Firepower Threat Defense 6.1 Basics Lab v2

Last Updated: 12-MAY-2017

About This Lab

The goal of this hands-on lab is to give a deployment engineer the skills necessary to successfully install and configure Cisco's latest version of Next Generation Firewall (NGFW). You will deploy Firepower Management Center (FMC) and Firepower Threat Defense (FTD) devices in a realistic network topology. Once the devices have a basic configuration you will learn how to use some of the new features and benefits of the integrated Firewall (FW) and Intrusion Prevention System (IPS). Though this lab is geared to teach the basics of FTD, throughout this lab there are questions and roadblocks to help you learn what should/shouldn't (or can/can't) be done. When approaching this lab come with your thinking caps on and engaged.

In this lab, Example Corp's bid to update their edge security devices has been awarded to your company! This is a complete rip-and-replace of their existing edge security devices. There are 3 sites involved: HQ, Remote1, and Remote2. Example Corp wants each site to have basic Internet connectivity that is centrally controlled (as much as possible), and that the traffic coming into and out of their sites is secured all the way through layer 7. They also have plans to interconnect the sites with a Site-to-Site VPN.

This lab includes the following Scenarios:

Requirements

The table below outlines the requirements for this preconfigured demonstration.

Table 1. Requirements

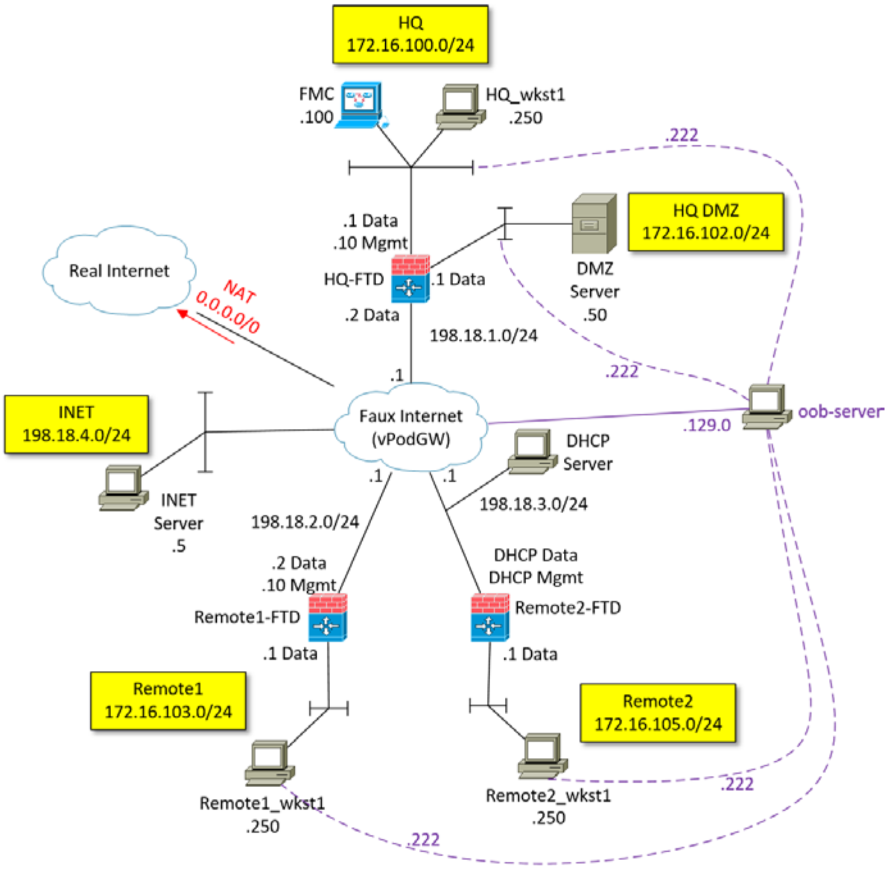
Required	Optional
• An HTML5 capable web browser.	• Laptop with Cisco AnyConnect and an RDP client.

Topology

Example Corp's HQ location consists of three networks: Inside (for internal PCs and servers), DMZ (for publicly accessible servers), and Outside (their Internet connection). In the DMZ there is a server hosting publicly facing web site and FTP/SSH services. The FTP and SSH should only be accessible from within the HQ LAN.

The remote sites are identical to each other in that they have a single LAN for the inside and are only connected to a single Internet connection.

Figure 1. Lab Topology



The purple dashed-lines and text indicate the Out-of-Band network that is used to provide RDP/SSH access to the respective workstations/servers within the lab. The purple network is not considered to be a part of the Example Corp topology.

All sites need their FTD edge device installed and configured to provide firewalling and IPS services. This means more than just Layer 3 NAT'ing and Layer 4 port filtering. Example Corp purchased Base, Threat, Malware, and URL licenses to secure each sites.

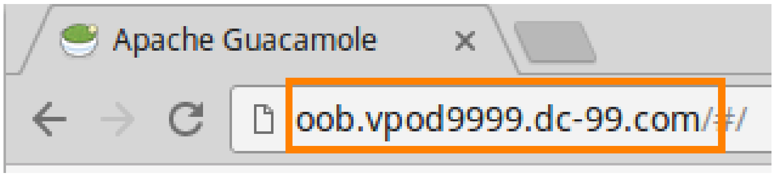
Note: Outside any of the Example Corp networks exists an Internet server that will be used to test the accessibility of Example Corp's publicly facing services and also produce nefarious activities.

Get Started

This lab environment is hosted by the dCloud organization within Cisco. You will be using the credentials provided on the dCloud website to establish an HTML5 "tunnel" from your workstation to the lab environment. You will use an HTML5 capable web browser (most modern day web browser will work) to connect from your workstation to a virtual machine (called oob) from which you can access all the other machines within the lab environment. The oob machine isn't "inline" in the lab environment and only provides Out of Band access to the machines that are actually "in" the lab. Make sure you are on the correct machine when attempting to perform the actions listed in this lab guide.

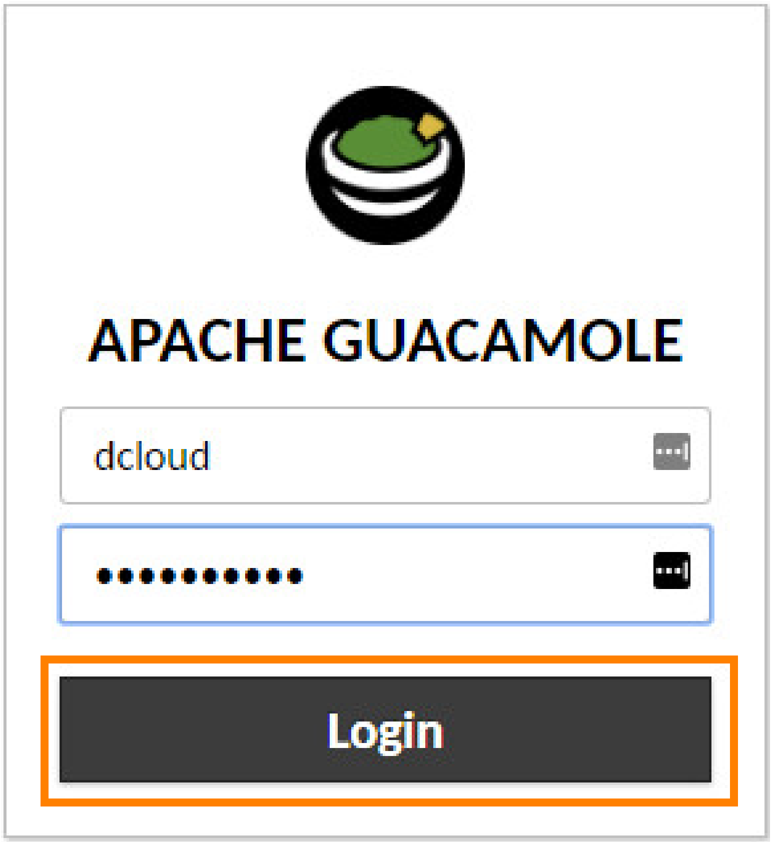
1. Go to http://dcloud.cisco.com and log in using your Cisco CCO credentials.
2. Get your lab's oob URL. It will be on the **Details** page of your dCloud session. (For example: oob.vpod9999.dc-99.com)
3. Using your local web browser access the oob URL. (For example: http://oob.vpod9999.dc-99.com)

Figure 2. Access oob webpage via your local browser



4. Log in with the username of **dcloud** and use your **Session ID** as the password.

Figure 3. Log into oob webpage



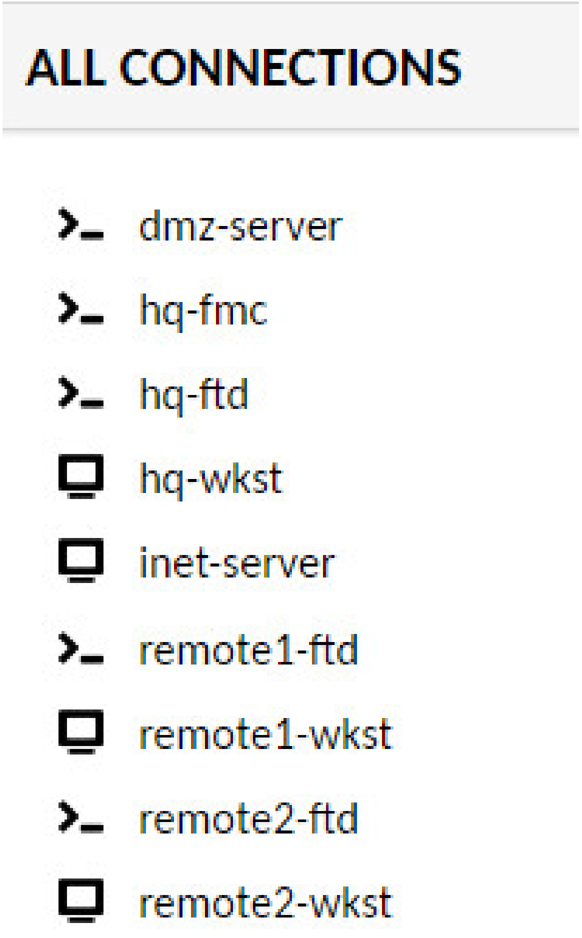
APACHE GUACAMOLE

dcloud

••••••••••

5. Once logged in you will have a link for each of the devices used in this lab. For **best practice**, right click on the link you want to use and **Open in a new tab**, otherwise you will navigate away from the main page and can't have more than one window open at a time.

Figure 4. List of oob webpage links used in this lab



ALL CONNECTIONS

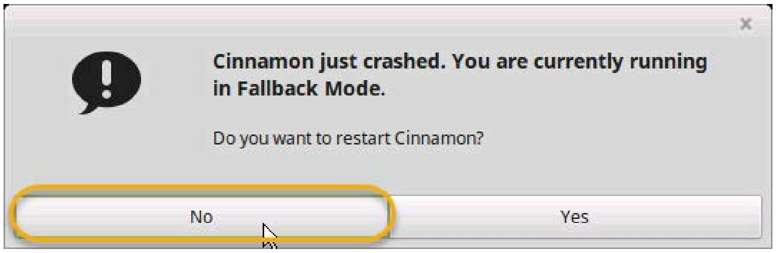
- dmz-server
- hq-fmc
- hq-ftd
- hq-wkst
- inet-server
- remote1-ftd
- remote1-wkst
- remote2-ftd
- remote2-wkst

6. (Optional) This would be a good time to test all the links to make sure all the VMs in the lab topology are working. **Right click** and **Open in a new tab** all the links listed.

Note: Having a new tab open for all the oob links is memory intensive on your computer. You may want to only open a few at a time and close the unused ones when not being referenced in the lab.

Note: The inet-server RDP session will report an error when you first attempt to access that desktop. Click **No** when asked to restart Cinnamon.

Figure 5. On inet-server, the Cinnamon desktop doesn't like xrdp.



Cinnamon just crashed. You are currently running in Fallback Mode.

Do you want to restart Cinnamon?

Page intentionally left blank.

Scenario 1. Installing the Firepower Management Center

Scenario Description

The Firepower Threat Defense (FTD) devices are not configurable via their CLI beyond setting up their Management Interfaces. In order to configure the data plane, you must use either the Firepower Device Manager (a new feature in Firepower version 6.1) or the Firepower Management Center (FMC).

In this scenario, you will configure a newly deployed virtual machine of the Firepower Management Center (FMC) that will be used to configure your FTD devices. You will also explore and discuss typical settings that could be set up in a real world deployment.

HQ-FMC Bootstrap (THIS SECTION HAS ALREADY BEEN DONE FOR YOU)

There are three methods to configure an FMC server's network settings.

- The settings can be configured at the deployment of the OVA file (if it is a virtual FMC).
- After the FMC is first booted up you can access the CLI and issue the command **sudo configure-network** and answer the questionnaire.
- After the FMC is first booted up you can access the webpage using the FMC's default IP address settings (192.168.45.45/24) and change the configuration from within there.

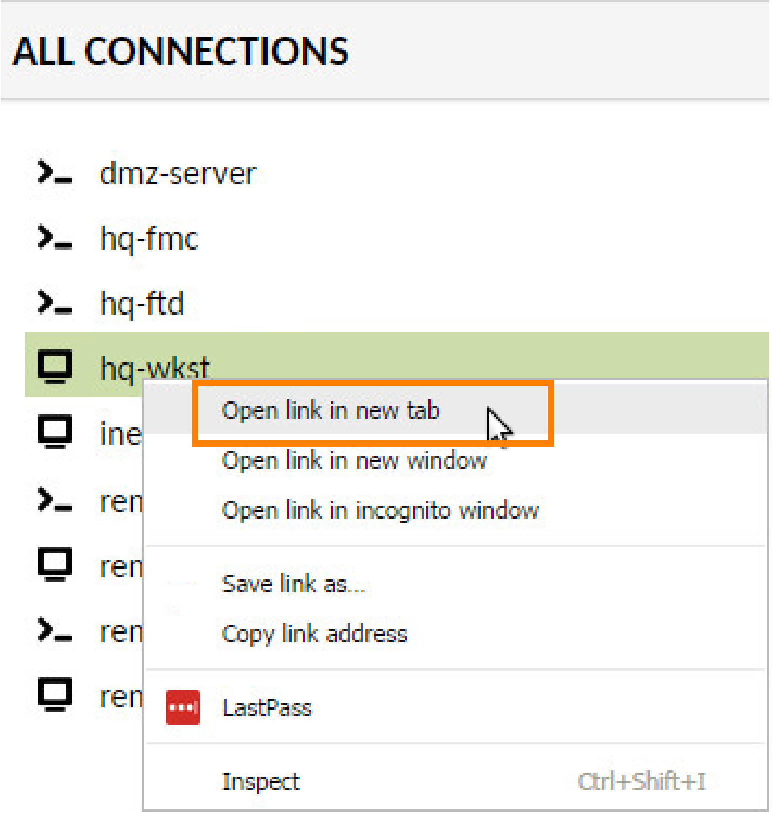
Due to limitations within the lab environment, the correct network configuration is already applied to the FMC for you. Refer to Appendix A to get details of how this was accomplished.

HQ-FMC Configuration

Once the OVA has been deployed and booted up it is time to customize it to meet Example Corp's needs.

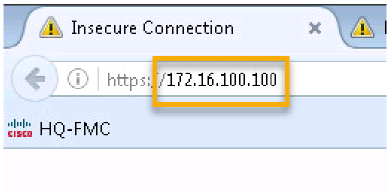
1. From the **oob webpage** open a connection to the **hq-wkst** link. The link will automatically log you into that desktop as Administrator/C1sco12345.

Figure 6. Open link to hq-wkst



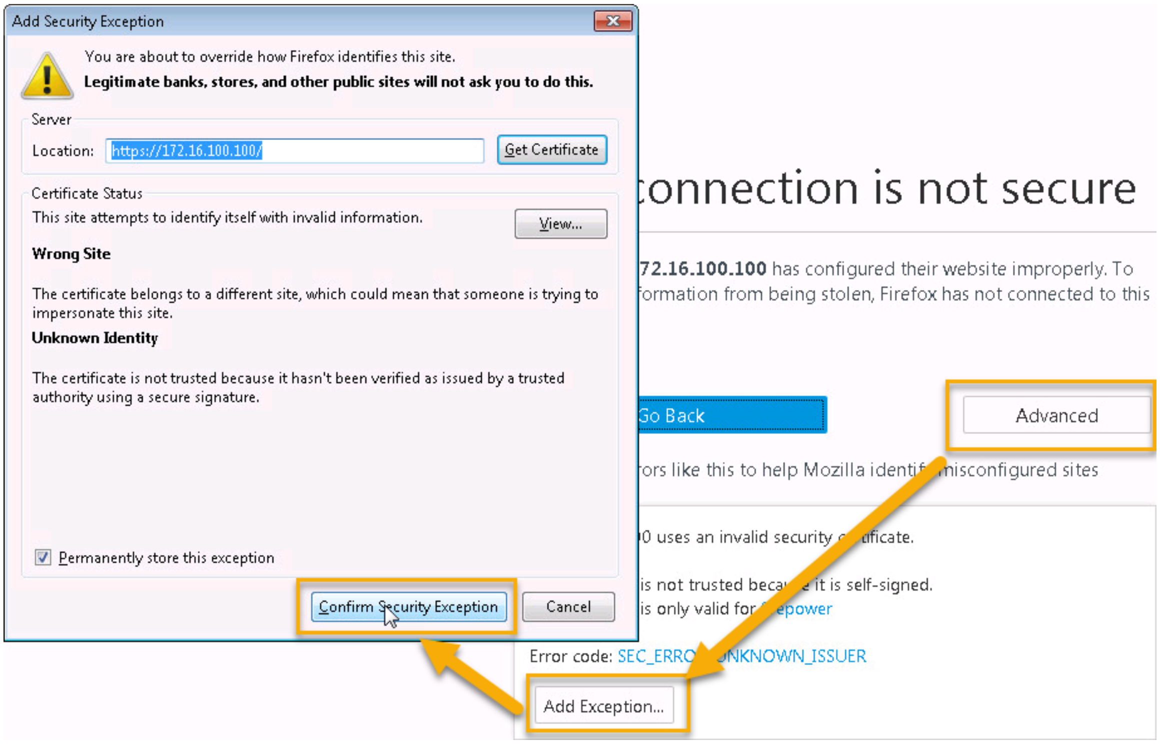
2. On **hq-wkst** open up **Firefox** and connect to **https://172.16.100.100**. (Firefox should auto load this page for you in the first tab.) The other tabs will fail to load as we haven't configured the hq-ftd firewall yet.

Figure 7. Access FMC URL



3. Accept the use of the self-signed certificate by clicking **Advanced > Add Exception** and then click the **Confirm Security Exception** in the popup window.

Figure 8. Accept SSL Self-Signed Cert from FMC



Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://172.16.100.100/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

connection is not secure

72.16.100.100 has configured their website improperly. To formation from being stolen, Firefox has not connected to this

ors like this to help Mozilla identif misconfigured sites

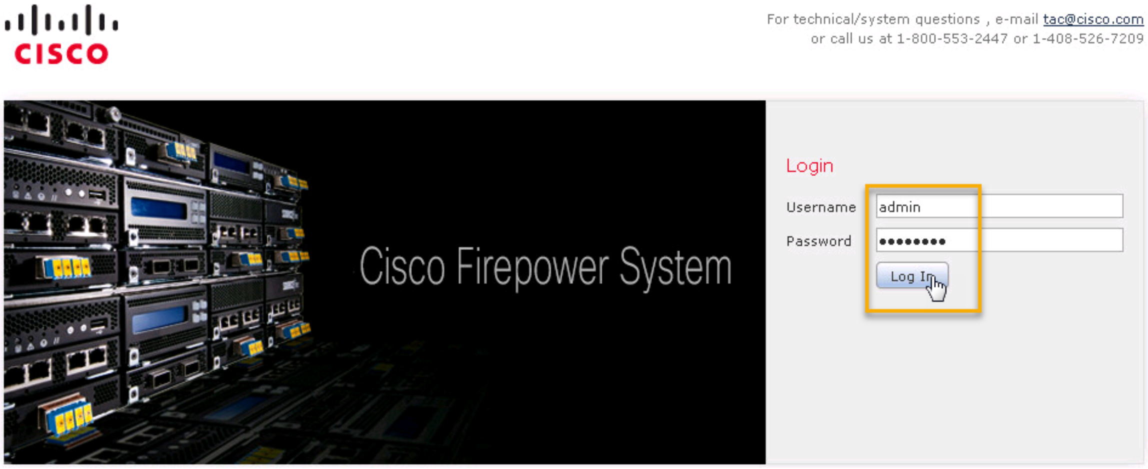
0 uses an invalid security ificate.

is not trusted beca it is self-signed.
is only valid for epower

Error code: SEC_ERRO NKNOWN_ISSUER

4. The default username and password for the FMC is **admin**/**Admin123**. Use this information to log into the webpage.

Figure 9. Log into FMC



For technical/system questions , e-mail tac@cisco.com
or call us at 1-800-553-2447 or 1-408-526-7209

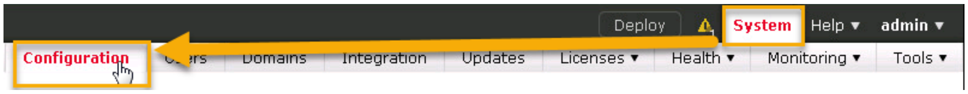
Login

Username: admin

Password: ••••••••

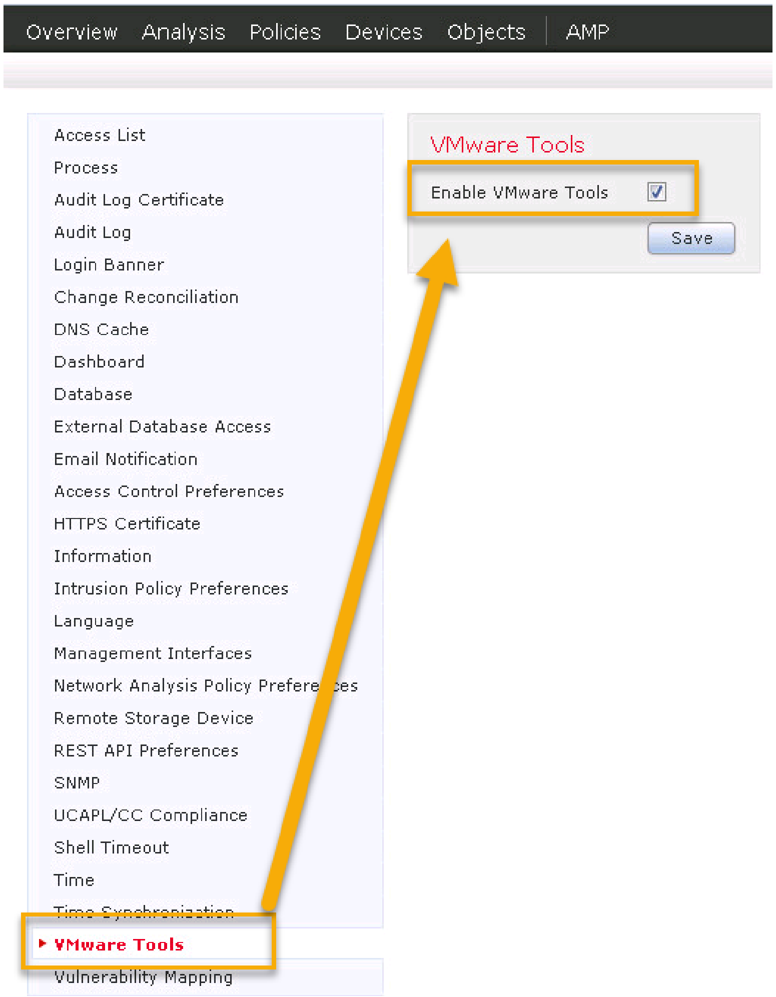
5. Now explore some of the options available for configuring, monitoring, and managing the FMC. Navigate to **System > Configuration**.

Figure 10. Navigation



6. Select **VMware Tools** from the left column menu. Ensure **Enable VMware Tools** checkbox is checked. (If not, check the box and click Save.) Obviously this is only important if you are running the FMC as a virtual machine on VMware. The nice thing is that it is enabled by default whereas there is no VMware Tools for the FTD virtual machines.

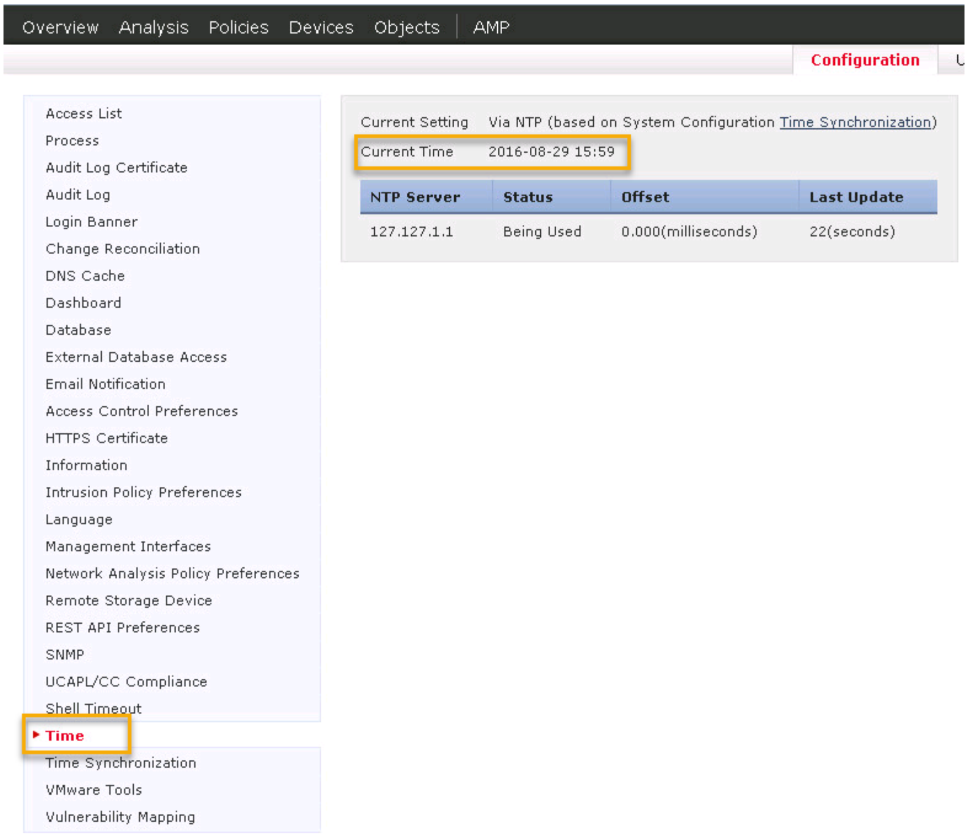
Figure 11. Ensure VMware Tools is Enabled



7. Select **Time** from the left column menu.

8. Notice the Current Time value. The default time zone for the FMC is Eastern. Example Corp is in the Mountain time zone. Time is very important when tracking events so you need to get the Date, Time, and Timezone to be as accurate as possible.

Figure 12. See the current time



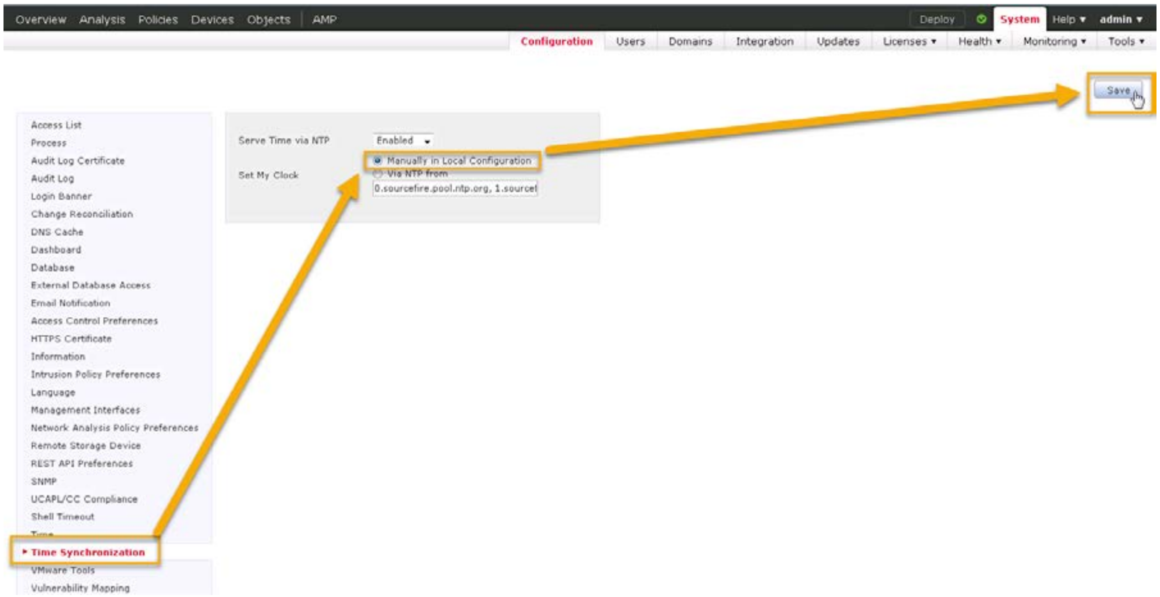
Current Setting Via NTP (based on System Configuration Time Synchronization)
Current Time 2016-08-29 15:59

NTP Server	Status	Offset	Last Update
127.127.1.1	Being Used	0.000(milliseconds)	22(seconds)

9. Select **Time Synchronization** from the left column menu.

10. Typically keeping the setting to NTP is preferred but to change the time zone you need to temporarily use the manual setting. Click the **Manually in Local Configuration** radio button and click **Save**.

Figure 13. Change to Manual time configuration



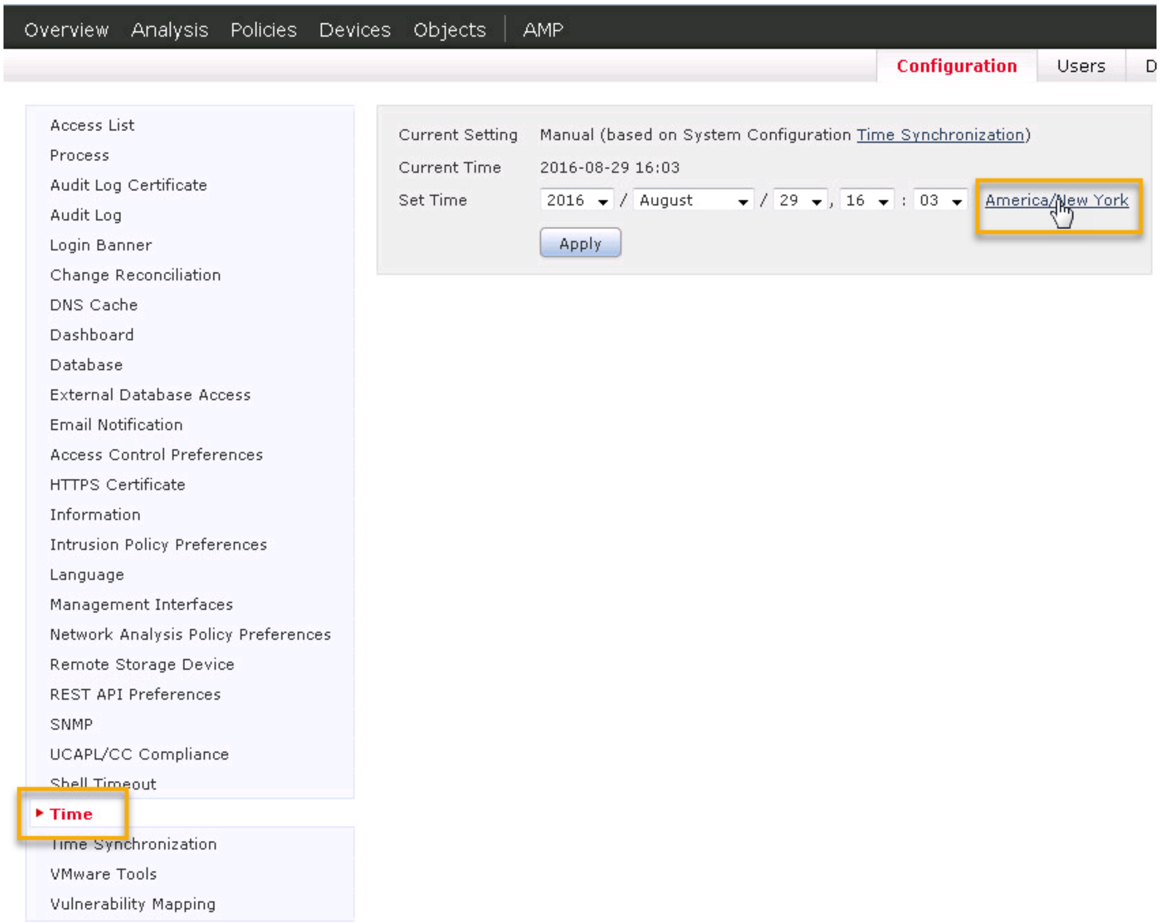
Serve Time via NTP: Enabled

Set My Clock: ● Manually in Local Configuration ○ Via NTP from 0.sourcefire.pool.ntp.org, 1.sourcef

11. It will take a minute but once the page refreshes select on the **Time** menu tab again.

12. Now you can set the Date, Time, and Time zone to be as accurate as possible. Click the **America/New York** link to modify the time zone.

Figure 14. Time to change the time zone



Current Setting Manual (based on System Configuration Time Synchronization)

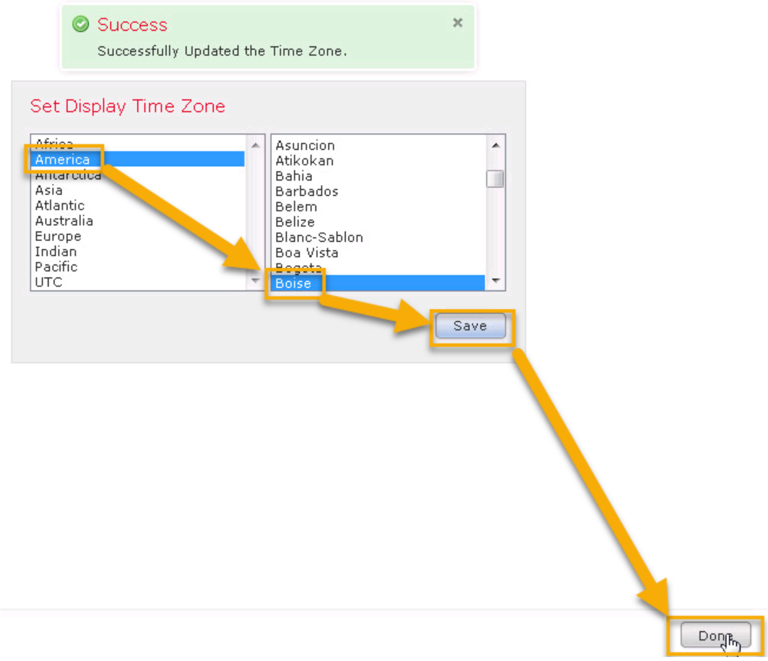
Current Time 2016-08-29 16:03

Set Time 2016 / August / 29 , 16 : 03

13. From the **Set Display Time Zone** popup window select **America** from the left column and **Boise** from the right column. Click **Save**.

14. When the page refreshes click **Done**.

Figure 15. Update time zone to Mountain



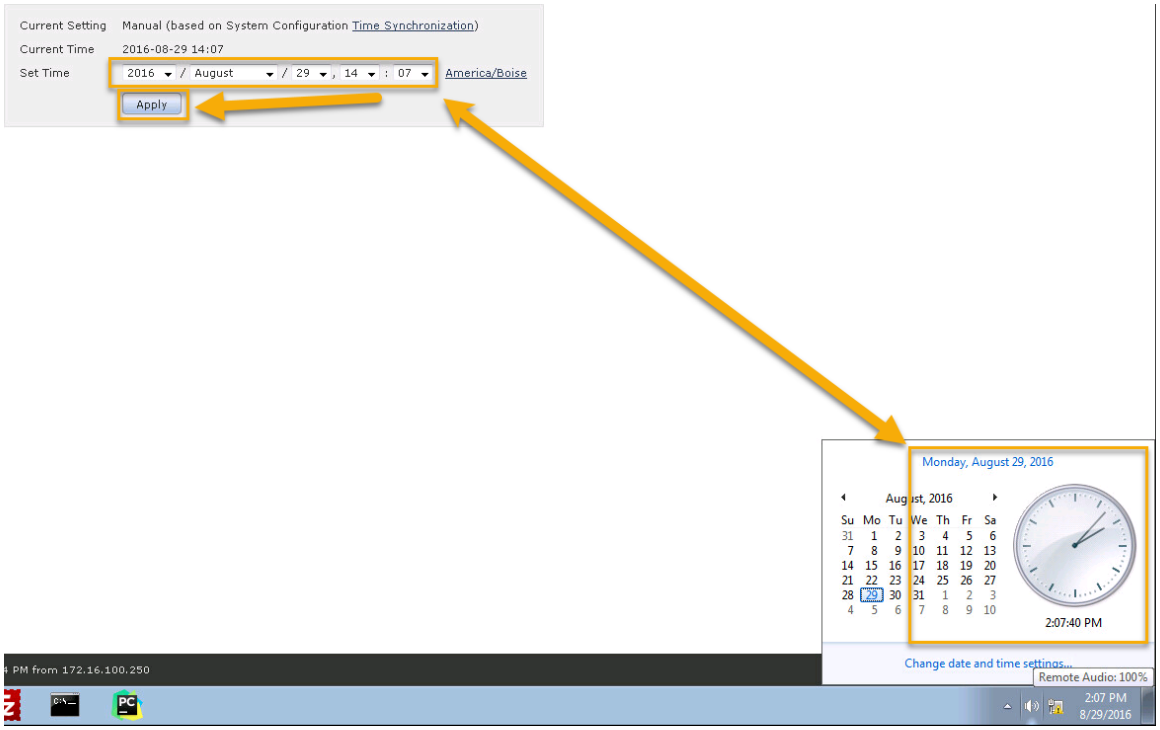
Success

Successfully Updated the Time Zone.

Set Display Time Zone

15. Using the **Set Time** dropdown menus set the time for the FMC to **match the time** of the hq-wkst clock then click **Apply**.

Figure 16. Set the time



Current Setting Manual (based on System Configuration Time Synchronization)

Current Time 2016-08-29 14:07

Set Time 2016 / August / 29 , 14 : 07 America/Boise

Monday, August 29, 2016

August, 2016

Su	Mo	Tu	We	Th	Fr	Sa
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

2:07:40 PM

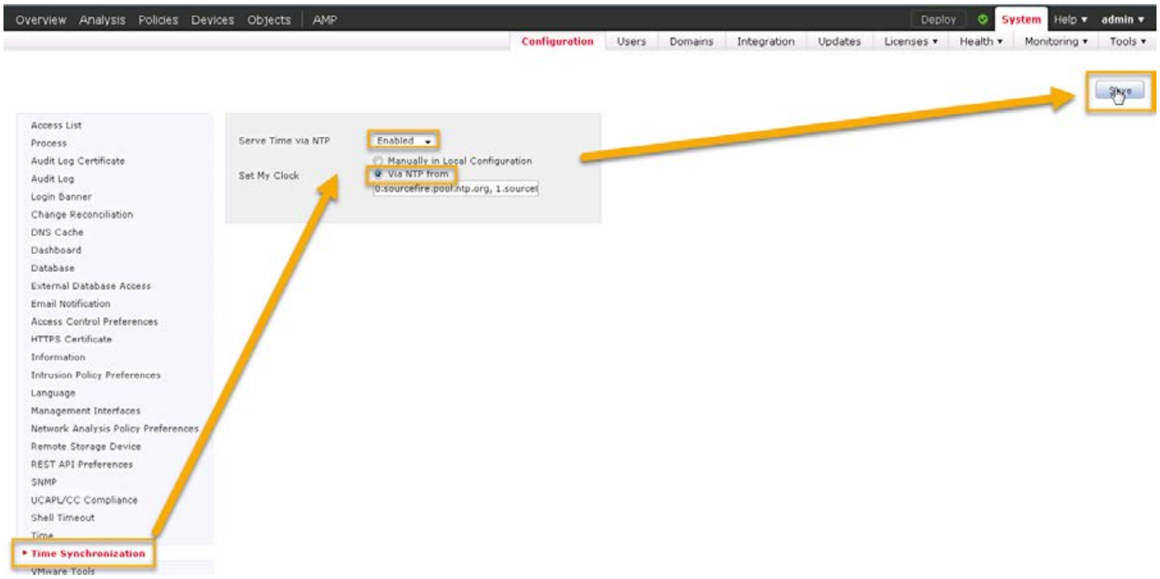
4 PM from 172.16.100.250

2:07 PM
8/29/2016

16. Return to the **Time Synchronization** menu tab again. Ensure that **Serve Time via NTP** is enabled (thus making the FMC an NTP server). Click the **Via NTP from** radio button and click **Save**. (The default NTP server list is “0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, 3.sourcefire.pool.ntp.org”.) Notice how you can set multiple NTP server sources by separating them by a comma.

The Save on this page take a long time to finish. Please be patient.

Figure 17. Back to NTP-based time



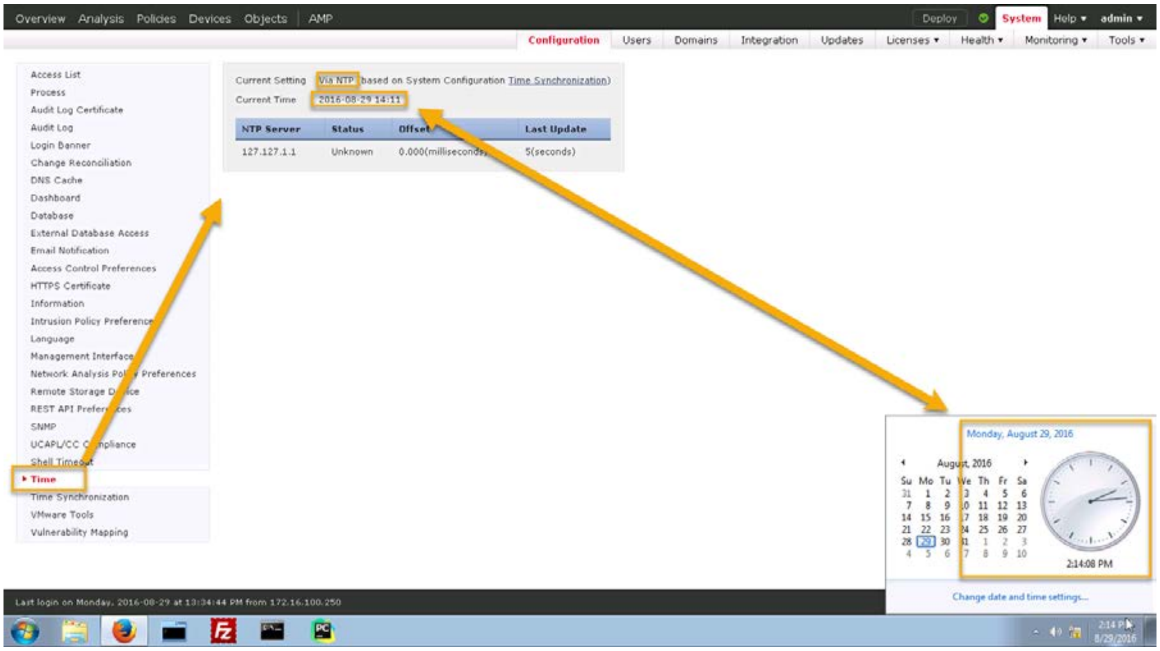
Serve Time via NTP: Enabled

Set My Clock: ○ Manually in Local Configuration ● Via NTP from

0.sourcefire.pool.ntp.org, 1.sourcef

17. Once the page has refreshed go back to the **Time** menu tab again and ensure the time is close to the same time as what is on hq-wkst. (Since the hq-ftd device is not yet configured the NTP service can't update so the time might be a little off until you get through Scenario 3.)

Figure 18. Double checking your time work



Current Setting Via NTP (based on System Configuration Time Synchronization)

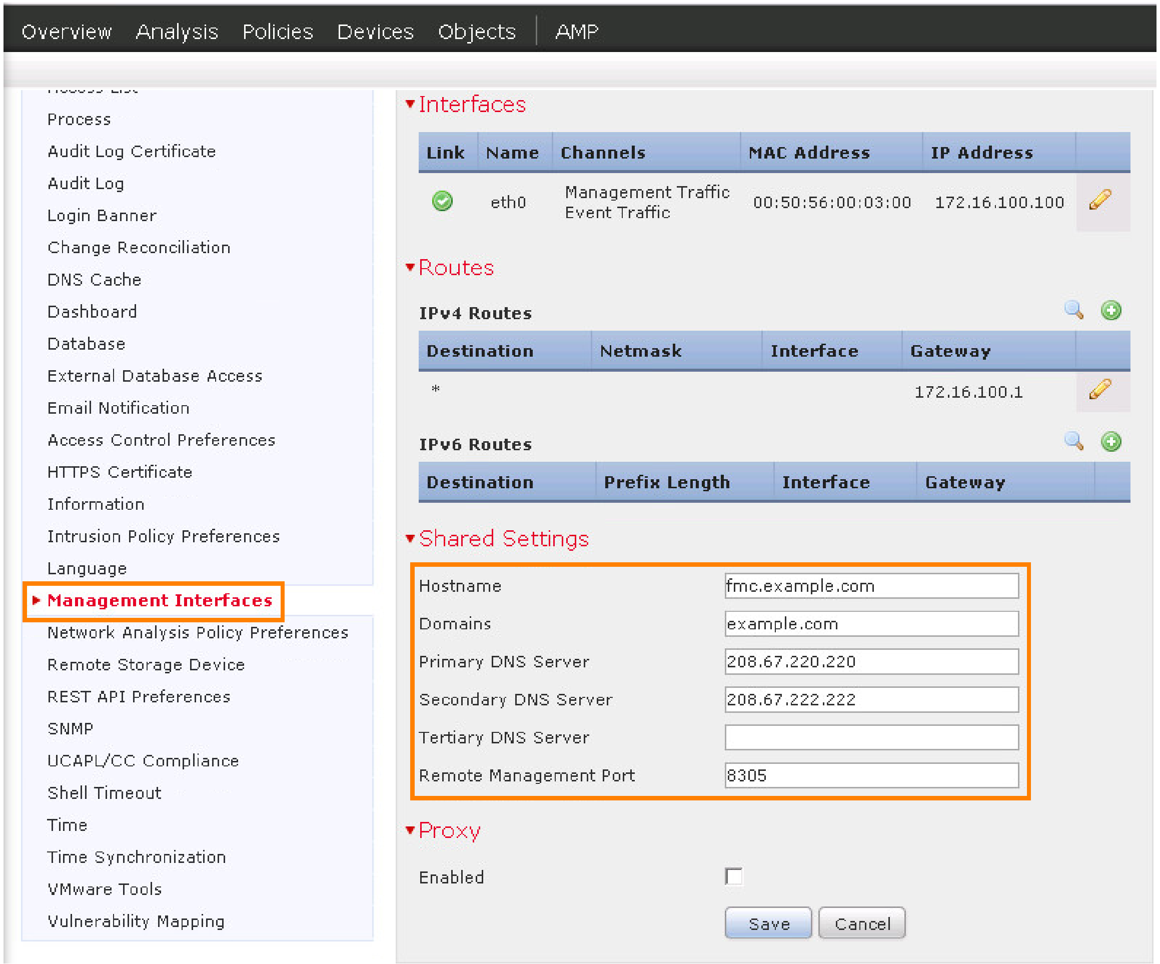
Current Time 2016-08-29 14:11

NTP Server	Status	Offset	Last Update
127.127.1.1	Unknown	0.000(milliseconds)	5(seconds)

Last login on Monday, 2016-08-29 at 13:34:44 PM from 172.16.100.250

18. Select the **Management Interfaces** tab from the left column of menu items. Notice how on this page you can set things such as Hostname, Domains, and DNS Servers.

Figure 19. Management Interface Stuff



Interfaces

Link	Name	Channels	MAC Address	IP Address
✓	eth0	Management Traffic Event Traffic	00:50:56:00:03:00	172.16.100.100

Routes

IPv4 Routes

Destination	Netmask	Interface	Gateway
*			172.16.100.1

IPv6 Routes

Destination	Prefix Length	Interface	Gateway

Shared Settings

Hostname	fmc.example.com
Domains	example.com
Primary DNS Server	208.67.220.220
Secondary DNS Server	208.67.222.222
Tertiary DNS Server	
Remote Management Port	8305

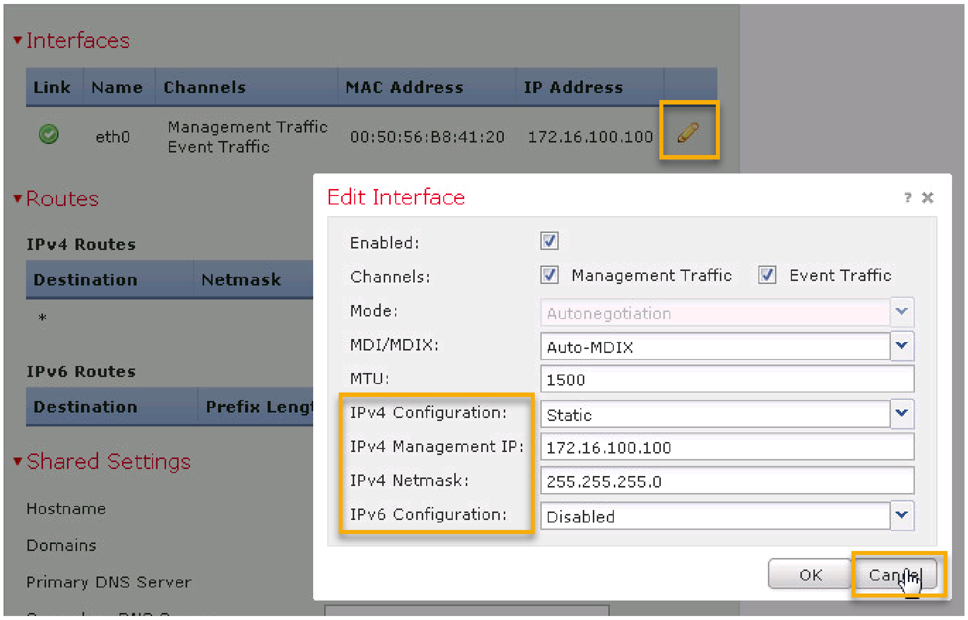
Proxy

Enabled □

The Remote Management Port is the TCP port used to communicate with the devices that this FMC manages.

19. Click the **pencil icon** next the IP address **172.16.100.100**. This is where you can change the IP address for the FMC and also, this is where you can set an IPv6 address if you so desire. Click **Cancel** when done reviewing the information.

Figure 20. Change IPv4/IPv6 addressing of FMC



▾Interfaces

Link	Name	Channels	MAC Address	IP Address
✓	eth0	Management Traffic Event Traffic	00:50:56:B8:41:20	172.16.100.100

▾Routes

IPv4 Routes

Destination	Netmask
*	

IPv6 Routes

Destination	Prefix Lengt

▾Shared Settings

Hostname

Domains

Primary DNS Server

Edit Interface

Enabled: ☑

Channels: ☑ Management Traffic ☑ Event Traffic

Mode: Autonegotiation

MDI/MDIX: Auto-MDIX

MTU: 1500

IPv4 Configuration: Static

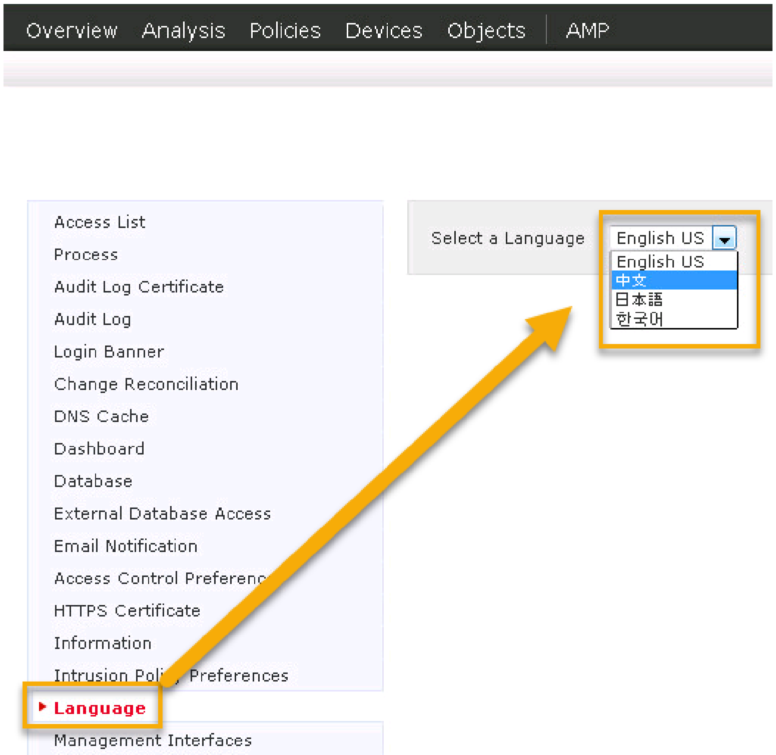
IPv4 Management IP: 172.16.100.100

IPv4 Netmask: 255.255.255.0

IPv6 Configuration: Disabled

20. Select the **Language** tab from the left column of menu items. Click the dropdown button for the **Select a Language** field and notice the list of available languages to change the FMC into.

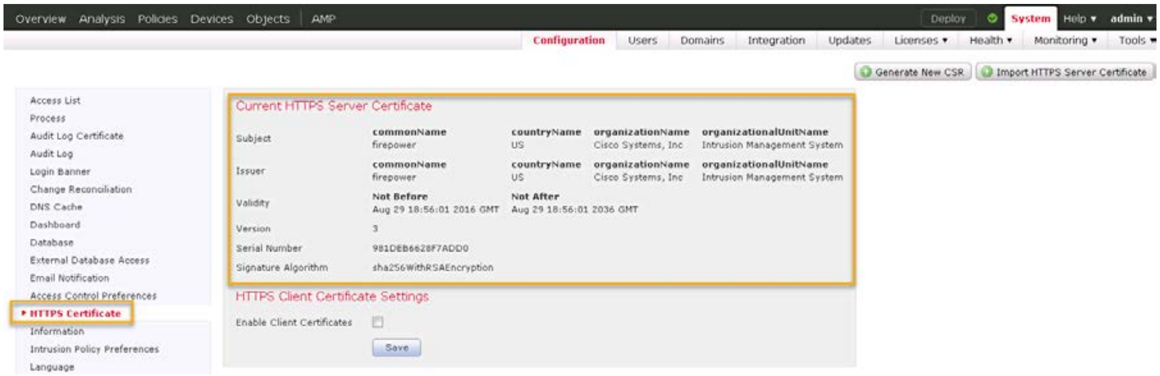
Figure 21. Language options for FMC



Select a Language: English US

21. Select the **HTTPS Certificate** tab from the left column of menu items. This page takes **a long time** to load but this is where you can install a legitimate certificate instead of using the self-signed one that is used by default.

Figure 22. Set up new SSL Certificates for FMC



Current HTTPS Server Certificate

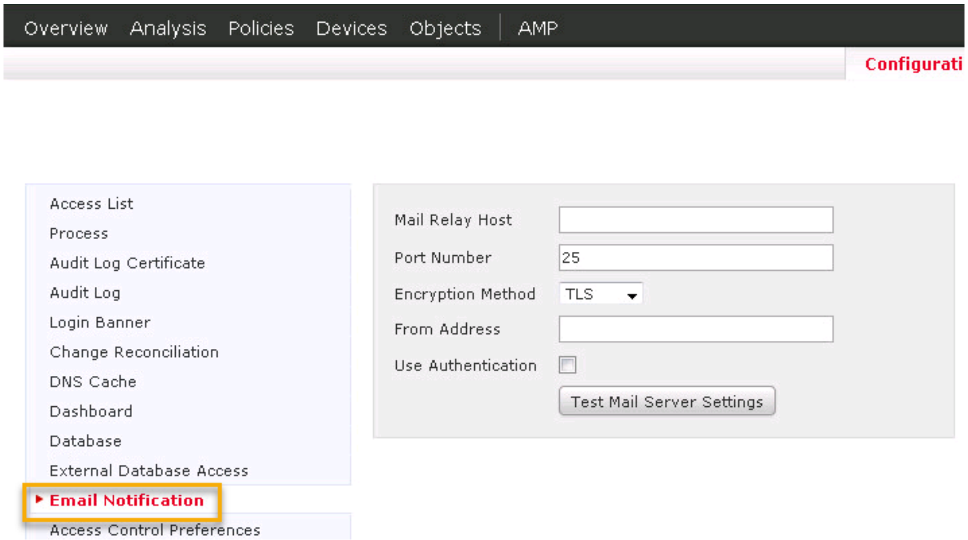
Subject	**commonName** firepower	**countryName** US	**organizationName** Cisco Systems, Inc	**organizationalUnitName** Intrusion Management System
Issuer	**commonName** firepower	**countryName** US	**organizationName** Cisco Systems, Inc	**organizationalUnitName** Intrusion Management System
Validity	**Not Before** Aug 29 18:56:01 2016 GMT	**Not After** Aug 29 18:56:01 2036 GMT		
Version	3			
Serial Number	981DEB6628F7ADD0			
Signature Algorithm	sha256WithRSAEncryption			

HTTPS Client Certificate Settings

Enable Client Certificates ☐

22. Select the **Email Notification** tab from the left column of menu items. There isn't a mail server in the lab but to set up an email server to send notifications/alerts to you'd do so on this page.

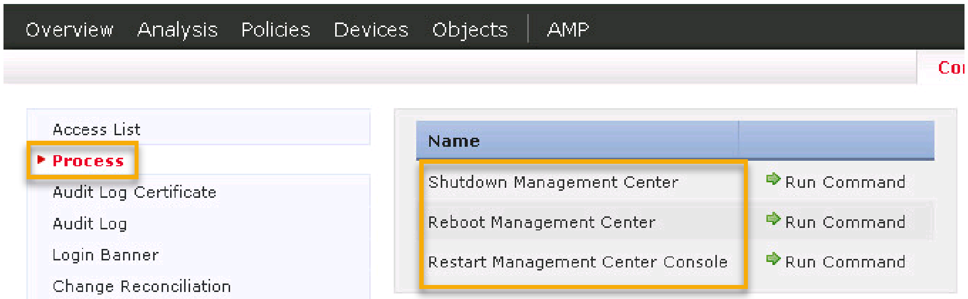
Figure 23. You'd configure an email server here



Mail Relay Host	
Port Number	25
Encryption Method	TLS
From Address	
Use Authentication	□

23. Select the **Process** tab from the left column of menu items. This is where you can gracefully shutdown, reboot, or restart FMC services.

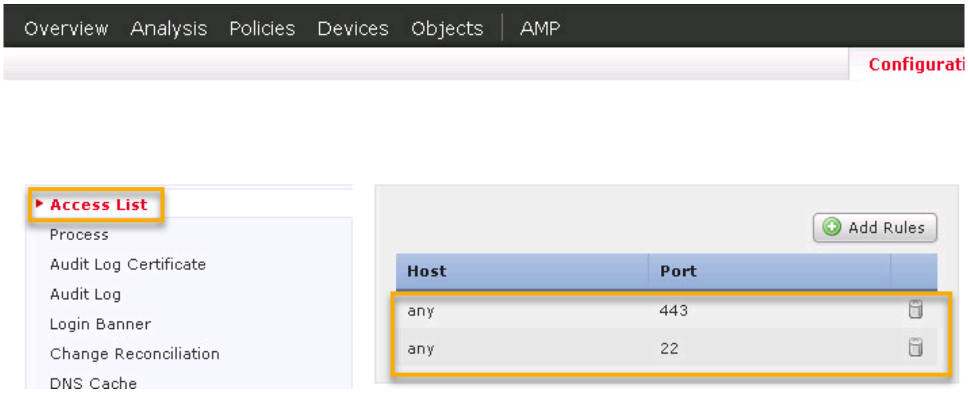
Figure 24. Commands to shutdown/reboot FMC



Name	
Shutdown Management Center	Run Command
Reboot Management Center	Run Command
Restart Management Center Console	Run Command

24. Select the **Access List** tab from the left column of menu items. This is where you can limit/control what IPs have access to the FMC.

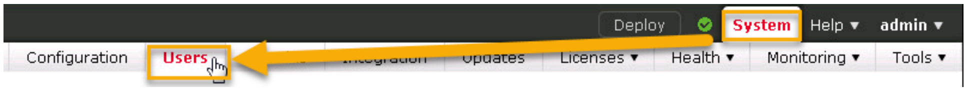
Figure 25. ACLs for FMC Access



Host	Port
any	443
any	22

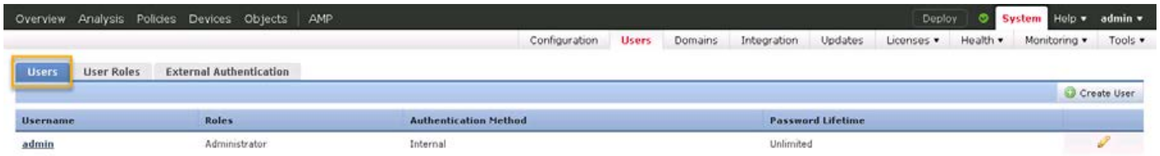
25. Navigate to **System > Users**.

Figure 26. Navigate to Users page



26. On the **Users** tab is a listing of all the locally configured users. As you can see only the “admin” user is configured by default. Later in the lab you will create a new user by returning to this page.

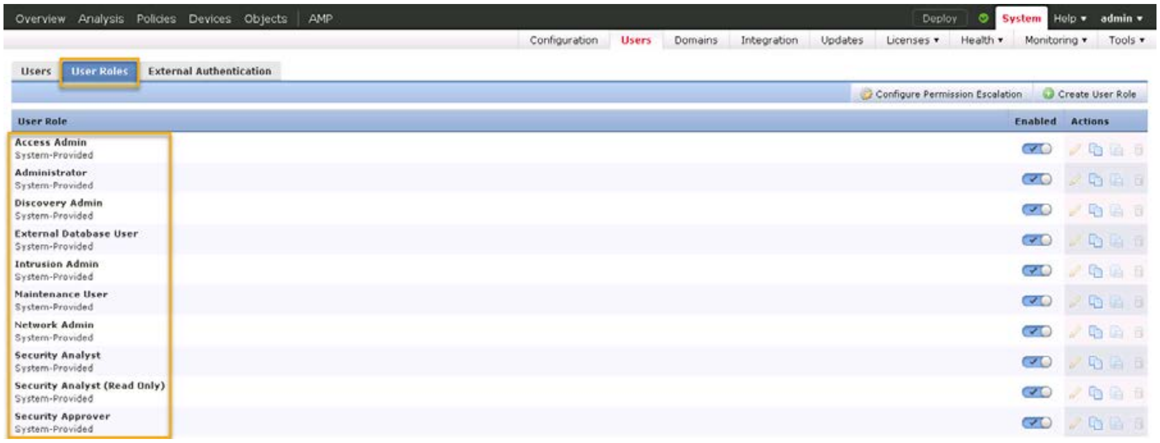
Figure 27. Users tab



Username	Roles	Authentication Method	Password Lifetime
admin	Administrator	Internal	Unlimited

27. Click the **User Roles** tab. Though it is beyond the scope for this lab you have a wide range of predefined user roles to use should you want to.

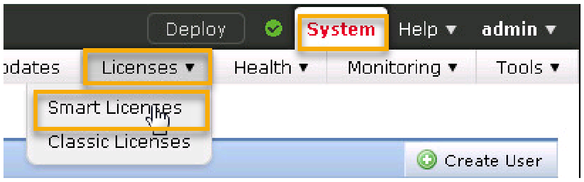
Figure 28. User Roles tab



User Role	Enabled	Actions
Access Admin System-Provided		
Administrator System-Provided		
Discovery Admin System-Provided		
External Database User System-Provided		
Intrusion Admin System-Provided		
Maintenance User System-Provided		
Network Admin System-Provided		
Security Analyst System-Provided		
Security Analyst (Read Only) System-Provided		
Security Approver System-Provided		

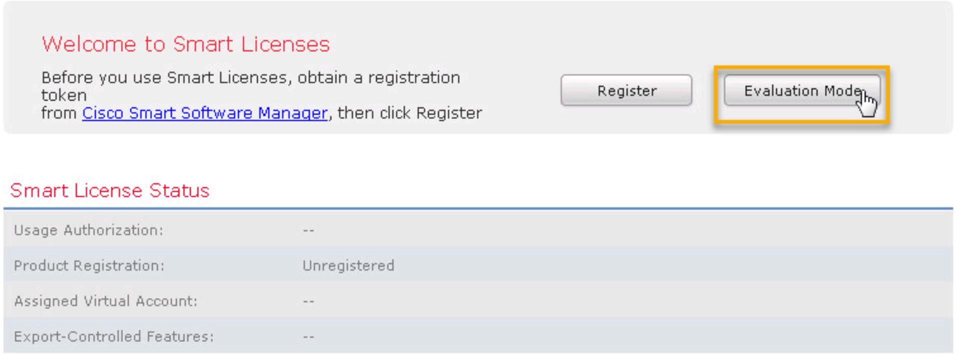
28. Finally, and most importantly, navigate to **System > Licenses > Smart Licenses**.

Figure 29. Navigate to Smart Licenses



29. Normally this is where you'd register your FMC with Cisco to get its assigned licenses. In the lab you are going to use the evaluation licenses. So, click **Evaluation Mode**.

Figure 30. Enable Eval Licenses



Welcome to Smart Licenses

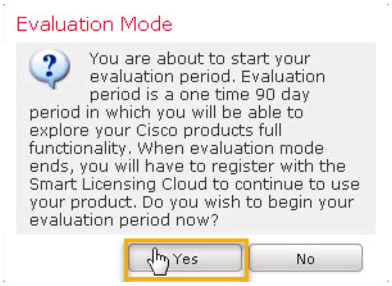
Before you use Smart Licenses, obtain a registration token
from Cisco Smart Software Manager, then click Register

Smart License Status

Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--

30. Click **Yes** to the 90-day evaluation mode warning.

Figure 31. Click Yes

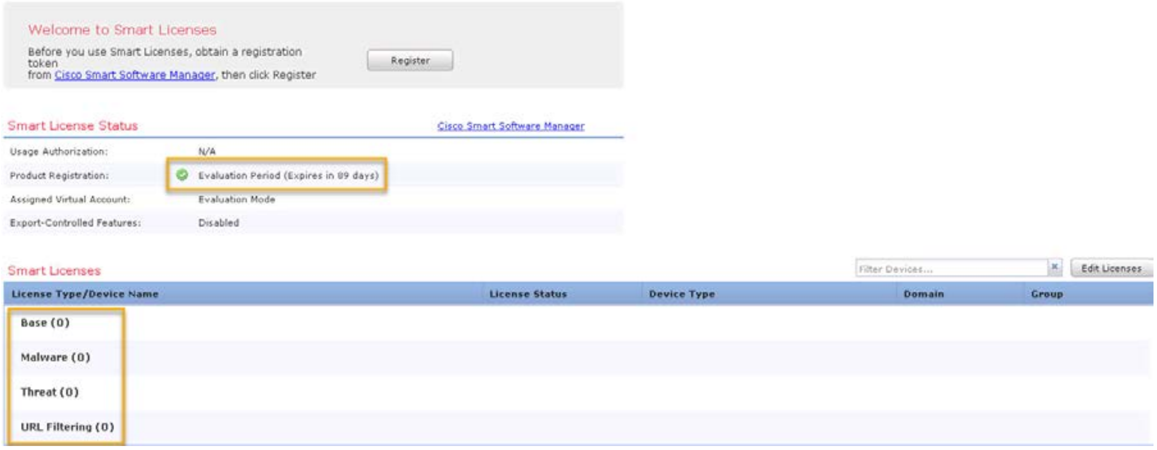


Evaluation Mode

You are about to start your evaluation period. Evaluation period is a one time 90 day period in which you will be able to explore your Cisco products full functionality. When evaluation mode ends, you will have to register with the Smart Licensing Cloud to continue to use your product. Do you wish to begin your evaluation period now?

31. Notice that you have 4 different types of licenses: **Base**, **Malware**, **Threat**, and **URL Filtering**. In the Evaluation Mode you get to play with all of them but in the real world you'd only see those which you had purchased.

Figure 32. List of Smart License



Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register

Smart License Status

Usage Authorization: N/A

Product Registration: Evaluation Period (Expires in 89 days)

Assigned Virtual Account: Evaluation Mode

Export-Controlled Features: Disabled

Smart Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Base (0)				
Malware (0)				
Threat (0)				
URL Filtering (0)				

Here is a brief description of the licenses:

Base: A perpetual license that is automatically included. This license covers anything that isn't considered an "optional term license". In other words, it covers everything but that which is discussed (covered) by the following term-based licenses.

Threat: A term-based license that analyzes network traffic for intrusions and exploits. It also has the ability to identify the file type of files being sent through the FTD device, such as documents, executables, PDFs, etc.

Malware: A term-based license that allows file policies to check for malware. This license is required if the use of Advanced Malware Protection (AMP) or AMP Threat Grid is desired.

URL Filtering: A term-based license that allows the use of categories and/or reputation-based URL filtering, such as gambling, social media, or using a "5 star" reputation system to filter URLs.

Scenario Summary

Though you didn’t do anything but set the time zone and enable evaluation mode for licensing there are a lot of configuration/customization to the FMC that could be done. Typical best practices would encourage you to set up email notifications, import a certificate, add various levels of users for access, and probably set up SNMP (which was a page you didn’t even look at).

Since the FMC cannot access the Internet (yet) it could be showing some alert pop-ups from time to time. You will remedy its lack of Internet access in the next few scenarios.

Page intentionally left blank.

Scenario 2. Installing the FTD at the HQ Site

Scenario Description

Now that initial FMC setup is complete, it is time to install the FTD at HQ (called hq-ftd) and add it into the FMC. In this scenario, you will bootstrap the FTD that is installed at the HQ location and then configure it to use the hq-fmc as its manager.

hq-ftd Bootstrap and FMC Integration

All the devices in this lab are virtual devices. As such, there are things you need to ensure are set up in order for the virtual FTD devices to function properly. Though it is beyond the scope of this lab here is one of the key things you need to watch out for:

Security Policy for a vSphere Standard Switch

For a vSphere switch, you can edit Layer 2 security policies and apply security policy exceptions for port groups used by the Firepower Threat Defense Virtual interfaces. The default settings will block correct operation of Firepower Threat Defense Virtual. See the following required settings:

Promiscuous Mode: Accept

MAC Address Changes: Accept

Forged Transmits: Accept

Firepower Threat Defense Virtual uses promiscuous mode to operate, and Firepower Threat Defense Virtual high availability depends on switching the MAC address between the active and the standby to operate correctly. These settings need to be modified to accept each of the parameters shown above by modifying the vSphere switch network properties. See the vSphere documentation for more information.

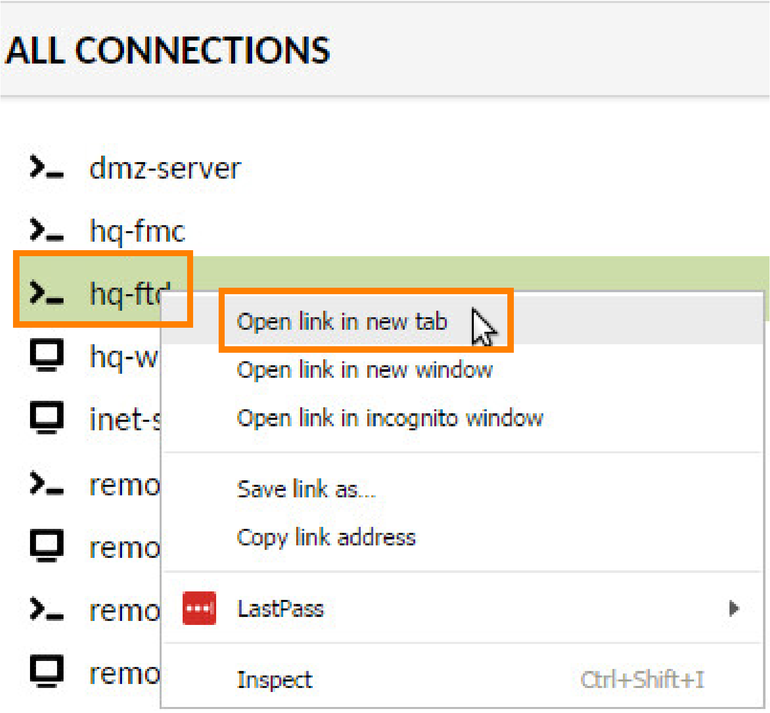
Note: This needs to be done on all networks that are configured for management and failover interfaces on Firepower Threat Defense Virtual sensors.

Since you cannot access the console of the virtual machines within this lab the initial configuration of the management interface of each FTD has already been done for you. The OVA deployment steps are shown in Appendix B.

The hq-ftd device has its management interface pre-configured for you with an IP address (172.16.100.10). This will allow us to access the FTD via SSH from hq-wkst as well as allow this FTD to communicate with hq-fmc.

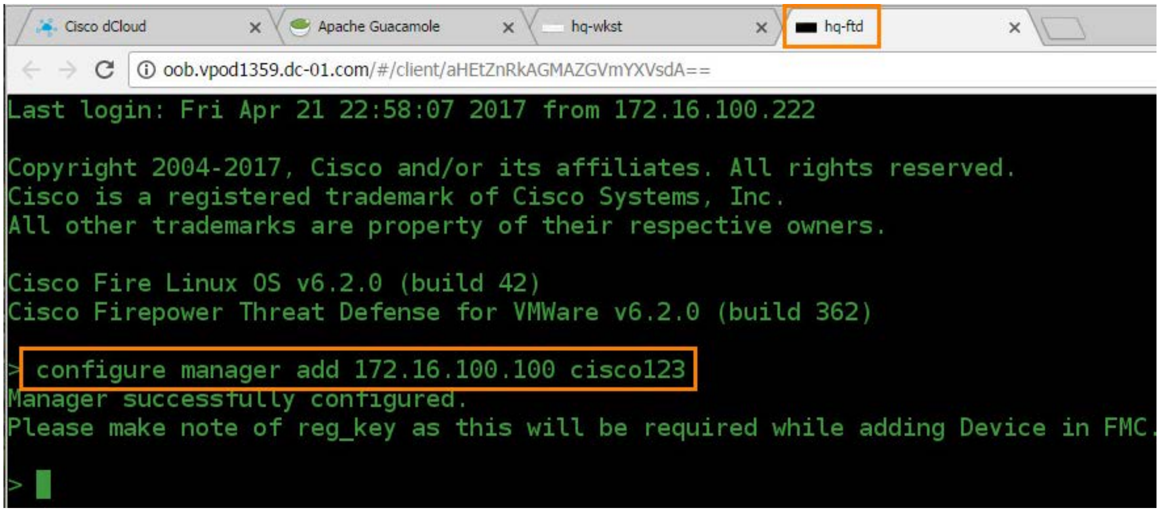
1. From the **oob webpage** open the **hq-ftd** link. This will launch an SSH session to 172.16.100.100 and auto log you in as admin/Admin123.

Figure 33. Open link to hq-ftd



2. To configure hq-ftd to use your recently configured FMC as its manager, issue this command: **configure manager add 172.16.100.100 cisco123**. (The “cisco123” is a pre-shared key and can be any alphanumeric sequence you desire. Remember it as you’ll need it for the FMC side of the configuration.)

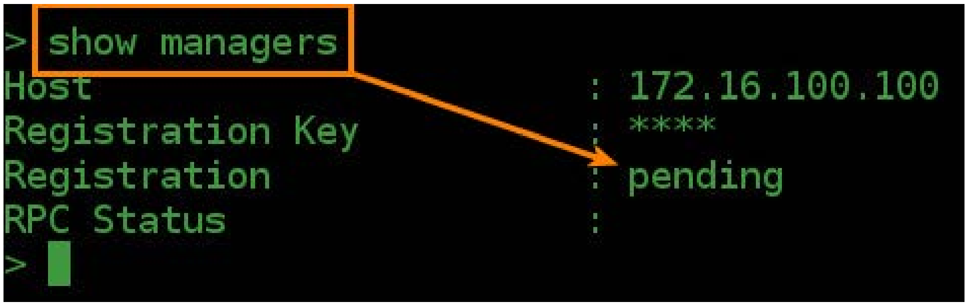
Figure 34. Register FTD to FMC



```
Last login: Fri Apr 21 22:58:07 2017 from 172.16.100.222

Copyright 2004-2017, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.0 (build 42)
Cisco Firepower Threat Defense for VMWare v6.2.0 (build 362)

> configure manager add 172.16.100.100 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

> 
```

3. Issue the command **show managers** to get a status of how the communication between this FTD and its configured FMC manager is going. Since you haven't done anything on the FMC side the Registration status should show "pending".

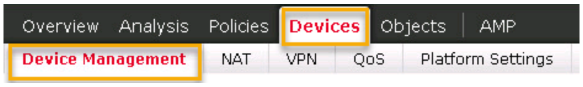
Figure 35. Show managers



```
> show managers
Host                       : 172.16.100.100
Registration Key           : ****
Registration               : pending
RPC Status                 :
> 
```

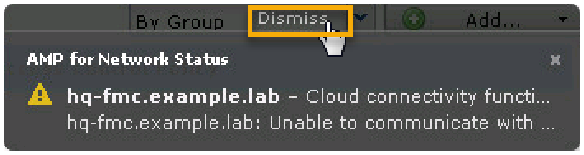
4. Return to hq-wkst. On the FMC management page, to complete the addition of this FTD to the FMC, Navigate to **Devices > Device Management**.

Figure 36. Navigate to Device Management



Note: Sometimes there might be a notification window that covers over the section of the screen you need to access. ALWAYS click Dismiss to remove the notification. If those messages are important you can find them elsewhere. During this lab they are just a nuisance.

Figure 37. Annoying Popup Notification Window.

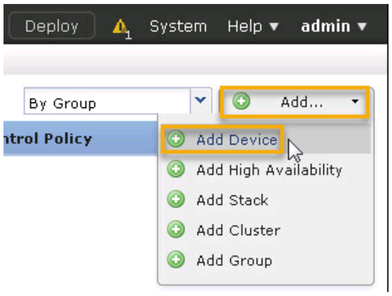


AMP for Network Status

⚠ hq-fmc.example.lab – Cloud connectivity functi...
hq-fmc.example.lab: Unable to communicate with ...

5. Click the **Add…** dropdown button and select **Add Device** from the options. (Though it is beyond the scope of this lab notice all the other types of "devices" that can be managed by the FMC.)

Figure 38. Add a new FTD device



6. In the subsequent popup window fill out the following information:

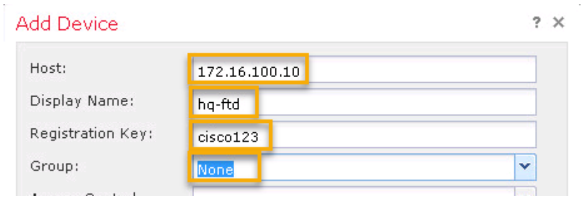
   a. Host: **172.16.100.10** (You could use a DNS name here but you don't have one set up. Also take note that this is the FTD's management IP address and not any of the data interface's IP addresses, which aren't set up yet anyway.)

   b. Display Name: **hq-ftd**

   c. Registration Key: **cisco123**

   d. Group: **None**

Figure 39. Part 1 of adding hq-ftd's information



Add Device

Host: 172.16.100.10

Display Name: hq-ftd

Registration Key: cisco123

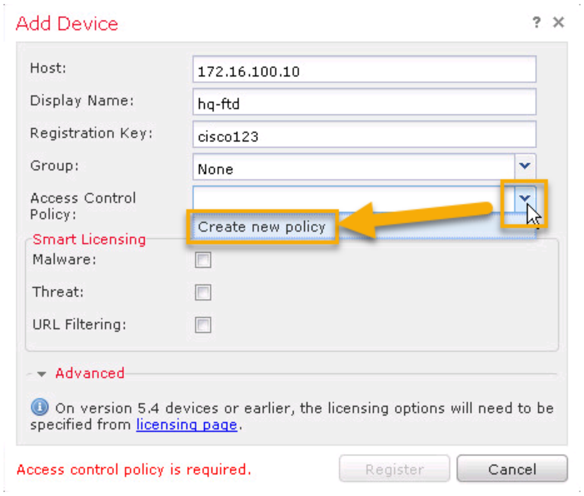
Group: None

The FMC comes with no pre-configured Access Control Policy (you can see that by clicking the down arrow and seeing that the only item listed is to "Create new policy"). For this lab you will create 3 different Access Control Policies. The first one, which you will be creating right now, will be the "base policy" or the common policy which all other policies will refer back to if they don't have a setting specifically defined. Think of this a hierarchy of policies and this one will be the most general. The other 2 polices, one for any FTD at HQ and the other for the remote FTDs, will be children of the base policy.

Note: The use of hierarchical policies is not necessarily a "best practices" method of using Access Control Policies. The intent here is to show off the capabilities of inheritance of policy rules (which will be shown later in the lab). There are many deployments where one Access Control Policy can be used for all FMC managed devices.

7. Access Control Policy: Select the **Create new policy** option from the dropdown menu

Figure 40. Create new ACP



Add Device

Host: 172.16.100.10

Display Name: hq-ftd

Registration Key: cisco123

Group: None

Access Control Policy: Create new policy

Smart Licensing

Malware: □

Threat: □

URL Filtering: □

Advanced

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

Access control policy is required.

8. Use the following to fill out the New Policy window's options:

   a. Name: **Base Policy**

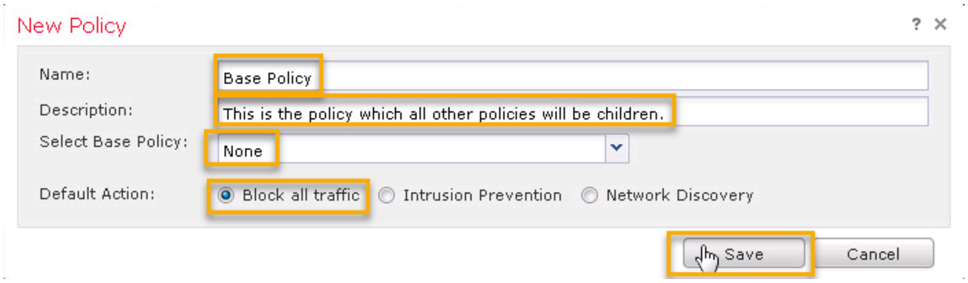
   b. Description: **This is the policy which all other policies will be children.**

   c. Select Base Policy: **None**

   d. Default Action: **Block all traffic**

   e. Click **Save**.

Figure 41. Creating new ACP



New Policy

Name: Base Policy

Description: This is the policy which all other policies will be children.

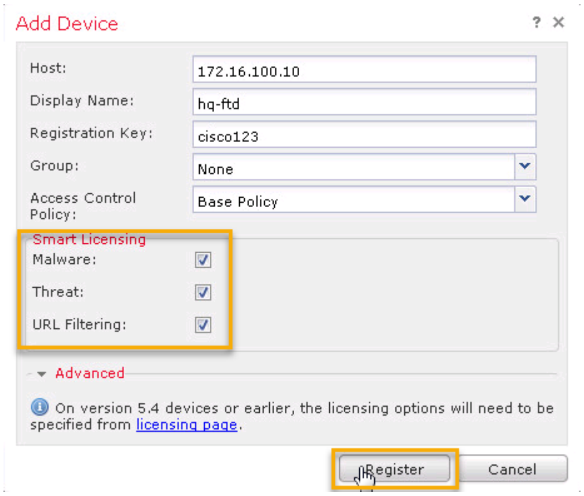
Select Base Policy: None

Default Action: ● Block all traffic ○ Intrusion Prevention ○ Network Discovery

9. Smart Licensing: The evaluation mode gives us access to all the licensable options. **Check all the boxes** (Malware, Threat, and URL Filtering).

10. Click **Register**. The registration process can take a minute or two.

Figure 42. Enable all the licenses and click Register



Add Device

Host: 172.16.100.10

Display Name: hq-ftd

Registration Key: cisco123

Group: None

Access Control Policy: Base Policy

Smart Licensing

Malware: ☑

Threat: ☑

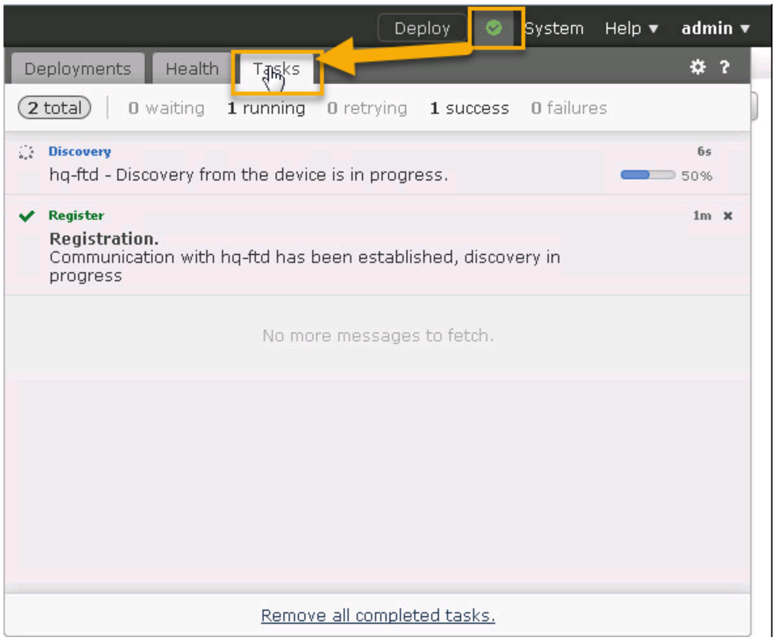
URL Filtering: ☑

Advanced

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

11. There is an icon just to the right of the Deploy button. It could be a red circle, a yellow triangle, or a green circle depending on the state of the FMC device. This is called the Message Center. More than likely it is a red circle right now though. Click on the **Message Center icon** and a popup window will appear with 3 tabs: Deployments, Health, and Tasks. Once the hq-ftd device has been successfully deployed it will show a green checkmark next to its name on the Deployments tab. To watch the progression, click on the **Tasks tab**.

Figure 43. The Message Center icon with tabs



2 total | 0 waiting 1 running 0 retrying 1 success 0 failures

Discovery 6s
hq-ftd - Discovery from the device is in progress. 50%

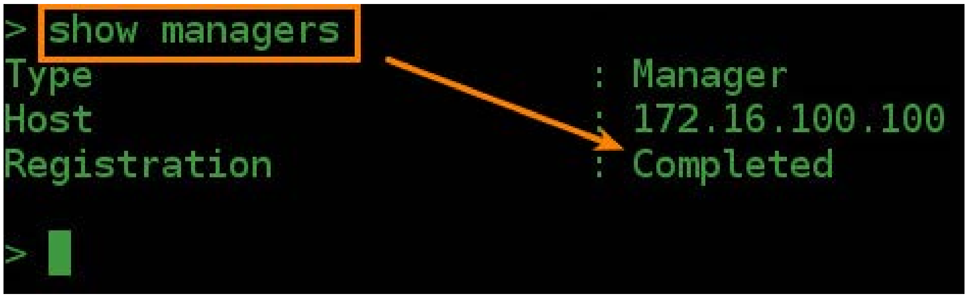
✓ Register 1m ✖
Registration.
Communication with hq-ftd has been established, discovery in progress

No more messages to fetch.

Remove all completed tasks.

12. The registration process takes about 3-5 minutes. Once the hq-ftd device appears on the Device Management page return to the **SSH tab** to **hq-ftd** and issue the command **show managers** again. Notice that the Registration status now shows Completed.

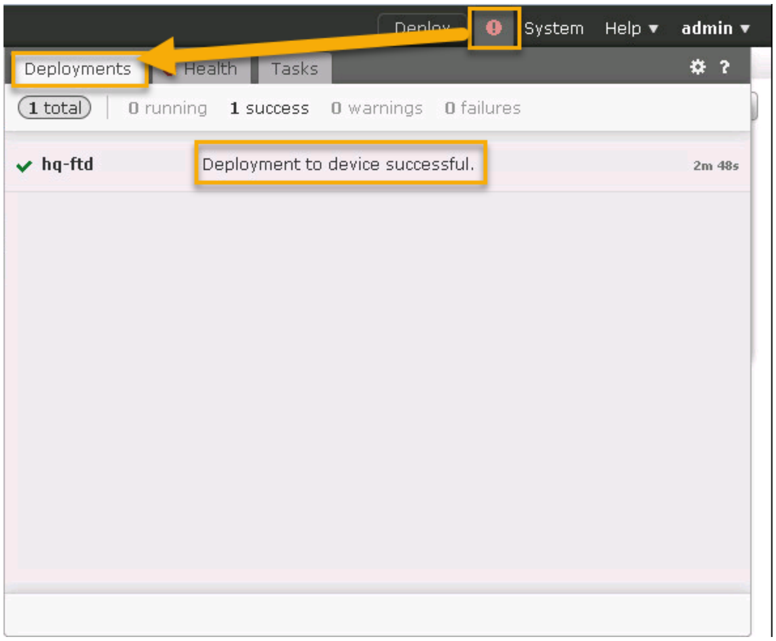
Figure 44. Show managers, again



```
> show managers
Type                    : Manager
Host                    : 172.16.100.100
Registration            : Completed

> 
```

13. In the FMC administration website click on the **Message Center** and then on the **Deployments tab**. Don’t proceed with the lab until the hq-ftd shows up on here with a green checkmark next to its name.

Figure 45. Message Center Deployment shows completed.



1 total | 0 running 1 success 0 warnings 0 failures

✓ hq-ftd Deployment to device successful. 2m 48s

The most common reason for a registration to fail is an incorrect IP address and/or mistyped shared secret. If your registration fails double check your information and try again.

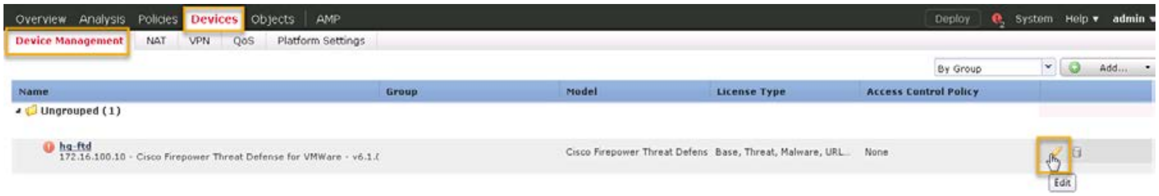
hq-ftd Data Interfaces Configuration

Now that the hq-ftd is being configured by the FMC it is time to start setting up the data interfaces on the hq-ftd device.

14. In case you browsed away, navigate to **Devices > Device Management**.

15. Once the hq-ftd device is available within the FMC click the **pencil icon** on the row associated with **hq-ftd**.

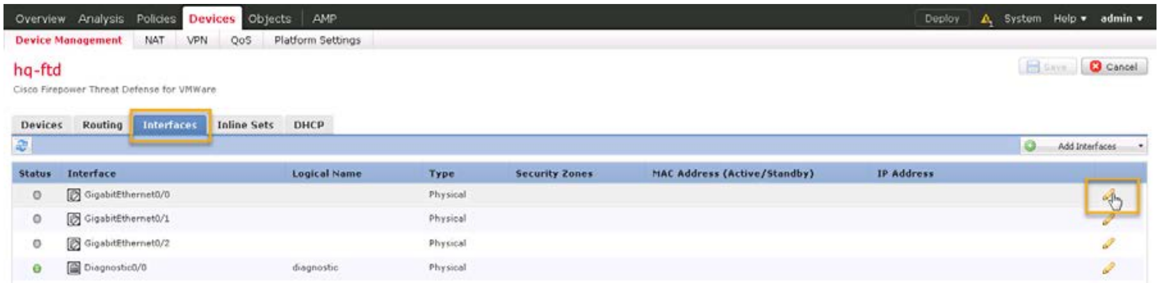
Figure 46. Edit hq-ftd



Name	Group	Model	License Type	Access Control Policy
Ungrouped (1)				
hq-ftd 172.16.100.10 - Cisco Firepower Threat Defense for VMWare - v6.1.(		Cisco Firepower Threat Defens	Base, Threat, Malware, URL...	None

16. This should take you to the **Interfaces tab** that lists all the available interfaces that can be used for user data packets. Take note that the interface configured as the “Management Interface” does NOT appear in this list. In this lab GigabitEthernet0/0 is connected to the HQ LAN (inside), GigabitEthernet0/1 is connected to the ISP (outside), and GigabitEthernet0/2 is connected to the DMZ (dmz). Click the **pencil icon** on the row for **GigabitEthernet0/0**.

Figure 47. Edit g0/0



hq-ftd

Cisco Firepower Threat Defense for VMWare

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
○	GigabitEthernet0/0		Physical			
○	GigabitEthernet0/1		Physical			
○	GigabitEthernet0/2		Physical			
●	Diagnostic0/0	diagnostic	Physical			

NOTE: Make sure that there are **Save** and **Cancel** buttons in the top right corner of the web page.
This is an ongoing problem that appears to be sensitive to which browser (and which version of browser) you are using. This lab, at the time of writing, has the most up-to-date version of Firefox installed (which was the recommended version). The only way I know to solve this issue is to navigate way from the current page by clicking on a totally different topic (say, NAT in the above screenshot) an the navigate back to where I was. Sometimes, holding SHIFT and clicking the Refresh button on the page will fix it too. You will lose any changes you’ve made on this page but you couldn’t of saved them anyway.

17. Use the following information to fill out the popup window:

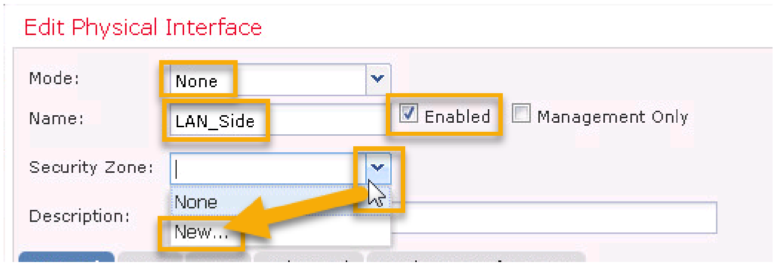
    a. Mode: **None**

    b. Name: **LAN_Side** (This could be anything descriptive. I chose to NOT call it Inside so as to not confuse with the Inside zone you are about to create.)

    c. Check the **Enabled** box.

    d. Security Zone: From the dropdown options select **New…**

Figure 48. Part 1 of editing g0/0



Edit Physical Interface

Mode: None

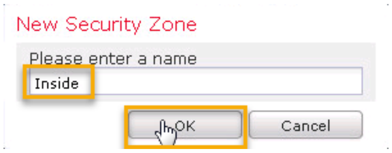
Name: LAN_Side ☑ Enabled □ Management Only

Security Zone:

Description:

18. Create the new zone called **Inside** and click **OK**.

Figure 49. Create Inside Zone



New Security Zone

Please enter a name

Inside

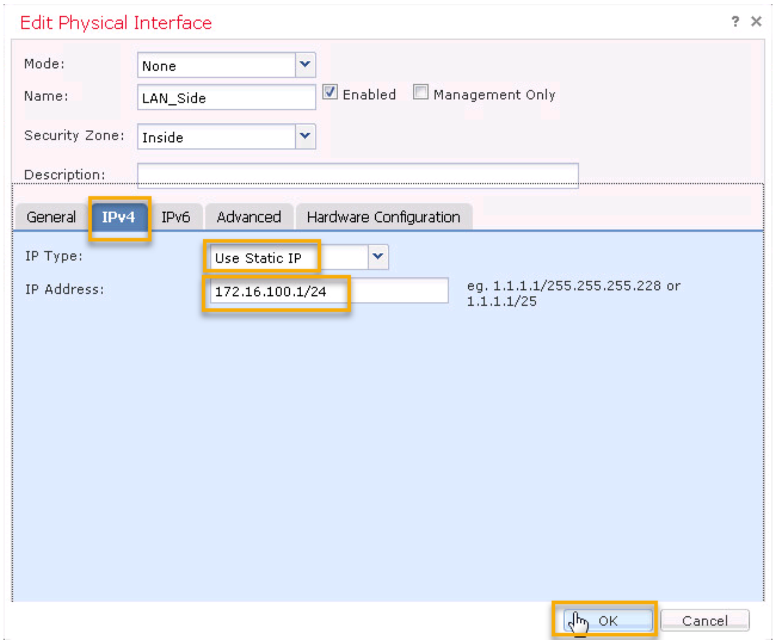
19. Click the **IPv4 tab**.

   a. IP Type: **Use Static IP**

   b. IP Address: **172.16.100.1/24**

20. Click **OK**.

Figure 50. Configure Data Plane IP and click OK



Edit Physical Interface

Mode: None

Name: LAN_Side ☑ Enabled □ Management Only

Security Zone: Inside

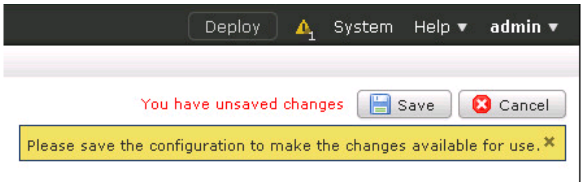
Description:

IP Type: Use Static IP

IP Address: 172.16.100.1/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

Notice the yellow text that now appears near the Save button. This is just a warning that you haven't saved these changes to the FMC, nor have these changes been pushed out to hq-ftd. Changes are cached locally in the browser until they are saved to the FMC. Then those changes will need to be deployed from the FMC to the selected devices. You will see more of this process throughout this lab.

Figure 51. Yellow Warning

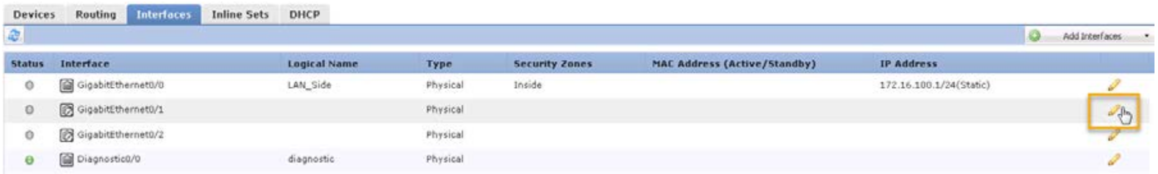


You have unsaved changes

Please save the configuration to make the changes available for use.

21. Click the **pencil icon** on the row for **GigabitEthernet0/1**.

Figure 52. Edit g0/1



Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0	LAN_Side	Physical	Inside		172.16.100.1/24(Static)
	GigabitEthernet0/1		Physical			
	GigabitEthernet0/2		Physical			
	Diagnostic0/0	diagnostic	Physical			

22. Use the following to fill out the popup window:

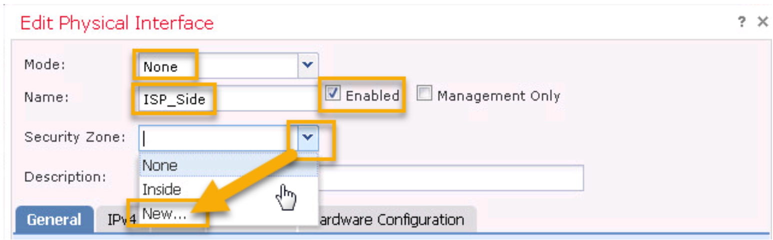
    a. Mode: **None**

    b. Name: **ISP_Side**

    c. Check the **Enabled** box.

    d. Security Zone: From the dropdown options select **New…**

Figure 53. Part 1 of editing g0/1


Edit Physical Interface

Mode: None

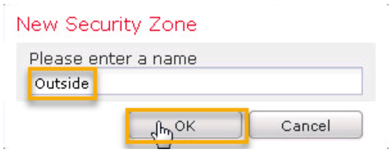
Name: ISP_Side ☑ Enabled □ Management Only

Security Zone:

Description:

23. Create the zoned named **Outside** and click **OK**.

Figure 54. Create Outside zone


New Security Zone

Please enter a name

Outside

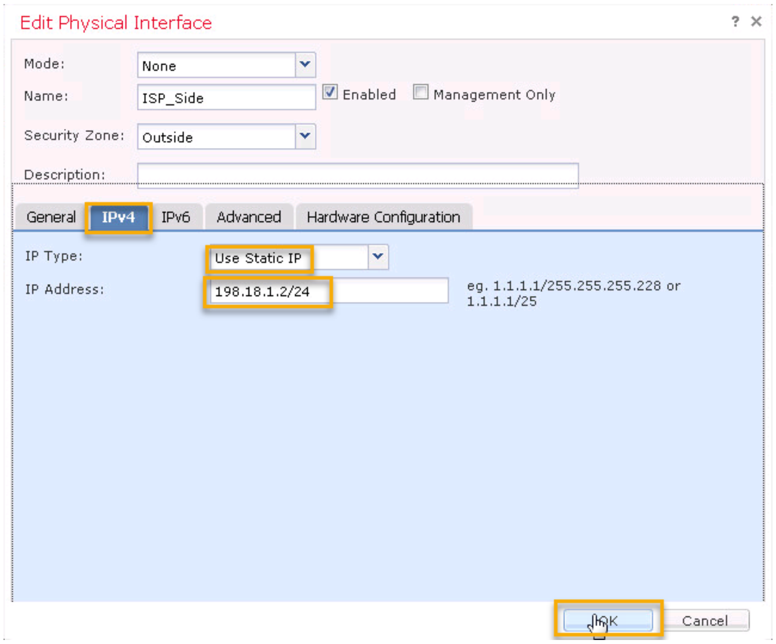
24. Click the **IPv4 tab**.

    a. IP Type: **Use Static IP**

    b. IP Address: **198.18.1.2/24**

25. Click **OK**.

Figure 55. Configure g0/1 IP and click OK



Edit Physical Interface

Mode: None

Name: ISP_Side ☑ Enabled □ Management Only

Security Zone: Outside

Description:

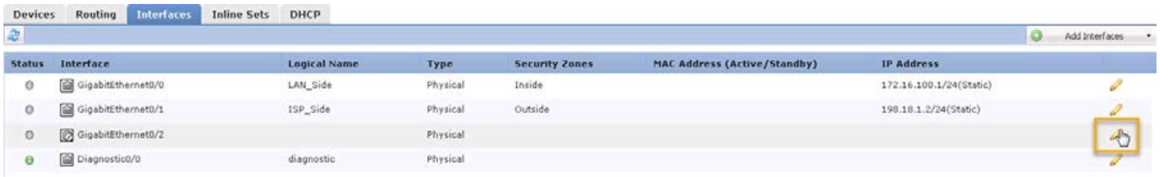
General | IPv4 | IPv6 | Advanced | Hardware Configuration

IP Type: Use Static IP

IP Address: 198.18.1.2/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

26. Click the **pencil icon** on the row for **GigabitEthernet0/2**.

Figure 56. Edit g0/2



Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
○	GigabitEthernet0/0	LAN_Side	Physical	Inside		172.16.100.1/24(Static)
○	GigabitEthernet0/1	ISP_Side	Physical	Outside		198.18.1.2/24(Static)
○	GigabitEthernet0/2		Physical			
●	Diagnostic0/0	diagnostic	Physical			

27. Use the following to fill out the popup window:

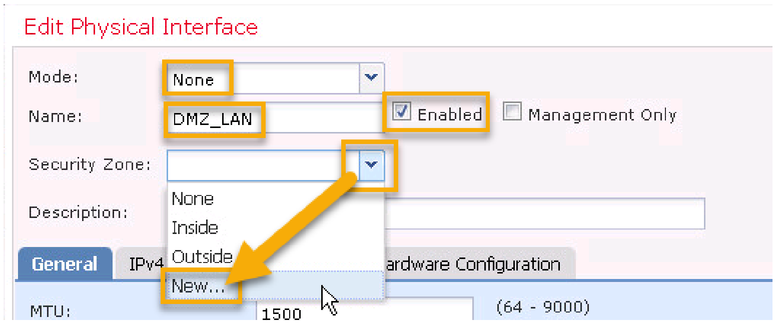
    a. Mode: **None**

    b. Name: **DMZ_LAN**

    c. Check the **Enabled** box.

    d. Security Zone: From the dropdown options select **New…**

Figure 57. Part 1 of configuring g0/2



Edit Physical Interface

Mode: None

Name: DMZ_LAN ☑ Enabled □ Management Only

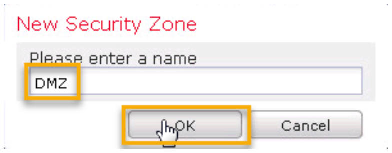
Security Zone:

Description:

MTU: 1500 (64 - 9000)

28. Create the zone named **DMZ** and click **OK**.

Figure 58. Create DMZ zone



New Security Zone

Please enter a name

DMZ

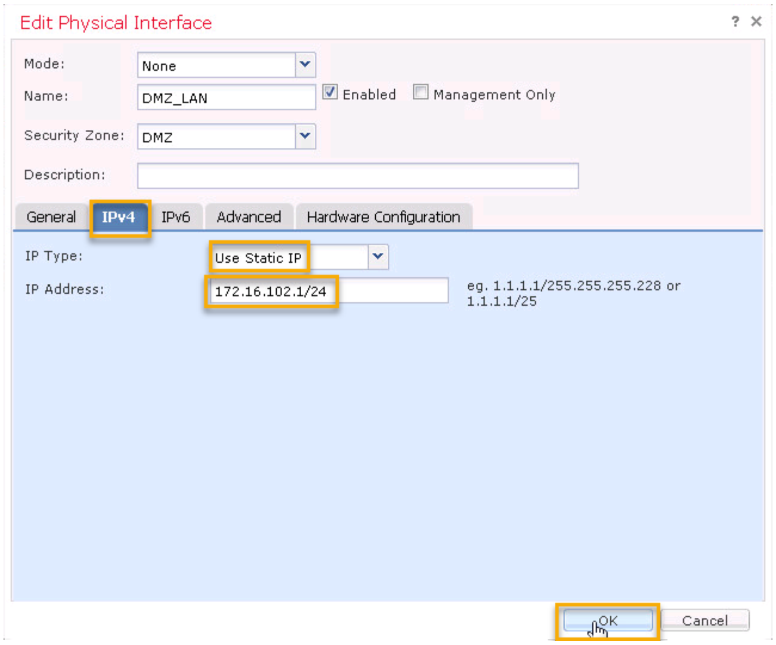
29. Click the **IPv4 tab**.

    a. IP Type: **Use Static IP**

    b. IP Address: **172.16.102.1/24**

30. Click **OK**.

Figure 59. Add g0/2 IP and click OK



Edit Physical Interface

Mode: None

Name: DMZ_LAN ☑ Enabled ☐ Management Only

Security Zone: DMZ

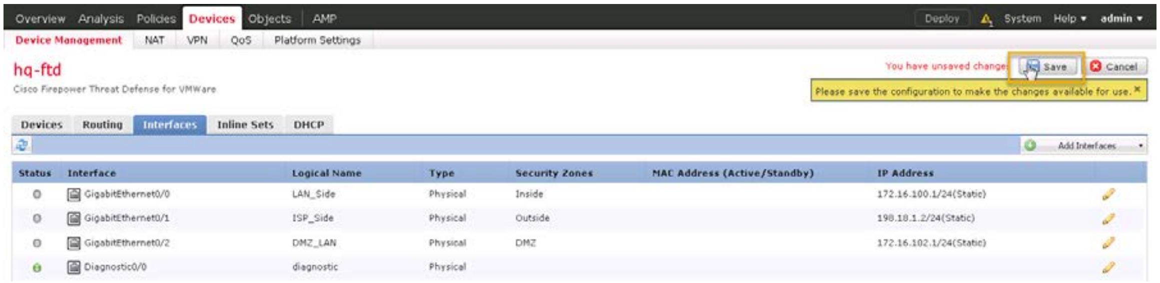
Description:

IP Type: Use Static IP

IP Address: 172.16.102.1/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

31. Double check your work against the next screenshot and then click **Save** in the upper right corner of the GUI. If you don’t do this now, then the newly created interface names and the security zones won’t be accessible in other parts of the GUI.

Figure 60. Hq-ftd interfaces configured



hq-ftd

Cisco Firepower Threat Defense for VMWare

You have unsaved change

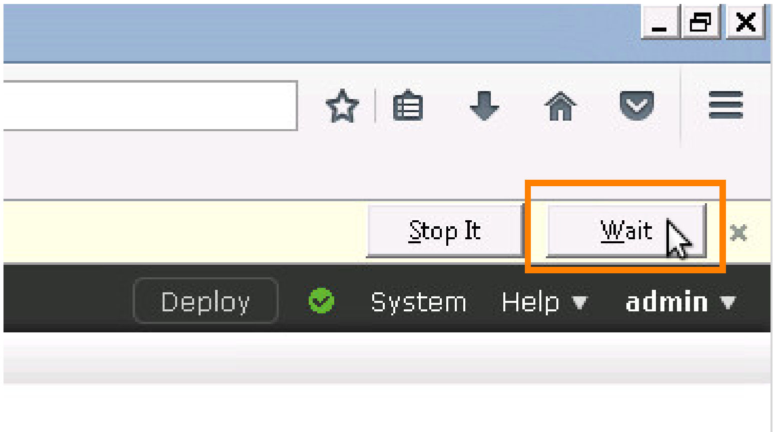
Please save the configuration to make the changes available for use.

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
○	GigabitEthernet0/0	LAN_Side	Physical	Inside		172.16.100.1/24(Static)
○	GigabitEthernet0/1	ISP_Side	Physical	Outside		198.18.1.2/24(Static)
○	GigabitEthernet0/2	DMZ_LAN	Physical	DMZ		172.16.102.1/24(Static)
●	Diagnostic0/0	diagnostic	Physical			

32. Click the **Routing tab**.

It is possible that you'll get the an error saying that the web page it taking too long when you click the Routing tab. This error appears to be an issue only seen in a virtualized FMC within the lab. It may occur on occasion. Please just click **Wait** to remove the message.

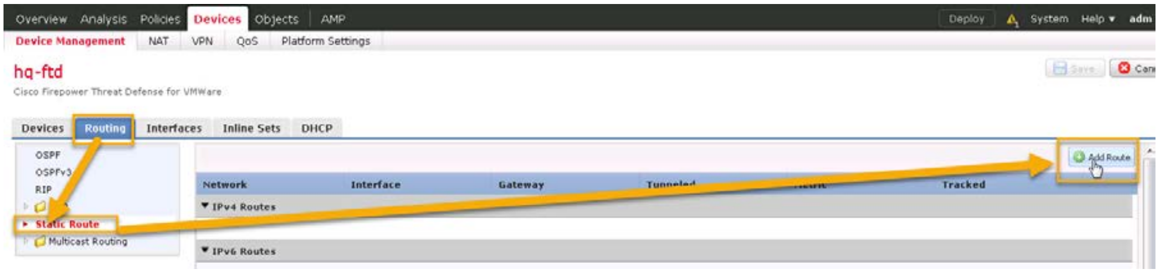
Figure 61. Possible error when clicking routing tab



33. As you can see you have several dynamic routing protocols that you can configure. Being that this network is simple you only need to set a static default route. Click on the **Static Route** menu option.

34. Click the **Add Route** button on the right side of the web page.

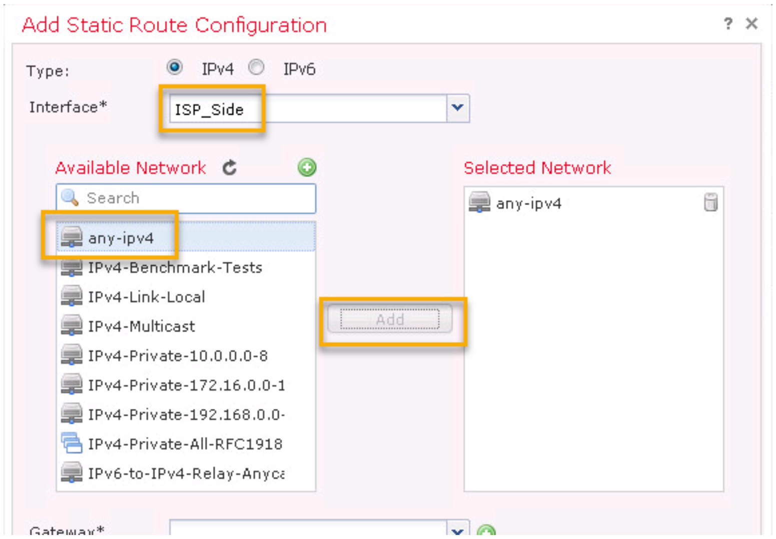
Figure 62. Add Static Route



35. Using the dropdown for the **Interface** option select **ISP_Side**.

36. From the **Available Networks list** of items select the **any-ipv4** option and then click the **Add** button to move it to the Selected Network list. This is equivalent to the 0.0.0.0/0 network.

Figure 63. Part 1 of adding static route



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface* ISP_Side

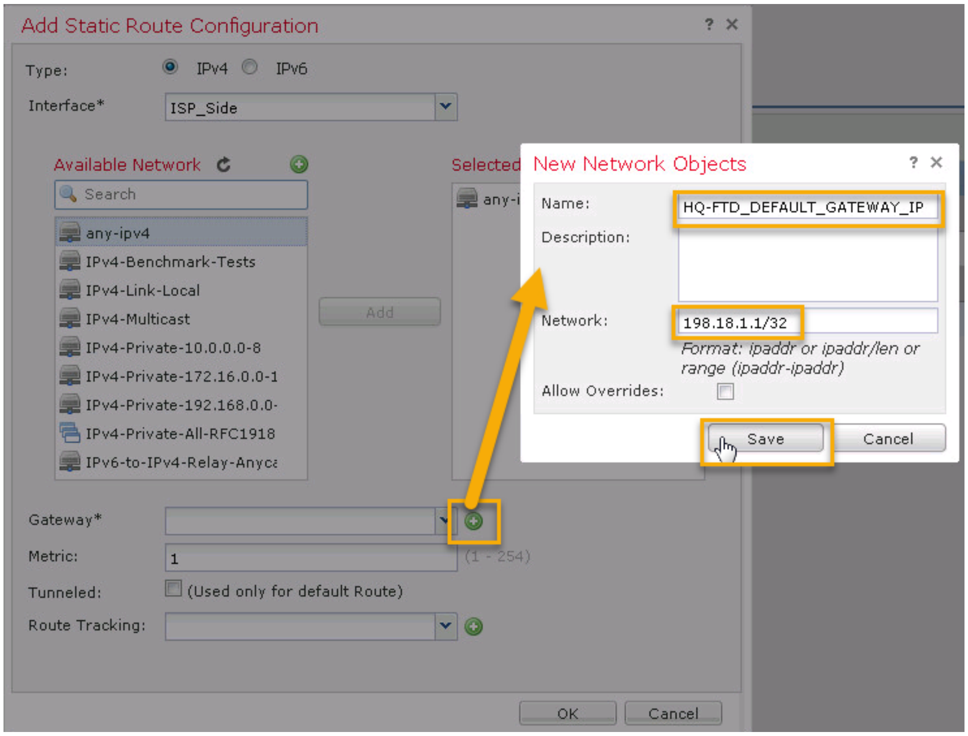
37. For the Gateway option you have 3 options: you could just type in the IP address for the ISP's next hop for the HQ outside network, you could use the dropdown to select an already created gateway (which you have none at this moment), or you could create a new Network Object by clicking the green plus icon. Though in this lab you will only have a few devices within this FMC it helps identify what an IP is by giving it a name. So, that said, click the **green plus icon** and let's create a Network Object and use the following to fill out the New Network Object popup window:

    a. Name: **HQ-FTD_DEFAULT_GATEWAY_IP** (Spaces are not permitted in this field so use underscores "_" instead.)

    b. Network: **198.18.1.1/32**

    c. Click **Save**.

Figure 64. Adding Network Object



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: ISP_Side

New Network Objects

Name: HQ-FTD_DEFAULT_GATEWAY_IP

Description:

Network: 198.18.1.1/32

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides: □

Gateway*:

Metric: 1 (1 - 254)

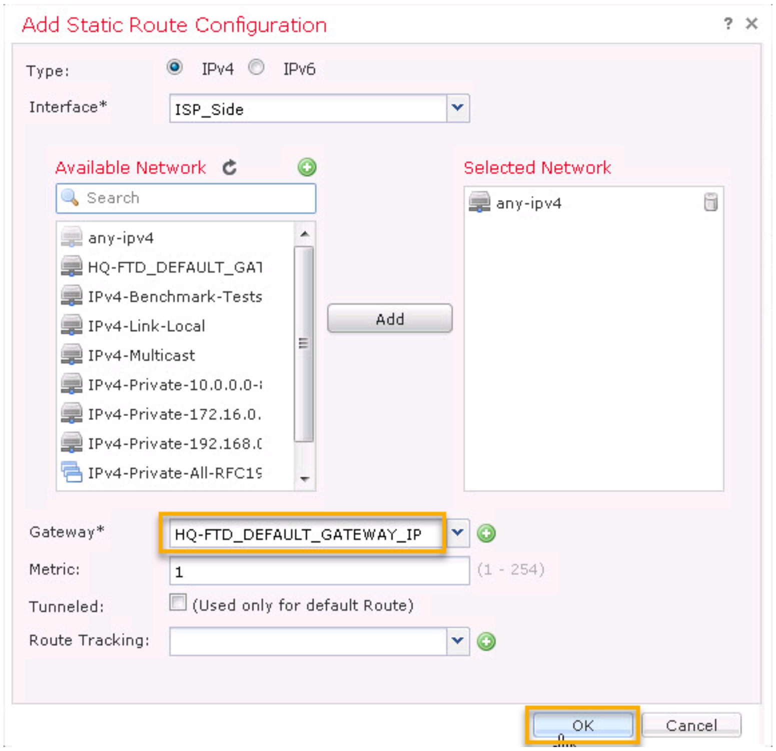
Tunneled: □ (Used only for default Route)

Route Tracking:

38. Now from the dropdown menu for the **Gateway option** select the newly created Network Object **HQ-FTD_DEFAULT_GATEWAY_IP**.

39. Click **OK** to add the static route.

Figure 65. Finish adding static route



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface* ISP_Side

Selected Network: any-ipv4

Gateway* HQ-FTD_DEFAULT_GATEWAY_IP

Metric: 1 (1 - 254)

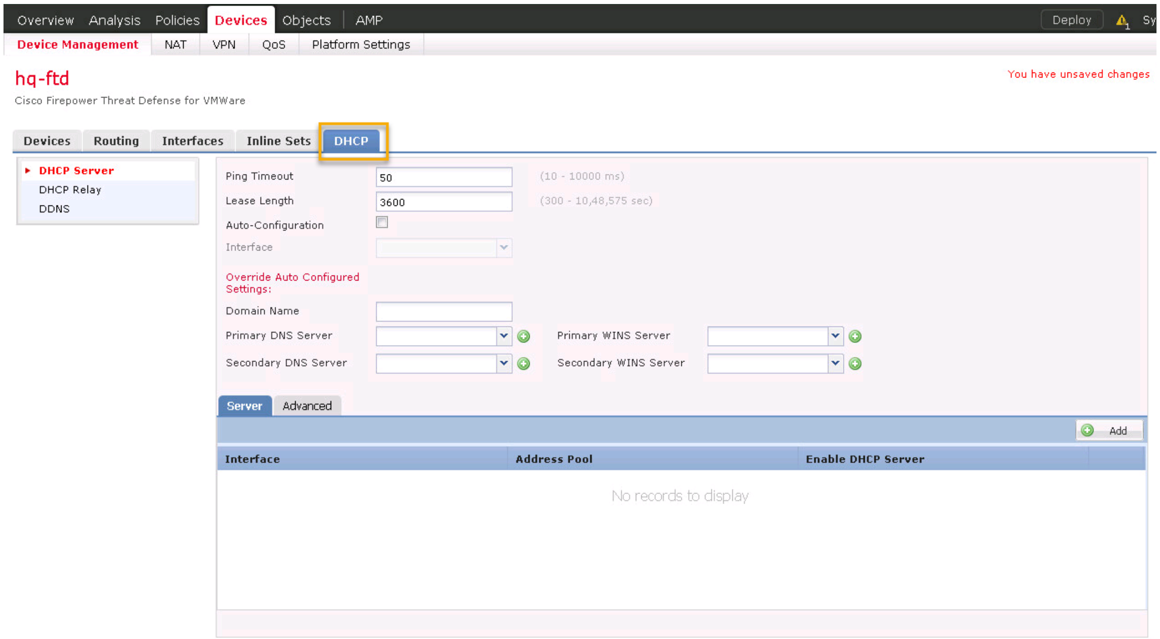
Tunneled: □ (Used only for default Route)

Route Tracking:

40. Click the **DHCP tab**.

41. You don't need DHCP in this lab but here is where you could set up this FTD to either relay DHCP request or be a DHCP server itself.

Figure 66. Where to set up DHCP, if needed



Ping Timeout	50	(10 - 10000 ms)
Lease Length	3600	(300 - 10,48,575 sec)
Auto-Configuration	☐	
Interface		

Override Auto Configured Settings:

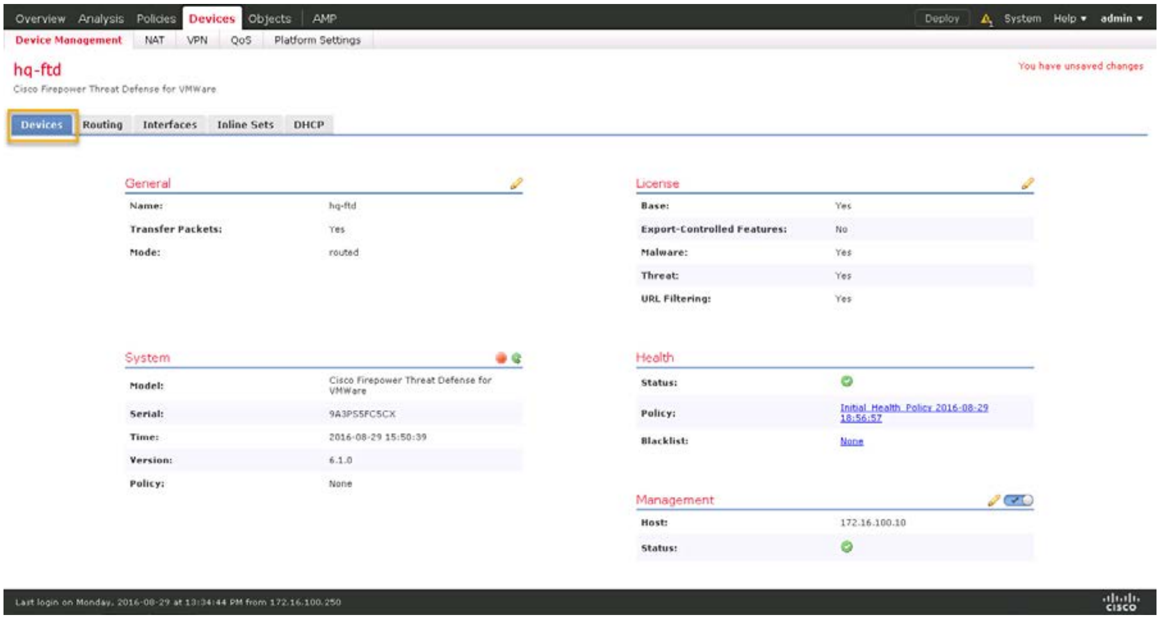
Domain Name			
Primary DNS Server		Primary WINS Server	
Secondary DNS Server		Secondary WINS Server	

Interface	Address Pool	Enable DHCP Server

42. Click the **Devices tab**.

43. The changes that can be made on this page are akin to what the setup wizard performed via the CLI with a few more options. You can change the Management interface's IP address, Shutdown or Restart this device, and even change the licensing of this device.

Figure 67. Devices Tab Info



hq-ftd

Cisco Firepower Threat Defense for VMWare

You have unsaved changes

General

Name: hq-ftd

Transfer Packets: Yes

Mode: routed

License

Base: Yes

Export-Controlled Features: No

Malware: Yes

Threat: Yes

URL Filtering: Yes

System

Model: Cisco Firepower Threat Defense for VMWare

Serial: 9A3PS5FC5CX

Time: 2016-08-29 15:50:39

Version: 6.1.0

Policy: None

Health

Status: ✓

Policy: Initial_Health_Policy 2016-08-29 18:56:57

Blacklist: None

Management

Host: 172.16.100.10

Status: ✓

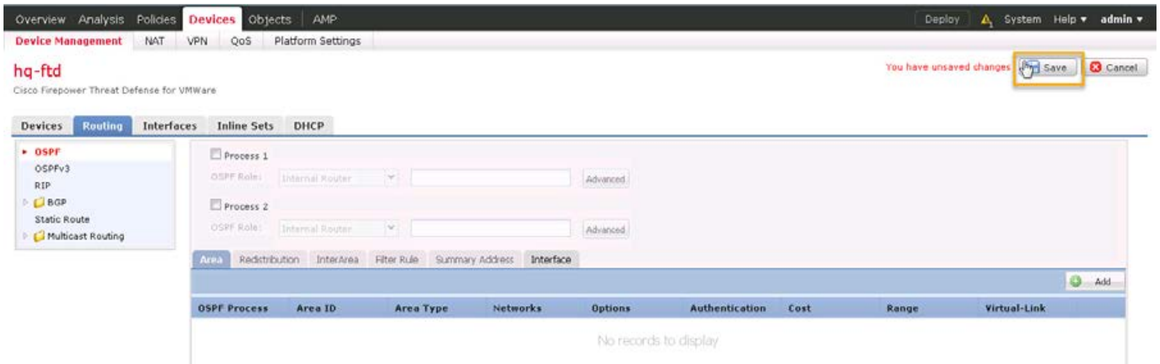
Last login on Monday, 2016-08-29 at 13:34:44 PM from 172.16.100.250

Note: To change an FTD's firewall mode (routed vs. transparent) would require the de-registration of the device from the FMC, changing the mode at the CLI of the FTD, and then re-registering that device with the FMC. This will remove all data plane configuration on that FTD device and it would need to be reprogrammed via the FMC.

44. Now that the data interfaces have IP addresses, and routing is configured it is time to save your changes. Click the **Save** button in the upper-right region of the web page.

Unfortunately, the Save button doesn't appear on every page so if you don't see it click on the **Routing tab** to refresh the screen and populate the **Save** button.

Figure 68. Save your changes



hq-ftd

Cisco Firepower Threat Defense for VMWare

You have unsaved changes

□ Process 1

OSPF Role: Internal Router

□ Process 2

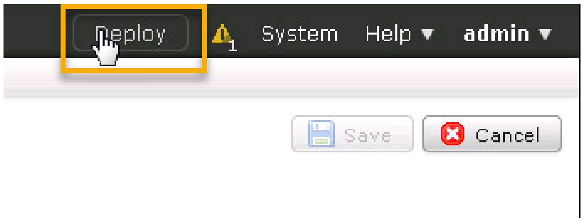
OSPF Role: Internal Router

OSPF Process	Area ID	Area Type	Networks	Options	Authentication	Cost	Range	Virtual-Link

No records to display

45. Though the changes you have made are saved to the FMC they have not been sent to the hq-ftd device yet. You use the Deploy button in the upper-right region of the web page to deploy configurations to the devices the FMC manages. Click the **Deploy** button now.

Figure 69. The Deploy Button



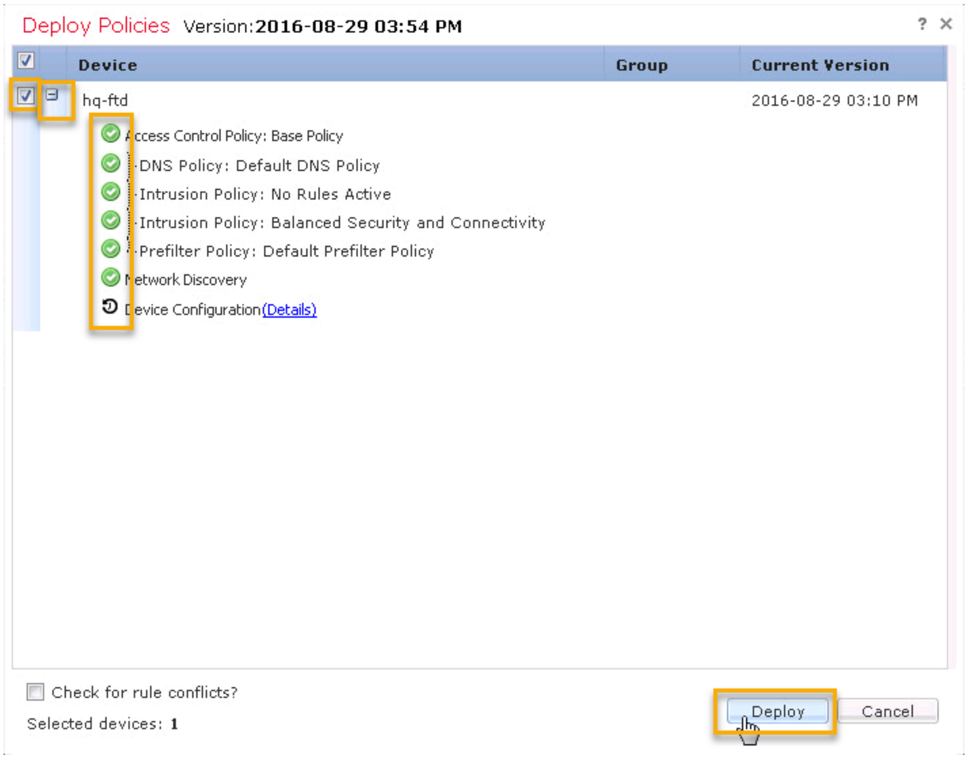
46. Only those devices that could be affected by the changes that have been made will be listed here. In your case you only have 1 device so that is obvious BUT in the real world where you might have 100s or 1000s of devices this is a handy feature so that you don’t have to sift through tons of devices to find the 1 or few that you want to push the changes to. That said, in many cases you’ll want to apply the changes to all the devices listed because you want to maintain a consistent ruleset across all the devices within the environment. (There is always the exception to the rule but in general you deploy your changes to all the devices listed.)

47. Check the box next to **hq-ftd**.

48. Click the **plus icon** next to the device's name. Though not highly informative, this listing of items shows what items will be affected/changed by this deployment. Those items with a green checkmark are currently up-to-date and won't be affected whereas those items with a black circular arrow will be affected.

49. Click **Deploy** to push the changes out to the selected device(s).

Figure 70. Push changes to hq-ftd



Deploy Policies Version:**2016-08-29 03:54 PM**

☑	Device	Group	Current Version
☑ ⊟	hq-ftd		2016-08-29 03:10 PM

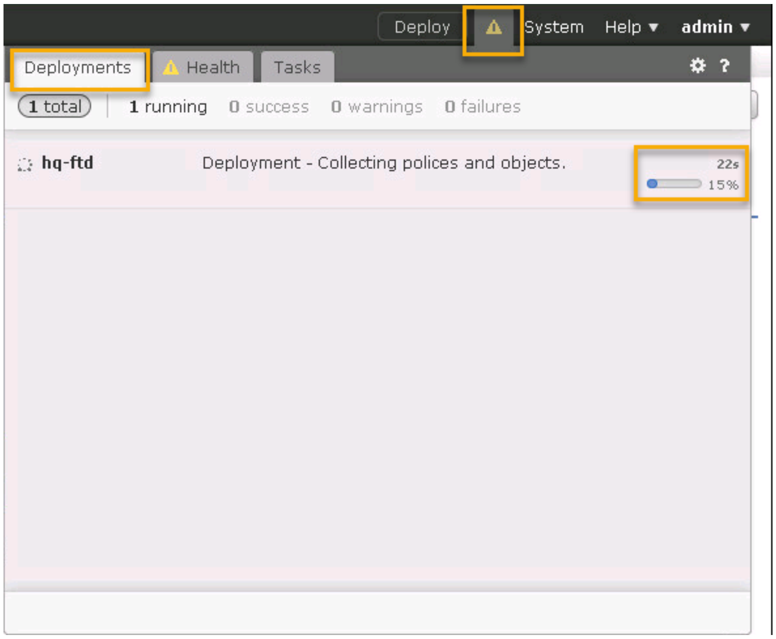
- ✓ Access Control Policy: Base Policy
- ✓ DNS Policy: Default DNS Policy
- ✓ Intrusion Policy: No Rules Active
- ✓ Intrusion Policy: Balanced Security and Connectivity
- ✓ Prefilter Policy: Default Prefilter Policy
- ✓ Network Discovery
- ↻ Device Configuration(Details)

□ Check for rule conflicts?

Selected devices: **1**

50. Click on the **Message Center icon** and wait until the deployment of the changes to hq-ftd are complete before continuing the lab. The deployment will take 1-2 minutes. Sometimes within this lab you will issue some show commands (or issue some sort of test, such as ping) prior to and the after deploying some sort of configuration. You can see when the changes have been deployed here to know when you should start testing the post-deployment step of that scenario.

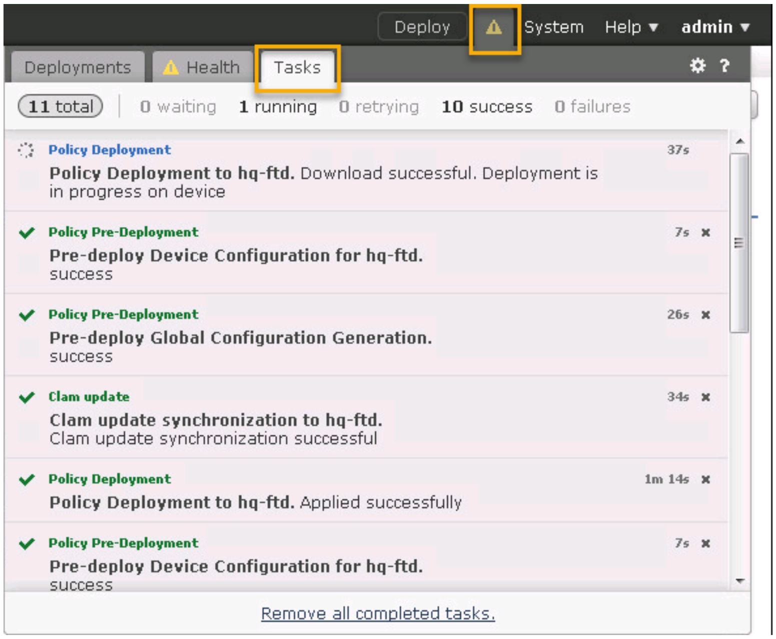
Figure 71. Deploying changes



1 total | 1 running 0 success 0 warnings 0 failures

hq-ftd Deployment - Collecting polices and objects. 22s 15%

Figure 72. Details of changes being made



11 total | 0 waiting 1 running 0 retrying 10 success 0 failures

Policy Deployment 37s
Policy Deployment to hq-ftd. Download successful. Deployment is in progress on device

✓ Policy Pre-Deployment 7s ✖
Pre-deploy Device Configuration for hq-ftd.
success

✓ Policy Pre-Deployment 26s ✖
Pre-deploy Global Configuration Generation.
success

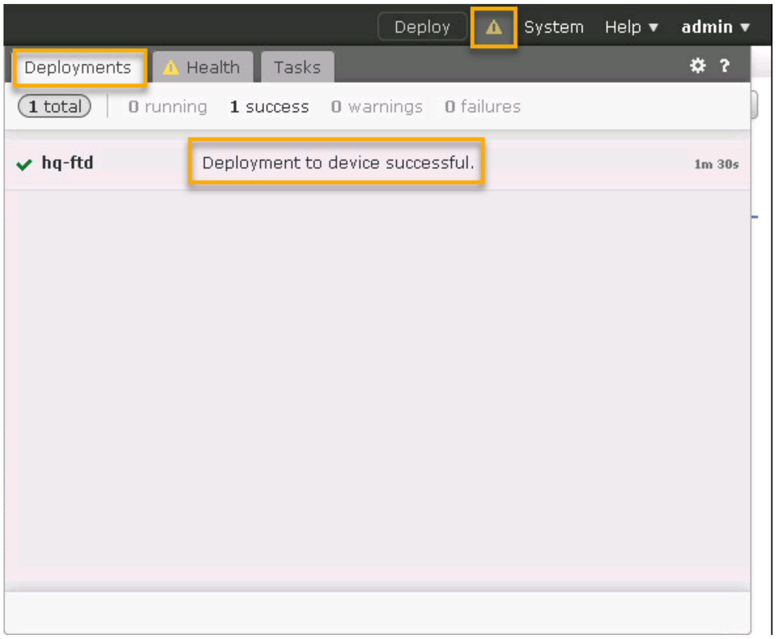
✓ Clam update 34s ✖
Clam update synchronization to hq-ftd.
Clam update synchronization successful

✓ Policy Deployment 1m 14s ✖
Policy Deployment to hq-ftd. Applied successfully

✓ Policy Pre-Deployment 7s ✖
Pre-deploy Device Configuration for hq-ftd.
success

Remove all completed tasks.

Figure 73. Changes are done deploying



✓ hq-ftd Deployment to device successful. 1m 30s

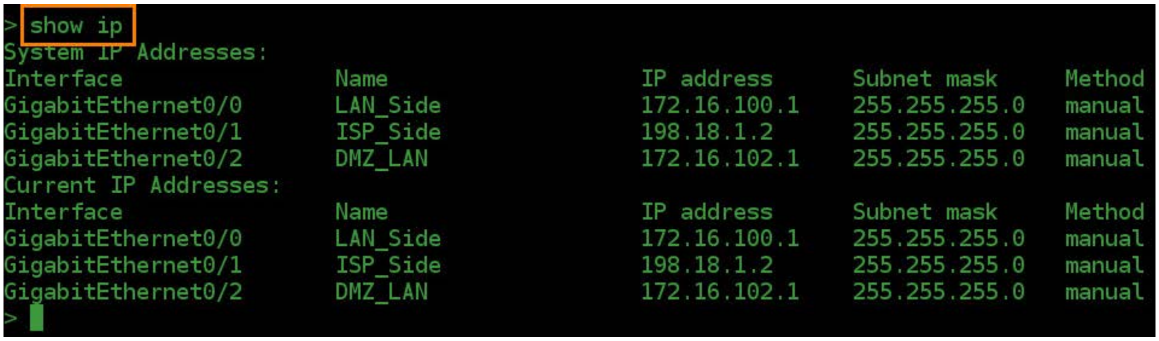
Do not continue until the status of the deployment shows that it has been completed successfully.

Testing hq-ftd Data Interfaces Configuration

51. Return to the SSH tab connected to **hq-ftd**.

52. Issue the command **show ip** to see a list of the interfaces and what IP addresses they are assigned to each interface.

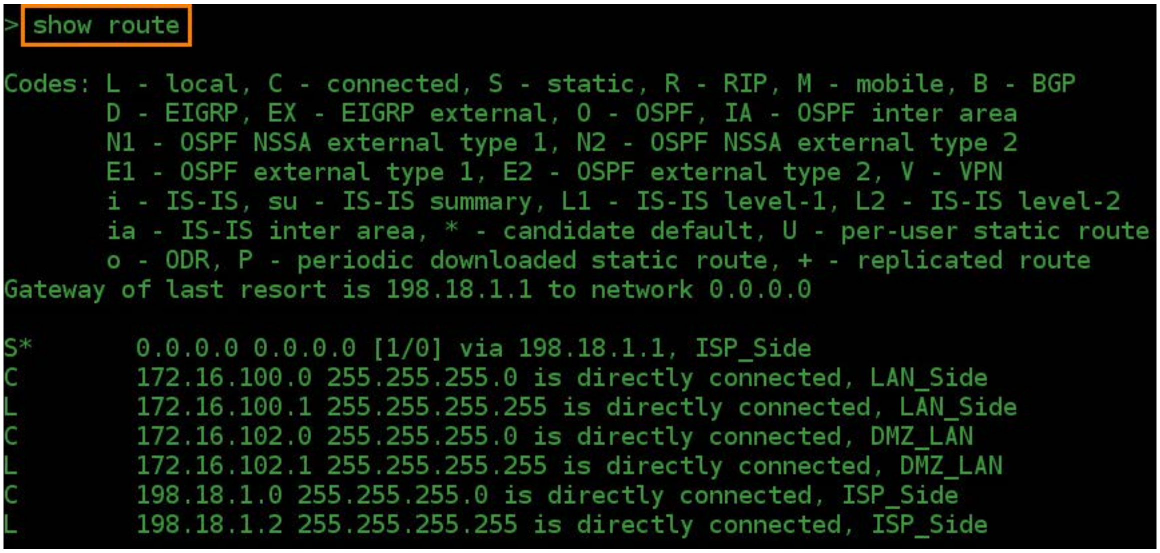
Figure 74. Show ip



```
> show ip
System IP Addresses:
Interface                Name                     IP address      Subnet mask     Method
GigabitEthernet0/0       LAN_Side                 172.16.100.1    255.255.255.0   manual
GigabitEthernet0/1       ISP_Side                 198.18.1.2      255.255.255.0   manual
GigabitEthernet0/2       DMZ_LAN                  172.16.102.1    255.255.255.0   manual
Current IP Addresses:
Interface                Name                     IP address      Subnet mask     Method
GigabitEthernet0/0       LAN_Side                 172.16.100.1    255.255.255.0   manual
GigabitEthernet0/1       ISP_Side                 198.18.1.2      255.255.255.0   manual
GigabitEthernet0/2       DMZ_LAN                  172.16.102.1    255.255.255.0   manual
>
```

53. Issue the command **show route** to see the data path’s routing table.

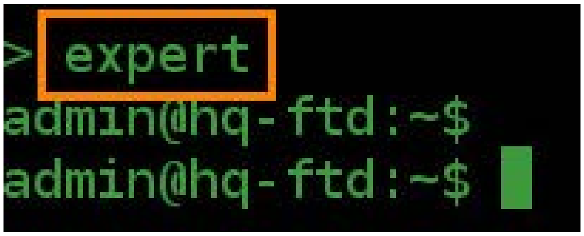
Figure 75. Show route



```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 198.18.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 198.18.1.1, ISP_Side
C        172.16.100.0 255.255.255.0 is directly connected, LAN_Side
L        172.16.100.1 255.255.255.255 is directly connected, LAN_Side
C        172.16.102.0 255.255.255.0 is directly connected, DMZ_LAN
L        172.16.102.1 255.255.255.255 is directly connected, DMZ_LAN
C        198.18.1.0 255.255.255.0 is directly connected, ISP_Side
L        198.18.1.2 255.255.255.255 is directly connected, ISP_Side
```

54. Issue the command **expert** to access the Linux shell.

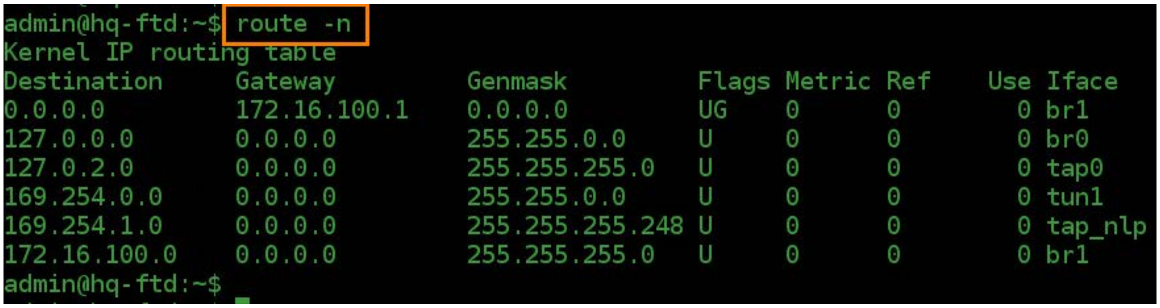
Figure 76. Change to expert mode



```
> expert
admin@hq-ftd:~$
admin@hq-ftd:~$
```

55. Type **route -n** and compare this routing table to the show route output. Why are they different? [Because when in expert mode you are looking at what the Management Interface sees while in firepower or FTD shells you are seeing what the data path looks like.]

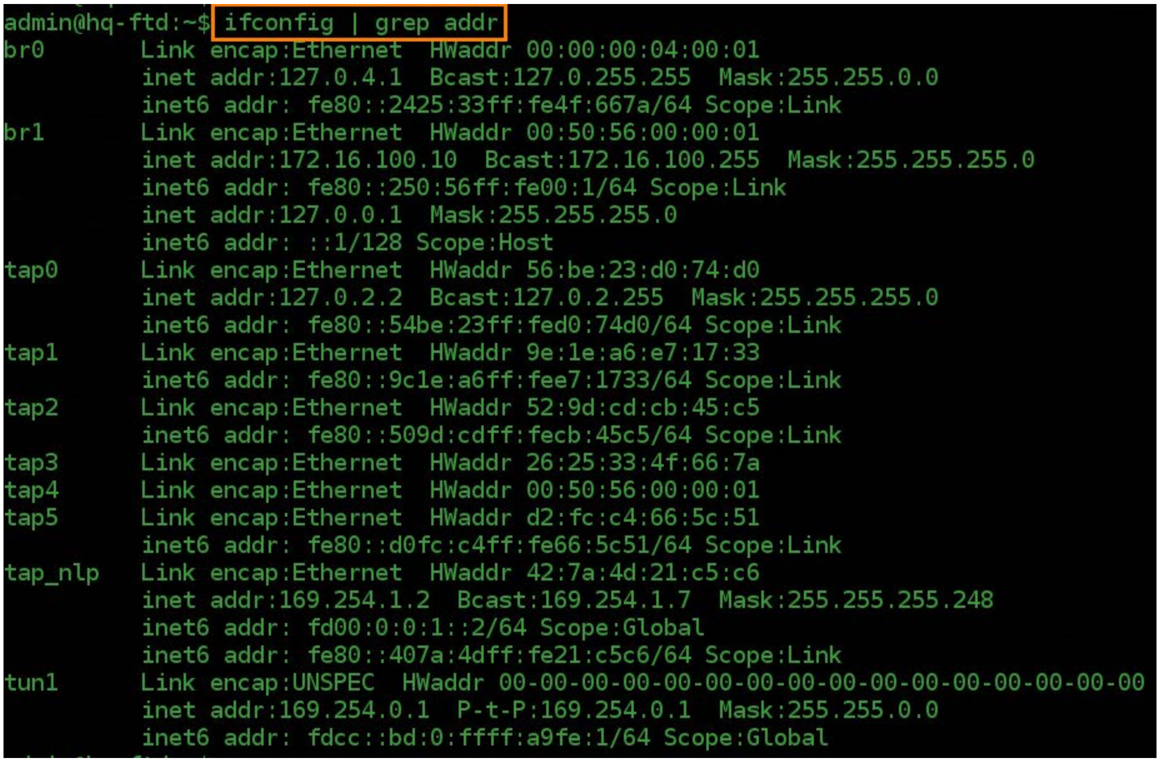
Figure 77. Route –n



```
admin@hq-ftd:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.100.1    0.0.0.0         UG    0      0        0 br1
127.0.0.0       0.0.0.0         255.255.0.0     U     0      0        0 br0
127.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 tap0
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 tun1
169.254.1.0     0.0.0.0         255.255.255.248 U     0      0        0 tap_nlp
172.16.100.0    0.0.0.0         255.255.255.0   U     0      0        0 br1
admin@hq-ftd:~$
```

56. Type ifconfig (or better yet **ifconfig | grep addr**) and compare the assigned IP addresses to interfaces with the output of the show ip command. Why are they different? [Because, when in expert mode, you are looking at what the Management Interface sees; while in firepower or FTD mode you are seeing what the data path looks like.]

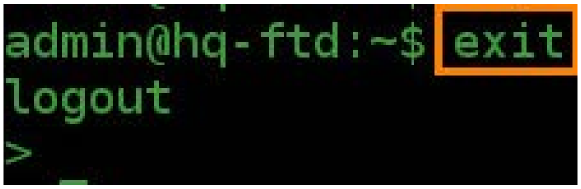
Figure 78. Ifconfig | grep addr



```
admin@hq-ftd:~$ ifconfig | grep addr
br0       Link encap:Ethernet  HWaddr 00:00:00:04:00:01
          inet addr:127.0.4.1  Bcast:127.0.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2425:33ff:fe4f:667a/64 Scope:Link
br1       Link encap:Ethernet  HWaddr 00:50:56:00:00:01
          inet addr:172.16.100.10  Bcast:172.16.100.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe00:1/64 Scope:Link
          inet addr:127.0.0.1  Mask:255.255.255.0
          inet6 addr: ::1/128 Scope:Host
tap0      Link encap:Ethernet  HWaddr 56:be:23:d0:74:d0
          inet addr:127.0.2.2  Bcast:127.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::54be:23ff:fed0:74d0/64 Scope:Link
tap1      Link encap:Ethernet  HWaddr 9e:1e:a6:e7:17:33
          inet6 addr: fe80::9c1e:a6ff:fee7:1733/64 Scope:Link
tap2      Link encap:Ethernet  HWaddr 52:9d:cd:cb:45:c5
          inet6 addr: fe80::509d:cdff:fecb:45c5/64 Scope:Link
tap3      Link encap:Ethernet  HWaddr 26:25:33:4f:66:7a
tap4      Link encap:Ethernet  HWaddr 00:50:56:00:00:01
tap5      Link encap:Ethernet  HWaddr d2:fc:c4:66:5c:51
          inet6 addr: fe80::d0fc:c4ff:fe66:5c51/64 Scope:Link
tap_nlp   Link encap:Ethernet  HWaddr 42:7a:4d:21:c5:c6
          inet addr:169.254.1.2  Bcast:169.254.1.7  Mask:255.255.255.248
          inet6 addr: fd00:0:0:1::2/64 Scope:Global
          inet6 addr: fe80::407a:4dff:fe21:c5c6/64 Scope:Link
tun1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:169.254.0.1  P-t-P:169.254.0.1  Mask:255.255.0.0
          inet6 addr: fdcc::bd:0:ffff:a9fe:1/64 Scope:Global
```

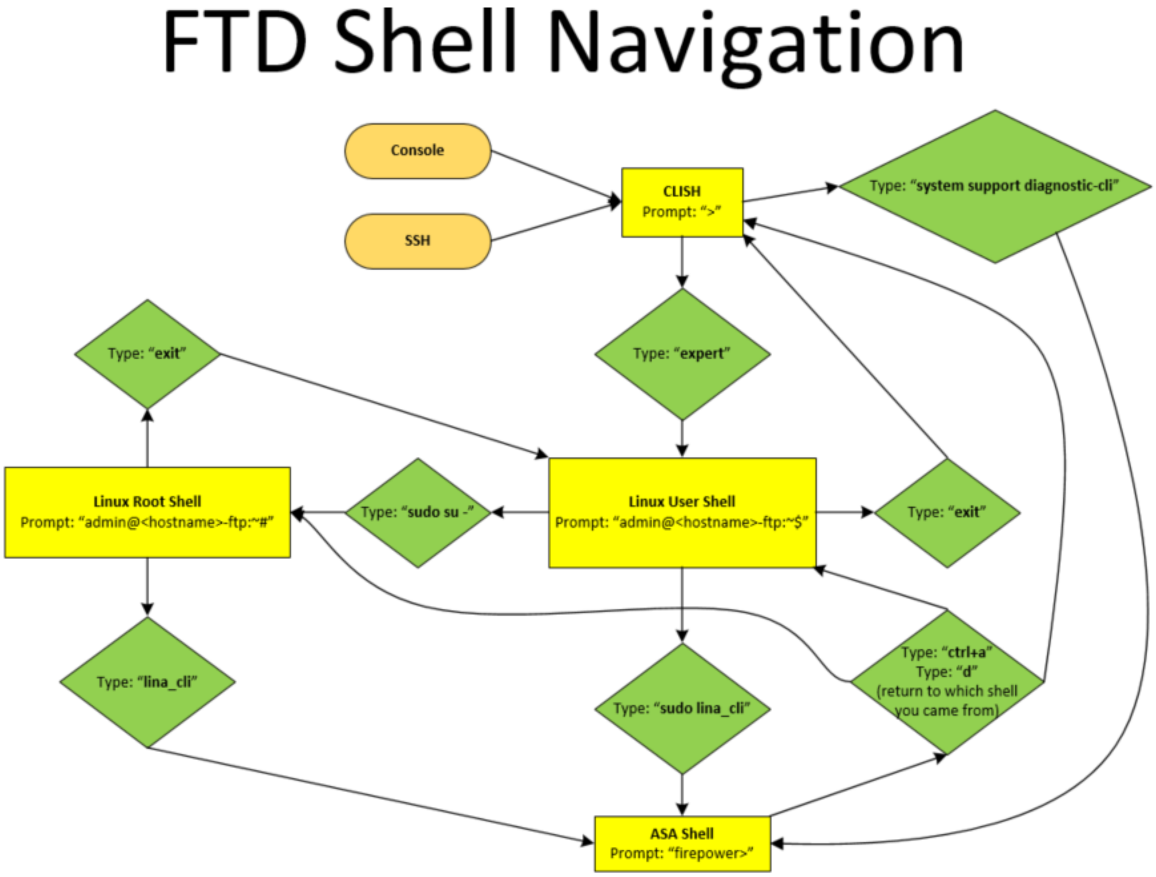
57. Type **exit** to return to the FTD shell.

Figure 79. Return to FTD shell



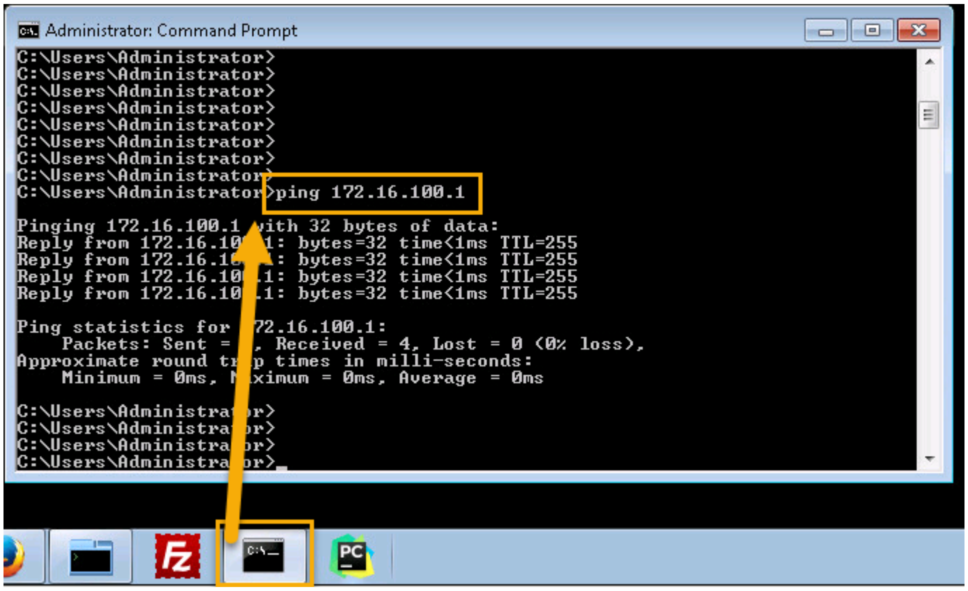
```
admin@hq-ftd:~$ exit
logout
>
```

Figure 80. FTD Shell Navigation



58. From hq-wkst you should be able to **ping 172.16.100.1**. Open a **CMD prompt** and do so.

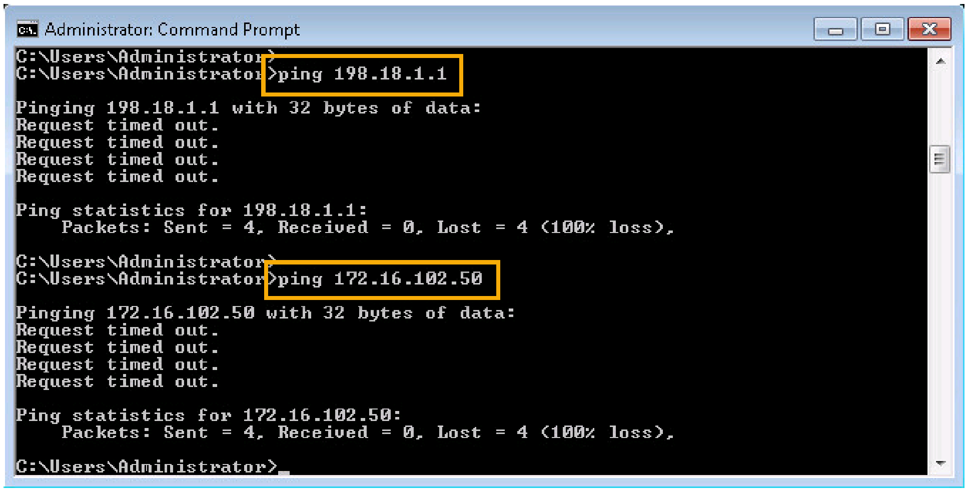
Figure 81. Ping hq-wkst default gateway



```
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>ping 172.16.100.1

Pinging 172.16.100.1 with 32 bytes of data:
Reply from 172.16.100.1: bytes=32 time<1ms TTL=255
Reply from 172.16.100.1: bytes=32 time<1ms TTL=255
Reply from 172.16.100.1: bytes=32 time<1ms TTL=255
Reply from 172.16.100.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>_
```

59. From hq-wkst you should NOT be able to **ping 198.18.1.1** (the ISP gateway IP for HQ), or **198.18.4.5** (the inet-server IP), or **172.16.102.50** (the dmz-server IP) why?

Figure 82. Can’t ping inet-server nor dmz-server



```
C:\Users\Administrator>
C:\Users\Administrator>ping 198.18.1.1

Pinging 198.18.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 198.18.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>
C:\Users\Administrator>ping 172.16.102.50

Pinging 172.16.102.50 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.102.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>_
```

Scenario Summary

Beyond setting up the Management interface on an FTD device, there is little configuration possible via the CLI. These devices must be configured either via the FMC or the Firepower Device Manager. Once the FTD is managed by the FMC configuration changes are made in the FMC and then pushed out to the FTD.

Scenario 3. Common Configurations for Example Corp Networks

Scenario Description

At this point hq-ftd is not configured enough for users behind it to access the Internet. This is because there are currently two things that are blocking those users. The first is that the Access Control Policy that is currently applied to hq-ftd has only one rule, which is the Default Action rule, and that rule is set to Block All Traffic. The second reason is that hq-ftd is not NAT'ting their packets. So even if the Access Control Policy was set to Permit the outside world doesn't know how to route traffic back to the 172.16.100.0/24 network.

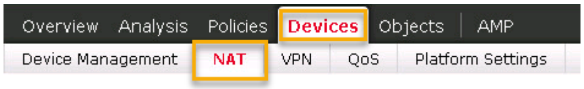
In this scenario you will fix these two issues. Along the way you will explore the ability to nest Access Control Policies as well as discuss the different ways to NAT in an FTD device.

Configure NAT for Example Corp Networks

Even though the hq-ftd device is in routed mode, has IP addresses on all its interfaces, and has a route (default route) it isn't translating the private IP address range 172.16.100.0/24 into something that is routable over the public Internet.

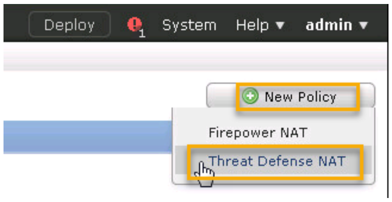
1. On hq-wkst and within the FMC administration webpage navigate to **Devices > NAT** to configure a NAT policy.

Figure 83. Navigate to NAT



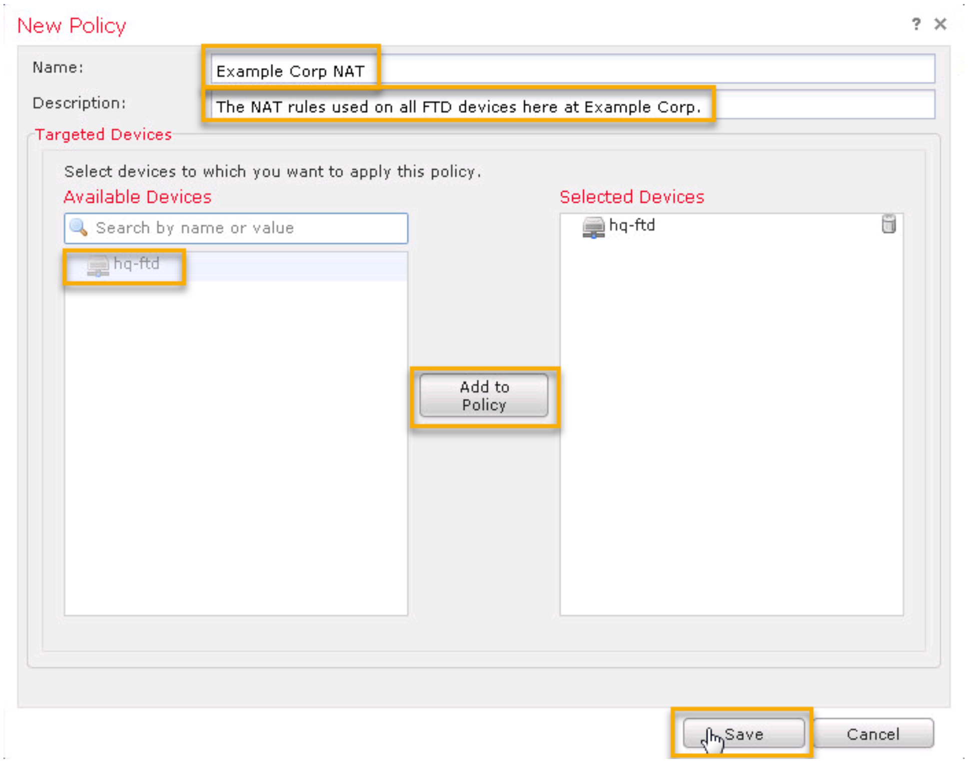
2. Click **New Policy** and select **Threat Defense NAT** from the dropdown list. This option is used to configure NAT on FTD devices. The other option, Firepower NAT, is used to configure NAT on devices running FirePower only.

Figure 84. Create NAT Policy



3. Use the following information to fill out the needed options:
    a. Name: **Example Corp NAT** (This NAT Policy will be pushed to all the FTD devices within your topology, eventually.)
    b. Description: **The NAT rules used on all FTD devices here at Example Corp.**
    c. Select the **hq-ftd** device from the **Available Devices** and click **Add to Policy** to move it over to the Selected Devices.
4. Click **Save**.

Figure 85. Save NAT Policy



New Policy

Name: Example Corp NAT

Description: The NAT rules used on all FTD devices here at Example Corp.

Targeted Devices

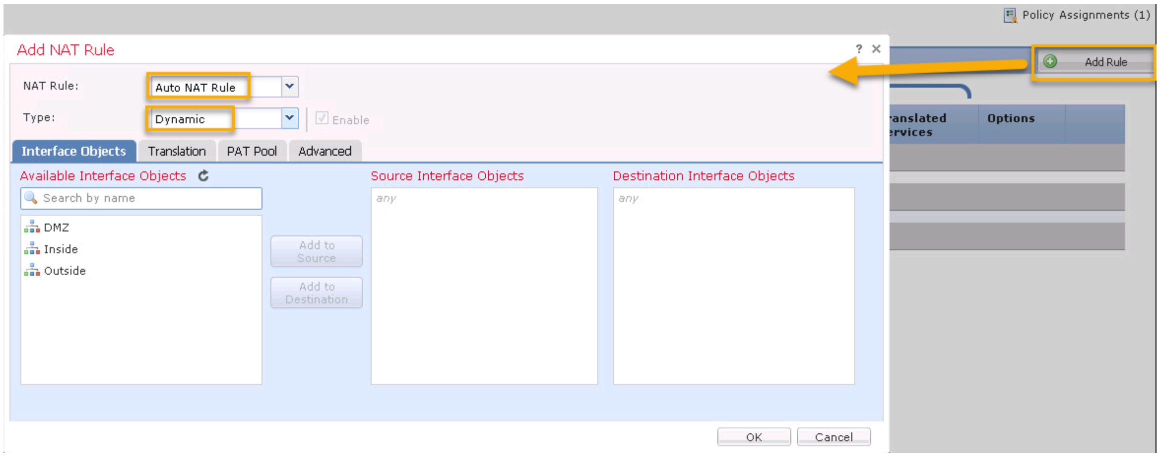
Select devices to which you want to apply this policy.

Available Devices: hq-ftd

Selected Devices: hq-ftd

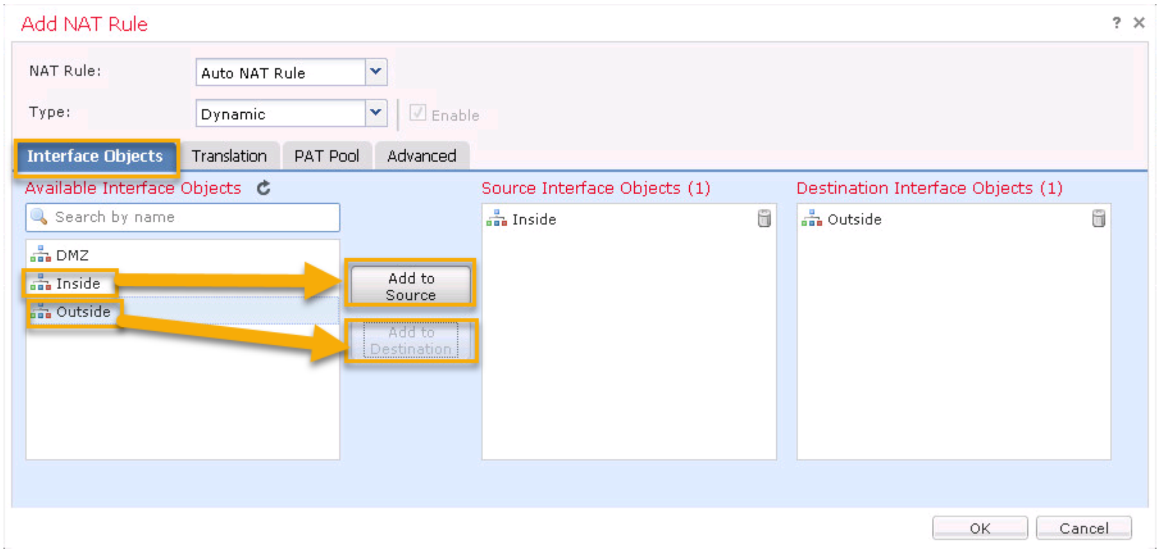
5. Now that the NAT policy is created you need to add some rules (i.e. translations) to it. Click the **Add Rule** button and use the following information to fill out the Add NAT Rule popup window:
    a. NAT Rule: **Auto NAT Rule**
    b. Type: **Dynamic**

Figure 86. Part 1 of adding NAT rule



6. On the Interface Objects tab:
    a. From the **Available Interface Objects** select **Inside** and then click the **Add to Source** button.
    b. From the **Available Interface Objects** select **Outside** and then click the **Add to Destination** button.
    c. Notice that these are ZONES and not really interfaces.

Figure 87. Add Zones to Rule



7. On the **Translation tab**:

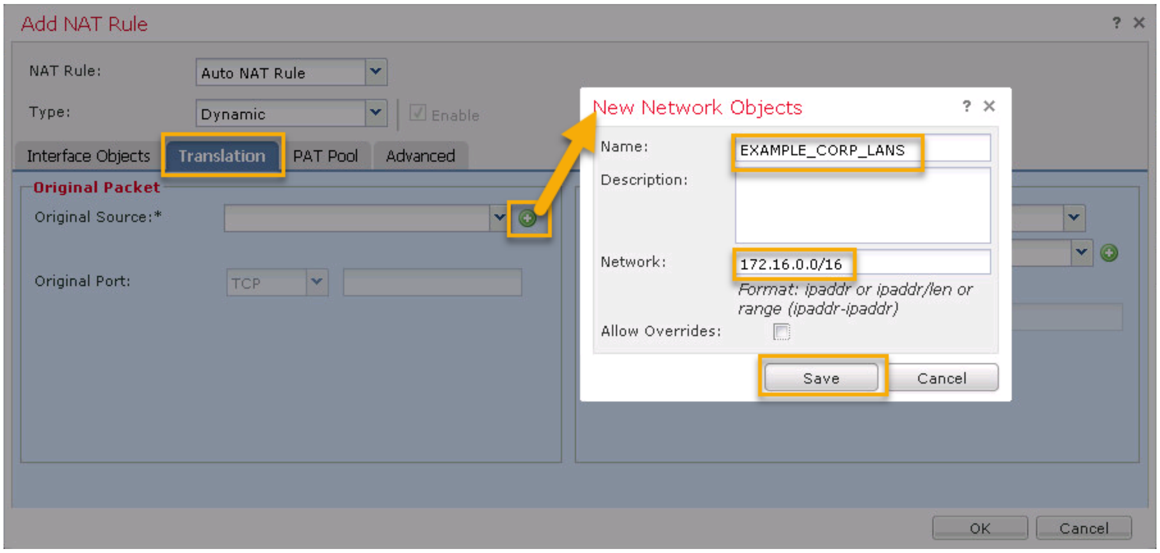
   a. Original Source: (You need to create a Network Object that encompasses all the Example Corp LANs.) Click the **green plus icon** and use the following information to fill out the needed info:

      i. Name: **EXAMPLE_CORP_LANS**

      ii. Network: **172.16.0.0/16**

      iii. Click **Save**.

Figure 88. Add Network Object



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Original Packet

Original Source:*

Original Port: TCP

New Network Objects

Name: EXAMPLE_CORP_LANS

Description:

Network: 172.16.0.0/16

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

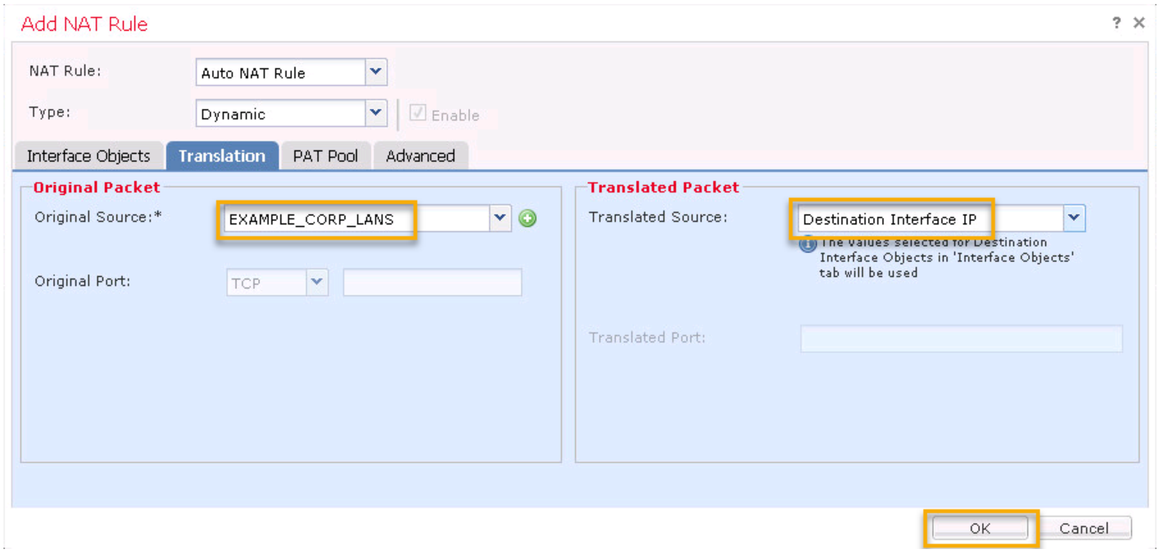
Allow Overrides: □

   b. Now select the newly created **EXAMPLE_CORP_LANS** from the dropdown menu.

   c. Translated Source: Select the **Destination Interface IP** from the dropdown menu.

8. Click **OK** to finish creating this rule. Note: This same rule will be applied to the Remote1 and Remote2 location's FTD devices once you get that far in the lab. Notice how this rule will equally apply to the Remote locations as it is to the HQ location (assuming those locations have interfaces assigned to the Inside and Outside zones).

Figure 89. Set up Translation Tab and Save



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic ☑ Enable

Original Packet

Original Source:* EXAMPLE_CORP_LANS

Original Port: TCP

Translated Packet

Translated Source: Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

A Note about Auto NAT and Manual NAT

Cisco recommends you use Auto NAT unless you need the extra features of Manual NAT. It is easier to configure and might be more stable for services such as VoIP.

Comparing Auto NAT and Manual NAT. The main differences between these two NAT types are:

How you define the real addresses:

Auto NAT – The NAT rule becomes a parameter for a network object. The network object IP address serves as the original (real) address.

Manual NAT – You identify a network object, or network group, for both the real and mapped addresses. In this case NAT is not a parameter of the network object; the network object (or network group) is a parameter of the NAT configuration. The ability to use a network object group for the real address means that manual NAT is more scalable.

How source and destination NAT is implemented:

Auto NAT – Each rule can apply to either the source or destination of the packet. So two rules might be used; one for the source IP address and one for the destination IP address. These two rules cannot be tied together to enforce a specific translation for a source/destination combination.

Manual NAT – A single rule translates both the source and destination of a packet. A packet matches one rule only and further rules are not checked. Even if you do not configure the optional destination address, a matching packet still matches one manual NAT rule only. The source and destination are tied together, so you can enforce different translations depending on the source/destination combination. For example sourceA/destinationB can have a different translation than sourceA/destinationC.

Order of NAT Rules:

Auto NAT – Automatically ordered in the NAT table.

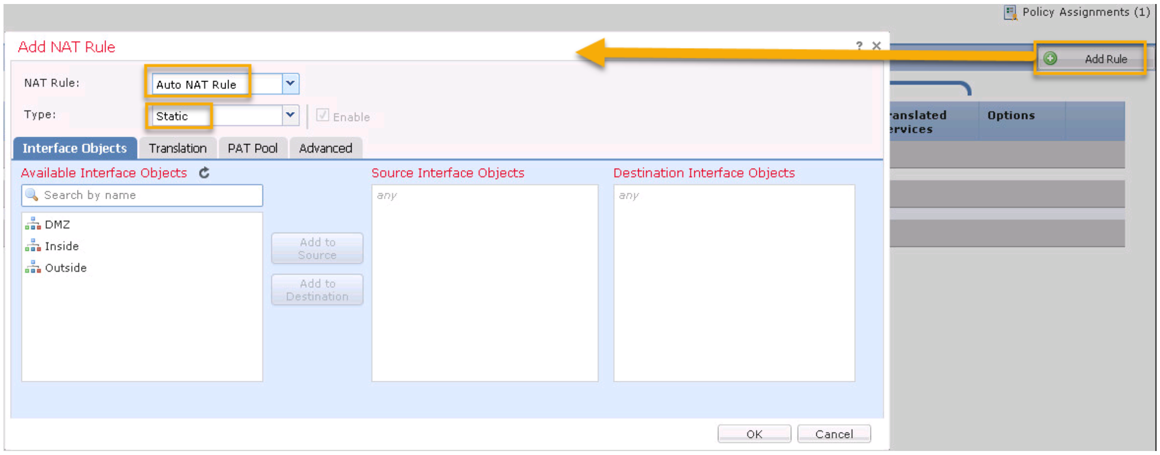
Manual NAT – Manually ordered in the NAT table (before or after Auto NAT rules).

9. Next, create a rule for the DMZ server. You won't be using this entry in the lab for a while but let's go ahead and configure the NAT translation while you are here. Click the **Add Rule** button.

    a. NAT Rule: **Auto NAT Rule**

    b. Type: **Static**

Figure 90. Add NAT Rule



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

Source Interface Objects: any

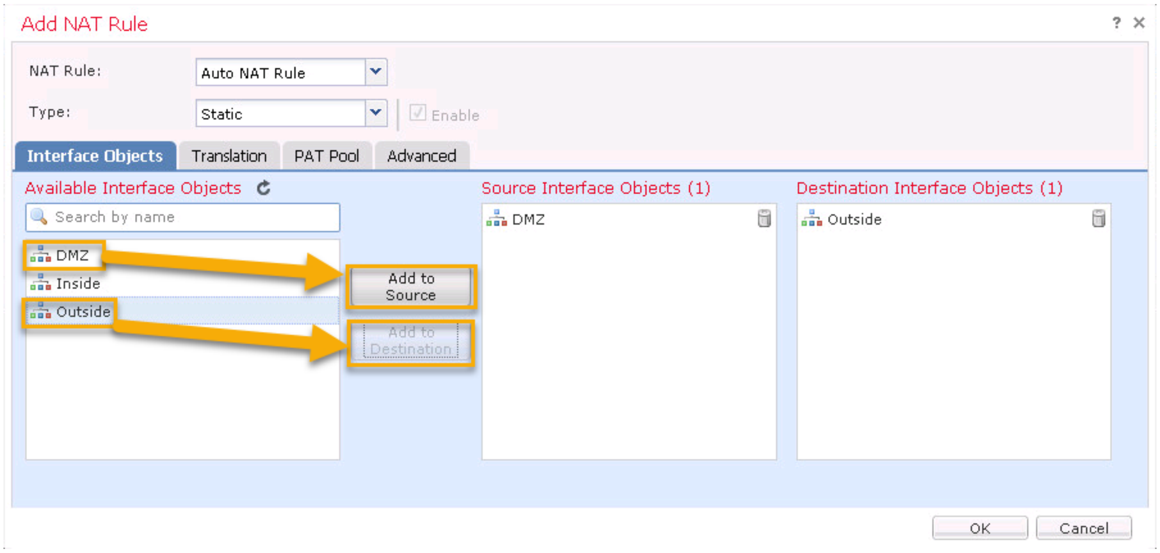
Destination Interface Objects: any

10. On the **Interface Objects tab**:

    a. From the **Available Interface Objects** select **DMZ** and then click the **Add to Source** button.

    b. From the **Available Interface Objects** select **Outside** and then click the **Add to Destination** button.

Figure 91. Interface Objects Tab



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

Source Interface Objects (1): DMZ

Destination Interface Objects (1): Outside

11. On the **Translation tab**:

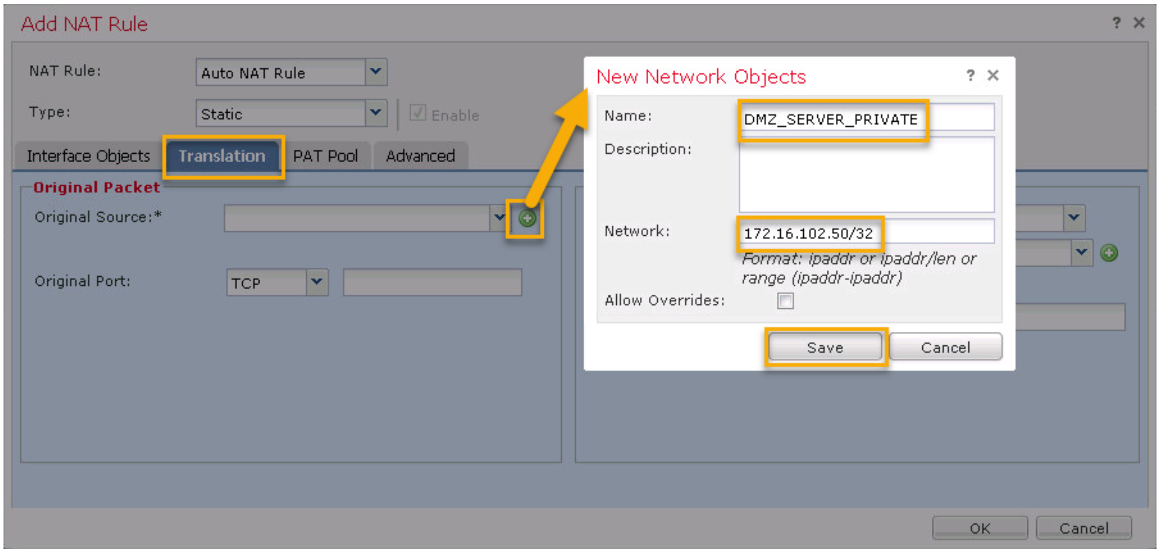
    a. You need to create a Network Objects for the DMZ Server's private and public IPs. Click the **green plus icon** and use the following information to fill out the needed info:

        i. Name: **DMZ_SERVER_PRIVATE**

        ii. Network: **172.16.102.50/32**

        iii. Click **Save**.

Figure 92. Add Network Object



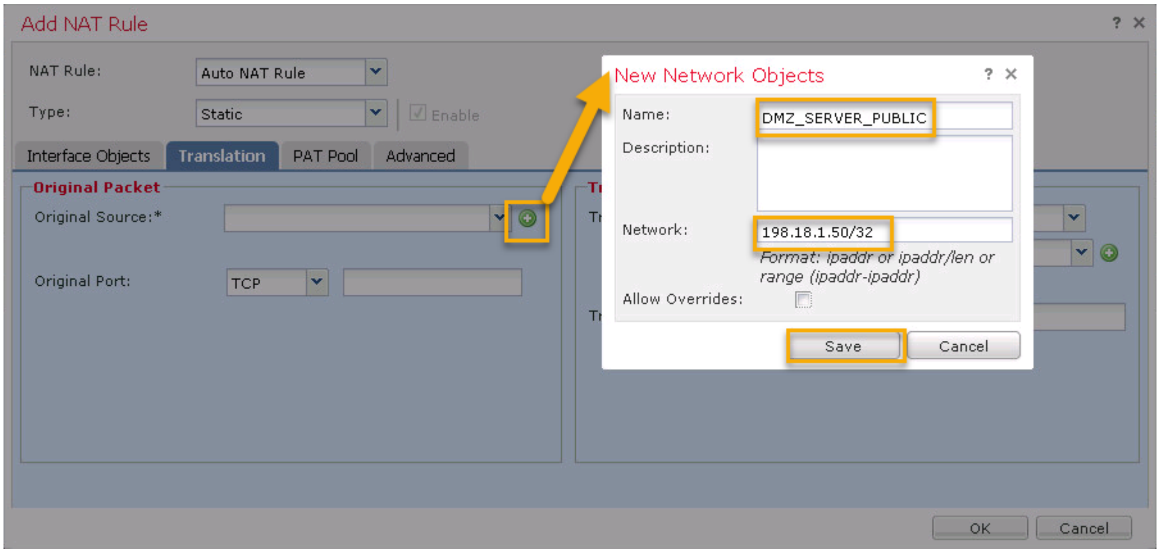
b. Click the **green plus icon** again and use the following information to build the DMZ Server's Public IP Network Object:

   i. Name: **DMZ_SERVER_PUBLIC**

   ii. Network: **198.18.1.50/32**

   iii. Click **Save**.

Figure 93. Add Network Object



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

New Network Objects

Name: DMZ_SERVER_PUBLIC

Description:

Network: 198.18.1.50/32

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides: □

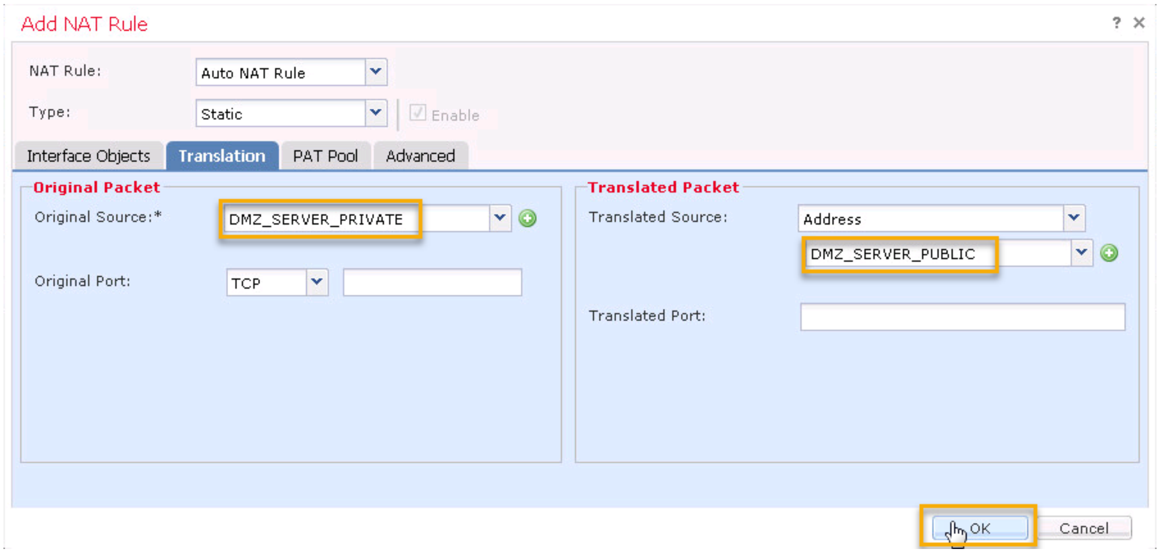
Original Port: TCP

c. Original Source: Select the **DMZ_SERVER_PRIVATE** from the dropdown menu.

d. Translated Source: Select the **DMZ_SERVER_PUBLIC** from the dropdown menu.

12. Click **OK** to finish creating this rule.

Figure 94. Set up Translation Tab and Save



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

Original Packet

Original Source:* DMZ_SERVER_PRIVATE

Original Port: TCP

Translated Packet

Translated Source: Address

DMZ_SERVER_PUBLIC

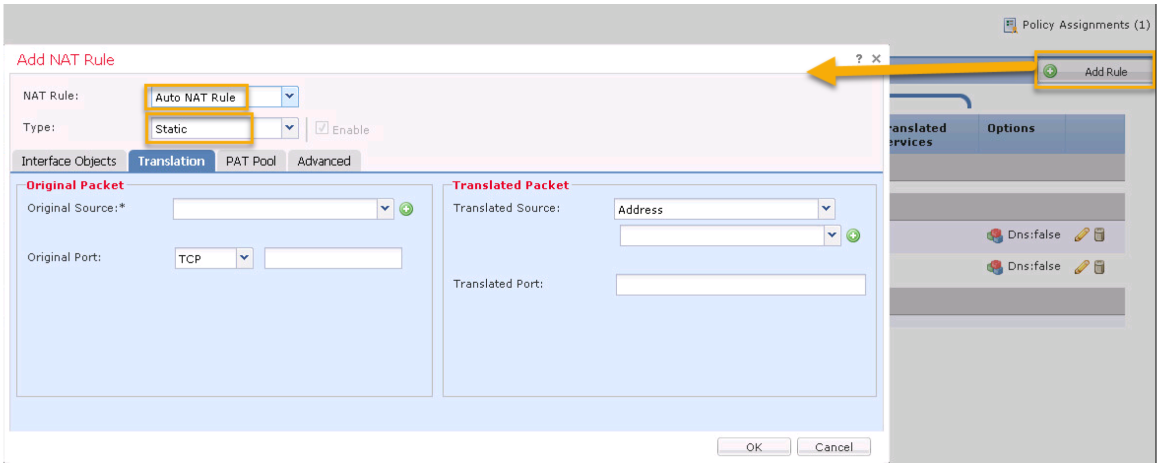
Translated Port:

13. You need one more NAT rule for the FMC, for when you register the remote2-ftd later in the lab. Click the **Add Rule** button.

    a. NAT Rule: **Auto NAT Rule**

    b. Type: **Static**

Figure 95. Add NAT rule

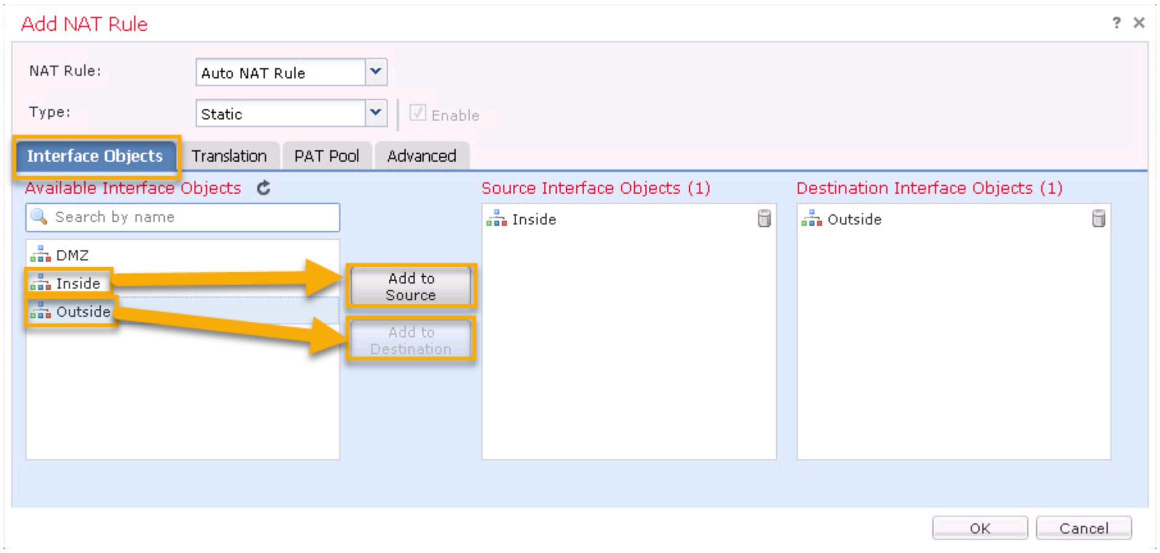


14. On the **Interface Objects tab**:

    a. From the **Available Interface Objects** select **Inside** and then click the **Add to Source** button.

    b. From the **Available Interface Objects** select **Outside** and then click the **Add to Destination** button.

Figure 96. Set up Interface Objects tab



15. On the **Translation tab**:

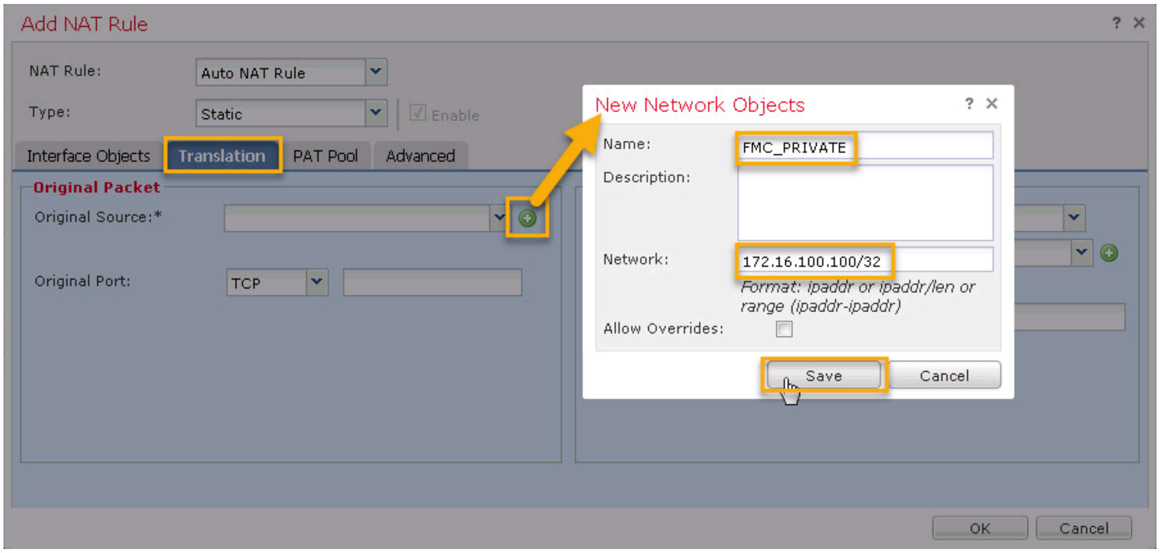
    a. You need to create a Network Objects for the FMC Server's private and public IPs. Click the **green plus icon** and use the following information to fill out the needed info:

        i. Name: **FMC_PRIVATE**

        ii. Network: **172.16.100.100/32**

        iii. Click **Save**.

Figure 97. Create Network Object



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

New Network Objects

Name: FMC_PRIVATE

Description:

Network: 172.16.100.100/32

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides: □

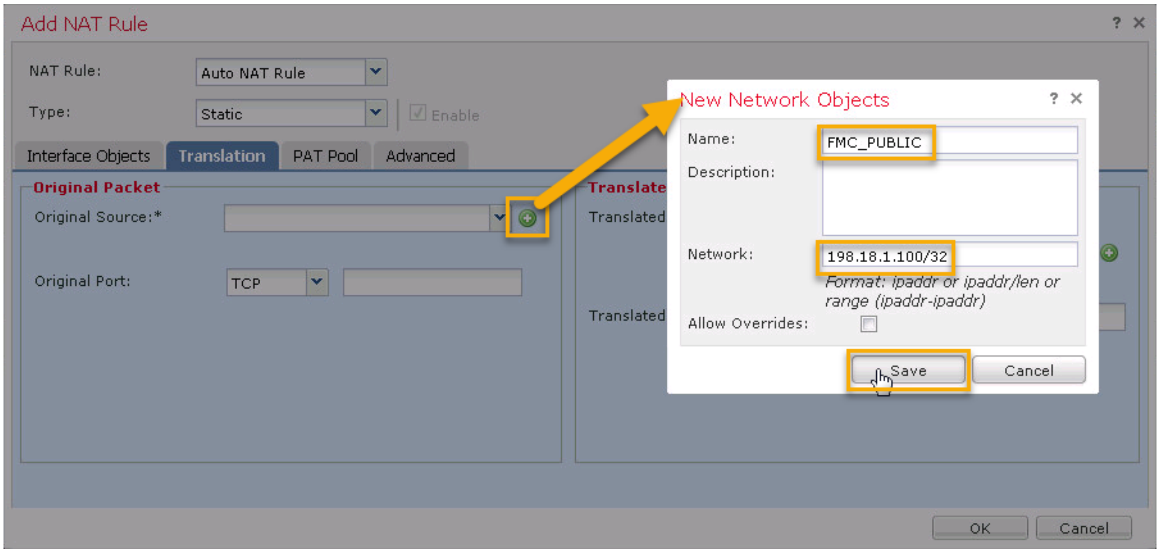
b. Click the **green plus icon** again and use the following information to build the FMC Server's Public IP Network Object:

   i. Name: **FMC_PUBLIC**

   ii. Network: **198.18.1.100/32**

   iii. Click **Save**.

Figure 98. Add Network Object



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

Original Packet

Original Source:*

Original Port: TCP

Translated Packet

New Network Objects

Name: FMC_PUBLIC

Description:

Network: 198.18.1.100/32

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

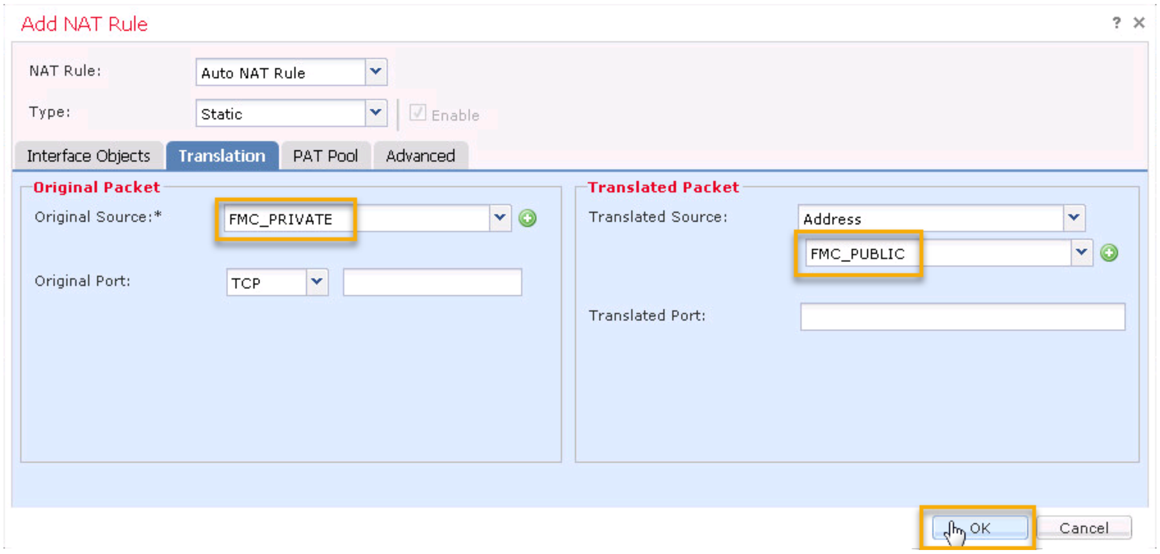
Allow Overrides: □

c. Original Source: Select the **FMC_PRIVATE** from the dropdown menu.

d. Translated Source: Select the **FMC_PUBLIC** from the dropdown menu.

16. Click **OK** to finish creating this rule.

Figure 99. Set up Translation tab and Save



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

Original Packet

Original Source:* FMC_PRIVATE

Original Port: TCP

Translated Packet

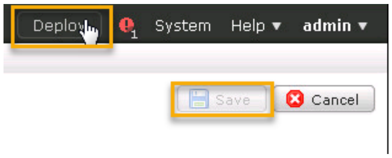
Translated Source: Address

FMC_PUBLIC

Translated Port:

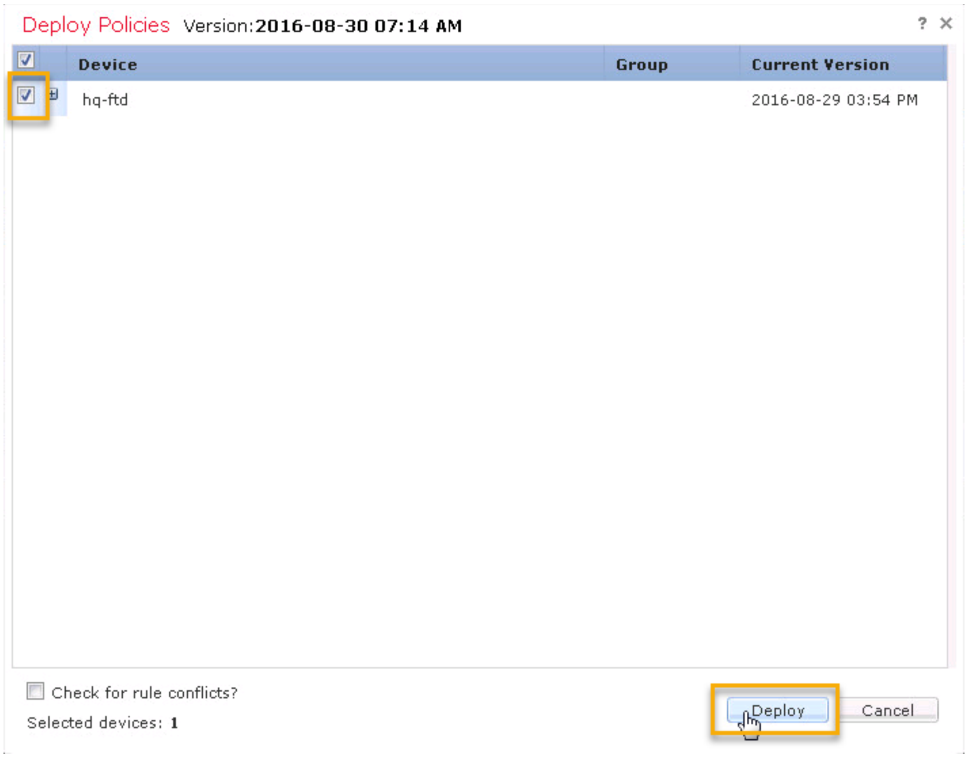
17. Click **Save** and then **Deploy**.

Figure 100. Save and Deploy



18. Select the **hq-ftd** device and then click **Deploy**.

Figure 101. Deploy to hq-ftd


Deploy Policies Version:**2016-08-30 07:14 AM**

☑	Device	Group	Current Version
☑ ⊞	hq-ftd		2016-08-29 03:54 PM

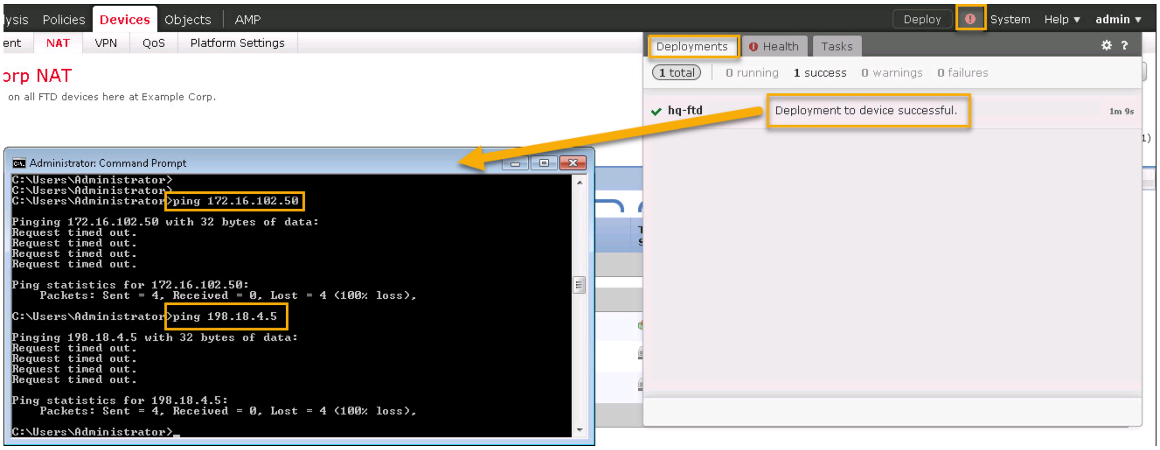
□ Check for rule conflicts?

Selected devices: **1**

Testing Access -- Failure

19. Once the deployment is complete, from hq-wkst, attempt to **ping 172.16.102.50** (dmz-server), and **198.18.4.5** (inet-server).

Figure 102. Failed pings



1 total | 0 running | 1 success | 0 warnings | 0 failures

✓ hq-ftd — Deployment to device successful. — 1m 9s

```
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>ping 172.16.102.50

Pinging 172.16.102.50 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.102.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 198.18.4.5

Pinging 198.18.4.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 198.18.4.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>_
```

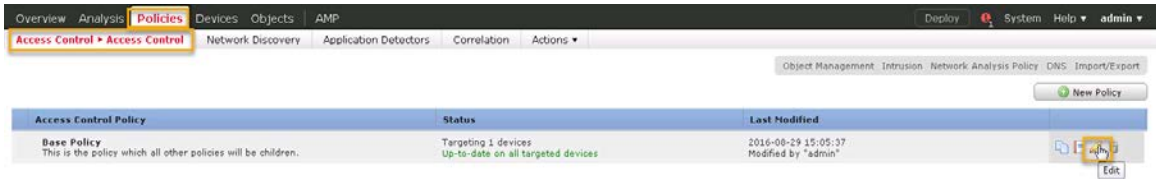
Why doesn’t this work? The FTD is set up with an Inside and Outside interfaces, it is in routed mode, it has a default route, and you have NAT translations set up but….

What is missing or not yet configured? Though your routing and interfaces are correct the Access Control Policy assigned to this FTD, currently the Base Policy Access Control Policy, has no rules so it takes the Default Action rule.

Do you remember what the Default Action setting is set at in the Base Policy Access Control Policy? It is Block All Traffic.

20. On hq-wkst in the FMC administration webpage navigate to **Policies > Access Control > Access Control** and click the **pencil icon** for the **Base Policy** row.

Figure 103. Edit Base Policy ACP

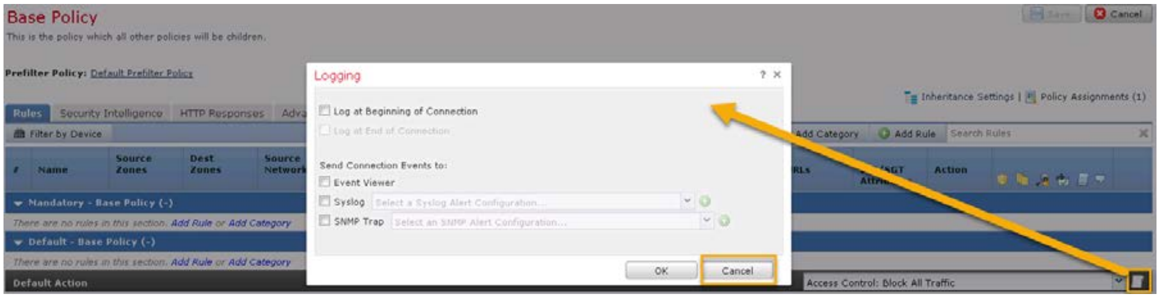


Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 1 devices Up-to-date on all targeted devices	2016-08-29 15:05:37 Modified by "admin"

21. Click on the **scroll icon** next to the Default Action’s dropdown menu arrow. Notice that no logging is enabled for this rule. That is why I had to “tell” you the answer since there would have been no audit trail for you to investigate. That said, it probably isn’t wise to log everything that hits the Default Action rule unless you design your policies such that this Default Action would only be triggered in rare and odd cases.

22. For now, click **Cancel** to exit the Logging popup window.

Figure 104. Scroll Icon



Base Policy

This is the policy which all other policies will be children.

Prefilter Policy: Default Prefilter Policy

▾ Mandatory - Base Policy (-)

There are no rules in this section. Add Rule or Add Category

▾ Default - Base Policy (-)

There are no rules in this section. Add Rule or Add Category

Default Action: Access Control: Block All Traffic

☐ Log at Beginning of Connection
☐ Log at End of Connection

Send Connection Events to:
☐ Event Viewer
☐ Syslog Select a Syslog Alert Configuration...
☐ SNMP Trap Select an SNMP Alert Configuration...

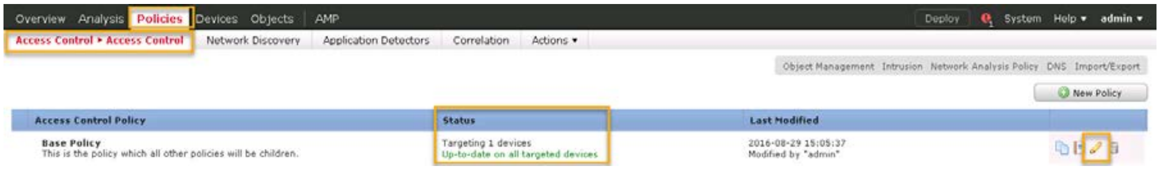
Set Up Access Control Policies

23. In FMC navigate to **Policies > Access Control > Access Control**.

24. Notice that currently you have one Access Control Policy (ACP) called Base Policy, that it is targeting 1 device, and that all the targeted devices are up-to-date. This is a quick way to see which policy has devices assigned to it and whether there are un-deployed changes.

25. Click the **pencil icon** on the row for the **Base Policy** to edit this policy.

Figure 105. ACP is up-to-date and Edit



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 1 devices Up-to-date on all targeted devices	2016-08-29 15:05:37 Modified by "admin"

26. Since the Base Policy will be the parent of all the other policies in Example Corp's design, let's create a rule here that allows traffic coming from an Example Corp's LAN IP addresses, anything from the 172.16.0.0/16 range, to be permitted access to any other IP address (IPv4 any). Click the **Add Rule** button. Use the following to fill out the necessary options:

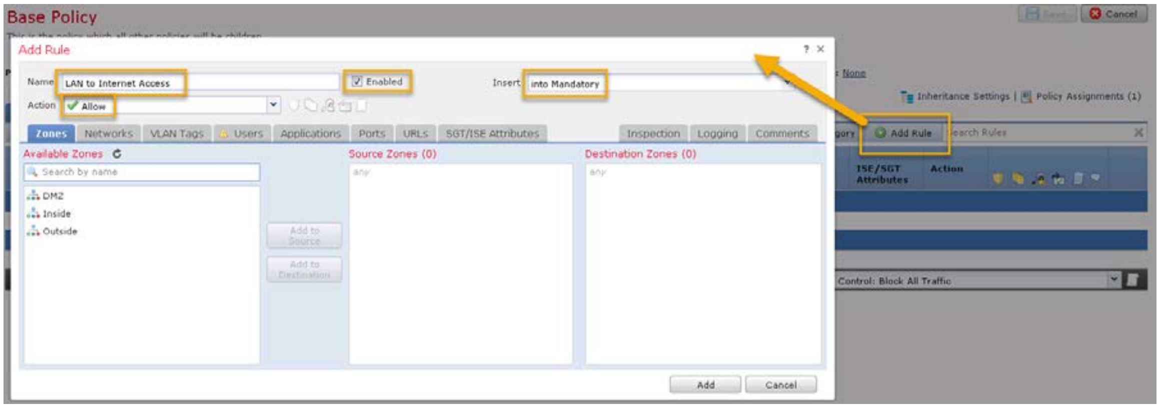
    a. Name: **LAN to Internet Access**

    b. Enabled: **Checked**

    c. Insert: **into Mandatory**

    d. Action: **Allow**

Figure 106. Part 1 of adding ACP rule



Name: LAN to Internet Access

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

When you click the dropdown menu button notice all the options you have to choose from. A whole lab could be created around implementing and testing all these combinations of options. In short use the following list to get an idea of what each are for:

Allow: Permit through the Firewall but check it against the SNORT rules.

Trust: Check it against the Firewall rules but don't check it against the SNORT rules.

Monitor: Send the traffic to SNORT for analysis and then determine whether to process through the Firewall rules.

Block: Don't allow through the Firewall (and thus don't sent to SNORT either) and don't send any sort of acknowledgement back to the source that you are blocking.

Block with Reset: Don't allow through the Firewall and let the source know its connection has been terminated.

Interactive Block: Notify the user that the action that triggered this rule is recommended to be blocked but that the user can choose to continue with this action should they feel it is okay to proceed.

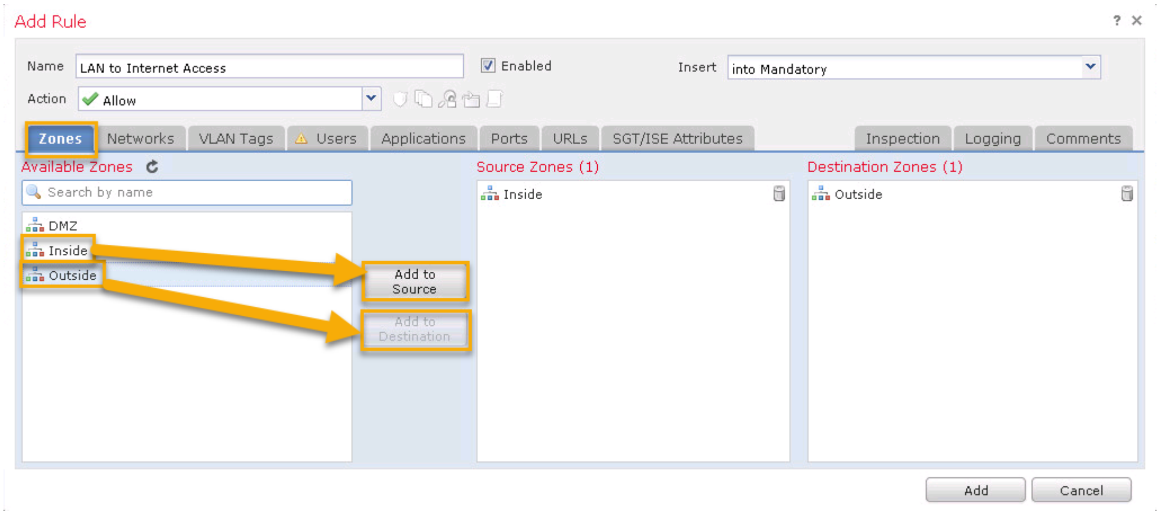
Interactive Block with reset: The same as the Interactive Block but this time, if the user chooses to not proceed with their action send a reset to the source.

27. On the **Zones tab**:

    a. From the **Available Zones** select **Inside** and then click the **Add to Source** button.

    b. From the **Available Zones** select **Outside** and then click the **Add to Destination** button.

Figure 107. Set up Zones tab



Add Rule

Name: LAN to Internet Access

☑ Enabled

Insert: into Mandatory

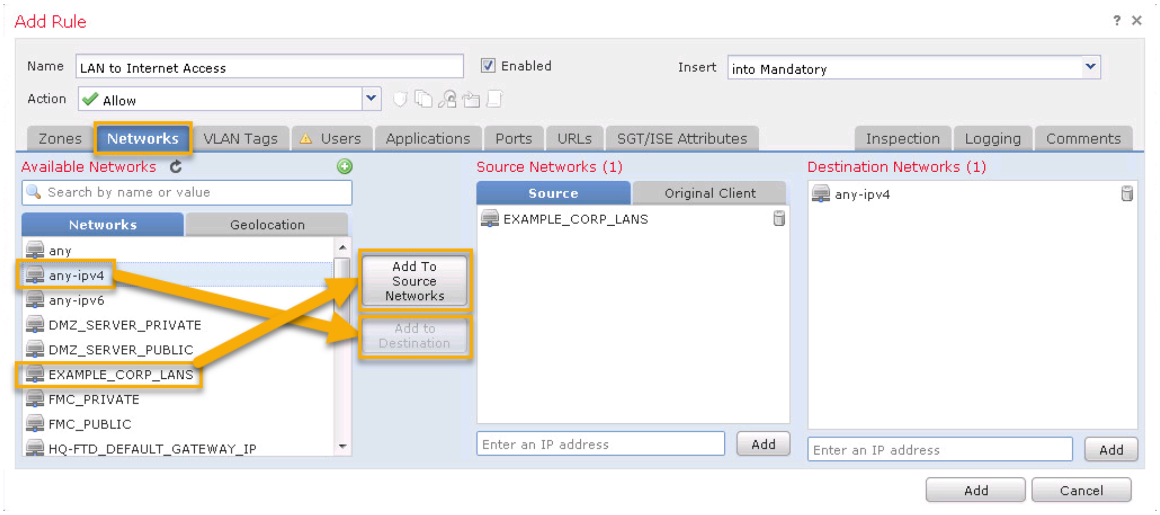
Action: ✓ Allow

28. On the **Networks tab**:

    a. From the **Available Networks** select **EXAMPLE_CORP_LANS** and then click the **Add to Source Networks** button.

    b. From the **Available Networks** select **any-ipv4** and then click the **Add to Destination** button.

Figure 108. Configure Networks tab



Name: LAN to Internet Access

☑ Enabled

Insert: into Mandatory

Action: Allow

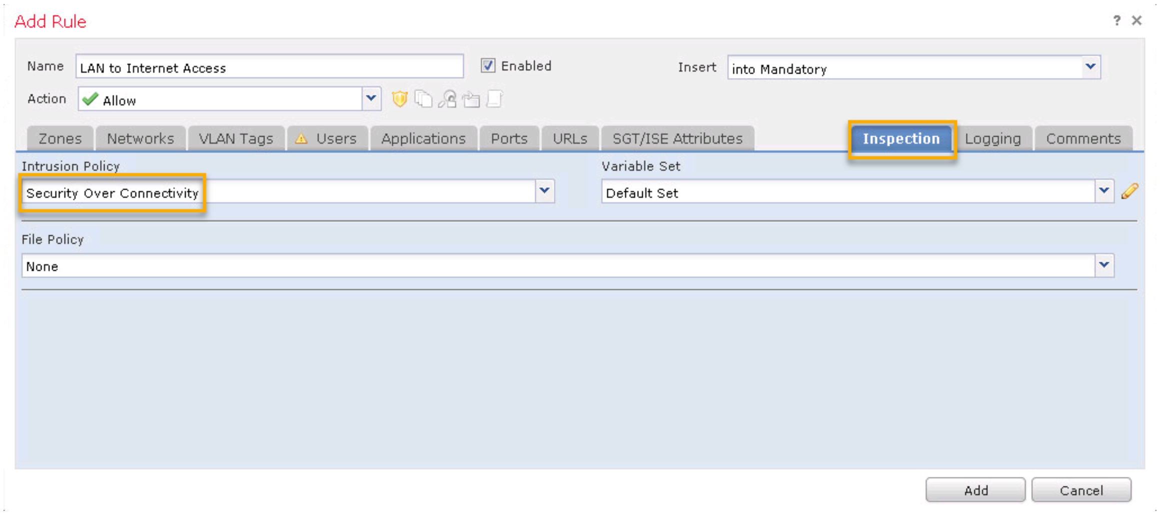
Available Networks: any, any-ipv4, any-ipv6, DMZ_SERVER_PRIVATE, DMZ_SERVER_PUBLIC, EXAMPLE_CORP_LANS, FMC_PRIVATE, FMC_PUBLIC, HQ-FTD_DEFAULT_GATEWAY_IP

Source Networks (1): EXAMPLE_CORP_LANS

Destination Networks (1): any-ipv4

29. On the **Inspection tab** set the Intrusion Policy field to **Security Over Connectivity** (More on this later but essentially this is the IPS rule that is applied to traffic matching this rule.)

Figure 109. Configure Inspection tab



Name: LAN to Internet Access

☑ Enabled

Insert: into Mandatory

Action: Allow

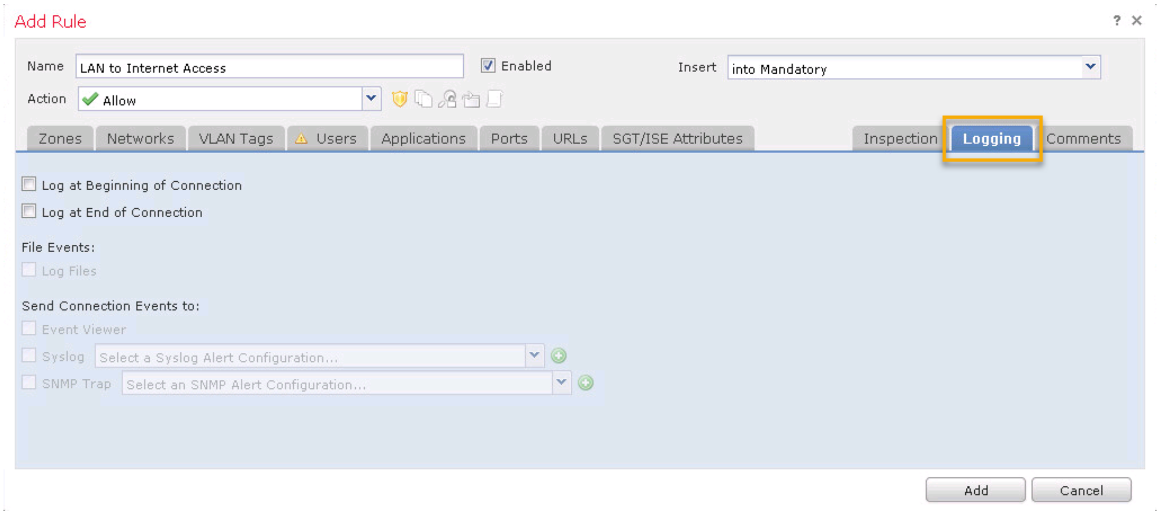
Intrusion Policy: Security Over Connectivity

Variable Set: Default Set

File Policy: None

30. On the **Logging tab** notice that you can log any time a packet or communication matches this rule. This particular rule will presumably get hit a lot (by all Example Corp users and servers that don't meet another rule) so logging might not be justified. That said, if you don't log it you don't know it exists. Knowing when to log, how much to log, and when not to log requires some monitoring and analysis for each deployment. In order to not dirty your event viewer, you will NOT be logging this rule's traffic during this lab.

Figure 110. No logging this ACP rule



Add Rule

Name: LAN to Internet Access ☑ Enabled Insert: into Mandatory

Action: Allow

□ Log at Beginning of Connection

□ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

□ Event Viewer

□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

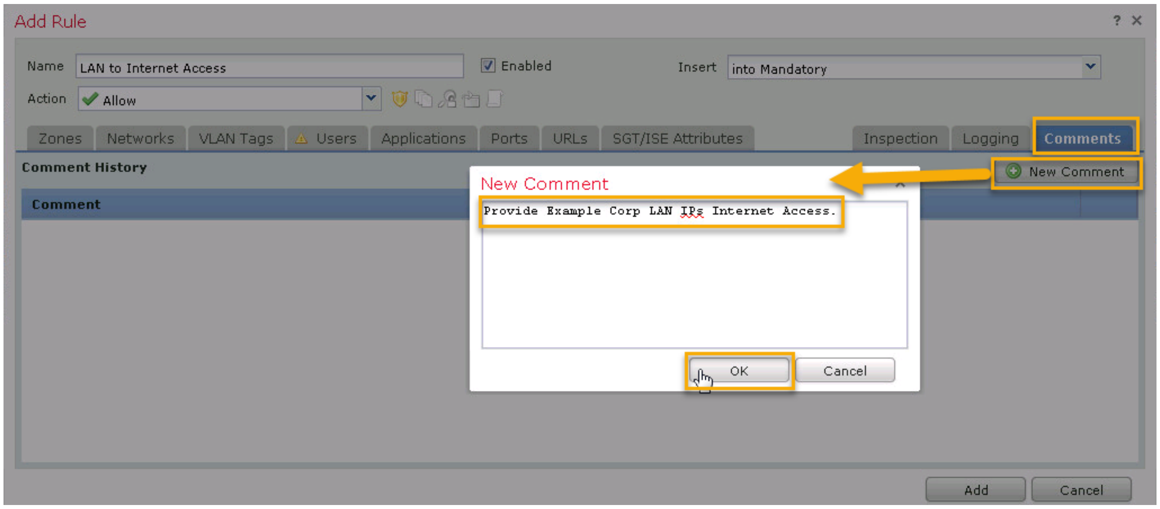
31. On the **Comments tab**:

    a. Click **New Comment**

    b. New Comment: **Provide Example Corp LAN IPs Internet Access.**

    c. Click **OK**.

Figure 111. Add a comment



Add Rule

Name: LAN to Internet Access ☑ Enabled Insert: into Mandatory

Action: Allow

Comment History

Comment

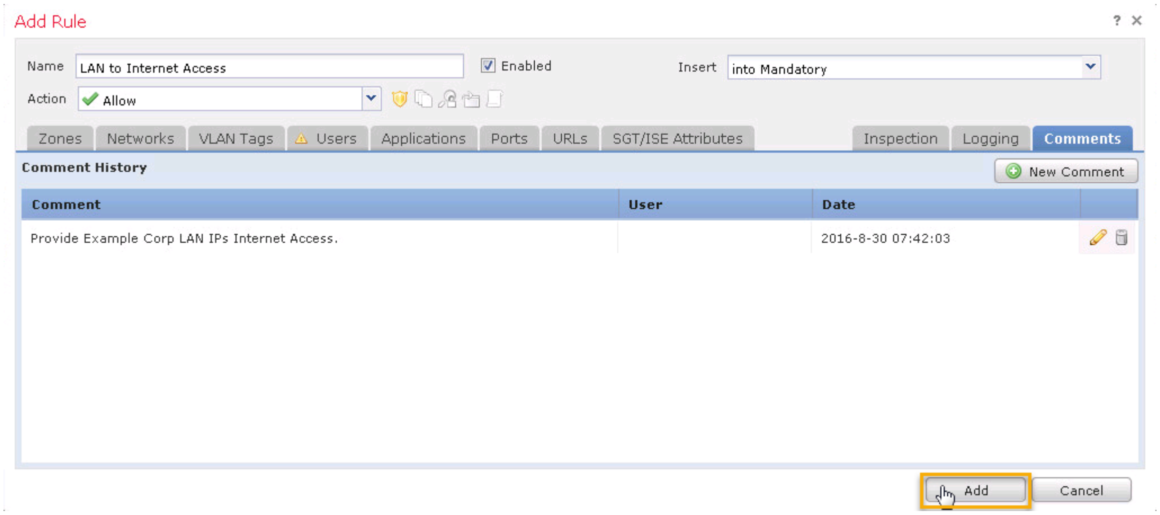
New Comment

Provide Example Corp LAN IPs Internet Access.

Note: Once you click Add/Save to this rule you will not be able to edit this comment. You can add new comments but this will remain as a permanent record of the actions taken. Also, it is possible to configure the FMC to mandate a comment be added via the options on the **System > Configuration > Access Control Preferences** page.

32. Click **Add**.

Figure 112. Add ACP Rule



Add Rule

Name: LAN to Internet Access ☑ Enabled Insert: into Mandatory

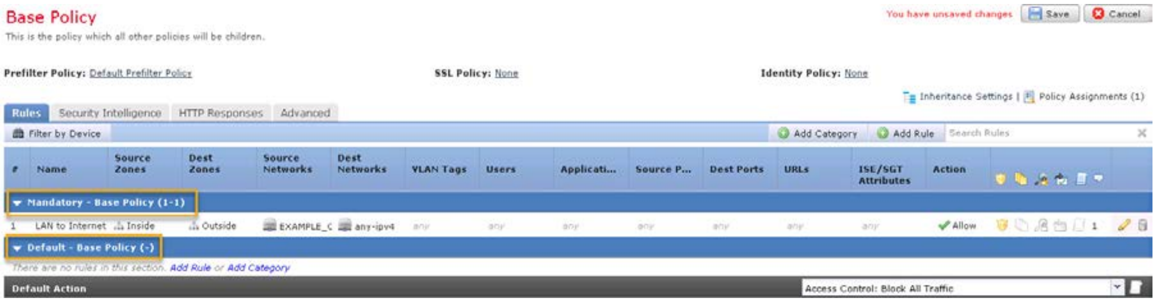
Action: Allow

Comment History

Comment	User	Date
Provide Example Corp LAN IPs Internet Access.		2016-8-30 07:42:03

Notice that this rule is in the Mandatory section and that the Mandatory section comes “before” the Default section of rules. Rules are checked in a top-down fashion. Once a rule is met no other rule is checked. This means that the Base Policy’s Mandatory rules will be checked for matches before any of the Default rules are checked.

Figure 113. Mandatory and Default ACP sections



Base Policy

This is the policy which all other policies will be children.

You have unsaved changes

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action
Mandatory - Base Policy (1-1)													
1	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	Allow
Default - Base Policy (-)													

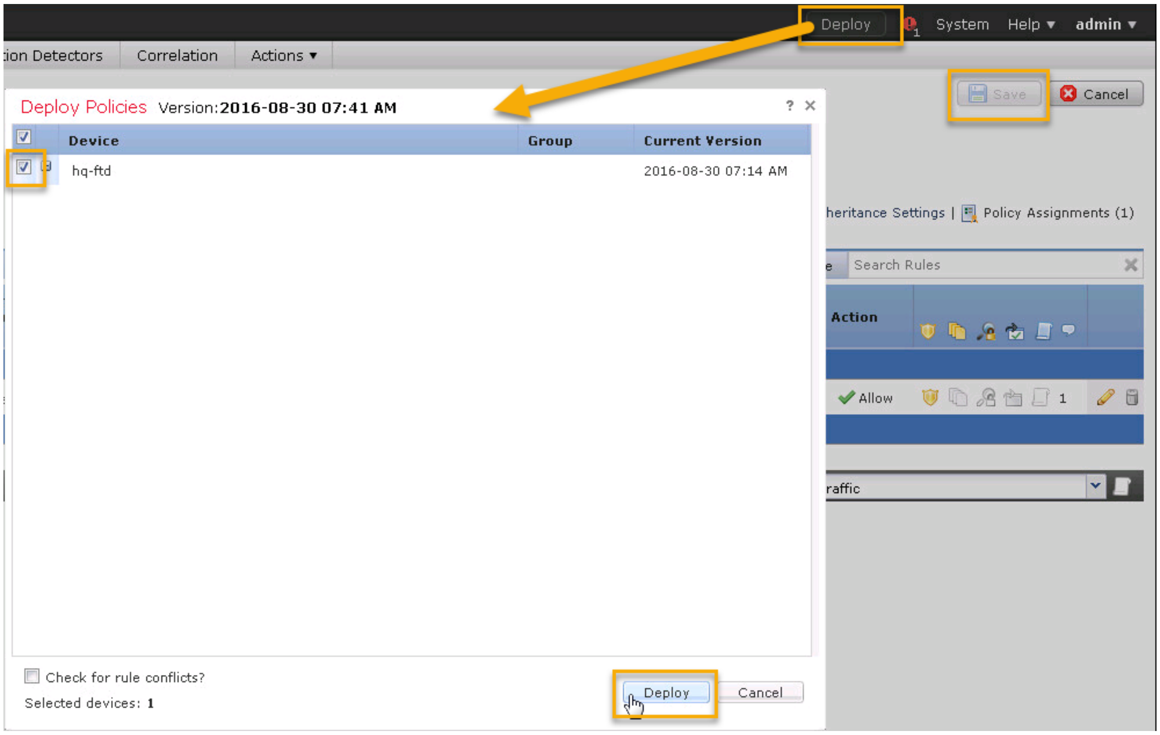
There are no rules in this section. Add Rule or Add Category

Default Action: Access Control: Block All Traffic

33. Click **Save** and then **Deploy**.

34. Select the **hq-ftd** device, and click **Deploy**.

Figure 114. Save and Deploy to hq-ftd



Deploy Policies Version:2016-08-30 07:41 AM

☑	Device	Group	Current Version
☑	hq-ftd		2016-08-30 07:14 AM

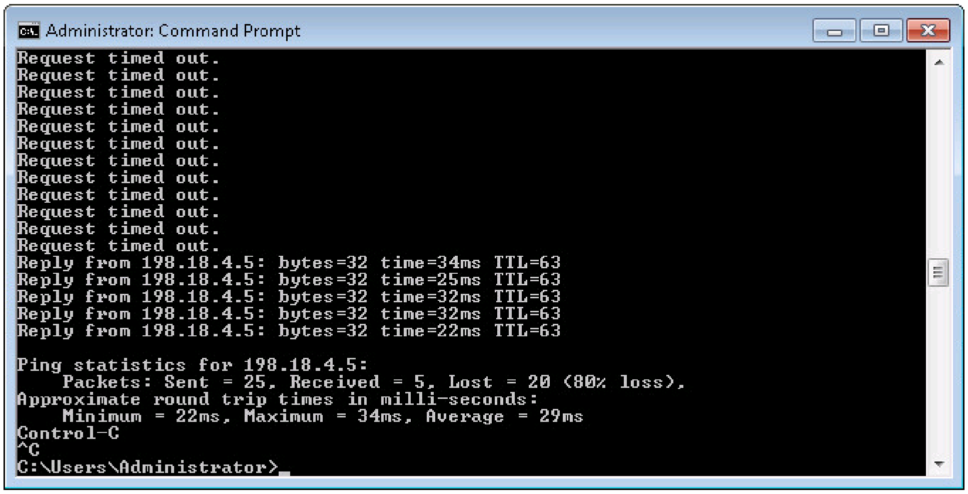
□ Check for rule conflicts?

Selected devices: 1

35. On hq-wkst open an **CMD prompt** and issue the command **ping –t 198.18.4.5**. Once the above policy is applied to hq-ftd these pings should start working.

36. Stop the pings with a **ctrl-c**.

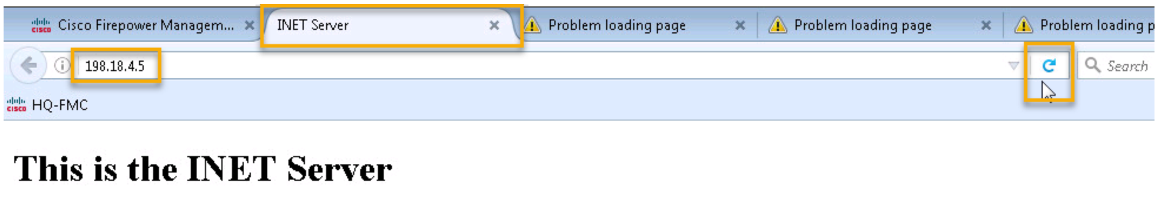
Figure 115. Ping inet-server



```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 198.18.4.5: bytes=32 time=34ms TTL=63
Reply from 198.18.4.5: bytes=32 time=25ms TTL=63
Reply from 198.18.4.5: bytes=32 time=32ms TTL=63
Reply from 198.18.4.5: bytes=32 time=32ms TTL=63
Reply from 198.18.4.5: bytes=32 time=22ms TTL=63

Ping statistics for 198.18.4.5:
    Packets: Sent = 25, Received = 5, Lost = 20 (80% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 34ms, Average = 29ms
Control-C
^C
C:\Users\Administrator>_
```

37. On hq-wkst in **Firefox**, open **http://198.18.4.5** (the second tab in the window). Click **refresh** and you should get the inet-server's web page.

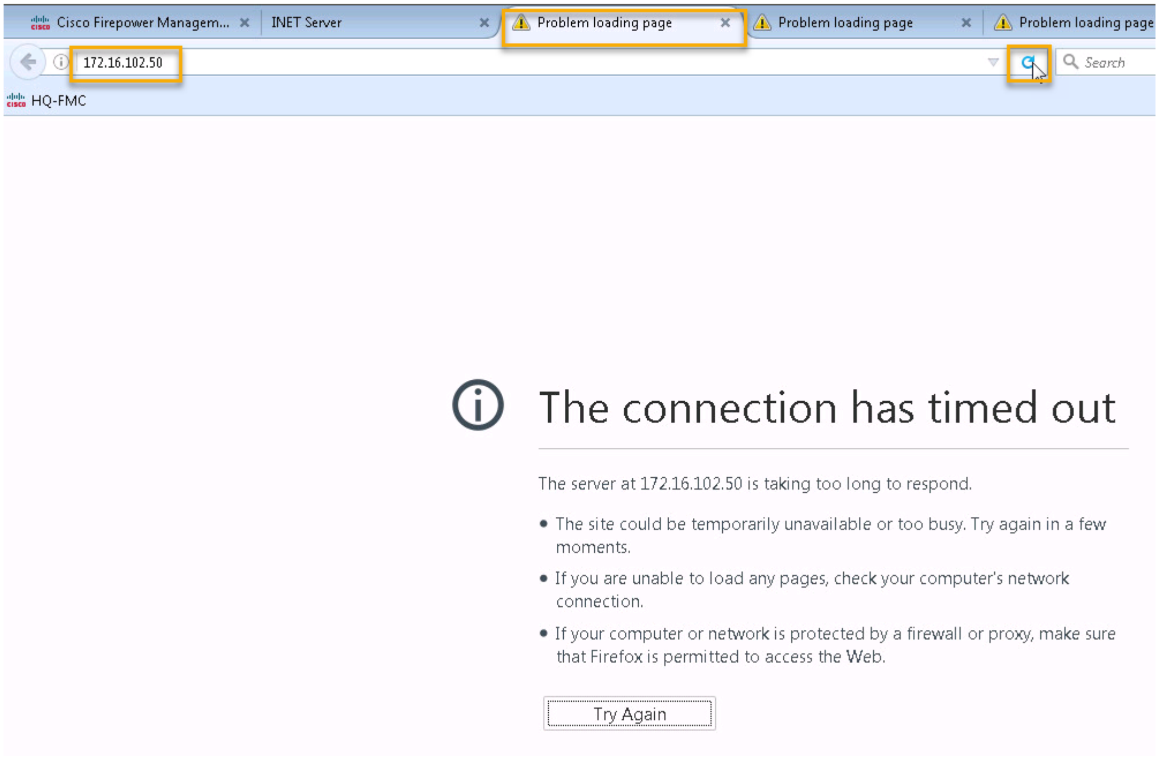
Figure 116. Access inet-server web page



This is the INET Server

38. The 3rd tab is **http://172.16.102.50**, the dmz-server, but this should **not** load. Why?

Figure 117. Failing access to dmz-server web page



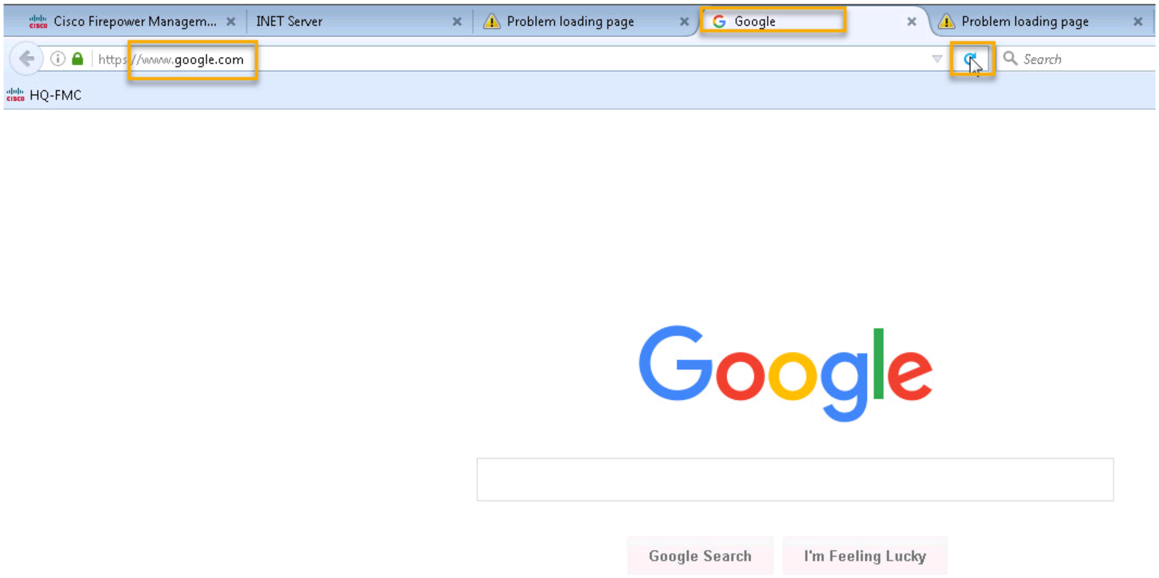
The connection has timed out

The server at 172.16.102.50 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

39. The 4th tab is the Google home page. This page should load.

Figure 118. Access Google web page



40. You can refresh the other tabs if you like but I think we've proven that you have Internet access from the HQ LAN.

In truth this topology could be fully functional by just applying the policy rules to this Base Policy. However, this is a lab environment and I wish to show you a bit about the intricacies of using inheritance between access control policies.

41. You need to move the hq-ftd to a new policy but first you need to create this new policy! In the FMC Administration GUI navigate to **Policies > Access Control > Access Control**.

42. Click the **New Policy** button and use the following to fill out the options:

    a. Name: **HQ Policy**

    b. Description: **Policy used for FTDs at HQ.**

    c. Select Base Policy: **Base Policy**

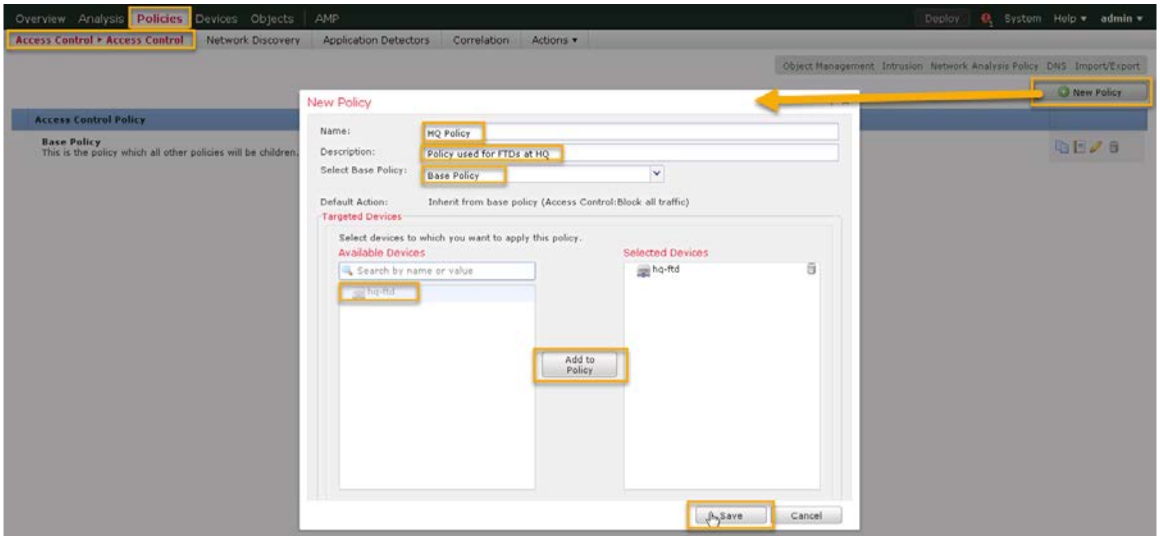
Notice how the “default action” is now inherited from the base policy and not configurable here. If you missed it, select None for the base policy to see the options re-appear. Be sure to end up selecting Base Policy before continuing.

43. Select the **hq-ftd** device from the **Available Devices** and click the **Add to Policy** button.

Note: A device can only be associated to one Access Control Policy at a time. Thus, using this hierarchical (or nested) policy method you can group common policies and then allow other policies to inherit those common policies but then allow them the freedom to set specific items too.

44. Click **Save**.

Figure 119. Create new ACP



Name: HQ Policy

Description: Policy used for FTDs at HQ

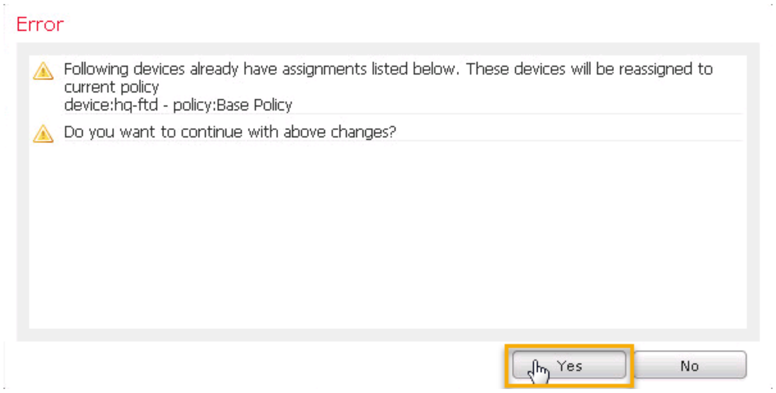
Select Base Policy: Base Policy

Default Action: Inherit from base policy (Access Control:Block all traffic)

Select devices to which you want to apply this policy.

45. Click **Yes** to confirm changing hq-ftd's policy.

Figure 120. Allow hq-ftd to change ACPs



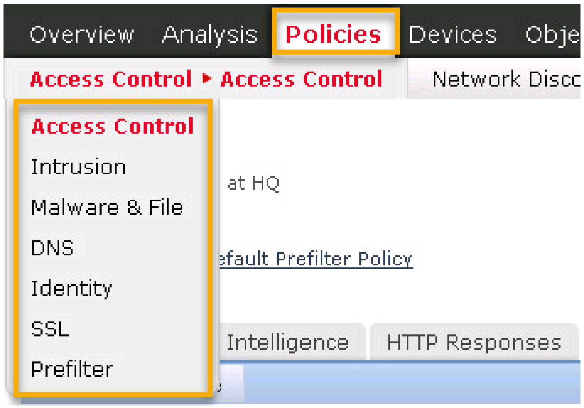
Error

Following devices already have assignments listed below. These devices will be reassigned to current policy
device:hq-ftd - policy:Base Policy

Do you want to continue with above changes?

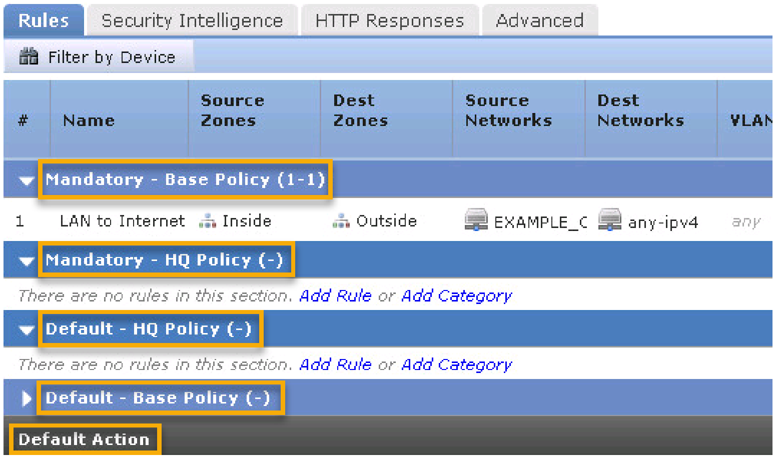
46. Once the policy has been created the FMC will display the configuration page for this policy. There are a LOT of things that can be configured on this page. Additionally, there are all sorts of "policies" that can be attached to an Access Control Policy: Prefilter Policies, SSL Policies, Identity Policies, etc. To get a small glimpse hover your mouse of the Policies > Access Control and see all the list of policy options. Each of these "other" policies are used by attaching them to an Access Control Policy.

Figure 121. Lots of Policies



47. Though you haven't created any policies yet for the HQ Policy access control policy you can see that the Base Policy rules are present. Expand the **Mandatory – Base Policy** section to see the previously created rule permitting Example Corp LAN IPs. Also, notice that you have 4 sections of rules. 2 sections are related to any rules created in the Base Policy and 2 sections are for any rules created in the HQ Policy section. The rules are processed in a top down fashion. (You can click the arrow icon next to each section to expand or contract that section for better viewing.)

Figure 122. Nesting of ACP sections



#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN
Mandatory - Base Policy (1-1)						
1	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any
Mandatory - HQ Policy (-)						
There are no rules in this section. Add Rule or Add Category						
Default - HQ Policy (-)						
There are no rules in this section. Add Rule or Add Category						
Default - Base Policy (-)						
Default Action						

48. To prove a point let's assume that for some reason you want to block the HQ LAN from accessing the Internet. Click the **Add Rule** button. You are going to create a rule exactly like the one you just created in the Base Policy but this time you will set the Action to block.

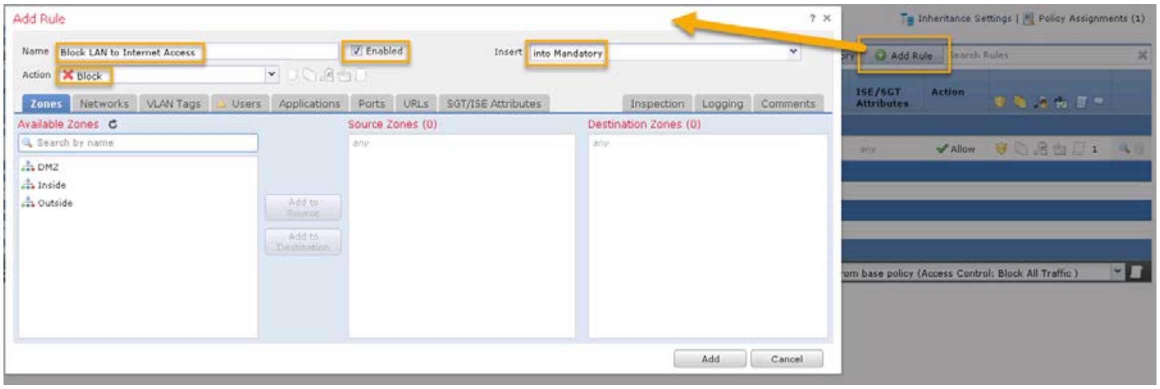
    a. Name: **Block LAN to Internet Access**

    b. Enabled: **Checked**

    c. Insert: **into Mandatory**

    d. Action: **Block**

Figure 123. Part 1 of adding rule


Add Rule

Name: Block LAN to Internet Access ☑ Enabled Insert: into Mandatory

Action: ✗ Block

Available Zones: DMZ, Inside, Outside

Source Zones (0): any

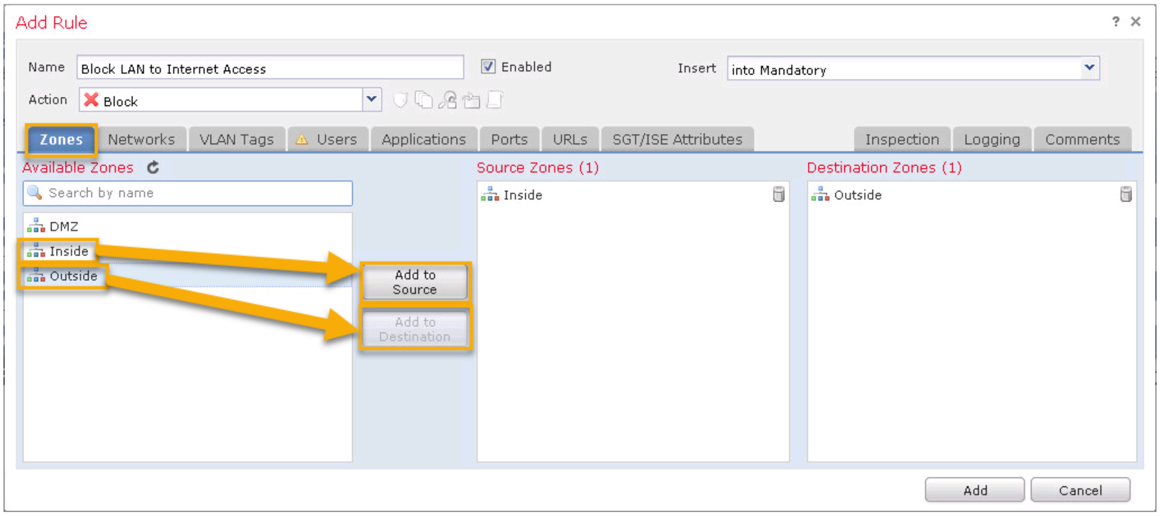
Destination Zones (0): any

49. On the **Zones tab**:

    a. From the **Available Zones** select **Inside** and then click the **Add to Source** button.

    b. From the **Available Zones** select **Outside** and then click the **Add to Destination** button.

Figure 124. Configure Zones tab



Add Rule

Name: Block LAN to Internet Access

☑ Enabled

Insert: into Mandatory

Action: Block

Available Zones: DMZ, Inside, Outside

Source Zones (1): Inside

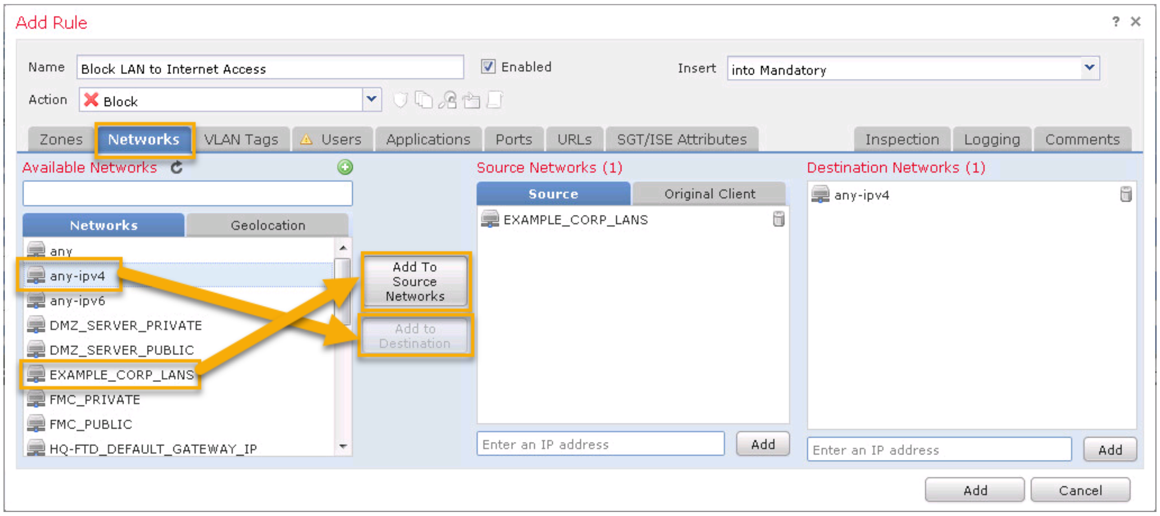
Destination Zones (1): Outside

50. On the **Networks tab**:

    a. From the **Available Networks** select **EXAMPLE_CORP_LANS** and then click the **Add to Source Networks** button.

    b. From the **Available Networks** select **any-ipv4** and then click the **Add to Destination** button.

Figure 125. Configure Networks tab



Add Rule

Name: Block LAN to Internet Access

☑ Enabled

Insert: into Mandatory

Action: Block

Available Networks: any, any-ipv4, any-ipv6, DMZ_SERVER_PRIVATE, DMZ_SERVER_PUBLIC, EXAMPLE_CORP_LANS, FMC_PRIVATE, FMC_PUBLIC, HQ-FTD_DEFAULT_GATEWAY_IP

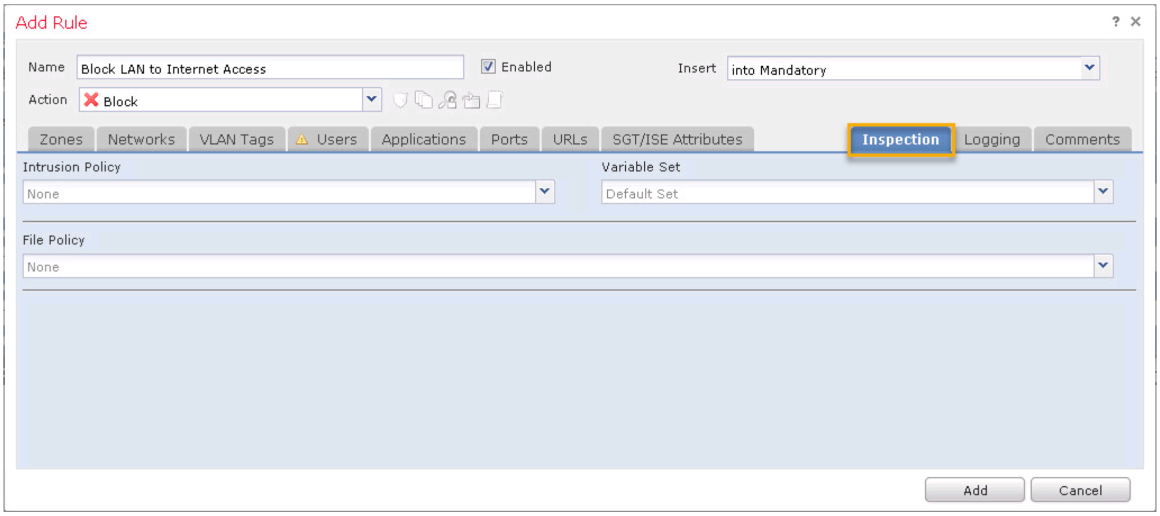
Source Networks (1): EXAMPLE_CORP_LANS

Destination Networks (1): any-ipv4

51. On the **Inspection tab**:

    a. Intrusion Policy: Notice that because your Action is Block you cannot set any of these fields.

Figure 126. Can't configure Inspection tab



Add Rule

Name: Block LAN to Internet Access

☑ Enabled

Insert: into Mandatory

Action: Block

Intrusion Policy: None

Variable Set: Default Set

File Policy: None

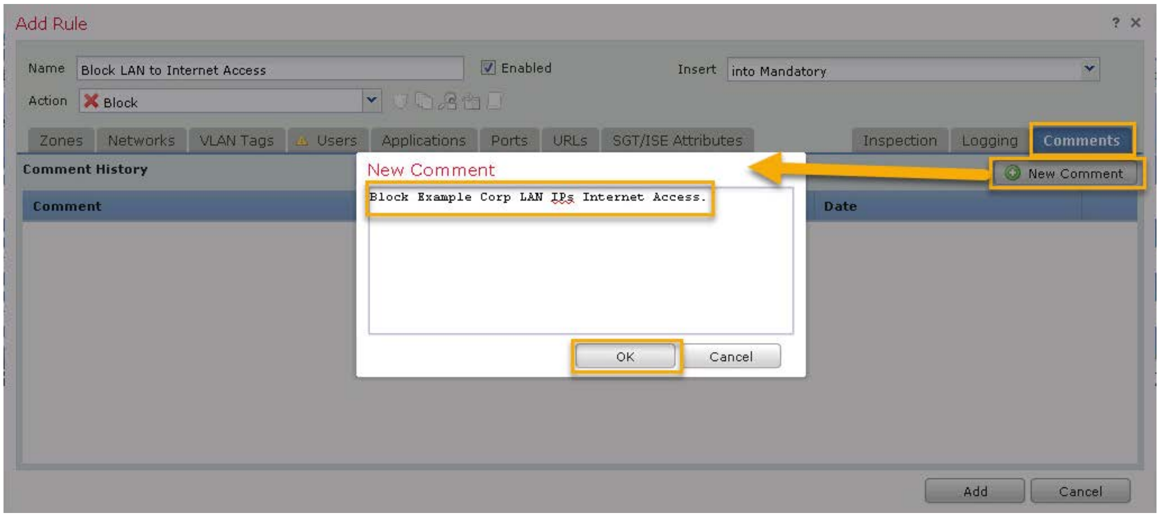
52. On the **Comments tab**:

    a. Click **New Comment**

    b. New Comment: **Block Example Corp LAN IPs Internet Access.**

    c. Click **OK.**

Figure 127. Add a comment



Add Rule

Name: Block LAN to Internet Access

☑ Enabled

Insert: into Mandatory

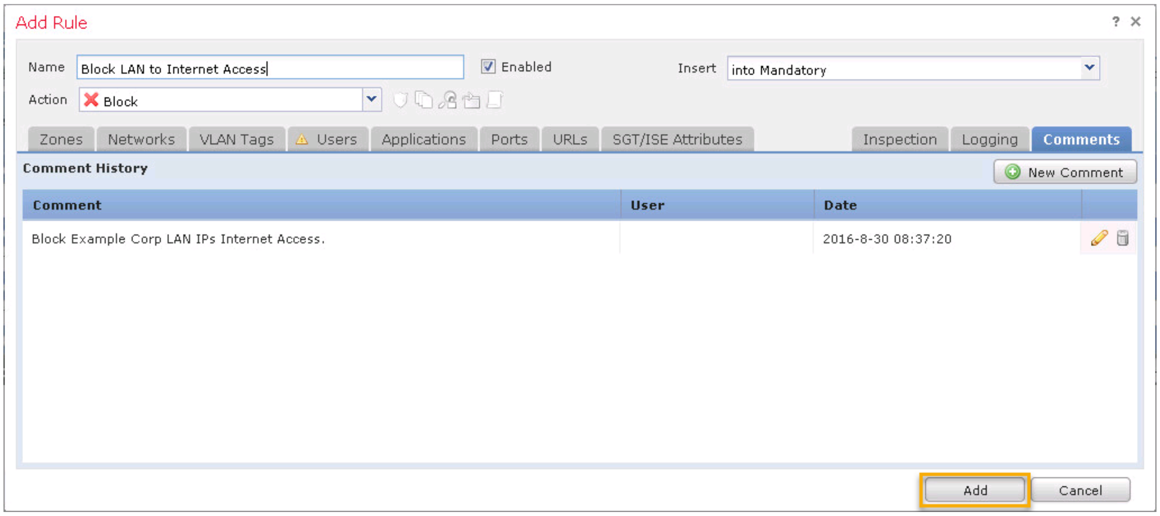
Action: Block

New Comment

Block Example Corp LAN IPs Internet Access.

53. Click **Add**.

Figure 128. Add rule



Add Rule

Name: Block LAN to Internet Access

☑ Enabled

Insert: into Mandatory

Action: Block

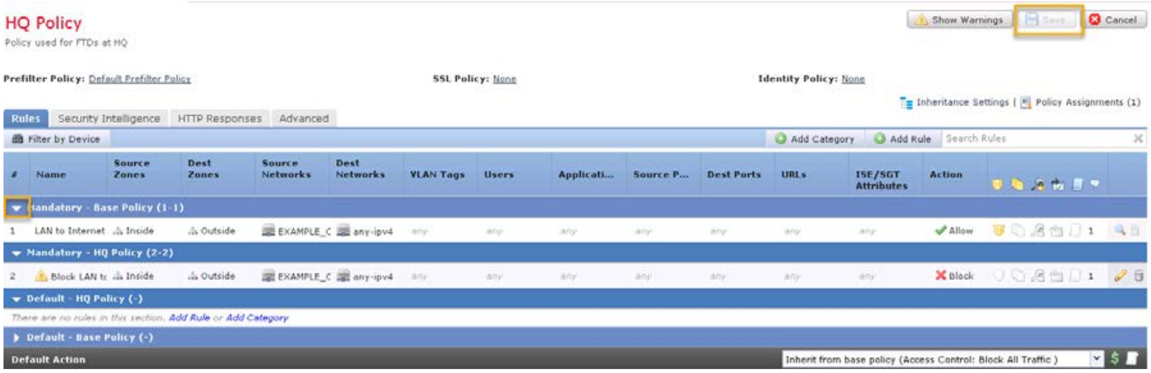
Comment History

Comment	User	Date
Block Example Corp LAN IPs Internet Access.		2016-8-30 08:37:20

54. Click **Save**.

55. Expand the **Mandatory – Base Policy** section again. Note that the previous rule still exists and its hierarchical relation to the newly created rule.

Figure 129. Save and Expand Mandatory – Base Policy section



HQ Policy

Policy used for FTDs at HQ

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

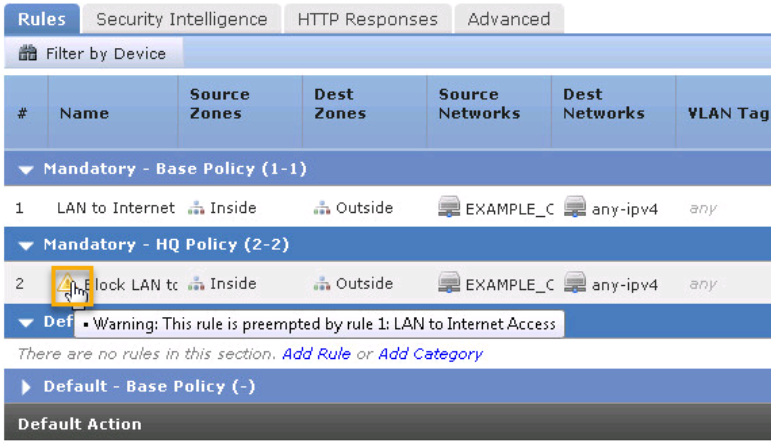
Identity Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action
‌andatory - Base Policy (1-1)													
1	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✓ Allow
Mandatory - HQ Policy (2-2)													
2	⚠ Block LAN tc	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✖ Block
Default - HQ Policy (-)													
There are no rules in this section. Add Rule or Add Category													
Default - Base Policy (-)													

Default Action: Inherit from base policy (Access Control: Block All Traffic)

56. Notice the **yellow triangle** next to the newly created rule. Hover your mouse over it and read the message. There is also a **Show Warnings button** next to the Save button that tells you the same information. FTD is smart enough to recognize that this rule will not be reached since the rule in the Mandatory – Base Policy comes first and encompasses all that is in this new rule. How can you fix this?

Figure 130. Yellow triangle warning

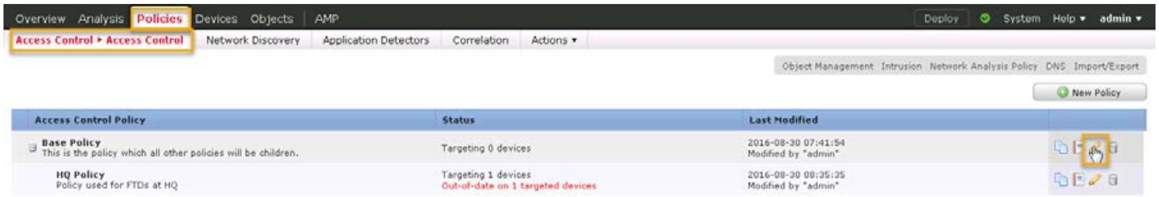


#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tag
Mandatory - Base Policy (1-1)						
1	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any
Mandatory - HQ Policy (2-2)						
2	Block LAN tc	Inside	Outside	EXAMPLE_C	any-ipv4	any
Def						
There are no rules in this section. Add Rule or Add Category						
Default - Base Policy (-)						
Default Action						

• Warning: This rule is preempted by rule 1: LAN to Internet Access

57. Navigate to the **Policies > Access Control > Access Control** page and click the **pencil icon** on the **Base Policy** line.

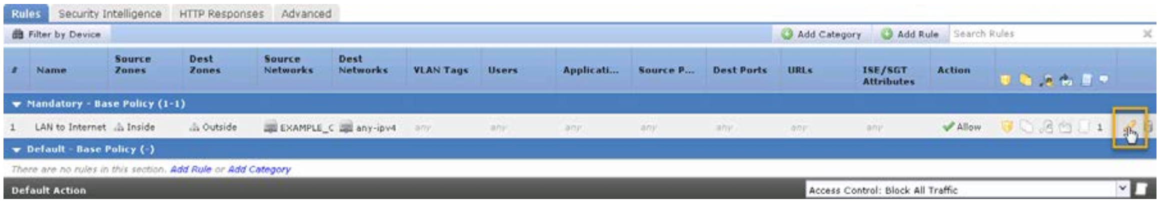
Figure 131. Edit Base Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-30 07:41:54 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Out-of-date on 1 targeted devices	2016-08-30 08:35:35 Modified by "admin"

58. Click the **pencil icon** on the **LAN to Internet Access** line.

Figure 132. Edit ACP rule



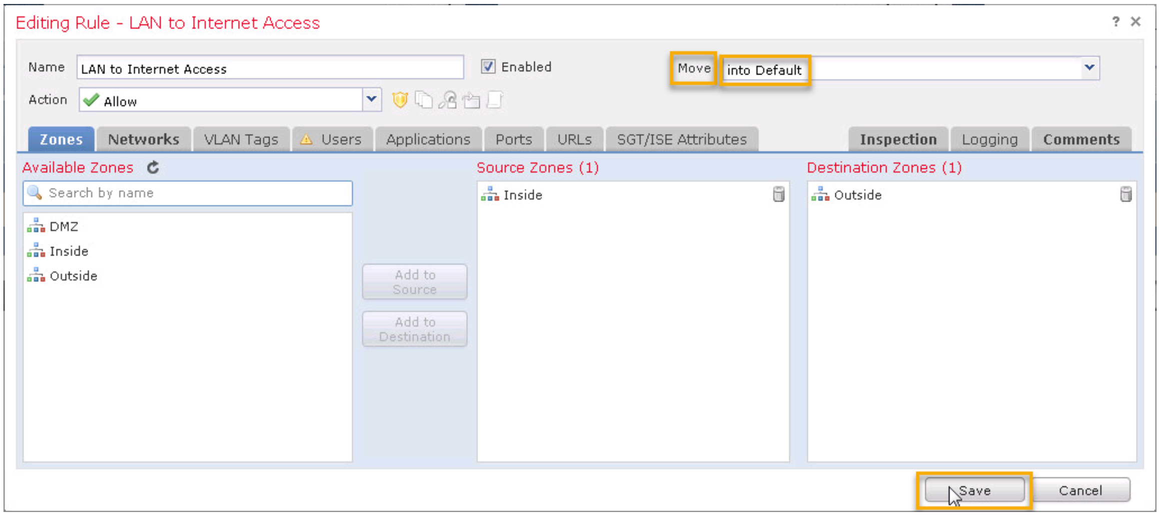
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action
Mandatory - Base Policy (1-1)													
1	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✓ Allow
Default - Base Policy (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													Access Control: Block All Traffic

59. Click the **Move** link.

60. Using the dropdown select **into Default**.

61. Click **Save** to save the change to this rule.

Figure 133. Move rule to into Default



Editing Rule - LAN to Internet Access

Name: LAN to Internet Access ☑ Enabled Move: into Default

Action: Allow

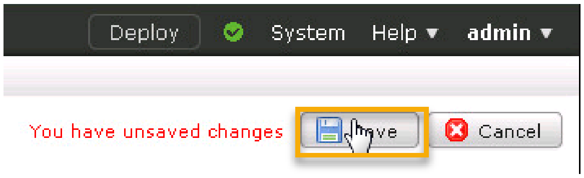
Available Zones: DMZ, Inside, Outside

Source Zones (1): Inside

Destination Zones (1): Outside

62. Click **Save** to save your changes.

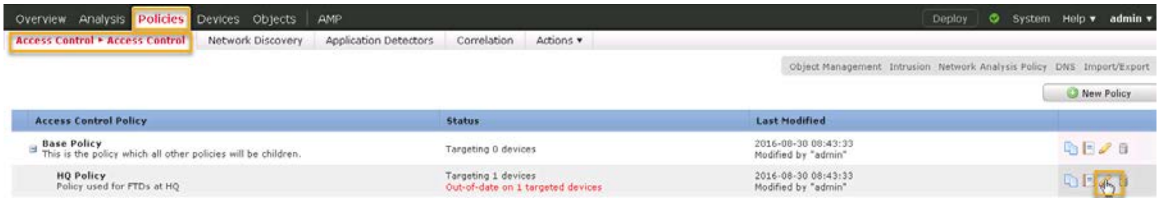
Figure 134. Save changes to FMC



You have unsaved changes

63. Return to editing the HQ Policy rule. (Navigate to **Policies > Access Control > Access Control**, click on the **pencil icon** on the row for **HQ Policy**.)

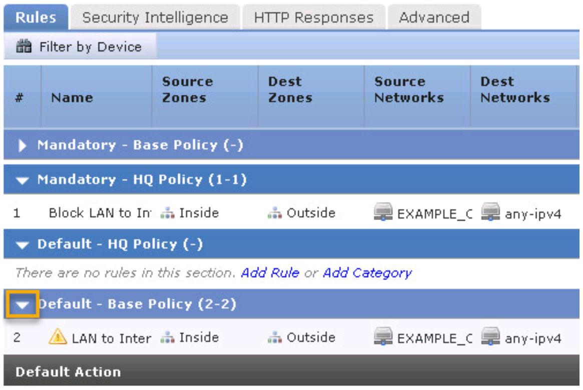
Figure 135. Edit HQ Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-30 08:43:33 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Out-of-date on 1 targeted devices	2016-08-30 08:43:33 Modified by "admin"

64. Expand the **Default – Base Policy** section and note that the LAN to Internet Access rule now has the yellow triangle warning us that it is being usurped by the Block LAN to Internet Access rule in the Mandatory – HQ Policy section. So what have you learned? The child policy is sandwiched between the parent policy's Mandatory and Default sections.

Figure 136. Order of ACP rules is important



Rules | Security Intelligence | HTTP Responses | Advanced

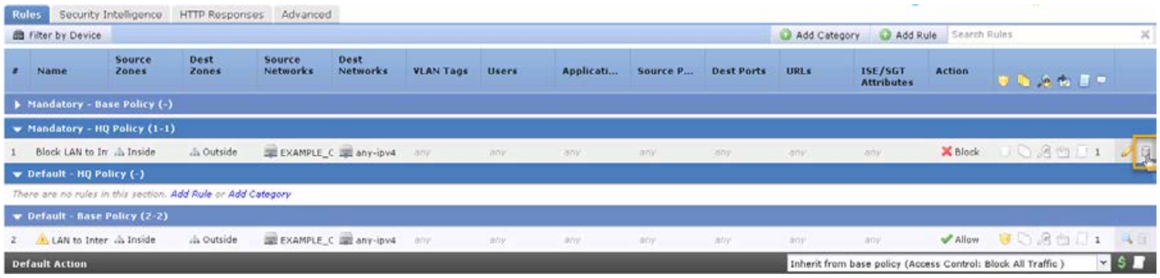
Filter by Device

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - Base Policy (-)					
Mandatory - HQ Policy (1-1)					
1	Block LAN to In	Inside	Outside	EXAMPLE_C	any-ipv4
Default - HQ Policy (-)					
There are no rules in this section. Add Rule or Add Category					
Default - Base Policy (2-2)					
2	⚠ LAN to Inter	Inside	Outside	EXAMPLE_C	any-ipv4
Default Action					

If you were to create a new Access Control Policy that then inherited the HQ Policy as its parent you'd see it was sandwiched between the HQ Policy's Mandatory and Default sections that were in turn sandwiched between the Base Policy's Mandatory and Default sections.

65. You really don't want to block all LAN traffic at HQ so let's delete the rule you created that is in the Mandatory – HQ Policy section. Click the **trashcan icon** on the row associated with the **Block LAN to Internet Access** rule.

Figure 137. Delete Block rule



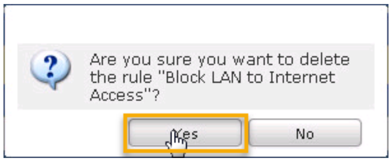
Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device | Add Category | Add Rule | Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
Mandatory - Base Policy (-)														
Mandatory - HQ Policy (1-1)														
1	Block LAN to In	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✗ Block	1
Default - HQ Policy (-)														
There are no rules in this section. Add Rule or Add Category														
Default - Base Policy (2-2)														
2	⚠ LAN to Inter	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✓ Allow	1
Default Action													Inherit from base policy (Access Control: Block All Traffic)	

66. Click **Yes** to confirm deleting this rule.

Figure 138. Confirm deletion



Are you sure you want to delete the rule "Block LAN to Internet Access"?

Yes | No

67. Since you are still modifying the HQ Policy policy let's finish out what you need for the DMZ. The DMZ server has SSH, FTP, and HTTP services running of which all should be accessible from HQ LAN but only HTTP should be accessible from other places (like the Internet or the Remote locations). Click **Add Rule** to create a new rule and then use the following to fill in the details:

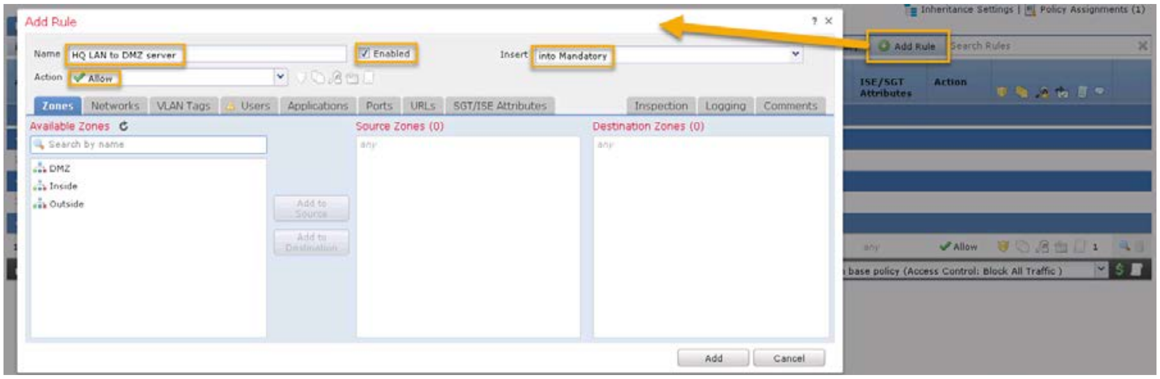
    a. Name: **HQ LAN to DMZ server**

    b. Enabled: **Checked**

    c. Insert: **into Mandatory**

    d. Action: **Allow**

Figure 139. Part 1 of adding a rule



Add Rule

Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

Available Zones: DMZ, Inside, Outside

Source Zones (0): any

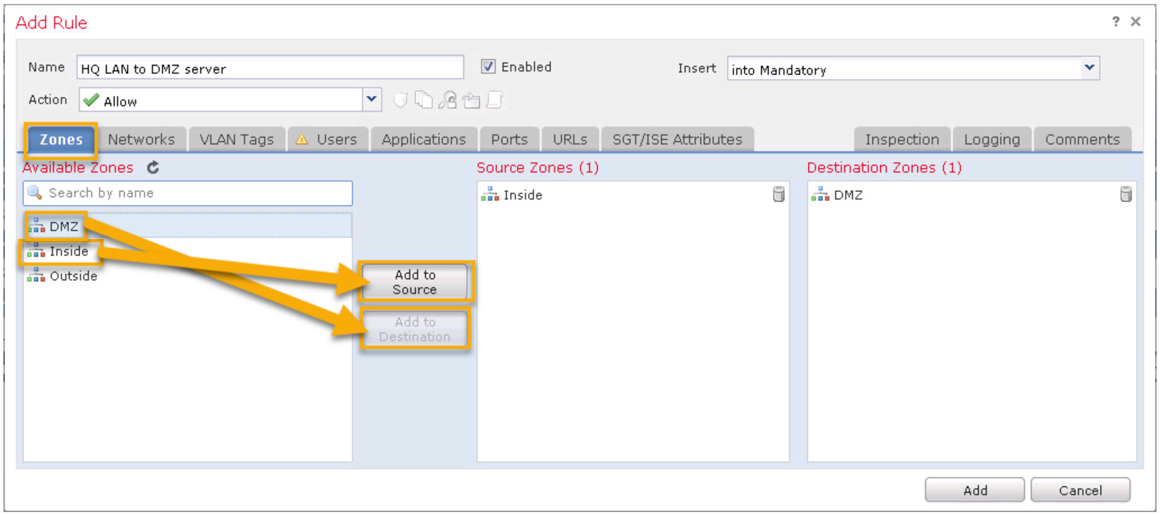
Destination Zones (0): any

68. In the **Zones tab**:

    a. From the **Available Zones** select **Inside** and then click the **Add to Source** button.

    b. From the **Available Zones** select **DMZ** and then click the **Add to Destination** button.

Figure 140. Configure Zones tab



Add Rule

Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

Available Zones: DMZ, Inside, Outside

Source Zones (1): Inside

Destination Zones (1): DMZ

69. On the **Networks tab**:

   a. You don't have an object created for the HQ LAN network yet. Click the **green plus icon** next to Available Networks.

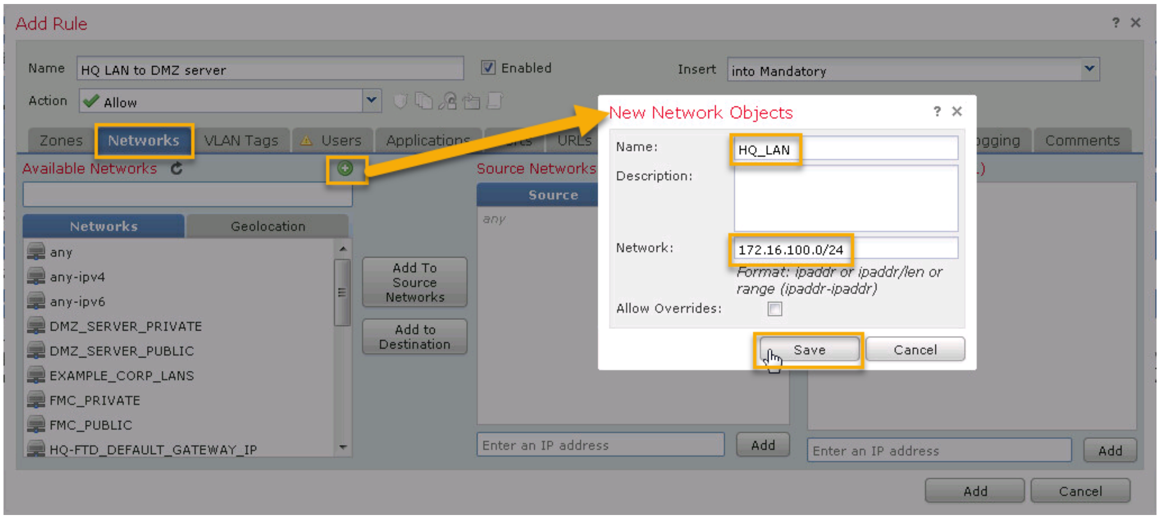
   b. In the New Network Objects window fill out the following:

      i. Name: **HQ_LAN**

      ii. Network: **172.16.100.0/24**

      iii. Click **Save**.

Figure 141. Create Network Object



Add Rule

Name: HQ LAN to DMZ server ☑ Enabled Insert: into Mandatory

Action: ✓ Allow

New Network Objects

Name: HQ_LAN

Description:

Network: 172.16.100.0/24

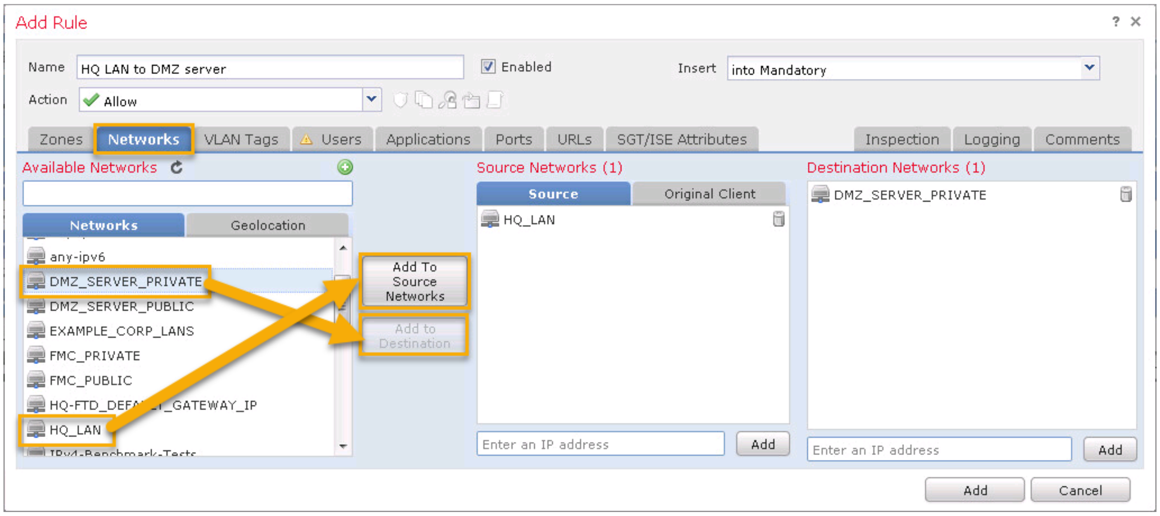
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides: □

   c. From the **Available Networks** select **HQ_LAN** and then click the **Add to Source Networks** button.

   d. From the **Available Networks** select **DMZ_SERVER_PRIVATE** and then click the **Add to Destination** button.

Figure 142. Configure Networks tab



Add Rule

Name: HQ LAN to DMZ server ☑ Enabled Insert: into Mandatory

Action: ✓ Allow

Source Networks (1): HQ_LAN

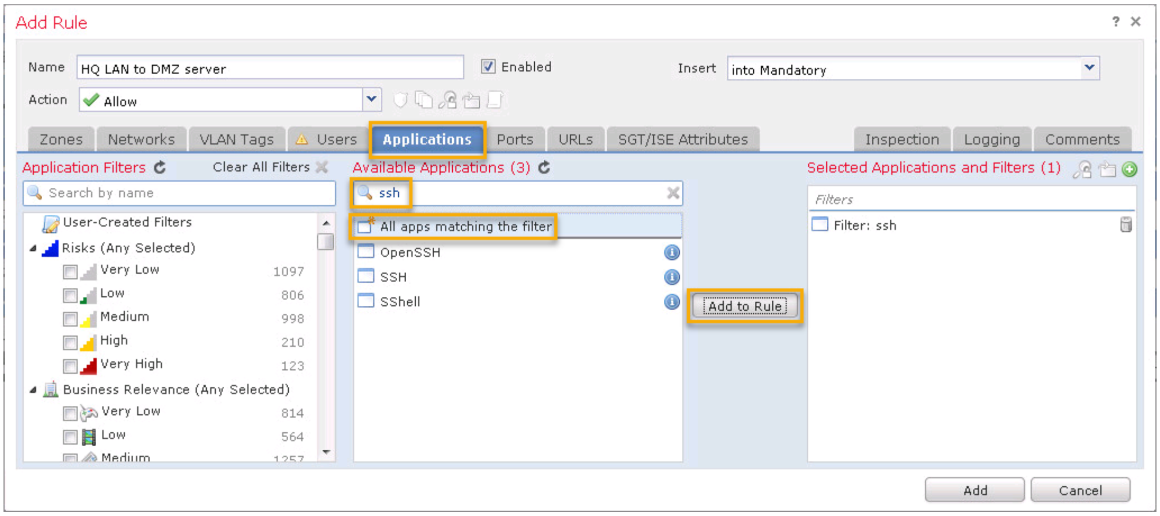
Destination Networks (1): DMZ_SERVER_PRIVATE

70. On the **Applications tab**:

   a. In the **Available Applications** search window type in **ssh**.

   b. Select the **All apps matching the filter** option from **Available Applications** and click the **Add to Rule** button.

Figure 143. Add ssh to rule



Add Rule

Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

Action: Allow

Available Applications (3)

ssh

Selected Applications and Filters (1)

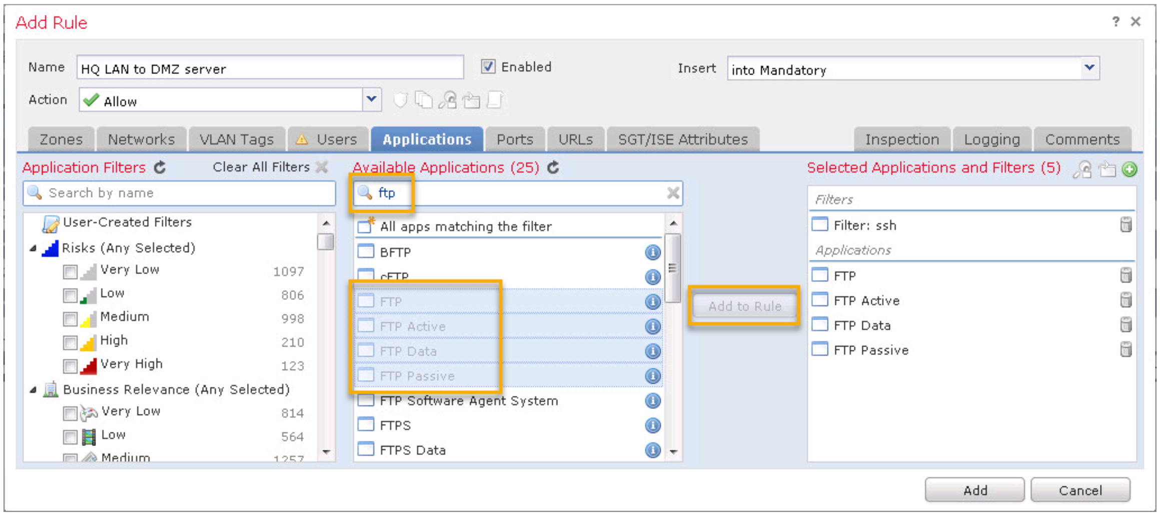
Filters

Filter: ssh

   c. In the **Available Applications** search window type in **ftp**.

   d. Select **FTP**, and then while holding the **SHIFT button** select **FTP Passive** (which will select the options in between as well) from the **Available Applications**. Click the **Add to Rule** button.

Figure 144. Add ftp to rule



Add Rule

Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

Action: Allow

Available Applications (25)

ftp

Selected Applications and Filters (5)

Filters

Filter: ssh

Applications

FTP

FTP Active

FTP Data

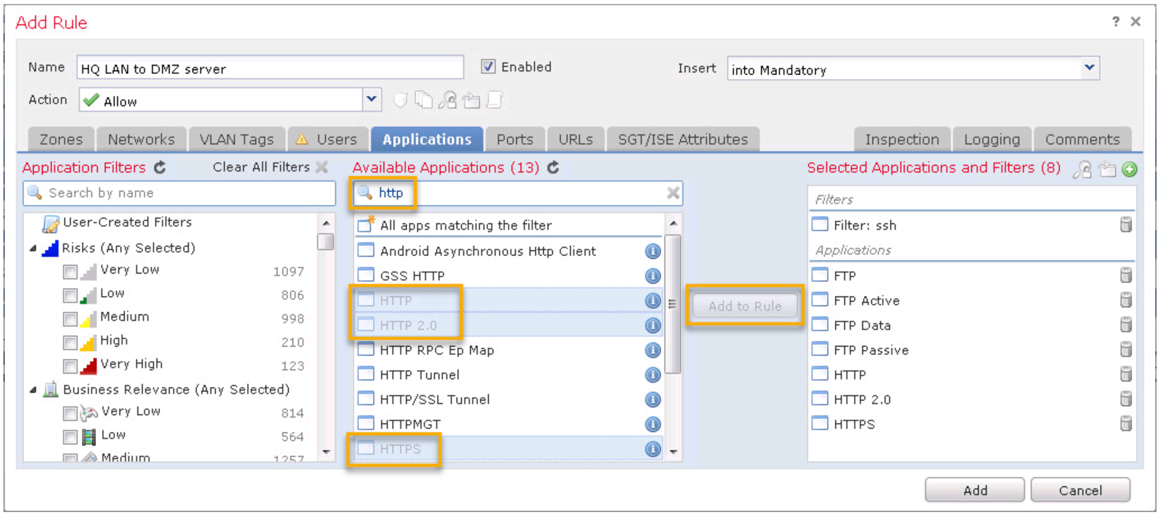
FTP Passive

e. In the **Available Applications** search window type in **http**.

f. While **holding down Ctrl** select **HTTP**, **HTTP 2.0**, and **HTTPS** options from **Available Applications** and then click the **Add to Rule** button.

The HTML5 server we are using (Guacamole) doesn't support holding SHIFT (or CTRL). Just select each and add them individually.

Figure 145. Add http/https to rule



Add Rule

Name: HQ LAN to DMZ server
☑ Enabled
Insert: into Mandatory
Action: ✓ Allow

Application Filters

- User-Created Filters
- Risks (Any Selected)
  - □ Very Low 1097
  - □ Low 806
  - □ Medium 998
  - □ High 210
  - □ Very High 123
- Business Relevance (Any Selected)
  - □ Very Low 814
  - □ Low 564
  - □ Medium 1257

Available Applications (13)

Search: http

- All apps matching the filter
- Android Asynchronous Http Client
- GSS HTTP
- HTTP
- HTTP 2.0
- HTTP RPC Ep Map
- HTTP Tunnel
- HTTP/SSL Tunnel
- HTTPMGT
- HTTPS

Selected Applications and Filters (8)

Filters

- Filter: ssh

Applications

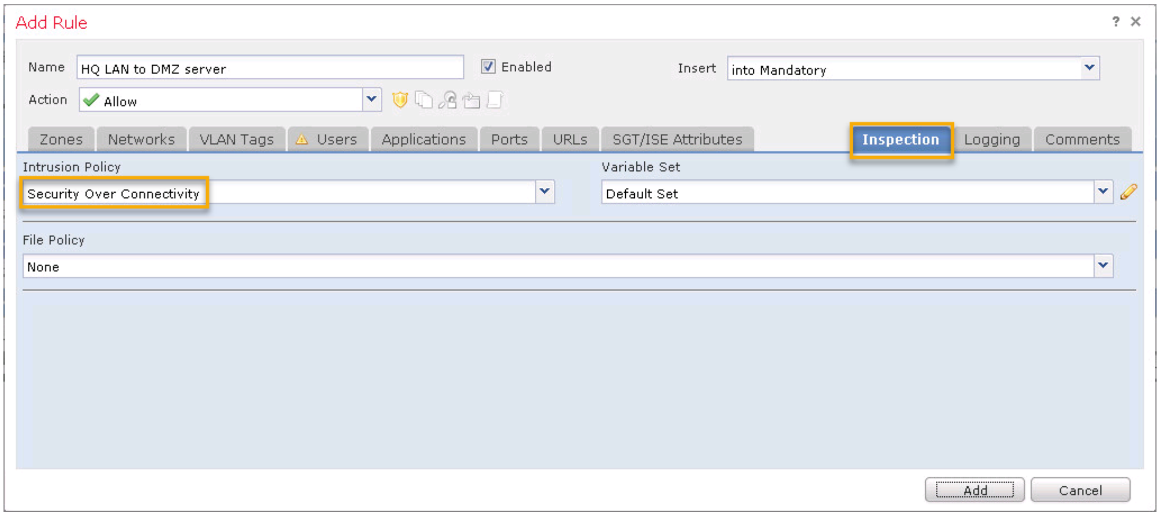
- FTP
- FTP Active
- FTP Data
- FTP Passive
- HTTP
- HTTP 2.0
- HTTPS

Notice that you can select All apps matching a filter, some of them in a row (using Shift), or some of them not continuously next to each other (using Ctrl). Also, did you notice how you didn't specify any UDP or TCP ports? The FTD actually goes well beyond just filtering based on "ports and protocols" of a traditional firewall. It will check the data stream and interpret whether this flow of traffic matches a particular rule no matter what port it is coming in on. For example, this rule would still be able to identify an HTTP connection even if that connection came in on port 8080, or 12345!

71. On the **Inspection tab**:

    a. Intrusion Policy: **Security Over Connectivity**

Figure 146. Configure Inspection tab



Add Rule

Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

Intrusion Policy: Security Over Connectivity

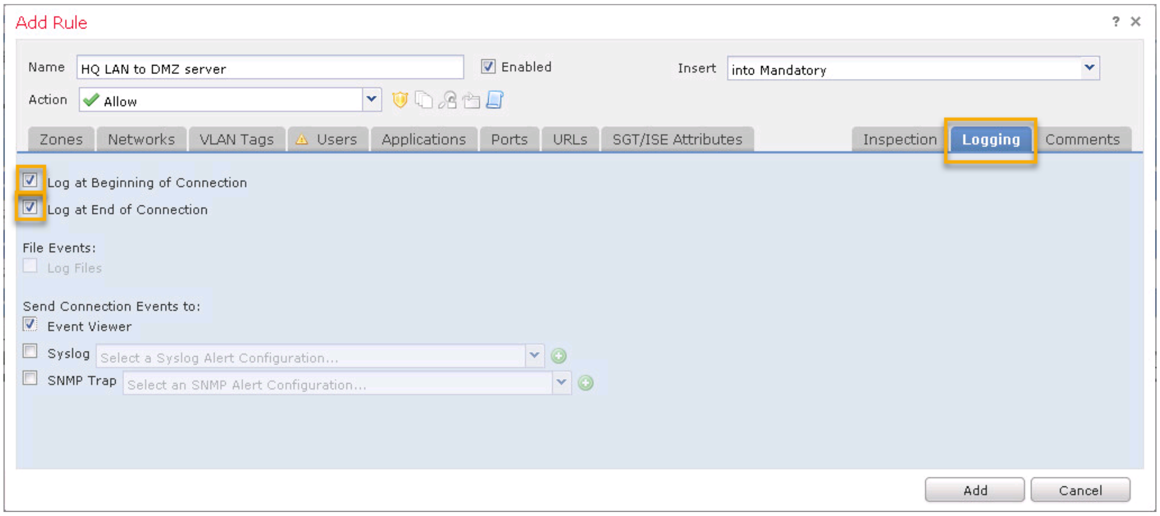
Variable Set: Default Set

File Policy: None

72. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** and **Log at the End of Connection** buttons. These options will allow us to know when someone accesses these applications from HQ LAN and when they close their connections too.

Figure 147. Configure the Logging tab



Add Rule

Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

☑ Log at Beginning of Connection

☑ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

□ Syslog: Select a Syslog Alert Configuration...

□ SNMP Trap: Select an SNMP Alert Configuration...

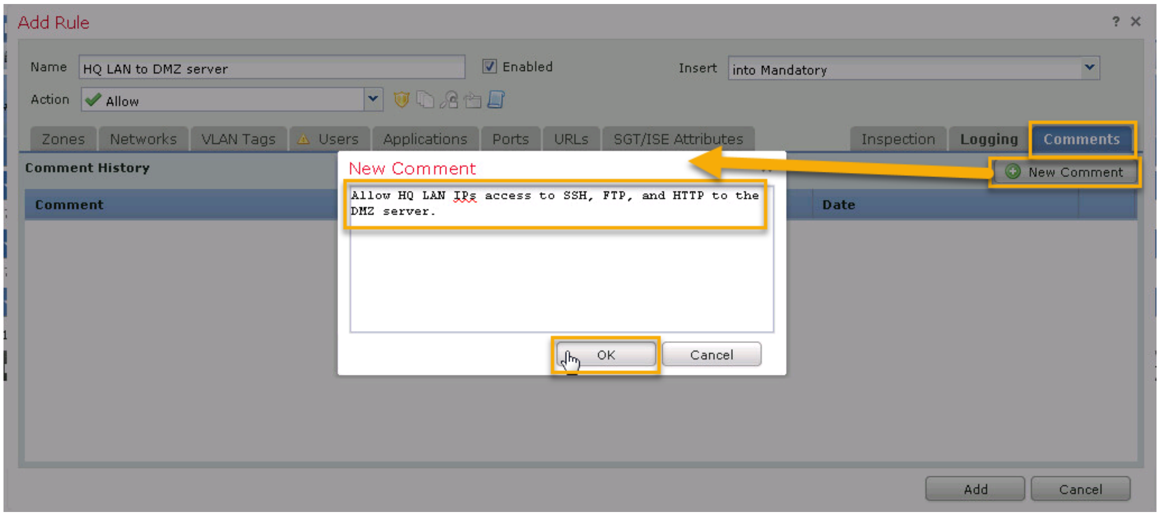
73. On the **Comments tab**:

    a. Click **New Comment**

    b. New Comment: **Allow HQ LAN IPs access to SSH, FTP, and HTTP to the DMZ server.**

    c. Click **OK**

Figure 148. Create comment



Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

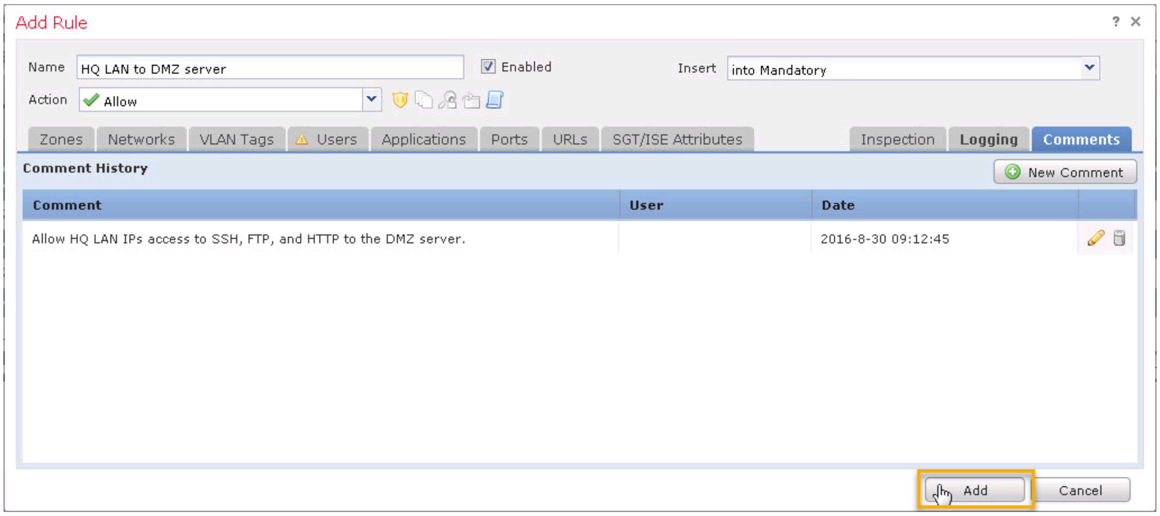
Action: ✓ Allow

New Comment

```
Allow HQ LAN IPs access to SSH, FTP, and HTTP to the
DMZ server.
```

74. Click **Add**.

Figure 149. Add the ACP rule



Name: HQ LAN to DMZ server

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

Comment History

Comment	User	Date
Allow HQ LAN IPs access to SSH, FTP, and HTTP to the DMZ server.		2016-8-30 09:12:45

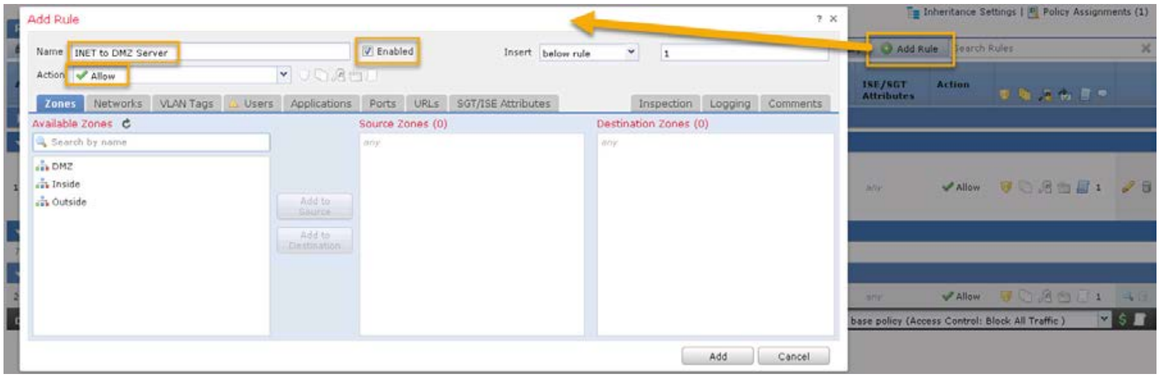
75. Create another rule only allowing HTTP access from the Internet to DMZ_Server. Click **Add Rule** and then use the following information to fill out the needed options:

    a. Name: **INET to DMZ Server**

    b. Enabled: **Checked**

    c. Action: **Allow**

Figure 150. Part 1 of adding ACP rule



Add Rule

Name: INET to DMZ Server

☑ Enabled

Action: ✓ Allow

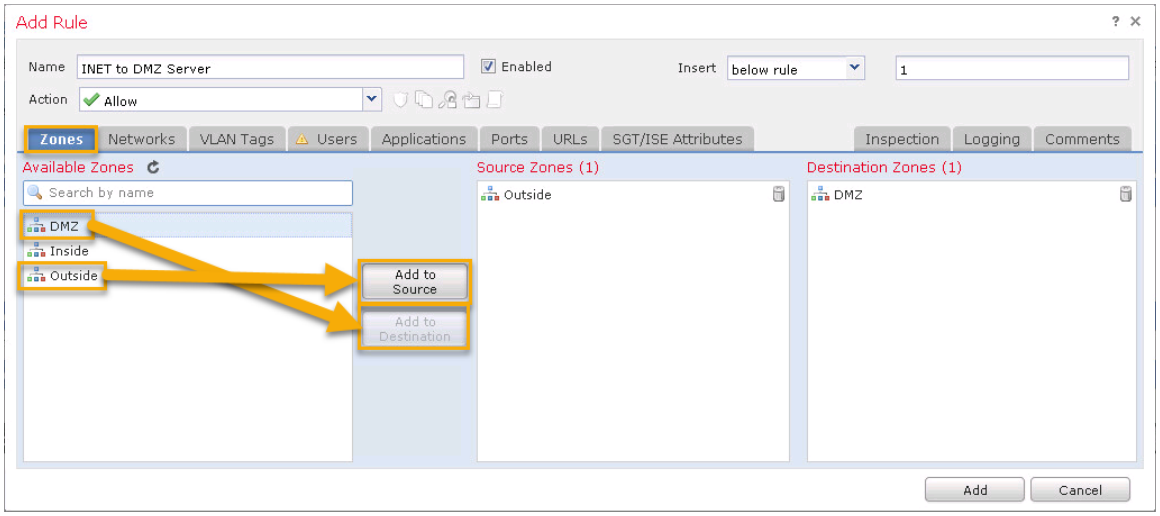
Insert: below rule 1

76. In the **Zones tab**:

    a. From the **Available Zones** select **Outside** and then click the **Add to Source** button.

    b. From the **Available Zones** select **DMZ** and then click the **Add to Destination** button.

Figure 151. Configure Zones tab



Add Rule

Name: INET to DMZ Server

☑ Enabled

Action: ✓ Allow

Insert: below rule 1

Source Zones (1): Outside

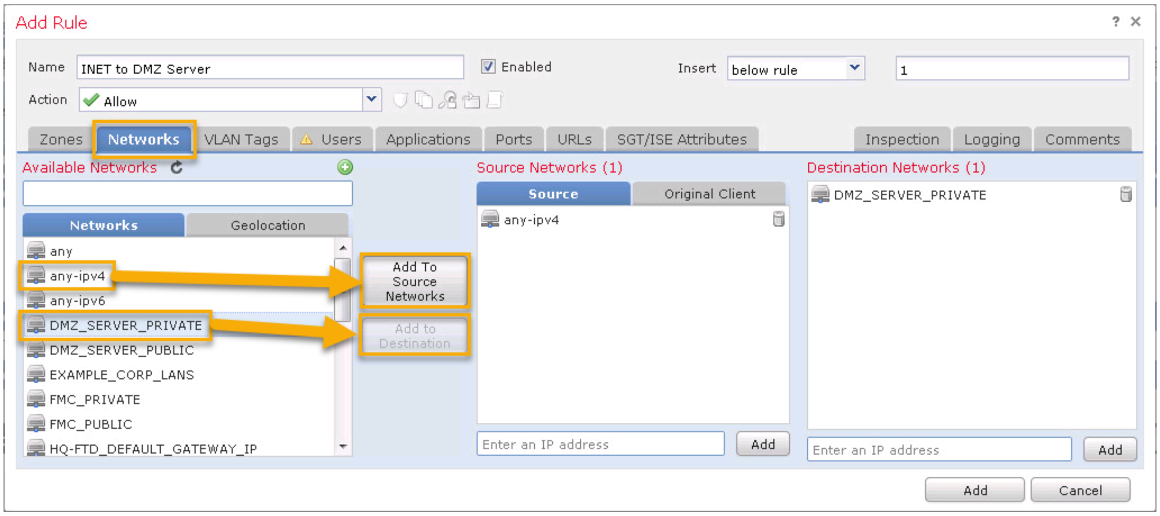
Destination Zones (1): DMZ

77. On the **Networks tab**:

    a. From the **Available Networks** list select **any-ipv4** and then click the **Add to Source Networks** button.

    b. From the **Available Networks** list select **DMZ_SERVER_PRIVATE** and then click the **Add to Destination** button.

Figure 152. Configure Networks tab



Add Rule

Name: INET to DMZ Server ☑ Enabled Insert: below rule 1

Action: ✓ Allow

Zones | **Networks** | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks

Networks | Geolocation

- any
- any-ipv4
- any-ipv6
- DMZ_SERVER_PRIVATE
- DMZ_SERVER_PUBLIC
- EXAMPLE_CORP_LANS
- FMC_PRIVATE
- FMC_PUBLIC
- HQ-FTD_DEFAULT_GATEWAY_IP

Source Networks (1)

Source | Original Client

- any-ipv4

Destination Networks (1)

- DMZ_SERVER_PRIVATE

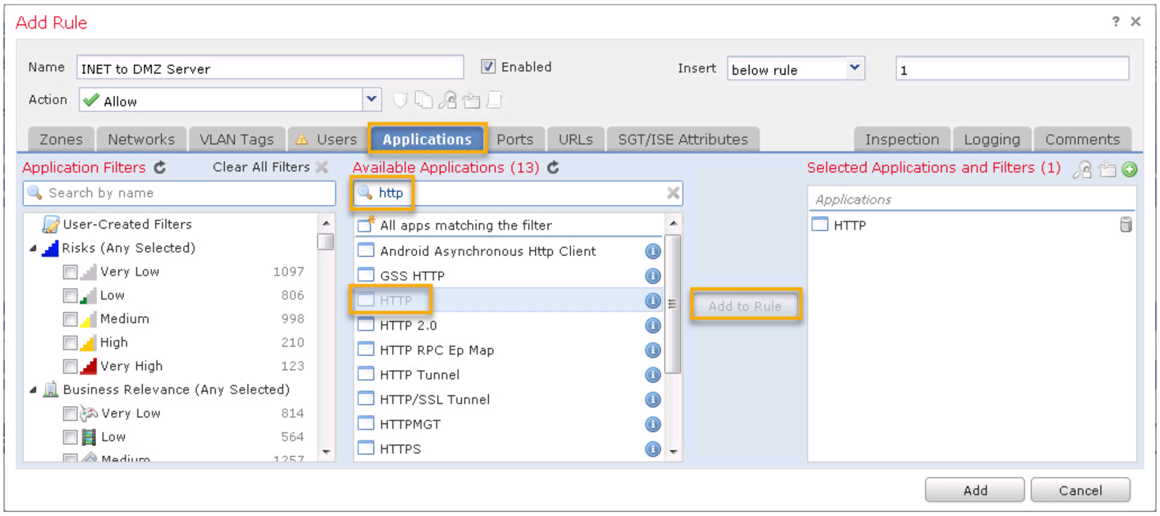
NOTE: NAT translation occurs before access control policies so you need to match against the post-NAT'ted address.

78. On the **Applications tab**:

    a. In the **Available Applications** section search for **http**.

    b. Select the **HTTP** result and click the **Add to Rule** button. (You could select the other options as you did in the previous rule but you have no way of testing them in this lab right now.)

Figure 153. Configure Applications tab



Add Rule

Name: INET to DMZ Server ☑ Enabled Insert: below rule 1

Action: ✓ Allow

Zones | Networks | VLAN Tags | Users | **Applications** | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Application Filters Clear All Filters

Search by name

User-Created Filters	
Risks (Any Selected)	
□ Very Low	1097
□ Low	806
□ Medium	998
□ High	210
□ Very High	123
Business Relevance (Any Selected)	
□ Very Low	814
□ Low	564
□ Medium	1257

Available Applications (13)

http

- □ All apps matching the filter
- □ Android Asynchronous Http Client
- □ GSS HTTP
- □ HTTP
- □ HTTP 2.0
- □ HTTP RPC Ep Map
- □ HTTP Tunnel
- □ HTTP/SSL Tunnel
- □ HTTPMGT
- □ HTTPS

Selected Applications and Filters (1)

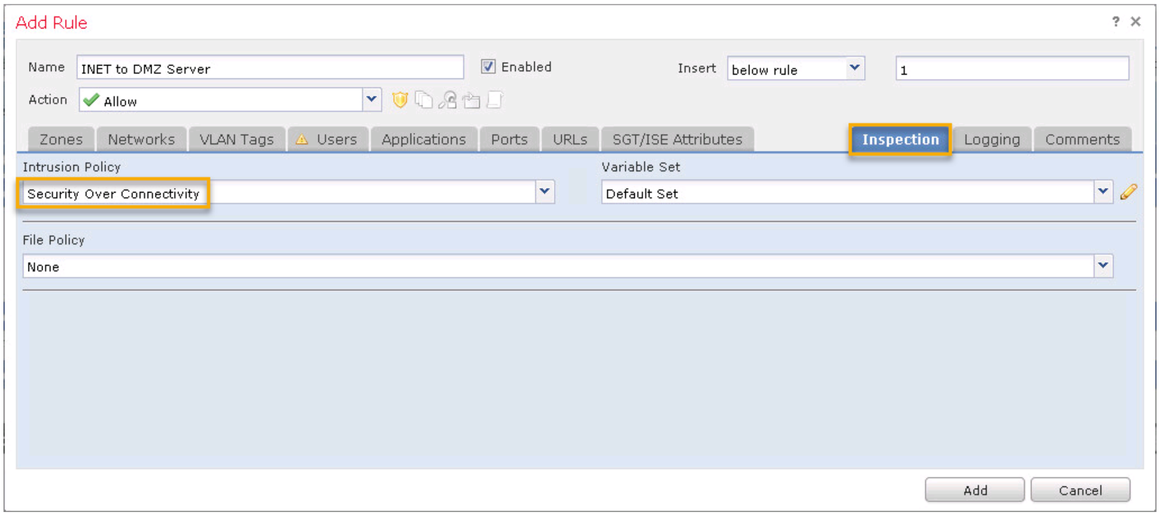
Applications

- □ HTTP

79. On the **Inspection tab**:

    a. Intrusion Policy: **Security Over Connectivity**

Figure 154. Configure Inspection tab



Name: INET to DMZ Server
☑ Enabled
Insert: below rule | 1
Action: ✓ Allow

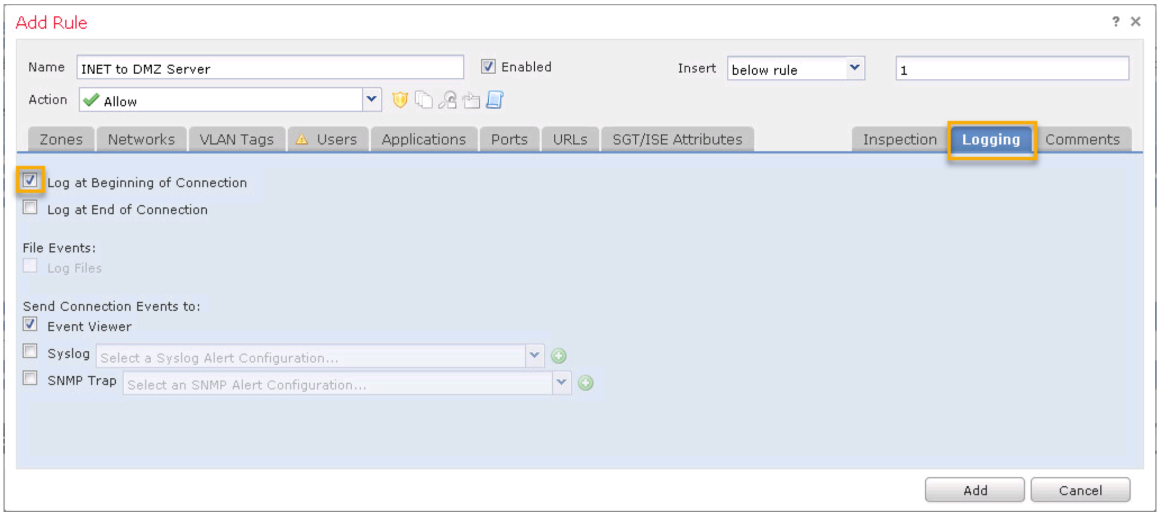
Intrusion Policy: Security Over Connectivity
Variable Set: Default Set

File Policy: None

80. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** button. (Note, in the real world this could create a lot of logs depending on how busy this web server is. You do it here as an exercise in the lab not as a recommendation.)

Figure 155. Configure Logging tab



Name: INET to DMZ Server
☑ Enabled
Insert: below rule | 1
Action: ✓ Allow

☑ Log at Beginning of Connection
□ Log at End of Connection

File Events:
□ Log Files

Send Connection Events to:
☑ Event Viewer
□ Syslog: Select a Syslog Alert Configuration...
□ SNMP Trap: Select an SNMP Alert Configuration...

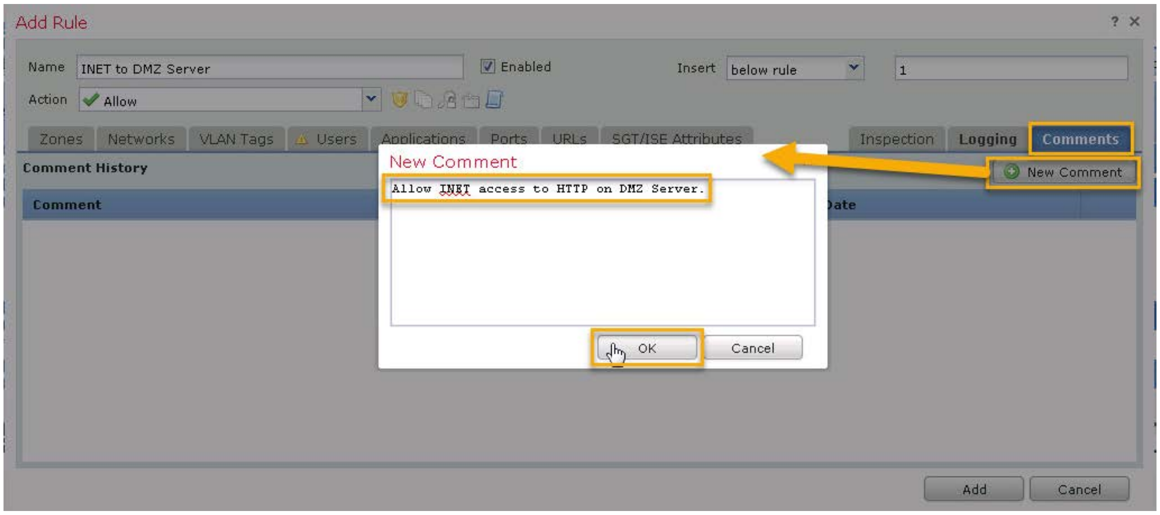
81. On the **Comments tab**:

    a. Click **New Comment**

        i. New Comment: **Allow INET access to HTTP on DMZ Server.**

        ii. Click **OK**

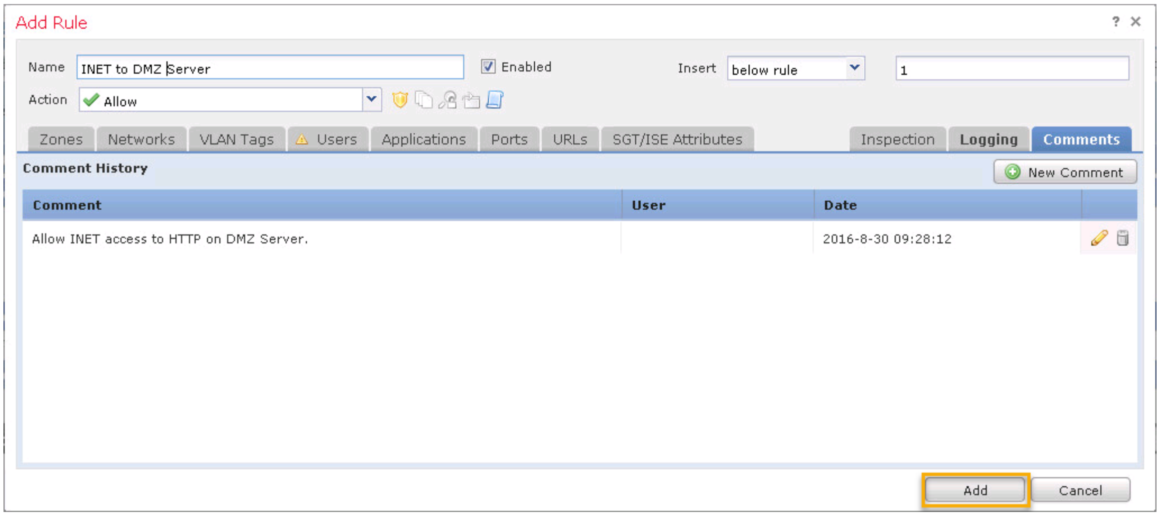
Figure 156. Add comment to rule



Allow INET access to HTTP on DMZ Server.

82. Click **Add**

Figure 157. Add rule



Comment	User	Date
Allow INET access to HTTP on DMZ Server.		2016-8-30 09:28:12

83. Click **Save**.

84. Before you deploy let’s take a moment and review what your Access Control Policy rulesets are saying.

    a. The **Mandatory – Base Policy section** has no rules BUT if there were some rules here they would be used first, assuming there was a match.

    b. The **Mandatory – HQ Policy section** has two rules, the ones you just created.

        i. The first rule allows SSH, FTP, and HTTP access to the DMZ server from the HQ LAN IP range. This rule will be tested for a match before the next rule.

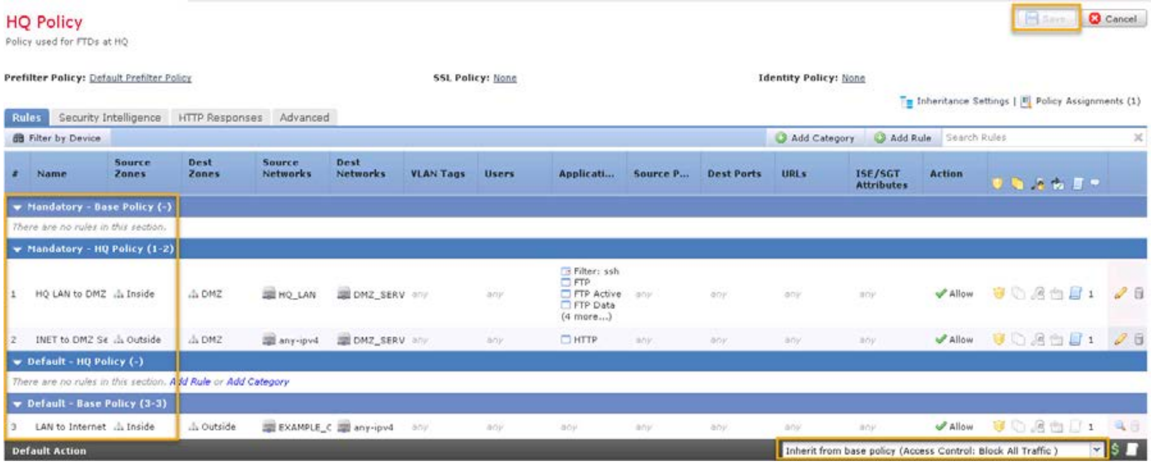
        ii. The second rule allows HTTP access to the DMZ server from the INET.

    c. The **Default – HQ Policy section** has no rules but any rule that would be here would be tested next for a match.

    d. The **Default – Base Policy section** has one rule that gives EXAMPLE_CORP_LANS IPs coming from the Inside zone access to any IP in the Outside zone. I word it this way because when you add in the Remote location’s FTD devices their Inside and Outside zones will be these same zones.

    e. Lastly you have the **Default Action**. In your case you have that set to be inherited from the Base Policy and that is set to Block All Traffic.

Figure 158. Save and Review ACP Rules



HQ Policy
Policy used for FTDs at HQ

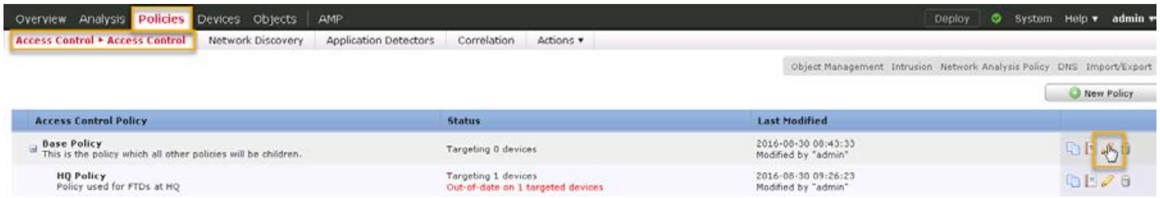
Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
▾ Mandatory - Base Policy (-)														
There are no rules in this section.														
▾ Mandatory - HQ Policy (1-2)														
1	HQ LAN to DMZ	Inside	DMZ	HQ_LAN	DMZ_SERV	any	any	Filter: ssh FTP FTP Active FTP Data (4 more...)	any	any	any	any	✓ Allow	1
2	INET to DMZ Se	Outside	DMZ	any-ipv4	DMZ_SERV	any	any	HTTP	any	any	any	any	✓ Allow	1
▾ Default - HQ Policy (-)														
There are no rules in this section. Add Rule or Add Category														
▾ Default - Base Policy (3-3)														
3	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✓ Allow	1

Default Action: Inherit from base policy (Access Control: Block All Traffic)

85. Now that you have addressed Example Corp’s IP addresses and their possible access control needs let’s add logging to the Default Action. You can’t edit the Default Action from within the HQ Policy access control policy so navigate to **Policies > Access Control > Access Control** and click the **pencil icon** for the **Base Policy** row.

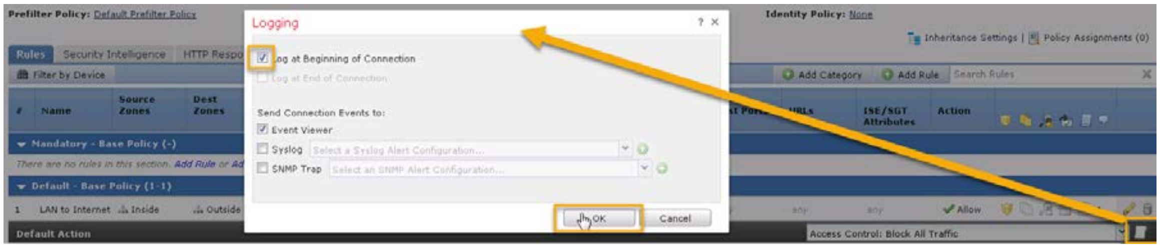
Figure 159. Edit Base Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-30 08:43:33 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Out-of-date on 1 targeted devices	2016-08-30 09:26:23 Modified by "admin"

86. Click the **scroll icon** next to the Default Action dropdown button.
87. Depending on how important you think these events might be you could select more alerting methods but for the lab you will just click the **Log at Beginning of Connection** and click **OK**.

Figure 160. Add logging to Default Action



Prefilter Policy: Default Prefilter Policy

Identity Policy: None

Logging

☑ Log at Beginning of Connection

□ Log at End of Connection

Send Connection Events to:

☑ Event Viewer

□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

#	Name	Source Zones	Dest Zones	...	URLs	ISE/SGT Attributes	Action
Mandatory - Base Policy (-)							
There are no rules in this section. Add Rule or Ad							
Default - Base Policy (1-1)							
1	LAN to Internet	Inside	Outside	any	any		Allow

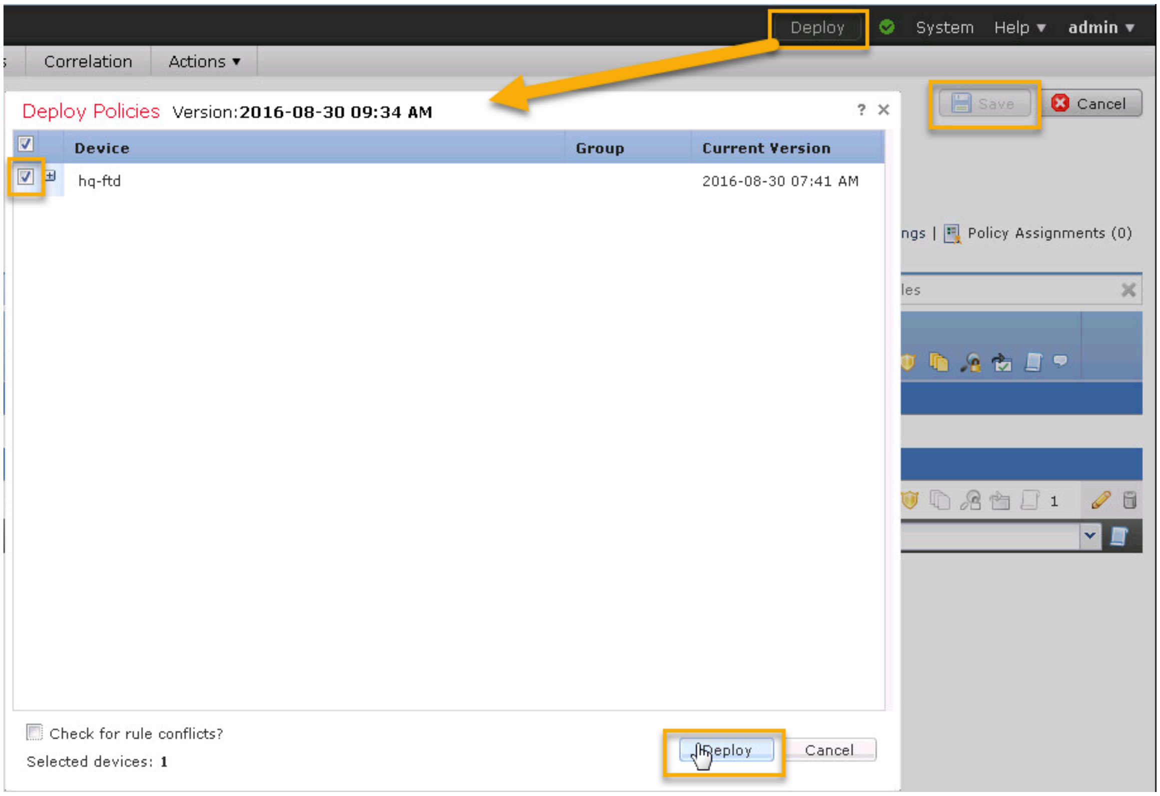
Default Action: Access Control: Block All Traffic

In the lab you will see hits to this Default Action whenever the DMZ server attempts to initiate communication out to the Internet as we didn't include the DMZ zone within the LAN to INET Access rule. This will appear mostly as DNS attempts to 8.8.8.8 from 172.16.102.50. If during testing of other rules this traffic gets too cumbersome to handle you can add the DMZ zone to the LAN to INET rule, or you can disable logging for the Default Action, or you can create a new rule to specifically identify the DMZ server traffic and block it (thus avoiding hitting the Default Action).

I think leaving the Default Action as a catch-all for anything you may have missed (or is nefarious, such as a spoofed source IP address) is a good thing. Other security engineers might suggest that the Default Action be used as a catch-all for certain known traffic flows (like the DMZ server as explained above) and that logging this type of traffic is not needed. Your thoughts might be somewhere in between. The point is that there is no Cisco recommendation on how to use the Default Action and the use of Access Control Policy rules. Application of these rules is highly subjective to the deployment and monitoring/tuning of the rules should be done regularly.

88. Click **Save**, **Deploy**, select the **hq-ftd** device, and then click the **Deploy** button to update the hq-ftd device with your changes.

Figure 161. Save and Deploy to hq-ftd



Deploy Policies Version:**2016-08-30 09:34 AM**

☑	Device	Group	Current Version
☑	hq-ftd		2016-08-30 07:41 AM

□ Check for rule conflicts?

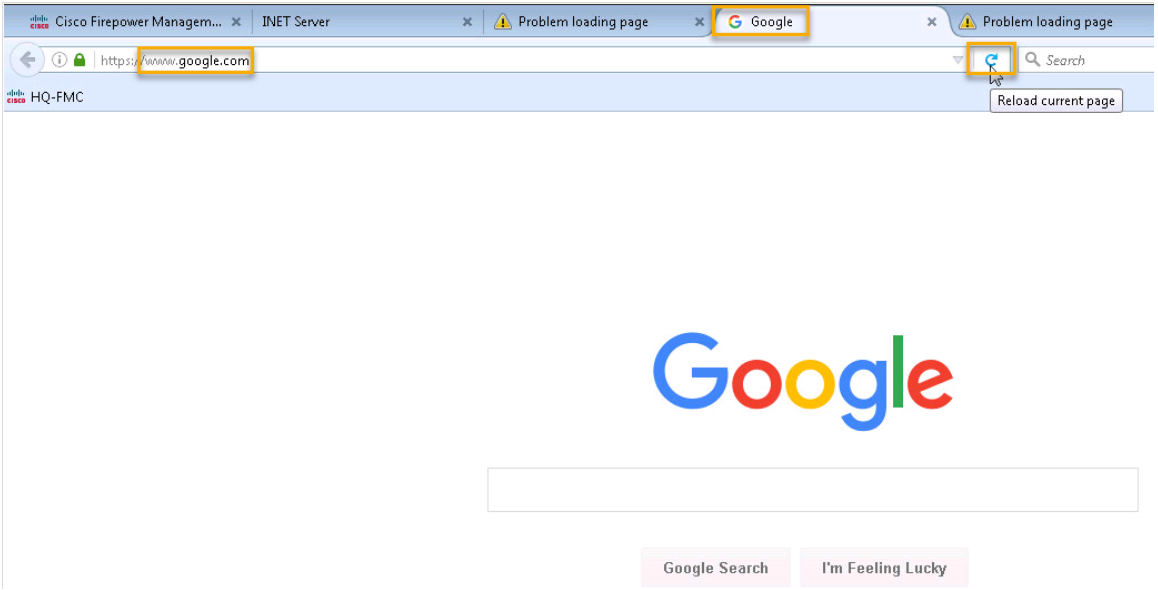
Selected devices: **1**

<u>Do not continue the lab until the deployed changes to hq-ftd via the FMC are complete.</u>

Testing INET Access and Access Control Policies for the HQ Location

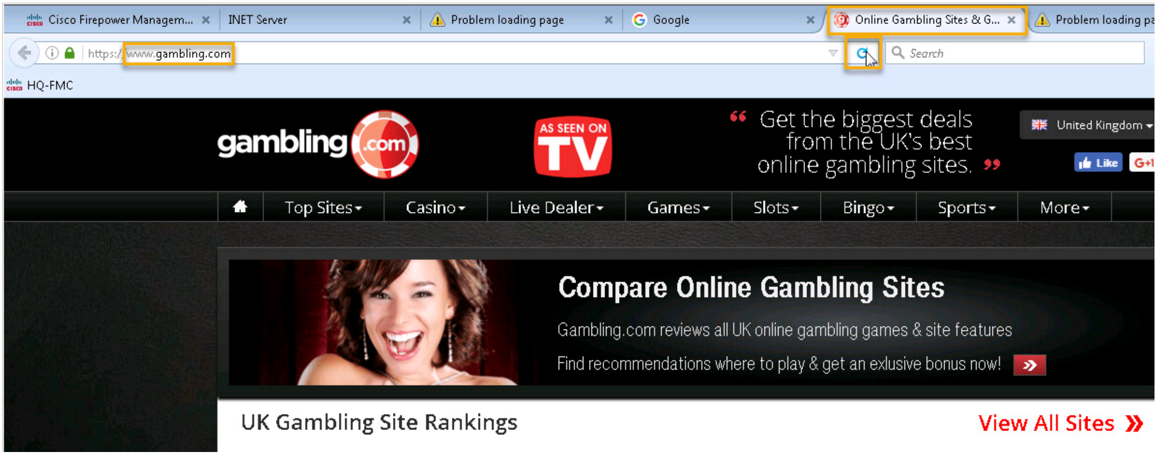
89. Once the deployment is completed, on **hq-wkst** browse to **the Google home page** (the 4th tab). This page should still resolve.

Figure 162. Google resolves



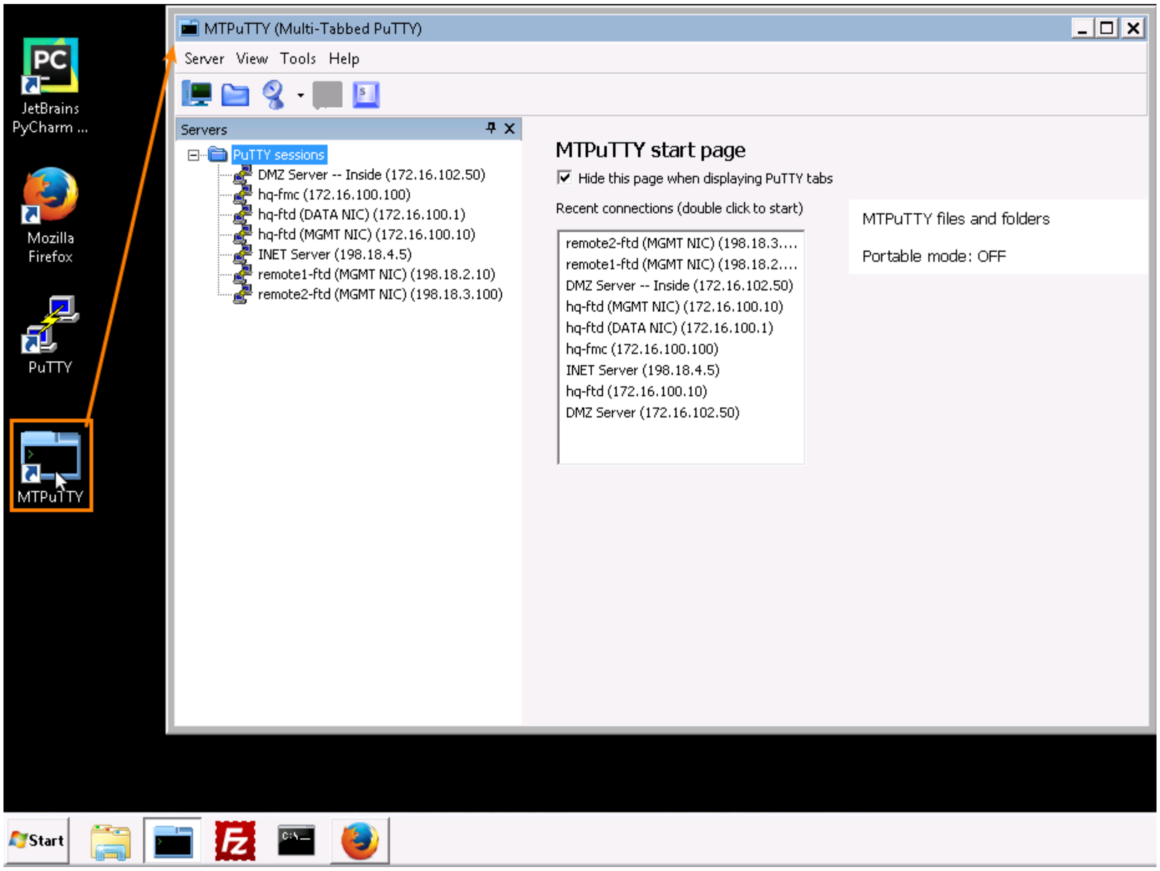
90. Go to **www.gambling.com** (the 5th tab) and this will resolve as well. (You don't want that to happen but we'll fix it in a later section of the lab.)

Figure 163. Gambling.com resolves


Cisco Firepower Managem...
INET Server
Problem loading page
Google
Online Gambling Sites & G...
Problem loading pa
https://www.gambling.com
Search
HQ-FMC
gambling.com
AS SEEN ON TV
Get the biggest deals from the UK's best online gambling sites.
United Kingdom
Like
Top Sites
Casino
Live Dealer
Games
Slots
Bingo
Sports
More
Compare Online Gambling Sites
Gambling.com reviews all UK online gambling games & site features
Find recommendations where to play & get an exlusive bonus now!
UK Gambling Site Rankings
View All Sites

91. Open **MTPutty**.

Figure 164. Open MTPuTTY



- PuTTY sessions
  - DMZ Server -- Inside (172.16.102.50)
  - hq-fmc (172.16.100.100)
  - hq-ftd (DATA NIC) (172.16.100.1)
  - hq-ftd (MGMT NIC) (172.16.100.10)
  - INET Server (198.18.4.5)
  - remote1-ftd (MGMT NIC) (198.18.2.10)
  - remote2-ftd (MGMT NIC) (198.18.3.100)

MTPuTTY start page

☑ Hide this page when displaying PuTTY tabs

Recent connections (double click to start)

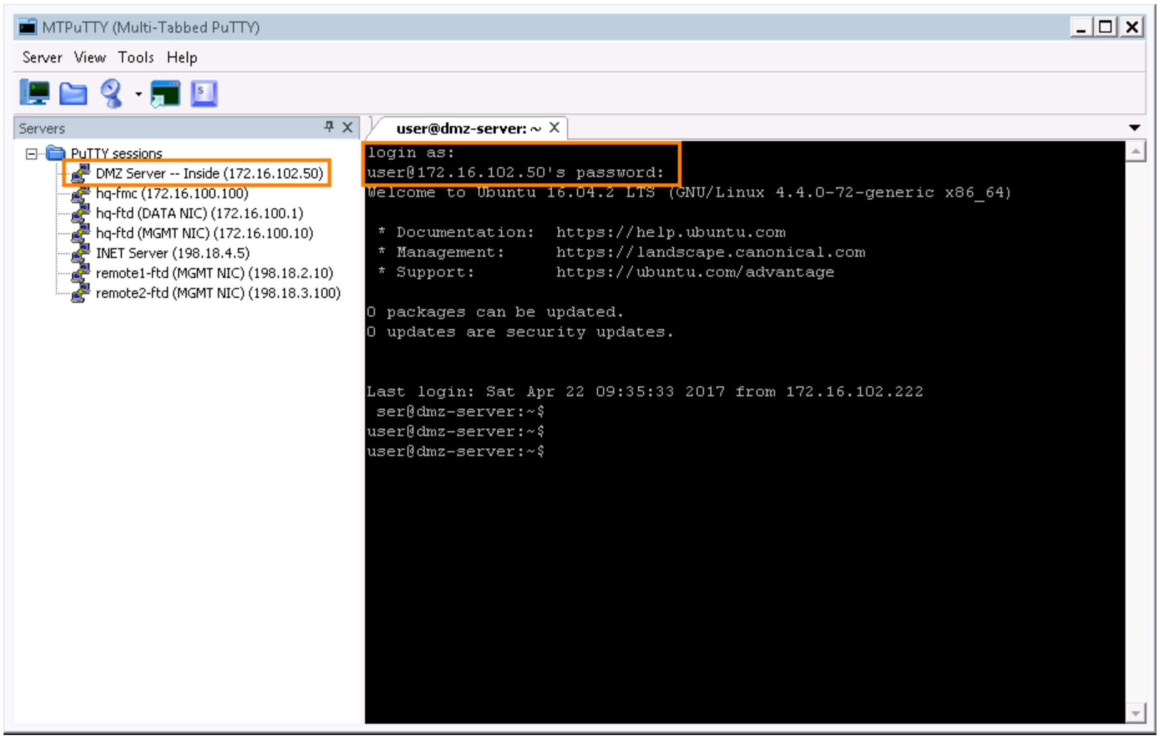
remote2-ftd (MGMT NIC) (198.18.3....
remote1-ftd (MGMT NIC) (198.18.2....
DMZ Server -- Inside (172.16.102.50)
hq-ftd (MGMT NIC) (172.16.100.10)
hq-ftd (DATA NIC) (172.16.100.1)
hq-fmc (172.16.100.100)
INET Server (198.18.4.5)
hq-ftd (172.16.100.10)
DMZ Server (172.16.102.50)

MTPuTTY files and folders

Portable mode: OFF

92. Using the **DMZ Server -- Inside** saved bookmark, ssh to 172.16.102.50. Login in as **user**/**C1sco12345**.

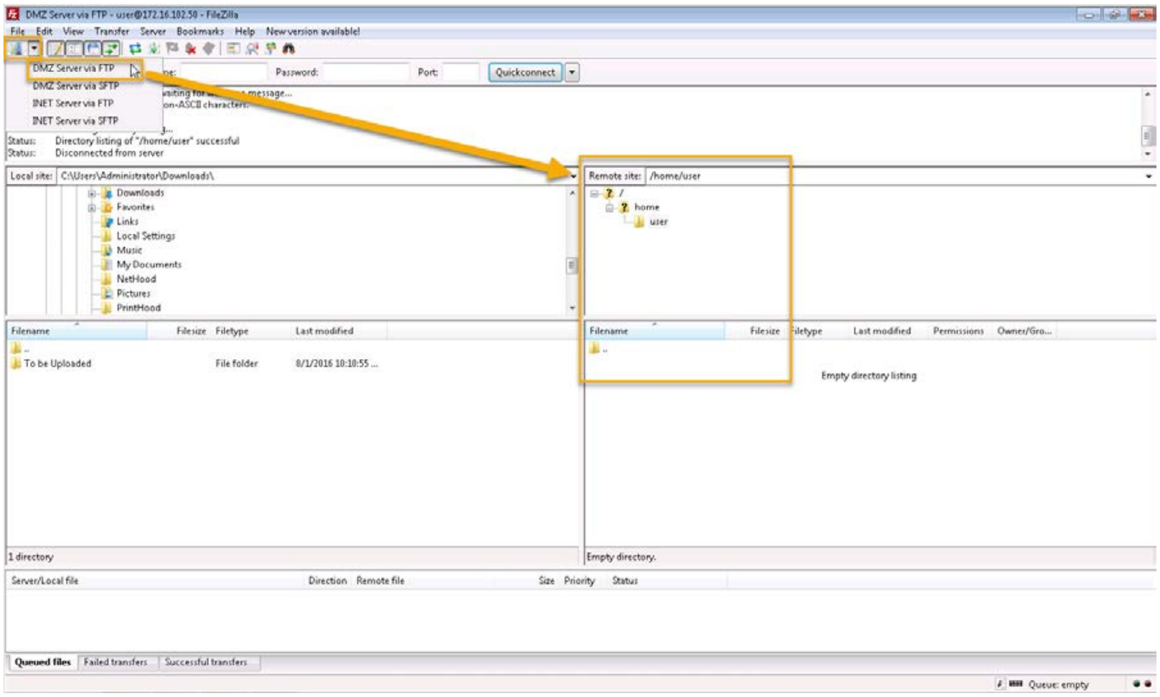
Figure 165. SSH to dmz-server works


MTPuTTY (Multi-Tabbed PuTTY)
Server View Tools Help
Servers
PuTTY sessions
DMZ Server -- Inside (172.16.102.50)
hq-fmc (172.16.100.100)
hq-ftd (DATA NIC) (172.16.100.1)
hq-ftd (MGMT NIC) (172.16.100.10)
INET Server (198.18.4.5)
remote1-ftd (MGMT NIC) (198.18.2.10)
remote2-ftd (MGMT NIC) (198.18.3.100)
user@dmz-server: ~

```
login as:
user@172.16.102.50's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Sat Apr 22 09:35:33 2017 from 172.16.102.222
 ser@dmz-server:~$
user@dmz-server:~$
user@dmz-server:~$
```

93. Open **FileZilla** and, using the **DMZ Server via FTP** bookmark, FTP to 172.16.102.50. Login in as **user**/**C1sco12345**.

Figure 166. FTP to dmz-server works



```
...aiting for ... message...
...on-ASCII characters.
...
Status:     Directory listing of "/home/user" successful
Status:     Disconnected from server
```

Local site: C:\Users\Administrator\Downloads\

Remote site: /home/user

Filename	Filesize	Filetype	Last modified
..			
To be Uploaded		File folder	8/1/2016 10:10:55 ...

1 directory

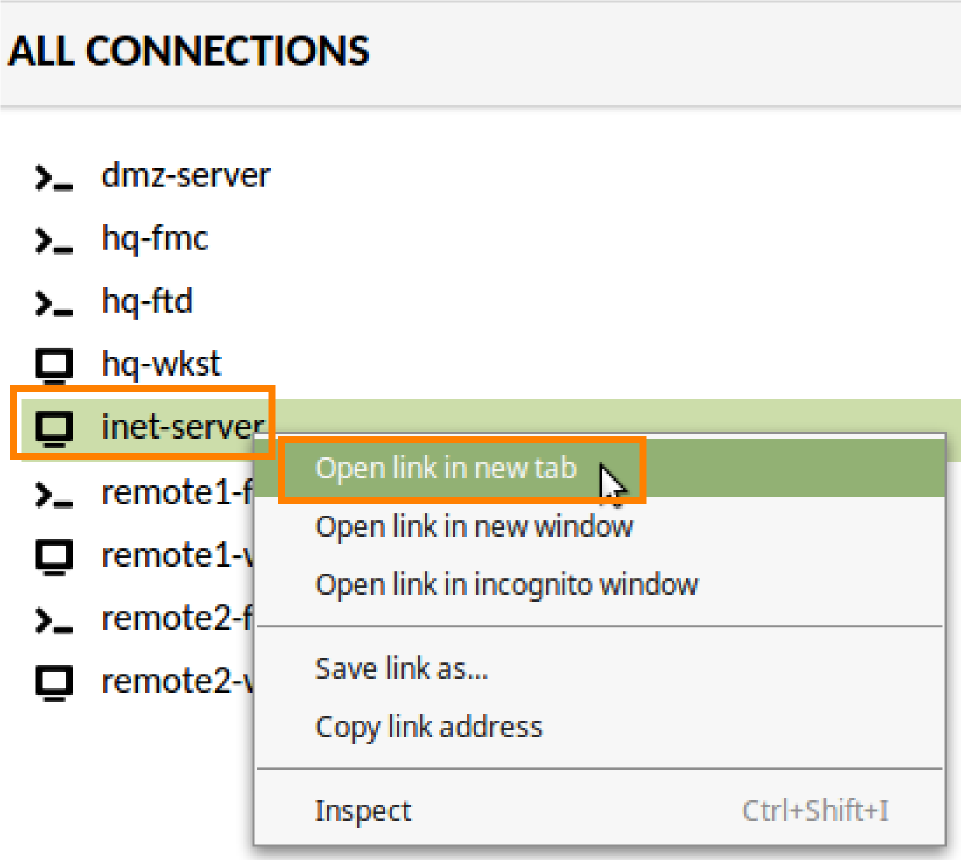
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					

Empty directory listing

Empty directory.

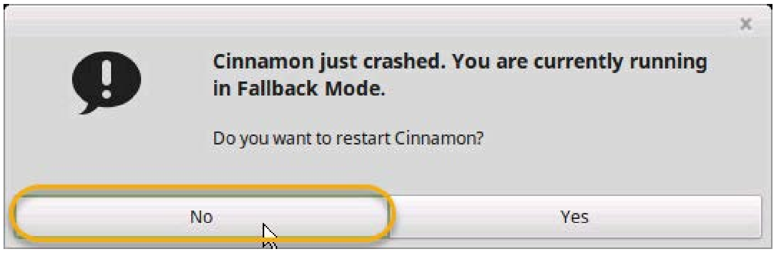
94. From the **oob webpage**, open a connection to the **inet-server**. This will auto log in as user/C1sco12345.

Figure 167. Connect to inet-server



95. Click **No** if asked to restart Cinnamon.

Figure 168. On inet-server, the Cinnamon desktop doesn't like xrdp.

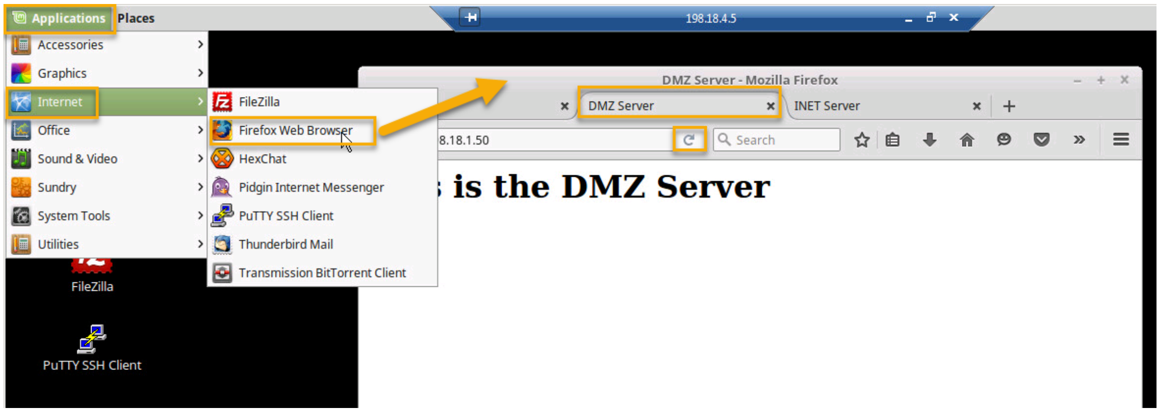


Cinnamon just crashed. You are currently running in Fallback Mode.

Do you want to restart Cinnamon?

96. Remember that the inet-server sits outside of the Example Corp network and represents an external user incoming to Example Corp services, such as their web site. In **Firefox** go to **http://198.18.1.50** (the DMZ Server).

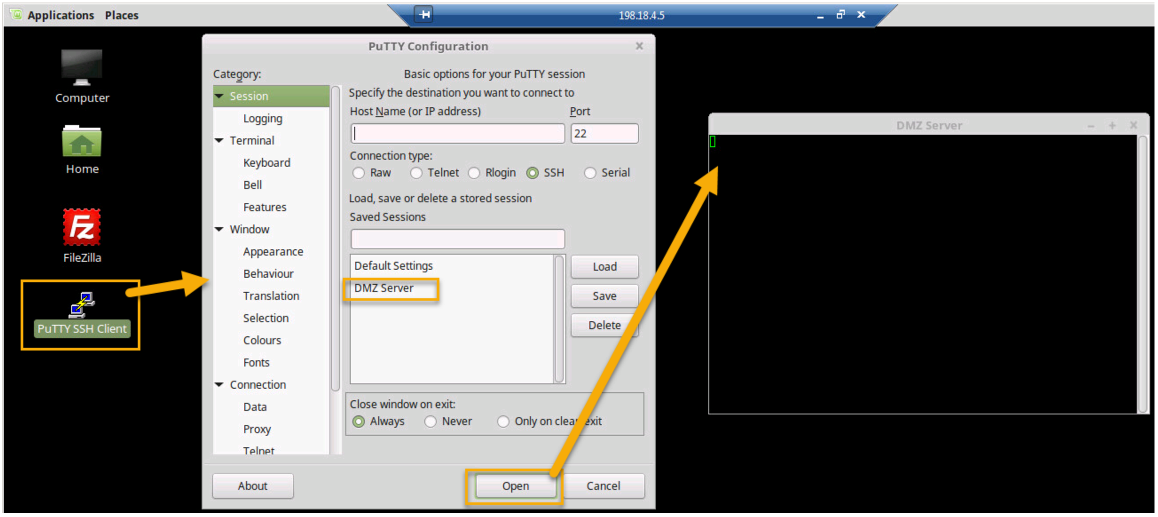
Figure 169. INET to dmz-server web page works



97. Open **Putty** and using the **DMZ Server** bookmark ssh to 198.18.1.50. Not only will this connection fail it also has the negative reaction of crashing the RDP session to the inet-server. Not sure why that is but you can reconnect the RDP session to the inet-server just fine.

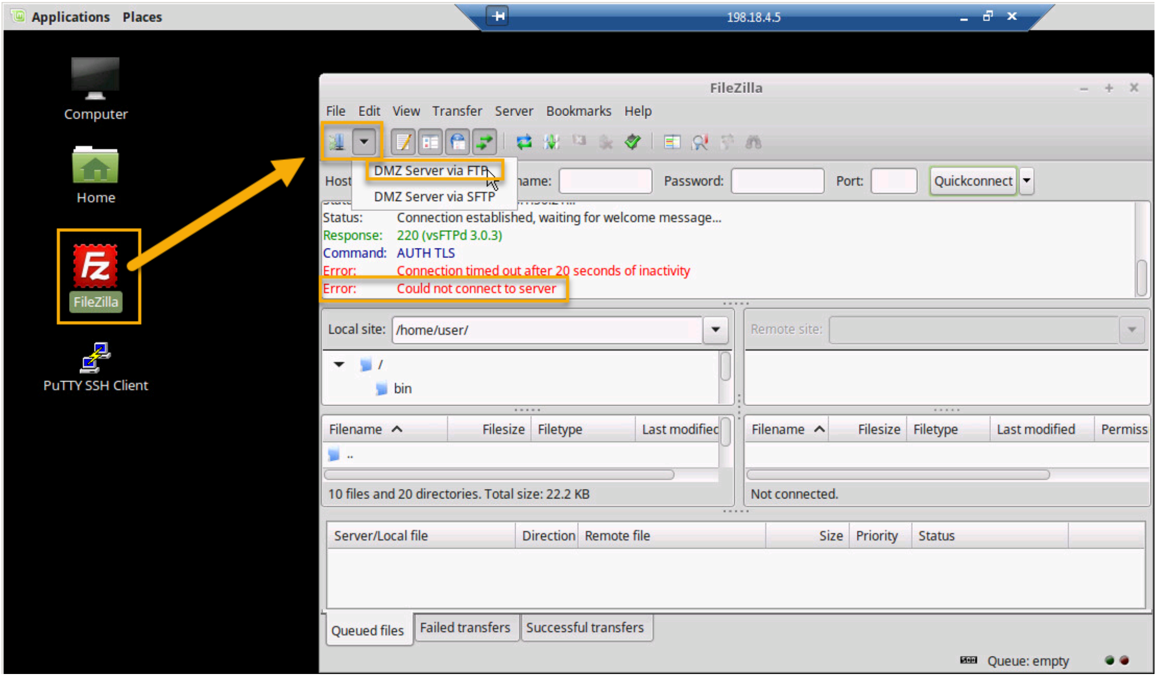
Note sure why but this crashes the RDP session as well. Just reconnect.

Figure 170. SSH to dmz-server fails



98. Open **FileZilla** and using the **DMZ Server via FTP** bookmark FTP to 198.18.1.50. This should fail.

Figure 171. FTP to dmz-server fails



```
Status:    Connection established, waiting for welcome message...
Response:  220 (vsFTPd 3.0.3)
Command:   AUTH TLS
Error:     Connection timed out after 20 seconds of inactivity
Error:     Could not connect to server
```

Local site: /home/user/

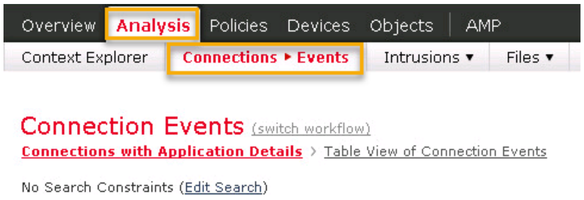
10 files and 20 directories. Total size: 22.2 KB

Not connected.

Queue: empty

99. On **hq-wkst**, return to FMC and navigate to **Analysis > Connections > Events**. Here is a log of the “connections” that you opted to enable logging for. (The “Log at Beginning” and “Log at End” settings).

Figure 172. Navigate to Connection Events



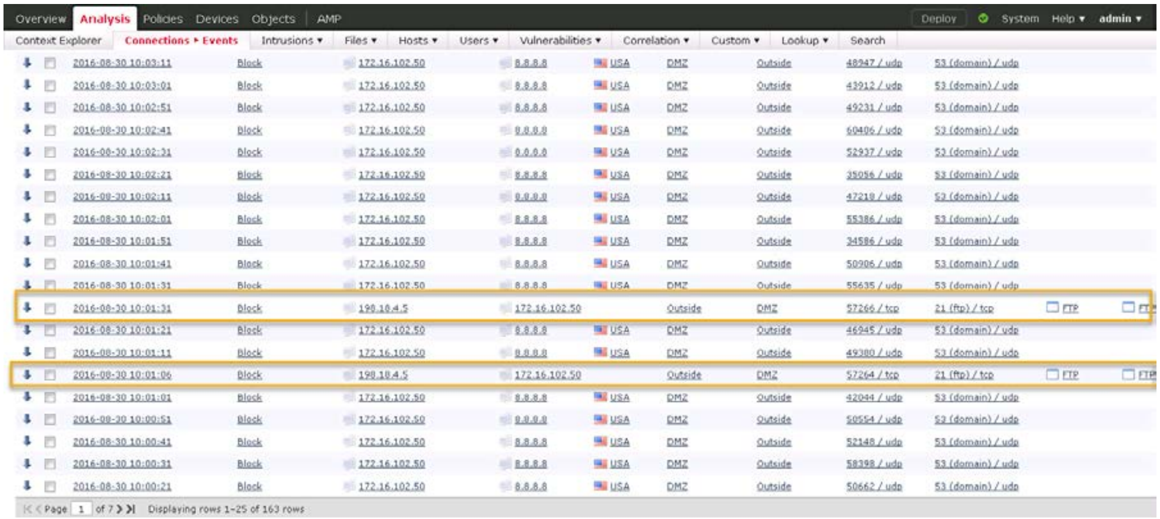
Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

100. The “First Packet” column related to the “Log at Beginning of Connection” setting and based on whether you had selected to “Log at End of Connection” or not will show in the “Last Packet” column. Take a moment and review the events here and try to correlate them to the actions you just took. You should be able to find the hq-wkst (172.16.100.250) HTTP, SSH, and FTP connections (which were allowed), the inet-server (198.18.4.5) HTTP connection (allowed) and it SSH and FTP (block) attempts.

Figure 173. Connection Events



⬇	□	2016-08-30 10:03:11	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	48947 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:03:01	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	43912 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:02:51	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	49231 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:02:41	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	60406 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:02:31	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	52937 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:02:21	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	35056 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:02:11	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	47218 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:02:01	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	55386 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:01:51	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	34586 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:01:41	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	50906 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:01:31	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	55635 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:01:31	Block	198.18.4.5	172.16.102.50		Outside	DMZ	57266 / tcp	21 (ftp) / tcp	□ FTP	□ FT
⬇	□	2016-08-30 10:01:21	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	46945 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:01:11	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	49380 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:01:06	Block	198.18.4.5	172.16.102.50		Outside	DMZ	57264 / tcp	21 (ftp) / tcp	□ FTP	□ FTP
⬇	□	2016-08-30 10:01:01	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	42044 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:00:51	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	50554 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:00:41	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	52148 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:00:31	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	58398 / udp	53 (domain) / udp	
⬇	□	2016-08-30 10:00:21	Block	172.16.102.50	8.8.8.8	USA	DMZ	Outside	50662 / udp	53 (domain) / udp	

|< < Page 1 of 7 > >| Displaying rows 1–25 of 163 rows

Did you notice all the Block attempts to 8.8.8.8? Which device is generating all that traffic? Which rule is being matched to block this traffic? Should we be logging all this traffic or should we tune the Access Control Policy rules to either permit this traffic or silence the logging of this traffic?

You can close the **inet-server** tab in your browser as it won’t be used again for a while.

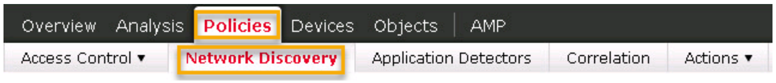
You can close the **hq-ftd** tab in your browser as it won’t be used again for a while.

Configure Network Discovery

Though not needed in order to establish a connection to the Internet, the Network Discovery feature of the FTD devices is used to learn information about what types of devices and their typical traffic patterns are communicating using the FTD device. The default setting for the Network Discovery is to analyze all traffic traversing it and attempt to categorize the sending device. Though this setting is good to start with you can narrow this discovery process down to just those devices within Example Corp’s network.

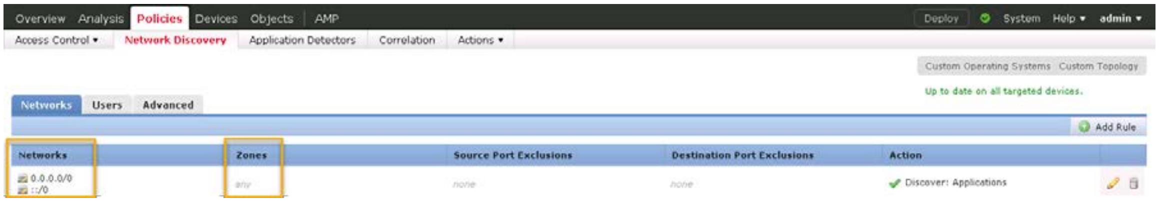
101. Navigate to **Policies > Network Discovery**.

Figure 174. Navigate to Network Discovery



102. Notice how the default rule checks all IP addresses from all zones. This means that the FTD device will also attempt to categorize traffic incoming from the Internet (which is pointless). Let’s tighten up this rule to only monitor traffic on the Example Corp networks.

Figure 175. Default rule



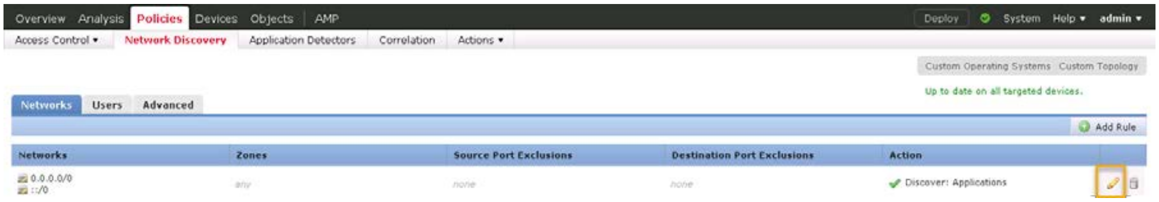
Up to date on all targeted devices.

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Applications

The information collected via the Network Discovery process is used in several places within the FTD/FMC security devices. One of the main things this data can do is help target the SNORT rules being used to remove unneeded rules and/or add rules to more streamline your FTD device’s performance. You will see more about this during Scenario 9 when you create a custom intrusion policy based on the Firepower Recommendations, which is based on the learned OSes and Applications gathered by the Network Discovery process.

103. The default rule is shown here. Click the **pencil icon** for that row.

Figure 176. Edit the current rule



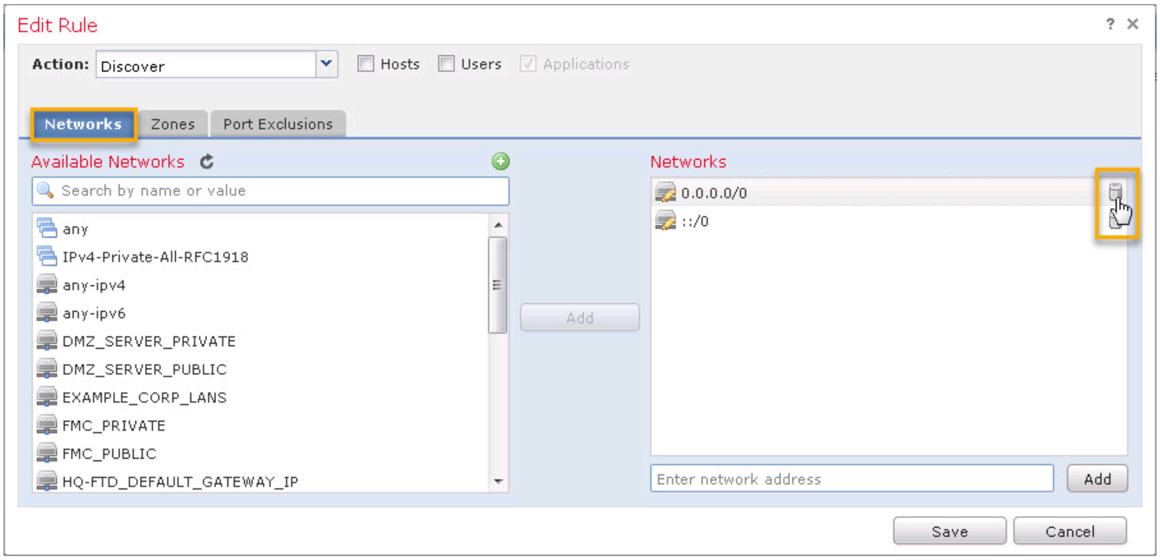
Up to date on all targeted devices.

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Applications

104. On the **Networks tab**:

   a. As you can see this rule is discovering “any” IP address. Click the **trashcan icon** for the **any** line in the **Networks column**.

Figure 177. Delete existing networks



Edit Rule

Action: Discover

□ Hosts □ Users ☑ Applications

Networks | Zones | Port Exclusions

Available Networks

Search by name or value

- any
- IPv4-Private-All-RFC1918
- any-ipv4
- any-ipv6
- DMZ_SERVER_PRIVATE
- DMZ_SERVER_PUBLIC
- EXAMPLE_CORP_LANS
- FMC_PRIVATE
- FMC_PUBLIC
- HQ-FTD_DEFAULT_GATEWAY_IP

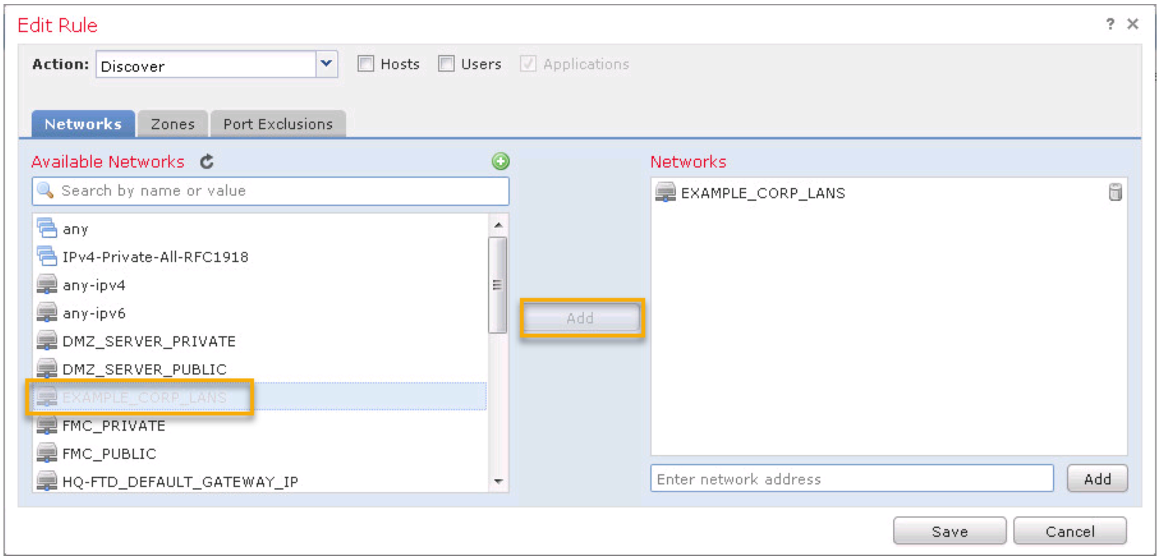
Networks

- 0.0.0.0/0
- ::/0

Enter network address

   b. From the **Available Networks** column select **EXAMPLE_CORP_LANS** and then click the **Add** button.

Figure 178. Configure Networks tab



Edit Rule

Action: Discover

□ Hosts □ Users ☑ Applications

Networks | Zones | Port Exclusions

Available Networks

Search by name or value

- any
- IPv4-Private-All-RFC1918
- any-ipv4
- any-ipv6
- DMZ_SERVER_PRIVATE
- DMZ_SERVER_PUBLIC
- EXAMPLE_CORP_LANS
- FMC_PRIVATE
- FMC_PUBLIC
- HQ-FTD_DEFAULT_GATEWAY_IP

Networks

- EXAMPLE_CORP_LANS

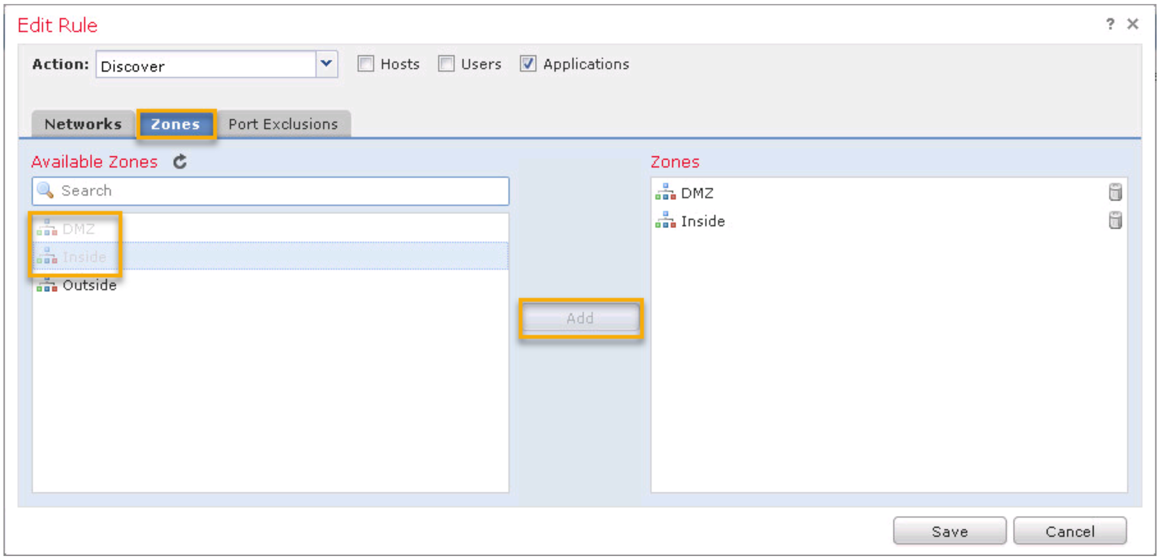
Enter network address

105. Click the **Zones tab**:

   a. From the **Available Zones** column select **Inside** and then click **Add**.

   b. From the **Available Zones** column select **DMZ** and then click **Add**.

Figure 179. Configure Zones tab



Edit Rule

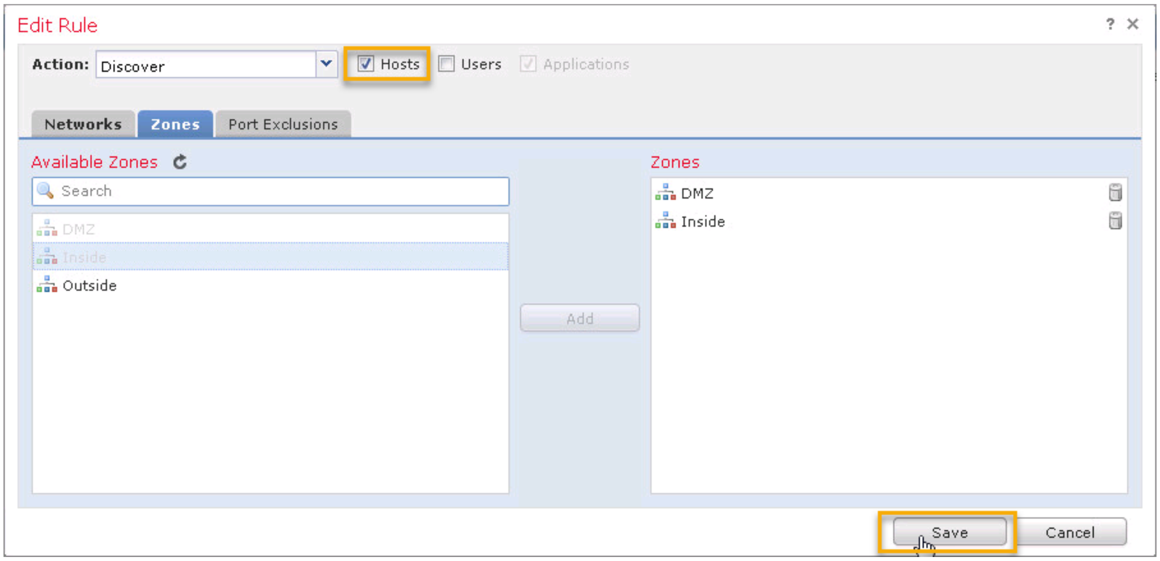
Action: Discover

□ Hosts □ Users ☑ Applications

106. From the check boxes along the top check the **Hosts box**.

107. Click **Save**.

Figure 180. Check hosts box and save



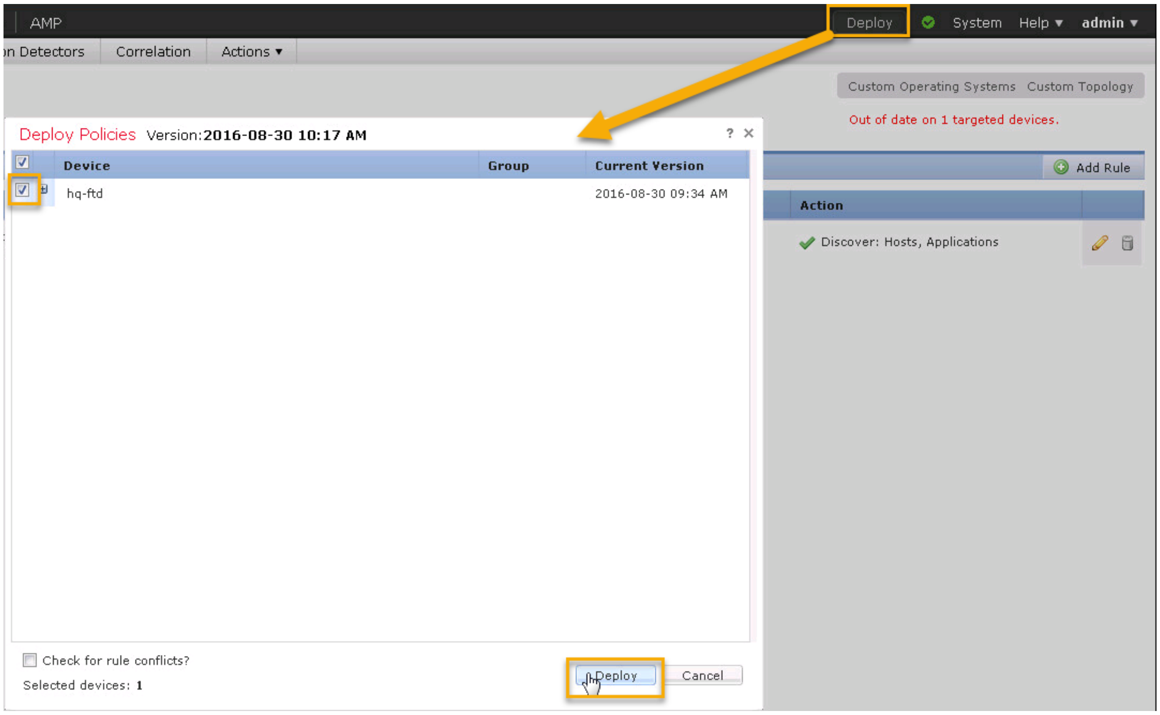
Edit Rule

Action: Discover

☑ Hosts □ Users ☑ Applications

108. Click **Deploy**, select **all the FTD devices**, and then click **Deploy**. From here on the hq-ftd device will attempt to learn what the Hosts and Applications are of the IP traffic traversing its Inside and/or DMZ zones.

Figure 181. Deploy changes



Out of date on 1 targeted devices.

Deploy Policies Version:2016-08-30 10:17 AM

☑	Device	Group	Current Version
☑	hq-ftd		2016-08-30 09:34 AM

Selected devices: 1

Scenario Summary

Different from the days of “single box” configuration and deployment, the FMC now configures groups of devices, with the same policies and rules, at a time. This means you can create more general rules (like setting up NAT from “inside” to “outside”) for the whole organization and push those policies to all the devices managed by the FMC. This will help keep deployments that have a lot of remote sites configured in a similar manner. The danger here is that if something gets misconfigured it is now misconfigured everywhere!

Access control policies have a lot of flexibility in the way rules can get applied. Using the hierarchal method of deploying policies allows a design where rules can be imposed to all devices, whether they have a rule that would otherwise countermand this rule, to specific rules for certain groups of devices (applied only to the child policy), to a “catch all” group for any rule set that “should” be implemented if it isn’t specified somewhere else. This is all confusing to explain in text but simply looking at the child policy’s ruleset will line out the order of rules and which trumps which.

Scenario 4. Installing the FTD at the Remote1 Site Using Static IP for Mgmt

Scenario Description

In this scenario, you will configure the remote1-ftd FTD device to be managed by the FMC. Then you will configure remote1-ftd's data plane and test the Remote1 LAN for Internet access.

Remote1 FTD Integration with FMC

Deploying remote/branch locations can be a bit tricky. You need to establish connectivity between the FTD's management interface and the FMC in order to push data plane configuration to the FTD. HOWEVER, without a data plane connection how do you establish the FTD management interface connection to the FTD?

Essentially, you are left with four options:

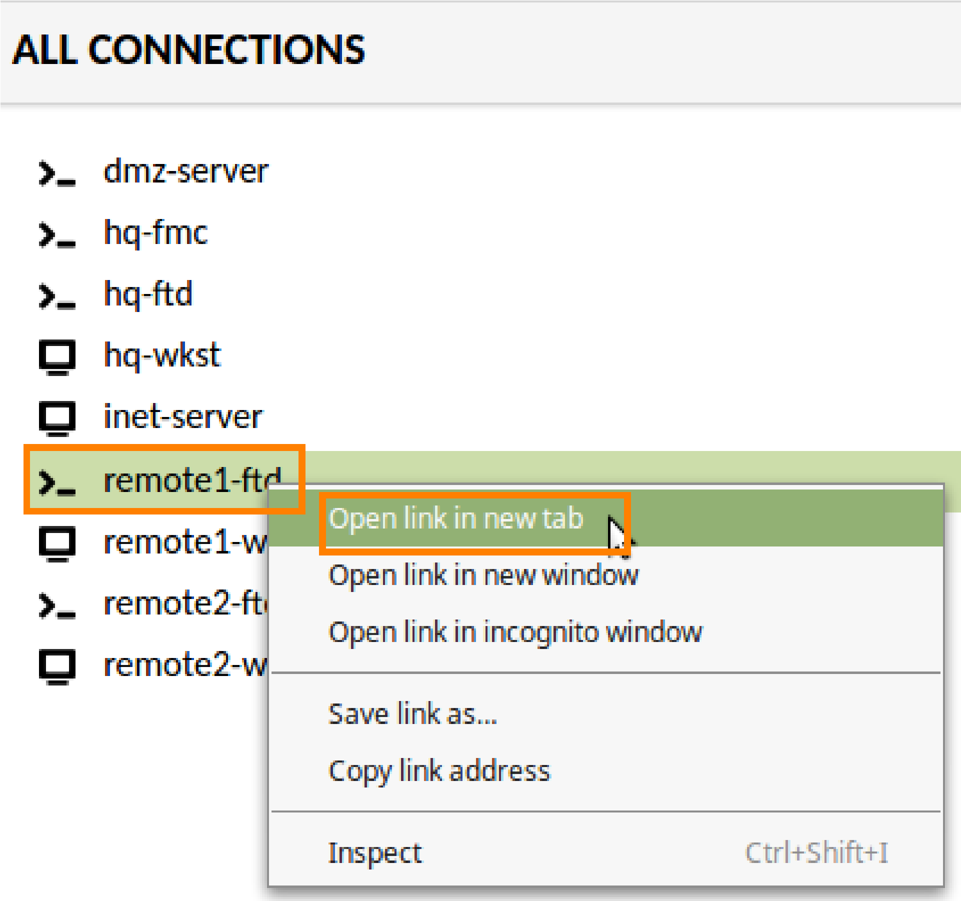
- As of version 6.1 of the FTD software, there is an on box manager called the Firepower Device Manager. However, it is only available for physical appliances. This means that any virtual FTD devices won't be able to use the Firepower Device Manager and are only configurable via the FMC. Additionally, even if you used the Firepower Device Manager, once you have the FTD device configured and you wanted to "switch over" to having it managed by the FMC all its data plane configuration is wiped out in preparation for the FMC to push a new configuration down. So the use of the Firepower Device Manager should only be used when you want to manage each remote/branch location in a decentralized fashion.
- Have a router at the remote/branch location already configured with a VPN/MPLS link to the HQ LAN so that the FTD's management interface can have an internal IP address yet still have a data path to the FMC prior to configuring the data plane.
- Put the FTD's Management NIC on the public facing side of the network with a public IP.
- Pre-configure the FTD's Data Interfaces, Routing, and Policies while it is connected to a LAN that gives IP access to the FMC. Either via a staging/lab environment that can emulate the remote/branch location's network design. This option is most dangerous of all because once this FTD is installed at the remote/branch location its data path to its management interface is through itself. This means that a misconfiguration of the data plane could sever the management NIC's access to the FMC, thus severing your ability to undo the configuration change!

In this lab you don't have the ability to pre-stage, nor do you have a router giving us an IP link back to the FMC, and you aren't using any physical FTDs. So your only option is to put the remote location's FTD's management network on the public network. This means that each remote site needs at least two public IPs (one for the Management Interface and one for the Data interface facing the "outside" zone). This isn't a "best practices" suggestion but it is a possible deployment strategy and it will show off how to add an FTD device to the FMC when they are separated by a NAT device (i.e. the FMC is behind a NAT device).

For the purposes of this lab the remote1 location has an FTD with a public static IP address assigned to its management NIC (198.18.2.10). As with the hq-ftd device the initial configuration of the management network has been done for you so that you can ssh to the remote1-ftd to finish the configuration.

1. From the **oob webpage** connect to **remote1-ftd**. This will auto login as admin/Admin123 on 198.18.2.10 (the remote1-ftd's management NIC IP).

Figure 182. SSH to remote1-ftd



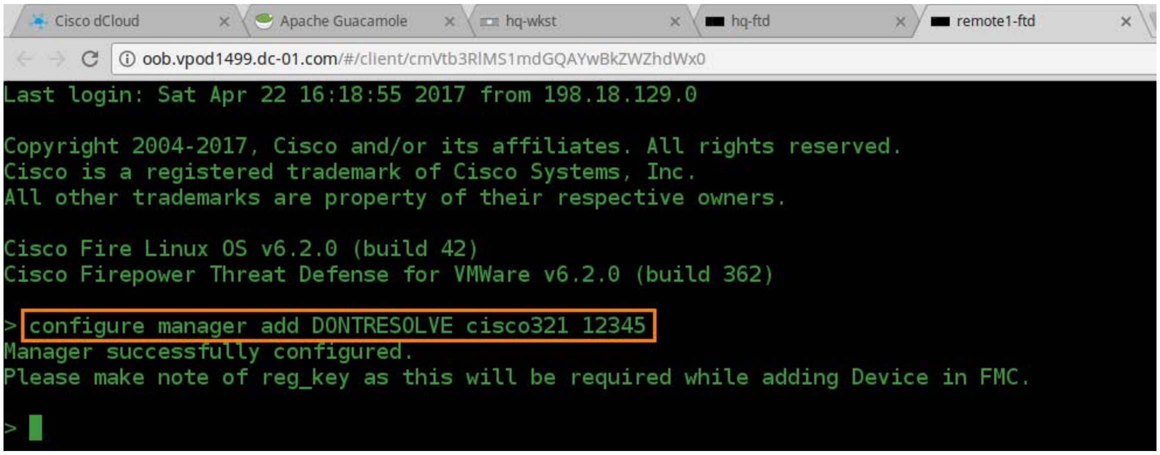
Since the FMC is behind a NAT device you have two options to get the remote1-ftd device registered with it. Either the remote1-ftd device needs a static IP address that the FMC can reach or you need to set up a static NAT address for the FMC that the remote1-ftd device can reach.

Though assigning a static IP address to each remote/branch FTD devices for the management IP address (bear in mind that you need two addresses from the ISP for each remote/branch FTD; one for management and one for the data interface) is probably not going to be that common, it is still a possibility. This section will show you that method.

You will use the more plausible method (where the remote/branch FTD only gets DHCP addresses from the ISP) when registering the remote2-ftd device later in the lab.

2. Though the IP address of the FMC is fixed, via the static NAT rule you created earlier, in this scenario you will assume that the public IP address that the FMC uses is unknown (or variable) and thus you will need to configure the remote1-ftd device to wait for the initial contact from the FMC. On the remote1-ftd CLI issue the command **configure manager add DONTRESOLVE cisco321 12345** to set up this FTD to await communication from the FMC.

Figure 183. Configure manager for remote1-ftd



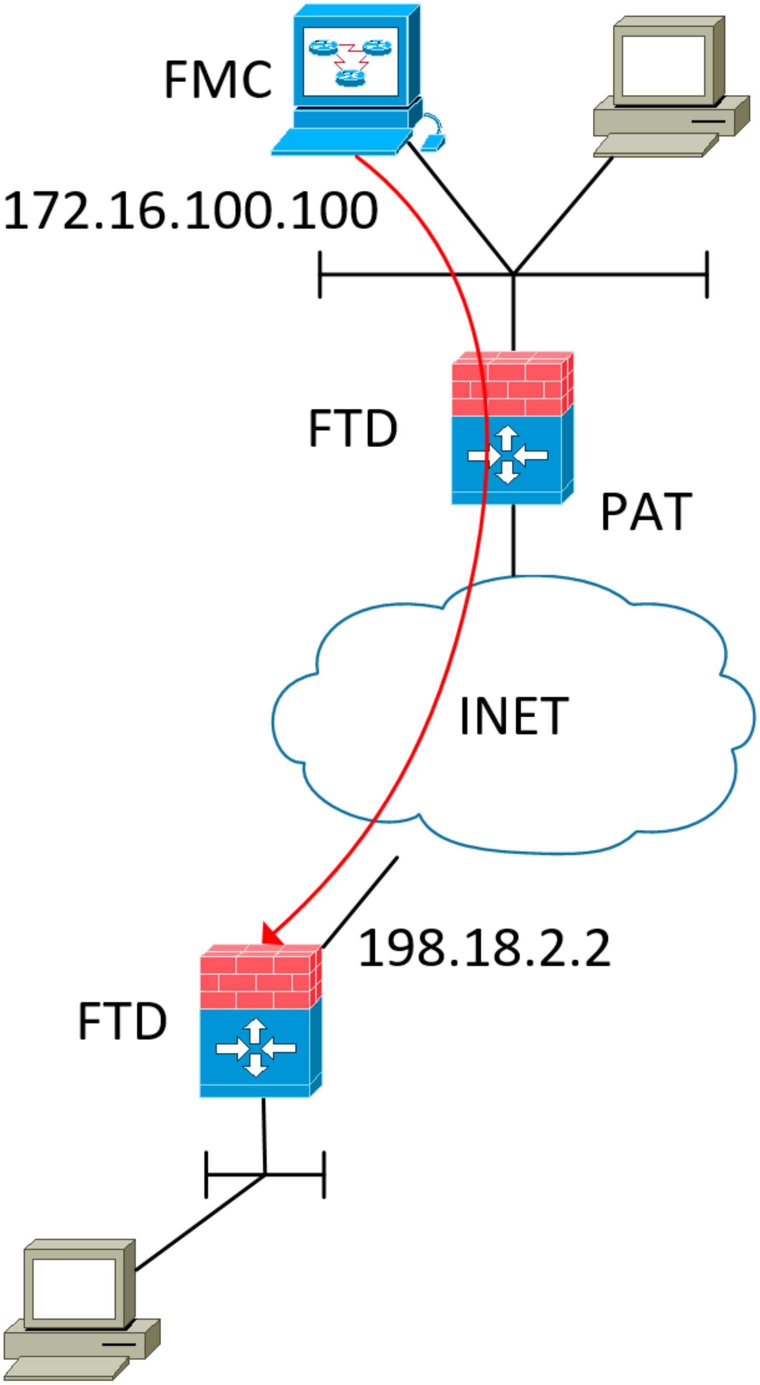
Cisco dCloud
Apache Guacamole
hq-wkst
hq-ftd
remote1-ftd
oob.vpod1499.dc-01.com/#/client/cmVtb3RlMS1mdGQAYwBkZWZhdWx0

```
Last login: Sat Apr 22 16:18:55 2017 from 198.18.129.0

Copyright 2004-2017, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.0 (build 42)
Cisco Firepower Threat Defense for VMWare v6.2.0 (build 362)

> configure manager add DONTRESOLVE cisco321 12345
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

> 
```

Since the FMC is sitting behind a NAT device (hq-ftd in this case) it doesn’t have a public IP to which you can associate this FTD to. Thus the “DONTRESOLVE” option vs. an actual IP address (along with the NAT-ID) will set this FTD up for communications from the FMC. Think of the “DONTRESOLVE” as a placeholder telling the command that you don’t have an IP for the FMC.

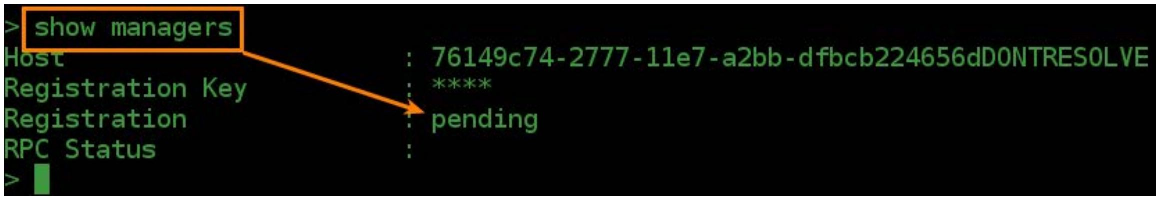
The “12345” part is the NAT-ID. This is a unique ID that will be used to identify this FTD to the FMC. (This means that each remote/branch FTD will need their own unique NAT ID.)

Figure 184. Direction of Registration Initialization



3. After a moment or two the “>” prompt will return. Issue the command **show managers** to see you have a Registration status of “pending”.

Figure 185. Show managers

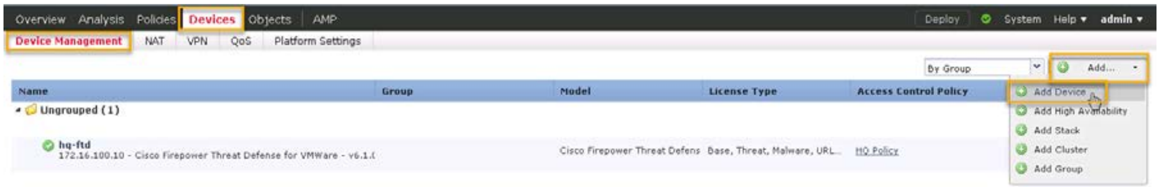


```
> show managers
Host                          : 76149c74-2777-11e7-a2bb-dfbcb224656dDONTRESOLVE
Registration Key              : ****
Registration                  : pending
RPC Status                    :
>
```

4. Return to the FMC administration website. Navigate to **Devices > Device Management**.

5. Click the **Add …** button and then select the **Add Device** option.

Figure 186. Add new device in FMC



Name	Group	Model	License Type	Access Control Policy
Ungrouped (1)				
hq-ftd 172.16.100.10 - Cisco Firepower Threat Defense for VMWare - v6.1.(		Cisco Firepower Threat Defens	Base, Threat, Malware, URL...	HQ Policy

6. Use the following information to fill in the necessary details. Take special note that you need to expand the “Advanced” section so you can add the NAT-ID value.

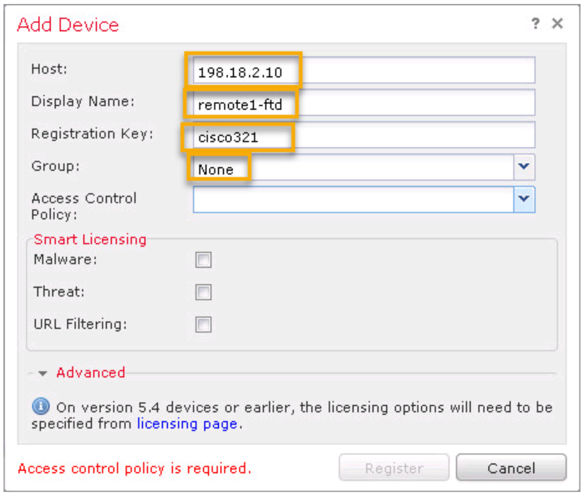
   a. Host: **198.18.2.10**

   b. Display Name: **remote1-ftd**

   c. Registration Key: **cisco321**

   d. Group: **None**

Figure 187. Part 1 of adding remote1-ftd to FMC



Add Device

Host: 198.18.2.10

Display Name: remote1-ftd

Registration Key: cisco321

Group: None

Access Control Policy:

Smart Licensing

Malware: □

Threat: □

URL Filtering: □

Advanced

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

Access control policy is required.

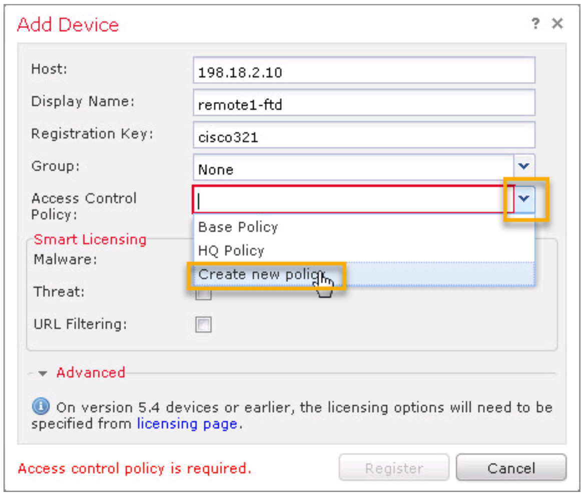
e. Access Control Policy: (You need to create a new policy for the Remote locations.) From the dropdown menu select **Create new policy** and then use the following to fill out the New Policy popup window.

   i. Name: **Remote Locations**

   ii. Select Base Policy: **Base Policy**

   iii. Click **Save**.

Figure 188. Create new ACP



Add Device

Host: 198.18.2.10

Display Name: remote1-ftd

Registration Key: cisco321

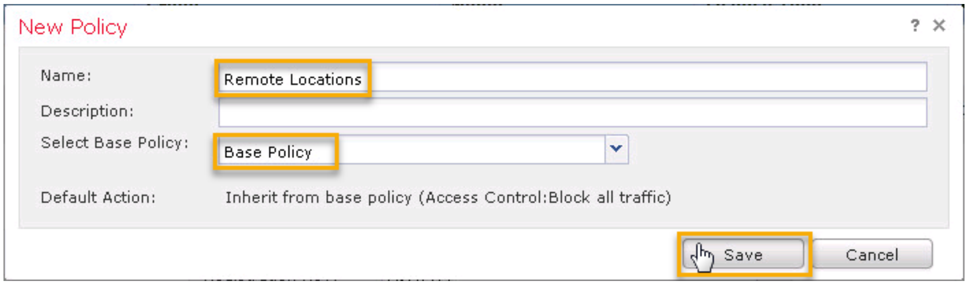
Group: None

Access Control Policy:

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

Access control policy is required.

Figure 189. New ACP



New Policy

Name: Remote Locations

Description:

Select Base Policy: Base Policy

Default Action: Inherit from base policy (Access Control:Block all traffic)

f. Ensure that the newly created policy is selected for the Access Control Policy.

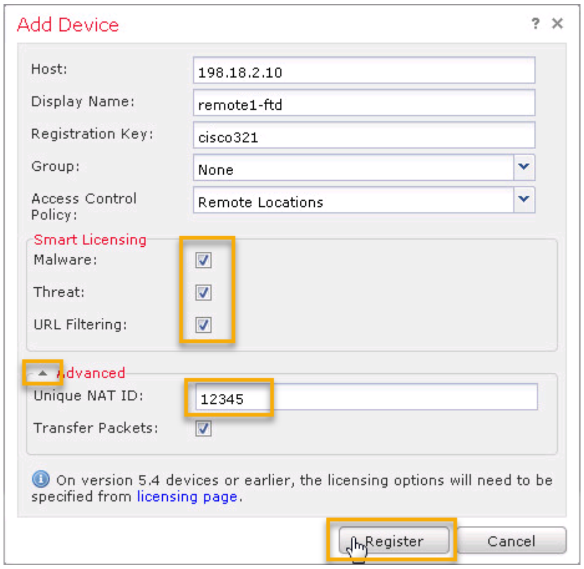
g. In the Smart Licensing section check all the boxes.

7. Expand the Advanced section by clicking the downward facing arrow next to the Advanced word.

   a. Unique NAT ID: **12345**

8. Click **Register**.

Figure 190. Finish adding remote1-ftd to FMC



Add Device

Host: 198.18.2.10

Display Name: remote1-ftd

Registration Key: cisco321

Group: None

Access Control Policy: Remote Locations

Smart Licensing

Malware: ☑

Threat: ☑

URL Filtering: ☑

Advanced

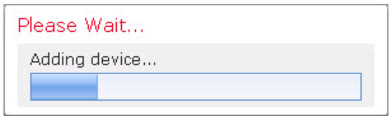
Unique NAT ID: 12345

Transfer Packets: ☑

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

9. The FMC will now reach out to the remote1-ftd device for registration, configuration synchronization, and to update any databases (such as the clam antivirus database). This process can take several minutes.

Figure 191. Status of registration



Please Wait...

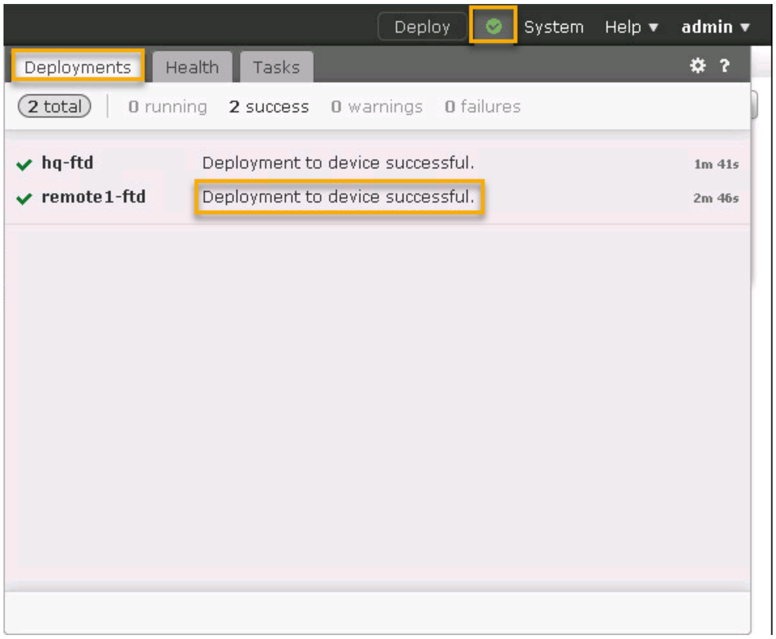
Adding device...

10. Once the FMC shows that it has found and registered with remote1-ftd return to the SSH session to remote1-ftd and re-issue the **show managers** command. You'll see that the Registration status show shows Completed.

Figure 192. Show managers, again

11. In the FMC, click the **Message Center icon** which is next to the Deploy button. Click the **Tasks tab**. This will show you the status of what is going on with the communication between the FMC and remote1-ftd. There are several databases and policies that need synchronized so this process can take several minutes. When it is done the icon next to remote1-ftd on the Device Management page will turn to a green checkmark.

Figure 193. Registration is complete



✓ hq-ftd	Deployment to device successful.	1m 41s
✓ remote1-ftd	Deployment to device successful.	2m 46s

Note: You might see errors regarding NTP sync (or errors about downloading database files). Given time these will resolve themselves. It is okay to ignore them for now.

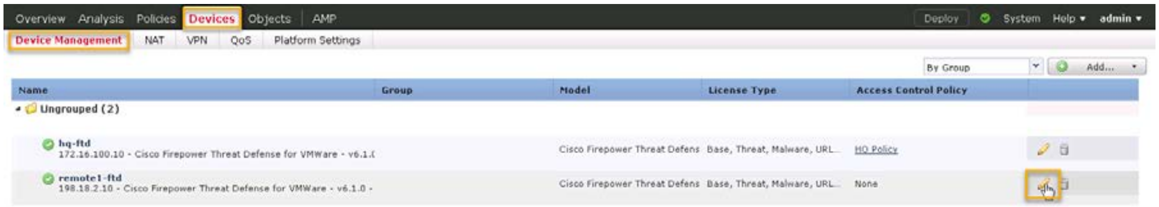
Don’t continue the lab until the remote1-ftd shows up with a green checkmark in the Message Center.

Configure remote1-ftd’s Data Plane

Now that the remote1-ftd is being configured by the FMC it is time to start setting up the data interfaces on the remote1-ftd device.

12. Navigate to Devices > Device Management.
13. Click the **pencil icon** on the row associated with **remote1-ftd**. This should take you to the Interfaces tab that lists all the available interfaces that can be used for accessing user data packets. In this lab GigabitEthernet0/0 is connected to the Remote1 LAN (inside) and GigabitEthernet0/1 is connected to the ISP (outside).

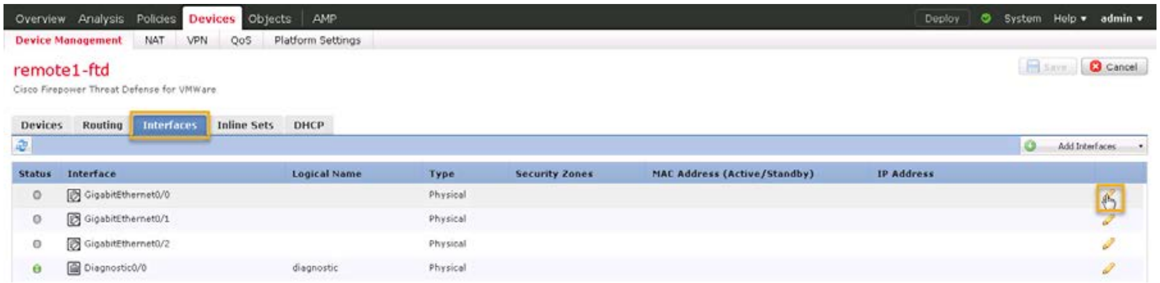
Figure 194. Edit remote1-ftd device



Name	Group	Model	License Type	Access Control Policy
Ungrouped (2)				
hq-ftd 172.16.100.10 - Cisco Firepower Threat Defense for VMWare - v6.1.(		Cisco Firepower Threat Defens	Base, Threat, Malware, URL...	HQ Policy
remote1-ftd 198.18.2.10 - Cisco Firepower Threat Defense for VMWare - v6.1.0 -		Cisco Firepower Threat Defens	Base, Threat, Malware, URL...	None

14. On the **Interfaces tab**, click the **pencil icon** on the row for **GigabitEthernet0/0**.

Figure 195. Edit g0/0



remote1-ftd
Cisco Firepower Threat Defense for VMWare

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
●	GigabitEthernet0/0		Physical			
●	GigabitEthernet0/1		Physical			
●	GigabitEthernet0/2		Physical			
●	Diagnostic0/0	diagnostic	Physical			

15. Use the following information to fill out the popup window:

    a. Mode: **None**

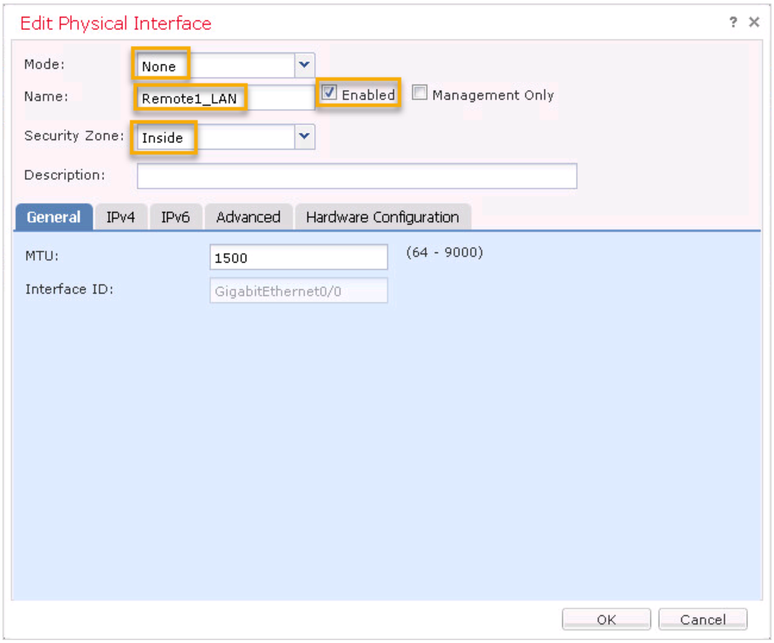
    b. Name: **Remote1_LAN**

    c. Check the **Enabled** box.

    d. Security Zone: **Inside**

This is the same Inside security zone that is applied to the hq-ftd device. So, any rules relating the Inside Zone will also be applied to this FTD's GigabitEthernet0/0 interface.

Figure 196. Part 1 of configuring g0/0



Edit Physical Interface

Mode: None

Name: Remote1_LAN ☑ Enabled □ Management Only

Security Zone: Inside

Description:

MTU: 1500 (64 - 9000)

Interface ID: GigabitEthernet0/0

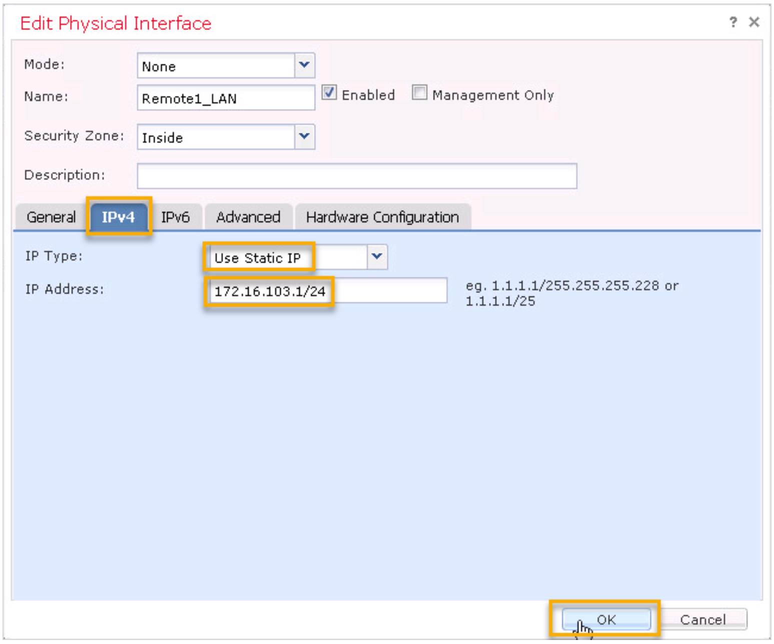
16. Click the **IPv4 tab**.

    a. IP Type: **Use Static IP**

    b. IP Address: **172.16.103.1/24**

17. Click **OK**.

Figure 197. Add IP and click OK



Edit Physical Interface

Mode: None

Name: Remote1_LAN ☑ Enabled □ Management Only

Security Zone: Inside

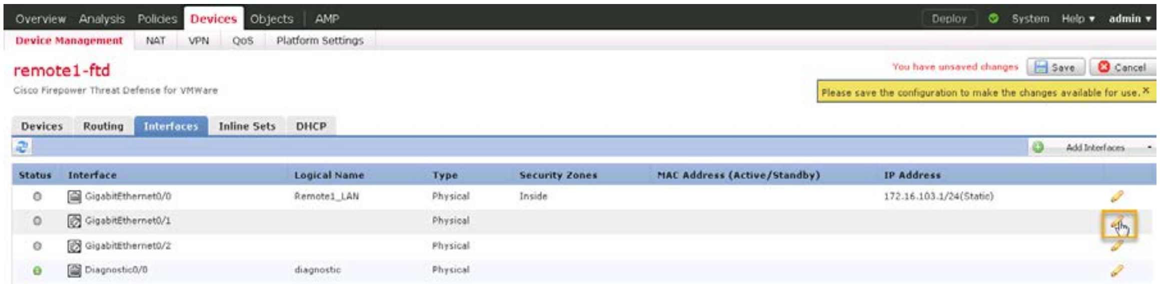
Description:

IP Type: Use Static IP

IP Address: 172.16.103.1/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

18. Click the **pencil icon** on the row for **GigabitEthernet0/1**.

Figure 198. Edit g0/1



remote1-ftd

Cisco Firepower Threat Defense for VMWare

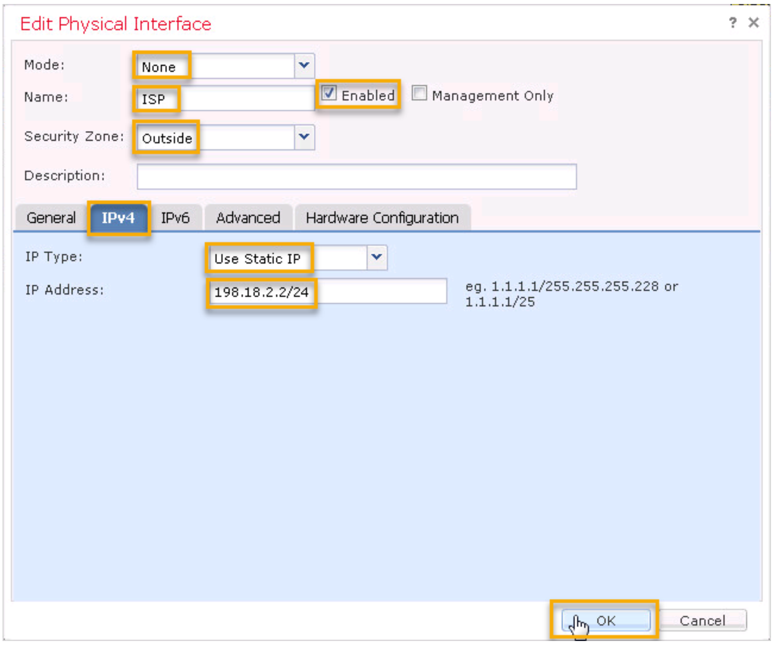
You have unsaved changes

Please save the configuration to make the changes available for use.

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
○	GigabitEthernet0/0	Remote1_LAN	Physical	Inside		172.16.103.1/24(Static)
○	GigabitEthernet0/1		Physical			
○	GigabitEthernet0/2		Physical			
●	Diagnostic0/0	diagnostic	Physical			

19. Use the following information to fill out the popup window:
    a. Mode: **None**
    b. Name: **ISP**
    c. Check the **Enabled** box.
    d. Security Zone: **Outside**
20. Click the **IPv4 tab**.
    a. IP Type: **Use Static IP**
    b. IP Address: **198.18.2.2/24**
21. Click **OK**.

Figure 199. Configure g0/1



Edit Physical Interface

Mode: None

Name: ISP ☑ Enabled □ Management Only

Security Zone: Outside

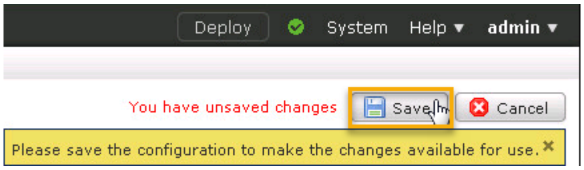
Description:

IP Type: Use Static IP

IP Address: 198.18.2.2/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

22. Click **Save** to apply the interface names and zones so you can reference them for the next steps.

Figure 200. Save to FMC before continuing



You have unsaved changes

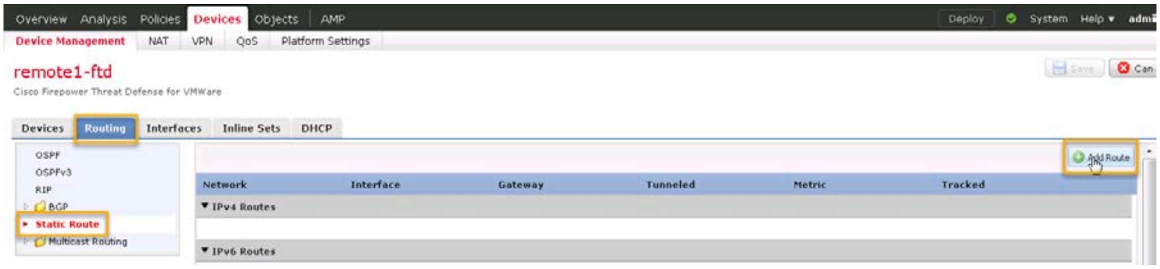
Please save the configuration to make the changes available for use.

23. Click the **Routing tab**.

24. Click on the **Static Route** menu option.

25. Click the **Add Route** button on the right side of the web page.

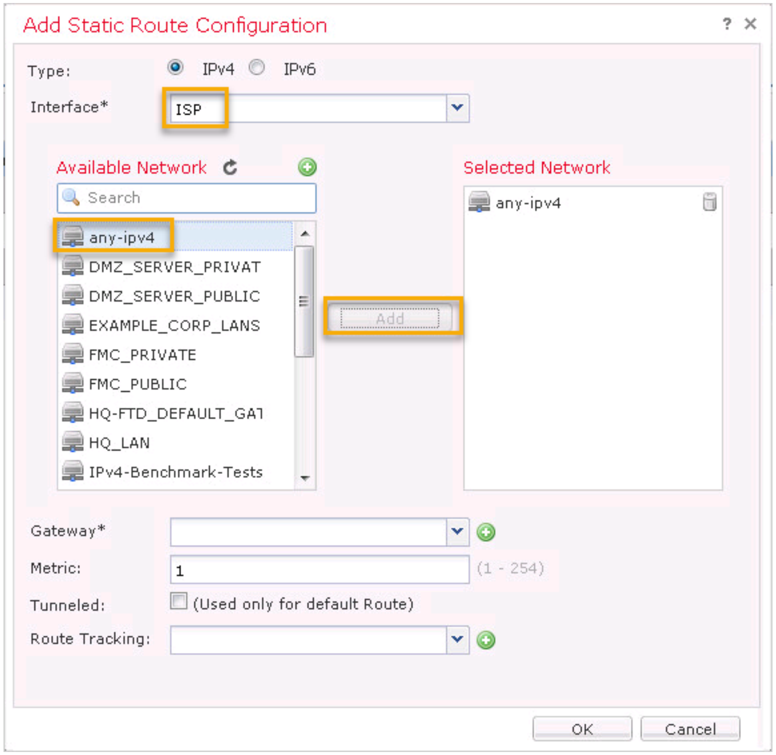
Figure 201. Start to add static route



26. Using the dropdown for the **Interface** option select **ISP**.

27. From the **Available Networks** list of items select the **any-ipv4** option and then click the **Add** button to move it to the Selected Network list. This is equivalent to the 0.0.0.0/0 network.

Figure 202. Part 1 of adding static route


Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface* ISP

Available Network

- any-ipv4
- DMZ_SERVER_PRIVAT
- DMZ_SERVER_PUBLIC
- EXAMPLE_CORP_LANS
- FMC_PRIVATE
- FMC_PUBLIC
- HQ-FTD_DEFAULT_GAT
- HQ_LAN
- IPv4-Benchmark-Tests

Selected Network

- any-ipv4

Gateway*

Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:

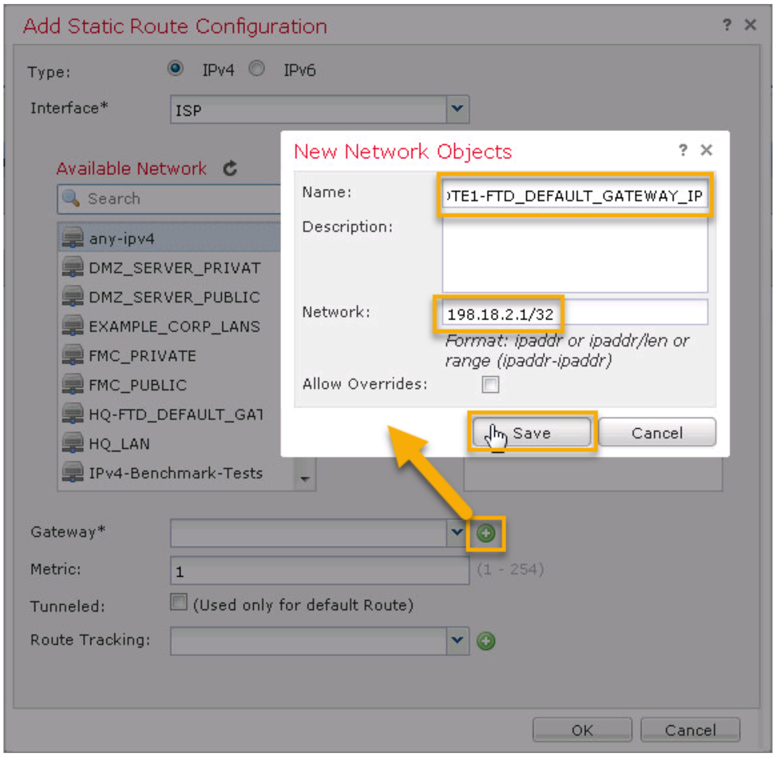
28. Next to the Gateway dropdown menu click the **green plus icon** and create a Network Object for the ISP's default gateway IP.

    a. Name: **REMOTE1-FTD_DEFAULT_GATEWAY_IP**

    b. Network: **198.18.2.1/32**

    c. Click **Save**.

Figure 203. Create Network Object



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: ISP

New Network Objects

Name: ›TE1-FTD_DEFAULT_GATEWAY_IP

Description:

Network: 198.18.2.1/32

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides: □

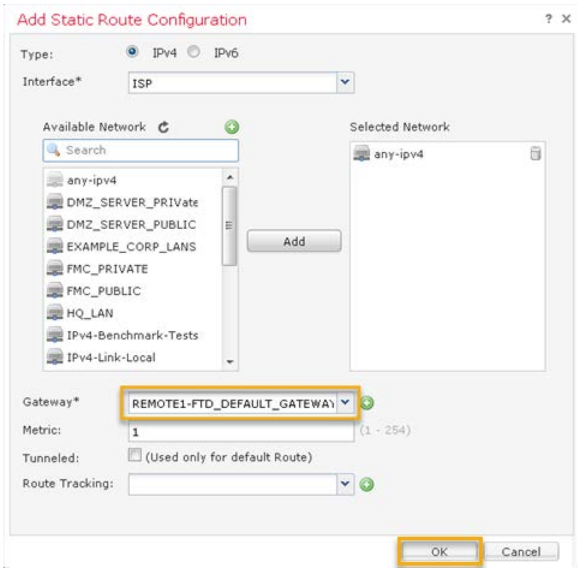
Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

29. For the **Gateway** option use the dropdown menu to select the **REMOTE1-FTD_DEFAULT_GATEWAY_IP** Network Object.

30. Click **OK** to add the static route.

Figure 204. Finish creating static route



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface* ISP

Available Network

- any-ipv4
- DMZ_SERVER_PRIVate
- DMZ_SERVER_PUBLIC
- EXAMPLE_CORP_LANS
- FMC_PRIVATE
- FMC_PUBLIC
- HQ_LAN
- IPv4-Benchmark-Tests
- IPv4-Link-Local

Selected Network

- any-ipv4

Gateway* REMOTE1-FTD_DEFAULT_GATEWAY

Metric: 1 (1 - 254)

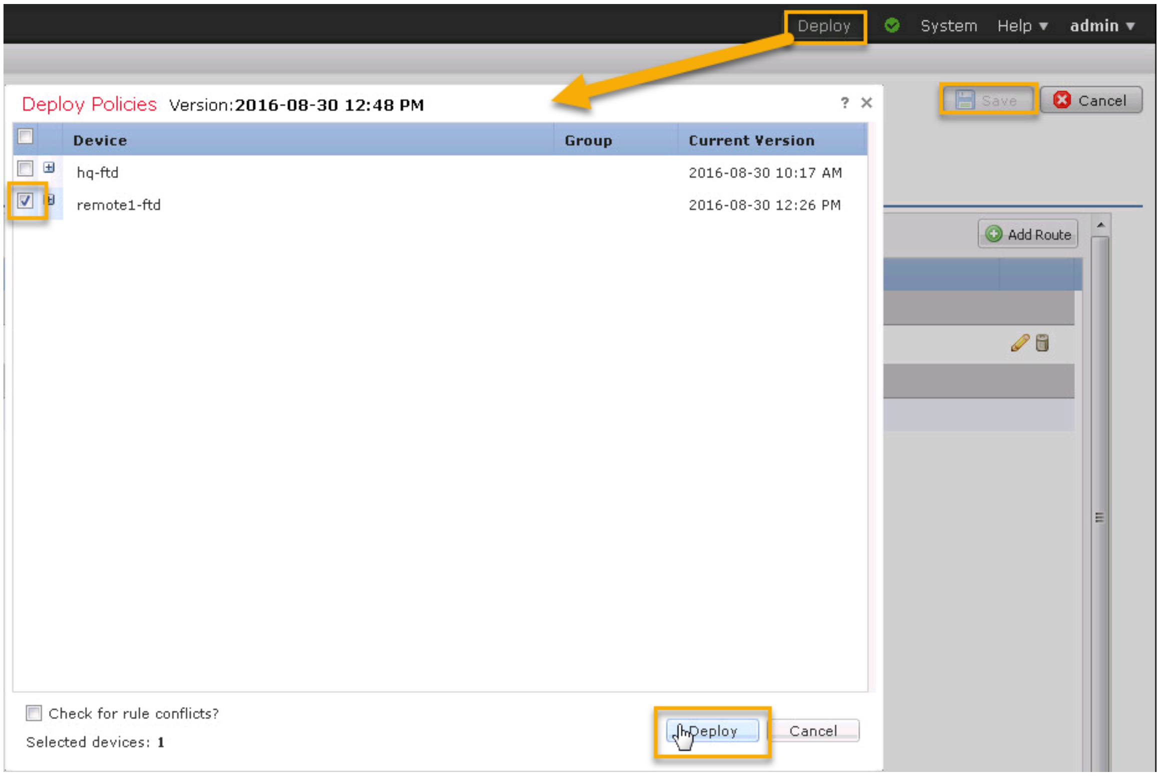
Tunneled: □ (Used only for default Route)

Route Tracking:

31. Click **Save** and then **Deploy**.

32. Select the **remote1-ftd** device, and click **Deploy** to push these changes to that device.

Figure 205. Save and Deploy to remote1-ftd



Deploy Policies Version:**2016-08-30 12:48 PM**

□	Device	Group	Current Version
□ ⊞	hq-ftd		2016-08-30 10:17 AM
☑ ⊞	remote1-ftd		2016-08-30 12:26 PM

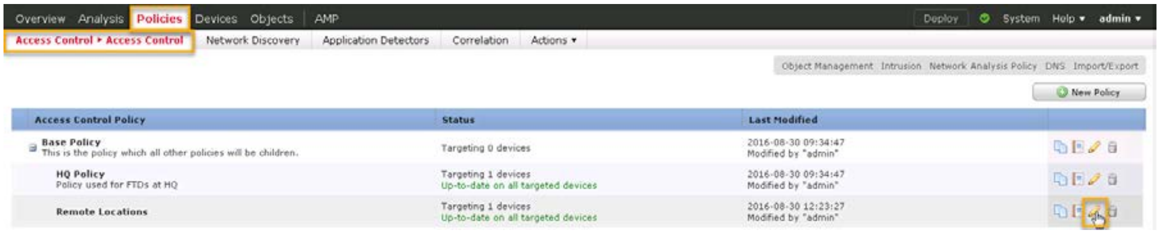
□ Check for rule conflicts?

Selected devices: **1**

Before you go to the testing phase let’s take a look at the Access Control Policies and the NAT Policies to see if you can predict what a ping and/or URL request from remote1-wkst might produce.

33. Go to **Policies > Access Control > Access Control** and click the **pencil icon** on the row for the **Remote Locations** policy.

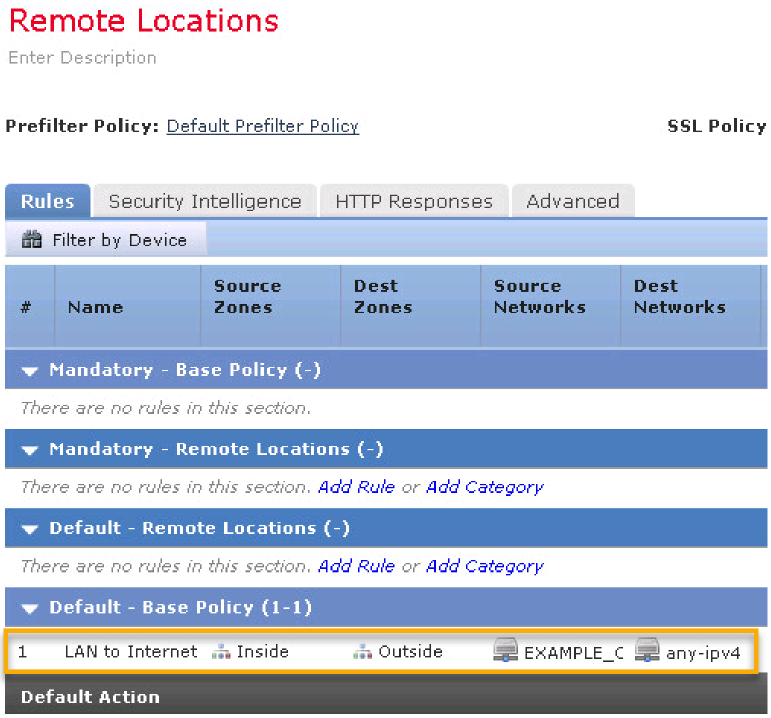
Figure 206. Edit Remote Locations ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-30 09:34:47 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-30 09:34:47 Modified by "admin"
Remote Locations	Targeting 1 devices Up-to-date on all targeted devices	2016-08-30 12:23:27 Modified by "admin"

34. Expand all the Policy sections. The only section that should have a rule in it is the **Default – Base Policy** section. This rule says that any IP in the Example Corp LAN IP range sourced from the Inside zone destined for the Outside zone will be allowed. So, without adding any new Access Control Policies it appears that ping and HTTP should work!

Figure 207. Expand all sections



Remote Locations

Enter Description

Prefilter Policy: Default Prefilter Policy

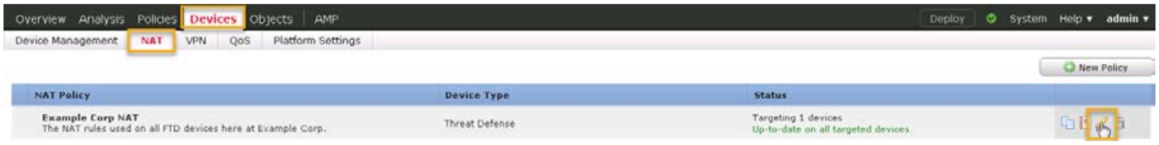
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - Base Policy (-)					
There are no rules in this section.					
Mandatory - Remote Locations (-)					
There are no rules in this section. Add Rule or Add Category					
Default - Remote Locations (-)					
There are no rules in this section. Add Rule or Add Category					
Default - Base Policy (1-1)					
1	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4
Default Action					

Notice that you do not see the other rules that you created earlier since they are associated with the other child Access Control Policy called HQ Policy.

35. Go to **Devices > NAT**.

36. Click the **pencil icon** for the **Example Corp NAT** policy.

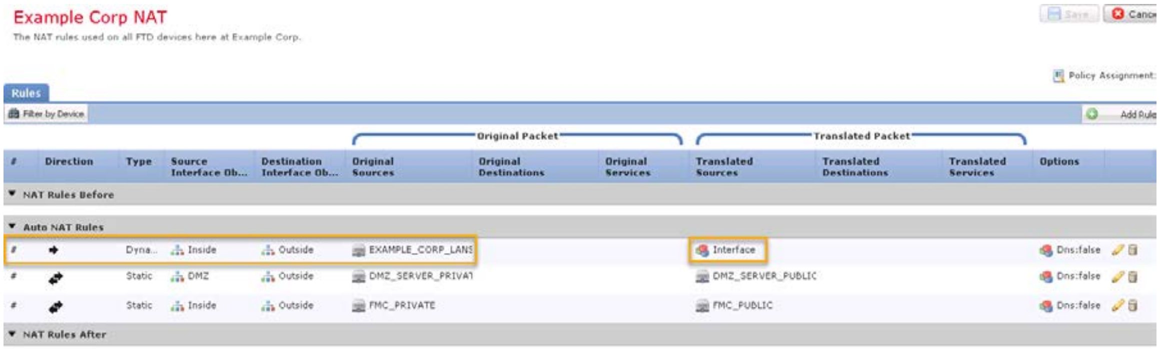
Figure 208. Edit NAT policy



NAT Policy	Device Type	Status
Example Corp NAT The NAT rules used on all FTD devices here at Example Corp.	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

37. Though there are three rules in this policy only one of them would be applicable to remote1-ftd. The remote-ftd device doesn't have an interface in the DMZ zone nor is the FMC static translation valid. So, the first NAT rule would apply. This rule states that an IP from the Example_Corp_LANs range, from an Inside zone destined for the Outside zone, would be NATted using the interface IP on this FTD where that interface is associated with the Outside zone. Thus, remote1-wkst IP traffic will be NATted based on this rule.

Figure 209. Review the NAT rules



Example Corp NAT

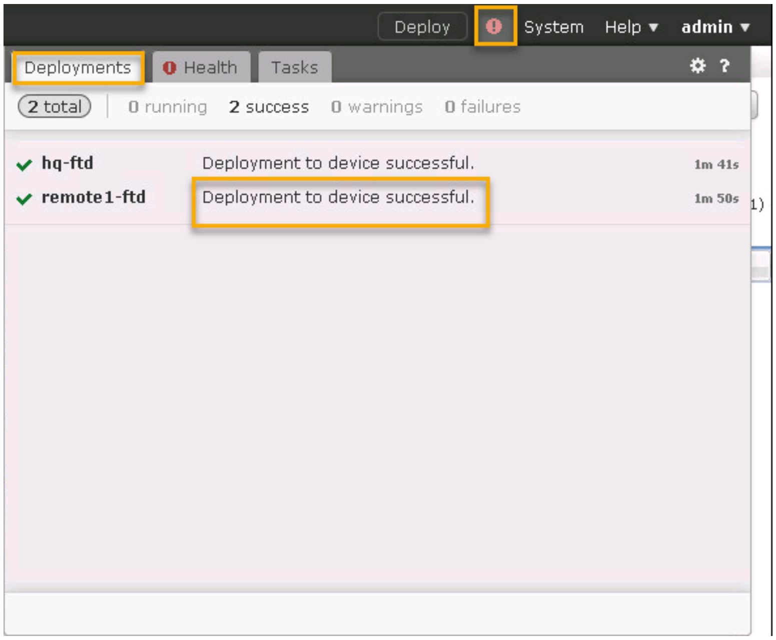
The NAT rules used on all FTD devices here at Example Corp.

					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Ob...	Destination Interface Ob...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
▼ Auto NAT Rules											
#	→	Dyna...	Inside	Outside	EXAMPLE_CORP_LANS			Interface			Dns:false
#	⇄	Static	DMZ	Outside	DMZ_SERVER_PRIVAT			DMZ_SERVER_PUBLIC			Dns:false
#	⇄	Static	Inside	Outside	FMC_PRIVATE			FMC_PUBLIC			Dns:false
▼ NAT Rules After											

Testing INET Access and Access Control Policies -- Failure

38. Check the **Message Center > Deployments** notifications to ensure that the remote1-ftd deployment is done.

Figure 210. Ensure deployment is complete



2 total | 0 running | 2 success | 0 warnings | 0 failures

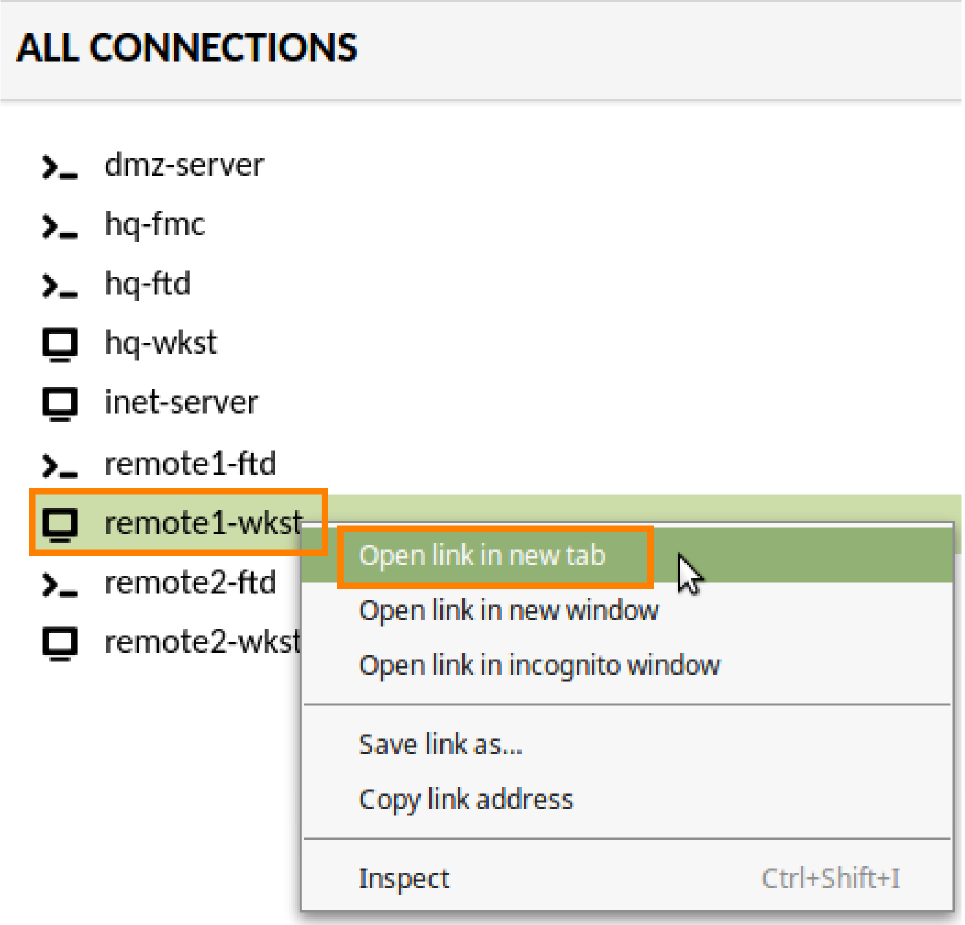
✓ hq-ftd Deployment to device successful. 1m 41s

✓ remote1-ftd Deployment to device successful. 1m 50s

Do not continue the lab until the deployed changes to remote1-ftd via the FMC are complete.

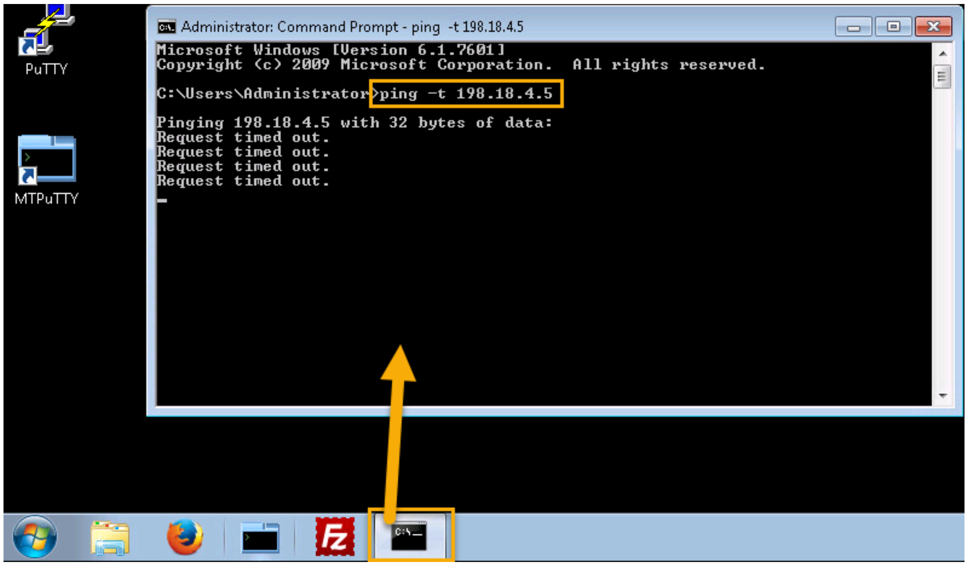
39. Using the connection on the **oob web page** on a **new tab** to **remote1-wkst**. This will auto log in as administrator/C1sco12345.

Figure 211. Connec to remote1-wkst



40. On remote1-wkst, open up a **CMD prompt** and issue the command **ping –t 198.18.4.5** (the inet-server). It fails. Why?

Figure 212. Failed pings



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ping -t 198.18.4.5

Pinging 198.18.4.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
_
```

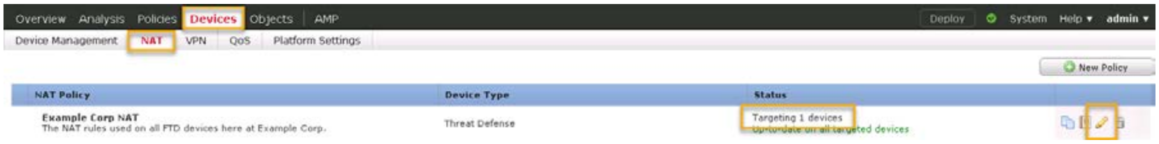
remote1-ftd Continued Configuration

The ping from remote1-wkst failed because even though an Access Control Policy is assigned during the process of registering an FTD with the FMC, other policies (such as any NAT policies) don't automatically get assigned to this new device. For now, the only configuration that remote1-FTD is lacking is a NAT policy. Let's resolve this issue:

41. On **hq-wkst** return to the FMC administration website. Go to **Devices > NAT**. Notice that the Example Corp NAT rule's Status is Targeting 1 device.

42. Click the **pencil icon** for this rule.

Figure 213. Review NAT Policy



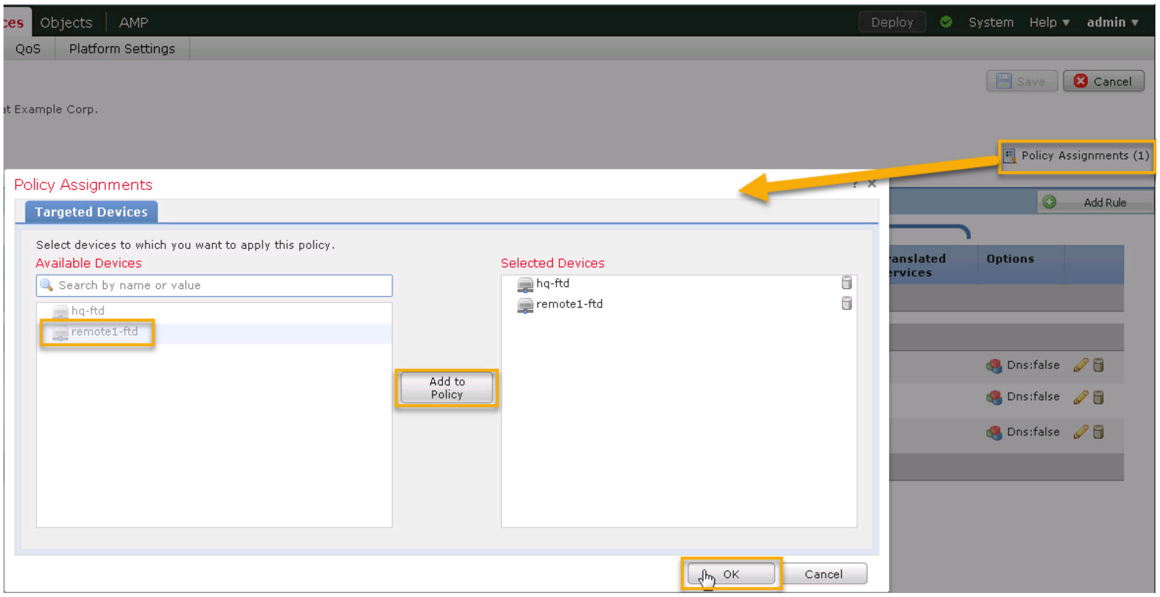
NAT Policy	Device Type	Status
Example Corp NAT The NAT rules used on all FTD devices here at Example Corp.	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

43. Click the **Policy Assignments** link in the upper right side of the web page.

44. From the **Available Devices** section click the **remote1-ftd** device and then click the **Add to Policy** button.

45. Click **OK**.

Figure 214. Add remote1-ftd to NAT policy



Policy Assignments

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

- hq-ftd
- remote1-ftd

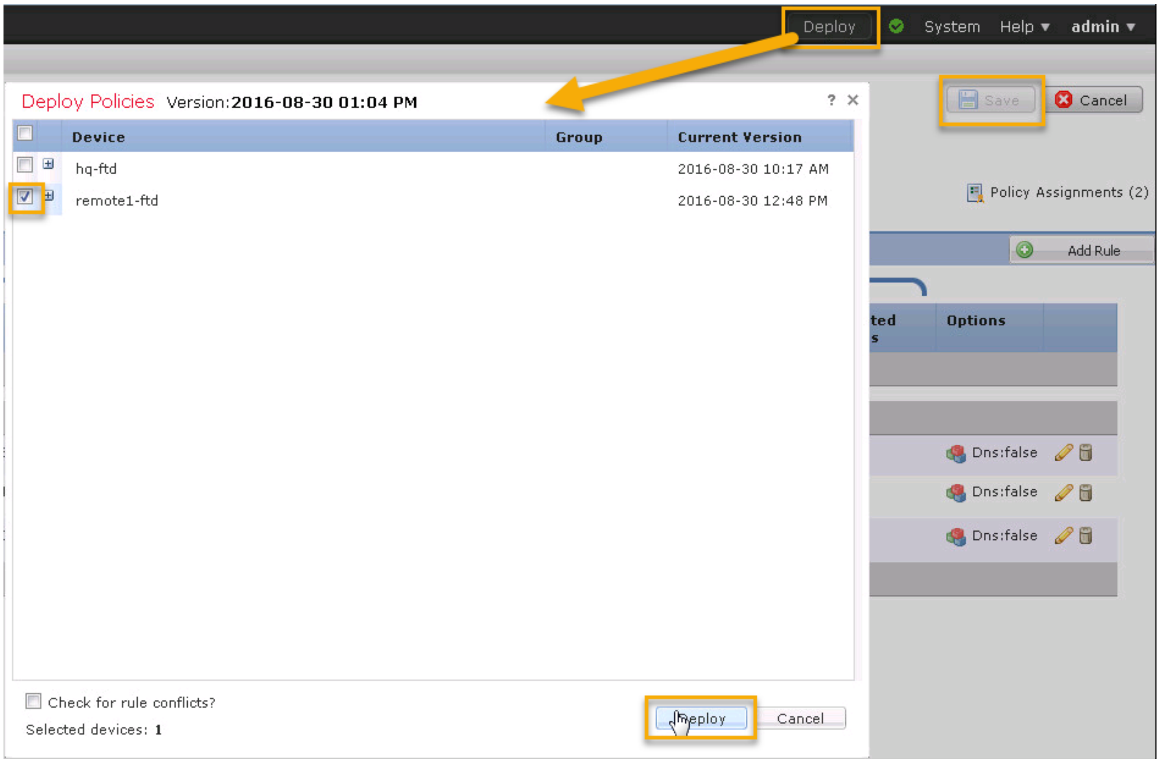
Selected Devices

- hq-ftd
- remote1-ftd

46. Click **Save**, then **Deploy**

47. Select the **remote1-ftd** device and click **Deploy**.

Figure 215. Save and Deploy to remote1-ftd



Deploy Policies Version:**2016-08-30 01:04 PM**

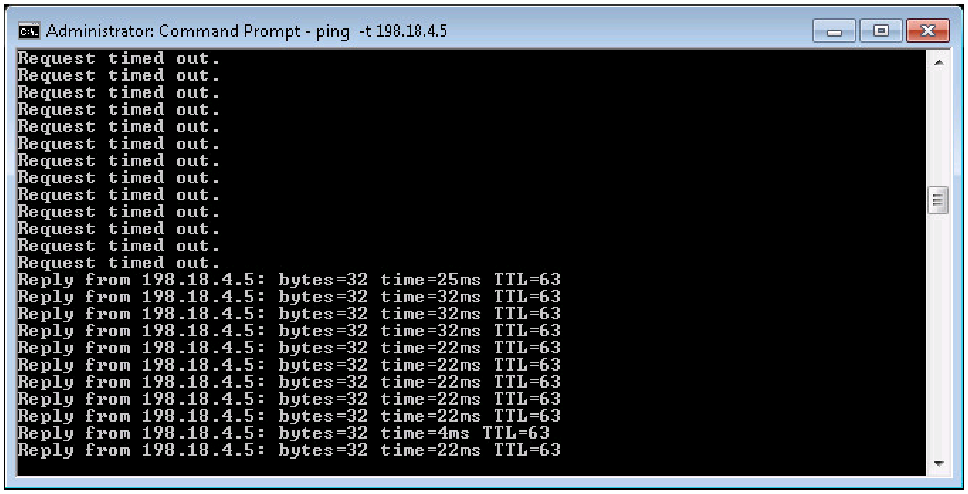
□	Device	Group	Current Version
□	hq-ftd		2016-08-30 10:17 AM
☑	remote1-ftd		2016-08-30 12:48 PM

□ Check for rule conflicts?

Selected devices: **1**

48. Once the deployment is finished the ping on remote1-wkst should start to work.

Figure 216. Pinging on remote1-wkst start working



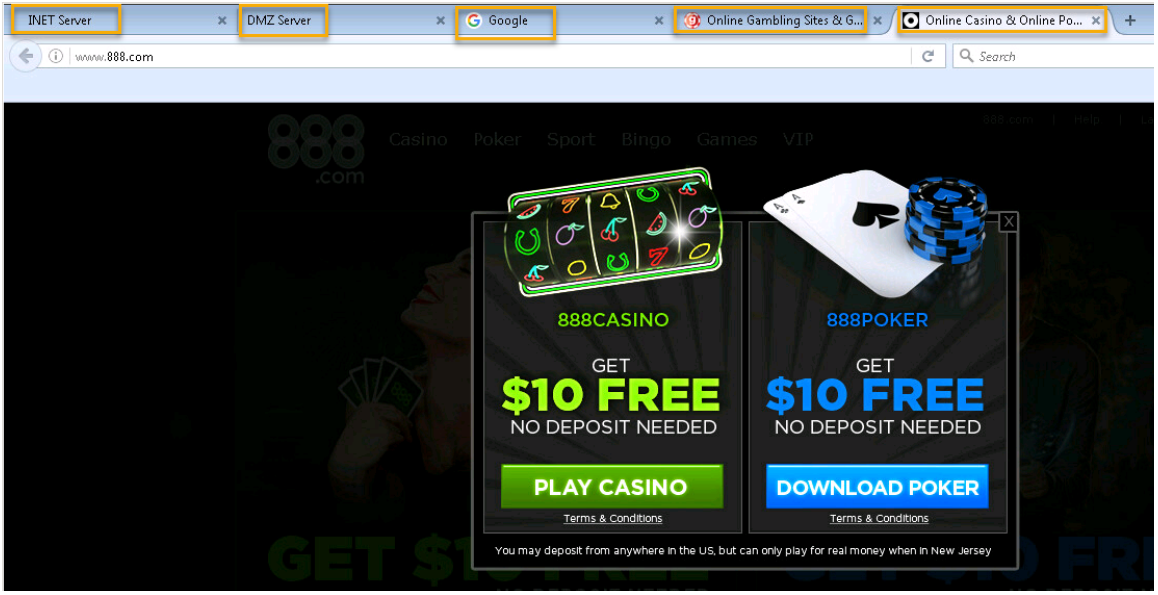
```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 198.18.4.5: bytes=32 time=25ms TTL=63
Reply from 198.18.4.5: bytes=32 time=32ms TTL=63
Reply from 198.18.4.5: bytes=32 time=32ms TTL=63
Reply from 198.18.4.5: bytes=32 time=32ms TTL=63
Reply from 198.18.4.5: bytes=32 time=22ms TTL=63
Reply from 198.18.4.5: bytes=32 time=22ms TTL=63
Reply from 198.18.4.5: bytes=32 time=22ms TTL=63
Reply from 198.18.4.5: bytes=32 time=22ms TTL=63
Reply from 198.18.4.5: bytes=32 time=22ms TTL=63
Reply from 198.18.4.5: bytes=32 time=4ms TTL=63
Reply from 198.18.4.5: bytes=32 time=22ms TTL=63
```

Testing INET Access and Access Control Policies -- Success

49. On **remote1-wkst** and open up **Firefox**.

50. **Refresh** each of the open tabs. They all should work. Note that two of the tabs: **www.gambling.com** and **www.888.com** work but eventually you don't want these to work.

Figure 217. Firefox tabs refreshed and working



You can close the **remote1-ftd** tab in your browser as it won't be used again for a while.

Scenario Summary

Not having a CLI method for configuring a devices data plane can be challenging. It is most important that you, as a deployment engineer, know that your options for deploying FTD devices are constrained by your ability to use some sort of "Manager" (whether that be the Firepower Device Manager or the FMC) to configure the FTD's data plane (and other features). The FTD's management NIC needs to have a "not through the FTD's data plane" path to the FMC, at least for the initial configuration of the FTD device. That said, it is dangerous to have the FTD's management network get access to the FMC via its own data plane. Should you lose that data plane you also lose the ability to manage that FTD device!

The only policy that gets applied during the registration process of an FTD device to the FMC is the Access Control Policy. This means other policies (that aren't directly attached to the Access Control Policy) need to be associated with this newly added FTD device. Depending on the company's deployment strategy you could add the newly registered device to the access control policy they will eventually use (like what you did in this lab) or you could have a "quarantine" access control policy that new devices get added to so that they can be configured fully before being put into the "production" access control policy.

Page intentionally left blank.

Scenario 5. Installing the FTD at the Remote2 Site Using DHCP IP for Mgmt

Scenario Description

This site, remote2, is going to be similarly configured as to site remote1 with one “small” change. This site’s outside interface(s) will not have static IP address assignments. This type of deployment will be seen more often in the real world than the use of static addressing. So, the management NIC and the “outside” data plane NIC will both be using DHCP to get their IP address from the ISP’s DHCP server.

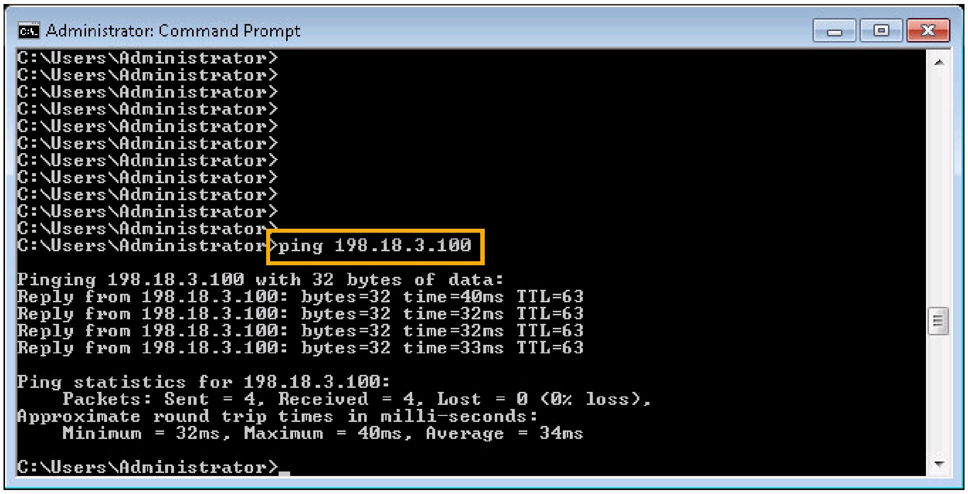
Registering remote2-ftd with hq-fmc

In this scenario, you will know the IP address of the FMC but not necessarily always know what the IP address of the FTD will be. This is because the management NIC is receiving its IP address from the ISP via DHCP. This is why you set up the FMC with a static NAT translation earlier in the lab!

> The trick with this configuration is that you’ll need access the remote2-ftd device just long enough to issue the command to associate it to hq-fmc. More than likely its IP address is 198.18.3.100 (the first in the DHCP pool) but you may have to test a few more IPs (.101 on up).

1. On **hq-wkst** open up a **CMD prompt** and **ping 198.18.3.100**. If you do not get a response then try 198.18.3.101, etc. The management NIC of remote2-ftd should be the only thing that will respond. If you make it to, say, .110 with no response talk with your lab proctor.

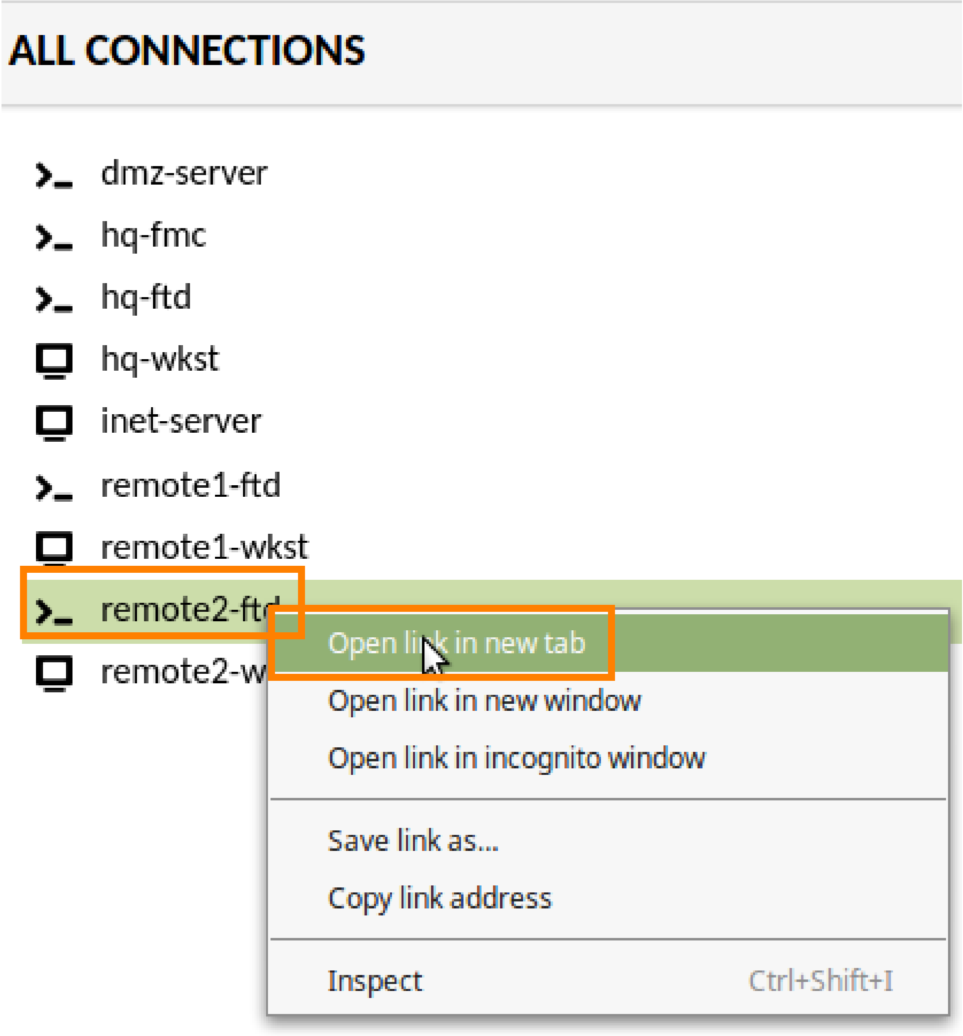
Figure 218. Finding remote2-ftd’s management IP



```
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>ping 198.18.3.100

Pinging 198.18.3.100 with 32 bytes of data:
Reply from 198.18.3.100: bytes=32 time=40ms TTL=63
Reply from 198.18.3.100: bytes=32 time=32ms TTL=63
Reply from 198.18.3.100: bytes=32 time=32ms TTL=63
Reply from 198.18.3.100: bytes=32 time=33ms TTL=63

Ping statistics for 198.18.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 40ms, Average = 34ms

C:\Users\Administrator>_
```

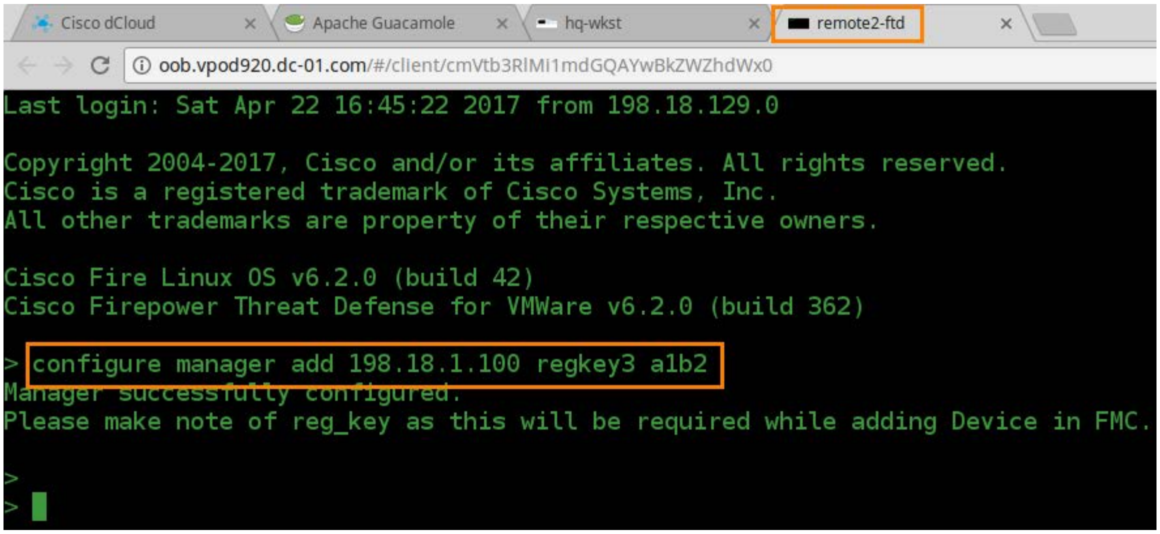
2. **IF** the remote2-ftd responds on 198.18.3.100 you can use the oob webpage link to connect to remote2-ftd. If you have found that remote2-ftd is on another IP then on hq-wkst open up PuTTY and access remote2-ftd via the IP you found. The credentials are **admin**/**Admin123**.

Figure 219. Connect to remote2-ftd



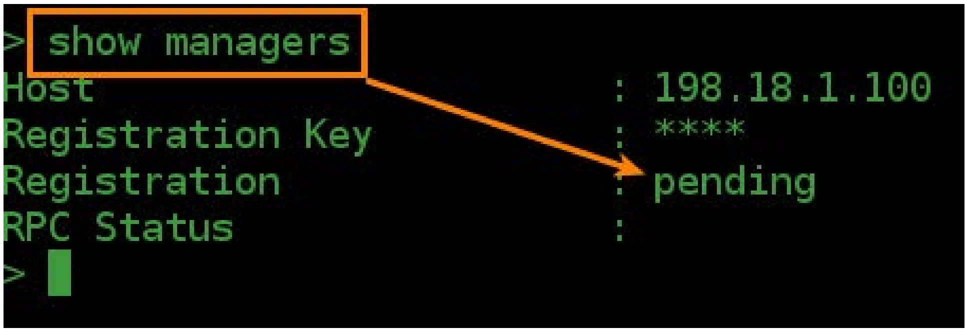
3. Issue the command **configure manager add 198.18.1.100 regkey3 a1b2**. Notice that this time you are using the static NAT public IP address of the FMC and not the “DONTRESOLVE” keyword. Also note that the registration key does NOT have to be unique for each FTD (though I tried to make it so in this lab) but the NAT ID does need to be unique.

Figure 220. Configure manager for remote2-ftd



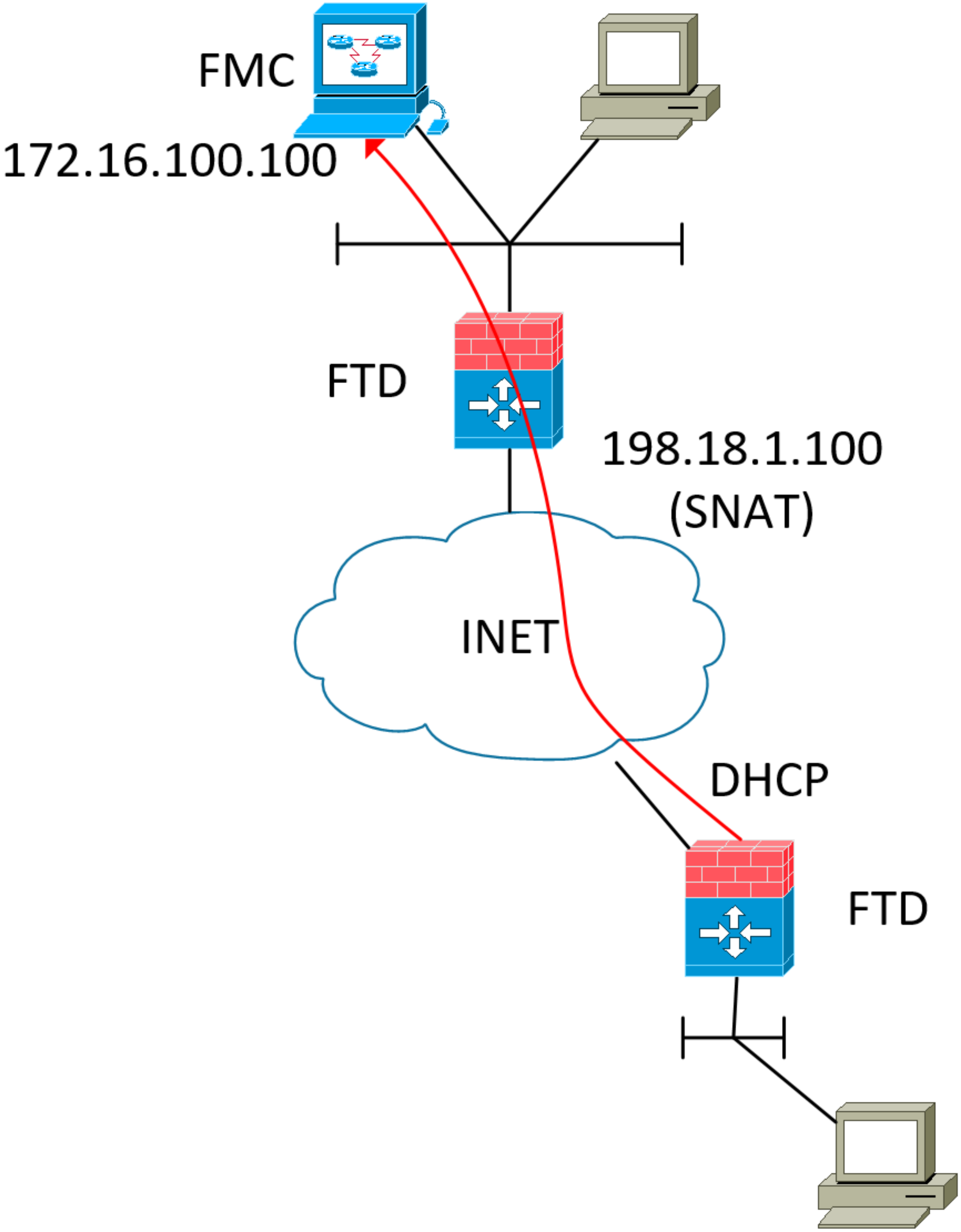
```
Last login: Sat Apr 22 16:45:22 2017 from 198.18.129.0

Copyright 2004-2017, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.0 (build 42)
Cisco Firepower Threat Defense for VMWare v6.2.0 (build 362)

> configure manager add 198.18.1.100 regkey3 a1b2
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
>
```

Figure 221. Show Managers



```
> show managers
Host                              : 198.18.1.100
Registration Key                  : ****
Registration                      : pending
RPC Status                        :
>
```

Figure 222. Direction of Registration Initialization

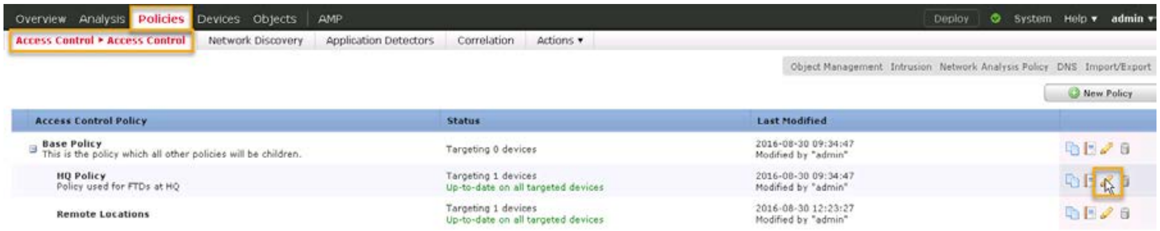


Though you have already set up the Static NAT translation for the FMC you haven't set up any Access Control Policy rules to allow incoming connection (from the outside zone) through the hq-ftd for the FMC. Since remote2-ftd will need to be the device to initiate the connection between itself and the FMC you need to add an Access Control Policy rule for this to happen.

4. In the FMC administration website navigate to **Policies > Access Control > Access Control**.

5. Click the **pencil icon** on the row associated with the **HQ Policy**.

Figure 223. Edit HQ Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-30 09:34:47 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-30 09:34:47 Modified by "admin"
Remote Locations	Targeting 1 devices Up-to-date on all targeted devices	2016-08-30 12:23:27 Modified by "admin"

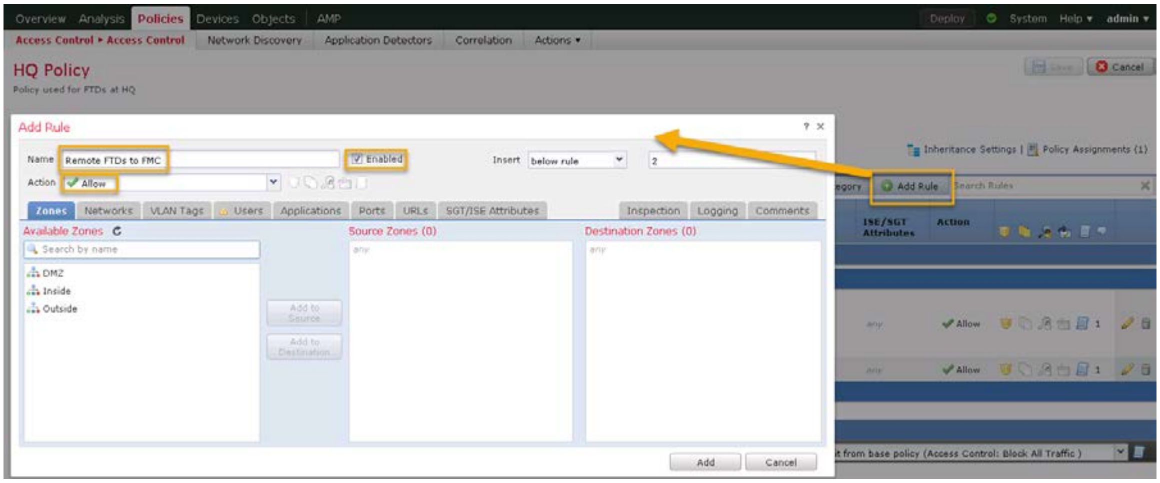
6. Click **Add Rule** and use the following to fill out the needed information.

   a. Name: **Remote FTDs to FMC**

   b. Enabled: **Checked**

   c. Action: **Allow**

Figure 224. Create a new rule, part 1



Name: Remote FTDs to FMC ☑ Enabled Insert: below rule 2

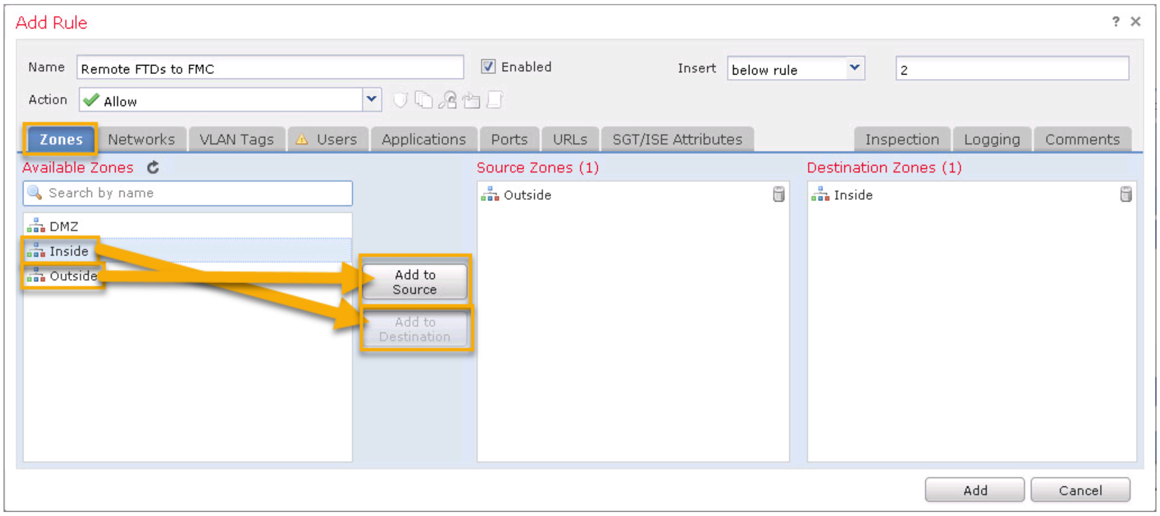
Action: ✓ Allow

7. On the **Zones tab**:

   a. From the **Available Zones** list select **Outside** and then click **Add to Source**.

   b. From the **Available Zones** list select **Inside** and then click **Add to Destination**.

Figure 225. Configure Zones tab



Add Rule

Name: Remote FTDs to FMC

☑ Enabled

Insert: below rule, 2

Action: Allow

Available Zones: DMZ, Inside, Outside

Source Zones (1): Outside

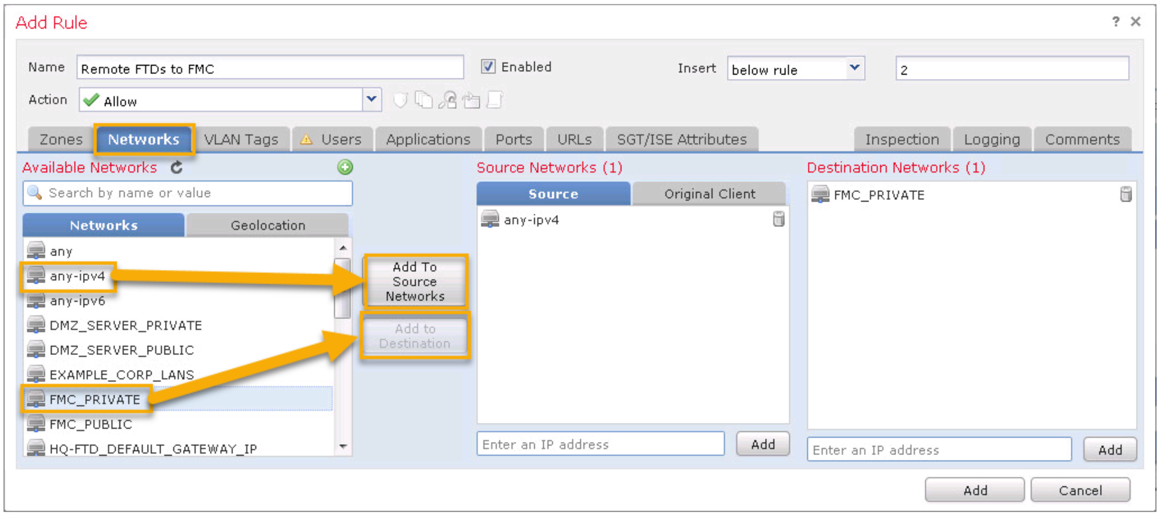
Destination Zones (1): Inside

8. On the **Networks tab**:

   a. From the **Available Networks** list select **any-ipv4** and click the **Add to Source Networks** button.

   b. From the **Available Networks** list select **FMC_PRIVATE** and click the **Add to Destination** button.

Figure 226. Configure Networks tab



Add Rule

Name: Remote FTDs to FMC

☑ Enabled

Insert: below rule, 2

Action: Allow

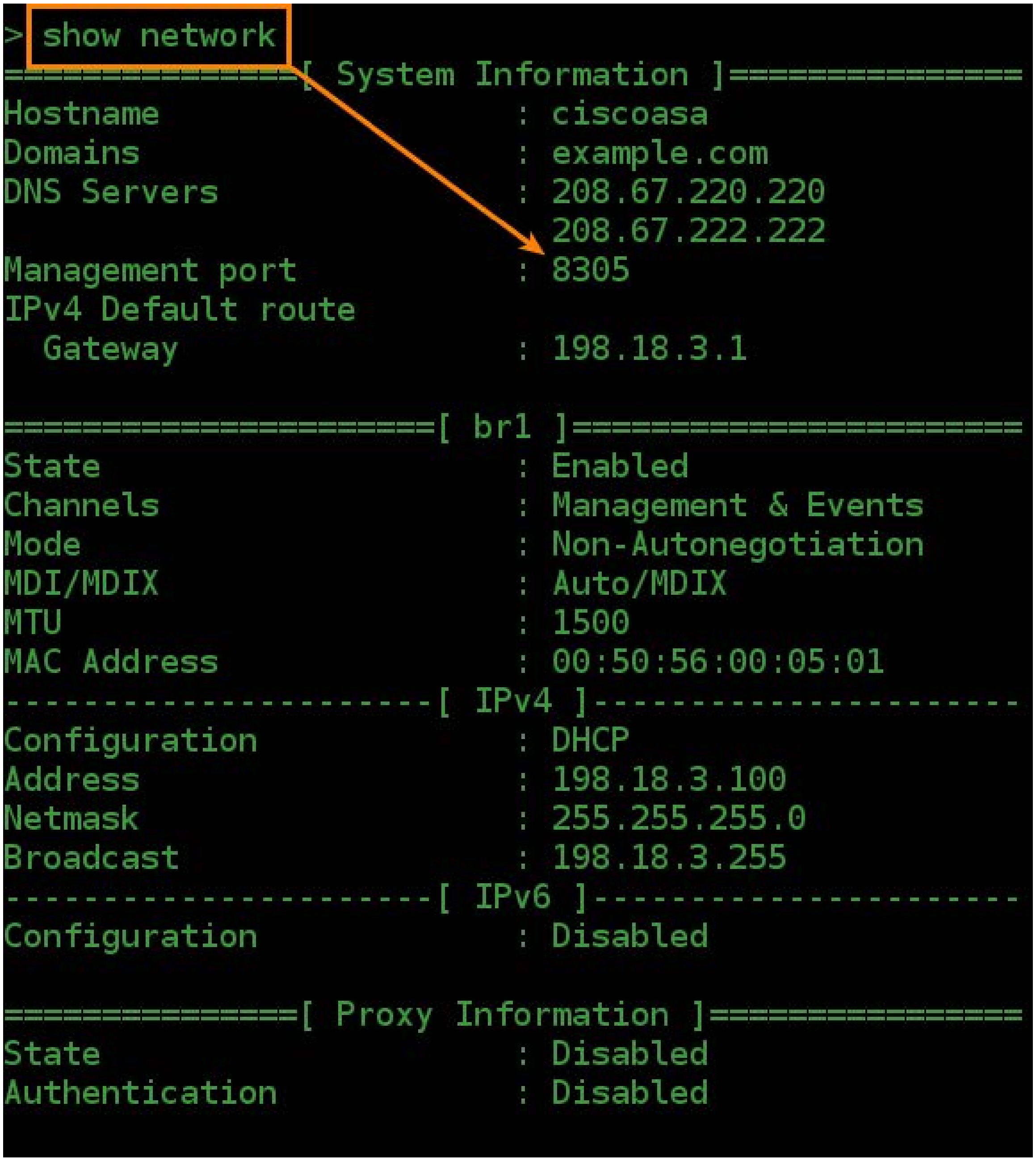
Available Networks: any, any-ipv4, any-ipv6, DMZ_SERVER_PRIVATE, DMZ_SERVER_PUBLIC, EXAMPLE_CORP_LANS, FMC_PRIVATE, FMC_PUBLIC, HQ-FTD_DEFAULT_GATEWAY_IP

Source Networks (1): any-ipv4

Destination Networks (1): FMC_PRIVATE

9. In order to know what port to expect, go over to the the tab open to **remote2-ftd** and issue the command **show network**. This command shows you the way the management network is set up. One of the values is the Management Port. This is the TCP port that is used to communicate between the FMC and FTD devices. This port, by default, is 8305.

Figure 227. Show network



```
> show network
===============[ System Information ]===============
Hostname                  : ciscoasa
Domains                   : example.com
DNS Servers               : 208.67.220.220
                            208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : 198.18.3.1

======================[ br1 ]=======================
State                     : Enabled
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:50:56:00:05:01
----------------------[ IPv4 ]----------------------
Configuration             : DHCP
Address                   : 198.18.3.100
Netmask                   : 255.255.255.0
Broadcast                 : 198.18.3.255
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled
```

10. Back in the FMC, go to the **Ports tab**:

    a. Click the **green plus icon** to add a new Port Object and use the following to fill out the popup window:

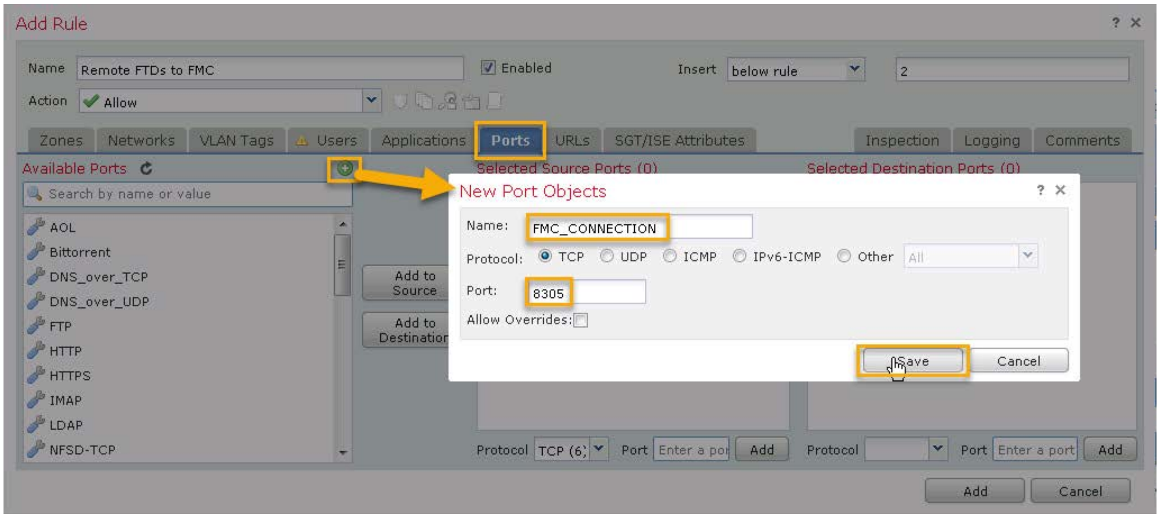
        i. Name: **FMC_CONNECTION**

        ii. Protocol: **TCP**

        iii. Port: **8305** (or whatever the “show network” Management Port is set to in your FTDs).

        iv. Click **Save**.

Figure 228. Create Port Object



Add Rule

Name: Remote FTDs to FMC ☑ Enabled Insert: below rule 2

Action: Allow

New Port Objects

Name: FMC_CONNECTION

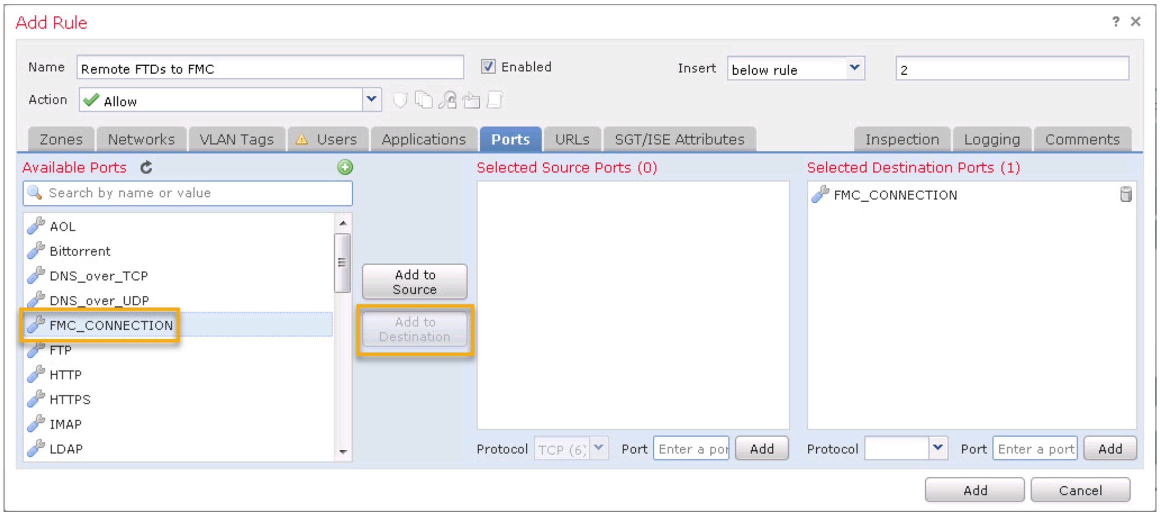
Protocol: ● TCP ○ UDP ○ ICMP ○ IPv6-ICMP ○ Other All

Port: 8305

Allow Overrides: □

    b. In the **Available Ports** list select **FMC_CONNECTION** and click the **Add to Destination**.

Figure 229. Configure Ports tab



Add Rule

Name: Remote FTDs to FMC ☑ Enabled Insert: below rule 2

Action: Allow

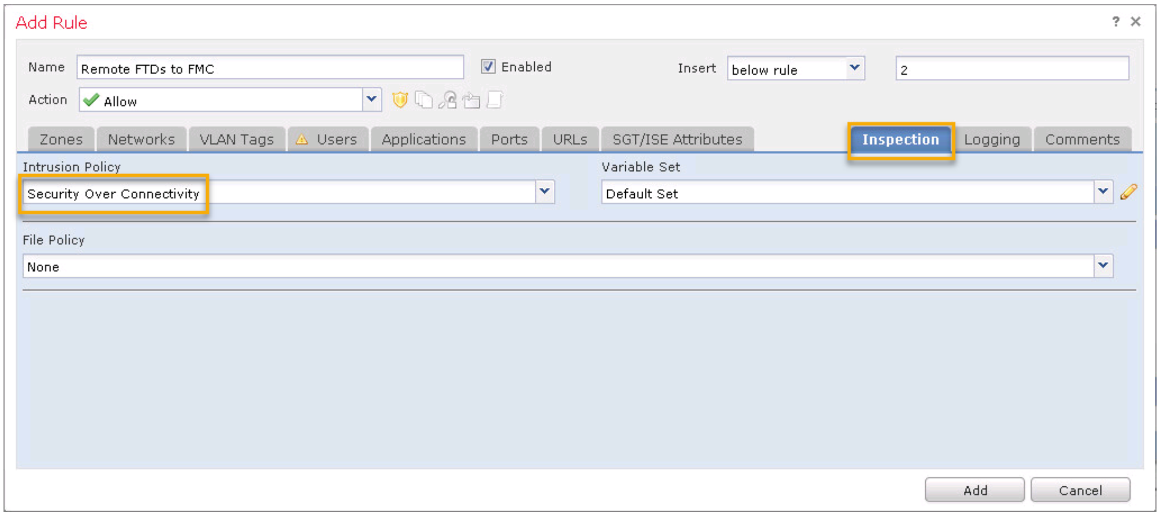
Selected Source Ports (0)

Selected Destination Ports (1): FMC_CONNECTION

11. On the **Inspection tab**:

    a. Intrusion Policy: **Security over Connectivity**

Figure 230. Configure the Inspection tab



Add Rule

Name: Remote FTDs to FMC ☑ Enabled Insert: below rule 2

Action: ✓ Allow

Intrusion Policy: Security Over Connectivity

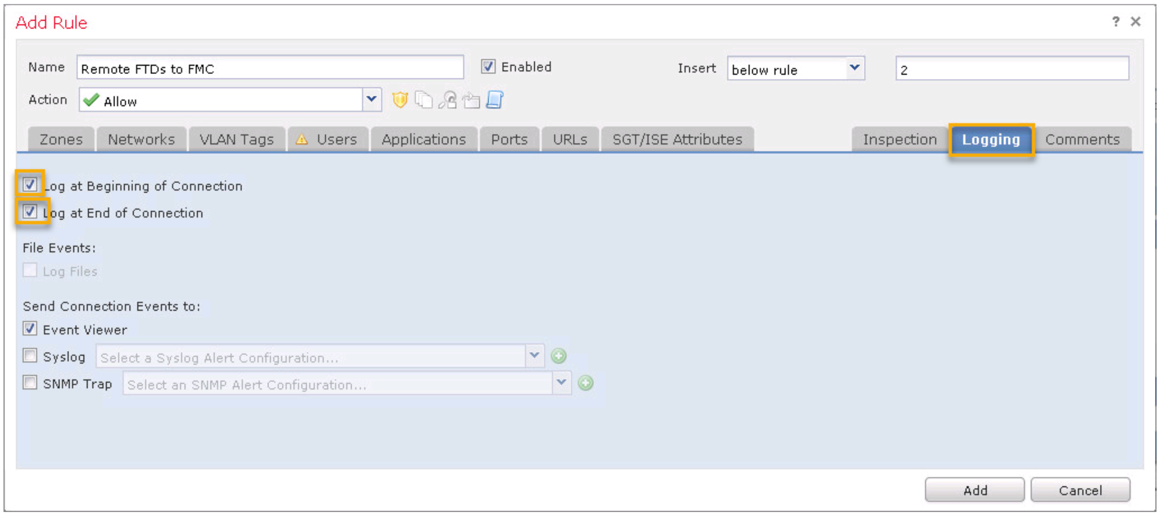
Variable Set: Default Set

File Policy: None

12. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** and **Log at End of Connection**. The use of this rule should only be used for communication between the FMC and FTD devices so logging those exchanges will prove useful should you need to troubleshoot.

Figure 231. Configure Logging tab



Add Rule

Name: Remote FTDs to FMC ☑ Enabled Insert: below rule 2

Action: ✓ Allow

☑ Log at Beginning of Connection

☑ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

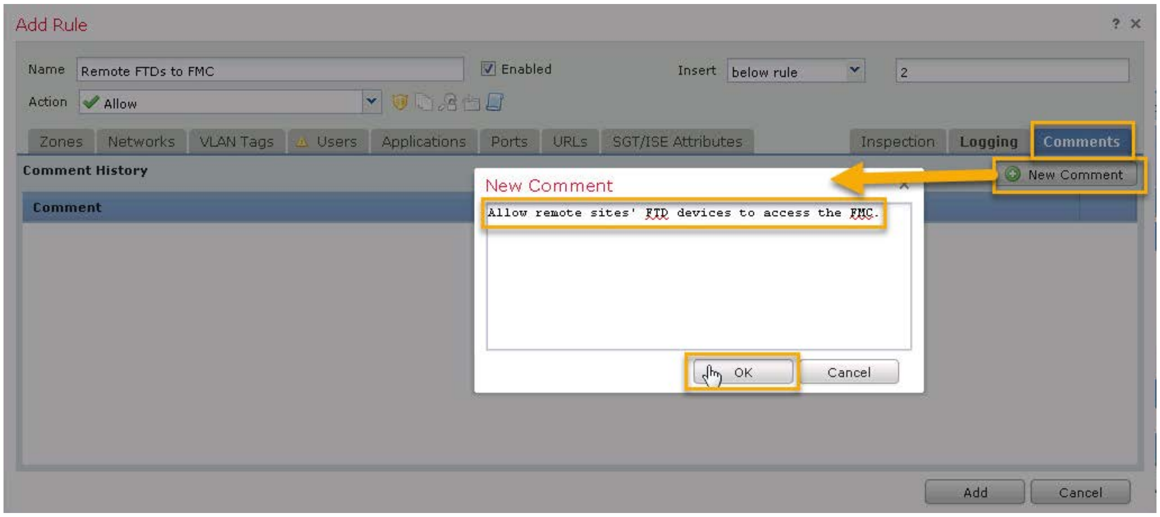
13. On the **Comments tab**:

    a. Click **New Comment** and use the following to fill out the popup window:

        i. New Comment: **Allow remote sites' FTD devices to access the FMC.**

        ii. Click **OK**.

Figure 232. Add a Comment



Add Rule

Name: Remote FTDs to FMC ☑ Enabled Insert: below rule 2

Action: Allow

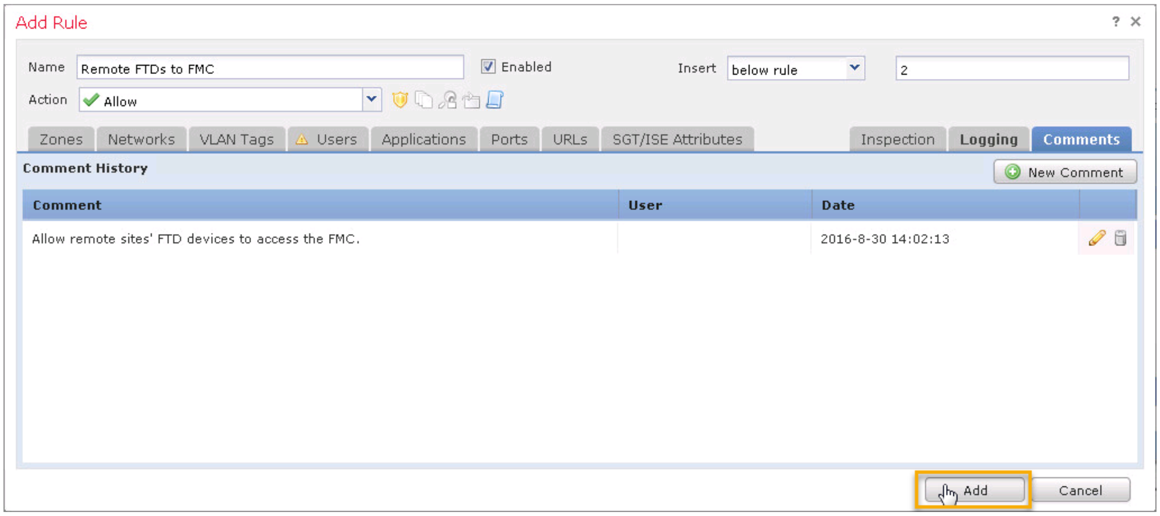
Comment History

New Comment

Allow remote sites' FTD devices to access the FMC.

14. Click **Add** to create this rule.

Figure 233. Finish the rule



Add Rule

Name: Remote FTDs to FMC ☑ Enabled Insert: below rule 2

Action: Allow

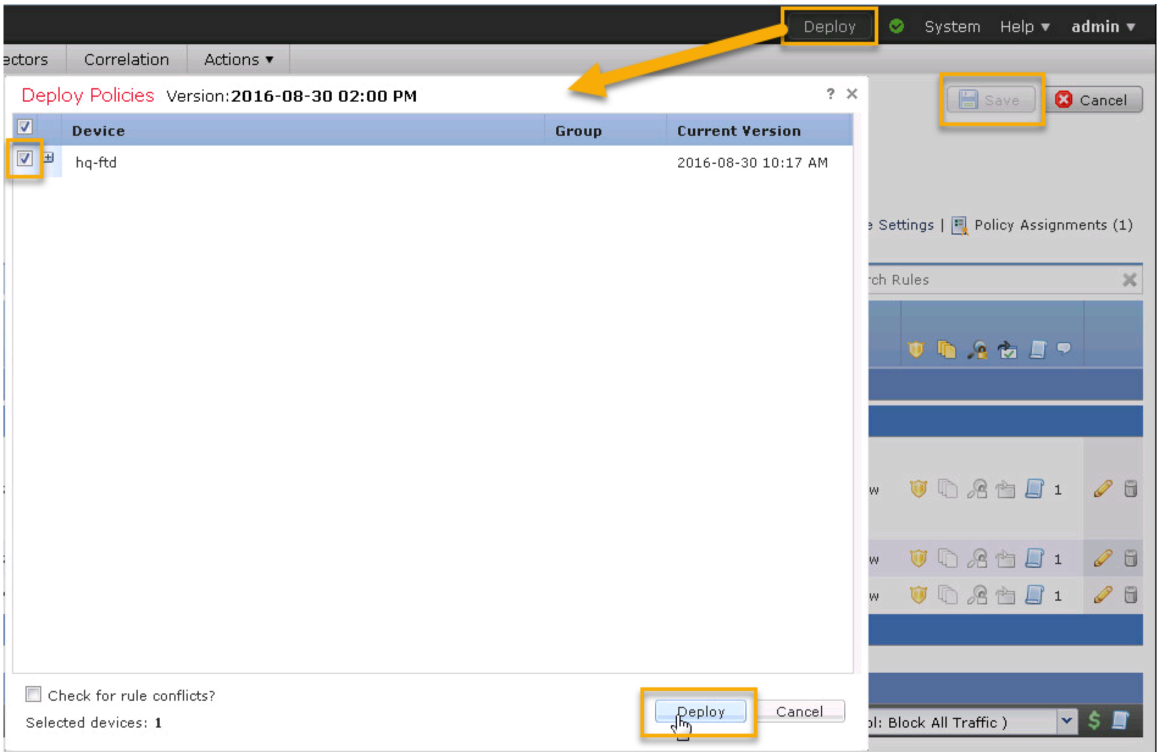
Comment History

Comment	User	Date
Allow remote sites' FTD devices to access the FMC.		2016-8-30 14:02:13

15. Click **Save** and then **Deploy**.

16. Select the **hq-ftd** device and then click **Deploy**.

Figure 234. Save and Deploy to hq-ftd



Deploy Policies Version:2016-08-30 02:00 PM

☑	Device	Group	Current Version
☑	hq-ftd		2016-08-30 10:17 AM

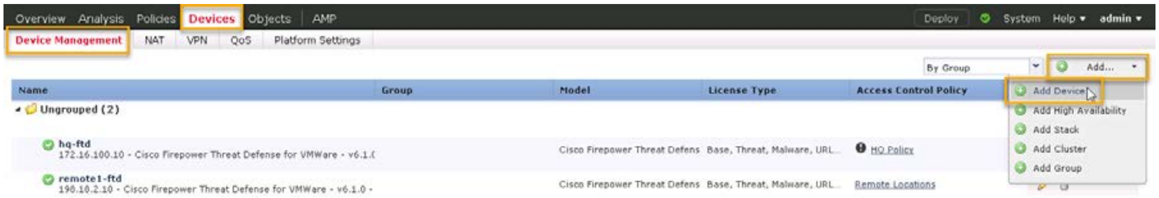
□ Check for rule conflicts?

Selected devices: **1**

17. It will take a minute or two for the HQ Policy on hq-ftd to be updated. In the meantime, you can start adding in the remote2-ftd device. Navigate to **Devices > Device Management**.

18. Click the **Add…** button and select **Add Device** from the dropdown menu.

Figure 235. Add new device



Name	Group	Model	License Type	Access Control Policy
Ungrouped (2)				
hq-ftd 172.16.100.10 - Cisco Firepower Threat Defense for VMWare - v6.1.(		Cisco Firepower Threat Defens	Base, Threat, Malware, URL…	HQ Policy
remote1-ftd 198.18.2.10 - Cisco Firepower Threat Defense for VMWare - v6.1.0 -		Cisco Firepower Threat Defens	Base, Threat, Malware, URL…	Remote Locations

19. Use the following information to fill out the popup window:

    a. Host: LEAVE EMPTY

    b. Display Name: **remote2-ftd**

    c. Registration Key: **regkey3**

    d. Group: **None**

    e. Access Control Policy: **Remote Locations**

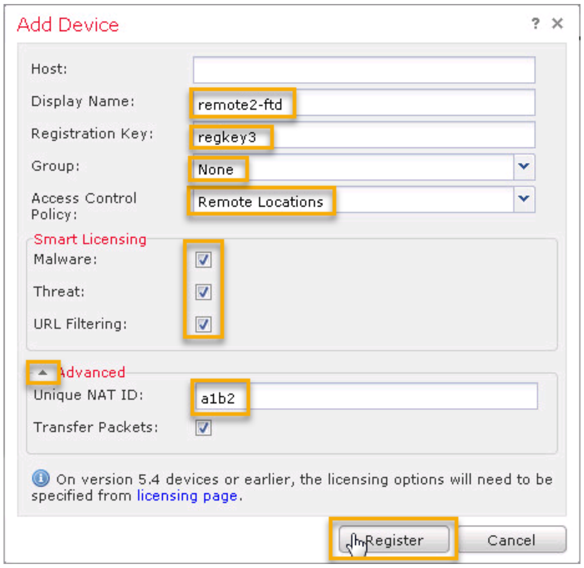
    f. Smart Licensing: Check all the boxes.

20. Expand the Advanced section.

    a. Unique NAT ID: **a1b2**

21. Click **Register**.

Figure 236. Add remote2-ftd device



Add Device

Host:

Display Name: remote2-ftd

Registration Key: regkey3

Group: None

Access Control Policy: Remote Locations

Smart Licensing

Malware: ☑

Threat: ☑

URL Filtering: ☑

Advanced

Unique NAT ID: a1b2

Transfer Packets: ☑

On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

Notice how you did NOT fill out the Host field. This time the FMC has to wait for an incoming connection from remote2-ftd using the correct Registration Key and Unique NAT ID. The registration process will take a few minutes. If you'd like you can issue the command **show managers** on the **remote2-ftd** device to see whether it is completed or not.

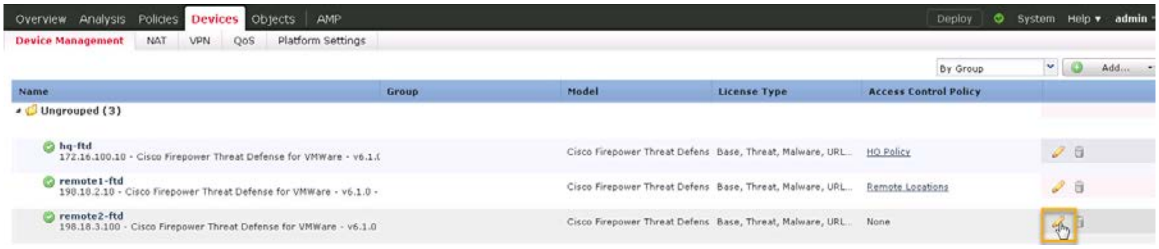
Do not continue the lab until remote2-ftd registration is complete.

Configure remote2-ftd's Data Plane

Now that the remote2-ftd device is being managed by the FMC it is time to configure its data plane.

22. As soon as the **remote2-ftd** device shows up in the Device Management list click the **pencil icon** associated with its row. Then use the following to fill out the needed information:

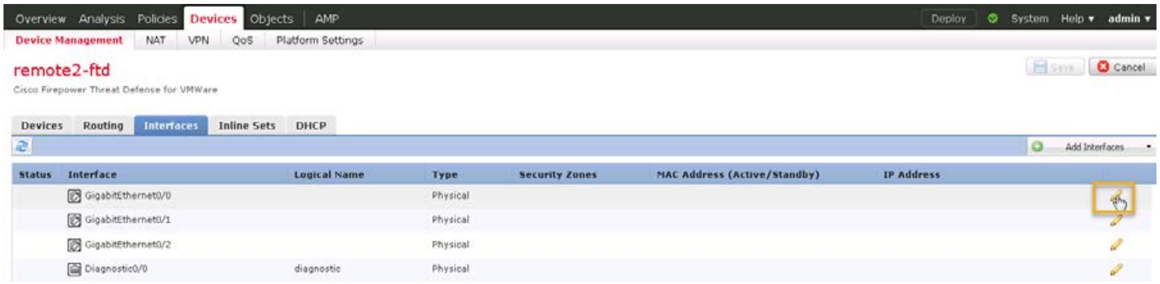
Figure 237. Edit remote2-ftd



Name	Group	Model	License Type	Access Control Policy
Ungrouped (3)				
hq-ftd 172.16.100.10 - Cisco Firepower Threat Defense for VMWare - v6.1.(		Cisco Firepower Threat Defens	Base, Threat, Malware, URL...	HQ Policy
remote1-ftd 198.18.2.10 - Cisco Firepower Threat Defense for VMWare - v6.1.0 -		Cisco Firepower Threat Defens	Base, Threat, Malware, URL...	Remote Locations
remote2-ftd 198.18.3.100 - Cisco Firepower Threat Defense for VMWare - v6.1.0		Cisco Firepower Threat Defens	Base, Threat, Malware, URL...	None

23. On the **Interfaces tab** click the **pencil icon** for the **GigabitEthernet0/0** row. This interface is connected to the remote2 LAN.

Figure 238. Edit g0/0



remote2-ftd

Cisco Firepower Threat Defense for VMWare

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0		Physical			
	GigabitEthernet0/1		Physical			
	GigabitEthernet0/2		Physical			
	Diagnostic0/0	diagnostic	Physical			

24. Use the following to configure GigabitEthernet0/0.

    a. Mode: **None**

    b. Name: **remote2_LAN**

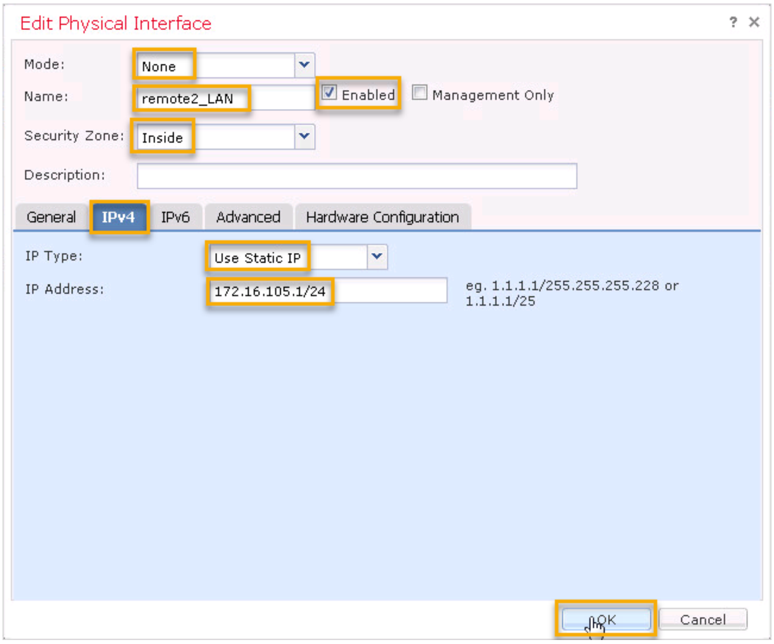
    c. Enabled: **Checked**

    d. Security Zone: **Inside**

25. On the **IPv4 tab** set the IP Address field to **172.16.105.1/24**.

26. Click **OK**.

Figure 239. Configured g0/0


Edit Physical Interface

Mode: None

Name: remote2_LAN ☑ Enabled □ Management Only

Security Zone: Inside

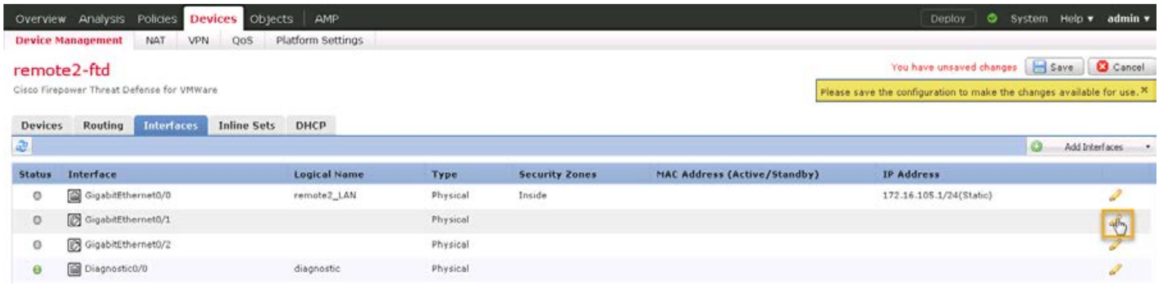
Description:

IP Type: Use Static IP

IP Address: 172.16.105.1/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

27. Click the **pencil icon** for the **GigabitEthernet0/1** row. This interface is connected to remote2's ISP.

Figure 240. Edit g0/1



remote2-ftd

Cisco Firepower Threat Defense for VMWare

You have unsaved changes

Please save the configuration to make the changes available for use.

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
○	GigabitEthernet0/0	remote2_LAN	Physical	Inside		172.16.105.1/24(Static)
○	GigabitEthernet0/1		Physical			
○	GigabitEthernet0/2		Physical			
●	Diagnostic0/0	diagnostic	Physical			

28. Use the following to configure GigabitEthernet0/1.

    a. Mode: **None**

    b. Name: **remote2_ISP**

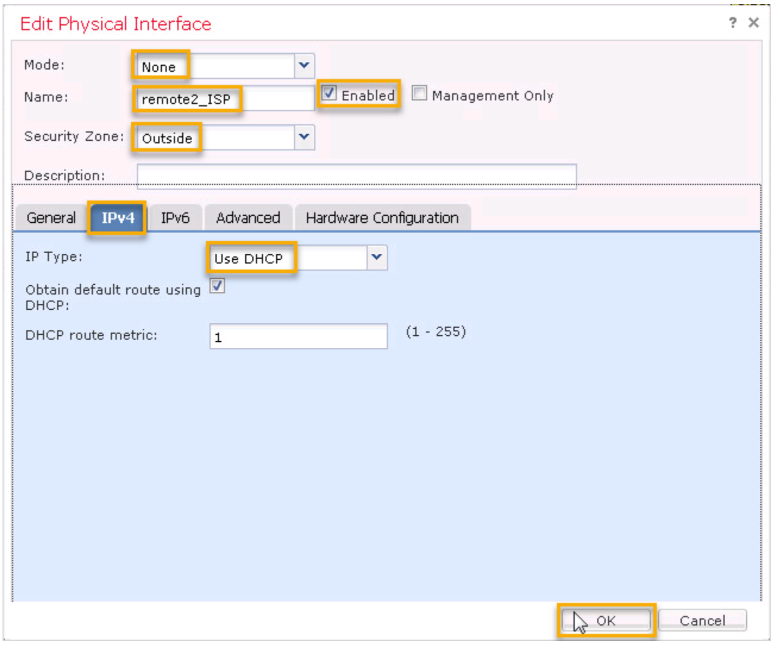
    c. Enabled: **Checked**

    d. Security Zone: **Outside**

29. On the **IPv4 tab** set the IP Type field to **Use DHCP**.

30. Click **OK**.

Figure 241. Configured g0/1



Edit Physical Interface

Mode: None

Name: remote2_ISP ☑ Enabled □ Management Only

Security Zone: Outside

Description:

IP Type: Use DHCP

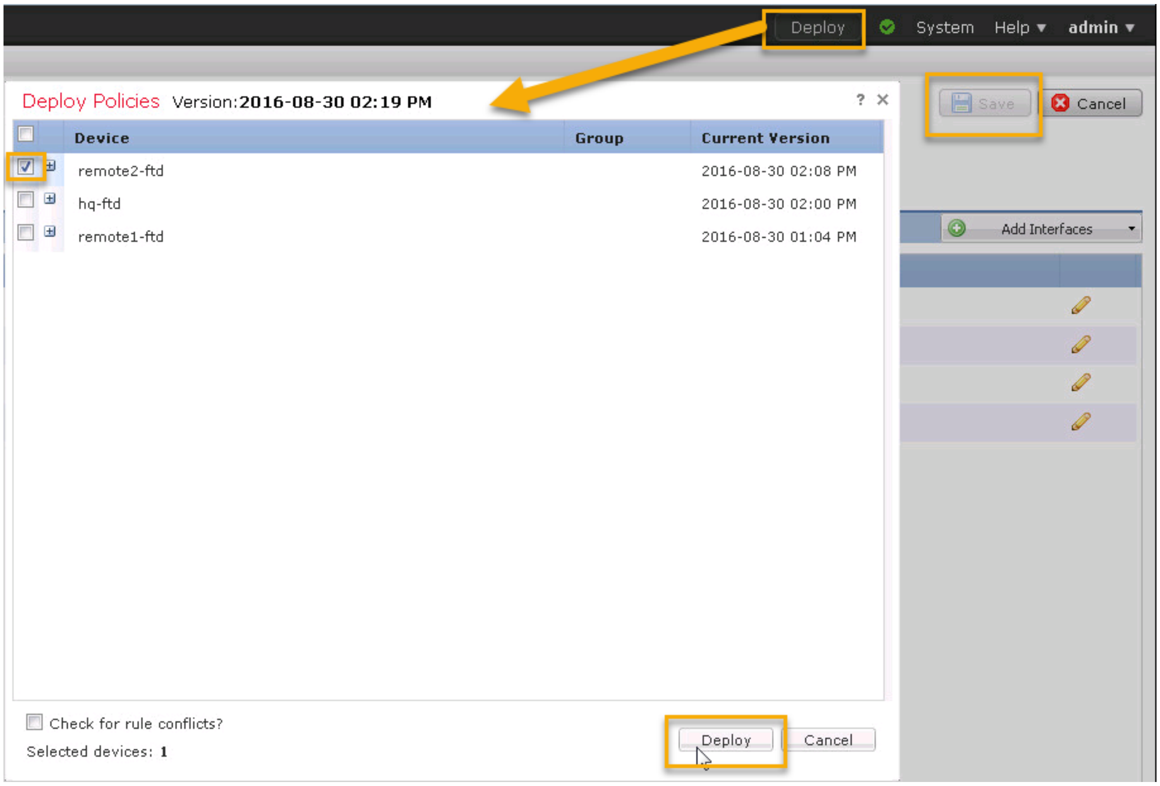
Obtain default route using DHCP: ☑

DHCP route metric: 1 (1 - 255)

31. Click **Save** and then **Deploy**.

32. Select the **remote2-ftd** device and click **Deploy**.

Figure 242. Save and Deploy to remote2-ftd



Deploy Policies Version:**2016-08-30 02:19 PM**

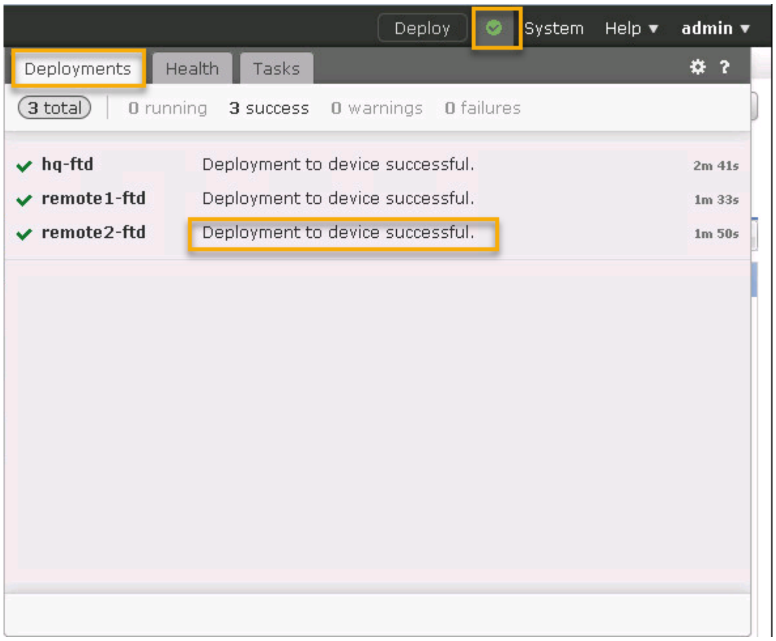
□	Device	Group	Current Version
☑ ⊞	remote2-ftd		2016-08-30 02:08 PM
□ ⊞	hq-ftd		2016-08-30 02:00 PM
□ ⊞	remote1-ftd		2016-08-30 01:04 PM

□ Check for rule conflicts?

Selected devices: **1**

33. Watch the **Message Center's Deployment tab** to ensure the deployment was completed and successful.

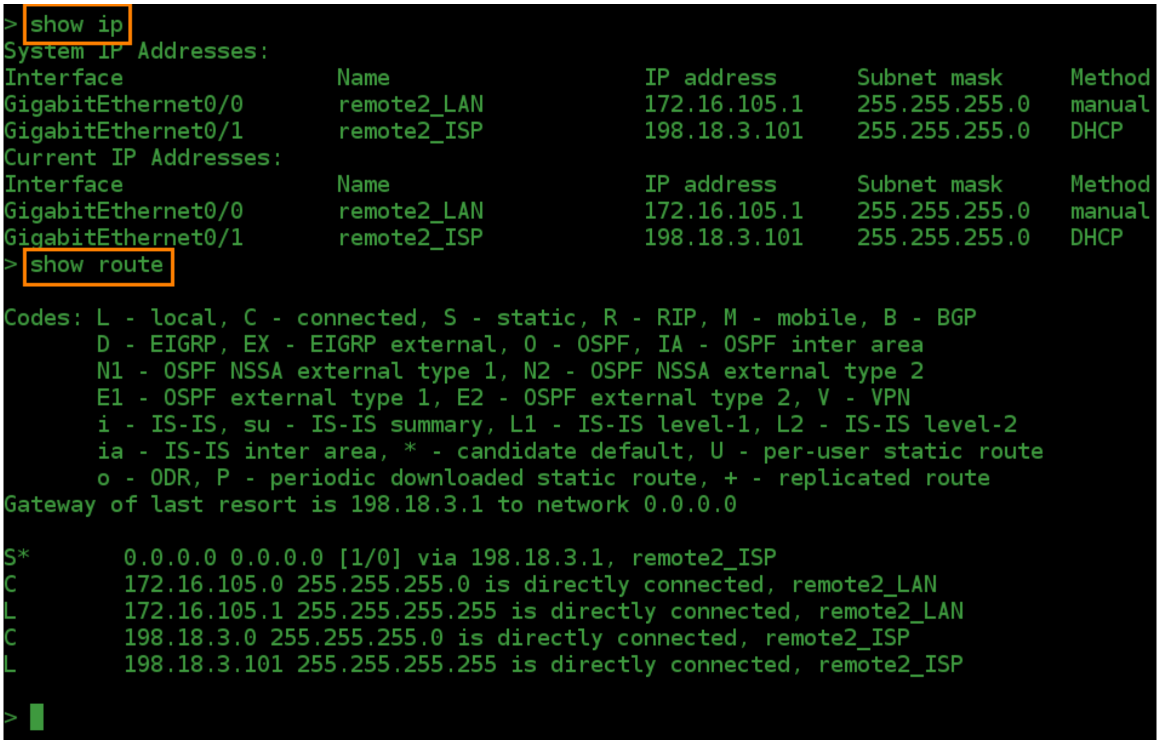
Figure 243. Deployment is complete



✓ hq-ftd Deployment to device successful. 2m 41s
✓ remote1-ftd Deployment to device successful. 1m 33s
✓ remote2-ftd Deployment to device successful. 1m 50s

34. Once the deployment is finished access the **remote2-ftd ssh session** and issue the commands **show ip** and **show route** to ensure that the remote2_ISP interface successfully got an IP address and default route from the ISP's DHCP server.

Figure 244. Show ip and show route



```
> show ip
System IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       remote2_LAN            172.16.105.1    255.255.255.0   manual
GigabitEthernet0/1       remote2_ISP            198.18.3.101    255.255.255.0   DHCP
Current IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       remote2_LAN            172.16.105.1    255.255.255.0   manual
GigabitEthernet0/1       remote2_ISP            198.18.3.101    255.255.255.0   DHCP
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 198.18.3.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 198.18.3.1, remote2_ISP
C        172.16.105.0 255.255.255.0 is directly connected, remote2_LAN
L        172.16.105.1 255.255.255.255 is directly connected, remote2_LAN
C        198.18.3.0 255.255.255.0 is directly connected, remote2_ISP
L        198.18.3.101 255.255.255.255 is directly connected, remote2_ISP

>
```

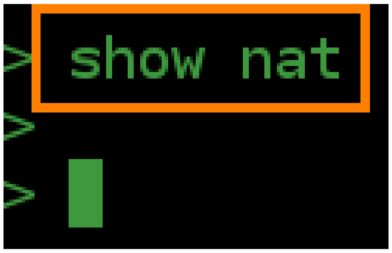
Testing INET Access – Phase 1

The heading of this section might give it away a bit but I’m going to ask anyway. If I were to access remote2-wkst and try to connect to the Internet would it work? Why or why not?

Remember that the registration process of an FTD device with the FMC only has the option of associating the Access Control Policy with the newly added FTD device. You then have to configure the data plane (assign IP addresses, routing, etc) to the FTD device. Additionally, assuming you need it, you have to also associate this new device with any NAT policies you have. In your case you have NOT associated remote2-ftd with your Example Corp NAT policy as of yet, so remote2-wkst will NOT be able to successfully access the Internet yet.

35. On **remote2-ftd** issue the command **show nat** to see its current NAT configuration. Notice there is not NAT configuration.

Figure 245. Show nat

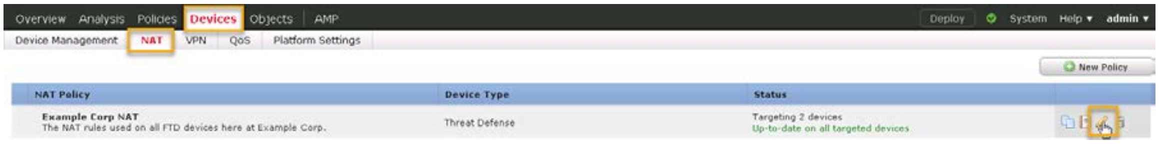


```
> show nat
>
> 
```

36. Let’s fix this now. On the FMC webpage navigate to **Devices > NAT**.

37. Click the **pencil icon** for the **Example Corp NAT** policy.

Figure 246. Edit NAT Policy



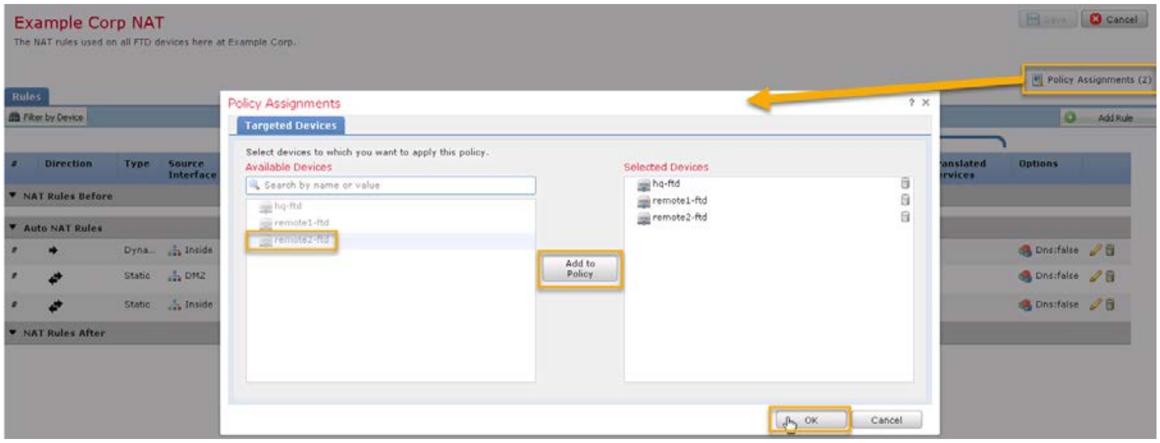
NAT Policy	Device Type	Status
Example Corp NAT The NAT rules used on all FTD devices here at Example Corp.	Threat Defense	Targeting 2 devices Up-to-date on all targeted devices

38. Click the **Policy Assignments** link.

39. Select **remote2-ftd** from the **Available Devices** list and click the **Add to Policy** button.

40. Click **OK**.

Figure 247. Assign remote2-ftd to NAT Policy


Example Corp NAT

The NAT rules used on all FTD devices here at Example Corp.

Policy Assignments

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

hq-ftd
remote1-ftd
remote2-ftd

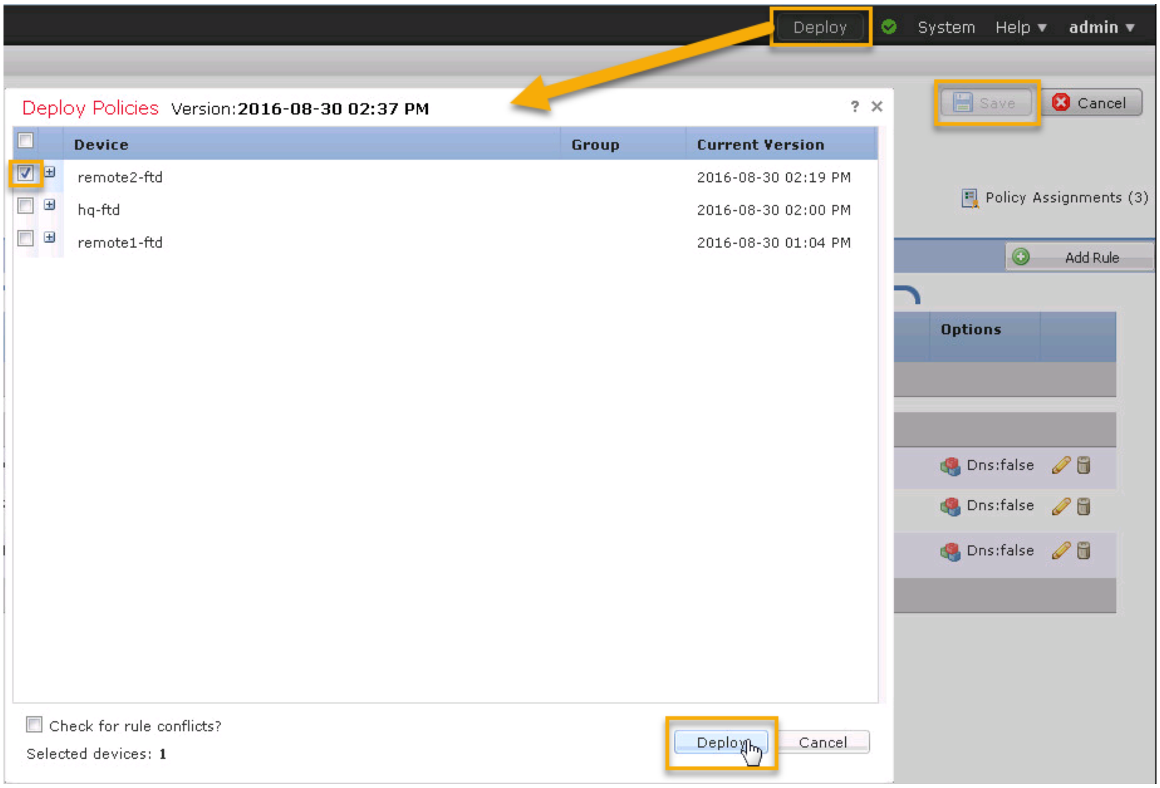
Selected Devices

hq-ftd
remote1-ftd
remote2-ftd

41. Click **Save** and then **Deploy**.

42. Select the **remote2-ftd** device and click **Deploy**.

Figure 248. Save and Deploy



Deploy Policies Version:**2016-08-30 02:37 PM**

	Device	Group	Current Version
☑ ⊞	remote2-ftd		2016-08-30 02:19 PM
□ ⊞	hq-ftd		2016-08-30 02:00 PM
□ ⊞	remote1-ftd		2016-08-30 01:04 PM

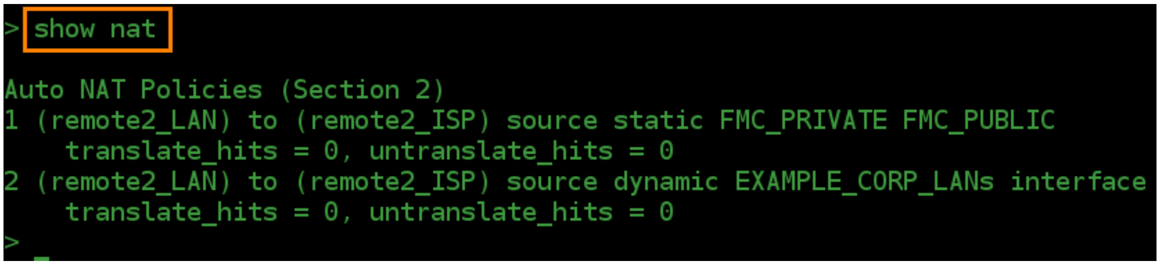
□ Check for rule conflicts?

Selected devices: **1**

From this point on in this lab guide I will just mention to “Save and Deploy” and list the devices with which the deployment is associated and not include any screenshots. Also, assume that the deployment needs to be fully successful before continuing in the lab.

43. Return to remote2-ftd and reissue the command **show nat**.

Figure 249. Reissue show nat on remote2-ftd.



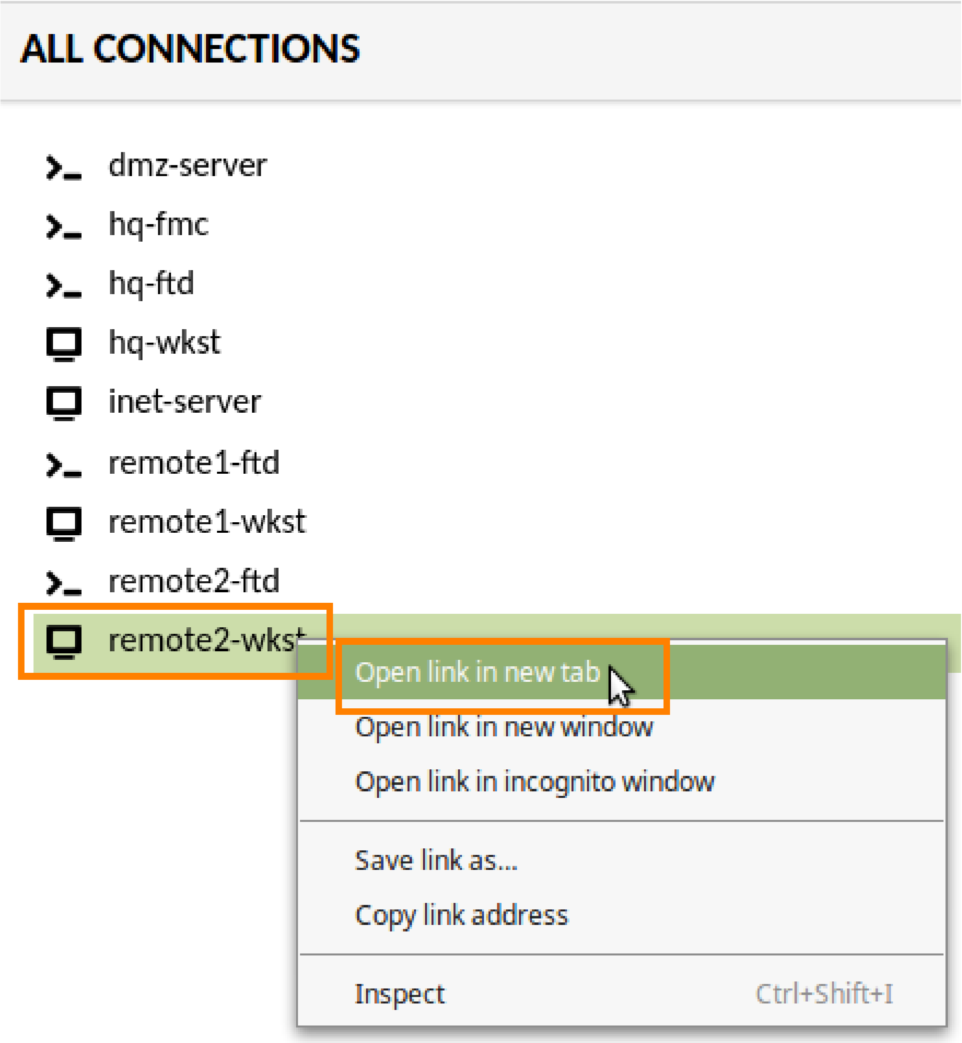
```
> show nat

Auto NAT Policies (Section 2)
1 (remote2_LAN) to (remote2_ISP) source static FMC_PRIVATE FMC_PUBLIC
    translate_hits = 0, untranslate_hits = 0
2 (remote2_LAN) to (remote2_ISP) source dynamic EXAMPLE_CORP_LANs interface
    translate_hits = 0, untranslate_hits = 0
>
```

Testing INET Access – Phase 2

Once the deployment to remote2-ftd is complete it is time to test remote2-wkst's ability to access the Internet.

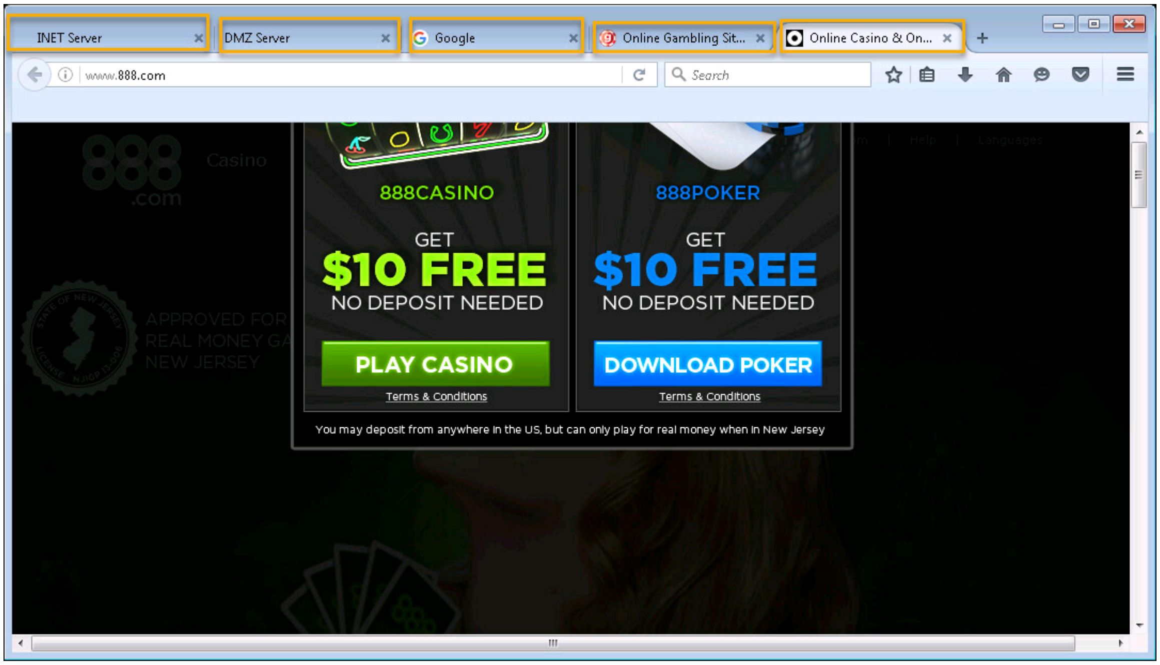
44. From the **oob web page** open a tab to **remote2-wkst**. This will auto log in as administrator/C1sco12345.

Figure 250. Connect to remote2-wkst



45. Open up **Firefox** and **refresh** each of the tabs. Each of them should render correctly!

Figure 251. Firefox on remote2-wkst works!


INET Server
DMZ Server
Google
Online Gambling Sit...
Online Casino & On...
www.888.com
Search
888 Casino .com
APPROVED FOR REAL MONEY GA NEW JERSEY
888CASINO
GET $10 FREE NO DEPOSIT NEEDED
PLAY CASINO
Terms & Conditions
888POKER
GET $10 FREE NO DEPOSIT NEEDED
DOWNLOAD POKER
Terms & Conditions
You may deposit from anywhere in the US, but can only play for real money when in New Jersey

You can close the **remote2-ftd** tab in your browser as it won't be used again for a while.

Scenario Summary

Did you notice how quickly you configured remote2-ftd compared to the previous FTD devices? Once all the policies are in place it is just a matter of registering an FTD device with the FMC, configuring its data plane IP networks, and adding the FTD device to the NAT policy. This is MUCH quicker than trying to configure each device from scratch!

In this scenario you saw that the management NIC of an FTD device can be set up via DHCP. This requires that you know the IP address of the FMC. And though you saw that the deployment of subsequent FTD devices gets easier/quicker you have even quicker tools for mass configuration of FTD devices via a REST API! (More about that later in the lab.)

Intermission #1

Traditionally we “kept the bad guys out” by filtering which L4 ports were permitted inbound and to which servers. Our mentality was that it was the endpoint device’s problem to ensure that if a vulnerability existed in their server’s service (like with IIS or Sharepoint) that they patch it. Going the other direction (inside to outside) traffic was generally uninhibited. Yes, you might block a few ports (like TCP/137 or TCP/47) but for the most part outbound traffic was permitted. However, in modern times most applications run on TCP ports 80 and 443; most attacks are delivered in packages that use the already open ports; most attacks are designed to exploit other vulnerabilities within a PC and then “call home” with further information on how to attack the network from within. These types of attacks are completely permitted using only traditional firewalling methods.

In the Next Generation Firewall (NGFW) you need the ability to look deeper into the packet and check its payload for potential malicious content; you need to concern yourself as much with what is outgoing from your networks as is incoming; you need to be able to monitor and track which devices are communicating with which within your networks and determine whether something nefarious is happening (and then be able to know which devices are compromised so you can remediate).

For the most part, everything that has been done in this lab up to this point was essentially configuring these FTD devices from Layer 1 to Layer 4 of the OSI model and anyone familiar with working with a traditional firewall would recognize this deployment. The next few scenarios delve into more of the “Next Generation” style filtering and monitoring aspects of the NGFW.

Page intentionally left blank.

Scenario 6. Configuring URL Filtering

Scenario Description

In the traditional firewall design the focus was on IP addresses, ports, and protocols (Layers 3 and 4 essentially). One of the ways that the evil doers of the world have found to get around this type of security design by using URLs to bounce their command and control connections around to different IP addresses. Even if it isn't a botnet that you are trying to thwart (or avoid), the ability to classify web content with the intention of filtering said content is an important feature to have!

This scenario has you implement a few business rules that Example Corp has around web content. The first rule is to not allow any user on their network to access a gambling website. The second, limits the access to social media websites. Apparently excessive time has been spent on Facebook and other social media sites. However, the HQ LAN needs access to Facebook (the justification is to update Example Corp's social presence).

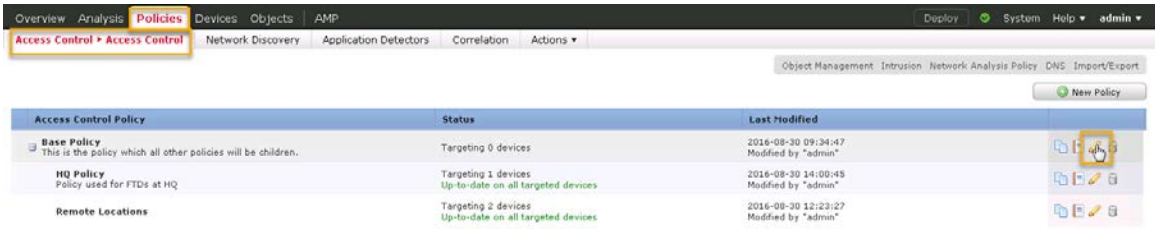
Create an ACP Category and Block Gambling URLs

In order to better organize the Access Control Rules, you will also create a new category to sort the rules beyond just the Mandatory and Default sections.

1. On **hq-wkst** access the FMC website and navigate to **Policies > Access Control > Access Control**.

2. Click the **pencil icon** for the **Base Policy**.

Figure 252. Edit the Base Policy



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-30 09:34:47 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-30 14:00:45 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-08-30 12:23:27 Modified by "admin"

Though a bit unnecessary for this lab you need to create a new category in the mandatory section of the Base Policy ACP called "No Gambling for you!!!". Categories are nice ways to organize your ACP rules. Think of them as sub-sections within the Mandatory or Default sections.

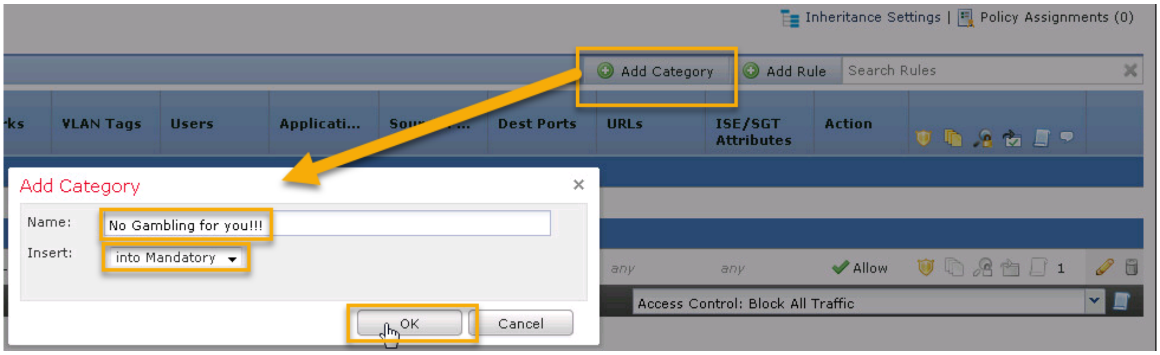
3. Click the **Add Category** button and use the following to fill out the popup window:

    a. Name: **No Gambling for you!!!**

    b. Insert: **into Mandatory**

    c. Click **OK**.

Figure 253. Create Category



Add Category

Name: No Gambling for you!!!

Insert: into Mandatory

4. Now to create the "No Gambling" rule. Click the **Add Rule** button and use the following to fill out the needed information:

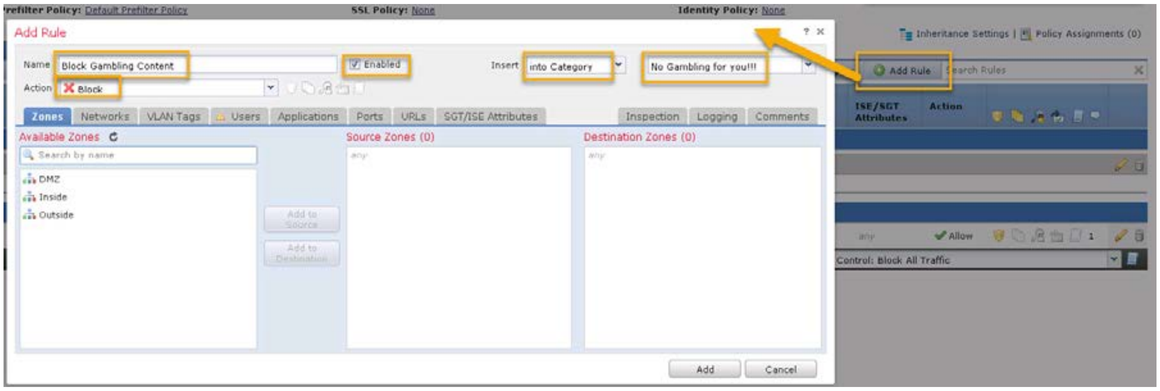
    a. Name: **Block Gambling Content**

    b. Enabled: **Checked**

    c. Insert: **into Category** and then select the **No Gambling for you!!!** Category

    d. Action: **Block**

Figure 254. Part 1 Add Rule



Add Rule

Name: Block Gambling Content

☑ Enabled

Insert: into Category

No Gambling for you!!!

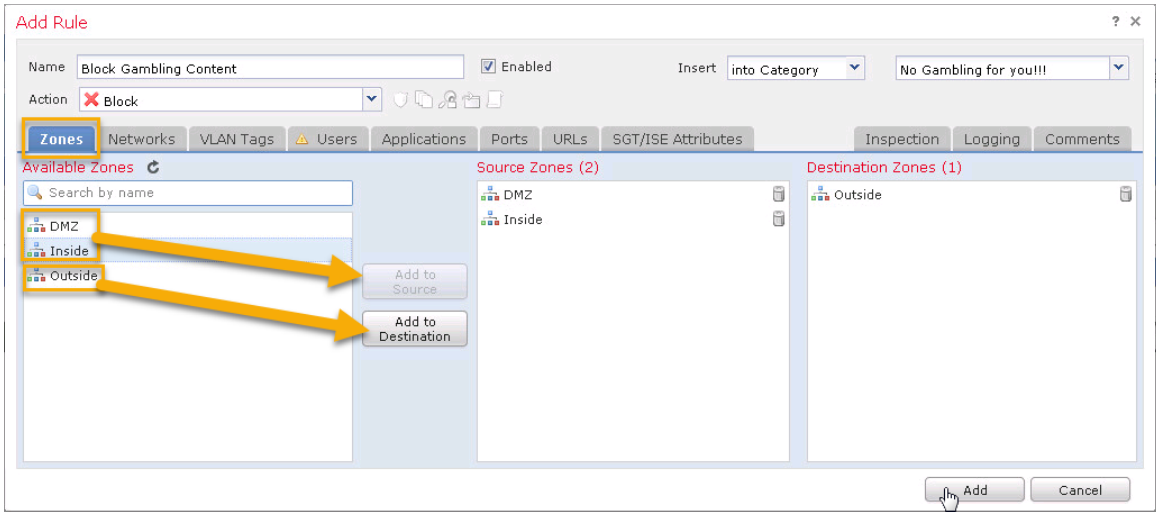
Action: Block

5. On the **Zones tab**:

   a. Select **Inside** and **DMZ** and click the **Add to Source** button.

   b. Select **Outside** and click the **Add to Destination** button.

Figure 255. Configure Zones tab



Add Rule

Name: Block Gambling Content ☑ Enabled Insert: into Category | No Gambling for you!!!

Action: Block

Source Zones (2): DMZ, Inside

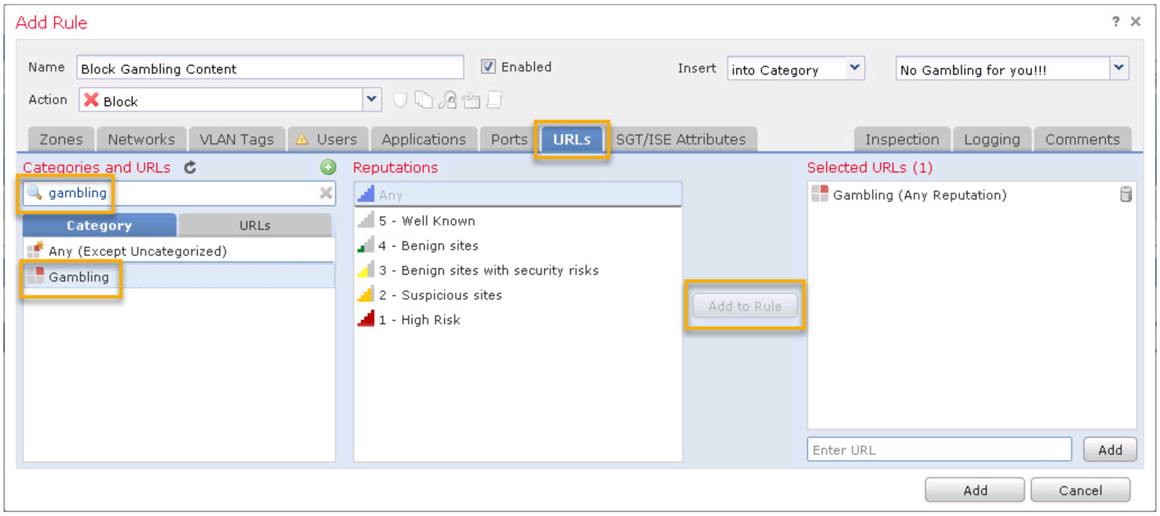
Destination Zones (1): Outside

6. On the **URLs tab**:

   a. In the search field type **gambling**.

   b. Select the **Gambling** result and click the **Add to Rule** button.

Figure 256. Configure URLs tab



Add Rule

Name: Block Gambling Content ☑ Enabled Insert: into Category | No Gambling for you!!!

Action: Block

Categories and URLs search: gambling

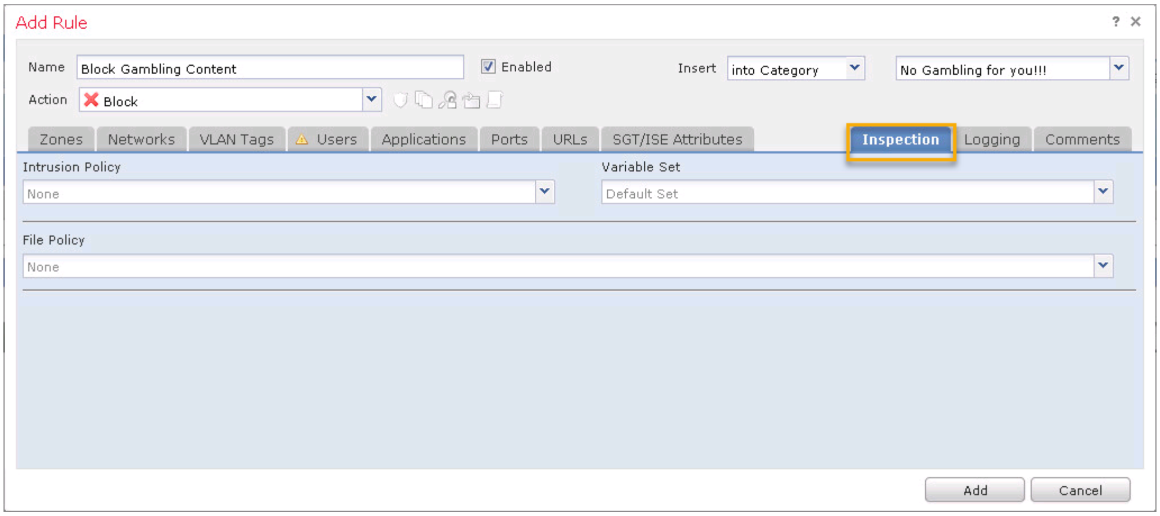
Selected URLs (1): Gambling (Any Reputation)

Notice how you could have also selected a level of reputation as well. In this case you want Any Reputation. That said, selecting a reputation level also selects any reputation level lower than itself. For example, if you had selected 2 – Suspicious sites then the 1 – High Risk reputation would have been selected as well.

7. On the **Inspection tab**:

    a. Since you are blocking this traffic at the ASA process there is no need to select the SNORT policy to use thus you cannot select anything here.

Figure 257. Can't configure Inspection tab



Add Rule

Name: Block Gambling Content ☑ Enabled Insert: into Category No Gambling for you!!!

Action: Block

Intrusion Policy: None

Variable Set: Default Set

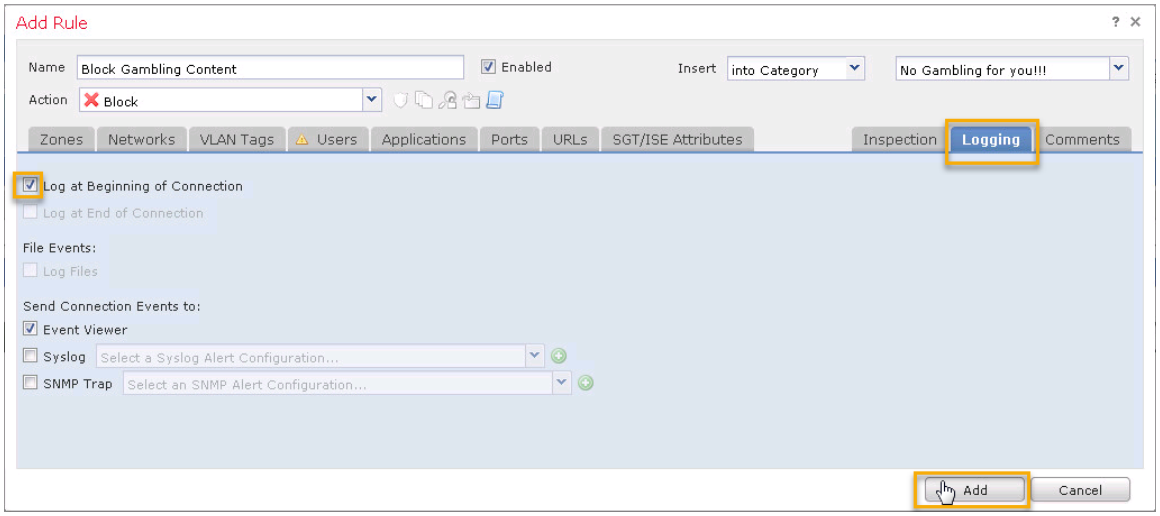
File Policy: None

8. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** box. Because you are blocking this traffic you cannot select the Log at End of Connection (since the traffic is immediately terminated).

9. Click **Add** to create this rule.

Figure 258. Configure Logging tab and Add rule.



Add Rule

Name: Block Gambling Content ☑ Enabled Insert: into Category No Gambling for you!!!

Action: Block

☑ Log at Beginning of Connection

□ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

Just to show off the other features of URL filtering you are going to create another rule and apply it in the No Gambling for you!!! category. This rule will block a specific URL (www.888.com). This URL should be blocked by the Gambling category but let's just pretend that isn't and that you need to manually block that URL.

In order to perform category or reputation URL filtering you need the URL license. However, to filter based on a URL object (or list of objects) you don't need the license.

10. Click the **Add Rule** button and use the following to fill out the needed information:

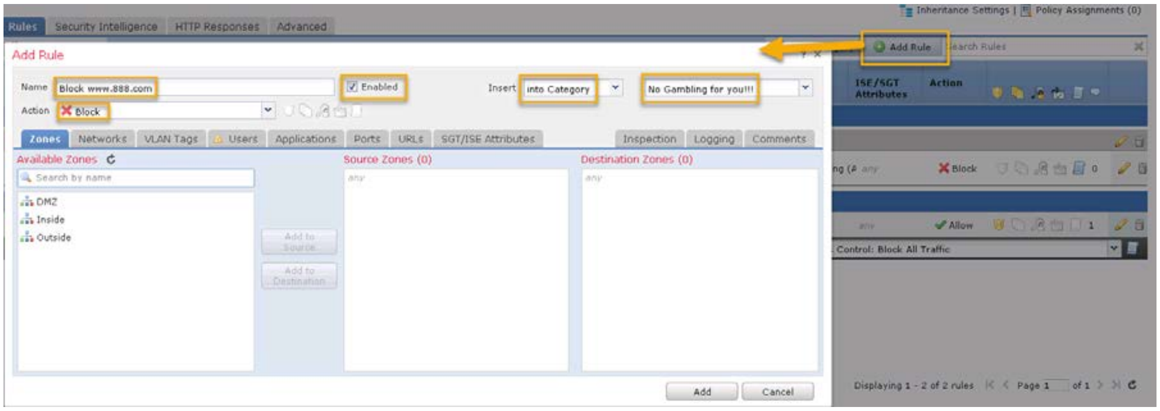
    a. Name: **Block www.888.com**

    b. Enabled: **Checked**

    c. Insert: **into Category** and then **No Gambling for you!!!** Category.

    d. Action: **Block**

Figure 259. Part 1 of Add Rule



Add Rule

Name: Block www.888.com

☑ Enabled

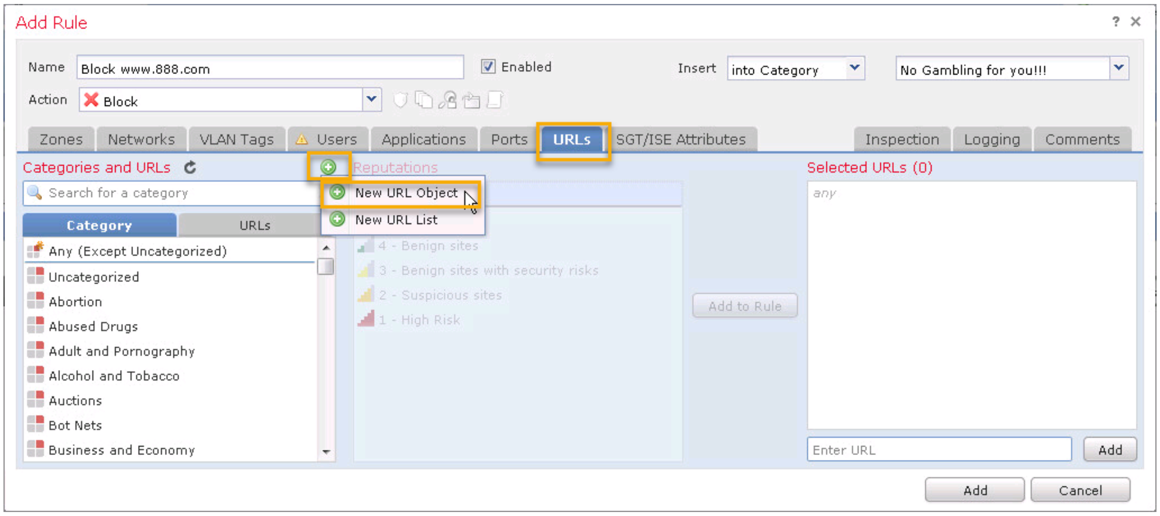
Insert: into Category — No Gambling for you!!!

Action: Block

11. On the **URLs tab**:

    a. Click the **green plus icon** and select **New URL Object** to create a new object.

Figure 260. Create URL Object



Add Rule

Name: Block www.888.com

☑ Enabled

Insert: into Category — No Gambling for you!!!

Action: Block

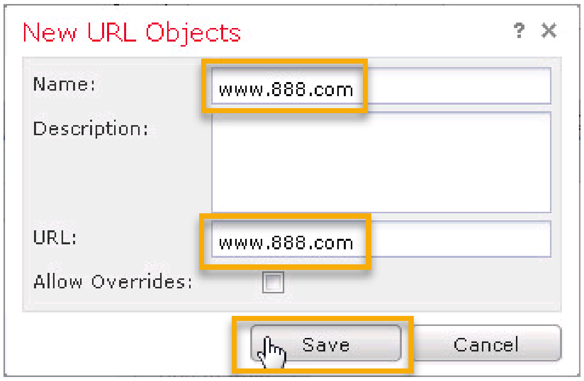
b. Use the following to fill out the information for the popup window:

i. Name: **www.888.com**

ii. URL: **www.888.com**

iii. Click **Save**.

Figure 261. Create URL Object



New URL Objects

Name: www.888.com

Description:

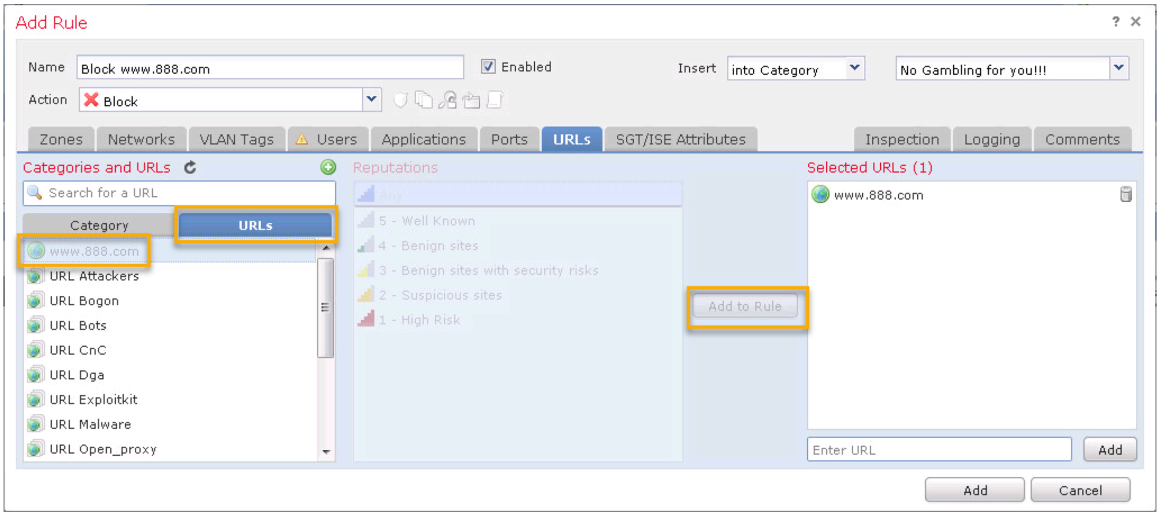
URL: www.888.com

Allow Overrides: □

c. Click the **URLs sub-tab** (underneath the Categories and URLs section).

i. Select **www.888.com** from the list and click the **Add to Rule** button.

Figure 262. Configure URLs tab



Add Rule

Name: Block www.888.com

☑ Enabled

Insert: into Category

No Gambling for you!!!

Action: ✗ Block

Categories and URLs

Search for a URL

www.888.com
URL Attackers
URL Bogon
URL Bots
URL CnC
URL Dga
URL Exploitkit
URL Malware
URL Open_proxy

Reputations

Any
5 - Well Known
4 - Benign sites
3 - Benign sites with security risks
2 - Suspicious sites
1 - High Risk

Selected URLs (1)

www.888.com

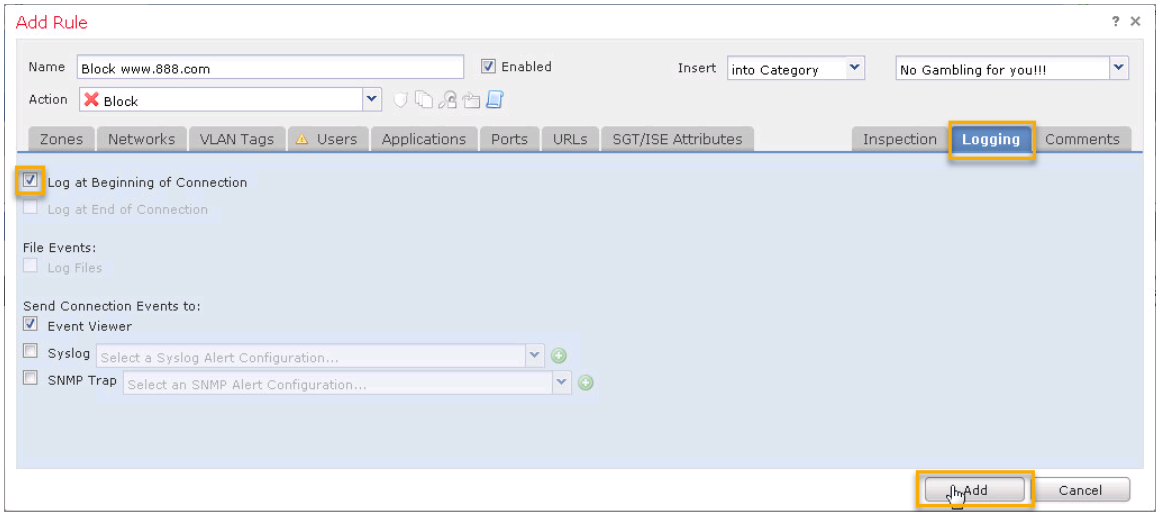
Enter URL

12. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** box.

13. Click **Add** to create this rule.

Figure 263. Configure Logging and Add rule



Add Rule

Name: Block www.888.com ☑ Enabled Insert: into Category | No Gambling for you!!!

Action: Block

☑ Log at Beginning of Connection

□ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

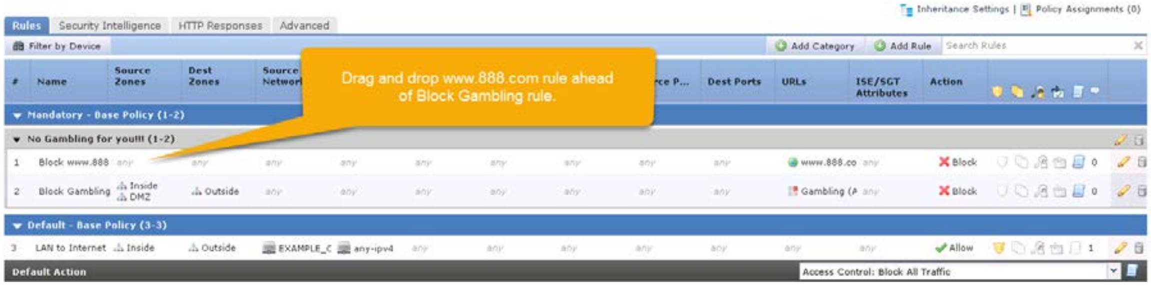
□ Syslog Select a Syslog Alert Configuration...

□ SNMP Trap Select an SNMP Alert Configuration...

Did you notice how little information you used to create this rule? You didn't specify any Zones or Networks. Basically any connection going through the FTD device wishing to access www.888.com will be blocked no matter what zone or source IP it is coming from. This is done to simplify the lab steps but this also means that any "outside" to "inside/DMZ" traffic would also be checked against this rule. This isn't optimal and probably shouldn't be considered a best practice. Generally, it is better to be more specific than general when creating rules.

14. The Block www.888.com rule shows up below the Block Gambling rule. Now, if this was a real scenario and you had created this rule because the Block Gambling rule was for some reason not catching www.888.com then the order of the rules wouldn't matter. In your case you want to ensure that you hit the Block www.888.com rule so **drag and drop** this rule up **above** the **Block Gambling** rule. Alternatively you can edit the Block www.888.com rule and use the Move link to move this rule above rule #1.

Figure 264. Move www.888.com rule up



Drag and drop www.888.com rule ahead of Block Gambling rule.

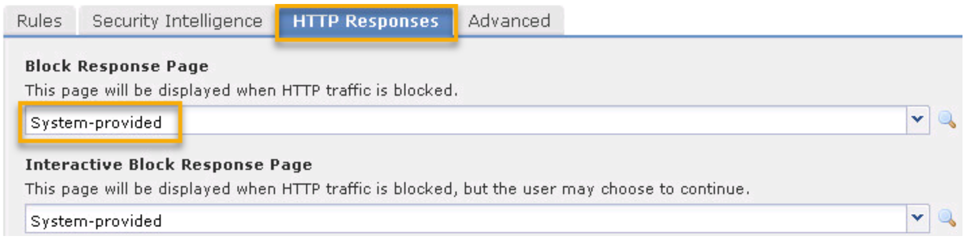
#	Name	Source Zones	Dest Zones	Source Networ					ce P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
	Mandatory - Base Policy (1-2)													
	No Gambling for you!!! (1-2)													
1	Block www.888	any	any	any	any	any	any	any	any	any	www.888.co	any	Block	0
2	Block Gambling	Inside DMZ	Outside	any	any	any	any	any	any	any	Gambling (A	any	Block	0
	Default - Base Policy (3-3)													
3	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	Allow	1

Default Action: Access Control: Block All Traffic

If you deployed this configuration as is, when someone tried to access, say www.gambling.com the page would just use the browsers default action it takes when the URL it tries to render fails. This might not be the best solution as it doesn't inform the user that their actions are futile.

15. Click on the **HTTP Responses tab** and modify the **Block Response Page** to be **System-provided**. This way the user will at least know that it isn't a down website but that they are not permitted to access this website.

Figure 265. Configure HTTP Responses



Block Response Page

This page will be displayed when HTTP traffic is blocked.

System-provided

Interactive Block Response Page

This page will be displayed when HTTP traffic is blocked, but the user may choose to continue.

System-provided

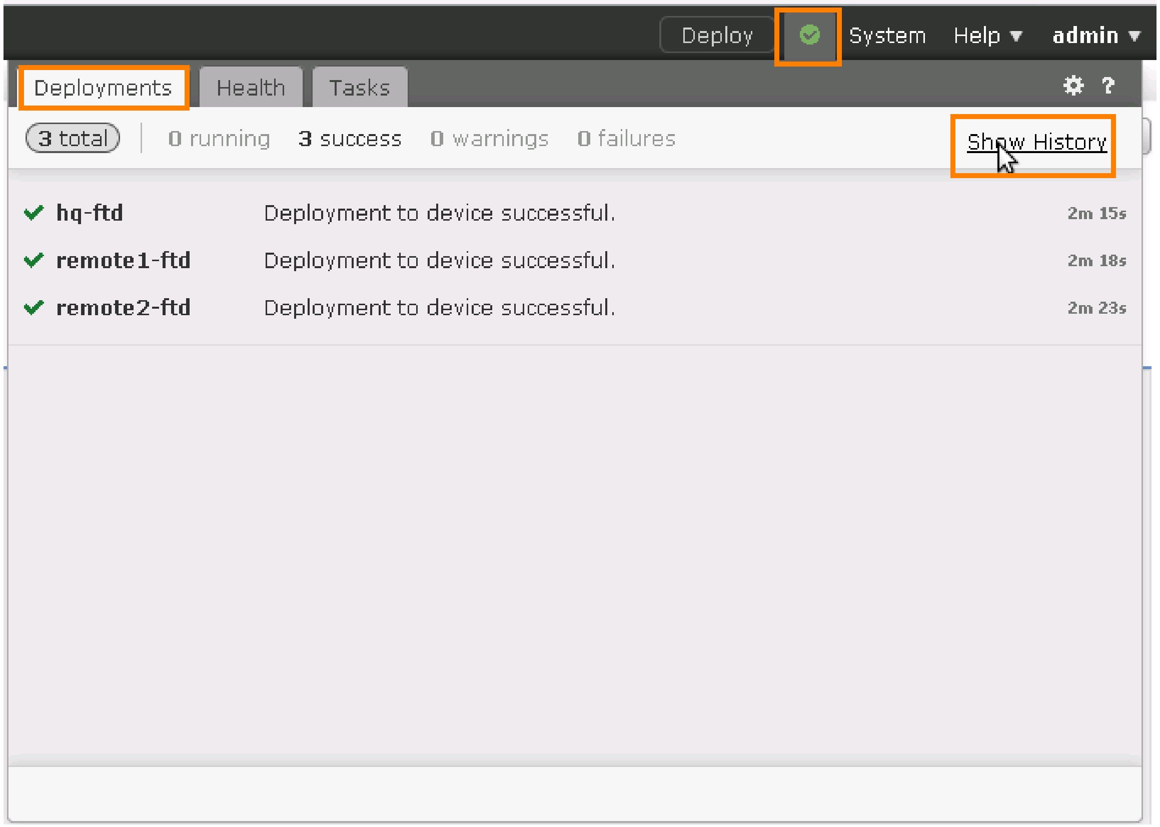
Note this is a "ACP-wide" setting. Thus any rule associated with Base Policy (or inherits the Base Policy) will use this changed setting. However, policies inheriting this feature and disable the inheritance and customize their own setting.

16. Click **Save**, **Deploy**, select **all the FTDs** and click **Deploy**.

Deployment History

17. As a side note, while we are waiting for the deployment to finish, click on **Message Center** and then the **Deployments tab**. On the Deployments tab click on the **Show History** link.

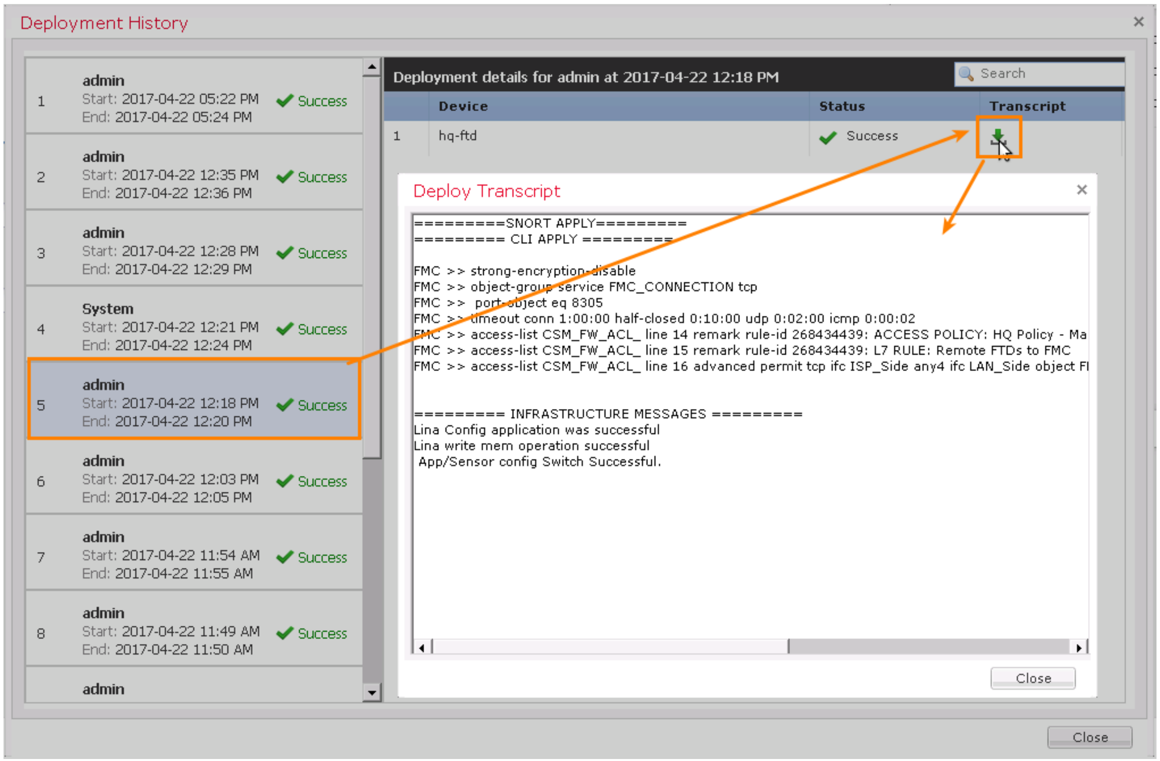
Figure 266. Navigate to Show history



✓ hq-ftd Deployment to device successful. 2m 15s
✓ remote1-ftd Deployment to device successful. 2m 18s
✓ remote2-ftd Deployment to device successful. 2m 23s

18. This is one of the new features in the v6.2.0 release of FTD. Here you can see a history of deployments. From the left hand column click on one of the deployments. Then, in the right hand side, click the download link to download the transcript of this deployment. This will then display the changes that were made in that deployment.

Figure 267. Show a particular deployment history



1	admin Start: 2017-04-22 05:22 PM End: 2017-04-22 05:24 PM	✓ Success
2	admin Start: 2017-04-22 12:35 PM End: 2017-04-22 12:36 PM	✓ Success
3	admin Start: 2017-04-22 12:28 PM End: 2017-04-22 12:29 PM	✓ Success
4	System Start: 2017-04-22 12:21 PM End: 2017-04-22 12:24 PM	✓ Success
5	admin Start: 2017-04-22 12:18 PM End: 2017-04-22 12:20 PM	✓ Success
6	admin Start: 2017-04-22 12:03 PM End: 2017-04-22 12:05 PM	✓ Success
7	admin Start: 2017-04-22 11:54 AM End: 2017-04-22 11:55 AM	✓ Success
8	admin Start: 2017-04-22 11:49 AM End: 2017-04-22 11:50 AM	✓ Success
	admin	

Deployment details for admin at 2017-04-22 12:18 PM

	Device	Status	Transcript
1	hq-ftd	✓ Success	

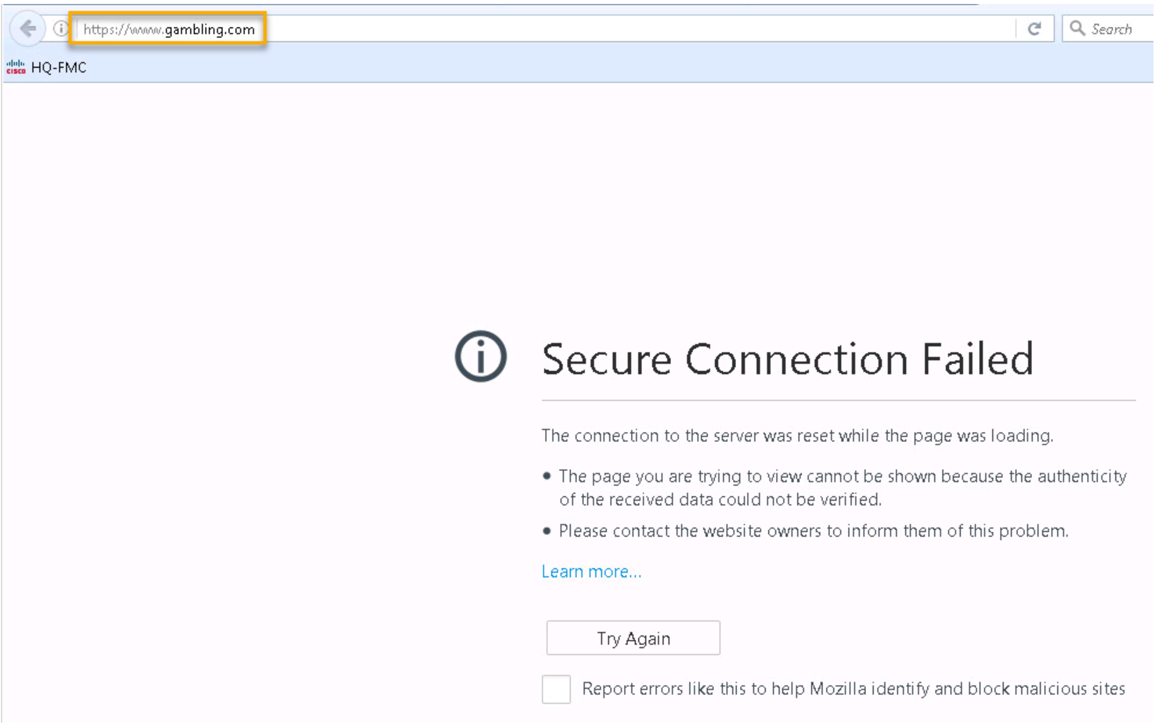
```
=========SNORT APPLY=========
========= CLI APPLY =========

FMC >> strong-encryption-disable
FMC >> object-group service FMC_CONNECTION tcp
FMC >>  port-object eq 8305
FMC >> timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
FMC >> access-list CSM_FW_ACL_ line 14 remark rule-id 268434439: ACCESS POLICY: HQ Policy - Ma
FMC >> access-list CSM_FW_ACL_ line 15 remark rule-id 268434439: L7 RULE: Remote FTDs to FMC
FMC >> access-list CSM_FW_ACL_ line 16 advanced permit tcp ifc ISP_Side any4 ifc LAN_Side object Fl


========= INFRASTRUCTURE MESSAGES =========
Lina Config application was successful
Lina write mem operation successful
 App/Sensor config Switch Successful.
```

19. When you are done reviewing the transcript click **Close** on the **Deploy Transcript** window and then **Close** on the **Deployment History** window.

Test URL Filtering of Gambling Websites

20. Once the deployment is complete attempt to access **www.gambling.com** and **www.888.com** from **any of the Example Corp workstations**. If you use the pre-populated tabs be sure to refresh those pages – preferably hold the SHIFT key down while you click the Refresh button.

Figure 268. No access to www.gambling.com



Secure Connection Failed

The connection to the server was reset while the page was loading.

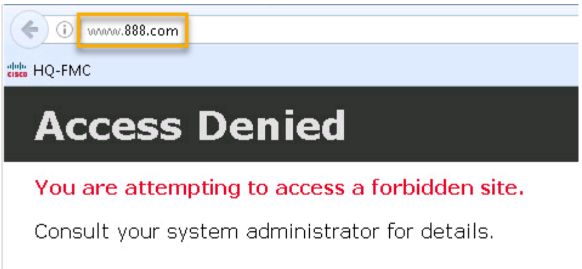
- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

Try Again

□ Report errors like this to help Mozilla identify and block malicious sites

Figure 269. No access to www.888.com



Access Denied

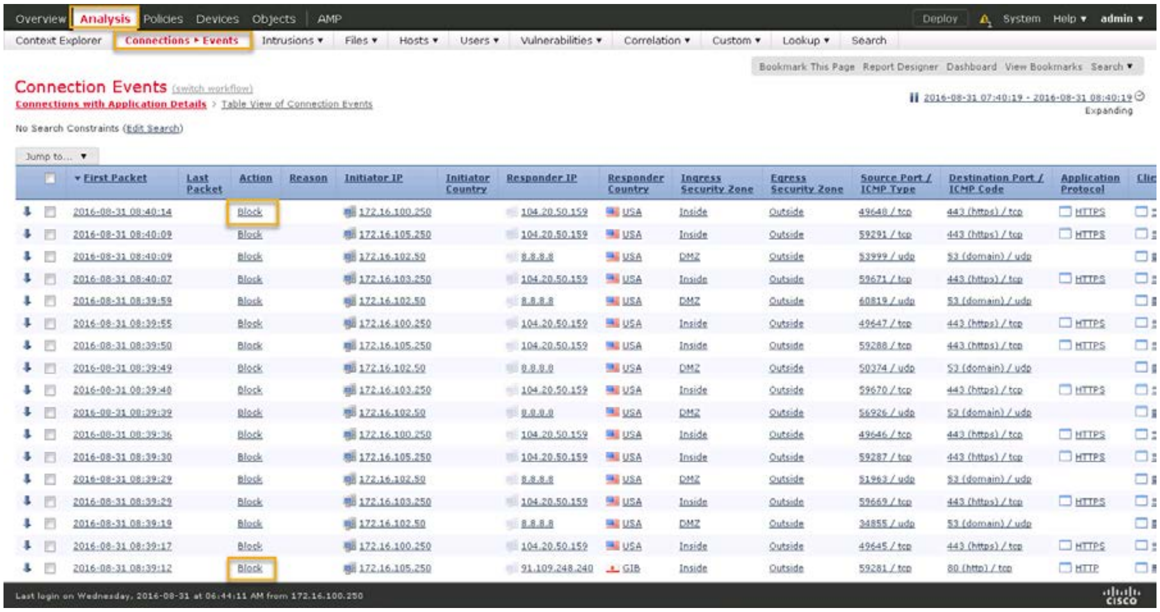
You are attempting to access a forbidden site.

Consult your system administrator for details.

Notice how www.gambling.com doesn't provide the "System-Provided" access denied webpage. Why is that? (I'll give you a hint. What protocol is being used to access www.gambling.com vs. www.888.com?)

21. Return to the FMC administration webpage. Navigate to **Analysis > Connections > Events** to view the logs of these attempted connections. You'll need to scroll to the right a lot to find the URL column to see which sites are being blocked. Also notice the URL Reputation column. You could have used this to further select which sites are permissible within the Gambling category had you wanted to.

Figure 270. Connection Events



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

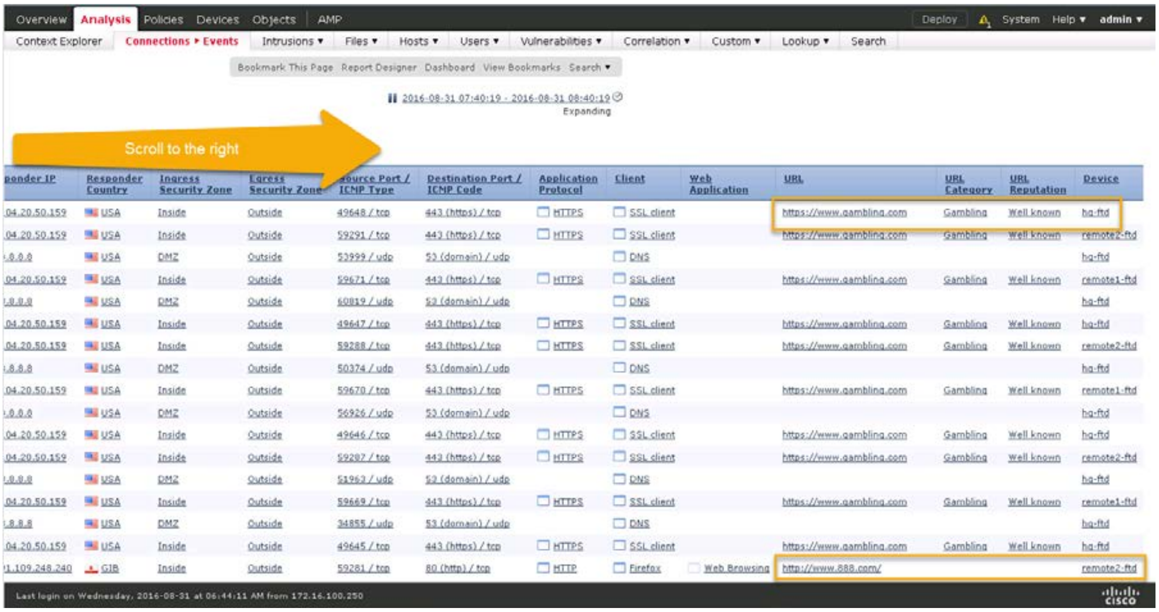
No Search Constraints (Edit Search)

2016-08-31 07:40:19 - 2016-08-31 08:40:19
Expanding

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Clie
2016-08-31 08:40:14		Block		172.16.100.250		104.20.50.159	USA	Inside	Outside	49648 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:40:09		Block		172.16.105.250		104.20.50.159	USA	Inside	Outside	59291 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:40:09		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	53999 / udp	53 (domain) / udp		
2016-08-31 08:40:07		Block		172.16.103.250		104.20.50.159	USA	Inside	Outside	59671 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:59		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	60819 / udp	53 (domain) / udp		
2016-08-31 08:39:55		Block		172.16.100.250		104.20.50.159	USA	Inside	Outside	49647 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:50		Block		172.16.105.250		104.20.50.159	USA	Inside	Outside	59288 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:49		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	50374 / udp	53 (domain) / udp		
2016-08-31 08:39:40		Block		172.16.103.250		104.20.50.159	USA	Inside	Outside	59670 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:39		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	56926 / udp	53 (domain) / udp		
2016-08-31 08:39:36		Block		172.16.100.250		104.20.50.159	USA	Inside	Outside	49646 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:30		Block		172.16.105.250		104.20.50.159	USA	Inside	Outside	59287 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:29		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	51963 / udp	53 (domain) / udp		
2016-08-31 08:39:29		Block		172.16.103.250		104.20.50.159	USA	Inside	Outside	59669 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:19		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	34855 / udp	53 (domain) / udp		
2016-08-31 08:39:17		Block		172.16.100.250		104.20.50.159	USA	Inside	Outside	49645 / tcp	443 (https) / tcp	HTTPS	
2016-08-31 08:39:12		Block		172.16.105.250		91.109.248.240	GIB	Inside	Outside	59281 / tcp	80 (http) / tcp	HTTP	

Last login on Wednesday, 2016-08-31 at 06:44:11 AM from 172.16.100.250

Figure 271. Scroll to the right



2016-08-31 07:40:19 - 2016-08-31 08:40:19
Expanding

ponder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
04.20.50.159	USA	Inside	Outside	49648 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	hq-ftd
04.20.50.159	USA	Inside	Outside	59291 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	remote2-ftd
.8.8.8	USA	DMZ	Outside	53999 / udp	53 (domain) / udp		DNS					hq-ftd
04.20.50.159	USA	Inside	Outside	59671 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	remote1-ftd
.8.8.8	USA	DMZ	Outside	60819 / udp	53 (domain) / udp		DNS					hq-ftd
04.20.50.159	USA	Inside	Outside	49647 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	hq-ftd
04.20.50.159	USA	Inside	Outside	59288 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	remote2-ftd
.8.8.8	USA	DMZ	Outside	50374 / udp	53 (domain) / udp		DNS					hq-ftd
04.20.50.159	USA	Inside	Outside	59670 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	remote1-ftd
.8.8.8	USA	DMZ	Outside	56926 / udp	53 (domain) / udp		DNS					hq-ftd
04.20.50.159	USA	Inside	Outside	49646 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	hq-ftd
04.20.50.159	USA	Inside	Outside	59287 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	remote2-ftd
.8.8.8	USA	DMZ	Outside	51963 / udp	53 (domain) / udp		DNS					hq-ftd
04.20.50.159	USA	Inside	Outside	59669 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	remote1-ftd
.8.8.8	USA	DMZ	Outside	34855 / udp	53 (domain) / udp		DNS					hq-ftd
04.20.50.159	USA	Inside	Outside	49645 / tcp	443 (https) / tcp	HTTPS	SSL client		https://www.gambling.com	Gambling	Well known	hq-ftd
1.109.248.240	GIB	Inside	Outside	59281 / tcp	80 (http) / tcp	HTTP	Firefox	Web Browsing	http://www.888.com/			remote2-ftd

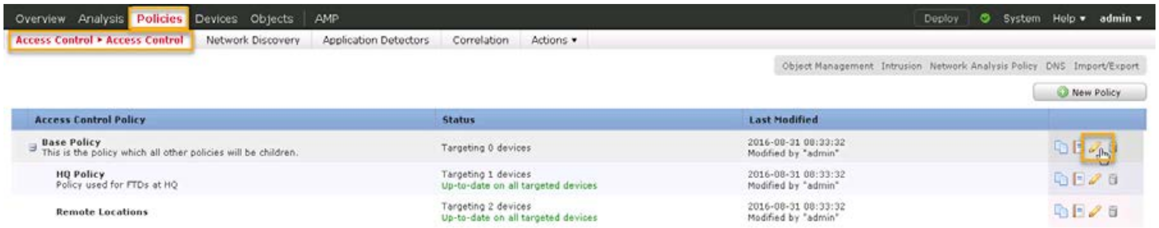
Last login on Wednesday, 2016-08-31 at 06:44:11 AM from 172.16.100.250

Create Social Media URL Filtering Rules

Now you need to create a rule in the Base Policy Default section blocking “social media”. You will then create a permissible rule in the HQ Policy’s Mandatory section allowing www.facebook.com. Use the following steps to accomplish this.

22. Navigate to **Policies > Access Control > Access Control**. Click the **pencil icon** on the row for the **Base Policy**.

Figure 272. Edit Base Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-31 08:33:32 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-31 08:33:32 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-08-31 08:33:32 Modified by "admin"

23. Click the **Add Rule** button and use the following to fill out the popup window.

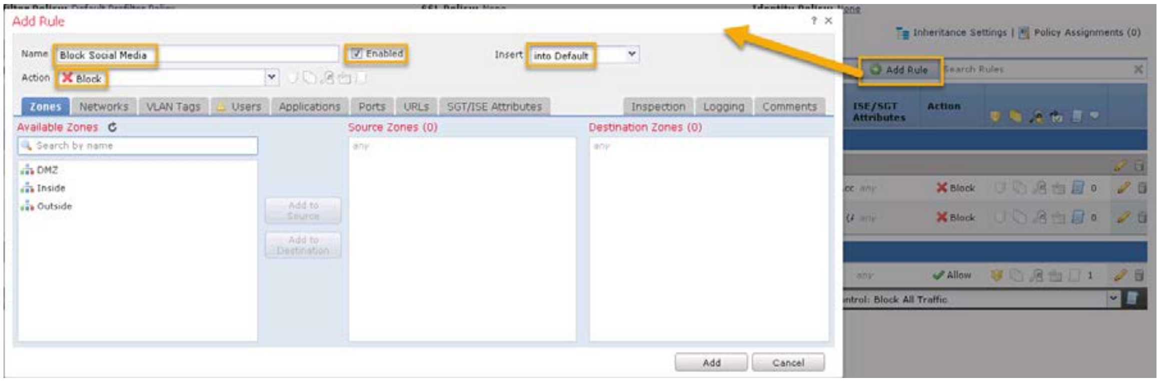
    a. Name: **Block Social Media**

    b. Enabled: **Checked**

    c. Insert: **into Default** (Why did you choose Default and not Mandatory?)

    d. Action: **Block**

Figure 273. Part 1 of Add rule



Add Rule

Name: Block Social Media

☑ Enabled

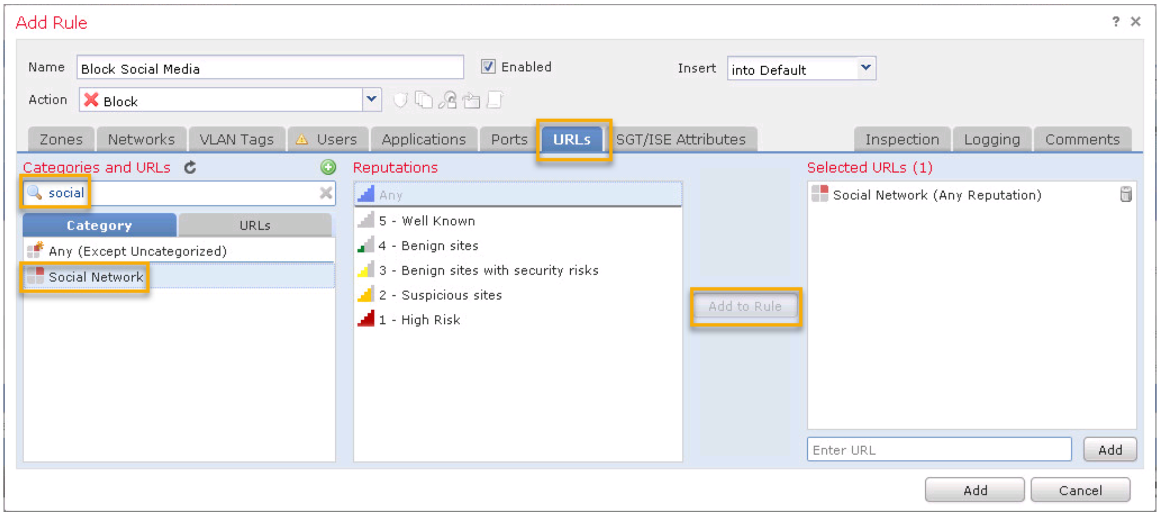
Insert: into Default

Action: ✖ Block

24. On the **URLs tab**:

    a. Search for **social** and then select **Social Network** from the list. Click the **Add to Rule** button.

Figure 274. Configure URLs tab



Add Rule

Name: Block Social Media

☑ Enabled

Insert: into Default

Action: Block

Categories and URLs: social

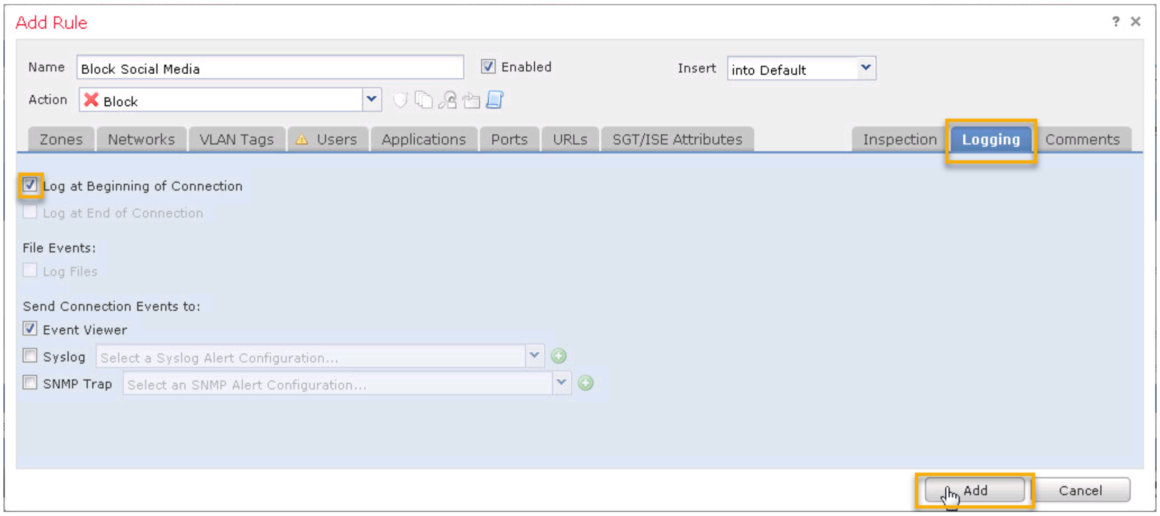
Selected URLs (1): Social Network (Any Reputation)

25. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** box.

26. Click **Add**.

Figure 275. Configure Logging tab and Add rule



Add Rule

Name: Block Social Media

☑ Enabled

Insert: into Default

Action: Block

☑ Log at Beginning of Connection

□ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

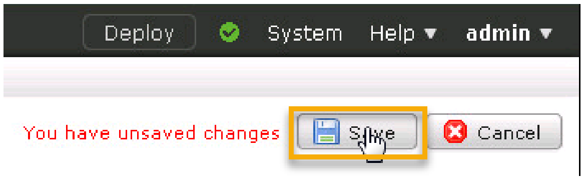
☑ Event Viewer

□ Syslog: Select a Syslog Alert Configuration...

□ SNMP Trap: Select an SNMP Alert Configuration...

27. Click **Save** before going on to edit the HQ Policy.

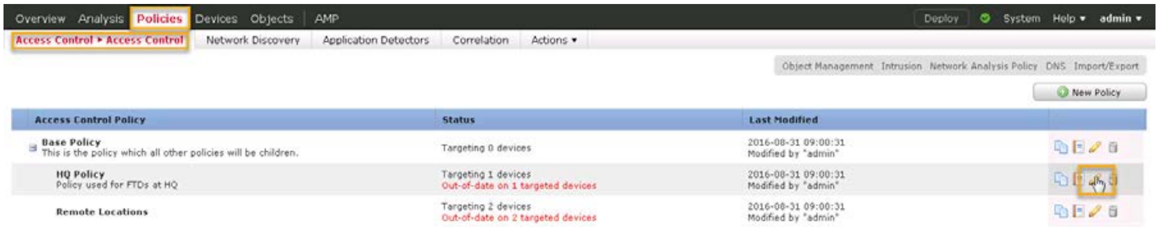
Figure 276. Save changes



You have unsaved changes

28. Navigate to **Policies > Access Control > Access Control** and click the **pencil icon** on the row for the **HQ Policy**.

Figure 277. Edit HQ Policy



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-31 09:00:31 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Out-of-date on 1 targeted devices	2016-08-31 09:00:31 Modified by "admin"
Remote Locations	Targeting 2 devices Out-of-date on 2 targeted devices	2016-08-31 09:00:31 Modified by "admin"

29. Click **Add Rule** and use the following to fill out the popup window.

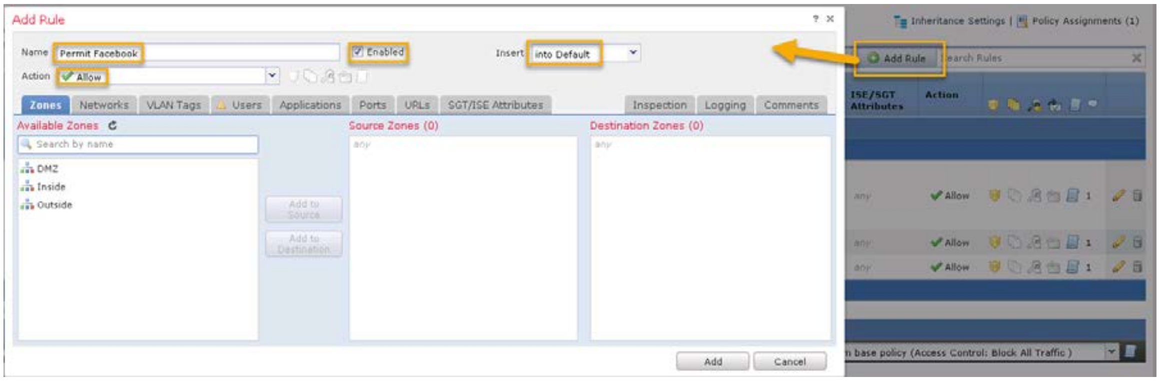
    a. Name: **Permit Facebook**

    b. Enabled: **Checked**

    c. Insert: **into Default**

    d. Action: **Allow**

Figure 278. Part 1 of adding a new rule



Add Rule

Name: Permit Facebook

☑ Enabled

Insert: into Default

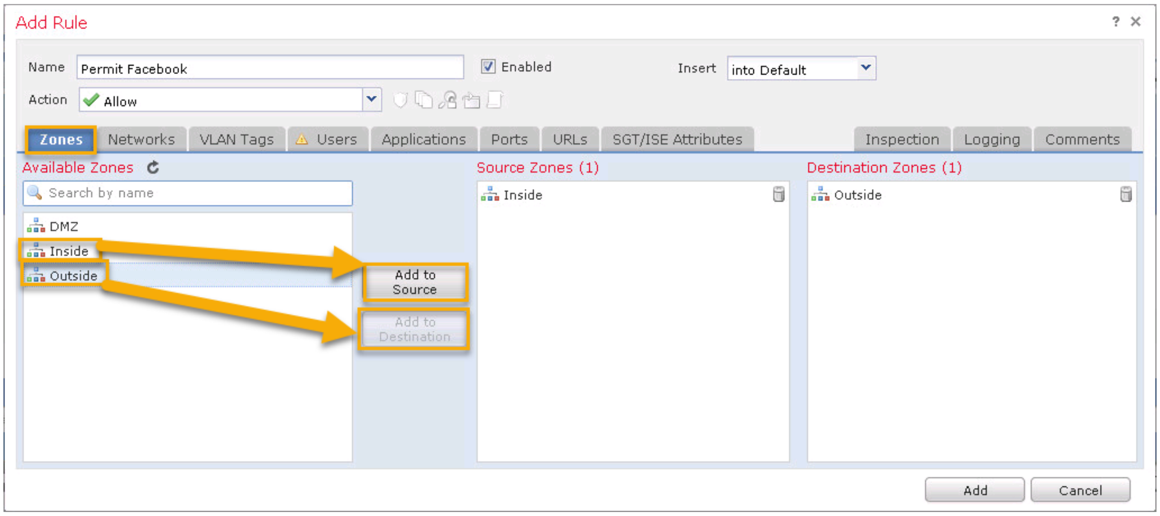
Action: ✓ Allow

30. On the **Zones tab**:

    a. Put **Inside** in the **Source Zones** section.

    b. Put **Outside** in the **Destination Zones** section.

Figure 279. Configure Zones tab



Add Rule

Name: Permit Facebook

☑ Enabled

Insert: into Default

Action: ✓ Allow

31. On the **URLs tab**:

    a. Click the **green plus icon** and create a **new URL Object** for www.facebook.com.

Figure 280. New URL Object

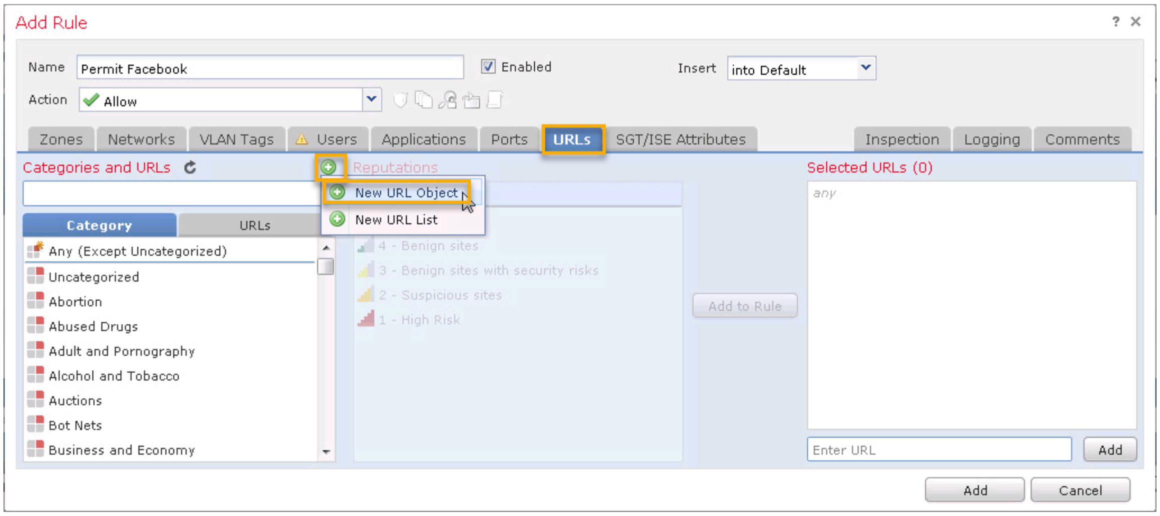
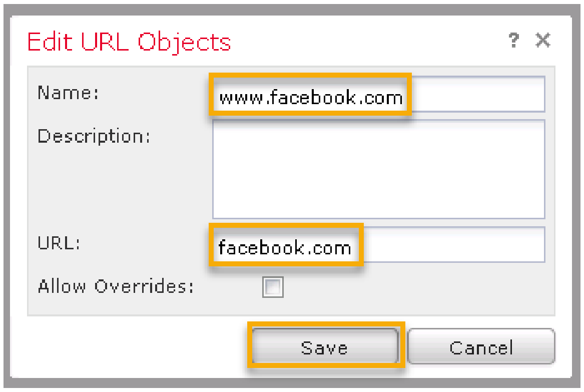


Figure 281. Create URL Object



Name: www.facebook.com

Description:

URL: facebook.com

Allow Overrides: □

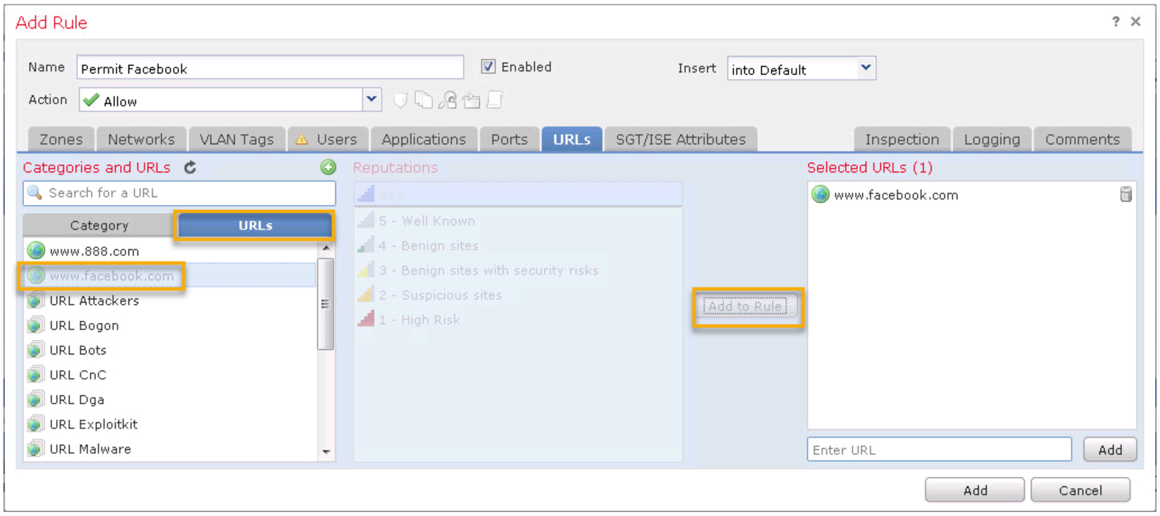
NOTE: When first creating this lab guide the Facebook URL Object’s URL was www.facebook.com. However, due to changes to Facebook’s homepage this section of the lab would fail where it used to work! (They made a change to refer to facebook.com instead of www.facebook.com which does not match our intended rule.) So, in order to make this part of the lab work we reduced the URL to just facebook.com.

The URL Objects are just text strings and will generate a match if/when any of the URL listed in the object matches part of the URL in the browser. So, technically we could make this object’s URL just “facebook” but then it would match against any URL that had the word facebook in it (such as facebook.is.lame.com). This may or may not be your intent, but in this lab we are trying to match against the REAL facebook website so trying to be as long of a match as possible is preferred. As a simple test, I created facebook.com.daxm.net, and pointed it to www.google.com. This will match our rule since “facebook.com” is in it, but obviously that was not our intent.

Unfortunately, the URL Object is just a string and is not a regular expression field. In that case, we could take care of this with a rule that matches something like “facebook.com[.]”.

b. Once created, select the **URL** for Facebook and click the **Add to Rule** button.

Figure 282. Configure URLs tab



Add Rule

Name: Permit Facebook

☑ Enabled

Insert: into Default

Action: ✓ Allow

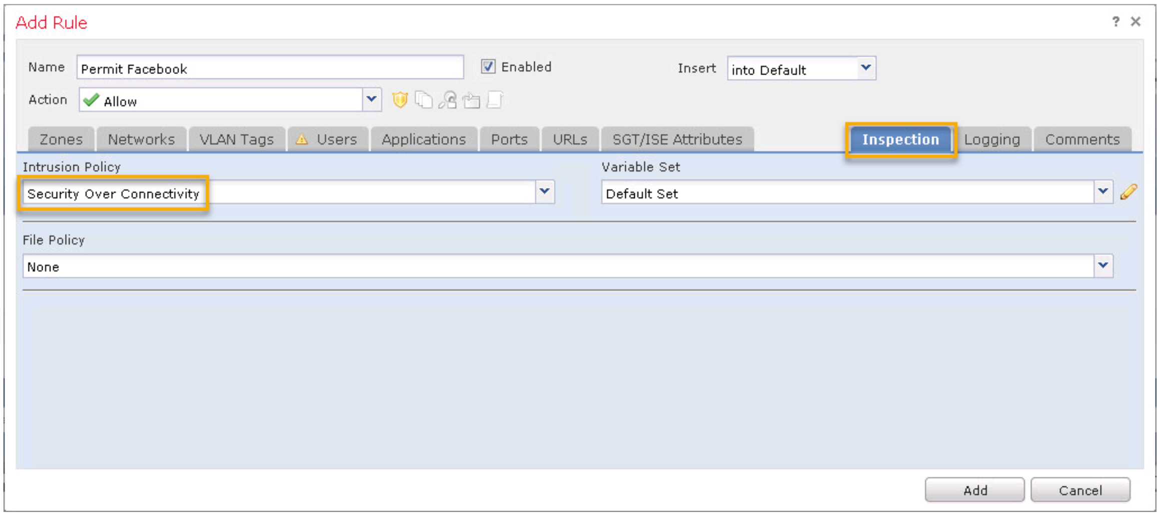
Selected URLs (1)

www.facebook.com

32. On the **Inspection tab**:

    a. Set the Intrusion Policy to **Security Over Connectivity**.

Figure 283. Configure Inspection tab



Add Rule

Name: Permit Facebook ☑ Enabled Insert: into Default

Action: ✓ Allow

Intrusion Policy: Security Over Connectivity

Variable Set: Default Set

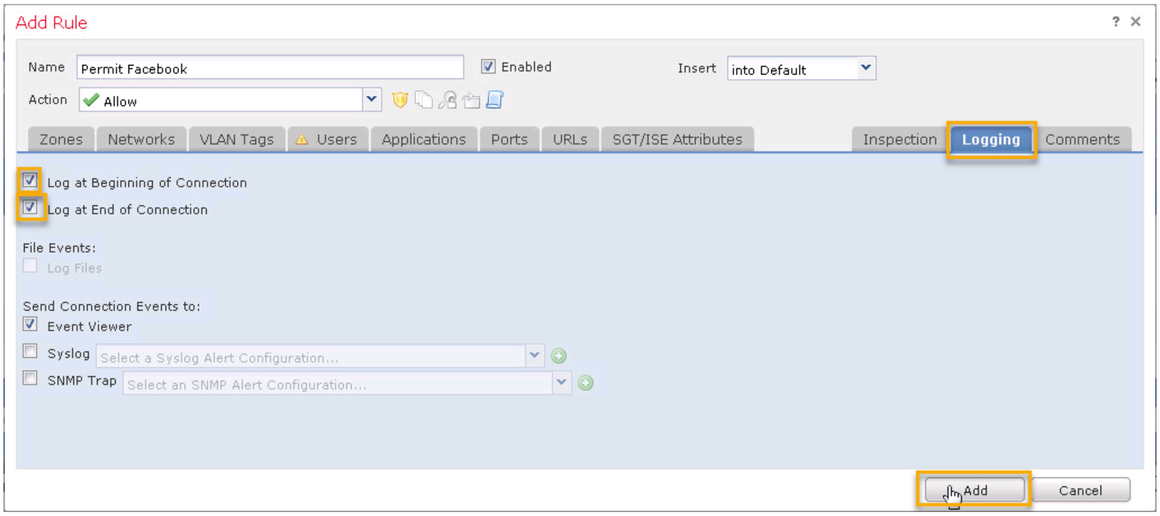
File Policy: None

33. On the **Logging tab**:

    a. Check both the **Log at Beginning of Connection** and **Log at End of Connection** boxes. (Arguably you could calculate how long someone was using Facebook with this combo.)

34. Click **Add** to create this rule.

Figure 284. Configure Logging tab and add rule



Add Rule

Name: Permit Facebook ☑ Enabled Insert: into Default

Action: ✓ Allow

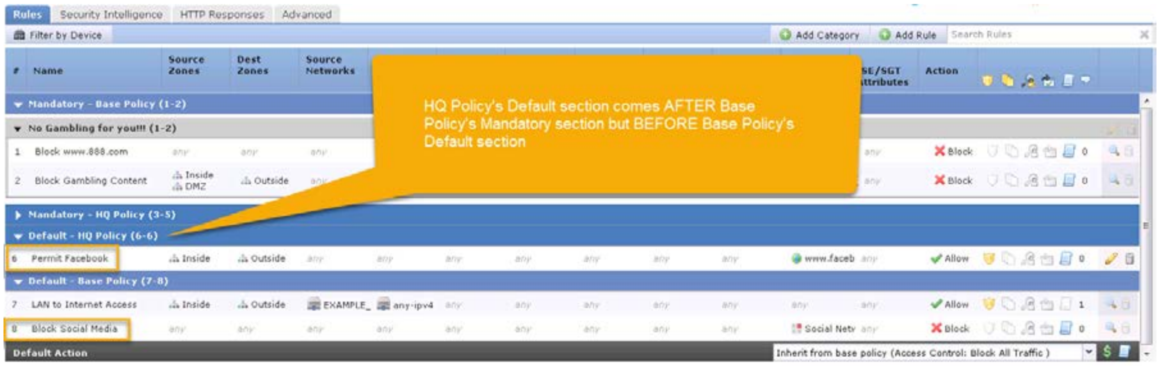
☑ Log at Beginning of Connection
☑ Log at End of Connection

File Events:
□ Log Files

Send Connection Events to:
☑ Event Viewer
□ Syslog Select a Syslog Alert Configuration...
□ SNMP Trap Select an SNMP Alert Configuration...

35. Expand the **Default – Base Policy** section to see why you put the Block Social Media in that section versus the **Mandatory – Base Policy**. The **Permit Facebook rule** would have never been reached had the Block Social Media had been put in the Mandatory – Base Policy section.

Figure 285. View order of ACP rules



#	Name	Source Zones	Dest Zones	Source Networks								SE/SGT ttributes	Action	
	Mandatory - Base Policy (1-2)													
	No Gambling for you!!! (1-2)													
1	Block www.888.com	any	any	any								any	Block	0
2	Block Gambling Content	Inside DMZ	Outside	any								any	Block	0
	Mandatory - HQ Policy (3-5)													
	Default - HQ Policy (6-6)													
6	Permit Facebook	Inside	Outside	any	any	any	any	any	any	any	www.faceb	any	Allow	0
	Default - Base Policy (7-8)													
7	LAN to Internet Access	Inside	Outside	EXAMPLE_	any-ipv4	any	any	any	any	any	any	any	Allow	1
8	Block Social Media	any	any	any	any	any	any	any	any	any	Social Netv	any	Block	0

Default Action: Inherit from base policy (Access Control: Block All Traffic)

HQ Policy's Default section comes AFTER Base Policy's Mandatory section but BEFORE Base Policy's Default section

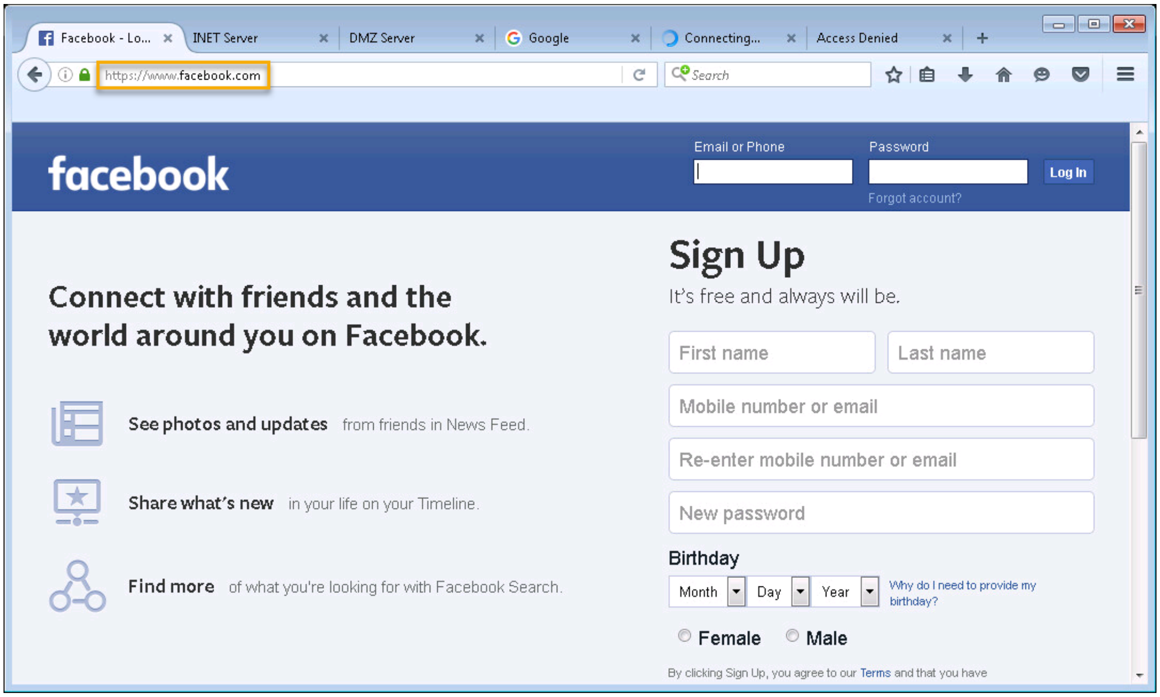
36. Click **Save**, then **Deploy**. Select **all the FTDs** and click **Deploy**.

Test Social Media URL Filtering Rules – Phase 1

Once the deployment to all the FTDs is complete, you need to verify the outcome of adding this URL filtering for social media. Given the title of this section, you should know that something is awry. ☺

37. From hq-wkst, you can get to www.facebook.com. However, remote1-wkst and remote2-wkst should not be able to access www.facebook.com but they can! Why?

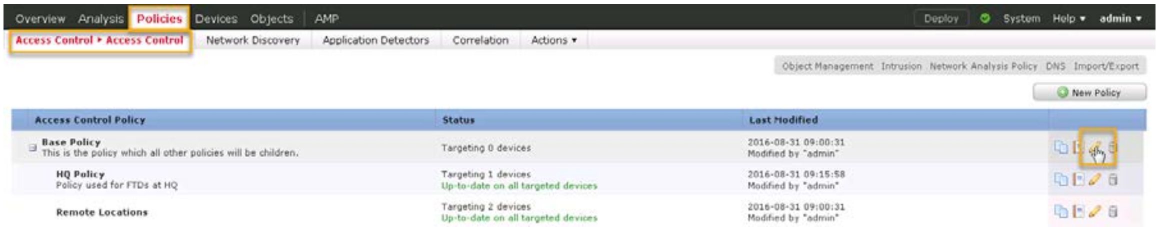
Figure 286. Success where it should have failed


Facebook - Lo...
INET Server
DMZ Server
Google
Connecting...
Access Denied
https://www.facebook.com
Search
facebook
Email or Phone
Password
Log In
Forgot account?
Sign Up
It's free and always will be.
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.
First name
Last name
Mobile number or email
Re-enter mobile number or email
New password
Birthday
Month
Day
Year
Why do I need to provide my birthday?
Female
Male
By clicking Sign Up, you agree to our Terms and that you have

Test Social Media URL Filtering Rules – Phase 2

38. The issue is with the order of the rules. To help you find the problem more quickly return to **hq-wkst** and navigate to **Policies > Access Control > Access Control** and **edit the Base Policy**. The rules are processed in a top-down fashion and the LAN to INET Access rule is matching your remote1-wkst and remote2-wkst attempts to go to www.facebook.com before you test the Block Social Media rule. You need to reorder the rules.

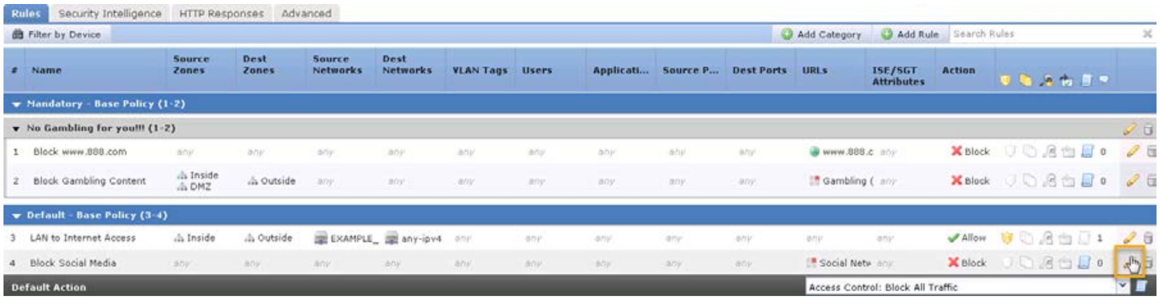
Figure 287. Edit Base Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-31 09:00:31 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-31 09:15:58 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-08-31 09:00:31 Modified by "admin"

39. **Edit** the **Block Social Media** rule.

Figure 288. Edit rule



Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device — Add Category — Add Rule — Search Rules

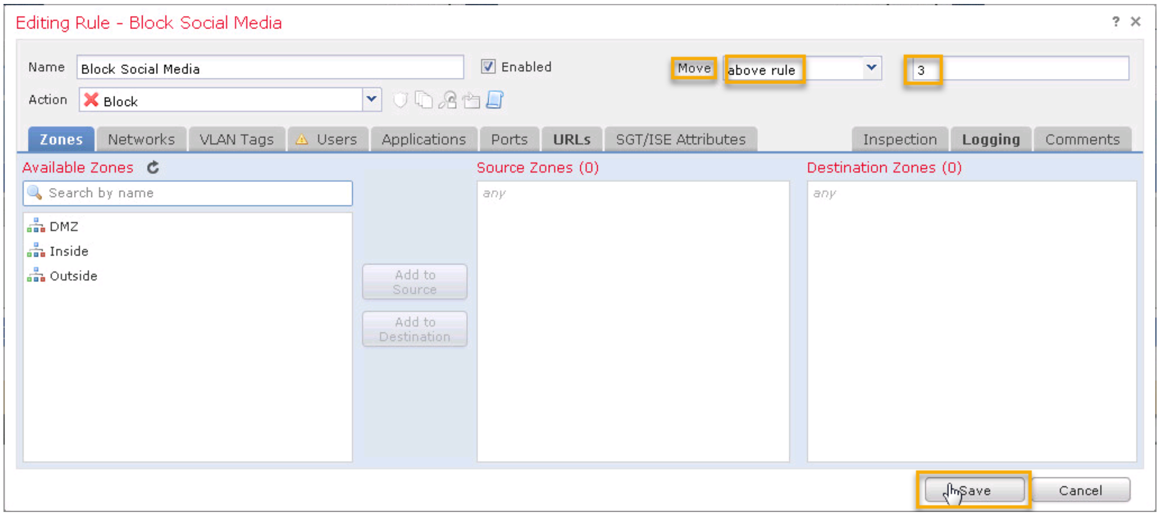
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
▼ Mandatory - Base Policy (1-2)														
▼ No Gambling for you!!! (1-2)														
1	Block www.888.com	any	any	any	any	any	any	any	any	any	www.888.c	any	✗ Block	0
2	Block Gambling Content	Inside DMZ	Outside	any	any	any	any	any	any	any	Gambling (	any	✗ Block	0
▼ Default - Base Policy (3-4)														
3	LAN to Internet Access	Inside	Outside	EXAMPLE_	any-ipv4	any	any	any	any	any	any	any	✓ Allow	1
4	Block Social Media	any	any	any	any	any	any	any	any	any	Social Netw	any	✗ Block	0
Default Action											Access Control: Block All Traffic			

40. Click the **Move** link and use the dropdown menus to select **above rule** and **3**.

If you have added other rules than those described in this lab guide then the rule number, 3 in this case, might be wrong and you'll have to use a different number for the reordering.

41. Click **Save** to save this rule.

Figure 289. Move and Save rule



Editing Rule - Block Social Media

Name: Block Social Media

☑ Enabled

Move: above rule — 3

Action: ✗ Block

Zones | Networks | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

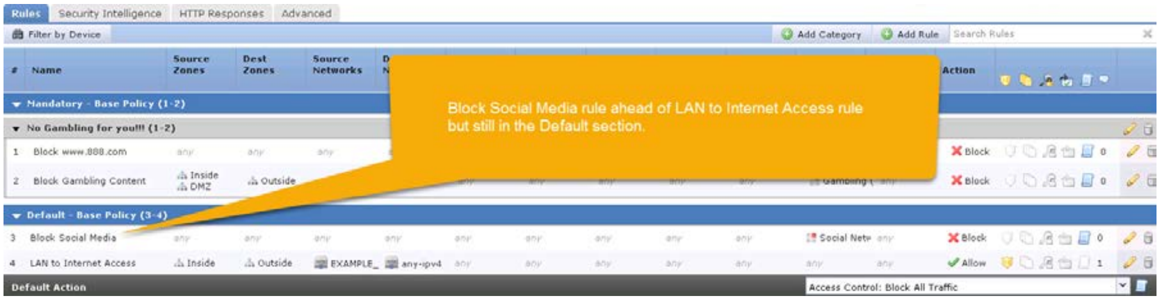
Available Zones: DMZ, Inside, Outside

Source Zones (0): any

Destination Zones (0): any

42. Double-check the order of the rules. The Block Social Media rule should be in the Default section BUT above the LAN to INET Access rule.

Figure 290. Check rule order



Block Social Media rule ahead of LAN to Internet Access rule but still in the Default section.

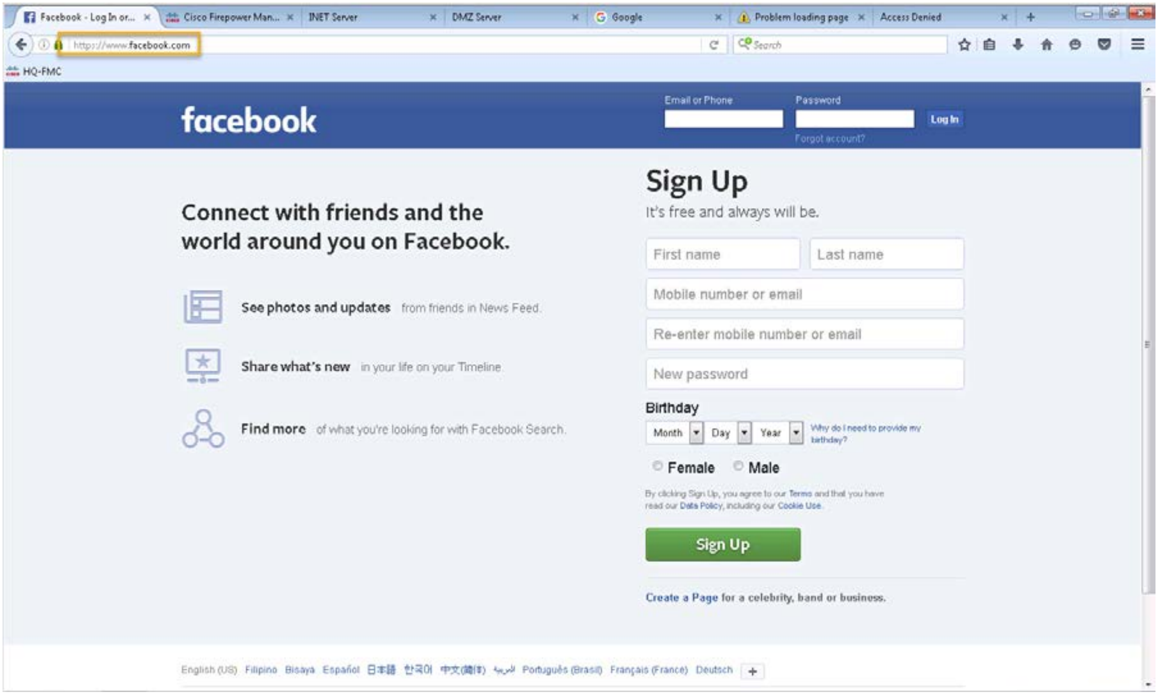
#	Name	Source Zones	Dest Zones	Source Networks	D N								Action	
	Mandatory - Base Policy (1-2)													
	No Gambling for you!!! (1-2)													
1	Block www.888.com	any	any	any									Block	0
2	Block Gambling Content	Inside DMZ	Outside			any	any	any	any	any	Gambling (	any	Block	0
	Default - Base Policy (3-4)													
3	Block Social Media	any	any	any	any	any	any	any	any	any	Social Netw	any	Block	0
4	LAN to Internet Access	Inside	Outside	EXAMPLE_	any-ipv4	any	any	any	any	any	any	any	Allow	1

Default Action: Access Control: Block All Traffic

43. Click **Save**, **Deploy**, select **all the devices** and click **Deploy**.

44. Retest by attempting to access www.facebook.com from each workstation. The HQ workstation will work while the remote1 and remote2 workstations will fail.

Figure 291. Access from hq-wkst works



http://www.facebook.com

Sign Up

It's free and always will be.

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.

First name

Last name

Mobile number or email

Re-enter mobile number or email

New password

Birthday

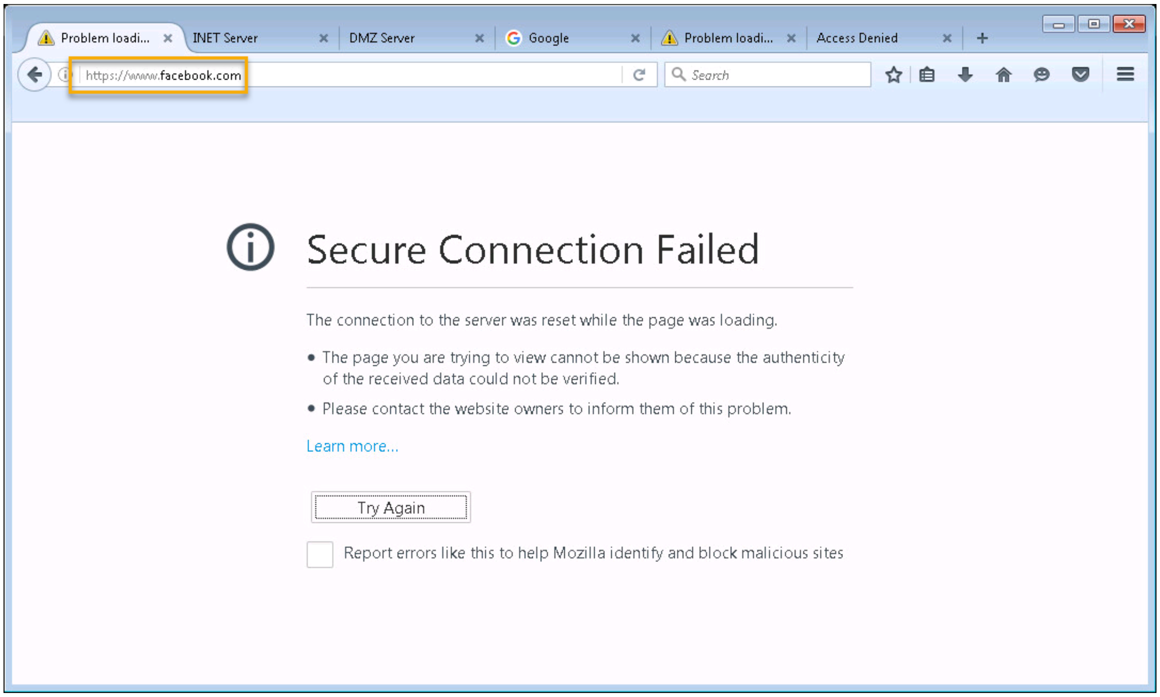
Why do I need to provide my birthday?

○ Female ○ Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

Create a Page for a celebrity, band or business.

Figure 292. Access from remote1-wkst fails



Secure Connection Failed

The connection to the server was reset while the page was loading.

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more...

Try Again

□ Report errors like this to help Mozilla identify and block malicious sites

Notice that you don't get the HTTP Response "system-defined" failure page. Why? (Because though you might have tried to access the HTTP version of Facebook it automatically redirects you to HTTPS. The HTTP Response page is ONLY for HTTP pages and not HTTPS ones. You may have noticed that same behavior with www.gambling.com test earlier in the lab.)

Scenario Summary

URL Filtering is a great tool to control the content allowed through a NGFW. This filtering can be highly customizable (based on reputation, or lists of URLs, or categories of content).

Scenario 7. SSL Policy Configuration

Scenario Description

More and more websites (both good and bad sites) are using SSL encryption to secure the connection between the client and the server. This is great for securing people’s credit card transactions but it is bad for security professionals who have been tasked with controlling the content that passes through their networks.

In this scenario you will be creating an SSL Policy that will allow the FTD devices to be a “Man in the Middle” (MiTM) devices for any SSL communications traversing them.

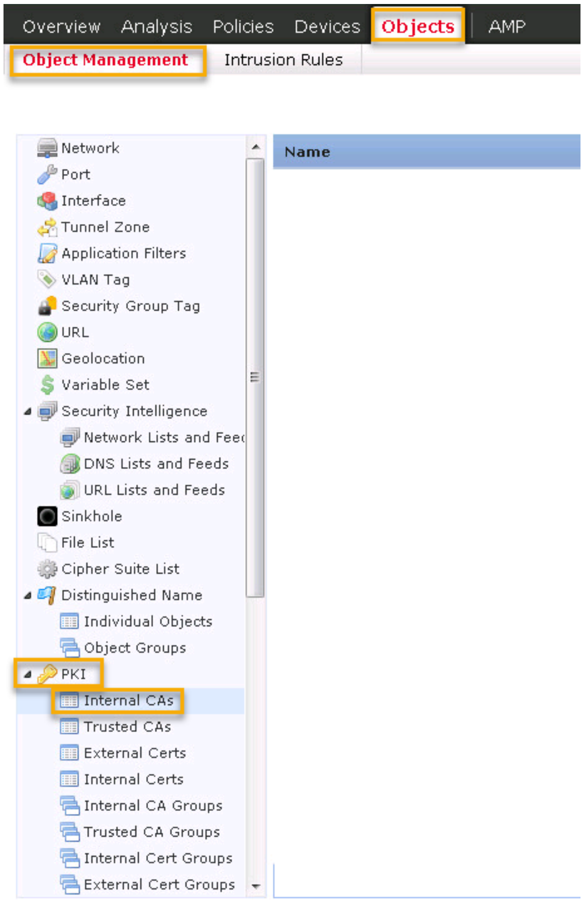
Note: There are other deployment methods for using the SSL Policy. This particular scenario is only showing how to decrypt and resign SSL communications. Other scenarios might not resign the packet but that requires the FTD to have the private key associated with the certificate being used.

Configure and Apply an SSL Policy

In order for the FTD devices to be a MiTM device they need a Certificate Authority (CA). Use the following to create a CA certificate so that the FMC is the CA.

1. In the FMC, navigate to **Objects > Object Management** section of the FMC website.
2. Select expand the **PKI option** from the left menu and select **Internal CAs**.

Figure 293. Navigate to Internal CAs



3. Click **Generate CA** and fill out the following:

   a. Name: **FMC_AS_A_CA**

   b. Country: **US**

   c. State: **ID**

   d. City: **Kimberly**

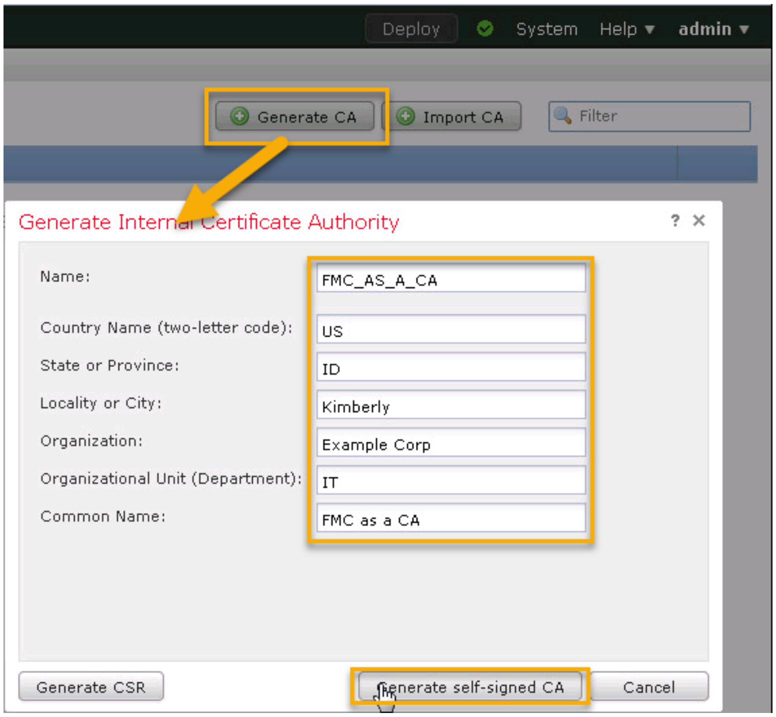
   e. Org: **Example Corp**

   f. Dept: **IT**

   g. Common Name: **FMC as a CA**

4. Click **Generate self-signed CA**

Figure 294. Create CA



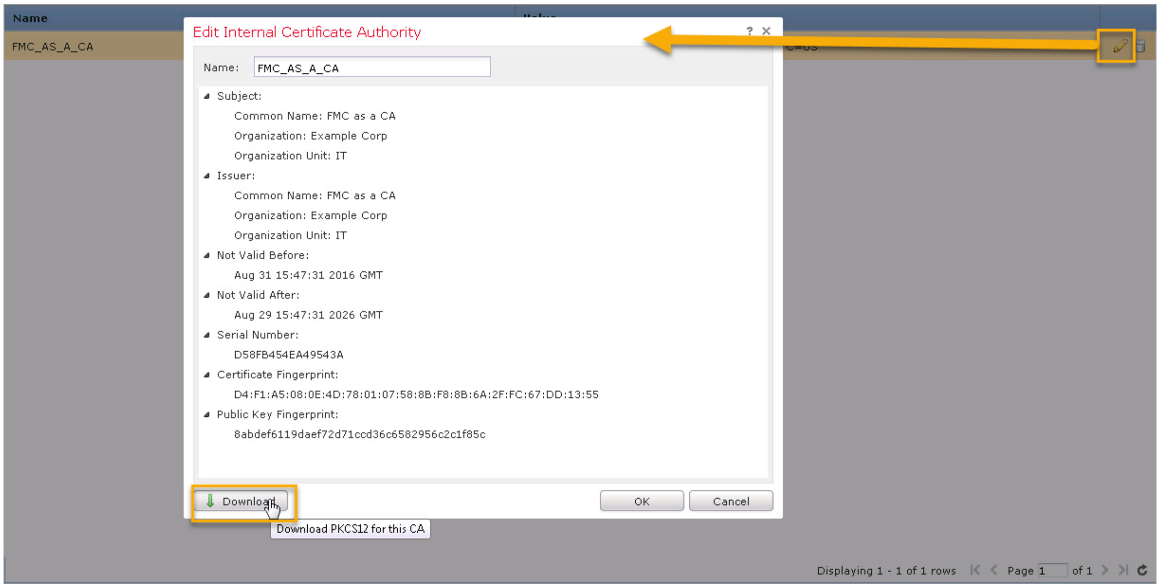
Generate Internal Certificate Authority

Name:	FMC_AS_A_CA
Country Name (two-letter code):	US
State or Province:	ID
Locality or City:	Kimberly
Organization:	Example Corp
Organizational Unit (Department):	IT
Common Name:	FMC as a CA

5. **Edit** the newly created CA. This will pop up a window showing you its details. Take note of the Expire Date as you'll need to renew this certificate prior to that date or all your SSL decryption policies will start to fail.

6. Click **Download** to download a copy of this certificate.

Figure 295. Download CA to hq-wkst



Edit Internal Certificate Authority

Name: FMC_AS_A_CA

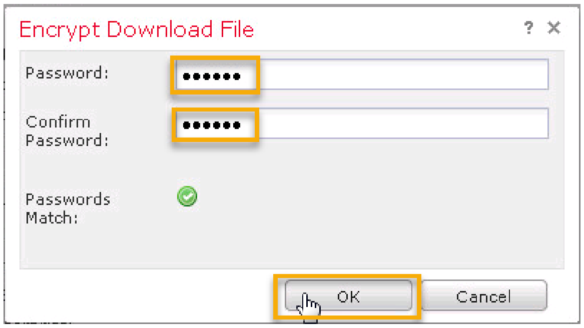
- Subject:
  - Common Name: FMC as a CA
  - Organization: Example Corp
  - Organization Unit: IT
- Issuer:
  - Common Name: FMC as a CA
  - Organization: Example Corp
  - Organization Unit: IT
- Not Valid Before:
  - Aug 31 15:47:31 2016 GMT
- Not Valid After:
  - Aug 29 15:47:31 2026 GMT
- Serial Number:
  - D58FB454EA49543A
- Certificate Fingerprint:
  - D4:F1:A5:08:0E:4D:78:01:07:58:8B:F8:8B:6A:2F:FC:67:DD:13:55
- Public Key Fingerprint:
  - 8abdef6119daef72d71ccd36c6582956c2c1f85c

Download PKCS12 for this CA

Displaying 1 - 1 of 1 rows

7. You will be asked to add/create a password to encrypt this downloaded certificate. Use **abc123** for the password and then click **OK**. If prompted don't save this password in Firefox.

Figure 296. Create password



Encrypt Download File

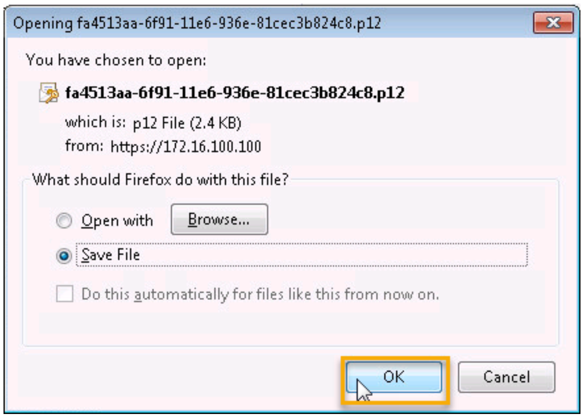
Password: ●●●●●●

Confirm Password: ●●●●●●

Passwords Match: ✓

8. When prompted, click **OK** to save the file. This will put it in the Downloads directory.

Figure 297. Save CA



Opening fa4513aa-6f91-11e6-936e-81cec3b824c8.p12

You have chosen to open:

fa4513aa-6f91-11e6-936e-81cec3b824c8.p12

which is: p12 File (2.4 KB)

from: https://172.16.100.100

What should Firefox do with this file?

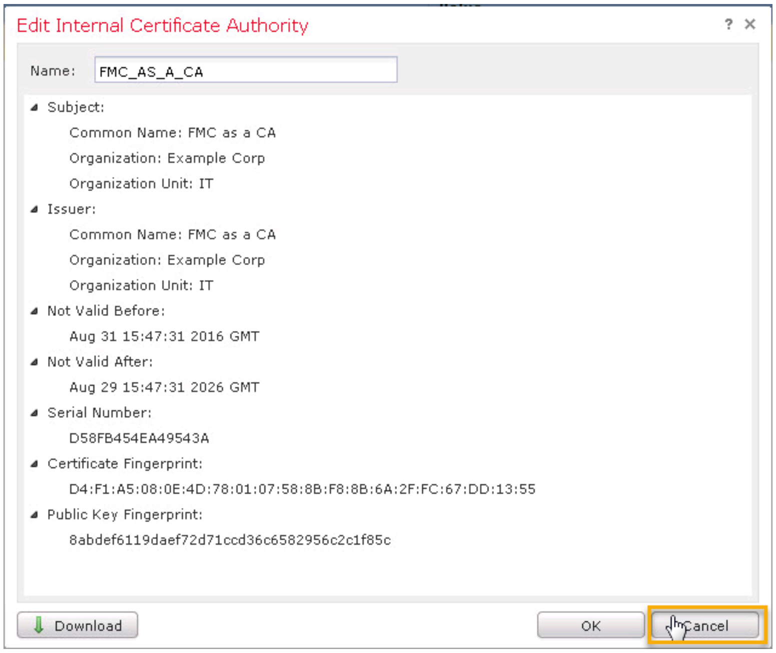
○ Open with [Browse...]

● Save File

□ Do this automatically for files like this from now on.

9. Click **Cancel** to exit editing the CA.

Figure 298. Cancel edit of CA



Edit Internal Certificate Authority

Name: FMC_AS_A_CA

Subject:

Common Name: FMC as a CA

Organization: Example Corp

Organization Unit: IT

Issuer:

Common Name: FMC as a CA

Organization: Example Corp

Organization Unit: IT

Not Valid Before:

Aug 31 15:47:31 2016 GMT

Not Valid After:

Aug 29 15:47:31 2026 GMT

Serial Number:

D58FB454EA49543A

Certificate Fingerprint:

D4:F1:A5:08:0E:4D:78:01:07:58:8B:F8:8B:6A:2F:FC:67:DD:13:55

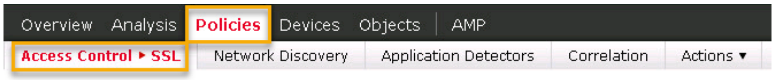
Public Key Fingerprint:

8abdef6119daef72d71ccd36c6582956c2c1f85c

Now that the CA certificate has been created and you have downloaded a copy of it (which you will use a little bit later in the lab) it is time to create the SSL Policy.

10. Navigate to **Policies > Access Control > SSL**.

Figure 299. Navigate to SSL Policy



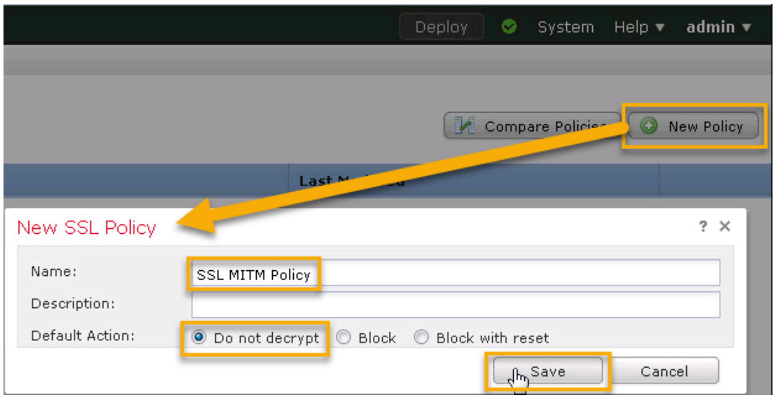
11. Click **New Policy** and fill out the following:

    a. Name: **SSL MITM Policy**

    b. Default Action: **Do not decrypt**

    c. Click **Save**.

Figure 300. Create new policy



New SSL Policy

Name: SSL MITM Policy

Description:

Default Action: ● Do not decrypt ○ Block ○ Block with reset

12. Now that you are in edit mode for the newly created SSL Policy, click **Add Rule** and use the following to fill out the popup window:

    a. Name: **MITM**

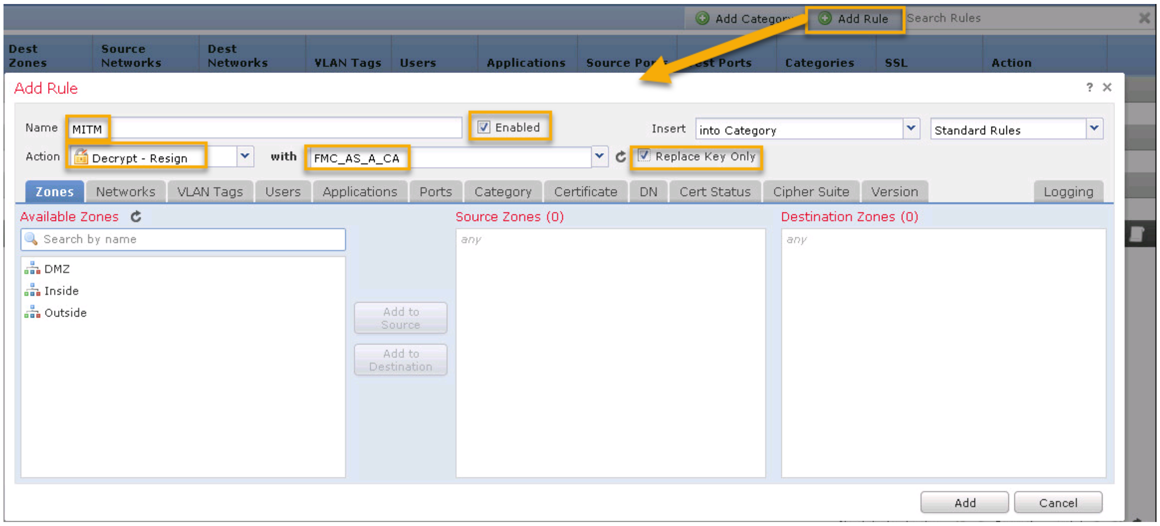
    b. Enabled: **Checked**

    c. Action: **Decrypt – Resign**

    d. With: **FMC_AS_A_CA**

    e. Replace Key Only: **Checked**

Figure 301. Part 1 of adding rule



Add Rule

Name: MITM ☑ Enabled Insert: into Category Standard Rules

Action: Decrypt - Resign with FMC_AS_A_CA ☑ Replace Key Only

Available Zones: DMZ, Inside, Outside

Source Zones (0): any

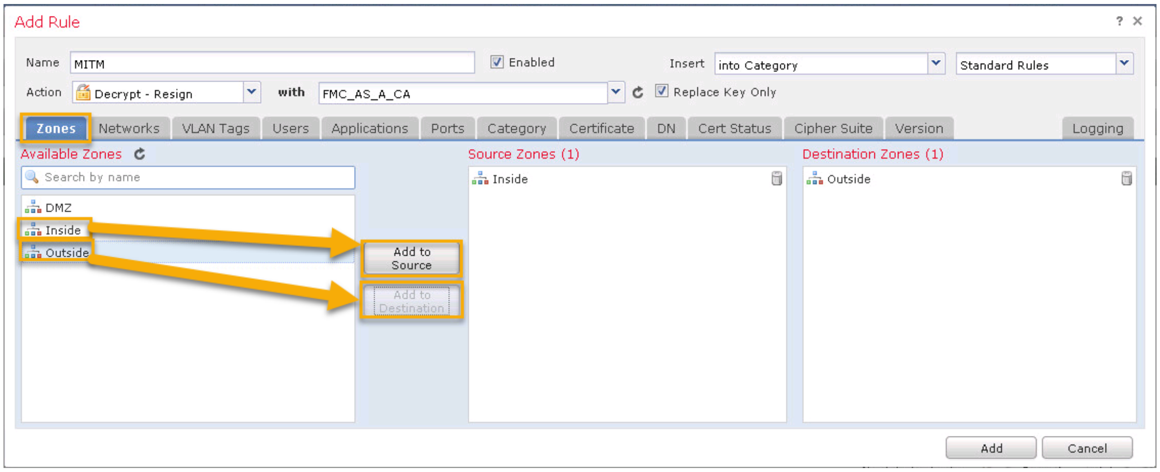
Destination Zones (0): any

13. On **Zones tab**:

    a. Source Zones: **Inside**

    b. Destination Zones: **Outside**

Figure 302. Configure Zones tab



Add Rule

Name: MITM ☑ Enabled Insert: into Category | Standard Rules

Action: Decrypt - Resign with FMC_AS_A_CA ☑ Replace Key Only

Available Zones: DMZ, Inside, Outside

Source Zones (1): Inside

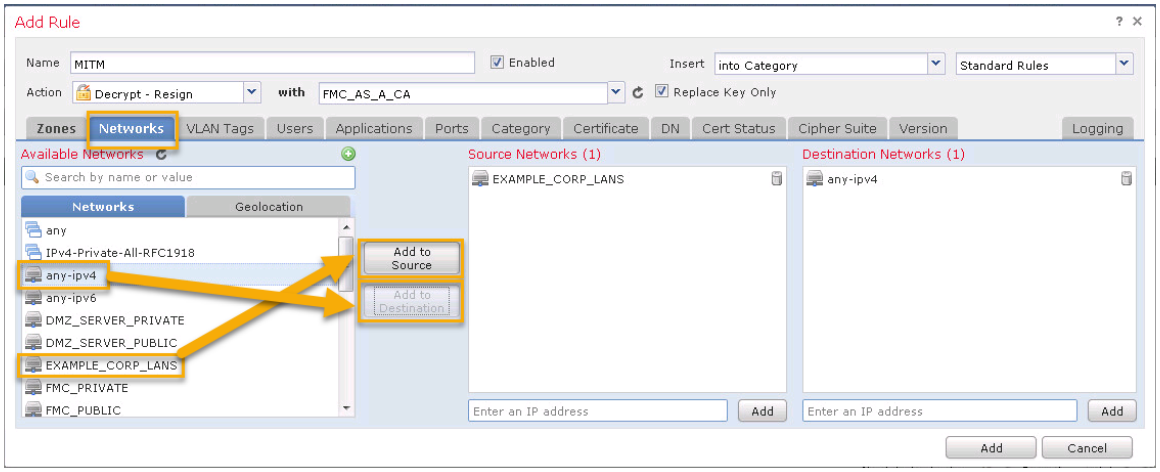
Destination Zones (1): Outside

14. On **Networks tab**:

    a. Source: **EXAMPLE_CORP_LANS**

    b. Destination: **any-ipv4**

Figure 303. Configure Networks tab



Add Rule

Name: MITM ☑ Enabled Insert: into Category | Standard Rules

Action: Decrypt - Resign with FMC_AS_A_CA ☑ Replace Key Only

Available Networks: any, IPv4-Private-All-RFC1918, any-ipv4, any-ipv6, DMZ_SERVER_PRIVATE, DMZ_SERVER_PUBLIC, EXAMPLE_CORP_LANS, FMC_PRIVATE, FMC_PUBLIC

Source Networks (1): EXAMPLE_CORP_LANS

Destination Networks (1): any-ipv4

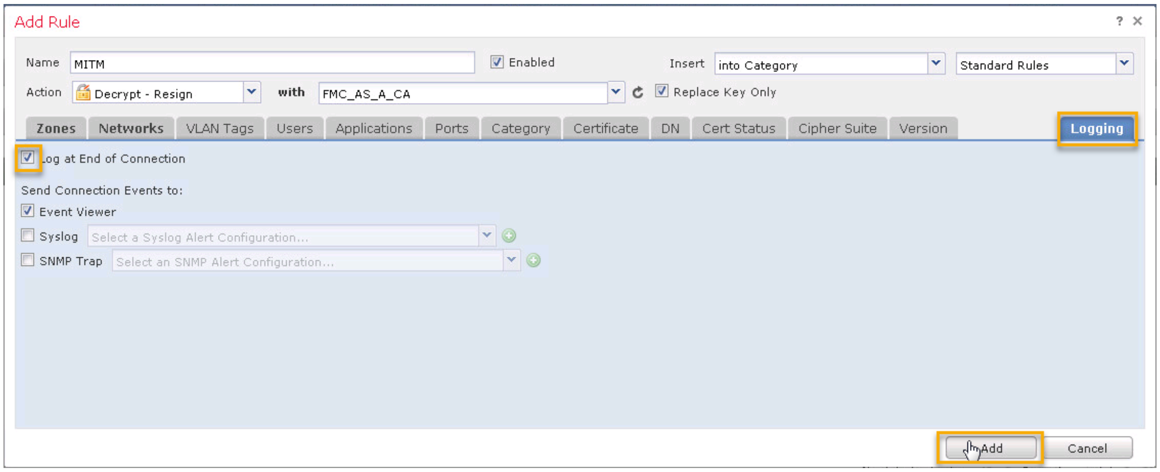
15. On the **Logging tab**:

    a. Check the **Log at End of Connection** box.

The Certificate, DN, Cert Status, Cipher Suite, and Version tabs can be used to further filter the type of certificate you wish to identify. This could be a way to block SSL session that are using weak and/or hacked versions of SSL.

16. Click **Add** to create this rule.

Figure 304. Configure Logging tab and Add rule



Name MITM ☑ Enabled Insert into Category Standard Rules
Action Decrypt - Resign with FMC_AS_A_CA ☑ Replace Key Only

☑ Log at End of Connection

Send Connection Events to:
☑ Event Viewer
□ Syslog Select a Syslog Alert Configuration...
□ SNMP Trap Select an SNMP Alert Configuration...

Decrypting and re-signing the connection between the FMC and remote FTDs (and other cloud services it uses) will not work. In order to not decrypt this traffic, you need two more rules in this SSL policy. One rule will match connections initiated from the remote FTD to the FMC and the other rule will match traffic initiated by the FMC going to the remote FTDs and/or cloud services. (You need both since remote1-ftd and remote2-ftd are using different methods in connecting to the FMC.) If you recall during the registration process remote1-ftd wasn’t given the FMC’s IP address (thus the FMC must initiate the connection) whereas the situation is the reverse with remote2-ftd (where the FMC doesn’t know remote2-ftd’s IP address so the remote2-ftd must initiate the connection).

17. Click **Add Rule** to begin the creation of this new rule. Use the following to fill out the popup window:

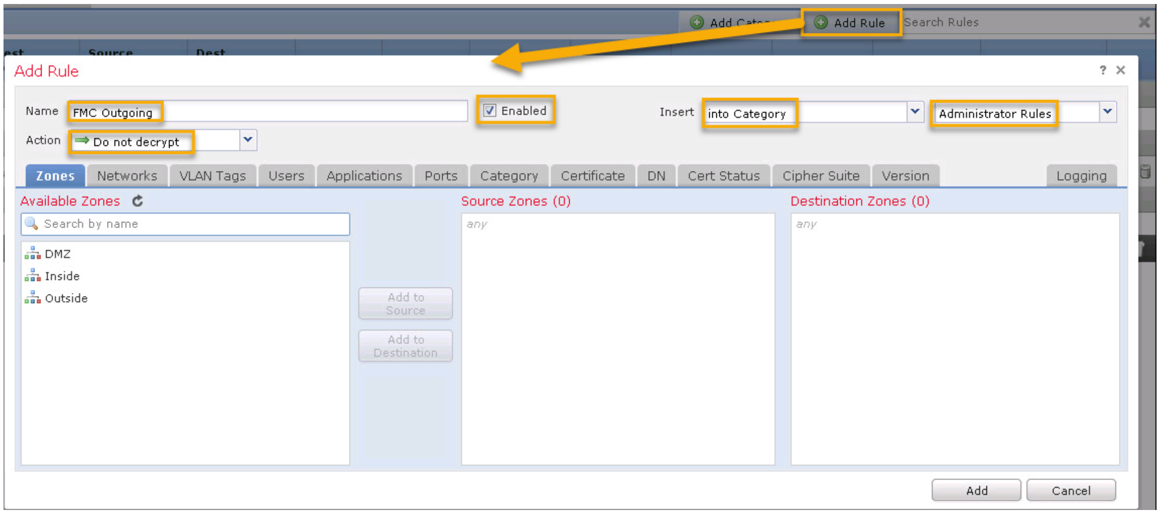
    a. Name: **FMC Outgoing**

    b. Enabled: **Checked**

    c. Insert: **into Category** and then **Administrator Rules**

    d. Action: **Do not decrypt**

Figure 305. Part 1 adding new rule



Add Rule

Name: FMC Outgoing

☑ Enabled

Insert: into Category — Administrator Rules

Action: Do not decrypt

Available Zones: DMZ, Inside, Outside

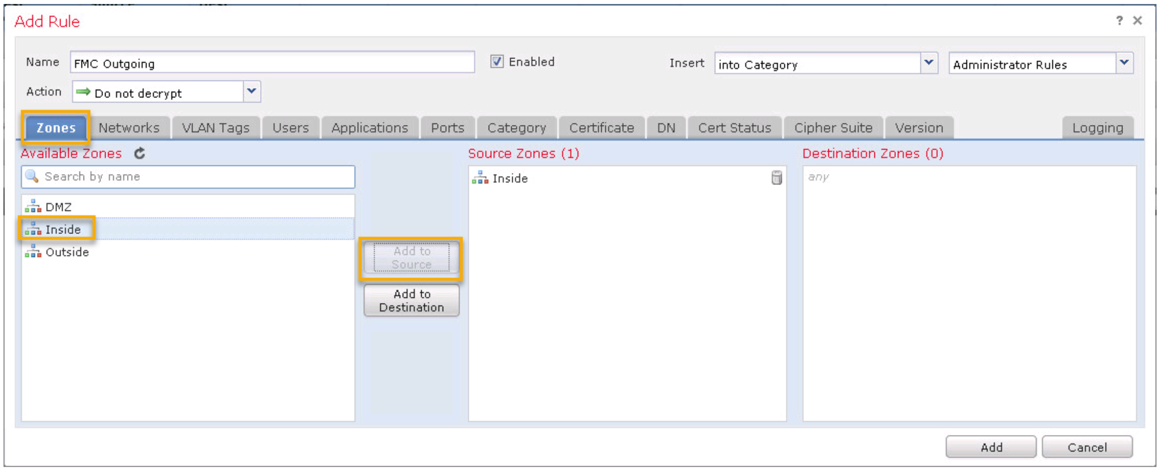
Source Zones (0): any

Destination Zones (0): any

18. On the **Zones tab**:

    a. Source Zones: **Inside**

Figure 306. Configure Zones tab



Add Rule

Name: FMC Outgoing

☑ Enabled

Insert: into Category — Administrator Rules

Action: Do not decrypt

Available Zones: DMZ, Inside, Outside

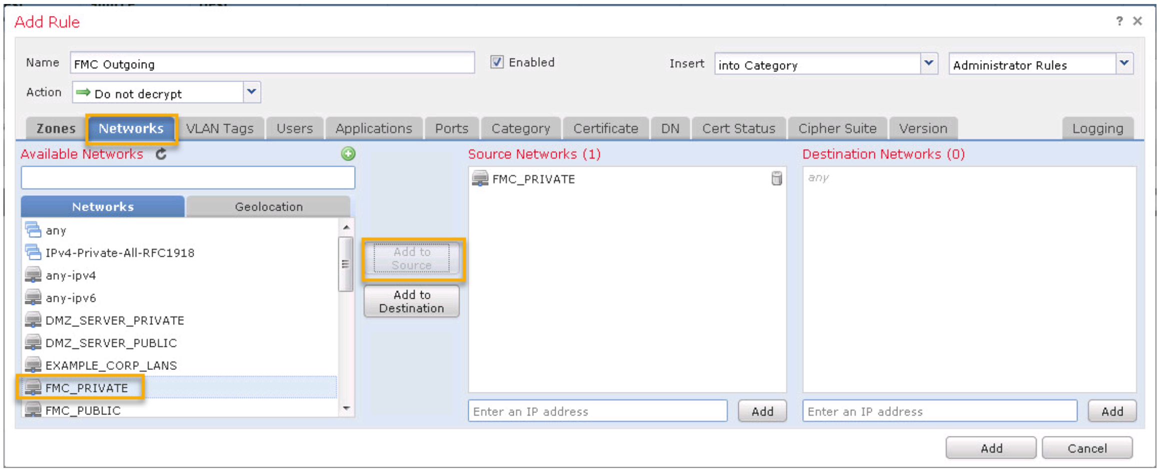
Source Zones (1): Inside

Destination Zones (0): any

19. On the **Networks tab**:

    a. Source Networks: **FMC_PRIVATE**

Figure 307. Configure Networks tab



Add Rule

Name: FMC Outgoing ☑ Enabled Insert: into Category | Administrator Rules

Action: Do not decrypt

Source Networks (1): FMC_PRIVATE

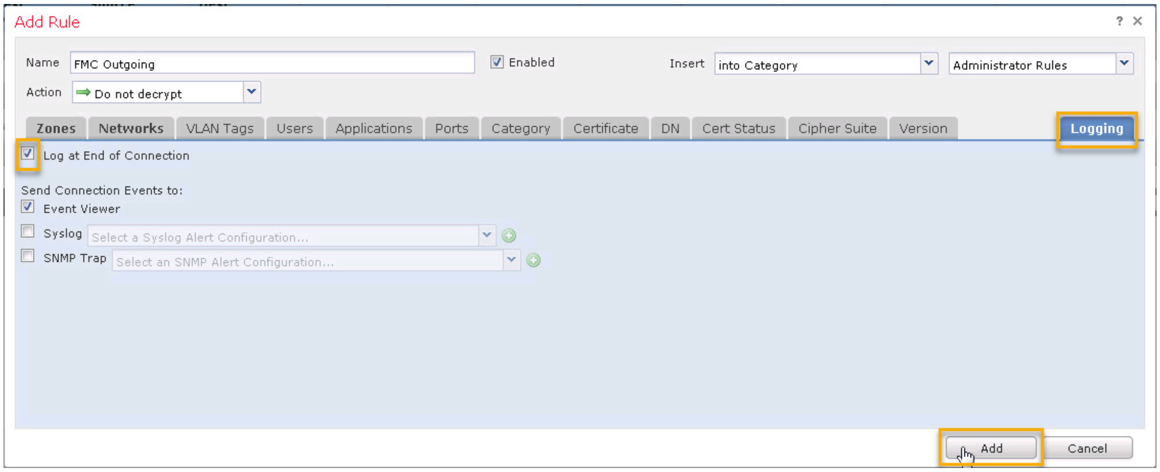
Destination Networks (0): any

20. On the **Logging tab**:

    a. **Log at the End of Connection** is checked.

21. Click **Add**.

Figure 308. Configure Logging and Add rule



Add Rule

Name: FMC Outgoing ☑ Enabled Insert: into Category | Administrator Rules

Action: Do not decrypt

☑ Log at End of Connection

Send Connection Events to:

☑ Event Viewer

☐ Syslog Select a Syslog Alert Configuration...

☐ SNMP Trap Select an SNMP Alert Configuration...

22. Click **Add Rule** again to create identify traffic coming the other direction. Use the following to fill out the popup window:

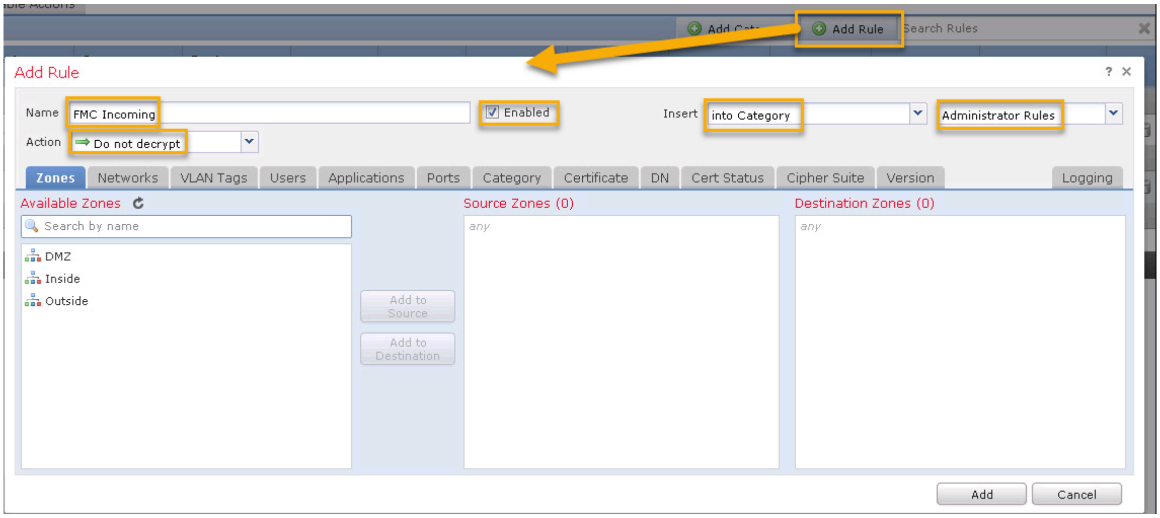
    a. Name: **FMC Incoming**

    b. Enabled: **Checked**

    c. Insert: **into Category** and then **Administrator Rules**

    d. Action: **Do not decrypt**

Figure 309. Add another rule



Add Rule

Name: FMC Incoming

☑ Enabled

Insert: into Category

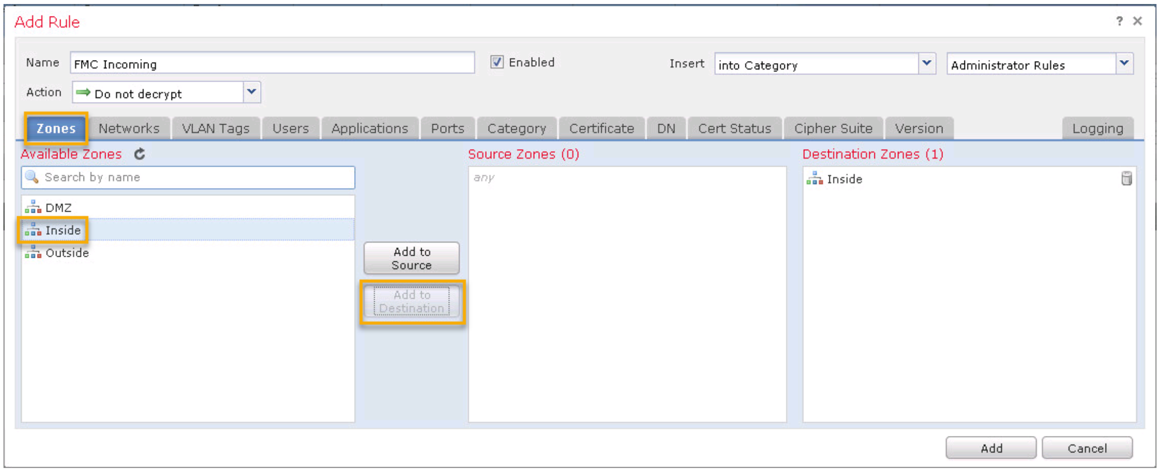
Administrator Rules

Action: Do not decrypt

23. On the **Zones tab**:

    a. Destination Zones: **Inside**

Figure 310. Configure Zones tab



Add Rule

Name: FMC Incoming

☑ Enabled

Insert: into Category

Administrator Rules

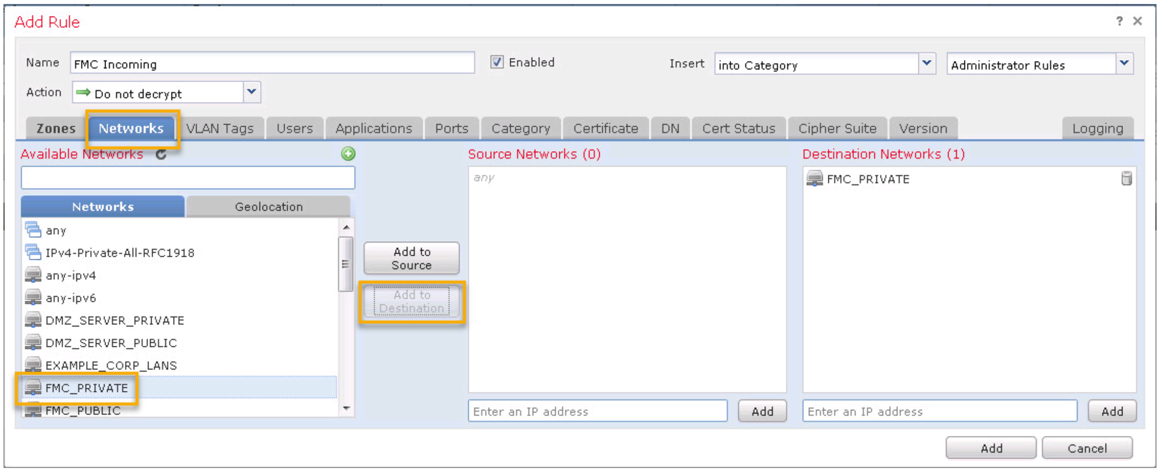
Action: Do not decrypt

Destination Zones (1): Inside

24. On the **Networks tab**:

    a. Destination Networks: **FMC_PRIVATE**

Figure 311. Configure Networks tab



Add Rule

Name: FMC Incoming
☑ Enabled
Insert: into Category | Administrator Rules
Action: Do not decrypt

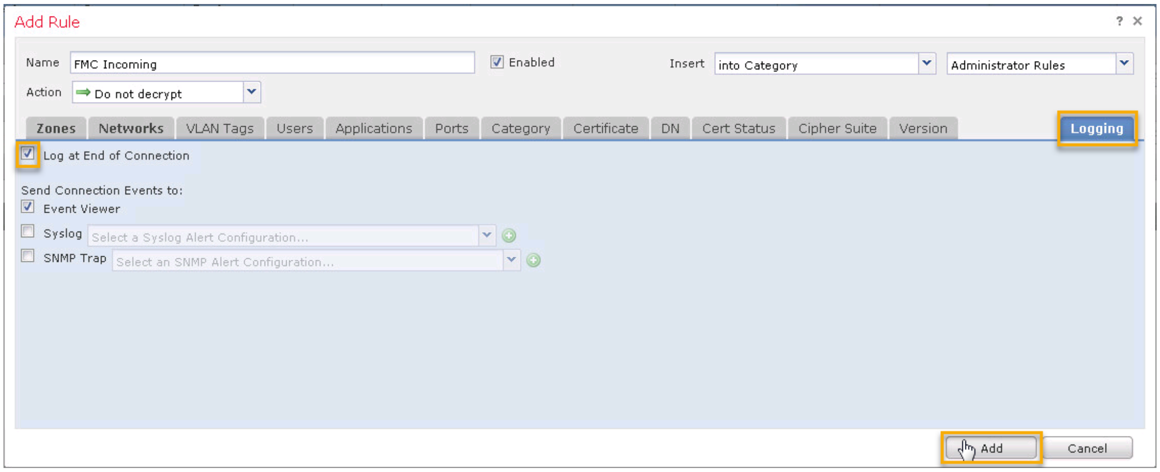
Available Networks
Source Networks (0): any
Destination Networks (1): FMC_PRIVATE

25. On the **Logging tab**:

    a. **Log at the End of Connection** is checked.

26. Click **Add**.

Figure 312. Configure Logging tab and add rule



Add Rule

Name: FMC Incoming
☑ Enabled
Insert: into Category | Administrator Rules
Action: Do not decrypt

☑ Log at End of Connection

Send Connection Events to:
☑ Event Viewer
☐ Syslog: Select a Syslog Alert Configuration...
☐ SNMP Trap: Select an SNMP Alert Configuration...

Though the above two rules should allow communication to and from the FMC to not be decrypted it appears there is a flaw in the order of operations somewhere "behind the scenes" within the FTD packet flow. I say this because there is a particular situation where communication with the FMC does not match either of these rules. In this lab we have an instance of this situation. The communication between the remote2-ftd and the FMC.

While this SSL policy is active (associated with an Access Control policy) any new SSL communications between remote2-ftd and the FMC (or vice versa) will fail. The existing connection will continue to work but if that connection is severed, for example, if you were to reboot remote2-ftd, the attempts to establish a new connection will fail. The only way to recover that connection is to disable the SSL policy, let remote2-ftd and FMC establish a connection, and then re-enable the SSL policy.

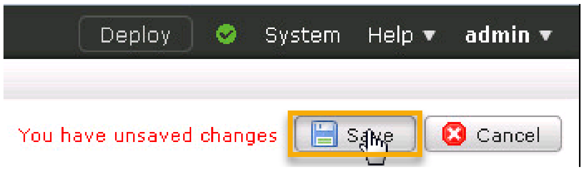
This situation appears not to affect the communication between remote1-ftd and the FMC which, to me, indicates this is a directional problem since the remote1-ftd is the “initiator” of the management connection to the FMC whereas remote2-ftd is the “responder” to the same type of connection.

Update! A student in one of the classes found a “work around” to this problem. To get the remote2-ftd session to work again, without removing the SSL Policy and re-adding it, he created a Prefilter Policy to identify this traffic and “fastpath” it through instead of relying on the SSL Policy “Don’t Decrypt” action. Though this works it isn’t optimal, since using a Prefilter Policy also skips a bunch of other Policies. So, if you HAVE to do it this way be sure to be as specific in your match criteria as possible to avoid any unexpected results.

Notice the other tabs in the Policy editor: Trusted CA Certificates and Undecryptable Actions. You won’t be doing anything with these today but they give you the ability to take further actions regarding this Policy.

27. Click **Save**.

Figure 313. Save changes to FMC



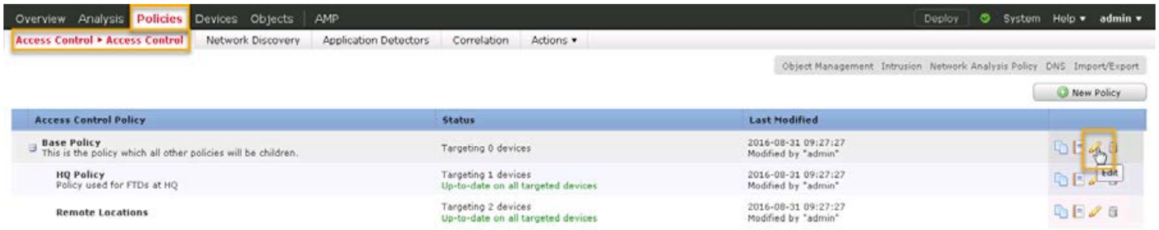
You have unsaved changes

Now that the SSL Policy has been created (and it has rules) it is time to associate it with an Access Control Policy. Since you want this SSL Policy to be applied to all Example Corp locations you need to associate it with the Base Policy.

28. Navigate to **Policies > Access Control > Access Control**.

29. **Edit** the **Base Policy**.

Figure 314. Edit Base Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-31 09:27:27 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-31 09:27:27 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-08-31 09:27:27 Modified by "admin"

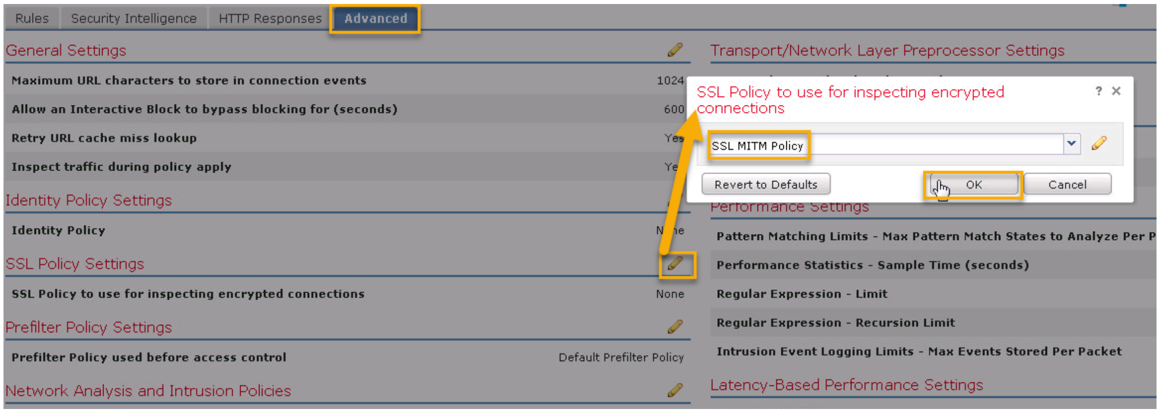
30. Click the **Advanced tab**.

31. Click the **pencil icon** next to the **SSL Policy Settings**.

    a. In the popup window **select** the **SSL MITM Policy** you just created.

    b. Click **OK**.

Figure 315. Apply SSL Policy to ACP



General Settings

Maximum URL characters to store in connection events 1024

Allow an Interactive Block to bypass blocking for (seconds) 600

Retry URL cache miss lookup Yes

Inspect traffic during policy apply Yes

Identity Policy Settings

Identity Policy None

SSL Policy Settings

SSL Policy to use for inspecting encrypted connections None

Prefilter Policy Settings

Prefilter Policy used before access control Default Prefilter Policy

Network Analysis and Intrusion Policies

Transport/Network Layer Preprocessor Settings

SSL Policy to use for inspecting encrypted connections

SSL MITM Policy

Performance Settings

Pattern Matching Limits - Max Pattern Match States to Analyze Per P

Performance Statistics - Sample Time (seconds)

Regular Expression - Limit

Regular Expression - Recursion Limit

Intrusion Event Logging Limits - Max Events Stored Per Packet

Latency-Based Performance Settings

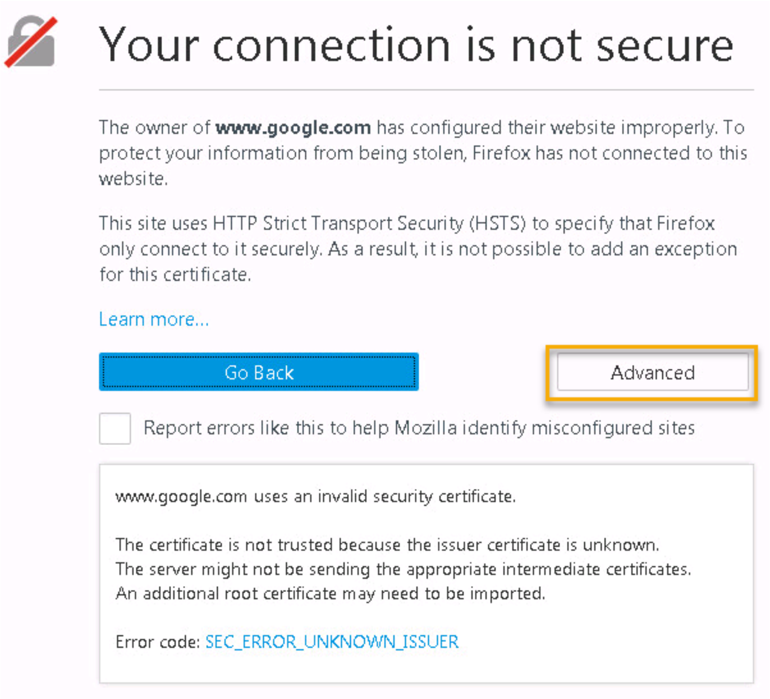
32. Click **Save** and then **Deploy**. Select **all the FTD devices** and click **Deploy**.

Browser Test – Phase 1

Now that the FMC has deployed the SSL Policy to the FTD devices, it is time to test.

33. On **hq-wkst,** open a new tab in **Firefox** and attempt to browse to **the Google home page**. Notice that a Certificate warning notice appears AND there is no way to Accept and Continue.

Figure 316. Can't accept the cert



Your connection is not secure

The owner of **www.google.com** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

This site uses HTTP Strict Transport Security (HSTS) to specify that Firefox only connect to it securely. As a result, it is not possible to add an exception for this certificate.

Learn more...

□ Report errors like this to help Mozilla identify misconfigured sites

www.google.com uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: SEC_ERROR_UNKNOWN_ISSUER

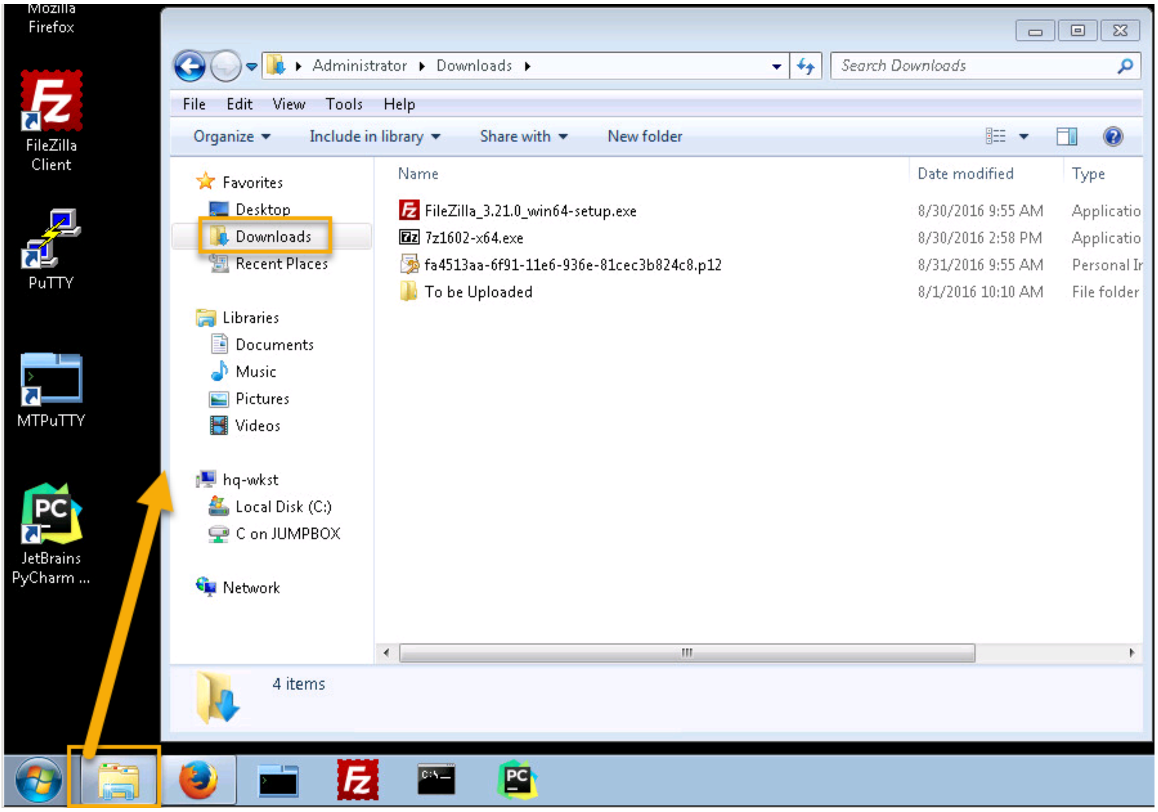
Right now the FTD device has decrypted the Google home page connection and then re-encrypted it using the FMC_AS_A_CA certificate. That Certificate Authority (the FMC) is not trusted by this computer nor the Firefox browser. This is the whole point of the certificate chain of trust. To stop “evildoers” from performing a MiTM attack and stealing your “encrypted” information.

Install FMC CA Certificate into hq-wkst

You need to install the FMC's CA Certificate as a trusted CA into the computer and then install the certificate into Firefox so that you can allow the FTD devices to be MiTM "attackers".

34. On **hq-wkst** open up **Windows Explorer** and navigate to the **Downloads** directory. (This is where you saved a copy of the CA certificate when you created the FMC CA.)

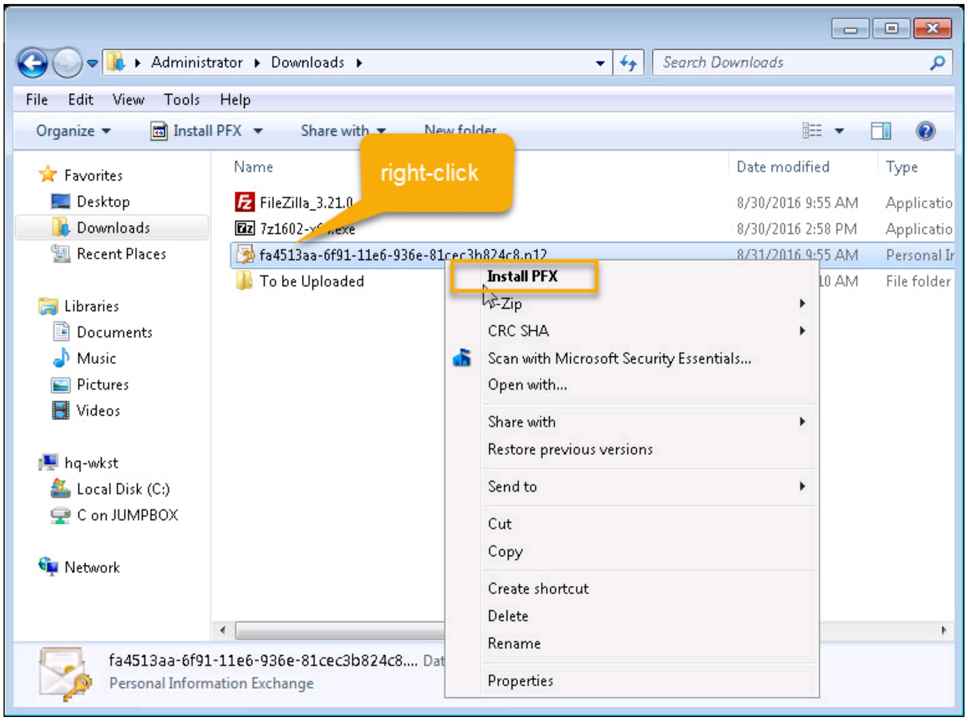
Figure 317. Go to Download directory



Name	Date modified	Type
FileZilla_3.21.0_win64-setup.exe	8/30/2016 9:55 AM	Applicatio
7z1602-x64.exe	8/30/2016 2:58 PM	Applicatio
fa4513aa-6f91-11e6-936e-81cec3b824c8.p12	8/31/2016 9:55 AM	Personal Ir
To be Uploaded	8/1/2016 10:10 AM	File folder

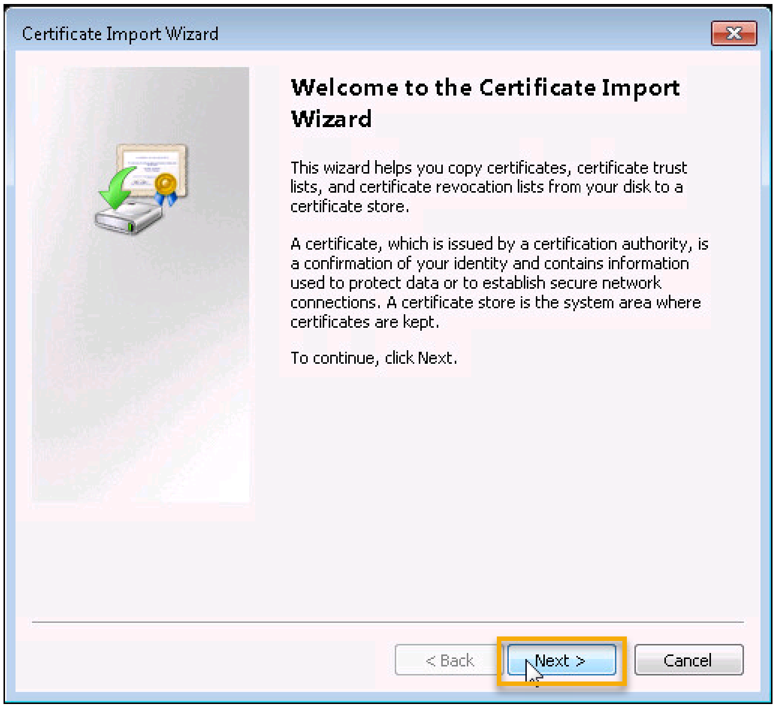
35. **Right-click** on the file and select **Install PFX**.

Figure 318. Install PFX



36. The Certificate Import Wizard will appear. Click **Next**.

Figure 319. Certificate Import Wizard Page 1



Welcome to the Certificate Import Wizard

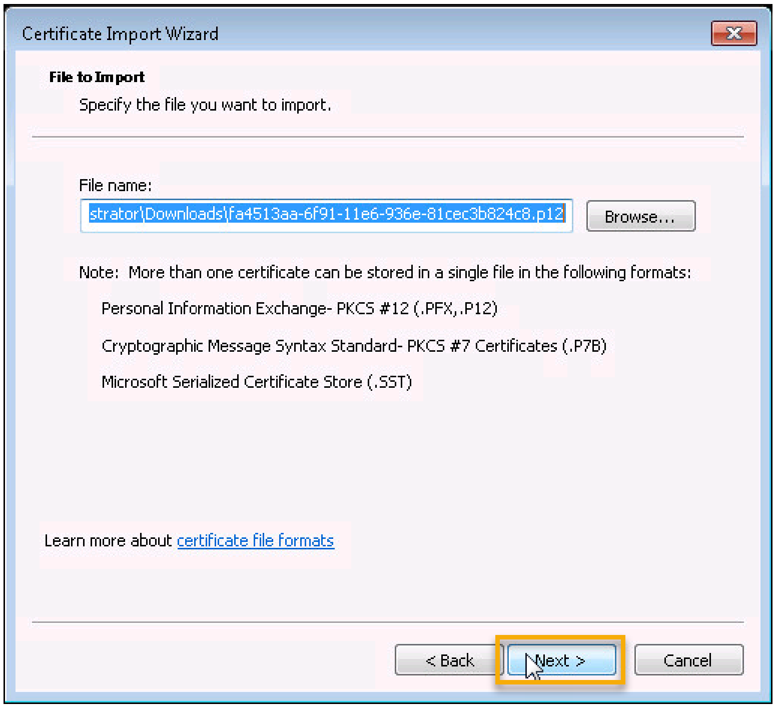
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

To continue, click Next.

37. The File to Import is already populated with your filename. Click **Next**.

Figure 320. Certificate Import Wizard Page 2



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

strator\Downloads\fa4513aa-6f91-11e6-936e-81cec3b824c8.p12

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

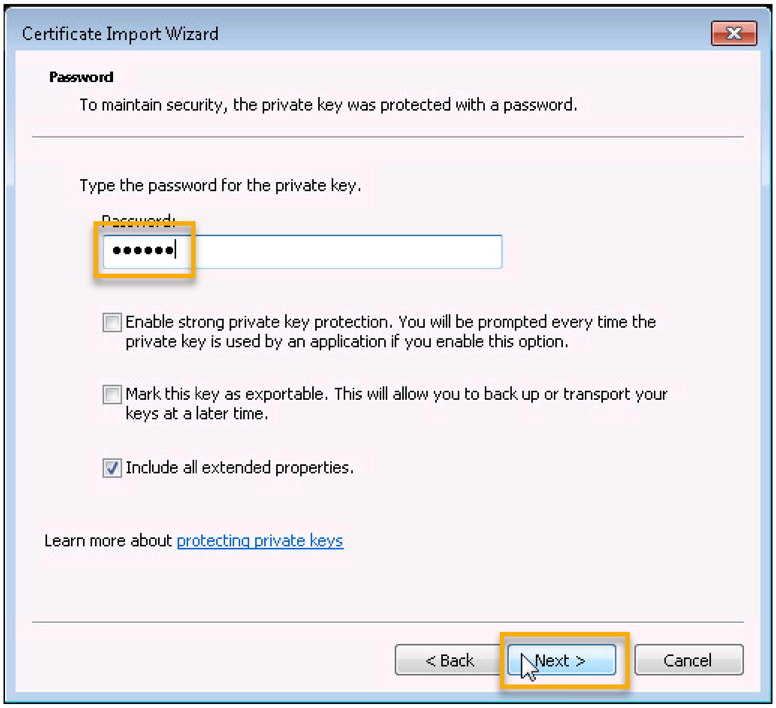
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

38. Type in the password **abc123** to decrypt the certificate. Click **Next**.

Figure 321. Certificate Import Wizard Page 3



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

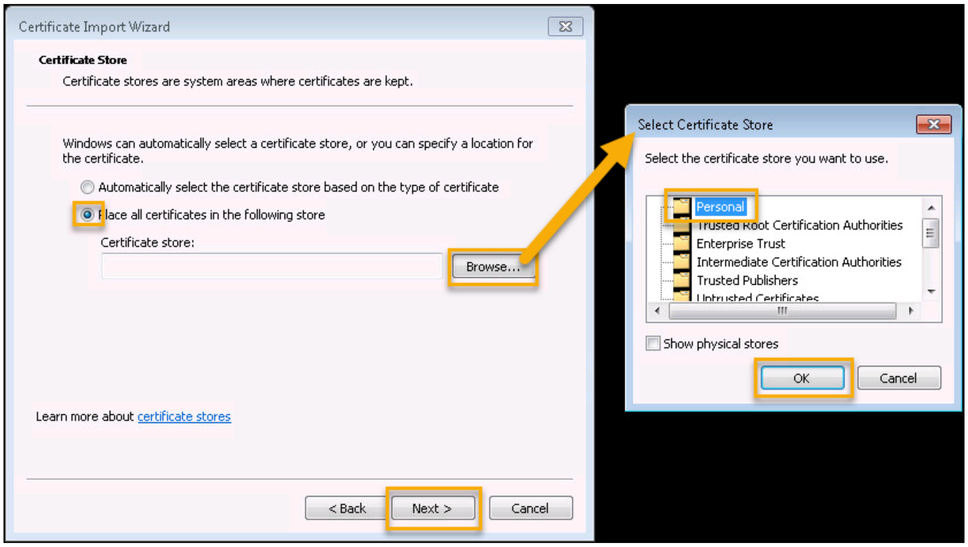
□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

39. Select the **Place all certificates in the following store**, click **Browse**, and select the **Personal folder**. Click **OK** and then click **Next**.

Figure 322. Certificate Import Wizard Page 4



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:

Learn more about certificate stores

Select Certificate Store

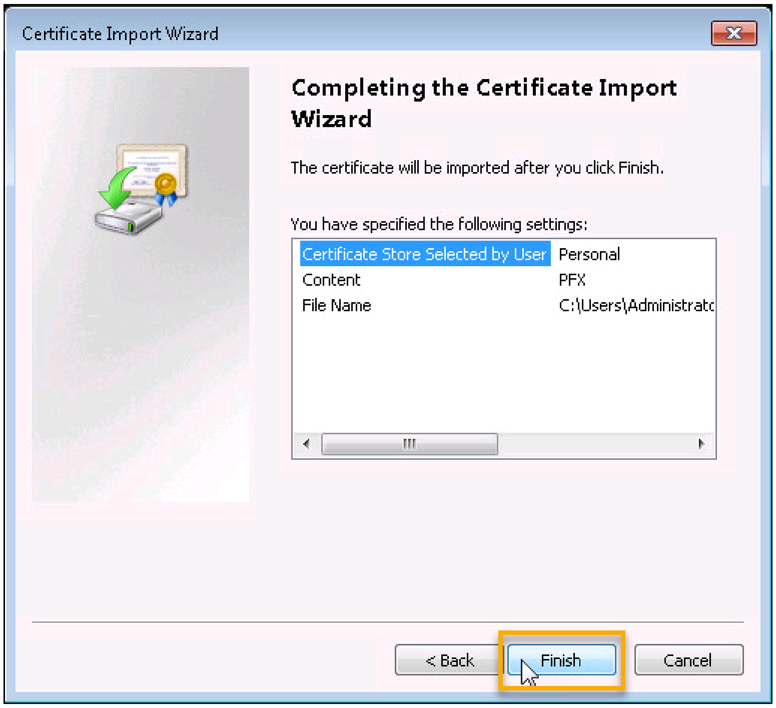
Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

40. Click **Finish** to import the certificate.

Figure 323. Certificate Import Wizard Page 5



Certificate Import Wizard

Completing the Certificate Import Wizard

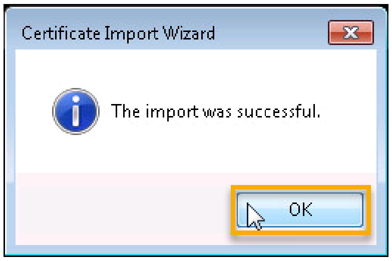
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\Administratc

41. Click **OK** to the Import Successful message.

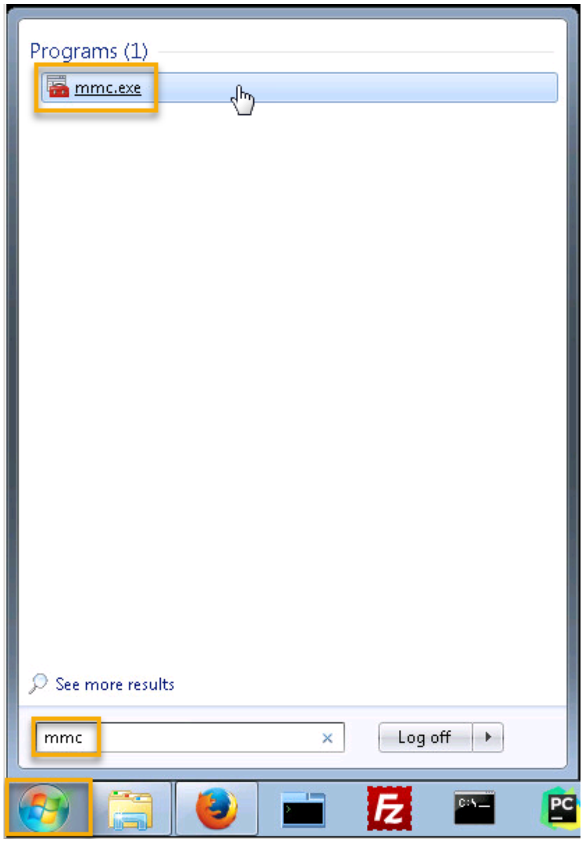
Figure 324. Confirm your success



Now that the certificate is installed you need to export a public cert from it to install into your browser:

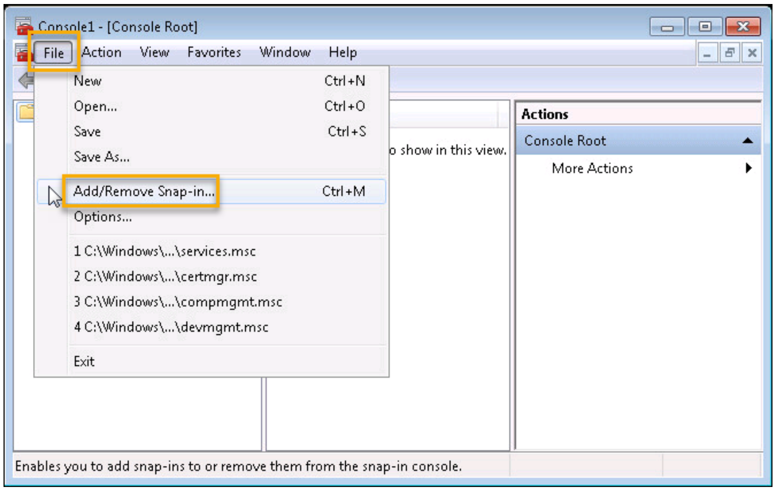
42. Click on **Start** and in the Search box type **mmc**. Click on the **mmc.exe** program that the search finds.

Figure 325. Launch mmc.exe



43. In the Console1 window click **File > Add/Remove Snap-in**.

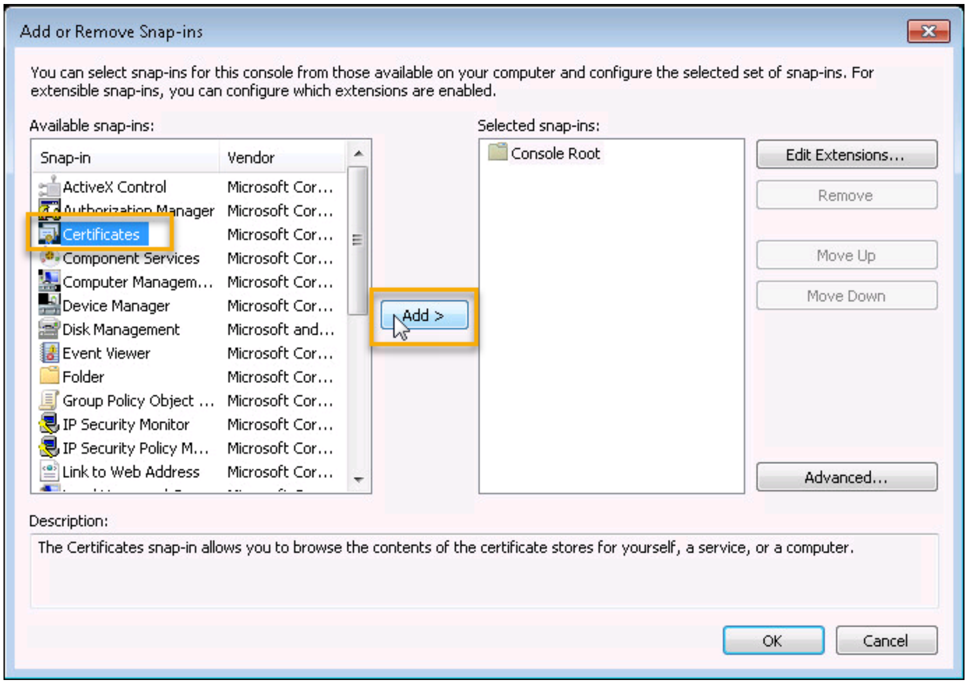
Figure 326. Add snap-in


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\...\services.msc
2 C:\Windows\...\certmgr.msc
3 C:\Windows\...\compmgmt.msc
4 C:\Windows\...\devmgmt.msc
Exit
o show in this view.
Actions
Console Root
More Actions

Enables you to add snap-ins to or remove them from the snap-in console.

44. From the left column select **Certificates** and click **Add>**.

Figure 327. Add Certificates console



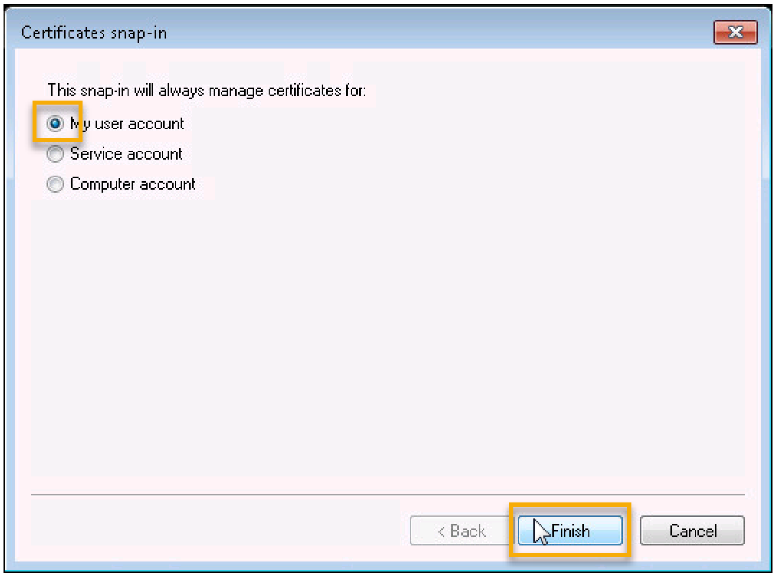
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

45. In the subsequent popup window select the **My user account** and click **Finish**.

Figure 328. Add Certificates console



Certificates snap-in

This snap-in will always manage certificates for:

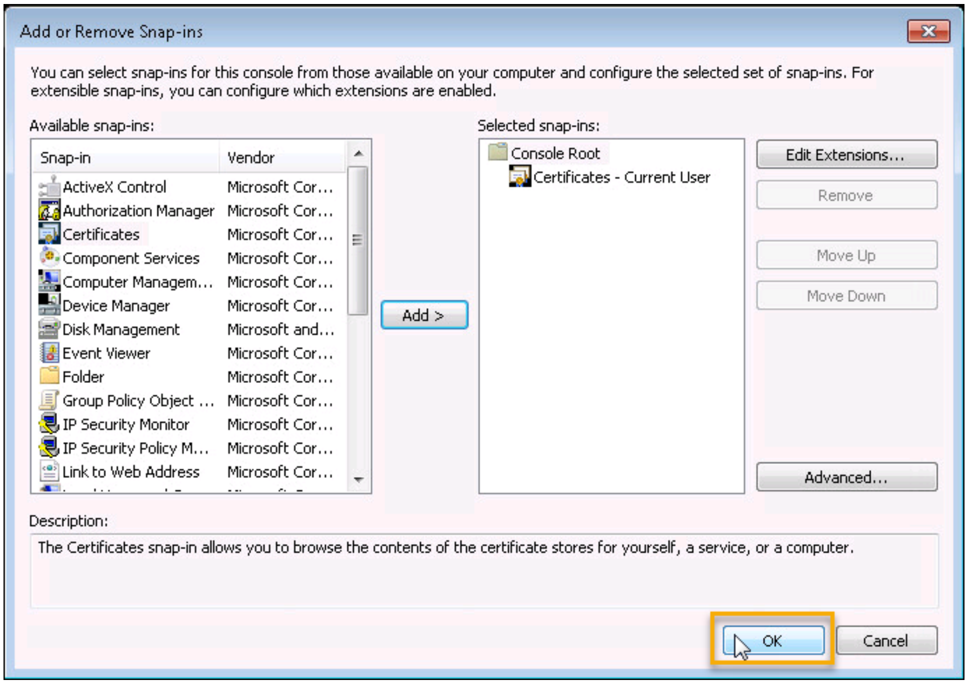
● My user account

○ Service account

○ Computer account

46. Click **OK**.

Figure 329. Click OK



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

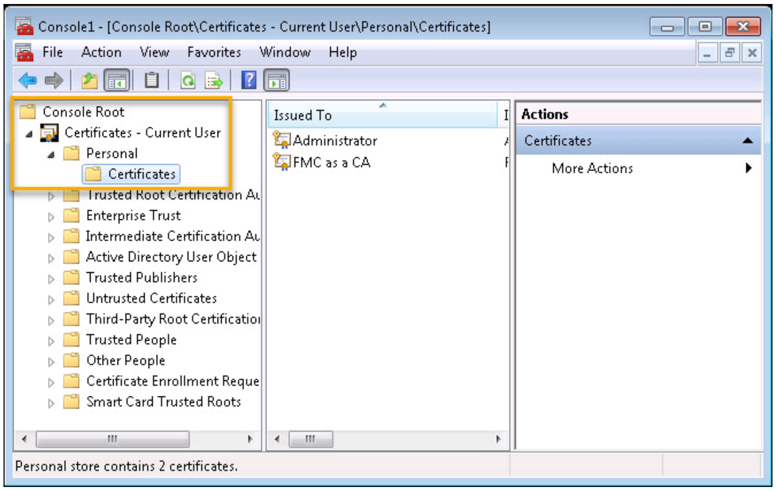
- Console Root
  - Certificates - Current User

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

47. Now that the Certificates snap-in has been added, from the left column list of folders drill down to **Console Root > Certificates – Current User > Personal > Certificates** and the right column will populate. The FMC CA certificate should be listed there.

Figure 330. Navigate to Certificates


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Other People
Certificate Enrollment Reque
Smart Card Trusted Roots
Issued To
Administrator
FMC as a CA
Actions
Certificates
More Actions

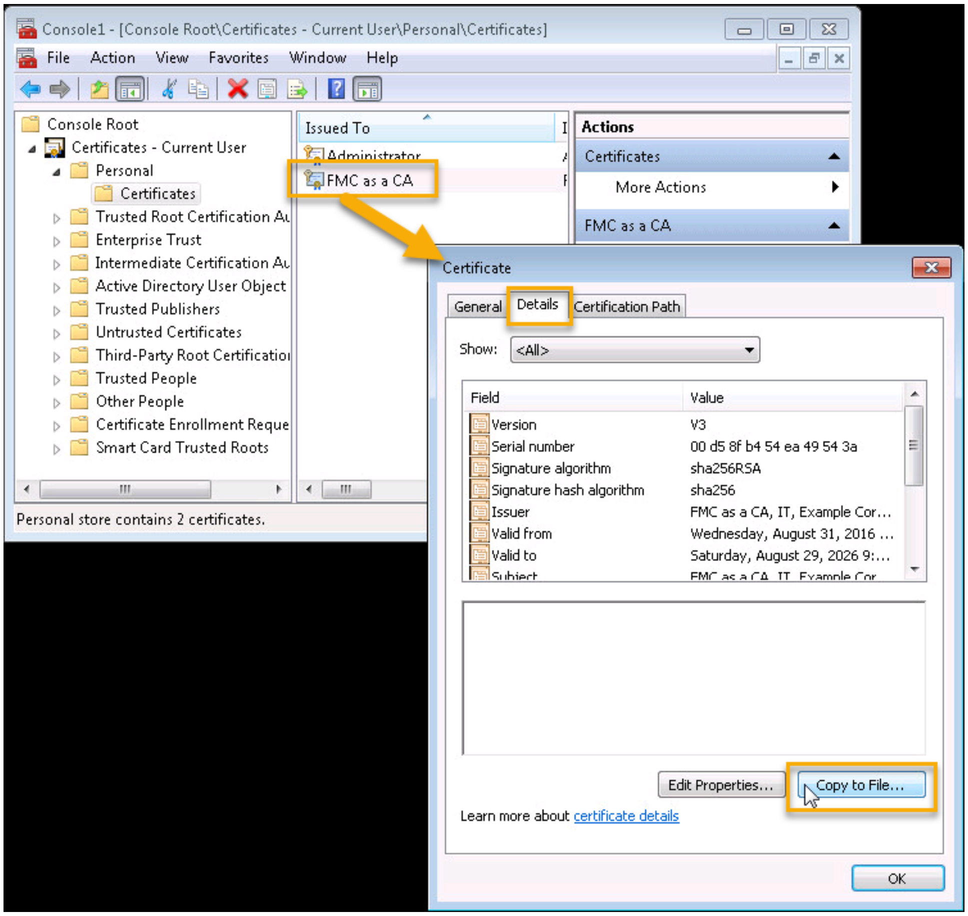
Personal store contains 2 certificates.

48. **Double-click** the **FMC as a CA** certificate.

49. Click the **Details tab**.

50. Click the **Copy to File** button.

Figure 331. Prepare to export



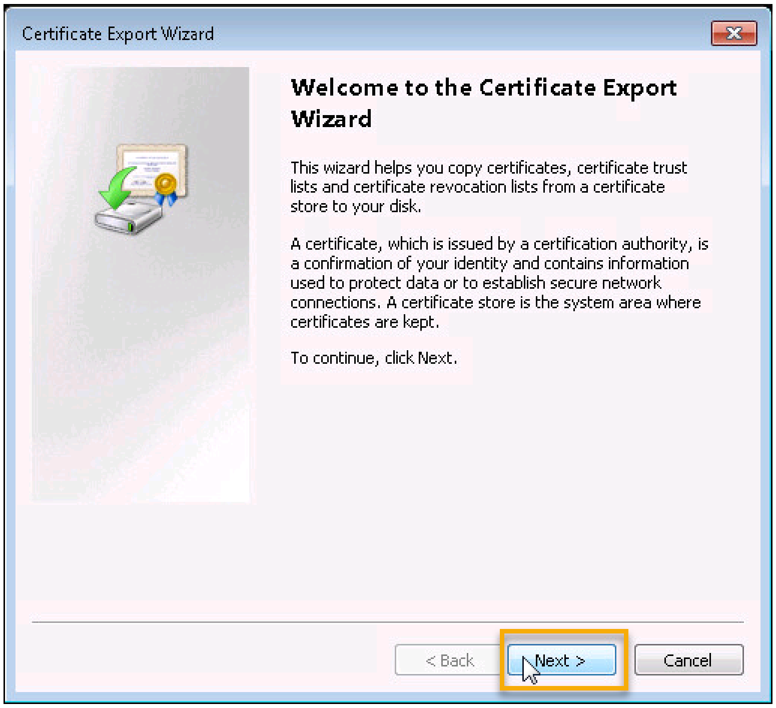
Personal store contains 2 certificates.

Field	Value
Version	V3
Serial number	00 d5 8f b4 54 ea 49 54 3a
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	FMC as a CA, IT, Example Cor...
Valid from	Wednesday, August 31, 2016 ...
Valid to	Saturday, August 29, 2026 9:...
Subject	FMC as a CA, IT, Example Cor

Learn more about certificate details

51. In the Certificate Export Wizard click **Next**.

Figure 332. Export Cert Page 1



Certificate Export Wizard

Welcome to the Certificate Export Wizard

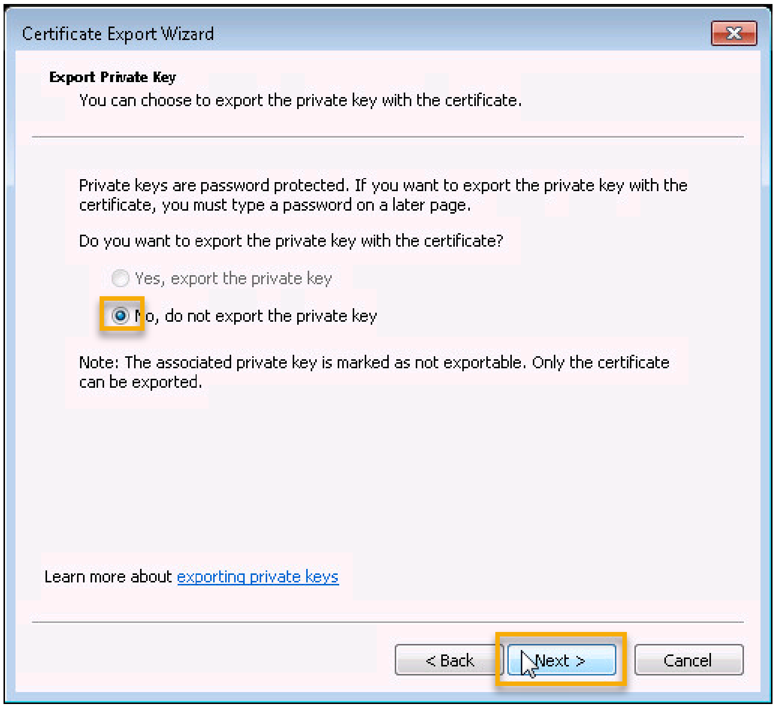
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

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.

To continue, click Next.

52. Ensure that the **No, do not export the private key** radio button is selected and click **Next**.

Figure 333. Export Cert Page 2



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

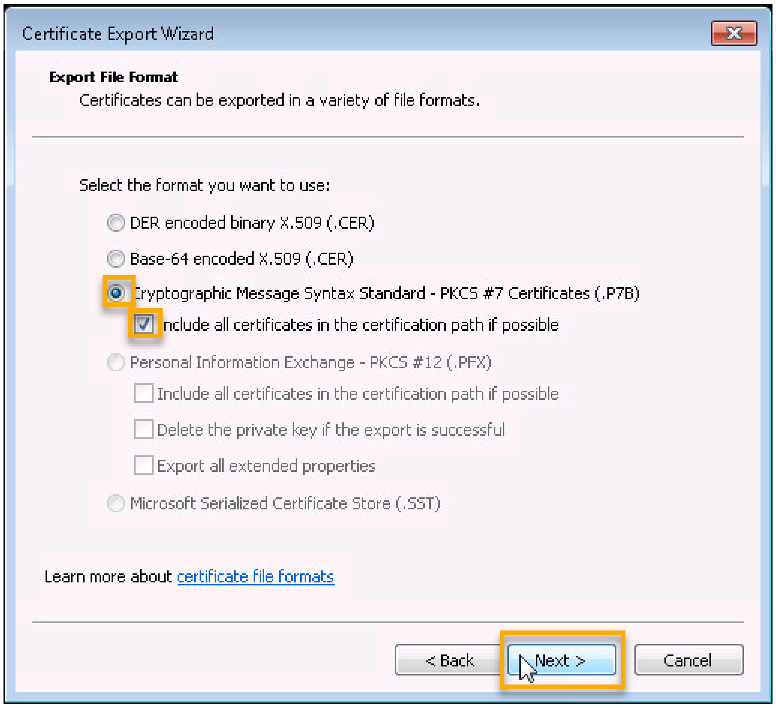
Note: The associated private key is marked as not exportable. Only the certificate can be exported.

Learn more about exporting private keys

53. Any of the file formats will do. I selected the **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)** option along with checking the **Include all certificates in the certification path if possible** box.

54. Click **Next**.

Figure 334. Export Cert Page 3



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☑ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

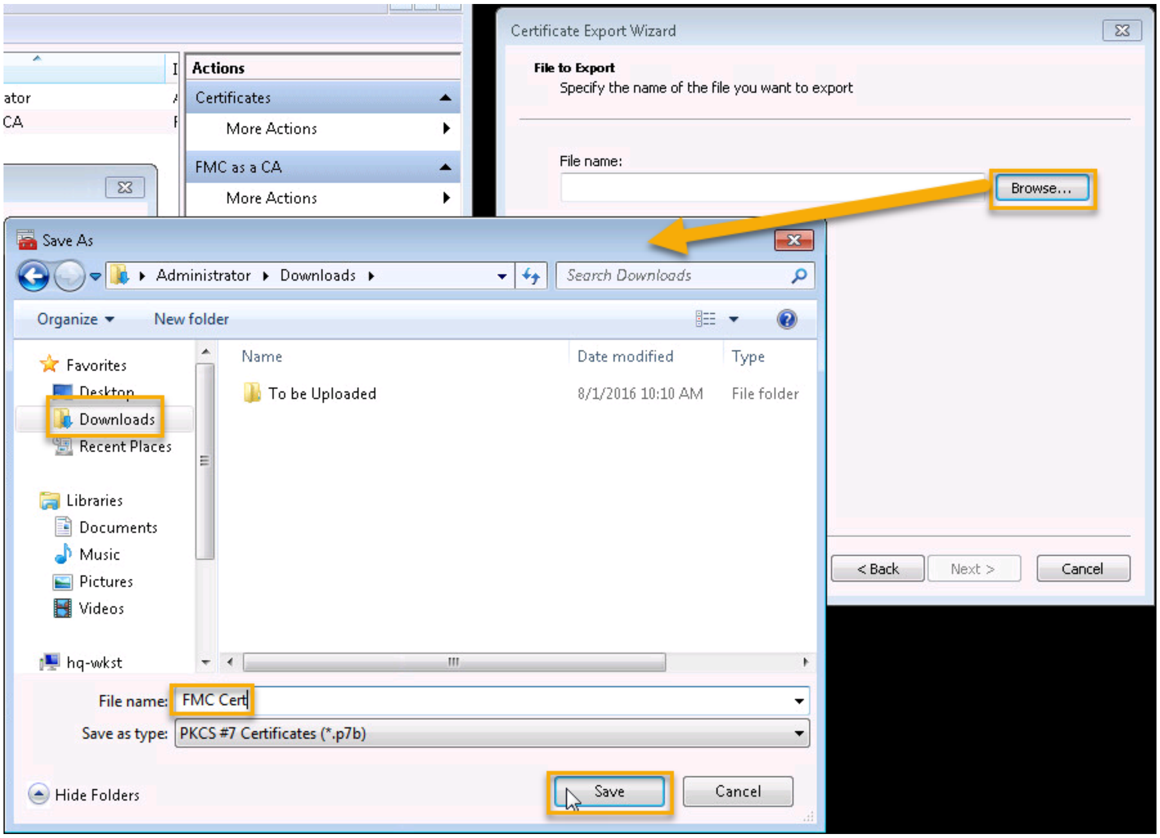
□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

55. Click **Browse…** and select the **Downloads** folder. Use **FMC Cert** for the File name. Click **Save**.

Figure 335. Export Cert Page 4



Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

Save As

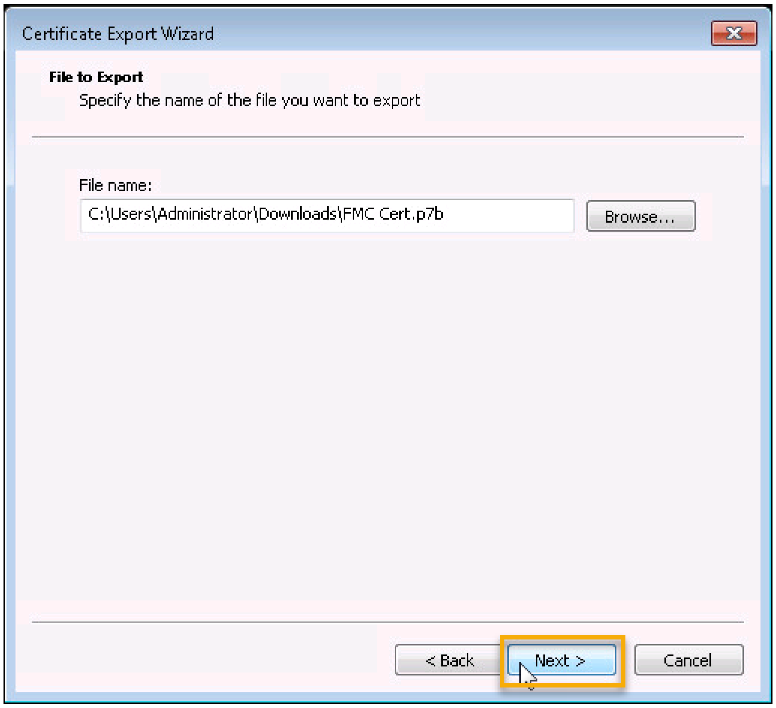
File name: FMC Cert

Save as type: PKCS #7 Certificates (*.p7b)

Name	Date modified	Type
To be Uploaded	8/1/2016 10:10 AM	File folder

56. Click **Next**.

Figure 336. Export Cert Page 5



Certificate Export Wizard

File to Export

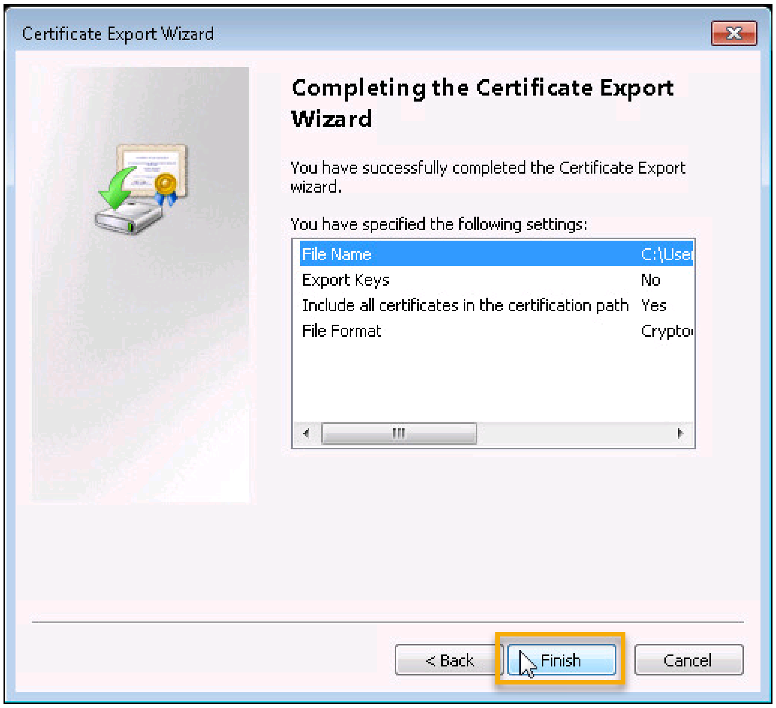
Specify the name of the file you want to export

File name:

C:\Users\Administrator\Downloads\FMC Cert.p7b

57. Click **Finish**

Figure 337. Export Cert Page 6



Certificate Export Wizard

Completing the Certificate Export Wizard

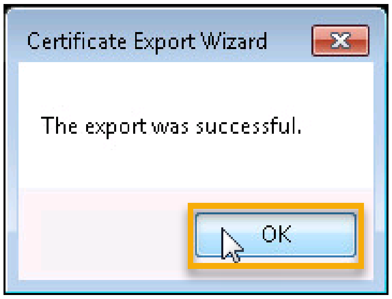
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Use
Export Keys	No
Include all certificates in the certification path	Yes
File Format	Crypto

58. Click **OK** on the Certificate Export Wizard popup window.

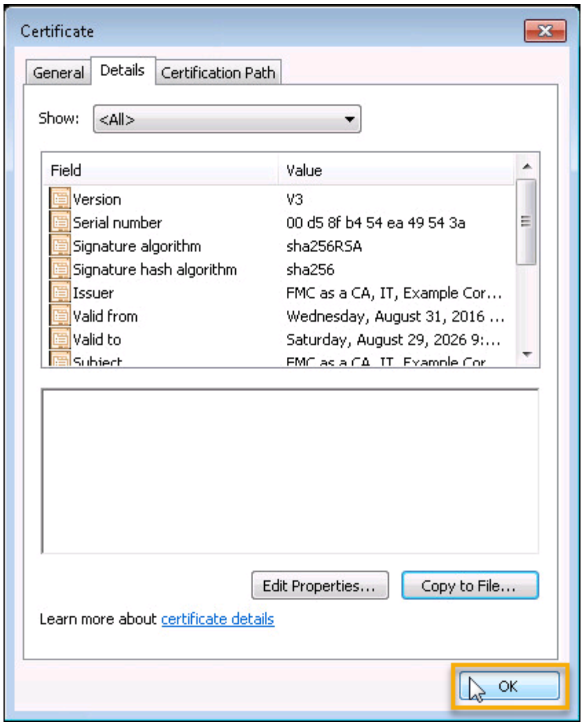
Figure 338. Click OK



The export was successful.

59. Click **OK** on the Certificate window.

Figure 339. Click OK



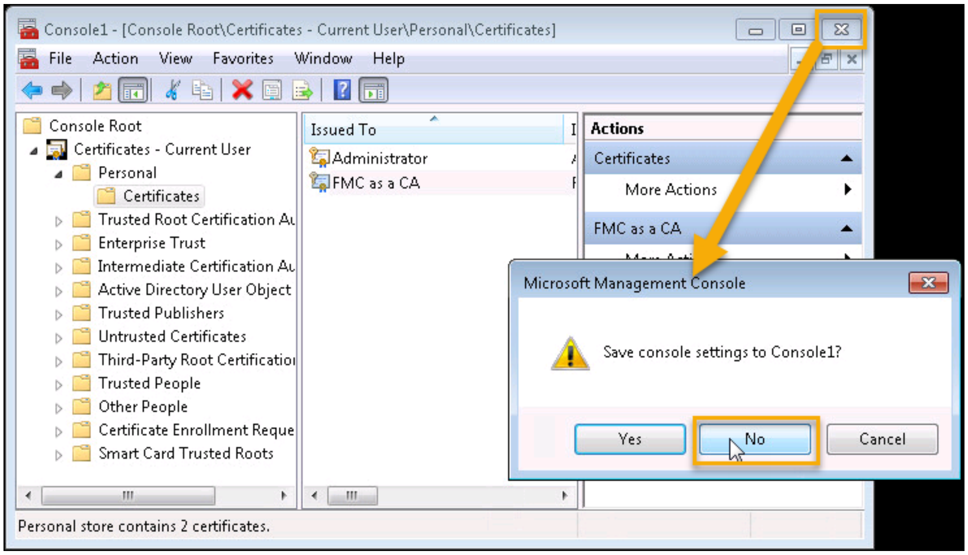
Show: <All>

Field	Value
Version	V3
Serial number	00 d5 8f b4 54 ea 49 54 3a
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	FMC as a CA, IT, Example Cor...
Valid from	Wednesday, August 31, 2016 ...
Valid to	Saturday, August 29, 2026 9:...
Subject	FMC as a CA, IT, Example Cor

Learn more about certificate details

60. **Close** the Console1 window. You don't need to save changes.

Figure 340. Close Console1



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Microsoft Management Console

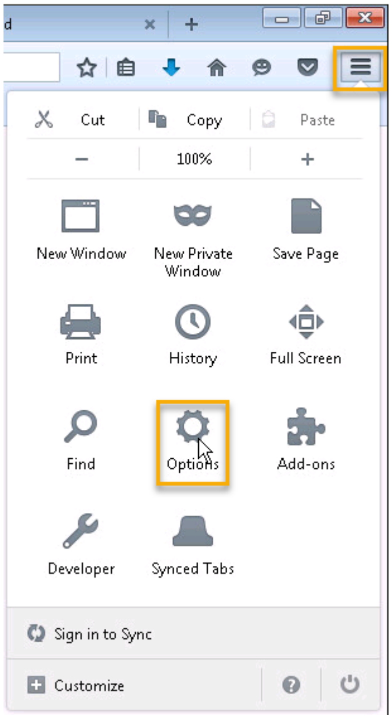
Save console settings to Console1?

Time to trust the FMC as a Certificate Authority within the Firefox browser.

61. Open **Firefox** and click the **hamburger menu**.

62. Select the **Options** item.

Figure 341. Open Firefox Options menu

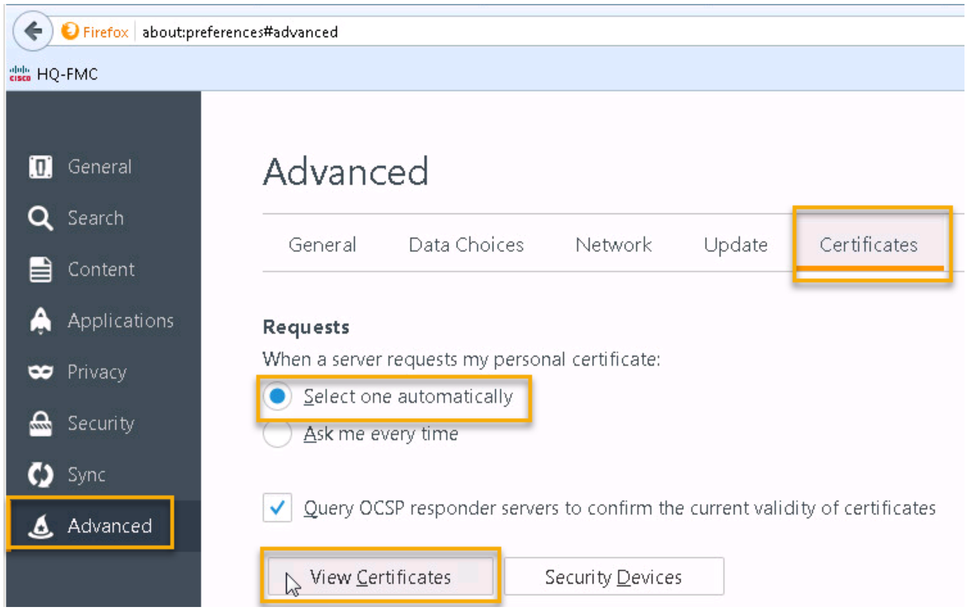


63. From the left side column of items select **Advanced** and then click **Certificates**.

64. Check the **Select one automatically** radio button.

65. Click the **View Certificates** button.

Figure 342. View Certificates



Advanced

Requests

When a server requests my personal certificate:

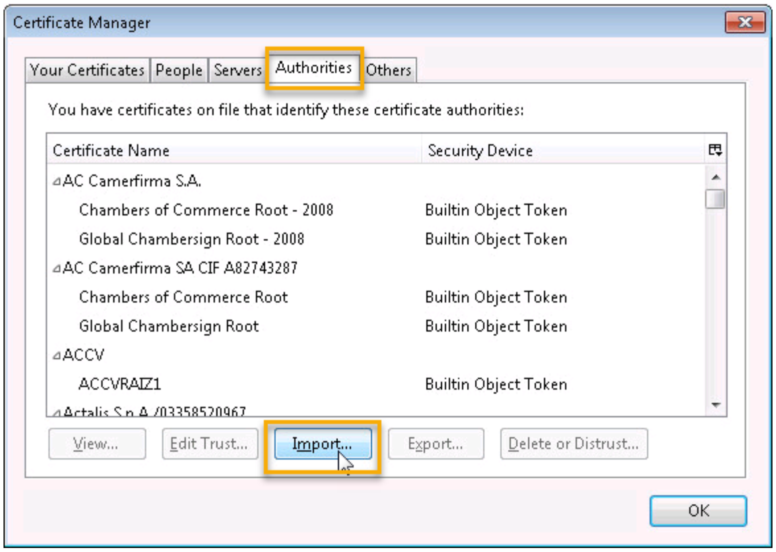
● Select one automatically

○ Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

66. Click the **Authorities tab** and then click the **Import** button.

Figure 343. Prepare to Import CA



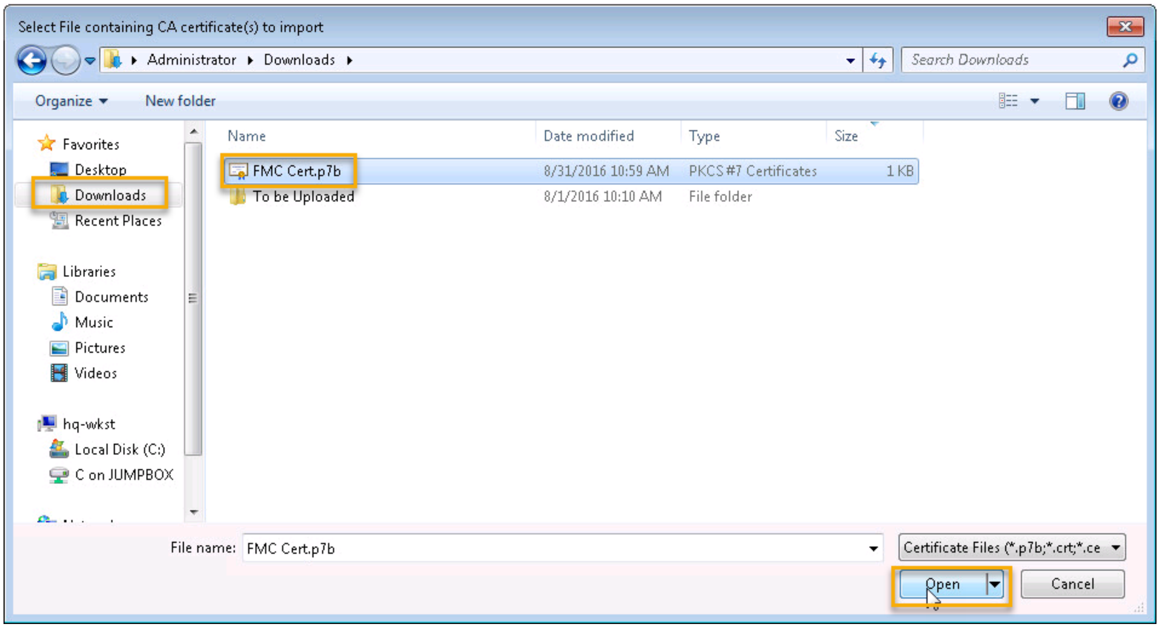
You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
⊿AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⊿AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
⊿ACCV	
ACCVRAIZ1	Builtin Object Token
⊿Actalis S.p.A./03358520967	

67. Browse to the Downloads folder and select the **FMC Cert.p7b** file. You may need to change the file filter option in the lower right corner of the Certificate to Import explorer window.

68. Click **Open**.

Figure 344. Select FMC CA Cert



Select File containing CA certificate(s) to import

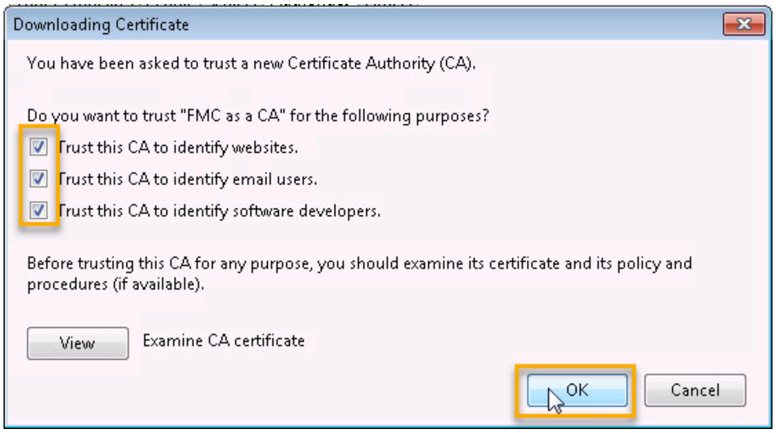
Name	Date modified	Type	Size
FMC Cert.p7b	8/31/2016 10:59 AM	PKCS #7 Certificates	1 KB
To be Uploaded	8/1/2016 10:10 AM	File folder	

File name: FMC Cert.p7b

Certificate Files (*.p7b;*.crt;*.ce

69. A popup window will ask when the FMC as a CA certificate should be trusted. Check **all the boxes** and then click **OK**.

Figure 345. Fully trust CA



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "FMC as a CA" for the following purposes?

☑ Trust this CA to identify websites.

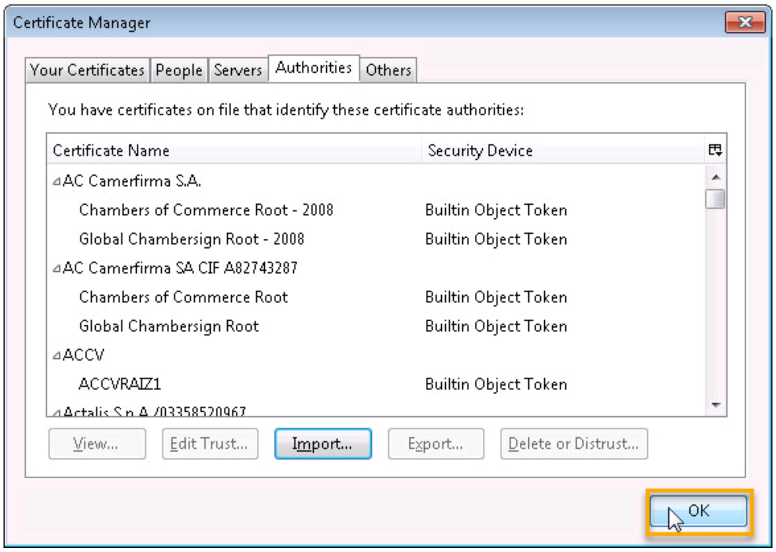
☑ Trust this CA to identify email users.

☑ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

70. Click **OK** on the Certificate Manager window to close it.

Figure 346. Click OK



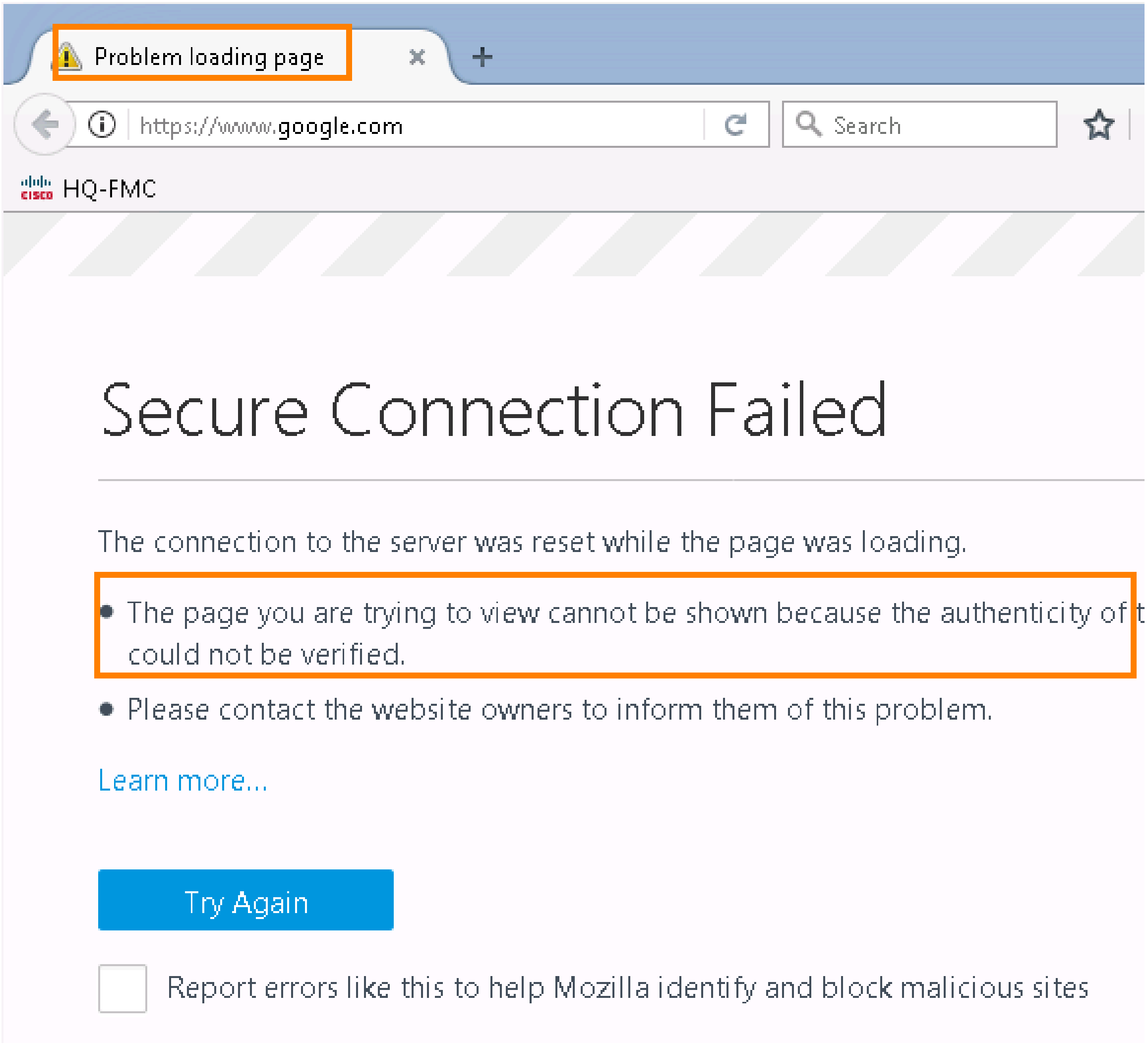
You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
⊿AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⊿AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
⊿ACCV	
ACCVRAIZ1	Builtin Object Token
⊿Actalis S.p.A./03358520967	

Browser Test – Phase 2

71. In the previous version of this lab just refreshing the page for https://www.google.com would work. Whether Google and/or Firefox has made changes this **no longer works**.

Figure 347. Google doesn't work in Firefox.



Secure Connection Failed

The connection to the server was reset while the page was loading.

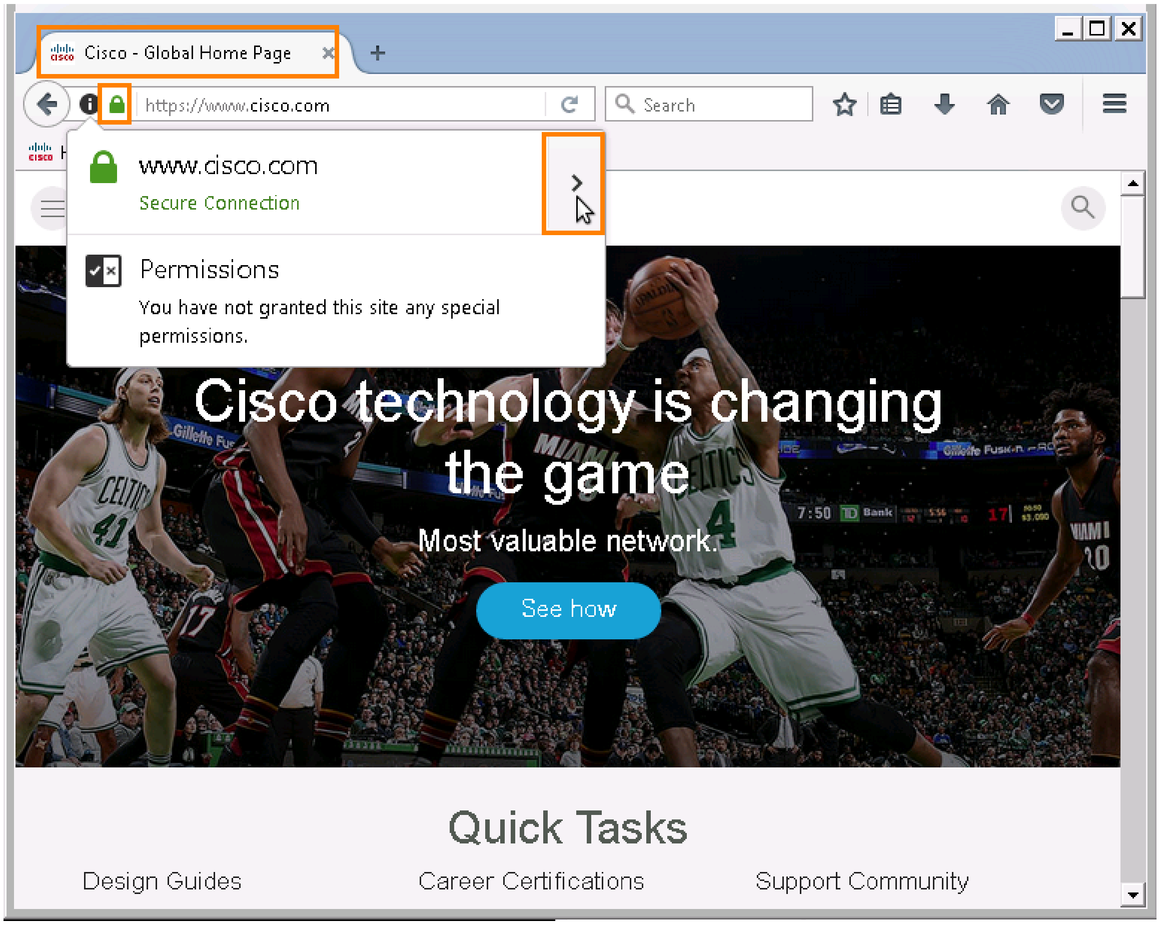
- The page you are trying to view cannot be shown because the authenticity of t could not be verified.
- Please contact the website owners to inform them of this problem.

□ Report errors like this to help Mozilla identify and block malicious sites

If you want to view https://www.google.com open up Internet Explorer.

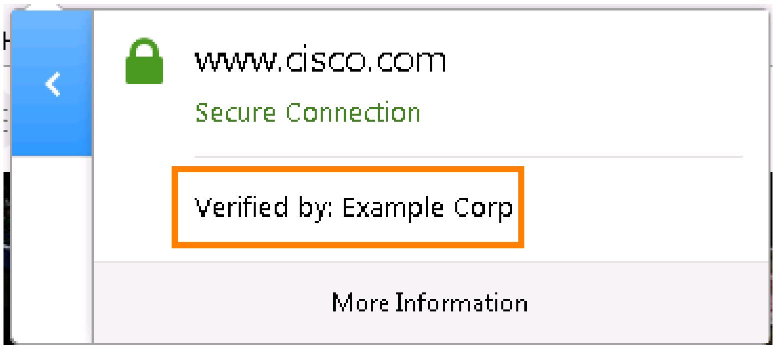
72. Instead, connect to **https://www.cisco.com**. Click the **green lock** icon and then the **greater than** sign.

Figure 348. https://www.cisco.com



73. Notice that this site was verified by Example Corp. This is because we "Trust" the certificate issued by the FMC.

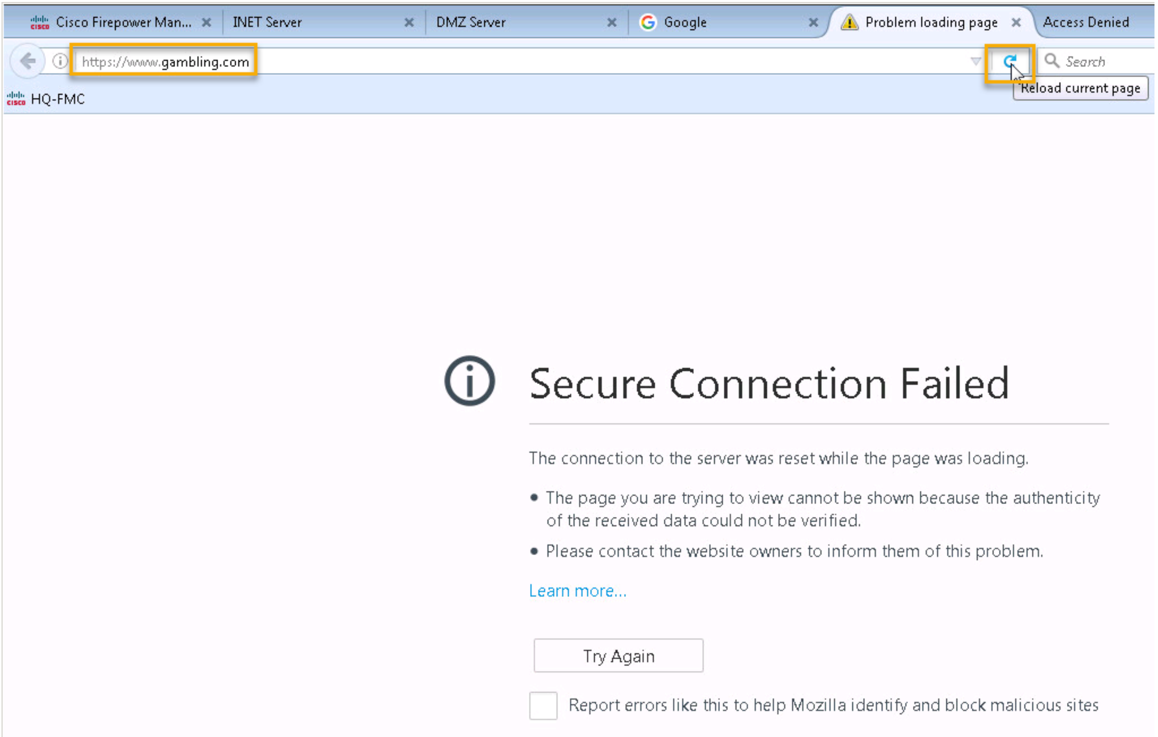
Figure 349. In Example Corp we Trust



Verified by: Example Corp

Figure 350. SAttempt to access **www.gambling.com**. Instead of just timing out, the web page will immediately end. You still don't get the "system-default" HTTP response page but at least it ends quickly.

Figure 351. No Gambling for you!!!



Secure Connection Failed

The connection to the server was reset while the page was loading.

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more...

Try Again

□ Report errors like this to help Mozilla identify and block malicious sites

Note: This page will take FOREVER to finally time out. Either wait for it or come back later to see this message.

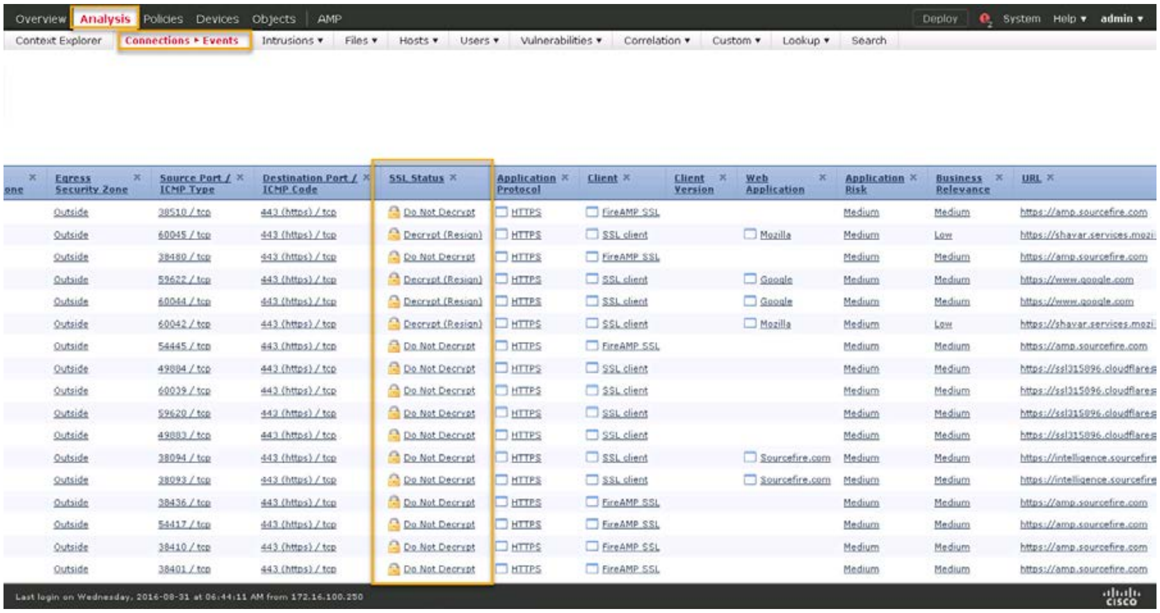
The reason www.gambling.com now behaves differently is that the SSL decryption engine resides in SNORT. So, when the initial encrypted packet comes in the ASA process recognizes it and "punts" it to the SNORT process for decryption. Once the decryption is done, the un-encrypted packet is then resent through the Access Control Policies, and this time it is recognized for having Gambling content. This means that it gets blocked but since it didn't come from the HTTP protocol the HTTP Response option isn't applied.

Analyze the Results

Now that you have successfully created a man-in-the-middle “hack” so that you can see the contents of an encrypted SSL connection let’s see what the logs show.

74. In the FMC, navigate to **Analysis > Connections > Events**.
75. In the Application Protocol column, click on the **HTTPS** of any row to drill down to looking at only HTTPS related events.
76. In the resulting list look around (you’ll probably have to scroll to the right) until you find the **SSL Status** column and where is says Decrypt (Resign). These rows were where the MITM hack was used so that the FTD could inspect the “encrypted” traffic.

Figure 352. See SSL Status column



one	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	Application Protocol	Client	Client Version	Web Application	Application Risk	Business Relevance	URL
	Outside	38510 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	FireAMP SSL			Medium	Medium	https://amp.sourcefire.com
	Outside	60045 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTPS	SSL client		Mozilla	Medium	Low	https://shavar.services.mozi
	Outside	38480 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	FireAMP SSL			Medium	Medium	https://amp.sourcefire.com
	Outside	59622 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTPS	SSL client		Google	Medium	Medium	https://www.google.com
	Outside	60044 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTPS	SSL client		Google	Medium	Medium	https://www.google.com
	Outside	60042 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTPS	SSL client		Mozilla	Medium	Low	https://shavar.services.mozi
	Outside	54445 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	FireAMP SSL			Medium	Medium	https://amp.sourcefire.com
	Outside	49884 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client			Medium	Medium	https://ssl315896.cloudflares
	Outside	60039 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client			Medium	Medium	https://ssl315896.cloudflares
	Outside	59620 / tcp	442 (https) / tcp	Do Not Decrypt	HTTPS	SSL client			Medium	Medium	https://ssl315896.cloudflares
	Outside	49883 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client			Medium	Medium	https://ssl315896.cloudflares
	Outside	38094 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client		Sourcefire.com	Medium	Medium	https://intelligence.sourcefire
	Outside	38093 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client		Sourcefire.com	Medium	Medium	https://intelligence.sourcefire
	Outside	38436 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	FireAMP SSL			Medium	Medium	https://amp.sourcefire.com
	Outside	54417 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	FireAMP SSL			Medium	Medium	https://amp.sourcefire.com
	Outside	38410 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	FireAMP SSL			Medium	Medium	https://amp.sourcefire.com
	Outside	38401 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	FireAMP SSL			Medium	Medium	https://amp.sourcefire.com

Last login on Wednesday, 2016-08-31 at 06:44:11 AM from 172.16.100.250

Scenario Summary

As you can see there are a lot of steps in setting up the use of an SSL Policy. The “chain of trust” must be met which means modifying configurations on the client workstations too. Granted most (if not all) of this could be done through some sort of group policy it doesn’t account for non-corporate asset devices that need Internet access (not to mention other possible devices, like IoT devices, that you might not be able to modify their authorities they trust).

Care must be taken when using the SSL decryption inspection policies. Not only does it have a huge processing impact on the FTD devices there is also the concern of privacy. For example, what if an Example Corp employee logs into their private banking website. Should that be decrypted? What if their banking information got hacked, is it possible that Example Corp be held responsible since they “could” have gather their employee’s credentials? This scenario is not a recommendation on how to deploy an SSL Policy but just an example of what “could” be done.

Until the hardware SSL decryption are available on the FTD hardware appliances expect about an 20% decrease in performance to the published maximum number of connections through an FTD device. Obviously there are no hardware SSL decryption engines available for the virtual FTDs.

Page intentionally left blank.

Scenario 8. Malware and File Detection Configuration

Scenario Description

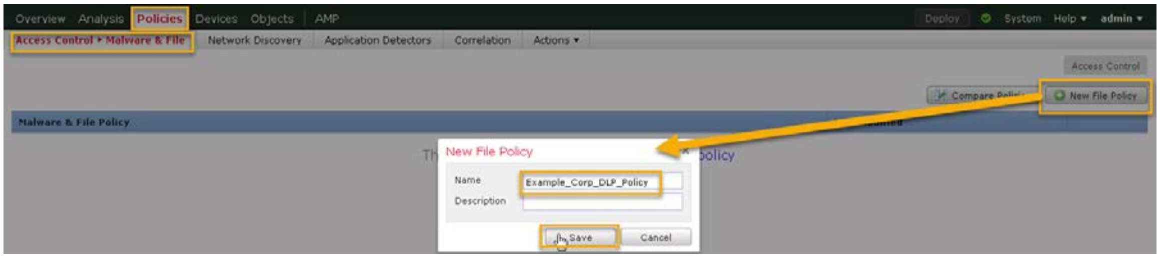
Example Corp knows that a major vector for malware and viruses infecting their networked computers is through file attachments to emails, file downloads off of web sites (or by any other means). They are also concerned about what files are leaving (being uploaded) from their networks out to the Internet. So their business requirements require that all downloaded office documents be inspected for malware, that any office document being uploaded to the Internet be permitted but logged, and that no executables be permitted (upload or download).

Create Malware & File Policy

Similar to how the SSL Policy flow worked you need to create the Malware & File Policy and then associate it with an Access Control Policy.

1. In the FMC website navigate to **Policies > Access Control > Malware & File**.
2. Click the **New File Policy** button.
    a. Name: **Example_Corp_DLP_Policy**
    b. Click **Save**.

Figure 353. Create new policy



Name: Example_Corp_DLP_Policy
Description:
Save

3. Now that the Policy exists you need to create your rules. Let’s start with the rule regarding document files coming from the Internet into Example Corp LANs. Click **Add Rule** to begin.

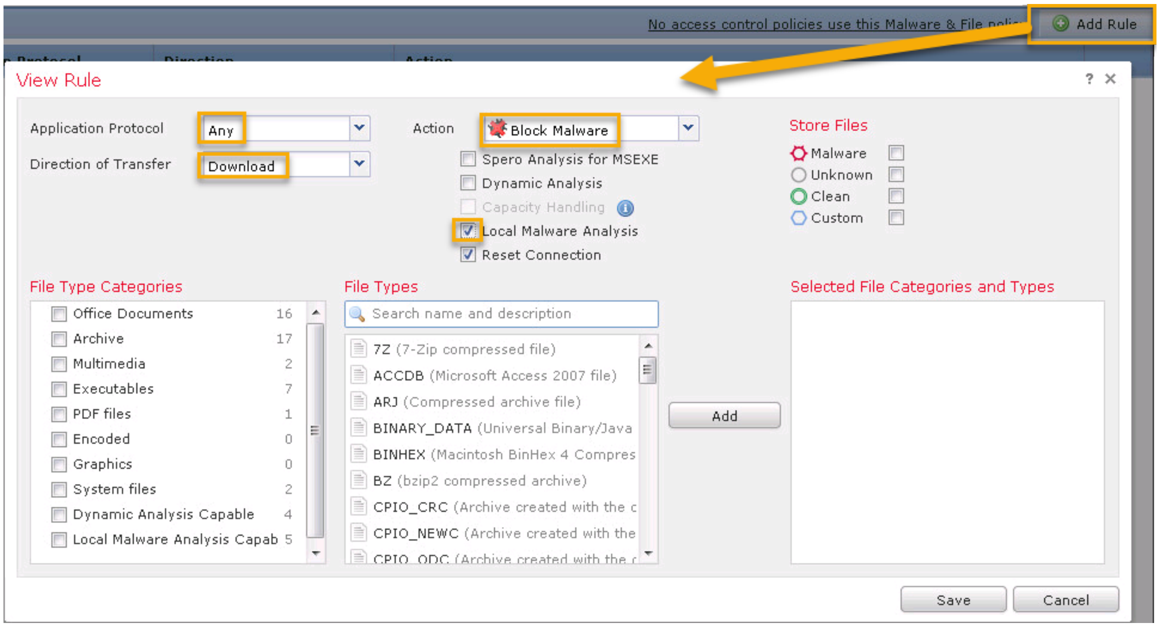
    a. Application Protocol: **Any** (You don’t care how it is transferred. You want to inspect these files for infections and malware.)

    b. Direction of Transfer: **Download**

    c. Action: **Block Malware**

    d. Check the **Local Malware Analysis** box.

Figure 354. Part 1 of adding new rule



Application Protocol: Any

Direction of Transfer: Download

Action: Block Malware

□ Spero Analysis for MSEXE
□ Dynamic Analysis
□ Capacity Handling
☑ Local Malware Analysis
☑ Reset Connection

Store Files
Malware □
Unknown □
Clean □
Custom □

File Type Categories

□ Office Documents	16
□ Archive	17
□ Multimedia	2
□ Executables	7
□ PDF files	1
□ Encoded	0
□ Graphics	0
□ System files	2
□ Dynamic Analysis Capable	4
□ Local Malware Analysis Capab	5

File Types

Search name and description

- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY_DATA (Universal Binary/Java
- BINHEX (Macintosh BinHex 4 Compres
- BZ (bzip2 compressed archive)
- CPIO_CRC (Archive created with the c
- CPIO_NEWC (Archive created with the
- CPIO_ODC (Archive created with the c

Here is a quick reference list of the different actions and some of their extended options:

Detect = checks first 1460 Bytes, determines the type of file and generates a log

Block = blocks the file based on first 1460 Bytes

Malware Cloud Lookup = Sends the SHA-256 hash of a file to the cloud for analysis and depending on the answer generates a log if the file is bad. Optionally, msexe files can be sent to cloud for Dynamic Analysis and/or SPERO analysis.

Block Malware = Sends the SHA-256 hash of a file to the cloud for analysis and depending on the answer blocks it if the file is bad. Optionally, msexe files can be sent to cloud for Dynamic Analysis and/or SPERO analysis.

Spero Analysis for MSEXE = checks apart from SHA-256 also some other parameters (e.g. DLLs that are called etc)

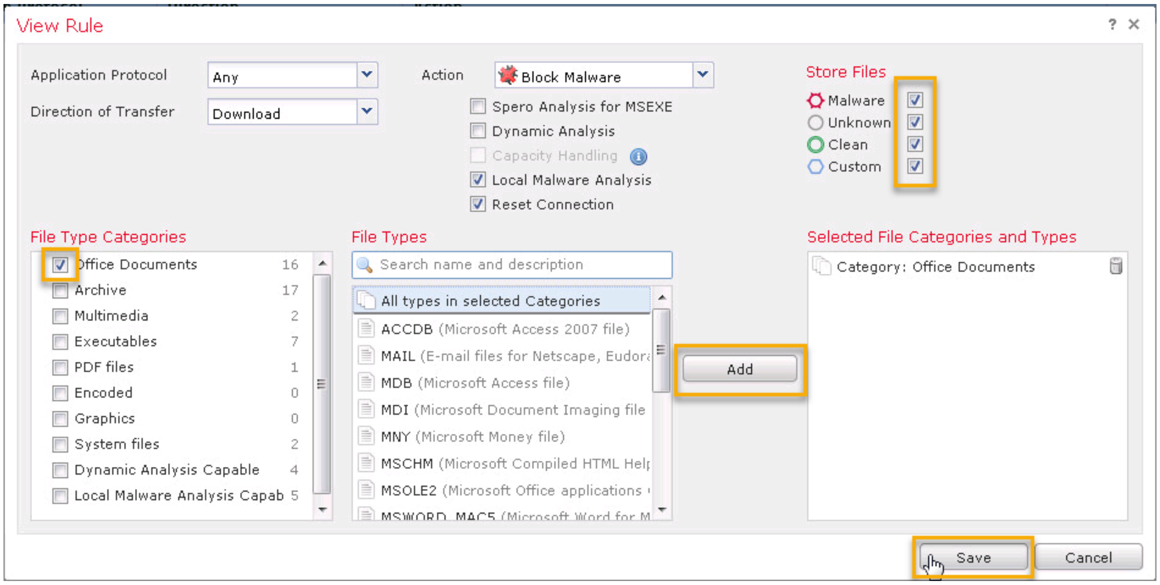
Dynamic Analysis = sends the file to the cloud for analysis. This can take 20-30 minutes

e. Check **all the boxes** for the **Store Files** option.

f. In the **File Type Categories** check the **Office Documents** box and click the **Add** button to move it to the Selected File Categories and Types.

g. Click **Save**.

Figure 355. Save new rule



View Rule

Application Protocol: Any

Direction of Transfer: Download

Action: Block Malware

☐ Spero Analysis for MSEXE
☐ Dynamic Analysis
☐ Capacity Handling
☑ Local Malware Analysis
☑ Reset Connection

Store Files
Malware ☑
Unknown ☑
Clean ☑
Custom ☑

File Type Categories

☑ Office Documents	16
☐ Archive	17
☐ Multimedia	2
☐ Executables	7
☐ PDF files	1
☐ Encoded	0
☐ Graphics	0
☐ System files	2
☐ Dynamic Analysis Capable	4
☐ Local Malware Analysis Capab	5

File Types

Search name and description

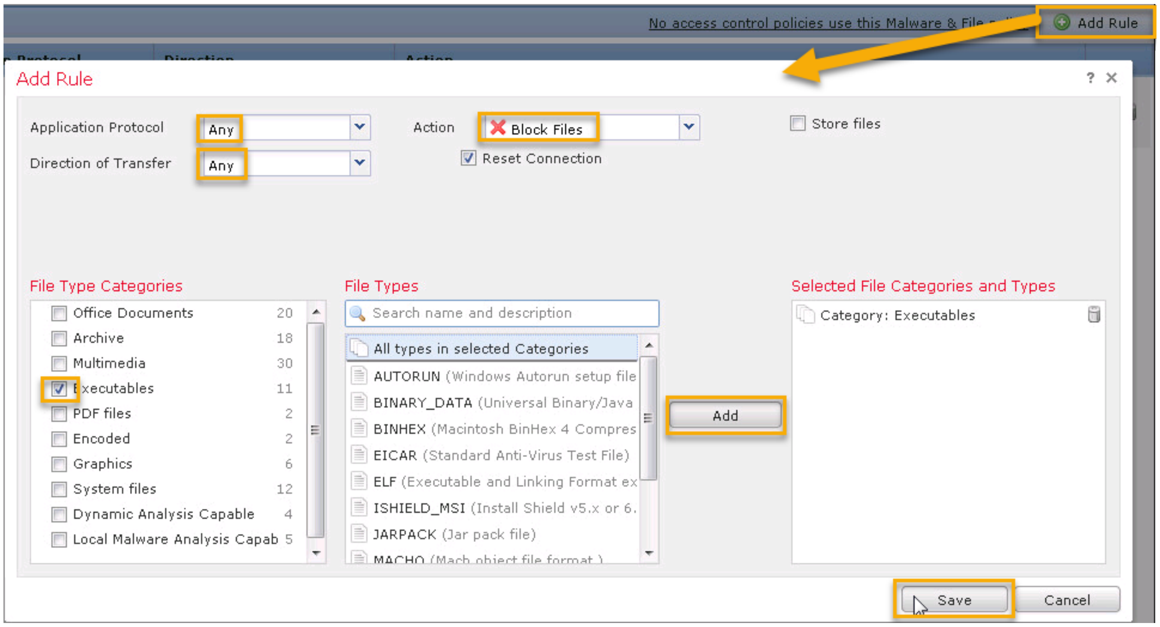
All types in selected Categories
ACCDB (Microsoft Access 2007 file)
MAIL (E-mail files for Netscape, Eudora
MDB (Microsoft Access file)
MDI (Microsoft Document Imaging file
MNY (Microsoft Money file)
MSCHM (Microsoft Compiled HTML Help
MSOLE2 (Microsoft Office applications
MSWORD_MAC5 (Microsoft Word for M

Selected File Categories and Types

Category: Office Documents

4. The next rule will be to block any transferring of an Executable (in either direction). Click the **Add Rule** button to begin.
    a. Application Protocol: **Any**
    b. Direction of Transfer: **Any**
    c. Action: **Block Files** (Note: Leave the “Reset Connection” box enabled as there are certain situations where the file can still get downloaded if the connection isn’t reset.)
    d. In the **File Type Categories** check the **Executables** box and click the **Add** button to move it to the Selected File Categories and Types.
    e. Click **Save**.

Figure 356. Create another rule



No access control policies use this Malware & File ...

Add Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Block Files

☑ Reset Connection

□ Store files

File Type Categories

□ Office Documents	20
□ Archive	18
□ Multimedia	30
☑ Executables	11
□ PDF files	2
□ Encoded	2
□ Graphics	6
□ System files	12
□ Dynamic Analysis Capable	4
□ Local Malware Analysis Capab	5

File Types

Search name and description

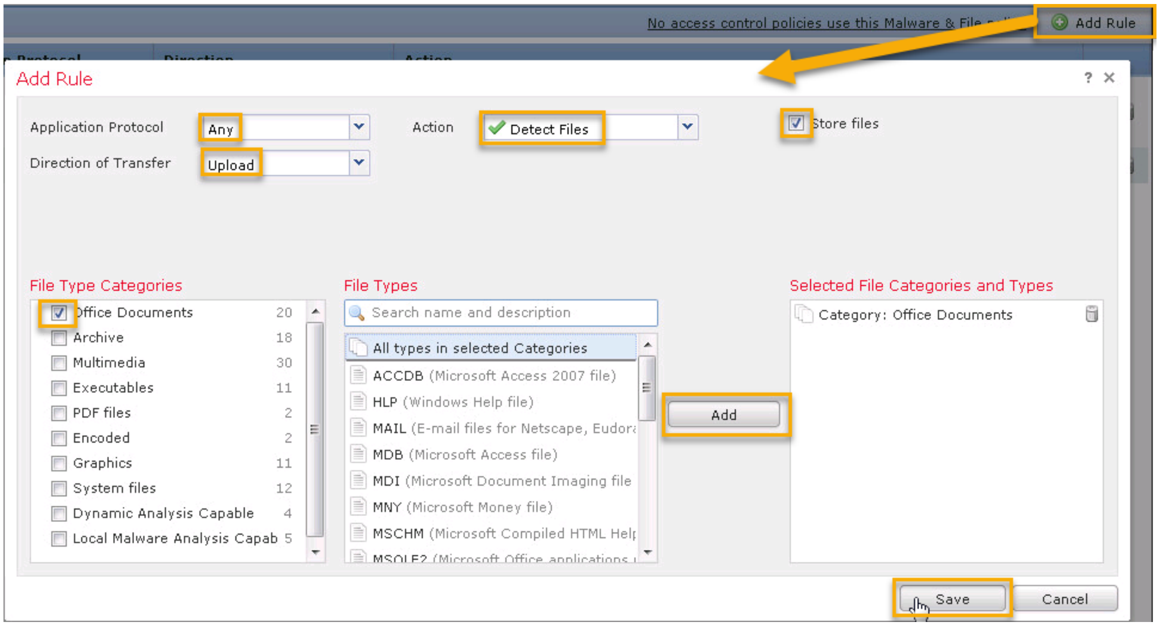
- All types in selected Categories
- AUTORUN (Windows Autorun setup file
- BINARY_DATA (Universal Binary/Java
- BINHEX (Macintosh BinHex 4 Compres
- EICAR (Standard Anti-Virus Test File)
- ELF (Executable and Linking Format ex
- ISHIELD_MSI (Install Shield v5.x or 6.
- JARPACK (Jar pack file)
- MACHO (Mach object file format)

Selected File Categories and Types

- Category: Executables

5. The last rule it to provide some level of detection of when any file gets sent out of the Example Corp LANs. Click **Add Rule** to create this rule.
   a. Application Protocol: **Any**
   b. Direction of Transfer: **Upload**
   c. Action: **Detect Files**
   d. Check the **Store Files** box.
   e. In the **File Type Categories** check the **Office Documents** box and click the **Add** button to move it to the Selected File Categories and Types.
   f. Click **Save**.

Figure 357. Create another rule



Application Protocol: Any

Direction of Transfer: Upload

Action: ✓ Detect Files

☑ Store files

File Type Categories

☑	Office Documents	20
□	Archive	18
□	Multimedia	30
□	Executables	11
□	PDF files	2
□	Encoded	2
□	Graphics	11
□	System files	12
□	Dynamic Analysis Capable	4
□	Local Malware Analysis Capab	5

File Types

Search name and description

- All types in selected Categories
- ACCDB (Microsoft Access 2007 file)
- HLP (Windows Help file)
- MAIL (E-mail files for Netscape, Eudora
- MDB (Microsoft Access file)
- MDI (Microsoft Document Imaging file
- MNY (Microsoft Money file)
- MSCHM (Microsoft Compiled HTML Help
- MSOLE2 (Microsoft Office applications

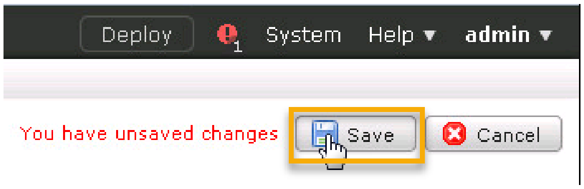
Selected File Categories and Types

- Category: Office Documents

Note: PDF files are not considered Office Documents but are a category all to themselves.

6. Click **Save**.

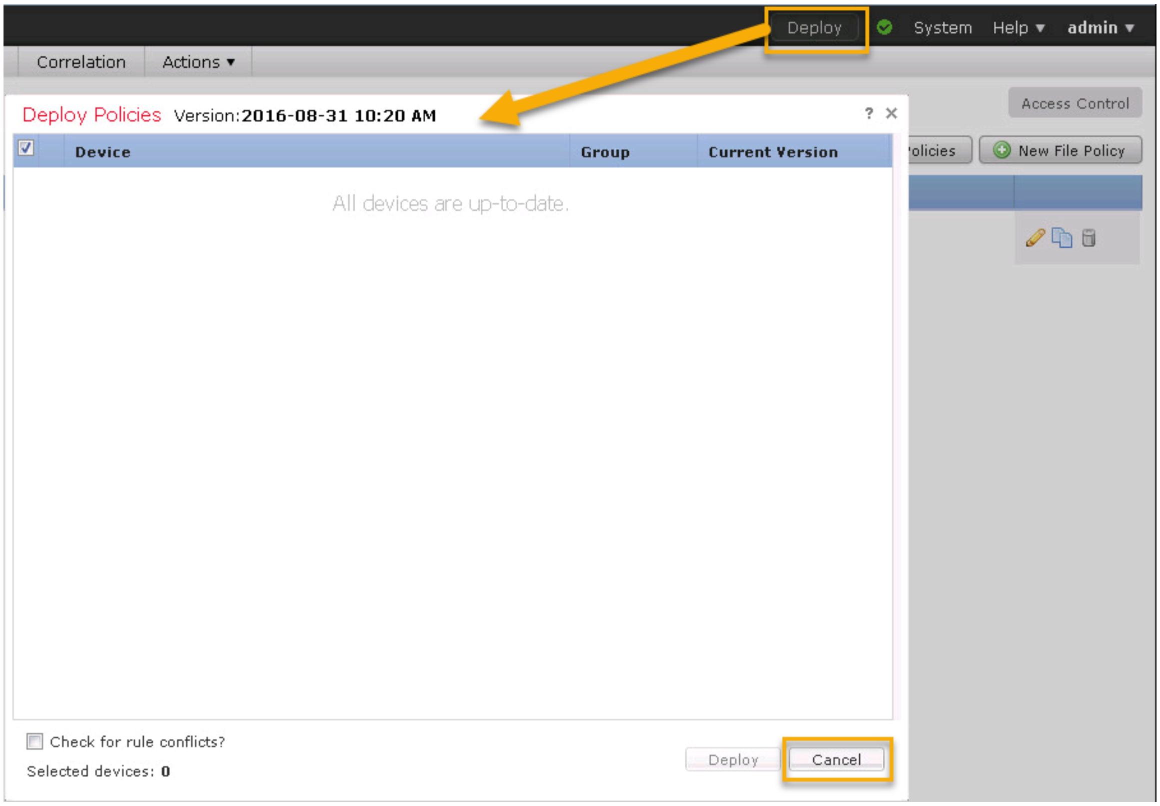
Figure 358. Save changes to FMC



You have unsaved changes

7. Click **Deploy** and then… why don't any devices show up? Though the Malware & File Policy has been created it needs to be associated with an ACP to actually be put into action. Click **Cancel** to return to the FMC GUI.

Figure 359. Nothing to Deploy, yet.



Deploy Policies Version:2016-08-31 10:20 AM

☑	Device	Group	Current Version

All devices are up-to-date.

☐ Check for rule conflicts?

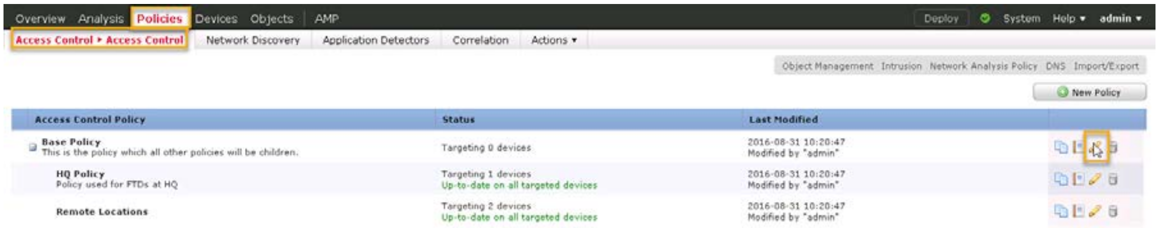
Selected devices: 0

Attach Malware & File Policy to ACP Base Policy

Now that the Malware & File Policy has been created and configured with rules it is time to associate it with the Base Policy Access Control Policy.

8. Navigate to **Policies > Access Control > Access Control** and edit the **Base Policy**.

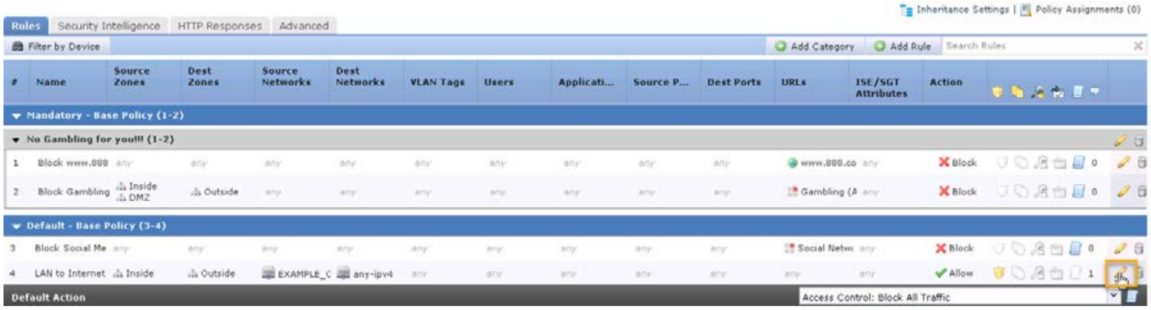
Figure 360. Edit the Base Policy



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-31 10:20:47 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-31 10:20:47 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-08-31 10:20:47 Modified by "admin"

9. **Edit** the **LAN to Internet Access** rule.

Figure 361. Edit the LAN to Internet Access rule



Inheritance Settings | Policy Assignments (0)

Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device | Add Category | Add Rule | Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
Mandatory - Base Policy (1-2)														
No Gambling for you!!! (1-2)														
1	Block www.888	any	any	any	any	any	any	any	any	any	www.888.co	any	Block	0
2	Block Gambling	Inside DMZ	Outside	any	any	any	any	any	any	any	Gambling (A	any	Block	0
Default - Base Policy (3-4)														
3	Block Social Me	any	any	any	any	any	any	any	any	any	Social Netw	any	Block	0
4	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	Allow	1

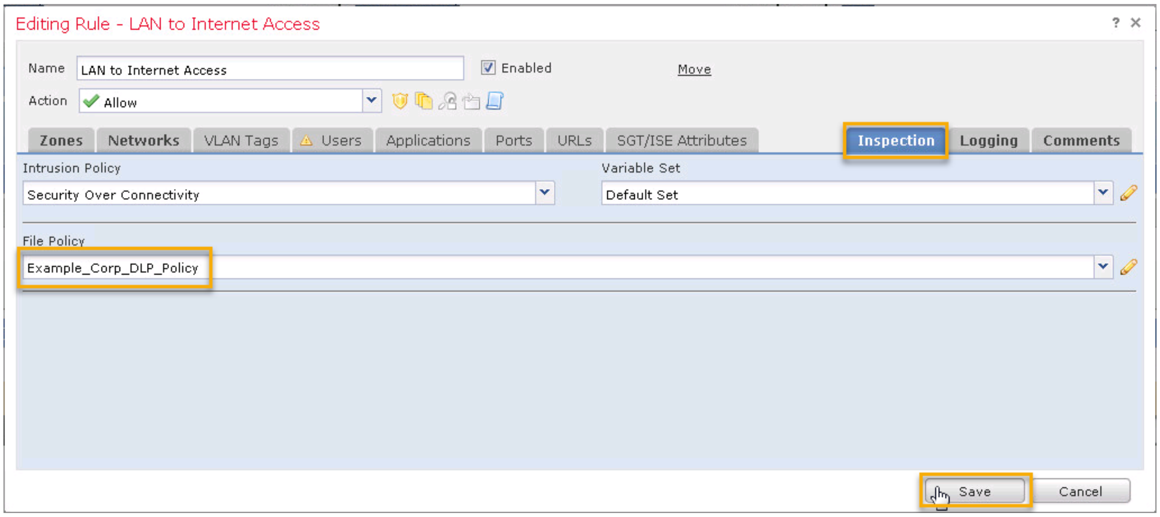
Default Action: Access Control: Block All Traffic

10. Click the **Inspections tab**.

11. Using the dropdown menu for the **File Policy** option select the **Example_Corp_DLP_Policy** from the list.

12. Click **Save** to save the modification to this rule.

Figure 362. Apply Policy and Save.



Editing Rule - LAN to Internet Access

Name: LAN to Internet Access ☑ Enabled Move

Action: Allow

Intrusion Policy: Security Over Connectivity

Variable Set: Default Set

File Policy: Example_Corp_DLP_Policy

13. Now click **Save** to save your changes. Then click **Deploy**, select **all the FTD** devices, and then click **Deploy**.

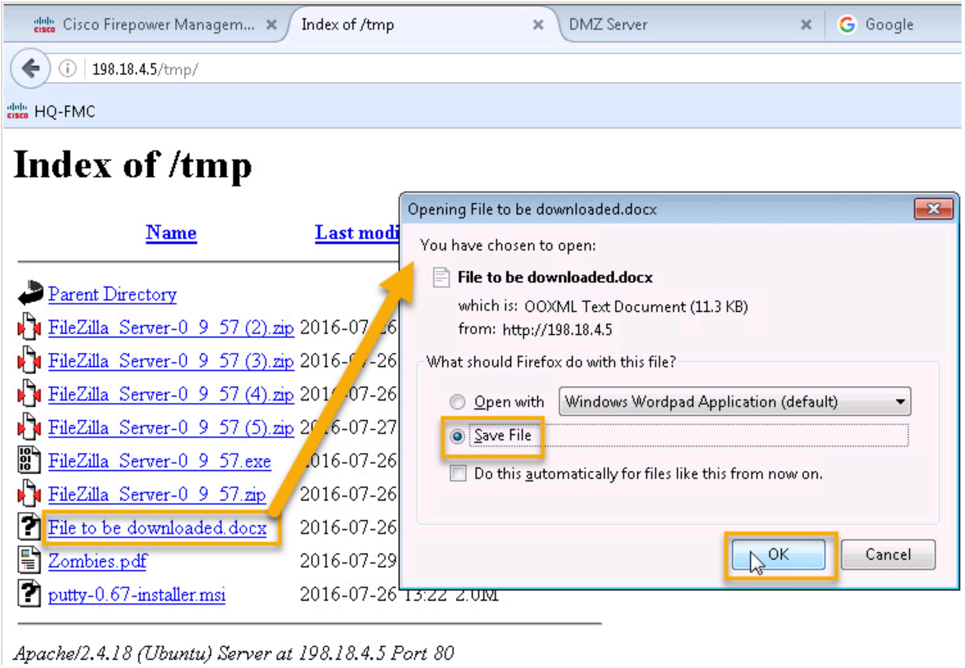
Perform Tests

Once the deployment is complete you will perform some tests to see what your Malware & File Policy can do.

14. On **hq-wkst** open a **Firefox** tab to **http://198.18.4.5/tmp** (this is the inet-server).

15. Download the **File to be downloaded.docx** file.

Figure 363. Download the file



Index of /tmp

Name	Last modi
Parent Directory	
FileZilla_Server-0_9_57 (2).zip	2016-07-26
FileZilla_Server-0_9_57 (3).zip	2016-07-26
FileZilla_Server-0_9_57 (4).zip	2016-07-26
FileZilla_Server-0_9_57 (5).zip	2016-07-27
FileZilla_Server-0_9_57.exe	2016-07-26
FileZilla_Server-0_9_57.zip	2016-07-26
File to be downloaded.docx	2016-07-26
Zombies.pdf	2016-07-29
putty-0.67-installer.msi	2016-07-26 13:22 2.0M

Apache/2.4.18 (Ubuntu) Server at 198.18.4.5 Port 80

Opening File to be downloaded.docx

You have chosen to open:

File to be downloaded.docx

which is: OOXML Text Document (11.3 KB)
from: http://198.18.4.5

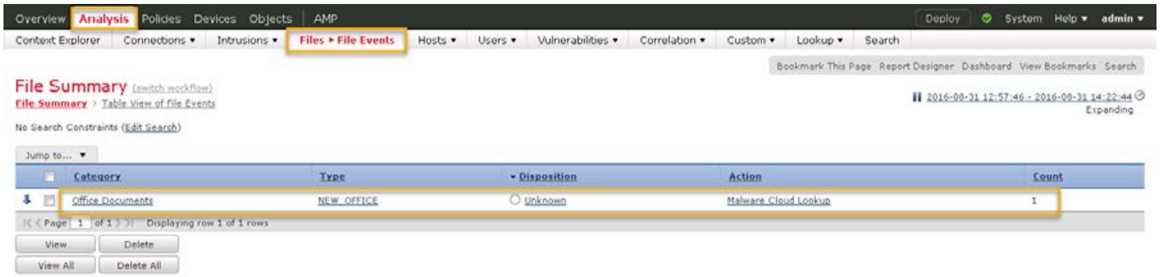
What should Firefox do with this file?

○ Open with Windows Wordpad Application (default)
● Save File
□ Do this automatically for files like this from now on.

OK Cancel

16. In the FMC GUI navigate to **Analysis > Files > File Events** and notice that this file was recognized and the Action is Malware Cloud Lookup. The first time this file is downloaded it is allowed BUT the FMC takes a note of this file and queries Cisco's cloud service to see if the signature of this file meets any of the known malware signatures.

Figure 364. View File Events



File Summary (switch workflow)
File Summary > Table View of File Events

2016-08-31 12:57:46 - 2016-08-31 14:22:44
Expanding

No Search Constraints (Edit Search)

Jump to... ▾

	Category	Type	Disposition	Action	Count
□	Office Documents	NEW_OFFICE	○ Unknown	Malware Cloud Lookup	1

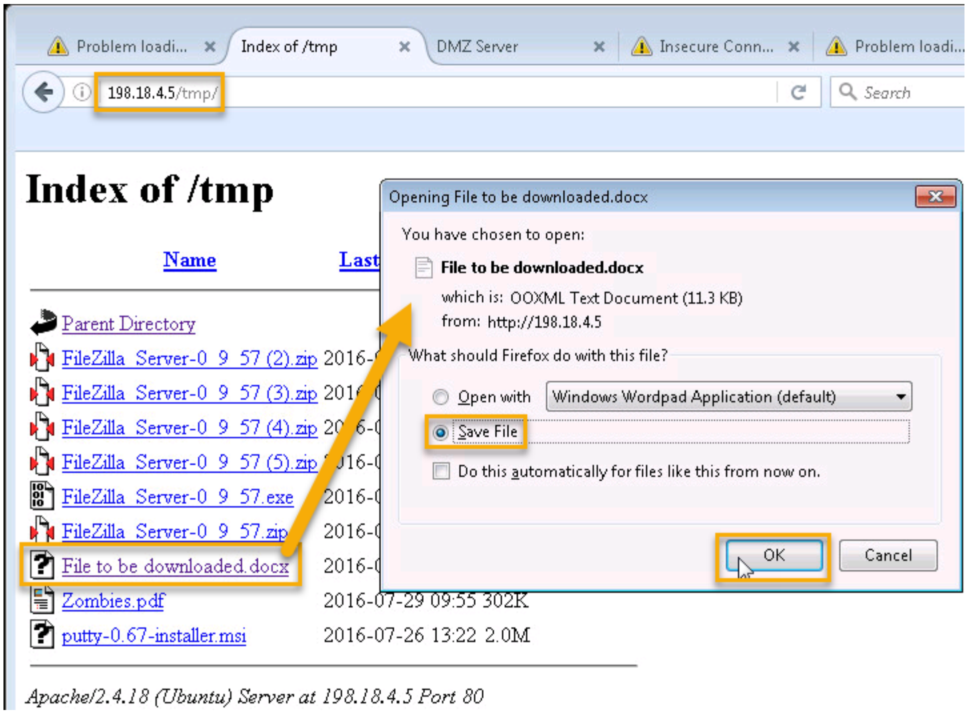
Page 1 of 1 Displaying row 1 of 1 rows

View Delete
View All Delete All

If nothing is displayed try opening up Chrome on hq-wkst and attempt to download that file.

17. On **remote1-wkst** open up **Firefox** and go to http://198.18.4.5/tmp and download the **File to be downloaded.docx** file.

Figure 365. Download file from remote1-wkst



Index of /tmp

Name Last

Parent Directory
FileZilla_Server-0_9_57 (2).zip 2016-
FileZilla_Server-0_9_57 (3).zip 2016
FileZilla_Server-0_9_57 (4).zip 2016-
FileZilla_Server-0_9_57 (5).zip 2016-
FileZilla_Server-0_9_57.exe 2016-
FileZilla_Server-0_9_57.zip 2016-
File to be downloaded.docx 2016-
Zombies.pdf 2016-07-29 09:55 302K
putty-0.67-installer.msi 2016-07-26 13:22 2.0M

Apache/2.4.18 (Ubuntu) Server at 198.18.4.5 Port 80

Opening File to be downloaded.docx

You have chosen to open:

File to be downloaded.docx

which is: OOXML Text Document (11.3 KB)
from: http://198.18.4.5

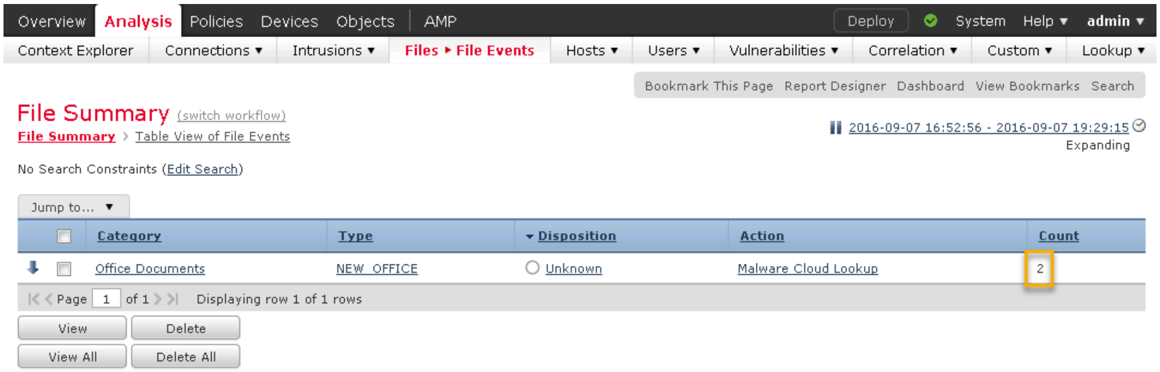
What should Firefox do with this file?

○ Open with Windows Wordpad Application (default)
● Save File
□ Do this automatically for files like this from now on.

OK Cancel

18. Return to the FMC GUI and click the **File Summary** link. (This is like refreshing this page. The Table View of File Events would provide a more detailed view.) Notice that the Count column now shows 2.

Figure 366. View File Events



File Summary (switch workflow)
File Summary > Table View of File Events

2016-09-07 16:52:56 - 2016-09-07 19:29:15
Expanding

No Search Constraints (Edit Search)

Jump to... ▾

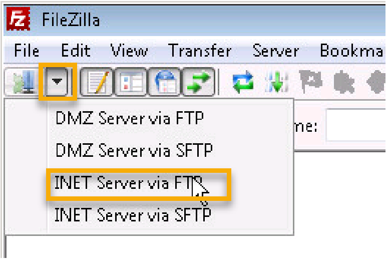
	Category	Type	Disposition	Action	Count
□	Office Documents	NEW_OFFICE	○ Unknown	Malware Cloud Lookup	2

Page 1 of 1 Displaying row 1 of 1 rows

View Delete
View All Delete All

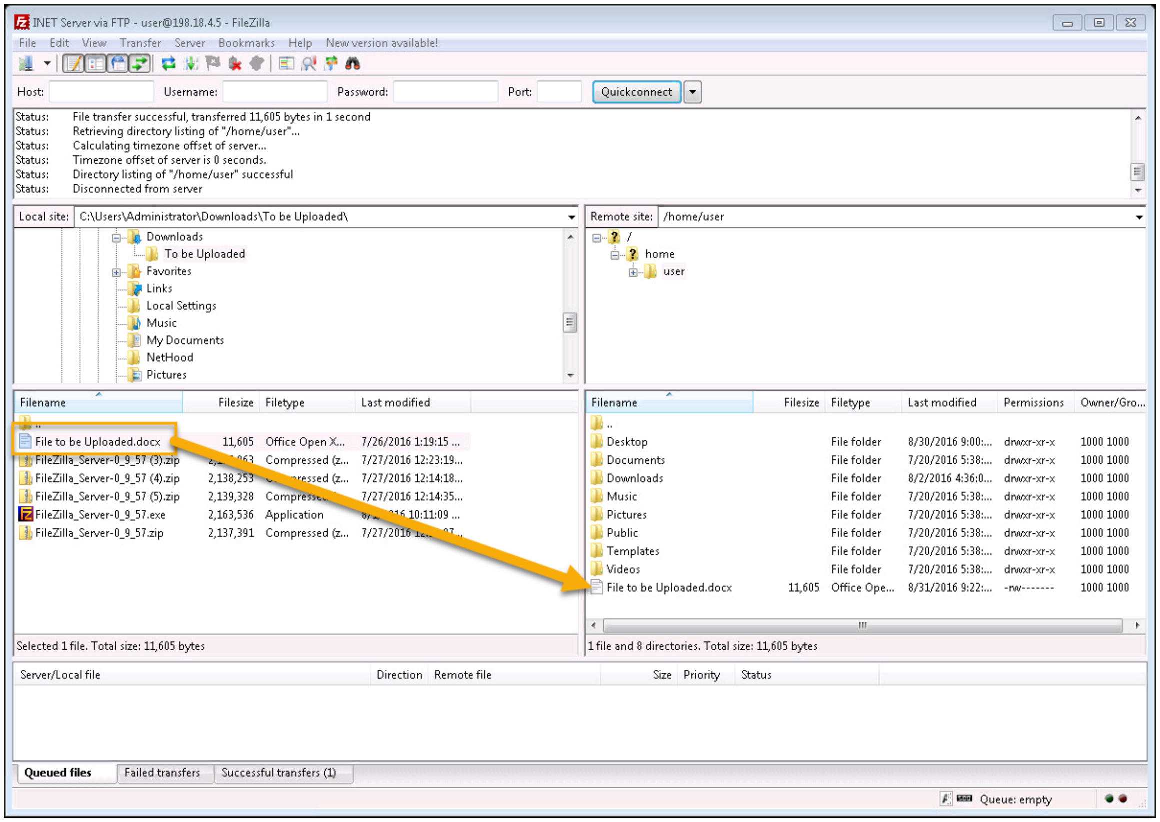
19. On **hq-wkst** open up **FileZilla** and use the **INET Server via FTP** bookmark to create an FTP connection to the inet-server.

Figure 367. Connect via FTP to inet-server



20. Upload the **File to be Uploaded.docx** file, located in the **To be Uploaded** folder in the **Downloads** directory.

Figure 368. FTP upload file


INET Server via FTP - user@198.18.4.5 - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
Host: Username: Password: Port: Quickconnect
Downloads
To be Uploaded
Favorites
Links
Local Settings
Music
My Documents
NetHood
Pictures
/
home
user
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers (1)
Queue: empty

```
Status:    File transfer successful, transferred 11,605 bytes in 1 second
Status:    Retrieving directory listing of "/home/user"...
Status:    Calculating timezone offset of server...
Status:    Timezone offset of server is 0 seconds.
Status:    Directory listing of "/home/user" successful
Status:    Disconnected from server
```

Local site: C:\Users\Administrator\Downloads\To be Uploaded\

Filename	Filesize	Filetype	Last modified
..			
File to be Uploaded.docx	11,605	Office Open X...	7/26/2016 1:19:15 ...
FileZilla_Server-0_9_57 (3).zip	[illegible]	Compressed (z...	7/27/2016 12:23:19...
FileZilla_Server-0_9_57 (4).zip	2,138,253	[illegible]	7/27/2016 12:14:18...
FileZilla_Server-0_9_57 (5).zip	2,139,328	Compresse[illegible]	7/27/2016 12:14:35...
FileZilla_Server-0_9_57.exe	2,163,536	Application	[illegible] 10:11:09 ...
FileZilla_Server-0_9_57.zip	2,137,391	Compressed (z...	7/27/2016 [illegible]

Selected 1 file. Total size: 11,605 bytes

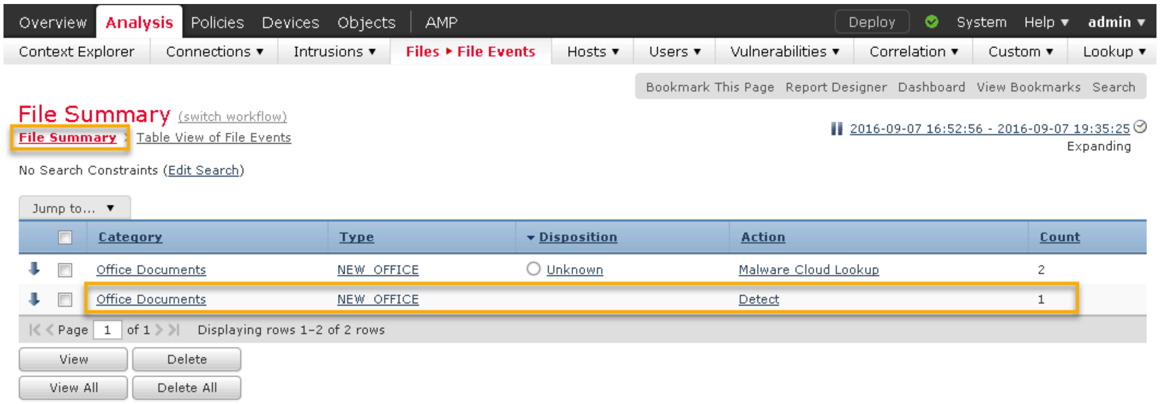
Remote site: /home/user

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
Desktop		File folder	8/30/2016 9:00:...	drwxr-xr-x	1000 1000
Documents		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Downloads		File folder	8/2/2016 4:36:0...	drwxr-xr-x	1000 1000
Music		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Pictures		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Public		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Templates		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Videos		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
File to be Uploaded.docx	11,605	Office Ope...	8/31/2016 9:22:...	-rw-------	1000 1000

1 file and 8 directories. Total size: 11,605 bytes

21. Return to the FMC GUI and click the **File Summary** link again. Notice that you have a new line and the Action is Detect. (Document files leaving the Example Corp network are allowed but are checked for Malware.)

Figure 369. View File Events



File Summary (switch workflow)

File Summary › Table View of File Events

2016-09-07 16:52:56 - 2016-09-07 19:35:25

Expanding

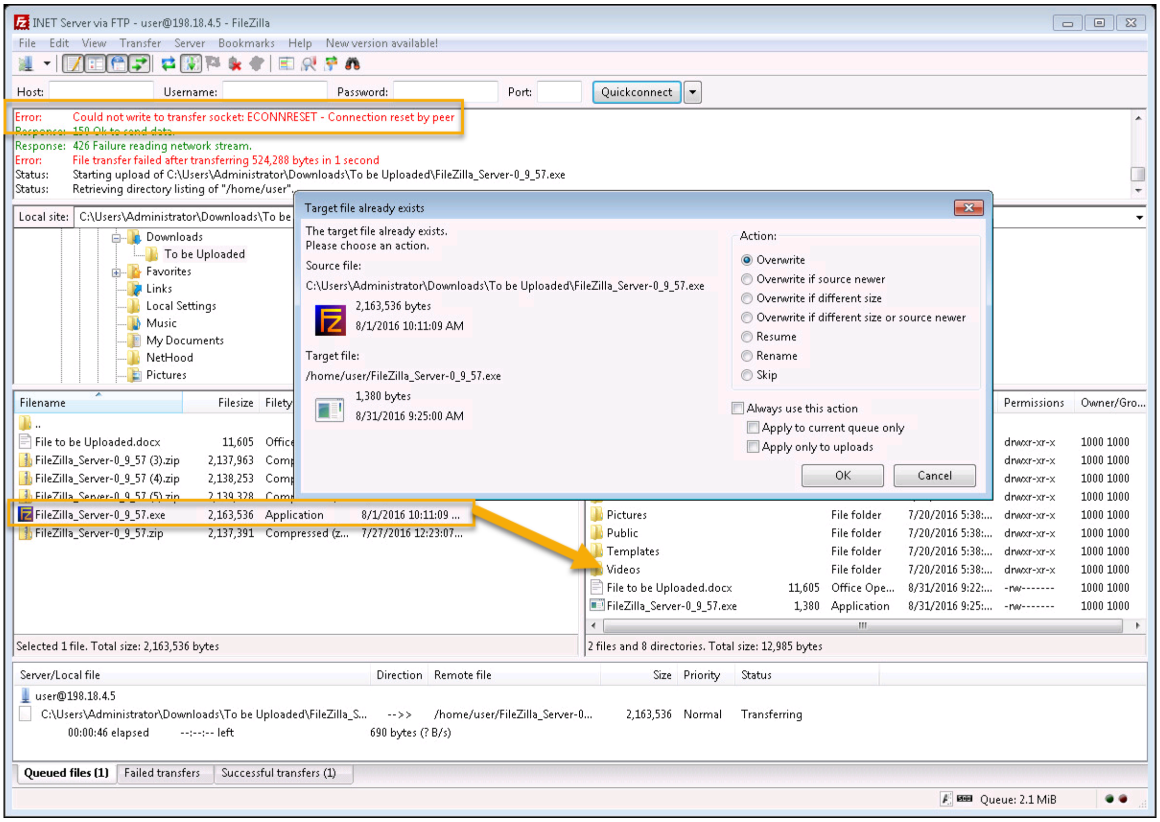
No Search Constraints (Edit Search)

	□	Category	Type	▾ Disposition	Action	Count
⬇	□	Office Documents	NEW_OFFICE	○ Unknown	Malware Cloud Lookup	2
⬇	□	Office Documents	NEW_OFFICE		Detect	1

Page 1 of 1 Displaying rows 1–2 of 2 rows

22. On **hq-wkst** attempt to upload the **FileZilla_Server-0_9_57.exe** file via FTP and download it using HTTP from the inet-server. Notice how each program behaves differently but the result is the same. The connection is reset as soon as the hq-ftd device recognizes that an EXE file is being transferred.

Figure 370. Try to download EXE file via FTP



```
Error:     Could not write to transfer socket: ECONNRESET - Connection reset by peer
Response:  150 Ok to send data.
Response:  426 Failure reading network stream.
Error:     File transfer failed after transferring 524,288 bytes in 1 second
Status:    Starting upload of C:\Users\Administrator\Downloads\To be Uploaded\FileZilla_Server-0_9_57.exe
Status:    Retrieving directory listing of "/home/user"...
```

Local site: C:\Users\Administrator\Downloads\To be

Target file already exists

The target file already exists.
Please choose an action.

Source file:
C:\Users\Administrator\Downloads\To be Uploaded\FileZilla_Server-0_9_57.exe
2,163,536 bytes
8/1/2016 10:11:09 AM

Target file:
/home/user/FileZilla_Server-0_9_57.exe
1,380 bytes
8/31/2016 9:25:00 AM

Action:
- ● Overwrite
- ○ Overwrite if source newer
- ○ Overwrite if different size
- ○ Overwrite if different size or source newer
- ○ Resume
- ○ Rename
- ○ Skip

□ Always use this action
□ Apply to current queue only
□ Apply only to uploads

Filename	Filesize	Filetype	Last modified
..			
File to be Uploaded.docx	11,605	Office	
FileZilla_Server-0_9_57 (3).zip	2,137,963	Comp	
FileZilla_Server-0_9_57 (4).zip	2,138,253	Comp	
FileZilla_Server-0_9_57 (5).zip	2,139,328	Comp	
FileZilla_Server-0_9_57.exe	2,163,536	Application	8/1/2016 10:11:09 ...
FileZilla_Server-0_9_57.zip	2,137,391	Compressed (z...	7/27/2016 12:23:07...

Selected 1 file. Total size: 2,163,536 bytes

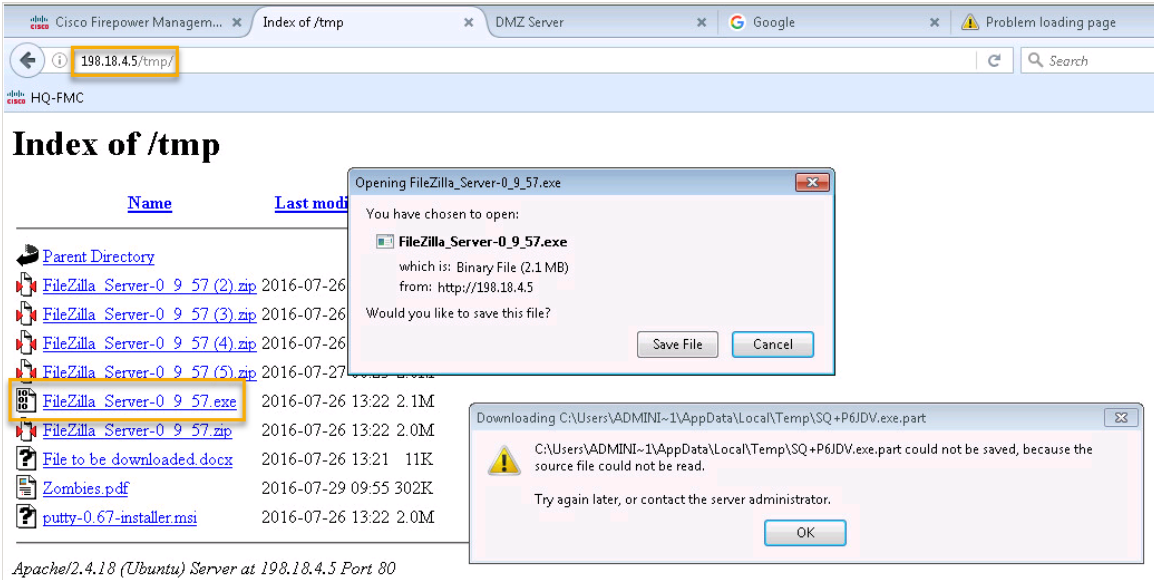
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
				drwxr-xr-x	1000 1000
				drwxr-xr-x	1000 1000
				drwxr-xr-x	1000 1000
				drwxr-xr-x	1000 1000
Pictures		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Public		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Templates		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
Videos		File folder	7/20/2016 5:38:...	drwxr-xr-x	1000 1000
File to be Uploaded.docx	11,605	Office Ope...	8/31/2016 9:22:...	-rw-------	1000 1000
FileZilla_Server-0_9_57.exe	1,380	Application	8/31/2016 9:25:...	-rw-------	1000 1000

2 files and 8 directories. Total size: 12,985 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status
user@198.18.4.5					
C:\Users\Administrator\Downloads\To be Uploaded\FileZilla_S...	-->>	/home/user/FileZilla_Server-0...	2,163,536	Normal	Transferring
00:00:46 elapsed --:--:-- left		690 bytes (? B/s)			

Note: Though you'll see the file in the destination folder, compare the file size of that file with the original and notice that it is only the first few bytes that get through before FTD blocks the download.

Figure 371. Try to download EXE via HTTP



Index of /tmp

Name	Last modi...	
Parent Directory		
FileZilla_Server-0_9_57 (2).zip	2016-07-26	
FileZilla_Server-0_9_57 (3).zip	2016-07-26	
FileZilla_Server-0_9_57 (4).zip	2016-07-26	
FileZilla_Server-0_9_57 (5).zip	2016-07-27	
FileZilla_Server-0_9_57.exe	2016-07-26 13:22	2.1M
FileZilla_Server-0_9_57.zip	2016-07-26 13:22	2.0M
File to be downloaded.docx	2016-07-26 13:21	11K
Zombies.pdf	2016-07-29 09:55	302K
putty-0.67-installer.msi	2016-07-26 13:22	2.0M

Apache/2.4.18 (Ubuntu) Server at 198.18.4.5 Port 80

Opening FileZilla_Server-0_9_57.exe

You have chosen to open:

FileZilla_Server-0_9_57.exe

which is: Binary File (2.1 MB)
from: http://198.18.4.5

Would you like to save this file?

Save File | Cancel

Downloading C:\Users\ADMINI~1\AppData\Local\Temp\SQ+P6JDV.exe.part

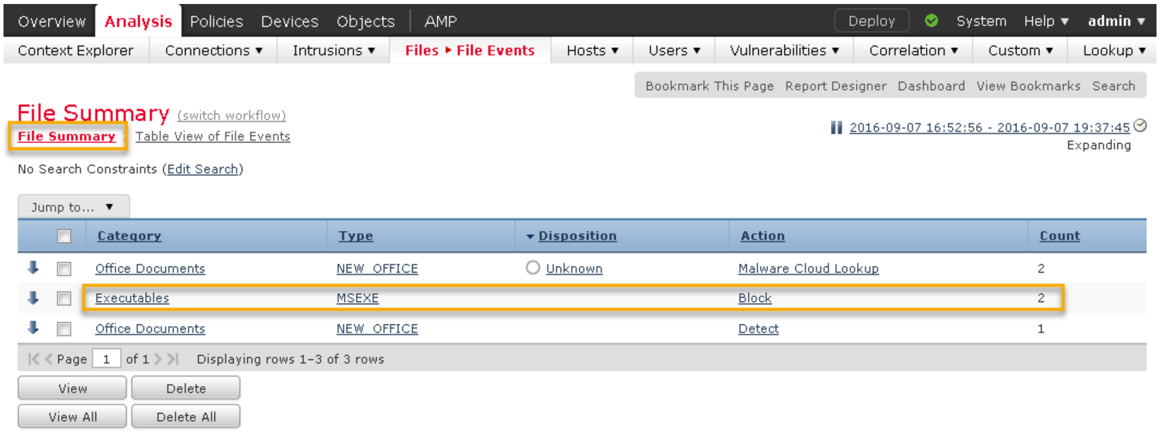
C:\Users\ADMINI~1\AppData\Local\Temp\SQ+P6JDV.exe.part could not be saved, because the source file could not be read.

Try again later, or contact the server administrator.

OK

23. Return to the FMC GUI and click the **File Summary** link again. Now you have an Executables row with an Action of Block. For further information, click the Table View of File Events to see each connection, the reason for the action, and even what protocol the file came over (scroll to the far right to see that).

Figure 372. View File Events



File Summary (switch workflow)

File Summary | Table View of File Events

2016-09-07 16:52:56 - 2016-09-07 19:37:45
Expanding

No Search Constraints (Edit Search)

	□	Category	Type	▾ Disposition	Action	Count
⬇	□	Office Documents	NEW_OFFICE	○ Unknown	Malware Cloud Lookup	2
⬇	□	Executables	MSEXE		Block	2
⬇	□	Office Documents	NEW_OFFICE		Detect	1

Page 1 of 1 Displaying rows 1–3 of 3 rows

The Malware & File policy will also check within compressed/archived files to ensure the files within the archive are also meeting the policy's rules. However, there are limitations to this checking. Nested archives (a zip file within a zip file) are only check two levels deep by default. (This is a configurable setting and can be changed to check up to three nested levels deep.) Also, only archives less than 1MB will be checked (again, by default and this value can be changed).

So, for example, the putty.zip file (less than 1MB) will be extracted and checked against the Malware and File rules but the FileZilla_Server-0_9_57.zip will NOT be checked since its file size is greater than 1MB. You can test this, if you wish, as there are these files, as well as nested zip files, in the /home/user/Downloads folder on the inet-server. Use FTP on hq-wkst to access this location.

It appears that .msi files are not considered executables. There is a putty-0.67-installer.msi file in the Downloads directory if you wish to try transferring it. It is also available for download off of the inet-server website.

Scenario Summary

Did you see the “flaw” in the way this Malware & File Policy is applied? It is applied to a specific rule in the ACP Base Policy. If another policy, say a “permit all” type policy was written and applied in the HQ Policy then the Base Policy rule where the Malware & File Policy is applied wouldn’t ever get hit by anything coming from HQ. It is great that the Malware & File Policy application is specific enough that you can target very specific ACP rules but that is also a danger. Watch closely as ACP rules are being created so that any Malware & File Rule that needs applied to this new ACP rule’s traffic also gets the same Malware & File rule applied.

Page intentionally left blank.

Scenario 9. Intrusion Policy

Scenario Description

Use the Intrusion Policies to better target specific detection methods for certain devices or networks. For example, there is no reason to check Microsoft server vulnerabilities against a Linux server. So the Intrusion Policy feature helps reduce the overhead that is used in the more general policies that come with the FTD device.

In this scenario you will create a custom Intrusion policy and apply it on the DMZ server related ACP rules. You will then see how the FTD/FMC devices learn about the Example Corp network and build a recommended list of Intrusion rules. Finally, you will learn about and modify the default Variable Set to better identify the Example Corp network.

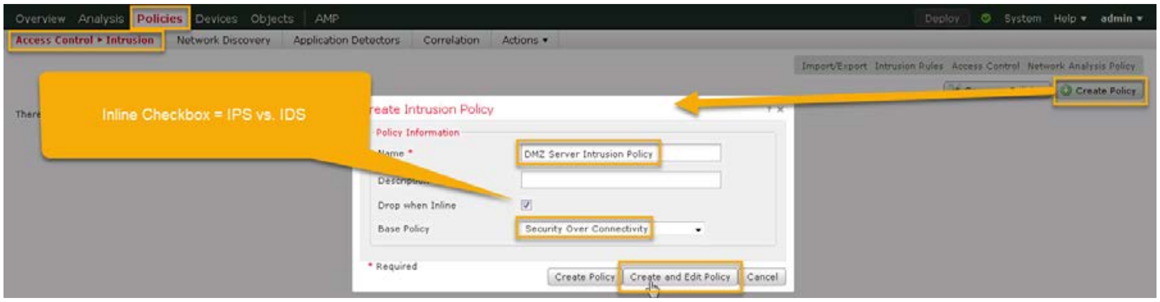
Intrusion Policies

Admittedly this section is a bit contrived since you don't have the ability to test "attacks" against these changes within the lab. That said, take the lessons learned and try to apply them to your real world scenarios to better fine tune your Intrusion policies to meet your customers' needs.

This first policy is an example of what you might want to do for a Linux server, such as the dmz-server, that is in your environment.

1. In the FMC GUI navigate to **Policies > Access Control > Intrusion**.
2. Click the **Create Policy** button and use the following to create the policy:
    a. Name: **DMZ Server Intrusion Policy**
    b. Base Policy: **Security Over Connectivity** (Notice this policy's Update date. This will be important later in the lab when you perform updates via Cisco's update services.)
3. Click the **Create and Edit Policy** button.

Figure 373. Create Intrusion Policy



Inline Checkbox = IPS vs. IDS

Create Intrusion Policy

Policy Information

Name * DMZ Server Intrusion Policy

Description

Drop when Inline ☑

Base Policy Security Over Connectivity

* Required

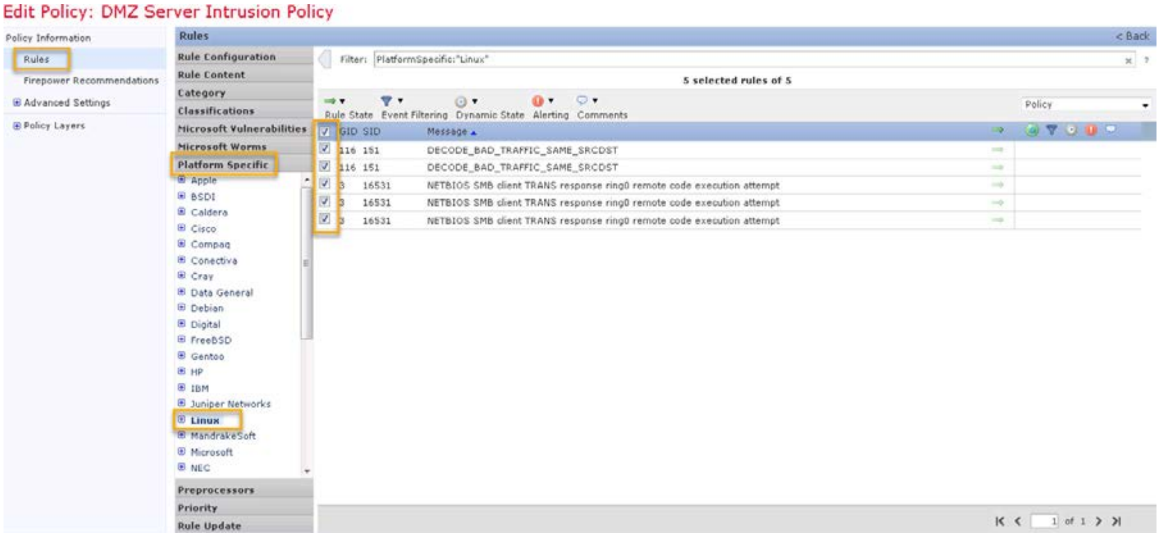
Note: In case you were wondering why the lab always has you selecting "Security Over Connectivity" for the Intrusion Policy was to give you had a common "base" intrusion policy. This is by no means mandatory but I wanted you to have a basis for comparison when creating a new Intrusion Policy. It isn't, per se, a Cisco recommendation to use the same Intrusion Policy everywhere but having fewer variables (different Intrusion Policies, in this example) to troubleshoot later on could be beneficial.

4. Click the **Rules** link in the left column.

   a. In the middle section expand the **Platform Specific** menu section and click the **Linux** link.

   b. Check **all the rules** that are then listed.

Figure 374. Select all the Linux rules



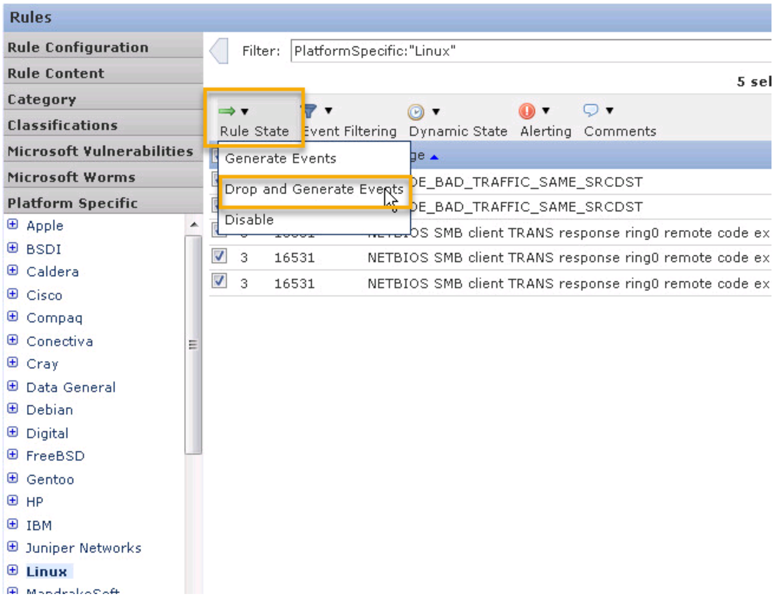
Filter: PlatformSpecific:"Linux"

5 selected rules of 5

	GID	SID	Message ▲
☑	116	151	DECODE_BAD_TRAFFIC_SAME_SRCDST
☑	116	151	DECODE_BAD_TRAFFIC_SAME_SRCDST
☑	3	16531	NETBIOS SMB client TRANS response ring0 remote code execution attempt
☑	3	16531	NETBIOS SMB client TRANS response ring0 remote code execution attempt
☑	3	16531	NETBIOS SMB client TRANS response ring0 remote code execution attempt

   c. Click **Rule State** and select **Drop and Generate Events** option.

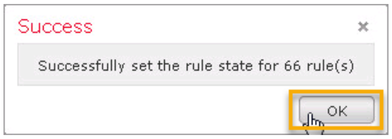
Figure 375. Select Drop and Generate Events



Filter: PlatformSpecific:"Linux"

d. Click **OK** on the Success popup window.

Figure 376. Click OK



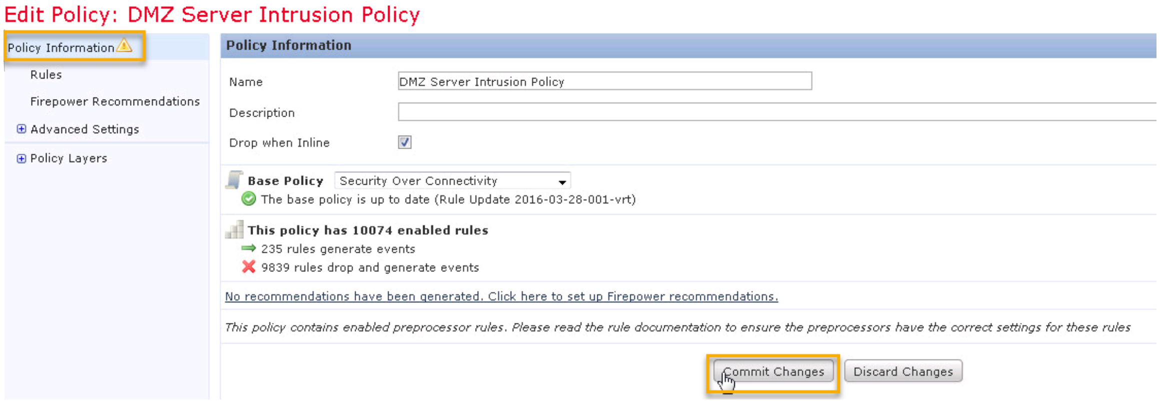
Success

Successfully set the rule state for 66 rule(s)

5. Click the **Policy Information** link.

6. Click **Commit Changes**.

Figure 377. Commit changes



Edit Policy: DMZ Server Intrusion Policy

Name: DMZ Server Intrusion Policy

Description:

Drop when Inline ☑

Base Policy: Security Over Connectivity

The base policy is up to date (Rule Update 2016-03-28-001-vrt)

This policy has 10074 enabled rules

235 rules generate events

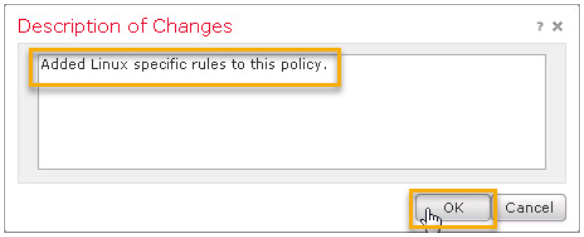
9839 rules drop and generate events

No recommendations have been generated. Click here to set up Firepower recommendations.

This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules

7. In the Description of Changes popup window give the following reason for the changes "**Added Linux specific rules to this policy.**" and then click **OK**.

Figure 378. Give justification for rule



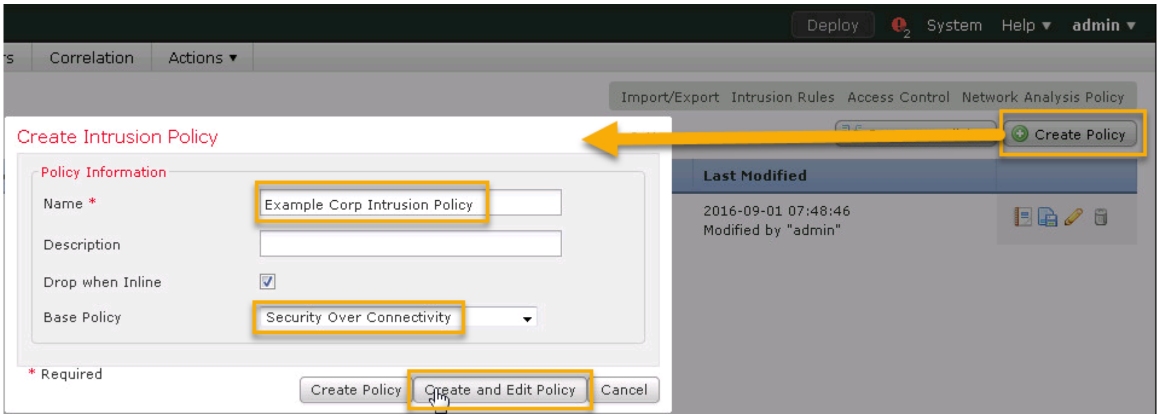
Description of Changes

Added Linux specific rules to this policy.

This second policy is an example of what you might do use for a global replacement of the Intrusion policy (instead of using one of the default policies that comes from Cisco). These are important as they can possibly improve the efficiency of your NGFW devices while at the same time better targeting those rules that best apply to your customer's network. That said, the NGFW devices need time to learn the customer's network so this type of change should probably be done on a follow-up visit and not during the initial deployment.

8. Click the **Create Policy** button again and use the following to create the policy:
    a. Name: **Example Corp Intrusion Policy**
    b. Base Policy: **Security over Connectivity**
9. Click the **Create and Edit Policy** button.

Figure 379. Create Intrusion Policy



2016-09-01 07:48:46
Modified by "admin"

Create Intrusion Policy

Policy Information

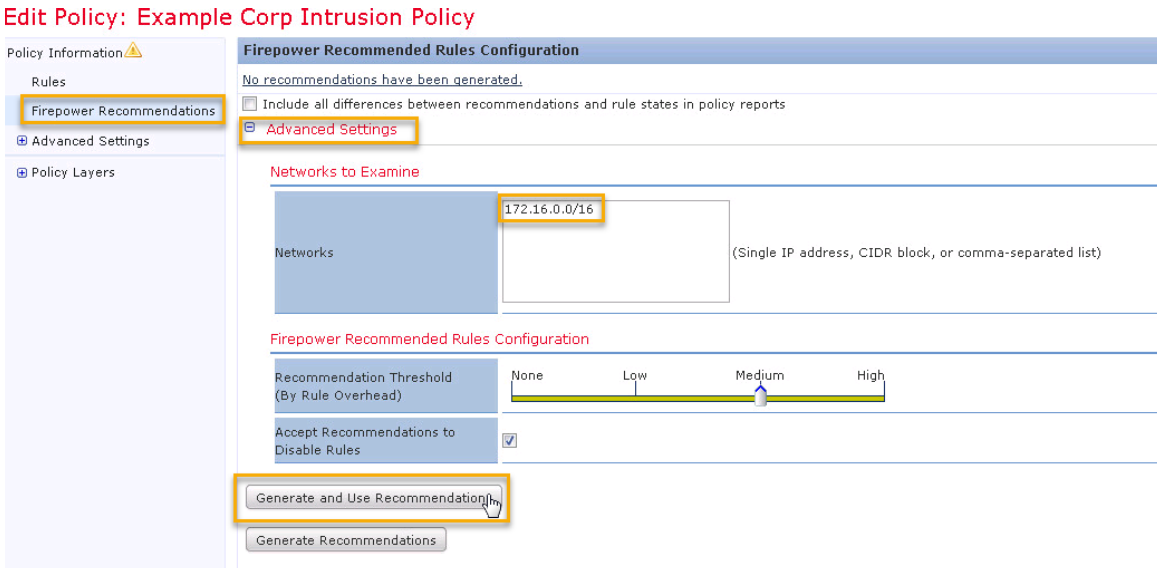
Name *	Example Corp Intrusion Policy
Description	
Drop when Inline	☑
Base Policy	Security Over Connectivity

* Required

10. Once the policy has been created click the **Firepower Recommendations** link from the left side menu.
11. Expand the **Advanced Settings** option in the right hand pane.
12. In the **Networks to Examine** field add **172.16.0.0/16** to better target the Example Corp networks.
13. Click the **Generate and Use Recommendations** button. (If this policy was already in production you might want to click the Generate Recommendations button first and see what changes are being suggested.)

Since this is a fairly fresh installation (and you only have a few hosts in the 172.16.0.0/16 network ranges) this would not be a good sample set for the Firepower Recommendations.

Figure 380. Build Firepower Recommendations


Edit Policy: Example Corp Intrusion Policy

Firepower Recommended Rules Configuration

No recommendations have been generated.

□ Include all differences between recommendations and rule states in policy reports

⊟ Advanced Settings

Networks to Examine

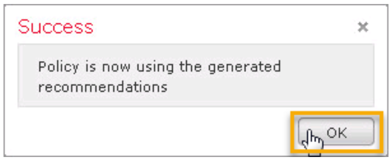
Networks	172.16.0.0/16	(Single IP address, CIDR block, or comma-separated list)

Firepower Recommended Rules Configuration

Recommendation Threshold (By Rule Overhead)	None Low [✓ Medium] High
Accept Recommendations to Disable Rules	☑

14. This process can take a minute or two. Click **OK** when the Success popup window appears.

Figure 381. Click OK

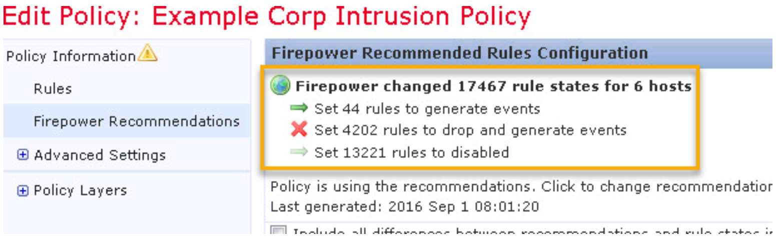


Success

Policy is now using the generated recommendations

15. Notice the changes that the Firepower Recommendations is recommending. It is modifying over 17,000 rules from the factory default rules in the Security over Connectivity policy! That should improve performance a bit.

Figure 382. View Recommendation’s Summary Info



Edit Policy: Example Corp Intrusion Policy

Firepower Recommended Rules Configuration

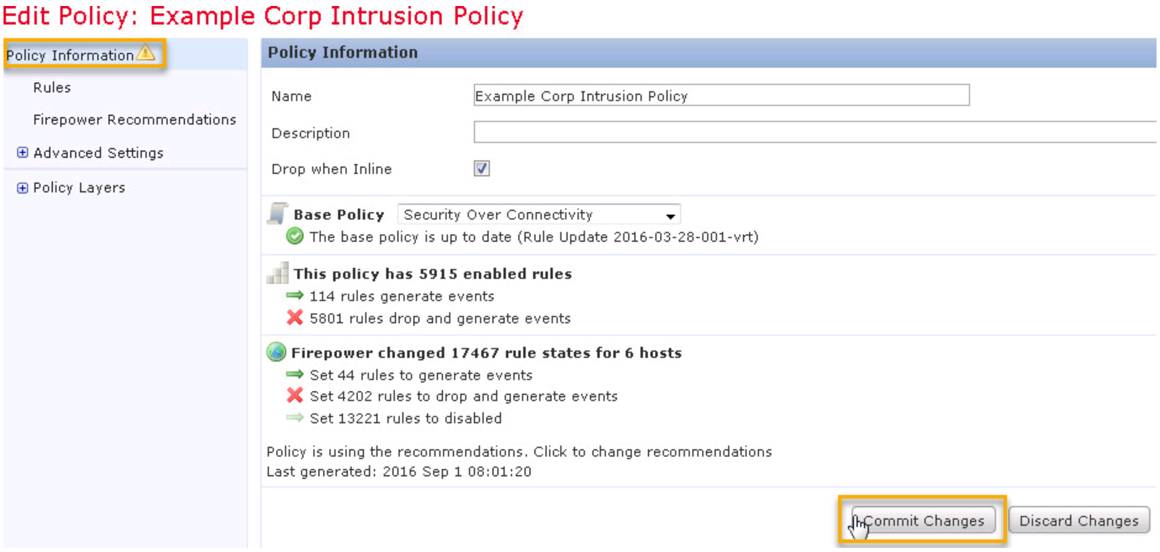
Firepower changed 17467 rule states for 6 hosts
- Set 44 rules to generate events
- Set 4202 rules to drop and generate events
- Set 13221 rules to disabled

Policy is using the recommendations. Click to change recommendatior
Last generated: 2016 Sep 1 08:01:20

16. Click the **Policy Information** link.

17. Click **Commit Changes**.

Figure 383. Commit Changes



Edit Policy: Example Corp Intrusion Policy

Policy Information

Name: Example Corp Intrusion Policy

Description:

Drop when Inline ☑

Base Policy: Security Over Connectivity

The base policy is up to date (Rule Update 2016-03-28-001-vrt)

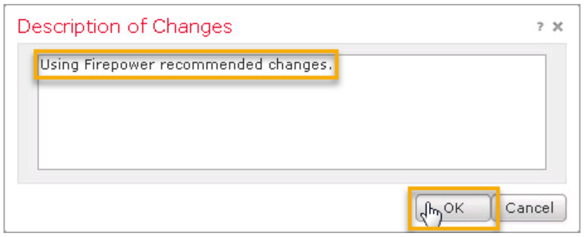
This policy has 5915 enabled rules
- 114 rules generate events
- 5801 rules drop and generate events

Firepower changed 17467 rule states for 6 hosts
- Set 44 rules to generate events
- Set 4202 rules to drop and generate events
- Set 13221 rules to disabled

Policy is using the recommendations. Click to change recommendations
Last generated: 2016 Sep 1 08:01:20

18. In the Description of Changes popup window type “**Using Firepower recommended changes.**” and click **OK**.

Figure 384. Add Comment



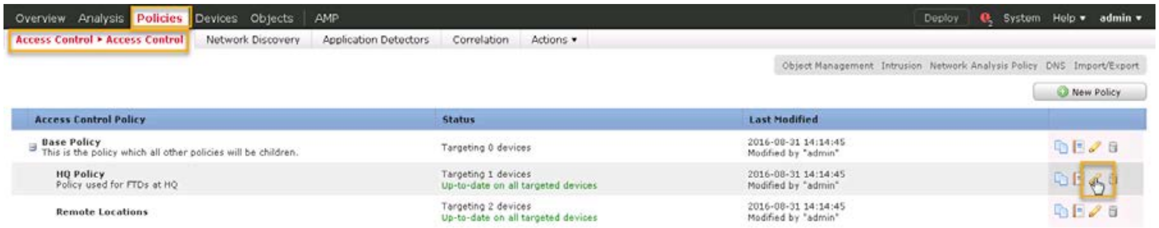
Description of Changes

Using Firepower recommended changes.

19. Time to apply the newly created Intrusion Policies. Navigate to **Policies > Access Control > Access Control**.

20. **Edit** the **HQ Policy**.

Figure 385. Edit HQ Policy ACP

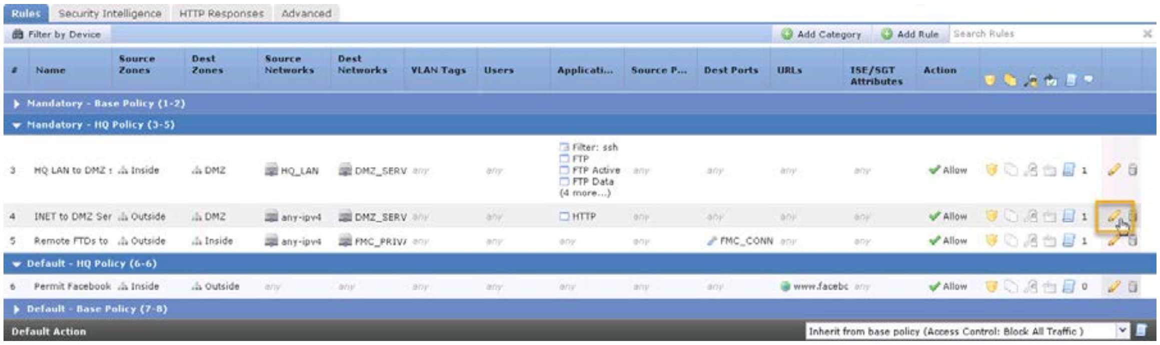


Overview Analysis Policies Devices Objects AMP
Deploy System Help ▾ admin ▾
Access Control ▸ Access Control
Network Discovery
Application Detectors
Correlation
Actions ▾
Object Management Intrusion Network Analysis Policy DNS Import/Export
New Policy

Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-08-31 14:14:45 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-08-31 14:14:45 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-08-31 14:14:45 Modified by "admin"

21. **Edit** the **INET to DMZ Server** rule (should be rule #4).

Figure 386. Edit Rule



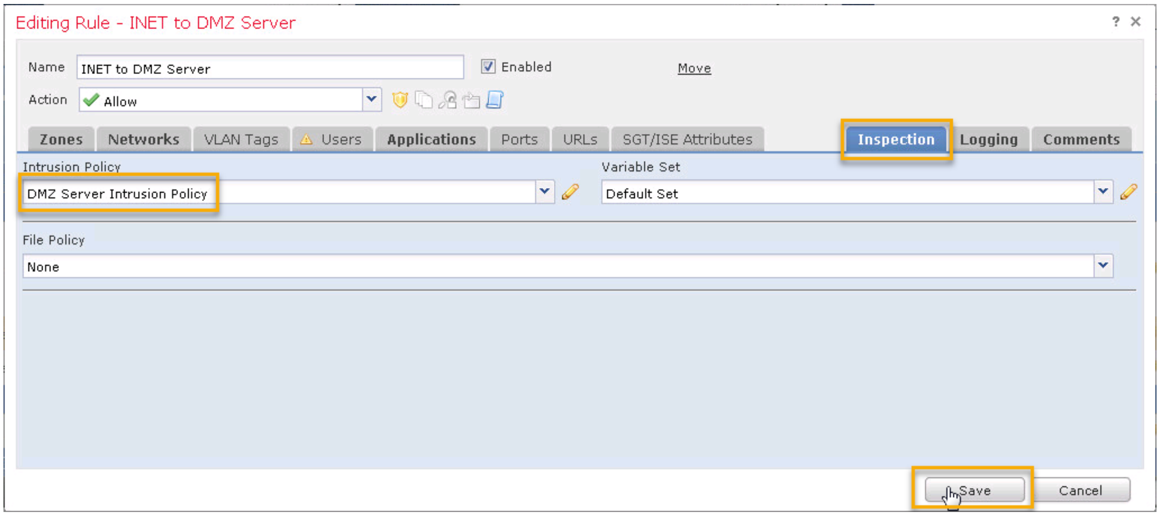
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
▸ Mandatory - Base Policy (1-2)														
▾ Mandatory - HQ Policy (3-5)														
3	HQ LAN to DMZ :	Inside	DMZ	HQ_LAN	DMZ_SERV	any	any	Filter: ssh FTP FTP Active FTP Data (4 more...)	any	any	any	any	✓ Allow	1
4	INET to DMZ Ser	Outside	DMZ	any-ipv4	DMZ_SERV	any	any	HTTP	any	any	any	any	✓ Allow	1
5	Remote FTDs to	Outside	Inside	any-ipv4	FMC_PRIV/	any	any	any	any	FMC_CONN	any	any	✓ Allow	1
▾ Default - HQ Policy (6-6)														
6	Permit Facebook	Inside	Outside	any	any	any	any	any	any	any	www.facebc	any	✓ Allow	0
▸ Default - Base Policy (7-8)														

Default Action: Inherit from base policy (Access Control: Block All Traffic)

22. Click the **Inspection tab** and select the **DMZ Server Intrusion Policy** for the Intrusion Policy.

23. Click **Save**.

Figure 387. Configure Inspection tab and Save



Editing Rule - INET to DMZ Server

Name: INET to DMZ Server ☑ Enabled Move

Action: ✓ Allow

Zones | Networks | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Intrusion Policy: DMZ Server Intrusion Policy

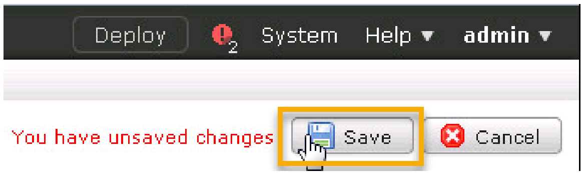
Variable Set: Default Set

File Policy: None

Save | Cancel

24. Click **Save** to save these changes to the FMC.

Figure 388. Save changes to FMC



You have unsaved changes

Save | Cancel

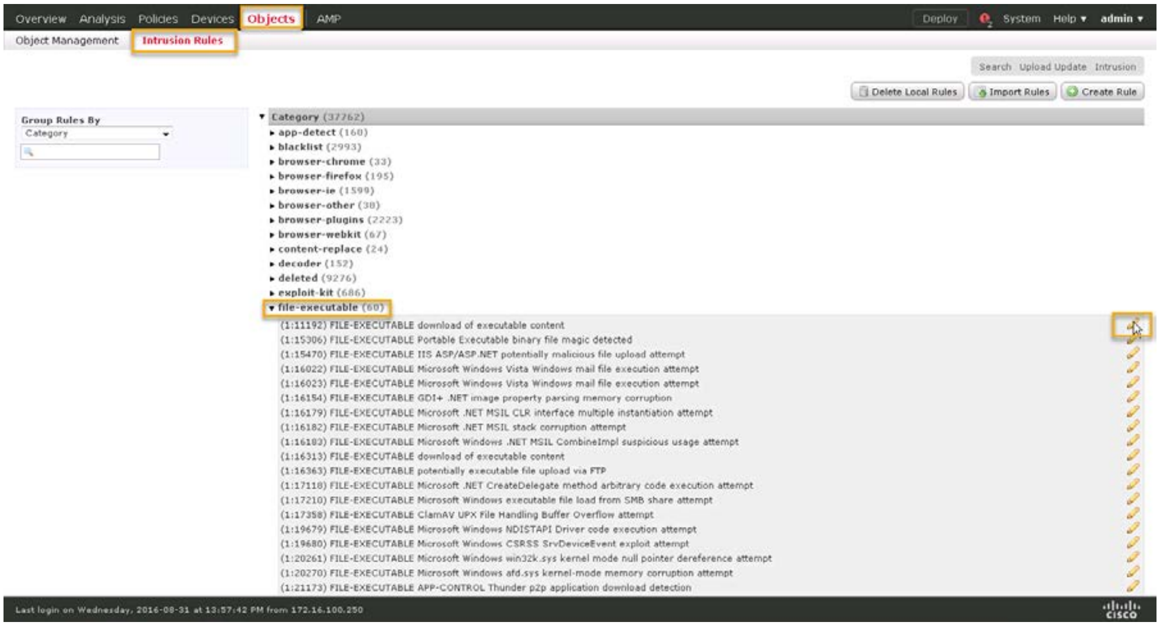
In the lab you don't have a method to test this DMZ Server Intrusion Policy but at least you have an understanding how to tune your intrusion policies and where to apply them.

Take note that the application of intrusion policies is done on a rule by rule basis. So, if Example Corp wanted to use the "Firepower Recommended Changes" intrusion policy you just created as their main intrusion policy then each Access Control Policy rule would need to be edited to specify this new policy. The good thing about having a "per ACP rule" level of granularity for which intrusion policy is being used is that you can create VERY customized intrusion policies that are designed based on what devices/applications are matching a specific ACP rule.

Variable Sets

25. A Variable Sets is a set of variables that can be used to customize the IPs, ports, and protocols used in certain Intrusion Rules. To see an example of this navigate to **Objects > Intrusion Rules**, expand the **file-executable category** and edit the first item: **(1:11192) FILE-EXECUTABLE** download of executable content.

Figure 389. Edit an Intrusion Rule Object

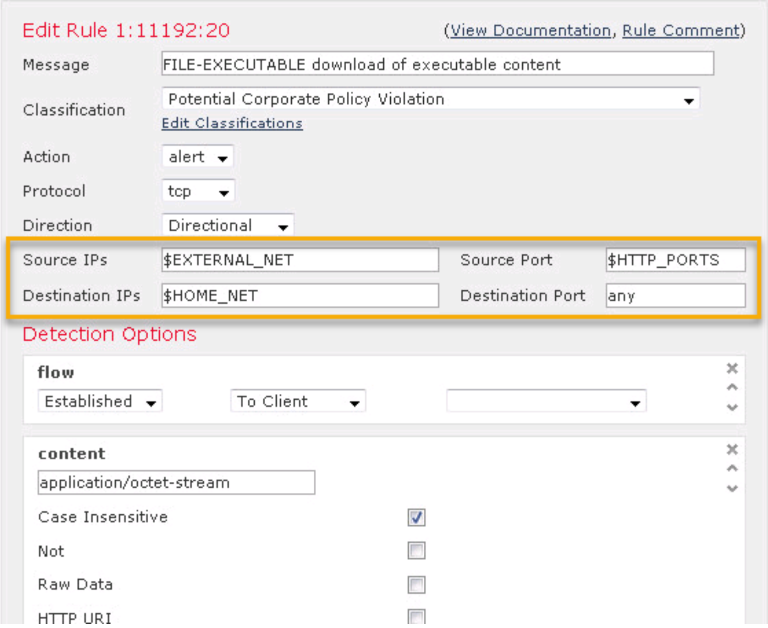


- ▾ Category (37762)
  - ▸ app-detect (160)
  - ▸ blacklist (2993)
  - ▸ browser-chrome (33)
  - ▸ browser-firefox (195)
  - ▸ browser-ie (1599)
  - ▸ browser-other (30)
  - ▸ browser-plugins (2223)
  - ▸ browser-webkit (67)
  - ▸ content-replace (24)
  - ▸ decoder (152)
  - ▸ deleted (9276)
  - ▸ exploit-kit (686)
  - ▾ file-executable (60)
    - (1:11192) FILE-EXECUTABLE download of executable content
    - (1:15306) FILE-EXECUTABLE Portable Executable binary file magic detected
    - (1:15470) FILE-EXECUTABLE IIS ASP/ASP.NET potentially malicious file upload attempt
    - (1:16022) FILE-EXECUTABLE Microsoft Windows Vista Windows mail file execution attempt
    - (1:16023) FILE-EXECUTABLE Microsoft Windows Vista Windows mail file execution attempt
    - (1:16154) FILE-EXECUTABLE GDI+ .NET image property parsing memory corruption
    - (1:16179) FILE-EXECUTABLE Microsoft .NET MSIL CLR interface multiple instantiation attempt
    - (1:16182) FILE-EXECUTABLE Microsoft .NET MSIL stack corruption attempt
    - (1:16183) FILE-EXECUTABLE Microsoft Windows .NET MSIL CombineImpl suspicious usage attempt
    - (1:16313) FILE-EXECUTABLE download of executable content
    - (1:16363) FILE-EXECUTABLE potentially executable file upload via FTP
    - (1:17118) FILE-EXECUTABLE Microsoft .NET CreateDelegate method arbitrary code execution attempt
    - (1:17210) FILE-EXECUTABLE Microsoft Windows executable file load from SMB share attempt
    - (1:17358) FILE-EXECUTABLE ClamAV UPX File Handling Buffer Overflow attempt
    - (1:19679) FILE-EXECUTABLE Microsoft Windows NDISTAPI Driver code execution attempt
    - (1:19680) FILE-EXECUTABLE Microsoft Windows CSRSS SrvDeviceEvent exploit attempt
    - (1:20261) FILE-EXECUTABLE Microsoft Windows win32k.sys kernel mode null pointer dereference attempt
    - (1:20270) FILE-EXECUTABLE Microsoft Windows afd.sys kernel-mode memory corruption attempt
    - (1:21173) FILE-EXECUTABLE APP-CONTROL Thunder p2p application download detection

Last login on Wednesday, 2016-08-31 at 13:57:42 PM from 172.16.100.250

26. Notice the **$EXTERNAL_NET**, **$HTTP_PORTS**, and **$HOME_NET** variables being used in this rule.

Figure 390. Use of Variable Set variables



Edit Rule 1:11192:20 (View Documentation, Rule Comment)

Message	FILE-EXECUTABLE download of executable content		
Classification	Potential Corporate Policy Violation Edit Classifications		
Action	alert		
Protocol	tcp		
Direction	Directional		
Source IPs	$EXTERNAL_NET	Source Port	$HTTP_PORTS
Destination IPs	$HOME_NET	Destination Port	any

Detection Options

flow

Established | To Client |

content

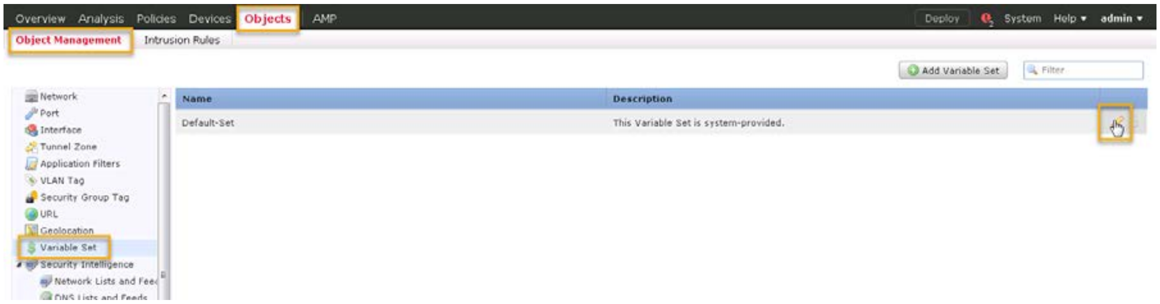
application/octet-stream

Case Insensitive	☑
Not	□
Raw Data	□
HTTP URI	□

27. Navigate to **Objects > Object Management** and from the list of item in the left column select **Variable Set**.

28. The Default-Set is the default variable set that is being used throughout the configurations we've created or used so far. Instead of creating a new Variable Set and needing to apply it everywhere it is best just to modify the Default-Set to match your network's settings. **Edit** the **Default-Set**.

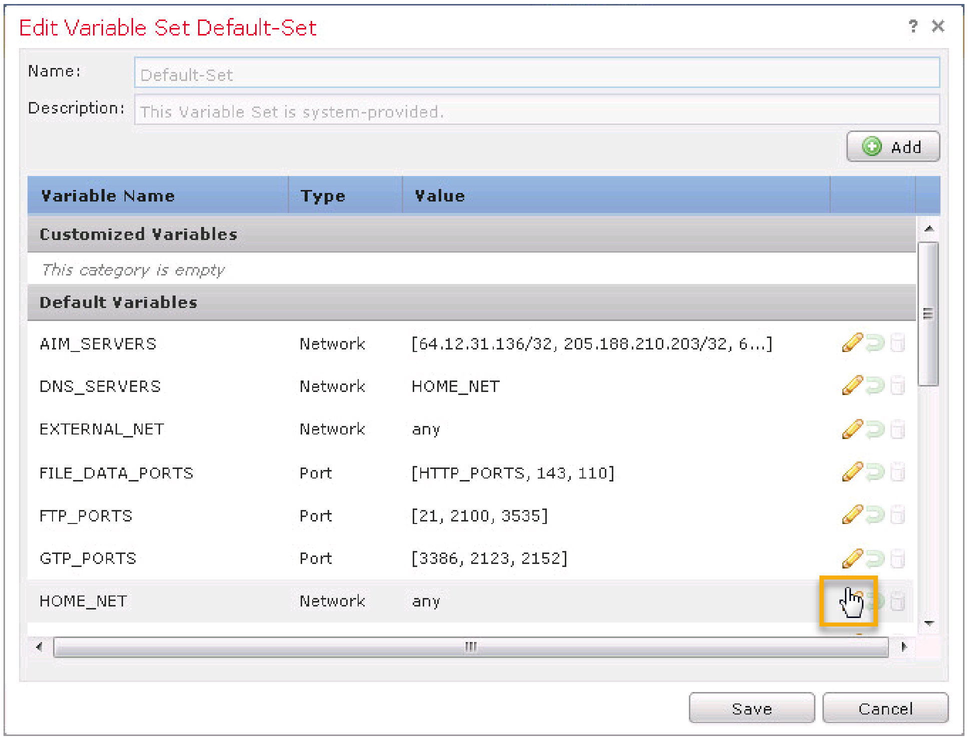
Figure 391. Edit Default Set Variable Set



Name	Description
Default-Set	This Variable Set is system-provided.

29. In the Edit Variable Set Default-Set popup window **edit** the **HOME_NET** variable.

Figure 392. Edit HOME_NET



Name: Default-Set

Description: This Variable Set is system-provided.

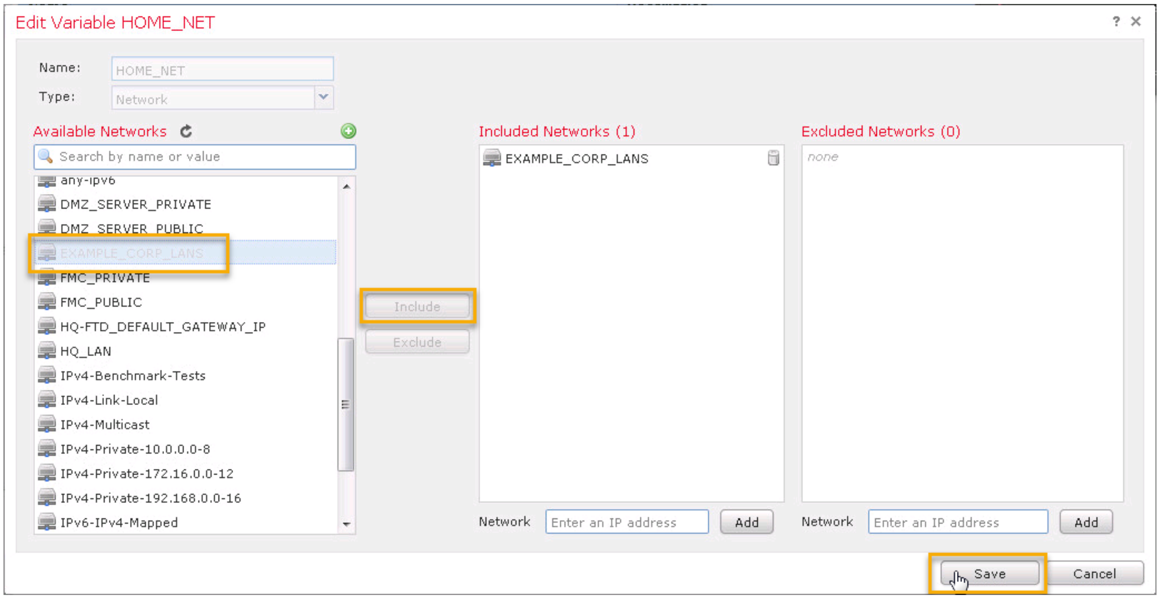
Variable Name	Type	Value
Customized Variables		
This category is empty		
Default Variables		
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
EXTERNAL_NET	Network	any
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]
HOME_NET	Network	any

30. Use the following to customize the HOME_NET variable:

    a. From the **Available Networks** select **EXAMPLE_CORP_LANS** and click the **Include** button.

    b. Click **Save**.

Figure 393. Save HOME_NET changes



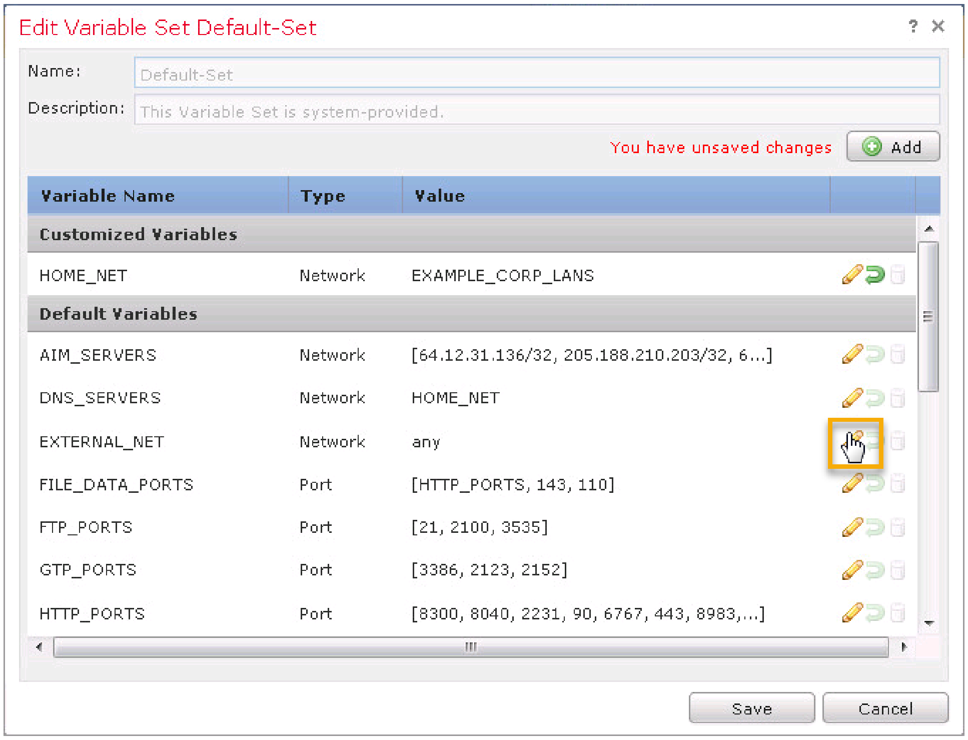
Edit Variable HOME_NET

Name: HOME_NET

Type: Network

31. **Edit** the **EXTERNAL_NET** variable.

Figure 394. Edit EXTERNAL_NET



Edit Variable Set Default-Set

Name: Default-Set

Description: This Variable Set is system-provided.

You have unsaved changes

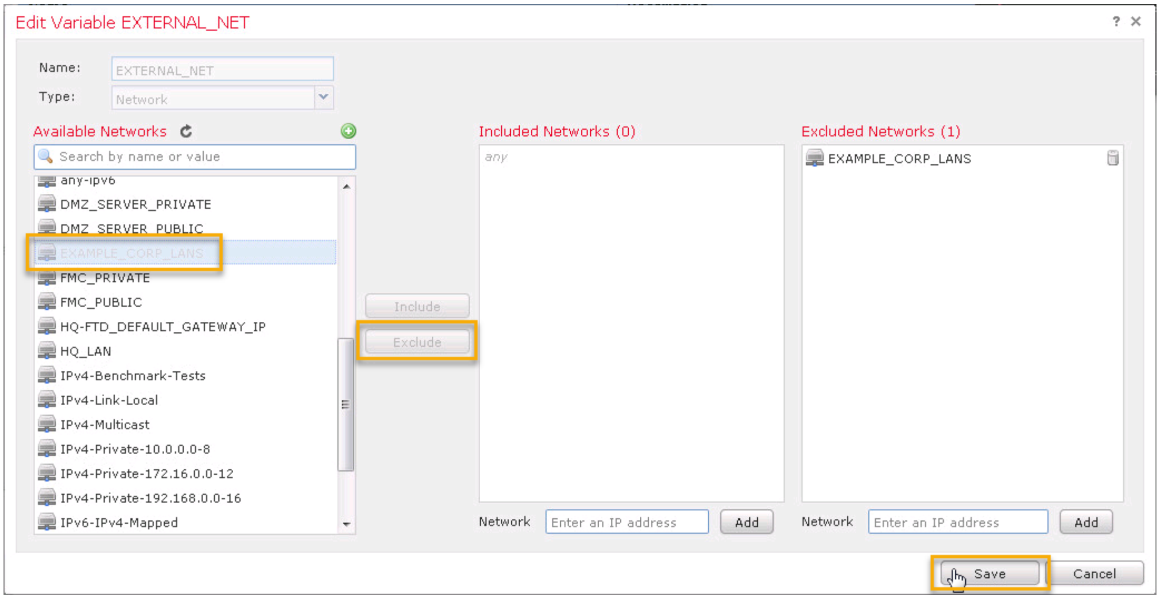
Variable Name	Type	Value
Customized Variables		
HOME_NET	Network	EXAMPLE_CORP_LANS
Default Variables		
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
EXTERNAL_NET	Network	any
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]

32. Use the following to customize the EXTERNAL_NET variable:

    a. From the **Available Networks** select **EXAMPLE_CORP_LANS** and click the **Exclude** button.

    b. Click **Save**.

Figure 395. Save EXTERNAL_NET



Edit Variable EXTERNAL_NET

Name: EXTERNAL_NET

Type: Network

Available Networks

Search by name or value

- any-ipv6
- DMZ_SERVER_PRIVATE
- DMZ_SERVER_PUBLIC
- EXAMPLE_CORP_LANS
- FMC_PRIVATE
- FMC_PUBLIC
- HQ-FTD_DEFAULT_GATEWAY_IP
- HQ_LAN
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv6-IPv4-Mapped

Included Networks (0)

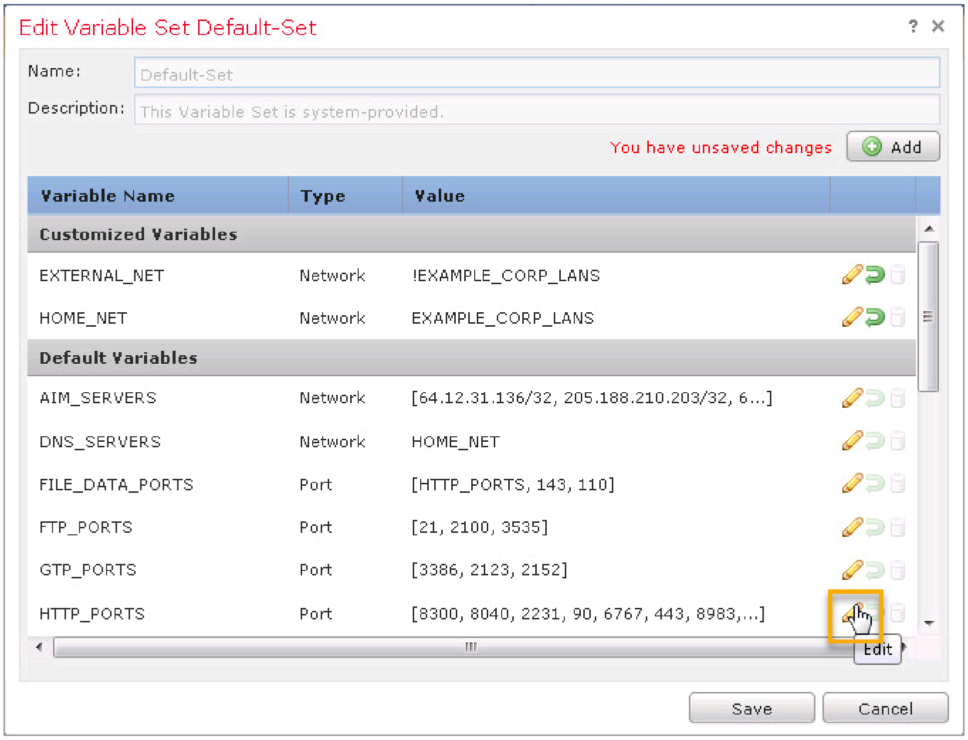
any

Excluded Networks (1)

EXAMPLE_CORP_LANS

33. Let's pretend that Example Corp has a special HTTP application that runs on port 8383. **Edit** the **HTTP_PORTS** variable.

Figure 396. Edit HTTP_PORTS



Name: Default-Set

Description: This Variable Set is system-provided.

You have unsaved changes

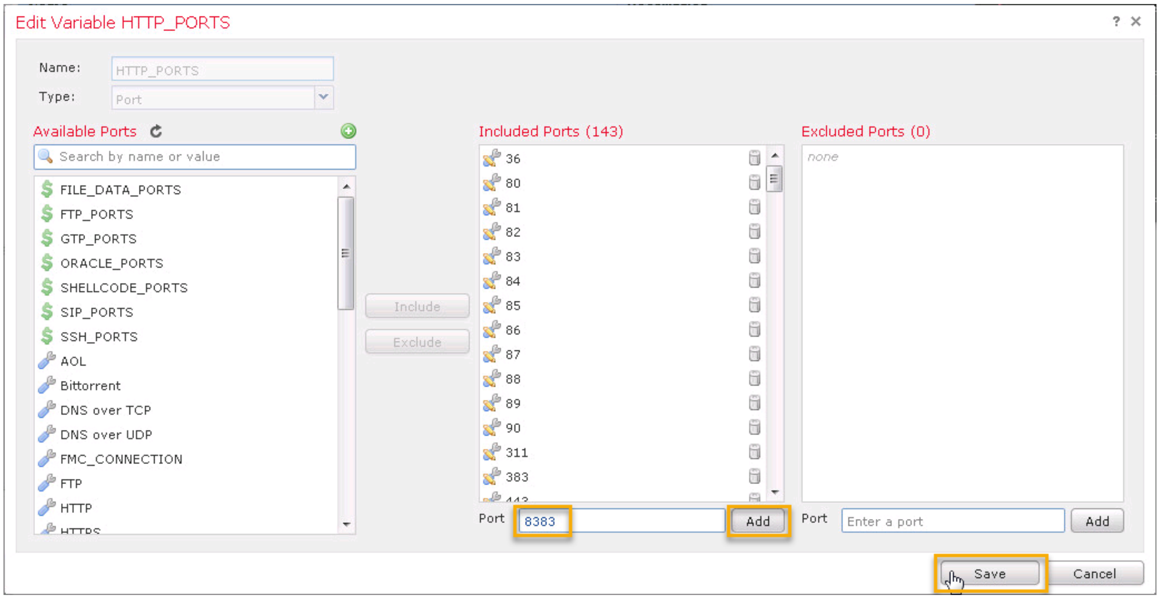
Variable Name	Type	Value
Customized Variables		
EXTERNAL_NET	Network	!EXAMPLE_CORP_LANS
HOME_NET	Network	EXAMPLE_CORP_LANS
Default Variables		
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]

34. Use the following to customize the HTTP_PORTS variable:

    a. In the **Port field** under the **Included Ports** column type **8383** and click **Add**.

    b. Click **Save**.

Figure 397. Save HTTP_PORTS variable



Edit Variable HTTP_PORTS

Name: HTTP_PORTS

Type: Port

Available Ports

Search by name or value

FILE_DATA_PORTS
FTP_PORTS
GTP_PORTS
ORACLE_PORTS
SHELLCODE_PORTS
SIP_PORTS
SSH_PORTS
AOL
Bittorrent
DNS over TCP
DNS over UDP
FMC_CONNECTION
FTP
HTTP
HTTPS

Included Ports (143)

36
80
81
82
83
84
85
86
87
88
89
90
311
383
443

Port: 8383

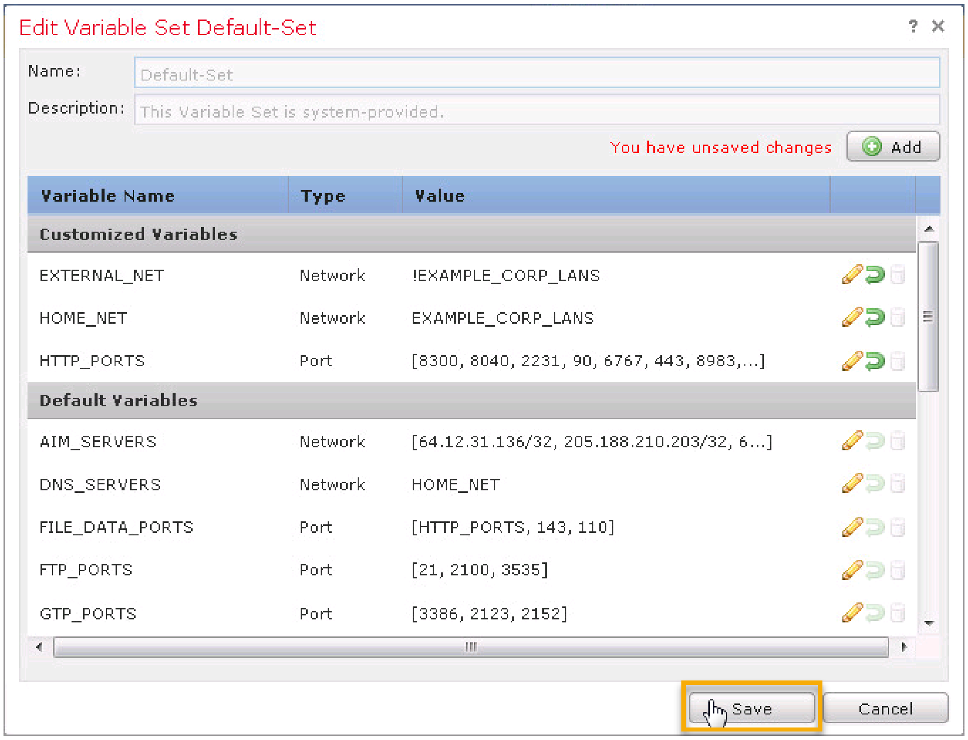
Excluded Ports (0)

none

Port: Enter a port

35. Click **Save** to save the Default-Set variable set.

Figure 398. Save Default Set Variable Set



Edit Variable Set Default-Set

Name: Default-Set

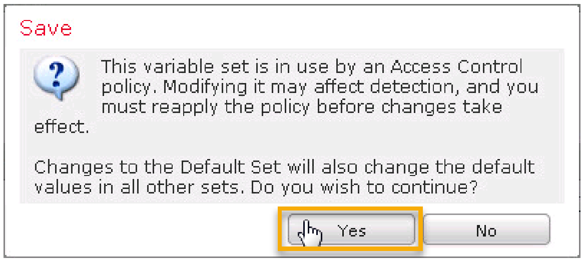
Description: This Variable Set is system-provided.

You have unsaved changes

Variable Name	Type	Value
Customized Variables		
EXTERNAL_NET	Network	!EXAMPLE_CORP_LANS
HOME_NET	Network	EXAMPLE_CORP_LANS
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]
Default Variables		
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]

36. In the popup warning window click **Yes** to change the default values.

Figure 399. Click Yes



Save

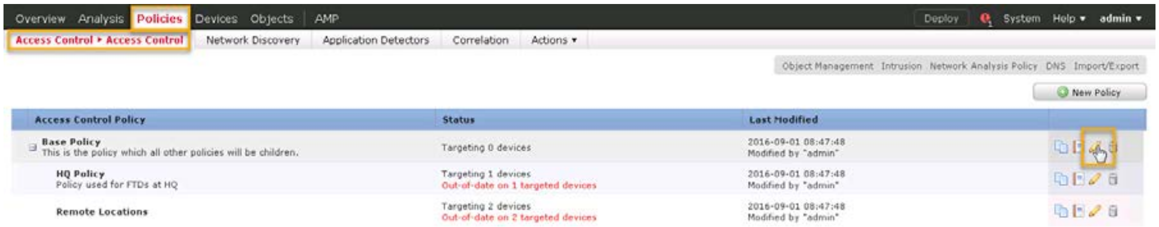
This variable set is in use by an Access Control policy. Modifying it may affect detection, and you must reapply the policy before changes take effect.

Changes to the Default Set will also change the default values in all other sets. Do you wish to continue?

37. As mentioned previously the Default-Set variable set is already being applied but to show you where you can change which variable set is being used navigate to **Policies > Access Control > Access Control**.

38. **Edit** the **Base Policy**.

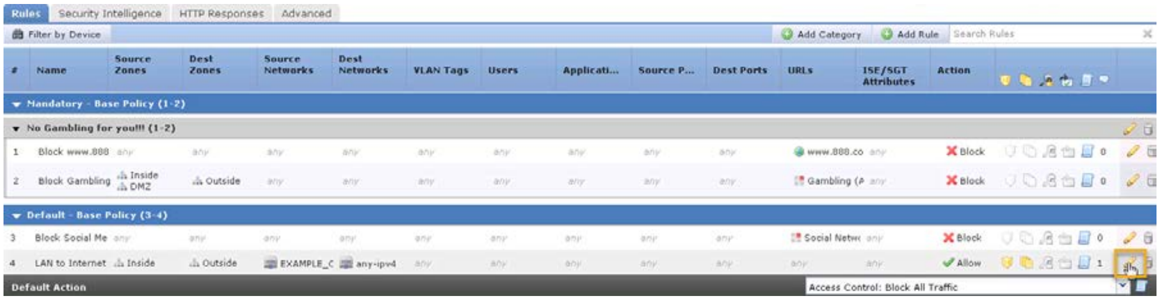
Figure 400. Edit Base Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-09-01 08:47:48 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Out-of-date on 1 targeted devices	2016-09-01 08:47:48 Modified by "admin"
Remote Locations	Targeting 2 devices Out-of-date on 2 targeted devices	2016-09-01 08:47:48 Modified by "admin"

39. **Edit** one of the rules.

Figure 401. Edit a rule



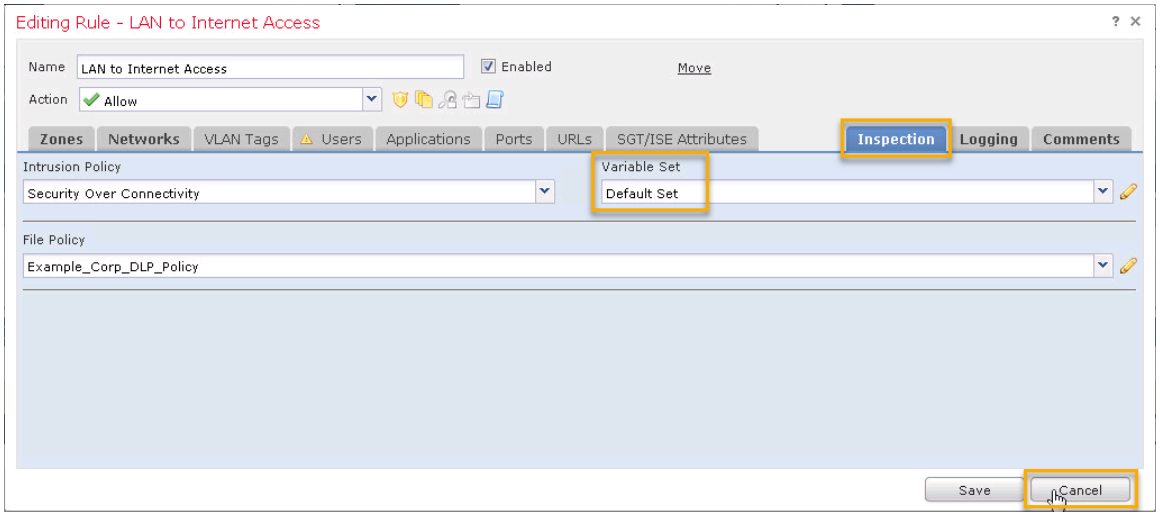
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
▾ Mandatory - Base Policy (1-2)														
▾ No Gambling for you!!! (1-2)														
1	Block www.888	any	any	any	any	any	any	any	any	any	www.888.co	any	✗ Block	0
2	Block Gambling	Inside DMZ	Outside	any	any	any	any	any	any	any	Gambling (A	any	✗ Block	0
▾ Default - Base Policy (3-4)														
3	Block Social Me	any	any	any	any	any	any	any	any	any	Social Netw	any	✗ Block	0
4	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✓ Allow	1

Default Action: Access Control: Block All Traffic

40. On the **Inspection tab** there is a field to set the Variable Set for this rule, and as you can see the Default Set is currently being used.

41. Click **Cancel** to exit editing this rule. (If asked, click **Yes** to not save changes.)

Figure 402. See where Variable Set is used



Editing Rule - LAN to Internet Access

Name: LAN to Internet Access ☑ Enabled

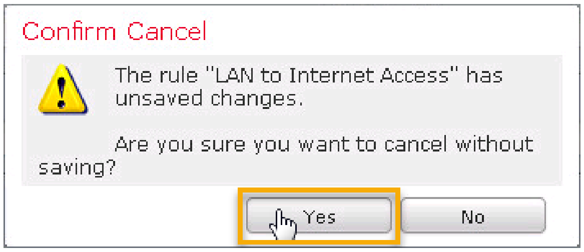
Action: Allow

Intrusion Policy: Security Over Connectivity

Variable Set: Default Set

File Policy: Example_Corp_DLP_Policy

Figure 403. Confirm Cancel



Confirm Cancel

The rule "LAN to Internet Access" has unsaved changes.

Are you sure you want to cancel without saving?

42. Click **Deploy**, select **all the FTD** devices, and then click **Deploy**. (Since you haven’t deployed since before the Intrusion policy application in the previous section this will deploy those changes as well as the changes you just made to the Default-Set variable set.)

Scenario Summary

Applying a customized Intrusion Policy can help focus a particular set of rules toward a particular device (or group of devices) in a network as well as reduce overhead of unneeded inspections. Additionally, with the information that the NGFW collects about the devices, ports, and protocols used in a network (via Network Discovery, which you modified/configured back in Scenario 3), the Firepower Recommendations configuration of an Intrusion Policy could be used to further tune a policy to a specific network. Bear in mind though that since each rule within an Access Control Policy could potentially have its own Intrusion Policy but that would make troubleshooting a nightmare. Try to use caution when customizing Intrusion Policies.

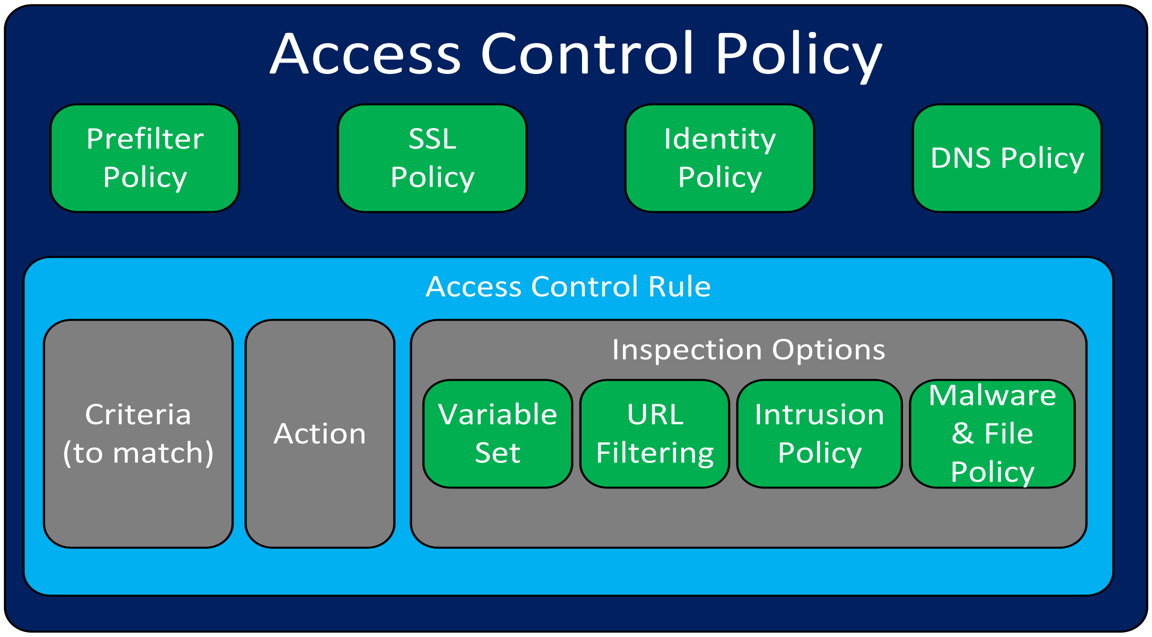
Cisco strongly recommends that you customize the Variable Set to better match your customer's network design. At a minimum modifying the HOME_NET and EXTERNAL_NET would provide a more focused view of your network.

Intermission #2

Before continuing with the lab I want to take a moment and review and collate all the policies you've just worked with (and more).

Each policy gets associated with an Access Control Policy in one way or another. Some are applied directly to the ACP whereas others are associated with a specific rule within an ACP. Use the following diagram to get an idea of how all the policies are applied.

Figure 404. ACP Diagram



This lab only introduces the ACP Rules, SSL Policy, URL Filtering, Intrusion Policy, and Malware & File Policy items shown above. As you can see there are more things to learn.

Scenario 10. Configure Platform Settings

Scenario Description

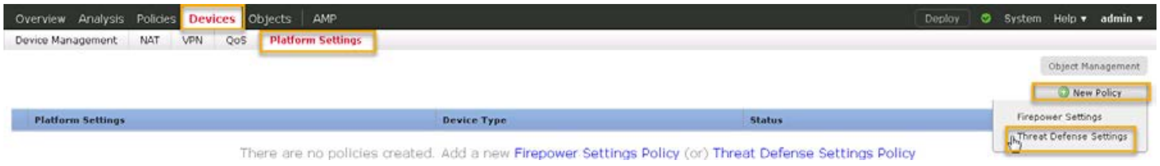
One of the great things about having centralized management is that you can apply a common policy across multiple devices. The Platform Settings options are just one of these settings that gives you the power to configure a common “experience” across all the FTD devices in the network.

Example Corp wants to permit SSH to its FTD device’s data plane IP addresses and have a common SMTP server that is used by all FTD devices. They also would like to increase the syslog buffer size to store more messages and instead of overwriting the overflow messages export them to an FTP server.

Configure Custom Platform Settings for Example Corp FTD Devices

1. Navigate to **Devices > Platform Settings**.
2. Click on **New Policy** and then select **Threat Defense Settings** from the dropdown list.

Figure 405. Create new policy



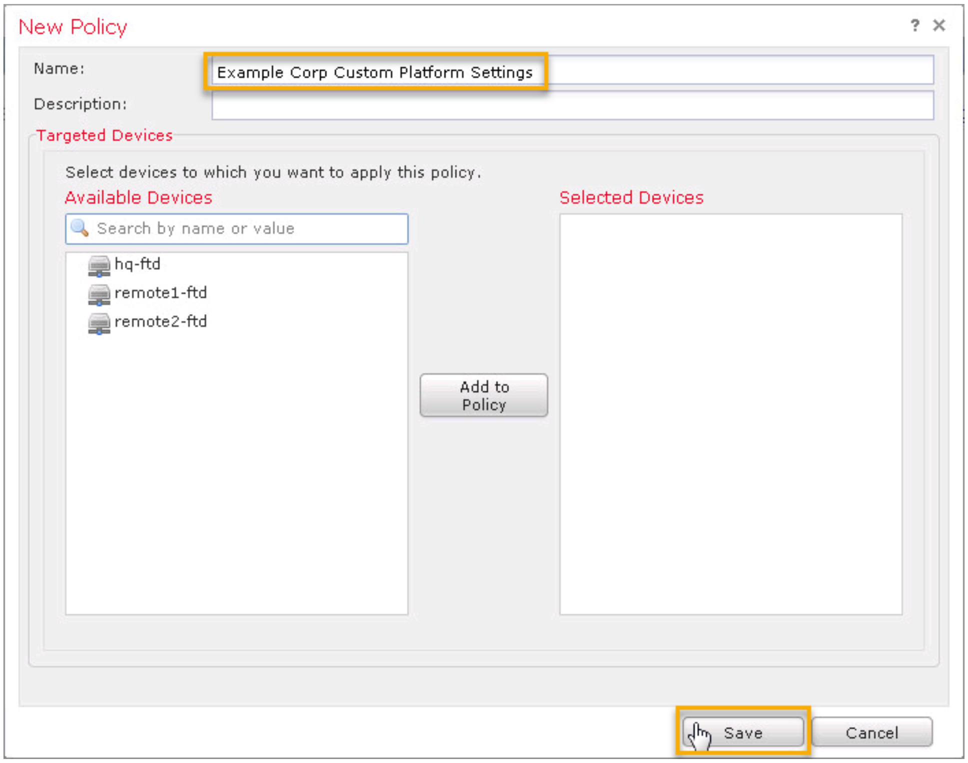
There are no policies created. Add a new Firepower Settings Policy (or) Threat Defense Settings Policy

3. Use the following to fill out the popup window:

   a. Name: **Example Corp Custom Platform Settings**

   b. Click **Save**. (You will associate these settings to the FTD devices later.)

Figure 406. Save policy



New Policy

Name: Example Corp Custom Platform Settings

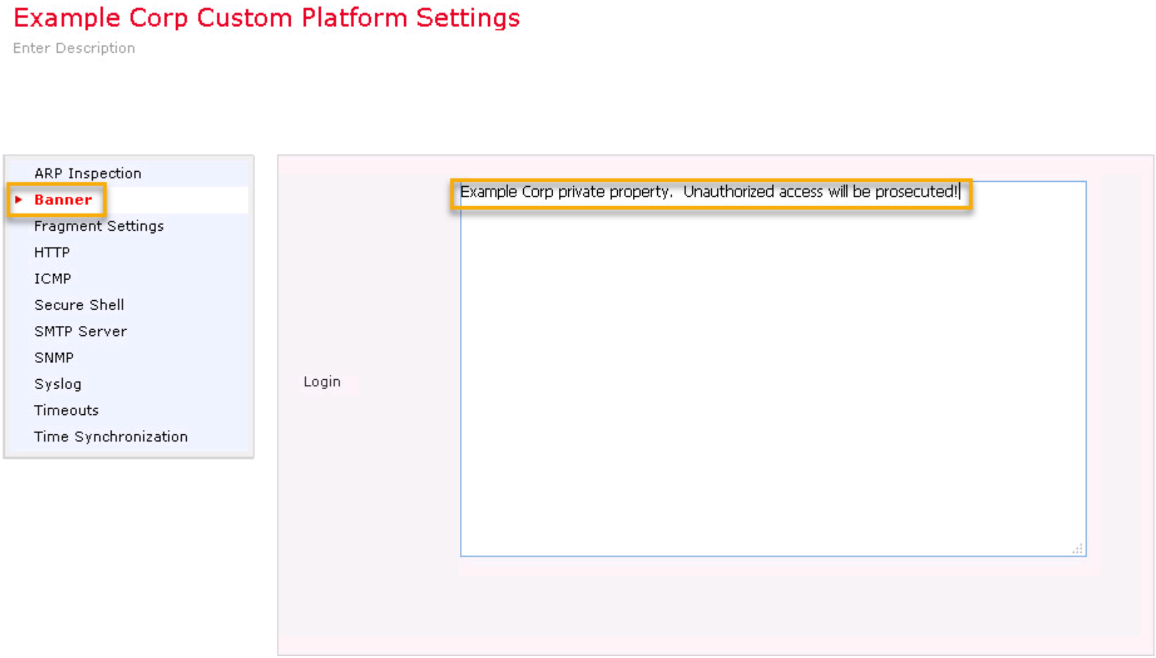
Description:

Targeted Devices

Select devices to which you want to apply this policy.

4. Click the **Banner** menu item and fill in the field with the following: **Example Corp private property. Unauthorized access will be prosecuted!**

Figure 407. Configure Banner



Example Corp Custom Platform Settings

Enter Description

Login: Example Corp private property. Unauthorized access will be prosecuted!

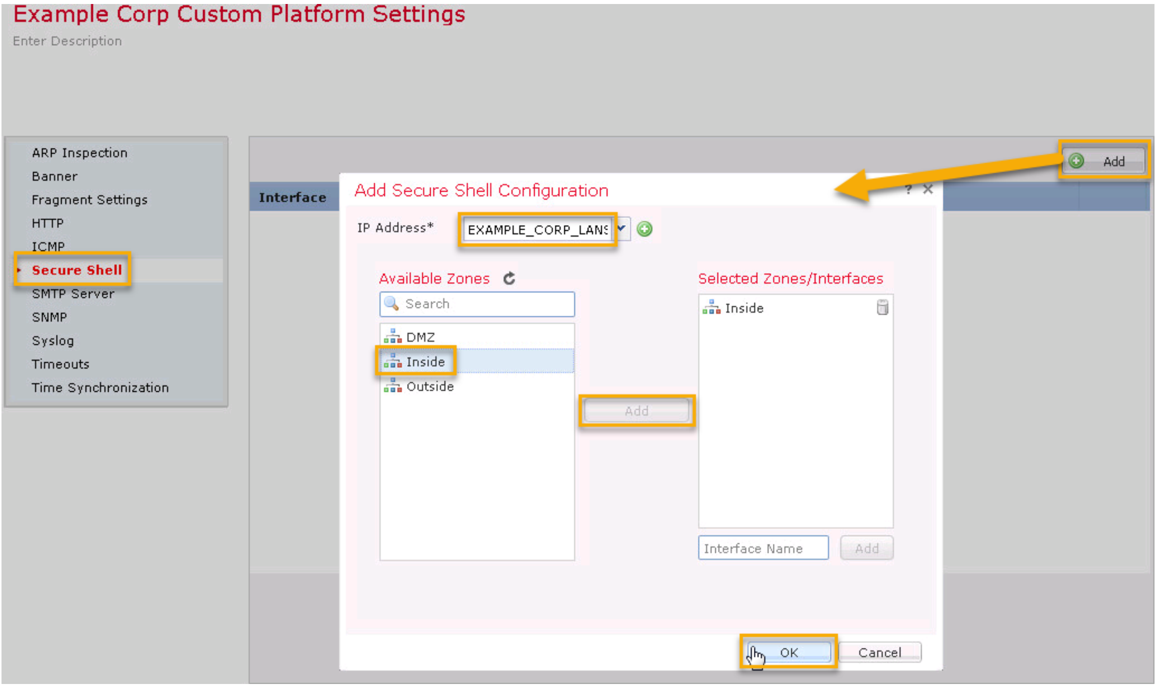
5. Click the **Secure Shell** menu item and then click **Add**.

   a. IP Address: **EXAMPLE_CORP_LANS**

   b. Add the **Inside** zone to **Selected Zones/Interfaces**.

   c. Click **OK**.

Figure 408. Configure SSH



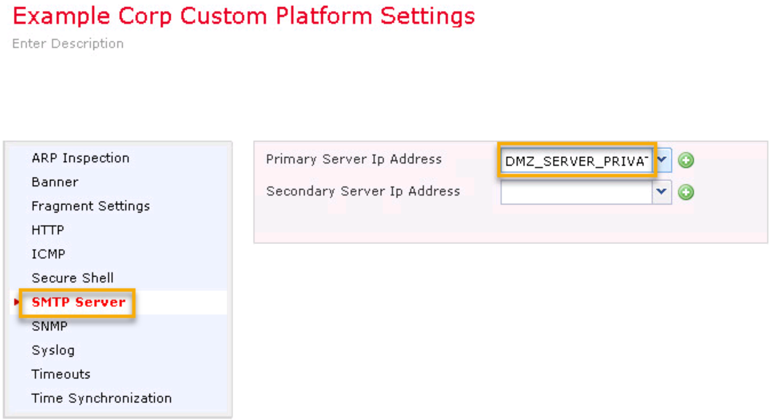
Example Corp Custom Platform Settings

Enter Description

6. Click the **SMTP Server** menu item:

   a. Primary Server Ip Address: **DMZ_SERVER_PRIVATE** (This server isn't actually running an SMTP service but you will configure this under the assumption that it is one of Example Corp's email servers.)

Figure 409. Configure SMTP Server



Example Corp Custom Platform Settings

Enter Description

Primary Server Ip Address: DMZ_SERVER_PRIVA

Secondary Server Ip Address:

7. Click the **Syslog** menu item:

8. On the **Logging Setup tab**:

    a. Enable Logging: **Checked**

    b. Memory Size of the Internal Buffer: **8192** (Once a log file reaches this point it will either be overwritten or copied to the FTP Server, based on the information filled in below.)

    c. FTP Server Buffer Wrap: **Checked**

    d. IP Address: **DMZ_SERVER_PRIVATE**

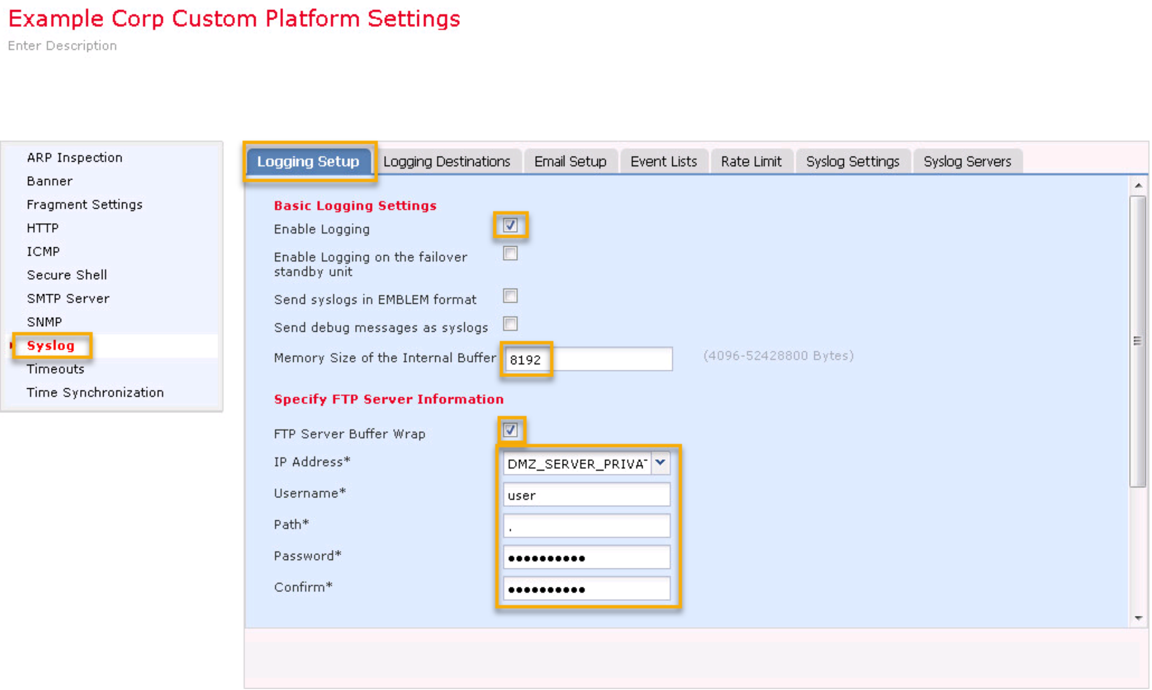
    e. Username: **user**

    f. Path: **.** (In Linux/UNIX the . "dot" represents the current directory.)

    g. Password: **C1sco12345**

    h. Confirm: **C1sco12345**

Figure 410. Part 1 Configure Syslog



Enable Logging ☑

Enable Logging on the failover standby unit □

Send syslogs in EMBLEM format □

Send debug messages as syslogs □

Memory Size of the Internal Buffer 8192 (4096-52428800 Bytes)

FTP Server Buffer Wrap ☑

IP Address* DMZ_SERVER_PRIVA

Username* user

Path* .

Password* ●●●●●●●●●●

Confirm* ●●●●●●●●●●

How will the remote1-ftd and remote2-ftd devices be able to send their overflow logs to the DMZ_SERVER_PRIVATE IP address? They won't, not at least until we get the VPN configured.

9. On the **Logging Destinations tab**:

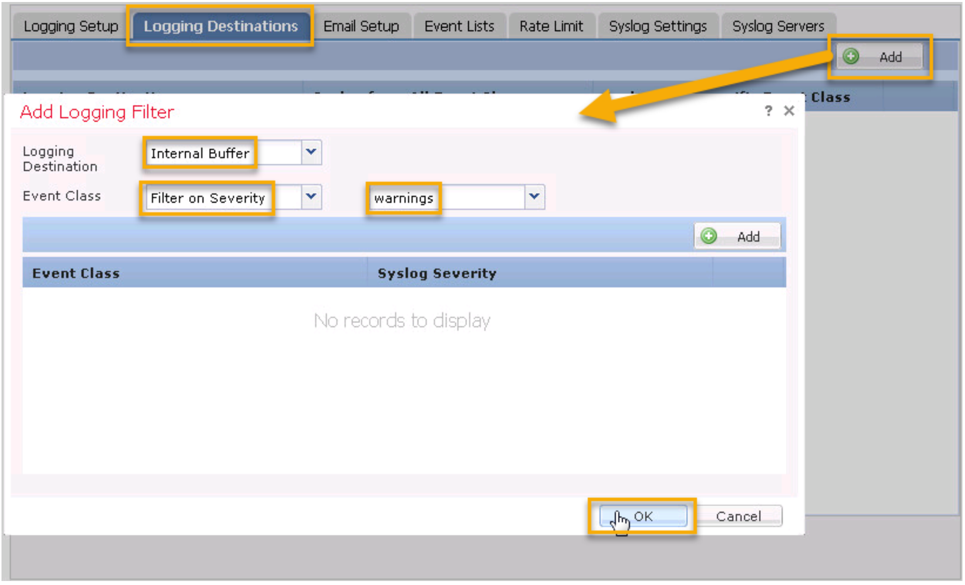
   a. Click **Add**.

      i. Logging Destination: **Internal Buffer**

      ii. Event Class: **Filter on Severity** and then **warnings.**

      iii. Click **OK**.

Figure 411. Configure Logging Destinations



Add Logging Filter

Logging Destination: Internal Buffer

Event Class: Filter on Severity   warnings

Event Class	Syslog Severity

No records to display

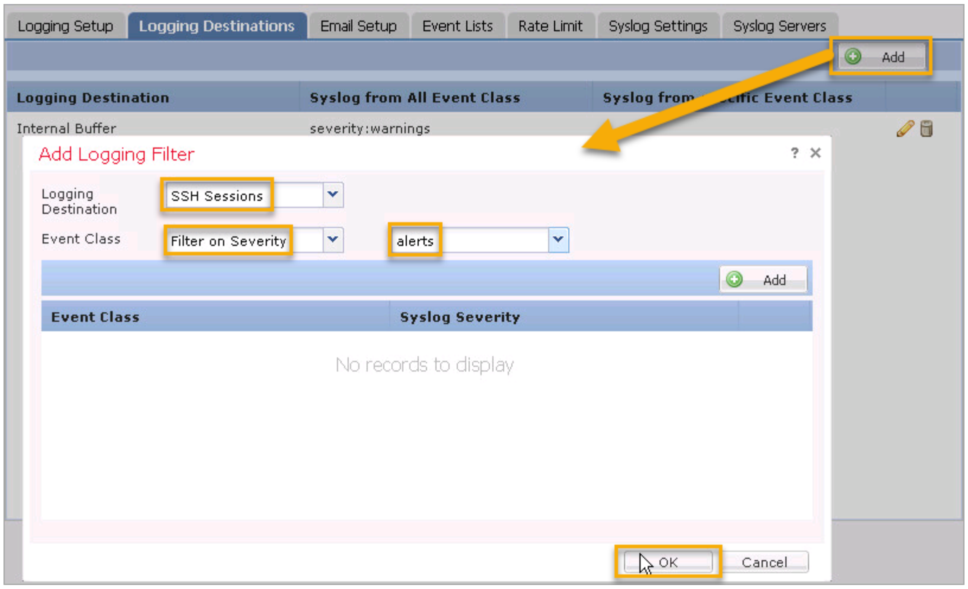
b. Click **Add**.

i. Logging Destination: **SSH Sessions**

ii. Event Class: **Filter on Severity** and then **alerts.**

iii. Click **OK**.

Figure 412. Configure Logging Destinations



Logging Destination	Syslog from All Event Class	Syslog from ...cific Event Class
Internal Buffer	severity:warnings	

Logging Destination: SSH Sessions

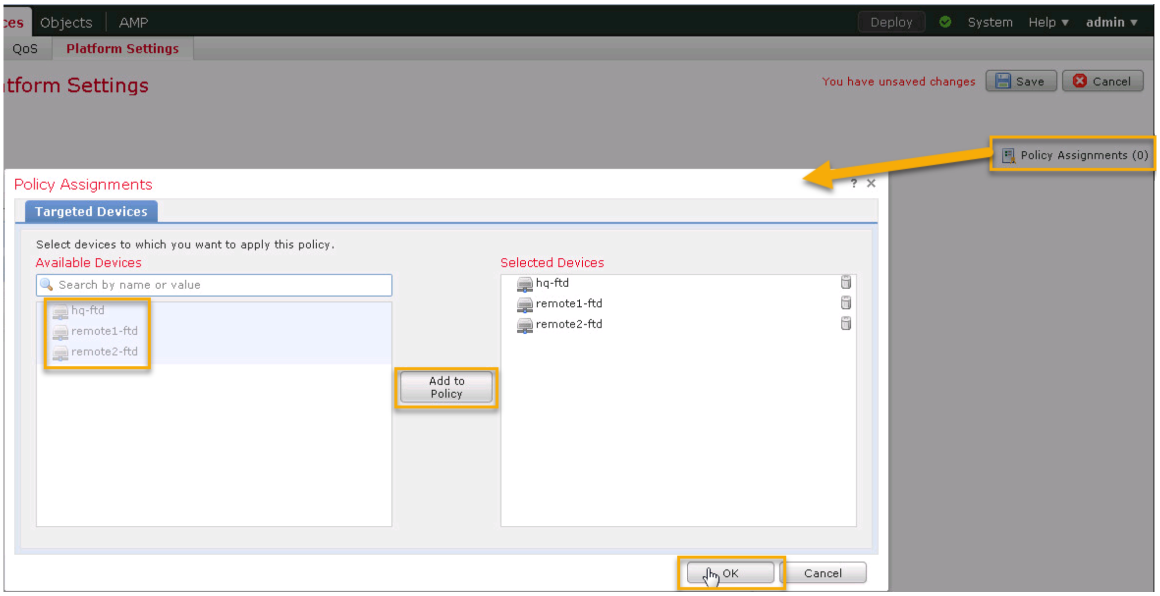
Event Class: Filter on Severity | alerts

Event Class	Syslog Severity

No records to display

10. Click **Policy Assignments**. Select **all the FTD** devices, click **Add to Policy**, and then click **OK**.

Figure 413. Assign Policy



You have unsaved changes

Select devices to which you want to apply this policy.

Available Devices
- hq-ftd
- remote1-ftd
- remote2-ftd

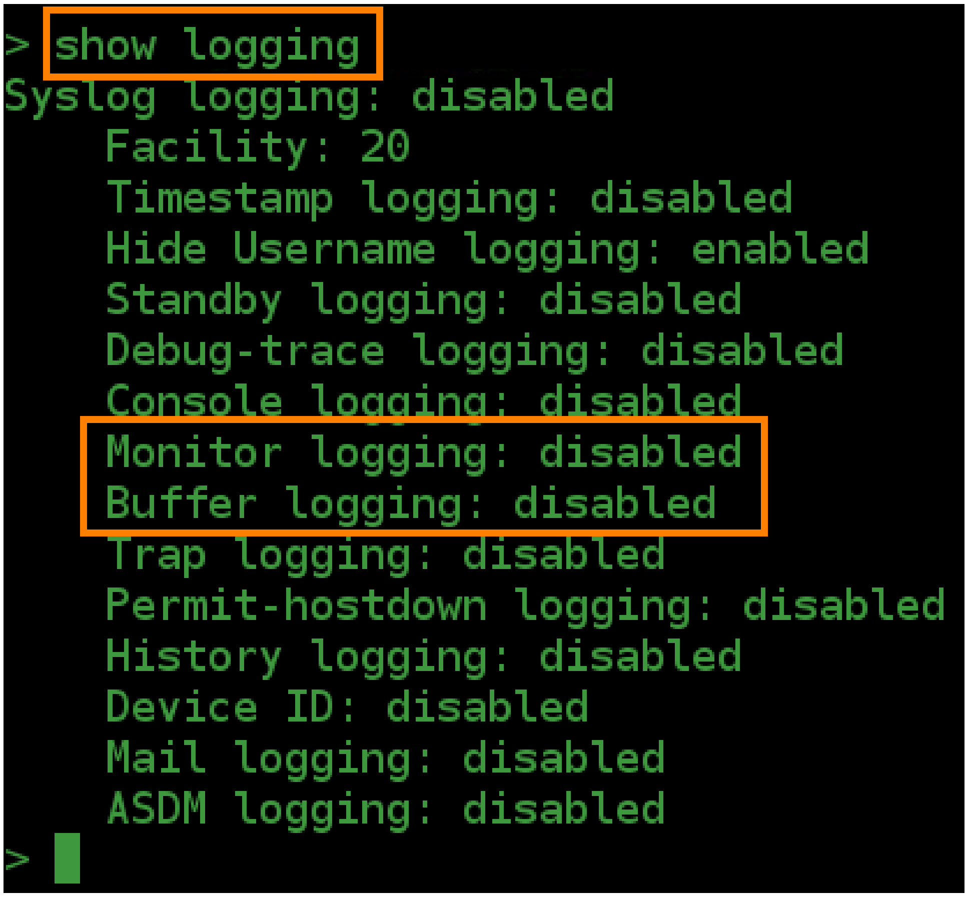
Selected Devices
- hq-ftd
- remote1-ftd
- remote2-ftd

11. Click **Save**, **Deploy**, select **all the FTD** devices and then click **Deploy**.

Testing

12. While waiting for the deployment to complete open a connection to **hq-ftd** from the **oob webpage**. This wil auto login as **admin**/**Admin123**. Issue the command **show logging**. Notice that all the logging destination are disabled.

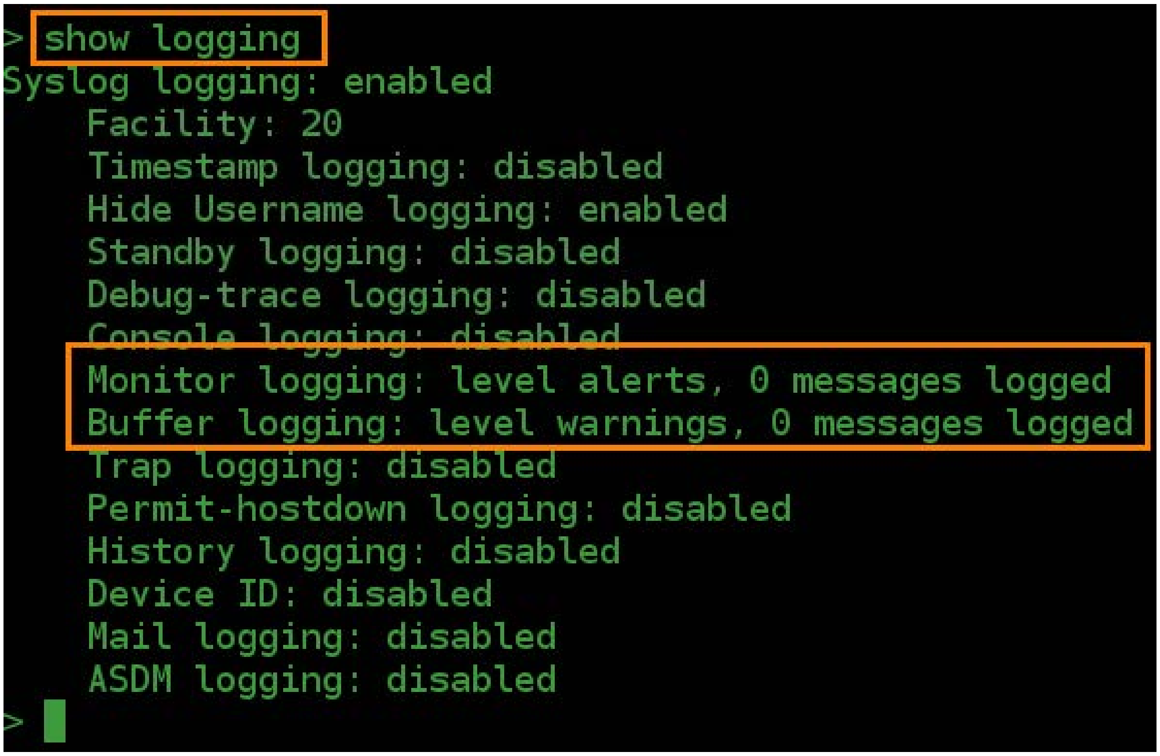
Figure 414. Show logging



```
> show logging
Syslog logging: disabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
>
```

13. After the deployment is successful re-issue the **show logging** command and notice that the **Monitor logging** and **Buffer logging** are now **enabled**. You may also see some of the logs at the bottom of this command.

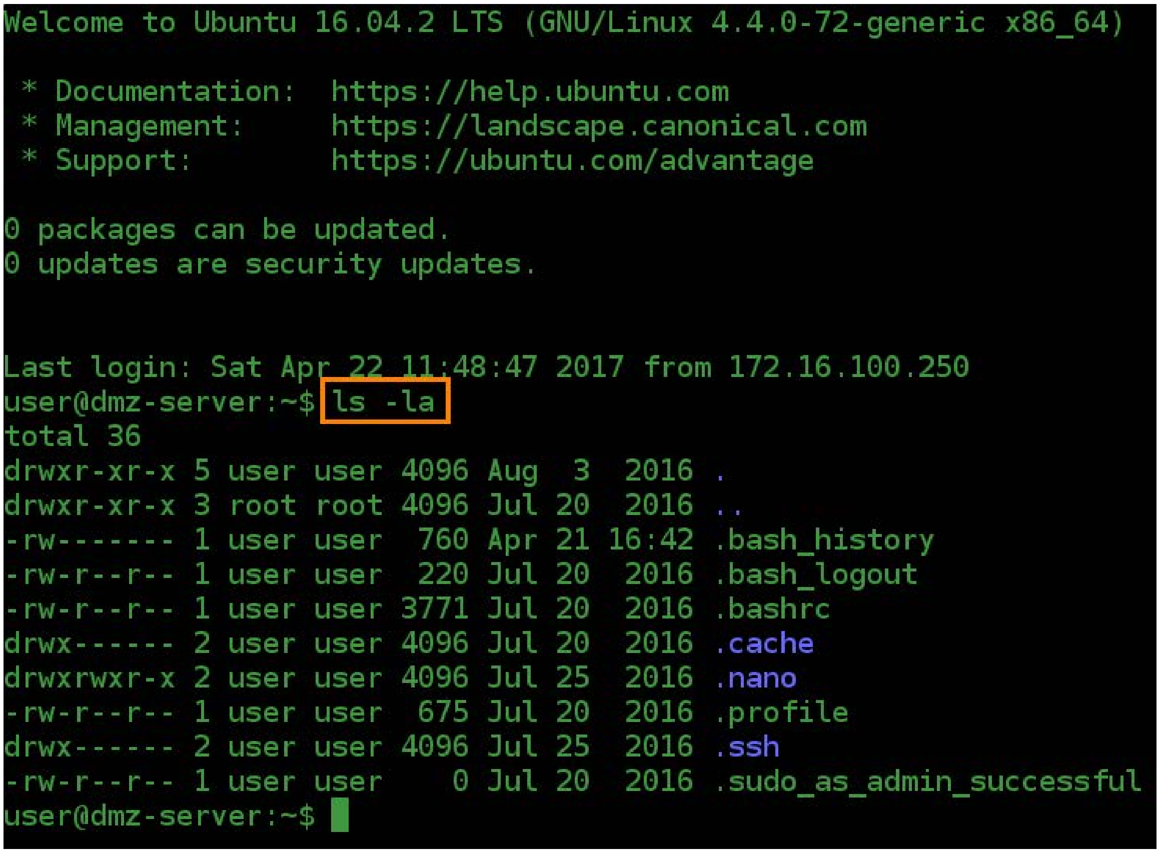
Figure 415. Show logging



```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: level alerts, 0 messages logged
    Buffer logging: level warnings, 0 messages logged
    Trap logging: disabled
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
> 
```

14. Open a connection to the **dmz-server** using the **oob wepage** link. This will auto login as **user**/**C1sco12345**. Issue the command **ls -la**. The buffer overflow file probably won't be here yet since you haven't generated 8192 bytes of syslog messages but if you had you could see these files here.

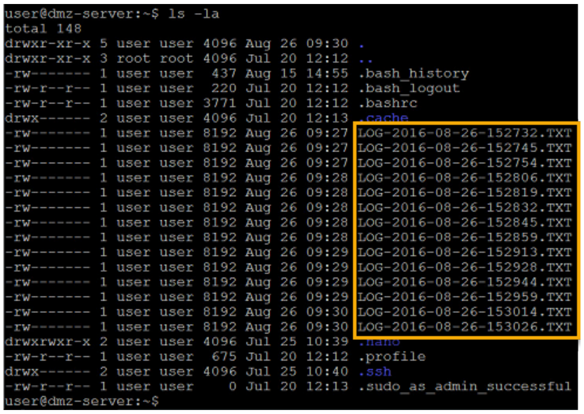
Figure 416. Show directory on dmz-server



```
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Sat Apr 22 11:48:47 2017 from 172.16.100.250
user@dmz-server:~$ ls -la
total 36
drwxr-xr-x 5 user user 4096 Aug  3  2016 .
drwxr-xr-x 3 root root 4096 Jul 20  2016 ..
-rw------- 1 user user  760 Apr 21 16:42 .bash_history
-rw-r--r-- 1 user user  220 Jul 20  2016 .bash_logout
-rw-r--r-- 1 user user 3771 Jul 20  2016 .bashrc
drwx------ 2 user user 4096 Jul 20  2016 .cache
drwxrwxr-x 2 user user 4096 Jul 25  2016 .nano
-rw-r--r-- 1 user user  675 Jul 20  2016 .profile
drwx------ 2 user user 4096 Jul 25  2016 .ssh
-rw-r--r-- 1 user user    0 Jul 20  2016 .sudo_as_admin_successful
user@dmz-server:~$
```

This is just an example. For the purposes of showing you these files I set the buffer level to debugging long enough to generate these files so that I could take the following screenshot.

Figure 417. Overflow Log Files on FTP Server



```
user@dmz-server:~$ ls -la
total 148
drwxr-xr-x 5 user user 4096 Aug 26 09:30 .
drwxr-xr-x 3 root root 4096 Jul 20 12:12 ..
-rw------- 1 user user  437 Aug 15 14:55 .bash_history
-rw-r--r-- 1 user user  220 Jul 20 12:12 .bash_logout
-rw-r--r-- 1 user user 3771 Jul 20 12:12 .bashrc
drwx------ 2 user user 4096 Jul 20 12:13 .cache
-rw------- 1 user user 8192 Aug 26 09:27 LOG-2016-08-26-152732.TXT
-rw------- 1 user user 8192 Aug 26 09:27 LOG-2016-08-26-152745.TXT
-rw------- 1 user user 8192 Aug 26 09:27 LOG-2016-08-26-152754.TXT
-rw------- 1 user user 8192 Aug 26 09:28 LOG-2016-08-26-152806.TXT
-rw------- 1 user user 8192 Aug 26 09:28 LOG-2016-08-26-152819.TXT
-rw------- 1 user user 8192 Aug 26 09:28 LOG-2016-08-26-152832.TXT
-rw------- 1 user user 8192 Aug 26 09:28 LOG-2016-08-26-152845.TXT
-rw------- 1 user user 8192 Aug 26 09:28 LOG-2016-08-26-152859.TXT
-rw------- 1 user user 8192 Aug 26 09:29 LOG-2016-08-26-152913.TXT
-rw------- 1 user user 8192 Aug 26 09:29 LOG-2016-08-26-152928.TXT
-rw------- 1 user user 8192 Aug 26 09:29 LOG-2016-08-26-152944.TXT
-rw------- 1 user user 8192 Aug 26 09:29 LOG-2016-08-26-152959.TXT
-rw------- 1 user user 8192 Aug 26 09:30 LOG-2016-08-26-153014.TXT
-rw------- 1 user user 8192 Aug 26 09:30 LOG-2016-08-26-153026.TXT
drwxrwxr-x 2 user user 4096 Jul 25 10:39 .nano
-rw-r--r-- 1 user user  675 Jul 20 12:12 .profile
drwx------ 2 user user 4096 Jul 25 10:40 .ssh
-rw-r--r-- 1 user user    0 Jul 20 12:13 .sudo_as_admin_successful
user@dmz-server:~$
```

Scenario Summary

Though this scenario was short it showed the power of centralized management. All FTD devices within the Example Corp network received the desired settings in one deployment push! Subsequent changes, should they be needed, only need to be changed in the FMC and then pushed to all the FTD devices. After which they will all have a common configuration profile!

Scenario 11. Example Corp VPN Setup

Scenario Description

In this scenario you will create a VPN between the three sites of Example Corp. Each remote site should have full IP connectivity to the other two sites.

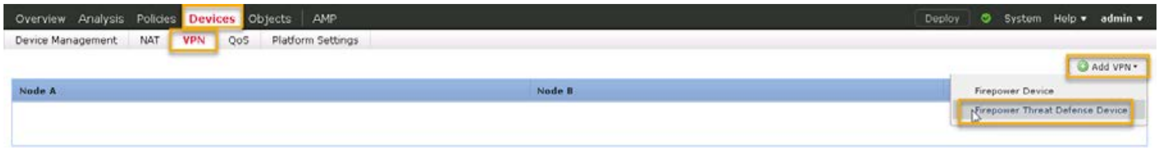
Select and Build a VPN Topology

There are three VPN topologies to choose from: Point to Point, Hub and Spoke, and Full Mesh. In order to select a solution there seems to be one major limitation and that is whether any of the participating FTDs is using DHCP on the interface where the VPN tunnel terminates. **If so, then the ONLY VPN topology you can use is the Hub and Spoke. The other two topology types require the participating FTD devices to use static IP assignments on their interfaces where the VPN tunnel terminates.**

Since the remote2-ftd is using DHCP on its “outside” interface the best topology option for Example Corp is the Hub and Spoke topology. That said, you can have more than one VPN configured. Technically you could create a Hub and Spoke VPN between hq-ftd and remote2-ftd and then have another VPN type, like Point to Point, between hq-ftd and remote1-ftd.

1. Navigate to **Devices > VPN**.
2. Click the **Add VPN** button and then select the **Firepower Threat Defense Device** from the dropdown menu.

Figure 418. Add VPN



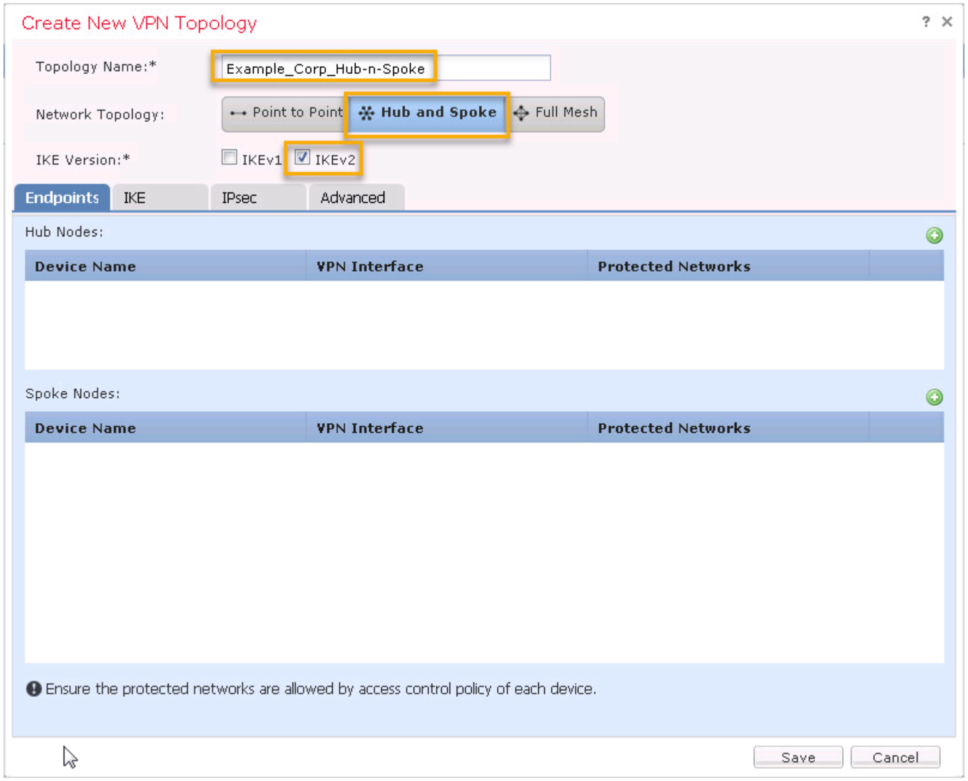
3. Use the following information to fill out the Create New VPN Topology popup window:

   a. Topology Name: **Example_Corp_Hub-n-Spoke**

   b. Network **Topology: Hub and Spoke**

   c. IKE Version: **IKEv2**

Figure 419. Part 1 Create VPN



Create New VPN Topology

Topology Name:* Example_Corp_Hub-n-Spoke

Network Topology: Point to Point | **Hub and Spoke** | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Device Name	VPN Interface	Protected Networks

Device Name	VPN Interface	Protected Networks

Ensure the protected networks are allowed by access control policy of each device.

4. On the **Endpoints tab**:

   a. Click the **green plus icon** for the **Hub Nodes** area and use the following to fill out the popup window:

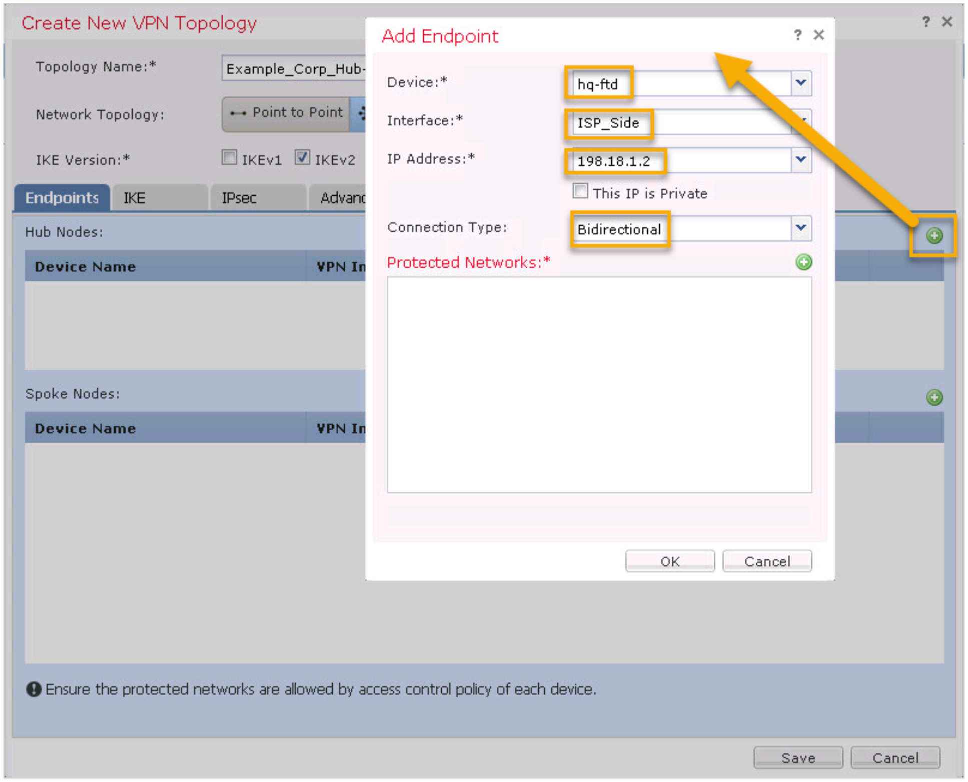
      i. Device: **hq-ftd**

      ii. Interface: **ISP_SIDE** (Notice how it is the interface name NOT the security zone.)

      iii. IP Address: **198.18.1.2**

      iv. Connection Type: **Bidirectional**

Figure 420. Part 1 Adding endpoints



Create New VPN Topology

Topology Name:* Example_Corp_Hub-

Network Topology: Point to Point

IKE Version:* ☐ IKEv1 ☑ IKEv2

Add Endpoint

Device:* hq-ftd

Interface:* ISP_Side

IP Address:* 198.18.1.2

☐ This IP is Private

Connection Type: Bidirectional

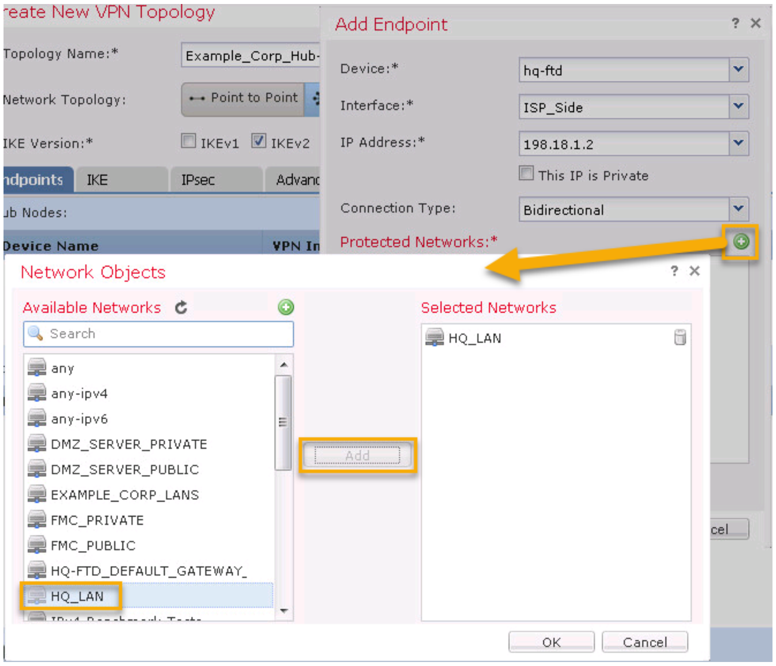
Protected Networks:*

Ensure the protected networks are allowed by access control policy of each device.

v. Protected Networks: Click the **green plus icon**

vi. Select the **HQ_LAN** and then click **Add**.

Figure 421. Add HQ_LAN



reate New VPN Topology

Topology Name:* Example_Corp_Hub-

Network Topology: Point to Point

IKE Version:* ☐ IKEv1 ☑ IKEv2

Add Endpoint

Device:* hq-ftd

Interface:* ISP_Side

IP Address:* 198.18.1.2

☐ This IP is Private

Connection Type: Bidirectional

Protected Networks:*

Network Objects

Available Networks

Search

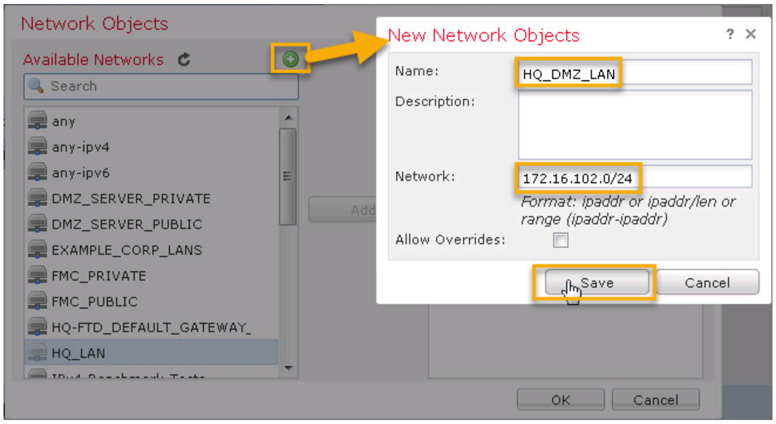
- any
- any-ipv4
- any-ipv6
- DMZ_SERVER_PRIVATE
- DMZ_SERVER_PUBLIC
- EXAMPLE_CORP_LANS
- FMC_PRIVATE
- FMC_PUBLIC
- HQ-FTD_DEFAULT_GATEWAY_
- HQ_LAN

Selected Networks

- HQ_LAN

vii. Create a new Network Object for the **172.16.102.0/24** (the HQ_DMZ_LAN).

Figure 422. Create Network Object



New Network Objects

Name: HQ_DMZ_LAN

Description:

Network: 172.16.102.0/24

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

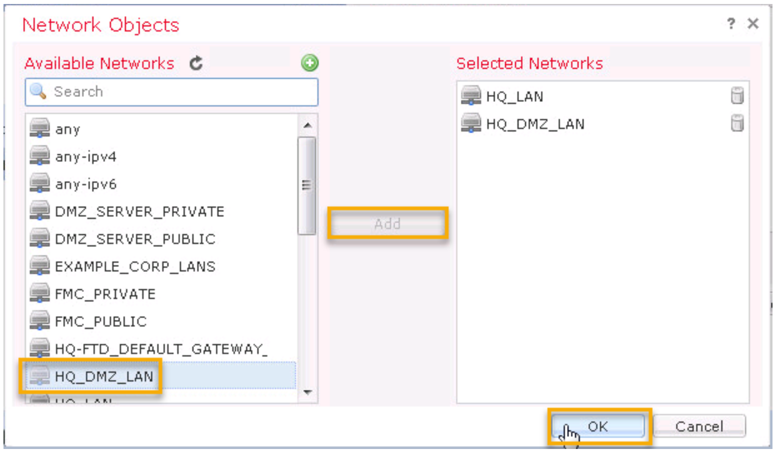
Allow Overrides: ☐

viii. Select **HQ_DMZ_LAN** and click **Add**.

ix. Ensure that both networks are in the Selected Networks area.

x. Click **OK**.

Figure 423. Add HQ_DMZ_LAN

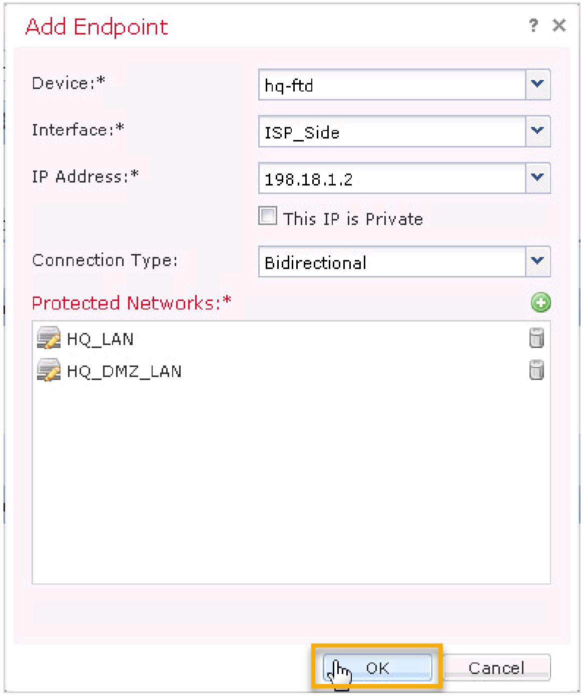


Selected Networks

- HQ_LAN
- HQ_DMZ_LAN

xi. Click **OK** to finish adding the hq-ftd endpoint to the Hub Nodes section.

Figure 424. Finish Hub Nodes



Device:* hq-ftd

Interface:* ISP_Side

IP Address:* 198.18.1.2

□ This IP is Private

Connection Type: Bidirectional

Protected Networks:*

- HQ_LAN
- HQ_DMZ_LAN

b. Click the **green plus icon** for the **Spoke Nodes** area and use the following to fill out the popup window:

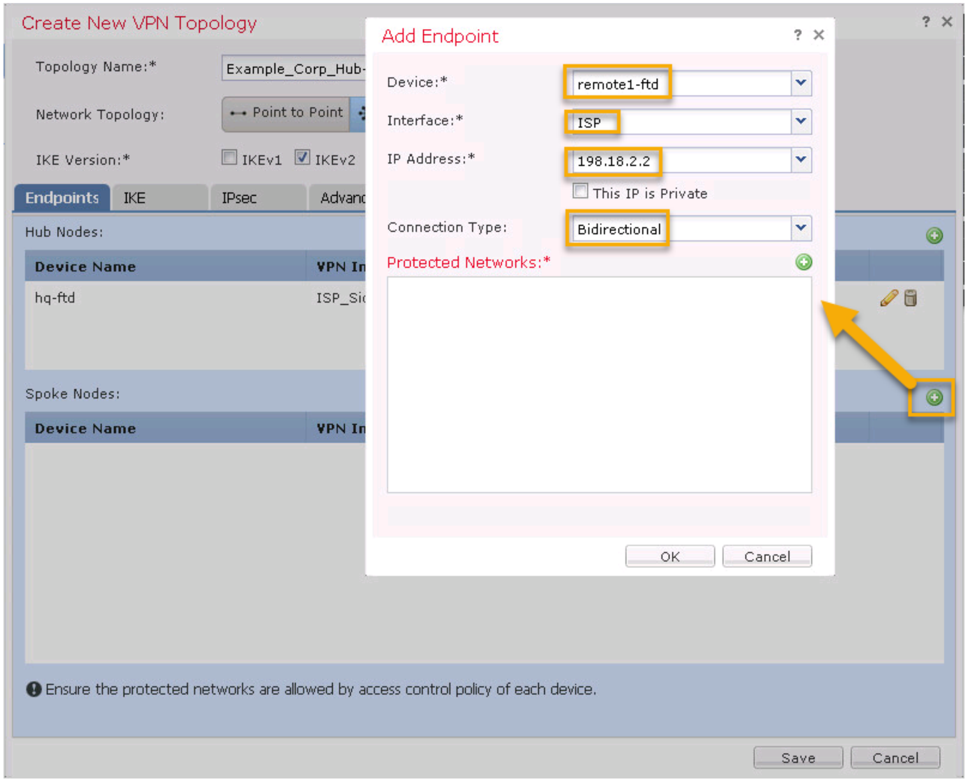
i. Device: **remote1-ftd**

ii. Interface: **ISP**

iii. IP Address: **198.18.2.2**

iv. Connection Type: **Bidirectional**

Figure 425. Part 1 Adding Spokes



Create New VPN Topology

Topology Name:* Example_Corp_Hub-

Network Topology: Point to Point

IKE Version:* □ IKEv1 ☑ IKEv2

Add Endpoint

Device:* remote1-ftd

Interface:* ISP

IP Address:* 198.18.2.2

□ This IP is Private

Connection Type: Bidirectional

Protected Networks:*

Hub Nodes:

Device Name	VPN In
hq-ftd	ISP_Si

Spoke Nodes:

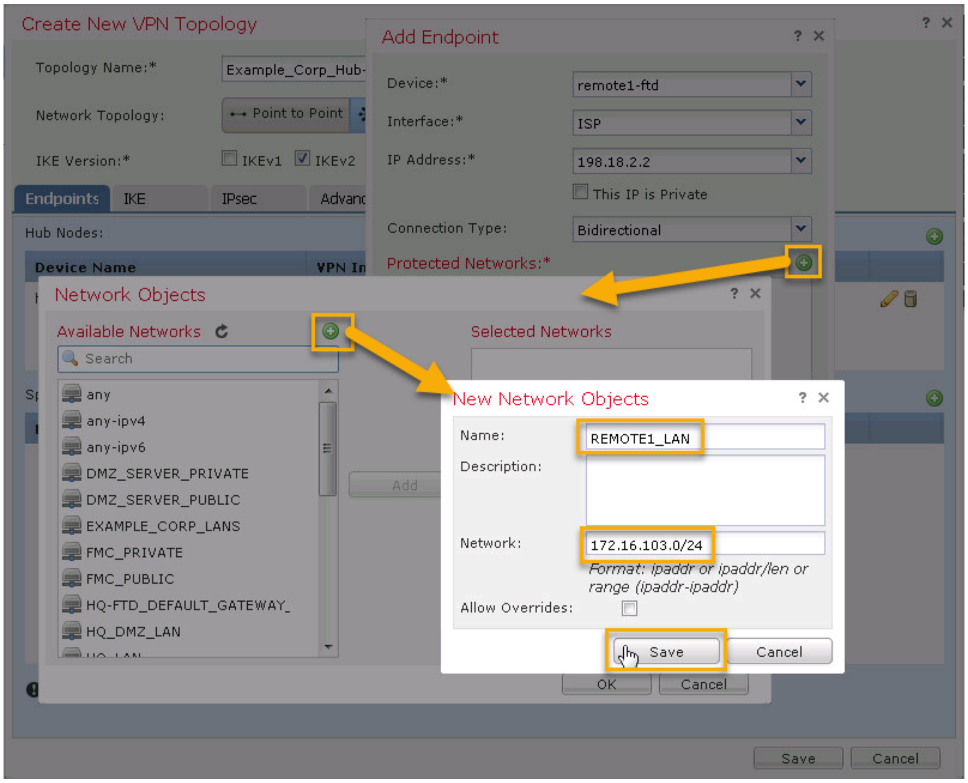
Device Name	VPN In

Ensure the protected networks are allowed by access control policy of each device.

v. Protected Networks: Click the **green plus icon**

vi. Create a new Network Object for the **172.16.103.0/24** (the REMOTE1_LAN)

Figure 426. Add REMOTE1_LAN



Create New VPN Topology

Topology Name:* Example_Corp_Hub-

Network Topology: Point to Point

IKE Version:* ☐ IKEv1 ☑ IKEv2

Add Endpoint

Device:* remote1-ftd

Interface:* ISP

IP Address:* 198.18.2.2

☐ This IP is Private

Connection Type: Bidirectional

Protected Networks:*

New Network Objects

Name: REMOTE1_LAN

Description:

Network: 172.16.103.0/24

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

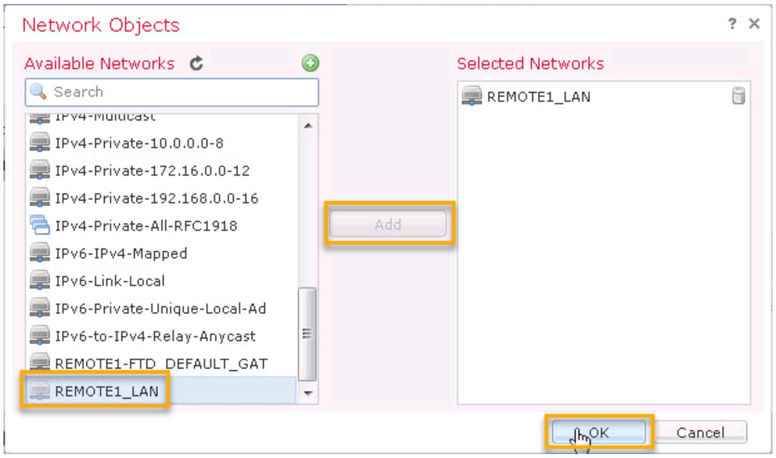
Allow Overrides: ☐

vii. Select **REMOTE1_LAN** and click **Add**.

viii. Ensure that the network is in the Selected Networks area.

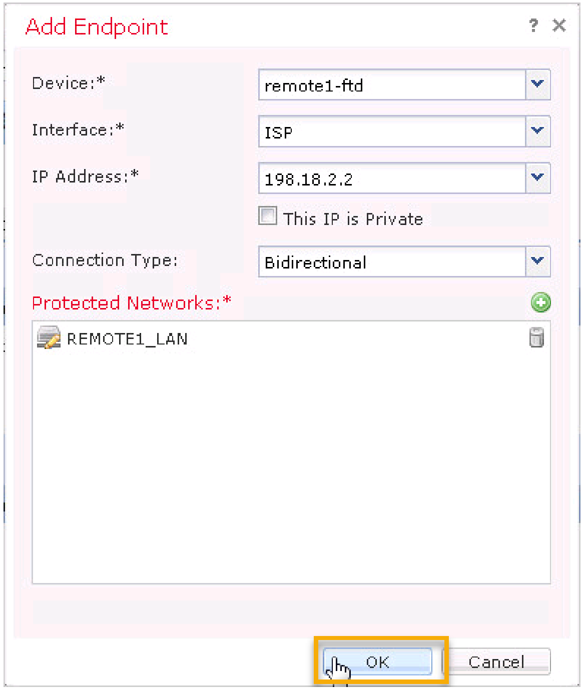
ix. Click **OK**.

Figure 427. Click OK



x. Click **OK** to finish adding the remote1-ftd endpoint to the Spoke Nodes section.

Figure 428. Click OK



Add Endpoint

Device:* remote1-ftd

Interface:* ISP

IP Address:* 198.18.2.2

□ This IP is Private

Connection Type: Bidirectional

Protected Networks:*

REMOTE1_LAN

c. Click the **green plus icon** for the **Spoke Nodes** area again and use the following to fill out the popup window:

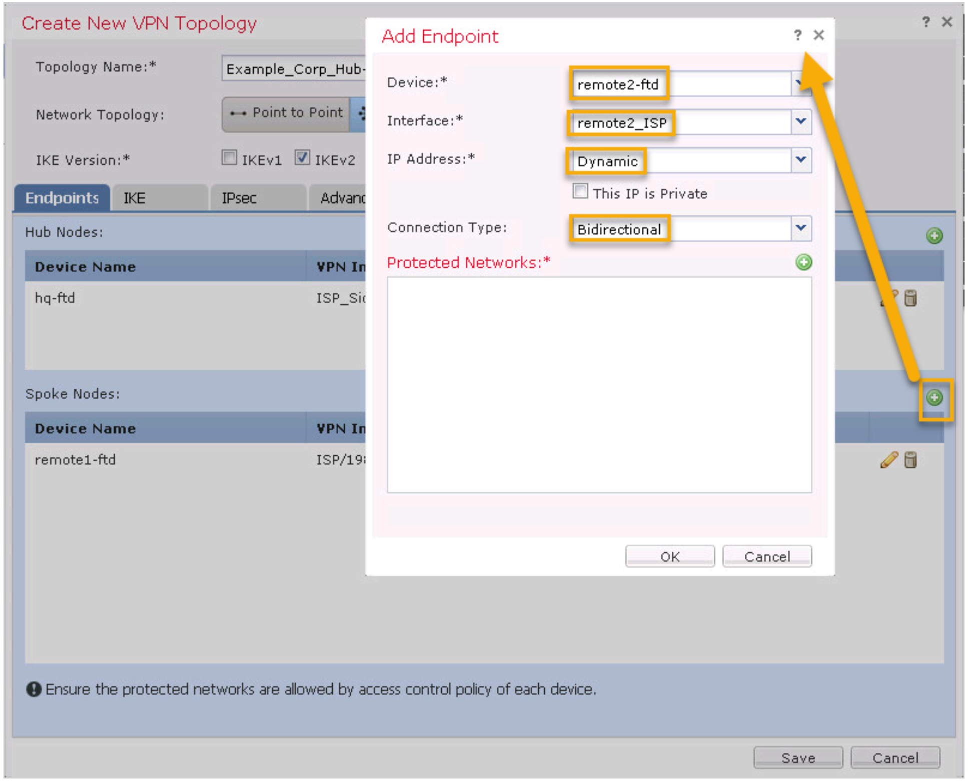
i. Device: **remote2-ftd**

ii. Interface: **remote2_ISP**

iii. IP Address: **Dynamic**

iv. Connection Type: **Bidirectional**

Figure 429. Part 1 Adding Node



Create New VPN Topology

Topology Name:* Example_Corp_Hub-

Network Topology: Point to Point

IKE Version:* ☐ IKEv1 ☑ IKEv2

Hub Nodes:

Device Name	VPN In
hq-ftd	ISP_Si

Spoke Nodes:

Device Name	VPN In
remote1-ftd	ISP/19

Add Endpoint

Device:* remote2-ftd

Interface:* remote2_ISP

IP Address:* Dynamic

☐ This IP is Private

Connection Type: Bidirectional

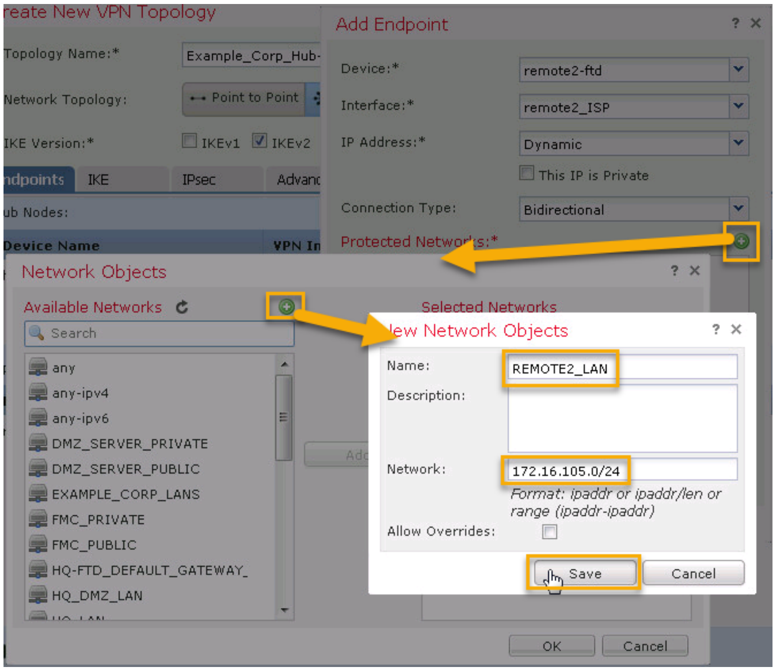
Protected Networks:*

Ensure the protected networks are allowed by access control policy of each device.

v. Protected Networks: Click the **green plus icon**

vi. Create a new Network Object for the **172.16.105.0/24** (the REMOTE2_LAN)

Figure 430. Create REMOTE2_LAN Network Object



reate New VPN Topology

Topology Name:* Example_Corp_Hub-

Network Topology: Point to Point

IKE Version:* ☐ IKEv1 ☑ IKEv2

Add Endpoint

Device:* remote2-ftd

Interface:* remote2_ISP

IP Address:* Dynamic

☐ This IP is Private

Connection Type: Bidirectional

Protected Networks:*

New Network Objects

Name: REMOTE2_LAN

Description:

Network: 172.16.105.0/24

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

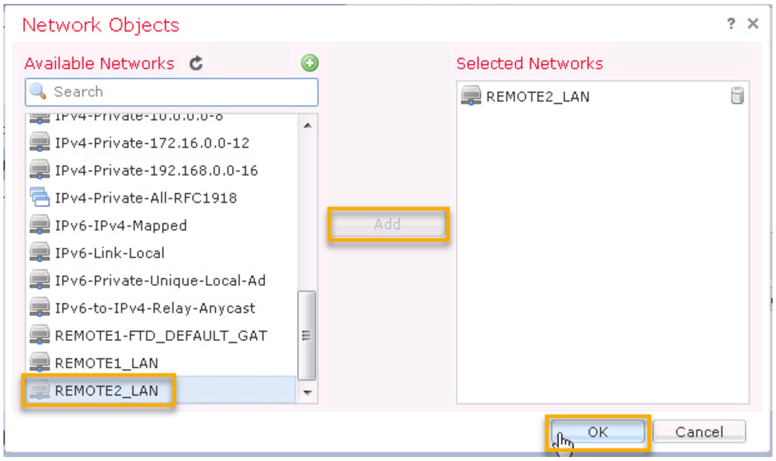
Allow Overrides: ☐

vii. Select **REMOTE2_LAN** and click **Add**.

viii. Ensure that the network is in the Selected Networks area.

ix. Click **OK**.

Figure 431. Click OK

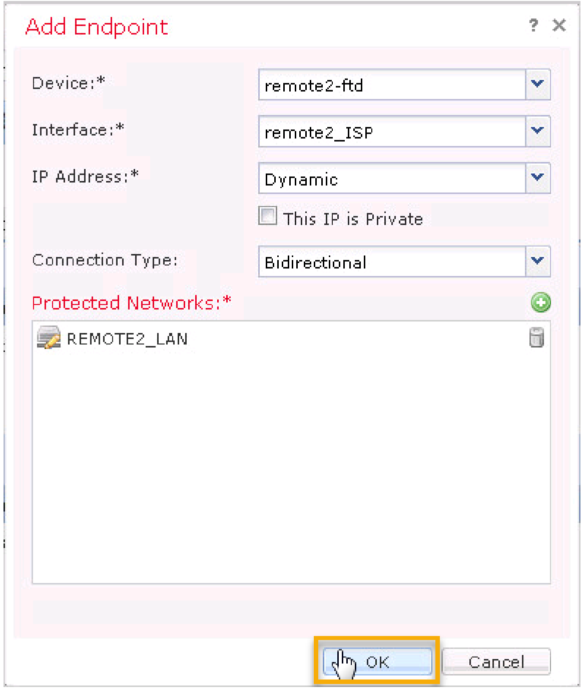


Network Objects

Selected Networks: REMOTE2_LAN

x. Click **OK** to finish adding the remote2-ftd endpoint to the Spoke Nodes section.

Figure 432. Click OK



Add Endpoint

Device:* remote2-ftd

Interface:* remote2_ISP

IP Address:* Dynamic

□ This IP is Private

Connection Type: Bidirectional

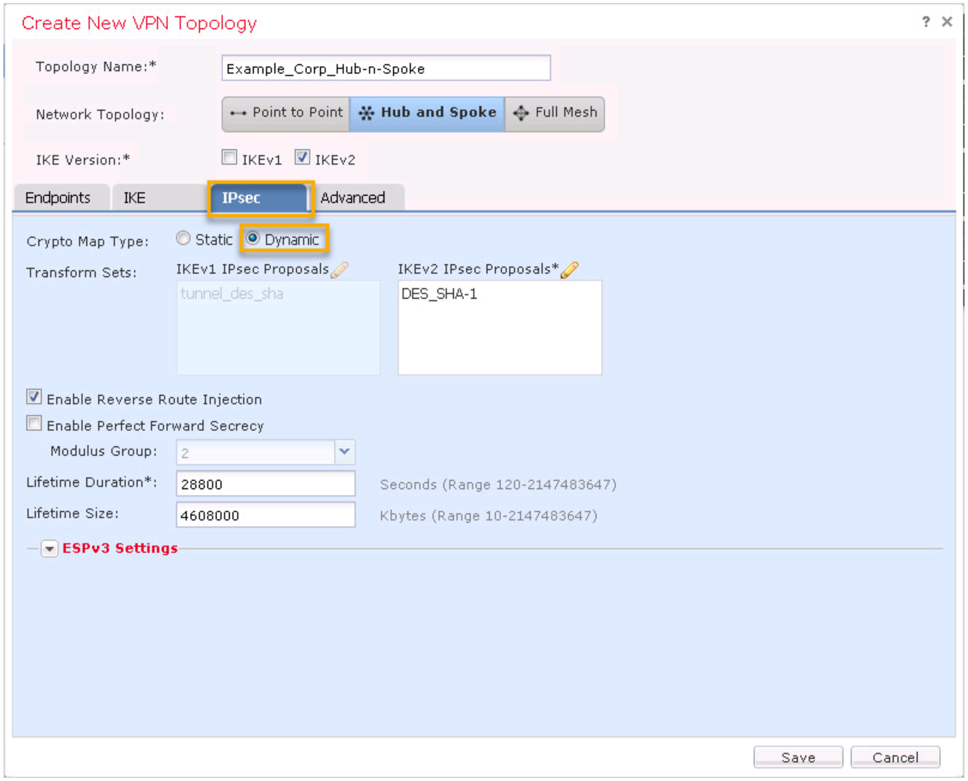
Protected Networks:*

REMOTE2_LAN

5. On the **IPsec tab**:

   a. Check the **Dynamic** button for the Crypto Map Type. (This is a requirement when endpoints with dynamic IPs are part of the VPN topology.)

Figure 433. Configure IPsec tab



Create New VPN Topology

Topology Name:* Example_Corp_Hub-n-Spoke

Network Topology: Point to Point | **Hub and Spoke** | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type: ○ Static ● Dynamic

Transform Sets: IKEv1 IPsec Proposals: tunnel_des_sha; IKEv2 IPsec Proposals*: DES_SHA-1

☑ Enable Reverse Route Injection

□ Enable Perfect Forward Secrecy

Modulus Group: 2

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

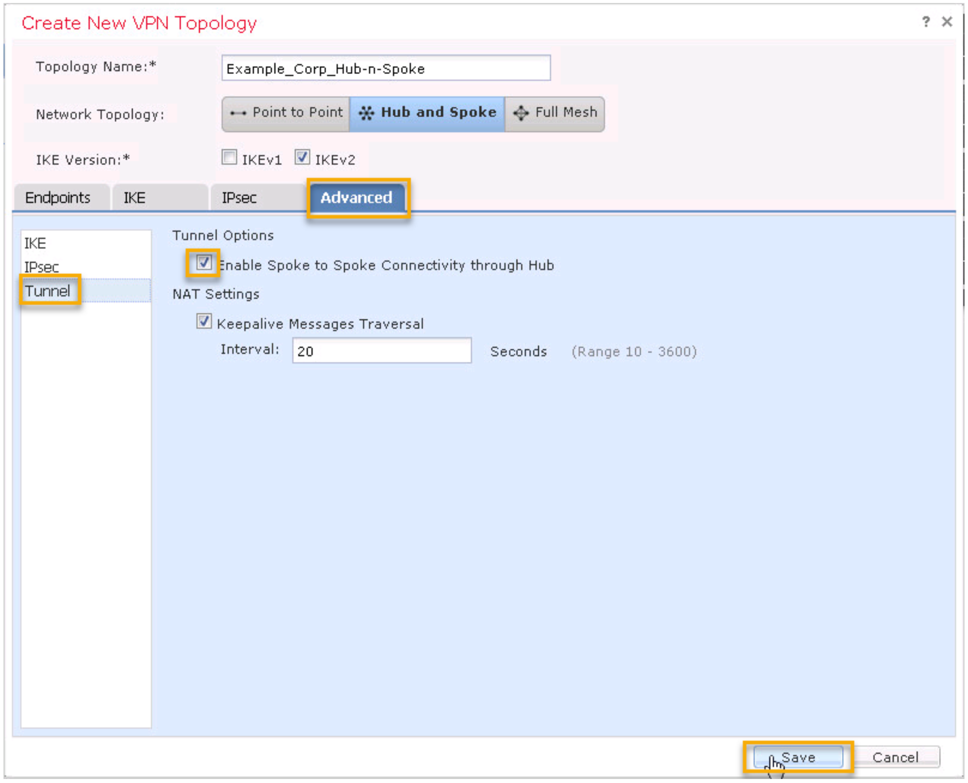
ESPv3 Settings

6. On the **Advanced tab**:

   a. Click the **Tunnel menu** option and then check the box to **Enable Spoke to Spoke Connectivity through Hub** to allow remote1 and remote2 to intercommunicate.

7. Click **Save**.

Figure 434. Save VPN



Create New VPN Topology

Topology Name:* Example_Corp_Hub-n-Spoke

Network Topology: Point to Point | **Hub and Spoke** | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Tunnel Options

☑ Enable Spoke to Spoke Connectivity through Hub

NAT Settings

☑ Keepalive Messages Traversal

Interval: 20 Seconds (Range 10 - 3600)

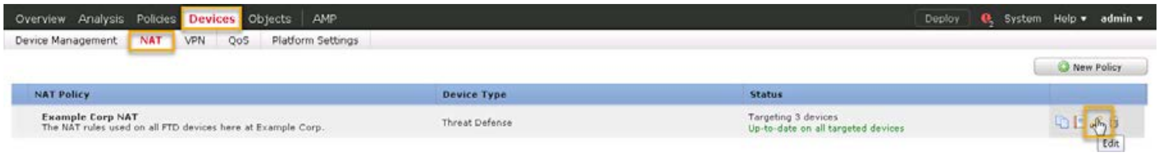
Configure NAT Identity

At this point you could deploy the VPN tunnel and the FTD devices would establish a tunnel connection between themselves. However, if you were to pass traffic, say ping hq-wkst from remote1-wkst, it wouldn't work. There are a couple more configuration items you need to consider.

The first of these items is Example Corp's NAT policy.

8. Navigate to **Devices > NAT** and **edit** the **Example Corp NAT** policy. What is the action for the rule for Example Corp LAN IPs traversing from an Inside zone to an Outside zone? (VPN tunnels are considered to be in the zone of the endpoint interface used to terminate the tunnel.) As you can see you have a Dynamic (think PAT) translation of EXAMPLE_CORP_LANS IP to the Interface IP.

Figure 435. Edit NAT



NAT Policy	Device Type	Status
Example Corp NAT The NAT rules used on all FTD devices here at Example Corp.	Threat Defense	Targeting 3 devices Up-to-date on all targeted devices

9. You need to create a new rule to perform identity NAT prior to the existing rule. Click **Add Rule** and use the following to fill out the popup window:

    a. Nat Rule: **Manual NAT Rule**

    b. Insert: **In Category** and then **NAT Rules Before**.

    c. Type: **Static**

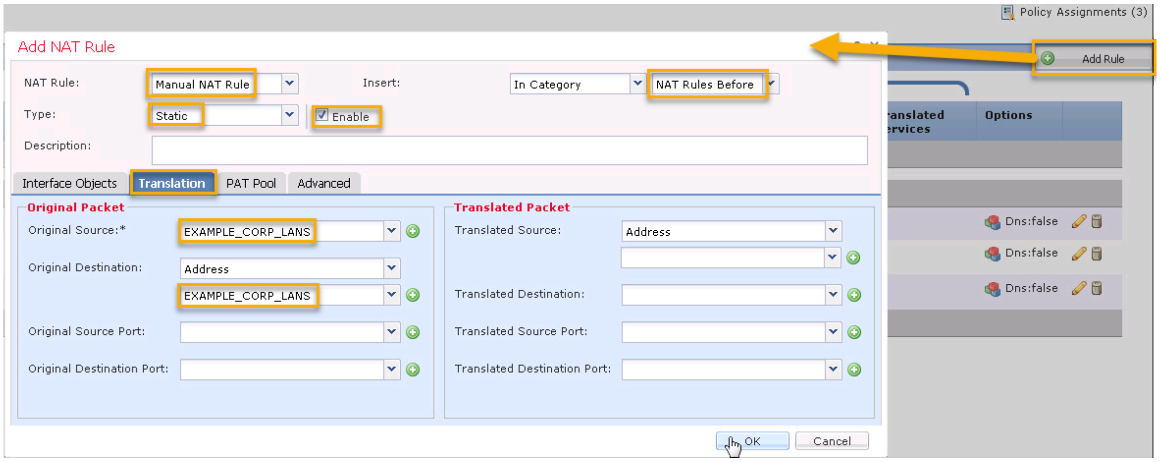
    d. Enable: **Checked**

10. On the **Translation tab**:

    a. Original Source: **EXAMPLE_CORP_LANS**

    b. Original Destination: **Address** and then **EXAMPLE_CORP_LANS**

Figure 436. Configure Translations tab



NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static ☑ Enable

Description:

Original Source:* EXAMPLE_CORP_LANS

Original Destination: Address

EXAMPLE_CORP_LANS

Original Source Port:

Original Destination Port:

Translated Source: Address

Translated Destination:

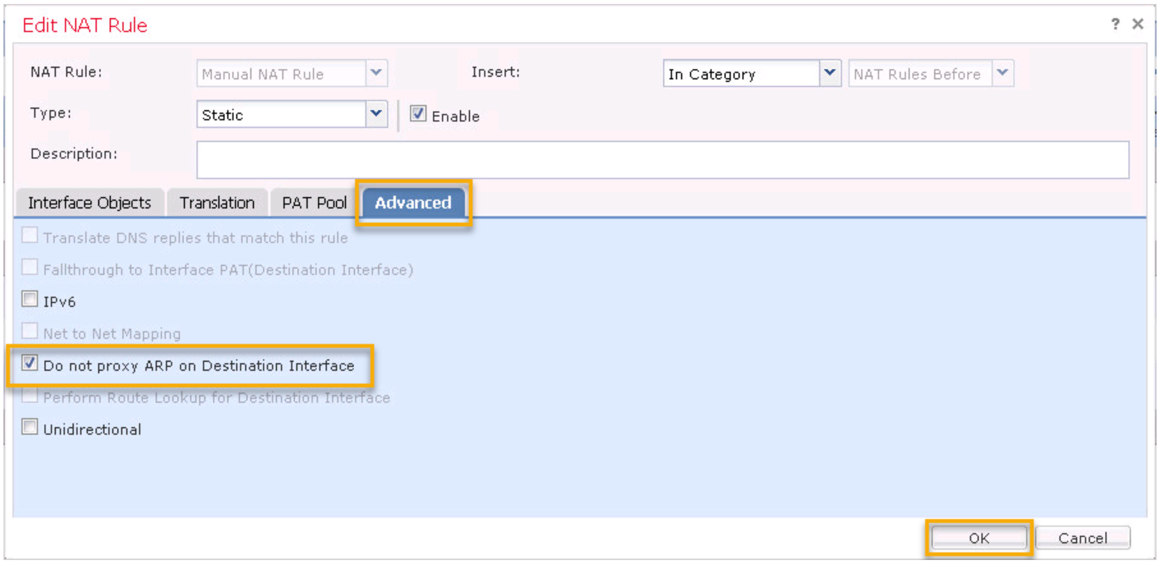
Translated Source Port:

Translated Destination Port:

11. On the Advanced tab check the **Do not proxy ARP on Destination Interface** option. If you don't do this then the local FTD will respond to ARPs even for requests that could be handled on the local LAN.

12. Click **OK**.

Figure 437. Death to proxy-arp!



Edit NAT Rule

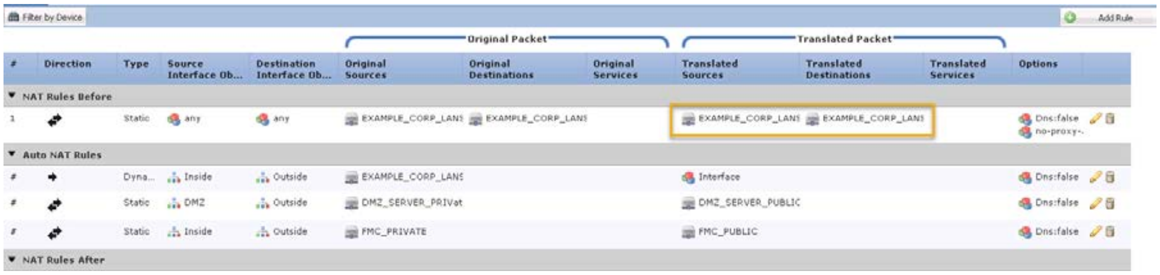
NAT Rule: Manual NAT Rule
Insert: In Category | NAT Rules Before
Type: Static ☑ Enable
Description:

□ Translate DNS replies that match this rule
□ Fallthrough to Interface PAT(Destination Interface)
□ IPv6
□ Net to Net Mapping
☑ Do not proxy ARP on Destination Interface
□ Perform Route Lookup for Destination Interface
□ Unidirectional

The VPN would work, without the "no proxy-ARP" being enabled but since we are using identity NAT to identify traffic it would start causing problems with connectivity on the local LAN. The FTD would answer any ARP related queries for all EXAMPLE_CORP_LANS IP to MAC queries, even for those that should be answered by a device on the local LAN.

13. Notice that the new rule auto populated the Translated Packet field to create the identity NAT.

Figure 438. Finished NAT Rule

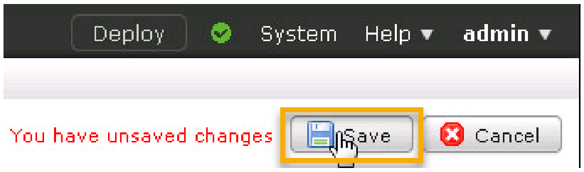


					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Ob...	Destination Interface Ob...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1	⇄	Static	any	any	EXAMPLE_CORP_LANS	EXAMPLE_CORP_LANS		EXAMPLE_CORP_LANS	EXAMPLE_CORP_LANS		Dns:false no-proxy-.
▼ Auto NAT Rules											
#	→	Dyna...	Inside	Outside	EXAMPLE_CORP_LANS			Interface			Dns:false
#	⇄	Static	DMZ	Outside	DMZ_SERVER_PRIVat			DMZ_SERVER_PUBLIC			Dns:false
#	⇄	Static	Inside	Outside	FMC_PRIVATE			FMC_PUBLIC			Dns:false
▼ NAT Rules After											

Notice how you didn't select any Source or Destination Zones. You also used a "blanket" IP address range to identify traffic that encompasses all the site's IP address ranges. For the purposes of this deployment the decision not to be more specific is fine but be aware of these decisions because IF later on you were to create a new Zone, say Customers, and use IP addresses out of the 172.16.0.0/16 network then those new LANs would be matched by this rule. That behavior might not be what you wanted. So, depending on the complexity (and paranoia) of the customer you may choose to create multiple NAT identity statements to be more specific on where that rule would apply.

14. Click **Save** to push these changes to the FMC.

Figure 439. Save to FMC



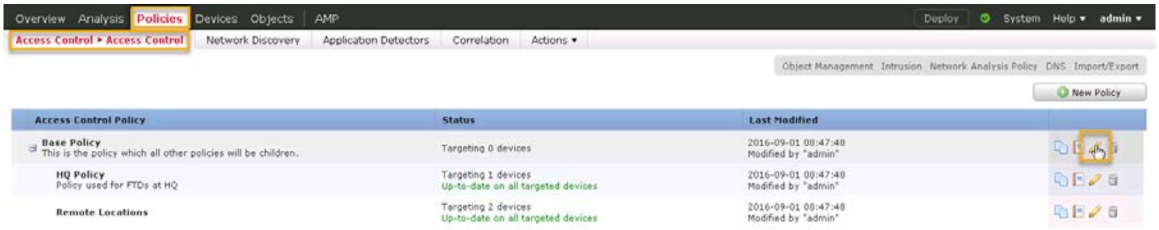
You have unsaved changes

Configure Access Control Policy Rules

The second issue you need to address is that traffic within a VPN tunnel still gets processed by the Access Control Policy rules.

15. Navigate to **Policies > Access Control > Access Control** and edit the **Base Policy**.

Figure 440. Edit Base Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-09-01 08:47:48 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-09-01 08:47:48 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-09-01 08:47:48 Modified by "admin"

You are editing the Base Policy because the rule you want to create will apply/affect all locations. Like with the NAT identity rule you created earlier, this one will be a general rule that could cause issues if further networks and/or zones where added to the Example Corp topology.

16. Click **Add Rule** and use the following to create a rule to permit Example Corp LAN IPs access to Example Corp LAN IPs from any zone:

    a. Name: **Allow VPN Traffic**

    b. Enabled: **Checked**

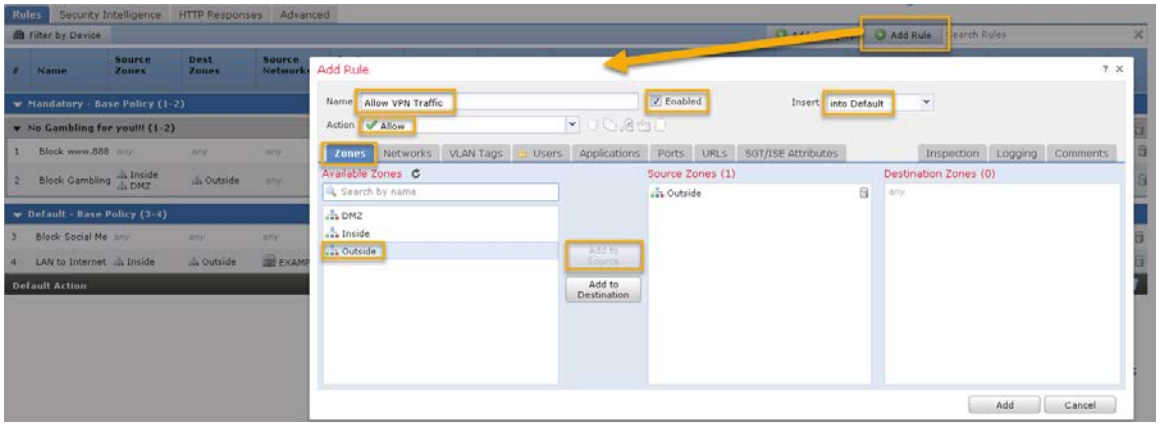
    c. Insert: **into Default**

    d. Action: **Allow**

17. On the **Zones tab**:

    a. Source Zones: **Outside**

Figure 441. Part 1 of Adding ACP rule

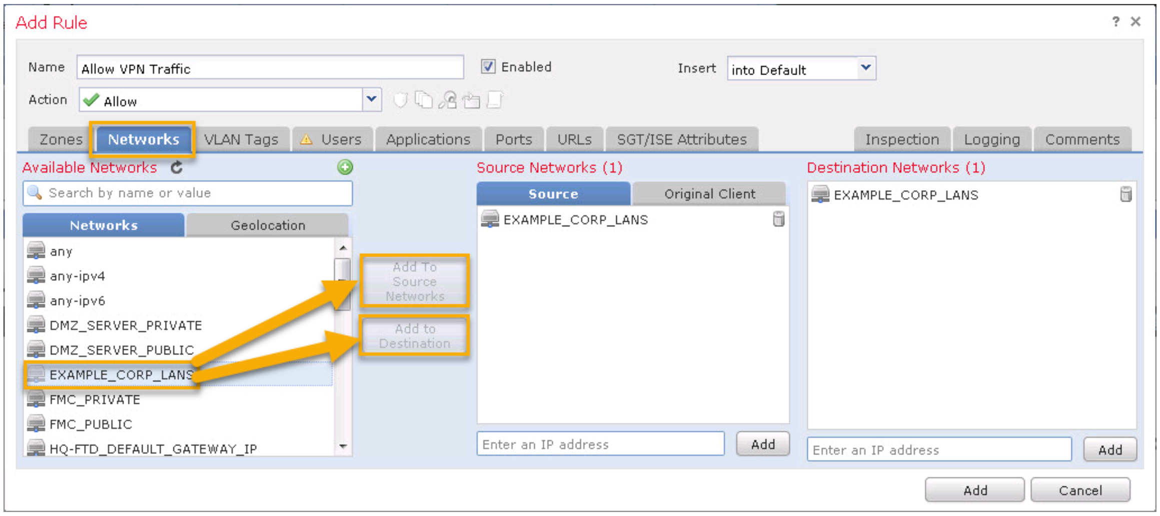


Name: Allow VPN Traffic
☑ Enabled
Insert: into Default
Action: Allow
Source Zones (1): Outside
Destination Zones (0): any

18. On the **Networks tab**:

    a. Put **EXAMPLE_CORP_LANS** in both the **Source Networks** and **Destination Networks** fields. (Select EXAMPLE_CORP_LANS and then click the Add to Source Networks and then the Add to Destination buttons.)

Figure 442. Configure Networks tab



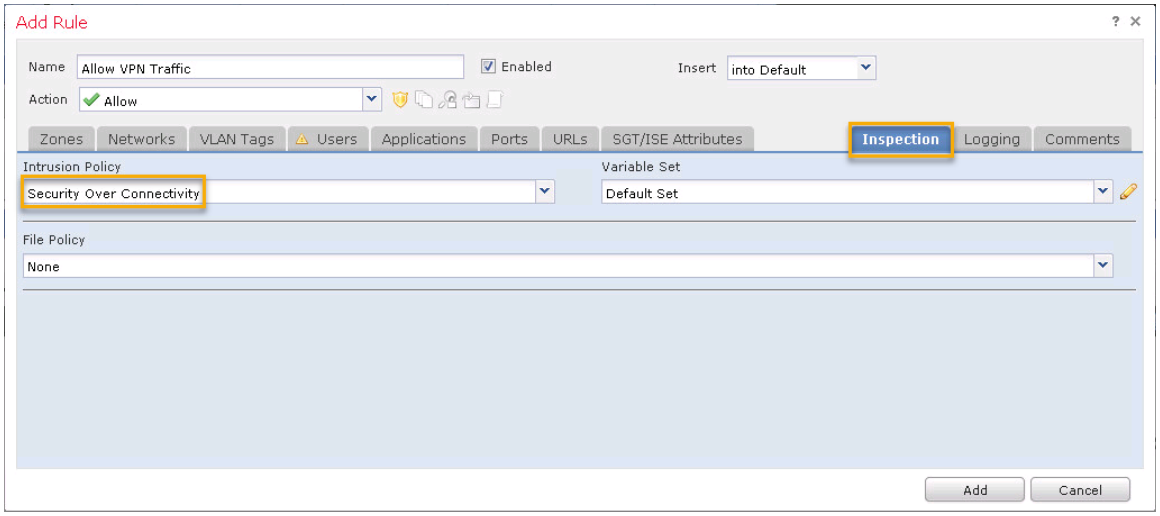
Name: Allow VPN Traffic
☑ Enabled
Insert: into Default
Action: ✓ Allow
Source Networks (1): EXAMPLE_CORP_LANS
Destination Networks (1): EXAMPLE_CORP_LANS

19. On the **Inspection tab**:

    a. Intrusion Policy: **Security Over Connectivity** (This "internal" to "internal" traffic might be a justifiable place to have a custom policy that only checks for the most egregious intrusion signatures.)

    b. It isn't in this lab but maybe a new File Policy that controls what files can be transferred over the VPN might be a good addition to this rule. Even if it the rule just monitored for Malware it could help reduce the spread of an infection.

Figure 443. Configure Inspection tab



Add Rule

Name: Allow VPN Traffic ☑ Enabled Insert: into Default

Action: ✓ Allow

Intrusion Policy: Security Over Connectivity

Variable Set: Default Set

File Policy: None

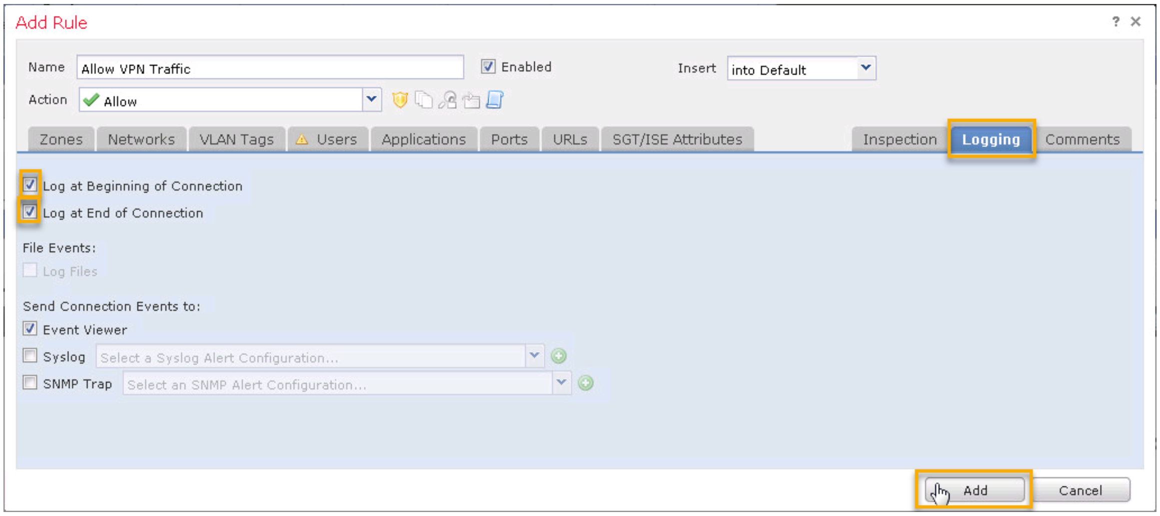
20. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** and **Log at End of Connection** buttons.

If you don’t log it then you don’t have a record it ever occurred. Do you need to log both the beginning and end? That is up to you and Example Corp IT admins. Depending on the load (and logs that are created) this could be trimmed back to just logging at the beginning of the connection.

21. Click **Add**.

Figure 444. Configure Logging and Add rule



Add Rule

Name: Allow VPN Traffic ☑ Enabled Insert: into Default

Action: ✓ Allow

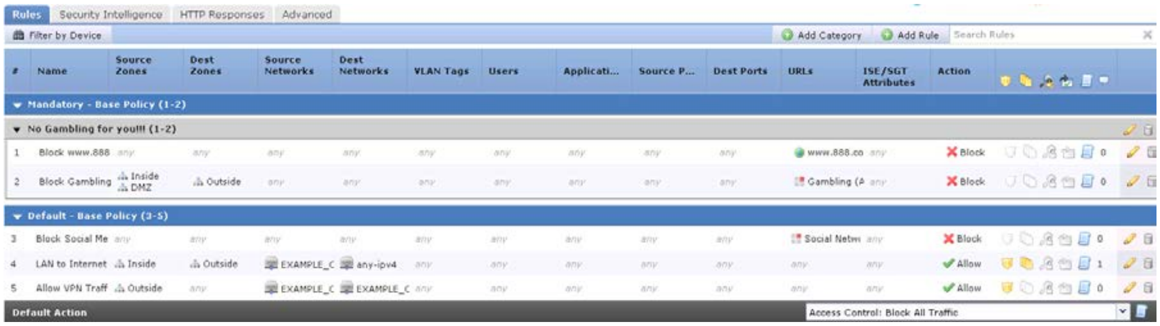
☑ Log at Beginning of Connection
☑ Log at End of Connection

File Events:
□ Log Files

Send Connection Events to:
☑ Event Viewer
□ Syslog Select a Syslog Alert Configuration...
□ SNMP Trap Select an SNMP Alert Configuration...

22. Before continuing take a look at the order of the rules. Do you see how the LAN to INET Access rule will be matched prior to the Allow VPN Traffic? Is this a problem? Why or why not?

Figure 445. Review ACP rules



#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action	
▾ Mandatory - Base Policy (1-2)														
▾ No Gambling for you!!! (1-2)														
1	Block www.888	any	any	any	any	any	any	any	any	any	www.888.co	any	✕ Block	0
2	Block Gambling	Inside DMZ	Outside	any	any	any	any	any	any	any	Gambling (A	any	✕ Block	0
▾ Default - Base Policy (3-5)														
3	Block Social Me	any	any	any	any	any	any	any	any	any	Social Netw	any	✕ Block	0
4	LAN to Internet	Inside	Outside	EXAMPLE_C	any-ipv4	any	any	any	any	any	any	any	✓ Allow	1
5	Allow VPN Traff	Outside	any	EXAMPLE_C	EXAMPLE_C	any	any	any	any	any	any	any	✓ Allow	0

Default Action: Access Control: Block All Traffic

Additionally, you “enabled” something that Example Corp expressly didn’t want. Can you see what it is? You will see it in the testing section and then you will fix it.

23. Click **Save**, **Deploy**, select **all devices** and then click **Deploy**.

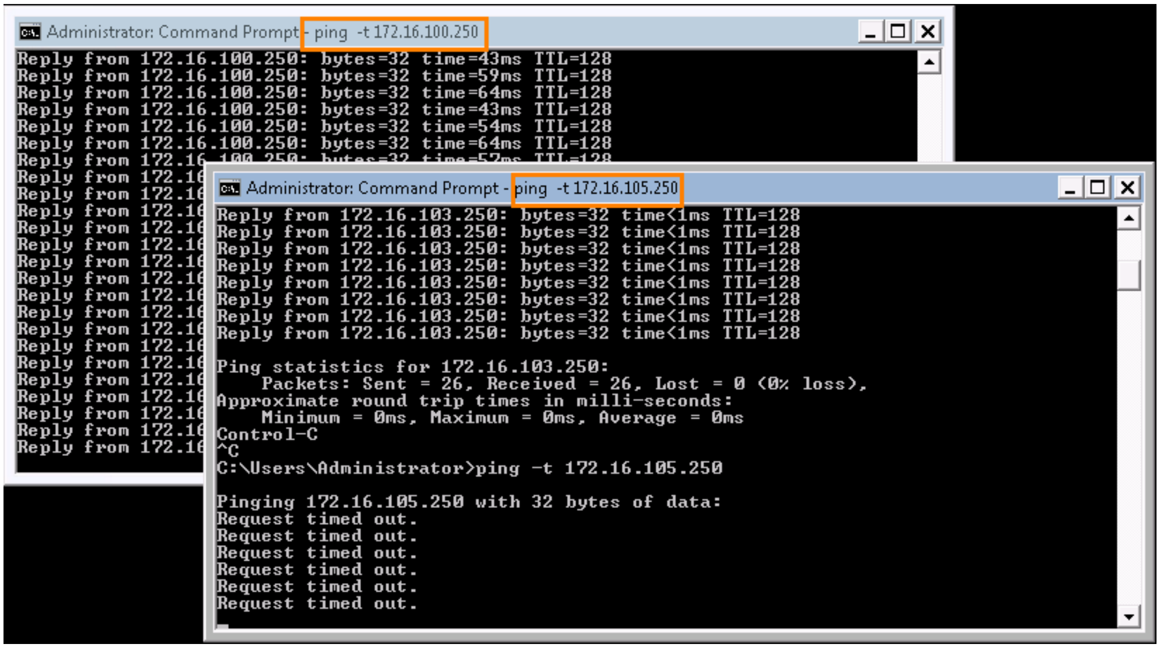
Verify and Test VPN Configuration

Now that the VPN is configured and deployed you are going to use some basic verification and “ping” tests to show that it is configured.

When issuing the ping commands below it might not work the first time you do it. It takes the FTD devices time to set up the VPN connection and/or the nature of the VPN requires that “interesting traffic” get generated from both ends of the VPN tunnel.

24. Starting with **remote1-wkst**, start **continuous pings** to **hq-wkst** and **remote2-wkst**. (hq-wkst is 172.16.100.250, remote1-wkst is 172.16.103.250, and remote2-wkst is 172.16.105.250). Take special note that the pings to hq-wkst will work but the pings to the remote2-wkst don’t. This is because the type of VPN that is set up requires the “Spoke” end to generate interesting traffic before any traffic can be sent through the VPN.

Figure 446. Starting pings on remote1-wkst first



Administrator: Command Prompt - ping -t 172.16.100.250

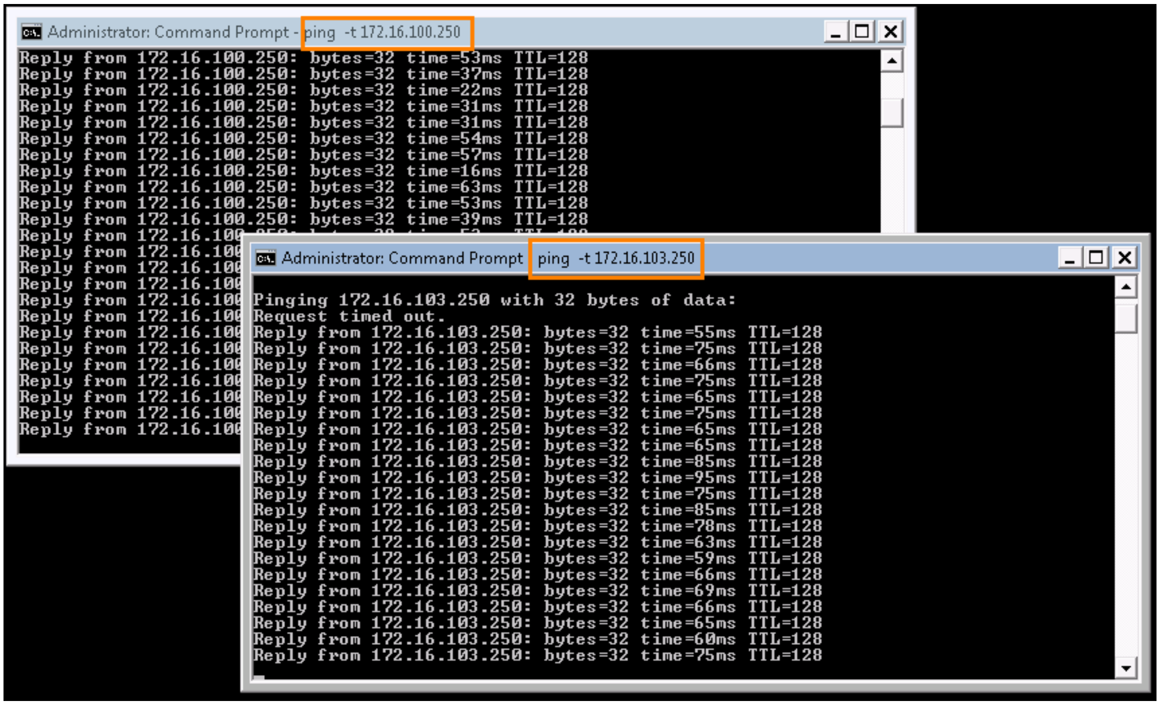
```
Reply from 172.16.100.250: bytes=32 time=43ms TTL=128
Reply from 172.16.100.250: bytes=32 time=59ms TTL=128
Reply from 172.16.100.250: bytes=32 time=64ms TTL=128
Reply from 172.16.100.250: bytes=32 time=43ms TTL=128
Reply from 172.16.100.250: bytes=32 time=54ms TTL=128
Reply from 172.16.100.250: bytes=32 time=64ms TTL=128
Reply from 172.16.100.250: bytes=32 time=57ms TTL=128
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
Reply from 172.16
```

Administrator: Command Prompt - ping -t 172.16.105.250

```
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128
Reply from 172.16.103.250: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.103.250:
    Packets: Sent = 26, Received = 26, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping -t 172.16.105.250

Pinging 172.16.105.250 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

25. Start **continuous pings** on **remote2-wkst** to **hq-wkst** and **remote1-wkst**. The pings will work to remote1-wkst from the start because interesting traffic has already been generated at the Remote1 location.

Figure 447. Then starting pings on remote2-wkst



Administrator: Command Prompt - ping -t 172.16.100.250

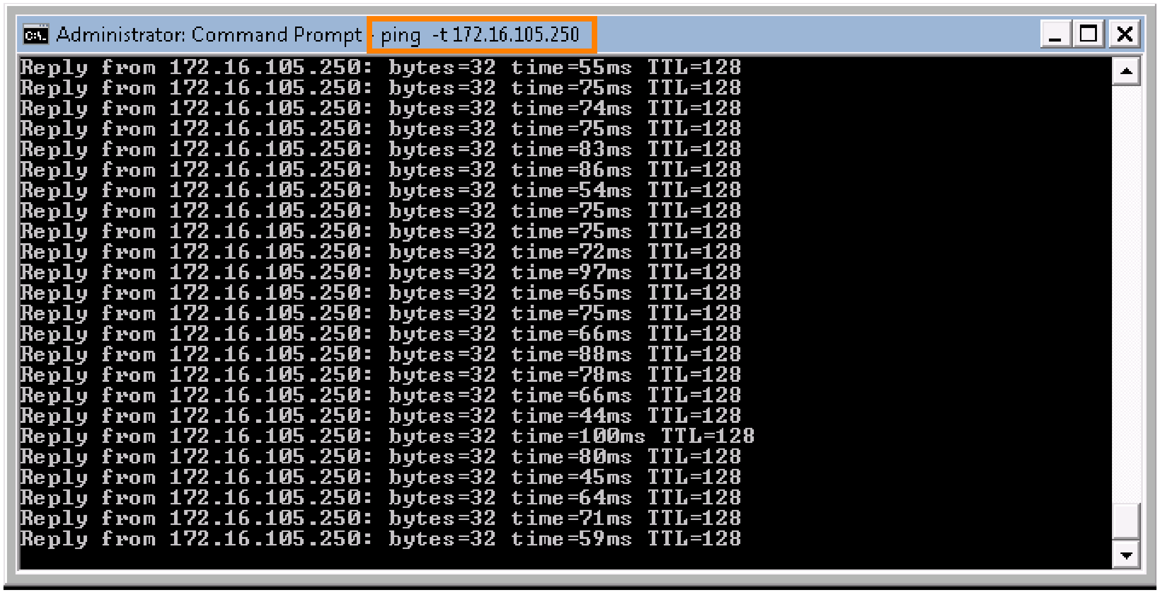
```
Reply from 172.16.100.250: bytes=32 time=53ms TTL=128
Reply from 172.16.100.250: bytes=32 time=37ms TTL=128
Reply from 172.16.100.250: bytes=32 time=22ms TTL=128
Reply from 172.16.100.250: bytes=32 time=31ms TTL=128
Reply from 172.16.100.250: bytes=32 time=31ms TTL=128
Reply from 172.16.100.250: bytes=32 time=54ms TTL=128
Reply from 172.16.100.250: bytes=32 time=57ms TTL=128
Reply from 172.16.100.250: bytes=32 time=16ms TTL=128
Reply from 172.16.100.250: bytes=32 time=63ms TTL=128
Reply from 172.16.100.250: bytes=32 time=53ms TTL=128
Reply from 172.16.100.250: bytes=32 time=39ms TTL=128
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
Reply from 172.16.100
```

Administrator: Command Prompt ping -t 172.16.103.250

```
Pinging 172.16.103.250 with 32 bytes of data:
Request timed out.
Reply from 172.16.103.250: bytes=32 time=55ms TTL=128
Reply from 172.16.103.250: bytes=32 time=75ms TTL=128
Reply from 172.16.103.250: bytes=32 time=66ms TTL=128
Reply from 172.16.103.250: bytes=32 time=75ms TTL=128
Reply from 172.16.103.250: bytes=32 time=65ms TTL=128
Reply from 172.16.103.250: bytes=32 time=75ms TTL=128
Reply from 172.16.103.250: bytes=32 time=65ms TTL=128
Reply from 172.16.103.250: bytes=32 time=65ms TTL=128
Reply from 172.16.103.250: bytes=32 time=85ms TTL=128
Reply from 172.16.103.250: bytes=32 time=95ms TTL=128
Reply from 172.16.103.250: bytes=32 time=75ms TTL=128
Reply from 172.16.103.250: bytes=32 time=85ms TTL=128
Reply from 172.16.103.250: bytes=32 time=78ms TTL=128
Reply from 172.16.103.250: bytes=32 time=63ms TTL=128
Reply from 172.16.103.250: bytes=32 time=59ms TTL=128
Reply from 172.16.103.250: bytes=32 time=66ms TTL=128
Reply from 172.16.103.250: bytes=32 time=69ms TTL=128
Reply from 172.16.103.250: bytes=32 time=66ms TTL=128
Reply from 172.16.103.250: bytes=32 time=65ms TTL=128
Reply from 172.16.103.250: bytes=32 time=60ms TTL=128
Reply from 172.16.103.250: bytes=32 time=75ms TTL=128
```

26. Return to **remote1-wkst** and the pings to **remote2-wkst** will now be working.

Figure 448. Pings work now.

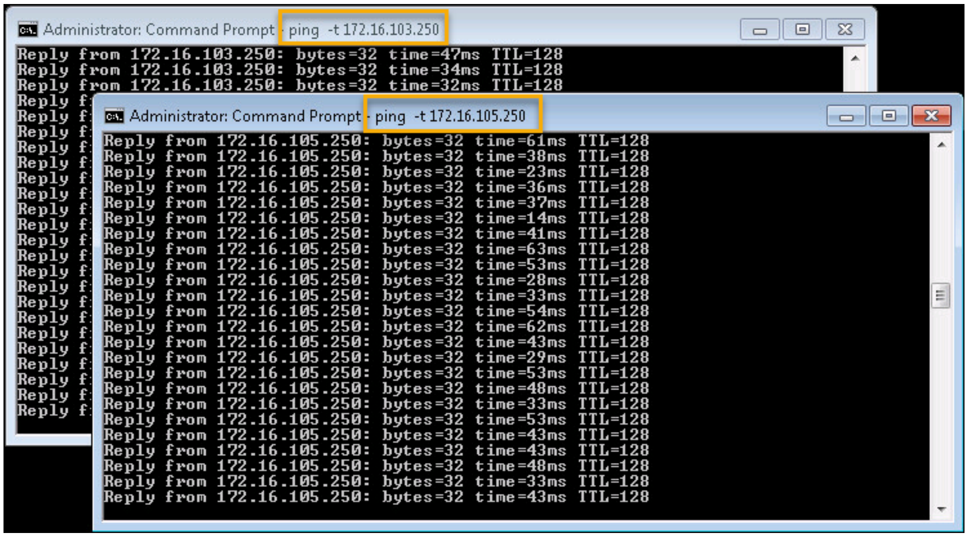


Administrator: Command Prompt - ping -t 172.16.105.250

```
Reply from 172.16.105.250: bytes=32 time=55ms TTL=128
Reply from 172.16.105.250: bytes=32 time=75ms TTL=128
Reply from 172.16.105.250: bytes=32 time=74ms TTL=128
Reply from 172.16.105.250: bytes=32 time=75ms TTL=128
Reply from 172.16.105.250: bytes=32 time=83ms TTL=128
Reply from 172.16.105.250: bytes=32 time=86ms TTL=128
Reply from 172.16.105.250: bytes=32 time=54ms TTL=128
Reply from 172.16.105.250: bytes=32 time=75ms TTL=128
Reply from 172.16.105.250: bytes=32 time=75ms TTL=128
Reply from 172.16.105.250: bytes=32 time=72ms TTL=128
Reply from 172.16.105.250: bytes=32 time=97ms TTL=128
Reply from 172.16.105.250: bytes=32 time=65ms TTL=128
Reply from 172.16.105.250: bytes=32 time=75ms TTL=128
Reply from 172.16.105.250: bytes=32 time=66ms TTL=128
Reply from 172.16.105.250: bytes=32 time=88ms TTL=128
Reply from 172.16.105.250: bytes=32 time=78ms TTL=128
Reply from 172.16.105.250: bytes=32 time=66ms TTL=128
Reply from 172.16.105.250: bytes=32 time=44ms TTL=128
Reply from 172.16.105.250: bytes=32 time=100ms TTL=128
Reply from 172.16.105.250: bytes=32 time=80ms TTL=128
Reply from 172.16.105.250: bytes=32 time=45ms TTL=128
Reply from 172.16.105.250: bytes=32 time=64ms TTL=128
Reply from 172.16.105.250: bytes=32 time=71ms TTL=128
Reply from 172.16.105.250: bytes=32 time=59ms TTL=128
```

27. On **hq-wkst** ping remote1-wkst and remote2-wkst.

Figure 449. Pings from hq-wkst



Administrator: Command Prompt - ping -t 172.16.103.250

```
Reply from 172.16.103.250: bytes=32 time=47ms TTL=128
Reply from 172.16.103.250: bytes=32 time=34ms TTL=128
Reply from 172.16.103.250: bytes=32 time=32ms TTL=128
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
Reply f
```

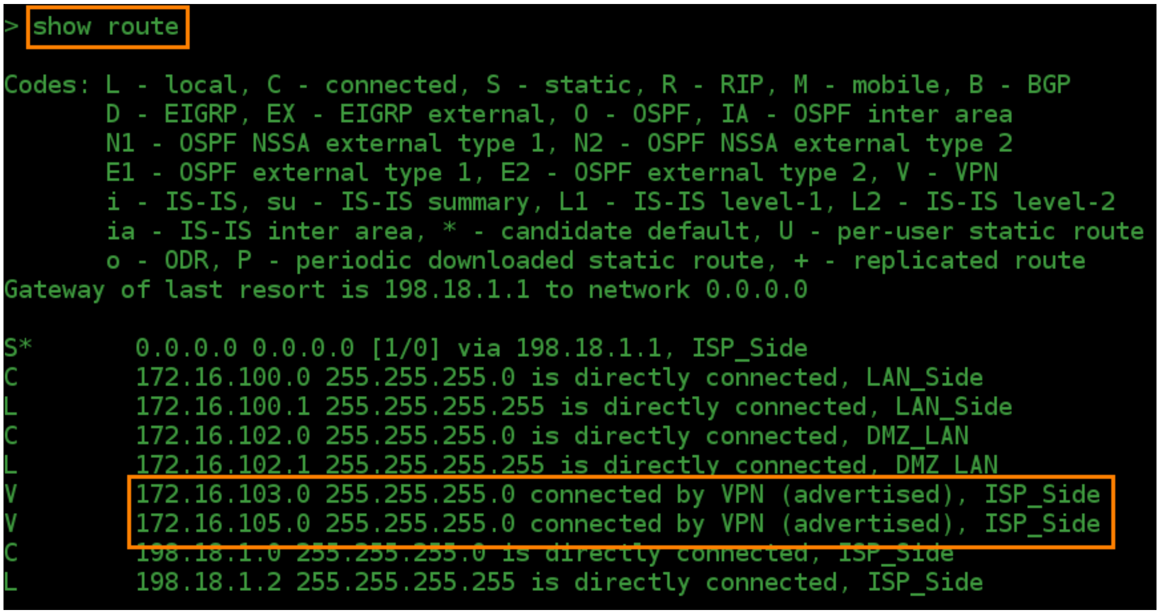
Administrator: Command Prompt - ping -t 172.16.105.250

```
Reply from 172.16.105.250: bytes=32 time=61ms TTL=128
Reply from 172.16.105.250: bytes=32 time=38ms TTL=128
Reply from 172.16.105.250: bytes=32 time=23ms TTL=128
Reply from 172.16.105.250: bytes=32 time=36ms TTL=128
Reply from 172.16.105.250: bytes=32 time=37ms TTL=128
Reply from 172.16.105.250: bytes=32 time=14ms TTL=128
Reply from 172.16.105.250: bytes=32 time=41ms TTL=128
Reply from 172.16.105.250: bytes=32 time=63ms TTL=128
Reply from 172.16.105.250: bytes=32 time=53ms TTL=128
Reply from 172.16.105.250: bytes=32 time=28ms TTL=128
Reply from 172.16.105.250: bytes=32 time=33ms TTL=128
Reply from 172.16.105.250: bytes=32 time=54ms TTL=128
Reply from 172.16.105.250: bytes=32 time=62ms TTL=128
Reply from 172.16.105.250: bytes=32 time=43ms TTL=128
Reply from 172.16.105.250: bytes=32 time=29ms TTL=128
Reply from 172.16.105.250: bytes=32 time=53ms TTL=128
Reply from 172.16.105.250: bytes=32 time=48ms TTL=128
Reply from 172.16.105.250: bytes=32 time=33ms TTL=128
Reply from 172.16.105.250: bytes=32 time=53ms TTL=128
Reply from 172.16.105.250: bytes=32 time=43ms TTL=128
Reply from 172.16.105.250: bytes=32 time=43ms TTL=128
Reply from 172.16.105.250: bytes=32 time=48ms TTL=128
Reply from 172.16.105.250: bytes=32 time=33ms TTL=128
Reply from 172.16.105.250: bytes=32 time=43ms TTL=128
```

Whew! Six continuous pings. In the excitement to get the VPN working did you happen to figure out what you enabled that you shouldn't have yet?

28. On the **hq-ftd tab**, issue the command **show route**. If the tunnel is configured, you should see some routes that are "connected by VPN".

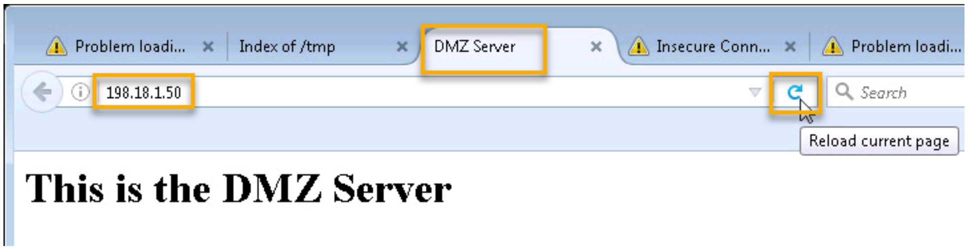
Figure 450. Show route



```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 198.18.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 198.18.1.1, ISP_Side
C        172.16.100.0 255.255.255.0 is directly connected, LAN_Side
L        172.16.100.1 255.255.255.255 is directly connected, LAN_Side
C        172.16.102.0 255.255.255.0 is directly connected, DMZ_LAN
L        172.16.102.1 255.255.255.255 is directly connected, DMZ_LAN
V        172.16.103.0 255.255.255.0 connected by VPN (advertised), ISP_Side
V        172.16.105.0 255.255.255.0 connected by VPN (advertised), ISP_Side
C        198.18.1.0 255.255.255.0 is directly connected, ISP_Side
L        198.18.1.2 255.255.255.255 is directly connected, ISP_Side
```

29. Once all the above pings work then on either **remote workstation** open up **Firefox** and go to **http://172.16.102.50** (the DMZ Server's internal IP address).

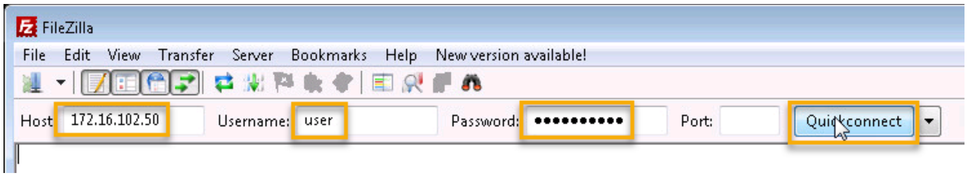
Figure 451. DMZ Server URL



This is the DMZ Server

30. On that same workstation open up **FileZilla** and use the **Quickconnect** fields to FTP to the DMZ server's internal IP address (**172.16.102.50**) and log in as **user**/**C1sco12345**. Don't use the saved link for the DMZ server because it used the DMZ server's outside IP address (198.18.1.50).

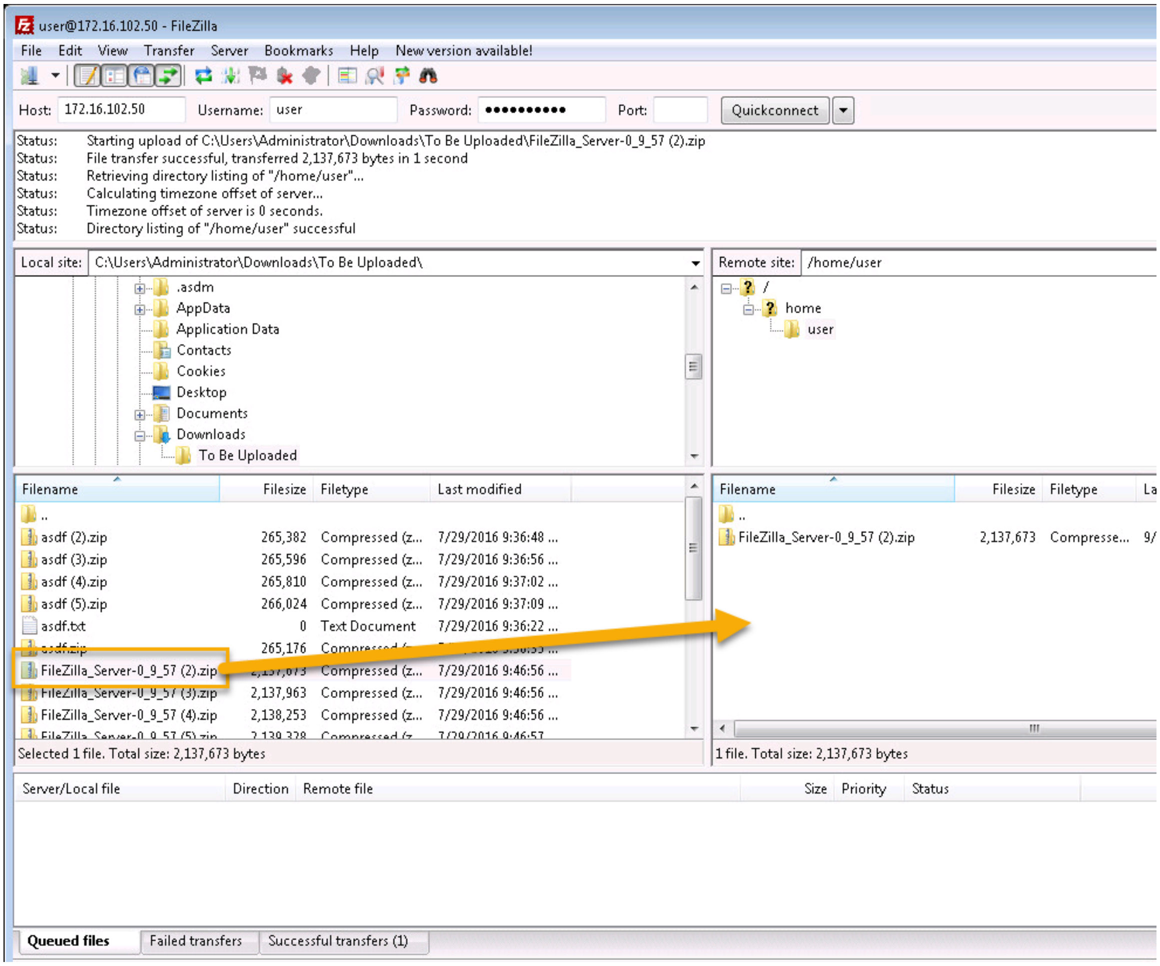
Figure 452. FTP to DMZ Server


FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
Quickconnect

Host: 172.16.102.50 Username: user Password: ●●●●●●●●●●● Port:

31. Once logged in select a file from the DMZ server and **upload** to the server. Oops. That succeeded!

Figure 453. Downloading file via FTP



Host: 172.16.102.50 Username: user Password: •••••••••• Port:

```
Status:    Starting upload of C:\Users\Administrator\Downloads\To Be Uploaded\FileZilla_Server-0_9_57 (2).zip
Status:    File transfer successful, transferred 2,137,673 bytes in 1 second
Status:    Retrieving directory listing of "/home/user"...
Status:    Calculating timezone offset of server...
Status:    Timezone offset of server is 0 seconds.
Status:    Directory listing of "/home/user" successful
```

Local site: C:\Users\Administrator\Downloads\To Be Uploaded\

- .asdm
- AppData
- Application Data
- Contacts
- Cookies
- Desktop
- Documents
- Downloads
  - To Be Uploaded

Remote site: /home/user

- /
  - home
    - user

Filename	Filesize	Filetype	Last modified
..			
asdf (2).zip	265,382	Compressed (z...	7/29/2016 9:36:48 ...
asdf (3).zip	265,596	Compressed (z...	7/29/2016 9:36:56 ...
asdf (4).zip	265,810	Compressed (z...	7/29/2016 9:37:02 ...
asdf (5).zip	266,024	Compressed (z...	7/29/2016 9:37:09 ...
asdf.txt	0	Text Document	7/29/2016 9:36:22 ...
asdf.zip	265,176	Compressed (z...	7/29/2016 9:36:33 ...
FileZilla_Server-0_9_57 (2).zip	2,137,673	Compressed (z...	7/29/2016 9:46:56 ...
FileZilla_Server-0_9_57 (3).zip	2,137,963	Compressed (z...	7/29/2016 9:46:56 ...
FileZilla_Server-0_9_57 (4).zip	2,138,253	Compressed (z...	7/29/2016 9:46:56 ...
FileZilla_Server-0_9_57 (5).zip	2,139,328	Compressed (z...	7/29/2016 9:46:57

Selected 1 file. Total size: 2,137,673 bytes

Filename	Filesize	Filetype	La
..			
FileZilla_Server-0_9_57 (2).zip	2,137,673	Compresse...	9/

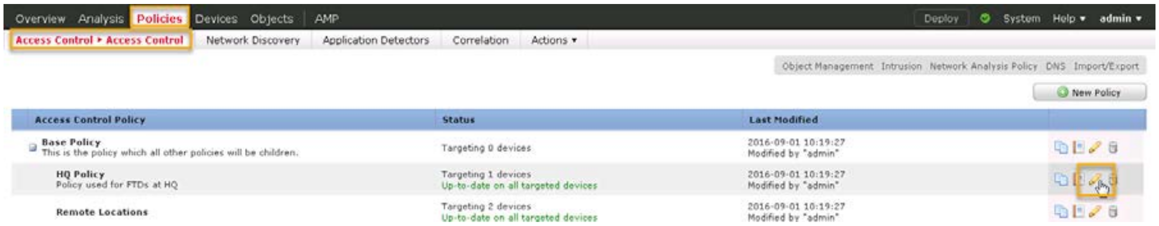
1 file. Total size: 2,137,673 bytes

Fix the Issue with the VPN Configuration

It was a long time back in the lab but, if you recall, Example Corp expressly stated that **only the HQ LAN should have FTP and SSH access to the DMZ server**. This is a case where being too permissive in your NAT and Access Control Policy rules had allowed something to happen that shouldn't. There are two ways to remedy this using the FTD devices. **Either you need to create an ACP rule specifically blocking this traffic or you need to remove the DMZ LAN from the protected VPN networks.** In this lab we are going to perform the former.

32. In the FMC administration website navigate to **Policies > Access Control > Access Control** and **edit** the **HQ Policy**.

Figure 454. Edit HQ Policy ACP



Access Control Policy	Status	Last Modified
Base Policy This is the policy which all other policies will be children.	Targeting 0 devices	2016-09-01 10:19:27 Modified by "admin"
HQ Policy Policy used for FTDs at HQ	Targeting 1 devices Up-to-date on all targeted devices	2016-09-01 10:19:27 Modified by "admin"
Remote Locations	Targeting 2 devices Up-to-date on all targeted devices	2016-09-01 10:19:27 Modified by "admin"

33. Click **Add Rule** and use the following to build a new rule to block the Remote sites from accessing the DMZ server using SSH or FTP.

There are several methods to setting fixing this issue. Trying to think beyond the immediate topology design I chose to create the rules in the HQ Policy policy instead of in the Base Policy so that IF, in the future, Example Corp wanted to create DMZ networks at each of the remote location the rule you are creating now would only affect THIS DMZ network. Alternatively, you could have put this rule in the Remote Locations Policy but then it could possibly affect other future configurations.

   a. Name: **Deny Access to DMZ Server**

   b. Enabled: **Checked**

   c. Insert: **below rule** and then **3**. (Rule #3 should be the HQ LAN to DMZ Server rule that permits the HQ LAN. This rule will now deny that same traffic to "catch-all" the rest of the networks.)

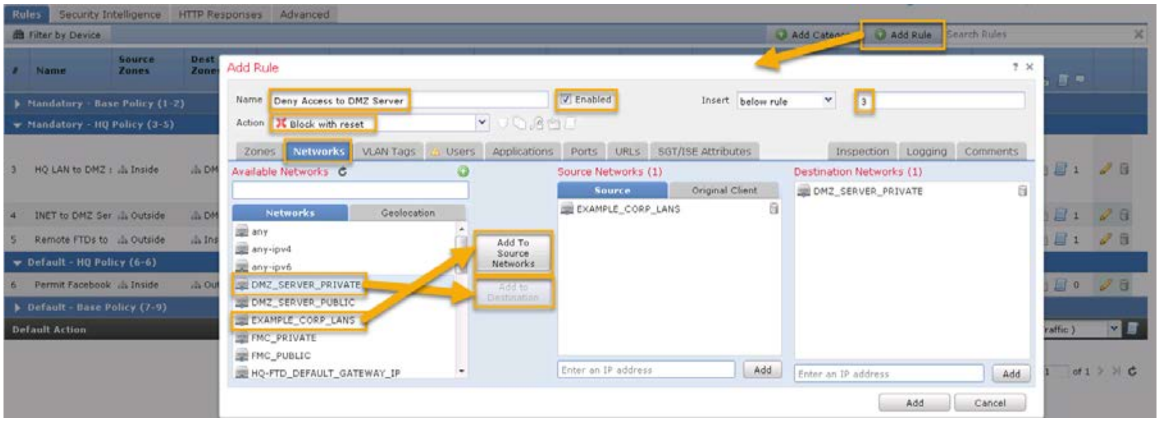
   d. Action: **Block with reset**

34. On the **Networks tab**:

   a. Source Networks: **EXAMPLE_CORP_LANS**

   b. Destination Networks: **DMZ_SERVER_PRIVATE**

Figure 455. Part 1 Adding rule



Name: Deny Access to DMZ Server
☑ Enabled
Insert: below rule 3
Action: Block with reset

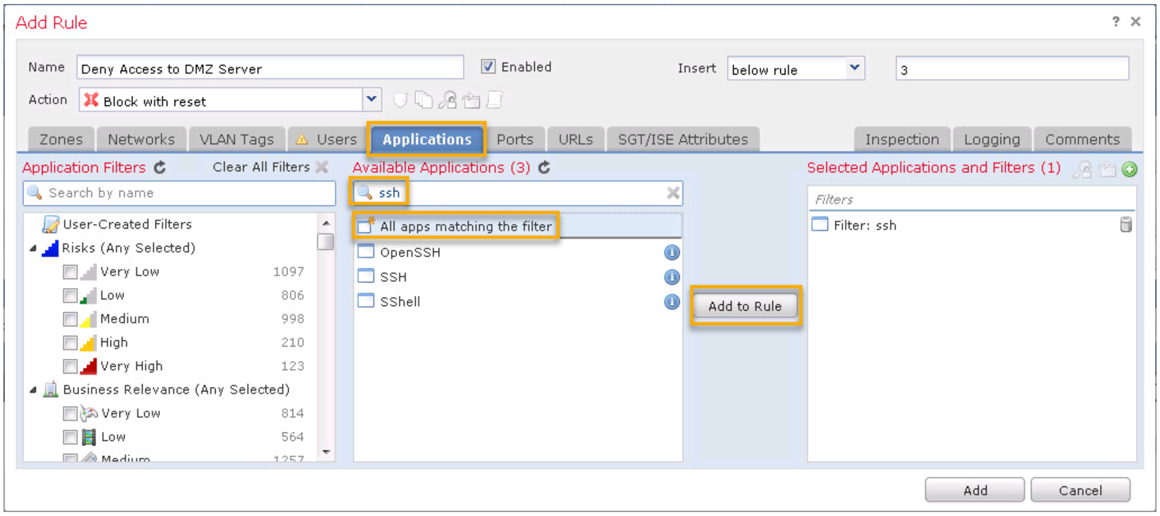
Source Networks (1)
EXAMPLE_CORP_LANS

Destination Networks (1)
DMZ_SERVER_PRIVATE

35. On the **Applications tab**:

    a. In **Available Applications** search for **ssh**. Then select the **All apps matching this filter** and click **Add to Rule**.

Figure 456. Add ssh to rule



Add Rule

Name: Deny Access to DMZ Server ☑ Enabled Insert: below rule 3

Action: Block with reset

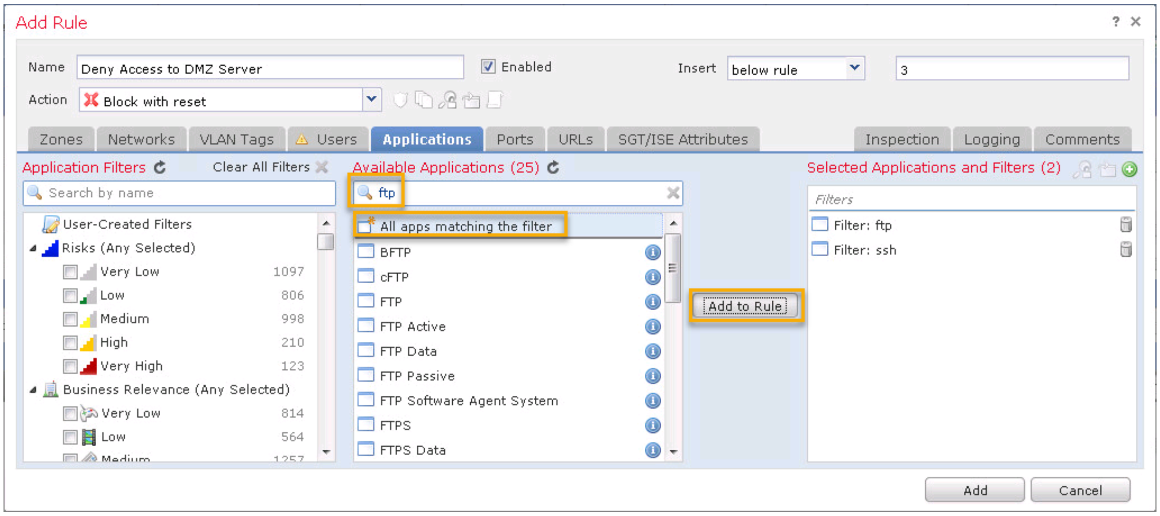
Available Applications (3): ssh

Selected Applications and Filters (1)

Filter: ssh

    b. In **Available Applications** search for **ftp**. Then select the **All apps matching this filter** and click **Add to Rule**.

Figure 457. Configure Applications tab



Add Rule

Name: Deny Access to DMZ Server ☑ Enabled Insert: below rule 3

Action: Block with reset

Available Applications (25): ftp

Selected Applications and Filters (2)

Filter: ftp

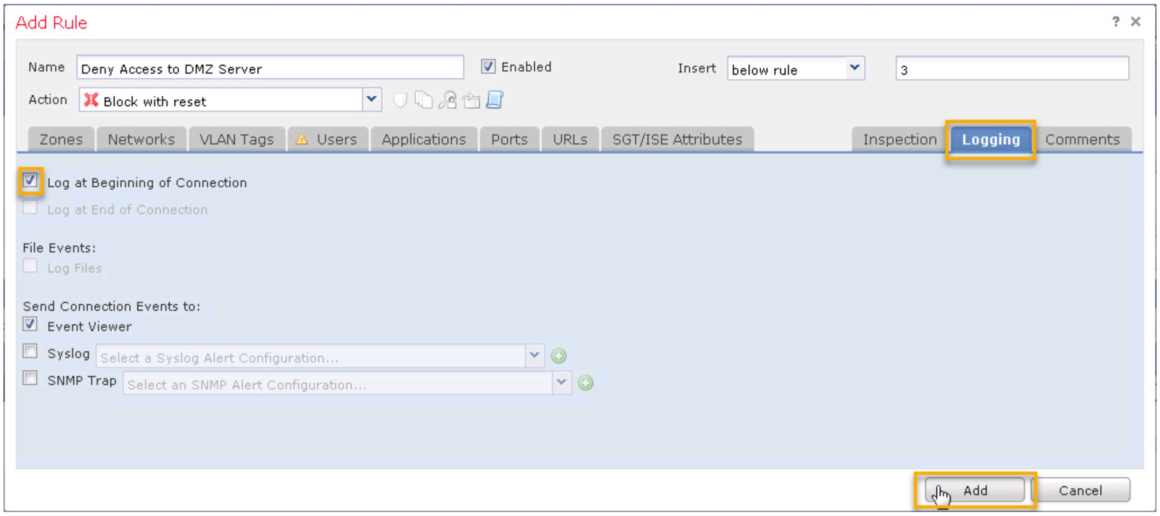
Filter: ssh

36. On the **Logging tab**:

    a. Check the **Log at Beginning of Connection** box.

37. Click **Add**

Figure 458. Configure Logging and Save



Name: Deny Access to DMZ Server
☑ Enabled
Insert: below rule
3
Action: Block with reset

☑ Log at Beginning of Connection
□ Log at End of Connection

File Events:
□ Log Files

Send Connection Events to:
☑ Event Viewer
□ Syslog Select a Syslog Alert Configuration...
□ SNMP Trap Select an SNMP Alert Configuration...

38. Click **Save**, **Deploy**, select **hq-ftd** and then click **Deploy**.

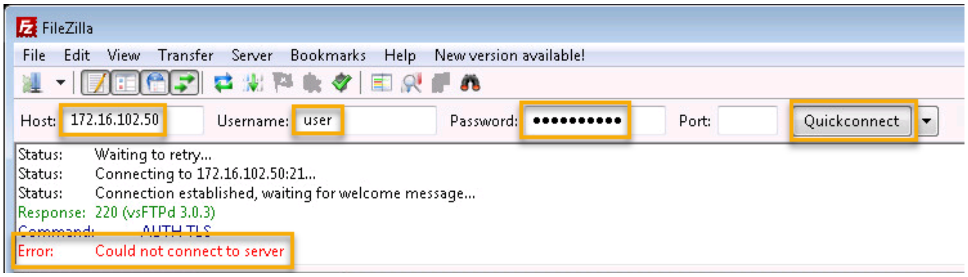
Did you notice how only the HQ FTD was available to deploy to? Why is that?

One of the down sides of configuring this rule this way is that traffic from the remote locations that would match this rule have to traverse the tunnel before they are blocked at hq-ftd. This is deemed acceptable since this traffic should be very limited. It is important to think of the flow of the traffic too when deciding where best to position your Access Control Policy rules.

39. Once the deployment has completed repeat the previous FTP test. On the **remote workstation** close and then reopen **FileZilla**.

40. Attempt to establish an **FTP** connection to **172.16.102.50** as **user**/**C1sco12345** again. This should fail.

Figure 459. Attempt to reconnect to DMZ via FileZilla

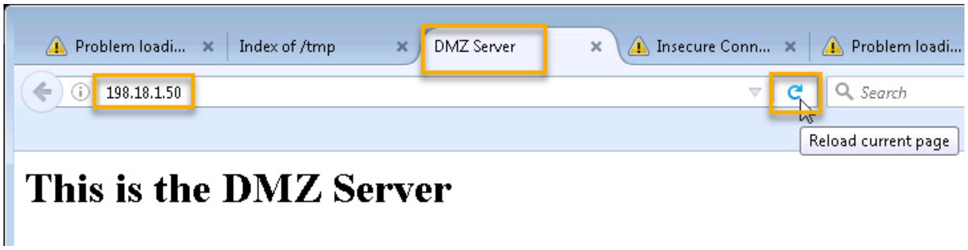


Host: 172.16.102.50 Username: user Password: ••••••••••• Port:

```
Status:     Waiting to retry...
Status:     Connecting to 172.16.102.50:21...
Status:     Connection established, waiting for welcome message...
Response:   220 (vsFTPd 3.0.3)
Command:    AUTH TLS
Error:      Could not connect to server
```

41. Make sure that this workstation still has access to the DMZ server's web page using the internal IP though. Go to **http://172.16.102.50**. This should work.

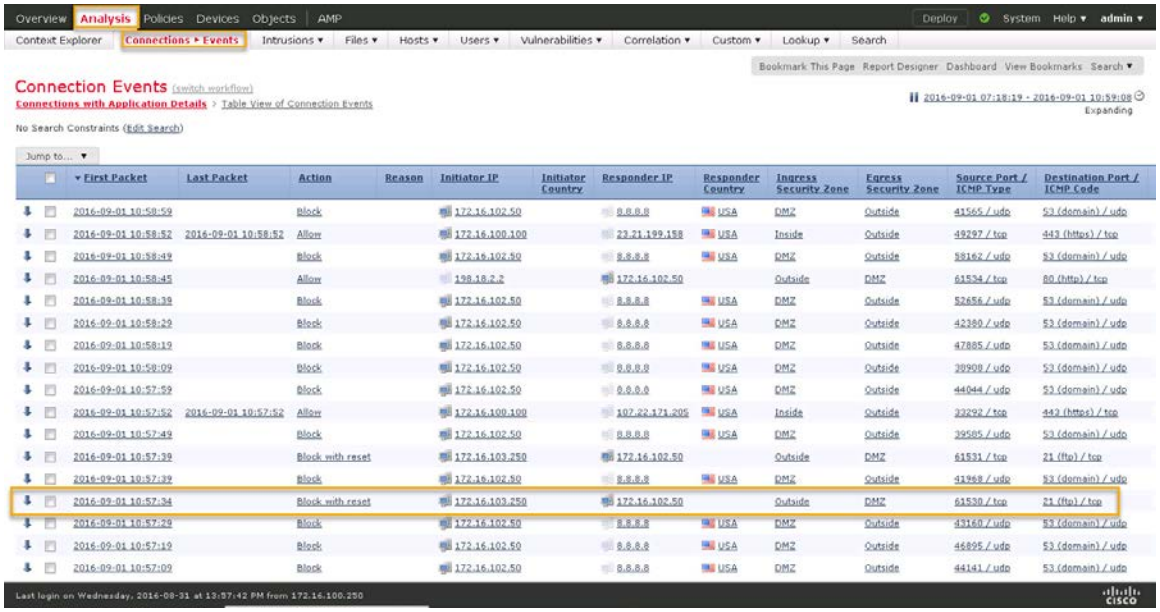
Figure 460. HTTP still works



This is the DMZ Server

42. Return to the FMC administration webpage and Navigate to **Analysis > Connections > Events**. Look for your most recent FTP attempt from the remote workstation to the DMZ server.

Figure 461. Review Connection Events



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

2016-09-01 07:18:19 - 2016-09-01 10:59:08
Expanding

□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
□	2016-09-01 10:58:59		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	41565 / udp	53 (domain) / udp
□	2016-09-01 10:58:52	2016-09-01 10:58:52	Allow		172.16.100.100		23.21.199.158	USA	Inside	Outside	49297 / tcp	443 (https) / tcp
□	2016-09-01 10:58:49		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	58162 / udp	53 (domain) / udp
□	2016-09-01 10:58:45		Allow		198.18.2.2		172.16.102.50		Outside	DMZ	61534 / tcp	80 (http) / tcp
□	2016-09-01 10:58:39		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	52656 / udp	53 (domain) / udp
□	2016-09-01 10:58:29		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	42380 / udp	53 (domain) / udp
□	2016-09-01 10:58:19		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	47885 / udp	53 (domain) / udp
□	2016-09-01 10:58:09		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	38908 / udp	53 (domain) / udp
□	2016-09-01 10:57:59		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	44044 / udp	53 (domain) / udp
□	2016-09-01 10:57:52	2016-09-01 10:57:52	Allow		172.16.100.100		107.22.171.205	USA	Inside	Outside	33292 / tcp	443 (https) / tcp
□	2016-09-01 10:57:49		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	39585 / udp	53 (domain) / udp
□	2016-09-01 10:57:39		Block with reset		172.16.103.250		172.16.102.50		Outside	DMZ	61531 / tcp	21 (ftp) / tcp
□	2016-09-01 10:57:39		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	41968 / udp	53 (domain) / udp
□	2016-09-01 10:57:34		Block with reset		172.16.103.250		172.16.102.50		Outside	DMZ	61530 / tcp	21 (ftp) / tcp
□	2016-09-01 10:57:29		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	43160 / udp	53 (domain) / udp
□	2016-09-01 10:57:19		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	46895 / udp	53 (domain) / udp
□	2016-09-01 10:57:09		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	44141 / udp	53 (domain) / udp

Last login on Wednesday, 2016-08-31 at 13:57:42 PM from 172.16.100.250

Scenario Summary

Currently the VPN capabilities of the FTD devices is for Site-to-Site VPNs. The remote connect (think AnyConnect VPN) ability still exists in the ASA code but hasn't been released yet in the FTD code. You should expect to see that ability in an upcoming version of the FTD code.

In this scenario you configured a Hub and Spoke VPN network between Example Corp's three sites. You also learned that testing more than "what should work" to include "what shouldn't work" is important as the initial VPN deployment enabled something that "shouldn't work".

Page intentionally left blank.

Scenario 12. FMC and FTD Maintenance

Scenario Description

Nothing is static in the information world: attacks change their behavior, bugs in systems need to be patched, IP address assignments change, etc. In concert with this, your FMC and FTD devices, which need to be monitored to confirm their health on a regular basis.

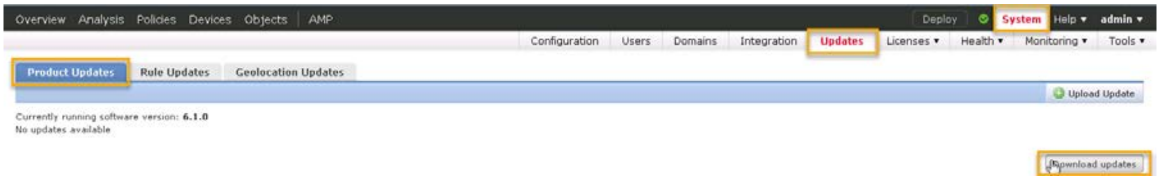
In this scenario you will learn how to update the available updates to the FMC and FTD devices, as well as learn about the different tests and health checks that are running to ensure the proper functioning of these devices.

Updating FMC Databases

Not that this step needs to be done first but rather it can take the longest (upwards of 45 minutes). So you start this scenario by looking at performing some of the updates that are available.

1. Navigate to **System > Updates**.
2. As you can see there are three tabs here. You will cover each and perform the latest update for each as well.
3. Click on the **Product Updates tab**:
4. At first you might think that there are no updates to be had based on the initial screen. Click on **Download updates** though and you should get some possible updates.

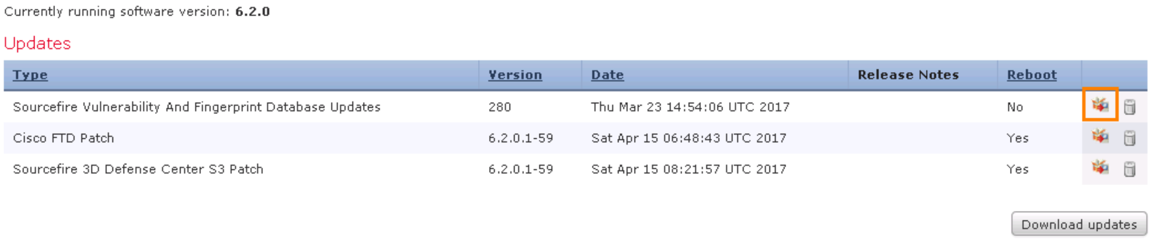
Figure 462. Download Updates



Currently running software version: **6.1.0**
No updates available

5. Once the page updates (which might take a minute or two) you should have at least one update that can be done. (As of the writing of this lab guide it was version 280 of the Sourcefire Vulnerability And Fingerprint Database Updates update.) On that row there are two links you can click. One installs the update and the other deletes it. Click the **Install** link.

Figure 463. Click Install



Currently running software version: **6.2.0**

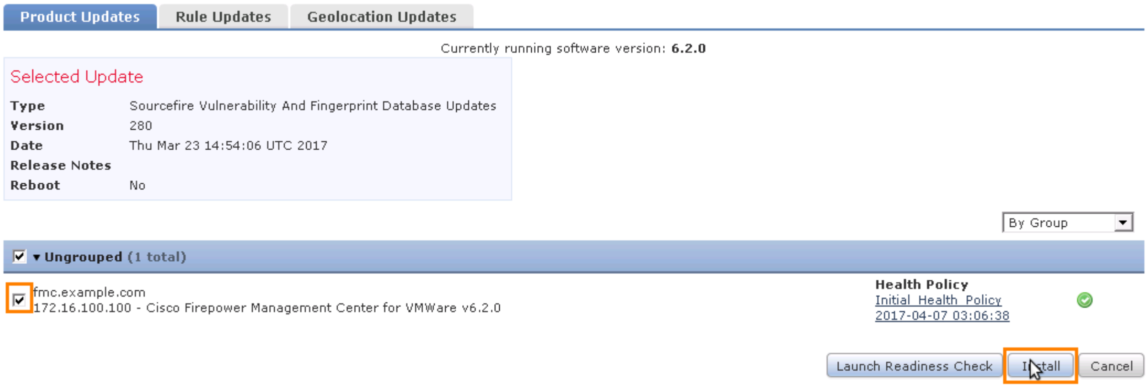
Updates

Type	Version	Date	Release Notes	Reboot	
Sourcefire Vulnerability And Fingerprint Database Updates	280	Thu Mar 23 14:54:06 UTC 2017		No	
Cisco FTD Patch	6.2.0.1-59	Sat Apr 15 06:48:43 UTC 2017		Yes	
Sourcefire 3D Defense Center S3 Patch	6.2.0.1-59	Sat Apr 15 08:21:57 UTC 2017		Yes	

The other updates on this page WILL cause the FTD and/or FMC devices to reboot as they are updates to the devices' OS. You are welcome to experiment but you risk changing (or breaking) steps in the lab.

6. Check the box for the **hq-fmc.example.lab** device and click **Install**.

Figure 464. Click Install



Currently running software version: **6.2.0**

Selected Update

Type	Sourcefire Vulnerability And Fingerprint Database Updates
Version	280
Date	Thu Mar 23 14:54:06 UTC 2017
Release Notes	
Reboot	No

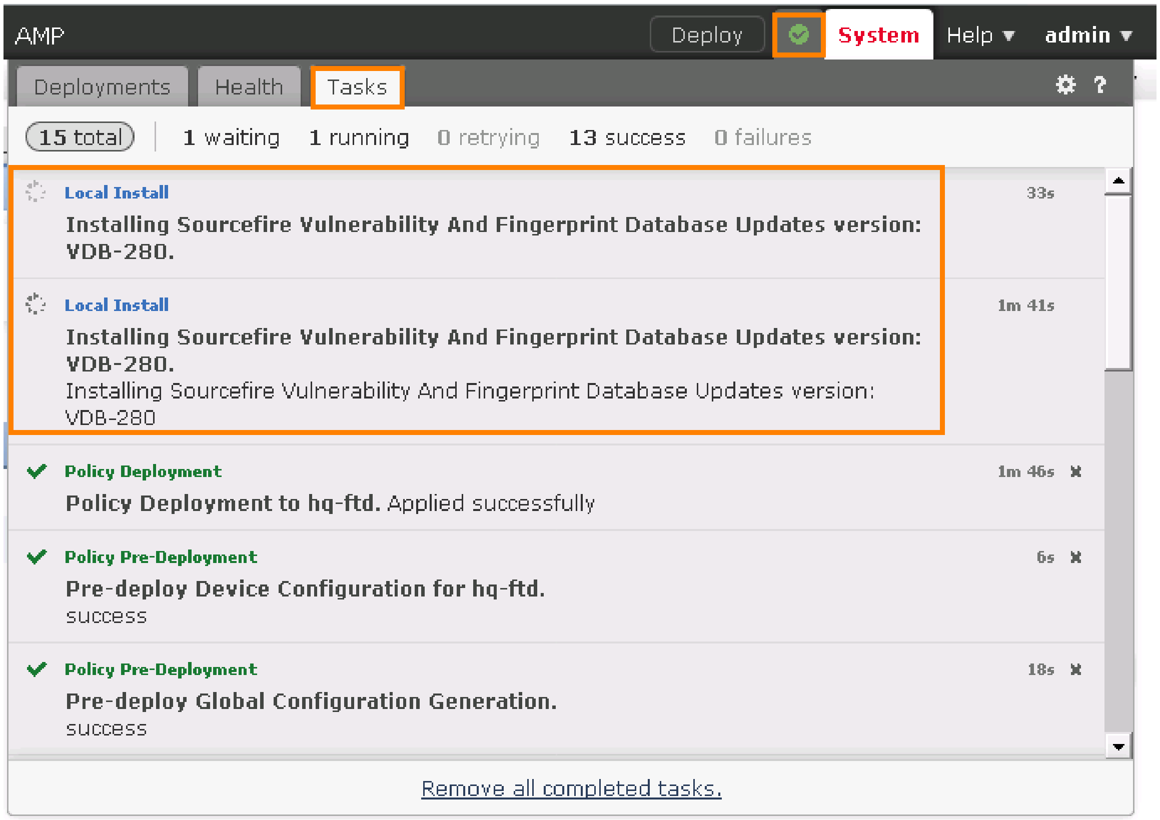
☑ ▾ **Ungrouped** (1 total)

☑ fmc.example.com
172.16.100.100 - Cisco Firepower Management Center for VMWare v6.2.0

Health Policy
Initial_Health_Policy
2017-04-07 03:06:38

7. In the **Message Center** on the **Tasks tab** you can see the progress of this update. This update takes about 10 minutes to install but feel free to continue the lab as you don't have to wait for the update to finish.

Figure 465. Message Center



15 total | 1 waiting | 1 running | 0 retrying | 13 success | 0 failures

Local Install 33s
Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-280.

Local Install 1m 41s
Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-280.
Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-280

✓ **Policy Deployment** 1m 46s
Policy Deployment to hq-ftd. Applied successfully

✓ **Policy Pre-Deployment** 6s
Pre-deploy Device Configuration for hq-ftd.
success

✓ **Policy Pre-Deployment** 18s
Pre-deploy Global Configuration Generation.
success

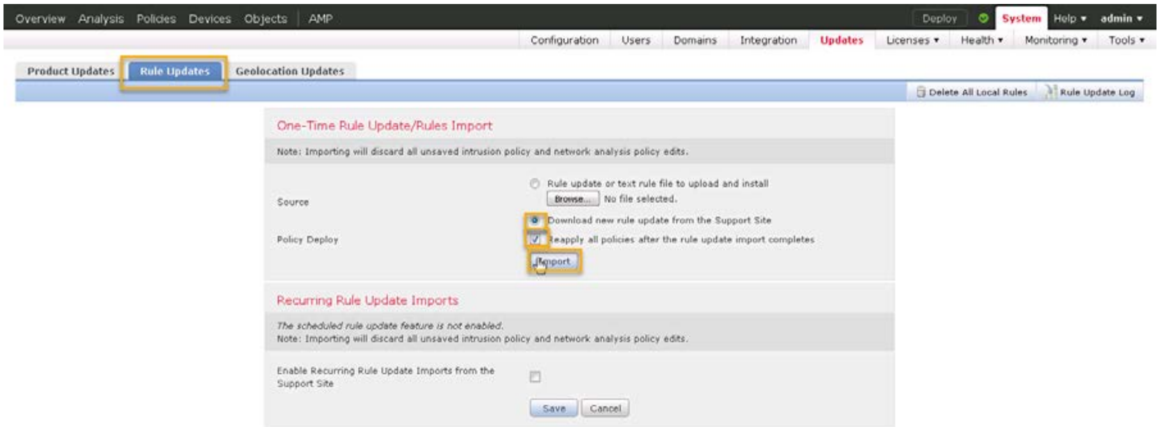
One thing to note here is that there is no "auto update" option for updates on this tab. The other tabs have that feature but this tab should be checked regularly to see if updates are available.

8. Click on the **Rules Updates tab**:

9. This page has more options than the last. As you can see, you can import a Rule update from an offline saved file or via the Support Site. Unless this FMC doesn't have Internet access the best option is to just allow it to reach out and grab the latest from the Support Site.

10. ***OPTIONAL STEP*** Click the **Download new rule update from the Support Site** radio button, check the **Reapply all policies after the rule update import completes** box and then click **Import**. The page will refresh BUT it will take about 10 minutes to do so. Do not browse away from the page.

Figure 466. Download and Import update



One-Time Rule Update/Rules Import

Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Source
○ Rule update or text rule file to upload and install
Browse... No file selected.
● Download new rule update from the Support Site

Policy Deploy
☑ Reapply all policies after the rule update import completes

Import

Recurring Rule Update Imports

The scheduled rule update feature is not enabled.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

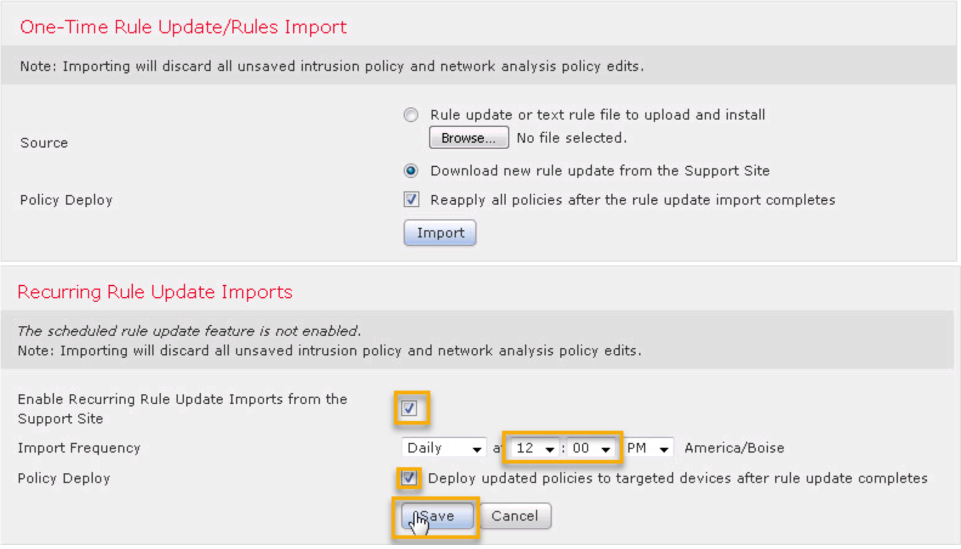
Enable Recurring Rule Update Imports from the Support Site □

Save Cancel

11. Take note of the Recurring Rule Update Imports section. With a few checks of the box you can have the FMC perform a regular check for updates and push those updates to the needed devices. Check the **Enable Recurring Rule Update Imports from the Support Site** box.

12. With that box check you can now set up the time and frequency of when updates are imported. You can also automatically deploy updates to the devices! For now, **set any time**, check the **Deploy updated policies to targeted devices after the rule update completes** box and click **Save**.

Figure 467. Enable Auto Updater



One-Time Rule Update/Rules Import

Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Source
○ Rule update or text rule file to upload and install
Browse... No file selected.
● Download new rule update from the Support Site

Policy Deploy
☑ Reapply all policies after the rule update import completes

Import

Recurring Rule Update Imports

The scheduled rule update feature is not enabled.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site ☑

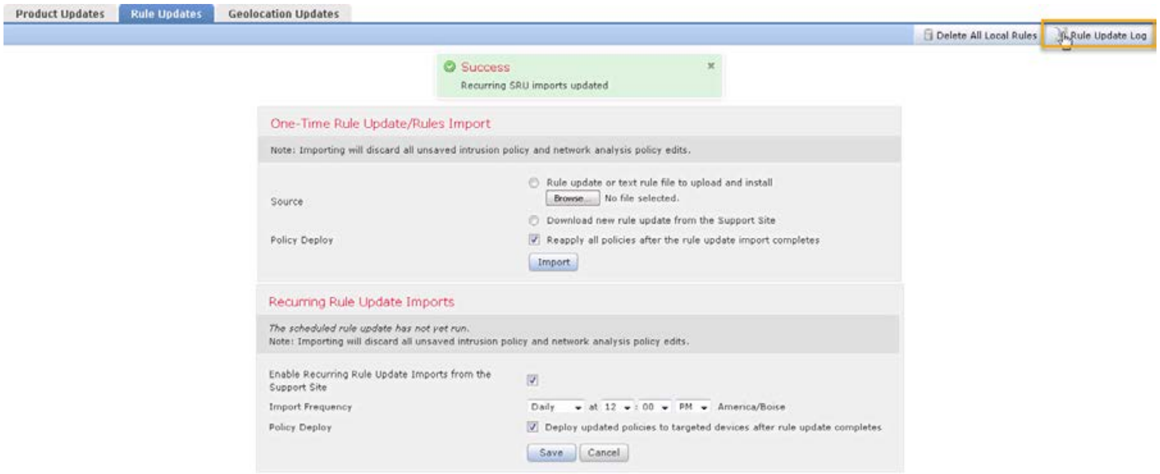
Import Frequency: Daily at 12 : 00 PM America/Boise

Policy Deploy ☑ Deploy updated policies to targeted devices after rule update completes

Save Cancel

13. Click the **Rule Update Log** to see a tabular list of want updates have been downloaded and when.

Figure 468. Click Rule Update Log



Success
Recurring SRU imports updated

One-Time Rule Update/Rules Import

Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Source
○ Rule update or text rule file to upload and install
Browse... No file selected.
○ Download new rule update from the Support Site

Policy Deploy
☑ Reapply all policies after the rule update import completes

Import

Recurring Rule Update Imports

The scheduled rule update has not yet run.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site ☑

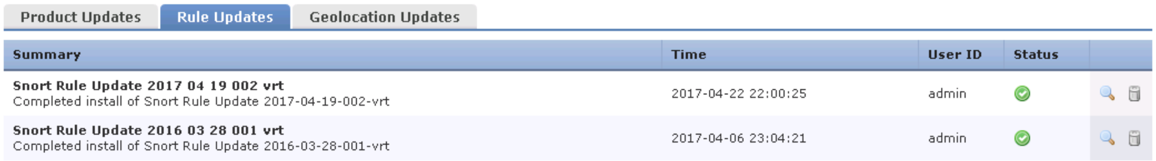
Import Frequency: Daily at 12 : 00 PM America/Boise

Policy Deploy ☑ Deploy updated policies to targeted devices after rule update completes

Save Cancel

14. View the log Summary.

Figure 469. View Log

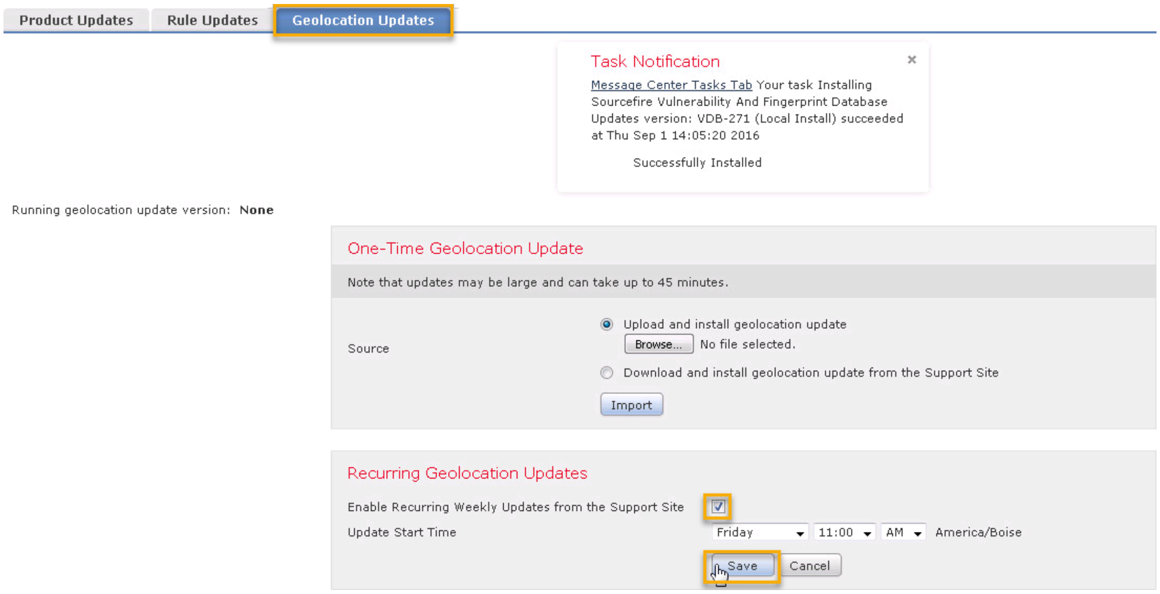


Summary	Time	User ID	Status
Snort Rule Update 2017 04 19 002 vrt Completed install of Snort Rule Update 2017-04-19-002-vrt	2017-04-22 22:00:25	admin	✓
Snort Rule Update 2016 03 28 001 vrt Completed install of Snort Rule Update 2016-03-28-001-vrt	2017-04-06 23:04:21	admin	✓

15. Click on the **Geolocation Updates tab**:

   a. The Geolocation Updates take the longest to download and install. So, let's set up the recurring settings first and then start the download. In the Recurring Geolocation Updates section check the **Enable Recurring Weekly Updates from the Support Site** box and click **Save**.

Figure 470. Enable Auto Updates



Task Notification

Message Center Tasks Tab Your task Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-271 (Local Install) succeeded at Thu Sep 1 14:05:20 2016

Successfully Installed

Running geolocation update version: **None**

One-Time Geolocation Update

Note that updates may be large and can take up to 45 minutes.

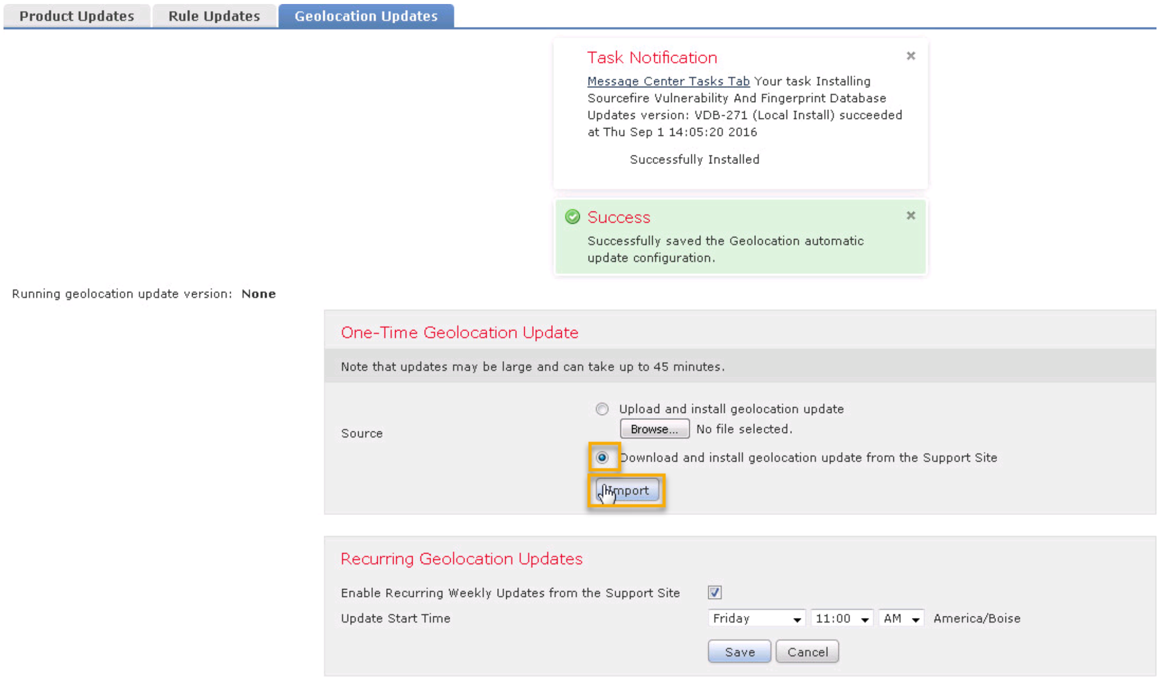
Source
● Upload and install geolocation update
Browse... No file selected.
○ Download and install geolocation update from the Support Site
Import

Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site ☑
Update Start Time: Friday 11:00 AM America/Boise

b. Now click the **Download and install geolocation update from the Support Site** radio button and then click **Import**.

Figure 471. Geolocation Updates



Task Notification

Message Center Tasks Tab Your task Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-271 (Local Install) succeeded at Thu Sep 1 14:05:20 2016

Successfully Installed

Success

Successfully saved the Geolocation automatic update configuration.

Running geolocation update version: **None**

One-Time Geolocation Update

Note that updates may be large and can take up to 45 minutes.

Source

○ Upload and install geolocation update

Browse... No file selected.

● Download and install geolocation update from the Support Site

Import

Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site ☑

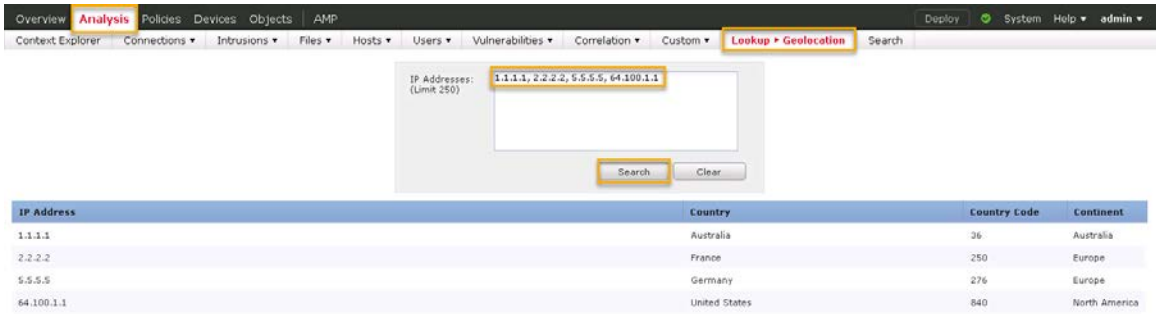
Update Start Time Friday 11:00 AM America/Boise

Whois and Geolocation Searches

This section doesn’t really belong in the “Monitoring and Maintenance” scenario but it is related to the Geolocation Database you have started to download. These two features provide informative information about an IP address, who owns it, and from what part of the world is it from.

16. Navigate to **Analysis > Lookup > Geolocation**.
17. In the textbox input the following IP address. **1.1.1.1, 2.2.2.2, 5.5.5.5 64.100.1.1**. You can separate the IPs with a space, a comma, or a new line (at least I tested each of these ways and they work).
18. Click **Search** and review the result. From this information you can determine the origin of the respective IP address.

Figure 472. See where IPs are Geolocated

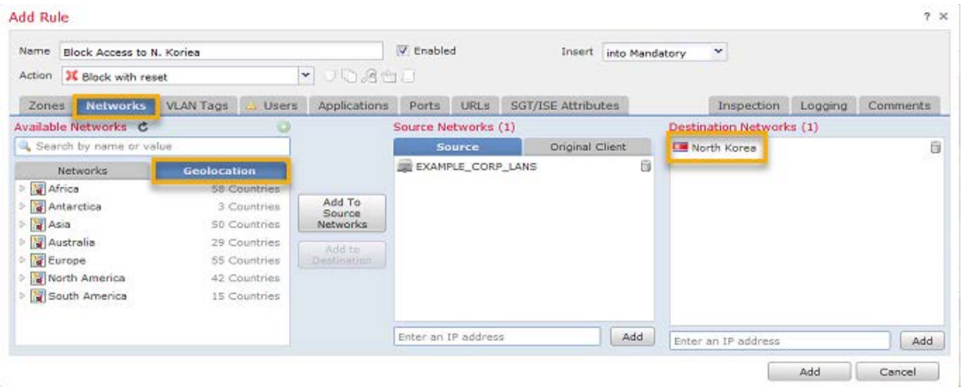


IP Addresses: (Limit 250) 1.1.1.1, 2.2.2.2, 5.5.5.5, 64.100.1.1

IP Address	Country	Country Code	Continent
1.1.1.1	Australia	36	Australia
2.2.2.2	France	250	Europe
5.5.5.5	Germany	276	Europe
64.100.1.1	United States	840	North America

19. This is only an example. The Geolocation database information can also be used in an ACP rule. You didn’t use this feature in this lab but the following screenshot shows you that you can create a rule to match against a geolocation database entry. In this example I created an ACP rule to block any traffic coming from EXAMPLE_CORP_LANS destined to the Geolocation of North Korea.

Figure 473. Block Access to North Korea



Name: Block Access to N. Koriea
☑ Enabled
Insert: into Mandatory
Action: Block with reset

Available Networks (Geolocation):

Africa	58 Countries
Antarctica	3 Countries
Asia	50 Countries
Australia	29 Countries
Europe	55 Countries
North America	42 Countries
South America	15 Countries

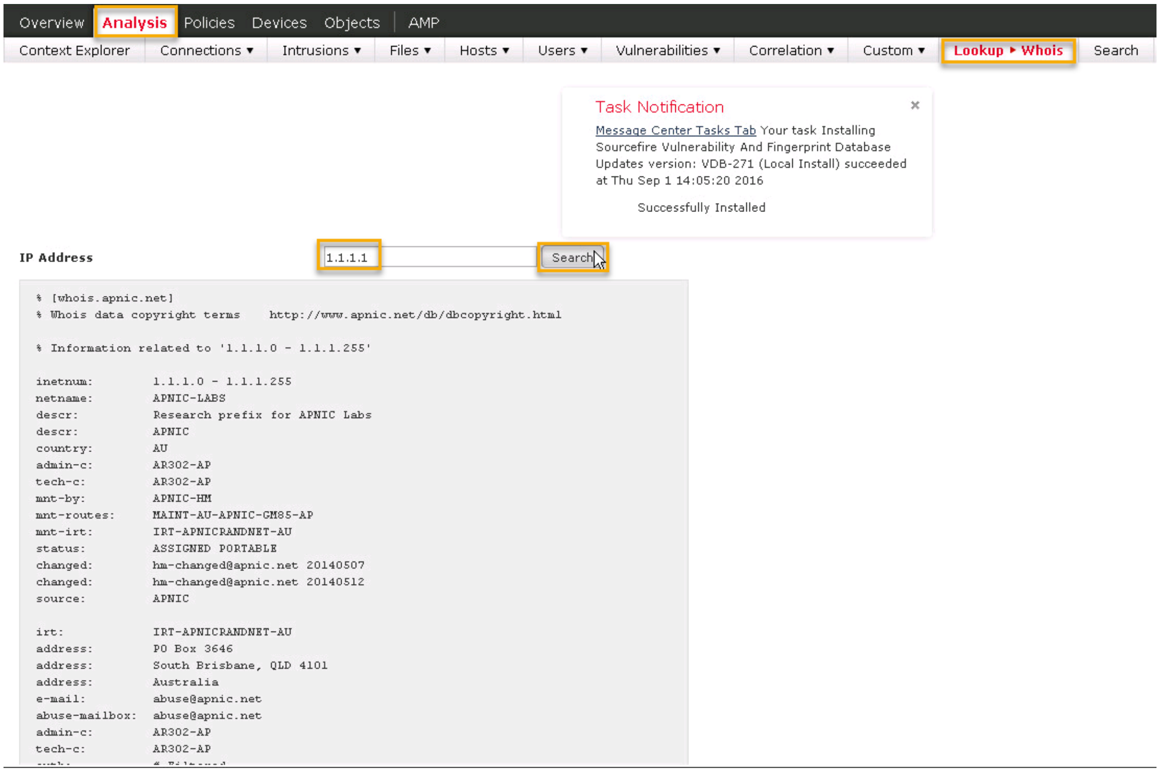
Source Networks (1): EXAMPLE_CORP_LANS

Destination Networks (1): North Korea

20. Navigate to **Analysis > Lookup > Whois**.

21. Use the same IP addresses from the Geolocation search to learn who has registered that IP and from what range of IPs is it from. Other IPs you might like to search are the 127.0.0.1 and 192.168.1.1 IPs.

Figure 474. Whois Results



Task Notification

Message Center Tasks Tab Your task Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-271 (Local Install) succeeded at Thu Sep 1 14:05:20 2016

Successfully Installed

IP Address 1.1.1.1 Search

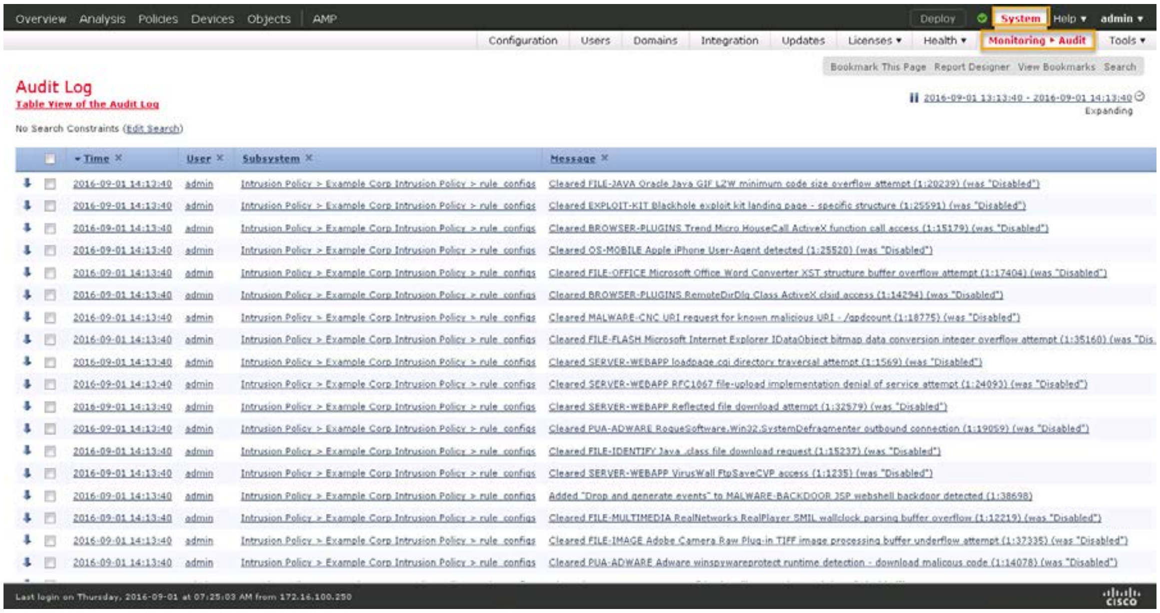
```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '1.1.1.0 - 1.1.1.255'

inetnum:        1.1.1.0 - 1.1.1.255
netname:        APNIC-LABS
descr:          Research prefix for APNIC Labs
descr:          APNIC
country:        AU
admin-c:        AR302-AP
tech-c:         AR302-AP
mnt-by:         APNIC-HM
mnt-routes:     MAINT-AU-APNIC-GM85-AP
mnt-irt:        IRT-APNICRANDNET-AU
status:         ASSIGNED PORTABLE
changed:        hm-changed@apnic.net 20140507
changed:        hm-changed@apnic.net 20140512
source:         APNIC

irt:            IRT-APNICRANDNET-AU
address:        PO Box 3646
address:        South Brisbane, QLD 4101
address:        Australia
e-mail:         abuse@apnic.net
abuse-mailbox:  abuse@apnic.net
admin-c:        AR302-AP
tech-c:         AR302-AP
auth:           # Filtered
```

System Monitor

The system monitor section contains great reporting information on the current status of what is going on in the management of the FMC and the devices it manages.

22. Navigate to **System > Monitoring > Audit**. This page lists all the actions that have been taken. Take a moment and look at the most recent entries and you can see it is an audit trail of all the things you've recently done on this FMC. Notice that the audit also keeps track of which user (or process) performed an action. This is a great case for having a unique login for each administrator.

Figure 475. Big Brother Knows Everything



Audit Log

Table View of the Audit Log

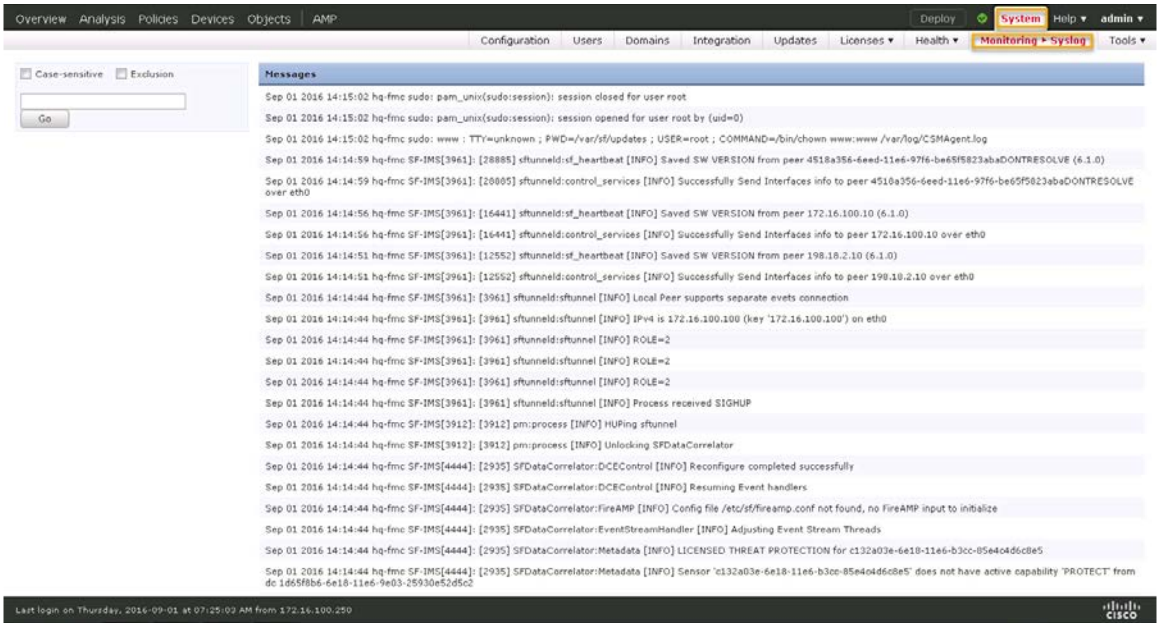
No Search Constraints (Edit Search)

2016-09-01 13:13:40 - 2016-09-01 14:13:40

	☐	▾ Time	User	Subsystem	Message
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared FILE-JAVA Oracle Java GIF LZW minimum code size overflow attempt (1:20239) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared EXPLOIT-KIT Blackhole exploit kit landing page - specific structure (1:25591) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared BROWSER-PLUGINS Trend Micro HouseCall ActiveX function call access (1:15179) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared OS-MOBILE Apple iPhone User-Agent detected (1:25520) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared FILE-OFFICE Microsoft Office Word Converter XST structure buffer overflow attempt (1:17404) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared BROWSER-PLUGINS RemoteDirDlg Class ActiveX clsid access (1:14294) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared MALWARE-CNC URI request for known malicious URI - /qpdcount (1:18775) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared FILE-FLASH Microsoft Internet Explorer IDataObject bitmap data conversion integer overflow attempt (1:35160) (was "Dis
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared SERVER-WEBAPP loadpage.cgi directory traversal attempt (1:1569) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared SERVER-WEBAPP RFC1867 file-upload implementation denial of service attempt (1:24093) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared SERVER-WEBAPP Reflected file download attempt (1:32579) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared PUA-ADWARE RogueSoftware.Win32.SystemDefragmenter outbound connection (1:19059) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared FILE-IDENTIFY Java .class file download request (1:15237) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared SERVER-WEBAPP VirusWall FtpSaveCVP access (1:1235) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Added "Drop and generate events" to MALWARE-BACKDOOR JSP webshell backdoor detected (1:38698)
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared FILE-MULTIMEDIA RealNetworks RealPlayer SMIL wallclock parsing buffer overflow (1:12219) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared FILE-IMAGE Adobe Camera Raw Plug-in TIFF image processing buffer underflow attempt (1:37335) (was "Disabled")
⬇	☐	2016-09-01 14:13:40	admin	Intrusion Policy > Example Corp Intrusion Policy > rule_configs	Cleared PUA-ADWARE Adware winspywareprotect runtime detection - download malicous code (1:14078) (was "Disabled")

23. Navigate to **System > Monitoring > Syslog**. As you might expect this is a view of the syslog buffer.

Figure 476. Syslog Buffer



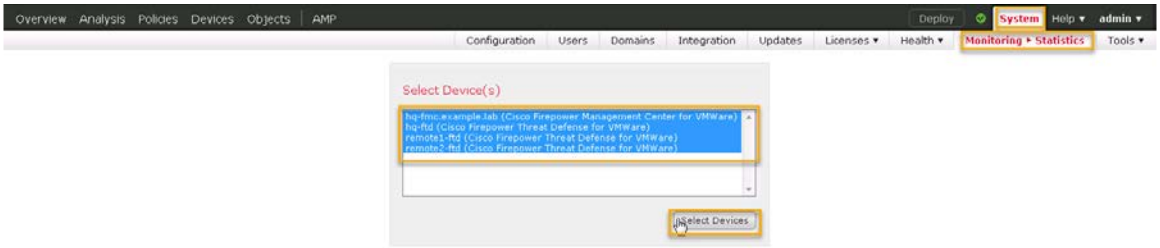
```
Sep 01 2016 14:15:02 hq-fmc sudo: pam_unix(sudo:session): session closed for user root
Sep 01 2016 14:15:02 hq-fmc sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 01 2016 14:15:02 hq-fmc sudo: www : TTY=unknown ; PWD=/var/sf/updates ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
Sep 01 2016 14:14:59 hq-fmc SF-IMS[3961]: [28885] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer 4518a356-6eed-11e6-97f6-be65f5823abaDONTRESOLVE (6.1.0)
Sep 01 2016 14:14:59 hq-fmc SF-IMS[3961]: [28885] sftunneld:control_services [INFO] Successfully Send Interfaces info to peer 4518a356-6eed-11e6-97f6-be65f5823abaDONTRESOLVE
over eth0
Sep 01 2016 14:14:56 hq-fmc SF-IMS[3961]: [16441] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer 172.16.100.10 (6.1.0)
Sep 01 2016 14:14:56 hq-fmc SF-IMS[3961]: [16441] sftunneld:control_services [INFO] Successfully Send Interfaces info to peer 172.16.100.10 over eth0
Sep 01 2016 14:14:51 hq-fmc SF-IMS[3961]: [12552] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer 198.18.2.10 (6.1.0)
Sep 01 2016 14:14:51 hq-fmc SF-IMS[3961]: [12552] sftunneld:control_services [INFO] Successfully Send Interfaces info to peer 198.18.2.10 over eth0
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3961]: [3961] sftunneld:sftunnel [INFO] Local Peer supports separate evets connection
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3961]: [3961] sftunneld:sftunnel [INFO] IPv4 is 172.16.100.100 (key '172.16.100.100') on eth0
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3961]: [3961] sftunneld:sftunnel [INFO] ROLE=2
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3961]: [3961] sftunneld:sftunnel [INFO] ROLE=2
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3961]: [3961] sftunneld:sftunnel [INFO] ROLE=2
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3961]: [3961] sftunneld:sftunnel [INFO] Process received SIGHUP
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3912]: [3912] pm:process [INFO] HUPing sftunnel
Sep 01 2016 14:14:44 hq-fmc SF-IMS[3912]: [3912] pm:process [INFO] Unlocking SFDataCorrelator
Sep 01 2016 14:14:44 hq-fmc SF-IMS[4444]: [2935] SFDataCorrelator:DCEControl [INFO] Reconfigure completed successfully
Sep 01 2016 14:14:44 hq-fmc SF-IMS[4444]: [2935] SFDataCorrelator:DCEControl [INFO] Resuming Event handlers
Sep 01 2016 14:14:44 hq-fmc SF-IMS[4444]: [2935] SFDataCorrelator:FireAMP [INFO] Config file /etc/sf/fireamp.conf not found, no FireAMP input to initialize
Sep 01 2016 14:14:44 hq-fmc SF-IMS[4444]: [2935] SFDataCorrelator:EventStreamHandler [INFO] Adjusting Event Stream Threads
Sep 01 2016 14:14:44 hq-fmc SF-IMS[4444]: [2935] SFDataCorrelator:Metadata [INFO] LICENSED THREAT PROTECTION for c132a03e-6e18-11e6-b3cc-85e4o4d6c8e5
Sep 01 2016 14:14:44 hq-fmc SF-IMS[4444]: [2935] SFDataCorrelator:Metadata [INFO] Sensor 'c132a03e-6e18-11e6-b3cc-85e4o4d6c8e5' does not have active capability 'PROTECT' from
dc 1d65f8b6-6e18-11e6-9e03-25930e52d5c2
```

Last login on Thursday, 2016-09-01 at 07:25:03 AM from 172.16.100.250

24. Navigate to **System > Monitoring > Statistics**.

25. Select at least one of the FTD devices and click **Select Devices**. (You can select all devices if you so choose to do so.)

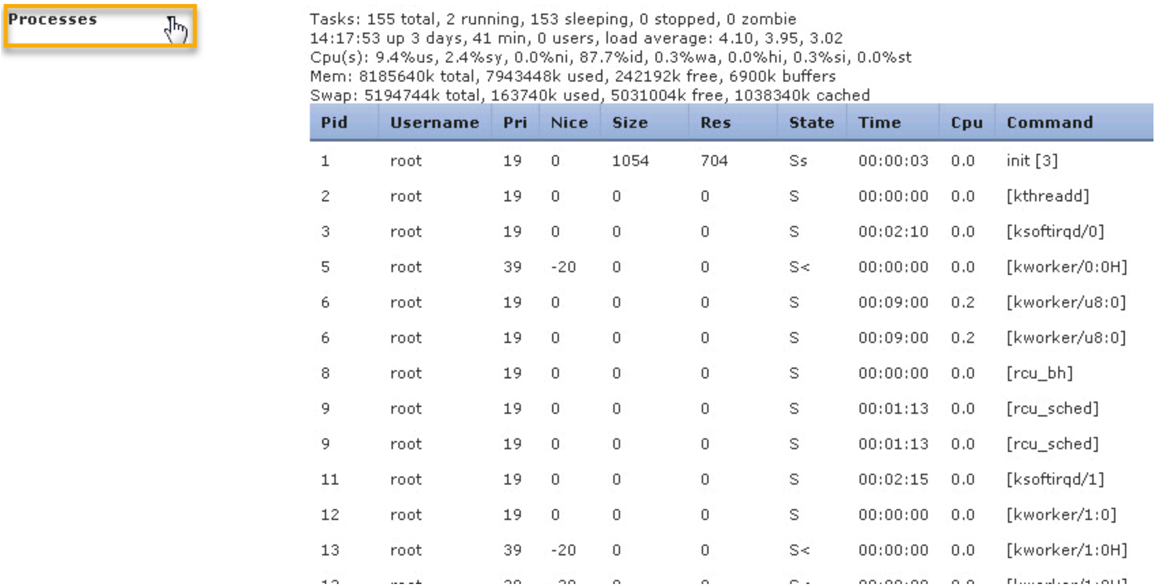
Figure 477. Select Devices to view Statistics



hq-fmc.example.lab (Cisco Firepower Management Center for VMWare)
hq-ftd (Cisco Firepower Threat Defense for VMWare)
remote1-ftd (Cisco Firepower Threat Defense for VMWare)
remote2-ftd (Cisco Firepower Threat Defense for VMWare)

26. When the page refreshes scroll down and notice the information that is gathered. Expand one of the **Processes links** and notice that you can even get a snapshot of what processes are currently running on that device. (For those of you who are familiar with Linux you should recognize most of this information as output from the “top” command.)

Figure 478. To “top” it all off



```
Tasks: 155 total, 2 running, 153 sleeping, 0 stopped, 0 zombie
14:17:53 up 3 days, 41 min, 0 users, load average: 4.10, 3.95, 3.02
Cpu(s): 9.4%us, 2.4%sy, 0.0%ni, 87.7%id, 0.3%wa, 0.0%hi, 0.3%si, 0.0%st
Mem: 8185640k total, 7943448k used, 242192k free, 6900k buffers
Swap: 5194744k total, 163740k used, 5031004k free, 1038340k cached
Pid  Username  Pri  Nice  Size  Res  State  Time      Cpu  Command
1    root      19   0     1054  704  Ss     00:00:03  0.0  init [3]
2    root      19   0     0     0    S      00:00:00  0.0  [kthreadd]
3    root      19   0     0     0    S      00:02:10  0.0  [ksoftirqd/0]
5    root      39   -20   0     0    S<     00:00:00  0.0  [kworker/0:0H]
6    root      19   0     0     0    S      00:09:00  0.2  [kworker/u8:0]
6    root      19   0     0     0    S      00:09:00  0.2  [kworker/u8:0]
8    root      19   0     0     0    S      00:00:00  0.0  [rcu_bh]
9    root      19   0     0     0    S      00:01:13  0.0  [rcu_sched]
9    root      19   0     0     0    S      00:01:13  0.0  [rcu_sched]
11   root      19   0     0     0    S      00:02:15  0.0  [ksoftirqd/1]
12   root      19   0     0     0    S      00:00:00  0.0  [kworker/1:0]
13   root      39   -20   0     0    S<     00:00:00  0.0  [kworker/1:0H]
```

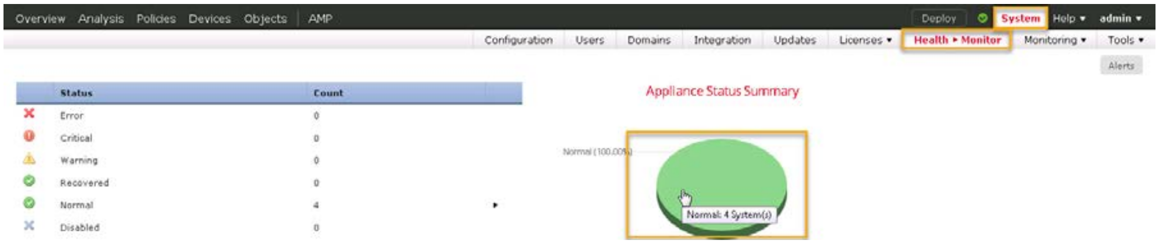
System Health

The System Health section is tightly related to what you see in the Message Center. This is where you see and customize what maintenance routines get run on which devices.

27. Navigate to **System > Health > Monitor**. Not the most informative of monitors but from here you can get a glimpse of the most urgent concerns regarding the health of any device that the FMC manages.

28. In order to get any information, you need to click on the **pie chart sections**.

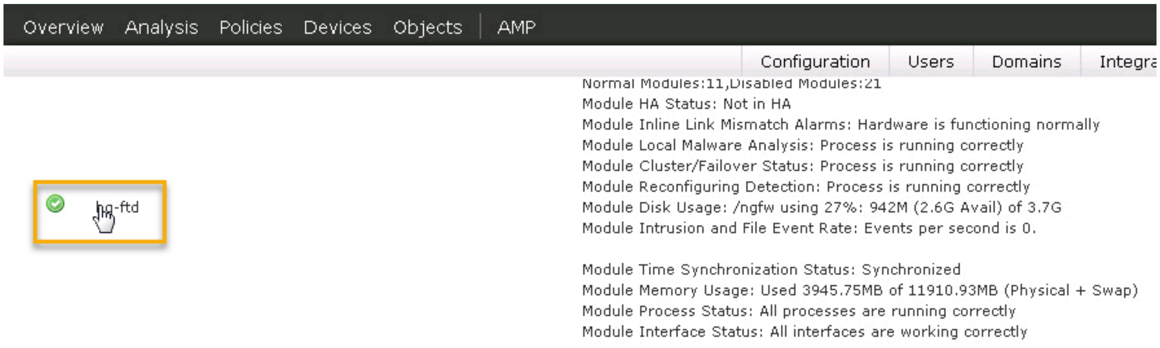
Figure 479. Click the sections of the pie chart



Status	Count
Error	0
Critical	0
Warning	0
Recovered	0
Normal	4
Disabled	0

29. Select one of the **FTD devices** to drill into it. (Though you can select the FMC device you won't see the Threat Defense CLI tab which is reference in a bit within this lab guide.)

Figure 480. Select an FTD device

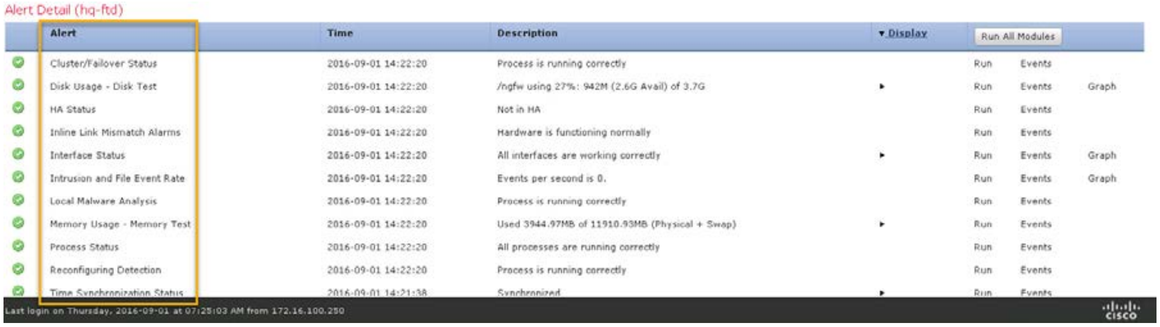


```
Normal Modules:11,Disabled Modules:21
Module HA Status: Not in HA
Module Inline Link Mismatch Alarms: Hardware is functioning normally
Module Local Malware Analysis: Process is running correctly
Module Cluster/Failover Status: Process is running correctly
Module Reconfiguring Detection: Process is running correctly
Module Disk Usage: /ngfw using 27%: 942M (2.6G Avail) of 3.7G
Module Intrusion and File Event Rate: Events per second is 0.

Module Time Synchronization Status: Synchronized
Module Memory Usage: Used 3945.75MB of 11910.93MB (Physical + Swap)
Module Process Status: All processes are running correctly
Module Interface Status: All interfaces are working correctly
```

30. Notice the **Alert Detail** section. This is a list of tests that are run regularly against this device. (At the time of writing the lab guide the Interface 'Management0/0 is not receiving any packets message has been popping up constantly! You will remedy that later in this scenario.)

If you haven't seen the error about the "Management0/0 not receiving any packets" don't worry about it. As I was developing this lab it was popping up constantly.

Figure 481. Alert Detail section



Alert Detail (hq-ftd)

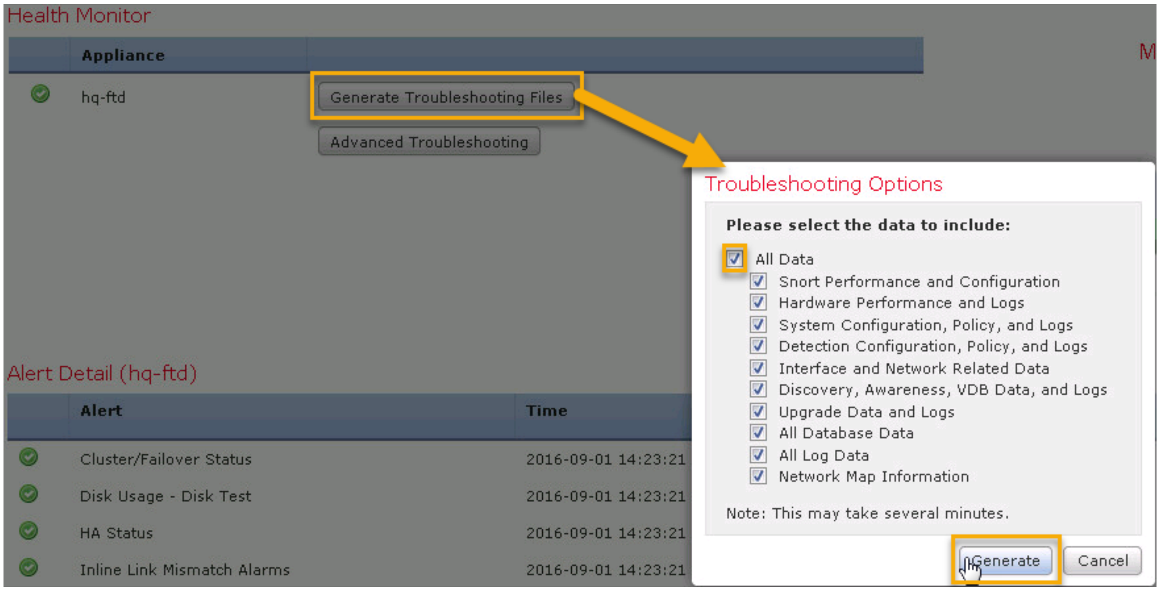
	Alert	Time	Description	▾ Display	Run All Modules		
✓	Cluster/Failover Status	2016-09-01 14:22:20	Process is running correctly		Run	Events	
✓	Disk Usage - Disk Test	2016-09-01 14:22:20	/ngfw using 27%: 942M (2.6G Avail) of 3.7G	▸	Run	Events	Graph
✓	HA Status	2016-09-01 14:22:20	Not in HA		Run	Events	
✓	Inline Link Mismatch Alarms	2016-09-01 14:22:20	Hardware is functioning normally		Run	Events	
✓	Interface Status	2016-09-01 14:22:20	All interfaces are working correctly	▸	Run	Events	Graph
✓	Intrusion and File Event Rate	2016-09-01 14:22:20	Events per second is 0.		Run	Events	Graph
✓	Local Malware Analysis	2016-09-01 14:22:20	Process is running correctly		Run	Events	
✓	Memory Usage - Memory Test	2016-09-01 14:22:20	Used 3944.97MB of 11910.93MB (Physical + Swap)	▸	Run	Events	
✓	Process Status	2016-09-01 14:22:20	All processes are running correctly		Run	Events	
✓	Reconfiguring Detection	2016-09-01 14:22:20	Process is running correctly		Run	Events	
✓	Time Synchronization Status	2016-09-01 14:21:38	Synchronized	▸	Run	Events	

Last login on Thursday, 2016-09-01 at 07:25:03 AM from 172.16.100.250

31. Click on the **Generate Troubleshooting Files** button.

32. In the subsequent popup window notice all the possible files you can generate. Click the **Generate** button. The file generation will take about 3 minutes to complete.

Figure 482. Generate Troubleshooting files



Health Monitor

	Appliance	
✓	hq-ftd	Generate Troubleshooting Files Advanced Troubleshooting

Troubleshooting Options

Please select the data to include:

- ☑ All Data
  - ☑ Snort Performance and Configuration
  - ☑ Hardware Performance and Logs
  - ☑ System Configuration, Policy, and Logs
  - ☑ Detection Configuration, Policy, and Logs
  - ☑ Interface and Network Related Data
  - ☑ Discovery, Awareness, VDB Data, and Logs
  - ☑ Upgrade Data and Logs
  - ☑ All Database Data
  - ☑ All Log Data
  - ☑ Network Map Information

Note: This may take several minutes.

Alert Detail (hq-ftd)

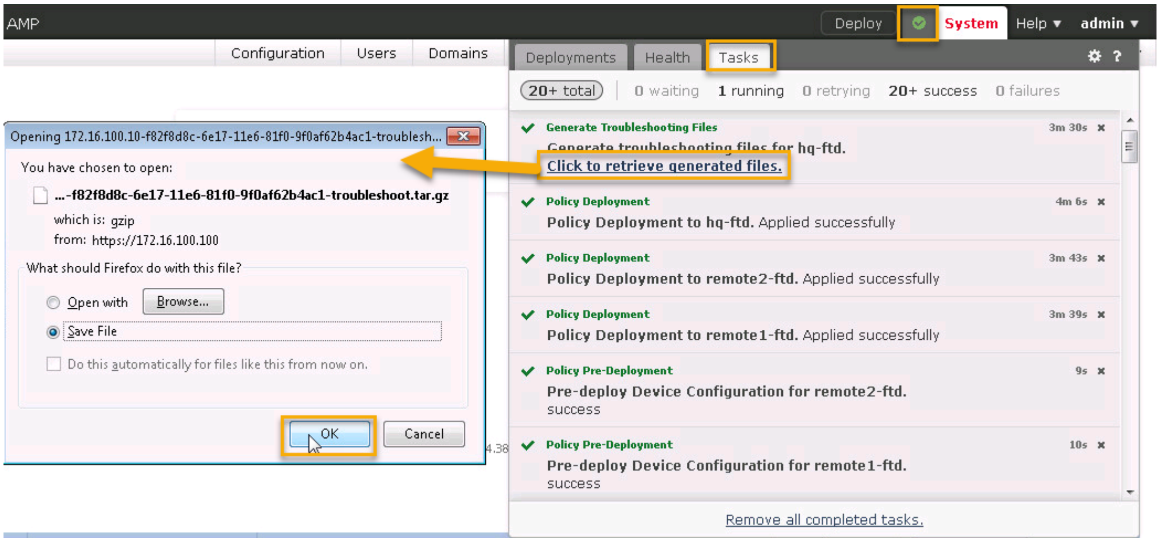
	Alert	Time
✓	Cluster/Failover Status	2016-09-01 14:23:21
✓	Disk Usage - Disk Test	2016-09-01 14:23:21
✓	HA Status	2016-09-01 14:23:21
✓	Inline Link Mismatch Alarms	2016-09-01 14:23:21

33. There will now be a Task Notification notice at the top of your browser window indicating that you can monitor the generation of these files by looking at the Tasks tab within the Message Center. Click the **Message Center Tasks Tab** link to open up this popup window.

34. Once the task to generate the troubleshooting files is complete click the **Click to retrieve generated files** link.

35. Click **OK** to save the file.

Figure 483. Save troubleshooting files



Opening 172.16.100.10-f82f8d8c-6e17-11e6-81f0-9f0af62b4ac1-troublesh...

You have chosen to open:

...-f82f8d8c-6e17-11e6-81f0-9f0af62b4ac1-troubleshoot.tar.gz

which is: gzip
from: https://172.16.100.100

What should Firefox do with this file?

○ Open with [Browse...]
● Save File
□ Do this automatically for files like this from now on.

[OK] [Cancel]

20+ total | 0 waiting | 1 running | 0 retrying | 20+ success | 0 failures

✓ **Generate Troubleshooting Files** 3m 30s ×
Generate troubleshooting files for hq-ftd.
Click to retrieve generated files.

✓ **Policy Deployment** 4m 6s ×
Policy Deployment to hq-ftd. Applied successfully

✓ **Policy Deployment** 3m 43s ×
Policy Deployment to remote2-ftd. Applied successfully

✓ **Policy Deployment** 3m 39s ×
Policy Deployment to remote1-ftd. Applied successfully

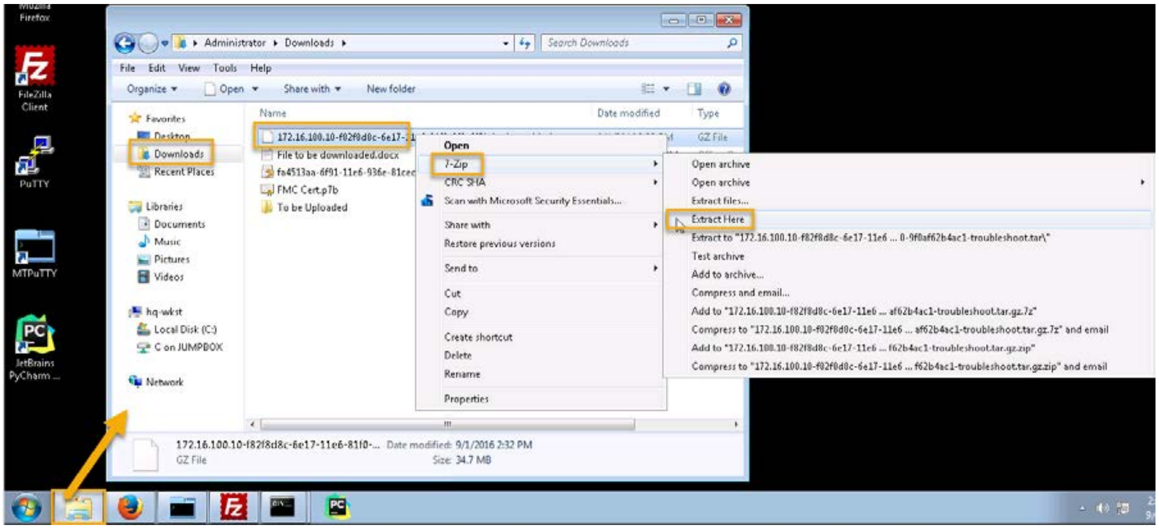
✓ **Policy Pre-Deployment** 9s ×
Pre-deploy Device Configuration for remote2-ftd.
success

✓ **Policy Pre-Deployment** 10s ×
Pre-deploy Device Configuration for remote1-ftd.
success

Remove all completed tasks.

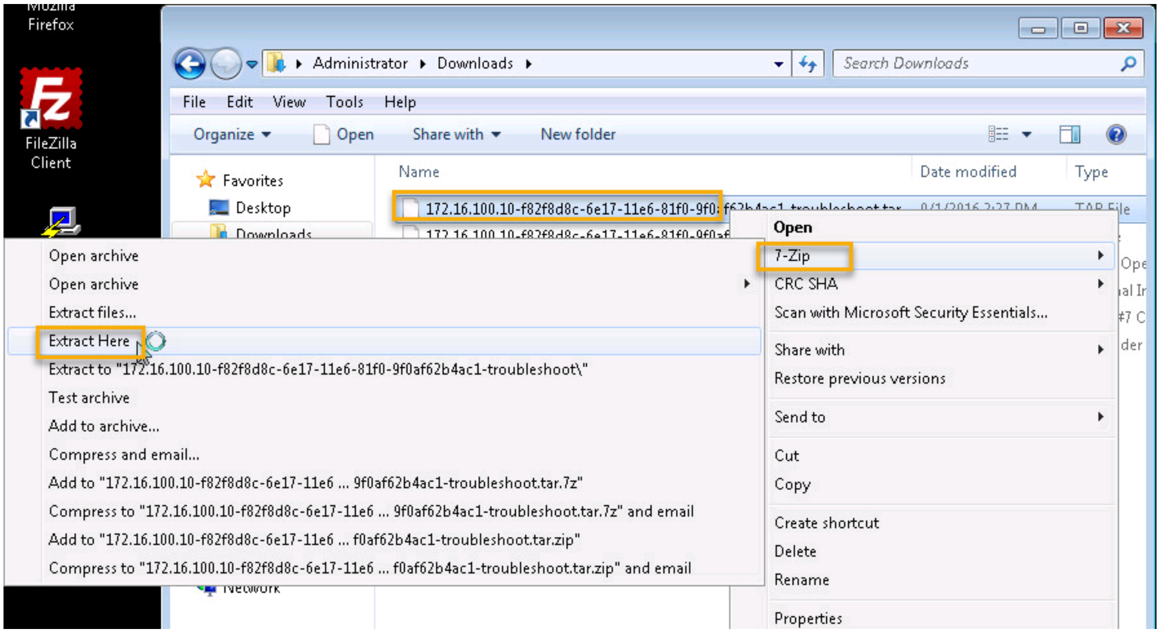
36. Open up **Windows Explorer**, navigate to the **Download** folder, **right-click** on the troubleshooting file, select **7zip > Extract Here**. This will uncompress the tar file.

Figure 484. Extract from gzip


Administrator ▸ Downloads ▸
Search Downloads
File Edit View Tools Help
Organize ▾ Open ▾ Share with ▾ New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
hq-wkst
Local Disk (C:)
C on JUMPBOX
Network
Name
Date modified
Type
172.16.100.10-f82f8d8c-6e17-
File to be downloaded.docx
fa4513aa-6f91-11e6-936e-81cec
FMC Cert.p7b
To be Uploaded
GZ File
Open
7-Zip
CRC SHA
Scan with Microsoft Security Essentials...
Share with
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Open archive
Open archive
Extract files...
Extract Here
Extract to "172.16.100.10-f82f8d8c-6e17-11e6 ... 0-9f0af62b4ac1-troubleshoot.tar\"
Test archive
Add to archive...
Compress and email...
Add to "172.16.100.10-f82f8d8c-6e17-11e6 ... af62b4ac1-troubleshoot.tar.gz.7z"
Compress to "172.16.100.10-f82f8d8c-6e17-11e6 ... af62b4ac1-troubleshoot.tar.gz.7z" and email
Add to "172.16.100.10-f82f8d8c-6e17-11e6 ... f62b4ac1-troubleshoot.tar.gz.zip"
Compress to "172.16.100.10-f82f8d8c-6e17-11e6 ... f62b4ac1-troubleshoot.tar.gz.zip" and email
172.16.100.10-f82f8d8c-6e17-11e6-81f0-... Date modified: 9/1/2016 2:32 PM
GZ File Size: 34.7 MB
FileZilla Client
PuTTY
MTPuTTY
JetBrains PyCharm ...

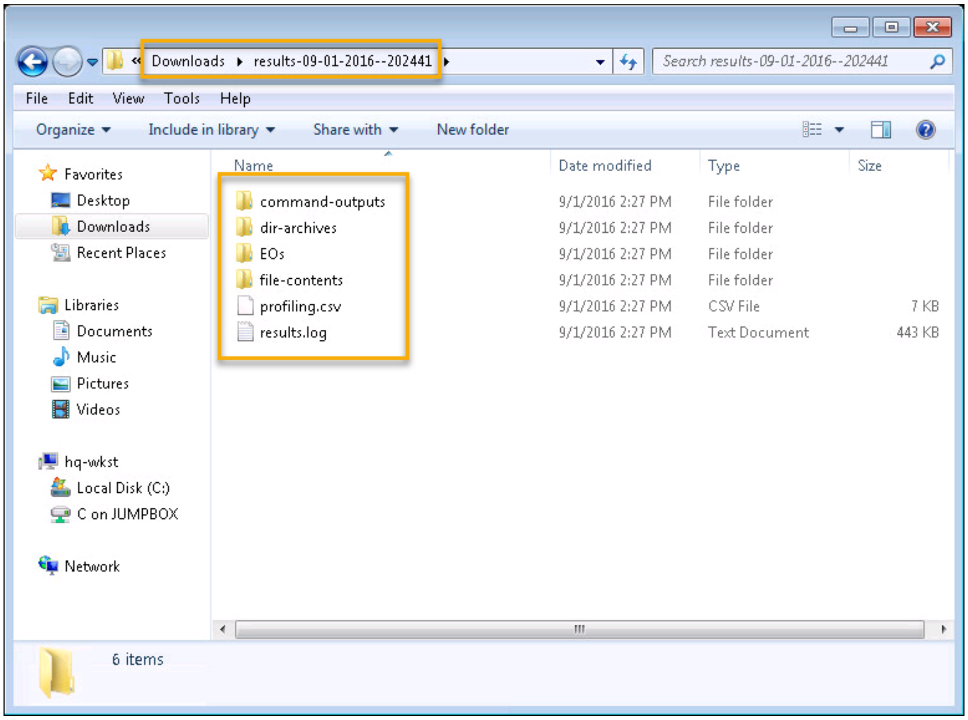
37. Perform the extraction process again on the new tar file. (**Right-click** the file, select **7zip > Extract Here**.)

Figure 485. Extract from tar


Firefox
FileZilla Client
Administrator ▸ Downloads ▸
Search Downloads
File Edit View Tools Help
Organize ▾ Open Share with ▾ New folder
Favorites
Desktop
Downloads
Name
Date modified
Type
172.16.100.10-f82f8d8c-6e17-11e6-81f0-9f0af62b4ac1-troubleshoot.tar
TAR File
Open archive
Open archive
Extract files...
Extract Here
Extract to "172.16.100.10-f82f8d8c-6e17-11e6-81f0-9f0af62b4ac1-troubleshoot\"
Test archive
Add to archive...
Compress and email...
Add to "172.16.100.10-f82f8d8c-6e17-11e6 ... 9f0af62b4ac1-troubleshoot.tar.7z"
Compress to "172.16.100.10-f82f8d8c-6e17-11e6 ... 9f0af62b4ac1-troubleshoot.tar.7z" and email
Add to "172.16.100.10-f82f8d8c-6e17-11e6 ... f0af62b4ac1-troubleshoot.tar.zip"
Compress to "172.16.100.10-f82f8d8c-6e17-11e6 ... f0af62b4ac1-troubleshoot.tar.zip" and email
Network
Open
7-Zip
CRC SHA
Scan with Microsoft Security Essentials...
Share with
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

38. Finally, you will have a folder containing all the troubleshooting files. Feel free to poke around in these folders and files.

Figure 486. Files, files, files!



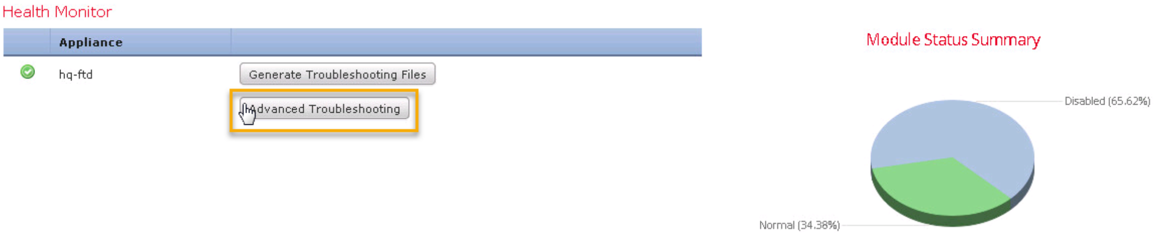
Downloads ▸ results-09-01-2016--202441

Name	Date modified	Type	Size
command-outputs	9/1/2016 2:27 PM	File folder	
dir-archives	9/1/2016 2:27 PM	File folder	
EOs	9/1/2016 2:27 PM	File folder	
file-contents	9/1/2016 2:27 PM	File folder	
profiling.csv	9/1/2016 2:27 PM	CSV File	7 KB
results.log	9/1/2016 2:27 PM	Text Document	443 KB

6 items

39. Return to the FMC Administration GUI and click the **Advanced Troubleshooting** button.

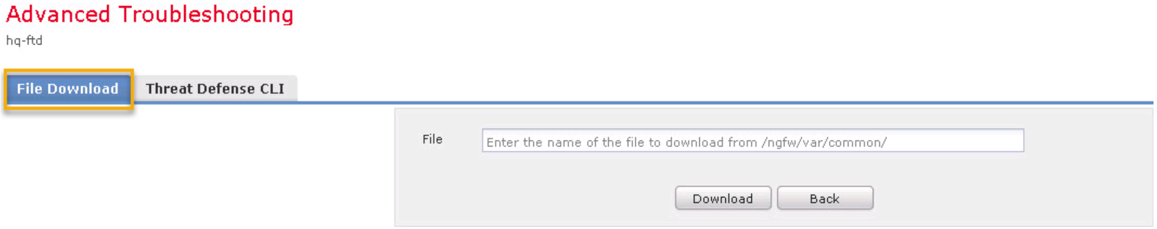
Figure 487. Advanced Troubleshooting



40. On the **File Download tab**:

   a. Here is where you can download files from this FTD device. More than likely this will be at the direction of a TAC engineer.

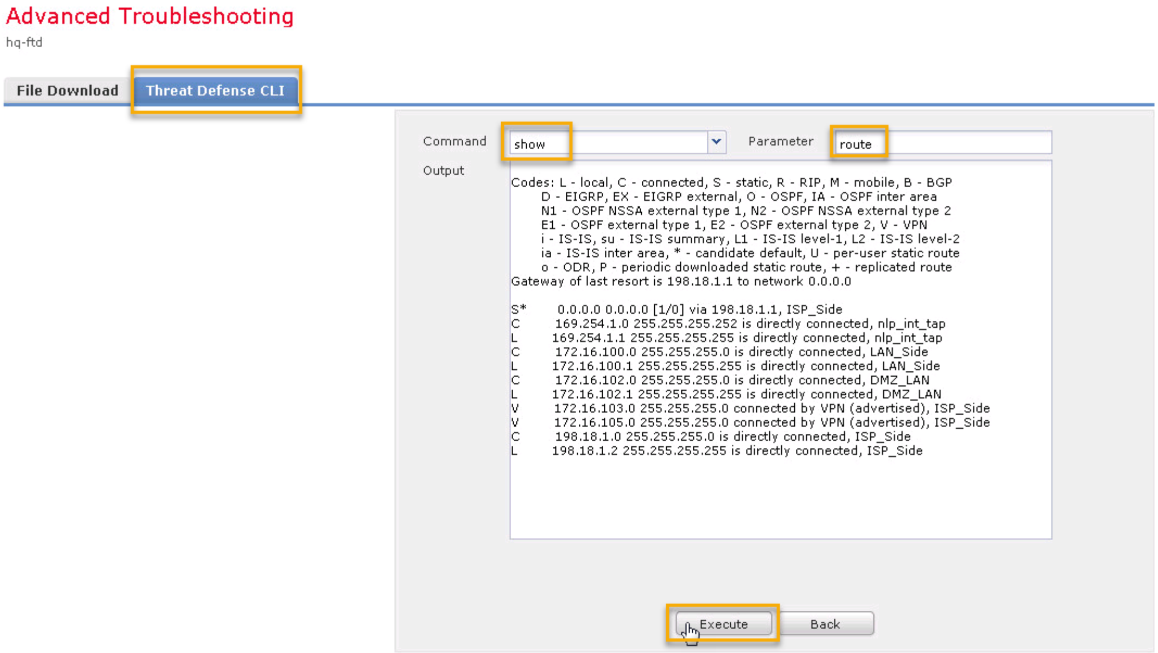
Figure 488. File Download tab



41. On the **Threat Defense CLI tab**:

    a. Here is where you can issue a limit selection of CLI commands against this device. Try it out. Issue the **show route** command.

Figure 489. Show route CLI



Command: show

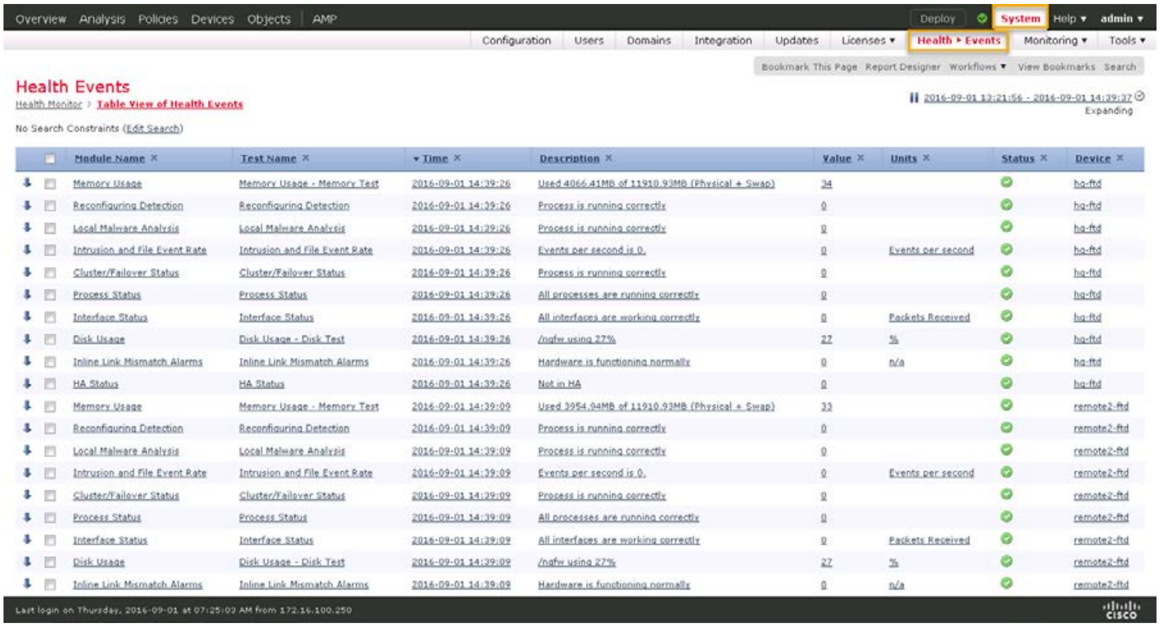
Parameter: route

Output

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 198.18.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 198.18.1.1, ISP_Side
C        169.254.1.0 255.255.255.252 is directly connected, nlp_int_tap
L        169.254.1.1 255.255.255.255 is directly connected, nlp_int_tap
C        172.16.100.0 255.255.255.0 is directly connected, LAN_Side
L        172.16.100.1 255.255.255.255 is directly connected, LAN_Side
C        172.16.102.0 255.255.255.0 is directly connected, DMZ_LAN
L        172.16.102.1 255.255.255.255 is directly connected, DMZ_LAN
V        172.16.103.0 255.255.255.0 connected by VPN (advertised), ISP_Side
V        172.16.105.0 255.255.255.0 connected by VPN (advertised), ISP_Side
C        198.18.1.0 255.255.255.0 is directly connected, ISP_Side
L        198.18.1.2 255.255.255.255 is directly connected, ISP_Side
```

42. **Skipping the Policy page for now**, navigate to **System > Health > Events**. This page is a tabular history of modules and tests that are running against each FMC managed device on a regular basis. You can use this to drill into specific problems you might be seeing to figure out how long that issue has been ongoing and whether it is an intermittent problem.

Figure 490. Health Events



Overview Analysis Policies Devices Objects AMP | Deploy System Help ▾ admin ▾

Configuration Users Domains Integration Updates Licenses ▾ Health ▸ Events Monitoring ▾ Tools ▾

Bookmark This Page Report Designer Workflows ▾ View Bookmarks Search

Health Events

Health Monitor > Table View of Health Events

No Search Constraints (Edit Search)

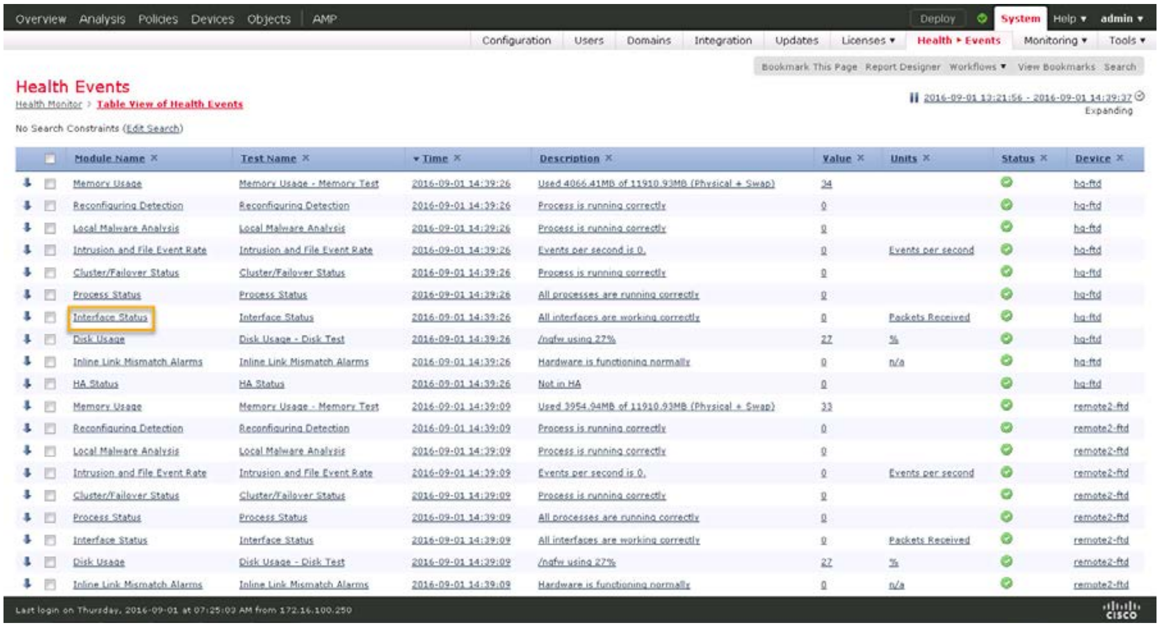
2016-09-01 13:21:56 - 2016-09-01 14:39:37
Expanding

	□	Module Name ✕	Test Name ✕	▾ Time ✕	Description ✕	Value ✕	Units ✕	Status ✕	Device ✕
⬇	□	Memory Usage	Memory Usage - Memory Test	2016-09-01 14:39:26	Used 4066.41MB of 11910.93MB (Physical + Swap)	34		✓	hq-ftd
⬇	□	Reconfiguring Detection	Reconfiguring Detection	2016-09-01 14:39:26	Process is running correctly	0		✓	hq-ftd
⬇	□	Local Malware Analysis	Local Malware Analysis	2016-09-01 14:39:26	Process is running correctly	0		✓	hq-ftd
⬇	□	Intrusion and File Event Rate	Intrusion and File Event Rate	2016-09-01 14:39:26	Events per second is 0.	0	Events per second	✓	hq-ftd
⬇	□	Cluster/Failover Status	Cluster/Failover Status	2016-09-01 14:39:26	Process is running correctly	0		✓	hq-ftd
⬇	□	Process Status	Process Status	2016-09-01 14:39:26	All processes are running correctly	0		✓	hq-ftd
⬇	□	Interface Status	Interface Status	2016-09-01 14:39:26	All interfaces are working correctly	0	Packets Received	✓	hq-ftd
⬇	□	Disk Usage	Disk Usage - Disk Test	2016-09-01 14:39:26	/ngfw using 27%	27	%	✓	hq-ftd
⬇	□	Inline Link Mismatch Alarms	Inline Link Mismatch Alarms	2016-09-01 14:39:26	Hardware is functioning normally	0	n/a	✓	hq-ftd
⬇	□	HA Status	HA Status	2016-09-01 14:39:26	Not in HA	0		✓	hq-ftd
⬇	□	Memory Usage	Memory Usage - Memory Test	2016-09-01 14:39:09	Used 3954.94MB of 11910.93MB (Physical + Swap)	33		✓	remote2-ftd
⬇	□	Reconfiguring Detection	Reconfiguring Detection	2016-09-01 14:39:09	Process is running correctly	0		✓	remote2-ftd
⬇	□	Local Malware Analysis	Local Malware Analysis	2016-09-01 14:39:09	Process is running correctly	0		✓	remote2-ftd
⬇	□	Intrusion and File Event Rate	Intrusion and File Event Rate	2016-09-01 14:39:09	Events per second is 0.	0	Events per second	✓	remote2-ftd
⬇	□	Cluster/Failover Status	Cluster/Failover Status	2016-09-01 14:39:09	Process is running correctly	0		✓	remote2-ftd
⬇	□	Process Status	Process Status	2016-09-01 14:39:09	All processes are running correctly	0		✓	remote2-ftd
⬇	□	Interface Status	Interface Status	2016-09-01 14:39:09	All interfaces are working correctly	0	Packets Received	✓	remote2-ftd
⬇	□	Disk Usage	Disk Usage - Disk Test	2016-09-01 14:39:09	/ngfw using 27%	27	%	✓	remote2-ftd
⬇	□	Inline Link Mismatch Alarms	Inline Link Mismatch Alarms	2016-09-01 14:39:09	Hardware is functioning normally	0	n/a	✓	remote2-ftd

Last login on Thursday, 2016-09-01 at 07:25:03 AM from 172.16.100.250

43. Click on the **Interface Status** link in the Module Name column.

Figure 491. Interface Status



Overview Analysis Policies Devices Objects AMP | Deploy System Help ▾ admin ▾

Configuration Users Domains Integration Updates Licenses ▾ Health ▸ Events Monitoring ▾ Tools ▾

Bookmark This Page Report Designer Workflows ▾ View Bookmarks Search

Health Events

Health Monitor > Table View of Health Events

No Search Constraints (Edit Search)

2016-09-01 13:21:56 - 2016-09-01 14:39:37
Expanding

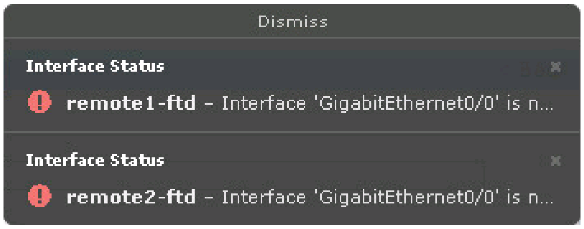
	□	Module Name ✕	Test Name ✕	▾ Time ✕	Description ✕	Value ✕	Units ✕	Status ✕	Device ✕
⬇	□	Memory Usage	Memory Usage - Memory Test	2016-09-01 14:39:26	Used 4066.41MB of 11910.93MB (Physical + Swap)	34		✓	hq-ftd
⬇	□	Reconfiguring Detection	Reconfiguring Detection	2016-09-01 14:39:26	Process is running correctly	0		✓	hq-ftd
⬇	□	Local Malware Analysis	Local Malware Analysis	2016-09-01 14:39:26	Process is running correctly	0		✓	hq-ftd
⬇	□	Intrusion and File Event Rate	Intrusion and File Event Rate	2016-09-01 14:39:26	Events per second is 0.	0	Events per second	✓	hq-ftd
⬇	□	Cluster/Failover Status	Cluster/Failover Status	2016-09-01 14:39:26	Process is running correctly	0		✓	hq-ftd
⬇	□	Process Status	Process Status	2016-09-01 14:39:26	All processes are running correctly	0		✓	hq-ftd
⬇	□	Interface Status	Interface Status	2016-09-01 14:39:26	All interfaces are working correctly	0	Packets Received	✓	hq-ftd
⬇	□	Disk Usage	Disk Usage - Disk Test	2016-09-01 14:39:26	/ngfw using 27%	27	%	✓	hq-ftd
⬇	□	Inline Link Mismatch Alarms	Inline Link Mismatch Alarms	2016-09-01 14:39:26	Hardware is functioning normally	0	n/a	✓	hq-ftd
⬇	□	HA Status	HA Status	2016-09-01 14:39:26	Not in HA	0		✓	hq-ftd
⬇	□	Memory Usage	Memory Usage - Memory Test	2016-09-01 14:39:09	Used 3954.94MB of 11910.93MB (Physical + Swap)	33		✓	remote2-ftd
⬇	□	Reconfiguring Detection	Reconfiguring Detection	2016-09-01 14:39:09	Process is running correctly	0		✓	remote2-ftd
⬇	□	Local Malware Analysis	Local Malware Analysis	2016-09-01 14:39:09	Process is running correctly	0		✓	remote2-ftd
⬇	□	Intrusion and File Event Rate	Intrusion and File Event Rate	2016-09-01 14:39:09	Events per second is 0.	0	Events per second	✓	remote2-ftd
⬇	□	Cluster/Failover Status	Cluster/Failover Status	2016-09-01 14:39:09	Process is running correctly	0		✓	remote2-ftd
⬇	□	Process Status	Process Status	2016-09-01 14:39:09	All processes are running correctly	0		✓	remote2-ftd
⬇	□	Interface Status	Interface Status	2016-09-01 14:39:09	All interfaces are working correctly	0	Packets Received	✓	remote2-ftd
⬇	□	Disk Usage	Disk Usage - Disk Test	2016-09-01 14:39:09	/ngfw using 27%	27	%	✓	remote2-ftd
⬇	□	Inline Link Mismatch Alarms	Inline Link Mismatch Alarms	2016-09-01 14:39:09	Hardware is functioning normally	0	n/a	✓	remote2-ftd

Last login on Thursday, 2016-09-01 at 07:25:03 AM from 172.16.100.250

44. Now you have drilled into the history of this test. I'm guessing that the delays in the virtualized environment is why this particular test fails intermittently.

45. Throughout the lab, have you been getting several popup indicators telling you that your FTD management interfaces are not receiving any packets?

Figure 492. Annoying Error Message



Interface Status

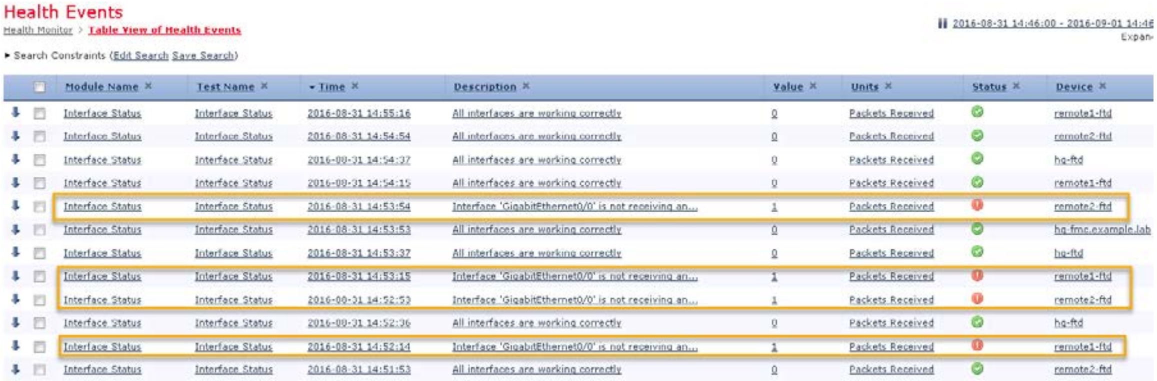
! **remote1-ftd** – Interface 'GigabitEthernet0/0' is n...

Interface Status

! **remote2-ftd** – Interface 'GigabitEthernet0/0' is n...

46. It might take some looking throughout the history of this particular test but you should find some failures.

Figure 493. Interface Status test failures



Health Events

Health Monitor > Table View of Health Events

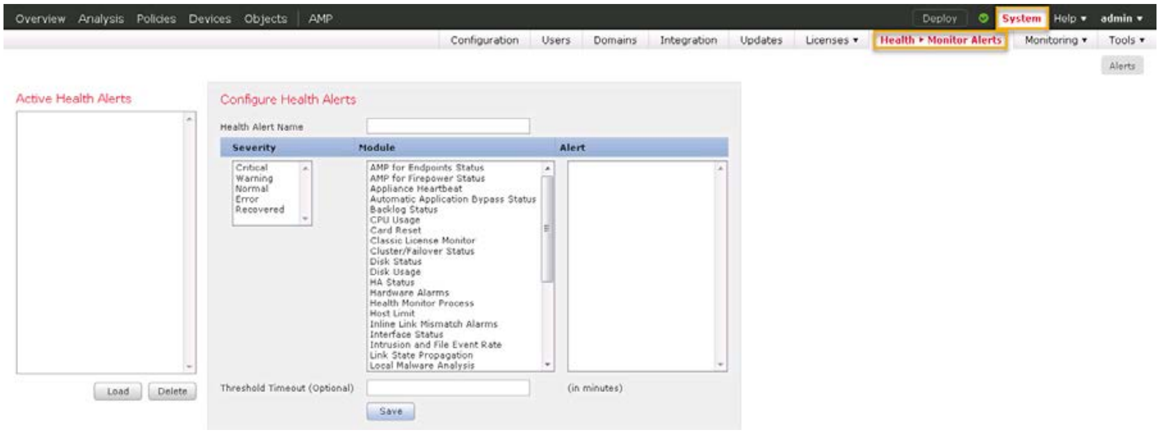
▸ Search Constraints (Edit Search Save Search)

2016-08-31 14:46:00 - 2016-09-01 14:46
Expan

	☐	Module Name	Test Name	Time	Description	Value	Units	Status	Device
⬇	☐	Interface Status	Interface Status	2016-08-31 14:55:16	All interfaces are working correctly	0	Packets Received	✓	remote1-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:54:54	All interfaces are working correctly	0	Packets Received	✓	remote2-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:54:37	All interfaces are working correctly	0	Packets Received	✓	hq-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:54:15	All interfaces are working correctly	0	Packets Received	✓	remote1-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:53:54	Interface 'GigabitEthernet0/0' is not receiving an...	1	Packets Received	!	remote2-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:53:53	All interfaces are working correctly	0	Packets Received	✓	hq-fmc.example.lab
⬇	☐	Interface Status	Interface Status	2016-08-31 14:53:37	All interfaces are working correctly	0	Packets Received	✓	hq-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:53:15	Interface 'GigabitEthernet0/0' is not receiving an...	1	Packets Received	!	remote1-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:52:53	Interface 'GigabitEthernet0/0' is not receiving an...	1	Packets Received	!	remote2-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:52:36	All interfaces are working correctly	0	Packets Received	✓	hq-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:52:14	Interface 'GigabitEthernet0/0' is not receiving an...	1	Packets Received	!	remote1-ftd
⬇	☐	Interface Status	Interface Status	2016-08-31 14:51:53	All interfaces are working correctly	0	Packets Received	✓	remote2-ftd

47. Before you "fix" these erroneous errors navigate to **System > Health > Monitor Alerts** page. Here you can create custom Health Alerts if one of the default tests doesn't cover what you want.

Figure 494. Monitors Alerts page



Active Health Alerts

Configure Health Alerts

Health Alert Name

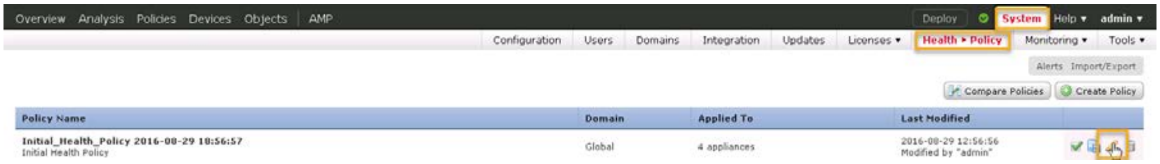
Severity	Module	Alert
Critical Warning Normal Error Recovered	AMP for Endpoints Status AMP for Firepower Status Appliance Heartbeat Automatic Application Bypass Status Backlog Status CPU Usage Card Reset Classic License Monitor Cluster/Failover Status Disk Status Disk Usage HA Status Hardware Alarms Health Monitor Process Host Limit Inline Link Mismatch Alarms Interface Status Intrusion and File Event Rate Link State Propagation Local Malware Analysis	

Threshold Timeout (Optional) (in minutes)

48. Finally let’s go to **System > Health > Policy**. This is the heart of the whole System Health configuration.

49. **Edit** the **Initial Health Policy**. From here you can adjust the timers, whether a test is run or not, or possibly event threshold values (if applicable).

Figure 495. Edit Health Policy

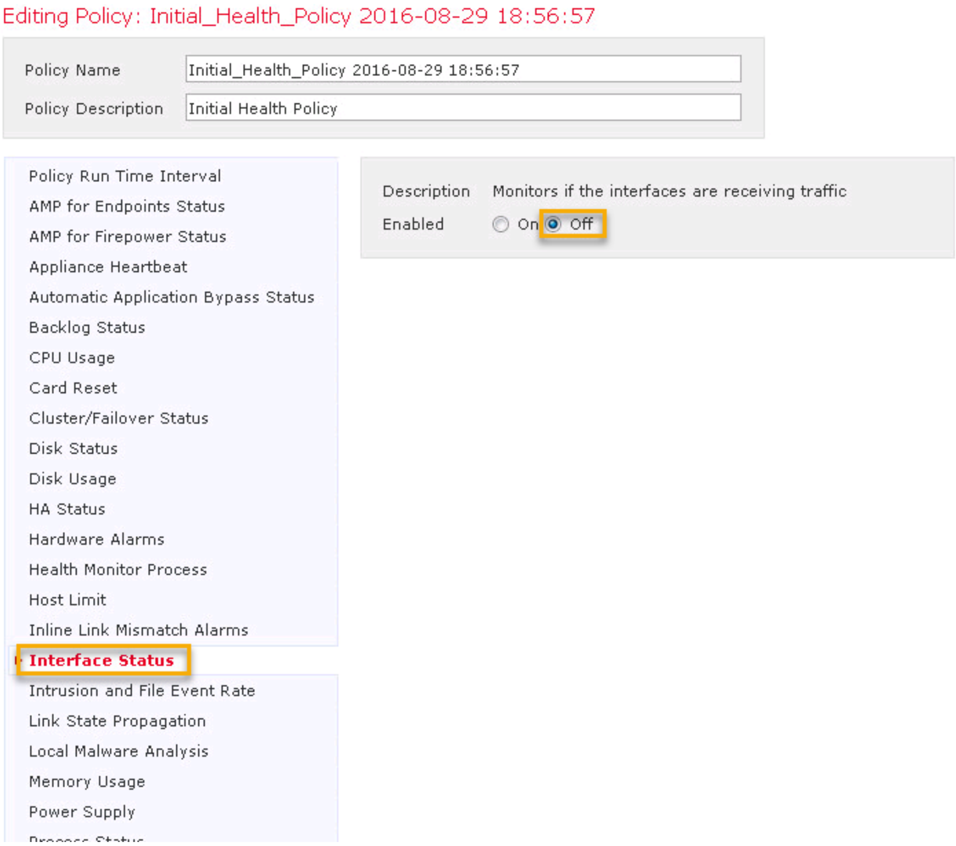


Policy Name	Domain	Applied To	Last Modified
Initial_Health_Policy 2016-08-29 18:56:57 Initial Health Policy	Global	4 appliances	2016-08-29 12:56:56 Modified by "admin"

50. Click the **Interface Status** link.

    a. Click the **Off** radio button.

Figure 496. Turn off Interface Status testing


Editing Policy: Initial_Health_Policy 2016-08-29 18:56:57

Policy Name: Initial_Health_Policy 2016-08-29 18:56:57

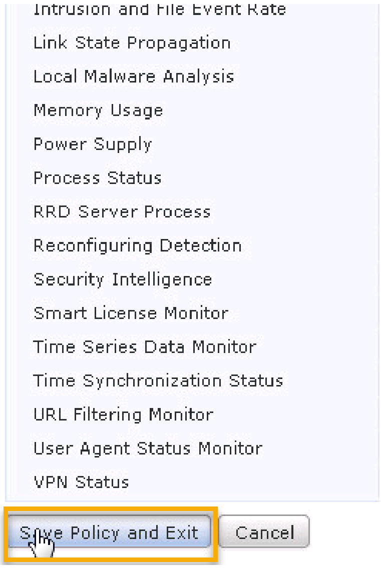
Policy Description: Initial Health Policy

Description: Monitors if the interfaces are receiving traffic

Enabled: ○ On ● Off

51. Scroll down and click **Save Policy and Exit**.

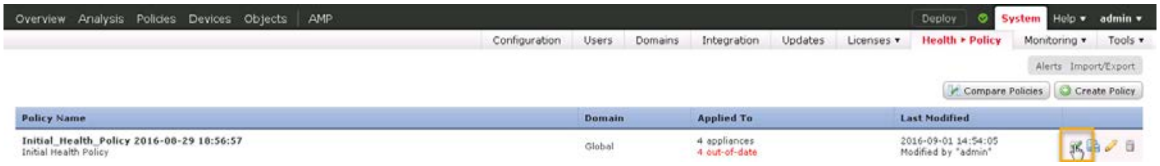
Figure 497. Save and Exit



Intrusion and File Event Rate
Link State Propagation
Local Malware Analysis
Memory Usage
Power Supply
Process Status
RRD Server Process
Reconfiguring Detection
Security Intelligence
Smart License Monitor
Time Series Data Monitor
Time Synchronization Status
URL Filtering Monitor
User Agent Status Monitor
VPN Status

52. Click the **green checkmark** (the apply button) on the **Initial Health Policy** policy row.

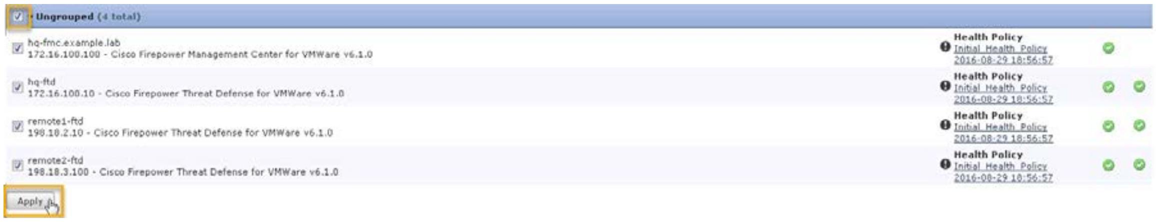
Figure 498. Click green checkmark



Policy Name	Domain	Applied To	Last Modified
Initial_Health_Policy 2016-08-29 18:56:57 Initial Health Policy	Global	4 appliances 4 out-of-date	2016-09-01 14:54:05 Modified by "admin"

53. Check the boxes next to **all the devices** and click **Apply**. (No more erroneous nagging messages about interfaces not receiving packets. YAY!)

Figure 499. Free of the tyranny of Interface Status warnings



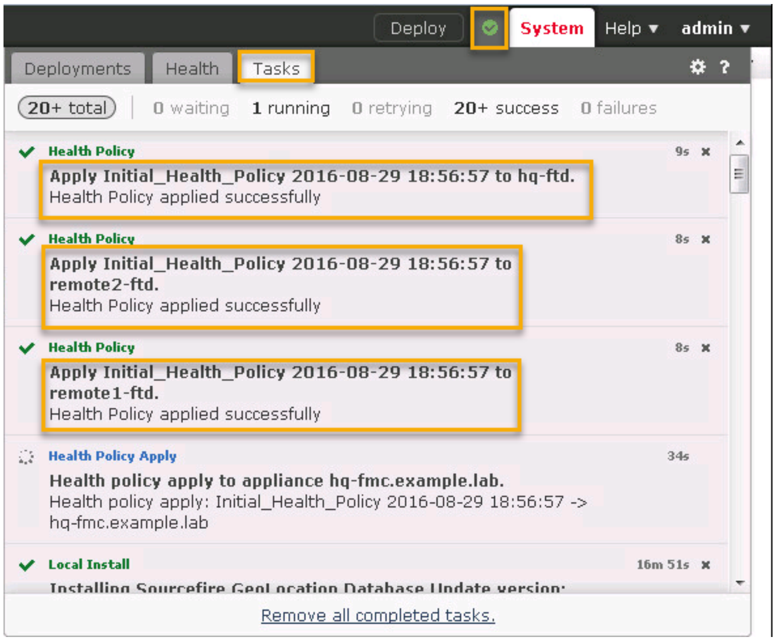
☑ **Ungrouped** (4 total)

☑	hq-fmc.example.lab 172.16.100.100 - Cisco Firepower Management Center for VMWare v6.1.0	**Health Policy** Initial_Health_Policy 2016-08-29 18:56:57
☑	hq-ftd 172.16.100.10 - Cisco Firepower Threat Defense for VMWare v6.1.0	**Health Policy** Initial_Health_Policy 2016-08-29 18:56:57
☑	remote1-ftd 198.18.2.10 - Cisco Firepower Threat Defense for VMWare v6.1.0	**Health Policy** Initial_Health_Policy 2016-08-29 18:56:57
☑	remote2-ftd 198.18.3.100 - Cisco Firepower Threat Defense for VMWare v6.1.0	**Health Policy** Initial_Health_Policy 2016-08-29 18:56:57

Blindly disabling tests is probably not the best idea. In this lab environment at least this particular test was constantly reporting and was always inaccurate. Whether that is a timer issue, a virtualization issue, or related to something you've done in this lab is unknown.

54. Once the deployment is complete the Message Center's Health tab should no longer show warnings/errors regarding interfaces not receiving packets.

Figure 500. Health Policy Updated on all Devices



Health Policy 9s
Apply Initial_Health_Policy 2016-08-29 18:56:57 to hq-ftd.
Health Policy applied successfully

Health Policy 8s
Apply Initial_Health_Policy 2016-08-29 18:56:57 to remote2-ftd.
Health Policy applied successfully

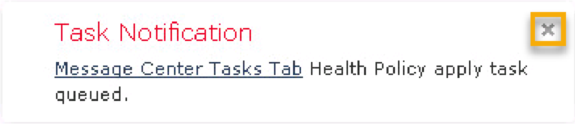
Health Policy 8s
Apply Initial_Health_Policy 2016-08-29 18:56:57 to remote1-ftd.
Health Policy applied successfully

Health Policy Apply 34s
Health policy apply to appliance hq-fmc.example.lab.
Health policy apply: Initial_Health_Policy 2016-08-29 18:56:57 -> hq-fmc.example.lab

Local Install 16m 51s
Installing Sourcefire GeoLocation Database Update version:

55. You will probably have a few Task Notification messages by now, from the database updates you did earlier. Click the **x** to close each of them out as they take up a lot of space. Feel free to close each of these messages as they appear.

Figure 501. Task Notification



Task Notification
Message Center Tasks Tab Health Policy apply task queued.

Scenario Summary

This scenario might seem boring since it was mostly about looking at lists of events, or health reports. That said, without a health and up-to-date system you cannot say with confidence that your Security Posture is worth all the money that was spent to acquire and configure it.

In this scenario you reviewed all the policies, regular tests that are run against the FMC and FTD devices. You also learned how to patch and update the FMC databases.

Scenario 13. FMC and FTD Data Monitoring

Scenario Description

Like the previous scenario this one is mostly geared toward learning about how to see the logging and reports that are available on the FMC. However, these logs are regarding data flowing through the FTD devices and not about maintenance or managing the FTD devices themselves.

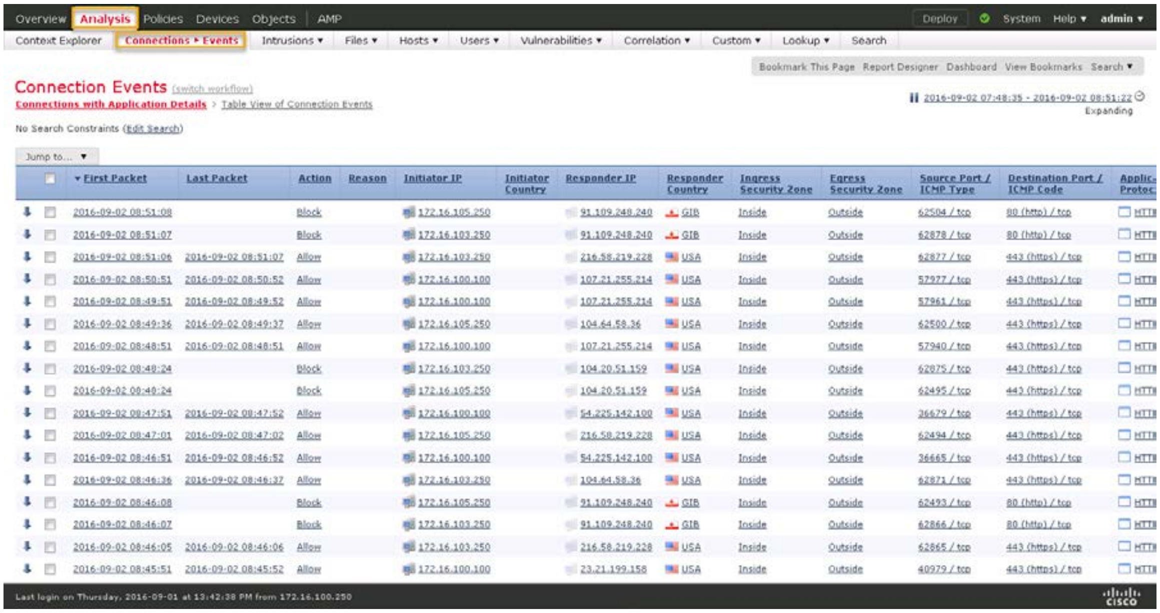
In this scenario you will explore the Connection Events, File Events, and the Host's Network Map features.

The Connection Events Viewer

The Connection Events viewer is where you find the details regarding Access Control Policy (and associated policies) Logging events. Though we've occasionally visited this location let's take a closer look.

1. Navigate to **Analysis > Connections > Events**. This is a tabular list of events that have occurred. The topmost being the most recent. Each row of these are really wide. You'll have to scroll to the right a LOT to see all the possible columns.

Figure 502. Connection Events



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

2016-09-02 07:48:35 - 2016-09-02 08:51:22
Expanding

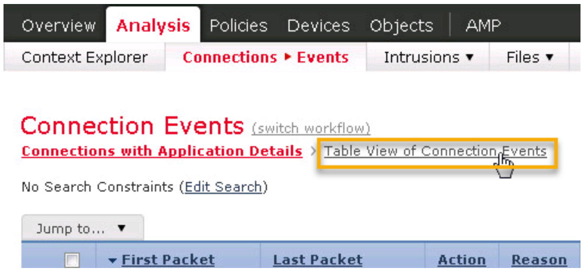
No Search Constraints (Edit Search)

	□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Applic-Protoc
⬇	□	2016-09-02 08:51:08		Block		172.16.105.250		91.109.248.240	GIB	Inside	Outside	62504 / tcp	80 (http) / tcp	HTT
⬇	□	2016-09-02 08:51:07		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62878 / tcp	80 (http) / tcp	HTT
⬇	□	2016-09-02 08:51:06	2016-09-02 08:51:07	Allow		172.16.103.250		216.58.219.228	USA	Inside	Outside	62877 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:50:51	2016-09-02 08:50:52	Allow		172.16.100.100		107.21.255.214	USA	Inside	Outside	57977 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:49:51	2016-09-02 08:49:52	Allow		172.16.100.100		107.21.255.214	USA	Inside	Outside	57961 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:49:36	2016-09-02 08:49:37	Allow		172.16.105.250		104.64.58.36	USA	Inside	Outside	62500 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:48:51	2016-09-02 08:48:51	Allow		172.16.100.100		107.21.255.214	USA	Inside	Outside	57940 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:48:24		Block		172.16.103.250		104.20.51.159	USA	Inside	Outside	62875 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:48:24		Block		172.16.105.250		104.20.51.159	USA	Inside	Outside	62495 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:47:51	2016-09-02 08:47:52	Allow		172.16.100.100		54.225.142.100	USA	Inside	Outside	36679 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:47:01	2016-09-02 08:47:02	Allow		172.16.105.250		216.58.219.228	USA	Inside	Outside	62494 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:46:51	2016-09-02 08:46:52	Allow		172.16.100.100		54.225.142.100	USA	Inside	Outside	36665 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:46:36	2016-09-02 08:46:37	Allow		172.16.103.250		104.64.58.36	USA	Inside	Outside	62871 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:46:08		Block		172.16.105.250		91.109.248.240	GIB	Inside	Outside	62493 / tcp	80 (http) / tcp	HTT
⬇	□	2016-09-02 08:46:07		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62866 / tcp	80 (http) / tcp	HTT
⬇	□	2016-09-02 08:46:05	2016-09-02 08:46:06	Allow		172.16.103.250		216.58.219.228	USA	Inside	Outside	62865 / tcp	443 (https) / tcp	HTT
⬇	□	2016-09-02 08:45:51	2016-09-02 08:45:52	Allow		172.16.100.100		23.21.199.158	USA	Inside	Outside	40979 / tcp	443 (https) / tcp	HTT

Last login on Thursday, 2016-09-01 at 13:42:38 PM from 172.16.100.250

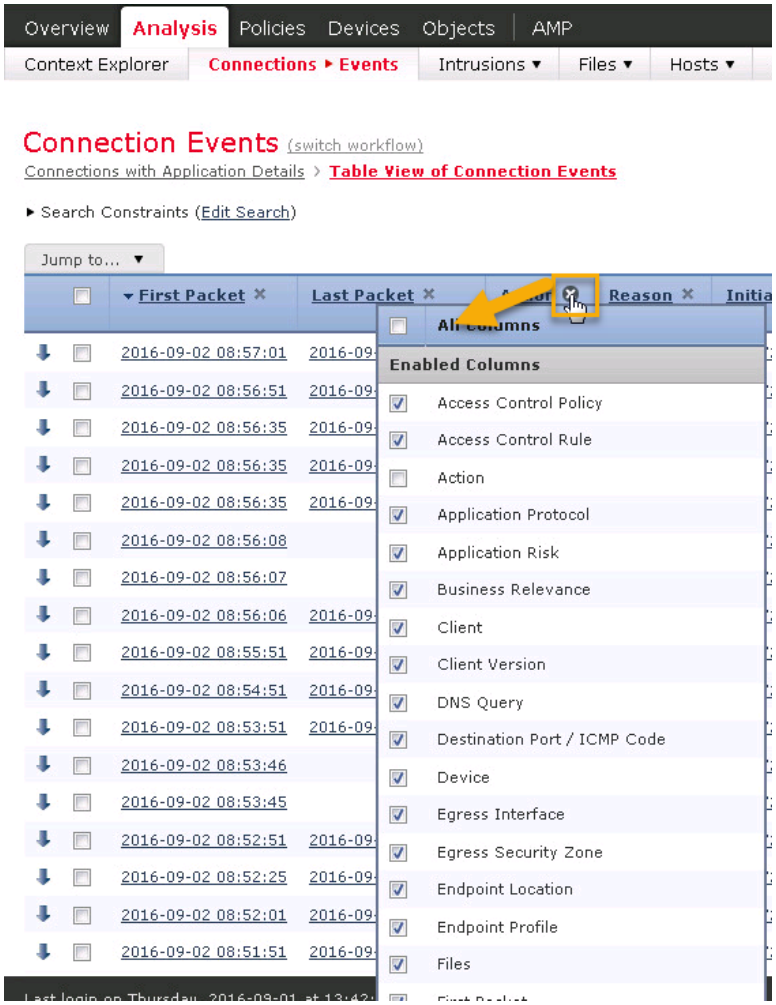
2. This page is just the “summary” page though. To get additional detail about each entry click the **Table View of Connection Events** link.

Figure 503. Click link



3. To change the number of columns being listed (either adding new ones or removing unused ones) click the **x** next to one of the column names. This will open up a list of all the possible columns and whether they are visible or not. This list is really long so scroll down to see all the options.

Figure 504. Selecting Columns



Connection Events (switch workflow)

Connections with Application Details › Table View of Connection Events

▸ Search Constraints (Edit Search)

Jump to... ▾

□	▾ First Packet ✕	Last Packet ✕	Reason ✕	Initia
□	2016-09-02 08:57:01	2016-09-		
□	2016-09-02 08:56:51	2016-09-		
□	2016-09-02 08:56:35	2016-09-		
□	2016-09-02 08:56:35	2016-09-		
□	2016-09-02 08:56:35	2016-09-		
□	2016-09-02 08:56:08			
□	2016-09-02 08:56:07			
□	2016-09-02 08:56:06	2016-09-		
□	2016-09-02 08:55:51	2016-09-		
□	2016-09-02 08:54:51	2016-09-		
□	2016-09-02 08:53:51	2016-09-		
□	2016-09-02 08:53:46			
□	2016-09-02 08:53:45			
□	2016-09-02 08:52:51	2016-09-		
□	2016-09-02 08:52:25	2016-09-		
□	2016-09-02 08:52:01	2016-09-		
□	2016-09-02 08:51:51	2016-09-		

□ All Columns

Enabled Columns

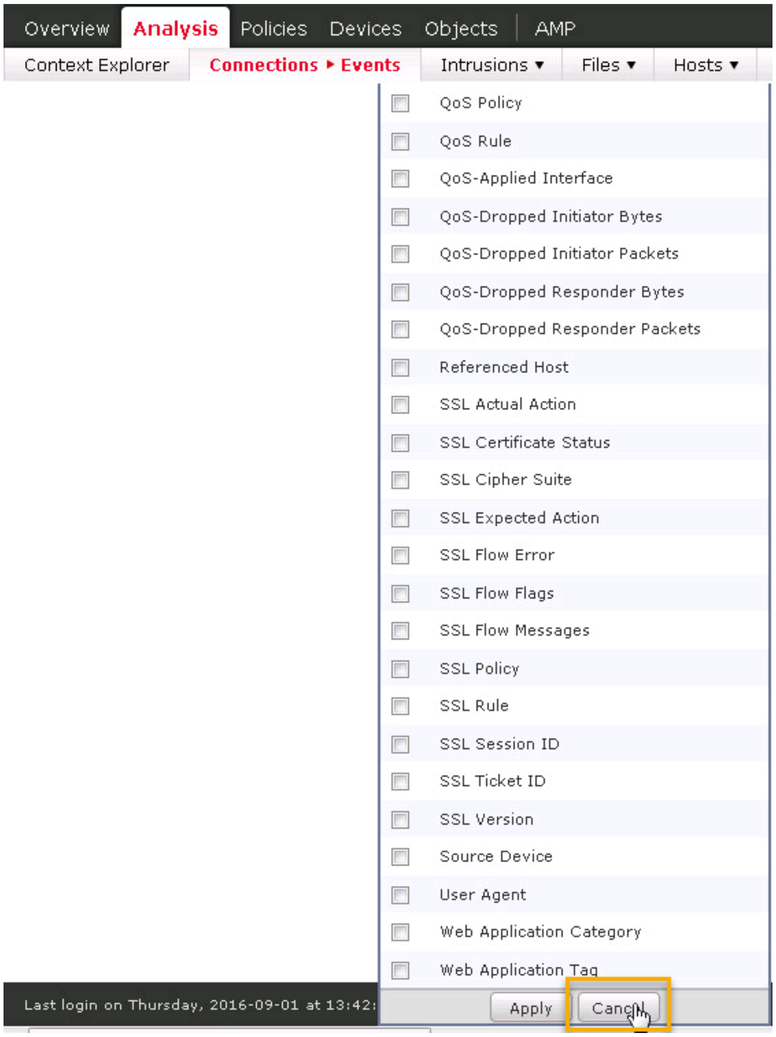
☑ Access Control Policy
☑ Access Control Rule
□ Action
☑ Application Protocol
☑ Application Risk
☑ Business Relevance
☑ Client
☑ Client Version
☑ DNS Query
☑ Destination Port / ICMP Code
☑ Device
☑ Egress Interface
☑ Egress Security Zone
☑ Endpoint Location
☑ Endpoint Profile
☑ Files
☑ First Packet

Last login on Thursday, 2016-09-01 at 13:42:

The column of which you clicked the x will now be de-selected. Be sure to re-select it if you want it to be viewed.

4. Once you have selected the desired list of viewable columns scroll to the bottom of the list and click **Apply**. If you don't wish to make any changes, select **Cancel**.

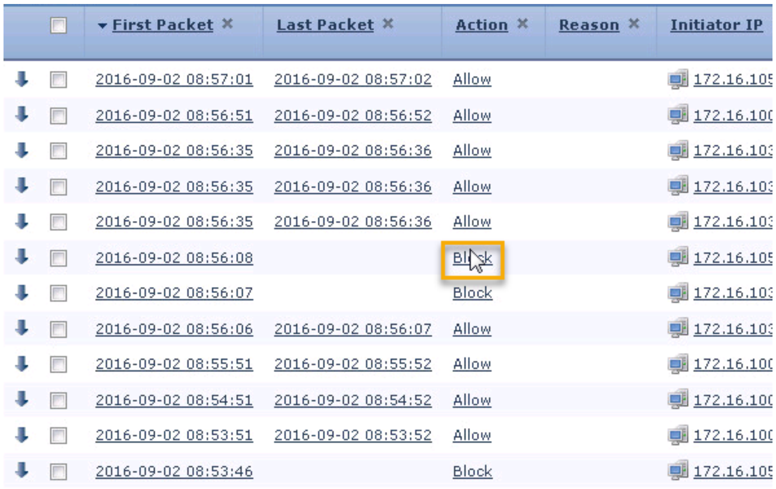
Figure 505. Click Cancel



☐ QoS Policy
☐ QoS Rule
☐ QoS-Applied Interface
☐ QoS-Dropped Initiator Bytes
☐ QoS-Dropped Initiator Packets
☐ QoS-Dropped Responder Bytes
☐ QoS-Dropped Responder Packets
☐ Referenced Host
☐ SSL Actual Action
☐ SSL Certificate Status
☐ SSL Cipher Suite
☐ SSL Expected Action
☐ SSL Flow Error
☐ SSL Flow Flags
☐ SSL Flow Messages
☐ SSL Policy
☐ SSL Rule
☐ SSL Session ID
☐ SSL Ticket ID
☐ SSL Version
☐ Source Device
☐ User Agent
☐ Web Application Category
☐ Web Application Tag

5. Clicking on any link from this list of events (such as the **Block link in the Action column**) you will be filtering this list to only events that have this particular feature.

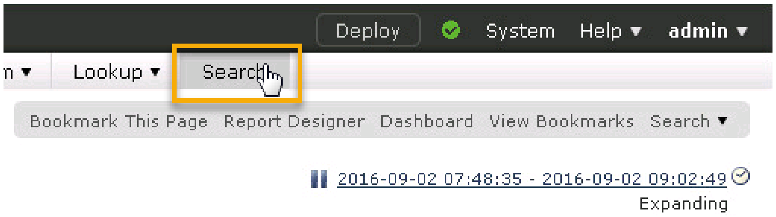
Figure 506. Filter by Block Action



	☐	▾ First Packet ✕	Last Packet ✕	Action ✕	Reason ✕	Initiator IP
⬇	☐	2016-09-02 08:57:01	2016-09-02 08:57:02	Allow		172.16.105
⬇	☐	2016-09-02 08:56:51	2016-09-02 08:56:52	Allow		172.16.100
⬇	☐	2016-09-02 08:56:35	2016-09-02 08:56:36	Allow		172.16.103
⬇	☐	2016-09-02 08:56:35	2016-09-02 08:56:36	Allow		172.16.103
⬇	☐	2016-09-02 08:56:35	2016-09-02 08:56:36	Allow		172.16.103
⬇	☐	2016-09-02 08:56:08		Block		172.16.105
⬇	☐	2016-09-02 08:56:07		Block		172.16.103
⬇	☐	2016-09-02 08:56:06	2016-09-02 08:56:07	Allow		172.16.103
⬇	☐	2016-09-02 08:55:51	2016-09-02 08:55:52	Allow		172.16.100
⬇	☐	2016-09-02 08:54:51	2016-09-02 08:54:52	Allow		172.16.100
⬇	☐	2016-09-02 08:53:51	2016-09-02 08:53:52	Allow		172.16.100
⬇	☐	2016-09-02 08:53:46		Block		172.16.105

6. Chances are though that what you are looking for won't be easily found in a busy production deployment. So, let's build some custom filters. Click the **Search tab**.

Figure 507. Click the Search button



2016-09-02 07:48:35 - 2016-09-02 09:02:49
Expanding

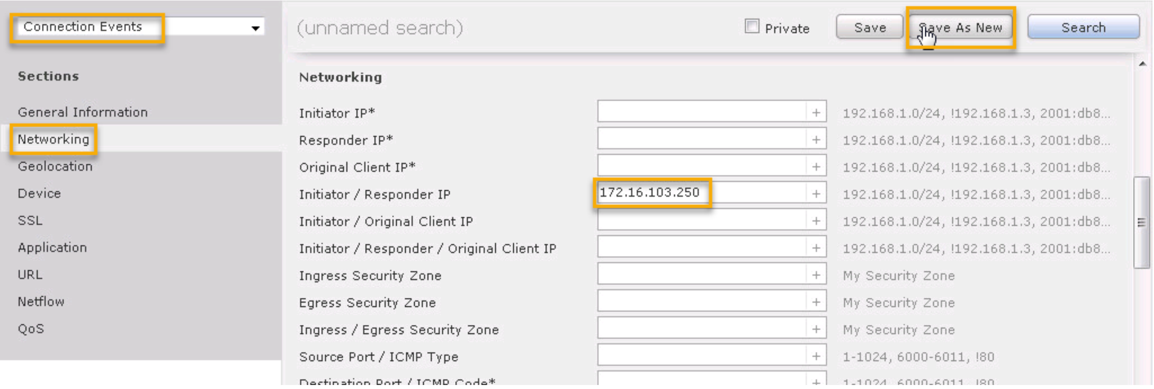
7. On the search tab you can create a custom search for any of the Analysis event logs. Select **Connection Events** from the dropdown list to change the view to only list the variables related to the Connection Events.

8. Click the **Networking** link to filter only the networking related fields.

    a. Create a filter that views all flows to/from the remote1-wkst (172.16.103.250). Since you want traffic from and to remote1-wkst put **172.16.103.250** in the **Initiator / Responder IP** field.

9. Click **Save As New**.

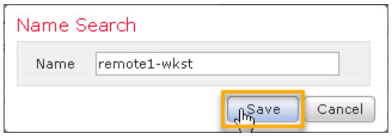
Figure 508. Build a filter



Initiator / Responder IP: 172.16.103.250

10. In the Name Search popup use **remote1-wkst** for the Name and then click **Save**.

Figure 509. Name and save

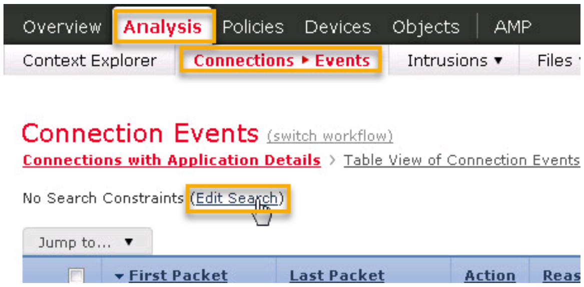


Name: remote1-wkst

11. Navigate to **Analysis > Connections > Events** again.

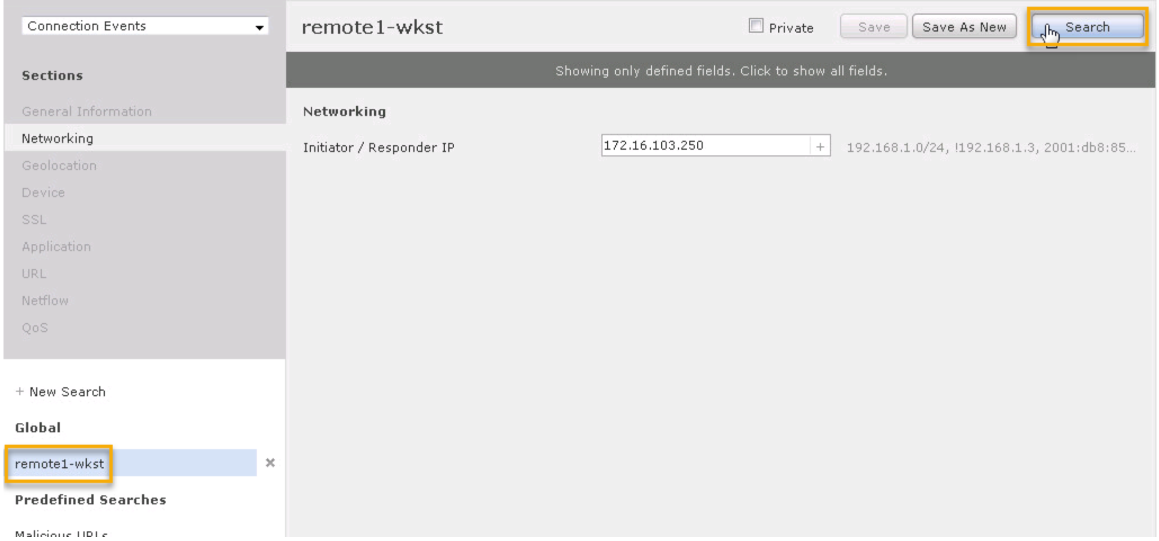
12. Click the **Edit Search** link.

Figure 510. Filter by Search



13. From the left side menu select the **remote1-wkst** link and then click **Search**. Now the list of events will only show flows related to remote1-wkst.

Figure 511. Filter by saved search



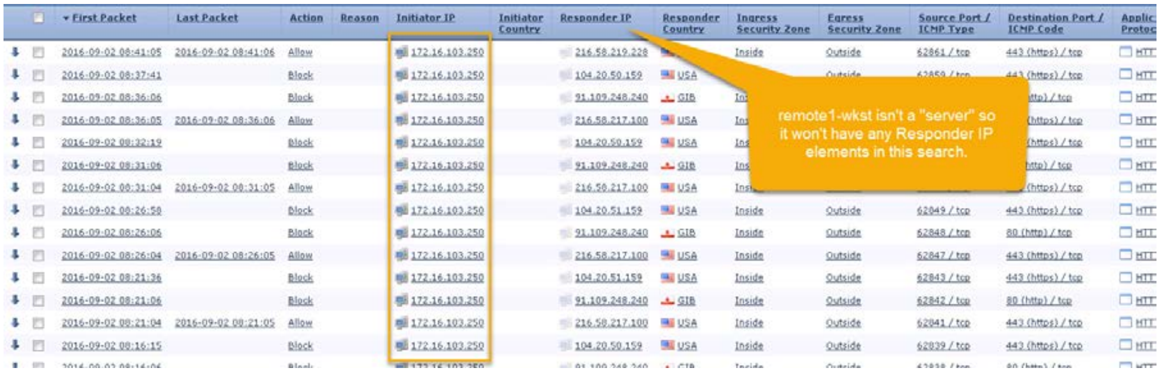
Showing only defined fields. Click to show all fields.

Networking

Initiator / Responder IP: 172.16.103.250 — 192.168.1.0/24, !192.168.1.3, 2001:db8:85...

14. Now the Connection Events are filtered based on any traffic to/from remote1-wkst.

Figure 512. Filtered Connection Events



First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Applic Protoc
2016-09-02 08:41:05	2016-09-02 08:41:06	Allow		172.16.103.250		216.58.219.228		Inside	Outside	62861 / tcp	443 (https) / tcp	HTT
2016-09-02 08:37:41		Block		172.16.103.250		104.20.50.159	USA		Outside	62859 / tcp	443 (https) / tcp	HTT
2016-09-02 08:36:06		Block		172.16.103.250		91.109.248.240	GIB	In			ttp) / tcp	HTT
2016-09-02 08:36:05	2016-09-02 08:36:06	Allow		172.16.103.250		216.58.217.100	USA	In			(https) / tcp	HTT
2016-09-02 08:32:19		Block		172.16.103.250		104.20.50.159	USA	Ins			(https) / tcp	HTT
2016-09-02 08:31:06		Block		172.16.103.250		91.109.248.240	GIB	Ins			http) / tcp	HTT
2016-09-02 08:31:04	2016-09-02 08:31:05	Allow		172.16.103.250		216.58.217.100	USA	Ins			(https) / tcp	HTT
2016-09-02 08:26:50		Block		172.16.103.250		104.20.51.159	USA	Inside	Outside	62849 / tcp	443 (https) / tcp	HTT
2016-09-02 08:26:06		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62848 / tcp	80 (http) / tcp	HTT
2016-09-02 08:26:04	2016-09-02 08:26:05	Allow		172.16.103.250		216.58.217.100	USA	Inside	Outside	62847 / tcp	443 (https) / tcp	HTT
2016-09-02 08:21:36		Block		172.16.103.250		104.20.51.159	USA	Inside	Outside	62843 / tcp	443 (https) / tcp	HTT
2016-09-02 08:21:06		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62842 / tcp	80 (http) / tcp	HTT
2016-09-02 08:21:04	2016-09-02 08:21:05	Allow		172.16.103.250		216.58.217.100	USA	Inside	Outside	62841 / tcp	443 (https) / tcp	HTT
2016-09-02 08:16:15		Block		172.16.103.250		104.20.50.159	USA	Inside	Outside	62839 / tcp	443 (https) / tcp	HTT
2016-09-02 08:16:06		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62838 / tcp	80 (http) / tcp	HTT

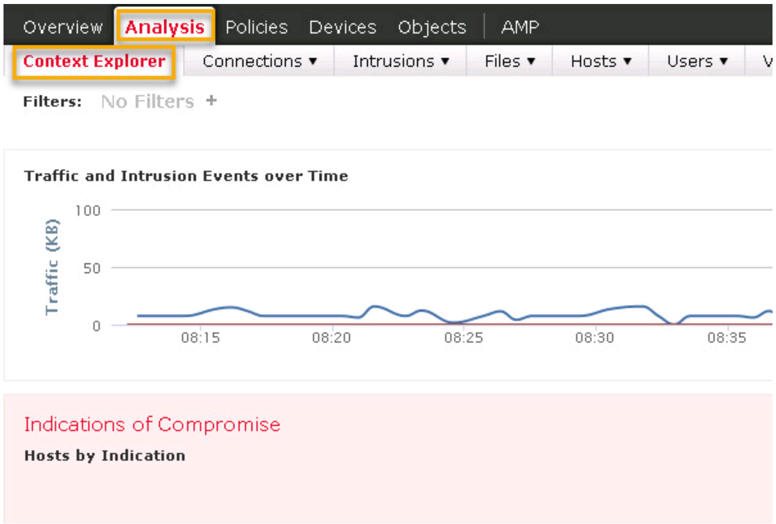
remote1-wkst isn't a "server" so it won't have any Responder IP elements in this search.

The Context Explorer

Your lab environment has not generated enough traffic to make this page worth visiting (nor have you had any compromises). That said, this a great place to start researching a possible infection within your company's network.

15. To view what this page looks like navigate to **Analysis > Context Explorer**.

Figure 513. Context Explorer

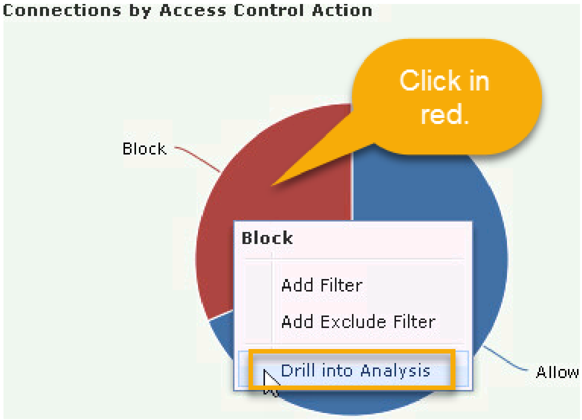


16. Scroll down and view the type of information that is gathered so far and at your disposal.

17. Find the **Connections by Access Control Action** section and click on the **red slice** of the pie chart.

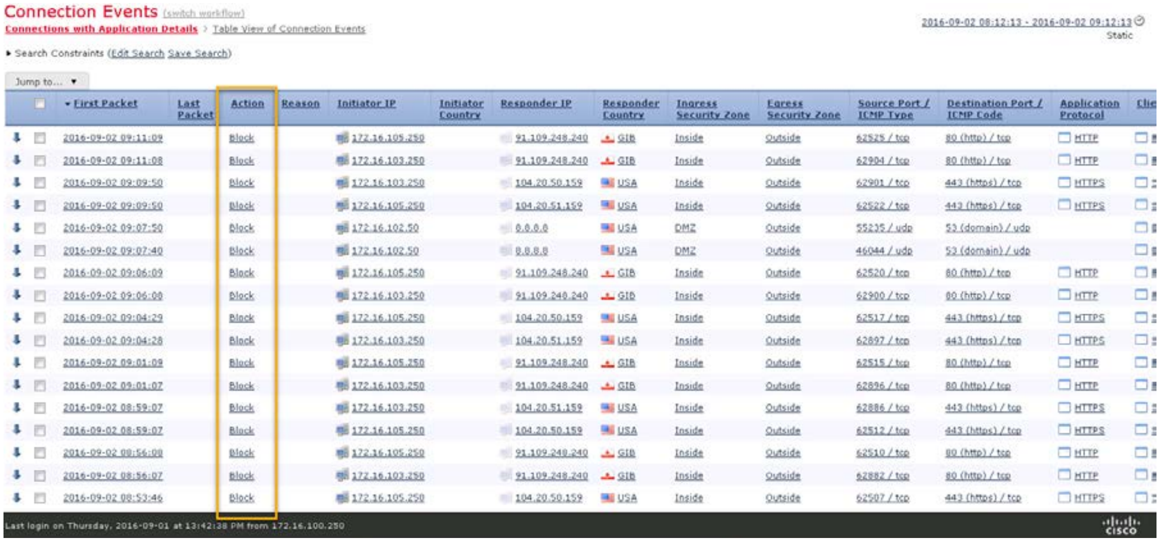
18. From the list of actions click **Drill into Analysis**.

Figure 514. Drill into Analysis



19. This is a quick way to see what Block actions have been taken by Access Control Policies.

Figure 515. Results



Connection Events (switch workflow)
Connections with Application Details > Table View of Connection Events

2016-09-02 08:12:13 - 2016-09-02 09:12:13
Static

▸ Search Constraints (Edit Search Save Search)

Jump to... ▾

	☐	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Clie
⬇	☐	2016-09-02 09:11:09		Block		172.16.105.250		91.109.248.240	GIB	Inside	Outside	62525 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 09:11:08		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62904 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 09:09:50		Block		172.16.103.250		104.20.50.159	USA	Inside	Outside	62901 / tcp	443 (https) / tcp	☐ HTTPS	☐
⬇	☐	2016-09-02 09:09:50		Block		172.16.105.250		104.20.51.159	USA	Inside	Outside	62522 / tcp	443 (https) / tcp	☐ HTTPS	☐
⬇	☐	2016-09-02 09:07:50		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	55235 / udp	53 (domain) / udp		☐
⬇	☐	2016-09-02 09:07:40		Block		172.16.102.50		8.8.8.8	USA	DMZ	Outside	46044 / udp	53 (domain) / udp		☐
⬇	☐	2016-09-02 09:06:09		Block		172.16.105.250		91.109.248.240	GIB	Inside	Outside	62520 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 09:06:08		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62900 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 09:04:29		Block		172.16.105.250		104.20.50.159	USA	Inside	Outside	62517 / tcp	443 (https) / tcp	☐ HTTPS	☐
⬇	☐	2016-09-02 09:04:28		Block		172.16.103.250		104.20.51.159	USA	Inside	Outside	62897 / tcp	443 (https) / tcp	☐ HTTPS	☐
⬇	☐	2016-09-02 09:01:09		Block		172.16.105.250		91.109.248.240	GIB	Inside	Outside	62515 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 09:01:07		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62896 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 08:59:07		Block		172.16.103.250		104.20.51.159	USA	Inside	Outside	62886 / tcp	443 (https) / tcp	☐ HTTPS	☐
⬇	☐	2016-09-02 08:59:07		Block		172.16.105.250		104.20.50.159	USA	Inside	Outside	62512 / tcp	443 (https) / tcp	☐ HTTPS	☐
⬇	☐	2016-09-02 08:56:08		Block		172.16.105.250		91.109.248.240	GIB	Inside	Outside	62510 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 08:56:07		Block		172.16.103.250		91.109.248.240	GIB	Inside	Outside	62882 / tcp	80 (http) / tcp	☐ HTTP	☐
⬇	☐	2016-09-02 08:53:46		Block		172.16.105.250		104.20.50.159	USA	Inside	Outside	62507 / tcp	443 (https) / tcp	☐ HTTPS	☐

Last login on Thursday, 2016-09-01 at 13:42:38 PM from 172.16.100.250

The Discovery Topology Map

Remember how you modified the Policies > Network Discovery from its default values to be more specific about passively detecting what hosts and applications are running through the FTD devices in Example Corp's network? This whole time throughout this lab the FTD devices have been monitoring the data traffic flowing through them and trying to categorize the type of Applications being used as well as the Operating Systems of each host.

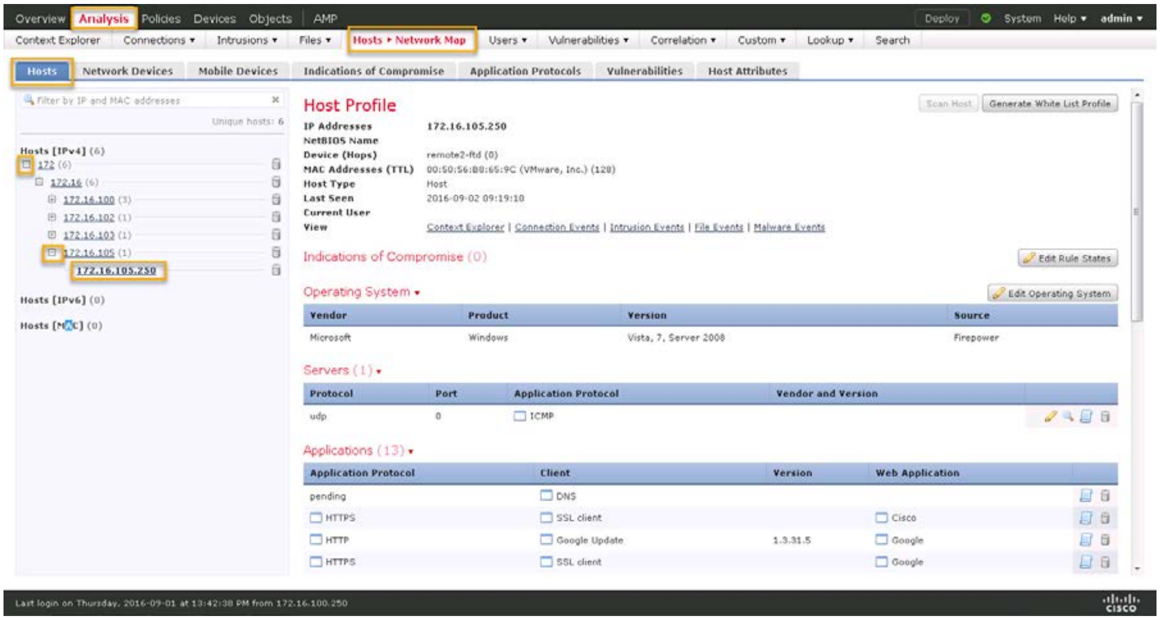
20. Navigate to **Analysis > Hosts > Network Map**. Each tab on this page correlates to some sort of analysis of the type of hosts, devices, and applications running on the Example Corp network.

21. On the **Hosts tab**:

    a. Expand the **Hosts [IPv4]** entry for **172** and see how it expands to show the all the discovered hosts in this IP range.

    b. Expand the **172.16.105** link and click on the **172.16.105.250** link. The right side of this page will populate with the information gathered (or suspected) about this IP address. Notice how the FTD has correctly learned that this is a Microsoft Windows 7 host.

Figure 516. Details of a Host



Unique hosts: 6

Hosts [IPv4] (6)
- 172 (6)
  - 172.16 (6)
    - 172.16.100 (3)
    - 172.16.102 (1)
    - 172.16.103 (1)
    - 172.16.105 (1)
      - 172.16.105.250

Hosts [IPv6] (0)

Hosts [MAC] (0)

Host Profile

IP Addresses	172.16.105.250
NetBIOS Name	
Device (Hops)	remote2-ftd (0)
MAC Addresses (TTL)	00:50:56:B8:65:9C (VMware, Inc.) (128)
Host Type	Host
Last Seen	2016-09-02 09:19:10
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (0)

Operating System ▾

Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008	Firepower

Servers (1) ▾

Protocol	Port	Application Protocol	Vendor and Version
udp	0	ICMP	

Applications (13) ▾

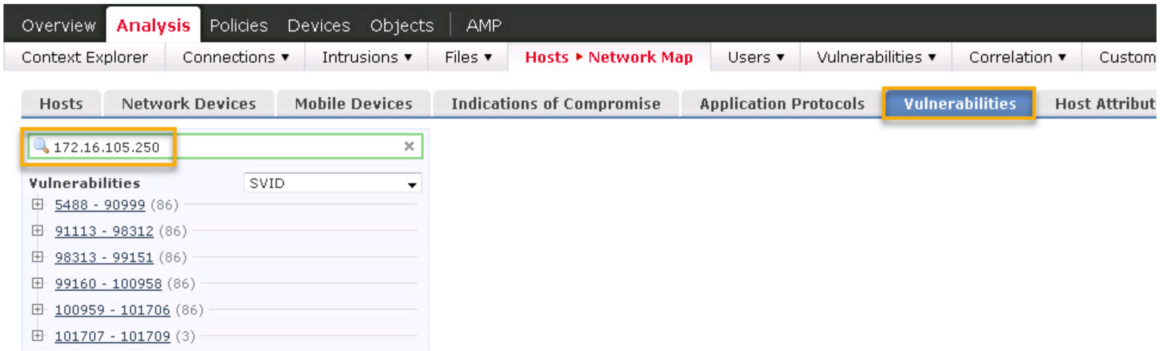
Application Protocol	Client	Version	Web Application
pending	DNS		
HTTPS	SSL client		Cisco
HTTP	Google Update	1.3.31.5	Google
HTTPS	SSL client		Google

Last login on Thursday, 2016-09-01 at 13:42:38 PM from 172.16.100.250

22. On the **Vulnerabilities tab**:

    a. In the search field type **172.16.105.250** (remote2-wkst IP) and click **Enter**. This will list all the possible vulnerabilities for this known host IP.

Figure 517. Filter Vulnerabilities by a particular discovered host



172.16.105.250

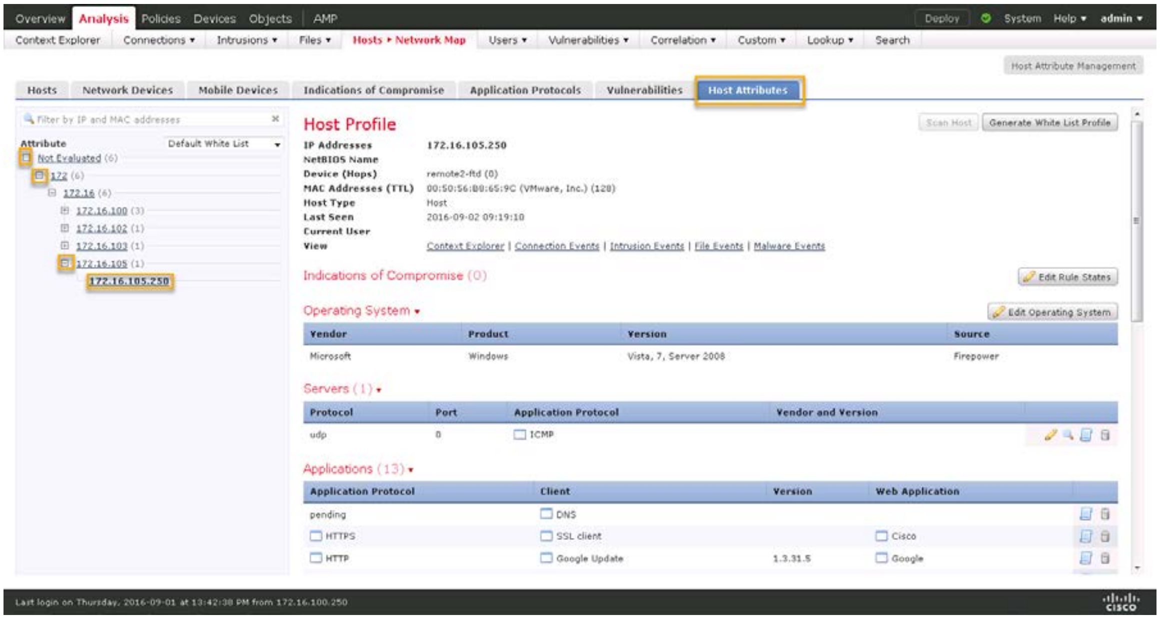
Vulnerabilities SVID

- 5488 - 90999 (86)
- 91113 - 98312 (86)
- 98313 - 99151 (86)
- 99160 - 100958 (86)
- 100959 - 101706 (86)
- 101707 - 101709 (3)

23. On the **Host Attributes tab**:

    a. Using the **Not Evaluated** menu drill down to **172.16.105.250** and again see detailed information about the remote2-wkst host.

Figure 518. More details about remote2-wkst



Host Profile

IP Addresses	172.16.105.250
NetBIOS Name	
Device (Hops)	remote2-ftd (0)
MAC Addresses (TTL)	00:50:56:B0:65:9C (VMware, Inc.) (128)
Host Type	Host
Last Seen	2016-09-02 09:19:10
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (0)

Operating System ▾

Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008	Firepower

Servers (1) ▾

Protocol	Port	Application Protocol	Vendor and Version
udp	0	ICMP	

Applications (13) ▾

Application Protocol	Client	Version	Web Application
pending	DNS		
HTTPS	SSL client		Cisco
HTTP	Google Update	1.3.31.5	Google

Last login on Thursday, 2016-09-01 at 13:42:38 PM from 172.16.100.250

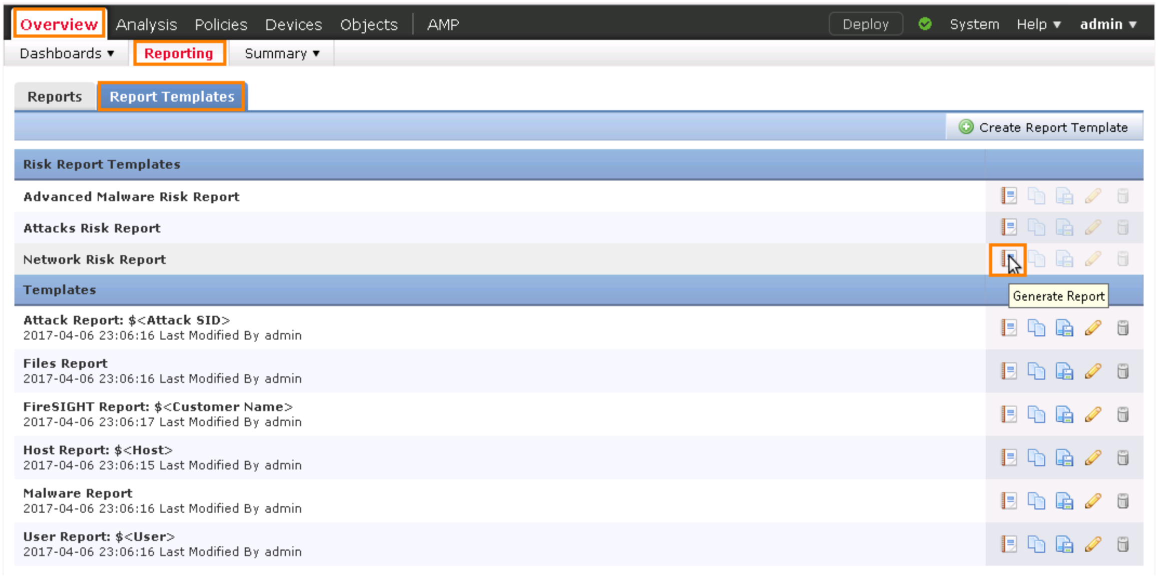
24. The other tabs don't have any information mostly because of how small your lab network is. You don't have any networking equipment nor any mobile devices. You haven't generated enough traffic to get a full application profile.

Risk Reports

25. Navigate to **Overview > Reporting** and click on the **Report Templates** tab.

26. Notice the three prebuilt Risk Report Templates. Click the **Generate Report** link for the **Network Risk Report** row.

Figure 519. Navigate to Risk Reports



Risk Report Templates

Advanced Malware Risk Report

Attacks Risk Report

Network Risk Report

Templates

Attack Report: $<Attack SID>
2017-04-06 23:06:16 Last Modified By admin

Files Report
2017-04-06 23:06:16 Last Modified By admin

FireSIGHT Report: $<Customer Name>
2017-04-06 23:06:17 Last Modified By admin

Host Report: $<Host>
2017-04-06 23:06:15 Last Modified By admin

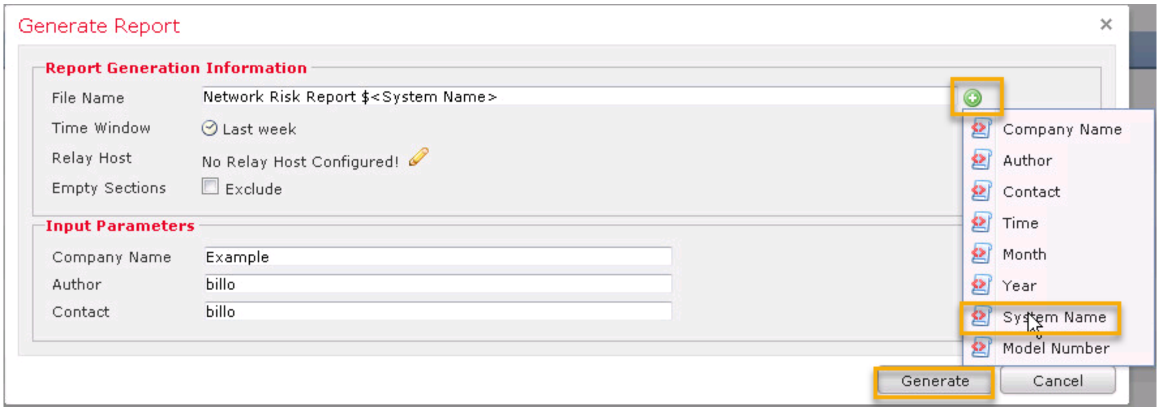
Malware Report
2017-04-06 23:06:16 Last Modified By admin

User Report: $<User>
2017-04-06 23:06:16 Last Modified By admin

27. Click the **green plus icon** on the **File Name** row. Notice how you can add addition information to customize the report. Select **System Name**.

28. Click **Generate** to create this report.

Figure 520. Generate report



Report Generation Information

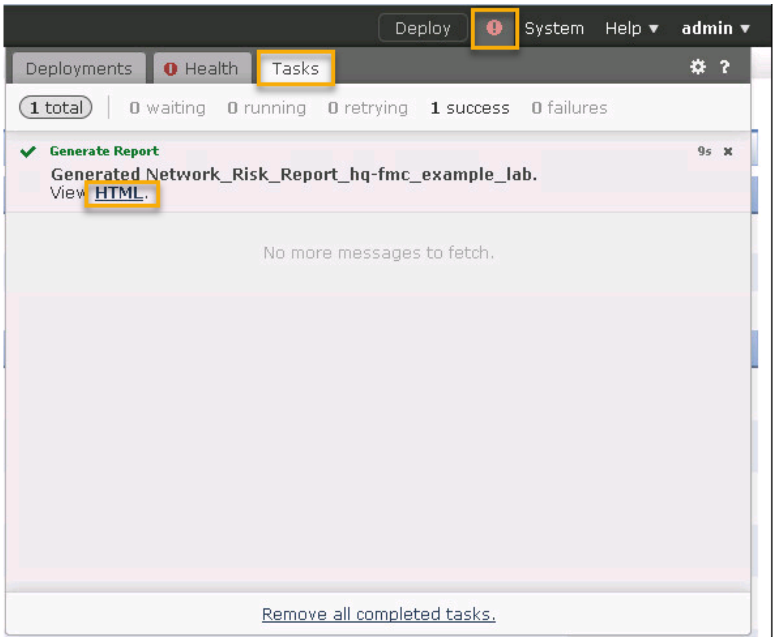
File Name	Network Risk Report $<System Name>
Time Window	Last week
Relay Host	No Relay Host Configured!
Empty Sections	□ Exclude

Input Parameters

Company Name	Example
Author	billo
Contact	billo

29. You can view the progress of the generation of this report in the **Message Center > Tasks tab**.
30. Once the report is generated click the **HTML** link or navigate to **Overview > Reporting > Reports** and click on the report. A new browser tab will load the report for viewing.

Figure 521. Message Center Tasks



1 total | 0 waiting 0 running 0 retrying 1 success 0 failures

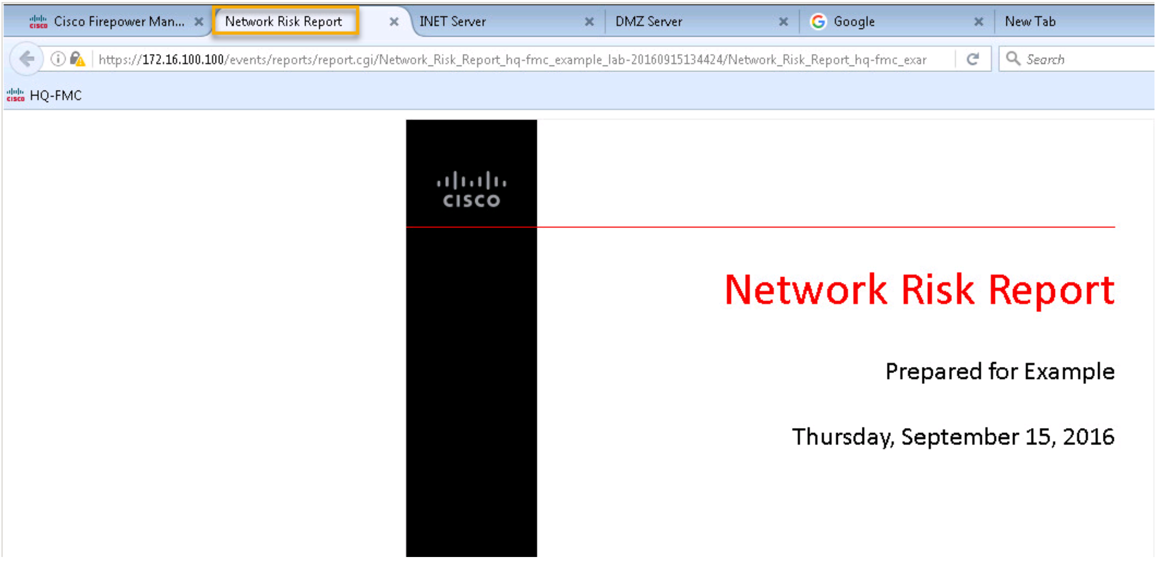
Generate Report
Generated Network_Risk_Report_hq-fmc_example_lab.
View HTML.

No more messages to fetch.

Remove all completed tasks.

31. Peruse the report. Bear in mind that this is a small network and recently installed so there shouldn't be much in the way of content. Pay more attention to the section headings.

Figure 522. Risk Report



https://172.16.100.100/events/reports/report.cgi/Network_Risk_Report_hq-fmc_example_lab-20160915134424/Network_Risk_Report_hq-fmc_exar

Network Risk Report

Prepared for Example

Thursday, September 15, 2016

If your needs require more/different information within a report you can create custom reports with the **Create Report Template** button on the **Overview > Reporting > Report Templates tab**.

Scenario Summary

This scenario shows you how to view the information that each FTD is gathering regarding the data flowing through each of them. This information is then sent to the FMC and correlated into events, charts, and details about the hosts, applications, and data flows that you can then use to troubleshoot issues within the customer's network.

Scenario 14. Introduction to API Programming the FMC

Scenario Description

As a deployment engineer this section will either be extremely important or not applicable. That said, having a basic knowledge of how the API programming works on the FMC is probably a good idea.

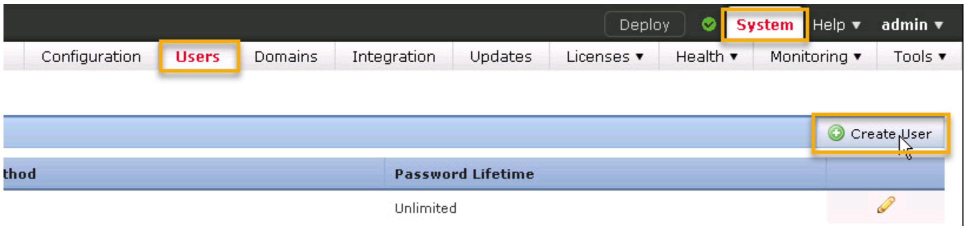
In this scenario you will learn how to send API requests to the FMC and how to interpret the results returned.

Create a New User

The FMC GUI only allows one logged in session per user. The API request will authenticate to the FMC as a user so it will count as a session. Thus, if you used the admin user in the API call it would either not work (since you are current logged in as admin) or it would work and your session with the FMC would be terminated. The only user that exists at the moment is admin.

1. On hq-wkst in the FMC GUI navigate to **System > Users** and click the **Create User** button.

Figure 523. Users



2. Use the following to create the new user.

   a. User Name: **apiadmin** (The username “admin” is pre-filled in here because FireFox has a saved username/password entry for 172.16.100.100.)

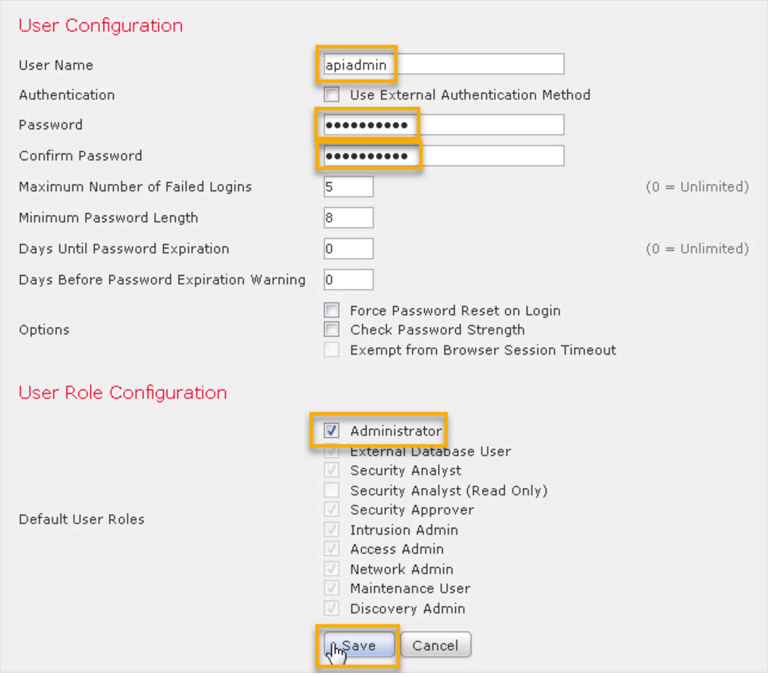
   b. Password: **C1sco12345**

   c. Confirm Password: **C1sco12345**

   d. User Role Configuration: Check the **Administrator** box. (Notice that the Exempt from Browser Session Timeout checkbox is now greyed out. Any user account assigned the administrator role cannot stay logged into the FMC website infinitely.)

   e. Click **Save**.

Figure 524. Create new User



User Configuration

User Name	apiadmin	
Authentication	□ Use External Authentication Method	
Password	••••••••••	
Confirm Password	••••••••••	
Maximum Number of Failed Logins	5	(0 = Unlimited)
Minimum Password Length	8	
Days Until Password Expiration	0	(0 = Unlimited)
Days Before Password Expiration Warning	0	
Options	□ Force Password Reset on Login □ Check Password Strength □ Exempt from Browser Session Timeout	

User Role Configuration

	☑ Administrator
Default User Roles	☑ External Database User ☑ Security Analyst □ Security Analyst (Read Only) ☑ Security Approver ☑ Intrusion Admin ☑ Access Admin ☑ Network Admin ☑ Maintenance User ☑ Discovery Admin

Notice that you are not going to “Save and Deploy”. This user account is related to accessing the FMC.

Using the API Explorer

FMC comes with an API Explorer feature that allows you to use/test API calls. This explorer also contains all the documentation for each API function.

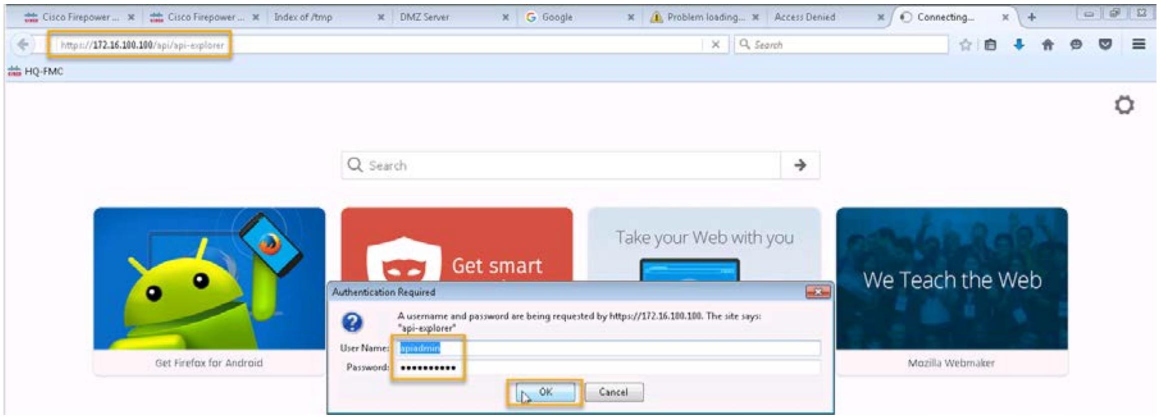
3. On hq-wkst, within **FireFox**, open a **new tab** and go to **https://172.16.100.100/api/api-explorer**.

4. In the Authentication Required popup windows log in using the new user credentials:

    a. User Name: **apiadmin**

    b. Password: **C1sco12345**

Figure 525. Log into API Explorer



Authentication Required

A username and password are being requested by https://172.16.100.100. The site says: "api-explorer"

User Name: apiadmin

Password: ••••••••••

OK Cancel

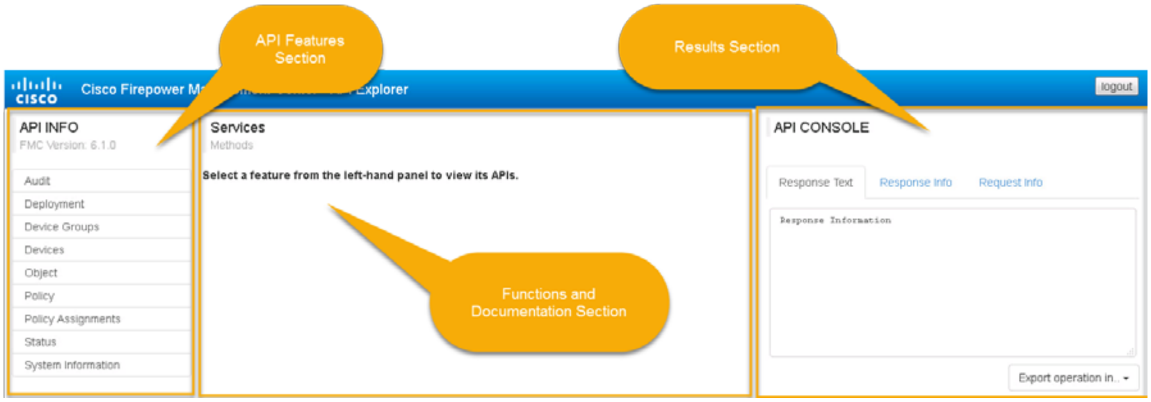
5. This page is broken into 3 parts, or columns:

    a. The leftmost column is a list of all the API features that are available.

    b. The middle column shows the documentation and functions for the selected API feature.

    c. The rightmost column gives the result of running the API function command. On some functions you can additionally add parameters and re-run the command from here too.

Figure 526. API Explorer GUI Layout

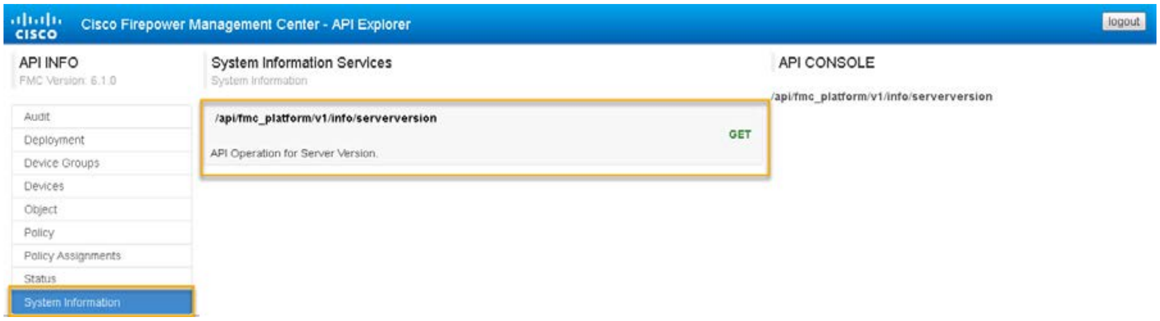


Select a feature from the left-hand panel to view its APIs.

6. From the left column click the **System Information** link.

    a. Notice how the middle column is now populated with all the API functions related to System Information feature. In this case there is only one function: The Server Version function.

Figure 527. Functions for System Information Features



API INFO
FMC Version: 6.1.0

System Information Services
System Information

/api/fmc_platform/v1/info/serverversion

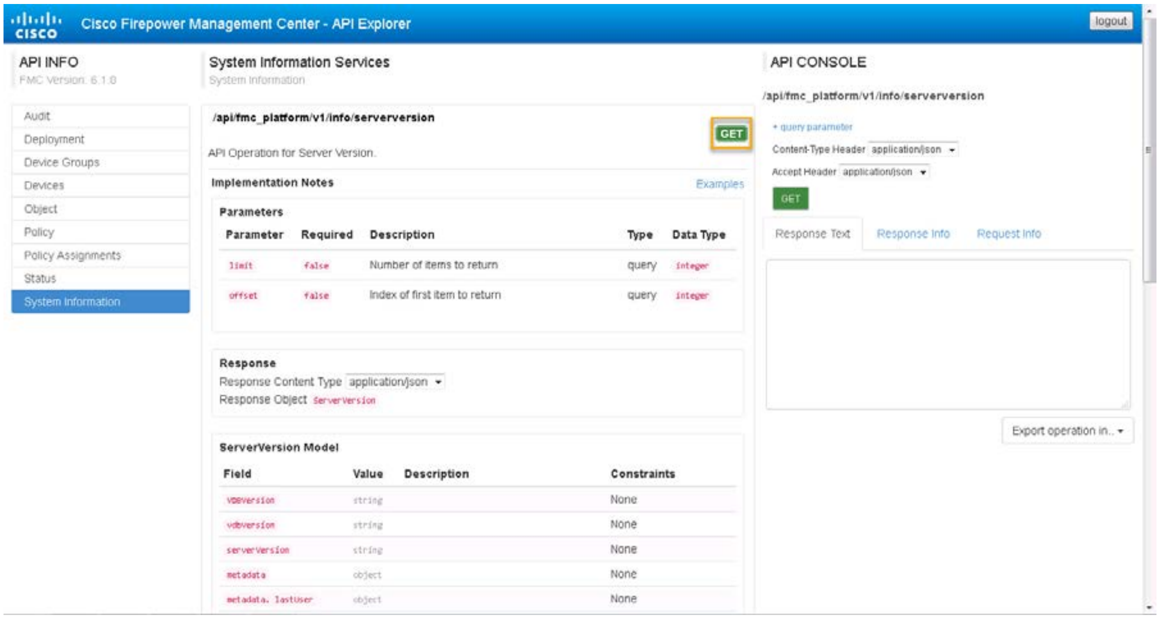
API Operation for Server Version.

API CONSOLE

/api/fmc_platform/v1/info/serverversion

    b. Click **GET** for this function. Now the middle and rightmost columns have populated with specific information regarding this function. The middle column is showing all “documentation” around this function. The rightmost column is where you can actually query the FMC for information.

Figure 528. Documentation and Functions for Server Version



API INFO
FMC Version: 6.1.0

System Information Services
System Information

/api/fmc_platform/v1/info/serverversion

API Operation for Server Version.

Implementation Notes

Parameters

Parameter	Required	Description	Type	Data Type
limit	false	Number of items to return	query	integer
offset	false	Index of first item to return	query	integer

Response
Response Content Type application/json
Response Object ServerVersion

ServerVersion Model

Field	Value	Description	Constraints
vDBVersion	string		None
vdbversion	string		None
serverVersion	string		None
metadata	object		None
metadata. lastUser	object		None

API CONSOLE

/api/fmc_platform/v1/info/serverversion

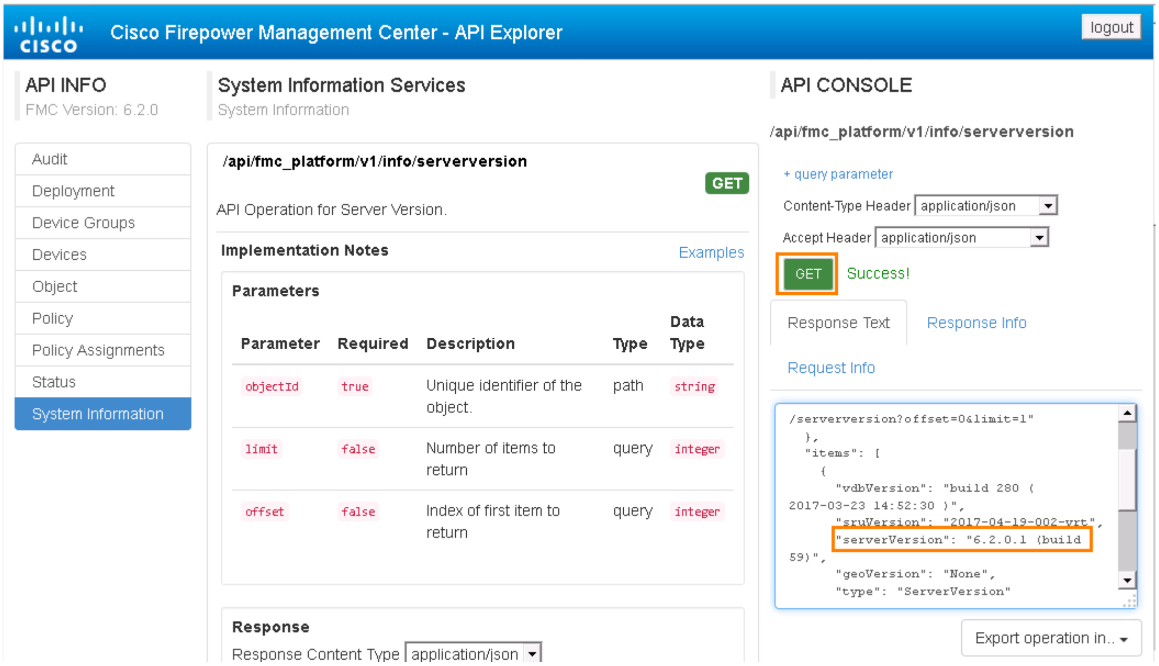
Content-Type Header application/json
Accept Header application/json

    c. In the rightmost column click the **GET** button.

    d. In the rightmost column the **Response Text tab** is now populated with what the FMC returned. This output is formatted in JSON which then can be parsed by some programmer’s program to get the information (such as the version of software the FMC is running in this case).

JSON (JavaScript Object Notation) is a minimal, readable format for structuring data. It is used primarily to transmit data between a server and web application, as an alternative to XML.

Figure 529. GET Server Version JSON



/api/fmc_platform/v1/info/serverversion

API Operation for Server Version.

Implementation Notes

Parameters

Parameter	Required	Description	Type	Data Type
objectId	true	Unique identifier of the object.	path	string
limit	false	Number of items to return	query	integer
offset	false	Index of first item to return	query	integer

Response

Response Content Type application/json

/api/fmc_platform/v1/info/serverversion

Content-Type Header application/json

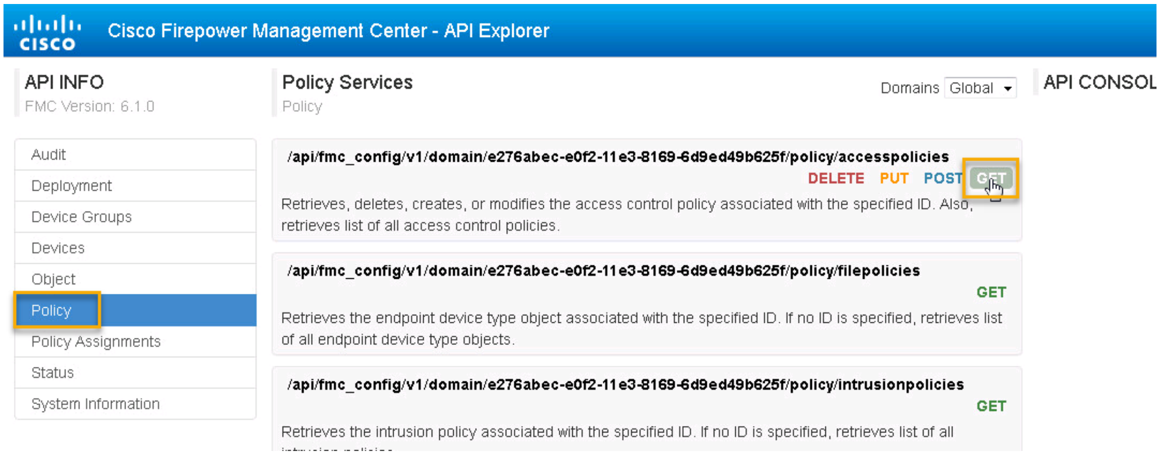
Accept Header application/json

```
/serverversion?offset=0&limit=1"
  },
  "items": [
    {
      "vdbVersion": "build 280 (
2017-03-23 14:52:30 )",
      "sruVersion": "2017-04-19-002-vrt",
      "serverVersion": "6.2.0.1 (build
59)",
      "geoVersion": "None",
      "type": "ServerVersion"
```

7. In the leftmost column click the **Policy** link.

    a. In the middle column click the **GET** action for the **Access Policies** link (the topmost GET).

Figure 530. GET Access Policies



/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies

Retrieves, deletes, creates, or modifies the access control policy associated with the specified ID. Also, retrieves list of all access control policies.

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/filepolicies

Retrieves the endpoint device type object associated with the specified ID. If no ID is specified, retrieves list of all endpoint device type objects.

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/intrusionpolicies

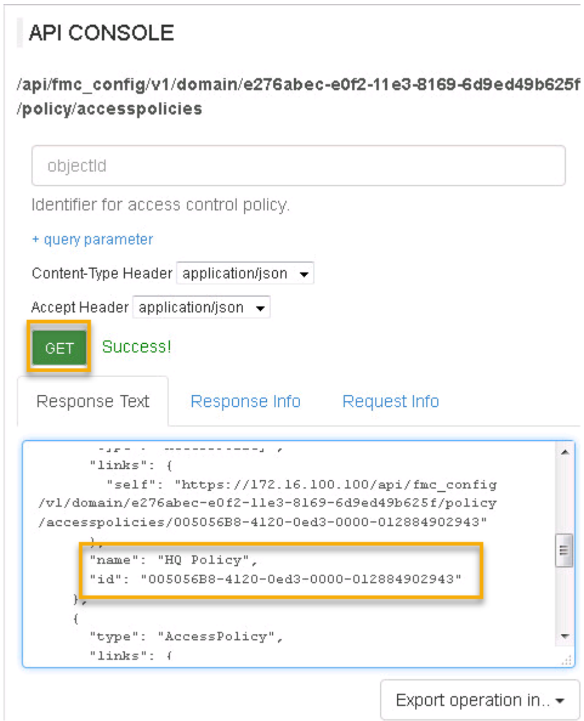
Retrieves the intrusion policy associated with the specified ID. If no ID is specified, retrieves list of all

b. In the right column click the **GET** button to retrieve a list of all the Access Control Policies that are currently configured on this FMC.

c. The output in the **Response Text tab** is a little hard to follow but it shouldn't be too hard to scroll through this output and find the "Base Policy", "HQ Policy", and "Remote Locations" policies.

d. Find the "**id**" value for the "**HQ Policy**" (it should be the line right below the HQ Policy name). Even though the mouse icon shows a slashed-out circle you can still use the mouse to highlight the ID's value.

Figure 531. GET Access Policies Results



API CONSOLE

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies

objectId

Identifier for access control policy.

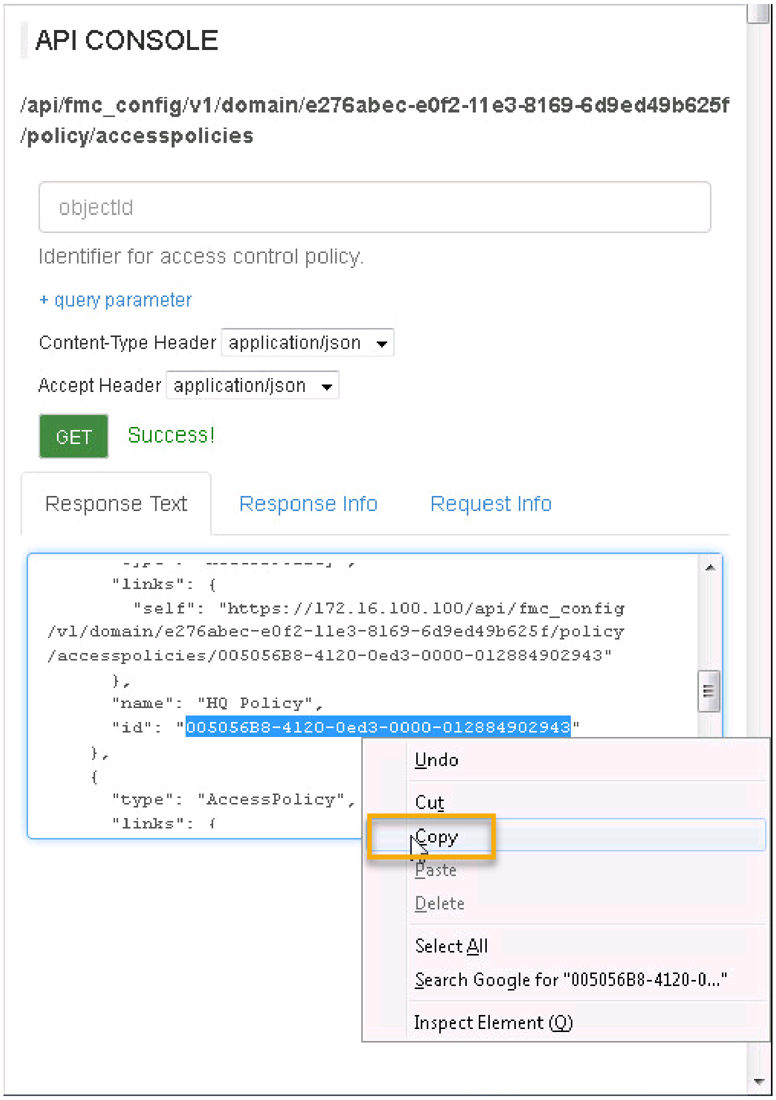
Content-Type Header: application/json

Accept Header: application/json

```
      "links": {
        "self": "https://172.16.100.100/api/fmc_config
/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy
/accesspolicies/005056B8-4120-0ed3-0000-012884902943"
      },
      "name": "HQ Policy",
      "id": "005056B8-4120-0ed3-0000-012884902943"
    },
    {
      "type": "AccessPolicy",
      "links": {
```

e. **Copy** the HQ Policy's **ID** value.

Figure 532. Copy HQ Policy ID



/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies

Identifier for access control policy.

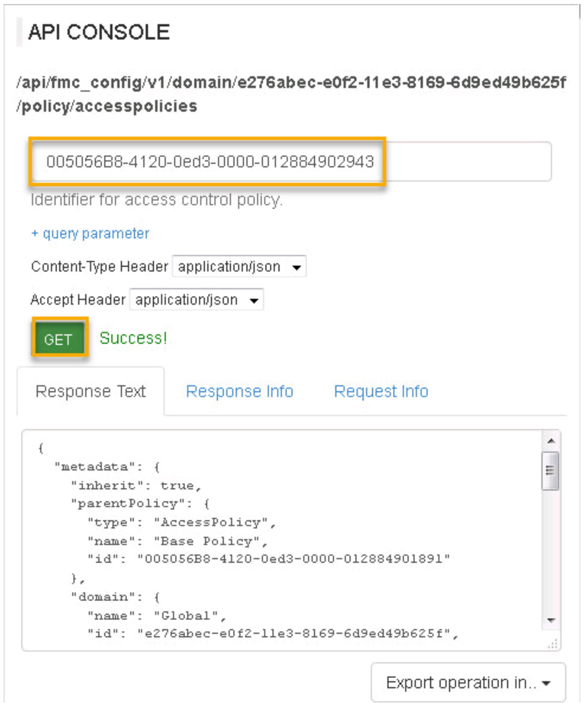
Content-Type Header application/json

Accept Header application/json

```
        "links": {
          "self": "https://172.16.100.100/api/fmc_config
/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy
/accesspolicies/005056B8-4120-0ed3-0000-012884902943"
        },
        "name": "HQ Policy",
        "id": "005056B8-4120-0ed3-0000-012884902943"
      },
      {
        "type": "AccessPolicy",
        "links": {
```

f. Paste it in the topmost field in the right column. Click the **GET** button again. This will “drill down” and just look at the HQ Policy information.

Figure 533. Paste into Field and GET again



API CONSOLE

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f /policy/accesspolicies

005056B8-4120-0ed3-0000-012884902943

Identifier for access control policy.

+ query parameter

Content-Type Header: application/json

Accept Header: application/json

GET Success!

Response Text | Response Info | Request Info

```
{
  "metadata": {
    "inherit": true,
    "parentPolicy": {
      "type": "AccessPolicy",
      "name": "Base Policy",
      "id": "005056B8-4120-0ed3-0000-012884901891"
    },
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
```

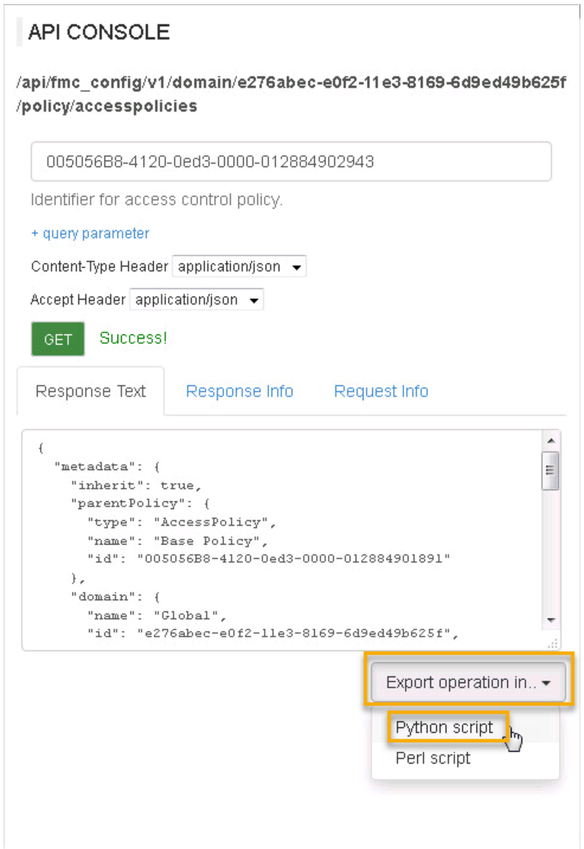
Export operation in..

Python Scripting the FMC API

The API Explorer can be used to create an example python script which then can be run without the need to open up the API Explorer website.

8. Click the **Export operation in…** link at the bottom of the right column. Select **Python script** from the dropdown list.

Figure 534. Export Python Script



API CONSOLE

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/policy/accesspolicies

005056B8-4120-0ed3-0000-012884902943

Identifier for access control policy.

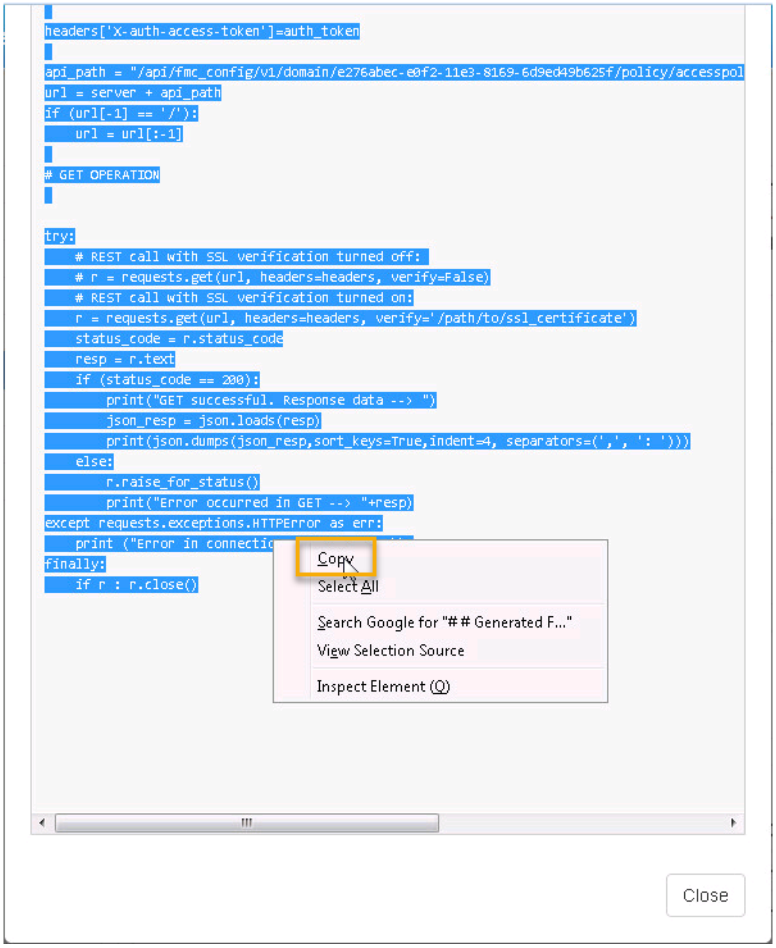
Content-Type Header: application/json

Accept Header: application/json

```
{
  "metadata": {
    "inherit": true,
    "parentPolicy": {
      "type": "AccessPolicy",
      "name": "Base Policy",
      "id": "005056B8-4120-0ed3-0000-012884901891"
    },
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
```

9. The middle column will now have a popup window showing the example python script, or rather a python script template. This “script” is not functional in its current state but can be used to build a valid script. **Highlight** all the green text and **copy** the text.

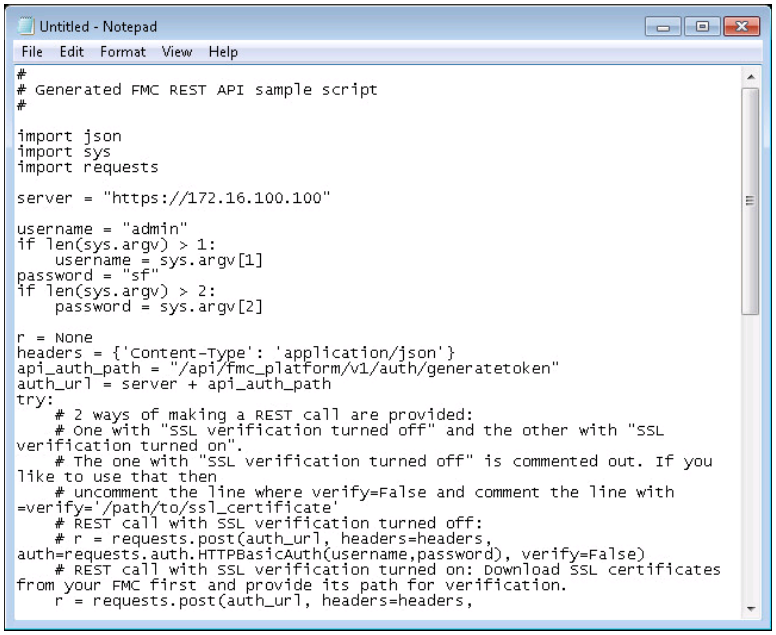
Figure 535. Copy python script text



```
headers['X-auth-access-token']=auth_token

api_path = "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspol
url = server + api_path
if (url[-1] == '/'):
    url = url[:-1]

# GET OPERATION


try:
    # REST call with SSL verification turned off:
    # r = requests.get(url, headers=headers, verify=False)
    # REST call with SSL verification turned on:
    r = requests.get(url, headers=headers, verify='/path/to/ssl_certificate')
    status_code = r.status_code
    resp = r.text
    if (status_code == 200):
        print("GET successful. Response data --> ")
        json_resp = json.loads(resp)
        print(json.dumps(json_resp,sort_keys=True,indent=4, separators=(',', ': ')))
    else:
        r.raise_for_status()
        print("Error occurred in GET --> "+resp)
except requests.exceptions.HTTPError as err:
    print ("Error in connectio
finally:
    if r : r.close()
```

10. **Paste** it into a **notepad** file.

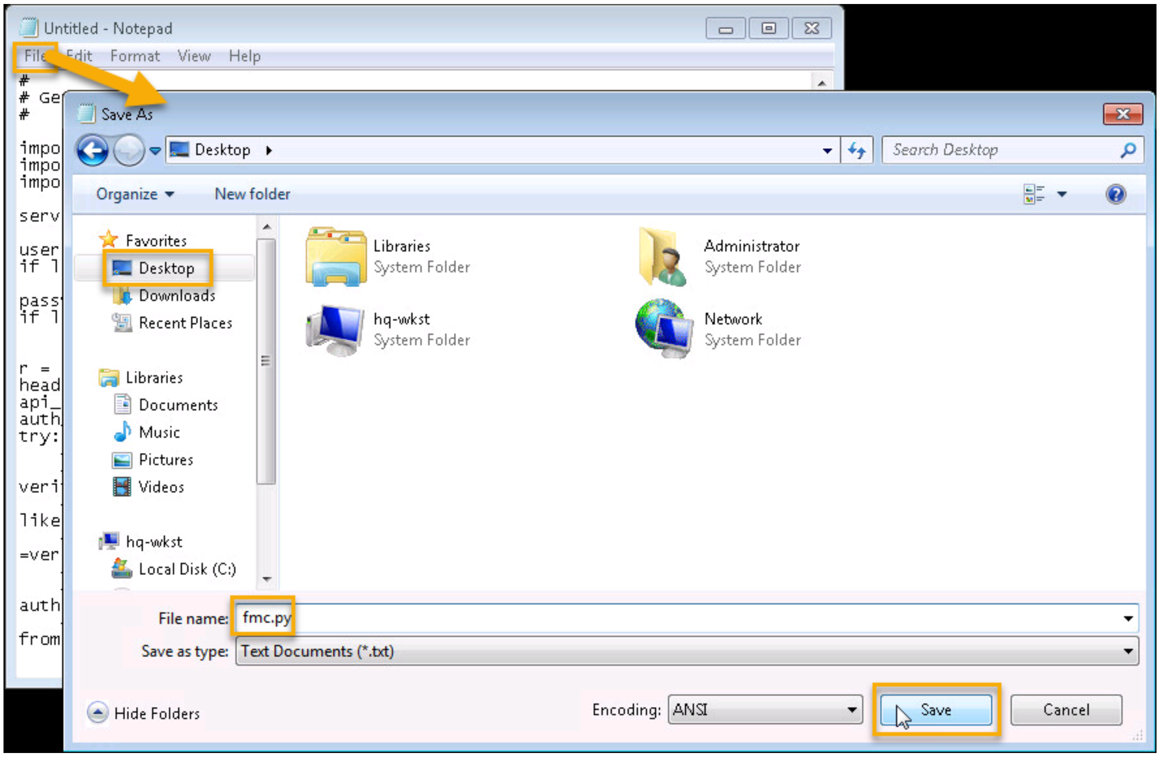
Figure 536. Open Notepad and paste text into it.



```
#
# Generated FMC REST API sample script
#

import json
import sys
import requests

server = "https://172.16.100.100"

username = "admin"
if len(sys.argv) > 1:
    username = sys.argv[1]
password = "sf"
if len(sys.argv) > 2:
    password = sys.argv[2]

r = None
headers = {'Content-Type': 'application/json'}
api_auth_path = "/api/fmc_platform/v1/auth/generatetoken"
auth_url = server + api_auth_path
try:
    # 2 ways of making a REST call are provided:
    # One with "SSL verification turned off" and the other with "SSL
verification turned on".
    # The one with "SSL verification turned off" is commented out. If you
like to use that then
    # uncomment the line where verify=False and comment the line with
=verify='/path/to/ssl_certificate'
    # REST call with SSL verification turned off:
    # r = requests.post(auth_url, headers=headers,
auth=requests.auth.HTTPBasicAuth(username,password), verify=False)
    # REST call with SSL verification turned on: Download SSL certificates
from your FMC first and provide its path for verification.
    r = requests.post(auth_url, headers=headers,
```

11. **Save** that notepad file as **fmc.py** to the **Desktop**.

Figure 537. Save the file



File name: fmc.py

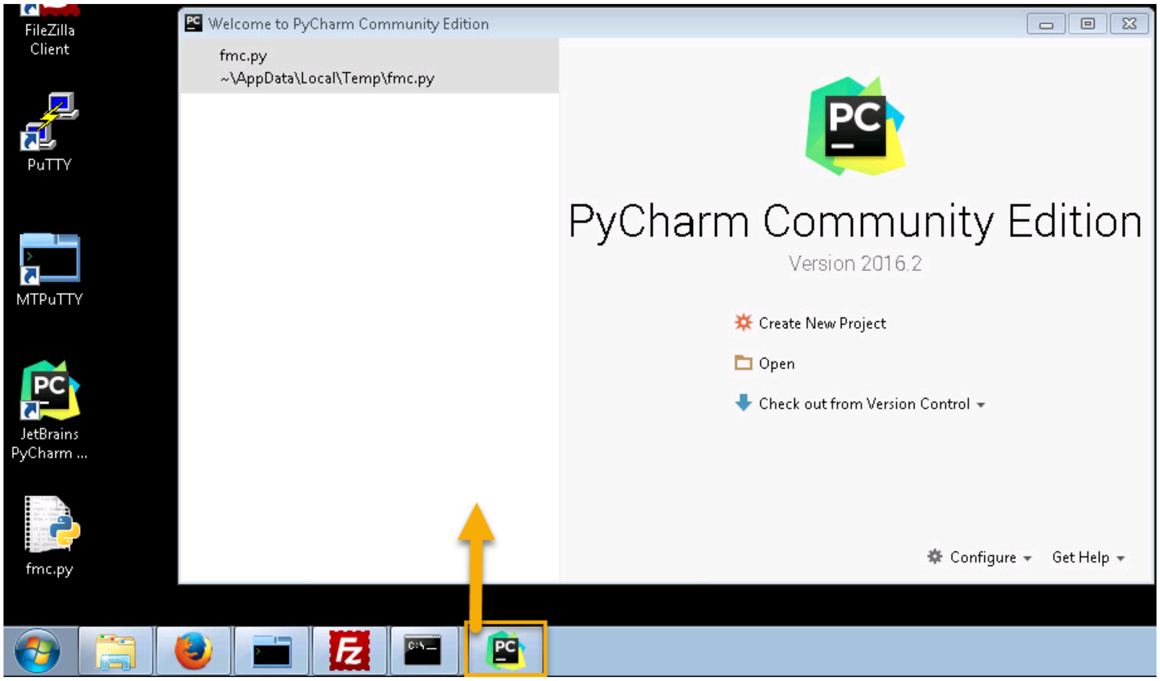
Save as type: Text Documents (*.txt)

Encoding: ANSI

12. A python IDE application, called PyCharm, has been installed on hq-wkst. This is an application that can be used to write and execute python scripts. Open **PyCharm** via the taskbar link.

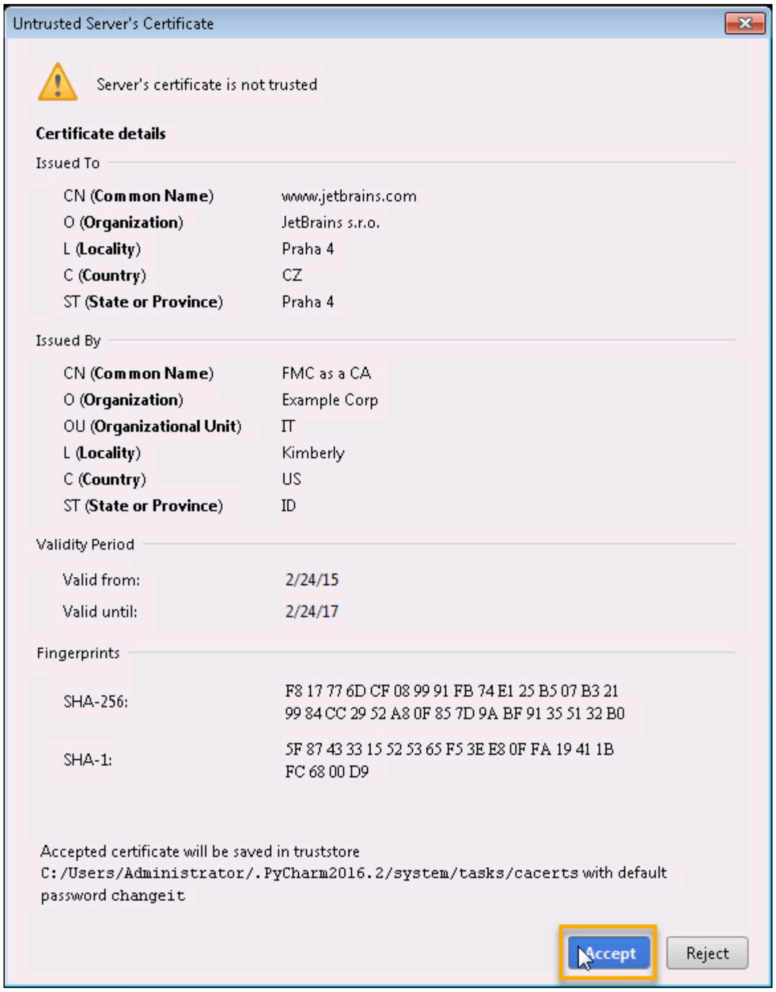
An integrated development environment (IDE) is a software suite that consolidates the basic tools developers need to write and test software.

Figure 538. Open PyCharm


FileZilla Client
PuTTY
MTPuTTY
JetBrains PyCharm ...
fmc.py
Welcome to PyCharm Community Edition
fmc.py
~\AppData\Local\Temp\fmc.py
PyCharm Community Edition
Version 2016.2
Create New Project
Open
Check out from Version Control
Configure
Get Help

13. Looks like the SSL Policy is still working. **Accept** the certificate when prompted.

Figure 539. Accept certificate



Untrusted Server's Certificate

Server's certificate is not trusted

Certificate details

Issued To

CN (**Common Name**)	www.jetbrains.com
O (**Organization**)	JetBrains s.r.o.
L (**Locality**)	Praha 4
C (**Country**)	CZ
ST (**State or Province**)	Praha 4

Issued By

CN (**Common Name**)	FMC as a CA
O (**Organization**)	Example Corp
OU (**Organizational Unit**)	IT
L (**Locality**)	Kimberly
C (**Country**)	US
ST (**State or Province**)	ID

Validity Period

Valid from:	2/24/15
Valid until:	2/24/17

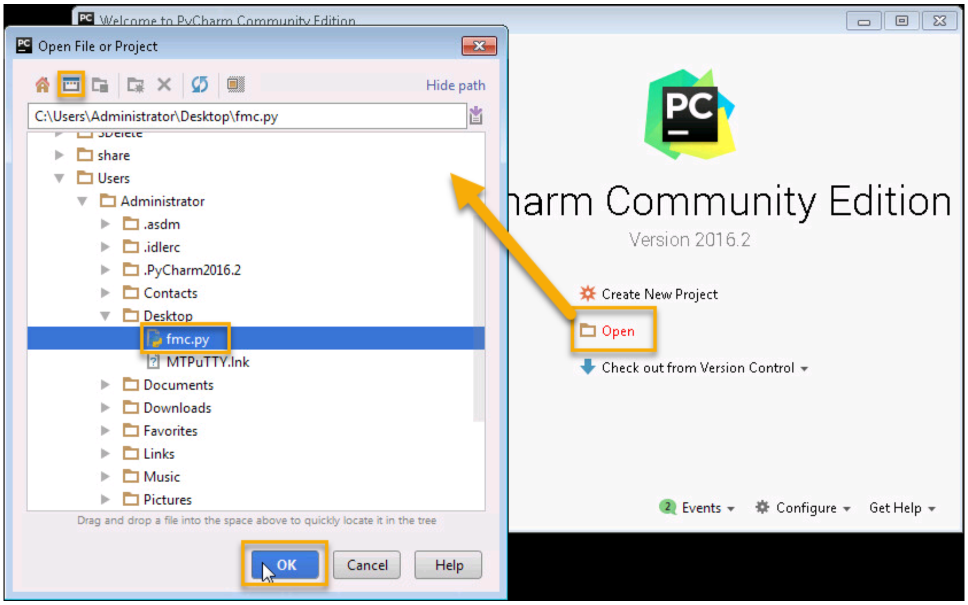
Fingerprints

SHA-256:	F8 17 77 6D CF 08 99 91 FB 74 E1 25 B5 07 B3 21 99 84 CC 29 52 A8 0F 85 7D 9A BF 91 35 51 32 B0
SHA-1:	5F 87 43 33 15 52 53 65 F5 3E E8 0F FA 19 41 1B FC 68 00 D9

Accepted certificate will be saved in truststore `C:/Users/Administrator/.PyCharm2016.2/system/tasks/cacerts` with default password `changeit`

14. Click **Open** and browse to the **Desktop** and select the **fmc.py** file. Click **OK**. The PyCharm application will now open the fmc.py file for editing.

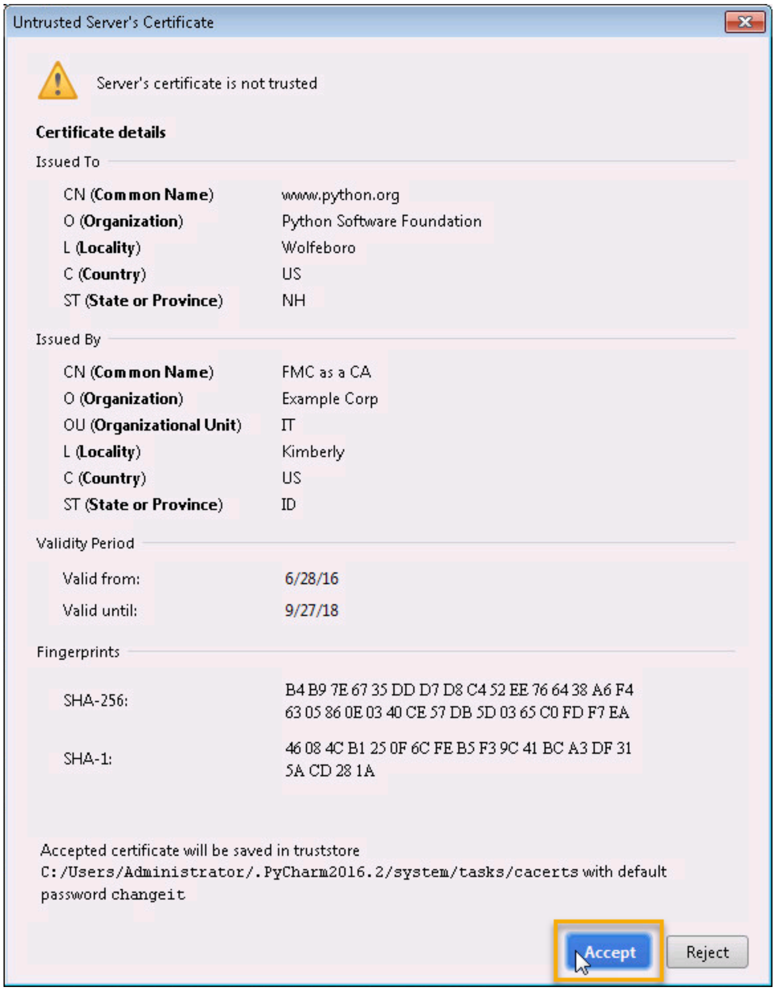
Figure 540. Open fmc.py



The following changes are by no means the “best practices” that a normal programmer would use. These changes are to get the script to run as quickly as possible to show you that it works. Typically, you would not want to statically assign the username and password in the file. Nor would you disable the certificate process.

15. I’m not sure what PyCharm is doing but **Accept** the certificates to continue.

Figure 541. Accept certificate again



Untrusted Server's Certificate

Server's certificate is not trusted

Certificate details

Issued To

CN (**Common Name**)	www.python.org
O (**Organization**)	Python Software Foundation
L (**Locality**)	Wolfeboro
C (**Country**)	US
ST (**State or Province**)	NH

Issued By

CN (**Common Name**)	FMC as a CA
O (**Organization**)	Example Corp
OU (**Organizational Unit**)	IT
L (**Locality**)	Kimberly
C (**Country**)	US
ST (**State or Province**)	ID

Validity Period

Valid from:	6/28/16
Valid until:	9/27/18

Fingerprints

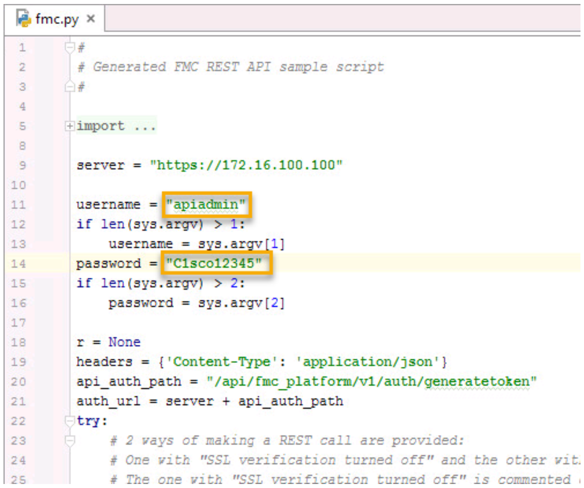
SHA-256:	B4 B9 7E 67 35 DD D7 D8 C4 52 EE 76 64 38 A6 F4 63 05 86 0E 03 40 CE 57 DB 5D 03 65 C0 FD F7 EA
SHA-1:	46 08 4C B1 25 0F 6C FE B5 F3 9C 41 BC A3 DF 31 5A CD 28 1A

Accepted certificate will be saved in truststore `C:/Users/Administrator/.PyCharm2016.2/system/tasks/cacerts` with default password `changeit`

16. Find the **username variable** and change its value to **apiadmin**. (Around line 11.)

17. Find the **password variable** and change its value to **C1sco12345**. (Around line 14.)

Figure 542. Set username/password in script

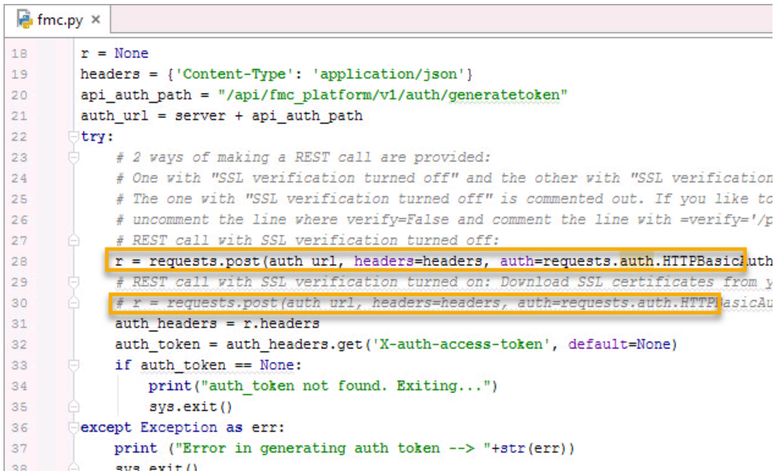


```
1   #
2   # Generated FMC REST API sample script
3   #
4
5   import ...
8
9   server = "https://172.16.100.100"
10
11  username = "apiadmin"
12  if len(sys.argv) > 1:
13      username = sys.argv[1]
14  password = "C1sco12345"
15  if len(sys.argv) > 2:
16      password = sys.argv[2]
17
18  r = None
19  headers = {'Content-Type': 'application/json'}
20  api_auth_path = "/api/fmc_platform/v1/auth/generatetoken"
21  auth_url = server + api_auth_path
22  try:
23      # 2 ways of making a REST call are provided:
24      # One with "SSL verification turned off" and the other wit
25      # The one with "SSL verification turned off" is commented
```

18. Find the **r = requests.post(auth_url, headers=headers,…** line. (Around line 30.) Comment out this line by putting a pound sign “**#**” in front of the r.

19. About 2 lines above this line there is another **# r= requests.post(…** line. (Around line 28.) It is currently commented out. **Remove** the **#** sign and extra whitespace between the # and r= from this line. This change will remove the requirement to have a certificate in order to communicate with the FMC via this script.

Figure 543. Turn off certs for this script

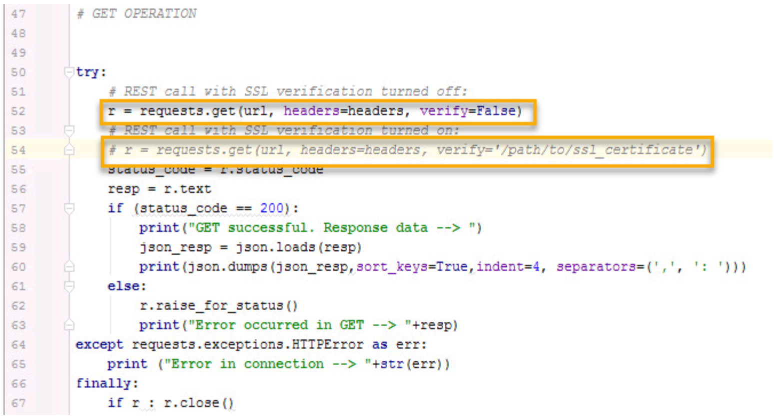


```
18  r = None
19  headers = {'Content-Type': 'application/json'}
20  api_auth_path = "/api/fmc_platform/v1/auth/generatetoken"
21  auth_url = server + api_auth_path
22  try:
23      # 2 ways of making a REST call are provided:
24      # One with "SSL verification turned off" and the other with "SSL verification
25      # The one with "SSL verification turned off" is commented out. If you like to
26      # uncomment the line where verify=False and comment the line with =verify='/p
27      # REST call with SSL verification turned off:
28      r = requests.post(auth_url, headers=headers, auth=requests.auth.HTTPBasicAuth
29      # REST call with SSL verification turned on: Download SSL certificates from y
30      # r = requests.post(auth_url, headers=headers, auth=requests.auth.HTTPBasicAu
31      auth_headers = r.headers
32      auth_token = auth_headers.get('X-auth-access-token', default=None)
33      if auth_token == None:
34          print("auth_token not found. Exiting...")
35          sys.exit()
36  except Exception as err:
37      print ("Error in generating auth token --> "+str(err))
38      sys.exit()
```

20. Around line 54 find the **r= requests.get(url,…** line and **comment it out**.

21. Around line 52 find the **# r = requests.get(url,…** line and **uncomment it**.

Figure 544. Turn off certs for this script, part 2

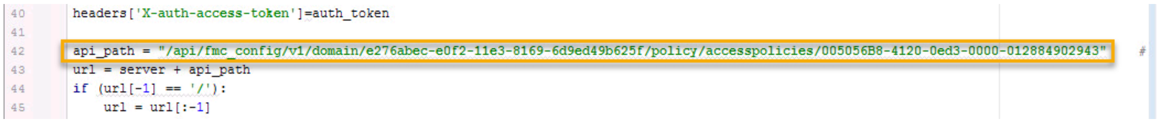


```
47  # GET OPERATION
48
49
50  try:
51      # REST call with SSL verification turned off:
52      r = requests.get(url, headers=headers, verify=False)
53      # REST call with SSL verification turned on:
54      # r = requests.get(url, headers=headers, verify='/path/to/ssl_certificate')
55      status_code = r.status_code
56      resp = r.text
57      if (status_code == 200):
58          print("GET successful. Response data --> ")
59          json_resp = json.loads(resp)
60          print(json.dumps(json_resp,sort_keys=True,indent=4, separators=(',', ': ')))
61      else:
62          r.raise_for_status()
63          print("Error occurred in GET --> "+resp)
64  except requests.exceptions.HTTPError as err:
65      print ("Error in connection --> "+str(err))
66  finally:
67      if r : r.close()
```

The python programming language is whitespace sensitive. Be sure that any leading whitespace on a line is removed so that the line starts at the same "space" as the line above it (unless you are starting a sub-section which would require the line above it to end in a ":" character).

22. This template is now ready for any GET type API call you'd like to make. Around line 42 there will be an **api_path variable** assignment.

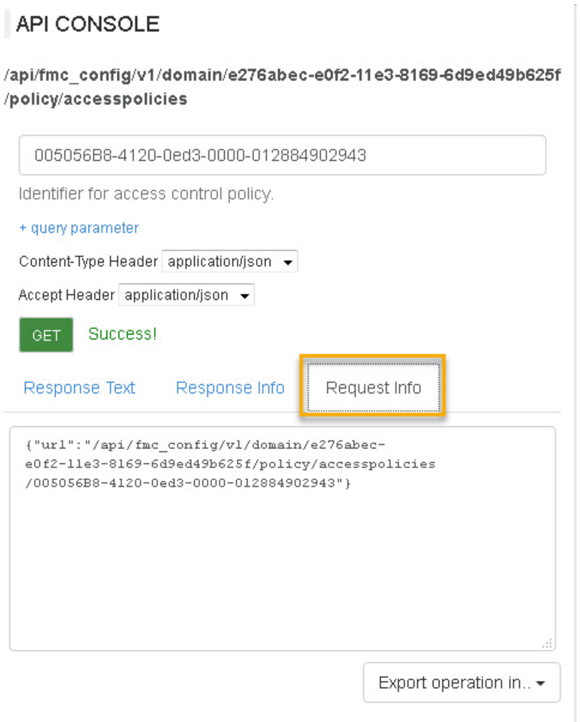
Figure 545. Finding the api_path variable



```
40  headers['X-auth-access-token']=auth_token
41
42  api_path = "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/005056B8-4120-0ed3-0000-012884902943"    #
43  url = server + api_path
44  if (url[-1] == '/'):
45      url = url[:-1]
```

23. Depending on where you “exported” this template this variable will be different. To find out what you should use for this variable return to the API Explorer webpage. In the rightmost column click the **Request Info tab**. This will display the URL that should be used in the api_path variable. **As it stands the api_path variable should be pre-assigned with your request for the HQ Policy Access Control Policy.**

Figure 546. Value for api_path variable



API CONSOLE

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f /policy/accesspolicies

005056B8-4120-0ed3-0000-012884902943

Identifier for access control policy.

Content-Type Header: application/json

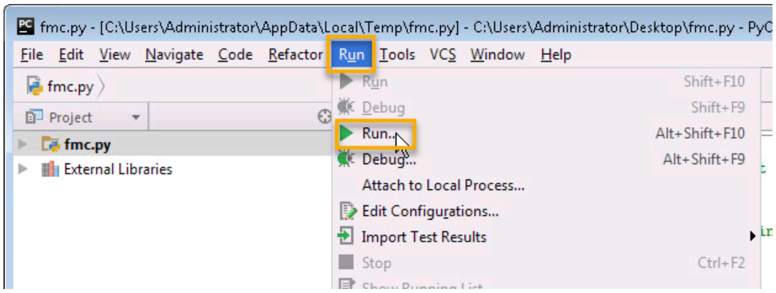
Accept Header: application/json

```
{"url":"/api/fmc_config/v1/domain/e276abec-
e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies
/005056B8-4120-0ed3-0000-012884902943"}
```

24. From the **PyCharm** menu select **Run > Run**.

Note: You may need to save your file before PyCharm allows you to run it.

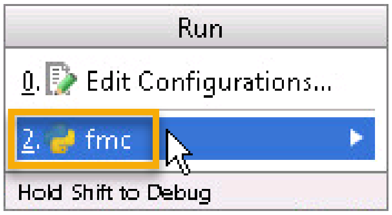
Figure 547. Select Run



fmc.py - [C:\Users\Administrator\AppData\Local\Temp\fmc.py] - C:\Users\Administrator\Desktop\fmc.py - PyC

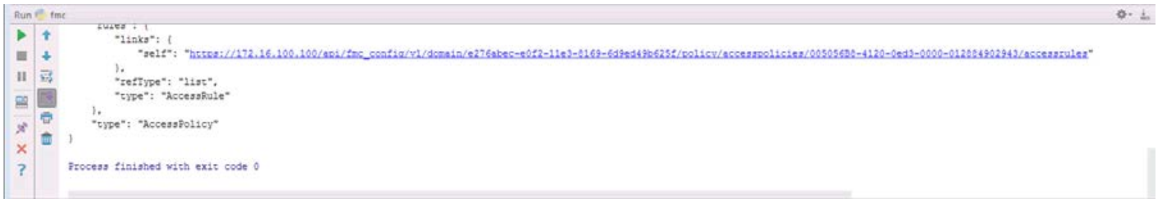
25. In the Run popup window select **fmc**.

Figure 548. Run fmc.py



26. The python script will now be run and the output will be displayed at the bottom of the PyCharm application.

Figure 549. Results of running fmc.py script



```
        "rules": {
            "links": {
                "self": "https://172.16.100.100/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/005056B8-4120-0ed3-0000-012884902943/accessrules"
            },
            "refType": "list",
            "type": "AccessRule"
        },
        "type": "AccessPolicy"
}

Process finished with exit code 0
```

Scenario Summary

Currently, in version 6.1 of the code, the API functions cannot program an FTD device. However, they can be used to query the FMC and gather information about how the manager has configured the FTD devices.

In this scenario you learned about the API Explorer website that comes with the FMC. You also learned a little about using the API GET action to query the FMC for information about how it is configured.

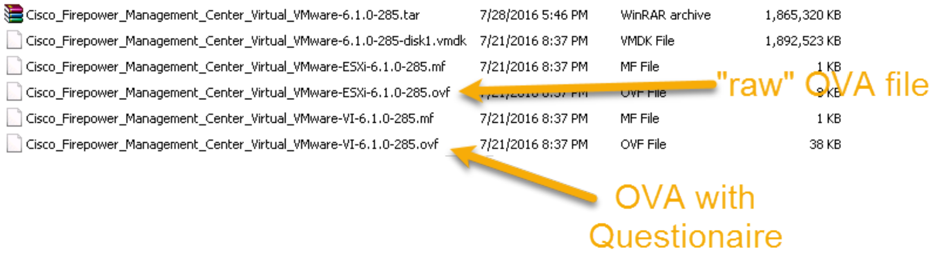
Congratulations, you have completed the whole lab!!!

Appendix A. FMC OVA Deployment

This appendix will show you how we deployed the hq-fmc VM in preparation for this lab. It also only shows how to deploy an FMC into a VMware environment.

There are two files you can use to deploy an OVA. One is the “raw” OVA file, which will need to be configured after its initial bootup is completed, and the other has a questionnaire that can be filled out prior/during deployment so that the device will be ready for use after its first bootup is completed. This appendix will show how to deploy the latter of these options.

Figure 1. Listing of files in OVA zip.



Cisco_Firepower_Management_Center_Virtual_VMware-6.1.0-285.tar	7/28/2016 5:46 PM	WinRAR archive	1,865,320 KB
Cisco_Firepower_Management_Center_Virtual_VMware-6.1.0-285-disk1.vmdk	7/21/2016 8:37 PM	VMDK File	1,892,523 KB
Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-6.1.0-285.mf	7/21/2016 8:37 PM	MF File	1 KB
Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-6.1.0-285.ovf	7/21/2016 8:37 PM	OVF File	9 KB
Cisco_Firepower_Management_Center_Virtual_VMware-VI-6.1.0-285.mf	7/21/2016 8:37 PM	MF File	1 KB
Cisco_Firepower_Management_Center_Virtual_VMware-VI-6.1.0-285.ovf	7/21/2016 8:37 PM	OVF File	38 KB

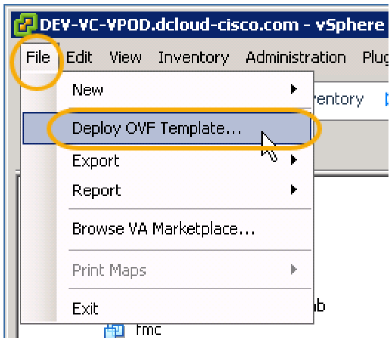
"raw" OVA file

OVA with Questionaire

The term OVA and OVF can be used interchangeably in this context. Essentially one term means that the virtual machine’s files are in a folder (like the screenshot shown above) while the other term means that the virtual machine’s “files” are all compressed in a single file.

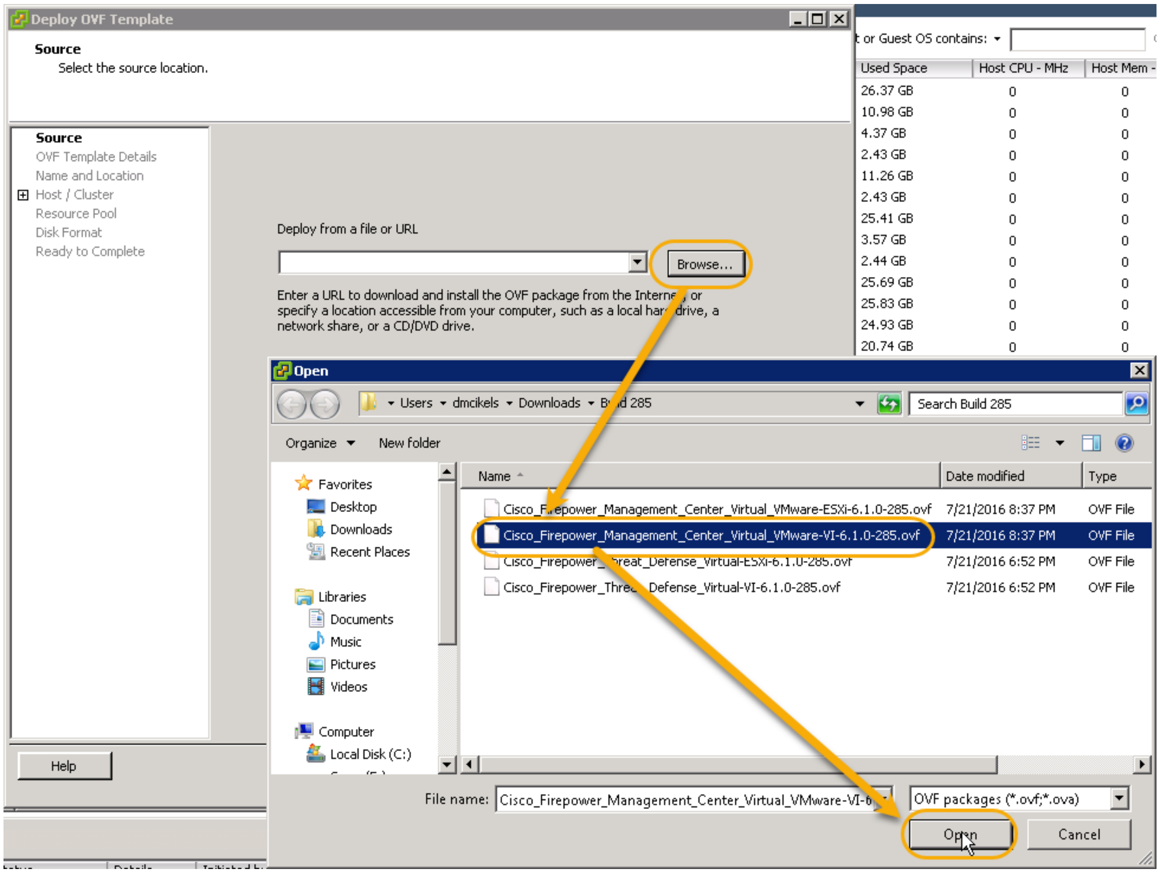
1. In VMware vCenter Client click **File > Deploy OVF Template**.

Figure 2. Deploy OVF Template



2. The Deploy OVF Template wizard will appear. Click **Browse** and navigate to the OVA file you want to deploy. **Select the file** and click **Open**.

Figure 3. Deploy OVF Template



Deploy OVF Template

Source

Select the source location.

- **Source**
- OVF Template Details
- Name and Location
- Host / Cluster
- Resource Pool
- Disk Format
- Ready to Complete

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

t or Guest OS contains:

Used Space	Host CPU - MHz	Host Mem -
26.37 GB	0	0
10.98 GB	0	0
4.37 GB	0	0
2.43 GB	0	0
11.26 GB	0	0
2.43 GB	0	0
25.41 GB	0	0
3.57 GB	0	0
2.44 GB	0	0
25.69 GB	0	0
25.83 GB	0	0
24.93 GB	0	0
20.74 GB	0	0

Open

Users ▸ dmckels ▸ Downloads ▸ Build 285

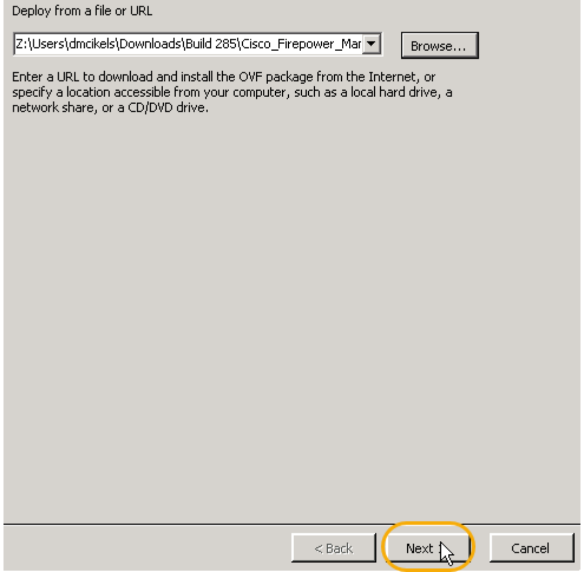
Name	Date modified	Type
Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-6.1.0-285.ovf	7/21/2016 8:37 PM	OVF File
Cisco_Firepower_Management_Center_Virtual_VMware-VI-6.1.0-285.ovf	7/21/2016 8:37 PM	OVF File
Cisco_Firepower_Threat_Defense_Virtual-ESXi-6.1.0-285.ovf	7/21/2016 6:52 PM	OVF File
Cisco_Firepower_Threat_Defense_Virtual-VI-6.1.0-285.ovf	7/21/2016 6:52 PM	OVF File

File name: Cisco_Firepower_Management_Center_Virtual_VMware-VI-6

OVF packages (*.ovf;*.ova)

3. With the proper file selected click **Next >**.

Figure 4. Select file



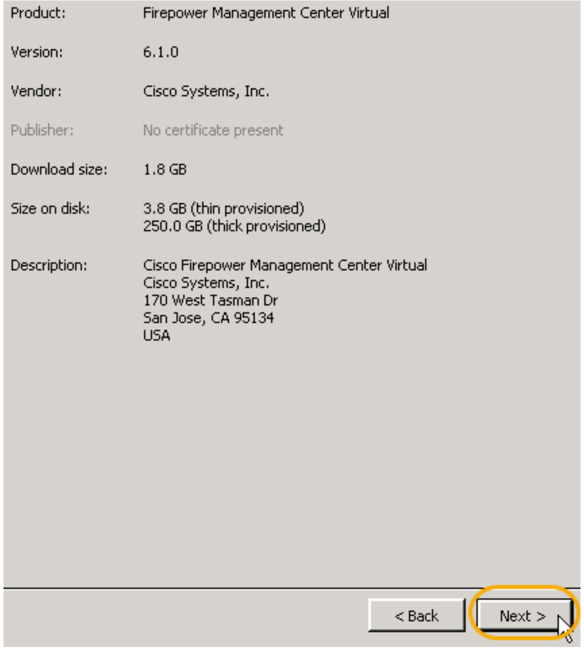
Deploy from a file or URL

Z:\Users\dmcikels\Downloads\Build 285\Cisco_Firepower_Mar

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

4. The next page will display some basic details of this OVA file. Click **Next >** to continue.

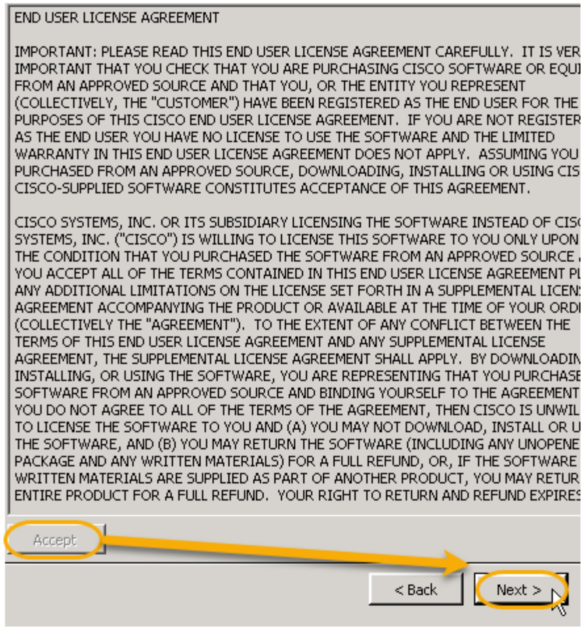
Figure 5. Click Next



Product:	Firepower Management Center Virtual
Version:	6.1.0
Vendor:	Cisco Systems, Inc.
Publisher:	No certificate present
Download size:	1.8 GB
Size on disk:	3.8 GB (thin provisioned) 250.0 GB (thick provisioned)
Description:	Cisco Firepower Management Center Virtual Cisco Systems, Inc. 170 West Tasman Dr San Jose, CA 95134 USA

5. **Accept** the EULA and click **Next >**.

Figure 6. Accept the EULA



END USER LICENSE AGREEMENT

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VER
IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUI
FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT
(COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE
PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTER
AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED
WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU
PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CIS
CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CIS
SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON
THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE
YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PL
ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICEN
AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORD
(COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE
TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE
AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADI
INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASE
SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT
YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWIL
TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR U
THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENE
PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE
WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETUR
ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES

The next few steps are variant depending on your VMware infrastructure (such as whether you have clustering enabled or not). So instead of showing step by step screenshots I'm going to just give you the steps until we are ready to start the freshly deployed VM.

6. Give the **VM a name**, specify which **folder** you wish to deploy it into and then click **Next >**.

7. If your VMware environment is configured for clustering you'll need to select the cluster to deploy to and click **Next >**. Otherwise you won't see this screen.

8. Specify which **ESX host** to deploy the VM to then click **Next >**.

9. Select the **datastore** to which the VM should be deployed to then click **Next >**.

10. Select how the disk should be formatted. The VMware environment I'm in doesn't allow anything other than Thin Provision. Click **Next >** to continue.

11. The management NIC of the FMC VM needs to be accessible. Select the appropriate VMware network for this NIC to attach to. Click **Next >** to continue.

12. Now you are to the “questionnaire” section. I used the following information to deploy the hq-fmc VM. Once I filled in fields I wanted I clicked **Next >** to continue.

    a. Admin Password: **Admin123**

    b. Hostname: **hq-fmc.example.lab**

    c. DNS1: **8.8.8.8**

    d. DNS Search Domains: **example.lab**

    e. IPv4 Configuration: **Manual**

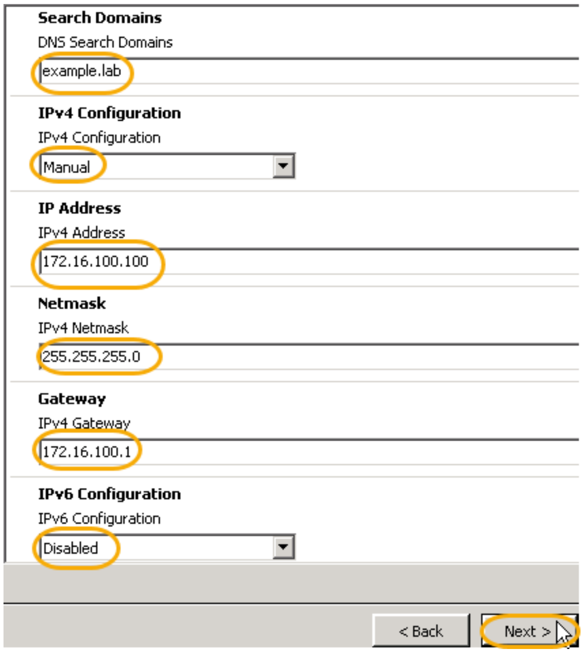
    f. IPv4 Address: **172.16.100.100**

    g. IPv4 Netmask: **255.255.255.0**

    h. IPv4 Gateway: **172.16.100.1**

    i. IPv6 Configuration: **Disabled**

Figure 7. Fill out Wizard



Search Domains

DNS Search Domains

example.lab

IPv4 Configuration

IPv4 Configuration

Manual

IP Address

IPv4 Address

172.16.100.100

Netmask

IPv4 Netmask

255.255.255.0

Gateway

IPv4 Gateway

172.16.100.1

IPv6 Configuration

IPv6 Configuration

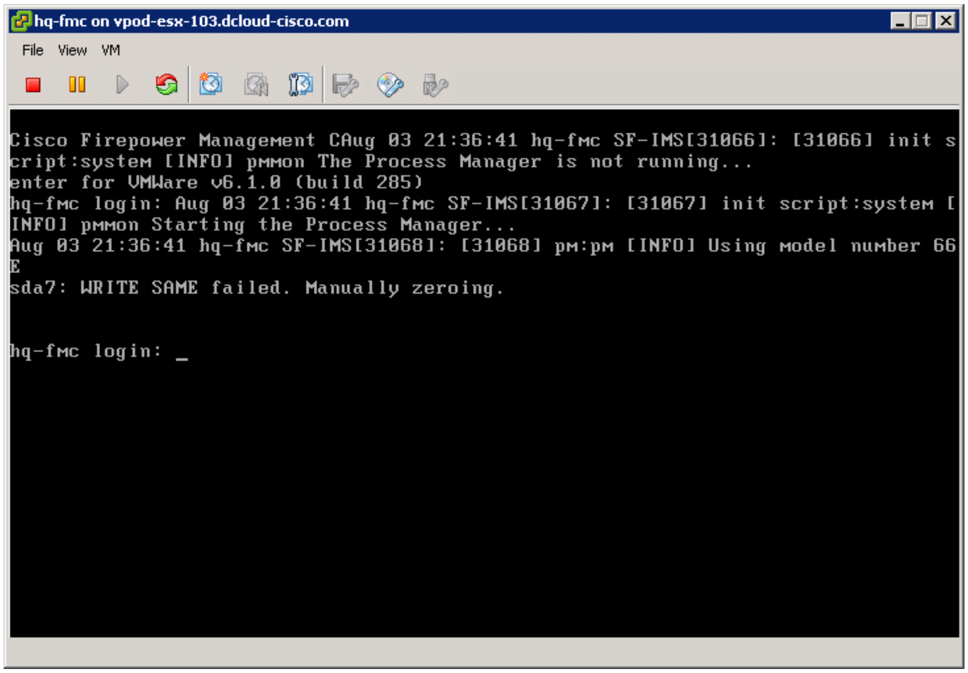
Disabled

If you use the other OVA file you’ll have to fill in this information either by using the “sudo configure-network” command once the VM is booted up or via its website using the default IP address of 192.168.45.45.

13. Click **Finish** on the final summary page to deploy this VM.

14. Once the VM has finished deploying start that VM and open the console to it. The initial bootup process will take about 30 minutes. You will know when it is done as you will be prompted to log in on the console.

Figure 8. Console of booted FMC



```
Cisco Firepower Management CAug 03 21:36:41 hq-fmc SF-IMS[31066]: [31066] init s
cript:system [INFO] pmmon The Process Manager is not running...
enter for VMWare v6.1.0 (build 285)
hq-fmc login: Aug 03 21:36:41 hq-fmc SF-IMS[31067]: [31067] init script:system [
INFO] pmmon Starting the Process Manager...
Aug 03 21:36:41 hq-fmc SF-IMS[31068]: [31068] pm:pm [INFO] Using model number 66
E
sda7: WRITE SAME failed. Manually zeroing.


hq-fmc login: _
```

Congratulations! You have deployed the FMC VM! Return to Scenario 1 to learn how to configure it from here.

Page intentionally left blank.

Appendix B. FTD OVA Deployment

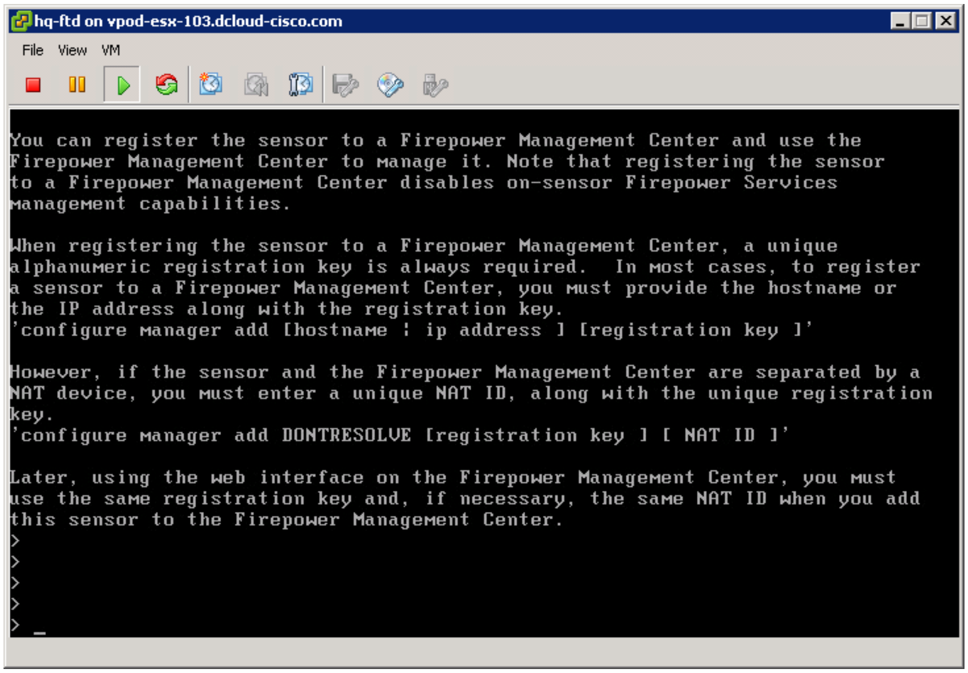
Deploying the FTD OVA file is very similar to how to deploy the FMC OVA as shown in Appendix A. Instead of duplicating all the steps I'll start with the questionnaire.

1. I filled in the following fields when deploying the hq-ftd FTD VM:
   a. Password: **Admin123**
   b. Hostname: **hq-ftd.example.lab**
   c. DNS1: **8.8.8.8**
   d. Search Domains: **example.lab**
   e. IPv4 Configuration: **Manual**
   f. IPv4 Address: **172.16.100.10** (the Management NIC's IP address)
   g. IPv4 Netmask: **255.255.255.0**
   h. IPv4 Gateway: **172.16.100.1**
   i. IPv6 Configuration: **Disabled**
   j. Firewall Mode: **routed**

This questionnaire also allows you to add the FMC registration information but I chose to leave that as part of the Scenario 2 tasks.

2. After filling in the above information and finishing the deployment of the VM I booted up the VM for the first time. The first time boot takes about 10 minutes and will allow you to log into the VM once it is complete. At this point you will be where Scenario 2 starts.

Figure 9. Booted FTD console



```
You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
>
>
>
> _
```

Page intentionally left blank.

Appendix C. Manage FTD with Firepower Device Manager

The Firepower Device Manager feature, which was released with the v6.1 code, is not available for virtual machine deployments of FTDs. So, instead of not showing it at all I used an ASA5516-X and "deployed" a version of the remote2-ftd FTD to show you what it entails.

Though this appendix is worded to have you build this out yourself these steps won't work in this lab since all your FTD devices are virtual machines.

Remote2-FTD Management Network Setup

Before you can use the Firepower Device Manager you need to get the Management interface configured. Like the previous FTD initial deployments you need to access the CLI and go through the setup wizard. Use the following information to fill out the wizard's questionnaire:

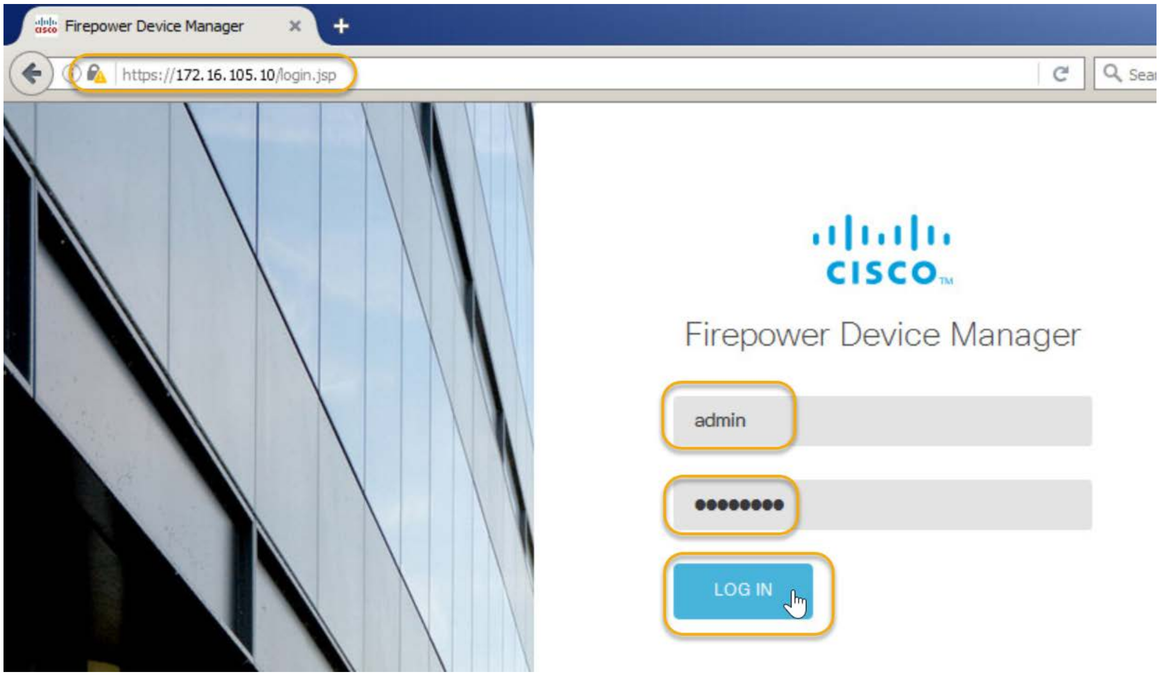
1. Log in as **admin**/**Admin123**
2. Press **Enter** to view the EULA, use the **Spacebar** to quickly scroll through and then accept the EULA by typing **yes** and pressing **Enter**.
3. You'll be dropped into the setup wizard.
    a. Set the password to **Admin123**
    b. Select **y** for configuring IPv4.
    c. Select **n** for configuring IPv6.
    d. Select **manual** for IPv4 addressing.
    e. Set the management interface IP address: **172.16.105.10**
    f. Set the subnet mask: **255.255.255.0**
    g. Set the IPv4 default gateway: **172.16.105.1**
    h. Set the FQDN: **remote2-ftd.example.lab**
    i. Set the DNS servers: **8.8.8.8**
    j. Set the search domains: **none**
    k. Manage the device locally? **Yes**
    l. Configure the firewall mode: **routed**

Remote2-FTD Data Plane Configuration

Now that the FTD device's management interface is configured you can access the Firepower Device Manager web page by accessing **https://172.16.105.10** from remote2_wkst.

4. Log in using **admin**/**Admin123**.

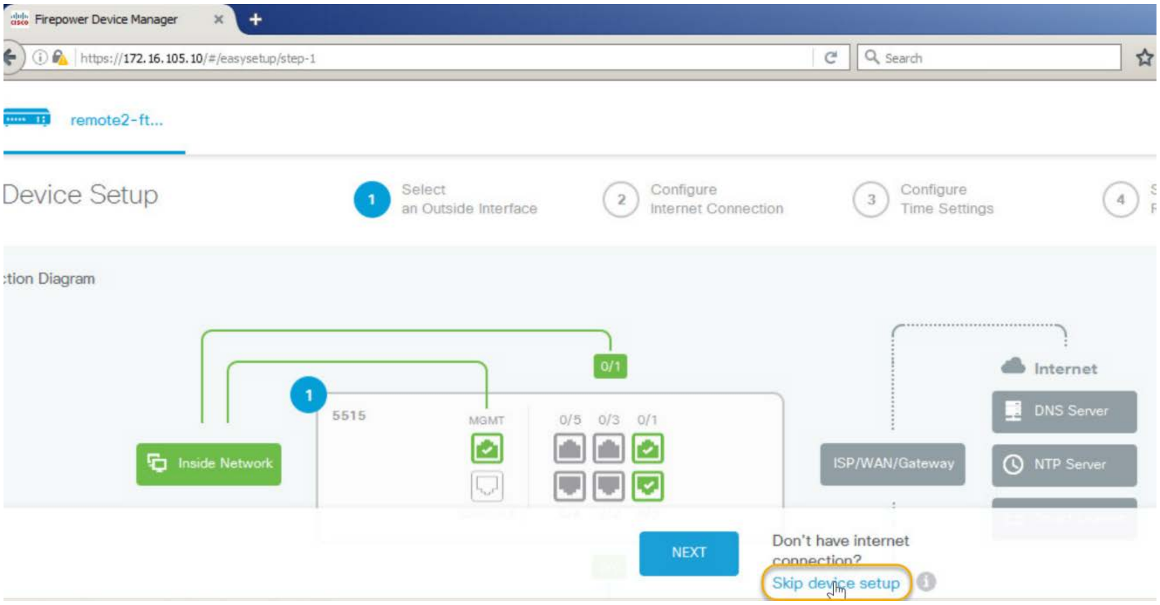
Figure 10. Initial Firepower Device Manager Page



The initial screen shows a "wiring diagram" of how the FTD device is cabled and to which zone each cable is connected. By default, the Mgmt and 0/1 interfaces are connected to the "inside Network" and interface 0/0 is connected to the "Outside Network". If you were able to cable the device such that 0/1 is "Inside" and 0/0 is "Outside" then you could use the setup wizard steps shown on the bottom of this page. There are a lot of assumptions (such as using DHCP for the outside NIC and 192.168.45.0/24 for the inside LAN) but using the wizard would certainly be the fastest method for configuring the basic needs for firewalling this location. In your case 0/0 is cabled to be in the "Inside" zone while 0/1 is cabled to the "Outside" zone and you aren't using the 192.168.45.0/24 IP range so you need to do some manual configuration.

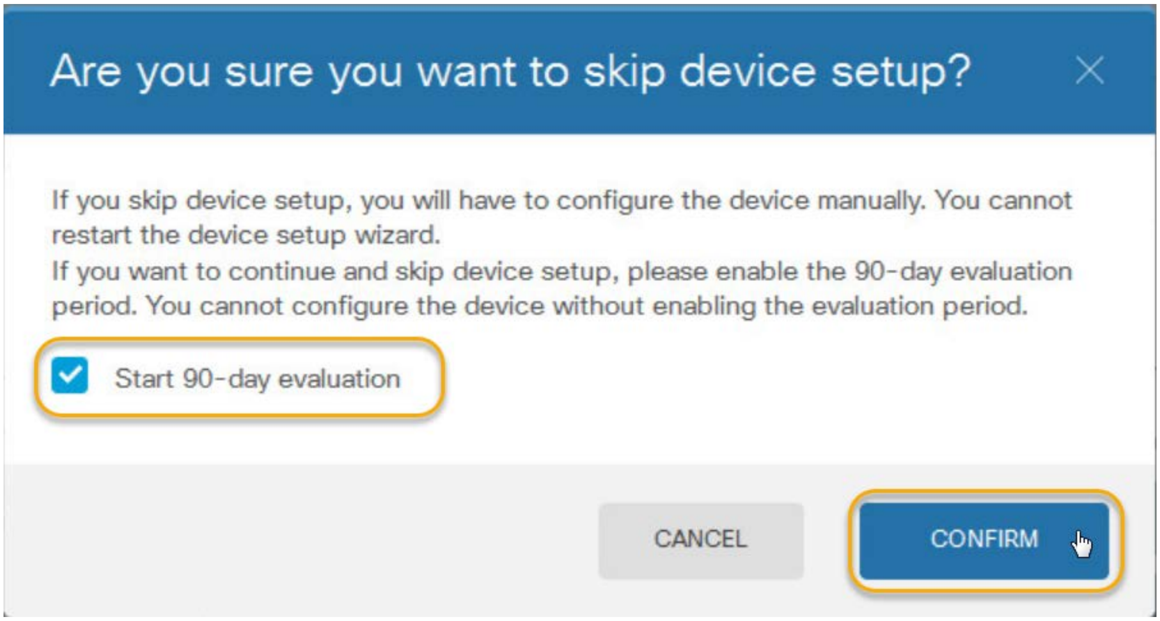
5. Click **Skip device setup** link.

Figure 11. Dashboard Page



6. In the popup window confirming that you want to skip the device setup click the box to **Start the 90-day evaluation** and then click **Confirm**.

Figure 12. Enable Eval License



Are you sure you want to skip device setup?

If you skip device setup, you will have to configure the device manually. You cannot restart the device setup wizard.

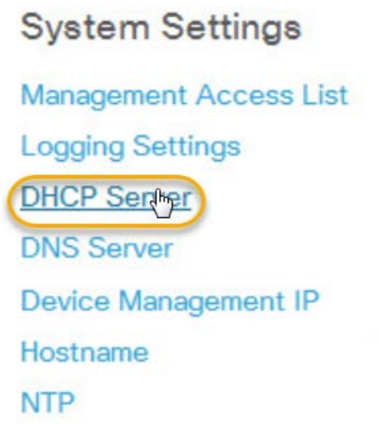
If you want to continue and skip device setup, please enable the 90-day evaluation period. You cannot configure the device without enabling the evaluation period.

☑ Start 90-day evaluation

7. The page, called the device dashboard, has changed a bit. The cabling diagram is still there but now you have several configuration menus as well.

8. Anyone remember having issues with trying to set up your “Inside” and “Outside” interfaces via ASDM in the ASA when you wanted to use a different IP range than the one given in the default configuration? Well, some of that headache still remains. Since you have opted to not use the default IP addressing scheme nor the default interface configuration you need to “fix” a few things before you can progress with your configuration. Namely you need to disable the DHCP server and delete the DHCP address pool. From the **System Settings menu** (along the right side of the web page) click **DHCP Server**.

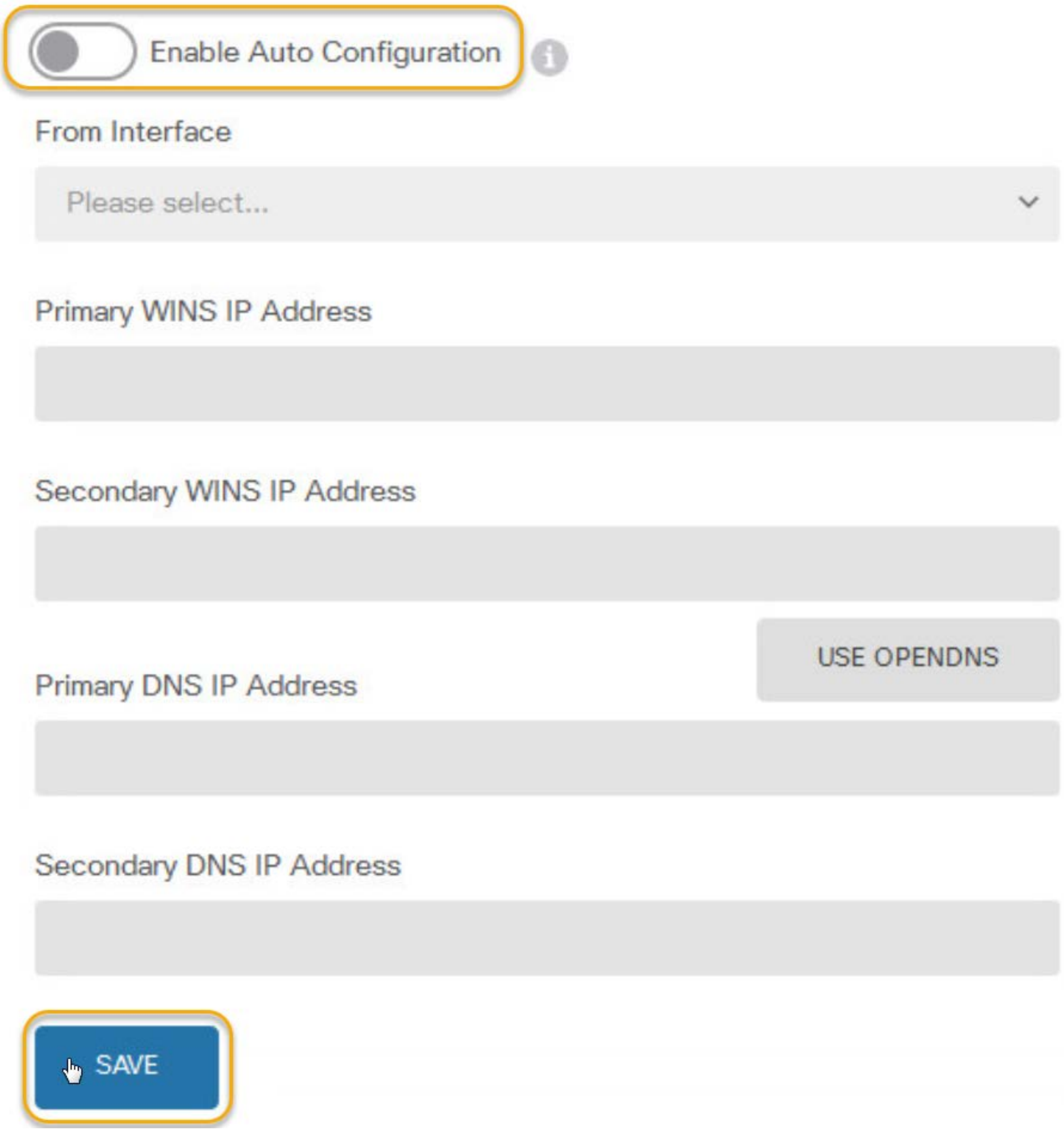
Figure 13. DHCP Server Link



9. Click the **toggle icon** for **Enable Auto Configuration** so that it greys out.

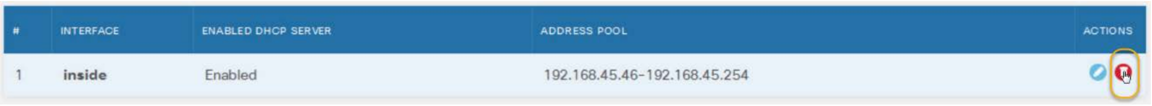
10. Click **Save**.

Figure 14. Disable DHCP



11. Scroll down and **delete the address pool** by hovering over that row and then along the right side of that row click the **red trash can icon**.

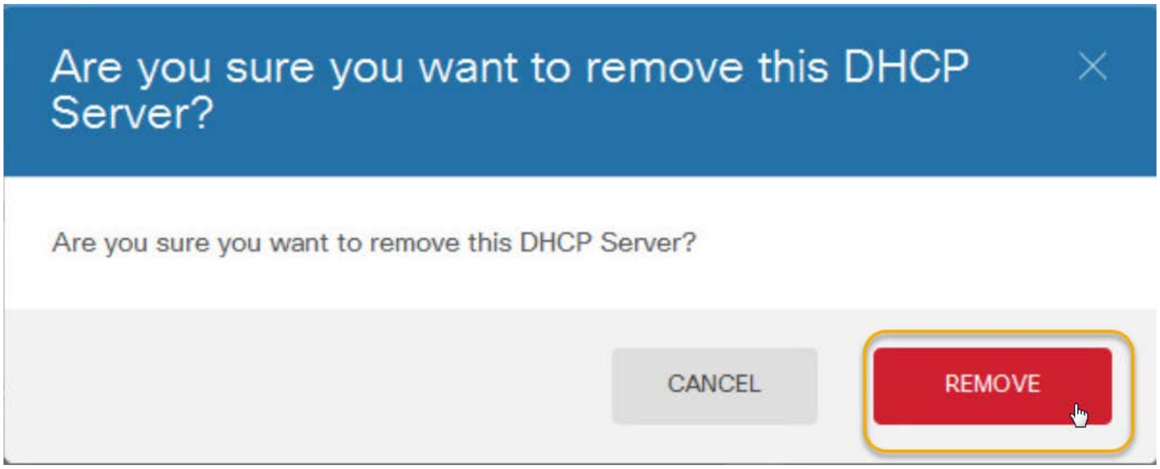
Figure 15. Delete DHCP Pool



#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL	ACTIONS
1	**inside**	Enabled	192.168.45.46-192.168.45.254	

12. Click **Remove** from the popup window.

Figure 16. Confirm removal of DHCP Pool

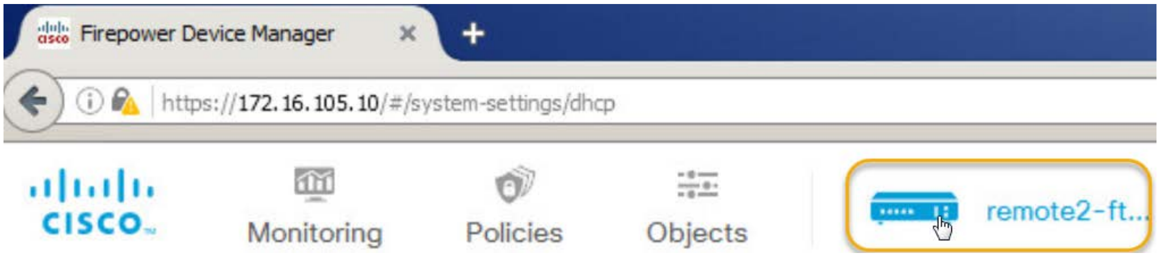


Are you sure you want to remove this DHCP Server?

Are you sure you want to remove this DHCP Server?

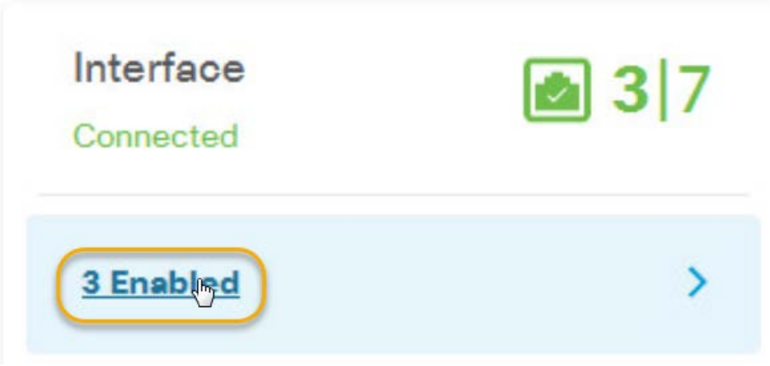
13. With the DHCP server configuration disabled and the DHCP address pool deleted you can now configure your interfaces in the right order and with the correct IP addressing. Return to the dashboard page by clicking the **remote2-ftd** menu button along the top of the page.

Figure 17. Return to the Dashboard



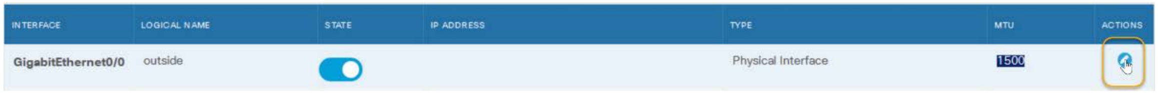
14. In the Interface section of the dashboard lick the **3 Enabled** link.

Figure 18. Click link to edit interfaces



15. When you hover over an interface its row changes color and a round pencil icon will appear on the far right of that row. Click the **pencil icon** for the **GigabitEthernet0/0** row.

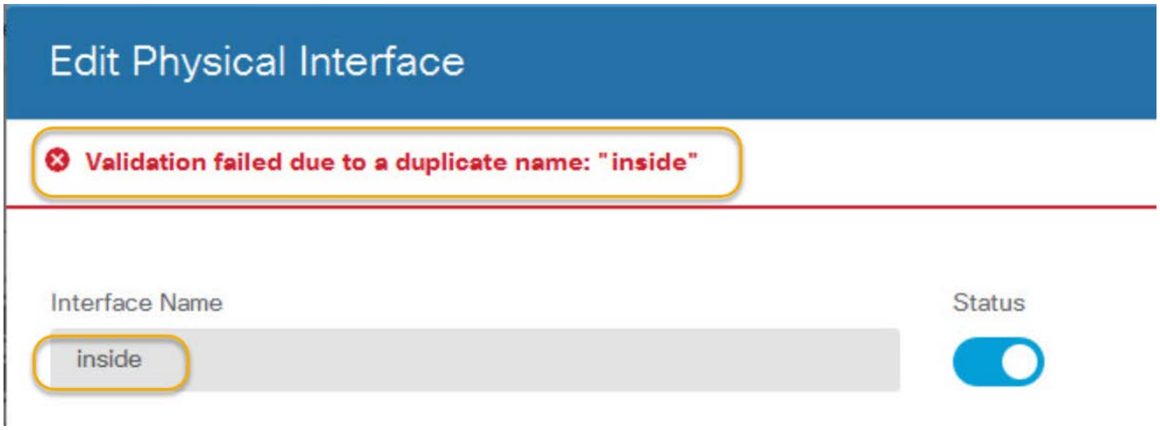
Figure 19. Edit g0/0



INTERFACE	LOGICAL NAME	STATE	IP ADDRESS	TYPE	MTU	ACTIONS
GigabitEthernet0/0	outside	●		Physical Interface	1500	✎

Note: This step will fail but you are doing this to show something. Change the Interface Name to inside and click Save. Notice the corresponding error message: Validation failed due to a duplicate name: “inside”. -- Each interface must have a unique name.

Figure 20. Attempt to rename the interface



Edit Physical Interface

Validation failed due to a duplicate name: "inside"

Interface Name: inside

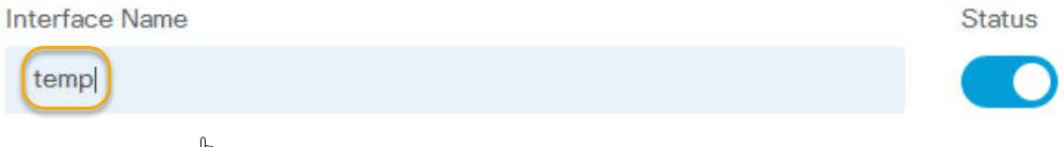
Status: ●

Note: I tried to be sneaky and use “Inside”, notice the capital “I”, and I got a different kind of warning telling me that an interface name cannot contain capitalization but that special characters “+”, “.”, “_”, and “-“ are permitted.

Also note that these are just the names of the interfaces and NOT the security zones. You will associate these named interfaces to zones later in this section.

16. Since “inside” and “outside” names are already taken change this interface’s name to **temp** and click **Save**. You will return to this interface in a moment.

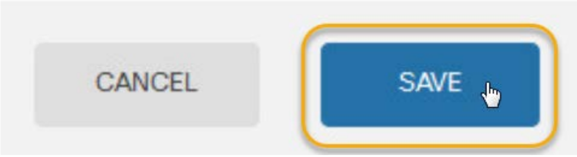
Figure 21. Rename the interface



Interface Name

temp

Figure 22. Click Save



17. Click the **pencil icon** for the **GigabitEthernet0/1** row and then use the following items to fill out the needed information:

    a. Interface Name: **outside**

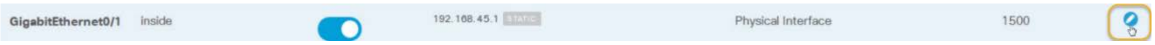
    b. IPv4 Address type: **Static**

    c. IPv4 Address: **198.18.3.2**

    d. IPv4 Subnet Mask: **255.255.255.0**

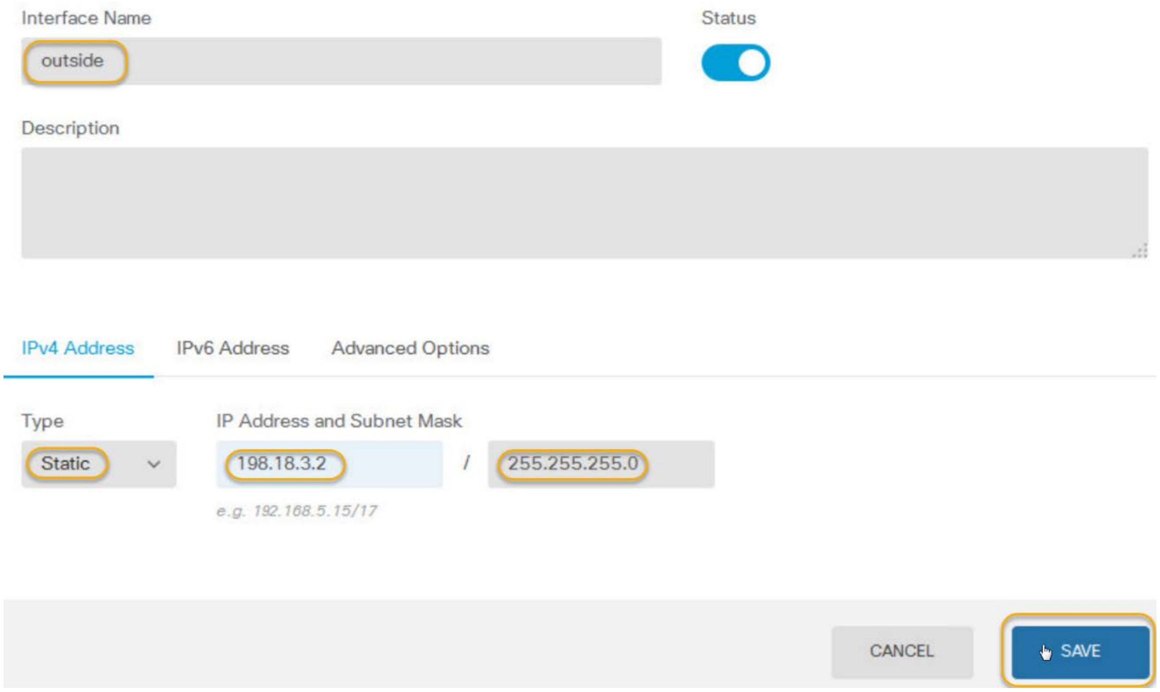
    e. Click **Save**.

Figure 23. Edit g0/1



GigabitEthernet0/1	inside	192.168.45.1 STATIC	Physical Interface	1500	

Figure 24. Configure g0/1



Interface Name: outside

Status

Description

Type: Static

IP Address and Subnet Mask: 198.18.3.2 / 255.255.255.0

e.g. 192.168.5.15/17

18. Now you can return to the GigabitEthernet0/0 interface and configure it correctly. Click the **pencil icon** for the **GigabitEthernet0/0** row. And use the following to fill out the needed information:

    a. Interface Name: **inside**

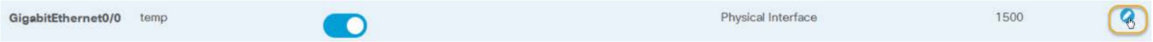
    b. IPv4 Address type: **Static**

    c. IPv4 Address: **172.16.105.1**

    d. IPv4 Subnet Mask: **255.255.255.0**

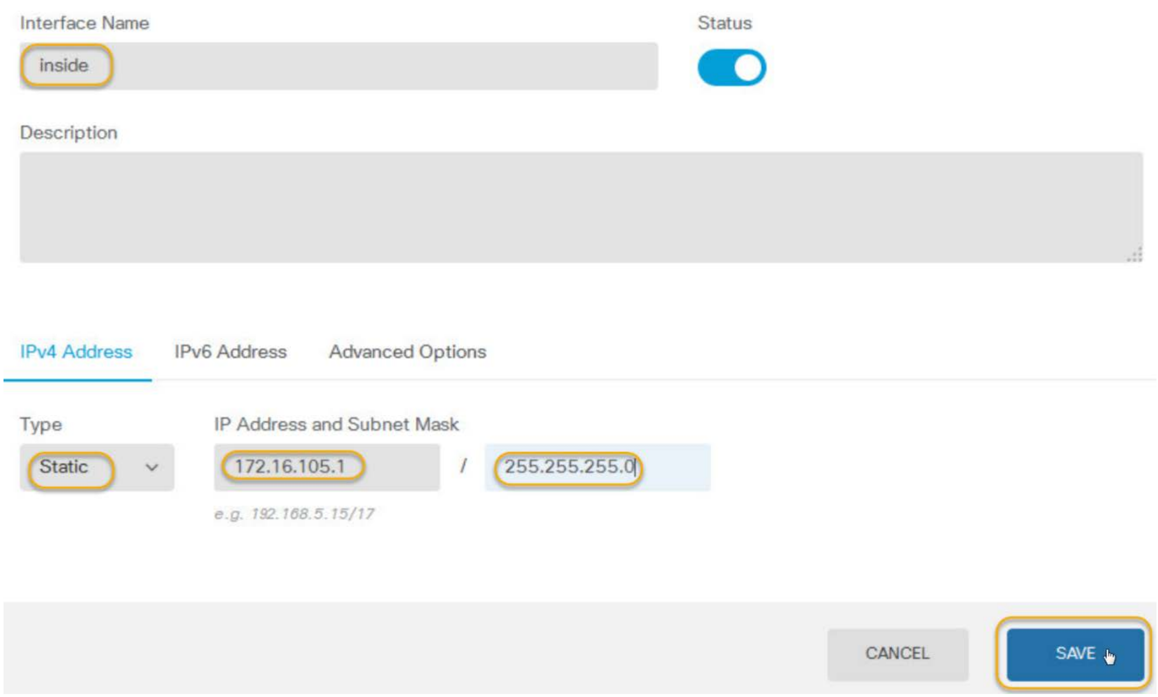
    e. Click **Save**.

Figure 25. Edit g0/0



GigabitEthernet0/0	temp	Physical Interface	1500

Figure 26. Configure g0/0



Interface Name: inside

Status

Description

IPv4 Address | IPv6 Address | Advanced Options

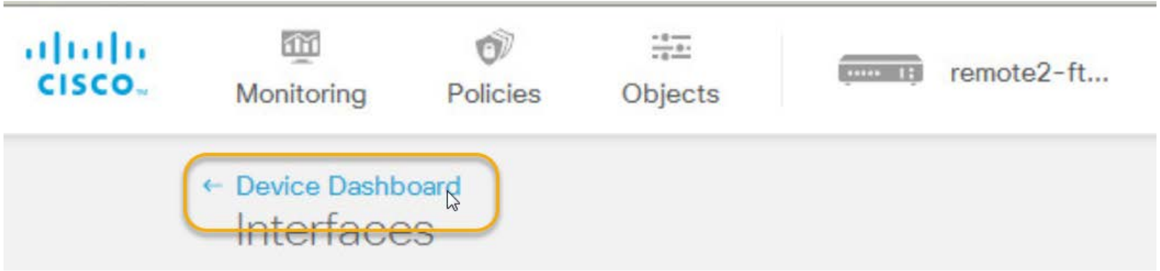
Type: Static

IP Address and Subnet Mask: 172.16.105.1 / 255.255.255.0

e.g. 192.168.5.15/17

19. Return to the Dashboard page by clicking the **Device Dashboard** link in the upper-left section of this page or by clicking the remote2-ftd menu item along the top of the page.

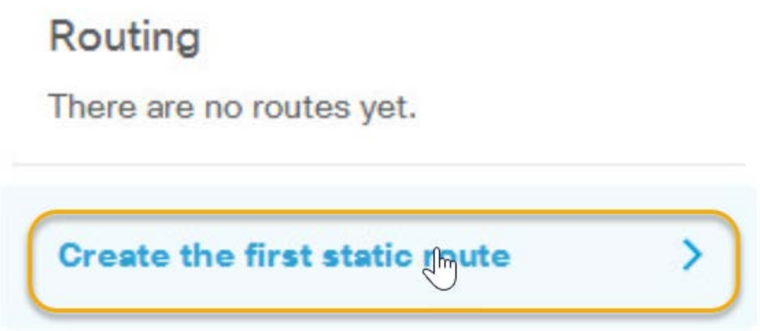
Figure 27. Return to the Dashboard



20. Notice that the Connection Diagram now reflects your cabling arrangement.

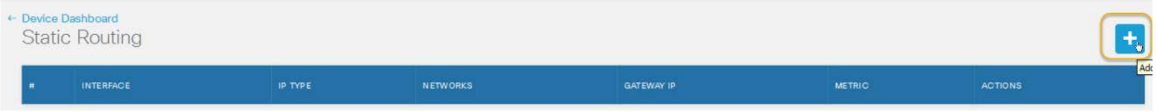
21. In the Routing section click the **Create the first static route** link.

Figure 28. Create a static route



22. Click the **plus icon** in the upper right corner of this page and then use the following to fill out the needed information:

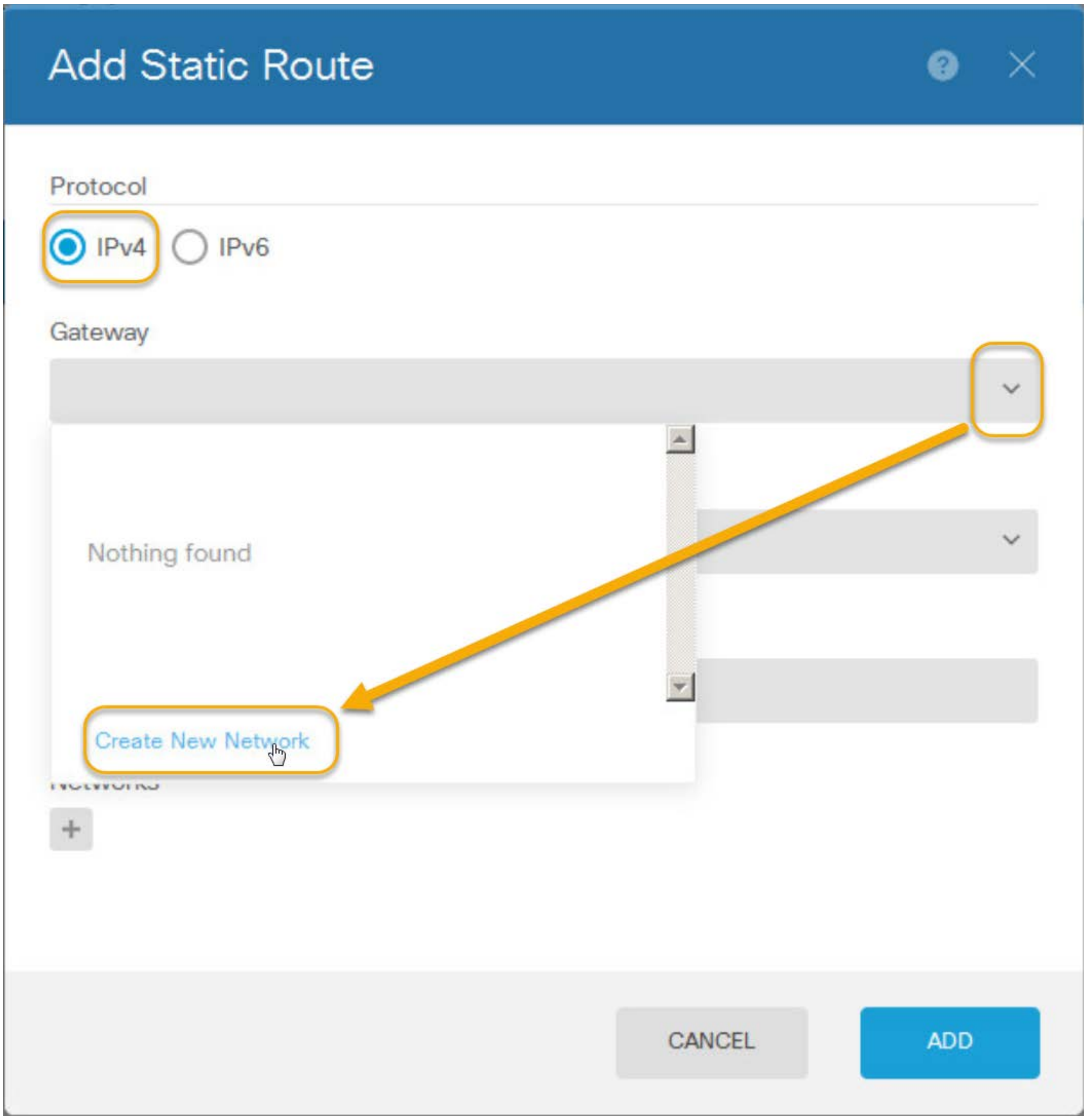
Figure 29. Add a route



a. Select **IPv4**.

b. From the dropdown menu for Gateway select **Create New Network**.

Figure 30. Configure the static route



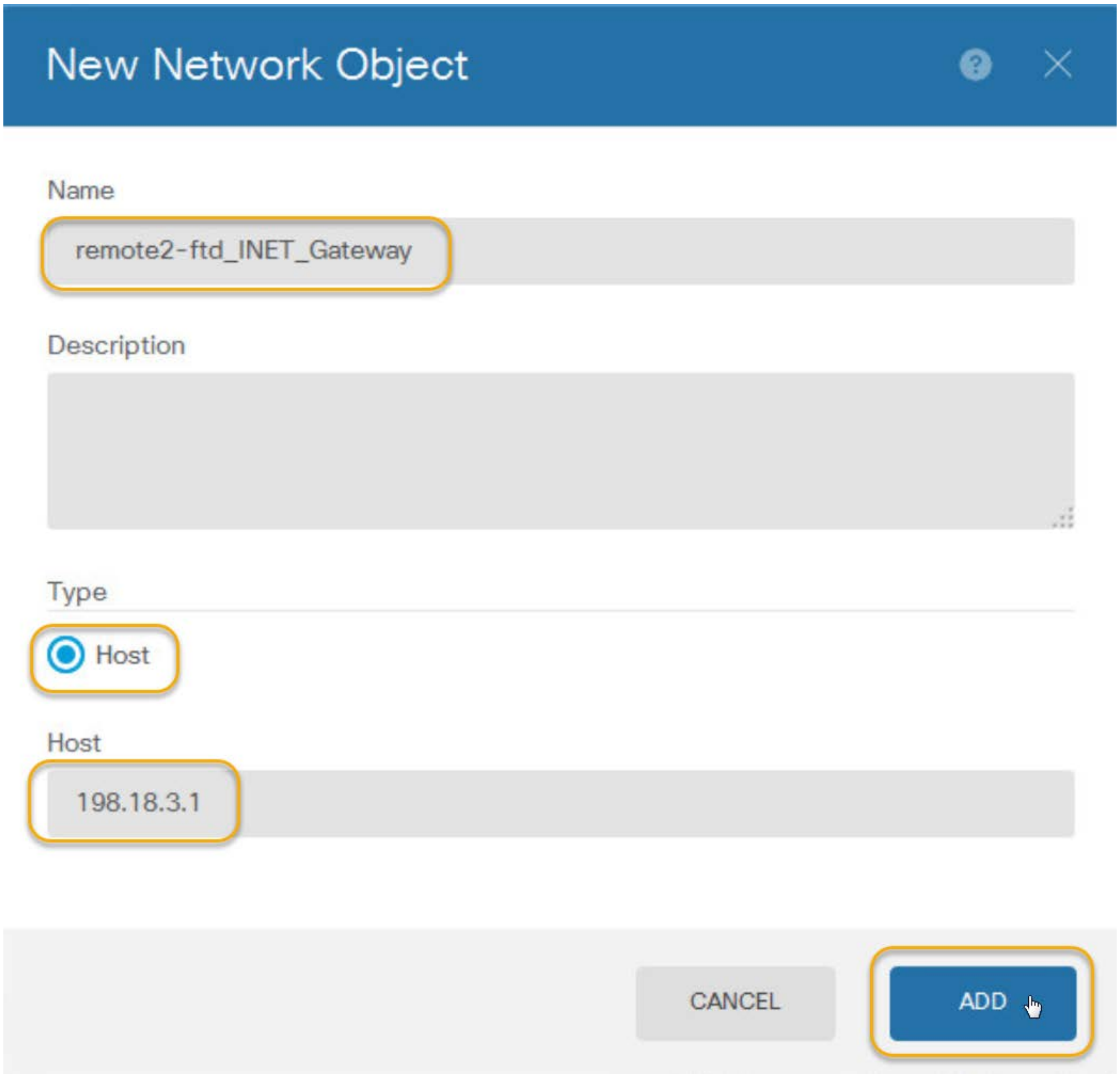
c. Use the following to fill out the needed information for the New Network Object popup window:

   i. Name: **remote2-ftd_INET_Gateway**

   ii. Host: **198.18.3.1**

   iii. Click **Add**.

Figure 31. Create a network object



New Network Object

Name: remote2-ftd_INET_Gateway

Description:

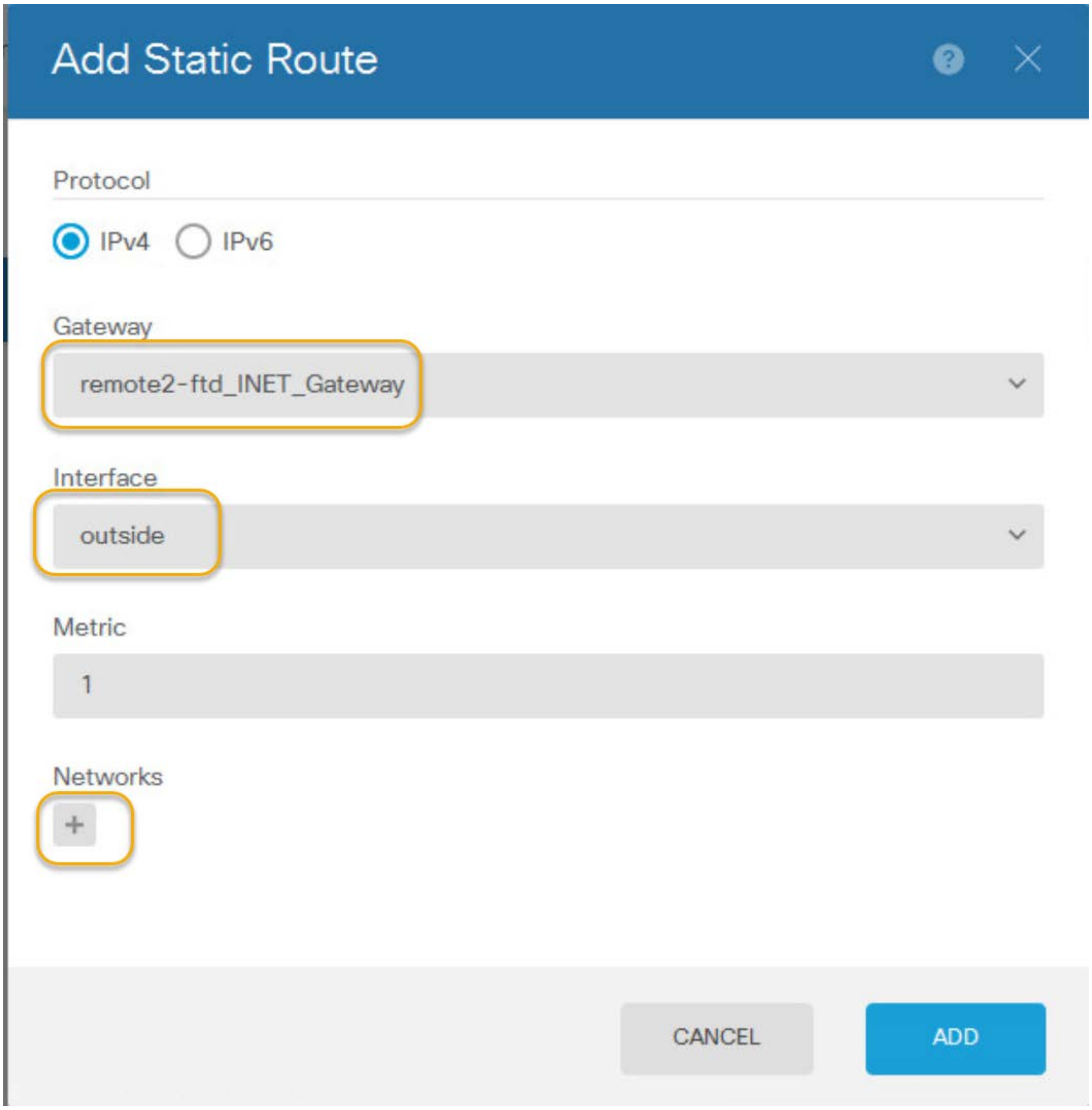
Type: ● Host

Host: 198.18.3.1

d. Gateway: **remote2-ftd_INET_Gateway**

e. Interface: **outside**

Figure 32. Continue filling out static route



Add Static Route

Protocol

● IPv4 ○ IPv6

Gateway

remote2-ftd_INET_Gateway

Interface

outside

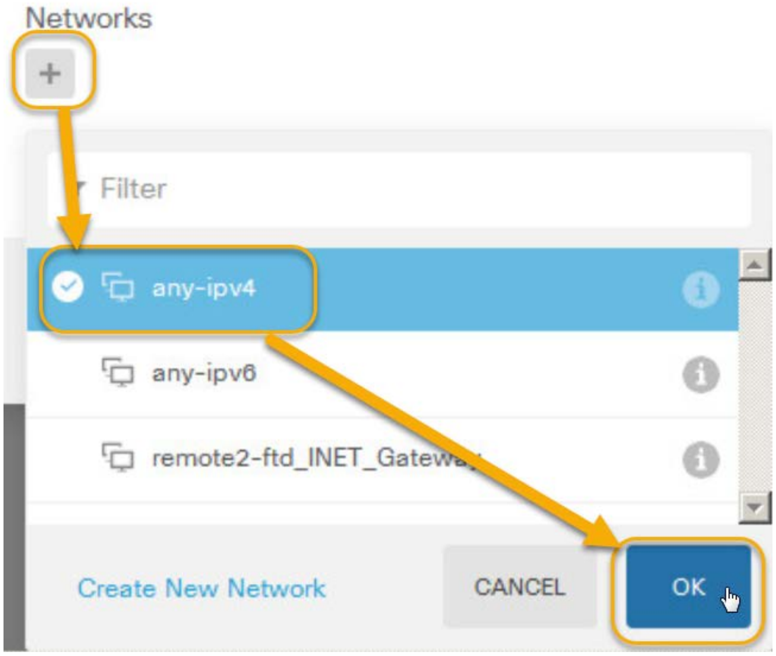
Metric

1

Networks

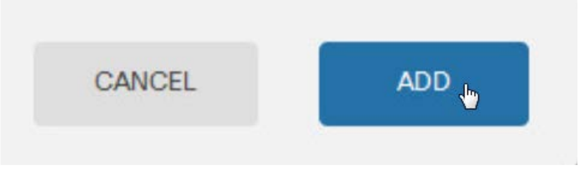
f. Network: Click the **plus icon** and select **any-ipv4** from the list and click **OK**.

Figure 33. Add Network to route



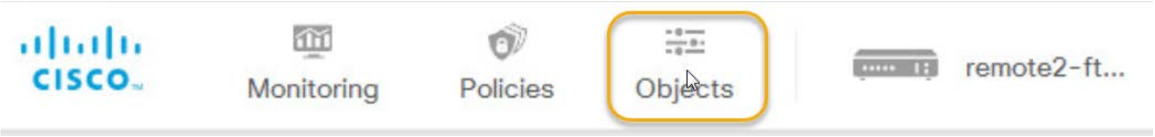
g. Click ADD to create this static route.

Figure 34. Click Add



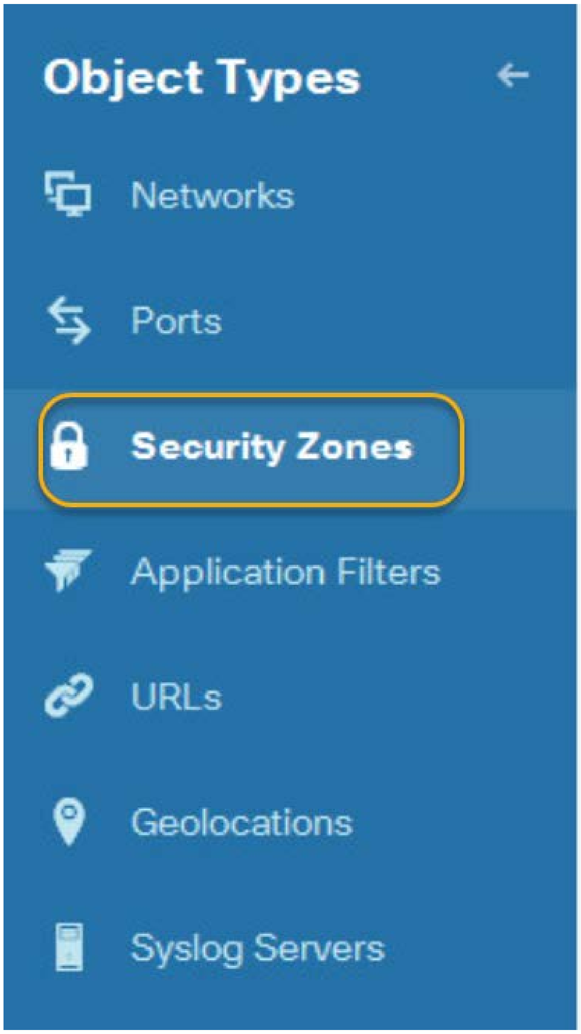
23. Now that the IP addressing and routing is configured it is time to associate these interfaces with the security zones. Click the **Objects** menu icon from along the top of the page.

Figure 35. Go to object page



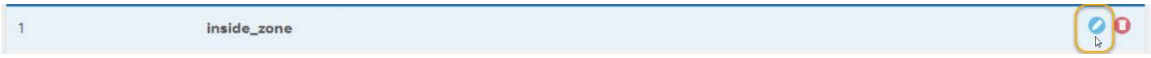
24. From the Object Types menu along the left of the page select **Security Zones**.

Figure 36. Select Security Zones



25. Hover over the **inside_zone** row and click the **pencil icon** for that row.

Figure 37. Edit the inside_zone

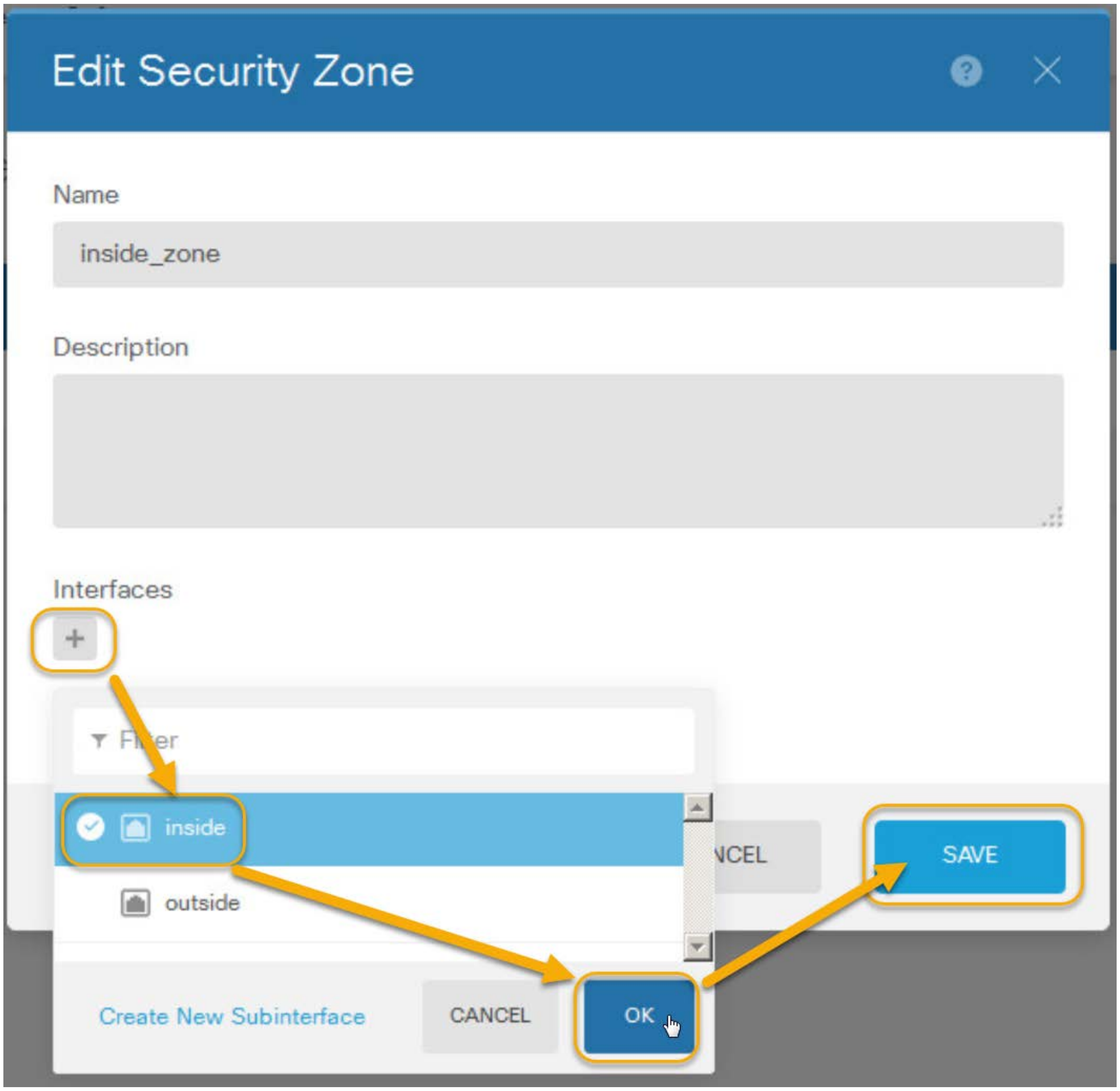

1 inside_zone

a. Click the **plus icon** in the Interfaces section and select the **inside** interface.

b. Click **OK** to add the **inside** interface to the inside_zone.

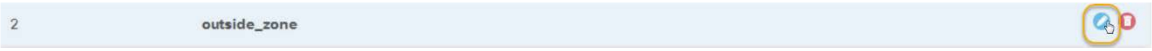
c. Click **SAVE**.

Figure 38. Configure the inside_zone



26. Hover over the **outside_zone** row and click the **pencil icon** for that row.

Figure 39. Edit the outside_zone

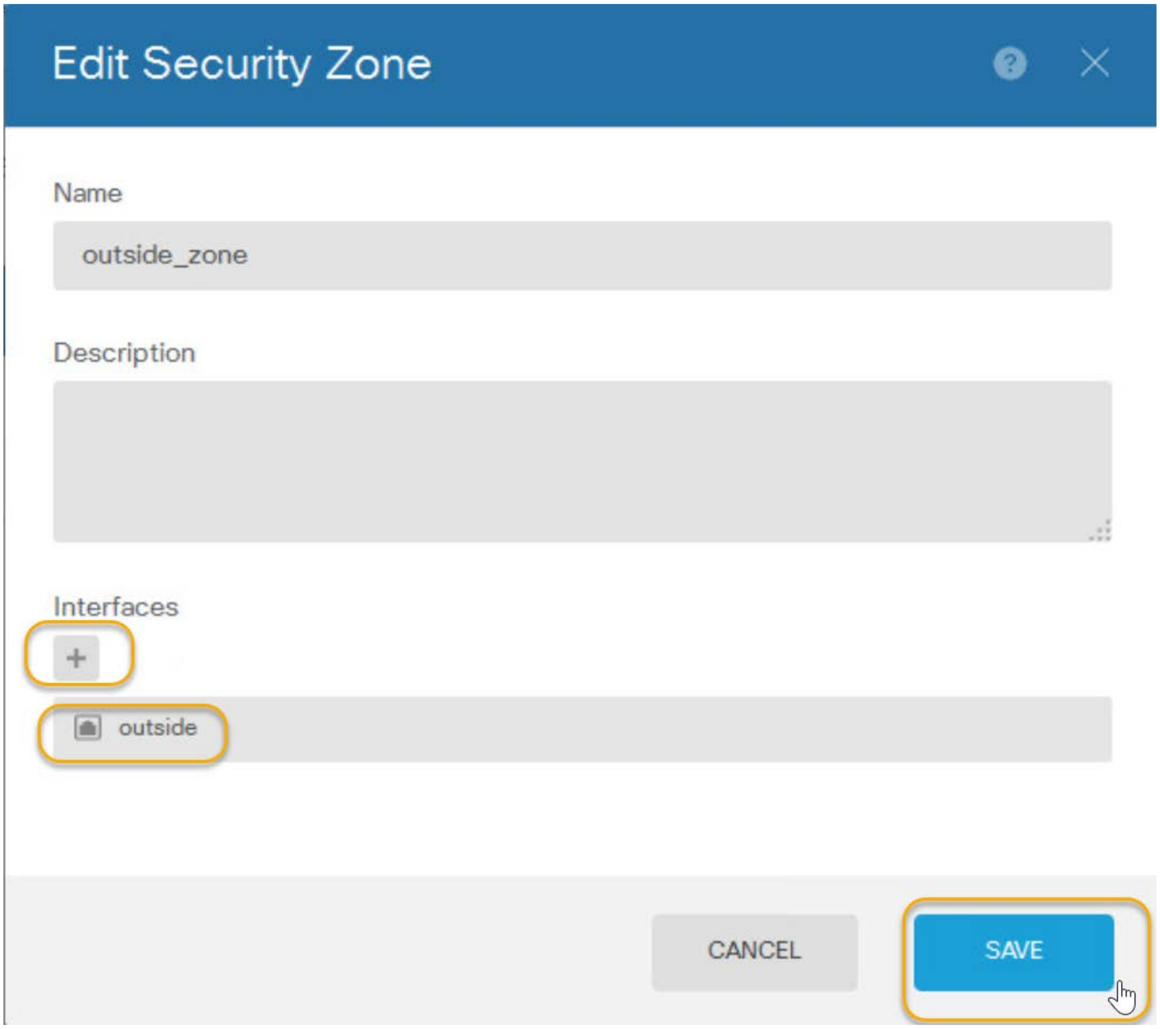


a. Click the **plus icon** in the Interfaces section and select the **outside** interface.

b. Click **OK**.

c. Click **SAVE**.

Figure 40. Configure the outside_zone



Edit Security Zone

Name

outside_zone

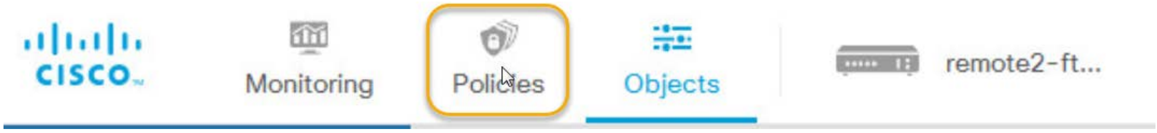
Description

Interfaces

outside

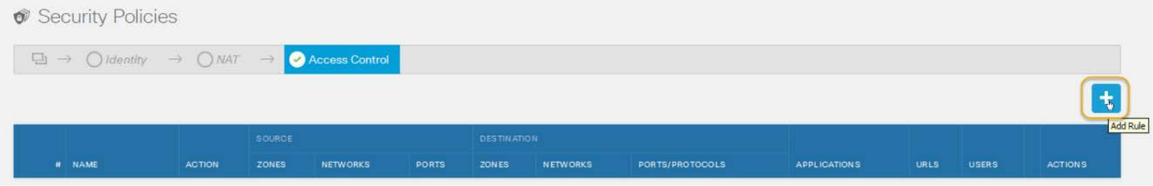
27. To allow traffic to flow through this FTD you need to configure NAT and your base Access Control Policy. Click the **Policies** menu item from along the top of the page.

Figure 41. Click the Policies link



28. Click the **plus icon** along the right side of this page to create a new **Access Control Policy**. Use the following to fill out the needed information:

Figure 42. Click the Access Control link

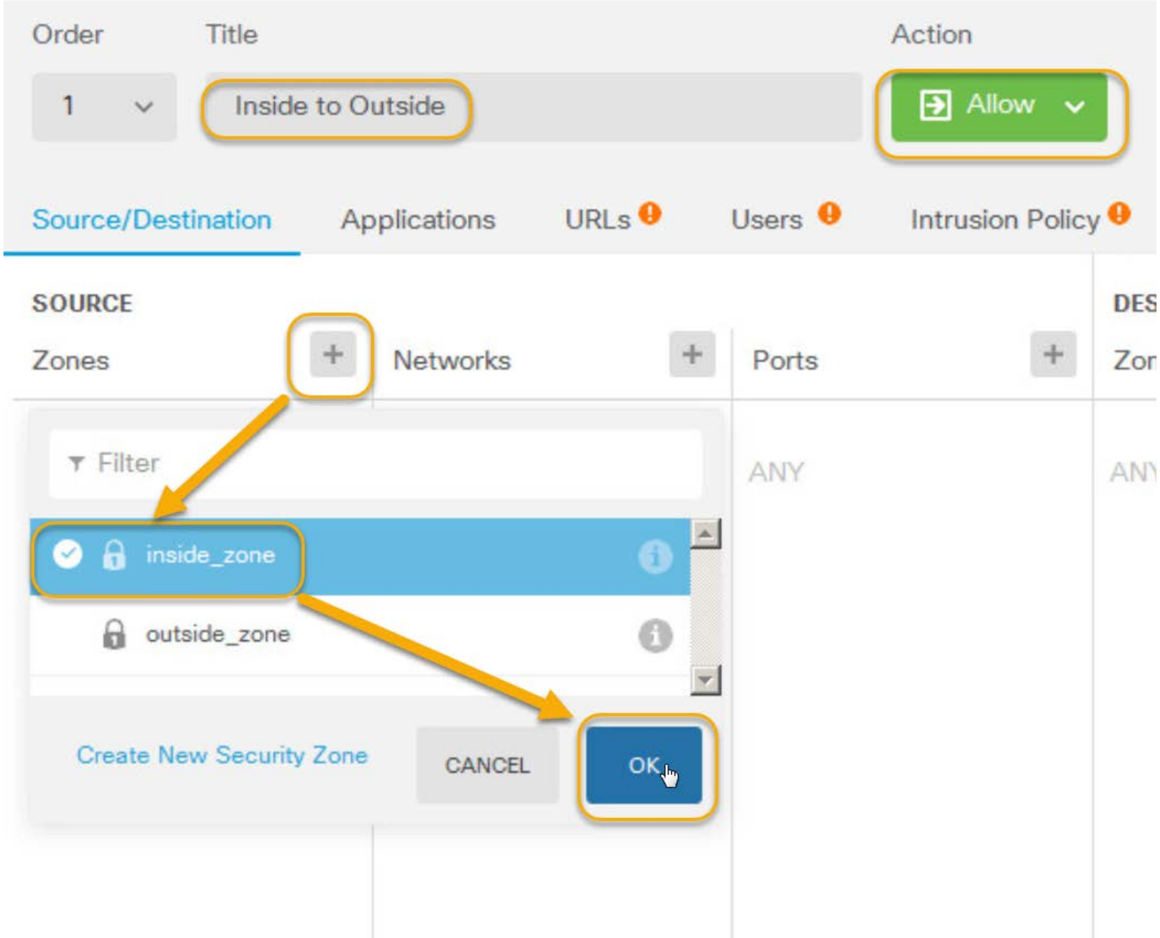


a. Title: **Inside to Outside**

b. Action: **Allow**

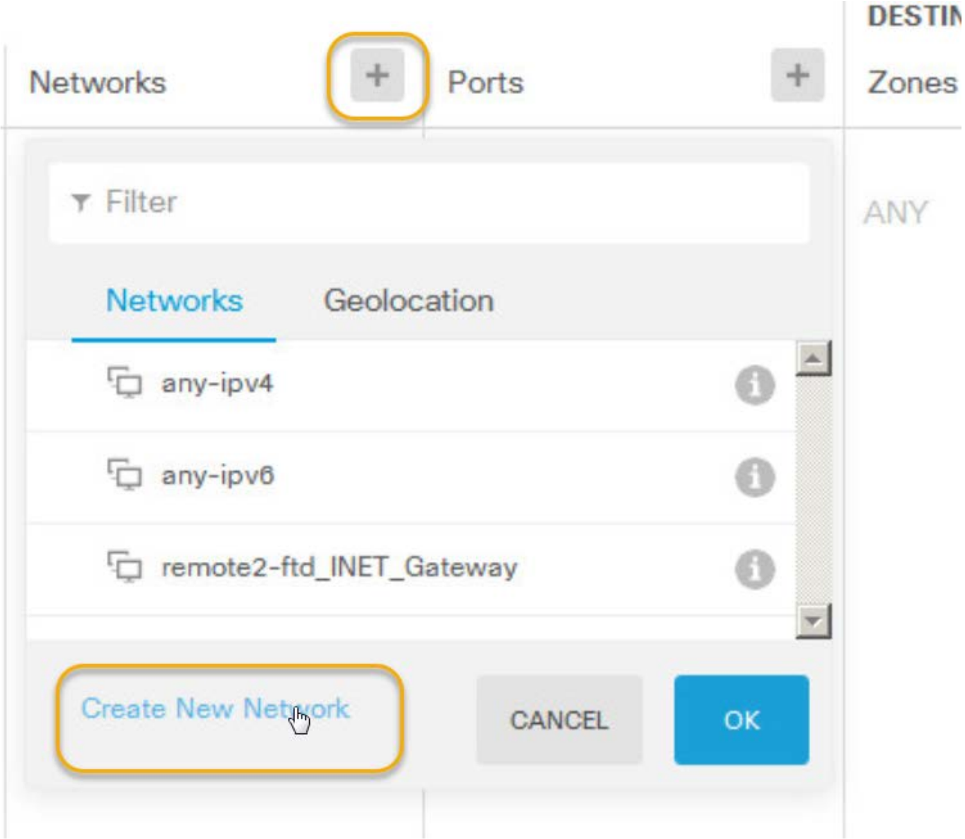
c. Source Zones: Click the **plus icon** and select **inside_zone**.

Figure 43. Configure Access Policy



d. Source Networks: Click the **plus icon** and then click the **Create New Network** link to add a new Network Object that will represent the **Remote2's LAN**.

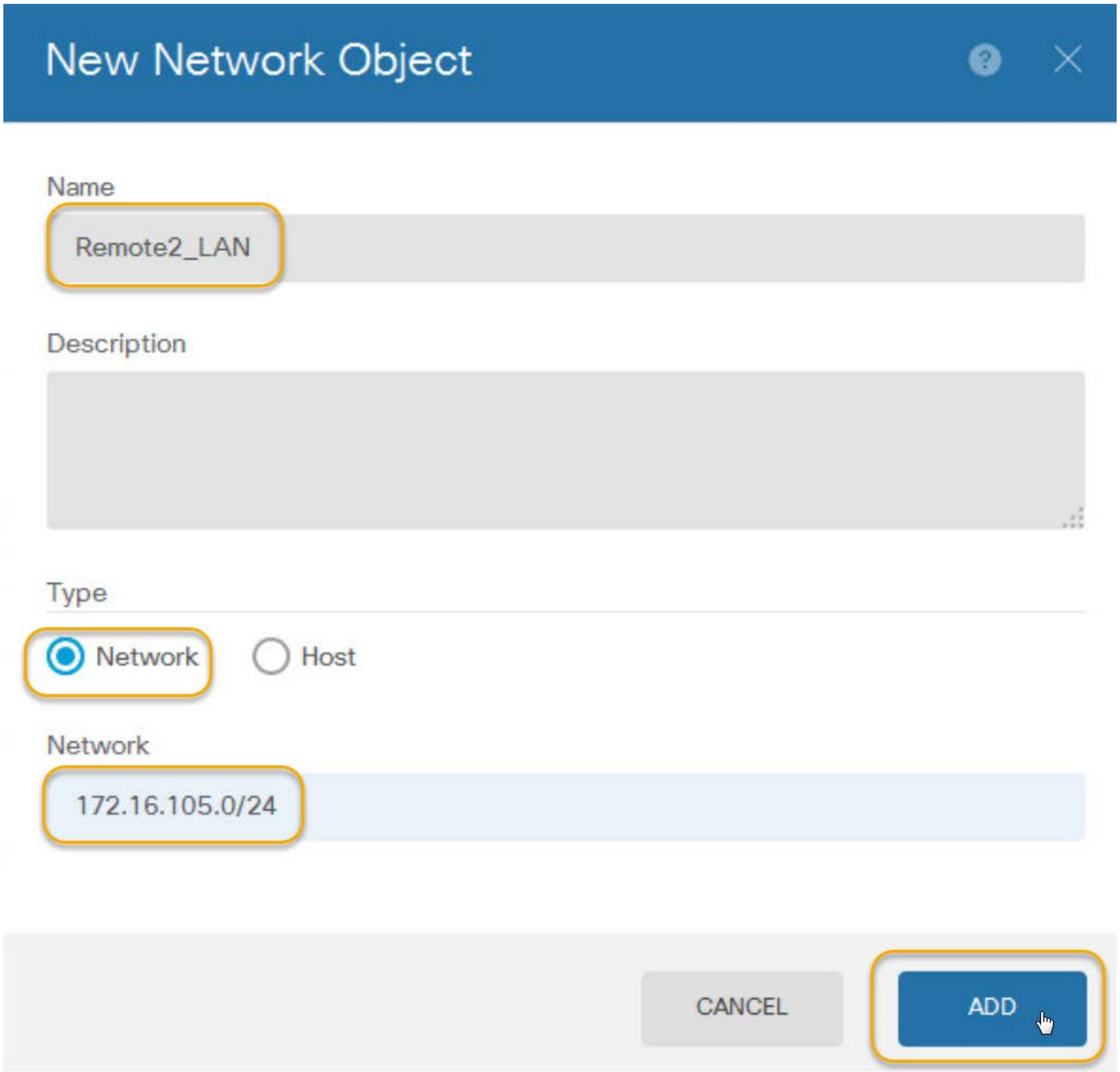
Figure 44. Create another network object



i. In the New Network Object popup window use the following to fill out the needed information:

1. Name: **Remote2_LAN**
2. Type: **Network**
3. Network: **172.16.105.0/24**
4. Click **ADD**.

Figure 45. Create another network object



New Network Object

Name: Remote2_LAN

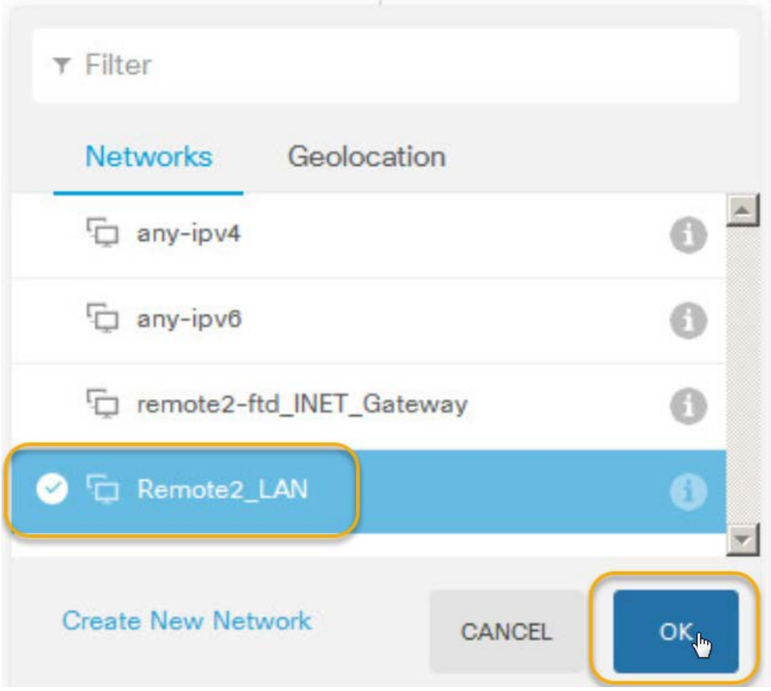
Description:

Type: ● Network ○ Host

Network: 172.16.105.0/24

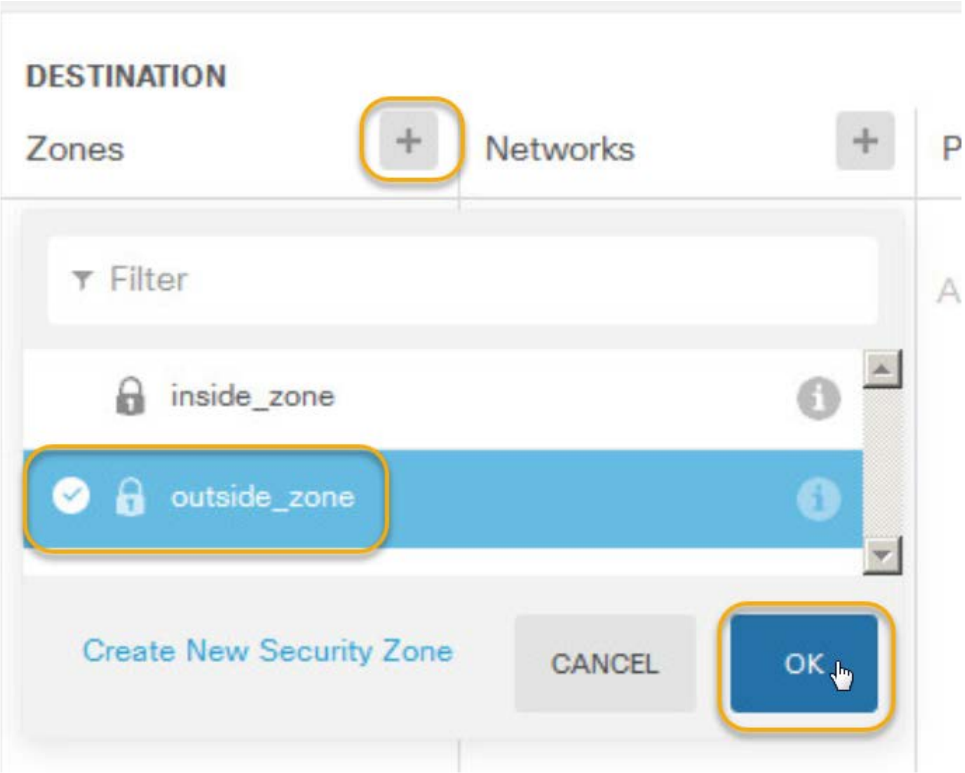
ii. Select the **Remote2_LAN** from the list of networks and click **OK**.

Figure 46. Select the Remote2_LAN object



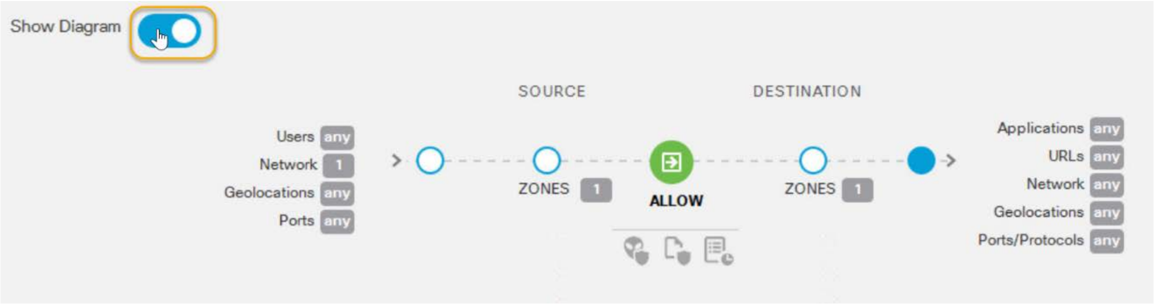
e. Destination Zones: outside_zone

Figure 47. Select outside_zon for the destination



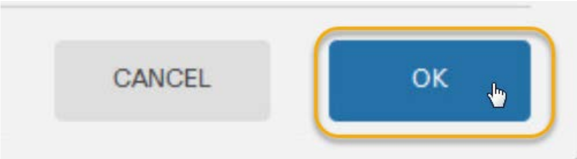
f. Toggle the **Show Diagram** button to display a graphical representation of this policy. (Once the policy is created you can also view this diagram by clicking the > icon next to the policy.)

Figure 48. Show diagram



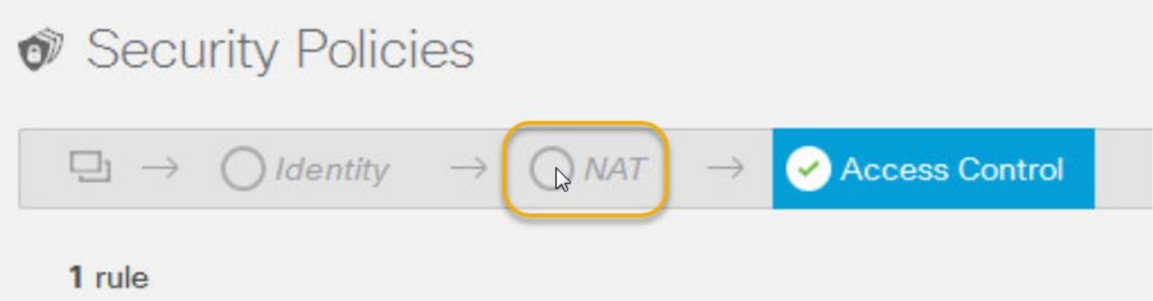
g. Click **OK** to create this policy.

Figure 49. Click OK



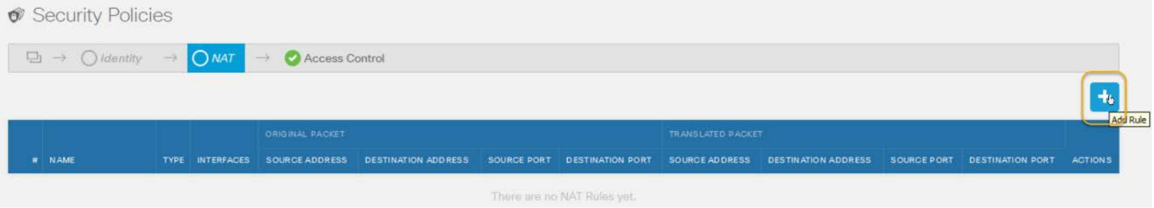
29. From the Security Policies menu click the **NAT** link.

Figure 50. Click NAT link



30. Click the **plus icon** to create a new NAT policy. Use the following to fill out the needed information:

Figure 51. Add a NAT rule



				ORIGINAL PACKET				TRANSLATED PACKET				
#	NAME	TYPE	INTERFACES	SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE PORT	DESTINATION PORT	SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE PORT	DESTINATION PORT	ACTIONS

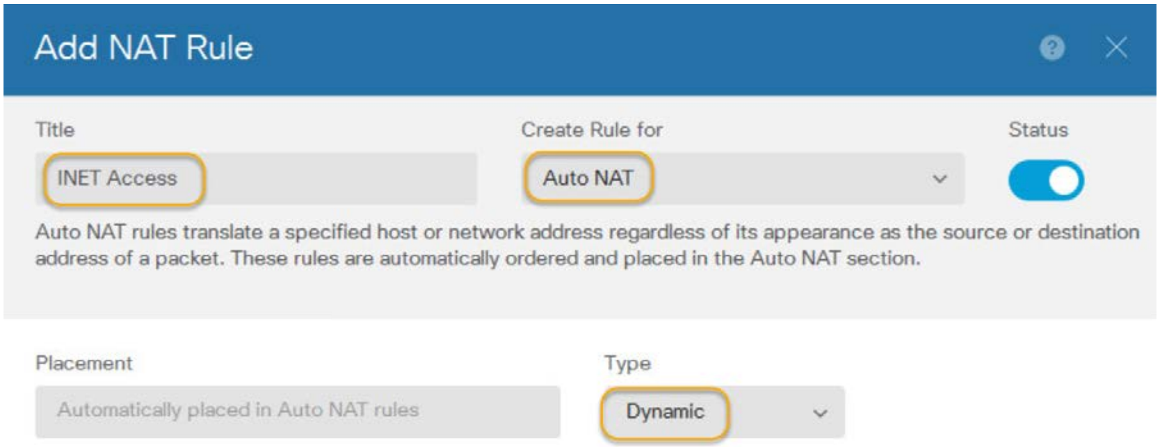
There are no NAT Rules yet.

a. Title: **INET Access**

b. Create Rule for: **Auto NAT**

c. Type: **Dynamic**

Figure 52. Configure NAT rule



Title: INET Access

Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules

Type: Dynamic

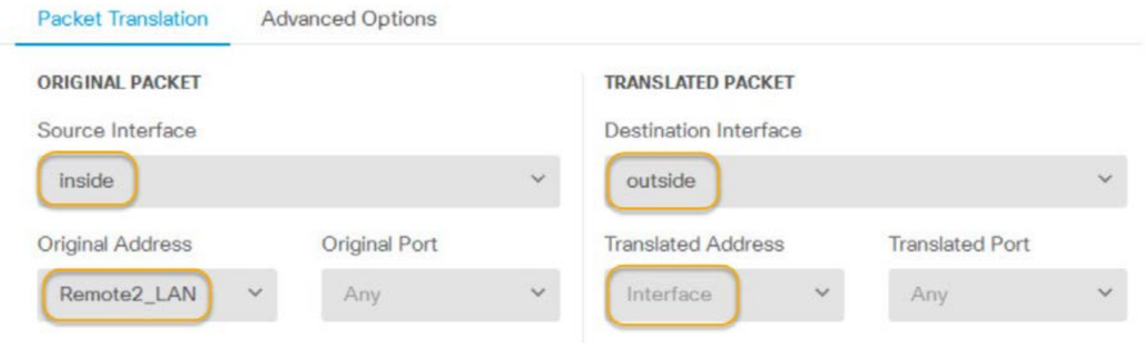
d. Source Interface: **inside**

e. Original Address: **Remote2_LAN**

f. Destination Interface: **outside**

g. Translated Address: **Interface**

Figure 53. Continue filling out NAT rule



ORIGINAL PACKET

Source Interface: inside

Original Address: Remote2_LAN

Original Port: Any

TRANSLATED PACKET

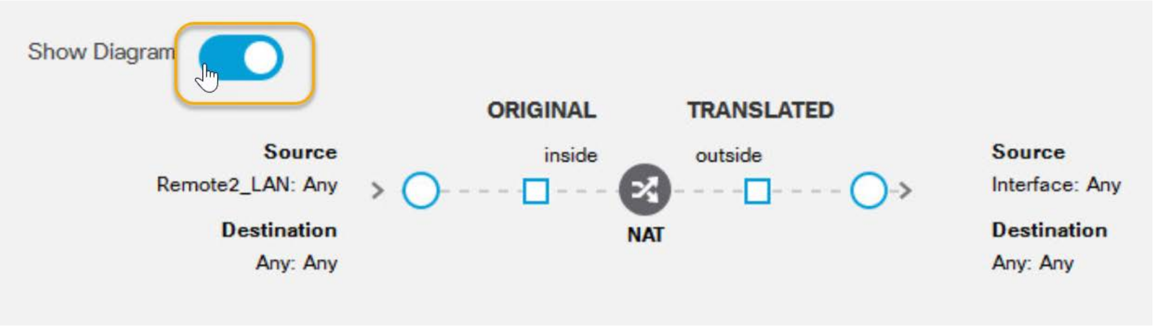
Destination Interface: outside

Translated Address: Interface

Translated Port: Any

h. Toggle the **Show Diagram** button to display a graphical representation of this policy. (Once the policy is created you can also view this diagram by clicking the > icon next to the policy.)

Figure 54. Show diagram

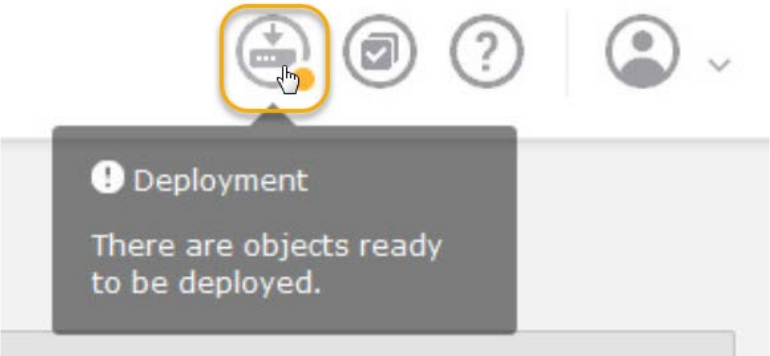


i. Click **OK** to create the NAT policy.

Figure 55. Click OK

31. Finally click the **Deployment** icon from the top menu. (It is the 4th icon from the right.)

Figure 56. Deploy Configuration

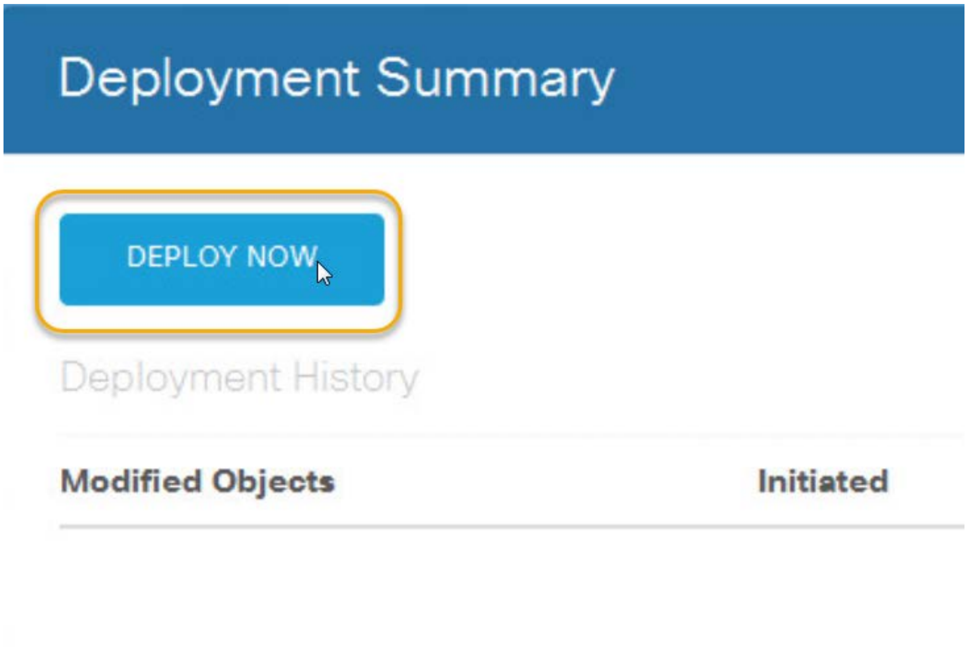


Deployment

There are objects ready to be deployed.

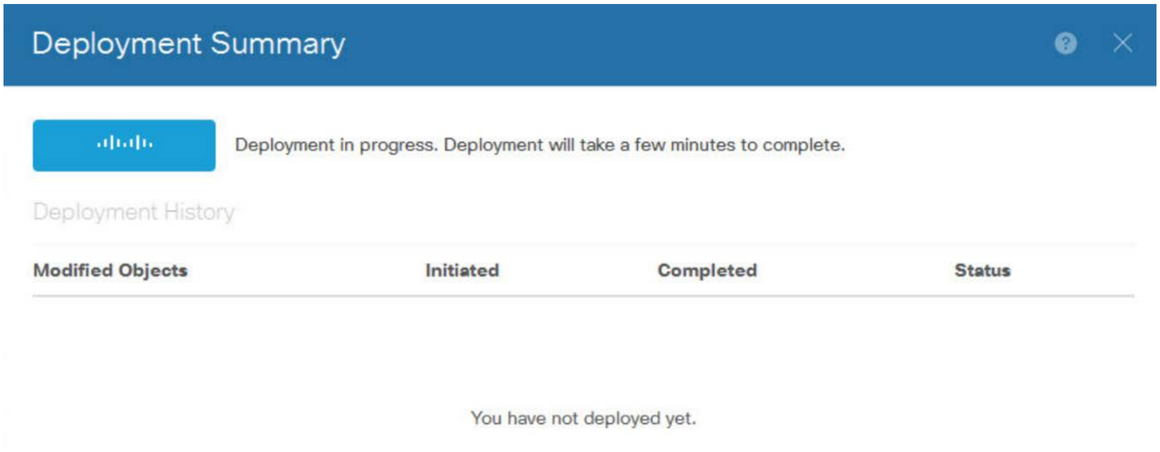
32. Click the **DEPLOY NOW** button. Given all the changes you have made (configuring the interfaces, assigning IP addresses, routing, NAT, Access Control) once this deployment is done you should be able to access the Internet from the Remote2_wkst PC.

Figure 57. Confirm Deployment



Deployment Summary

Figure 58. More confirm deployment



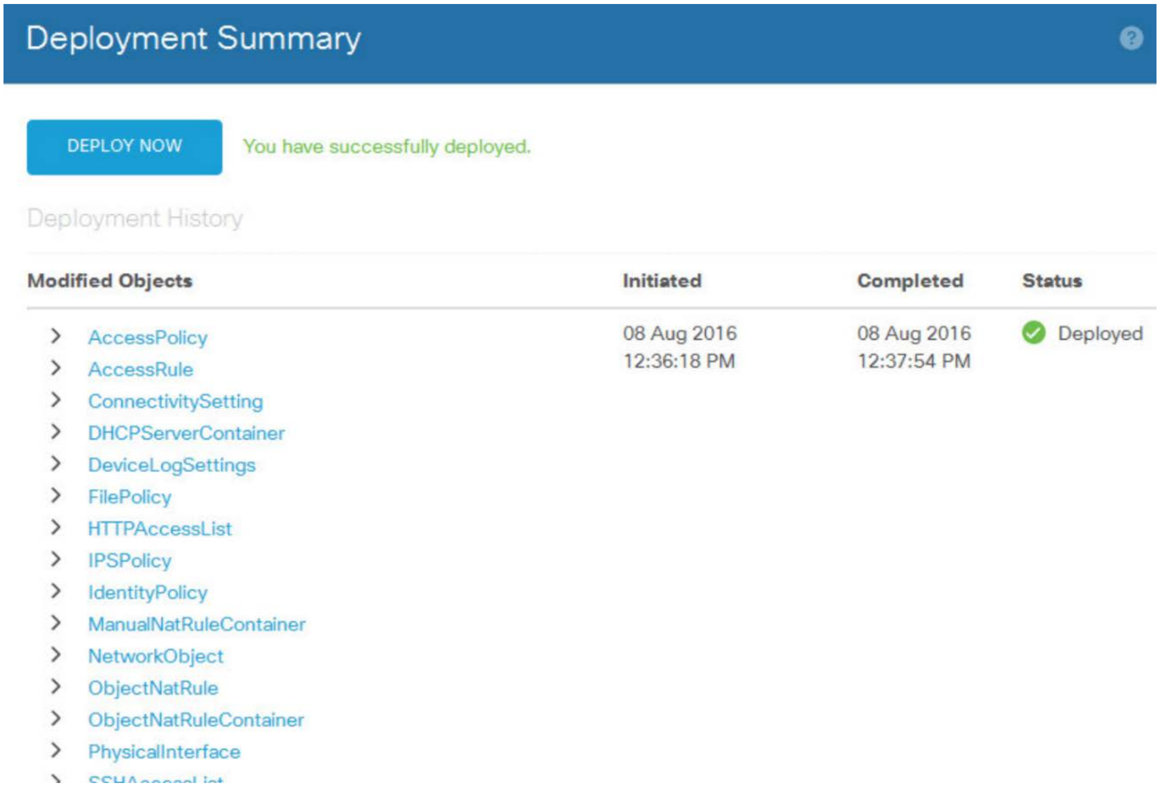
Deployment Summary

Deployment in progress. Deployment will take a few minutes to complete.

You have not deployed yet.

33. Once the Deployment Summary window show that the deployment is done close that popup window.

Figure 59. Successful deployment



You have successfully deployed.

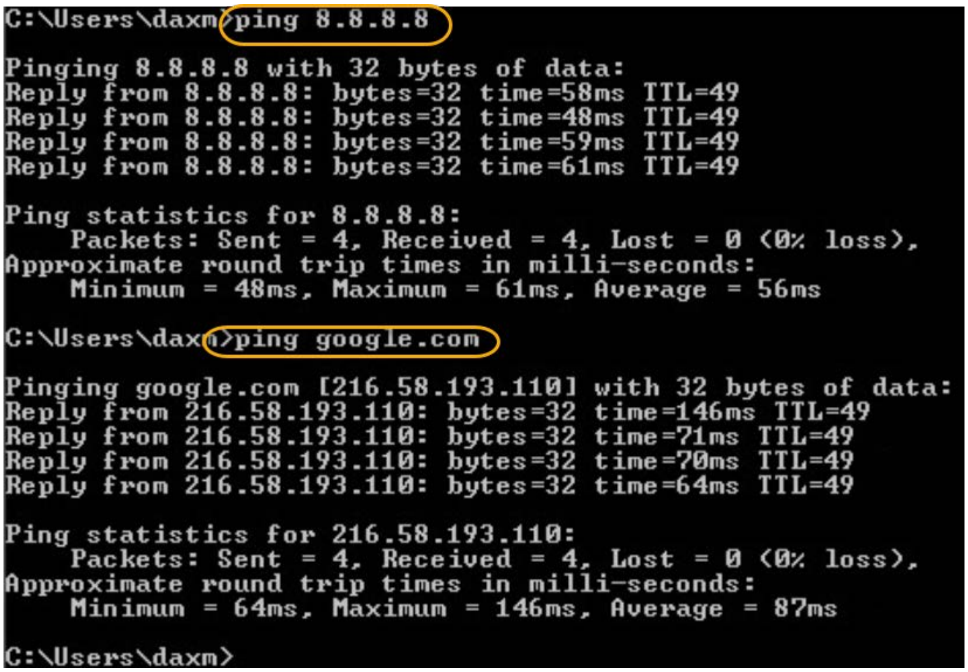
Deployment History

Modified Objects	Initiated	Completed	Status
AccessPolicy	08 Aug 2016 12:36:18 PM	08 Aug 2016 12:37:54 PM	✓ Deployed
AccessRule			
ConnectivitySetting			
DHCPServerContainer			
DeviceLogSettings			
FilePolicy			
HTTPAccessList			
IPSPolicy			
IdentityPolicy			
ManualNatRuleContainer			
NetworkObject			
ObjectNatRule			
ObjectNatRuleContainer			
PhysicalInterface			
SSHAccessList			

Testing Remote2-FTD Configuration

34. On **remote2-wkst** open up a **CMD prompt** and type **ping 8.8.8.8** as an initial test. This should succeed. A further test would be to ping google.com to ensure DNS resolution works too.

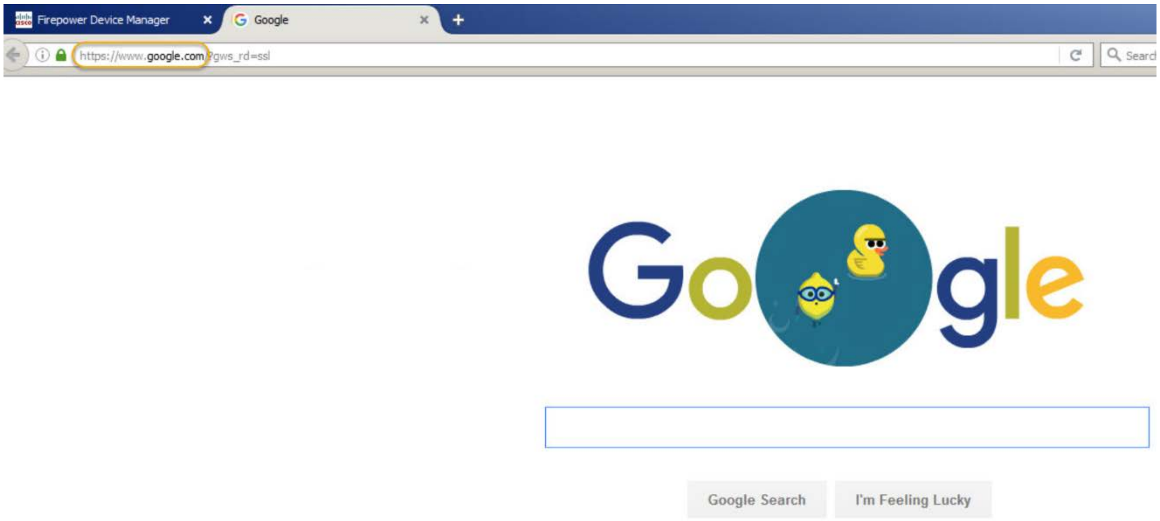
Figure 60. Ping test on remote2-wkst



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

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=58ms TTL=49
Reply from 8.8.8.8: bytes=32 time=48ms TTL=49
Reply from 8.8.8.8: bytes=32 time=59ms TTL=49
Reply from 8.8.8.8: bytes=32 time=61ms TTL=49

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 61ms, Average = 56ms

C:\Users\daxm>ping google.com

Pinging google.com [216.58.193.110] with 32 bytes of data:
Reply from 216.58.193.110: bytes=32 time=146ms TTL=49
Reply from 216.58.193.110: bytes=32 time=71ms TTL=49
Reply from 216.58.193.110: bytes=32 time=70ms TTL=49
Reply from 216.58.193.110: bytes=32 time=64ms TTL=49

Ping statistics for 216.58.193.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 64ms, Maximum = 146ms, Average = 87ms

C:\Users\daxm>
```

35. Open a new tab in **FireFox** and go to the Google home page to ensure the Access Control policy is also allowing HTTP.

Figure 61. Access google.com



Scenario Summary

The Firepower Device Manager is just as capable in configuring the FTD device as is the FMC. It does have its limits though. For example, you cannot configure a VPN tunnel using the Firepower Device Manager. Additionally, and obviously, using the Firepower Device Manager means that each FTD device is configured individually. This leaves room for misconfigurations and differences between FTD devices (which makes compliance to regulations difficult to maintain and build reports for).

Page intentionally left blank.

Appendix D. Upgrading ASA5515-X to FTD

Caveats

The caveats for upgrading an ASA to the FTD code mostly reside on what version of ROMMON you have. In order to get to the minimum ROMMON mode you might need to upgrade your ASA code first. In this appendix the required ROMMON code has already been met (and thus is beyond the scope of this document).

Install Boot Image

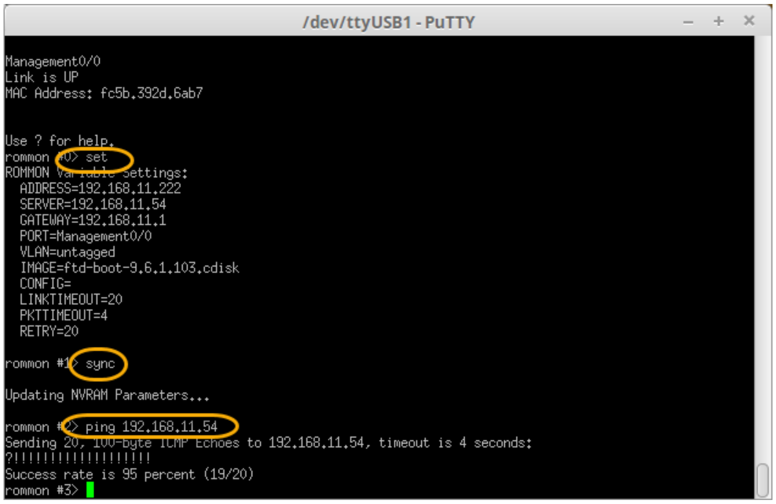
The boot image is a very simple operating system that is designed to boot your ASA NOT using the local hard drive. Think of this much like “booting from CD” when installing a new operating system on your PC. Use the following steps to install and boot the boot image.

36. **Power on your ASA** and break the normal boot process to enter ROMMON mode by pressing **ESC** when prompted.
37. Prepare your system to tftp upload the boot image file. Use the **set** command to see your current settings and then adjust each variable to match your network’s criteria. Note: There are two possible boot image file types: cdisk or lfbff. Depending on what type of ASA you have you have to select the correct one. For an ASA5515-X you use the cdisk version.

The variables are assigned by using their name (say ADDRESS) followed by an equal “=” sign followed by the value. Notice there are NO spaces. For example: ADDRESS=192.168.11.54 not ADDRESS = 192.168.11.54.

38. Once the variables are correct use the **sync** command to ensure they are save in ROMMON.
39. **Ping** your **tftp server** to ensure you have access.

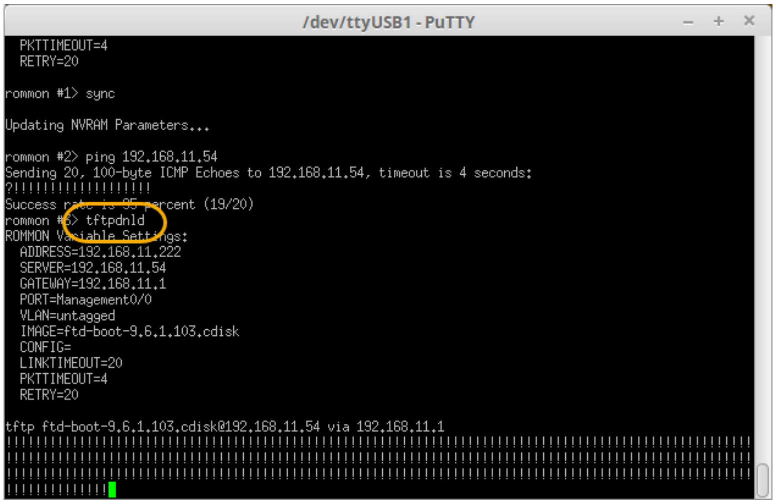
Figure 62. Prepare for tftpdnld



```
Management0/0
Link is UP
MAC Address: fc5b.392d.6ab7


Use ? for help.
rommon #0> set
ROMMON Variable Settings:
  ADDRESS=192.168.11.222
  SERVER=192.168.11.54
  GATEWAY=192.168.11.1
  PORT=Management0/0
  VLAN=untagged
  IMAGE=ftd-boot-9.6.1.103.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #1> sync

Updating NVRAM Parameters...

rommon #2> ping 192.168.11.54
Sending 20, 100-byte ICMP Echoes to 192.168.11.54, timeout is 4 seconds:
?!!!!!!!!!!!!!!!!!!!
Success rate is 95 percent (19/20)
rommon #3>
```

40. Use the **tftpdnld** command to start the tftp download process. Once the download is complete the system will reboot and you HAVE to break the normal boot process again in order to load the boot image or your ASA will just boot to its normal ASA code. This is probably the hardest part of this process just because you have to attentively watch the tftp download and reboot process. You'll only have 30 seconds to select the boot image option before the ASA will boot normally. If you miss it you'll need to re-tftp download the boot image file again.

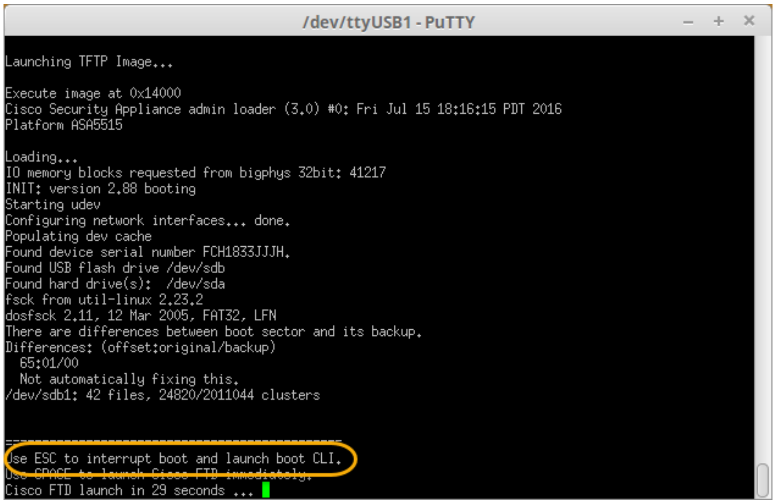
Figure 63. Initiate tftpdnld



```
  PKTTIMEOUT=4
  RETRY=20

rommon #1> sync

Updating NVRAM Parameters...

rommon #2> ping 192.168.11.54
Sending 20, 100-byte ICMP Echoes to 192.168.11.54, timeout is 4 seconds:
?!!!!!!!!!!!!!!!!!!!
Success rate is 95 percent (19/20)
rommon #3> tftpdnld
ROMMON Variable Settings:
  ADDRESS=192.168.11.222
  SERVER=192.168.11.54
  GATEWAY=192.168.11.1
  PORT=Management0/0
  VLAN=untagged
  IMAGE=ftd-boot-9.6.1.103.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp ftd-boot-9.6.1.103.cdisk@192.168.11.54 via 192.168.11.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
```

41. Press **ESC** to load the boot image when prompted.

Figure 64. Press ESC



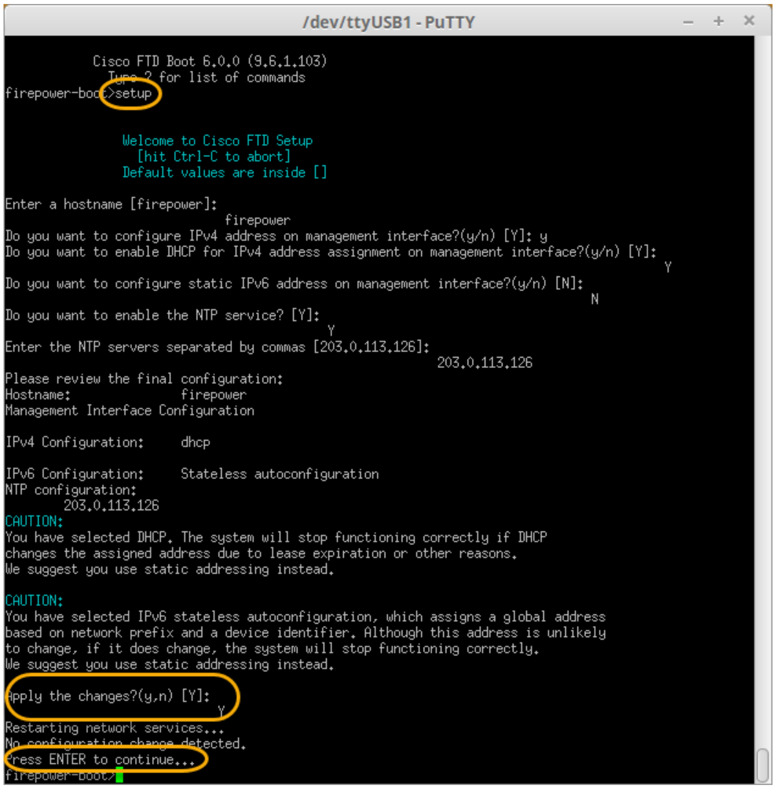
```

Launching TFTP Image...

Execute image at 0x14000
Cisco Security Appliance admin loader (3.0) #0: Fri Jul 15 18:16:15 PDT 2016
Platform ASA5515

Loading...
IO memory blocks requested from bigphys 32bit: 41217
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
Populating dev cache
Found device serial number FCH1833JJJH.
Found USB flash drive /dev/sdb
Found hard drive(s):  /dev/sda
fsck from util-linux 2.23.2
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
There are differences between boot sector and its backup.
Differences: (offset:original/backup)
  65:01/00
  Not automatically fixing this.
/dev/sdb1: 42 files, 24820/2011044 clusters


==============================================
Use ESC to interrupt boot and launch boot CLI.
Use SPACE to launch Cisco FTD immediately.
Cisco FTD launch in 29 seconds ...
```

Install FTD Image

Once the ASA has booted the boot image you are ready to upgrade the code on the ASA hard drive to the FTD code. This process WILL erase all settings and operating system that was on this ASA previously and is NOT reversible once the hard drive has been formatted.

42. Issue the command **setup**. This will start a short questionnaire wizard to set up basic network connectivity, similar to what you did in ROMMON mode.

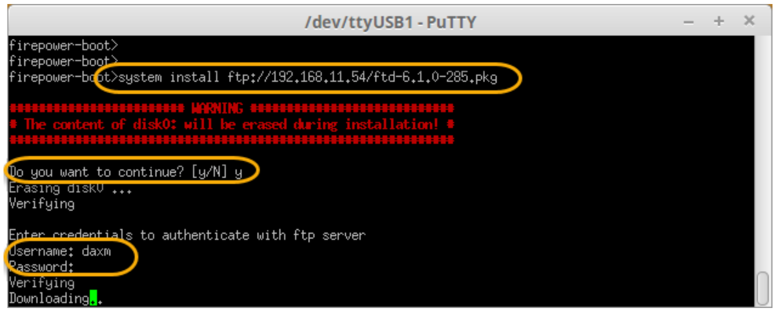
Figure 65. Type setup



```
            Cisco FTD Boot 6.0.0 (9.6.1.103)
              Type ? for list of commands
firepower-boot>setup


                Welcome to Cisco FTD Setup
                  [hit Ctrl-C to abort]
                Default values are inside []

Enter a hostname [firepower]:
                              firepower
Do you want to configure IPv4 address on management interface?(y/n) [Y]: y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]:
                                                                                           Y
Do you want to configure static IPv6 address on management interface?(y/n) [N]:
                                                                                N
Do you want to enable the NTP service? [Y]:
                                            Y
Enter the NTP servers separated by commas [203.0.113.126]:
                                                           203.0.113.126
Please review the final configuration:
Hostname:                 firepower
Management Interface Configuration

IPv4 Configuration:       dhcp

IPv6 Configuration:       Stateless autoconfiguration
NTP configuration:
        203.0.113.126
CAUTION:
You have selected DHCP. The system will stop functioning correctly if DHCP
changes the assigned address due to lease expiration or other reasons.
We suggest you use static addressing instead.

CAUTION:
You have selected IPv6 stateless autoconfiguration, which assigns a global address
based on network prefix and a device identifier. Although this address is unlikely
to change, if it does change, the system will stop functioning correctly.
We suggest you use static addressing instead.

Apply the changes?(y,n) [Y]:
                             Y
Restarting network services...
No configuration change detected.
Press ENTER to continue...
firepower-boot>
```

43. Unlike downloading the boot image file you must use http, https, or ftp to download the FTD code package file. Issue the command **system install** to download the package file.

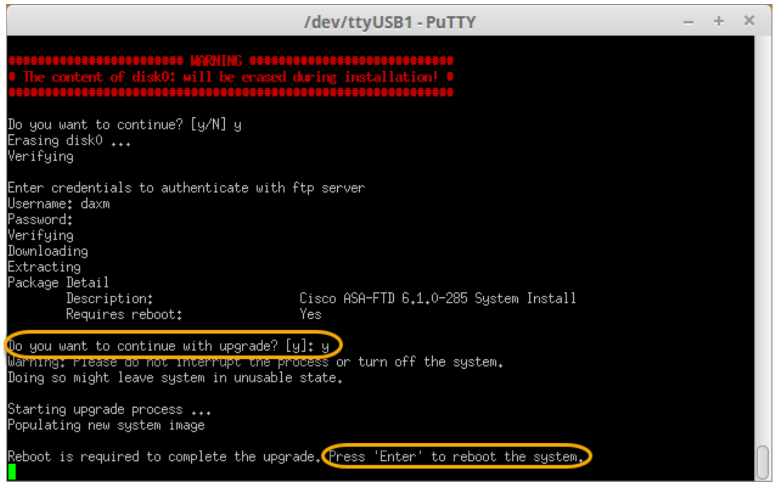
Figure 66. Download pkg file



```
firepower-boot>
firepower-boot>
firepower-boot>system install ftp://192.168.11.54/ftd-6.1.0-285.pkg

######################## WARNING ############################
# The content of disk0: will be erased during installation! #
#############################################################

Do you want to continue? [y/N] y
Erasing disk0 ...
Verifying

Enter credentials to authenticate with ftp server
Username: daxm
Password:
Verifying
Downloading..
```

44. Once the package file is downloaded type in **Yes** to upgrade the ASA. Once the upgrade is complete press **ENTER** to reload the ASA and boot it up using the new FTD software!

Figure 67. Confirm upgrade process



```
######################## WARNING ############################
# The content of disk0: will be erased during installation! #
#############################################################

Do you want to continue? [y/N] y
Erasing disk0 ...
Verifying

Enter credentials to authenticate with ftp server
Username: daxm
Password:
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FTD 6.1.0-285 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

To configure the freshly installed FTD software see Appendix B for information on how to configure the management interface. Then visit either Appendix C (to use the Firepower Device Manager) or Scenario 2 to register this FTD to the FMC.