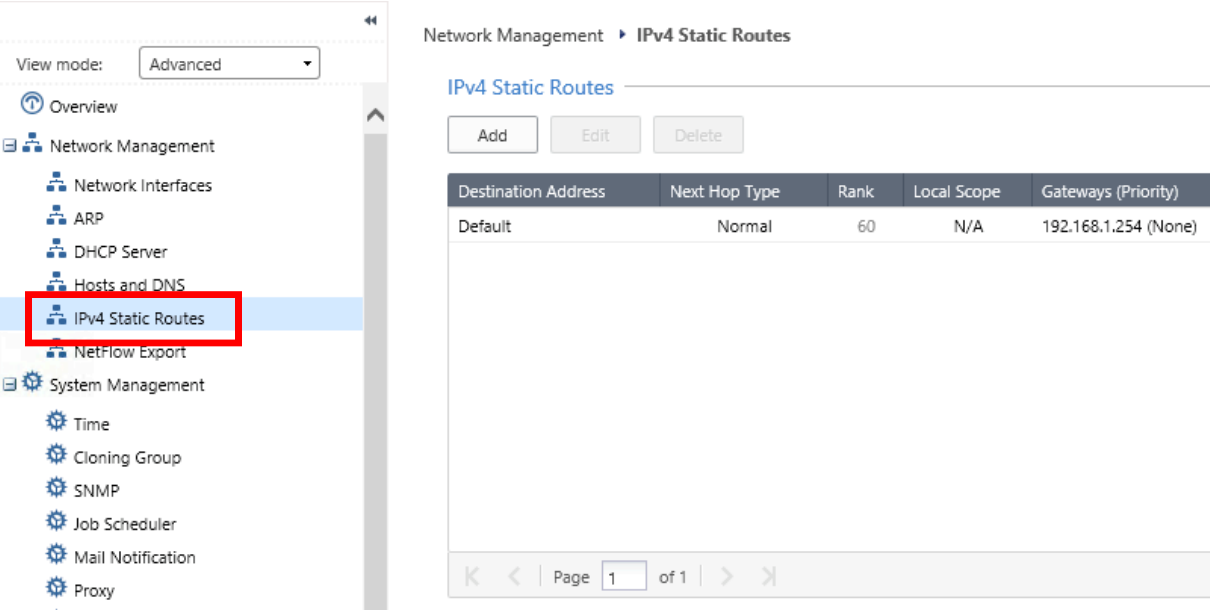
Apply

Hosts

Add | Edit | Delete

Host Name	IPv4 Address	IPv6 Address
NY-FW-1	10.0.0.1	
localhost	127.0.0.1	::1

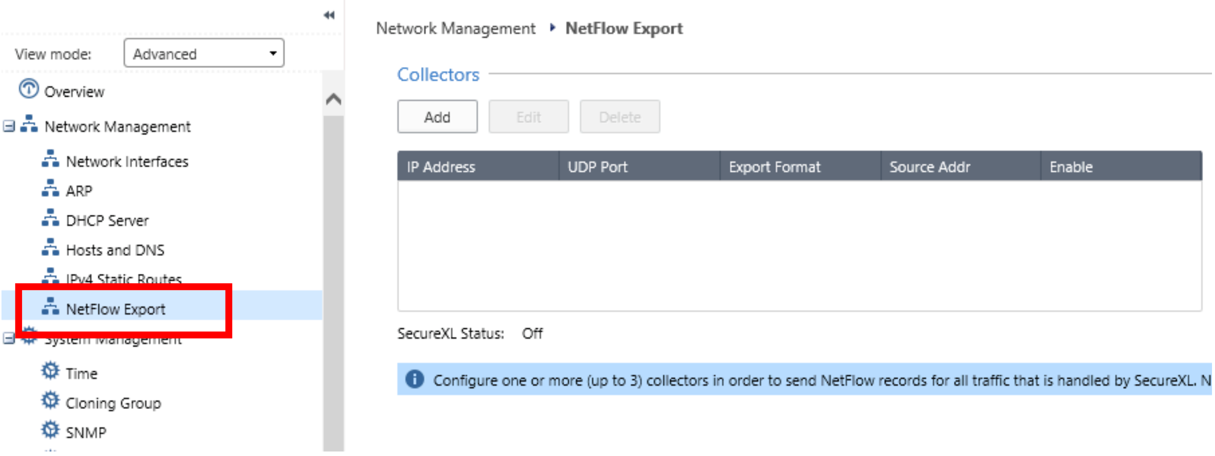
In **IPv4 Static Routes** sub-menu, as you may probably imagine, you can define static routing.



IPv4 Static Routes

Destination Address	Next Hop Type	Rank	Local Scope	Gateways (Priority)
Default	Normal	60	N/A	192.168.1.254 (None)

The last sub-menu available in Network Management category is **Netflow Export**, here you can define netflow collectors for receiving traffic from Gaia appliances.



Collectors

IP Address	UDP Port	Export Format	Source Addr	Enable

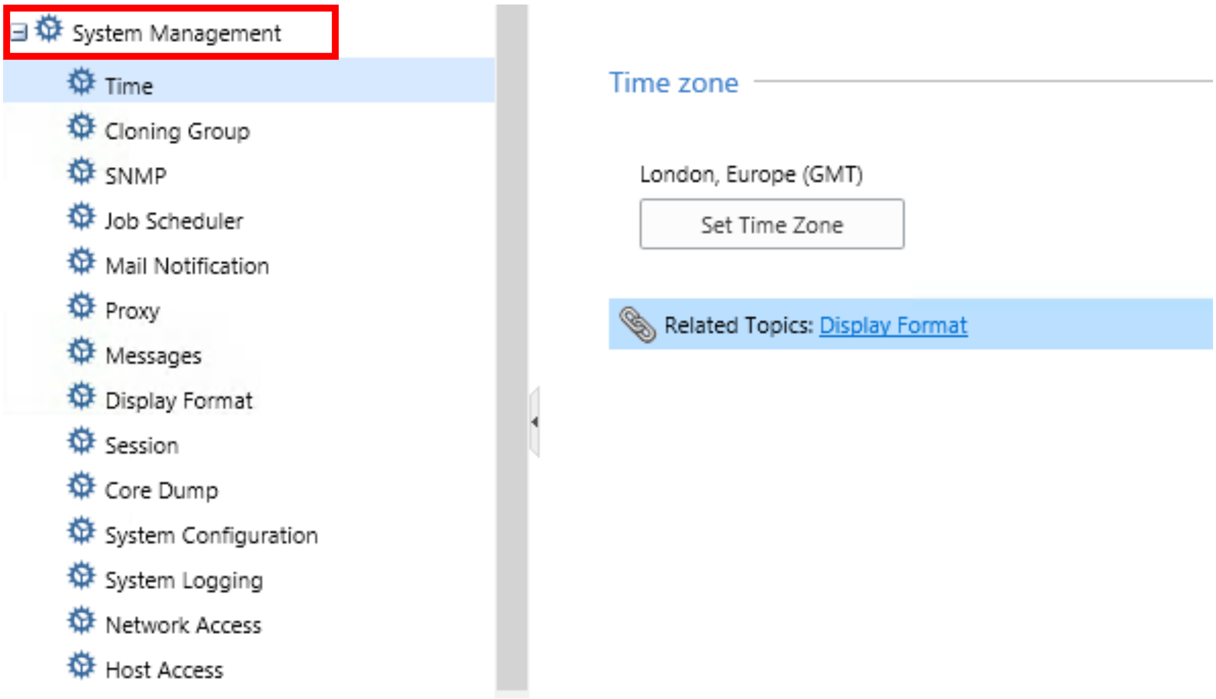
SecureXL Status: Off

Configure one or more (up to 3) collectors in order to send NetFlow records for all traffic that is handled by SecureXL. N

The second category available in the menu is :

2. System Management Menu

I will go through some of the most important sub-menus, but I highly advise you that you go through all of them, at least to see and understand that different configuration options are available. This way you will get more familiar with the Web UI and feel more comfortable when you need to work with it.



Time - set time, date and timezone on your appliance; this is an important topic, because you want your logs to have correct timestamps if you need to investigate some events, at some point. Keeping your infrastructure time synced is a recommended practice and I advise you to follow along

SNMP – set SNMPv2 and v3 communities and define traps

Mail Notification – define mail server and an email address to send notifications to

System Logging – logging related configurations; define external logging server, different than SMS

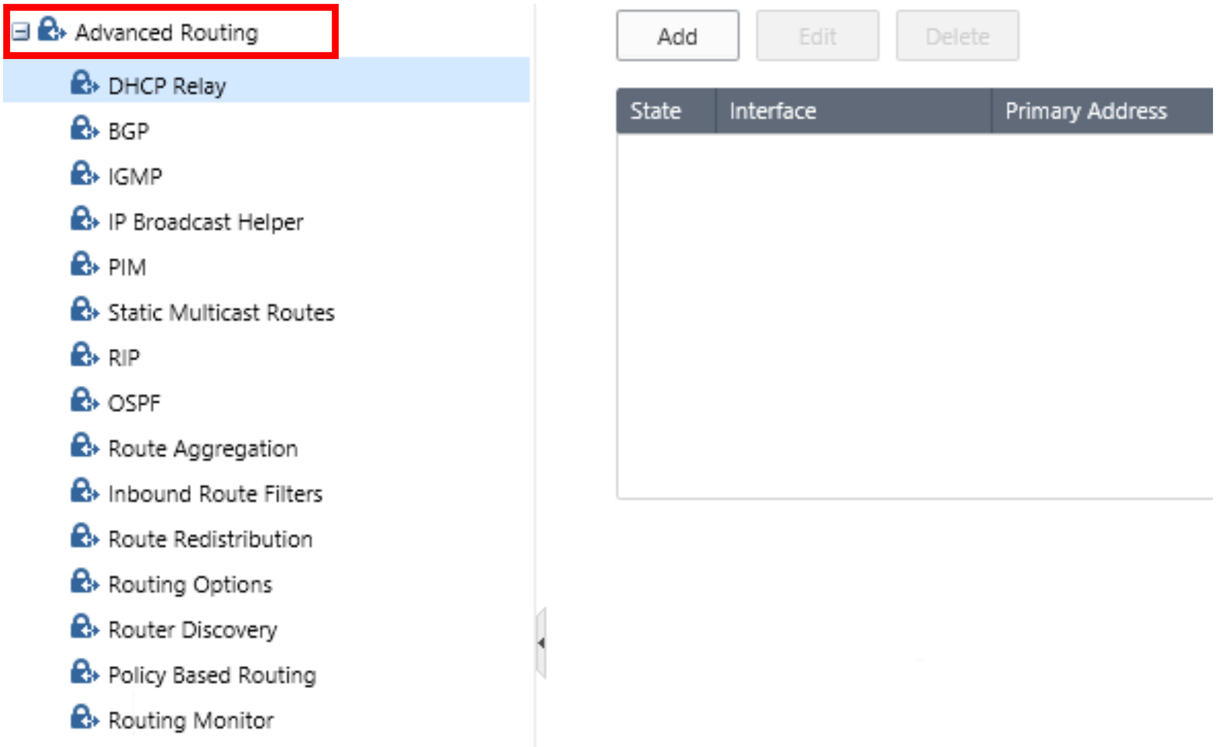
Host Access – define who is allowed to connect to the Gaia appliance

3. Advanced Routing Menu

The Advanced Routing Menu includes all routing capabilities of the Check Point Gaia appliance. As you could see earlier, static routing is covered in a different sub-menu(Network Management -> IPv4 Static Routes), this menu covers only dynamic routing.

In a nutshell, this menu covers advanced routing capabilities, DHCP relay, multicast routing (IGMP, PIM, static multicast routing), route aggregation and redistribution, routing filters, policy-based routing and routing monitoring.

We may explore some of these functionalities as we progress through the course, for now it is sufficient you know that these functionalities exist.

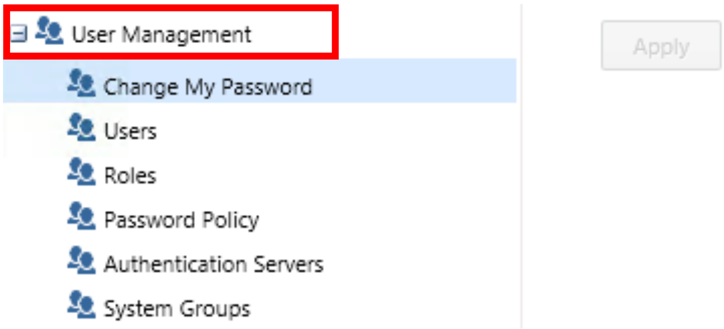


4. User Management Menu

The functionalities that are made available in this menu are very important if you want or you need to segregate duties in the organization. For example, the Network Operations Center (NOC) is divided into two levels. Level 1 is responsible for monitoring, opening tickets and easy troubleshooting and Level 2 is the Expert level where only complicated issues are treated.

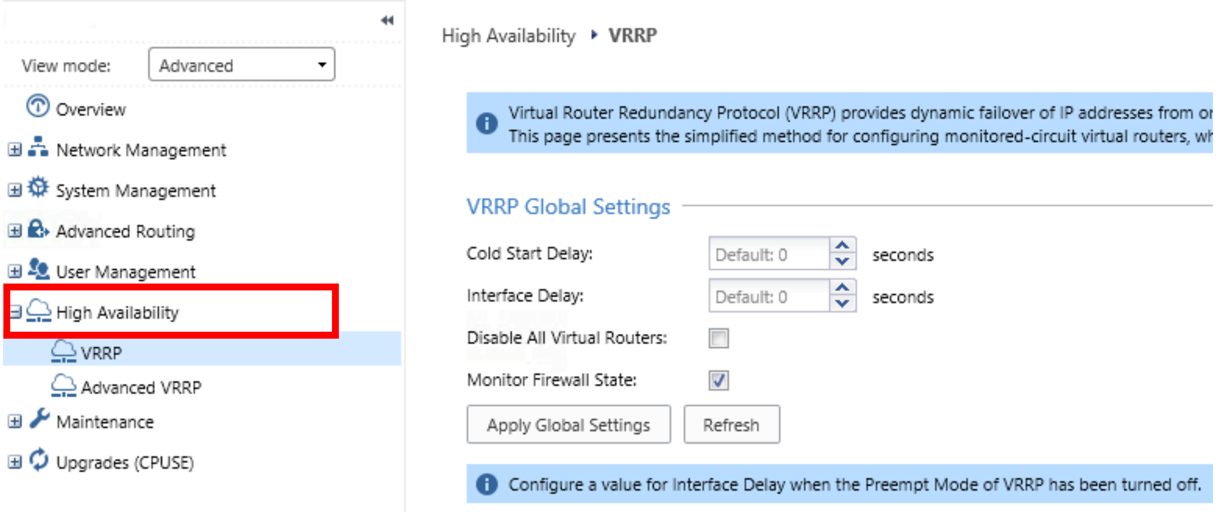
You may want, for example, to create users for Level 1 with only Read Only rights on the Check Point gateways and FULL admin rights for Level 2 department. This is something that you can accomplish through custom users and roles and we will have a separate Lab dedicated to this topic.

Let’s have a short overview of what’s included in this menu. You can change your password here, create users, create roles, change or customize the default password policy (for example, password complexity -> password should contain at least two character types, letters and numbers), define external authentication servers (RADIUS, TACACS+) and define system groups.



5. High Availability Menu

This menu includes two sub-menus, VRRP and Advanced VRRP, and here is where you can implement VRRP related configuration for high availability purposes (a secondary gateway can take over if the primary fails).
VRRP is an open-standard and it accomplishes the same thing as HSRP, for example, which is Cisco proprietary.



Virtual Router Redundancy Protocol (VRRP) provides dynamic failover of IP addresses from o
This page presents the simplified method for configuring monitored-circuit virtual routers, wh

VRRP Global Settings

Cold Start Delay: Default: 0 seconds

Interface Delay: Default: 0 seconds

Disable All Virtual Routers: □

Monitor Firewall State: ☑

Configure a value for Interface Delay when the Preempt Mode of VRRP has been turned off.

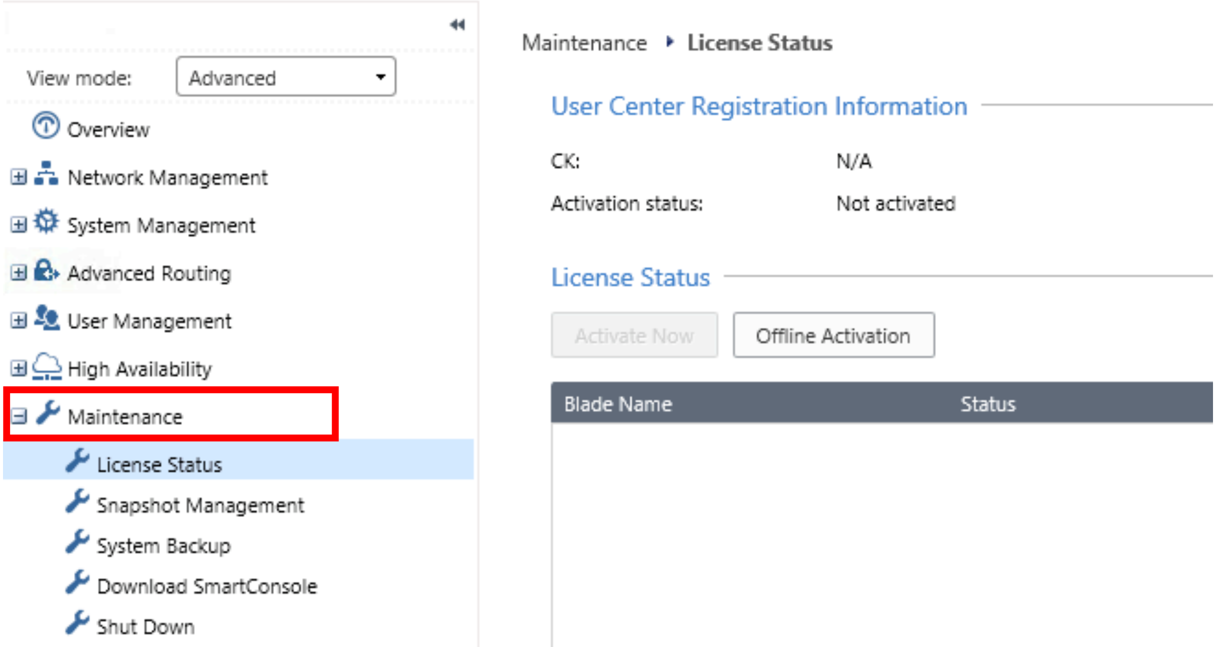
6. Maintenance Menu

In the maintenance menu you can check the licensing status or do the actual licensing activation of the Check Point Gateway.

Another topic that needs your attention is backup. Two types of backup are available: System Backup – which will backup the gateway configuration and Snapshot Management – which will backup the entire gateway – operating system image plus the configuration.

Download **SmartConsole** is the sub-menu you will access when downloading and installing the management application and this will be covered in a future lab.

The last sub-menu, **Shut Down**, provides the ability to shut down or restart the appliance in the correct way, so not by powering off the appliance from the power button.



User Center Registration Information

CK: N/A

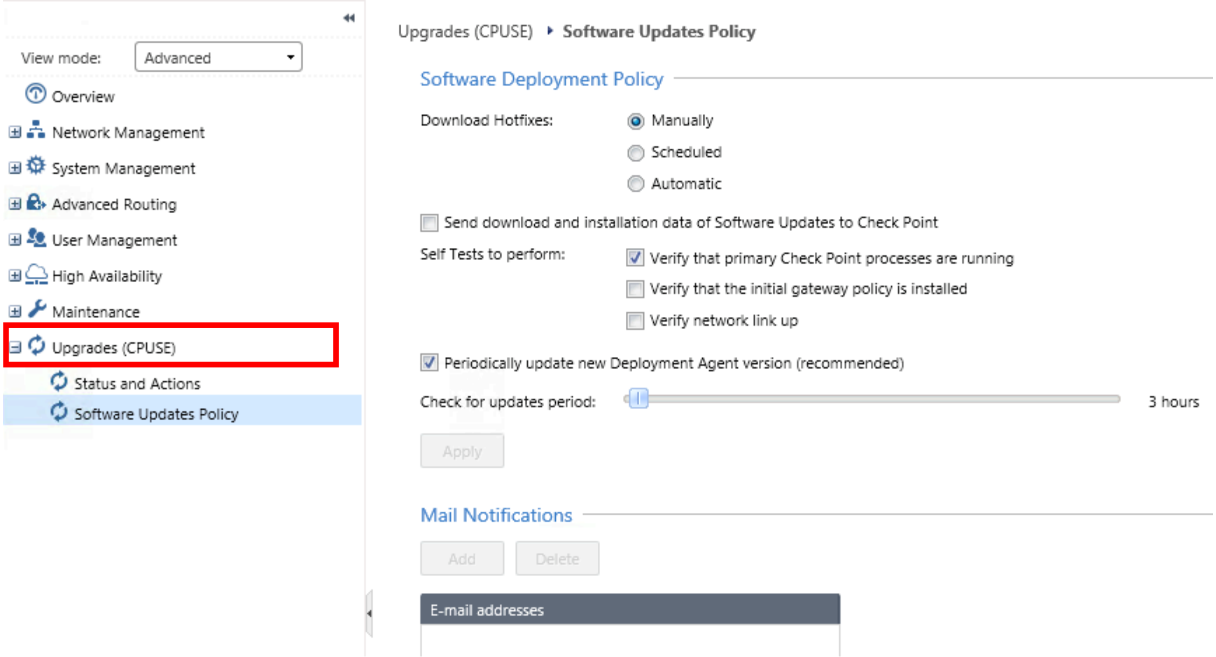
Activation status: Not activated

License Status

Blade Name	Status

7. Upgrades (CPUSE)

The last menu covers the software updates and update policy related to your Check Point appliance.



Software Deployment Policy

Download Hotfixes: ● Manually ○ Scheduled ○ Automatic

□ Send download and installation data of Software Updates to Check Point

Self Tests to perform: ☑ Verify that primary Check Point processes are running

□ Verify that the initial gateway policy is installed

□ Verify network link up

☑ Periodically update new Deployment Agent version (recommended)

Check for updates period: 3 hours

Mail Notifications

E-mail addresses

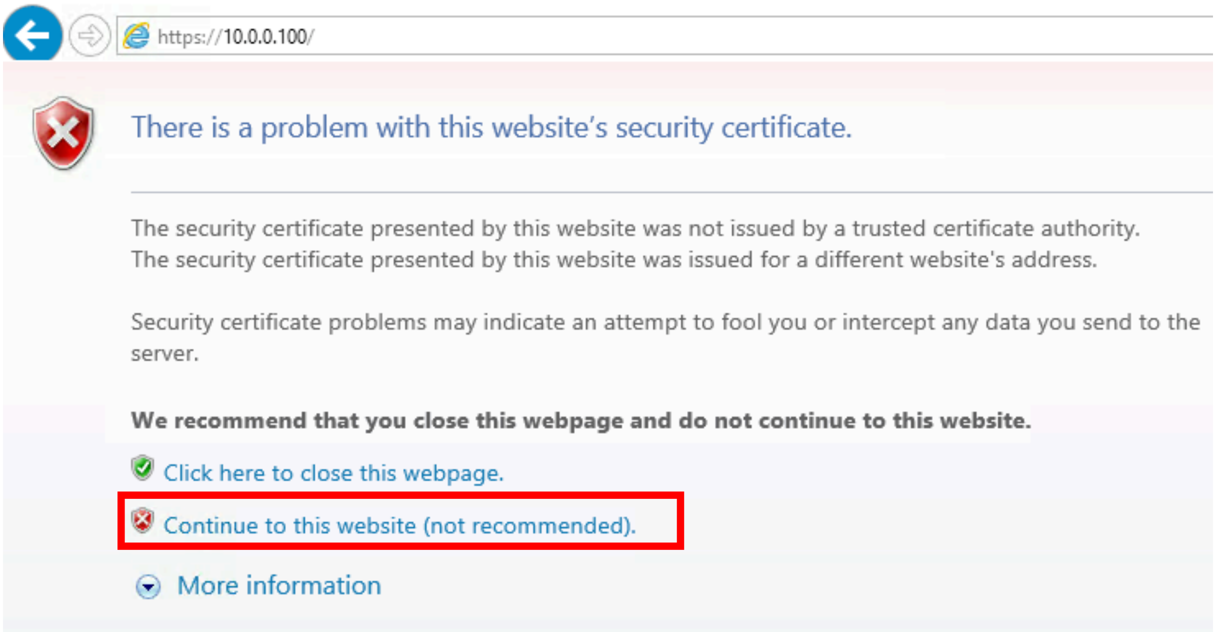
8.0 Lab: First Time Wizard on NY-SMS-1

Lab Objectives

- Run the First Time Wizard on NY-SMS-1 through WEB UI

Open a browser, classic Internet Explorer (not Edge), on MGMT PC and navigate to : ***https://10.0.0.100***

You will receive a warning related to the Digital Certificate the NY-SMS-1 is presenting when connecting through secure HTTP (HTTPS).



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

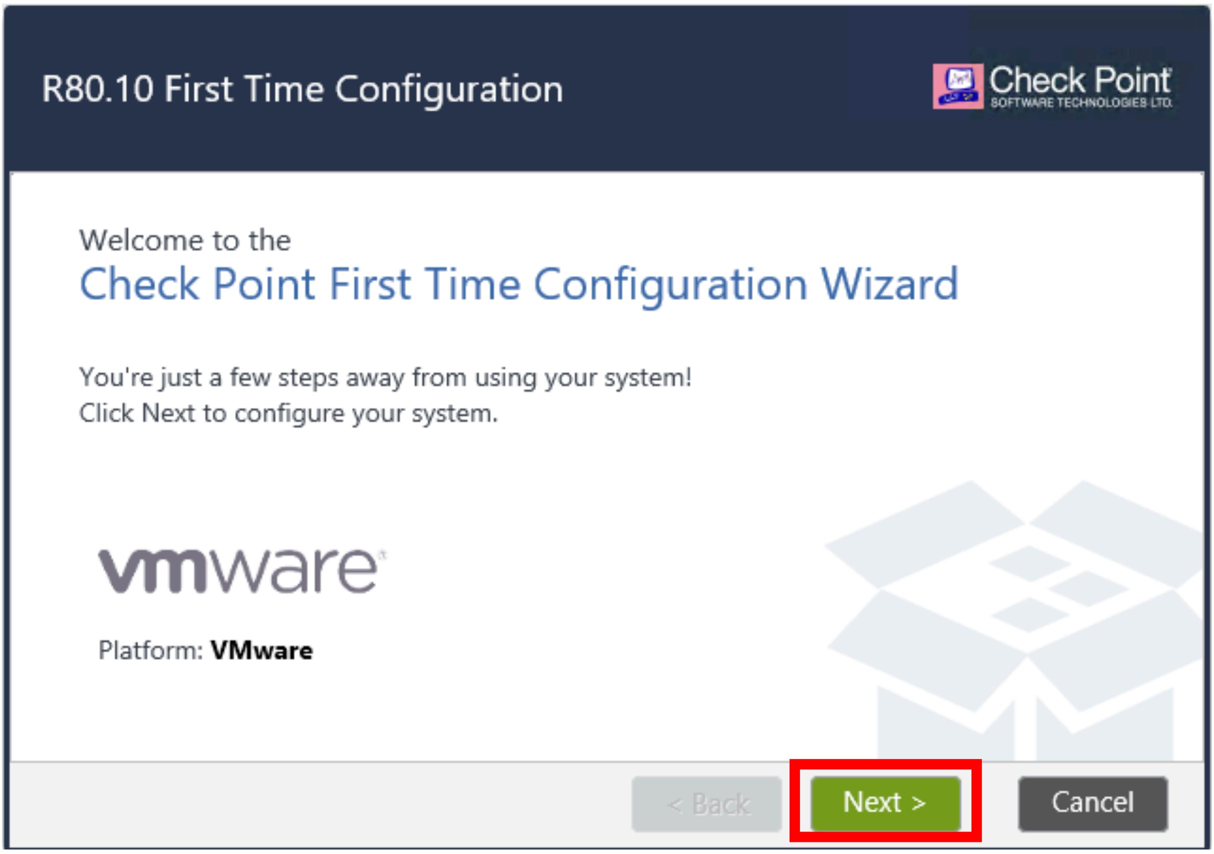
More information

Click on ***"Continue to this site (not recommended)"*** and you will be directed to Gaia Portal R80.10. Please enter login credentials as defined in the previous configuration steps. As mentioned previously, I am using ***admin/admin123*** as my username and password authentication pair.

Enter username and password and hit **Enter.**

Let's start the Check Point First Time Wizard for New York HQ Security Management Server.

Click **Next** to begin.



R80.10 First Time Configuration

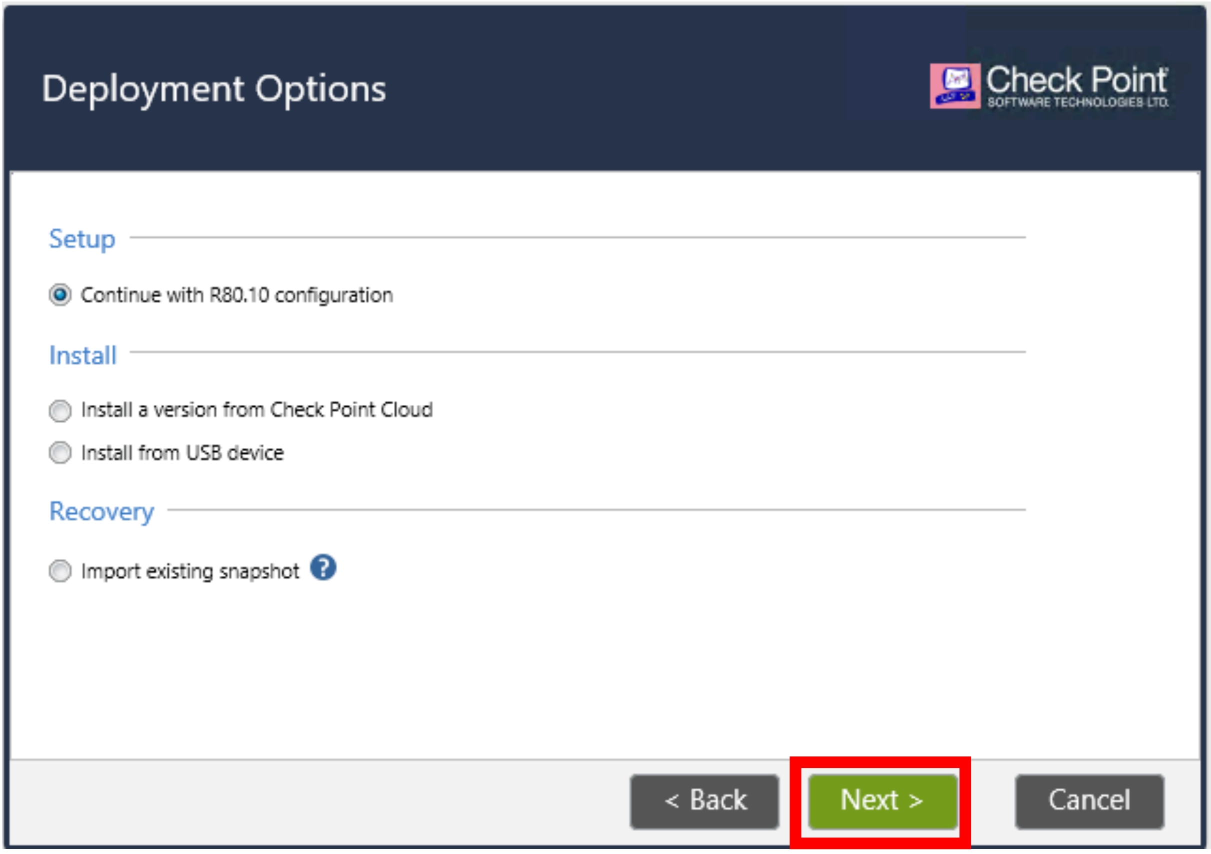
Welcome to the

Check Point First Time Configuration Wizard

You're just a few steps away from using your system!
Click Next to configure your system.

Platform: **VMware**

1. Leave the first option selected ***"Continue with R80.10 configuration"*** and click **Next** to continue.



Deployment Options

Setup

● Continue with R80.10 configuration

Install

○ Install a version from Check Point Cloud

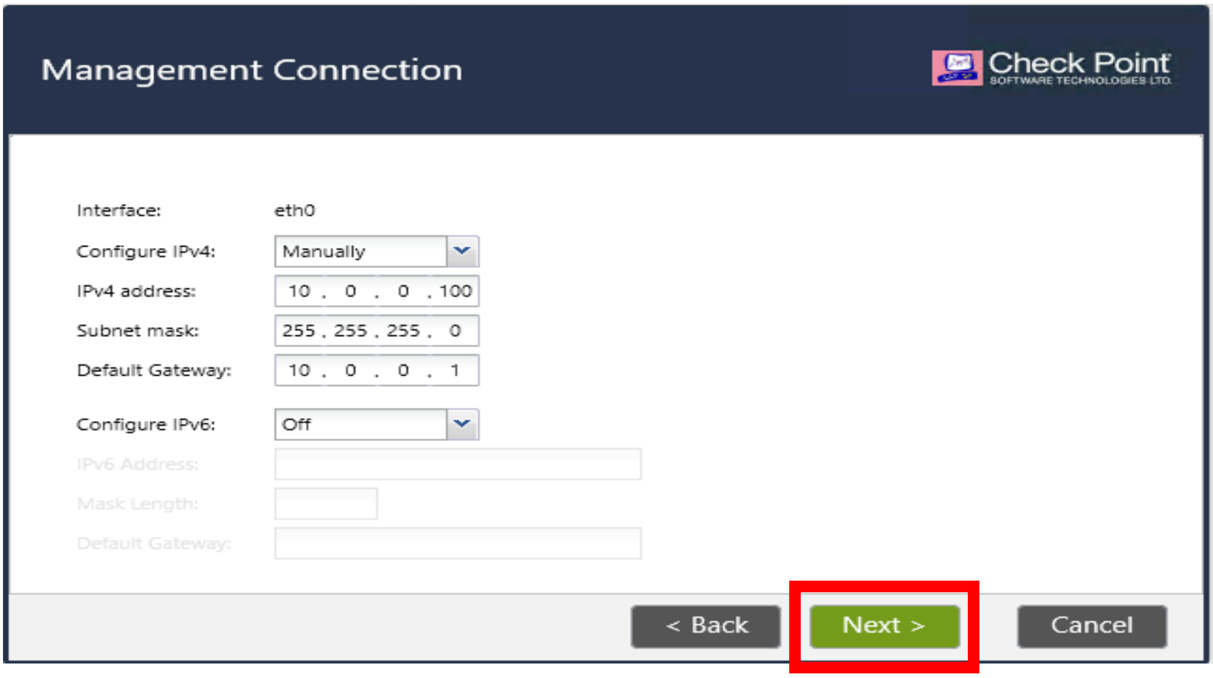
○ Install from USB device

Recovery

○ Import existing snapshot

2. Management connection

Confirm management port and IP addressing information. Remember that we have entered this information when installing Gaia OS on SMS, in a previous lab. Do not modify anything, click **Next** to continue.



Management Connection

Interface: eth0

Configure IPv4: Manually

IPv4 address: 10 . 0 . 0 . 100

Subnet mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 0 . 0 . 1

Configure IPv6: Off

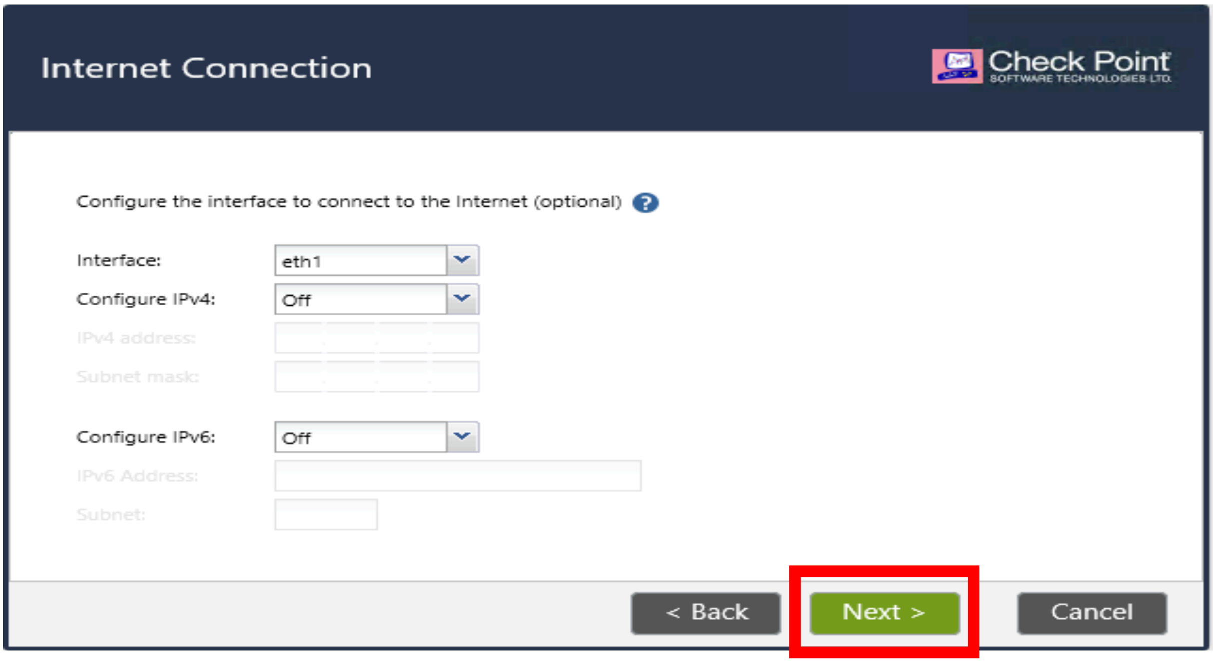
IPv6 Address:

Mask Length:

Default Gateway:

3. Internet Connection.

No need to change anything here. Anyway, we are using a single port on the SMS server and connection to Internet will use the same default gateway as the Management PC : 10.0.0.1. Do not modify anything, just click **Next** to continue.



Internet Connection

Configure the interface to connect to the Internet (optional)

Interface: eth1

Configure IPv4: Off

IPv4 address:

Subnet mask:

Configure IPv6: Off

IPv6 Address:

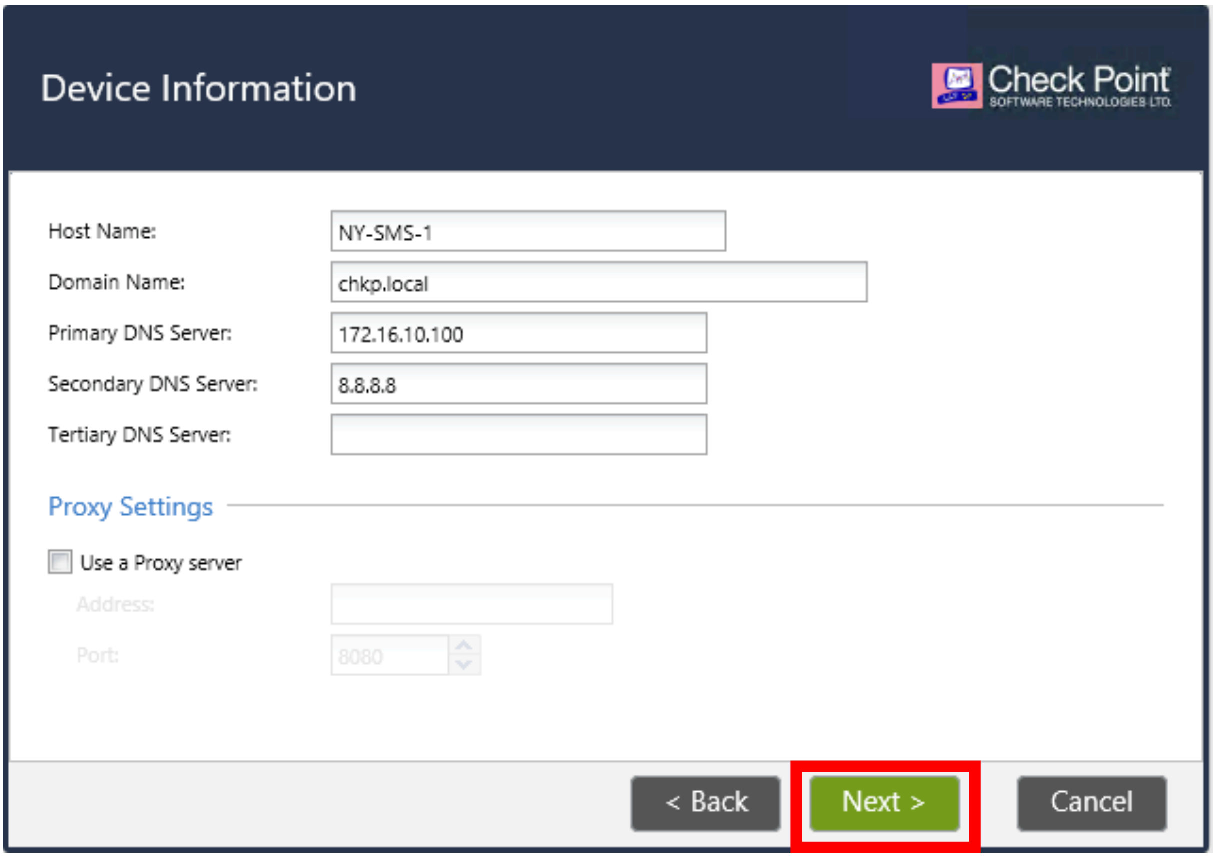
Subnet:

4. Device Information

Please fill in the necessary details as per below table.

Parameter	Value
Host Name	NY-SMS-1
Domain Name	chkp.local
Primary DNS Server	172.16.10.100
Secondary DNS Server	8.8.8.8
Tertiary DNS	<Leave Blank>

Click **Next** to continue.



Device Information

Host Name: NY-SMS-1

Domain Name: chkp.local

Primary DNS Server: 172.16.10.100

Secondary DNS Server: 8.8.8.8

Tertiary DNS Server:

Proxy Settings

□ Use a Proxy server

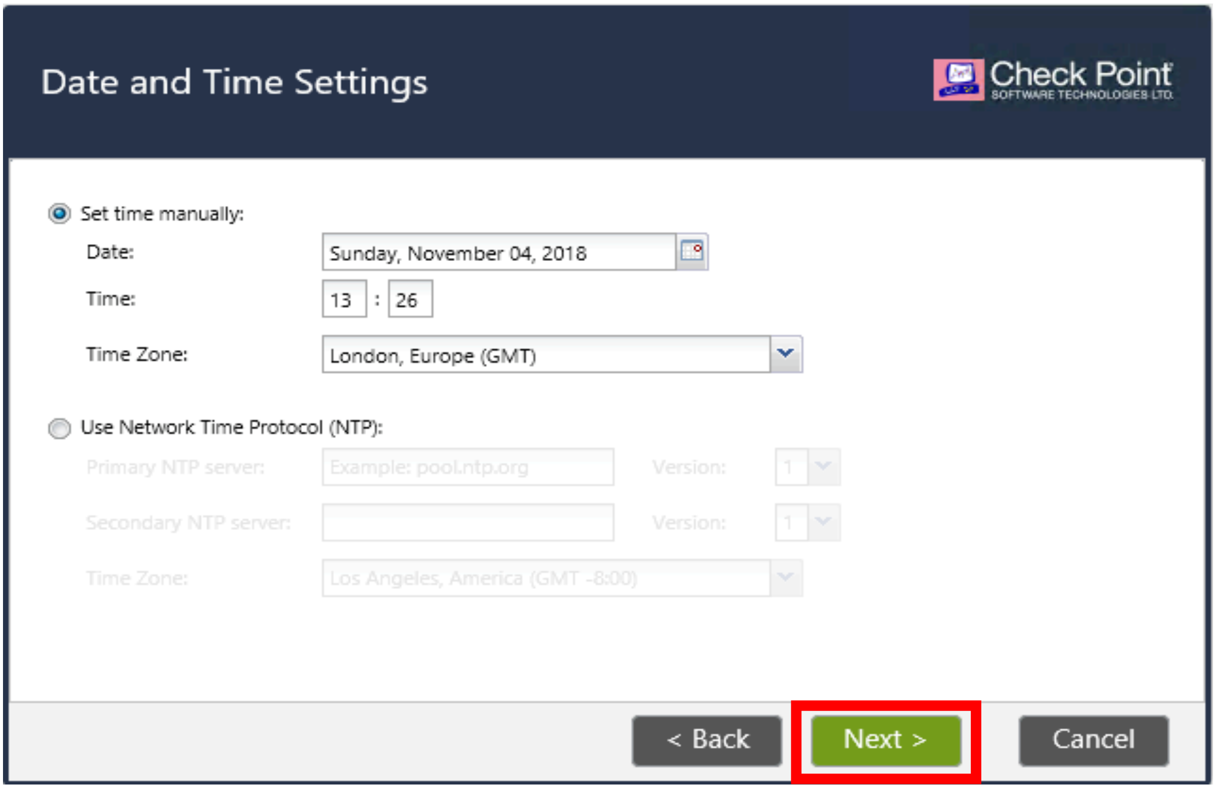
Address:

Port: 8080

5. Date and Time settings

Configure Date and Time settings according to your location.

Click **Next** to continue.



Date and Time Settings

● Set time manually:

Date: Sunday, November 04, 2018

Time: 13 : 26

Time Zone: London, Europe (GMT)

○ Use Network Time Protocol (NTP):

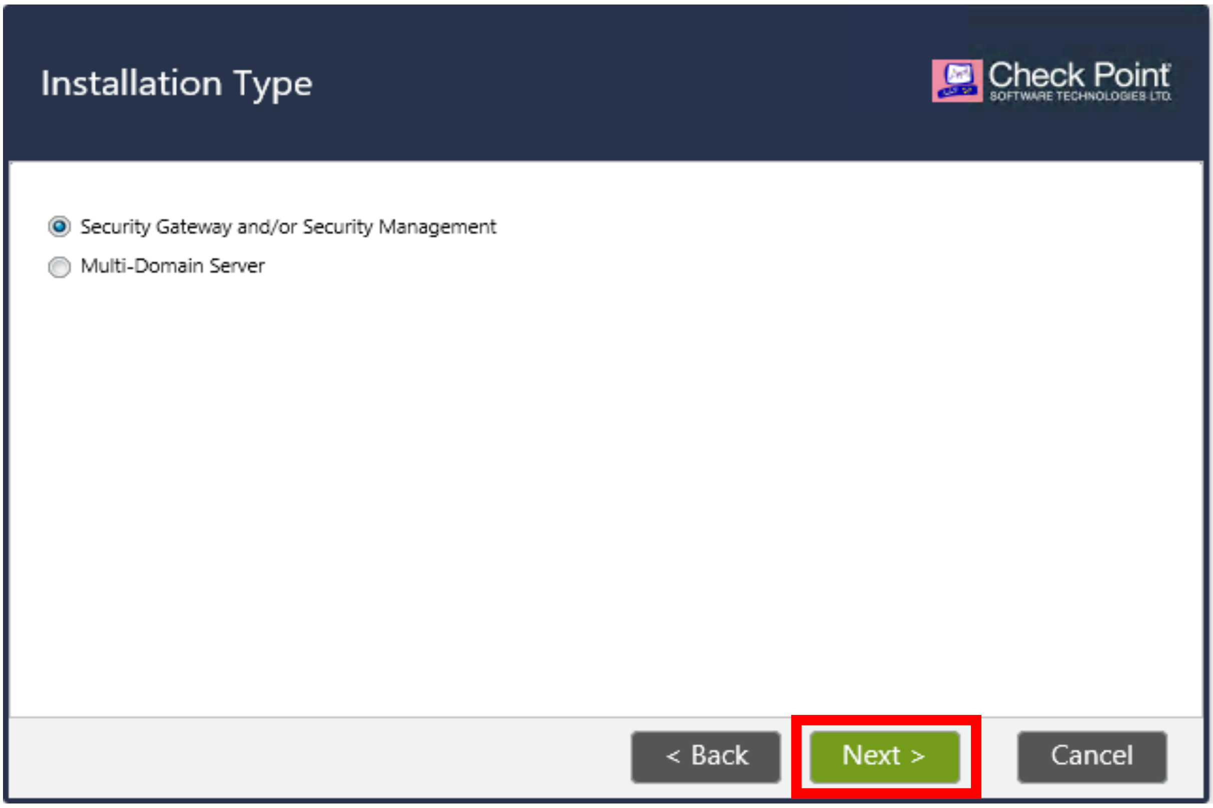
Primary NTP server: Example: pool.ntp.org Version: 1

Secondary NTP server: Version: 1

Time Zone: Los Angeles, America (GMT -8:00)

6. Installation type

This is a Security Management Server installation, so leave the first option selected and click **Next** to continue.



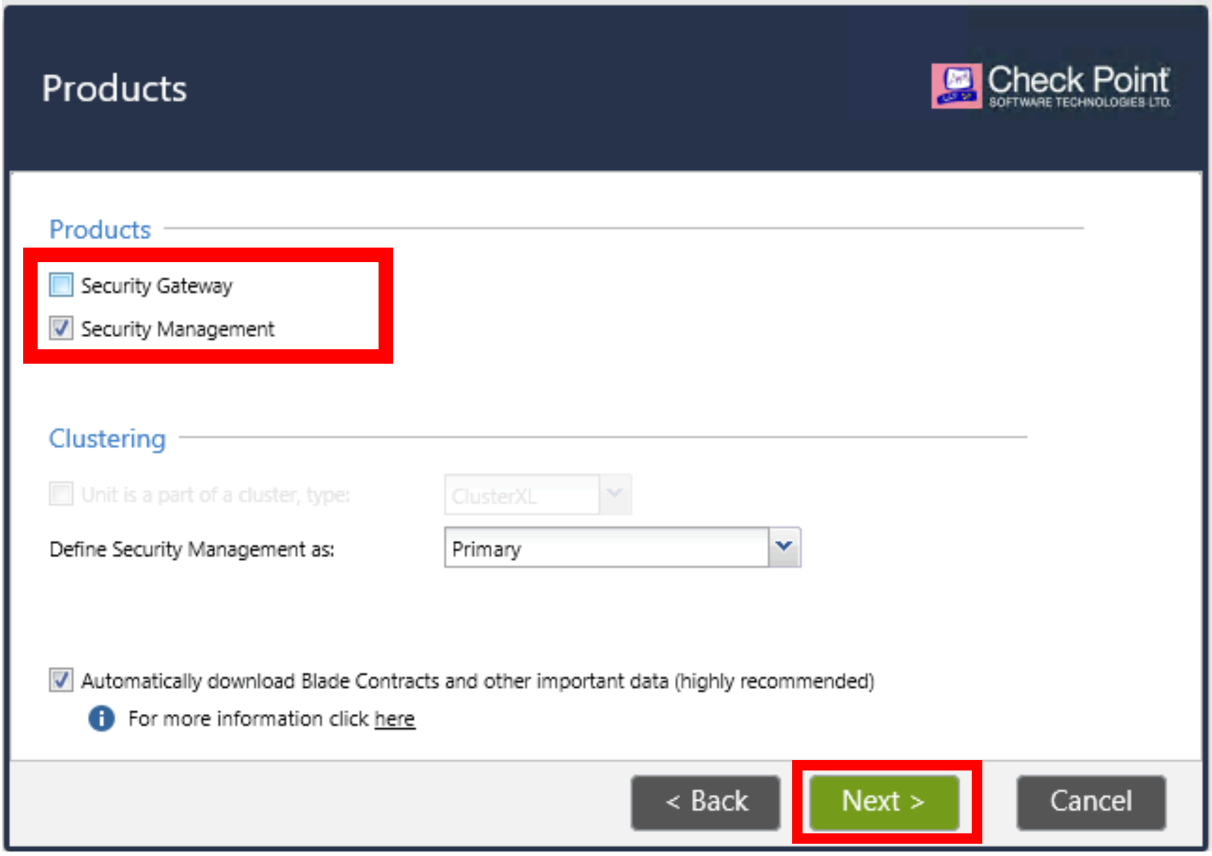
Installation Type

● Security Gateway and/or Security Management

○ Multi-Domain Server

7. Products

This is a critical step during the wizard. In the lab topology we can see that we are NOT running in standalone mode, we are running in distributed mode. Security Gateway and Management Server are running on different machines. In this case, please **deselect** the first option **Security Gateway** and click **Next** to continue.



Products

Products

□ Security Gateway

☑ Security Management

Clustering

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

Define Security Management as: Primary

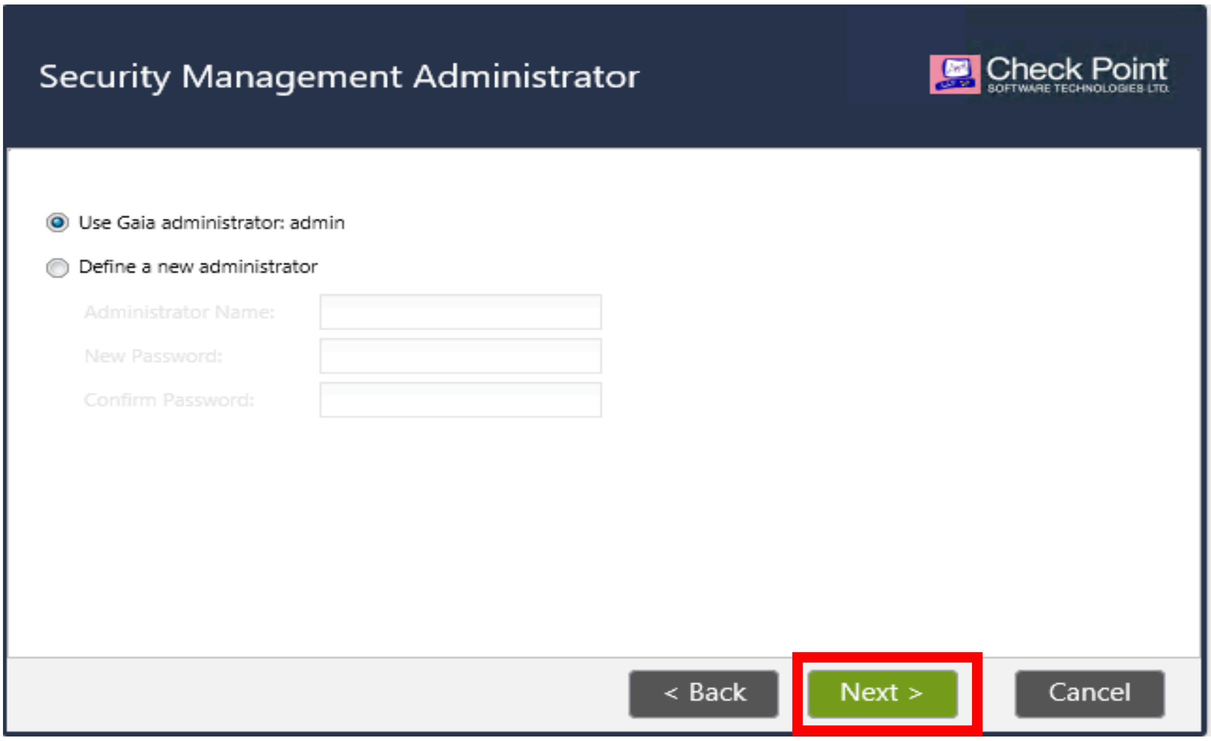
☑ Automatically download Blade Contracts and other important data (highly recommended)

For more information click here

8. Security Management Administrator

In this step you can define a new administrator account, a different one from the default **admin** account. This is an optional step, not needed, it depends on what you need to do or it may depend also on company policy or specific requirements that you may receive during the implementation.

Leave the first option checked – **Use Gaia administrator: admin** and click **Next** to continue.



Security Management Administrator

● Use Gaia administrator: admin

○ Define a new administrator

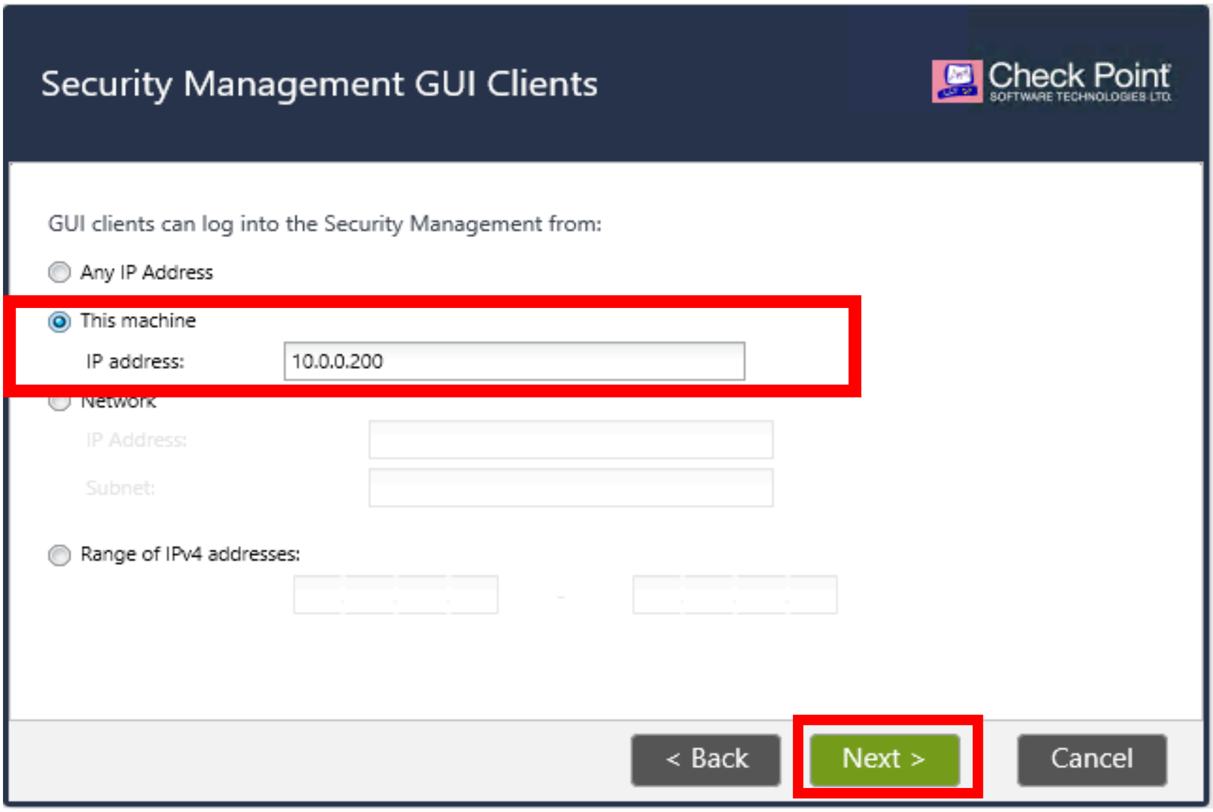
Administrator Name:

New Password:

Confirm Password:

9. Security Management GUI Clients

In this step, you can define what are the allowed IP addresses to connect to the Management Server. Clicking on **This Machine** option means that connections only from the MGMT PC, that has the IP address of 10.0.0.200, will be accepted by the SMS. Click **Next** to continue.



Security Management GUI Clients

GUI clients can log into the Security Management from:

○ Any IP Address

● This machine

IP address: 10.0.0.200

○ Network

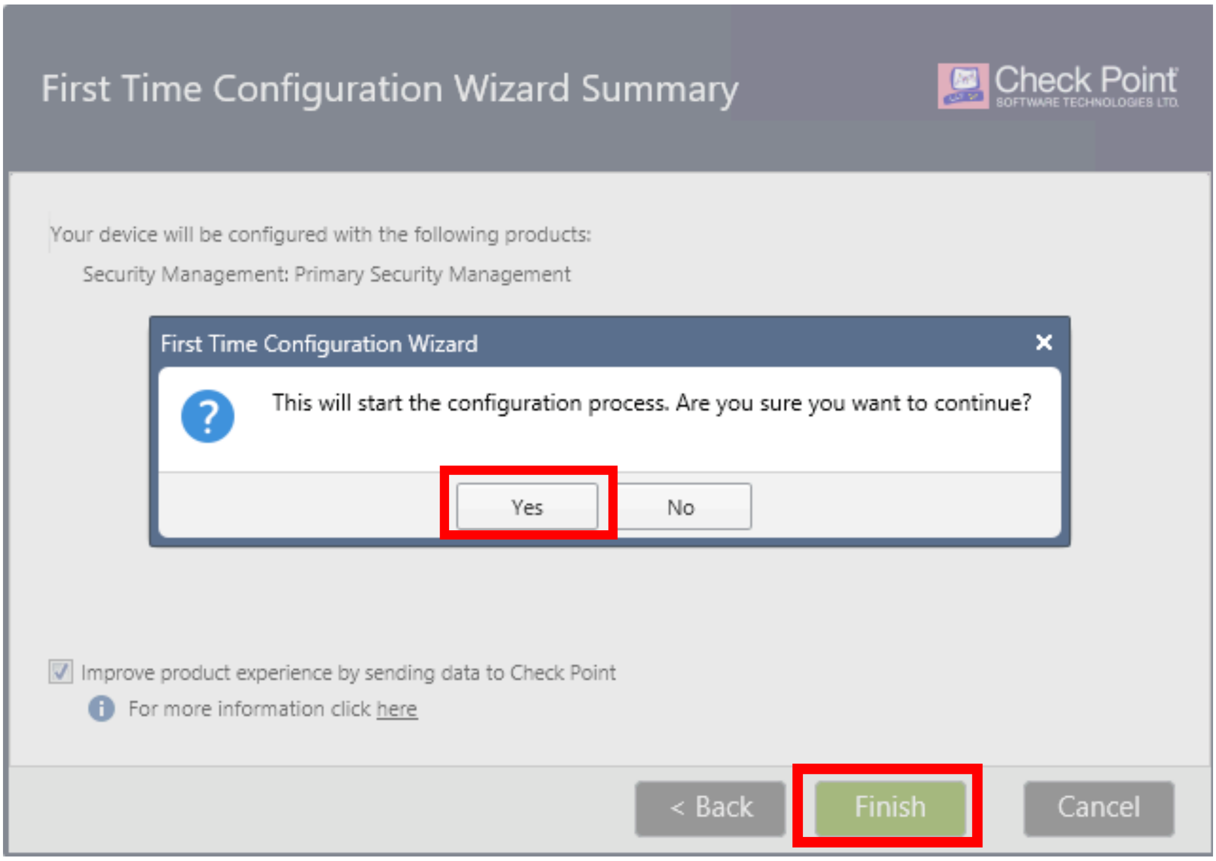
IP Address:

Subnet:

○ Range of IPv4 addresses:

10. First Time Wizard Summary

Please note that the summary confirms your selection in a previous step and we can see that this installation is a **Security Management Server** installation. Click **Finish** and **Yes** and the FTW installation starts.



First Time Configuration Wizard Summary

Your device will be configured with the following products:

Security Management: Primary Security Management

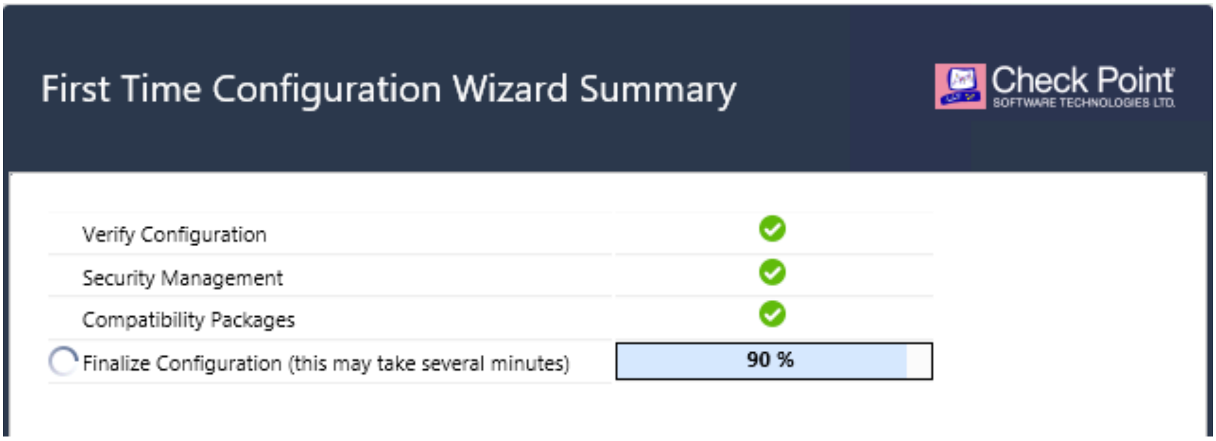
First Time Configuration Wizard

This will start the configuration process. Are you sure you want to continue?

☑ Improve product experience by sending data to Check Point

For more information click here

The installation will take 5-10 minutes, depending on your PC or server hardware specifications.

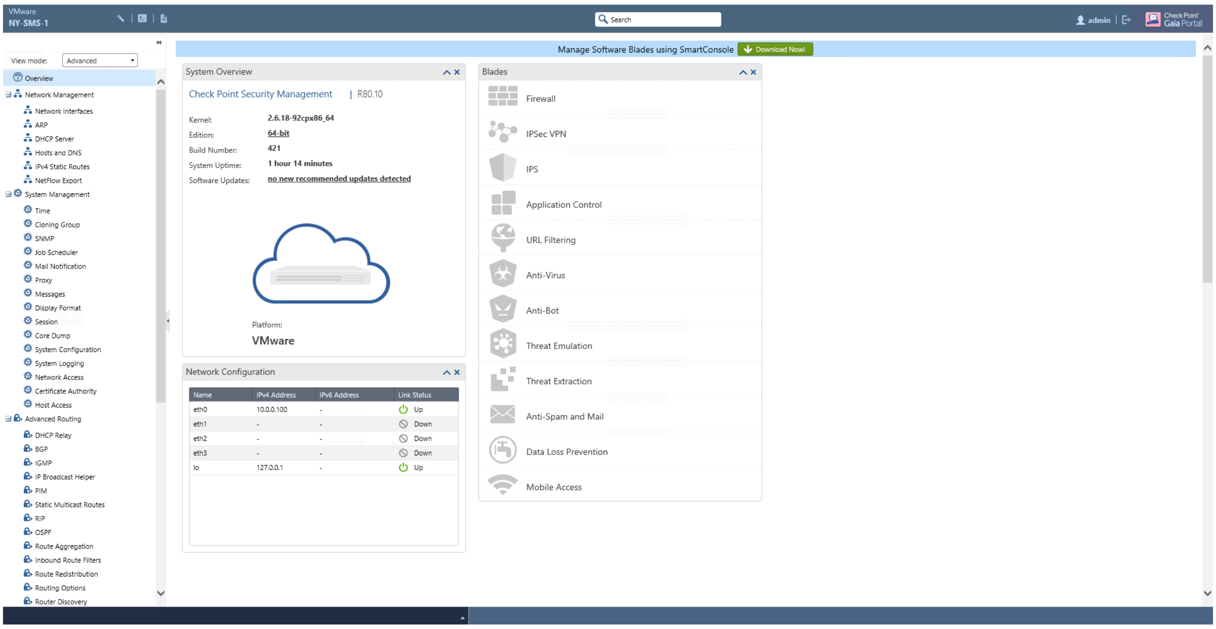


First Time Configuration Wizard Summary

Verify Configuration	✓
Security Management	✓
Compatibility Packages	✓
Finalize Configuration (this may take several minutes)	90 %

11. Verification

After installation succeeds, you are presented with login page again. Type your username and password as defined previously (admin / admin123) and the SMS Web UI will be presented to you.



System Overview

Check Point Security Management | R80.10

Kernel: 2.6.18-92cpx86_64
Edition: 64-bit
Build Number: 421
System Uptime: 1 hour 14 minutes
Software Updates: no new recommended updates detected

Platform:
VMware

Network Configuration

Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.0.0.100	-	Up
eth1	-	-	Down
eth2	-	-	Down
eth3	-	-	Down
lo	127.0.0.1	-	Up

This concludes First Time Wizard installation on New York Security Management Server.

9.0 Lab: Introduction to Gaia OS CLI

Lab Objectives

- Get familiar with Gaia Command Line Interface (CLI)
- Learn what are the available help tools in the CLI
- Learn the fundamental commands on CLI

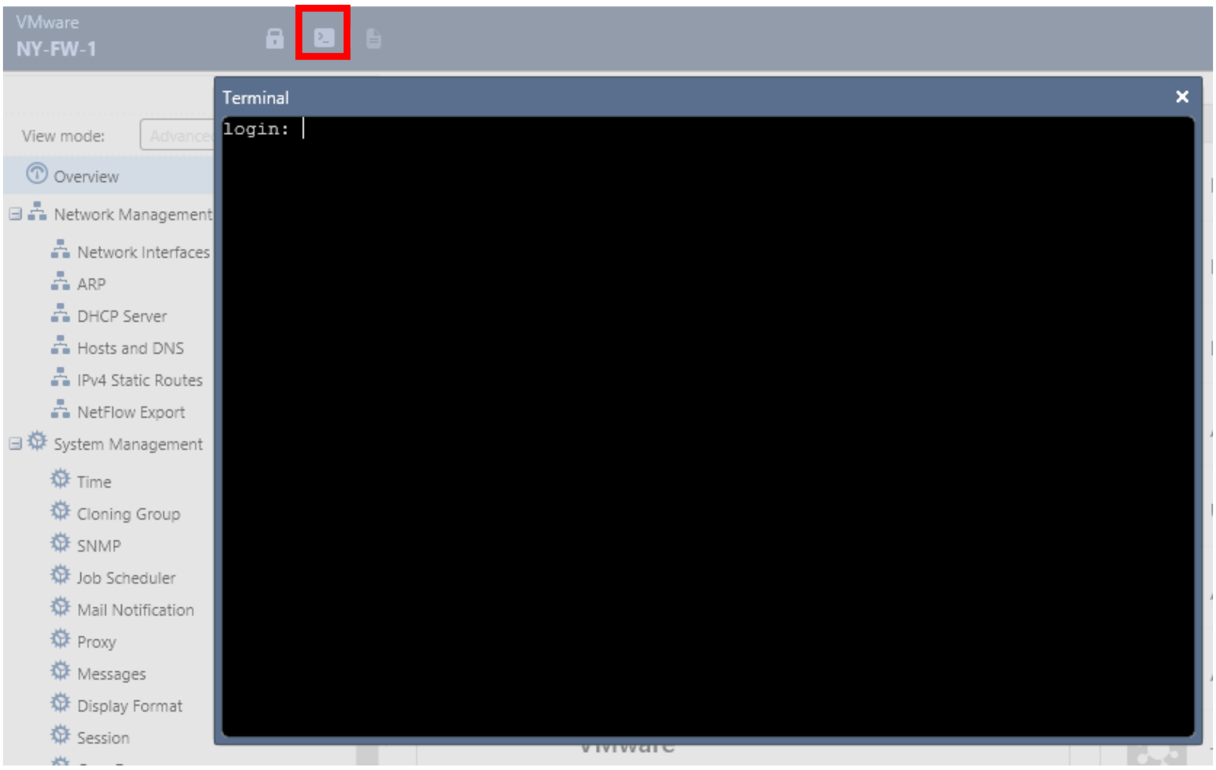
In **Lab 7 - Introduction to Gaia Web UI** I have introduced you the first possibility to operate and work with Gaia OS. In this Lab, we will start working with Command Line Interface (CLI) in the Gaia OS.

CLI can be used via SSH connection to Check Point appliance, open a CLI shell directly from the Web UI (screenshot below) or if connecting a direct cable to the console port of the gateway from your PC. When you right-click on the device in GNS3 or EVE-NG and choose **Console** you are actually simulating the last option – connecting to the device through console serial port.

```
This system is for authorized use only.
login: admin
Password:
NY-FW-1> expert
Enter expert password:

Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@NY-FW-1:0]# who
admin    ttyS0       Nov  8 03:47 -> Serial Port Connection
```

First you have to know that the CLI has two operation modes, CLISH and Expert mode. The default mode is CLISH. The **clish** mode does not provide access to all the advanced features that the system provides. In order to access the **expert** mode, you would have to type the **expert** command, set a password for expert mode and then login to **expert** mode.

If you want to return to clish mode, you would have to type **exit** command while in expert mode. If you login to a Check Point device directly in expert mode (if default shell has been changed to expert) and you want to navigate to clish mode, then you would have to type **clish** command and you will be provided clish shell access.



```
login:
```

Commands are organized in the CLI into groups or categories. If you want to configure the system you start the command with **set**. Let's take an example, but first login to NY-FW-1 or NY-SMS-1. While in console, type **?** and some output will be generated. No need to hit ENTER, output is generated immediately.

```
NY-FW-1> ?
<TAB> key can be used to complete / fetch the keyword.
<ESC><ESC> key can be used to see possible command completions.
'?' key can be used to get help on feature / keyword.
UP/DOWN arrow keys can be used to browse thru command history.
LEFT/RIGHT arrow keys can be used to edit command.
'!!','!nn','!-nn' etc. are valid form of executing history cmd.

At more prompt, following keys can be used-
SPACE key to see the next page.
ENTER key to see the next line.
Q/q key to exit to the cli prompt.

Useful commands:
show interface <TAB>
set interface <TAB>
add user <TAB>
save config
show commands
```

As you can see from the output, help is provided in the CLI shell. You can type **set** command and then hit <TAB> once on your keyboard, in order to see what is the next possible command or word to follow the **set** command.

```
NY-FW-1> set <hit TAB>
aaa                  - Authentication authorization and accounting
aggregate                - Configure aggregate routes
arp                  - Configure the parameters related to ARP
as                  - Configure Autonomous System Number
backup                 - Restore the configuration of the system
backup-scheduled        - Set an existing scheduling of a backup
bgp                  - Configure Border Gateway Protocol (BGP)

<output omitted>
```

The other nice tool that is provided is this. Type **set** command and the hit <ESC> twice (two times). You will be provided a list with full commands list that starts with **set** keyword.

```
NY-FW-1> set <ESC> <ESC>
set aaa radius-servers NAS-IP VALUE
set aaa radius-servers default-shell VALUE
set aaa radius-servers priority VALUE host VALUE
set aaa radius-servers priority VALUE new-priority VALUE
set aaa radius-servers priority VALUE port VALUE
set aaa radius-servers priority VALUE prompt-secret
set aaa radius-servers priority VALUE secret VALUE
set aaa radius-servers priority VALUE timeout VALUE

<output omitted>
```

These are great tools that can help in the beginning of your journey with Check Point security gateway. I advise you to start using those right away in order to get comfortable with the CLI, as the CLI is absolutely more powerful that the Web UI, less or no errors that you will be encountering and the right way to become a true Check Point Security Engineer.

Next category on the list is **show**. You will using commands starting with **show** keyword in order to see what is the result of the configuration applied. For example, let's find out what is my current configuration on the Security Gateway as related to my interfaces.

```
NY-FW-1> show in<TAB>
inactivity-timeout - show inactivity timeout
installer        - Show deployment agent information
interface         - interface All
interfaces        - Lists all interfaces
```

I type **show in** and then I hit **TAB.** Maybe I don't know the rest of the command. I will be provided all the valid possibilities of the next keyword that is accepted and that starts with **in**.

```
NY-FW-1> show interface eth2
state on
mac-addr 50:00:00:02:00:02
type ethernet
link-state link up
mtu 1500
auto-negotiation Not configured
speed 1000M
ipv6-autoconfig Not configured
duplex full
monitor-mode Not configured
link-speed 1000M/full
comments
ipv4-address 10.0.0.1/24
ipv6-address Not Configured
ipv6-local-link-address Not Configured

Statistics:
TX bytes:71873954 packets:76992 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:9712497 packets:62244 errors:0 dropped:0 overruns:0 frame:0
```

So this is the information related to eth2, our management interface. We can see that the link state is up, the IPv4 address and other information is well. Can we check the actual configuration that is applied to my interfaces ? Of course:

```
NY-FW-1> show configuration interface
set interface eth2 link-speed 1000M/full
set interface eth2 state on
set interface eth2 ipv4-address 10.0.0.1 mask-length 24

<output omitted>
```

Don’t forget to save your configuration when you finish applying the changes to the working config. Use **save config** in order to save the configuration and have it available after a reboot or power off event.

An interesting option and a great learning tool is the following command: **show command feature <feature>.**

This helps you find what are the available commands specific to a feature that you are looking at. Let’s take an example. I am trying to find out what are the available commands that relate to **interfaces**, for example.

```
NY-FW-1> show commands feature interface
add interface VALUE 6in4 VALUE remote VALUE ttl VALUE
add interface VALUE alias VALUE
add interface VALUE loopback VALUE
add interface VALUE vlan VALUE
delete interface VALUE 6in4 VALUE force
delete interface VALUE alias VALUE
delete interface VALUE ipv4-address
delete interface VALUE ipv6-address
delete interface VALUE loopback VALUE force
delete interface VALUE vlan VALUE force
set interface VALUE ipv4-address VALUE mask-length VALUE
set interface VALUE ipv4-address VALUE subnet-mask VALUE
set interface VALUE ipv6-address VALUE mask-length VALUE
set interface VALUE monitor-mode VALUE
set interface VALUE rx-ringsize VALUE
set interface VALUE tx-ringsize VALUE
set interface VALUE { comments VALUE mac-addr VALUE mtu VALUE state VALUE link-
speed VALUE auto-negotiation VALUE }
set interface VALUE { ipv6-autoconfig VALUE }
show interface VALUE 6in4s
show interface VALUE alias VALUE
show interface VALUE aliases
show interface VALUE all

<output omitted>
```

The nice part ? You are provided a complete list with all commands, from all categories or groups, like I mentioned in the beginning of this Lab. Commands that related to **interface** can start with **add, delete, set** and **show.** It’s self-explanatory, you get the idea.

10.0 Lab: CLI Expert Mode First Time Wizard on L-FW-1

Lab Objectives

- Understand config_system file for CLI FTW
- Run the First Time Wizard on L-FW-1 from the CLI Expert Mode

After you install Gaia OS, as you could understand up to this point, you need to run the First Time Wizard in order to finish OS installation and be able to access the machine on the Web UI.

Although it looks more “fancy” or even easier to do the FTW inside a browser, CLI is what you may want to get accommodated over the longer run. It is less error prone, it provides a fast way to implement what needs to be done and you can also automate your work through CLI.

We will have a dedicated lab on how to get started with CLI, most common commands, how to search for different options available and so on, but I couldn’t just skip it for now and not introduce running the FTW in the CLI Expert Mode. As you will see now, it is more faster, efficient and I believe that you will enjoy working in CLI once you start to get comfortable.

First of all, in Command Line Interface or CLI, there are two modes available:

- Clish (CLI shell), and
- Expert Mode

Open console to London Firewall L-FW-1 and login using **admin/admin123**:

```
This system is for authorized use only.
login: admin
Password:
In order to configure your system, please access the Web UI and finish the First Time
Wizard.
gw-030000>
```

Instead of using a web browser to run the First Time Wizard, we will run it here, using the CLI. We are now logged in the L-FW-1 and we are in CLISH mode. In order to enter **expert mode**, we have to type **expert** command, but as you can see, we are asked to first define a password for **expert** mode.

```
gw-030000> expert
Expert password has not been defined. To set expert password, use the command "set
expert-password".
```

Let’s first define the **expert mode** password. I will use admin123 as the password here as well :

```
gw-030000> set expert-password
Enter new expert password: admin123
Enter new expert password (again): admin123
gw-030000>
```

Now, let’s login to expert mode:

```
gw-030000> expert
Enter expert password:admin123


Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@gw-030000:0]#
```

Please note that the **config_system** utility is not an interactive tool and it will be used only for first time configuration and not for any ongoing system configurations.

The **config_system** utility can be used in two ways in order to run the First Time Wizard:

- config_system --config-string <String of Parameters and Values>
- config_system -f <File Name>

The first option is to run the command and include a list of all parameters that need to be executed by the script in a linear concatenated fashion. Here is an example:

"hostname=myhost&domainname=somedomain.com&timezone='America/Indiana/Indianapolis'&ftw_sic_key=aaaa&install_security_gw=true etc“

You will include here all the parameters and use & between each argument.

I find this option not a very good option as I may not be able to know all the parameters from the memory, right ?

Instead the second option is great. Here is the thing, we will create a configuration file, set inside all the necessary parameters that we need and use this file to be run by the **config_system** utility.

Let's first create the configuration file. As a start, if you just type the **config_system** command, without any arguments, here is the result :

```
[Expert@gw-030000:0]# config_system
Error: options are missing
Usage: config_system <options>
where config_system options include:
  -f|--config-file <path>      Read first time wizard configuration
                         from <path>.
  -s|--config-string <string>  Read first time wizard configuration
                         from string.
  -t|--create-template <path>  Write first time wizard  configuration
                         template file in <path>.
   --dry-run                   Verify that first time wizard
                         configuration file is valid.
  -l|--list-params             List configurable parameters.

If both, configuration file and string, were provided, configuration
string will be ignored.
Configuration string should consist of parameters separated by '&'.
Each parameter should include key followed by value e.g. param1=value.
For the list of all configurable parameters and their descriptions,
create configuration template file with config_system -t <path> .
```

The **-l option** can provide us the list of configurable parameters. This could be used in the case you want to run the first option for **config_system** utility.

Instead, we will use the **-t option** to create the template configuration file. The console it's expecting the following command:

config_system -t <path>

Please note that while in expert mode, this is a linux like environment, so linux commands will be used. Don't worry if you are new to linux world, it will be super simple. So we have to specify the location, or path, where to put the configuration, or template, file. Let's first see where are we now in the file system, in Expert mode :

```
[Expert@gw-030000:0]# pwd
/home/admin
[Expert@gw-030000:0]#
```

We are in /home/admin, we will use this path when generating the template file. Next, use **ls** command to list what files are available in /home/admin :

```
[Expert@gw-030000:0]# config_system -t /home/admin/FTW
[Expert@gw-030000:0]# ls
FTW
[Expert@gw-030000:0]#
```

So now we have the **FTW** configuration file created. Please note that FTW is just a name that I have chosen, just arbitrary. Any name could have been used here. The next thing to do is open FTW file and edit or **set the parameters for First Time Wizard**. We will set the parameters that we would be configuring through Web UI, it's the same thing.

In linux, you can use the **vi** command to open a file and edit it. Let's use **vi** command now :

```
[Expert@gw-030000:0]# vi FTW
```

And the FTW file created earlier opens.

```
##############################################################################
#                                                                            #
#                                                 #
#                Products configuration                     #
#                                                 #
#   For keys below set "true"/"false" after '='  within the quotes     #
##############################################################################
#

# Install Security Gateway.
install_security_gw=true

# Enable DAIP (dynamic ip) gateway.
# Should be "false" if CXL or Security Management enabled
gateway_daip="false"

# Enable/Disable CXL.
gateway_cluster_member=

# Install Security Management.
install_security_managment=false

# Optional parameters, only one of the parameters below can be "true".
# If no primary of secondary specified, log server will be installed.
# Requires Security Management to be installed.
install_mgmt_primary=
install_mgmt_secondary=

# Provider-1 parameters
# e.g: install_mds_primary=true
#     install_mds_secondary=false
#     install_mlm=false
#     install_mds_interface=eth0
install_mds_primary=
install_mds_secondary=
install_mlm=
install_mds_interface=

# Automatically download Blade Contracts and other important data (highly recommended)
# It is highly recommended to keep this setting enabled, to ensure smooth operation of Check Point products.
# for more info see sk94508
#
# possible values: "true" / "false"
download_info="true"

# Improve product experience by sending data to Check Point
# If you enable this setting, the Security Management Server and Security Gateways may upload data that will
# help Check Point provide you with optimal services.
# for more info see sk94509
#
# possible values: "true" / "false"
upload_info="false"

# In case of Smart1 SmartEvent appliance, choose
# Security Management only, log server will be installed automatically
```

```
############################################################################
#
#                                                      #
#                   Products Parameters                          #
#                                                      #
#             For keys below set value after '='                    #
############################################################################
#

# Management administrator configuration
# Set to "gaia_admin" if you wish to use the Gaia 'admin' account.
# Set to "new_admin" if you wish to configure a new admin account.
# Must be provided, if Security Management installed
mgmt_admin_radio=gaia_admin

# In case you chose to configure a new Management admin account,
# you must fill in the credentials.
# Management administrator name
mgmt_admin_name=

# Management administrator password
mgmt_admin_passwd=

# Management GUI clients
# choose which GUI clients can log into the Security Management
# (e.g. any, 1.2.3.4, 192.168.0.0/24)
#
# Set to "any" if any host allowed to connect to management
# Set to "range" if range of IPs allowed to connect to management
# Set to "network" if IPs from specific network allowed to connect
# to management
# Set to "this" if it' a single IP
# Must be provided if Security Management installed
mgmt_gui_clients_radio=any
#
# In case of "range", provide the first and last IPs in dotted format
mgmt_gui_clients_first_ip_field=
mgmt_gui_clients_last_ip_field=
#
# In case of "network", provide IP in dotted format and netmask length
# in range 0-32
mgmt_gui_clients_ip_field=
mgmt_gui_clients_subnet_field=
#
# In case of a single IP
mgmt_gui_clients_hostname=
# Secure Internal Communication key, e.g. "aaaa"
# Must be provided, if primary Security Management not installed
ftw_sic_key=admin123

############################################################################
#
#                                                  #
#      Operating System configuration - optional section             #
#                                                  #
#           For keys below set value after '='                 #
############################################################################
#

# Password (hash) of user admin.
# To get hash of admin password from configured system:
#      dbget passwd:admin:passwd
# OR
#      grep admin /etc/shadow | cut -d: -f2
#
# IMPORTANT! In order to preserve the literal value of each character
# in hash, enclose hash string within the quotes.
#      e.g admin_hash='put_here_your_hash_string'
#
# Optional parameter
admin_hash=''

# Interface name, optional parameter
iface=eth1

# Management interface IP in dotted format (e.g. 1.2.3.4),
# management interface mask length (in range 0-32, e,g 24 ) and
# default gateway.
# Pay attention, that if you run first time configuration remotely
# and you change IP, in order to maintain the connection,
# an old IP address will be retained  as a secondary IP address.
# This secondary IP address can be delete later.
# Your session will be disconnected after first time configuration
# process.
# Optional parameter, requires "iface" to be specified
# IPv6 address format: 0000:1111:2222:3333:4444:5555:6666:7777
# ipstat_v4 manually/off
# ipstat_v6 manually/off
ipstat_v4=manually
ipaddr_v4=201.0.1.1
masklen_v4=24
default_gw_v4=201.0.1.254
```

```
ipstat_v6=off
ipaddr_v6=
masklen_v6=
default_gw_v6=

# Host Name e.g host123, optional parameter
hostname=L-FW-1

# Domain Name e.g. checkpoint.com, optional parameter
domainname=chkp.local

# Time Zone in format Area/Region (e.g America/New_York or Etc/GMT-5)
# Pay attention that GMT offset should be in classic UTC notation:
# GMT-5 is 5 hours behind UTC (i.e. west to Greenwich)
# Enclose time zone string within the quotes.
# Optional parameter
timezone=''

# NTP servers
# NTP parameters are optional
ntp_primary=
ntp_primary_version=
ntp_secondary=
ntp_secondary_version=

# DNS - IP address of primary, secondary, tertiary DNS servers
# DNS parameters are optional.
primary=172.16.10.100
secondary=8.8.8.8
tertiary=

# Proxy Settings - Address and port of Proxy server
# Proxy Settings are optional
proxy_address=
proxy_port=

##########################################################################
#
#                                                        #
#                   Post installation parameters                   #
#                                                        #
#    For keys below set "true"/"false" after '='  within the quotes     #
##########################################################################
#
# Optional parameter, if not specified the default is false
reboot_if_required=true
```

Vi is a linux file editor that you will find most probably on any linux or unix machine. This is a reason of why you may want to get comfortable with it.

In order to get into editing mode, because now the FTW file is open but you can't edit anything, please type **"i"** (from INSERT). Please note that in your console the following appears, that confirm you are in editing mode :

-- INSERT –

Please use arrows to navigate through the file and change/add/set the parameters as you can see above, in green.

When finished editing, type **ESC** on your keyboard. You will see that –INSERT— closes. Now type **:wq!** which means w-write, q-quit and ! – override.

You are now returned to expert mode:

```
"FTW" 190L, 5990C written
[Expert@gw-030000:0]#
```

Now, before we use the configuration file just edited and run the First Time Wizard, we have the ability to test it and see if the file has any errors :

```
[Expert@gw-030000:0]# config_system -f FTW --dry-run
dos2unix: converting file FTW to UNIX format ...

Validating configuration file:  Done

Configuration file/string is valid
[Expert@gw-030000:0]#
```

We can now safely run the First Time Wizard with the configuration file as no errors have been detected:

```
[Expert@gw-030000:0]# config_system -f FTW
dos2unix: converting file FTW to UNIX format ...

Validating configuration file:  Done
Configuring OS parameters:      Done
Configuring products:           Done
```

```
First time configuration was completed!

Reboot will be performed in order to complete the installation
[Expert@gw-030000:0]#
```

After 1-2 minutes the L-FW-1 reboots. Let us now authenticate and do some verification. We will verify if IP address has been configured correct on eth1 and default route inserted in routing table pointing to the right IP:

```
This system is for authorized use only.
login: admin
Password:admin123
L-FW-1> show configuration interface
set interface eth0 state on
set interface eth0 auto-negotiation on
set interface eth0 ipv4-address 192.168.1.1 mask-length 24
set interface eth1 link-speed 1000M/full
set interface eth1 state on
set interface eth1 ipv4-address 201.0.1.1 mask-length 24
L-FW-1> show route
Codes: C - Connected, S - Static, R - RIP, B - BGP (D - Default),
    O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA)
    A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed,
    U - Unreachable, i - Inactive

S       0.0.0.0/0          via 201.0.1.254, eth1, cost 0, age 78
C       127.0.0.0/8        is directly connected, lo
C       192.168.1.0/24     is directly connected, eth0
C       201.0.1.0/24       is directly connected, eth1
```

Configuration looks good !

11.0 Lab: Users and Roles in the Web UI

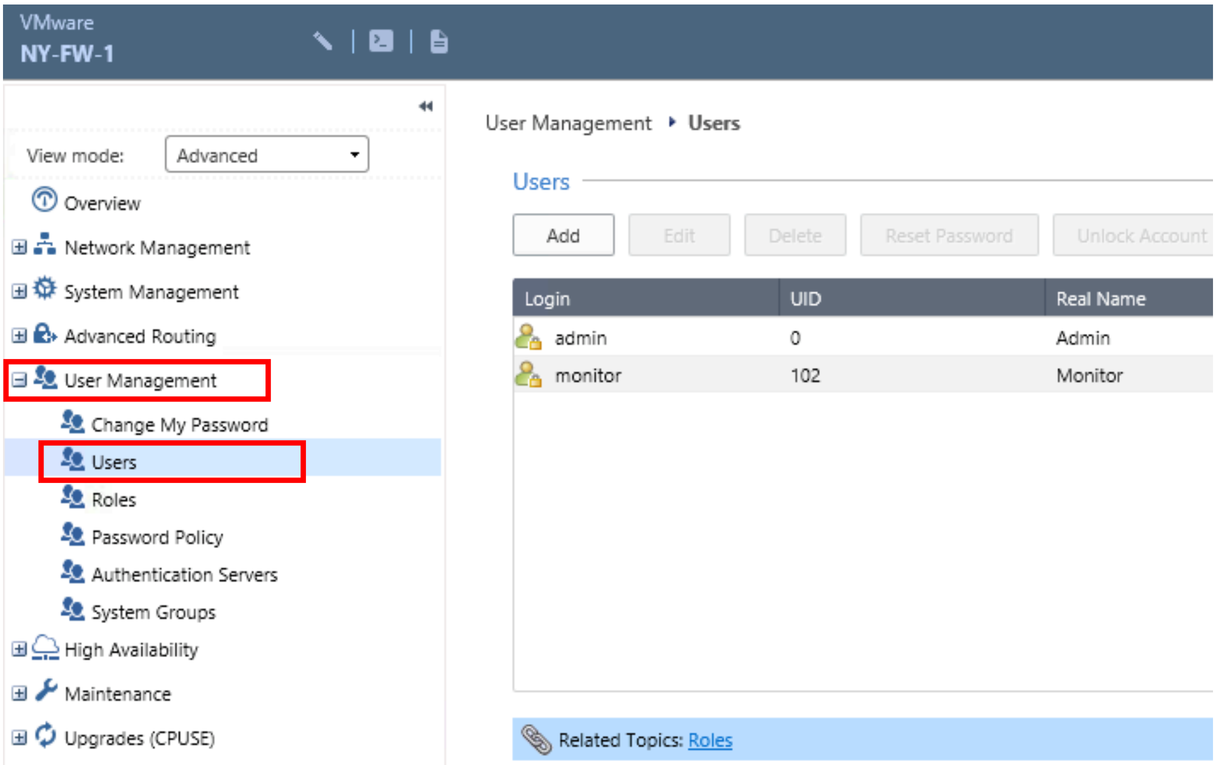
Lab Objectives

- Create custom roles in the Web UI
- Attach the roles to a user and run verification tests

Users and Roles specific information and configuration is available in the **User Management** menu in Web UI. Depending on the company's policy and functional roles in the IT department, sometimes multiple user types are needed. In this lab you will learn how to create, verify and delete a new custom user, that has a custom role attached. What is actually a role ?

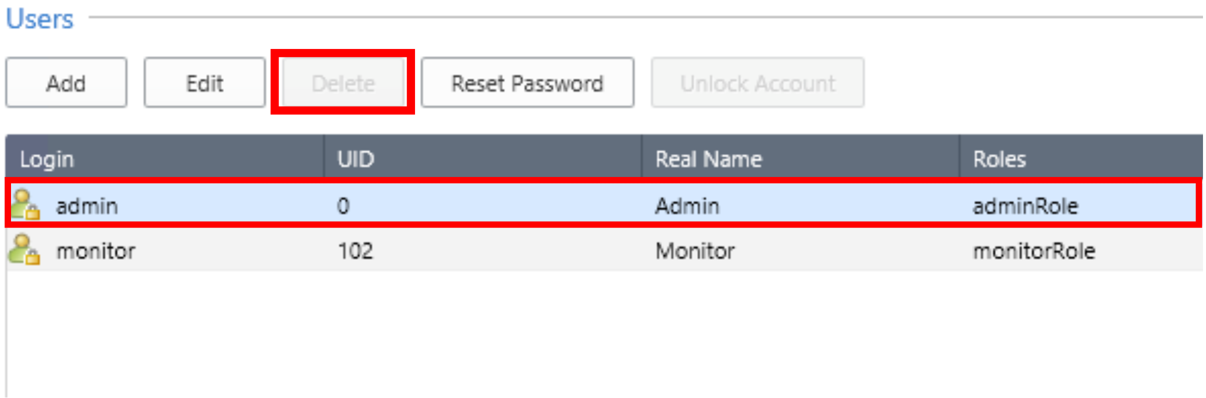
Users defined on a Gaia system (security gateway or security management system) can have read-write access to Gaia OS features and functionalities, or can have read only access (can view, but can't modify settings). Through **Roles** and **Role-Based Administration(RBA)** you can create custom permissions and assign this to your users, new or existing. Simply said, you can assign to a user read-write permissions for some specific features and read only permissions for other features. RBA is a powerful tool available in the Gaia OS, so let's go through an example now.

Login to the NY-FW-1 Web UI and navigate to **User Management -> Users**:



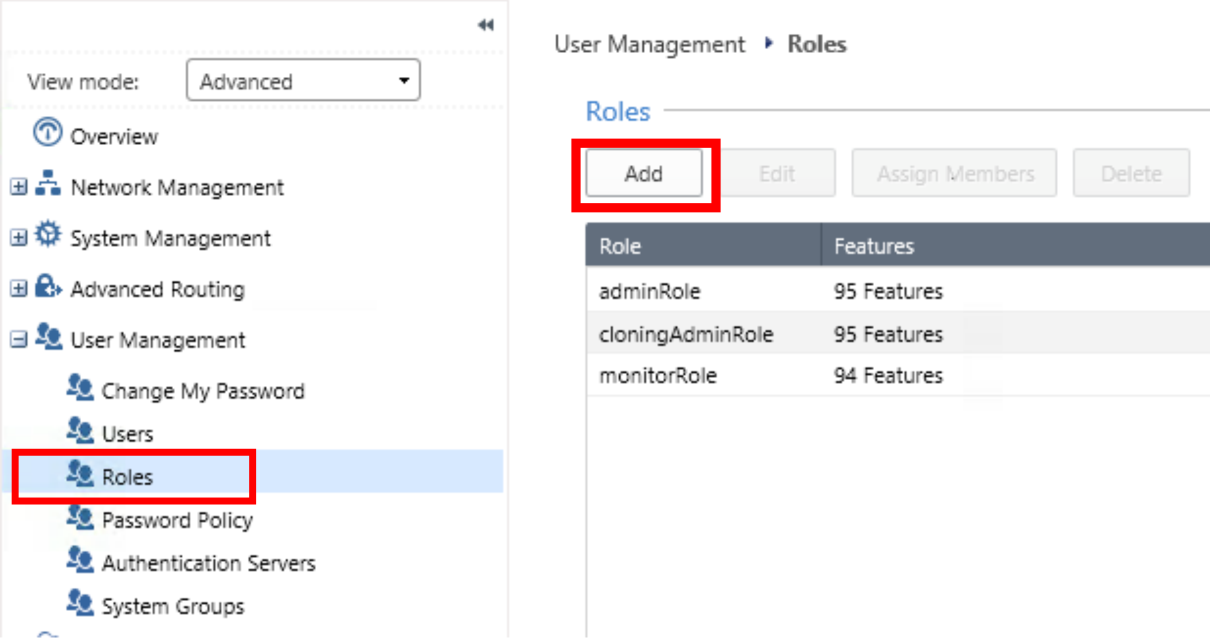
Login	UID	Real Name
admin	0	Admin
monitor	102	Monitor

Please note that by default two users are available: **admin** and **monitor**, admin user has read write permissions (assigned through role adminRole), while monitor user has read only permissions (assigned through monitorRole). These two users can’t be deleted and you can see this if you click on any of the two and look at the Delete button, it’s greyed out.



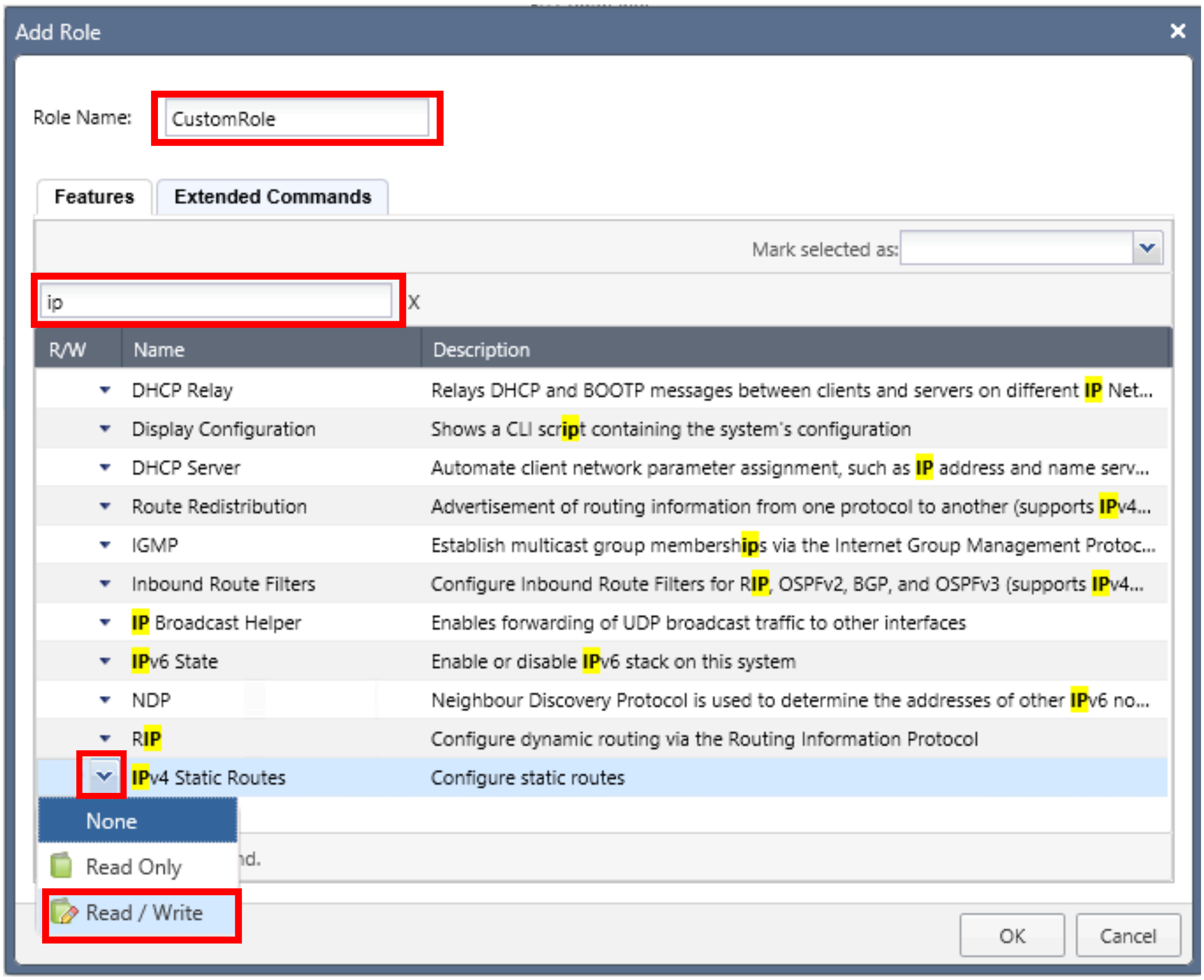
Login	UID	Real Name	Roles
admin	0	Admin	adminRole
monitor	102	Monitor	monitorRole

In order to create a custom Role (non-standard) and assign specific features, read write and read only to the Role, click on the **Roles** sub-menu and then click **Add**:



Role	Features
adminRole	95 Features
cloningAdminRole	95 Features
monitorRole	94 Features

In the **Role Name** field, type **CustomRole** and now let’s add some features to this new role. Type **ip** in the search bar and **ip** related features are displayed. Click on the small arrow next to **IPv4 Static Routes** and select **Read/Write**. We have now assigned to the **CustomRole** the read/write capability to create and modify IPv4 static routes.



Role Name: CustomRole

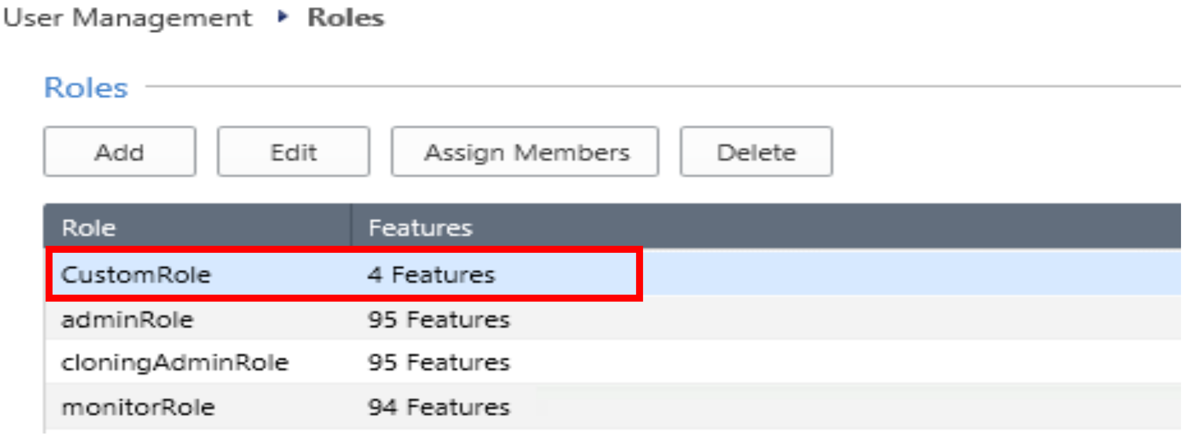
ip

R/W	Name	Description
▾	DHCP Relay	Relays DHCP and BOOTP messages between clients and servers on different IP Net...
▾	Display Configuration	Shows a CLI script containing the system's configuration
▾	DHCP Server	Automate client network parameter assignment, such as IP address and name serv...
▾	Route Redistribution	Advertisement of routing information from one protocol to another (supports IPv4...
▾	IGMP	Establish multicast group memberships via the Internet Group Management Protoc...
▾	Inbound Route Filters	Configure Inbound Route Filters for RIP, OSPFv2, BGP, and OSPFv3 (supports IPv4...
▾	IP Broadcast Helper	Enables forwarding of UDP broadcast traffic to other interfaces
▾	IPv6 State	Enable or disable IPv6 stack on this system
▾	NDP	Neighbour Discovery Protocol is used to determine the addresses of other IPv6 no...
▾	RIP	Configure dynamic routing via the Routing Information Protocol
▾	IPv4 Static Routes	Configure static routes

Follow the same process and assign the following features to the **CustomRole**:

Parameter	Value	
Time	Read/Write	
Network Interfaces	Read/Write	
Management Interface	Read Only	
Roles	Read Only	

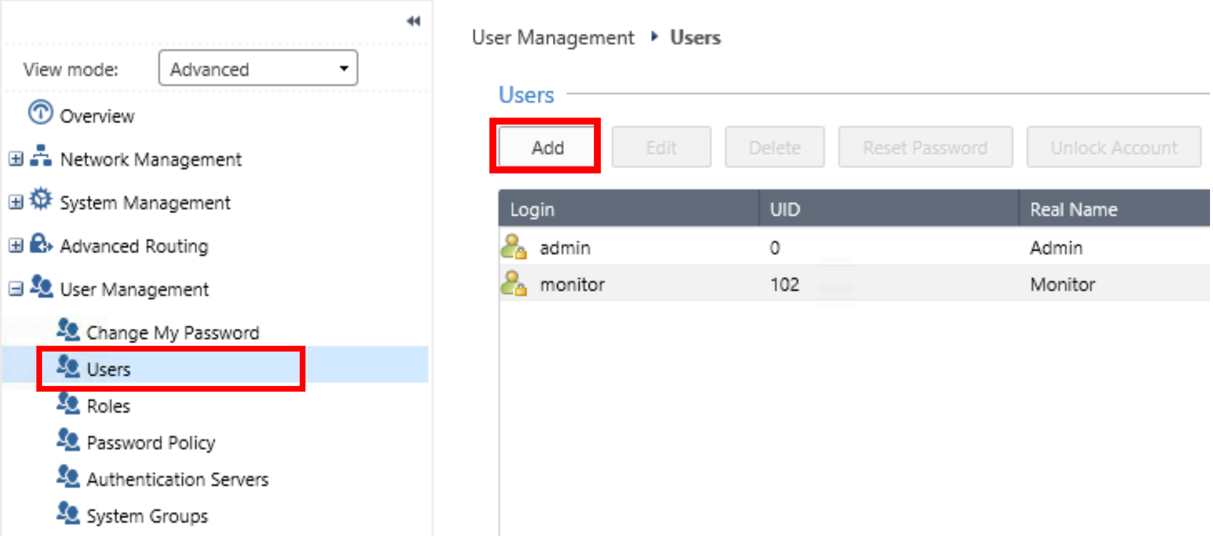
Click **OK** and the new Role is added to the list.



Role	Features
CustomRole	4 Features
adminRole	95 Features
cloningAdminRole	95 Features
monitorRole	94 Features

We have now defined a new role that has been assigned 5 features. Now, we will define a new user and assign this **CustomRole** to this user.

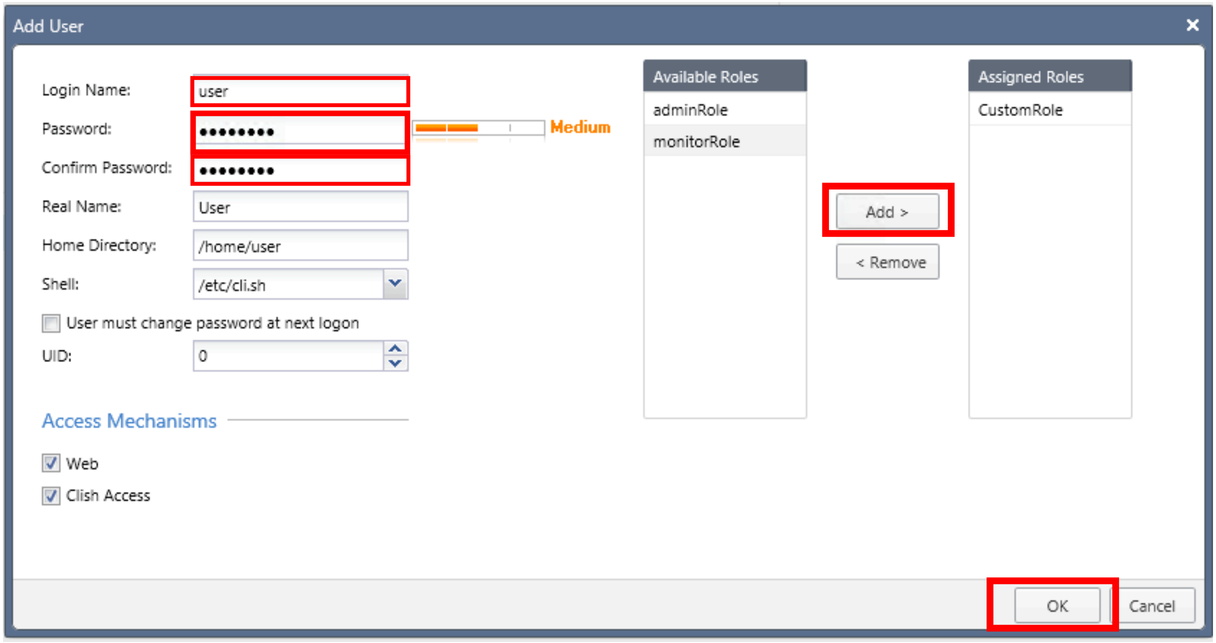
Click on the **Users** sub-menu inside the **User Management** menu and then click **Add** to add a new user.



Login	UID	Real Name
admin	0	Admin
monitor	102	Monitor

Fill in the following details, select **CustomRole** in the Available Roles column and click Add to add the Role in the Assigned Roles column. Click **OK** to apply the configuration.

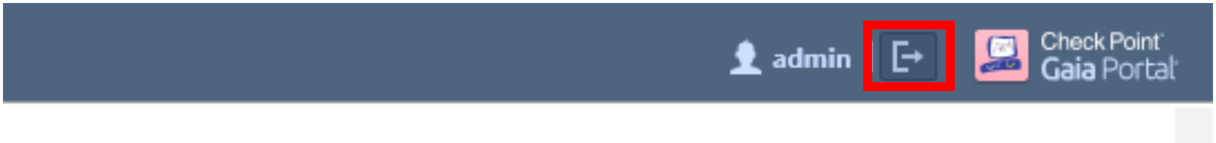
Parameter	Value
Login Name	user
Password	admin123
Confirm Password	admin123



Login Name: user
Password: •••••••• Medium
Confirm Password: ••••••••
Real Name: User
Home Directory: /home/user
Shell: /etc/cli.sh
□ User must change password at next logon
UID: 0
☑ Web
☑ Clish Access

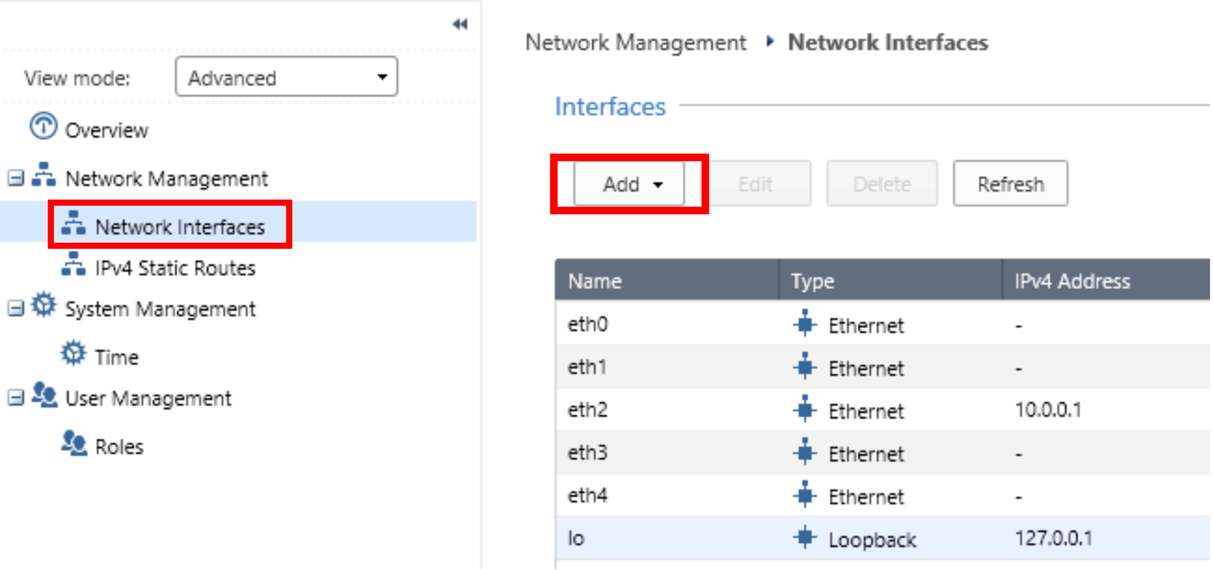
Verification:

Sign out by clicking the sign out button in the top-right corner



and login with the new created username and password: user/admin123.

After successful login, please note that you are now being presented a restricted view of the Web UI, as opposed to the full view in the case of **admin** username.

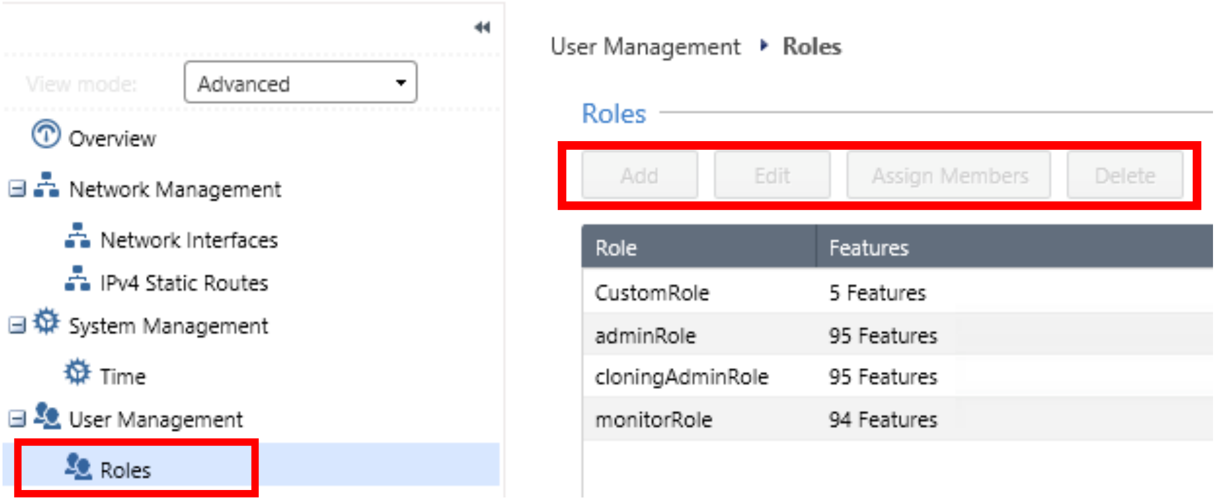


Name	Type	IPv4 Address
eth0	Ethernet	-
eth1	Ethernet	-
eth2	Ethernet	10.0.0.1
eth3	Ethernet	-
eth4	Ethernet	-
lo	Loopback	127.0.0.1

Remember that some of the features added to the **CustomRole** were added with Read/Write permissions, while others were added with Read Only permissions.

For example, if you click on **Network Interfaces** you can observe that **Add** button is active. This means that we can add interfaces, so modifications are allowed (Read/Write permissions).

On the contrary, if you click on **Roles** under **User Management** menu, you would be able to see all the available roles, but the Add/Edit/Delete buttons are greyed out. This is due to the fact that the Roles features added to the new CustomRole were added with Read Only permissions.



Role	Features
CustomRole	5 Features
adminRole	95 Features
cloningAdminRole	95 Features
monitorRole	94 Features

Sign out and login into console CLI shell using user/admin123. Then type **set** and hit TAB to see what are the available commands to follow the **set** keyword.

```
This system is for authorized use only.
login: user
Password: admin123
NY-FW-1> set <TAB>
bonding      - Configure bonding interfaces
clienv       - CLI environment variables.
config-lock  - Enable / Disable exclusive config access.
date         - Set current date
interface    - Displays the interface related parameters
ping         - Configure ping parameters
pppoe        - Set PPPoE
static-route - Configure an IPv4 static route
time         - Set current time
timezone     - Set system time zone
```

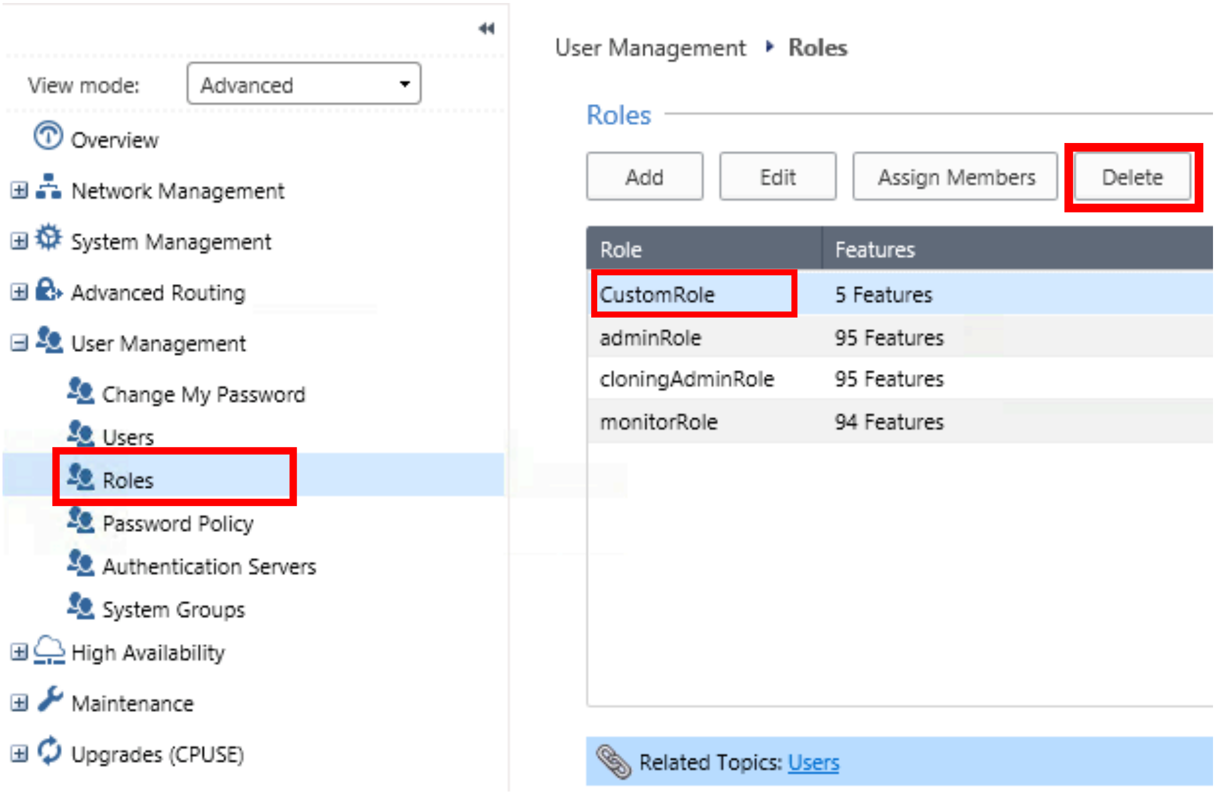
Remember that the only features added to the CustomRole with Read/Write permissions were IPv4 Static Routes, Network Interfaces and Time. As you can see above, when using the **set** command, which needs write permissions to configure the system, only these features can be configured.

Let’s check now what commands are available for **show** command set, which means Read Only and Read Write features available for this CustomRole.

Type **show** and hit TAB to see what are the available commands to follow the **show** keyword. We can observe now that we are given the possibility to see information related to RBA – role-based administration and the management interface. The last two features were added with Read Only permissions.

```
NY-FW-1> show <TAB>
bonding      - Display summary of bonding interfaces
bridging     - Display summary of bridging interfaces
clienv       - CLI environment variables.
clock        - Show current date and time
commands     - Show All Commands.
config-lock  - Show exclusive access settings.
config-state - Show state of configuration
date         - Show current date
interface    - interface All
interfaces   - Lists all interfaces
management   - management interface configuration
ping         - Show ping parameters
pppoe        - Show PPPoE
rba          - Role-based administration configuration
route        - Show routing table information
time         - Show current time
timezone     - Show system time zone
uptime       - show system uptime
NY-FW-1>
```

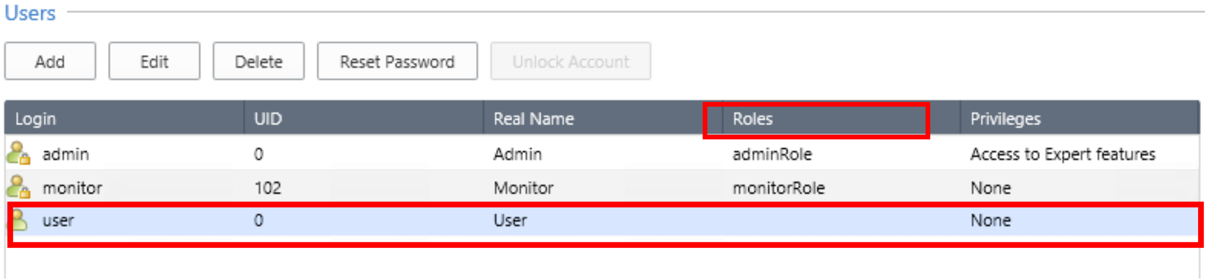
To delete a User and or Role, simply navigate to the **User** or **Roles sub-menus**, select it and click **Delete.**



View mode: Advanced

Role	Features
CustomRole	5 Features
adminRole	95 Features
cloningAdminRole	95 Features
monitorRole	94 Features

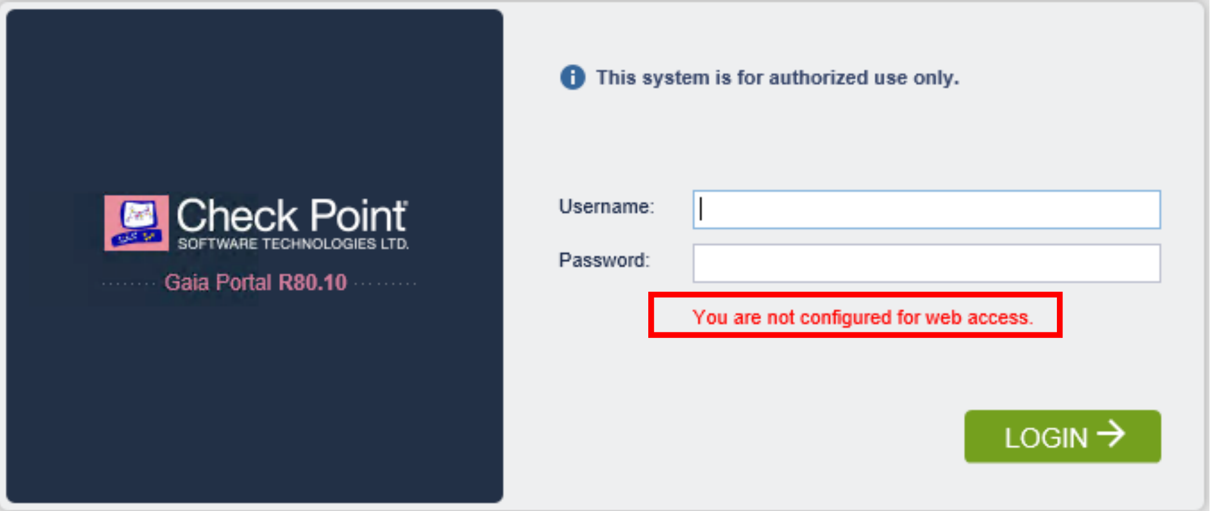
If you navigate now to the **Users sub-menu**, you can see that the user **user** has no Roles attached.



Users

Login	UID	Real Name	Roles	Privileges
admin	0	Admin	adminRole	Access to Expert features
monitor	102	Monitor	monitorRole	None
user	0	User		None

If you now try to login with **user/admin123** you will get rejected.



This system is for authorized use only.

Username:

Password:

You are not configured for web access.

This is because in the Role attached to the user, remember, it is specified if the user is allowed to login into the Web UI and or the CLI.

12.0 Lab: Users and Roles in the CLI

Lab Objectives

- Create custom roles in the Command Line Interface (CLI)
- Attach the roles to a user and run verification tests

In this Lab we will create another user – **user2**, assign a custom role as well and restrict usage to only access the CLI, so Web UI access will not be permitted.

Login to **NY-FW-1** CLI console using the **admin/admin123** username and password and let's add **user2.**

```
NY-FW-1> add user user2 uid 0 homedir /home/user2
WARNING Must set password and a role before user can login.
- Use 'set user USER password' to set password.
- Use 'add rba user USER roles ROLE' to set a role.

NY-FW-1>
```

You can use TAB for help with auto-completing the command. Please note the messages displayed in the CLISH. We must set a password for user2 and, in order to become a valid user, we must assign a role. Let's first assign the password **admin123** to this new user – **user2.**

```
NY-FW-1> set user user2 password
New password:admin123
Verify new password:admin123
NY-FW-1>
```

Next, we need to define a role.

```
NY-FW-1> add rba role CustomRole2 domain-type System readwrite-features
backup,license,route
NY-FW-1> add rba role CustomRole2 domain-type System readonly-features
configuration,time
NY-FW-1>
```

Features that will be added to readwrite or readonly must be separated by comma (,) and no spaces are allowed.

Now, let's assign the new created role, **CustomRole2**, to our **user2** user.

```
NY-FW-1> add rba user user2 roles CustomRole2
NY-FW-1>
```

Verification:

Log out from **NY-FW-1** session and login with new user : **user2/admin123**.

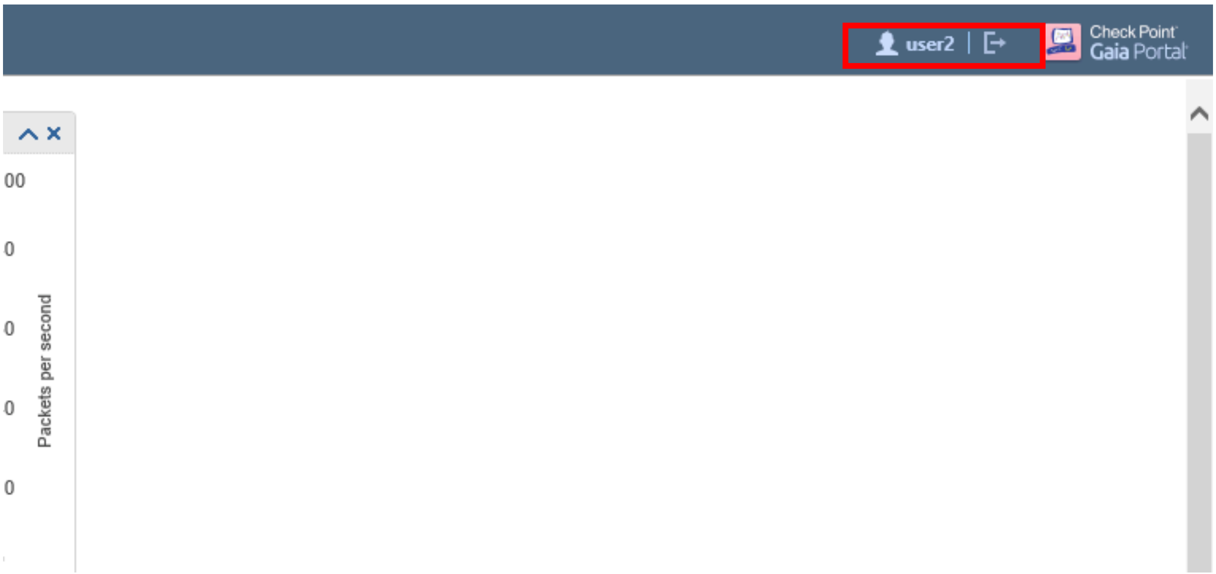
Observe the **set** and **show** permissions that **user2** is allocated:

```
This system is for authorized use only.
login: user2
Password: admin123
NY-FW-1> set <TAB>
backup      - Restore the configuration of the system
clienv      - CLI environment variables.
config-lock - Enable / Disable exclusive config access.
NY-FW-1> show
backup        - Show the status of the latest backup/restore
backups       - List of local backups
clienv        - CLI environment variables.
commands      - Show All Commands.
config-lock   - Show exclusive access settings.
config-state  - Show state of configuration
configuration - Show Configuration
ipv6          - Show IPv6 configuration and state
restore       - Restore the configuration of the system
route         - Show routing table information
uptime        - show system uptime
NY-FW-1>
```

Please note that by default, if not specified explicitly, both access methods are added to the user. Let’s verify the current status:

```
NY-FW-1> show rba user user2
User
   user2
   access-mechanism CLI
   access-mechanism Web-UI
   role CustomRole2
NY-FW-1>
```

Let’s validate that we can authenticate into Web UI through **user2**.



Indeed we can, so now let’s change the default behaviour and permit login to only the CLI.

```
NY-FW-1> delete rba user user2 access-mechanisms Web-UI
NY-FW-1> show rba user user2
User
    user2
    access-mechanism CLI
    role CustomRole2
NY-FW-1>
```

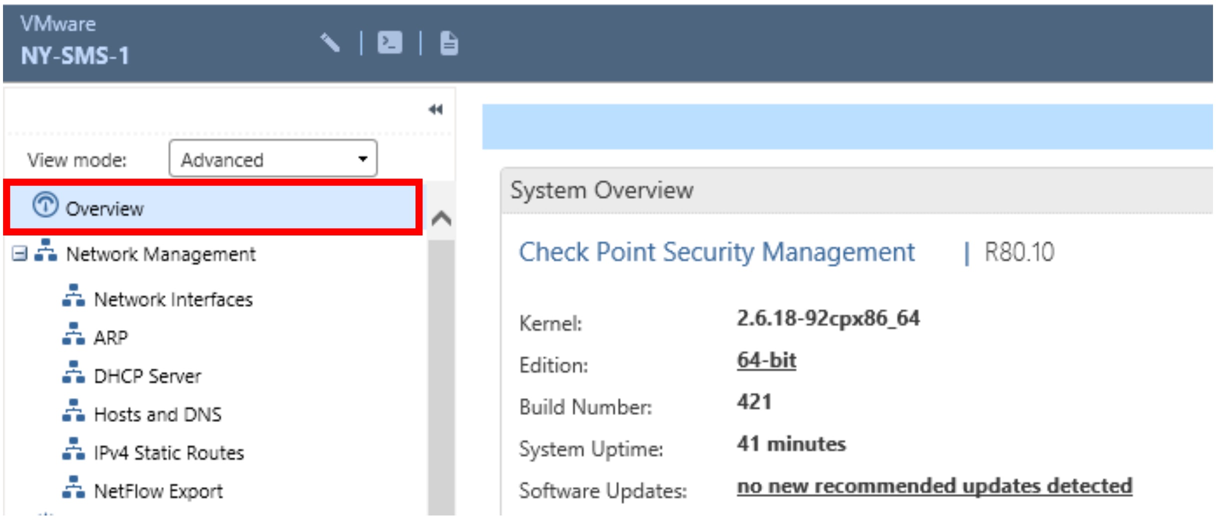
13.0 Lab: Install SmartConsole on Management PC

Lab Objectives

- Install SmartConsole on MGMT PC

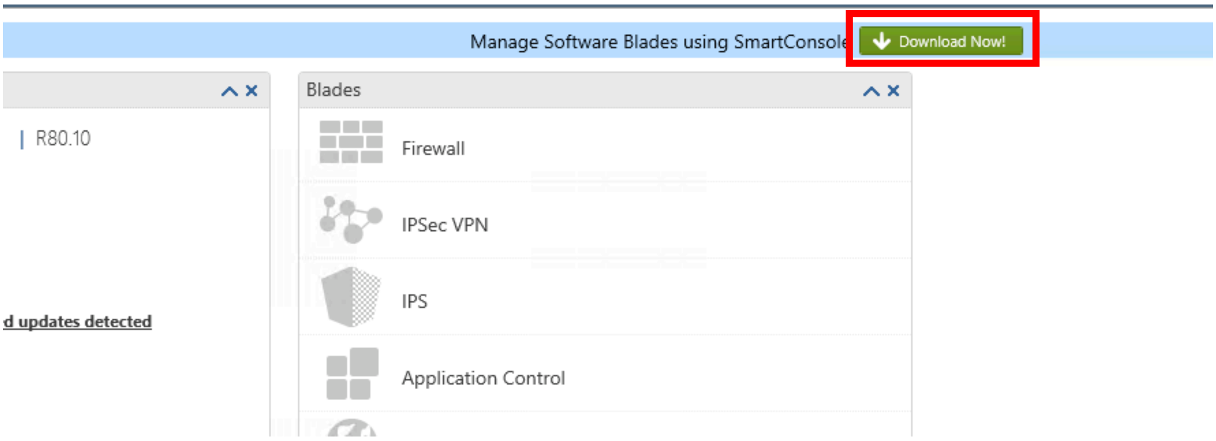
In this lab you will install SmartConsole applications package. Before we start the installation, we need the software package available on the Management station. The good news is that you can download the SmartConsole package straight from the Web UI package. Please login to Web UI page by navigating to NY-SMS-1 https://10.0.0.100 web page.

Once logged in, you can initiate the software download in one of the following ways. Select **Overview** menu

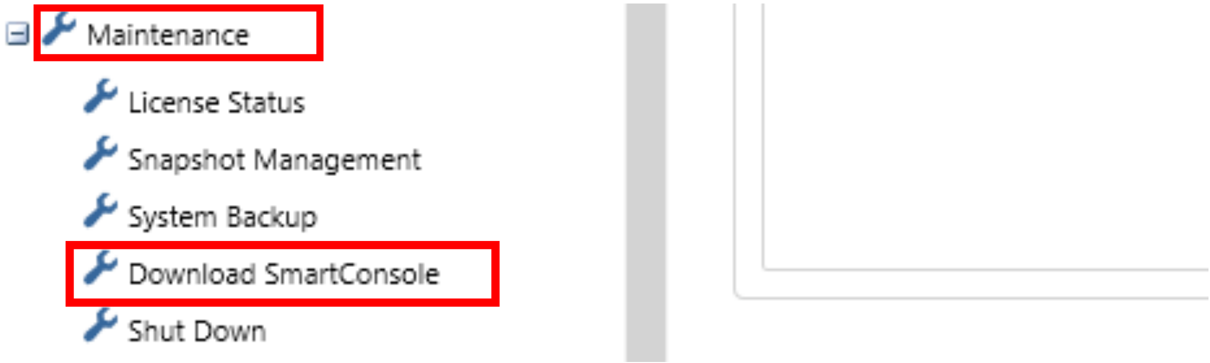


Kernel: 2.6.18-92cpx86_64
Edition: 64-bit
Build Number: 421
System Uptime: 41 minutes
Software Updates: no new recommended updates detected

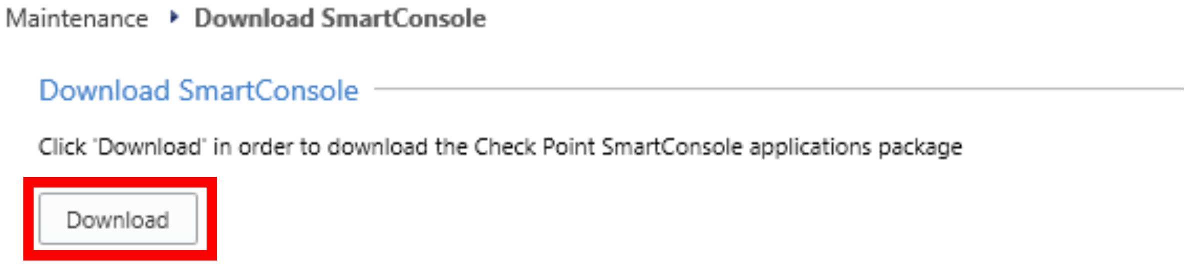
and the **Download Now!** button is available at the top of the page :



The second option is available if you navigate on the left menu down to **Maintenance** submenu. Click on **Maintenance,** then click on **Download SmartConsole:**



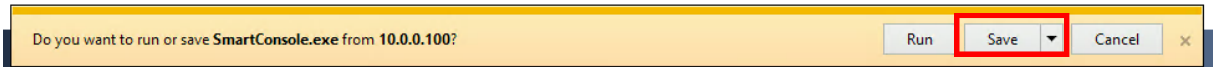
At the top, on the right-side of the page, the **Download** button is available in order to download SmartConsole applications package.



Click 'Download' in order to download the Check Point SmartConsole applications package

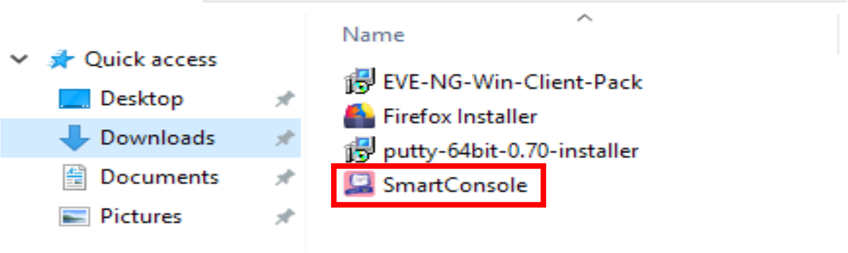
Whatever option you choose, please initiate download now, so that we can continue with software installation afterwards.

Click **Save** in order to save the software locally on the management PC.

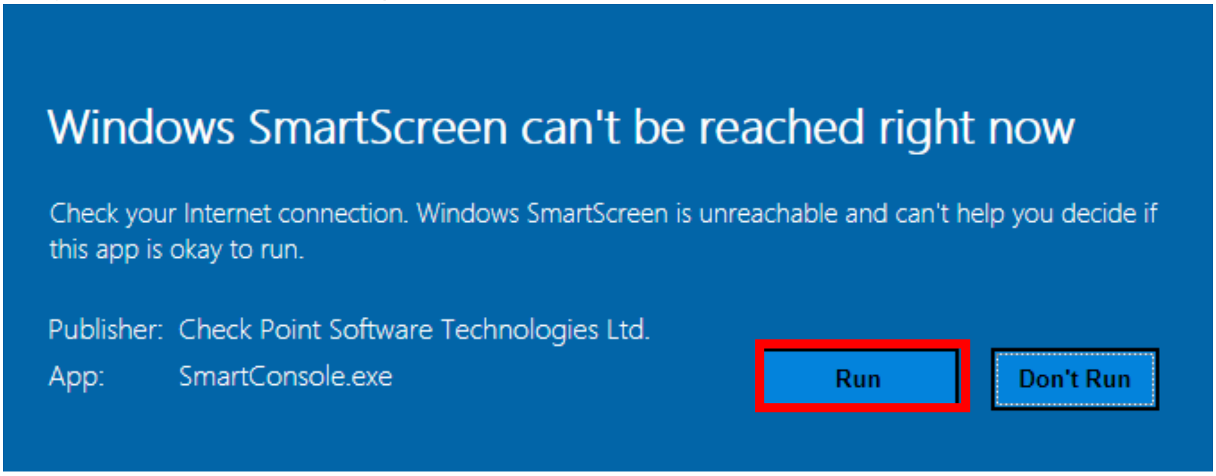


Do you want to run or save **SmartConsole.exe** from **10.0.0.100**?

Navigate to the Downloads folder on the Management PC and double-click **SmartConsole** application:



Depending on what Windows OS you are running on the management PC, you may receive the following screen:



Windows SmartScreen can't be reached right now

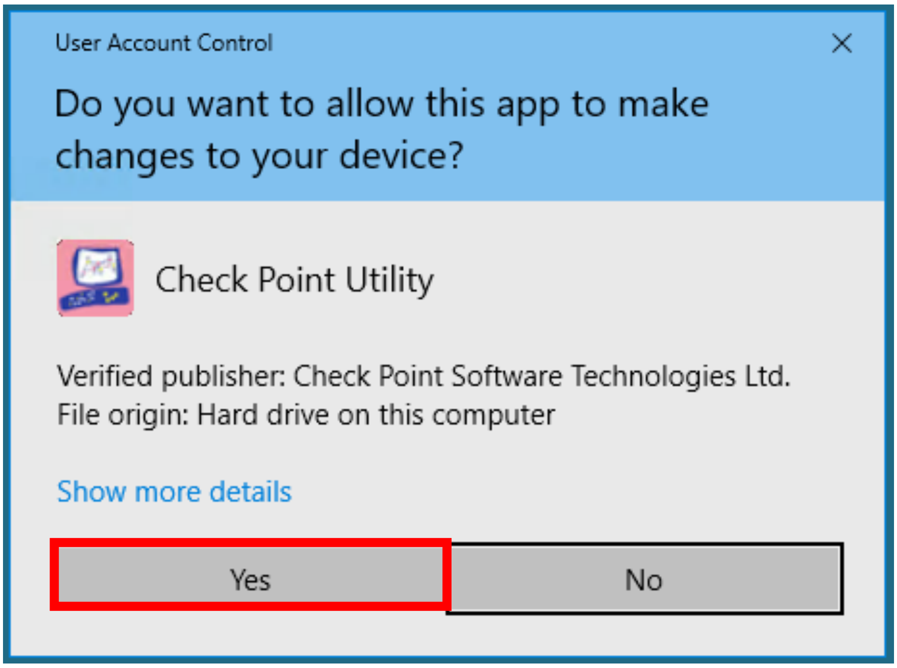
Check your Internet connection. Windows SmartScreen is unreachable and can't help you decide if this app is okay to run.

Publisher: Check Point Software Technologies Ltd.

App: SmartConsole.exe

If this is the case, please click **Run** and continue with the installation.

Installation will now start, files will be verified and extracted. If you are using Windows10, you may receive the following screen:



User Account Control

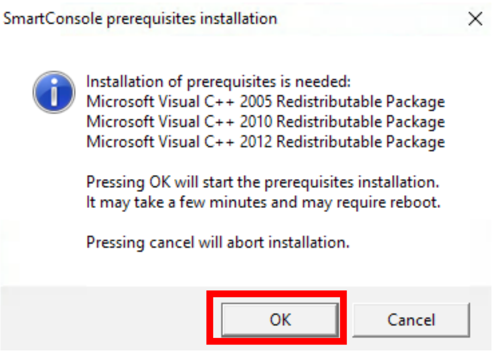
Do you want to allow this app to make changes to your device?

Check Point Utility

Verified publisher: Check Point Software Technologies Ltd.
File origin: Hard drive on this computer

Please select **Yes** and continue with the installation.

Next, SmartConsole prerequisites are being displayed. Please select **OK** in order to continue with the software installation.



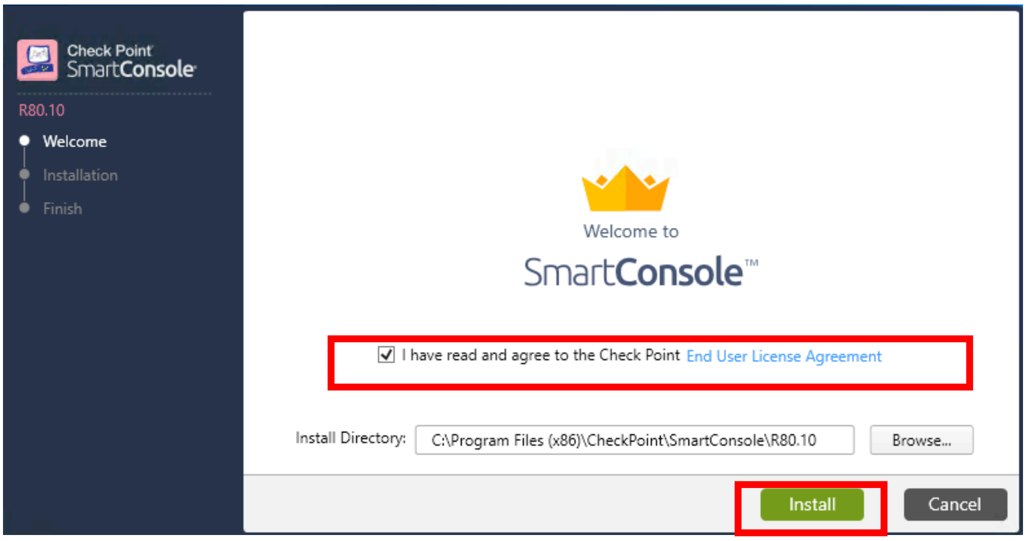
SmartConsole prerequisites installation

Installation of prerequisites is needed:
Microsoft Visual C++ 2005 Redistributable Package
Microsoft Visual C++ 2010 Redistributable Package
Microsoft Visual C++ 2012 Redistributable Package

Pressing OK will start the prerequisites installation.
It may take a few minutes and may require reboot.

Pressing cancel will abort installation.

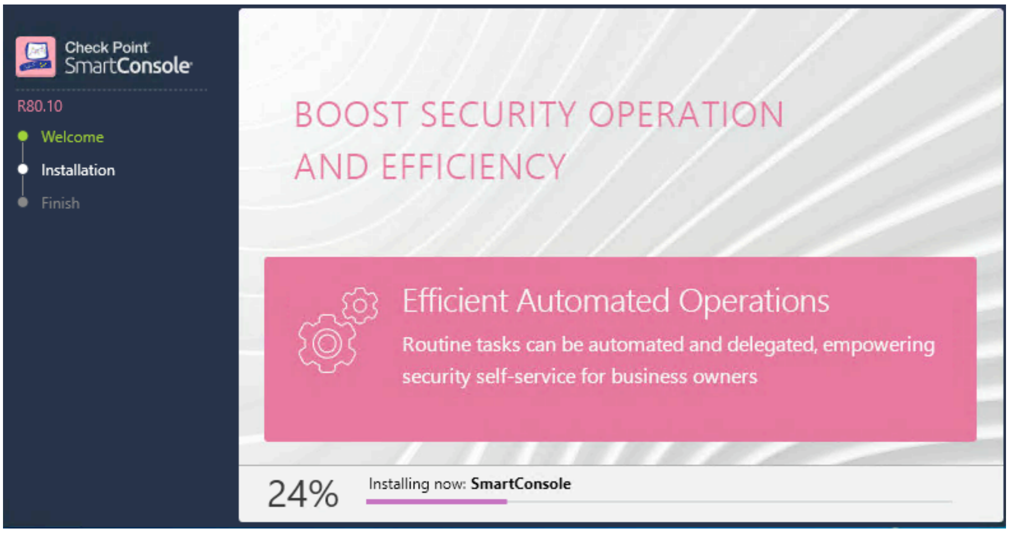
Microsoft Visual C++ packages are being installed now and the next screen will ask you where do you want SmartConsole to be installed. Please leave installation path as it is, confirm that you have read and you agree Check Point EULA by ticking the box and click the **Install** button:



☑ I have read and agree to the Check Point End User License Agreement

Install Directory: C:\Program Files (x86)\CheckPoint\SmartConsole\R80.10

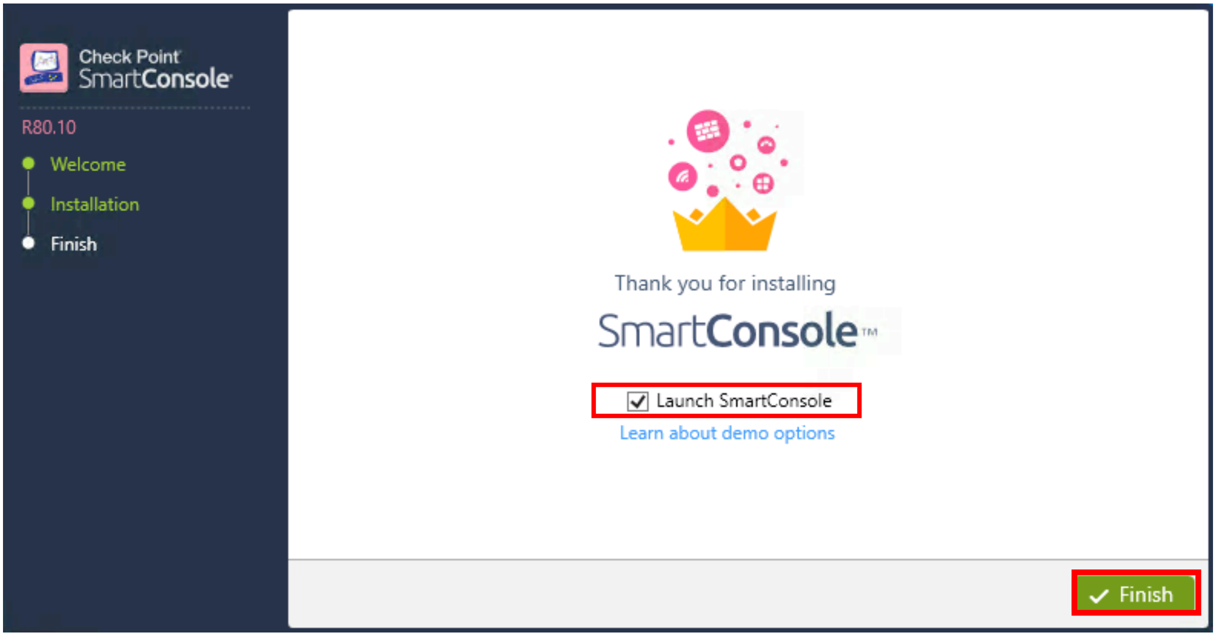
Installation is now in progress and it will last between 5 to 10 minutes, depending on the hardware performance you are running the lab on.



Check Point SmartConsole
R80.10
Welcome
Installation
Finish
BOOST SECURITY OPERATION AND EFFICIENCY
Efficient Automated Operations
Routine tasks can be automated and delegated, empowering security self-service for business owners

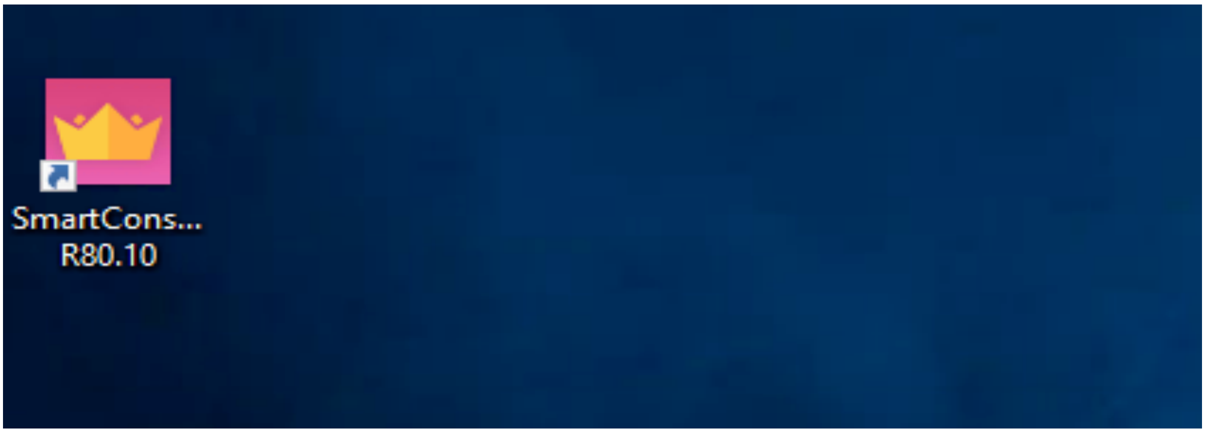
24% Installing now: SmartConsole

Once the installation is completed, you will be presented with a final screen:



Unselect **Launch SmartConsole** and click **Finish** button.

A shortcut icon will be delivered on your Desktop. We will manually launch SmartConsole application in the next lab when we will add NY-FW-1 Security Gateway to NY-SMS-1 Security Management Server.

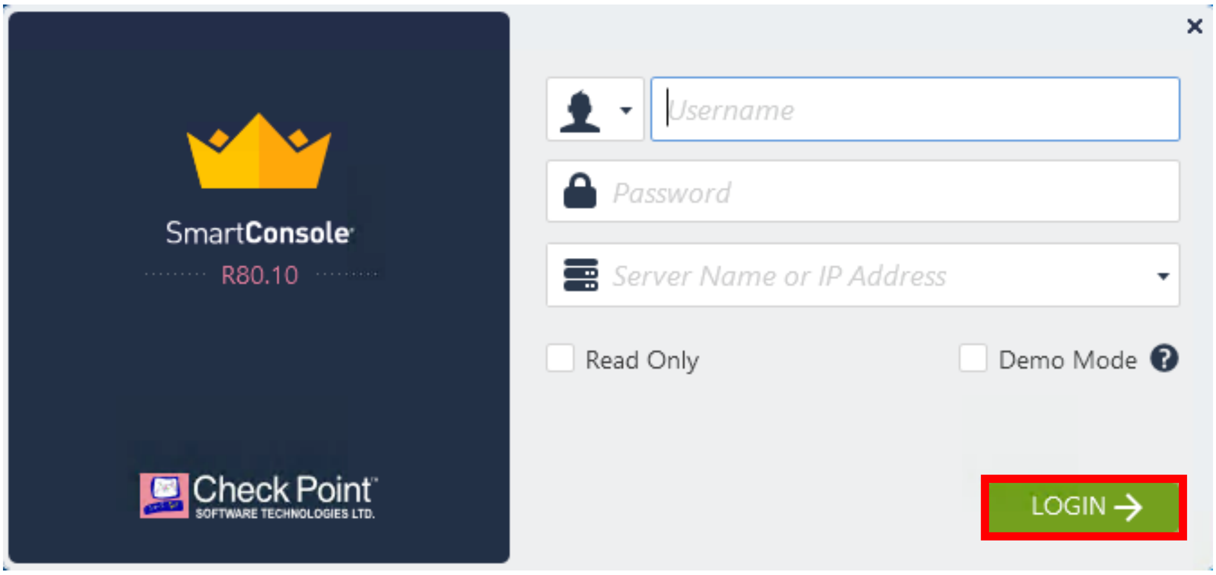


14.0 Lab: Add NY-FW-1 Security Gateway to NY-SMS-1 Security Management Server

Lab Objectives

- Learn how to add Security Gateways to the Security Management Server

Let's start and first launch the SmartConsole application. Please double-click the SmartConsole application and the following screen will be displayed:

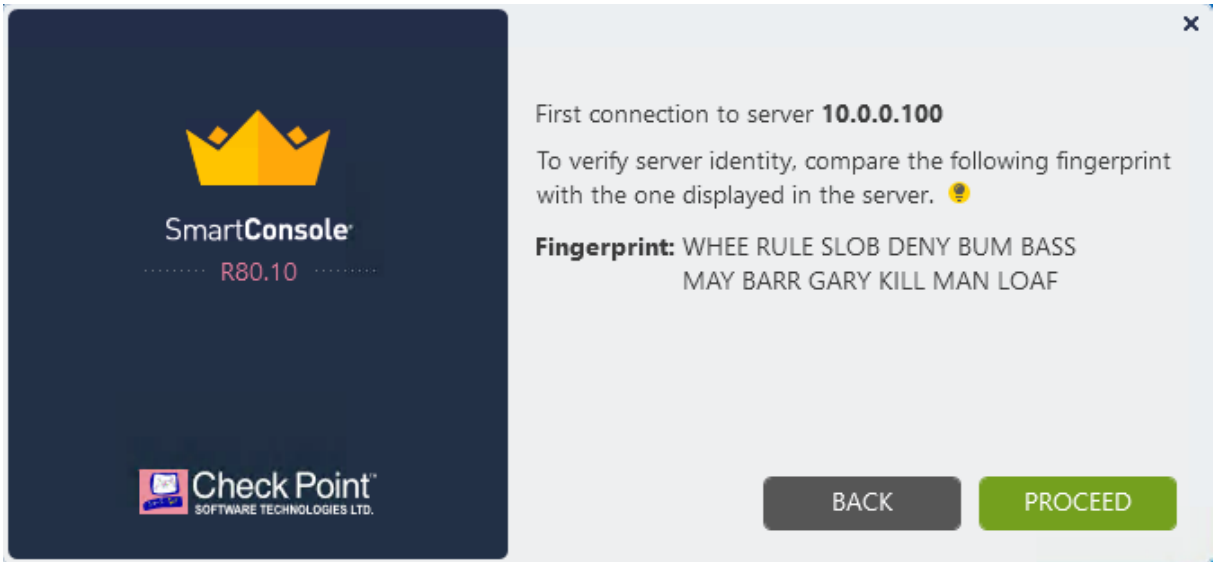


Please fill in the following details and click **LOGIN** in order to connect to NY-SMS-1 Security Management Server.

Parameter	Value
Username	admin
Password	admin123
Server Name or IP Address	10.0.0.100

Because this is your first time when you are connecting to the NY-SMS-1 management server, you are now being presented a Certificate Fingerprint. What is the purpose of this ?

Imagine the following scenario. You want to make sure that you are connecting indeed to your security management server and you are not a victim of a man-in-the-middle attack. Simply put, your session has not been hijacked and you are not filling in the authentication credentials so that a potential attacker steals these credentials. In order to make sure you are on the safe side, you can do a verification in this step.



First connection to server **10.0.0.100**

To verify server identity, compare the following fingerprint with the one displayed in the server.

Fingerprint: WHEE RULE SLOB DENY BUM BASS
MAY BARR GARY KILL MAN LOAF

Login on the NY-SMS-1 CLI console and run the **cpconfig** command while in **clish** mode, no need to navigate to **expert** mode:

```
NY-SMS-1> cpconfig
This program will let you re-configure
your Check Point Security Management Server configuration.


Configuration Options:
----------------------
(1)  Licenses and contracts
(2)  Administrator
(3)  GUI Clients
(4)  SNMP Extension
(5)  Random Pool
(6)  Certificate Authority
(7)  Certificate's Fingerprint
(8)  Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

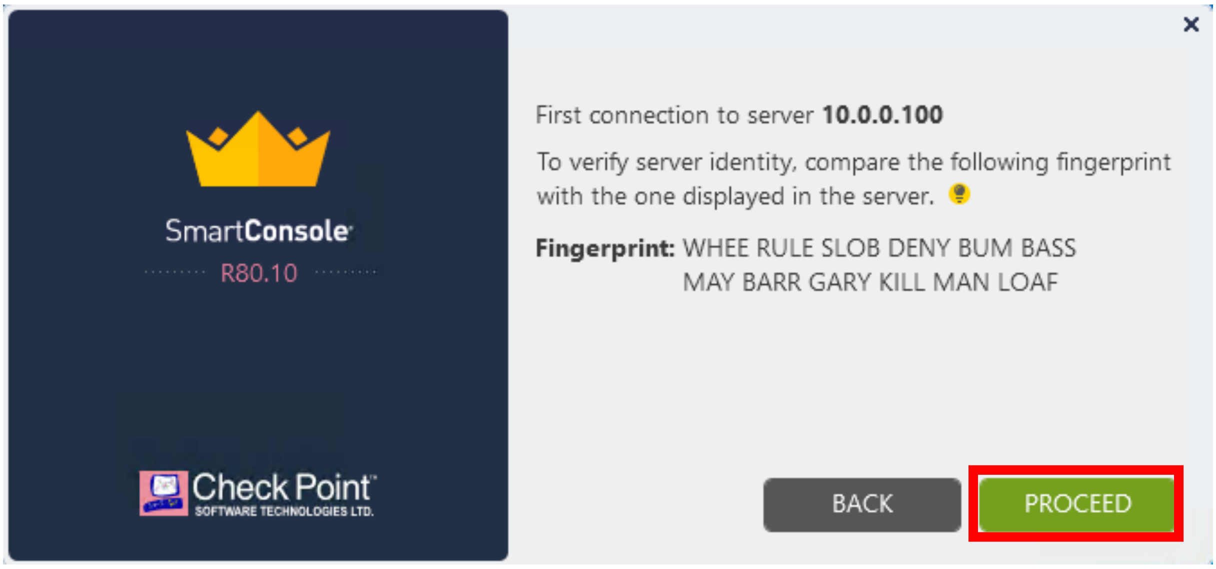
Type **7** and hit **enter:**

```
Enter your choice (1-9) :7



Configuring Certificate's Fingerprint...
========================================
The following text is the fingerprint of this Security Management Server:
WHEE RULE SLOB DENY BUM BASS MAY BARR GARY KILL MAN LOAF

Do you want to save it to a file? (y/n) [n] ?
```

You can now compare the two fingerprints, the one that SMS is presenting in the CLI and the one that you get in the SmartConsole, while connecting for the first time to the management server. This is how you verify that you are connecting to the management server that you think you are.
Type **n** as we don’t need to save the fingerprint and then type **9** in order to exit **cpconfig** menu.

```
Do you want to save it to a file? (y/n) [n] ? n

Configuration Options:
---------------------
(1)  Licenses and contracts
(2)  Administrator
(3)  GUI Clients
(4)  SNMP Extension
(5)  Random Pool
(6)  Certificate Authority
(7)  Certificate's Fingerprint
(8)  Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :9

Thank You...
NY-SMS-1>
```

As the fingerprint is the same as per our validation, please click **PROCEED:**

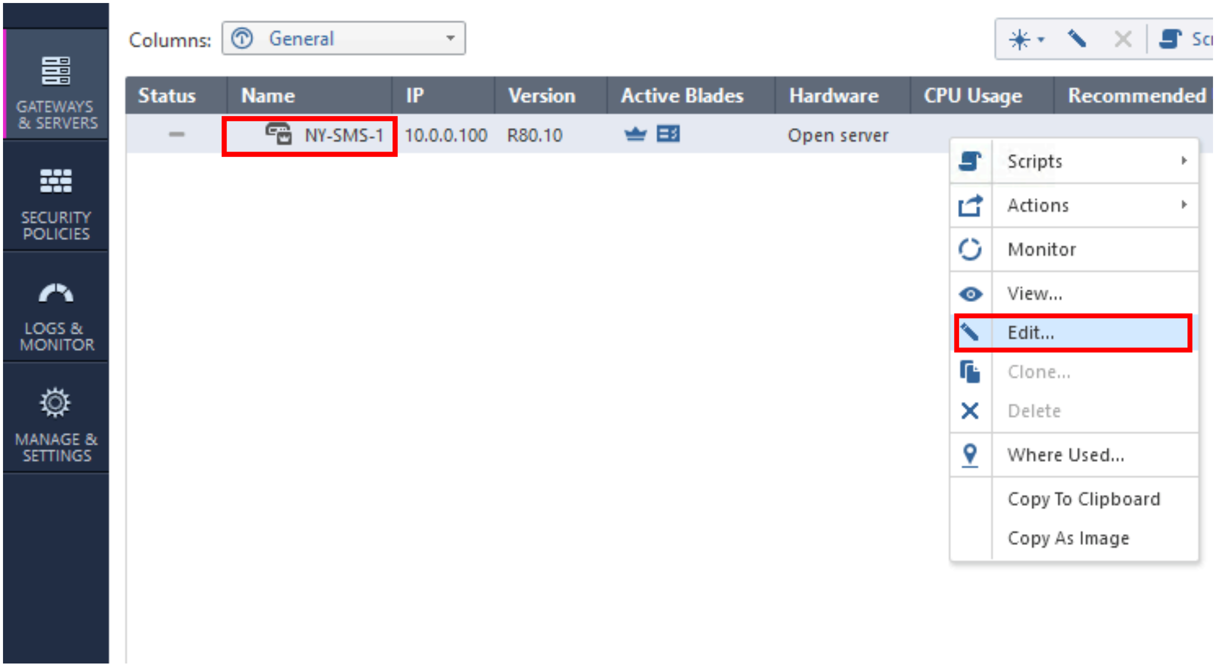


First connection to server **10.0.0.100**

To verify server identity, compare the following fingerprint with the one displayed in the server.

Fingerprint: WHEE RULE SLOB DENY BUM BASS MAY BARR GARY KILL MAN LOAF

Before we actually add NY-FW-1 security gateway to the SMS, let's first activate some important functionalities on the Management Server.
While in **Gateways and Servers** menu, double-click NY-SMS-1 in the list or right-click it and select **Edit**:



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended
—	NY-SMS-1	10.0.0.100	R80.10		Open server		

In order to have a powerful, fast and useful management server, we need to enable two functionalities:

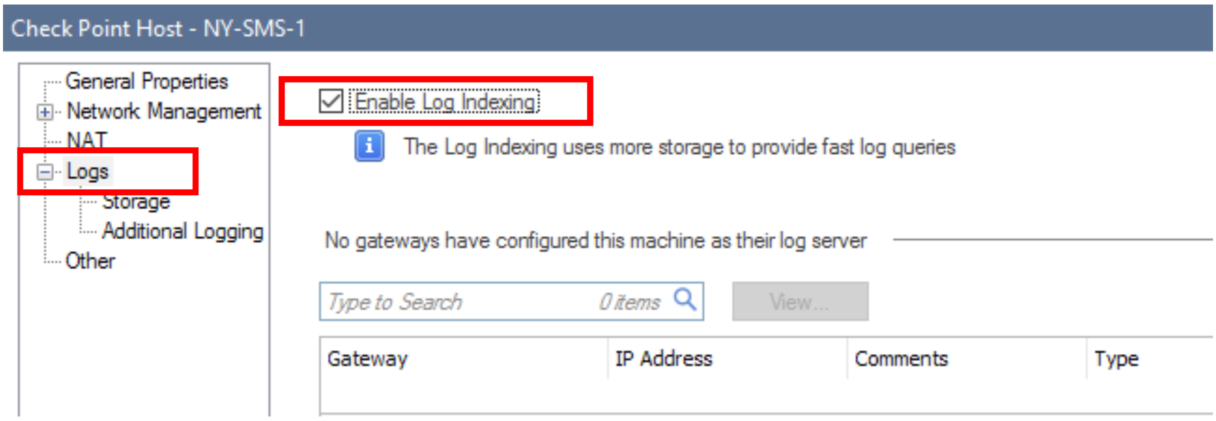
- Log Indexer
- SmartEvent server and Correlation Unit

Log Indexer will use more storage for the logs it receives from the security gateways , but will "organize" them in a way that will provide faster results when running queries in the logs. Simply said, you will wait less time when searching events in the logs by activating **Log Indexer**.

The second functionality is related to **SmartEvent**. We have gone through the Software Blades in Module 1 and briefly touched on each and every one available. We will activare SmartEvent functionalities now.

Activating SmartEvent functionalities, the Security Management Server will be able to correlate events from logs that it receives from the firewalls (security gateways). This means that only meaningful information will be provided and displayed to the IT Administrator of the system.

Let's now activate these two functionalities. Navigate to **Logs** menu and select on the right-side **Enable Log Indexing:**


Check Point Host - NY-SMS-1

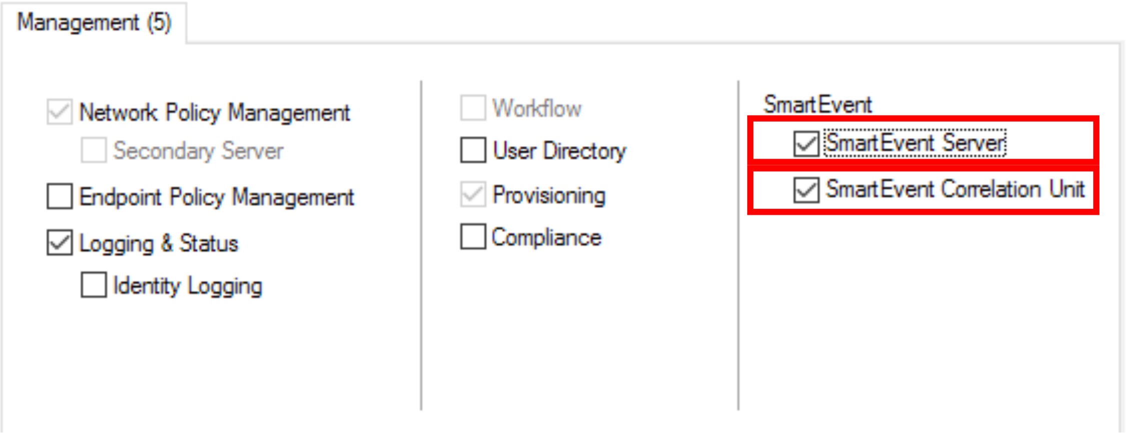
☑ Enable Log Indexing

The Log Indexing uses more storage to provide fast log queries

No gateways have configured this machine as their log server

Gateway	IP Address	Comments	Type

Next, navigate to **General Properties** and select the two options under **SmartEvent** category:

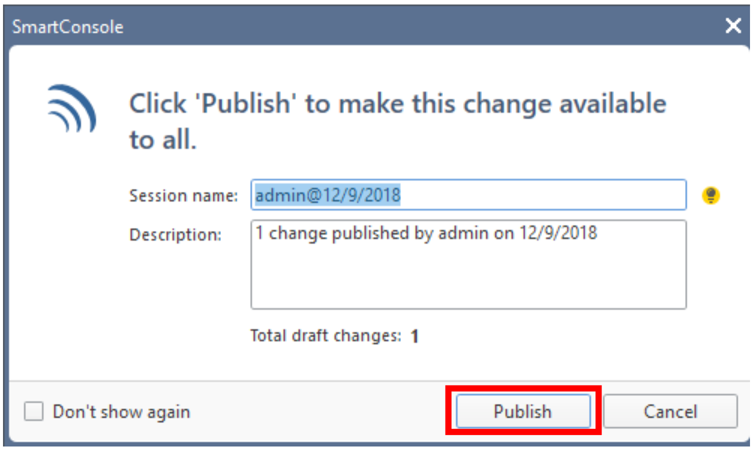

Management (5)

☑ Network Policy Management
□ Secondary Server
□ Endpoint Policy Management
☑ Logging & Status
□ Identity Logging

□ Workflow
□ User Directory
☑ Provisioning
□ Compliance

SmartEvent
☑ SmartEvent Server
☑ SmartEvent Correlation Unit

Click **OK.** In order to save changes, click **Publish** in the top-middle button and then click **Publish** in the screen that is displayed.



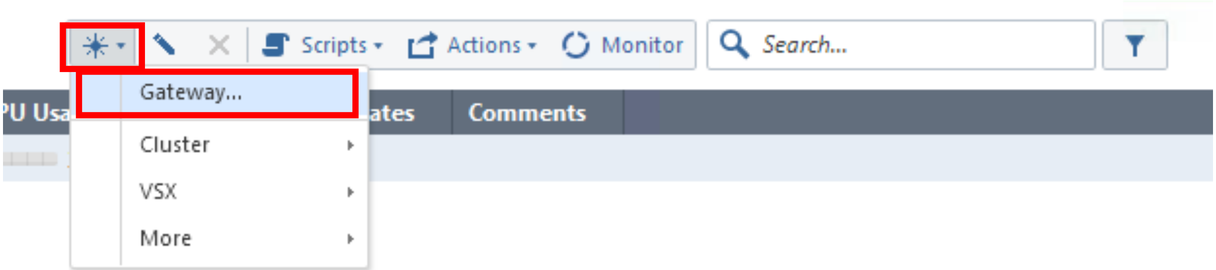
Click 'Publish' to make this change available to all.

Session name: admin@12/9/2018

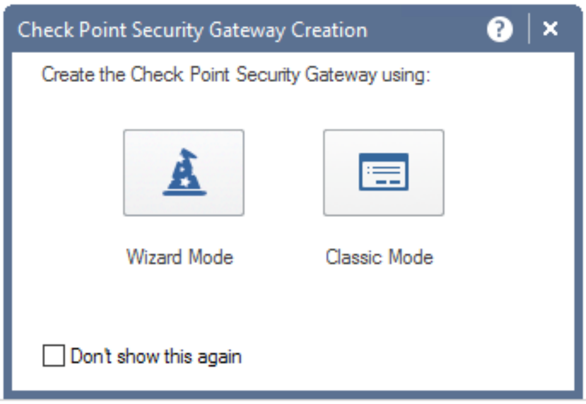
Description: 1 change published by admin on 12/9/2018

Total draft changes: 1

Let’s now add our first gateway in the management server. On the top-middle bar, click on **New** button and then click on **Gateway.**



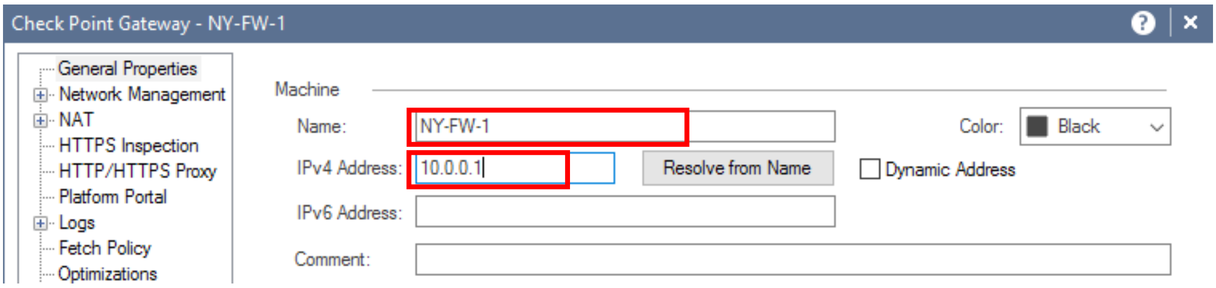
Select **Classic Mode**. We will add the London L-FW-1 in a later lab using **Wizard Mode**.



Create the Check Point Security Gateway using:

Fill in necessary details as follows:

Parameter	Value
Name	NY-FW-1
IPv4 Address	10.0.0.1



Check Point Gateway - NY-FW-1

Name: NY-FW-1

IPv4 Address: 10.0.0.1

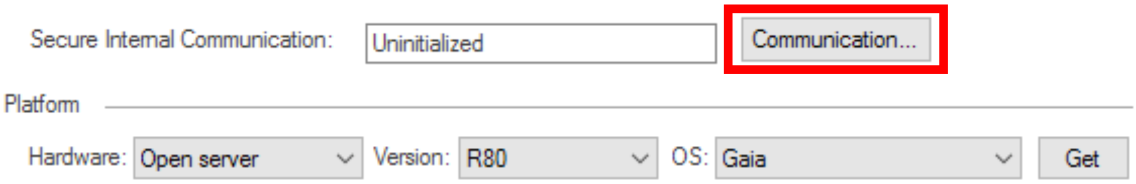
IPv6 Address:

Comment:

Color: Black

□ Dynamic Address

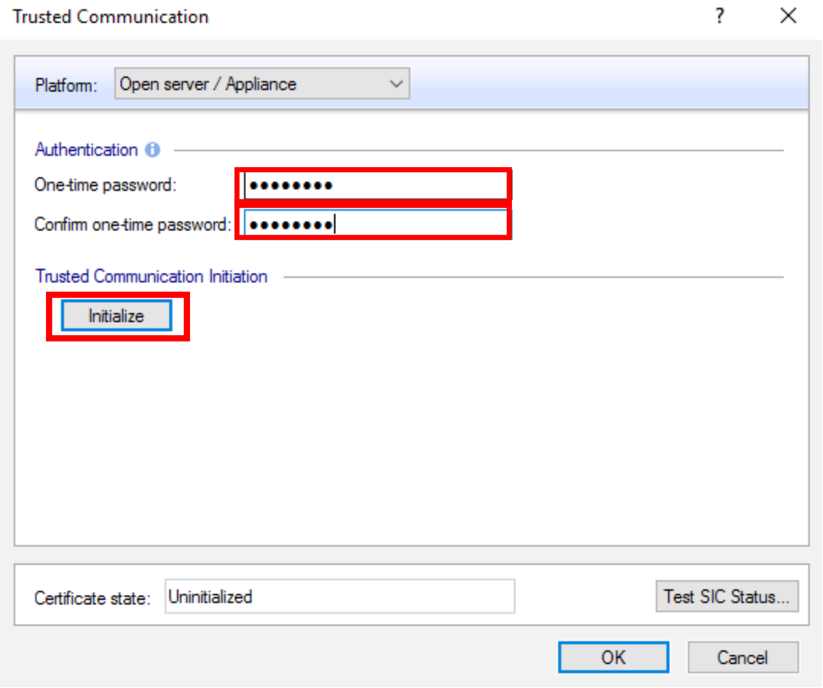
Now, let's establish Secure Internal Communication or SIC between SMS and the Security Gateway. Click **Communication** button



Secure Internal Communication: Uninitialized

Hardware: Open server Version: R80 OS: Gaia

and the following screen is displayed:



Trusted Communication

Platform: Open server / Appliance

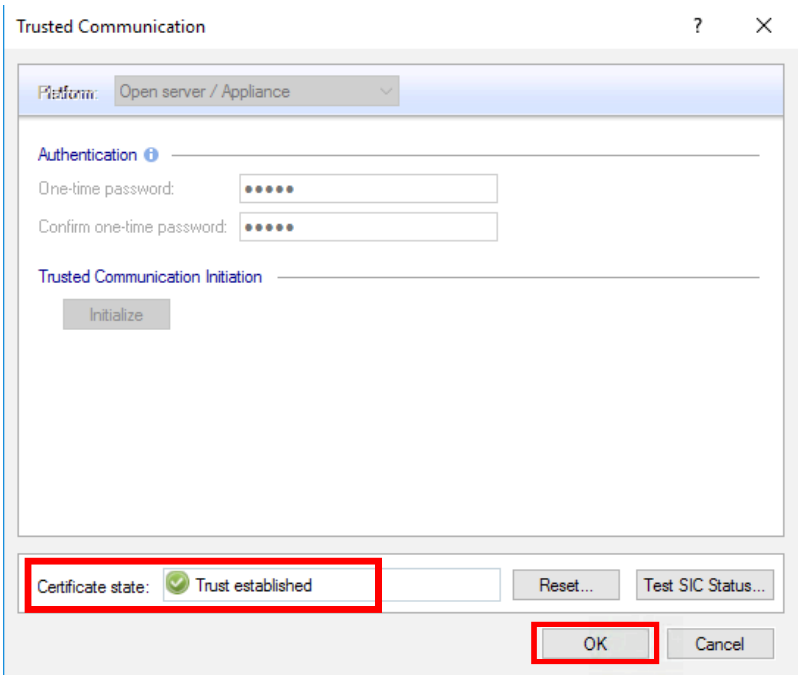
One-time password: ••••••••

Confirm one-time password: ••••••••

Certificate state: Uninitialized

Please type the password **admin123** in both fields and then click **Initialize**.

After the one-time password is being used, the Security Management Server and the new added Security Gateway will authenticate themselves using digital certificates, with the SMS acting as the CA. Please note that now, once SIC is established, the Trust state changes to Established.



Trusted Communication

Platform: Open server / Appliance

Authentication

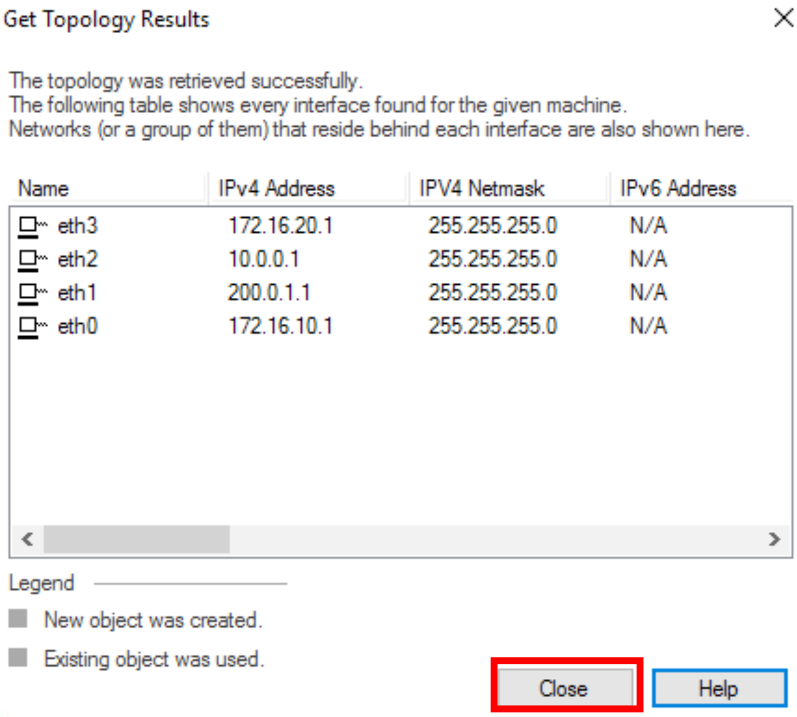
One-time password: •••••

Confirm one-time password: •••••

Trusted Communication Initiation

Certificate state: Trust established

Click **OK**. Please note that the SMS will import the SG interface configuration at this point. This is the reason I mentioned in previous lectures that interfaces and associated IP addresses need to be configured before enrolling the gateway in the SMS. A topology overview is displayed now:



Get Topology Results

The topology was retrieved successfully.
The following table shows every interface found for the given machine.
Networks (or a group of them) that reside behind each interface are also shown here.

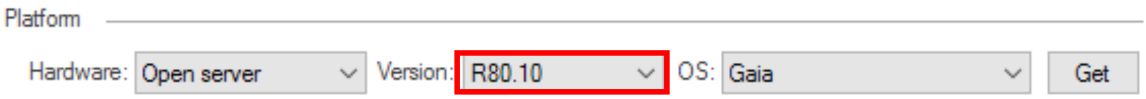
Name	IPv4 Address	IPV4 Netmask	IPv6 Address
eth3	172.16.20.1	255.255.255.0	N/A
eth2	10.0.0.1	255.255.255.0	N/A
eth1	200.0.1.1	255.255.255.0	N/A
eth0	172.16.10.1	255.255.255.0	N/A

Legend

▨ New object was created.

▨ Existing object was used.

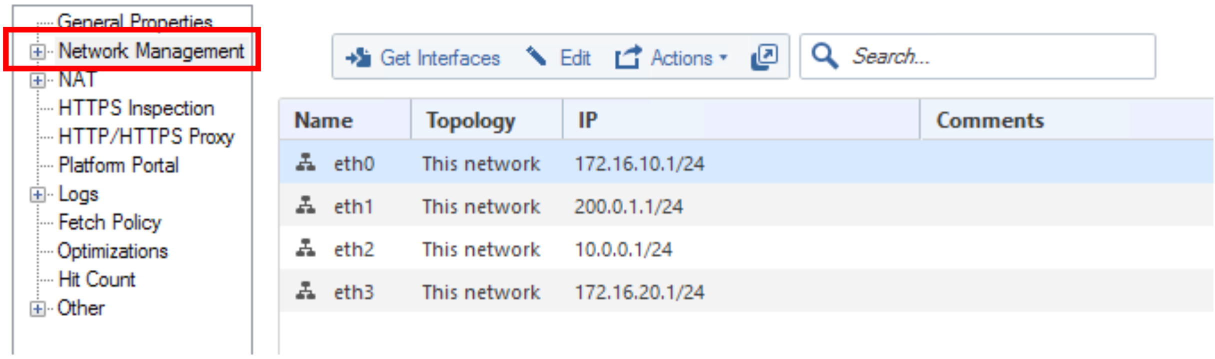
Click **Close.** Please note that now, when communication is established between SMS and SG, we can see that version has been updated to the correct one. R80 was presented generic, now R80.10 is displayed:



Platform

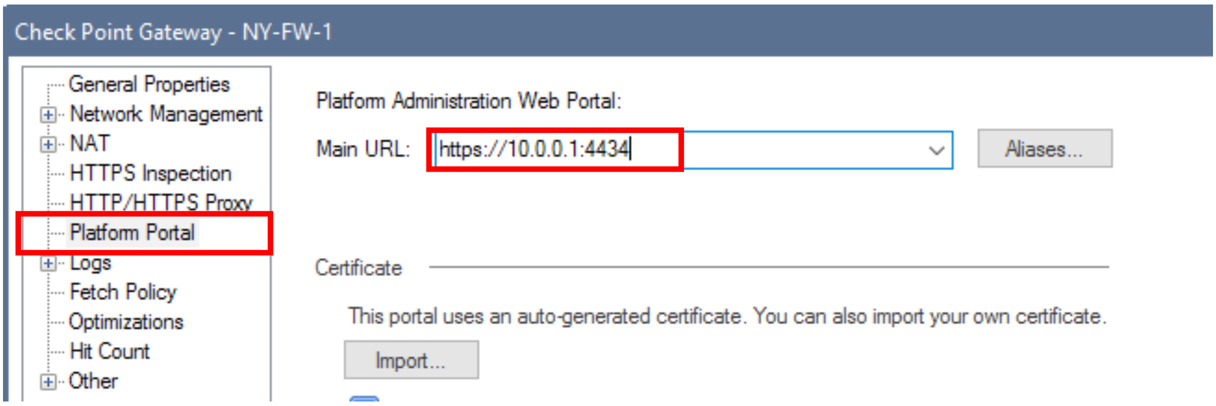
Hardware: Open server Version: R80.10 OS: Gaia

Also, if you click on **Network Management** menu, you can verify that correct interfaces information has been imported correctly.



Name	Topology	IP	Comments
eth0	This network	172.16.10.1/24	
eth1	This network	200.0.1.1/24	
eth2	This network	10.0.0.1/24	
eth3	This network	172.16.20.1/24	

If you navigate to **Platform Portal**, you can modify the default portal. Currently, the appliance can be accessed through https protocol, using default port. This behaviour can be changed if we want or need to. For example, we could say that Web UI is accessible through https protocol, but on custom port 4434. In this case, we would modify the link as follows:



Check Point Gateway - NY-FW-1

Platform Administration Web Portal:

Main URL: https://10.0.0.1:4434

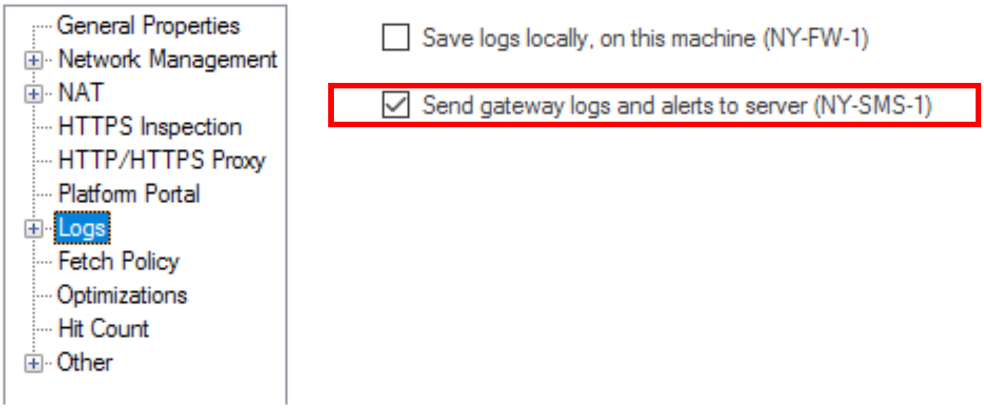
Certificate

This portal uses an auto-generated certificate. You can also import your own certificate.

Please remove 4434 port number and leave the link as it was initially.

Now, navigate on **Logs** menu. You will validate the default behaviour of logs storage and analysis.

Ok, as expected, logs are by default sent to the Security Management Server (SMS), where they are stored and analysed by the SmartEvent server.



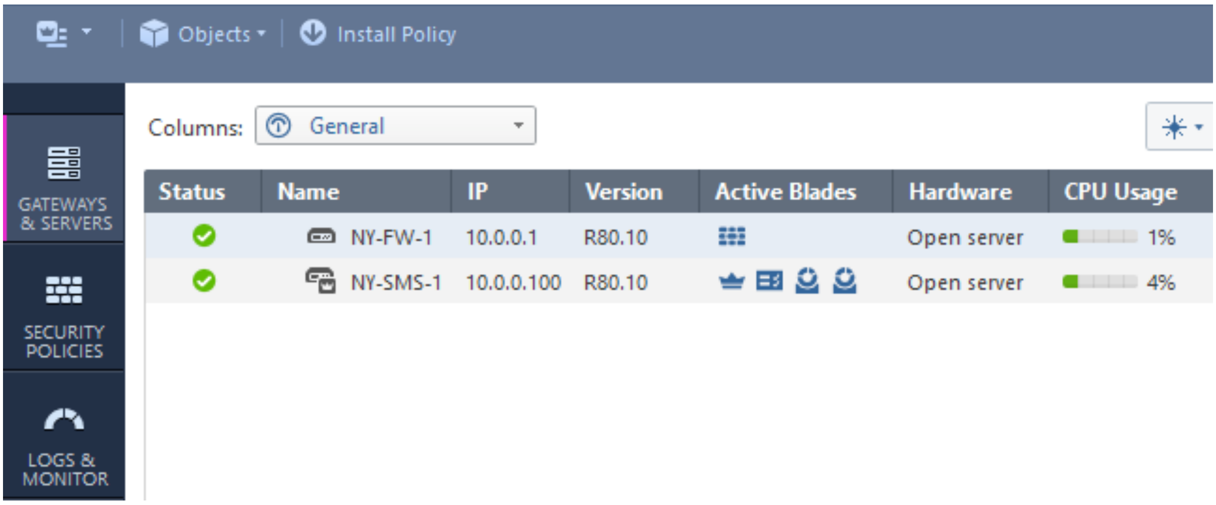
□ Save logs locally, on this machine (NY-FW-1)

☑ Send gateway logs and alerts to server (NY-SMS-1)

The other menus will be discussed, as needed, in later labs as we progress with the course.

Click **OK** and **Publish** changes, just like earlier in this lab.

As of now, we have two appliances listed in the **Gateways & Servers** list:

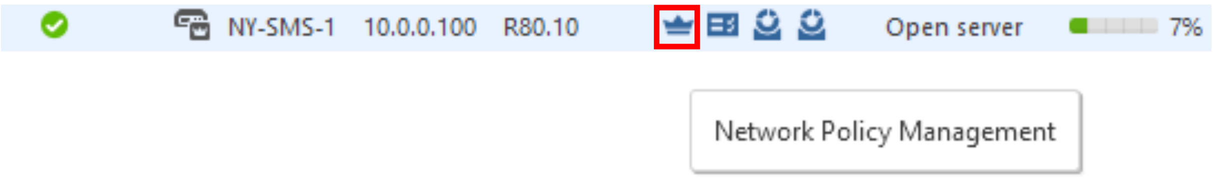


Columns: General

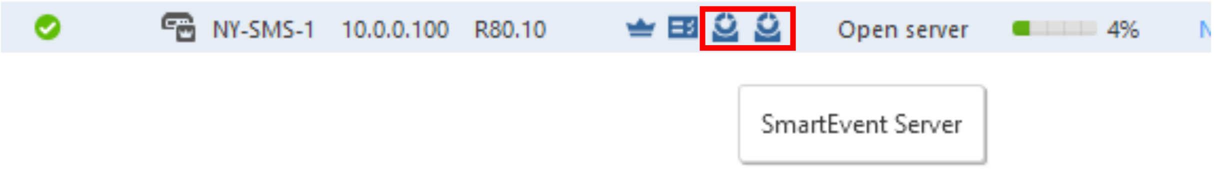
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage
✓	NY-FW-1	10.0.0.1	R80.10		Open server	1%
✓	NY-SMS-1	10.0.0.100	R80.10		Open server	4%

How could someone distinguish between the two if the naming of these appliances would be unknown to that person? How can you know who is the SMS and who is the SG ?

Please take a look at the **Active Blades** column. If you hover your mouse cursor over the first icon, then information is displayed about that specific Software Blade . The **Network Policy Management** blade is active only on the SMS server – where are policies defined and later pushed on the SGs.



The same applies for 3rd and 4th icons which refer to SmartEvent server and Correlation Unit.



15.0 Lab: Reset SIC between NY-SMS-1 and NY-FW-1

Lab Objectives

- Learn how to reset and re-establish SIC between SMS and SGs if SIC OTP or certificates have been leaked

If the SIC one-time password (OTP) or the certificates get leaked, the trust state is compromised. The SIC must be reset and re-established and has to be performed on both sides, the SMS and the SGs.
The SMS also acts as a CA and provides certificates for authentication after using OTP. When SIC is reset, the SMS will revoke the certificate of the specific SG and will store this information in a list. This list is called the CRL – Certificate Revocation List and is basically a list of revoked certificates.

Always try to ask yourself questions while studying a new technology. This will help you better understand the new topic and the information will stay with you for a longer time. So, why is the CRL list important and what's its role ?
The CRL list is sent to all enrolled gateways with the SMS and if the CRL list is not the same on the two respective gateways, well, the two gateways cannot trust each other (authenticate) and, as an example, they will not establish site-to-site VPN.

Let's now reset the trust state and learn how to re-establish it with a "new" OTP. Actually, we will use the same OTP, but imagine that a new OTP will be used, just as if we needed to change it in a real world scenario.

Connect to NY-FW-1 clish console and type the **cpconfig** command. Type **5** and hit enter:

```
NY-FW-1> cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1)  Licenses and contracts
(2)  SNMP Extension
(3)  PKCS#11 Token
(4)  Random Pool
(5)  Secure Internal Communication

Enter your choice (1-10) :5
```

```
Configuring Secure Internal Communication...
==============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Trust established

 Would you like re-initialize communication? (y/n) [n] ? y
```

Type **y** in order to re-initialize the SIC communication, and then type **y** again.

```
Note: The Secure Internal Communication will be reset now,
and all Check Point Services will be stopped (cpstop).
No communication will be possible until you reset and
re-initialize the communication properly!
Are you sure? (y/n) [n] ? y
Enter Activation Key: admin123
Retype Activation Key:admin123
```

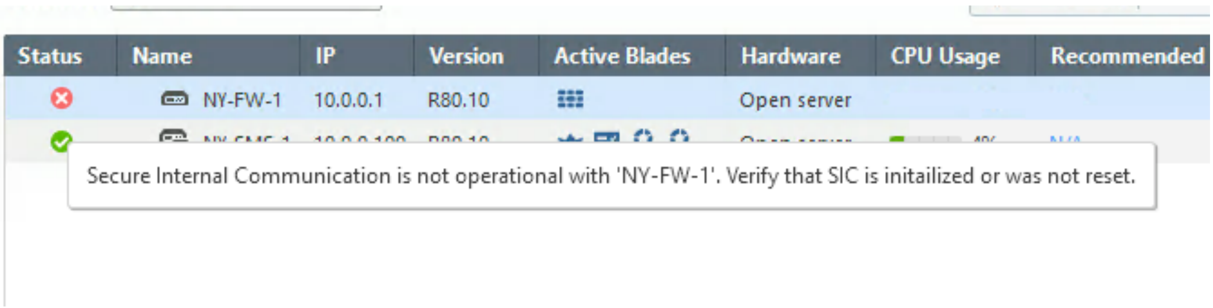
SIC has been reset successfully. Type **10** in order to exit the **cpconfig** menu and hit **enter**.

```
The Secure Internal Communication was successfully initialized


Configuration Options:
----------------------
(1)  Licenses and contracts
(2)  SNMP Extension
(3)  PKCS#11 Token
(4)  Random Pool
(5)  Secure Internal Communication
(6)  Enable cluster membership for this gateway
(7)  Disable Check Point SecureXL
(8)  Check Point CoreXL
(9)  Automatic start of Check Point Products

(10) Exit

Enter your choice (1-10) :10
```

Right after you hit enter, all processes are stopped and then restarted on the Security Gateway.

```
Thank You...
cpwd_admin:
Process DASERVICE terminated
Mobile Access: Stopping MoveFileDemuxer service (if needed)
Mobile Access: MoveFileDemuxer is not running
Mobile Access: Mobile Access blade is disabled or already shut down
Mobile Access: Push notification is disabled or already shut down
Mobile Access: Reverse Proxy for HTTP traffic is disabled or already shut down.
Mobile Access: Reverse Proxy for HTTPS traffic is disabled or already shut down.
Mobile Access: Successfully stopped Mobile Access services
Stopping SmartView Monitor daemon ...
SmartView Monitor daemon is not running
Stopping SmartView Monitor kernel ...
Driver 0 is already down
Driver 1 is already down
SmartView Monitor kernel stopped
rtmstop: SmartView Monitor kernel is not loaded
FloodGate-1 is already stopped.
Stopping sessions database
VPN-1/FW-1 stopped

<output omitted>

FireWall-1: Starting fwd

Process DASERVICE started successfully (pid=4415)
cpridstop: cprid watchdog stopped
cpridstop: cprid stopped
cpridstart: Starting cprid
NY-FW-1>
```

Now, connect to SmartConsole in order to reset SIC from the SMS side. Before we reset the SIC, please take note at the NY-FW-1 object and observe the error message. In the Status column, the NY-FW-1 is marked with a red cross and if you hover your mouse over this, a self-explanatory message is displayed.



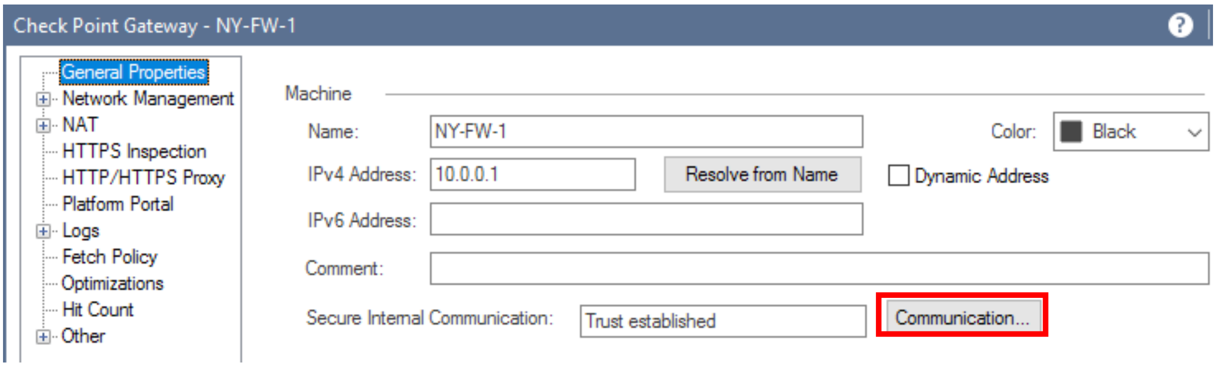
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended
☒	NY-FW-1	10.0.0.1	R80.10		Open server		
✓	NY-SMS-1	10.0.0.100	R80.10		Open server	4%	N/A

Secure Internal Communication is not operational with 'NY-FW-1'. Verify that SIC is initailized or was not reset.

SIC is not operational with NY-FW-1. Verify that SIC is initialized or was not reset.

Now, let's reset SIC from the SMS side. Double-click or right-click on the NY-FW-1 gateway object in the list and select **Edit menu.**

Click on **Communication** button.



Check Point Gateway - NY-FW-1

Machine

Name: NY-FW-1

IPv4 Address: 10.0.0.1

IPv6 Address:

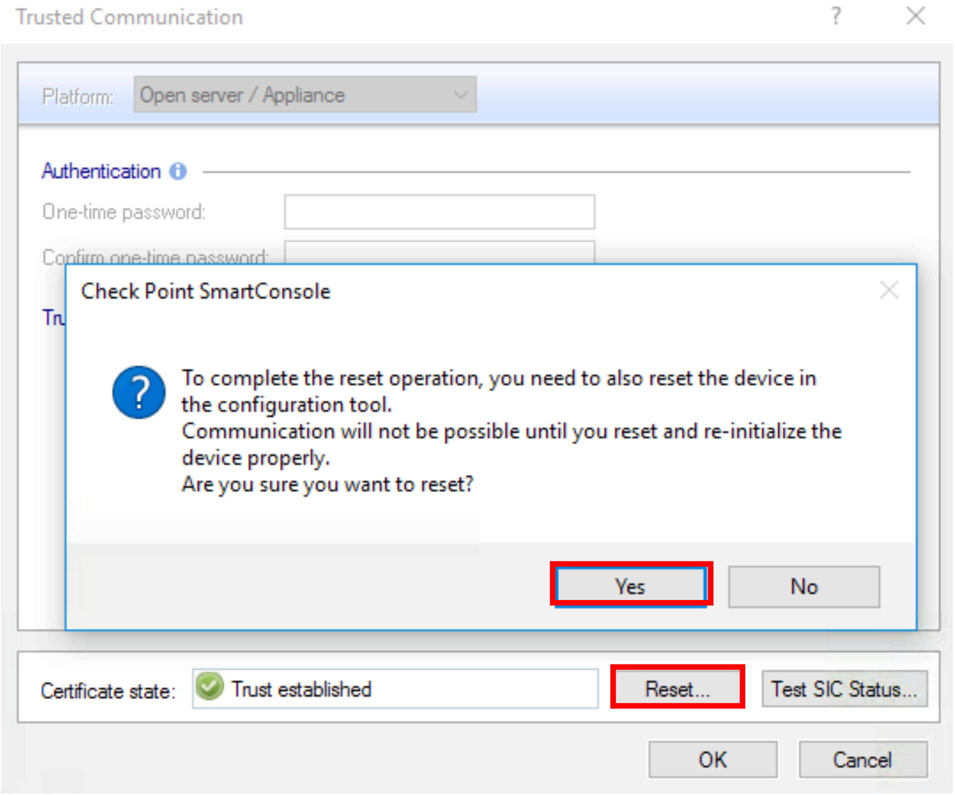
Comment:

Color: Black

□ Dynamic Address

Secure Internal Communication: Trust established

The **Trusted Communication** screen is displayed. Click on **Reset** and then click on **Yes**.



Trusted Communication

Platform: Open server / Appliance

Authentication

One-time password:

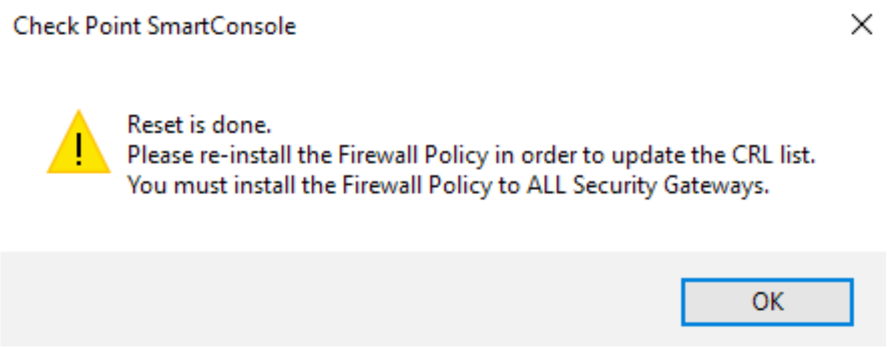
Confirm one-time password:

Check Point SmartConsole

To complete the reset operation, you need to also reset the device in the configuration tool.
Communication will not be possible until you reset and re-initialize the device properly.
Are you sure you want to reset?

Certificate state: Trust established

Please take note about the message displayed :

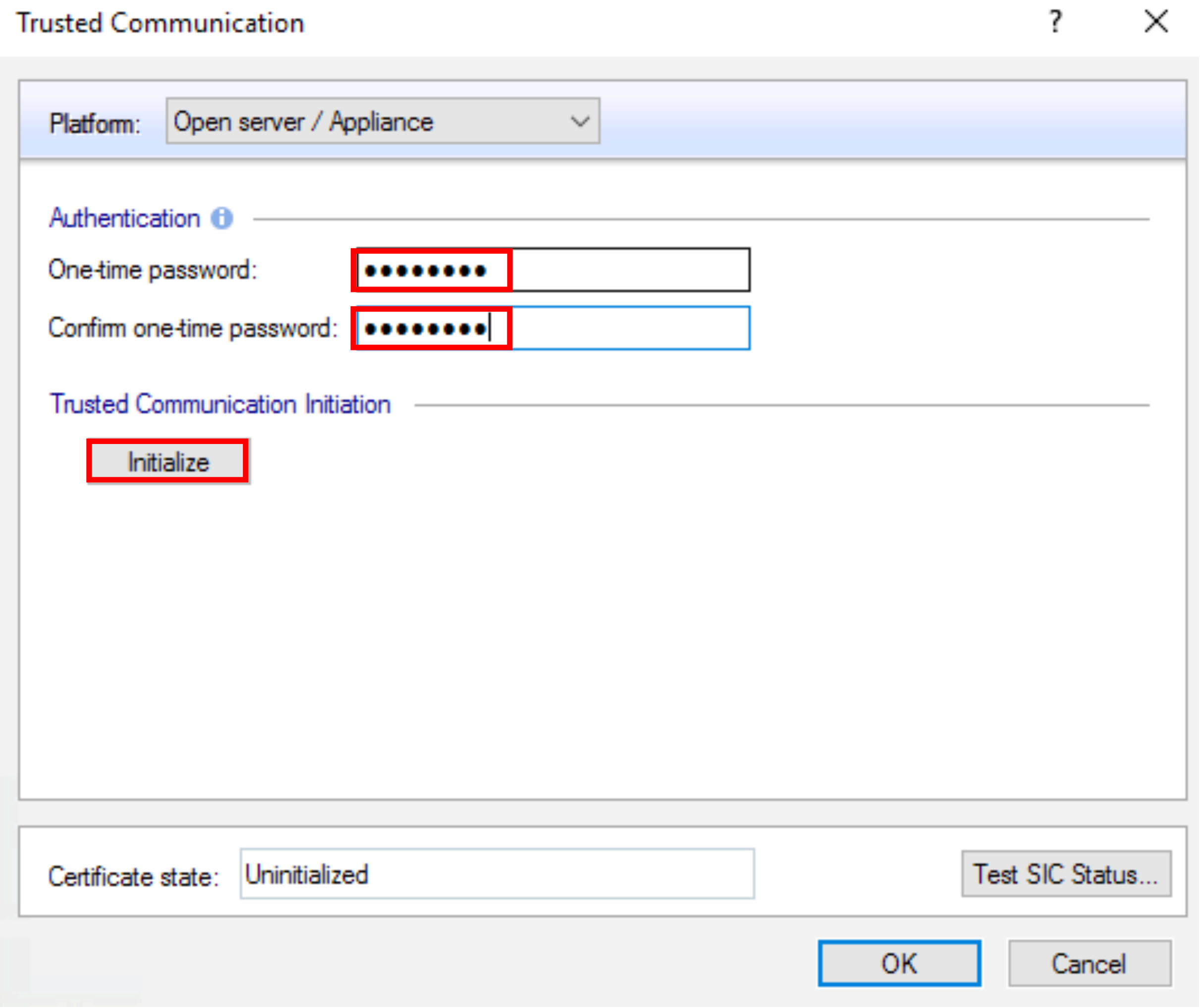


Check Point SmartConsole

Reset is done.
Please re-install the Firewall Policy in order to update the CRL list.
You must install the Firewall Policy to ALL Security Gateways.

The CRL list will be updated and we need to re-install the policy on all SGs. We will start to work with Security Policies in a future lab.

Let’s now re-enter and confirm the one-time password – **admin123**, and click **Intialize** button.



Trusted Communication

Platform: Open server / Appliance

Authentication

One-time password: ••••••••

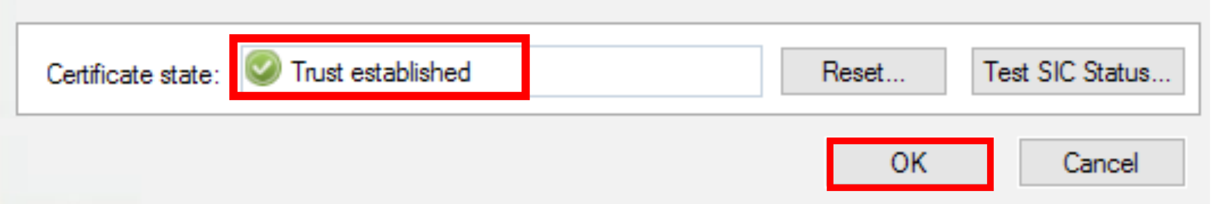
Confirm one-time password: ••••••••

Trusted Communication Initiation

Certificate state: Uninitialized

Please note that SIC has been established and the Certificate state shows as **Trust established.**

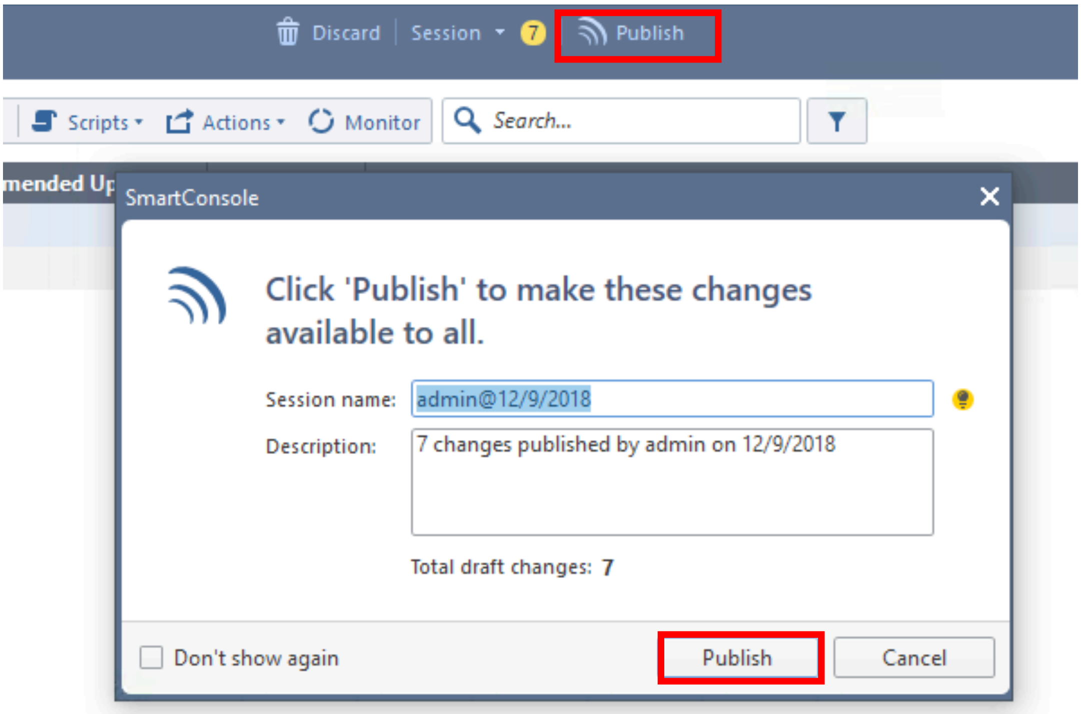
Click **OK.**



Certificate state: Trust established

Again, the topology is retrieved from the SG, click **Close** and **Close** again.

Now, **Publish** the changes. As we can see, 7 changes have been made and in order to save the changes and make them available we will first click on **Publish** at the top and again **Publish** in the screen that is displayed.



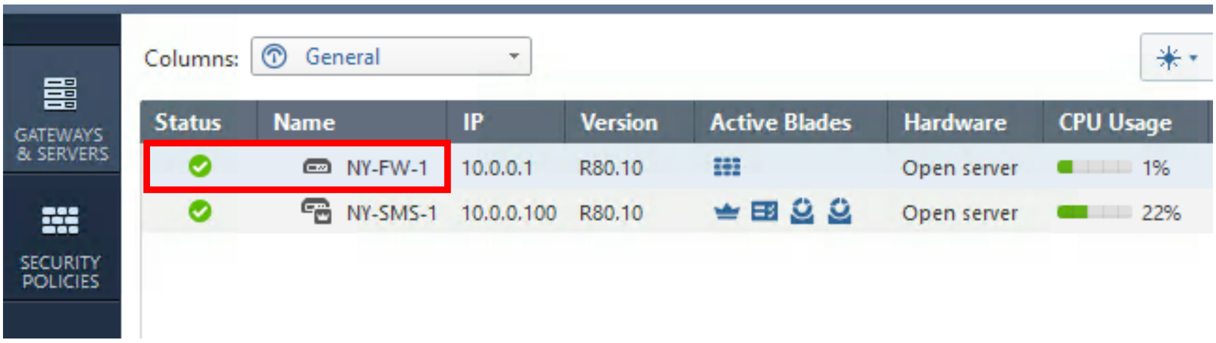
Click 'Publish' to make these changes available to all.

Session name: admin@12/9/2018

Description: 7 changes published by admin on 12/9/2018

Total draft changes: 7

Please note that now the NY-FW-1 state changes in the **Gateways&Servers** menu list and show the green tick:



Columns: General

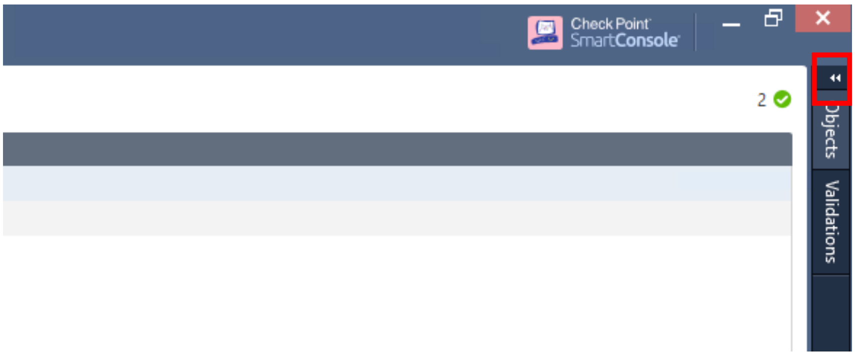
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage
✓	NY-FW-1	10.0.0.1	R80.10		Open server	1%
✓	NY-SMS-1	10.0.0.100	R80.10		Open server	22%

16.0 Lab: Configure New York Objects in SmartConsole

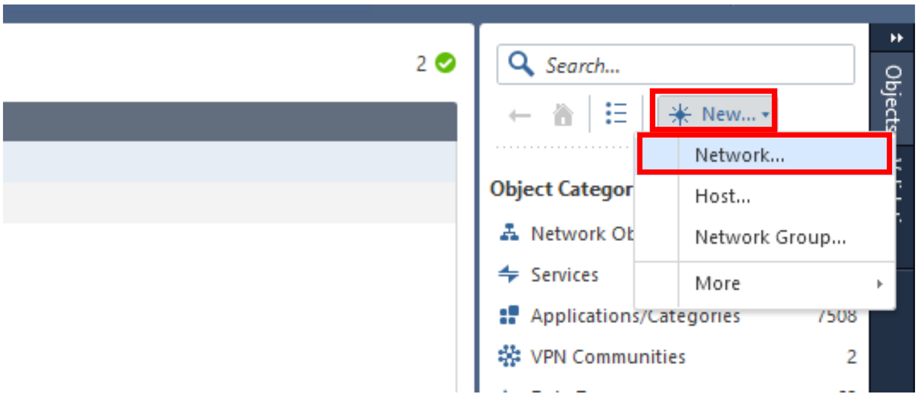
Lab Objectives

- Define in SmartConsole R80.10 New York subnet and host objects
- At the end of the lab, the following objects should be created:
    - Network Objects:
        - NY-LAN-NET
        - NY-MGMT-NET
        - NY-DMZ-NET
    - Host Objects:
        - NY-MGMT-PC
        - NY-LAN-1
        - NY-AD-SERVER
        - NY-DMZ-SERVER

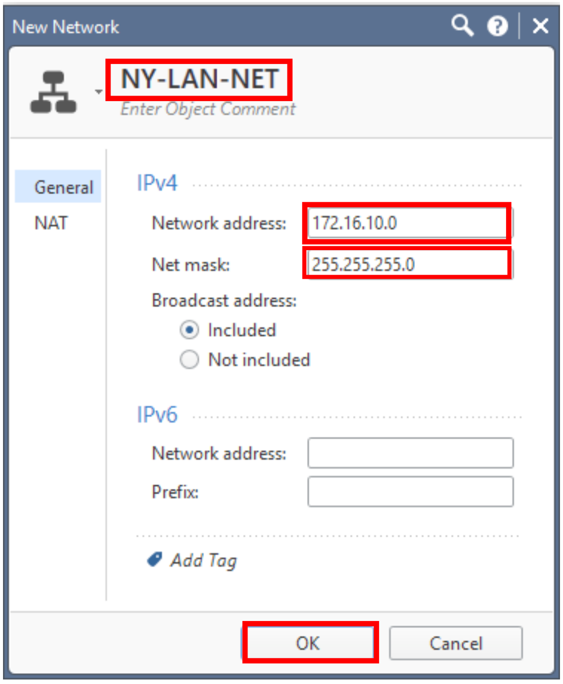
Let's start with the Network Objects. In SmartConsole, in the top-right corner, click on double arrow to maximize the panel, if it's not already opened.



Next, click on **New -> Network**:



Fill in the **Object Name**, **Network Address** and **Net mask**, as you can see below and then click **OK**:



New Network

NY-LAN-NET

Enter Object Comment

IPv4

Network address: 172.16.10.0

Net mask: 255.255.255.0

Broadcast address:

● Included

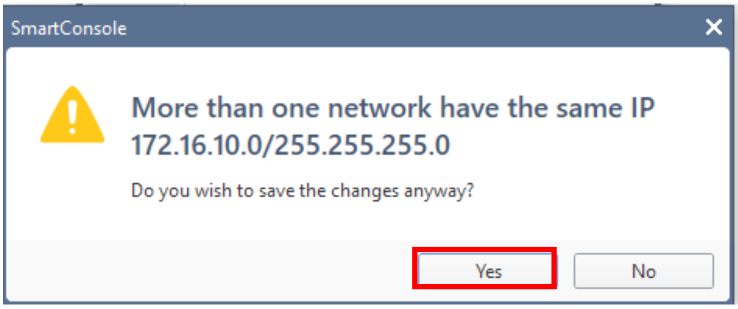
○ Not included

IPv6

Network address:

Prefix:

You may be displayed the following message. If this is the case, just click **Yes**.

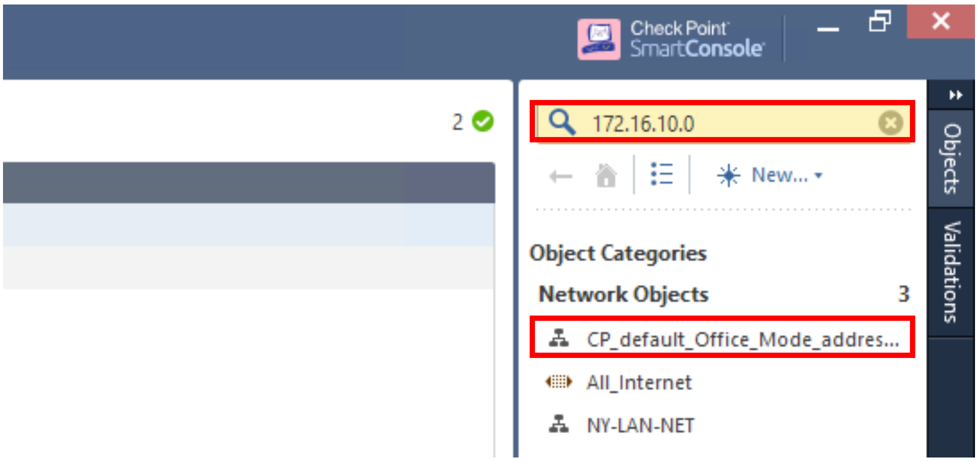


SmartConsole

More than one network have the same IP 172.16.10.0/255.255.255.0

Do you wish to save the changes anyway?

Check Point automatically creates some objects, by default, and this is one of them. In the search bar, if you search for **172.16.10.0** you will see that another object already exists, having the same IPv4 subnet assigned:



172.16.10.0

Object Categories

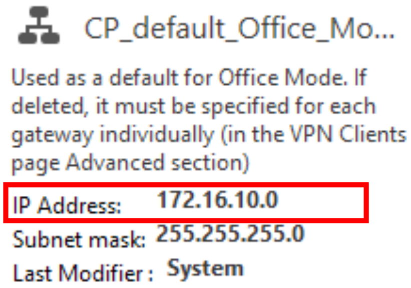
Network Objects 3

CP_default_Office_Mode_addres...

All_Internet

NY-LAN-NET

Click on **CP_default_Office_Mode_addresses_pool** and in the bottom-right corner the following information is displayed:



CP_default_Office_Mo...

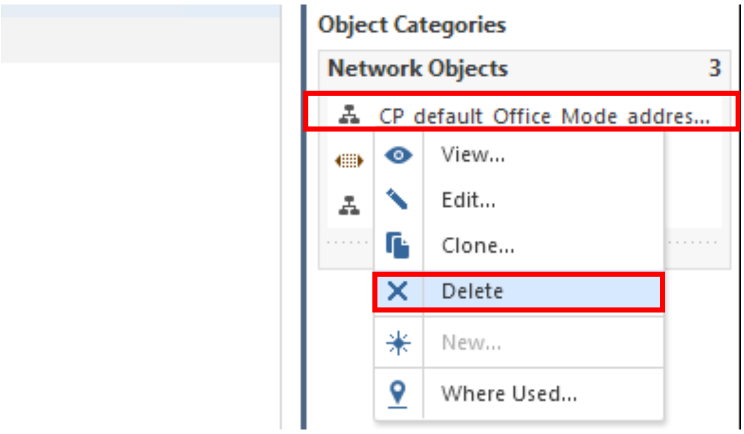
Used as a default for Office Mode. If deleted, it must be specified for each gateway individually (in the VPN Clients page Advanced section)

IP Address: 172.16.10.0

Subnet mask: 255.255.255.0

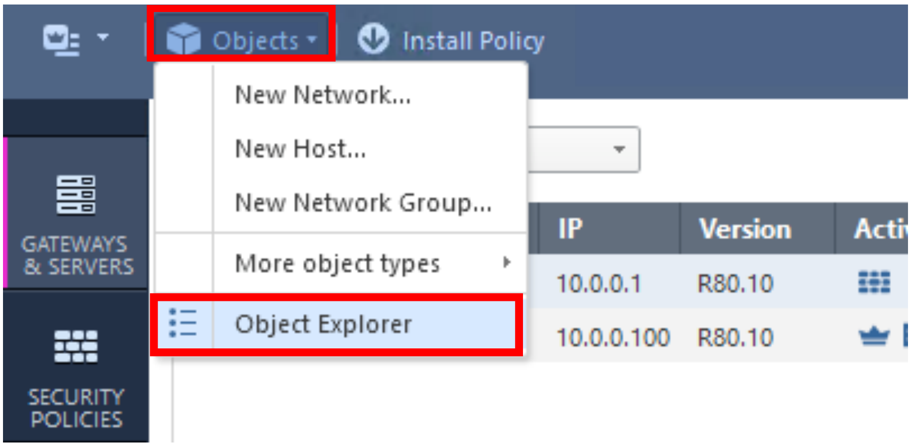
Last Modifier : System

All the objects available in SmartConsole are kept in a separate database. In order to keep the objects database "clean" and avoid any confusions or unexpected behaviours, it is best to not have multiple objects pointing to the same host IP or IPv4 subnet. Let's delete the object automatically created by the system.

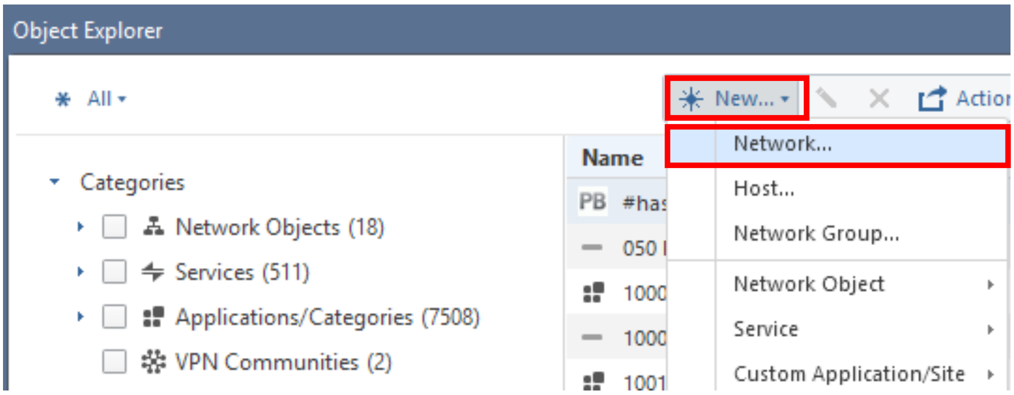


Right-click on the object and then select **Delete**. Confirm the action by clicking **Yes**.

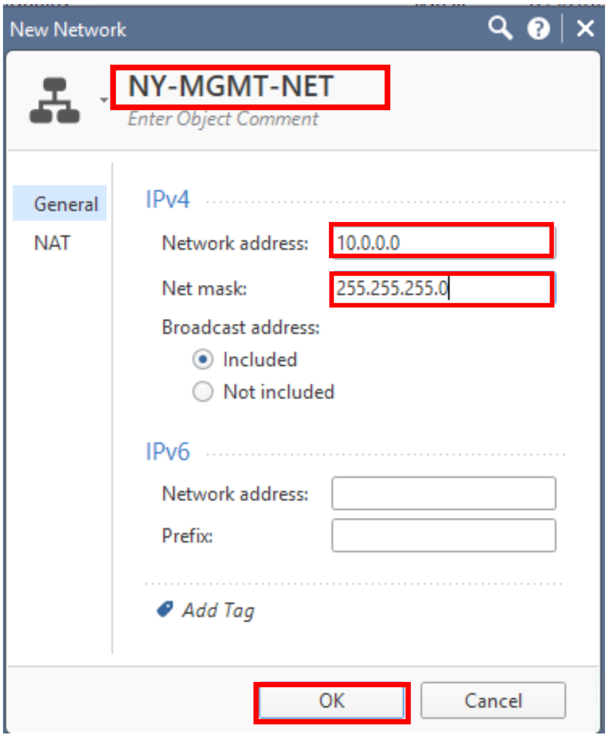
Let's continue with the second Network Object, but now let's start different. In the top-left corner, click on **Objects** and then **Object Explorer**:



Now, click on **New** and then click on **Network**:



Everything is the same now and we can continue like we did for the previous network object. Fill in the necessary details for NY-MGMT-NET, like you can see below. Click **OK** when you are done.



NY-MGMT-NET

Network address: 10.0.0.0

Net mask: 255.255.255.0

Network address:

Prefix:

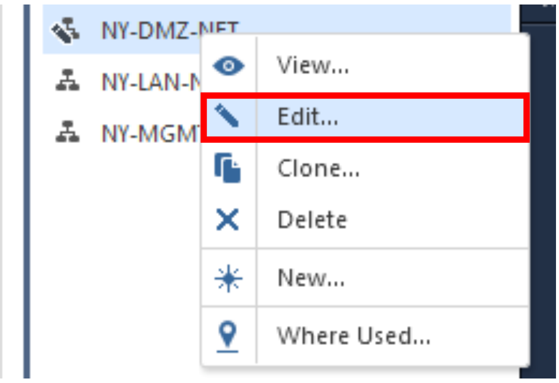
Continue and add the last two network objects, following either option 1 or 2. Below are the necessary details for NY-DMZ-NET network objects:

Parameter	Value
Object Name	NY-DMZ-NET
Network Address	172.16.20.0
Net mask	255.255.255.0

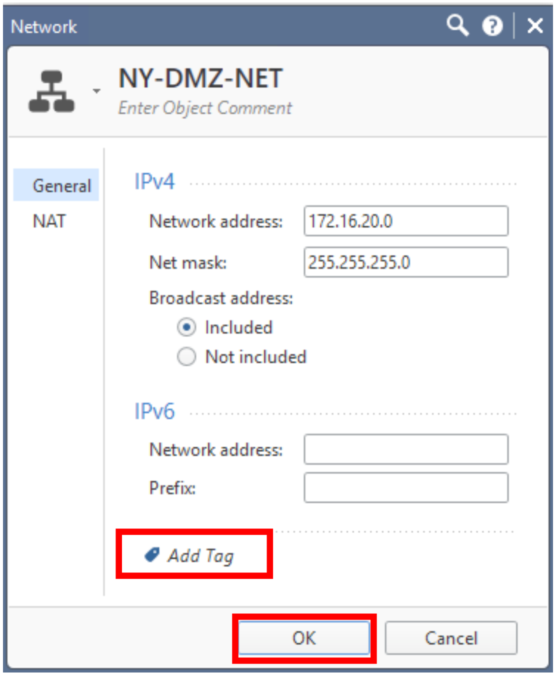
As a best practice, you can also add TAGs to objects. Now, why would you do that?

Object tags are keywords or labels that you can assign to the network objects or groups of objects **for search purposes**. Imagine that you are managing a big network of 1000 sites and at some point you are searching for a specific object, that you don't know the name, but you know that the object is used for a site. If you have defined a TAG when creating the object, you can search by using that TAG.

For these three objects, let's add also the tag: **HQ**. If this hasn't been done already when creating the object, you can do it at a later time by editing the object. Right-click an object in the **Network** list and click **Edit**:



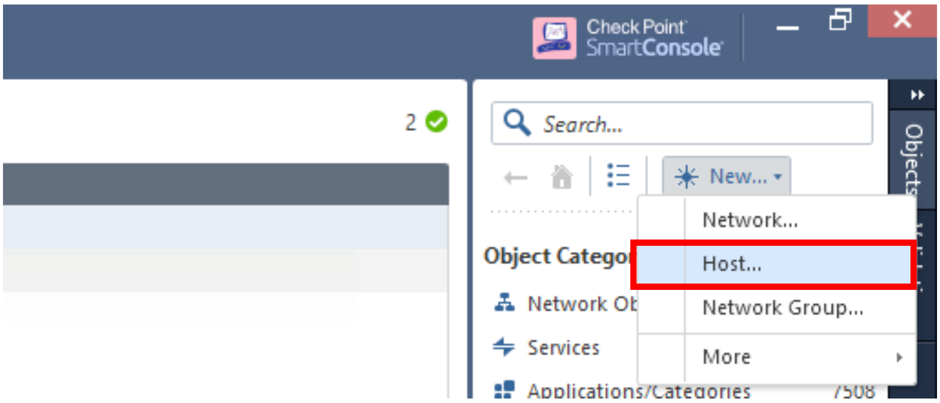
Click on **Add Tag,** type **HQ** and hit **Enter** to add the tag. Click **OK** when done.



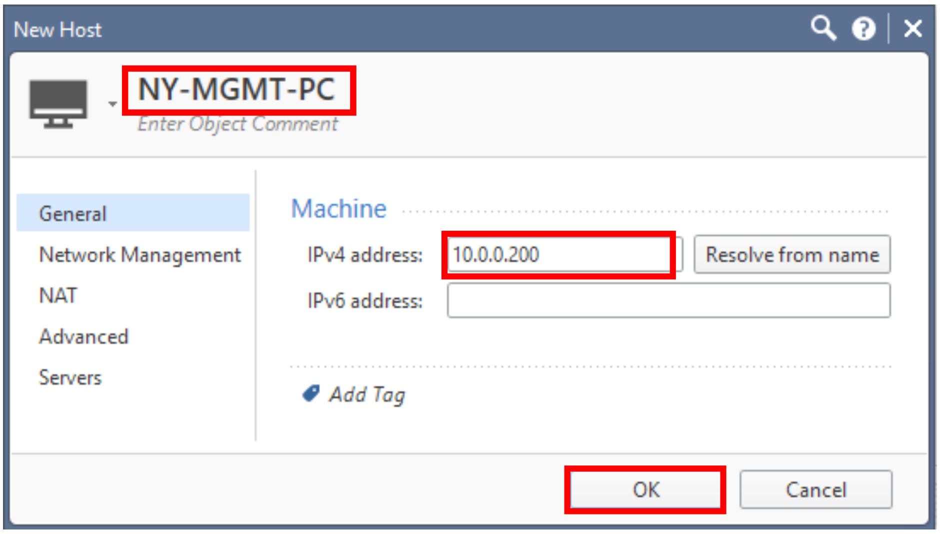
Network address: 172.16.20.0
Net mask: 255.255.255.0
Broadcast address:
● Included
○ Not included
Network address:
Prefix:

You may want to do the same for the other two network object as well.

Now, let’s continue and add the Host Objects. Following the same procedure, as you did in the first place, now you select **Host** instead of **Network**:



Fill in the necessary details and click **OK**.



NY-MGMT-PC

IPv4 address: 10.0.0.200

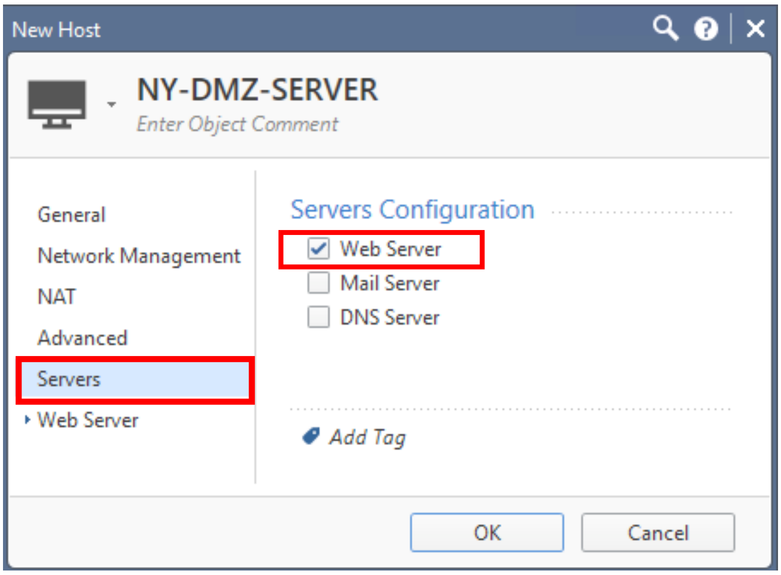
Continue and add the other three host objects as well: NY-LAN-1, NY-AD-SERVER and NY-DMZ-SERVER, using the information below:

Parameter	Value
Object Name	NY-LAN-1
IPv4 Address	172.16.10.200

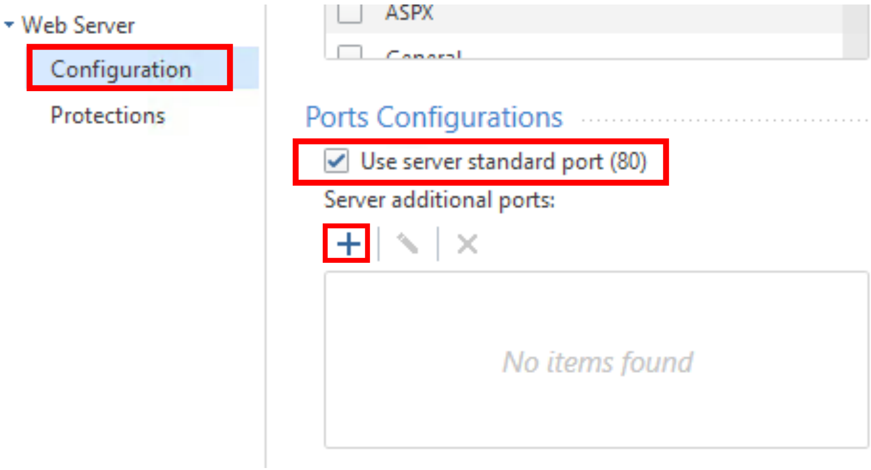
Parameter	Value
Object Name	NY-AD-SERVER
IPv4 Address	172.16.10.100

Parameter	Value
Object Name	NY-DMZ-SERVER
IPv4 Address	172.16.20.100

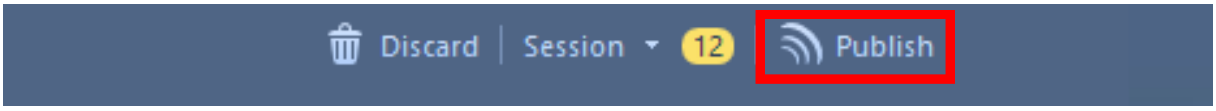
When adding the NY-DMZ-SERVER host object, please note that we can set now different options. Click on **Servers** menu on the left and select the **Web Server** option. This DMZ server will be configured later as web and ftp server, at least, so it is a good idea to enable it now as a web server.



After clicking on **Web Server**, on the left-side a new option appears: **Web Server.** If you expand the **Web Server** option, more information is displayed. You can change here, for example, or add another port the web server will be listening on (click on the +). By default, the web (http) server is listening on TCP port 80, but you can add whatever suits your needs: 443 (https), 8080, etc.



After you finished adding both network and host objects, don't forget to **Publish** the changes.

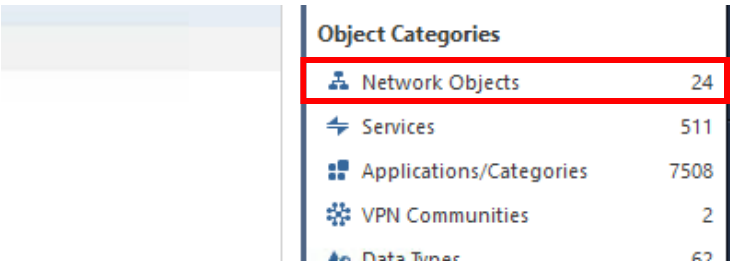


17.0 Lab: Add Anti-Spoofing and Security Zones Intelligence to NY-FW-1

Lab Objectives

- Configure security zones on NY-FW-1 interfaces
- Check anti-spoofing configuration (detect vs. prevent)

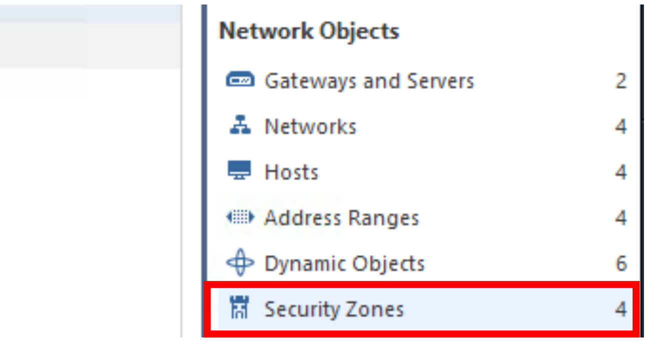
By default, four security zones are created and exist in the SmartConsole. Because security zones are actually objects, this means that we should be able to find them in the object panel. In the top-right corner, in the **Objects Category** click on **Network Objects** ,



Object Categories

Network Objects	24
Services	511
Applications/Categories	7508
VPN Communities	2
Data Types	62

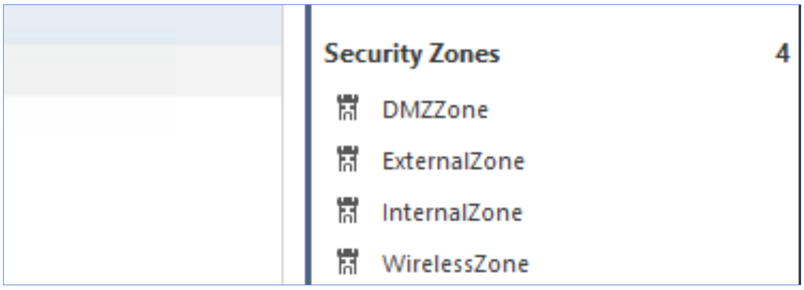
and then click on **Security Zones:**



Network Objects

Gateways and Servers	2
Networks	4
Hosts	4
Address Ranges	4
Dynamic Objects	6
Security Zones	4

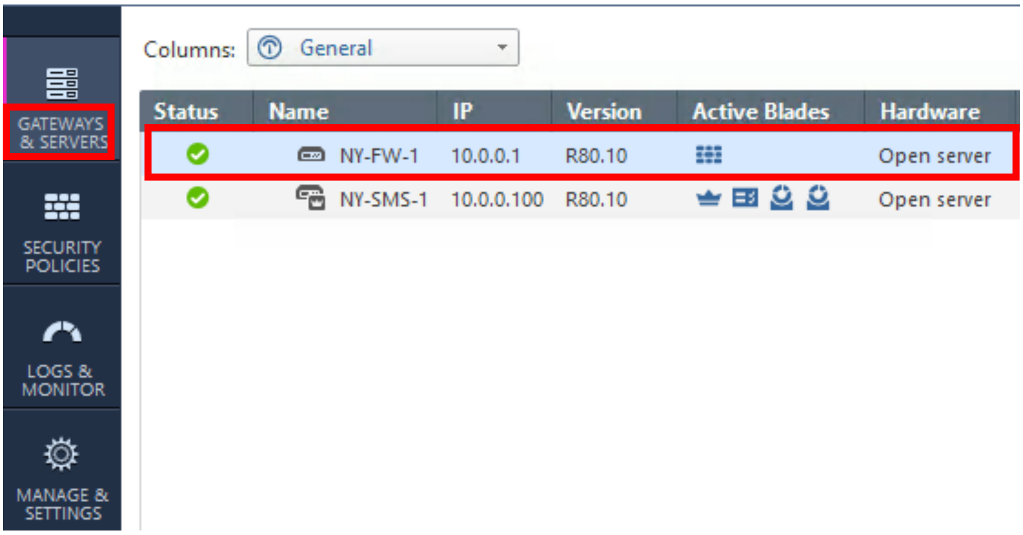
Now we can see the four security zones already defined on the system and we will use these, no need to define new ones:



Security Zones 4

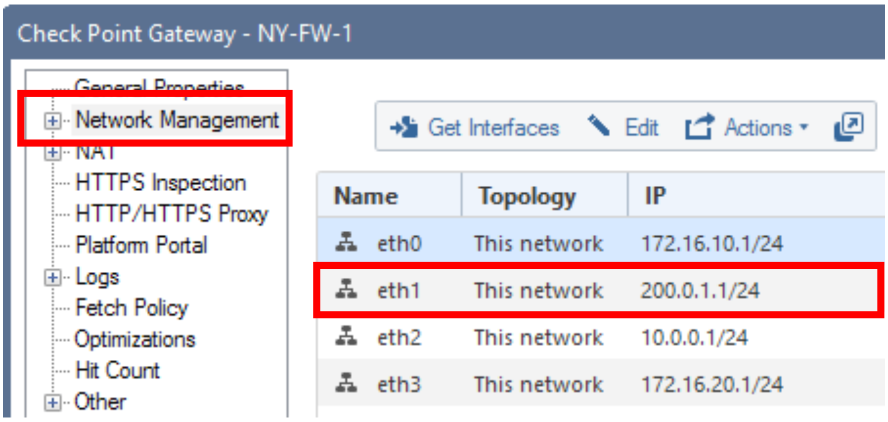
DMZZone
ExternalZone
InternalZone
WirelessZone

While in the **Gateway&Servers** menu, double-click anywhere on NY-FW-1 line



Status	Name	IP	Version	Active Blades	Hardware
✓	NY-FW-1	10.0.0.1	R80.10		Open server
✓	NY-SMS-1	10.0.0.100	R80.10		Open server

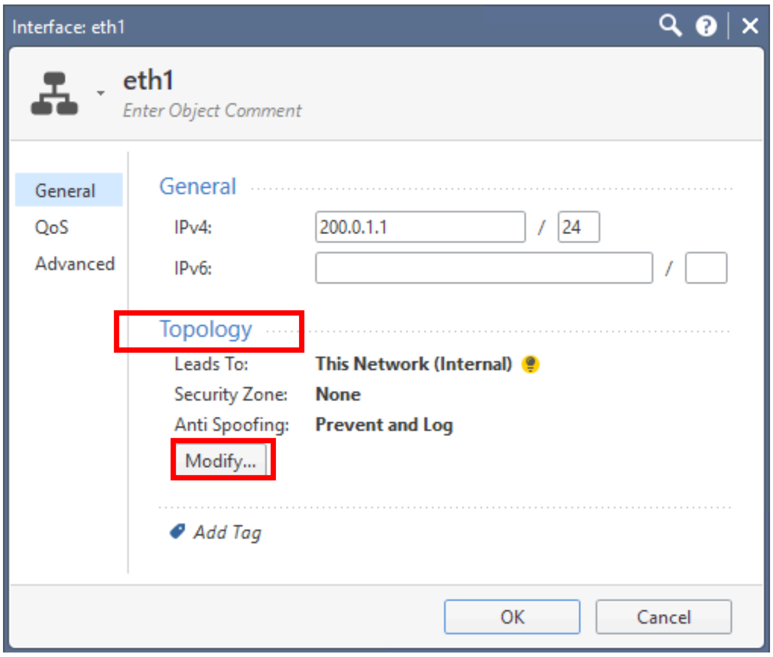
and the gateway properties window will open. Navigate to **Network Management** menu on the left and you will be able to see all interfaces of NY-FW-1.



Name	Topology	IP
eth0	This network	172.16.10.1/24
eth1	This network	200.0.1.1/24
eth2	This network	10.0.0.1/24
eth3	This network	172.16.20.1/24

Please observe that all interfaces are placed in terms of **Topology** into **This Network**. There is nothing different between them, although one interface is connecting to outside or Internet, one is connecting to local LAN, one is connecting to DMZ server and the last one is connecting the Management subnet.

Double click on eth1 – connecting to external network and let’s explore what we can configure here.



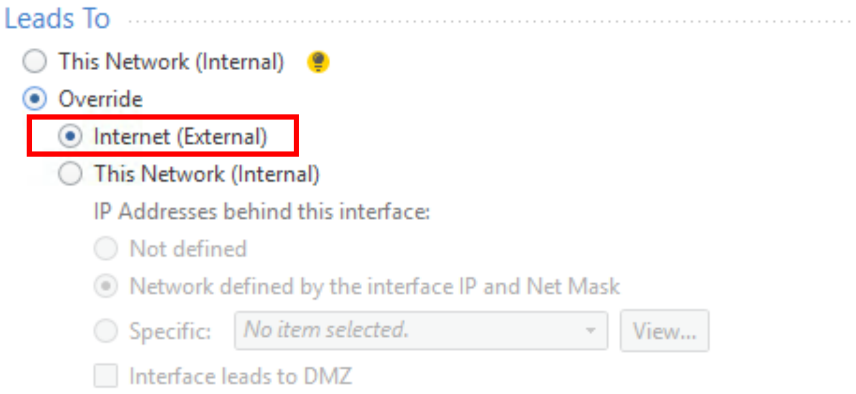
Interface: eth1

eth1
Enter Object Comment

General
IPv4: 200.0.1.1 / 24
IPv6: /

Topology
Leads To: This Network (Internal)
Security Zone: None
Anti Spoofing: Prevent and Log

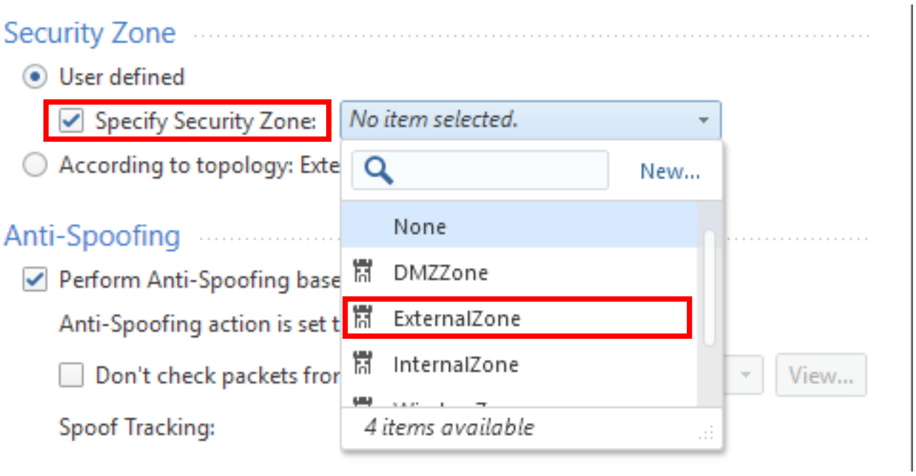
We are interested in the **Topology** section, so please click on **Modify**. No we modify the default configuration and basically we define the topology, how the security gateway will treat the interfaces, as belonging to what ? part of the network.



Leads To
○ This Network (Internal)
● Override
● Internet (External)
○ This Network (Internal)
IP Addresses behind this interface:
○ Not defined
● Network defined by the interface IP and Net Mask
○ Specific: No item selected.
□ Interface leads to DMZ

As this interface is connected to external network (Internet), please select the **Override** option and then **Internet** option.

In terms of **Security Zone**, we can either select **According to topology: ExternalZone** (now it makes more sense what does the topology mean) or we can manually select the zone by first selecting **Specify Security Zone** and selecting from the list **ExternalZone.**



Security Zone

● User defined

☑ Specify Security Zone: No item selected.

○ According to topology: Exte

Anti-Spoofing

☑ Perform Anti-Spoofing base

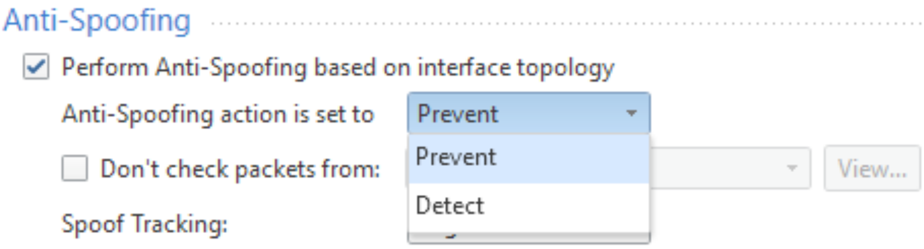
Anti-Spoofing action is set t

□ Don't check packets fror

Spoof Tracking:

Select it from the list and let’s move on to Spoofing options.

Now it’s even more obvious what topology means from the gateways perspective. The first option says that anti-spoofing will be performed based on interface topology. In other words, for example, if I see packets that arrive on interface on External network with a destination of Internal network, but they pretend to be part of Internal network, I will act as the anti-spoofing action is set to. Below two options are presented, **Prevent** and **Detect.** Prevent will block the packet, will Detect will only report the problem depending on **Spoof Tracking** configuration: none (do nothing), log (generate log) or alert (create an alert, i.e. send an email to IT Admin, etc).



Anti-Spoofing

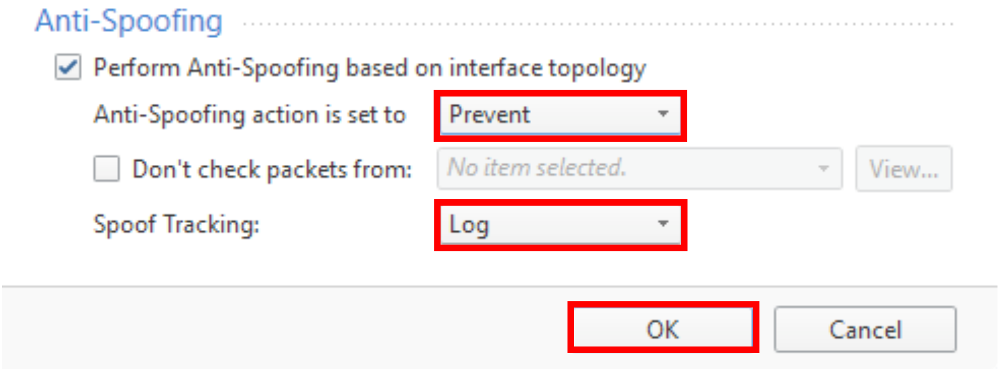
☑ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to: Prevent

□ Don't check packets from:

Spoof Tracking:

Let’s select **Prevent** and **Log.** Click **OK** when you finished.



Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

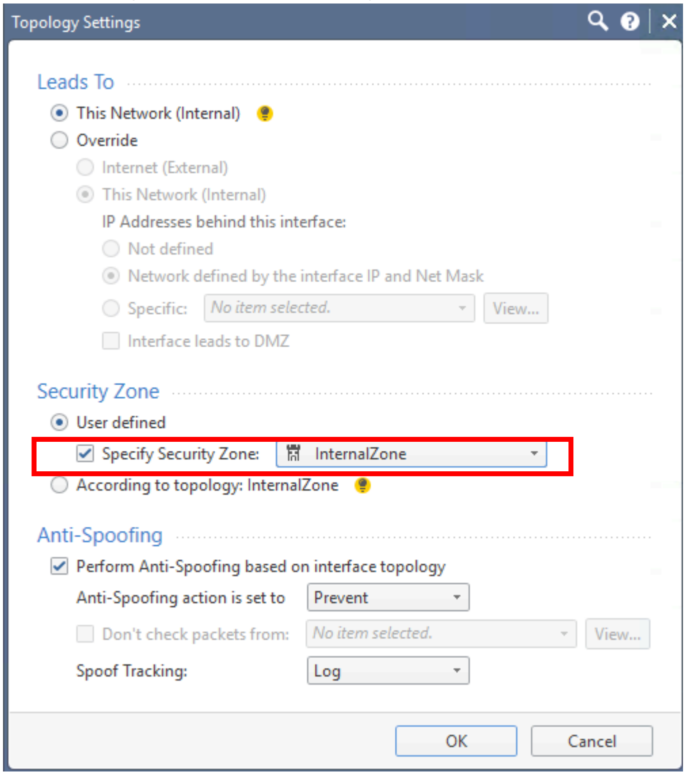
Anti-Spoofing action is set to: Prevent

□ Don't check packets from: No item selected.

Spoof Tracking: Log

Now, let’s continue and configure settings for the rest of NY-FW-1 interfaces.

Settings for eth0 (in my case) connecting to internal LAN and eth2 connecting to management subnet. Specified Security Zone as **InternalZone**:



Topology Settings

Leads To

● This Network (Internal)

○ Override

○ Internet (External)

● This Network (Internal)

IP Addresses behind this interface:

○ Not defined

● Network defined by the interface IP and Net Mask

○ Specific: No item selected. View...

□ Interface leads to DMZ

Security Zone

● User defined

☑ Specify Security Zone: InternalZone

○ According to topology: InternalZone

Anti-Spoofing

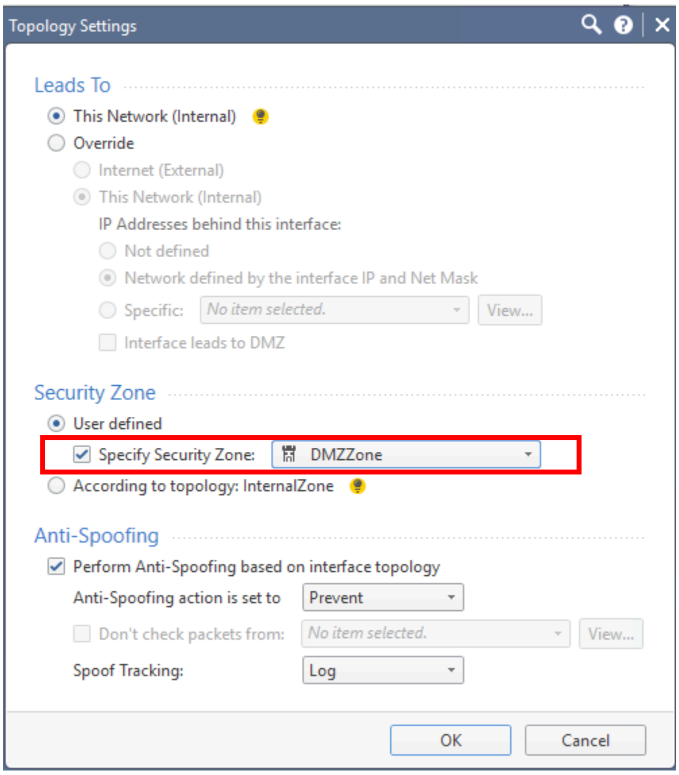
☑ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to: Prevent

□ Don't check packets from: No item selected. View...

Spoof Tracking: Log

In case of eth3, connecting to DMZ, please select **DMZZone** as your security zone:



Topology Settings

Leads To

● This Network (Internal)

○ Override

○ Internet (External)

● This Network (Internal)

IP Addresses behind this interface:

○ Not defined

● Network defined by the interface IP and Net Mask

○ Specific: No item selected. View...

□ Interface leads to DMZ

Security Zone

● User defined

☑ Specify Security Zone: DMZZone

○ According to topology: InternalZone

Anti-Spoofing

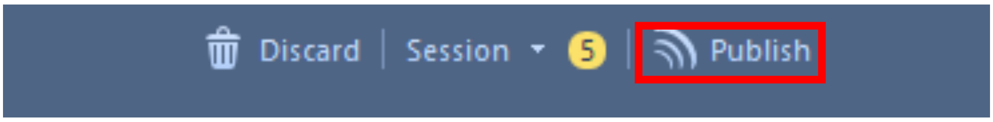
☑ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to: Prevent

□ Don't check packets from: No item selected. View...

Spoof Tracking: Log

As always, when you are done configuring, don't forget to **Publish** the changes:

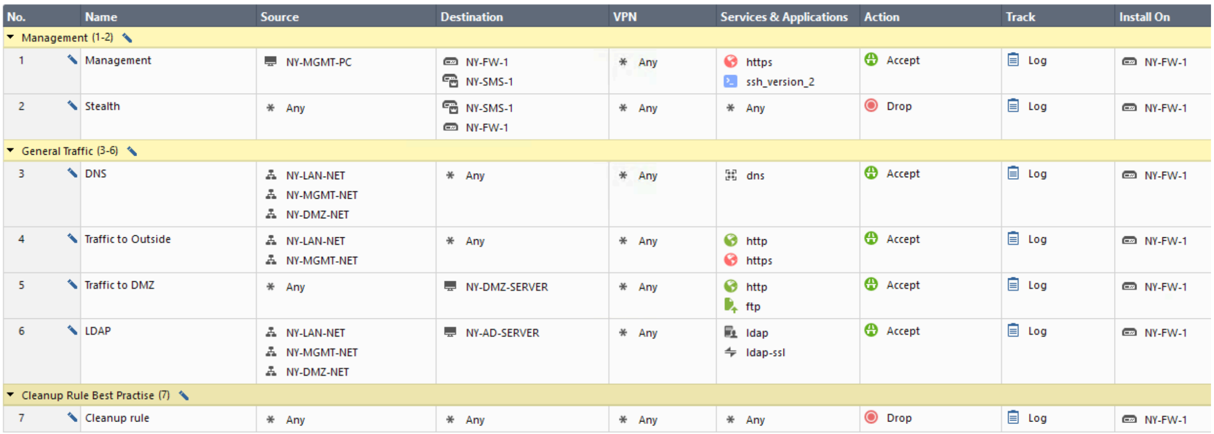


Please note that the number of changes that is displayed on the right of the **Section** (yellow circle) may vary. Make sure that you configured and applied the settings to all interfaces and at the end just **Publish** the changes.

18.0 Lab: Configure a Basic Access Control Policy for New York HQ

Lab Objectives

- Deploy a basic Access Control Policy on New York HQ Firewall
- Organize the rule base with Section Titles
- At the end of this lab the rule base should look like the one below:

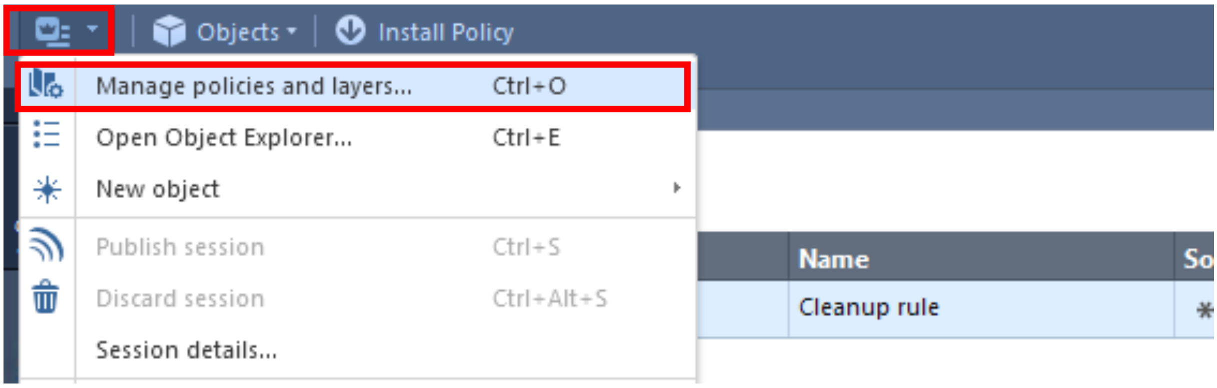


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Management (1-2)								
1	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1	Any	https ssh_version_2	Accept	Log	NY-FW-1
2	Stealth	Any	NY-SMS-1 NY-FW-1	Any	Any	Drop	Log	NY-FW-1
General Traffic (3-6)								
3	DNS	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	Any	Any	dns	Accept	Log	NY-FW-1
4	Traffic to Outside	NY-LAN-NET NY-MGMT-NET	Any	Any	http https	Accept	Log	NY-FW-1
5	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Accept	Log	NY-FW-1
6	LDAP	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	NY-AD-SERVER	Any	ldap ldap-ssl	Accept	Log	NY-FW-1
Cleanup Rule Best Practise (7)								
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	NY-FW-1

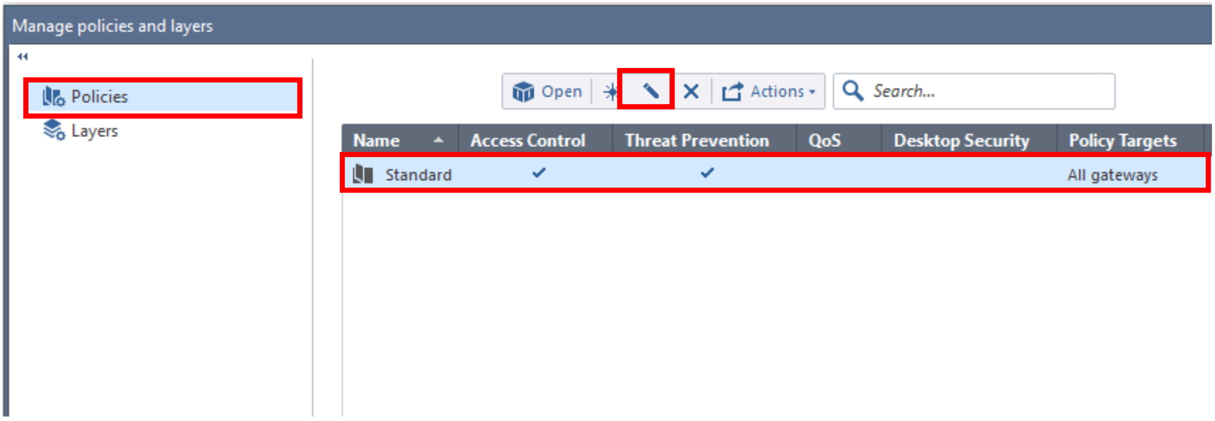
Let’s start with the management rules.

Access to the Check Point machines, SMS and the security gateways, should be limited to only allowed IP(s) or specific subnets. Following this best practice, we will create a rule that permits only https and ssh version 2 traffic to both SMS server and Check Point Security Gateways – NY-FW-1 in this case.

Before we start, let’s change the current name of the policy (policy package) that’s being applied to the NY-FW-1. In SmartConsole, navigate to main menu and select **Manage policies and layers :**


Objects
Install Policy
Manage policies and layers... Ctrl+O
Open Object Explorer... Ctrl+E
New object
Publish session Ctrl+S
Discard session Ctrl+Alt+S
Session details...
Name
So
Cleanup rule

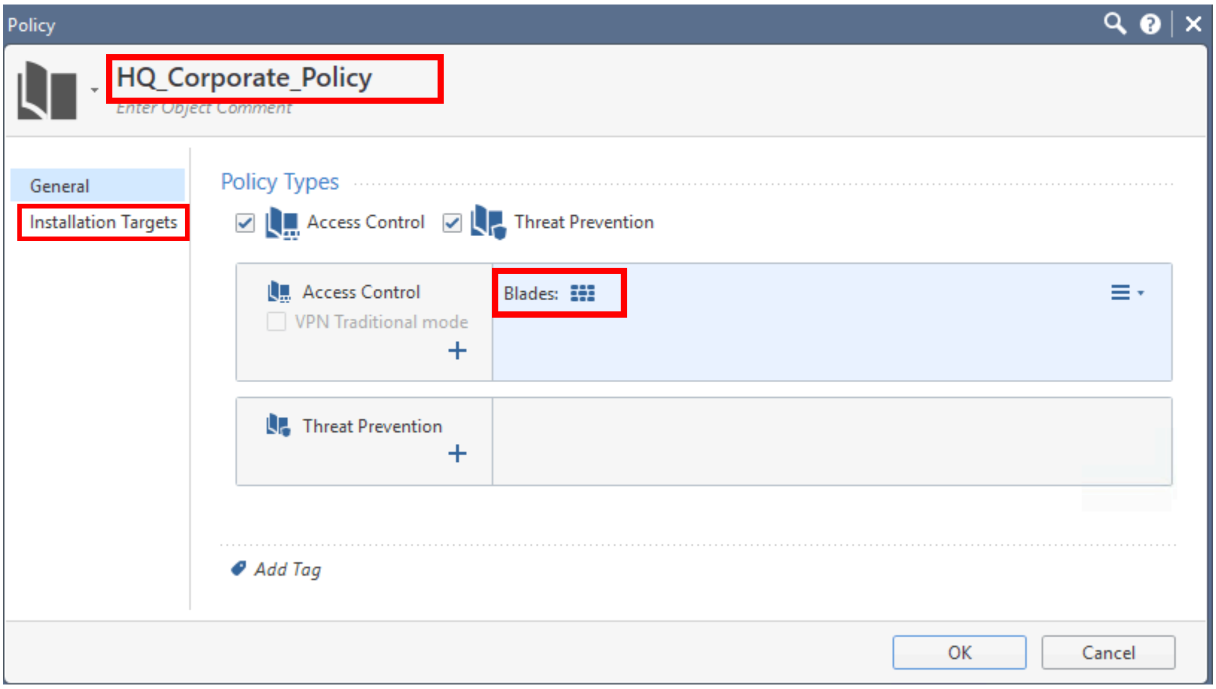
As you can see, we currently have only one policy package and the name is **Standard.**



Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets
Standard	✓	✓			All gateways

Click on edit button (pencil icon) in the middle and let us now change the name of the policy package from **Standard** to **HQ_Corporate_Policy**. As you can see, the Corporate_Policy package contains two policies, the Access Control and Threat Prevention policy, respectively.

In this lab, we are creating a basic Access Control policy only with Firewall software blade activated on the NY-FW-1. As we progress, in the upcoming labs, we will activate the rest of the blades as well: Application Control and URL Filtering and Content Awareness.



Policy

HQ_Corporate_Policy

Enter Object Comment

General

Installation Targets

Policy Types

☑ Access Control ☑ Threat Prevention

Access Control

□ VPN Traditional mode

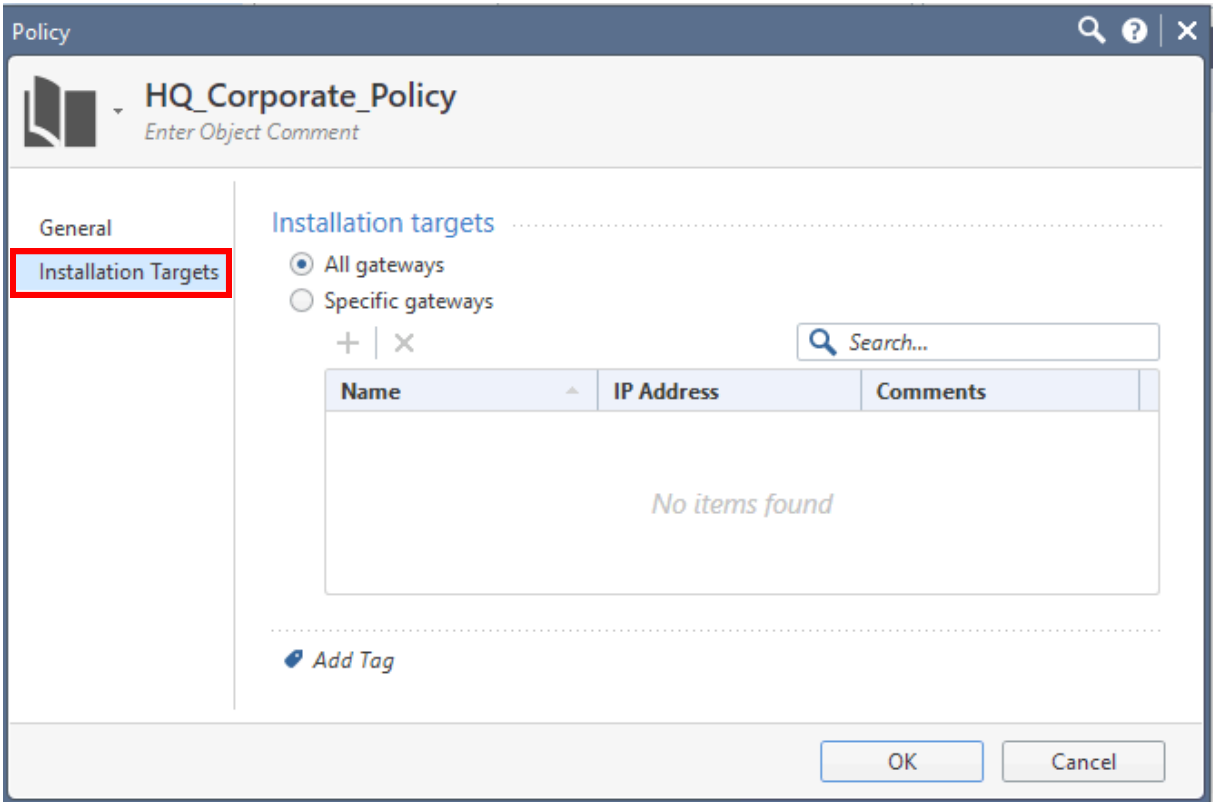
Blades:

Threat Prevention

Add Tag

OK Cancel

Let’s click on **Installation Targets** menu. Here we can define where will this policy package be installed.



Policy

HQ_Corporate_Policy

Enter Object Comment

General

Installation Targets

Installation targets

● All gateways

○ Specific gateways

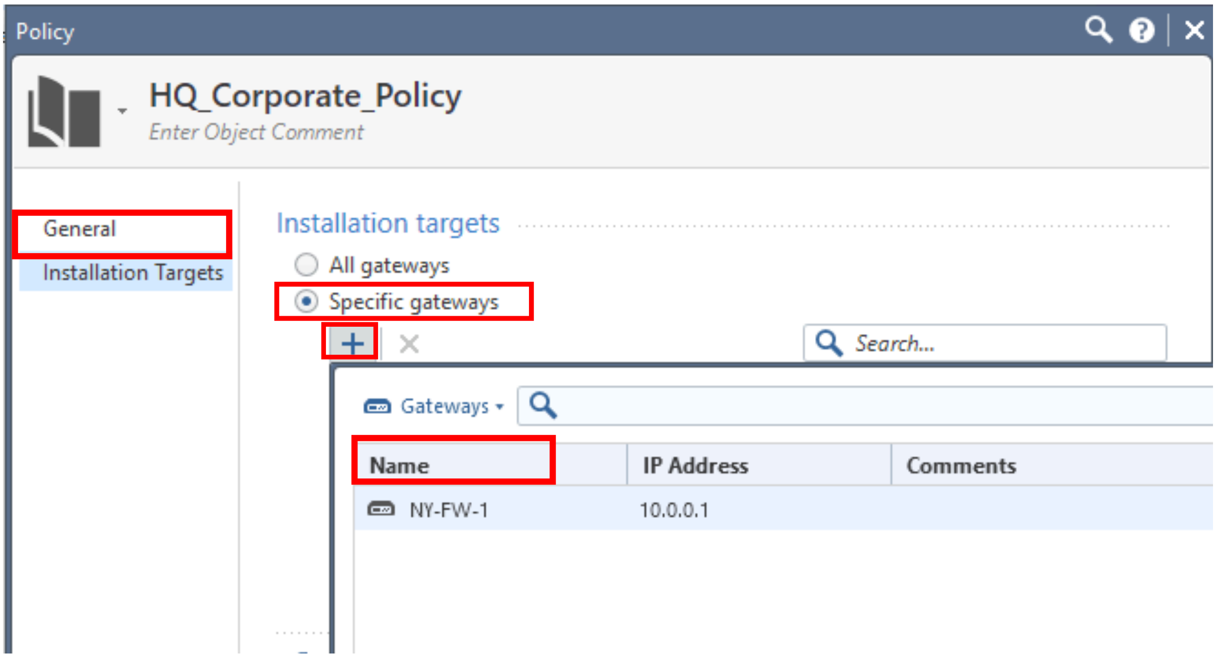
Search...

Name	IP Address	Comments
No items found		

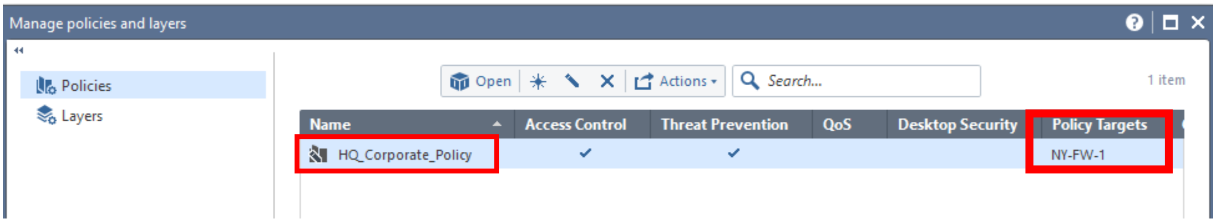
Add Tag

OK Cancel

By default, the installation target is set to **All gateways**, but we will change this to be specific and configure here NY-FW-1. So this policy package will be installed only on NY-FW-1 security gateway.

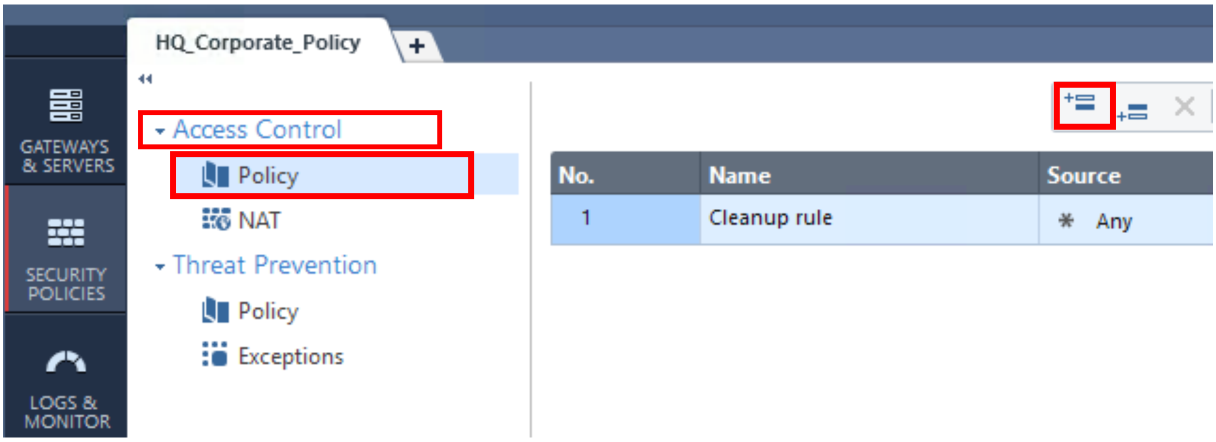


Select **NY-FW-1**, click **OK** and it should look like this:



Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets
HQ_Corporate_Policy	✓	✓			NY-FW-1

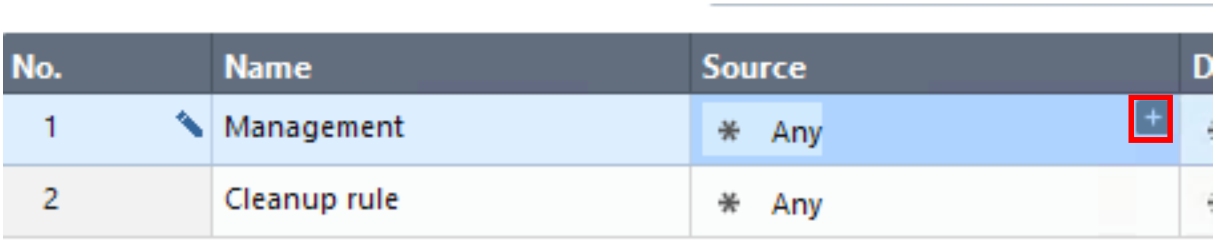
Now, let’s navigate to **Security Policies -> Access Control -> Policy** and add our first rule.



No.	Name	Source
1	Cleanup rule	Any

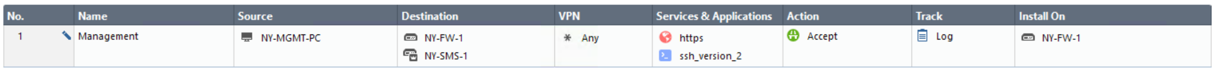
Click on the Cleanup rule and then click on icon **Add rule above**. A new rule is added on top of the existing rule and we can edit it now. This rule will be the Management rule, permitting access to SMS and NY-FW-1 only from MGMT PC.

Enter the name of the rule – Management and continue adding the source. Click on the **+** sign



No.	Name	Source	D
1	Management	✱ Any	
2	Cleanup rule	✱ Any	

and select **NY-MGMT-PC** as the source. Continue with the rest of the fields and make sure your rule will match the following:

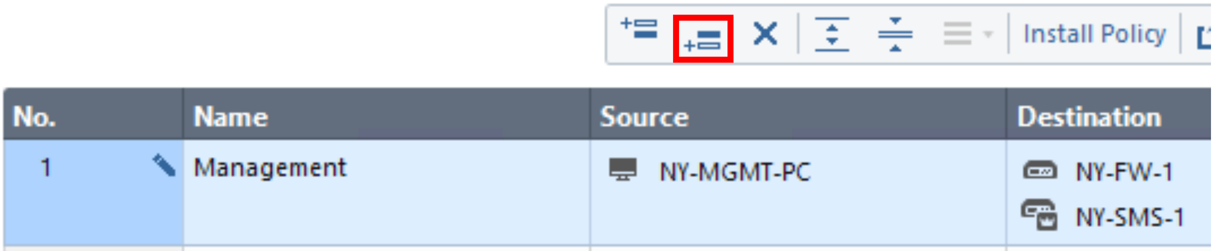


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1	✱ Any	https ssh_version_2	Accept	Log	NY-FW-1

Remember the Best Practise we talked about in Module 6 ? Stealth and Cleanup Rules should be configured in every rule base.

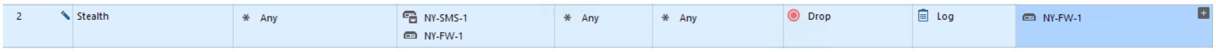
Now, let’s add the Stealth rule. The idea is that you first allow management traffic specifically as we did we rule 1 – Management and afterwards you deny any other attempt of connecting to the Check Point machines.

Select rule 1 and click on **Add rule below** icon:



No.	Name	Source	Destination
1	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1

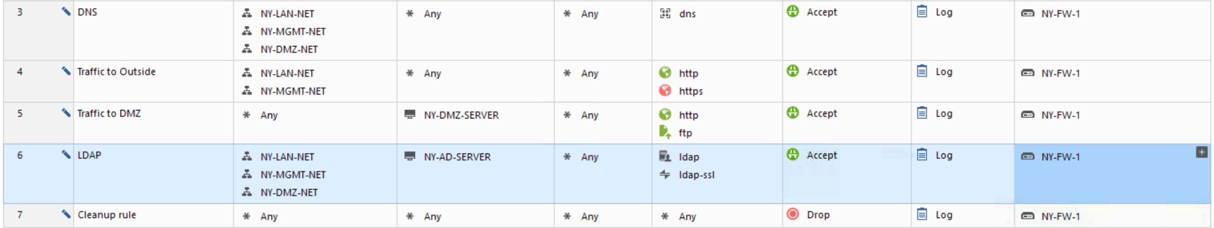
When done, your rule should look like the following:



2	Stealth	✱ Any	NY-SMS-1 NY-FW-1	✱ Any	✱ Any	Drop	Log	NY-FW-1

Next, let’s add some traffic general rules. We will permit DNS in a rule and outgoing traffic in a separate rule, traffic to DMZ in another rule, LDAP traffic separate as well and last rule will be the explicit Cleanup rule.

Your new rules should look like this:

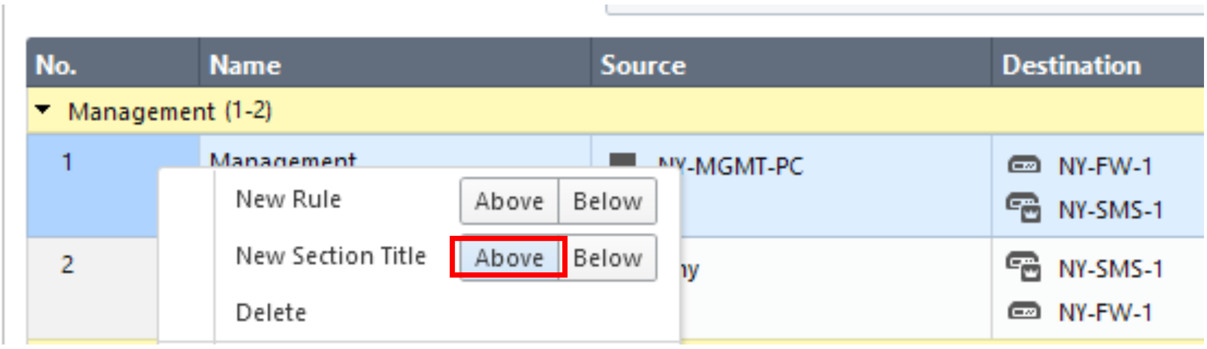


3	DNS	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	Any	Any	dns	Accept	Log	NY-FW-1
4	Traffic to Outside	NY-LAN-NET NY-MGMT-NET	Any	Any	http https	Accept	Log	NY-FW-1
5	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Accept	Log	NY-FW-1
6	LDAP	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	NY-AD-SERVER	Any	ldap ldap-ssl	Accept	Log	NY-FW-1
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	NY-FW-1

In terms of organizing the rule base, it's a good idea to introduce **Sections.** This way you "document" your rule base and make it easy to read, while creating it.

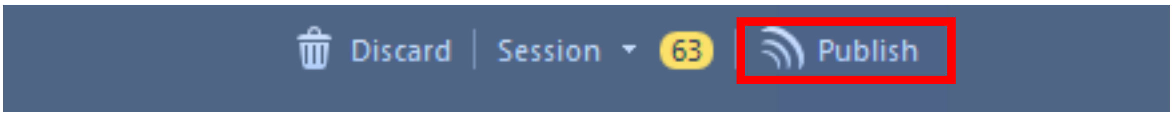
Let's create three sections: Management, General Traffic and Cleanup Rule Best Practice.

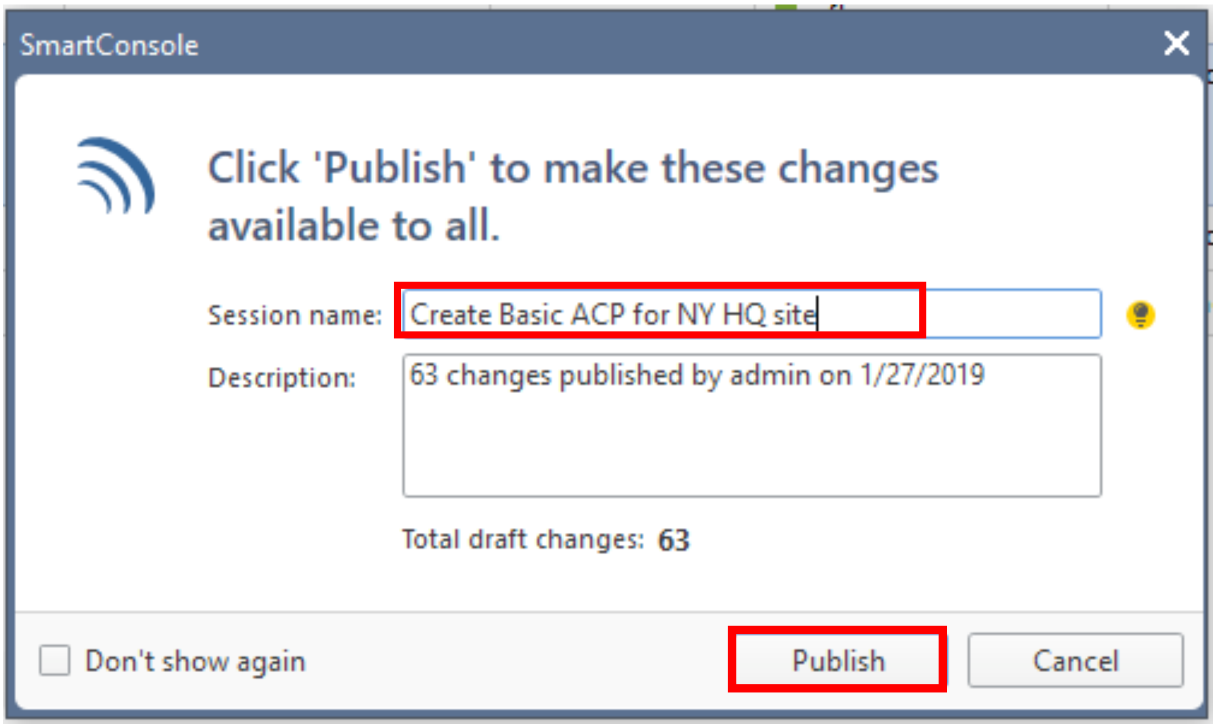
Right-click on the first rule in the rule base and click on **Above** in the **New Section Title** row. This will add a new Section Title that you can afterwards change the name to **Management.**



Continue and add another two section titles, General Traffic for rules 3-6 and Cleanup rule (explicit, right?) above the last rule.

When you are done, don't forget to **Publish** the changes





SmartConsole

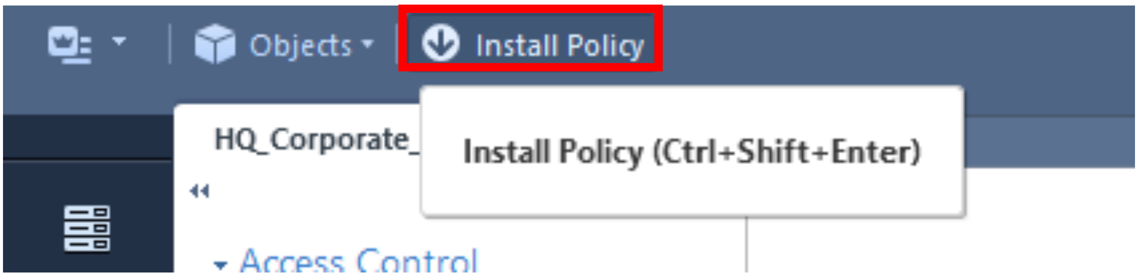
Click 'Publish' to make these changes available to all.

Session name: Create Basic ACP for NY HQ site

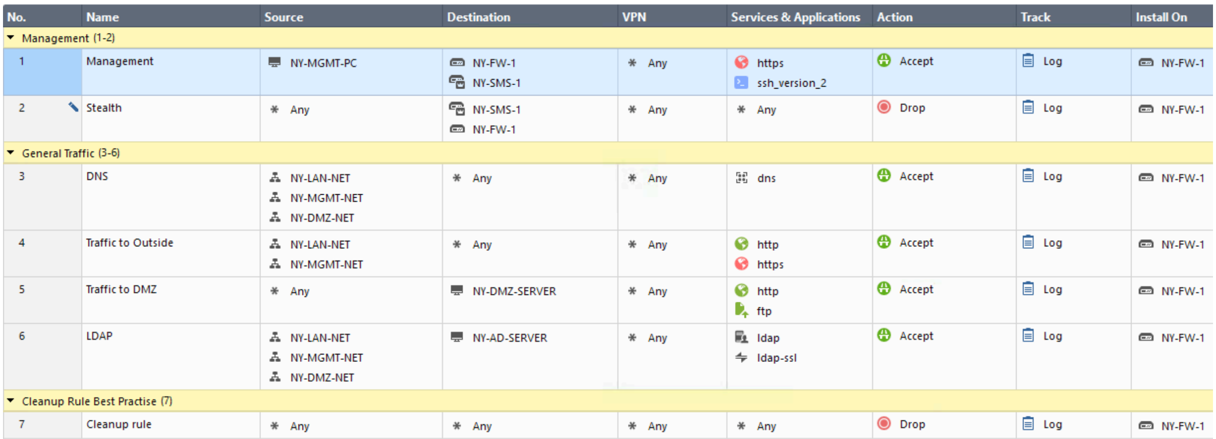
Description: 63 changes published by admin on 1/27/2019

Total draft changes: 63

and install the newly created policy.



Your new basic ACP should look like this in the end:



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Management (1-2)								
1	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1	Any	https ssh_version_2	Accept	Log	NY-FW-1
2	Stealth	Any	NY-SMS-1 NY-FW-1	Any	Any	Drop	Log	NY-FW-1
General Traffic (3-6)								
3	DNS	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	Any	Any	dns	Accept	Log	NY-FW-1
4	Traffic to Outside	NY-LAN-NET NY-MGMT-NET	Any	Any	http https	Accept	Log	NY-FW-1
5	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Accept	Log	NY-FW-1
6	LDAP	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	NY-AD-SERVER	Any	ldap ldap-ssl	Accept	Log	NY-FW-1
Cleanup Rule Best Practise (7)								
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	NY-FW-1

19.0 Lab: Configure Hide NAT for New York HQ LANs

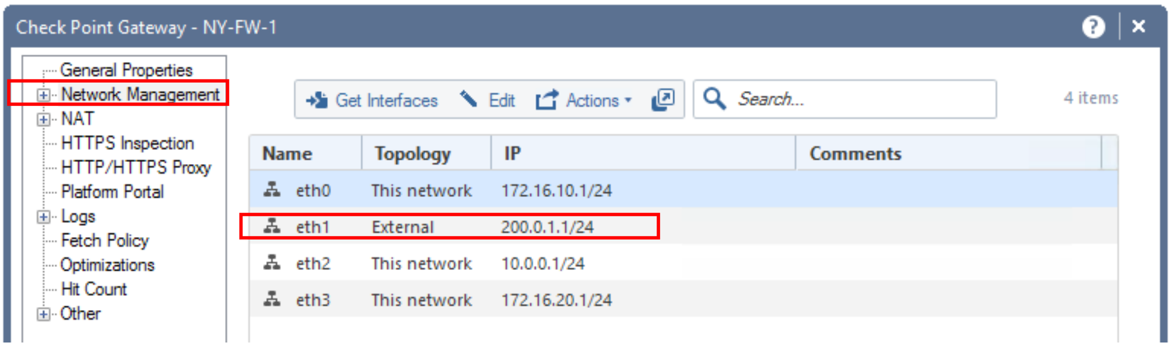
Lab Objectives

- Connect to Internet LAN, DMZ and MGMT LANs
- Configure and test Hide NAT both at gateway level and object level

Automatic Hide NAT can be configured in two ways, at the gateway level for all **Internal** subnets or at the object level, per object. **Internal** subnets refers to the Topology the Security Gateway is aware of. This is where the configuration of the Topology comes in handy and proves one more time it's useful.

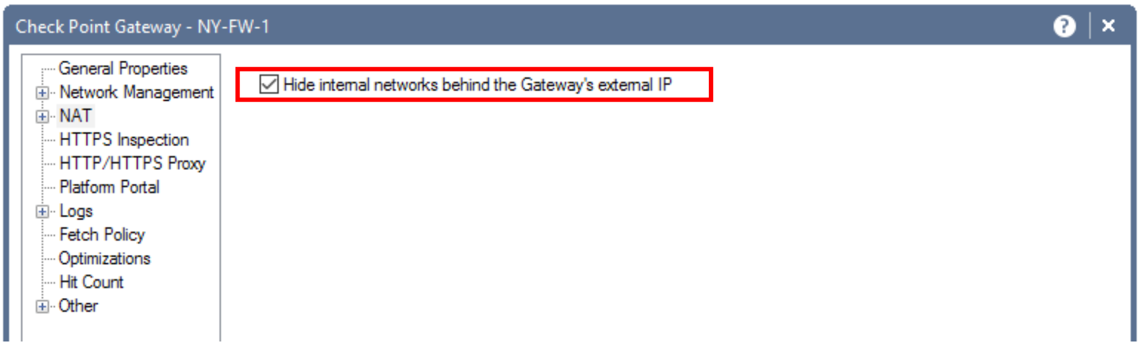
Let's start and first enable Automatic Hide NAT for all Internal subnets. One more thing, it's called automatic because the NAT rules are added automatically by SmartConsole in the NAT rule base. The other option, Manual NAT, would mean that you manually configure the NAT rules and add them one by one to the NAT Rule Base.

Open SmartConsole and go to **Gateways and Servers** main menu on the left side. Double-click on NY-FW-1 and navigate to **Network Management** menu on the left:



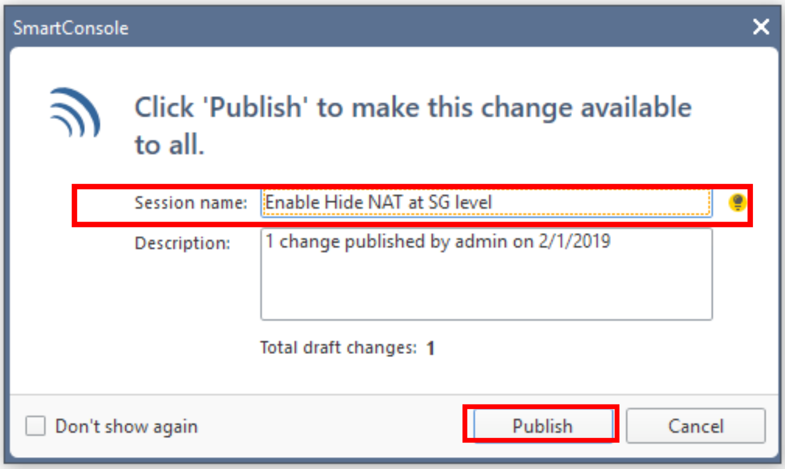
Name	Topology	IP	Comments
eth0	This network	172.16.10.1/24	
eth1	External	200.0.1.1/24	
eth2	This network	10.0.0.1/24	
eth3	This network	172.16.20.1/24	

You can see here that only eth1 is **External** the rest of the interfaces are **Internal** networks. Next, go to **NAT** menu on the left and enable **Hide NAT:**



☑ Hide internal networks behind the Gateway's external IP

Click **OK** when done. Let’s now **Publish** the changes, **Install** the policy and run **Verification** tests.



SmartConsole

Click 'Publish' to make this change available to all.

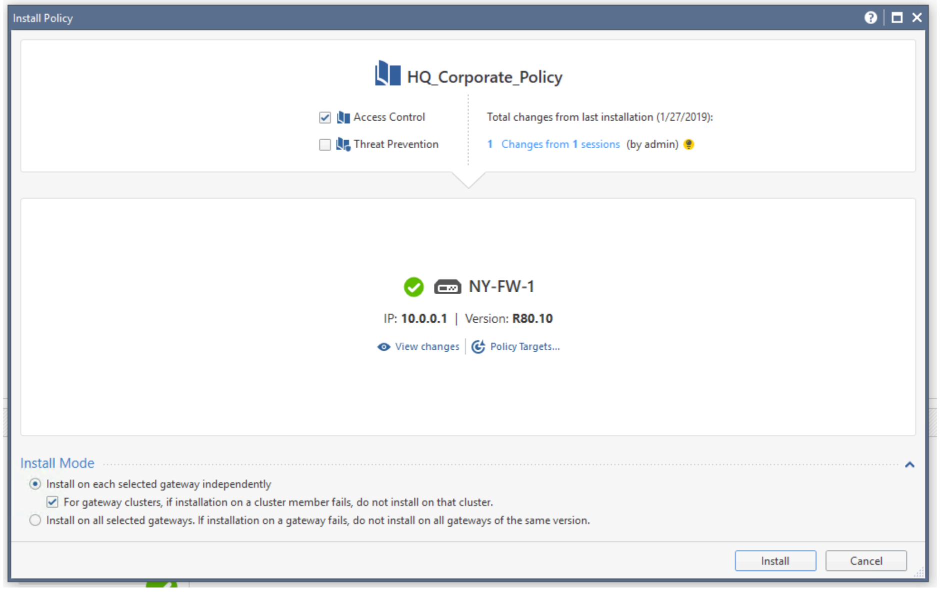
Session name: Enable Hide NAT at SG level

Description: 1 change published by admin on 2/1/2019

Total draft changes: **1**

□ Don't show again

Install policy:



Install Policy

HQ_Corporate_Policy

☑ Access Control

□ Threat Prevention

Total changes from last installation (1/27/2019):

1 Changes from 1 sessions (by admin)

NY-FW-1

IP: **10.0.0.1** | Version: **R80.10**

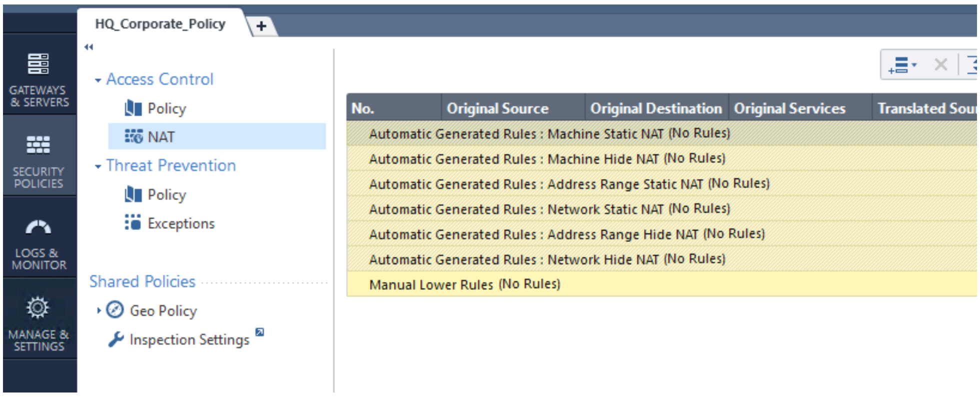
Install Mode

● Install on each selected gateway independently

☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

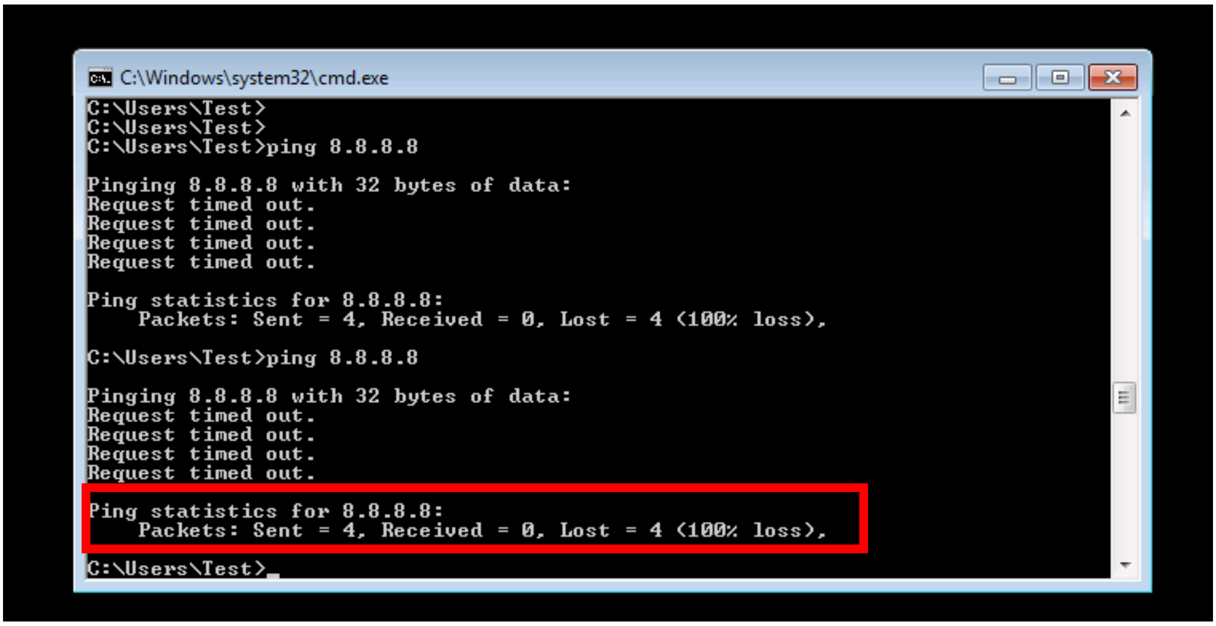
○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

Let’s check if any NAT rules have been created in the NAT rule base:



No.	Original Source	Original Destination	Original Services	Translated Sou
Automatic Generated Rules : Machine Static NAT (No Rules)				
Automatic Generated Rules : Machine Hide NAT (No Rules)				
Automatic Generated Rules : Address Range Static NAT (No Rules)				
Automatic Generated Rules : Network Static NAT (No Rules)				
Automatic Generated Rules : Address Range Hide NAT (No Rules)				
Automatic Generated Rules : Network Hide NAT (No Rules)				
Manual Lower Rules (No Rules)				

No NAT rule appear as to be created in the NAT rule base. Let's run a verification test. Go to NY-LAN-1 host PC and initiate an icmp session to Google DNS – 8.8.8.8:

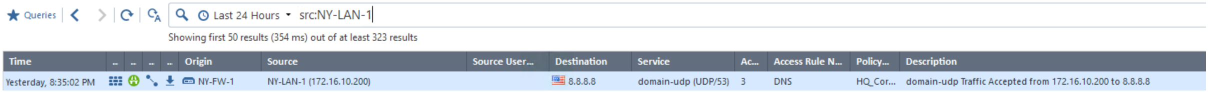


```
C:\Users\Test>
C:\Users\Test>
C:\Users\Test>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Test>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Test>_
```

Now, why is ping not working ? It should work right ?

Let's investigate. Let's go to **Logs&Monitor** and check the logs.

Open one of the logs like you see below:



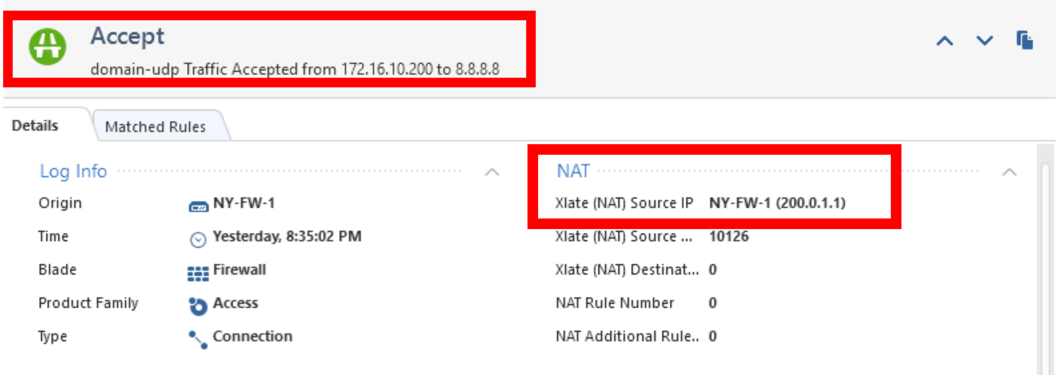
src:NY-LAN-1

Showing first 50 results (354 ms) out of at least 323 results

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Yesterday, 8:35:02 PM					NY-FW-1	NY-LAN-1 (172.16.10.200)		8.8.8.8	domain-udp (UDP/53)	3	DNS	HQ_Cor...	domain-udp Traffic Accepted from 172.16.10.200 to 8.8.8.8

Type in the search bar, in order to sort through the logs, src:NY-LAN-1, so that we see only logs generated for traffic that has been sourced by NY-LAN-1 host.

Double-click on the log and we see that traffic was accepted by the NY-FW-1 and indeed that NAT has been done :



Accept
domain-udp Traffic Accepted from 172.16.10.200 to 8.8.8.8

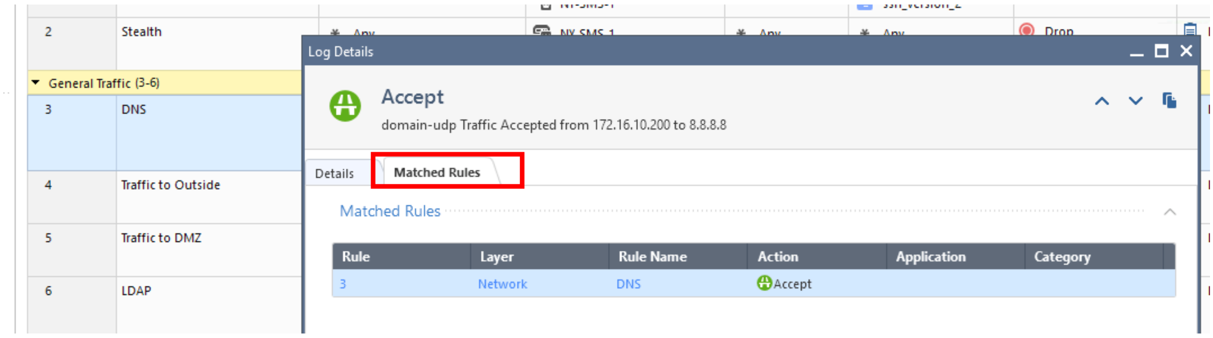
Log Info

Origin	NY-FW-1
Time	Yesterday, 8:35:02 PM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Source IP	NY-FW-1 (200.0.1.1)
Xlate (NAT) Source ...	10126
Xlate (NAT) Destinat...	0
NAT Rule Number	0
NAT Additional Rule..	0

Click on **Matched Rules** tab in order to see what rule in the rule base did it match.



2	Stealth	Any	NY-SMS-1	Any	Any	Drop
General Traffic (3-6)						
3	DNS					
4	Traffic to Outside					
5	Traffic to DMZ					
6	LDAP					

Log Details

Accept

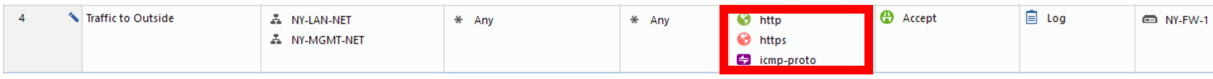
domain-udp Traffic Accepted from 172.16.10.200 to 8.8.8.8

Matched Rules

Rule	Layer	Rule Name	Action	Application	Category
3	Network	DNS	Accept		

We can see that the DNS request was matched by rule 3 and if you click on 3 in the background the rule base is opened and rule 3 is highlighted.

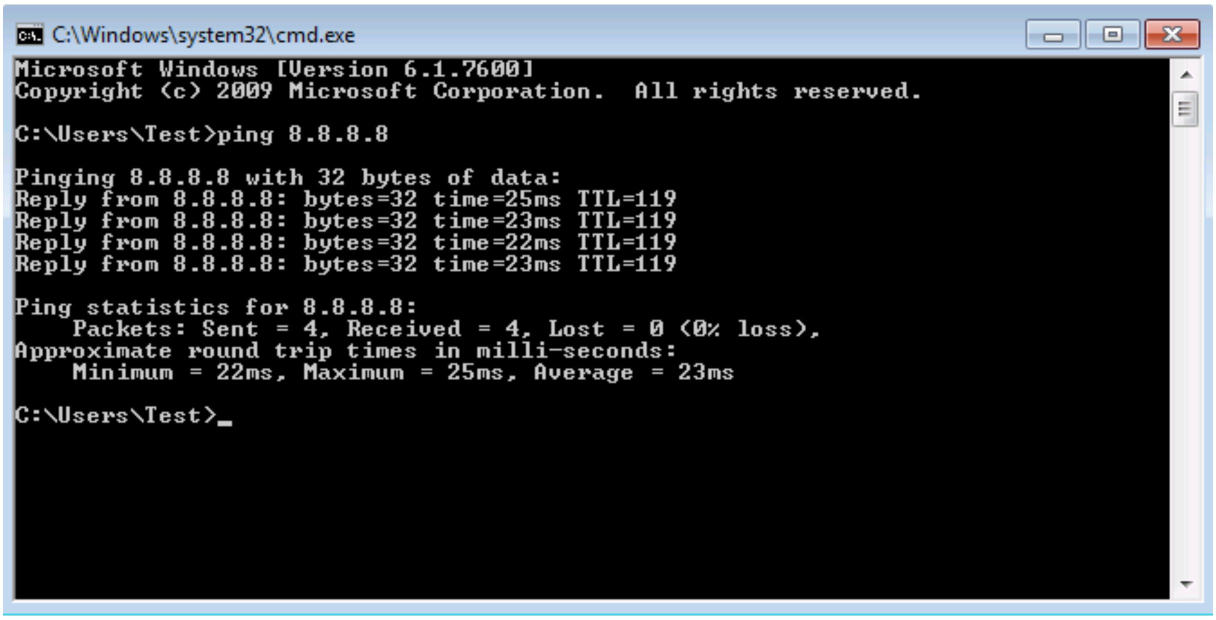
If we want the ICMP traffic to be successful, we will need to modify the Rule Base, for example the Outgoing Traffic rule and add ICMP protocol there. Let’s do this now:



4	Traffic to Outside	NY-LAN-NET NY-MGMT-NET	Any	Any	http https icmp-proto	Accept	Log	NY-FW-1

Publish changes and install policy !

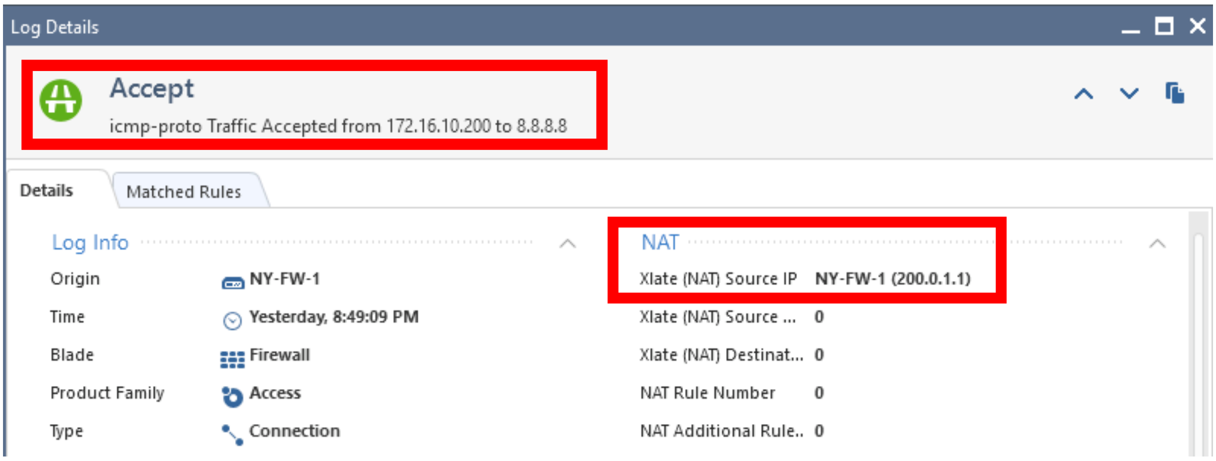
Now let’s test again icmp to 8.8.8.8 on NY-LAN-1 PC – Success !



C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Test>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=119
Reply from 8.8.8.8: bytes=32 time=23ms TTL=119
Reply from 8.8.8.8: bytes=32 time=22ms TTL=119
Reply from 8.8.8.8: bytes=32 time=23ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 25ms, Average = 23ms

C:\Users\Test>_
```

Let’s identify traffic on **Logs&Monitor:**



Log Details

Accept

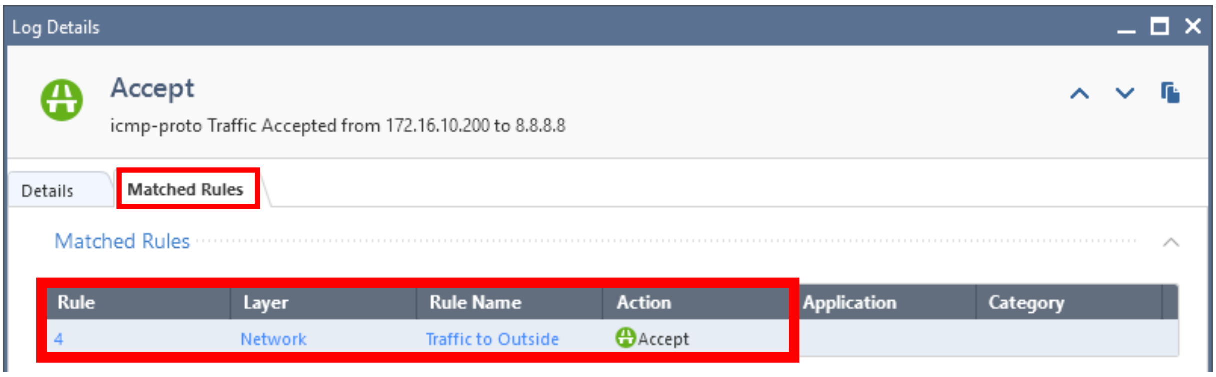
icmp-proto Traffic Accepted from 172.16.10.200 to 8.8.8.8

Log Info

Origin	NY-FW-1
Time	Yesterday, 8:49:09 PM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Source IP	NY-FW-1 (200.0.1.1)
Xlate (NAT) Source ...	0
Xlate (NAT) Destinat...	0
NAT Rule Number	0
NAT Additional Rule..	0



Log Details

Accept

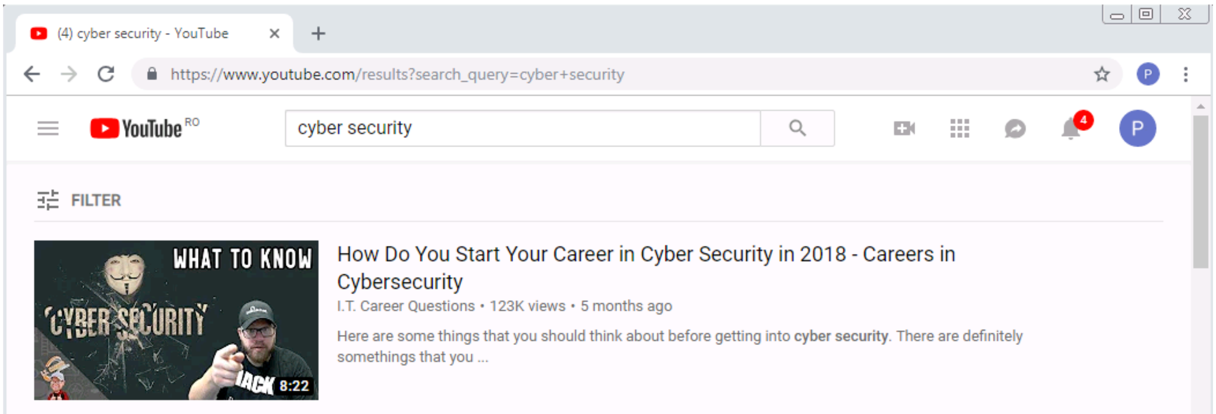
icmp-proto Traffic Accepted from 172.16.10.200 to 8.8.8.8

Matched Rules

Rule	Layer	Rule Name	Action	Application	Category
4	Network	Traffic to Outside	Accept		

Traffic is accepted and we can see that it was matched by rule 4, where we added ICMP-PROTO in the **Services&Applications** column.

On the other hand, web traffic – http and https is working fine, as it is already part of the same rule, rule no. 4. Let's test connectivity to www.youtube.com on the same NY-LAN-1 PC:



(4) cyber security - YouTube

https://www.youtube.com/results?search_query=cyber+security

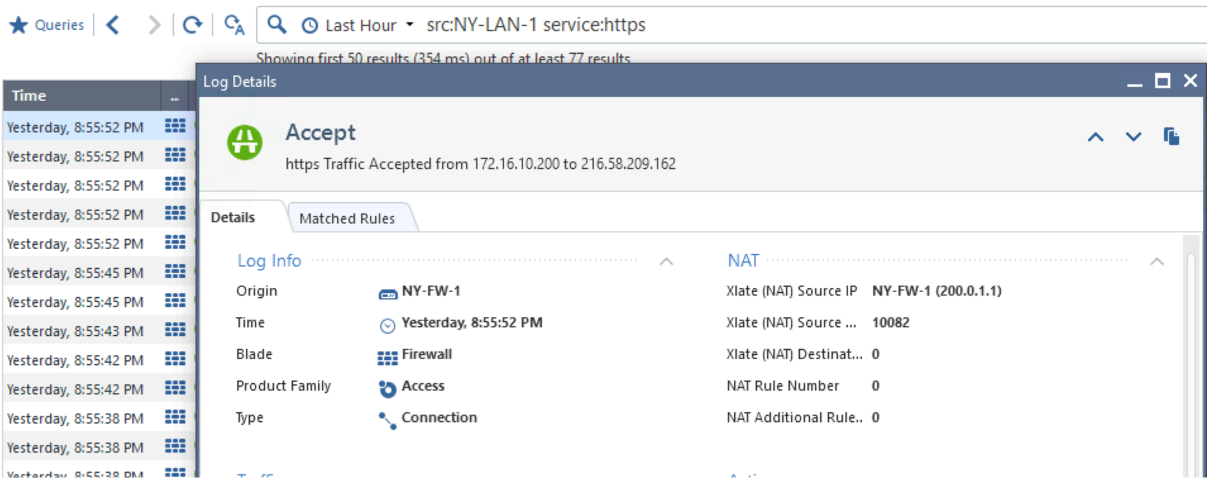
How Do You Start Your Career in Cyber Security in 2018 - Careers in Cybersecurity

I.T. Career Questions • 123K views • 5 months ago

Here are some things that you should think about before getting into cyber security. There are definitely somethings that you ...

Works fine, as expected !

Currently we can not identify in the Logs what was the exact connection to YouTube as traffic is encrypted – HTTPS. We will be able to do this after we configure HTTPS inspection on NY-FW-1, which means we will be able to “look inside” the encrypted packets.


Queries
Last Hour
src:NY-LAN-1 service:https
Showing first 50 results (354 ms) out of at least 77 results
Time
Log Details

Accept

https Traffic Accepted from 172.16.10.200 to 216.58.209.162

Time
Yesterday, 8:55:52 PM
Yesterday, 8:55:52 PM
Yesterday, 8:55:52 PM
Yesterday, 8:55:52 PM
Yesterday, 8:55:52 PM
Yesterday, 8:55:45 PM
Yesterday, 8:55:45 PM
Yesterday, 8:55:43 PM
Yesterday, 8:55:42 PM
Yesterday, 8:55:42 PM
Yesterday, 8:55:38 PM
Yesterday, 8:55:38 PM

Log Info

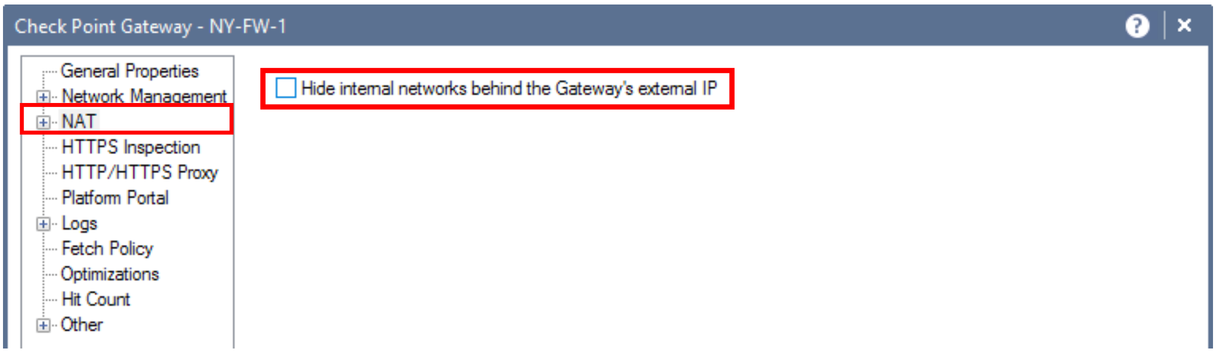
Origin	NY-FW-1
Time	Yesterday, 8:55:52 PM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Source IP	NY-FW-1 (200.0.1.1)
Xlate (NAT) Source ...	10082
Xlate (NAT) Destinat...	0
NAT Rule Number	0
NAT Additional Rule..	0

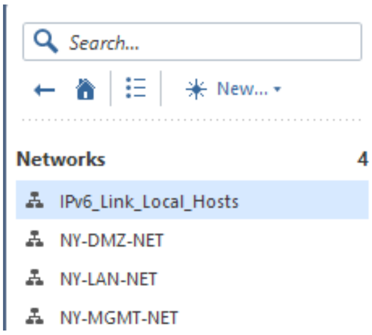
Let’s now enable Hide NAT at the object level. **Why is this option available ?**

Well, maybe you don’t want to enable internet access to all your internal LANs, so this means you will enable it only on desired or needed subnets. Navigate to **Gateways&Servers,** double-click the NY-FW-1, navigate to **NAT** menu and disable the general **Hide NAT** option.

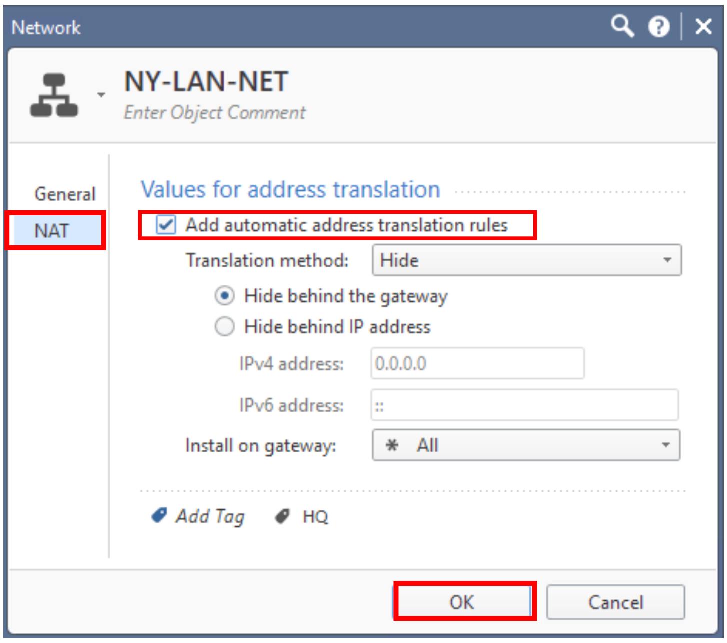


□ Hide internal networks behind the Gateway's external IP

Now, let’s navigate to **Objects** on the right -> **Network Objects -> Networks**:



Double-click **NY-LAN-NET**, go to **NAT** menu and enable **Add automatic address translation rules** option:



Network

NY-LAN-NET

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Hide

● Hide behind the gateway

○ Hide behind IP address

IPv4 address: 0.0.0.0

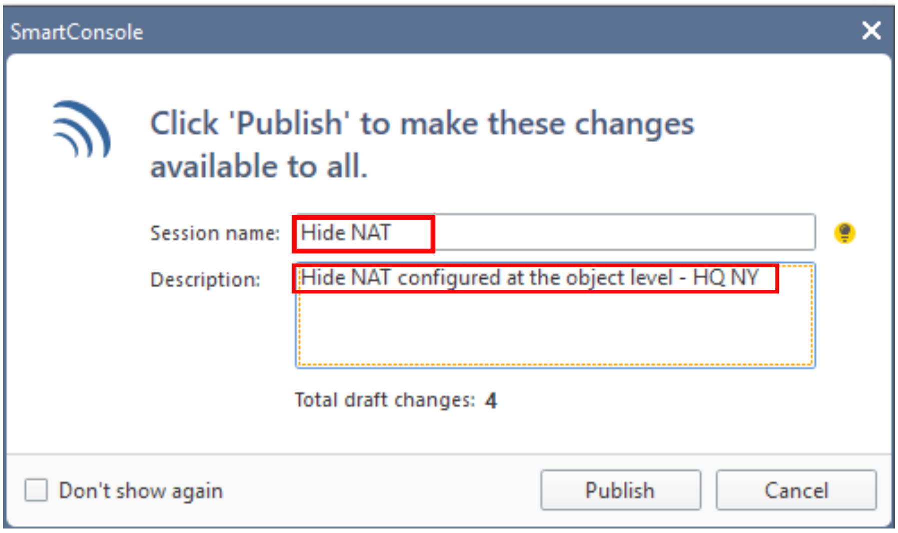
IPv6 address: ::

Install on gateway: ✱ All

Leave the rest of the option as they are. This will enable automatic NAT (so NAT rules will be added automatically to the NAT rule base), the type of NAT is HIDE NAT (Translation method - Hide) and the public IP address of the gateway will be used as the NAT translated IP.

Click **OK** and implement the same setting for the other two subnets – DMZ and MGMT.

Publish the changes:



SmartConsole

Click 'Publish' to make these changes available to all.

Session name: Hide NAT

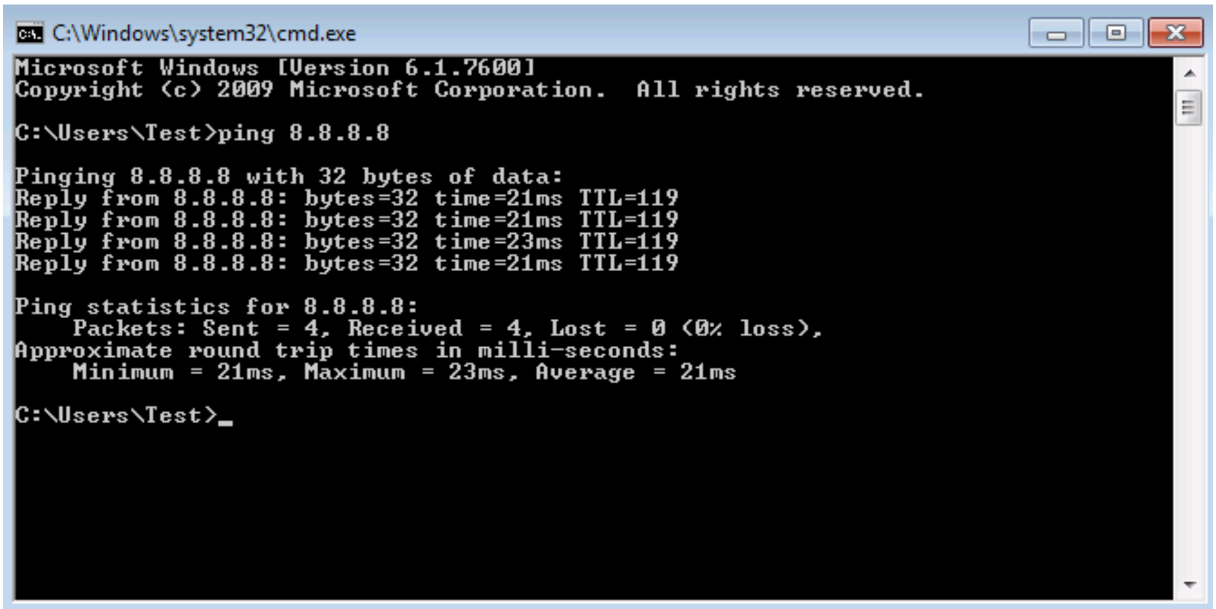
Description: Hide NAT configured at the object level - HQ NY

Total draft changes: 4

☐ Don't show again

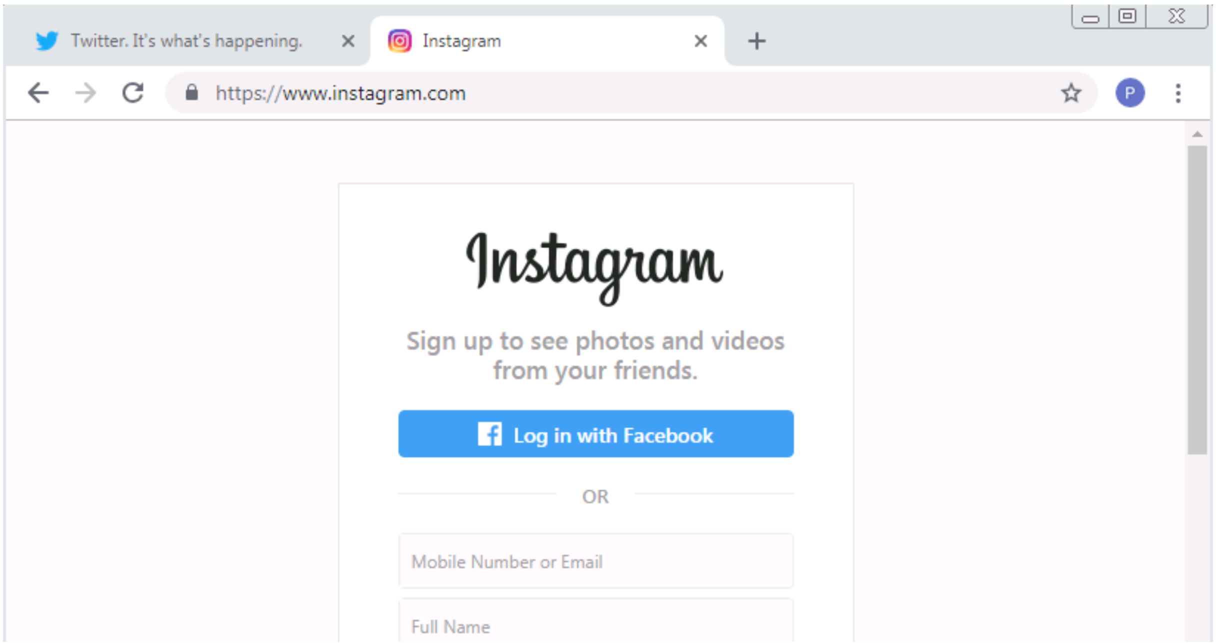
and install the policy.

Let's test again connectivity to internet:

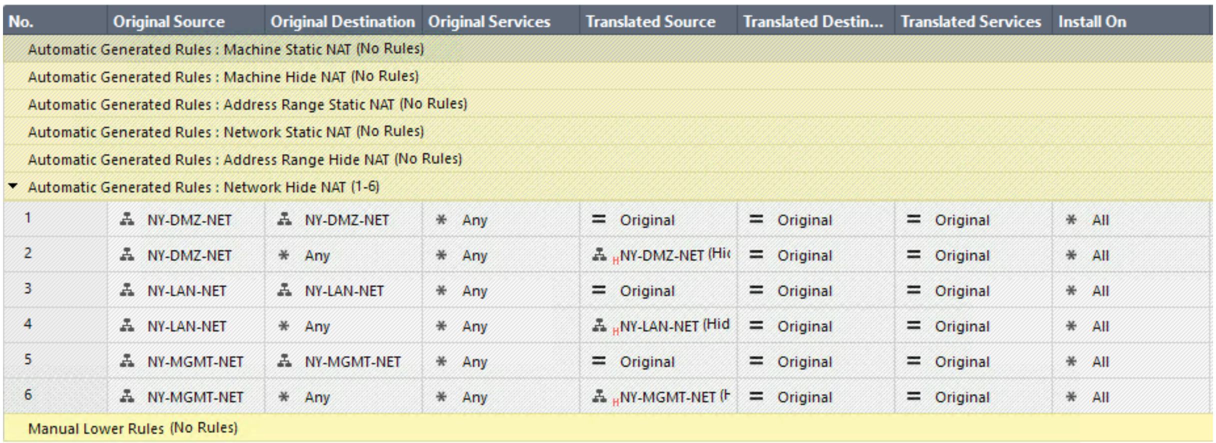


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Test>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=21ms TTL=119
Reply from 8.8.8.8: bytes=32 time=21ms TTL=119
Reply from 8.8.8.8: bytes=32 time=23ms TTL=119
Reply from 8.8.8.8: bytes=32 time=21ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 23ms, Average = 21ms

C:\Users\Test>_
```

And https traffic:


Twitter. It's what's happening.
Instagram
https://www.instagram.com
Instagram
Sign up to see photos and videos from your friends.
Log in with Facebook
OR
Mobile Number or Email
Full Name

Please note that as opposed to the previous configuration, now NAT rules appear in the NAT rule base. SmartConsole created 2 NAT rules for every object hide NAT configuration. First rule prevents NAT from happening when traffic goes inside that specific subnet (i.e. traffic from 2 hosts in the same subnet), while the second NAT rule addresses the hide NAT. In this second rule, please observ that **Original Source** and **Translated Source** columns are being populated.



No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On
Automatic Generated Rules : Machine Static NAT (No Rules)							
Automatic Generated Rules : Machine Hide NAT (No Rules)							
Automatic Generated Rules : Address Range Static NAT (No Rules)							
Automatic Generated Rules : Network Static NAT (No Rules)							
Automatic Generated Rules : Address Range Hide NAT (No Rules)							
Automatic Generated Rules : Network Hide NAT (1-6)							
1	NY-DMZ-NET	NY-DMZ-NET	Any	Original	Original	Original	All
2	NY-DMZ-NET	Any	Any	NY-DMZ-NET (Hi	Original	Original	All
3	NY-LAN-NET	NY-LAN-NET	Any	Original	Original	Original	All
4	NY-LAN-NET	Any	Any	NY-LAN-NET (Hid	Original	Original	All
5	NY-MGMT-NET	NY-MGMT-NET	Any	Original	Original	Original	All
6	NY-MGMT-NET	Any	Any	NY-MGMT-NET (H	Original	Original	All
Manual Lower Rules (No Rules)							

As this NAT is configured at the network object level, the rules appear under **Automatic Generated Rules: Network Hide NAT.**

20.0 Lab: Configure Static NAT in New York Site

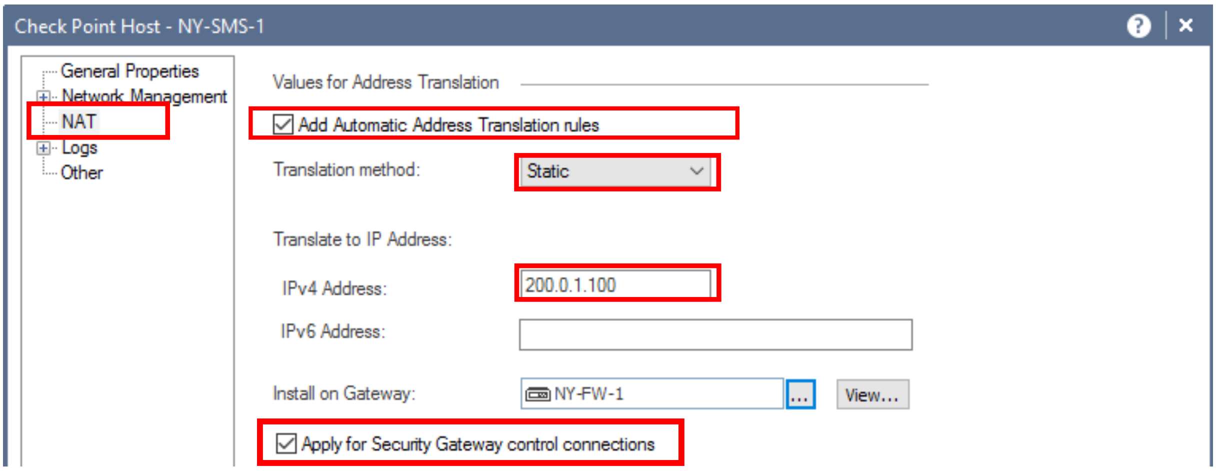
Lab Objectives

- Configure Static NAT for SMS, DMZ and AD servers
- Verify and test Static NAT configuration

In this lab, we will configure static NAT for several objects in NY HQ site. The difference between static and hide NAT is that through static NAT we "publish" the internal NY objects and make them available for access from outside world, from the internet. Specifically, the NY-SMS-1 management server must be available for connections from L-FW-1 in order to register this new gateways and be able to remotely manage it. Next, the DMZ server, as it will both a web and ftp server, it needs to be accessible by remote users, from the outside world. Same applies for AD server, which is needed for remote users connecting to HQ site.

Let's start with NY-SMS-1 management server.

Navigate to **Object** on the right-side of SmartConsole and edit NY-SMS-1 object. Go to **NAT** menu on the left and fill in the details, as outlined below:


Check Point Host - NY-SMS-1

Values for Address Translation

☑ Add Automatic Address Translation rules

Translation method: Static

Translate to IP Address:

IPv4 Address: 200.0.1.100

IPv6 Address:

Install on Gateway: NY-FW-1

☑ Apply for Security Gateway control connections

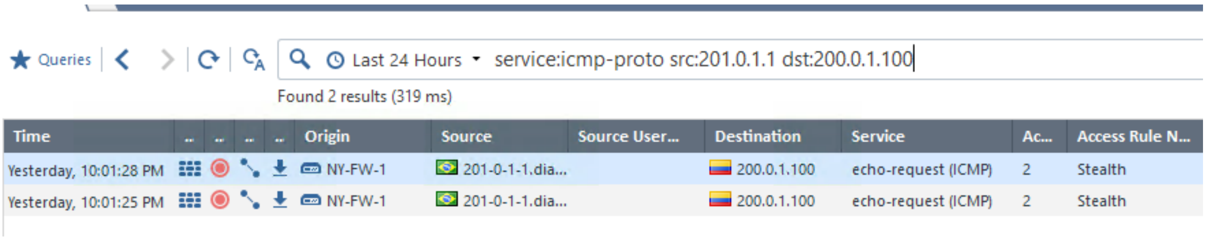
First enable **Add Automatic Address Translation rules**, define the Translation method as **Static**, fill in the public IP address which will be mapped to the SMS private IP address, select on which SG will this NAT rule be applied and very important enable **Apply for Security Gateway control connections**. This last option relates to the fact that control or management connections will be done through this public IP for management of remote gateways.

Click **OK** when done.

Let’s test the configuration. Go the L-FW-1 cli and ping 200.0.1.100 the public IP mapped to NY-SMS-1:

```
L-FW-1> ping 200.0.1.100
PING 200.0.1.100 (200.0.1.100) 56(84) bytes of data.

--- 200.0.1.100 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5001ms
```

ICMP session is not successful. Let’s investigate in **Logs&Monitor**:



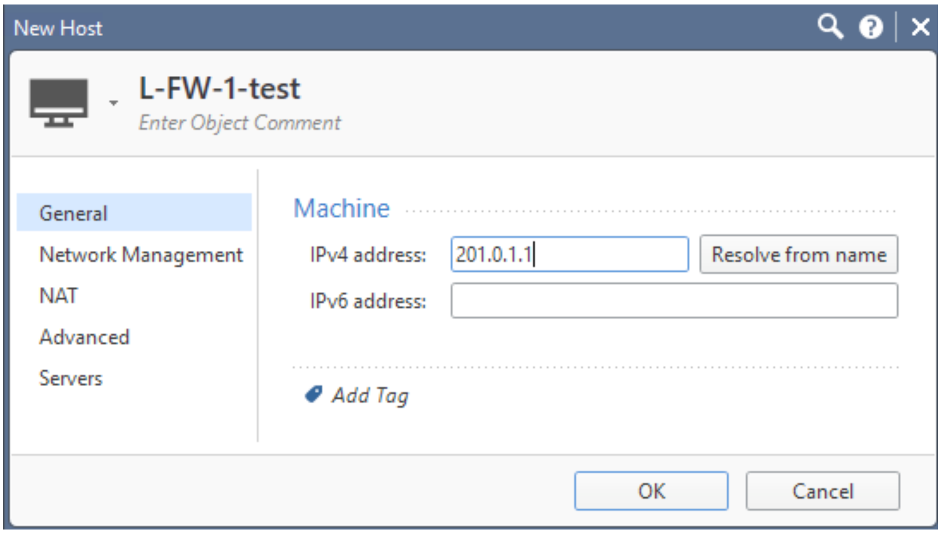
Last 24 Hours service:icmp-proto src:201.0.1.1 dst:200.0.1.100

Found 2 results (319 ms)

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Yesterday, 10:01:28 PM					NY-FW-1	201-0-1-1.dia...		200.0.1.100	echo-request (ICMP)	2	Stealth
Yesterday, 10:01:25 PM					NY-FW-1	201-0-1-1.dia...		200.0.1.100	echo-request (ICMP)	2	Stealth

Ok, so we see that traffic was dropped because of Stealth rule, which dictates who can access NY-SMS-1 and NY-FW-1 and this is NY-MGMT-PC and only this host. Also, please note that only https and sshv2 protocols are permitted.

So, in order to test and have the test functional, we should test with ssh for example and, again, as a test, add the IP of L-FW-1 to the list of hosts permitted to manage NY-SMS-1, so in rule 1 – Management. Let’s create a host object – **L-FW-1-test:**



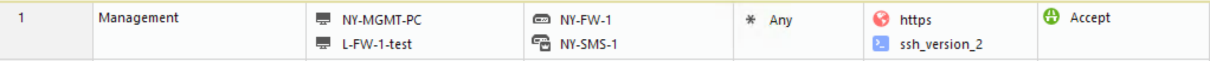
L-FW-1-test

Enter Object Comment

IPv4 address: 201.0.1.1

IPv6 address:

and modify rule 1 – Management:



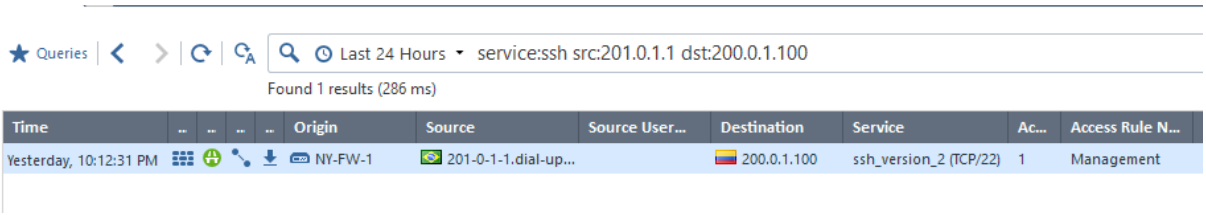
1	Management	NY-MGMT-PC L-FW-1-test	NY-FW-1 NY-SMS-1	Any	https ssh_version_2	Accept

Now, in the source column, we also have L-FW-1-test object, which means that https and ssh version2 traffic from this host should be permitted. As icmp is not in the list, it makes no sense to try it. Let’s try to ssh to NY-SMS-1 from L-FW-1, this should work as ssh is permitted. Login to expert mode in L-FW-1 and initiate ssh connection:

```
L-FW-1> expert
Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@L-FW-1:0]# ssh admin@200.0.1.100
The authenticity of host '200.0.1.100 (200.0.1.100)' can't be established.
RSA key fingerprint is 66:ea:5d:1d:81:70:51:50:32:cd:eb:1d:3c:6f:57:d0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '200.0.1.100' (RSA) to the list of known hosts.
This system is for authorized use only.
admin@200.0.1.100's password: <admin123>   <<< password entered in this step
Last login: Fri Feb  1 03:48:17 2019
NY-SMS-1>
NY-SMS-1>
```

Great, this validates completely that static NAT is correct and NY-SMS-1 is reachable from internet.

Finally, let’s examine the Logs. Filter the Logs by entering in the search bar the following: **service:ssh src:200.0.1.1 dst:200.0.1.100**

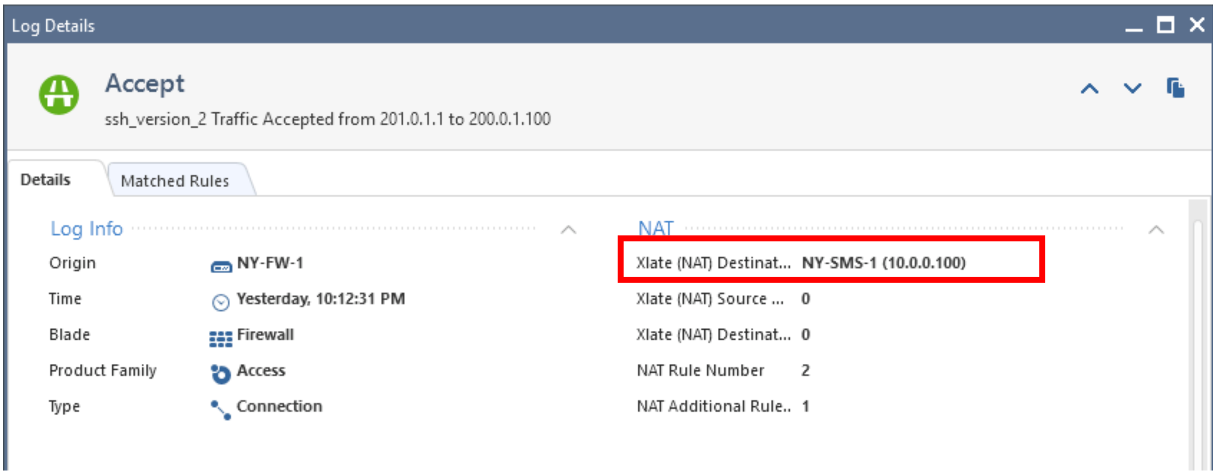


service:ssh src:201.0.1.1 dst:200.0.1.100

Found 1 results (286 ms)

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Yesterday, 10:12:31 PM					NY-FW-1	201-0-1-1.dial-up...		200.0.1.100	ssh_version_2 (TCP/22)	1	Management

The session is permitted, we saw it already, this confirms it with logging. Double-click it and take a look inside also.



Log Details

Accept

ssh_version_2 Traffic Accepted from 201.0.1.1 to 200.0.1.100

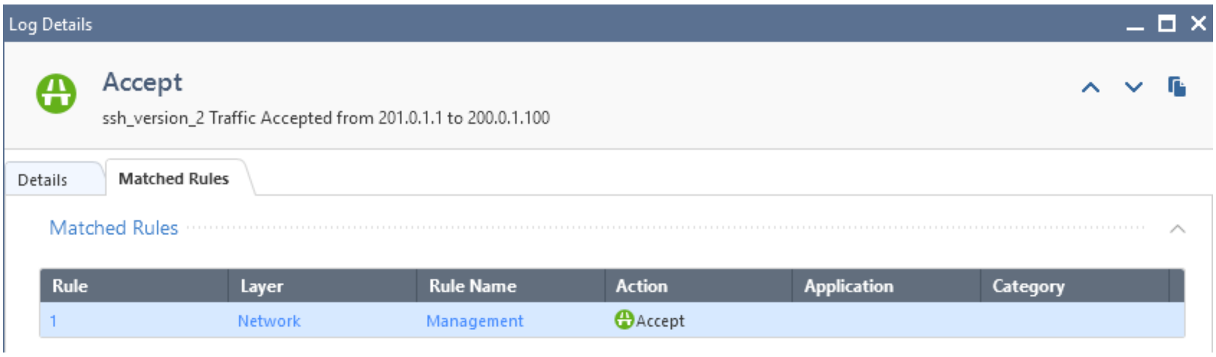
Log Info

Origin	NY-FW-1
Time	Yesterday, 10:12:31 PM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Destinat...	NY-SMS-1 (10.0.0.100)
Xlate (NAT) Source ...	0
Xlate (NAT) Destinat...	0
NAT Rule Number	2
NAT Additional Rule..	1

NAT was performed and specifically in this direction, internet to inside, the destination was NATted, from 200.0.1.100 to 10.0.0.100, as you can see in the log. If you click on **Matched Rules**, you will see that the session was matched by **Management** rule:



Log Details

Accept

ssh_version_2 Traffic Accepted from 201.0.1.1 to 200.0.1.100

Matched Rules

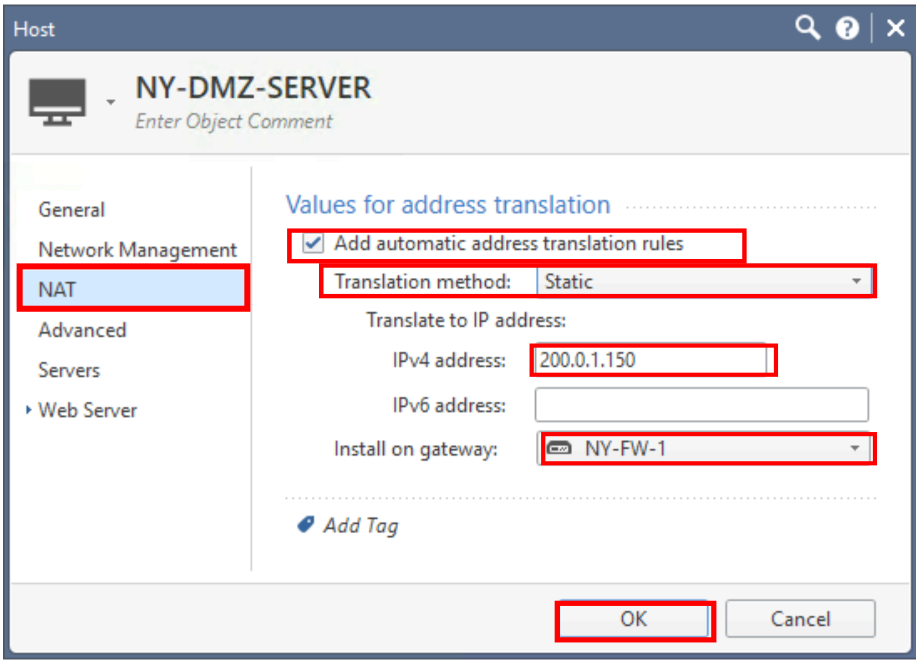
Rule	Layer	Rule Name	Action	Application	Category
1	Network	Management	Accept		

Don’t forget to clean the configuration :

- Rule 1 – Management, erase NY-LAN-1-test
- Delete NY-LAN-1-test object from SmartConsole

Now, let’s configure static NAT for NY-DMZ and NY-AD servers.

Navigate to **Objects** and edit NY-DMZ-SERVER object. Navigate to **NAT** menu and configure the settings as outlined below:



NY-DMZ-SERVER

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Static

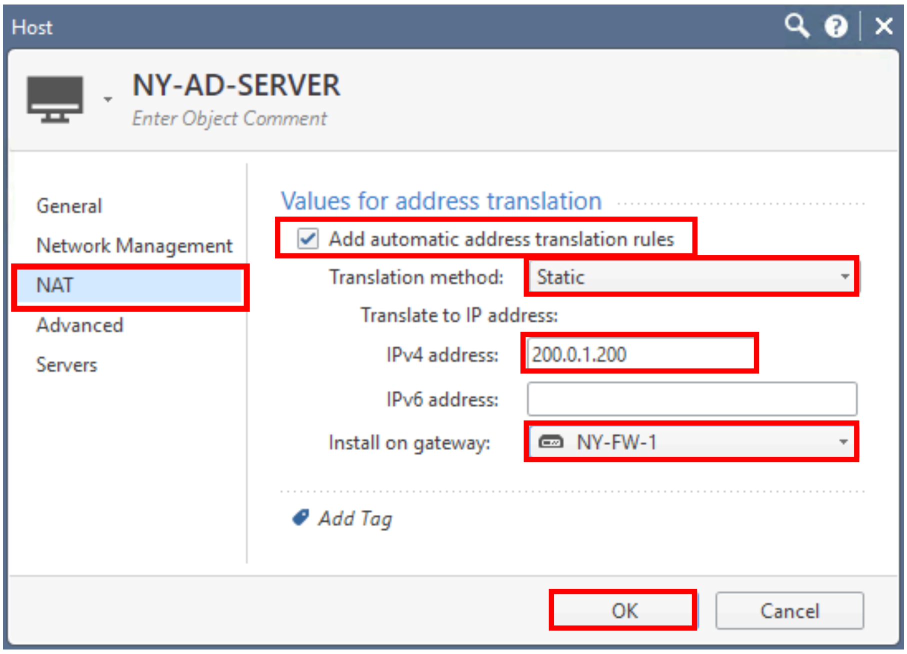
Translate to IP address:

IPv4 address: 200.0.1.150

IPv6 address:

Install on gateway: NY-FW-1

Now edit the NY-AD-SERVER also:



NY-AD-SERVER

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Static

Translate to IP address:

IPv4 address: 200.0.1.200

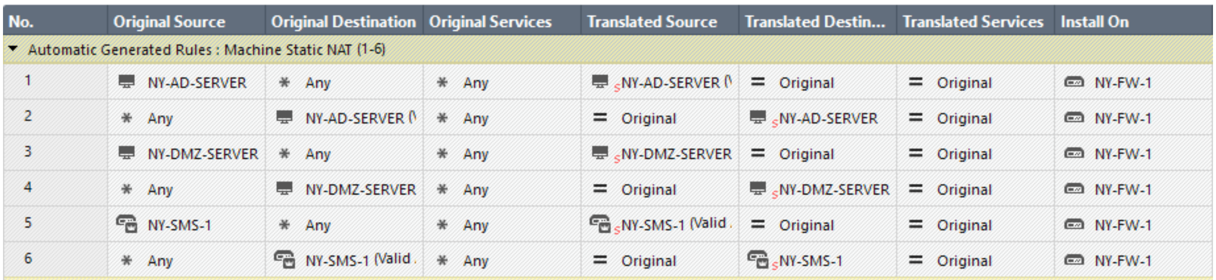
IPv6 address:

Install on gateway: NY-FW-1

Publish the changes and install the policy.

Now, if you take a look at the NAT Rule Base, you will see the rule base populated with entries in the **Machine Static NAT** category.

The NAT Rule Base should look like below:



No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On
▾ Automatic Generated Rules : Machine Static NAT (1-6)							
1	NY-AD-SERVER	* Any	* Any	NY-AD-SERVER (	= Original	= Original	NY-FW-1
2	* Any	NY-AD-SERVER (	* Any	= Original	NY-AD-SERVER	= Original	NY-FW-1
3	NY-DMZ-SERVER	* Any	* Any	NY-DMZ-SERVER	= Original	= Original	NY-FW-1
4	* Any	NY-DMZ-SERVER	* Any	= Original	NY-DMZ-SERVER	= Original	NY-FW-1
5	NY-SMS-1	* Any	* Any	NY-SMS-1 (Valid .	= Original	= Original	NY-FW-1
6	* Any	NY-SMS-1 (Valid .	* Any	= Original	NY-SMS-1	= Original	NY-FW-1

In order to test connectivity to NY-DMZ-SERVER, web and ftp server, we would need to first install these two functionalities on the Ubuntu DMZ server.

This will be addressed separately in the next lab and after that we will be able to test web and ftp access, from outside world (London LAN user and or Remote User).

21.0 Lab: Configure NY-DMZ-SERVER as HTTP and FTP server

Lab Objectives

- Enable HTTP and FTP functionalities on NY-DMZ-SERVER
- Verify and test access to HTTP and FTP server from outside user

NY-DMZ-SERVER is a Ubuntu 18.04 machine. In order for it to be an HTTP and FTP server, it needs to be configured so that it will serve this roles.

Let’s first start with HTTP server role.

As with any Linux machine, it’s a good idea to start with getting your machine up to date. The two commands to run here are **sudo apt-get update** and **sudo apt-get upgrade**. **Sudo** keyword is the equivalent in Windows operating systems when you right-click on an item and select **Run as Administrator**.

```
user@Ubuntu18:~$ sudo apt-get update
[sudo] password for user: <type_user_password_here>
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic InRelease [242 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:4 http://security.ubuntu.com/ubuntu bionic-security/main i386 Packages [197 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]

<output omitted>

Get:68 http://us.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP-11
Metadata [7,344 B]
Get:69 http://us.archive.ubuntu.com/ubuntu bionic-backports/universe DEP-11 48x48
Icons [29 B]
Get:70 http://us.archive.ubuntu.com/ubuntu bionic-backports/universe DEP-11 64x64
Icons [29 B]
Fetched 45.4 MB in 14s (3,301 kB/s)
Reading package lists... Done
user@Ubuntu18:~$
user@Ubuntu18:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done

<output omitted>
```

```
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 base-files
amd64 10.1ubuntu2.3 [60.4 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 bsdutils amd64
1:2.31.1-0.4ubuntu3.3 [60.4 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 tar amd64
1.29b-2ubuntu0.1 [234 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 dpkg amd64
1.19.0.5ubuntu2.1 [1,140 kB

<output omitted>

Setting up libreoffice-help-en-us (1:6.0.7-0ubuntu0.18.04.2) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for initramfs-tools (0.130ubuntu3) ...
update-initramfs: Generating /boot/initrd.img-4.15.0-20-generic
Processing triggers for dbus (1.12.2-1ubuntu1) ...
user@Ubuntu18:~$
```

Depending on your hardware that you are running your lab topology on, you can expect around 15-30 minutes for the update and upgrade to finish. Also, very important is the bandwidth that Ubuntu server has available, because it will download a lot of packets from Ubuntu repositories – from the internet.

I am currently using as the Internet Router the Mikrotik RouterOS. Consumes very little CPU and memory and doesn't limit bandwidth. Great choice, I highly recommend it, and there is also a video lecture published on #howto setup the Mikrotik Router.

Let's now launch the Apache Web server installation:

```
user@Ubuntu18:~$ sudo apt-get install apache2
[sudo] password for user: <type_user_password_here >
Reading package lists... Done

<output omitted>

Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libapr1 amd64 1.6.3-2
[90.9 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1 amd64 1.6.1-
2 [84.4 kB]
```

```
<output omitted>

Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.11) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for ufw (0.35-5) ...
user@Ubuntu18:~$
```

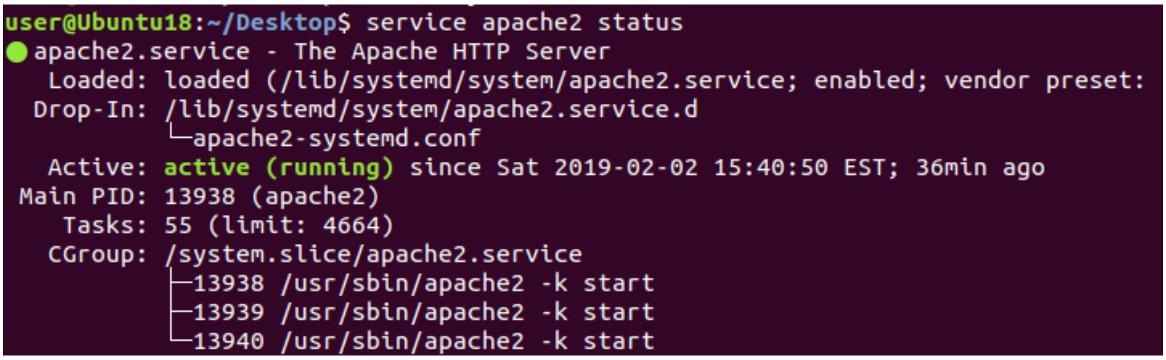
There are several profiles available on the machine now, as related to HTTP service. The “Apache Full” enables access to HTTP and HTTPS (ports 80 and 443). Let’s verify this:

```
user@Ubuntu18:~$ sudo ufw app info "Apache Full"
Profile: Apache Full
Title: Web Server (HTTP,HTTPS)
Description: Apache v2 is the next generation of the omnipresent Apache web
server.

Ports:
  80,443/tcp
```

We will apply this profile on incoming direction in order to permit access to http and https. Actually we are allowing this by updating the firewall rules of the Ubuntu server:

```
user@Ubuntu18:~$ sudo ufw allow in "Apache Full"
Rules updated
Rules updated (v6)
user@Ubuntu18:~$
```

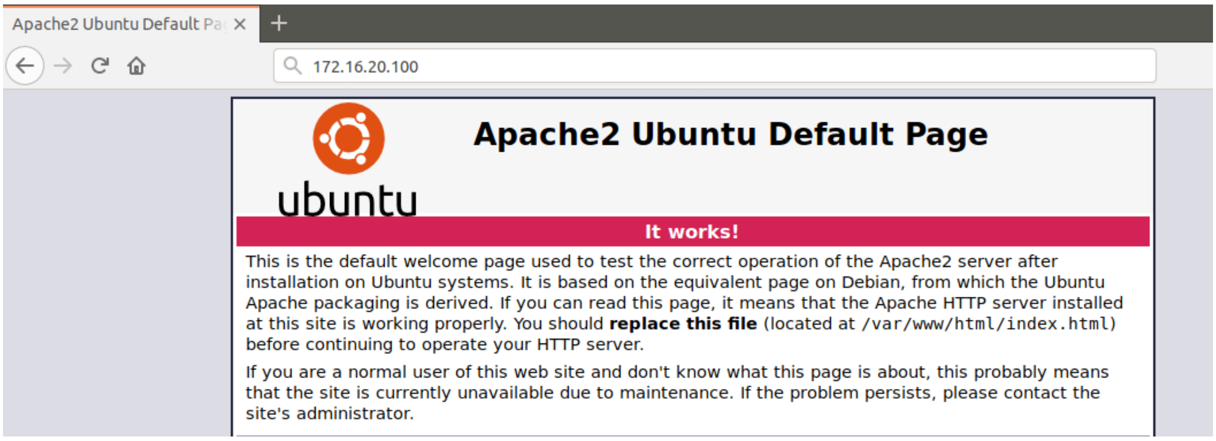
Now, we can do a fast test and see if the server is running, both on cli and trying to actually access the default home page. On the cli, you can run the following command : **service apache2 status**



```
user@Ubuntu18:~/Desktop$ service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset:
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Sat 2019-02-02 15:40:50 EST; 36min ago
 Main PID: 13938 (apache2)
    Tasks: 55 (limit: 4664)
   CGroup: /system.slice/apache2.service
           ├─13938 /usr/sbin/apache2 -k start
           ├─13939 /usr/sbin/apache2 -k start
           └─13940 /usr/sbin/apache2 -k start
```

Open Firefox browser and navigate to http://172.16.20.100, the NY-DMZ-SERVER internal IP address:

The browser should return the default web page after a successful apache2 package installation:



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Now, let’s continue and install FTP service. First thing, we install the VSFTPD package:

```
user@Ubuntu18:~$ sudo apt-get install vsftpd
[sudo] password for user:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  Vsftpd

<output omitted>

user@Ubuntu18:~$
```

Before we do anything, let' make a backup of a current VSFTPD server configuration file and then edit the vsftpd.conf file :

```
user@Ubuntu18:~$ sudo mv /etc/vsftpd.conf /etc/vsftpd.conf_orig
user@Ubuntu18:~$
user@Ubuntu18:~$ sudo nano /etc/vsftpd.conf
```

A new window will open, corresponding to vsftpd.conf file. The following code represents a simple FTP server configuration, just copy and paste it inside:

```
listen=NO
listen_ipv6=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
pasv_enable=Yes
pasv_min_port=10000
pasv_max_port=10100
allow_writeable_chroot=YES
```

CTRL+X after you pasted the configuration and press “**Y**” on your keyboard in order to accept the changes.
Please run the next command in order to allow incoming traffic to FTP ports:

```
user@Ubuntu18:~$ sudo ufw allow from any to any port 20,21,10000:10100 proto tcp
Rules updated
Rules updated (v6)
user@Ubuntu18:~$
```

And restart VSFTP server in order to apply the new changes:

```
user@Ubuntu18:~$ sudo service vsftpd restart
```

Next, let’s create a FTP user and password pair that will be used for authentication when connecting to the FTP server:

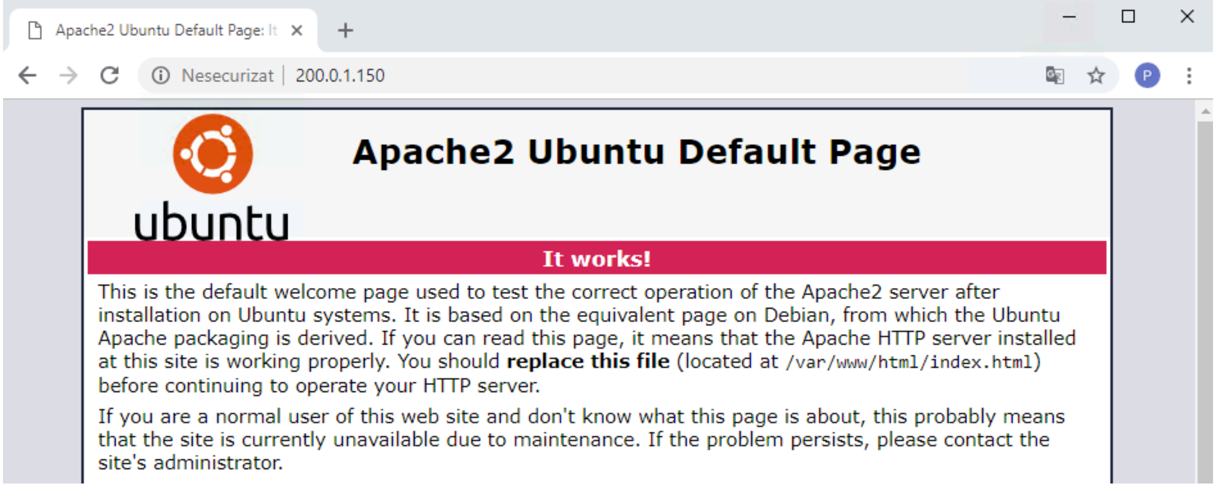
```
user@Ubuntu18:~$ sudo useradd -m ftpuser
user@Ubuntu18:~$ sudo passwd ftpuser
Enter new UNIX password: <admin123>
Retype new UNIX password: <admin123>
passwd: password updated successfully
```

Now, I will create a simple text file that will be accessible to user that connects to FTP server.

```
user@Ubuntu18:~$ sudo bash -c "echo FTP TEST CCSA R80.10 BOOTCAMP >
/home/ftpuser/FTP-TEST"
user@Ubuntu18:~$
user@Ubuntu18:~$ cat /home/ftpuser/FTP-TEST
FTP TEST CCSA R80.10 BOOTCAMP
```

Installation of both WEB and FTP services on NY-DMZ-SERVER is complete. It's now time to test access to these services from "outside world", from the internet. We will initiate http and ftp sessions from the REMOTE_USER Windows PC.

We will start first with HTTP. Open a browser and navigate to the public static NAT IP that we configured for NY-DMZ-SERVER : http://200.0.1.150



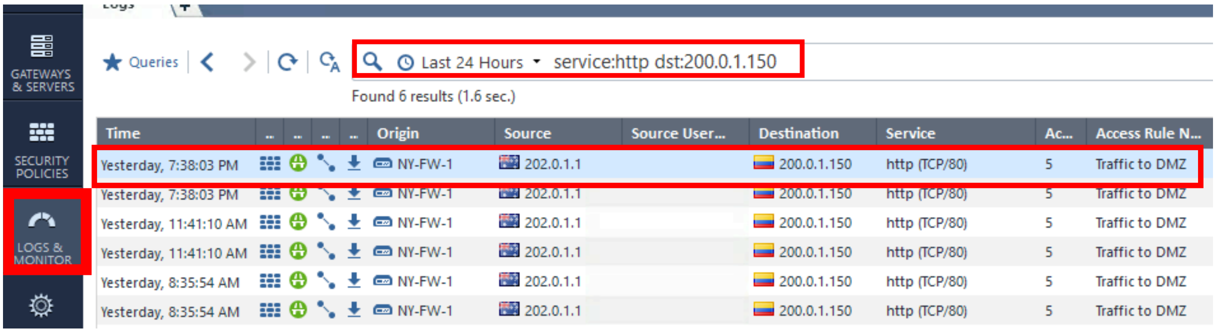
Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

The page loads successfully. Let's now investigate this through **Logs&Monitor** in SmartConsole. In the search bar, enter the following filter: **service:http dst:200.0.1.150** -> HTTP traffic with a destination of 200.0.1.150

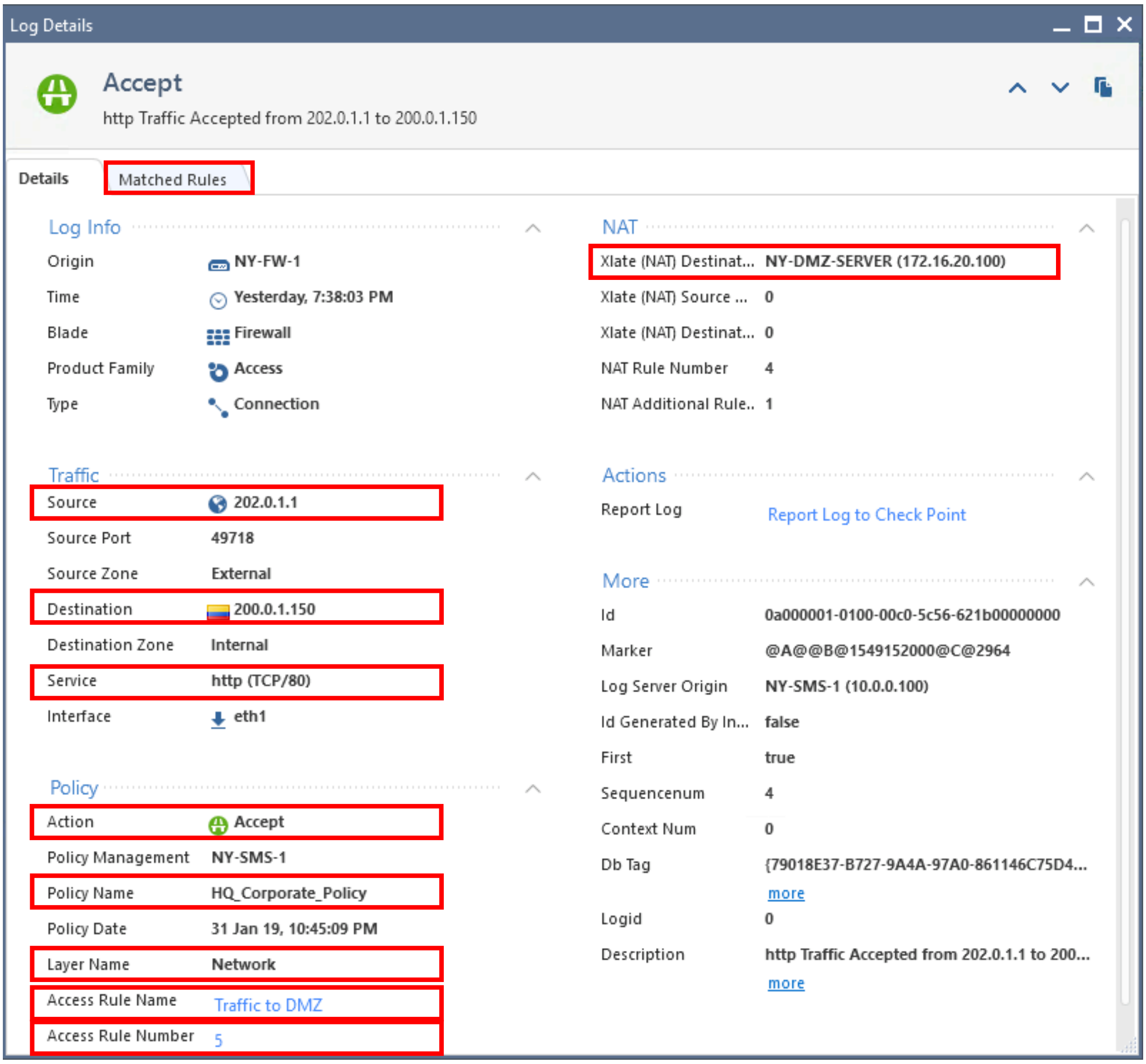


Last 24 Hours service:http dst:200.0.1.150

Found 6 results (1.6 sec.)

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Yesterday, 7:38:03 PM					NY-FW-1	202.0.1.1		200.0.1.150	http (TCP/80)	5	Traffic to DMZ
Yesterday, 7:38:03 PM					NY-FW-1	202.0.1.1		200.0.1.150	http (TCP/80)	5	Traffic to DMZ
Yesterday, 11:41:10 AM					NY-FW-1	202.0.1.1		200.0.1.150	http (TCP/80)	5	Traffic to DMZ
Yesterday, 11:41:10 AM					NY-FW-1	202.0.1.1		200.0.1.150	http (TCP/80)	5	Traffic to DMZ
Yesterday, 8:35:54 AM					NY-FW-1	202.0.1.1		200.0.1.150	http (TCP/80)	5	Traffic to DMZ
Yesterday, 8:35:54 AM					NY-FW-1	202.0.1.1		200.0.1.150	http (TCP/80)	5	Traffic to DMZ

Double-click on most recent log to open it and let's analyze it.



Log Details

Accept

http Traffic Accepted from 202.0.1.1 to 200.0.1.150

Details | Matched Rules

Log Info

Origin	NY-FW-1
Time	Yesterday, 7:38:03 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	202.0.1.1
Source Port	49718
Source Zone	External
Destination	200.0.1.150
Destination Zone	Internal
Service	http (TCP/80)
Interface	eth1

Policy

Action	Accept
Policy Management	NY-SMS-1
Policy Name	HQ_Corporate_Policy
Policy Date	31 Jan 19, 10:45:09 PM
Layer Name	Network
Access Rule Name	Traffic to DMZ
Access Rule Number	5

NAT

Xlate (NAT) Destinat...	NY-DMZ-SERVER (172.16.20.100)
Xlate (NAT) Source ...	0
Xlate (NAT) Destinat...	0
NAT Rule Number	4
NAT Additional Rule..	1

Actions

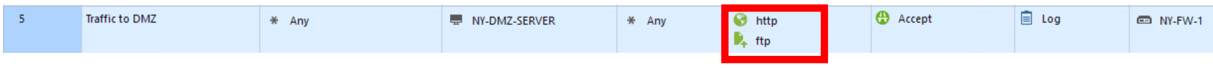
Report Log	Report Log to Check Point

More

Id	0a000001-0100-00c0-5c56-621b00000000
Marker	@A@@B@1549152000@C@2964
Log Server Origin	NY-SMS-1 (10.0.0.100)
Id Generated By In...	false
First	true
Sequencenum	4
Context Num	0
Db Tag	{79018E37-B727-9A4A-97A0-861146C75D4... more
Logid	0
Description	http Traffic Accepted from 202.0.1.1 to 200... more

HTTP traffic – service http (TCP 80) is coming from source 202.0.1.1, going to 200.0.1.150. Destination NAT is performed and the real destination IP of this traffic is 172.16.20.100 – the NY-DMZ-SERVER.

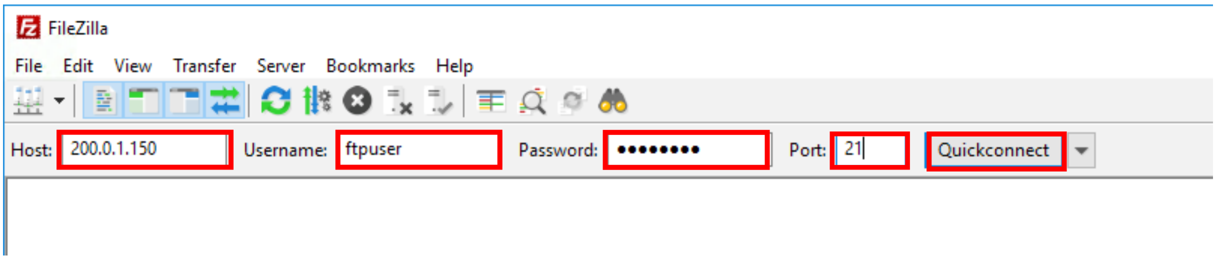
Packets are matched against HQ_Corporate_Policy and specifically by Network (this is the name) layer, the Access Rule name – Traffic to DMZ, rule number 5. If you click on rule 5, it will open in the background:



5	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Accept	Log	NY-FW-1

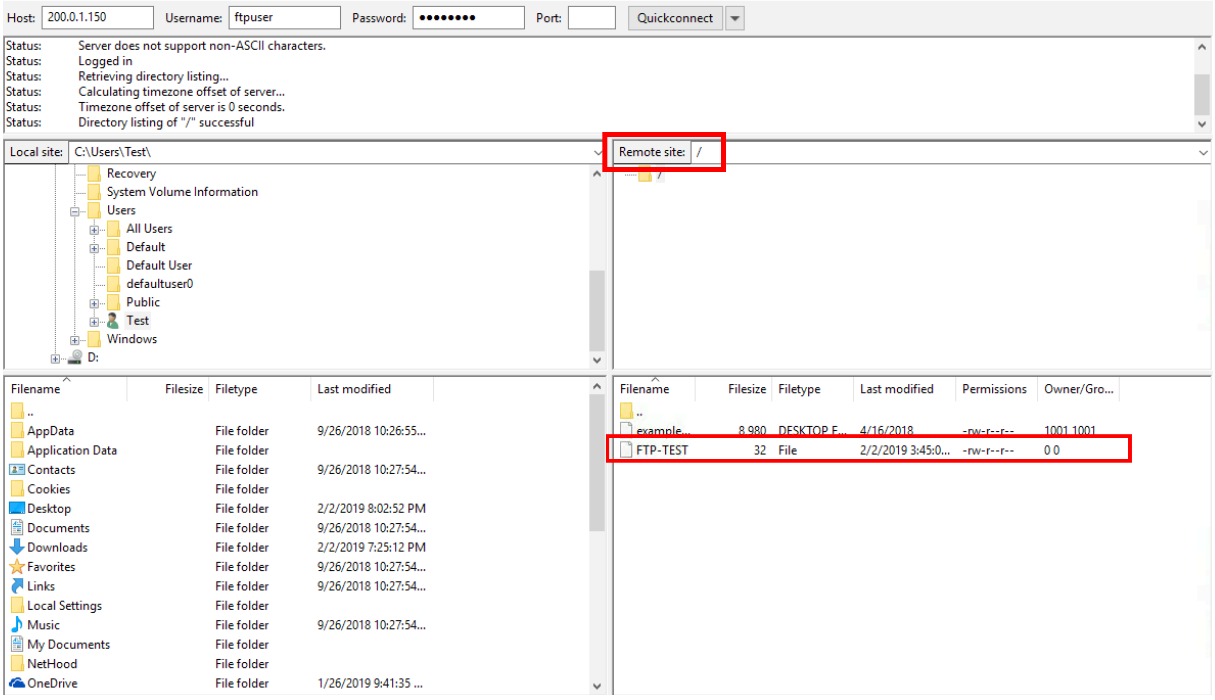
Traffic to be matched in this rule : http and ftp.

Now, let's initiate a FTP session from the REMOTE_USER PC. Open Filezilla FTP client on the PC and initiate a FTP session to the DMZ:



Host: 200.0.1.150 Username: ftpuser Password: •••••••• Port: 21

Side note, username is ftpuser, password is **admin123**, as we defined it earlier on NY-DMZ-SERVER. Click **Quickconnect**



Host: 200.0.1.150 Username: ftpuser Password: •••••••• Port:

```
Status:    Server does not support non-ASCII characters.
Status:    Logged in
Status:    Retrieving directory listing...
Status:    Calculating timezone offset of server...
Status:    Timezone offset of server is 0 seconds.
Status:    Directory listing of "/" successful
```

Local site: C:\Users\Test\

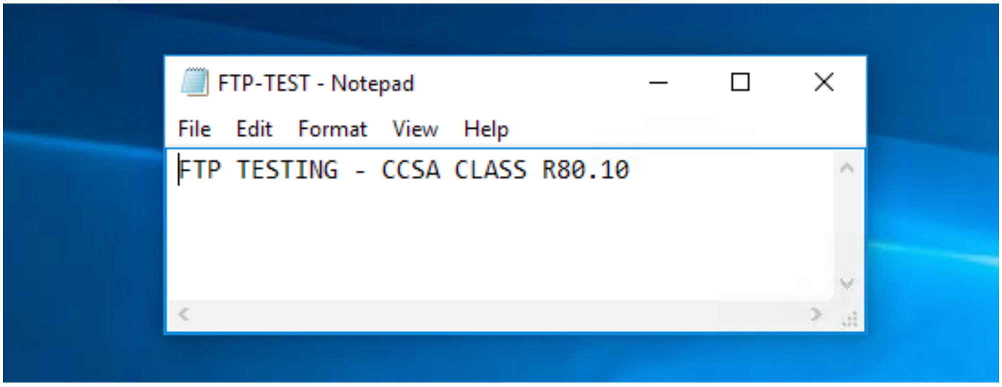
Remote site: /

```
Recovery
System Volume Information
Users
    All Users
    Default
    Default User
    defaultuser0
    Public
    Test
Windows
D:
```

Filename	Filesize	Filetype	Last modified
..			
AppData		File folder	9/26/2018 10:26:55...
Application Data		File folder	
Contacts		File folder	9/26/2018 10:27:54...
Cookies		File folder	
Desktop		File folder	2/2/2019 8:02:52 PM
Documents		File folder	9/26/2018 10:27:54...
Downloads		File folder	2/2/2019 7:25:12 PM
Favorites		File folder	9/26/2018 10:27:54...
Links		File folder	9/26/2018 10:27:54...
Local Settings		File folder	
Music		File folder	9/26/2018 10:27:54...
My Documents		File folder	
NetHood		File folder	
OneDrive		File folder	1/26/2019 9:41:35 ...

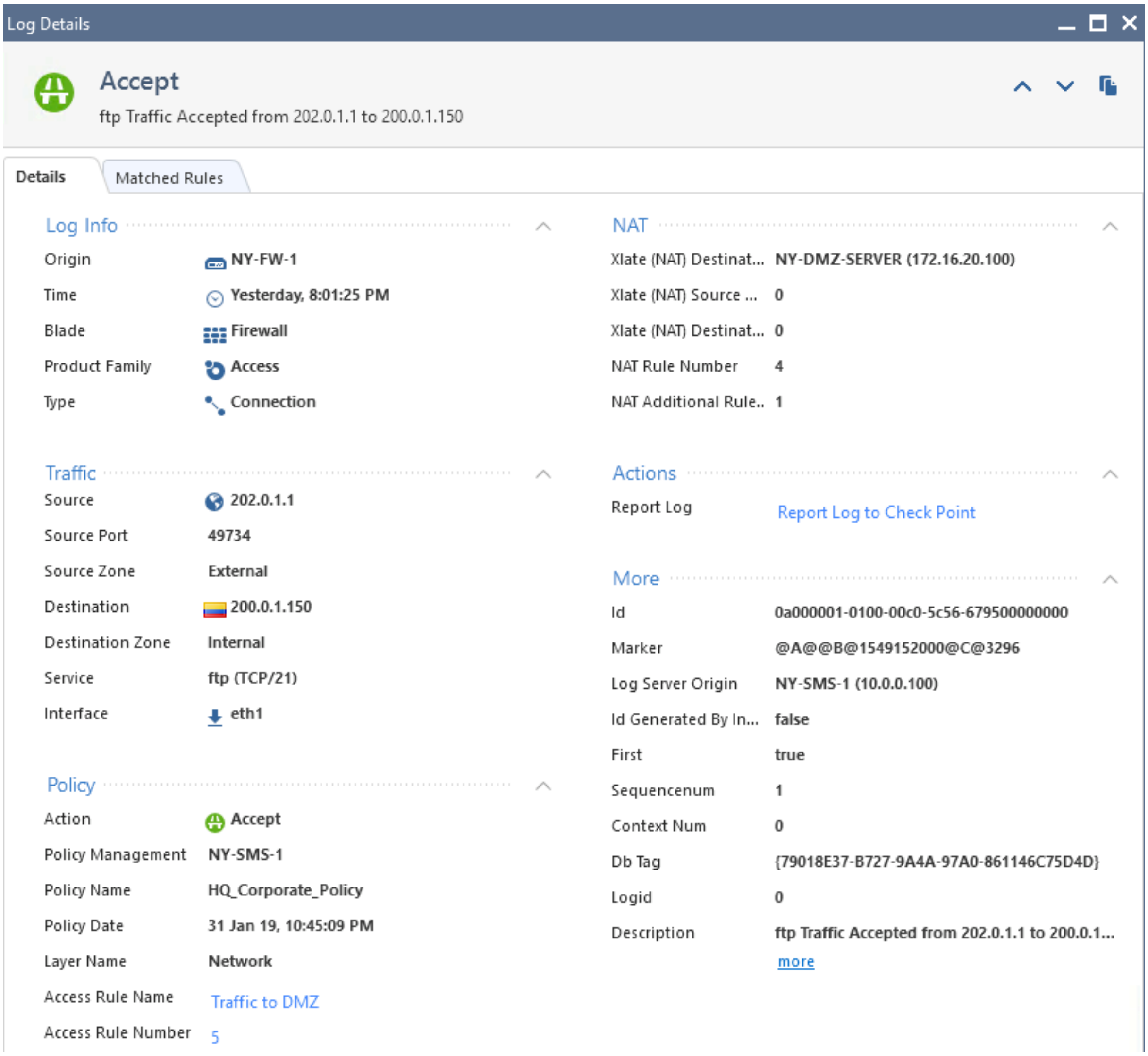
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
example...	8,980	DESKTOP F...	4/16/2018	-rw-r--r--	1001 1001
FTP-TEST	32	File	2/2/2019 3:45:0...	-rw-r--r--	0 0

On the Remote site, after successfully connecting to FTP server, we see the FTP-TEST file available for download. Remember that we defined this file earlier. Either right-click on FTP-TEST file or select it and drag-and-drop on the Desktop and open it :



```
FTP TESTING - CCSA CLASS R80.10
```

Let’s quickly now identify this traffic in Logs&Monitor. In the search bar, filter the logs with the following: **service:ftp dst:200.0.1.150**



Log Details

Accept

ftp Traffic Accepted from 202.0.1.1 to 200.0.1.150

Log Info

Origin	NY-FW-1
Time	Yesterday, 8:01:25 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	202.0.1.1
Source Port	49734
Source Zone	External
Destination	200.0.1.150
Destination Zone	Internal
Service	ftp (TCP/21)
Interface	eth1

Policy

Action	Accept
Policy Management	NY-SMS-1
Policy Name	HQ_Corporate_Policy
Policy Date	31 Jan 19, 10:45:09 PM
Layer Name	Network
Access Rule Name	Traffic to DMZ
Access Rule Number	5

NAT

Xlate (NAT) Destinat...	NY-DMZ-SERVER (172.16.20.100)
Xlate (NAT) Source ...	0
Xlate (NAT) Destinat...	0
NAT Rule Number	4
NAT Additional Rule..	1

Actions

Report Log	Report Log to Check Point

More

Id	0a000001-0100-00c0-5c56-679500000000
Marker	@A@@B@1549152000@C@3296
Log Server Origin	NY-SMS-1 (10.0.0.100)
Id Generated By In...	false
First	true
Sequencenum	1
Context Num	0
Db Tag	{79018E37-B727-9A4A-97A0-861146C75D4D}
Logid	0
Description	ftp Traffic Accepted from 202.0.1.1 to 200.0.1... more

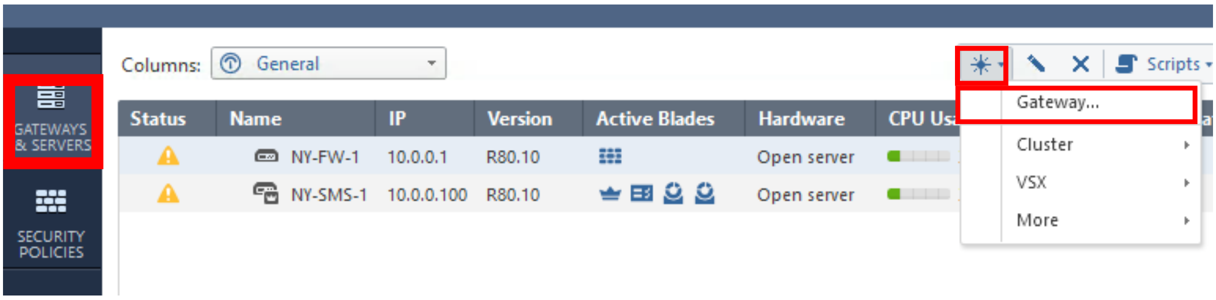
22.0 Lab: Add Remote London Security Gateway to NY-SMS-1 Management Server

Lab Objectives

- Create and add new remote gateway to NY-SMS-1
- Establish and validate SIC with NY-SMS-1

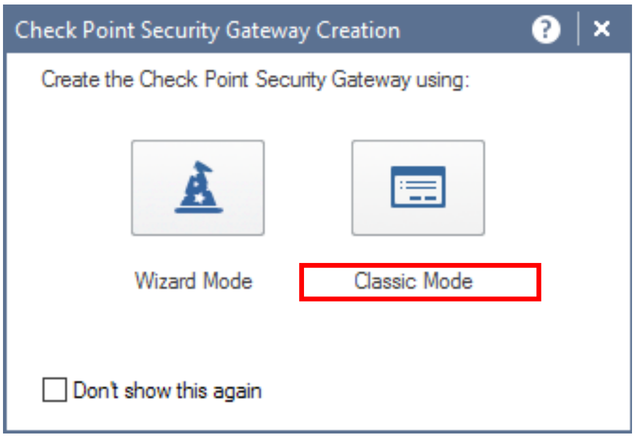
In order to have the London firewall added to our management server, we would need to do a couple of things. First, we will create the gateway, publish the changes and install the Corporate Policy, but we will not try to establish SIC. The reason behind this approach is that we will first want to make the NY-SMS-1 and NY-FW-1 aware of the new gateway and permit the management traffic to the SMS. If we try to establish SIC before we have the gateway listed in the SmartConsole, connection will fail.

Let's start by connecting to the SmartConsole and navigate to **Gateways&Servers** menu. Click to add a new **Gateway**:



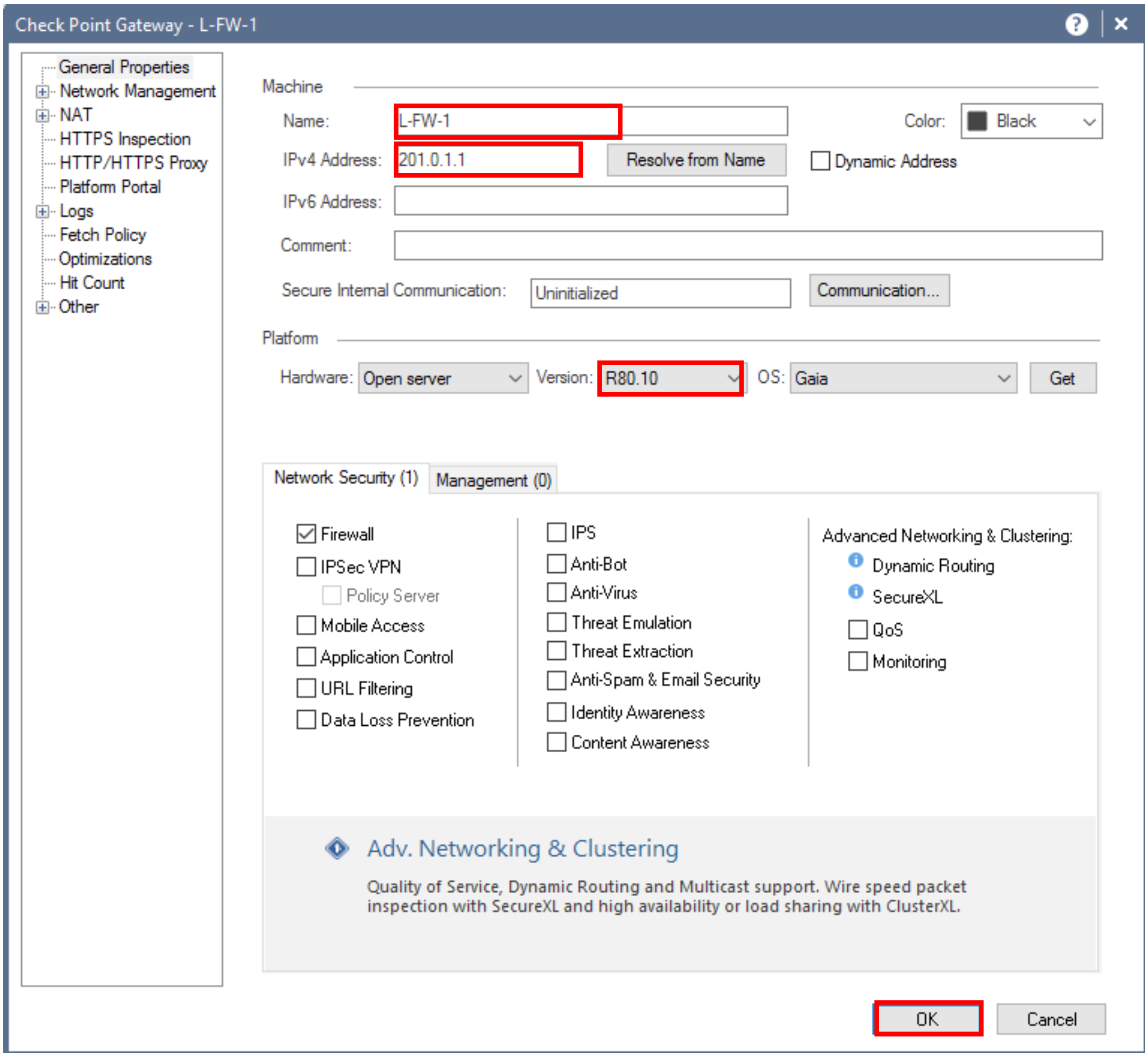
Status	Name	IP	Version	Active Blades	Hardware	CPU Us
⚠	NY-FW-1	10.0.0.1	R80.10		Open server	
⚠	NY-SMS-1	10.0.0.100	R80.10		Open server	

Select **Classic Mode:**



Create the Check Point Security Gateway using:

and fill in the following information:



Check Point Gateway - L-FW-1

Machine

Name: L-FW-1

Color: Black

IPv4 Address: 201.0.1.1

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Uninitialized

Platform

Hardware: Open server

Version: R80.10

OS: Gaia

☑ Firewall
□ IPSec VPN
□ Policy Server
□ Mobile Access
□ Application Control
□ URL Filtering
□ Data Loss Prevention

□ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
□ Identity Awareness
□ Content Awareness

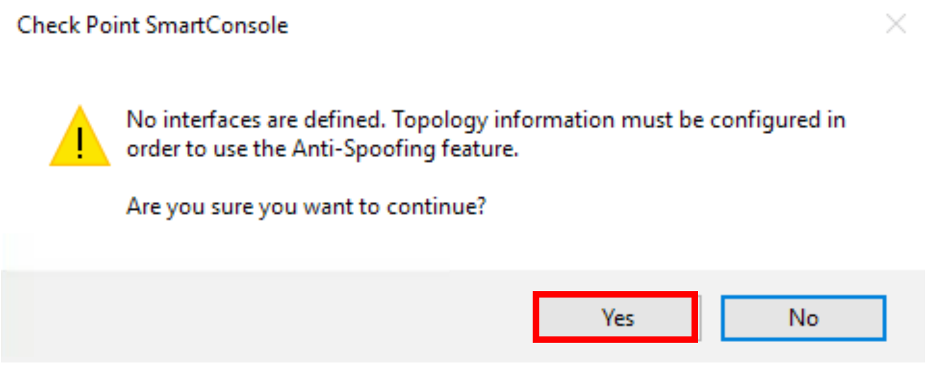
Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
□ Monitoring

Adv. Networking & Clustering

Quality of Service, Dynamic Routing and Multicast support. Wire speed packet inspection with SecureXL and high availability or load sharing with ClusterXL.

Click **OK** when done.

A warning will be displayed, but we can just ignore it at this point:



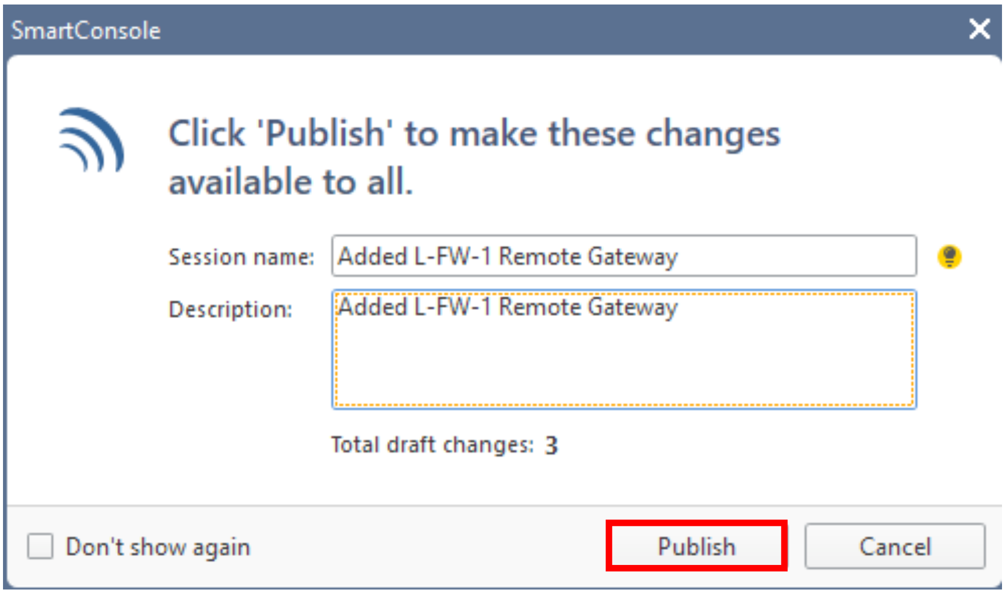
Check Point SmartConsole

No interfaces are defined. Topology information must be configured in order to use the Anti-Spoofing feature.

Are you sure you want to continue?

SmartConsole is complaining because no information about interfaces' Topology is available. This will be solved after establishing the SIC and information about the interfaces will be pulled by the SMS.

For now, just publish the changes:



SmartConsole

Click 'Publish' to make these changes available to all.

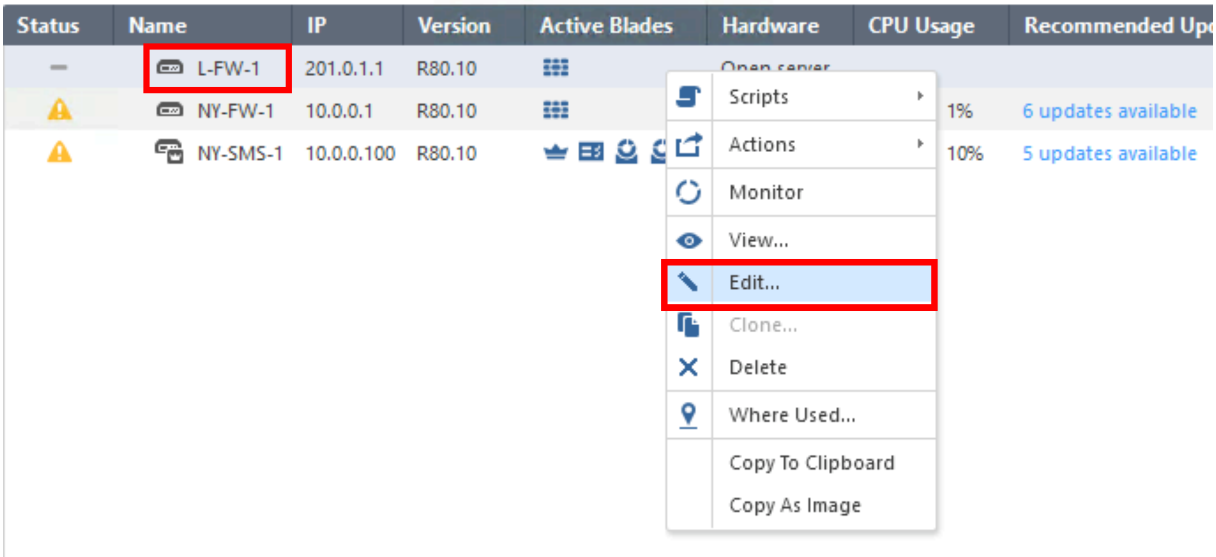
Session name: Added L-FW-1 Remote Gateway

Description: Added L-FW-1 Remote Gateway

Total draft changes: 3

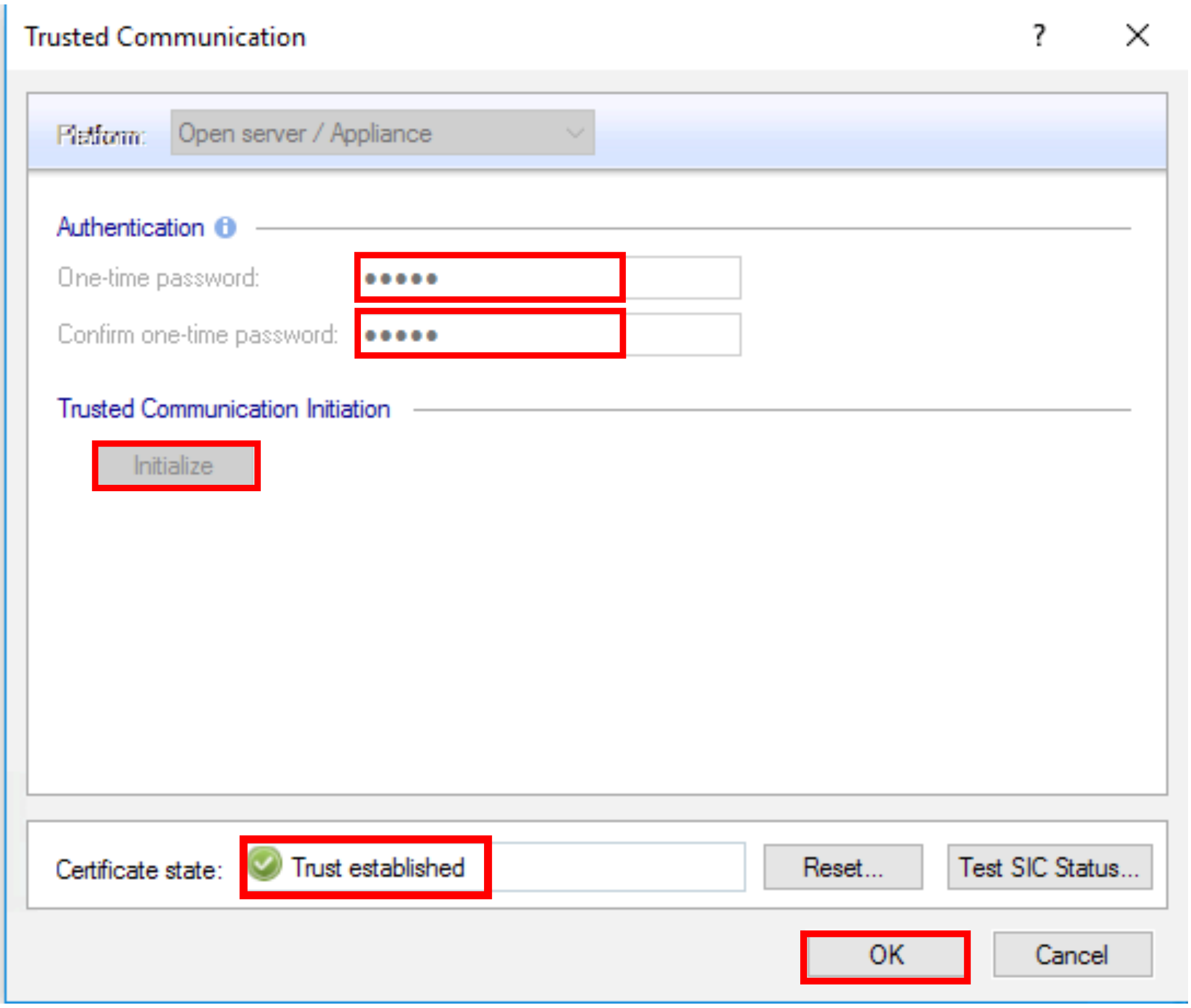
and install the HQ_Corporate_Policy on NY-FW-1.

Now, open the L-FW-1 gateway. Right-click and select **Edit**, or just double-click it:



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Up
–	L-FW-1	201.0.1.1	R80.10		Open server		
⚠	NY-FW-1	10.0.0.1	R80.10			1%	6 updates available
⚠	NY-SMS-1	10.0.0.100	R80.10			10%	5 updates available

Click on **Communication** and following window appears.



Trusted Communication

Platform: Open server / Appliance

Authentication

One-time password: •••••

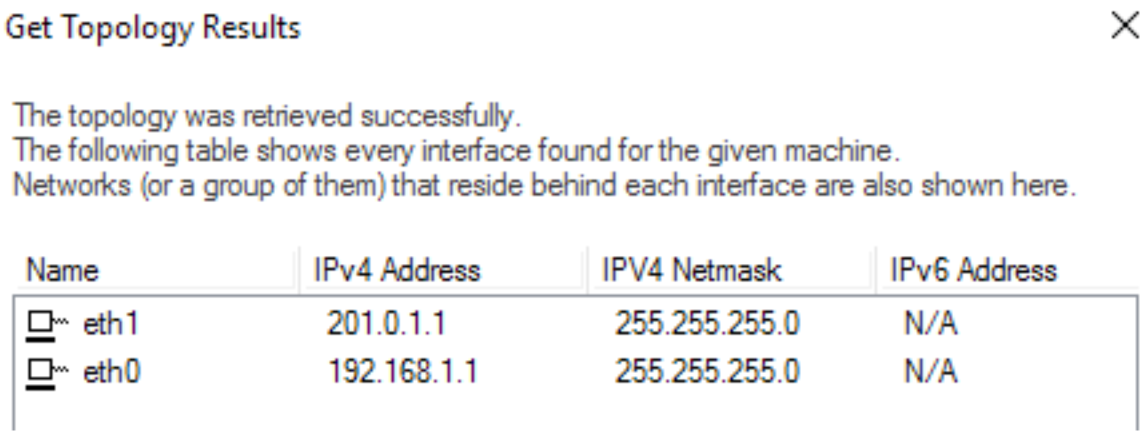
Confirm one-time password: •••••

Trusted Communication Initiation

Certificate state: Trust established

Enter the one-time password – **admin123**, confirm the password once again – **admin123** and click **Initialize**. Trust relationship is established, you can now click **OK.**

Because SIC is up now, the SMS will pull information from the gateway related to the interfaces that is has configured.

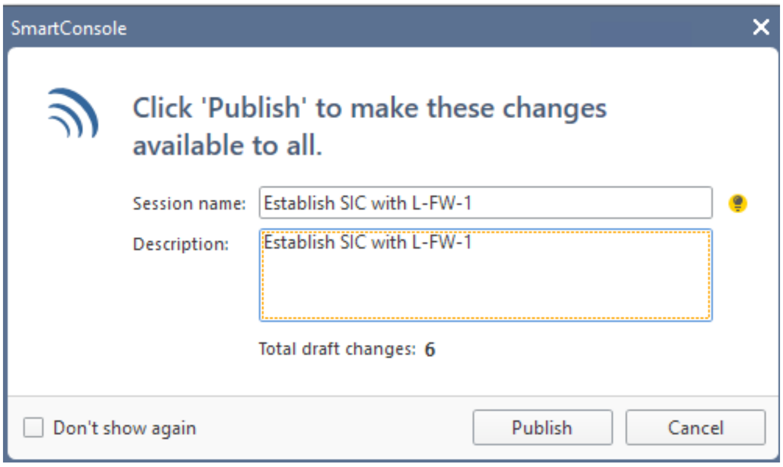


Get Topology Results

The topology was retrieved successfully.
The following table shows every interface found for the given machine.
Networks (or a group of them) that reside behind each interface are also shown here.

Name	IPv4 Address	IPV4 Netmask	IPv6 Address
eth1	201.0.1.1	255.255.255.0	N/A
eth0	192.168.1.1	255.255.255.0	N/A

Click **Close**, then **OK.** Publish the changes again and install the policy on NY-FW-1.



SmartConsole

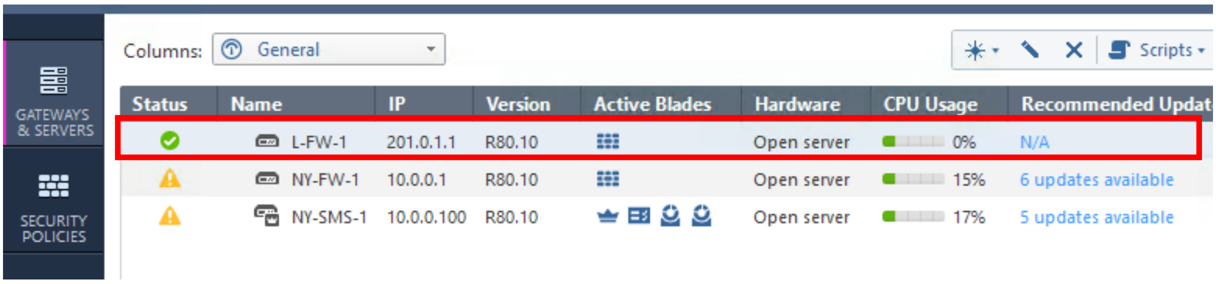
Click 'Publish' to make these changes available to all.

Session name: Establish SIC with L-FW-1

Description: Establish SIC with L-FW-1

Total draft changes: 6

Installation was done successfully, the London gateway – L-FW-1 appears now in the list, all green. The other two are presenting a warning in my case now, complaining that licensing will expire soon, just that.



Columns: General

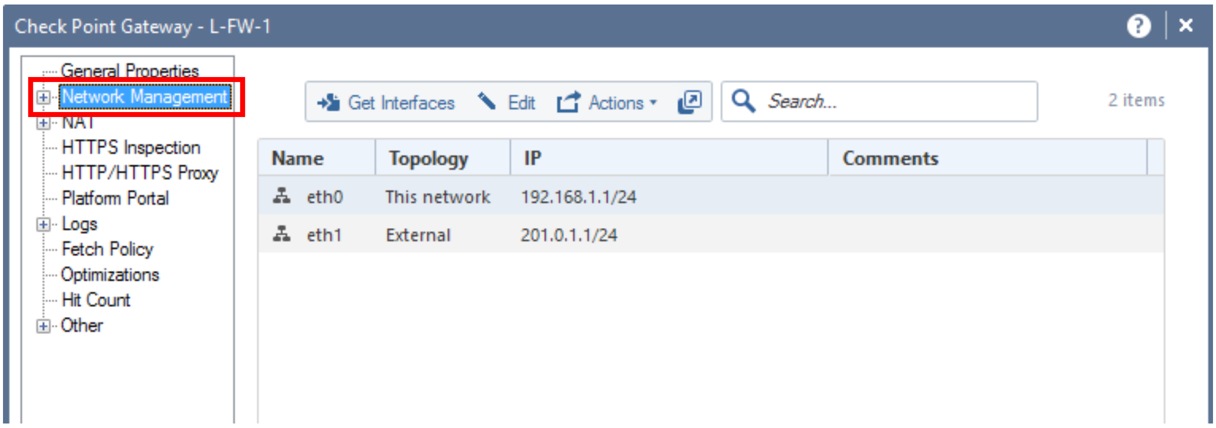
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updat
✓	L-FW-1	201.0.1.1	R80.10		Open server	0%	N/A
⚠	NY-FW-1	10.0.0.1	R80.10		Open server	15%	6 updates available
⚠	NY-SMS-1	10.0.0.100	R80.10		Open server	17%	5 updates available

23.0 Lab: Configure and Verify Topology, SZ and Anti-spoofing on London Branch Gateway

Lab Objectives

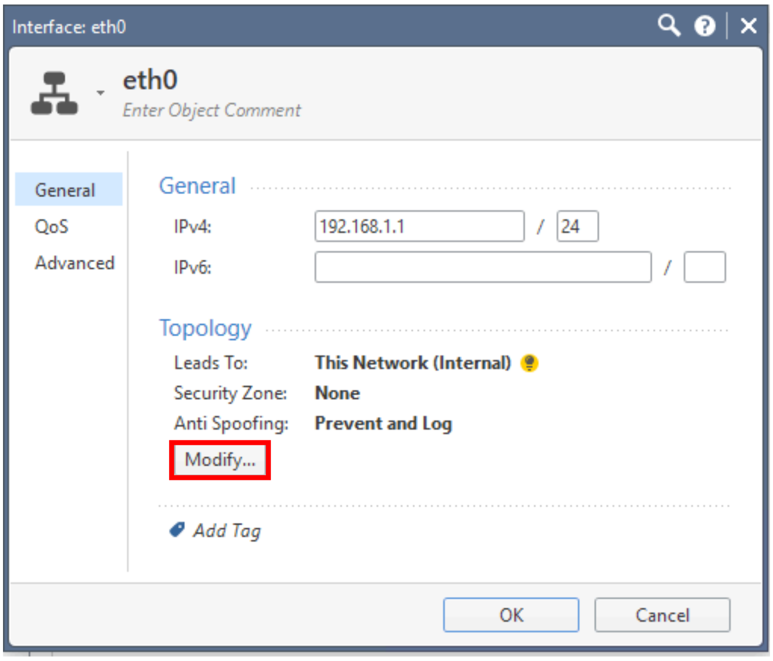
- Define topology for London FW interfaces
- Define Security Zones and Anti-Spoofing

Open L-FW-1 gateway object in order to edit it and go to **Network Management** menu on the left.



Name	Topology	IP	Comments
eth0	This network	192.168.1.1/24	
eth1	External	201.0.1.1/24	

Let's start with eth0. Select it and click on **Edit.**



IPv4: 192.168.1.1 / 24

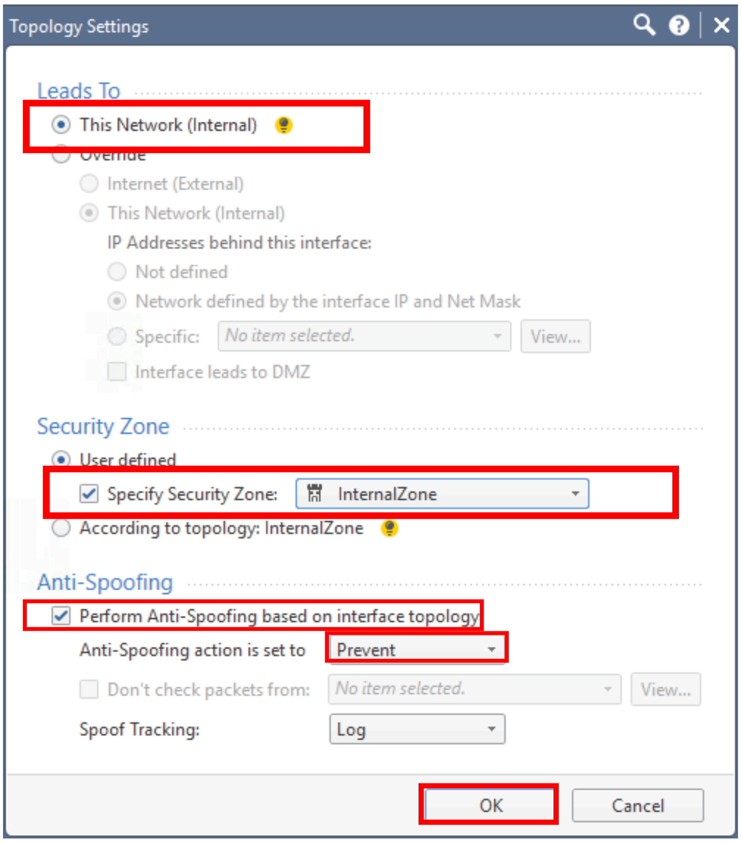
IPv6: /

Leads To: This Network (Internal)

Security Zone: None

Anti Spoofing: Prevent and Log

Click on **Modify** ...



Topology Settings

Leads To

● This Network (Internal)

○ Override

○ Internet (External)

● This Network (Internal)

IP Addresses behind this interface:

○ Not defined

● Network defined by the interface IP and Net Mask

○ Specific: No item selected. View...

□ Interface leads to DMZ

Security Zone

● User defined

☑ Specify Security Zone: InternalZone

○ According to topology: InternalZone

Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to: Prevent

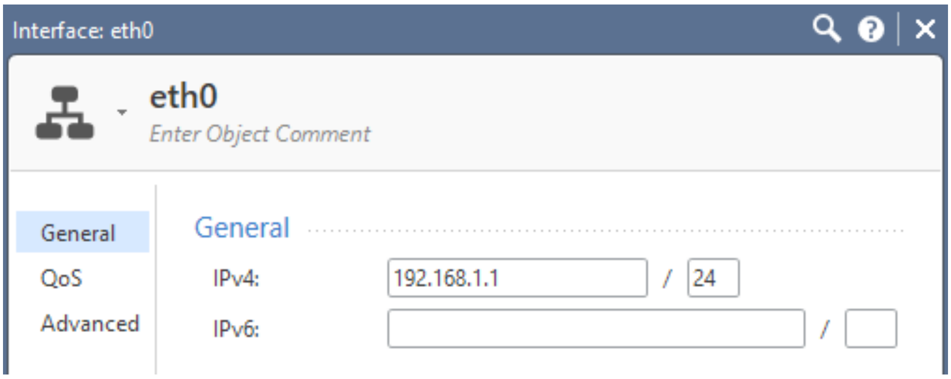
□ Don't check packets from: No item selected. View...

Spoof Tracking: Log

OK Cancel

Click **OK** when done.

In the IPv4 field I see that the IP address is 192.168.1.1. If this is the true for you too, please follow along.



Interface: eth0

eth0

Enter Object Comment

General

IPv4: 192.168.1.1 / 24

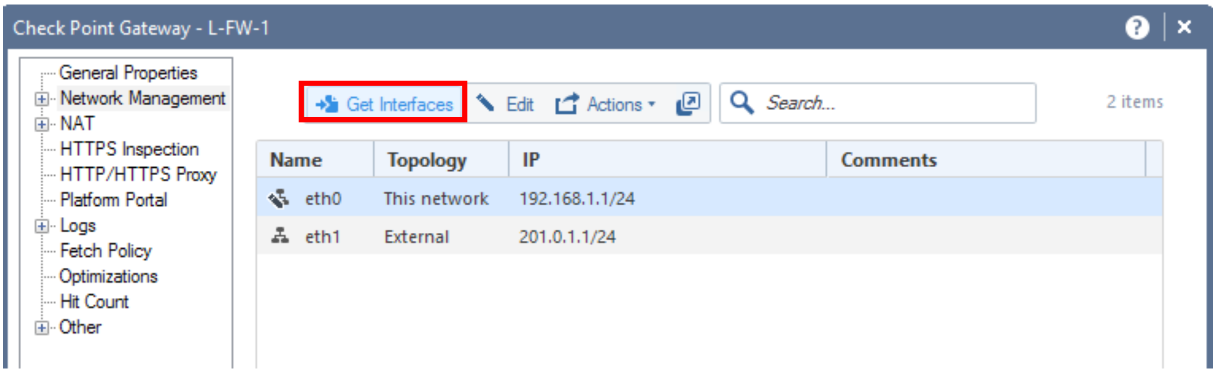
IPv6: /

We will modify the IP address of eth0 and after that we will pull the information again from SMS server side and the IP address should be updated here as well.

I am going to change the IP address through CLI.

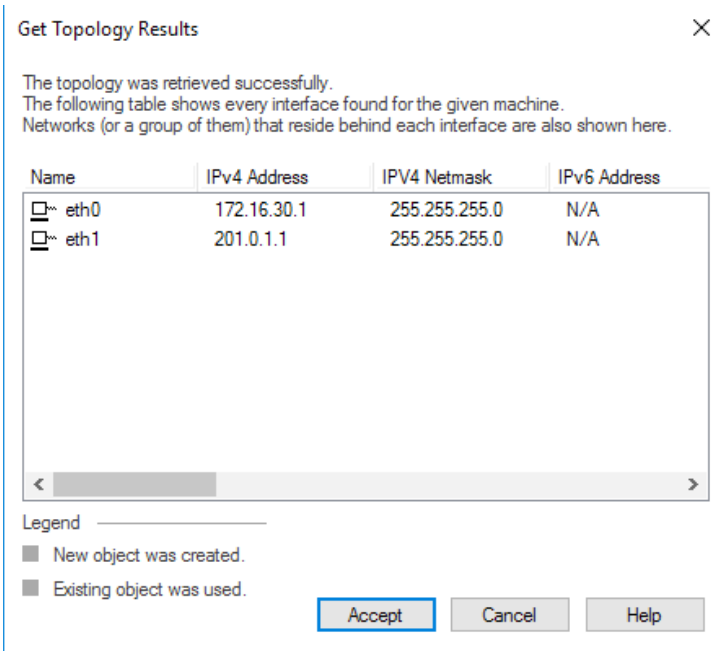
```
L-FW-1> show configuration interface
set interface eth0 state on
set interface eth0 auto-negotiation on
set interface eth0 ipv4-address 192.168.1.1 mask-length 24
set interface eth1 link-speed 1000M/full
set interface eth1 state on
set interface eth1 ipv4-address 201.0.1.1 mask-length 24
set interface eth2 state off
set interface eth3 state off
set interface lo state on
set interface lo ipv4-address 127.0.0.1 mask-length 8
L-FW-1> set interface eth0 ipv4-address 172.16.30.1 mask-length 24
L-FW-1> save config
L-FW-1> show interface eth0
state on
mac-addr 50:00:00:03:00:00
type ethernet
link-state link up
mtu 1500
auto-negotiation on
speed 1000M
ipv6-autoconfig Not configured
duplex full
monitor-mode Not configured
link-speed 1000M/full
comments
ipv4-address 172.16.30.1/24
L-FW-1>
```

Now, click on **Get Interfaces** and the Topology will be “downloaded” again.



Name	Topology	IP	Comments
eth0	This network	192.168.1.1/24	
eth1	External	201.0.1.1/24	

You may receive a warning message stating that the current topology will be overwritten. If this is the case, please confirm/accept changes.



Get Topology Results

The topology was retrieved successfully.
The following table shows every interface found for the given machine.
Networks (or a group of them) that reside behind each interface are also shown here.

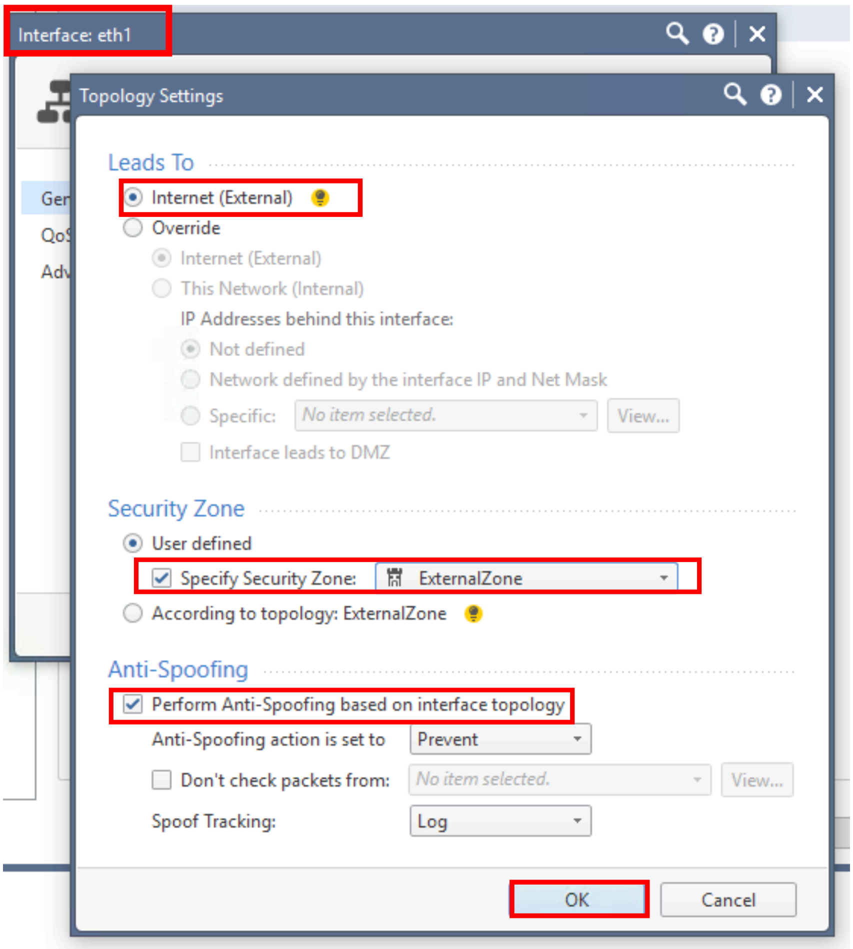
Name	IPv4 Address	IPV4 Netmask	IPv6 Address
eth0	172.16.30.1	255.255.255.0	N/A
eth1	201.0.1.1	255.255.255.0	N/A

Legend

▨ New object was created.

▨ Existing object was used.

Now the IPv4 addresses look good, click **Accept.** Don’t forget to confirm settings for external interface too, eth1:



Interface: eth1

Topology Settings

Leads To

● Internet (External)

○ Override

○ Internet (External)

○ This Network (Internal)

IP Addresses behind this interface:

○ Not defined

○ Network defined by the interface IP and Net Mask

○ Specific: No item selected.

□ Interface leads to DMZ

Security Zone

● User defined

☑ Specify Security Zone: ExternalZone

○ According to topology: ExternalZone

Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to: Prevent

□ Don't check packets from: No item selected.

Spoof Tracking: Log

Publish Changes and Install the Policy!

24.0 Lab: Define a New Policy Package for Branch Gateways

Lab Objectives

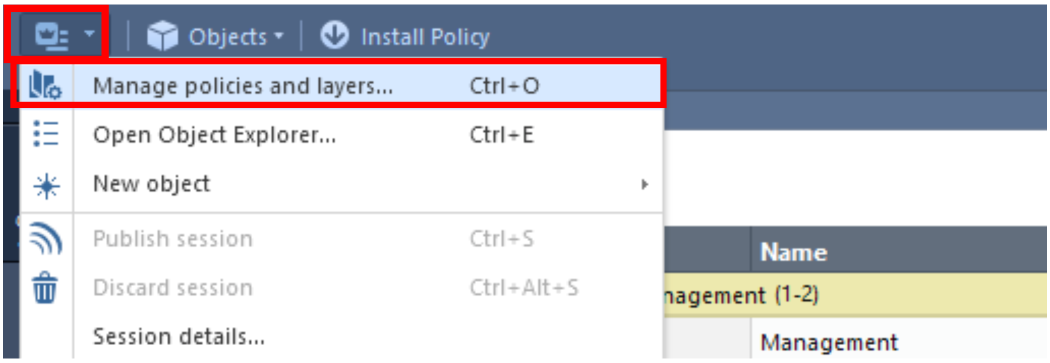
- Create a new policy package that will be used for London Branch

In this short lab, we will define a new Policy Package that will be used for London Branch gateway. Can you remember what a policy package is ?

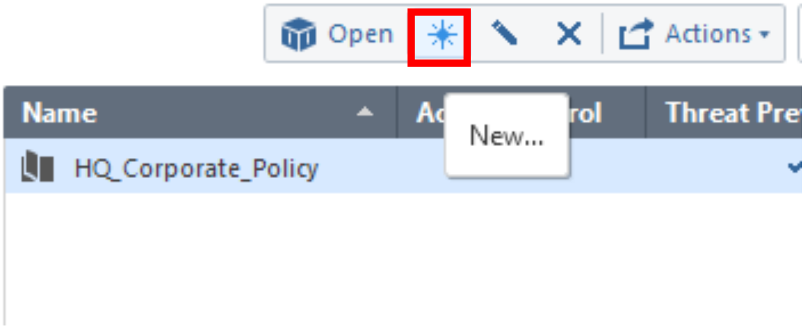
You can think of the policy package as a container that puts together all the security policies that will be installed on the respective gateway. With that said, the policy package is comprised of Access Control Policy, Threat Prevention Policy, QoS and Desktop Policies.

In this lab we define the **Branch_Policy** so that in the next lab we define the Access Control Policy that will be installed on the London Branch gateway.

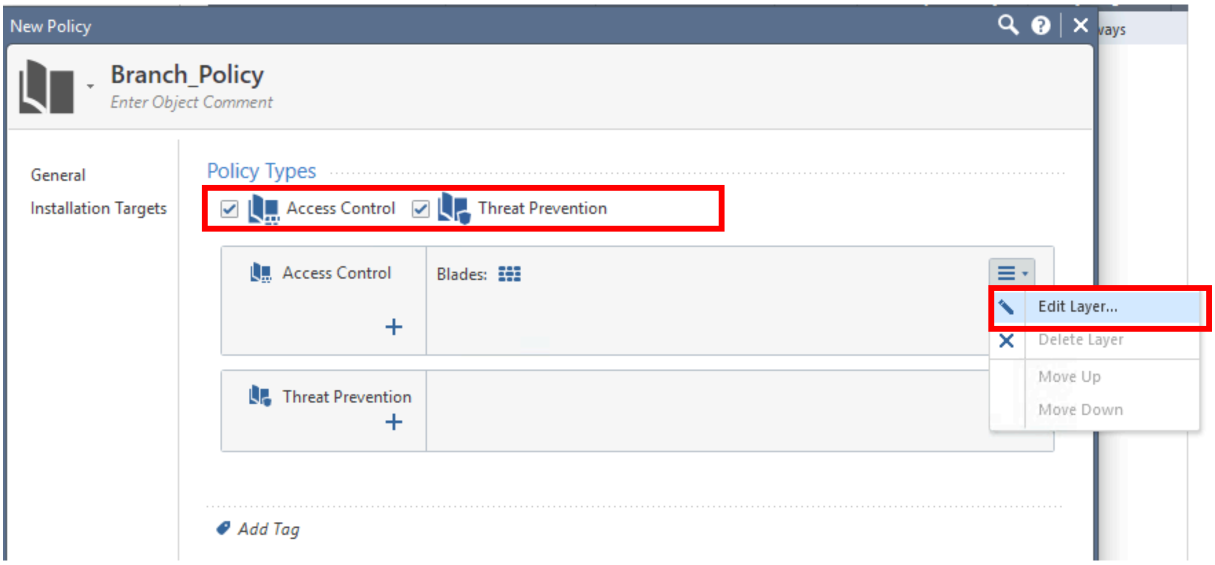
In the top left corner, click on **Menu** and then enter the **Manage policies and layers** menu.



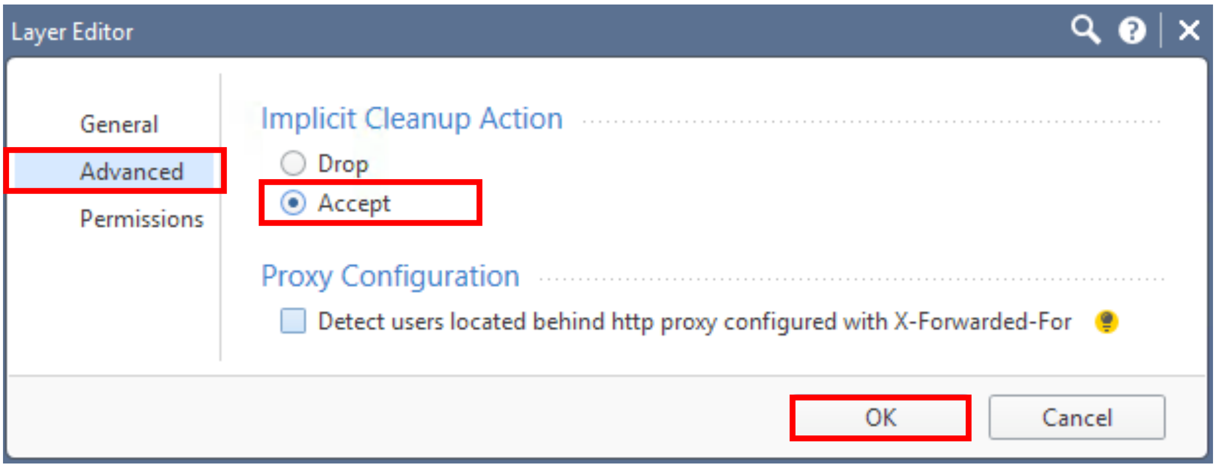
Now, click on **New** and let's define the necessary details.



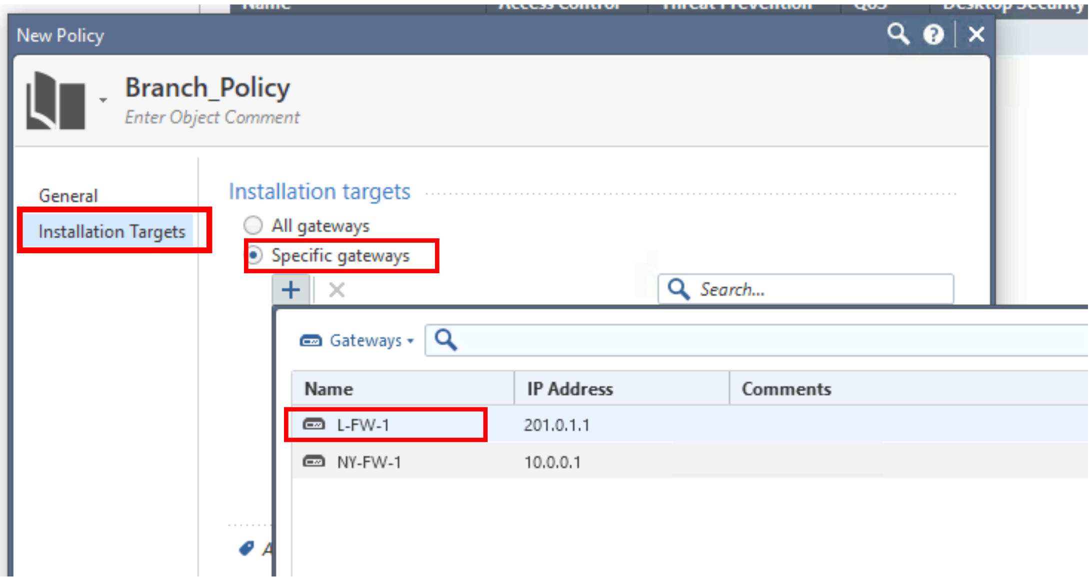
This policy package will include, at a later time also the Threat Prevention policy, so select it here.



Let’s edit the Network layer, that currently contains only one blade – Firewall.

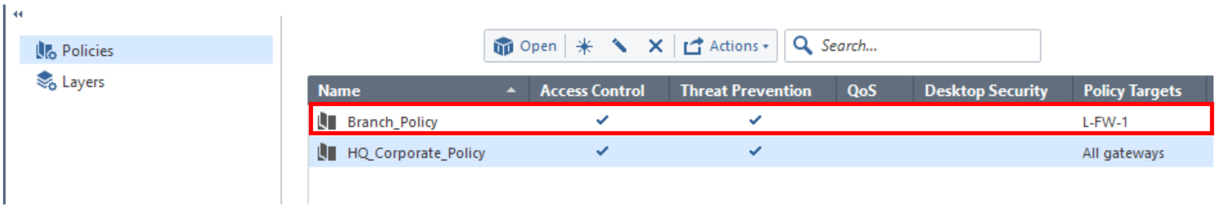


Next, go to **Installation Targets,** in order to define where this Policy Package will be installed, select L-FW-1:



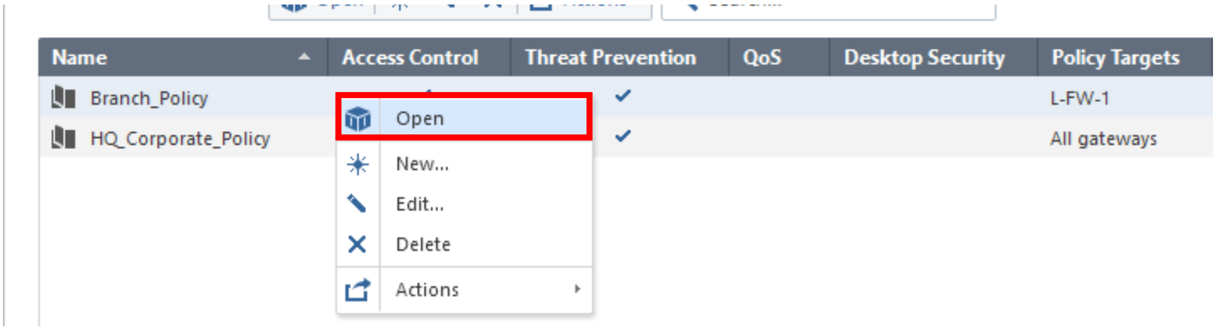
Name	IP Address	Comments
L-FW-1	201.0.1.1	
NY-FW-1	10.0.0.1	

Click **OK** when done. The new policy package is added to the list:



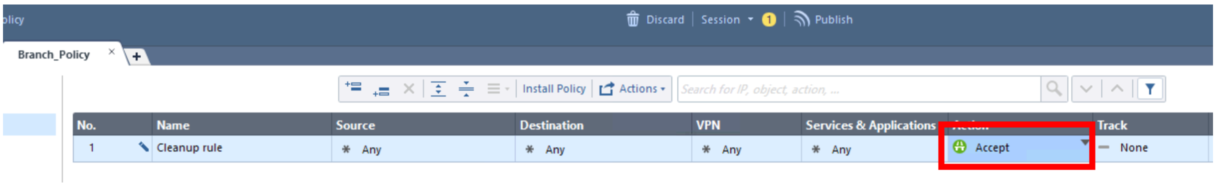
Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets
Branch_Policy	✓	✓			L-FW-1
HQ_Corporate_Policy	✓	✓			All gateways

Let’s do a small change in the Branch_Policy befor we wrap up this lab.



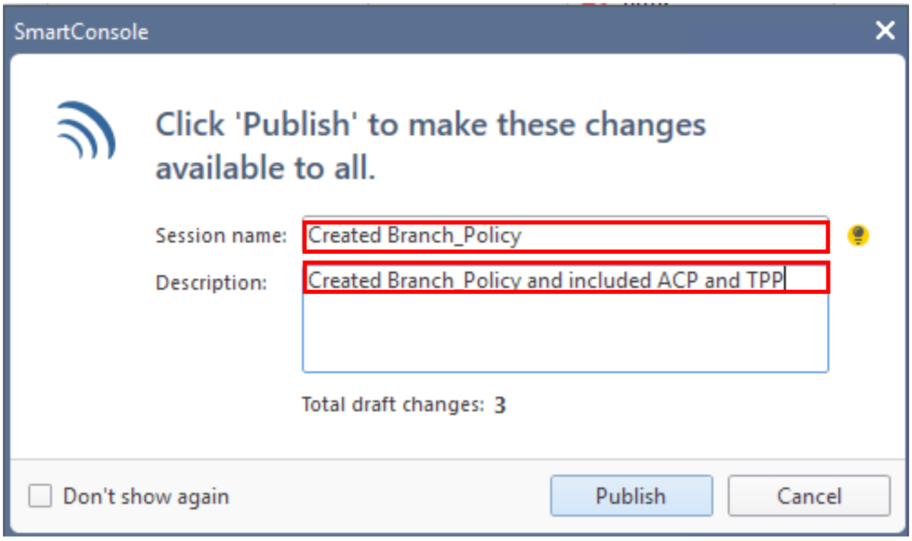
Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets
Branch_Policy		✓			L-FW-1
HQ_Corporate_Policy		✓			All gateways

Right-click on Branch_Policy and select **Open.** Please note that now the tab you are working on is named – **Branch_**Policy, as expected. Modify the default action to **Accept** and,



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Cleanup rule	Any	Any	Any	Any	Accept	None

as always, don’t forget to publish the changes and Install Policy:



Click 'Publish' to make these changes available to all.

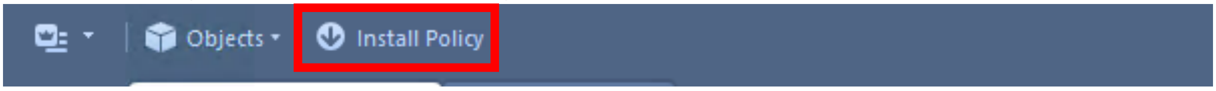
Session name: Created Branch_Policy

Description: Created Branch_Policy and included ACP and TPP

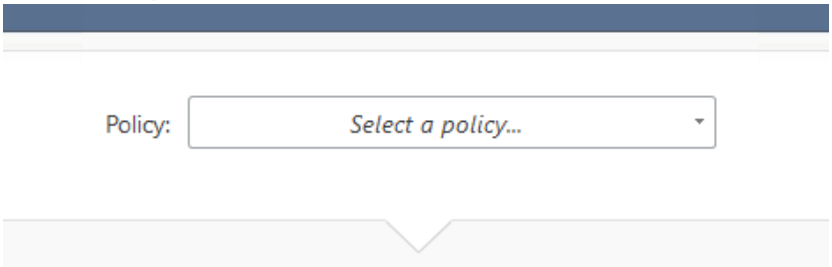
Total draft changes: 3

□ Don't show again

Now, when you click **Install Policy**,

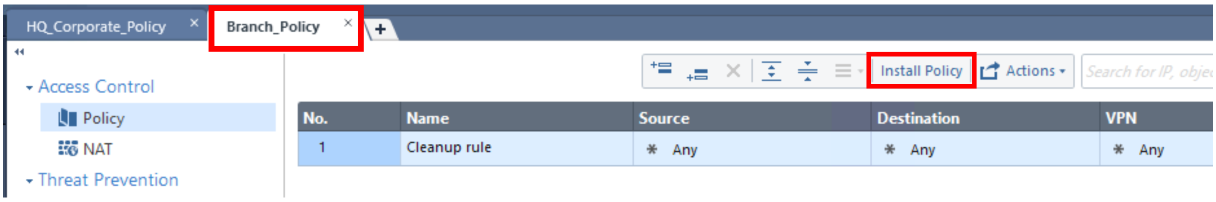


you are asked to select which policy you are going to install and this makes sense as we have two policies available.



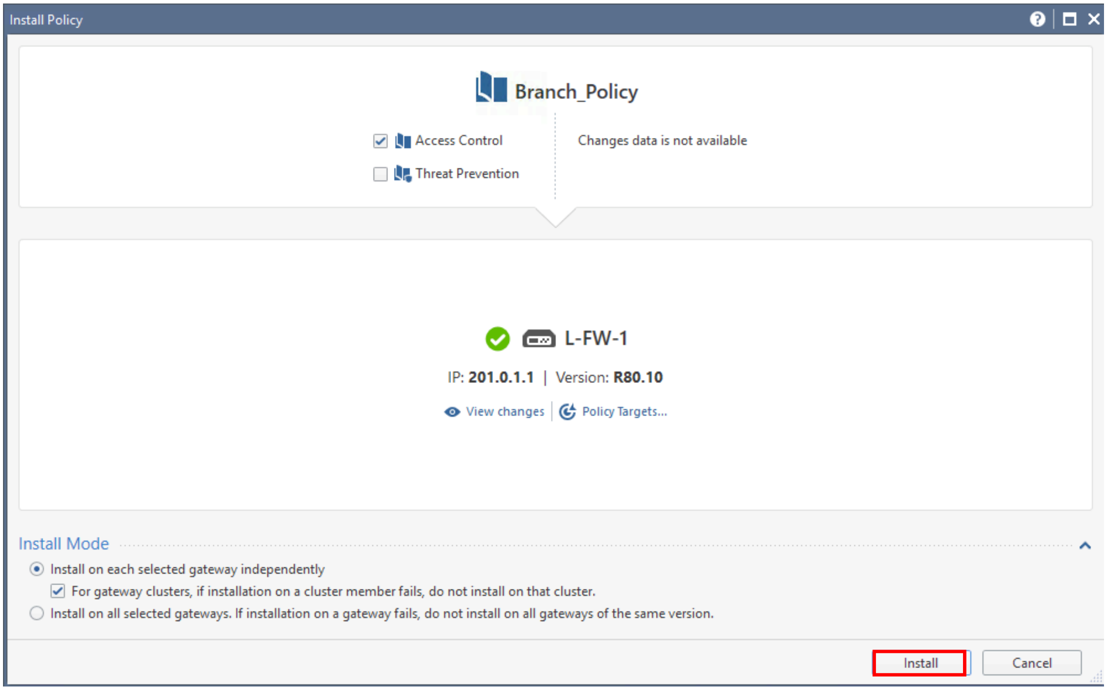
Policy: *Select a policy...*

This happens if you click the general **Install Policy** button. If you are inside a policy, for example the **Branch_Policy** and you click the **Install Policy** button, SmartConsole will know what policy you want to install and will the trigger the policy installation window:



No.	Name	Source	Destination	VPN
1	Cleanup rule	✱ Any	✱ Any	✱ Any

Click on **Install** and the **Branch_Policy** will be installed on the London Branch Gateway.



Install Policy

Branch_Policy

☑ Access Control

□ Threat Prevention

Changes data is not available

L-FW-1

IP: **201.0.1.1** | Version: **R80.10**

Install Mode

● Install on each selected gateway independently

☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

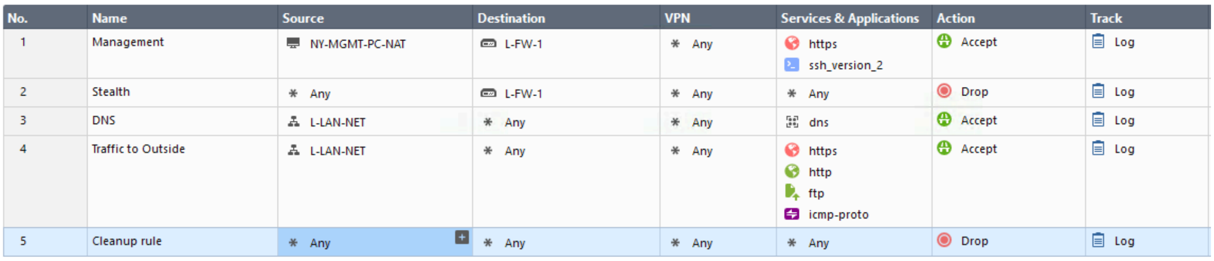
25.0 Lab: Configure a Basic Access Control Policy for London Branch Gateway

Lab Objectives

- Configure a Basic Access Control Policy for the London remote gateway in a similar manner like you did for the NY HQ Gateway – NY-FW-1

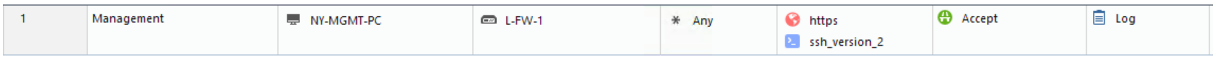
Following the same approach as for NY-FW-1, you will now build a basic access control policy for London Gateway.

When this lab is completed, the Access Control Policy Rule Base should look like this :



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Management	NY-MGMT-PC-NAT	L-FW-1	* Any	https ssh_version_2	Accept	Log
2	Stealth	* Any	L-FW-1	* Any	* Any	Drop	Log
3	DNS	L-LAN-NET	* Any	* Any	dns	Accept	Log
4	Traffic to Outside	L-LAN-NET	* Any	* Any	https http ftp icmp-proto	Accept	Log
5	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log

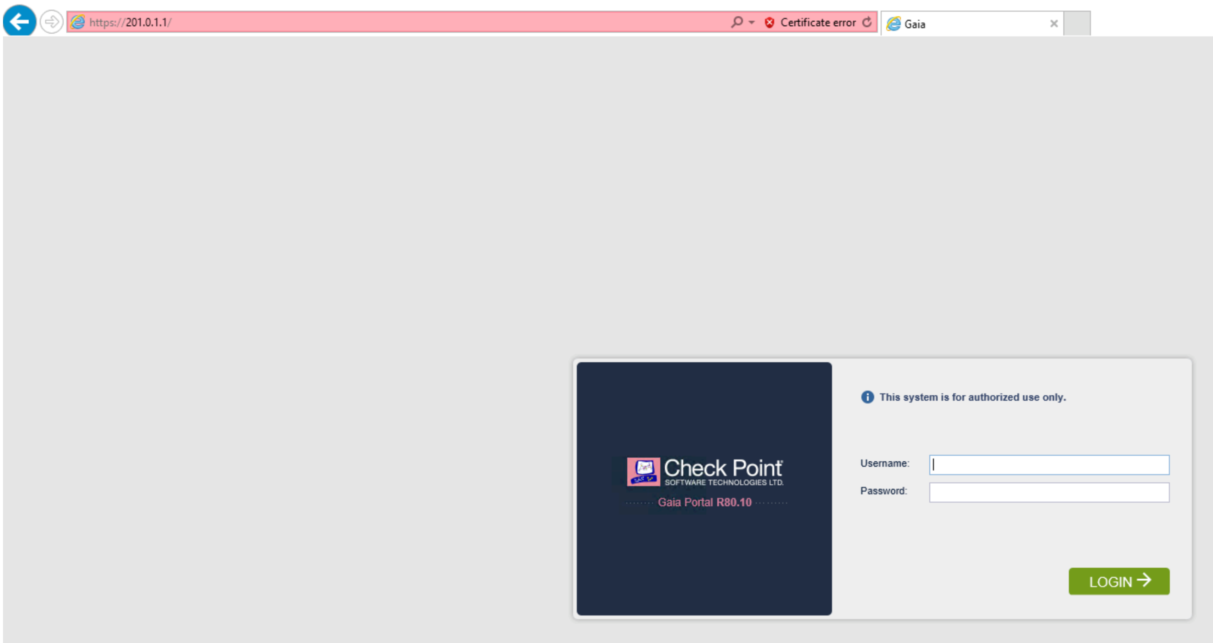
We start by adding the Management rule, above the default Cleanup rule :



1	Management	NY-MGMT-PC	L-FW-1	Any	https ssh_version_2	Accept	Log

Let’s make a test, first publish the changes and install the Branch Policy.

Now, from the NY-MGMT-PC, initiate a connection to https://201.0.1.1 which represents L-FW-1:

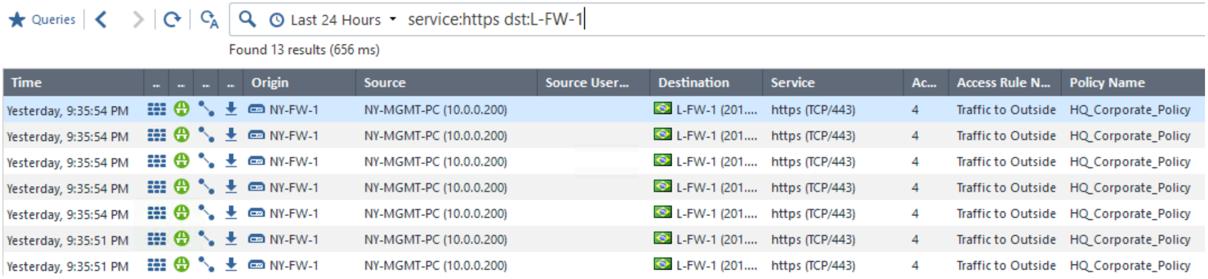


This system is for authorized use only.

Username:

Password:

Connection is successful, let’s investigate the logs. In SmartConsole, go to **Logs&Monitor** and filter the logs with the following: **service:https dst:L-FW-1**



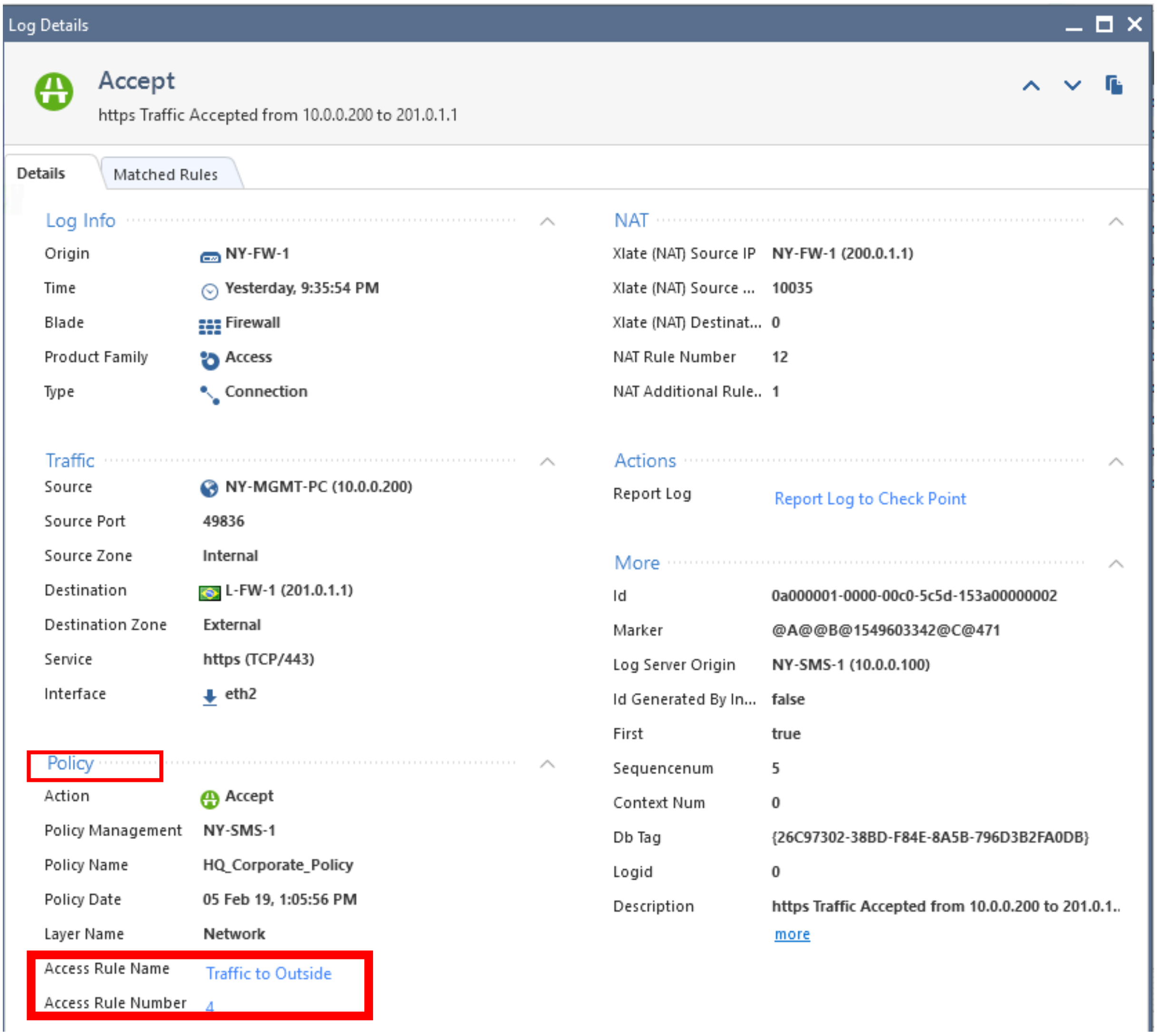
service:https dst:L-FW-1

Found 13 results (656 ms)

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy Name
Yesterday, 9:35:54 PM					NY-FW-1	NY-MGMT-PC (10.0.0.200)		L-FW-1 (201....	https (TCP/443)	4	Traffic to Outside	HQ_Corporate_Policy
Yesterday, 9:35:54 PM					NY-FW-1	NY-MGMT-PC (10.0.0.200)		L-FW-1 (201....	https (TCP/443)	4	Traffic to Outside	HQ_Corporate_Policy
Yesterday, 9:35:54 PM					NY-FW-1	NY-MGMT-PC (10.0.0.200)		L-FW-1 (201....	https (TCP/443)	4	Traffic to Outside	HQ_Corporate_Policy
Yesterday, 9:35:54 PM					NY-FW-1	NY-MGMT-PC (10.0.0.200)		L-FW-1 (201....	https (TCP/443)	4	Traffic to Outside	HQ_Corporate_Policy
Yesterday, 9:35:54 PM					NY-FW-1	NY-MGMT-PC (10.0.0.200)		L-FW-1 (201....	https (TCP/443)	4	Traffic to Outside	HQ_Corporate_Policy
Yesterday, 9:35:51 PM					NY-FW-1	NY-MGMT-PC (10.0.0.200)		L-FW-1 (201....	https (TCP/443)	4	Traffic to Outside	HQ_Corporate_Policy
Yesterday, 9:35:51 PM					NY-FW-1	NY-MGMT-PC (10.0.0.200)		L-FW-1 (201....	https (TCP/443)	4	Traffic to Outside	HQ_Corporate_Policy

Open the top log and let’s take a look at what information is presented.

Look closer at what is presented in the Policy section. Traffic is matched, in the HQ_Corporate_Policy by the **Outgoing** rule, rule number 4. Yes the connection is working, but since this is management traffic, it should reside in the management specific rule – first rule.



Accept

https Traffic Accepted from 10.0.0.200 to 201.0.1.1

Log Info

Origin	NY-FW-1
Time	Yesterday, 9:35:54 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	NY-MGMT-PC (10.0.0.200)
Source Port	49836
Source Zone	Internal
Destination	L-FW-1 (201.0.1.1)
Destination Zone	External
Service	https (TCP/443)
Interface	eth2

Policy

Action	Accept
Policy Management	NY-SMS-1
Policy Name	HQ_Corporate_Policy
Policy Date	05 Feb 19, 1:05:56 PM
Layer Name	Network
Access Rule Name	Traffic to Outside
Access Rule Number	4

NAT

Xlate (NAT) Source IP	NY-FW-1 (200.0.1.1)
Xlate (NAT) Source ...	10035
Xlate (NAT) Destinat...	0
NAT Rule Number	12
NAT Additional Rule..	1

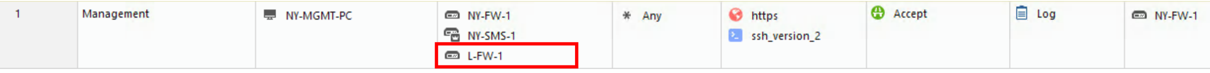
Actions

Report Log	Report Log to Check Point

More

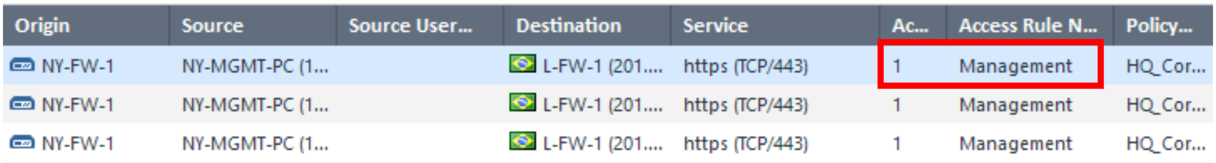
Id	0a000001-0000-00c0-5c5d-153a00000002
Marker	@A@@B@1549603342@C@471
Log Server Origin	NY-SMS-1 (10.0.0.100)
Id Generated By In...	false
First	true
Sequencenum	5
Context Num	0
Db Tag	{26C97302-38BD-F84E-8A5B-796D3B2FA0DB}
Logid	0
Description	https Traffic Accepted from 10.0.0.200 to 201.0.1.. more

Let's modify the Management rule on HQ_Corporate_Policy and add L-FW-1 to the Destination column.



1	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1 L-FW-1	Any	https ssh_version_2	Accept	Log	NY-FW-1

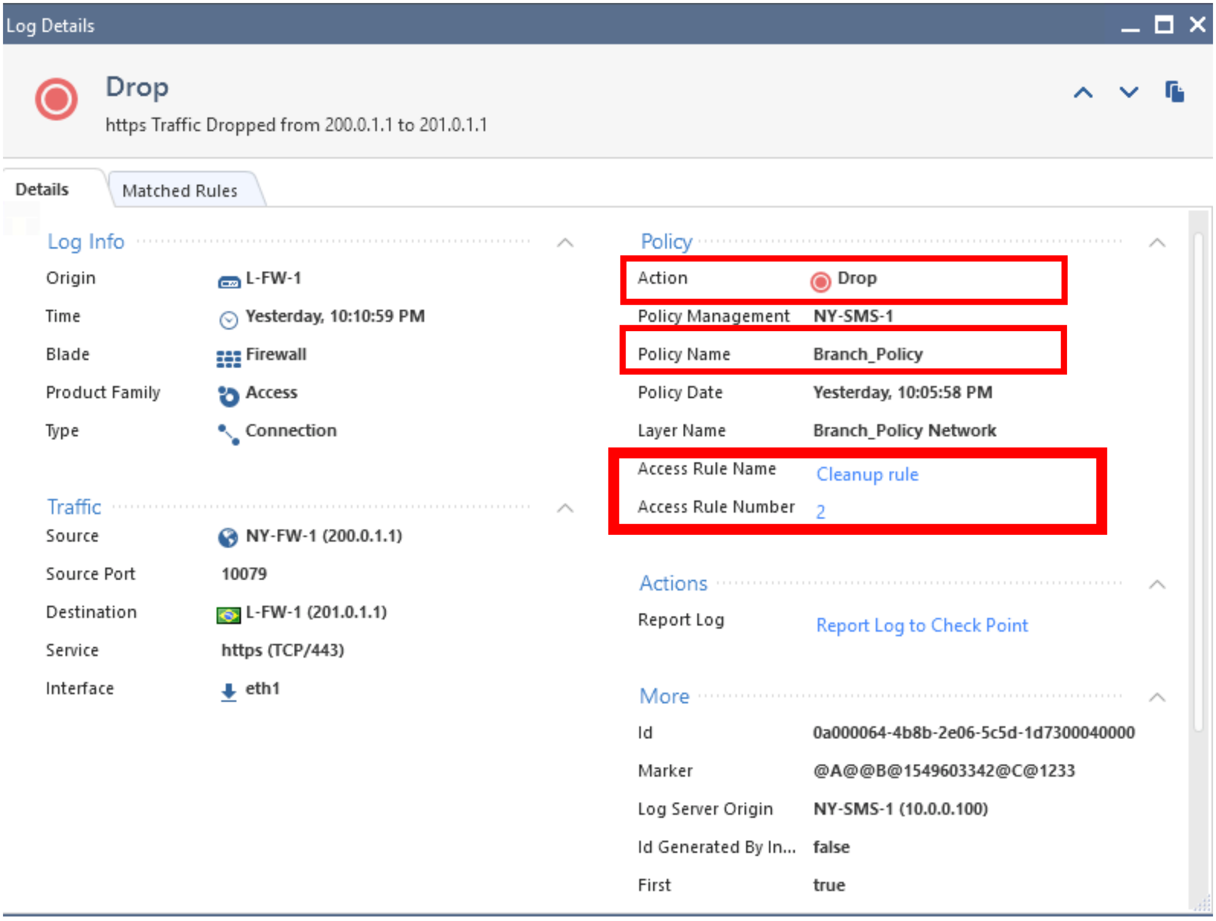
Publish changes, install HQ policy and let's test again now. Now, the traffic is being matched by rule 1 – Management, in the HQ_Corporate_Policy Rule Base.



Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...
NY-FW-1	NY-MGMT-PC (1...		L-FW-1 (201....	https (TCP/443)	1	Management	HQ_Cor...
NY-FW-1	NY-MGMT-PC (1...		L-FW-1 (201....	https (TCP/443)	1	Management	HQ_Cor...
NY-FW-1	NY-MGMT-PC (1...		L-FW-1 (201....	https (TCP/443)	1	Management	HQ_Cor...

But is it traffic really reaching L-FW-1 ?

Filter the logs with the following: **service:https src:200.0.1.1 dst:201.0.1.1 :**



Log Details

Drop

https Traffic Dropped from 200.0.1.1 to 201.0.1.1

Details | Matched Rules

Log Info

Origin	L-FW-1
Time	Yesterday, 10:10:59 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	NY-FW-1 (200.0.1.1)
Source Port	10079
Destination	L-FW-1 (201.0.1.1)
Service	https (TCP/443)
Interface	eth1

Policy

Action	Drop
Policy Management	NY-SMS-1
Policy Name	Branch_Policy
Policy Date	Yesterday, 10:05:58 PM
Layer Name	Branch_Policy Network
Access Rule Name	Cleanup rule
Access Rule Number	2

Actions

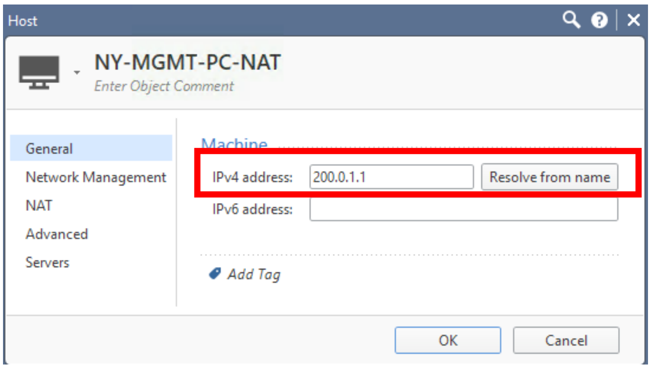
Report Log	Report Log to Check Point

More

Id	0a000064-4b8b-2e06-5c5d-1d7300040000
Marker	@A@@B@1549603342@C@1233
Log Server Origin	NY-SMS-1 (10.0.0.100)
Id Generated By In...	false
First	true

Traffic is being dropped by the Branch Policy, as it is being matched by the Cleanup Rule. The management rule permits traffic to L-FW-1, but if it is coming from NY-MGMT-PC – 10.0.0.100 IP address. Because traffic is being source NAT-ed when leaving the NY-FW-1 gateway, the IP address changes to 200.0.1.1 – Hide NAT – the external IP address of NY-FW-1.

I will create a new object – NY-MGMT-PC-NAT and assign the IP address of 200.0.1.1. Then we will modify the source object in the Management rule on Branch Policy:



Host

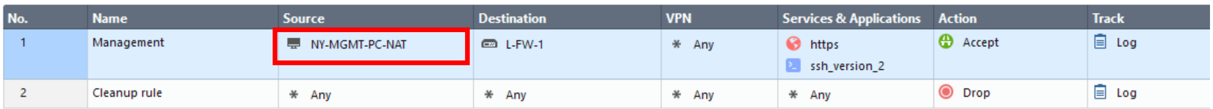
NY-MGMT-PC-NAT

Enter Object Comment

Machine

IPv4 address: 200.0.1.1

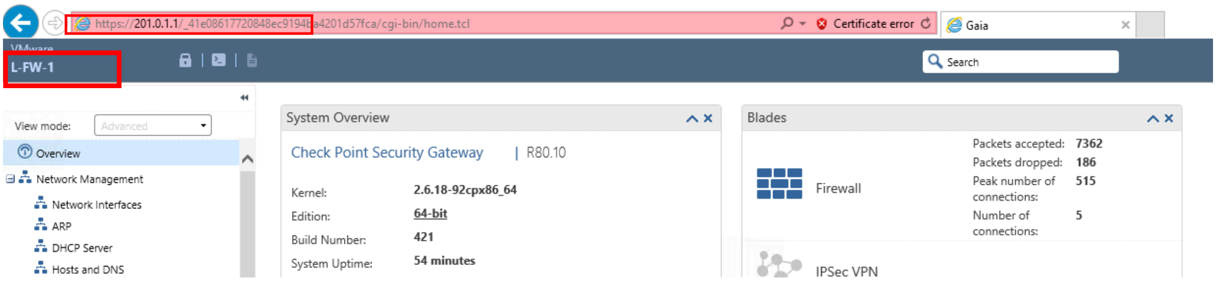
IPv6 address:



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Management	NY-MGMT-PC-NAT	L-FW-1	Any	https ssh_version_2	Accept	Log
2	Cleanup rule	Any	Any	Any	Any	Drop	Log

Now, let's try again. Initiate a https connection to L-FW-1 : https://201.0.1.1

This time it works :



https://201.0.1.1/_41e08617720848ec9194ba4201d57fca/cgi-bin/home.tcl

Certificate error

Gaia

L-FW-1

View mode: Advanced

Overview

Network Management

Network Interfaces

ARP

DHCP Server

Hosts and DNS

System Overview

Check Point Security Gateway | R80.10

Kernel:	2.6.18-92cpx86_64
Edition:	64-bit
Build Number:	421
System Uptime:	54 minutes

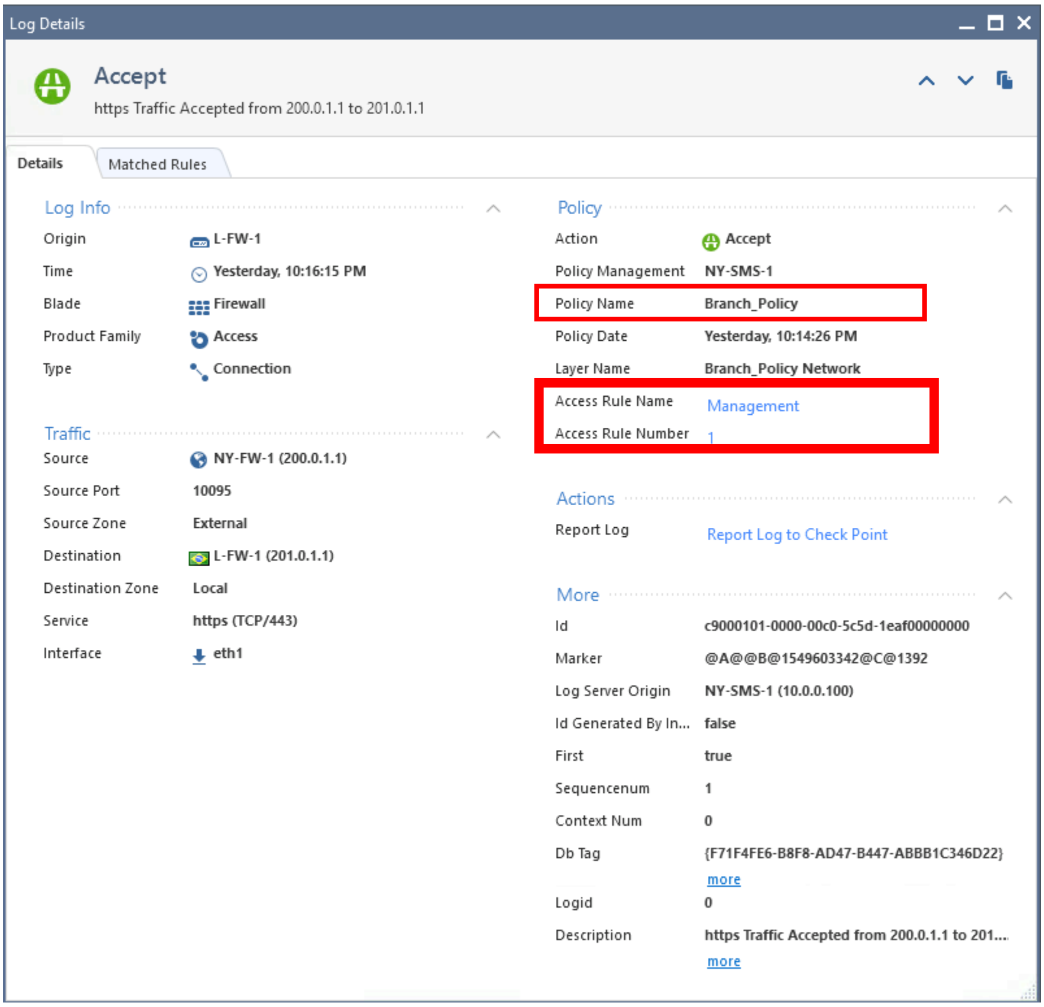
Blades

Firewall

Packets accepted:	7362
Packets dropped:	186
Peak number of connections:	515
Number of connections:	5

IPSec VPN

And the logs confirm this as well :



Log Details

Accept

https Traffic Accepted from 200.0.1.1 to 201.0.1.1

Log Info

Origin	L-FW-1
Time	Yesterday, 10:16:15 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	NY-FW-1 (200.0.1.1)
Source Port	10095
Source Zone	External
Destination	L-FW-1 (201.0.1.1)
Destination Zone	Local
Service	https (TCP/443)
Interface	eth1

Policy

Action	Accept
Policy Management	NY-SMS-1
Policy Name	Branch_Policy
Policy Date	Yesterday, 10:14:26 PM
Layer Name	Branch_Policy Network
Access Rule Name	Management
Access Rule Number	1

Actions

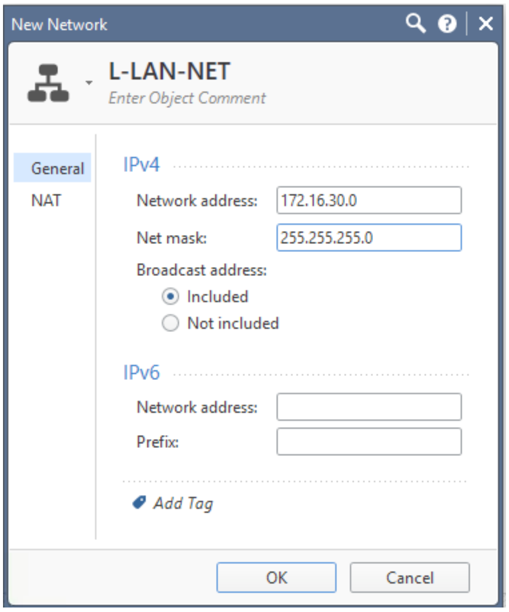
Report Log	Report Log to Check Point

More

Id	c9000101-0000-00c0-5c5d-1eaf00000000
Marker	@A@@B@1549603342@C@1392
Log Server Origin	NY-SMS-1 (10.0.0.100)
Id Generated By In...	false
First	true
Sequencenum	1
Context Num	0
Db Tag	{F71F4FE6-B8F8-AD47-B447-ABBB1C346D22} more
Logid	0
Description	https Traffic Accepted from 200.0.1.1 to 201... more

Let's continue now with the rest of the rules for London Gateway.

The second rule is the Stealth Rule. For the 3rd and 4th rule I need to create a new object – the London internal LAN object:



New Network

L-LAN-NET

Enter Object Comment

IPv4

Network address: 172.16.30.0

Net mask: 255.255.255.0

Broadcast address:

● Included

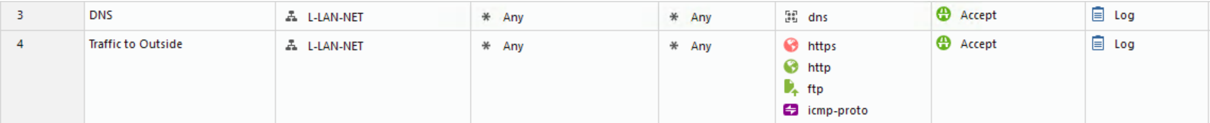
○ Not included

IPv6

Network address:

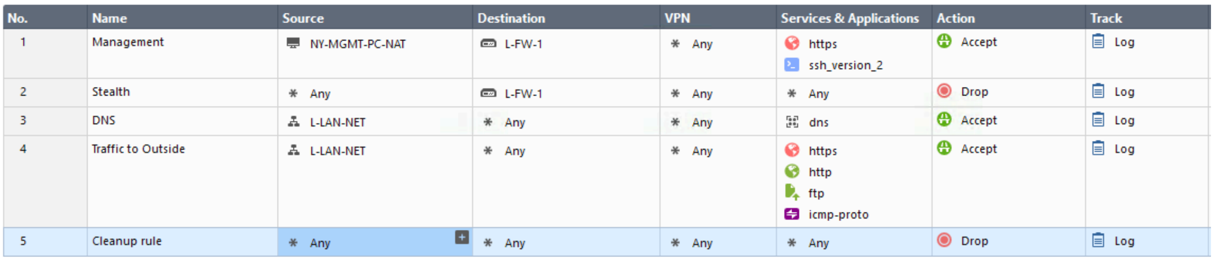
Prefix:

Add the DNS and Outgoing traffic rule as below:



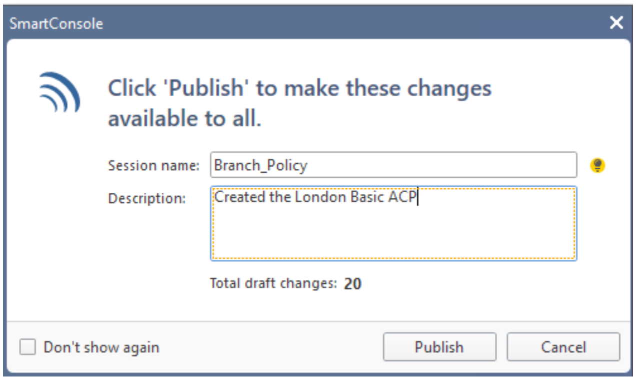
3	DNS	L-LAN-NET	Any	Any	dns	Accept	Log
4	Traffic to Outside	L-LAN-NET	Any	Any	https http ftp icmp-proto	Accept	Log

The new Access Control Policy rule base should look like this:



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Management	NY-MGMT-PC-NAT	L-FW-1	Any	https ssh_version_2	Accept	Log
2	Stealth	Any	L-FW-1	Any	Any	Drop	Log
3	DNS	L-LAN-NET	Any	Any	dns	Accept	Log
4	Traffic to Outside	L-LAN-NET	Any	Any	https http ftp icmp-proto	Accept	Log
5	Cleanup rule	Any	Any	Any	Any	Drop	Log

You may have got used to it already now, publish the changes and install the new policy to London GW.



SmartConsole

Click 'Publish' to make these changes available to all.

Session name: Branch_Policy

Description: Created the London Basic ACP

Total draft changes: 20

□ Don't show again

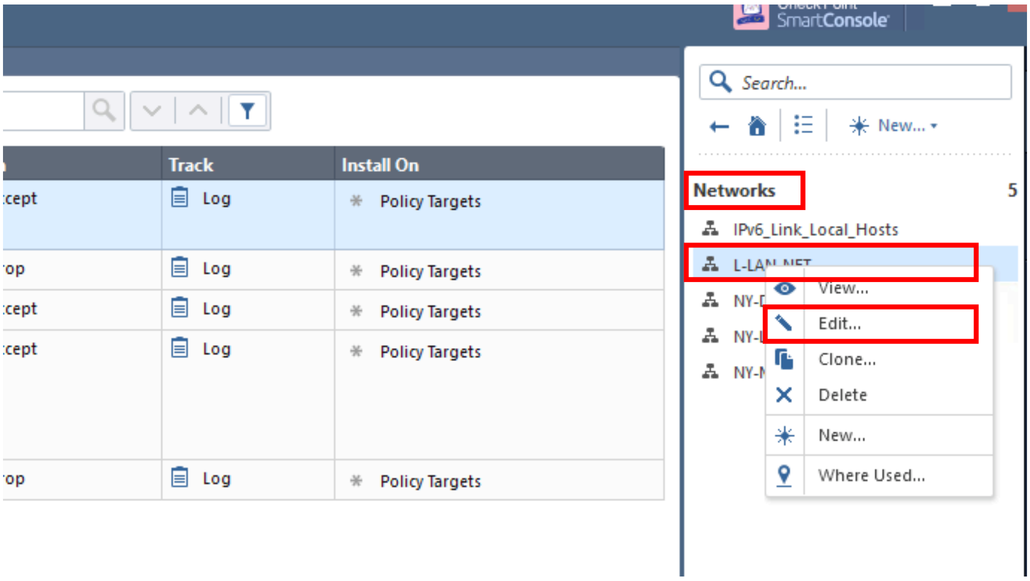
26.0 Lab: Configure Hide NAT and provide Branch Users Internet Connectivity

Lab Objectives

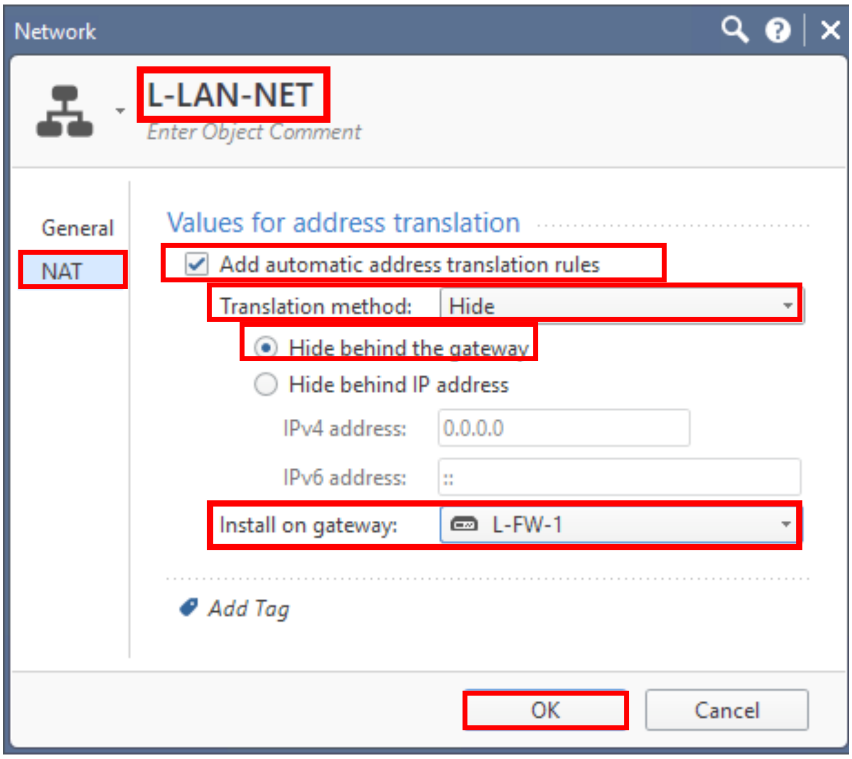
- Configure Hide NAT in order to connect London internal users to Internet

This lab will be very short. We will configure Hide NAT for the London Branch in order to provide internet connectivity to London LAN users.

We will enable Hide NAT at the object level, so this is a good time to connect to Check Point SmartConsole. Go to **Objects** on the top right and navigate to **Network Objects** and then to **Networks.** Right-click on **L-LAN-NET** and click **Edit.**



L-LAN-NET window will be displayed, see below.



Network

L-LAN-NET

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Hide

● Hide behind the gateway

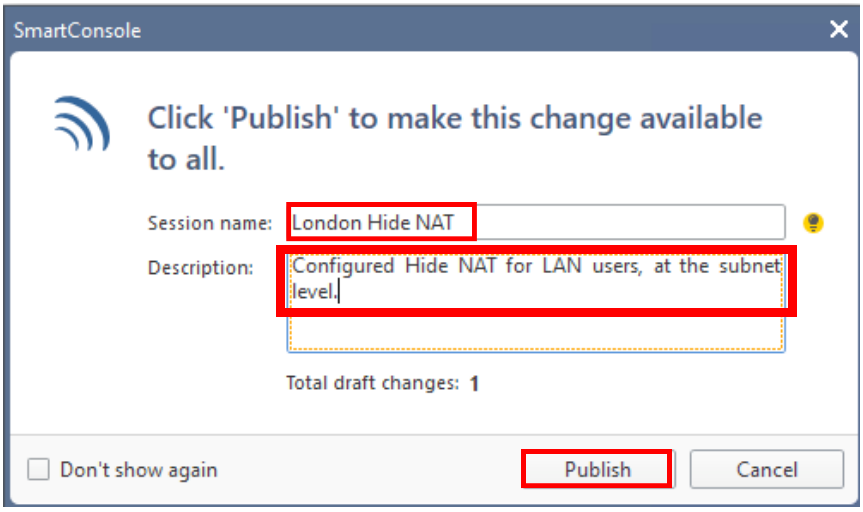
○ Hide behind IP address

IPv4 address: 0.0.0.0

IPv6 address: ::

Install on gateway: L-FW-1

Now, let’s publish the changes



SmartConsole

Click 'Publish' to make this change available to all.

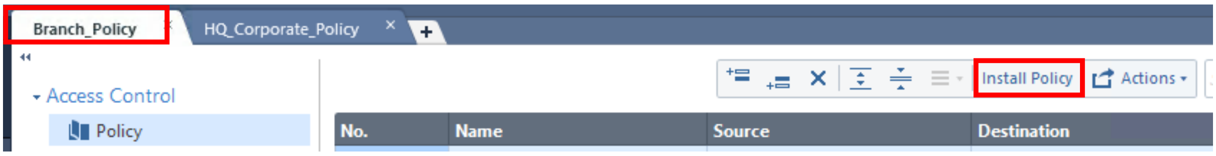
Session name: London Hide NAT

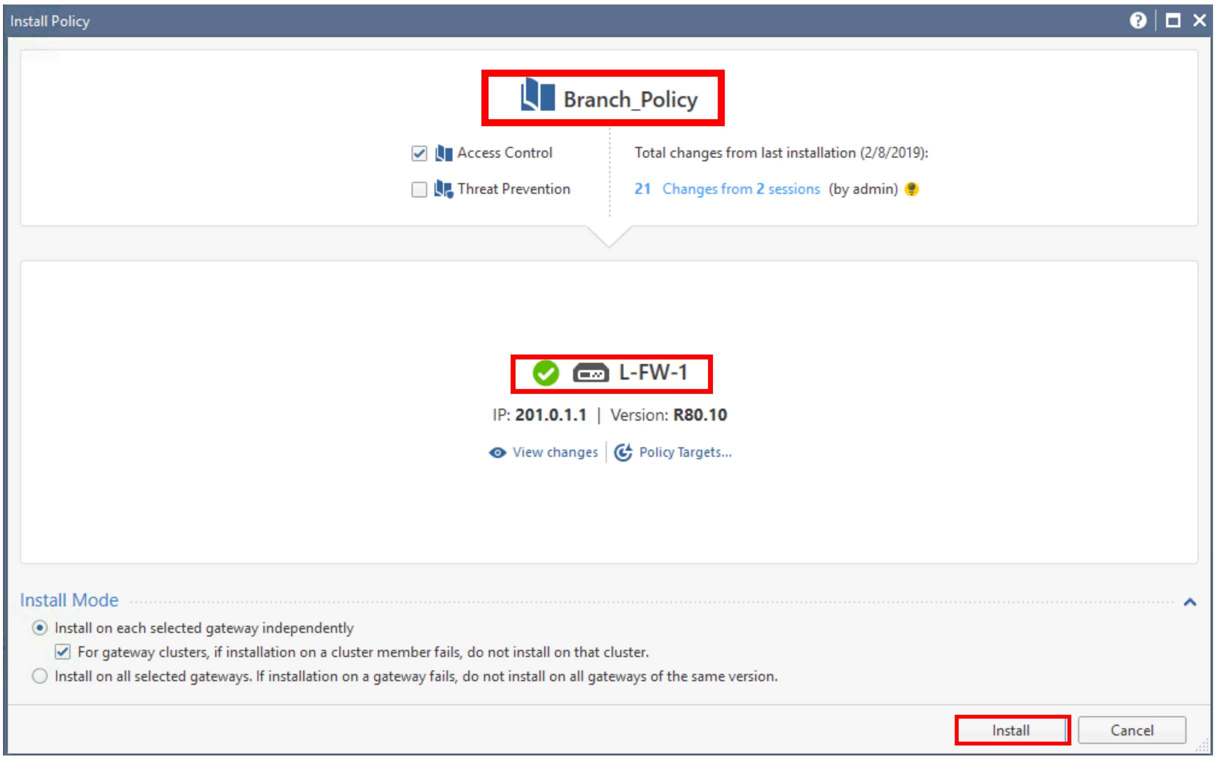
Description: Configured Hide NAT for LAN users, at the subnet level.

Total draft changes: 1

☐ Don't show again

And install the policy on London Gateway L-FW-1:





Install Policy

Branch_Policy

☑ Access Control

□ Threat Prevention

Total changes from last installation (2/8/2019):

21 Changes from 2 sessions (by admin)

L-FW-1

IP: 201.0.1.1 | Version: R80.10

View changes | Policy Targets...

Install Mode

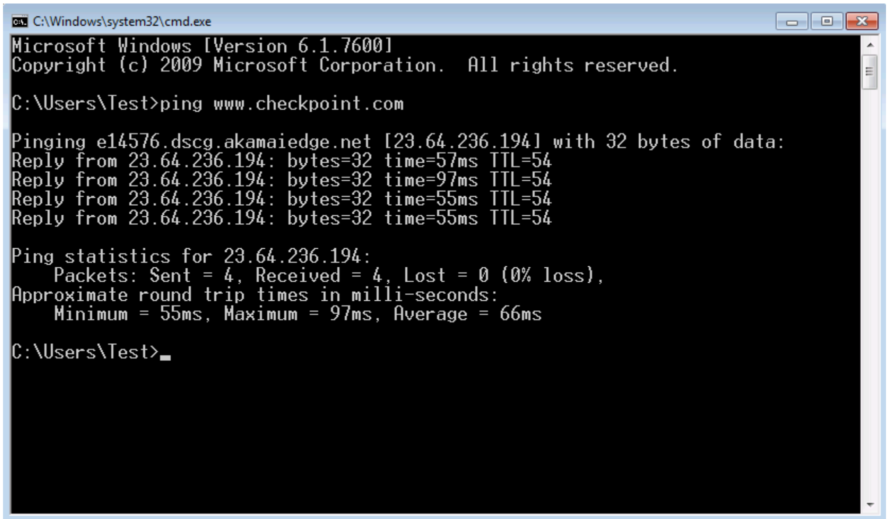
● Install on each selected gateway independently

☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

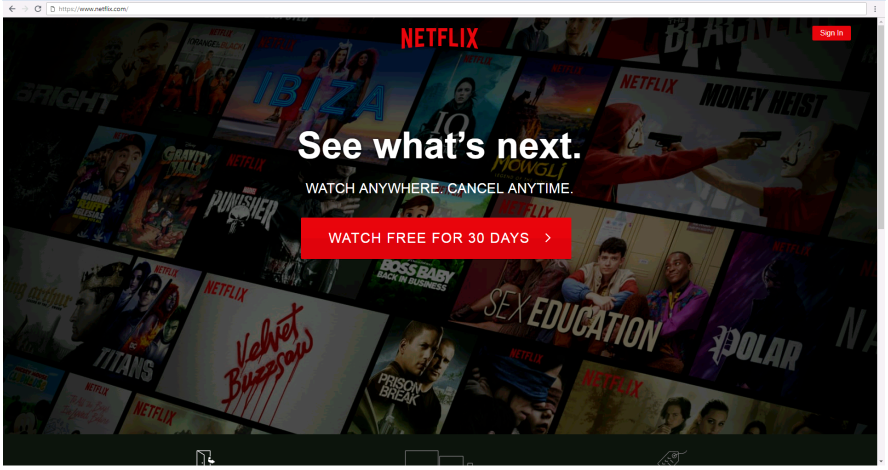
Install | Cancel

Connect to L-LAN-1 user and let's test internet connectivity:

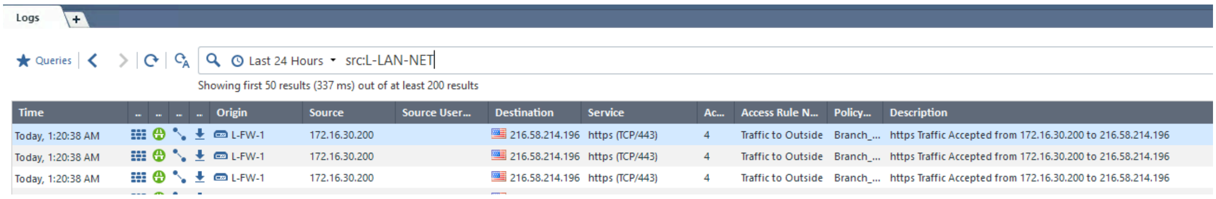


C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Test>ping www.checkpoint.com

Pinging e14576.dscg.akamaiedge.net [23.64.236.194] with 32 bytes of data:
Reply from 23.64.236.194: bytes=32 time=57ms TTL=54
Reply from 23.64.236.194: bytes=32 time=97ms TTL=54
Reply from 23.64.236.194: bytes=32 time=55ms TTL=54
Reply from 23.64.236.194: bytes=32 time=55ms TTL=54

Ping statistics for 23.64.236.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 97ms, Average = 66ms

C:\Users\Test>_
```



If we take a look in the **Logs&Monitor** and filter the logs with the following filter: **src:L-LAN-NET**

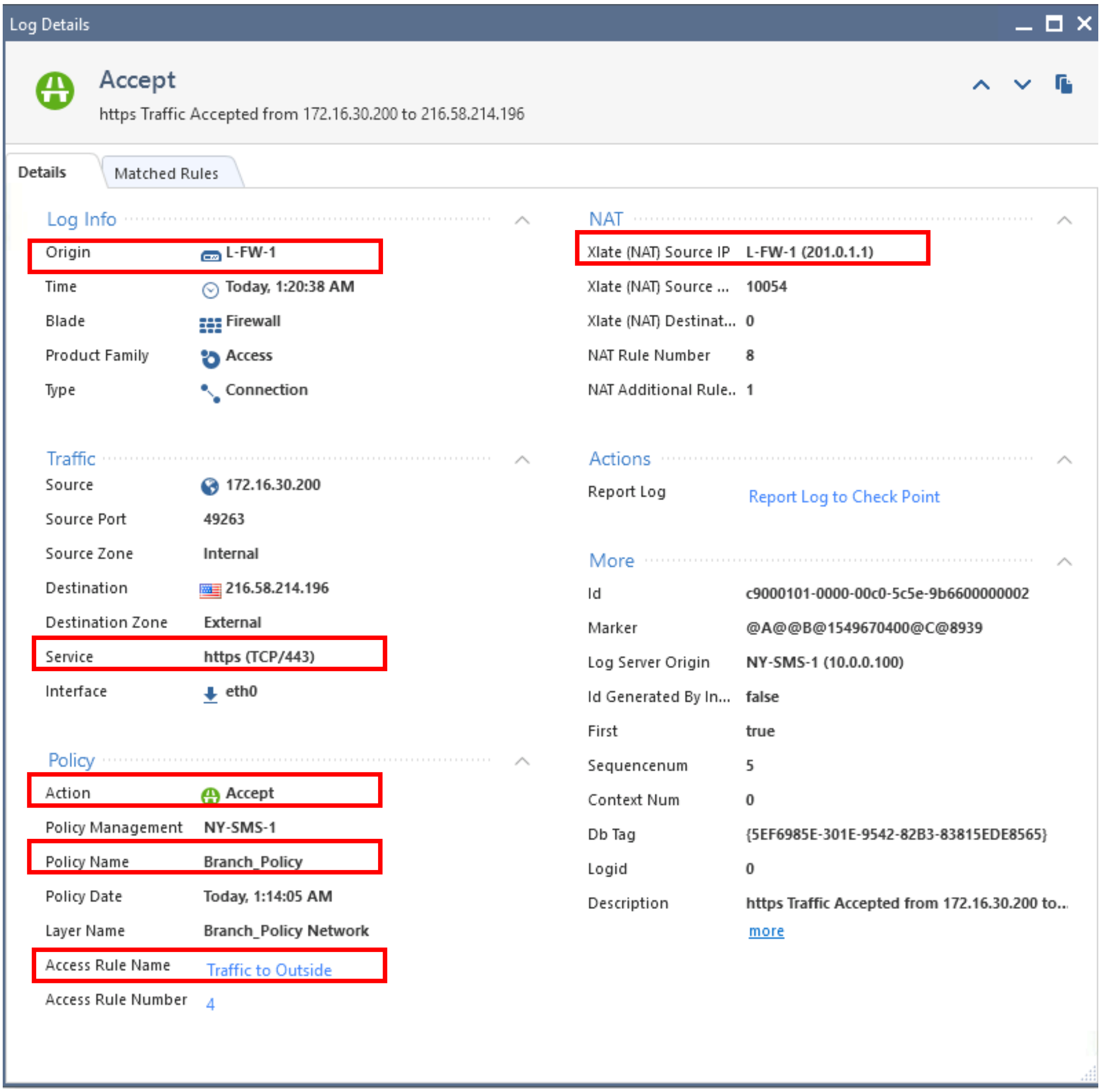


Last 24 Hours src:L-LAN-NET

Showing first 50 results (337 ms) out of at least 200 results

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 1:20:38 AM					L-FW-1	172.16.30.200		216.58.214.196	https (TCP/443)	4	Traffic to Outside	Branch_...	https Traffic Accepted from 172.16.30.200 to 216.58.214.196
Today, 1:20:38 AM					L-FW-1	172.16.30.200		216.58.214.196	https (TCP/443)	4	Traffic to Outside	Branch_...	https Traffic Accepted from 172.16.30.200 to 216.58.214.196
Today, 1:20:38 AM					L-FW-1	172.16.30.200		216.58.214.196	https (TCP/443)	4	Traffic to Outside	Branch_...	https Traffic Accepted from 172.16.30.200 to 216.58.214.196

we can definitely see logs. Double-click on latest log, at the top :



Accept

https Traffic Accepted from 172.16.30.200 to 216.58.214.196

Log Info

Origin	L-FW-1
Time	Today, 1:20:38 AM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	172.16.30.200
Source Port	49263
Source Zone	Internal
Destination	216.58.214.196
Destination Zone	External
Service	https (TCP/443)
Interface	eth0

Policy

Action	Accept
Policy Management	NY-SMS-1
Policy Name	Branch_Policy
Policy Date	Today, 1:14:05 AM
Layer Name	Branch_Policy Network
Access Rule Name	Traffic to Outside
Access Rule Number	4

NAT

Xlate (NAT) Source IP	L-FW-1 (201.0.1.1)
Xlate (NAT) Source ...	10054
Xlate (NAT) Destinat...	0
NAT Rule Number	8
NAT Additional Rule..	1

Actions

Report Log	Report Log to Check Point

More

Id	c9000101-0000-00c0-5c5e-9b6600000002
Marker	@A@@B@1549670400@C@8939
Log Server Origin	NY-SMS-1 (10.0.0.100)
Id Generated By In...	false
First	true
Sequencenum	5
Context Num	0
Db Tag	{5EF6985E-301E-9542-82B3-83815EDE8565}
Logid	0
Description	https Traffic Accepted from 172.16.30.200 to.. more

Origin – Log was generated by L-FW-1, Service – traffic was HTTPS, Accept – traffic was accepted – Branch_Policy and forwarded – Rule 4 and Source NAT took place.

27.0 Lab: Configure Outbound HTTPS Inspection on NY and London Gateways

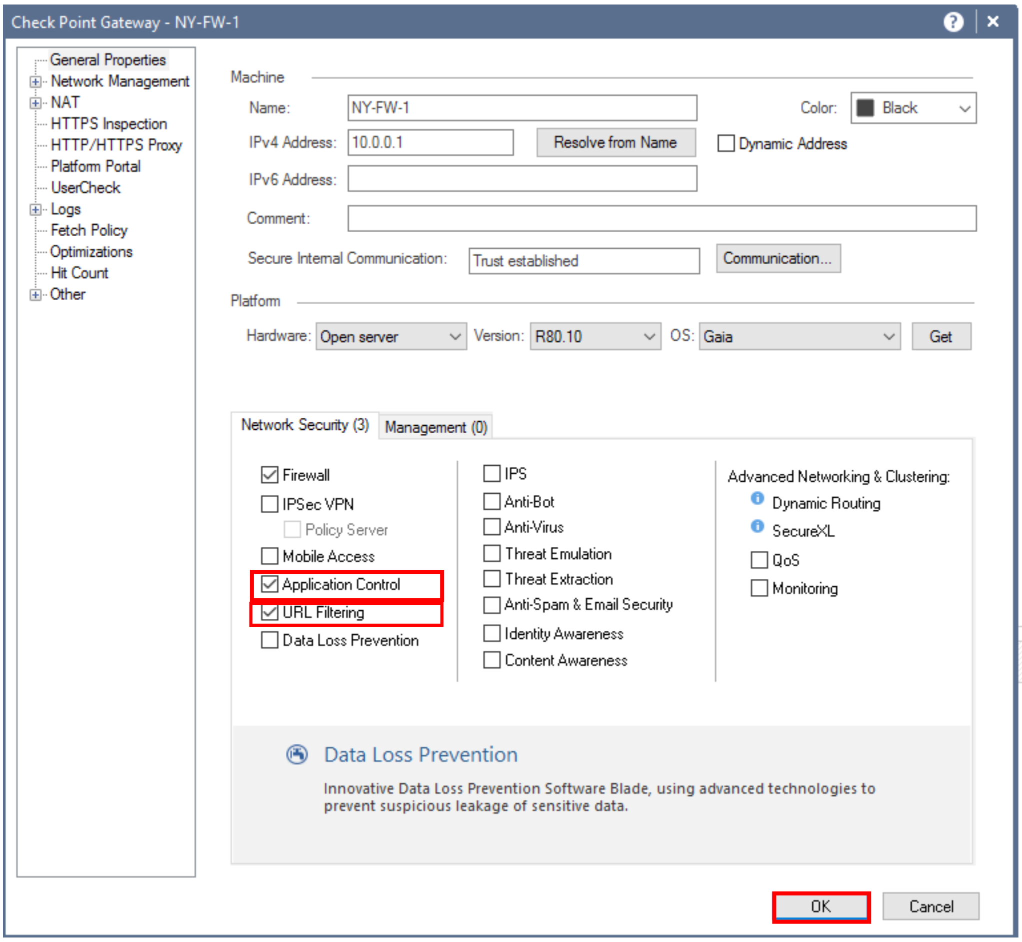
Lab Objectives

- Verify the HTTPS currently used for HTTPs connection
- Configure HTTPS inspection on both SGs – NY and London

Before we start the actual configuration of HTTPS inspection in our lab environment, it's actually a great idea to do some verifications and testing and observe how the network is performing, prior implementing any changes.

Following the successful configuration, in this lab and the following two, we will be able to see the actual traffic inside encrypted HTTPS also, so at this point it's a good idea to enable both **Application Control** and **URL Filtering** software blades on our Security Gateways.

Open SmartConsole and navigate to **Gateways&Servers.** Double-click on **NY-FW-1** and enable the two software blades:



Check Point Gateway - NY-FW-1

General Properties
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Platform Portal
UserCheck
Logs
Fetch Policy
Optimizations
Hit Count
Other

Machine

Name: NY-FW-1
Color: Black
IPv4 Address: 10.0.0.1
Resolve from Name
□ Dynamic Address
IPv6 Address:
Comment:
Secure Internal Communication: Trust established
Communication...

Platform

Hardware: Open server
Version: R80.10
OS: Gaia
Get

Network Security (3) | Management (0)

☑ Firewall
□ IPSec VPN
□ Policy Server
□ Mobile Access
☑ Application Control
☑ URL Filtering
□ Data Loss Prevention

□ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
□ Identity Awareness
□ Content Awareness

Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
□ Monitoring

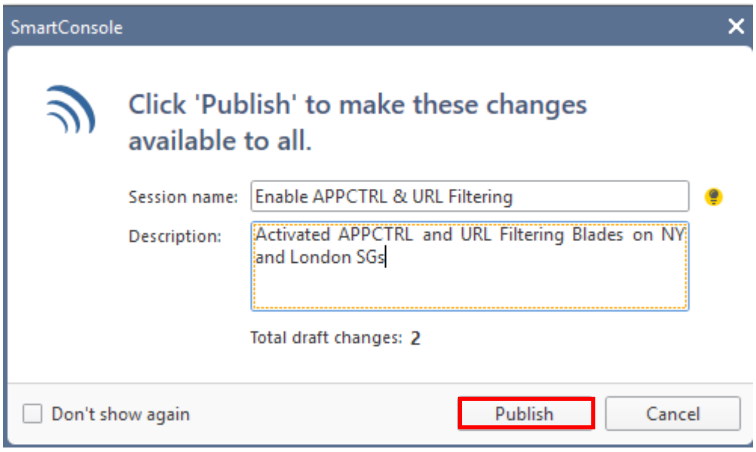
Data Loss Prevention

Innovative Data Loss Prevention Software Blade, using advanced technologies to prevent suspicious leakage of sensitive data.

OK | Cancel

Now, please go ahead and enable **Application Control** and **URL Filtering** software blades on L-FW-1 security gateway as well.

Publish the changes and install both policies, HQ_Corporate_Policy and Branch_Policy.



SmartConsole

Click 'Publish' to make these changes available to all.

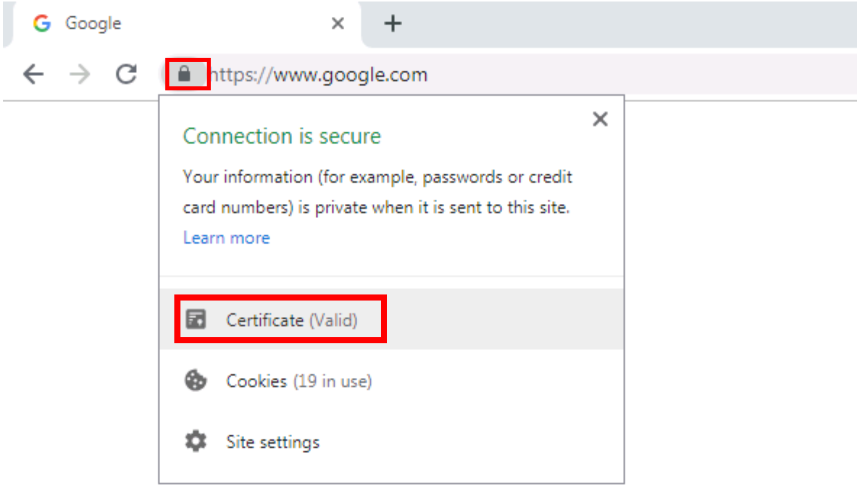
Session name: Enable APPCTRL & URL Filtering

Description: Activated APPCTRL and URL Filtering Blades on NY and London SGs

Total draft changes: 2

From NY-LAN-1 user, open a browser (for example Google Chrome) and navigate to https://google.com. In this step, the idea is to take a look at what certificate is the browser on NY-LAN-1 user using when establishing a secure connection with the Google Web Server.

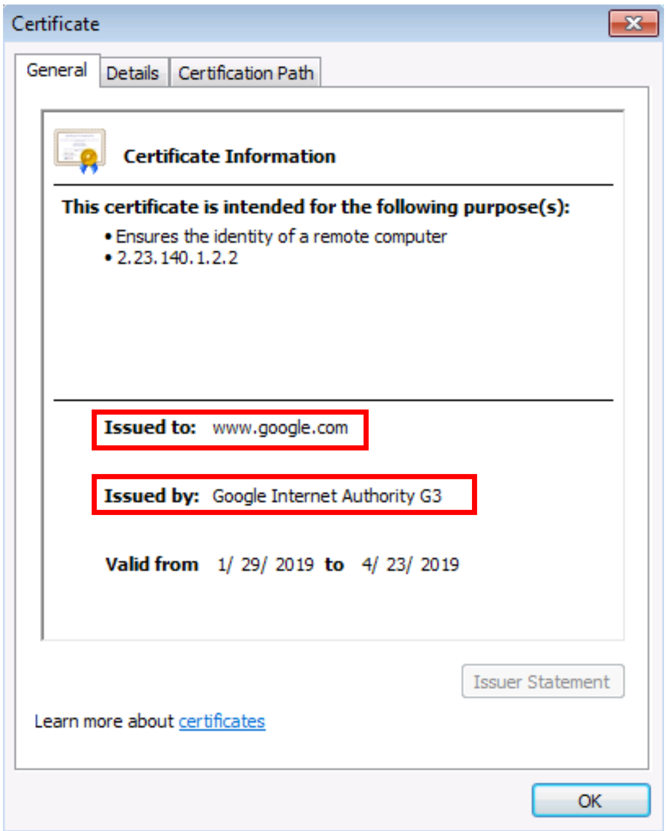
Click on the lock icon and then click on **Certificate.**



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

As you can see below, the certificate has been **issued to** (which means who is going to use it) www.google.com and the Certificate Authority that has issued the Certificate (**issued by**) is Google Internet Authority G3.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- 2.23.140.1.2.2

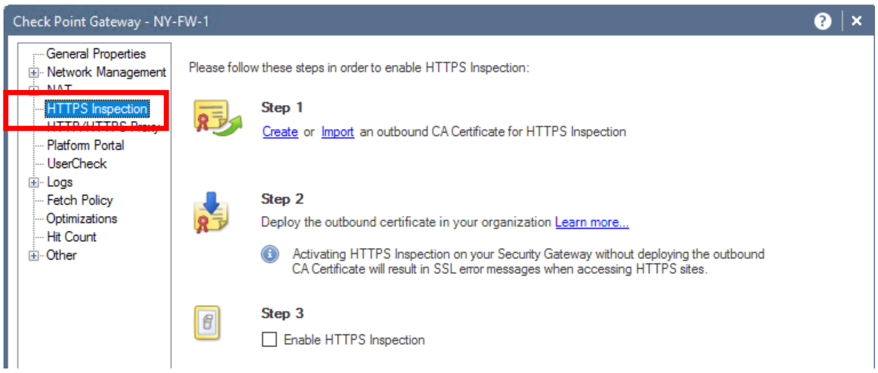
Issued to: www.google.com

Issued by: Google Internet Authority G3

Valid from 1/ 29/ 2019 **to** 4/ 23/ 2019

Learn more about certificates

Now, let’s enable HTTPS Inspection on NY-FW-1, first. Open NY-FW-1 gateway properties page and navigate to **HTTPS Inspection** on the left menu:



Please follow these steps in order to enable HTTPS Inspection:

Step 1
Create or Import an outbound CA Certificate for HTTPS Inspection

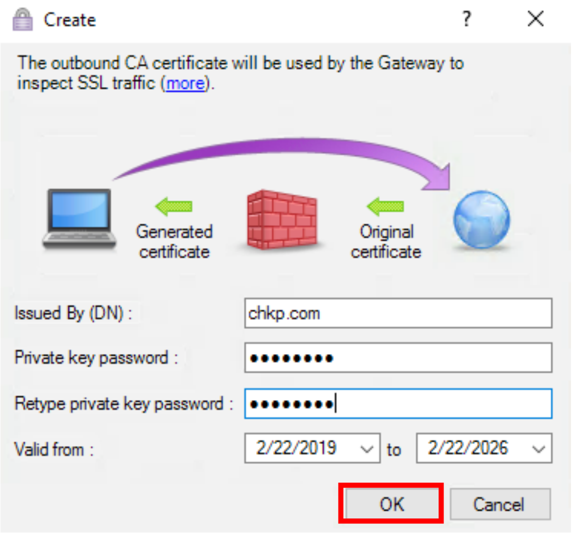
Step 2
Deploy the outbound certificate in your organization Learn more...

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3
☐ Enable HTTPS Inspection

As you can see as being presented in the window, we have to create in Step 1 a Certificate that is going to be used for Outbound HTTPS inspection. This is the certificate that is going to be used in order to establish the SSL tunnel with the client – source that will initiate the HTTPS connection. Click **Create** and fill in the necessary details:

Issued by – chkp.com -> this is just as an example
Private key – admin123
Retype private key – admin123



The outbound CA certificate will be used by the Gateway to inspect SSL traffic (more).

Issued By (DN) : chkp.com

Private key password : ••••••••

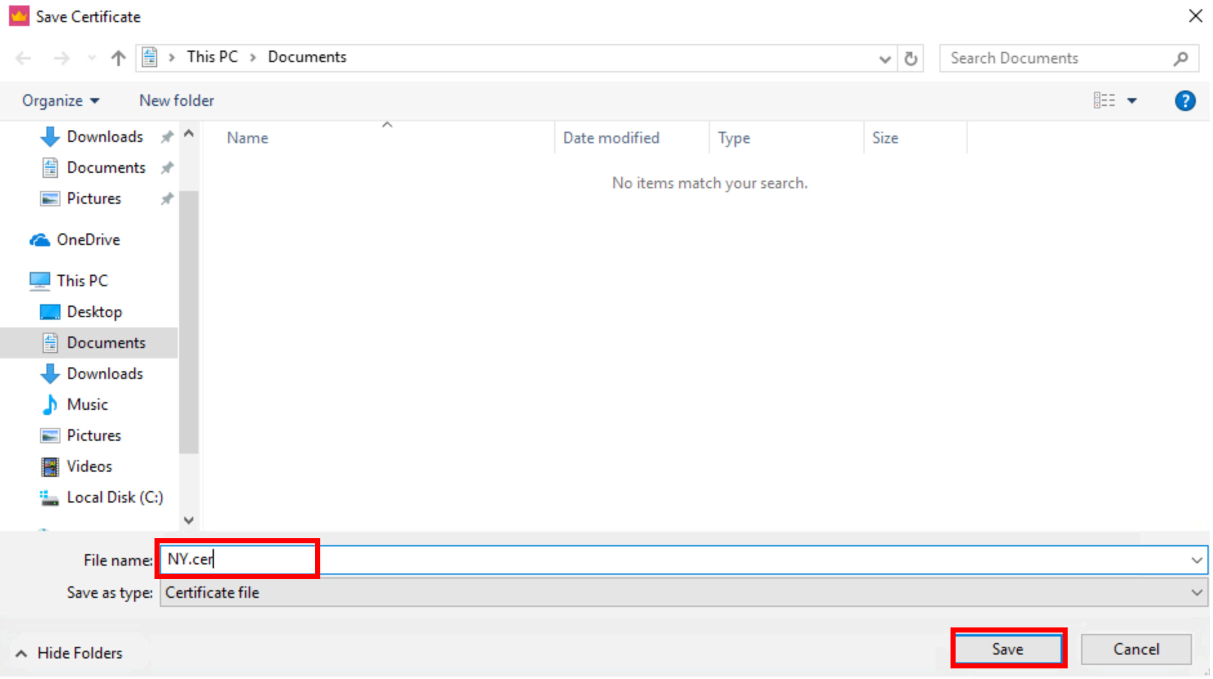
Retype private key password : ••••••••

Valid from : 2/22/2019 to 2/22/2026

Click **OK** when finished; now the certificate is being created.

In Step2, we will export the just created certificate in order to have it available later and install it on LAN users. More on this topic later.

Click **Export Certificate** and save the certificate as **NY.cer**.

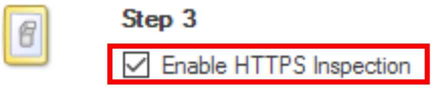


No items match your search.

File name: NY.cer

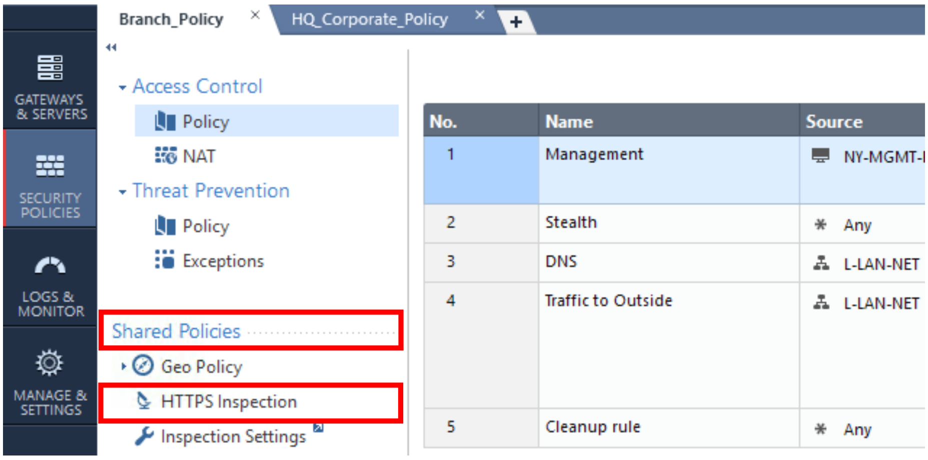
Save as type: Certificate file

Last step, step 3, enable **HTTPS Inspection** and click **OK**.



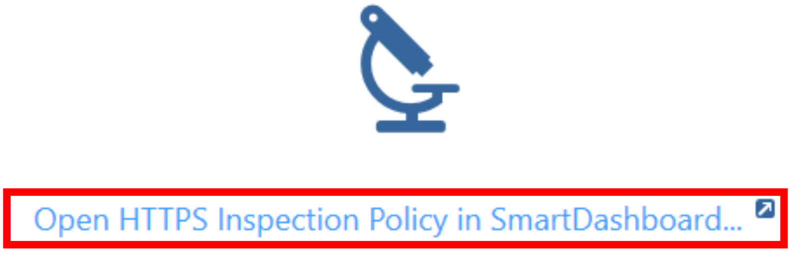
☑ Enable HTTPS Inspection

Now, we can go to Security Policies and under the **Shared Policies** click on **HTTPS Inspection**:



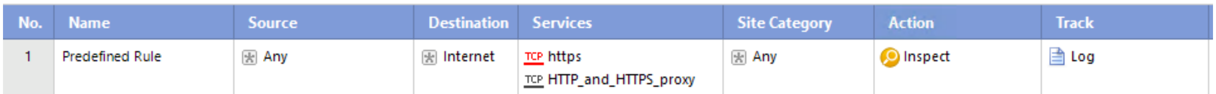
No.	Name	Source
1	Management	NY-MGMT-I
2	Stealth	Any
3	DNS	L-LAN-NET
4	Traffic to Outside	L-LAN-NET
5	Cleanup rule	Any

and then navigate to HTTPS Inspection Policy:



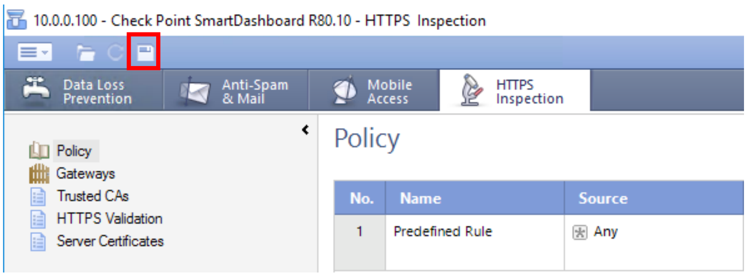
Rule number 1 is the Predefined Rule or the default rule that comes installed when enabling HTTPS Inspection. This is similar to the Cleanup Rule that is present when creating an Access Control Policy.

In order to actually see what is happening with our HTTPS traffic, we need to enable logging. In the **Track** column, right-click and select from the menu the **Log** option.



No.	Name	Source	Destination	Services	Site Category	Action	Track
1	Predefined Rule	Any	Internet	https HTTP_and_HTTPS_proxy	Any	Inspect	Log

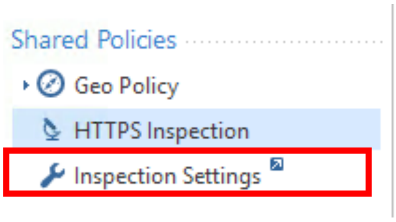
Now, let’s save the changes (click on Update button) and we can then close SmartDashboard.



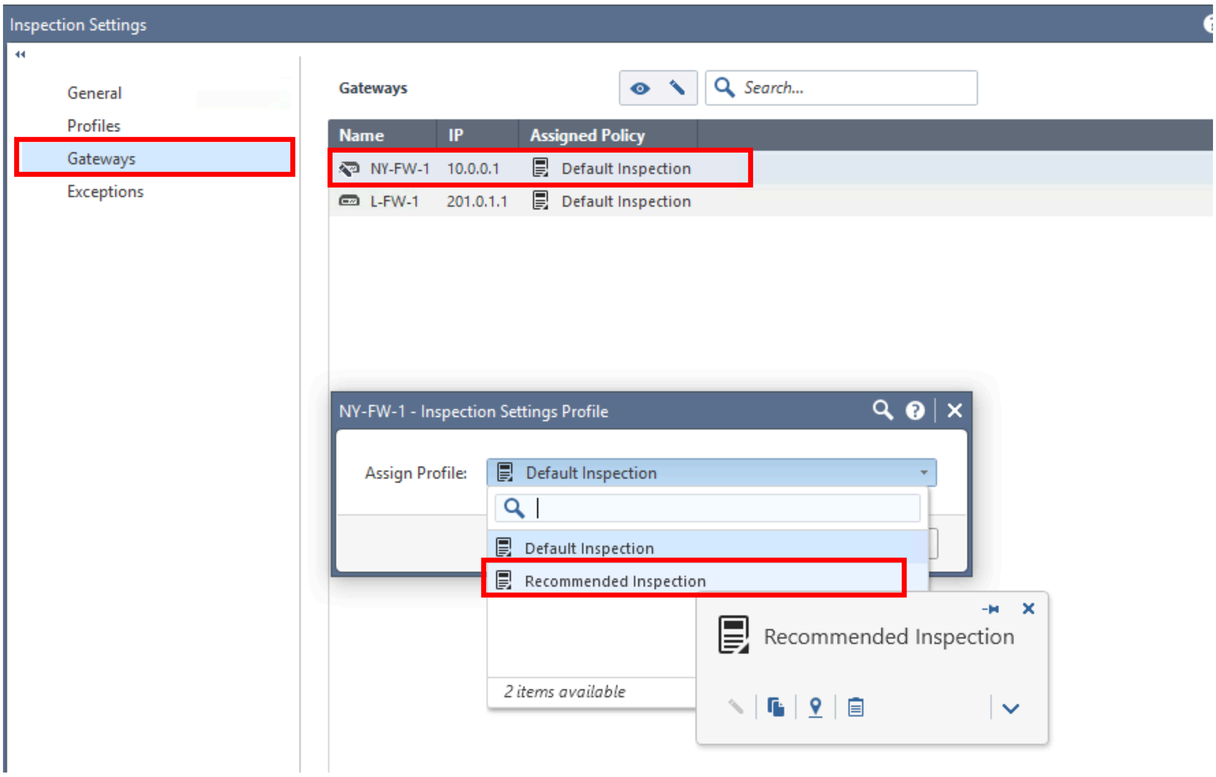
No.	Name	Source
1	Predefined Rule	Any

Returning back to SmartConsole, there is one more thing to do. Currently both gateways are using a HTTPS Inspection profile that is called – Default Inspection. This is not the most aggressive and "accurate" that we can use so let's change to the other profile that is already available – Recommended profile.

Under **Shared Policies**, click on **Inspection Settings**



Click on **Gateways** and then double-click **NY-FW-1**. Select in the **Assign Profile** drop-down menu the **Recommended Inspection** profile and confirm your choice by clicking **OK.**



Name	IP	Assigned Policy
NY-FW-1	10.0.0.1	Default Inspection
L-FW-1	201.0.1.1	Default Inspection

Assign Profile: Default Inspection

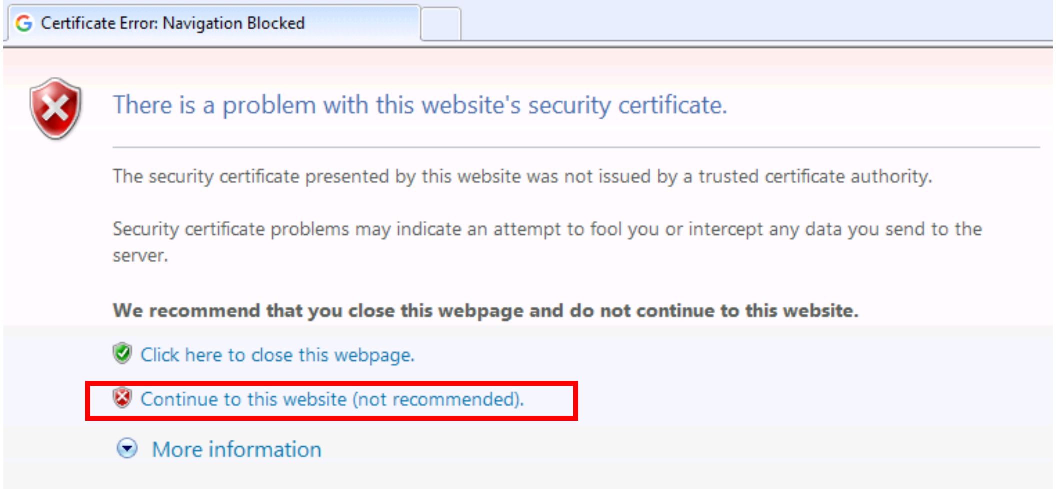
- Default Inspection
- Recommended Inspection

Repeat the same steps and activate the **Recommended Inspection** profile for London security gateway as well.

Now, publish and install both security policies, Corporate and Branch Policy.

Now, let’s do some testing. On the NY-LAN-1 user PC, navigate again to https://google.com in Internet Explorer browser.

We are now being displayed an error in the browser – **Certificate Error**:



Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

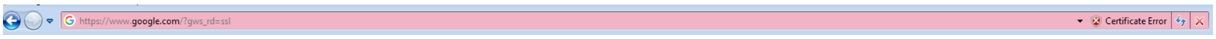
The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

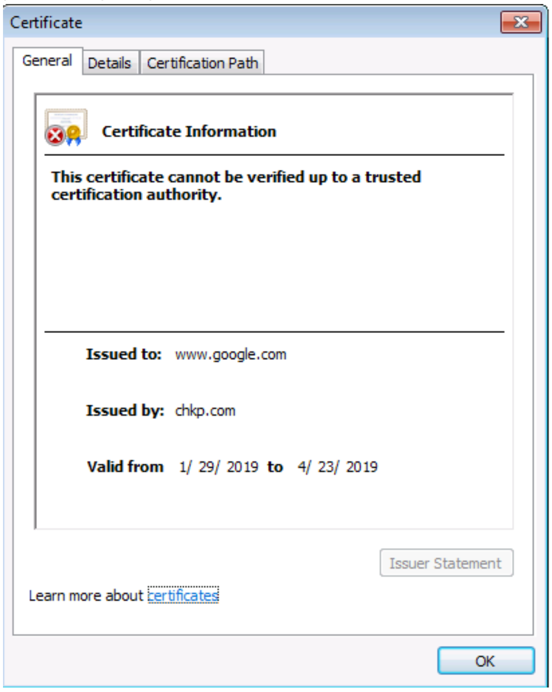
Click here to close this webpage.
Continue to this website (not recommended).
More information

Click on **Continue to this website** and the web page opens. Please take a close look at the URL tab:



https://www.google.com/?gws_rd=ssl

On the right side, there is some important information displayed – **Certificate Error.** Click on it and then click on **View Certificates**. Now information about the current Certificate being used between the client’s browser and the Check Point security gateway is displayed:



Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: www.google.com

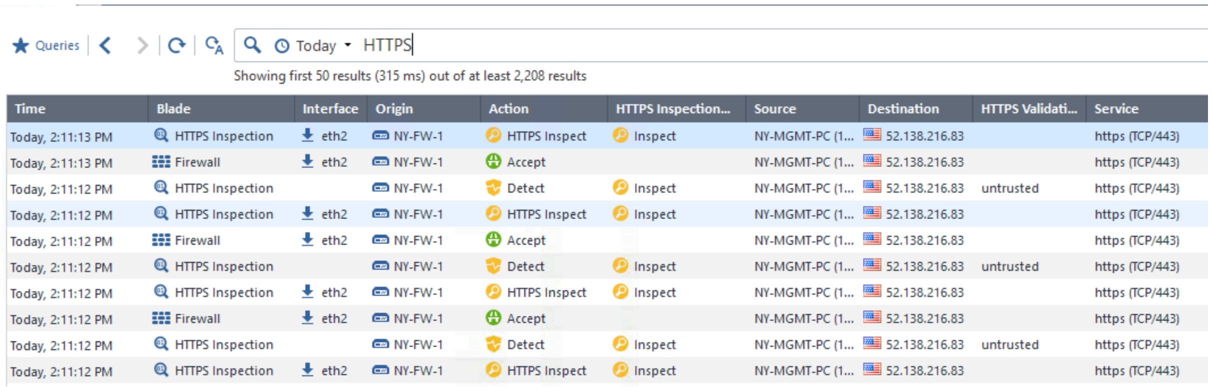
Issued by: chkp.com

Valid from 1/ 29/ 2019 **to** 4/ 23/ 2019

The certificate was issued for www.google.com use, and it was issued by **chkp.com,** which is actually the certificate we have defined when enabling the HTTPS Inspection.

Let’s now take a look at the logs in the **Logs&Monitor** section.

In the search bar, you can type **HTTPS** and you will see now a lot of events that have the action of **Inspect.** This indeed confirms that configuration has been successful.



HTTPS

Showing first 50 results (315 ms) out of at least 2,208 results

Time	Blade	Interface	Origin	Action	HTTPS Inspection...	Source	Destination	HTTPS Validati...	Service
Today, 2:11:13 PM	HTTPS Inspection	eth2	NY-FW-1	HTTPS Inspect	Inspect	NY-MGMT-PC (1...	52.138.216.83		https (TCP/443)
Today, 2:11:13 PM	Firewall	eth2	NY-FW-1	Accept		NY-MGMT-PC (1...	52.138.216.83		https (TCP/443)
Today, 2:11:12 PM	HTTPS Inspection		NY-FW-1	Detect	Inspect	NY-MGMT-PC (1...	52.138.216.83	untrusted	https (TCP/443)
Today, 2:11:12 PM	HTTPS Inspection	eth2	NY-FW-1	HTTPS Inspect	Inspect	NY-MGMT-PC (1...	52.138.216.83		https (TCP/443)
Today, 2:11:12 PM	Firewall	eth2	NY-FW-1	Accept		NY-MGMT-PC (1...	52.138.216.83		https (TCP/443)
Today, 2:11:12 PM	HTTPS Inspection		NY-FW-1	Detect	Inspect	NY-MGMT-PC (1...	52.138.216.83	untrusted	https (TCP/443)
Today, 2:11:12 PM	HTTPS Inspection	eth2	NY-FW-1	HTTPS Inspect	Inspect	NY-MGMT-PC (1...	52.138.216.83		https (TCP/443)
Today, 2:11:12 PM	Firewall	eth2	NY-FW-1	Accept		NY-MGMT-PC (1...	52.138.216.83		https (TCP/443)
Today, 2:11:12 PM	HTTPS Inspection		NY-FW-1	Detect	Inspect	NY-MGMT-PC (1...	52.138.216.83	untrusted	https (TCP/443)
Today, 2:11:12 PM	HTTPS Inspection	eth2	NY-FW-1	HTTPS Inspect	Inspect	NY-MGMT-PC (1...	52.138.216.83		https (TCP/443)

28.0 Lab: Install the CA Certificate on LAN users' PCs

Lab Objectives

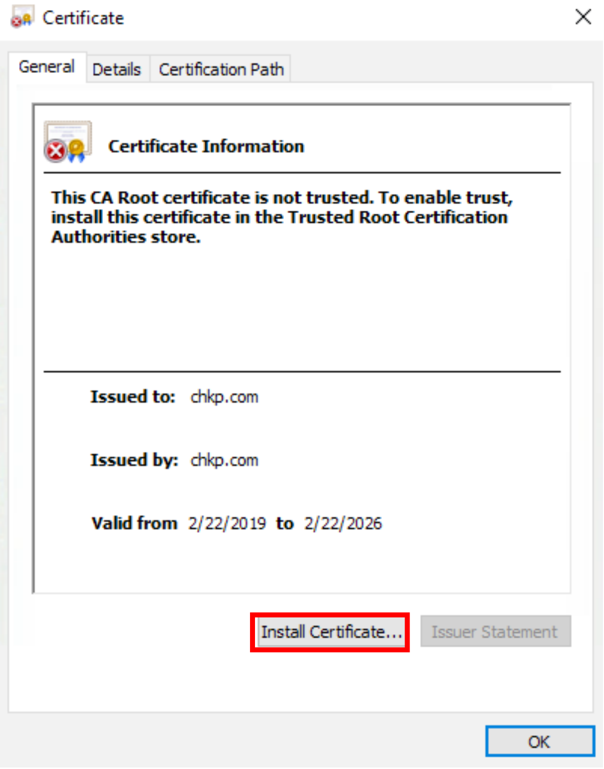
- Deploy the chkp.com locally generated certificate on LAN users' PC

In this lab we will install the certificate we have generated in the previous lab on the LAN users. We will do this on NY-LAN-1, NY-MGMT-PC and L-LAN-1.

In the lab environment I am working on, NY-LAN-1 and L-LAN-1 are Windows 7 machines, while the management PC is running Windows 10. I will be doing the installation on all of these just that I highlight the potential differences while installing a certificate if running W7 or W10 operating system.

Technically speaking, we only need this to be done on LAN users – NY-LAN-1 and L-LAN-1, because this are the PCs that are going out to the Internet.

In order to start the process, double-click the certificate – NY. Click **Install Certificate** button:



Certificate Information

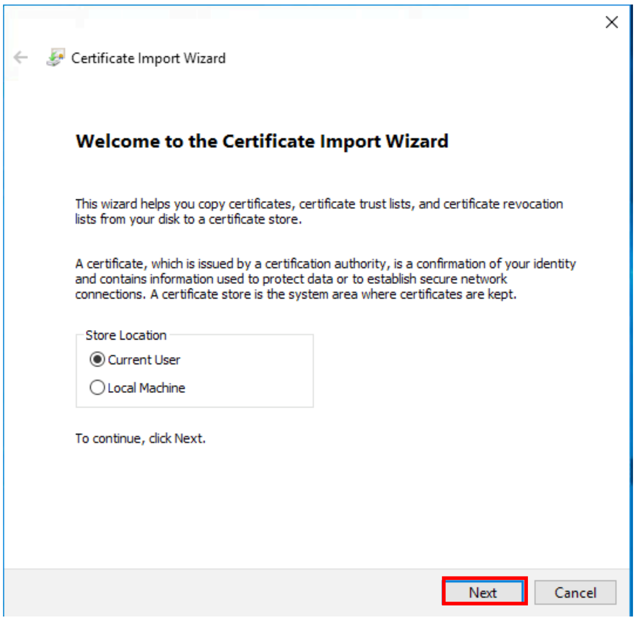
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: chkp.com

Issued by: chkp.com

Valid from 2/22/2019 to 2/22/2026

Leave everything as it is and click **Next** now :



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

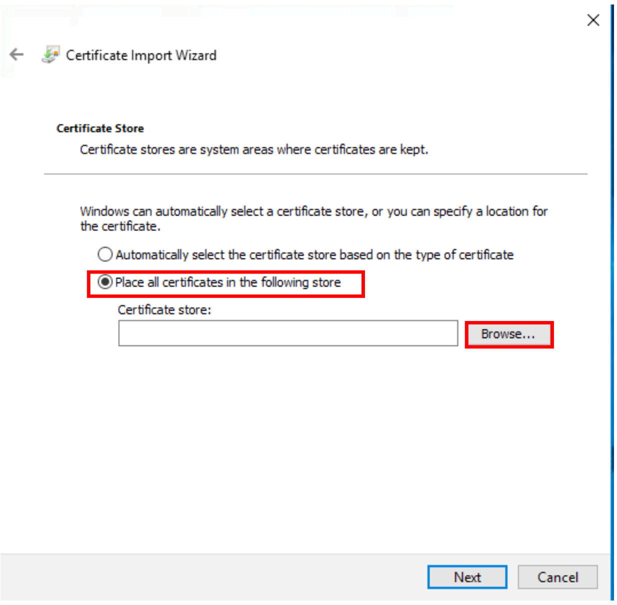
Store Location

● Current User

○ Local Machine

To continue, click Next.

We will manually select now where to place the certificate:



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

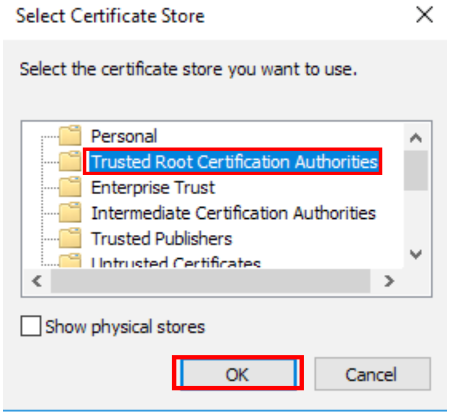
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Select **Trusted Root Certification Authorities** from the list



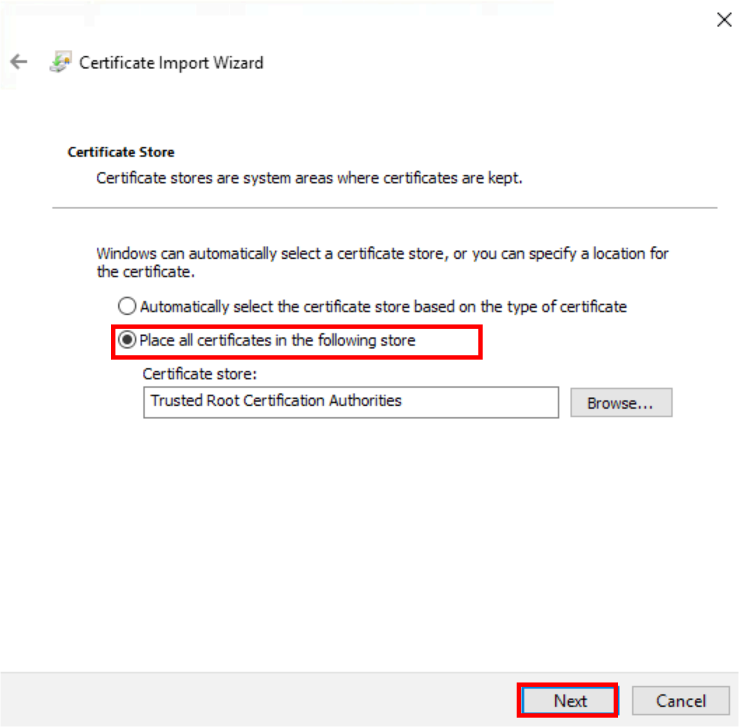
Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates

□ Show physical stores

and then click **Next**:



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

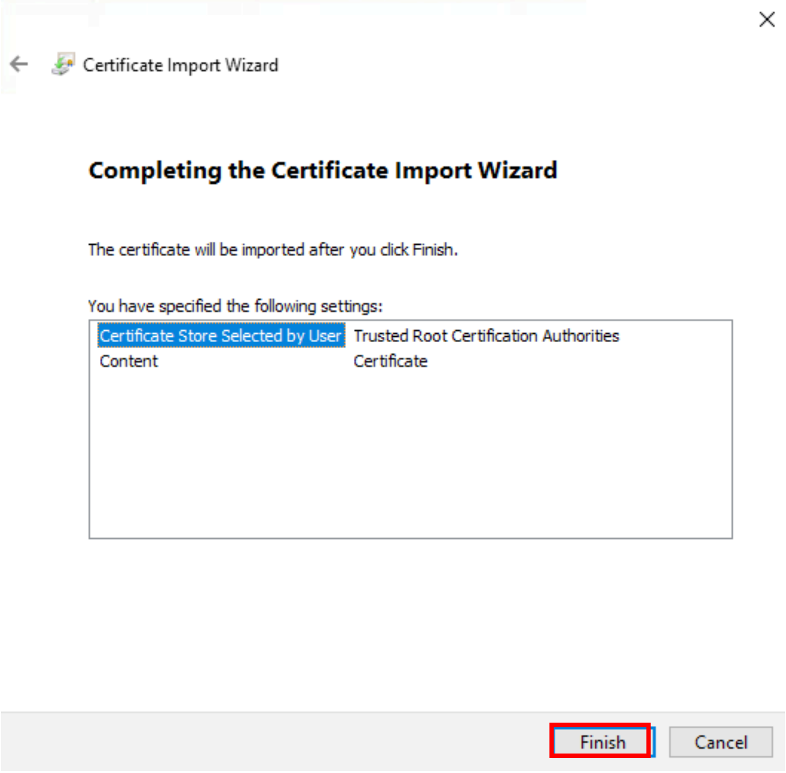
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Next, click **Finish**:



Certificate Import Wizard

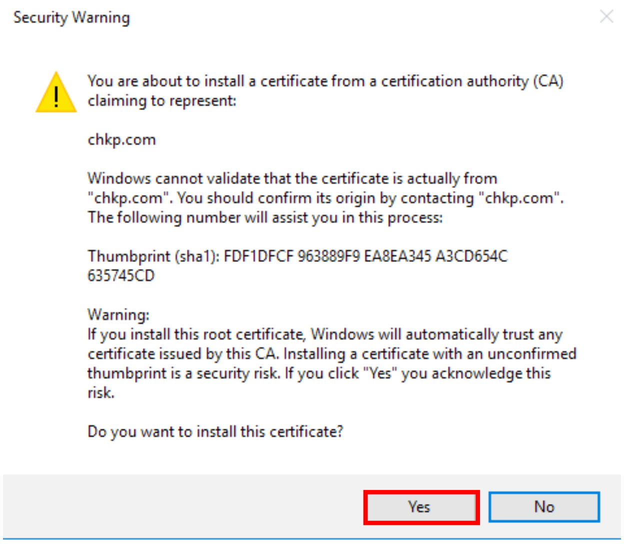
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Now, you should confirm that you want to install the certificate, so click **Yes**.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

chkp.com

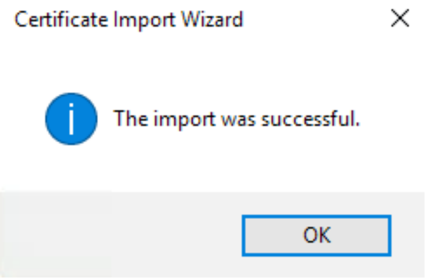
Windows cannot validate that the certificate is actually from "chkp.com". You should confirm its origin by contacting "chkp.com". The following number will assist you in this process:

Thumbprint (sha1): FDF1DFCF 963889F9 EA8EA345 A3CD654C 635745CD

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

and you should receive now a confirmation that the certificate import was successful.



Certificate Import Wizard

The import was successful.

Now, let's import the certificate on NY-LAN-1 and L-LAN-1 PCs. In order to do that, we need to get the NY Certificate on these machines. One method would be to use some kind of document sharing method – google drive, dropbox etc. If following this method, upload NY.cer file to your favourite choice and then download it on NY and London user PCs.

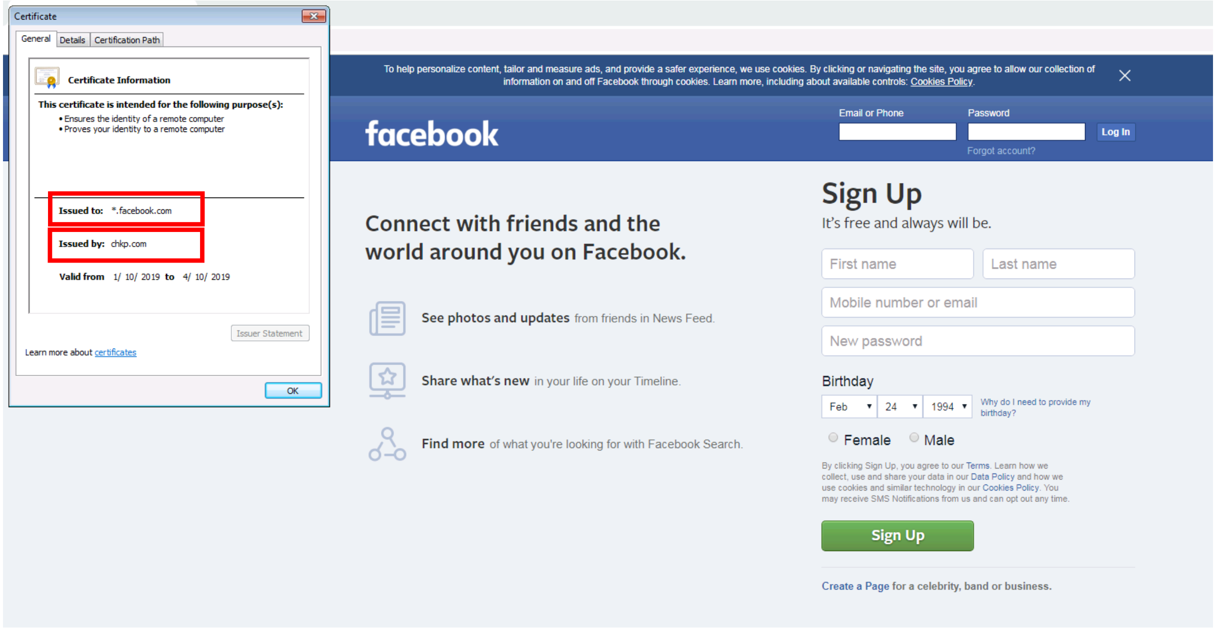
Please note that you may need to temporary disable HTTPS inspection on NY-FW-1 and L-FW-1 in order to succeed. Have tried several methods to download the certificate from different vendors – dropbox, drive, etc but because of certificate error … the page simply doesn't load and download is nearly impossible.

Don't forget to enable back HTTP Inspection (Step3 checkbox) after successfully completing the download.

Installation on Windows 7 machine is actually the same, no differences in the windows on menus displayed, so use the same steps as outlined above !!

Now, let’s run some verification steps. We now expect to see that the browsers are using the chkp.com certificate and no errors are displayed in the browsers while using HTTPS.

Open a browser in NY-LAN-1 or L-LAN-1 and navigate to https://facebook.com for example. Examine what Certificate is currently being used:



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

Issued to: *.facebook.com

Issued by: chkp.com

Valid from 1/ 10/ 2019 **to** 4/ 10/ 2019

Learn more about certificates

To help personalize content, tailor and measure ads, and provide a safer experience, we use cookies. By clicking or navigating the site, you agree to allow our collection of information on and off Facebook through cookies. Learn more, including about available controls: Cookies Policy.

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what’s new in your life on your Timeline.

Find more of what you’re looking for with Facebook Search.

It’s free and always will be.

Birthday: Feb 24 1994

○ Female ○ Male

By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Data Policy and how we use cookies and similar technology in our Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Create a Page for a celebrity, band or business.

This confirms that HTTPS is working and the browser is now using, without throwing any errors, the locally generated certificate – chkp.com.

29.0 Lab: Configure HTTPS Inspection Bypass Rules

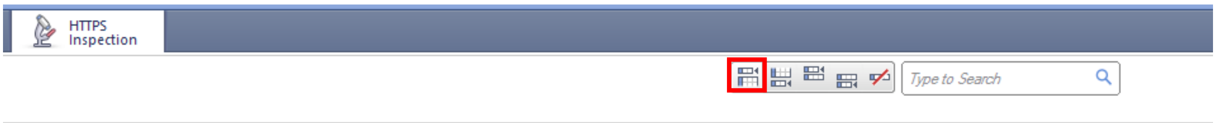
Lab Objectives

- Learn how to configure HTTPS bypass rules in order to exclude traffic from being inspected

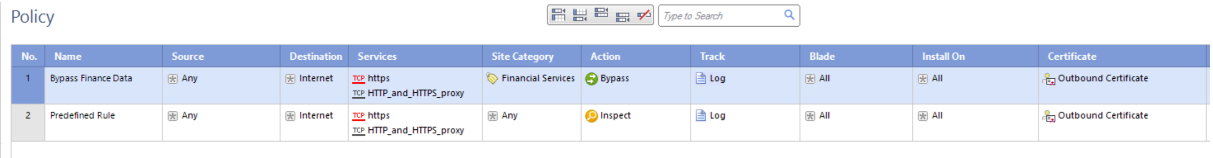
In some situations, you will need to exclude traffic from HTTPS inspection, for different reasons: private financial data (banks), healthcare specific information (personal health records information), etc.

In this lab we will configure a new rule in the HTTPS Inspection Policy rule base in order to exempt from inspection finance traffic. This means that, for example, the Check Point security gateway will not “look” inside packets that are destined to financial institutions. This way we are protecting the client’s privacy : authentication credentials, account information, etc.

Navigate to HTTPS Inspection Policy in SmartDashboard and let’s add another rule to the top of our HTTPS Inspection Rule Base.

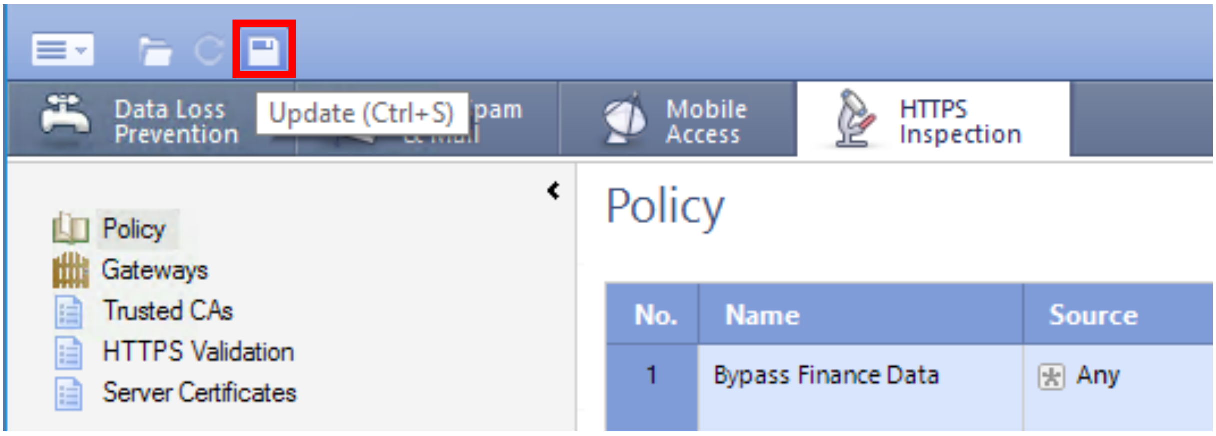


When complete, your new Rule Base should look like you can see below:



No.	Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Certificate
1	Bypass Finance Data	Any	Internet	TCP https TCP HTTP_and_HTTPS_proxy	Financial Services	Bypass	Log	All	All	Outbound Certificate
2	Predefined Rule	Any	Internet	TCP https TCP HTTP_and_HTTPS_proxy	Any	Inspect	Log	All	All	Outbound Certificate

Don’t forget to save the changes and then close SmartDashboard.



No.	Name	Source
1	Bypass Finance Data	Any

You should now go to SmartConsole, publish the changes and install the policies, for both HQ and Branch sites.

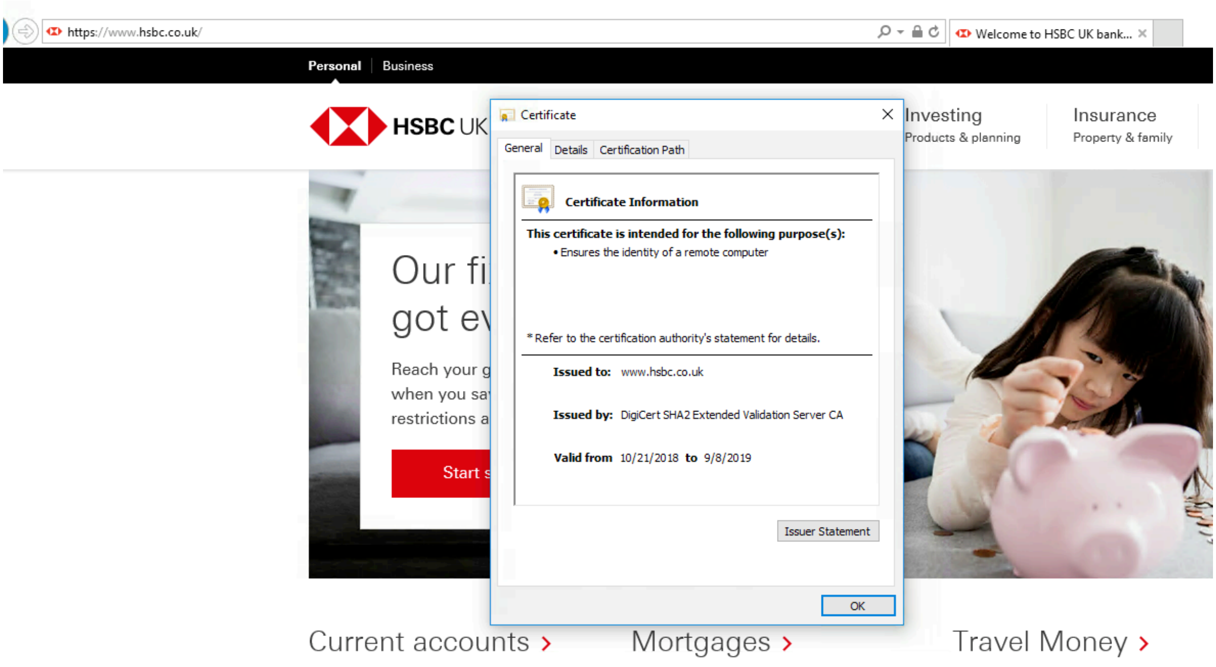
Now, how are we going to verify that indeed traffic is not inspected, but bypassed ?

Open up a browser and let's navigate to https://www.hsbc.co.uk and https://www.jpmorganchase.com some of the largest banks here in UK and also in the USA.

Financial traffic BYPASS verification consists of two steps: first, we should see that the browser established HTTPS connection with these two websites using a Public Certificate and not using the chkp.com certificate we generated and second, we should see logs in **Logs&Monitor** with the action of **Bypass.**

Here is the information for https://hsbc.co.uk:

The certificate being used for end-to-end encryption is issued by DigiCert.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

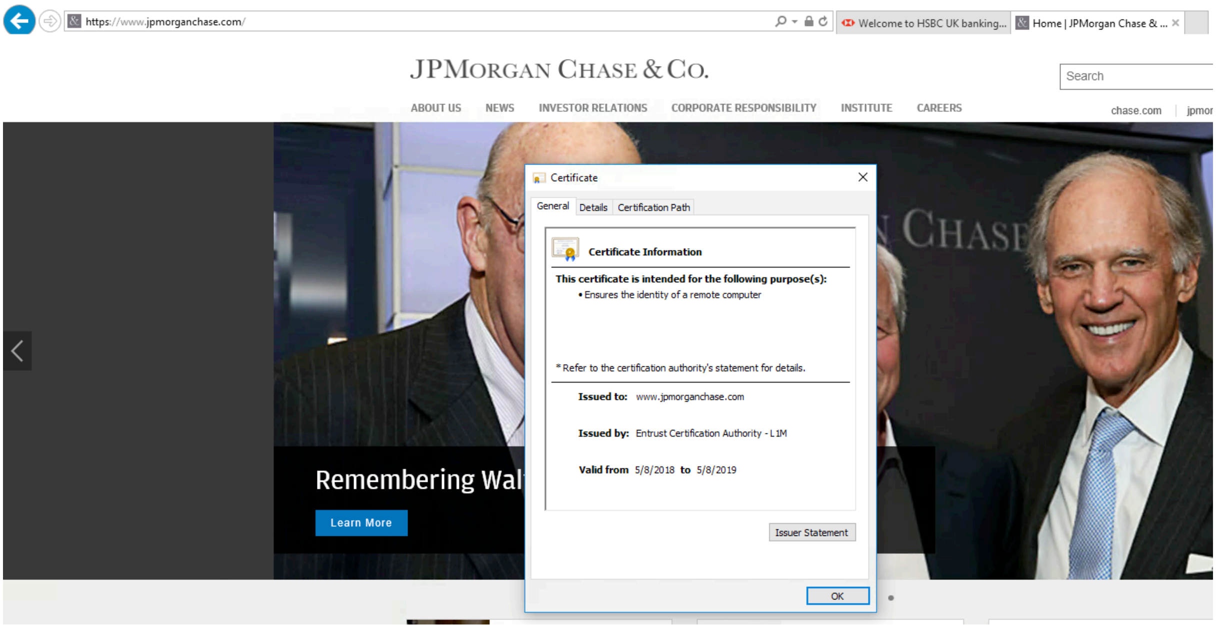
Issued to: www.hsbc.co.uk

Issued by: DigiCert SHA2 Extended Validation Server CA

Valid from 10/21/2018 to 9/8/2019

Let's take a look now also at connection to JP Morgan.

Certificate used has been issued by Entrust, which is again what we expected.



https://www.jpmorganchase.com/

Welcome to HSBC UK banking... | Home | JPMorgan Chase & ...

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.jpmorganchase.com

Issued by: Entrust Certification Authority - L1M

Valid from 5/8/2018 **to** 5/8/2019

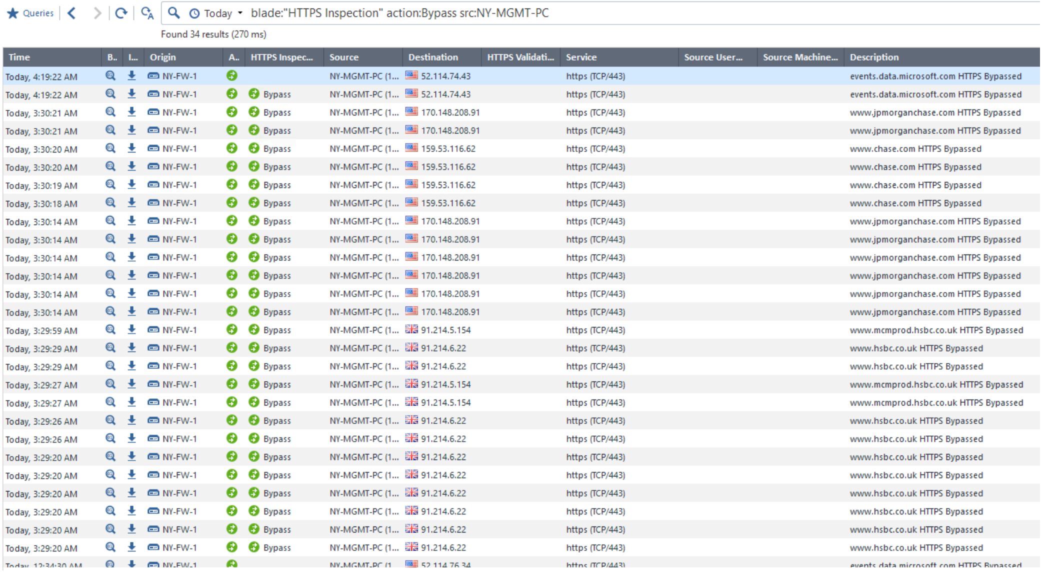
Let's now examine the Logs generated. Filter the logs with the following:

blade:"HTTPS Inspection" action:Bypass src:NY-MGMT-PC

taking into account that the source of the HTTPS sessions is in my case the NY-MGMT-PC. If you are running the tests from NY-LAN-1 PC, please modify the source in the search query accordingly.

blade:"HTTPS Inspection" action:Bypass src:NY-LAN-1

Please note that this is not necessary, but I would say that it is recommended, in order to not spend time on digging for the logs you need to validate or investigate some specific issue.

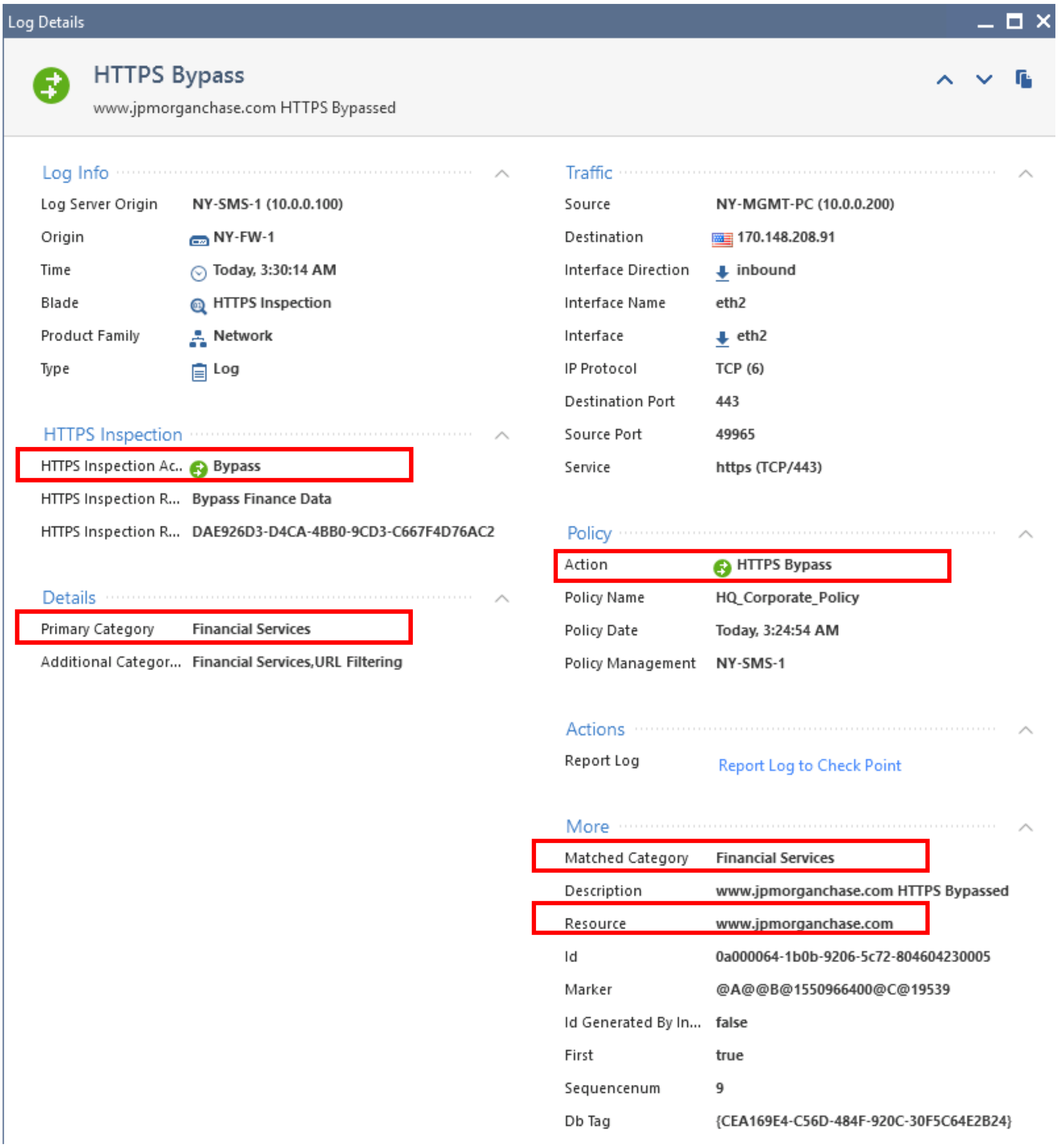


Today ▾ blade:"HTTPS Inspection" action:Bypass src:NY-MGMT-PC

Found 34 results (270 ms)

Time	B..	I...	Origin	A..	HTTPS Inspec...	Source	Destination	HTTPS Validati...	Service	Source User...	Source Machine...	Description
Today, 4:19:22 AM	🔍	⬇	NY-FW-1	●		NY-MGMT-PC (1...	52.114.74.43		https (TCP/443)			events.data.microsoft.com HTTPS Bypassed
Today, 4:19:22 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	52.114.74.43		https (TCP/443)			events.data.microsoft.com HTTPS Bypassed
Today, 3:30:21 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:30:21 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:30:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	159.53.116.62		https (TCP/443)			www.chase.com HTTPS Bypassed
Today, 3:30:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	159.53.116.62		https (TCP/443)			www.chase.com HTTPS Bypassed
Today, 3:30:19 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	159.53.116.62		https (TCP/443)			www.chase.com HTTPS Bypassed
Today, 3:30:18 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	159.53.116.62		https (TCP/443)			www.chase.com HTTPS Bypassed
Today, 3:30:14 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:30:14 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:30:14 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:30:14 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:30:14 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:30:14 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	170.148.208.91		https (TCP/443)			www.jpmorganchase.com HTTPS Bypassed
Today, 3:29:59 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.5.154		https (TCP/443)			www.mcmprod.hsbc.co.uk HTTPS Bypassed
Today, 3:29:29 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:29 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:27 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.5.154		https (TCP/443)			www.mcmprod.hsbc.co.uk HTTPS Bypassed
Today, 3:29:27 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.5.154		https (TCP/443)			www.mcmprod.hsbc.co.uk HTTPS Bypassed
Today, 3:29:26 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:26 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 3:29:20 AM	🔍	⬇	NY-FW-1	●	Bypass	NY-MGMT-PC (1...	91.214.6.22		https (TCP/443)			www.hsbc.co.uk HTTPS Bypassed
Today, 12:34:30 AM	🔍	⬇	NY-FW-1	●		NY-MGMT-PC (1	52.114.76.34		https (TCP/443)			events.data.microsoft.com HTTPS Bypassed

Let’s open up one of the logs in order to better see what’s happening:



Log Details

HTTPS Bypass

www.jpmorganchase.com HTTPS Bypassed

Log Info

Log Server Origin	NY-SMS-1 (10.0.0.100)
Origin	NY-FW-1
Time	Today, 3:30:14 AM
Blade	HTTPS Inspection
Product Family	Network
Type	Log

HTTPS Inspection

HTTPS Inspection Ac...	Bypass
HTTPS Inspection R...	Bypass Finance Data
HTTPS Inspection R...	DAE926D3-D4CA-4BB0-9CD3-C667F4D76AC2

Details

Primary Category	Financial Services
Additional Categor...	Financial Services,URL Filtering

Traffic

Source	NY-MGMT-PC (10.0.0.200)
Destination	170.148.208.91
Interface Direction	inbound
Interface Name	eth2
Interface	eth2
IP Protocol	TCP (6)
Destination Port	443
Source Port	49965
Service	https (TCP/443)

Policy

Action	HTTPS Bypass
Policy Name	HQ_Corporate_Policy
Policy Date	Today, 3:24:54 AM
Policy Management	NY-SMS-1

Actions

Report Log	Report Log to Check Point

More

Matched Category	Financial Services
Description	www.jpmorganchase.com HTTPS Bypassed
Resource	www.jpmorganchase.com
Id	0a000064-1b0b-9206-5c72-804604230005
Marker	@A@@B@1550966400@C@19539
Id Generated By In...	false
First	true
Sequencenum	9
Db Tag	{CEA169E4-C56D-484F-920C-30F5C64E2B24}

30.0 Lab: Install Active Directory on Windows Server 2012

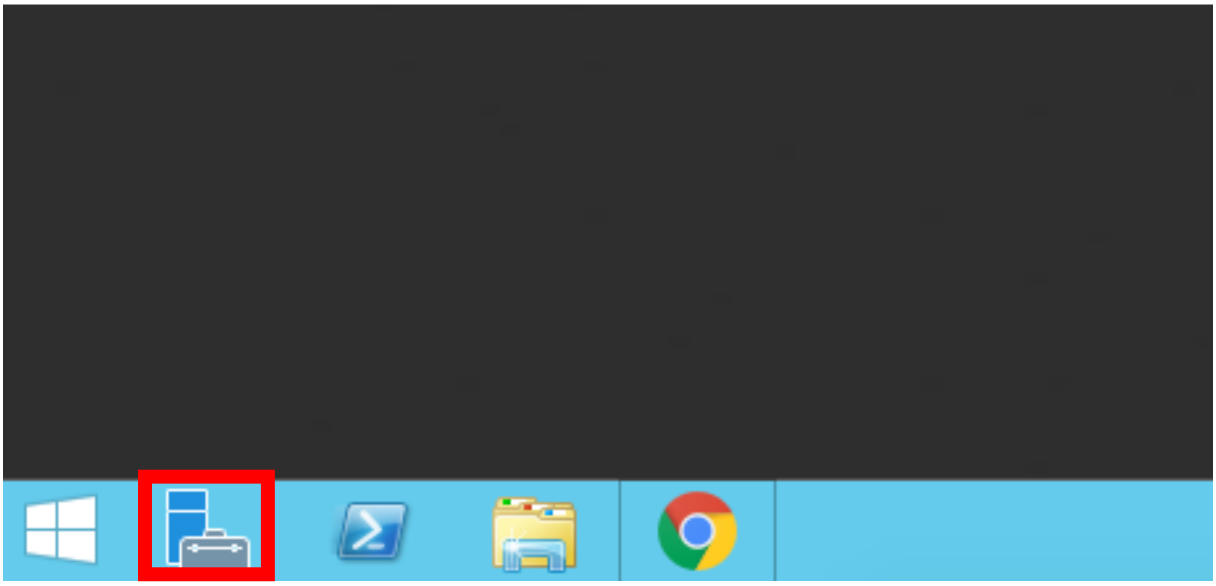
Lab Objectives

- Install and Configure Active Directory on Windows Server 2012

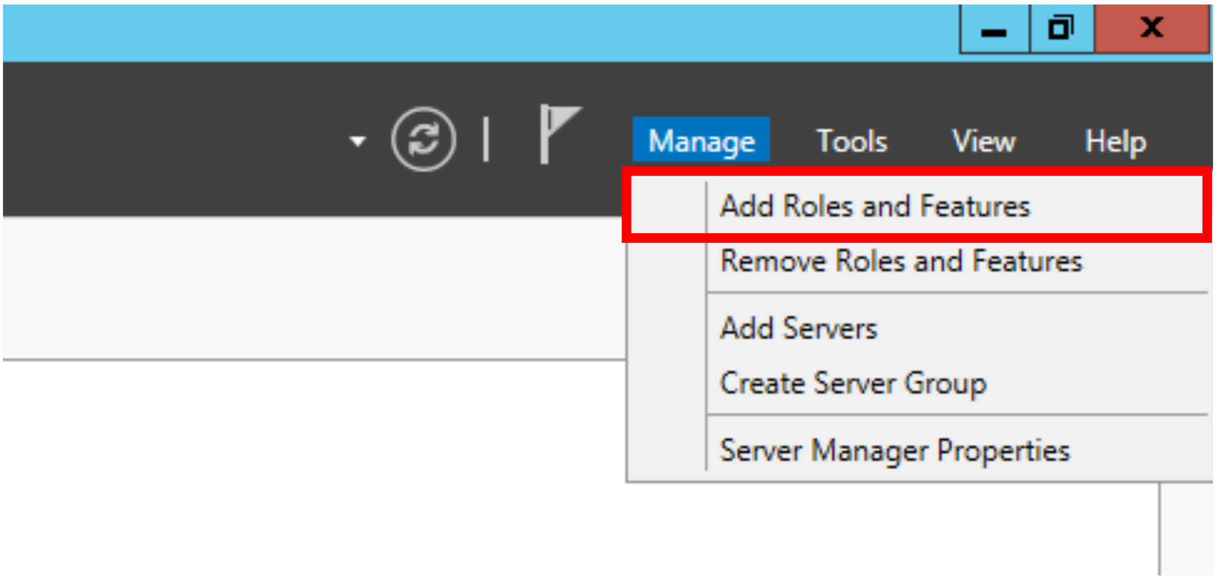
We have completed up to now HTTPS Inspection configuration. We will next take care of Check Point Identity Awareness software blade configuration, which actually means Check Point integration with Microsoft Windows Server.

Not only that we need and want HTTPS inspection configured, we want to have complete visibility into users' activity and not only IP addresses. After Identity Awareness configuration is complete, we will be able to see in Logs and Monitor section all logs as they relate to a specific user, and not just the IP address is using. Working in a large organisation, with hundreds, or even thousands of users wouldn't help in this case, when analysing logs.

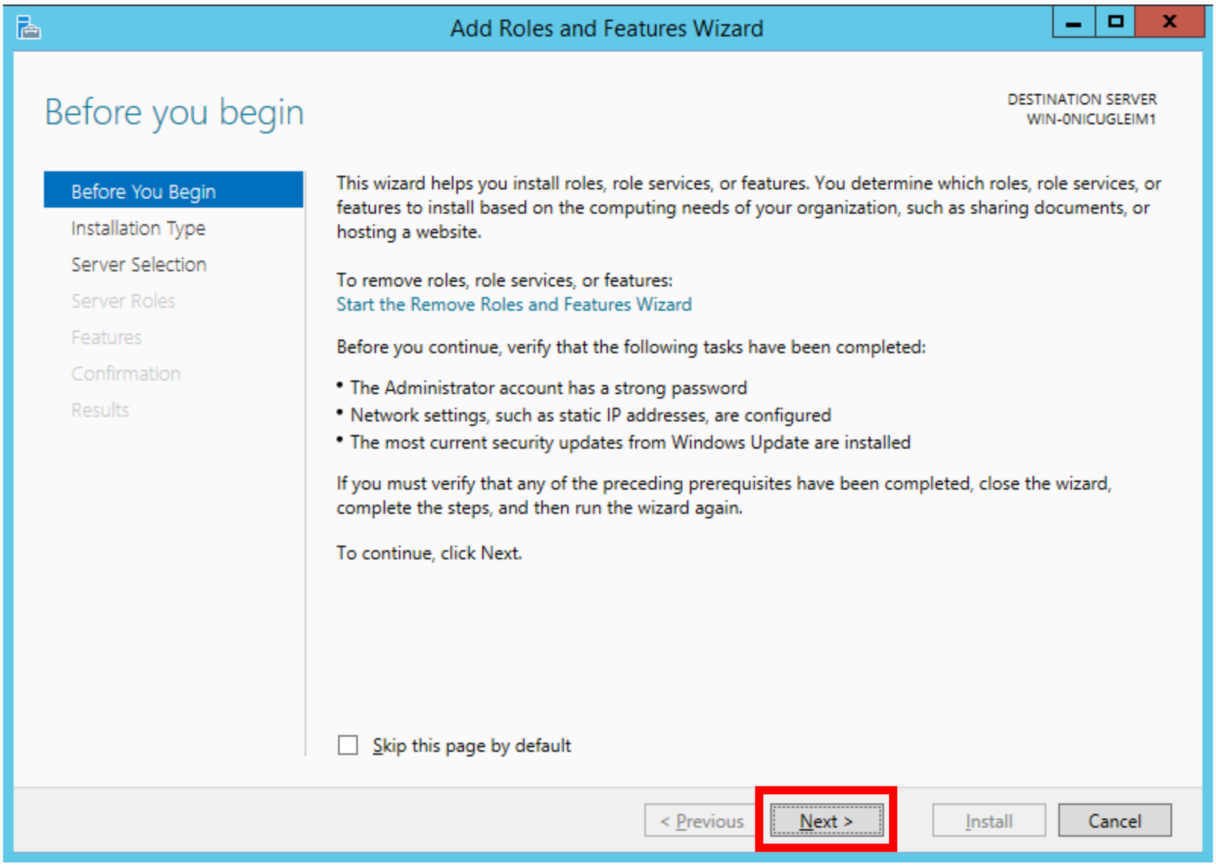
So now, we will start with Microsoft Windows Server 2012 configuration. We need to first add the Active Directory role on the machine. Here's how you can do that. Log into the machine and open **Server Manager**:



Now, in the top right corner, click on **Manage** and click on **Add Roles and Features**, as outlined below:



and continue with the wizard as you can see below. Click **Next** in order to begin the installation:



Before you begin

DESTINATION SERVER
WIN-0NICUGLEIM1

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

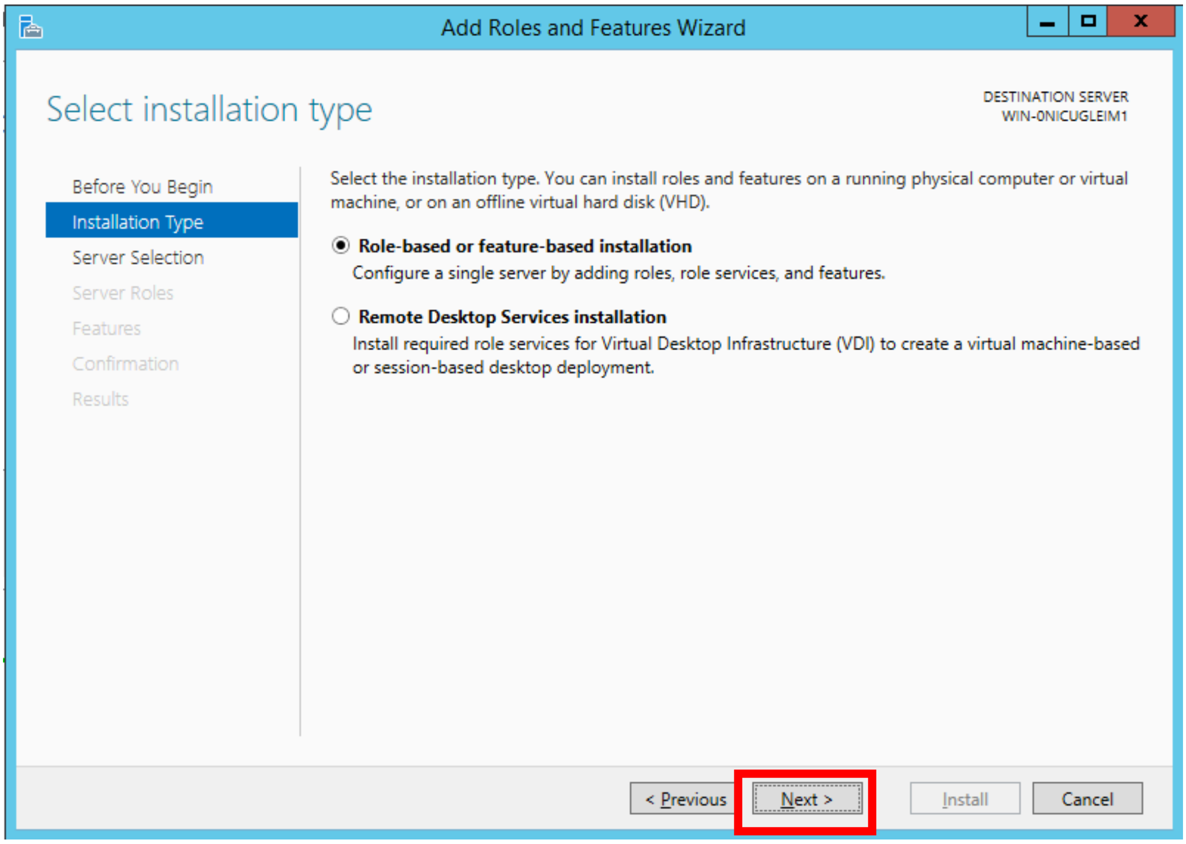
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

In the next step, the **Role-based** installation is what we need, so just click on **Next:**



Add Roles and Features Wizard

Select installation type

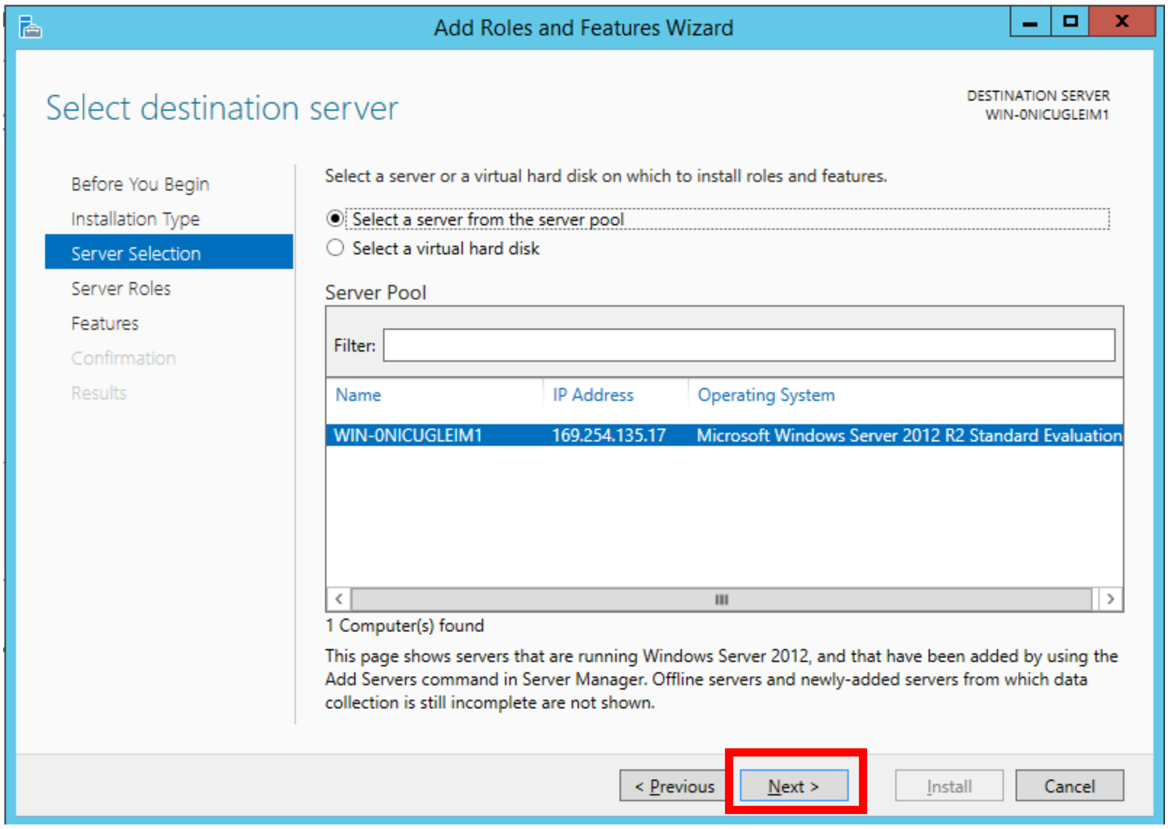
DESTINATION SERVER
WIN-0NICUGLEIM1

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

As we have only one server, we don’t need to select anything here, just click **Next**:



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-0NICUGLEIM1

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

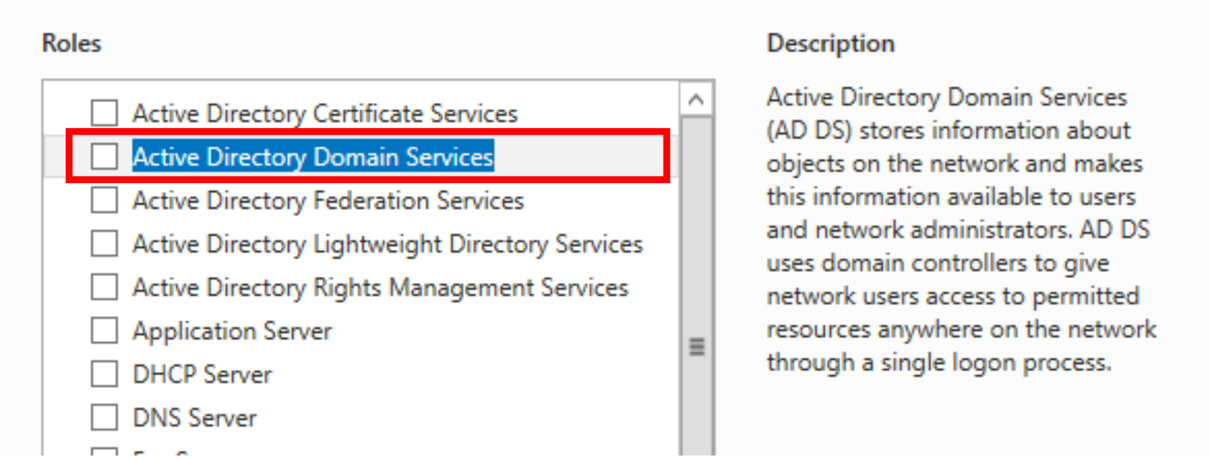
Filter:

Name	IP Address	Operating System
WIN-0NICUGLEIM1	169.254.135.17	Microsoft Windows Server 2012 R2 Standard Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Now we need to select the server role, so click on **Active Directory Domain Services** checkbox, at the beginning of the line:



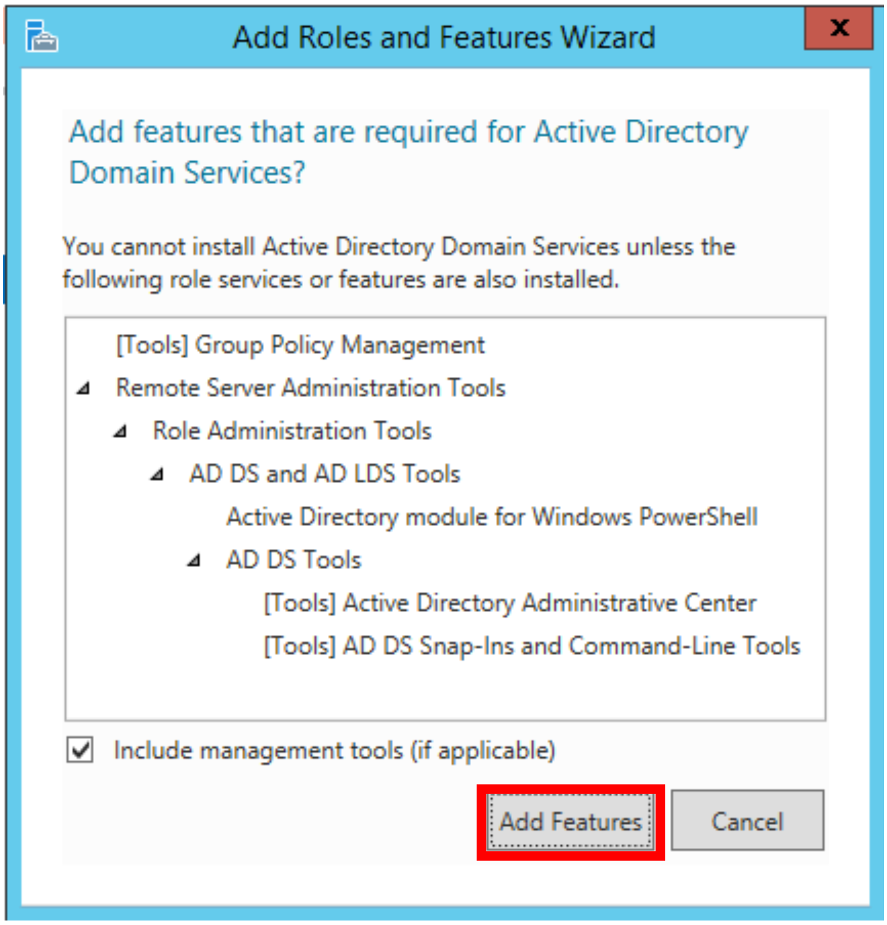
Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

and click on **Add Features**:



Add Roles and Features Wizard

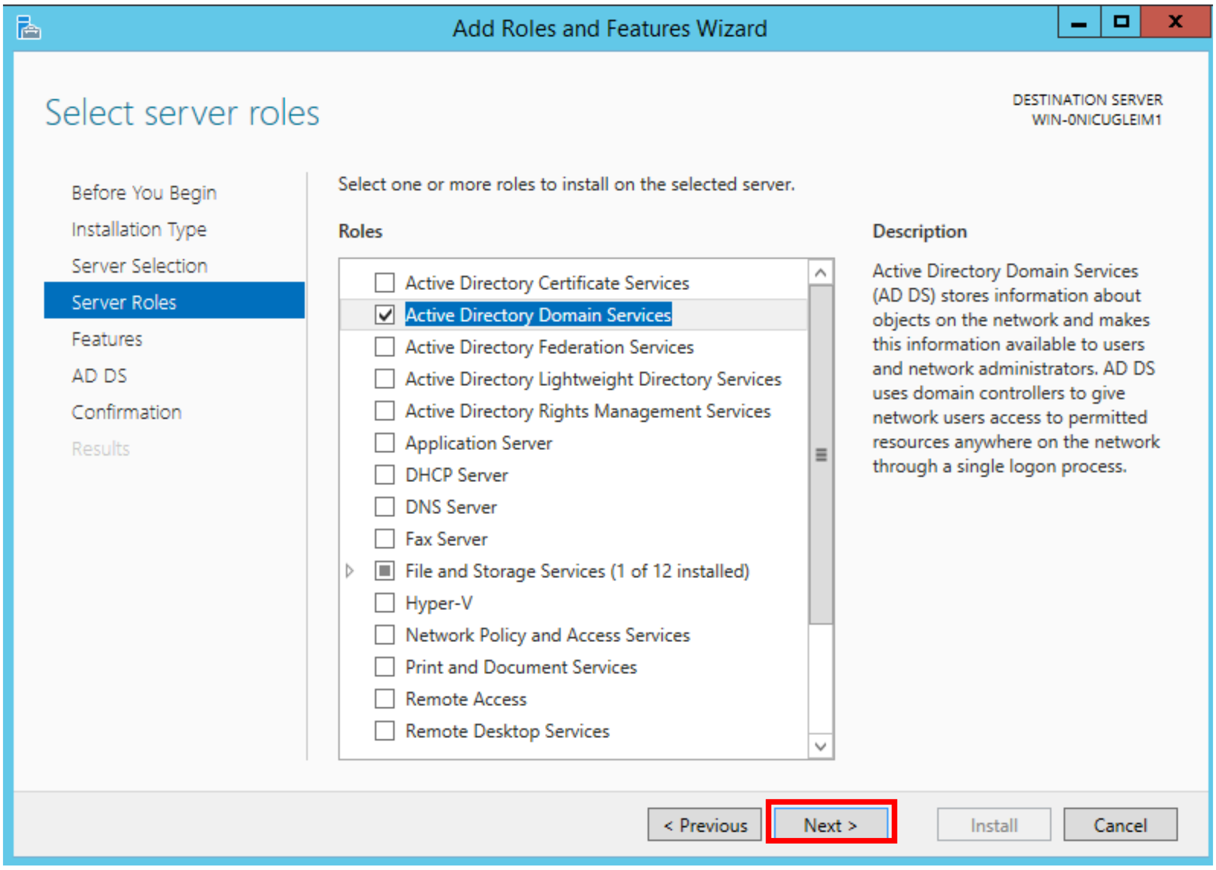
Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

```
[Tools] Group Policy Management
◢ Remote Server Administration Tools
    ◢ Role Administration Tools
        ◢ AD DS and AD LDS Tools
                Active Directory module for Windows PowerShell
            ◢ AD DS Tools
                    [Tools] Active Directory Administrative Center
                    [Tools] AD DS Snap-Ins and Command-Line Tools
```

☑ Include management tools (if applicable)

In order to continue, just click on **Next**:



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-0NICUGLEIM1

Select one or more roles to install on the selected server.

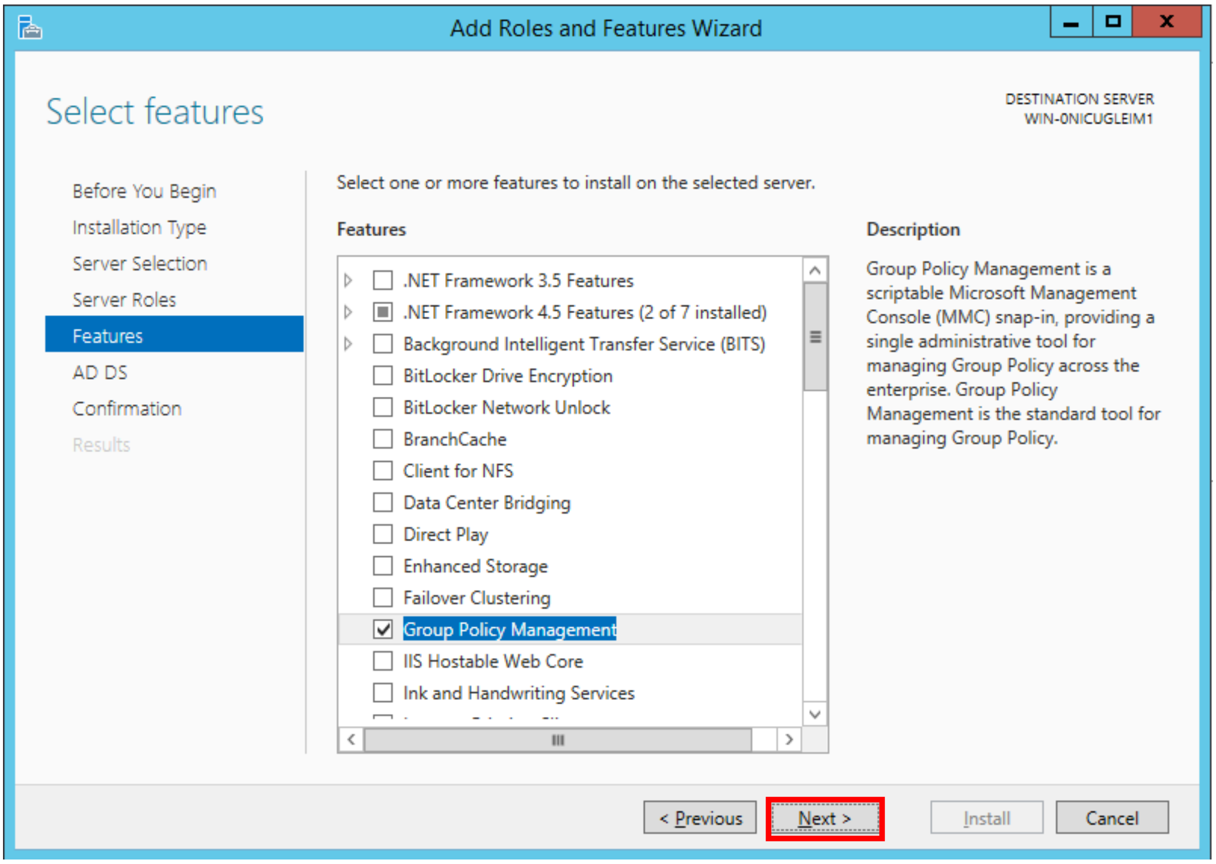
Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

For the **Features,** we leave everything as it is and just click **Next**:



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-0NICUGLEIM1

Select one or more features to install on the selected server.

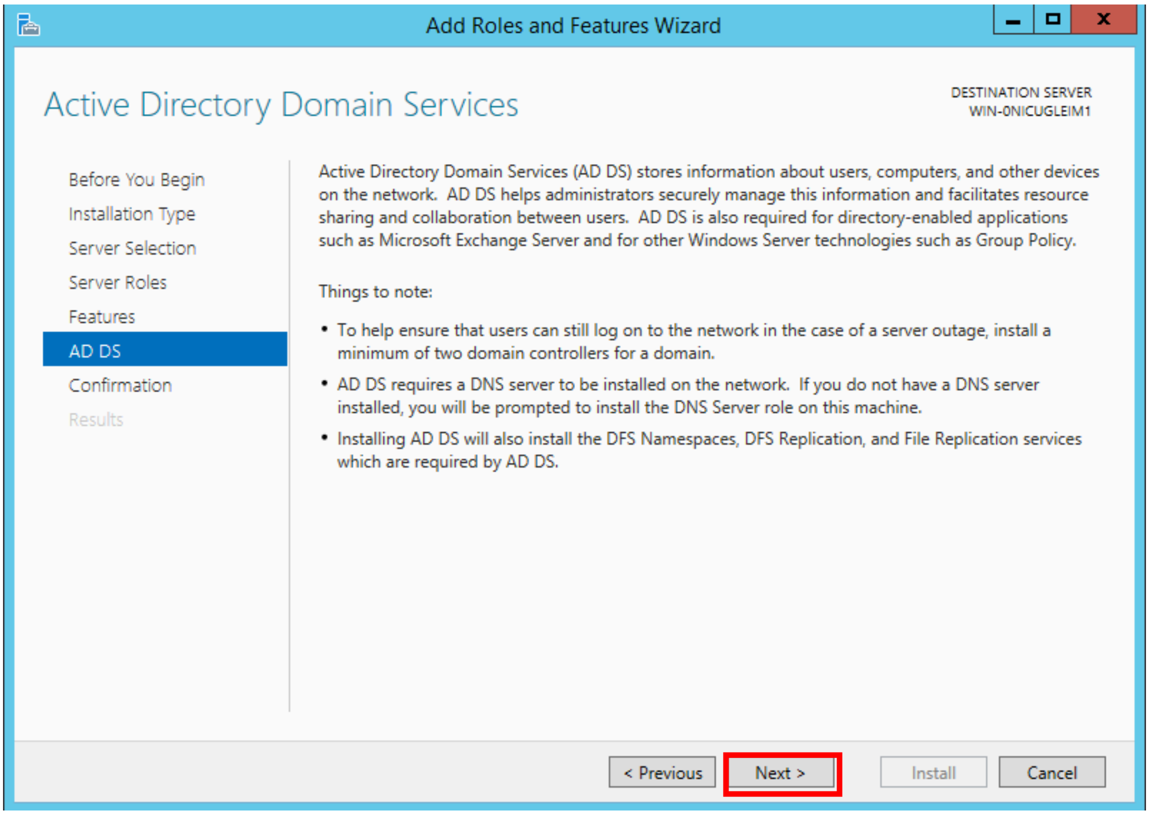
Features

- ☐ .NET Framework 3.5 Features
- ■ .NET Framework 4.5 Features (2 of 7 installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☑ Group Policy Management
- ☐ IIS Hostable Web Core
- ☐ Ink and Handwriting Services

Description

Group Policy Management is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing Group Policy across the enterprise. Group Policy Management is the standard tool for managing Group Policy.

And **Next** again:



Active Directory Domain Services

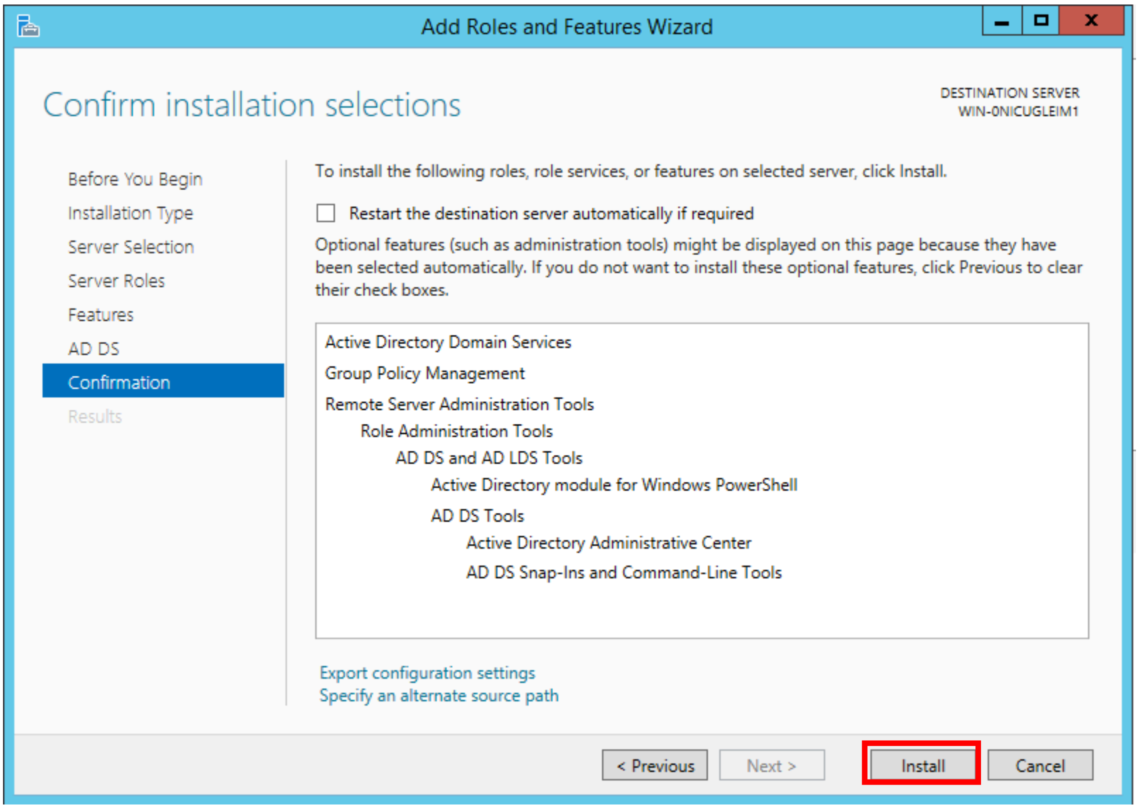
DESTINATION SERVER
WIN-0NICUGLEIM1

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
- Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS.

Last step, just click on **Install**



Confirm installation selections

DESTINATION SERVER
WIN-0NICUGLEIM1

To install the following roles, role services, or features on selected server, click Install.

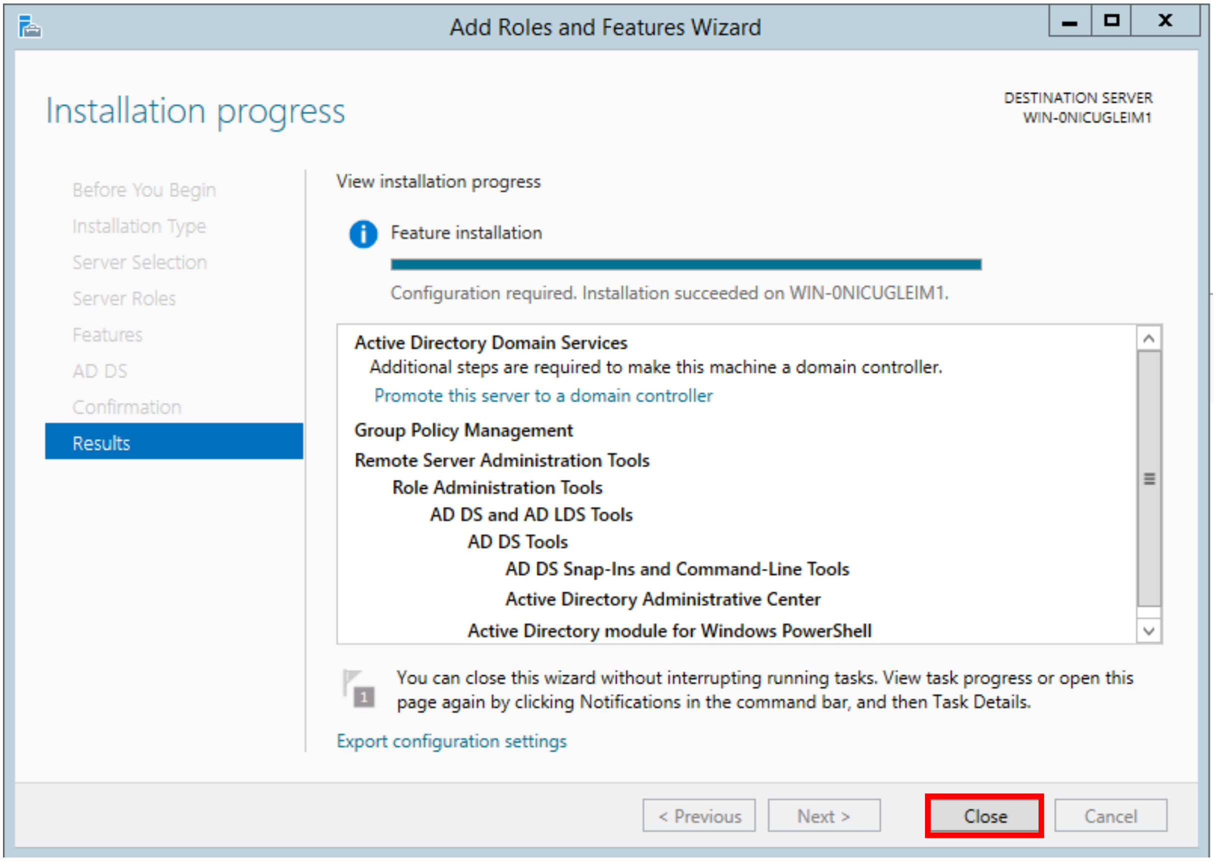
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - AD DS Tools
        - Active Directory Administrative Center
        - AD DS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path

In order to complete installation, please click on **Close**:



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-0NICUGLEIM1

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-0NICUGLEIM1.

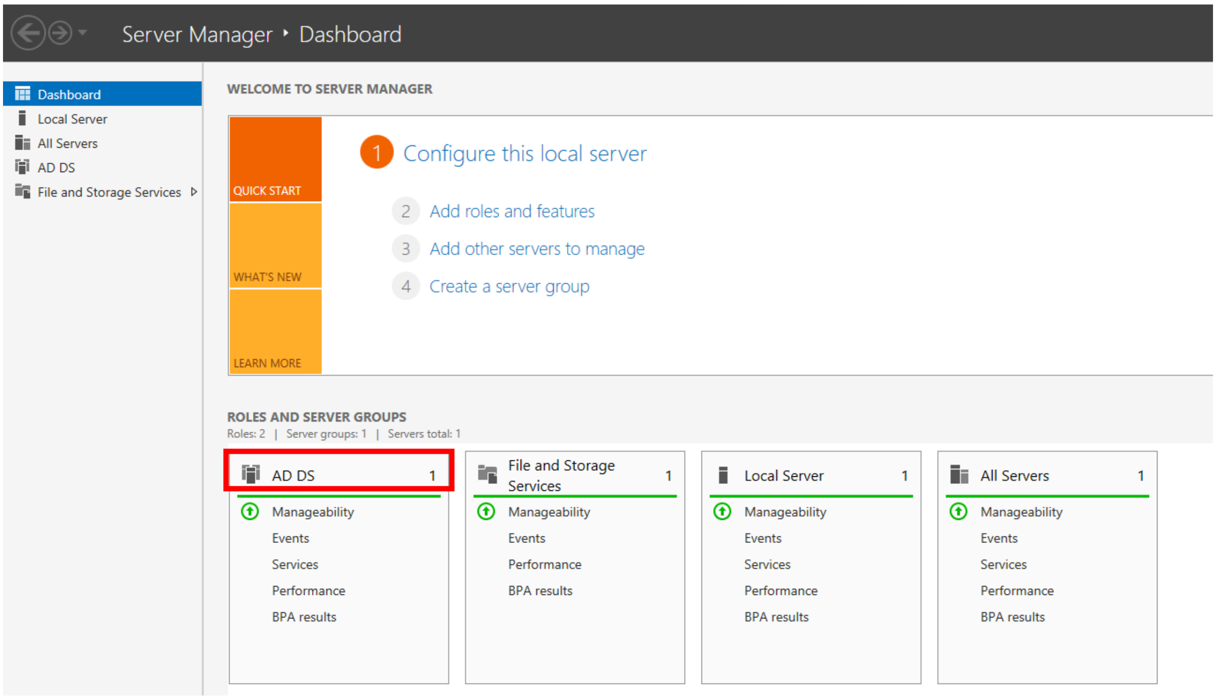
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller

Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
AD DS Tools
AD DS Snap-Ins and Command-Line Tools
Active Directory Administrative Center
Active Directory module for Windows PowerShell

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

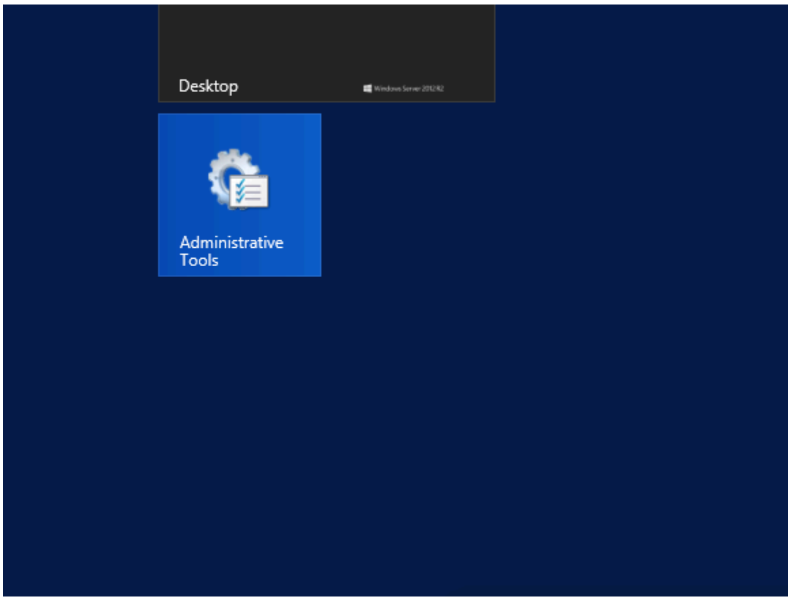
Export configuration settings

You should now have in your Server Manager Dashboard a new role present, the **AD DS – Active Directory Domain Services:**

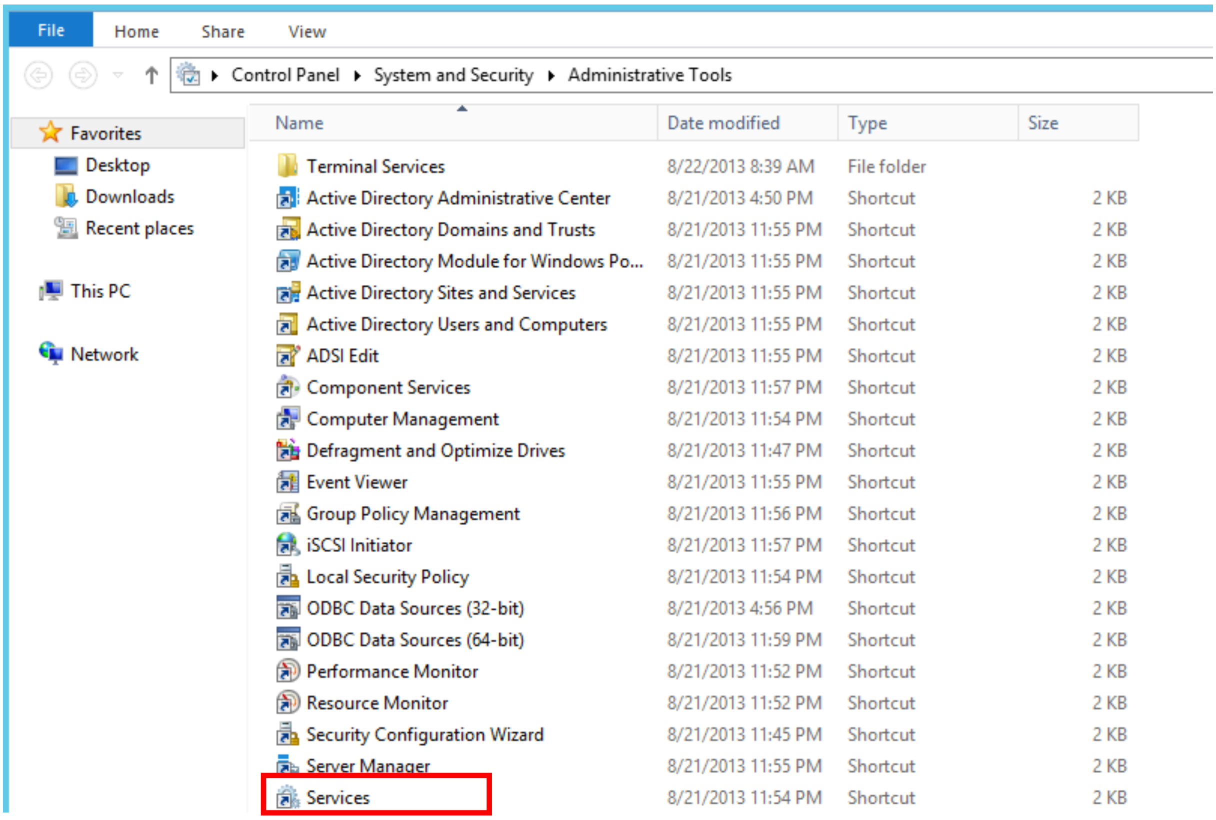


Before you can promote the server to domain controller, you must start the remote registry service by using the following steps.

Click on start in the left-down corner and click on **Administrative Tools.**



Next, open **Services:**



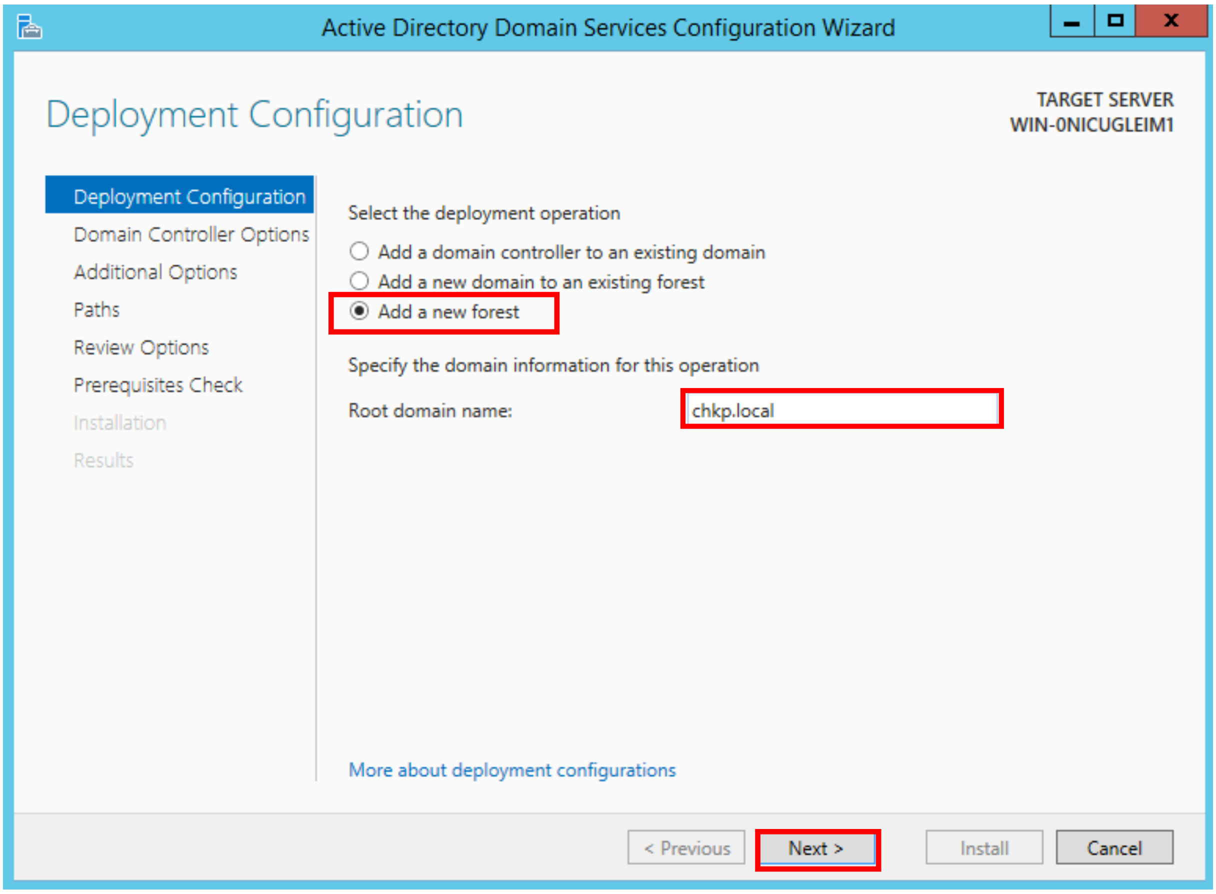
Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Active Directory Administrative Center	8/21/2013 4:50 PM	Shortcut	2 KB
Active Directory Domains and Trusts	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Module for Windows Po...	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Sites and Services	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Users and Computers	8/21/2013 11:55 PM	Shortcut	2 KB
ADSI Edit	8/21/2013 11:55 PM	Shortcut	2 KB
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
Group Policy Management	8/21/2013 11:56 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/21/2013 11:59 PM	Shortcut	2 KB
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Security Configuration Wizard	8/21/2013 11:45 PM	Shortcut	2 KB
Server Manager	8/21/2013 11:55 PM	Shortcut	2 KB
Services	8/21/2013 11:54 PM	Shortcut	2 KB

and search for **Remote Registry.** Right-click, select **Start** and you can close the **Services** window.

Now, let's continue with AD server configuration. In order to do this, in the top-right corner, click on the Notifications yellow flag and continue by clicking on **Promote this server to a domain controller.**

Now, we can start the **Deployment Configuration.**

Since this is our first server that we are deploying, we need to add a domain, and our domain is "**chkp.local". ** Select **Add a new forest,**complete **chkp.local** in the Root domain name and click **Next**:



Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

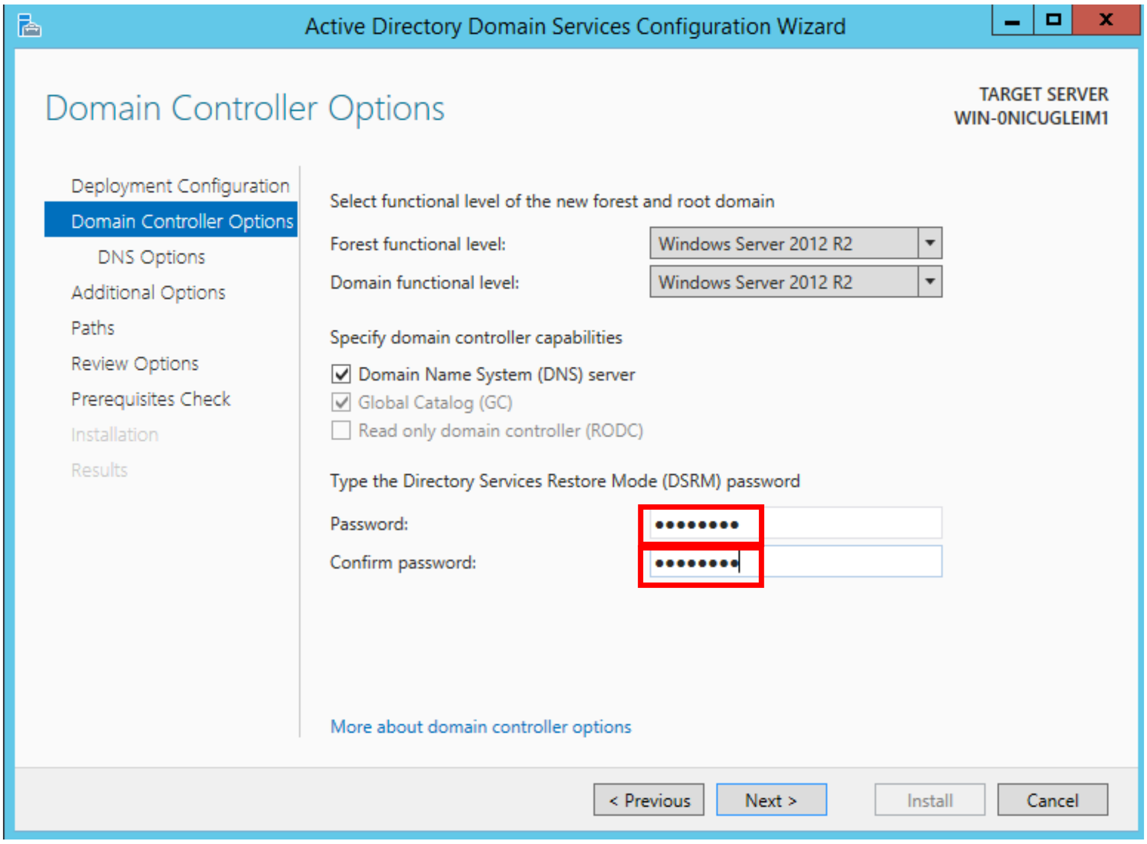
Specify the domain information for this operation

Root domain name: chkp.local

Enter password for DSRM. I will use **Admin123**, don't forget to confirm password as well.

Leave the other options as they are, no modifications needed.

Click **Next.**



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-0NICUGLEIM1

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

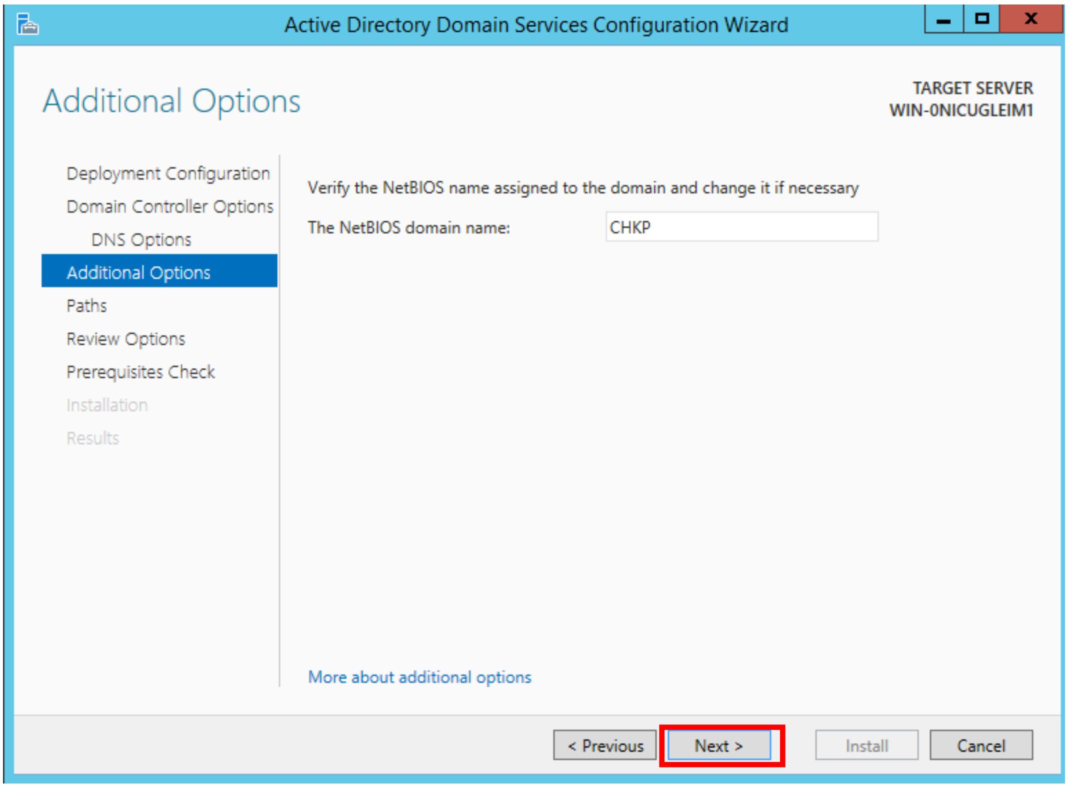
Type the Directory Services Restore Mode (DSRM) password

Password: ••••••••

Confirm password: ••••••••

Click **Next** again, never mind for now the DNS error.

Another two **Next** clicks, as you can see below:



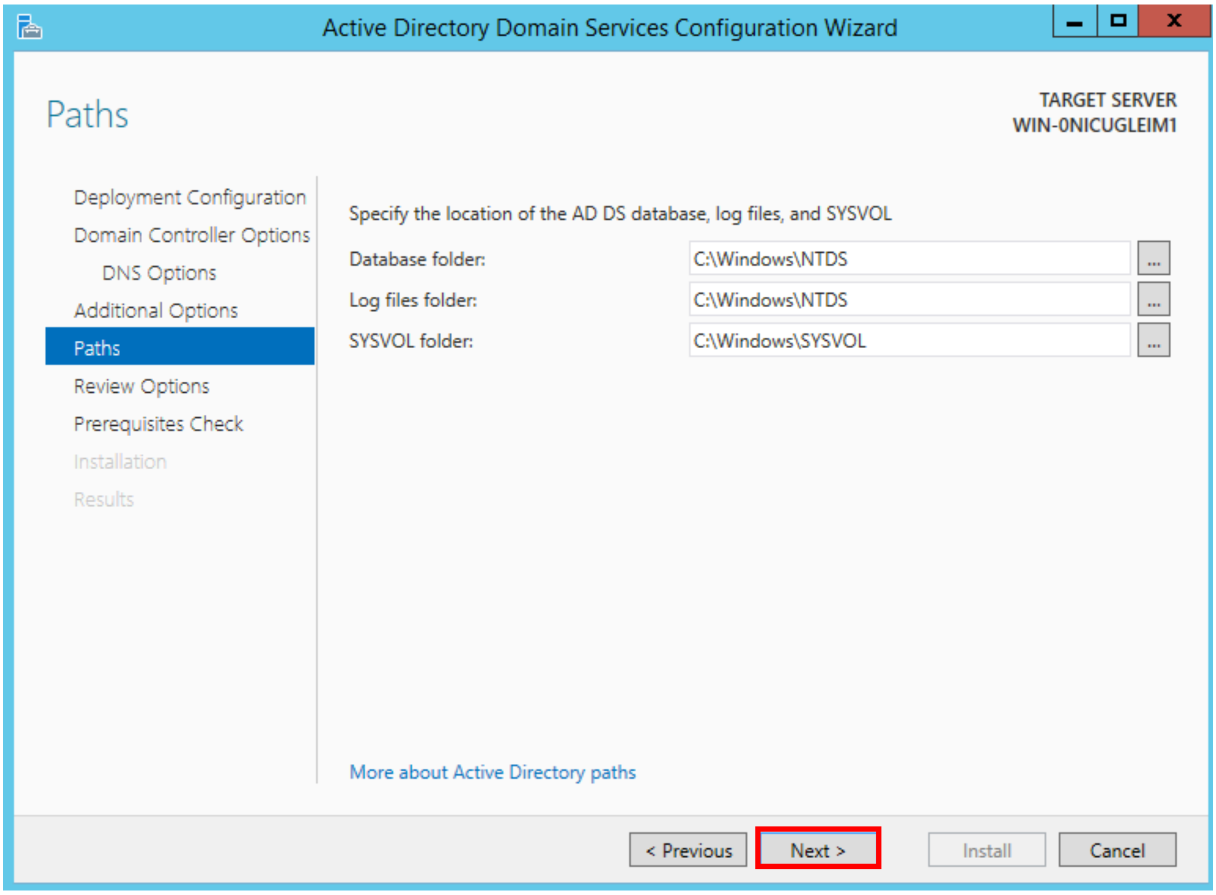
Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER
WIN-0NICUGLEIM1

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: CHKP



Active Directory Domain Services Configuration Wizard

Paths

TARGET SERVER
WIN-0NICUGLEIM1

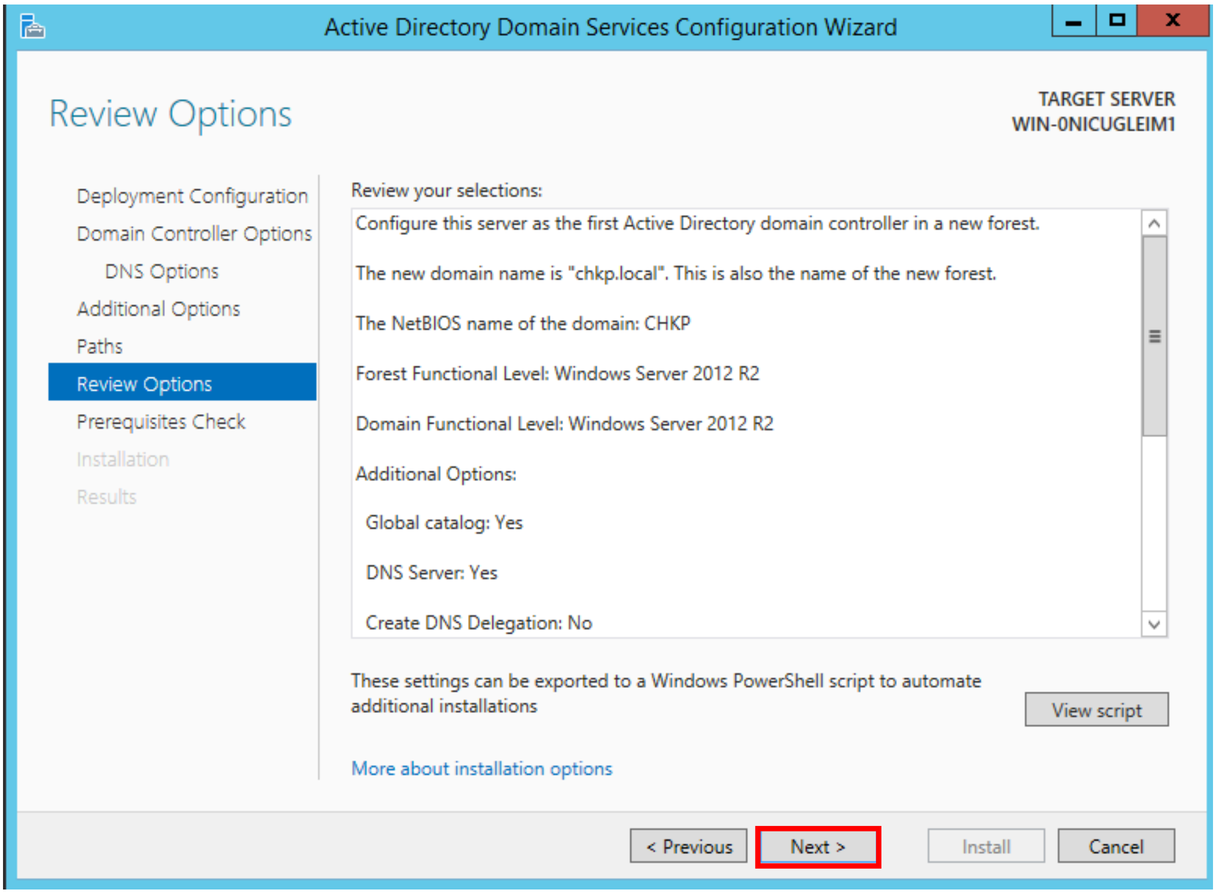
Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

More about Active Directory paths



Active Directory Domain Services Configuration Wizard

Review Options

TARGET SERVER
WIN-0NICUGLEIM1

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "chkp.local". This is also the name of the new forest.

The NetBIOS name of the domain: CHKP

Forest Functional Level: Windows Server 2012 R2

Domain Functional Level: Windows Server 2012 R2

Additional Options:

Global catalog: Yes

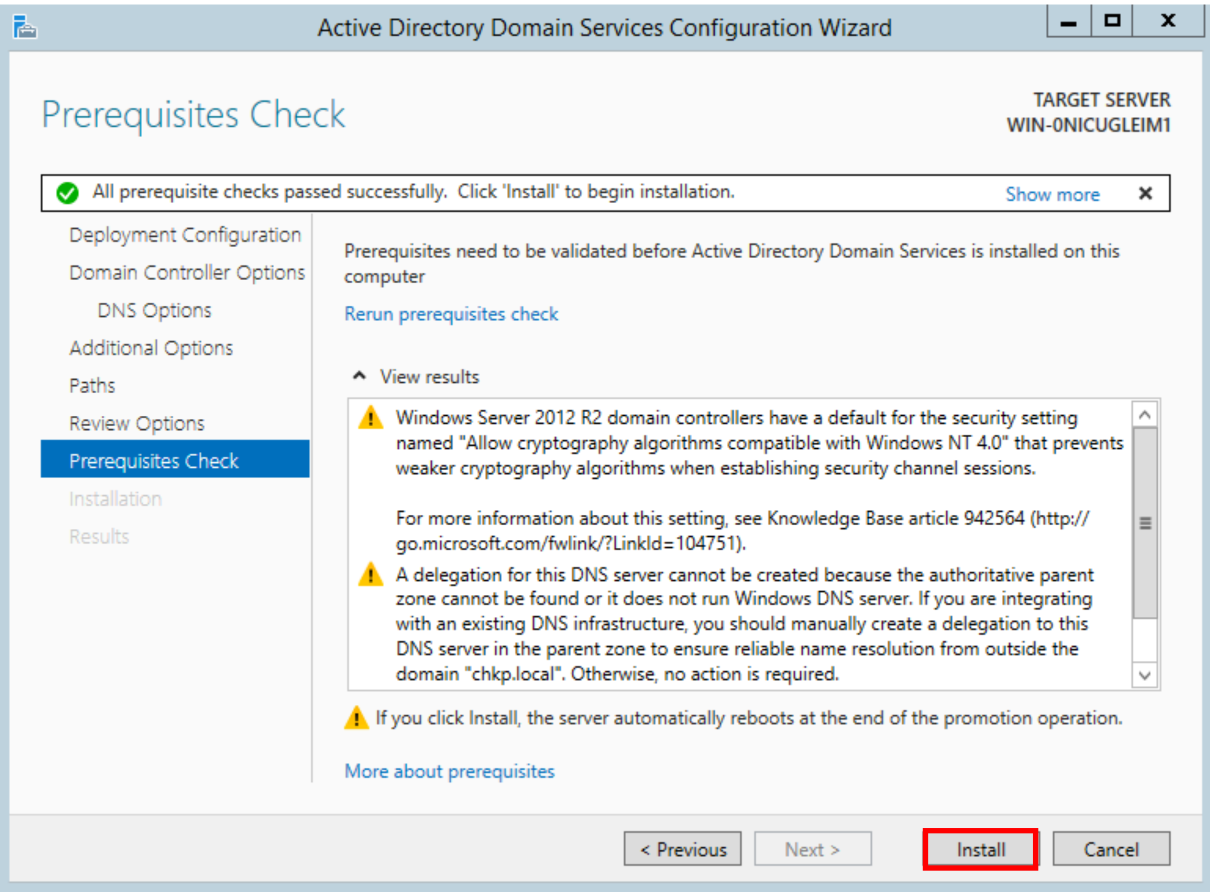
DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

More about installation options

After Prerequisites Check is complete, please click **Install** in order to begin installation:



Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
WIN-0NICUGLEIM1

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more ✕

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Rerun prerequisites check

View results

⚠ Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

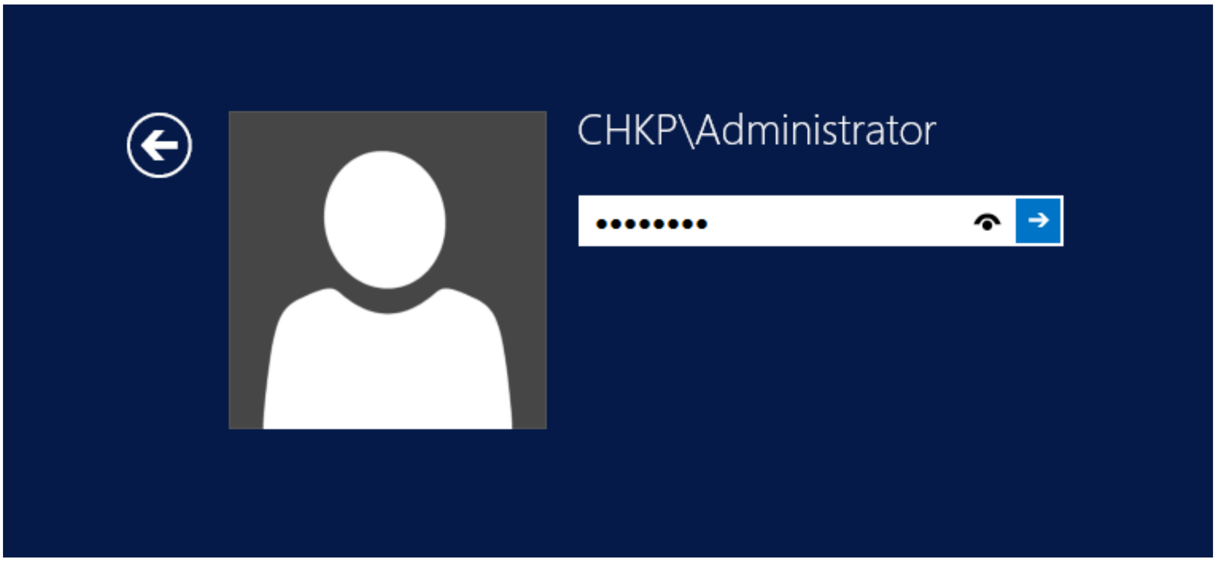
⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "chkp.local". Otherwise, no action is required.

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

More about prerequisites

When the installation is complete, the NY-AD server will reboot.

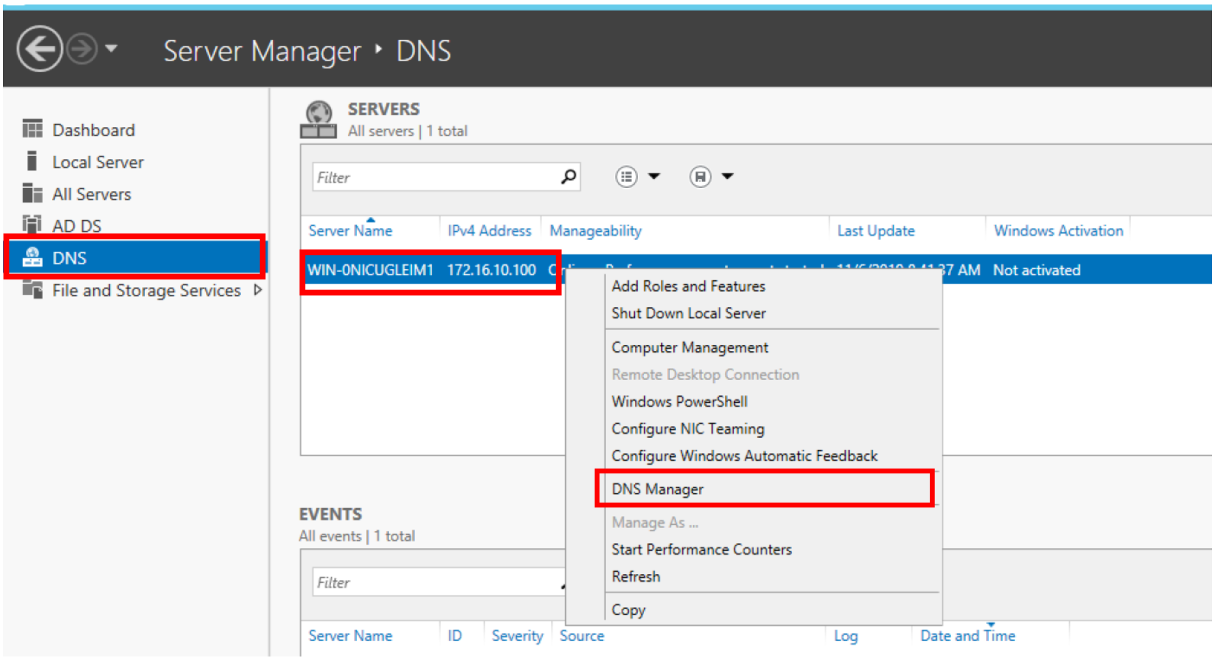
Now, when you will login again, you will see the change, presenting the domain (CHKP), before the Administrator login:



CHKP\Administrator

Next, we need to verify that the AD server also acts as the DNS server for **chkp.local** domain. Let's see how we can do this.

While in your **Server Manager Dashboard,** click on DNS in order to select it, then right-click on the server and select **DNS Manager**:

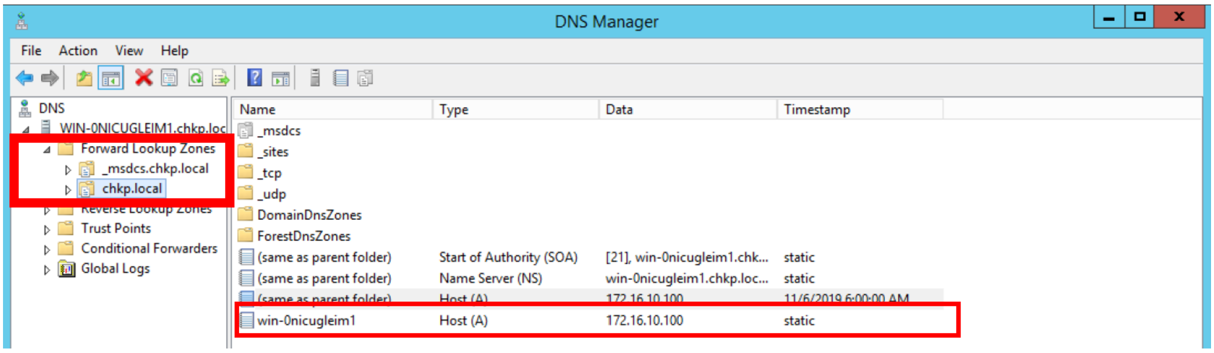


Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-0NICUGLEIM1	172.16.10.100	O	7 AM	Not activated

Server Name	ID	Severity	Source	Log	Date and Time

While we did the configuration for AD, DNS server also completed, remember there was a step where we ignored DNS warning.

We can see that we have a **Forward Lookup Zone – chkp.local** and on the right-side menu we can see that there is a static mapping between chkp.local and the IP address of the DNS Server – 172.16.10.100.

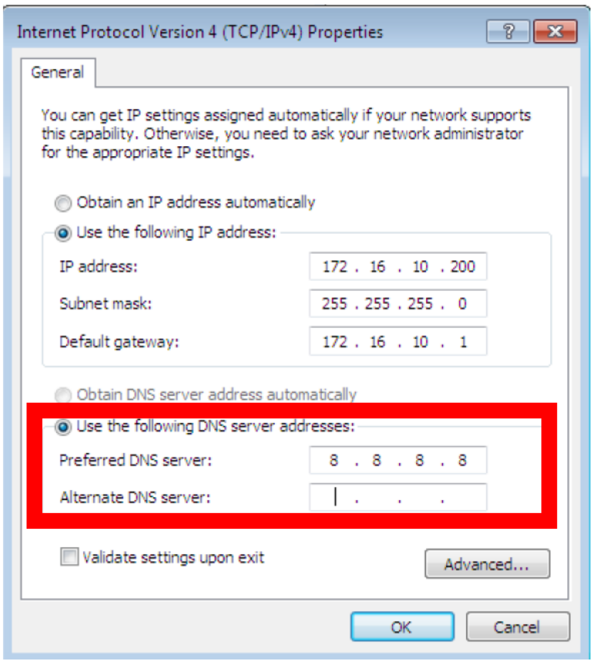


Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[21], win-0nicugleim1.chk...	static
(same as parent folder)	Name Server (NS)	win-0nicugleim1.chkp.loc...	static
(same as parent folder)	Host (A)	172.16.10.100	11/6/2019 6:00:00 AM
win-0nicugleim1	Host (A)	172.16.10.100	static

Good! The next thing that we need to do is create a user on the AD server and then enrol the NY-LAN-1 PC into the newly created domain. Before that, let's test our new DNS server and make sure things work as expected.

While in NY-LAN-1 PC, open **Command Prompt** (Start -> Command Prompt).

Our current IPv4 settings on the NY-LAN-PC are the following, with Google DNS server set 8.8.8.8 (left snapshot). We will change the DNS server on the machine to point to our DNS (and AD) server, with first option to local server and for anything that can not be resolved locally, to ask Google DNS – 8.8.8.8.



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.

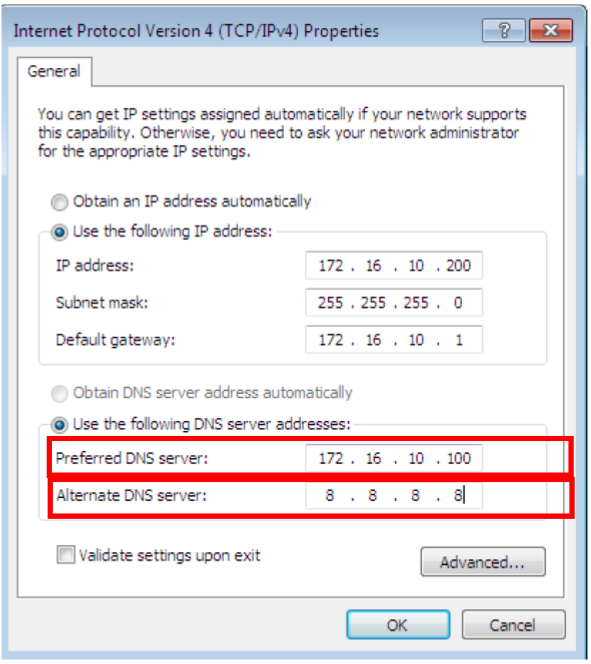
○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 16 . 10 . 200
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 16 . 10 . 1

○ 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



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: 172 . 16 . 10 . 200
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 16 . 10 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 172 . 16 . 10 . 100
Alternate DNS server: 8 . 8 . 8 . 8

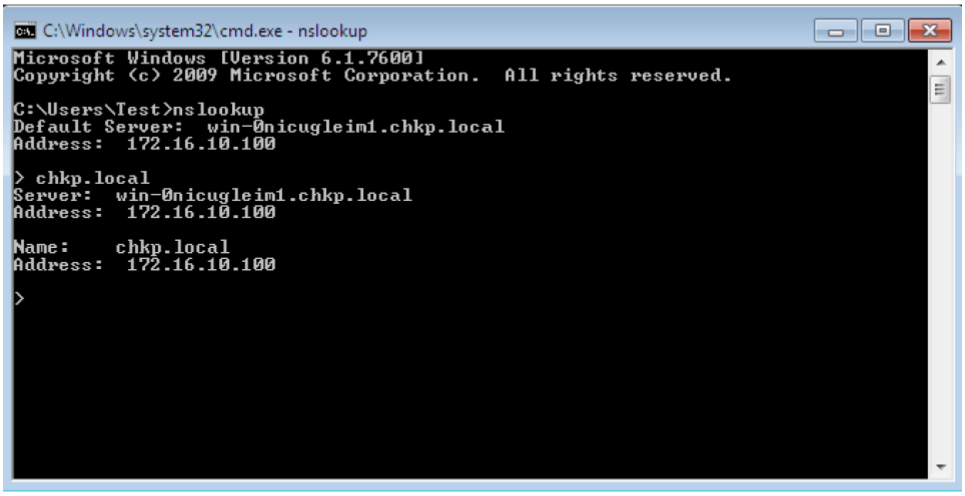
□ Validate settings upon exit

When done, just click **OK** in order to confirm the configuration change.

Now let’s see how we test the DNS server configuration. As a next step, we will enrol the PC in the domain and for this to happen, the DNS server needs to be able to respond to DNS queries about who is **chkp.local**, what is the corresponding IP address. Indeed, the answer is itself, so let’s test this.

While in Command Prompt, type the **nslookup** command. The default server in my case is presented along with the IP address – 172.16.10.100. If you don’t see anything here, then it means that you don’t have Reverse Lookup Zone configured. No worries, it’s not needed at this moment and is out of the scope of this course.

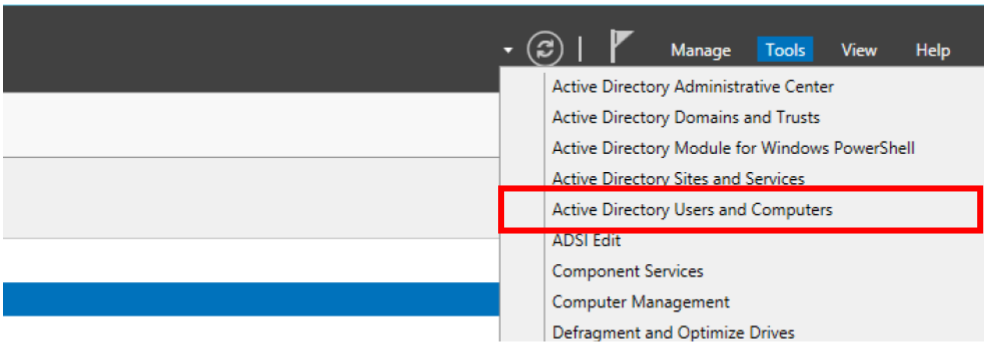
Next, you type **chkp.local** command, basically asking the DNS server, what is the corresponding IP address to this domain address. The response is self-explanatory, the server itself is the one responding to DNS queries sent to this domain name and you are also presented the IP address.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Test>nslookup
Default Server:  win-0nicugleim1.chkp.local
Address:  172.16.10.100

> chkp.local
Server:  win-0nicugleim1.chkp.local
Address:  172.16.10.100

Name:    chkp.local
Address:  172.16.10.100

>
```

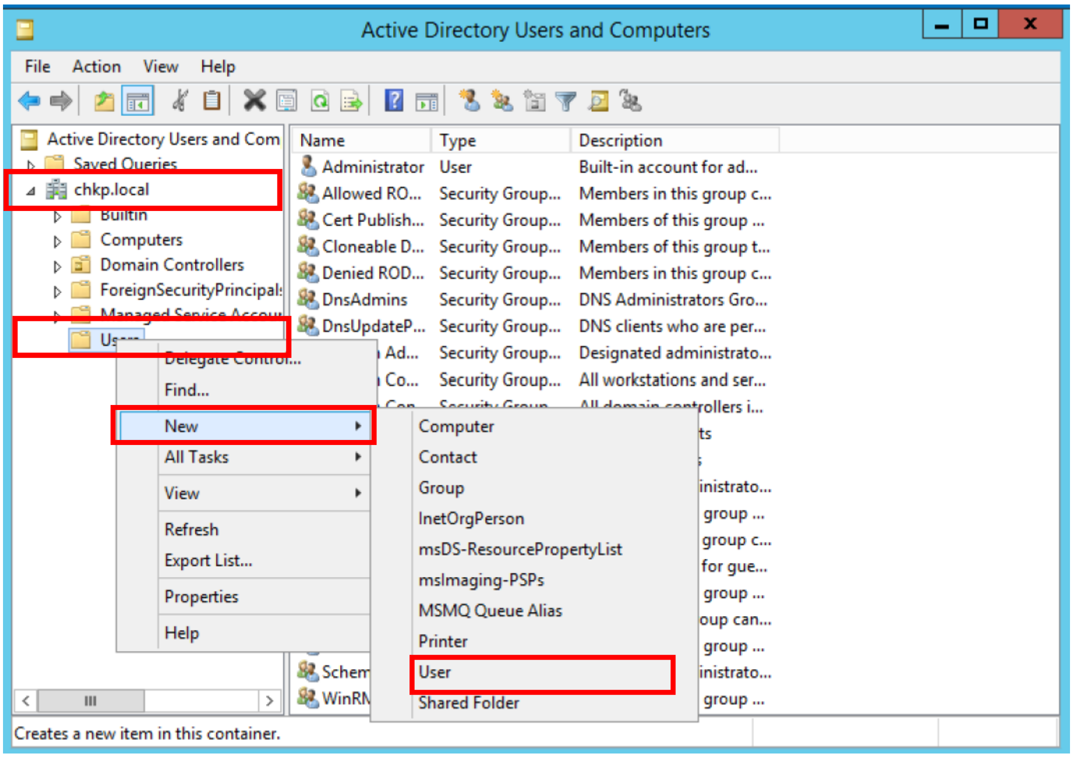
Great, so the DNS server is working as expected. Last thing to do is to create a user in the chkp.local domain, user that will be used by the NY-LAN-PC. So, let’s do this next.

In the Server Dashboard, in the top-right corner click on **Tools** and then click on **Active Directory Users and Computers**.

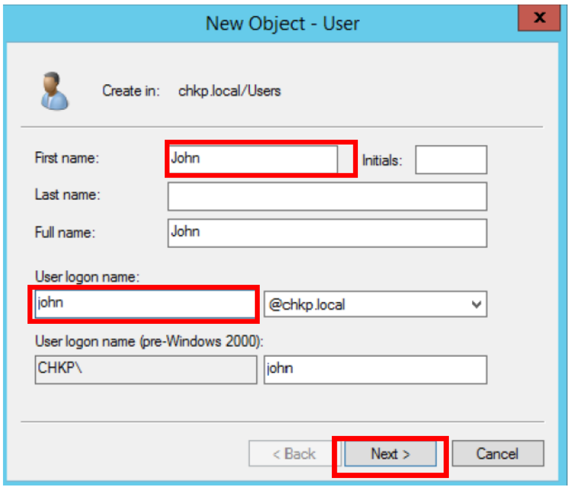


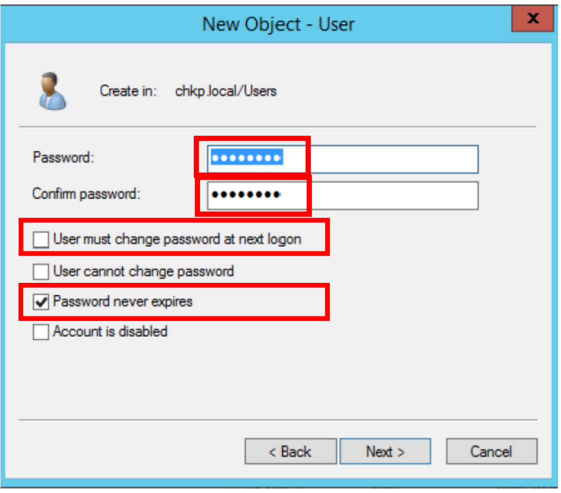
Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives

Extend the domain **chkp.local** , right-click on **Users,** then go to **New** and then to **User.**


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
chkp.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accou
Users
Delegate Control...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ResourcePropertyList
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder
Name
Type
Description
Administrator User Built-in account for ad...
Allowed RO... Security Group... Members in this group c...
Cert Publish... Security Group... Members of this group ...
Cloneable D... Security Group... Members of this group t...
Denied ROD... Security Group... Members in this group c...
DnsAdmins Security Group... DNS Administrators Gro...
DnsUpdateP... Security Group... DNS clients who are per...
Creates a new item in this container.

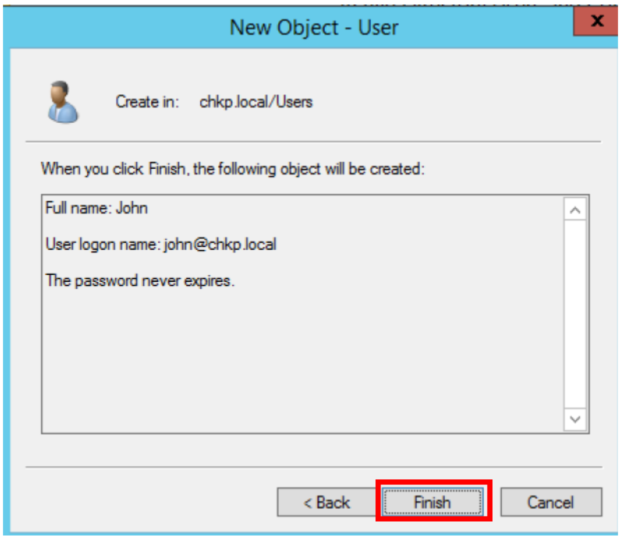
Enter first name as **John** and also enter logon name as **john**, as highlighted below. When done, click **Next** in order to continue (left screenshot):




New Object - User
Create in: chkp.local/Users
Password: ••••••••
Confirm password: ••••••••
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Account is disabled
< Back
Next >
Cancel

Now, define a password for the user, I will be using **Admin123** and confirm the password **Admin123.** Also, make sure that the password never expires, and that user will not have to change password when first logging in (right screenshot, above).

When done, just **Finish** in order to complete the user setup.



New Object - User

Create in: chkp.local/Users

When you click Finish, the following object will be created:

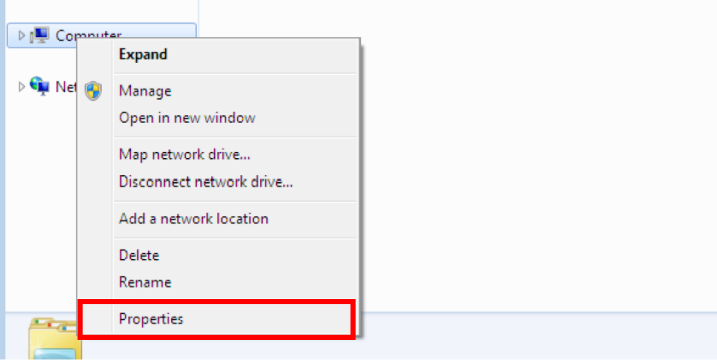
Full name: John

User logon name: john@chkp.local

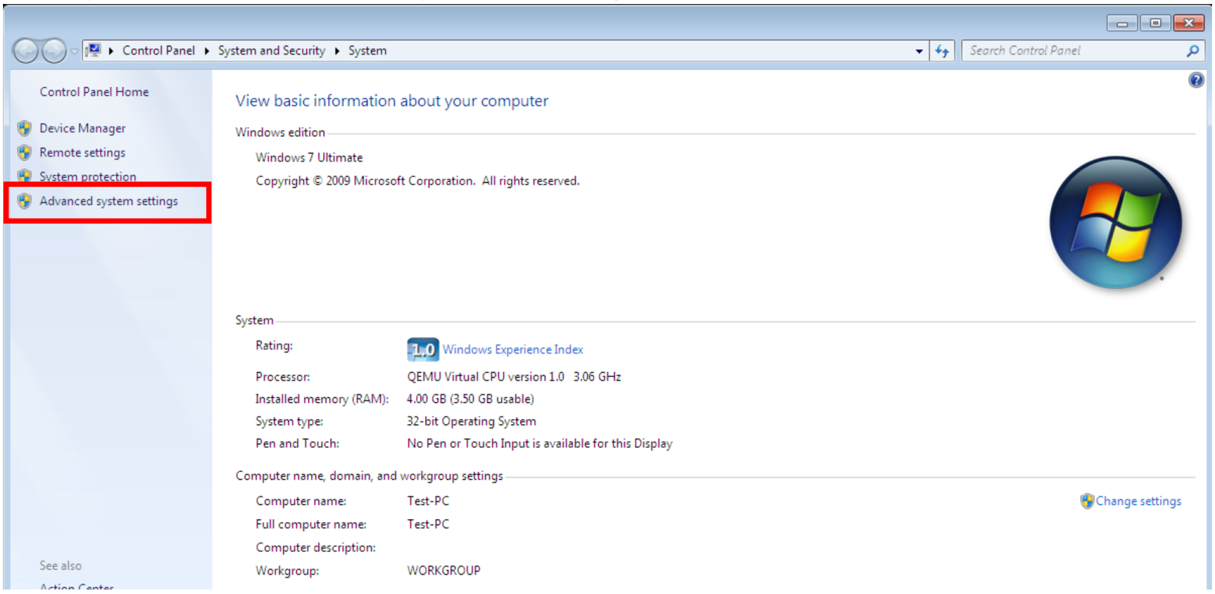
The password never expires.

Now, let’s switch to NY-LAN-PC and enrol the PC in the new domain chkp.local.

Open windows explorer (windows key + E) and right click on your computer, select **Properties.**



Finally, click on **Advanced system settings.**



View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

System

Rating: 1.0 Windows Experience Index

Processor: QEMU Virtual CPU version 1.0 3.06 GHz

Installed memory (RAM): 4.00 GB (3.50 GB usable)

System type: 32-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

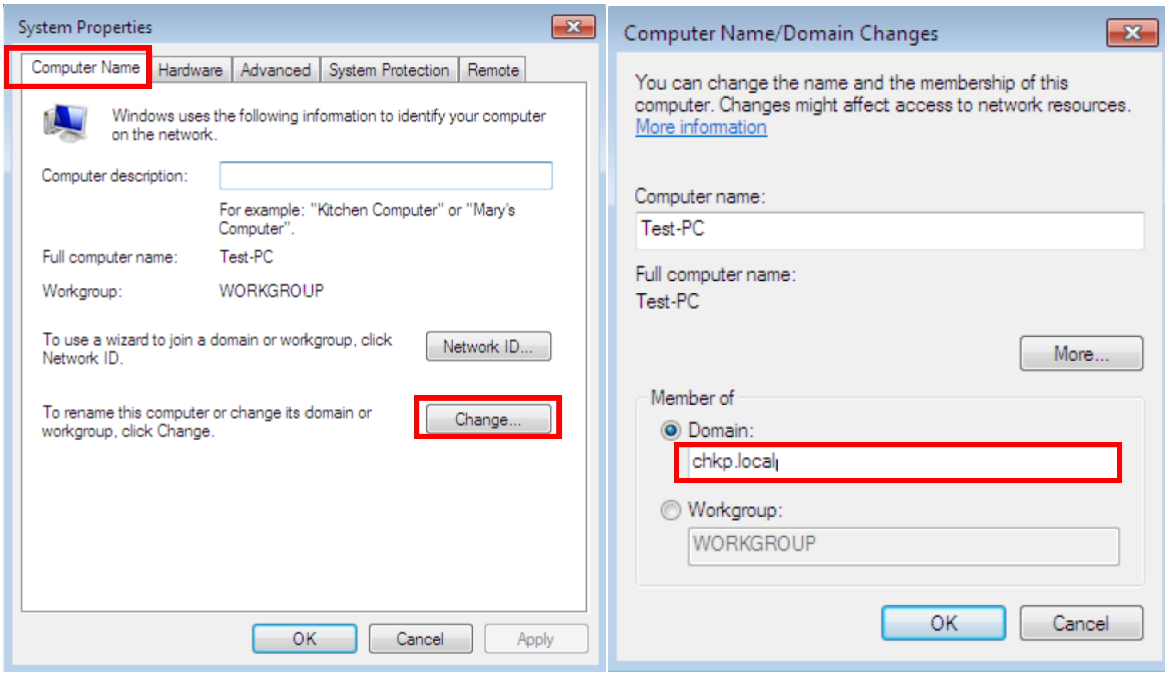
Computer name: Test-PC

Full computer name: Test-PC

Computer description:

Workgroup: WORKGROUP

At the top, navigate to **Computer Name** and click on **Change.**



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Test-PC

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: Test-PC

Full computer name: Test-PC

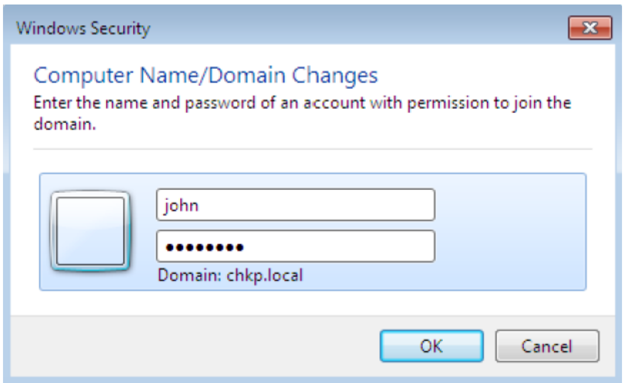
Member of

● Domain: chkp.local

○ Workgroup: WORKGROUP

Click on **Domain** and enter the domain name **chkp.local.**

Now you need to enter the credentials of the user, that we have just created a moment ago. Username **john** and password **Admin123.**



Computer Name/Domain Changes

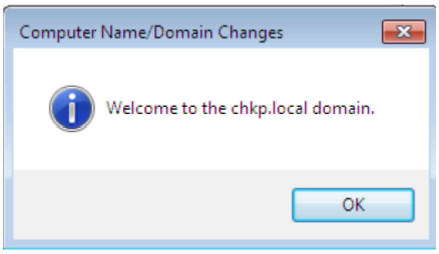
Enter the name and password of an account with permission to join the domain.

john

••••••••

Domain: chkp.local

Click **OK** and you should receive a Welcome message:

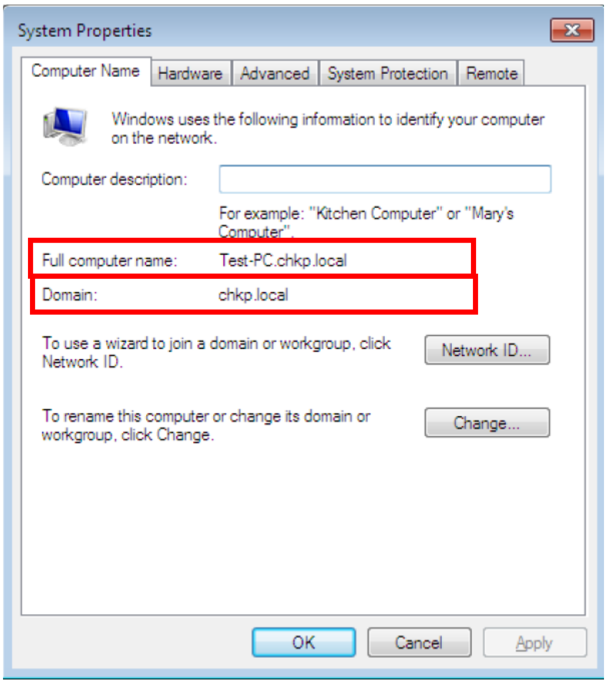


Welcome to the chkp.local domain.

You will be asked to restart the NY-LAN-PC and now you will login with the user credentials for the Domain (john / Admin123).

Most probably you will need to select **Switch User** (after ctrl+alt+delete) and enter the above credentials.

If we now navigate again to System Properties -> Computer Name, we will see that the NY-LAN-PC is part of the domain now.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Test-PC.chkp.local

Domain: chkp.local

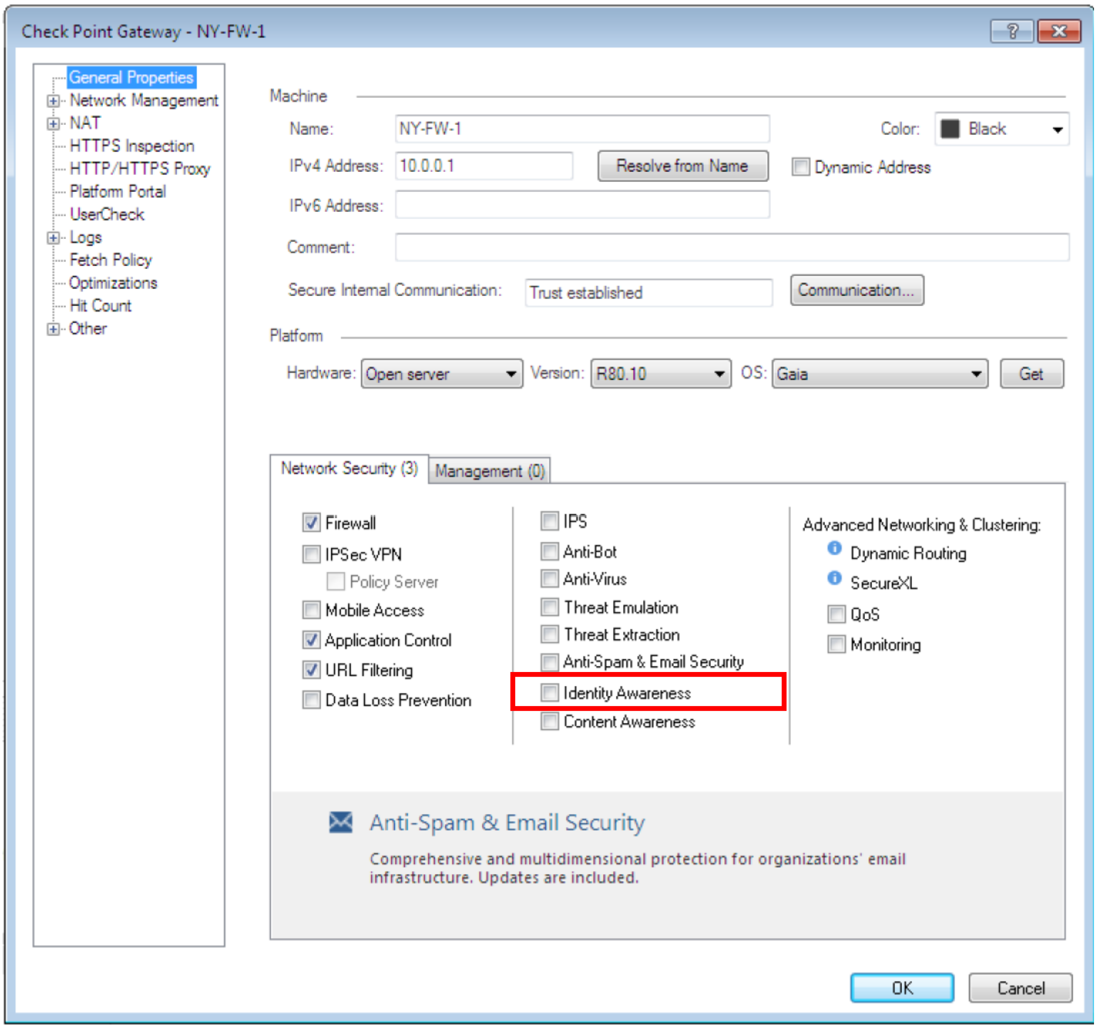
To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

So now, last step is to configure the integration between Check Point and Microsoft Active Directory.

We would need to enable **Identity Awareness** software blade on NY-FW-1, so for this I will go to **Gateway and Servers** and open the **NY-FW-1** object.

In order to start the wizard, just click **Identity Awareness** software blade.



Check Point Gateway - NY-FW-1

Machine

Name: NY-FW-1

Color: Black

IPv4 Address: 10.0.0.1

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server

Version: R80.10

OS: Gaia

☑ Firewall
□ IPSec VPN
□ Policy Server
□ Mobile Access
☑ Application Control
☑ URL Filtering
□ Data Loss Prevention

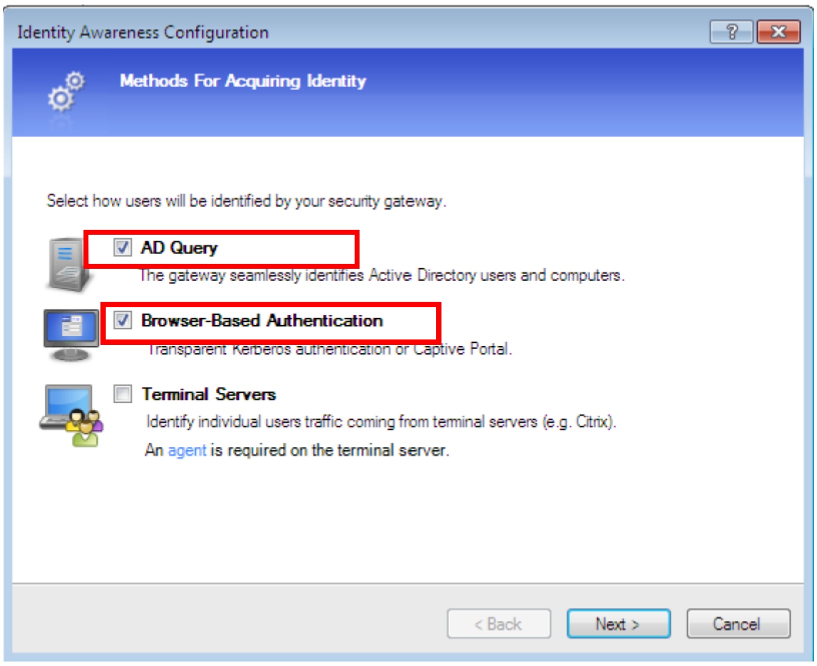
□ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
□ Identity Awareness
□ Content Awareness

Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
□ Monitoring

Anti-Spam & Email Security

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

Enable the first two options and click **Next**:



Identity Awareness Configuration

Methods For Acquiring Identity

Select how users will be identified by your security gateway.

☑ AD Query
The gateway seamlessly identifies Active Directory users and computers.

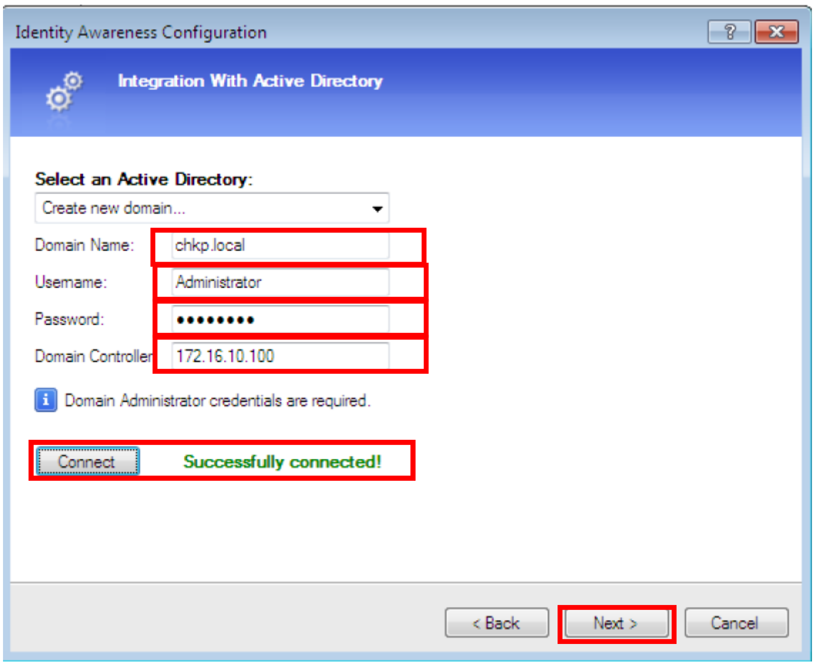
☑ Browser-Based Authentication
Transparent Kerberos authentication or Captive Portal.

□ Terminal Servers
Identify individual users traffic coming from terminal servers (e.g. Citrix).
An agent is required on the terminal server.

Now, fill in the Domain Name – **chkp.local**, username – **Administrator** and Password – **Admin123** and last the IP address of the AD server – 172.16.10.100.

Please note that we are using the Administrator credentials of the AD server.

When done, click **Connect** in order to test connectivity to AD server, after that click **Next** in order to continue:



Identity Awareness Configuration

Integration With Active Directory

Select an Active Directory: Create new domain...

Domain Name: chkp.local

Username: Administrator

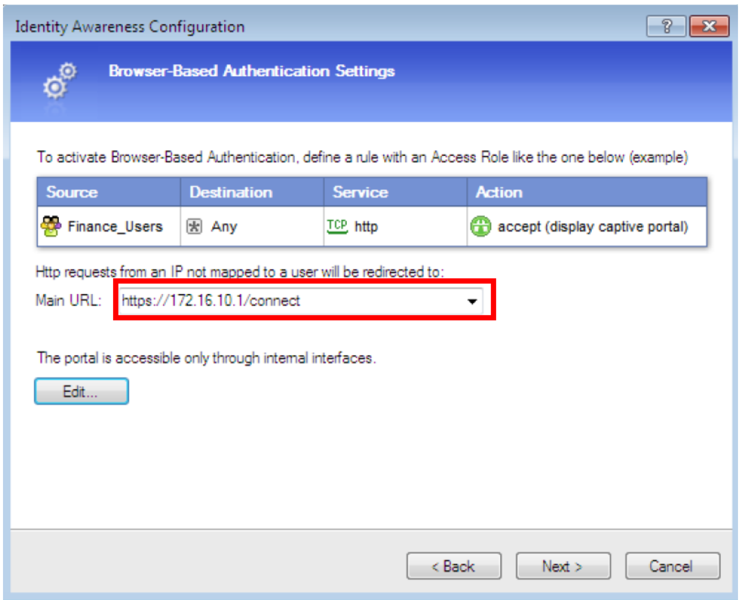
Password: ••••••••

Domain Controller: 172.16.10.100

Domain Administrator credentials are required.

Successfully connected!

Replace the IP in the link below in order to match the IP address of the NY-FW-1 on the internal LAN subnet – **172.16.10.1**



Identity Awareness Configuration

Browser-Based Authentication Settings

To activate Browser-Based Authentication, define a rule with an Access Role like the one below (example)

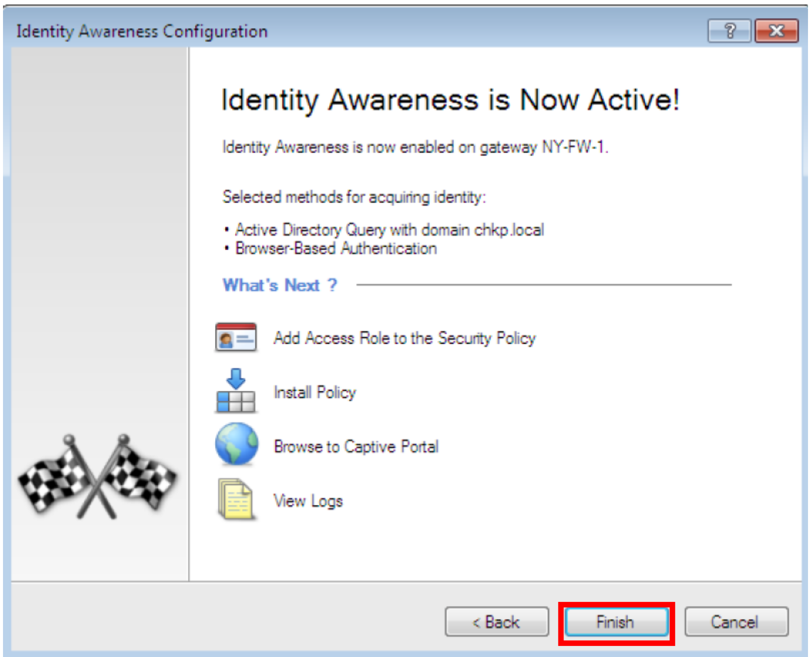
Source	Destination	Service	Action
Finance_Users	Any	http	accept (display captive portal)

Http requests from an IP not mapped to a user will be redirected to:

Main URL: https://172.16.10.1/connect

The portal is accessible only through internal interfaces.

Click **Next** and then **Finish**:



Identity Awareness is Now Active!

Identity Awareness is now enabled on gateway NY-FW-1.

Selected methods for acquiring identity:

- Active Directory Query with domain chkp.local
- Browser-Based Authentication

What's Next ?

Add Access Role to the Security Policy

Install Policy

Browse to Captive Portal

View Logs

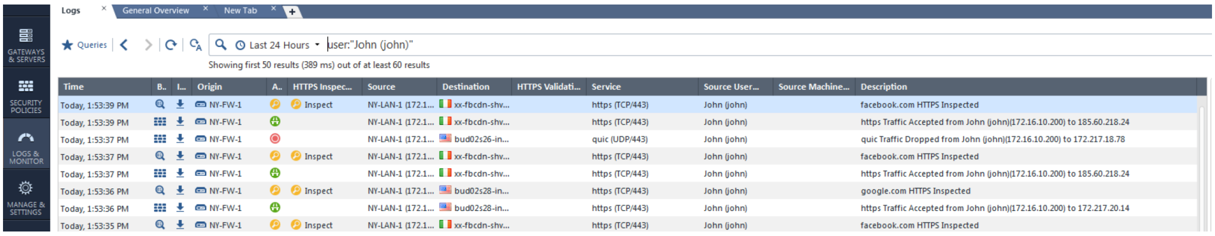
Great, now Identity Awareness is active !

So, why all this? If we now generate some events or traffic on the NY-LAN-PC and then inspect them in Logs and Monitor in Check Point SmartConsole, we should be able to see the username in the logs, and not just the IP address. Let's test this right away.

Now, let's **Publish** changes and install **HQ_Corporate_Policy** on NY-FW-1.

I will open a page to **facebook.com** and one to **youtube.com** and then check the logs in SmartConsole.
(please note that you may need to redeploy the certificate again on the PC as you may receive errors when trying to navigate to different websites).

In the search bar, I will filter logs based on Username, entering the following: **User:John**. You will see that after you enter **User:** the username John will appear in order to autocomplete.

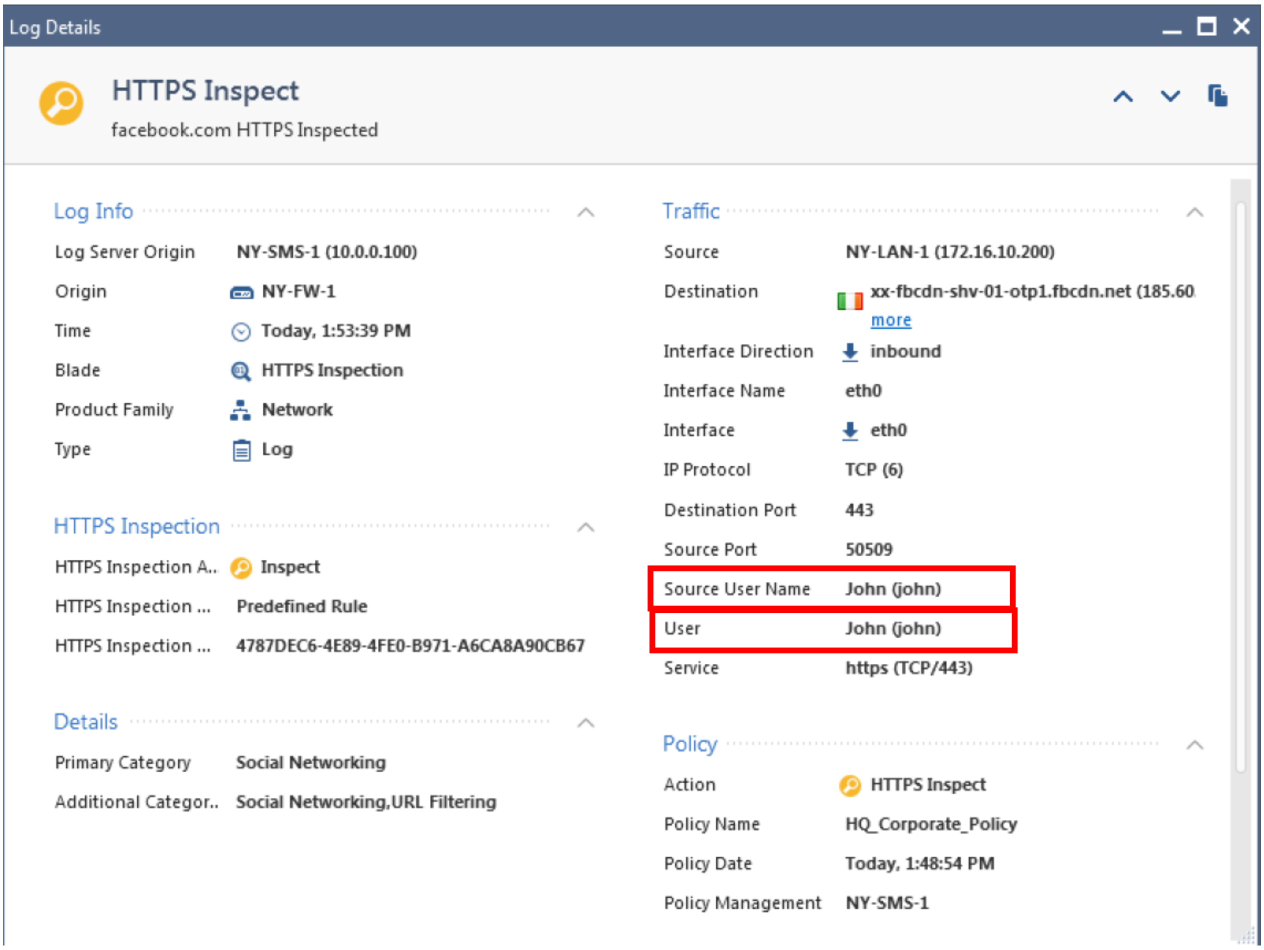


Last 24 Hours user:"John (john)"

Showing first 50 results (389 ms) out of at least 60 results

Time	B..	I...	Origin	A..	HTTPS Inspec...	Source	Destination	HTTPS Validati...	Service	Source User...	Source Machine...	Description
Today, 1:53:39 PM			NY-FW-1		Inspect	NY-LAN-1 (172.1...	xx-fbcdn-shv...		https (TCP/443)	John (john)		facebook.com HTTPS Inspected
Today, 1:53:39 PM			NY-FW-1			NY-LAN-1 (172.1...	xx-fbcdn-shv...		https (TCP/443)	John (john)		https Traffic Accepted from John (john)(172.16.10.200) to 185.60.218.24
Today, 1:53:37 PM			NY-FW-1			NY-LAN-1 (172.1...	bud02s26-in...		quic (UDP/443)	John (john)		quic Traffic Dropped from John (john)(172.16.10.200) to 172.217.18.78
Today, 1:53:37 PM			NY-FW-1		Inspect	NY-LAN-1 (172.1...	xx-fbcdn-shv...		https (TCP/443)	John (john)		facebook.com HTTPS Inspected
Today, 1:53:37 PM			NY-FW-1			NY-LAN-1 (172.1...	xx-fbcdn-shv...		https (TCP/443)	John (john)		https Traffic Accepted from John (john)(172.16.10.200) to 185.60.218.24
Today, 1:53:36 PM			NY-FW-1		Inspect	NY-LAN-1 (172.1...	bud02s28-in...		https (TCP/443)	John (john)		google.com HTTPS Inspected
Today, 1:53:36 PM			NY-FW-1			NY-LAN-1 (172.1...	bud02s28-in...		https (TCP/443)	John (john)		https Traffic Accepted from John (john)(172.16.10.200) to 172.217.20.14
Today, 1:53:35 PM			NY-FW-1		Inspect	NY-LAN-1 (172.1...	xx-fbcdn-shv...		https (TCP/443)	John (john)		facebook.com HTTPS Inspected

Let’s open one of the logs:



HTTPS Inspect

facebook.com HTTPS Inspected

Log Info

Log Server Origin	NY-SMS-1 (10.0.0.100)
Origin	NY-FW-1
Time	Today, 1:53:39 PM
Blade	HTTPS Inspection
Product Family	Network
Type	Log

HTTPS Inspection

HTTPS Inspection A..	Inspect
HTTPS Inspection ...	Predefined Rule
HTTPS Inspection ...	4787DEC6-4E89-4FE0-B971-A6CA8A90CB67

Details

Primary Category	Social Networking
Additional Categor..	Social Networking,URL Filtering

Traffic

Source	NY-LAN-1 (172.16.10.200)
Destination	xx-fbcdn-shv-01-otp1.fbcdn.net (185.60 more
Interface Direction	inbound
Interface Name	eth0
Interface	eth0
IP Protocol	TCP (6)
Destination Port	443
Source Port	50509
Source User Name	John (john)
User	John (john)
Service	https (TCP/443)

Policy

Action	HTTPS Inspect
Policy Name	HQ_Corporate_Policy
Policy Date	Today, 1:48:54 PM
Policy Management	NY-SMS-1

And here it is … Source User Name – **John.**

This confirms that indeed Identity Awareness integration with Microsoft Active Directory was successful and running with no problem!

31.0 Lab: App Control and URL Filtering Activation and Update on NY-SMS-1

Lab Objectives

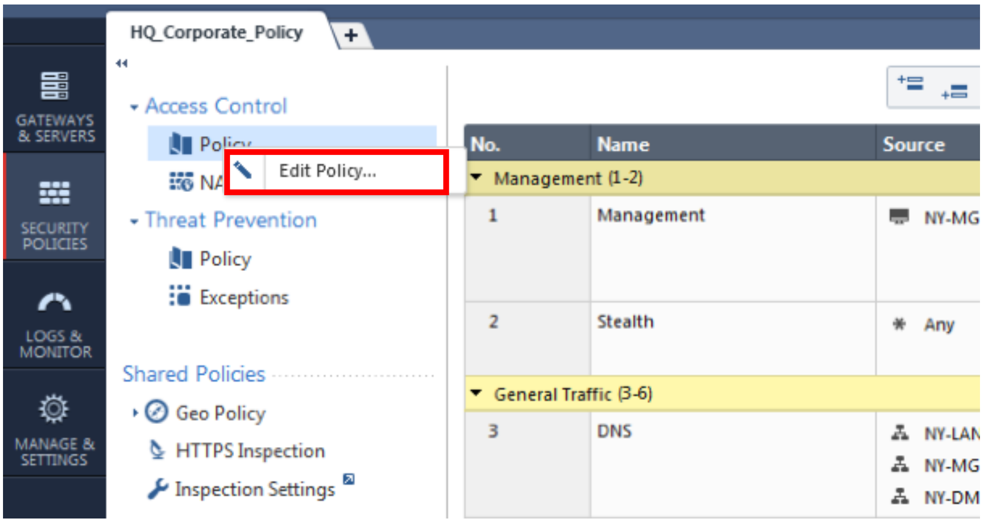
- Activate Application Control and URL Filtering Software Blades on NY-FW-1
- Verify and update if necessary APPCTL & URLF Software Blades

We now have both HTTPS Inspection and Identity Awareness configured and activated, which brings great benefits. We have complete visibility over what websites are accessed by the what users and all the applications they are using.

We can now deploy Application Control and URL Filtering software blades and use this information in order to create a secure access control policy for the organization. We will be activating later on **Content Awareness** software blade in order to control how date is being used in the organization, in what direction – download or upload. Also, we will be activating the **Compliance** software blade, which will come really handy and help us to analyse our configuration and compare it to current security best practices.

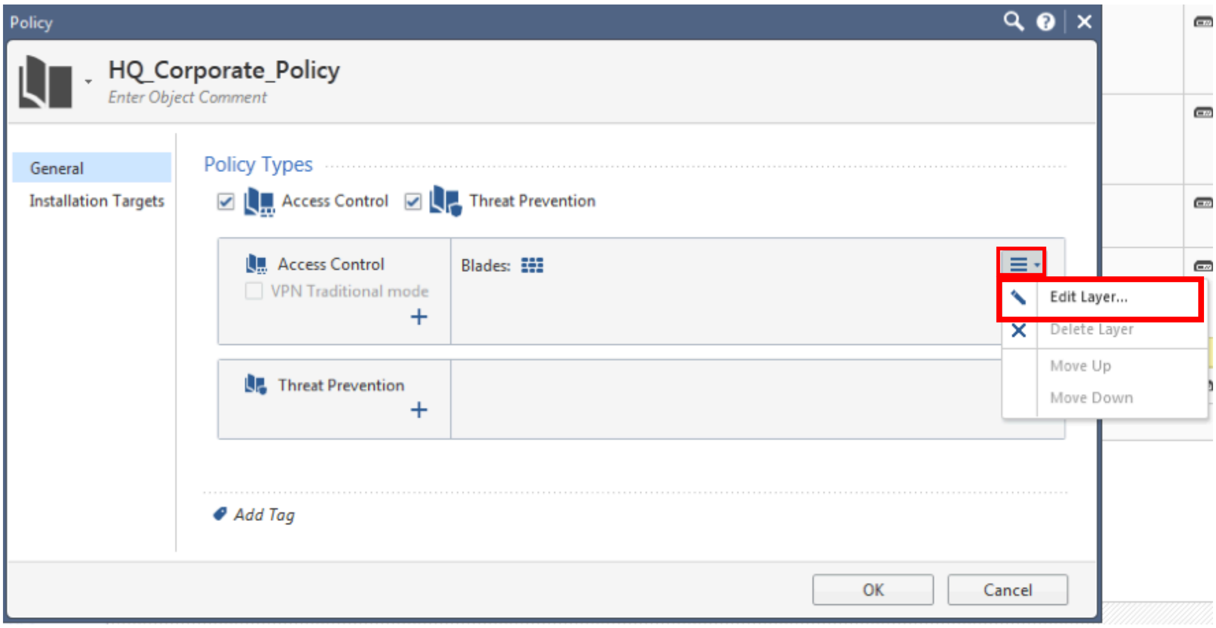
Let's enable in Access Control Policy Layer also the Application Control and URL Filtering blade. If you just enable the software blade at the gateway level, but you don't enable it at the layer level, then the capabilities of the specific blade will not be used.

Select **Security Policies,** right-click on Access Control policy and select **Edit.**

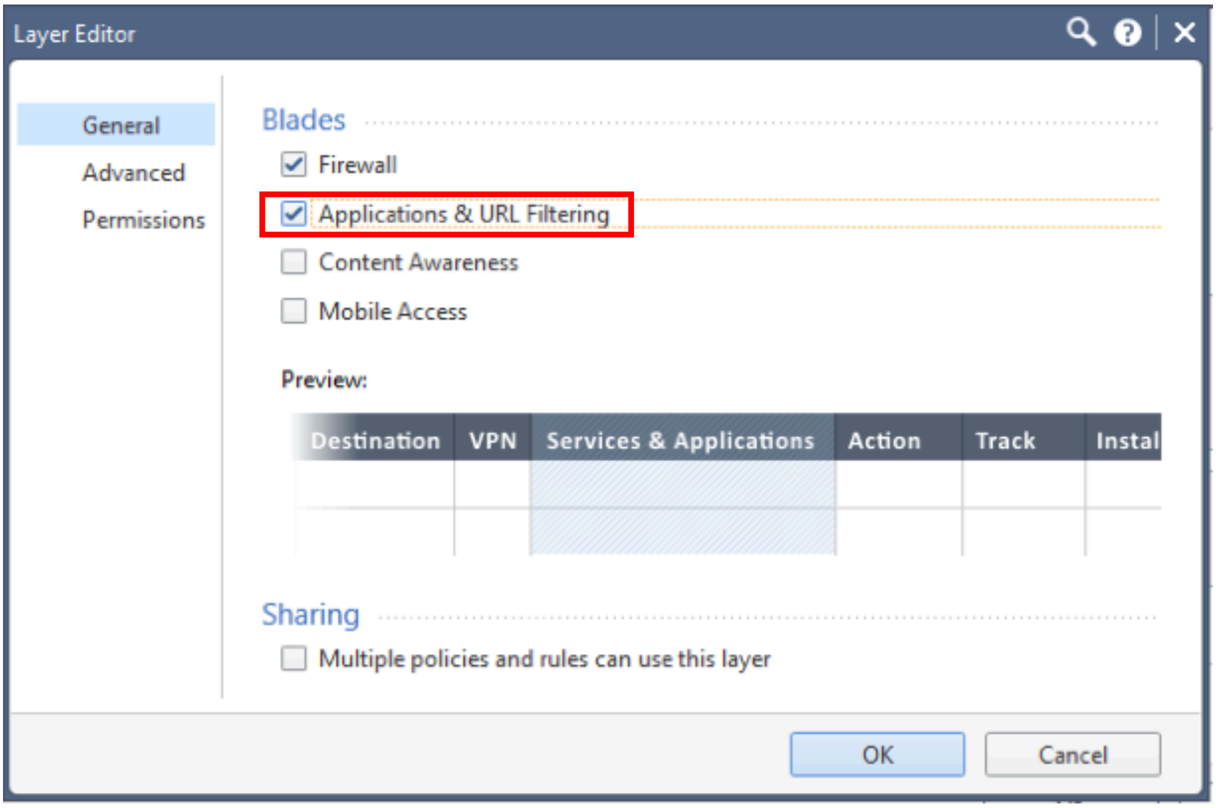


No.	Name	Source
Management (1-2)		
1	Management	NY-MG
2	Stealth	Any
General Traffic (3-6)		
3	DNS	NY-LAN NY-MG NY-DM

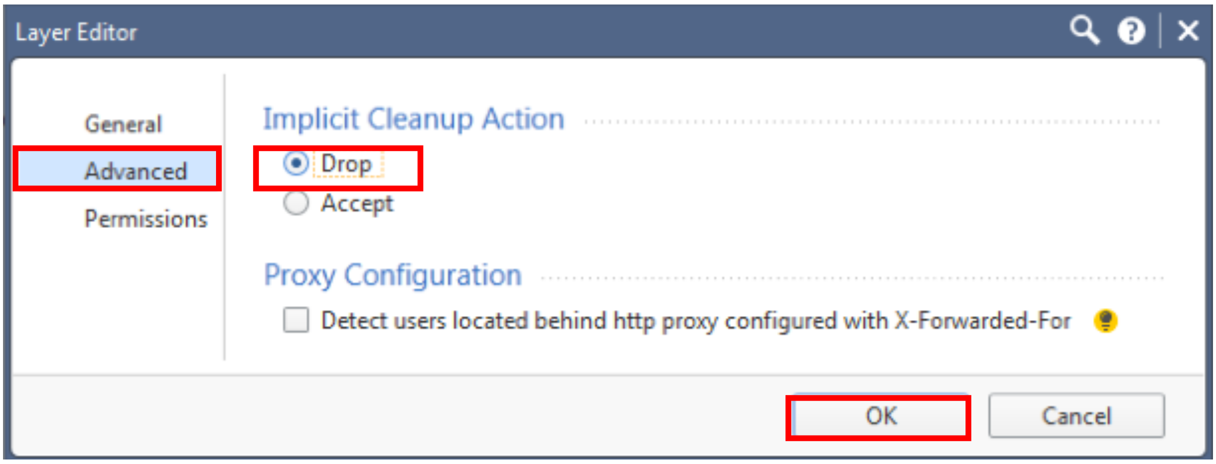
Let's edit the Access Control Layer:



and also enable **Applications & URL Filtering**:



Click on **Advanced** and verify the Implicit Cleanup action. If it wasn't already, let's select here **Drop**.



Layer Editor

Implicit Cleanup Action

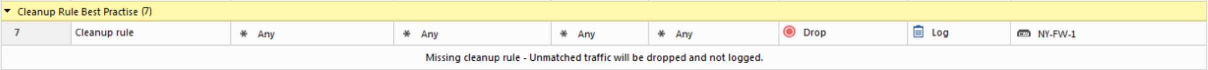
● Drop

○ Accept

Proxy Configuration

□ Detect users located behind http proxy configured with X-Forwarded-For

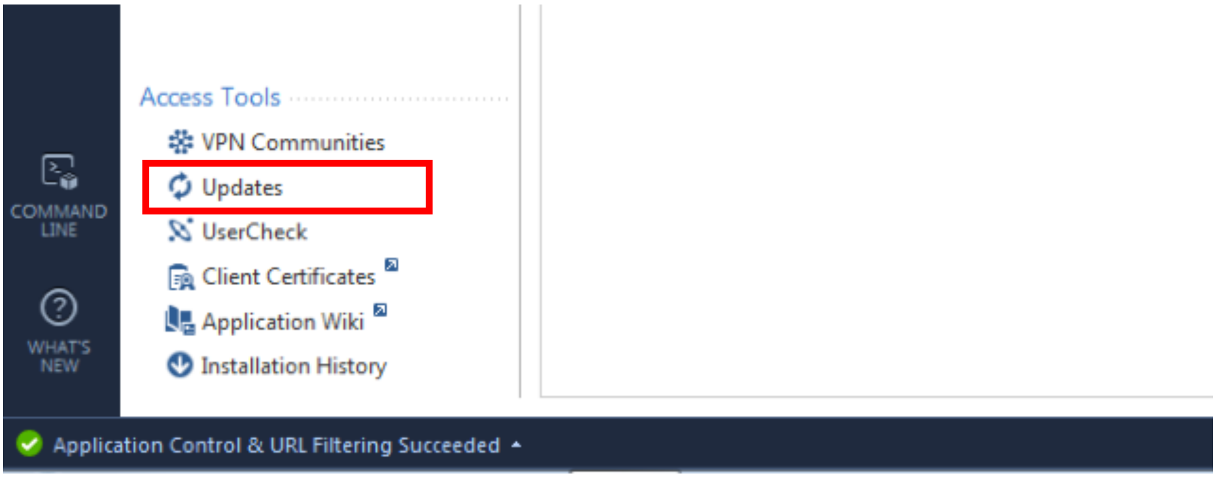
Check Point recommends that we have an explicit Drop in our rule base and we do, it’s the Cleanup Rule, the last rule in our current rule base.



▾ Cleanup Rule Best Practise (7)								
7	Cleanup rule	✱ Any	✱ Any	✱ Any	✱ Any	● Drop	Log	NY-FW-1
Missing cleanup rule - Unmatched traffic will be dropped and not logged.								

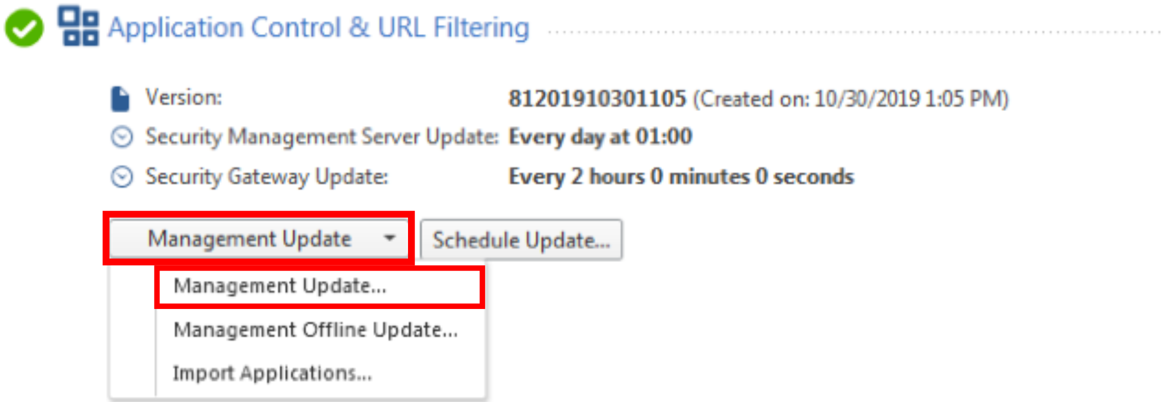
Before moving on, let’s make sure the Applications and URL Filtering database is up-to-date. These databases update automatically by default, without further configuration, but let’s make sure everything looks fine.

In the **Security Policies** menu, at the bottom on the left-hand side, under **Access Tools**, click on **Updates**:



Application Control & URL Filtering Succeeded

Application Control & URL Filtering databases look good, they are up-to date. Alternatively, you can trigger the databases’ update by selecting **Management Update**, as you can see below:



Application Control & URL Filtering

Version: 81201910301105 (Created on: 10/30/2019 1:05 PM)

Security Management Server Update: Every day at 01:00

Security Gateway Update: Every 2 hours 0 minutes 0 seconds

32.0 Lab: Block High Risk and Inappropriate Content Categories

Lab Objectives

- Implement best practices and block high risk and inappropriate content categories

When designing the Access Control policy, there is one question that could come up. What are the best practices or what should I block and or permit as in regards to Applications?

I recommend following Check Point best practices and these are highlighted in a SecureKnowledge document – SK112249. These SK is available at the following URL:

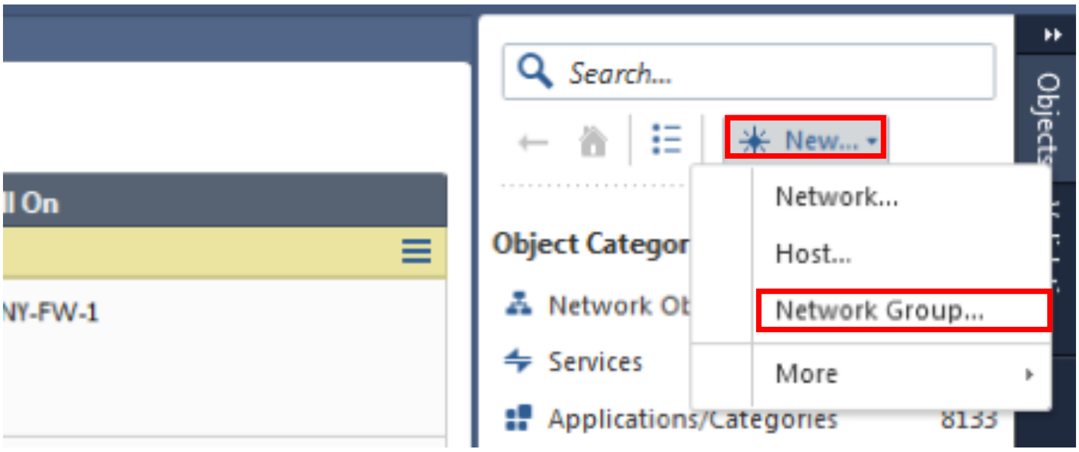
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112249

As explained in the SK, there are two ways to enforce application control policy:

- **Blacklist** - Block any undesired traffic and allow everything else
- **Whitelist** - Allow any application or network protocol that you want accessible

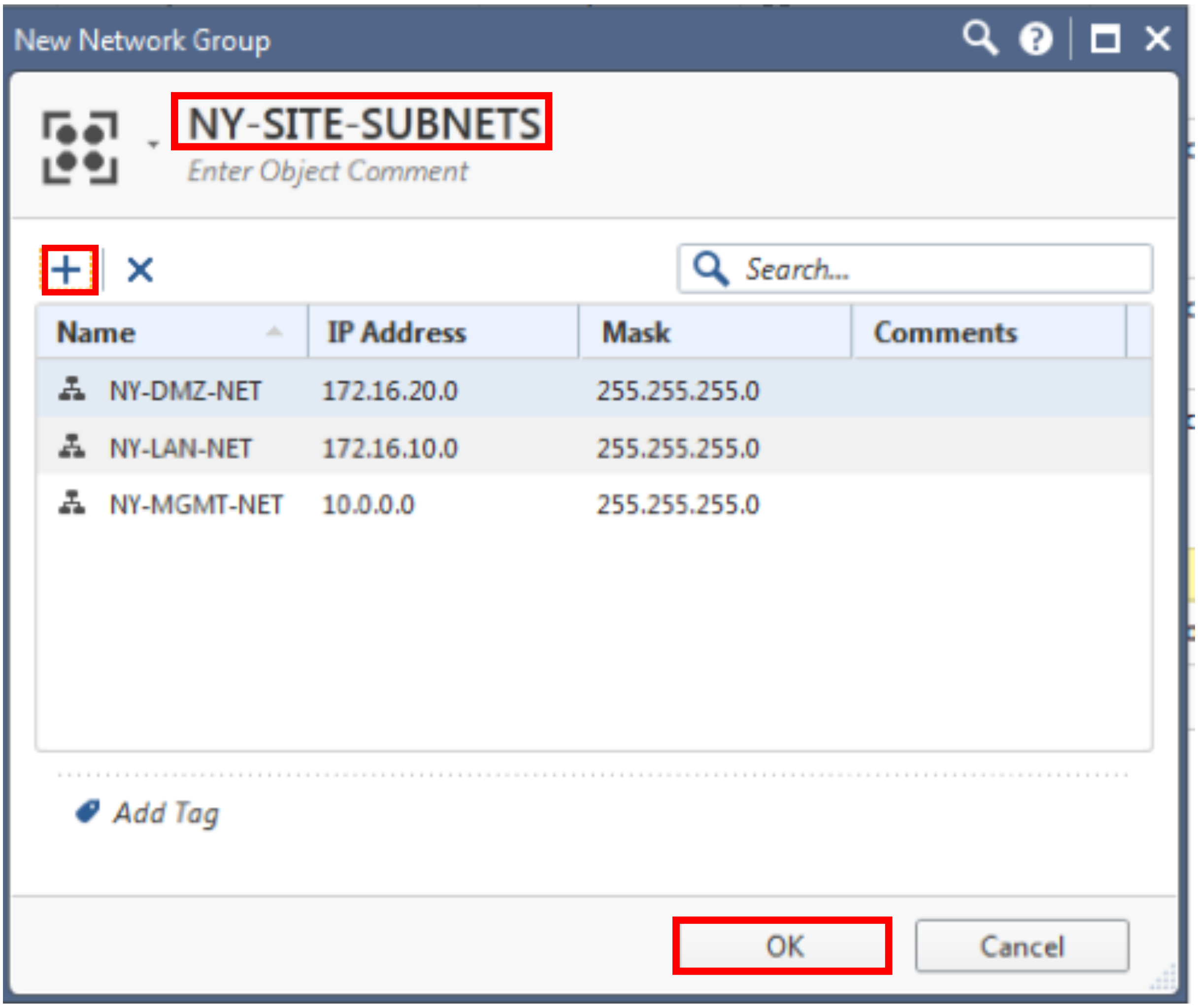
Following on, we will implement the first option and block all undesired content categories within our policy.

First, let's create a group object and include our New York three subnets – NY-LAN-NET, NY-MGMT-NET and NY-DMZ-NET. It is easier for the Administrator to use single objects instead of using multiple object, when defining policies.



At the top-right corner, with the object pane expanded, select **New** and then **Network Group**, as you can see above.

Define a name for your new network group – **NY-SITE-SUBNETS**, and click the **+** in order to select the New York subnets that you want to include.



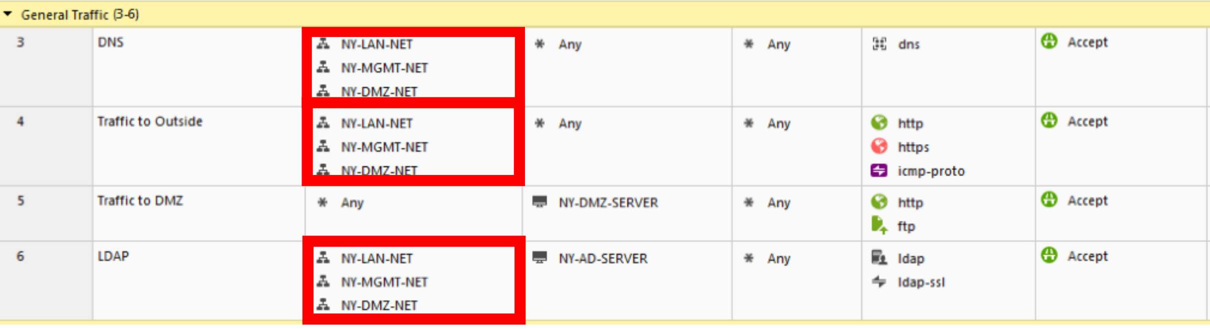
New Network Group

NY-SITE-SUBNETS

Enter Object Comment

Name	IP Address	Mask	Comments
NY-DMZ-NET	172.16.20.0	255.255.255.0	
NY-LAN-NET	172.16.10.0	255.255.255.0	
NY-MGMT-NET	10.0.0.0	255.255.255.0	

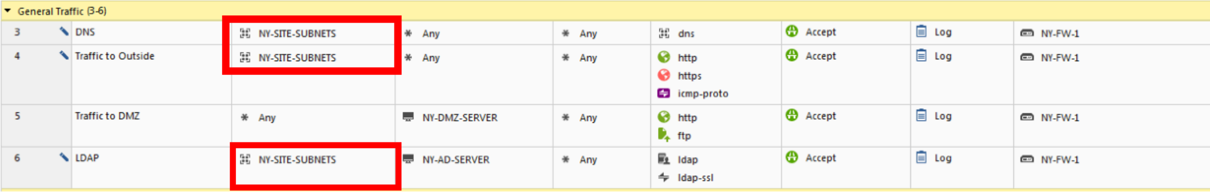
When done, click **OK** in order to close the window. Now we will replace the source objects with this single object. Here is how the rule base looks now:



General Traffic (3-6)

3	DNS	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	Any	Any	dns	Accept
4	Traffic to Outside	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	Any	Any	http https icmp-proto	Accept
5	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Accept
6	LDAP	NY-LAN-NET NY-MGMT-NET NY-DMZ-NET	NY-AD-SERVER	Any	ldap ldap-ssl	Accept

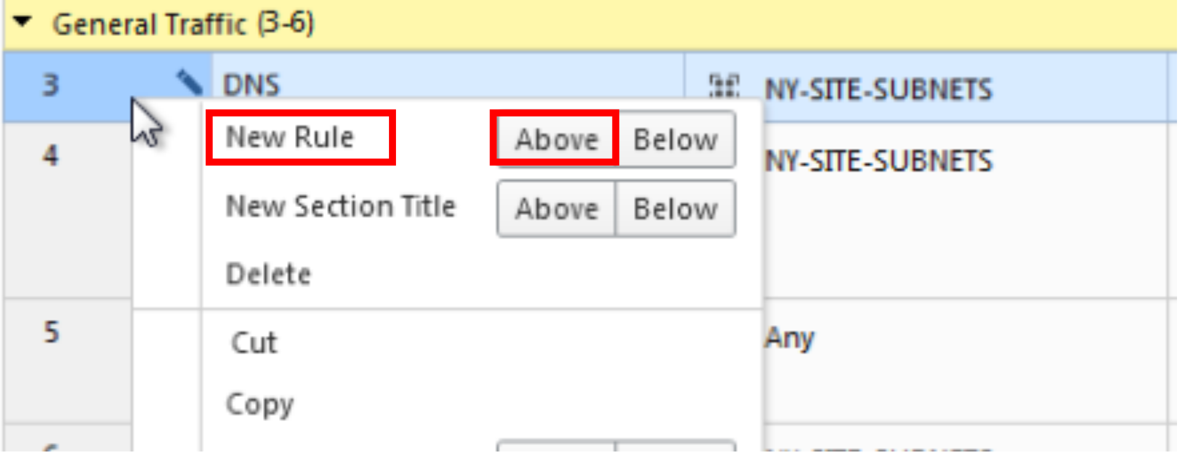
Below the simplified version:



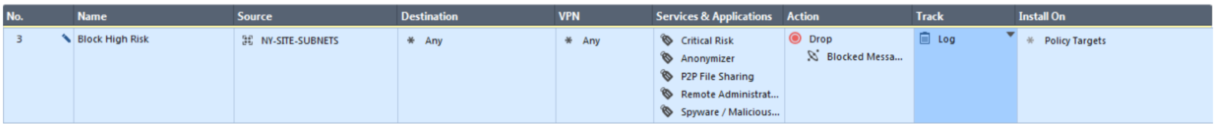
General Traffic (3-6)

3	DNS	NY-SITE-SUBNETS	Any	Any	dns	Accept	Log	NY-FW-1
4	Traffic to Outside	NY-SITE-SUBNETS	Any	Any	http https icmp-proto	Accept	Log	NY-FW-1
5	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Accept	Log	NY-FW-1
6	LDAP	NY-SITE-SUBNETS	NY-AD-SERVER	Any	ldap ldap-ssl	Accept	Log	NY-FW-1

Now, let’s add a rule above rule 3 in order to implement Check Point Best Practices. Right-click on 3 and select **New Rule – Above**:

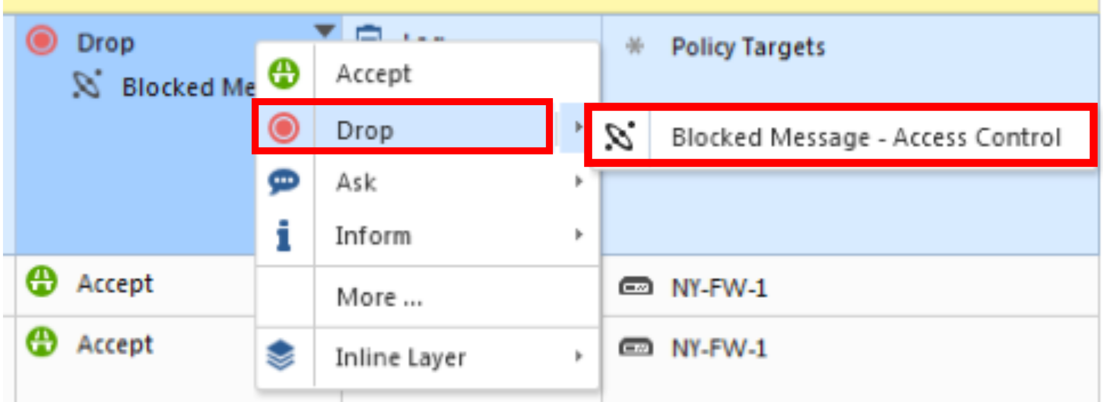


The new rule should look like the following:

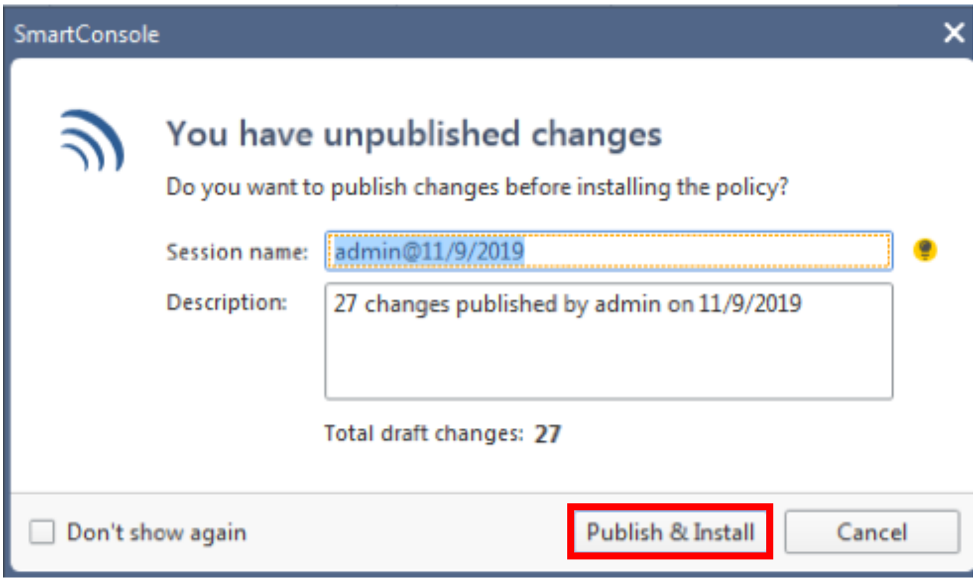


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
3	Block High Risk	NY-SITE-SUBNETS	Any	Any	Critical Risk Anonymizer P2P File Sharing Remote Administrat... Spyware / Malicious...	Drop Blocked Messa...	Log	Policy Targets

Please note that in the **Action** column, I have selected the **Drop** action and also **Blocked Message – Access Control**. Applying this action means that the content will be blocked and the user will be displayed a message in the browser, that announces the block action. Right-click on **Drop** and click the arrow to the right in order to extend and select the advanced option.



Last step, let's just **Publish** changes and **Install Policy.**



SmartConsole

You have unpublished changes

Do you want to publish changes before installing the policy?

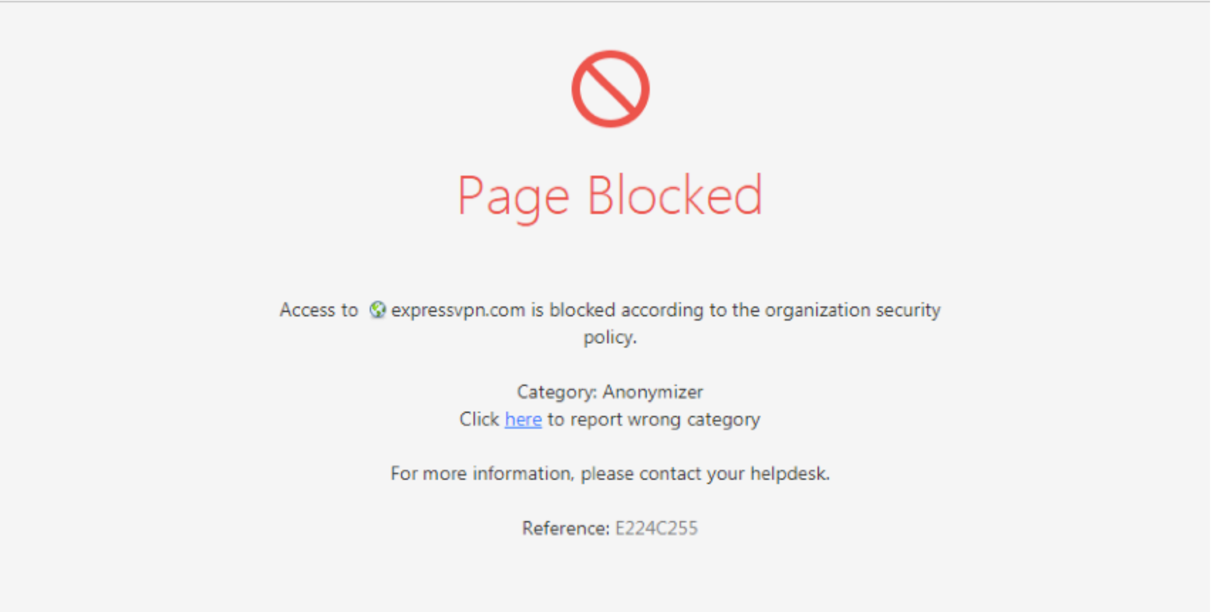
Session name: admin@11/9/2019

Description: 27 changes published by admin on 11/9/2019

Total draft changes: 27

□ Don't show again

If you now try to access a website like www.expressvpn.com, from NY-LAN-PC, the connection will be blocked and the following message will be displayed:



Page Blocked

Access to expressvpn.com is blocked according to the organization security policy.

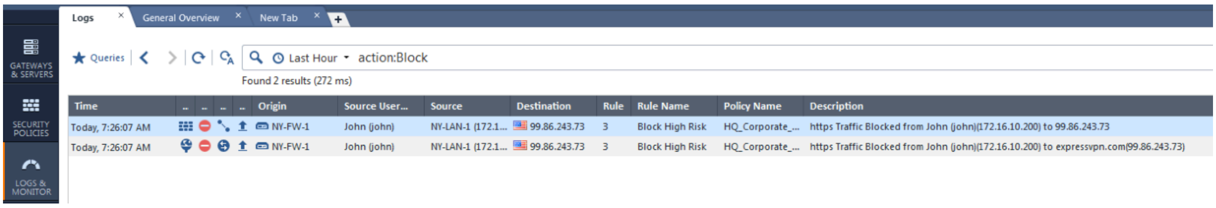
Category: Anonymizer
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: E224C255

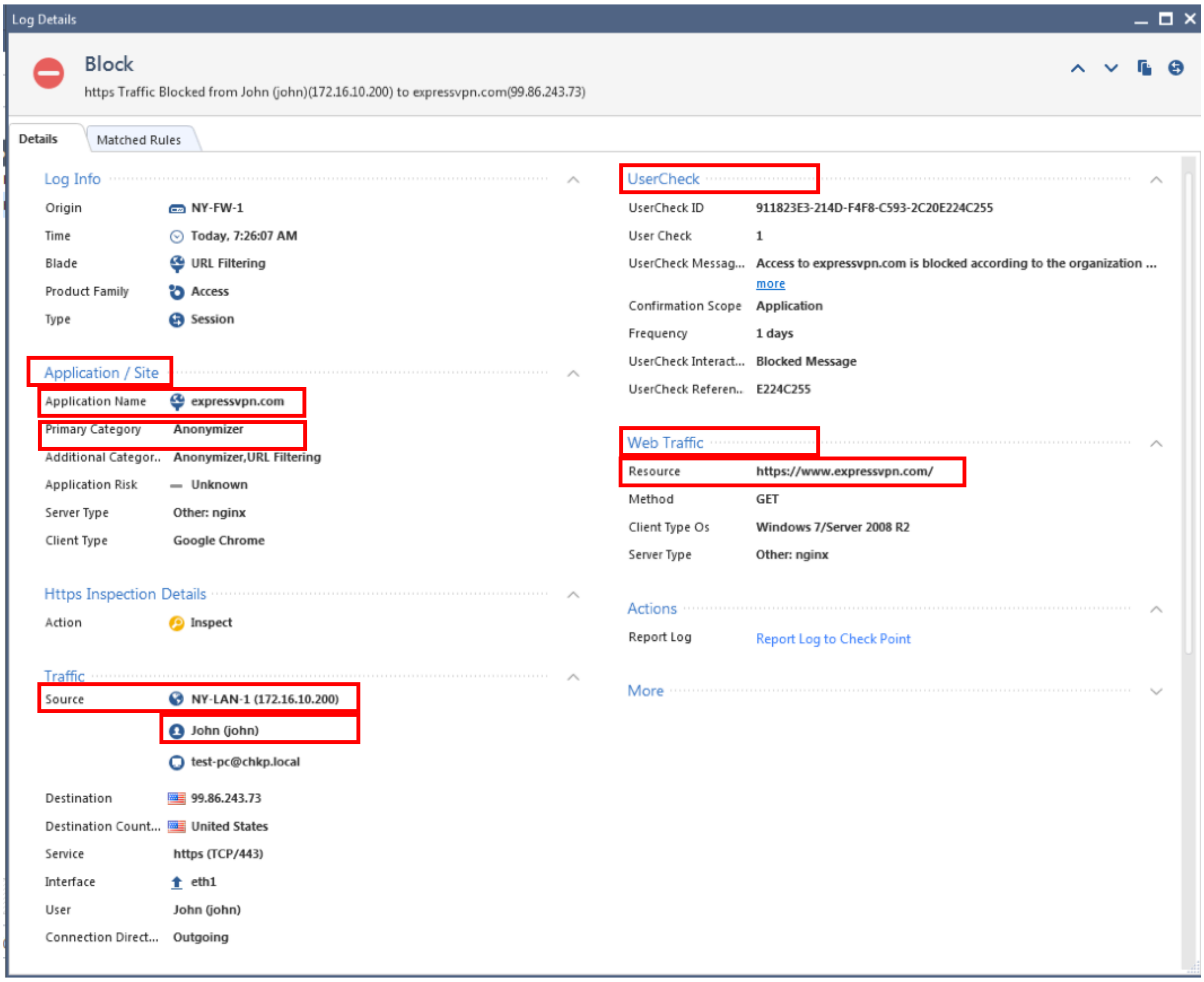
This is called a **UserCheck** page and the message can be customized as needed in order to match preferences or organization rules.

Let's take a look in **Logs&Monitor** and identify the log associated with this action. I will filter the logs with **Last Hour** and **action:Block**:



Time	..	..	..	..	Origin	Source User...	Source	Destination	Rule	Rule Name	Policy Name	Description
Today, 7:26:07 AM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	99.86.243.73	3	Block High Risk	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to 99.86.243.73
Today, 7:26:07 AM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	99.86.243.73	3	Block High Risk	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to expressvpn.com(99.86.243.73)

All information is available as you can see:



Block

https Traffic Blocked from John (john)(172.16.10.200) to expressvpn.com(99.86.243.73)

Log Info

Origin	NY-FW-1
Time	Today, 7:26:07 AM
Blade	URL Filtering
Product Family	Access
Type	Session

Application / Site

Application Name	expressvpn.com
Primary Category	Anonymizer
Additional Categor..	Anonymizer,URL Filtering
Application Risk	— Unknown
Server Type	Other: nginx
Client Type	Google Chrome

Https Inspection Details

Action	Inspect

Traffic

Source	NY-LAN-1 (172.16.10.200) John (john) test-pc@chkp.local
Destination	99.86.243.73
Destination Count...	United States
Service	https (TCP/443)
Interface	eth1
User	John (john)
Connection Direct...	Outgoing

UserCheck

UserCheck ID	911823E3-214D-F4F8-C593-2C20E224C255
User Check	1
UserCheck Messag...	Access to expressvpn.com is blocked according to the organization ... more
Confirmation Scope	Application
Frequency	1 days
UserCheck Interact...	Blocked Message
UserCheck Referen..	E224C255

Web Traffic

Resource	https://www.expressvpn.com/
Method	GET
Client Type Os	Windows 7/Server 2008 R2
Server Type	Other: nginx

Actions

Report Log	Report Log to Check Point

More

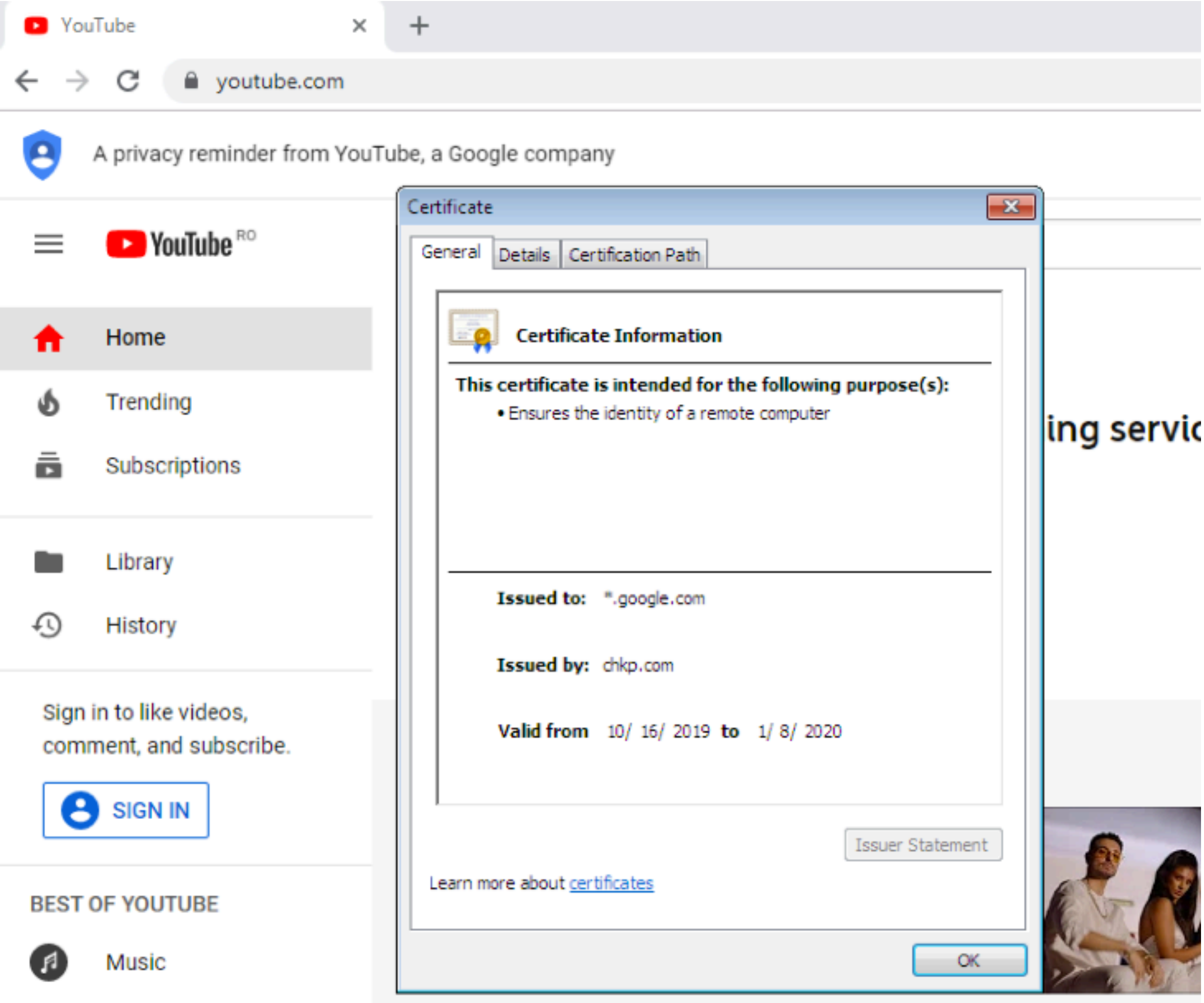
Application/Site – expressvpn.com
Primary Category – Anonymizer
Source – NY-LAN-1 and also the User – john
UserCheck information
Web Traffic Resource – https://www.expressvpn.com

33.0 Lab: Limit or Block Media Streaming (Youtube) Bandwidth Usage

Lab Objectives

- Limit or Block Media Streaming (Youtube) Bandwidth Usage

First, let’s try to access **youtube.com** and we see that this action is allowed. We can also see that HTTPS inspection works fine and our certificate looks fine.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

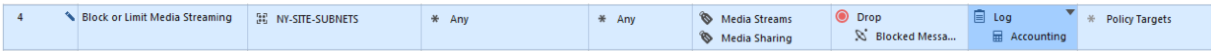
Issued to: *.google.com

Issued by: chkp.com

Valid from 10/ 16/ 2019 **to** 1/ 8/ 2020

YouTube
youtube.com
A privacy reminder from YouTube, a Google company
YouTube RO
Home
Trending
Subscriptions
Library
History
Sign in to like videos, comment, and subscribe.
SIGN IN
BEST OF YOUTUBE
Music
Issuer Statement
Learn more about certificates
OK
ing servic

Let’s go back to **Security Policies** and add another rule, below the previously added rule3, so this will be rule 4. Right click on 3 and select **Add Rule – Below:**

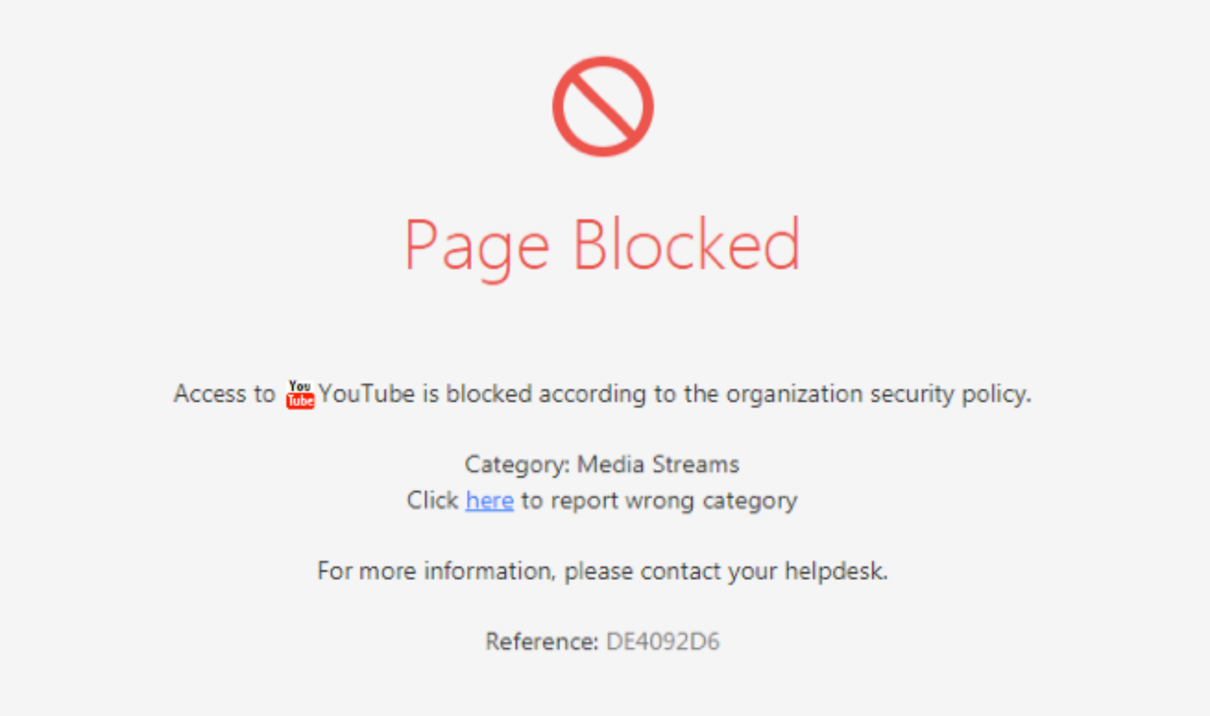


4	Block or Limit Media Streaming	NY-SITE-SUBNETS	Any	Any	Media Streams Media Sharing	Drop Blocked Messa...	Log Accounting	Policy Targets

In order to enforce the change, **Publish and Install Policy.**

Now, access to https://www.youtube.com should be blocked, but let’s verify.

And we can see that indeed access to youtube.com has been blocked.



Page Blocked

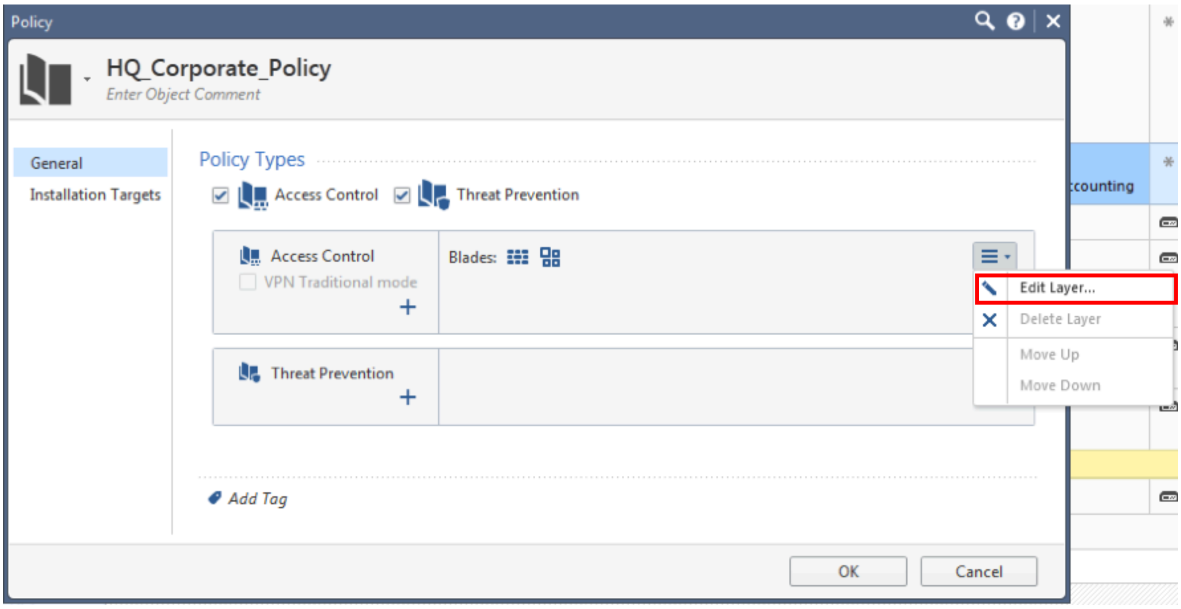
Access to YouTube is blocked according to the organization security policy.

Category: Media Streams
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: DE4092D6

In order to limit access to youtube.com and not block it, we need to activate the **Content Awareness** software blade. Content Awareness blade provides the ability to implement complex policies including conditions at the content level – which way should I permit or restrict traffic (download or upload), how much bandwidth should I permit? etc … Let's include now **Content Awareness** blade in the Policy Layer. Edit Access Control Policy:

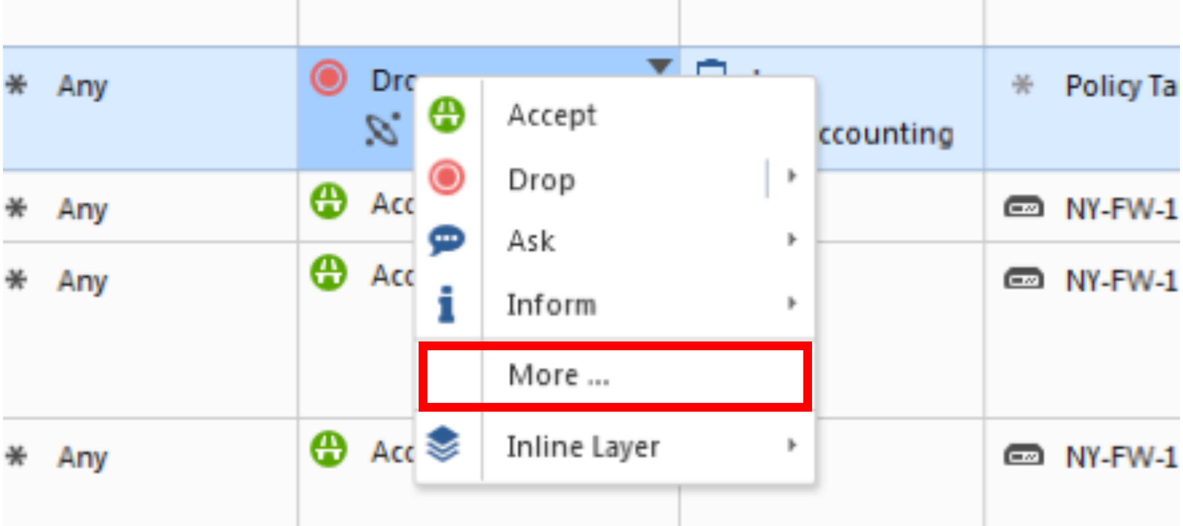


Policy

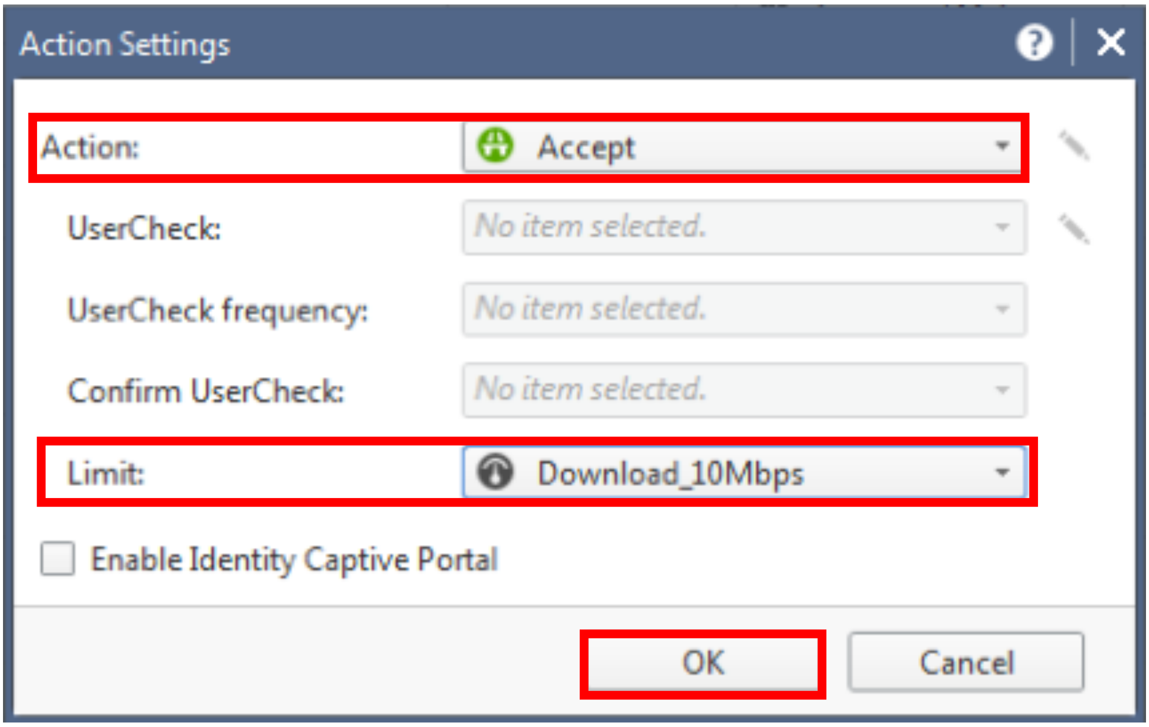
HQ_Corporate_Policy
Enter Object Comment

Now, **Publish** and **Install** the **HQ_Corporate_Policy.**

Right-click on **Drop** in rule 4 and select **More.**



Select Action – Accept and Limit – Download_10Mbps:


Action Settings

Action: Accept

UserCheck: No item selected.

UserCheck frequency: No item selected.

Confirm UserCheck: No item selected.

Limit: Download_10Mbps

□ Enable Identity Captive Portal

Click on and again **Publish** and **Install** the HQ_Corporate_Policy in order to enforce the policy.

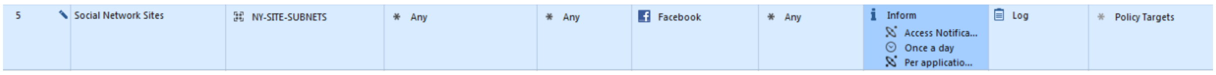
34.0 Lab: Block or Inform Users - Social Network Sites (FaceBook)

Lab Objectives

- Block or Inform Users - Social Network Sites (Facebook)

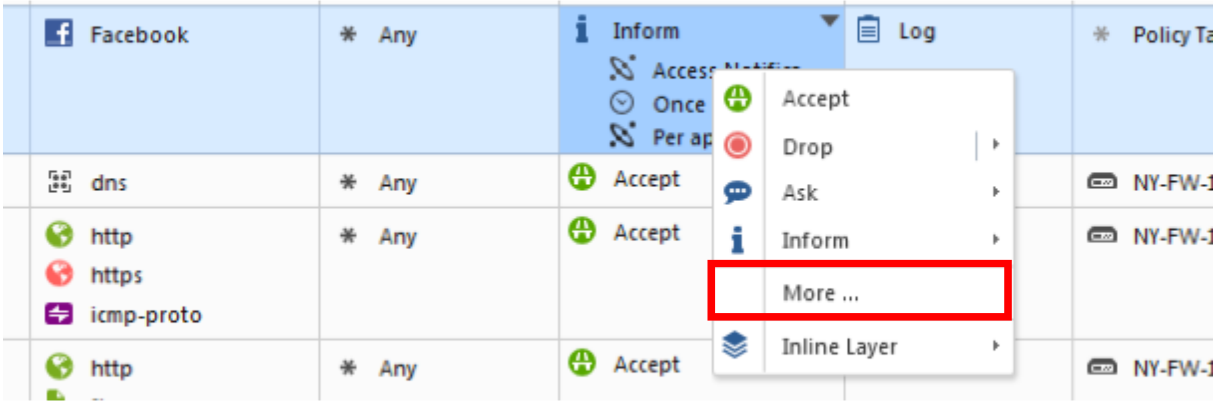
We will add a new rule, below rule 4, so this will be rule 5:

- Name: Social Network Sites
- Source: NY-SITE-SUBNETS
- Destination: Any
- Services & Applications: Facebook
- Action: Inform, Access Notification



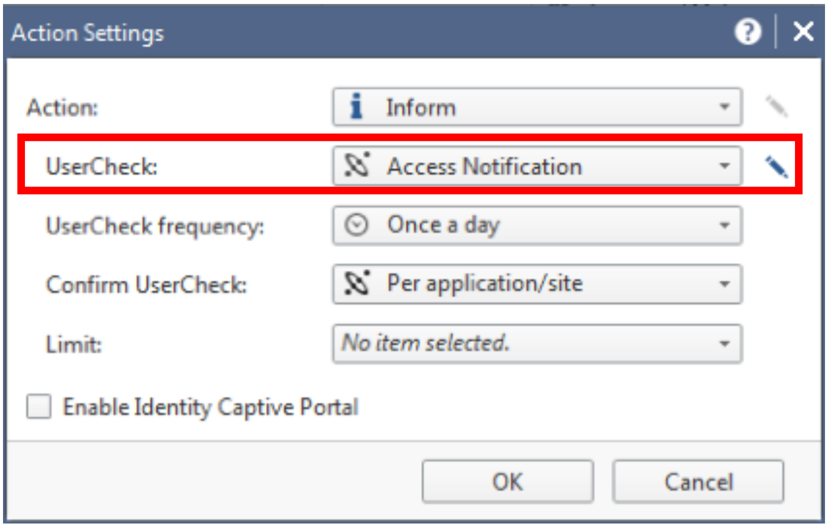
5	Social Network Sites	NY-SITE-SUBNETS	Any	Any	Facebook	Any	Inform Access Notifica... Once a day Per applicatio...	Log	Policy Targets

Right-click on Inform Action and select **More.**



Facebook	Any	Inform Access Notifica... Once Per ap...	Log	Policy Ta...
dns	Any	Accept		NY-FW-1
http https icmp-proto	Any	Accept		NY-FW-1
http	Any	Accept		NY-FW-1

Let’s take a look at the options here:



Action Settings

Action: Inform

UserCheck: Access Notification

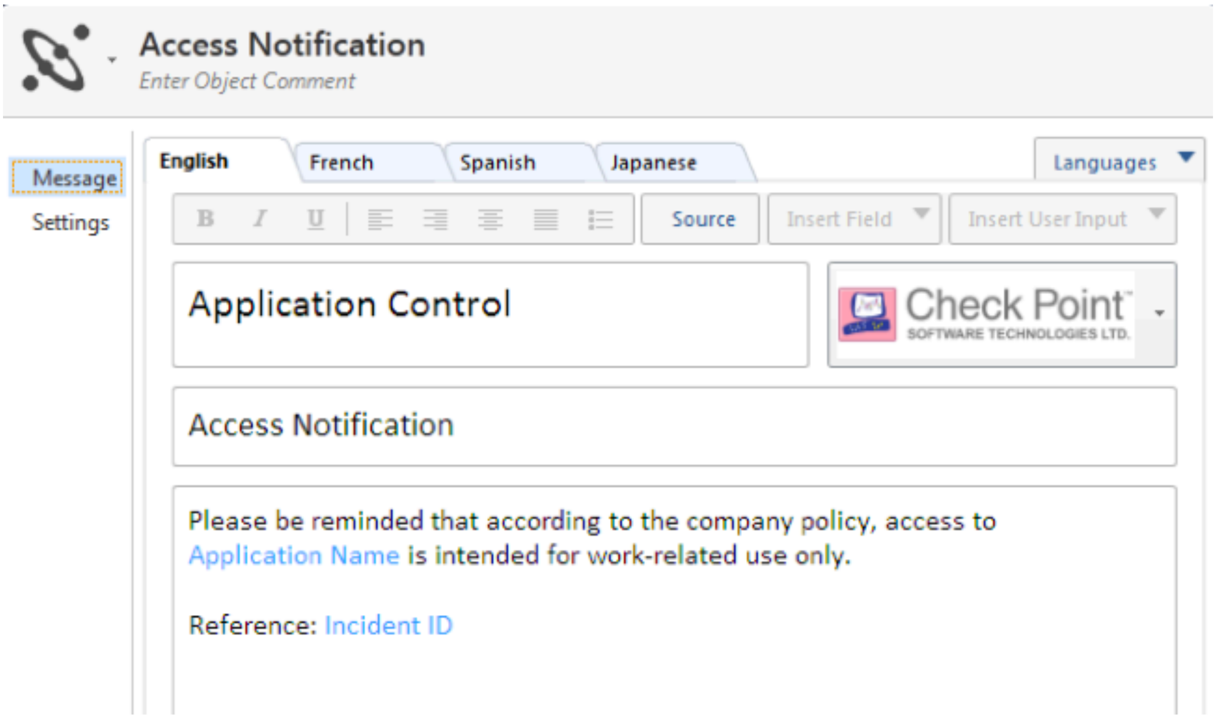
UserCheck frequency: Once a day

Confirm UserCheck: Per application/site

Limit: *No item selected.*

□ Enable Identity Captive Portal

We can modify the UserCheck message by clicking on the pencil on the right, and define our own message that we want to be displayed to the end user. Here is how the default message looks like:



Application Control

Access Notification

Please be reminded that according to the company policy, access to Application Name is intended for work-related use only.

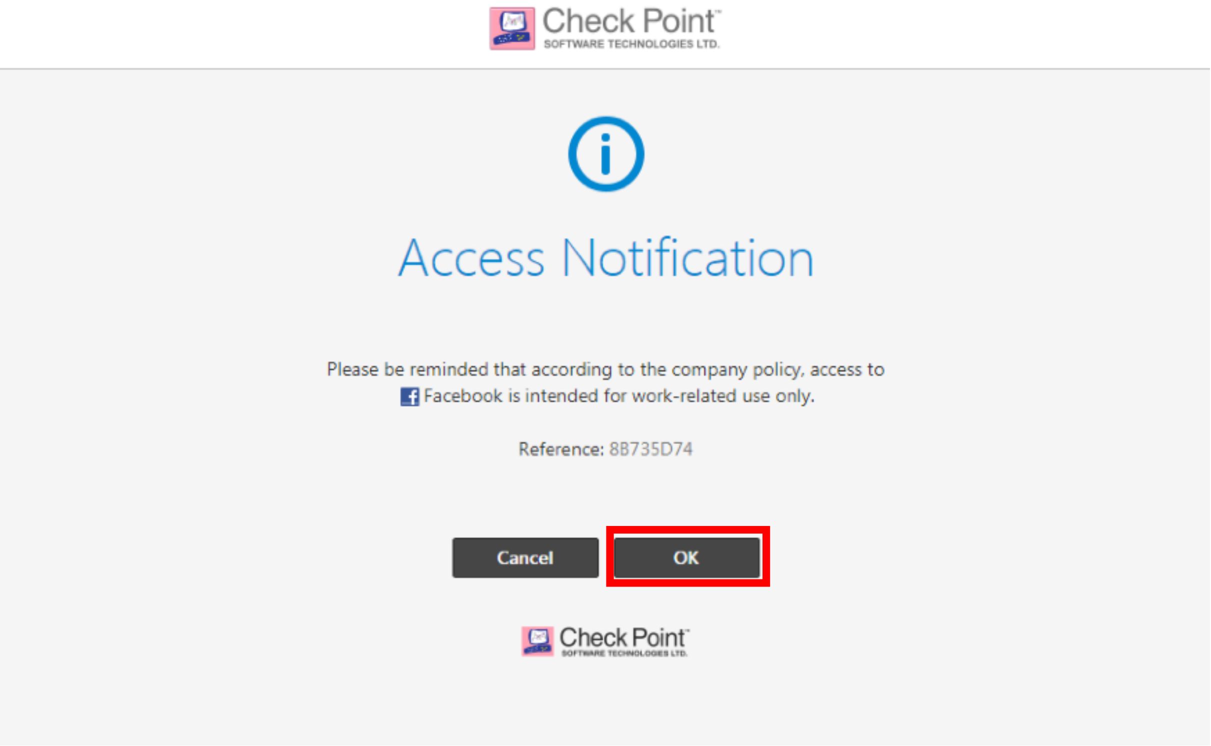
Reference: Incident ID

We also have different options available in order to select how often the UserCheck message is shown to the user and if we want this message to be displayed per application, per category, etc.

Also, don't forget to include the Logging option, so that we have visibility over the traffic when checking in Logs&Monitor.

Publish and **Install** the policy now, next we will test this functionality.

Now, when you try to navigate to https://www.facebook.com, you will first be displayed an **Access Notification** message:

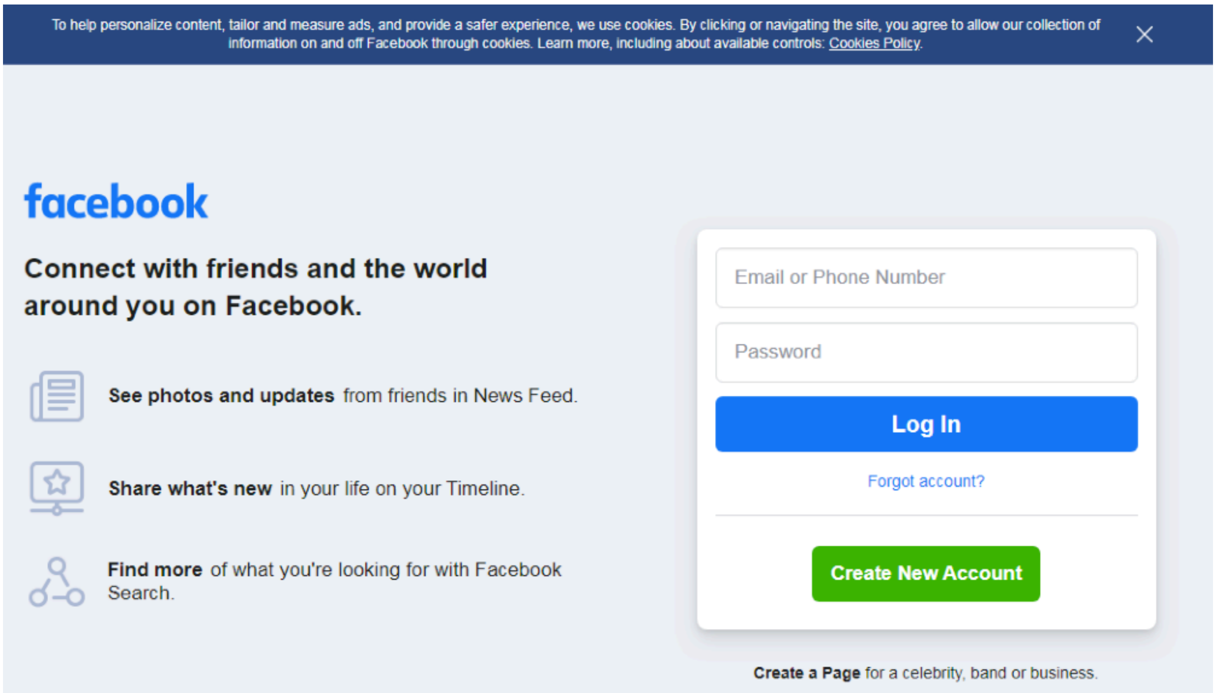


Access Notification

Please be reminded that according to the company policy, access to Facebook is intended for work-related use only.

Reference: 8B735D74

Click on **OK** and you will be provided access to social networking website – facebook.



To help personalize content, tailor and measure ads, and provide a safer experience, we use cookies. By clicking or navigating the site, you agree to allow our collection of information on and off Facebook through cookies. Learn more, including about available controls: Cookies Policy.

facebook

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

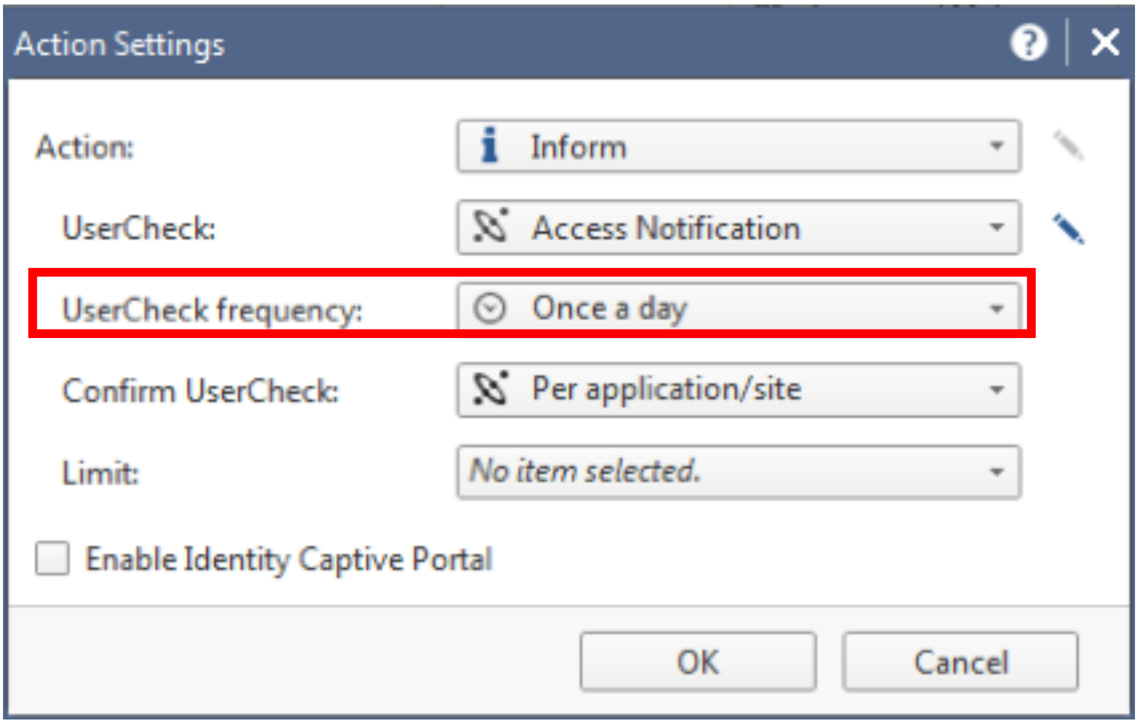
Share what's new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

Create a Page for a celebrity, band or business.

Please note that if you open a new tab and browse again to facebook.com, this time you will not be displayed any message. This is fine and it is based on the configuration we have implemented.

We have selected the UserCheck frequency – **Once per day**.



Action Settings

Action: Inform

UserCheck: Access Notification

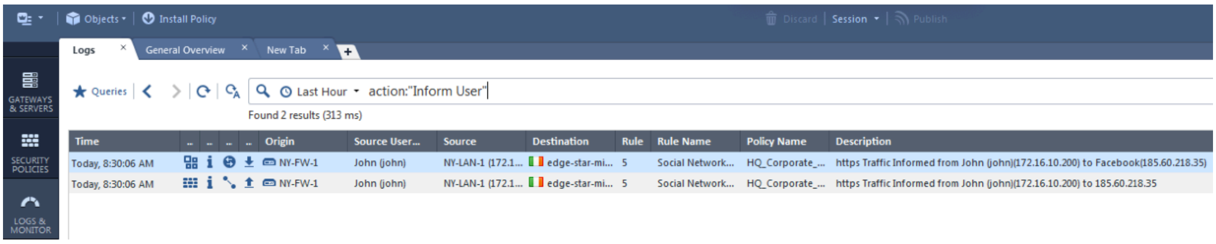
UserCheck frequency: Once a day

Confirm UserCheck: Per application/site

Limit: *No item selected.*

□ Enable Identity Captive Portal

Let’s now search for the associated log in Logs&Monitor. The filtering condition will be in this case **action:”Inform User”**.



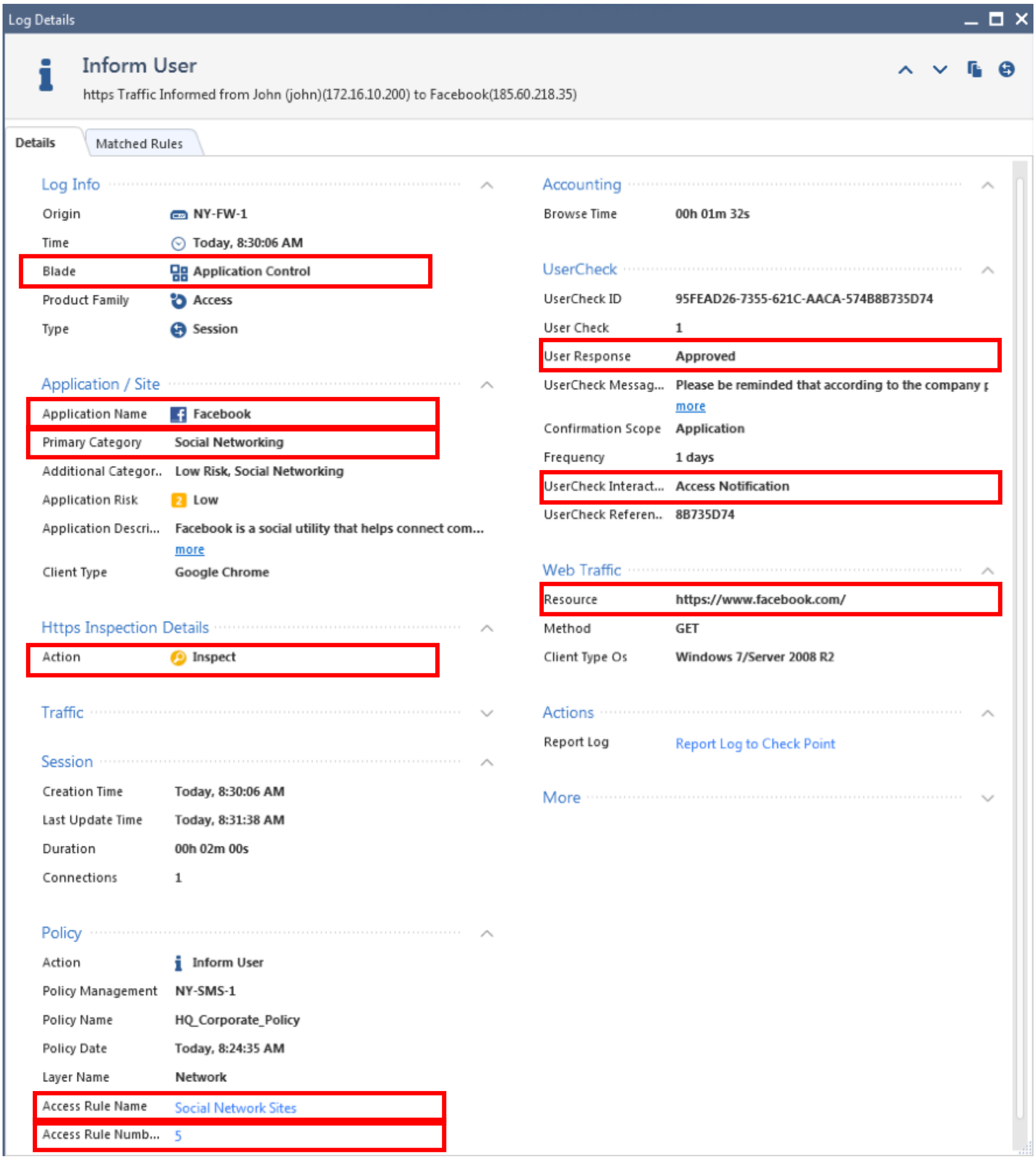
Last Hour action:"Inform User"

Found 2 results (313 ms)

Time	..	..	..	..	Origin	Source User...	Source	Destination	Rule	Rule Name	Policy Name	Description
Today, 8:30:06 AM		ℹ			NY-FW-1	John (john)	NY-LAN-1 (172.1...	edge-star-mi...	5	Social Network...	HQ_Corporate_...	https Traffic Informed from John (john)(172.16.10.200) to Facebook(185.60.218.35)
Today, 8:30:06 AM		ℹ			NY-FW-1	John (john)	NY-LAN-1 (172.1...	edge-star-mi...	5	Social Network...	HQ_Corporate_...	https Traffic Informed from John (john)(172.16.10.200) to 185.60.218.35

We will open the top log and take a look. Check Point Software Technologies is the cybersecurity leader in terms security technologies and management capabilities.

All information is available in one page, please take a look below:



Inform User

https Traffic Informed from John (john)(172.16.10.200) to Facebook(185.60.218.35)

Log Info

Origin	NY-FW-1
Time	Today, 8:30:06 AM
Blade	Application Control
Product Family	Access
Type	Session

Application / Site

Application Name	Facebook
Primary Category	Social Networking
Additional Categor..	Low Risk, Social Networking
Application Risk	2 Low
Application Descri...	Facebook is a social utility that helps connect com... more
Client Type	Google Chrome

Https Inspection Details

Action	Inspect

Traffic

Session

Creation Time	Today, 8:30:06 AM
Last Update Time	Today, 8:31:38 AM
Duration	00h 02m 00s
Connections	1

Policy

Action	Inform User
Policy Management	NY-SMS-1
Policy Name	HQ_Corporate_Policy
Policy Date	Today, 8:24:35 AM
Layer Name	Network
Access Rule Name	Social Network Sites
Access Rule Numb...	5

Accounting

Browse Time	00h 01m 32s

UserCheck

UserCheck ID	95FEAD26-7355-621C-AACA-574B8B735D74
User Check	1
User Response	Approved
UserCheck Messag...	Please be reminded that according to the company p more
Confirmation Scope	Application
Frequency	1 days
UserCheck Interact...	Access Notification
UserCheck Referen..	8B735D74

Web Traffic

Resource	https://www.facebook.com/
Method	GET
Client Type Os	Windows 7/Server 2008 R2

Actions

Report Log	Report Log to Check Point

More

35.0 Lab: Block Inappropriate Content (Gambling, Alcohol, etc)

Lab Objectives

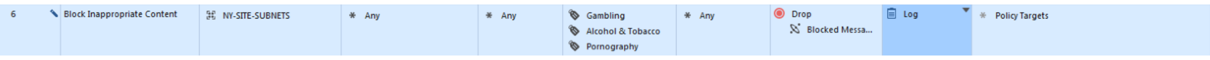
- Block Inappropriate Content (Gambling, Alcohol, etc)

Next, let’s define another rule, below rule 5 (so this will be rule 6), in order to block inappropriate content like gambling, alcohol, pornography.

Details of the new rule as follows:

- Name: Block Inappropriate Content
- Source: NY-SITE-SUBNETS
- Destination: Any
- Services & Applications: Categories – Gambling, Alcohol&Tobacco, Pornography
- Action: Drop – Blocked Message
- Track: Log

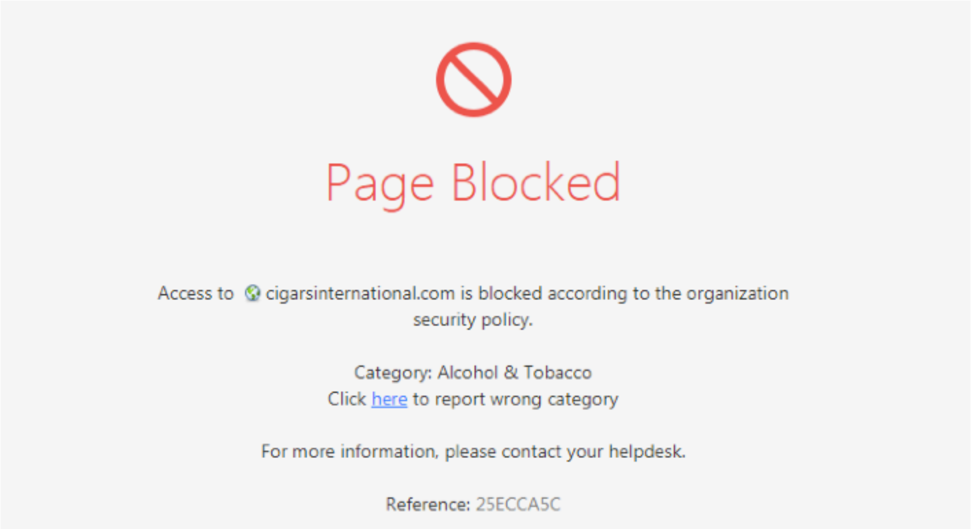
Right-click on number 5 in the first column and add this rule. Rule 6 should look as below:



6	Block Inappropriate Content	NY-SITE-SUBNETS	Any	Any	Gambling Alcohol & Tobacco Pornography	Any	Drop Blocked Messa...	Log	Policy Targets

Pretty easy, right? Let’s test this new rule, so first we need to **Publish** and **Install** the changes on NY-FW-1. We will try to access a website, that fits into Alcohol & Tobacco category and the request should be blocked, displaying a Blocked Message.

As expected, the page was blocked:



Page Blocked

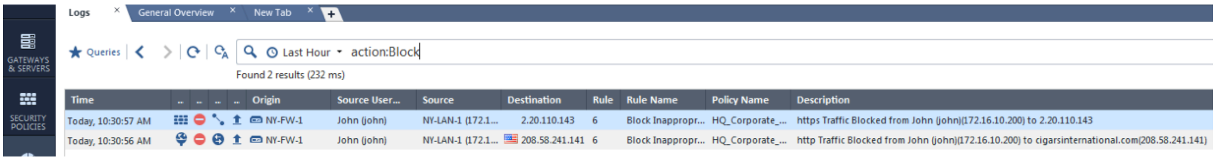
Access to cigarsinternational.com is blocked according to the organization security policy.

Category: Alcohol & Tobacco
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: 25ECCA5C

Let’s consult **Logs & Monitor** section, in order to identify the respective log. I have filtered the logs with **action:Block**, minimizing the output by selecting **Last Hour** logs:

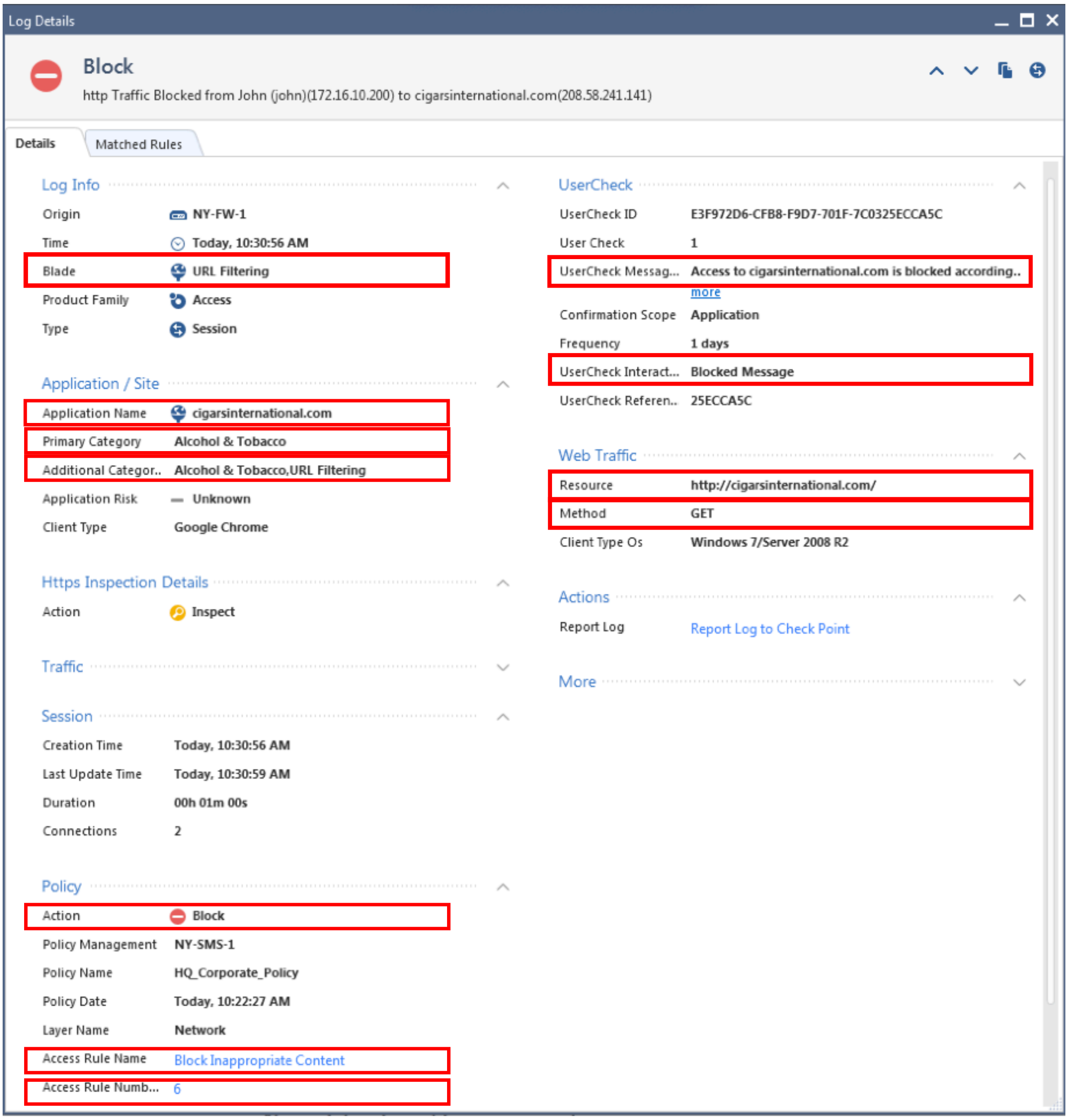


Last Hour action:Block

Found 2 results (232 ms)

Time	..	..	..	..	Origin	Source User...	Source	Destination	Rule	Rule Name	Policy Name	Description
Today, 10:30:57 AM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	2.20.110.143	6	Block Inappropr...	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to 2.20.110.143
Today, 10:30:56 AM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	208.58.241.141	6	Block Inappropr...	HQ_Corporate_...	http Traffic Blocked from John (john)(172.16.10.200) to cigarsinternational.com(208.58.241.141)

If you open the second log, you will see that all necessary information is available for analysis:



Block

http Traffic Blocked from John (john)(172.16.10.200) to cigarsinternational.com(208.58.241.141)

Log Info

Origin NY-FW-1
Time Today, 10:30:56 AM
Blade URL Filtering
Product Family Access
Type Session

Application / Site

Application Name cigarsinternational.com
Primary Category Alcohol & Tobacco
Additional Categor.. Alcohol & Tobacco,URL Filtering
Application Risk Unknown
Client Type Google Chrome

Https Inspection Details

Action Inspect

Traffic

Session

Creation Time Today, 10:30:56 AM
Last Update Time Today, 10:30:59 AM
Duration 00h 01m 00s
Connections 2

Policy

Action Block
Policy Management NY-SMS-1
Policy Name HQ_Corporate_Policy
Policy Date Today, 10:22:27 AM
Layer Name Network
Access Rule Name Block Inappropriate Content
Access Rule Numb... 6

UserCheck

UserCheck ID E3F972D6-CFB8-F9D7-701F-7C0325ECCA5C
User Check 1
UserCheck Messag... Access to cigarsinternational.com is blocked according..
more
Confirmation Scope Application
Frequency 1 days
UserCheck Interact... Blocked Message
UserCheck Referen.. 25ECCA5C

Web Traffic

Resource http://cigarsinternational.com/
Method GET
Client Type Os Windows 7/Server 2008 R2

Actions

Report Log Report Log to Check Point

More

36.0 Lab: Create Custom Application Object and Allow Access

Lab Objectives

- Define a custom application
- Define a new rule and allow access to the custom application (Remember Rule order is important!)

Let’s suppose that you need to provide access to an application or website that falls into the Alcohol and Tobacco category. How would you do that? Rule 6 is blocking access to these categories.

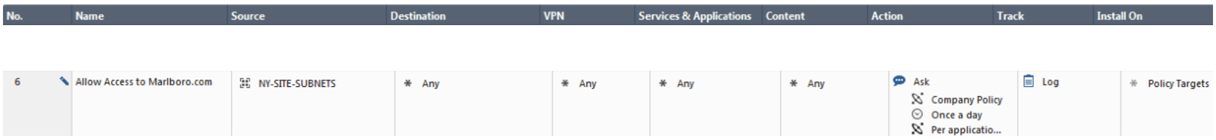
Remember that rule order is important and the traffic is analysed against the Rule base in a top-down fashion. This means that if you place a rule above rule 6, for example as rule 5, and permit traffic to this new website, then it will be allowed. The only thing is that rule 5 must be more specific than rule 6, in order to not override it.

As an example, let’s suppose that you want to **Allow** access to https://marlboro.com . This is a website that falls under **Alcohol & Tobacco** category, so we would need to create a new rule and place it before rule 6. We will create a custom application object now and include this URL – https://marlboro.com

Right-click on 6 and select **New Rule – Above.** Define the new rule as follows:

- Name: Allow Access to Marlboro.com
- Source: NY-SITE-SUBNETS
- Destination: Any
- Services & Applications: Marlboro
- Action: Ask – Company Policy, Once per day, Per Application
- Track: Log

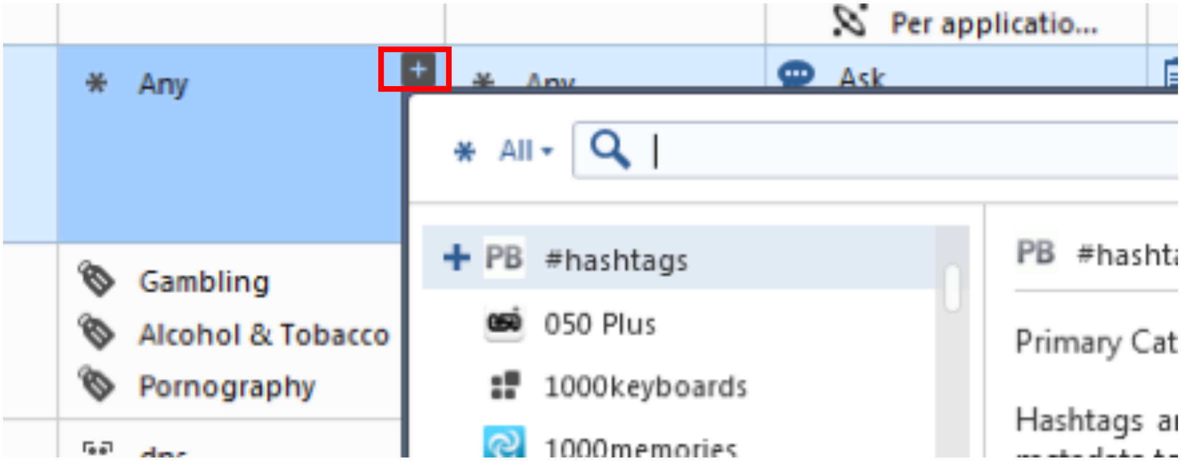
The new rule should look as the following:



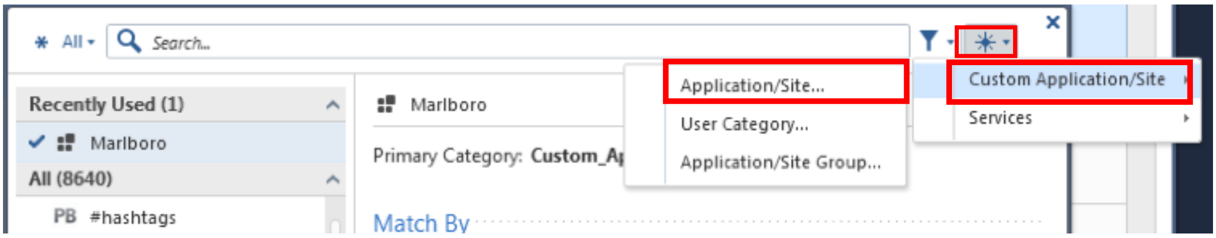
No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track	Install On
6	Allow Access to Marlboro.com	NY-SITE-SUBNETS	✱ Any	✱ Any	✱ Any	✱ Any	Ask Company Policy Once a day Per applicatio...	Log	✱ Policy Targets

In the **Services & Applications** tab we would need to create the custom application – Marlboro. Here is how we can do this.

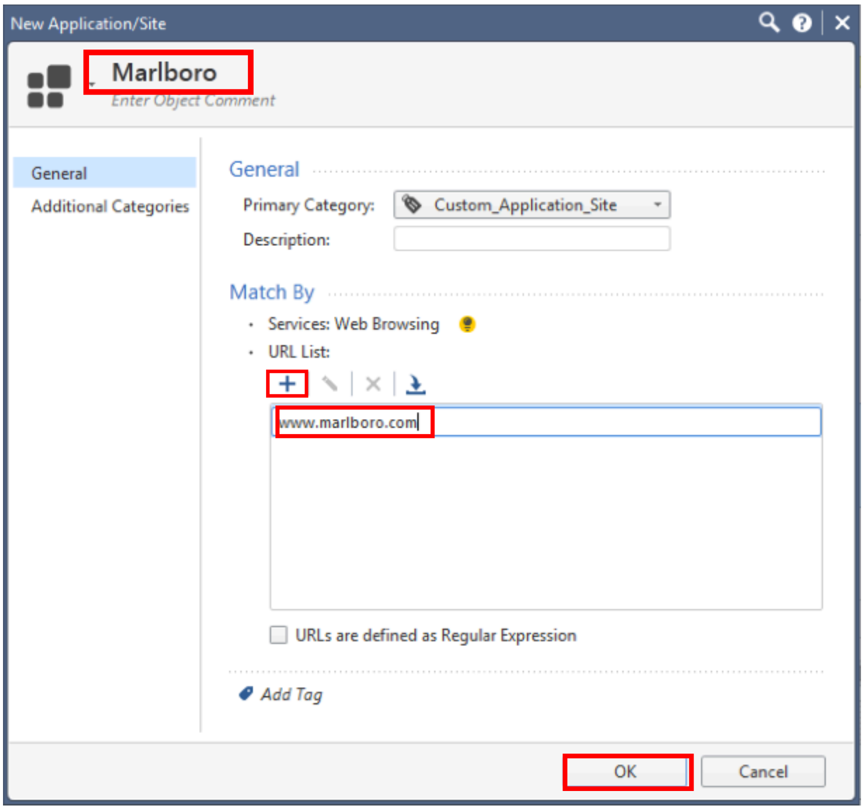
Click the **+** sign and a new window appears:



In this new window, click in the top-right corner on the asterisk button and select **Custom Application/Site** and then **Application/Site**:



Enter **Marlboro** for the application name and click the **+** sign in order to add the URL to www.marlboro.com website:



Marlboro

General

Primary Category: Custom_Application_Site

Description:

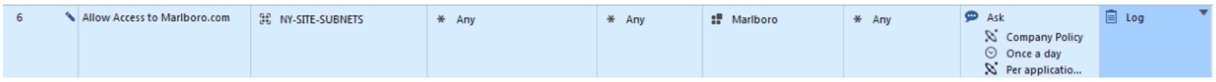
Match By

- Services: Web Browsing
- URL List:

www.marlboro.com

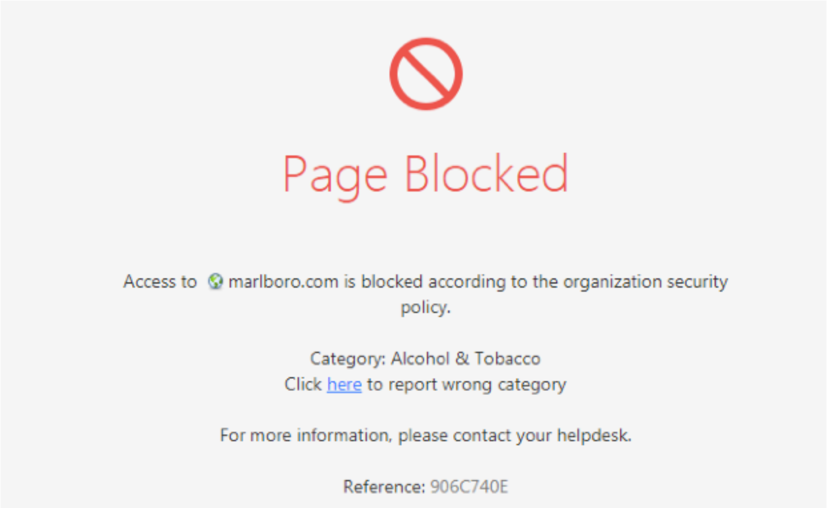
□ URLs are defined as Regular Expression

The new rule, rule 6, should now look as follows:



6	Allow Access to Marlboro.com	NY-SITE-SUBNETS	Any	Any	Marlboro	Any	Ask Company Policy Once a day Per applicatio...	Log

Let's test access to https://marlboro.com before and after installing the policy. Now access is being blocked:



Page Blocked

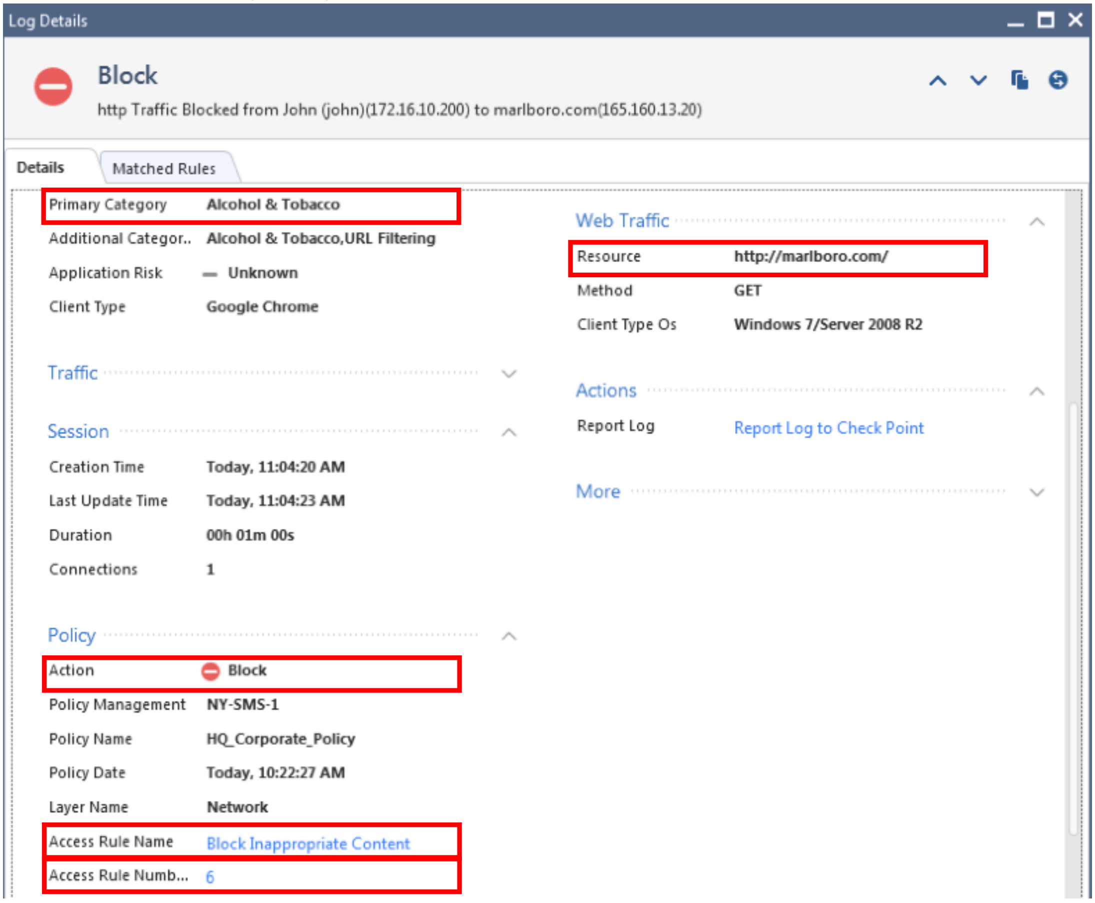
Access to marlboro.com is blocked according to the organization security policy.

Category: Alcohol & Tobacco
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: 906C740E

and we can see from the associated log that this traffic matched under current rule 6 – before new policy installation:



Block
http Traffic Blocked from John (john)(172.16.10.200) to marlboro.com(165.160.13.20)

Primary Category	Alcohol & Tobacco
Additional Categor..	Alcohol & Tobacco,URL Filtering
Application Risk	— Unknown
Client Type	Google Chrome

Traffic

Session

Creation Time	Today, 11:04:20 AM
Last Update Time	Today, 11:04:23 AM
Duration	00h 01m 00s
Connections	1

Policy

Action	Block
Policy Management	NY-SMS-1
Policy Name	HQ_Corporate_Policy
Policy Date	Today, 10:22:27 AM
Layer Name	Network
Access Rule Name	Block Inappropriate Content
Access Rule Numb...	6

Web Traffic

Resource	http://marlboro.com/
Method	GET
Client Type Os	Windows 7/Server 2008 R2

Actions

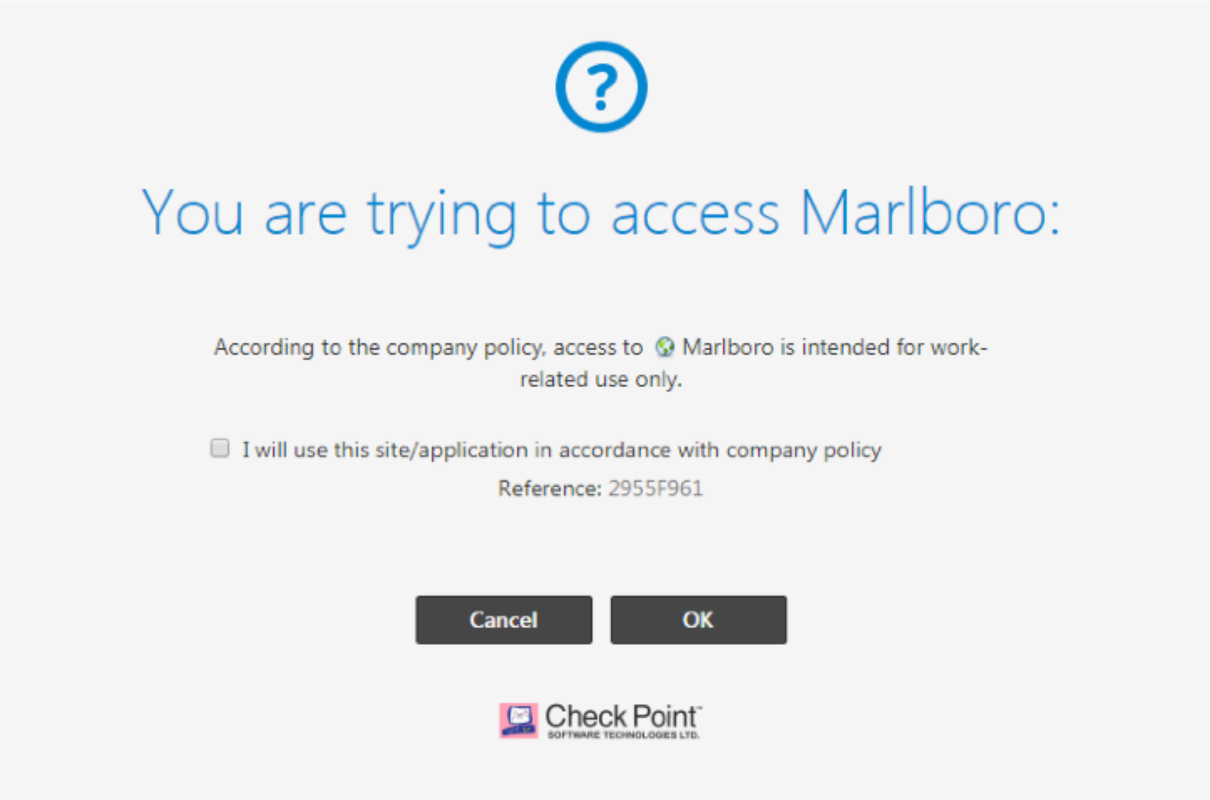
Report Log	Report Log to Check Point

More

Now, let’s publish changes and install the policy and observe the changes.

I will refresh the browser and hopefully the page will load now.

Now when you try to access **Marlboro.com** you will be presented a message, similar to the following:



You are trying to access Marlboro:

According to the company policy, access to Marlboro is intended for work-related use only.

□ I will use this site/application in accordance with company policy

Reference: 2955F961

Just tick the box, click **OK** and access should be allowed access now.

37.0 Lab: Content Awareness - Block Download of Specific Files

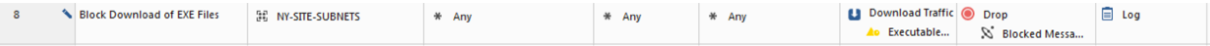
Lab Objectives

- Prevent malicious content entering the organization
- Block download of *.exe files

Let’s make sure that we block download of executable files into our organization. We will now define a rule, considering the following:

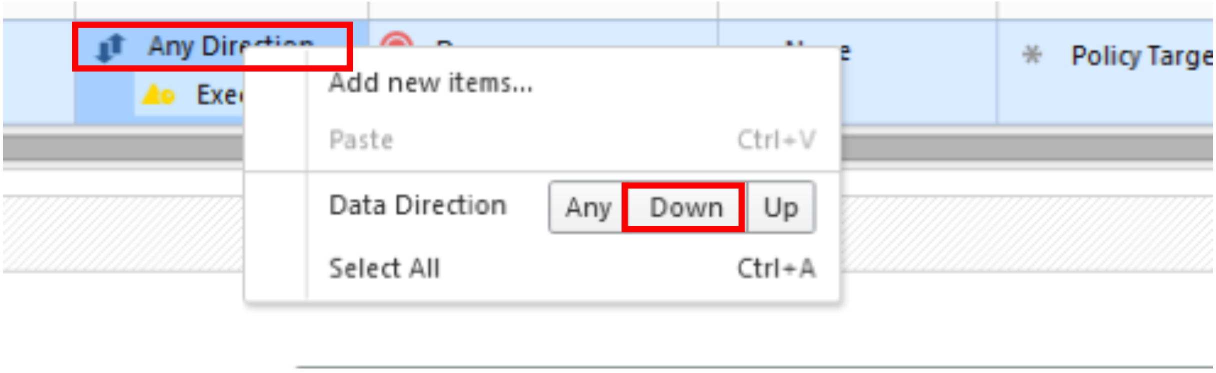
- Name: Block Download of EXE Files
- Source: NY-SITE-SUBNETS
- Destination: Any
- Content: Download Traffic – Executable Files
- Action: Drop – Blocked Message
- Track: Log

Let’s add this rule after rule 7, making this rule 8. When done, it should look like the following:

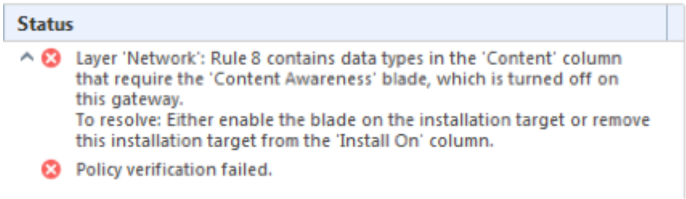


8	Block Download of EXE Files	NY-SITE-SUBNETS	Any	Any	Any	Download Traffic Executable...	Drop Blocked Messa...	Log

Select **Executable File** in the Content column and modify the direction to **Download.** Right-click on **Any Direction** and select **Down.**



In order to enforce the changes, **Publish** and **Install** the policy. Policy installation fails and we get this error message:

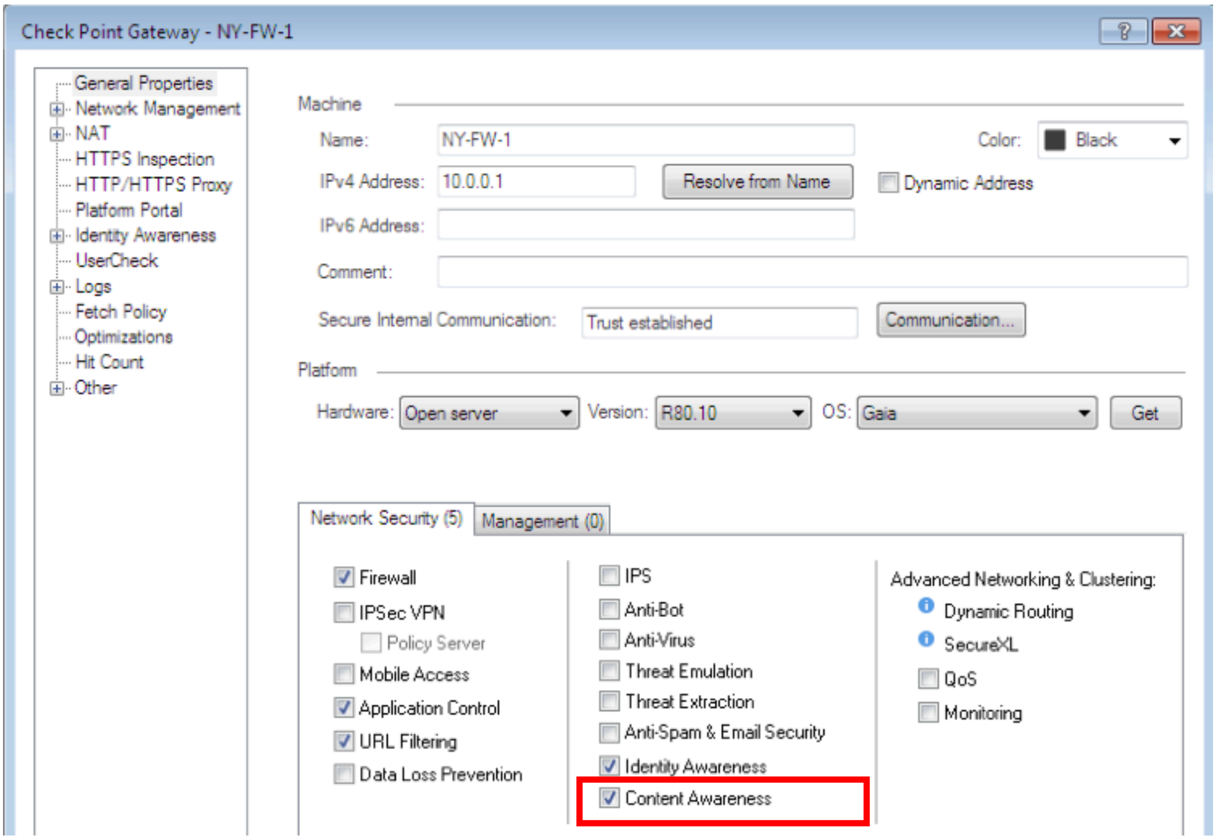


Status

Layer 'Network': Rule 8 contains data types in the 'Content' column that require the 'Content Awareness' blade, which is turned off on this gateway.
To resolve: Either enable the blade on the installation target or remove this installation target from the 'Install On' column.

Policy verification failed.

Let’s enable **Content Awareness** at the gateway level. Open NY-FW-1 and select this blade in order to activate it.



Machine

Name: NY-FW-1 Color: Black

IPv4 Address: 10.0.0.1 □ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server Version: R80.10 OS: Gaia

Network Security (5) | Management (0)

- ☑ Firewall
- □ IPSec VPN
  - □ Policy Server
- □ Mobile Access
- ☑ Application Control
- ☑ URL Filtering
- □ Data Loss Prevention
- □ IPS
- □ Anti-Bot
- □ Anti-Virus
- □ Threat Emulation
- □ Threat Extraction
- □ Anti-Spam & Email Security
- ☑ Identity Awareness
- ☑ Content Awareness

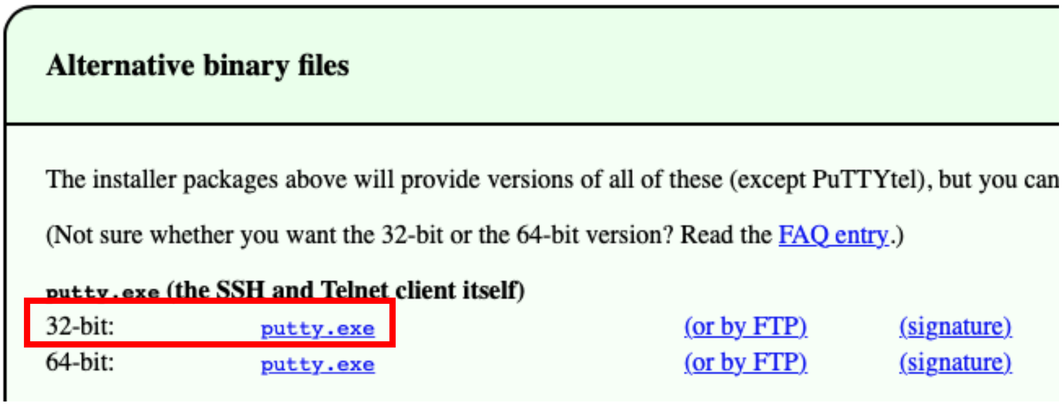
Advanced Networking & Clustering:
- Dynamic Routing
- SecureXL
- □ QoS
- □ Monitoring

Now, when we publish and install the policy, it succeeds, so when proceed with testing. Let’s test the new rule.

We will try to download Putty, a popular ssh client for windows. Just navigate to this link:

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

scroll down and try to download **putty.exe**:



Alternative binary files

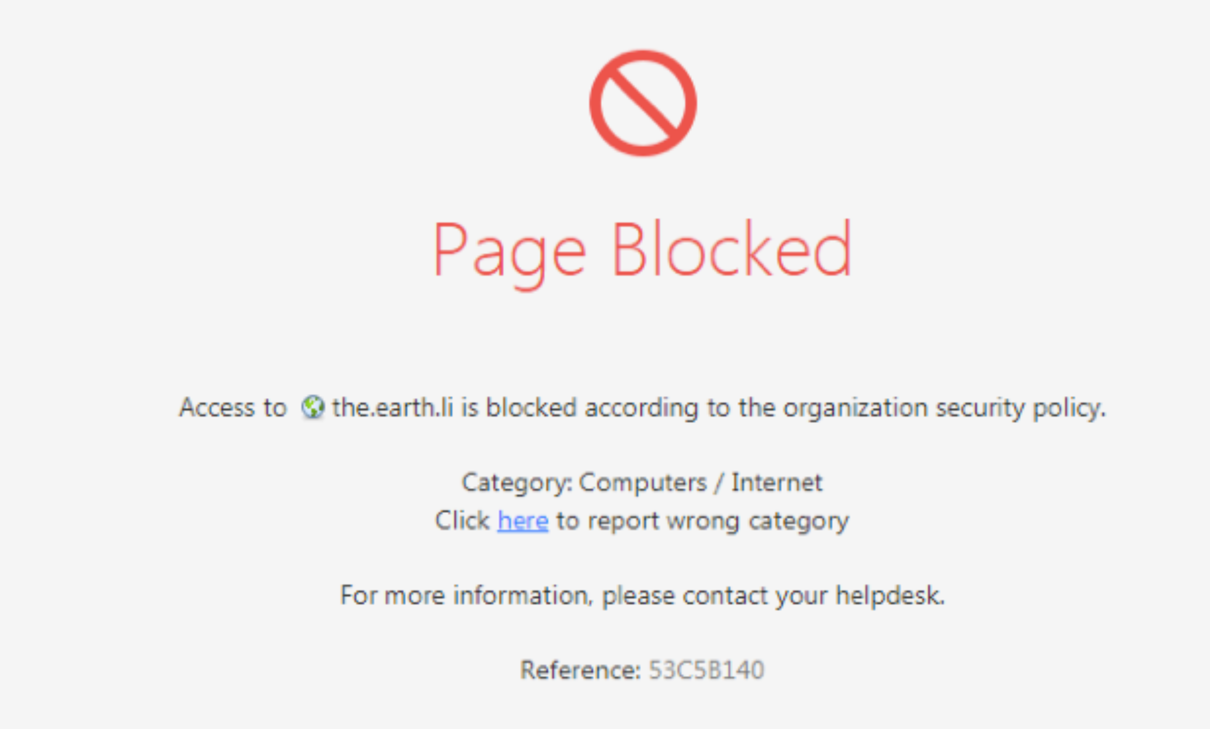
The installer packages above will provide versions of all of these (except PuTTYtel), but you can

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

putty.exe (the SSH and Telnet client itself)

32-bit:	putty.exe	(or by FTP)	(signature)
64-bit:	putty.exe	(or by FTP)	(signature)

The download will be blocked:



Page Blocked

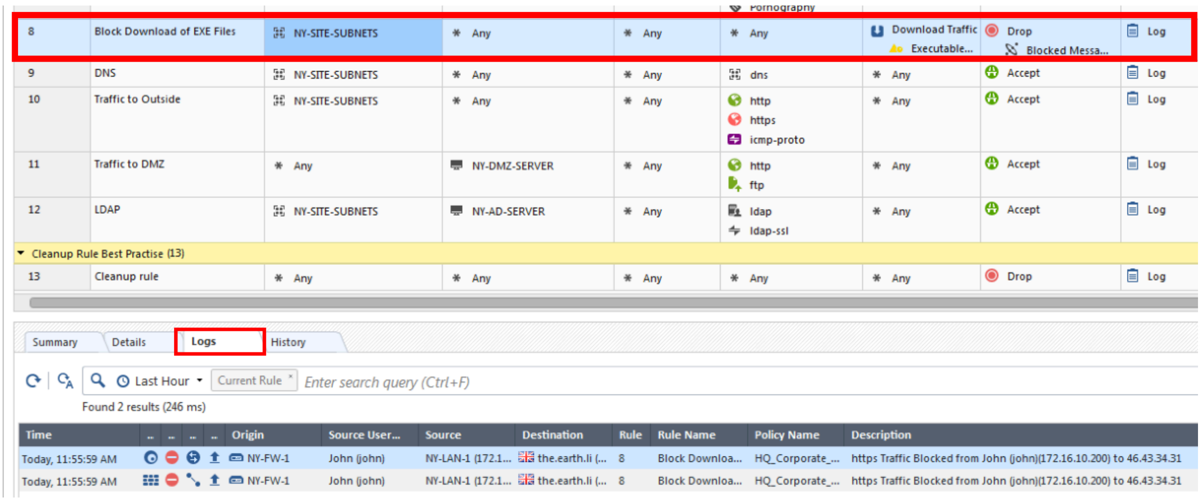
Access to the.earth.li is blocked according to the organization security policy.

Category: Computers / Internet
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: 53C5B140

Here is another method to analyse logs, but probably a more efficient one. While in the **Security Policies**, just click on the new rule added, rule 8, and select at the bottom the **Logs** menu. You will see here just logs that matched this rule:

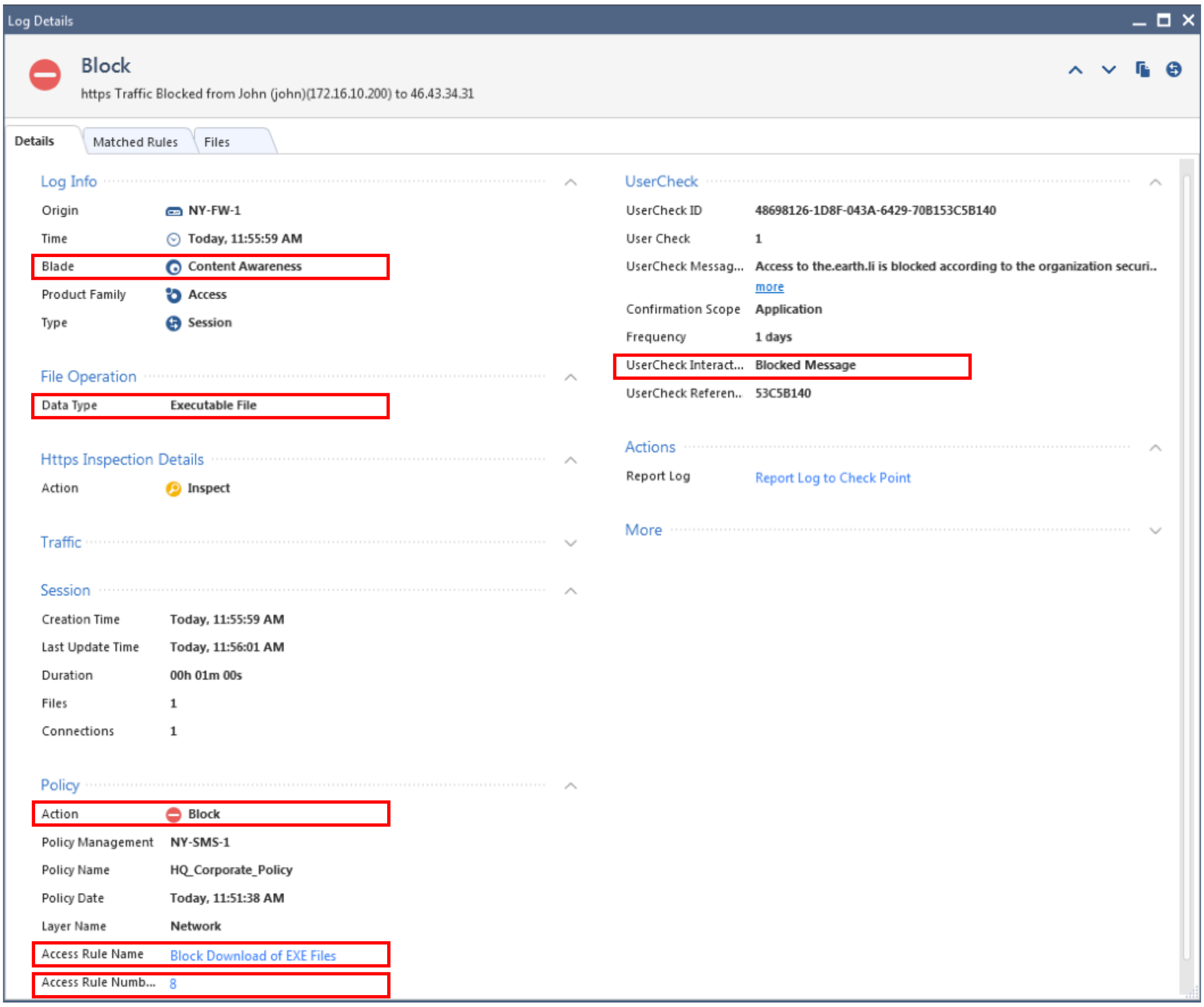


					Pornography			
8	Block Download of EXE Files	NY-SITE-SUBNETS	Any	Any	Any	Download Traffic Executable...	Drop Blocked Messa...	Log
9	DNS	NY-SITE-SUBNETS	Any	Any	dns	Any	Accept	Log
10	Traffic to Outside	NY-SITE-SUBNETS	Any	Any	http https icmp-proto	Any	Accept	Log
11	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Any	Accept	Log
12	LDAP	NY-SITE-SUBNETS	NY-AD-SERVER	Any	ldap ldap-ssl	Any	Accept	Log
Cleanup Rule Best Practise (13)								
13	Cleanup rule	Any	Any	Any	Any	Any	Drop	Log

Found 2 results (246 ms)

Time	..	..	..	..	Origin	Source User...	Source	Destination	Rule	Rule Name	Policy Name	Description
Today, 11:55:59 AM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	the.earth.li (...	8	Block Downloa...	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to 46.43.34.31
Today, 11:55:59 AM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	the.earth.li (...	8	Block Downloa...	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to 46.43.34.31

Let’s open one of the logs and take a closer look:



Block

https Traffic Blocked from John (john)(172.16.10.200) to 46.43.34.31

Log Info

Origin	NY-FW-1
Time	Today, 11:55:59 AM
Blade	Content Awareness
Product Family	Access
Type	Session

File Operation

Data Type	Executable File

Https Inspection Details

Action	Inspect

Traffic

Session

Creation Time	Today, 11:55:59 AM
Last Update Time	Today, 11:56:01 AM
Duration	00h 01m 00s
Files	1
Connections	1

Policy

Action	Block
Policy Management	NY-SMS-1
Policy Name	HQ_Corporate_Policy
Policy Date	Today, 11:51:38 AM
Layer Name	Network
Access Rule Name	Block Download of EXE Files
Access Rule Numb...	8

UserCheck

UserCheck ID	48698126-1D8F-043A-6429-70B153C5B140
User Check	1
UserCheck Messag...	Access to the.earth.li is blocked according to the organization securi.. more
Confirmation Scope	Application
Frequency	1 days
UserCheck Interact...	Blocked Message
UserCheck Referen..	53C5B140

Actions

Report Log	Report Log to Check Point

More

This log answers to the following questions:

- Which Check Point blade generated this log?
- What is the Data Type?
- What was the Action?
- Which Rule was the traffic matched on?
- What is the Rule number?
- What UserCheck message was displayed?

Great logging and reporting from Check Point.

38.0 Lab: Data Loss Prevention - Block Upload of PCI Credit Card Numbers

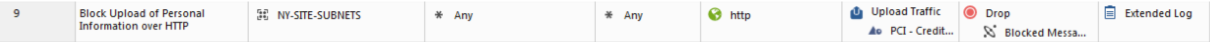
Lab Objectives

- Prevent uploading of personal information over HTTP – DLP

Details for the new rule, rule9, as follows:

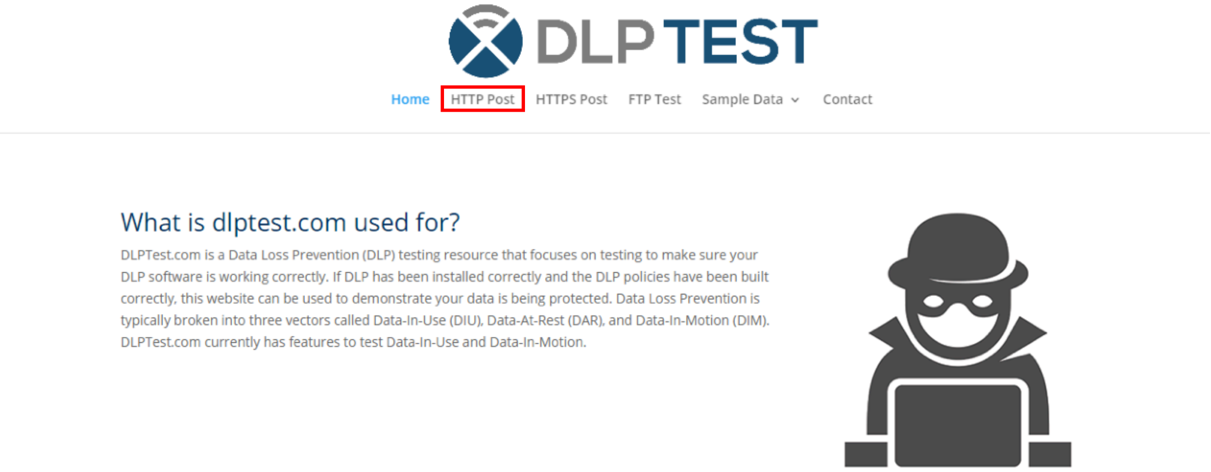
- Name: Block Upload of Personal Information over HTTP
- Source: NY-SITE-SUBNETS
- Destination: Any
- Content: Upload Traffic – PCI – Credit Card Numbers
- Services & Applications: HTTP
- Action: Drop – Blocked Message
- Track: Extended Log

Rule 9 should like as you can see below:



9	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	✱ Any	✱ Any	http	Upload Traffic PCI - Credit...	Drop Blocked Messa...	Extended Log

In order to test the new rule, please navigate to https://dlptest.com

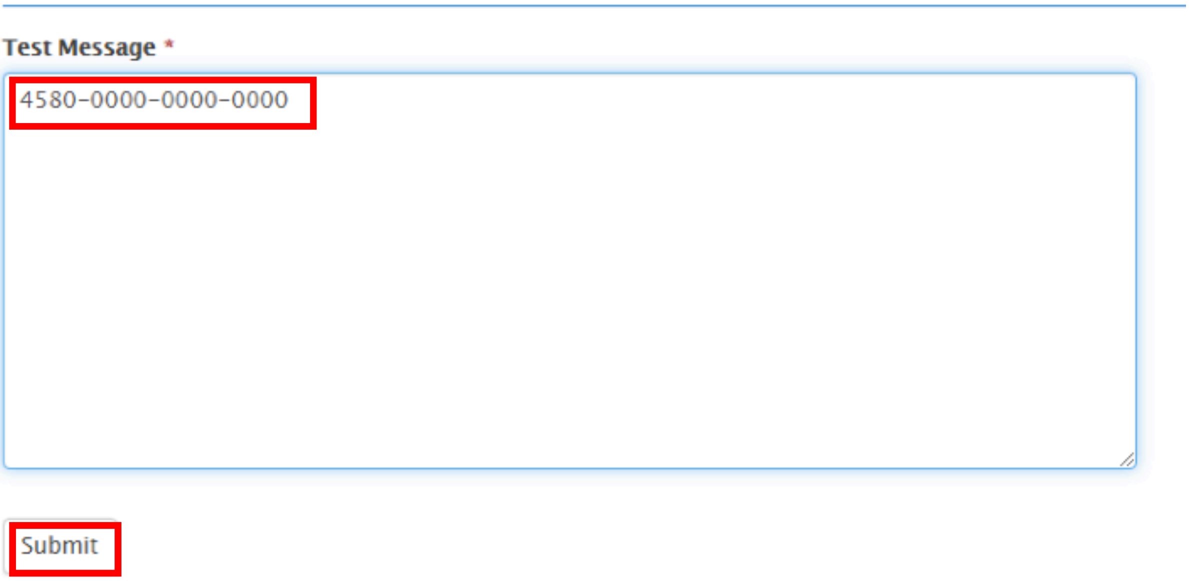


What is dlptest.com used for?

DLPTest.com is a Data Loss Prevention (DLP) testing resource that focuses on testing to make sure your DLP software is working correctly. If DLP has been installed correctly and the DLP policies have been built correctly, this website can be used to demonstrate your data is being protected. Data Loss Prevention is typically broken into three vectors called Data-In-Use (DIU), Data-At-Rest (DAR), and Data-In-Motion (DIM). DLPTest.com currently has features to test Data-In-Use and Data-In-Motion.

and select **HTTP Post** from the top menu.

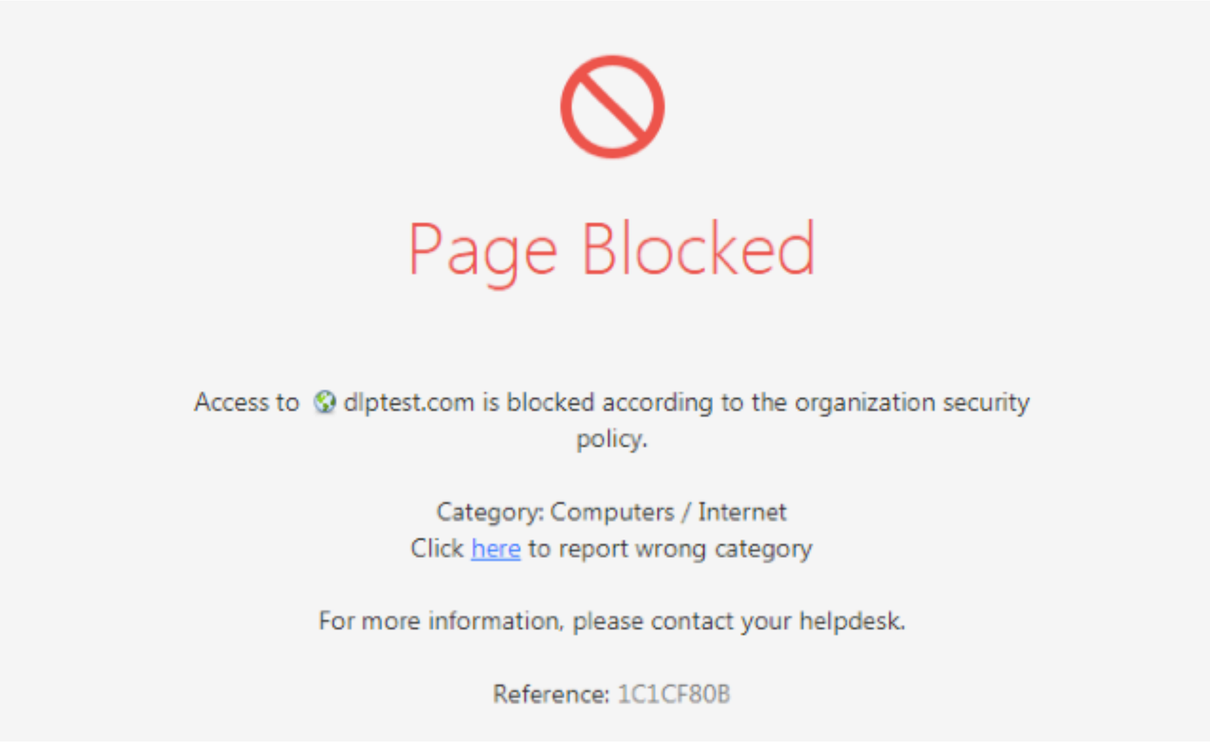
We will simulate that we enter a Credit Card Number in the **Text Message** box and then click **Submit**.



Test Message *

4580-0000-0000-0000

The upload is blocked and the **Blocked Message** is displayed:



Page Blocked

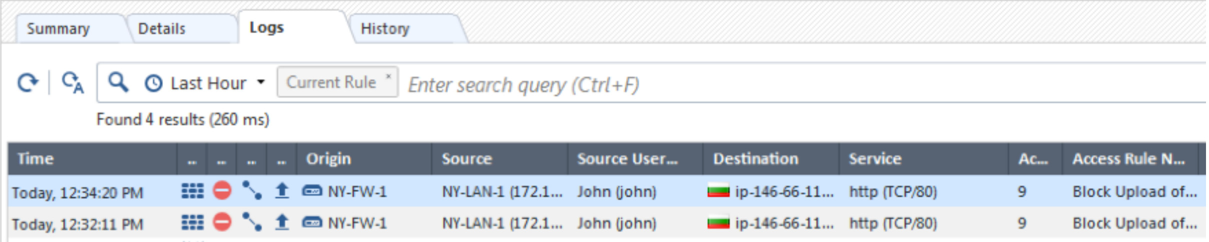
Access to dlptest.com is blocked according to the organization security policy.

Category: Computers / Internet
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: 1C1CF80B

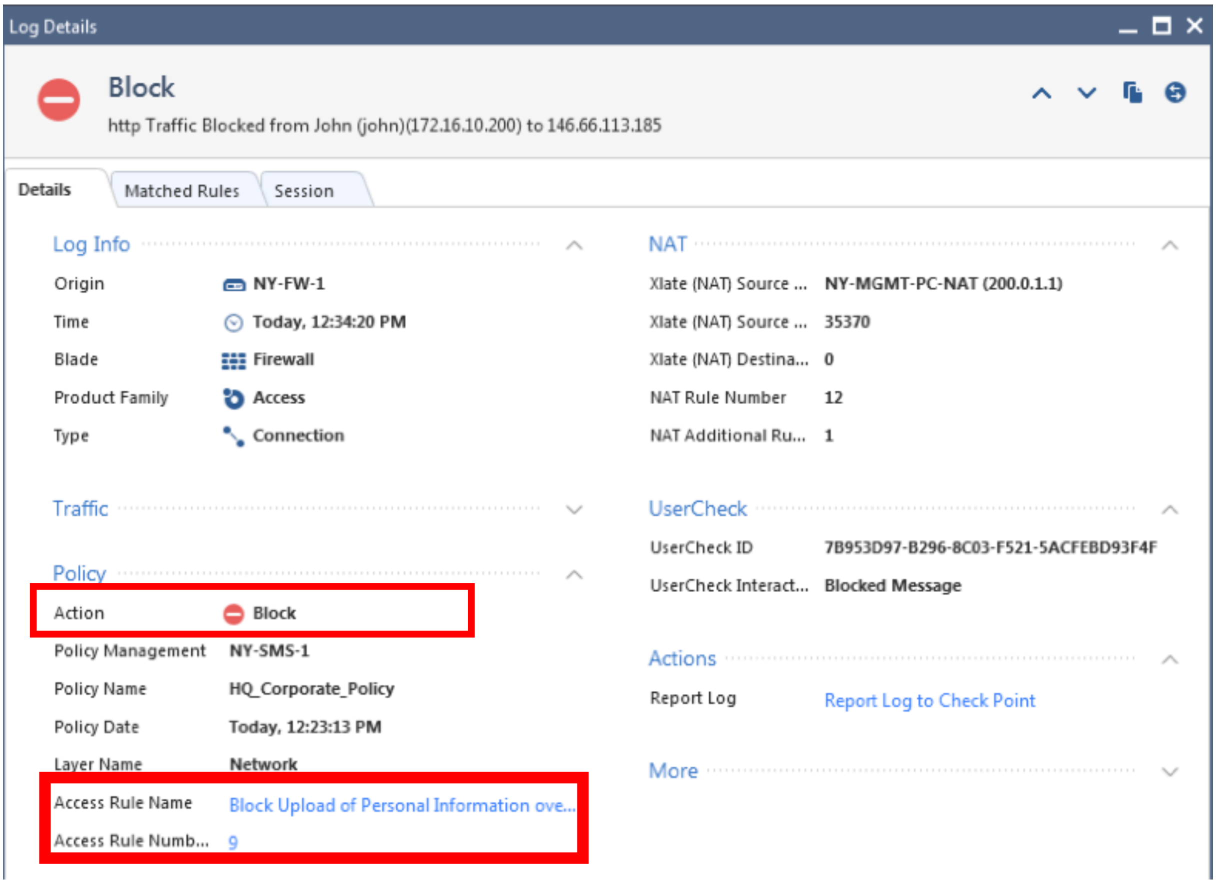
Here are the corresponding logs:



Found 4 results (260 ms)

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 12:34:20 PM		⛔		↑	NY-FW-1	NY-LAN-1 (172.1...	John (john)	ip-146-66-11...	http (TCP/80)	9	Block Upload of...
Today, 12:32:11 PM		⛔		↑	NY-FW-1	NY-LAN-1 (172.1...	John (john)	ip-146-66-11...	http (TCP/80)	9	Block Upload of...

And one of the logs:



Log Details

Block

http Traffic Blocked from John (john)(172.16.10.200) to 146.66.113.185

Log Info

Origin NY-FW-1
Time Today, 12:34:20 PM
Blade Firewall
Product Family Access
Type Connection

Traffic

Policy

Action Block
Policy Management NY-SMS-1
Policy Name HQ_Corporate_Policy
Policy Date Today, 12:23:13 PM
Layer Name Network
Access Rule Name Block Upload of Personal Information ove...
Access Rule Numb... 9

NAT

Xlate (NAT) Source ... NY-MGMT-PC-NAT (200.0.1.1)
Xlate (NAT) Source ... 35370
Xlate (NAT) Destina... 0
NAT Rule Number 12
NAT Additional Ru... 1

UserCheck

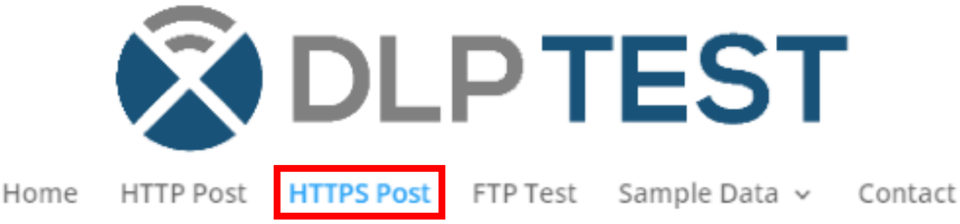
UserCheck ID 7B953D97-B296-8C03-F521-5ACFEBD93F4F
UserCheck Interact... Blocked Message

Actions

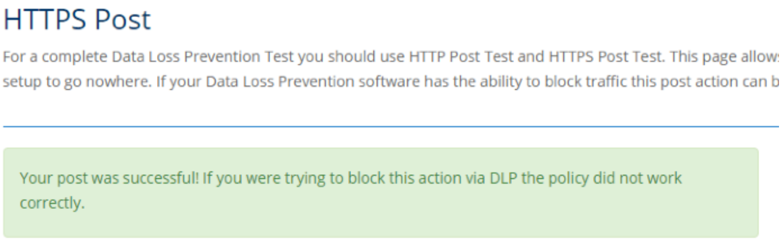
Report Log Report Log to Check Point

More

If you try the upload over HTTPS, then it will work:



HTTP is not secure, so that's the reason we are blocking this type of uploading. HTTPS (HTTP SECURE) is a reliable option in case uploading PCI – Credit Card Numbers is needed, so it needs to work.



HTTPS Post

For a complete Data Loss Prevention Test you should use HTTP Post Test and HTTPS Post Test. This page allow: setup to go nowhere. If your Data Loss Prevention software has the ability to block traffic this post action can b

Your post was successful! If you were trying to block this action via DLP the policy did not work correctly.

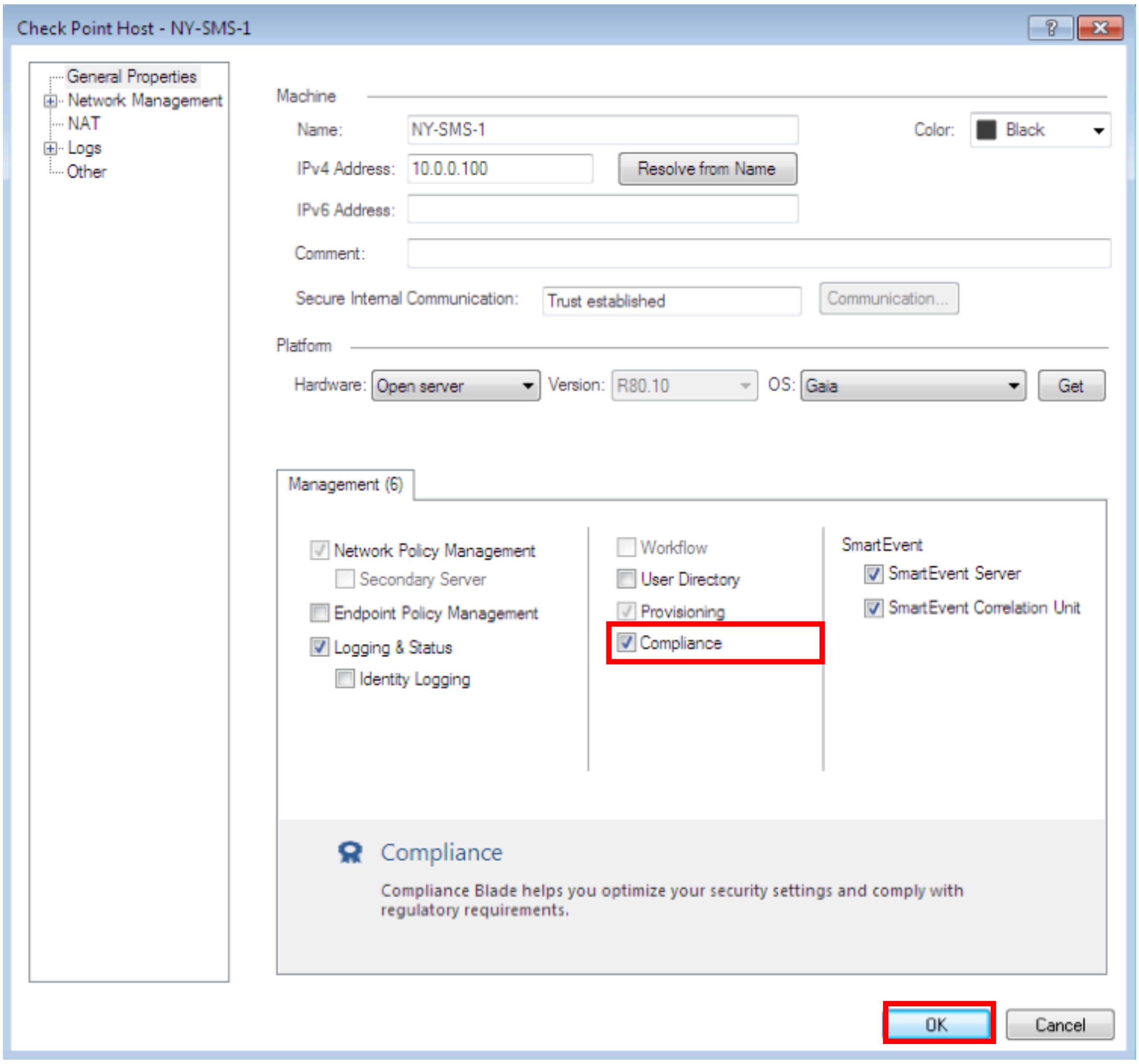
39.0 Lab: Activate Compliance Blade and Compare Policy to Industry Best Practices

Lab Objectives

- Activate Compliance Software Blade on Management Server
- Compare current policy to Industry Security Best Practices

Check Point Compliance Software Blade helps you optimize your security settings and comply with regulatory requirements. This software blade is activated at the management server level, so this is what we will do next.

While in **Gateways & Servers,** open **NY-SMS-1** object and select **Compliance** blade.



Check Point Host - NY-SMS-1

Machine

Name: NY-SMS-1

IPv4 Address: 10.0.0.100

IPv6 Address:

Comment:

Color: Black

Secure Internal Communication: Trust established

Platform

Hardware: Open server

Version: R80.10

OS: Gaia

Management (6)

- ☑ Network Policy Management
- □ Secondary Server
- □ Endpoint Policy Management
- ☑ Logging & Status
- □ Identity Logging
- □ Workflow
- □ User Directory
- ☑ Provisioning
- ☑ Compliance

SmartEvent

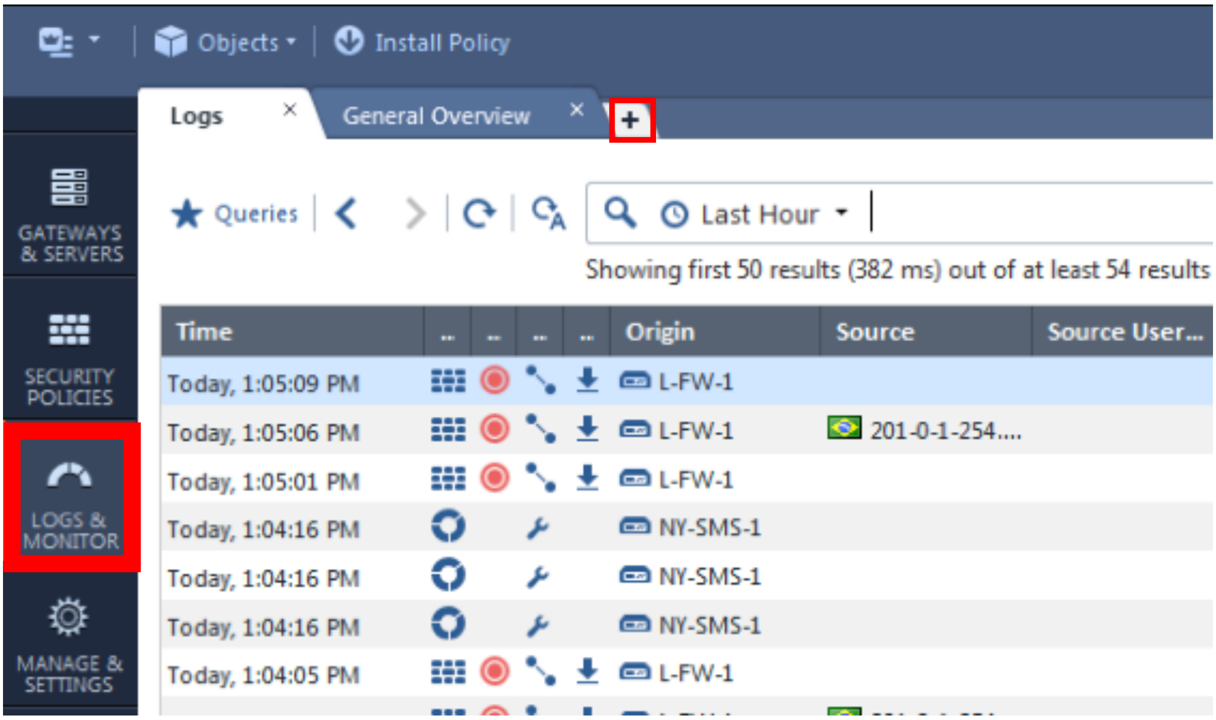
- ☑ SmartEvent Server
- ☑ SmartEvent Correlation Unit

Compliance

Compliance Blade helps you optimize your security settings and comply with regulatory requirements.

Click **OK** in order to confirm the changes. **Publish** the changes and **Install** the policy.

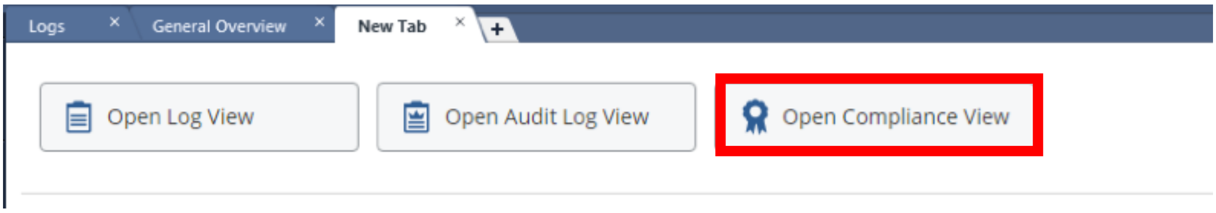
Now let's take a look at what information is available after activating the **Compliance** blade. Go to **Logs & Monitor**, click the **+** sign in order to open a new tab:



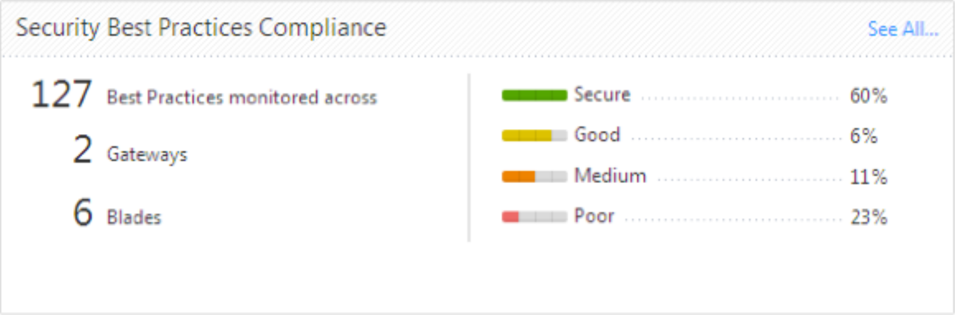
Showing first 50 results (382 ms) out of at least 54 results

Time	...	...	...	...	Origin	Source	Source User...
Today, 1:05:09 PM					L-FW-1		
Today, 1:05:06 PM					L-FW-1	201-0-1-254....	
Today, 1:05:01 PM					L-FW-1		
Today, 1:04:16 PM					NY-SMS-1		
Today, 1:04:16 PM					NY-SMS-1		
Today, 1:04:16 PM					NY-SMS-1		
Today, 1:04:05 PM					L-FW-1		

Now, please click on **Open Compliance View**.



We can now see how is our security implemented as opposed to industry best practices.



Security Best Practices Compliance

127 Best Practices monitored across

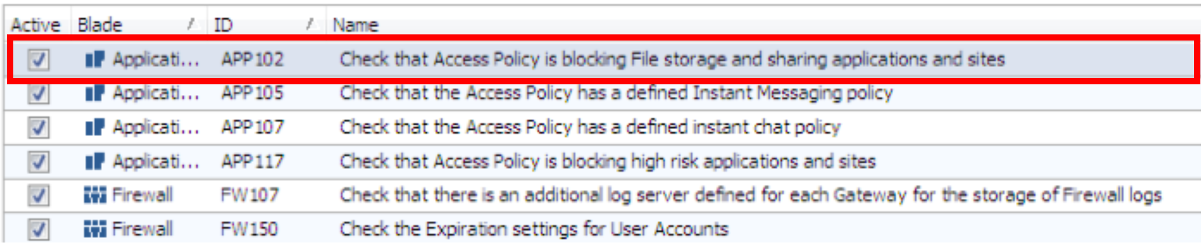
2 Gateways

6 Blades

Secure	60%
Good	6%
Medium	11%
Poor	23%

There are 127 best practices being monitored and we have 2 security gateways, with 6 blades activated. We can click on **Poor** and understand more what could be fixed in order to increase our security level.

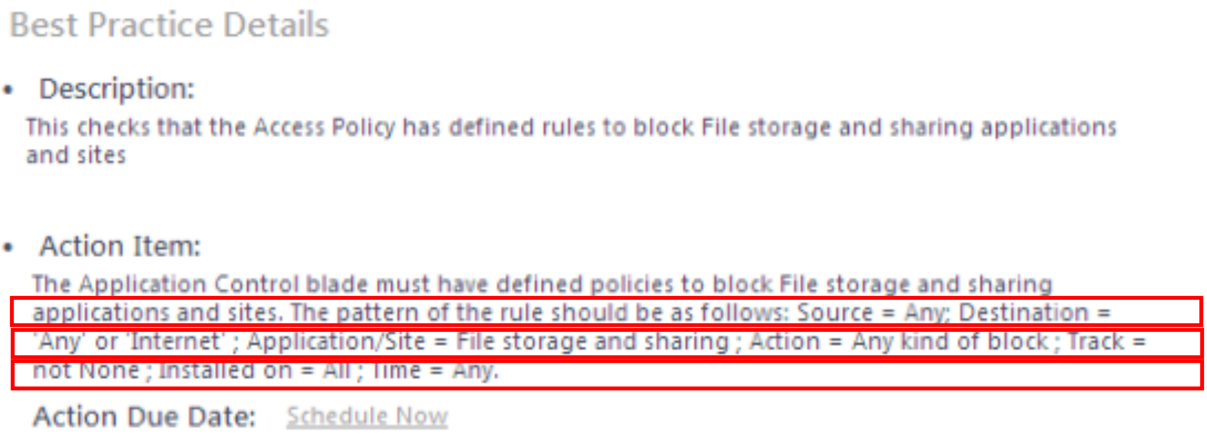
As an example, let's take the first one in the list:



Active	Blade	ID	Name
☑	Applicati...	APP102	Check that Access Policy is blocking File storage and sharing applications and sites
☑	Applicati...	APP105	Check that the Access Policy has a defined Instant Messaging policy
☑	Applicati...	APP107	Check that the Access Policy has a defined instant chat policy
☑	Applicati...	APP117	Check that Access Policy is blocking high risk applications and sites
☑	Firewall	FW107	Check that there is an additional log server defined for each Gateway for the storage of Firewall logs
☑	Firewall	FW150	Check the Expiration settings for User Accounts

At the bottom, detailed explanation is provided, but also a solution to fix the problem.

1. What are the Best Practices?

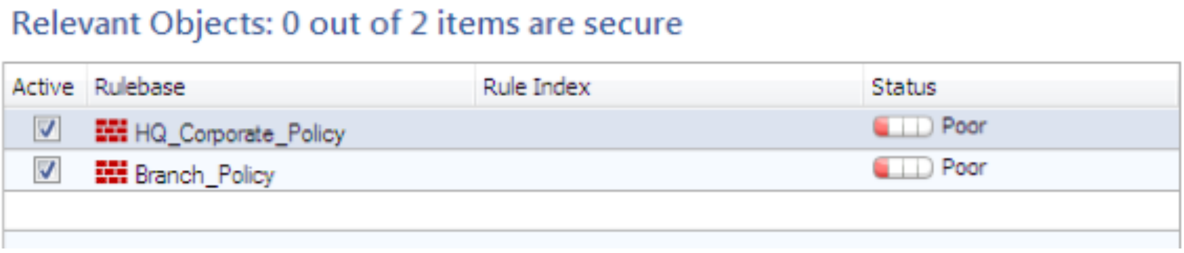


Best Practice Details

- Description:
  This checks that the Access Policy has defined rules to block File storage and sharing applications and sites
- Action Item:
  The Application Control blade must have defined policies to block File storage and sharing applications and sites. The pattern of the rule should be as follows: Source = Any; Destination = 'Any' or 'Internet' ; Application/Site = File storage and sharing ; Action = Any kind of block ; Track = not None ; Installed on = All ; Time = Any.

  Action Due Date: Schedule Now

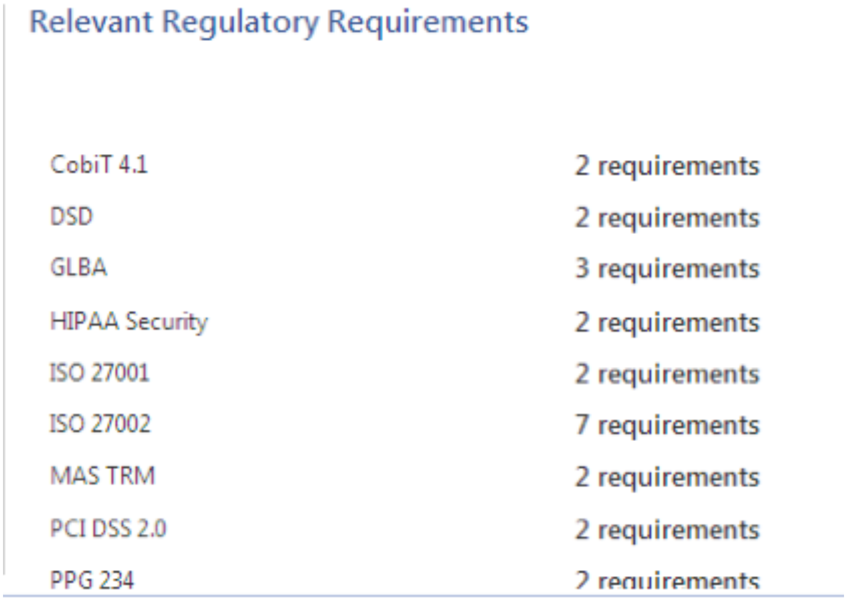
2. Where should I install the new policy containing the NEW recommended rule?



Relevant Objects: 0 out of 2 items are secure

Active	Rulebase	Rule Index	Status
☑	HQ_Corporate_Policy		Poor
☑	Branch_Policy		Poor

3. What are the relevant regulatory requirements that need this change to be implemented?



Relevant Regulatory Requirements

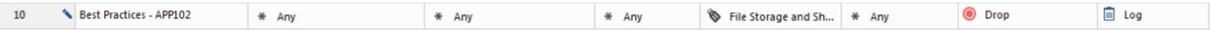
CobiT 4.1	2 requirements
DSD	2 requirements
GLBA	3 requirements
HIPAA Security	2 requirements
ISO 27001	2 requirements
ISO 27002	7 requirements
MAS TRM	2 requirements
PCI DSS 2.0	2 requirements
PPG 234	2 requirements

Let’s create another rule, rule 10 (after rule 9 that we have just defined), in order to implement this best practice. The rule details are provided in the **Action Items** above, under Question 1.

The details for Rule 10:

- Source: Any
- Destination: Any
- Application/Site: File storage and sharing
- Action: Block
- Track: Log

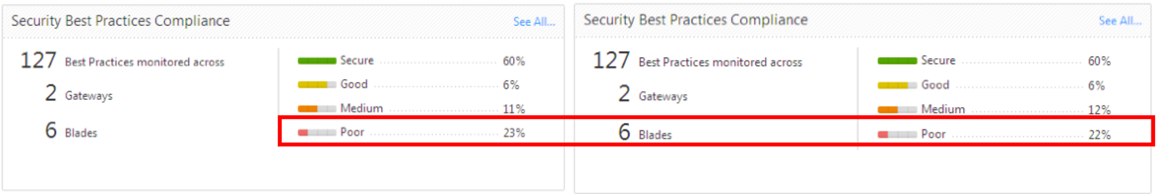
Here is how the new rule should look like:



10	Best Practices - APP102	Any	Any	Any	File Storage and Sh...	Any	Drop	Log

Publish and **Install** the HQ_Corporate_Policy.

Let’s take a look again at the Compliance View. On the left-side you can see the view before implementing the change, on the right-side the new view. We can see that we improved the security level from 23% Poor to 22% Poor, so we lowered the problem surface.



Security Best Practices Compliance — See All...

127 Best Practices monitored across
2 Gateways
6 Blades

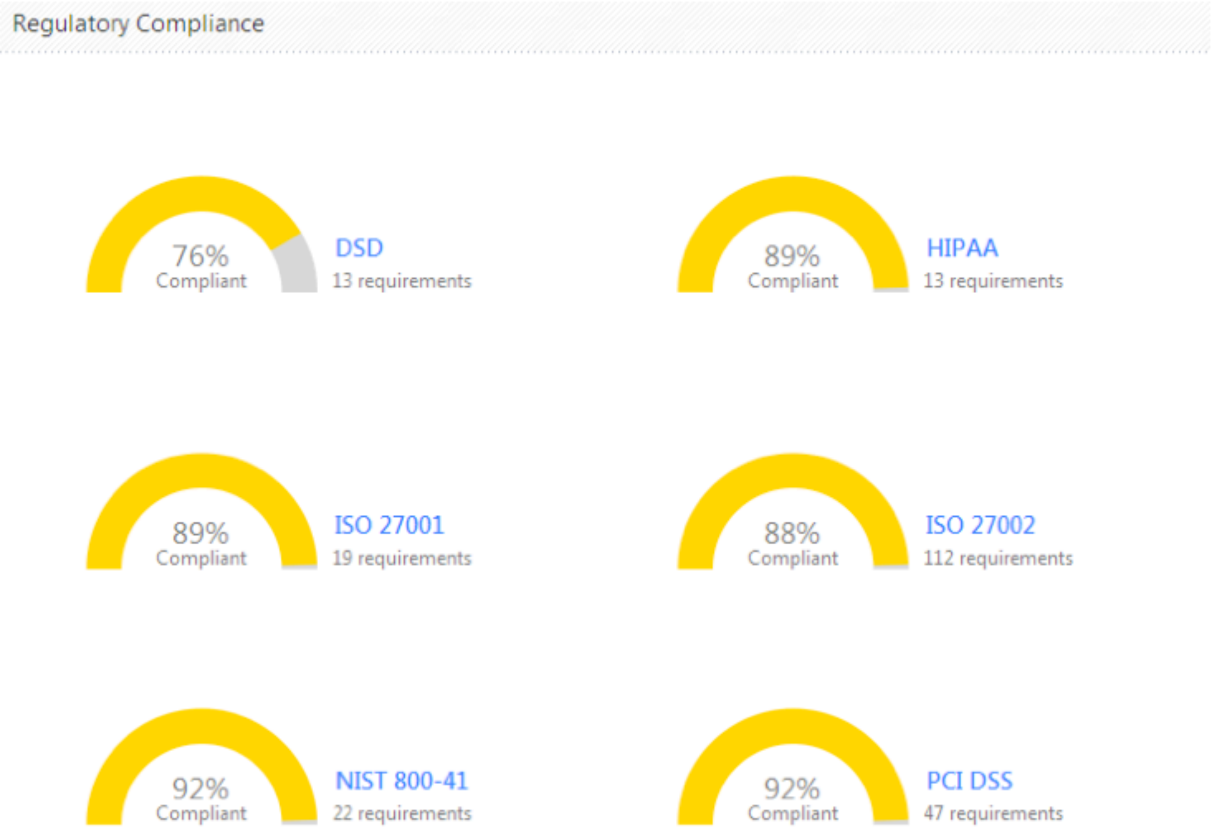
Secure	60%
Good	6%
Medium	11%
Poor	23%

Security Best Practices Compliance — See All...

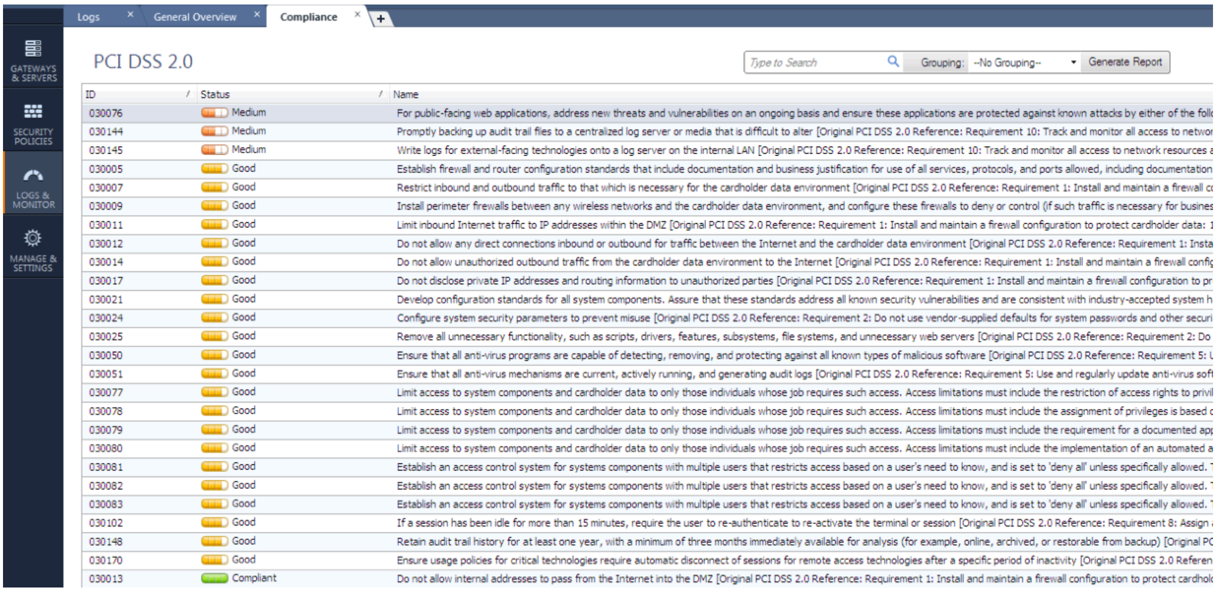
127 Best Practices monitored across
2 Gateways
6 Blades

Secure	60%
Good	6%
Medium	12%
Poor	22%

Also, if you need to comply to a standard, let's take **PCI DSS** as an example, a detailed report is available:



Click on **PCI DSS** and you will get a view on necessary changes so that you increase the compliance level from 92% current to 100%.



PCI DSS 2.0

ID	Status	Name
030076	Medium	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the foll
030144	Medium	Promptly backing up audit trail files to a centralized log server or media that is difficult to alter [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to networ
030145	Medium	Write logs for external-facing technologies onto a log server on the internal LAN [Original PCI DSS 2.0 Reference: Requirement 10: Track and monitor all access to network resources a
030005	Good	Establish firewall and router configuration standards that include documentation and business justification for use of all services, protocols, and ports allowed, including documentation
030007	Good	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall co
030009	Good	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for busines
030011	Good	Limit inbound Internet traffic to IP addresses within the DMZ [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: 1
030012	Good	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment [Original PCI DSS 2.0 Reference: Requirement 1: Insta
030014	Good	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall config
030017	Good	Do not disclose private IP addresses and routing information to unauthorized parties [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to pr
030021	Good	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system h
030024	Good	Configure system security parameters to prevent misuse [Original PCI DSS 2.0 Reference: Requirement 2: Do not use vendor-supplied defaults for system passwords and other securi
030025	Good	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers [Original PCI DSS 2.0 Reference: Requirement 2: Do
030050	Good	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software [Original PCI DSS 2.0 Reference: Requirement 5: U
030051	Good	Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs [Original PCI DSS 2.0 Reference: Requirement 5: Use and regularly update anti-virus soft
030077	Good	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the restriction of access rights to privil
030078	Good	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the assignment of privileges is based c
030079	Good	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the requirement for a documented app
030080	Good	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the implementation of an automated a
030081	Good	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to 'deny all' unless specifically allowed. T
030082	Good	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to 'deny all' unless specifically allowed. T
030083	Good	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to 'deny all' unless specifically allowed. T
030102	Good	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session [Original PCI DSS 2.0 Reference: Requirement 8: Assign a
030148	Good	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup) [Original PC
030170	Good	Ensure usage policies for critical technologies require automatic disconnect of sessions for remote access technologies after a specific period of inactivity [Original PCI DSS 2.0 Referen
030013	Compliant	Do not allow internal addresses to pass from the Internet into the DMZ [Original PCI DSS 2.0 Reference: Requirement 1: Install and maintain a firewall configuration to protect cardhold

The view starts from least compliant, going down to compliant measures, shown in Green – Compliant.

40.0 Lab: Configure Web Traffic Inline Layer for Applications & URL Filtering Rules

Lab Objectives

- Create an inline layer for Applications rules

At this moment, we have a fully functional Access Control policy that reduces the risk for your organization and all employees. The Access Control policy is now able to control and educate the internal users on safe using the internet, through Actions such as Ask, Inform, as you have seen in previous labs and **Module 12 - Configuring Advanced Access Control Policies**.

Also, we covered some of the best practices and there is more to be covered in this direction, following the next labs and lectures in **Module 13 - Optimizing R80 Rule Base - Inline and Ordered Layers**.

In addition to having a policy that matches our organization needs, there are some hidden goals as well, such as:

- Possibility to apply same policy to other gateways (this will be as a shared layer)
- Increase performance

As explained in the first two lectures of Module 13, there are some best practices to follow when designing the Access Control rule base. Efficient rule matching is very important, and this helps improving the overall performance.

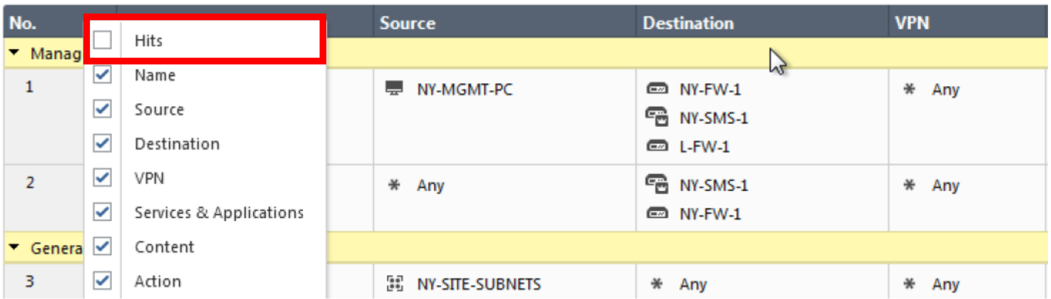
Continuing on, here are the most important facts that you may want to take into consideration in order to implement a good efficient rule matching:

1. You should place the rules that check the source, destination and port numbers (so this are network rules, with Firewall Blade active) at the top of the rule base. The reason is that the network rules are checked first, before any other advanced software blades.
2. Rules that contain applications and content should be placed after network rules (this refers to Applications & URL Filtering and Content Awareness software blades)
3. Rules that contain applications or content should not contain "***Any"*** in the source or the destination fields

What's the reason behind the above 2 and 3 best practices?

Here is the "trick". Application Control and Content Awareness rules require content inspection, which means that they can affect overall performance. This is a solid argument of why rule base optimization should be implemented or design the Rule Base following the best practices from the beginning.

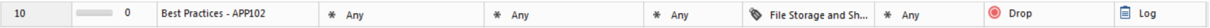
One way to improve the performance is to add layers to our existing policy – inline and or ordered layers. The main idea is that the first connection will traverse the rule base from the top to the bottom of the rule base until a match is found. Also, rules with a high hit count should be placed at the top of our rule base in order to optimize the policy. In order for the hit count to be available, this can be enabled by **right-click**ing on the first row in the policy and selecting **Hits**, as you can see below:



No.	Source	Destination	VPN
Manag			
1	NY-MGMT-PC	NY-FW-1 NY-SMS-1 L-FW-1	Any
2	Any	NY-SMS-1 NY-FW-1	Any
Genera			
3	NY-SITE-SUBNETS	Any	Any

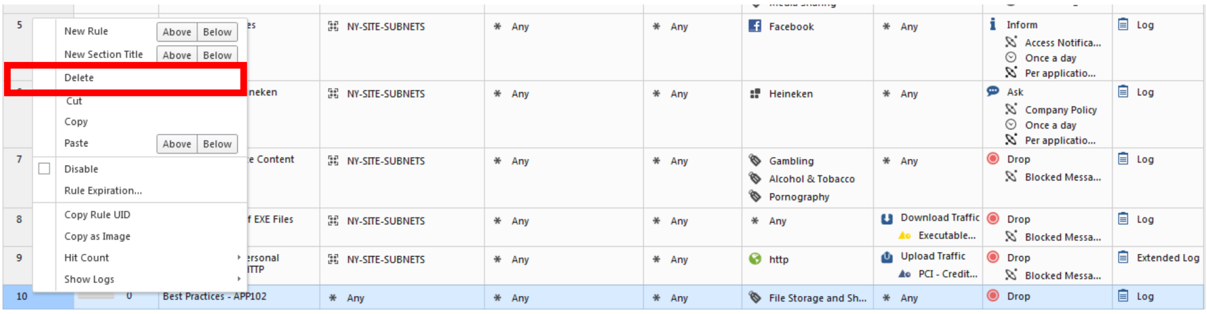
So, we will now continue and optimize our policy targeting the Application Control rules. We could either create an ordered layer and insert our application rules there, or we could create an inline layer. For this lab, we will choose the second option.

Before implementing any changes, let's clean our existing policy and delete the last rule we added previously – **Best Practices – APP102.**



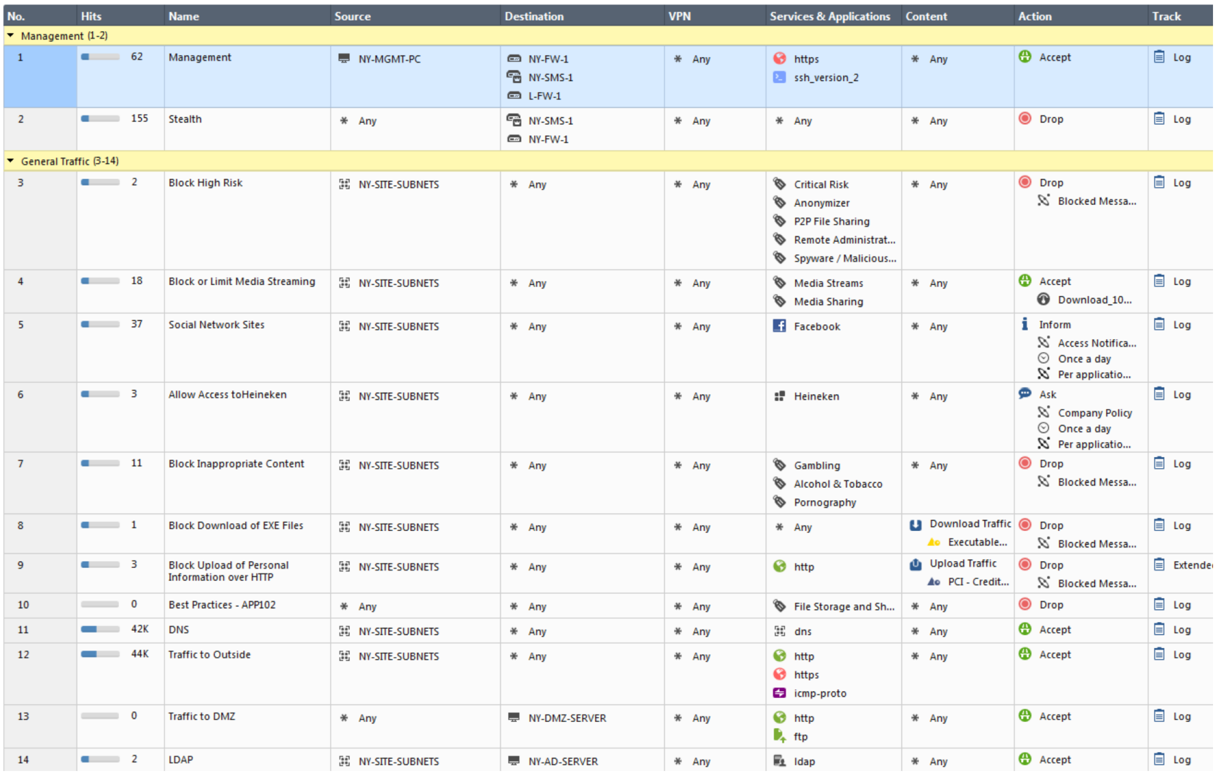
10	0	Best Practices - APP102	Any	Any	Any	File Storage and Sh...	Any	Drop	Log

In order to do this, right-click on 10 in the first column and select **Delete**:



5		es	NY-SITE-SUBNETS	Any	Any	Facebook	Any	Inform Access Notifica... Once a day Per applicatio...	Log
		neken	NY-SITE-SUBNETS	Any	Any	Heineken	Any	Ask Company Policy Once a day Per applicatio...	Log
7		e Content	NY-SITE-SUBNETS	Any	Any	Gambling Alcohol & Tobacco Pornography	Any	Drop Blocked Messa...	Log
8		f EXE Files	NY-SITE-SUBNETS	Any	Any	Any	Download Traffic Executable...	Drop Blocked Messa...	Log
9		ersonal TTP	NY-SITE-SUBNETS	Any	Any	http	Upload Traffic PCI - Credit...	Drop Blocked Messa...	Extended Log
10	0	Best Practices - APP102	Any	Any	Any	File Storage and Sh...	Any	Drop	Log

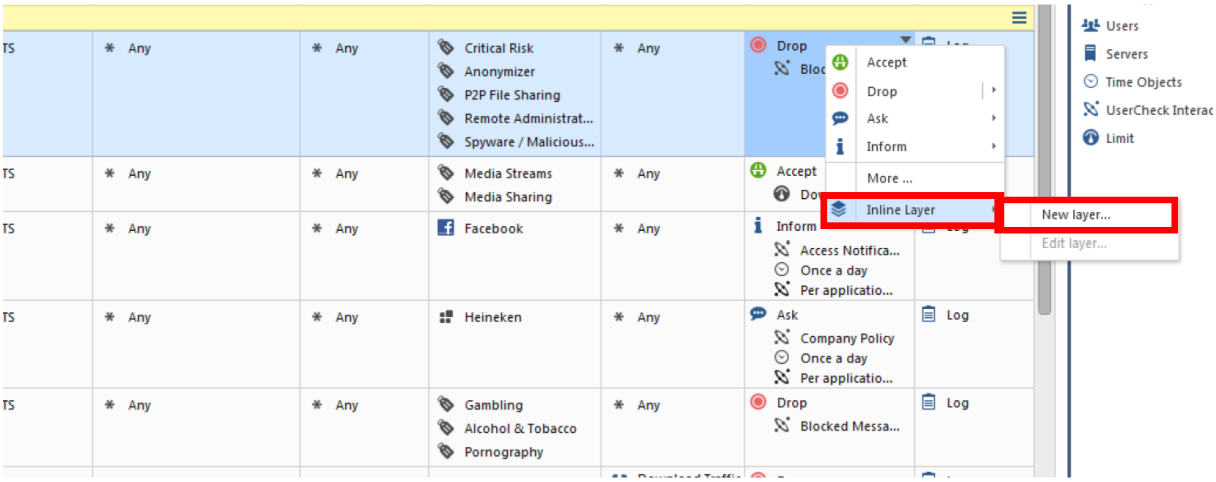
Currently, here is how our policy looks like:



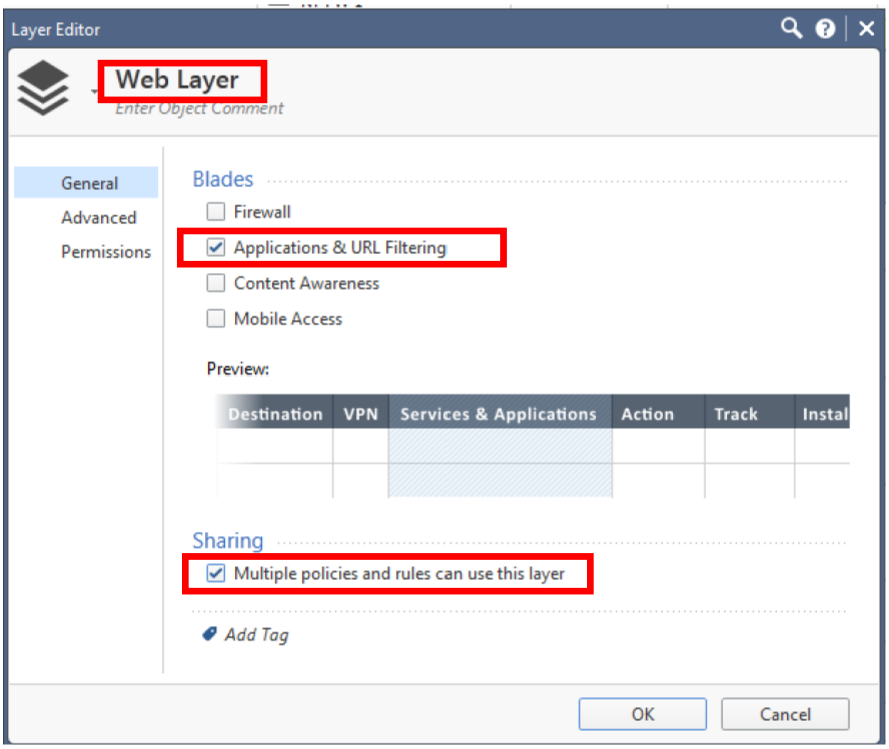
No.	Hits	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
▾ Management (1-2)									
1	62	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1 L-FW-1	* Any	https ssh_version_2	* Any	Accept	Log
2	155	Stealth	* Any	NY-SMS-1 NY-FW-1	* Any	* Any	* Any	Drop	Log
▾ General Traffic (3-14)									
3	2	Block High Risk	NY-SITE-SUBNETS	* Any	* Any	Critical Risk Anonymizer P2P File Sharing Remote Administrat... Spyware / Malicious...	* Any	Drop Blocked Messa...	Log
4	18	Block or Limit Media Streaming	NY-SITE-SUBNETS	* Any	* Any	Media Streams Media Sharing	* Any	Accept Download_10...	Log
5	37	Social Network Sites	NY-SITE-SUBNETS	* Any	* Any	Facebook	* Any	Inform Access Notifica... Once a day Per applicatio...	Log
6	3	Allow Access toHeineken	NY-SITE-SUBNETS	* Any	* Any	Heineken	* Any	Ask Company Policy Once a day Per applicatio...	Log
7	11	Block Inappropriate Content	NY-SITE-SUBNETS	* Any	* Any	Gambling Alcohol & Tobacco Pornography	* Any	Drop Blocked Messa...	Log
8	1	Block Download of EXE Files	NY-SITE-SUBNETS	* Any	* Any	* Any	Download Traffic Executable...	Drop Blocked Messa...	Log
9	3	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	* Any	* Any	http	Upload Traffic PCI - Credit...	Drop Blocked Messa...	Extende
10	0	Best Practices - APP102	* Any	* Any	* Any	File Storage and Sh...	* Any	Drop	Log
11	42K	DNS	NY-SITE-SUBNETS	* Any	* Any	dns	* Any	Accept	Log
12	44K	Traffic to Outside	NY-SITE-SUBNETS	* Any	* Any	http https icmp-proto	* Any	Accept	Log
13	0	Traffic to DMZ	* Any	NY-DMZ-SERVER	* Any	http ftp	* Any	Accept	Log
14	2	LDAP	NY-SITE-SUBNETS	NY-AD-SERVER	* Any	ldap	* Any	Accept	Log

In this lab, we will create an inline layer for rules 3 to 7. First, let's add a new rule. Right-click on 3 and select **New Rule – Above.** Give it a name – **Web Traffic**, drag-and-drop the source from another rule – **NY-SITE-SUBNETS** and select **ExternalZone** for destination field. Add **ExternalZone** in the destination column to all rules.

In the 3rd rule (the new rule), right-click on the **Block** in the action column, select **Inline Layer** and **New Layer**:



Give this layer a name – **Web Layer**, enable only **Applications & URL Filtering** and enable **Sharing** option at the bottom.



Web Layer
Enter Object Comment

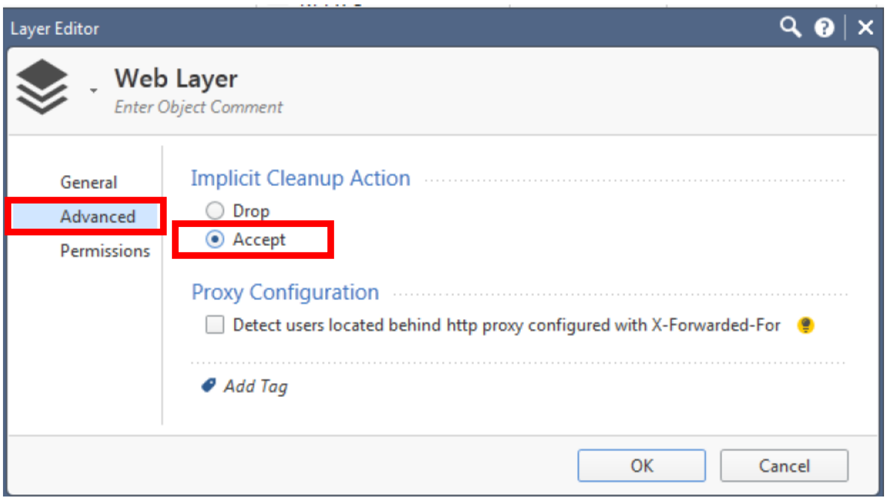
Blades
- □ Firewall
- ☑ Applications & URL Filtering
- □ Content Awareness
- □ Mobile Access

Preview:

Destination	VPN	Services & Applications	Action	Track	Instal

Sharing
- ☑ Multiple policies and rules can use this layer

When configuration is complete, select **Advanced** and change **Implicit Cleanup Action** to **Accept.**

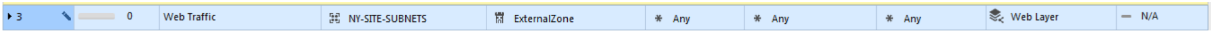


Web Layer
Enter Object Comment

Implicit Cleanup Action
- ○ Drop
- ● Accept

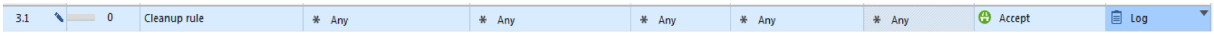
Proxy Configuration
- □ Detect users located behind http proxy configured with X-Forwarded-For

When complete, click **OK** in order to continue. This will create our new inline layer – **Web Layer.**



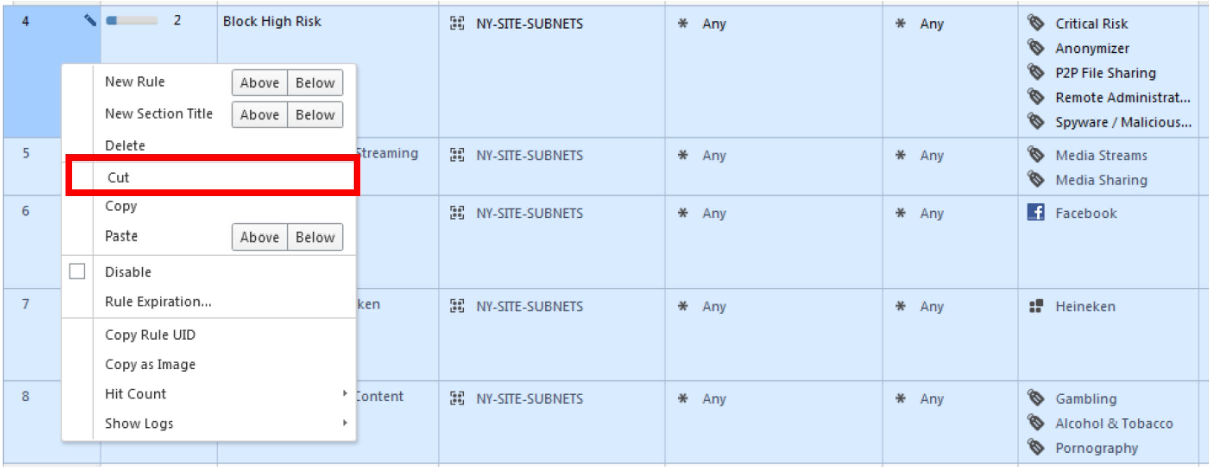
3	0	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any	Any	Any	Web Layer	N/A

The explicit **Cleanup** rule 3.1 has the action to **Drop**, please change this to **Allow** before moving on and change **Track** to **Log** the event.



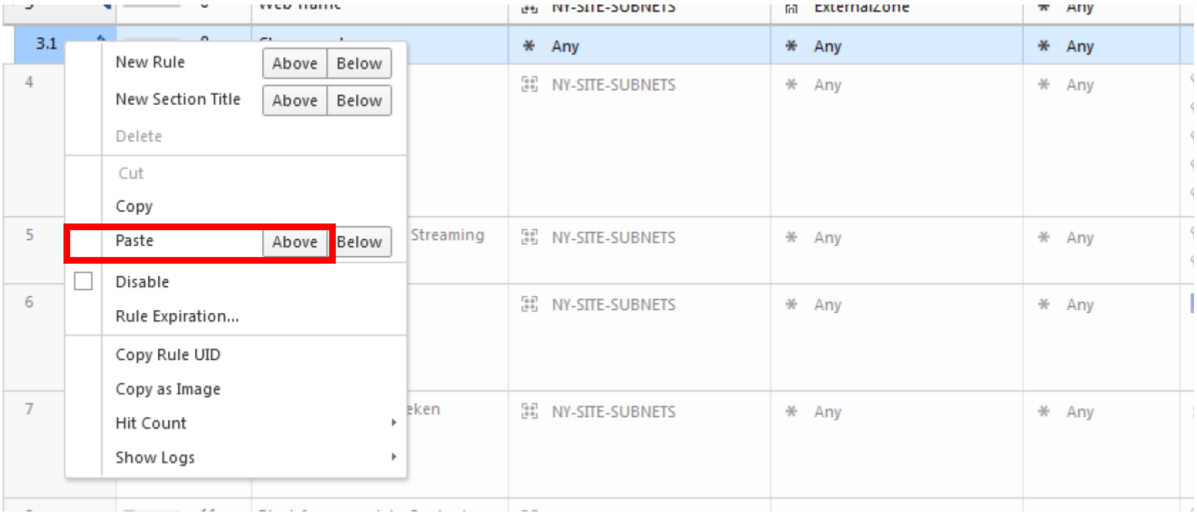
3.1	0	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

Select rules 4 to 8. Click on 4 and hold down **Shift** and then click on 8. Then right-click and select **Cut.**



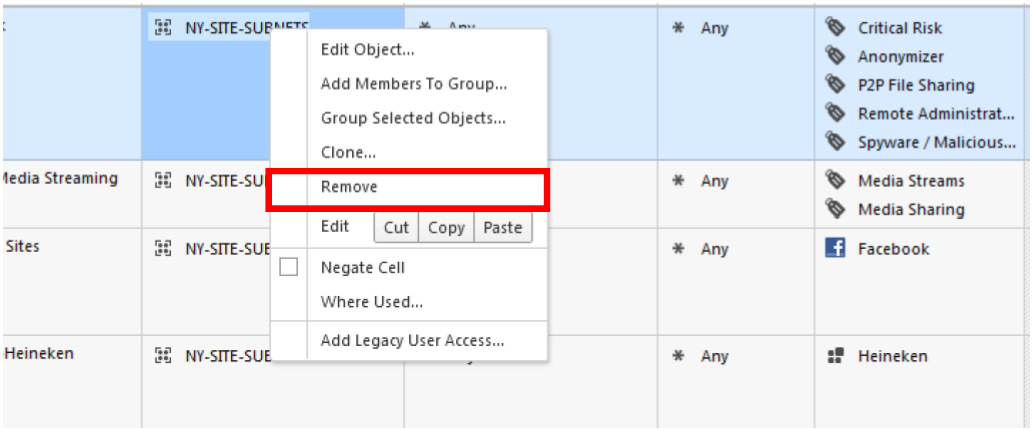
4	2	Block High Risk	NY-SITE-SUBNETS	Any	Any	Critical Risk Anonymizer P2P File Sharing Remote Administrat... Spyware / Malicious...
5		...treaming	NY-SITE-SUBNETS	Any	Any	Media Streams Media Sharing
6			NY-SITE-SUBNETS	Any	Any	Facebook
7		...ken	NY-SITE-SUBNETS	Any	Any	Heineken
8		...ontent	NY-SITE-SUBNETS	Any	Any	Gambling Alcohol & Tobacco Pornography

Next, right-click on 3 and select **Paste – Above**:



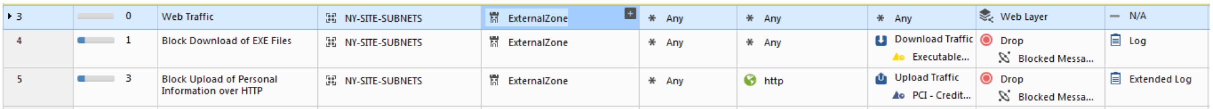
3	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any
3.1		Any	Any	Any
4		NY-SITE-SUBNETS	Any	Any
5	Streaming	NY-SITE-SUBNETS	Any	Any
6		NY-SITE-SUBNETS	Any	Any
7	...eken	NY-SITE-SUBNETS	Any	Any

We will make our rules more general, so we will now remove the NY-SITE-SUBNETS from the source column of rules 3.1-3.5.



	NY-SITE-SUBNETS	Any	Any	Critical Risk Anonymizer P2P File Sharing Remote Administrat... Spyware / Malicious...
Media Streaming	NY-SITE-SU		Any	Media Streams Media Sharing
Sites	NY-SITE-SUE		Any	Facebook
Heineken	NY-SITE-SUE		Any	Heineken

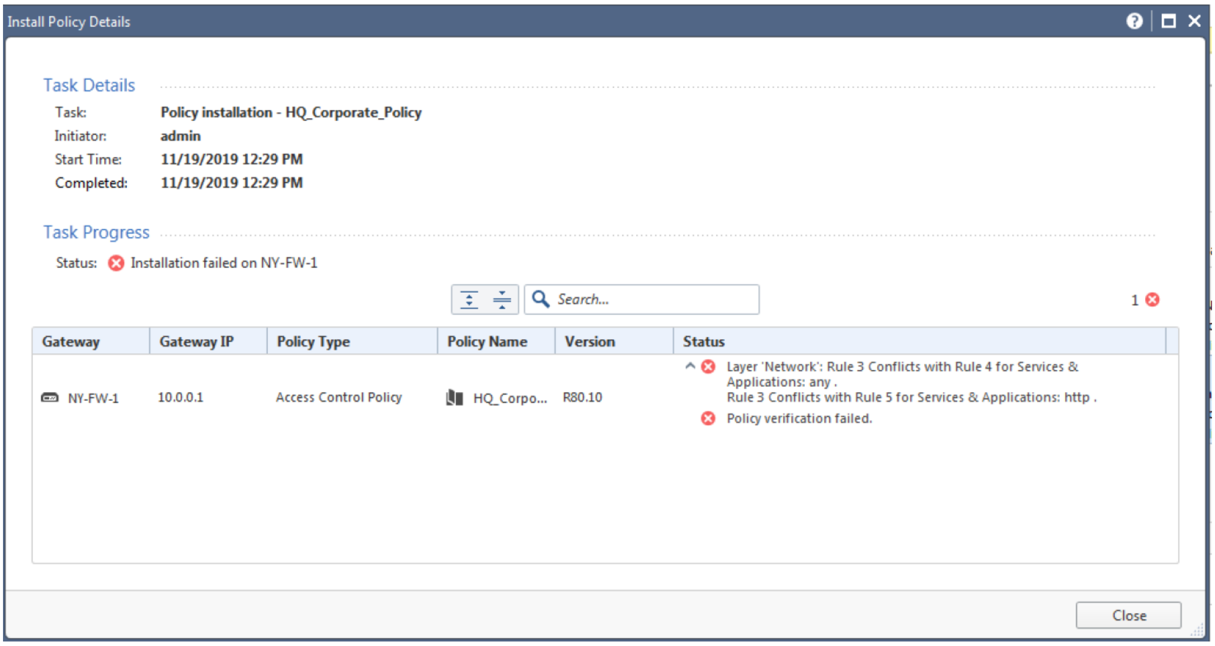
This is how the policy looks right now.



3	0	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any	Any	Any	Web Layer	N/A
4	1	Block Download of EXE Files	NY-SITE-SUBNETS	ExternalZone	Any	Any	Download Traffic Executable...	Drop Blocked Messa...	Log
5	3	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	ExternalZone	Any	http	Upload Traffic PCI - Credit...	Drop Blocked Messa...	Extended Log

Now, let's **publish** the changes and **install** the policy.

Policy installation fails and here is the error displayed:



Install Policy Details

Task Details

Task: **Policy installation - HQ_Corporate_Policy**
Initiator: **admin**
Start Time: **11/19/2019 12:29 PM**
Completed: **11/19/2019 12:29 PM**

Task Progress

Status: Installation failed on NY-FW-1

Gateway	Gateway IP	Policy Type	Policy Name	Version	Status
NY-FW-1	10.0.0.1	Access Control Policy	HQ_Corpo...	R80.10	Layer 'Network': Rule 3 Conflicts with Rule 4 for Services & Applications: any . Rule 3 Conflicts with Rule 5 for Services & Applications: http . Policy verification failed.

Rule 3 – the inline layer, has configured for **Services & Applications** column the **Any** option. The same for rule 4 – **Any.** Rule 5 has **http** selected in this column.

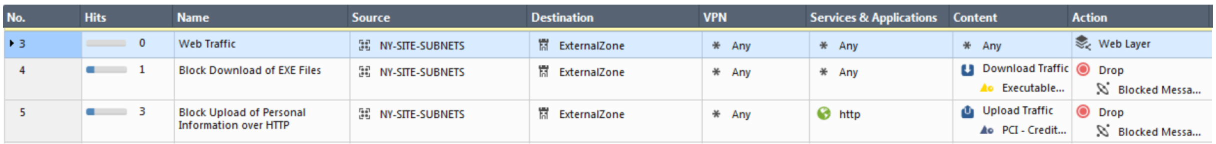
The main idea is that rule 3 overrides both rules, 4 and 5, so traffic will never match rules 4 or 5. This issue will be addressed in the next lab.

41.0 Lab: Configure Data Inline Layer for Content Awareness Rules

Lab Objectives

- Create an Inline Layer for Content rules

Examining rules 3 to 5,



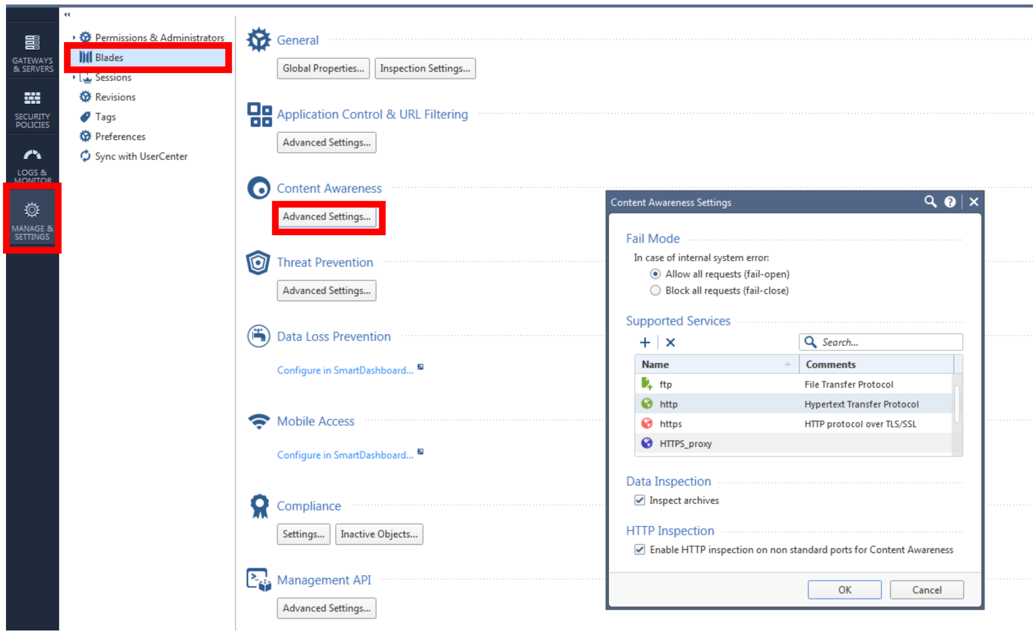
No.	Hits	Name	Source	Destination	VPN	Services & Applications	Content	Action
3	0	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any	Any	Any	Web Layer
4	1	Block Download of EXE Files	NY-SITE-SUBNETS	ExternalZone	Any	Any	Download Traffic Executable...	Drop Blocked Messa...
5	3	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	ExternalZone	Any	http	Upload Traffic PCI - Credit...	Drop Blocked Messa...

we see that for in **Services & Applications** column, we have a problem. The **Any** option in rule 3 overrides rule 4 and 5, so now we need to change somehow the setup.

Remember that we should have the most specific rules at the top and the rest, more general, to follow these ones. We will take rules 4 and 5 and move them in an Inline Layer above rule 3 and in order to not have the same behaviour and policy install failure, we will insert in the **Services** column some specific services.

Rules 4 and 5 are **Content Awareness** related. What are the services encompassed in this blade? Let's find out.

In SmartConsole, please navigate to **Manage&Settings**, **Blades** and select **Content Awareness Advanced Settings.**



Content Awareness Settings

Fail Mode

In case of internal system error:

● Allow all requests (fail-open)

○ Block all requests (fail-close)

Supported Services

Name	Comments
ftp	File Transfer Protocol
http	Hypertext Transfer Protocol
https	HTTP protocol over TLS/SSL
HTTPS_proxy	

Data Inspection

☑ Inspect archives

HTTP Inspection

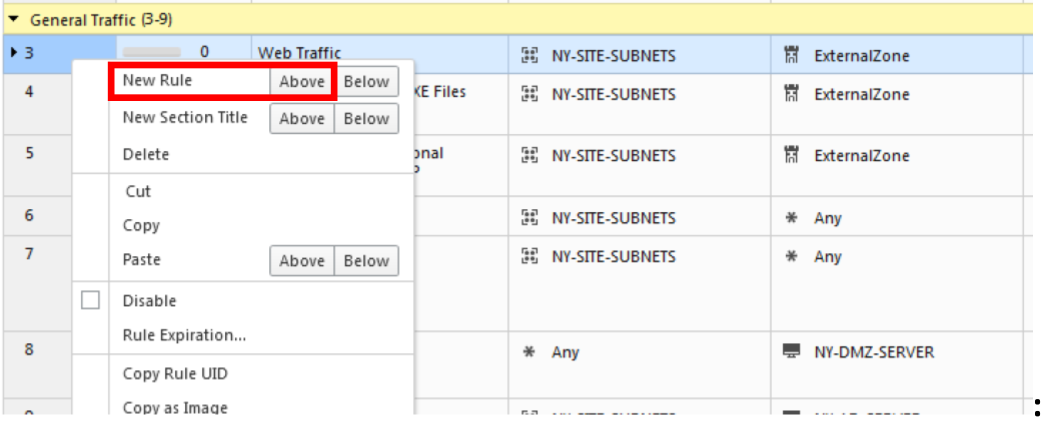
☑ Enable HTTP inspection on non standard ports for Content Awareness

OK Cancel

In the **Supported Services** we see what services are matched by **Content Awareness**: http, https, ftp, http proxy, https proxy and smtp.

We will now add a rule above, above rule 3, in order to fix the problem and hopefully for the Access Control policy to install successfully.

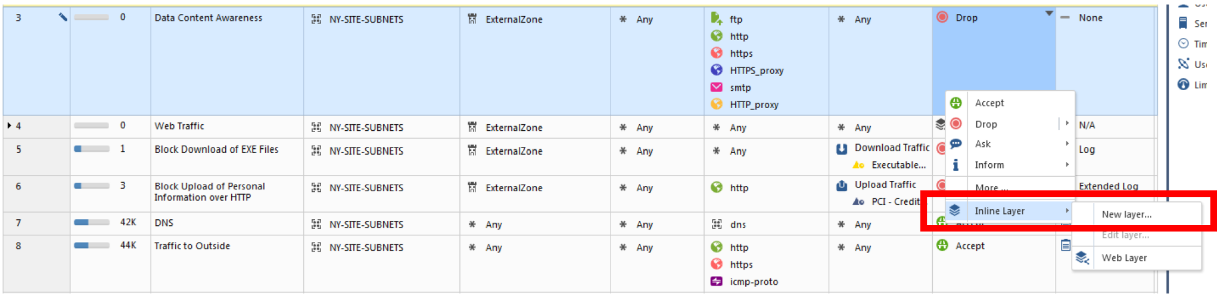
Right-click on 3 and select **New Rule – Above**:



General Traffic (3-9)

3	0	Web Traffic	NY-SITE-SUBNETS	ExternalZone
4		XE Files	NY-SITE-SUBNETS	ExternalZone
5		onal	NY-SITE-SUBNETS	ExternalZone
6			NY-SITE-SUBNETS	Any
7			NY-SITE-SUBNETS	Any
8			Any	NY-DMZ-SERVER

For this new rule, let's define the name – **Data Content Awareness**, source – **NY-SITE-SUBNETS**, destination – **ExternalZone**, services&applications – **ftp, http, https, http_proxy, https_proxy, smtp**, action – **Inline Layer -> New Layer**.



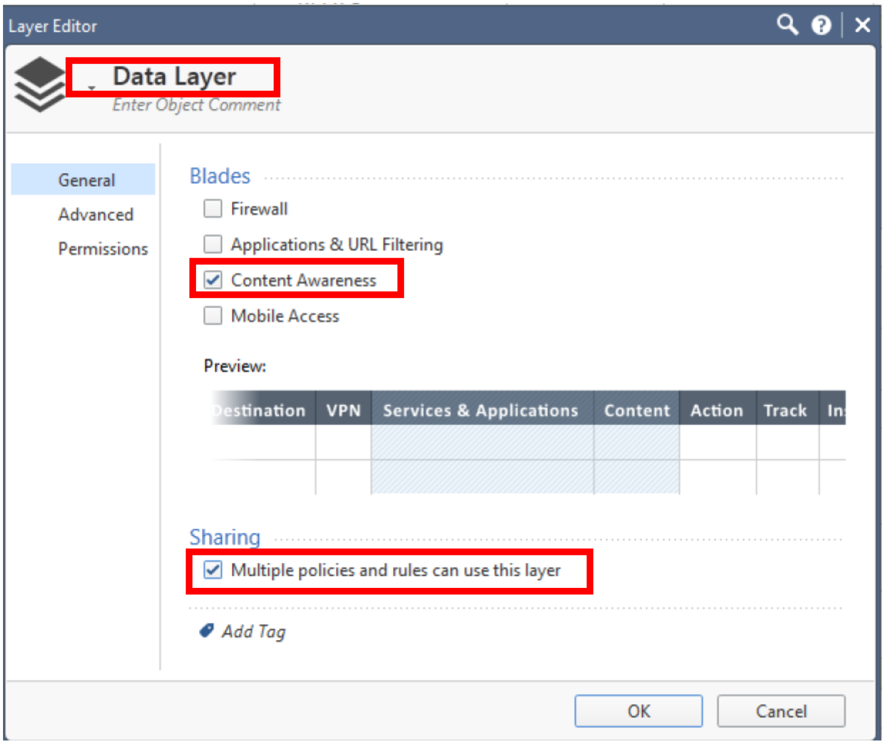
3	0	Data Content Awareness	NY-SITE-SUBNETS	ExternalZone	Any	ftp http https HTTPS_proxy smtp HTTP_proxy	Any	Drop	None
4	0	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any	Any	Any		N/A
5	1	Block Download of EXE Files	NY-SITE-SUBNETS	ExternalZone	Any	Any	Download Traffic Executable...		Log
6	3	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	ExternalZone	Any	http	Upload Traffic PCI - Credit		Extended Log
7	42K	DNS	NY-SITE-SUBNETS	Any	Any	dns	Any		
8	44K	Traffic to Outside	NY-SITE-SUBNETS	Any	Any	http https icmp-proto	Any	Accept	

Let's complete the following:

- Name: **Data Layer**
- Blades: **Content Awareness**
- Sharing (Multiple policies and rules can use this layer) – **Enabled**

Also, let's modify the **Implicit Cleanup Action** to **Accept**, in the **Advanced** section.

Please take a look at the screenshots below:



Layer Editor

Data Layer

Enter Object Comment

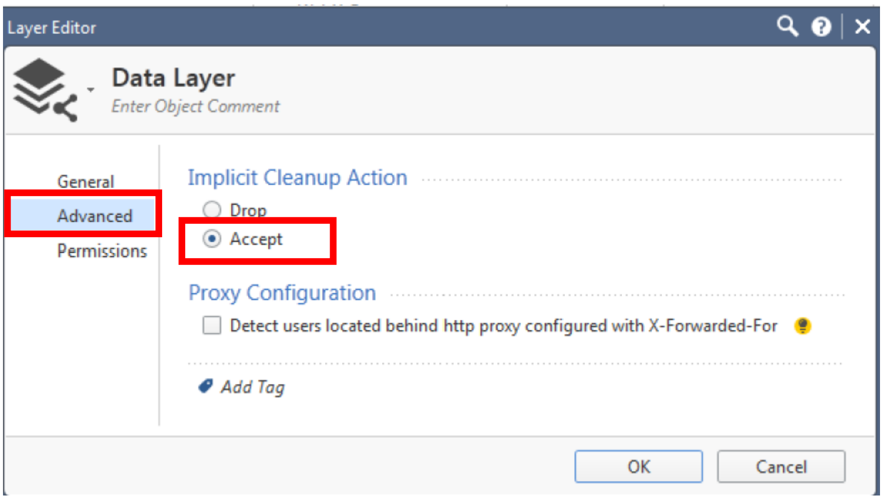
Blades

- □ Firewall
- □ Applications & URL Filtering
- ☑ Content Awareness
- □ Mobile Access

Preview:

Sharing

- ☑ Multiple policies and rules can use this layer



Layer Editor

Data Layer

Enter Object Comment

Implicit Cleanup Action

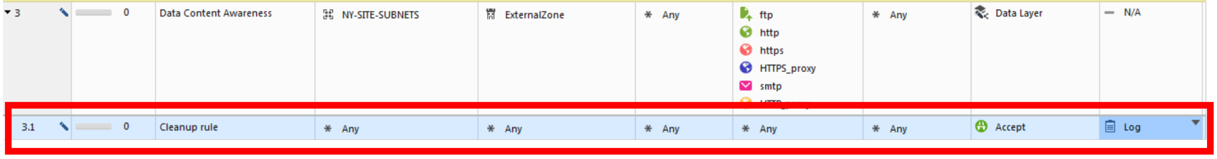
- ○ Drop
- ● Accept

Proxy Configuration

- □ Detect users located behind http proxy configured with X-Forwarded-For

In order to continue, please click **OK** now.

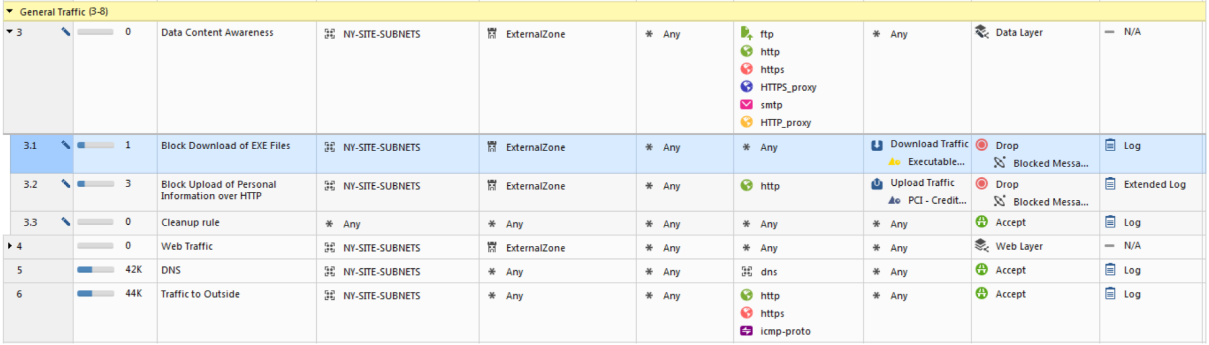
Please make sure that the Action for the new Cleanup Rule – 3.1 is set to **Accept.**



▾ 3		0	Data Content Awareness	NY-SITE-SUBNETS	ExternalZone	Any	ftp http https HTTPS_proxy smtp	Any	Data Layer	N/A
3.1		0	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

We will next take rules 4 and 5 and insert them under the new **Data Content Awareness** inline layer. We can **cut** and **paste** like we did before, or we can simply **drag-and-drop** these two rules between 3 and 3.1.

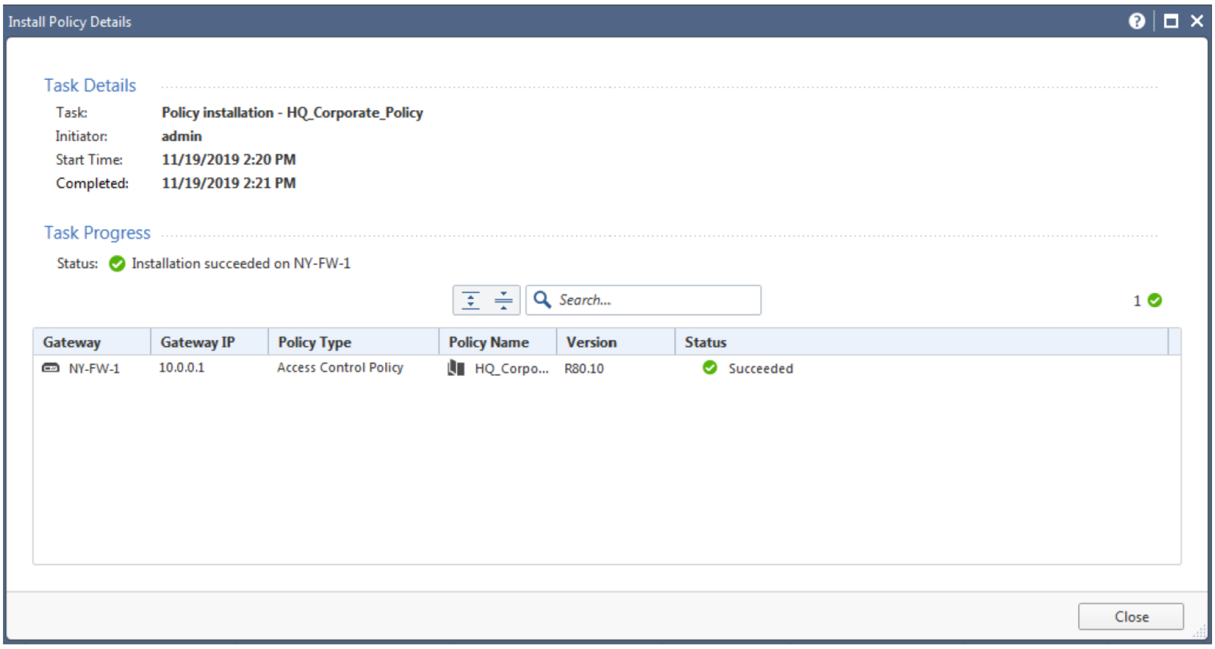
Your new policy should look like this now:



General Traffic (3-8)									
3	0	Data Content Awareness	NY-SITE-SUBNETS	ExternalZone	Any	ftp http https HTTPS_proxy smtp HTTP_proxy	Any	Data Layer	N/A
3.1	1	Block Download of EXE Files	NY-SITE-SUBNETS	ExternalZone	Any	Any	Download Traffic Executable...	Drop Blocked Messa...	Log
3.2	3	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	ExternalZone	Any	http	Upload Traffic PCI - Credit...	Drop Blocked Messa...	Extended Log
3.3	0	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log
4	0	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any	Any	Any	Web Layer	N/A
5	42K	DNS	NY-SITE-SUBNETS	Any	Any	dns	Any	Accept	Log
6	44K	Traffic to Outside	NY-SITE-SUBNETS	Any	Any	http https icmp-proto	Any	Accept	Log

Let’s now publish and install the policy.

Policy installation succeeds this time, no errors encountered:



Task Details

Task: **Policy installation - HQ_Corporate_Policy**
Initiator: **admin**
Start Time: **11/19/2019 2:20 PM**
Completed: **11/19/2019 2:21 PM**

Task Progress

Status: ✓ Installation succeeded on NY-FW-1

Gateway	Gateway IP	Policy Type	Policy Name	Version	Status
NY-FW-1	10.0.0.1	Access Control Policy	HQ_Corpo...	R80.10	✓ Succeeded

42.0 Lab: Configure Content Awareness Ordered Layer

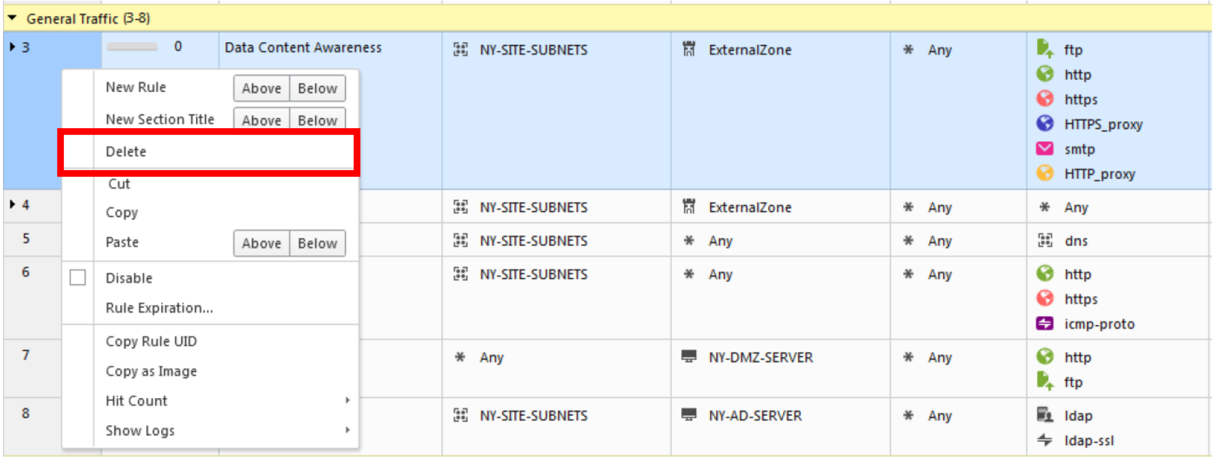
Lab Objectives

- Create a new Ordered Layer for Content Awareness related rules

Now we have a fully functional Access Control security policy, but we still have some problems to fix. **Remember the best practices!**

Application Control & Content Awareness rules require content inspection and should be placed lower in the rule base in order to optimize the performance of the policy.

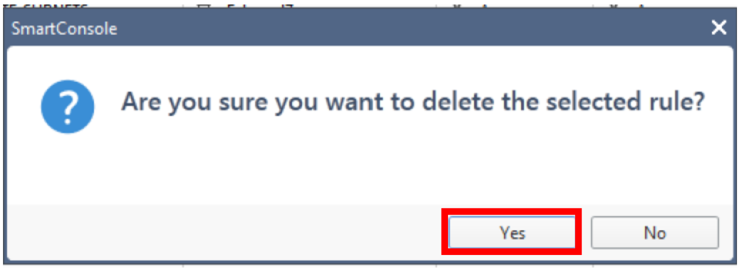
Let's now use **Ordered Layers** and improve our policy. We will next delete rule 3 – **Data Content Awareness** inline layer.



General Traffic (3-8)

3	0	Data Content Awareness	NY-SITE-SUBNETS	ExternalZone	Any	ftp http https HTTPS_proxy smtp HTTP_proxy
4			NY-SITE-SUBNETS	ExternalZone	Any	Any
5			NY-SITE-SUBNETS	Any	Any	dns
6			NY-SITE-SUBNETS	Any	Any	http https icmp-proto
7			Any	NY-DMZ-SERVER	Any	http ftp
8			NY-SITE-SUBNETS	NY-AD-SERVER	Any	ldap ldap-ssl

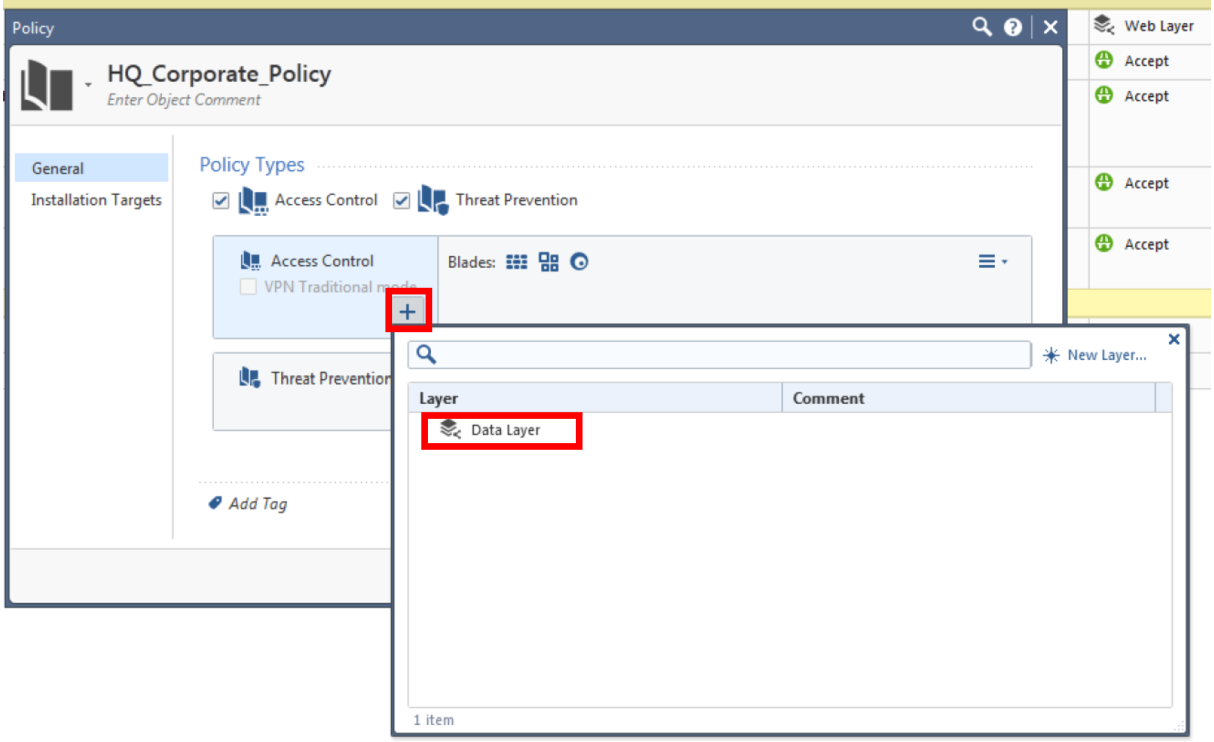
Click **Yes** in order to confirm the change:



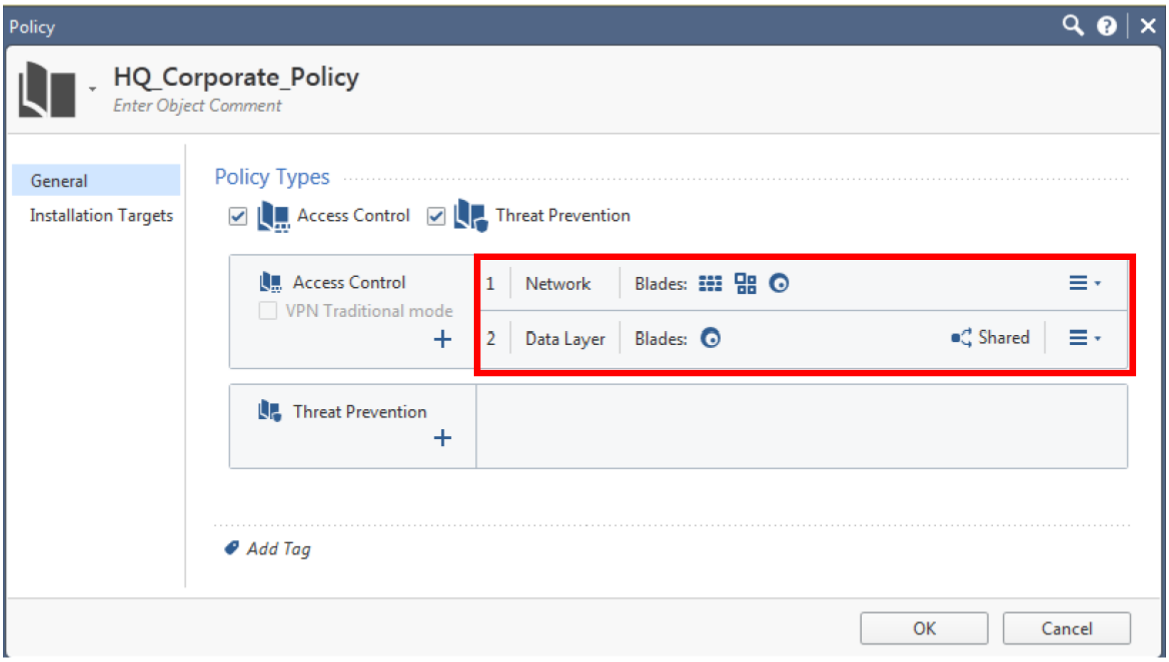
Are you sure you want to delete the selected rule?

Let's now edit our current policy. You will now see the real value of creating layers and enabling them for reuse, by clicking the **Sharing** option.

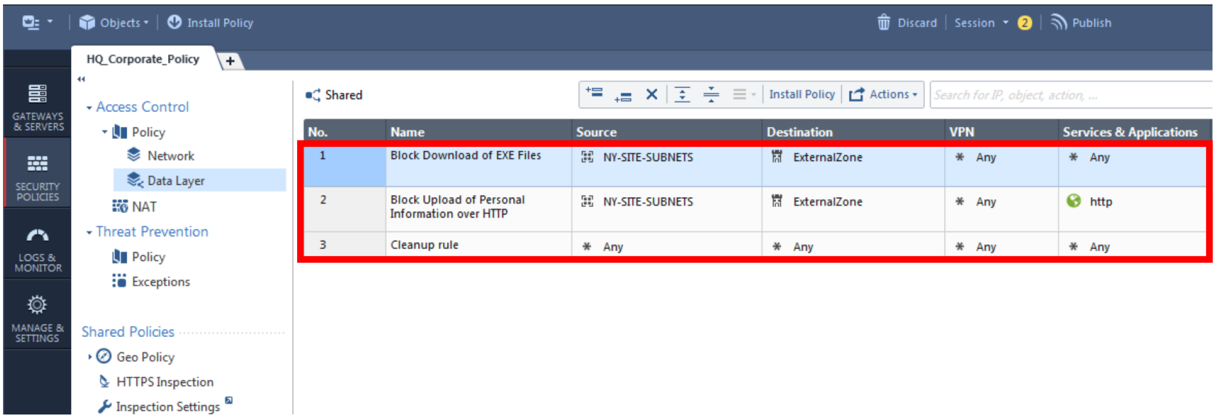
Let’s add another layer – **Ordered** and select **Data Layer** from the list below. This is the layer we have previously created, good thing that we enabled the **Sharing** option:



We now have two ordered layers, **Network** and **Data** Layer, as you can see below:

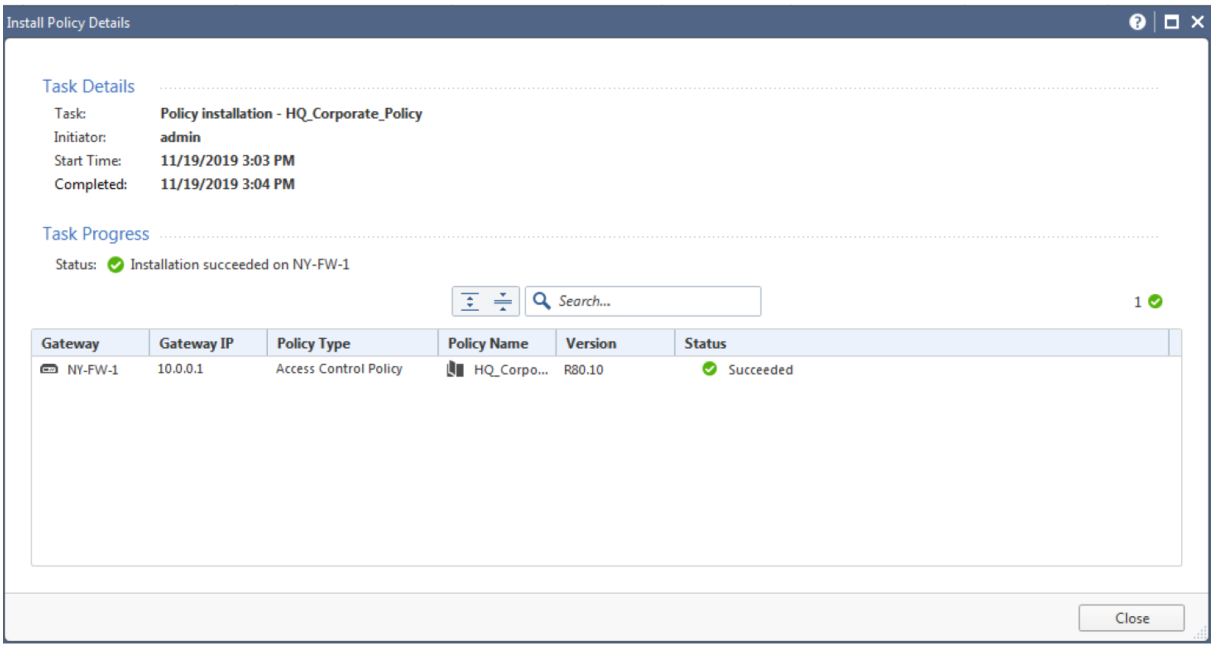


We can now see the change in the Access Control policy, two ordered layers. If you now click on the **Data Layer** layer, you will see rules we have defined in a previous lab:



No.	Name	Source	Destination	VPN	Services & Applications
1	Block Download of EXE Files	NY-SITE-SUBNETS	ExternalZone	Any	Any
2	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	ExternalZone	Any	http
3	Cleanup rule	Any	Any	Any	Any

Finally, let’s publish the changes and install **HQ_Corporate_Policy** policy. Installation has succeeded and we are now ready to continue with the next lab.



Task Details

Task: Policy installation - HQ_Corporate_Policy
Initiator: admin
Start Time: 11/19/2019 3:03 PM
Completed: 11/19/2019 3:04 PM

Task Progress

Status: ✓ Installation succeeded on NY-FW-1

Gateway	Gateway IP	Policy Type	Policy Name	Version	Status
NY-FW-1	10.0.0.1	Access Control Policy	HQ_Corpo...	R80.10	✓ Succeeded

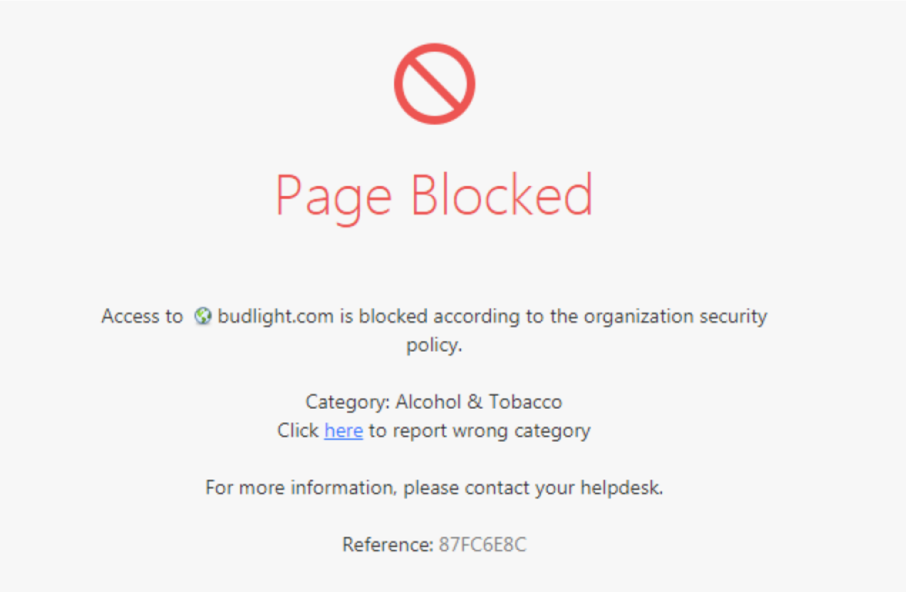
43.0 Lab: Final Policy Verification and Testing

Lab Objectives

- Run tests and verify the new policy
- Connect to alcohol and websites. Check policy and logs
- Attempt to download *.EXE files. Check policy and logs

Ok, so now let's test our new policy and examine the corresponding logs. First, we will try to connect to a website that falls under alcohol category.

We will try to browse to **www.budlight.com** and we see that our page is **blocked**, as expected:



Page Blocked

Access to budlight.com is blocked according to the organization security policy.

Category: Alcohol & Tobacco
Click here to report wrong category

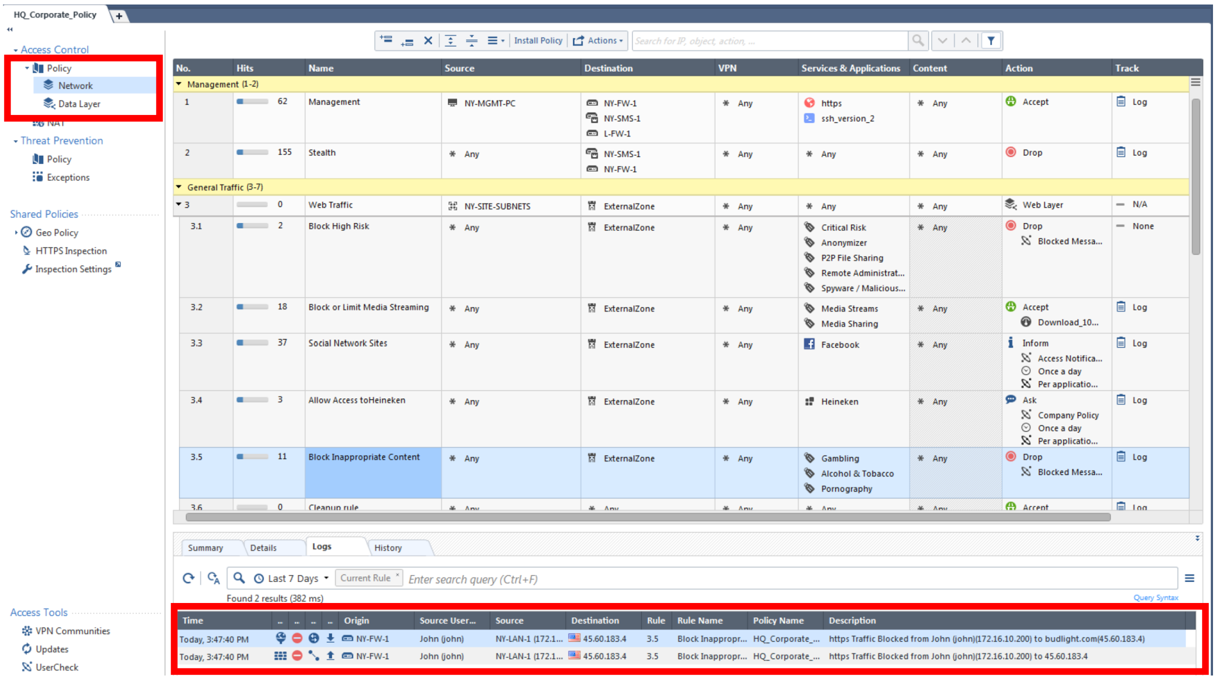
For more information, please contact your helpdesk.

Reference: 87FC6E8C

Let's analyse the corresponding logs. I will select the **Network** layer and from the rules, I will select rule 3.5 which is blocking traffic to www.budlight.com.

We can see that we currently have two logs tied to this rule – rule 3.5.

Please take a look below:

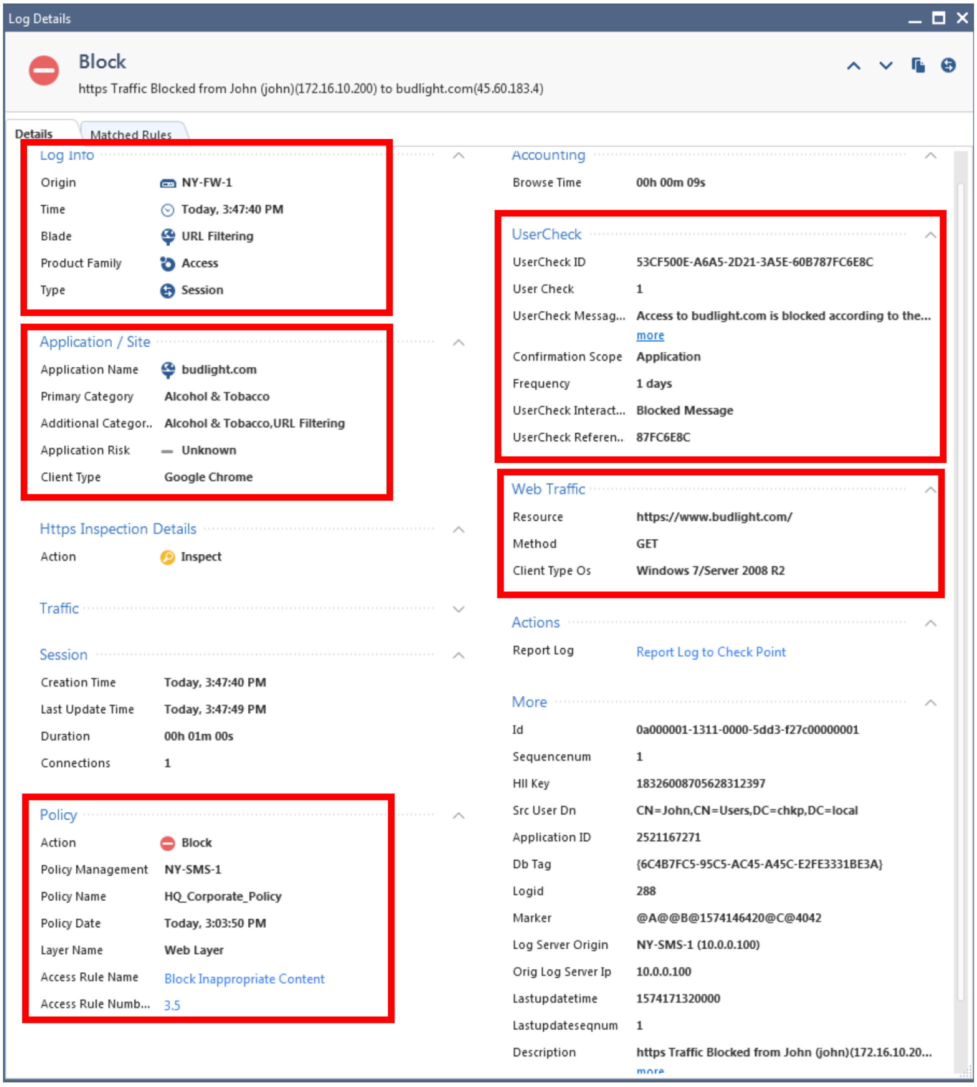


No.	Hits	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
Management (1-2)									
1	62	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1 L-FW-1	Any	https ssh_version_2	Any	Accept	Log
2	155	Stealth	Any	NY-SMS-1 NY-FW-1	Any	Any	Any	Drop	Log
General Traffic (3-7)									
3	0	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any	Any	Any	Web Layer	N/A
3.1	2	Block High Risk	Any	ExternalZone	Any	Critical Risk Anonymizer P2P File Sharing Remote Administrat... Spyware / Malicious...	Any	Drop Blocked Messa...	None
3.2	18	Block or Limit Media Streaming	Any	ExternalZone	Any	Media Streams Media Sharing	Any	Accept Download_10...	Log
3.3	37	Social Network Sites	Any	ExternalZone	Any	Facebook	Any	Inform Access Notifica... Once a day Per applicatio...	Log
3.4	3	Allow Access toHeineken	Any	ExternalZone	Any	Heineken	Any	Ask Company Policy Once a day Per applicatio...	Log
3.5	11	Block Inappropriate Content	Any	ExternalZone	Any	Gambling Alcohol & Tobacco Pornography	Any	Drop Blocked Messa...	Log
3.6	0	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

Found 2 results (382 ms)

Time	..	..	..	..	Origin	Source User...	Source	Destination	Rule	Rule Name	Policy Name	Description
Today, 3:47:40 PM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	45.60.183.4	3.5	Block Inappropr...	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to budlight.com(45.60.183.4)
Today, 3:47:40 PM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	45.60.183.4	3.5	Block Inappropr...	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to 45.60.183.4

Let’s open the first log:



Block

https Traffic Blocked from John (john)(172.16.10.200) to budlight.com(45.60.183.4)

Log Info
Origin NY-FW-1
Time Today, 3:47:40 PM
Blade URL Filtering
Product Family Access
Type Session

Application / Site
Application Name budlight.com
Primary Category Alcohol & Tobacco
Additional Categor.. Alcohol & Tobacco,URL Filtering
Application Risk Unknown
Client Type Google Chrome

Https Inspection Details
Action Inspect

Traffic

Session
Creation Time Today, 3:47:40 PM
Last Update Time Today, 3:47:49 PM
Duration 00h 01m 00s
Connections 1

Policy
Action Block
Policy Management NY-SMS-1
Policy Name HQ_Corporate_Policy
Policy Date Today, 3:03:50 PM
Layer Name Web Layer
Access Rule Name Block Inappropriate Content
Access Rule Numb... 3.5

Accounting
Browse Time 00h 00m 09s

UserCheck
UserCheck ID 53CF500E-A6A5-2D21-3A5E-60B787FC6E8C
User Check 1
UserCheck Messag... Access to budlight.com is blocked according to the... more
Confirmation Scope Application
Frequency 1 days
UserCheck Interact... Blocked Message
UserCheck Referen.. 87FC6E8C

Web Traffic
Resource https://www.budlight.com/
Method GET
Client Type Os Windows 7/Server 2008 R2

Actions
Report Log Report Log to Check Point

More
Id 0a000001-1311-0000-5dd3-f27c00000001
Sequencenum 1
Hll Key 18326008705628312397
Src User Dn CN=John,CN=Users,DC=chkp,DC=local
Application ID 2521167271
Db Tag {6C4B7FC5-95C5-AC45-A45C-E2FE3331BE3A}
Logid 288
Marker @A@@B@1574146420@C@4042
Log Server Origin NY-SMS-1 (10.0.0.100)
Orig Log Server Ip 10.0.0.100
Lastupdatetime 1574171320000
Lastupdateseqnum 1
Description https Traffic Blocked from John (john)(172.16.10.20... more

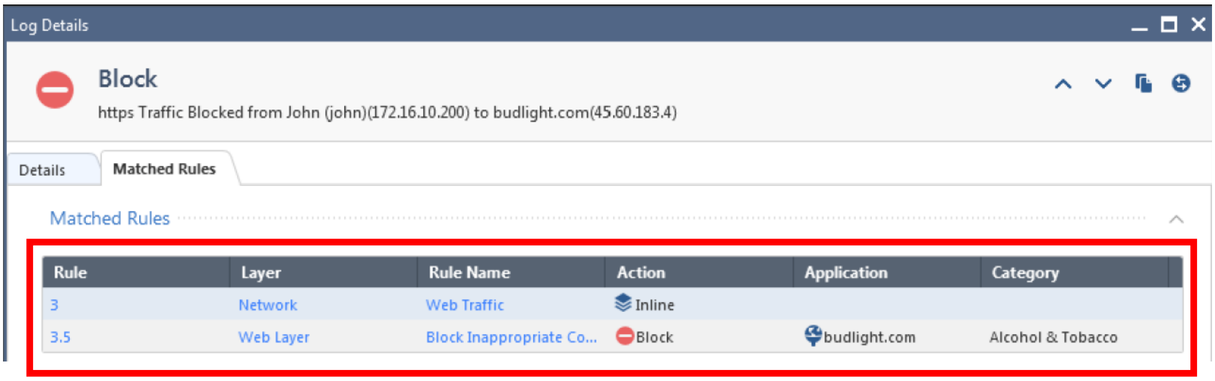
Log was generated by NY-FW-1, blade used – **URL Filtering**. For the application, information is self-explanatory: budlight.com was the website accessed and it falls under **Alcohol & Tobacco** category.

For the policy now, we see that the action was **Block** and we also see the rule match – **Block Inappropriate Content** and the exact rule is **3.5**.

UserCheck information is also available. We are able to confirm the configuration and that the blocked message is displayed and also we can see what is the **blocked message.**

Web Traffic highlights relevant information related to the exact resource being accessed. The **resource** is https://www.budlight.com, this was a GET resource, coming from a Windows 7 machine.

Also, let's take a look at the **Matched Rules** tab:



Block

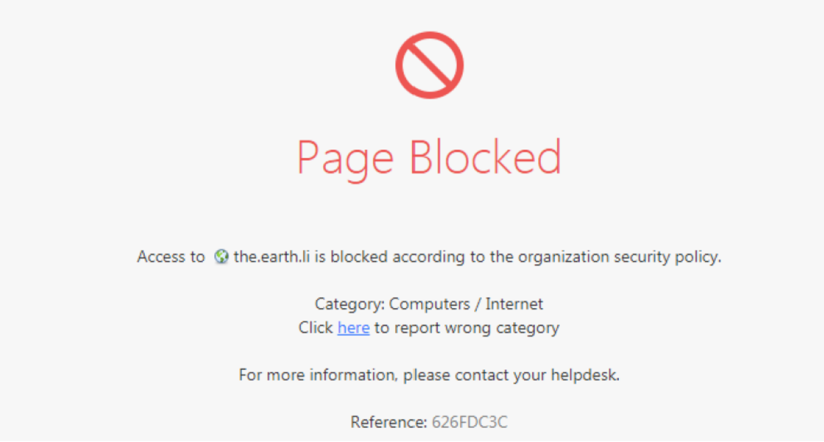
https Traffic Blocked from John (john)(172.16.10.200) to budlight.com(45.60.183.4)

Matched Rules

Rule	Layer	Rule Name	Action	Application	Category
3	Network	Web Traffic	Inline		
3.5	Web Layer	Block Inappropriate Co...	Block	budlight.com	Alcohol & Tobacco

So, the traffic was first matched against the **Parent Rule,** part of the **Network Layer** and then it was matched against Rule 3.5, part of the **Web Layer.**

Second verification follows. Let's try to download putty.EXE again and page is blocked, as expected.



Page Blocked

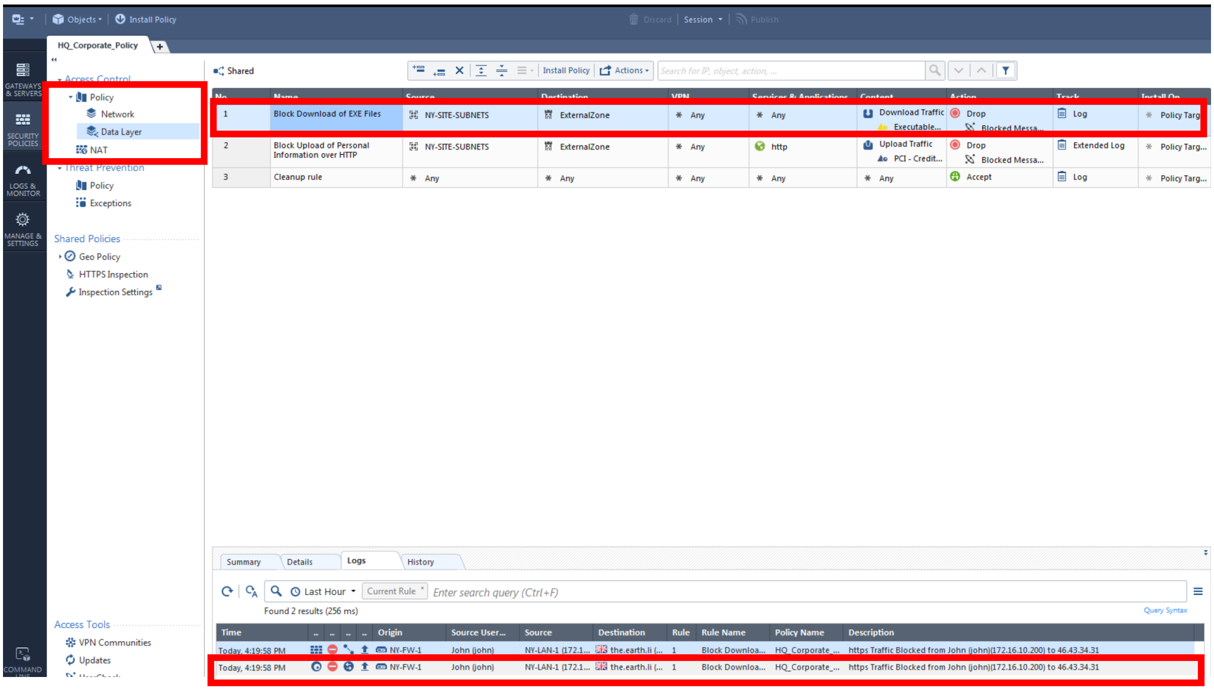
Access to the.earth.li is blocked according to the organization security policy.

Category: Computers / Internet
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: 626FDC3C

Now, let’s analyse the logs. I could search for the logs in the traditional way and filter the logs with **blade:Content Awareness** or, because I know which rules was actually hit, I will select the **Ordered Data Layer**, under the Network layer and select first rule – **Block Download of EXE Files**.



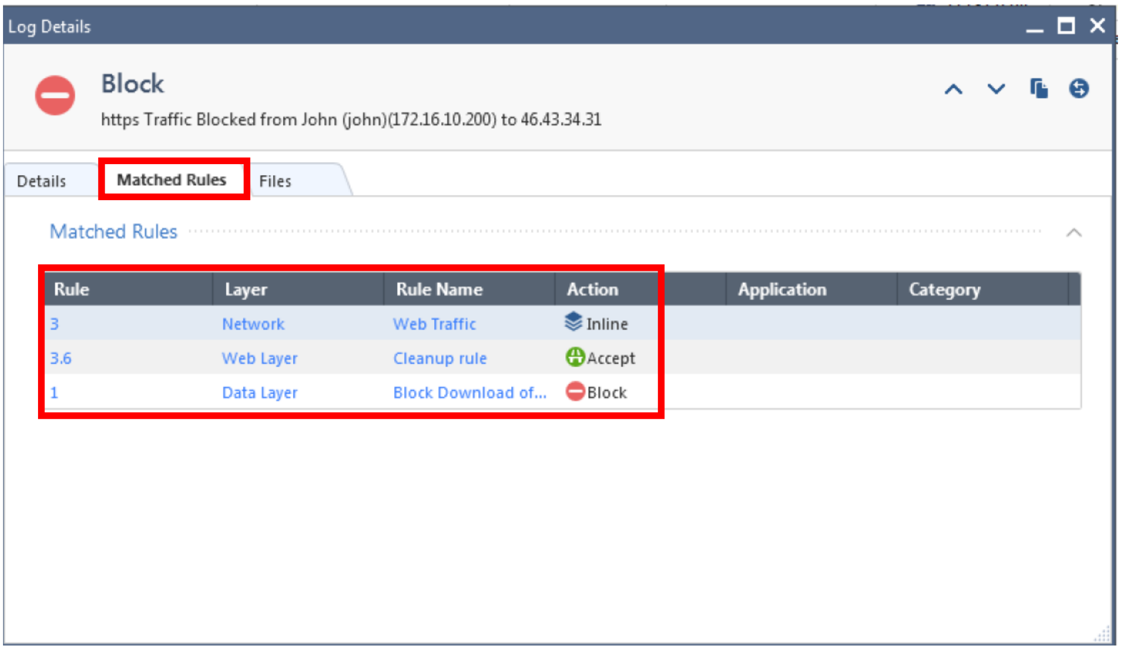
No	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track	Install On
1	Block Download of EXE Files	NY-SITE-SUBNETS	ExternalZone	Any	Any	Download Traffic Executable...	Drop Blocked Messa...	Log	Policy Targ
2	Block Upload of Personal Information over HTTP	NY-SITE-SUBNETS	ExternalZone	Any	http	Upload Traffic PCI - Credit...	Drop Blocked Messa...	Extended Log	Policy Targ...
3	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log	Policy Targ...

Found 2 results (256 ms)

Time	..	..	..	..	Origin	Source User...	Source	Destination	Rule	Rule Name	Policy Name	Description
Today, 4:19:58 PM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	the.earth.li (...	1	Block Downloa...	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to 46.43.34.31
Today, 4:19:58 PM					NY-FW-1	John (john)	NY-LAN-1 (172.1...	the.earth.li (...	1	Block Downloa...	HQ_Corporate_...	https Traffic Blocked from John (john)(172.16.10.200) to 46.43.34.31

I can see that there are two logs (I filtered the output for the Last Hour). I will open the second log, the one that has in the second column the **Content Awareness** blade and select the second tab – **Matched Rules**.

We can see here the exact matching rule flow:



Block

https Traffic Blocked from John (john)(172.16.10.200) to 46.43.34.31

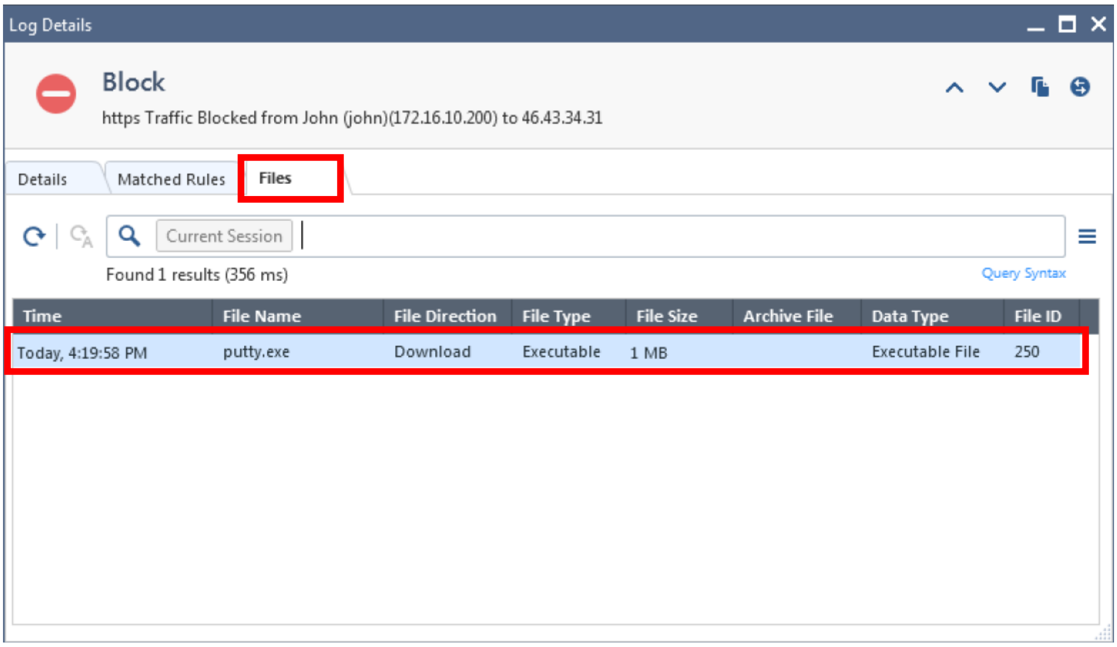
Matched Rules

Rule	Layer	Rule Name	Action	Application	Category
3	Network	Web Traffic	Inline		
3.6	Web Layer	Cleanup rule	Accept		
1	Data Layer	Block Download of...	Block		

First, the connection was matched against the **Network Layer**, specifically against the parent rule of the web inline layer. Since it matched the parent rule, the traffic was matched next against the sub-rules. Because none of the rules 3.1 up to 3.5 were a match, traffic was matched against the **Cleanup Rule**, 3.6, which has the **Action** to **Allow.**

Last, following ordered layers' rules, the traffic was matched against the next ordered layer – Data Layer. The traffic was matched against the first rule, blocking download access of putty.EXE file.

In order to validate this, we can click on the 3rd tab, **Files** and see the exact file name that was blocked:



Block

https Traffic Blocked from John (john)(172.16.10.200) to 46.43.34.31

Found 1 results (356 ms)

Time	File Name	File Direction	File Type	File Size	Archive File	Data Type	File ID
Today, 4:19:58 PM	putty.exe	Download	Executable	1 MB		Executable File	250

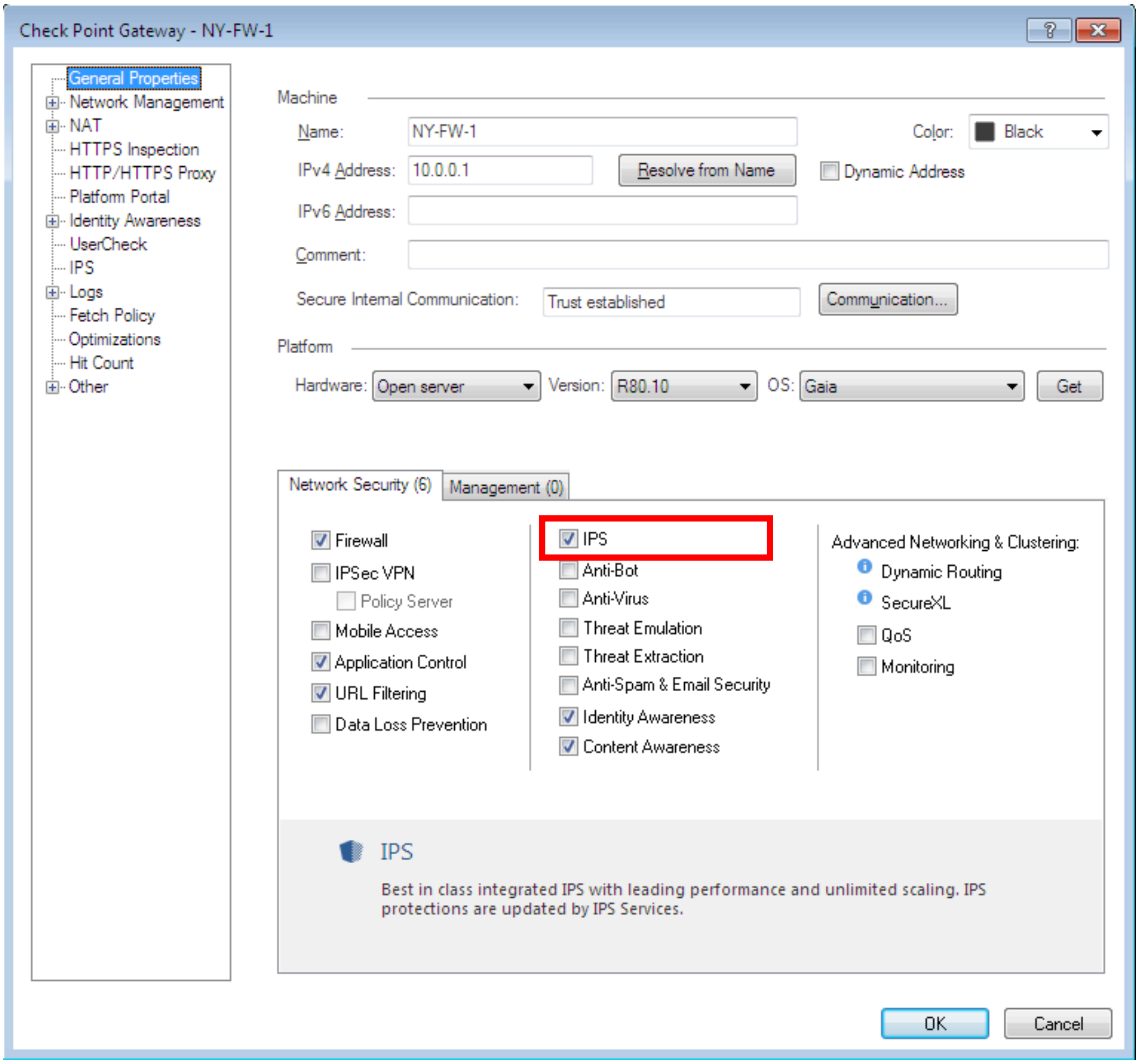
… and here is the confirmation, **File Name – putty.exe.**

44.0 Lab: Configure IPS Protection Profile

Lab Objectives

- Activate Check Point IPS software blade
- Configure IPS Protection Profile

First thing that we need to do now is to activate the IPS software blade. As we are working on New York site, we will have to open **NY-FW-1** object and enable the IPS blade:



Check Point Gateway - NY-FW-1

Machine

Name: NY-FW-1

Color: Black

IPv4 Address: 10.0.0.1

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server

Version: R80.10

OS: Gaia

☑ Firewall
□ IPSec VPN
□ Policy Server
□ Mobile Access
☑ Application Control
☑ URL Filtering
□ Data Loss Prevention

☑ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
☑ Identity Awareness
☑ Content Awareness

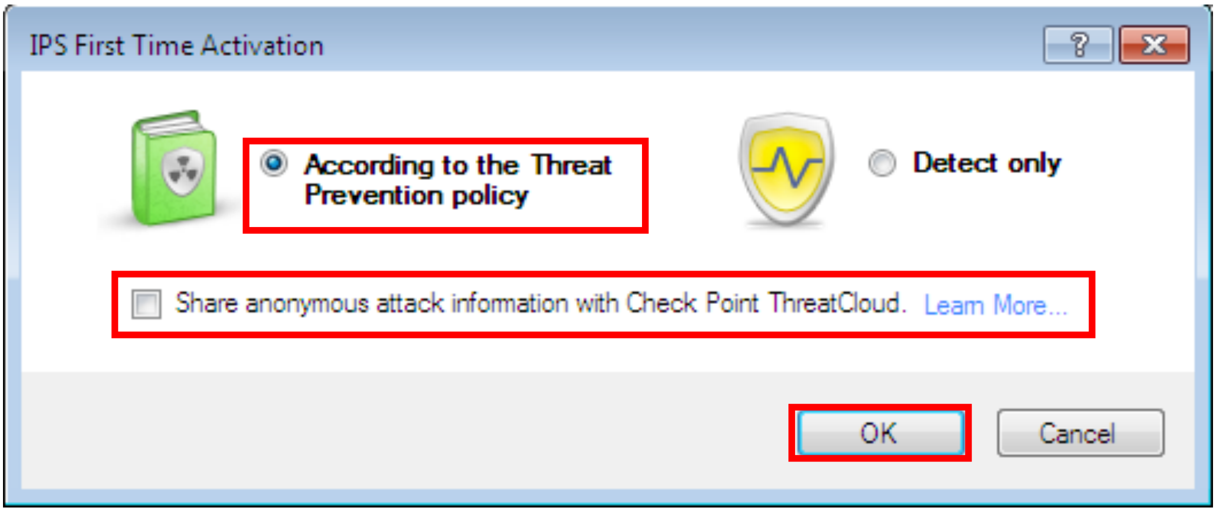
Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
□ Monitoring

IPS

Best in class integrated IPS with leading performance and unlimited scaling. IPS protections are updated by IPS Services.

Once you tick the **IPS** blade, immediately the IPS activation setup begins.

Now, there are two options displayed. The default option, **According to the Threat Prevention policy** represents IPS, which stands for Intrusion **Prevention** System, so this is **prevention** and not **detection.**



IPS First Time Activation

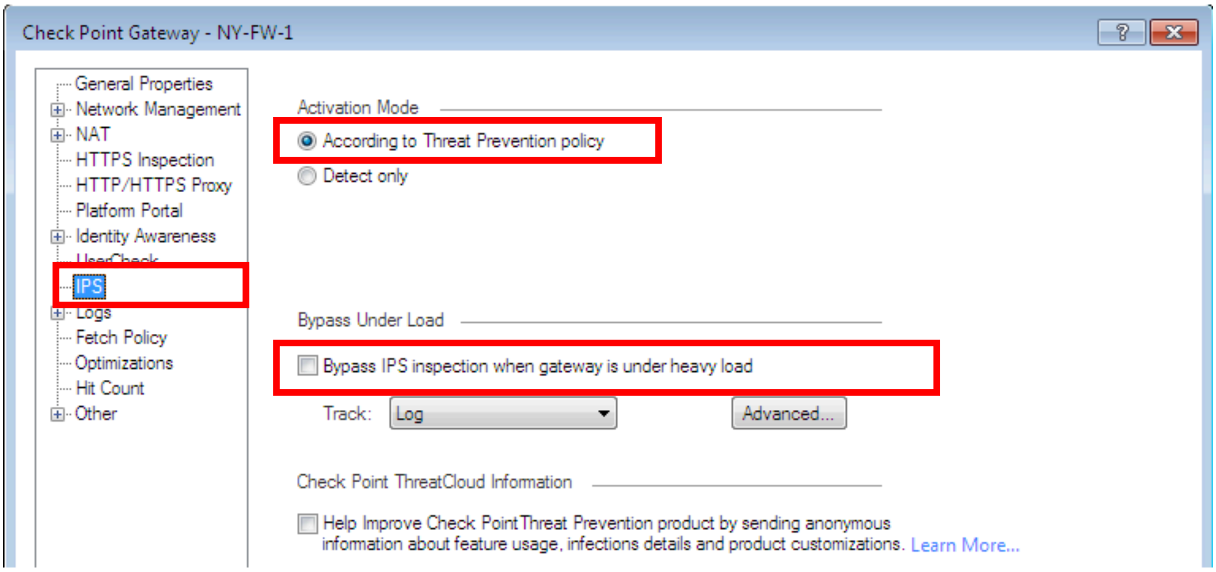
● According to the Threat Prevention policy

○ Detect only

□ Share anonymous attack information with Check Point ThreatCloud. Learn More...

If you select the second option – **Detect only**, you would then configure your appliance to act as an IDS – Intrusion Detection System, which means that it will only detect malicious activities, but will not stop them.

Just leave the default option selected, uncheck the sharing information option at the bottom and click **OK** in order to continue. We are now back in the main page of NY-FW-1. Click on **IPS** on the left-hand side menu and make sure that **IPS** functionality is there, and not Detection.



Check Point Gateway - NY-FW-1

Activation Mode

● According to Threat Prevention policy

○ Detect only

Bypass Under Load

□ Bypass IPS inspection when gateway is under heavy load

Track: Log

Check Point ThreatCloud Information

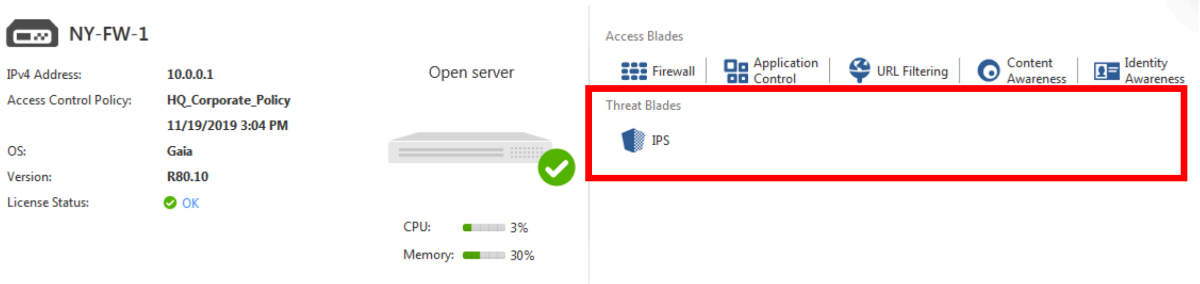
□ Help Improve Check Point Threat Prevention product by sending anonymous information about feature usage, infections details and product customizations. Learn More...

One interesting option is the **Bypass IPS inspection when the gateway is under heavy load**. By the default is unchecked and it is the recommended option. Why is that?

If you check this option, it means that if the gateway is experience high load, it will just skip IPS verification and this drastically affects the overall security standards in any organization. I would rather prefer to wait a little bit so that the Security Gateway processes the traffic and after that forwards the clean traffic to the intended destination.

In order to continue, just click **OK.**

We can immediately see the change, IPS is displayed now as the first Threat Prevention active blade.


NY-FW-1

IPv4 Address: 10.0.0.1
Access Control Policy: HQ_Corporate_Policy
11/19/2019 3:04 PM
OS: Gaia
Version: R80.10
License Status: OK

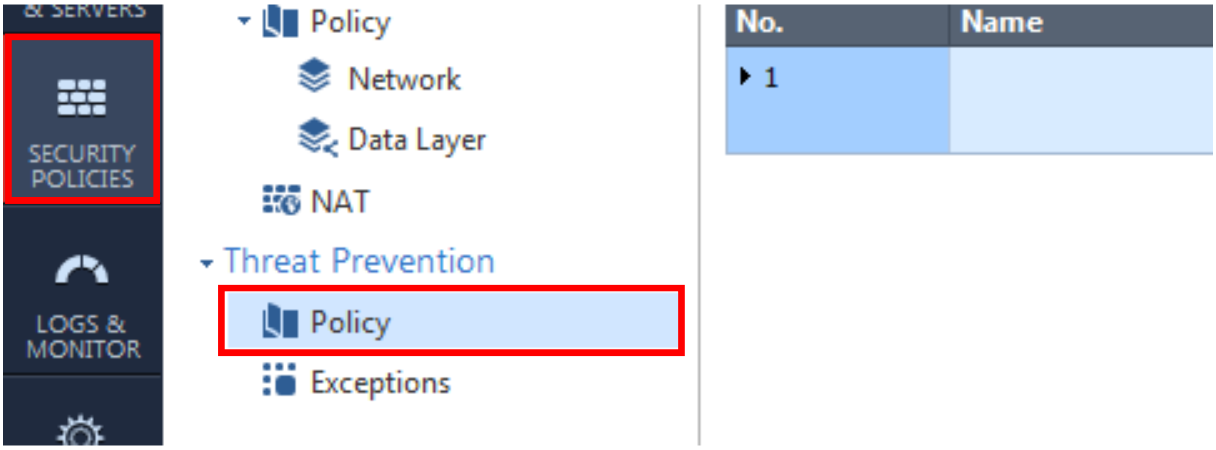
Open server

CPU: 3%
Memory: 30%

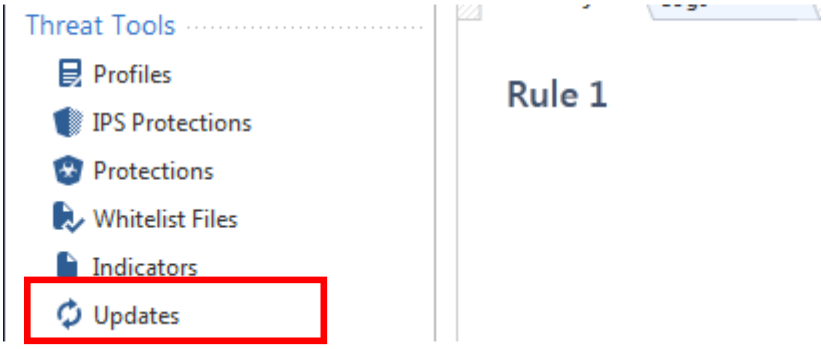
Access Blades: Firewall, Application Control, URL Filtering, Content Awareness, Identity Awareness

Threat Blades: IPS

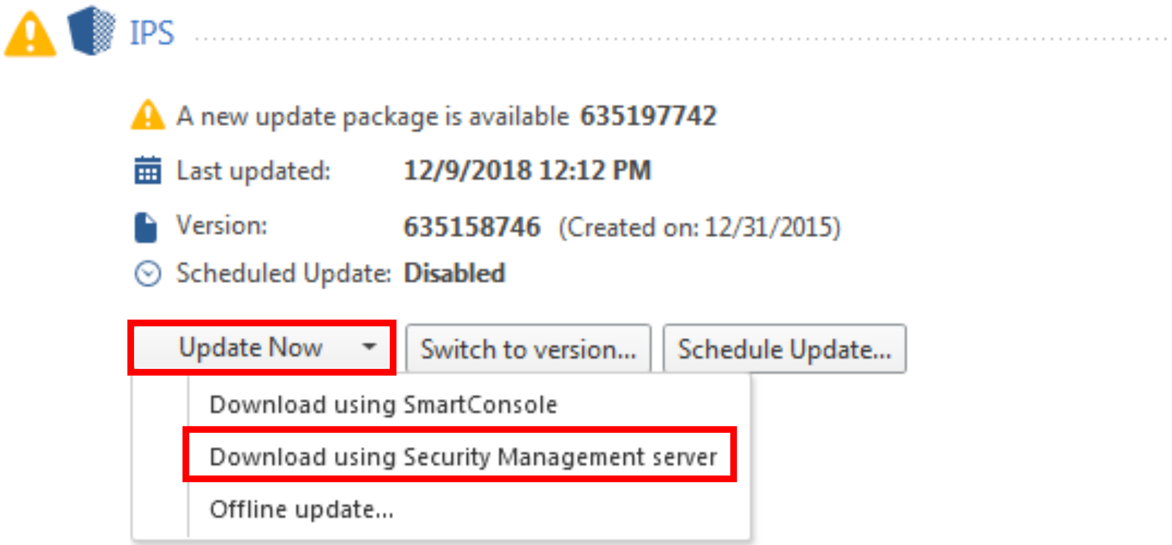
Before we continue with IPS and actually almost any Threat Prevention software blade, we should first update the database in order to benefit of the latest protections. In case of IPS, go to **Security Policies** on the left and click on **Policy** under **Threat Prevention**:



Next, click on **Updates** at the bottom left-side of SmartConsole.



If any update is available for IPS Database and must probably there is, your screen should look similar to the following:



IPS

A new update package is available 635197742

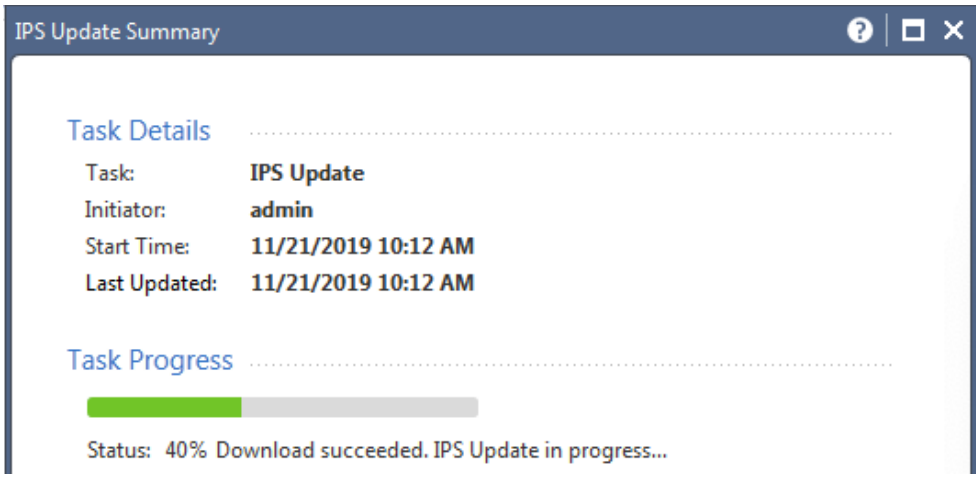
Last updated: 12/9/2018 12:12 PM

Version: 635158746 (Created on: 12/31/2015)

Scheduled Update: Disabled

Update Now
Switch to version...
Schedule Update...
Download using SmartConsole
Download using Security Management server
Offline update...

A new task is immediately started and you can monitor the progress by clicking on the bottom-left menu, just like for a policy install:



IPS Update Summary

Task Details

Task: IPS Update

Initiator: admin

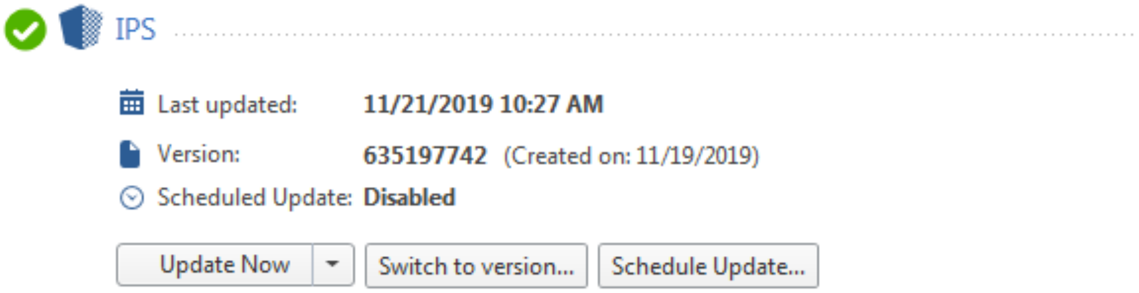
Start Time: 11/21/2019 10:12 AM

Last Updated: 11/21/2019 10:12 AM

Task Progress

Status: 40% Download succeeded. IPS Update in progress...

The update will take some time, depending on the underlying hardware and how much resources you have allocated to the Security Management Server. When complete, you should see that IPS is up-to-date, in the **Security Policy -> Threat Prevention Policy -> Updates**.

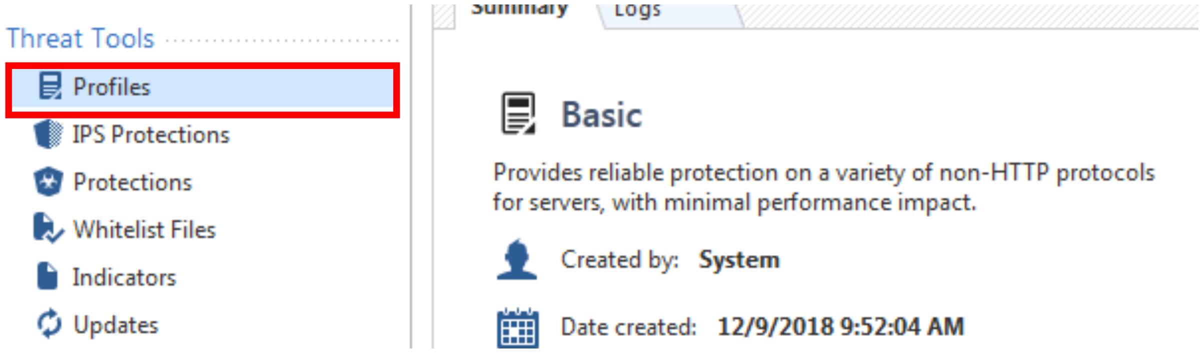


Last updated: 11/21/2019 10:27 AM

Version: 635197742 (Created on: 11/19/2019)

Scheduled Update: Disabled

Now, we will create a new IPS profile. In order to do this, click on **Profiles**, just above the **Updates** menu,



Basic

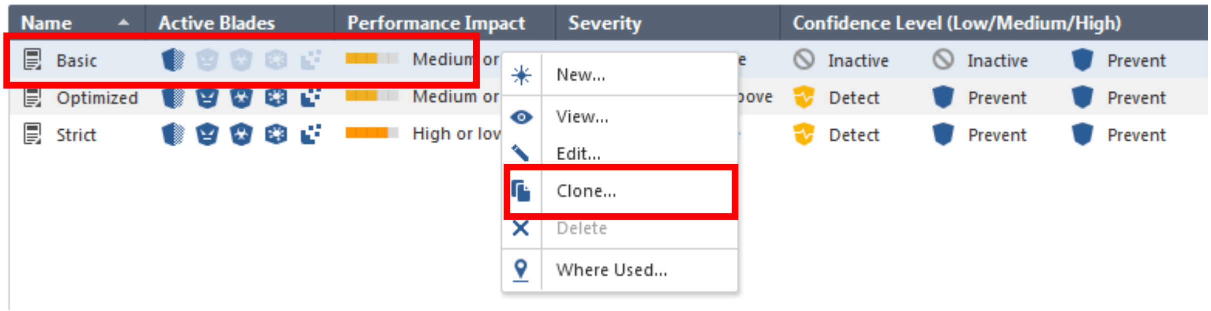
Provides reliable protection on a variety of non-HTTP protocols for servers, with minimal performance impact.

Created by: System

Date created: 12/9/2018 9:52:04 AM

and you will be displayed the three default IPS profiles – Basic, Optimized and Strict.

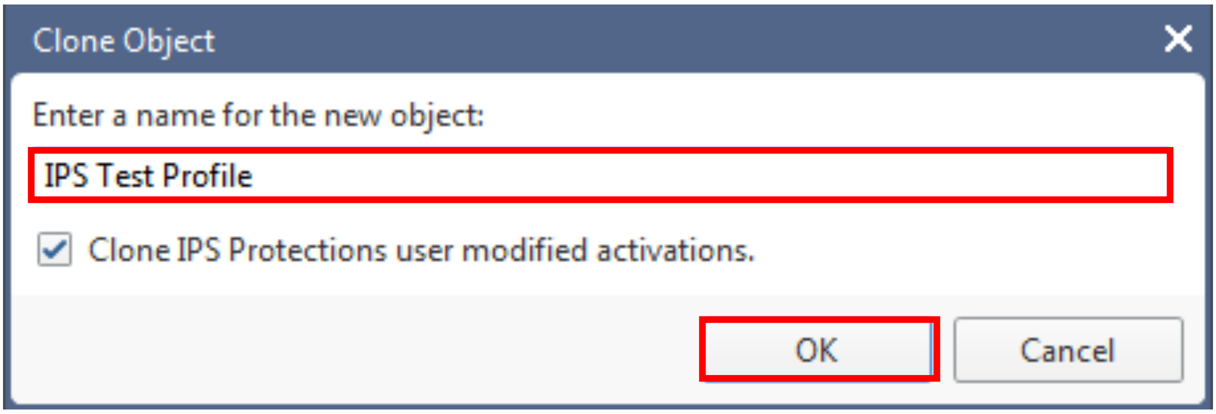
Select the **Basic** profile, right-click on it and select **Clone** option.



Name	Active Blades	Performance Impact	Severity	Confidence Level (Low/Medium/High)		
Basic		Medium or	e	Inactive	Inactive	Prevent
Optimized		Medium or	bove	Detect	Prevent	Prevent
Strict		High or low		Detect	Prevent	Prevent

Just in case we want to revert the changes and come back to the original profile – **Basic**, we wouldn't be able to do that if we implement any changes on it. So we will clone it, so create a new one and configure what we need on this new IPS profile.

I will name the profile as **IPS Test Profile** and click **OK** in order to continue.



Clone Object

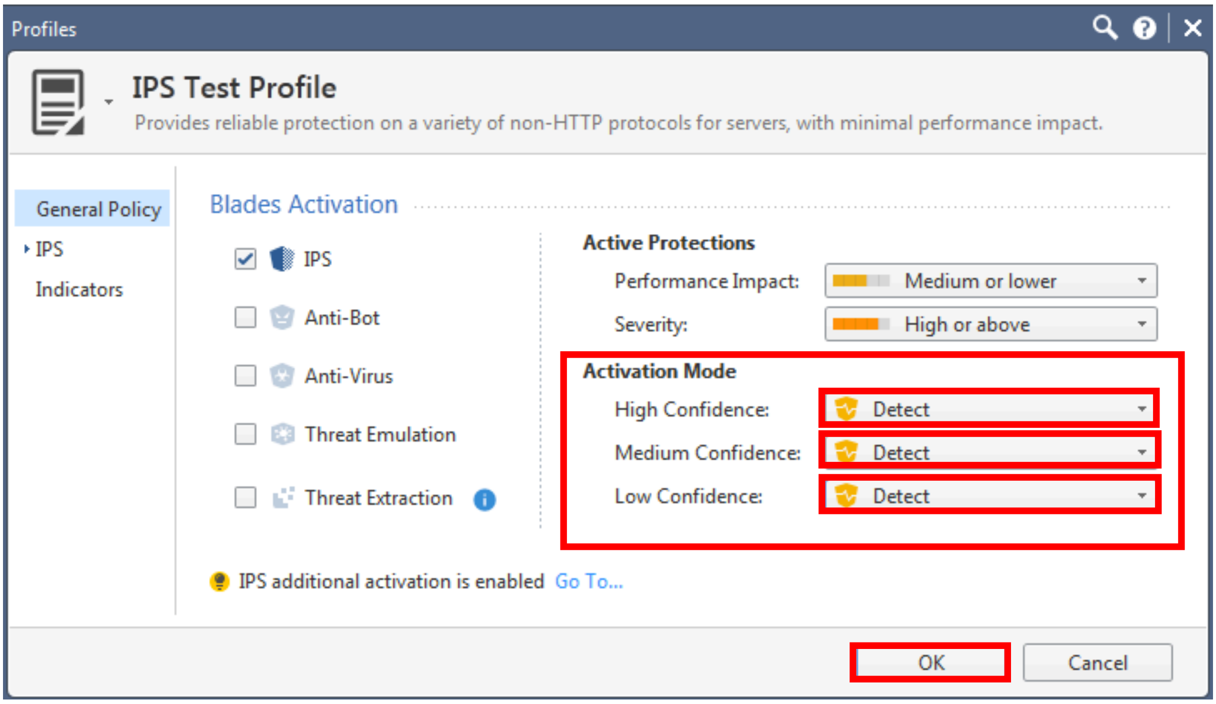
Enter a name for the new object:

IPS Test Profile

☑ Clone IPS Protections user modified activations.

Now, I will right-click on the new IPS profile – **IPS Test Profile** and select **Edit**.

For now, I will configure **Detect** in the **Activation Mode.** This means that no matter how confident the security gateway is on a specific attack that it sees, it will not block the traffic, it will detect it and log it, but nothing more.



Profiles

IPS Test Profile

Provides reliable protection on a variety of non-HTTP protocols for servers, with minimal performance impact.

Blades Activation

☑ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction

Active Protections

Performance Impact: Medium or lower

Severity: High or above

Activation Mode

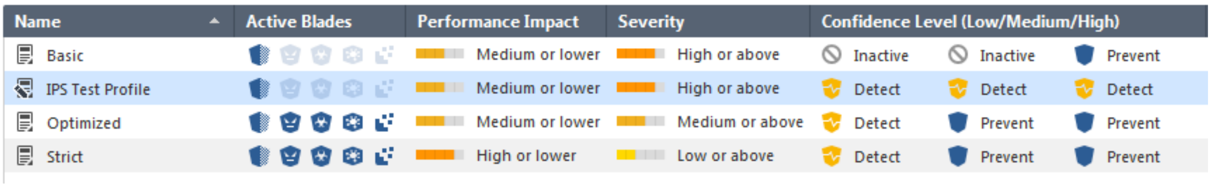
High Confidence: Detect

Medium Confidence: Detect

Low Confidence: Detect

IPS additional activation is enabled Go To...

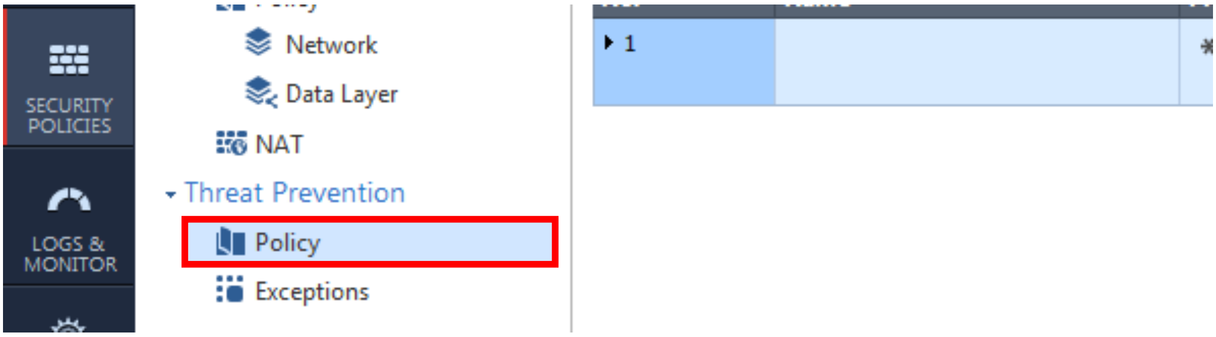
Click **OK** in order to continue. We now have 4 IPS profiles available:



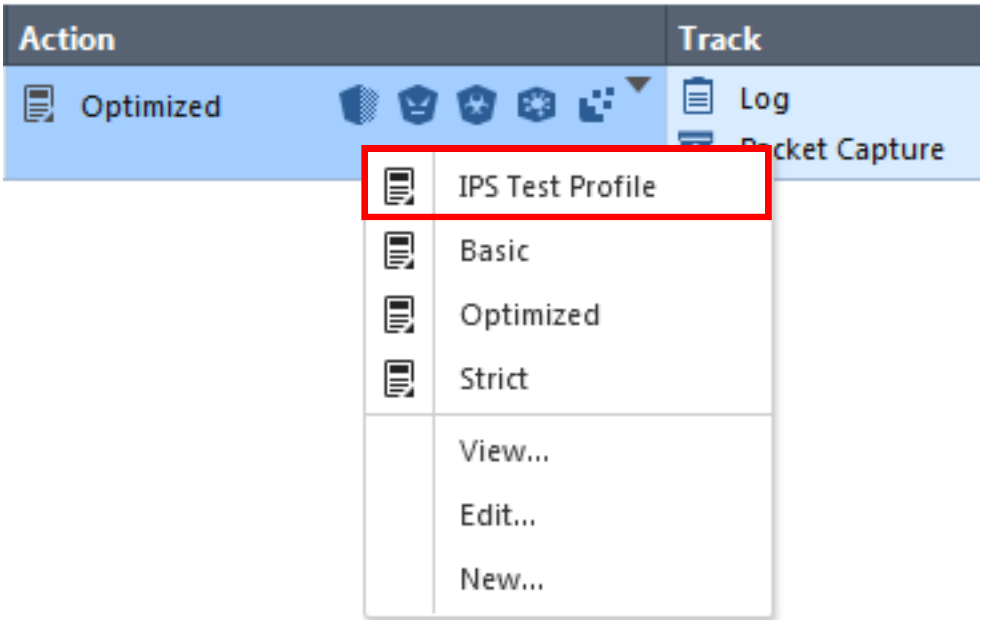
Name	Active Blades	Performance Impact	Severity	Confidence Level (Low/Medium/High)		
Basic		Medium or lower	High or above	Inactive	Inactive	Prevent
IPS Test Profile		Medium or lower	High or above	Detect	Detect	Detect
Optimized		Medium or lower	Medium or above	Detect	Prevent	Prevent
Strict		High or lower	Low or above	Detect	Prevent	Prevent

And we would like to apply our **IPS Test Profile** to the **Threat Prevention** policy.

Click on **Policy** under **Threat Prevention**:



Right-click on the **Action** column and select our profile – **IPS Test Profile**:



Now, let's publish and install the **Threat Prevention** policy, along with the **Access Control** policy. Theoretically speaking, we could unselect Access Control policy when initiating the policy install, as no modifications were made here.

This can help with resources optimization while pushing large policies to a lot of Check Point devices.

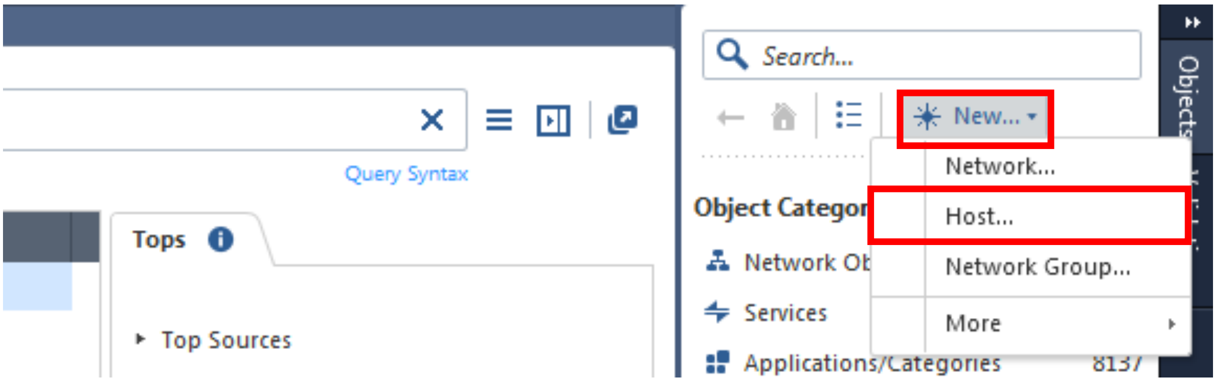
45.0 Lab: IPS Setup - Verification and Testing

Lab Objectives

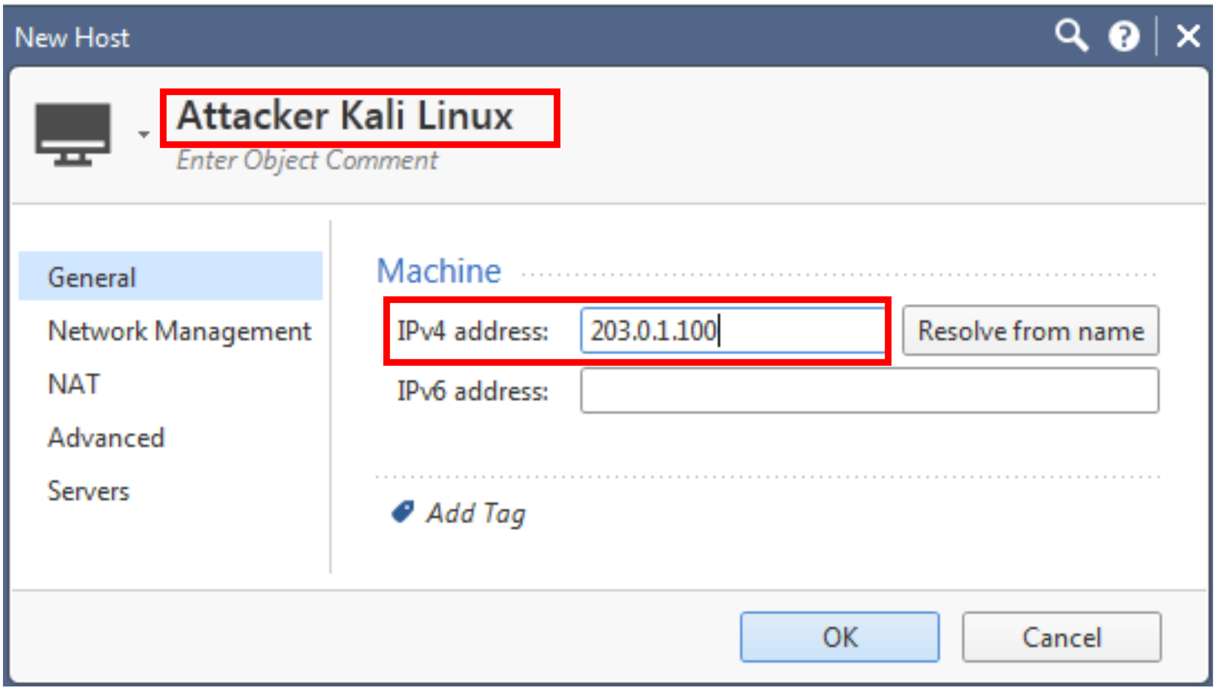
- Run verification and testing for IPS Blade

Before we continue, let’s create a new **Host Object** in SmartConsole in order to define the **Attacker Kali Linux** machine.

At the top-right corner, expand the **Objects** panel and click on **New** and **Host**:



Let’s name this object – **Attacker Kali Linux** and insert the IPv4 address as **203.0.1.100**.



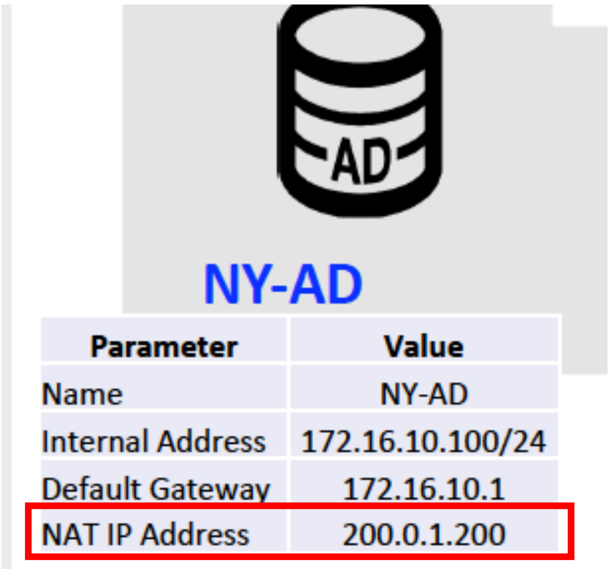
Attacker Kali Linux

IPv4 address: 203.0.1.100

IPv6 address:

Now, let’s publish and install the HQ_Corporate_Policy.

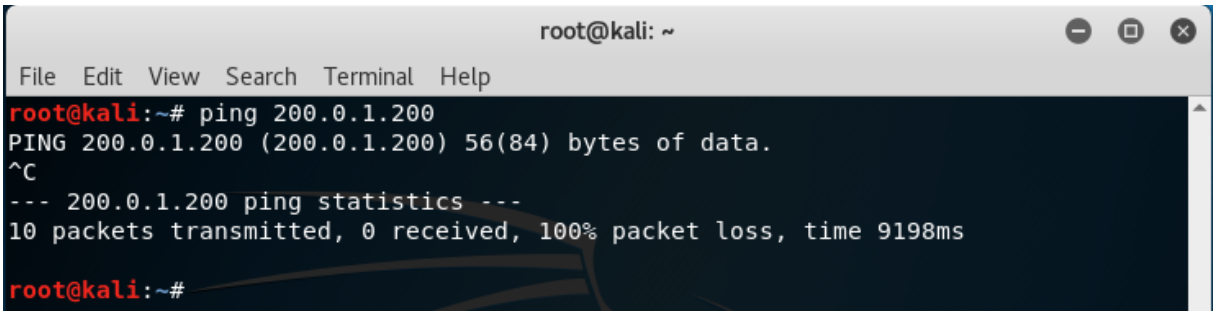
If you take a look on the diagram – **Course Lab Diagram v2.0**, you will notice that NY-AD server also has NAT IP address information attached.



Parameter	Value
Name	NY-AD
Internal Address	172.16.10.100/24
Default Gateway	172.16.10.1
NAT IP Address	200.0.1.200

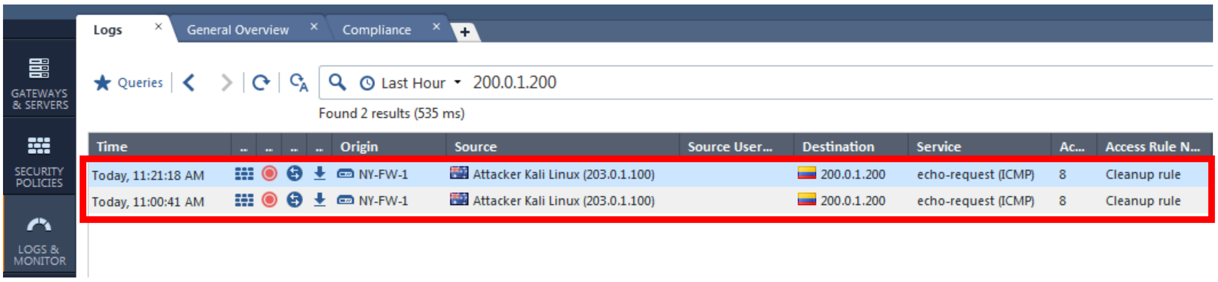
We will send attack toward this IP address. Remember that some labs ago we have configured static NAT on NY-FW-1 and exposed to internet multiple objects: NY-SMS-1, NY-AD and NY-DMZ. All of these objects have NAT IP Address information displayed on the diagram, just for ease of use.

On the Kali Linux Machine, let's now initiate a ping session towards the AD server – 200.0.1.200 IP address.



```
root@kali:~# ping 200.0.1.200
PING 200.0.1.200 (200.0.1.200) 56(84) bytes of data.
^C
--- 200.0.1.200 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9198ms

root@kali:~#
```

If we take a look at the logs, filter using the **200.0.1.200** IP address:



Last Hour 200.0.1.200

Found 2 results (535 ms)

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 11:21:18 AM					NY-FW-1	Attacker Kali Linux (203.0.1.100)		200.0.1.200	echo-request (ICMP)	8	Cleanup rule
Today, 11:00:41 AM					NY-FW-1	Attacker Kali Linux (203.0.1.100)		200.0.1.200	echo-request (ICMP)	8	Cleanup rule

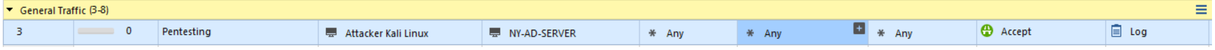
we see that currently the connections are being blocked by the **Cleanup Rule**, which is now Rule 8 in the Access Control Policy, after optimizing our policy with inline and ordered layers.

In order to test IPS functionality, we will now add a new rule in the Access Control rule base in order to permit ICMP traffic from **Attacker Kali Linux** to **NY-AD** server. We don't want our traffic to be blocked by the Firewall blade, we want to see IPS in action.

So, I will add a rule above rule 3 – Web Traffic, with the following details:

Name – Pentesting
Source – Attacker Kali Linux
Destination – NY-AD-SERVER
Services & Applications – Any
Action – Accept
Tracking – Log

The new rule should like the one below:

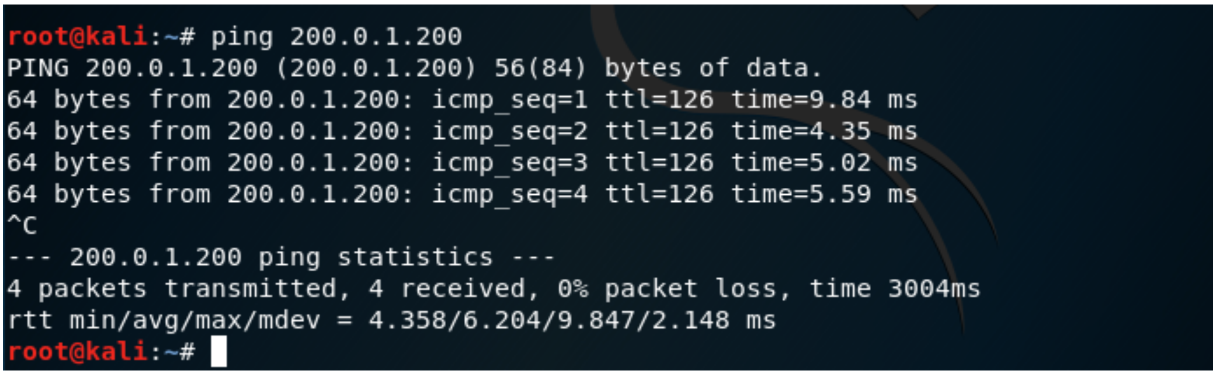


General Traffic (3-8)

3	0	Pentesting	Attacker Kali Linux	NY-AD-SERVER	Any	Any	Any	Accept	Log

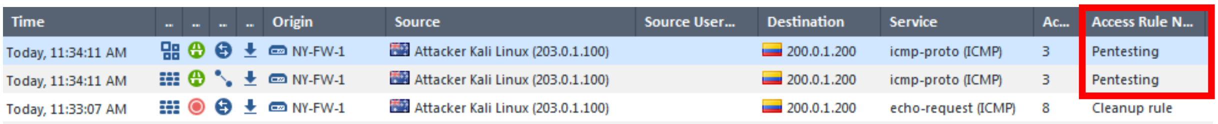
Now, publish the changes and install HQ policy.

After the policy is successfully installed, we should we able to see that ICMP is working now from **Attacker Kali Linux** to **NY-AD-Server:**



```
root@kali:~# ping 200.0.1.200
PING 200.0.1.200 (200.0.1.200) 56(84) bytes of data.
64 bytes from 200.0.1.200: icmp_seq=1 ttl=126 time=9.84 ms
64 bytes from 200.0.1.200: icmp_seq=2 ttl=126 time=4.35 ms
64 bytes from 200.0.1.200: icmp_seq=3 ttl=126 time=5.02 ms
64 bytes from 200.0.1.200: icmp_seq=4 ttl=126 time=5.59 ms
^C
--- 200.0.1.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 4.358/6.204/9.847/2.148 ms
root@kali:~# 
```

and that we see **Accept** logs on the management server:



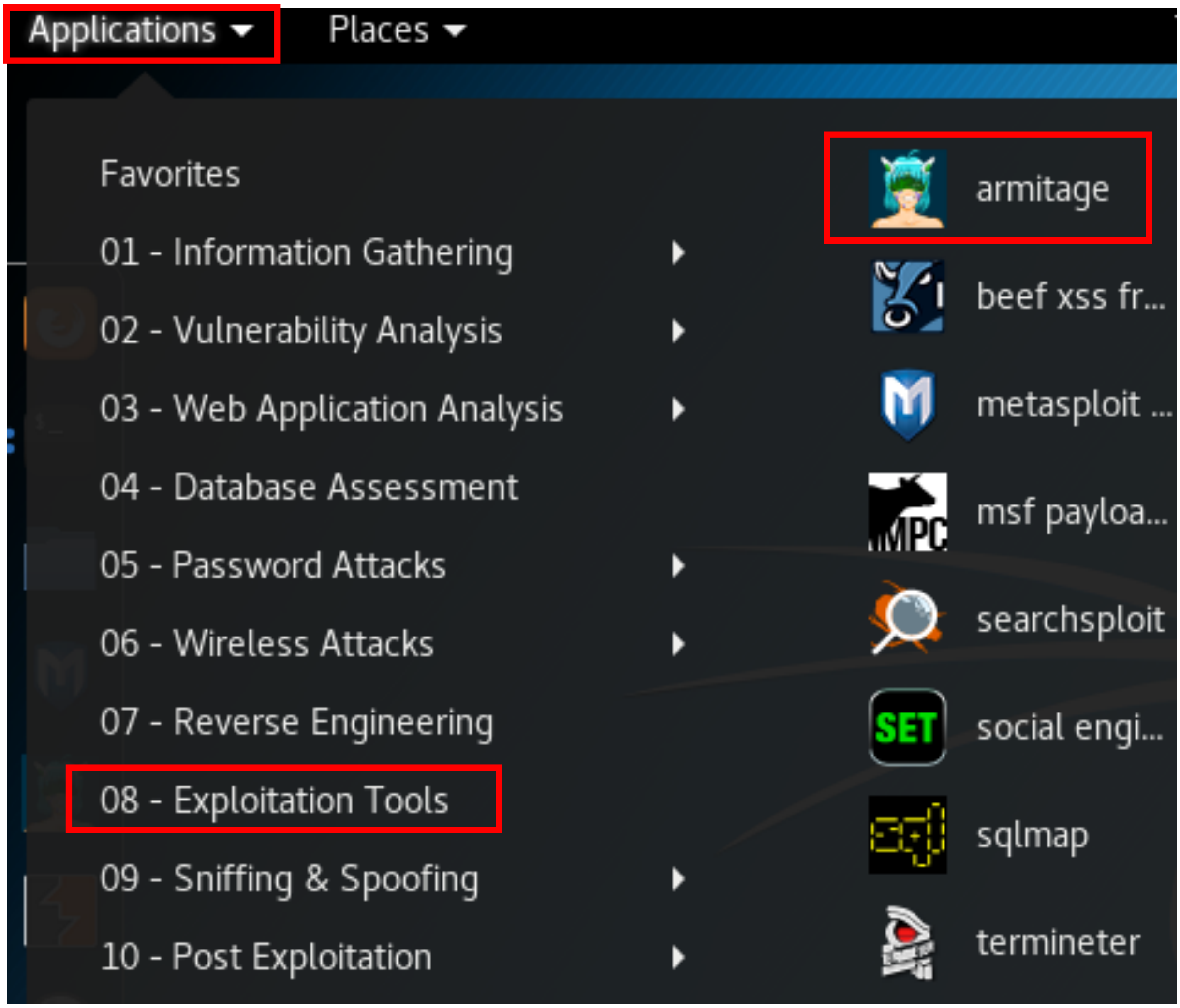
Time	...	...	...	...	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 11:34:11 AM					NY-FW-1	Attacker Kali Linux (203.0.1.100)		200.0.1.200	icmp-proto (ICMP)	3	Pentesting
Today, 11:34:11 AM					NY-FW-1	Attacker Kali Linux (203.0.1.100)		200.0.1.200	icmp-proto (ICMP)	3	Pentesting
Today, 11:33:07 AM					NY-FW-1	Attacker Kali Linux (203.0.1.100)		200.0.1.200	echo-request (ICMP)	8	Cleanup rule

As you can see in the last column above, traffic is being permitted due to our new rule – **Pentesting**.

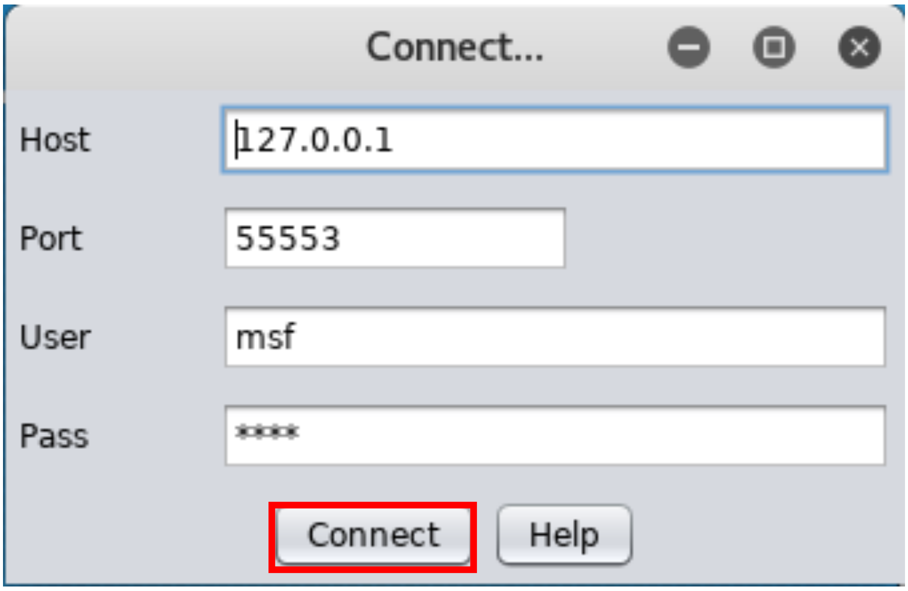
Now we will launch an attack from Attacker Linux Machine and if everything is working as expected, we should be able to see some IPS logs, with the action of **Detect.**

On the Kali Linux machine, we will launch an attack, trying to exploit a well-known vulnerability **MS12-020**. We will use a built-in attack tool, **Armitage**.

Click on **Applications** in the top-left corner, next **08-Exploitation Tools** and last **armitage**.



Now, we will leave all the options as they are (default state) and just click on **Connect**.



Connect...

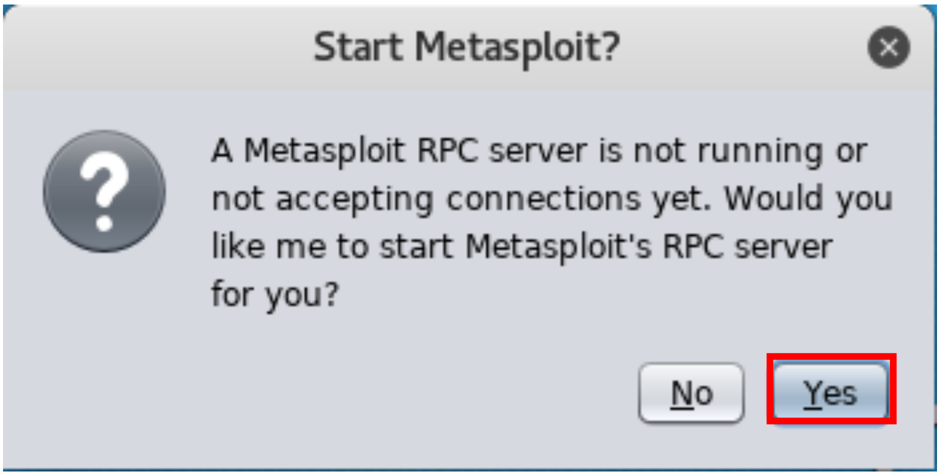
Host 127.0.0.1

Port 55553

User msf

Pass ****

In the next screen confirm that you want the Metasploit server to start by clicking **Yes**:



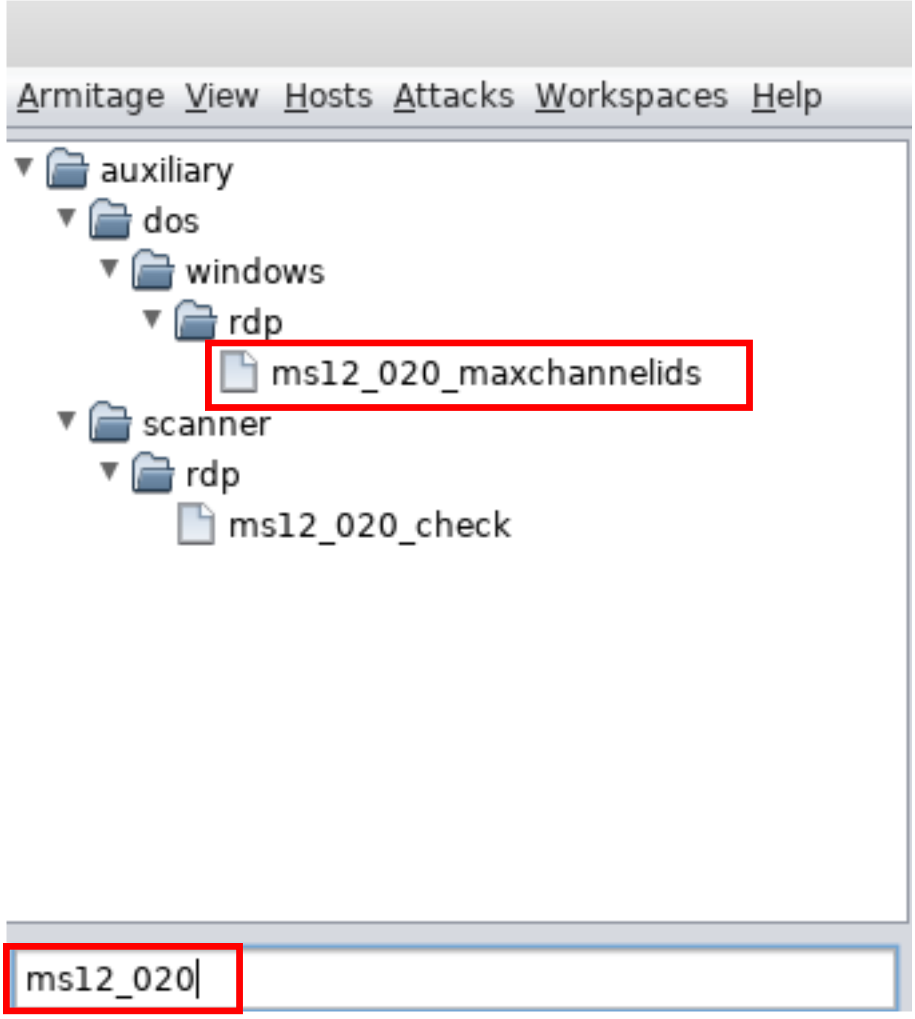
Start Metasploit?

A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?

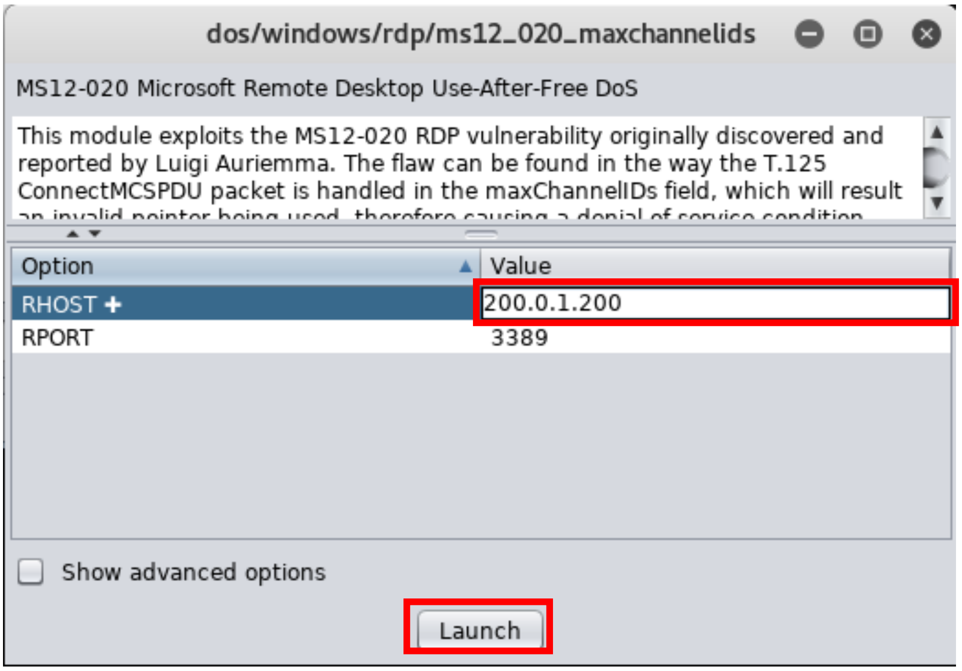
If you search for this vulnerability on the internet, you will find a detailed description of what it does. Here is a brief summary:

“The Remote Desktop Protocol (RDP) implementation does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that was not properly initialized”.

Now that **Armitage** is running, let’s search the vulnerability code in the search bar. Again, we will search for **MS12_020**, just see below.



Double-click on the upper selection, see above, and a new window will open:



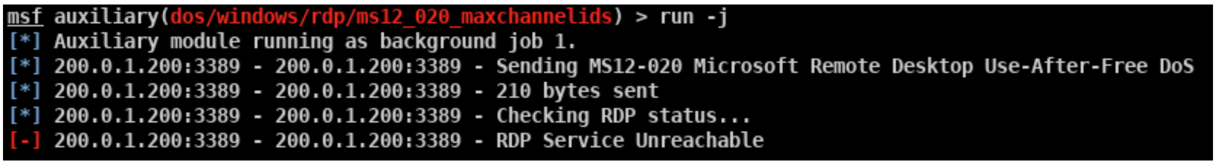
MS12-020 Microsoft Remote Desktop Use-After-Free DoS

This module exploits the MS12-020 RDP vulnerability originally discovered and reported by Luigi Auriemma. The flaw can be found in the way the T.125 ConnectMCSPDU packet is handled in the maxChannelIDs field, which will result an invalid pointer being used, therefore causing a denial of service condition.

Option	Value
RHOST ✚	200.0.1.200
RPORT	3389

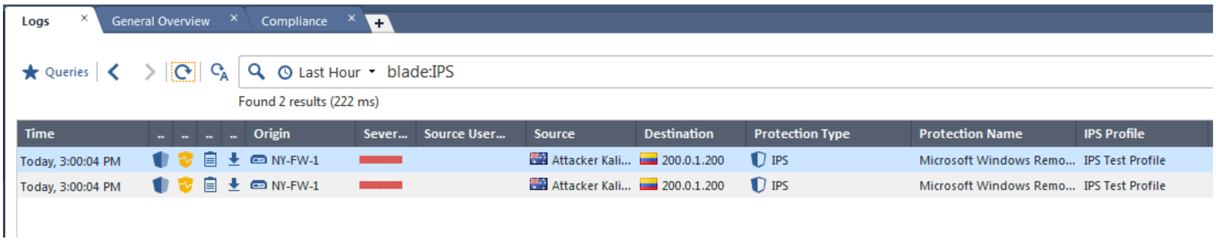
Now double-click in the **Value** column and enter the IP of NY-AD-SERVER – **200.0.1.200** and after that just click on **Launch**.

Once the code execution is run, the output in the Armitage console should look similar to the following:



```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run -j
[*] Auxiliary module running as background job 1.
[*] 200.0.1.200:3389 - 200.0.1.200:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 200.0.1.200:3389 - 200.0.1.200:3389 - 210 bytes sent
[*] 200.0.1.200:3389 - 200.0.1.200:3389 - Checking RDP status...
[-] 200.0.1.200:3389 - 200.0.1.200:3389 - RDP Service Unreachable
```

Let’s now switch to SmartConsole and search for **IPS** logs. The below output confirms the IPS logs:

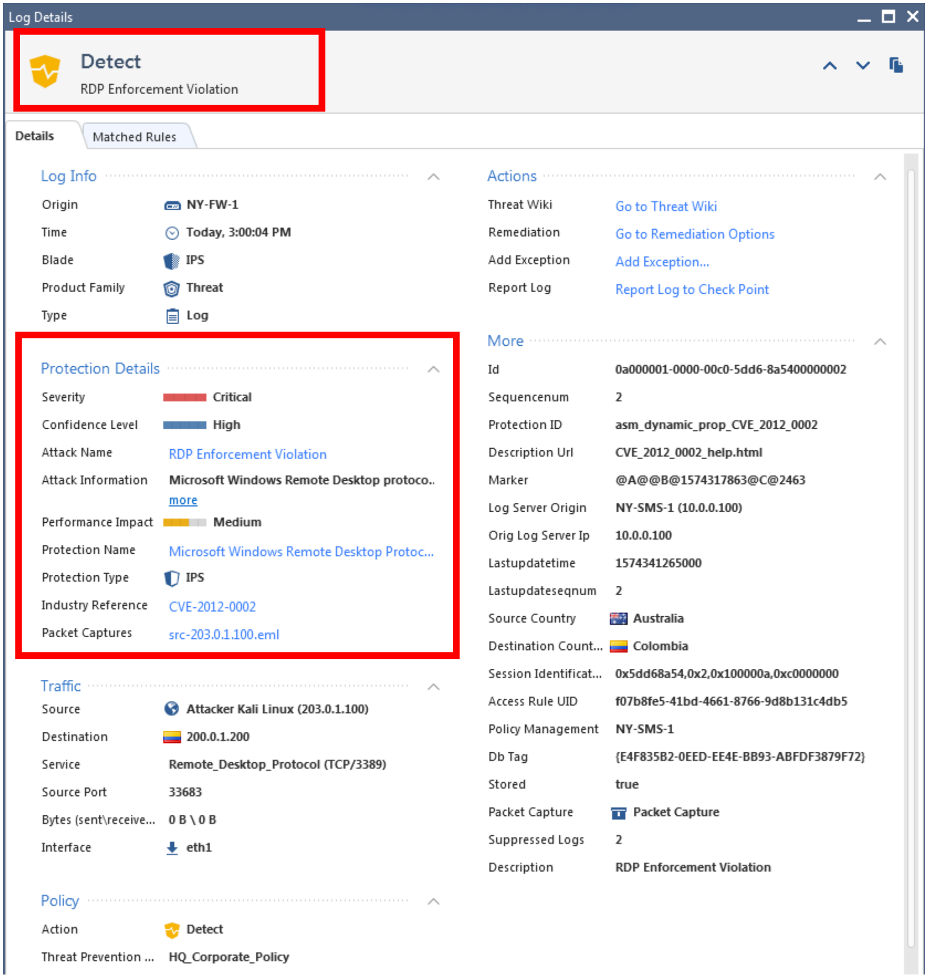


blade:IPS

Found 2 results (222 ms)

Time	..	..	..	..	Origin	Sever...	Source User...	Source	Destination	Protection Type	Protection Name	IPS Profile
Today, 3:00:04 PM					NY-FW-1	🟥		Attacker Kali...	200.0.1.200	IPS	Microsoft Windows Remo...	IPS Test Profile
Today, 3:00:04 PM					NY-FW-1	🟥		Attacker Kali...	200.0.1.200	IPS	Microsoft Windows Remo...	IPS Test Profile

If we now open one of the logs:



Detect

RDP Enforcement Violation

Log Info

Origin	NY-FW-1
Time	Today, 3:00:04 PM
Blade	IPS
Product Family	Threat
Type	Log

Protection Details

Severity	Critical
Confidence Level	High
Attack Name	RDP Enforcement Violation
Attack Information	Microsoft Windows Remote Desktop protoco.. more
Performance Impact	Medium
Protection Name	Microsoft Windows Remote Desktop Protoc...
Protection Type	IPS
Industry Reference	CVE-2012-0002
Packet Captures	src-203.0.1.100.eml

Traffic

Source	Attacker Kali Linux (203.0.1.100)
Destination	200.0.1.200
Service	Remote_Desktop_Protocol (TCP/3389)
Source Port	33683
Bytes (sent\receive...	0 B \ 0 B
Interface	eth1

Policy

Action	Detect
Threat Prevention ...	HQ_Corporate_Policy

Actions

Threat Wiki	Go to Threat Wiki
Remediation	Go to Remediation Options
Add Exception	Add Exception...
Report Log	Report Log to Check Point

More

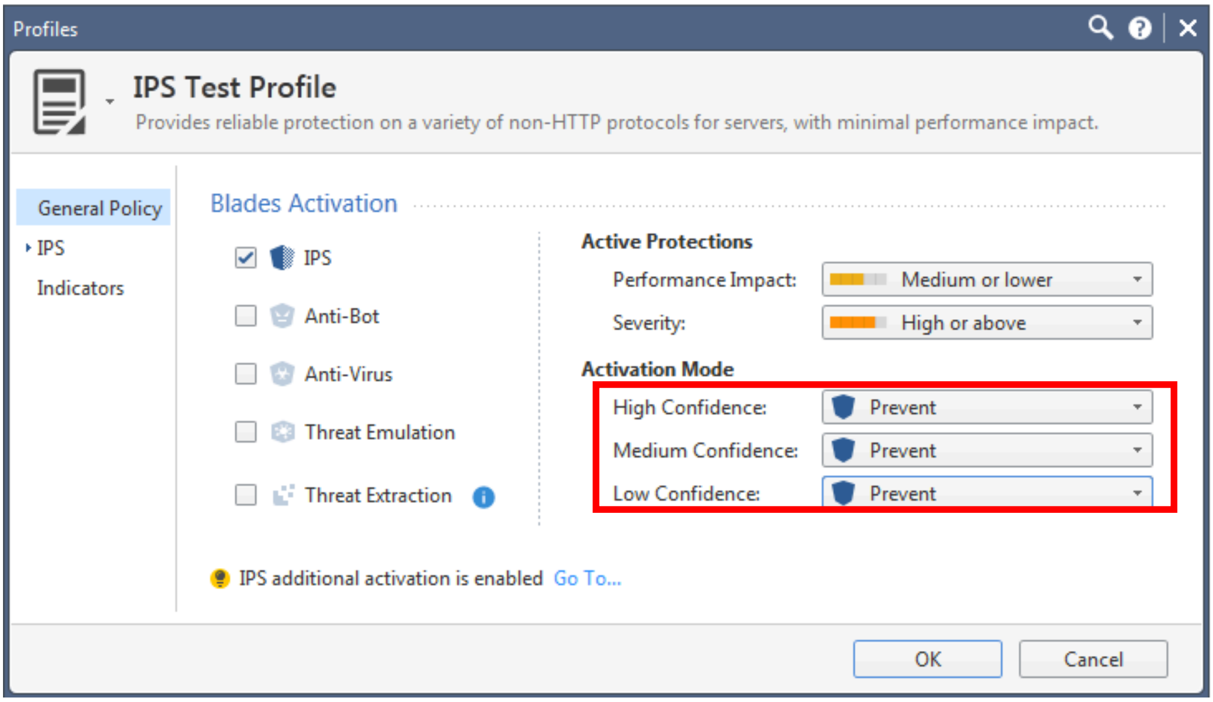
Id	0a000001-0000-00c0-5dd6-8a5400000002
Sequencenum	2
Protection ID	asm_dynamic_prop_CVE_2012_0002
Description Url	CVE_2012_0002_help.html
Marker	@A@@B@1574317863@C@2463
Log Server Origin	NY-SMS-1 (10.0.0.100)
Orig Log Server Ip	10.0.0.100
Lastupdatetime	1574341265000
Lastupdateseqnum	2
Source Country	Australia
Destination Count...	Colombia
Session Identificat...	0x5dd68a54,0x2,0x100000a,0xc0000000
Access Rule UID	f07b8fe5-41bd-4661-8766-9d8b131c4db5
Policy Management	NY-SMS-1
Db Tag	{E4F835B2-0EED-EE4E-BB93-ABFDF3879F72}
Stored	true
Packet Capture	Packet Capture
Suppressed Logs	2
Description	RDP Enforcement Violation

We can find good information about the attack. First of all, and most important is that the attack was detected, and not blocked.

Protection Details section is also important and highlights Protection name, which Blade actually was used in the Process – and it is **IPS.** Also, good as a reference for further documentation, the **industry reference** is also present here – CVE-2012-0002, where CVE stands for Common Vulnerabilities and Exposures. The rest are pretty self-explanatory.

Last thing to do in this lab is changing the IPS Activation Mode from **Detect** to **Prevent**. Go to **Security Policies,** under Threat Prevention go to **Policies,** right-click on the Action Column – **IPS Test Profile** and select **Edit.**

The configuration should look as below, click **OK** when done.


Profiles

IPS Test Profile

Provides reliable protection on a variety of non-HTTP protocols for servers, with minimal performance impact.

Blades Activation

☑ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction

Active Protections

Performance Impact: Medium or lower
Severity: High or above

Activation Mode

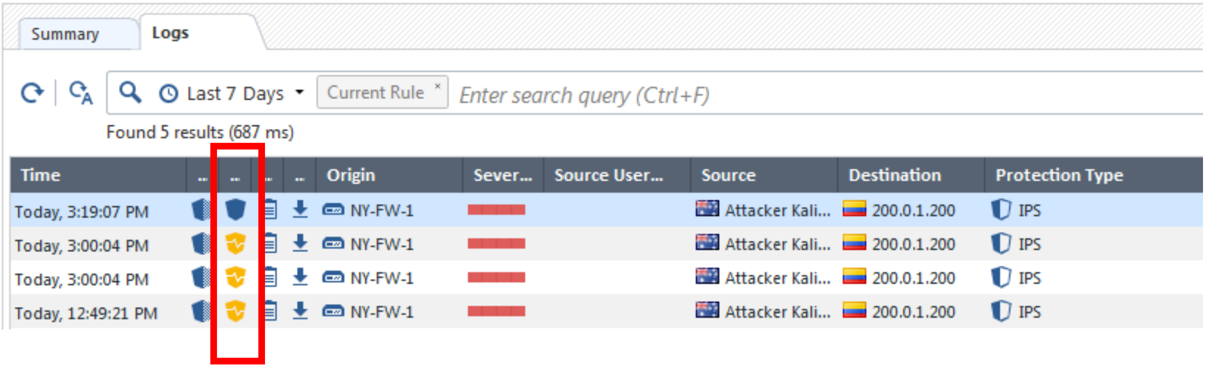
High Confidence: Prevent
Medium Confidence: Prevent
Low Confidence: Prevent

IPS additional activation is enabled Go To...

Publish the changes and install the HQ policy.

After installation is complete, run again the attack from the **Attacker Kali Linux** machine.

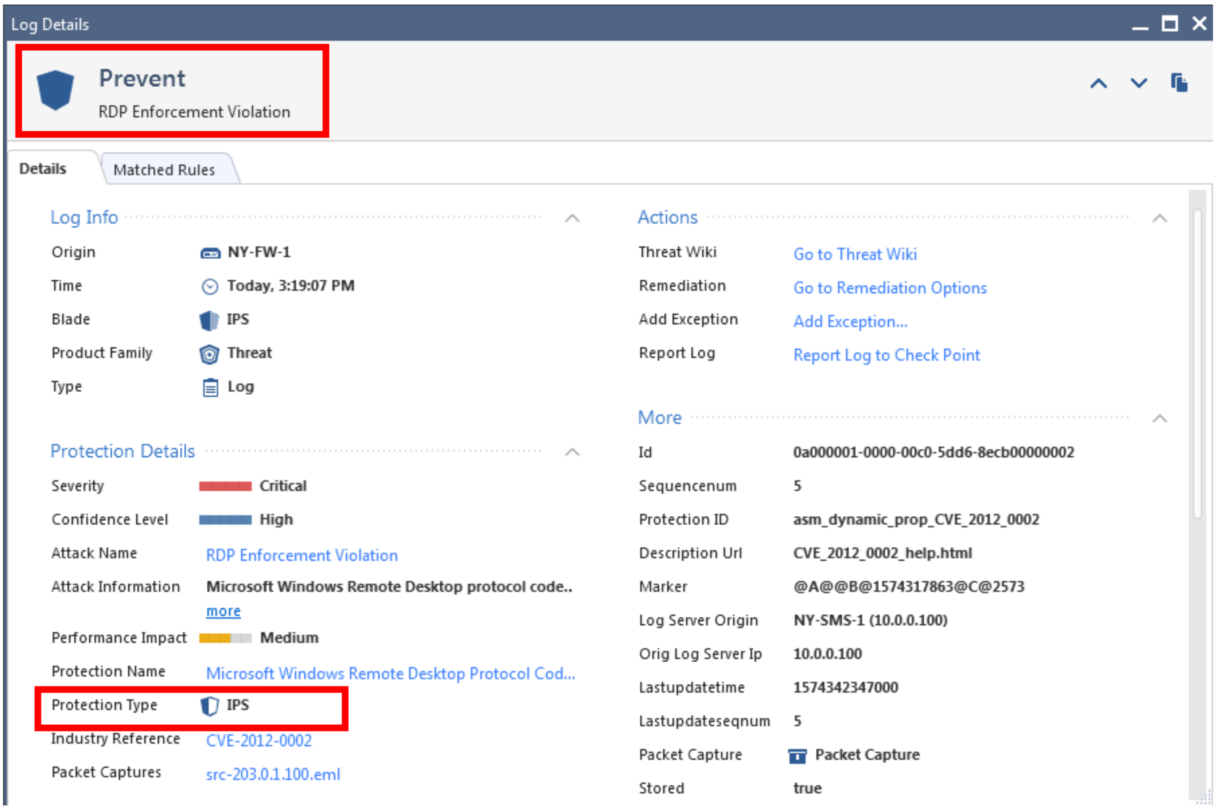
Next, we will examine the logs again. While in **Threat Prevention** policy, if you select the rule in the rule base, you will be able to see logs for this specific rule, at the bottom, just like in case of Access Control Policies.



Found 5 results (687 ms)

Time	..	..	..	..	Origin	Sever...	Source User...	Source	Destination	Protection Type
Today, 3:19:07 PM					NY-FW-1			Attacker Kali...	200.0.1.200	IPS
Today, 3:00:04 PM					NY-FW-1			Attacker Kali...	200.0.1.200	IPS
Today, 3:00:04 PM					NY-FW-1			Attacker Kali...	200.0.1.200	IPS
Today, 12:49:21 PM					NY-FW-1			Attacker Kali...	200.0.1.200	IPS

Even before I open any logs I can tell that something has changed. Before changing the IPS profile activation mode the action was to **Detect** and this is the yellow shield, now with activation mode in **Prevent**, I see a blue shield. I will open this log, the top one:



Prevent
RDP Enforcement Violation

Log Info

Origin	NY-FW-1
Time	Today, 3:19:07 PM
Blade	IPS
Product Family	Threat
Type	Log

Protection Details

Severity	Critical
Confidence Level	High
Attack Name	RDP Enforcement Violation
Attack Information	Microsoft Windows Remote Desktop protocol code.. more
Performance Impact	Medium
Protection Name	Microsoft Windows Remote Desktop Protocol Cod...
Protection Type	IPS
Industry Reference	CVE-2012-0002
Packet Captures	src-203.0.1.100.eml

Actions

Threat Wiki	Go to Threat Wiki
Remediation	Go to Remediation Options
Add Exception	Add Exception...
Report Log	Report Log to Check Point

More

Id	0a000001-0000-00c0-5dd6-8ecb00000002
Sequencenum	5
Protection ID	asm_dynamic_prop_CVE_2012_0002
Description Url	CVE_2012_0002_help.html
Marker	@A@@B@1574317863@C@2573
Log Server Origin	NY-SMS-1 (10.0.0.100)
Orig Log Server Ip	10.0.0.100
Lastupdatetime	1574342347000
Lastupdateseqnum	5
Packet Capture	Packet Capture
Stored	true

Most important fact, protection type is **IPS** and this time we are blocking the attack, not just detecting it.

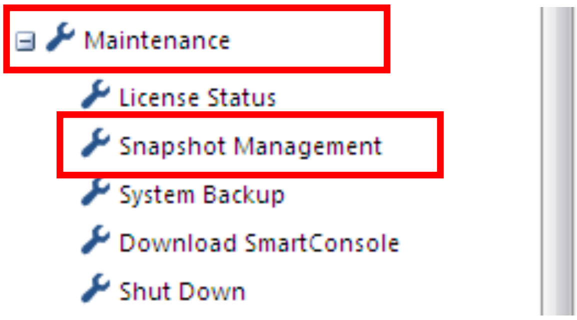
46.0 Lab: Check Point Backup and Restore Options

Lab Objectives

- Explore snapshot management backup option
- Configure SMS and NY-FW-1 backup – Gaia Web UI & Clish
- Configure system level configuration backup – Gaia Web UI & Clish
- Configure scheduled backup

The first backup option available – snapshot, represents the most complete backup you can run on Gaia OS. It encompasses both system configuration and Gaia OS level configuration. Important fact is that the resulting backup can only be used and reverted to the same type of Check Point appliance. You can't take a snapshot of a 3000 series appliance and use that in a 5000 series Check Point appliance.

You can perform a snapshot backup either in the Gaia Portal or using the clash (CLI Shell). Let's take a look in the Gaia Portal and locate this configuration option. First, log in to the Gaia portal and scroll down on the left-hand side menu until **Maintenance** menu is visible. Click on **Snapshot Management** option:

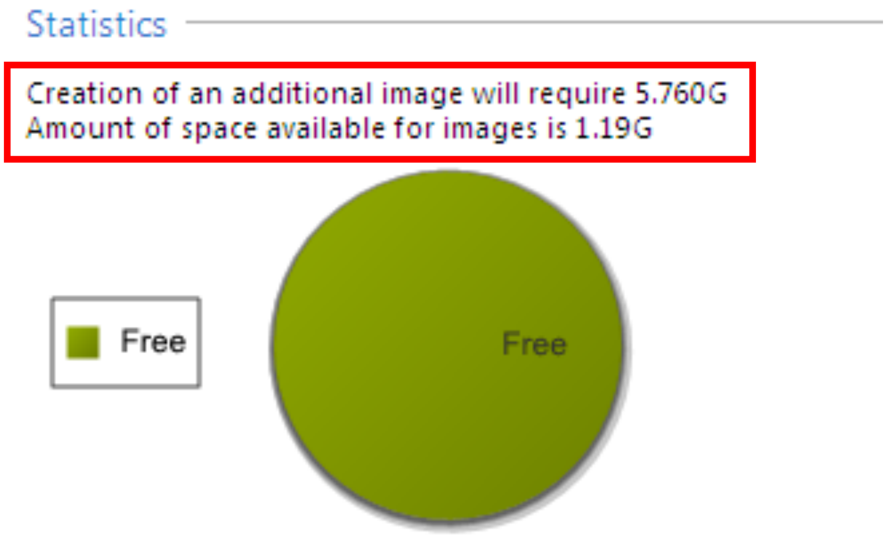


Before running a complete backup – snapshot, there is one thing that needs to be checked. Few questions that make sense at this point:

- Is there enough disk space available in order to store the new backup?
- What file size will the new snapshot backup be?

This information is available both at Gaia Web UI and clish level.

In the Gaia Portal, just before you start a new snapshot, take a look at the information below:



Statistics

Creation of an additional image will require 5.760G
Amount of space available for images is 1.19G

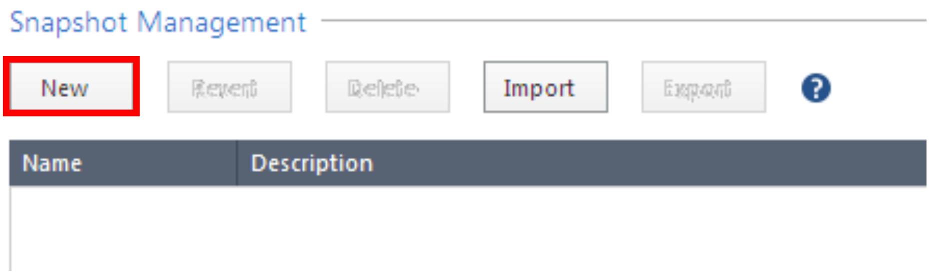
In my case, I can’t create snapshot since I don’t have enough disk space. A new snapshot backup will need 5,76G of space and I have only 1.19G available.

The same information is available if you are using CLISH:

```
NY-FW-1> show snapshots
Creation of an additional restore point will need 5.760G
Amount of space available for restore points is 1.19G
```

In my case, disk space is limited since I optimized my server as much as possible in order to be able to run the whole lab topology.

In order to complete a snapshot backup, the steps are easy and very straightforward. In the Gaia Portal, just click on **New** option:



and provide a Name and Description for the new snapshot backup.

If you like working at the CLI level, use the following command in order to first create the snapshot:

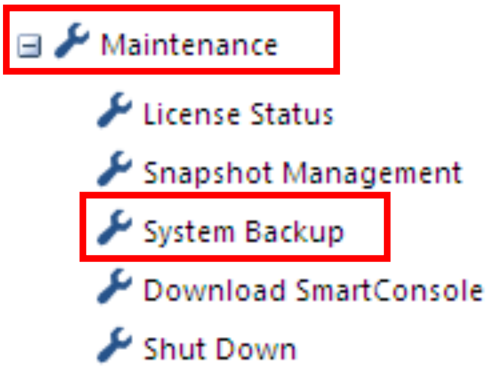
```
NY-FW-1> add snapshot
add snapshot VALUE desc VALUE
```

and when you need to use a previous snapshot (revert, export or import a previous snapshot) use the following commands:

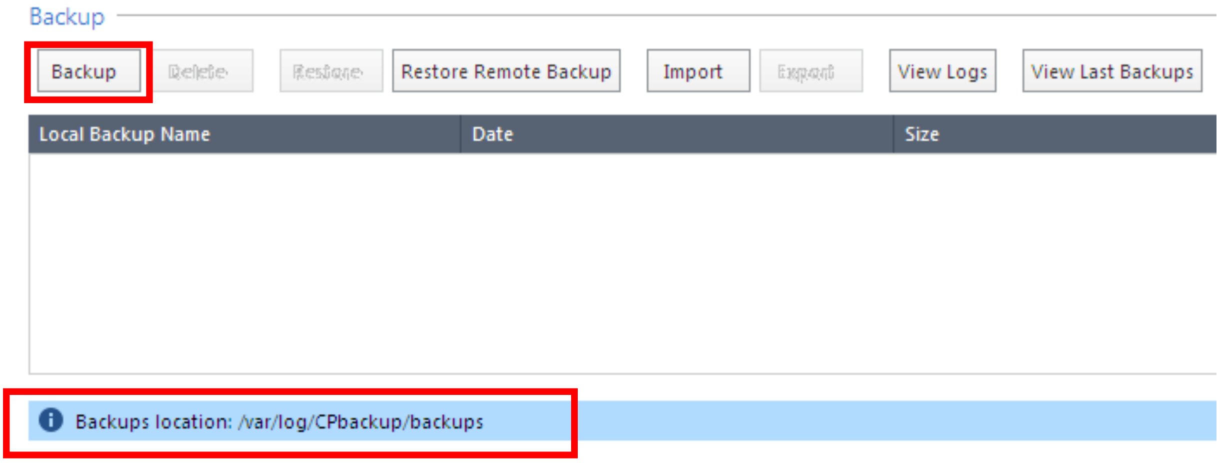
```
NY-FW-1> set snapshot (press twice the ESC key on your keyboard and all the possible
commands that start with set snapshot are displayed below)
set snapshot export VALUE path VALUE name VALUE
set snapshot import VALUE path VALUE name VALUE
```

Now, let’s explore the second option – system backup and restore.

We will first create a backup to our SMS server using the Gaia Portal. Scroll down again the left-hand side menu and under **Maintenance** menu click on **System Backup**:



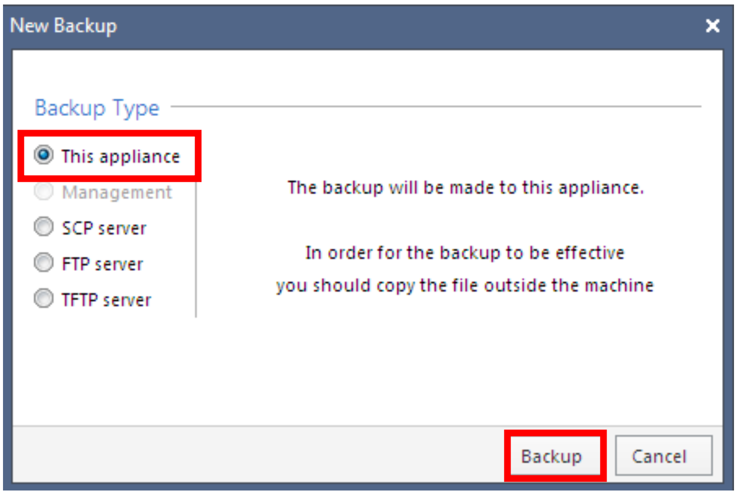
Please note the path to your backups is presented on the screen:



Backups location: /var/log/CPbackup/backups

In order to initiate a **system backup**, just click on **Backup**, as highlighted above.

Next, you need to decide where will the new backup file be stored, either locally on the machine or on a remote server. In this lab, we will select the first option **This appliance** and the backup file will be stored locally on this machine:



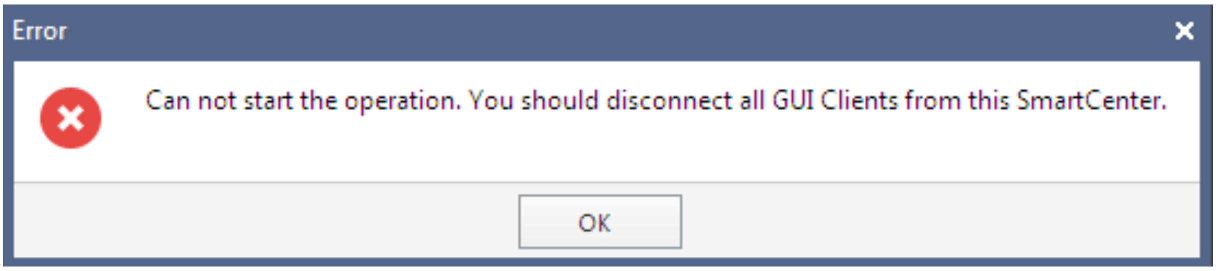
Backup Type

● This appliance
○ Management
○ SCP server
○ FTP server
○ TFTP server

The backup will be made to this appliance.

In order for the backup to be effective
you should copy the file outside the machine

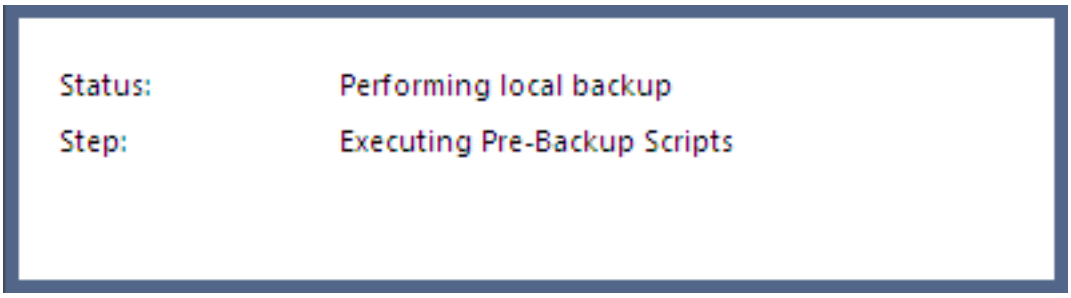
In order to continue, just click on **Backup**. At this moment, if you still have the SmartConsole open, you will receive the below error:



Can not start the operation. You should disconnect all GUI Clients from this SmartCenter.

Simply close the SmartConsole and initiate backup operation again.

If the backup process is started successfully, you should be displayed a similar window, like the one below:



Status: Performing local backup

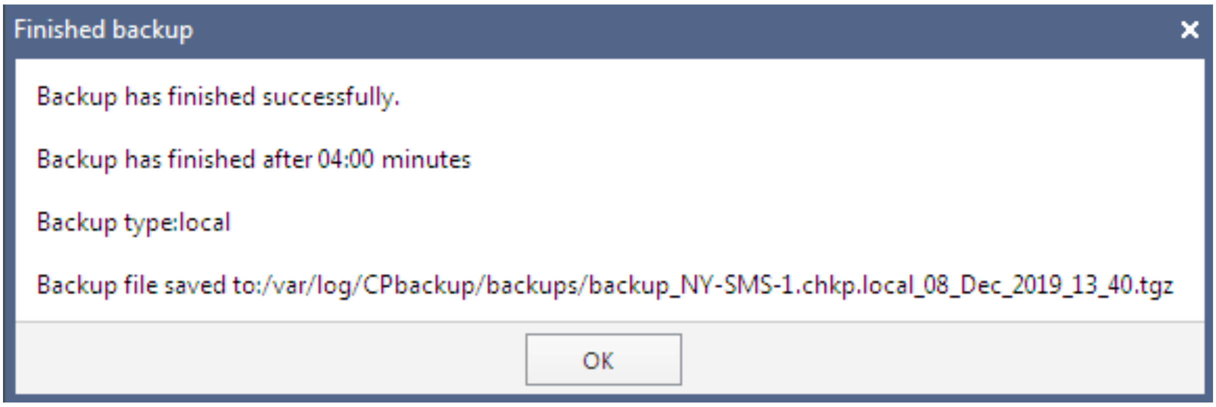
Step: Executing Pre-Backup Scripts

At this moment, not that much information is displayed in the Gaia Portal. You can gain some visibility on the backup process at the CLI level.

```
NY-SMS-1> show backups
Backups location: /var/log/CPbackup/backups

backup_NY-SMS-1.chkp.local_08_Dec_2019_13_40.tgz Sun, Dec 08, 2019 141.59 MB
NY-SMS-1> show backups
Backups location: /var/log/CPbackup/backups

backup_NY-SMS-1.chkp.local_08_Dec_2019_13_40.tgz Sun, Dec 08, 2019 176.52 MB
```

Running the **show backups** command twice highlights that indeed the process is running and I can see that the backup file size is growing, which is a good indication of course.

Once the backup is completed, I am provided in the Gaia portal the following message – **Finished backup**



Finished backup

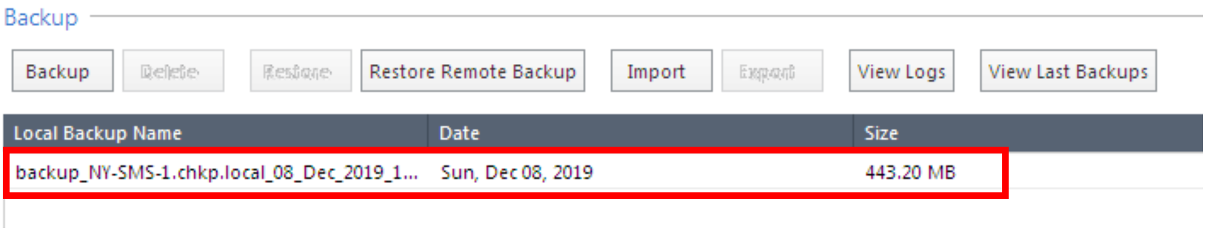
Backup has finished successfully.

Backup has finished after 04:00 minutes

Backup type:local

Backup file saved to:/var/log/CPbackup/backups/backup_NY-SMS-1.chkp.local_08_Dec_2019_13_40.tgz

The information is updated in the Web UI and I can now see the latest backup:

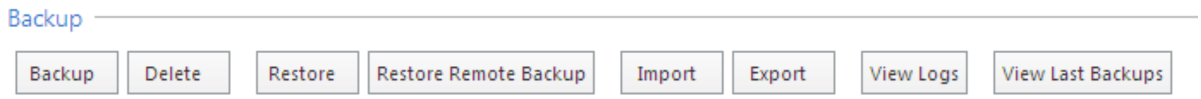


Local Backup Name	Date	Size
backup_NY-SMS-1.chkp.local_08_Dec_2019_1...	Sun, Dec 08, 2019	443.20 MB

I can check the information as well, at the CLI level:

```
NY-SMS-1> show backups
Backups location: /var/log/CPbackup/backups

backup_NY-SMS-1.chkp.local_08_Dec_2019_13_40.tgz Sun, Dec 08, 2019 443.20 MB
```

Selecting this backup file in the Web UI, I can see what I can do with it:



I can select **Restore** in order to restore the configuration on the NY-SMS-1 to this backup configuration, I can restore the configuration on the SMS using a remote backup file, I can delete the backup file or export it.

Let's now create a **system backup** of the NY-FW-1 appliance, but this time at the CLI level. Type **add backup** and double press ESC key on your keyboard. Here are the options:

```
NY-FW-1> add backup
add backup ftp ip VALUE path VALUE username VALUE [ password VALUE interactive ]
add backup local [ interactive ]
add backup scp ip VALUE path VALUE username VALUE [ password VALUE interactive ]
add backup tftp ip VALUE [ interactive ]
```

Since we will store the backup locally on the machine, I will type the complete command – **add backup local**

```
NY-FW-1> add backup local
Creating backup package. Use the command 'show backup status' to monitor creation
progress.
In order for the backup to be effective you should copy the file outside the machine.
NY-FW-1> show backup status
Performing local backup
Step: Executing Pre-Backup Scripts
Progress: 4%
NY-FW-1> show backup status
Performing local backup
Step: Executing Pre-Backup Scripts
Progress: 7%
```

The backup process starts immediately and you can monitor the progress by using the **show backup status** command, as highlighted above.

```
NY-FW-1> show backup status
local backup succeeded.
Backup file location: /var/log/CPbackup/backups/backup_NY-FW-
1.chkp.local_08_Dec_2019_14_06.tgz
Backup process finished in 00:18 seconds
Backup Date: 08-Dec-2019 14:06:43
```

Once complete, the output should change as highlighted above – **local backup succeeded**.

At a later time, if needed, you can use the backup file in order to restore the configuration saved:

```
NY-FW-1> set backup restore
ftp        - Restore from the configuration stored on ftp server
local      - Restore from locally saved configuration
management - Restore from the configuration stored on management server
scp        - Restore from the configuration stored on scp server
tftp       - Restore from the configuration stored on tftp server
```

In our case, since the backup is being stored locally on the machine, we can initiate a configuration restore by using the **local** option.

The last option available is the system level configuration backup, which is performed at the CLI level. This option is useful when you need to preserve information such as interface IP addressing, routing information, etc.

Let’s configure a system level configuration backup for NY-FW-1.

```
NY-FW-1> save configuration NY-FW-1-Config-File
NY-FW-1> expert
Enter expert password:

Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@NY-FW-1:0]# pwd
/home/admin
[Expert@NY-FW-1:0]# ls
NY-FW-1-Config-File  last_dump.log
```

```
 [Expert@NY-FW-1:0]# cat NY-FW-1-Config-File
#
# Configuration of NY-FW-1
# Language version: 13.1v1
#
# Exported by admin on Sun Dec  8 14:15:22 2019
#
set installer policy check-for-updates-period 3
set installer policy periodically-self-update on
set installer policy send-cpuse-data off
set installer policy auto-compress-snapshot on
set installer policy self-test install-policy off
set installer policy self-test network-link-up off
set installer policy self-test start-processes on
set arp table cache-size 4096
set arp table validity-timeout 60
set arp announce 2
set message banner on

set message motd off

set message caption off
set core-dump enable
set core-dump total 1000
set core-dump per_process 2
set clienv debug 0
set clienv echo-cmd off
set clienv output pretty
set clienv prompt "%M"
set clienv rows 0
set clienv syntax-check off
set dns suffix chkp.local
set dns primary 8.8.8.8
set domainname chkp.local
set edition 64-bit
set expert-password-hash $1$DBDBBZBB$qDpnJuBoGsOJnEUe7qUBA0
set format date dd-mmm-yyyy
set format time 24-hour
set format netmask Dotted
set hostname NY-FW-1
add allowed-client host any-host
set web table-refresh-rate 15
set web session-timeout 10
set web ssl-port 443
set web ssl3-enabled off

<output omitted>
```

I use the command **save configuration <File Name>** and provide a name for the resulting configuration file. The new configuration file is stored under the /home/admin folder, so I navigate to this folder in order to check the configuration file is there.

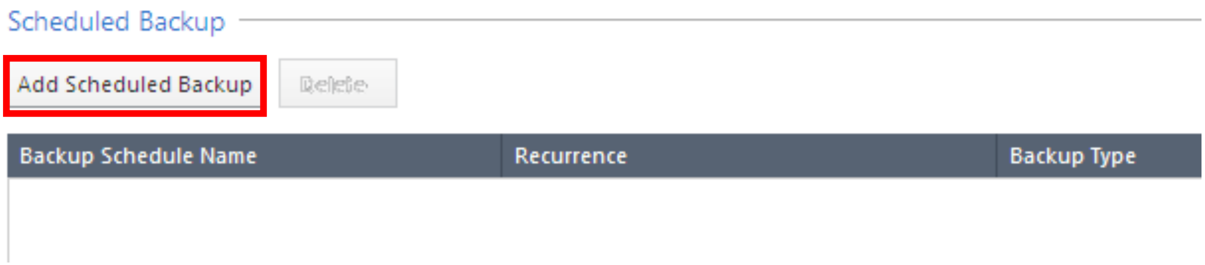
Typing **ls** will list all the files under a folder and this highlights the new configuration file - **NY-FW-1-Config-File**. I can see the content by using another linux command – **cat**.

At a later time, if I need to restore the configuration to this one, I can use the **load configuration <File Name>** command, at the CLI level.

```
NY-FW-1> load configuration NY-FW-1-Config-File
Done.
```

The last thing to cover in this lab is scheduled backups. I need to be able to schedule backups, so these are done automatically, at regular intervals. Scheduled backups configuration is available both in Gaia portal and at the CLI level.

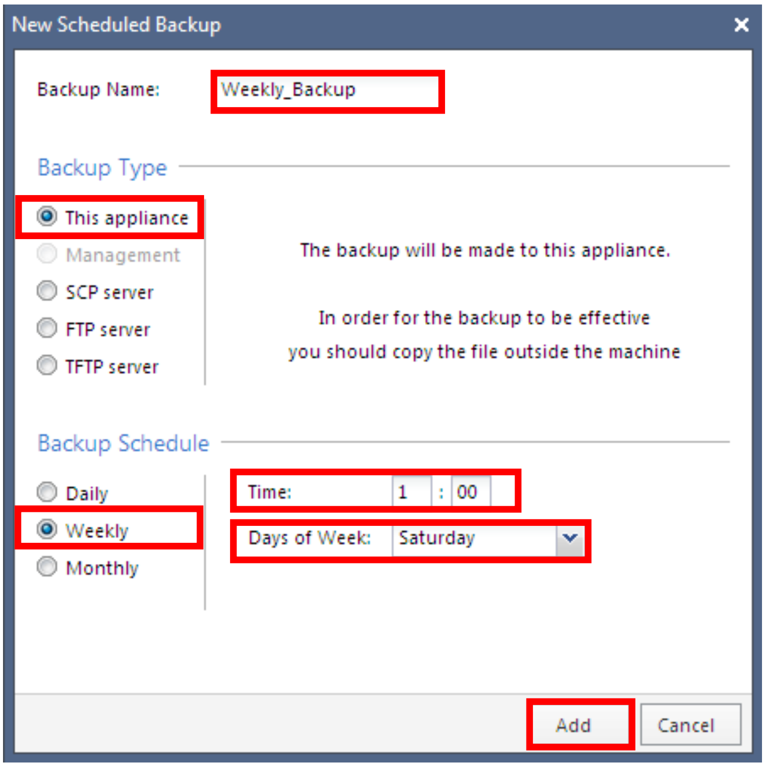
In Gaia Web UI, under **Maintenance – System Backup**, there is the **Scheduled Backup** option:



Backup Schedule Name	Recurrence	Backup Type

As an example, let’s configure automatic scheduled backups for our SMS server. In order to start the configuration, click on **Add Scheduled Backup**.

Fill in a name for the scheduled backup file, select where the backup file will be stored and configure the backup frequency. As an example, I have selected to create a weekly backup, each Saturday, at 1:00 AM. When configuration is complete, just click **Add** in order to finish the process.



New Scheduled Backup

Backup Name: Weekly_Backup

Backup Type

● This appliance
○ Management
○ SCP server
○ FTP server
○ TFTP server

The backup will be made to this appliance.

In order for the backup to be effective you should copy the file outside the machine

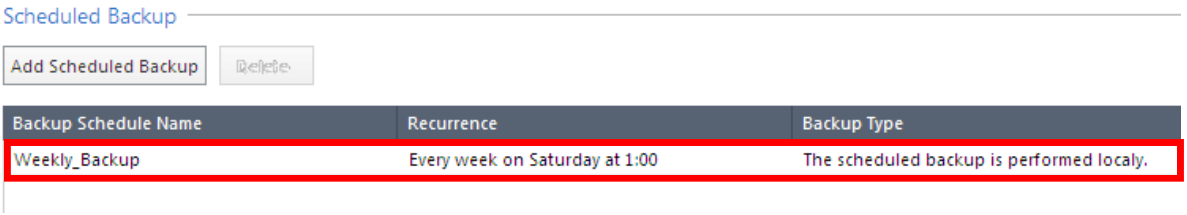
Backup Schedule

○ Daily
● Weekly
○ Monthly

Time: 1 : 00

Days of Week: Saturday

Once the backup is complete, you should see the new backup file in the Web UI:



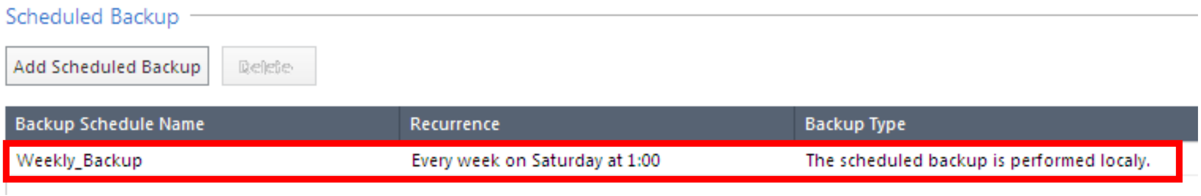
Scheduled Backup

Backup Schedule Name	Recurrence	Backup Type
Weekly_Backup	Every week on Saturday at 1:00	The scheduled backup is performed localy.

If you like more to work at the CLI level, you can do the same in clish. Below the command I used to configure a scheduled backup on NY-FW-1, on a weekly basis, on Saturday, at 1:00AM.

```
NY-FW-1> set backup-scheduled name Weekly_Backup recurrence weekly days 6 time 1:00
Backup was successfully scheduled.
```

Checking the Web UI on NY-FW-1, backup is confirmed:



Scheduled Backup

Backup Schedule Name	Recurrence	Backup Type
Weekly_Backup	Every week on Saturday at 1:00	The scheduled backup is performed localy.

47.0 Lab: Configure site-to-site VPN between New York and London

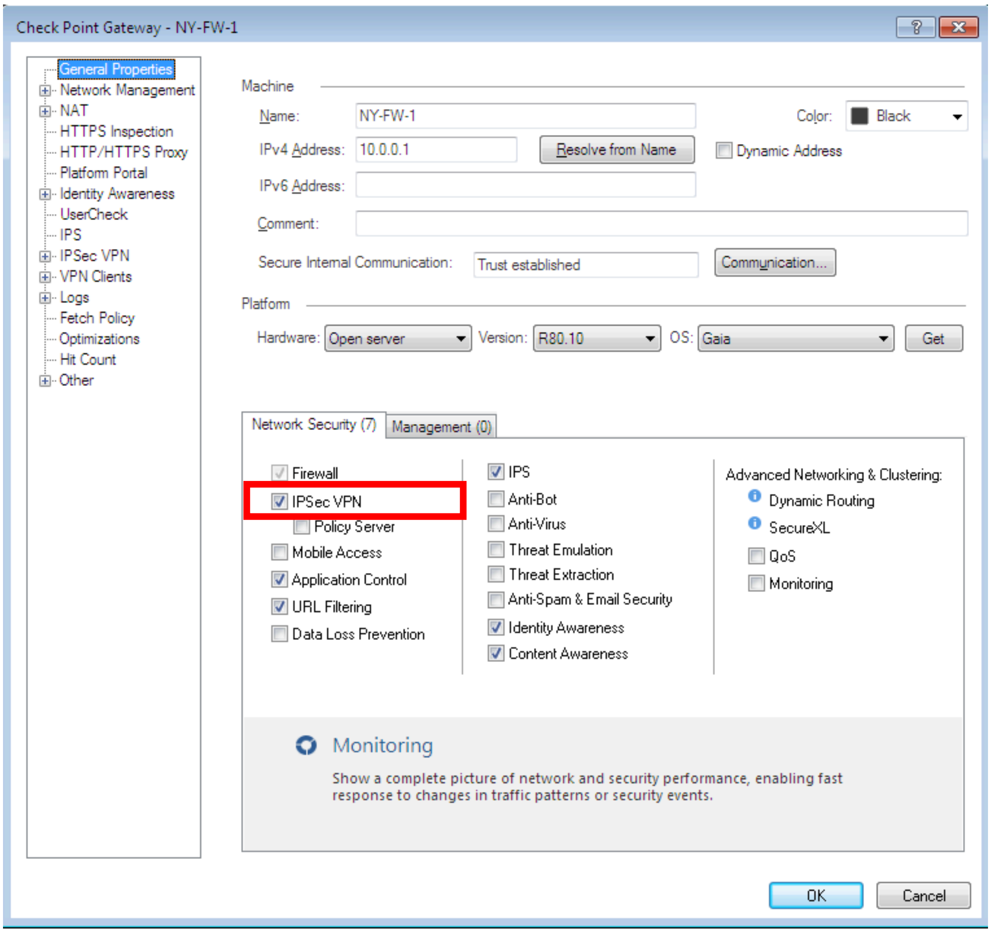
Lab Objectives

- Configure VPN Domains
- Create the VPN Community
- Modify the Access Control Rule Base to accommodate the VPN traffic
- Full VPN Setup Testing

In this lab we will configure a site-to-site VPN between New York and London sites. We will be using the New York SMS server as the CA authority, as this server will generate the certificates to be used in the VPN setup.

First, we need to define the VPN domains for both sites. This is when we specify what traffic goes into the VPN tunnel, so what traffic we want to encrypt actually.

We will start with the New York site. Let's open the NY-FW-1 object and first we need to activate the **IPsec VPN** software blade.



Check Point Gateway - NY-FW-1

Machine

Name: NY-FW-1

Color: Black

IPv4 Address: 10.0.0.1

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server

Version: R80.10

OS: Gaia

☑ Firewall
☑ IPSec VPN
□ Policy Server
□ Mobile Access
☑ Application Control
☑ URL Filtering
□ Data Loss Prevention

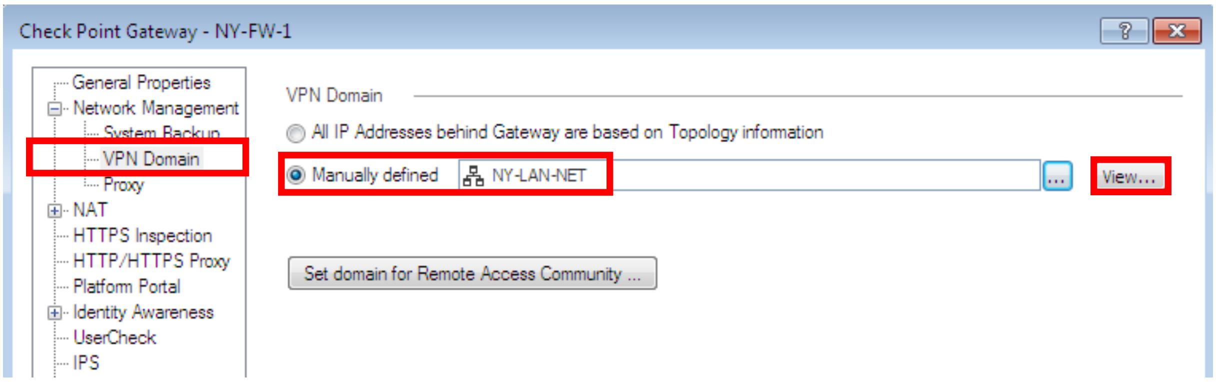
☑ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
☑ Identity Awareness
☑ Content Awareness

Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
□ Monitoring

Monitoring

Show a complete picture of network and security performance, enabling fast response to changes in traffic patterns or security events.

Next, let's expand the **Network Management** menu and select the **VPN Domain**. We will manually define here the VPN domain and specifically select the NY-LAN-NET – 172.16.10.0/24 subnet..



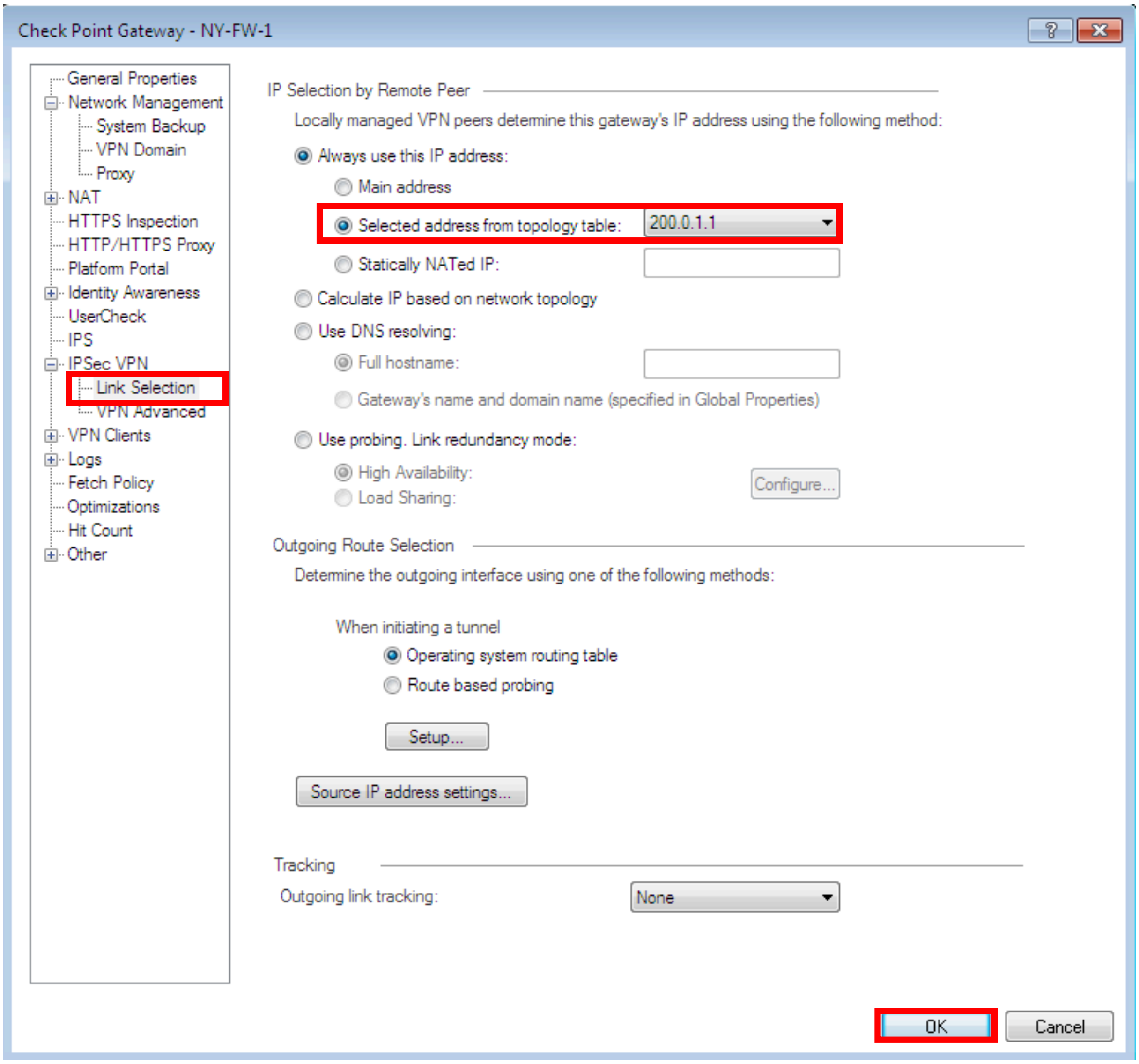
Check Point Gateway - NY-FW-1

VPN Domain

○ All IP Addresses behind Gateway are based on Topology information

● Manually defined NY-LAN-NET

Now, let's expand **IPsec VPN** menu and select **Link Selection**:



Check Point Gateway - NY-FW-1

IP Selection by Remote Peer

Locally managed VPN peers determine this gateway's IP address using the following method:

● Always use this IP address:

○ Main address

● Selected address from topology table: 200.0.1.1

○ Statically NATed IP:

○ Calculate IP based on network topology

○ Use DNS resolving:

● Full hostname:

○ Gateway's name and domain name (specified in Global Properties)

○ Use probing. Link redundancy mode:

● High Availability:

○ Load Sharing:

Outgoing Route Selection

Determine the outgoing interface using one of the following methods:

When initiating a tunnel

● Operating system routing table

○ Route based probing

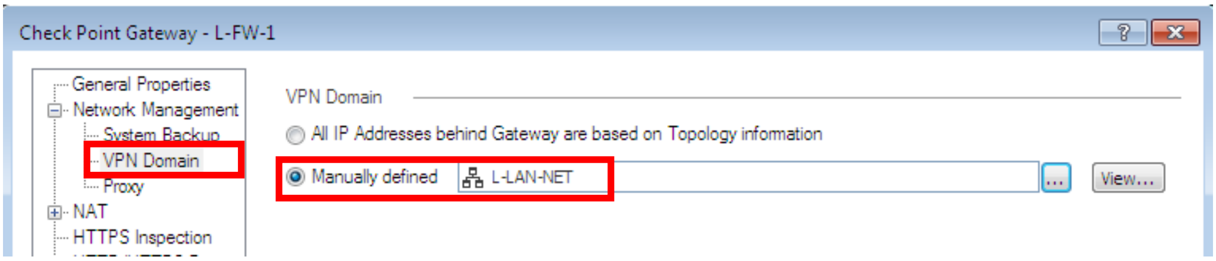
Tracking

Outgoing link tracking: None

We want to make sure that each time we initiate the tunnel, we will use the external IP address, so we will statically define it here, by manually selecting it from available options. Configuration setting has been highlighted below.

When configuration is complete, just click **OK** in order to continue.

Now, let's define the VPN domain for London site as well. I will open the L-FW-1 object and first enable **IPsec VPN** software blade. For the VPN domain, let's select **L-LAN-NET** – 172.16.30.0/24 subnet, which we now from the Lab Diagram that it corresponds to internal LAN of London site.



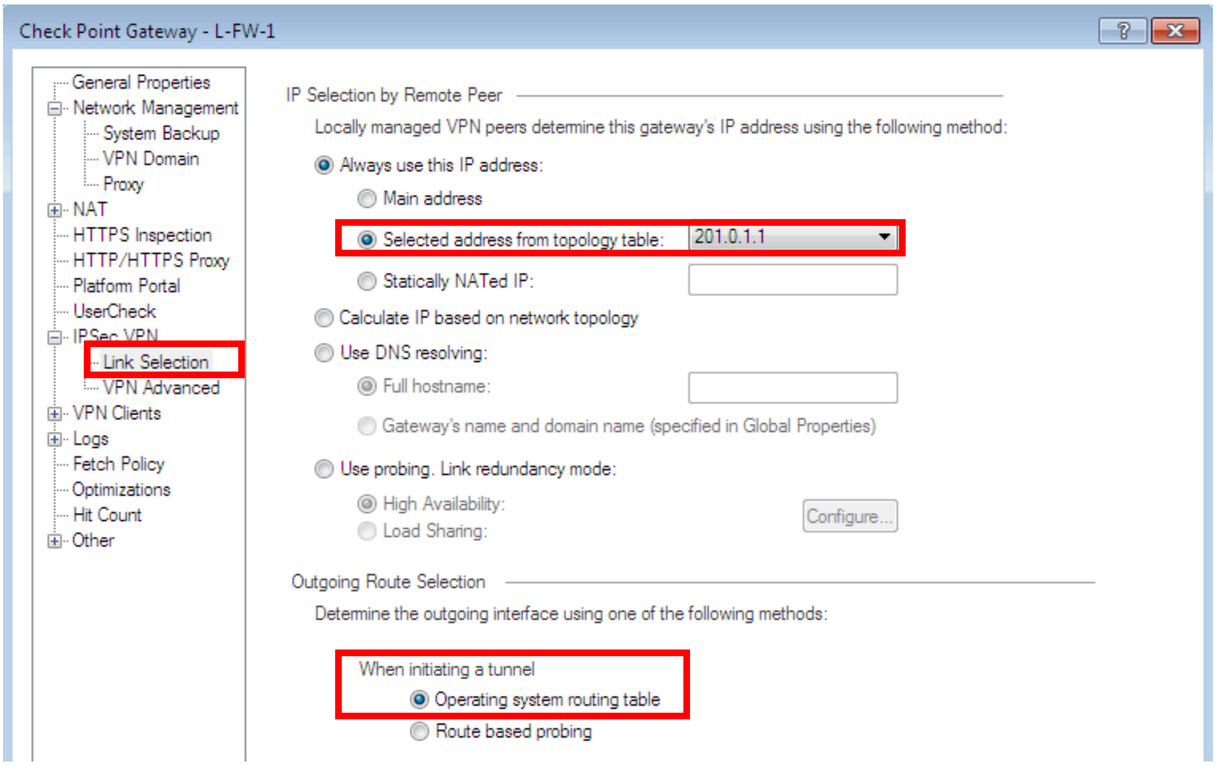
Check Point Gateway - L-FW-1

VPN Domain

○ All IP Addresses behind Gateway are based on Topology information

● Manually defined L-LAN-NET

For the link selection, we will make sure now that the London security gateway will always use the external IP address when initiating the VPN tunnel and it makes sense to happen this way.



Check Point Gateway - L-FW-1

IP Selection by Remote Peer

Locally managed VPN peers determine this gateway's IP address using the following method:

● Always use this IP address:

○ Main address

● Selected address from topology table: 201.0.1.1

○ Statically NATed IP:

○ Calculate IP based on network topology

○ Use DNS resolving:

● Full hostname:

○ Gateway's name and domain name (specified in Global Properties)

○ Use probing. Link redundancy mode:

● High Availability:

○ Load Sharing:

Outgoing Route Selection

Determine the outgoing interface using one of the following methods:

When initiating a tunnel

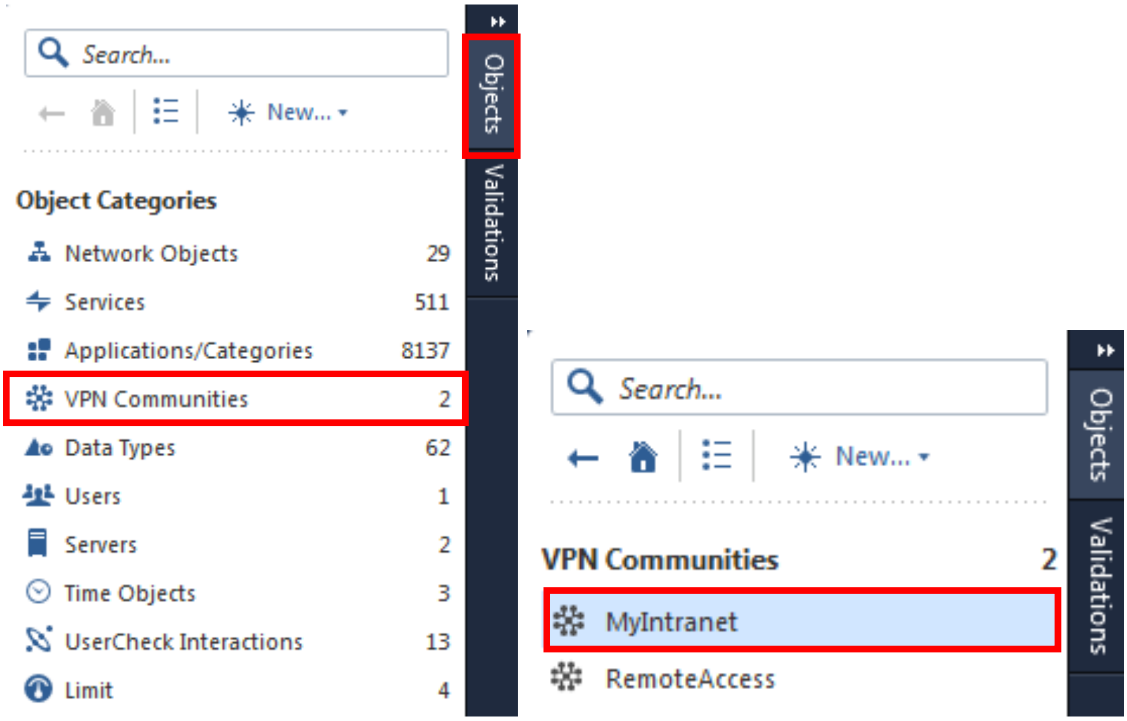
● Operating system routing table

○ Route based probing

How do I determine the outgoing interface of the traffic ? Based on the routing table of the security gateway. When configuration is complete, just click **OK**.

Finally, let's publish the changes.

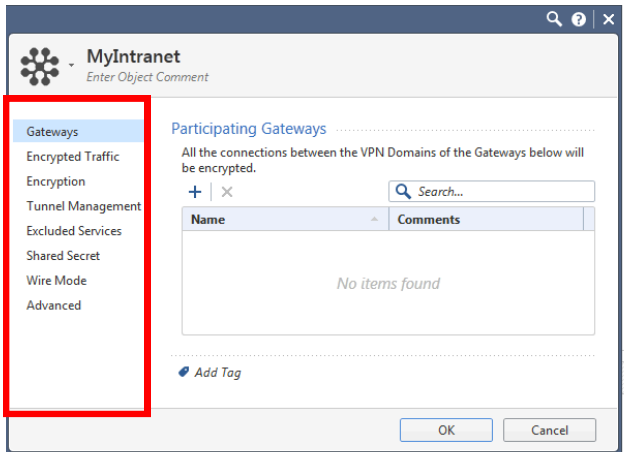
We will continue now with the second step, VPN community configuration. We could create a new VPN community or edit the existing one. In the top-right corner, expand the **Objects** panel if it's not expanded already, select **VPN Communities** and then **My Intranet** VPN community:



Let's stop for a second. As the names of the two VPN communities express, one is for remote access VPNs and the other – **MyIntranet** is for site-to-site VPNs, probably, right ?

In the video lectures, we have gone through the two types of site-to-site VPNs – mesh and star. How do we know which kind of VPN community is this ?

One easy way is to take a look in the **MyIntranet** menus once you open the object and see if **VPN Routing** menu is available. We know that VPN routing applies to Star VPN Communities, so if this menu is not available than the VPN community is the mesh type. On the left you have the **MyIntranet** VPN community and on the right there's a new VPN community – star type.



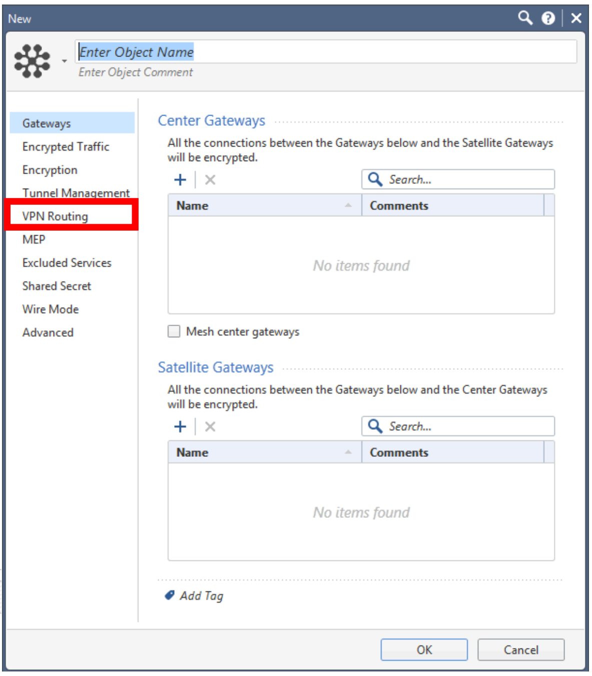
MyIntranet

Enter Object Comment

Participating Gateways

All the connections between the VPN Domains of the Gateways below will be encrypted.

Name	Comments
No items found	



New

Enter Object Name

Enter Object Comment

Center Gateways

All the connections between the Gateways below and the Satellite Gateways will be encrypted.

Name	Comments
No items found	

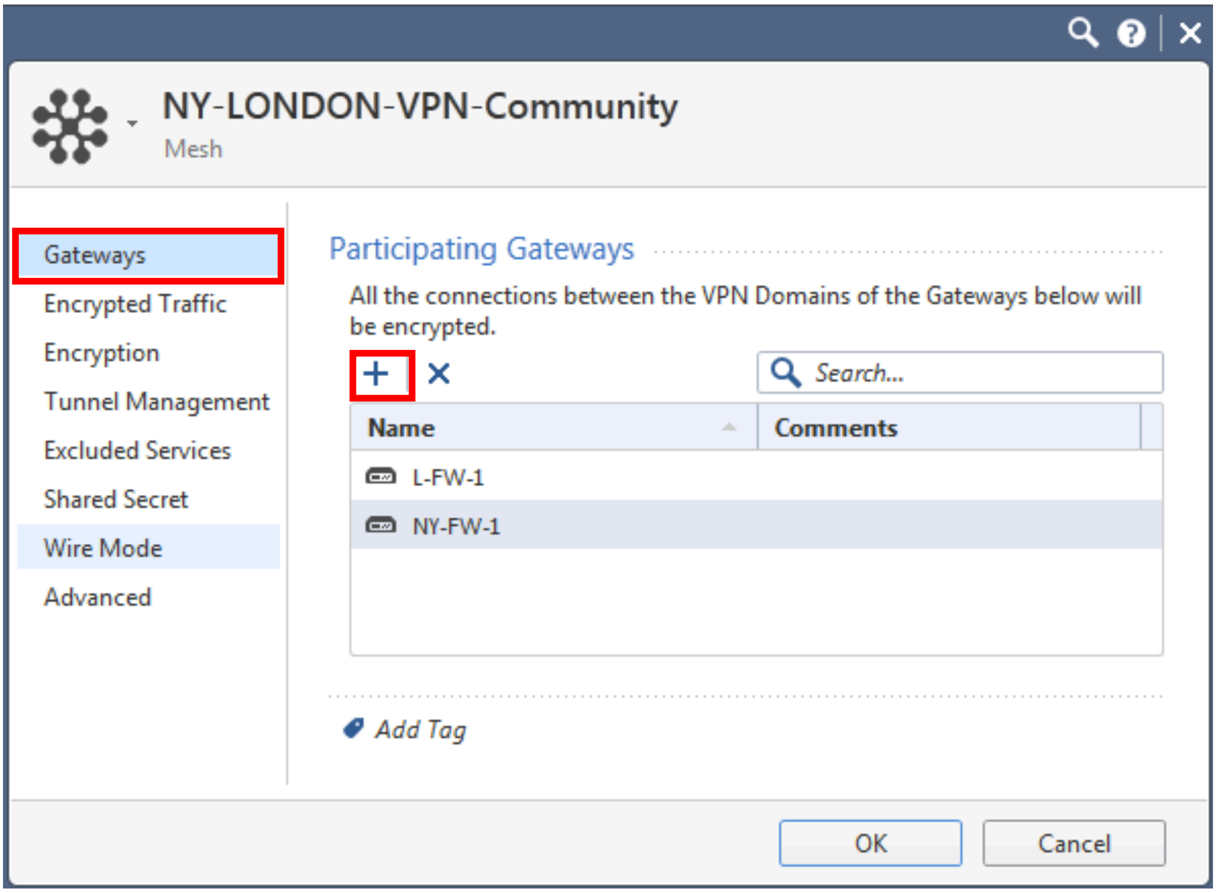
□ Mesh center gateways

Satellite Gateways

All the connections between the Gateways below and the Center Gateways will be encrypted.

Name	Comments
No items found	

So let’s edit the existing **MyIntranet** community.



NY-LONDON-VPN-Community

Mesh

Participating Gateways

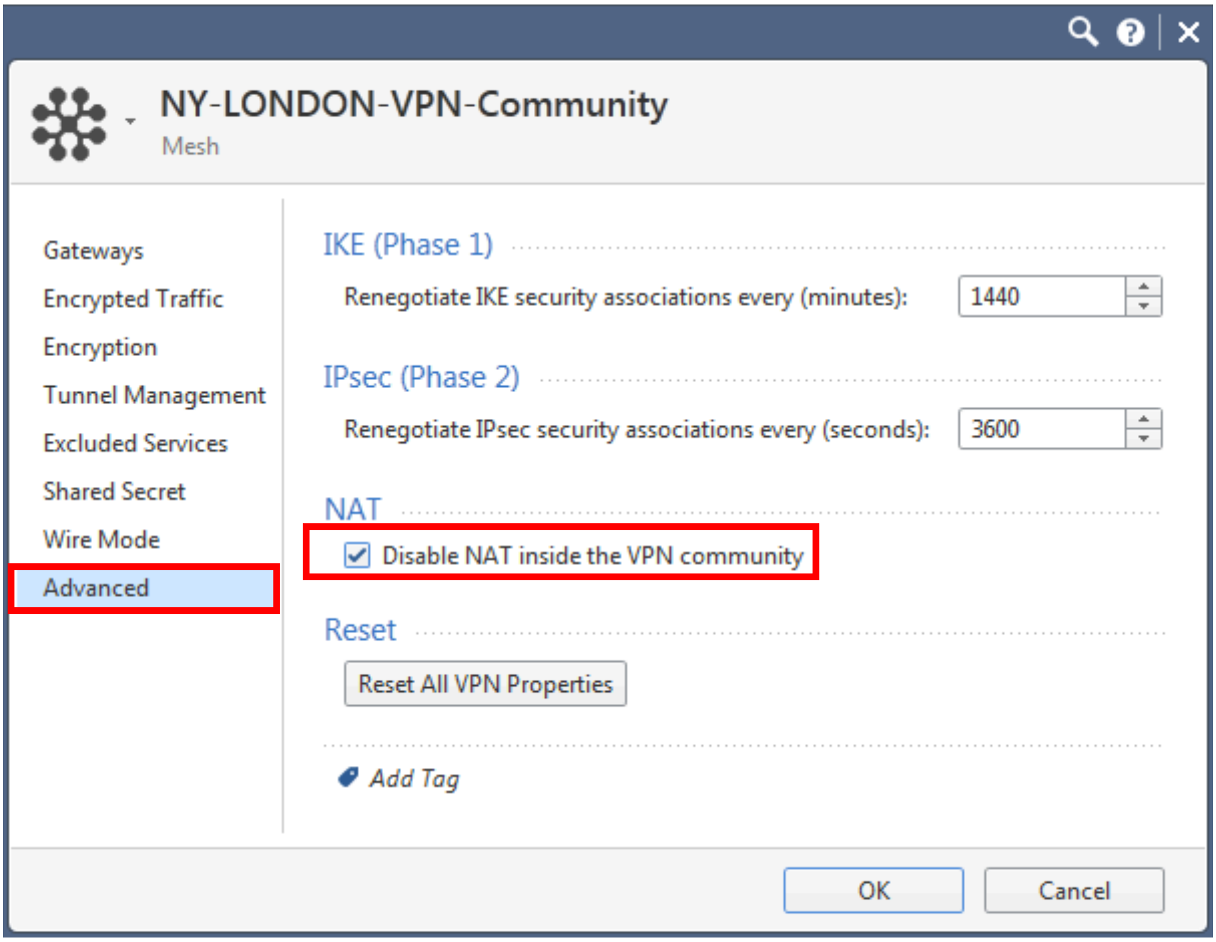
All the connections between the VPN Domains of the Gateways below will be encrypted.

Name	Comments
L-FW-1	
NY-FW-1	

I will define the name – **NY-LONDON-VPN-Community** and add the **Mesh** comment.

Let's first select the participating gateways, so what security gateways will be encrypting traffic (VPN Domain) ? Please click on the **+** sign and select actually the only two gateways available – NY-FW-1 and L-FW-1.

One more setting is needed and this is related to NAT. Select **Advanced** from the left menu:



NY-LONDON-VPN-Community
Mesh

IKE (Phase 1)

Renegotiate IKE security associations every (minutes): 1440

IPsec (Phase 2)

Renegotiate IPsec security associations every (seconds): 3600

NAT

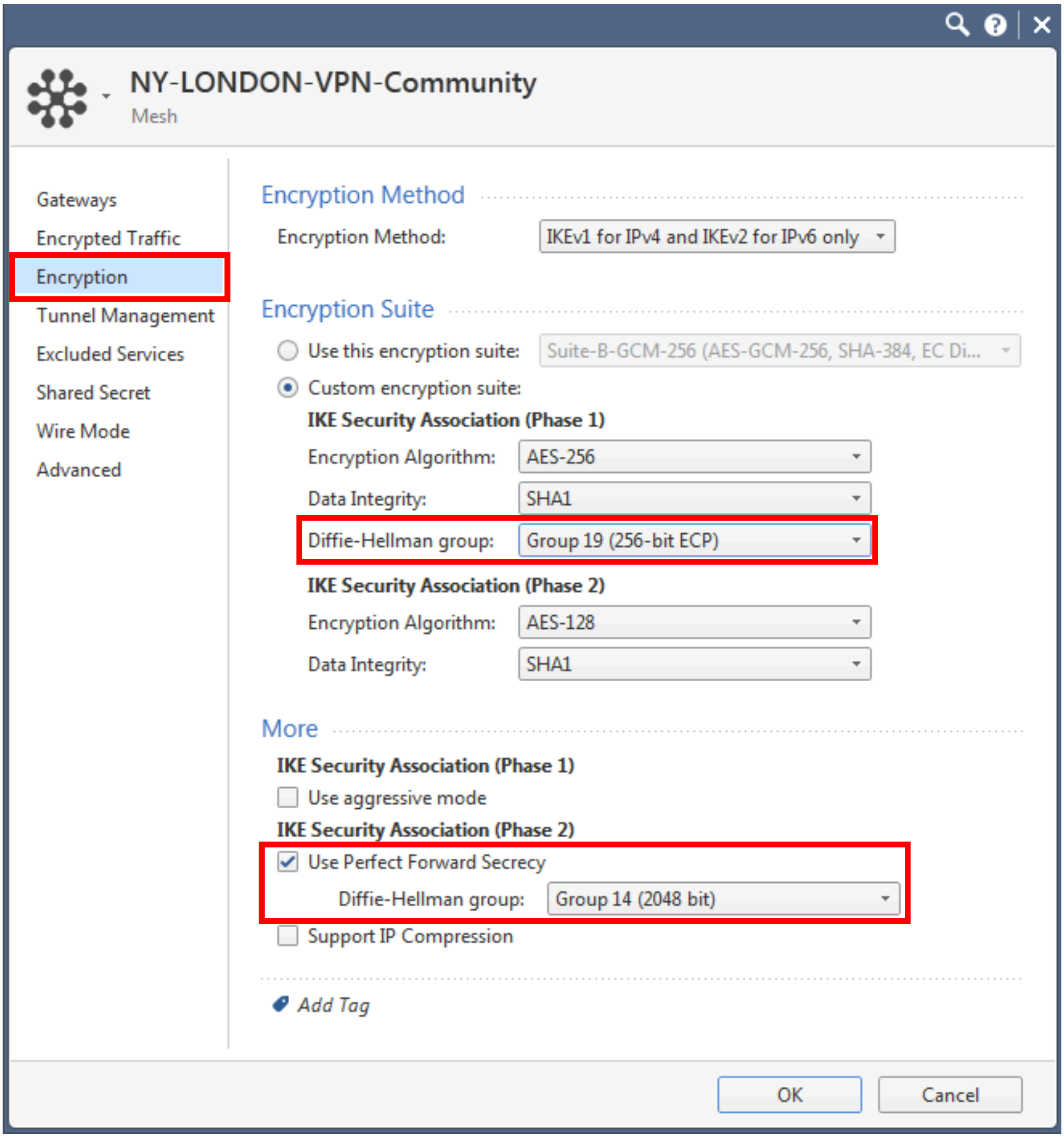
☑ Disable NAT inside the VPN community

Reset

This setting is important if you have objects that are configured with static NAT.

Let's now take a look at the encryption settings. Please select the third menu – **Encryption**. We will do some modifications on the default configuration.

For Phase 1, we will change the Diffie-Hellman Group, so the hashing algorithm, from DH-2 to a more secure one – DH-19. Also, let's enable **Perfect Forward Secrecy** and we will use also a more advanced Diffie-Hellman group – Group 14.



NY-LONDON-VPN-Community

Mesh

Encryption Method

Encryption Method: IKEv1 for IPv4 and IKEv2 for IPv6 only

Encryption Suite

○ Use this encryption suite: Suite-B-GCM-256 (AES-GCM-256, SHA-384, EC Di...

● Custom encryption suite:

IKE Security Association (Phase 1)

Encryption Algorithm: AES-256

Data Integrity: SHA1

Diffie-Hellman group: Group 19 (256-bit ECP)

IKE Security Association (Phase 2)

Encryption Algorithm: AES-128

Data Integrity: SHA1

More

IKE Security Association (Phase 1)

□ Use aggressive mode

IKE Security Association (Phase 2)

☑ Use Perfect Forward Secrecy

Diffie-Hellman group: Group 14 (2048 bit)

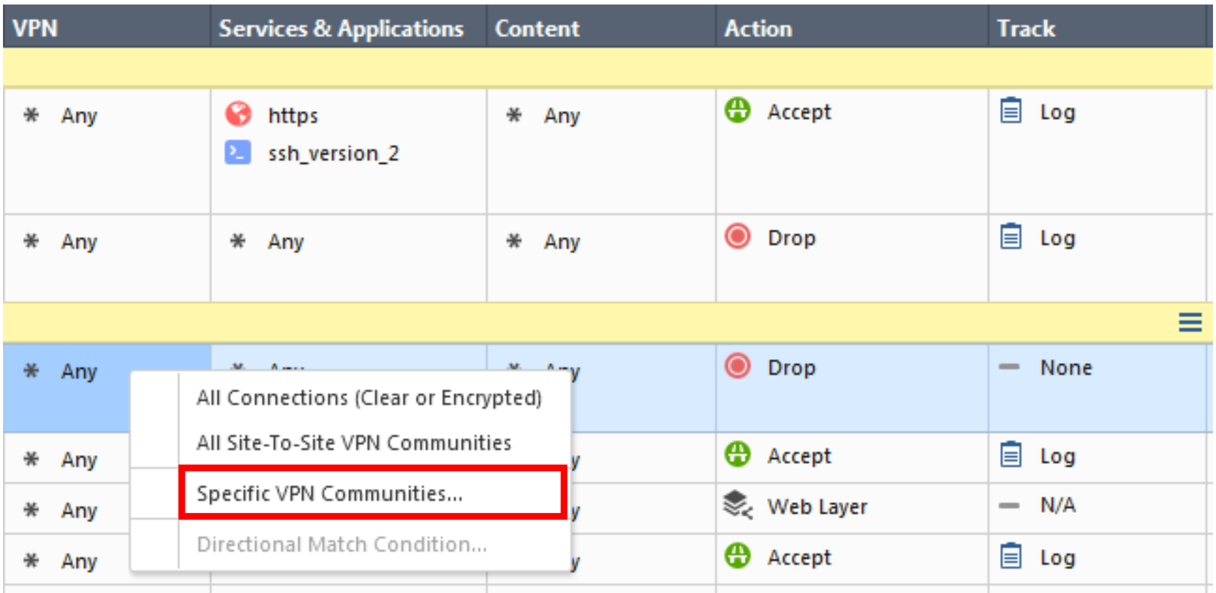
□ Support IP Compression

Click **OK** in order to continue.

Last step in the process is to configure a new Rule in the Rule Base destined to the VPN traffic and also make sure that no NAT is performed for traffic between subnets in the two sites, New York and London.

First let’s edit the **HQ_Corporate_Policy**, so this refers to New York site. Let’s add a new rule above the **Pentesting** rule, so this will be rule 3. We will name it **VPN Traffic to London**, for both source and destination select the two internal subnets – NY-LAN-NET and L-LAN-NET.

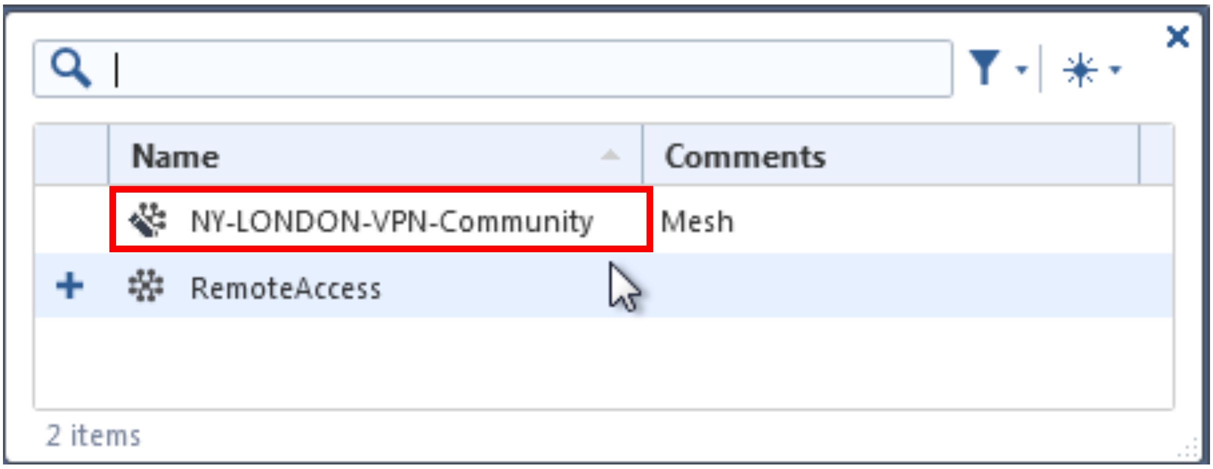
Next, for the VPN column, right-click in the VPN field and select **Specific VPN Communities**



VPN	Services & Applications	Content	Action	Track
Any	https ssh_version_2	Any	Accept	Log
Any	Any	Any	Drop	Log
Any	Any	Any	Drop	None
Any		y	Accept	Log
Any		y	Web Layer	N/A
Any		y	Accept	Log

All Connections (Clear or Encrypted)
All Site-To-Site VPN Communities
Specific VPN Communities...
Directional Match Condition...

and now select the previously configured community:

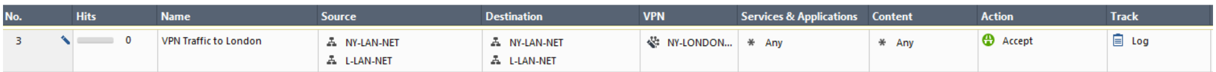


Name	Comments
NY-LONDON-VPN-Community	Mesh
RemoteAccess	

2 items

The Action will be **Accept** and let's configure to **Log** the traffic.

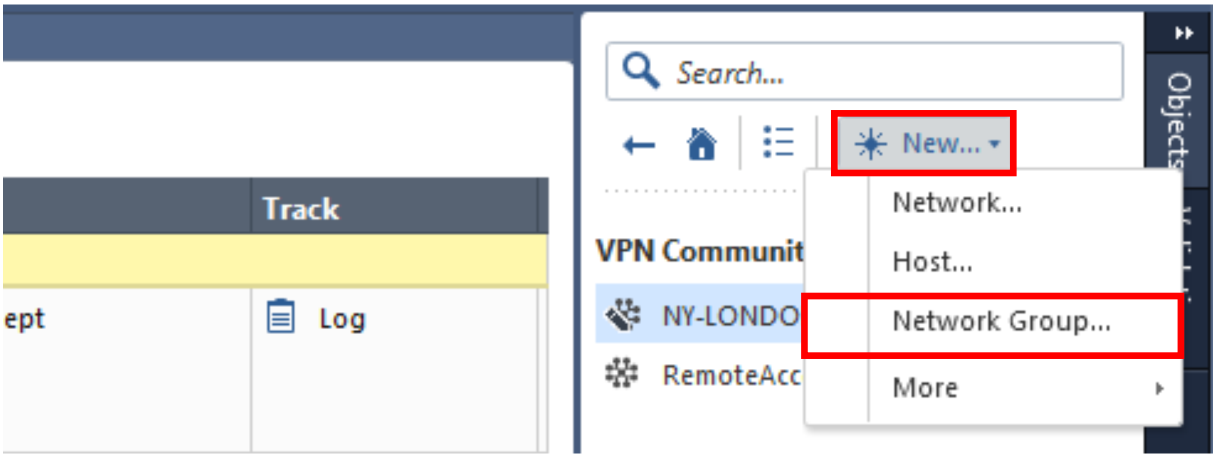
When complete, the new rule should look similar to the one below:



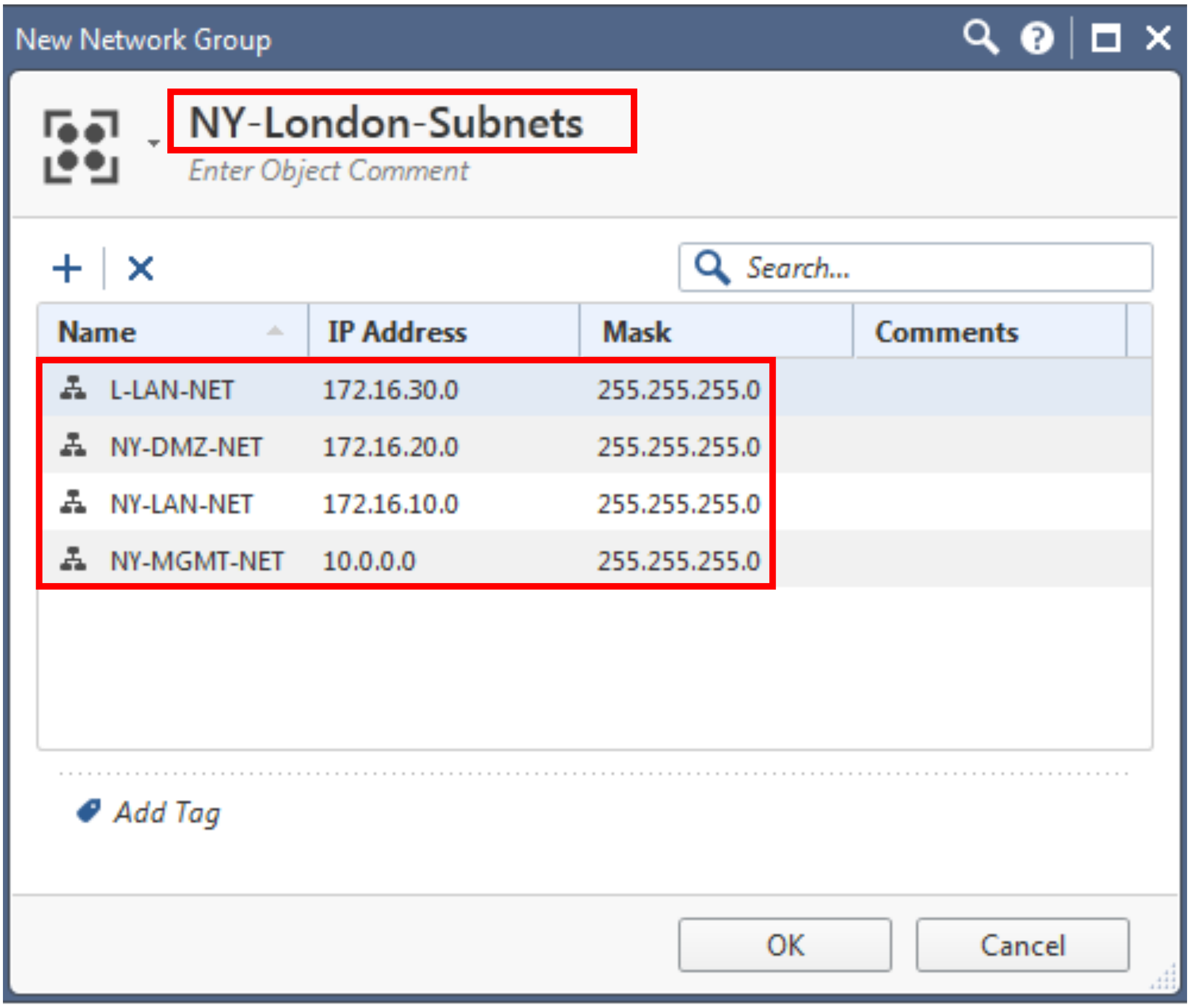
No.	Hits	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
3	0	VPN Traffic to London	NY-LAN-NET L-LAN-NET	NY-LAN-NET L-LAN-NET	NY-LONDON...	Any	Any	Accept	Log

Now, let's concentrate on the NAT configuration. We will first create a new object – Network Group type, than encompasses all internal subnets from both sites and then configure static NAT that will basically deny traffic NAT translation between these subnets.

In the top-right corner, select **New** to create a new object and then **New Network Group**.



I will name the new Network Group as **NY-London-Subnets** and include below all the subnets in these two sites:


New Network Group

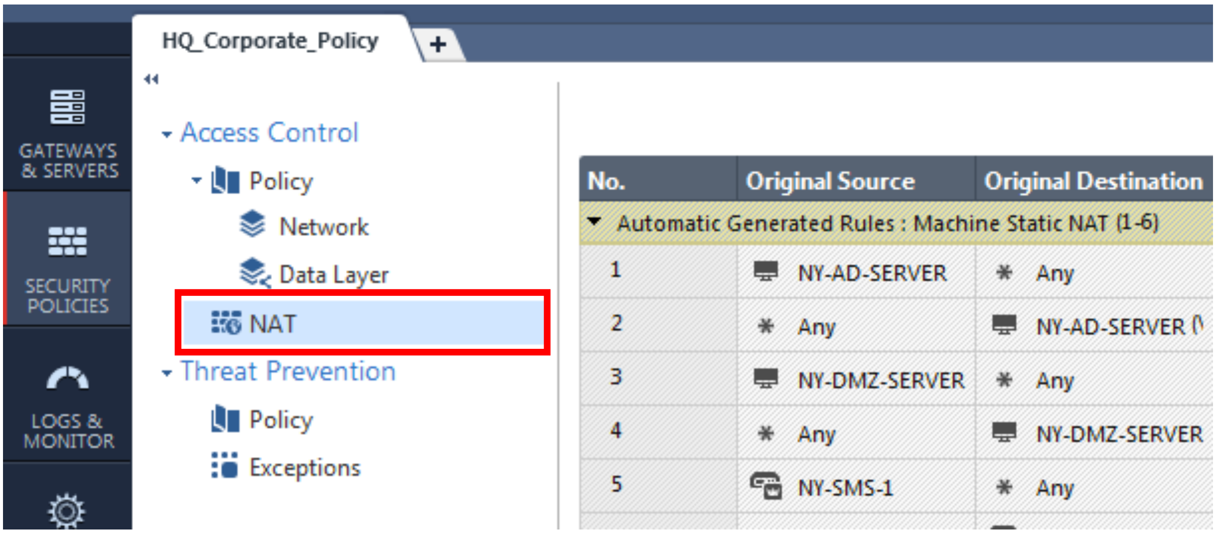
NY-London-Subnets

Enter Object Comment

Name	IP Address	Mask	Comments
L-LAN-NET	172.16.30.0	255.255.255.0	
NY-DMZ-NET	172.16.20.0	255.255.255.0	
NY-LAN-NET	172.16.10.0	255.255.255.0	
NY-MGMT-NET	10.0.0.0	255.255.255.0	

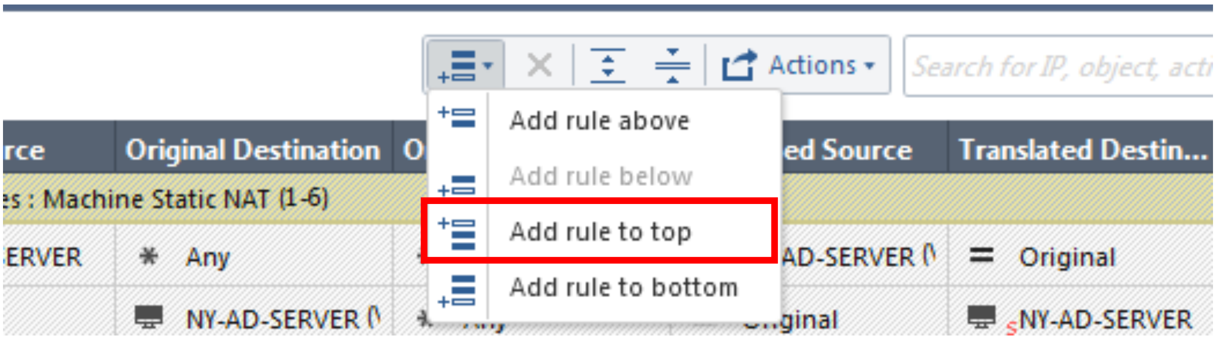
Click **OK** in order to continue.

Now, let's switch to the NAT policy:

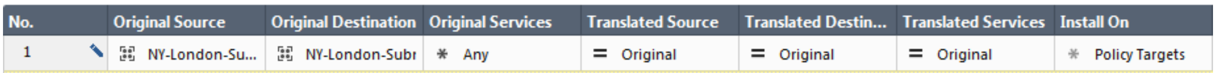


No.	Original Source	Original Destination
Automatic Generated Rules : Machine Static NAT (1-6)		
1	NY-AD-SERVER	Any
2	Any	NY-AD-SERVER (\
3	NY-DMZ-SERVER	Any
4	Any	NY-DMZ-SERVER
5	NY-SMS-1	Any

and add a new rule at the top of the NAT Rule Base. Click on the first button and select **Add rule to top**:



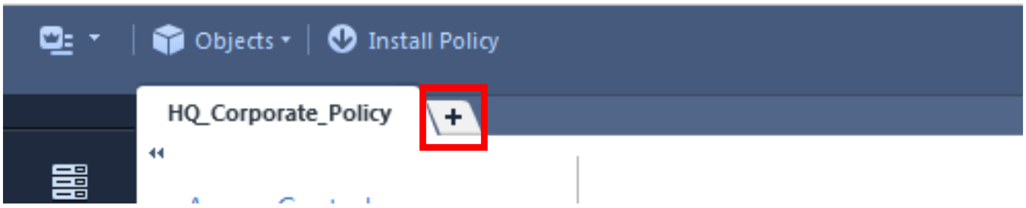
For the Original Source and Original Destination we will select the new Network Group – NY-London-Subnets and leave everything as it is, by default.



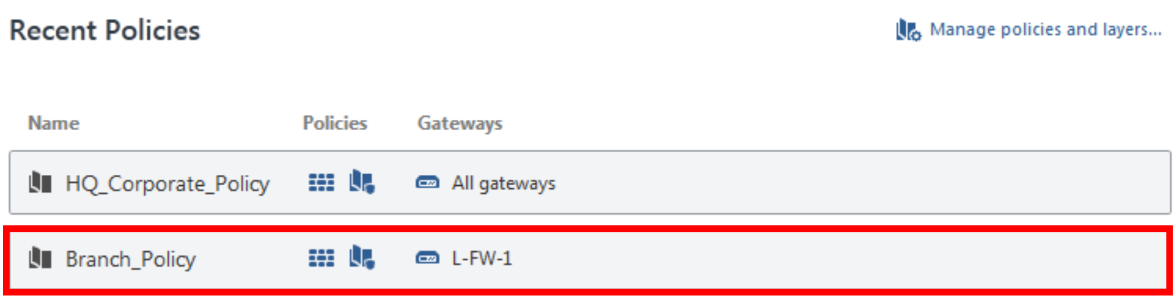
No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On
1	NY-London-Su...	NY-London-Subı	Any	= Original	= Original	= Original	Policy Targets

Finally, let's publish the changes and install the HQ_Corporate_Policy.

Now, we will go through the same steps, but this time for London site. Let's first open a new tab for the **Branch_Policy** by clicking on the **+** sign:



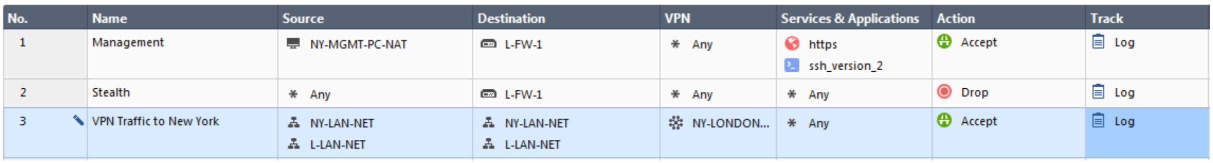
and double-click **Branch_Policy**:



Recent Policies

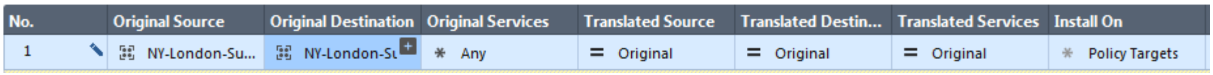
Name	Policies	Gateways
HQ_Corporate_Policy		All gateways
Branch_Policy		L-FW-1

Let’s add a new rule above the DNS rule, following the same configuration as for the London site. The new rule should look like the one below:



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Management	NY-MGMT-PC-NAT	L-FW-1	Any	https ssh_version_2	Accept	Log
2	Stealth	Any	L-FW-1	Any	Any	Drop	Log
3	VPN Traffic to New York	NY-LAN-NET L-LAN-NET	NY-LAN-NET L-LAN-NET	NY-LONDON...	Any	Accept	Log

Now, let’s add another rule to the NAT policy. Again, we will add a new rule to the top and it should look similar to the one below:

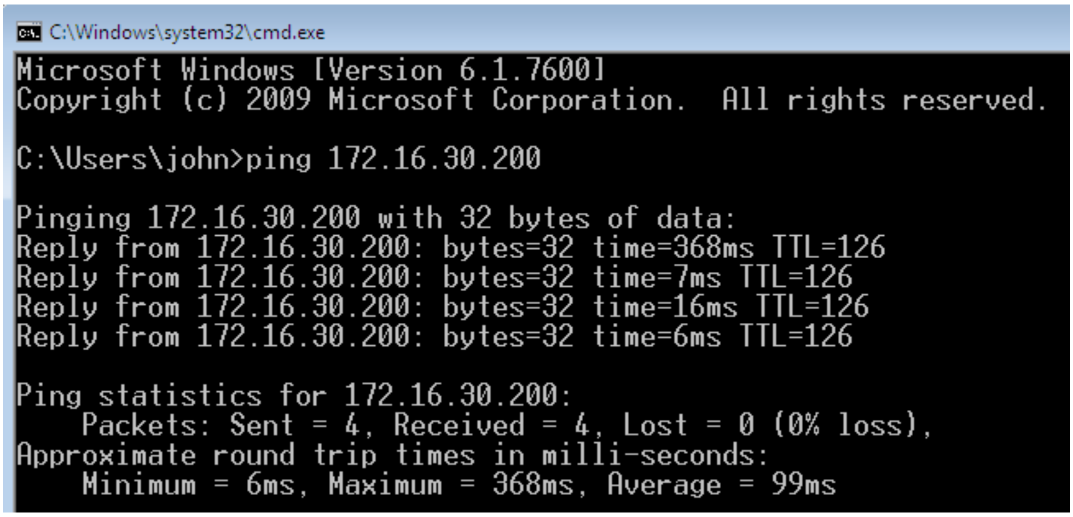


No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On
1	NY-London-Su...	NY-London-Su	Any	= Original	= Original	= Original	Policy Targets

Finally, let’s publish the changes and install the **Branch_Policy.**

Let’s verify our VPN setup.

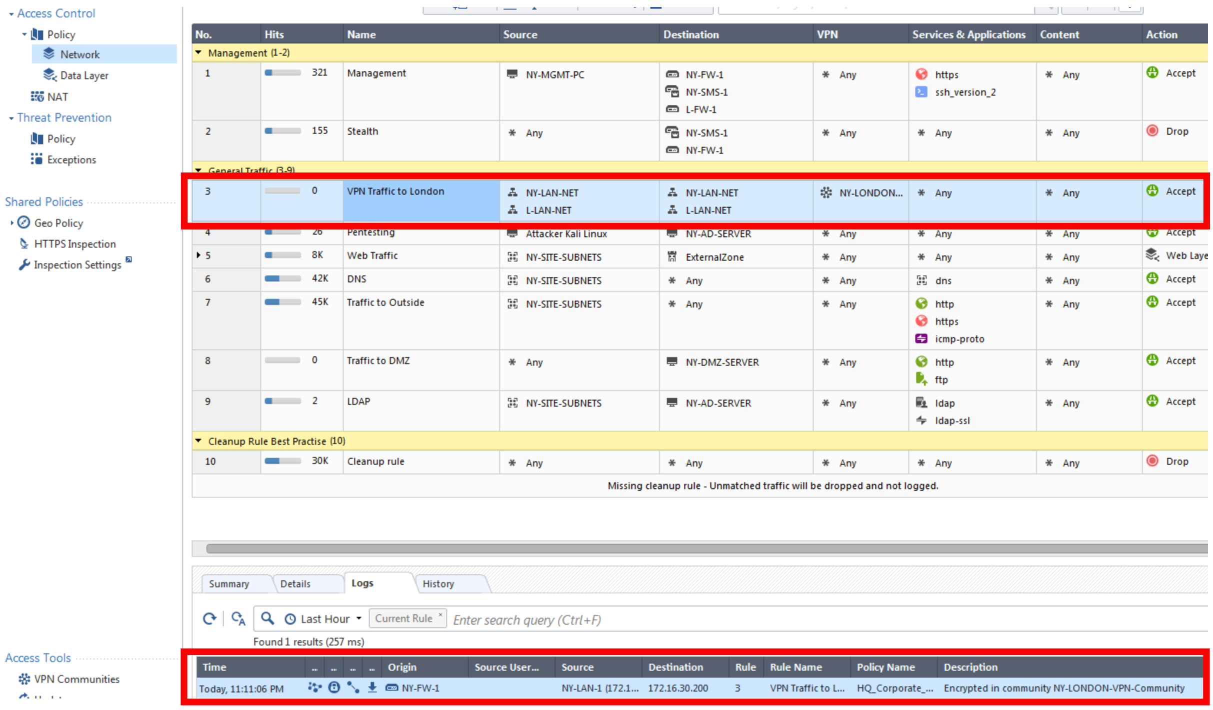
From the NY-LAN-1 PC, I will initiate an ICMP session to L-LAN-1 PC. If the ping is successful, then this is a good indication that VPN is up and running.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\john>ping 172.16.30.200

Pinging 172.16.30.200 with 32 bytes of data:
Reply from 172.16.30.200: bytes=32 time=368ms TTL=126
Reply from 172.16.30.200: bytes=32 time=7ms TTL=126
Reply from 172.16.30.200: bytes=32 time=16ms TTL=126
Reply from 172.16.30.200: bytes=32 time=6ms TTL=126

Ping statistics for 172.16.30.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 368ms, Average = 99ms
```

So it looks like ping is working. What about the logs ?

I am currently working in the HQ_Corporate_Policy and I have selected the new VPN rule. Also, at the bottom, I have selected the **Logs** tab and I see that there is one log available:



No.	Hits	Name	Source	Destination	VPN	Services & Applications	Content	Action
Management (1-2)								
1	321	Management	NY-MGMT-PC	NY-FW-1 NY-SMS-1 L-FW-1	Any	https ssh_version_2	Any	Accept
2	155	Stealth	Any	NY-SMS-1 NY-FW-1	Any	Any	Any	Drop
General Traffic (3-9)								
3	0	VPN Traffic to London	NY-LAN-NET L-LAN-NET	NY-LAN-NET L-LAN-NET	NY-LONDON...	Any	Any	Accept
4	26	Pentesting	Attacker Kali Linux	NY-AD-SERVER	Any	Any	Any	Accept
5	8K	Web Traffic	NY-SITE-SUBNETS	ExternalZone	Any	Any	Any	Web Laye
6	42K	DNS	NY-SITE-SUBNETS	Any	Any	dns	Any	Accept
7	45K	Traffic to Outside	NY-SITE-SUBNETS	Any	Any	http https icmp-proto	Any	Accept
8	0	Traffic to DMZ	Any	NY-DMZ-SERVER	Any	http ftp	Any	Accept
9	2	LDAP	NY-SITE-SUBNETS	NY-AD-SERVER	Any	ldap ldap-ssl	Any	Accept
Cleanup Rule Best Practise (10)								
10	30K	Cleanup rule	Any	Any	Any	Any	Any	Drop

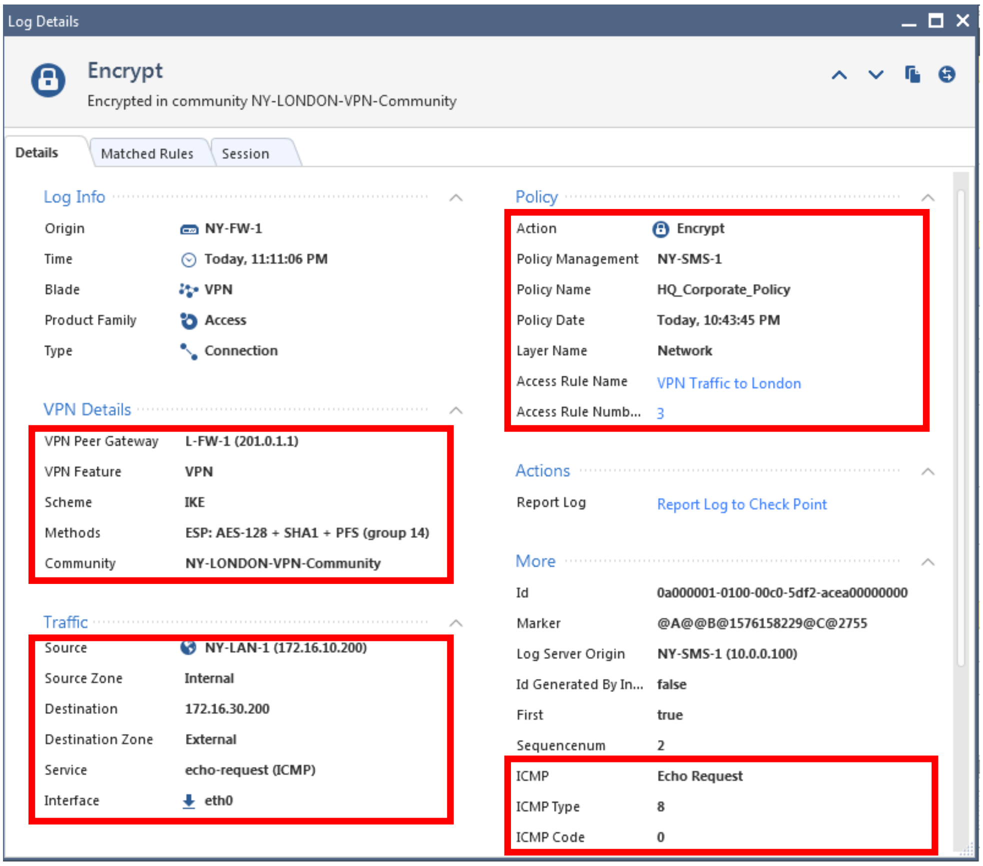
Missing cleanup rule - Unmatched traffic will be dropped and not logged.

Summary | Details | Logs | History

Last Hour | Current Rule | Enter search query (Ctrl+F)

Found 1 results (257 ms)

Time	...	...	...	...	Origin	Source User...	Source	Destination	Rule	Rule Name	Policy Name	Description
Today, 11:11:06 PM					NY-FW-1		NY-LAN-1 (172.1...	172.16.30.200	3	VPN Traffic to L...	HQ_Corporate_...	Encrypted in community NY-LONDON-VPN-Community



Log Details

Encrypt

Encrypted in community NY-LONDON-VPN-Community

Details | Matched Rules | Session

Log Info

Origin	NY-FW-1
Time	Today, 11:11:06 PM
Blade	VPN
Product Family	Access
Type	Connection

VPN Details

VPN Peer Gateway	L-FW-1 (201.0.1.1)
VPN Feature	VPN
Scheme	IKE
Methods	ESP: AES-128 + SHA1 + PFS (group 14)
Community	NY-LONDON-VPN-Community

Traffic

Source	NY-LAN-1 (172.16.10.200)
Source Zone	Internal
Destination	172.16.30.200
Destination Zone	External
Service	echo-request (ICMP)
Interface	eth0

Policy

Action	Encrypt
Policy Management	NY-SMS-1
Policy Name	HQ_Corporate_Policy
Policy Date	Today, 10:43:45 PM
Layer Name	Network
Access Rule Name	VPN Traffic to London
Access Rule Numb...	3

Actions

Report Log	Report Log to Check Point

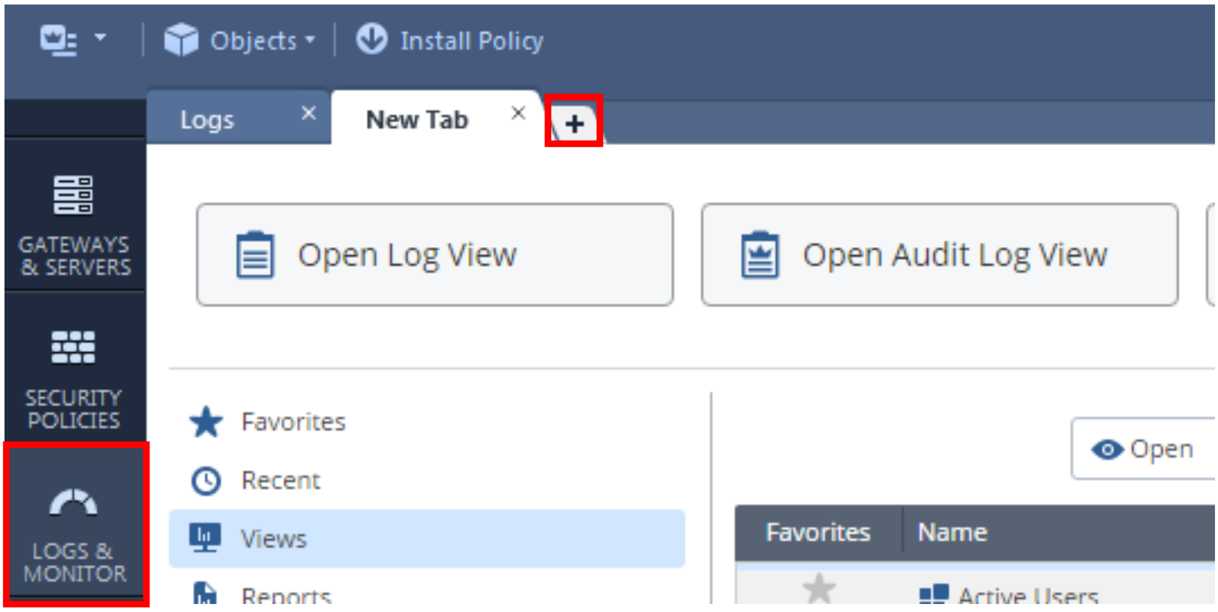
More

Id	0a000001-0100-00c0-5df2-acea00000000
Marker	@A@@B@1576158229@C@2755
Log Server Origin	NY-SMS-1 (10.0.0.100)
Id Generated By In...	false
First	true
Sequencenum	2
ICMP	Echo Request
ICMP Type	8
ICMP Code	0

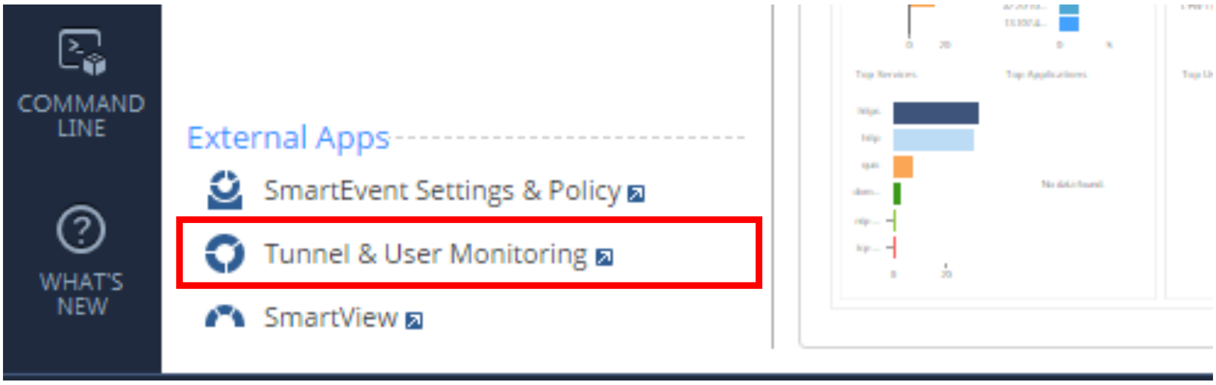
Analysing the log, I can see all this great information in one place:

- What are the VPN details ? Who is the VPN peer ? What security mechanisms have been enforced ? What VPN community is being used?
- Next is type of traffic. What is the source and destination ? What traffic is this (service) ?
- What is the Security Policy being used ? What was the action ? – Encrypt. What rules did the traffic match on?
- More details about session and traffic highlighted also.

One great tool that you can use for VPN tunnels is **SmartView Monitor.** In SmartConsole, go to **Logs&Monitor** and open a new tab.

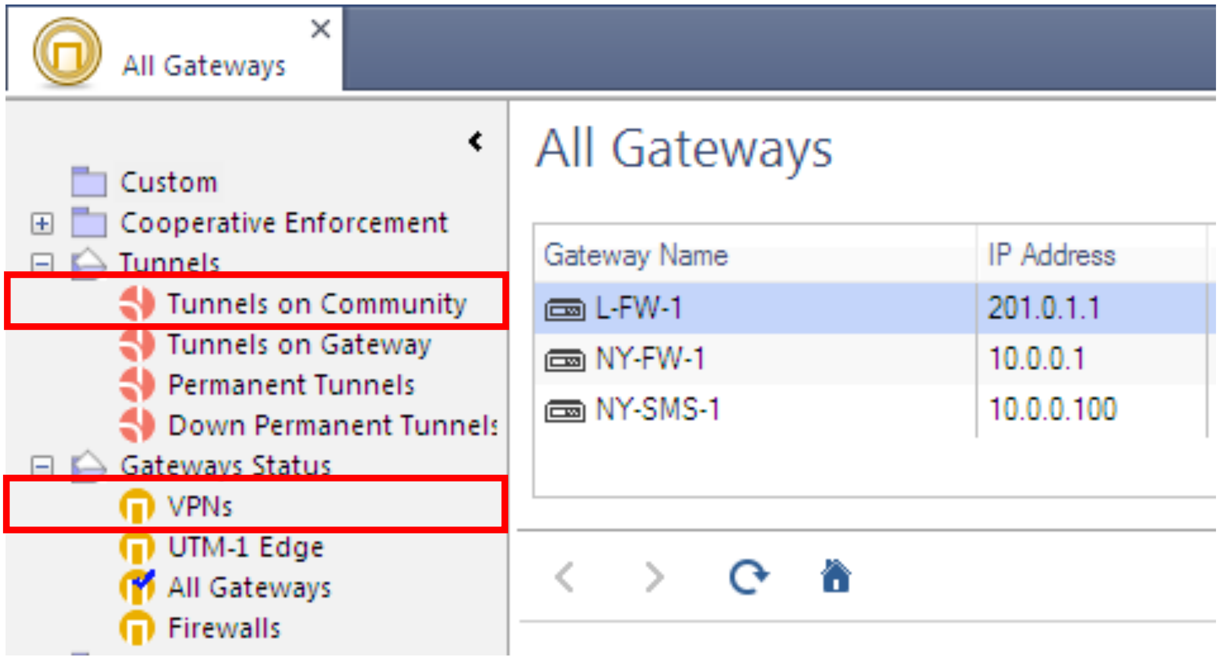


In the bottom-left corner, select **Tunnel & User Monitoring**:



and **Smartview Monitor** application will open.

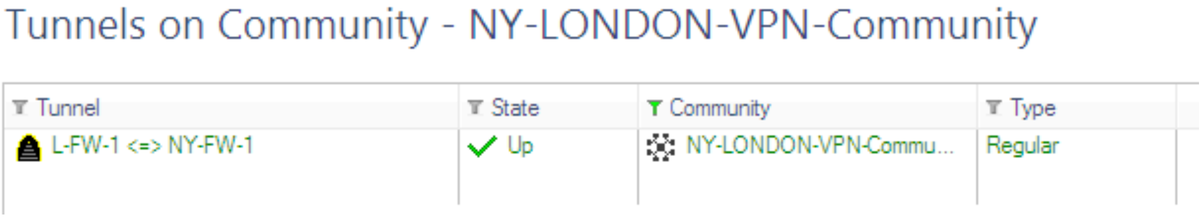
In the top-left corner, you can select **Tunnels -> Tunnels on Community**



All Gateways

Gateway Name	IP Address
L-FW-1	201.0.1.1
NY-FW-1	10.0.0.1
NY-SMS-1	10.0.0.100

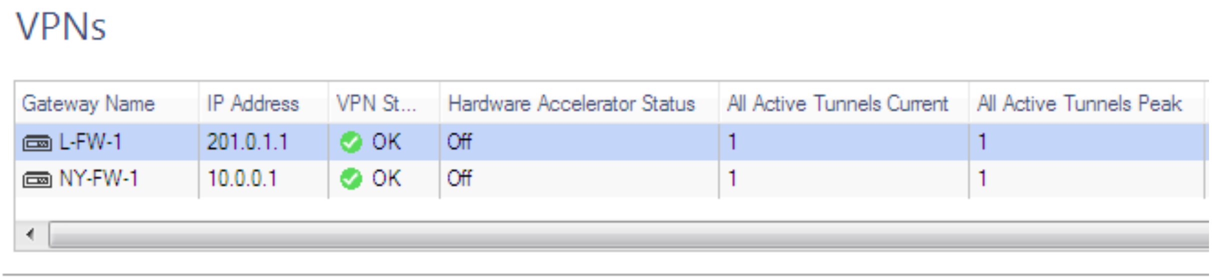
in order to see the status of all VPN tunnels in a specific VPN Community:



Tunnels on Community - NY-LONDON-VPN-Community

Tunnel	State	Community	Type
L-FW-1 <=> NY-FW-1	✓ Up	NY-LONDON-VPN-Commu...	Regular

or **VPNs** under Gateways Status:



VPNs

Gateway Name	IP Address	VPN St...	Hardware Accelerator Status	All Active Tunnels Current	All Active Tunnels Peak
L-FW-1	201.0.1.1	✓ OK	Off	1	1
NY-FW-1	10.0.0.1	✓ OK	Off	1	1