Firepower Threat Defense 6.1 Basics Lab v1

Last Updated: 2-NOVEMBER-2016

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 and, unfortunately, there is no conversion tool to migrate the existing setup to this new device (more service hours for you!). 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 preconfigured FTD Basics lab includes the following Scenarios:

Scenario 1. Installing the Firepower Management Center
Scenario 2. Installing the FTD at the HQ Site
Scenario 3. Common Configurations for Example Corp Networks
Scenario 4. Installing the FTD at the Remote1 Site
Scenario 5. Installing the FTD at the Remote2 Site
Scenario 6. Configuring URL Filtering
Scenario 7. SSL Policy Configuration
Scenario 8. Malware and File Detection Configuration
Scenario 9. Intrusion Policy
Scenario 10. Configure Platform Settings
Scenario 11. Example Corp VPN Setup
Scenario 12. FMC and FTD Maintenance
Scenario 13. FMC and FTD Data Monitoring
Scenario 14. Introduction to API Programming the FMC
Appendix A. FMC OVA Deployment
Appendix B. FTD OVA Deployment
Appendix C. Manage FTD with Firepower Device Manager
Appendix D. Upgrading ASA5515-X to FTD

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Resources

For more information:

- View the content overview: https://dcloud-cms.cisco.com/demo/cisco-ftd-6-1-basics-lab-v1
- Visit the Cisco dCloud help page: https://dcloud-cms.cisco.com/help
- Access all available Cisco dCloud content: https://dcloud.cisco.com
- Contact Us: https://dcloud-cms.cisco.com/help/contact-us-security

Requirements

The table below outlines the requirements for this preconfigured demonstration.

Table 1. Requirements

Required	Optional
• Laptop with Cisco AnyConnect®	• No optional requirements for this lab.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

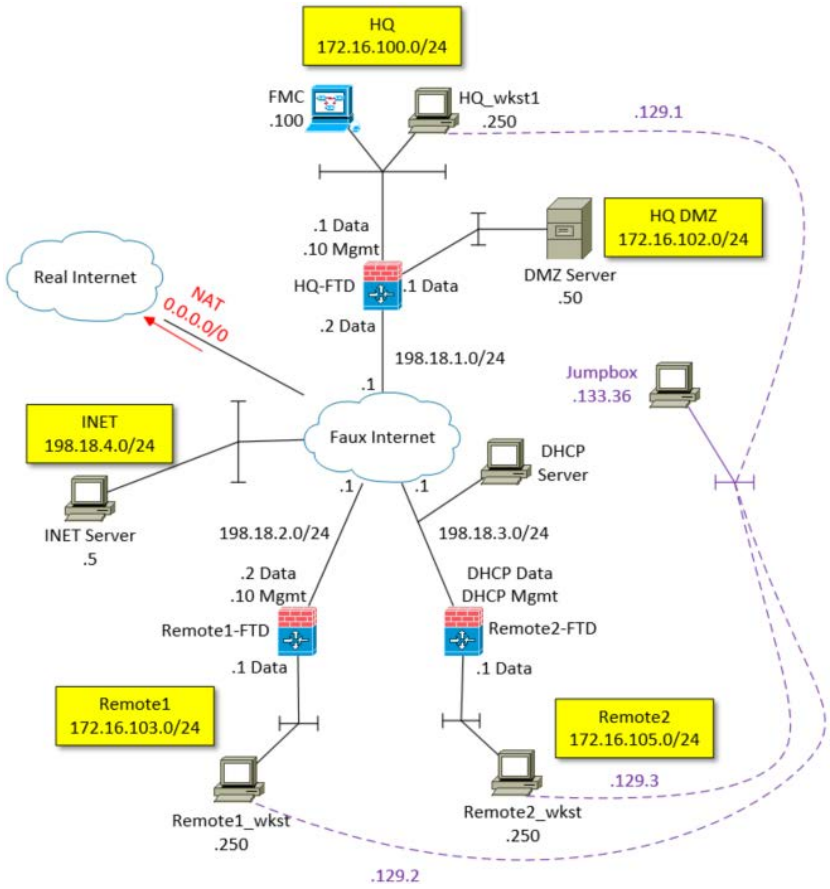
https://t.me/learningnets

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 access to the respective workstations 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

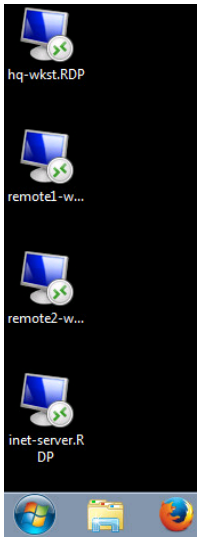
https://t.me/learningnets

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 AnyConnect VPN tunnel from your workstation to the lab environment. You will use an RDP client to connect from your workstation to a virtual machine (called Jumpbox) from which you can access all the other machines within the lab environment. The Jumpbox 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 VPN URL, username, and password information.
3. Using Cisco's AnyConnect VPN client access the URL and log in using the username and password that you got from the dCloud website.
4. Connect to the workstation with **Cisco AnyConnect VPN** [Show Me How].
5. Once connected, you should be able to ping 198.18.133.36 (the Jumpbox IP).
6. Connect to the **local RDP client on your laptop** [Show Me How].
    a. Workstation 1: **198.18.133.36**, Username: **administrator**, Password: **C1sco12345**
7. Notice that on the desktop there are 4 saved RDP sessions, one for each of the machines you'll need to access throughout the lab. Please open a connection to all 4 desktops to ensure that they are all reachable.

Figure 2. RDP Shortcuts on Jumpbox Desktop

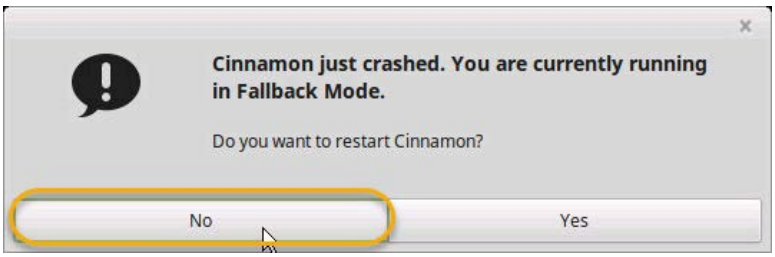


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 either use 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.

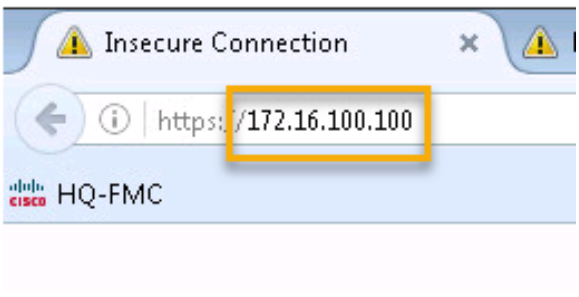
Due to limitations within the lab environment the correct network configuration is already applied to the FMC for you. Refer to Appendix A to get details of how this was accomplished.

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. 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 4. Access FMC URL

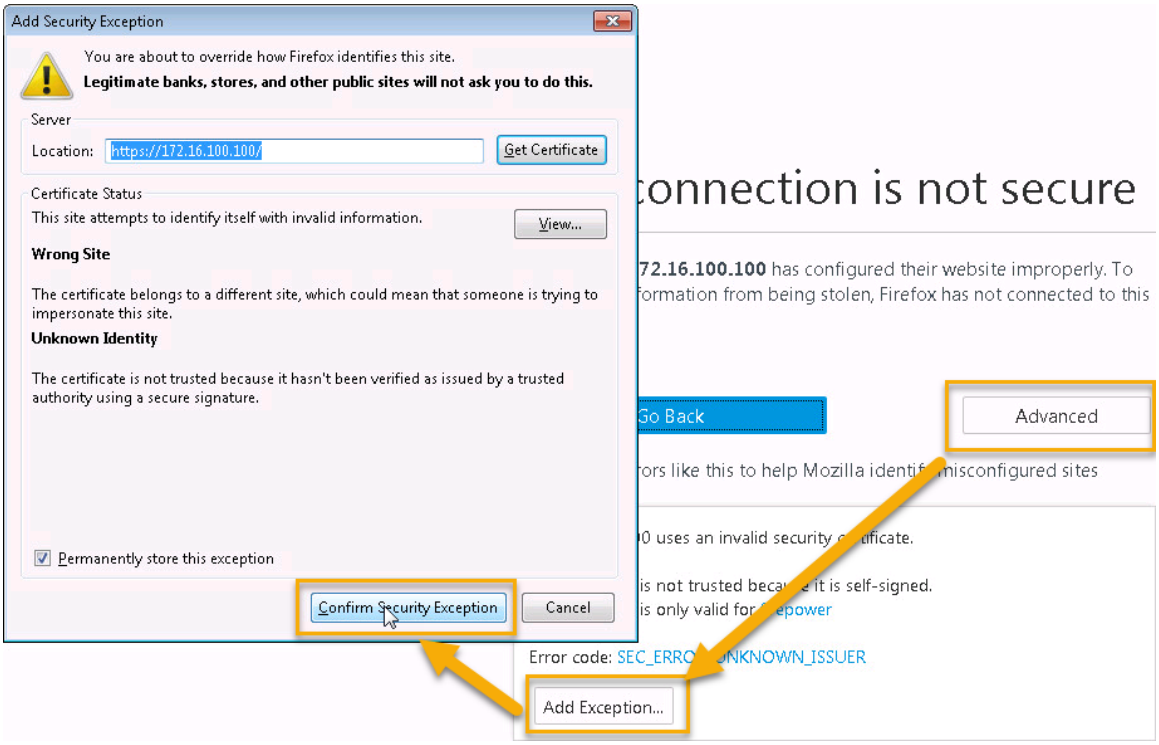


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

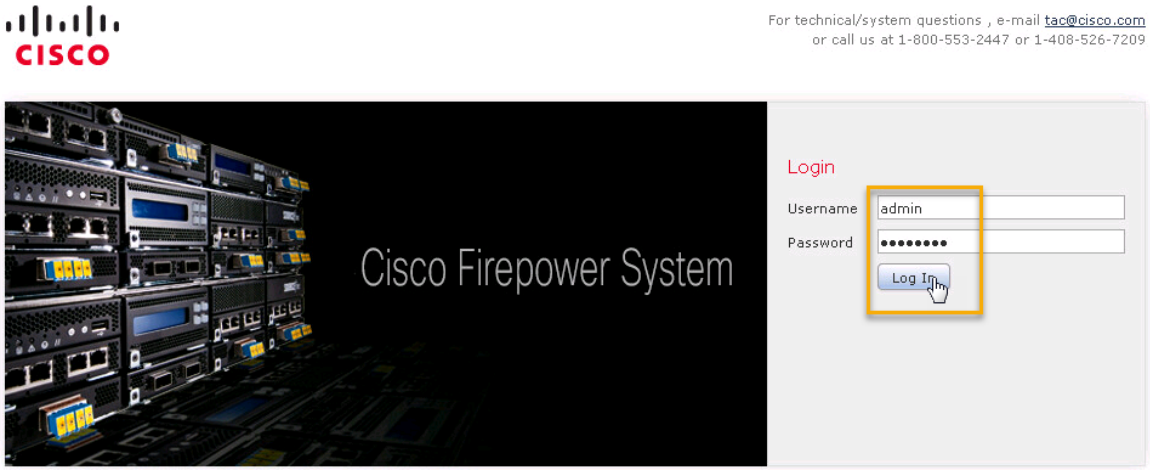
2. Accept the use of the self-signed certificate by clicking **Advanced > Add Exception** and then click the **Confirm Security Exception** in the popup window.

Figure 5. Accept SSL Self-Signed Cert from FMC



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

Figure 6. Log into FMC

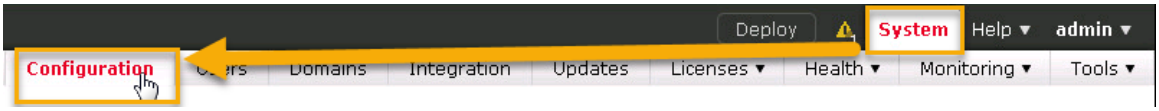


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

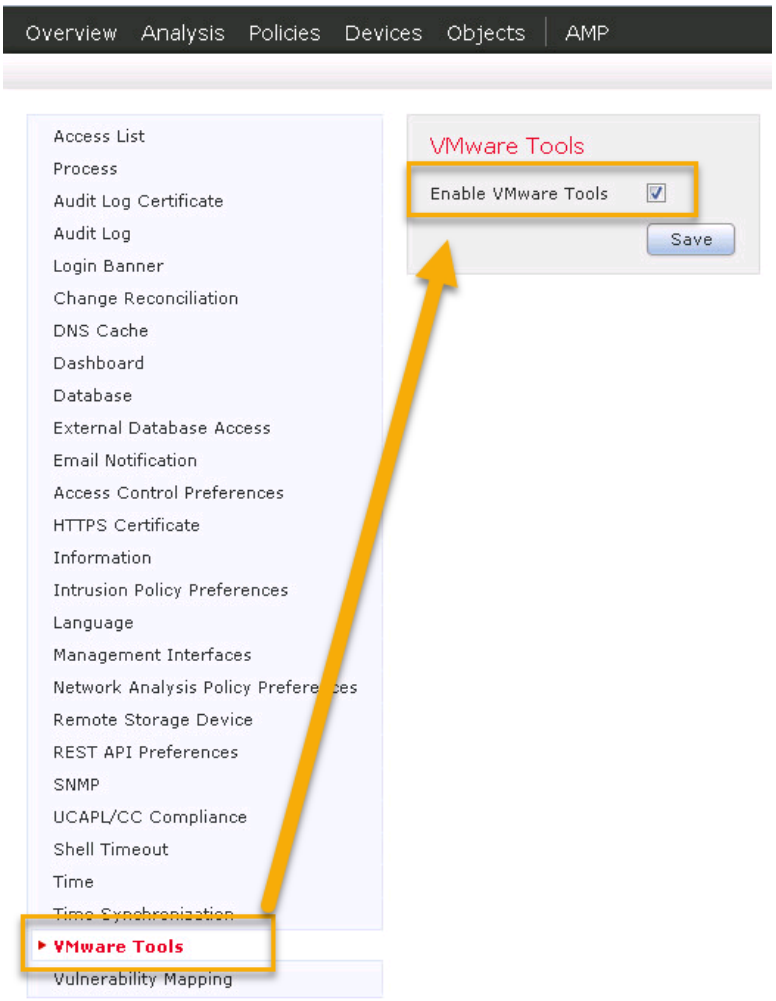
4. Now explore some of the options available for configuring, monitoring, and managing the FMC. Navigate to **System > Configuration**.

Figure 7. Navigation



5. 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 8. Ensure VMware Tools is Enabled

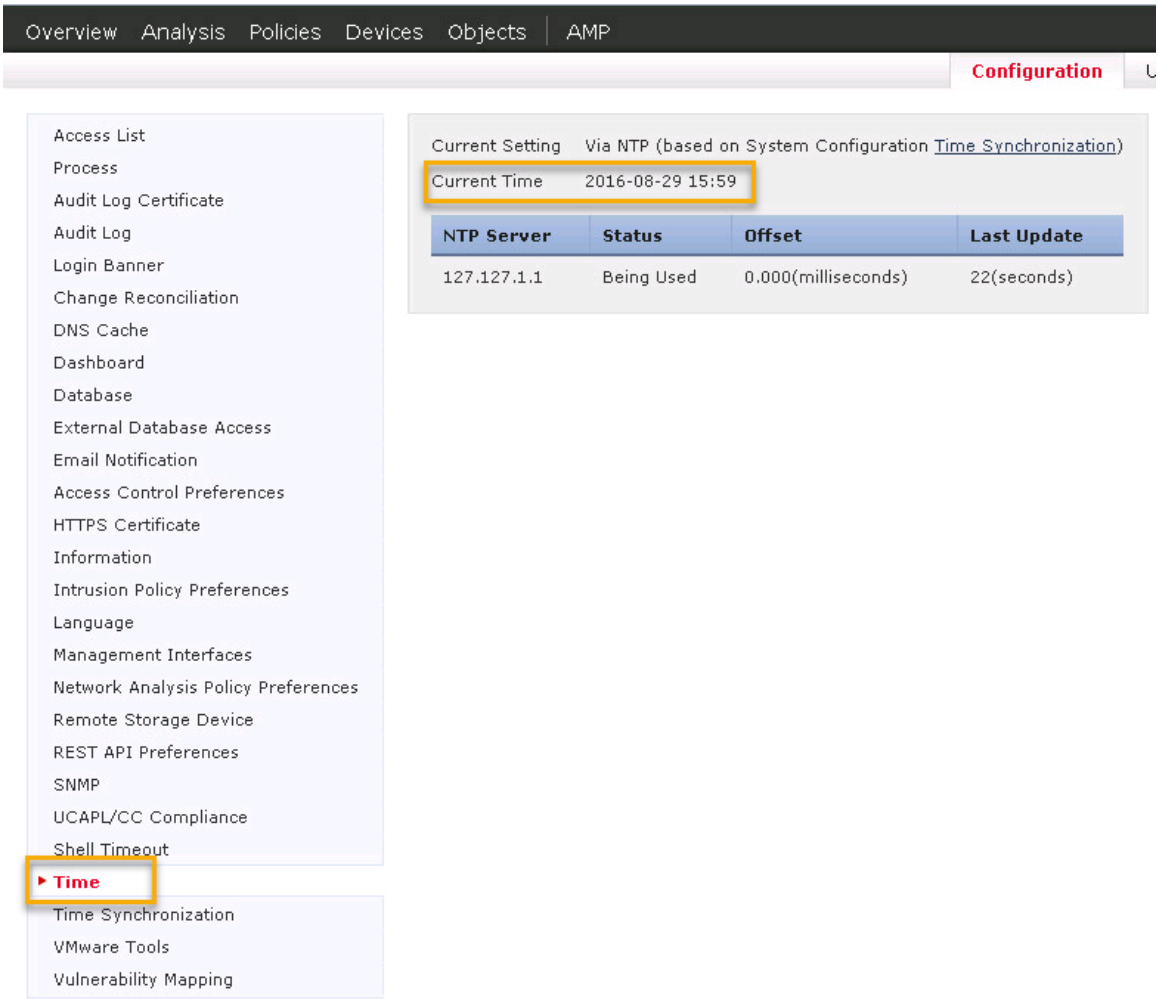


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 9. See the current time



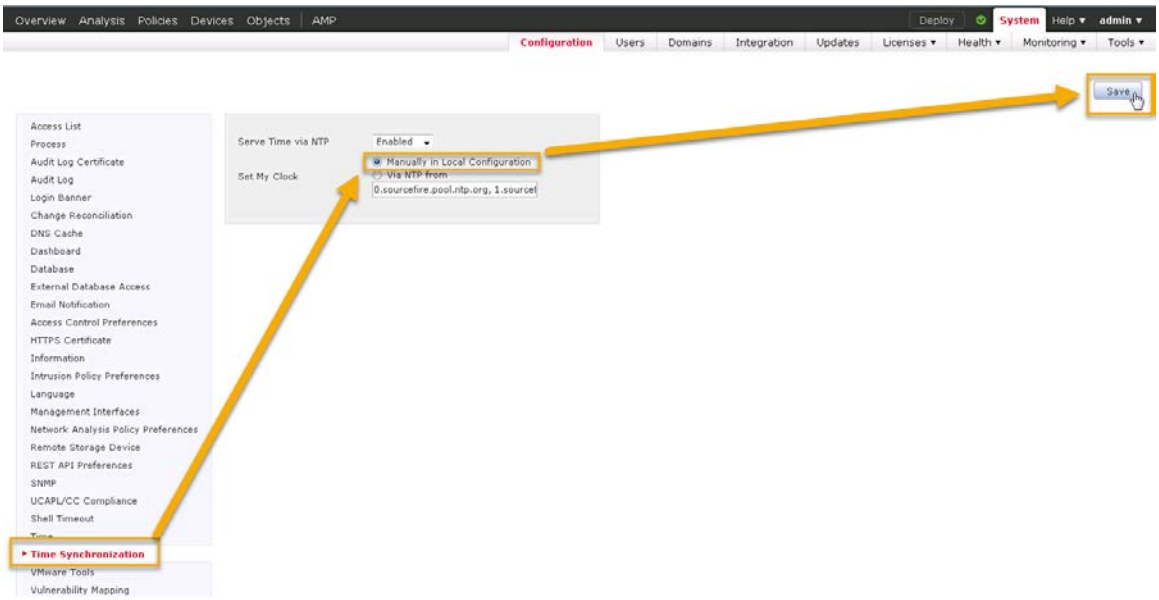
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

9. 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 10. Change to Manual time configuration



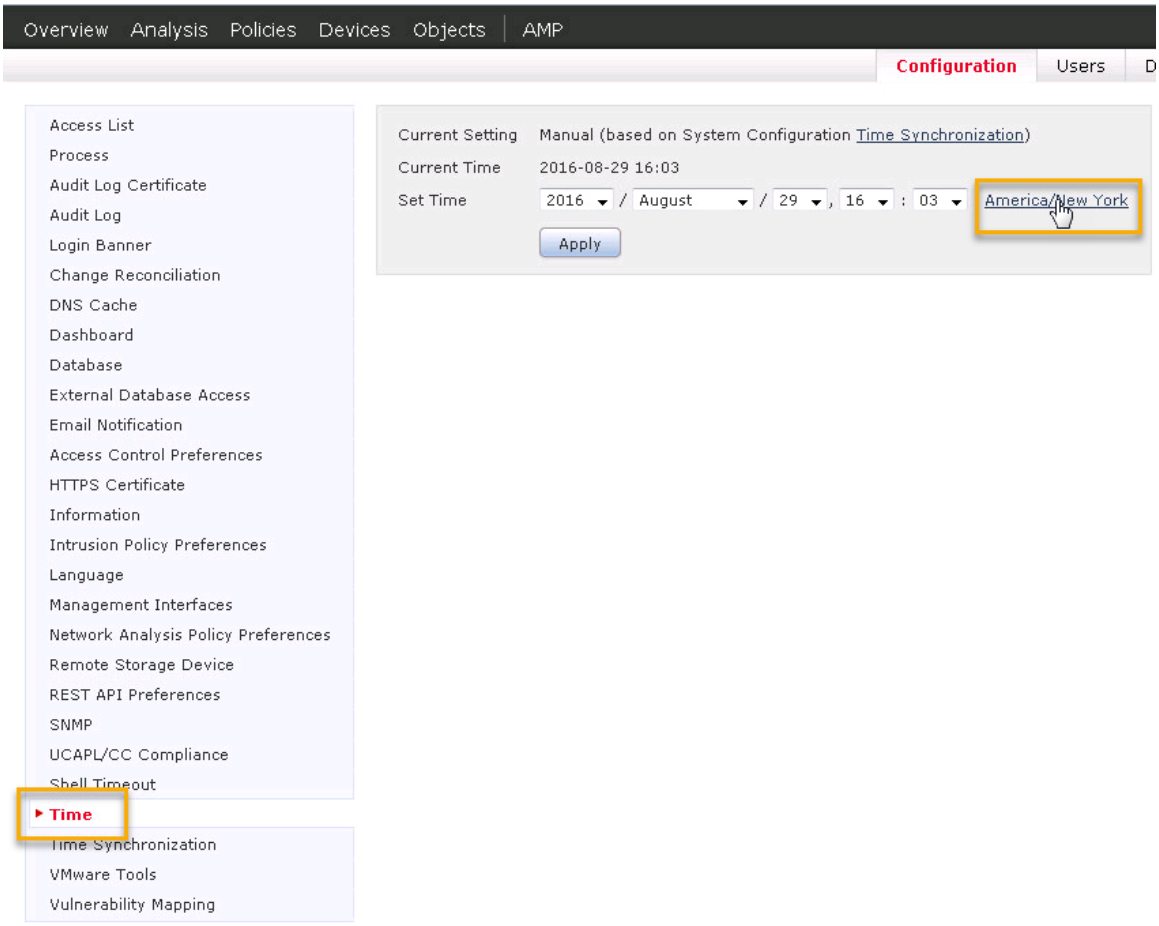
10. It will take a minute but once the page refreshes select on the **Time** menu tab again.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

11. 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 11. Time to change the time zone

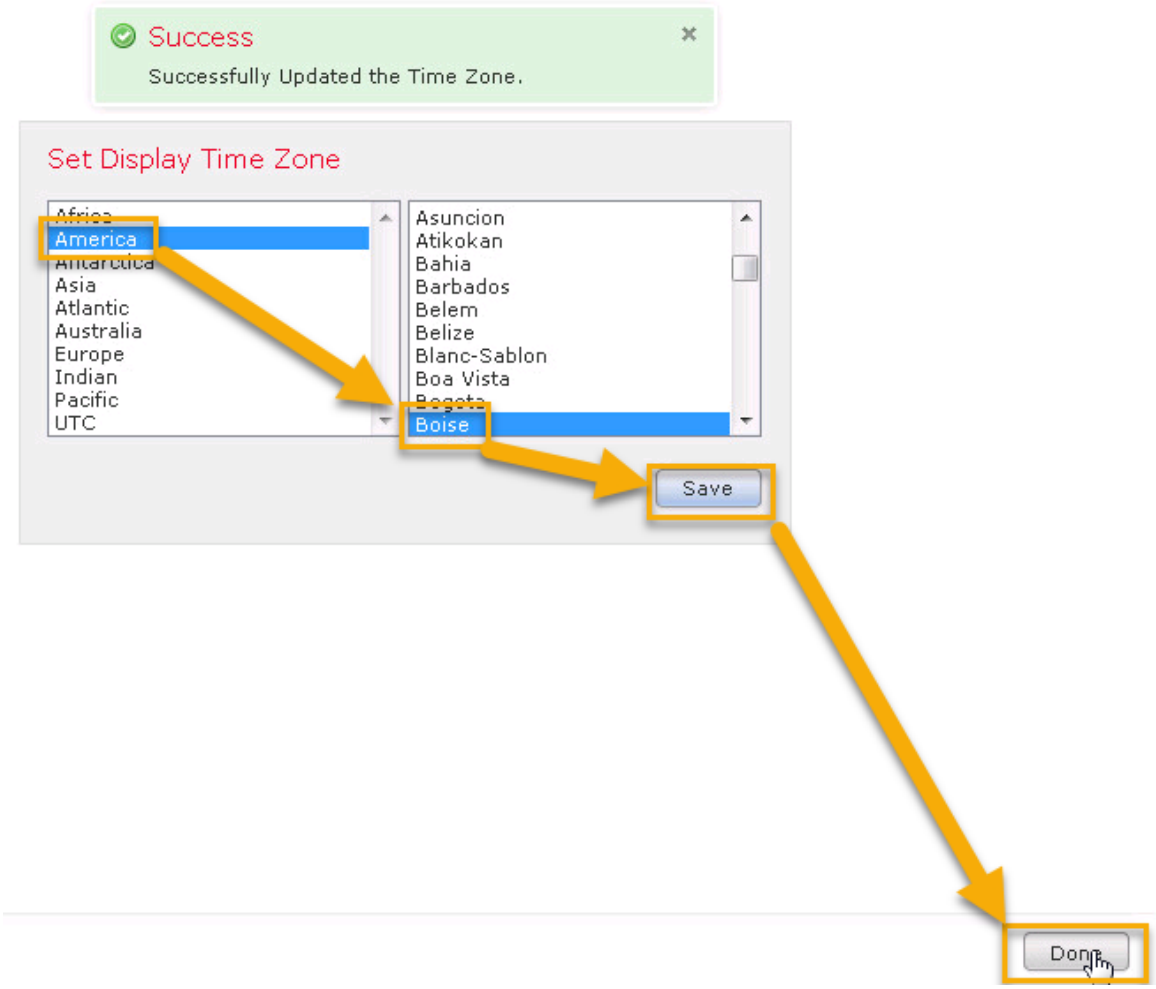


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

12. From the **Set Display Time Zone** popup window select **America** from the left column and **Boise** from the right column. Click **Save**.
13. When the page refreshes click **Done**.

Figure 12. Update time zone to Mountain

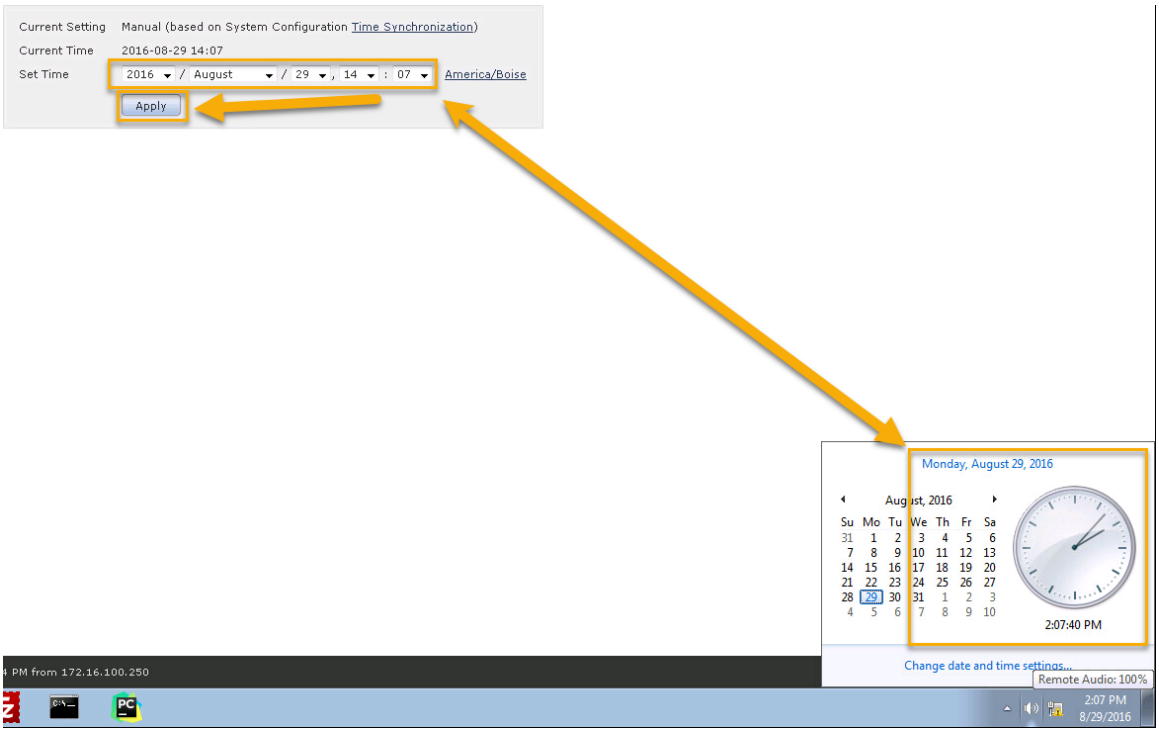


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

14. 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 13. Set the time



15. Return to the **Time Synchronization** menu tab again.

16. Ensure that **Serve Time via NTP** is enabled (thus making the FMC an NTP server).

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

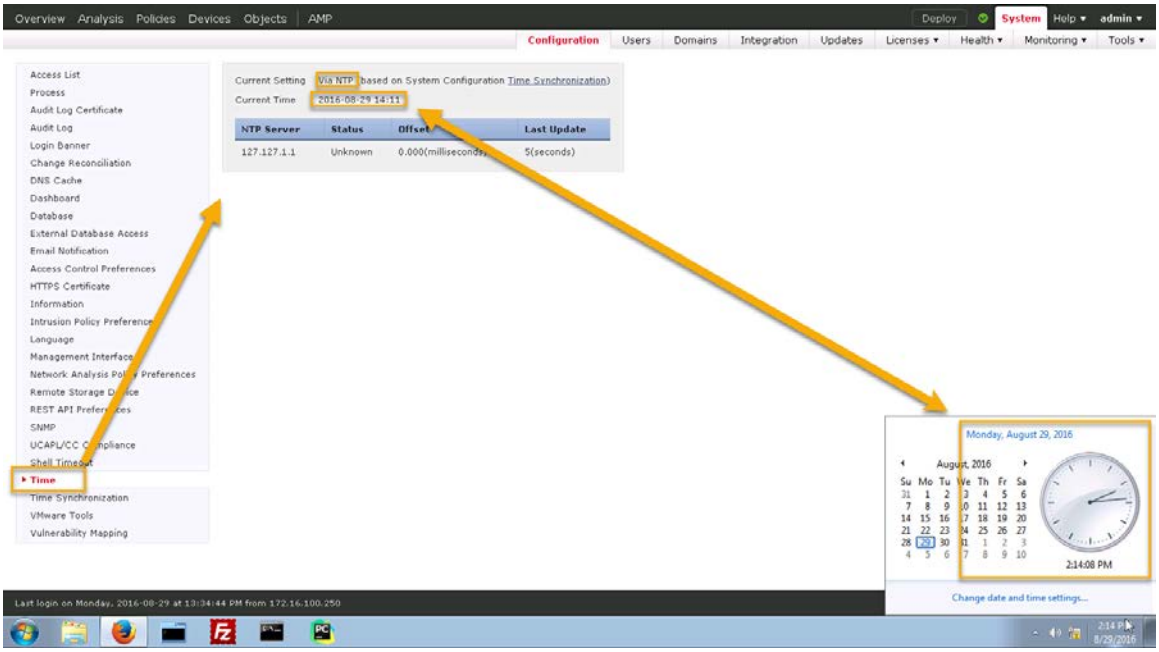
17. Click the **Via NTP from** radio button and click **Save**. (The default NTP server list is “0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, 3.sourcefire.pool.ntp.org”.) Notice how you can set multiple NTP server sources by separating them by a comma.

Figure 14. Back to NTP-based time



18. 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 15. Double checking your time work

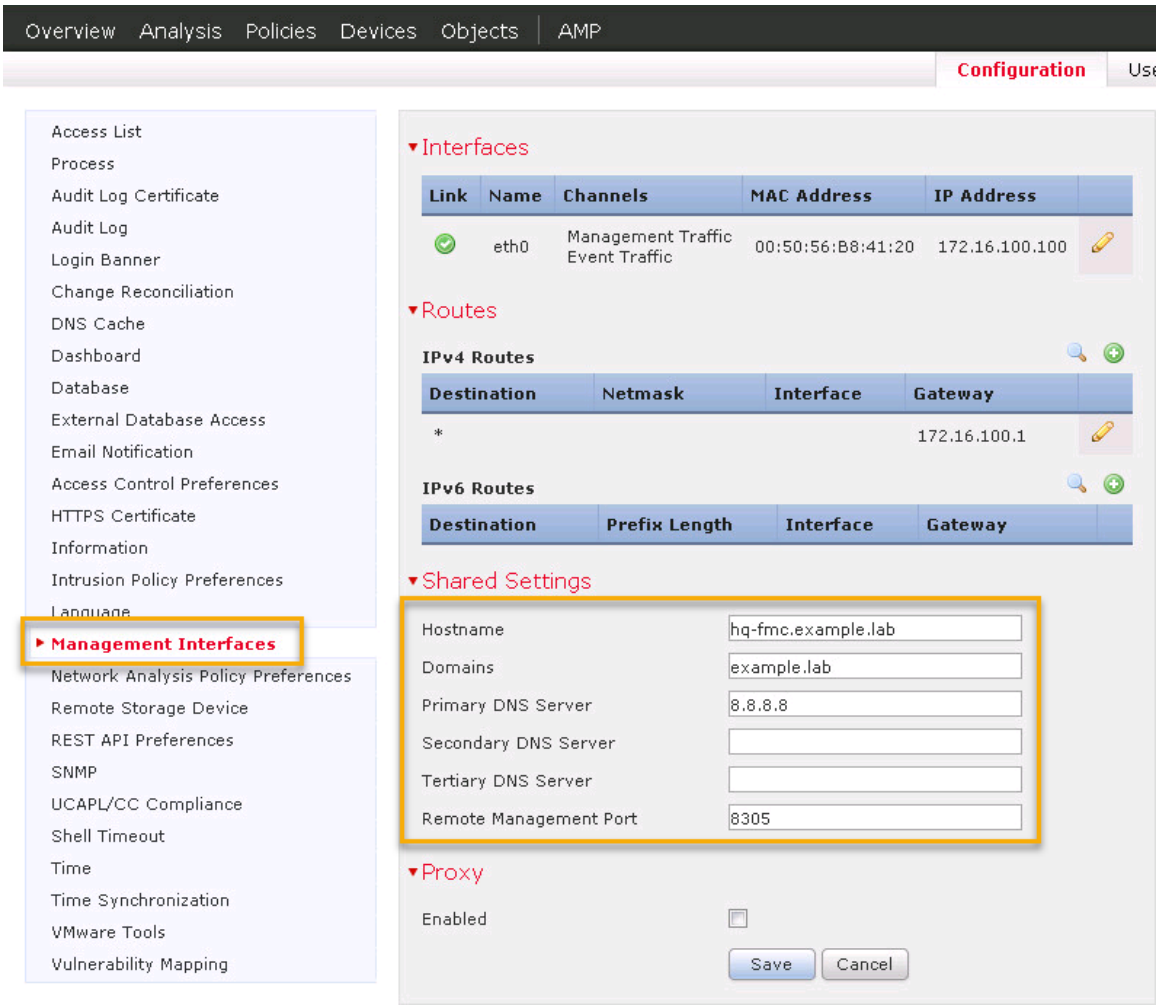


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 16. Management Interface Stuff



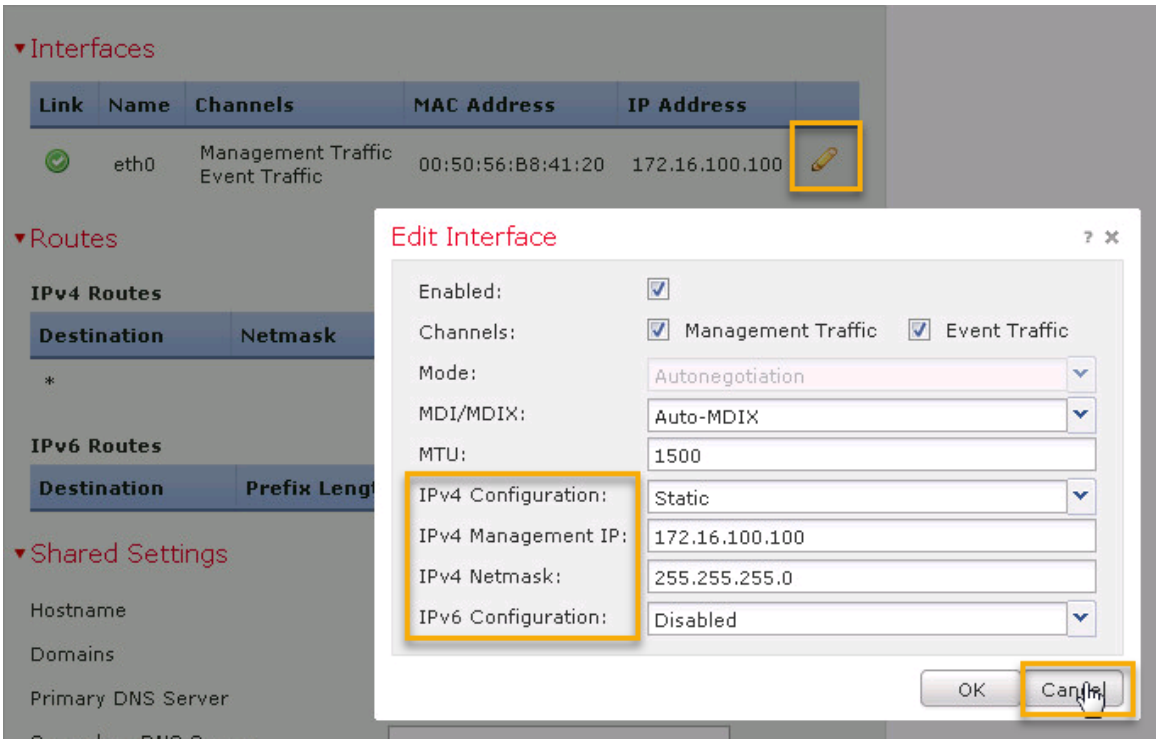
The Remote Management Port is the TCP port used to communicate with the devices that this FMC manages.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

21. 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.
22. Click **Cancel**.

Figure 17. Change IPv4/IPv6 addressing of FMC

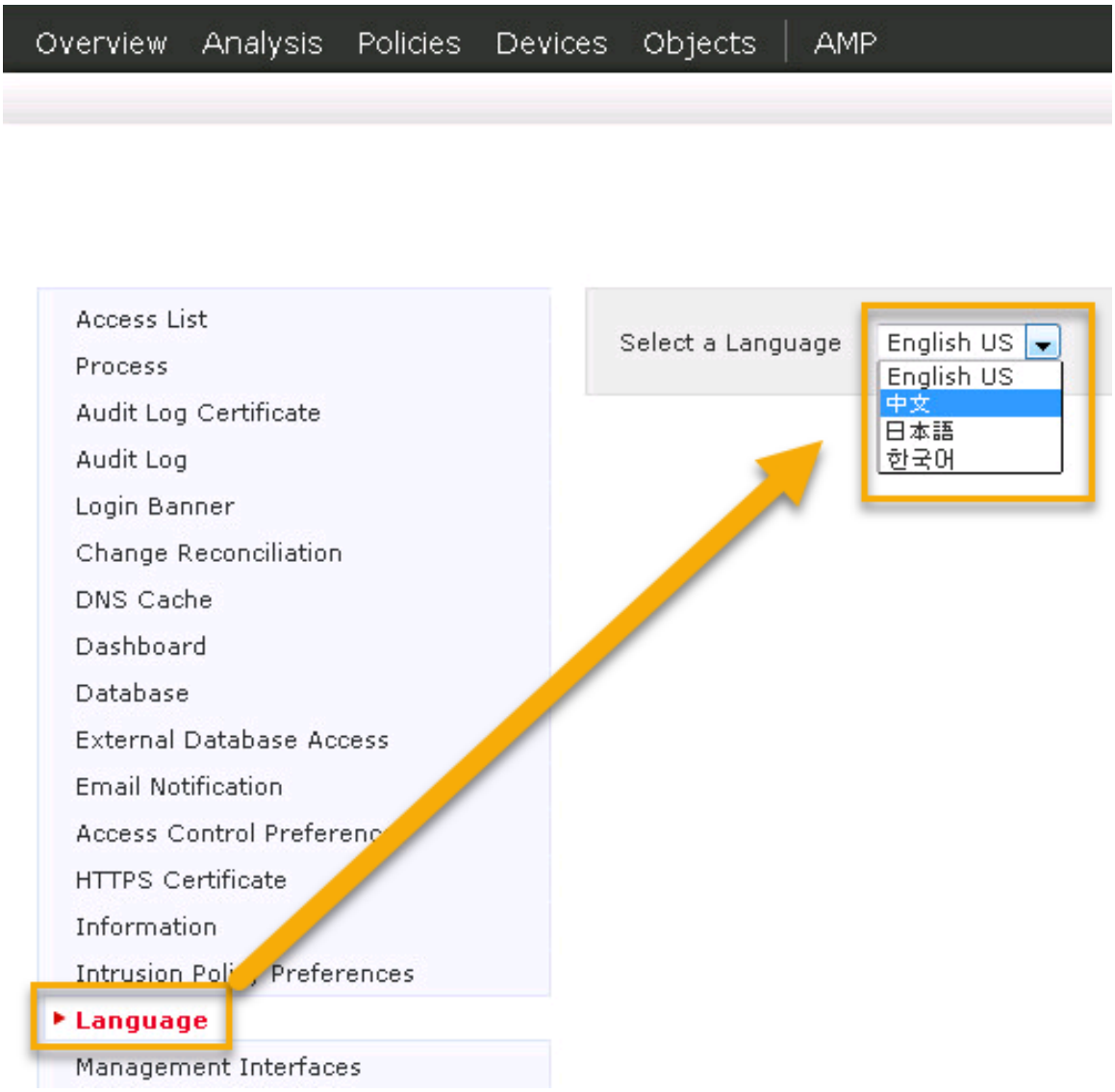


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 18. Language options for FMC

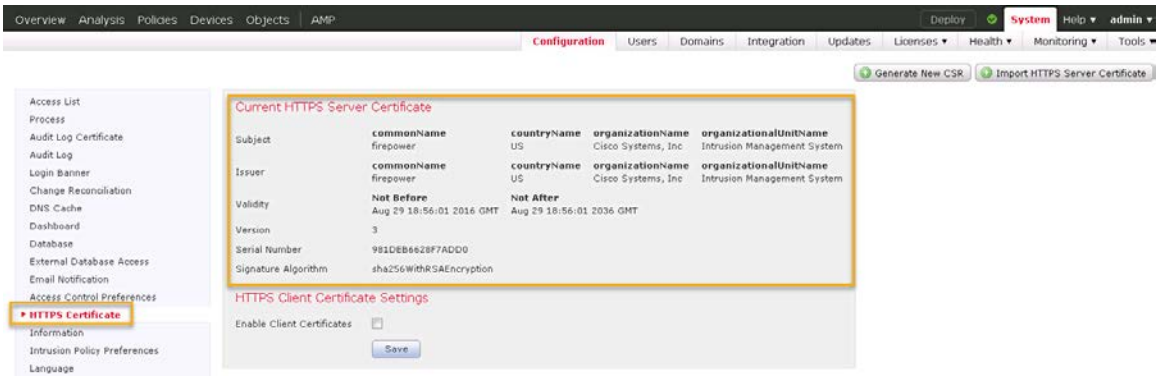


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

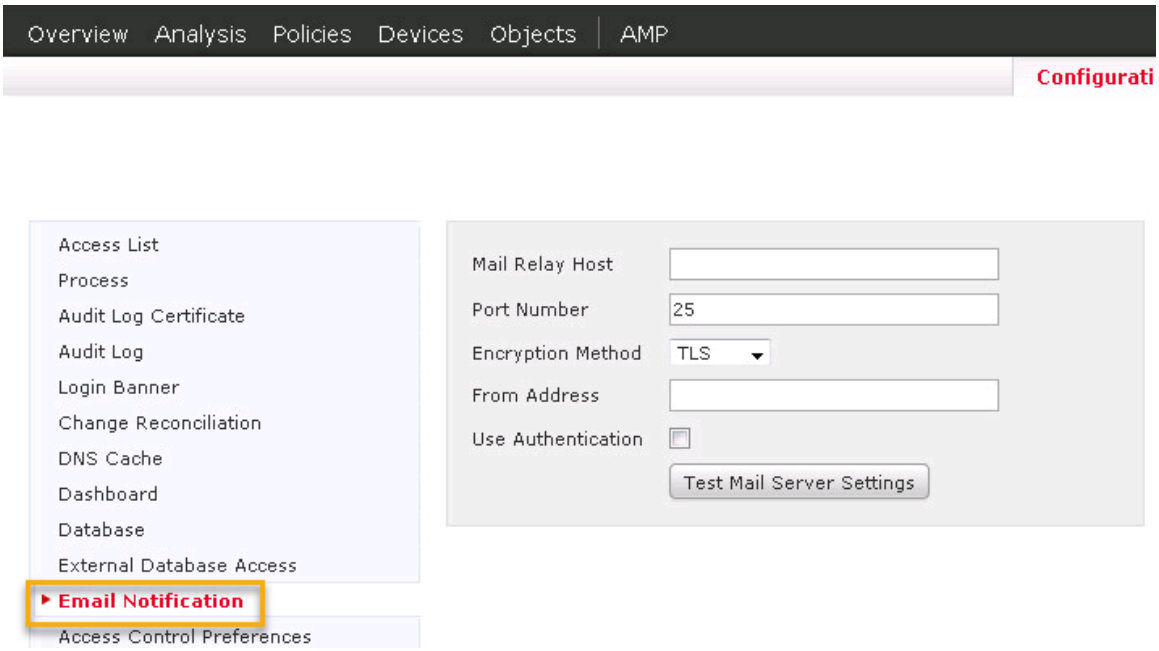
25. Select the **HTTPS Certificate** tab from the left column of menu items.
26. This page takes **a long time** to load but this is where you can install a legitimate certificate instead of using the self-signed one that is used by default.

Figure 19. Set up new SSL Certificates for FMC



27. Select the **Email Notification** tab from the left column of menu items.
28. 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 20. You'd configure an email server here

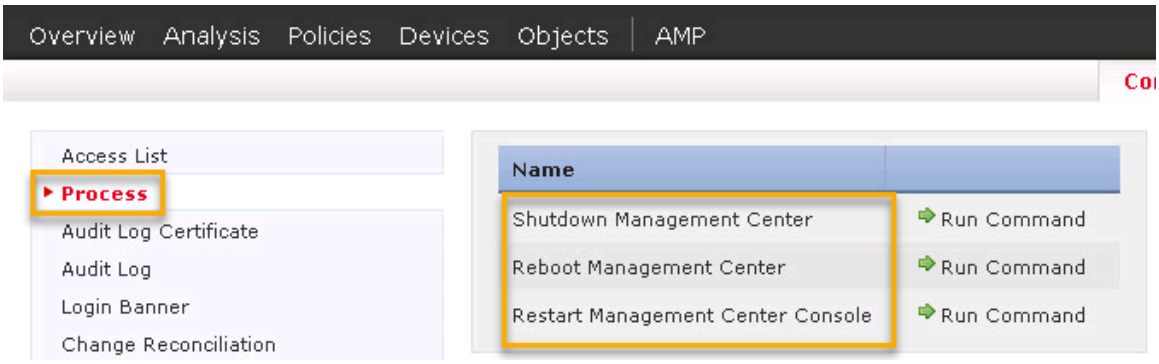


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

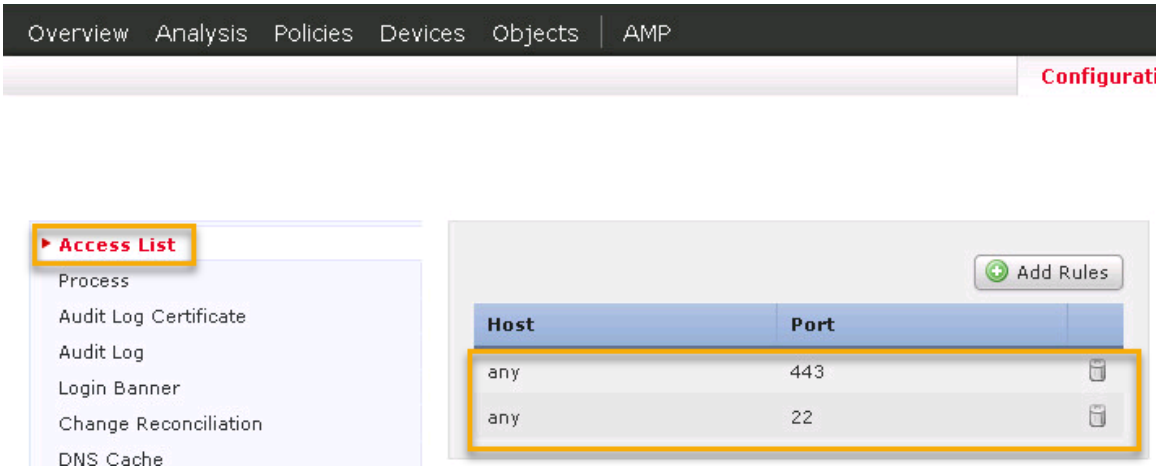
29. Select the **Process** tab from the left column of menu items.
30. This is where you can gracefully shutdown, reboot, or restart FMC services.

Figure 21. Commands to shutdown/reboot FMC



31. Finally, select the **Access List** tab from the left column of menu items.
32. This is where you can limit/control what IPs have access to the FMC.

Figure 22. ACLs for FMC Access



33. Navigate to **System > Users**.

Figure 23. Navigate to Users page



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

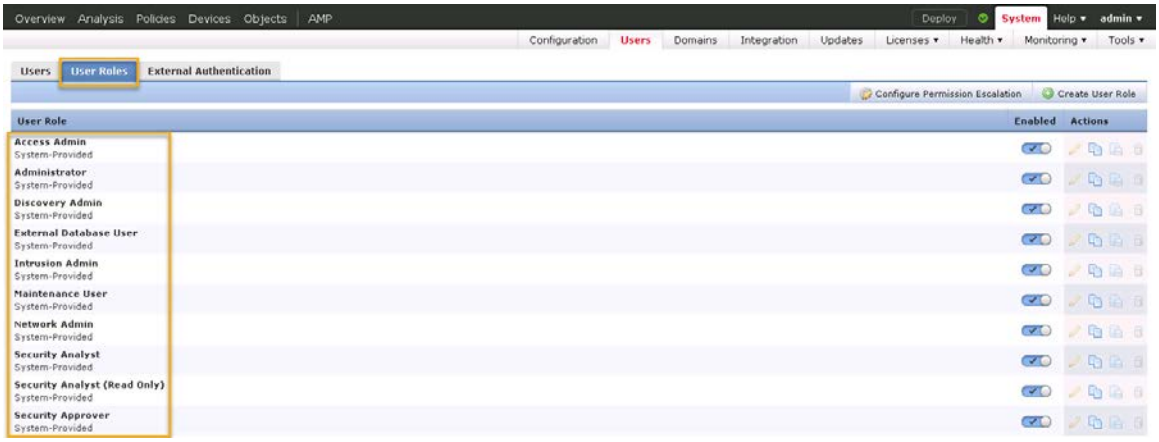
34. On the **Users** tab is a listing of all the locally configured users. As you can see only the “admin” user is configured by default. Later in the lab you will create a new user by returning to this page.

Figure 24. Users tab



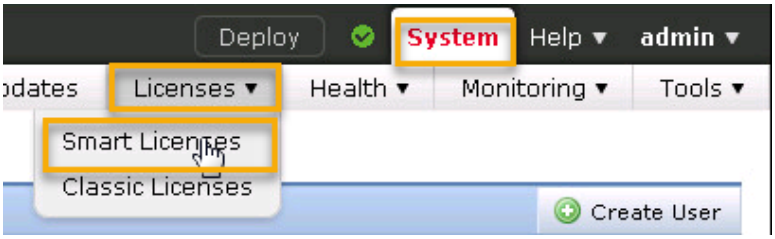
35. Click the **User Roles** tab. Though it is beyond the scope for this lab you have a wide range of predefined user roles to use should you want to.

Figure 25. User Roles tab



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

Figure 26. Navigate to Smart Licenses

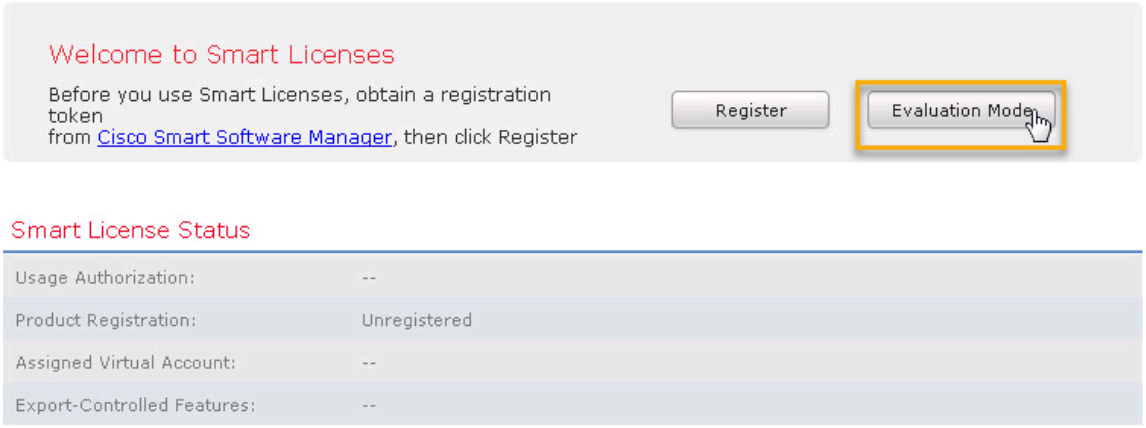


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

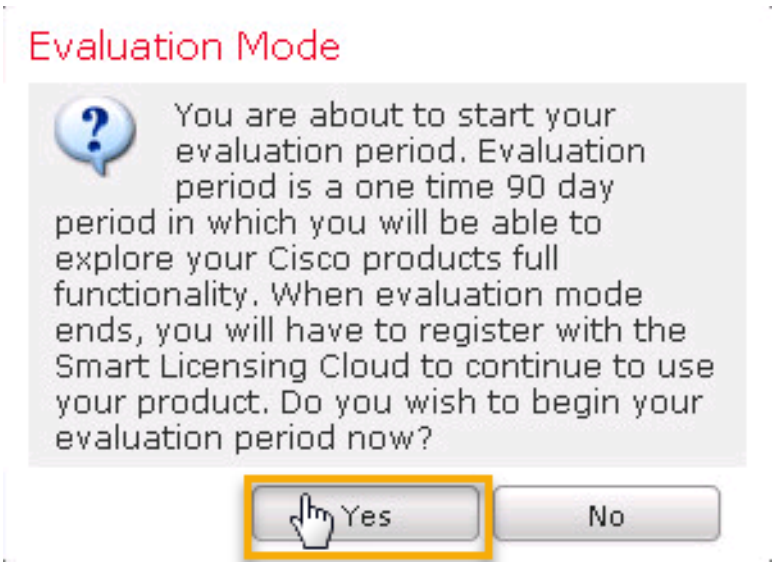
37. Normally this is where you'd register your FMC with Cisco to get its assigned licenses. In the lab you are going to use the evaluation licenses. So, click **Evaluation Mode**.

Figure 27. Enable Eval Licenses



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

Figure 28. Click Yes

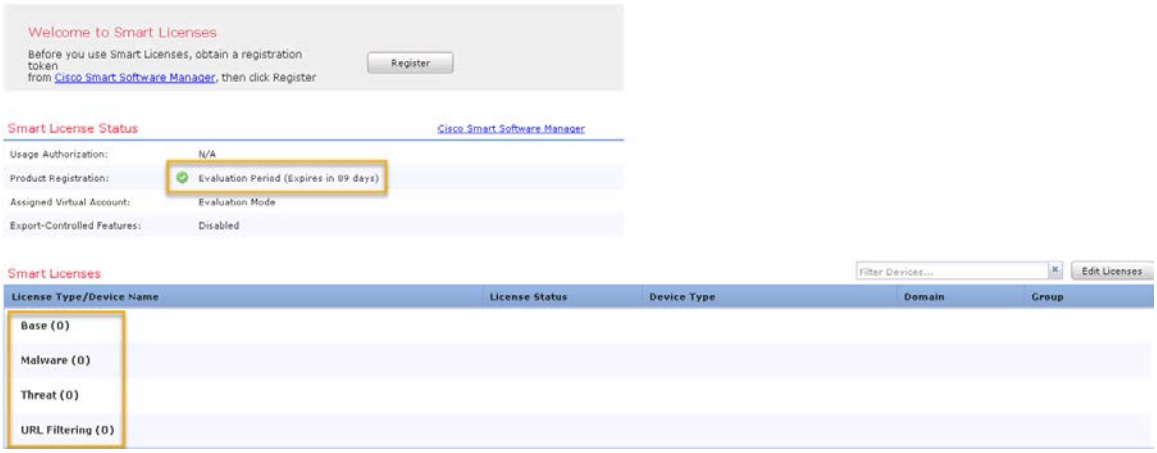


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

39. 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 29. List of Smart License



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: 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

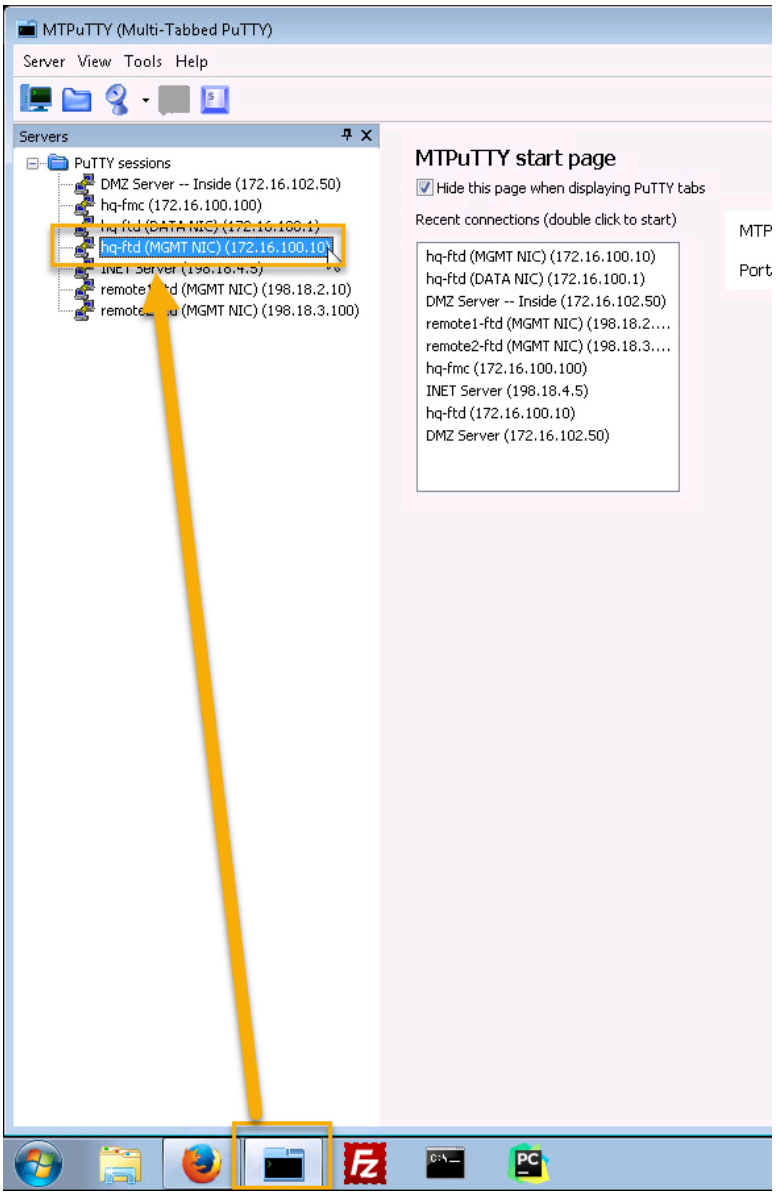
The hq-ftd device has its management interface pre-configured for you with an IP address (172.16.100.10). This will allow us to access the FTD via SSH from hq-wkst as well as allow this FTD to communicate with hq-fmc.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

1. On **hq-wkst** open up **MTPuTTY** and double-click the **hq-ftd (MGMT NIC)** link.

Figure 30. SSH to hq-ftd



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

2. Click **Yes** to the Security warning and **login** as **admin**/**Admin123**. (The Security warning appears because the FMC and FTD devices have been deployed over and over during the development of this lab but the original SSH certificate is stored in the PuTTY sessions.)

Figure 31. Accept New ssh-rsa key

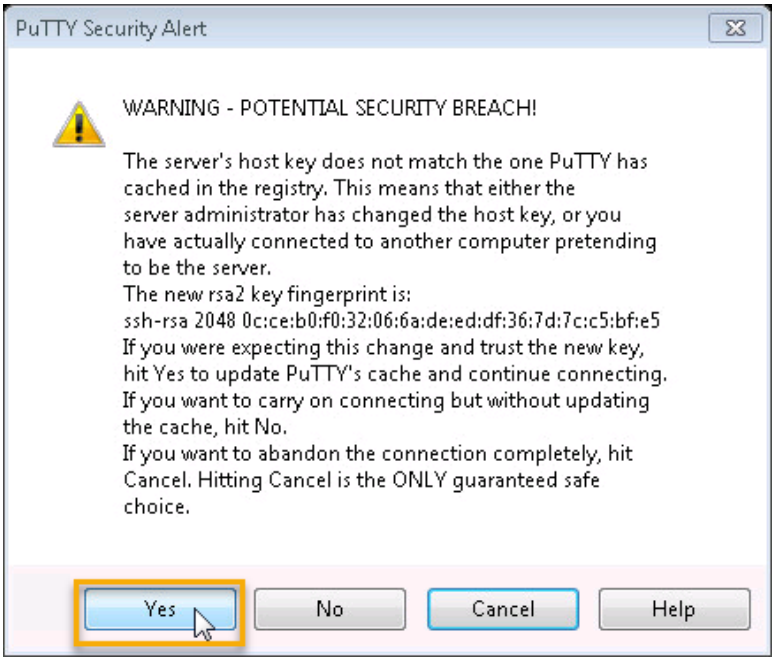
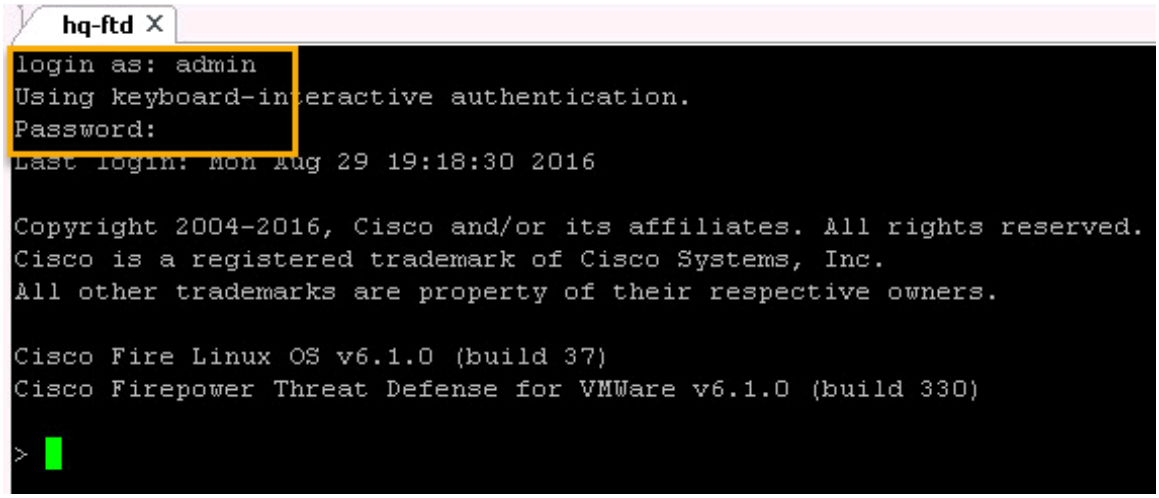


Figure 32. Log into hq-ftd

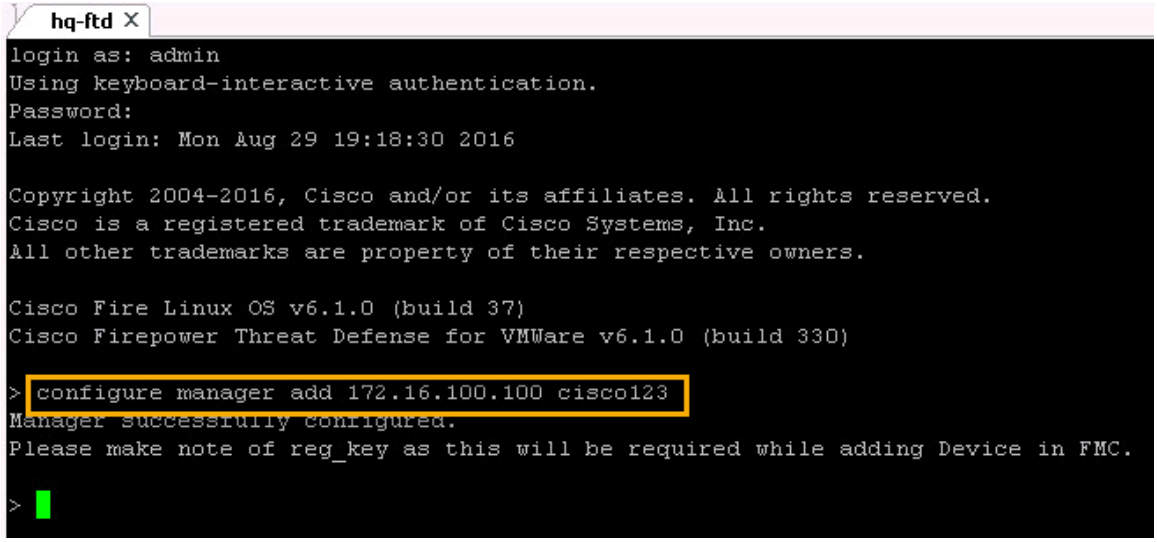


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

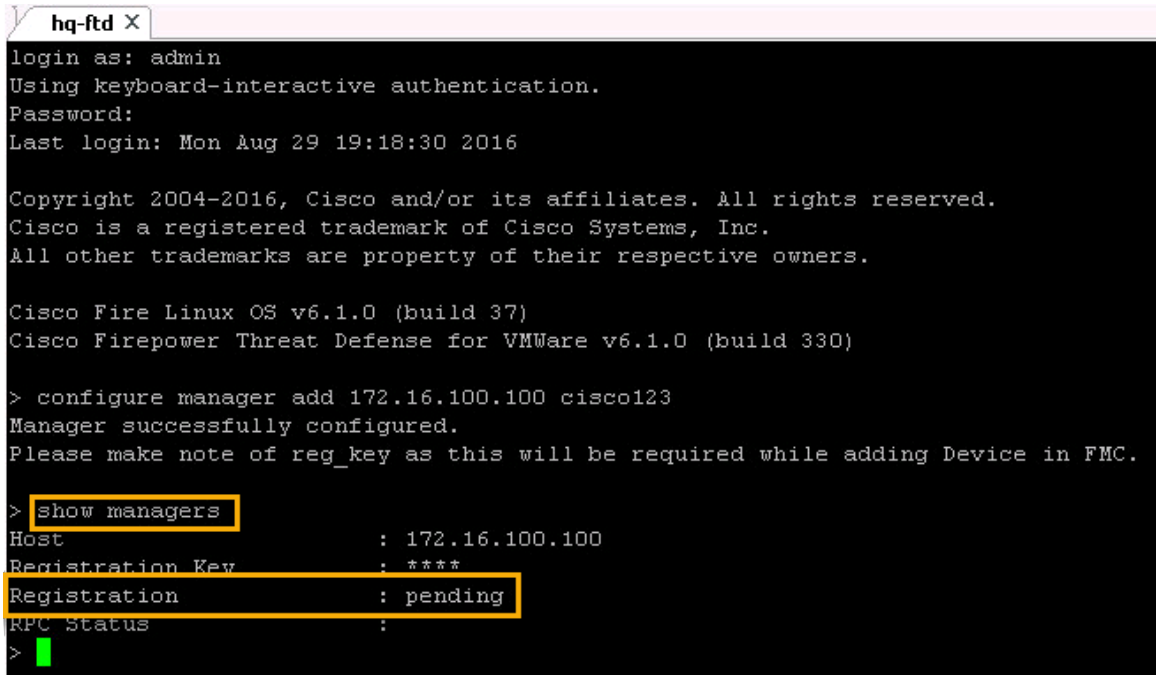
3. To configure hq-ftd to use your recently configured FMC as its manager issue this command: **configure manager add 172.16.100.100 cisco123**. (The “cisco123” is a pre-shared key and can be any alphanumeric sequence you desire. Remember it as you’ll need it for the FMC side of the configuration.)

Figure 33. Register FTD to FMC



4. 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 34. Show managers



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

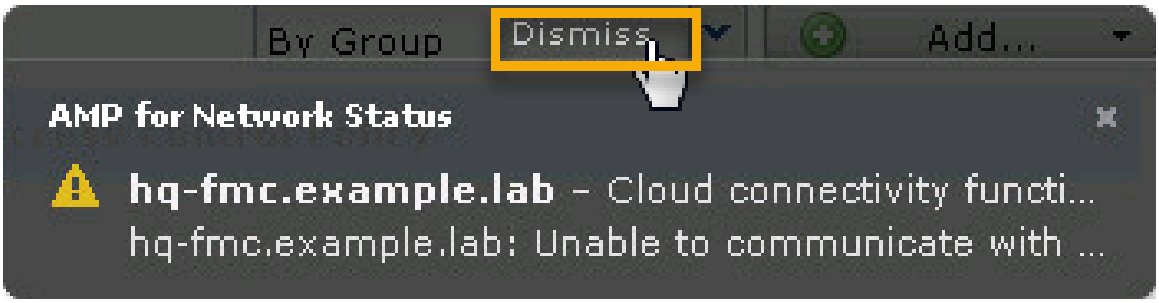
5. Return to the FMC management page to complete the addition of this FTD to the FMC. Navigate to **Devices > Device Management**.

Figure 35. Navigate to Device Management



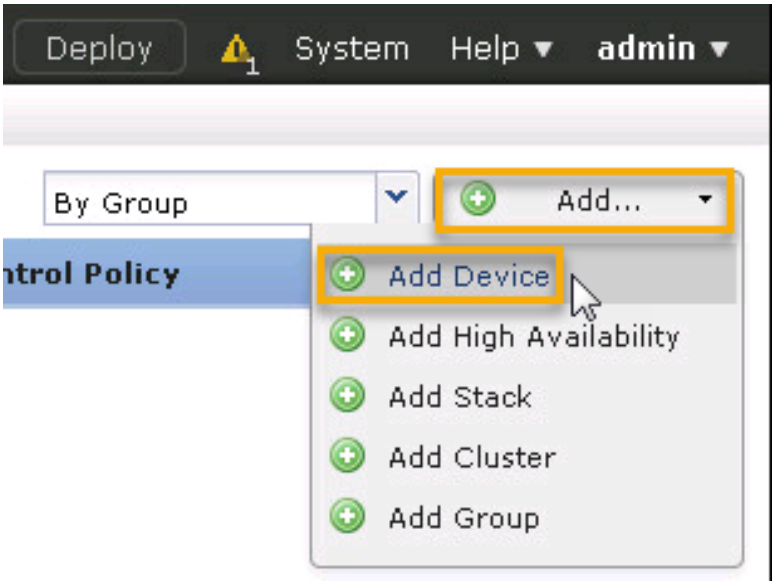
Note: Sometimes there might be a notification window that covers over the section of the screen you need to access. ALWAYS click Dismiss to remove the notification. If those messages are important you can find them elsewhere. During this lab they are just a nuisance.

Figure 36. Annoying Popup Notification Window.



6. 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 37. Add a new FTD device



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

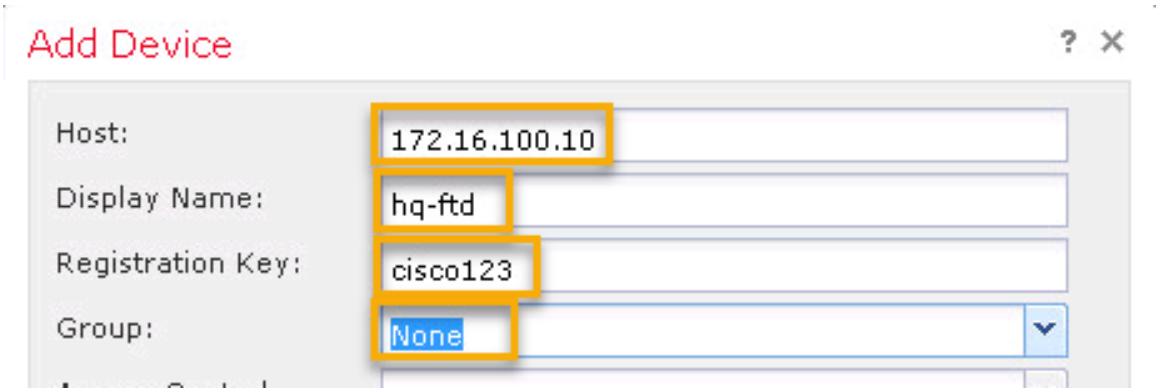
    a. Host: **172.16.100.10** (You could use a DNS name here but you don't have one set up. Also take note that this is the FTD's management IP address and not any of the data interface's IP addresses, which aren't set up yet anyway.)

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

    c. Registration Key: **cisco123**

    d. Group: **None**

Figure 38. Part 1 of adding hq-ftd's information



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.

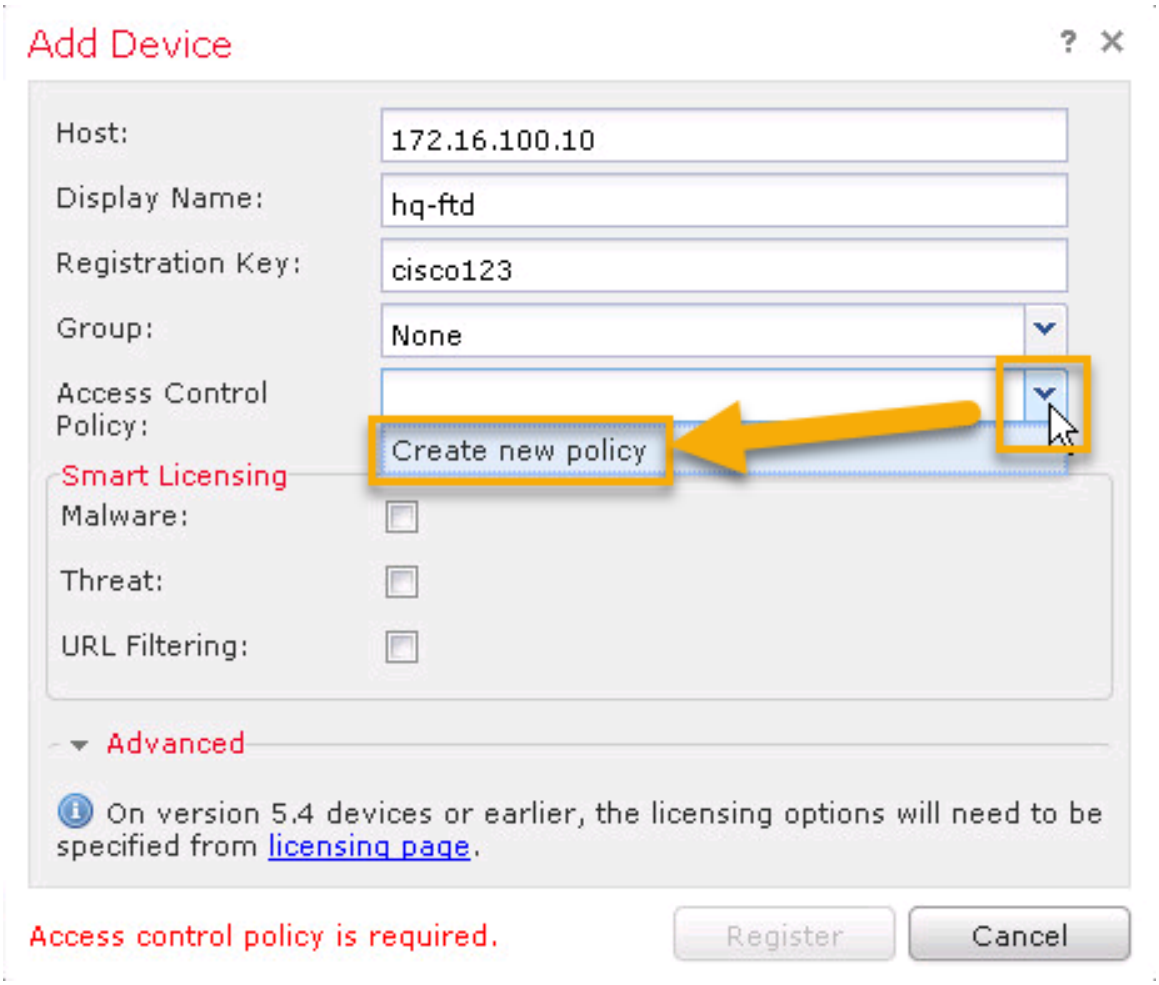
Note: The use of hierarchical policies is not necessarily a "best practices" method of using Access Control Policies. The intent here is to show off the capabilities of inheritance of policy rules (which will be shown later in the lab). There are many deployments where one Access Control Policy can be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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 39. Create new ACP

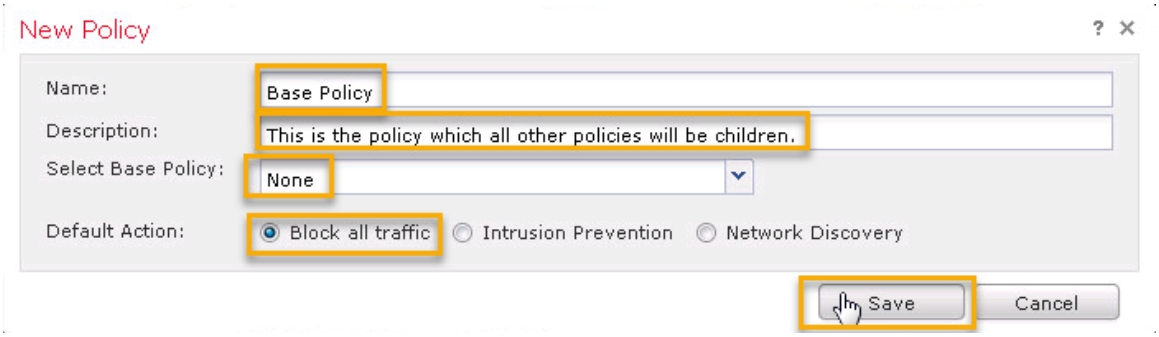


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

9. 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 40. Creating new ACP

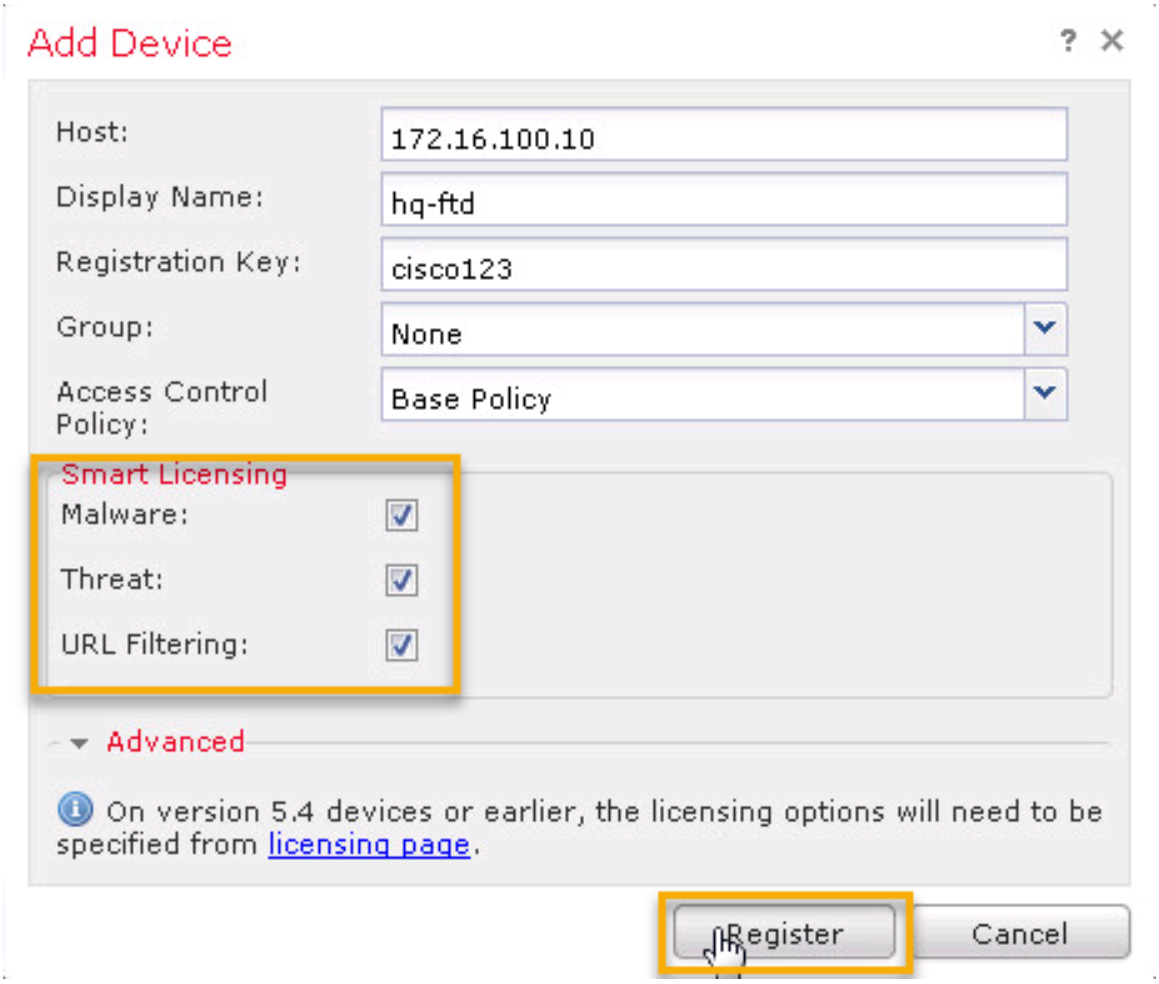


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

10. Smart Licensing: The evaluation mode gives us access to all the licensable options. **Check all the boxes** (Malware, Threat, and URL Filtering).
11. Click **Register**. The registration process can take a minute or two.

Figure 41. Enable all the licenses and click Register

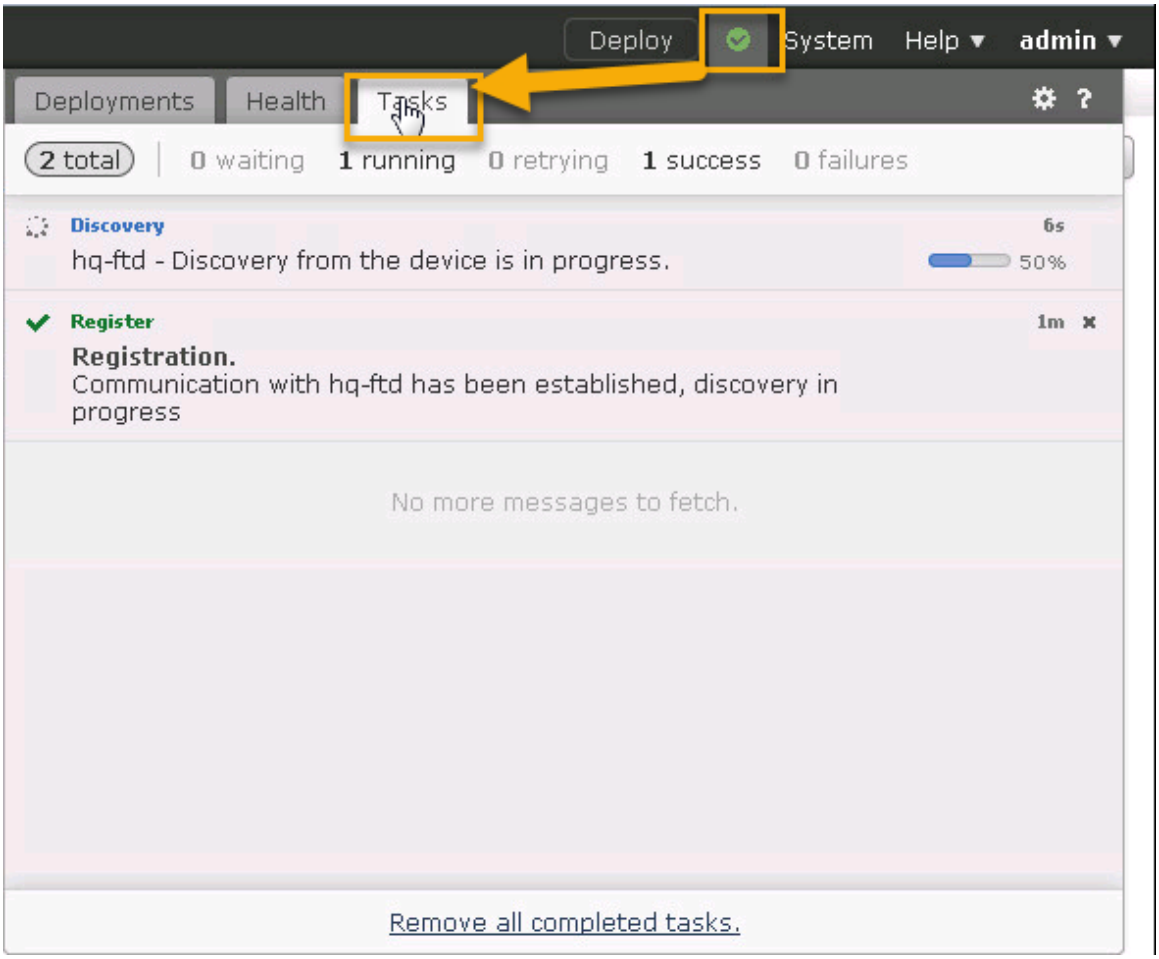


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

12. 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 42. The Message Center icon with tabs

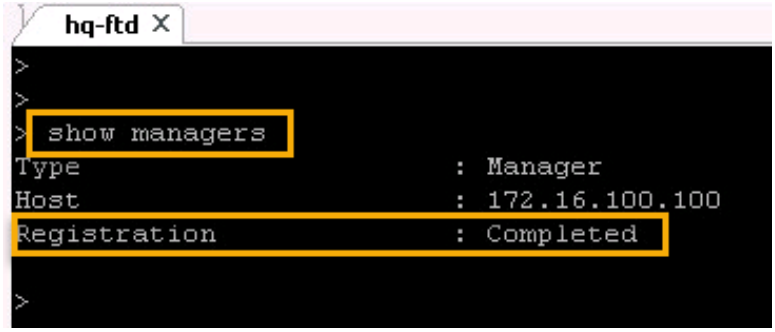


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

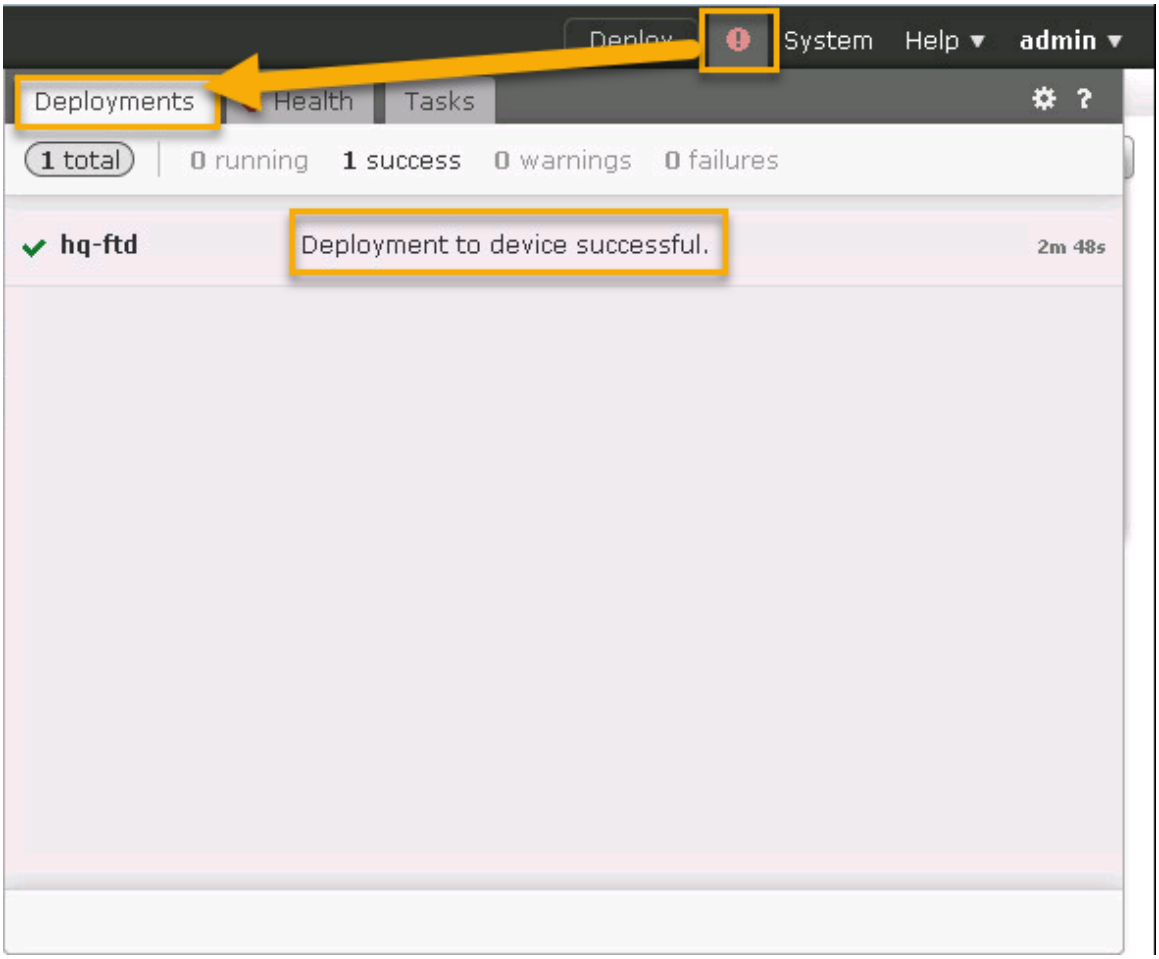
13. The registration process takes about 3-5 minutes. Once the hq-ftd device appears on the Device Management page return to the SSH window to hq-ftd and issue the command **show managers** again. Notice that the Registration status now shows Completed.

Figure 43. Show managers, again



14. 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 44. Message Center Deployment shows completed.



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

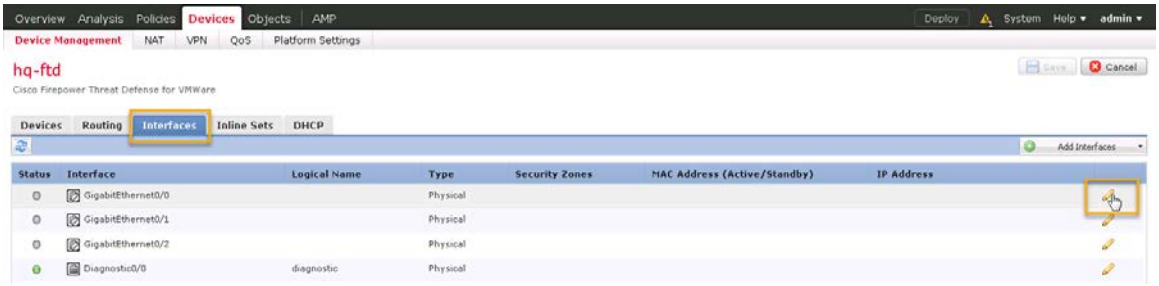
15. In case you browsed away, navigate to **Devices > Device Management**.
16. Once the hq-ftd device is available within the FMC click the **pencil icon** on the row associated with **hq-ftd**.

Figure 45. Edit hq-ftd



17. 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 46. Edit g0/0



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

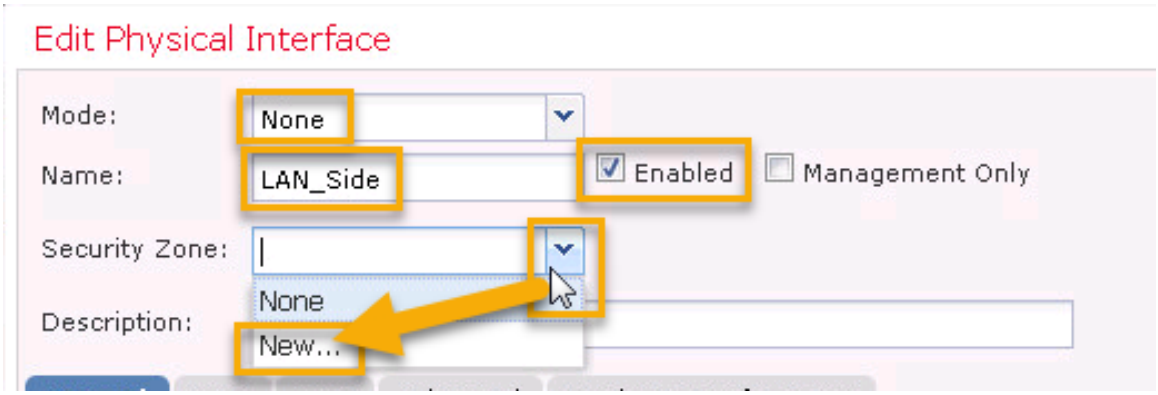
    a. Mode: **None**

    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.

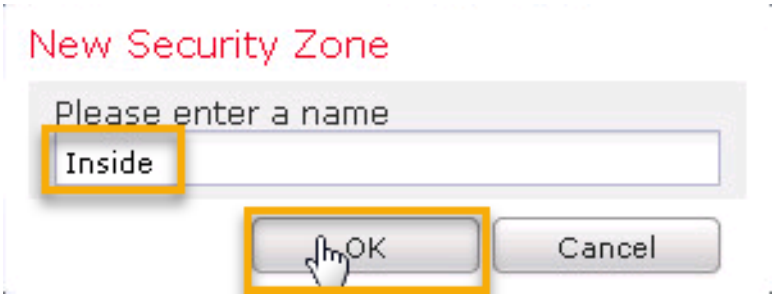
    d. Security Zone: From the dropdown options select **New…**

Figure 47. Part 1 of editing g0/0



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

Figure 48. Create Inside Zone

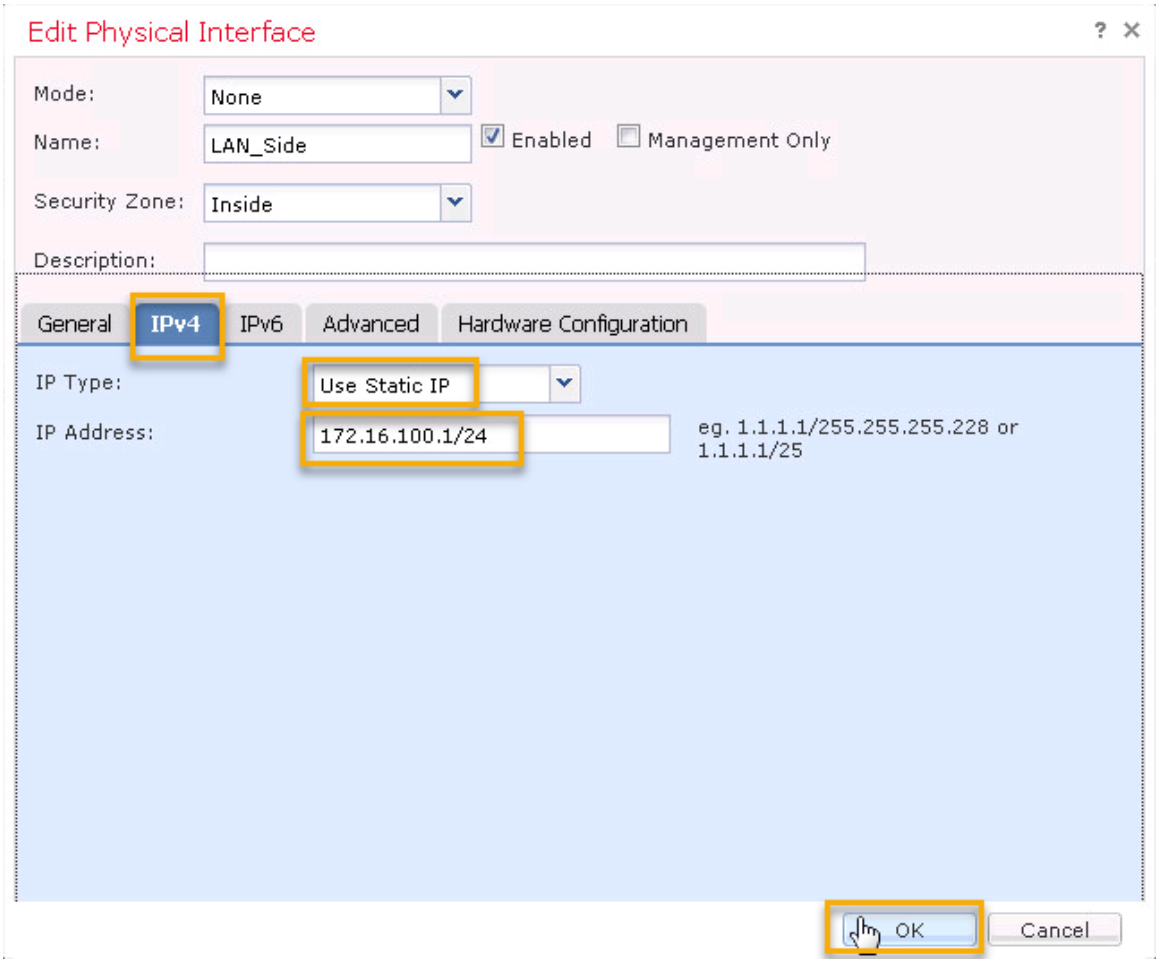


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

20. Click the **IPv4 tab**.
    a. IP Type: **Use Static IP**
    b. IP Address: **172.16.100.1/24**
21. Click **OK**.

Figure 49. Configure Data Plane IP and click OK

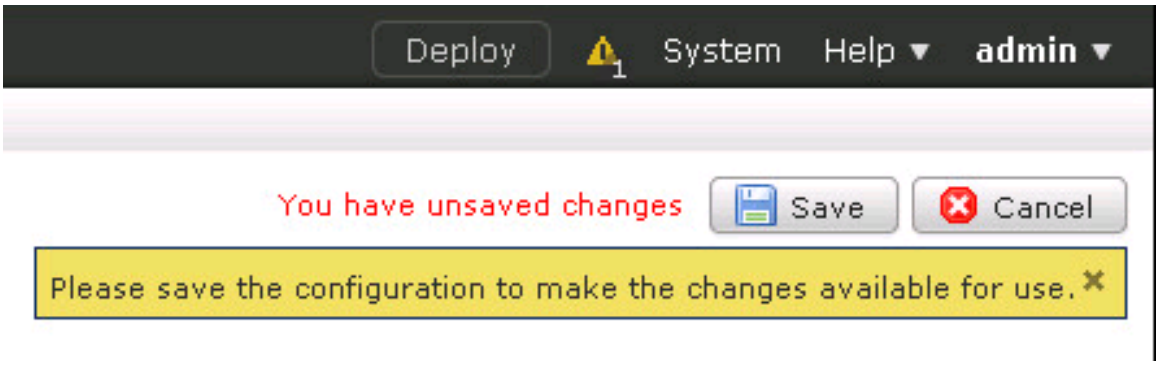


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

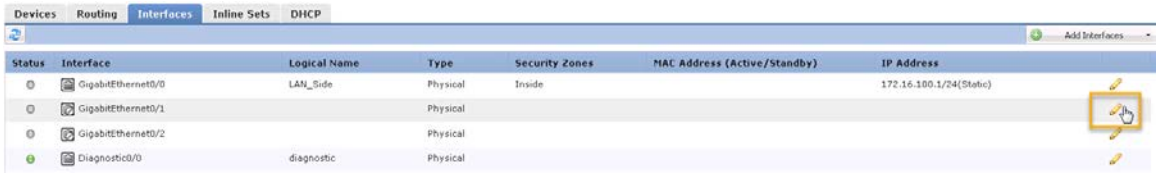
Notice the yellow text that now appears near the Save button. This is just a warning that you haven't saved these changes to the FMC, nor have these changes been pushed out to hq-ftd. Changes are cached locally in the browser until they are saved to the FMC. Then those changes will need to be deployed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

Figure 50. Yellow Warning



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

Figure 51. Edit g0/1



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

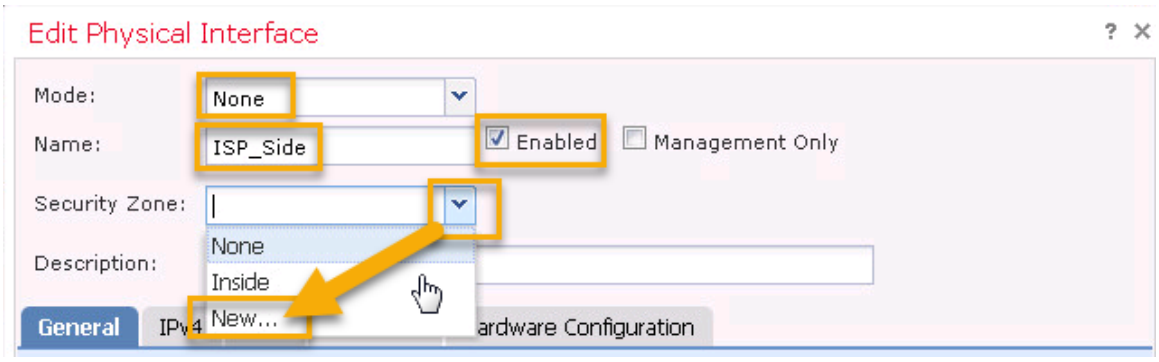
    a. Mode: **None**

    b. Name: **ISP_Side**

    c. Check the **Enabled** box.

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

Figure 52. Part 1 of editing g0/1

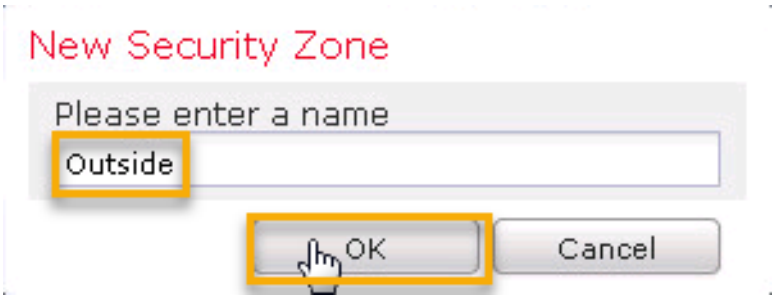


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

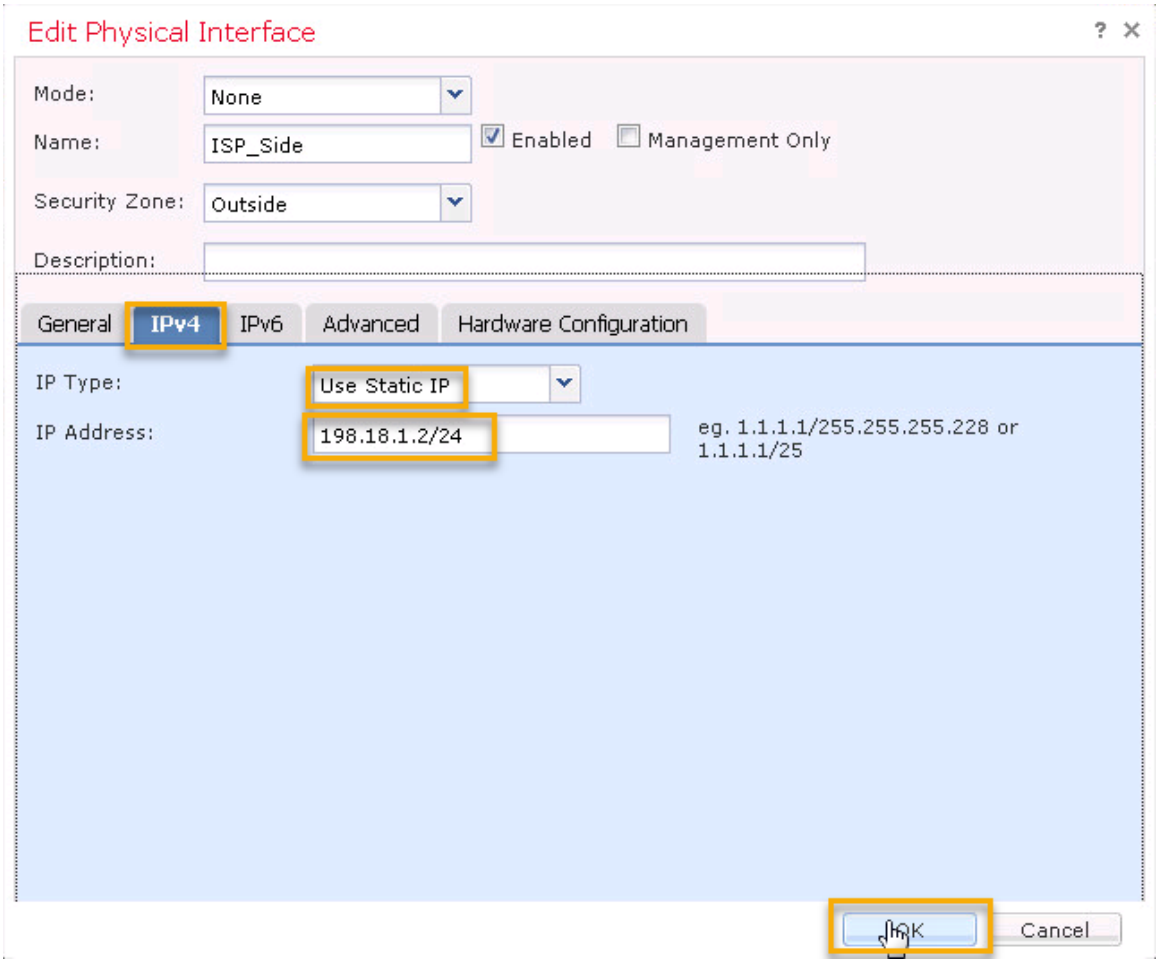
24. Create the zoned named **Outside** and click **OK**.

Figure 53. Create Outside zone



25. Click the **IPv4 tab**.
    a. IP Type: **Use Static IP**
    b. IP Address: **198.18.1.2/24**
26. Click **OK**.

Figure 54. Configure g0/1 IP and click OK

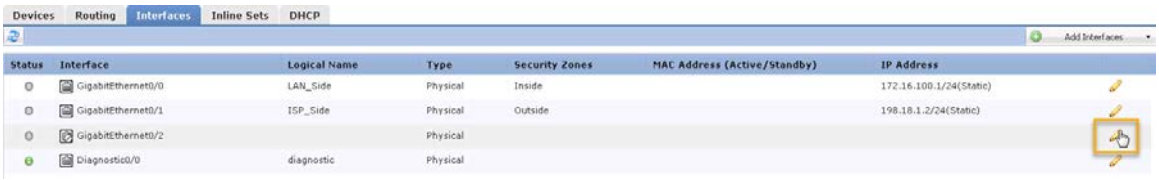


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 55. Edit g0/2



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

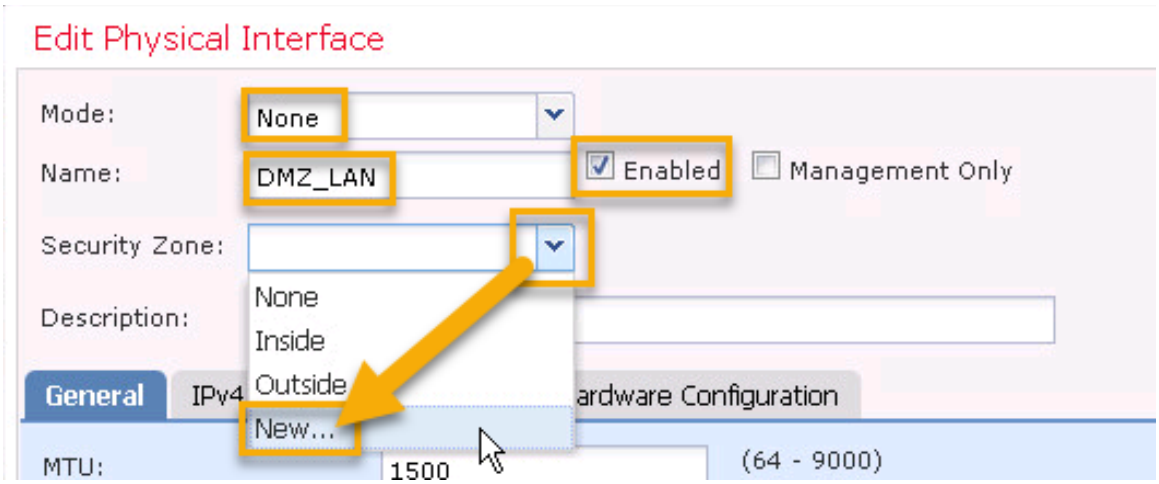
    a. Mode: **None**

    b. Name: **DMZ_LAN**

    c. Check the **Enabled** box.

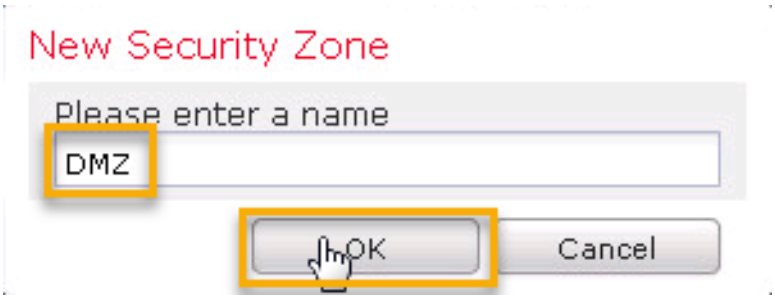
    d. Security Zone: From the dropdown options select **New…**

Figure 56. Part 1 of configuring g0/2



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

Figure 57. Create DMZ zone

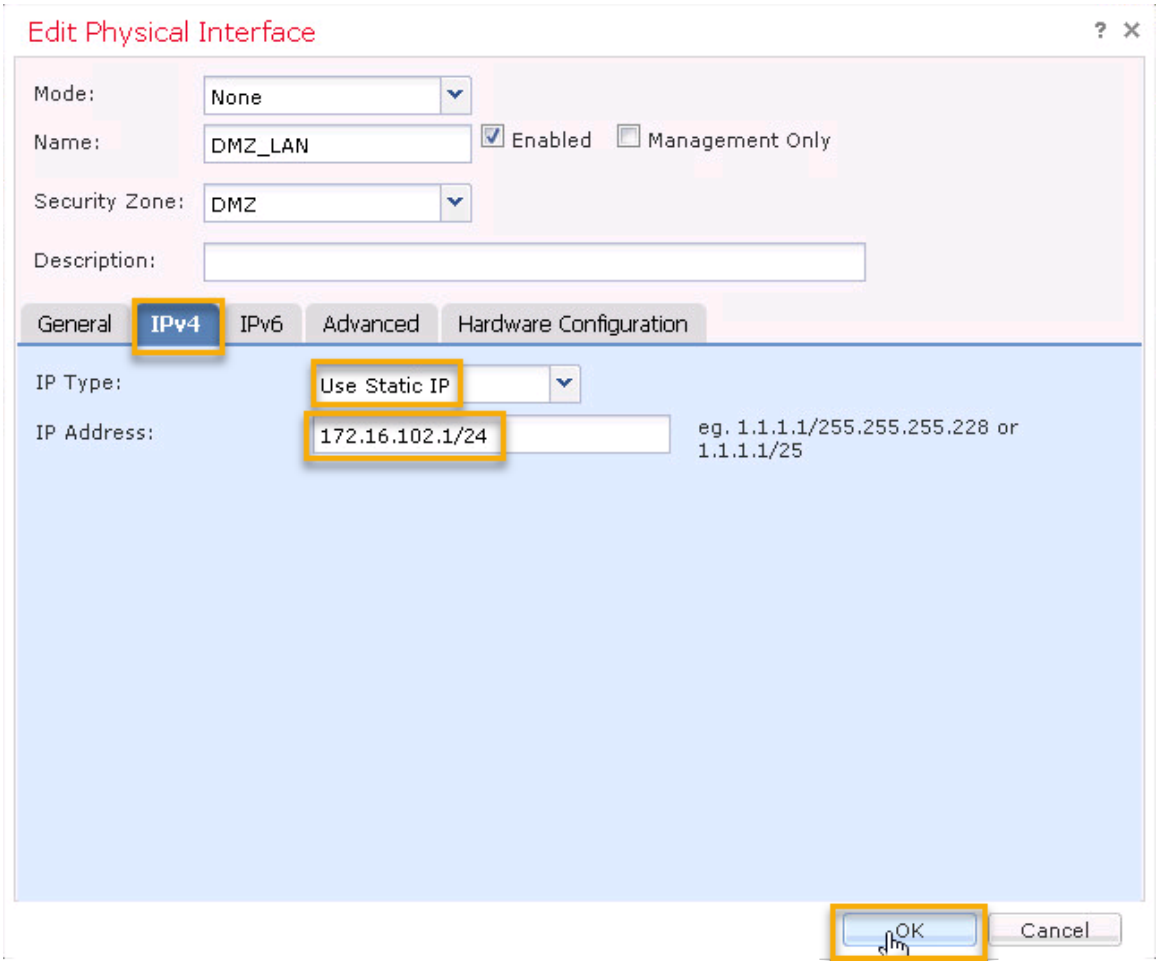


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

30. Click the **IPv4 tab**.
    a. IP Type: **Use Static IP**
    b. IP Address: **172.16.102.1/24**
31. Click **OK**.

Figure 58. Add g0/2 IP and click OK

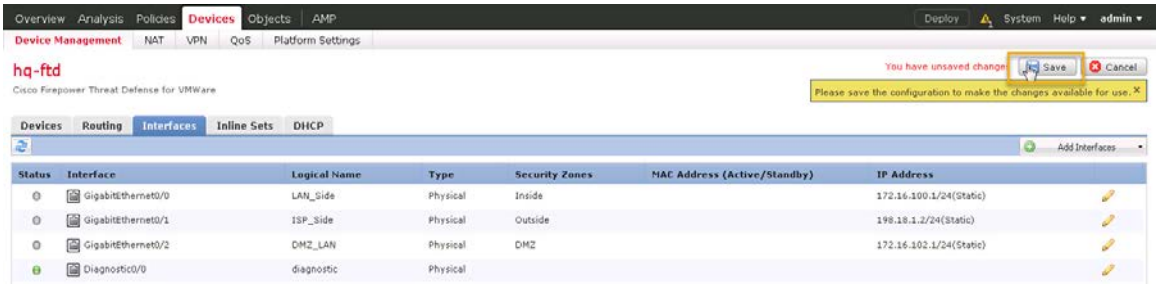


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

32. 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.

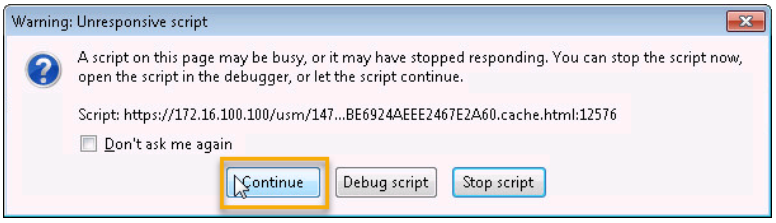
Figure 59. Hq-ftd interfaces configured



33. Click the **Routing tab**.

It is possible that you'll get the following error 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 **Continue** to remove the message.

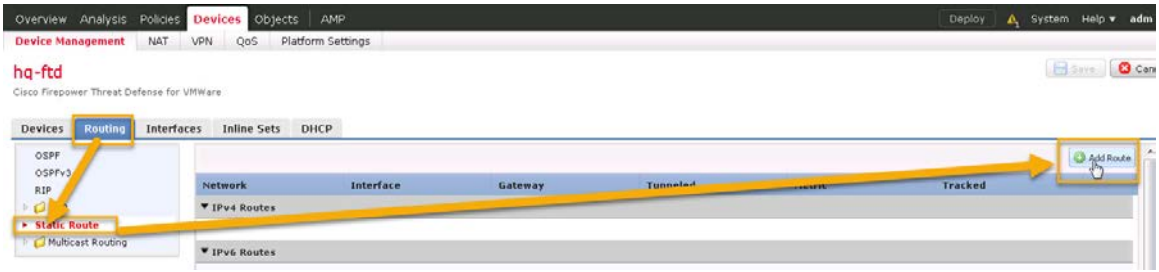
Figure 60. Possible error when clicking routing tab



34. 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.

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

Figure 61. Add Static Route

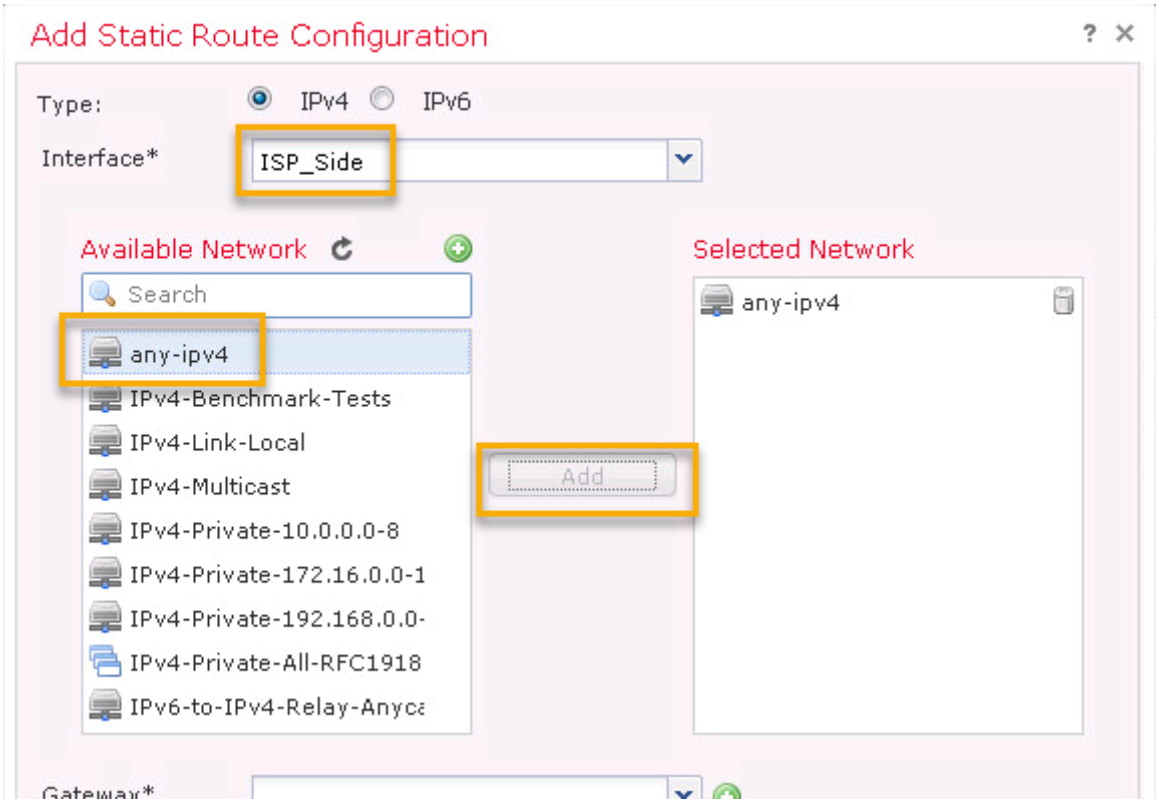


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

36. Using the dropdown for the **Interface** option select **ISP_Side**.
37. 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 62. Part 1 of adding static route

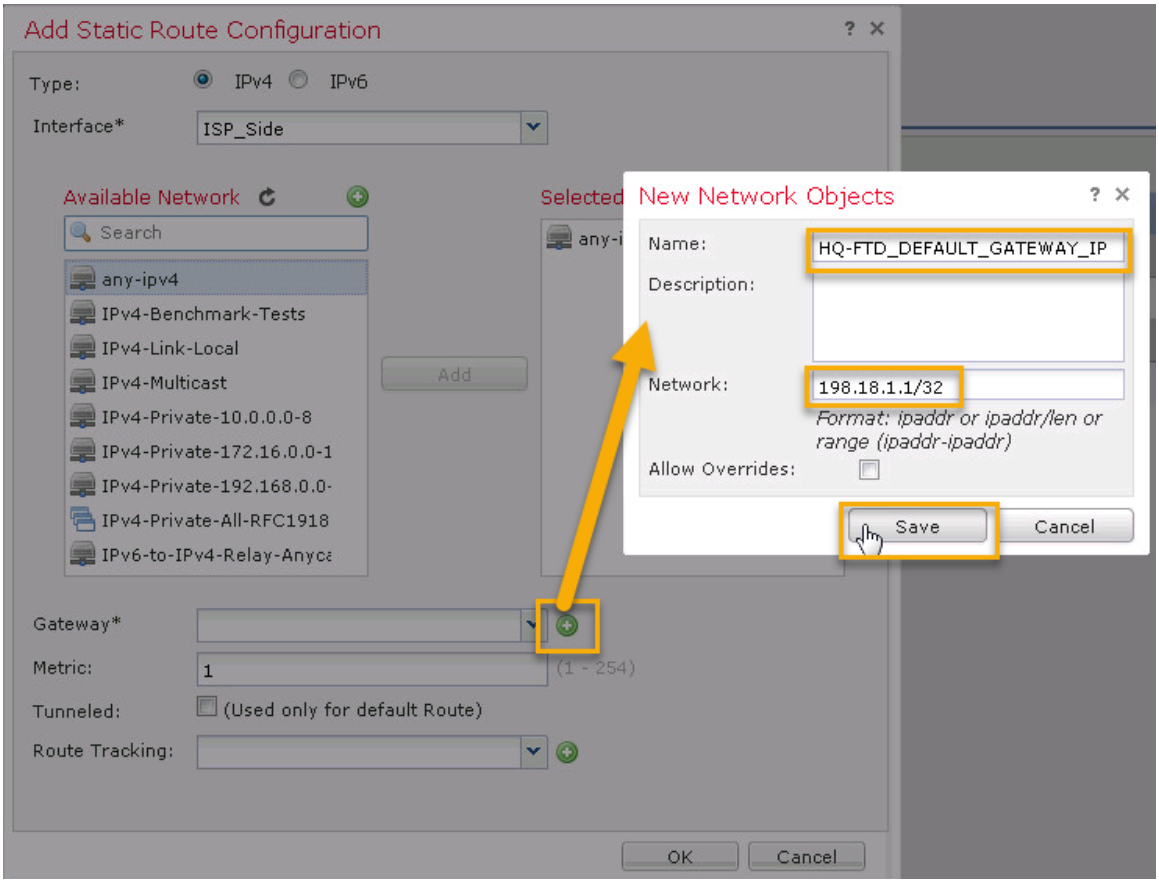


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

38. 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 63. Adding Network Object



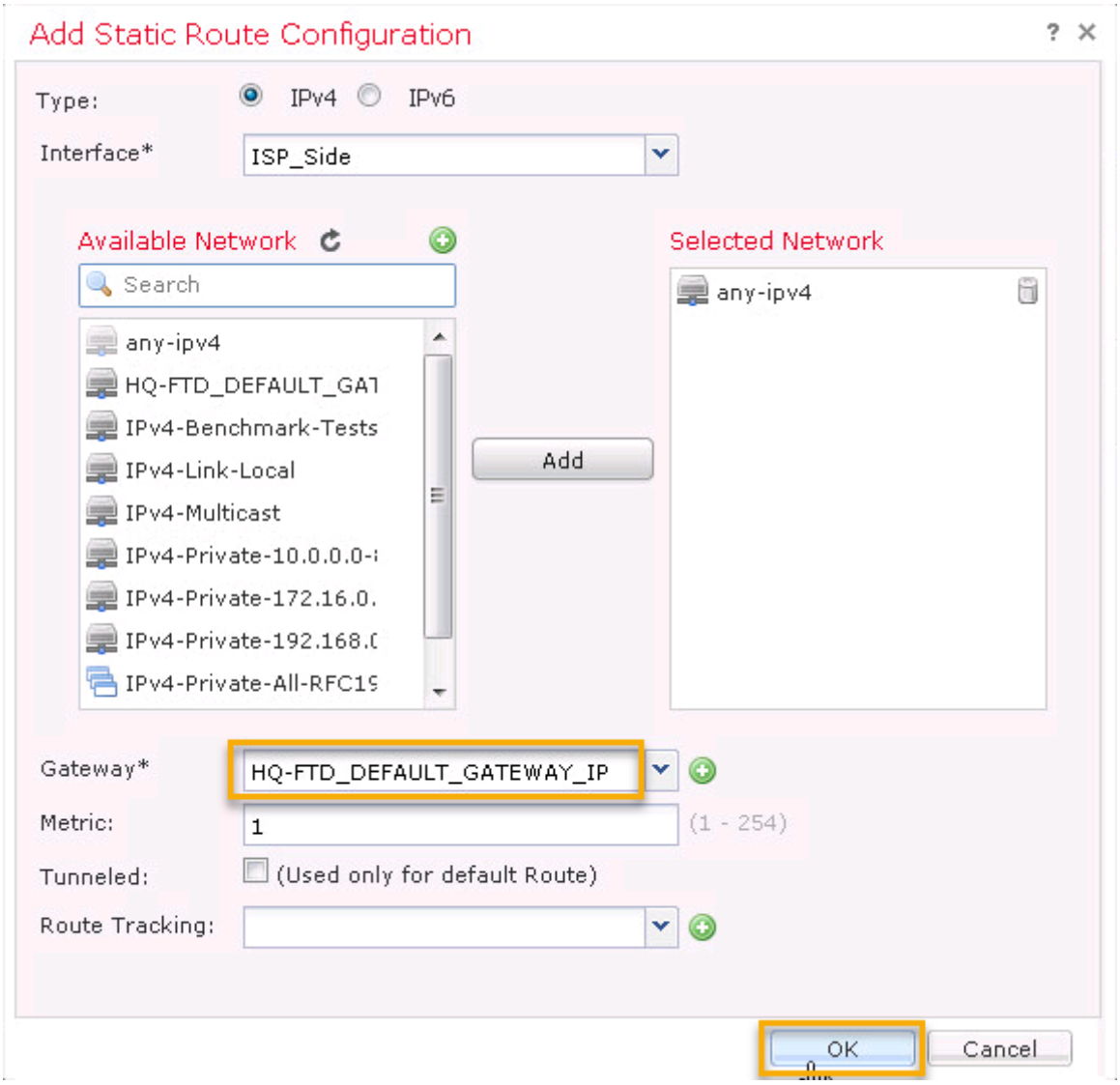
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

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

Figure 64. Finish adding static route

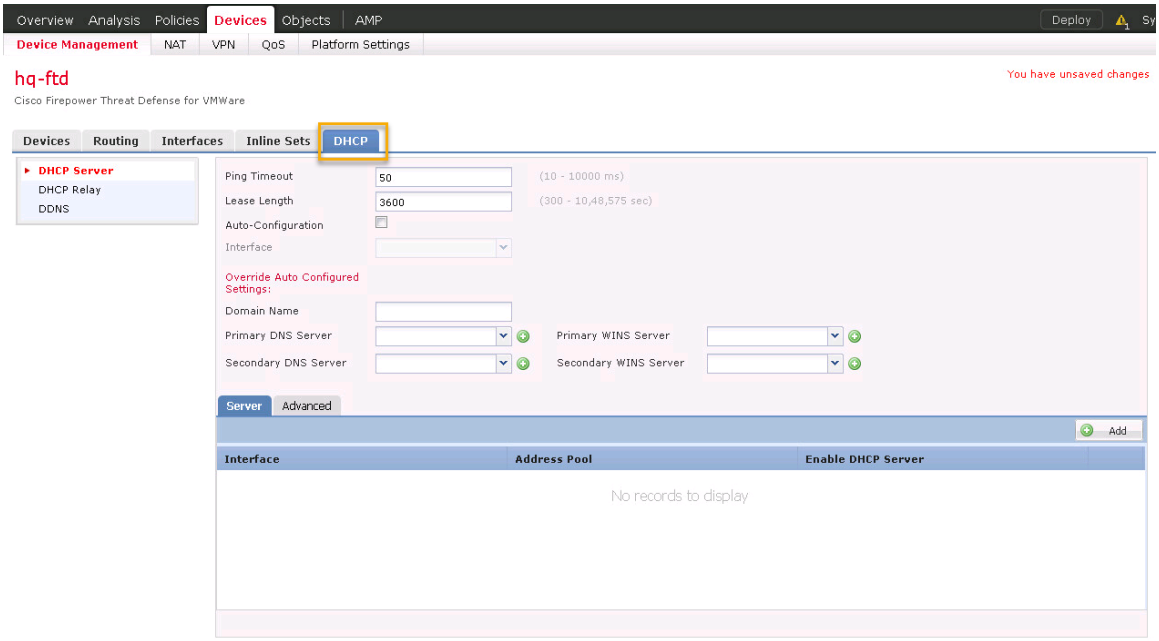


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

41. Click the **DHCP tab**.
42. 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 65. Where to set up DHCP, if needed

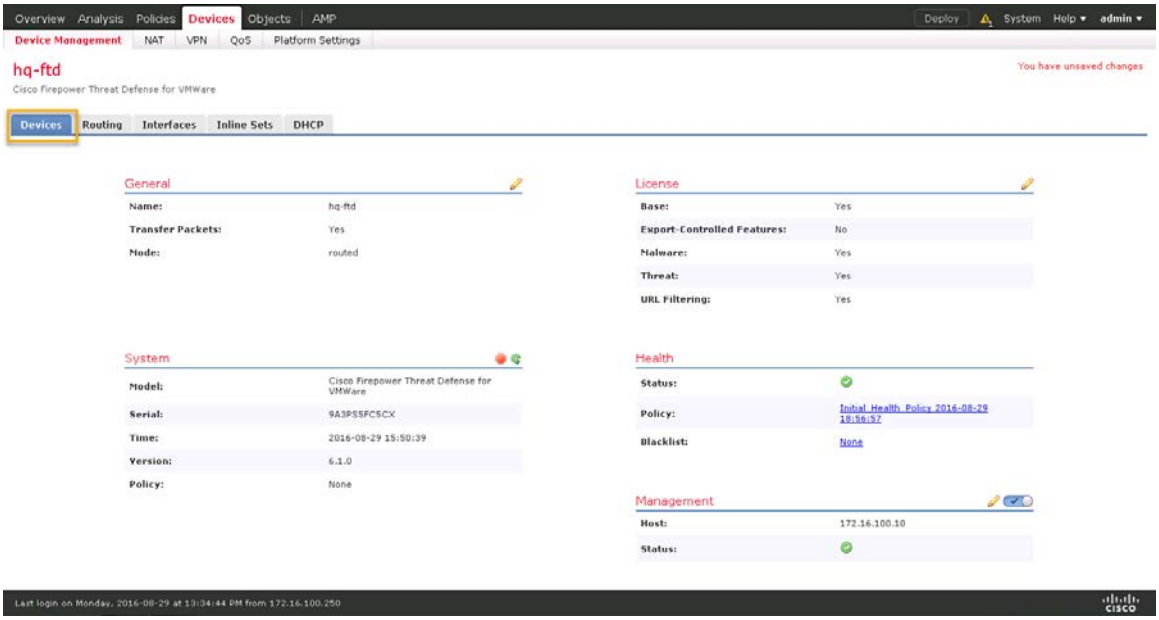


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

43. Click the **Devices tab**.
44. 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 66. Devices Tab Info



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

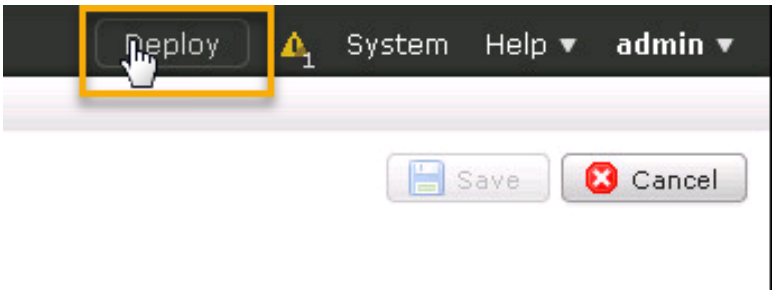
45. Now that the data interfaces have IP addresses, and routing is configured it is time to save your changes. Click the Save button in the upper-right region of the web page. Unfortunately, the Save button doesn't appear on every page so if you don't see it click on the **Routing tab** to refresh the screen and populate the **Save** button.

Figure 67. Save your changes



46. 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 68. The Deploy Button



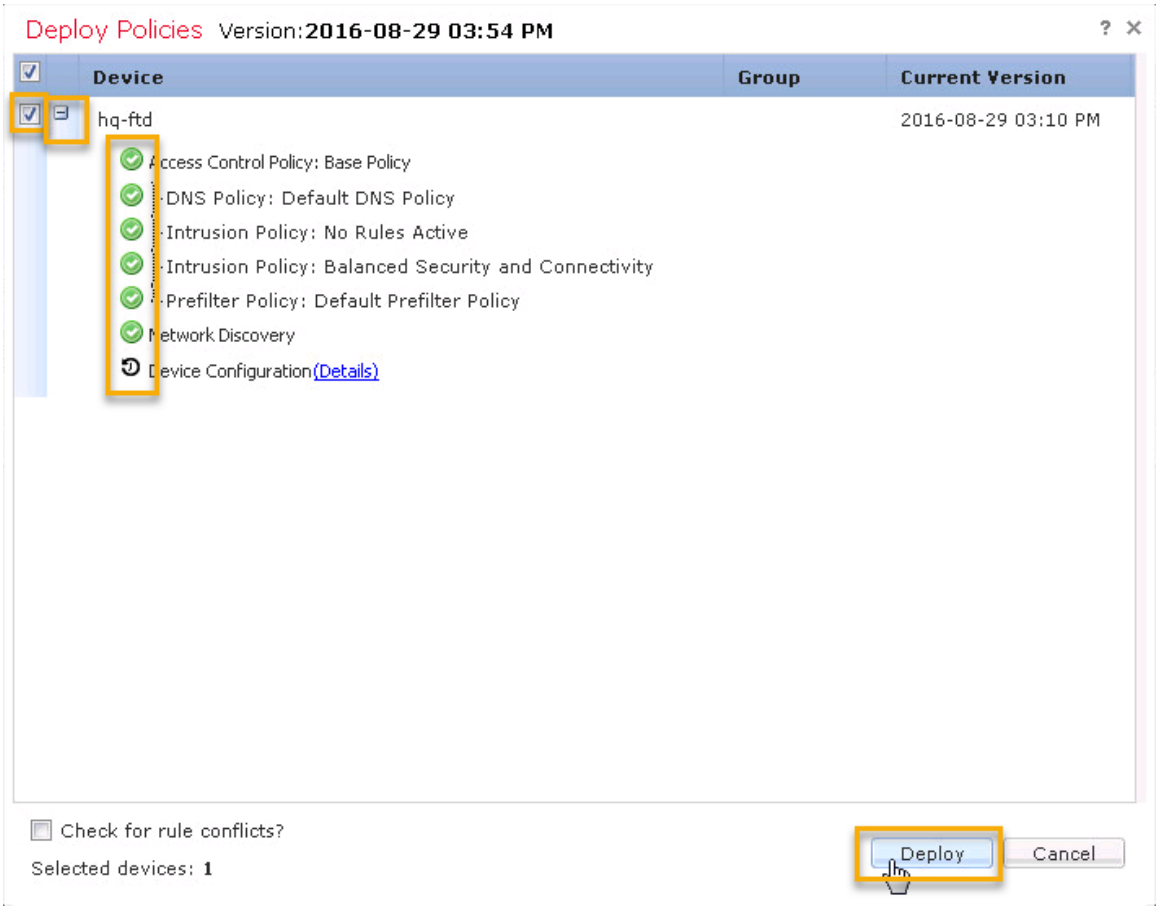
47. Only those devices that could be affected by the changes that have been made will be listed here. In your case you only have 1 device so that is obvious BUT in the real world where you might have 100s or 1000s of devices this is a handy feature so that you don't have to sift through tons of devices 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.)

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

48. Check the box next to **hq-ftd**.
49. 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.
50. Click **Deploy** to push the changes out to the selected device(s).

Figure 69. Push changes to hq-ftd

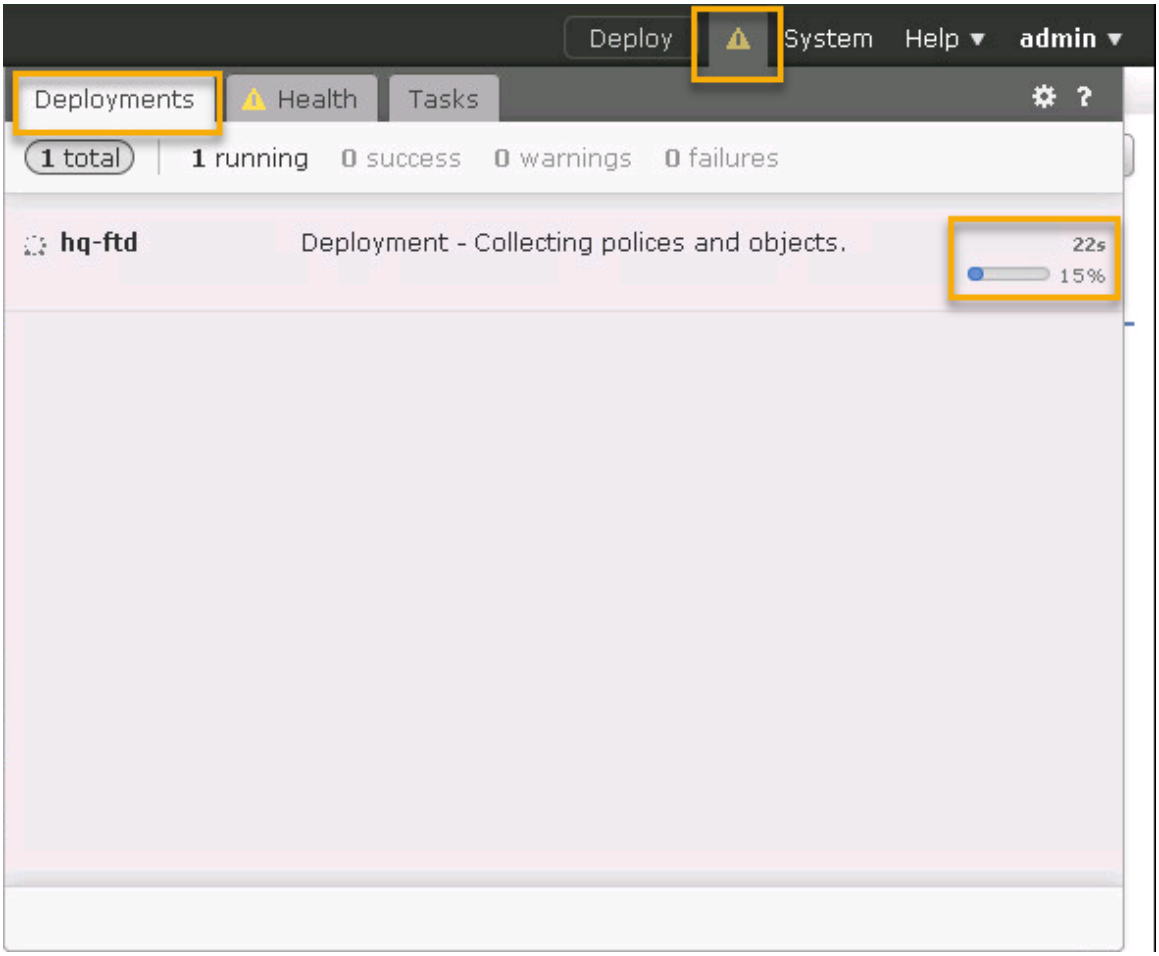


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

51. 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.

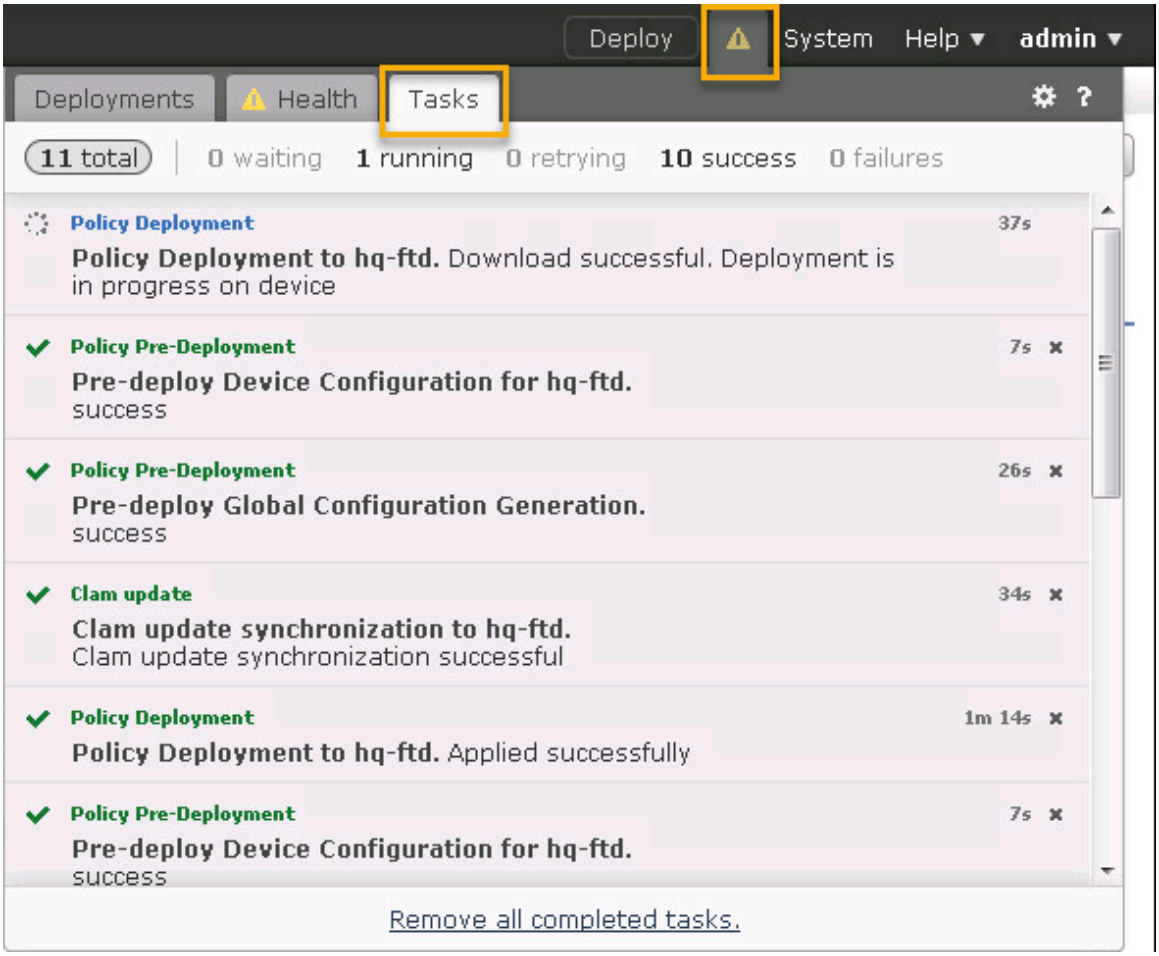
Figure 70. Deploying changes



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

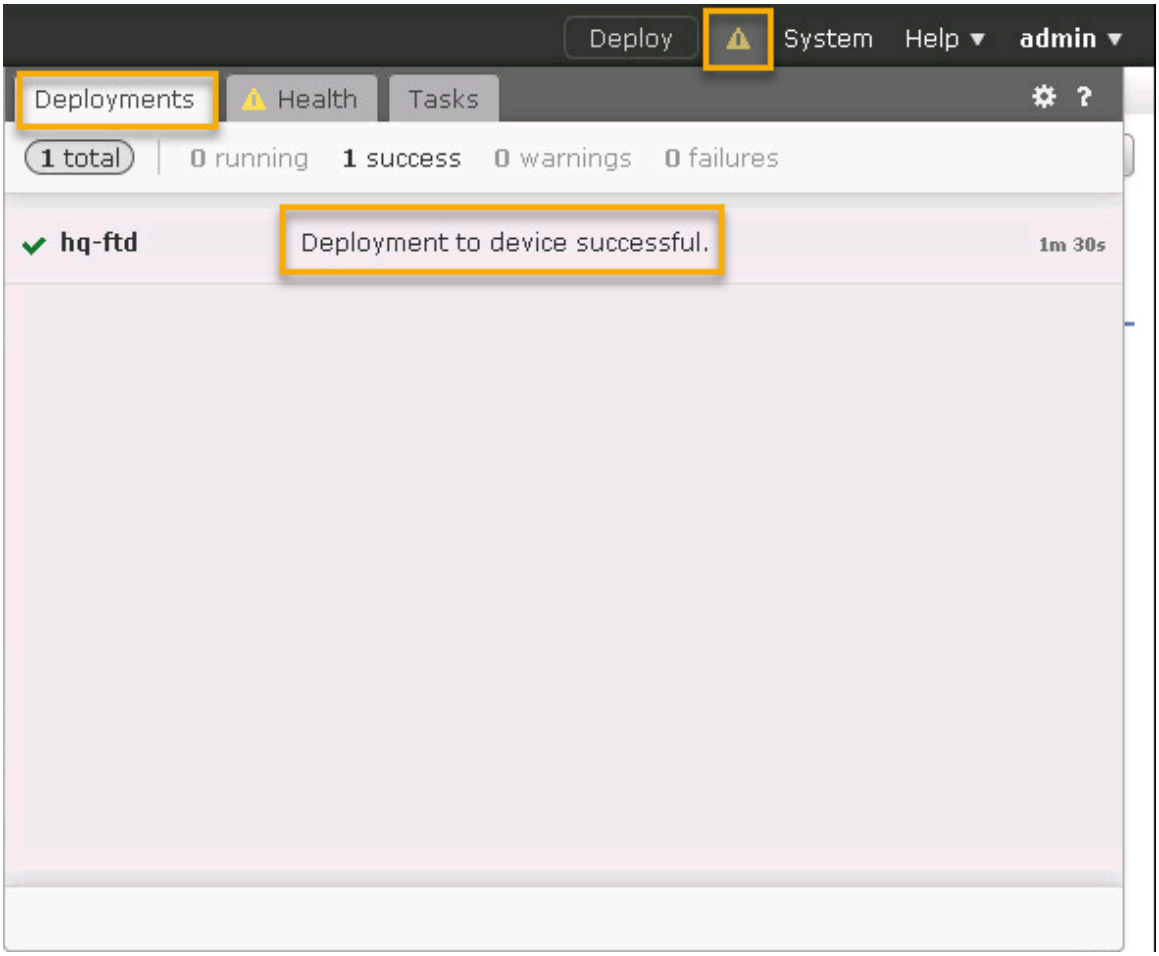
Figure 71. Details of changes being made



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Figure 72. Changes are done deploying



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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

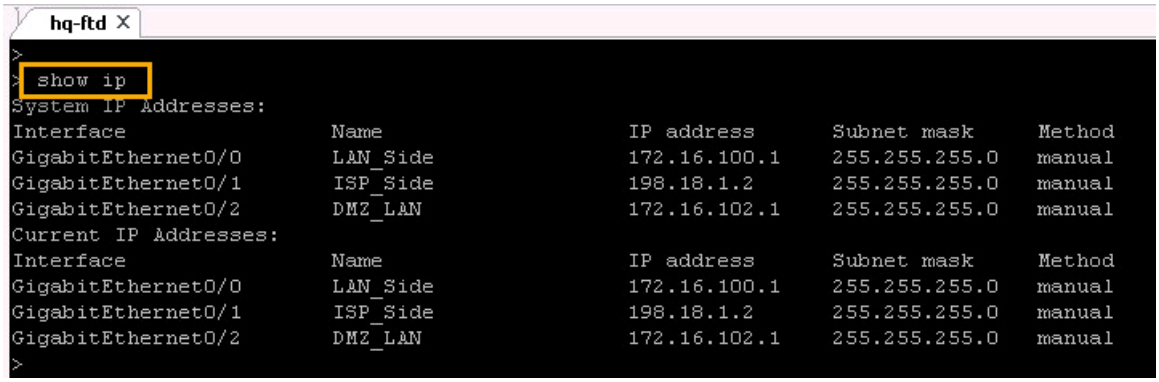
https://t.me/learningnets

Testing hq-ftd Data Interfaces Configuration

52. Return to the SSH session to the hq-ftd.

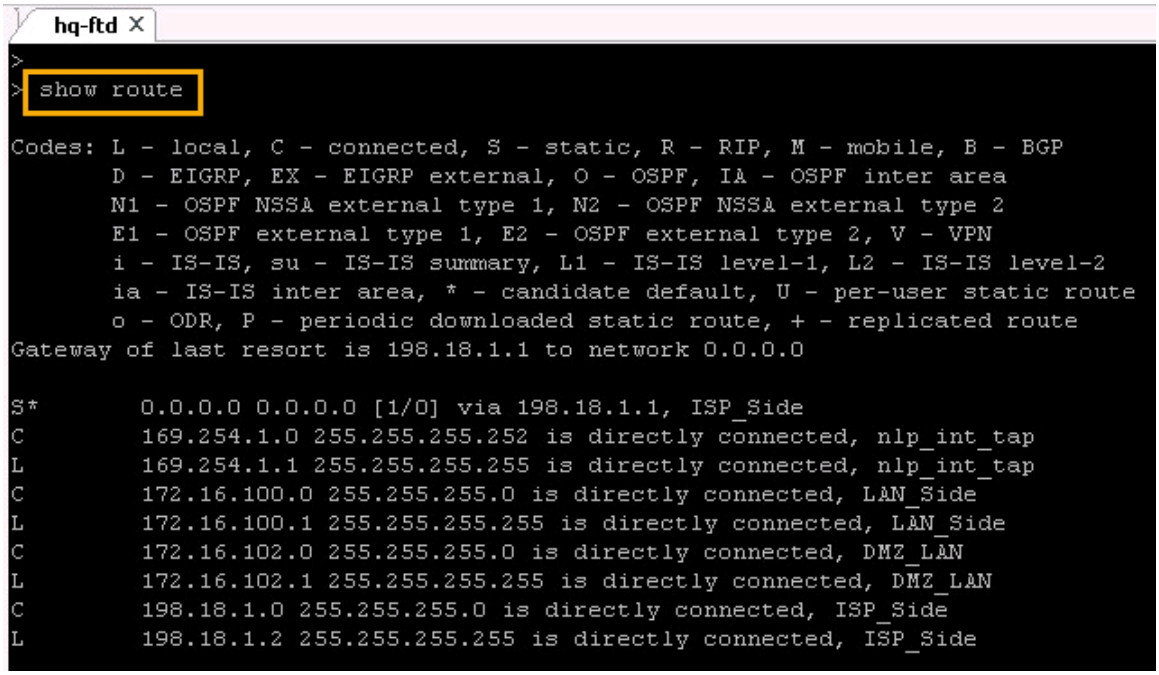
53. Issue the command **show ip** to see a list of the interfaces and what IP addresses they are assigned.

Figure 73. Show ip



54. Issue the command **show route** to see the data path's routing table.

Figure 74. Show route



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

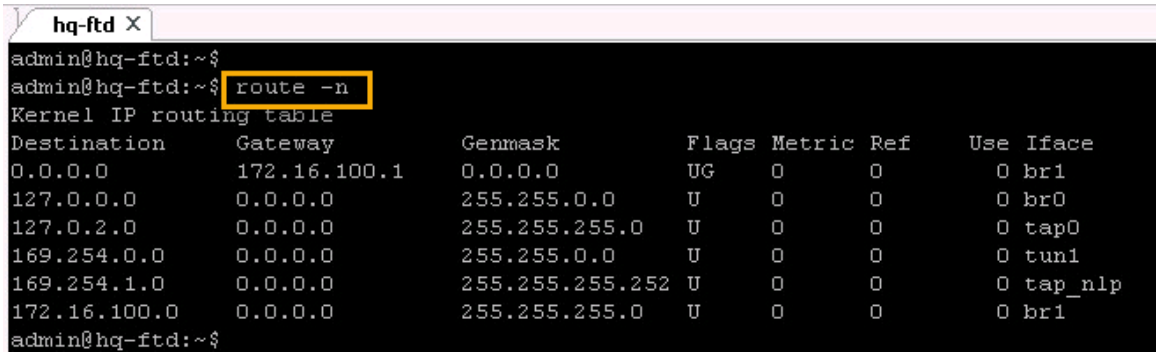
55. Issue the command **expert** to access the Linux shell.

Figure 75. Change to expert mode



56. 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 76. Route –n

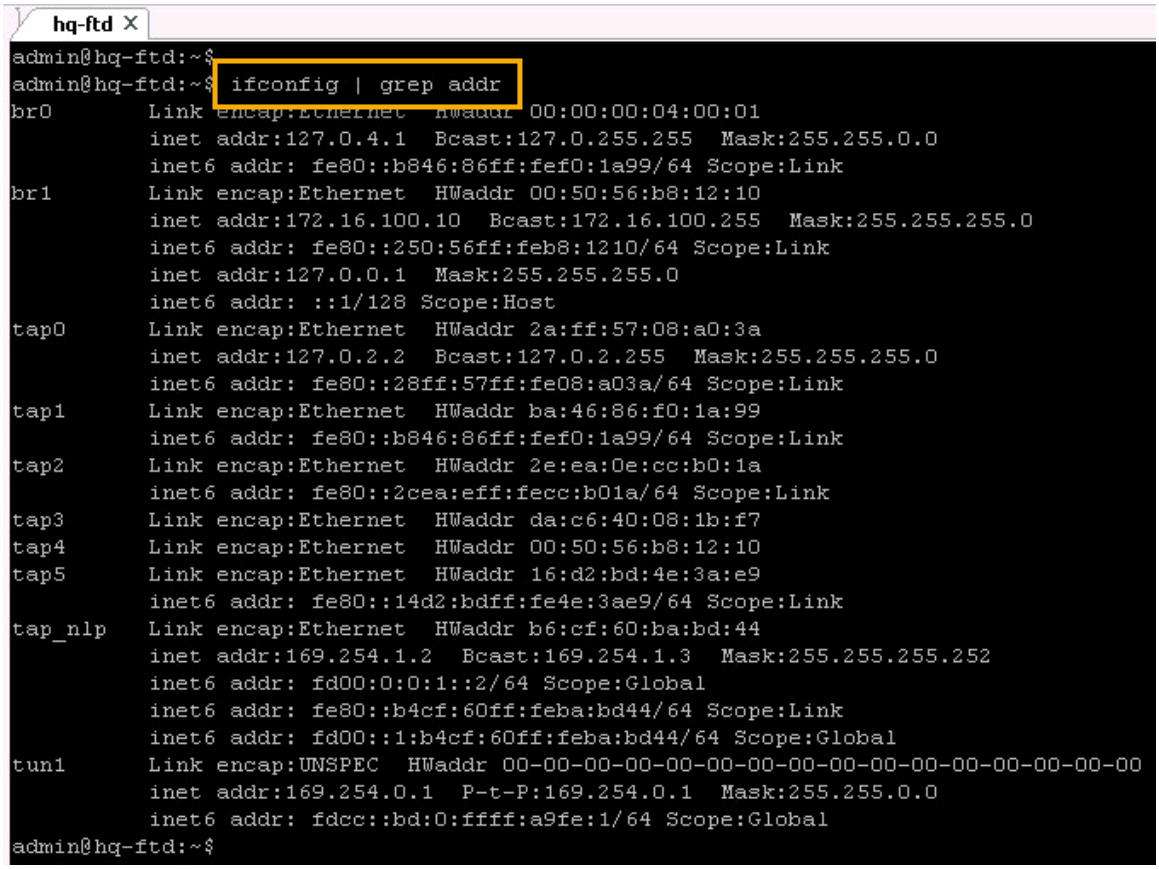


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

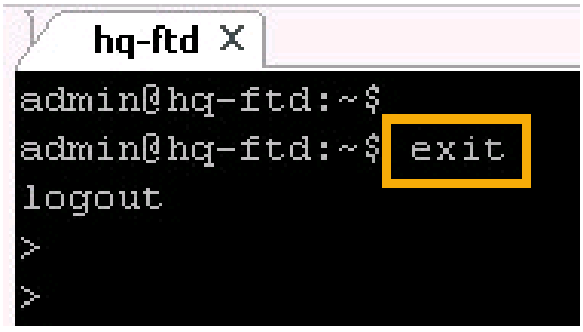
57. Type ifconfig (or better yet **ifconfig | grep addr**) and compare the assigned IP addresses to interfaces with the output of the show ip command. Why are they different? [Because, when in expert mode, you are looking at what the Management Interface sees; while in firepower or FTD mode you are seeing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

Figure 77. Ifconfig | grep addr



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

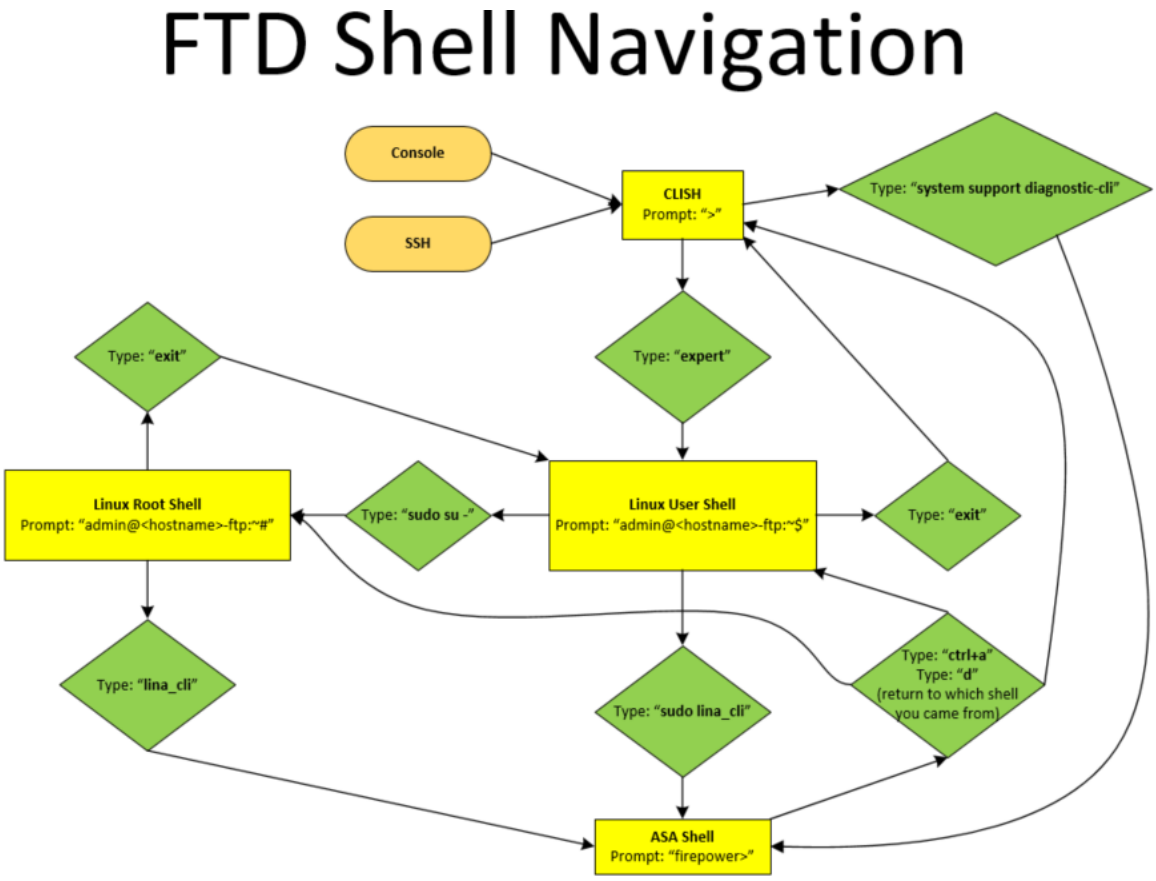
Figure 78. Return to FTD shell



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Figure 79. FTD Shell Navigation

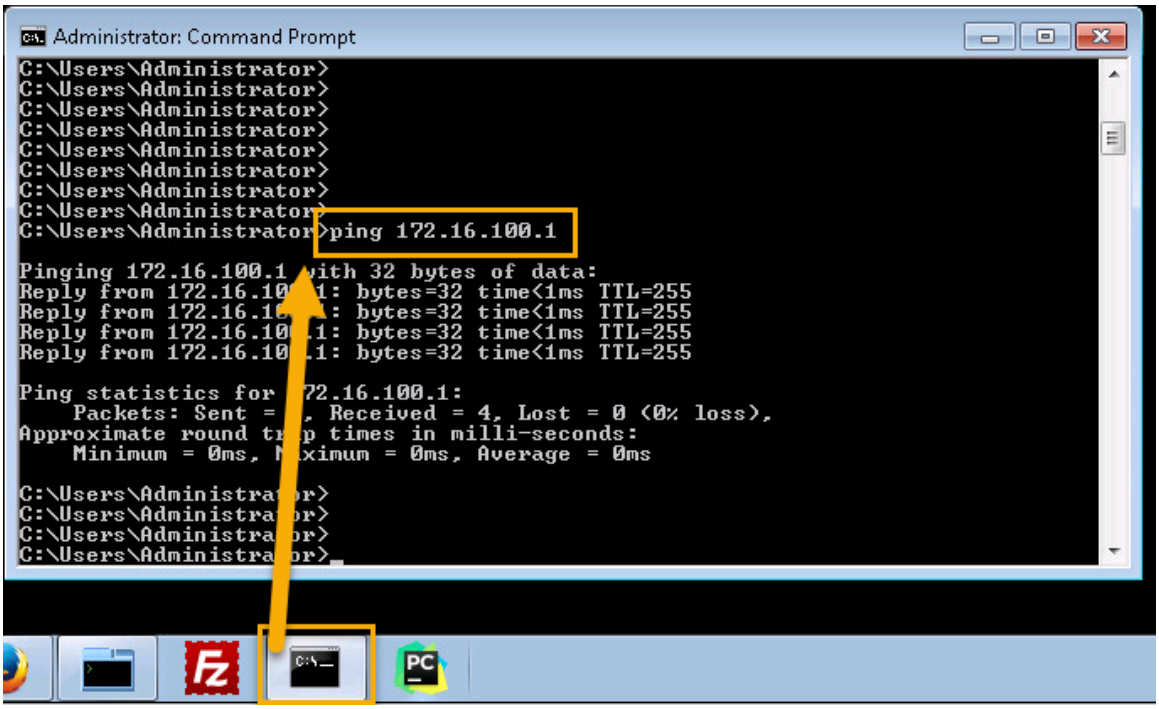


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

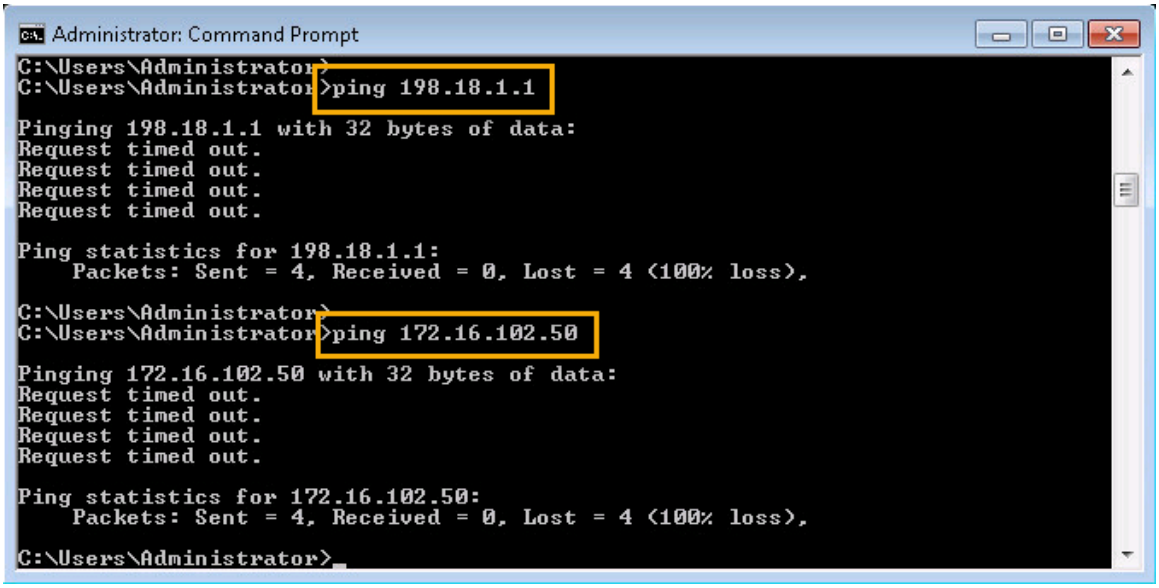
59. From hq-wkst you should be able to **ping 172.16.100.1**. Open a **CMD prompt** and do so.

Figure 80. Ping hq-wkst default gateway



60. 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 81. Can't ping inet-server nor dmz-server



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

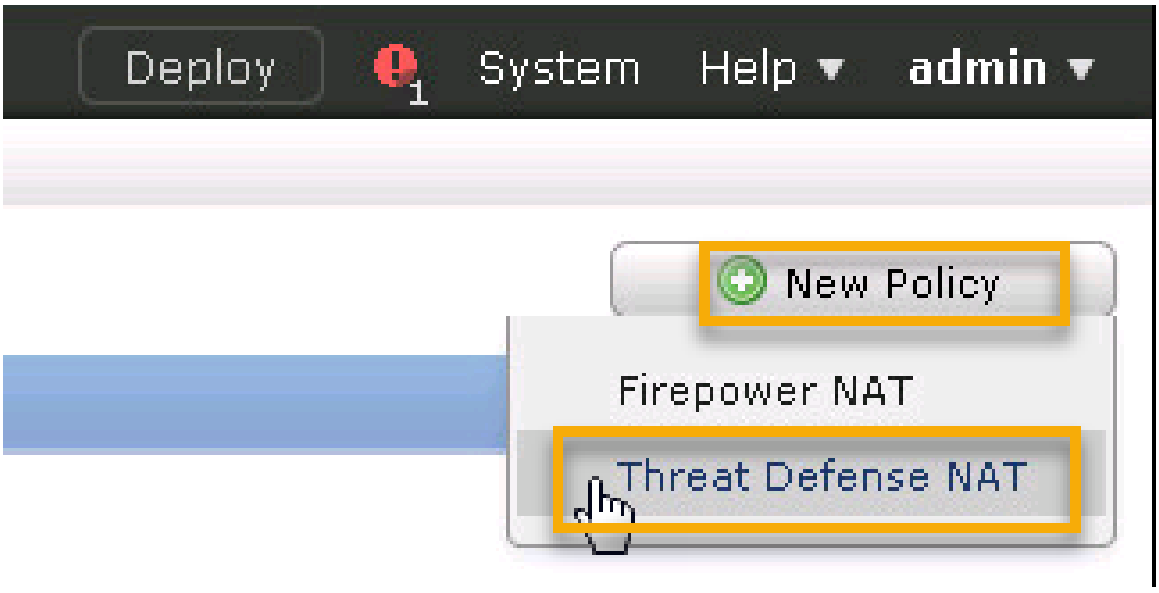
1. On hq-wkst and within the FMC administration webpage navigate to **Devices > NAT** to configure a NAT policy.

Figure 82. 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 83. Create NAT Policy

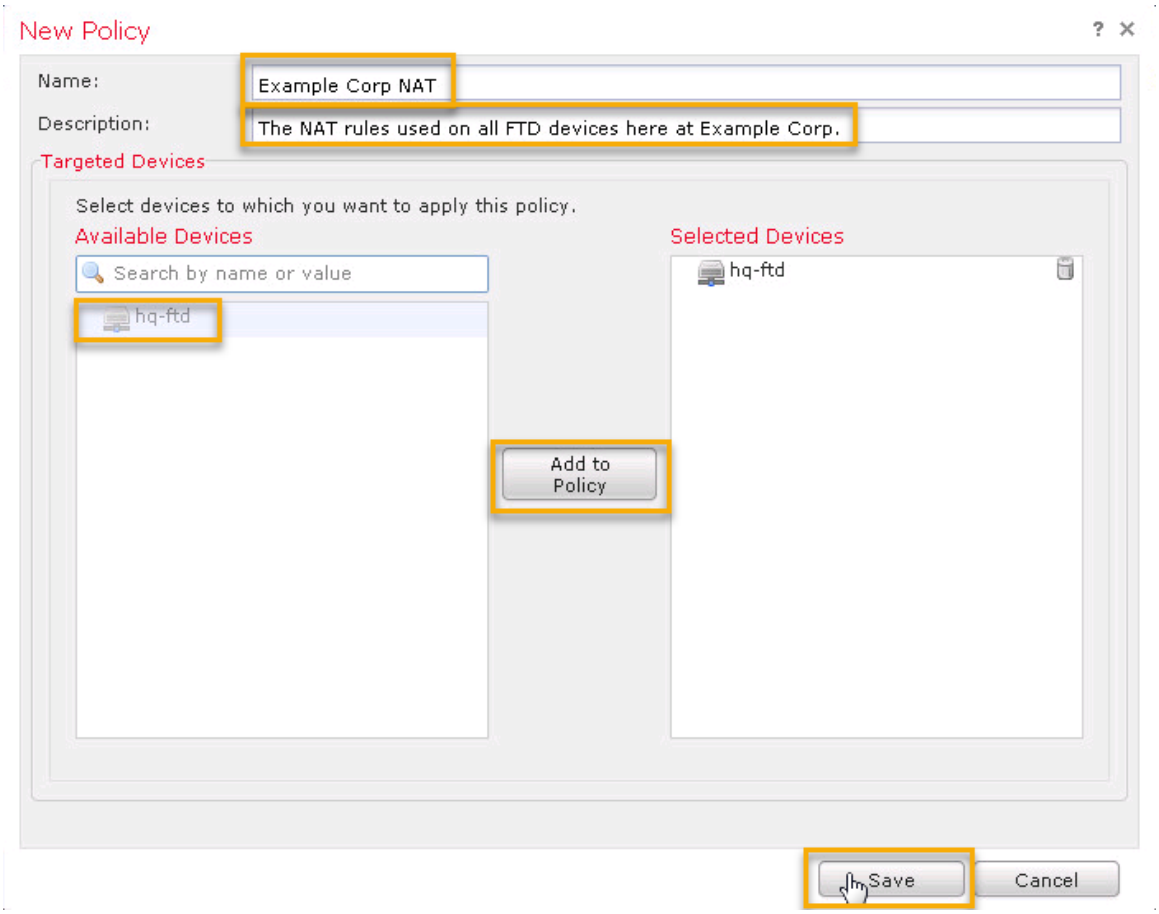


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 84. Save NAT Policy



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

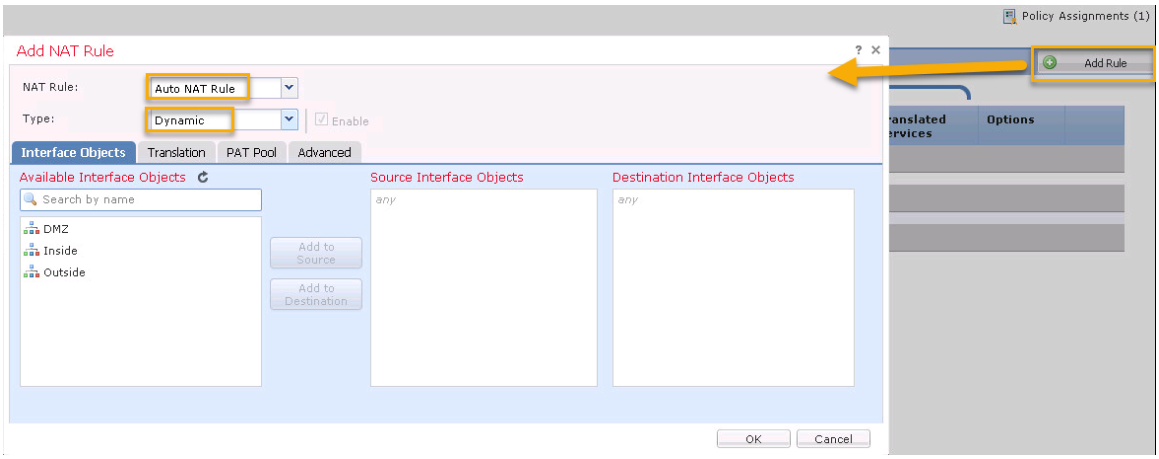
https://t.me/learningnets

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 85. Part 1 of adding NAT rule



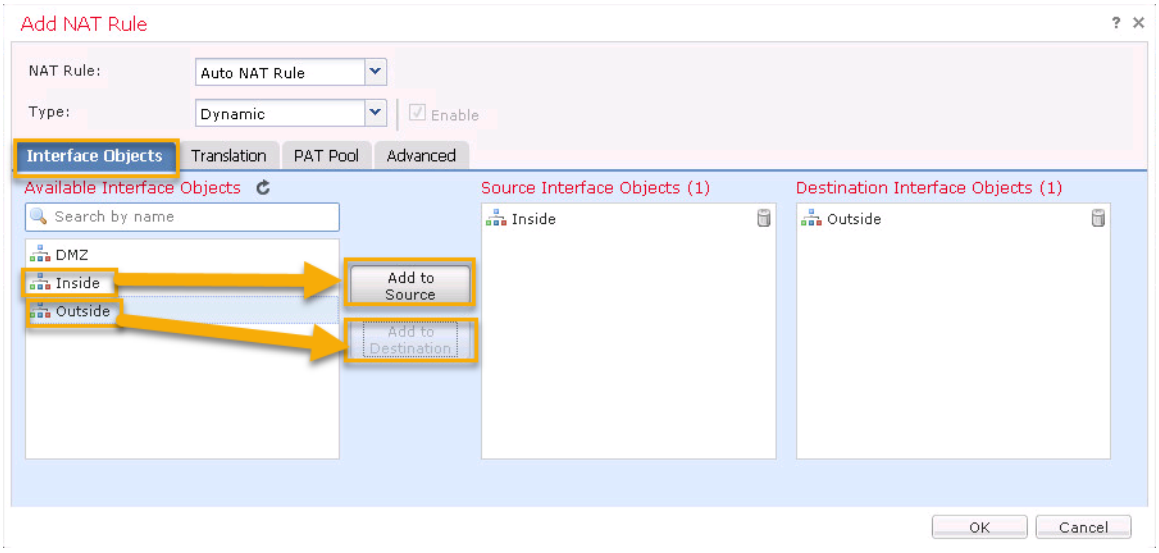
6. On the Interface Objects tab:

    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 86. Add Zones to Rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

7. On the **Translation tab**:

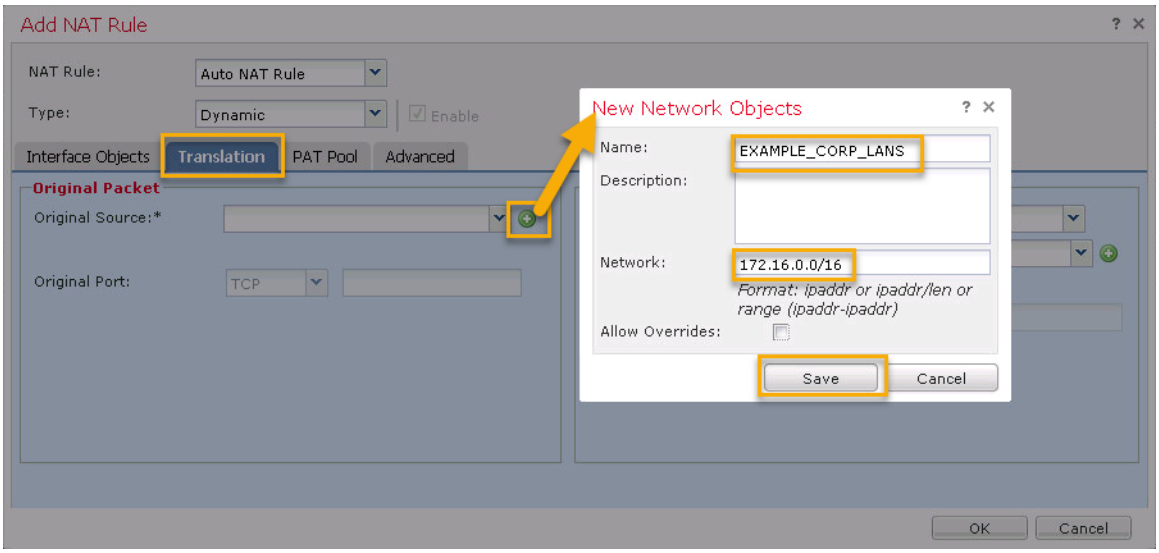
    a. Original Source: (You need to create a Network Object that encompasses all the Example Corp LANs.) Click the **green plus icon** and use the following information to fill out the needed info:

        i. Name: **EXAMPLE_CORP_LANS**

        ii. Network: **172.16.0.0/16**

        iii. Click **Save**.

Figure 87. Add Network Object



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

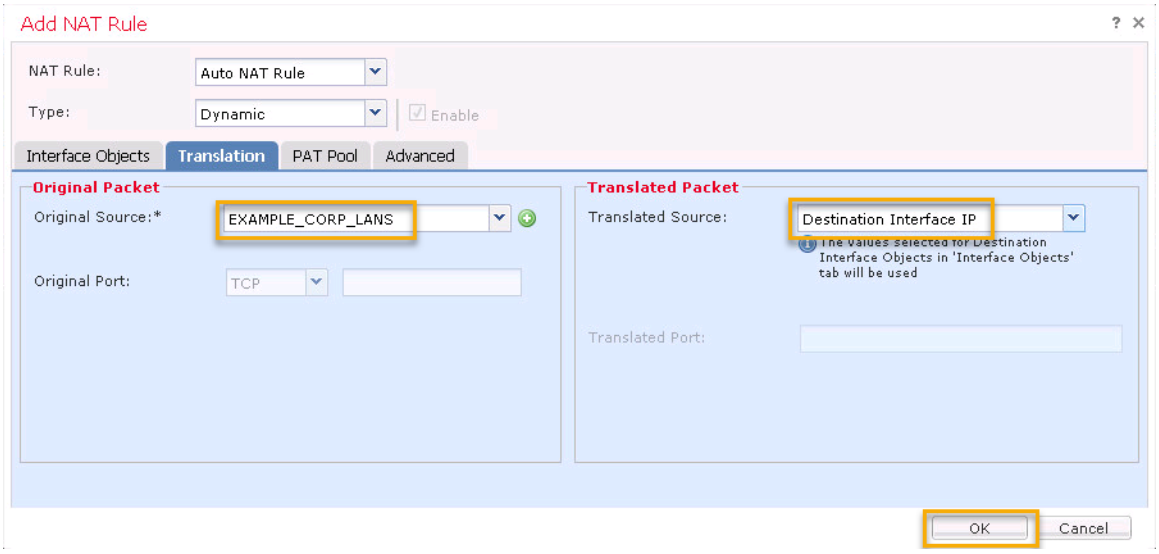
https://t.me/learningnets

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 88. Set up Translation Tab and Save



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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).

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

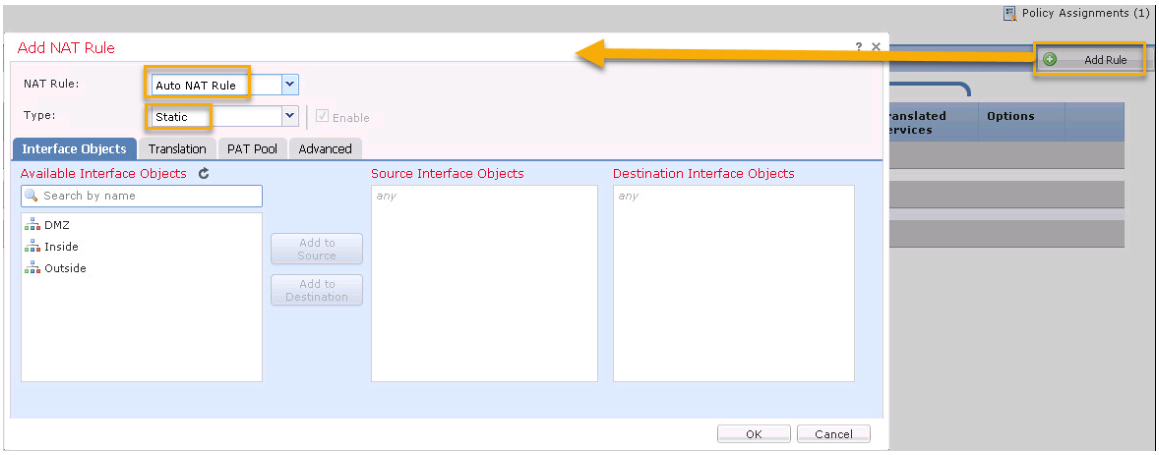
https://t.me/learningnets

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 89. Add NAT Rule

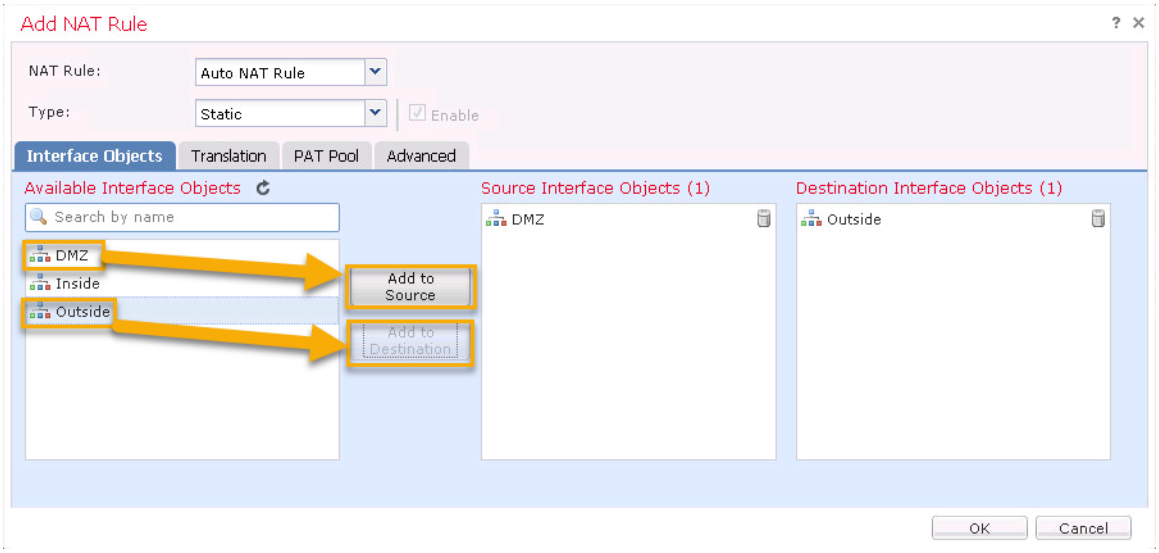


10. On the **Interface Objects tab**:

    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 90. Interface Objects Tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

11. On the **Translation tab**:

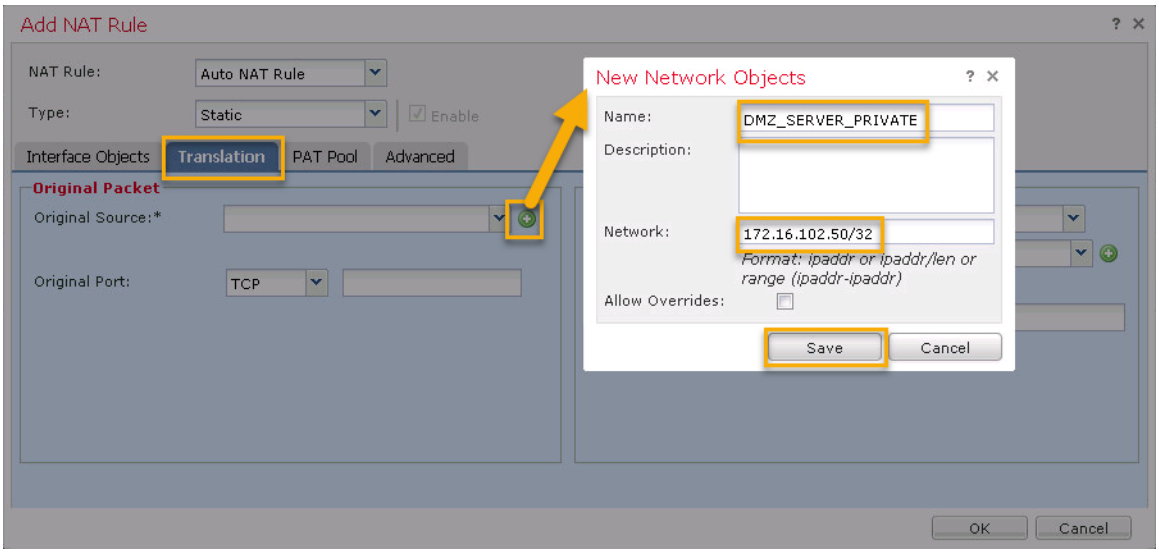
    a. You need to create a Network Objects for the DMZ Server's private and public IPs. Click the **green plus icon** and use the following information to fill out the needed info:

        i. Name: **DMZ_SERVER_PRIVATE**

        ii. Network: **172.16.102.50/32**

        iii. Click **Save**.

Figure 91. Add Network Object



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

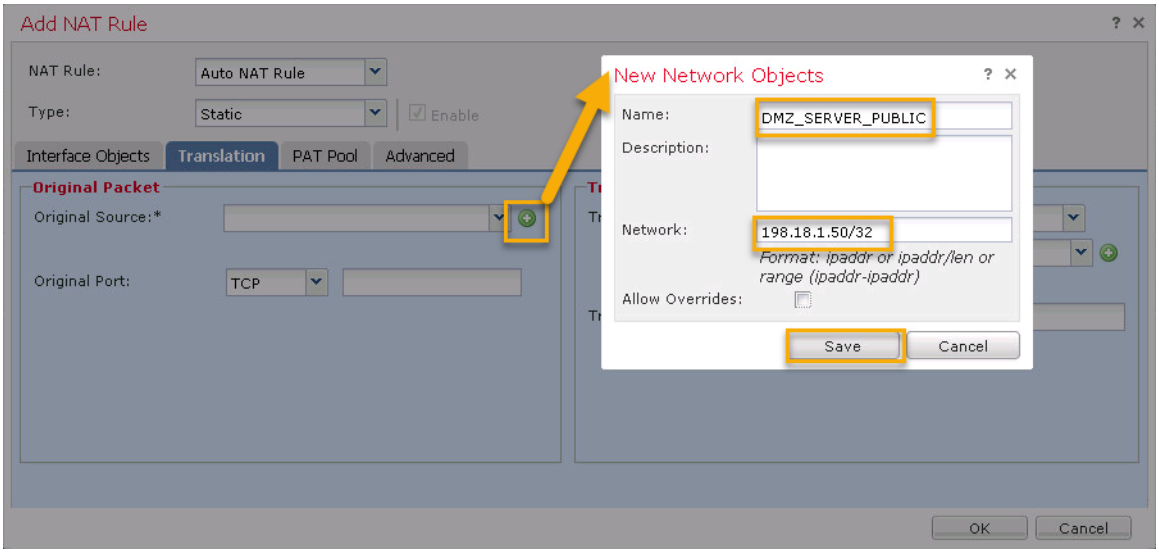
b. Click the **green plus icon** again and use the following information to build the DMZ Server's Public IP Network Object:

   i. Name: **DMZ_SERVER_PUBLIC**

   ii. Network: **198.18.1.50/32**

   iii. Click **Save**.

Figure 92. Add Network Object

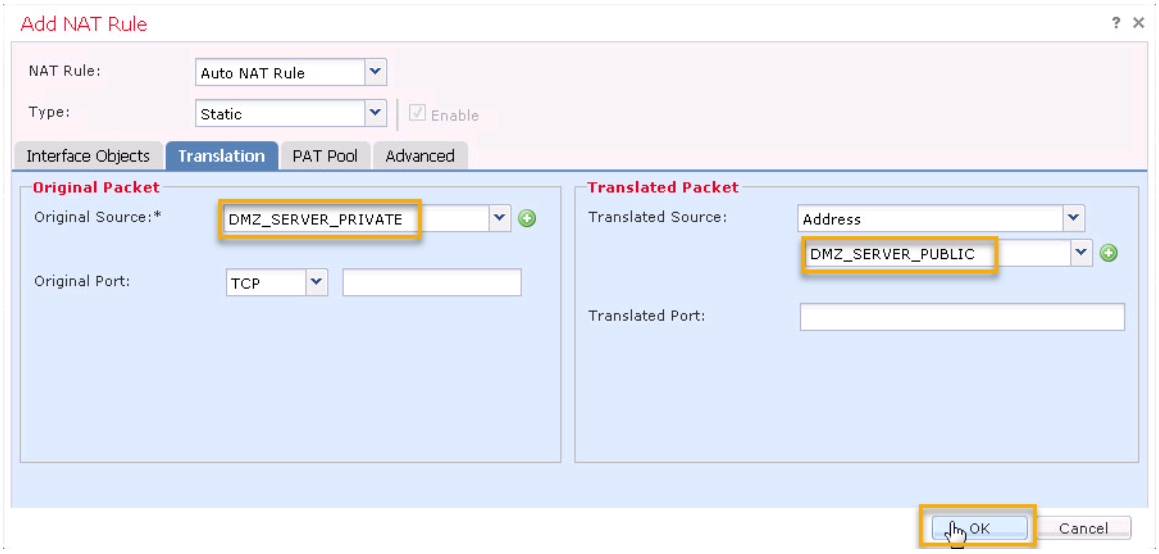


c. Original Source: Select the **DMZ_SERVER_PRIVATE** from the dropdown menu.

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

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

Figure 93. Set up Translation Tab and Save



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

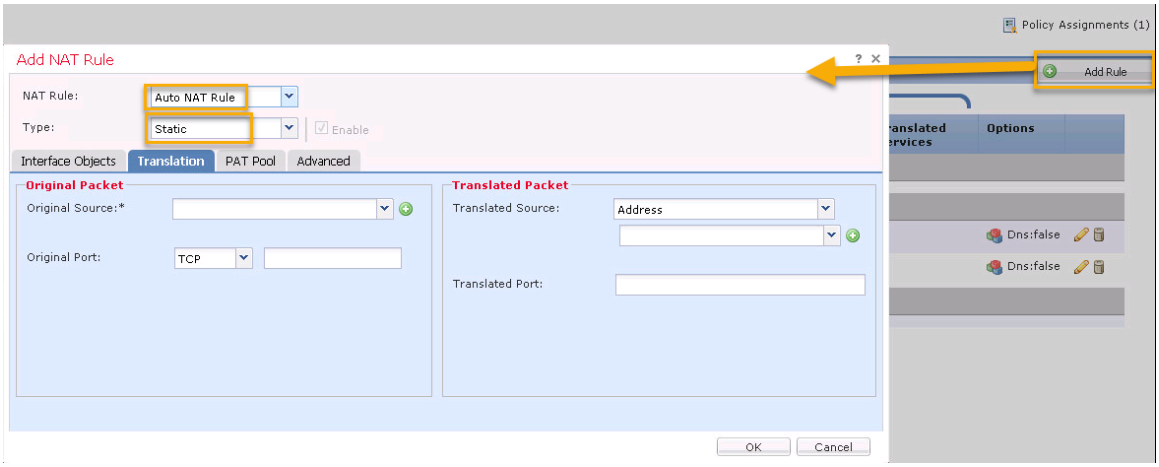
https://t.me/learningnets

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 94. Add NAT rule

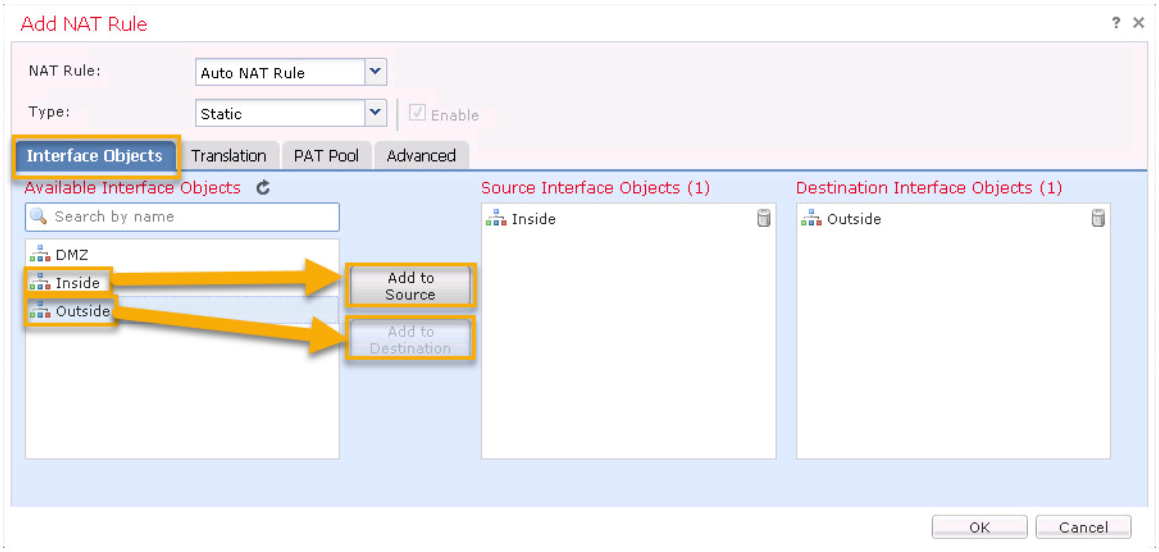


14. On the **Interface Objects tab**:

    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 95. Set up Interface Objects tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

15. On the **Translation tab**:

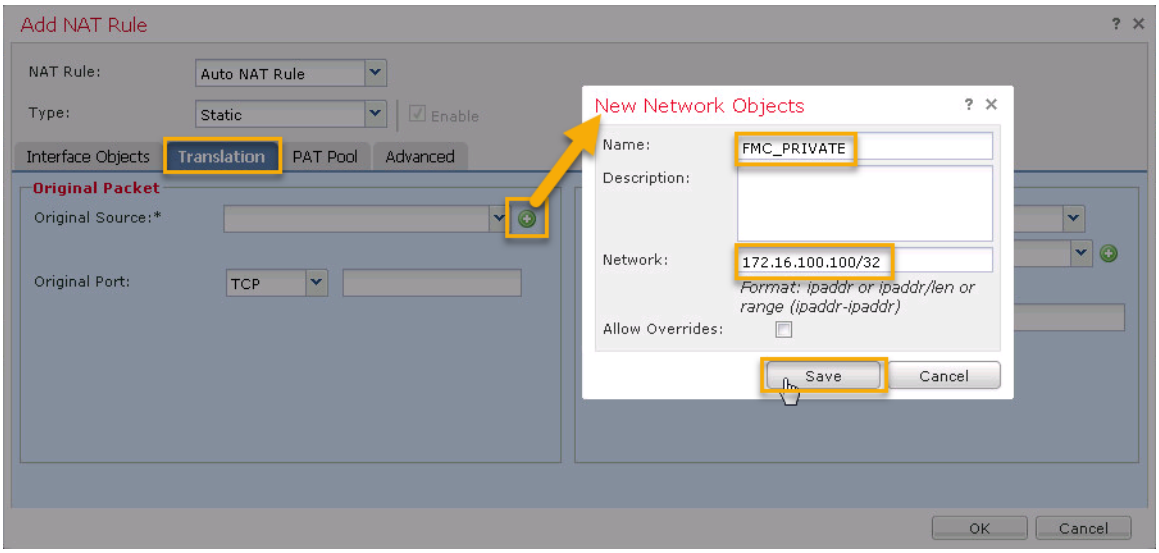
    a. You need to create a Network Objects for the FMC Server's private and public IPs. Click the **green plus icon** and use the following information to fill out the needed info:

        i. Name: **FMC_PRIVATE**

        ii. Network: **172.16.100.100/32**

        iii. Click **Save**.

Figure 96. Create Network Object



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

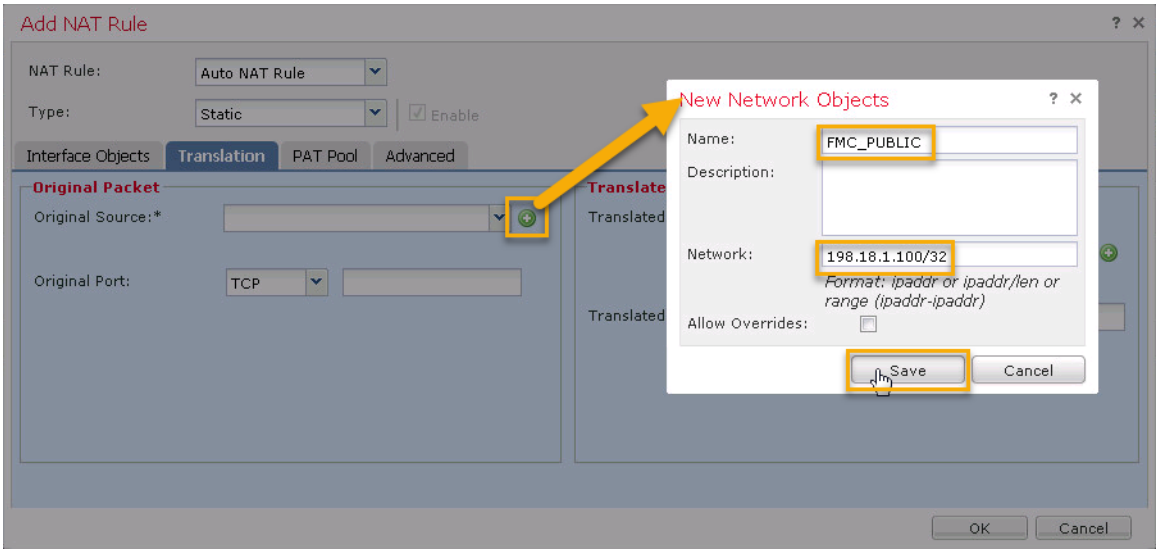
b. Click the **green plus icon** again and use the following information to build the FMC Server's Public IP Network Object:

   i. Name: **FMC_PUBLIC**

   ii. Network: **198.18.1.100/32**

   iii. Click **Save**.

Figure 97. Add Network Object

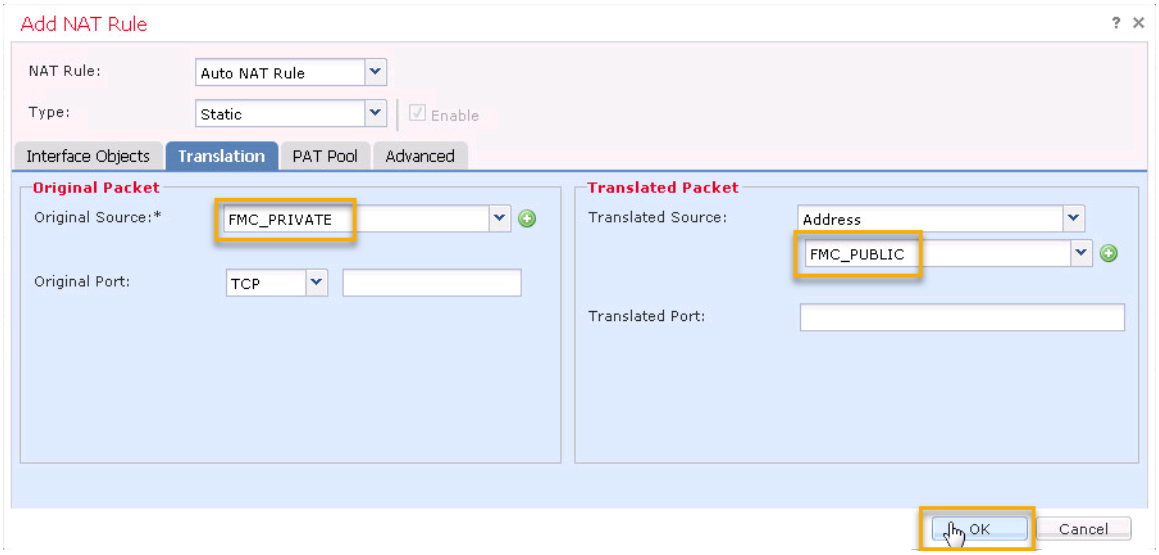


c. Original Source: Select the **FMC_PRIVATE** from the dropdown menu.

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

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

Figure 98. Set up Translation tab and Save

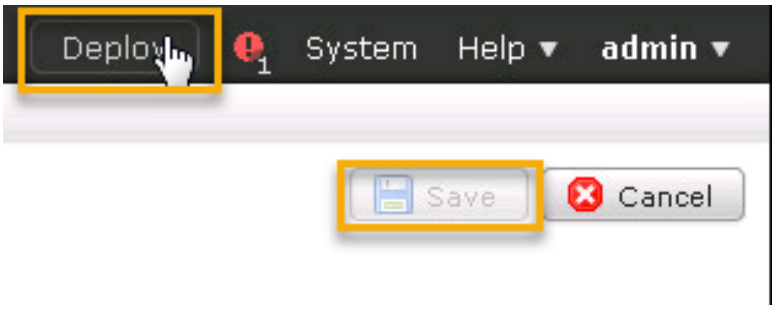


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

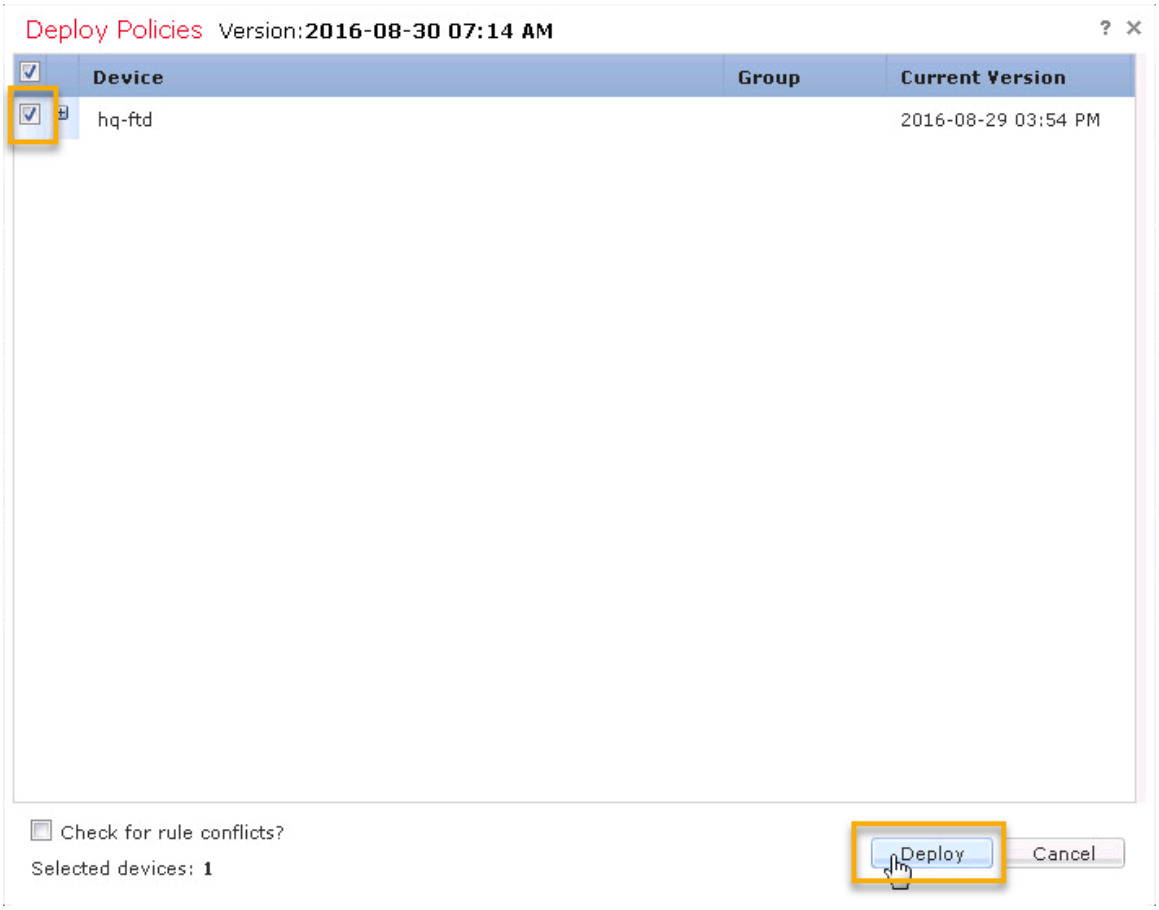
17. Click **Save** and then **Deploy**.

Figure 99. Save and Deploy



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

Figure 100. Deploy to hq-ftd



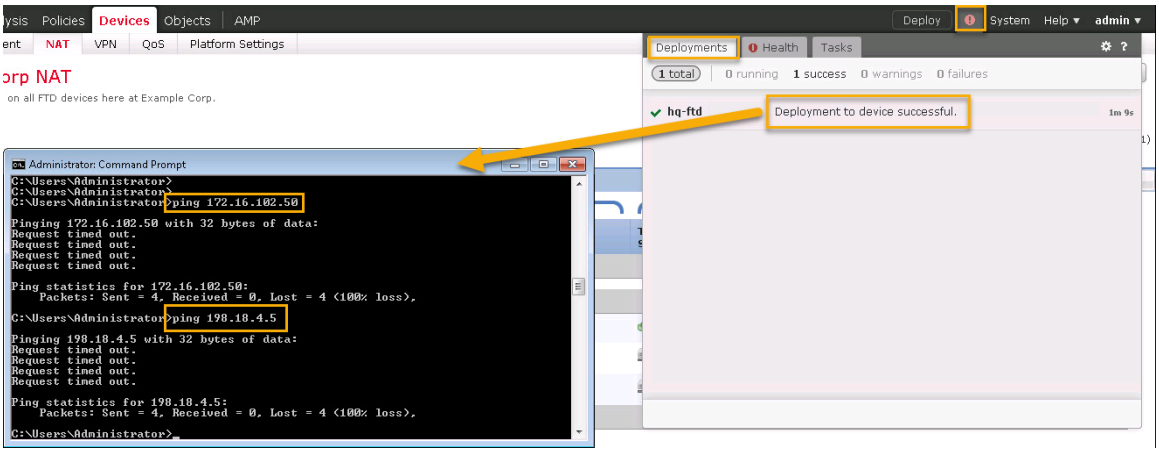
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 101. Failed pings



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 102. Edit Base Policy ACP

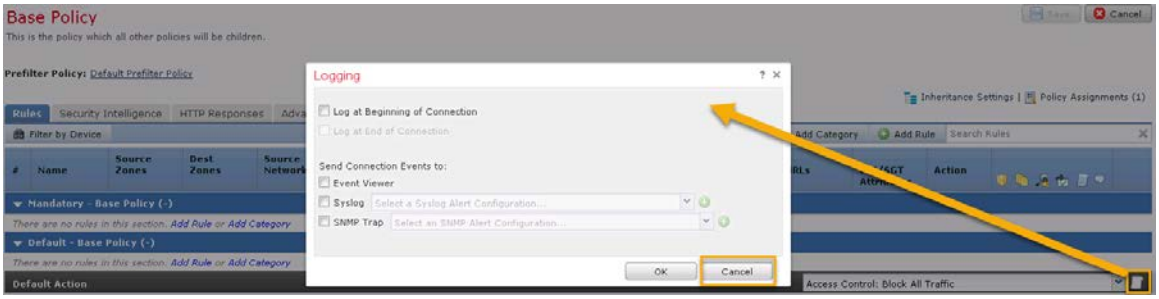


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 103. Scroll Icon



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 104. ACP is up-to-date and Edit



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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:

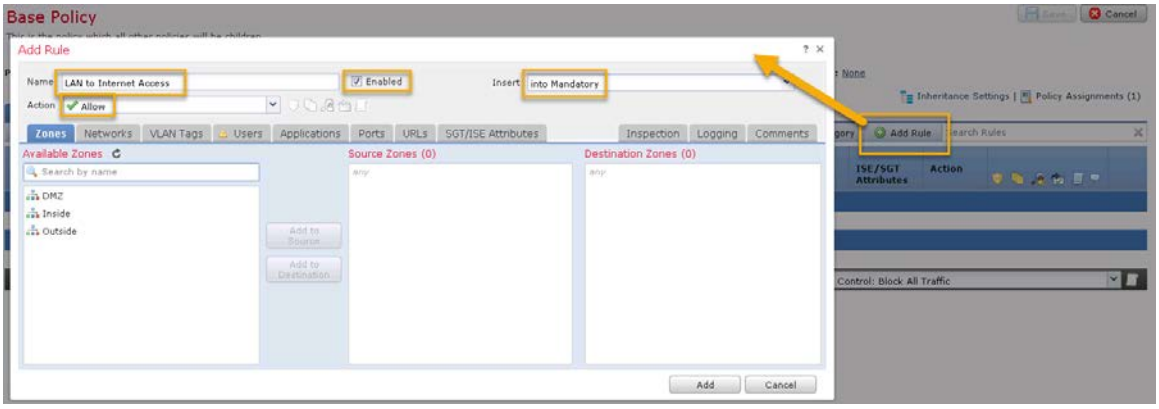
    a. Name: **LAN to Internet Access**

    b. Enabled: **Checked**

    c. Insert: **into Mandatory**

    d. Action: **Allow**

Figure 105. Part 1 of adding ACP rule



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

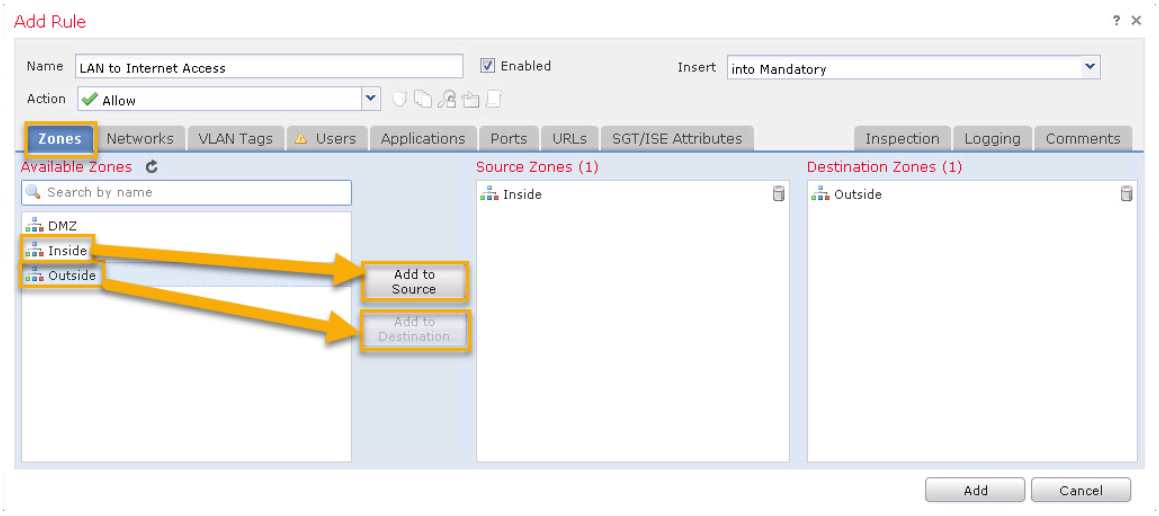
https://t.me/learningnets

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 106. Set up Zones tab

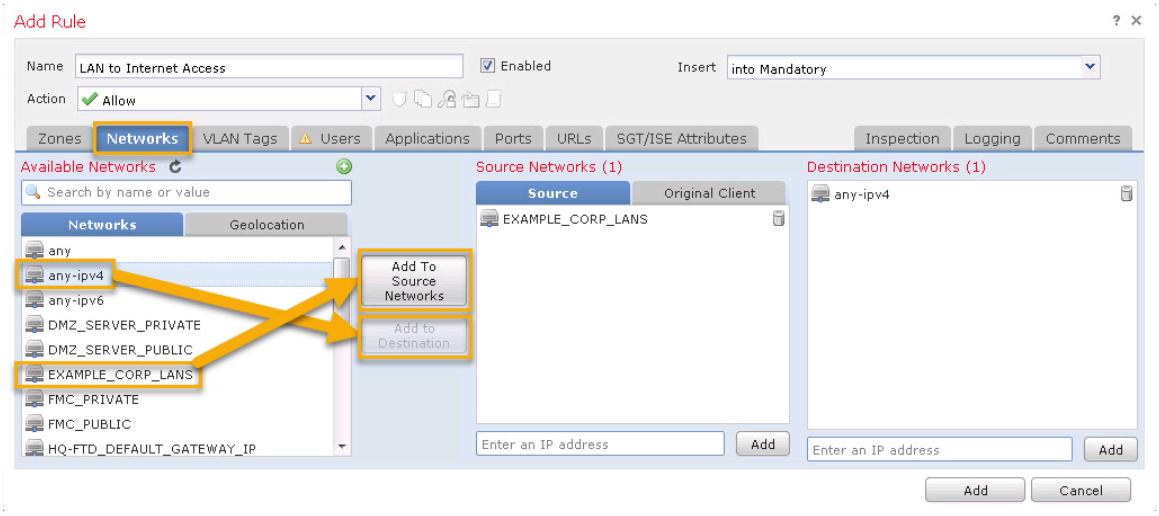


28. On the **Networks tab**:

    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 107. Configure Networks tab

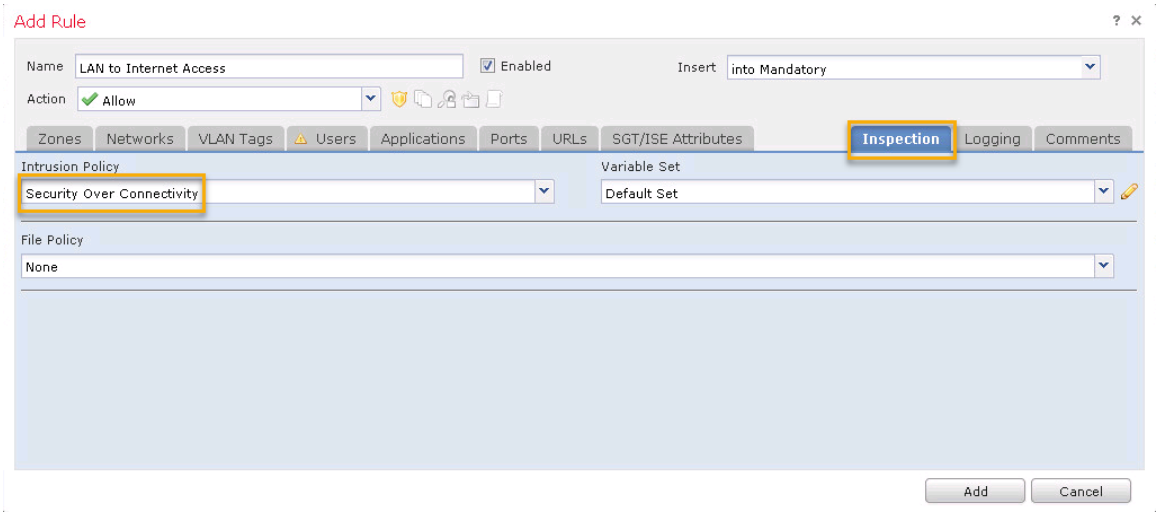


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

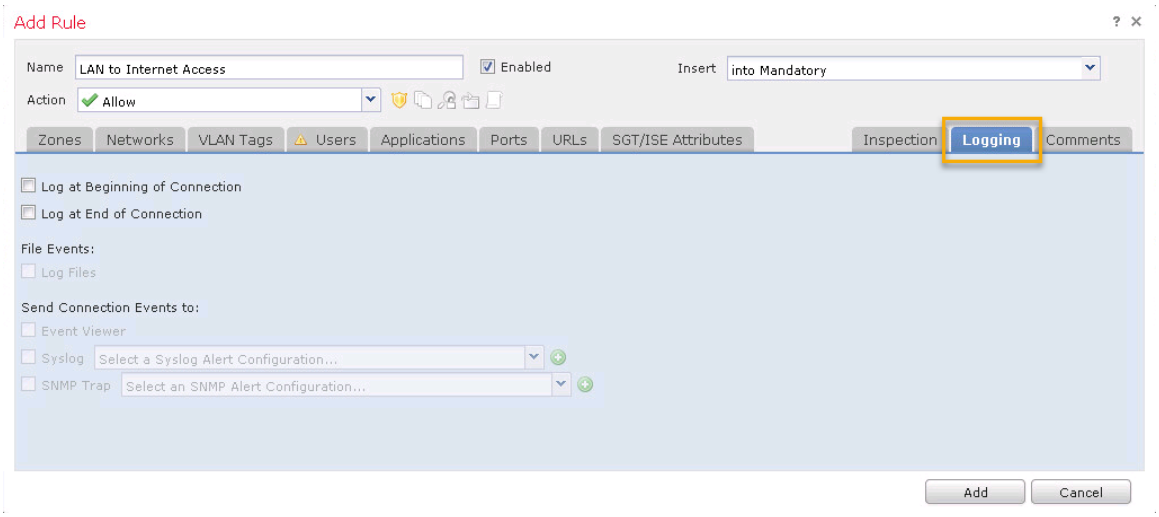
29. On the **Inspection tab** set the Intrusion Policy field to **Security Over Connectivity** (More on this later but essentially this is the IPS rule that is applied to traffic matching this rule.)

Figure 108. Configure Inspection tab



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 109. No logging this ACP rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

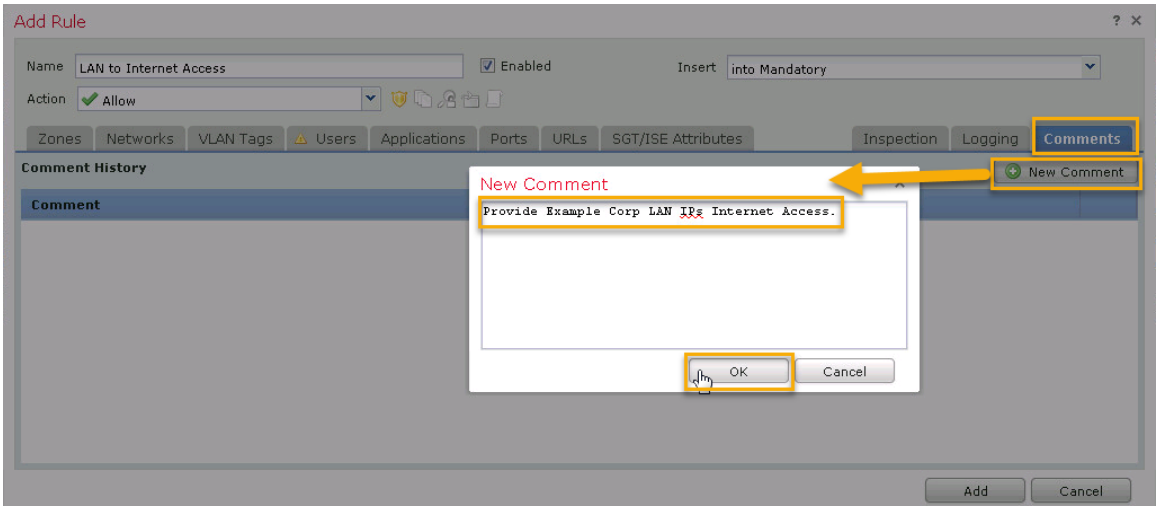
31. On the **Comments tab**:

    a. Click **New Comment**

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

    c. Click **OK**.

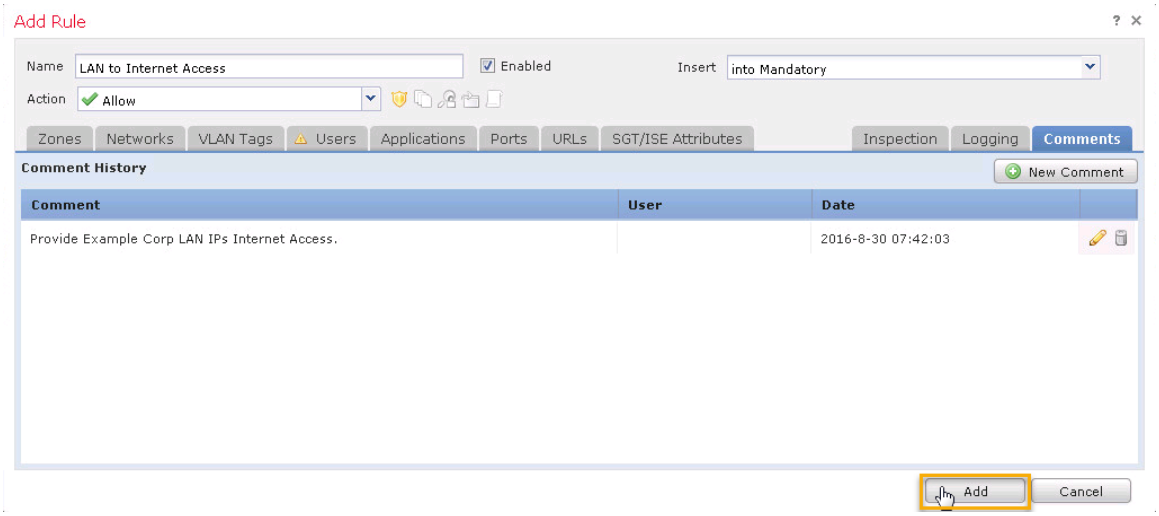
Figure 110. Add a comment



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 111. Add ACP Rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

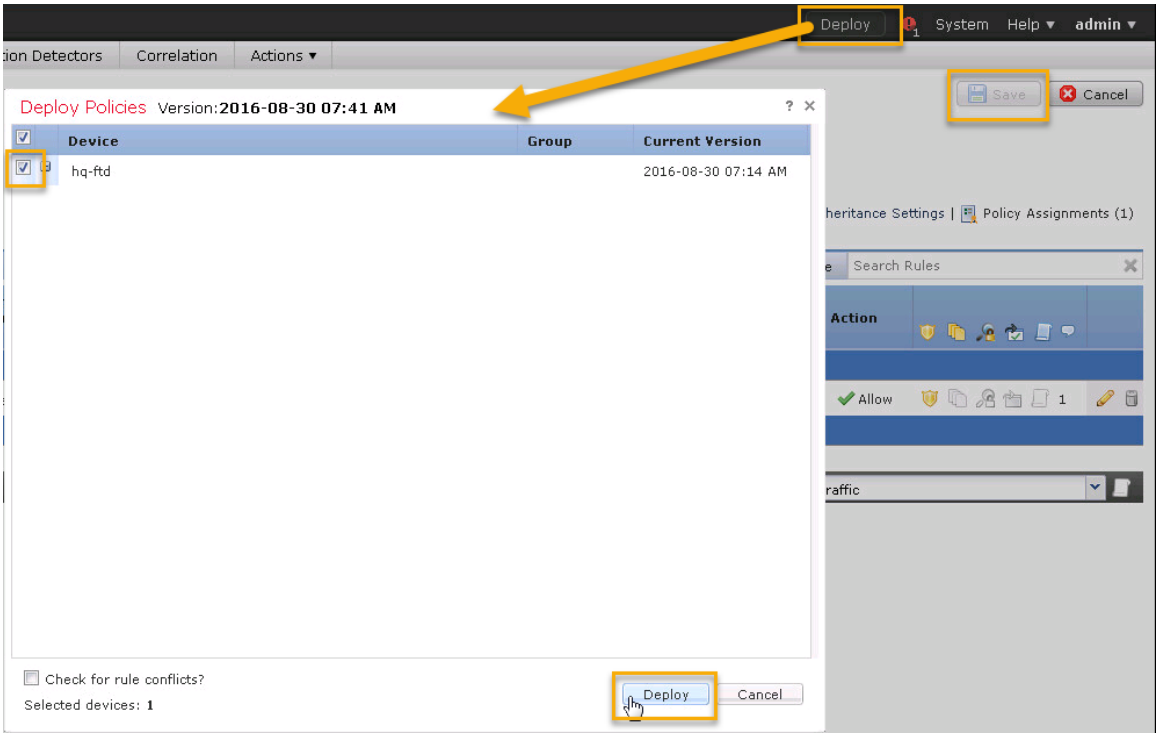
Figure 112. Mandatory and Default ACP sections



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

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

Figure 113. Save and Deploy to hq-ftd

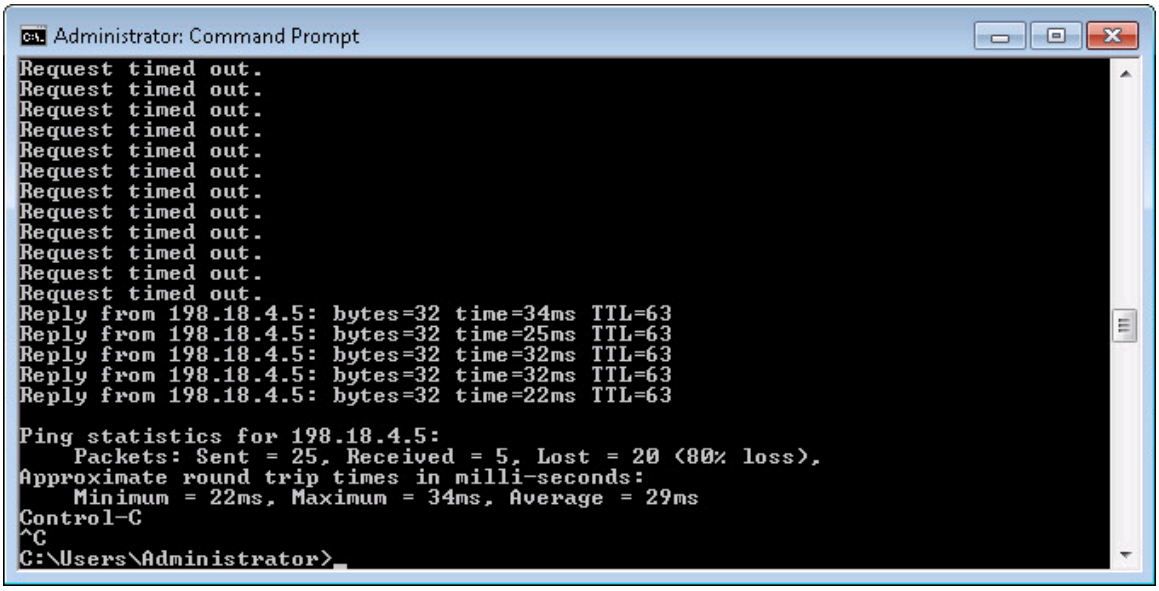


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

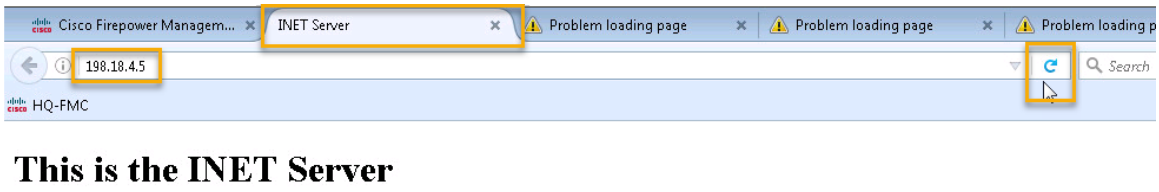
35. On hq-wkst open an **CMD prompt** and issue the command **ping –t 198.18.4.5**. Once the above policy is applied to hq-ftd these pings should start working.
36. Stop the pings with a **ctrl-c**.

Figure 114. Ping inet-server



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 115. Access inet-server web page

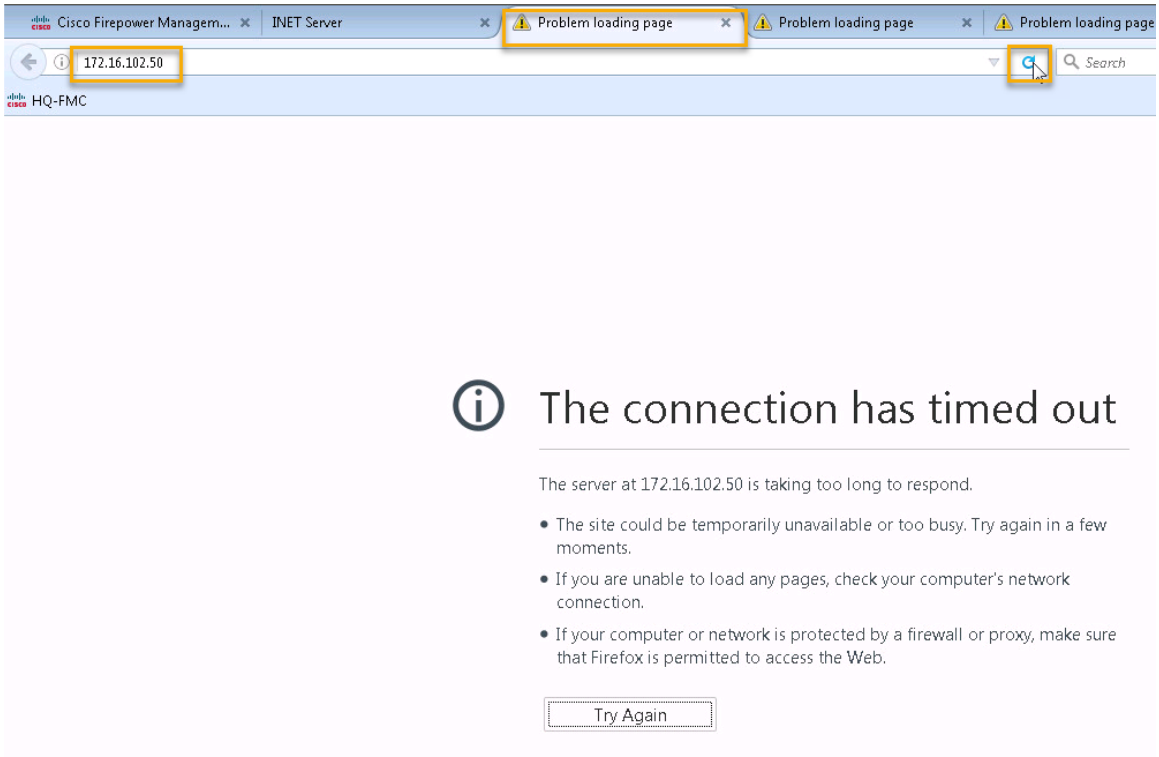


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

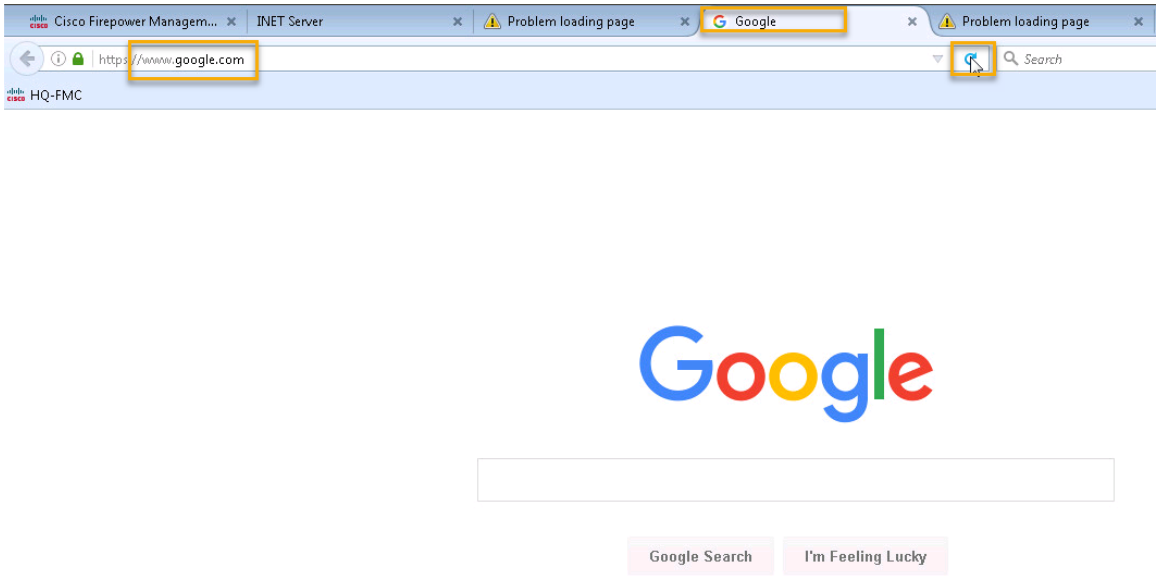
38. The 3rd tab is **http://172.16.102.50**, the dmz-server, but this should **not** load. Why?

Figure 116. Failing access to dmz-server web page



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

Figure 117. Access Google web page



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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**

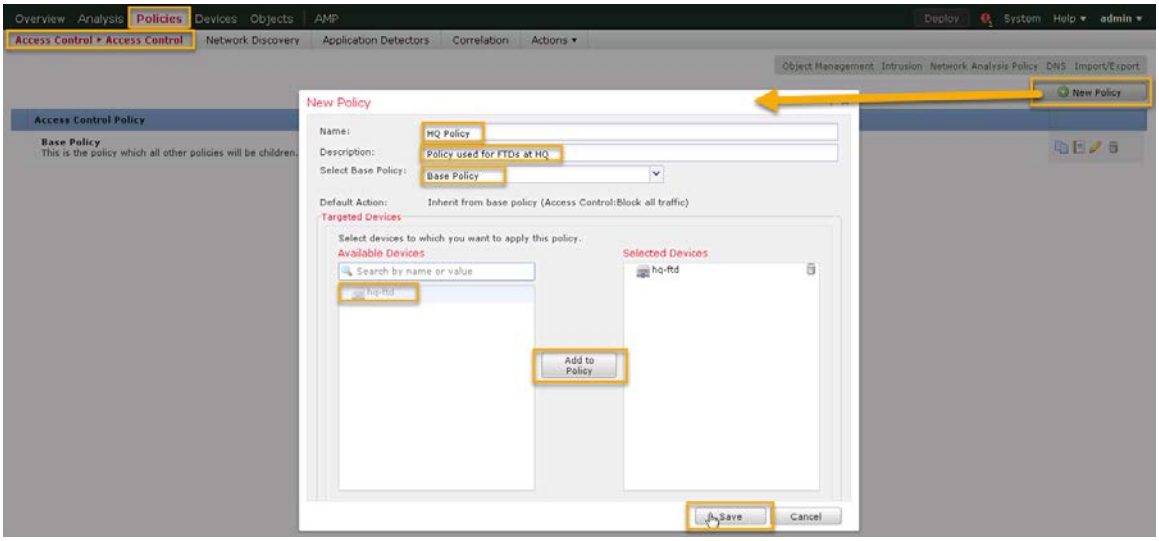
Notice how the "default action" is now inherited from the base policy and not configurable here. If you missed it, select None for the base policy to see the options re-appear. Be sure to end up selecting Base Policy before continuing.

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 118. Create new ACP

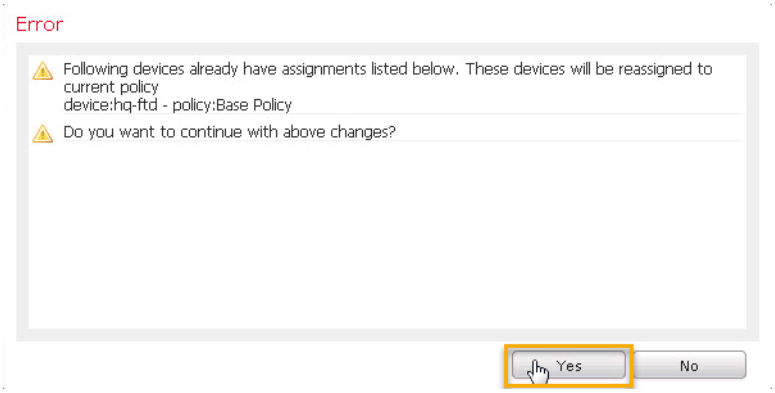


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

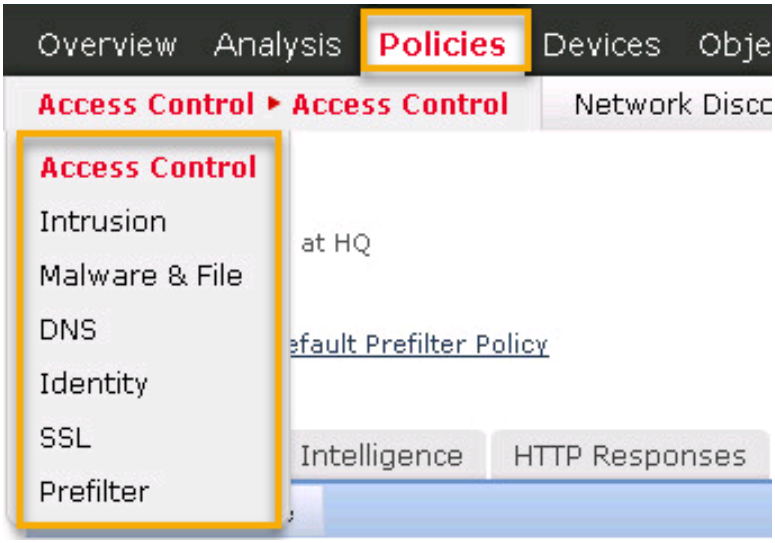
45. Click **Yes** to confirm changing hq-ftd's policy.

Figure 119. Allow hq-ftd to change ACPs



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 120. Lots of Policies

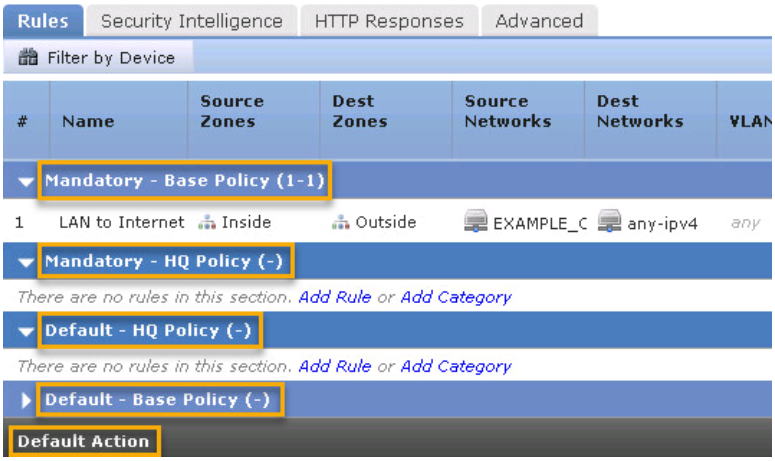


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 121. Nesting of ACP sections



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.

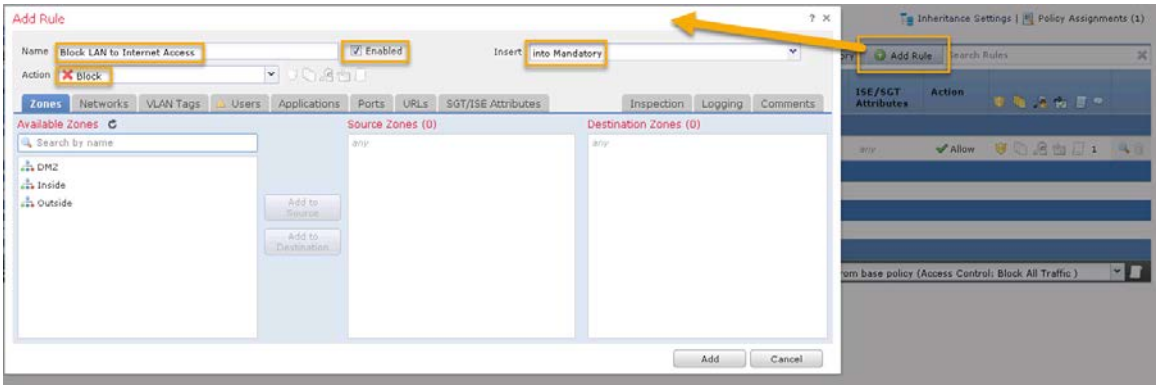
    a. Name: **Block LAN to Internet Access**

    b. Enabled: **Checked**

    c. Insert: **into Mandatory**

    d. Action: **Block**

Figure 122. Part 1 of adding rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

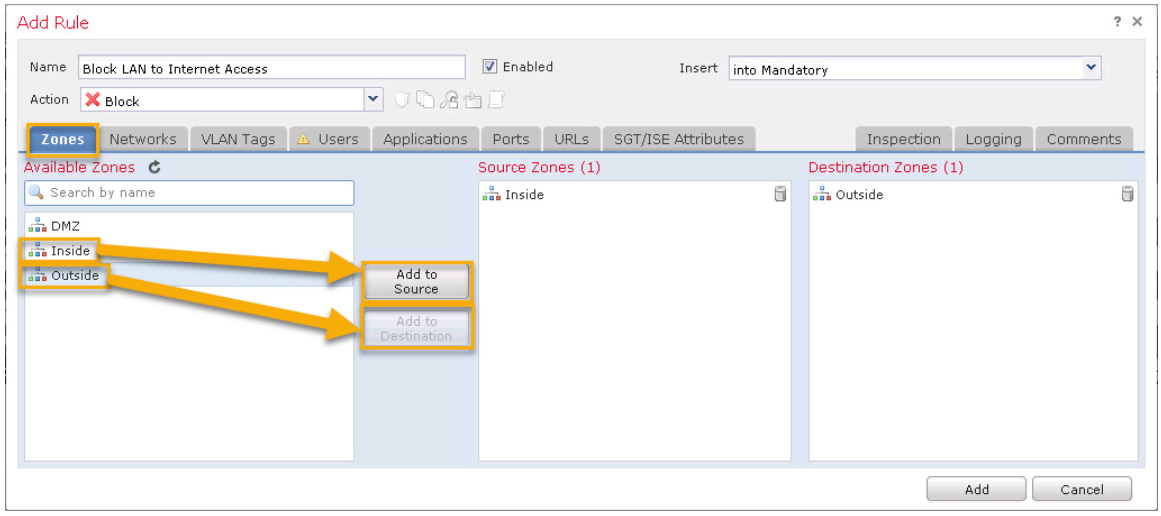
https://t.me/learningnets

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 123. Configure Zones tab

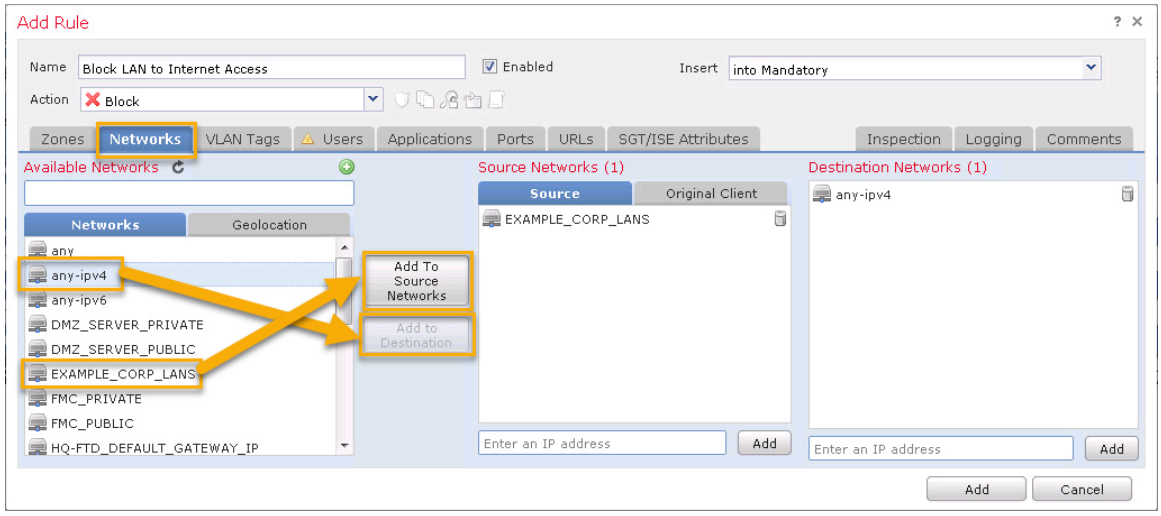


50. On the **Networks tab**:

    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 124. Configure Networks tab



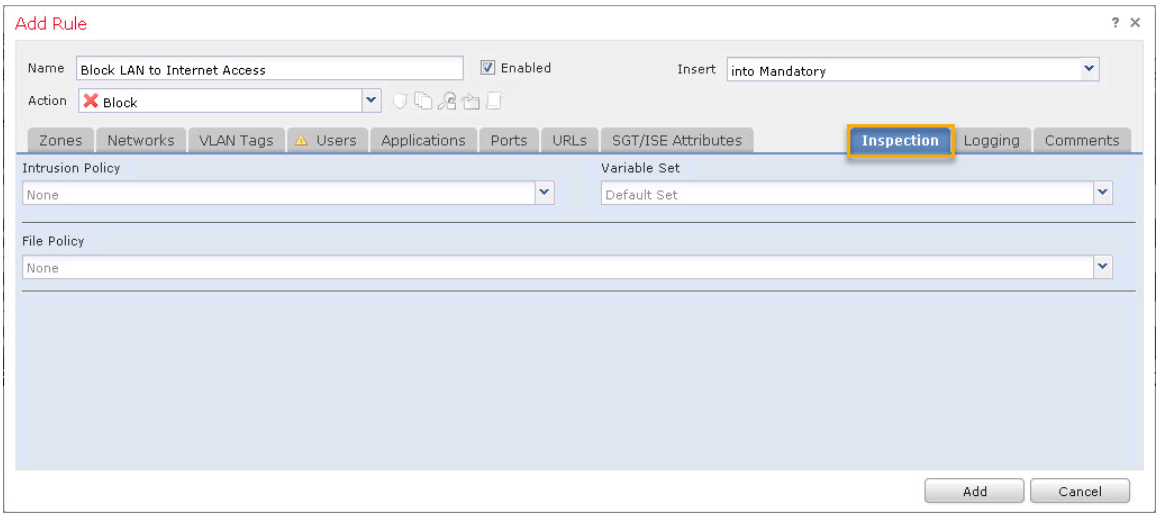
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

51. On the **Inspection tab**:

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

Figure 125. Can't configure Inspection tab



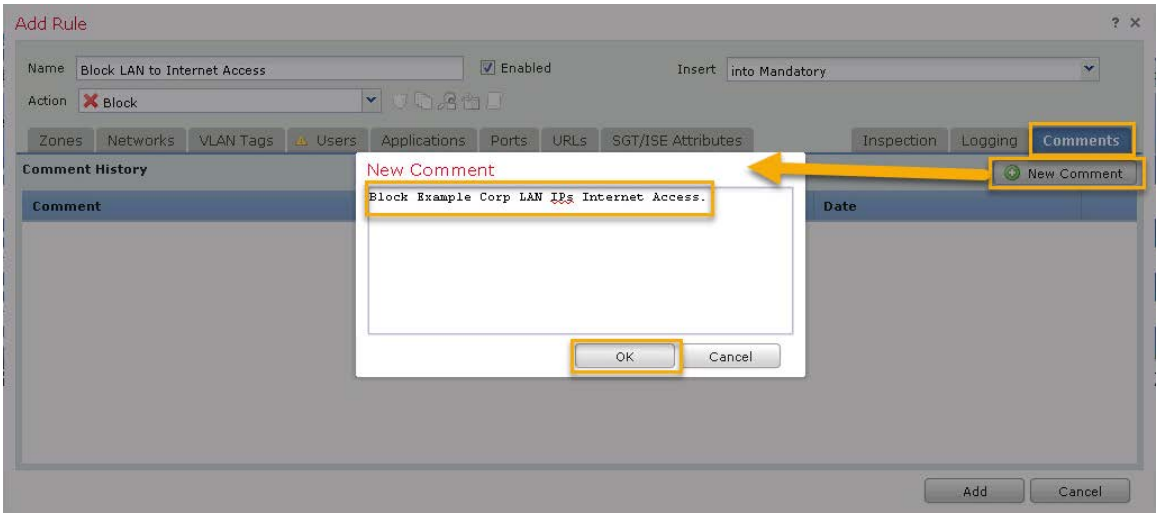
52. On the **Comments tab**:

    a. Click **New Comment**

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

    c. Click **OK.**

Figure 126. Add a comment

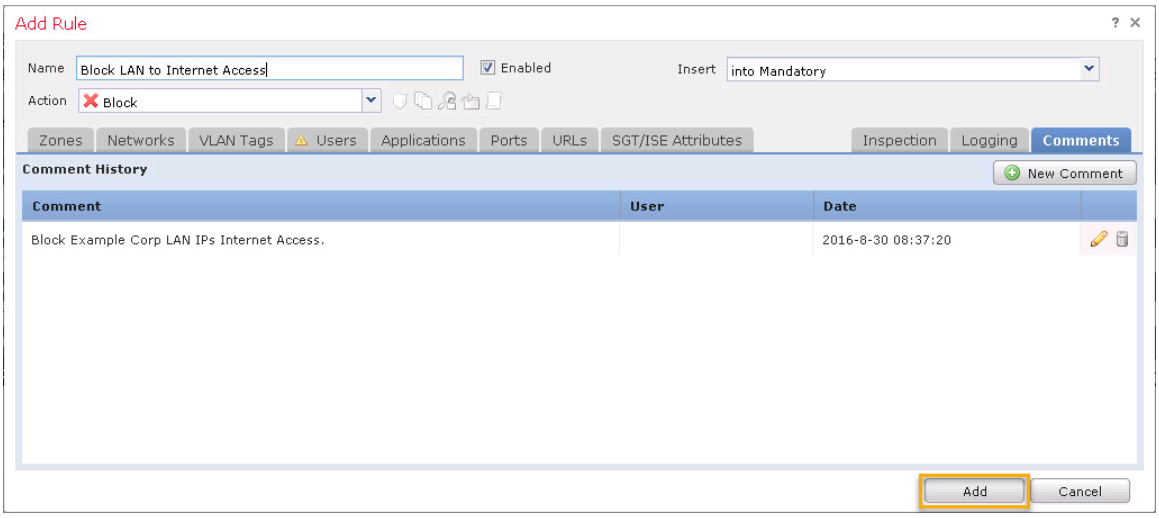


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

53. Click **Add**.

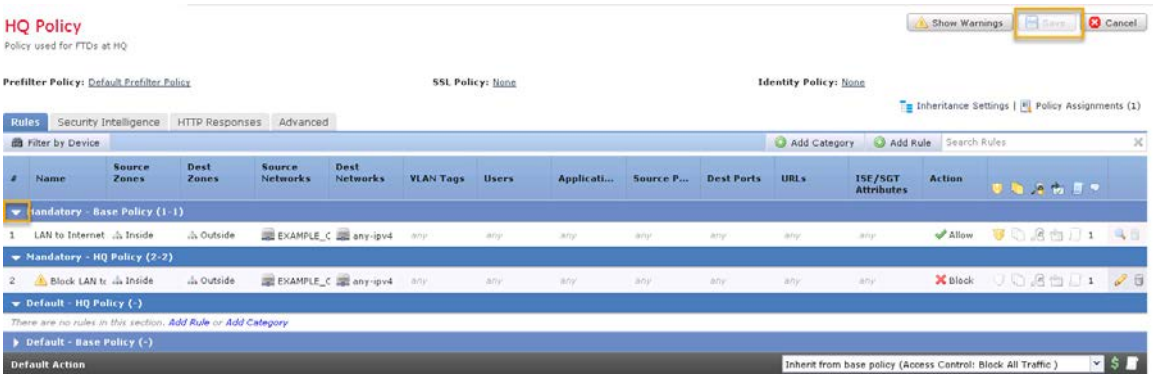
Figure 127. Add rule



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.

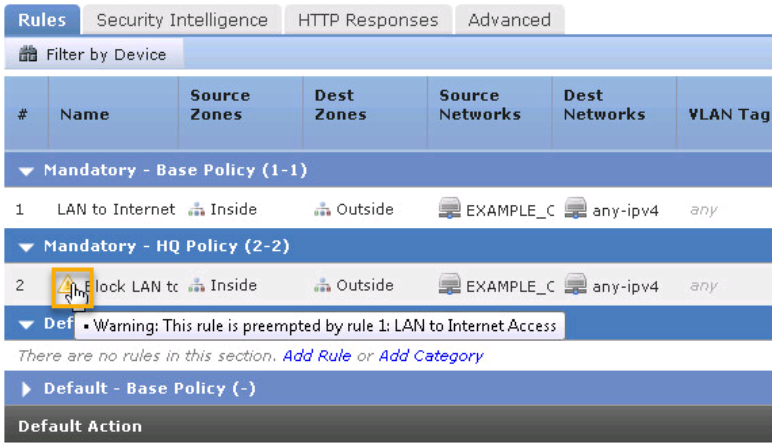
Figure 128. Save and Expand Mandatory – Base Policy section



https://t.me/learningnets

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 129. Yellow triangle warning



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

Figure 130. Edit Base Policy ACP



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

Figure 131. Edit ACP rule

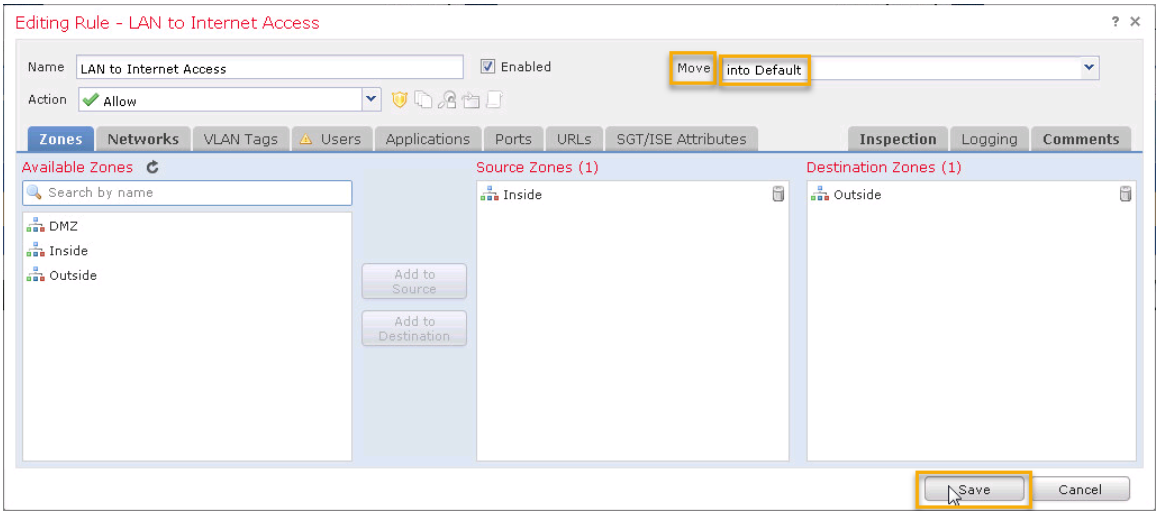


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

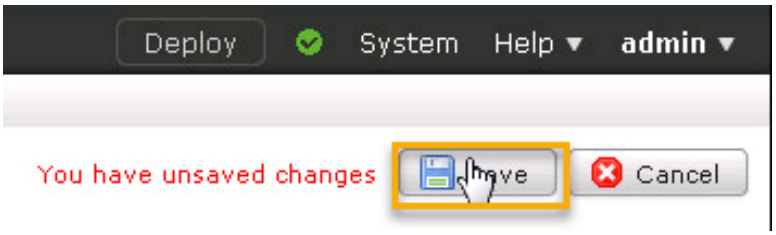
59. Click the **Move** link.
60. Using the dropdown select **into Default**.
61. Click **Save** to save the change to this rule.

Figure 132. Move rule to into Default



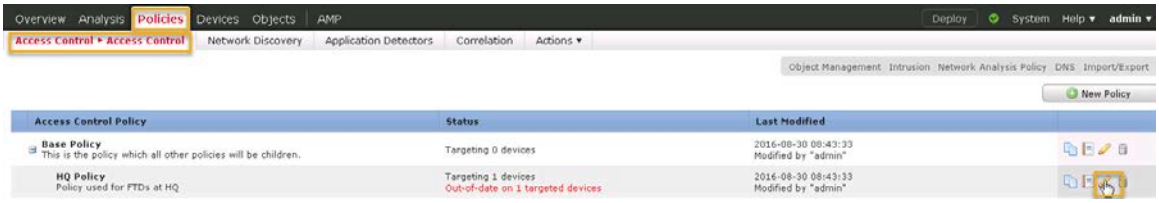
62. Click **Save** to save your changes.

Figure 133. Save changes to FMC



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 134. Edit HQ Policy ACP

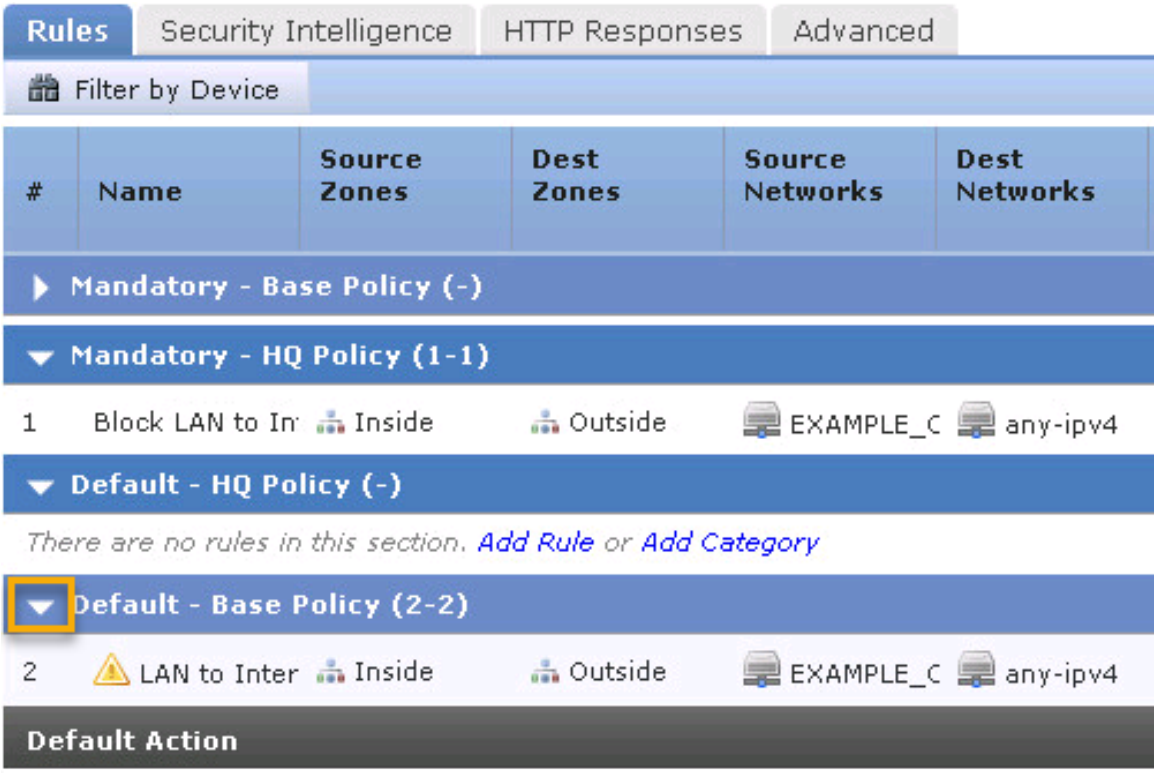


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

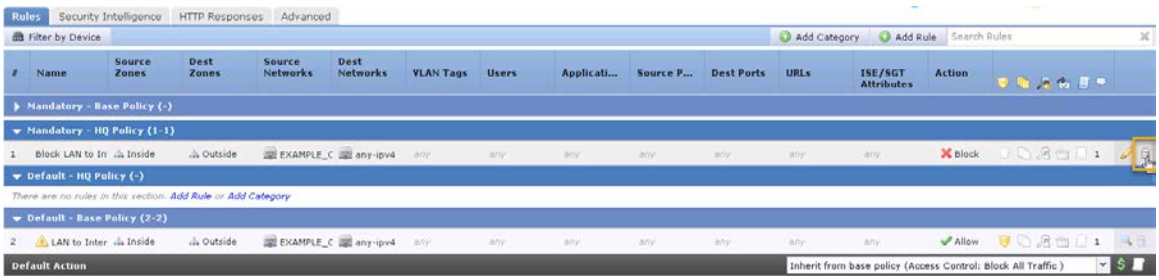
Figure 135. Order of ACP rules is important



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 136. Delete Block rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 137. Confirm deletion



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:

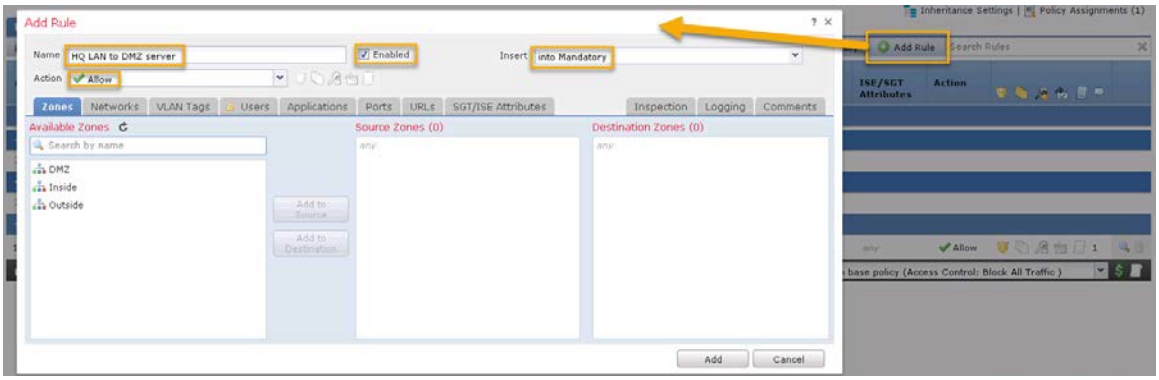
    a. Name: **HQ LAN to DMZ server**

    b. Enabled: **Checked**

    c. Insert: **into Mandatory**

    d. Action: **Allow**

Figure 138. Part 1 of adding a rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

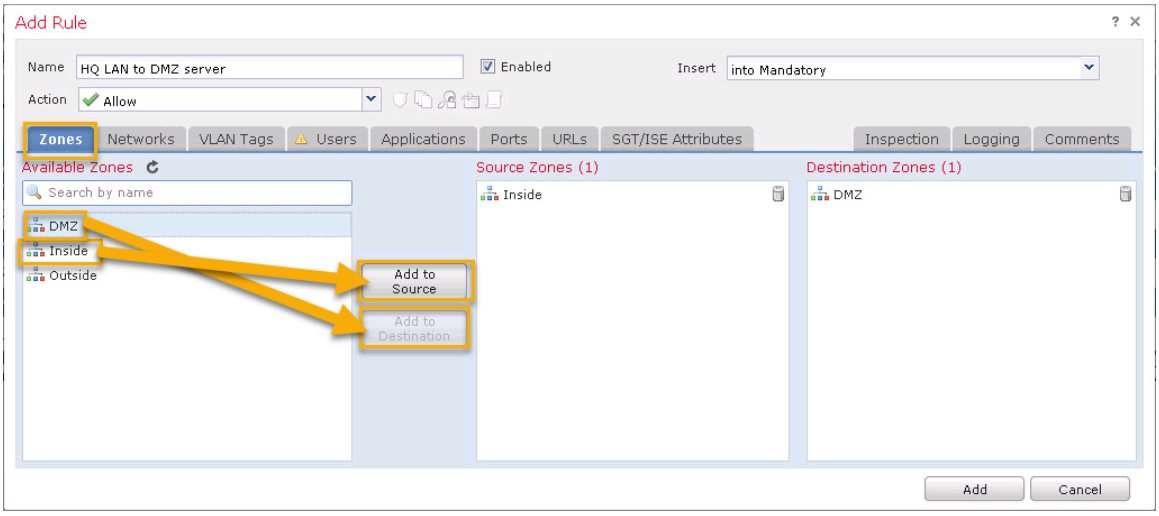
https://t.me/learningnets

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 139. Configure Zones tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

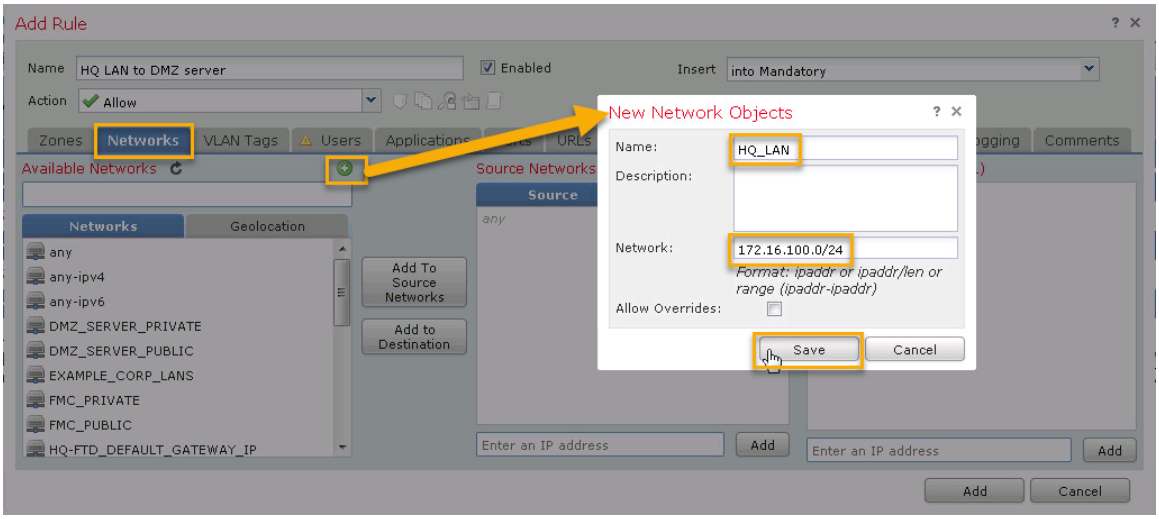
    b. In the New Network Objects window fill out the following:

        i. Name: **HQ_LAN**

        ii. Network: **172.16.100.0/24**

        iii. Click **Save**.

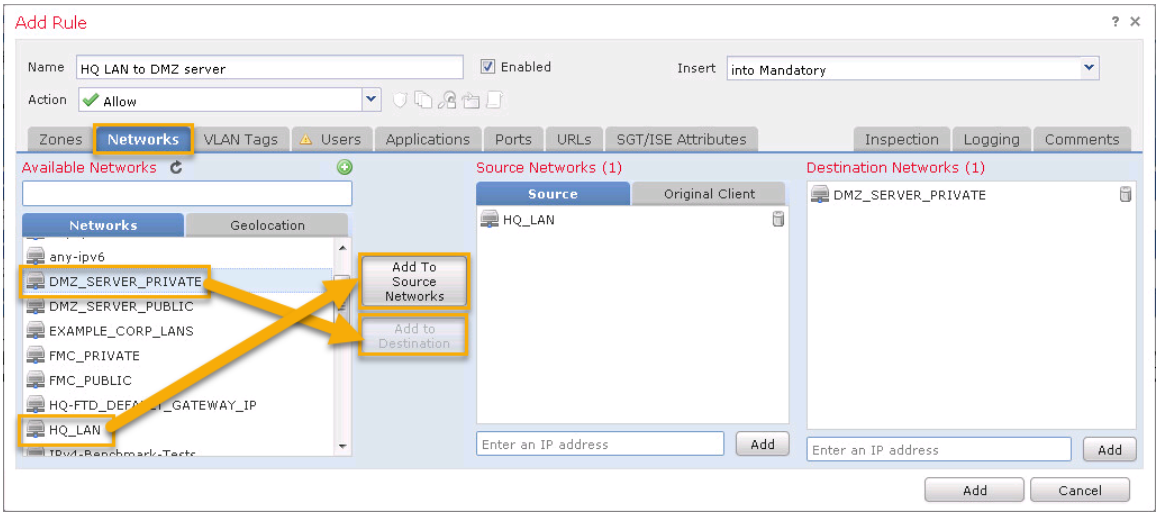
Figure 140. Create Network Object



    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 141. Configure Networks tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

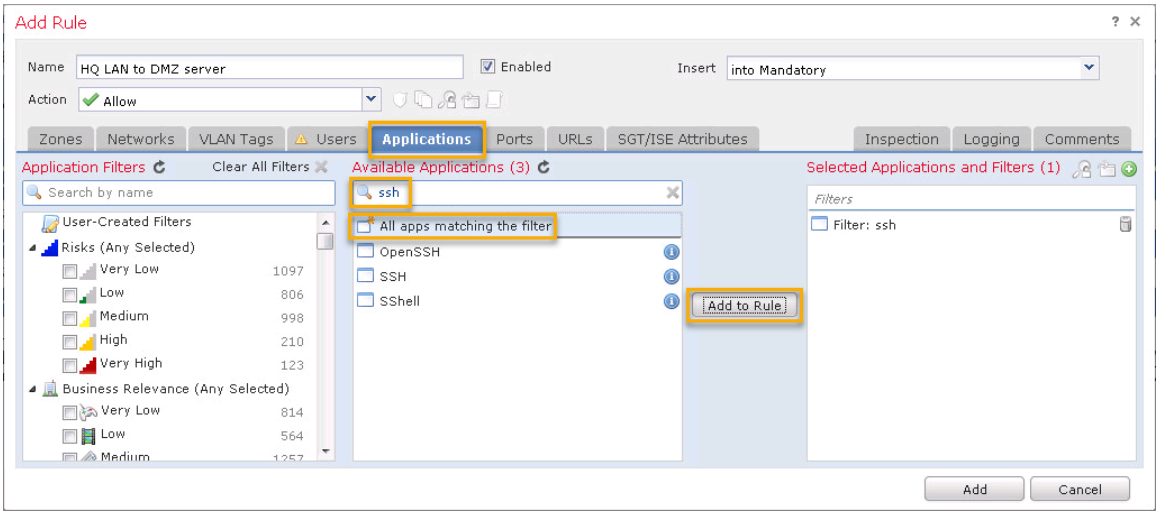
https://t.me/learningnets

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.

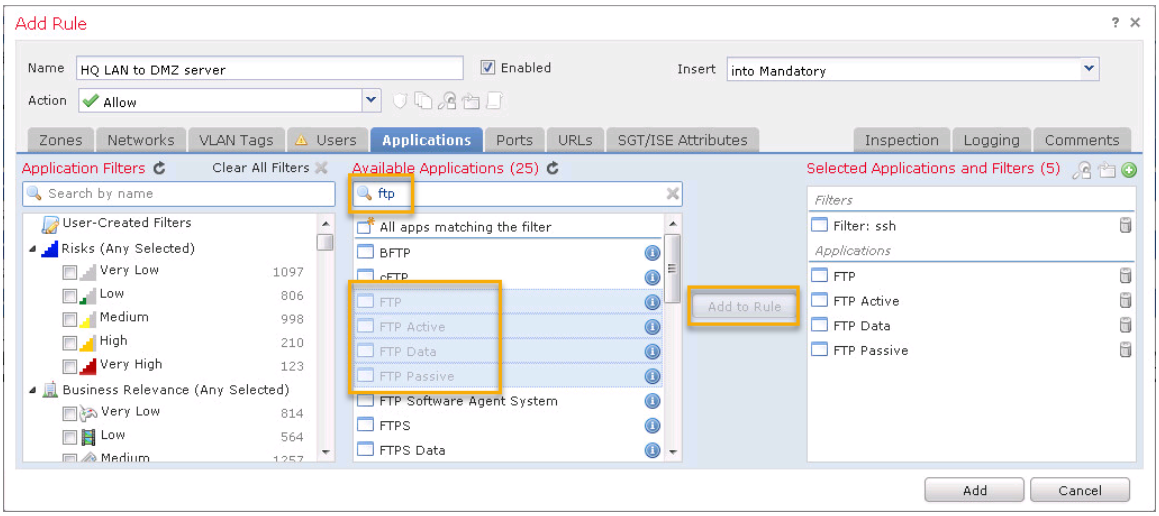
Figure 142. Add ssh to rule



    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 143. Add ftp to rule



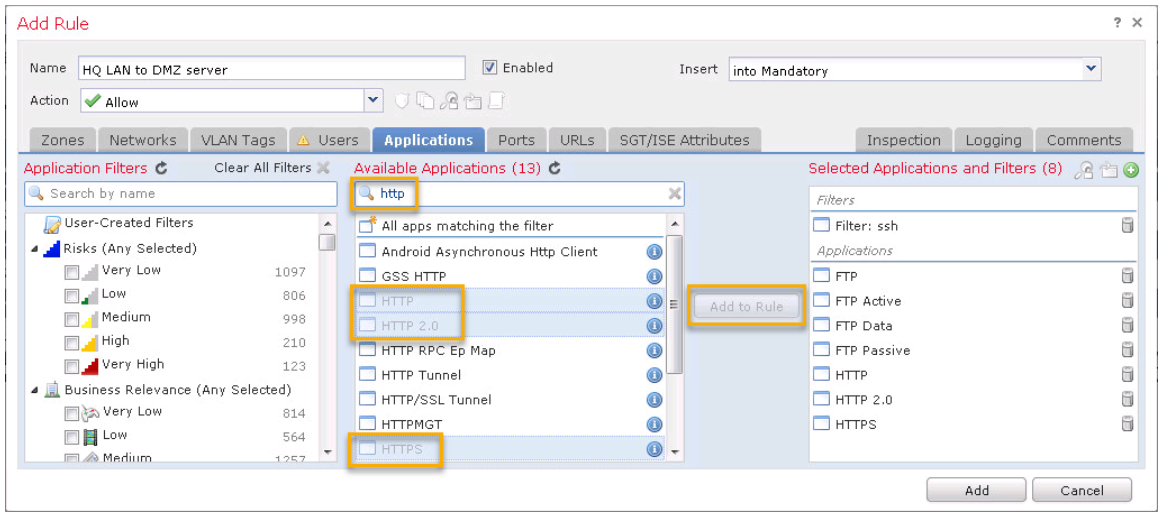
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

Figure 144. Add http/https to rule

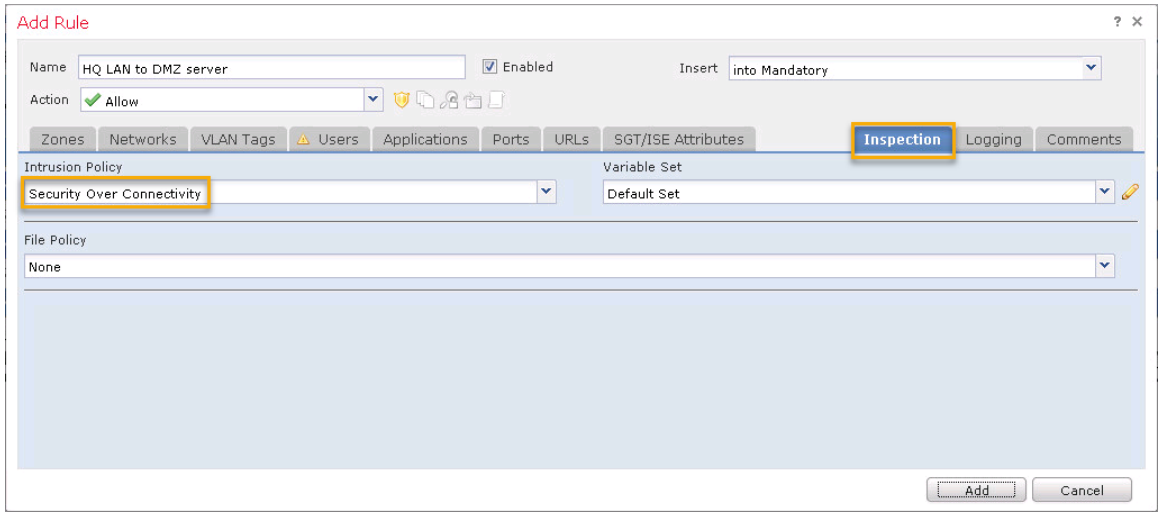


Notice that you can select All apps matching a filter, some of them in a row (using Shift), or some of them not continuously next to each other (using Ctrl). Also, did you notice how you didn't specify any UDP or TCP ports? The FTD actually goes well beyond just filtering based on "ports and protocols" 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 145. Configure Inspection tab



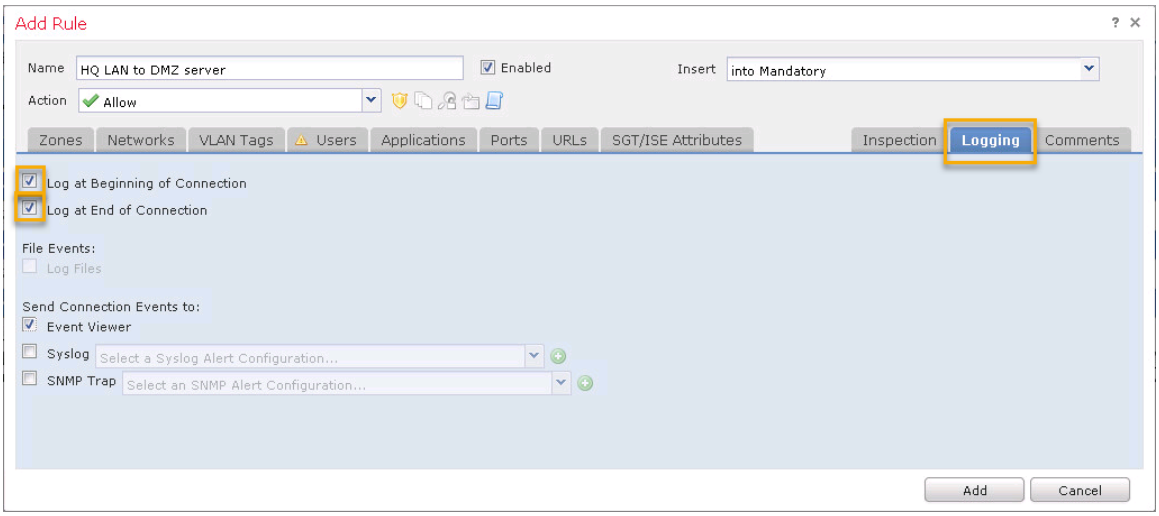
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 146. Configure the Logging tab



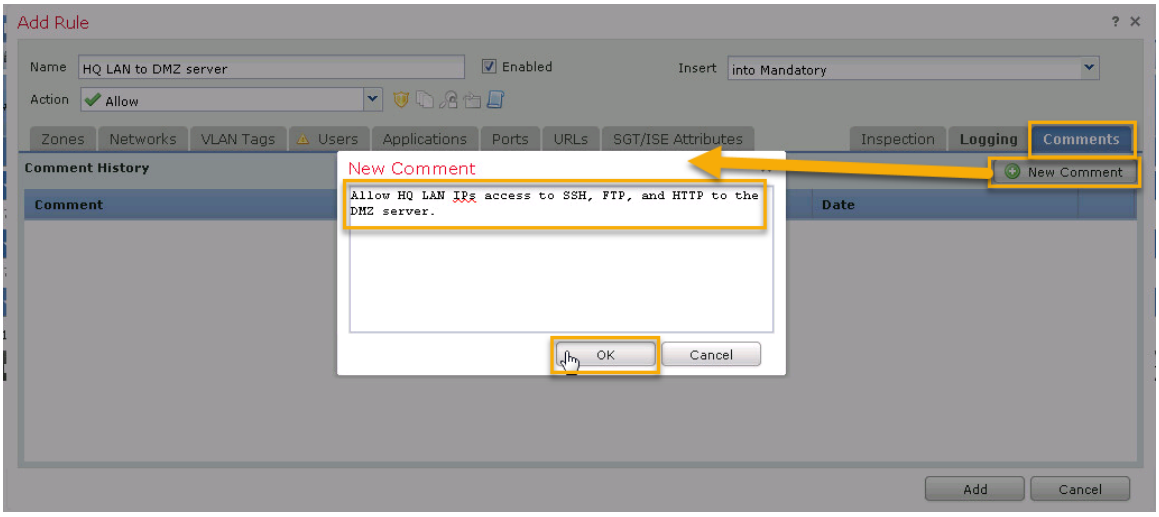
73. On the **Comments tab**:

    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 147. Create comment

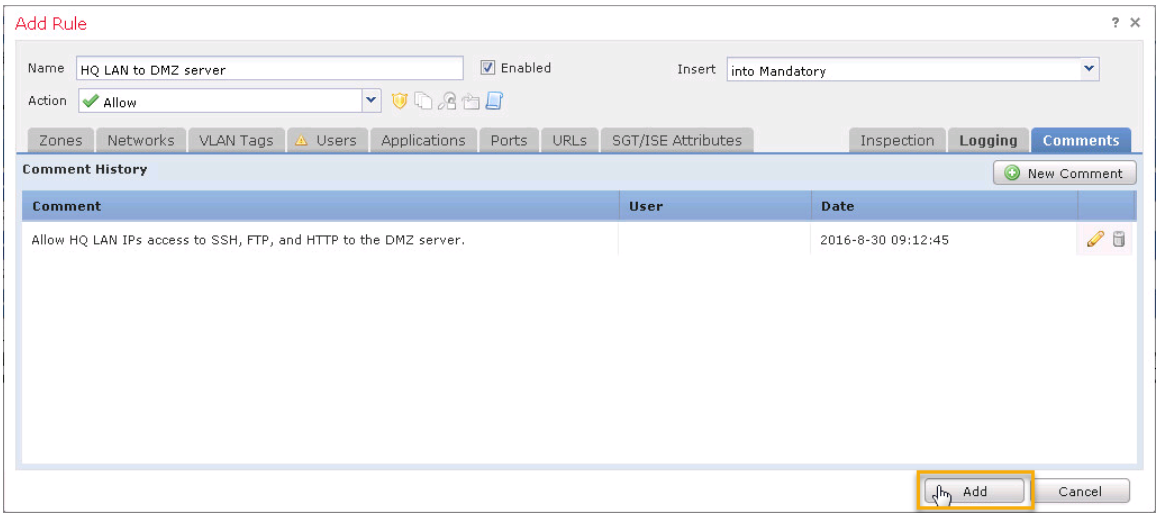


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

74. Click **Add**.

Figure 148. Add the ACP rule



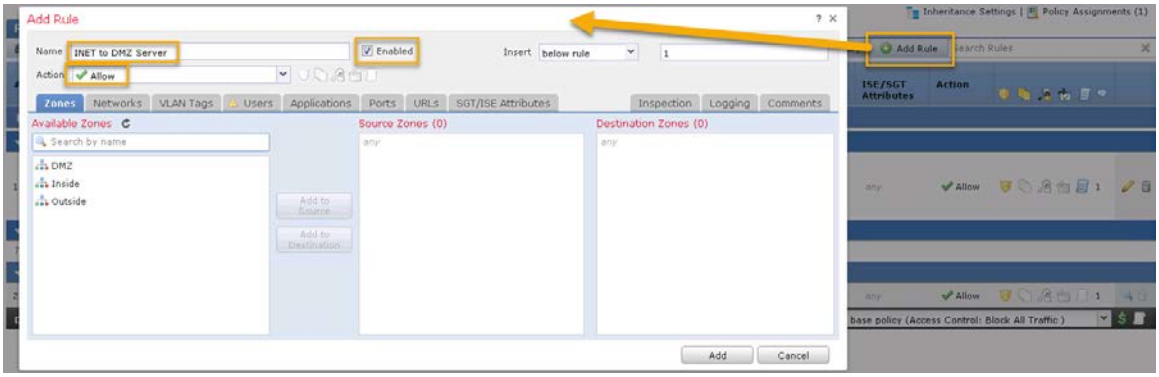
75. Create another rule only allowing HTTP access from the Internet to DMZ_Server. Click **Add Rule** and then use the following information to fill out the needed options:

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

    b. Enabled: **Checked**

    c. Action: **Allow**

Figure 149. Part 1 of adding ACP rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

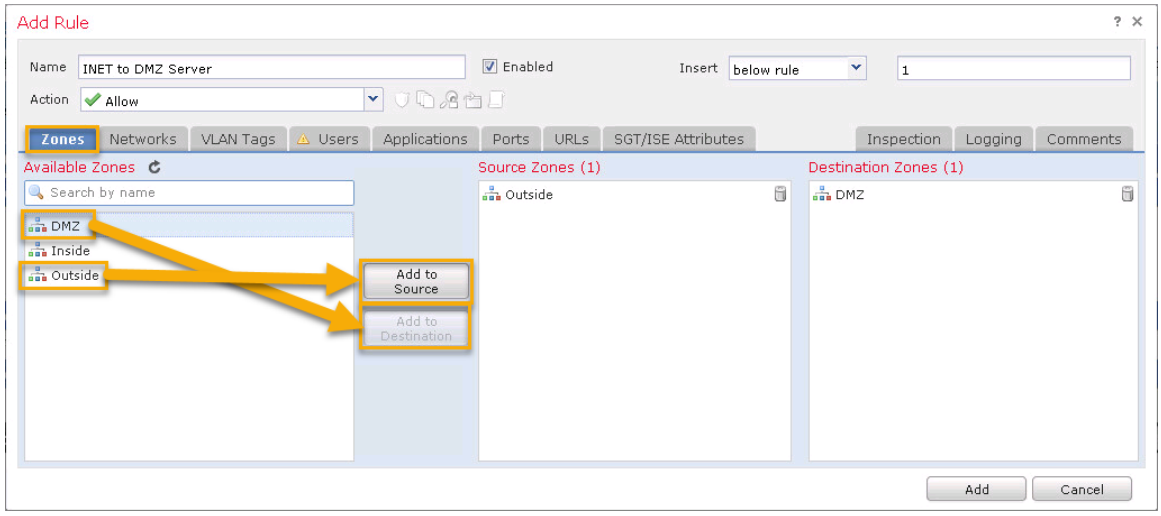
https://t.me/learningnets

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 150. Configure Zones tab

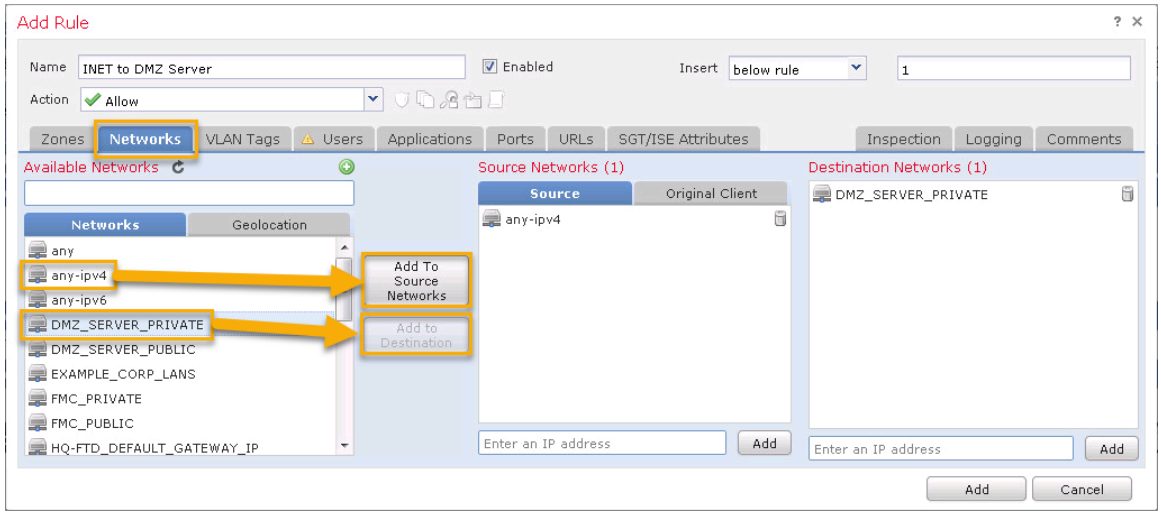


77. On the **Networks tab**:

    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 151. Configure Networks tab



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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

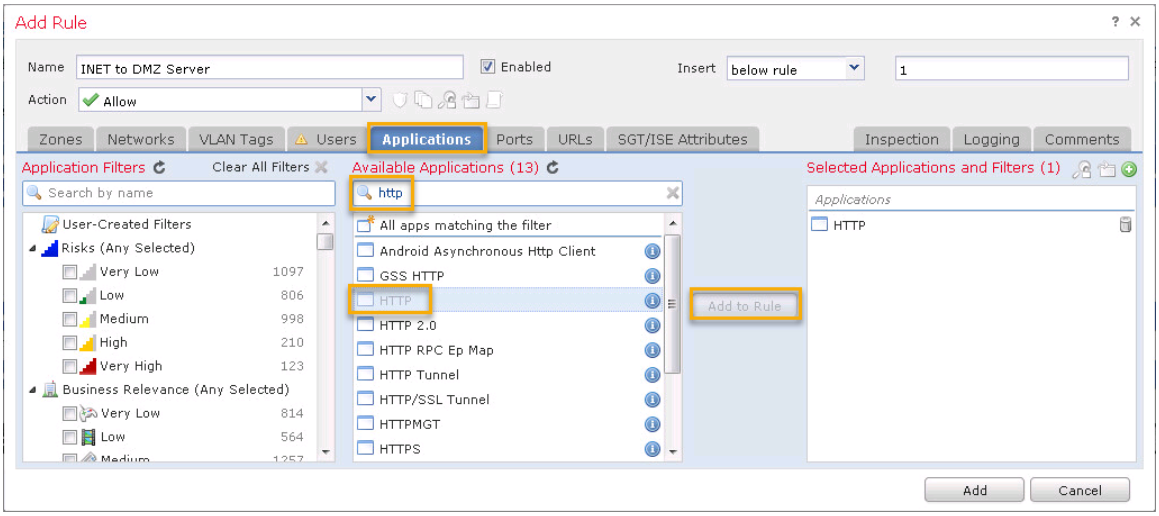
https://t.me/learningnets

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.)

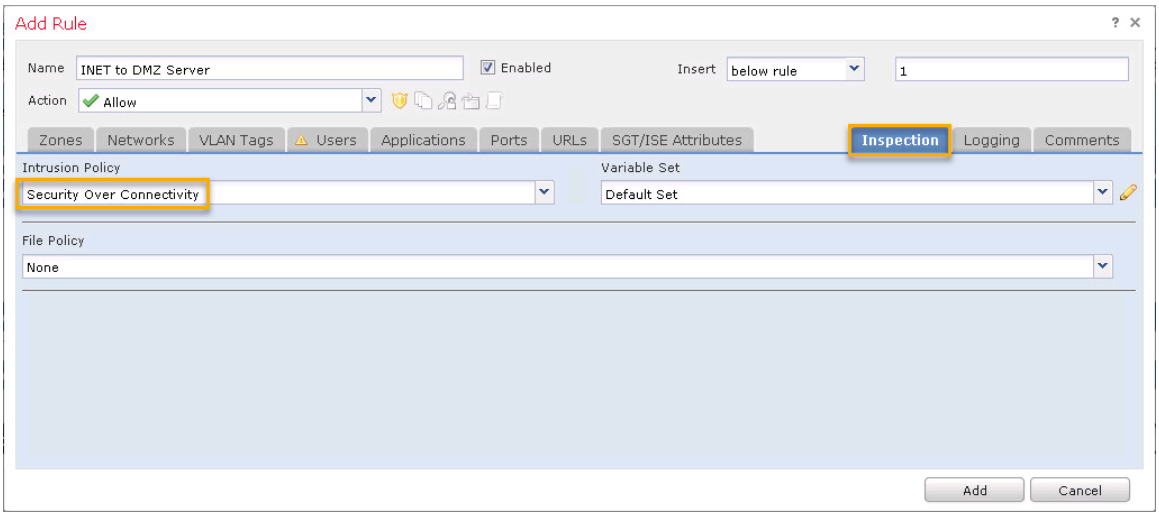
Figure 152. Configure Applications tab



79. On the **Inspection tab**:

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

Figure 153. Configure Inspection tab



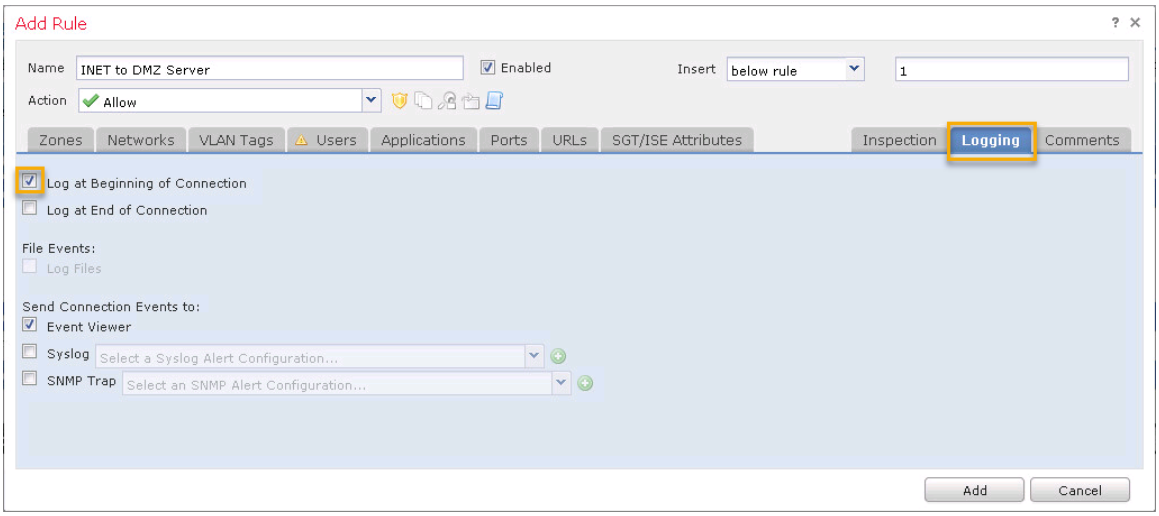
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 154. Configure Logging tab



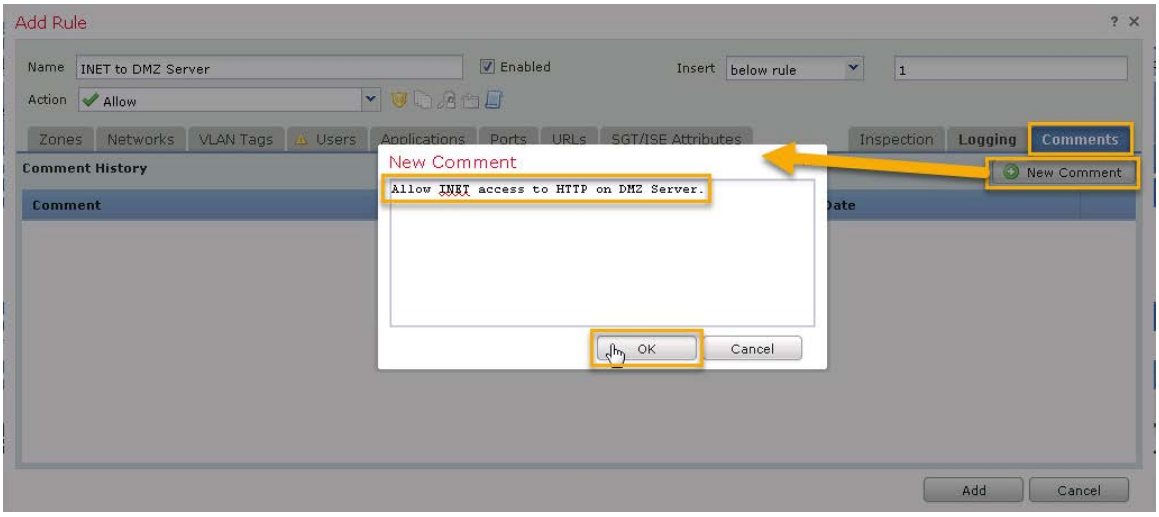
81. On the **Comments tab**:

    a. Click **New Comment**

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

        ii. Click **OK**

Figure 155. Add comment to rule

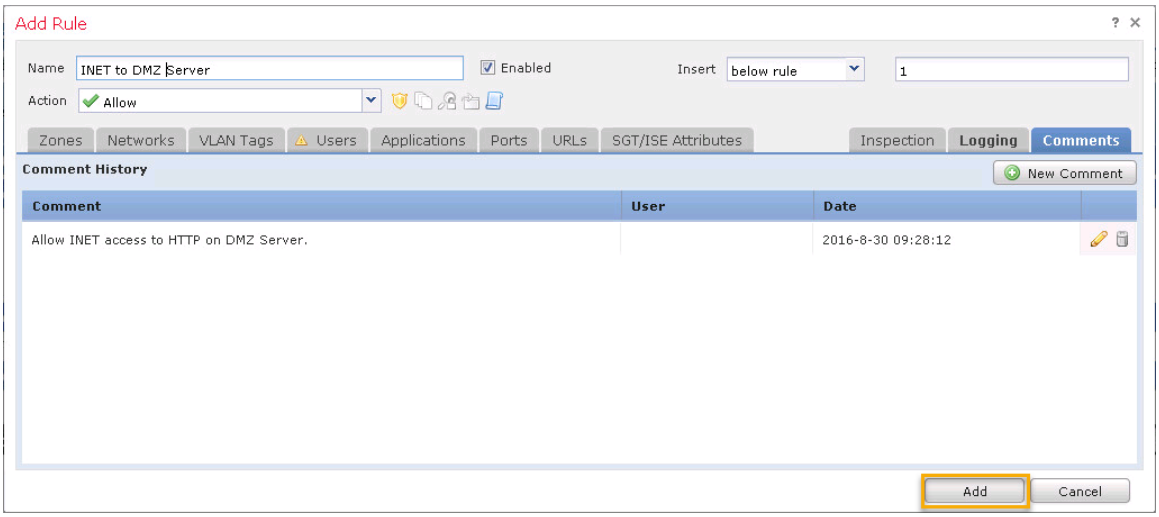


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

82. Click **Add**

Figure 156. Add rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

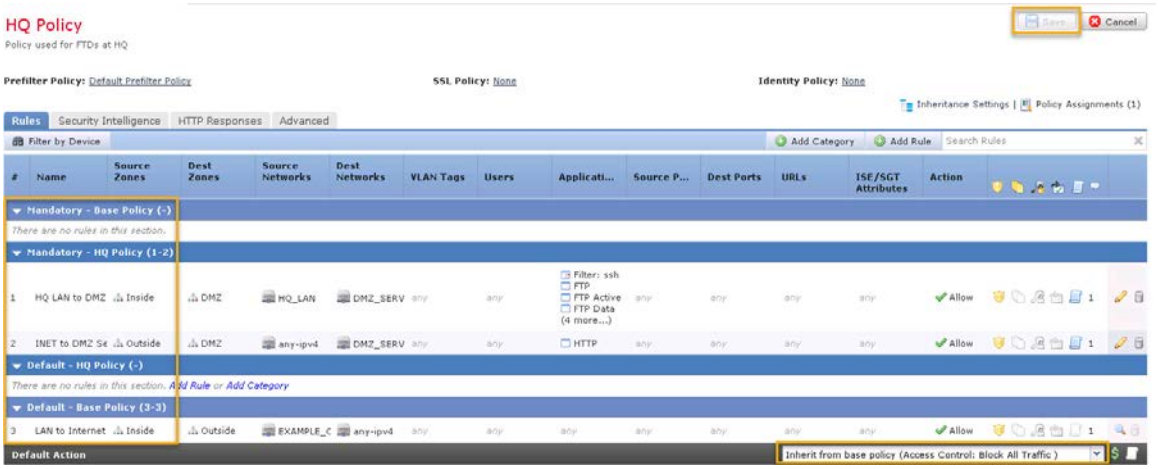
        ii. The second rule allows HTTP access to the DMZ server from the INET.

    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 157. Save and Review ACP Rules



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 158. Edit Base Policy ACP

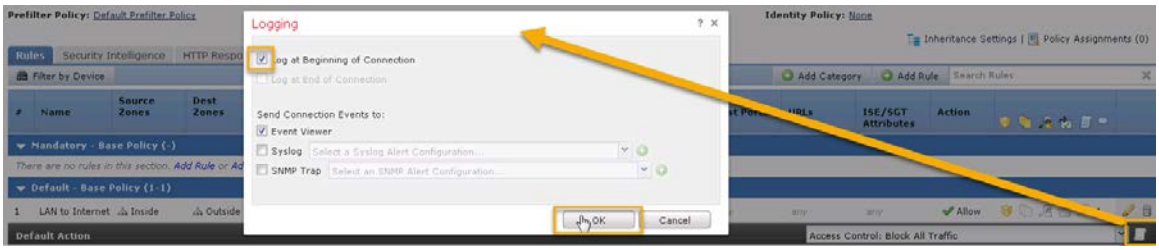


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 159. Add logging to Default Action



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).

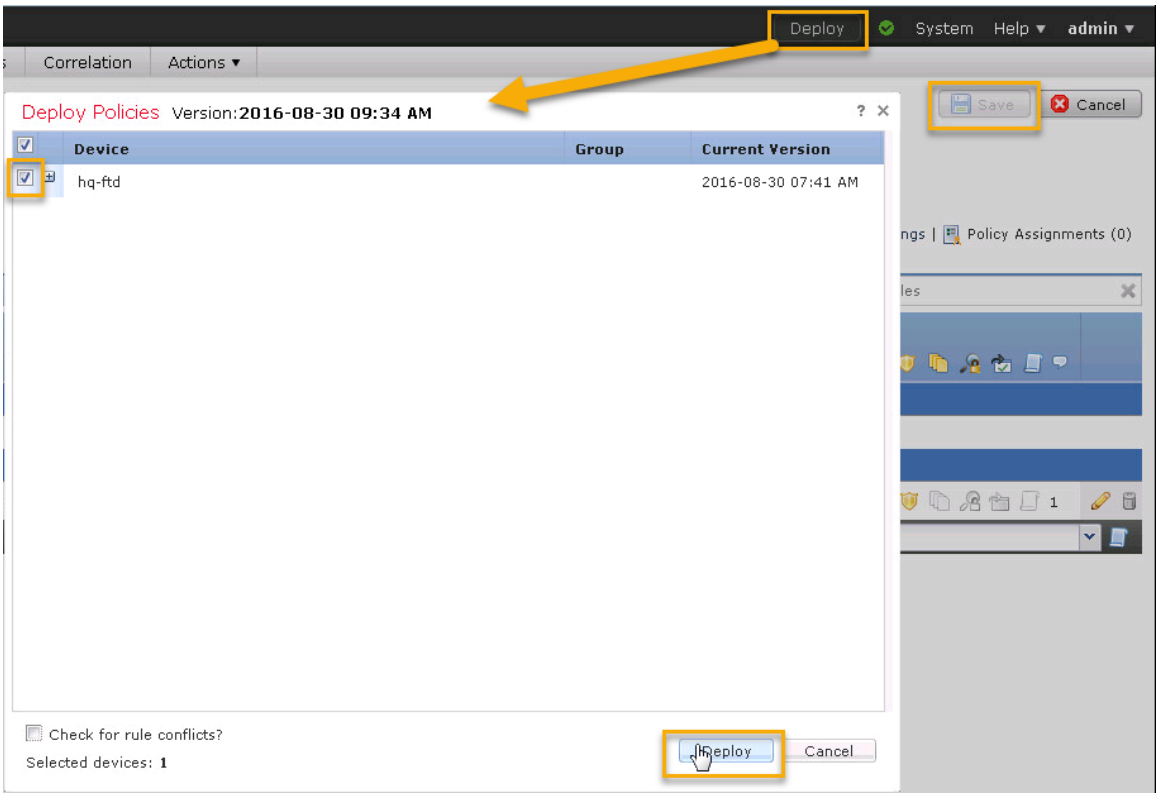
I think leaving the Default Action as a catch-all for anything you may have missed (or is nefarious, such as a spoofed source IP address) is a good thing. Other security engineers might suggest that the Default Action be used as a catch-all for certain known traffic flows (like the DMZ server as explained 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 160. Save and Deploy to hq-ftd



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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

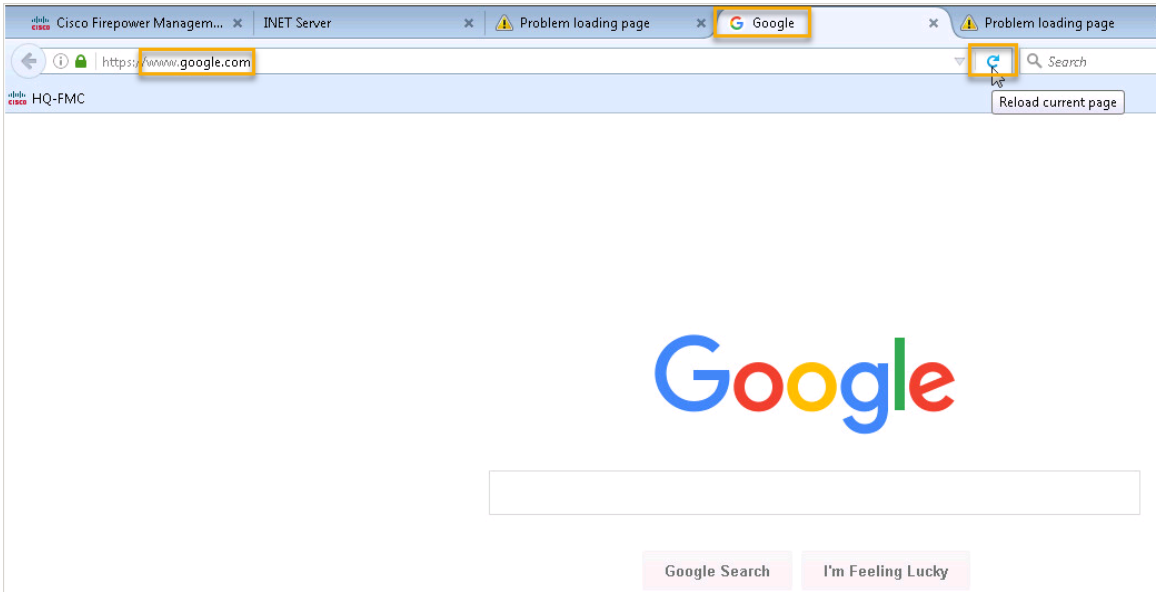
https://t.me/learningnets

Testing INET Access and Access Control Policies for the HQ Location

89. Once the deployment is completed, on **hq-wkst** perform the following tests:

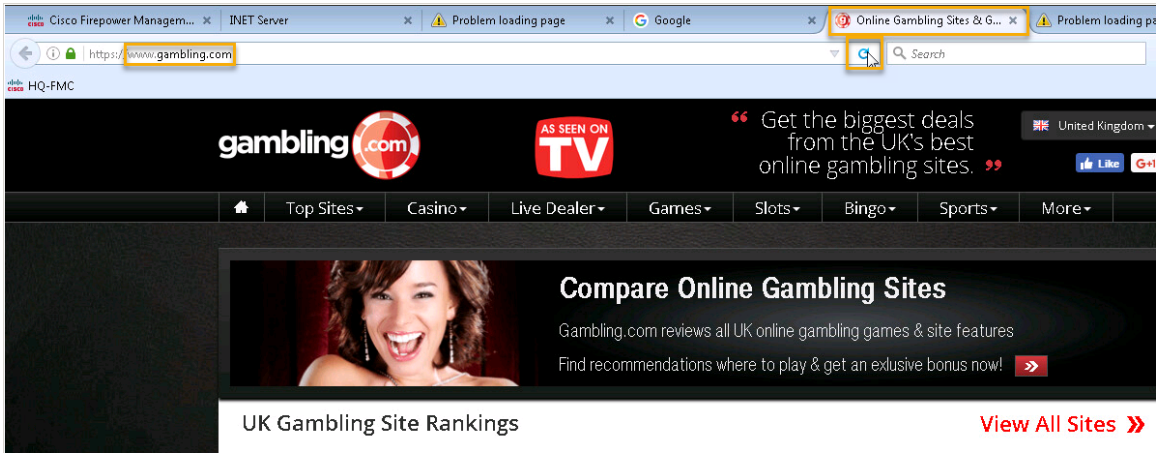
    a. In **Firefox** browse to **the Google home page** (the 4th tab). This page should still resolve.

Figure 161. Google resolves



    b. 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 162. Gambling.com resolves

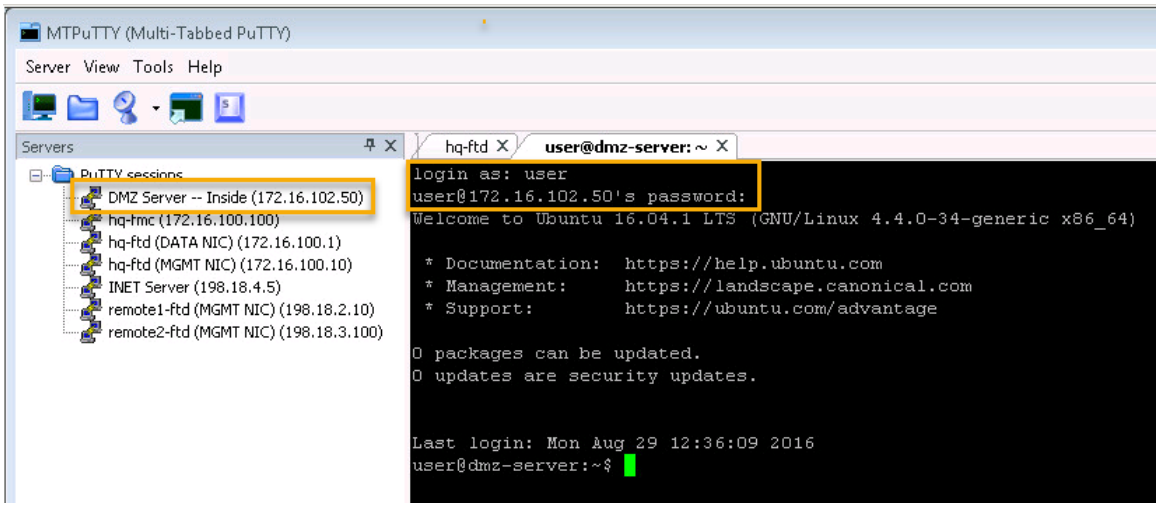


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

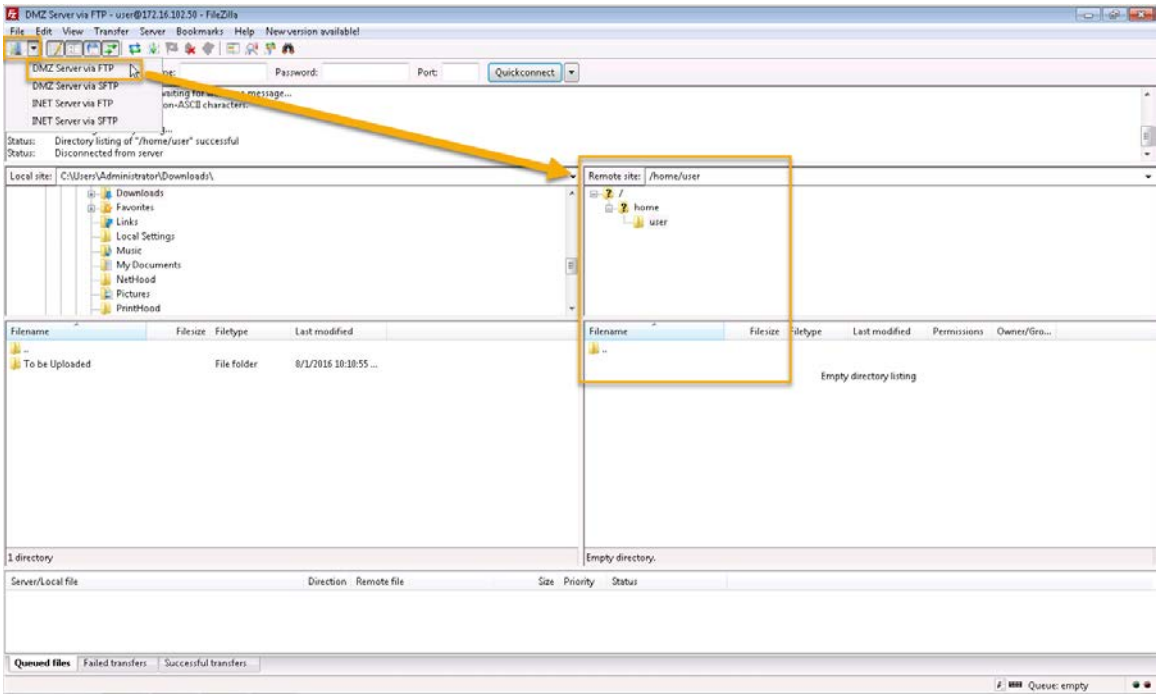
c. Open **MTPutty** and using the **DMZ Server -- Inside** saved bookmark, ssh to 172.16.102.50. Login in as **user/C1sco12345**.

Figure 163. SSH to dmz-server works



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

Figure 164. FTP to dmz-server works



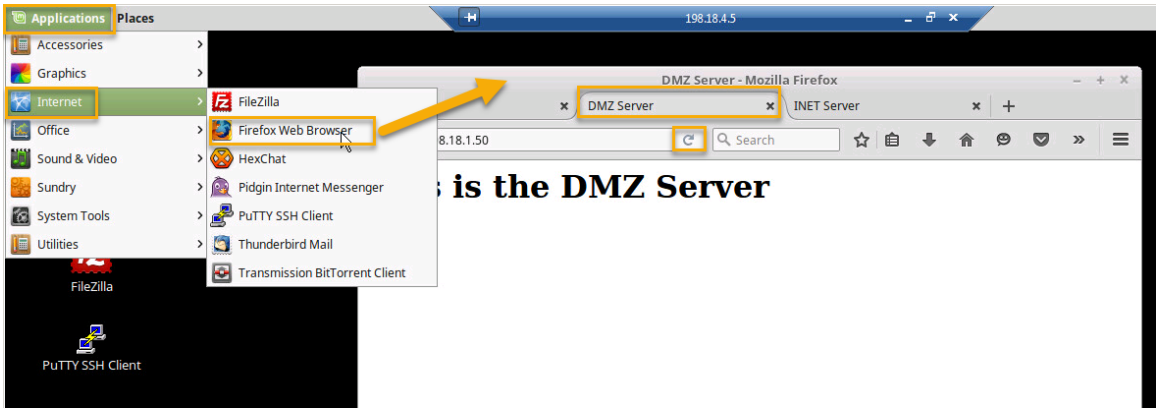
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

90. Switch over to the RDP session to the inet-server. 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. On the **inet-server** perform the following tests:

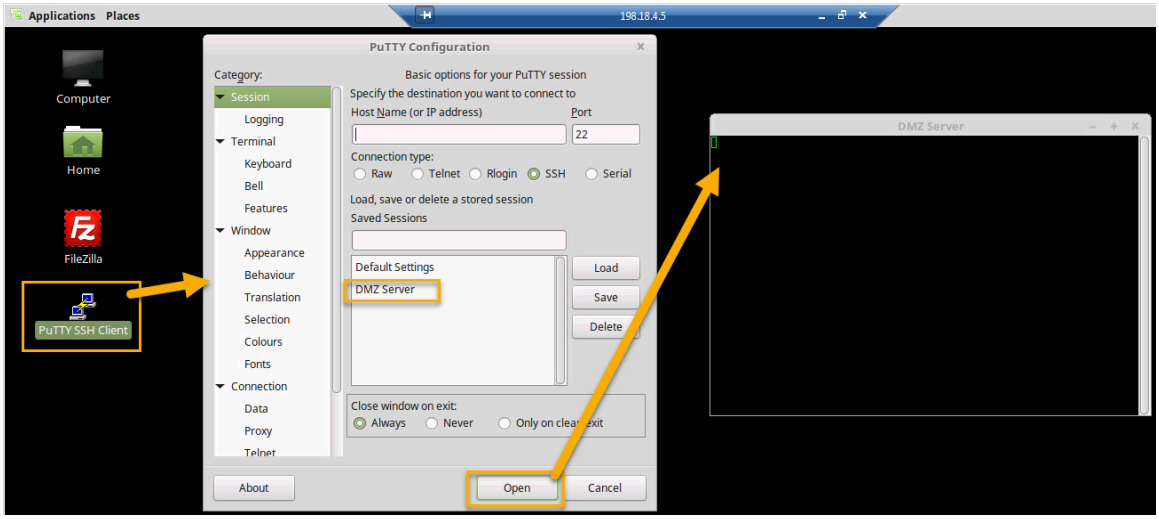
    a. In **Firefox** go to **http://198.18.1.50** (the DMZ Server).

Figure 165. INET to dmz-server web page works



    b. 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.

Figure 166. SSH to dmz-server fails

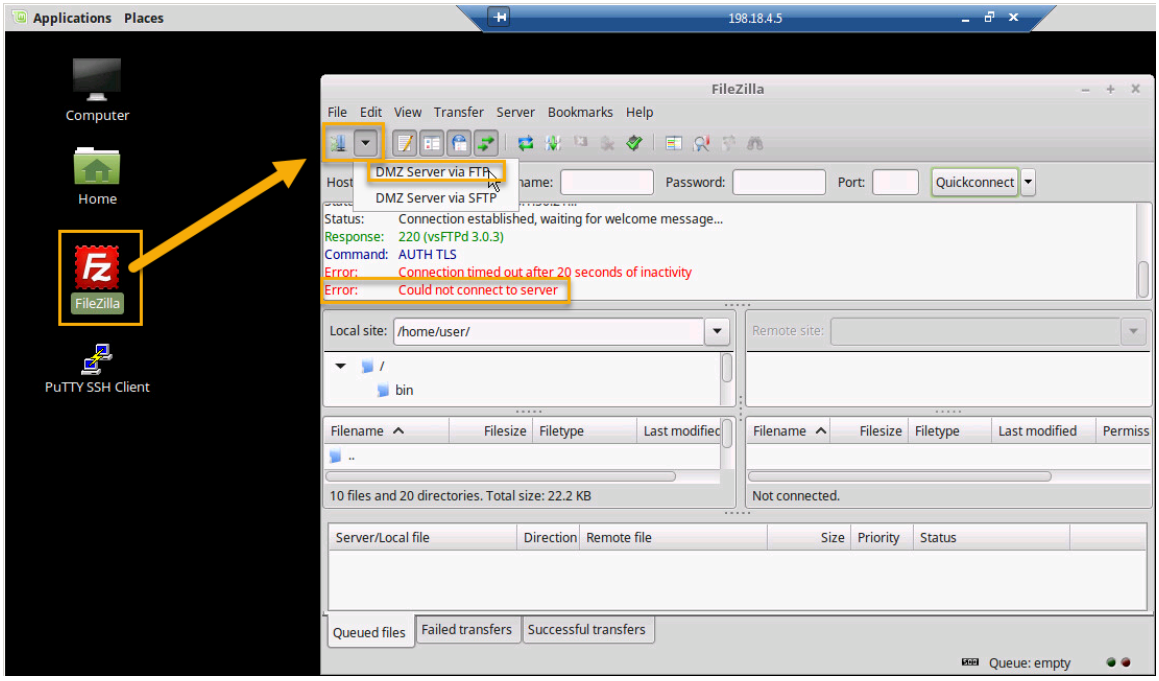


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

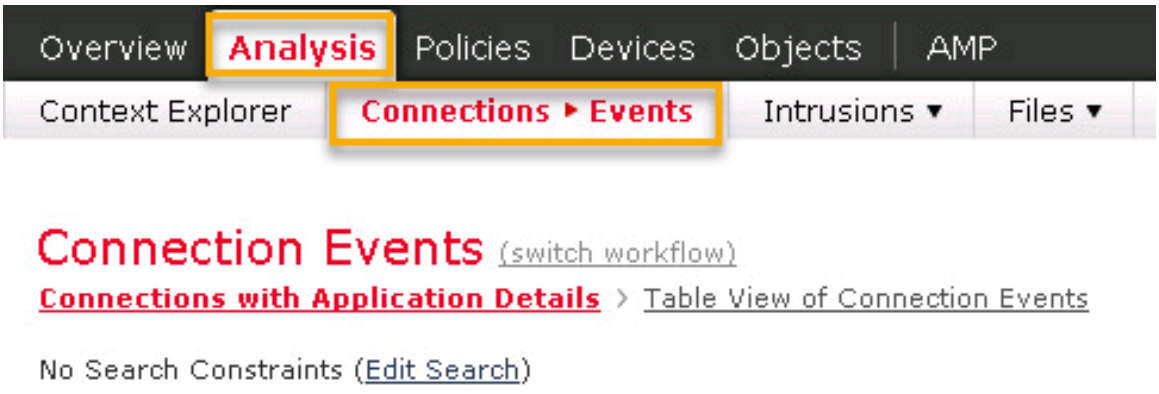
c. Open **FileZilla** and using the **DMZ Server via FTP** bookmark FTP to 198.18.1.50. This should fail.

Figure 167. FTP to dmz-server fails



91. 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 168. Navigate to Connection Events

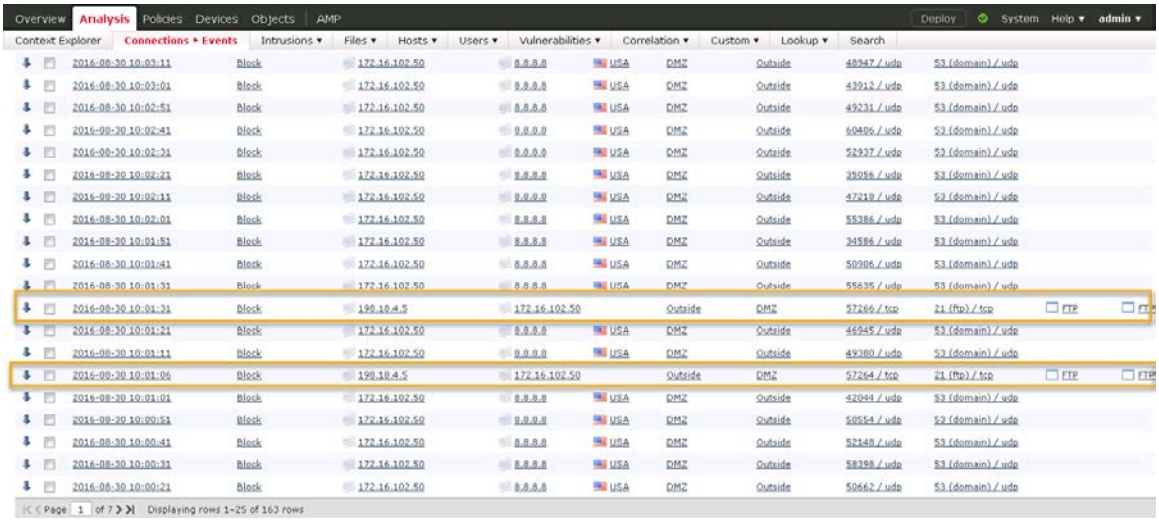


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

92. 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 169. Connection Events



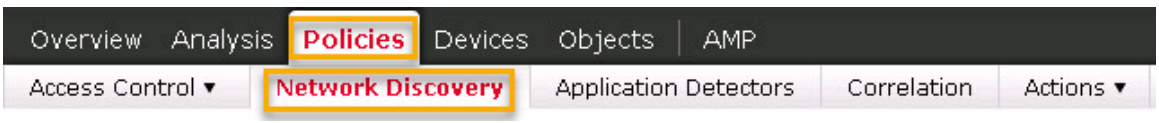
Did you notice all the Block attempts to 8.8.8.8? Which device is generating all that traffic? Which rule is being matched to block this traffic? Should we be logging all this traffic or should we tune the Access Control Policy rules to either permit this traffic or silence the logging of this traffic?

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.

93. Navigate to Policies > Network Discovery.

Figure 170. Navigate to Network Discovery

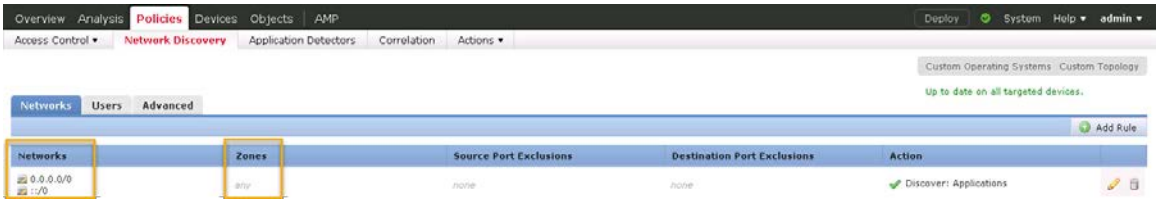


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

94. 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.

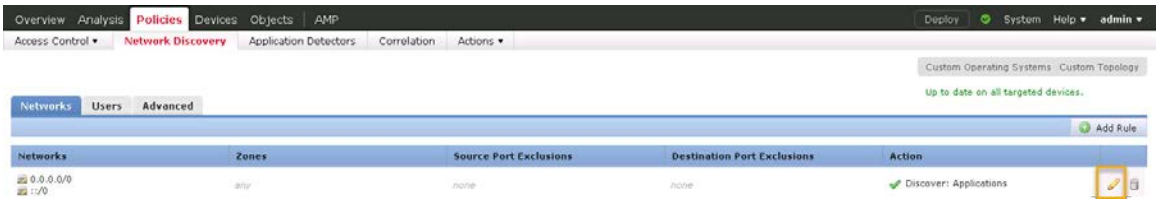
Figure 171. Default rule



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.

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

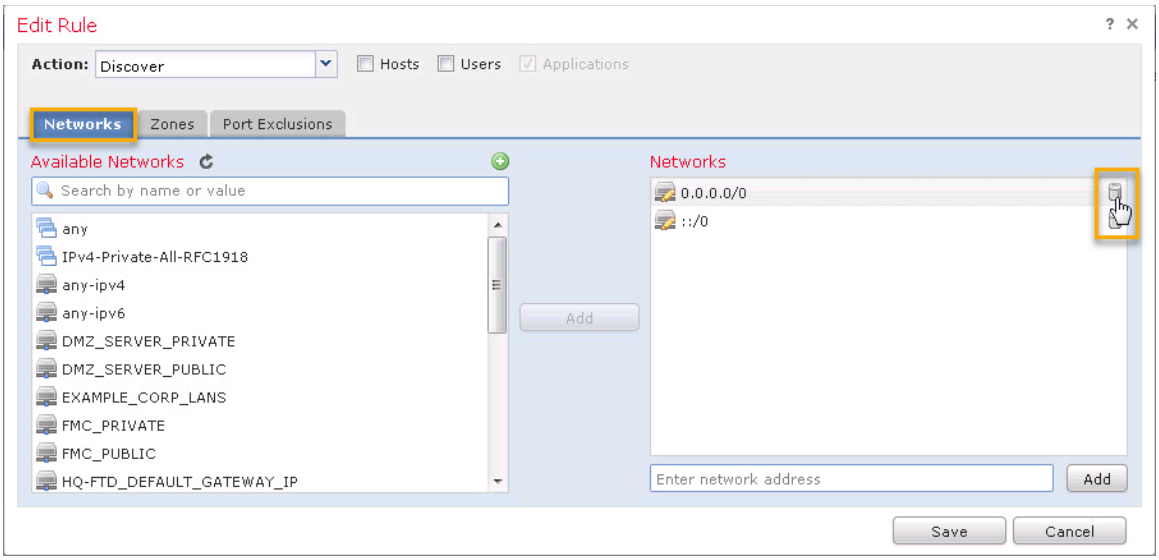
Figure 172. Edit the current rule



96. 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 173. Delete existing networks

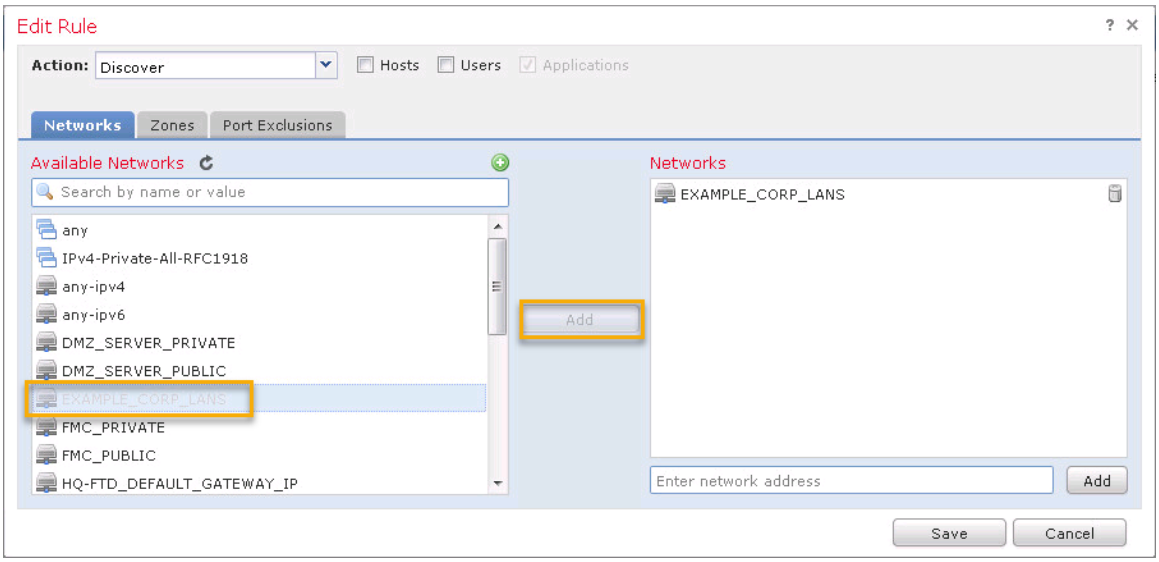


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 174. Configure Networks tab

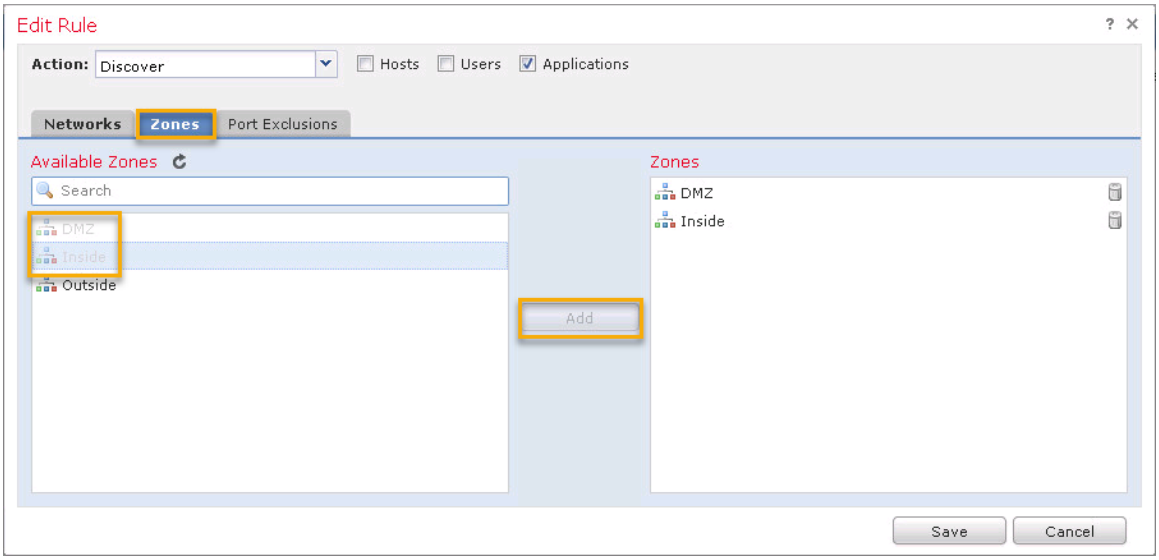


97. Click the **Zones tab**:

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 175. Configure Zones tab



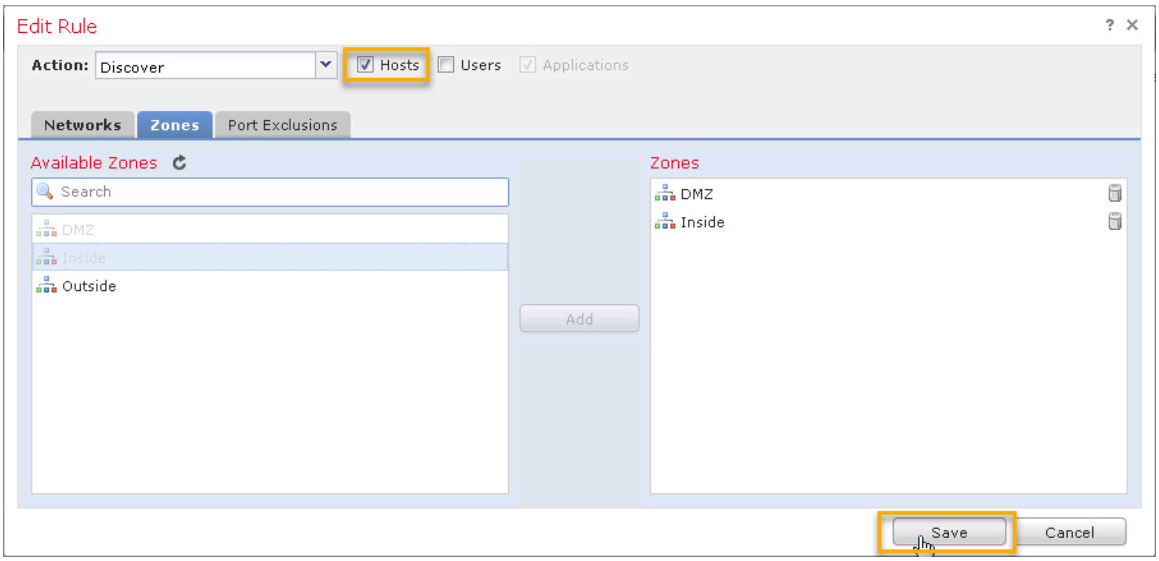
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

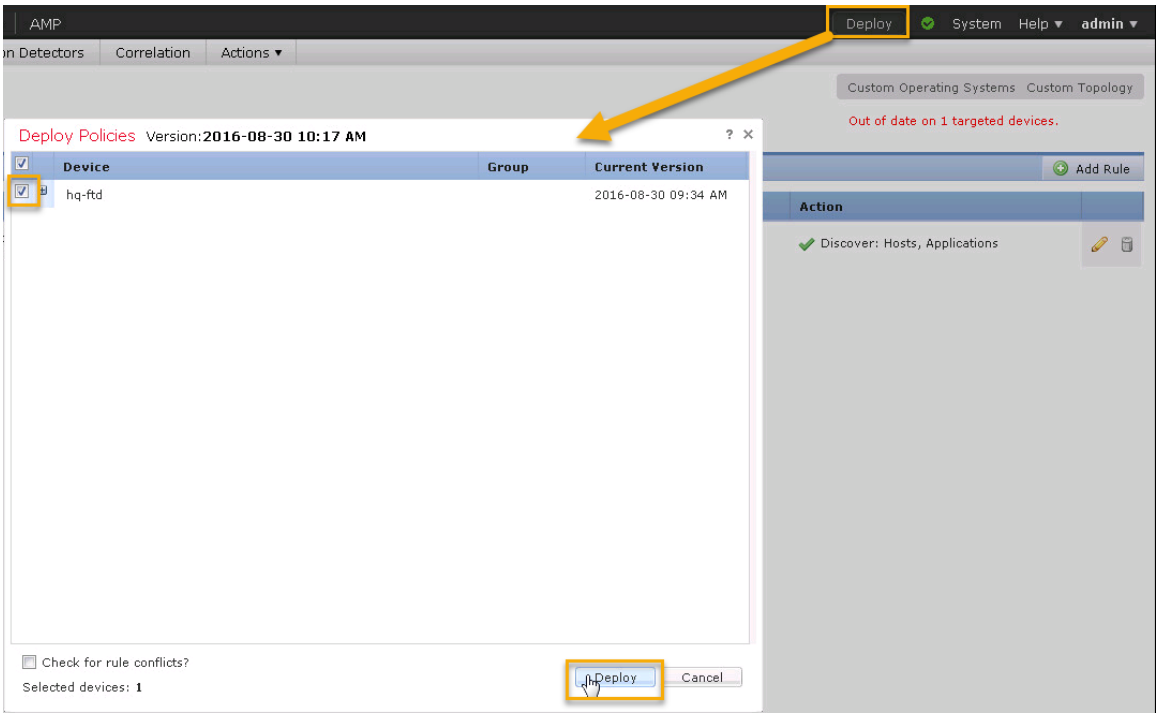
99. Click **Save**.

Figure 176. Check hosts box and save



100. 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 177. Deploy changes



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Scenario 4. Installing the FTD at the Remote1 Site

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. BUT 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).

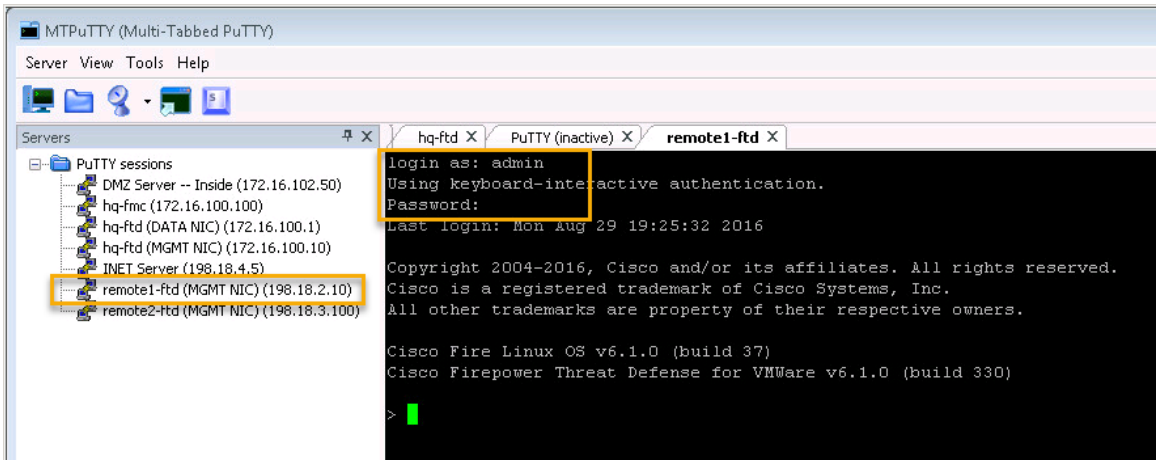
For the purposes of this lab the remote1 location has an FTD with a public static IP address assigned to its management NIC (198.18.2.10). As with the hq-ftd device the initial configuration of the management network has been done for you so that you can ssh to the remote1-ftd to finish the configuration.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

1. On hq-wkst use the connection in the **MTPuTTY** program use the **remote1-ftd (MGMT NIC)** bookmark to ssh to remote1-ftd's management IP address (198.18.2.10). Login as **admin**/**Admin123**.

Figure 178. 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.

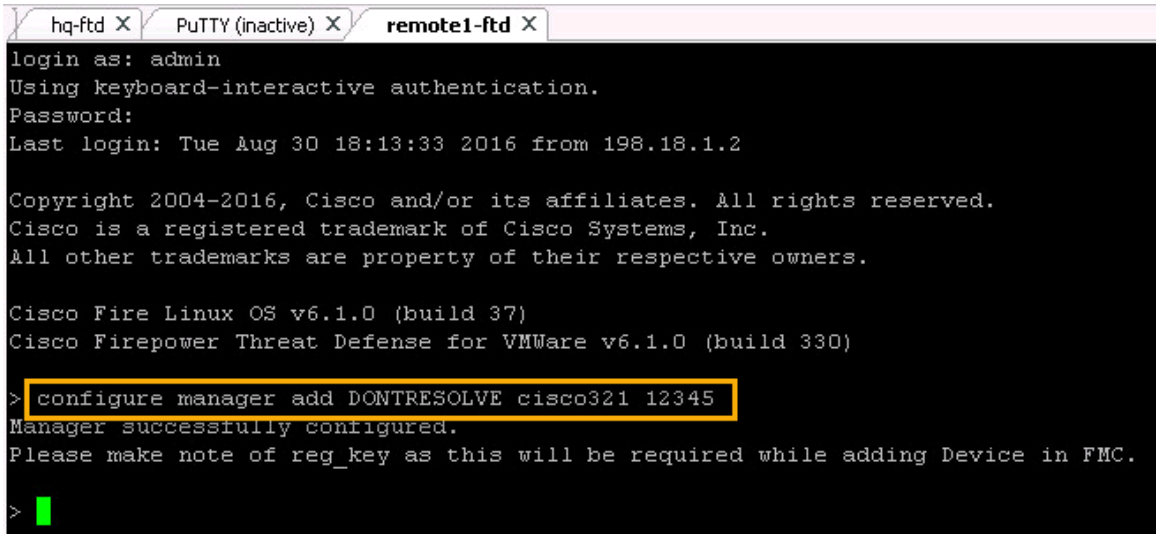
You will use the more plausible method (where the remote/branch FTD only gets DHCP addresses from the ISP) when registering the remote2-ftd device later in the lab.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 179. Configure manager for remote1-ftd



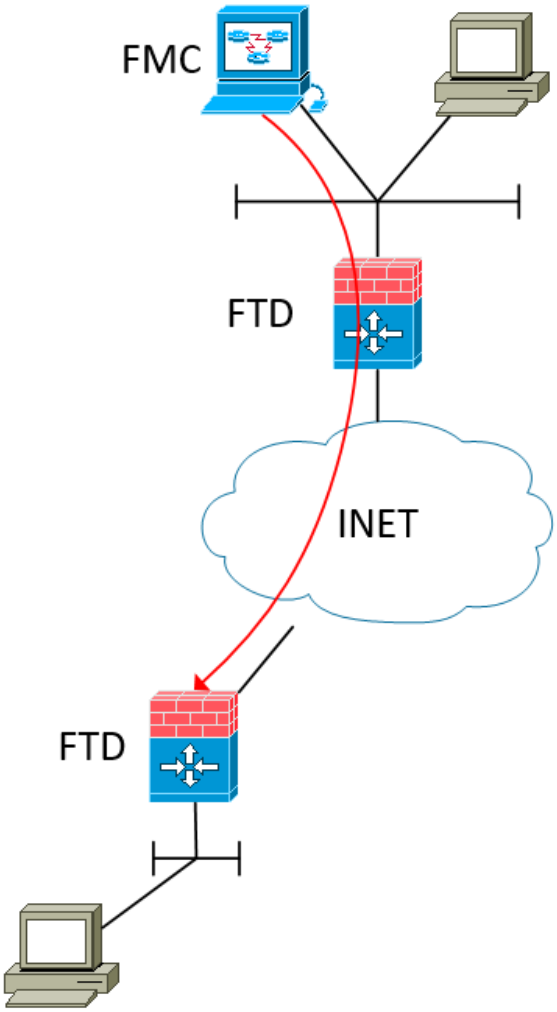
Since the FMC is sitting behind a NAT device (hq-ftd in this case) it doesn't have a public IP to which you can associate this FTD to. Thus the "DONTRESOLVE" option vs. an actual IP address (along with the NAT-ID) will set this FTD up for communications from the FMC.

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.)

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Figure 180. Direction of Registration Initialization

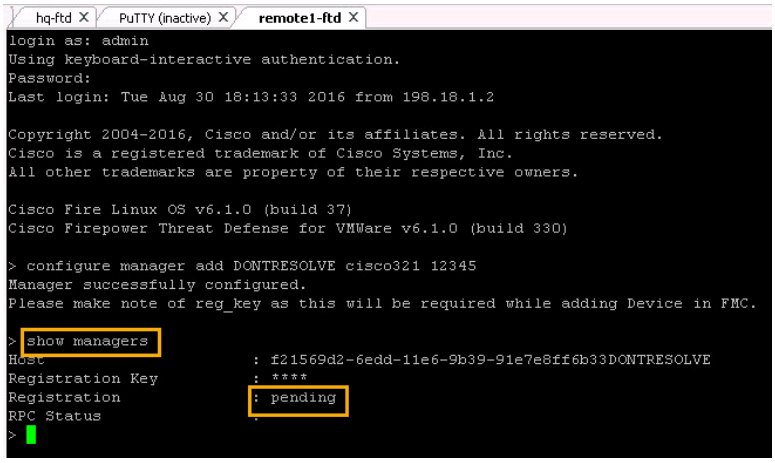


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 181. Show managers



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 182. Add new device in FMC

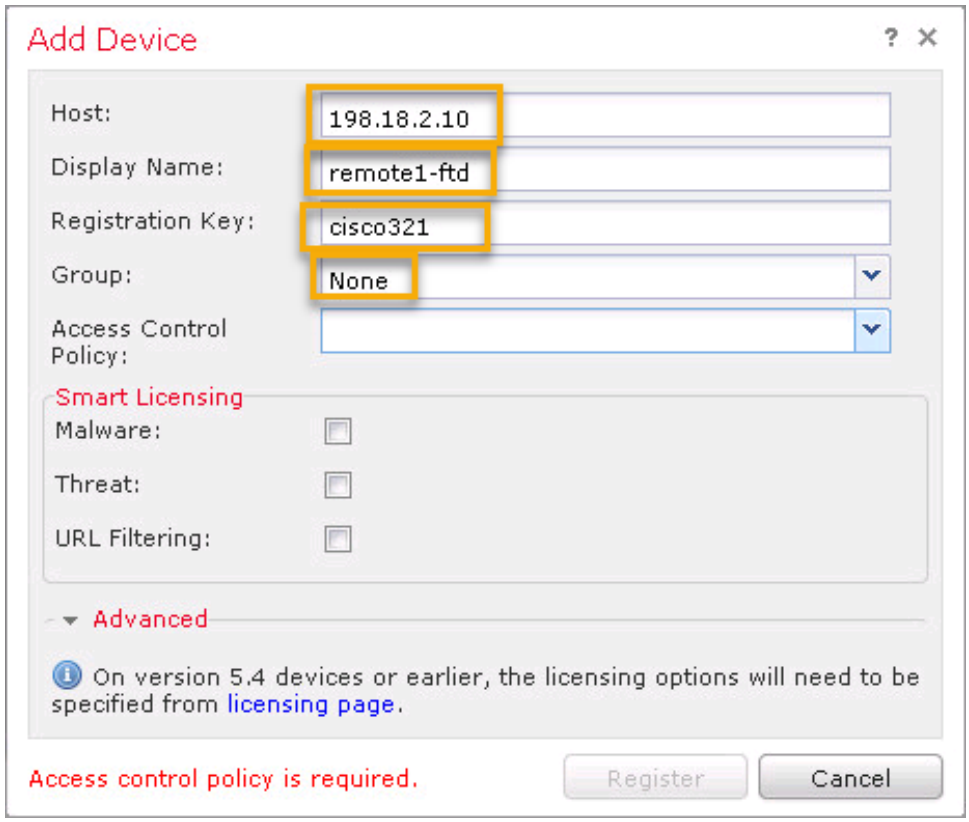


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 183. Part 1 of adding remote1-ftd to FMC



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 184. Create new ACP

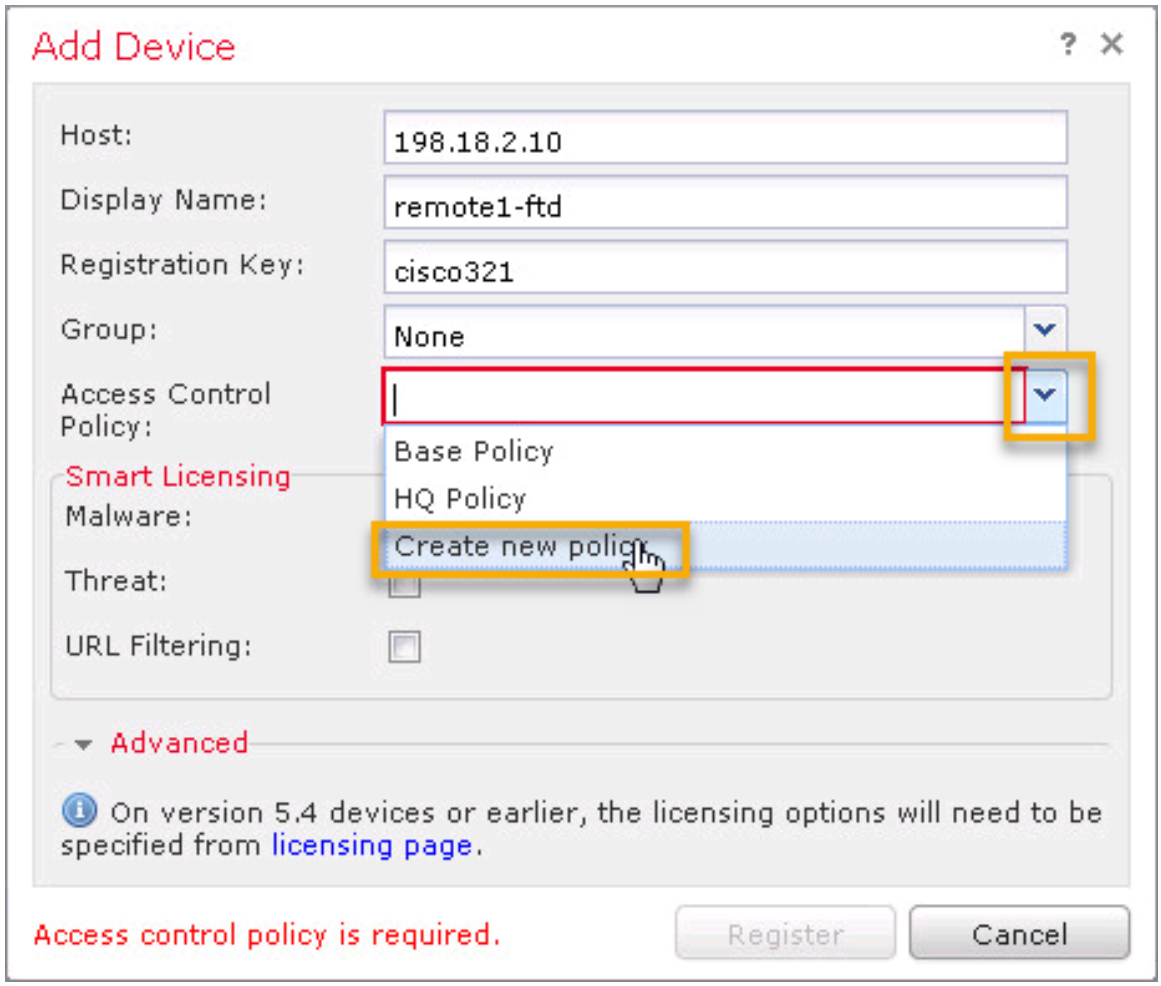
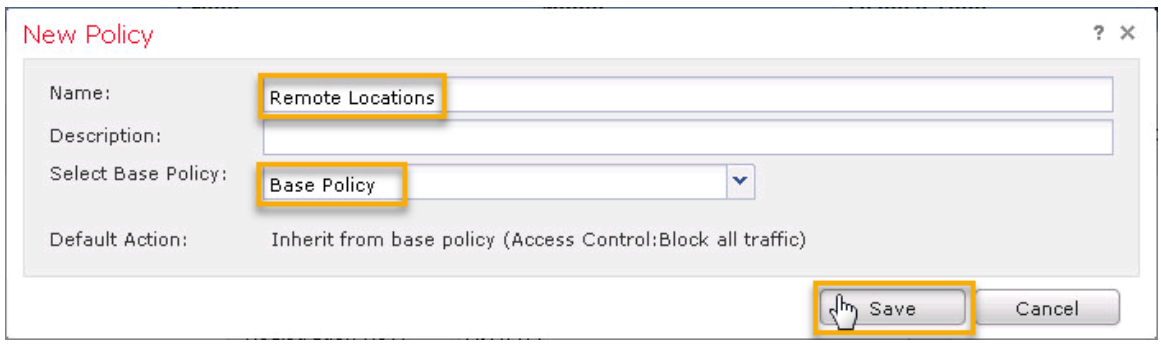


Figure 185. New ACP



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

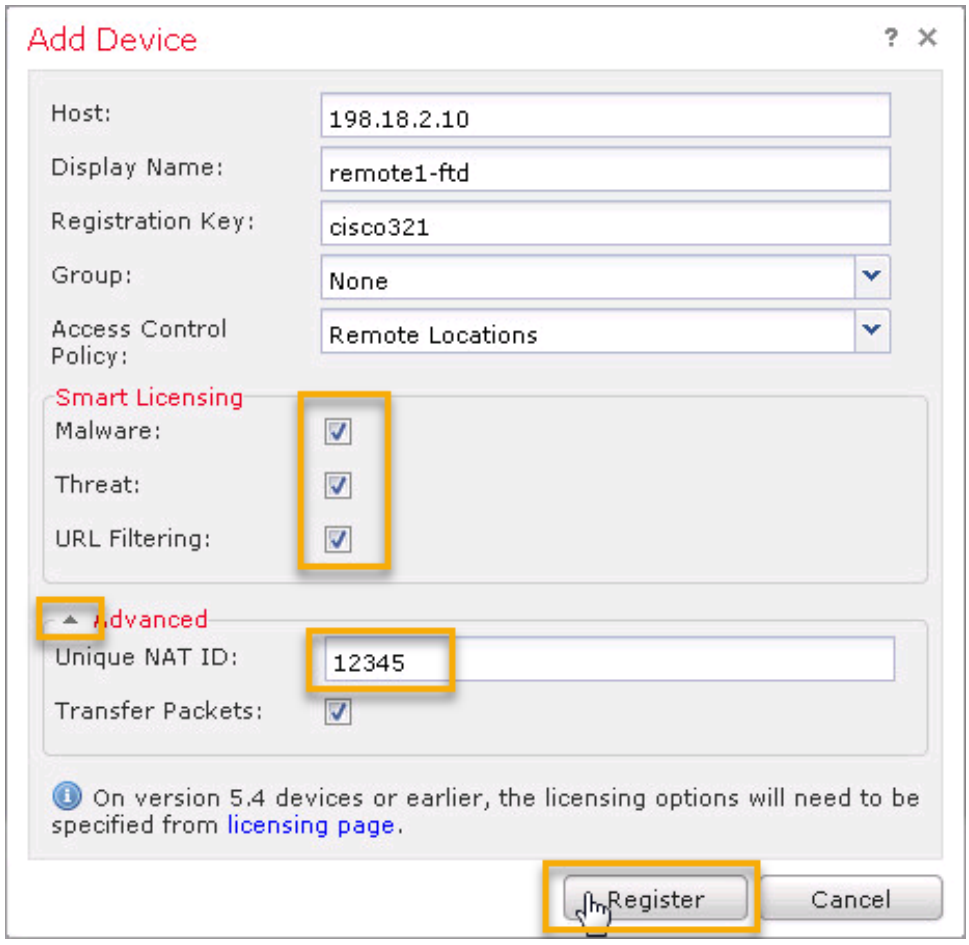
g. In the Smart Licensing section check all the boxes.

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 186. Finish adding remote1-ftd to FMC

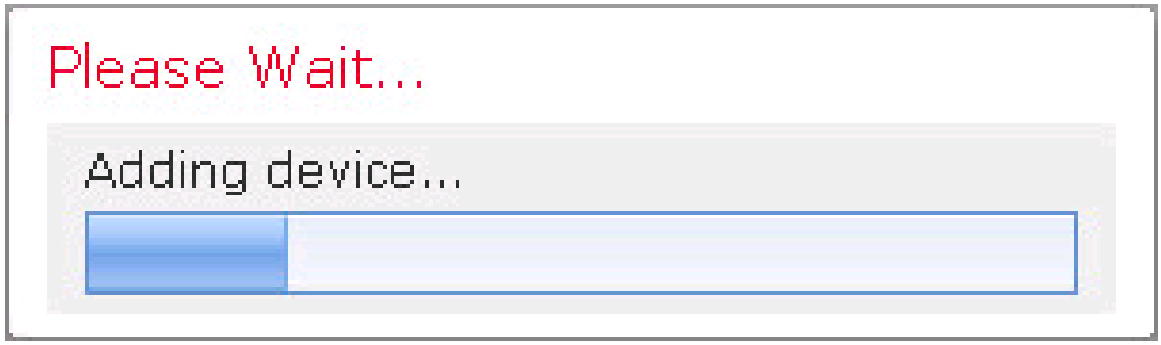


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

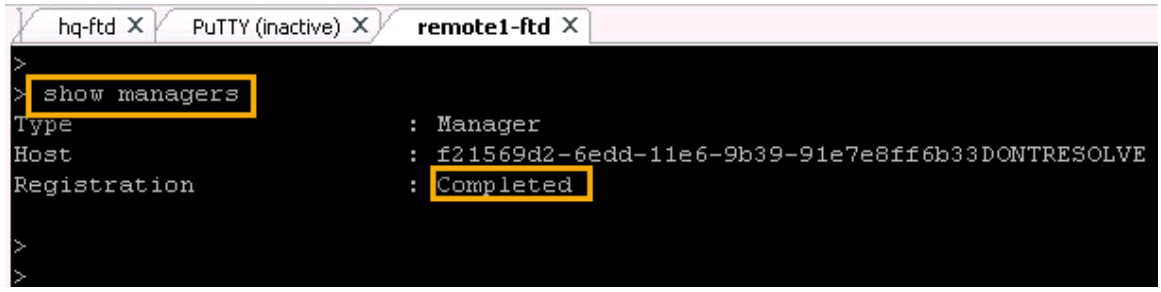
Figure 187. Status of registration



<insert a note about the needs regarding bandwidth here.>

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 188. Show managers, again

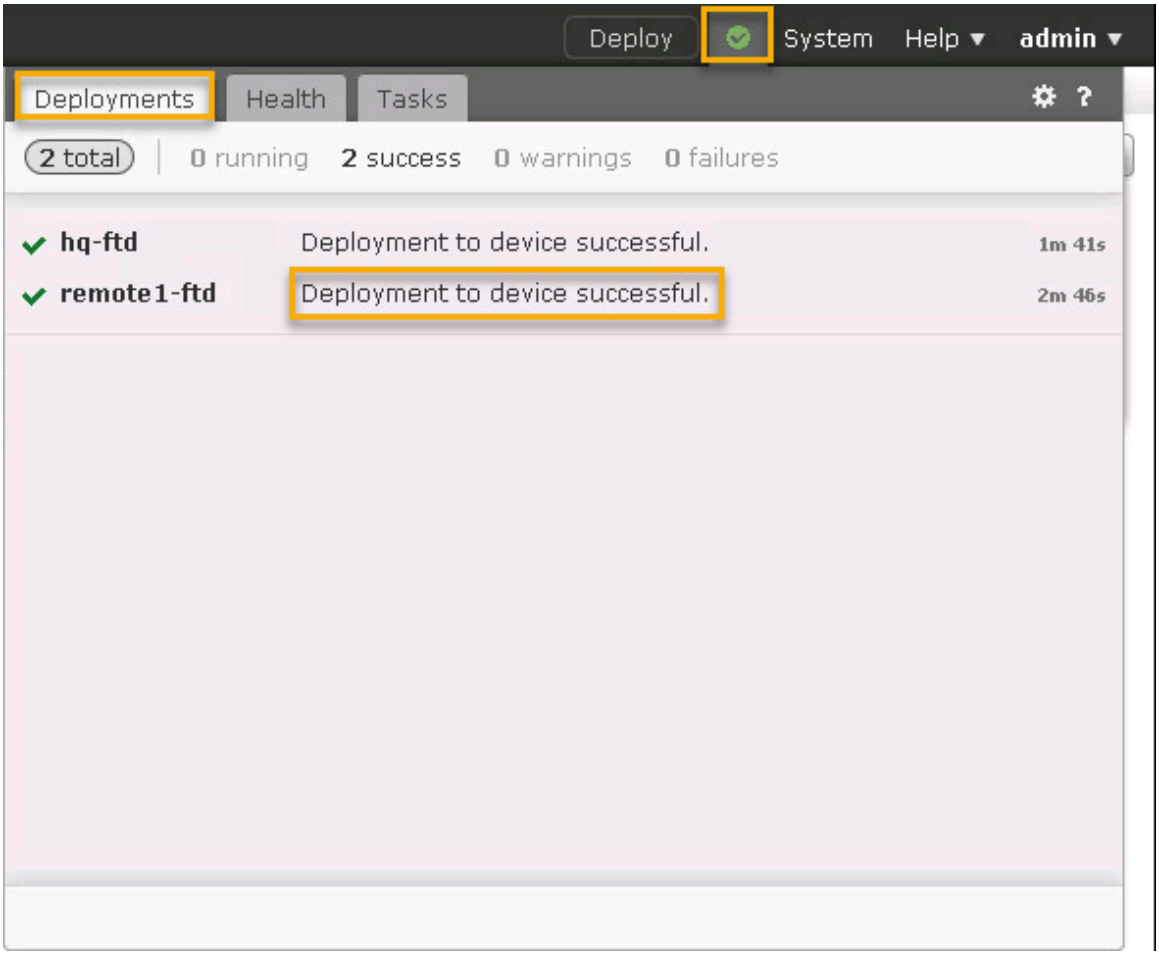


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 189. Registration is complete



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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 190. Edit remote1-ftd device



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

Figure 191. Edit g0/0



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

    a. Mode: **None**

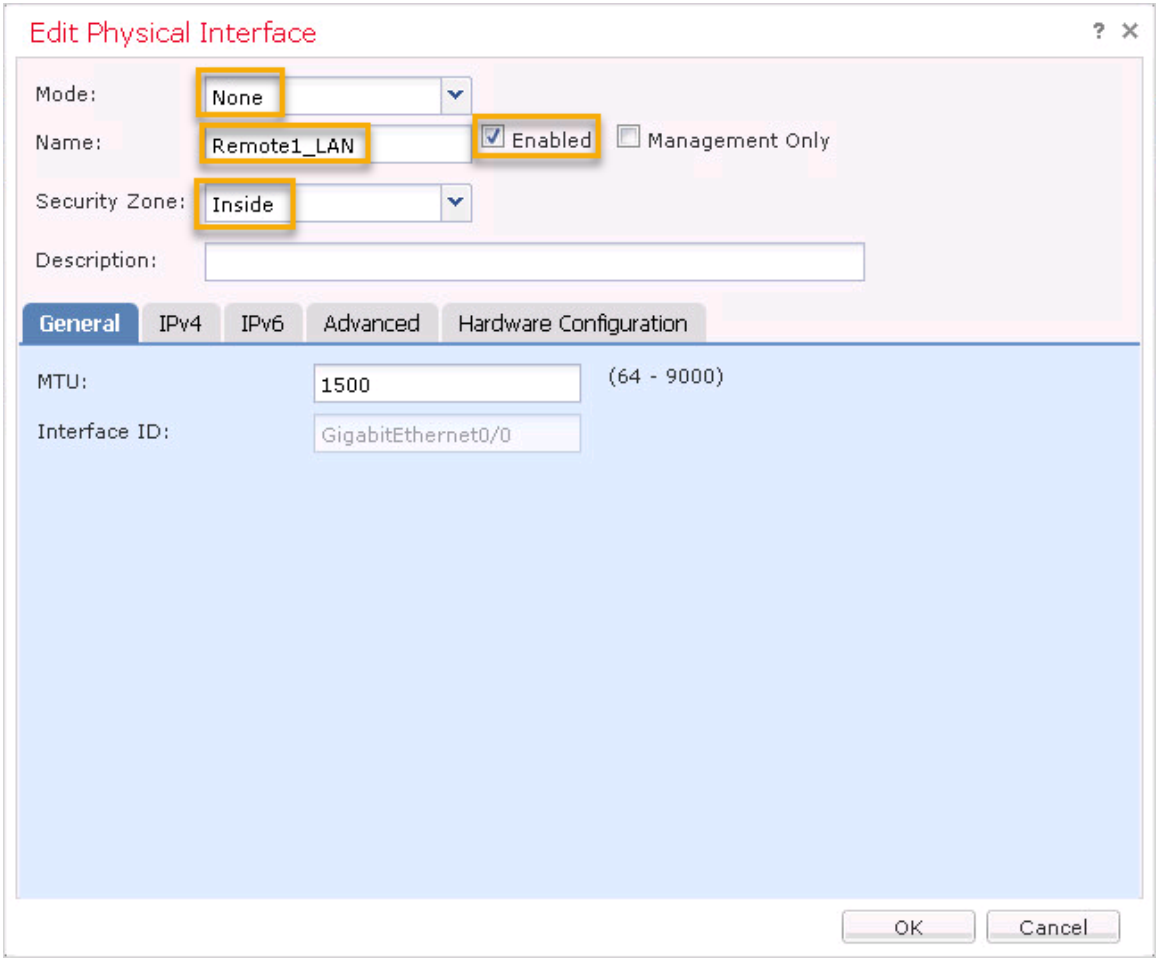
    b. Name: **Remote1_LAN**

    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 192. Part 1 of configuring g0/0

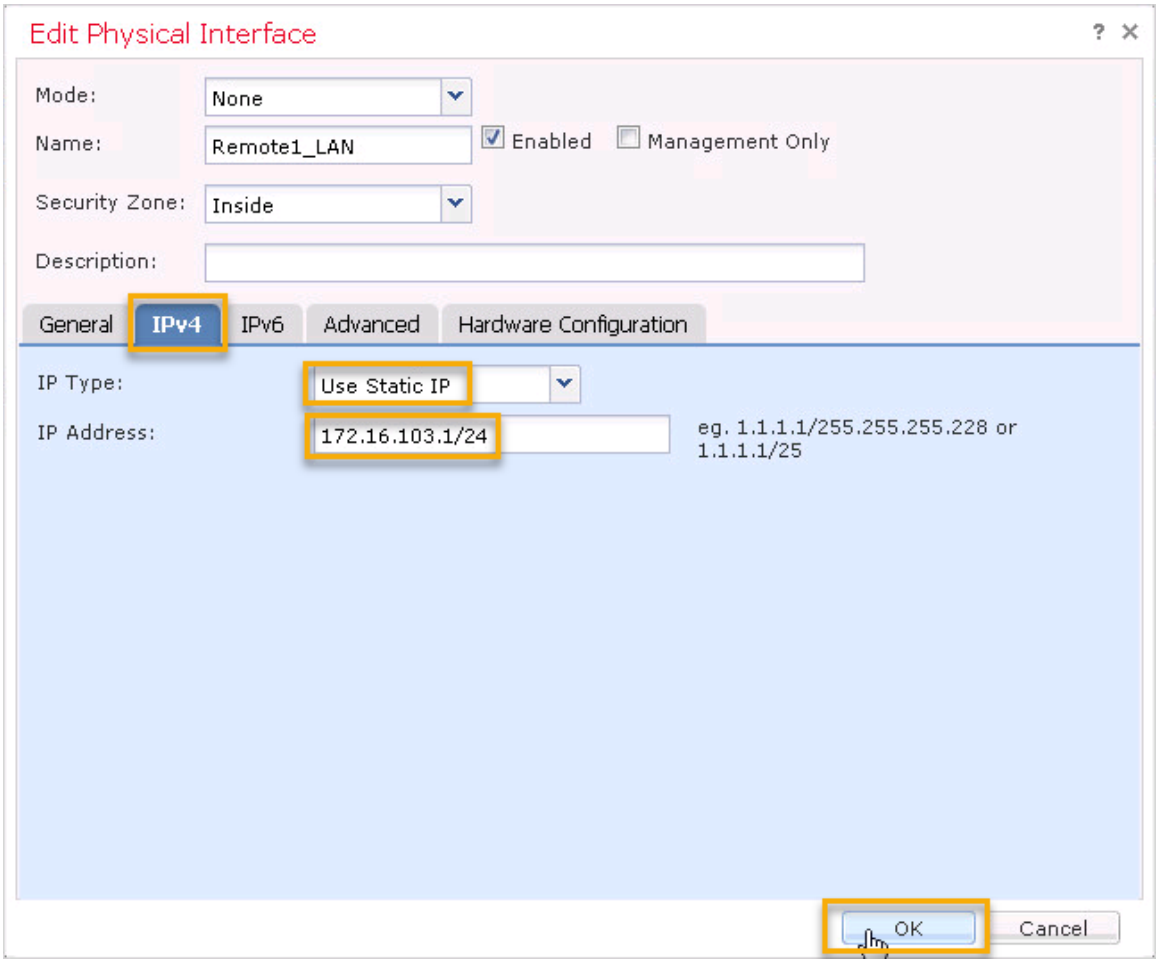


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

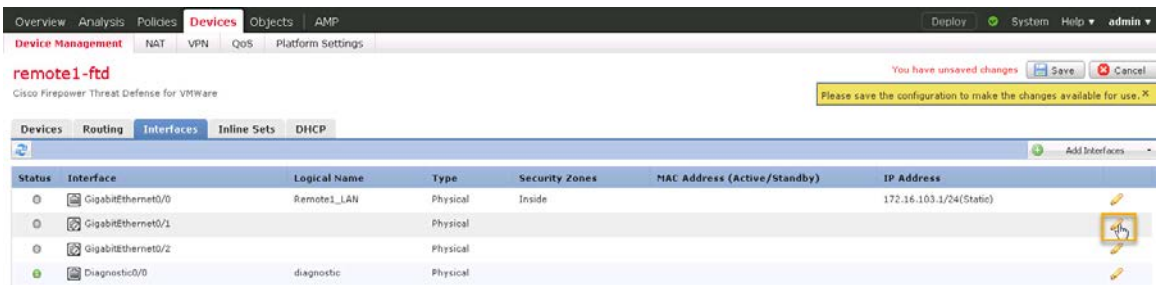
16. Click the **IPv4 tab**.
    a. IP Type: **Use Static IP**
    b. IP Address: **172.16.103.1/24**
17. Click **OK**.

Figure 193. Add IP and click OK



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

Figure 194. Edit g0/1

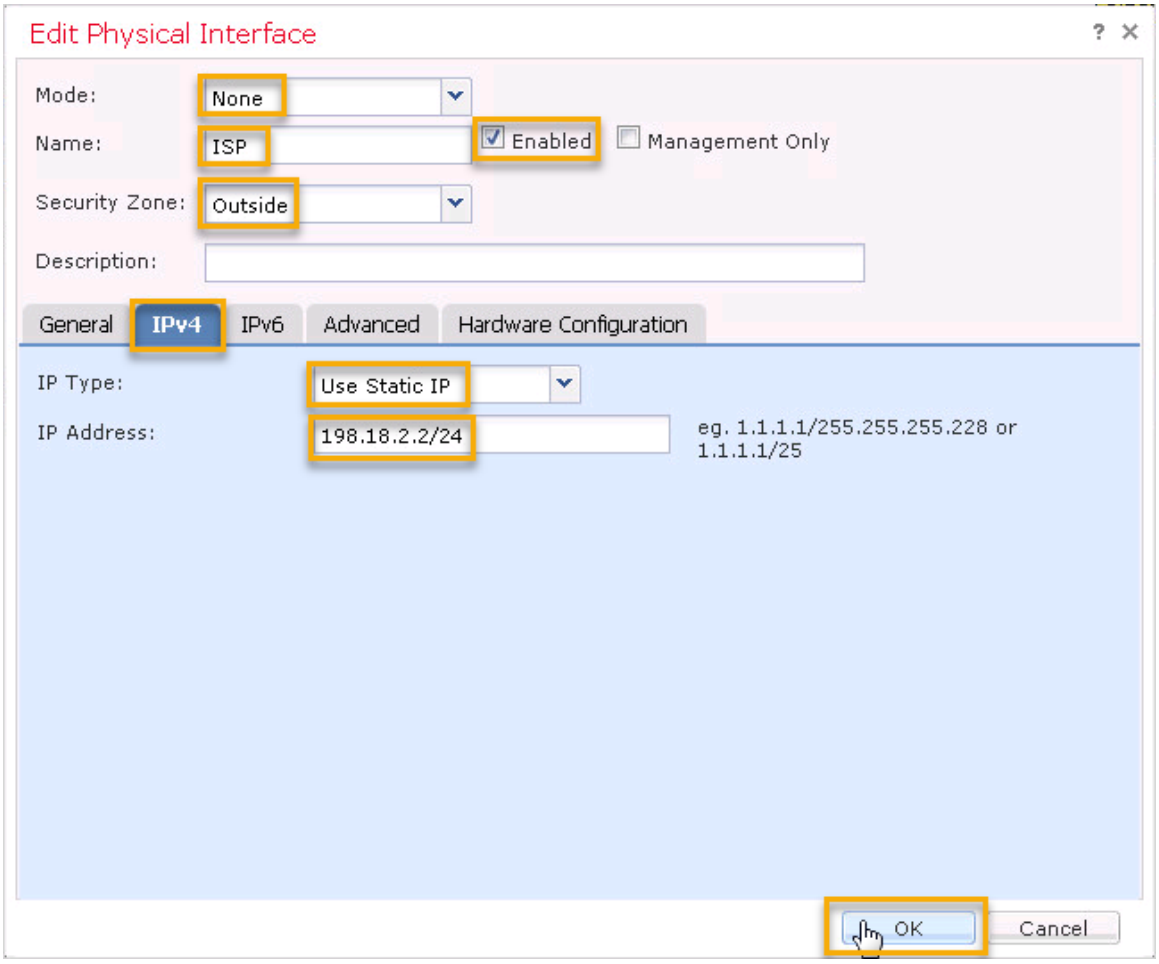


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 195. Configure g0/1

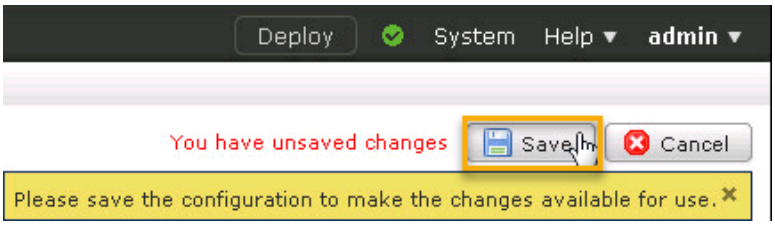


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 196. Save to FMC before continuing



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 197. Start to add static route

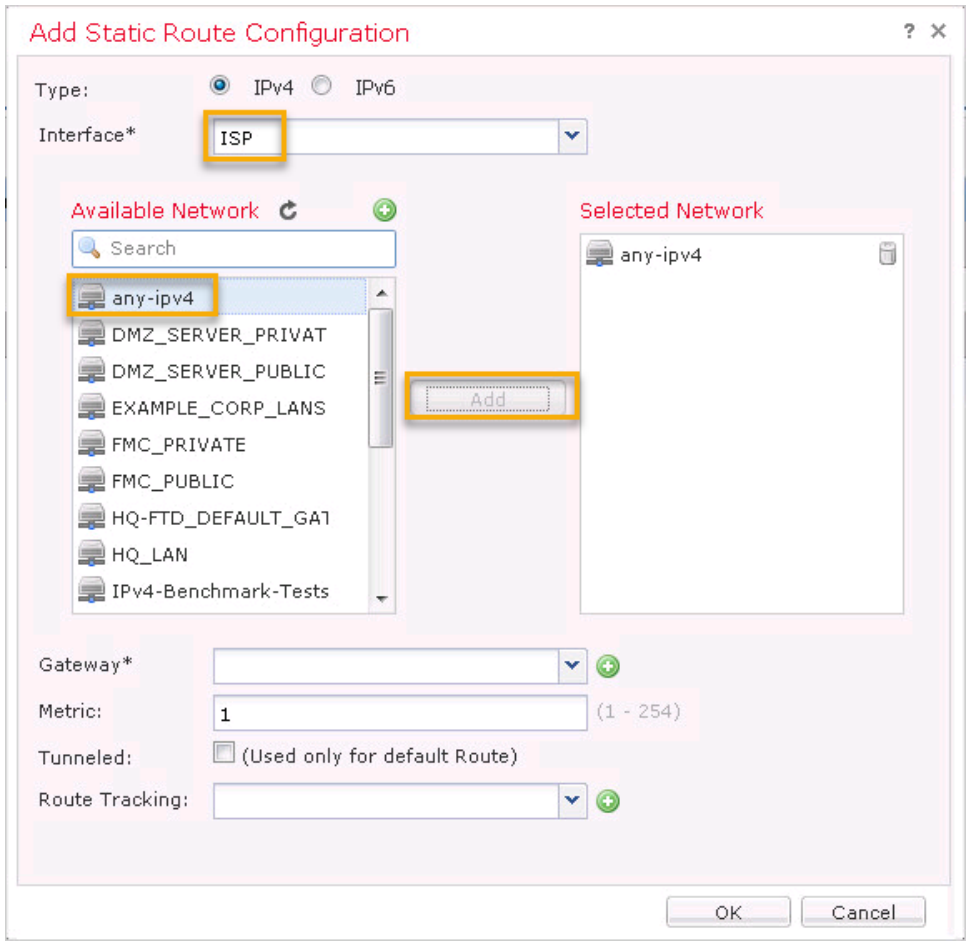


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 198. Part 1 of adding static route



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

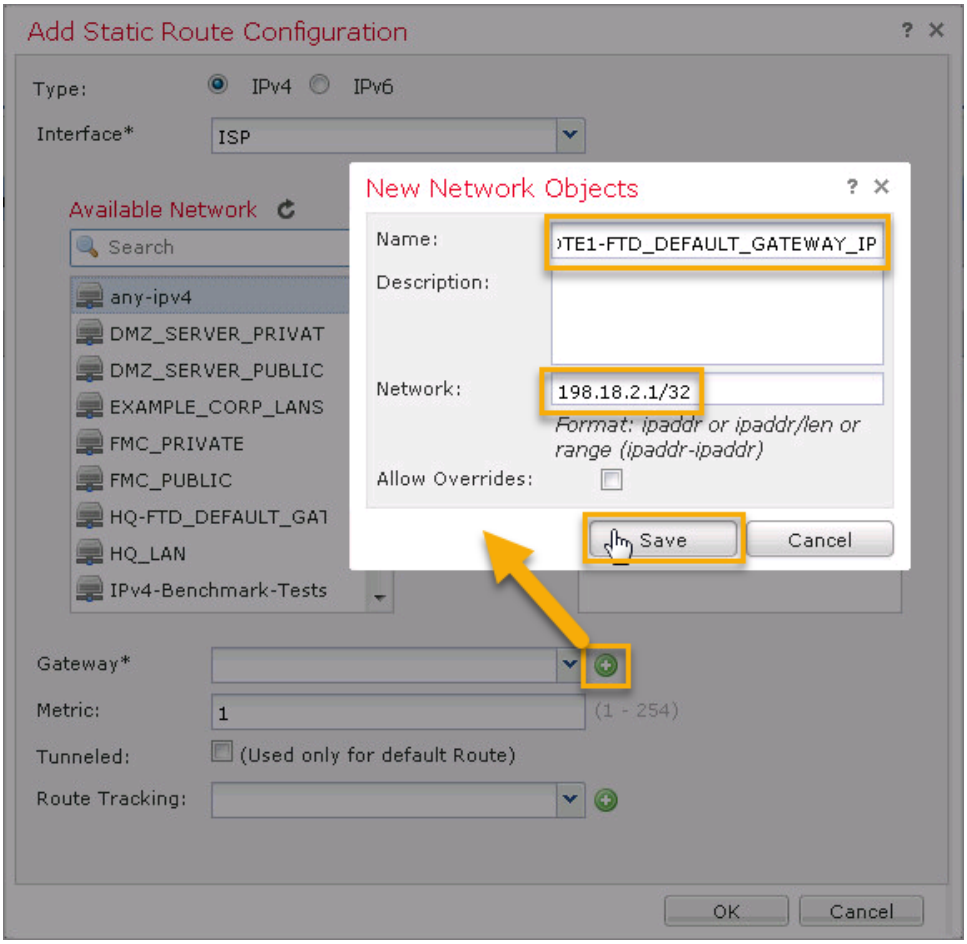
28. Next to the Gateway dropdown menu click the **green plus icon** and create a Network Object for the ISP's default gateway IP.

    a. Name: **REMOTE1-FTD_DEFAULT_GATEWAY_IP**

    b. Network: **198.18.2.1/32**

    c. Click **Save**.

Figure 199. Create Network Object



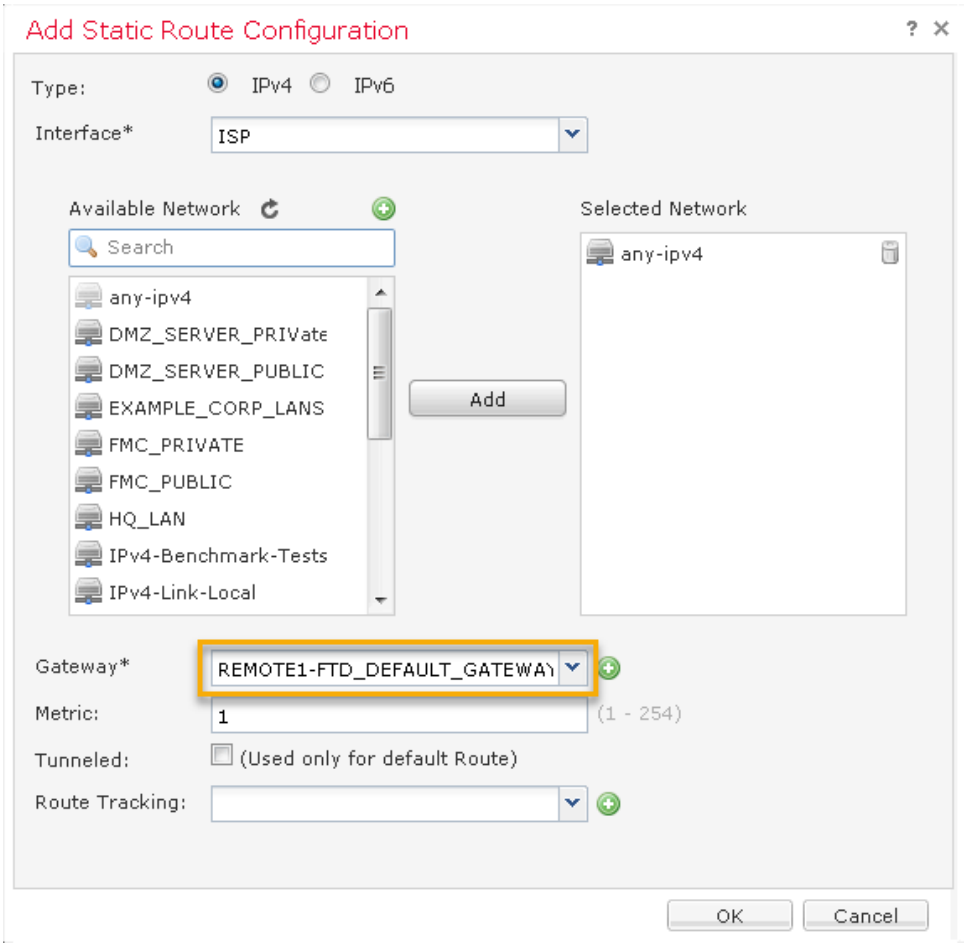
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 200. Finish creating static route



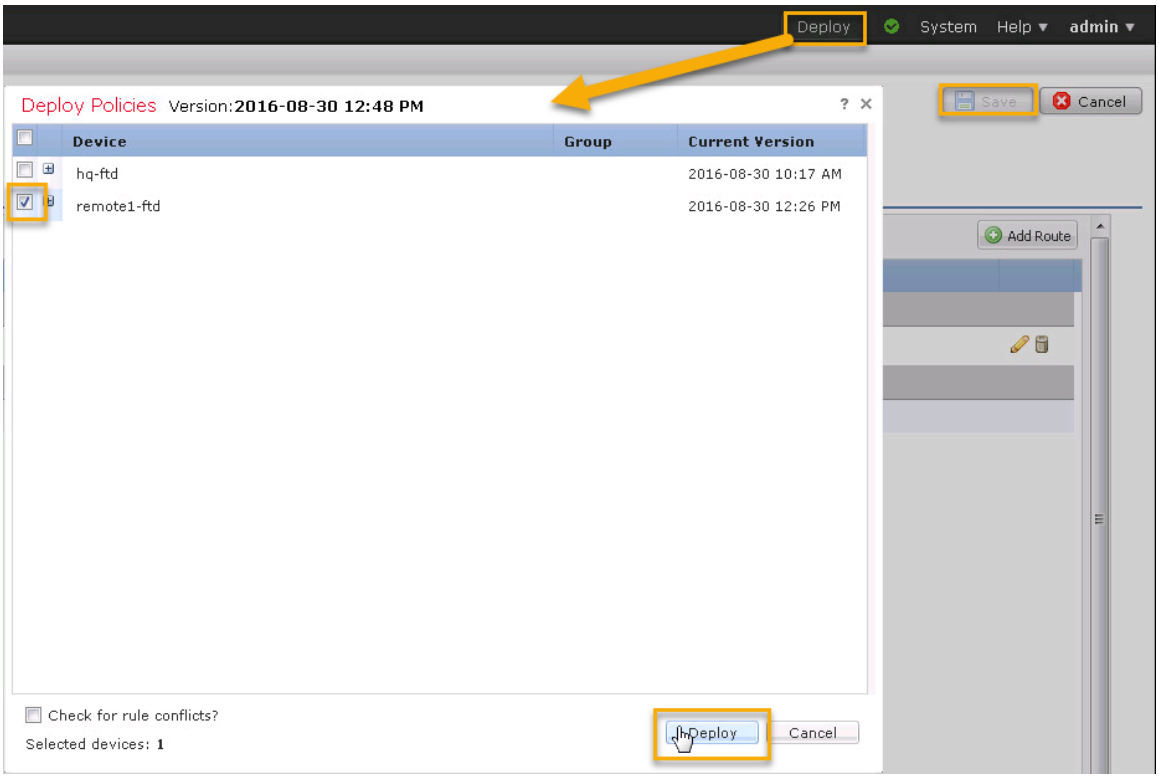
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

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

Figure 201. Save and Deploy to remote1-ftd



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 202. Edit Remote Locations ACP

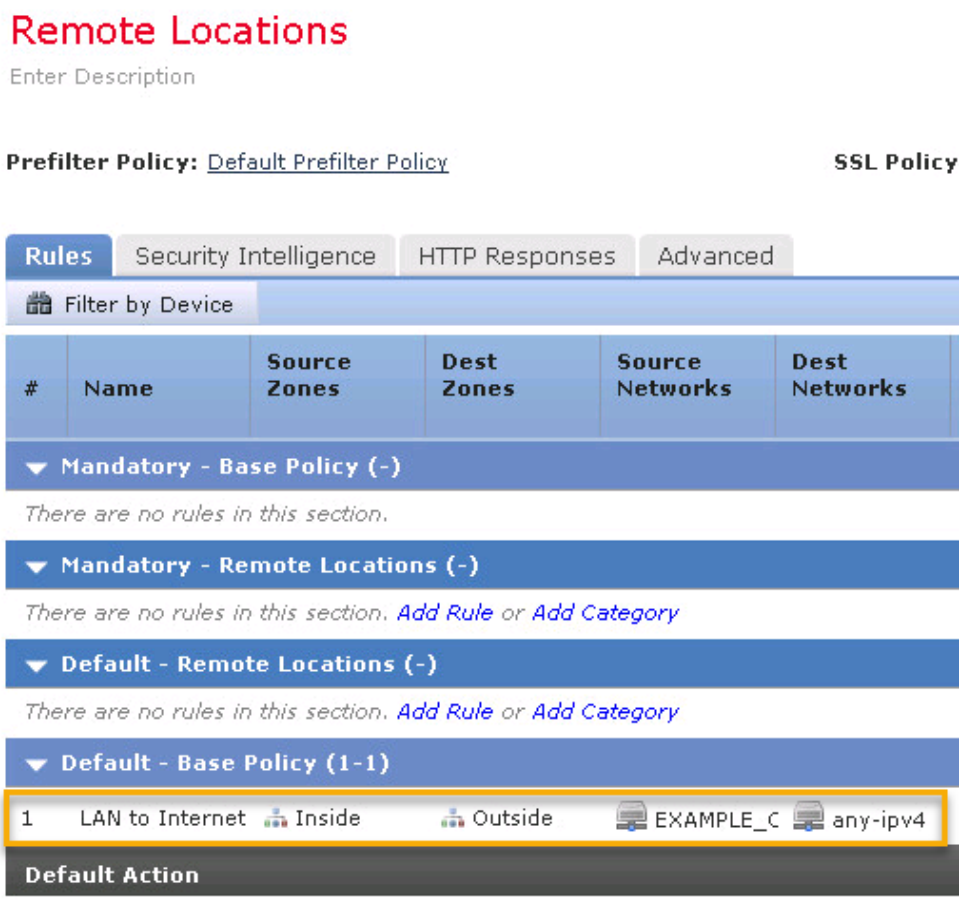


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 203. Expand all sections



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 204. Edit NAT policy

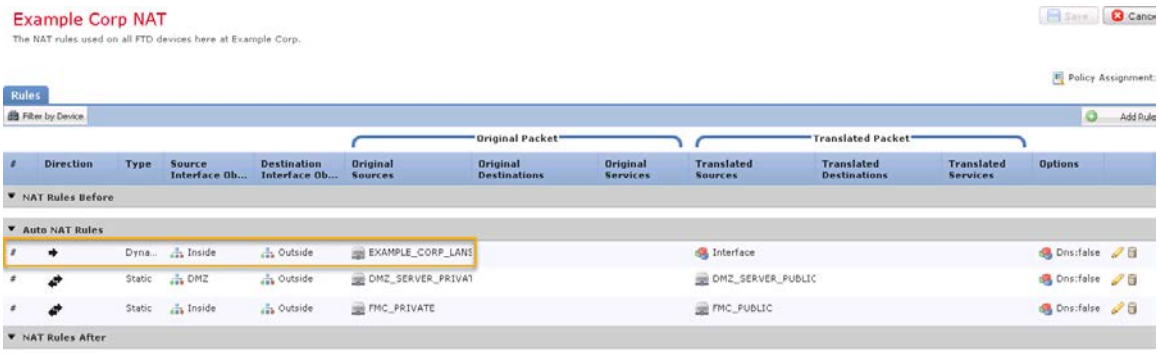


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

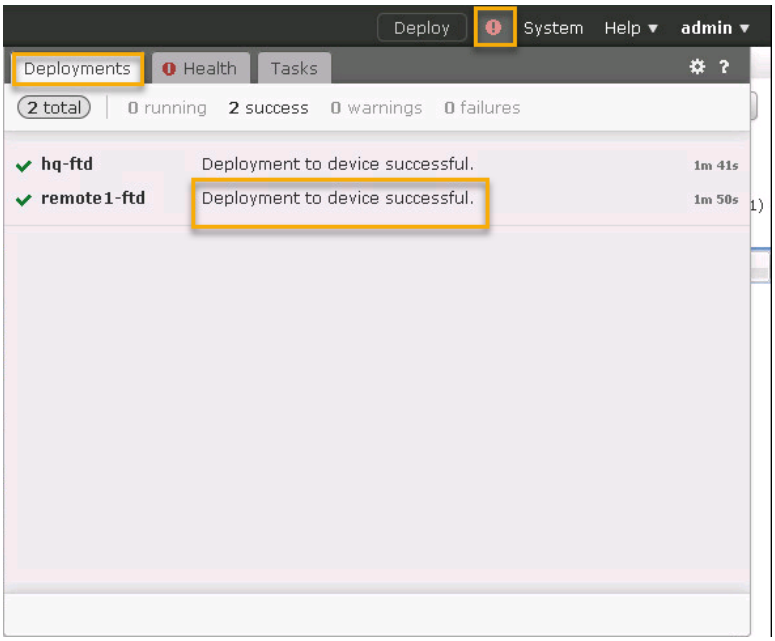
Figure 205. Review the NAT rules



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 206. Ensure deployment is complete



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

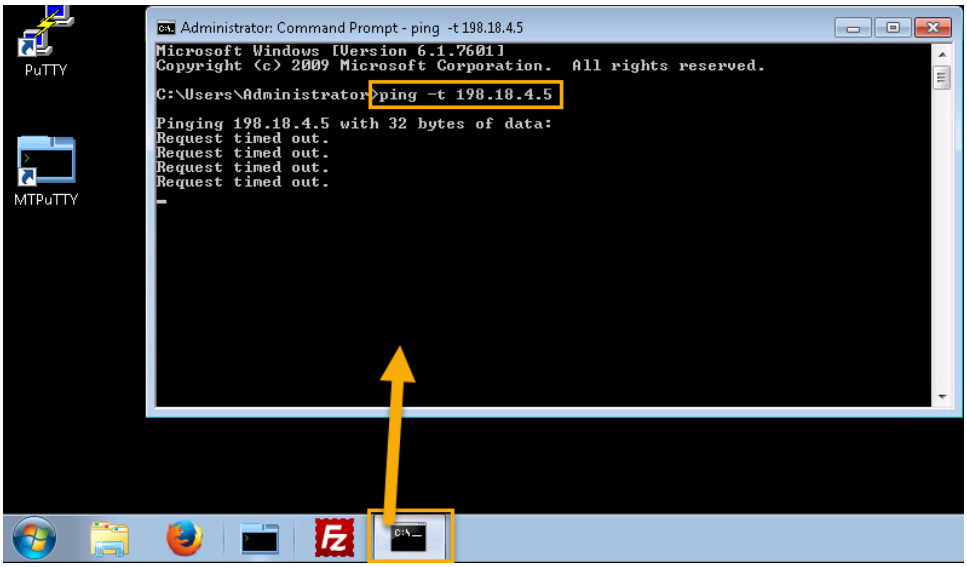
https://t.me/learningnets

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

39. **RDP** to **remote1-wkst** using the Desktop shortcut on the Jumpbox.

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 207. Failed pings



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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:

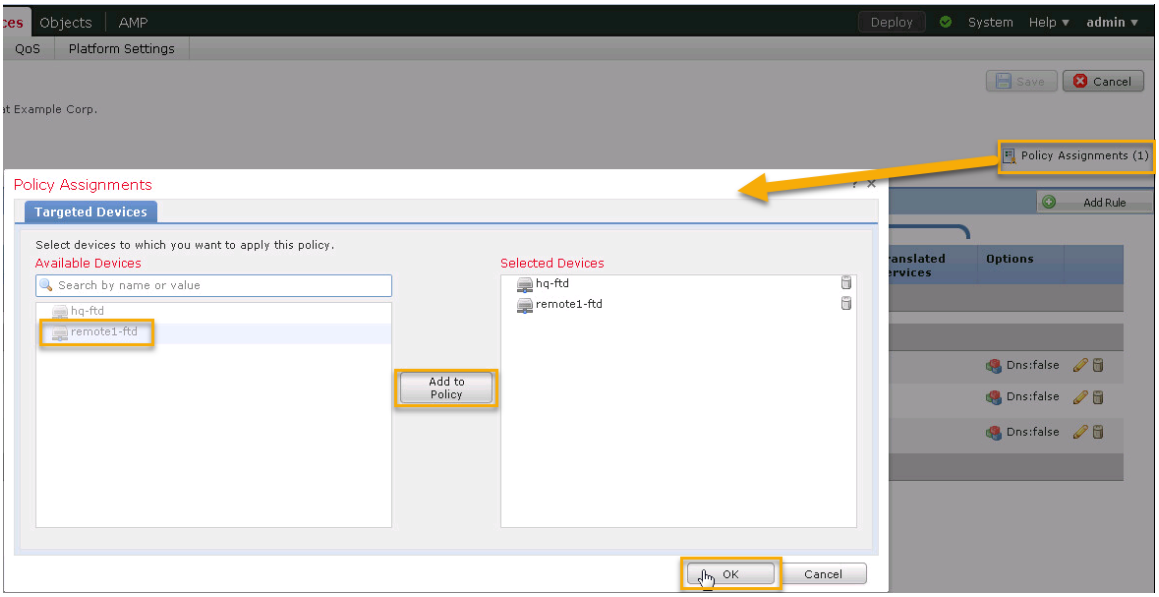
41. On **hq-wkst** return to the FMC administration website. Go to **Devices > NAT**. Notice that the Example Corp NAT rule's Status is Targeting 1 device.
42. Click the **pencil icon** for this rule.

Figure 208. Review NAT Policy



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 209. Add remote1-ftd to NAT policy



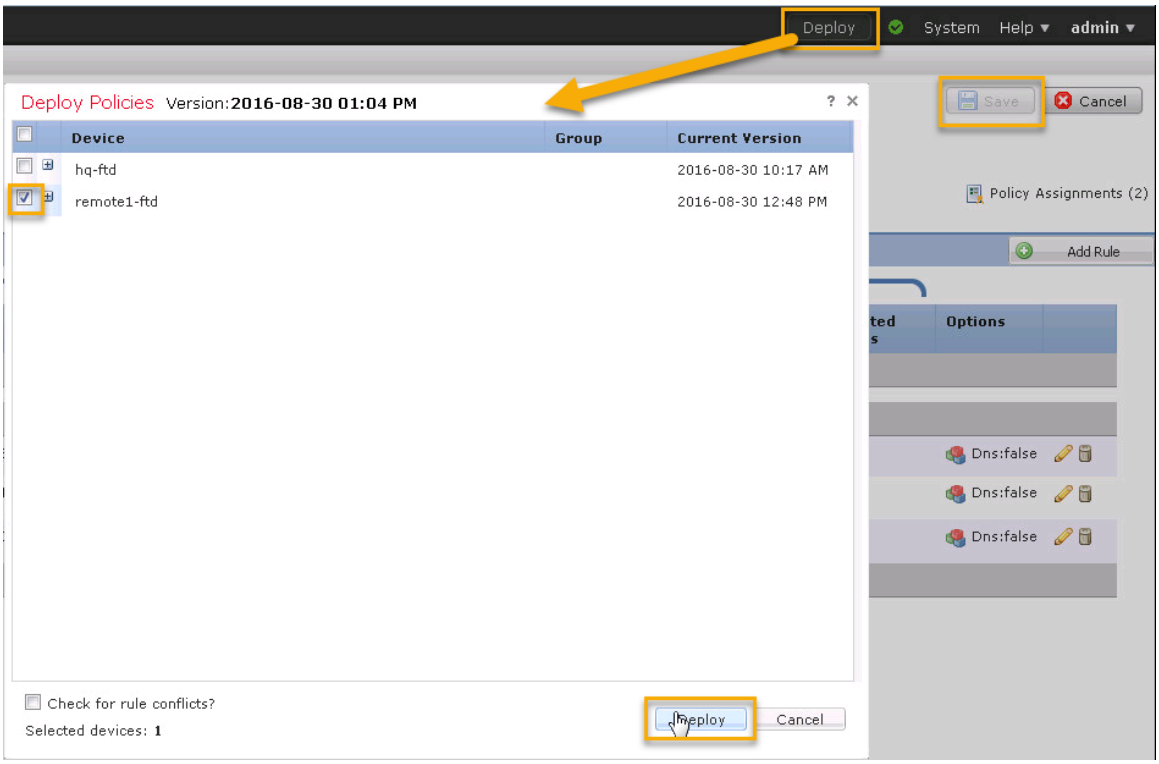
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

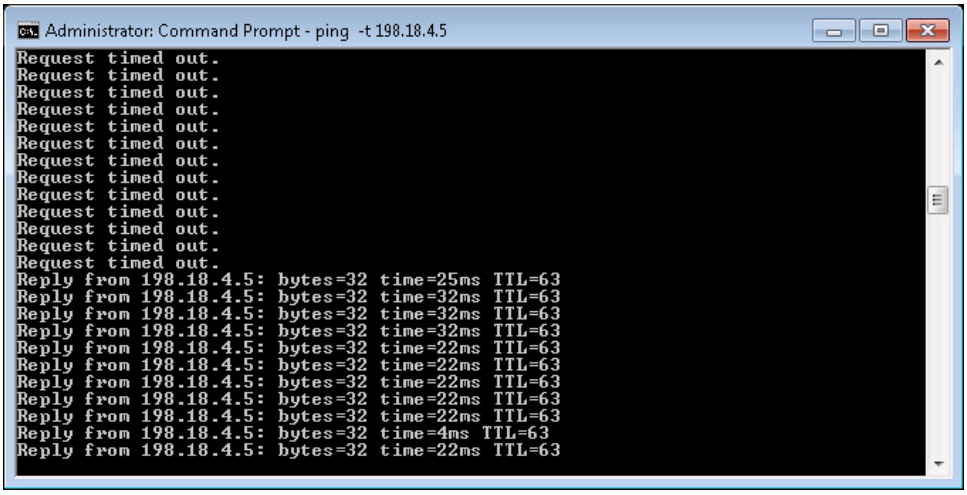
47. Select the **remote1-ftd** device and click **Deploy**.

Figure 210. Save and Deploy to remote1-ftd



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

Figure 211. Pinging on remote1-wkst start working



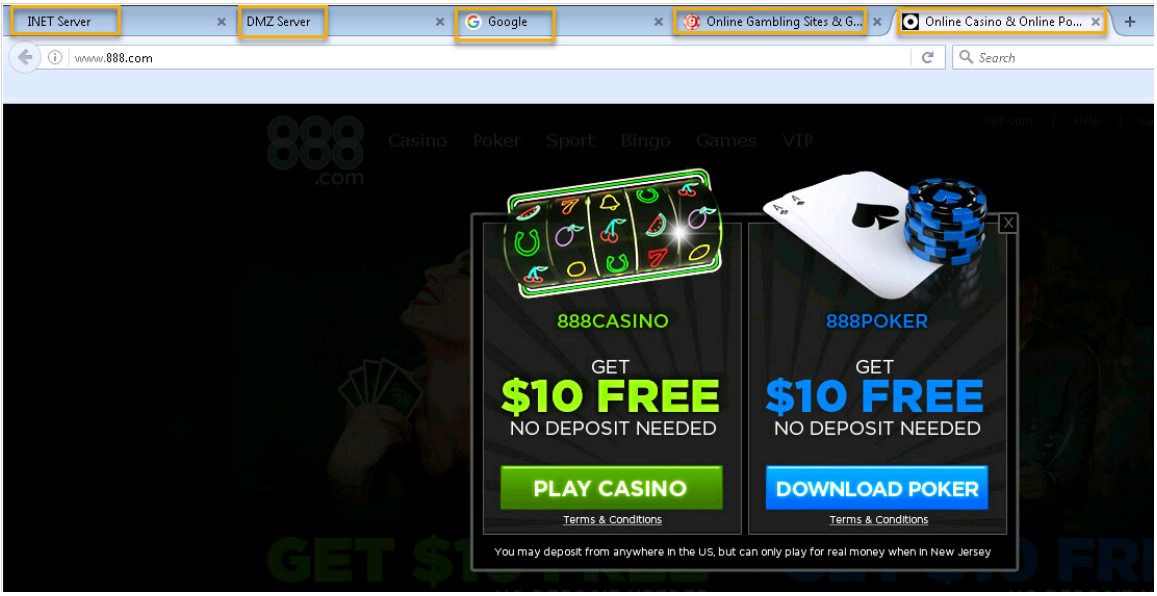
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 212. Firefox tabs refreshed and working



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Scenario 5. Installing the FTD at the Remote2 Site

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.

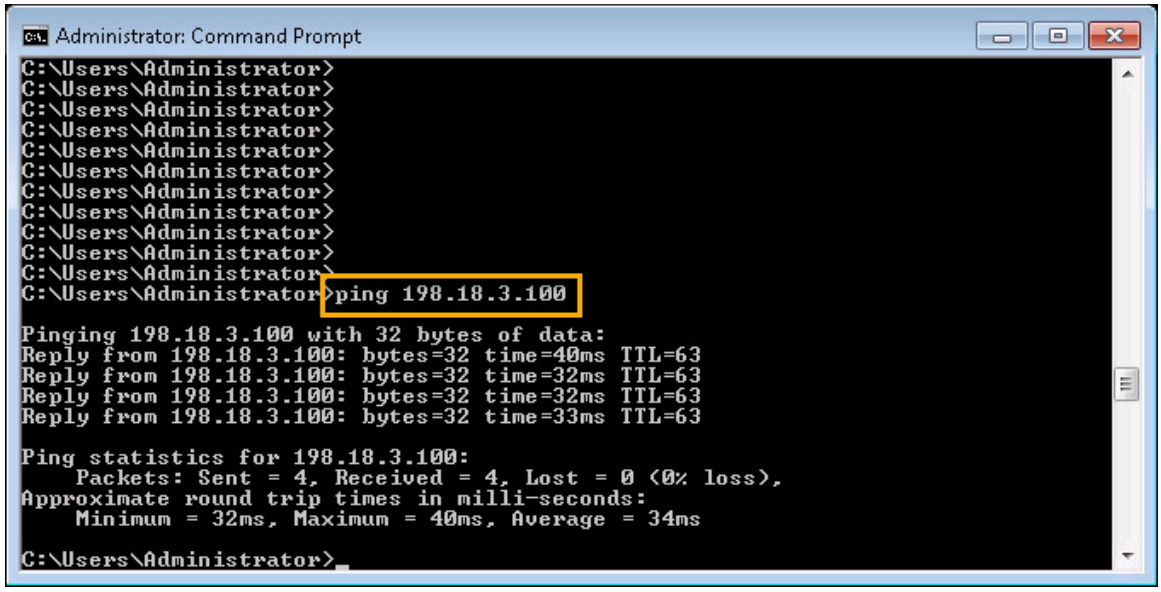
Registering remote2-ftd with hq-fmc

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).

51. 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 213. Finding remote2-ftd’s management IP



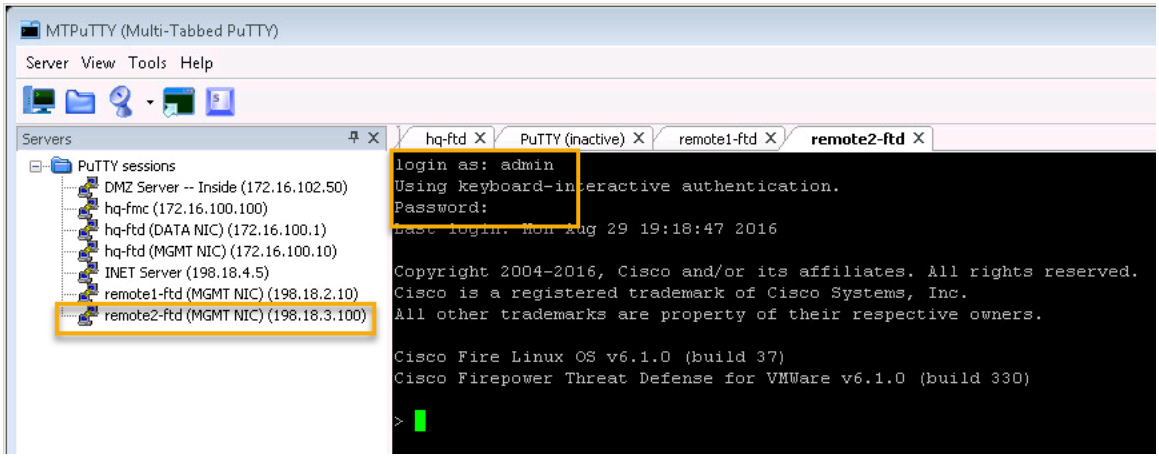
52. On **hq-wkst** the link in the **MTPuTTY** program to ssh to **remote2-ftd** assumes 198.18.3.100. If you have found that remote2-ftd is on another IP then open up PuTTY and access remote2-ftd via the IP you found.

53. SSH to remote2-ftd and log in as **admin**/**Admin123**.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

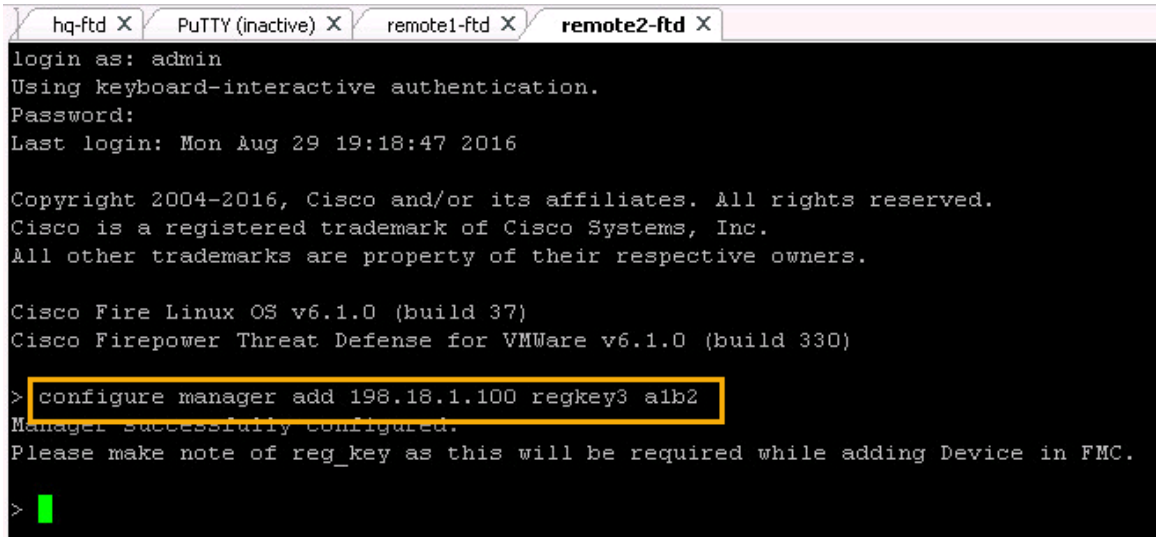
https://t.me/learningnets

Figure 214. SSH to remote2-ftd Mgmt NIC



54. 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.

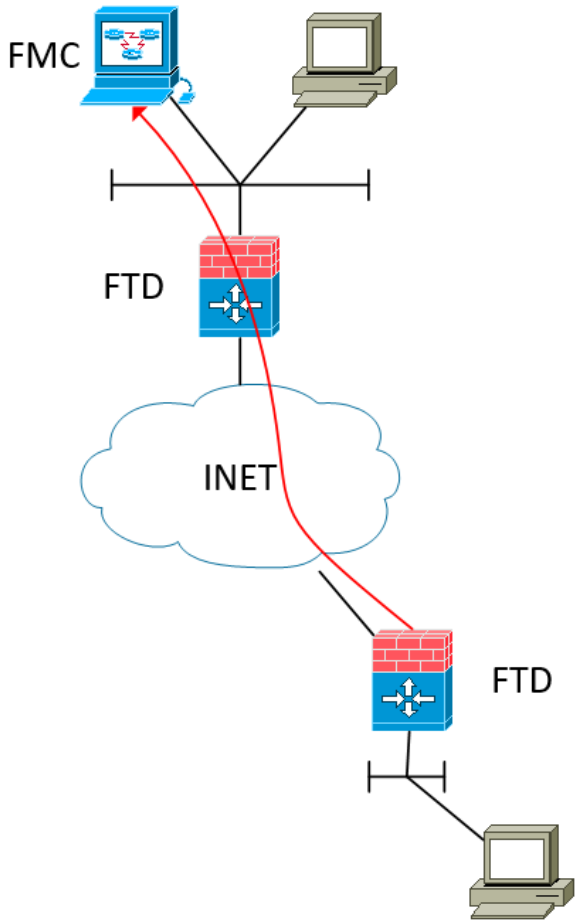
Figure 215. Configure manager for remote2-ftd



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Figure 216. 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.

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

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

Figure 217. Edit HQ Policy ACP



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

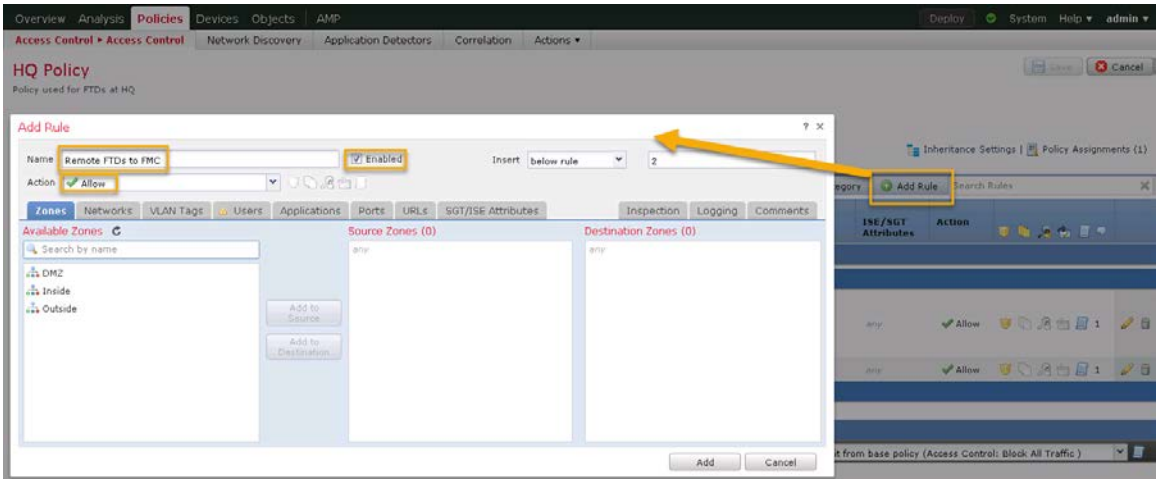
57. Click **Add Rule** and use the following to fill out the needed information.

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

    b. Enabled: **Checked**

    c. Action: **Allow**

Figure 218. Create a new rule, part 1

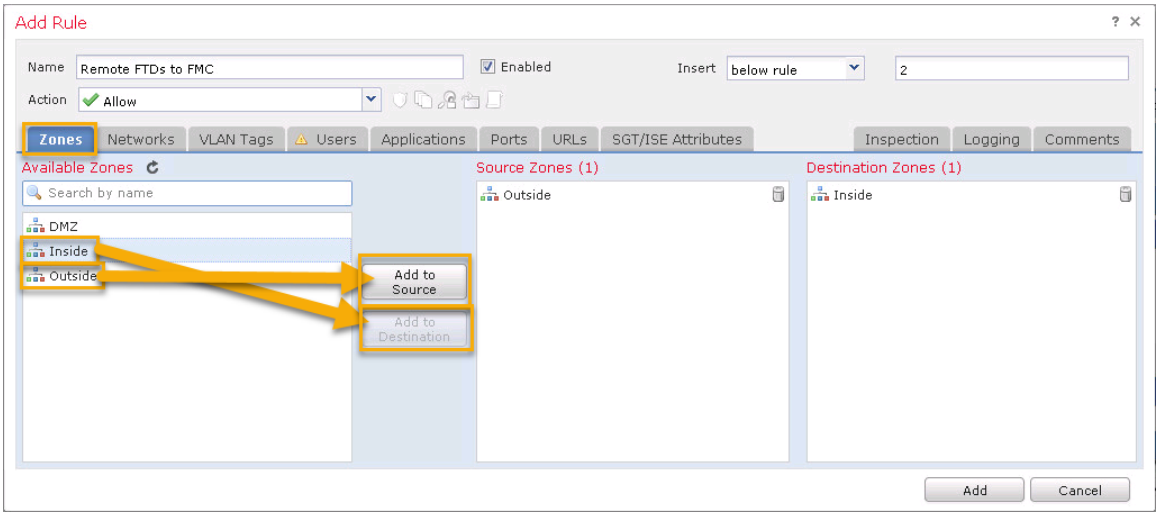


58. On the **Zones tab**:

    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 219. Configure Zones tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

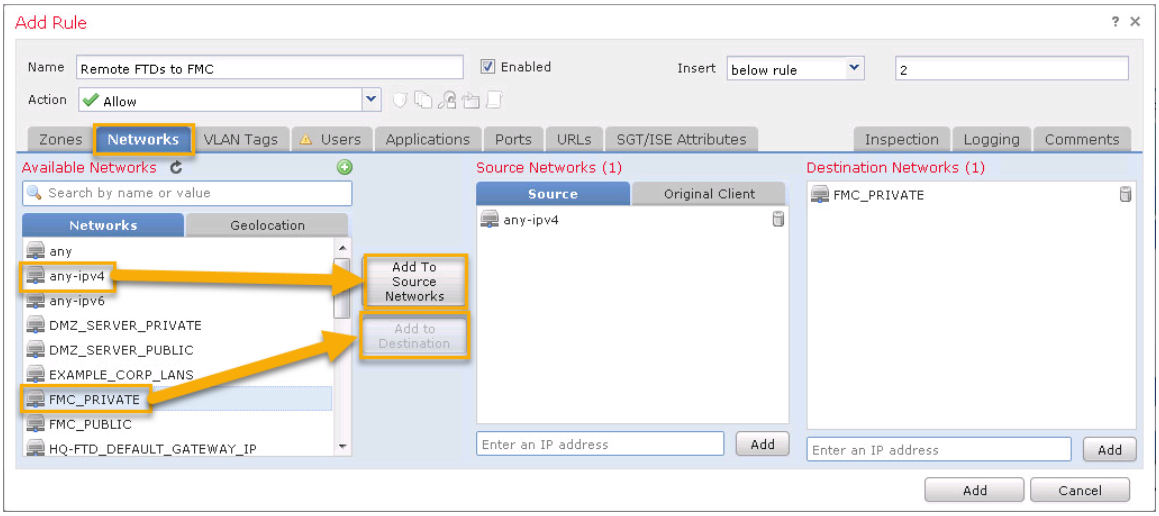
https://t.me/learningnets

59. 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 220. Configure Networks tab

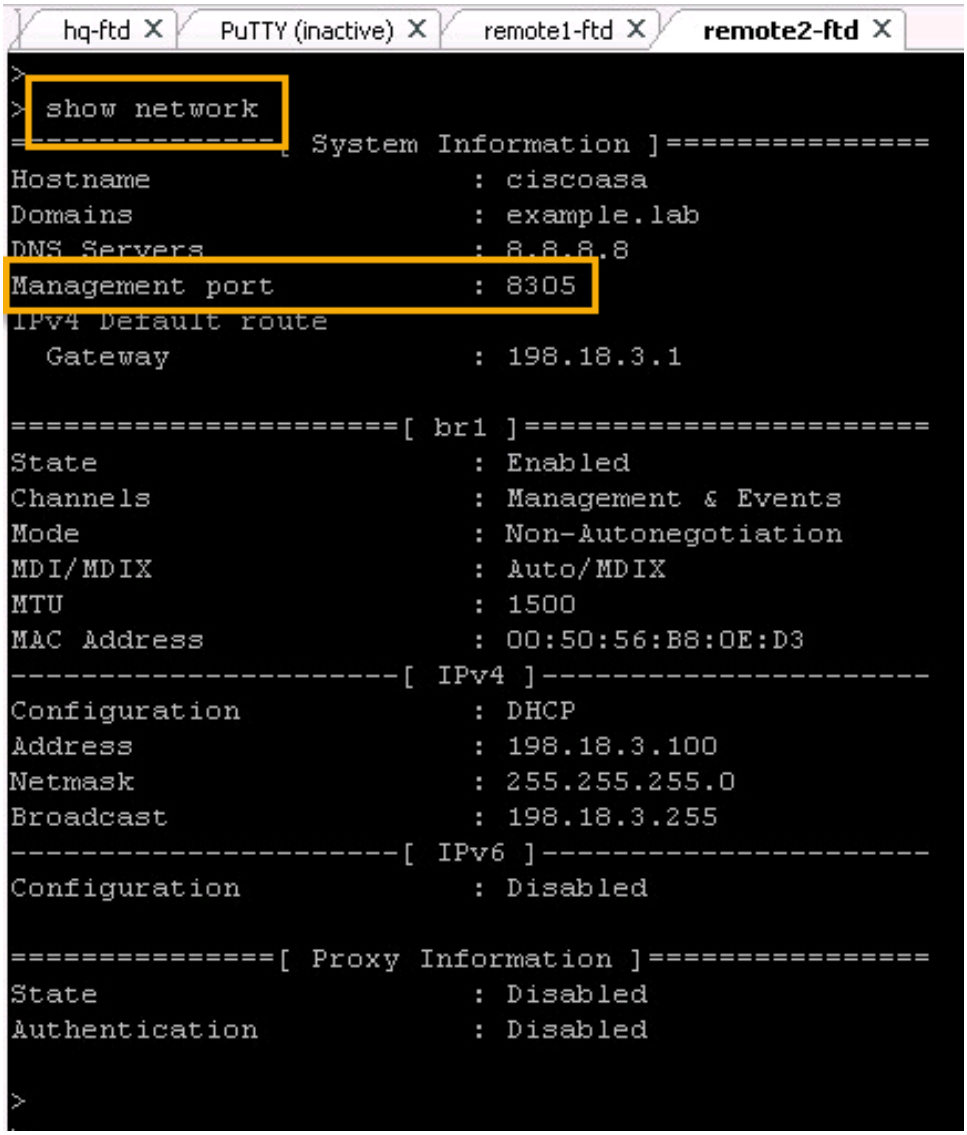


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

60. In order to know what port to expect, go over to the **ssh session** 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 221. Show network



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

61. 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:

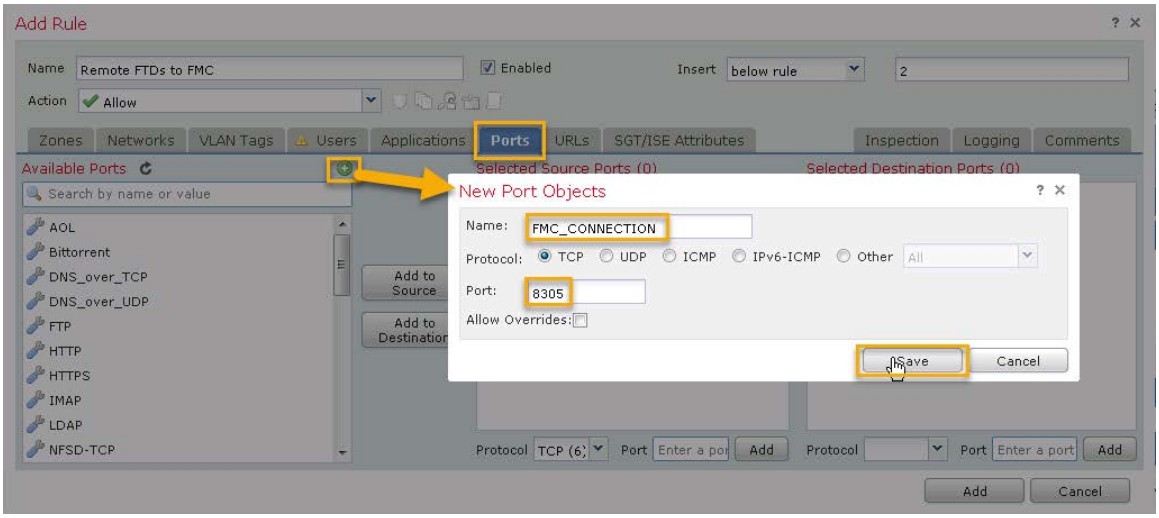
        i. Name: **FMC_CONNECTION**

        ii. Protocol: **TCP**

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

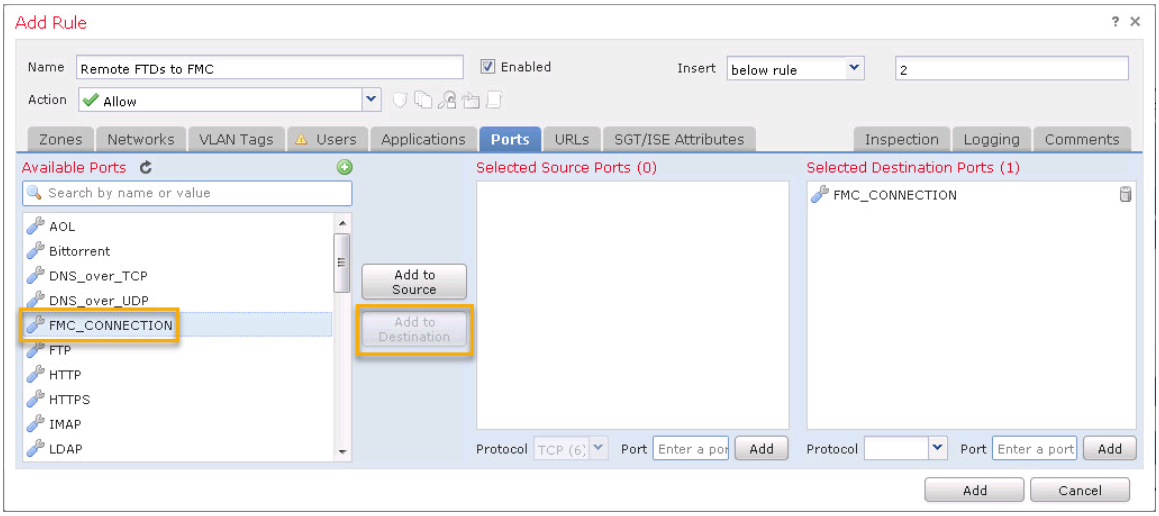
        iv. Click **Save**.

Figure 222. Create Port Object



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

Figure 223. Configure Ports tab



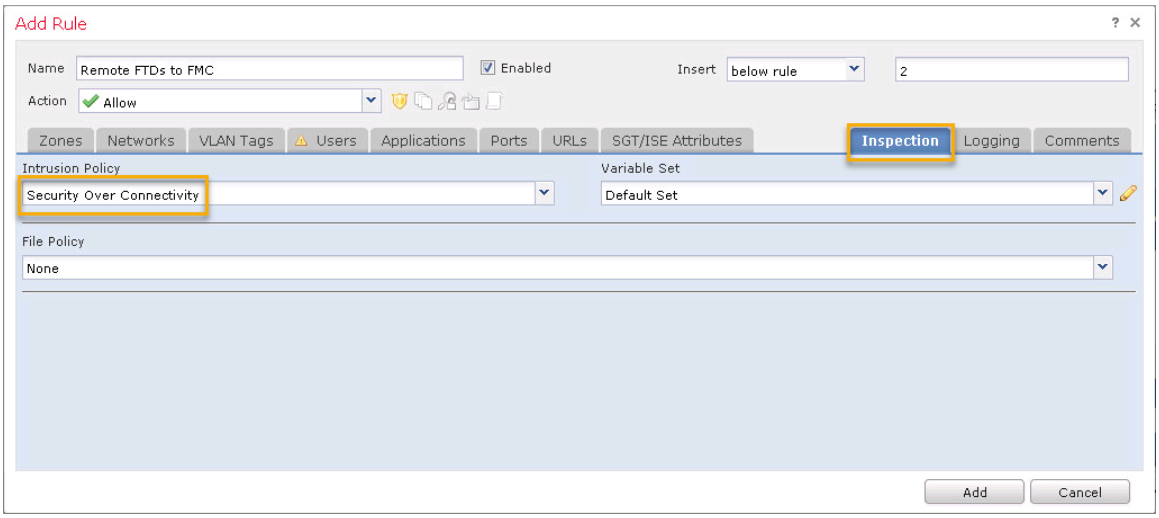
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

62. On the **Inspection tab**:

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

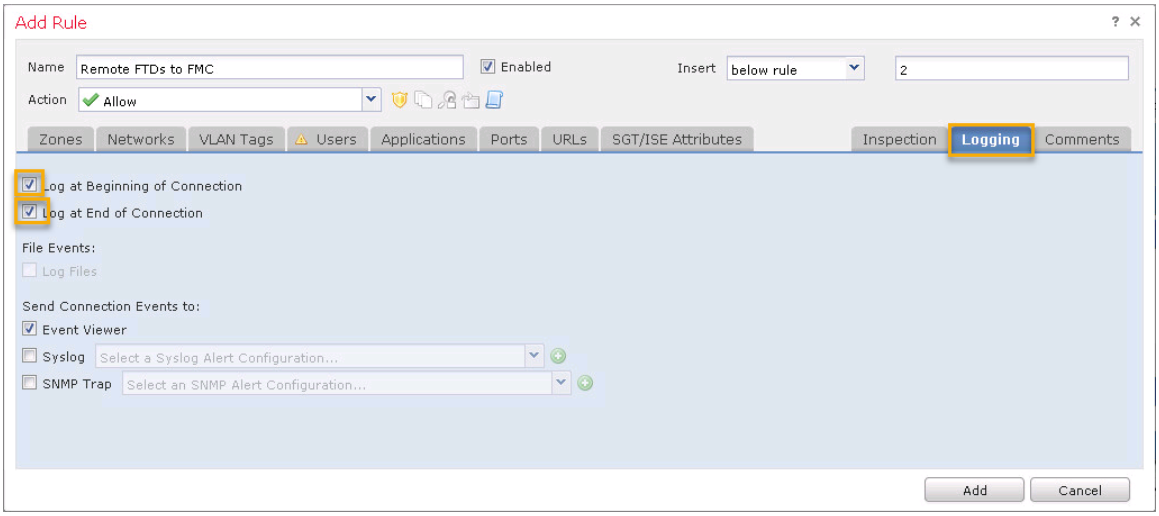
Figure 224. Configure the Inspection tab



63. 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 225. Configure Logging tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

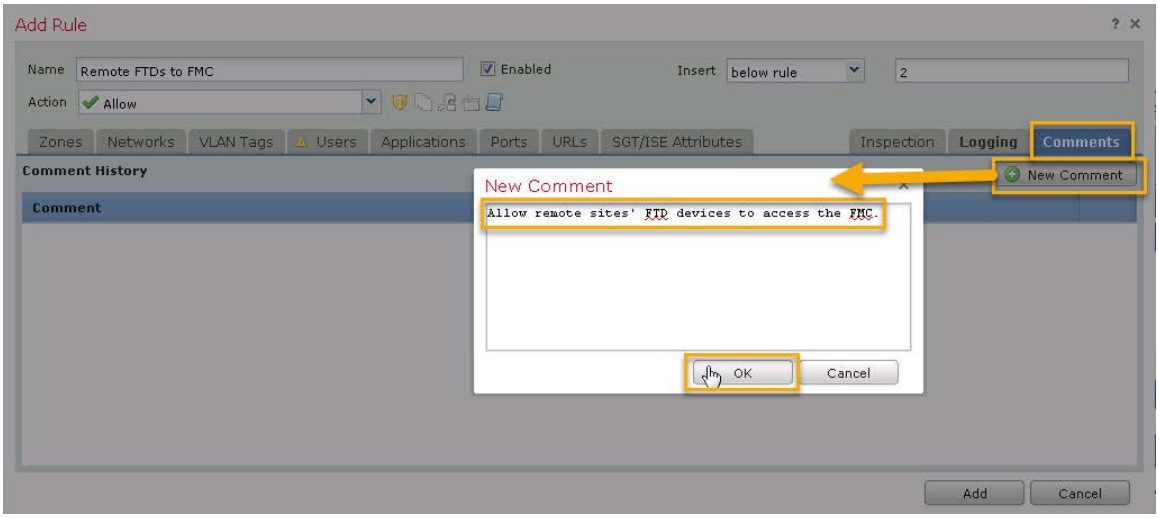
64. On the **Comments tab**:

    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.**

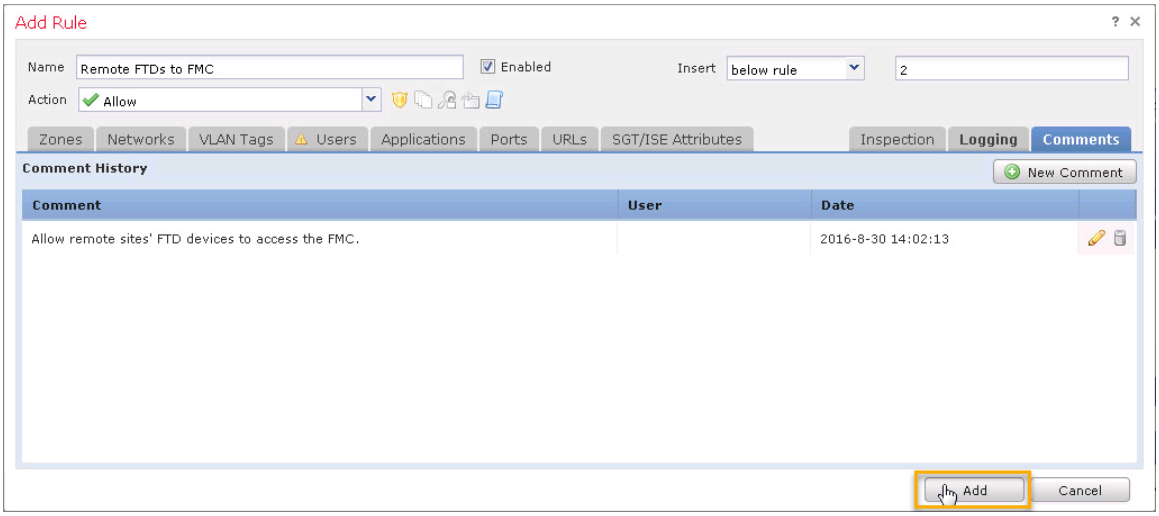
        ii. Click **OK**.

Figure 226. Add a Comment



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

Figure 227. Finish the rule



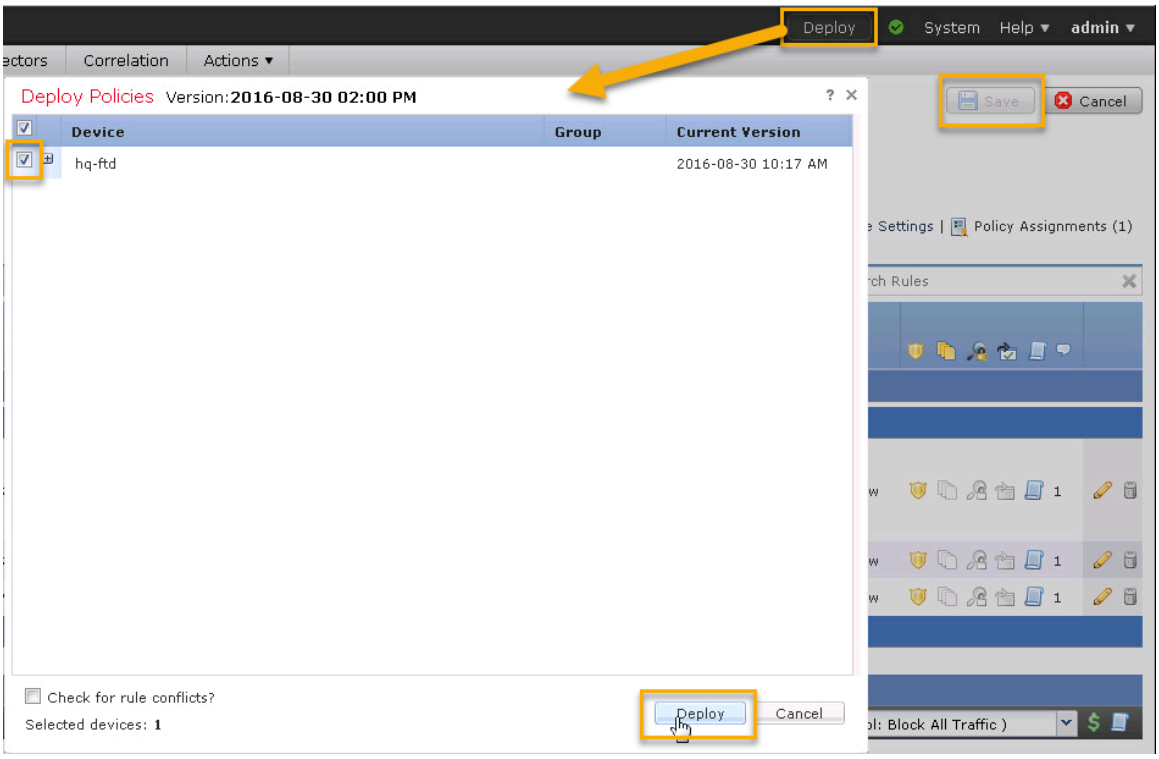
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

66. Click **Save** and then **Deploy**.

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

Figure 228. Save and Deploy to hq-ftd



68. 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**.

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

Figure 229. Add new device

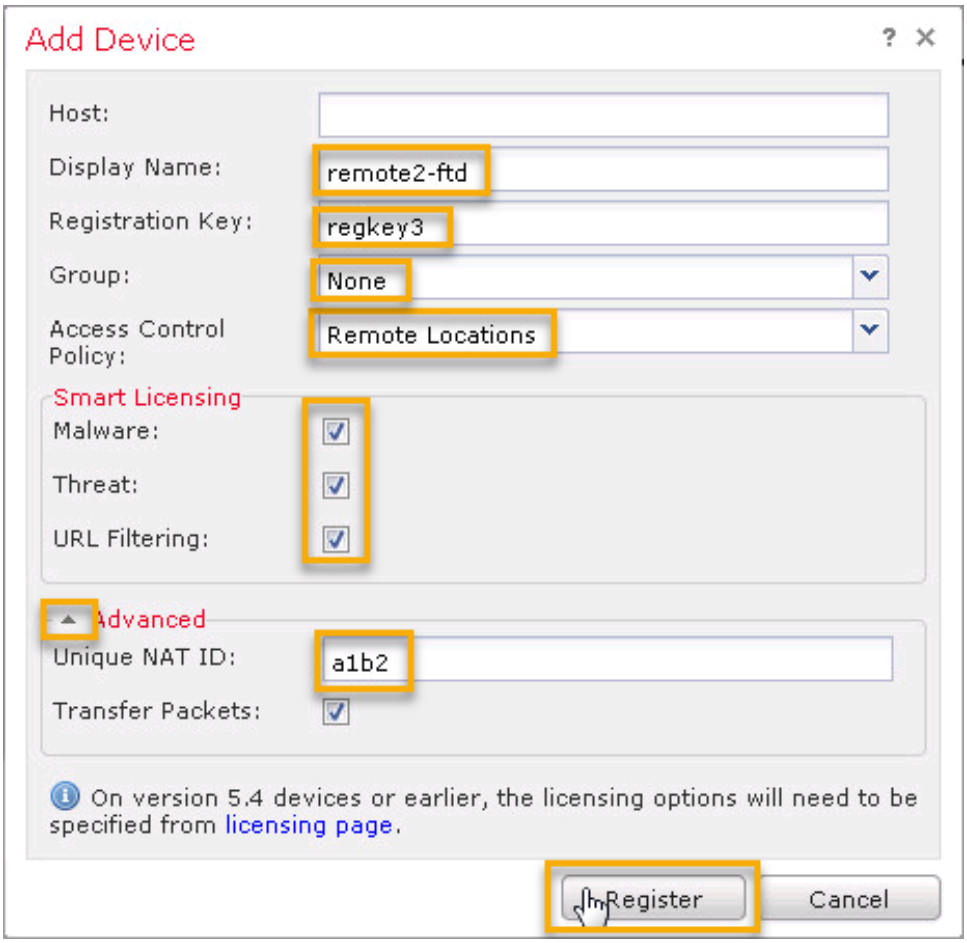


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

70. 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.
71. Expand the Advanced section.
    a. Unique NAT ID: **a1b2**
72. Click **Register**.

Figure 230. Add remote2-ftd device



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

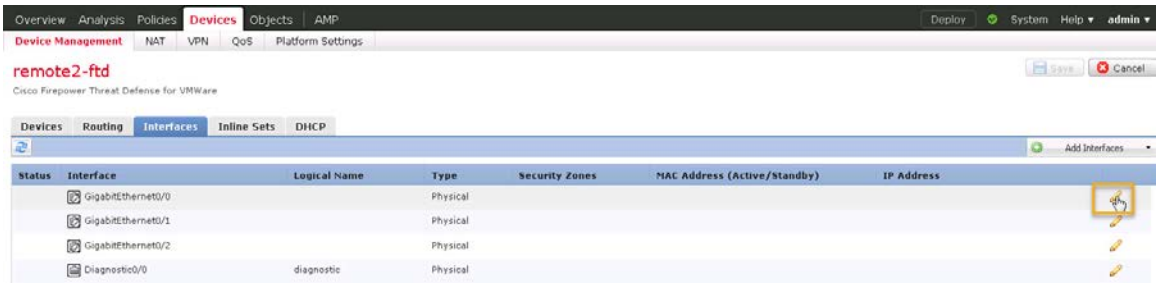
73. As soon as the **remote2-ftd** device shows up in the Device Management list click the **pencil icon** associated with its row. Then use the following to fill out the needed information:

Figure 231. Edit remote2-ftd



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

Figure 232. Edit g0/0

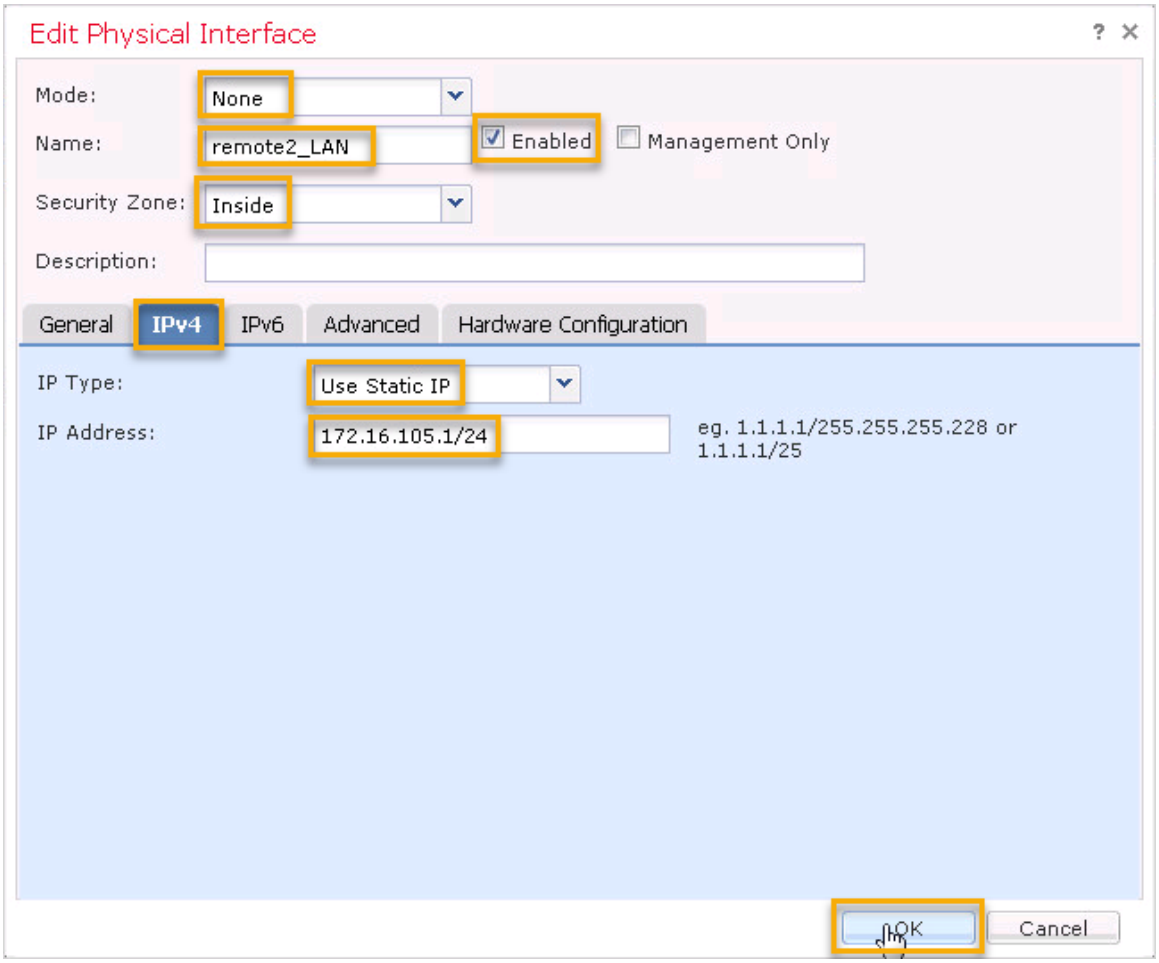


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

75. Use the following to configure GigabitEthernet0/0.
    a. Mode: **None**
    b. Name: **remote2_LAN**
    c. Enabled: **Checked**
    d. Security Zone: **Inside**
76. On the **IPv4 tab** set the IP Address field to **172.16.105.1/24**.
77. Click **OK**.

Figure 233. Configured g0/0

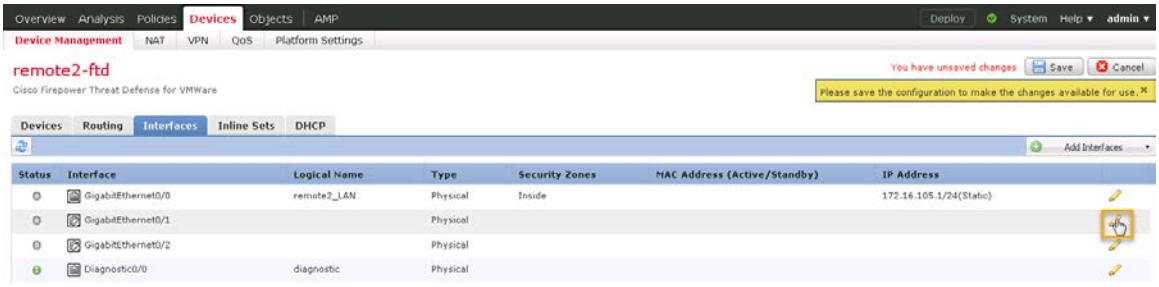


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

Figure 234. Edit g0/1

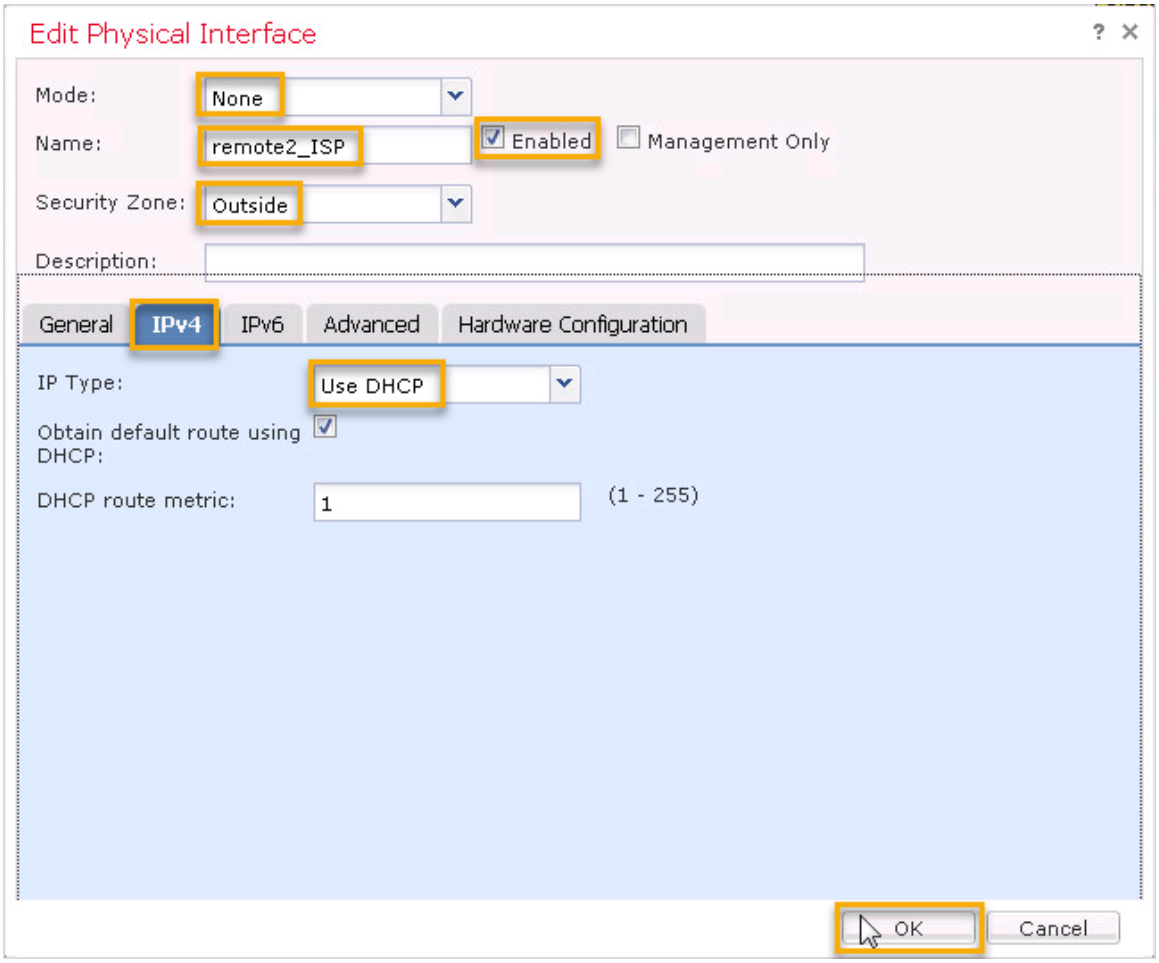


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

79. Use the following to configure GigabitEthernet0/1.
    a. Mode: **None**
    b. Name: **remote2_ISP**
    c. Enabled: **Checked**
    d. Security Zone: **Outside**
80. On the **IPv4 tab** set the IP Type field to **Use DHCP**.
81. Click **OK**.

Figure 235. Configured g0/1



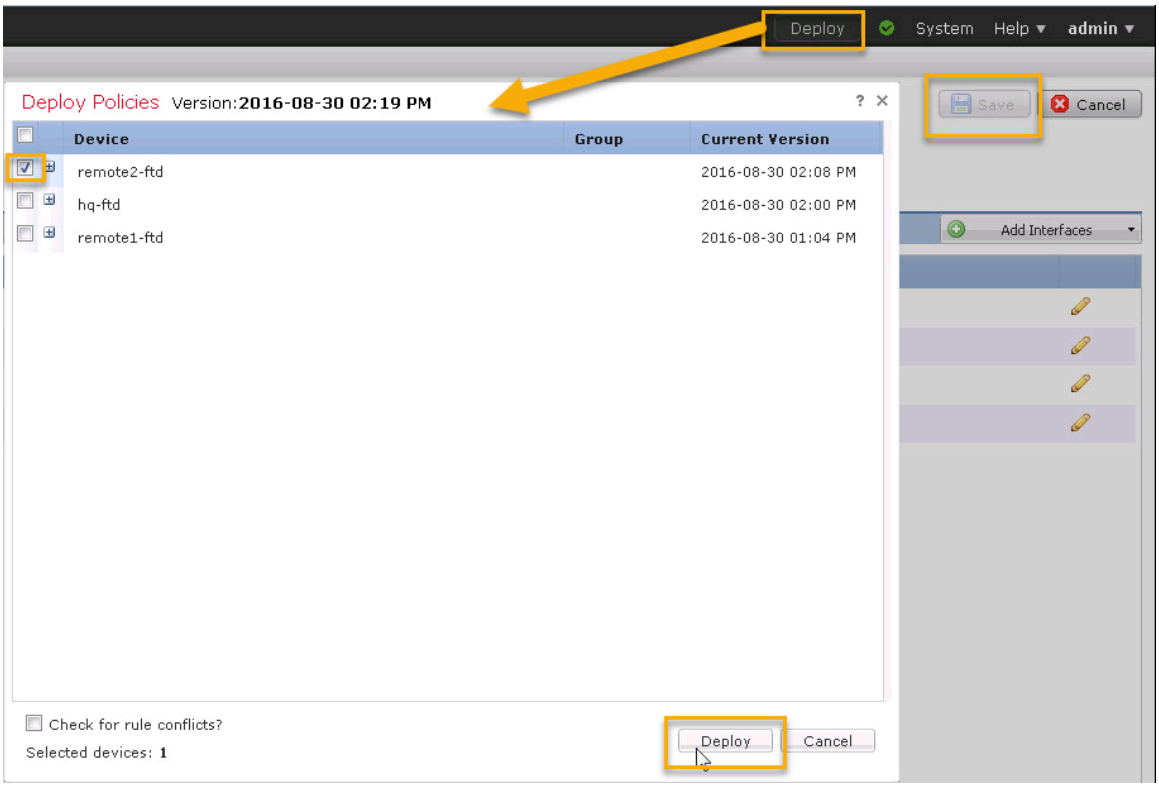
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

82. Click **Save** and then **Deploy**.

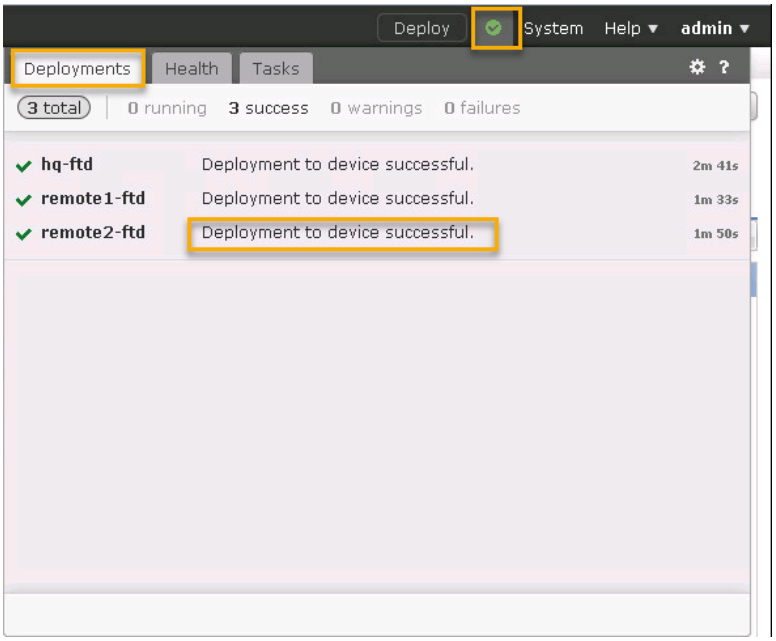
83. Select the **remote2-ftd** device and click **Deploy**.

Figure 236. Save and Deploy to remote2-ftd



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

Figure 237. Deployment is complete

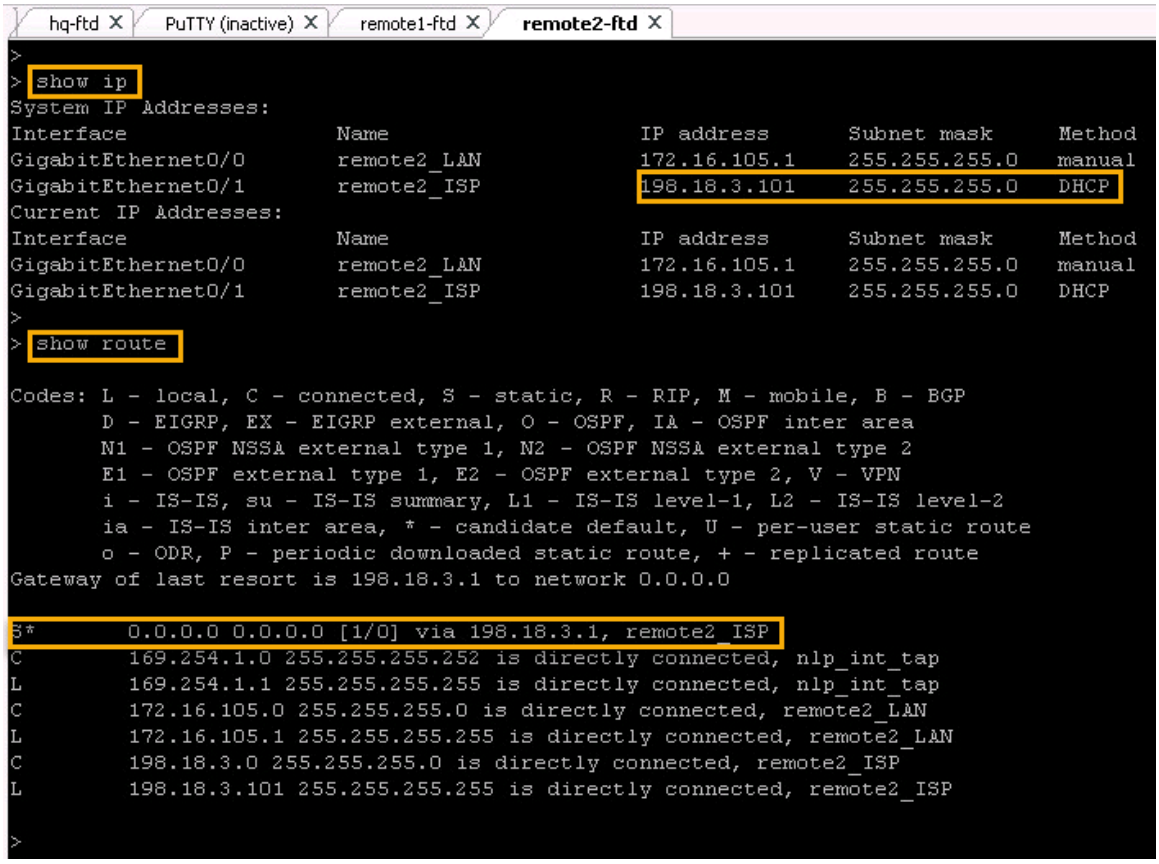


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

85. 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 238. Show ip and show route



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

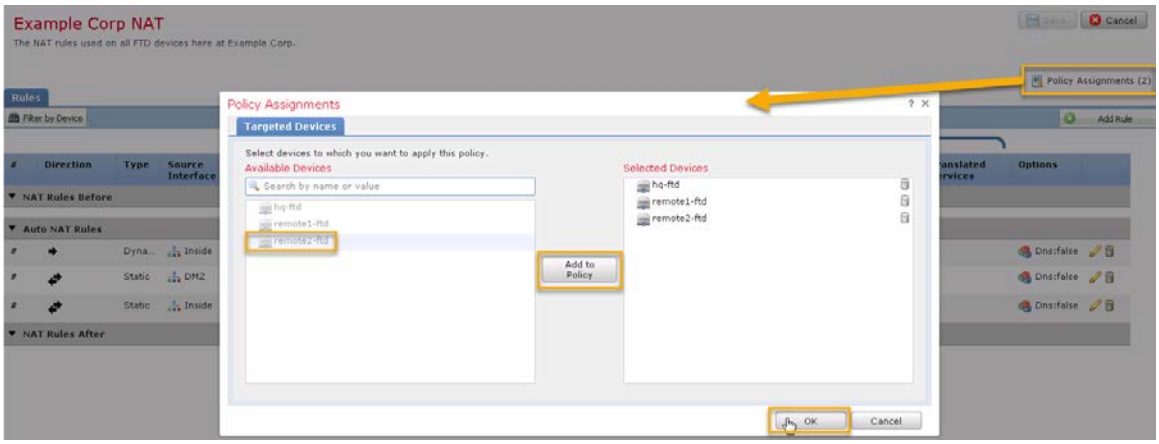
86. Let's fix this now. On the FMC webpage navigate to **Devices > NAT**.
87. Click the **pencil icon** for the **Example Corp NAT** policy.

Figure 239. Edit NAT Policy



88. Click the **Policy Assignments** link.
89. Select **remote2-ftd** from the **Available Devices** list and click the **Add to Policy** button.
90. Click **OK**.

Figure 240. Assign remote2-ftd to NAT Policy

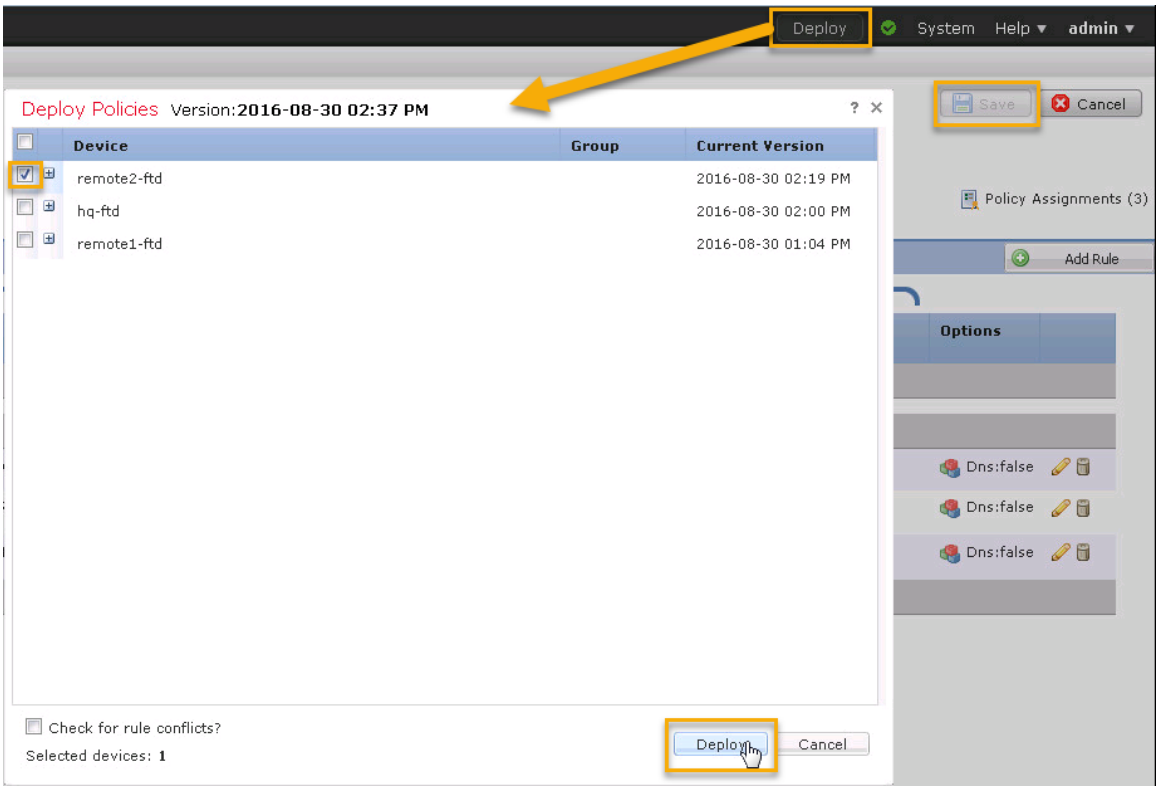


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

91. Click **Save** and then **Deploy**.
92. Select the **remote2-ftd** device and click **Deploy**.

Figure 241. Save and Deploy



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

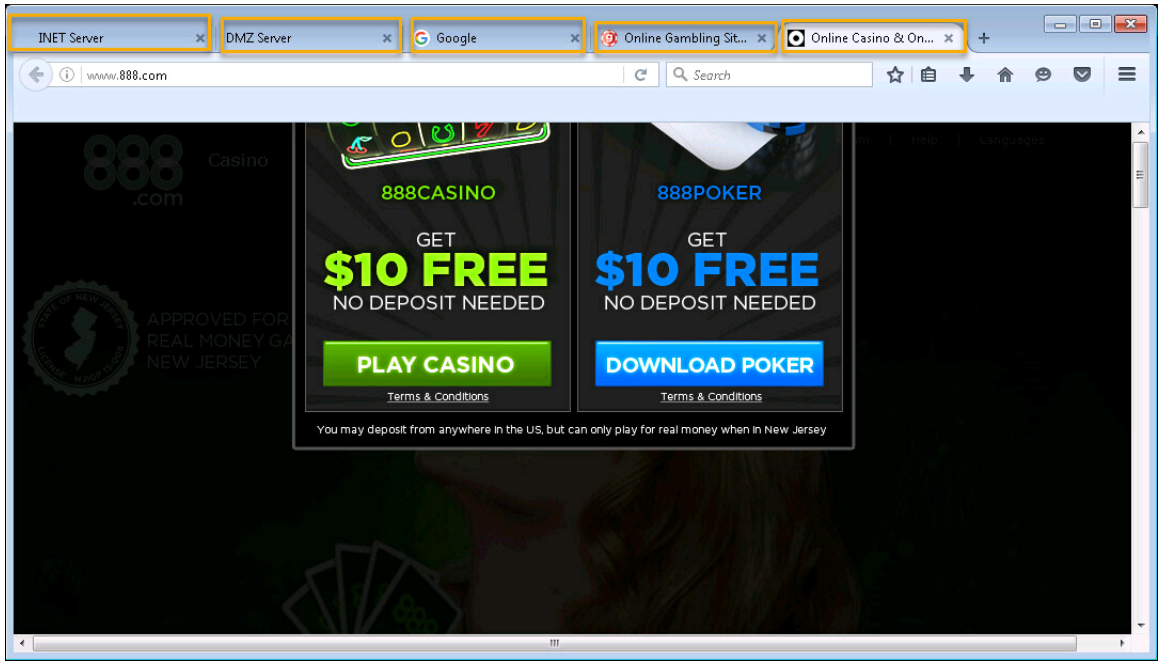
Testing INET Access – Phase 2

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

93. From the **Jumpbox**, **RDP** to **remote2-wkst**. (198.18.129.3 is the NIC set up for RDP.)

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

Figure 242. Firefox on remote2-wkst works!



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.)

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

95. On **hq-wkst** access the FMC website and navigate to **Policies > Access Control > Access Control**.
96. Click the **pencil icon** for the **Base Policy**.

Figure 243. Edit the Base Policy



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

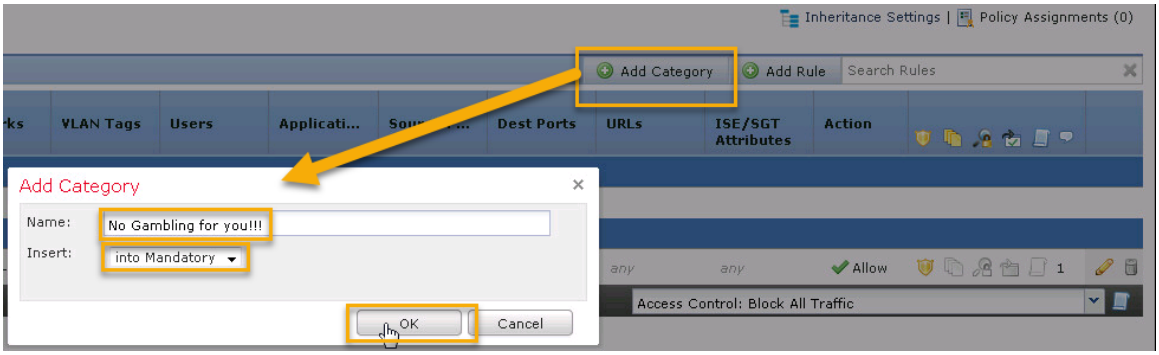
97. Click the **Add Category** button and use the following to fill out the popup window:

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

    b. Insert: **into Mandatory**

    c. Click **OK**.

Figure 244. Create Category



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

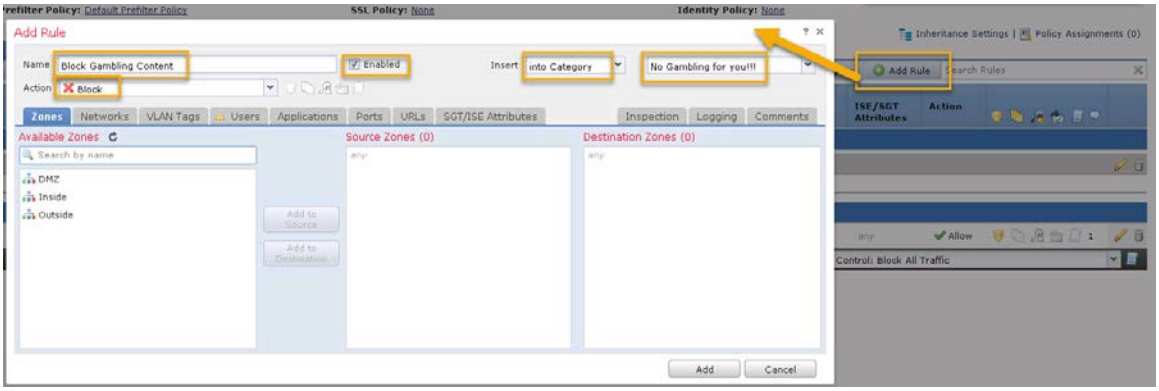
    a. Name: **Block Gambling Content**

    b. Enabled: **Checked**

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

    d. Action: **Block**

Figure 245. Part 1 Add Rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

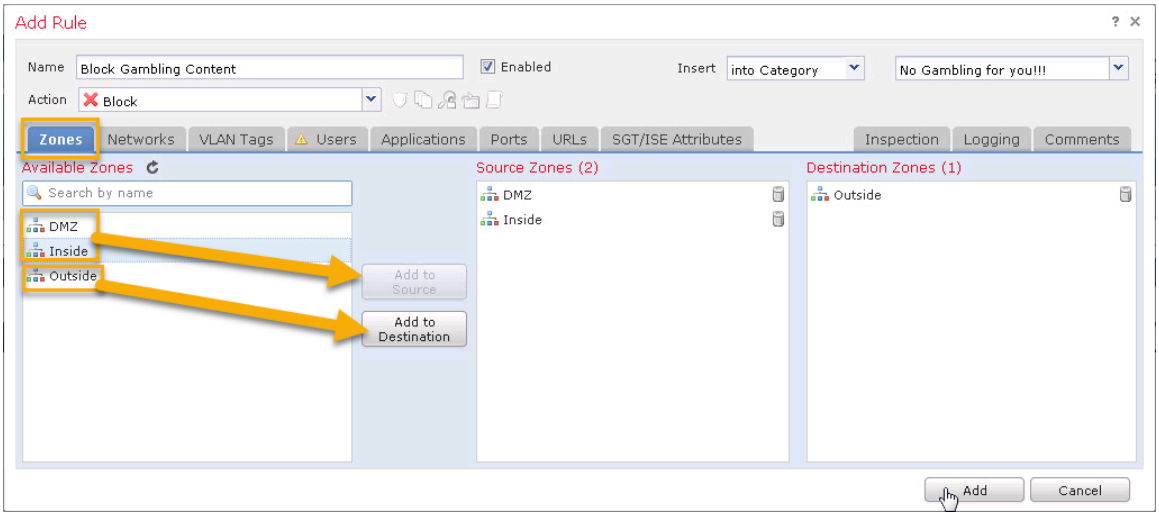
https://t.me/learningnets

99. 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 246. Configure Zones tab

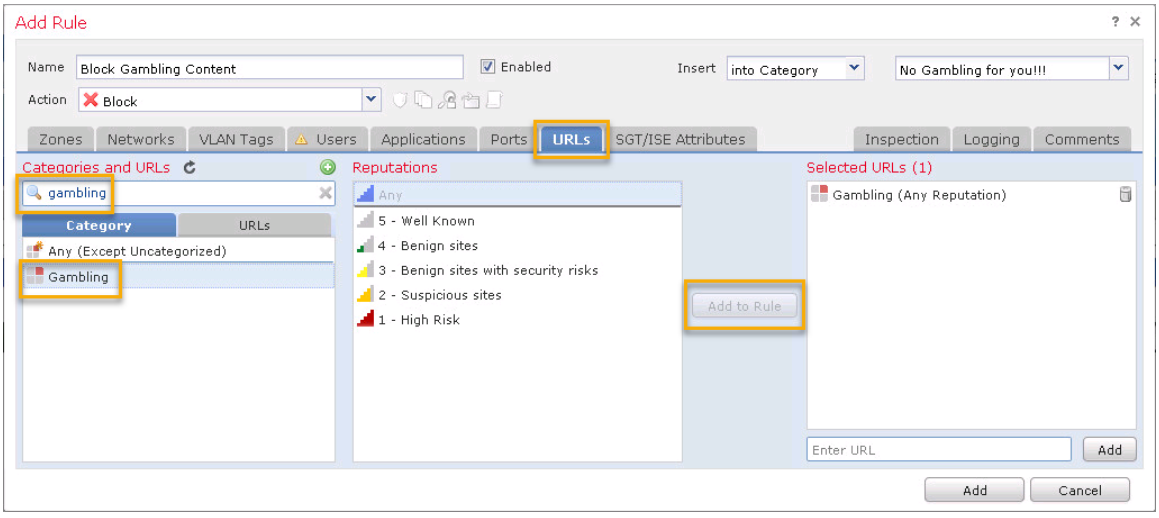


100. On the **URLs tab**:

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

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

Figure 247. Configure URLs tab



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.

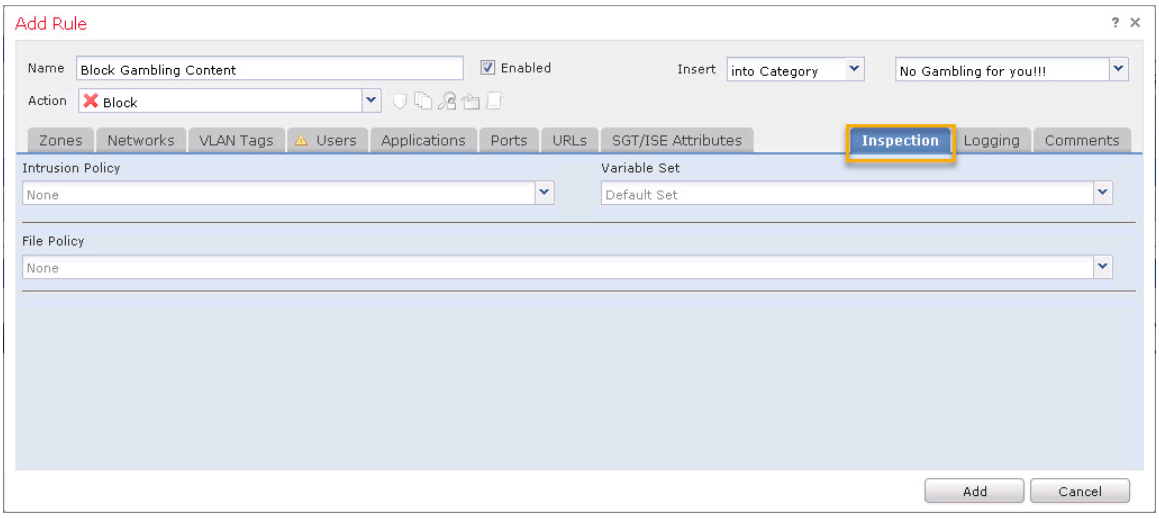
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

101. 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 248. Can't configure Inspection tab

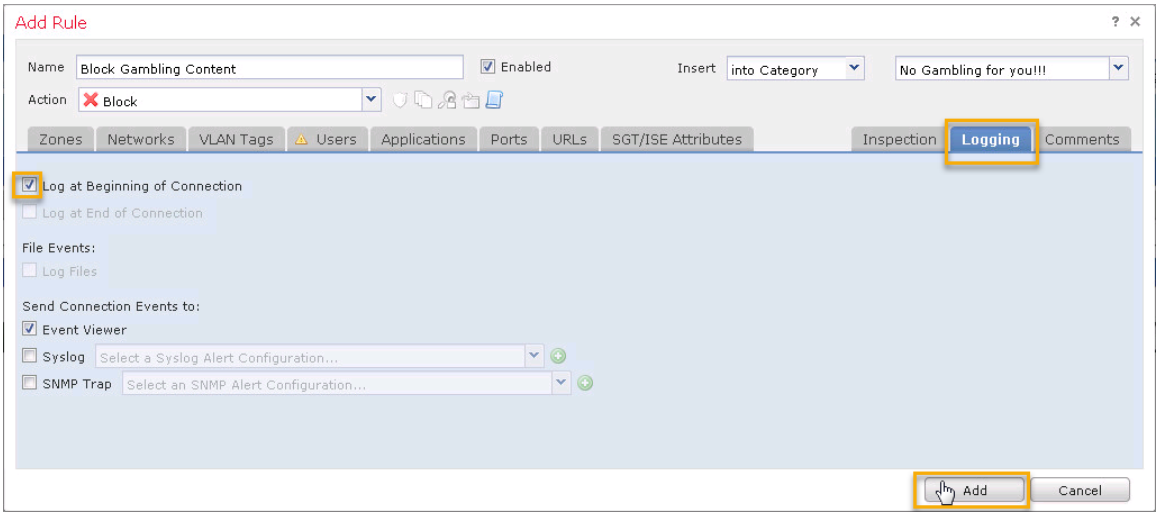


102. On the **Logging tab**:

    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).

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

Figure 249. Configure Logging tab and Add rule.



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

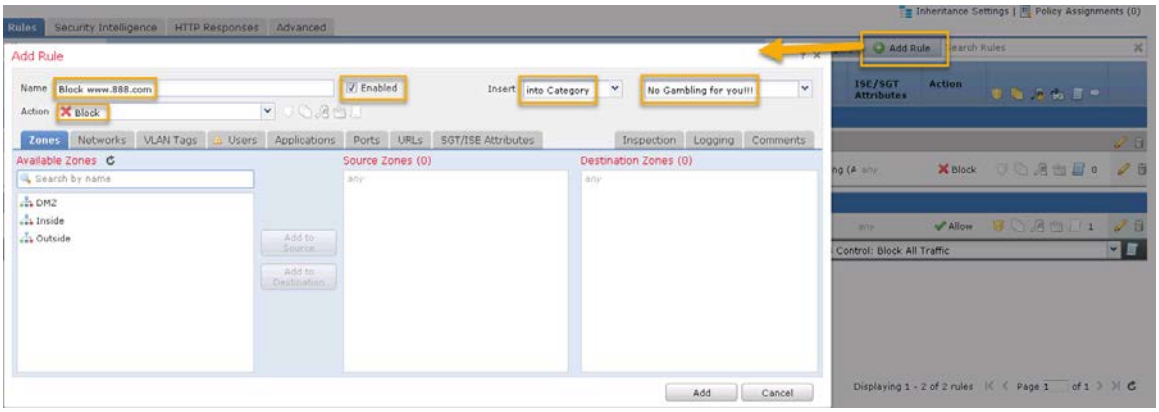
    a. Name: **Block www.888.com**

    b. Enabled: **Checked**

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

    d. Action: **Block**

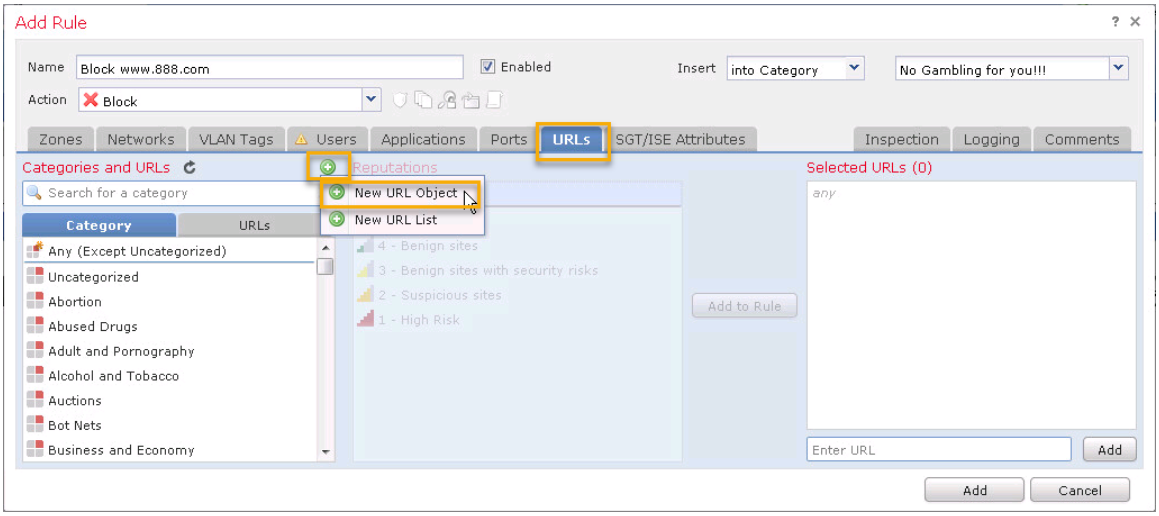
Figure 250. Part 1 of Add Rule



105. On the **URLs tab**:

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

Figure 251. Create URL Object



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

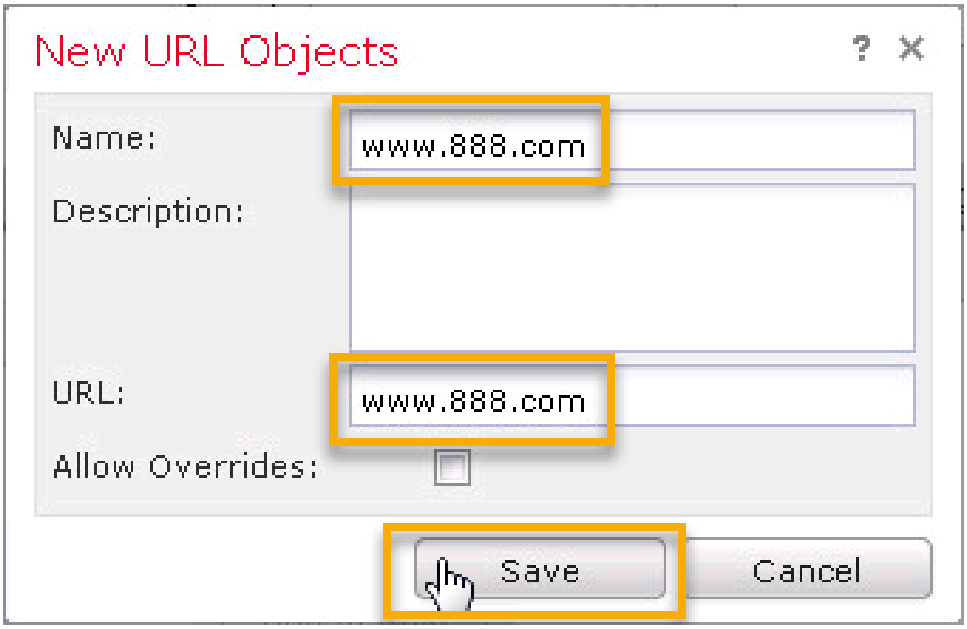
b. Use the following to fill out the information for the popup window:

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

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

iii. Click **Save**.

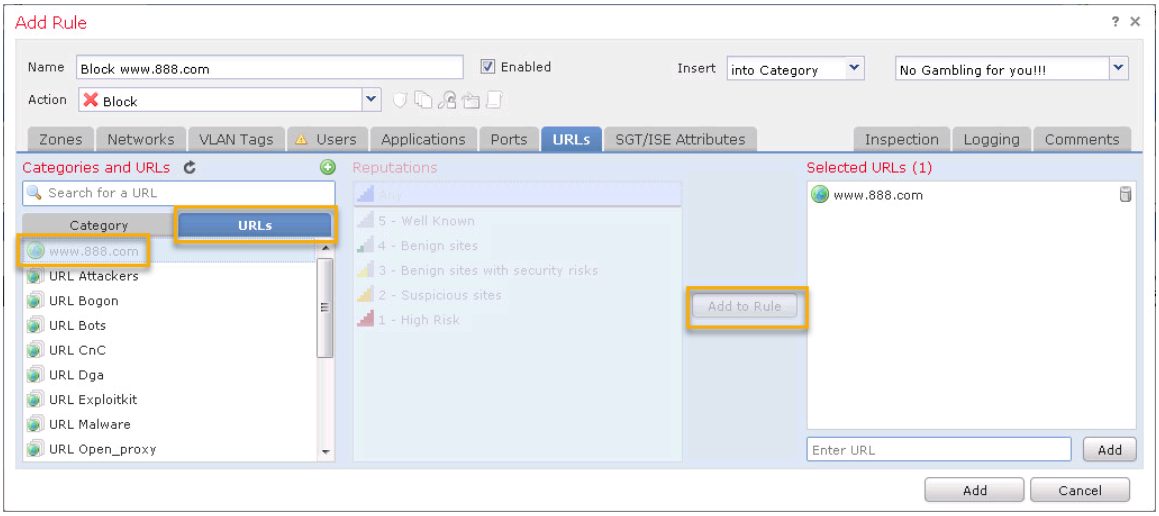
Figure 252. Create URL Object



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 253. Configure URLs tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

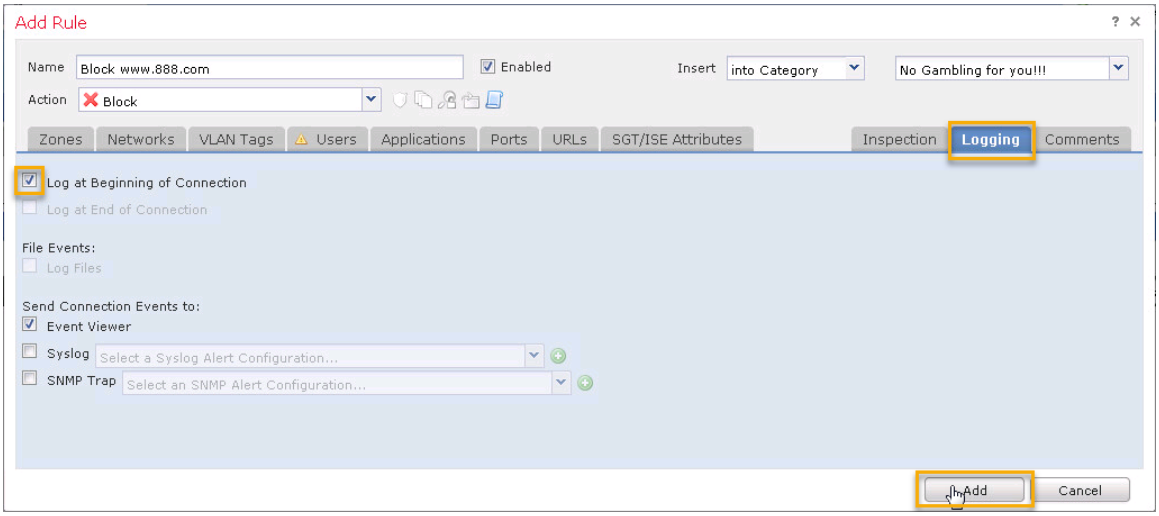
https://t.me/learningnets

106. On the **Logging tab**:

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

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

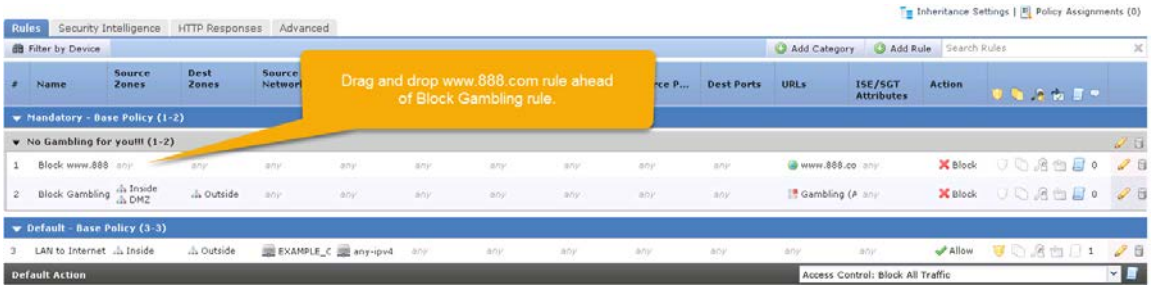
Figure 254. Configure Logging and Add rule



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.

108. 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 255. Move www.888.com rule up



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

109. 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 256. Configure HTTP Responses



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.

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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Test URL Filtering of Gambling Websites

111. 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 257. No access to www.gambling.com

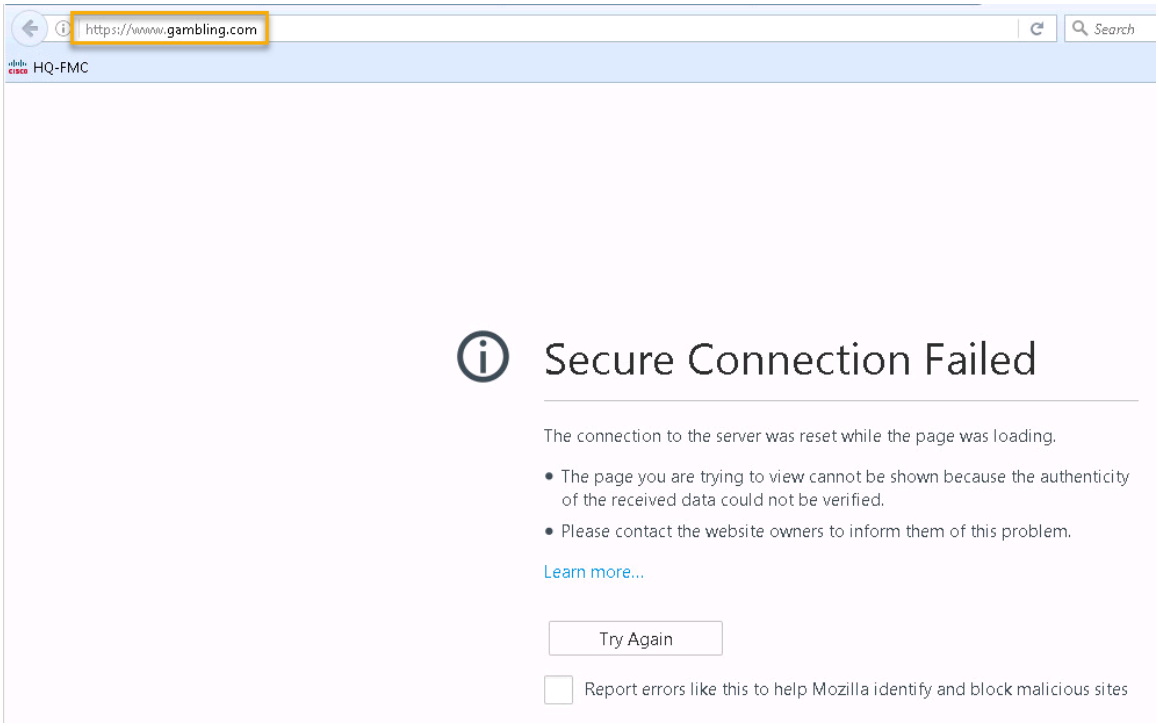
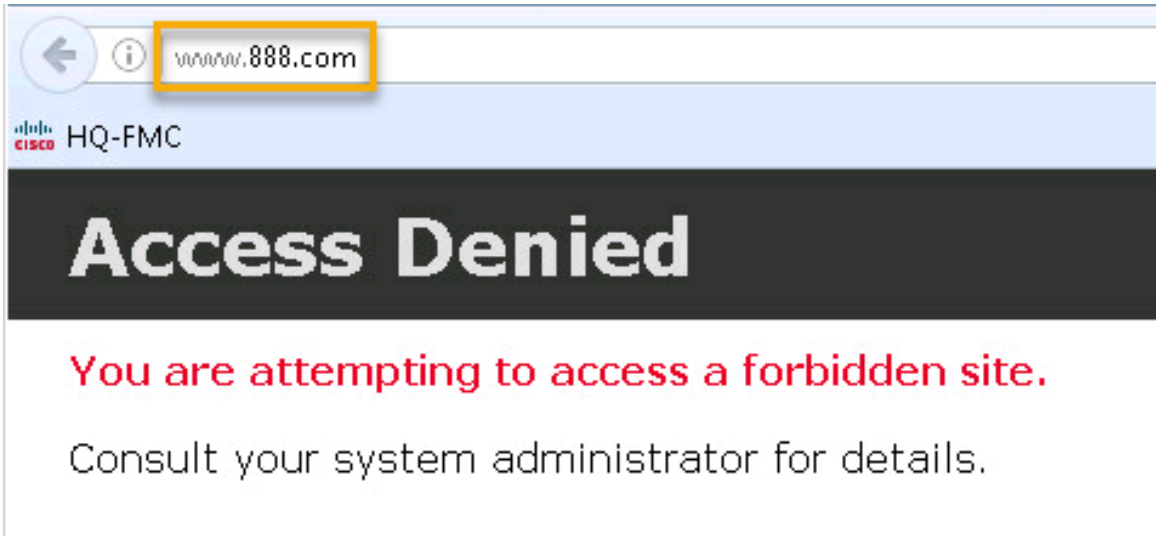


Figure 258. No access to www.888.com



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?)

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

112. 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 259. Connection Events

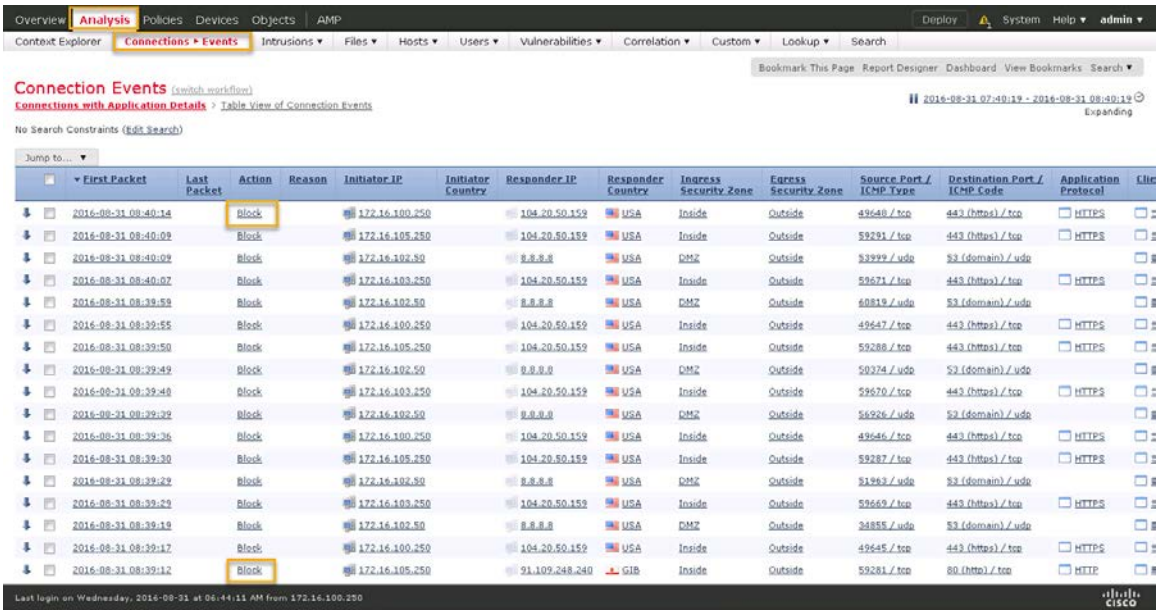
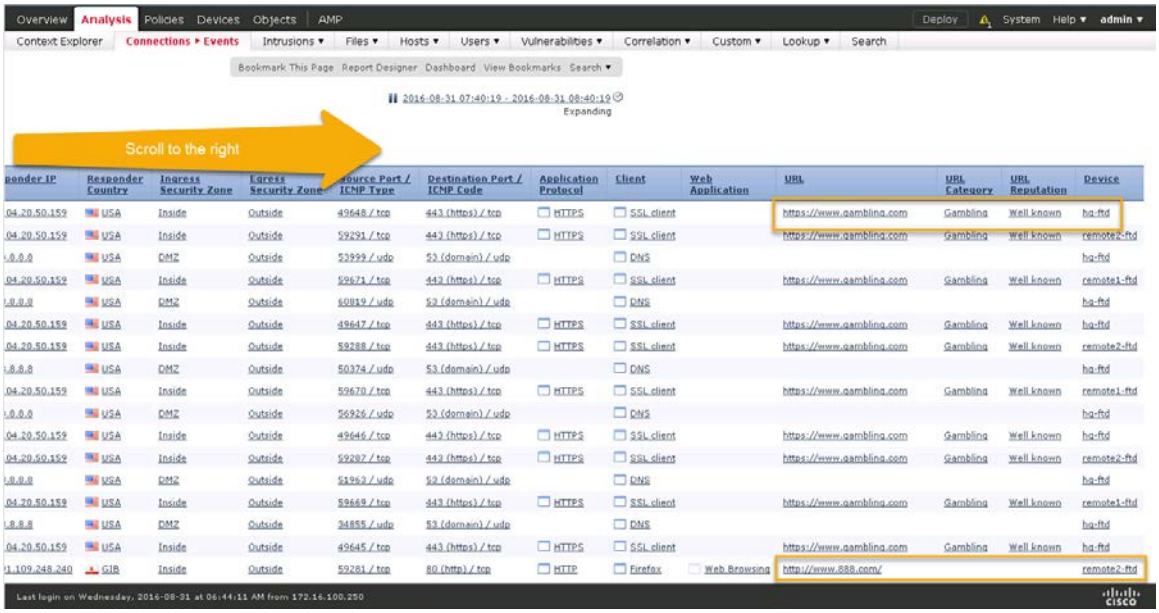


Figure 260. Scroll to the right



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

113. Navigate to Policies > Access Control > Access Control. Click the pencil icon on the row for the Base Policy.

Figure 261. Edit Base Policy ACP



114. Click the **Add Rule** button and use the following to fill out the popup window.

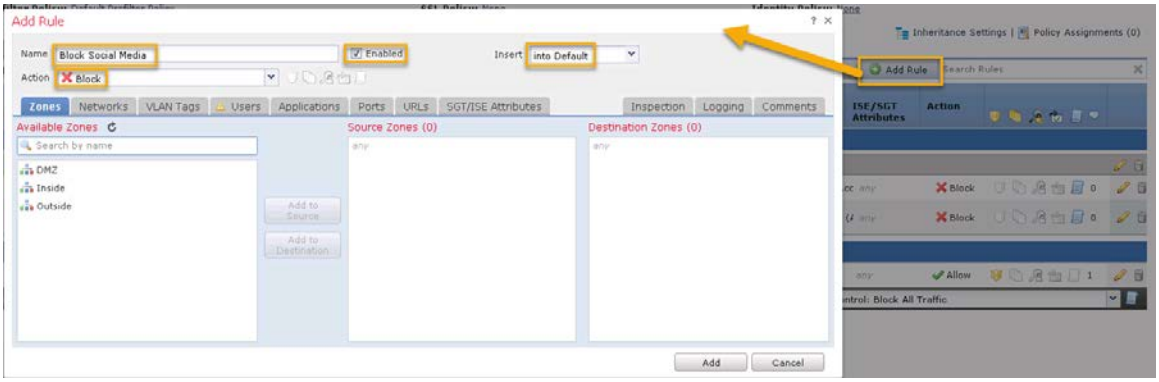
a. Name: **Block Social Media**

b. Enabled: **Checked**

c. Insert: **into Default** (Why did you choose Default and not Mandatory?)

d. Action: **Block**

Figure 262. Part 1 of Add rule



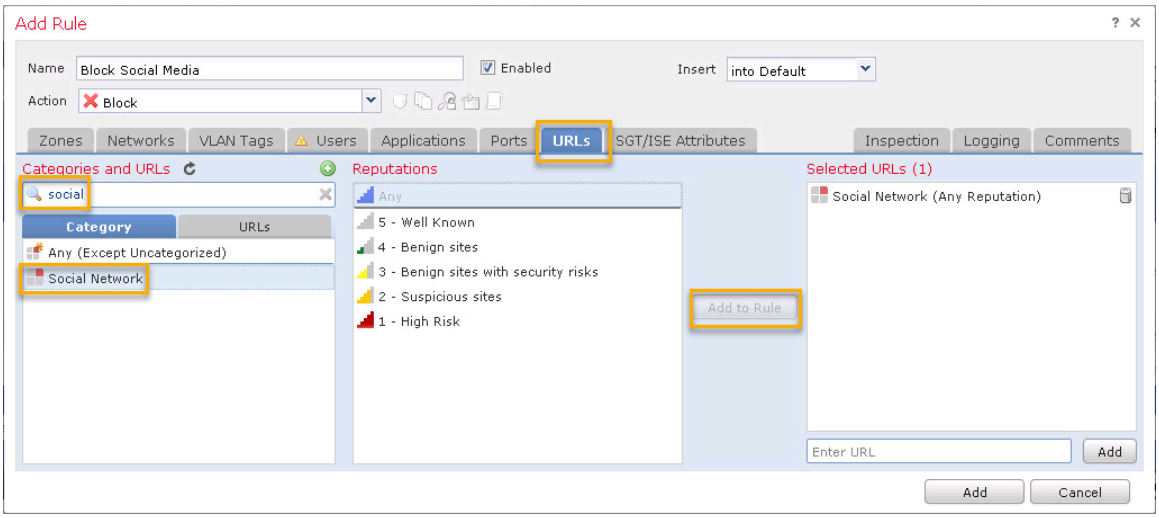
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

115. On the **URLs tab**:

    a. Search for **social** and then select **Social Network** from the list. Click the **Add to Rule** button.

Figure 263. Configure URLs tab

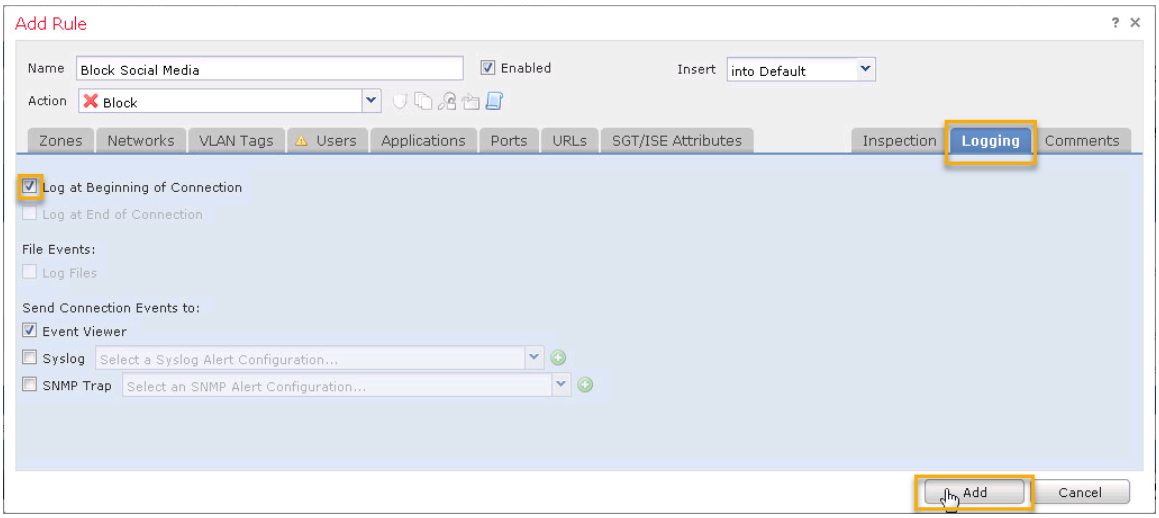


116. On the **Logging tab**:

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

117. Click **Add**.

Figure 264. Configure Logging tab and Add rule

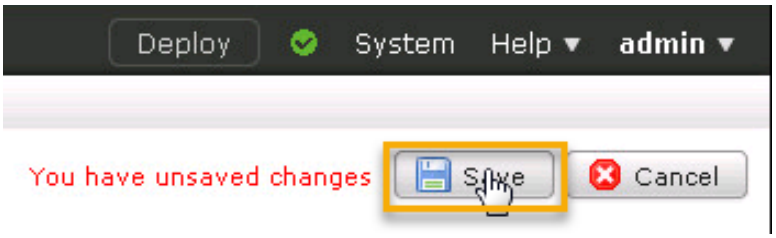


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

118. Click **Save** before going on to edit the HQ Policy.

Figure 265. Save changes



119. Navigate to **Policies > Access Control > Access Control** and click the **pencil icon** on the row for the **HQ Policy**.

Figure 266. Edit HQ Policy



120. Click **Add Rule** and use the following to fill out the popup window.

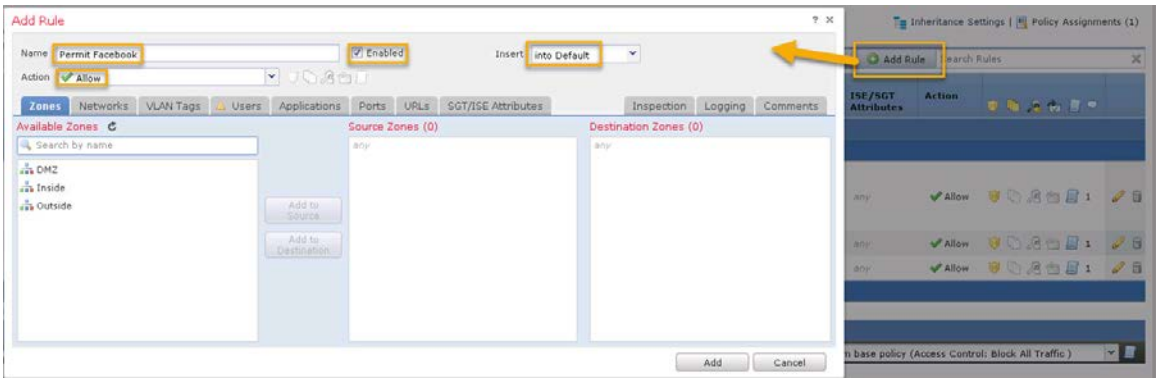
a. Name: **Permit Facebook**

b. Enabled: **Checked**

c. Insert: **into Default**

d. Action: **Allow**

Figure 267. Part 1 of adding a new rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

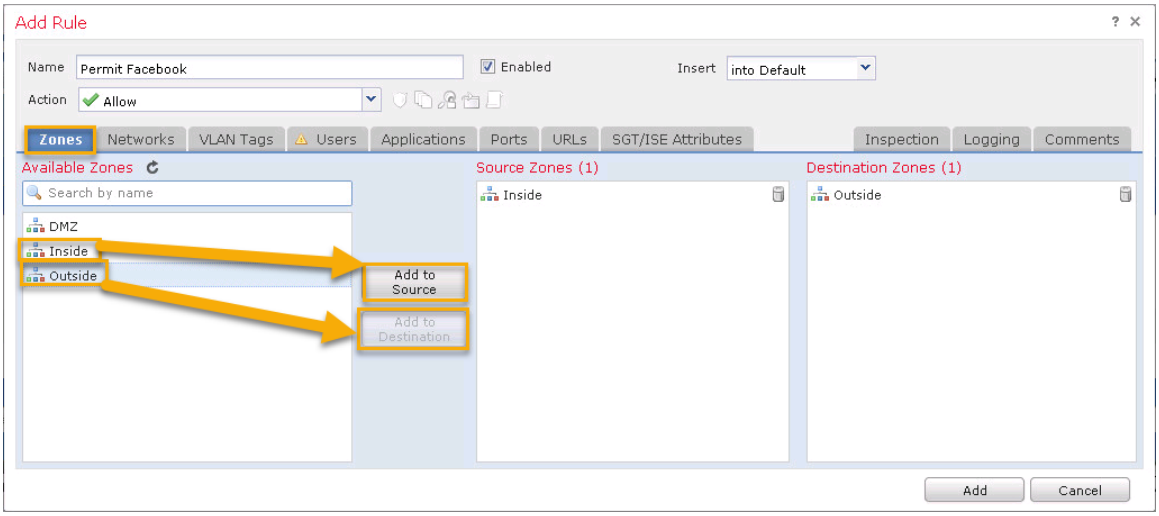
https://t.me/learningnets

121. On the **Zones tab**:

    a. Put **Inside** in the **Source Zones** section.

    b. Put **Outside** in the **Destination Zones** section.

Figure 268. Configure Zones tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

122. On the **URLs tab**:

a. Click the **green plus icon** and create a **new URL Object** for www.facebook.com.

Figure 269. New URL Object

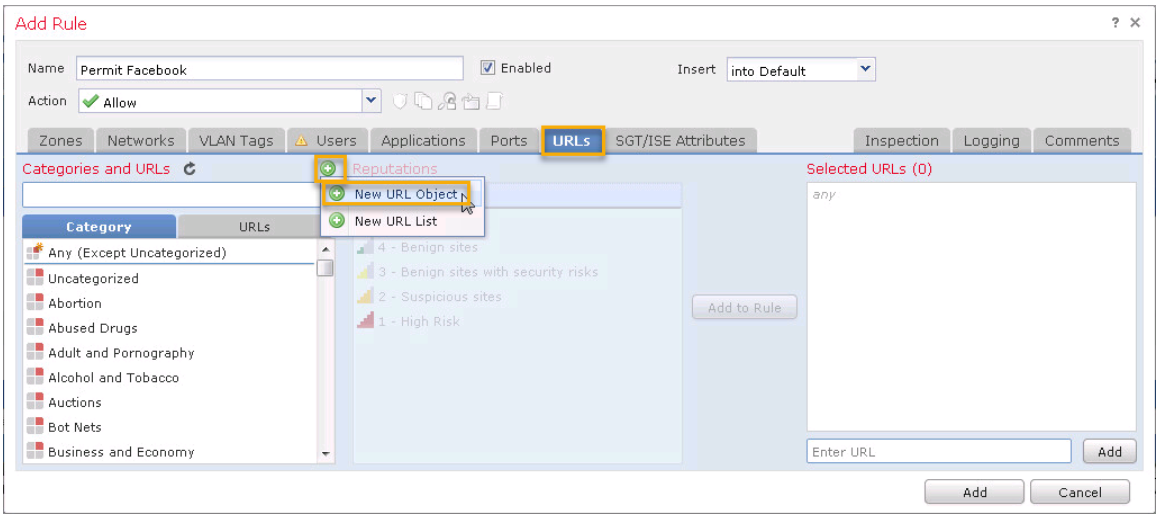
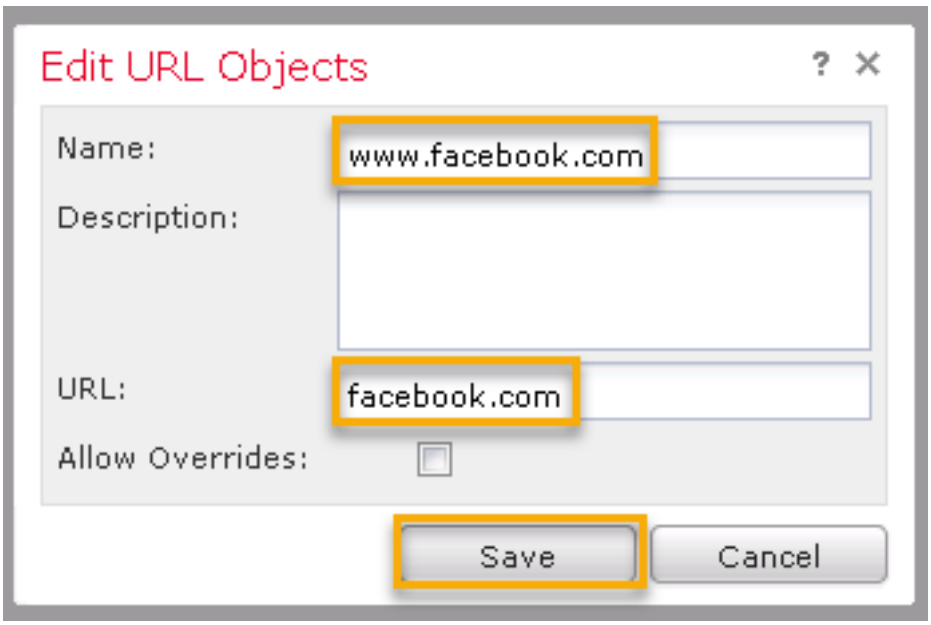


Figure 270. Create URL Object



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

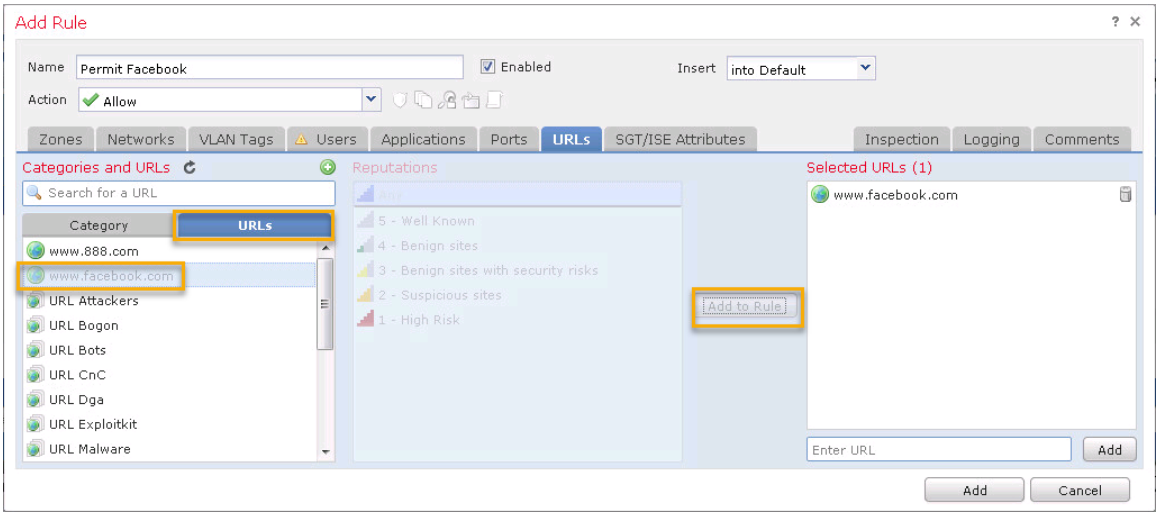
NOTE: When first creating this lab guide the Facebook URL Object's URL was www.facebook.com. However, due to changes to Facebook's homepage this section of the lab would fail where it used to work! (They made a change to refer to facebook.com instead of www.facebook.com which does not match our intended 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 271. Configure URLs tab



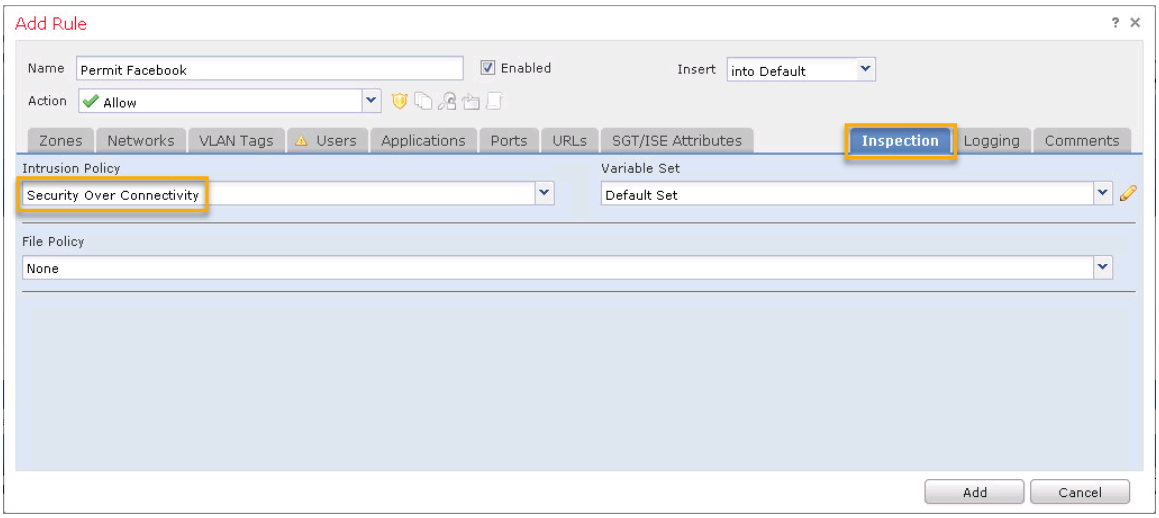
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

123. On the **Inspection tab**:

    a. Set the Intrusion Policy to **Security Over Connectivity**.

Figure 272. Configure Inspection tab

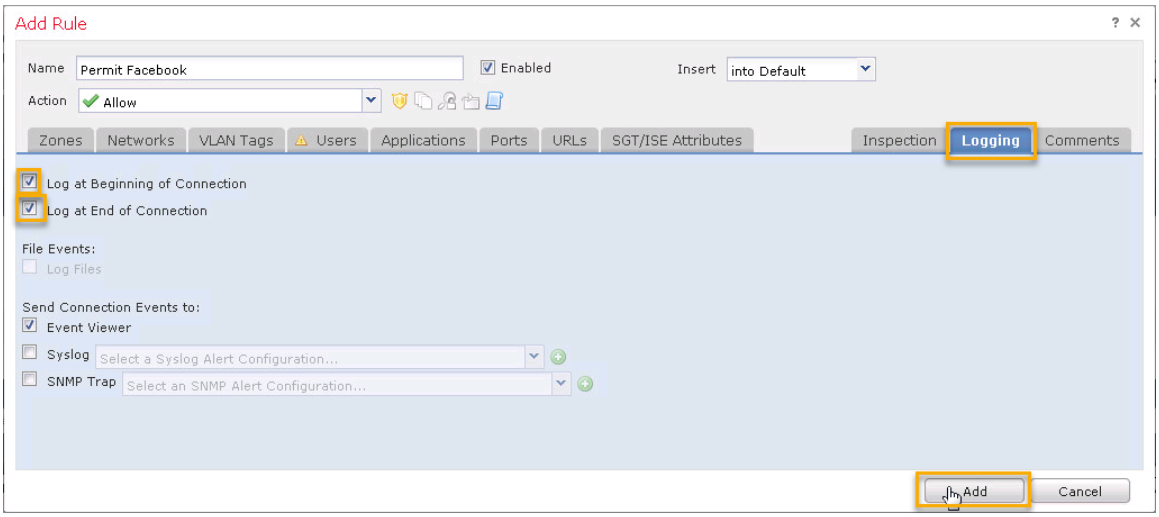


124. On the **Logging tab**:

    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.)

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

Figure 273. Configure Logging tab and add rule

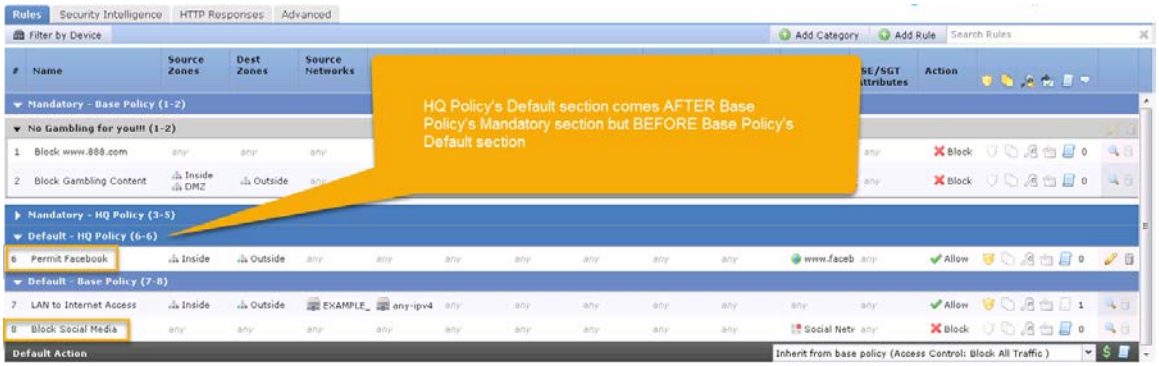


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

126. 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 274. View order of ACP rules



127. Click **Save**, then **Deploy**. Select **all the FTDs** and click **Deploy**.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

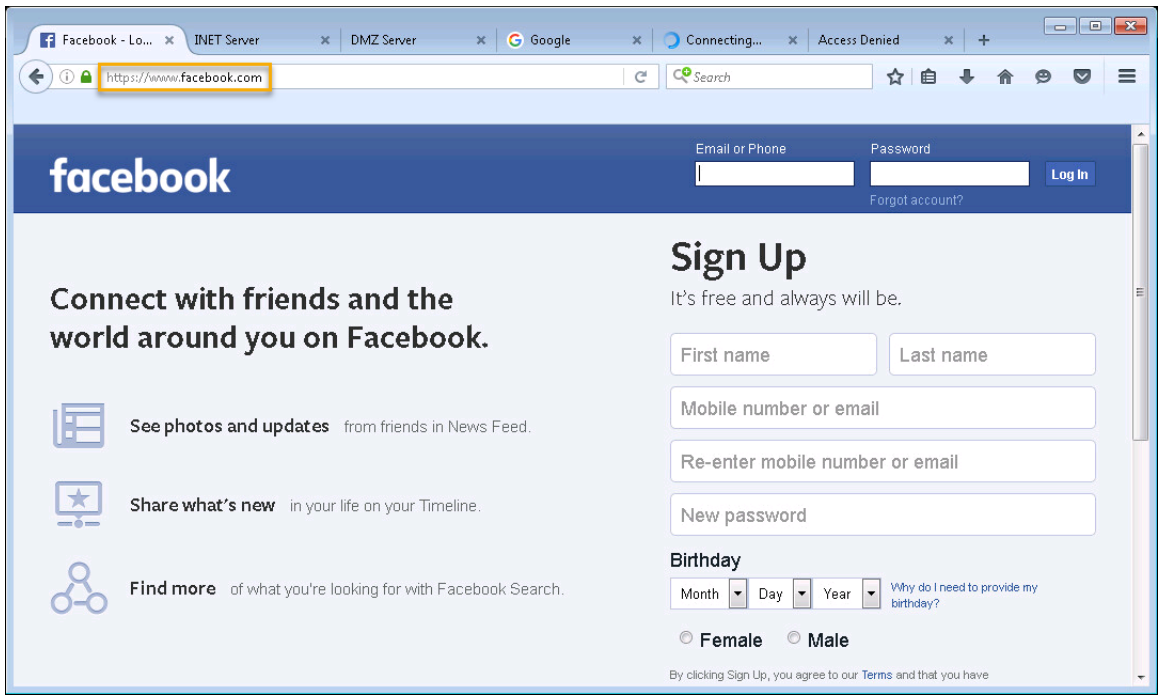
https://t.me/learningnets

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. ☺

128. 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 275. Success where it should have failed



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Test Social Media URL Filtering Rules – Phase 2

129. 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 276. Edit Base Policy ACP



130. **Edit** the **Block Social Media** rule.

Figure 277. Edit rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

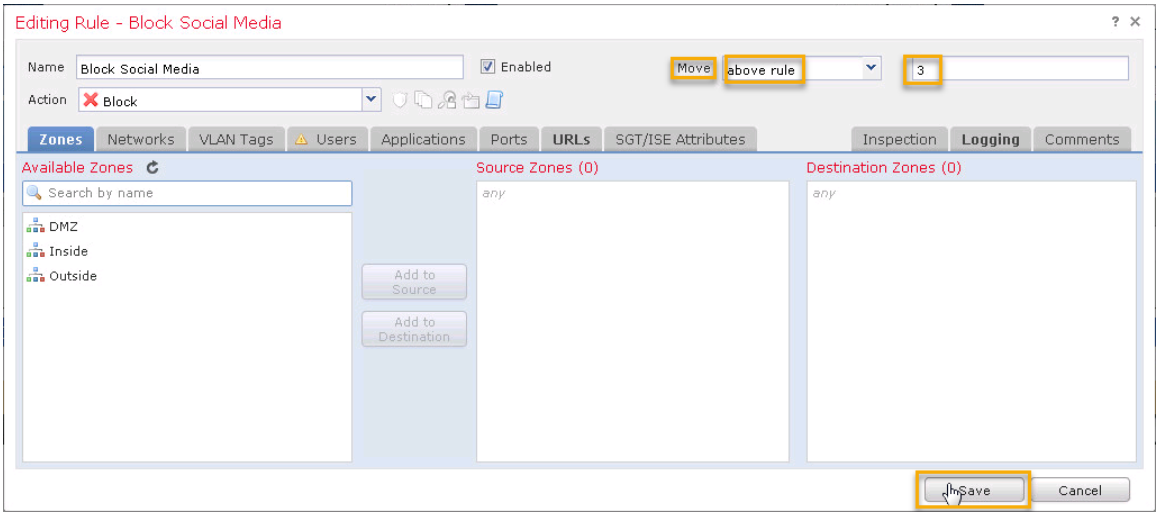
https://t.me/learningnets

131. 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.

132. Click **Save** to save this rule.

Figure 278. Move and Save rule



133. 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 279. Check rule order



134. Click **Save**, **Deploy**, select **all the devices** and click **Deploy**.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

135. 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 280. Access from hq-wkst works

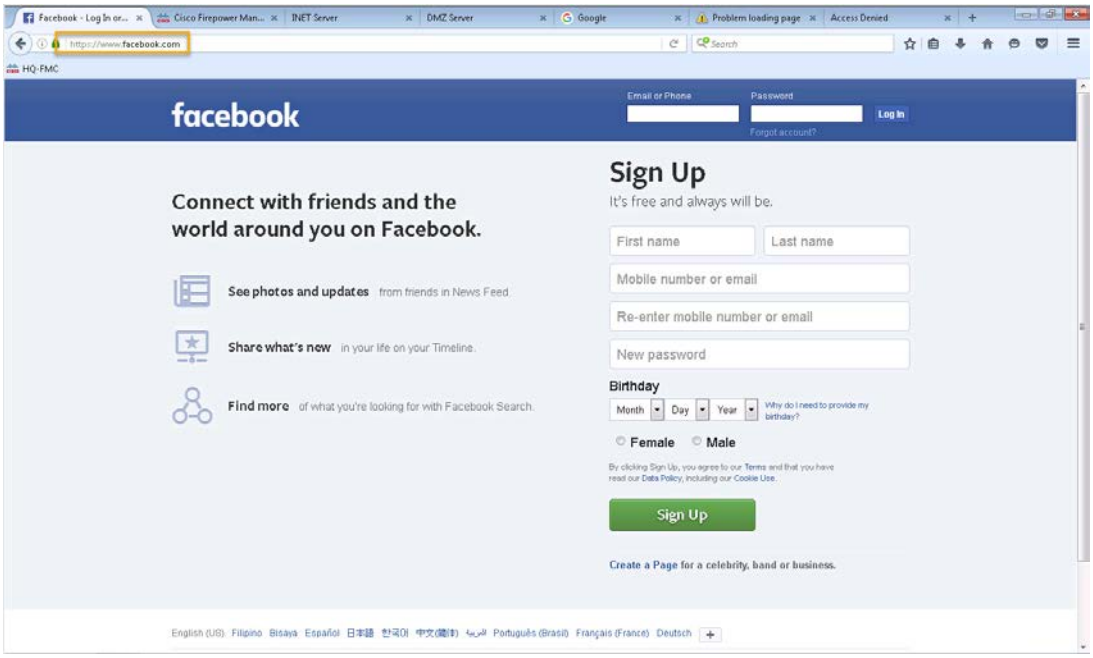
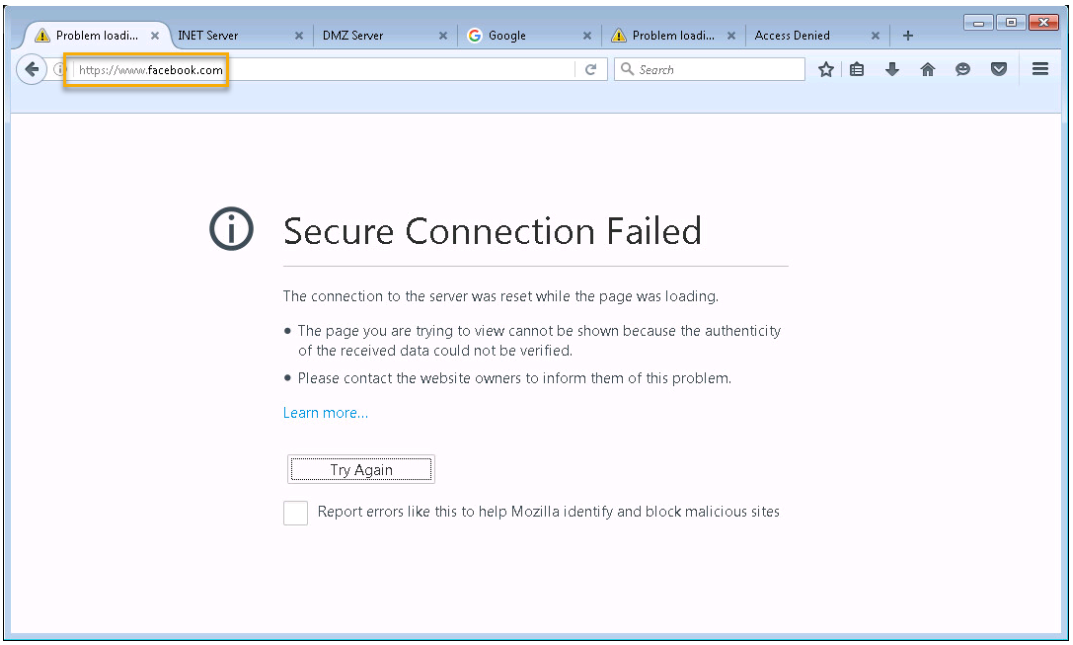


Figure 281. Access from remote1-wkst fails



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.)

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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).

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

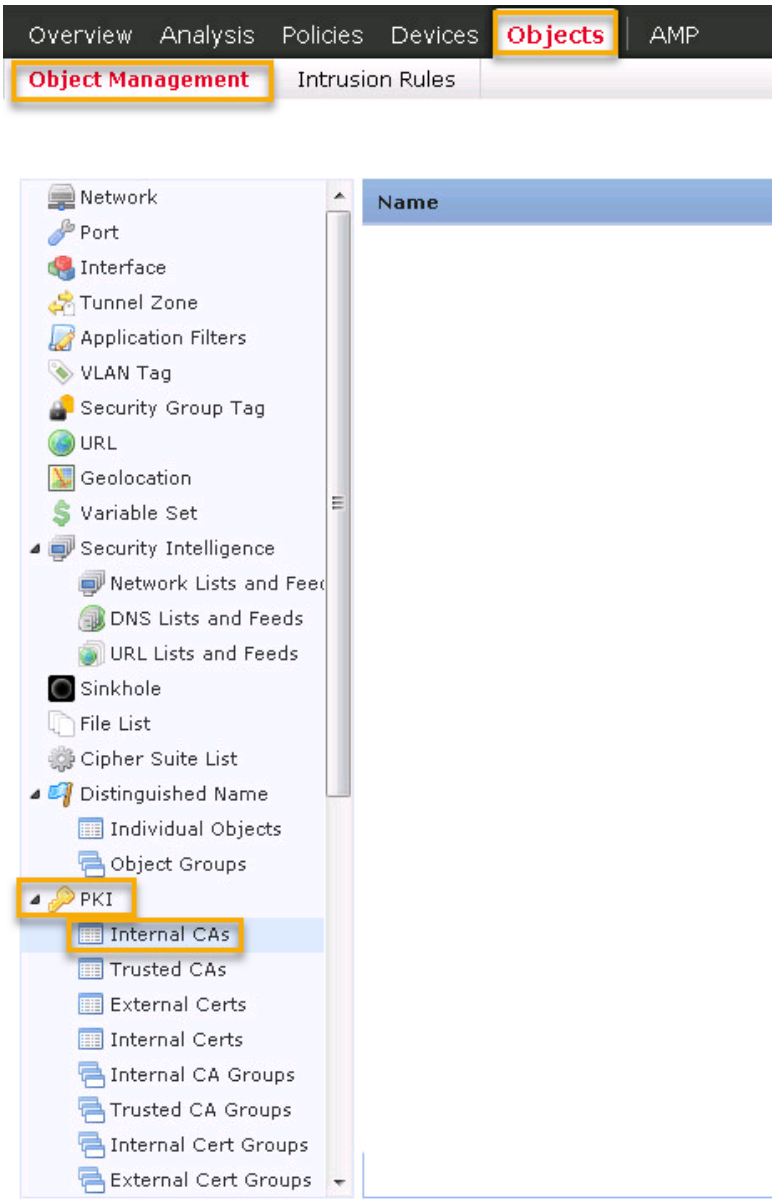
Configure and Apply an SSL Policy

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.

136. In the FMC, navigate to **Objects > Object Management** section of the FMC website.

137. Select expand the **PKI option** from the left menu and select **Internal CAs**.

Figure 282. Navigate to Internal CAs



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

138. Click **Generate CA** and fill out the following:

    a. Name: **FMC_AS_A_CA**

    b. Country: **US**

    c. State: **ID**

    d. City: **Kimberly**

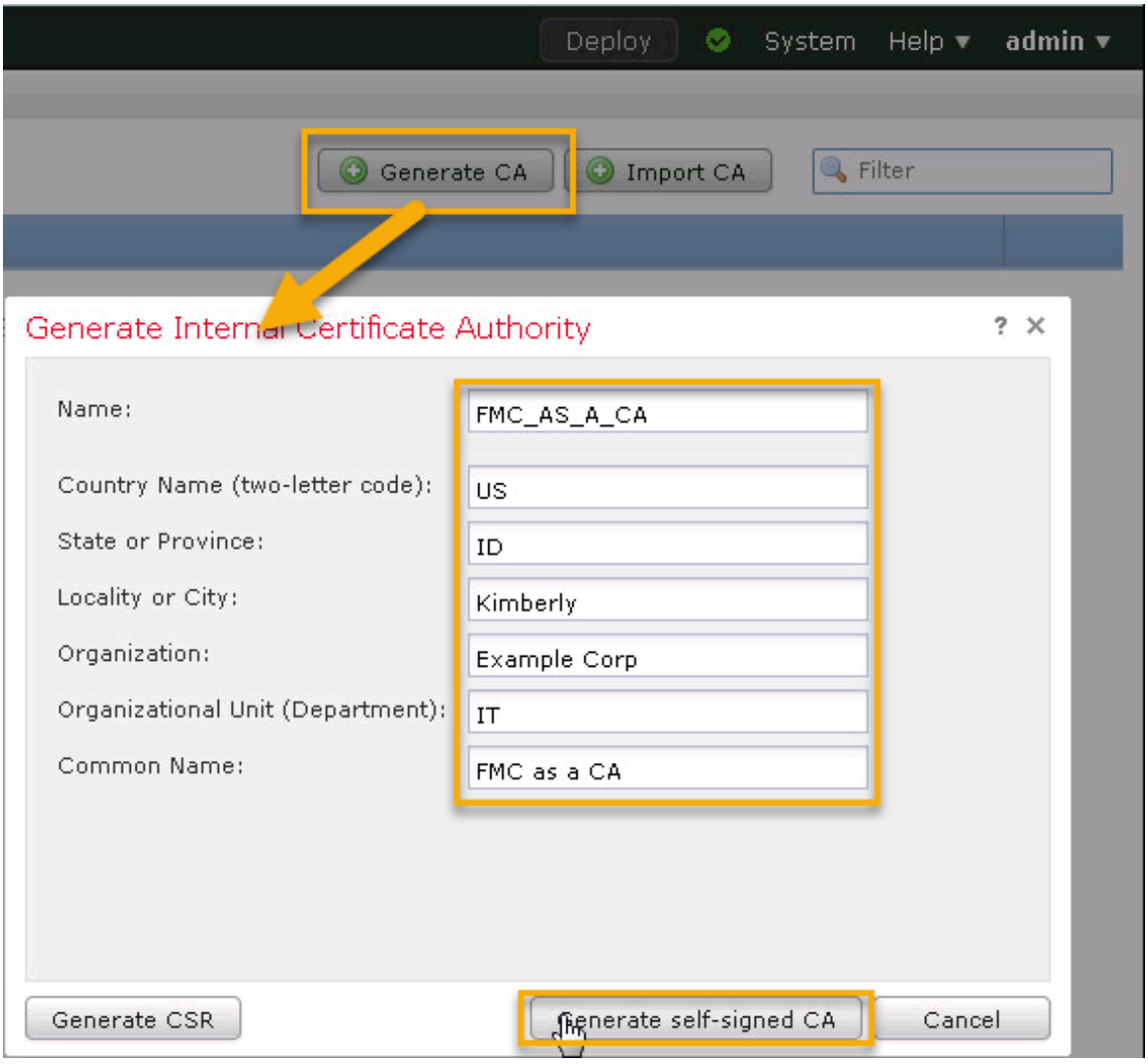
    e. Org: **Example Corp**

    f. Dept: **IT**

    g. Common Name: **FMC as a CA**

139. Click **Generate self-signed CA**

Figure 283. Create CA



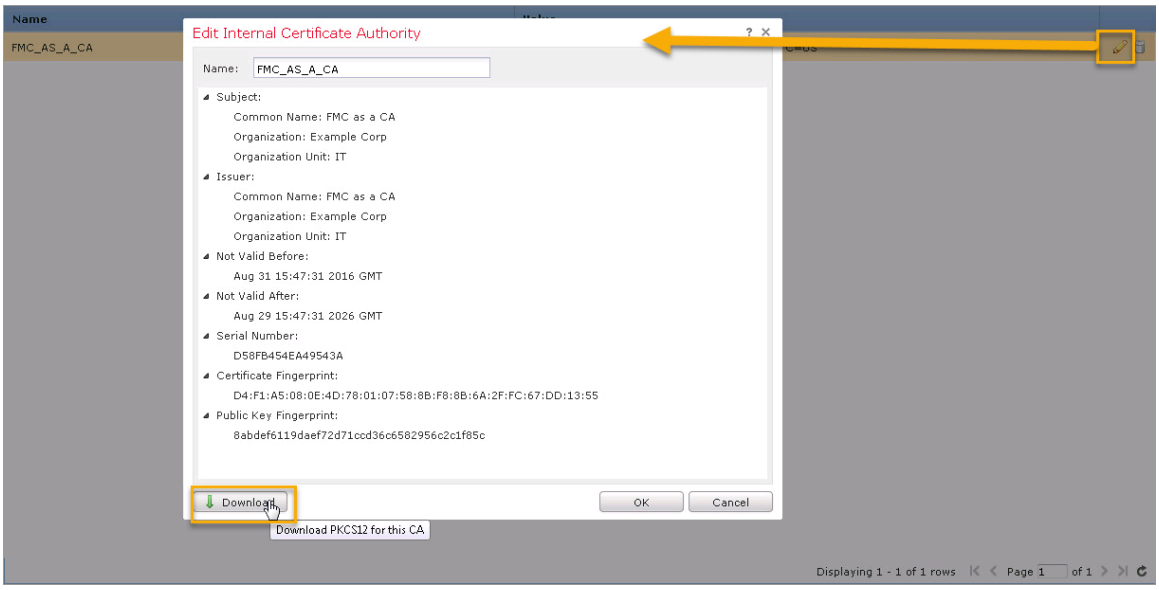
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

140. **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.

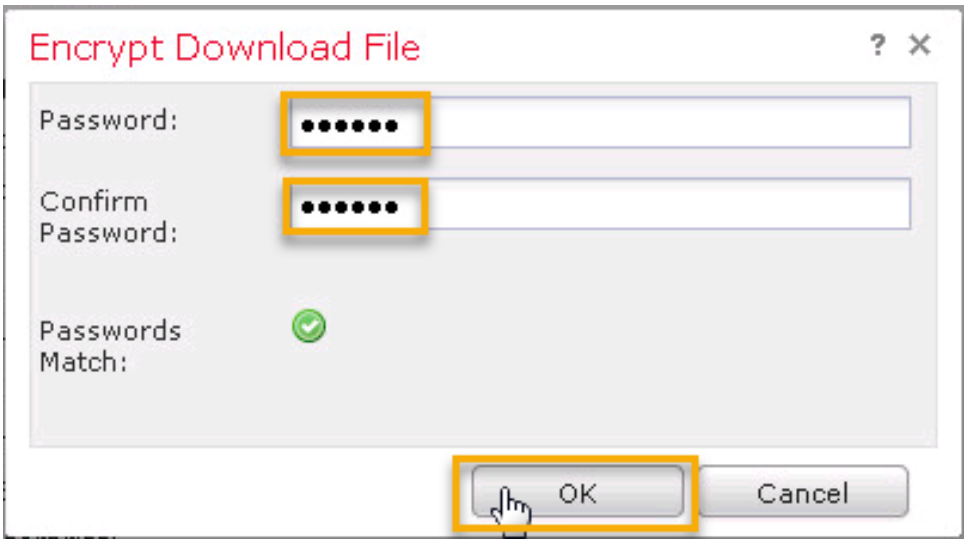
141. Click **Download** to download a copy of this certificate.

Figure 284. Download CA to hq-wkst



142. 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 285. Create password

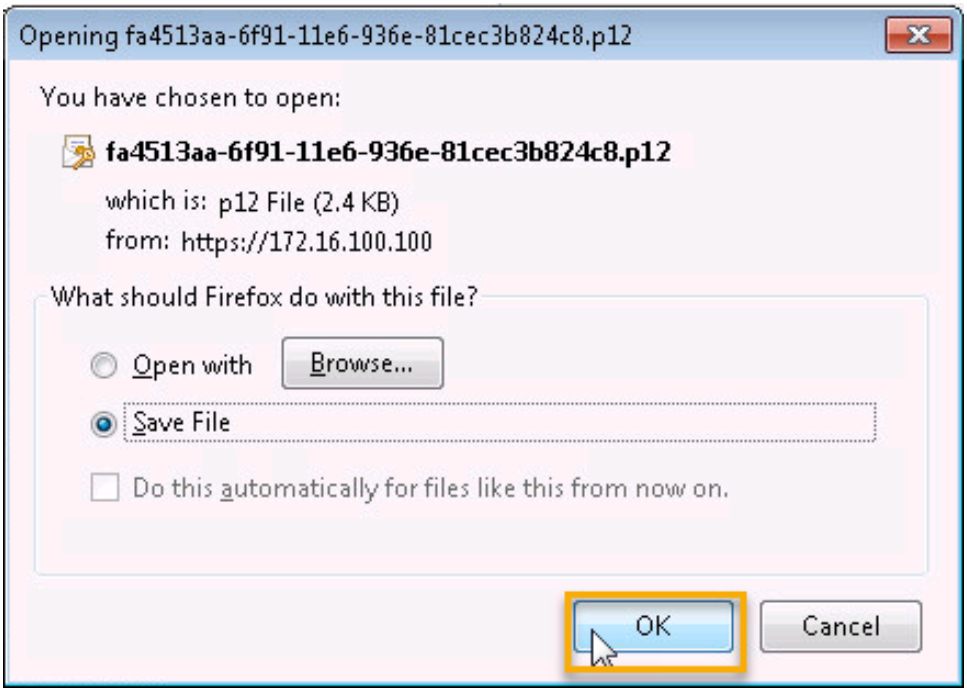


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

143.When prompted, click **OK** to save the file. This will put it in the Downloads directory.

Figure 286. Save CA

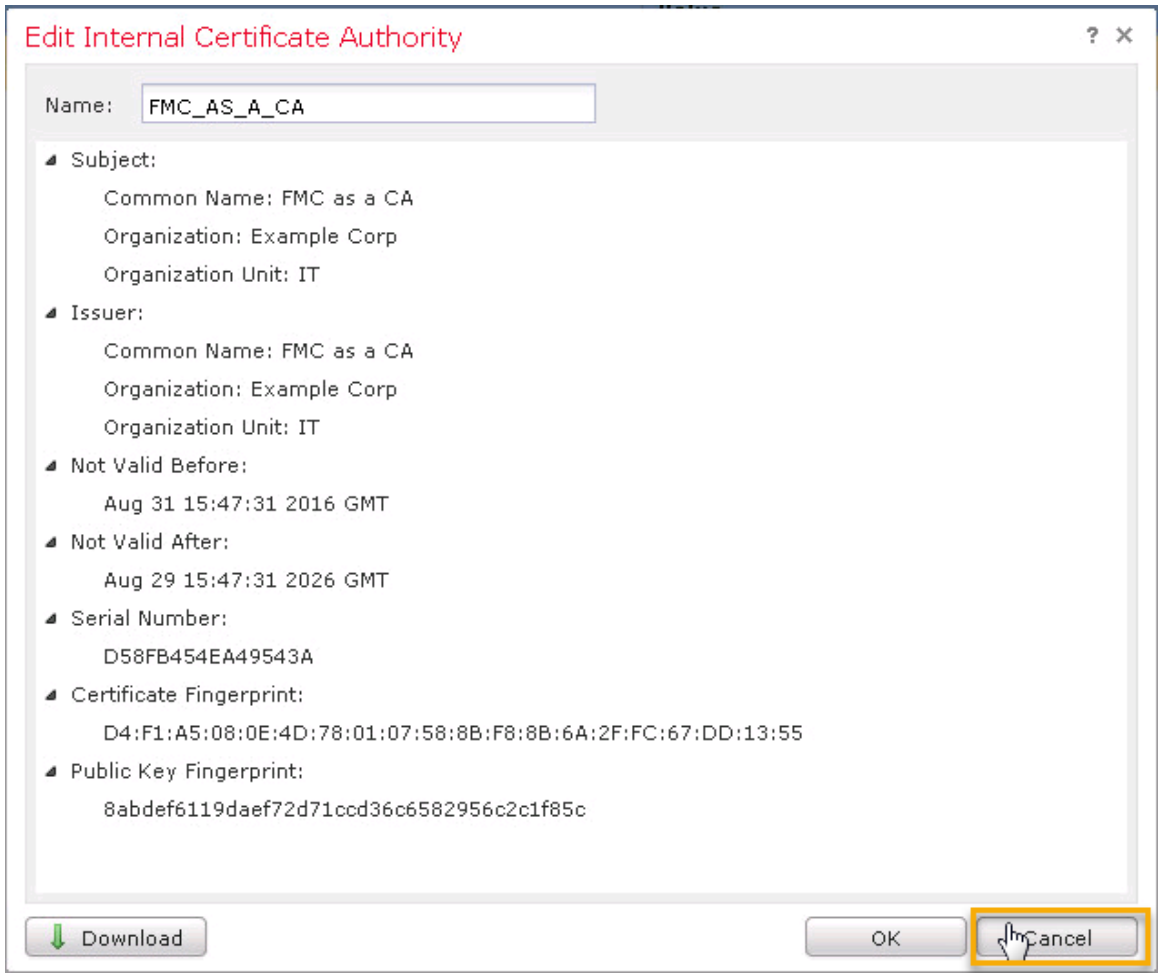


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

144.Click **Cancel** to exit editing the CA.

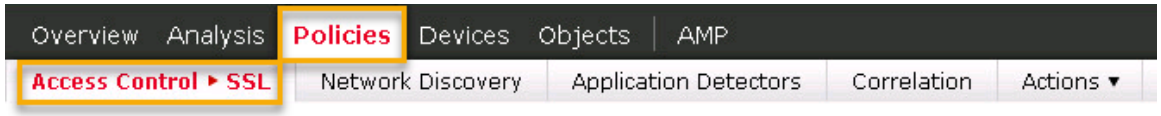
Figure 287. Cancel edit of CA



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.

145.Navigate to **Policies > Access Control > SSL**.

Figure 288. Navigate to SSL Policy



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

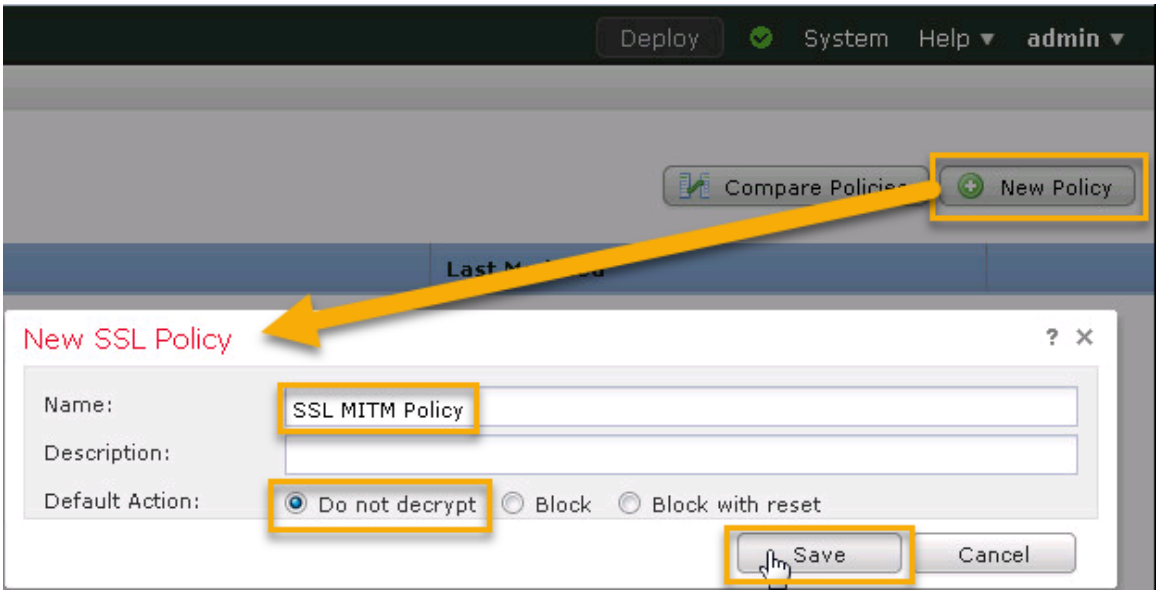
146. Click **New Policy** and fill out the following:

a. Name: **SSL MITM Policy**

b. Default Action: **Do not decrypt**

c. Click **Save**.

Figure 289. Create new policy



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

147. 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**

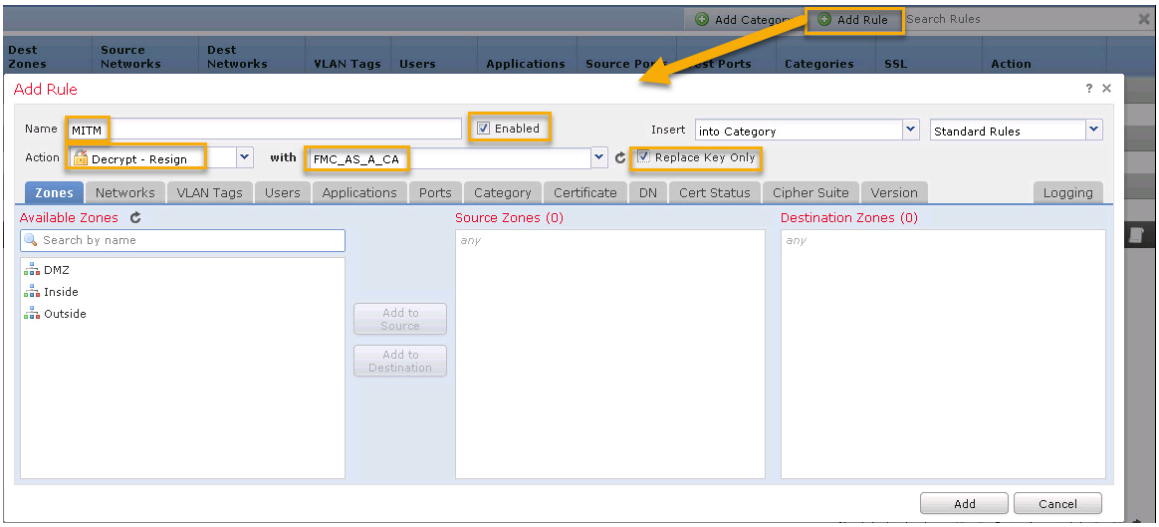
    b. Enabled: **Checked**

    c. Action: **Decrypt – Resign**

    d. With: **FMC_AS_A_CA**

    e. Replace Key Only: **Checked**

Figure 290. Part 1 of adding rule

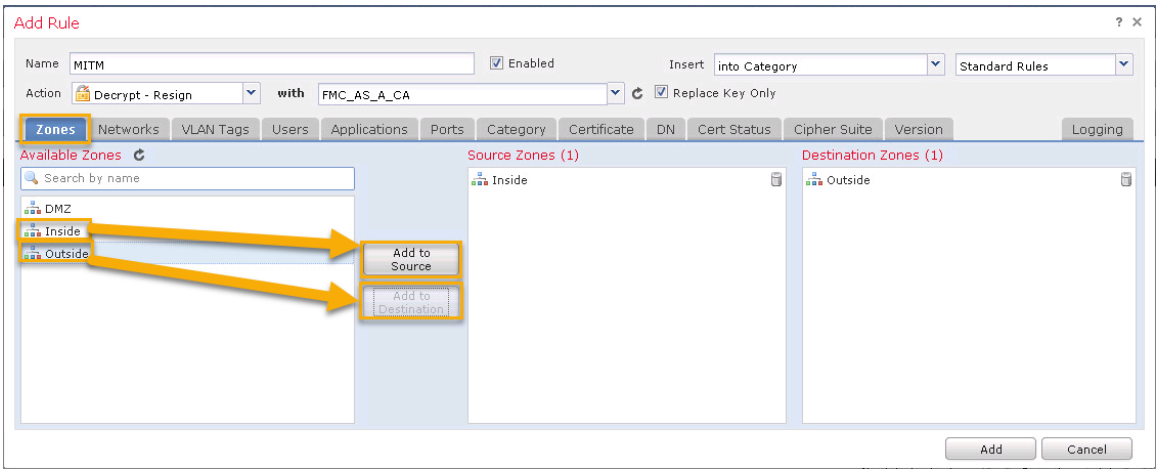


148. On **Zones tab**:

    a. Source Zones: **Inside**

    b. Destination Zones: **Outside**

Figure 291. Configure Zones tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

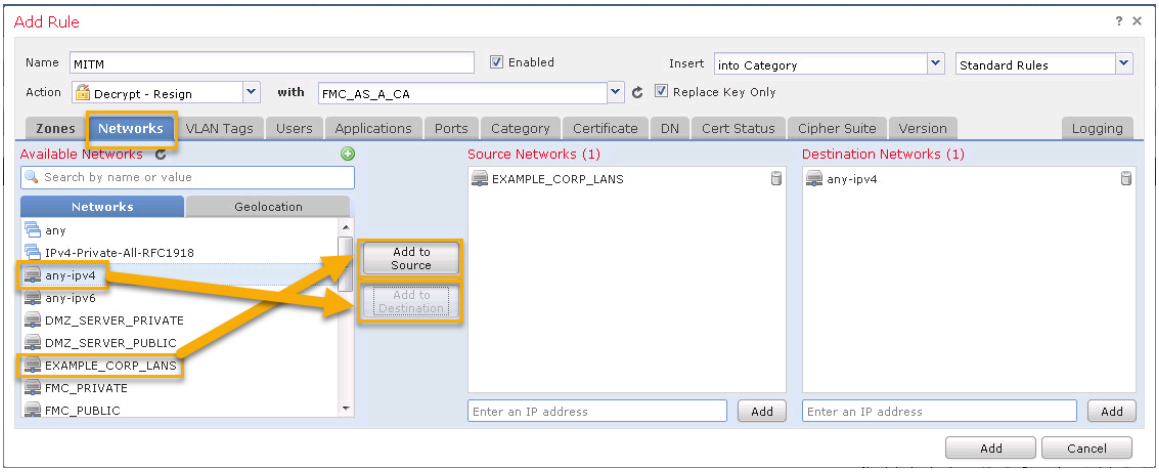
https://t.me/learningnets

149. On **Networks tab**:

    a. Source: **EXAMPLE_CORP_LANS**

    b. Destination: **any-ipv4**

Figure 292. Configure Networks tab



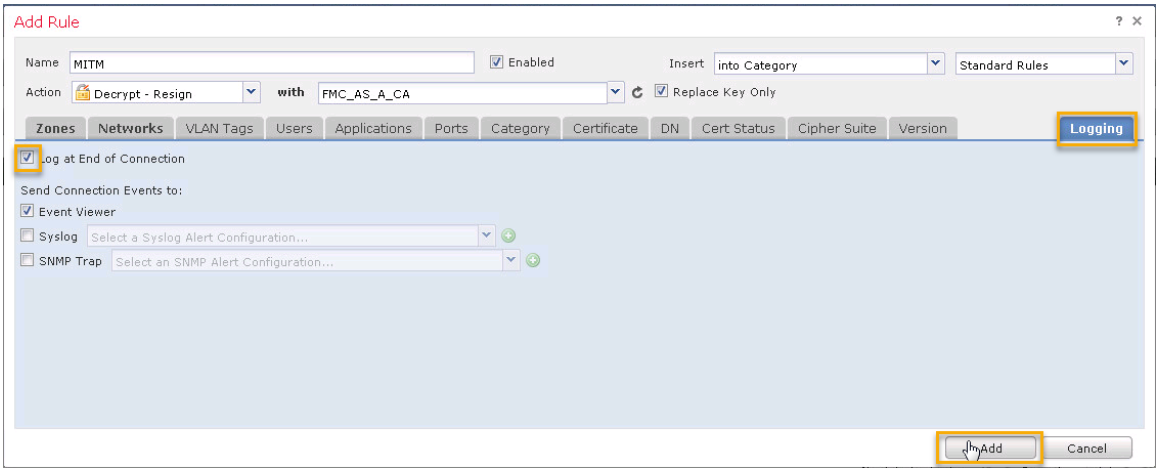
150. On the **Logging tab**:

    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.

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

Figure 293. Configure Logging tab and Add rule



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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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).

152. Click **Add Rule** to being the creation of this new rule. Use the following to fill out the popup window:

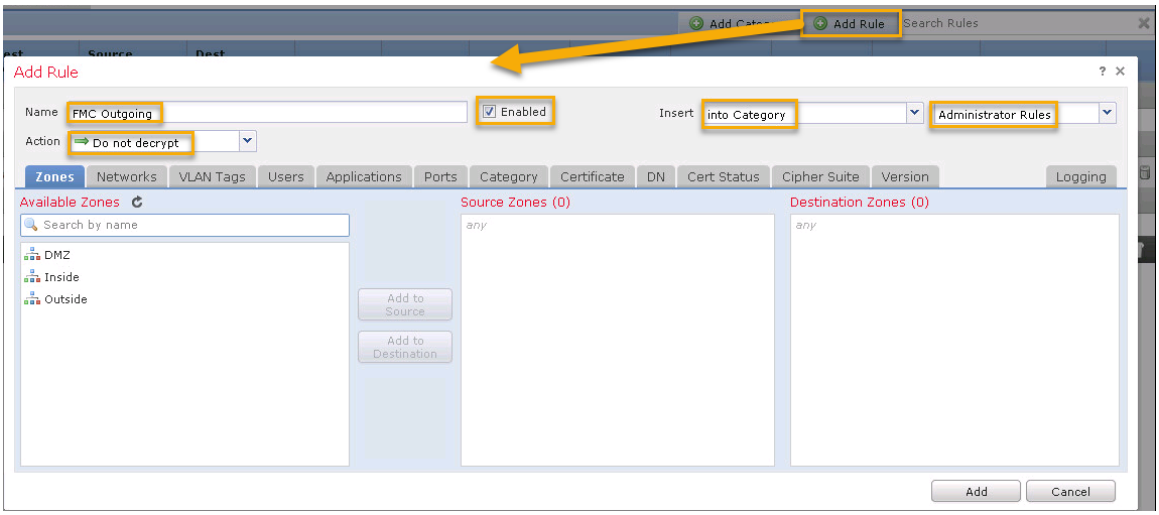
    a. Name: **FMC Outgoing**

    b. Enabled: **Checked**

    c. Insert: **into Category** and then **Administrator Rules**

    d. Action: **Do not decrypt**

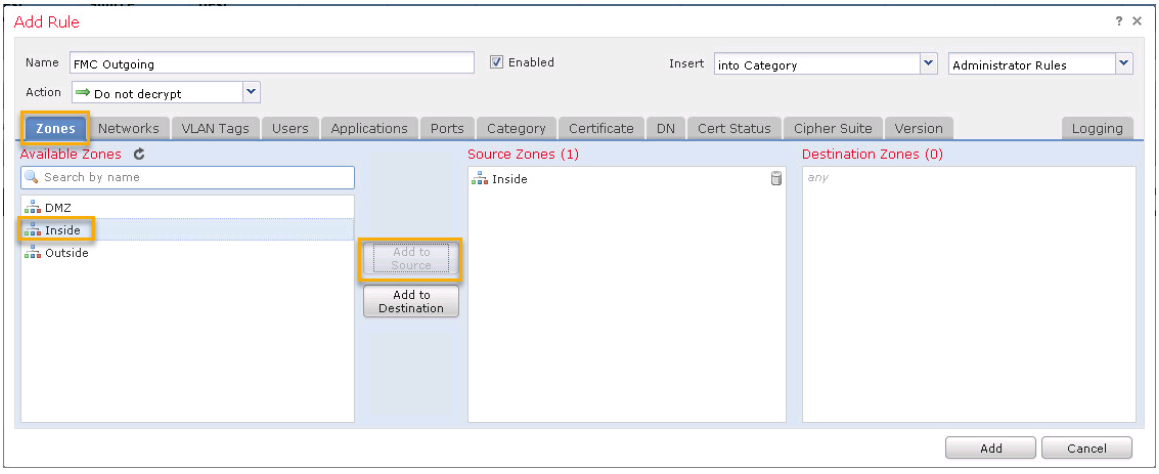
Figure 294. Part 1 adding new rule



153. On the **Zones tab**:

    a. Source Zones: **Inside**

Figure 295. Configure Zones tab



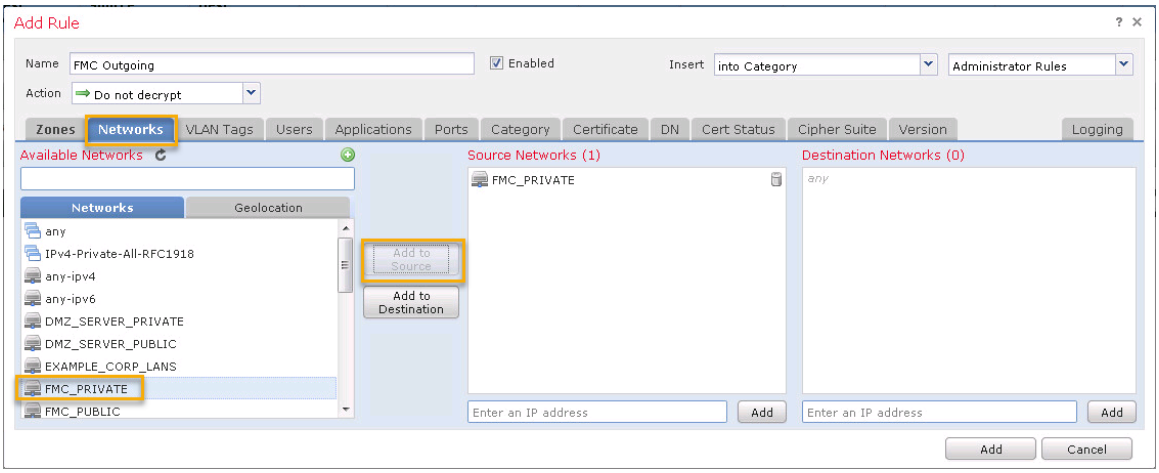
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

154. On the **Networks tab**:

    a. Source Networks: **FMC_PRIVATE**

Figure 296. Configure Networks tab

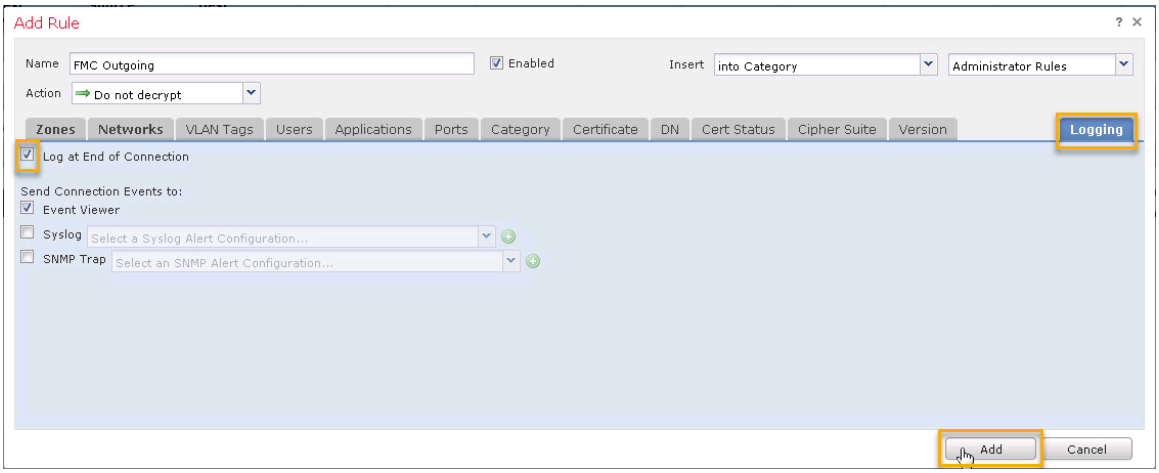


155. On the **Logging tab**:

    a. **Log at the End of Connection** is checked.

156. Click **Add**.

Figure 297. Configure Logging and Add rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

157. Click **Add Rule** again to create identify traffic coming the other direction. Use the following to fill out the popup window:

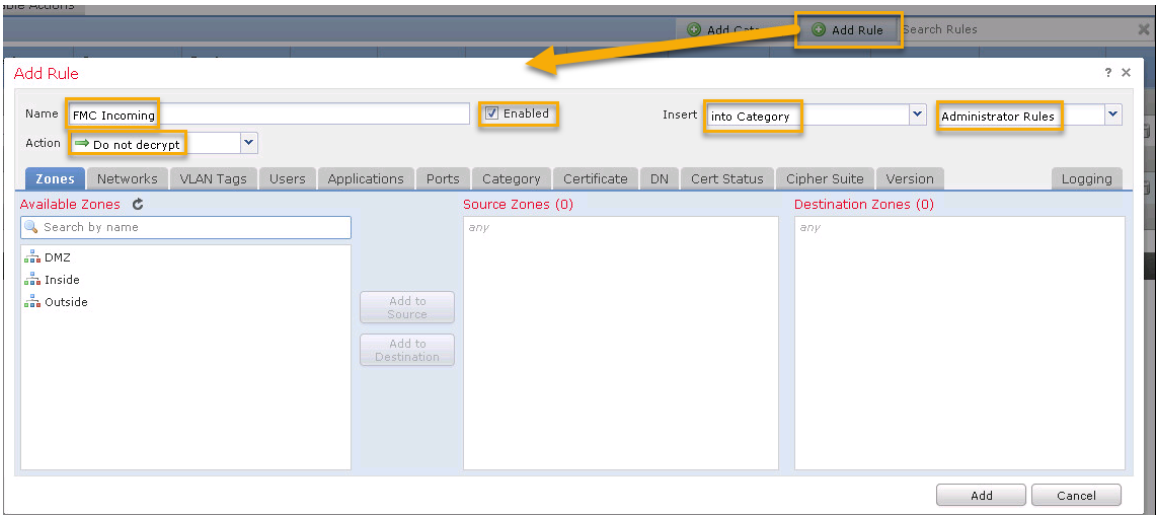
    a. Name: **FMC Incoming**

    b. Enabled: **Checked**

    c. Insert: **into Category** and then **Administrator Rules**

    d. Action: **Do not decrypt**

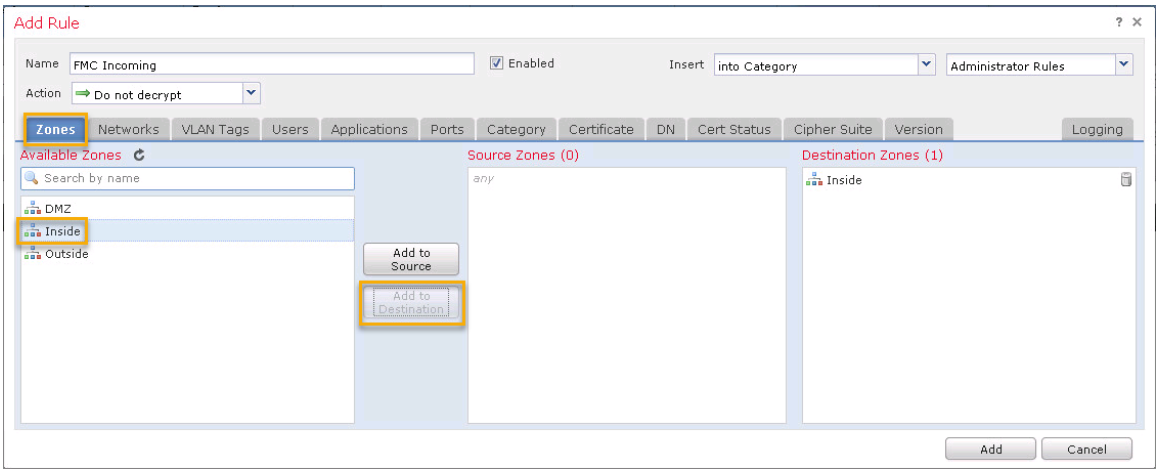
Figure 298. Add another rule



158. On the **Zones tab**:

    a. Destination Zones: **Inside**

Figure 299. Configure Zones tab



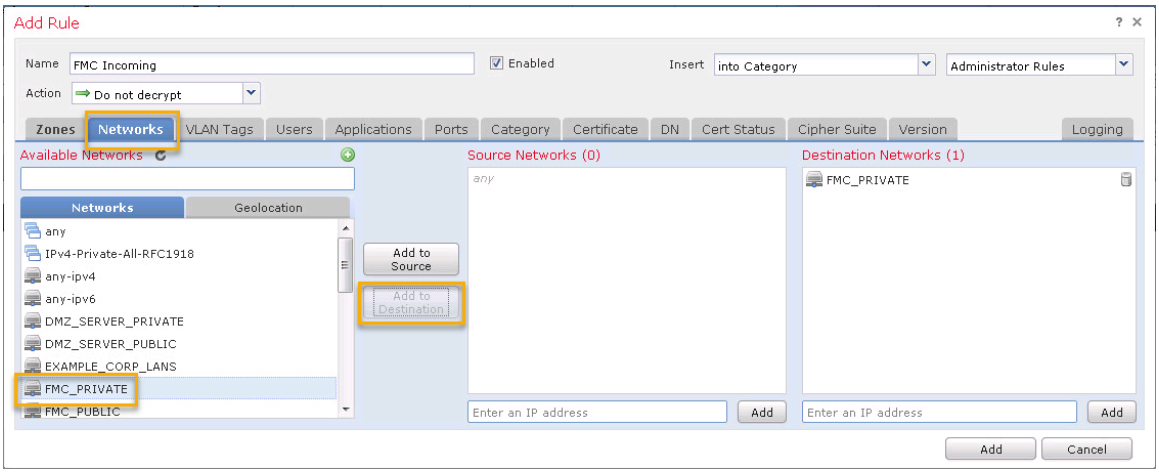
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

159. On the **Networks tab**:

    a. Destination Networks: **FMC_PRIVATE**

Figure 300. Configure Networks tab

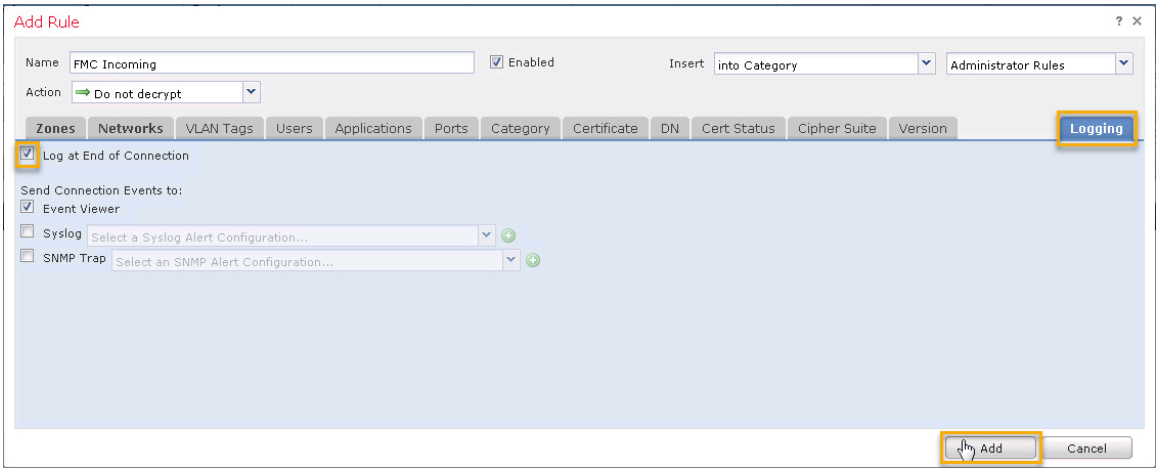


160. On the **Logging tab**:

    a. **Log at the End of Connection** is checked.

161. Click **Add**.

Figure 301. Configure Logging tab and add rule



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

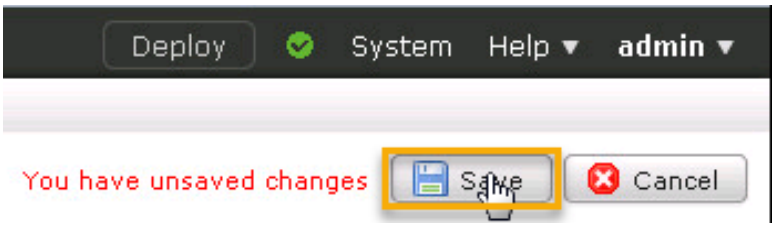
https://t.me/learningnets

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. Bug ID is “blah”.

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.

162. Click **Save**.

Figure 302. Save changes to FMC



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.

163. Navigate to **Policies > Access Control > Access Control**.

164. **Edit** the **Base Policy**.

Figure 303. Edit Base Policy ACP



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

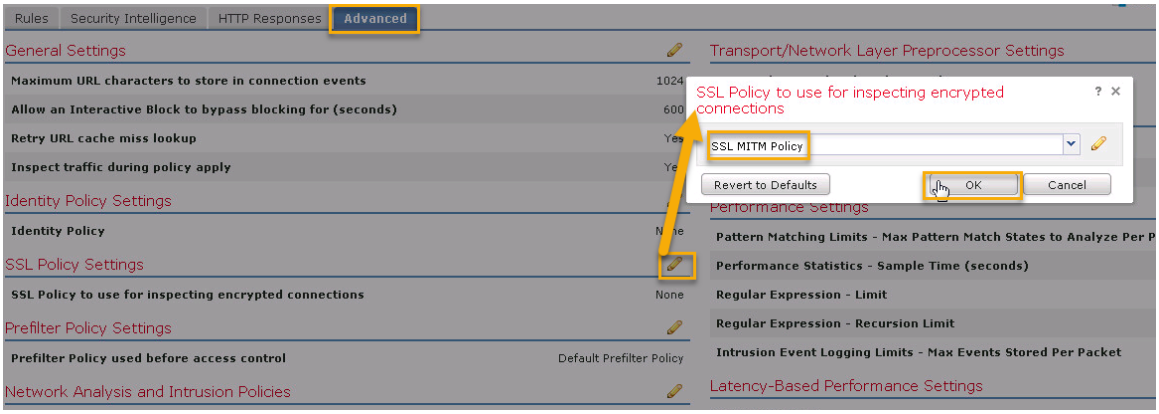
165. Click the **Advanced tab**.

166. 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 304. Apply SSL Policy to ACP



167. Click **Save** and then **Deploy**. Select **all the FTD devices** and click **Deploy**.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

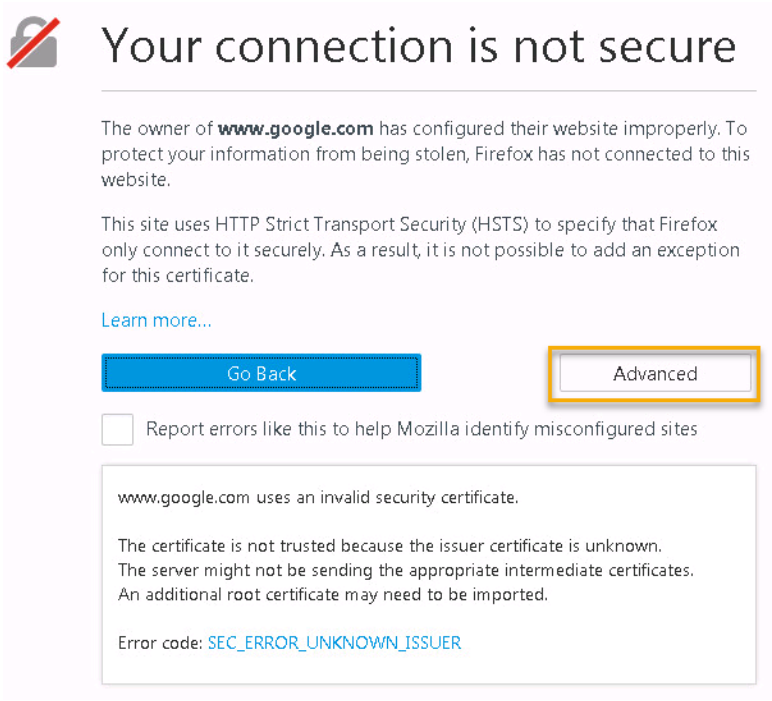
https://t.me/learningnets

Browser Test – Phase 1

Now that the FMC has deployed the SSL Policy to the FTD devices, it is time to test.

168. 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 305. Can't accept the cert



Essentially 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

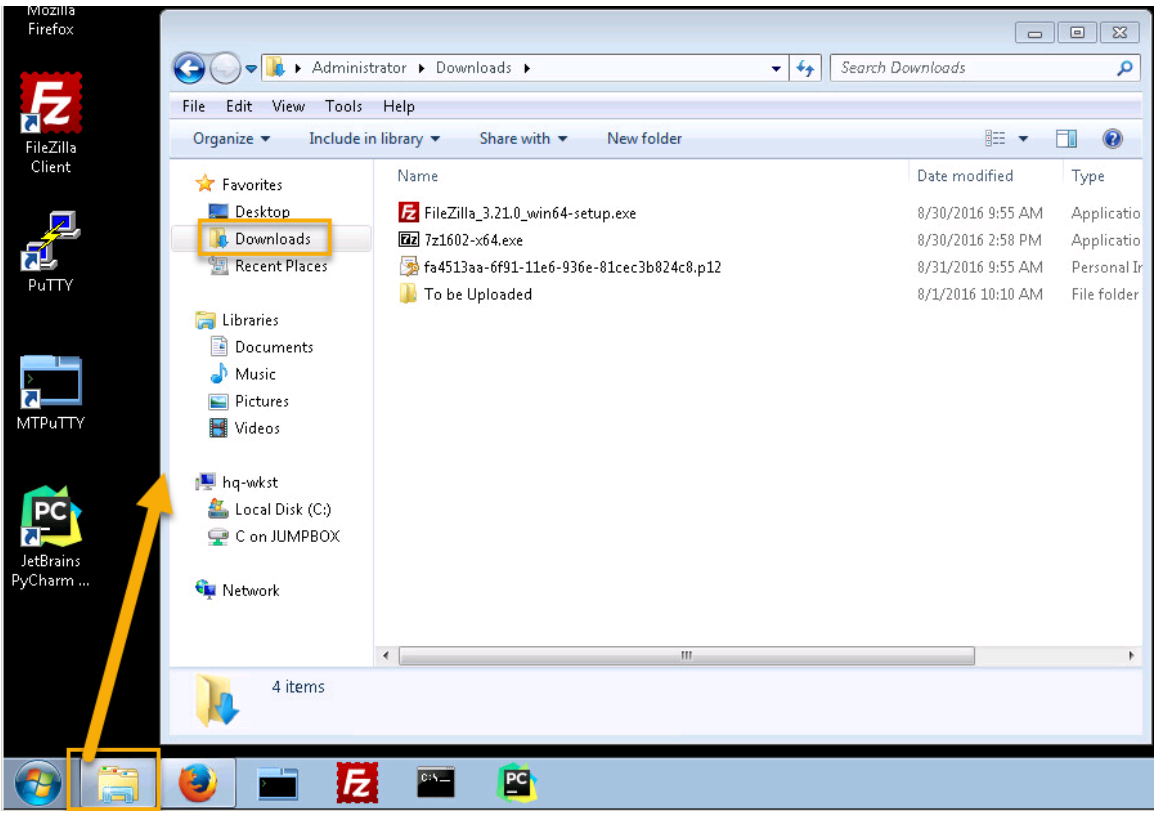
https://t.me/learningnets

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".

169. 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 306. Go to Download directory

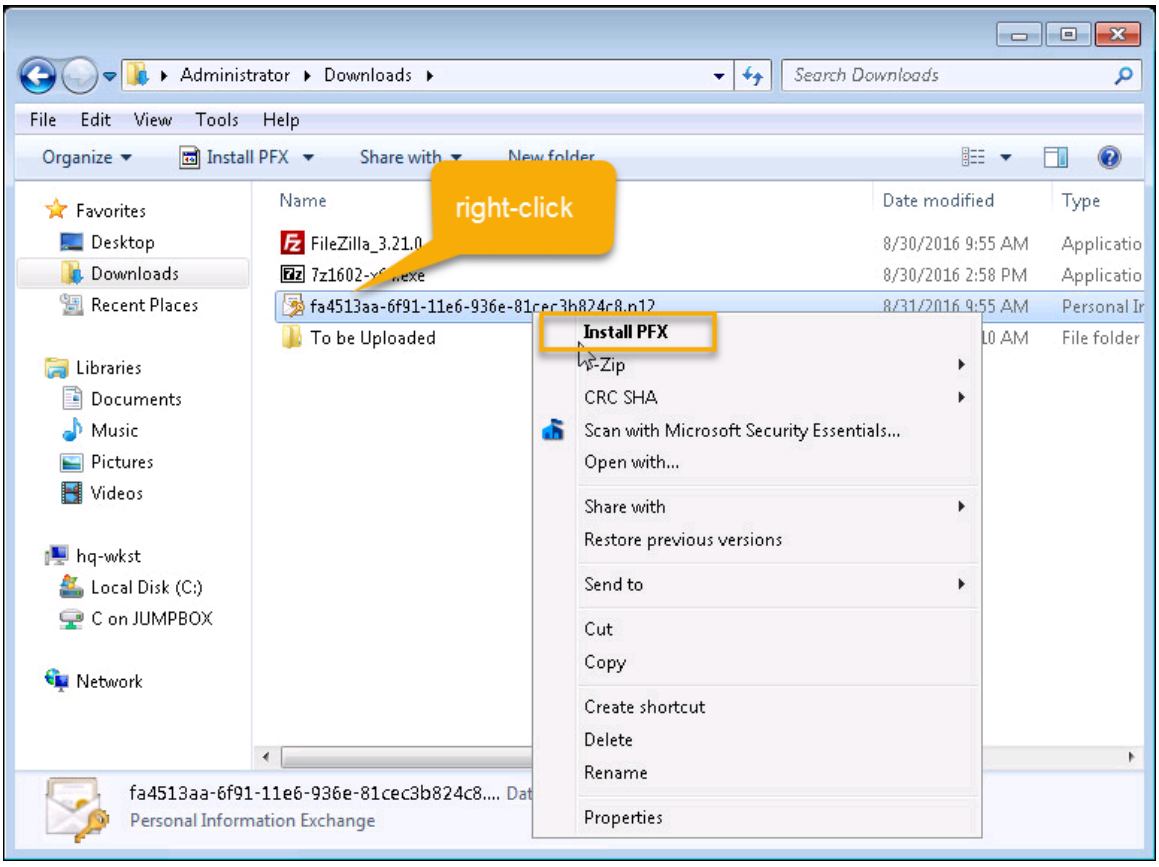


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

170. **Right-click** on the file and select **Install PFX**.

Figure 307. Install PFX

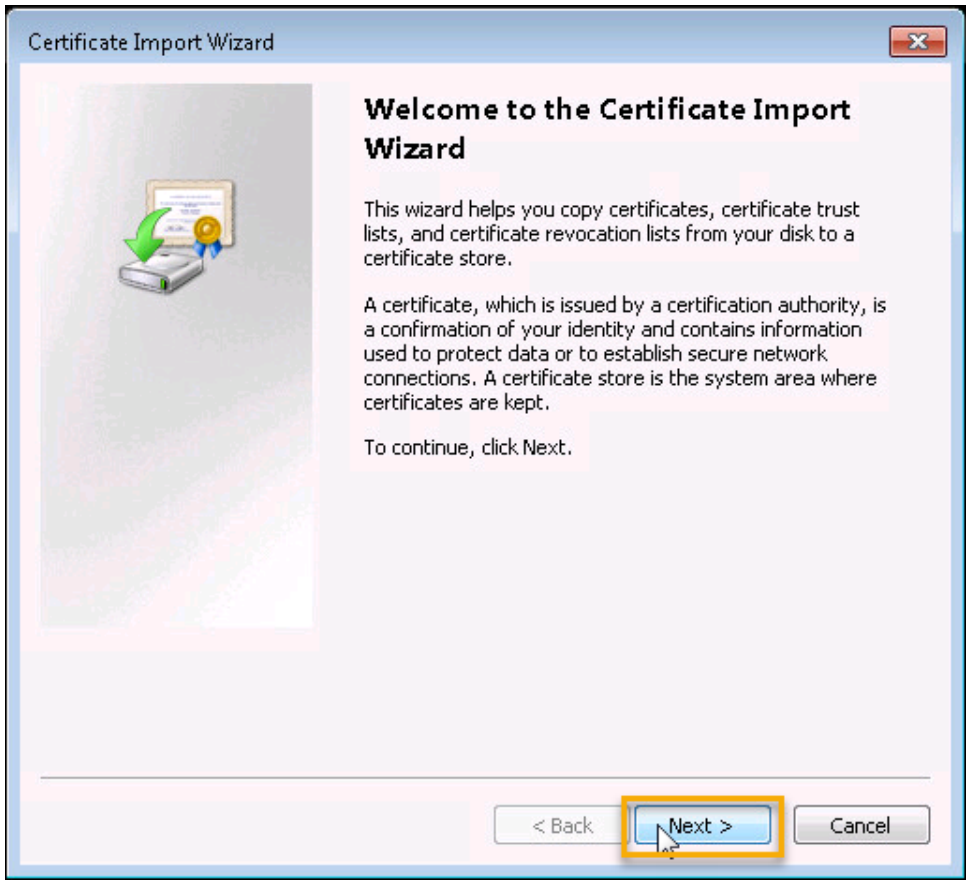


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

171. The Certificate Import Wizard will appear. Click **Next**.

Figure 308. Certificate Import Wizard Page 1

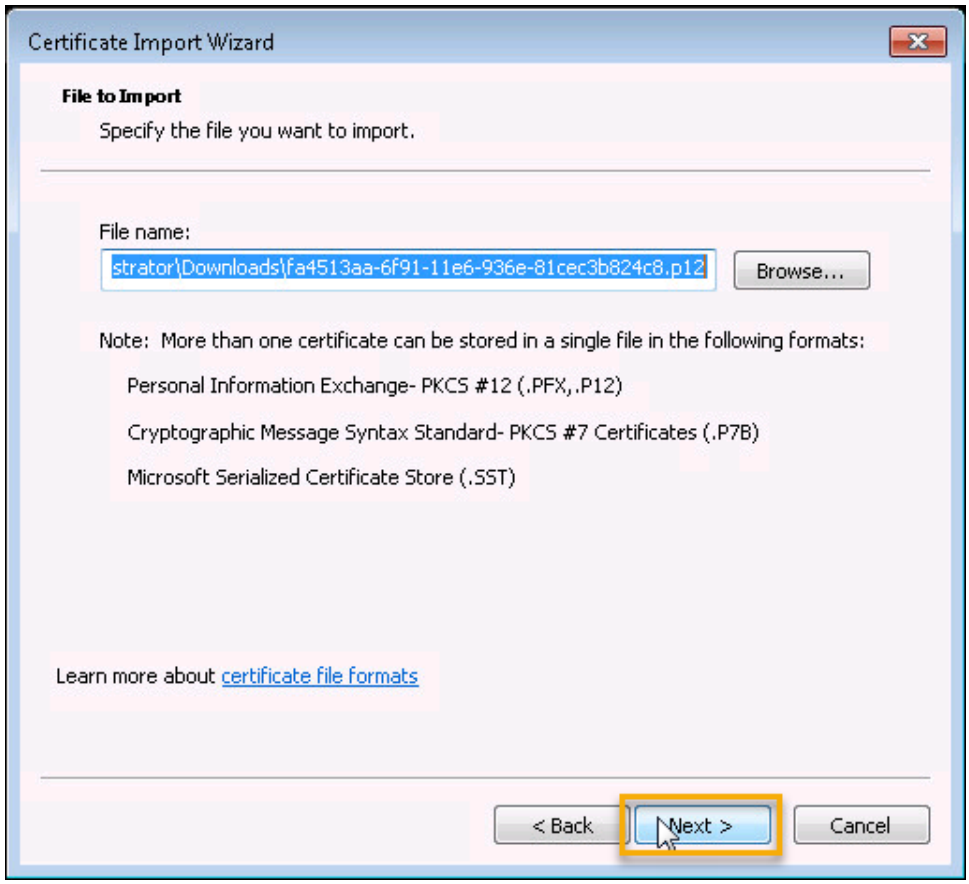


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

172. The File to Import is already populated with your filename. Click **Next**.

Figure 309. Certificate Import Wizard Page 2

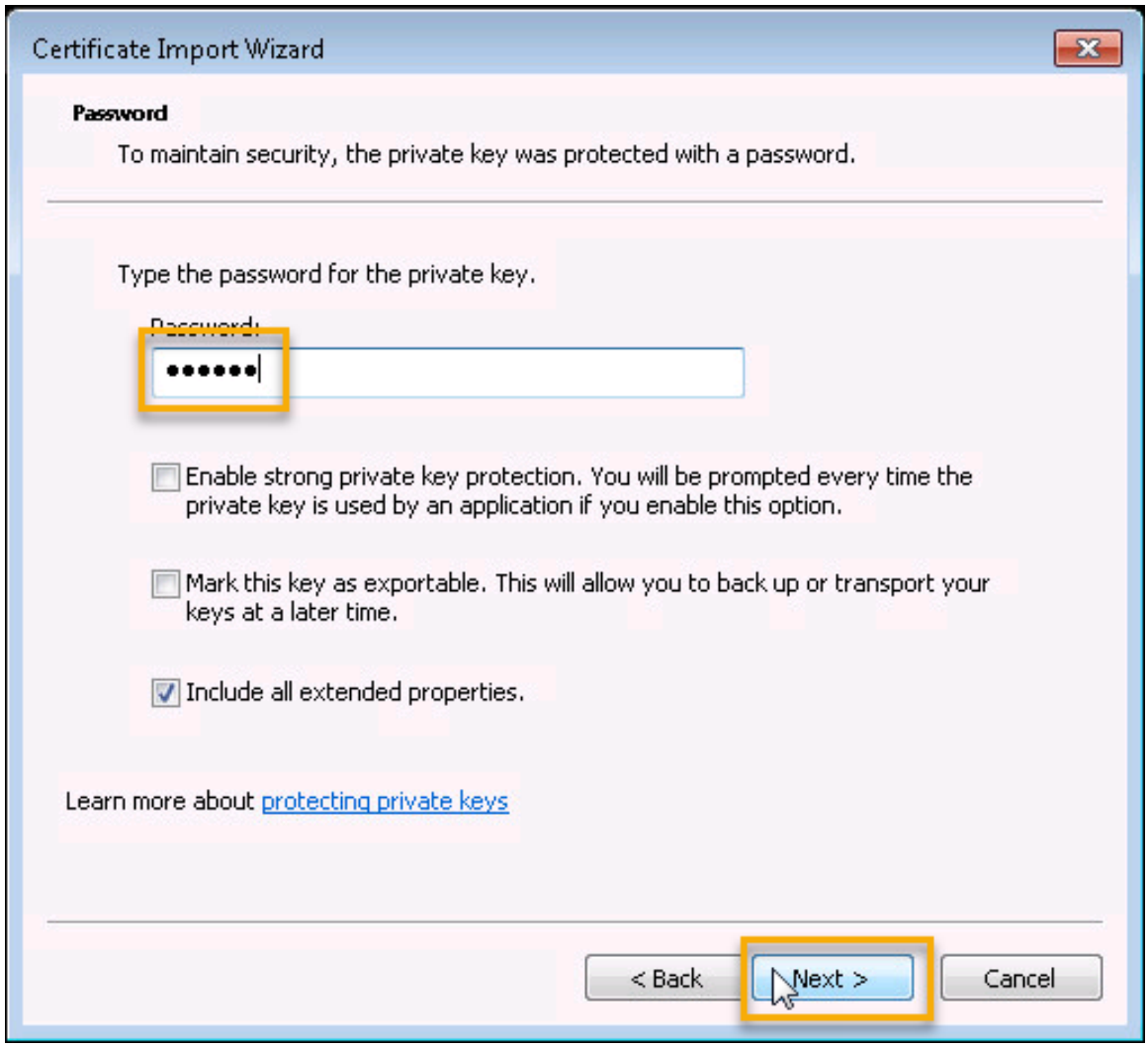


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

173. Type in the password **abc123** to decrypt the certificate. Click **Next**.

Figure 310. Certificate Import Wizard Page 3

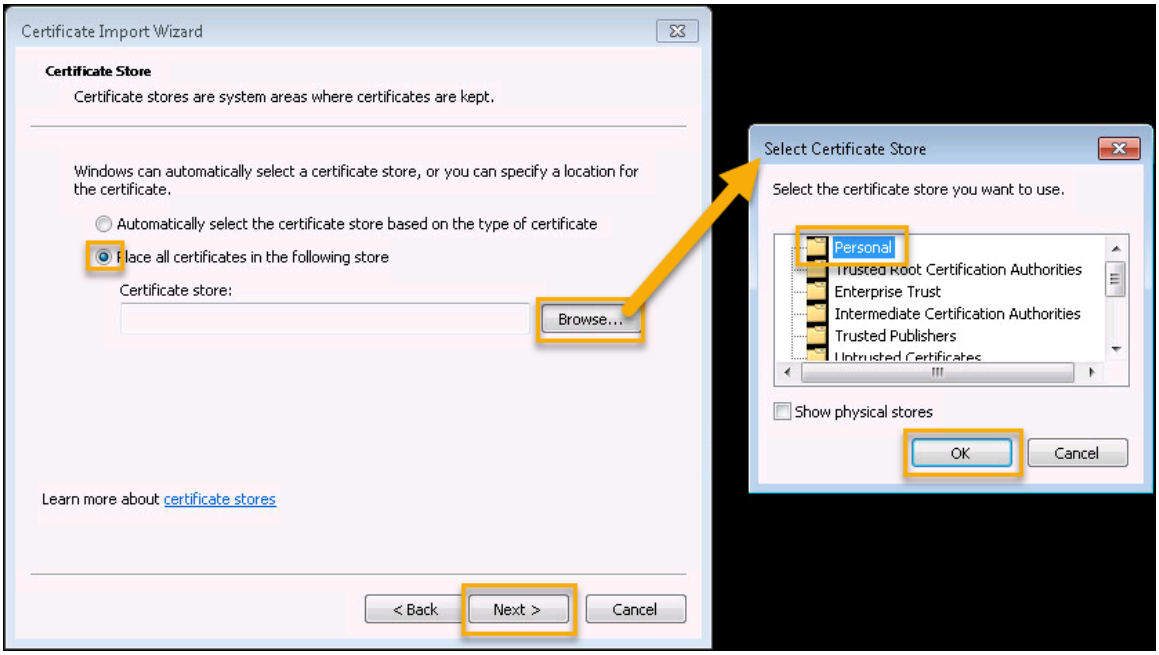


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

174. Select the **Place all certificates in the following store**, click **Browse**, and select the **Personal folder**. Click **OK** and then click **Next**.

Figure 311. Certificate Import Wizard Page 4

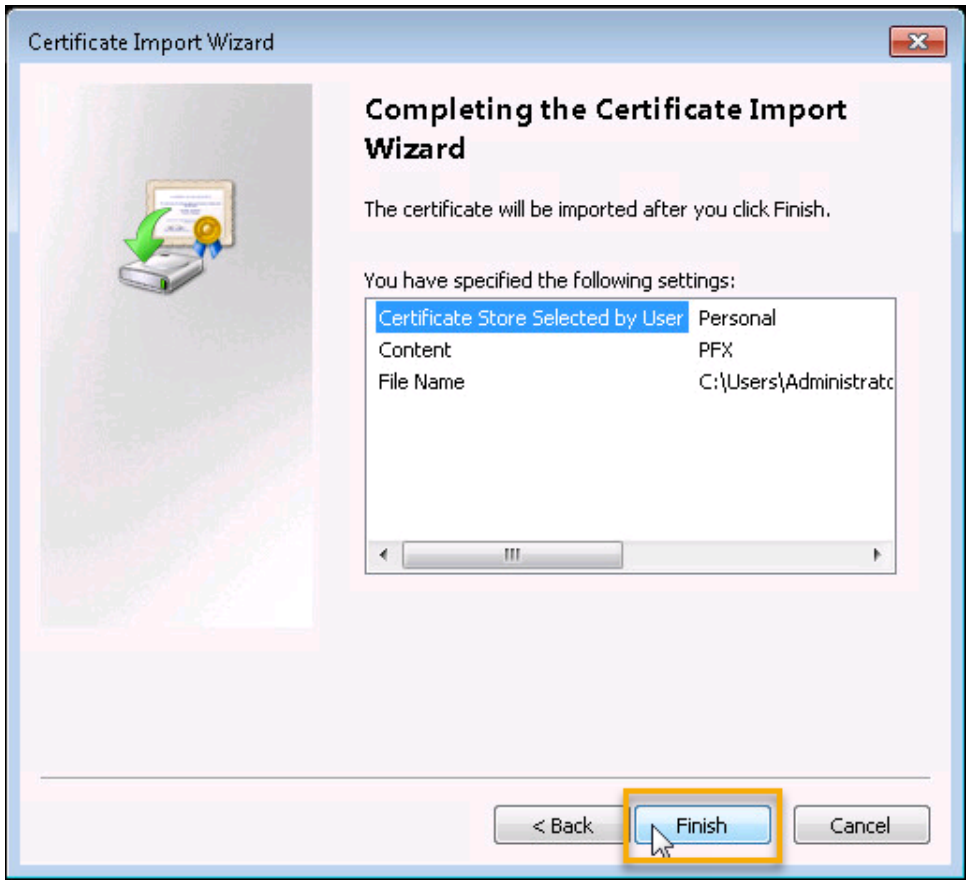


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

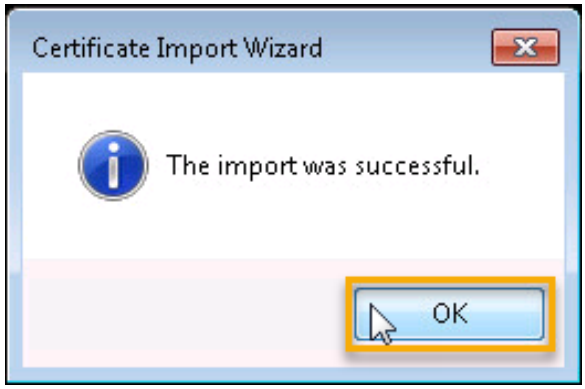
175. Click **Finish** to import the certificate.

Figure 312. Certificate Import Wizard Page 5



176. Click **OK** to the Import Successful message.

Figure 313. Confirm your success



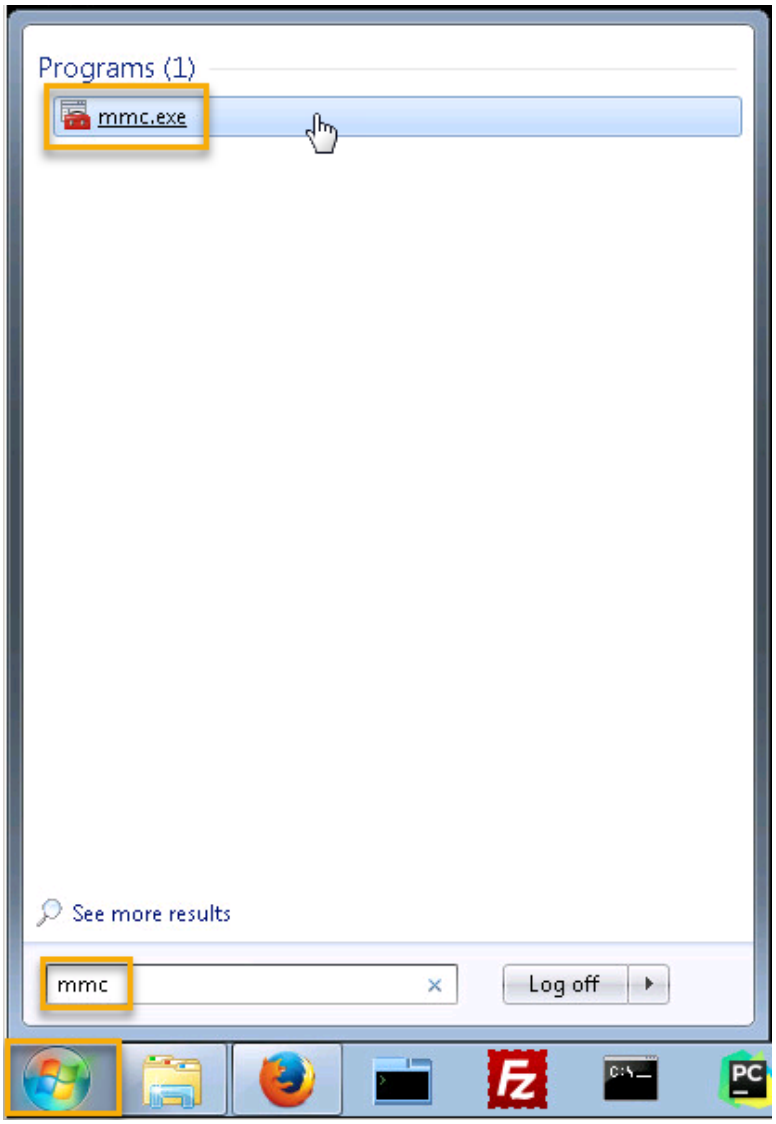
Now that the certificate is installed you need to export a public cert from it to install into your browser:

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

177.Click on **Start** and in the Search box type **mmc**. Click on the **mmc.exe** program that the search finds.

Figure 314. Launch mmc.exe

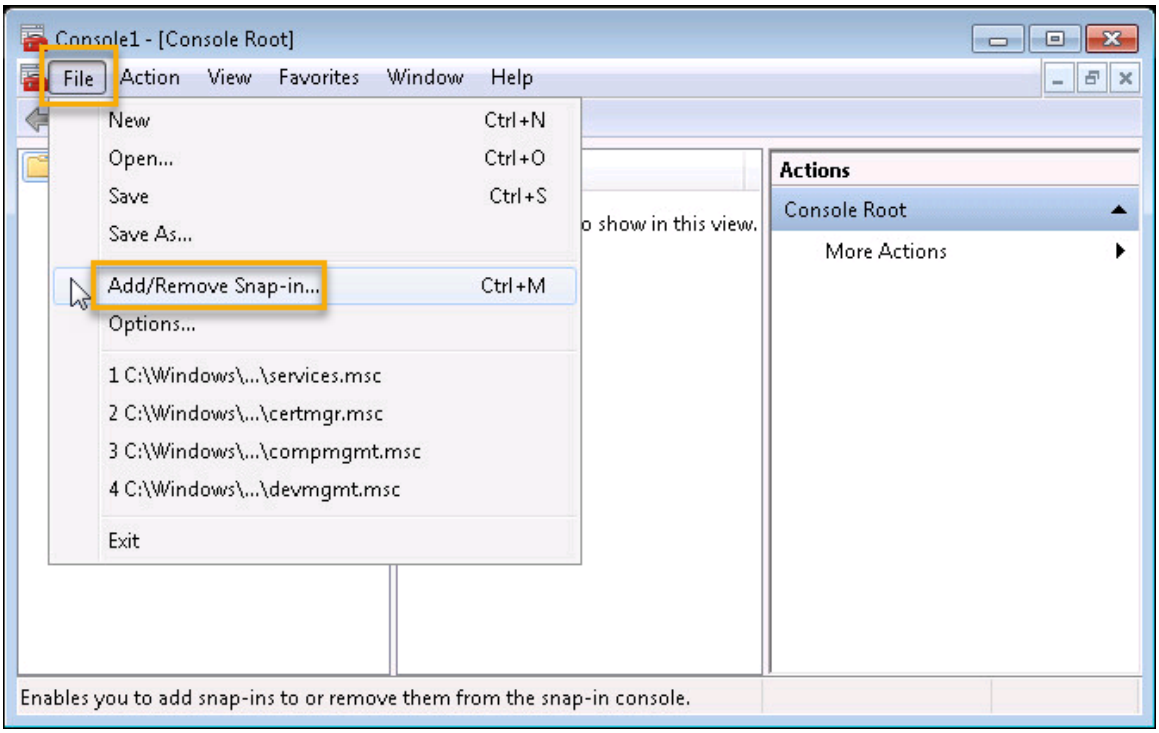


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

178. In the Console1 window click **File > Add/Remove Snap-in**.

Figure 315. Add snap-in

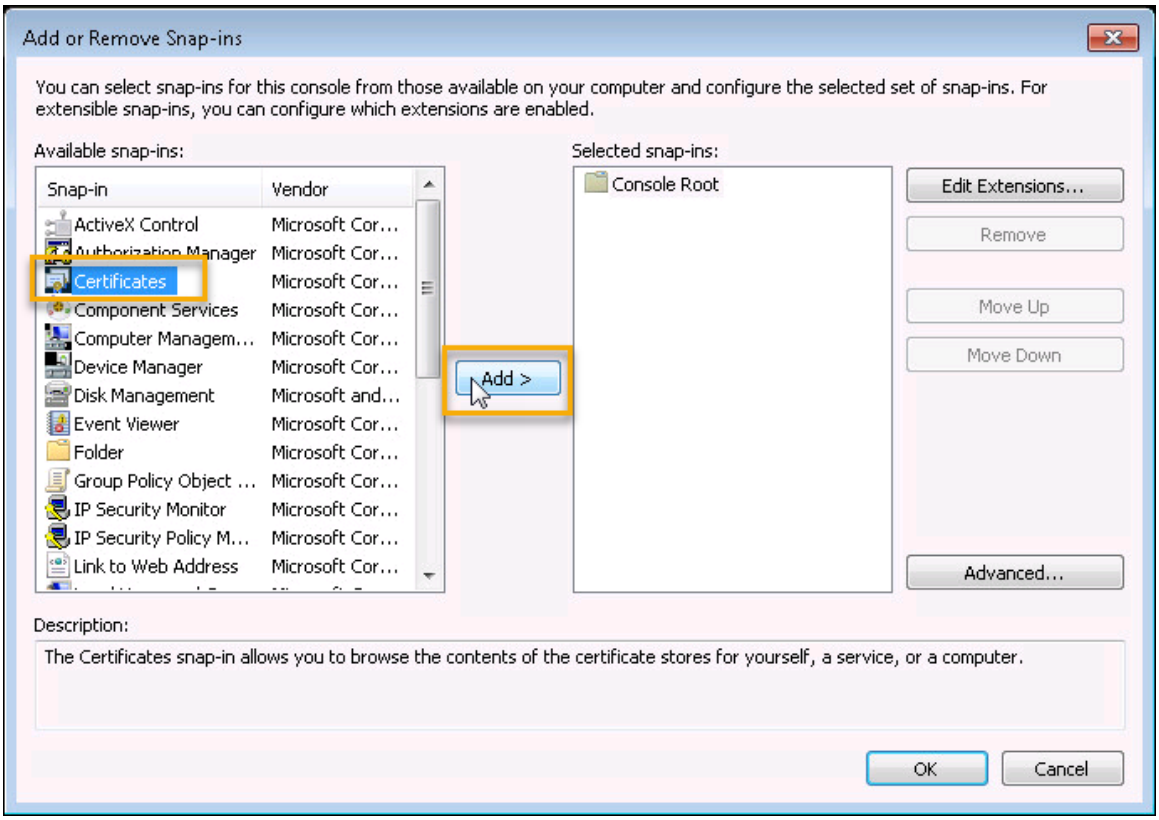


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

179. From the left column select **Certificates** and click **Add>**.

Figure 316. Add Certificates console

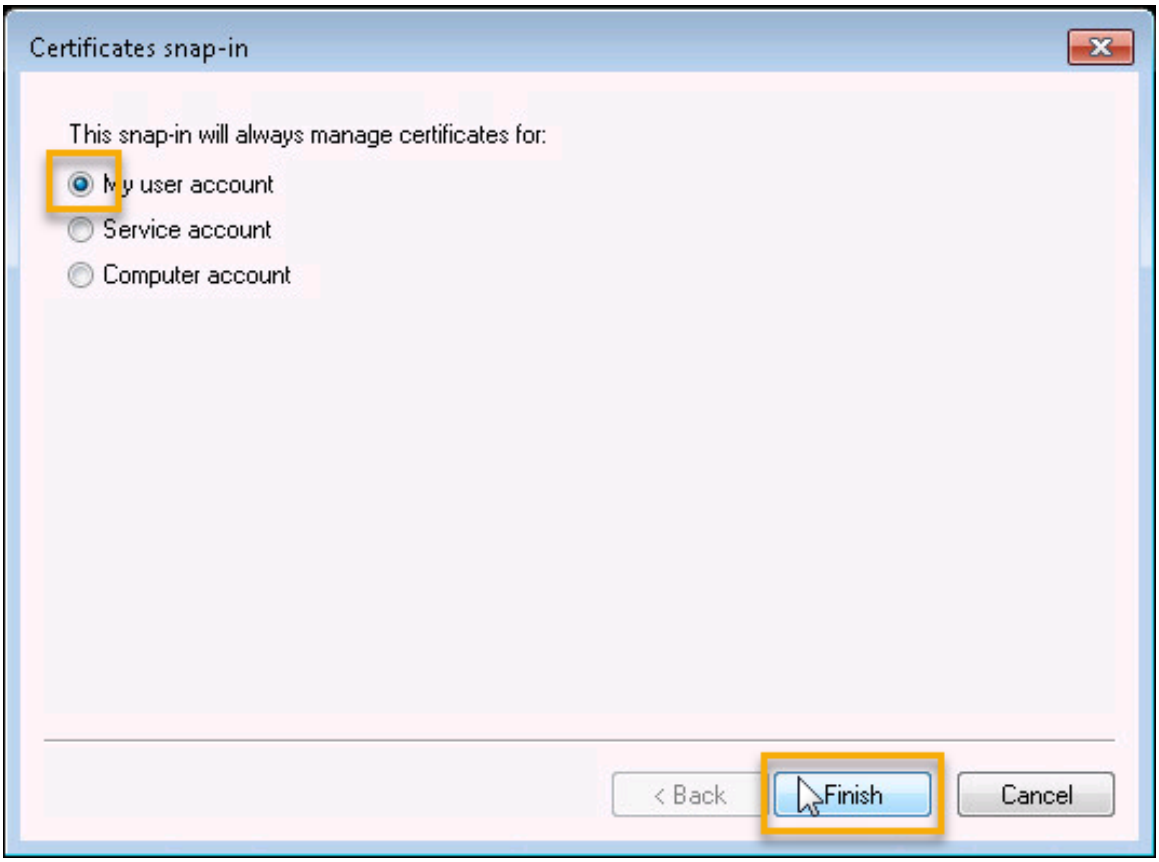


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

180. In the subsequent popup window select the **My user account** and click **Finish**.

Figure 317. Add Certificates console

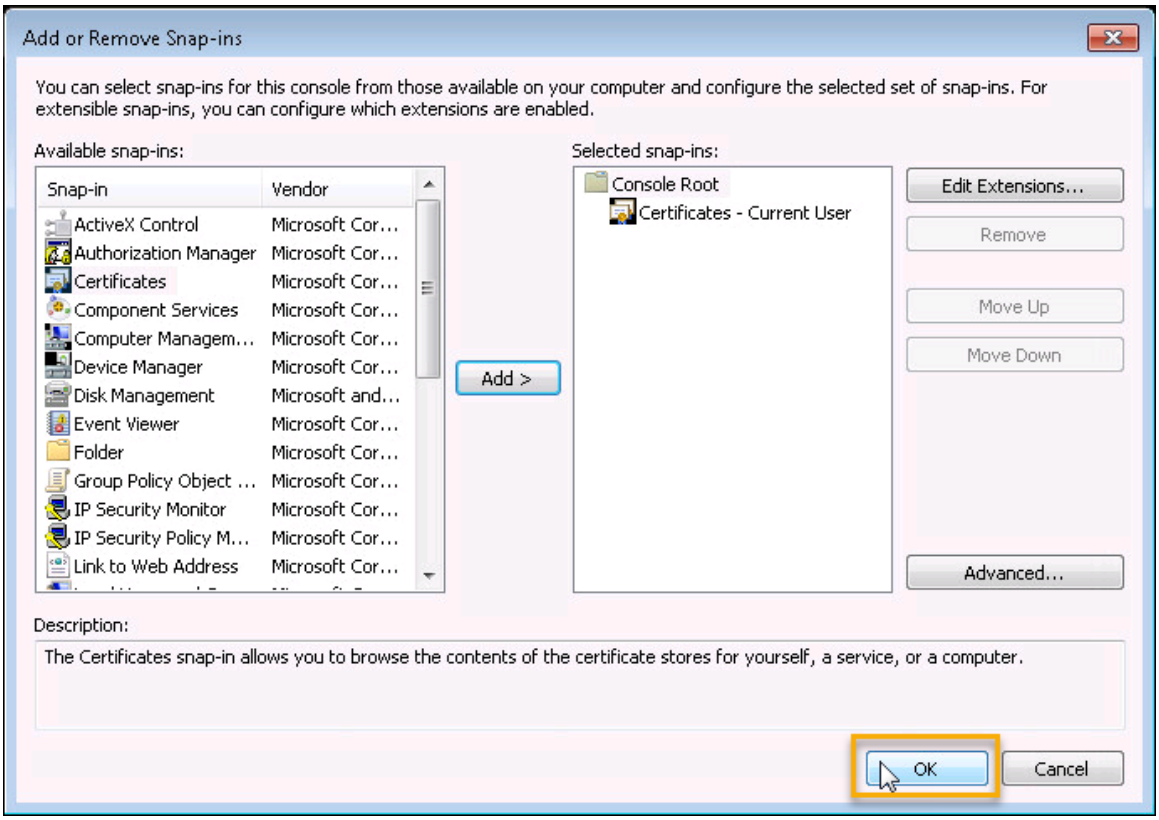


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

181. Click **OK**.

Figure 318. Click OK

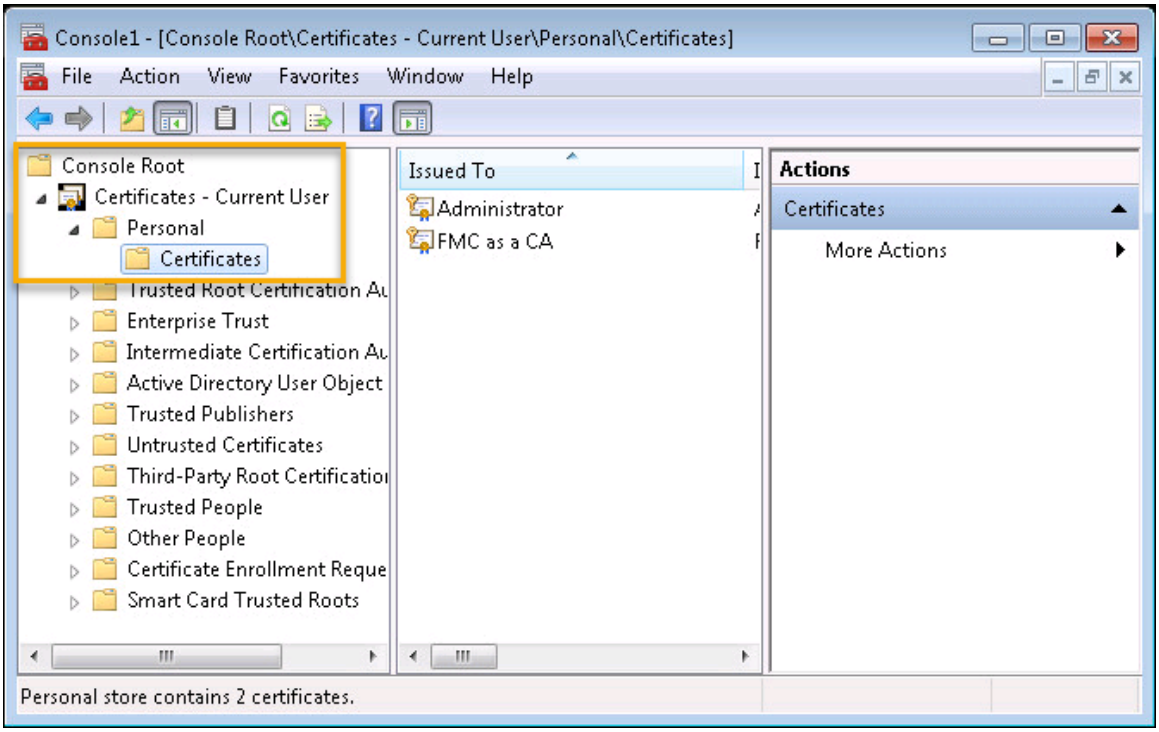


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

182. 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 319. Navigate to Certificates



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

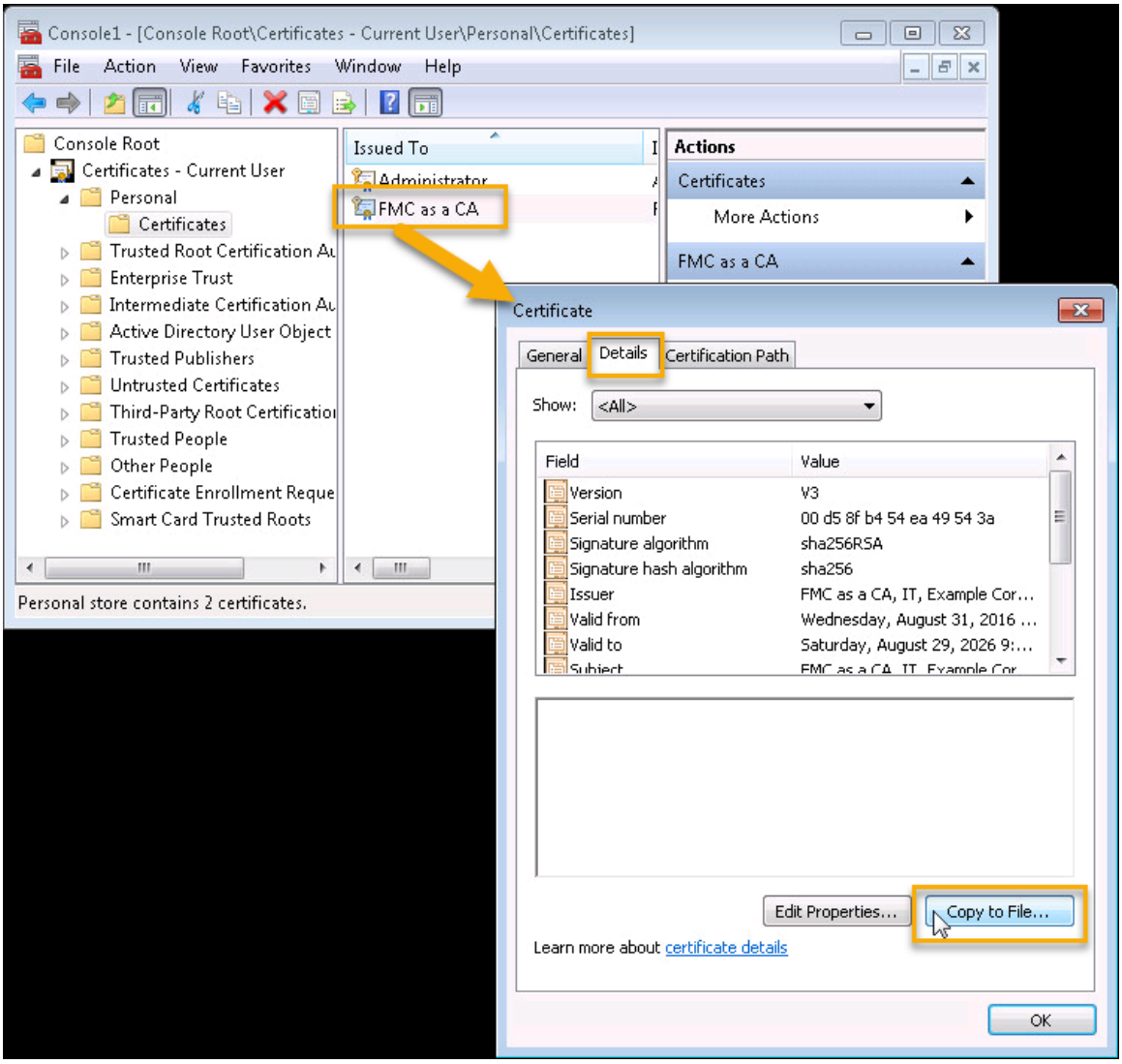
https://t.me/learningnets

183. **Double-click** the **FMC as a CA** certificate.

184. Click the **Details tab**.

185. Click the **Copy to File** button.

Figure 320. Prepare to export

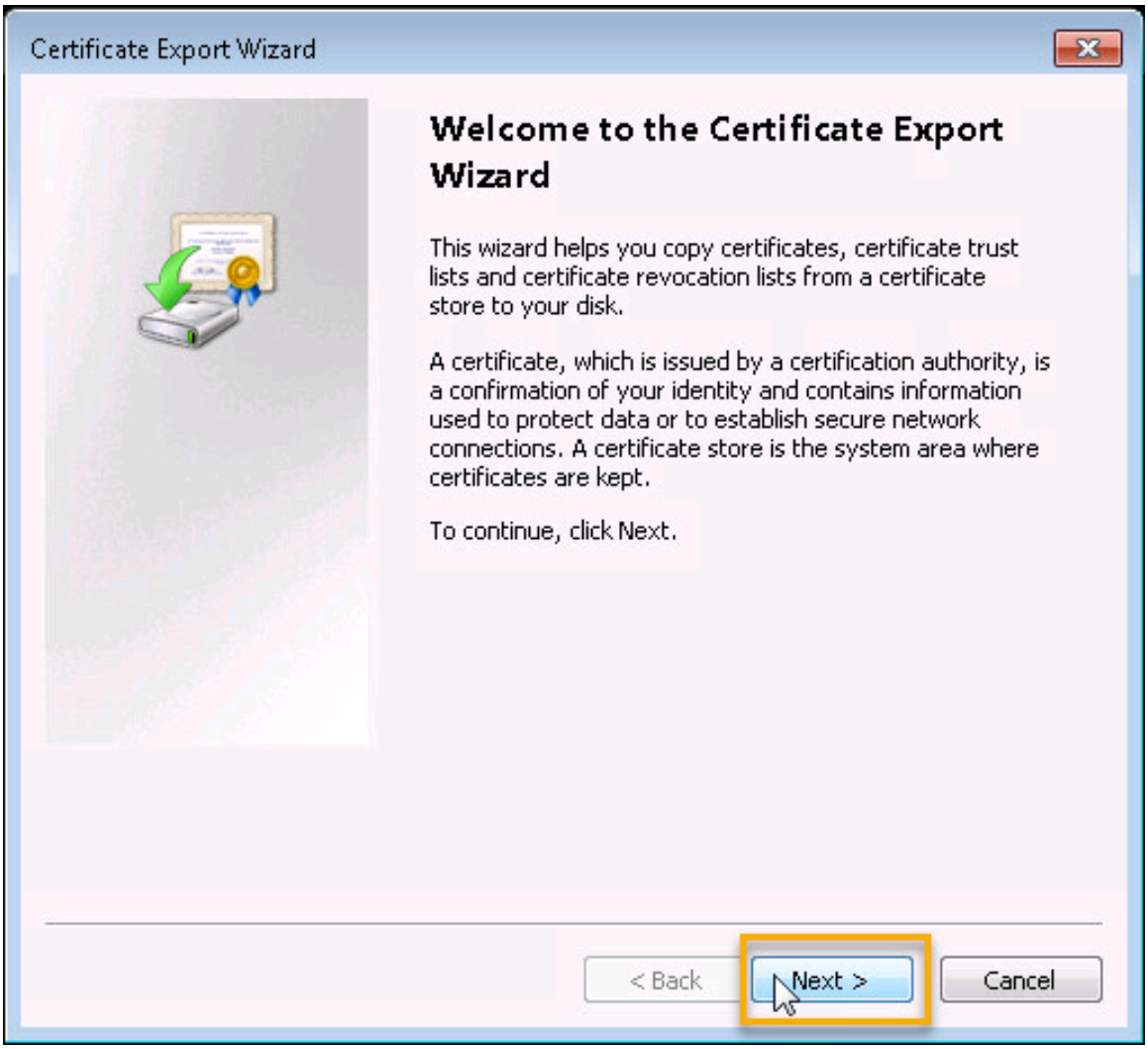


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

186. In the Certificate Export Wizard click **Next**.

Figure 321. Export Cert Page 1

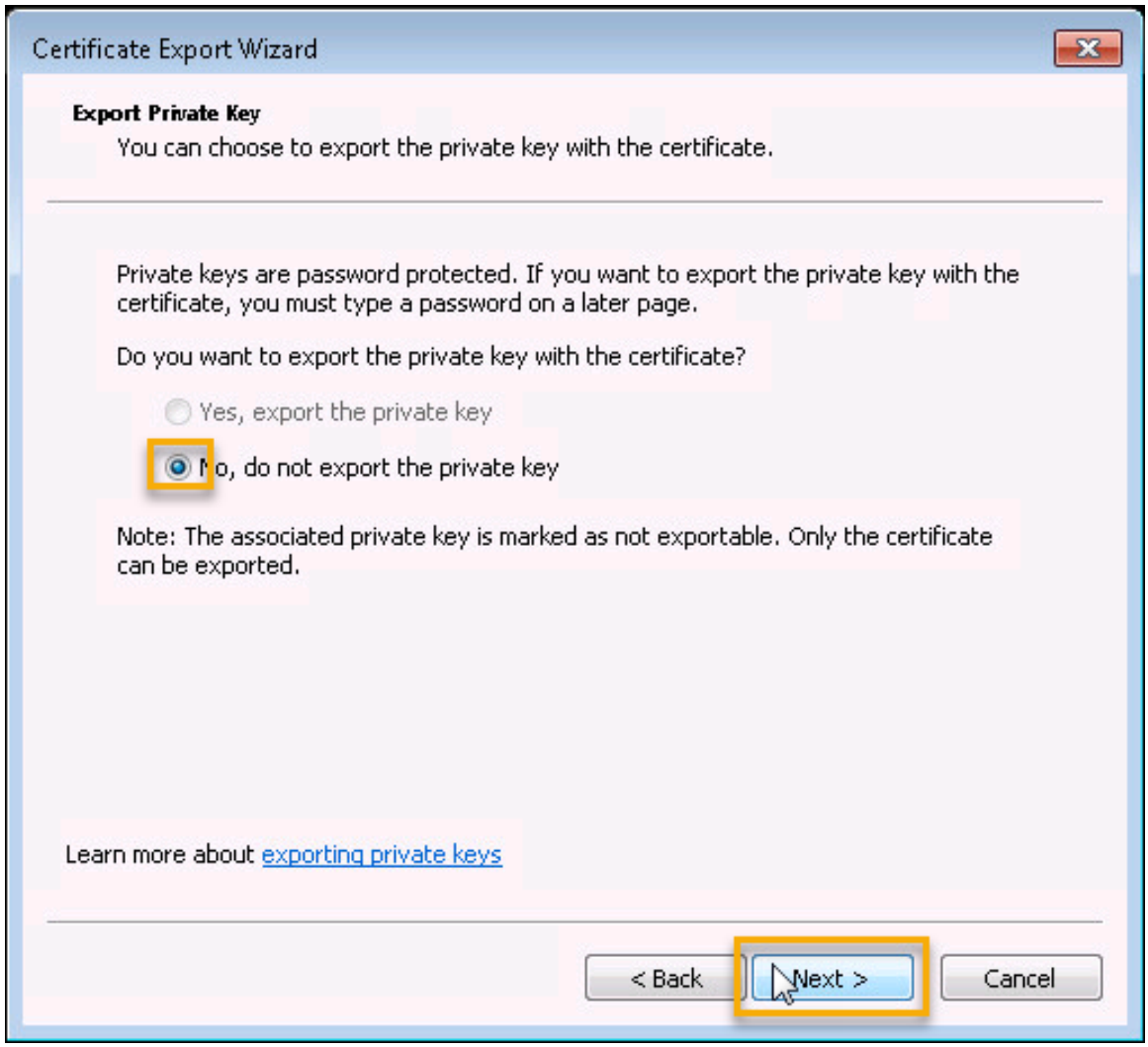


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

187. Ensure that the **No, do not export the private key** radio button is selected and click **Next**.

Figure 322. Export Cert Page 2



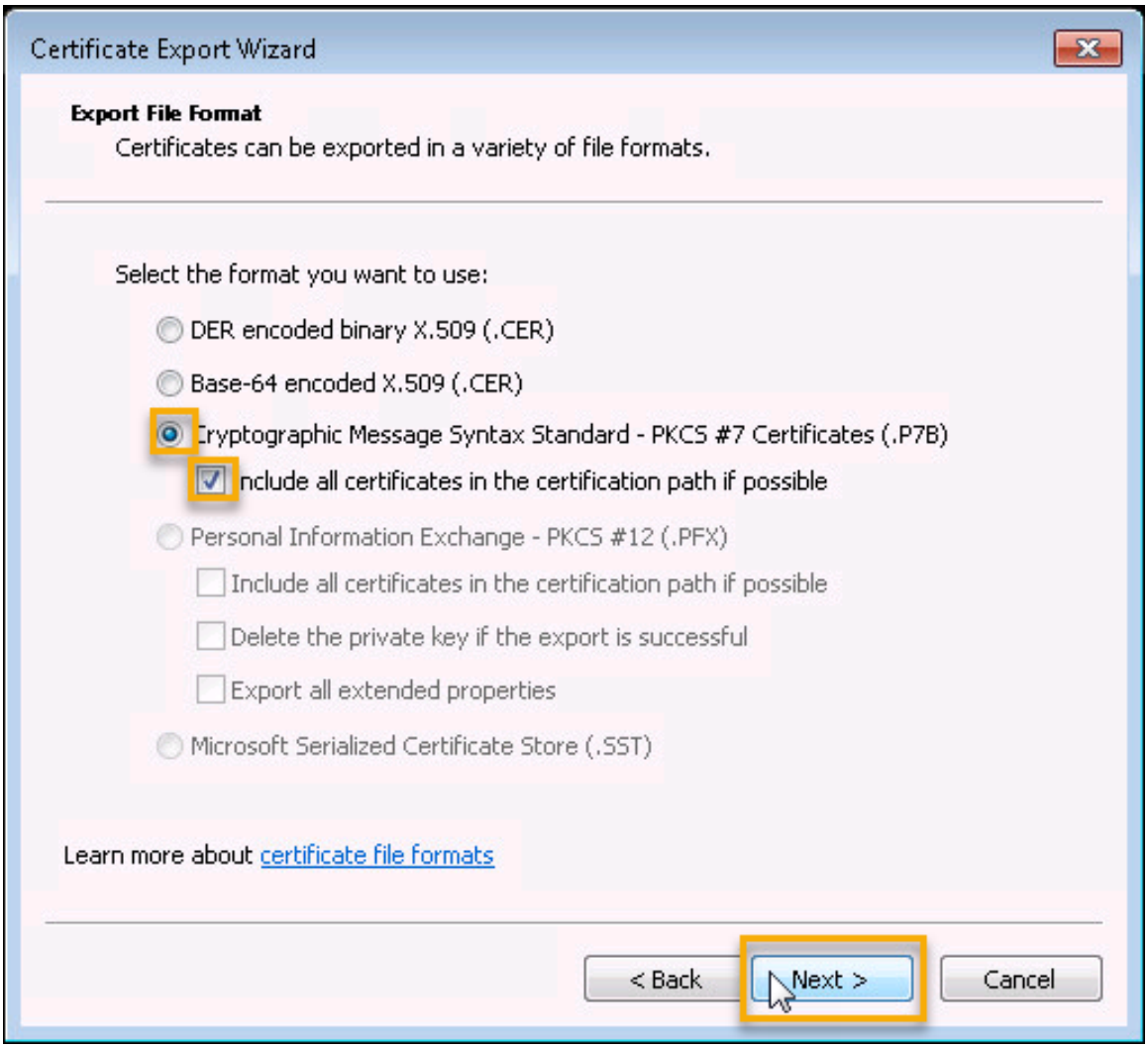
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

188. 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.

189. Click **Next**.

Figure 323. Export Cert Page 3

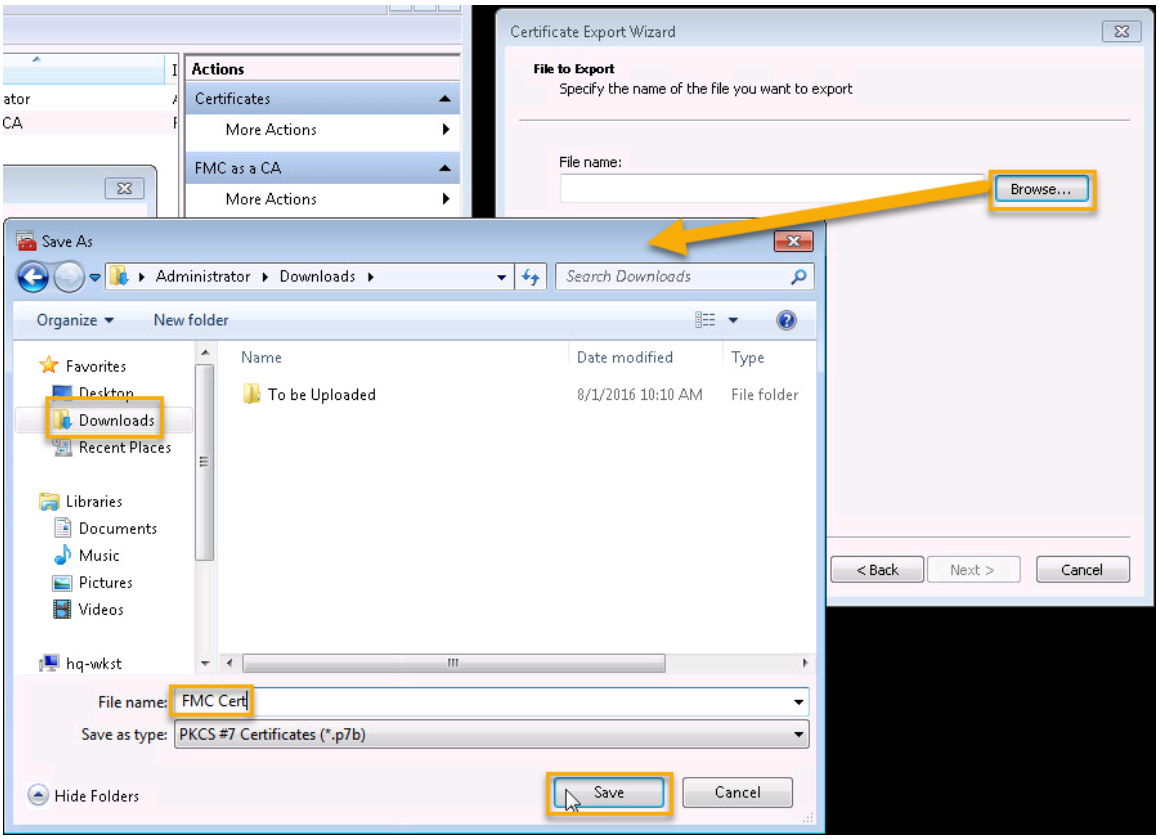


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

190. Click **Browse…** and select the **Downloads** folder. Use **FMC Cert** for the File name. Click **Save**.

Figure 324. Export Cert Page 4

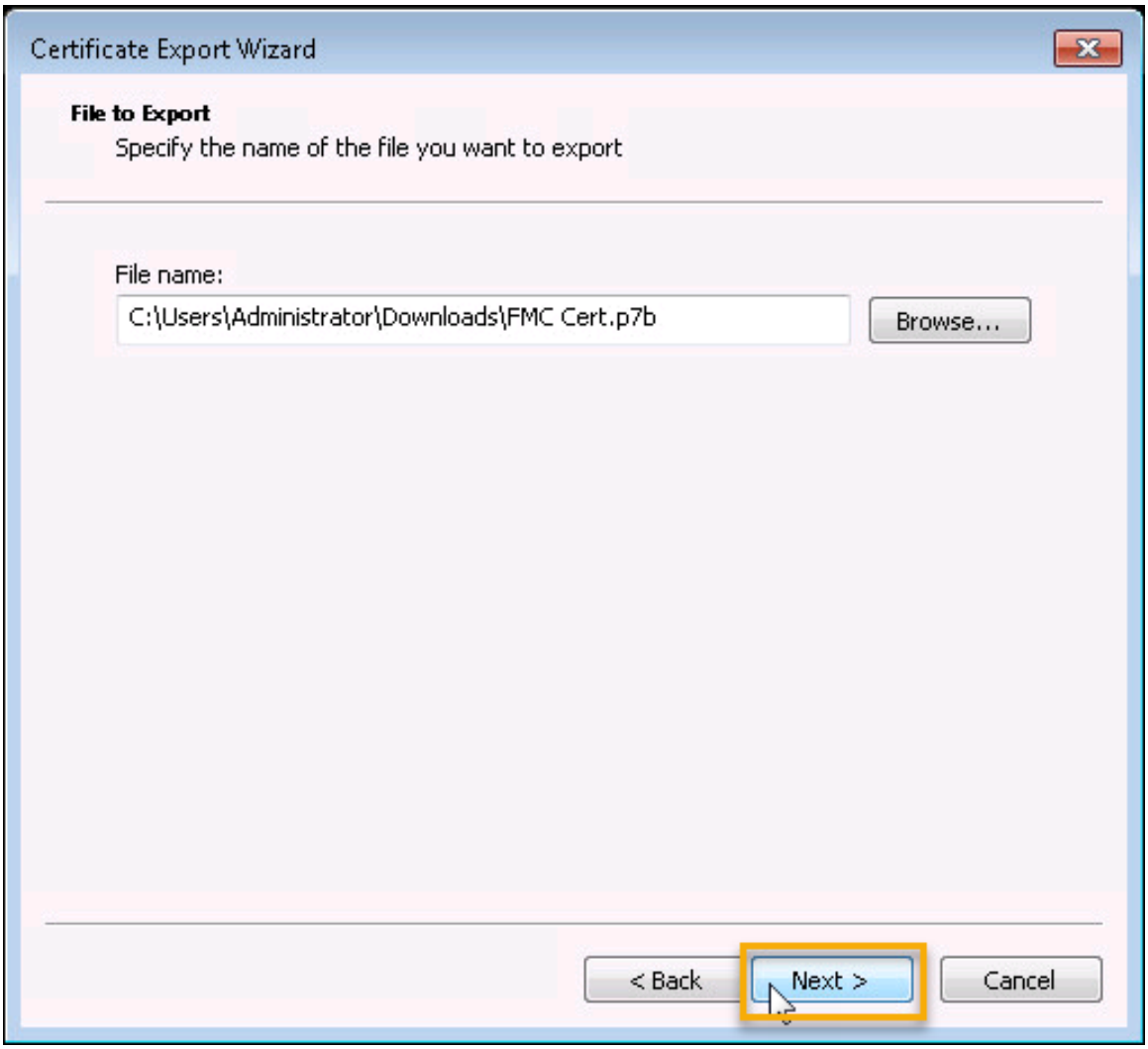


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

191. Click **Next**.

Figure 325. Export Cert Page 5

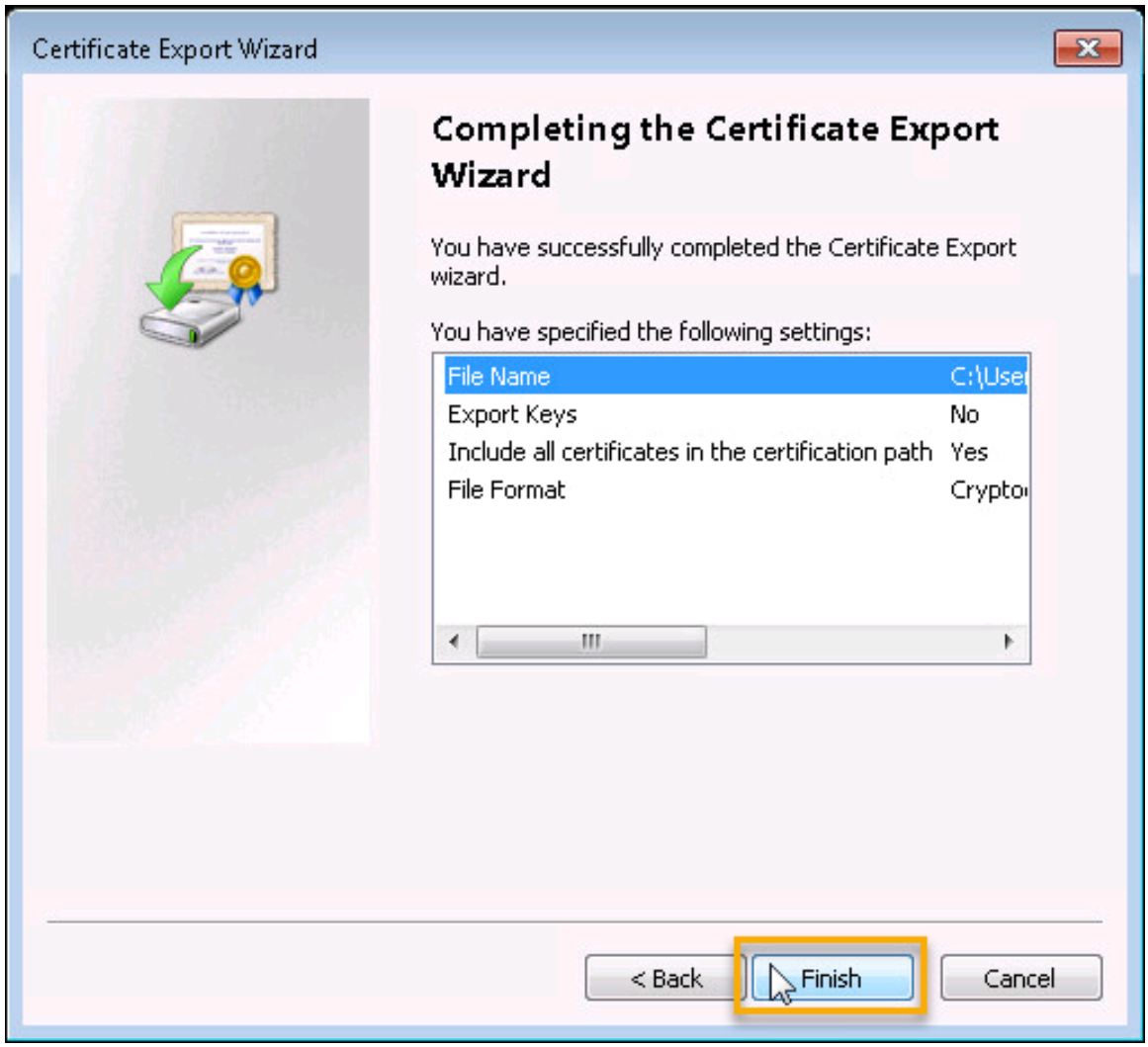


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

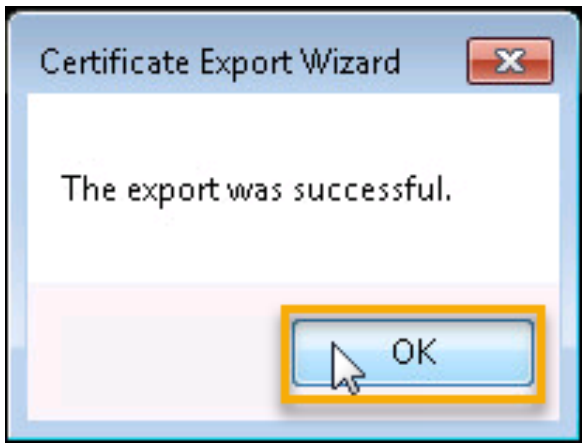
192.Click **Finish**

Figure 326. Export Cert Page 6



193.Click **OK** on the Certificate Export Wizard popup window.

Figure 327. Click OK

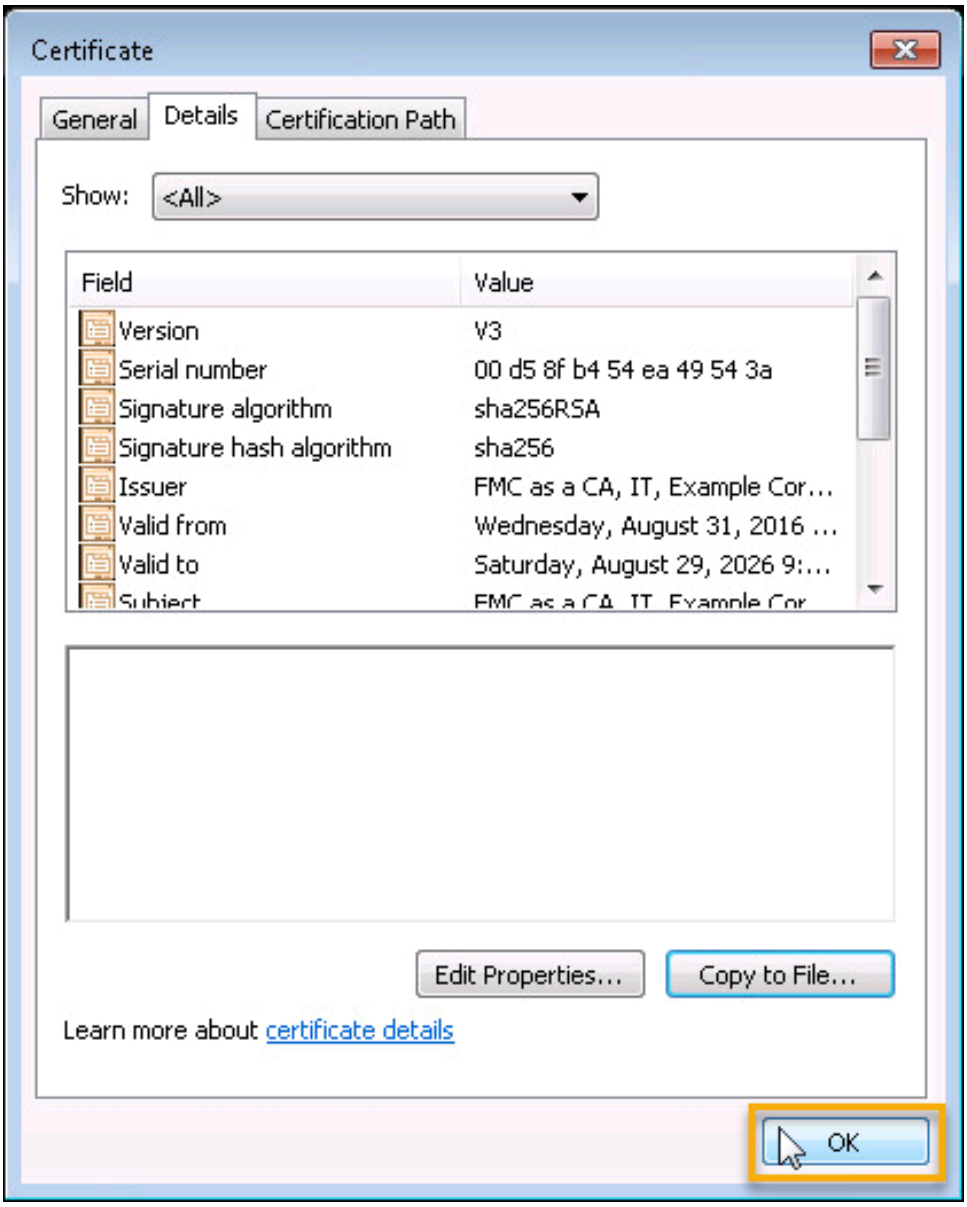


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

194. Click **OK** on the Certificate window.

Figure 328. Click OK

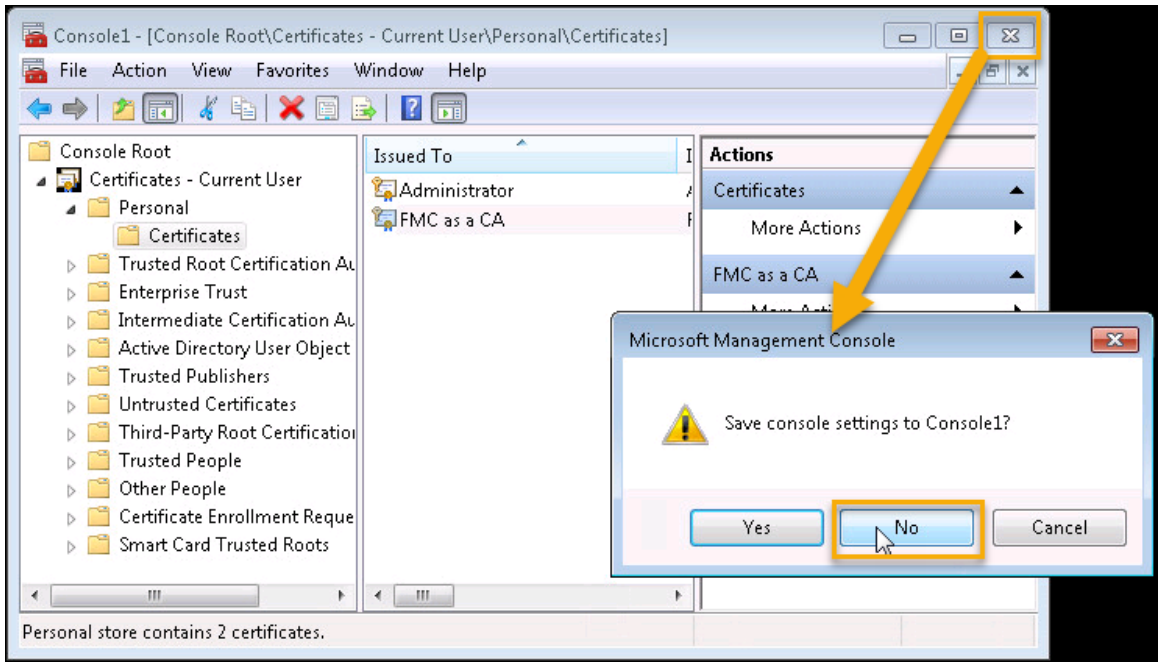


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

195.**Close** the Console1 window. You don't need to save changes.

Figure 329. Close Console1



Time to trust the FMC as a Certificate Authority within the Firefox browser.

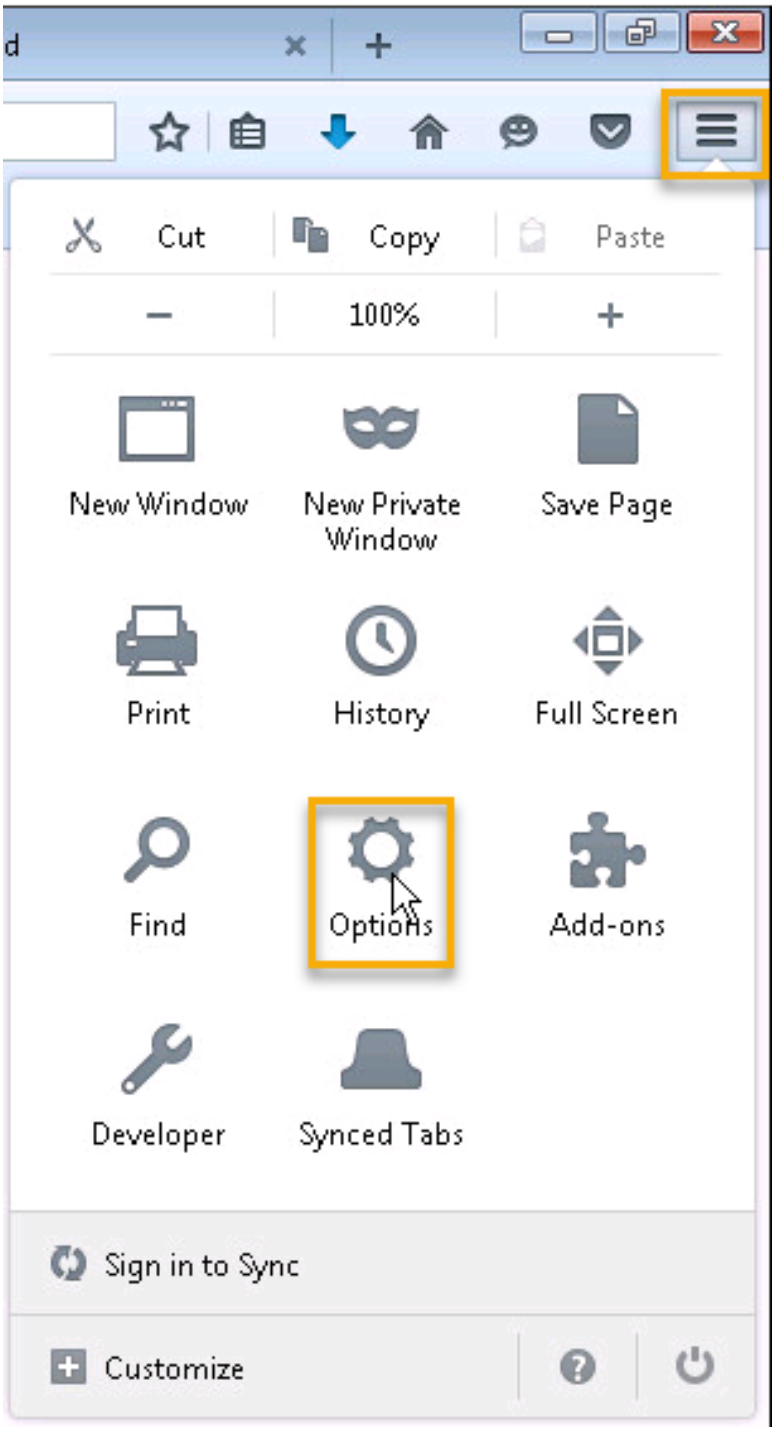
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

196. Open **Firefox** and click the **hamburger menu**.

197. Select the **Options** item.

Figure 330. Open Firefox Options menu



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

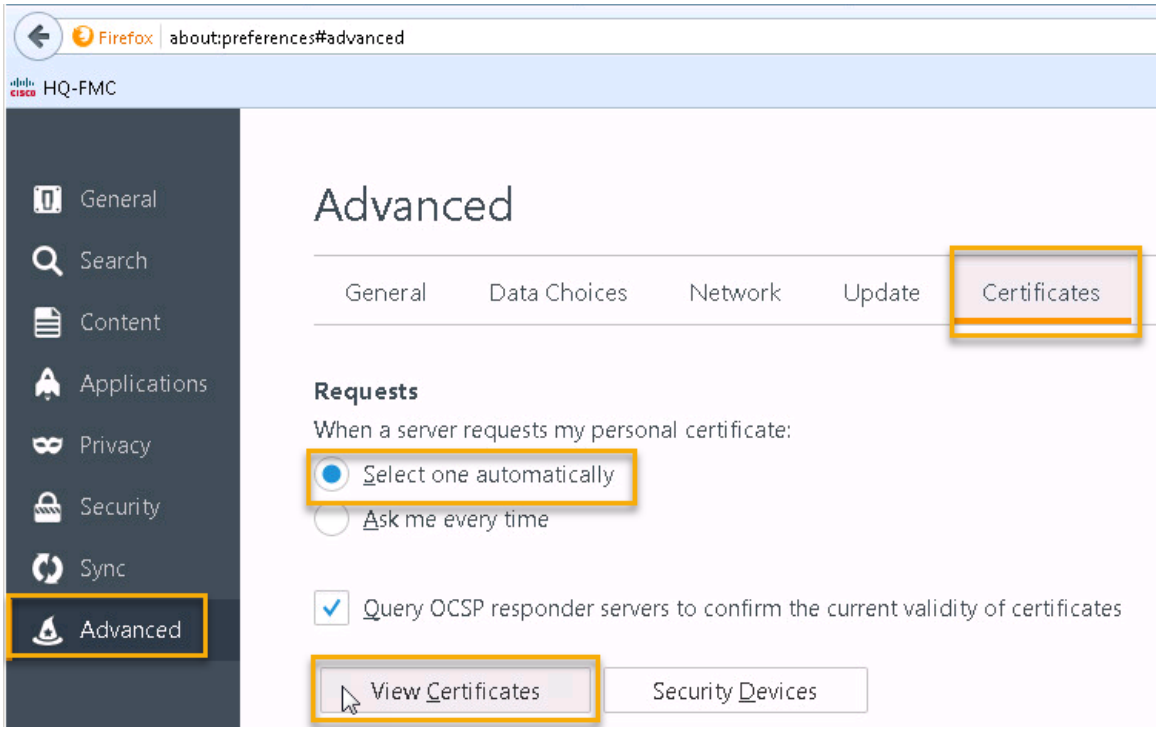
https://t.me/learningnets

198. From the left side column of items select **Advanced** and then click **Certificates**.

199. Check the **Select one automatically** radio button.

200. Click the **View Certificates** button.

Figure 331. View Certificates

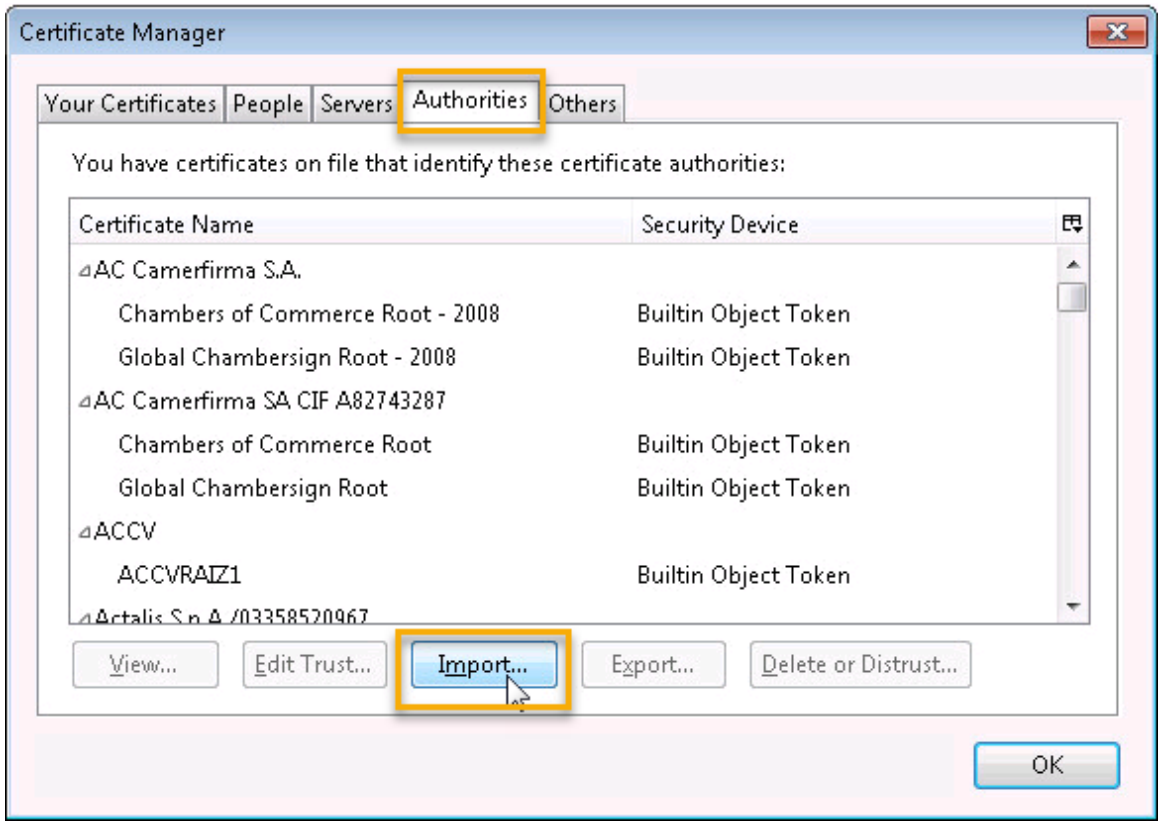


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

201. Click the **Authorities tab** and then click the **Import** button.

Figure 332. Prepare to Import CA



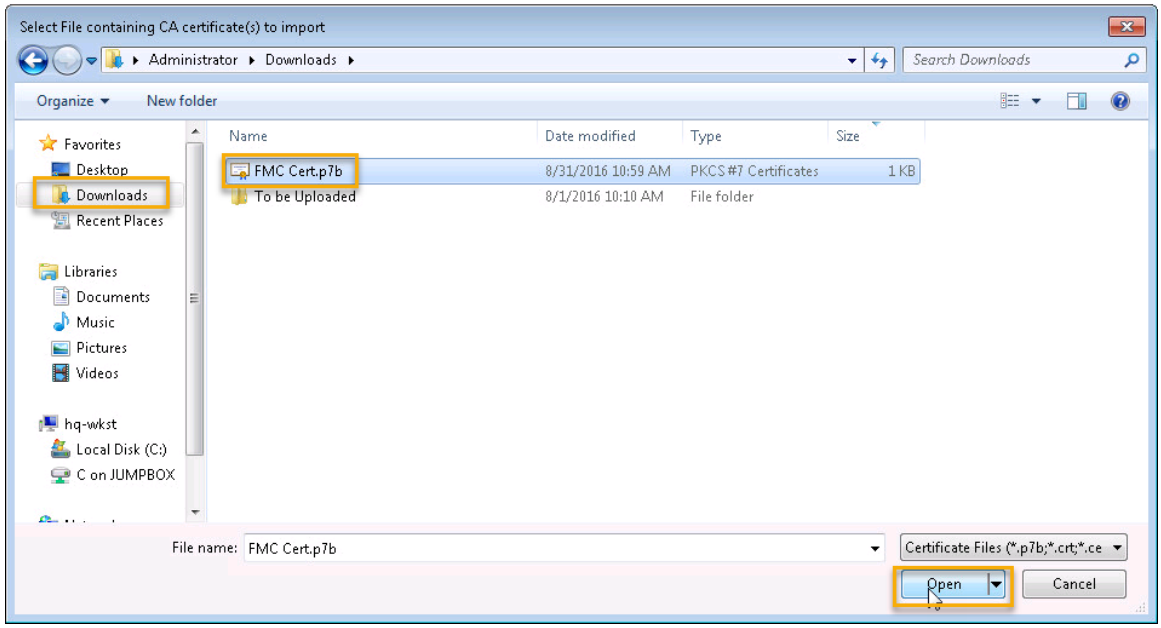
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

202. 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.

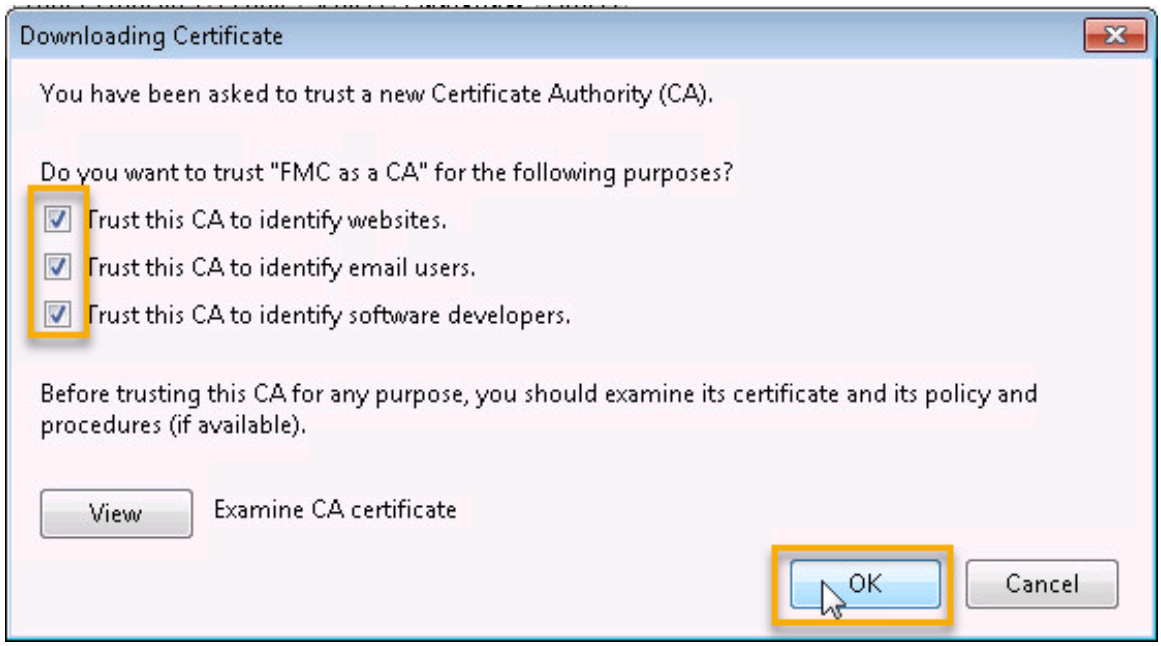
203. Click **Open**.

Figure 333. Select FMC CA Cert



204. A popup window will ask when the FMC as a CA certificate should be trusted. Check **all the boxes** and then click **OK**.

Figure 334. Fully trust CA

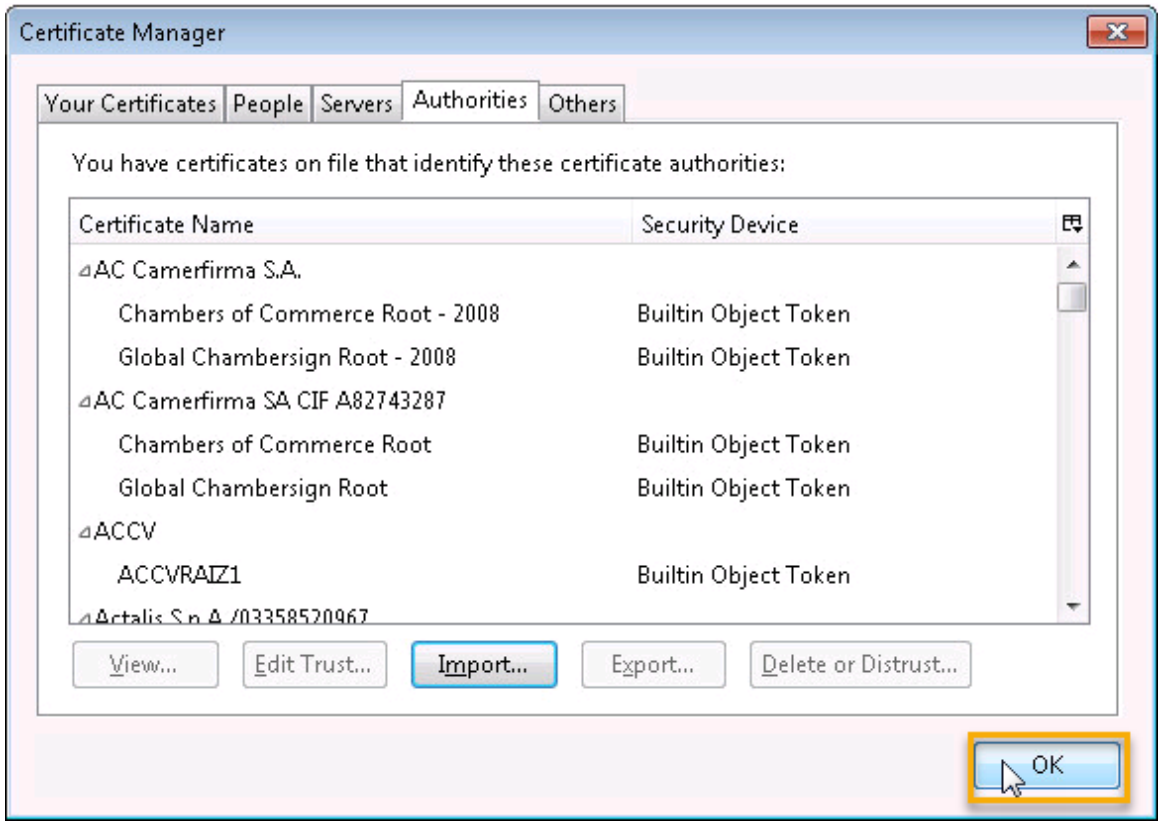


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

205. Click **OK** on the Certificate Manager window to close it.

Figure 335. Click OK



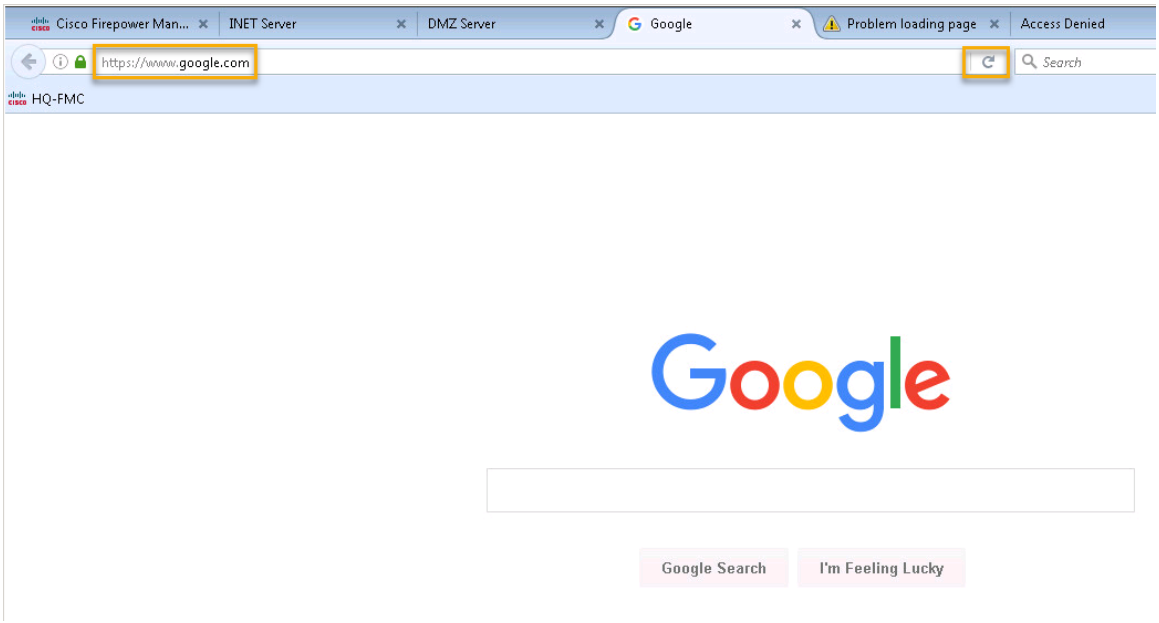
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Browser Test – Phase 2

206.Now **refresh** the **the Google tab**. This time it will work!

Figure 336. Success in getting to google.com

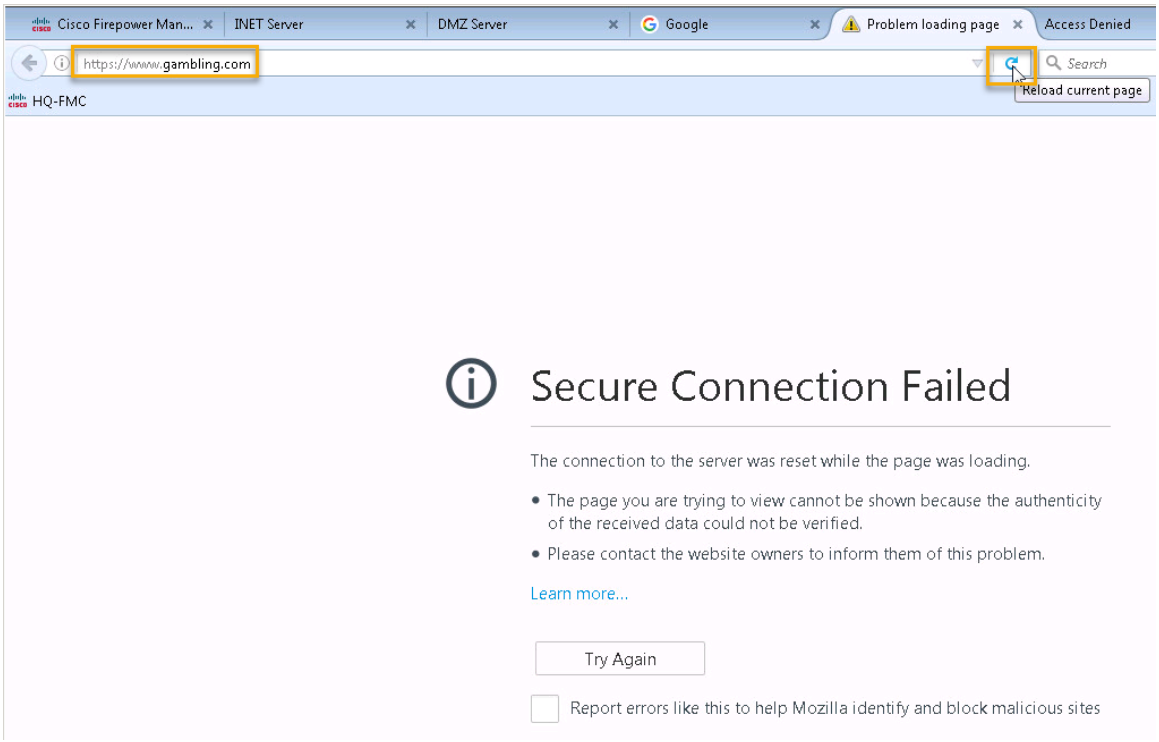


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

207. Attempt 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 337. No Gambling for you!!!



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Analyze the Results

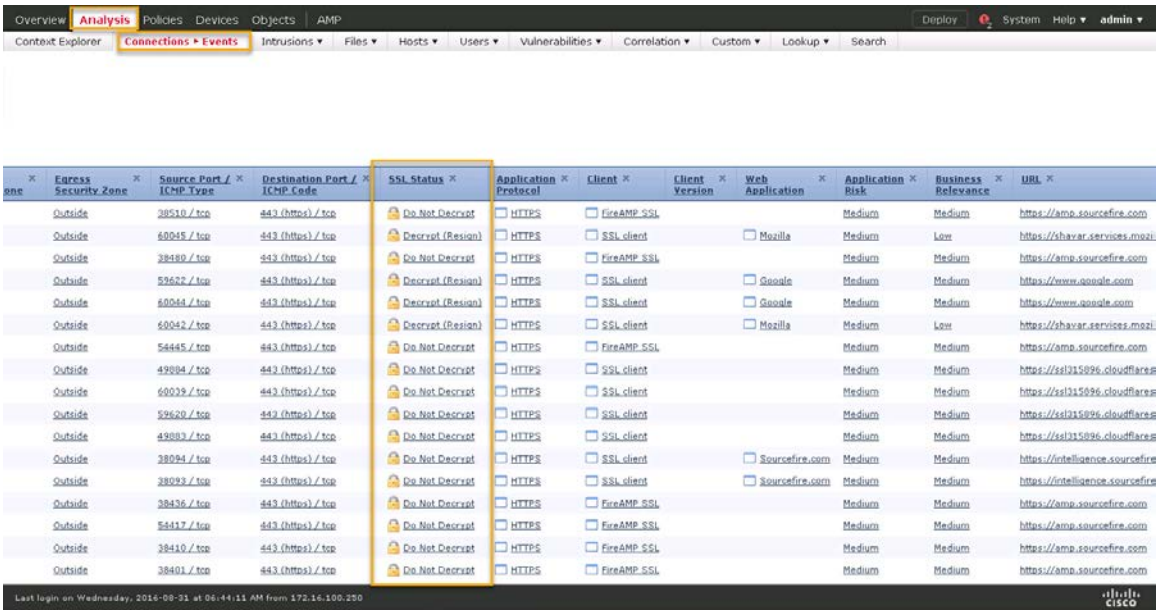
Now that you have successfully created a man-in-the-middle “hack” so that you can see the contents of an encrypted SSL connection let’s see what the logs show.

208. In the FMC, navigate to Analysis > Connections > Events.

209. In the Application Protocol column, click on the **HTTPS** of any row to drill down to looking at only HTTPS related events.

210. 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 338. See SSL Status column



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

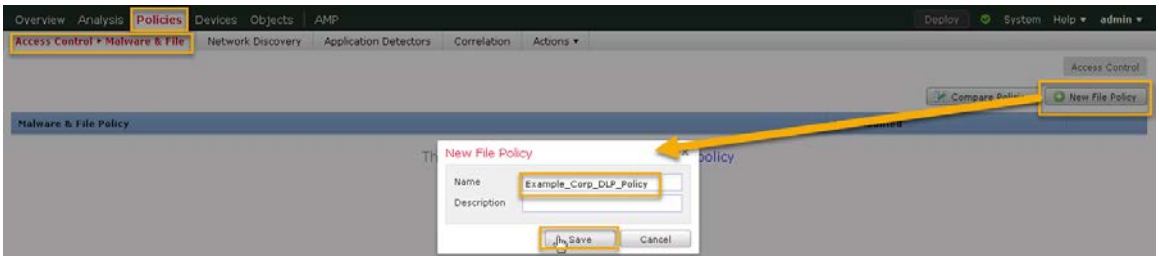
211. In the FMC website navigate to **Policies > Access Control > Malware & File**.

212. Click the **New File Policy** button.

    a. Name: **Example_Corp_DLP_Policy**

    b. Click **Save**.

Figure 339. Create new policy



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

213. 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.

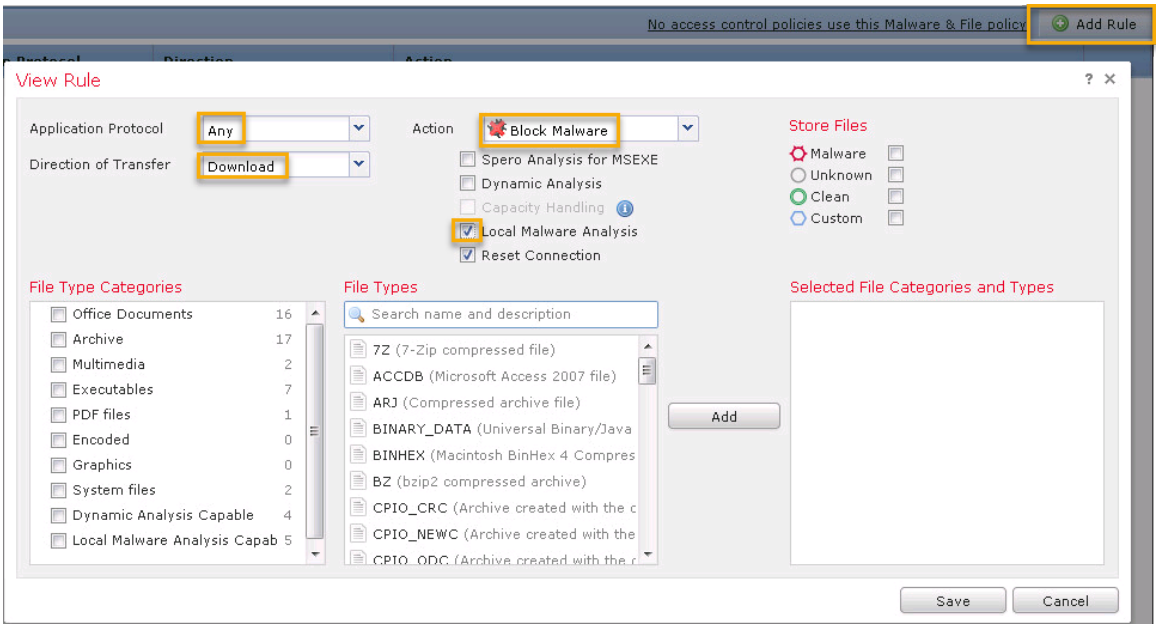
    a. Application Protocol: **Any** (You don't care how it is transferred. You want to inspect these files for infections and malware.)

    b. Direction of Transfer: **Download**

    c. Action: **Block Malware**

    d. Check the **Local Malware Analysis** box.

Figure 340. Part 1 of adding new rule



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 = 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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

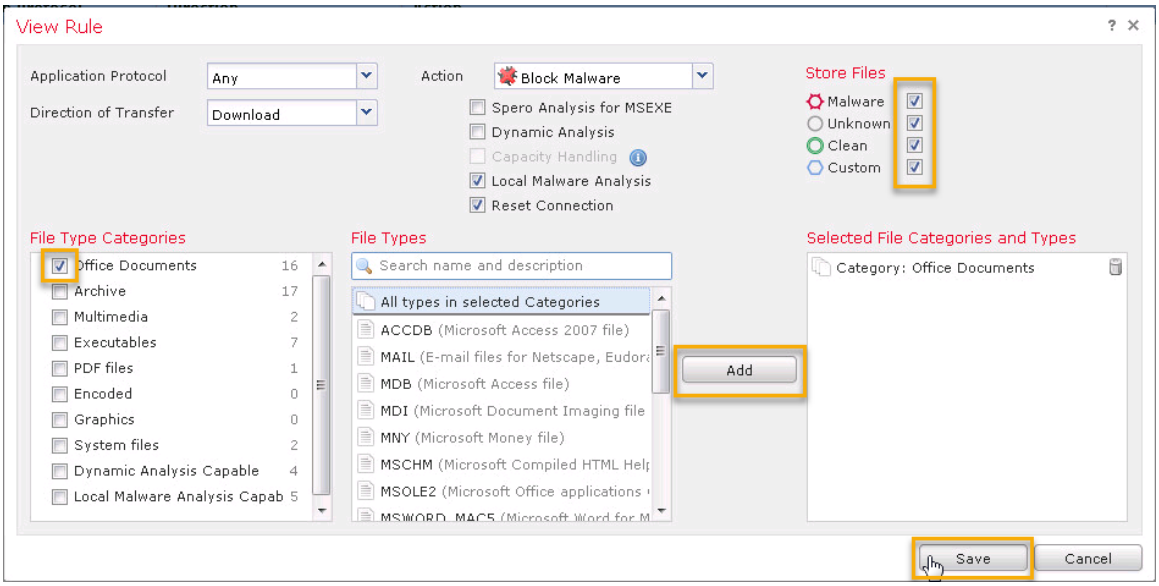
https://t.me/learningnets

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 341. Save new rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

214. 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**

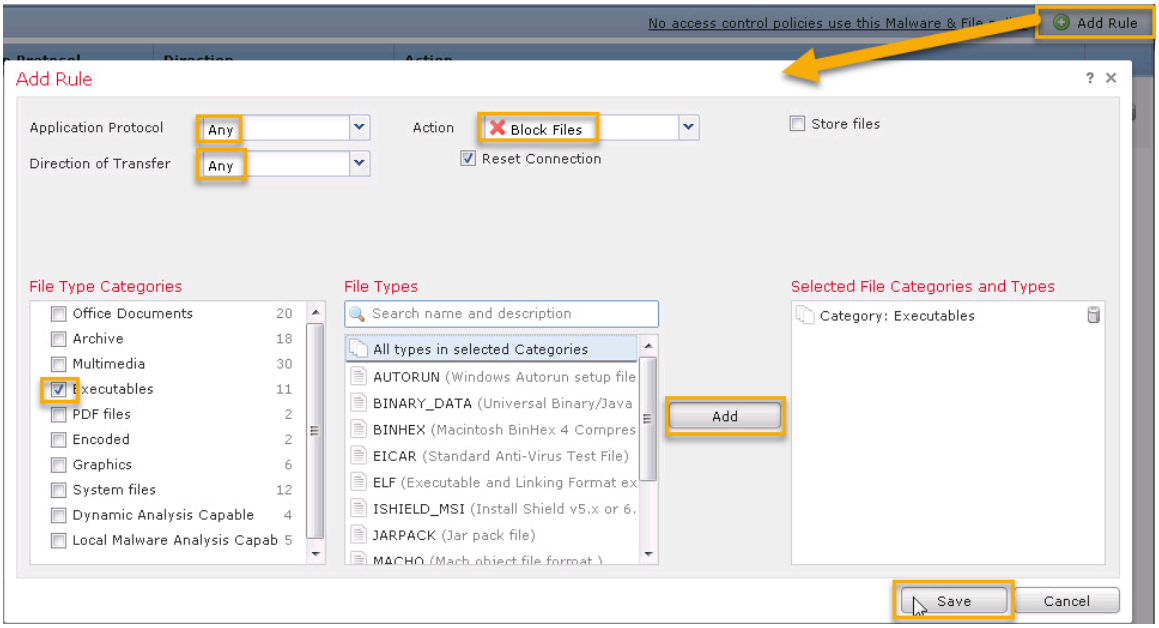
b. Direction of Transfer: **Any**

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 342. Create another rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

215. 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**

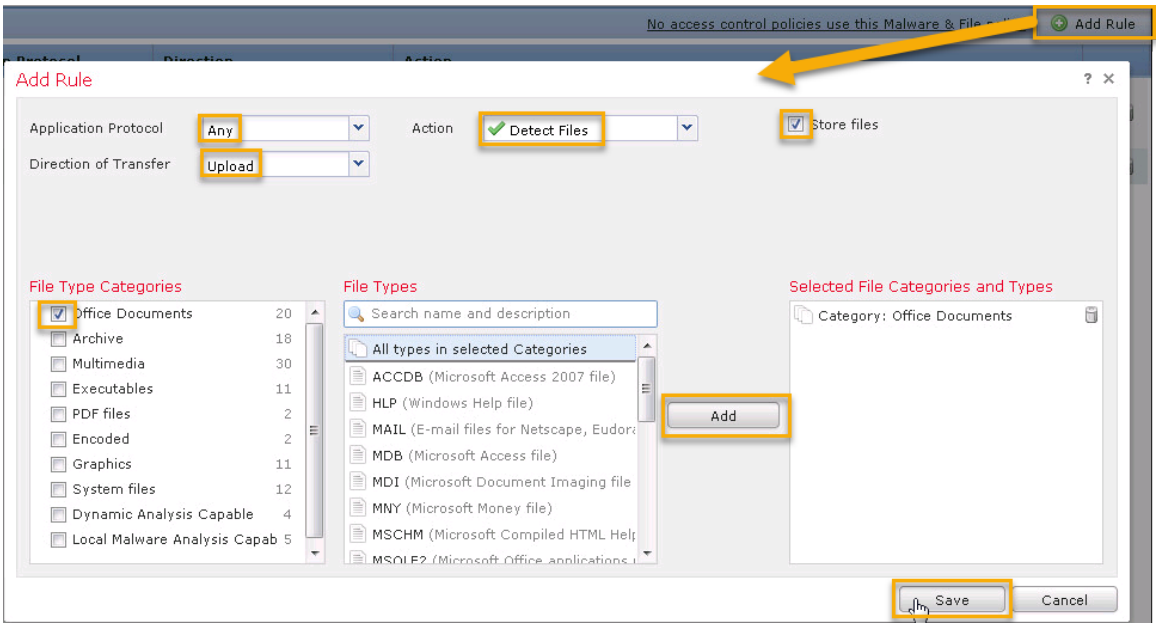
    c. Action: **Detect Files**

    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**.

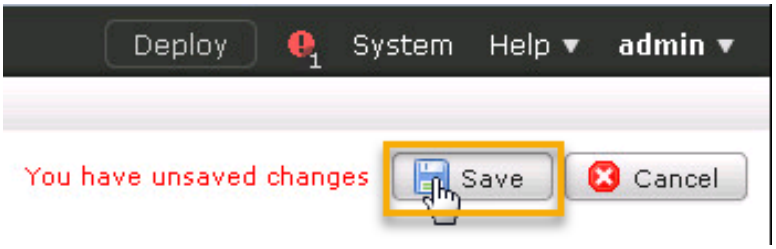
Figure 343. Create another rule



Note: PDF files are not considered Office Documents but are a category all to themselves.

216. Click **Save**.

Figure 344. Save changes to FMC

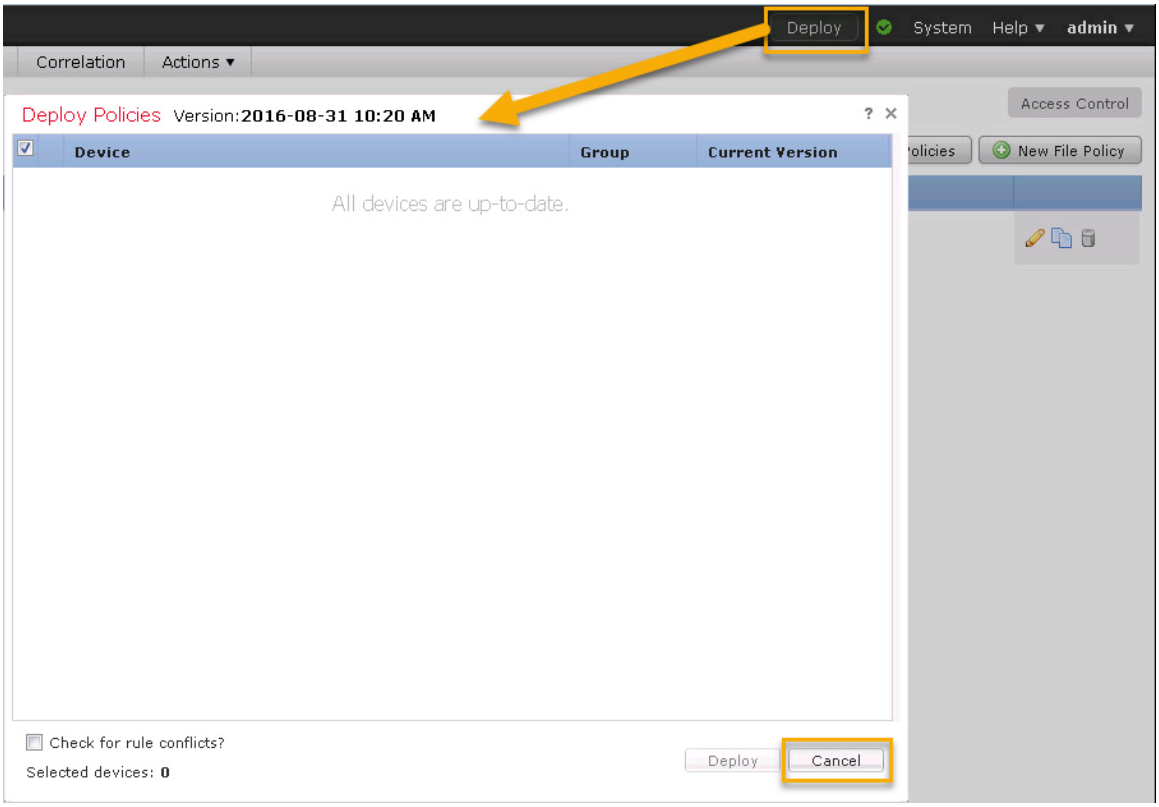


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

217. 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 345. Nothing to Deploy, yet.



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.

218. Navigate to Policies > Access Control > Access Control and edit the Base Policy.

Figure 346. Edit the Base Policy



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

219. **Edit** the **LAN to Internet Access** rule.

Figure 347. Edit the LAN to Internet Access rule

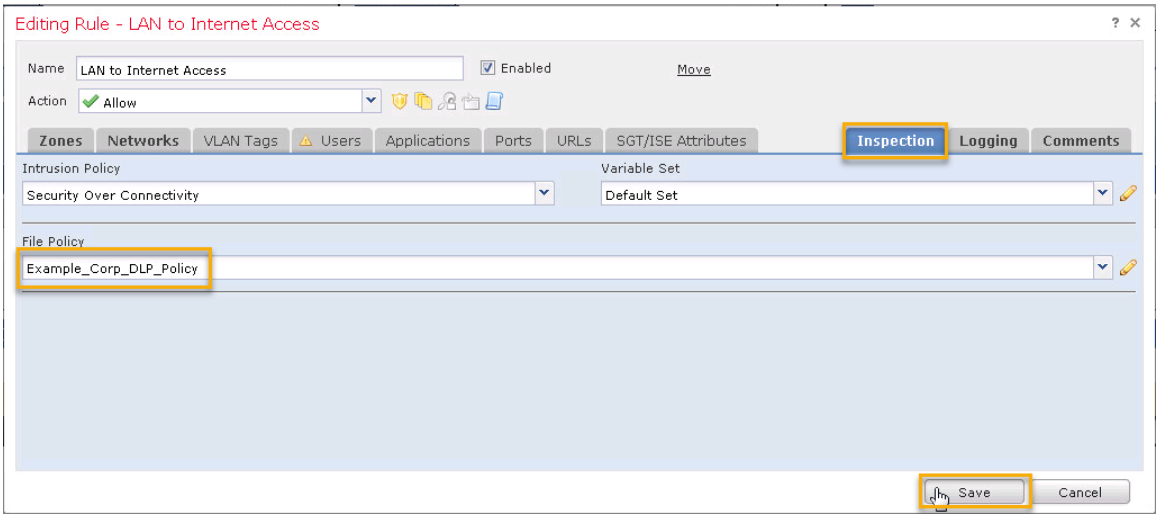


220. Click the **Inspections tab**.

221. Using the dropdown menu for the **File Policy** option select the **Example_Corp_DLP_Policy** from the list.

222. Click **Save** to save the modification to this rule.

Figure 348. Apply Policy and Save.



223. Now click **Save** to save your changes. Then click **Deploy**, select **all the FTD** devices, and then click **Deploy**.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

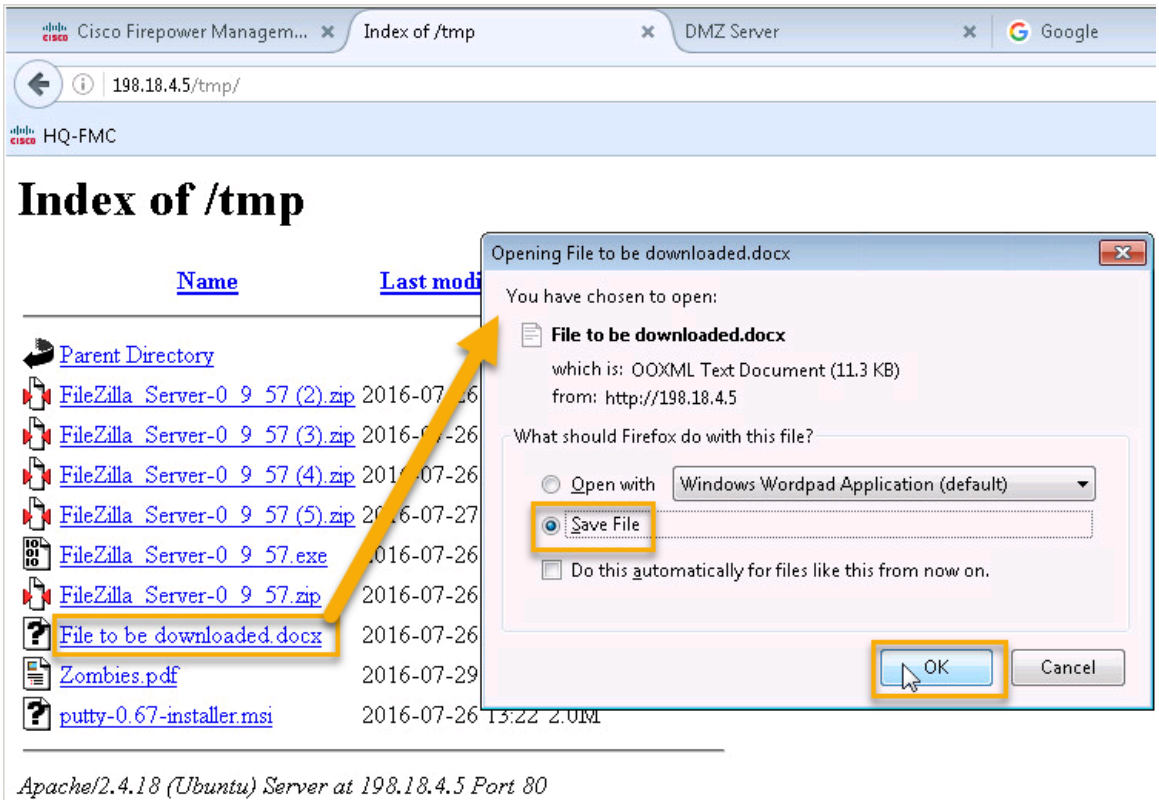
Perform Tests

Once the deployment is complete you will perform some tests to see what your Malware & File Policy can do.

224. On **hq-wkst** open a **Firefox** tab to **http://198.18.4.5/tmp** (this is the inet-server).

225. Download the **File to be downloaded.docx** file.

Figure 349. Download the file



226. 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 350. View File Events

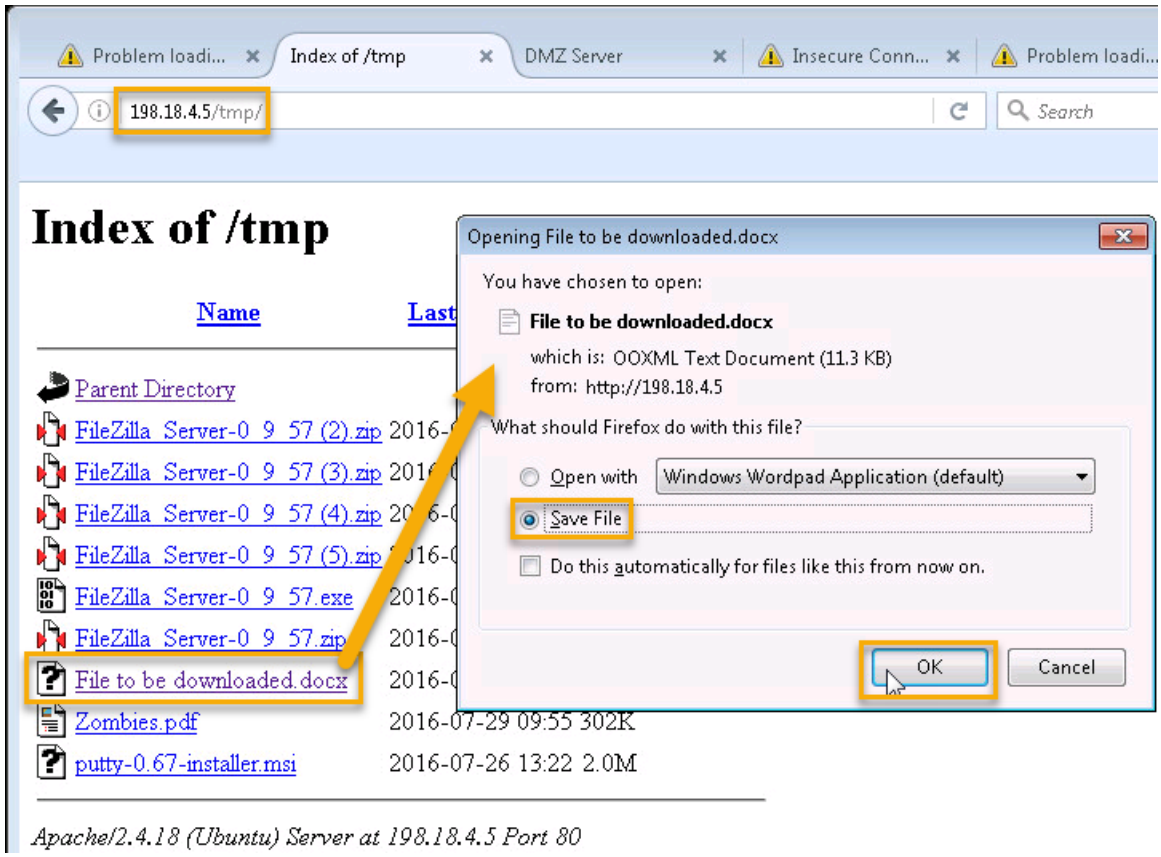


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

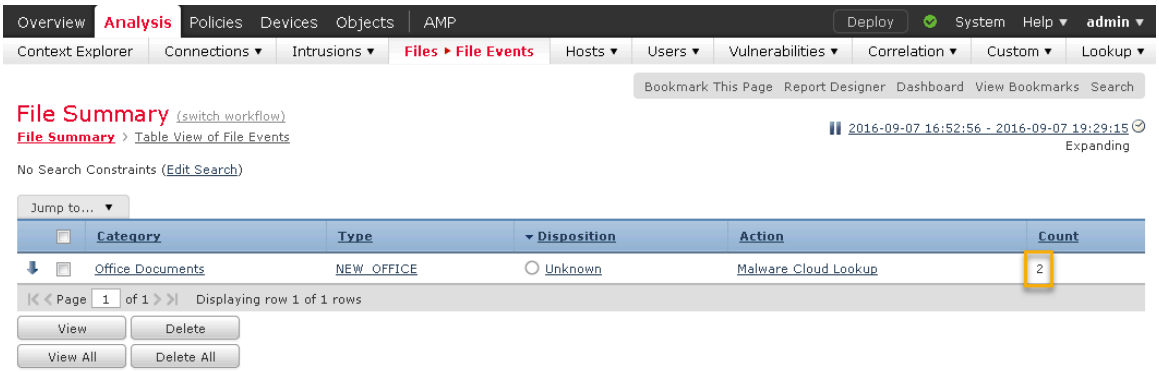
227. On **remote1-wkst** open up **Firefox** and go to **http://198.18.4.5/tmp** and download the **File to be downloaded.docx** file.

Figure 351. Download file from remote1-wkst



228. 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 352. View File Events

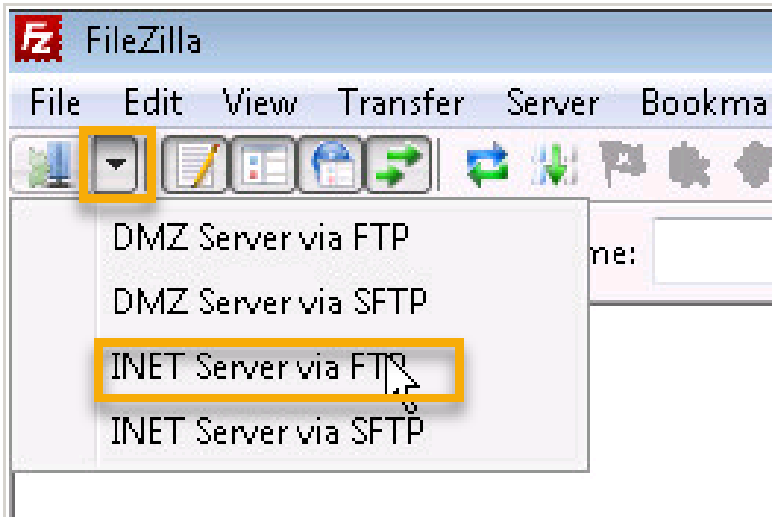


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

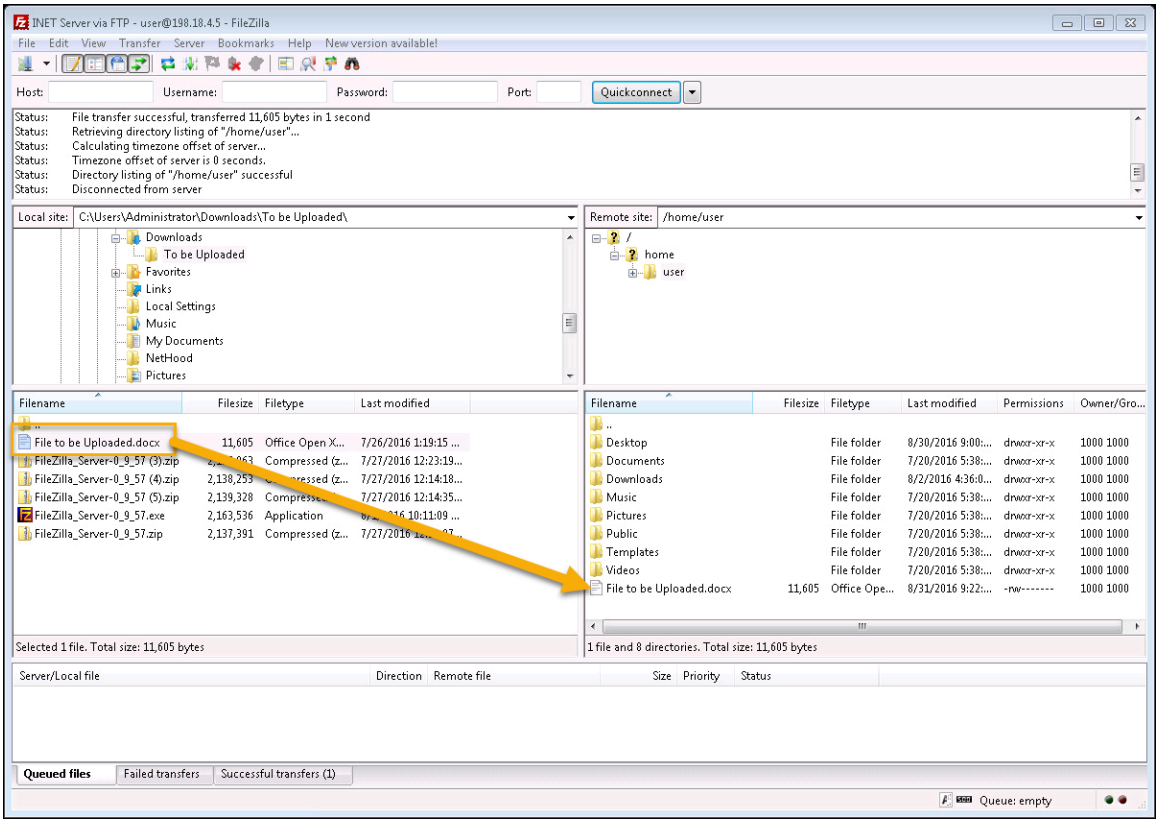
229. On **hq-wkst** open up **FileZilla** and use the **INET Server via FTP** bookmark to create an FTP connection to the inet-server.

Figure 353. Connect via FTP to inet-server



230. Upload the **File to be Uploaded.docx** file, located in the **To be Uploaded** folder in the **Downloads** directory.

Figure 354. FTP upload file

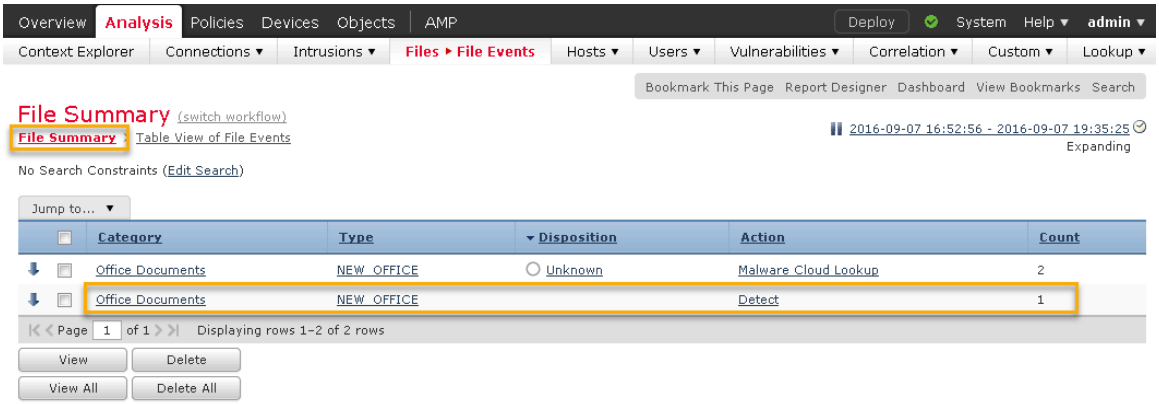


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

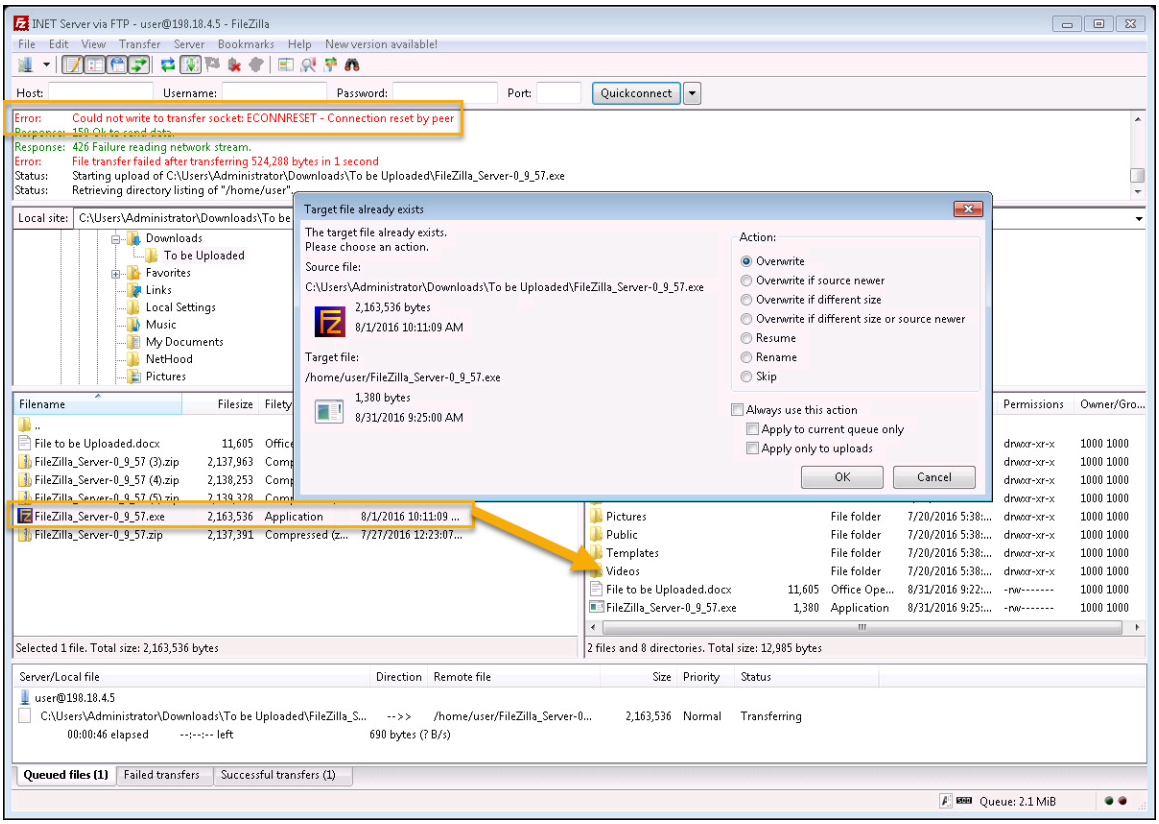
231. Return to the FMC GUI and click the **File Summary** link again. Notice that you have a new line and the Action is Detect. (Document files leaving the Example Corp network are allowed but are checked for Malware.)

Figure 355. View File Events



232. On **hq-wkst** attempt to download the **FileZilla_Server-0_9_57.exe** file via FTP and 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.

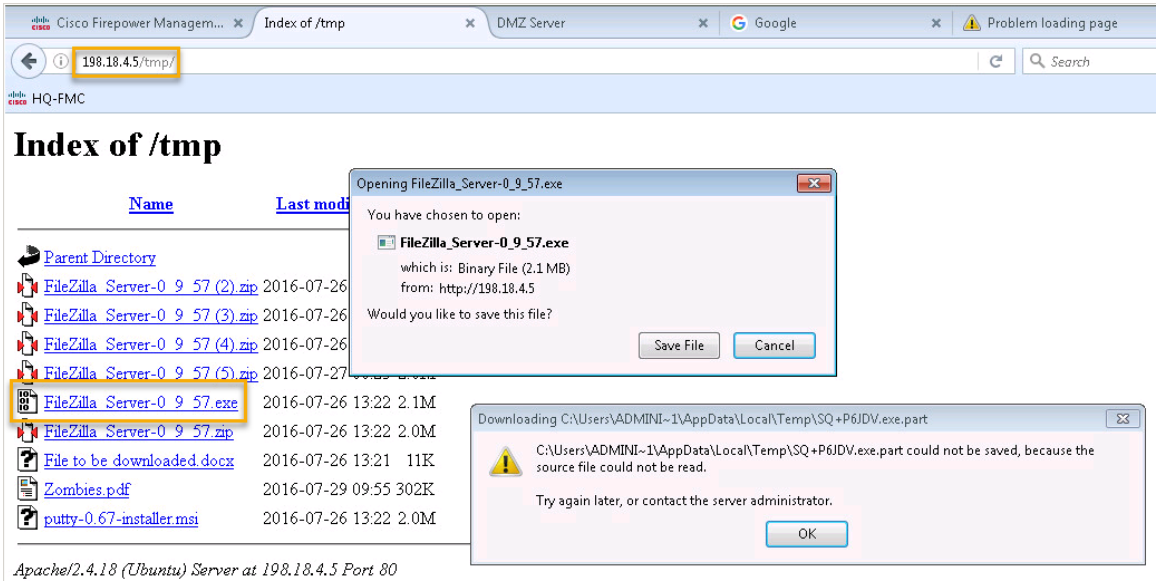
Figure 356. Try to download EXE file via FTP



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

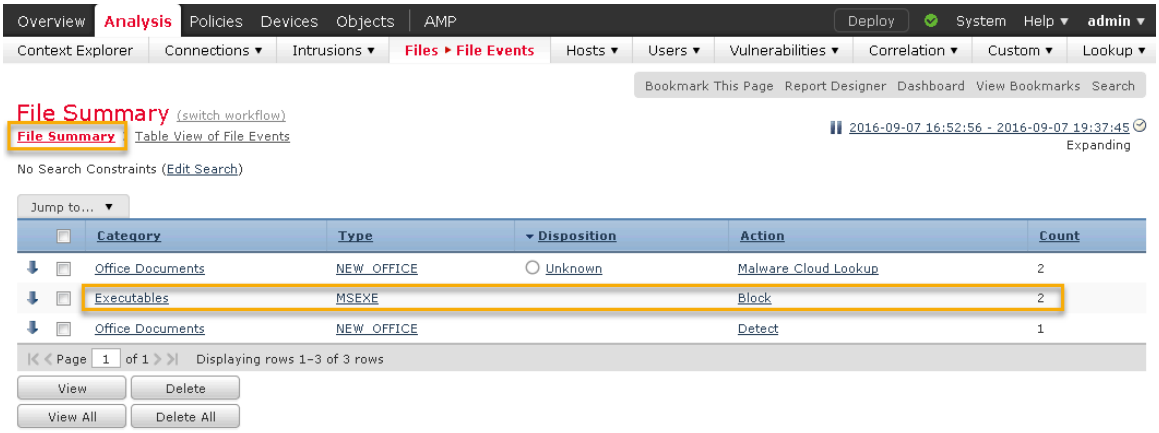
https://t.me/learningnets

Figure 357. Try to download EXE via HTTP



233. 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 358. View File Events



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Scenario 9. Intrusion Policy

Scenario Description

The use of the Intrusion Policies is 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.

234. In the FMC GUI navigate to **Policies > Access Control > Intrusion**.

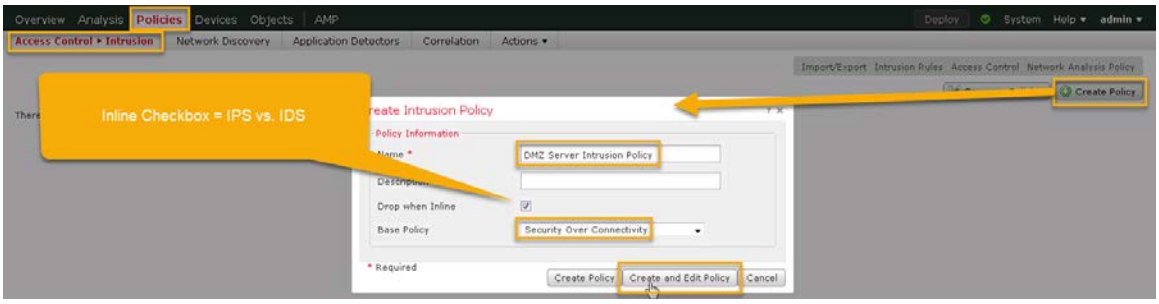
235. Click the **Create Policy** button and use the following to create the policy:

    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.)

236. Click the **Create and Edit Policy** button.

Figure 359. Create Intrusion Policy



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

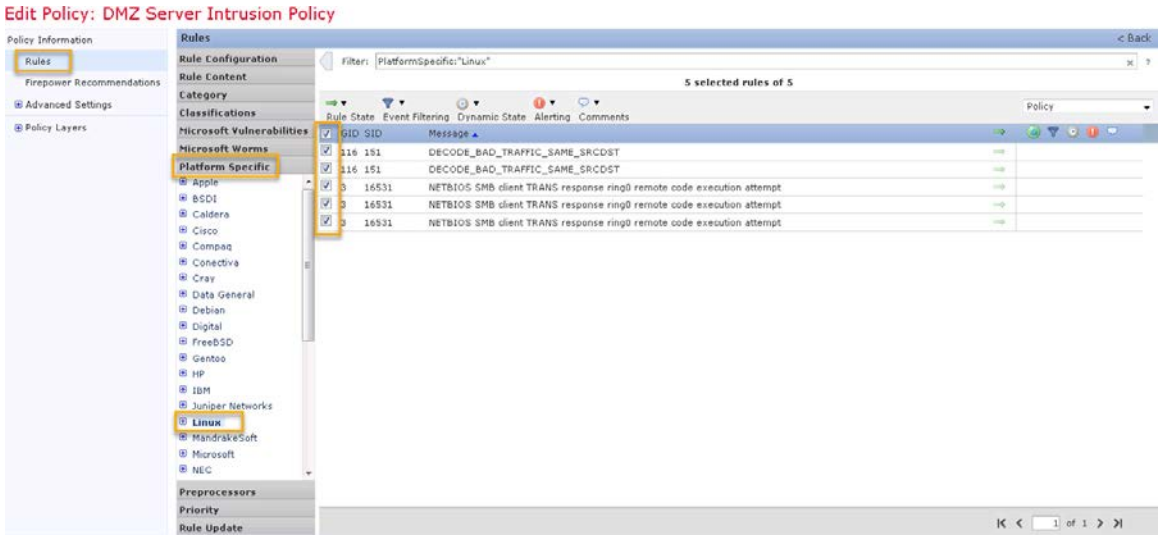
https://t.me/learningnets

237. 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 360. Select all the Linux rules

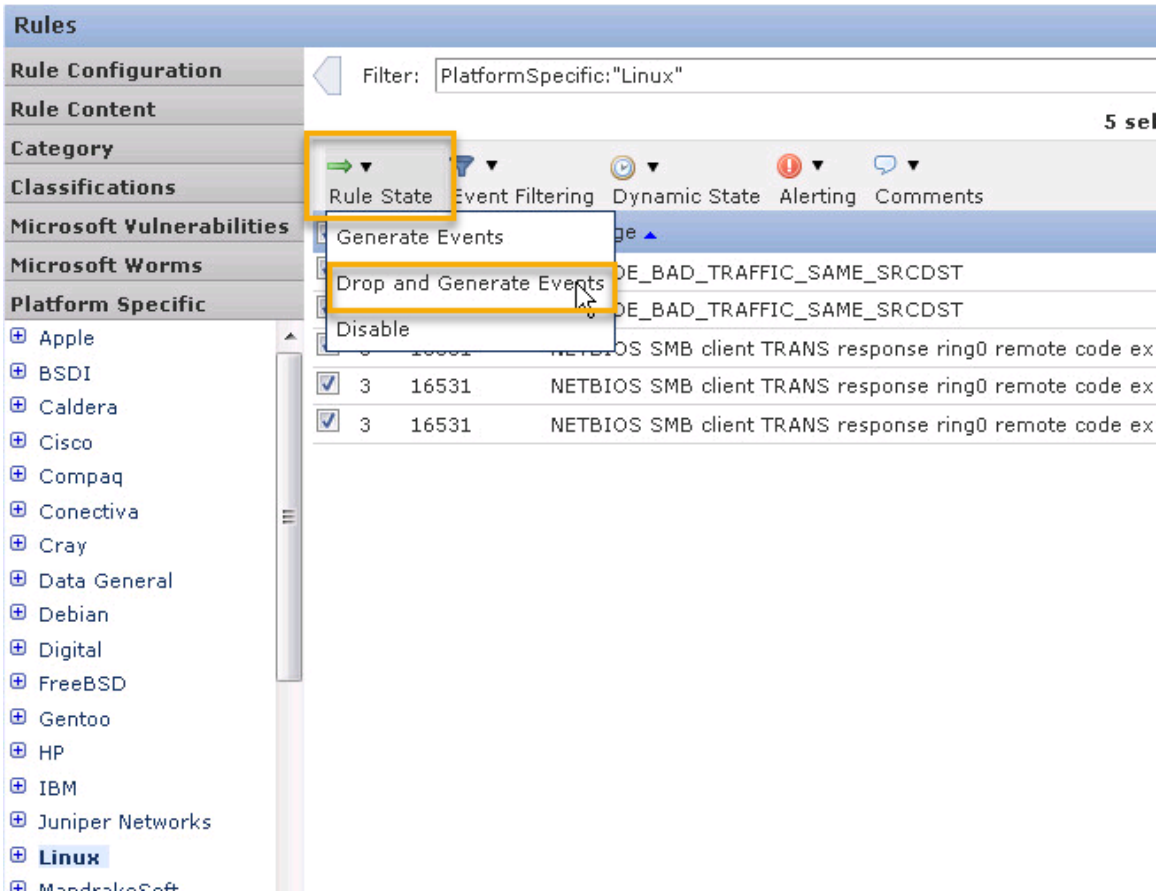


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

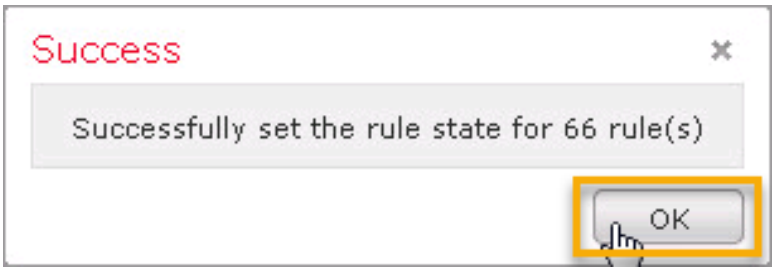
c. Click **Rule State** and select **Drop and Generate Events** option.

Figure 361. Select Drop and Generate Events



d. Click **OK** on the Success popup window.

Figure 362. Click OK



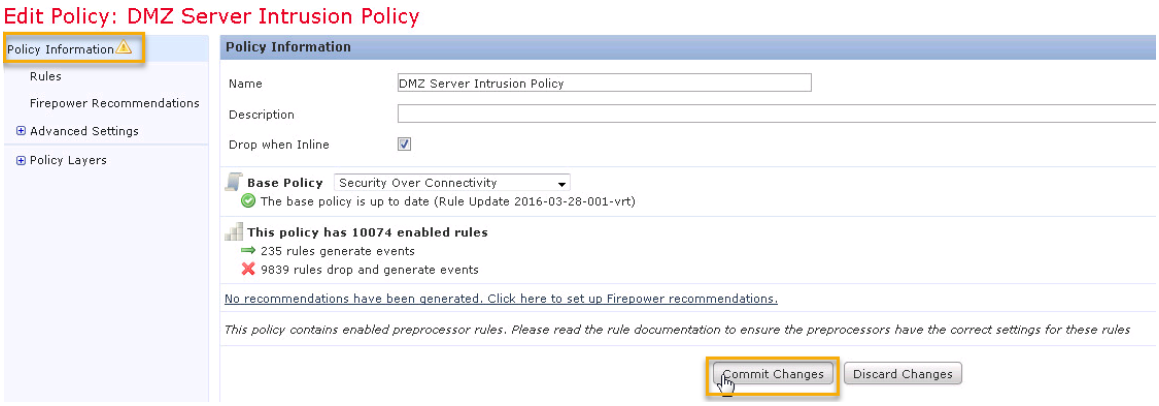
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

238. Click the **Policy Information** link.

239. Click **Commit Changes**.

Figure 363. Commit changes



240. 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 364. Give justification for rule



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

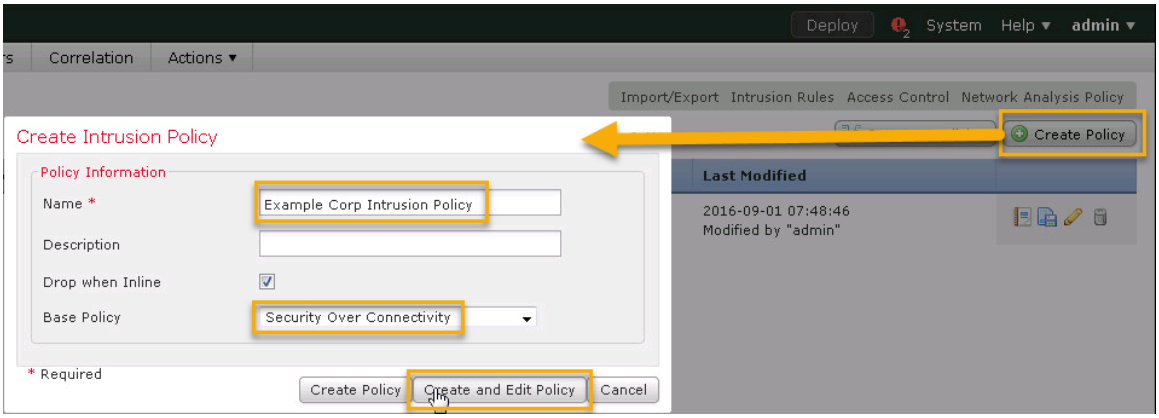
241. Click the **Create Policy** button again and use the following to create the policy:

    a. Name: **Example Corp Intrusion Policy**

    b. Base Policy: **Security over Connectivity**

242. Click the **Create and Edit Policy** button.

Figure 365. Create Intrusion Policy



243. Once the policy has been created click the **Firepower Recommendations** link from the left side menu.

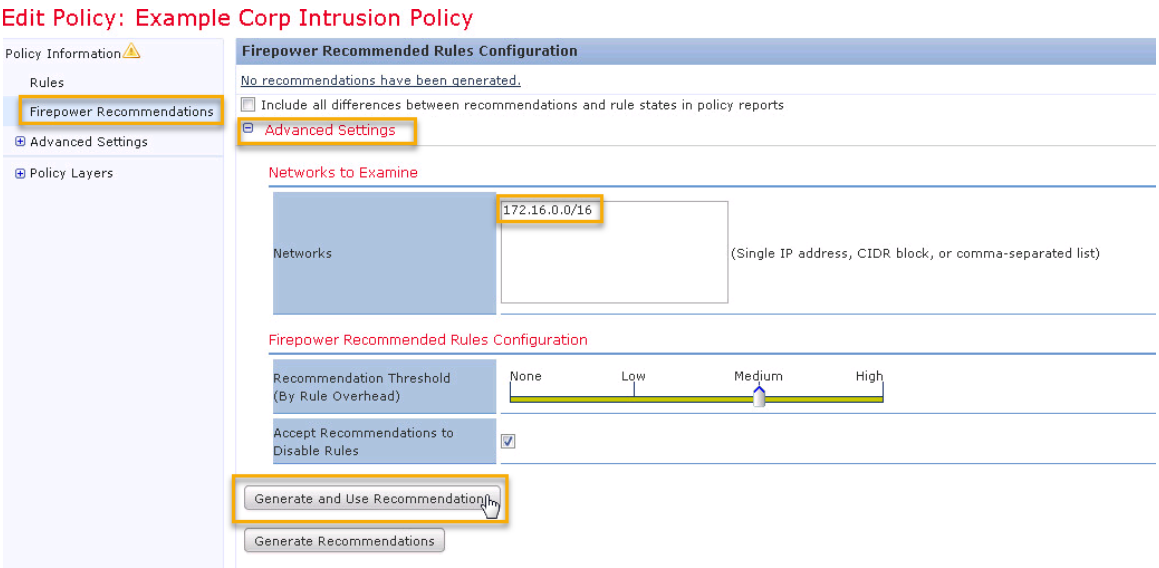
244. Expand the **Advanced Settings** option in the right hand pane.

245. In the **Networks to Examine** field add **172.16.0.0/16** to better target the Example Corp networks.

246. 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 366. Build Firepower Recommendations

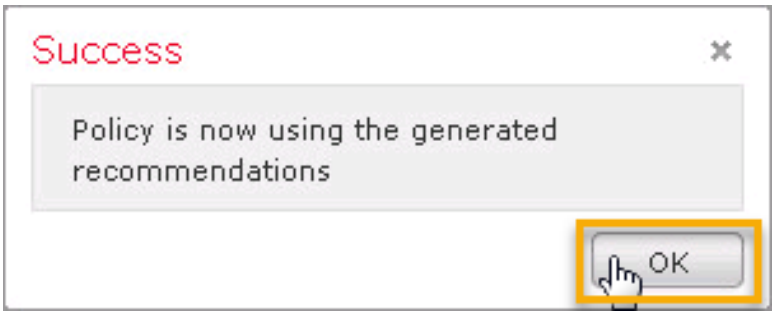


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

247. This process can take a minute or two. Click **OK** when the Success popup window appears.

Figure 367. Click OK



248. 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.

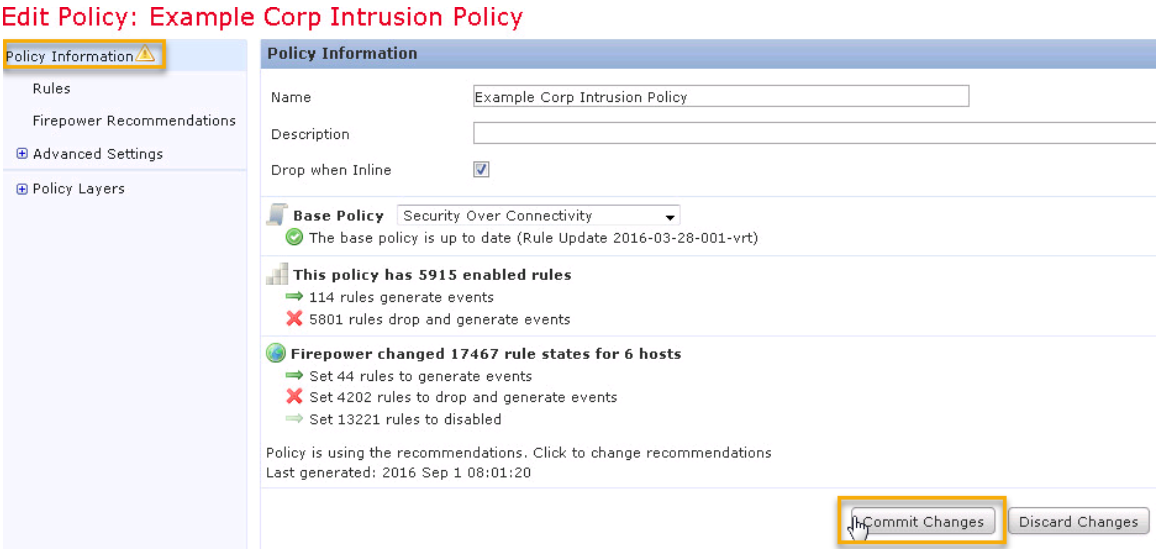
Figure 368. View Recommendation's Summary Info



249. Click the **Policy Information** link.

250. Click **Commit Changes**.

Figure 369. Commit Changes

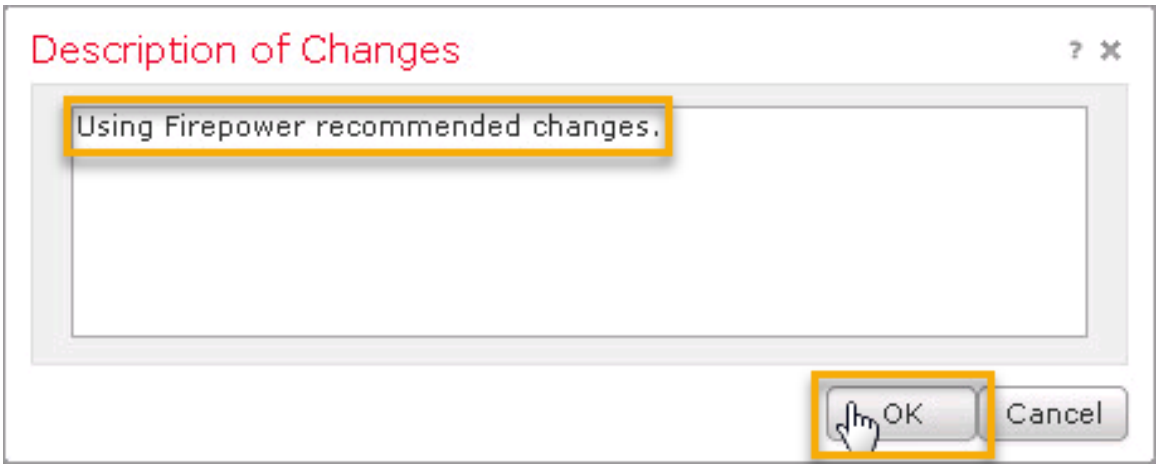


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

251. In the Description of Changes popup window type "**Using Firepower recommended changes.**" and click **OK**.

Figure 370. Add Comment



252. Time to apply the newly created Intrusion Policies. Navigate to **Policies > Access Control > Access Control**.

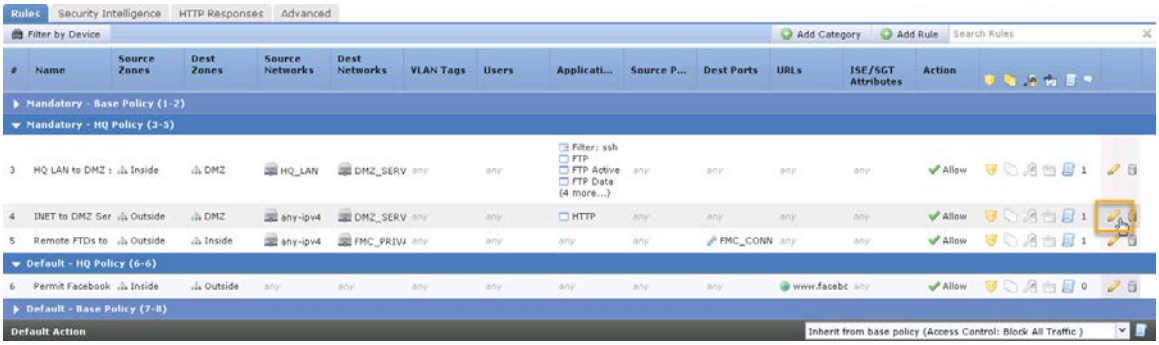
253. **Edit** the **HQ Policy**.

Figure 371. Edit HQ Policy ACP



254. **Edit** the **INET to DMZ Server** rule (should be rule #4).

Figure 372. Edit Rule



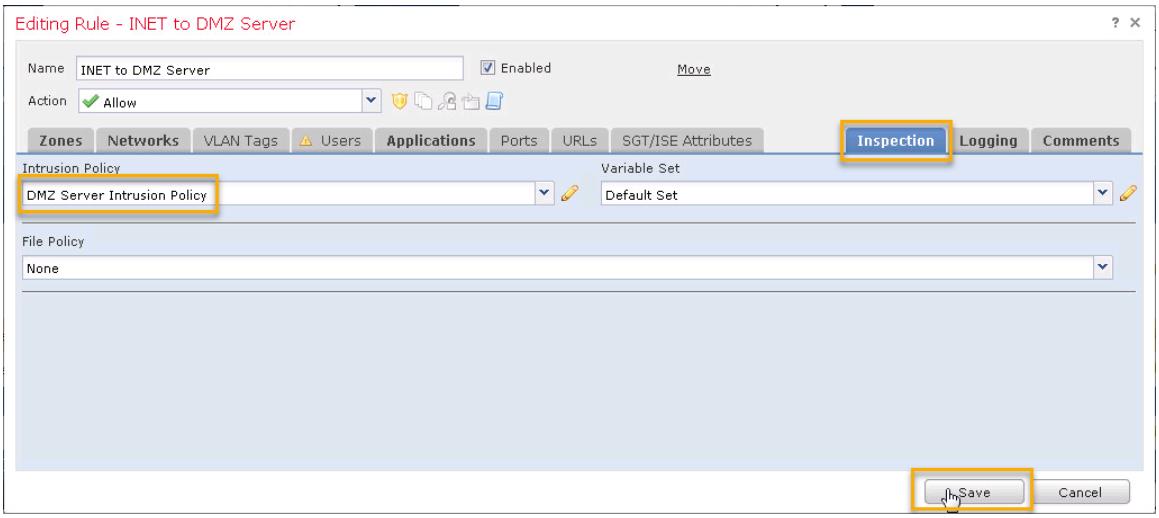
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

255. Click the **Inspection tab** and select the **DMZ Server Intrusion Policy** for the Intrusion Policy.

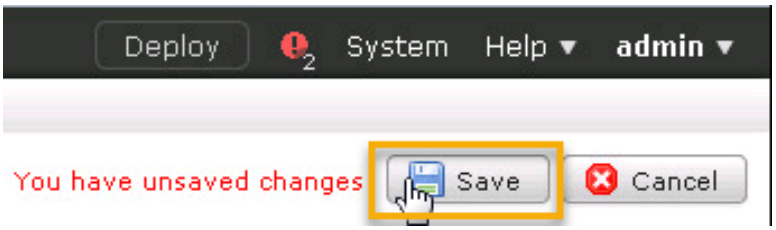
256. Click **Save**.

Figure 373. Configure Inspection tab and Save



257. Click **Save** to save these changes to the FMC.

Figure 374. Save changes to FMC



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.

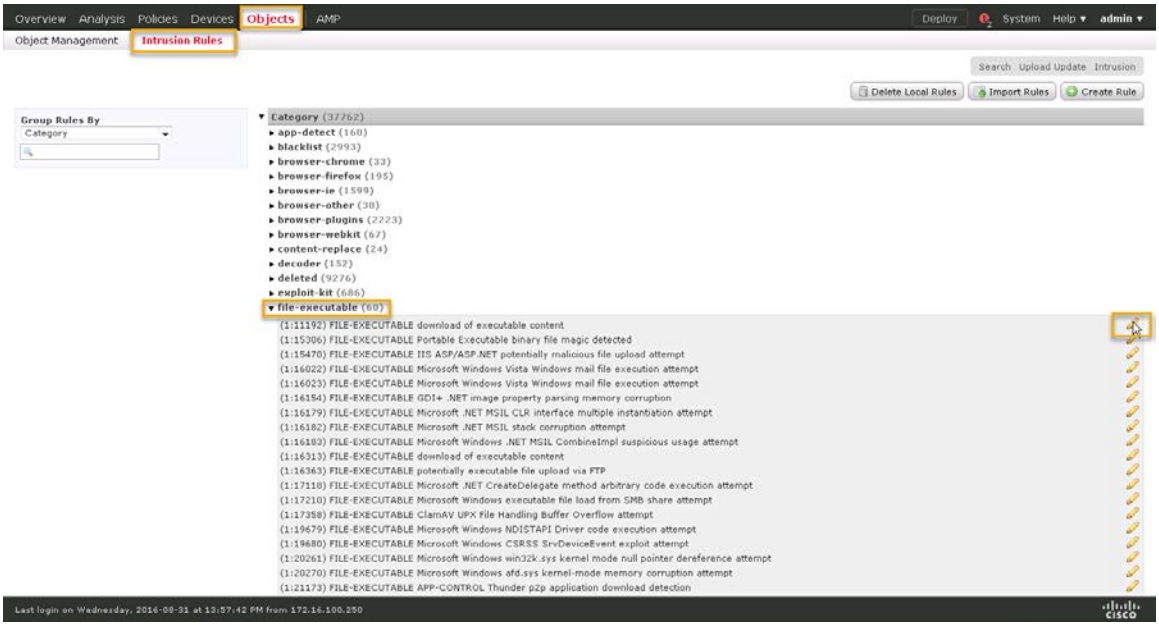
Variable Sets

258. 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

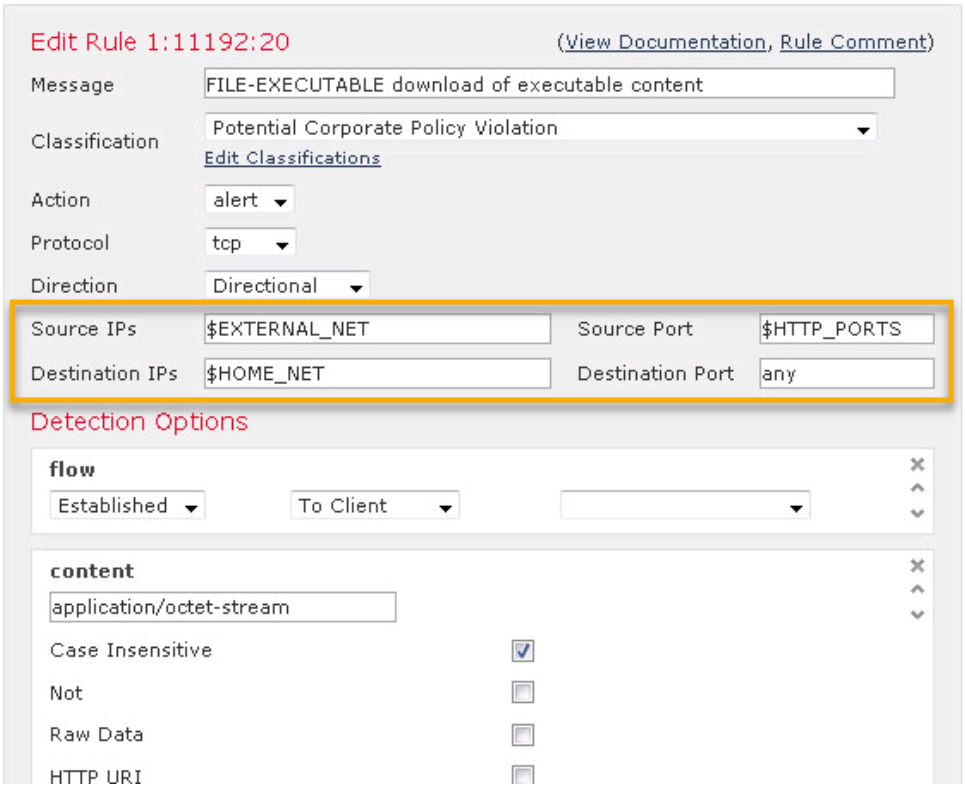
https://t.me/learningnets

Figure 375. Edit an Intrusion Rule Object



259. Notice the **$EXTERNAL_NET**, **$HTTP_PORTS**, and **$HOME_NET** variables being used in this rule.

Figure 376. Use of Variable Set variables



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

260. Navigate to **Objects > Object Management** and from the list of item in the left column select **Variable Set**.

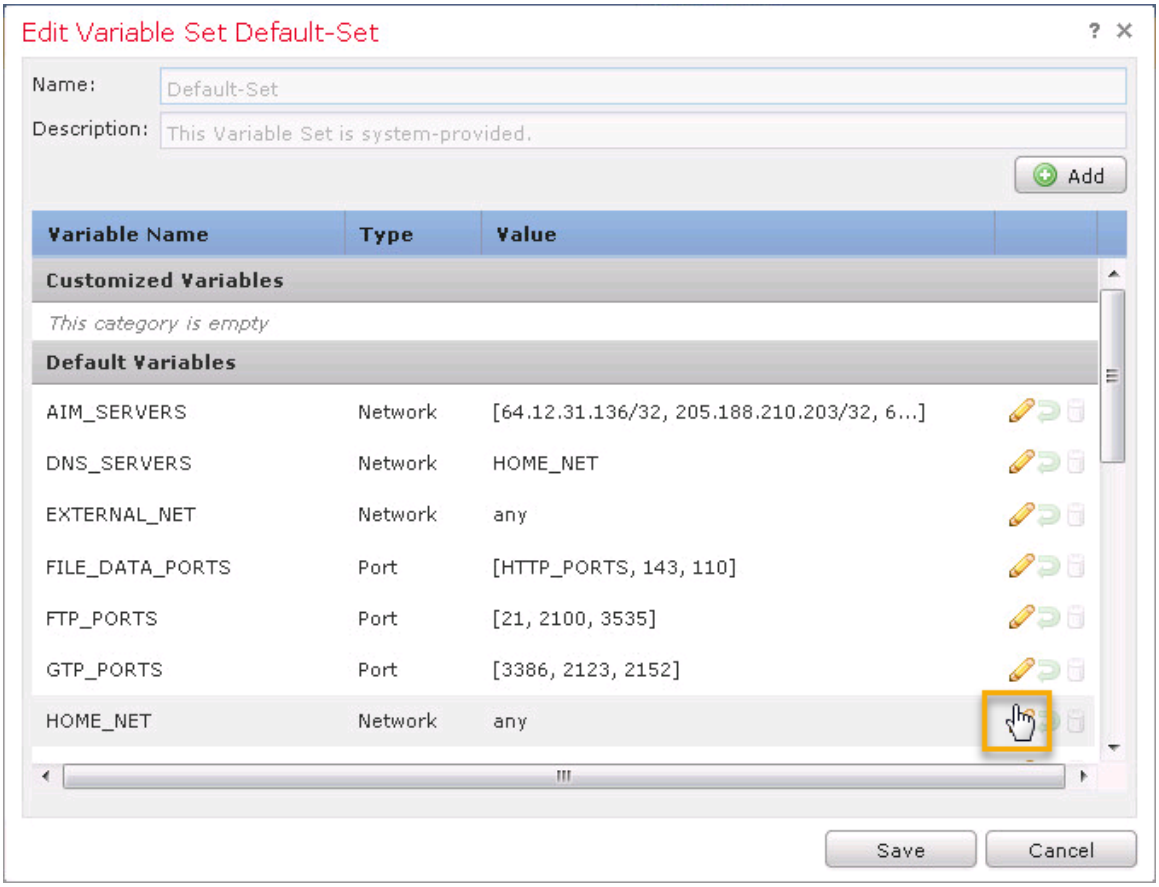
261. The Default-Set is the default variable set that is being used throughout the configurations we've created or used so far. Instead of creating a new Variable Set and needing to apply it everywhere it is best just to modify the Default-Set to match your network's settings. **Edit** the **Default-Set**.

Figure 377. Edit Default Set Variable Set



262. In the Edit Variable Set Default-Set popup window **edit** the **HOME_NET** variable.

Figure 378. Edit HOME_NET



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

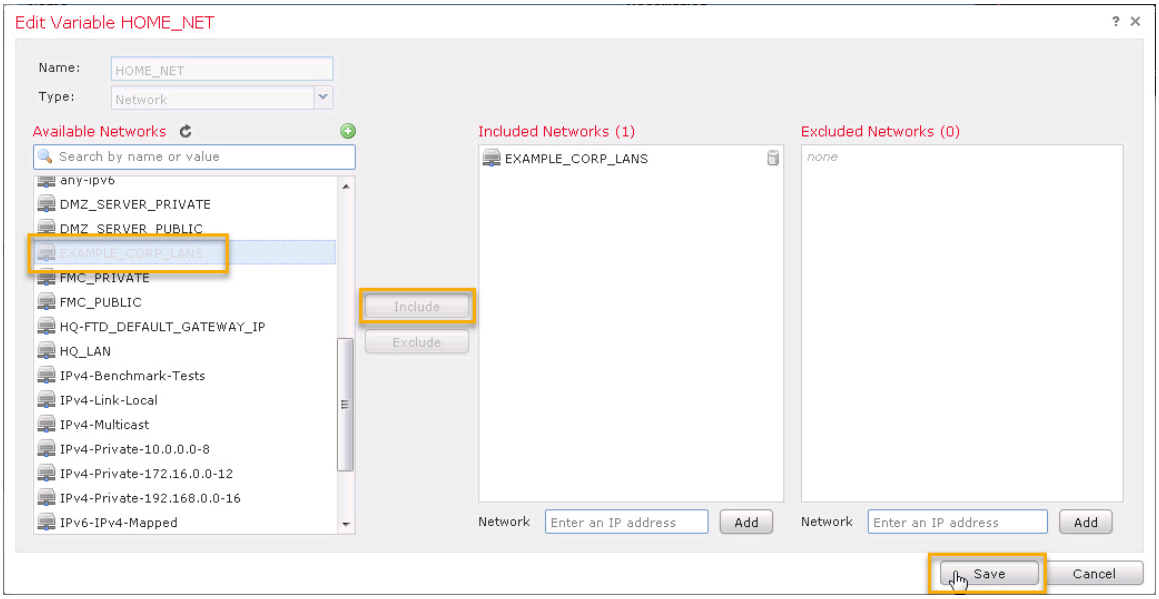
https://t.me/learningnets

263. 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 379. Save HOME_NET changes

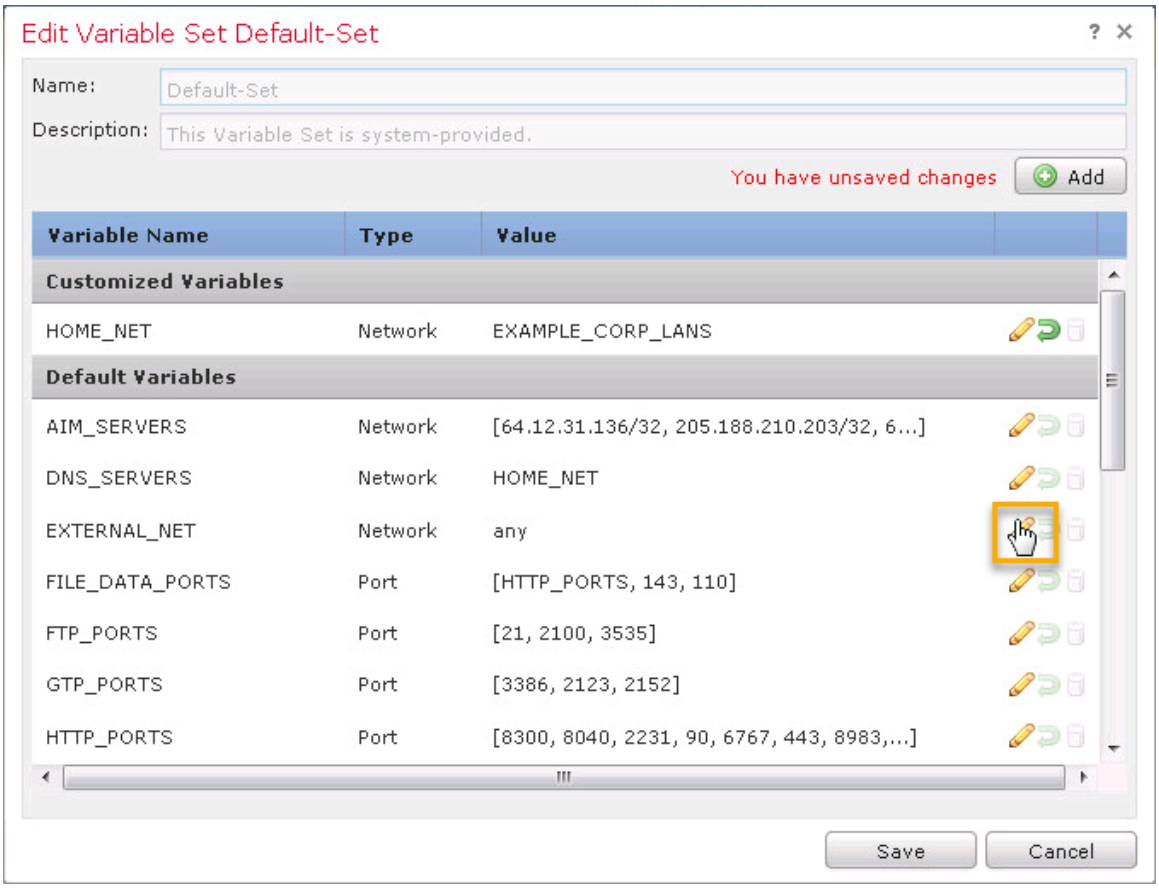


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

264.**Edit** the **EXTERNAL_NET** variable.

Figure 380. Edit EXTERNAL_NET



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

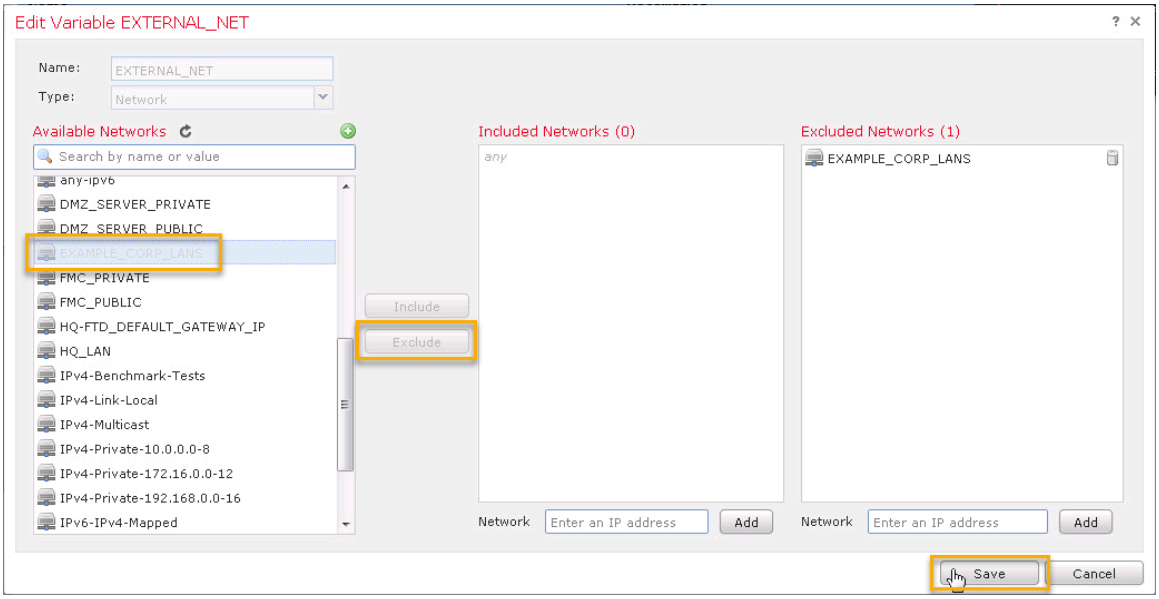
https://t.me/learningnets

265. 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 381. Save EXTERNAL_NET

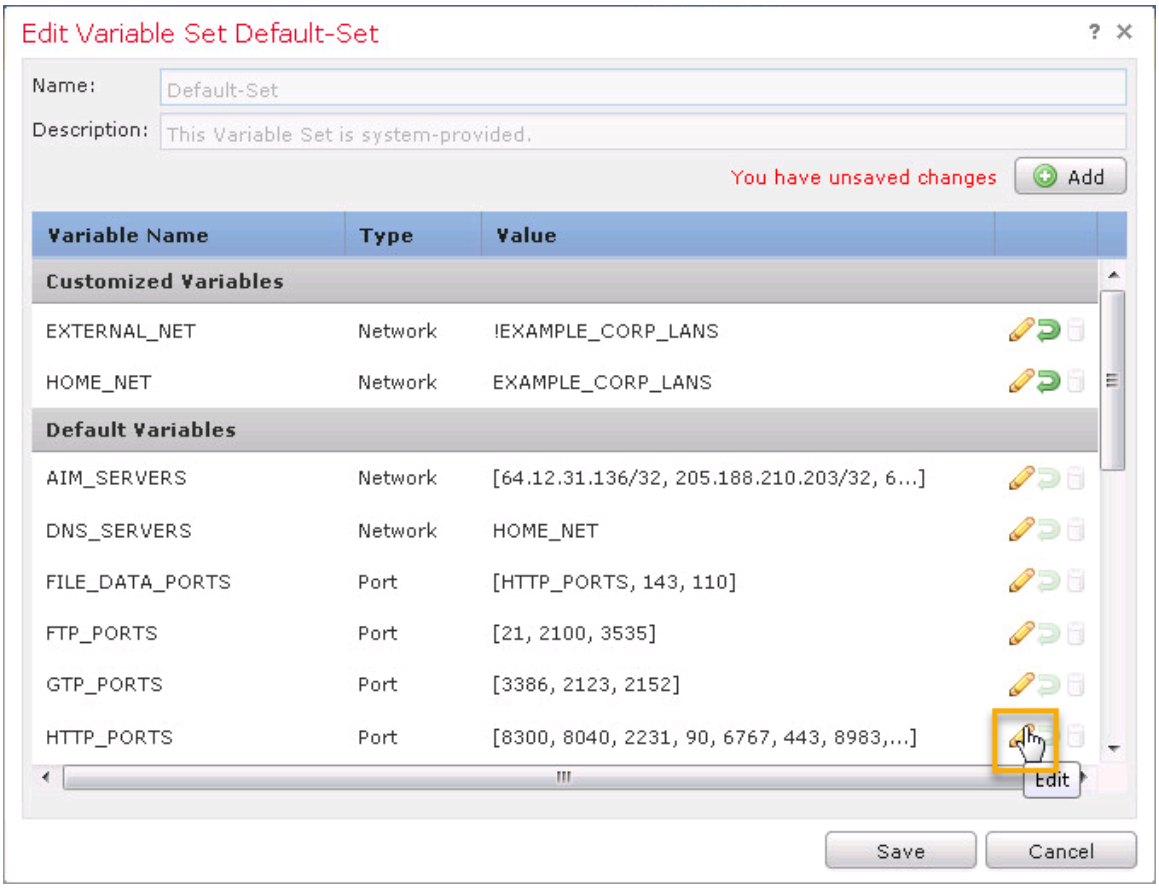


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

266.Let's pretend that Example Corp has a special HTTP application that runs on port 8383. **Edit** the **HTTP_PORTS** variable.

Figure 382. Edit HTTP_PORTS



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

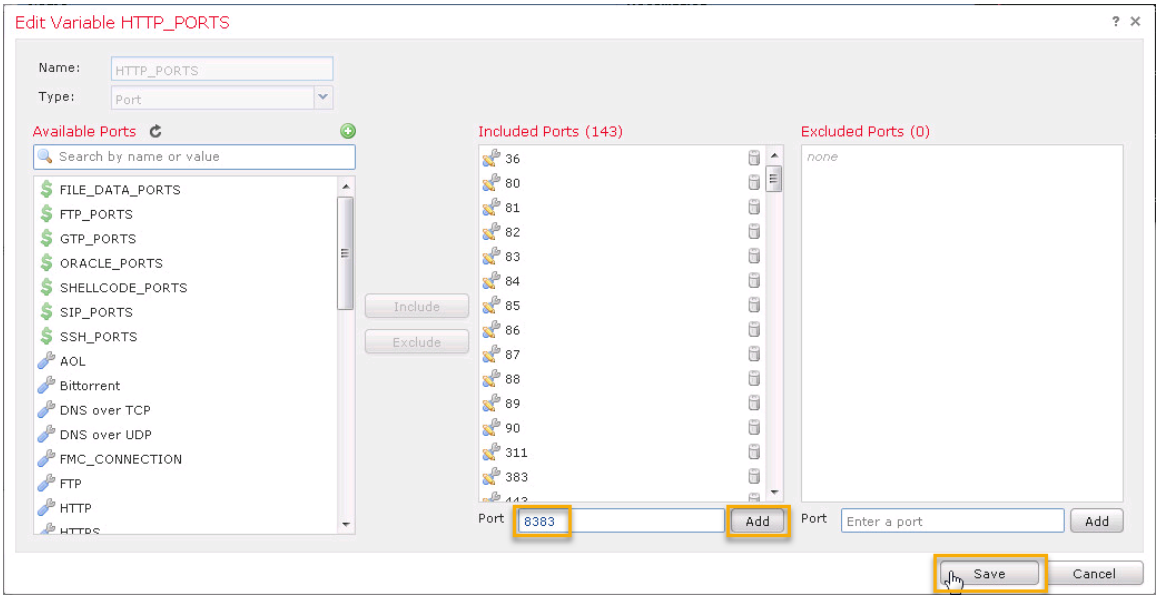
https://t.me/learningnets

267. 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 383. Save HTTP_PORTS variable

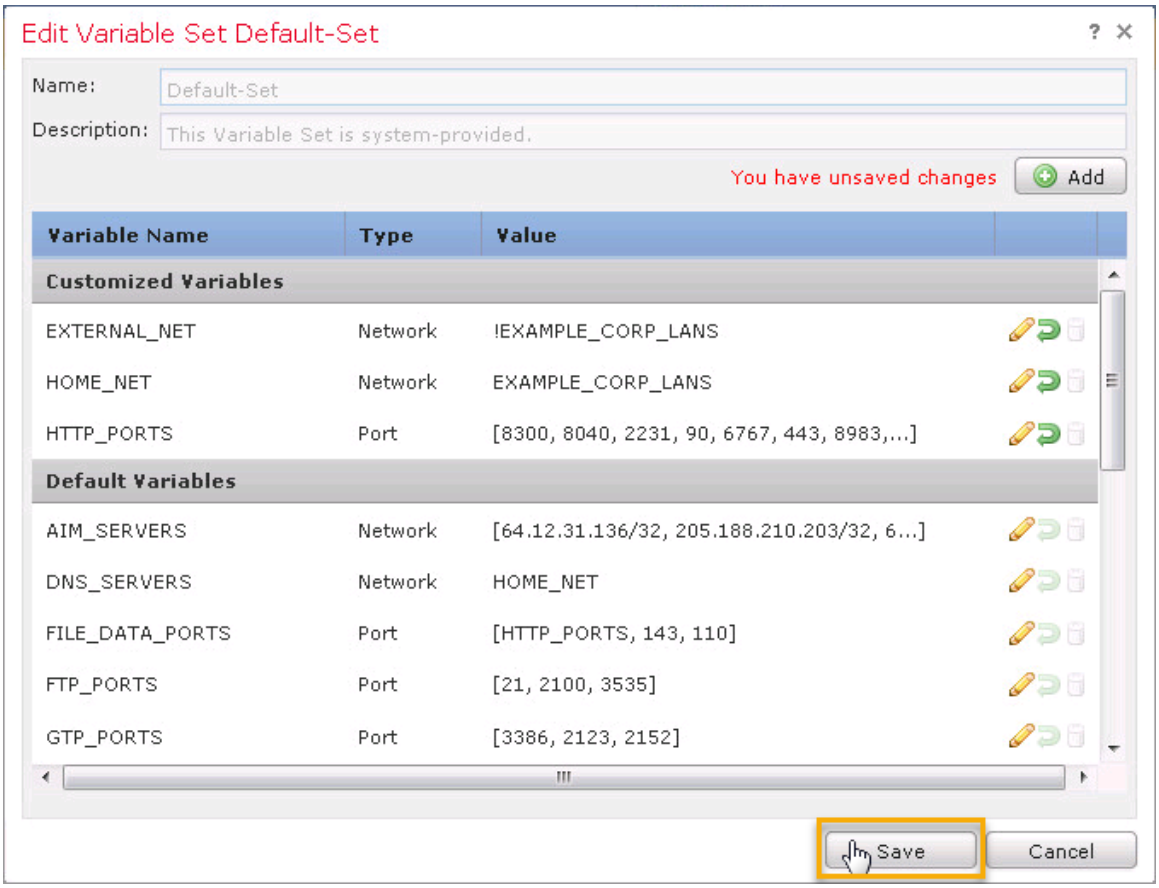


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

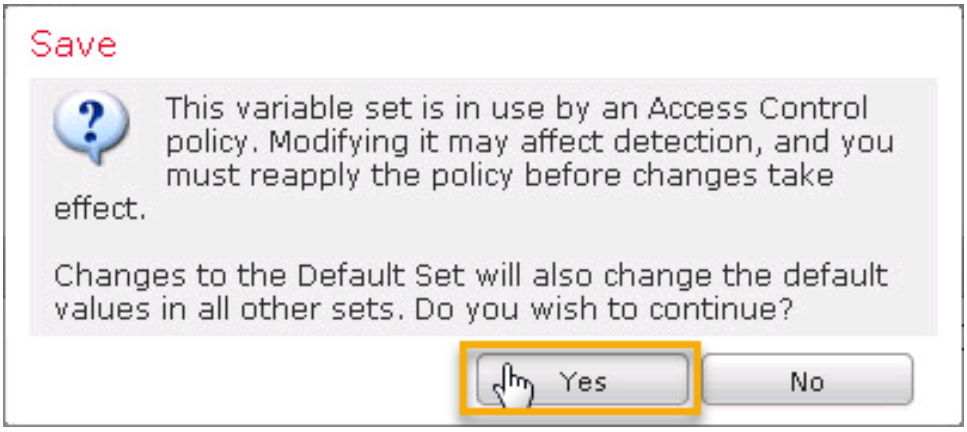
268. Click **Save** to save the Default-Set variable set.

Figure 384. Save Default Set Variable Set



269. In the popup warning window click **Yes** to change the default values.

Figure 385. Click Yes



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

270. 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**.

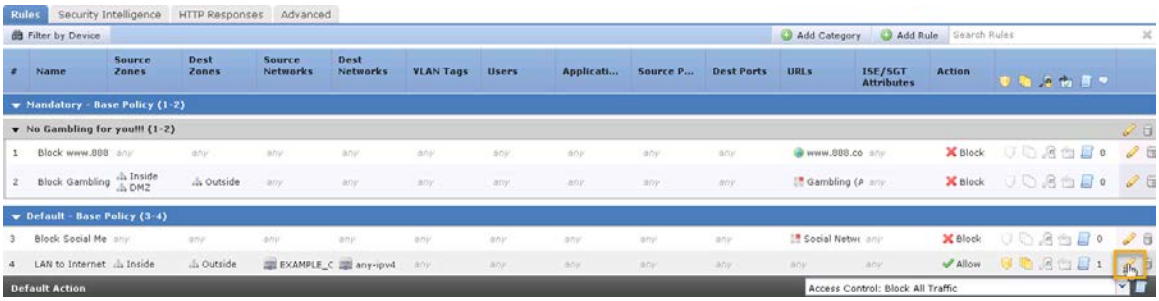
271. **Edit** the **Base Policy**.

Figure 386. Edit Base Policy ACP



272. **Edit** one of the rules.

Figure 387. Edit a rule



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

273. 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.

274. Click **Cancel** to exit editing this rule. (If asked, click **Yes** to not save changes.)

Figure 388. See where Variable Set is used

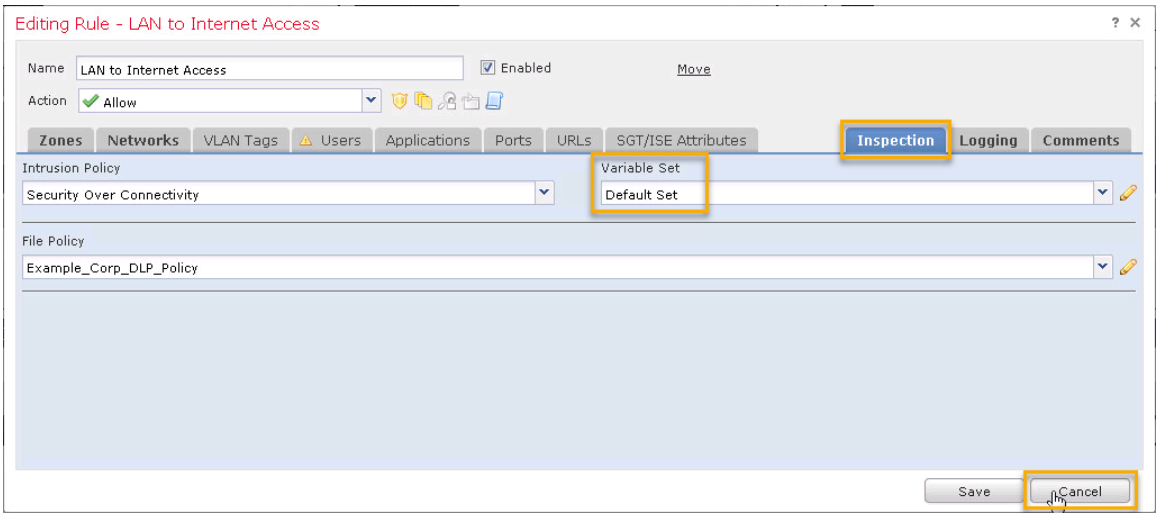
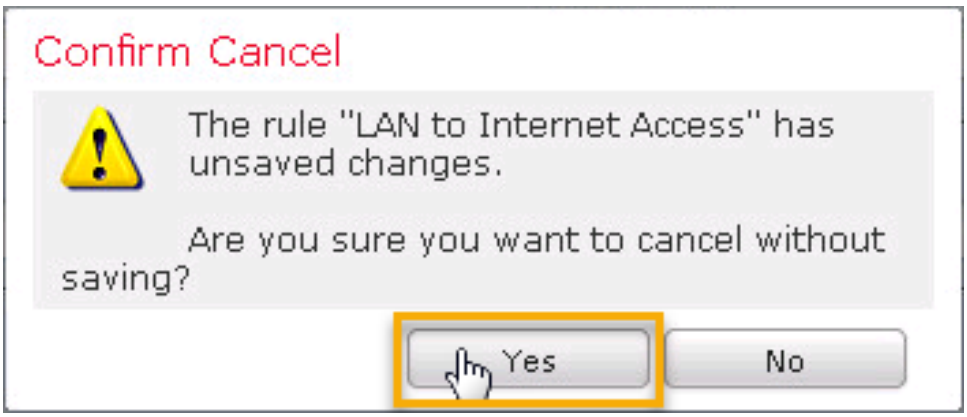


Figure 389. Confirm Cancel



275. 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.)

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

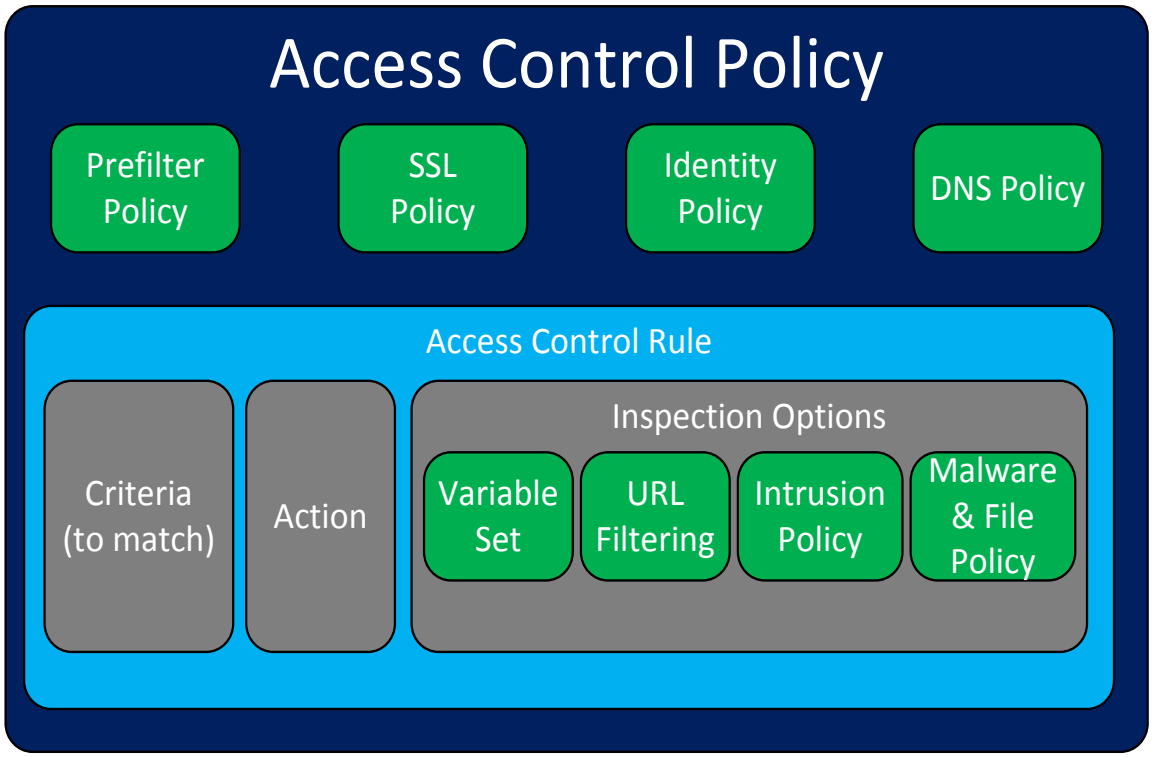
https://t.me/learningnets

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 390. 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

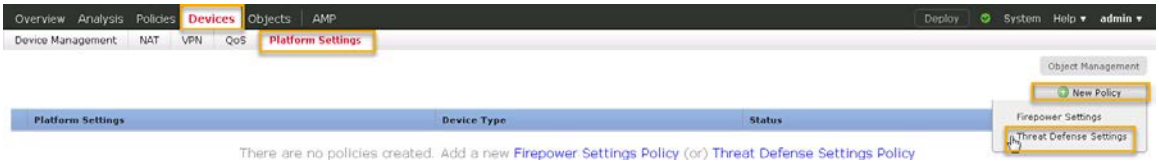
Example Corp wants to permit SSH to its FTD device’s data plane IP addresses and have a common SMTP server that is used by all FTD devices. They also would like to increase the syslog buffer size to store more messages and instead of overwriting the overflow messages export them to an FTP server.

Configure Custom Platform Settings for Example Corp FTD Devices

276. Navigate to **Devices > Platform Settings**.

277. Click on **New Policy** and then select **Threat Defense Settings** from the dropdown list.

Figure 391. Create new policy



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

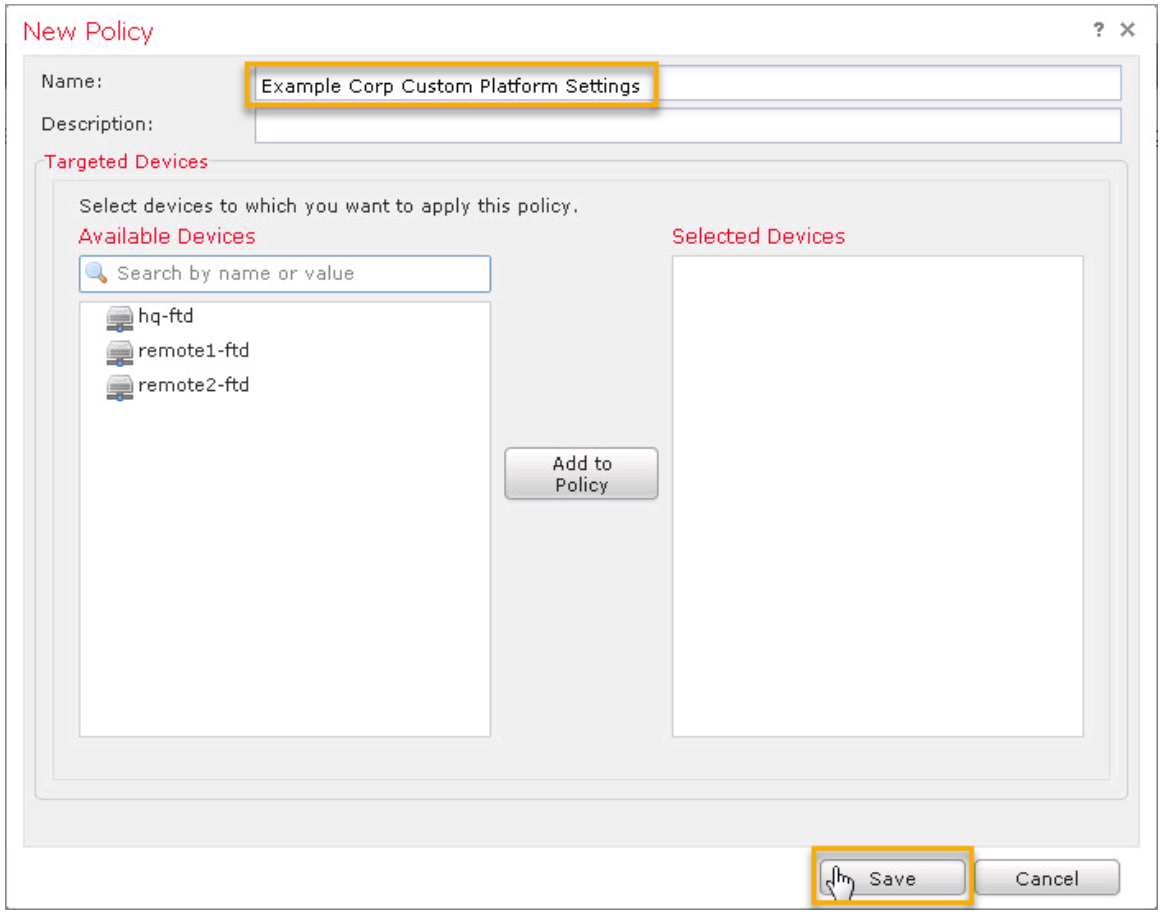
https://t.me/learningnets

278. 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 392. Save policy

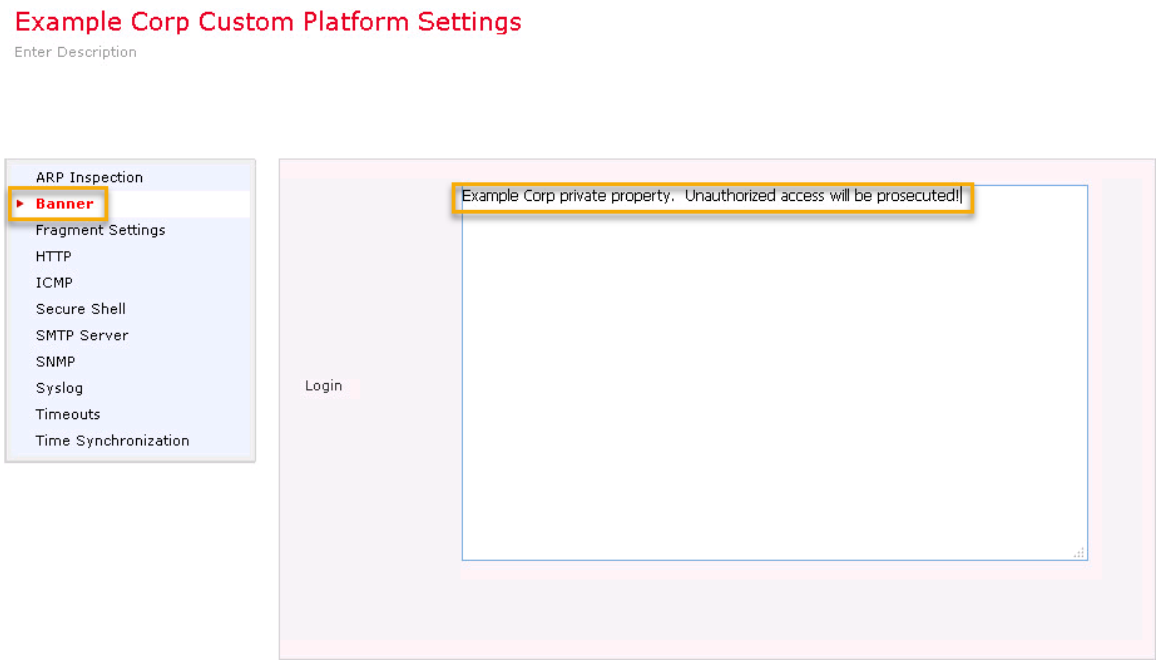


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

279. Click the **Banner** menu item and fill in the field with the following: **Example Corp private property. Unauthorized access will be prosecuted!**

Figure 393. Configure Banner



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

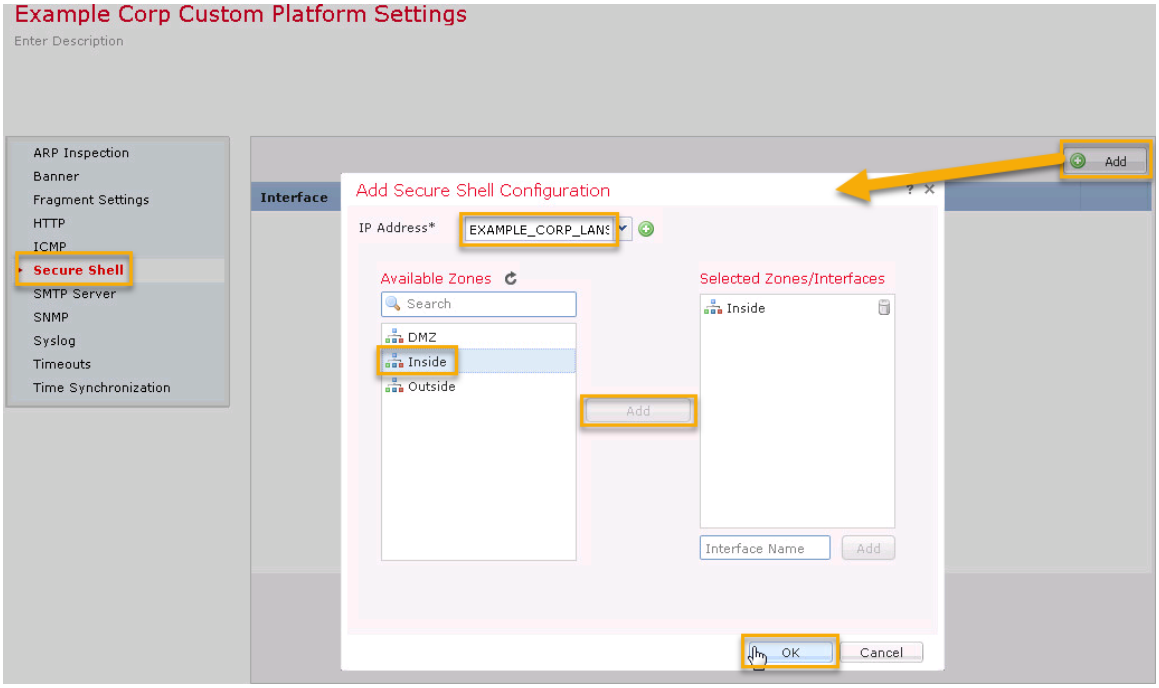
280. Click the **Secure Shell** menu item and then click **Add**.

a. IP Address: **EXAMPLE_CORP_LANS**

b. Add the **Inside** zone to **Selected Zones/Interfaces**.

c. Click **OK**.

Figure 394. Configure SSH



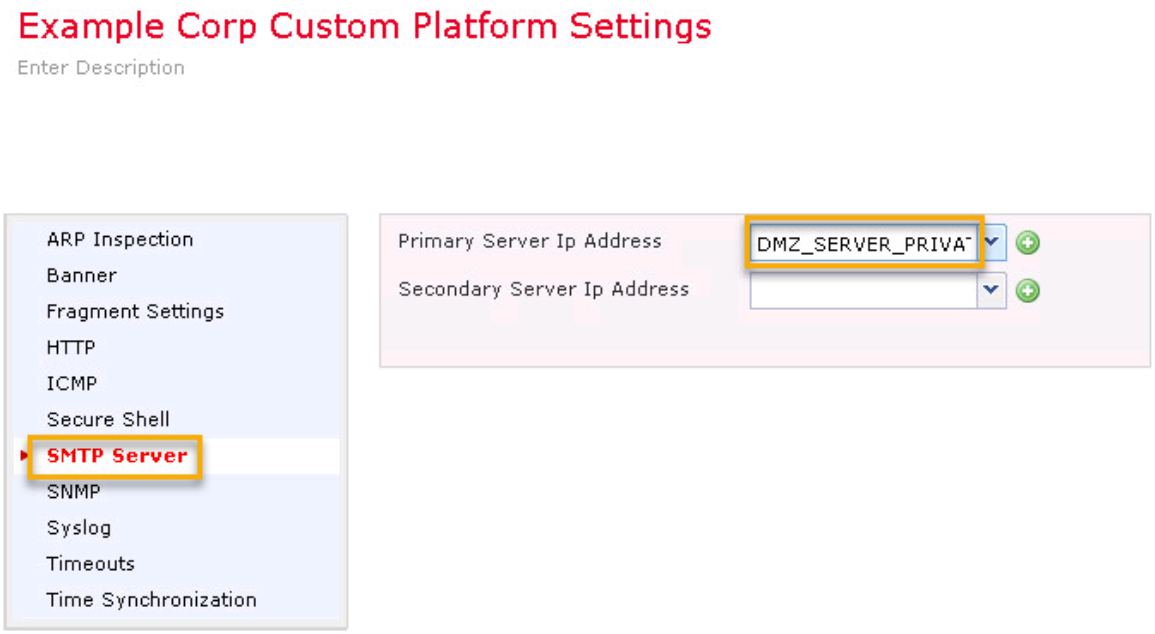
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

281. 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 395. Configure SMTP Server



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

282. Click the **Syslog** menu item:

283. 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**

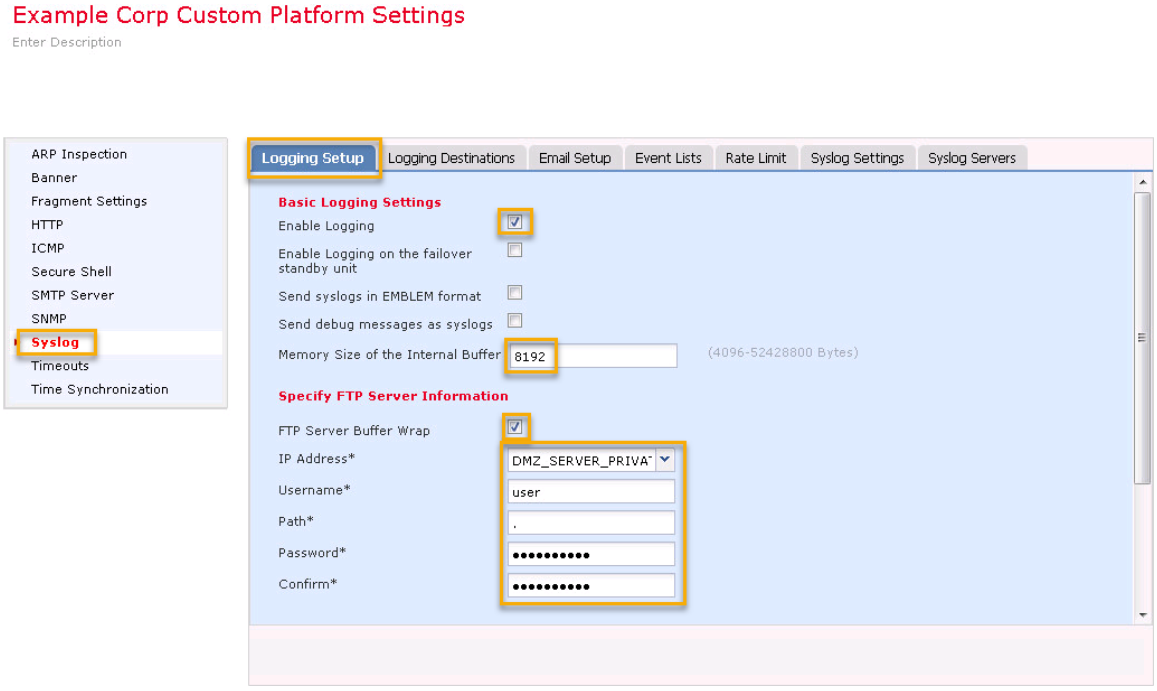
   e. Username: **user**

   f. Path: **.** (In Linux/UNIX the . “dot” represents the current directory.)

   g. Password: **C1sco12345**

   h. Confirm: **C1sco12345**

Figure 396. Part 1 Configure Syslog



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

284. On the **Logging Destinations tab**:

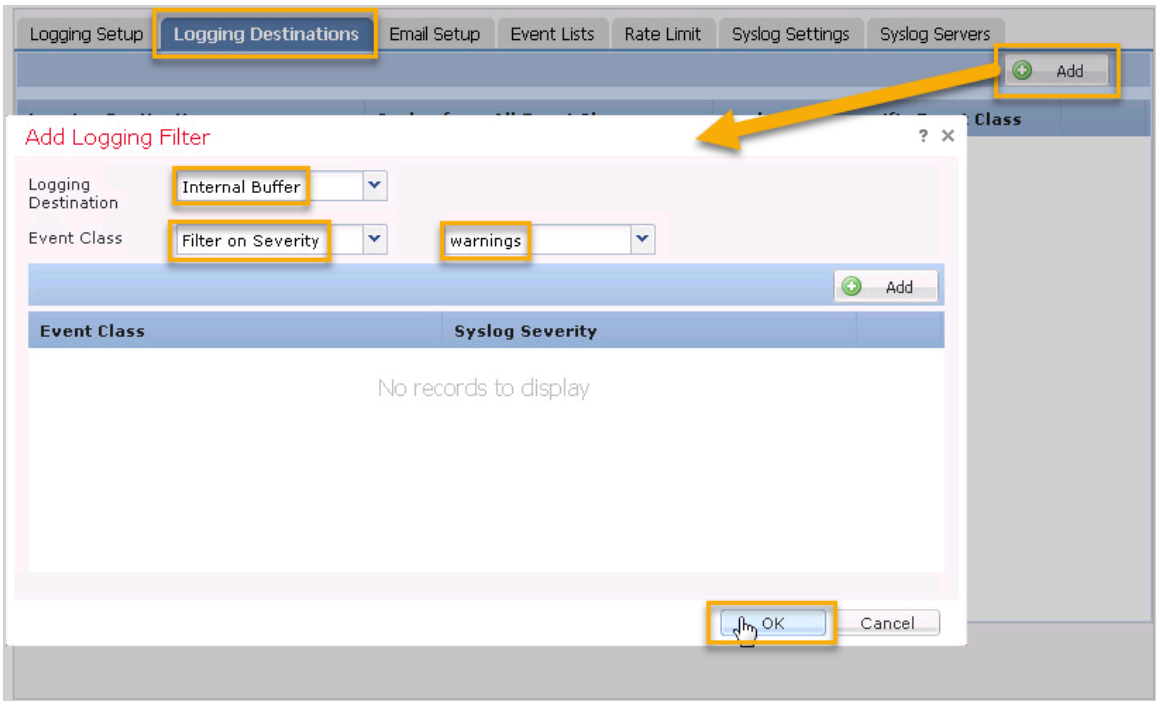
a. Click **Add**.

i. Logging Destination: **Internal Buffer**

ii. Event Class: **Filter on Severity** and then **warnings.**

iii. Click **OK**.

Figure 397. Configure Logging Destinations



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

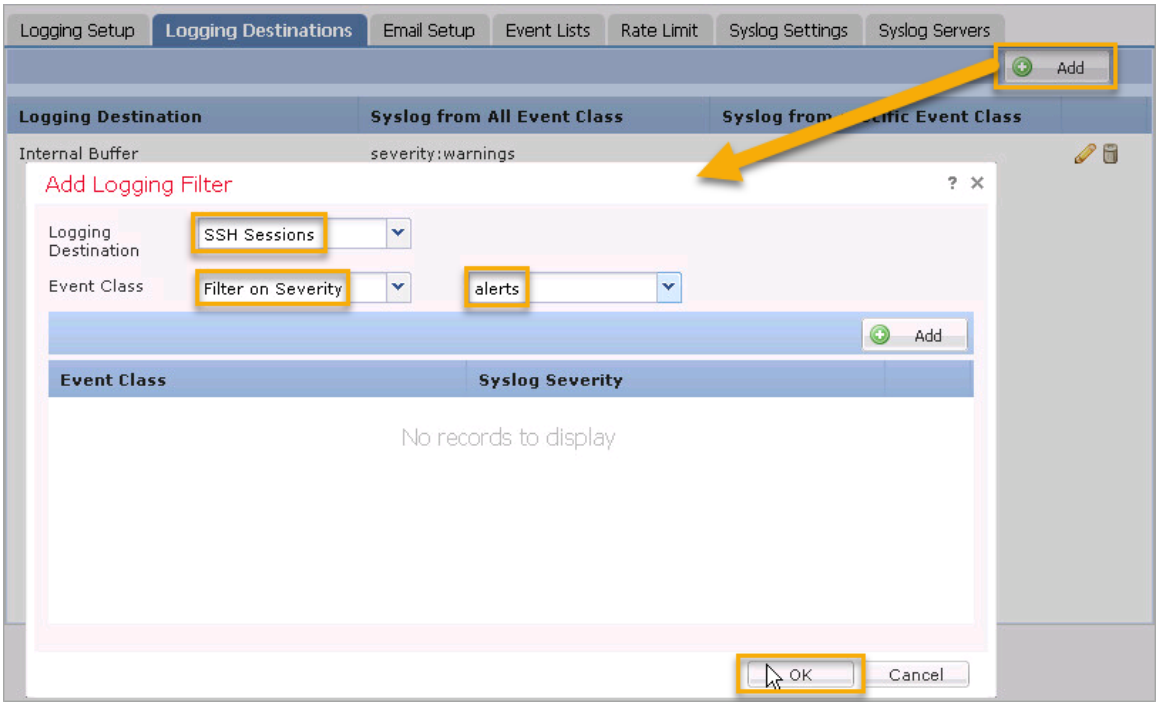
b. Click **Add**.

i. Logging Destination: **SSH Sessions**

ii. Event Class: **Filter on Severity** and then **alerts.**

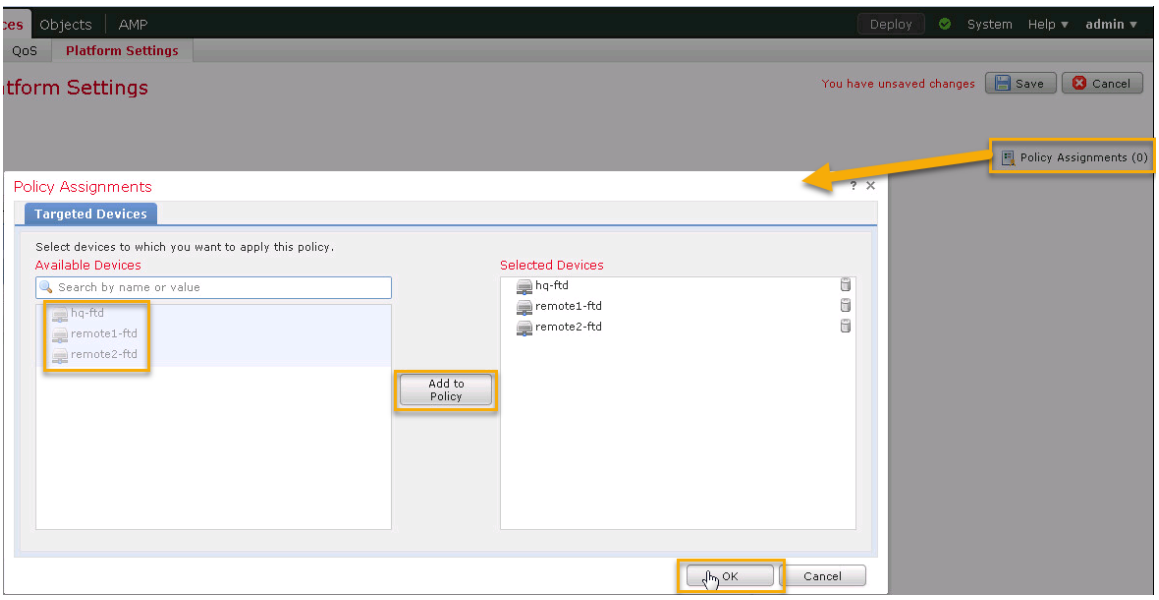
iii. Click **OK**.

Figure 398. Configure Logging Destinations



285. Click **Policy Assignments**. Select **all the FTD** devices, click **Add to Policy**, and then click **OK**.

Figure 399. Assign Policy



286. Click **Save**, **Deploy**, select **all the FTD** devices and then click **Deploy**.

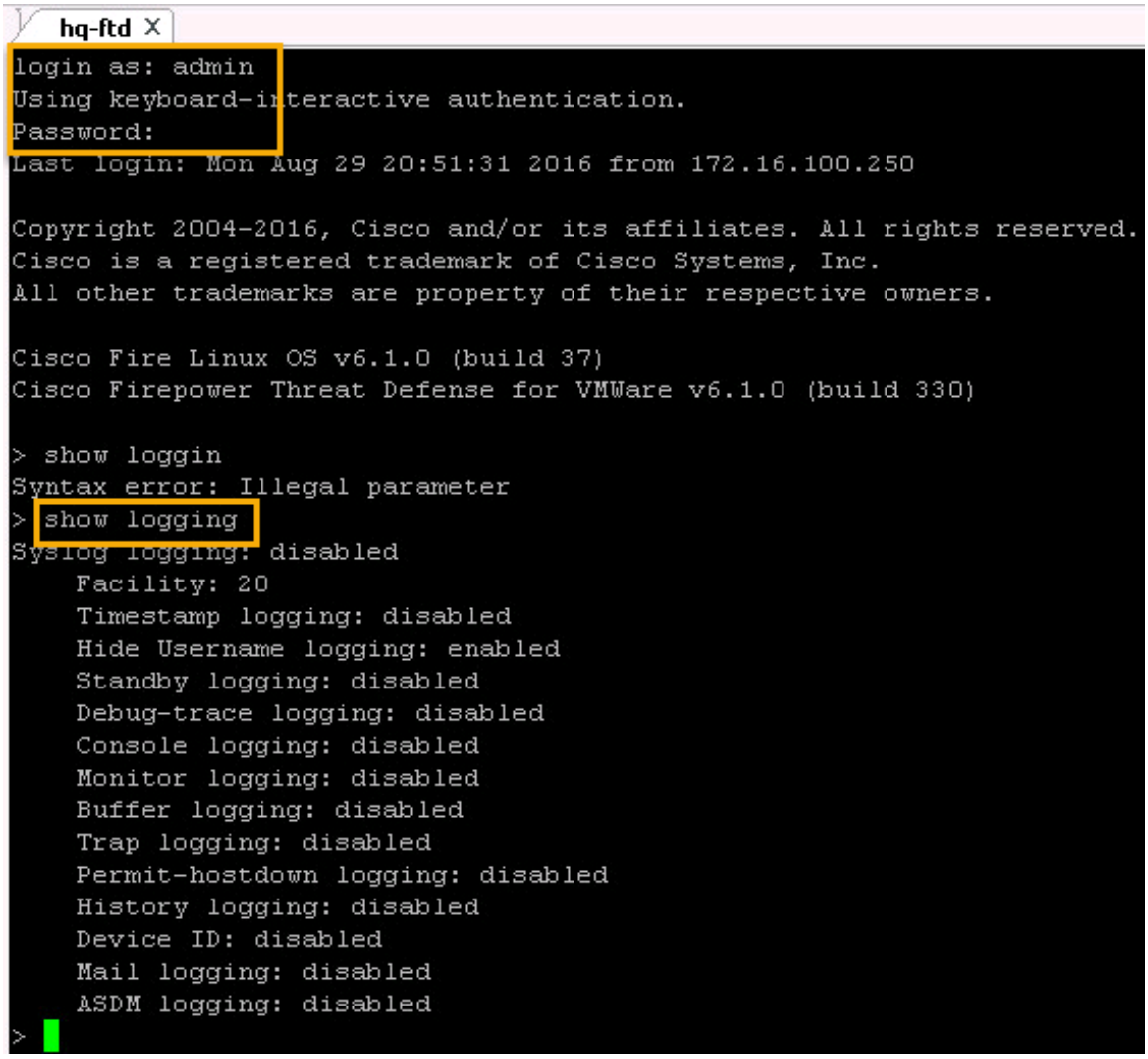
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Testing

287. While waiting for the deployment to complete use the **MTPuTTY** bookmark and ssh to the **hq-ftd (MGMT NIC)**. Log in as **admin**/**Admin123** and issue the command **show logging**. Notice that all the logging destination are disabled.

Figure 400. Show logging

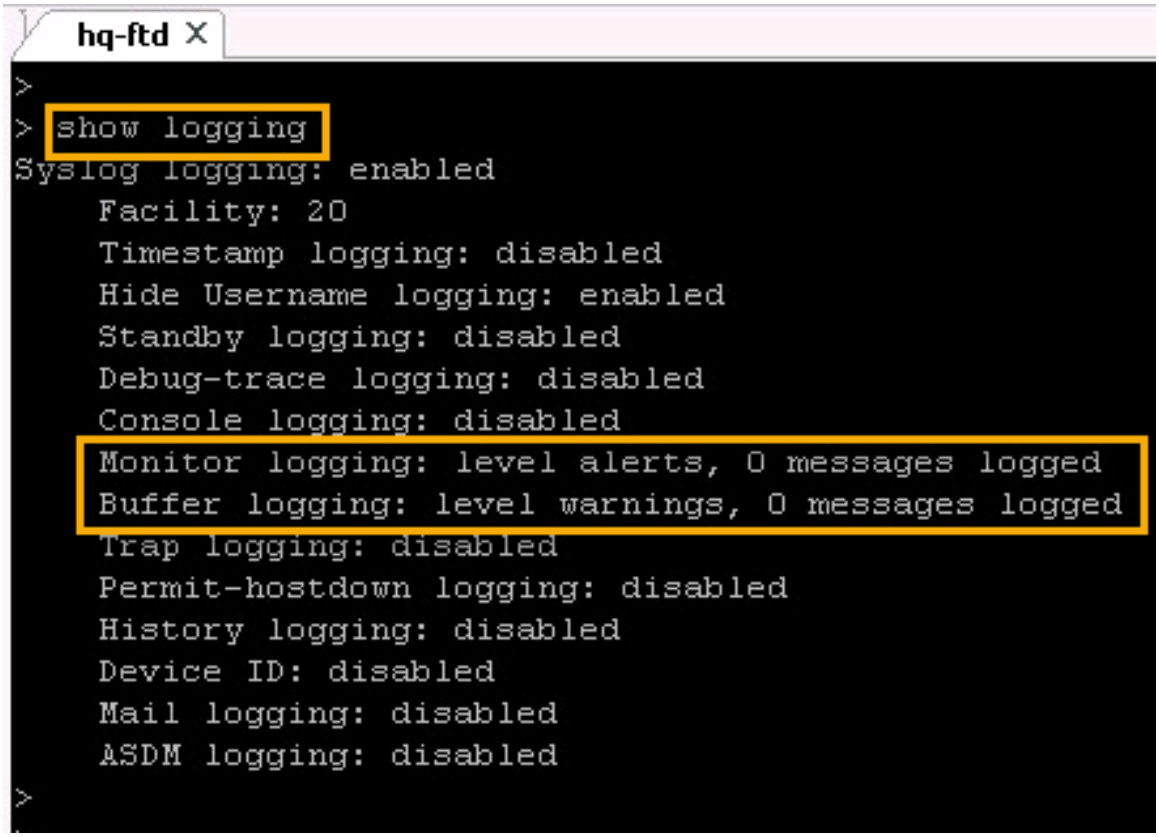


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

288. 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 401. Show logging



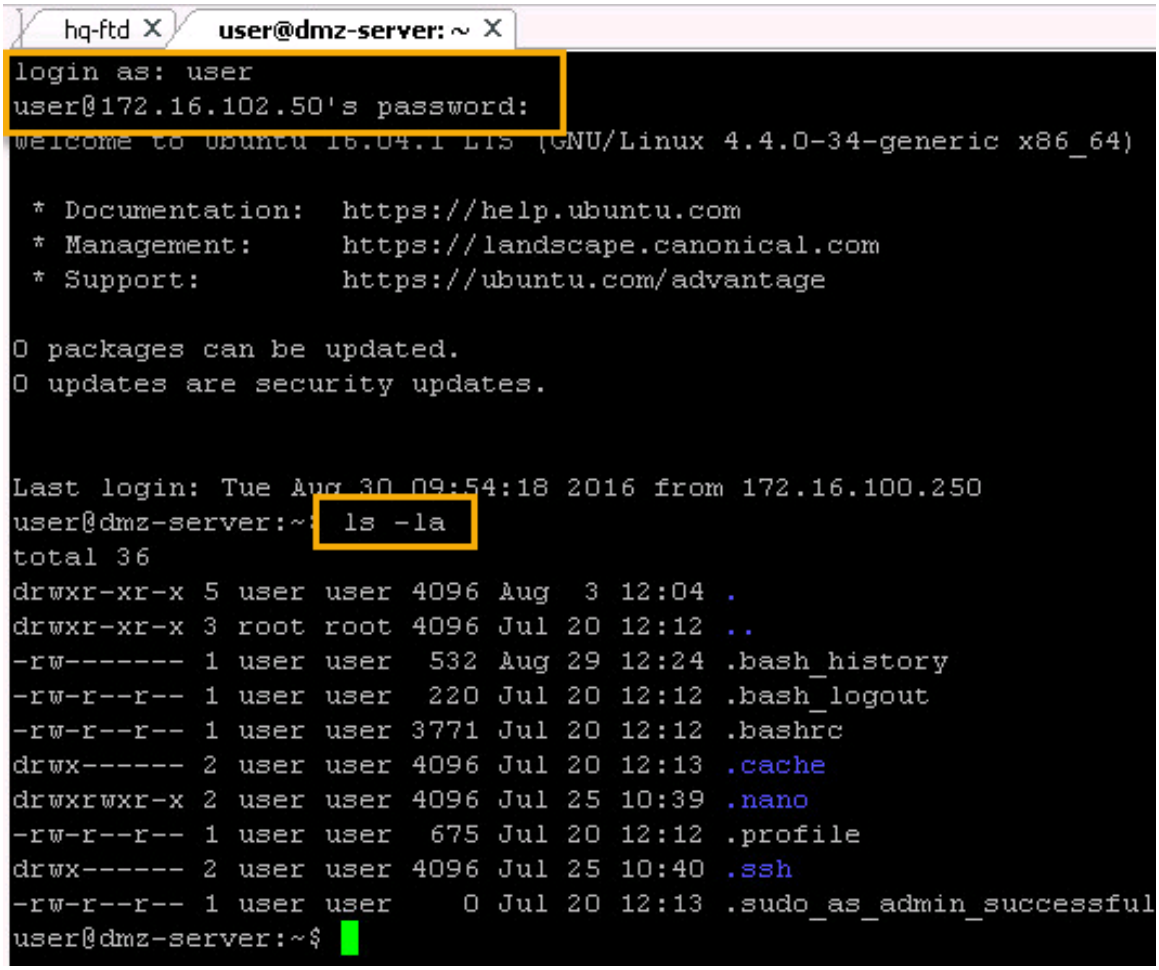
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

289. In **MTPuTTY** ssh to the **DMZ Server – Inside** and login as **user**/**C1sco12345**.

290. 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 402. Show directory on dmz-server

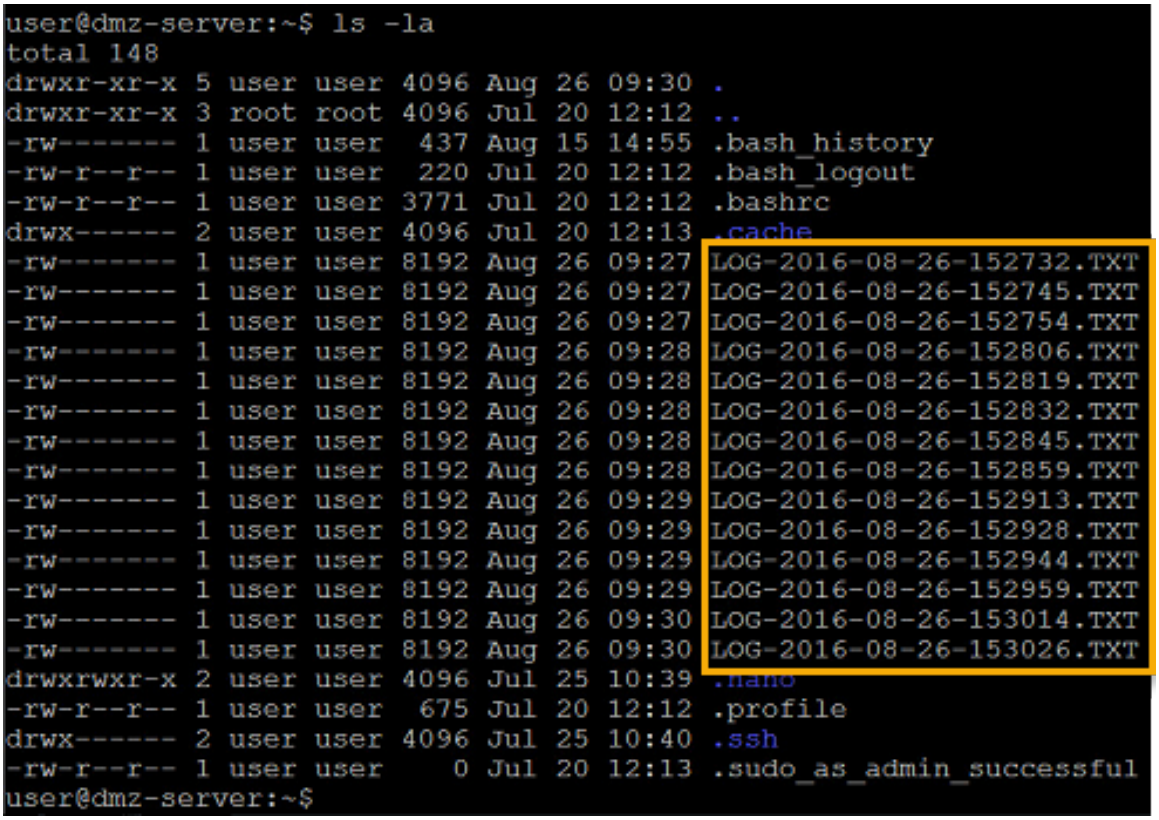


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 403. Overflow Log Files on FTP 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!

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

291. Navigate to **Devices > VPN**.

292. Click the **Add VPN** button and then select the **Firepower Threat Defense Device** from the dropdown menu.

Figure 404. Add VPN



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

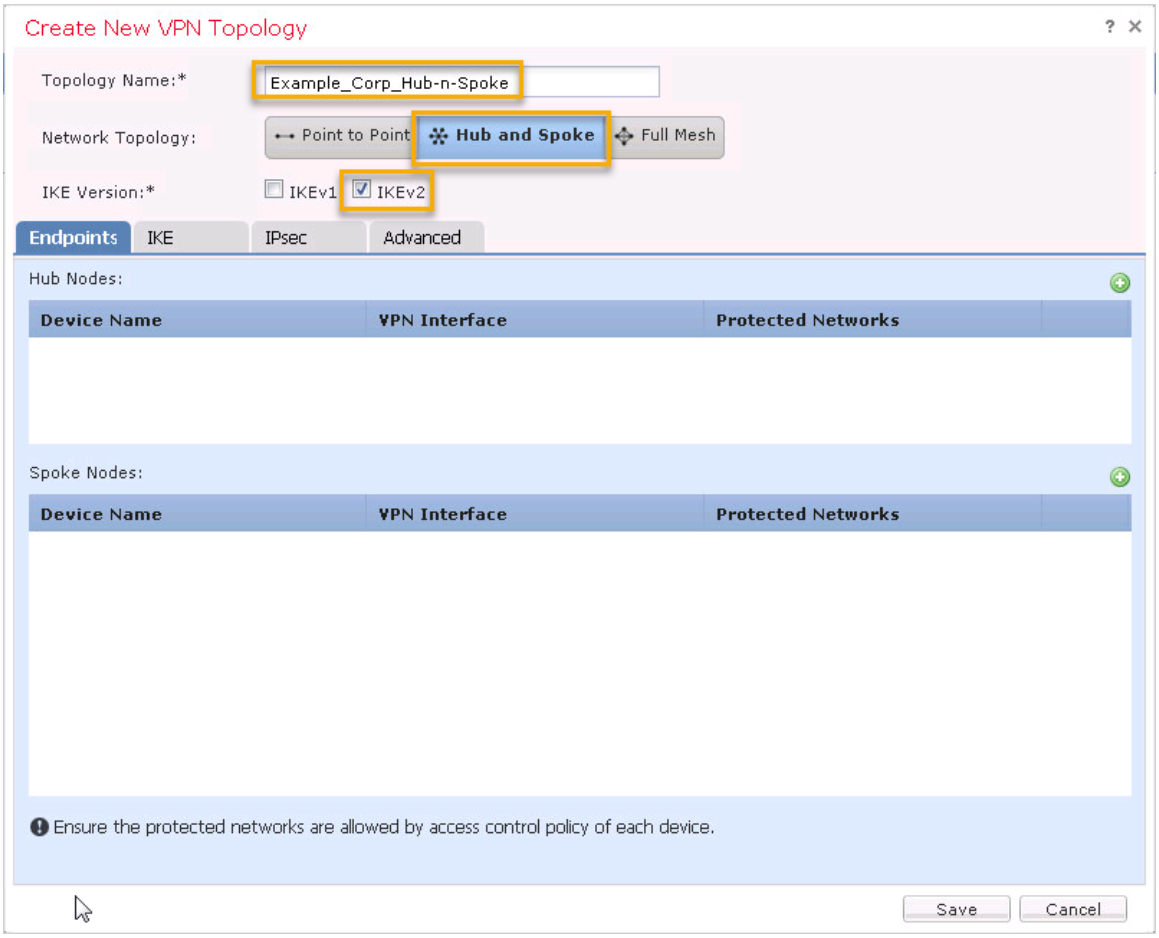
293. Use the following information to fill out the Create New VPN Topology popup window:

a. Topology Name: **Example_Corp_Hub-n-Spoke**

b. Network **Topology: Hub and Spoke**

c. IKE Version: **IKEv2**

Figure 405. Part 1 Create VPN



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

294. 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:

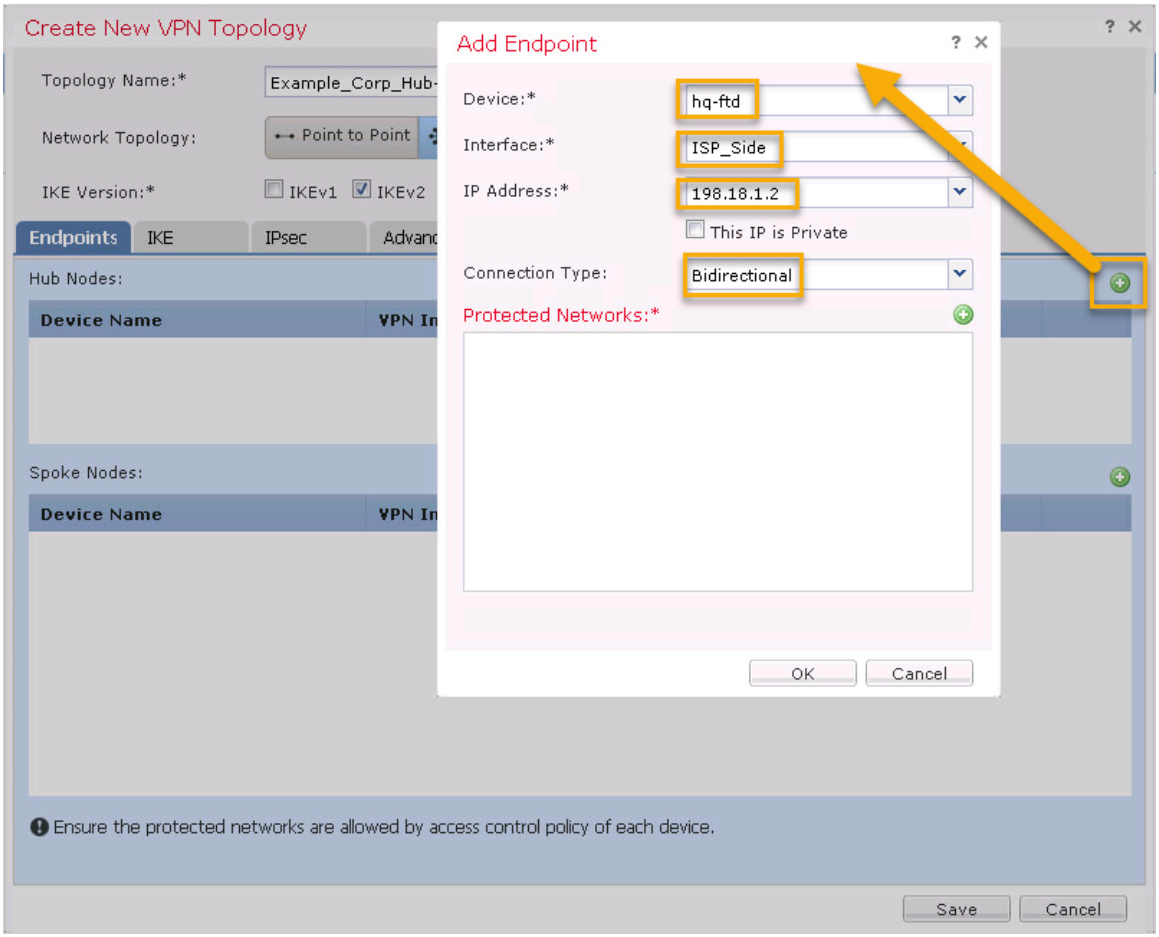
i. Device: **hq-ftd**

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 406. Part 1 Adding endpoints



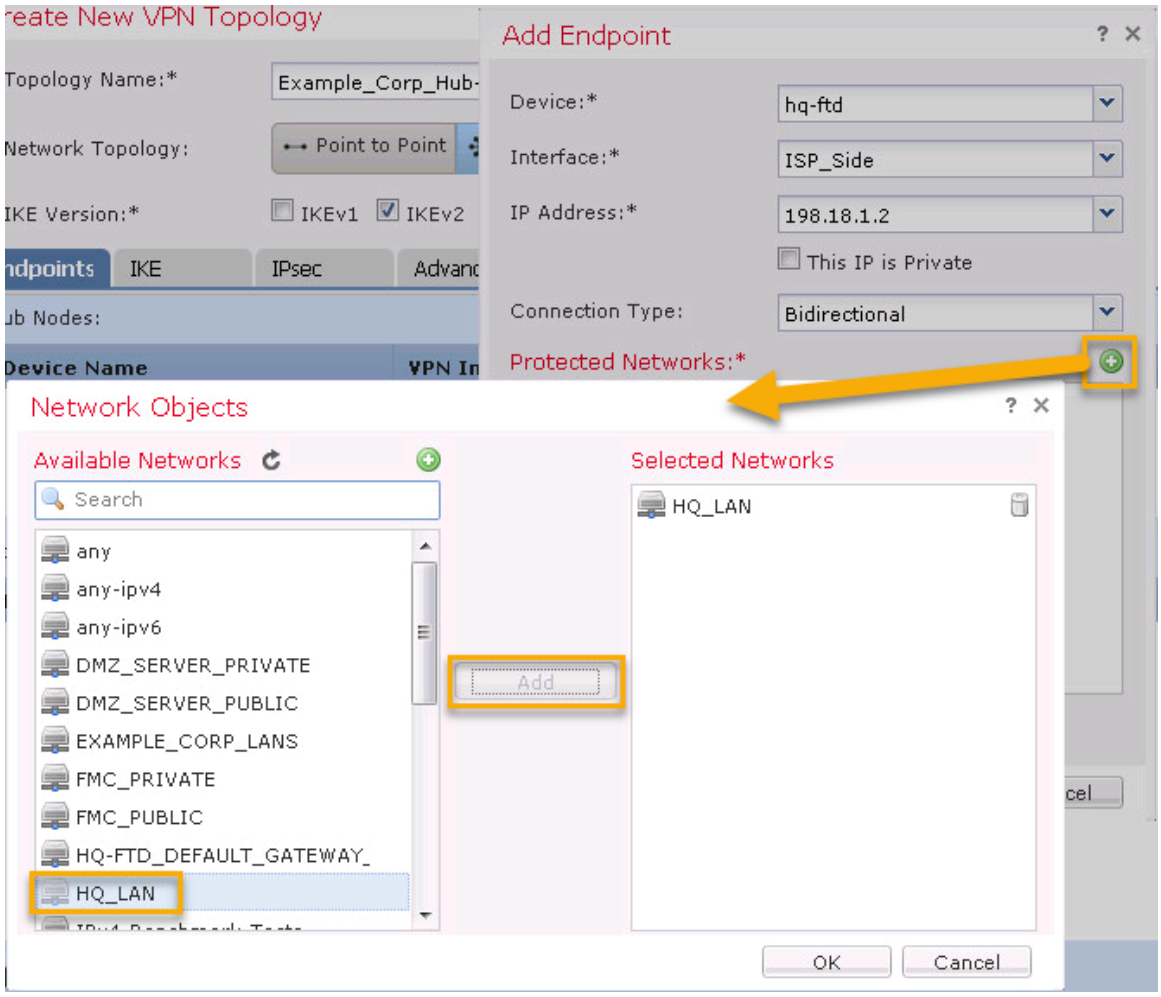
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

v. Protected Networks: Click the **green plus icon**

vi. Select the **HQ_LAN** and then click **Add**.

Figure 407. Add HQ_LAN

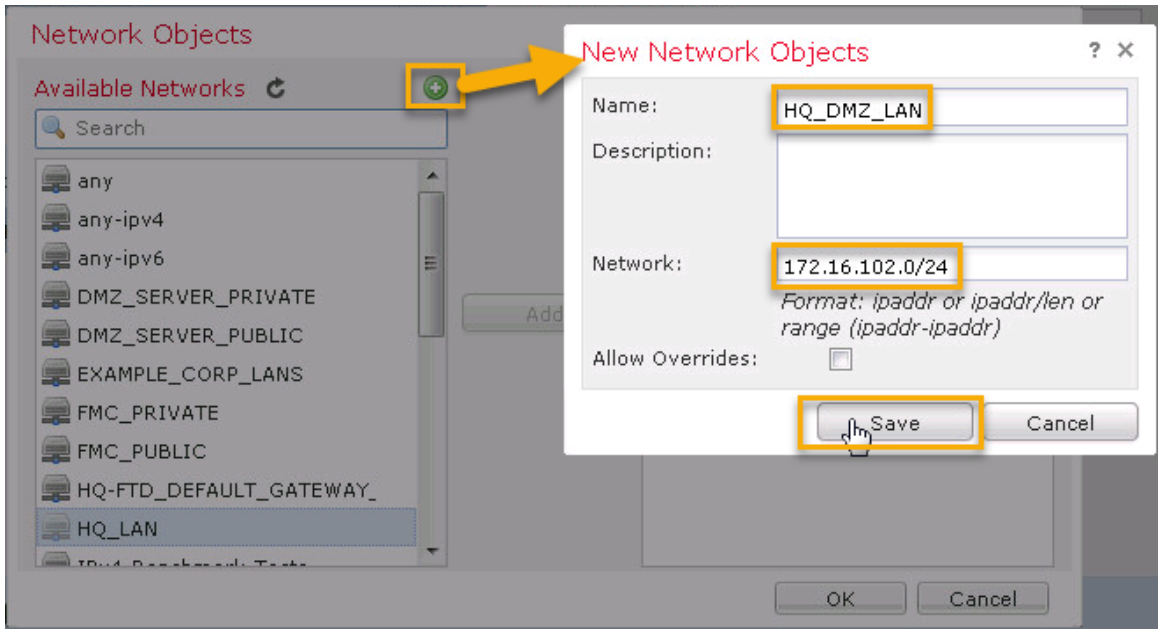


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

vii. Create a new Network Object for the **172.16.102.0/24** (the HQ_DMZ_LAN).

Figure 408. Create Network Object

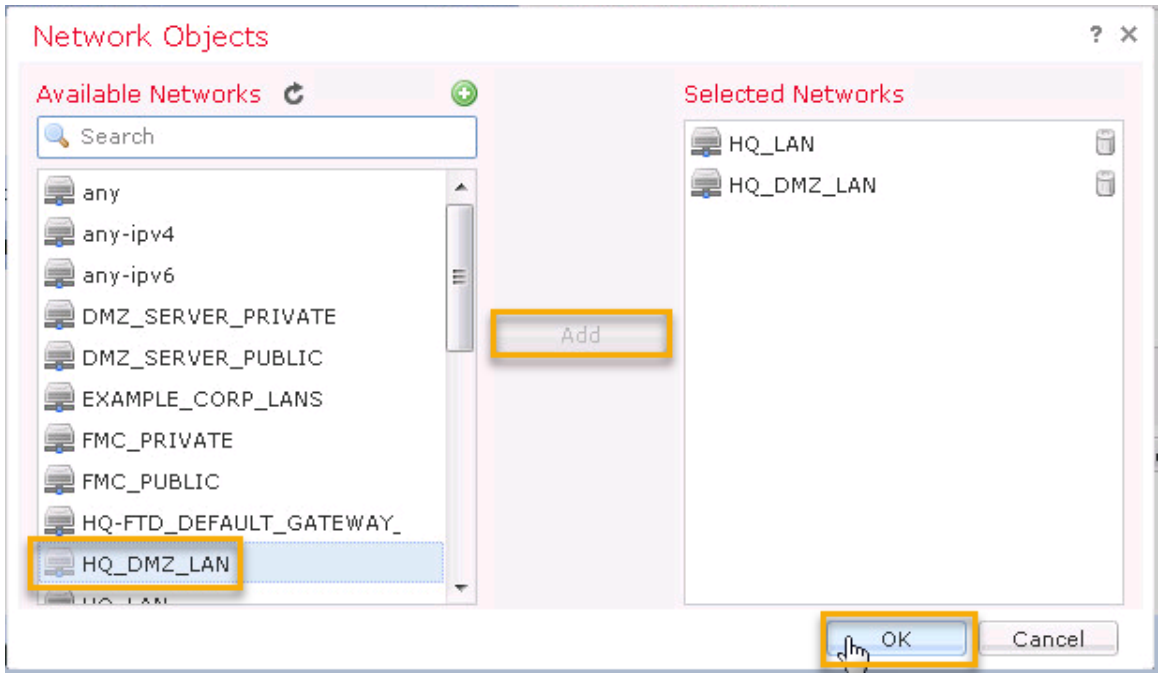


viii. Select **HQ_DMZ_LAN** and click **Add**.

ix. Ensure that both networks are in the Selected Networks area.

x. Click **OK**.

Figure 409. Add HQ_DMZ_LAN

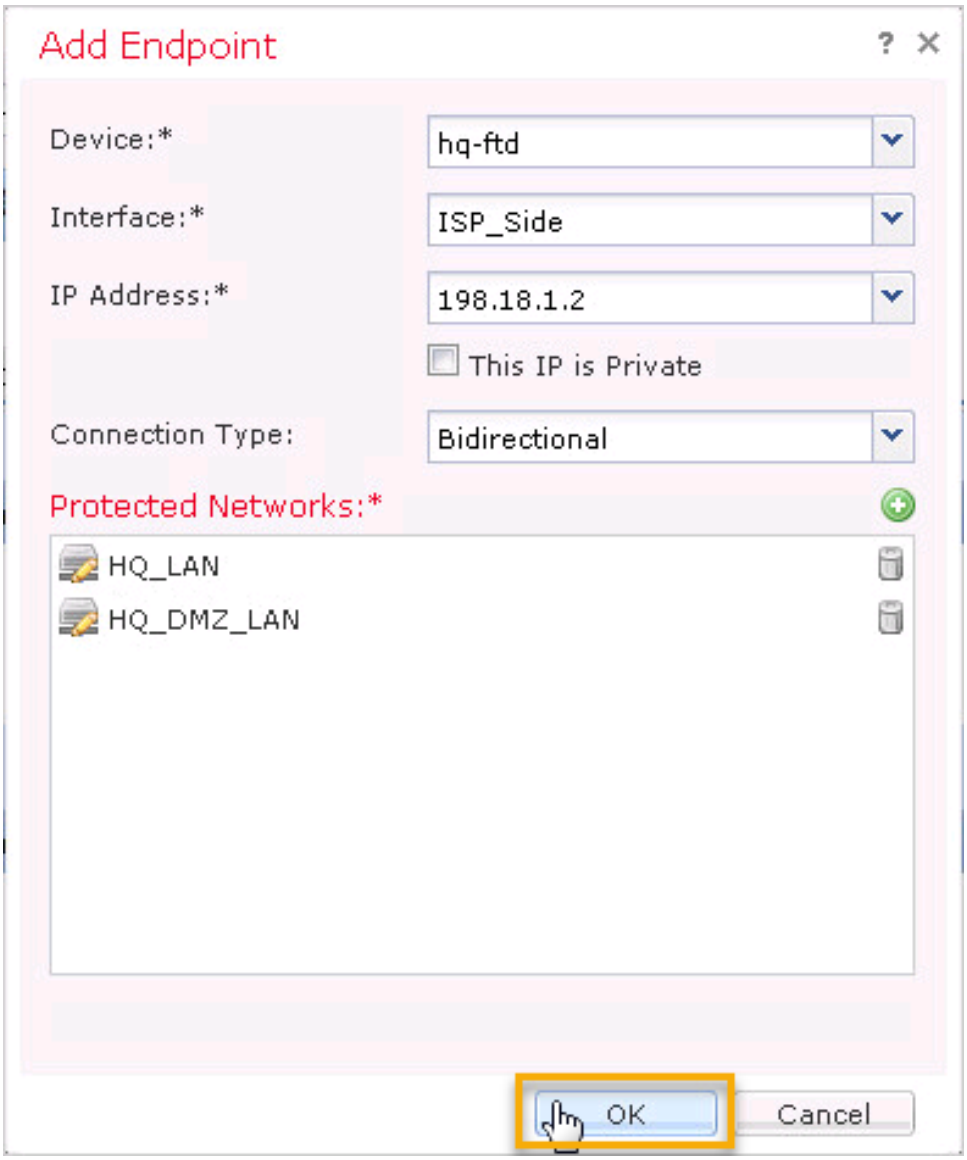


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

xi. Click **OK** to finish adding the hq-ftd endpoint to the Hub Nodes section.

Figure 410. Finish Hub Nodes



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

b. Click the **green plus icon** for the **Spoke Nodes** area and use the following to fill out the popup window:

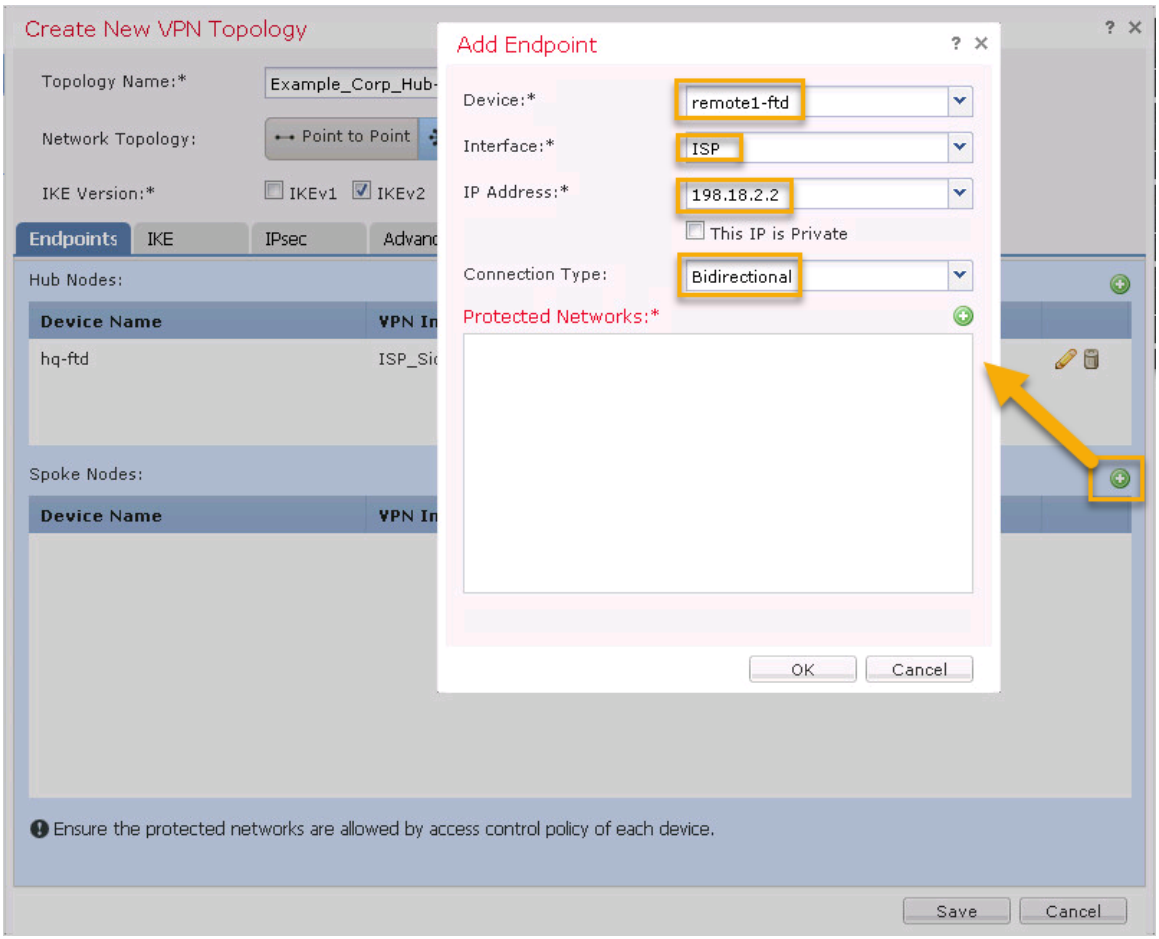
i. Device: **remote1-ftd**

ii. Interface: **ISP**

iii. IP Address: **198.18.2.2**

iv. Connection Type: **Bidirectional**

Figure 411. Part 1 Adding Spokes



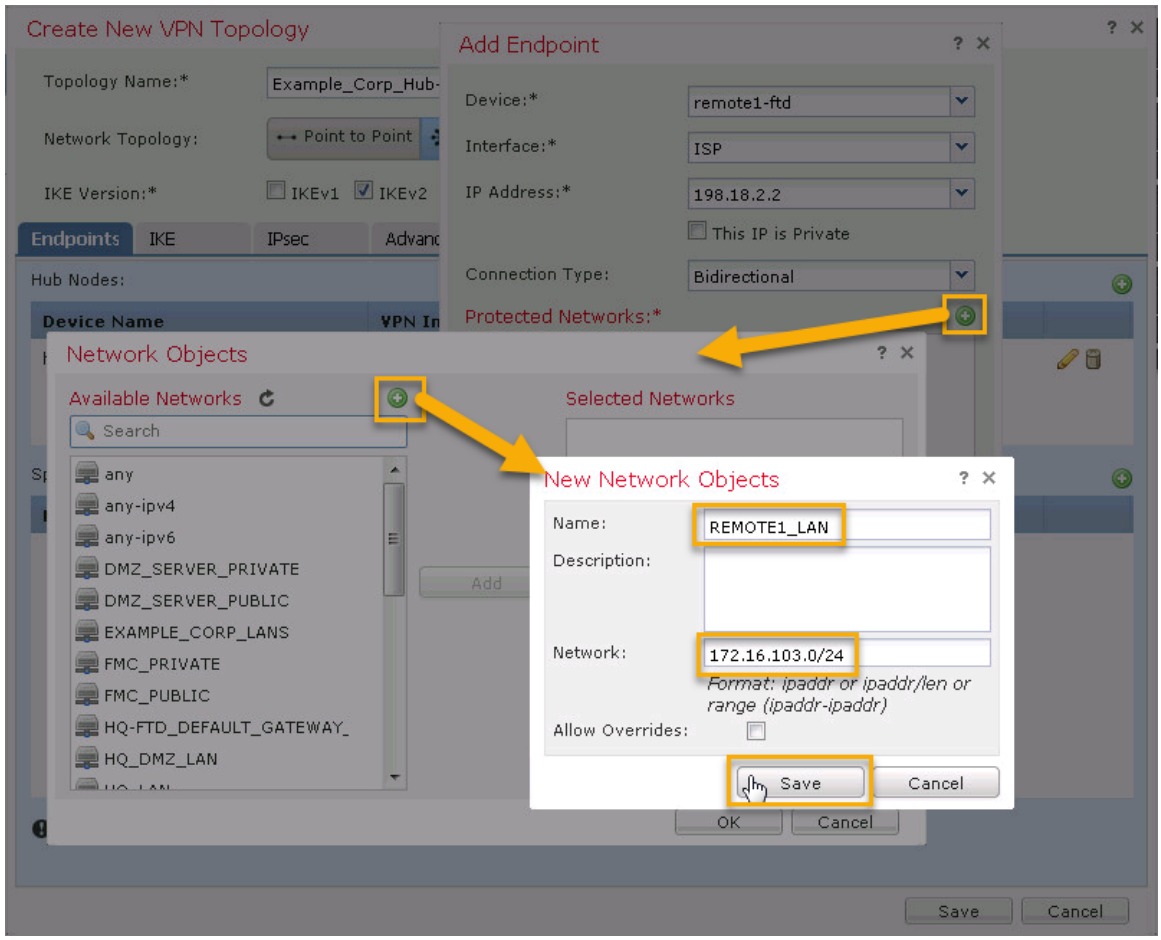
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 412. Add REMOTE1_LAN



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

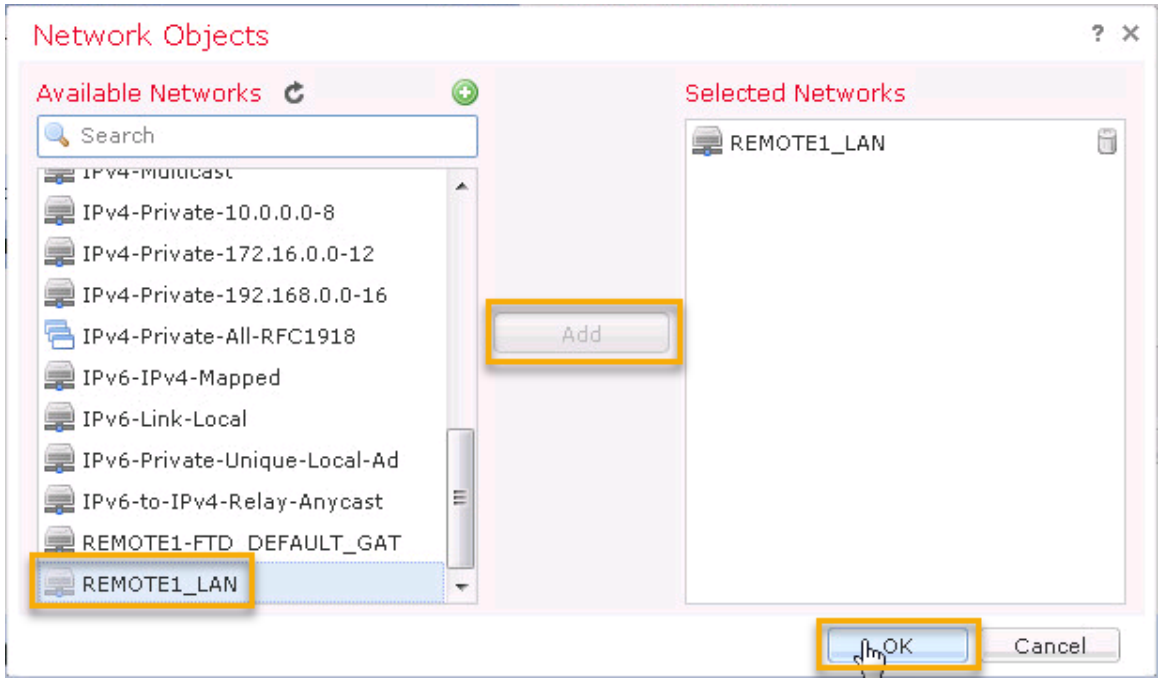
https://t.me/learningnets

vii. Select **REMOTE1_LAN** and click **Add**.

viii. Ensure that the network is in the Selected Networks area.

ix. Click **OK**.

Figure 413. Click OK

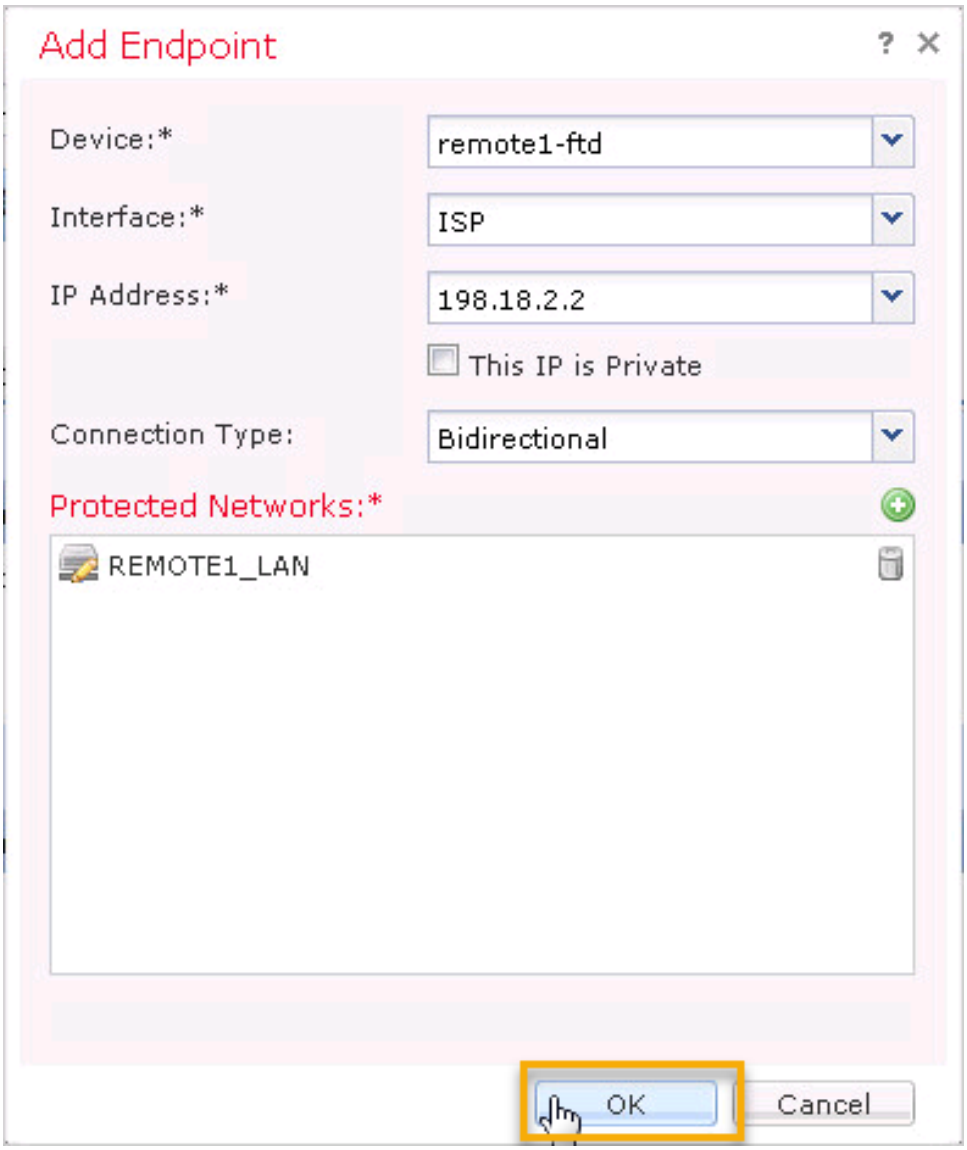


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

x. Click **OK** to finish adding the remote1-ftd endpoint to the Spoke Nodes section.

Figure 414. Click OK



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

c. Click the **green plus icon** for the **Spoke Nodes** area again and use the following to fill out the popup window:

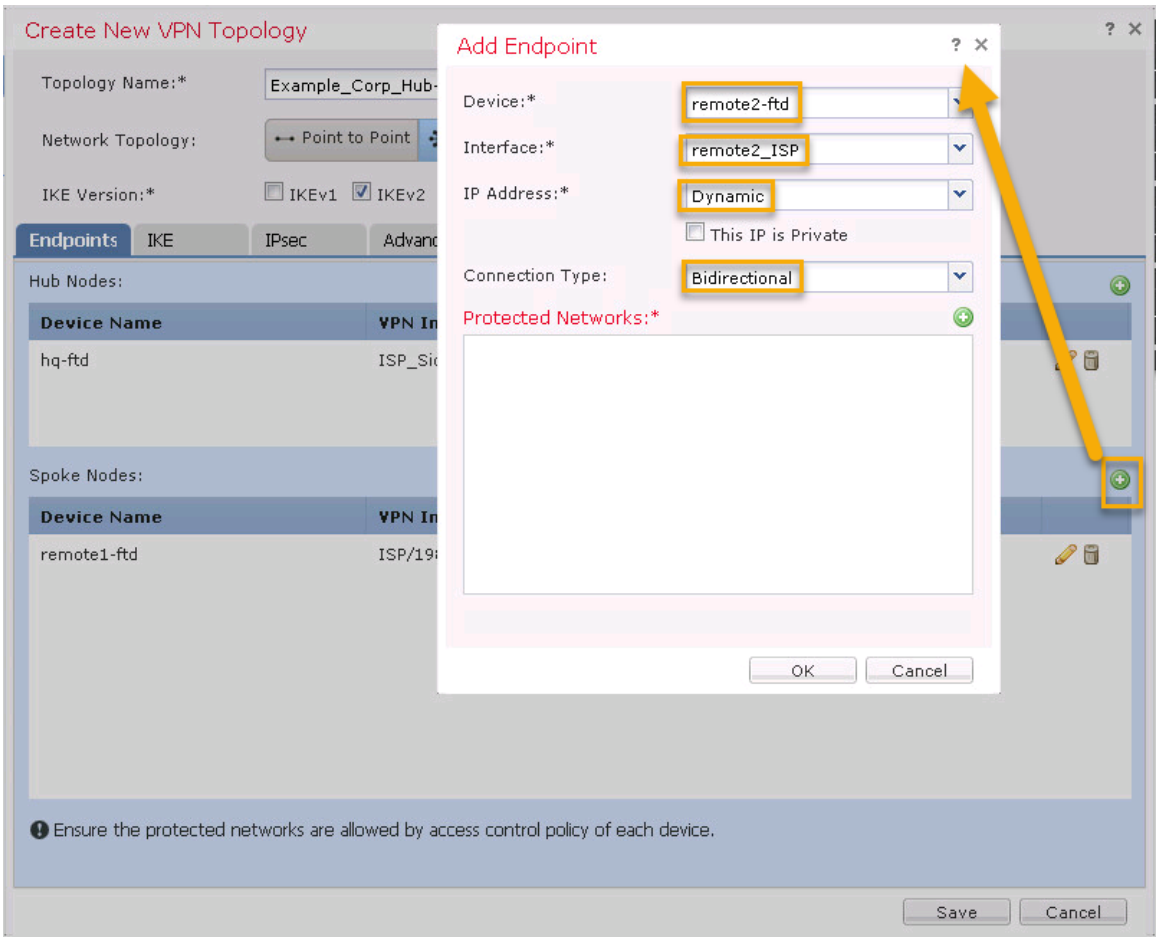
i. Device: **remote2-ftd**

ii. Interface: **remote2_ISP**

iii. IP Address: **Dynamic**

iv. Connection Type: **Bidirectional**

Figure 415. Part 1 Adding Node



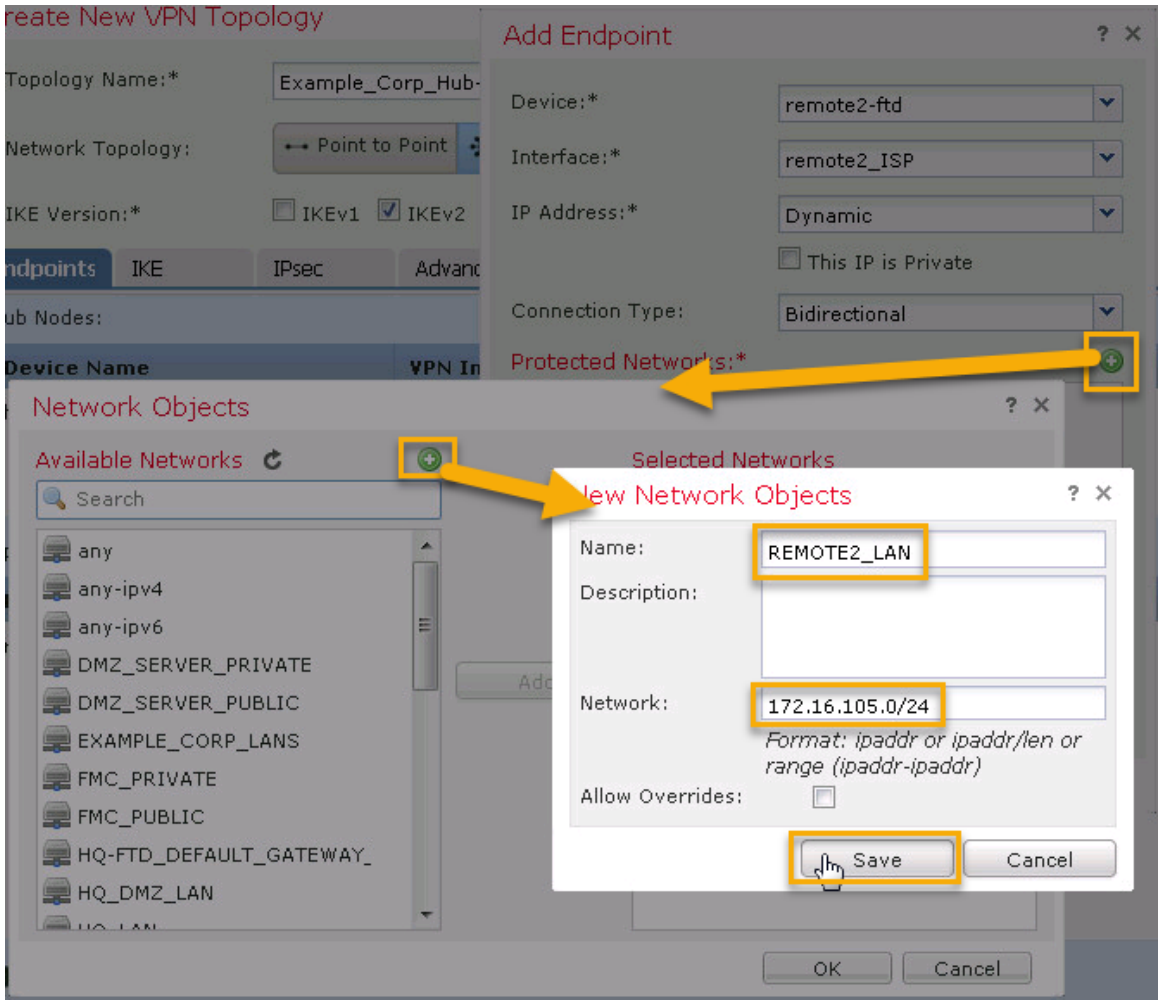
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 416. Create REMOTE2_LAN Network Object



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

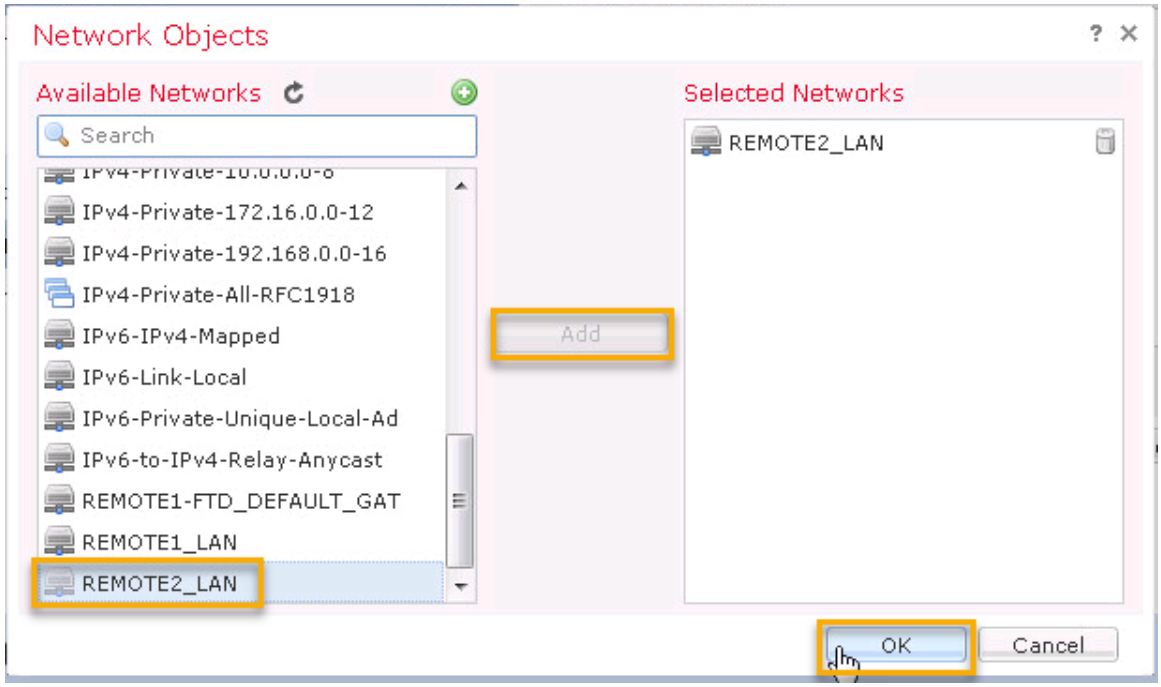
https://t.me/learningnets

vii. Select **REMOTE2_LAN** and click **Add**.

viii. Ensure that the network is in the Selected Networks area.

ix. Click **OK**.

Figure 417. Click OK

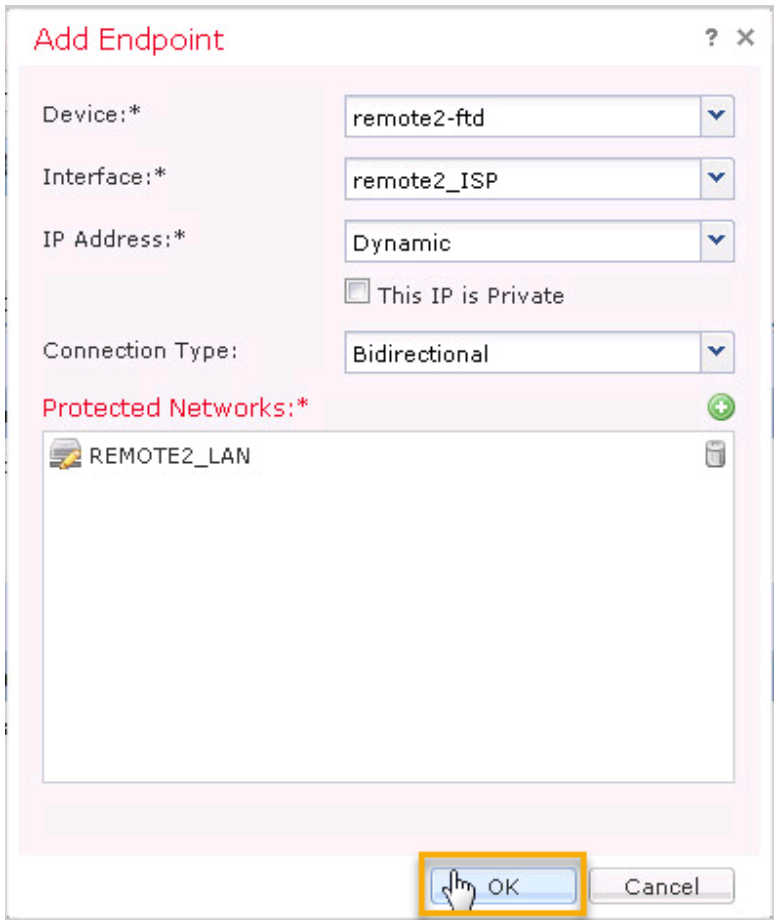


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

x. Click **OK** to finish adding the remote2-ftd endpoint to the Spoke Nodes section.

Figure 418. Click OK



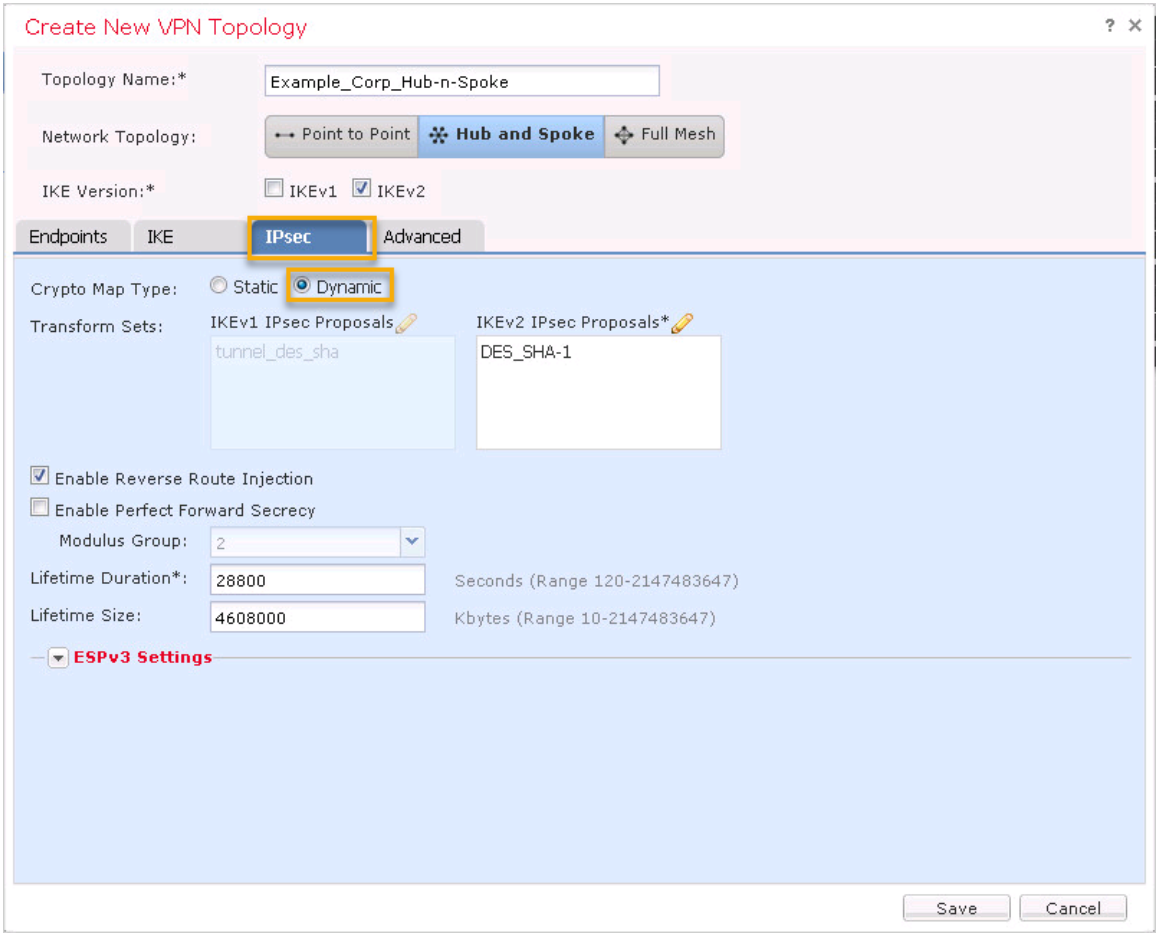
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

295. 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 419. Configure IPsec tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

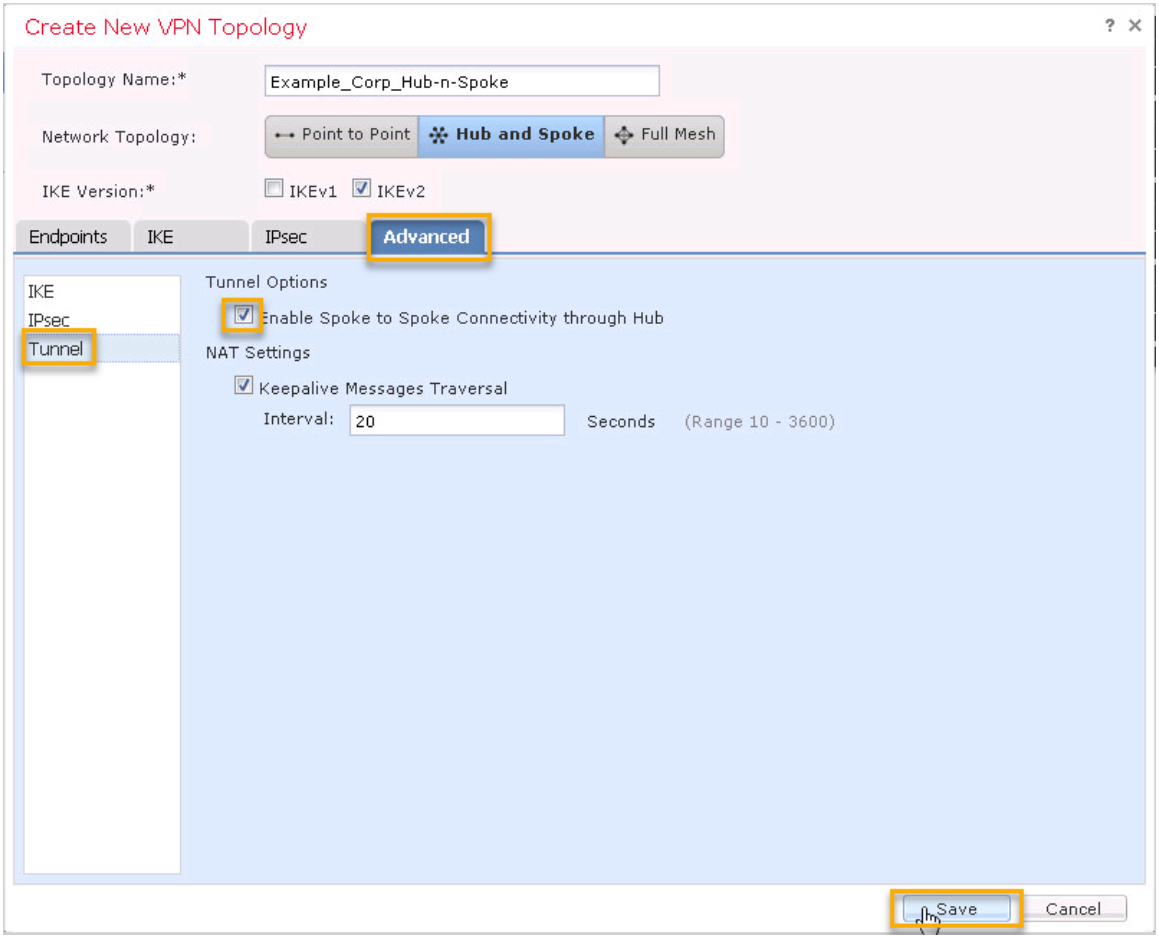
https://t.me/learningnets

296. 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.

297. Click **Save**.

Figure 420. Save VPN



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

298. 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 421. Edit NAT



299. 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**

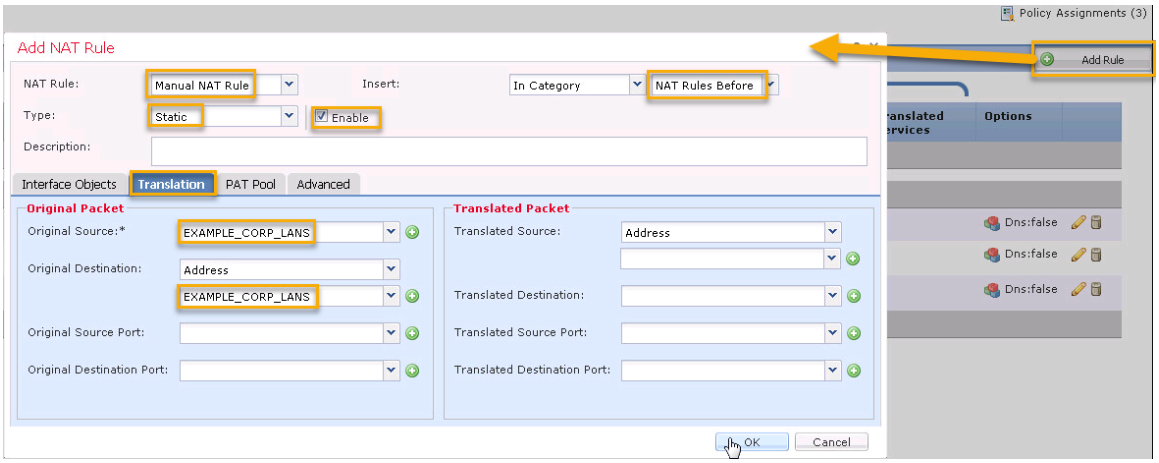
    d. Enable: **Checked**

300. On the **Translation tab**:

    a. Original Source: **EXAMPLE_CORP_LANS**

    b. Original Destination: **Address** and then **EXAMPLE_CORP_LANS**

Figure 422. Configure Translations tab



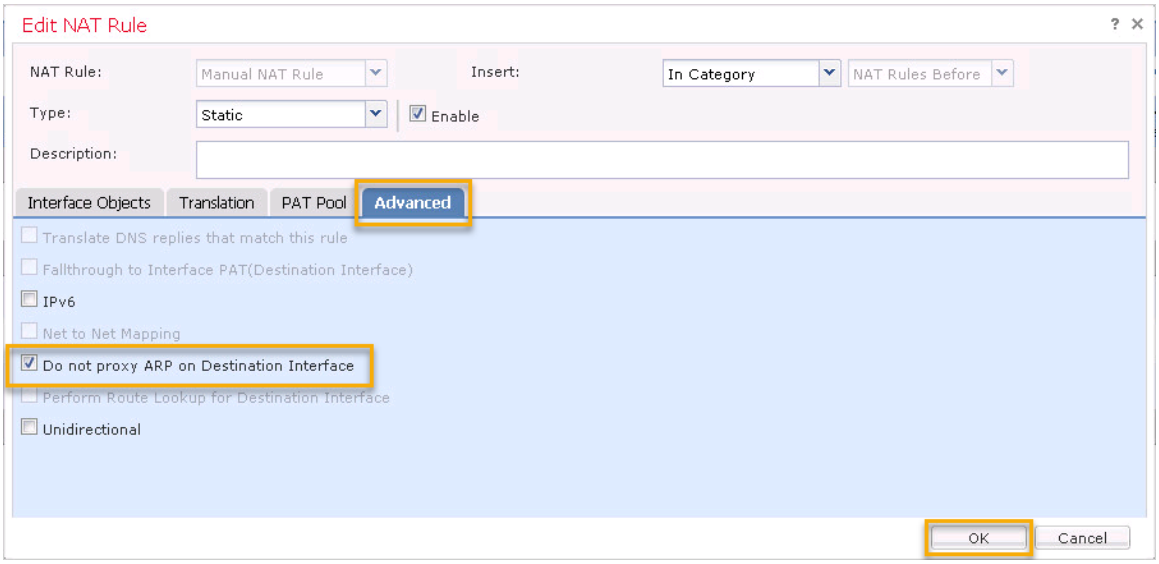
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

301. 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.

302. Click **OK**.

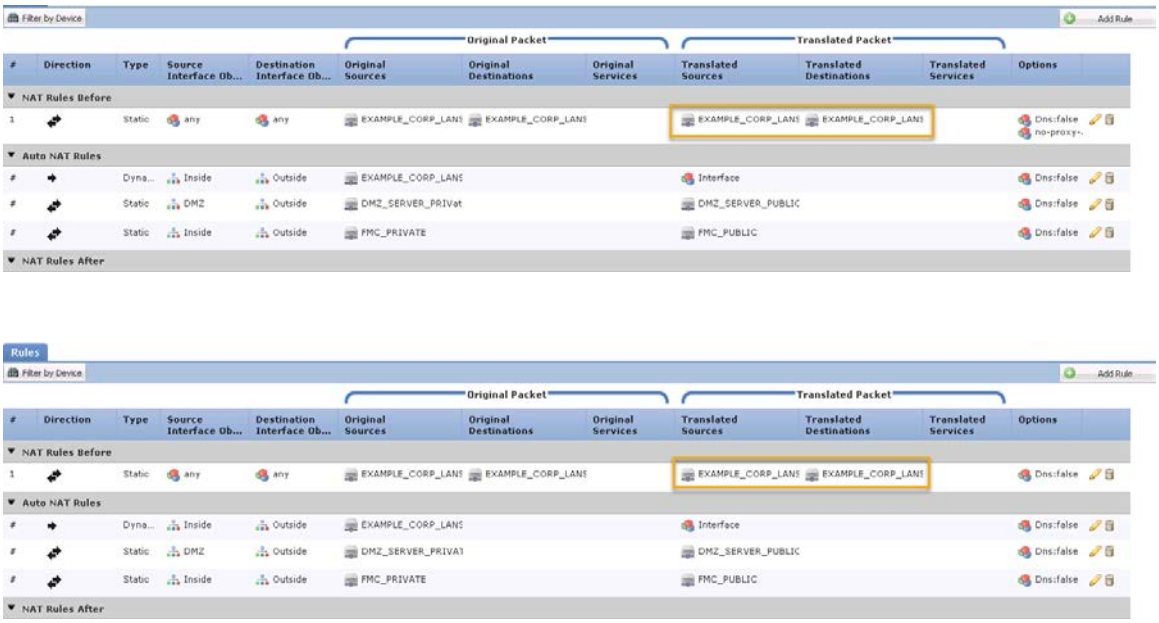
Figure 423. Death to proxy-arp!



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.

303. Notice that the new rule auto populated the Translated Packet field to create the identity NAT.

Figure 424. Finished NAT Rule



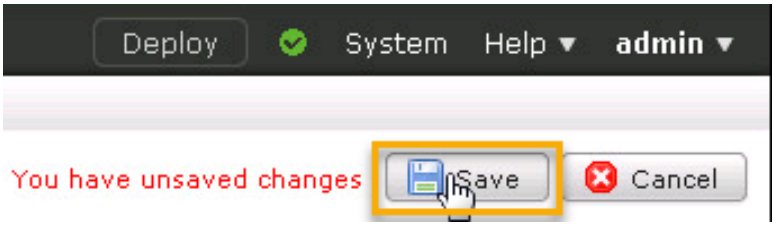
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

304. Click **Save** to push these changes to the FMC.

Figure 425. Save to FMC



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.

305. Navigate to Policies > Access Control > Access Control and edit the Base Policy.

Figure 426. Edit Base Policy ACP



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

306. 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**

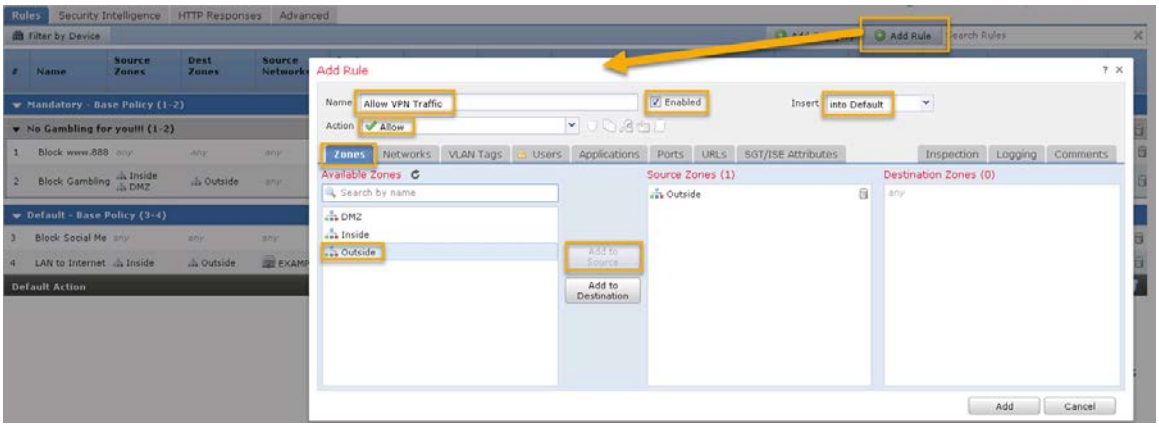
    c. Insert: **into Default**

    d. Action: **Allow**

307. On the **Zones tab**:

    a. Source Zones: **Outside**

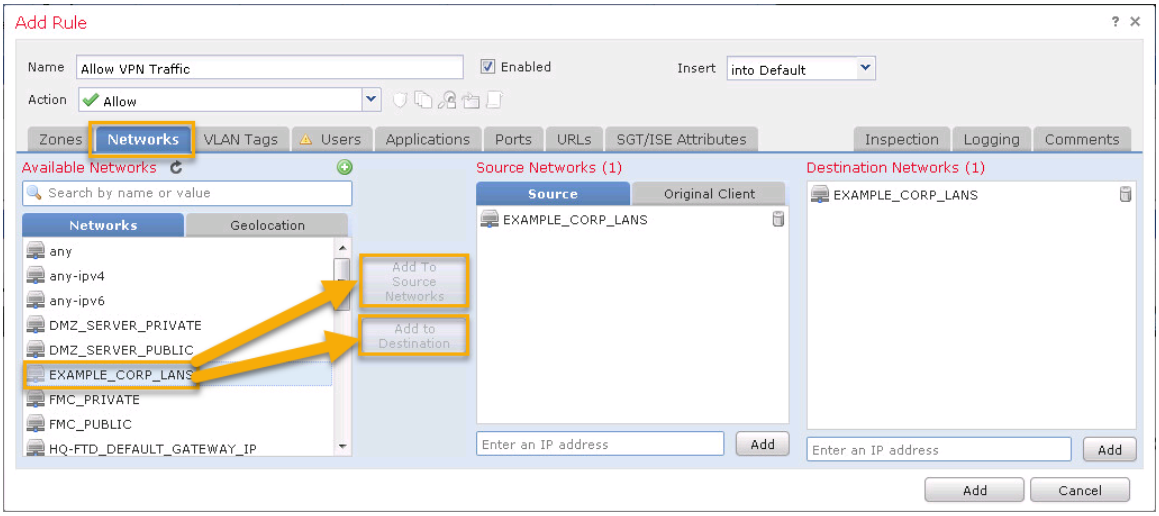
Figure 427. Part 1 of Adding ACP rule



308. 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 428. Configure Networks tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

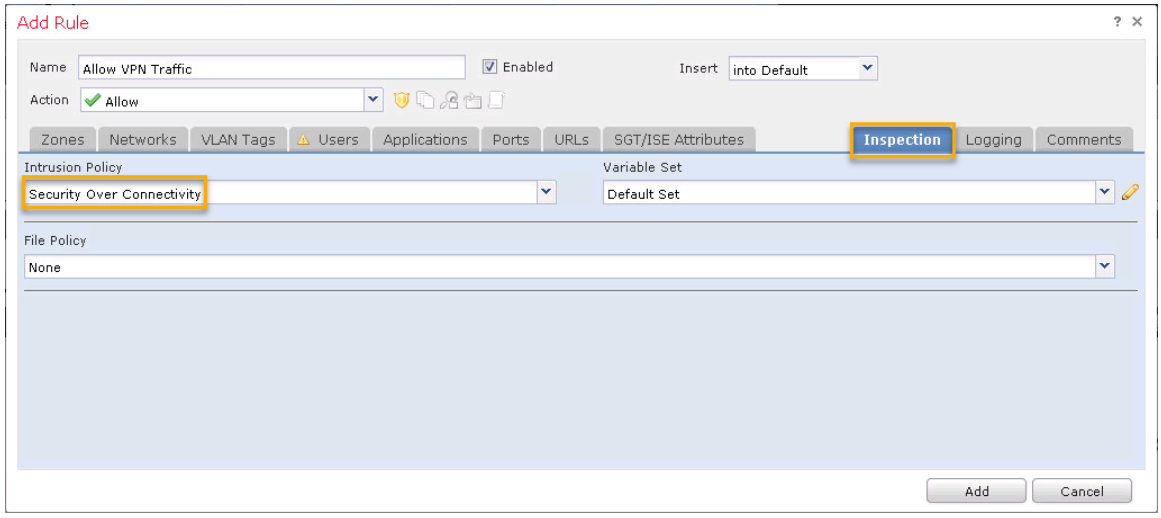
https://t.me/learningnets

309. 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 429. Configure Inspection tab



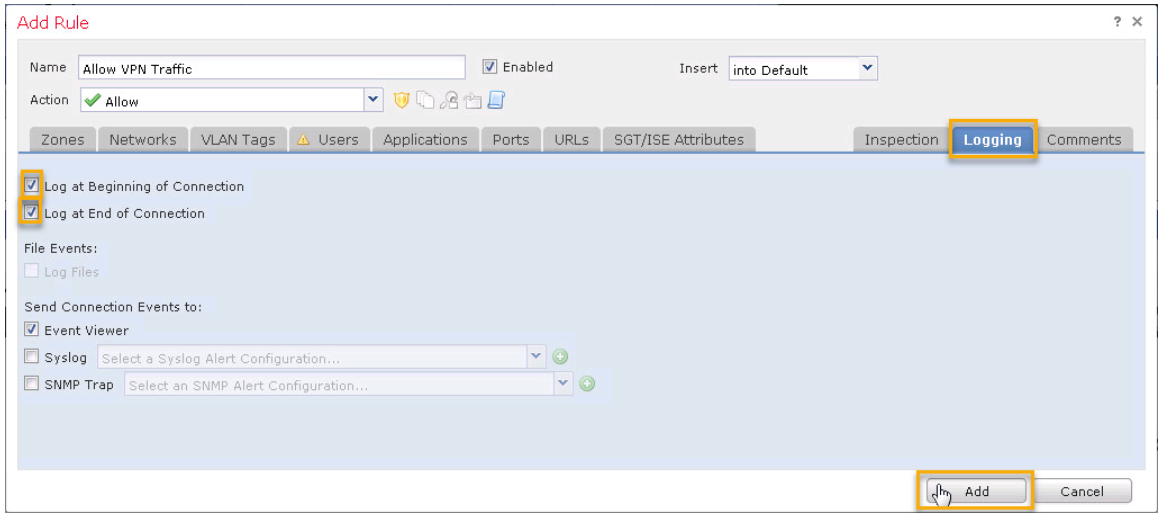
310. On the **Logging tab**:

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.

311. Click **Add**.

Figure 430. Configure Logging and Add rule

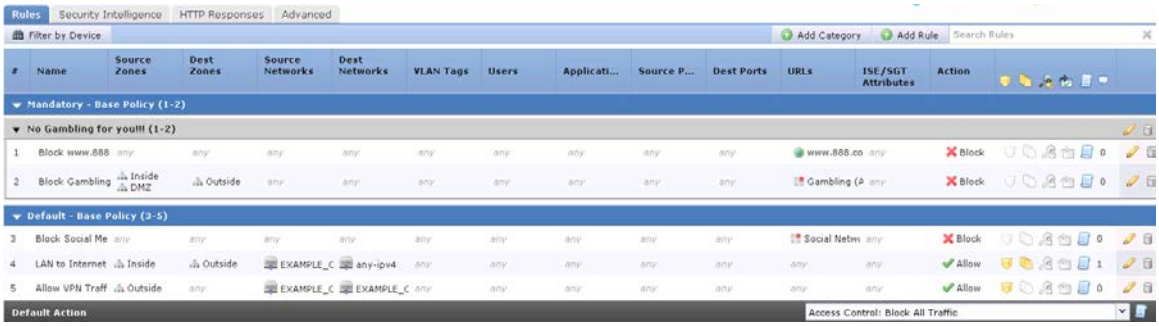


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

312. 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 431. Review ACP rules



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.

313. 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.

314. On **hq-wkst** open a **CMD prompt** for each of the following:

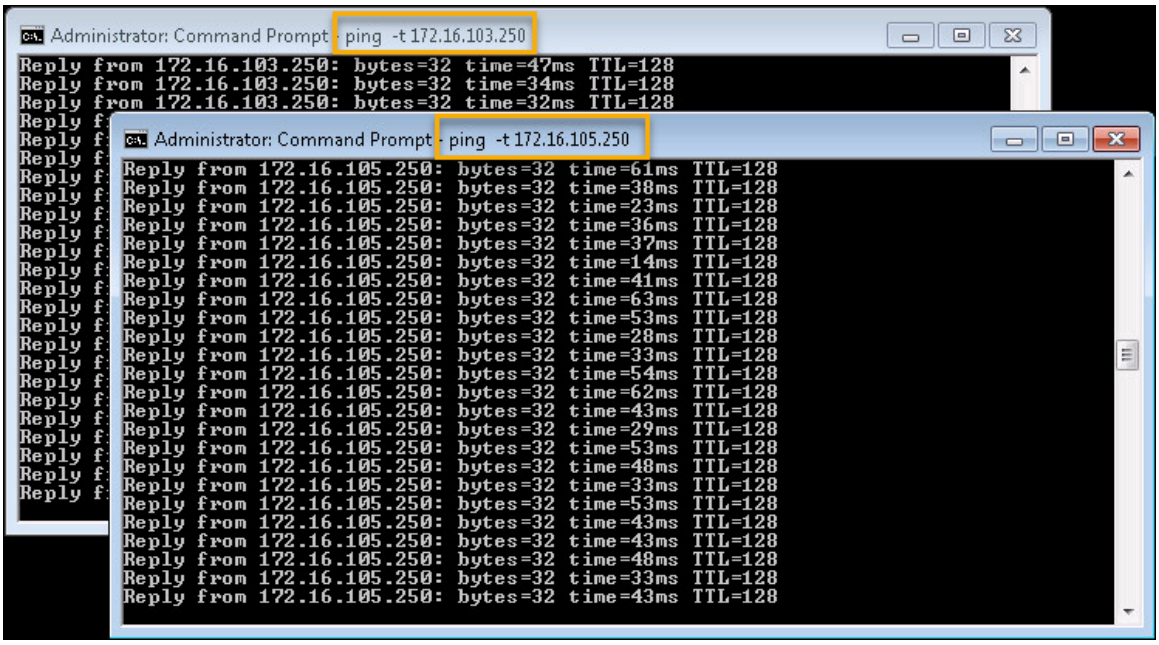
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

a. **ping –t 172.16.103.250** (remote1-wkst).

b. **ping –t 172.16.105.250** (remote2-wkst).

Figure 432. Pings from hq-wkst



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

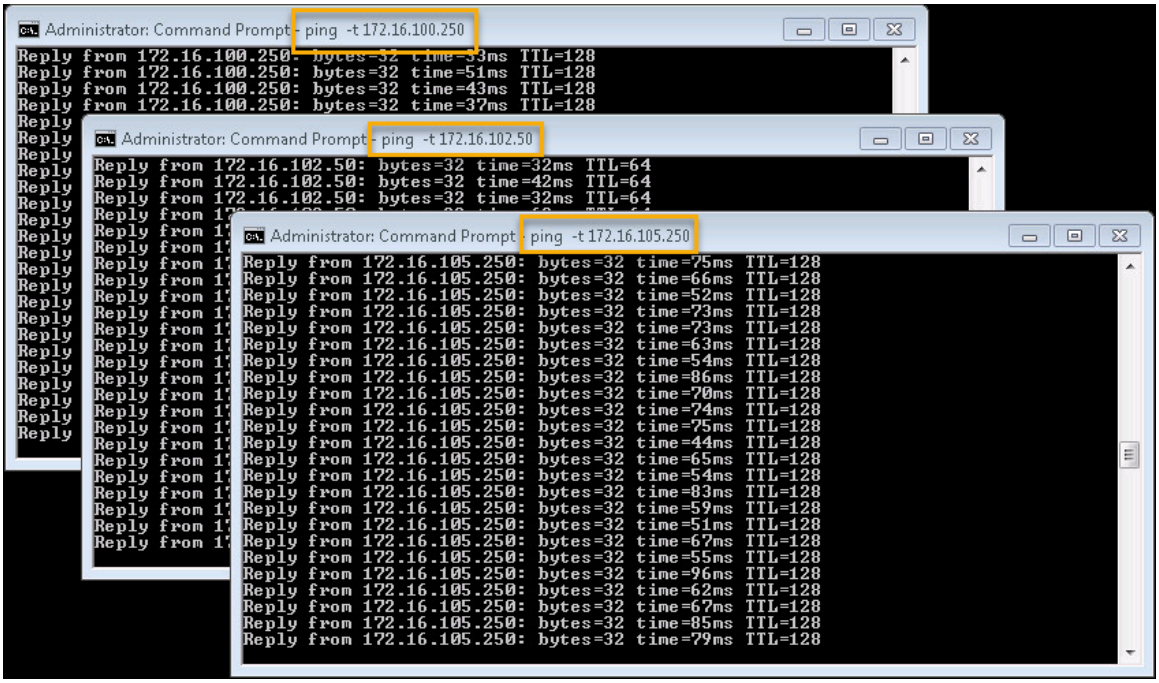
315. On **remote1-wkst** open a **CMD prompt** for each of the following:

a. **ping –t 172.16.100.250** (hq-wkst)

b. **ping –t 172.16.102.50** (dmz-server)

c. **ping –t 172.16.105.250** (remote2-wkst)

Figure 433. Pings from remote1-wkst



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

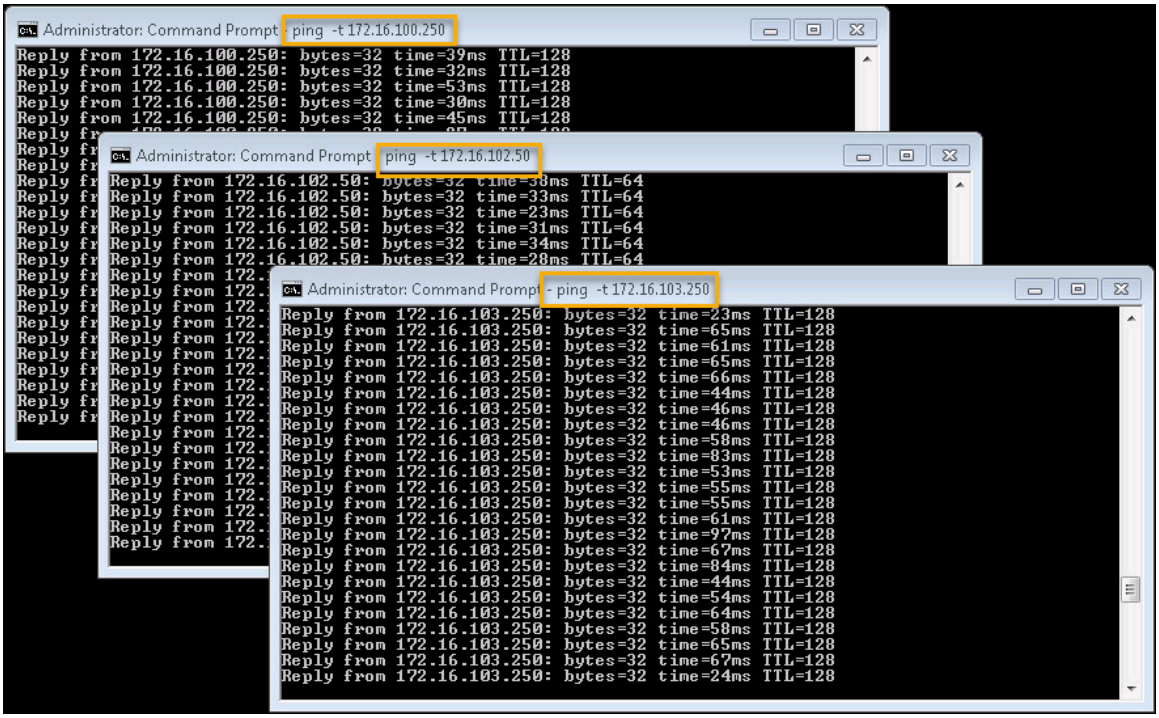
316. On **remote2-wkst** open a **CMD prompt** for each of the following:

a. **ping –t 172.16.100.250** (hq-wkst)

b. **ping –t 172.16.102.50** (dmz-server)

c. **ping –t 172.16.103.250** (remote1-wkst)

Figure 434. Pings from remote2-wkst



Ensure that all the above ping tests work before continuing.

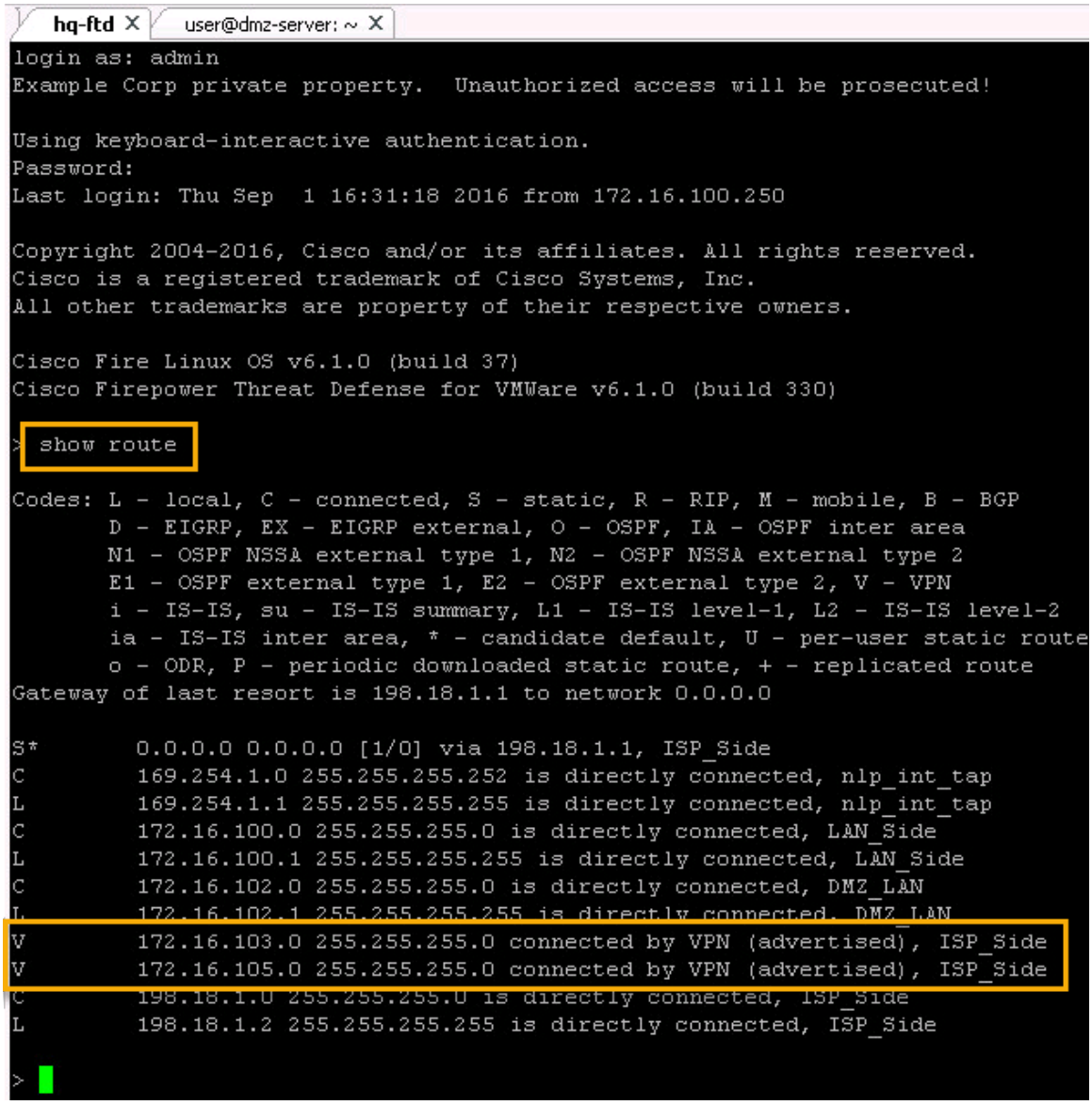
Whew! Eight continuous pings. In the excitement to get the VPN working did you happen to figure out what you enabled that you shouldn't have yet?

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

317. Using the MTPuTTY bookmark ssh to **hq-ftd (MGMT NIC)** and issue the command **show route**. If the tunnel is configured, you should see some routes that are “connected by VPN”.

Figure 435. Show route

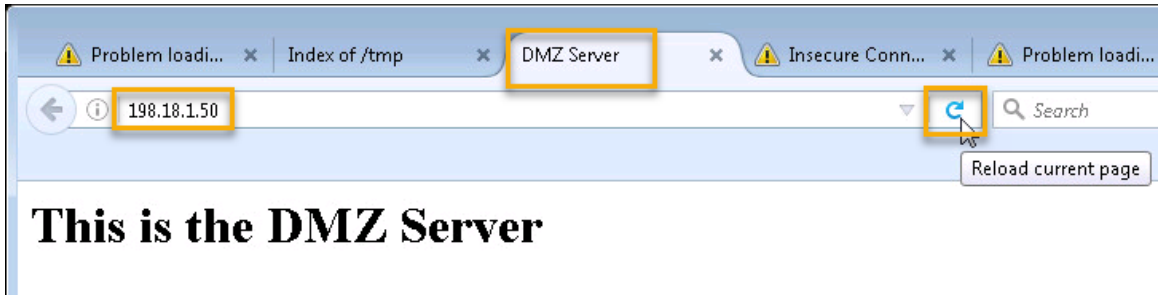


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

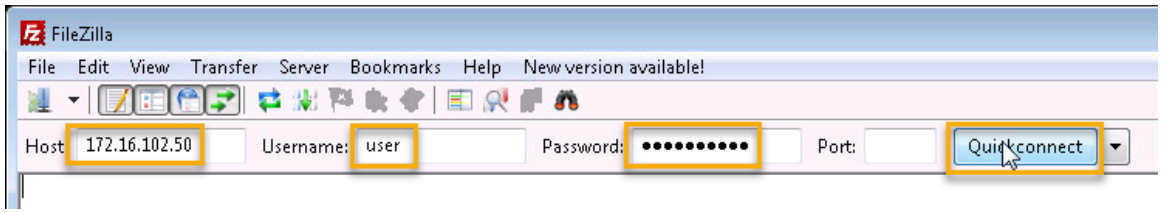
318. Once all the above pings work then on either **remote workstation** open up **Firefox** and go to **http://172.16.102.50** (the DMZ Server's internal IP address).

Figure 436. DMZ Server URL



319. 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 437. FTP to DMZ Server

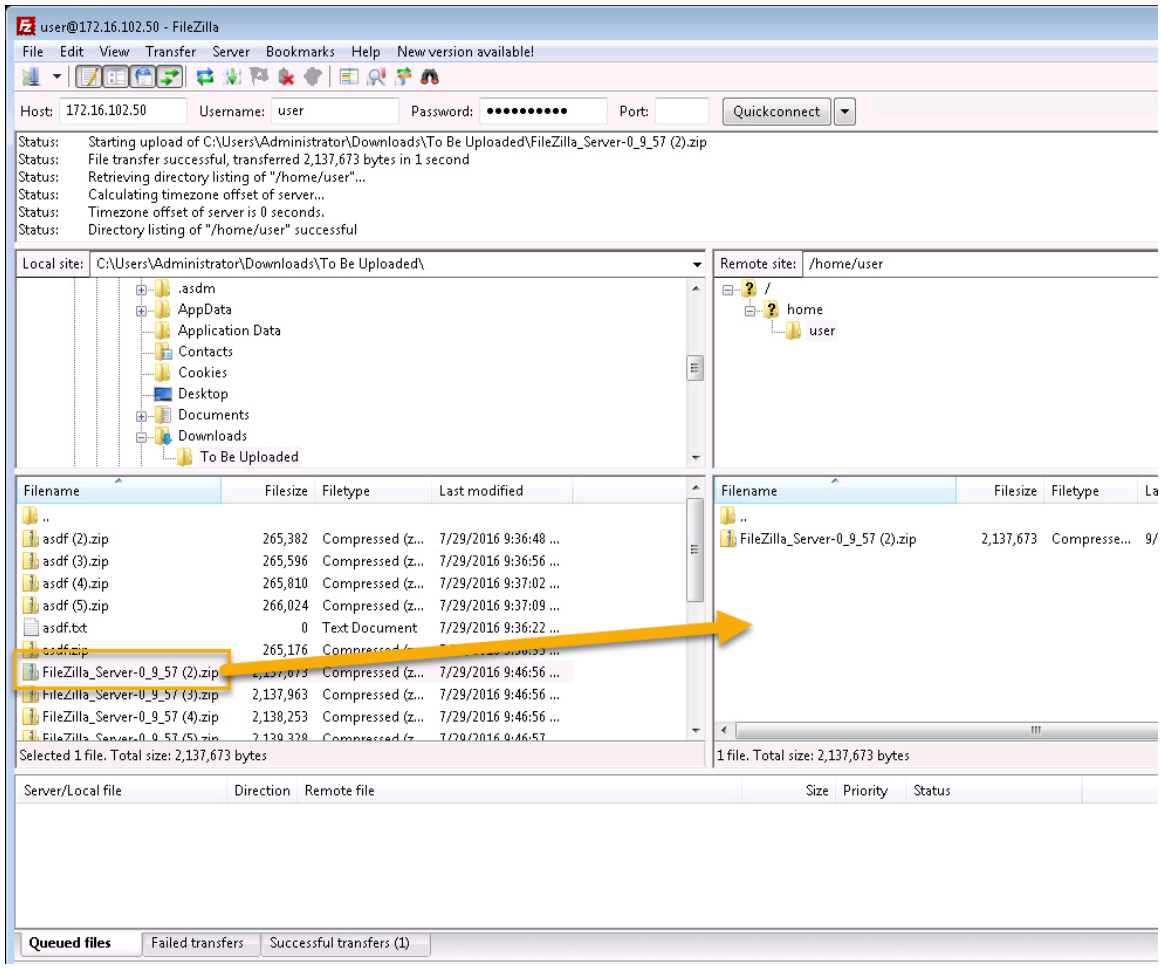


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

320. Once logged in select a file from the DMZ server and **upload** to the server. Oops. That succeeded!

Figure 438. Downloading file via FTP



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

321. In the FMC administration website navigate to **Policies > Access Control > Access Control** and **edit** the **HQ Policy**.

Figure 439. Edit HQ Policy ACP



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

322. 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.)

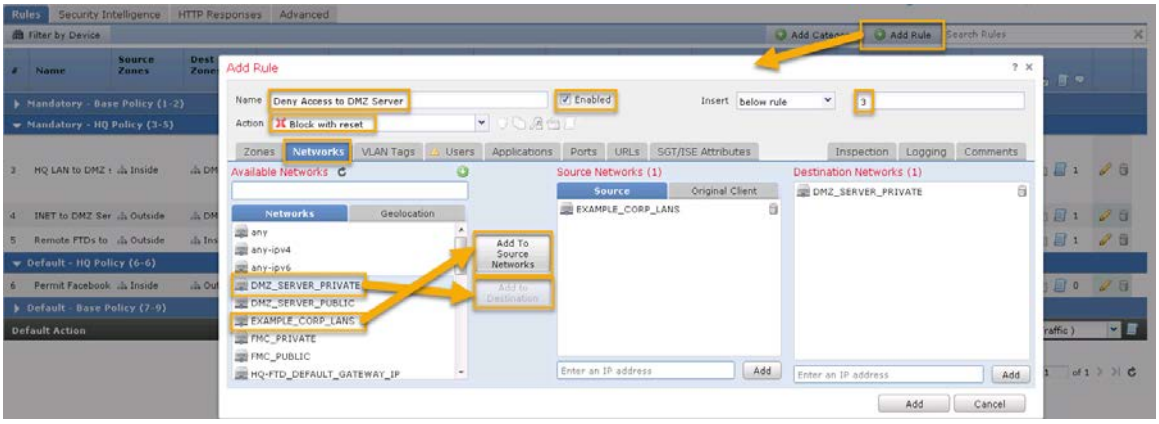
d. Action: **Block with reset**

323. On the **Networks tab**:

a. Source Networks: **EXAMPLE_CORP_LANS**

b. Destination Networks: **DMZ_SERVER_PRIVATE**

Figure 440. Part 1 Adding rule



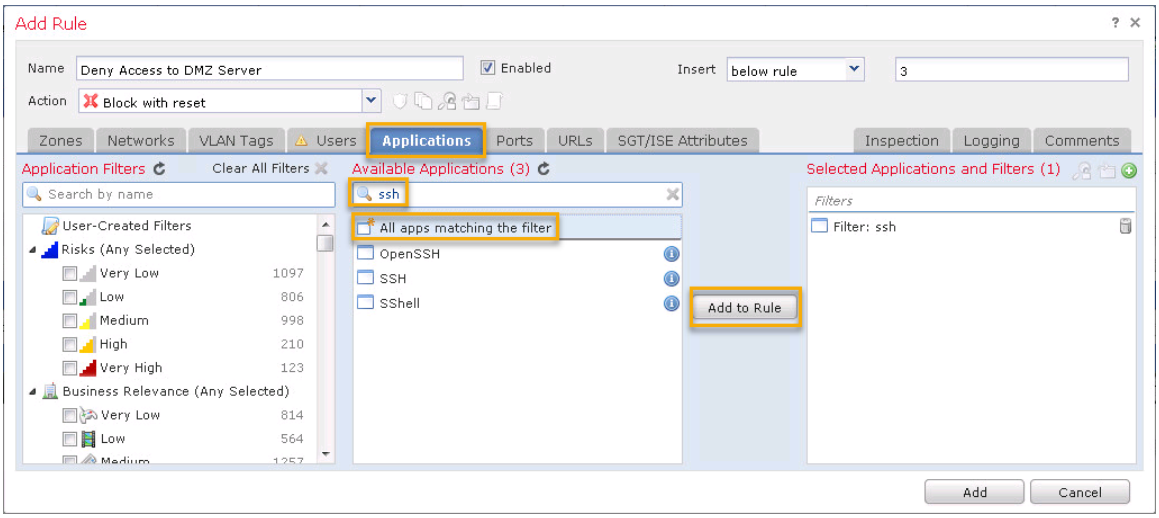
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

324. On the **Applications tab**:

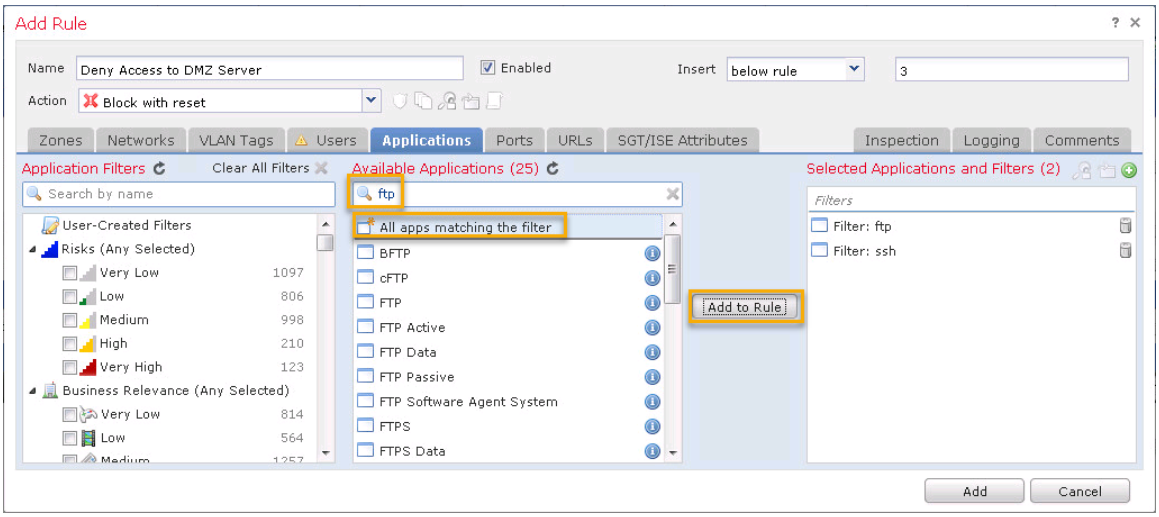
a. In **Available Applications** search for **ssh**. Then select the **All apps matching this filter** and click **Add to Rule**.

Figure 441. Add ssh to rule



b. In **Available Applications** search for **ftp**. Then select the **All apps matching this filter** and click **Add to Rule**.

Figure 442. Configure Applications tab



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

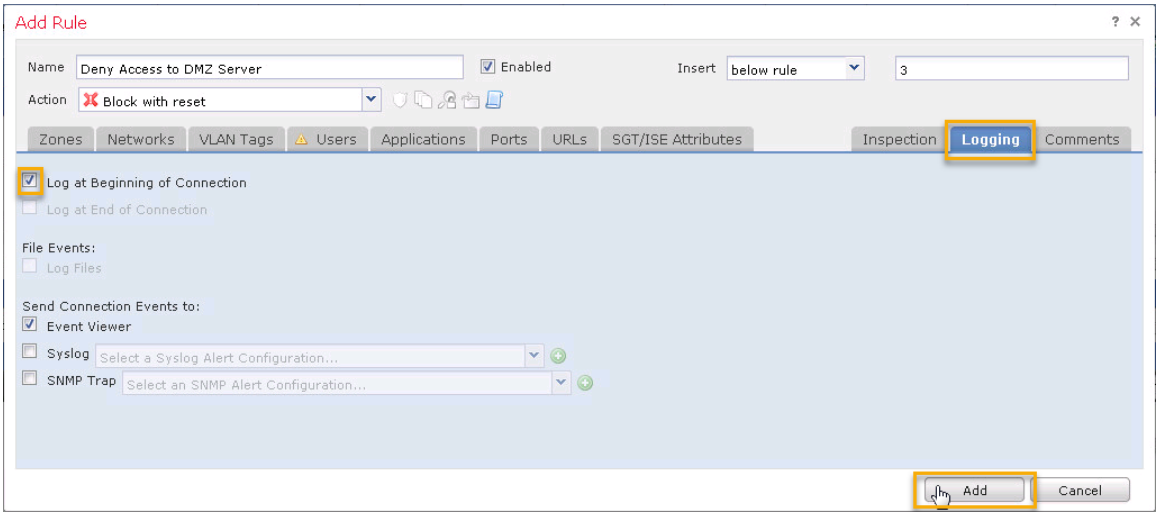
https://t.me/learningnets

325. On the **Logging tab**:

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

326. Click **Add**

Figure 443. Configure Logging and Save



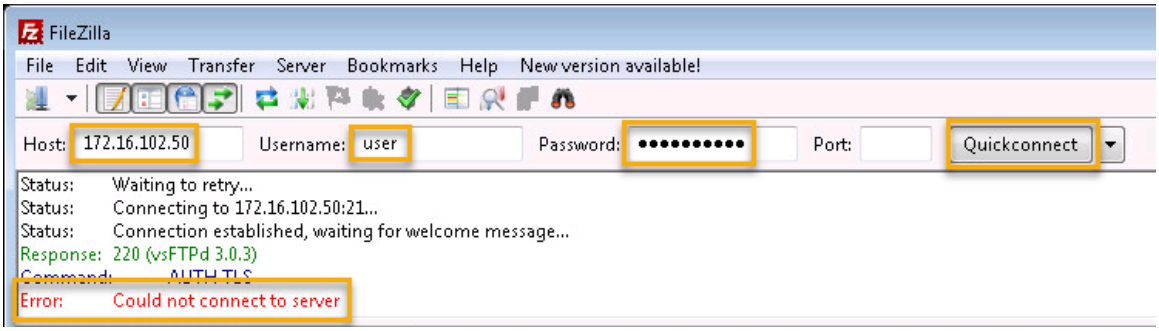
327. Click **Save**, **Deploy**, select **hq-ftd** and then click **Deploy**.

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.

328. Once the deployment has completed repeat the previous FTP test. On the **remote workstation** close and then reopen **FileZilla**.

329. Attempt to establish an **FTP** connection to **172.16.102.50** as **user/C1sco12345** again. This should fail.

Figure 444. Attempt to reconnect to DMZ via FileZilla

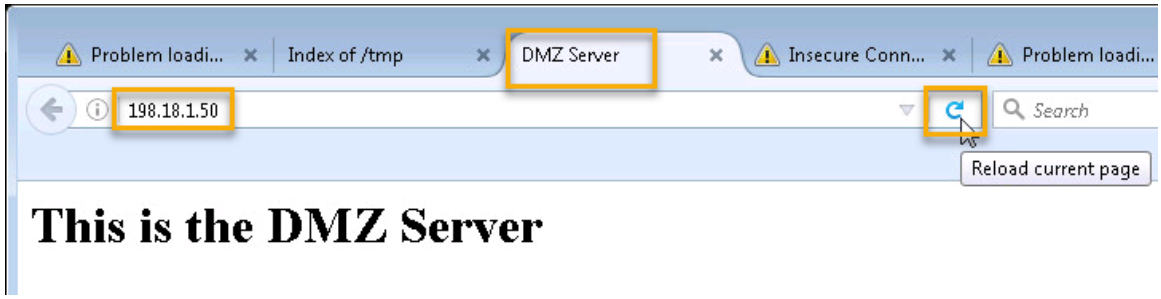


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

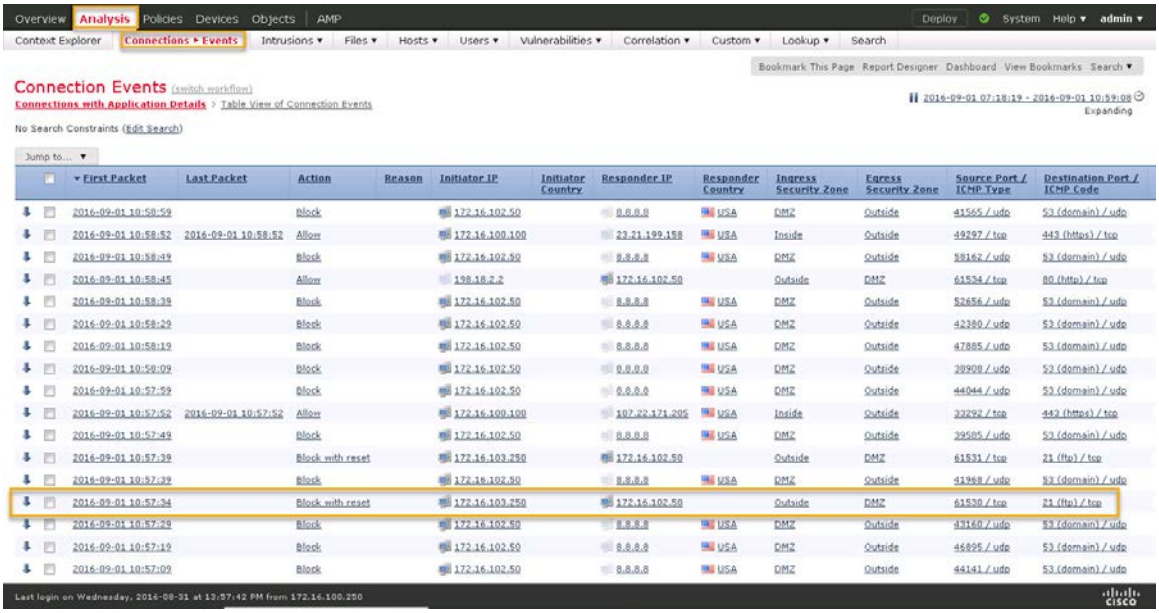
330. Make sure that this workstation still has access to the DMZ server's web page using the internal IP though. Go to **http://172.16.102.50**. This should work.

Figure 445. HTTP still works



331. 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 446. Review Connection Events



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".

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

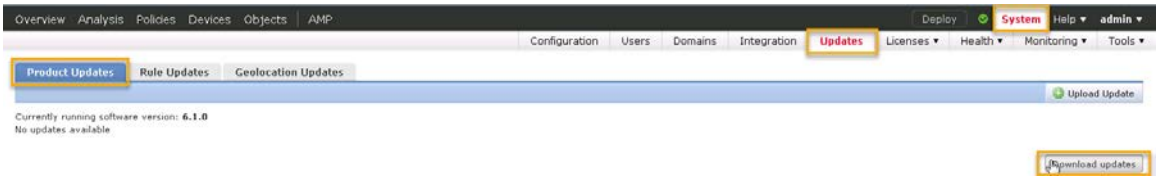
332. Navigate to **System > Updates**.

333. As you can see there are three tabs here. You will cover each and perform the latest update for each as well.

334. Click on the **Product Updates tab**:

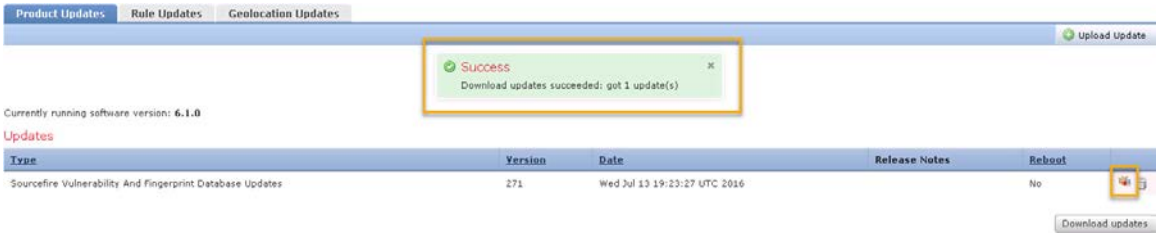
335. At first you might think that there are no updates to be had based on the initial screen. Click on **Download updates** though and you should get some possible updates.

Figure 447. Download Updates



336. 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 271 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 448. Click Install

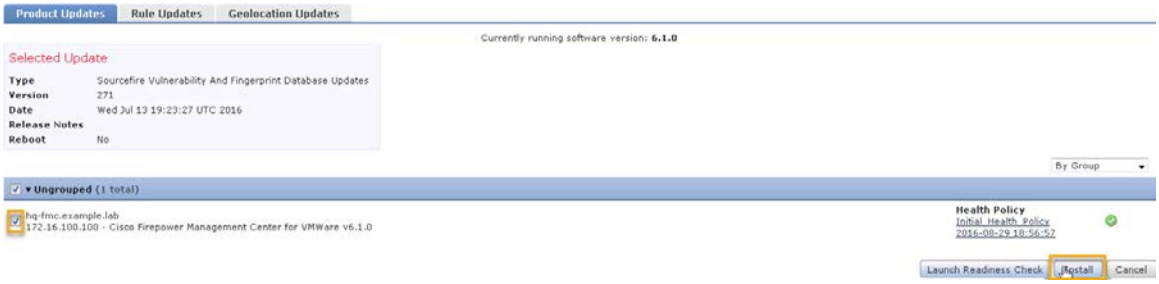


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

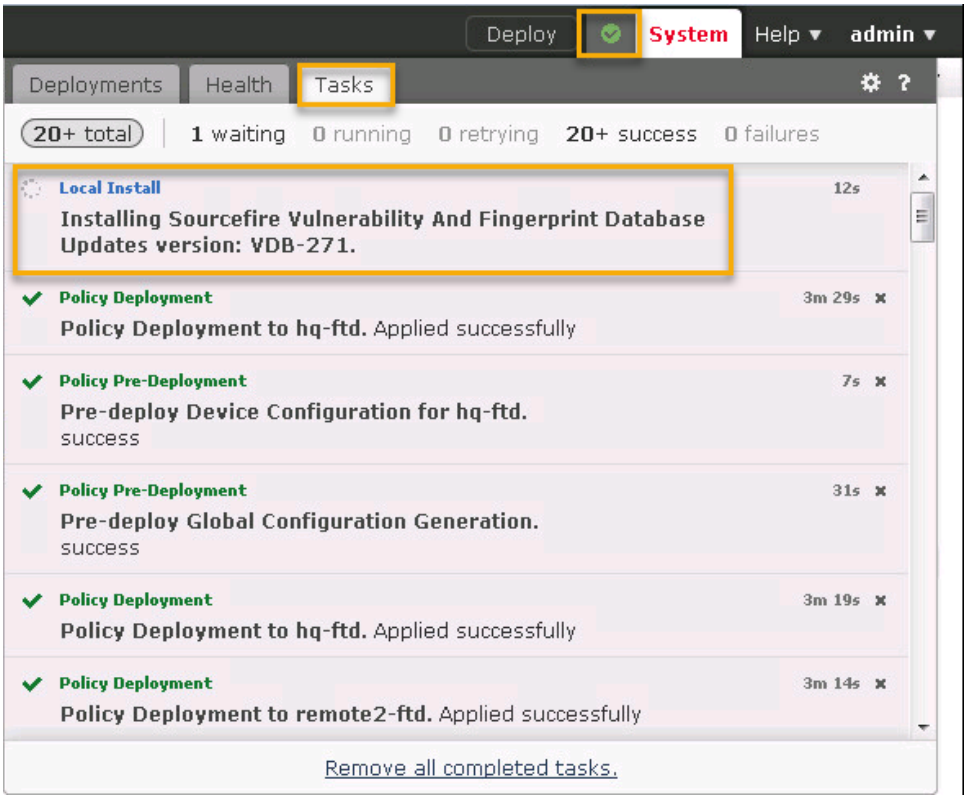
337. Check the box for the **hq-fmc.example.lab** device and click **Install**.

Figure 449. Click Install



338. 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 450. Message Center



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

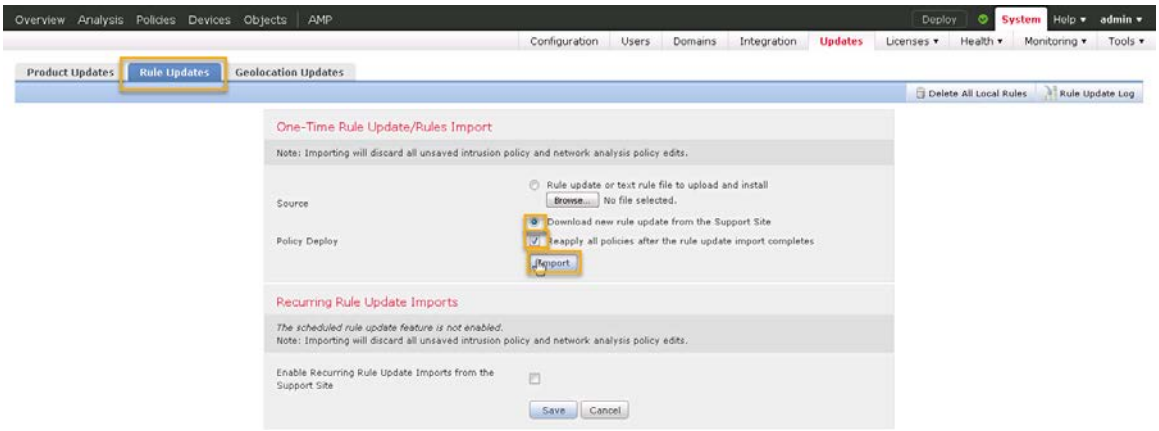
https://t.me/learningnets

339. Click on the **Rules Updates tab**:

340. 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.

341. ***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 451. Download and Import update



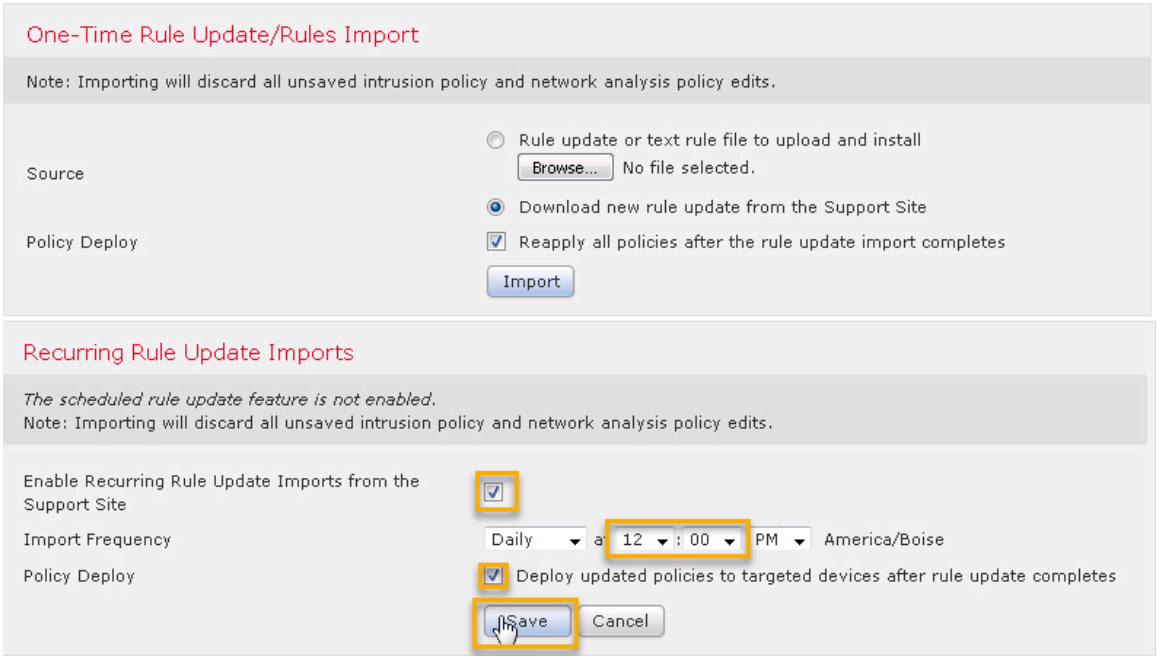
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

342. 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.

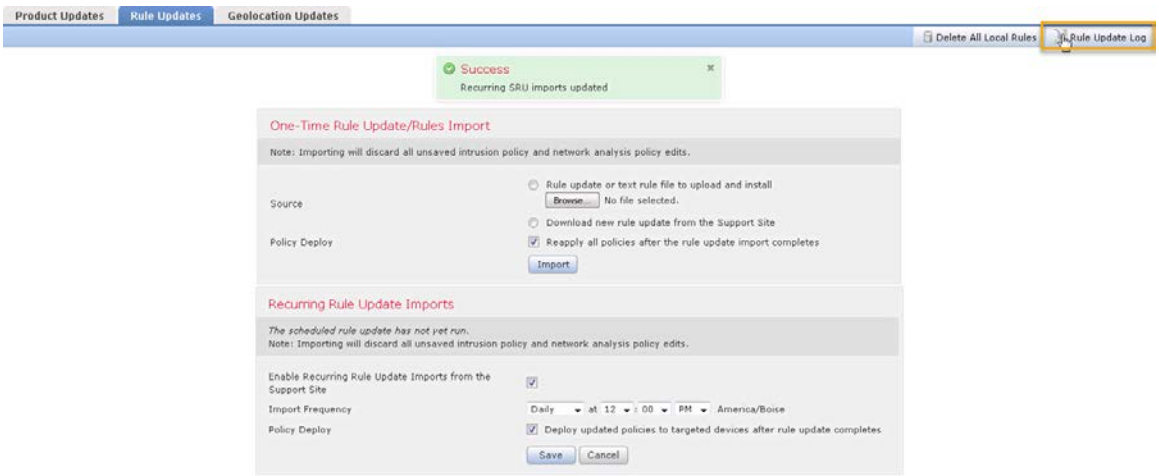
343. With that box check you can now set up the time and frequency of when updates are imported. You can also automatically deploy updates to the devices! For now, **set any time**, check the **Deploy updated policies to targeted devices after the rule update completes** box and click **Save**.

Figure 452. Enable Auto Updater



344. Click the **Rule Update Log** to see a tabular list of want updates have been downloaded and when.

Figure 453. Click Rule Update Log



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

345. View the log Summary.

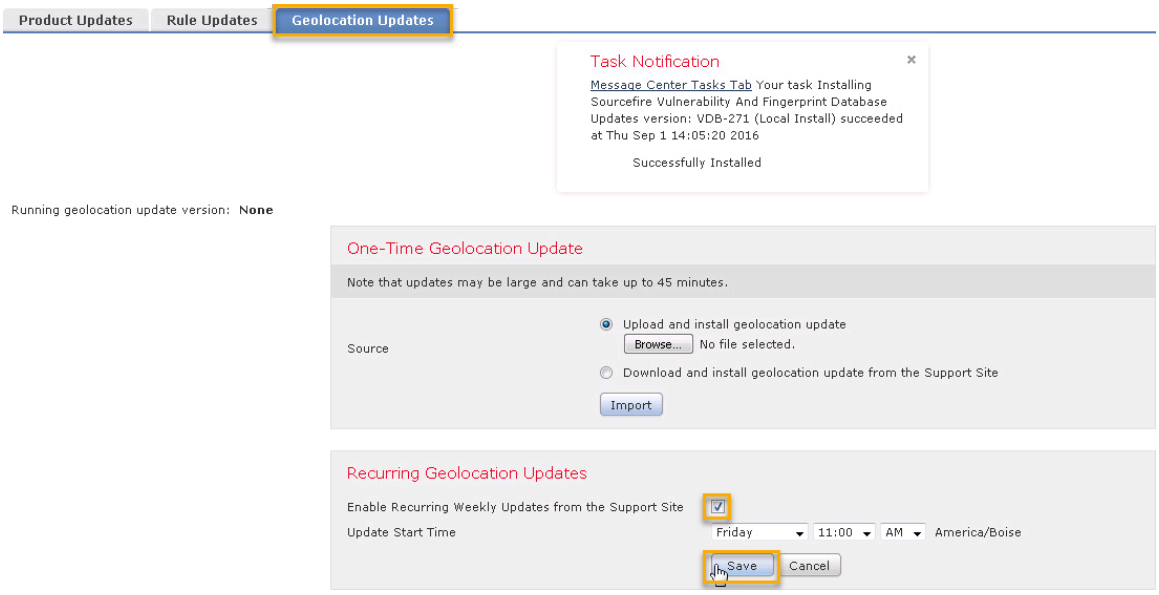
Figure 454. View Log



346. 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 455. Enable Auto Updates

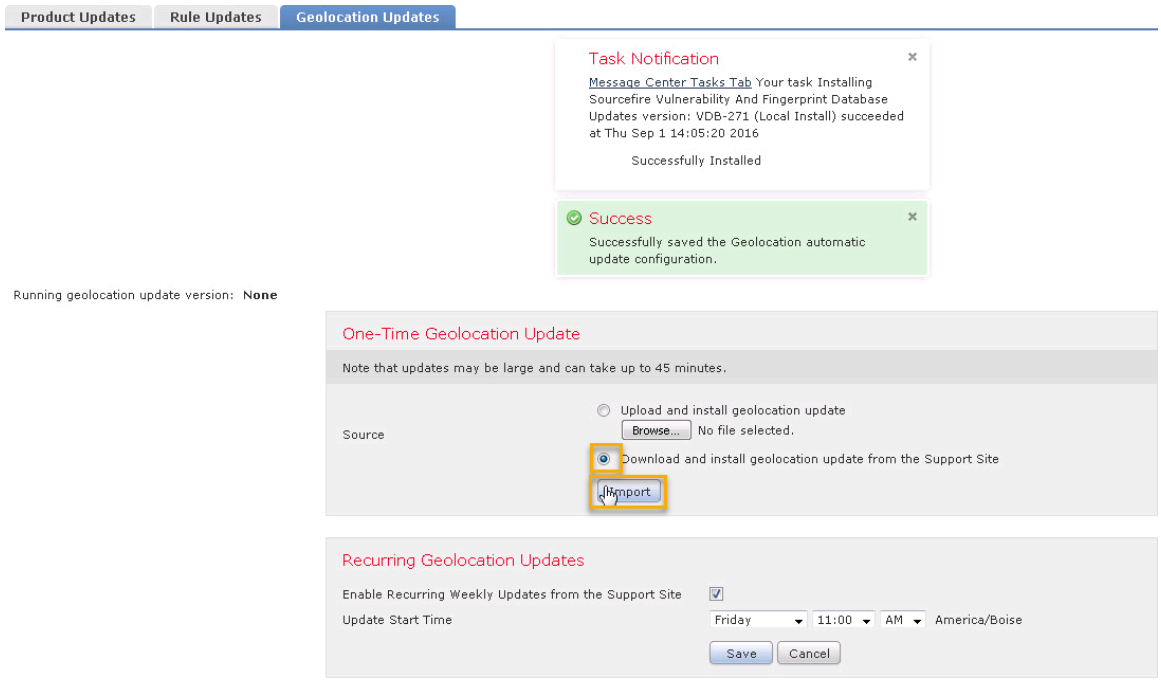


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

b. Now click the **Download and install geolocation update from the Support Site** radio button and then click **Import**.

Figure 456. Geolocation Updates



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Whois and Geolocation Searches

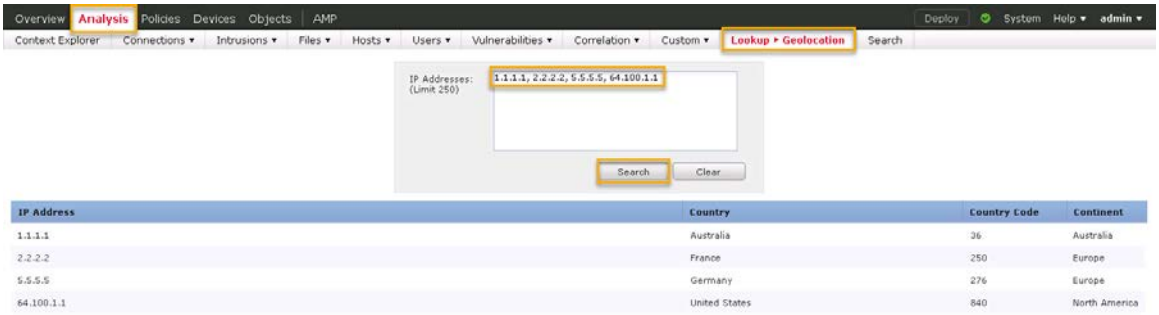
This section doesn't really belong in the "Monitoring and Maintenance" scenario but it is related to the Geolocation Database you have started to download. These two features provide informative information about an IP address, who owns it, and from what part of the world is it from.

347. Navigate to Analysis > Lookup > Geolocation.

348. 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).

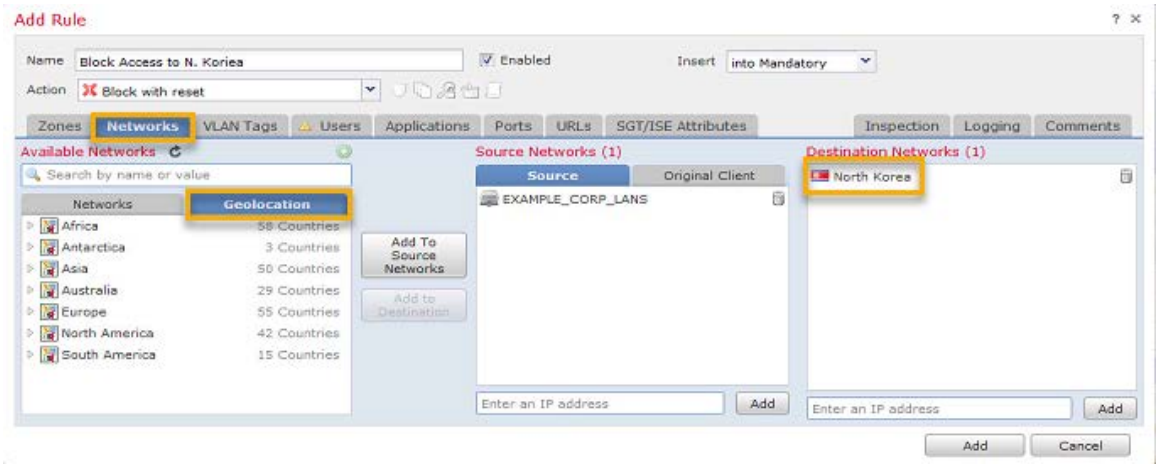
349. Click **Search** and review the result. From this information you can determine the origin of the respective IP address.

Figure 457. See where IPs are Geolocated



350. 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 458. Block Access to North Korea



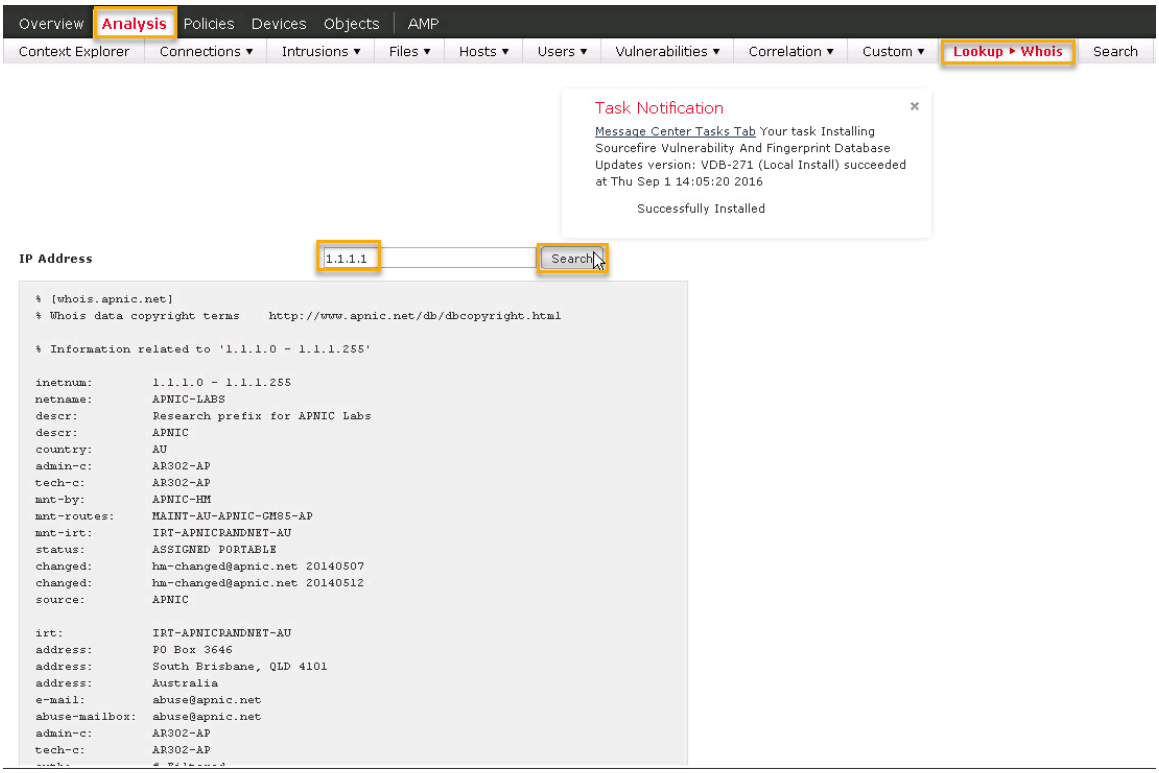
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

351. Navigate to **Analysis > Lookup > Whois**.

352. 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 459. Whois Results



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

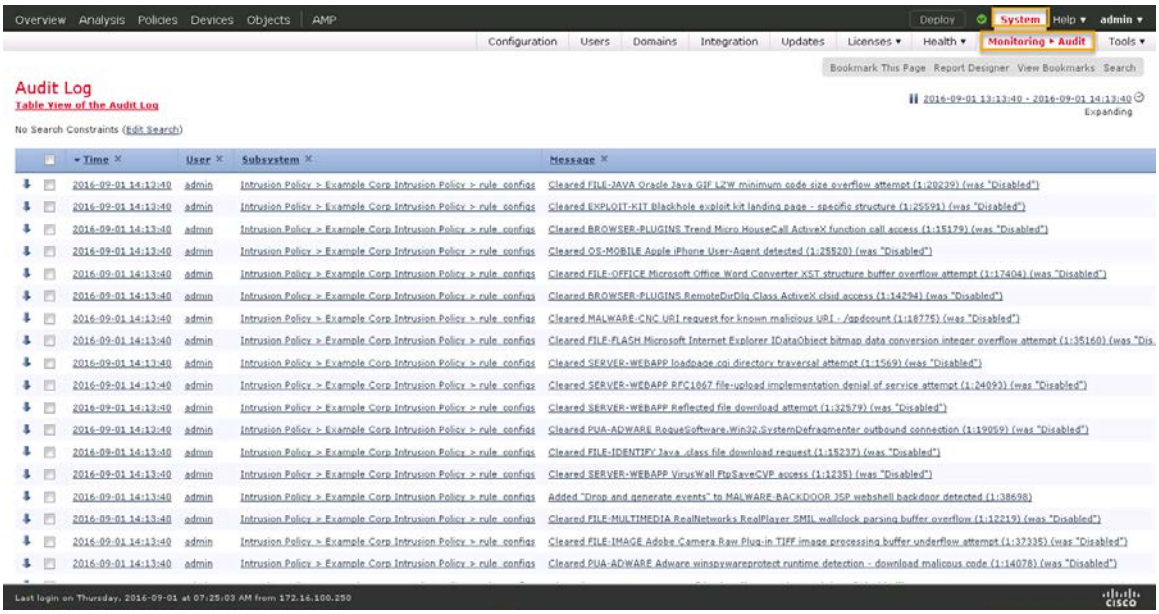
https://t.me/learningnets

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.

353. 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 460. Big Brother Knows Everything

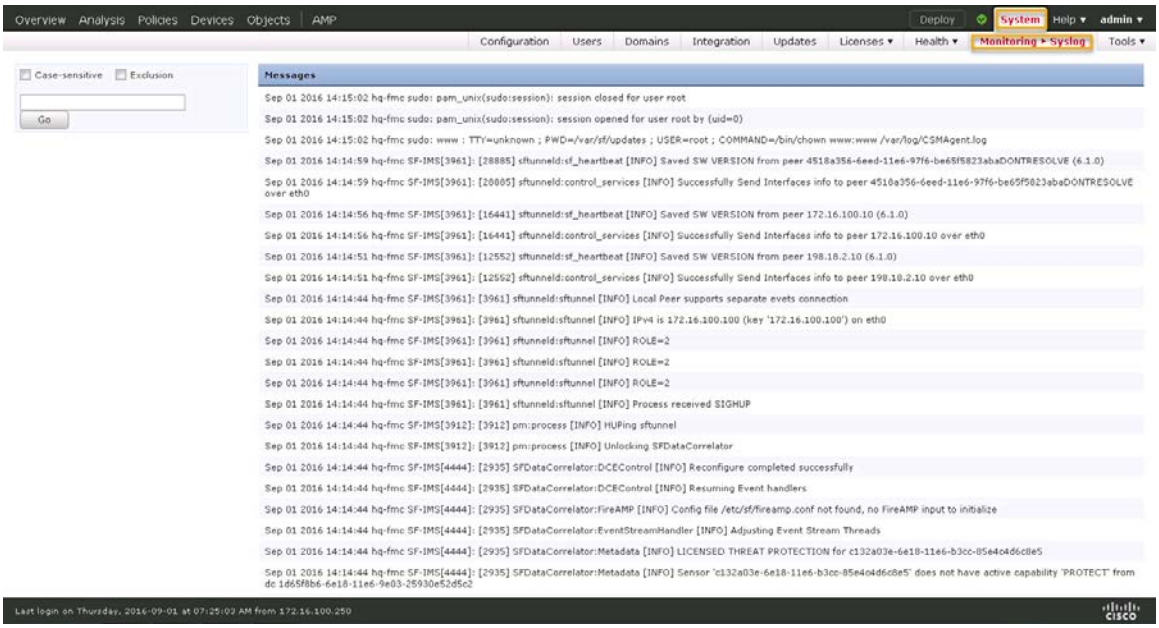


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

354. Navigate to **System > Monitoring > Syslog**. As you might expect this is a view of the syslog buffer.

Figure 461. Syslog Buffer



355. Navigate to **System > Monitoring > Statistics**.

356. 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 462. Select Devices to view Statistics

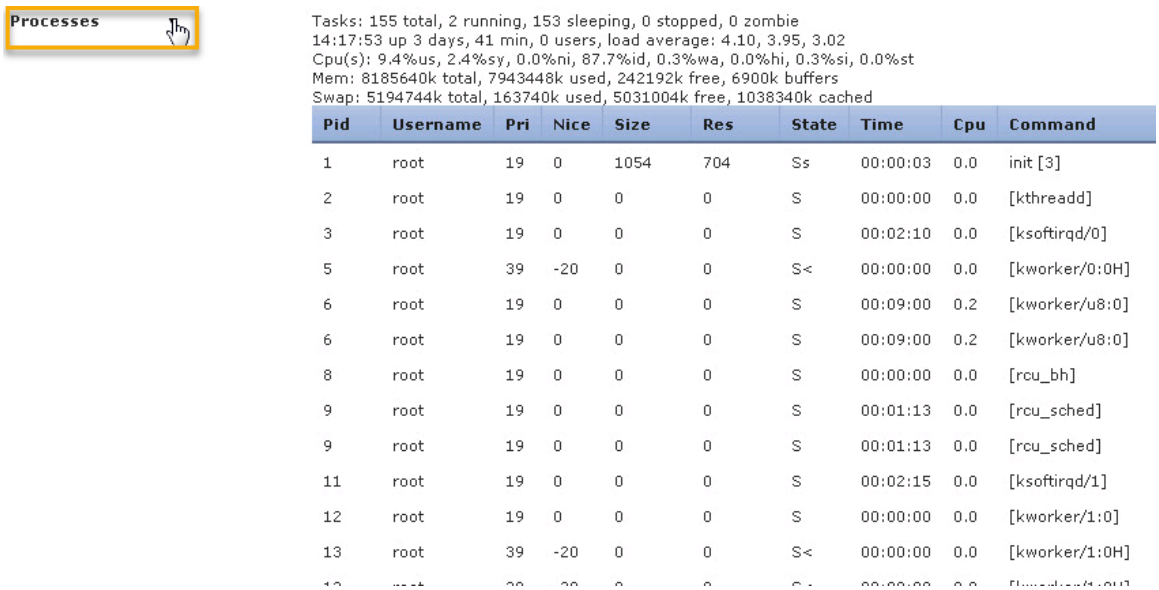


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

357. 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 463. To “top” it all off



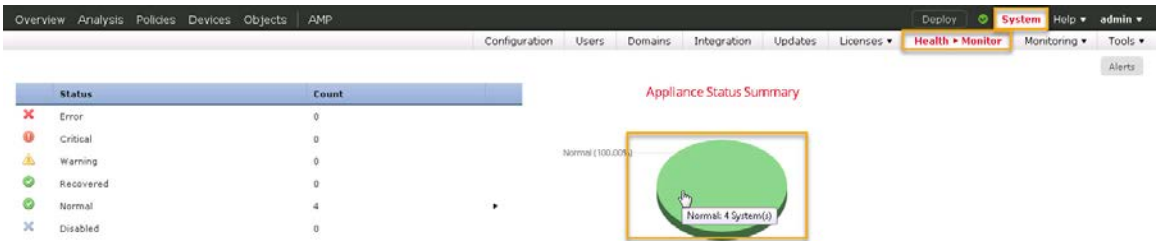
System Health

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.

358. 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.

359. In order to get any information, you need to click on the **pie chart sections**.

Figure 464. Click the sections of the pie chart

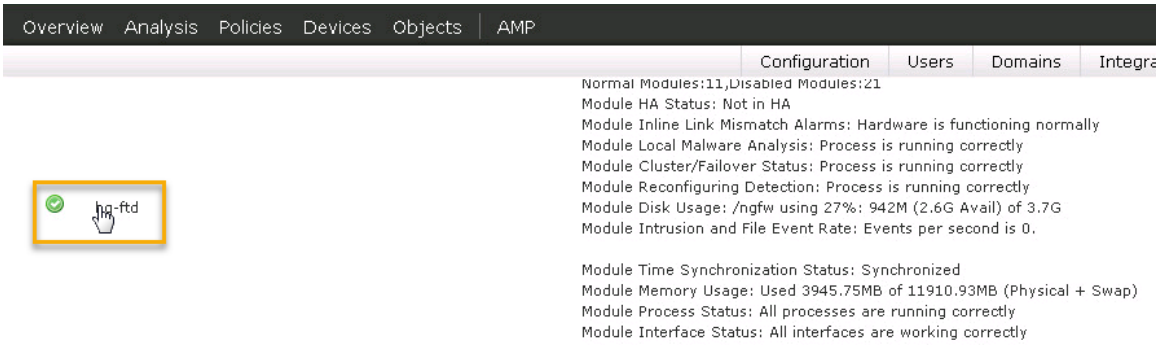


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

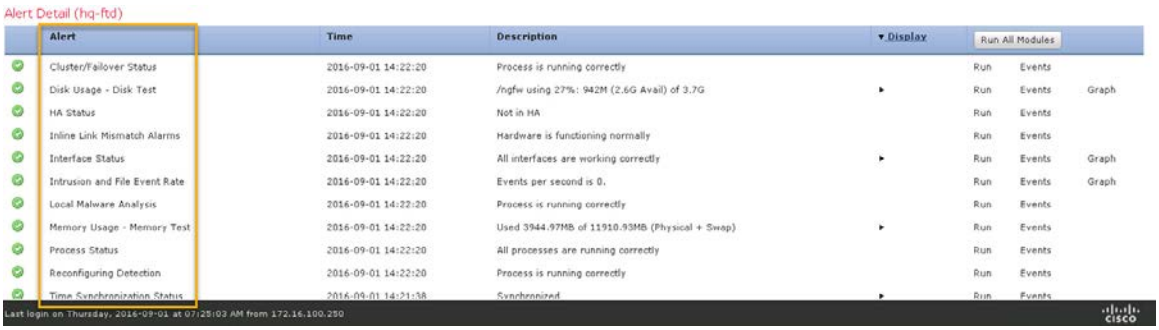
360. Select one of the **FTD devices** to drill into it. (Though you can select the FMC device you won't see the Threat Defense CLI tab which is reference in a bit within this lab guide.)

Figure 465. Select an FTD device



361. 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.)

Figure 466. Alert Detail section



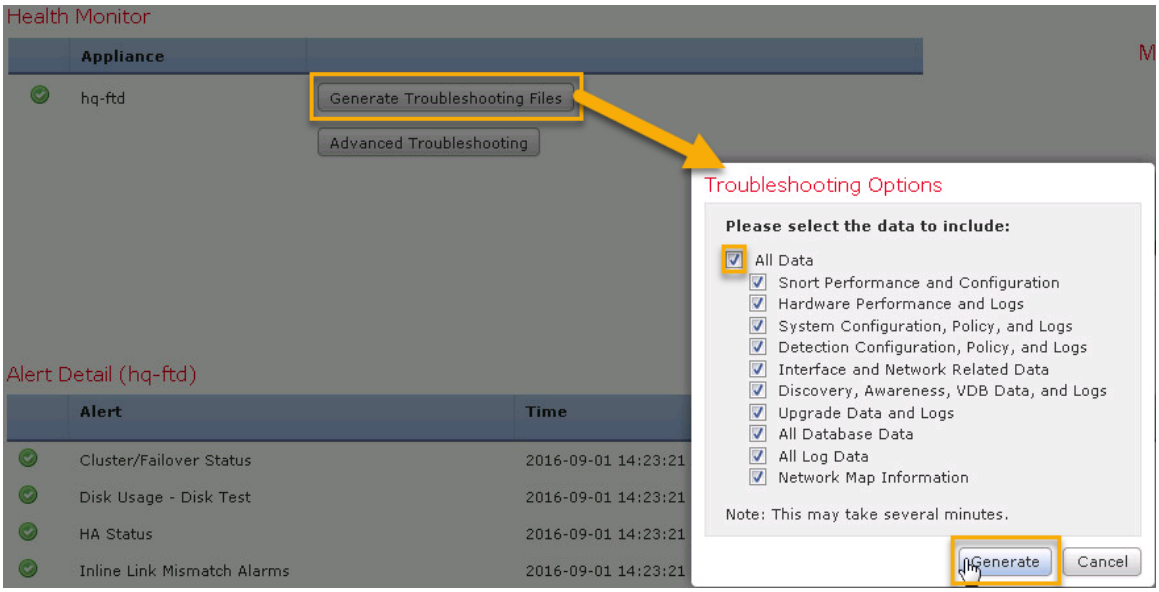
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

362. Click on the **Generate Troubleshooting Files** button.

363. 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 467. Generate Troubleshooting files

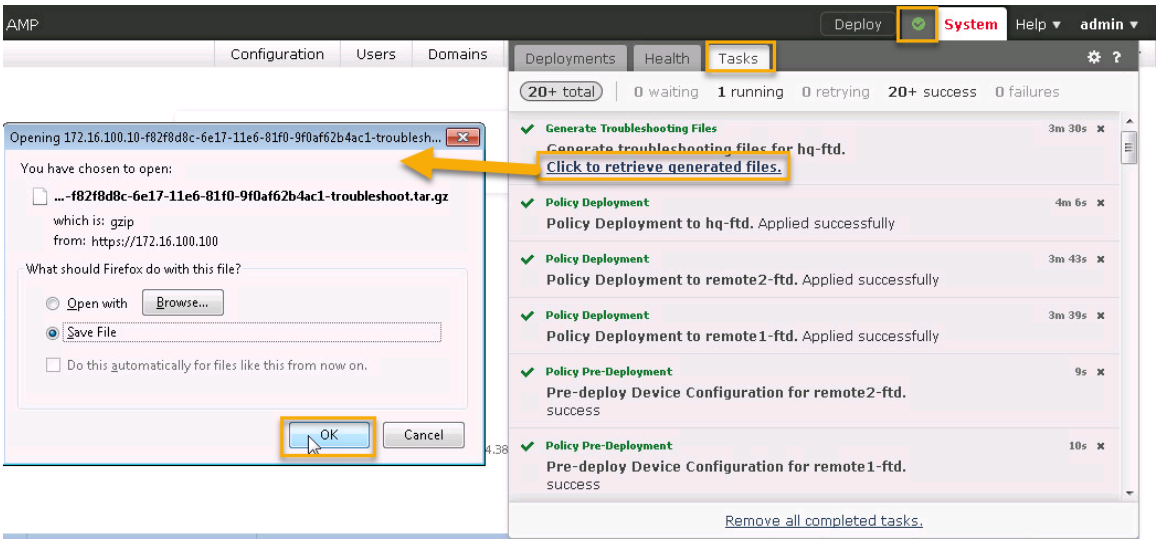


364. There will now be a Task Notification notice at the top of your browser window indicating that you can monitor the generation of these files by looking at the Tasks tab within the Message Center. Click the **Message Center Tasks Tab** link to open up this popup window.

365. Once the task to generate the troubleshooting files is complete click the **Click to retrieve generated files** link.

366. Click **OK** to save the file.

Figure 468. Save troubleshooting files

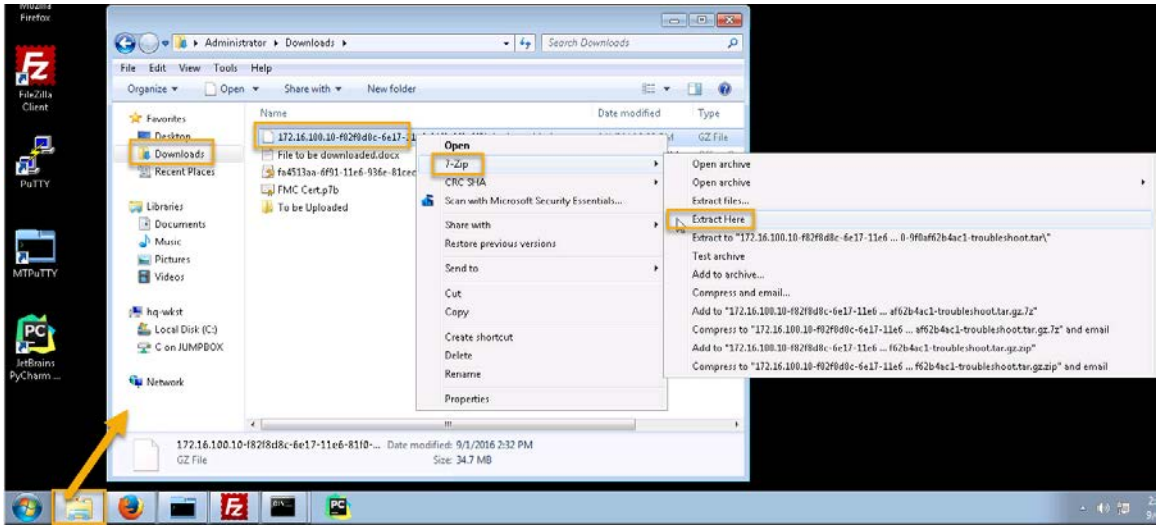


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

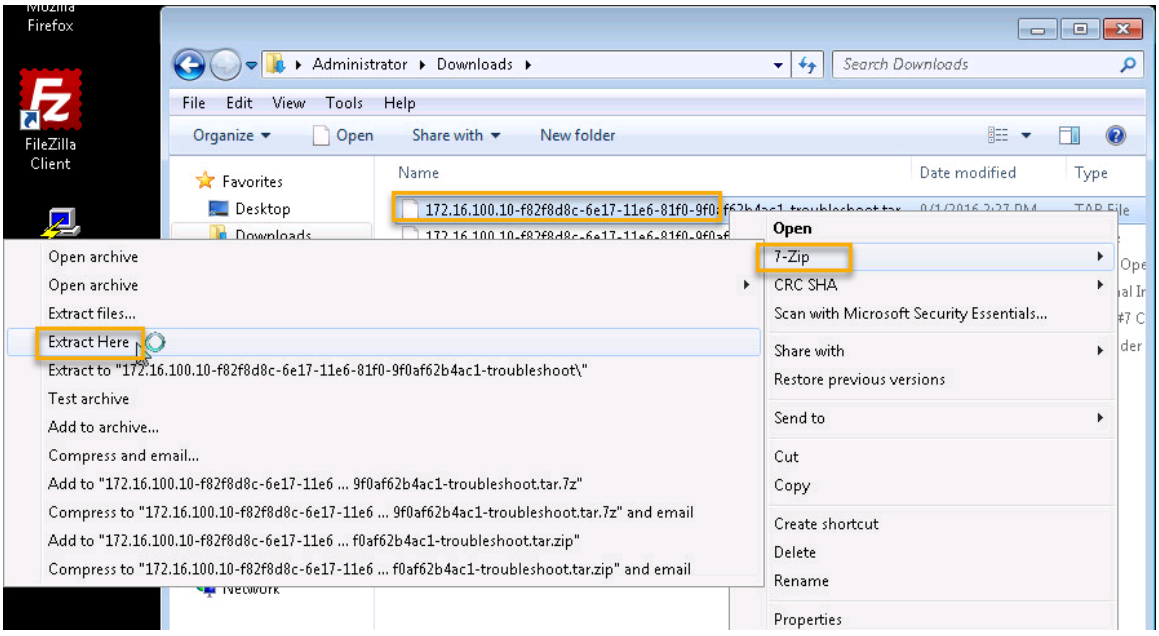
367. Open up **Windows Explorer**, navigate to the **Download** folder, **right-click** on the troubleshooting file, select **7zip > Extract Here**. This will uncompress the tar file.

Figure 469. Extract from gzip



368. Perform the extraction process again on the new tar file. (**Right-click** the file, select **7zip > Extract Here**.)

Figure 470. Extract from tar

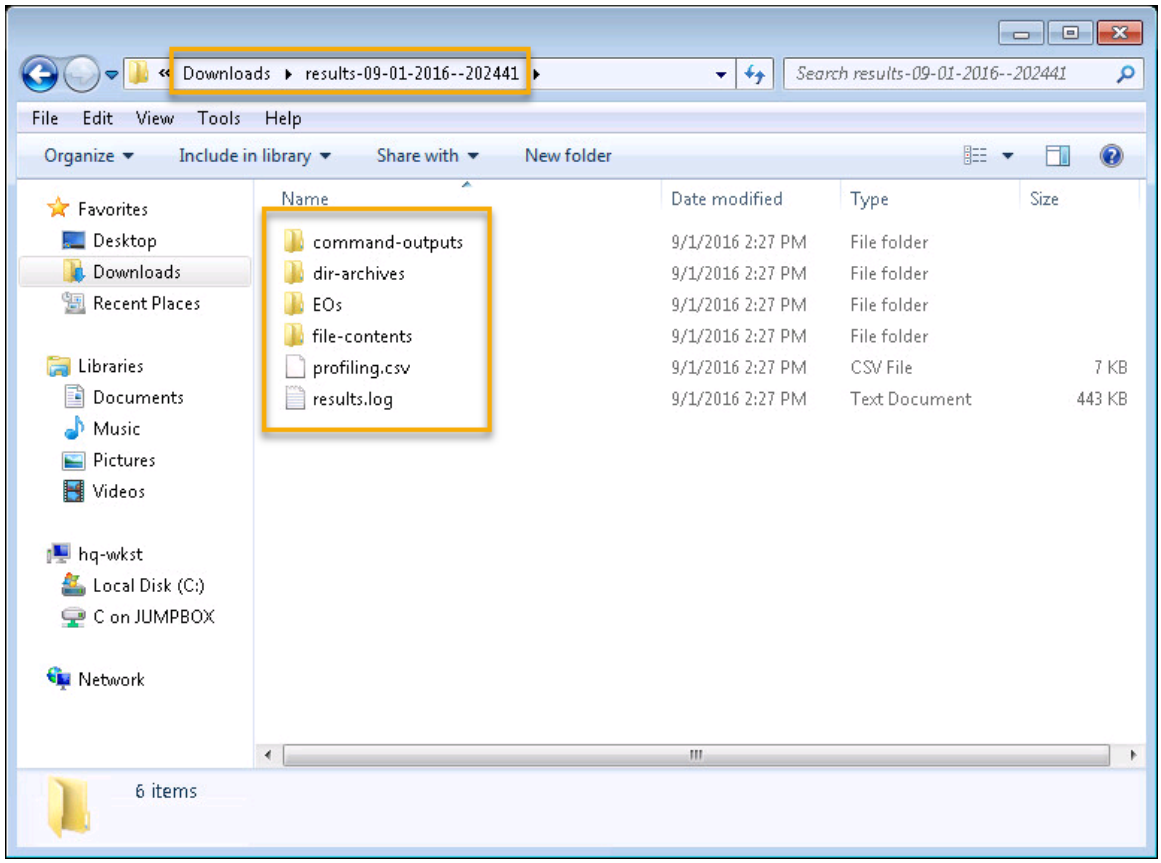


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

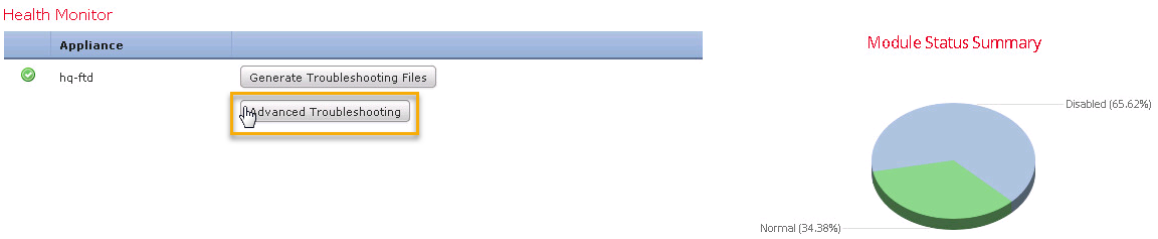
369. Finally, you will have a folder containing all the troubleshooting files. Feel free to poke around in these folders and files.

Figure 471. Files, files, files!



370. Return to the FMC Administration GUI and click the **Advanced Troubleshooting** button.

Figure 472. Advanced Troubleshooting



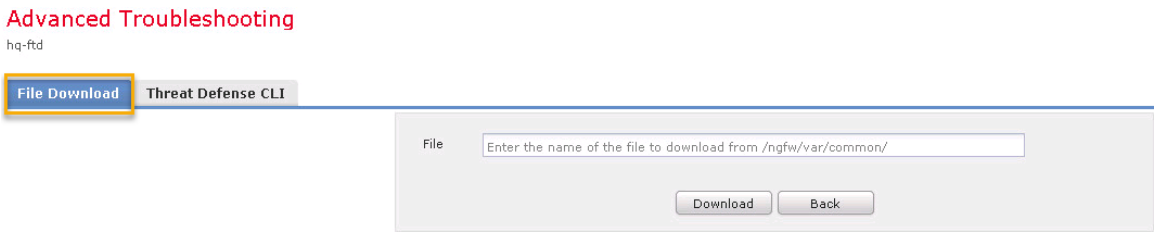
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

371. 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.

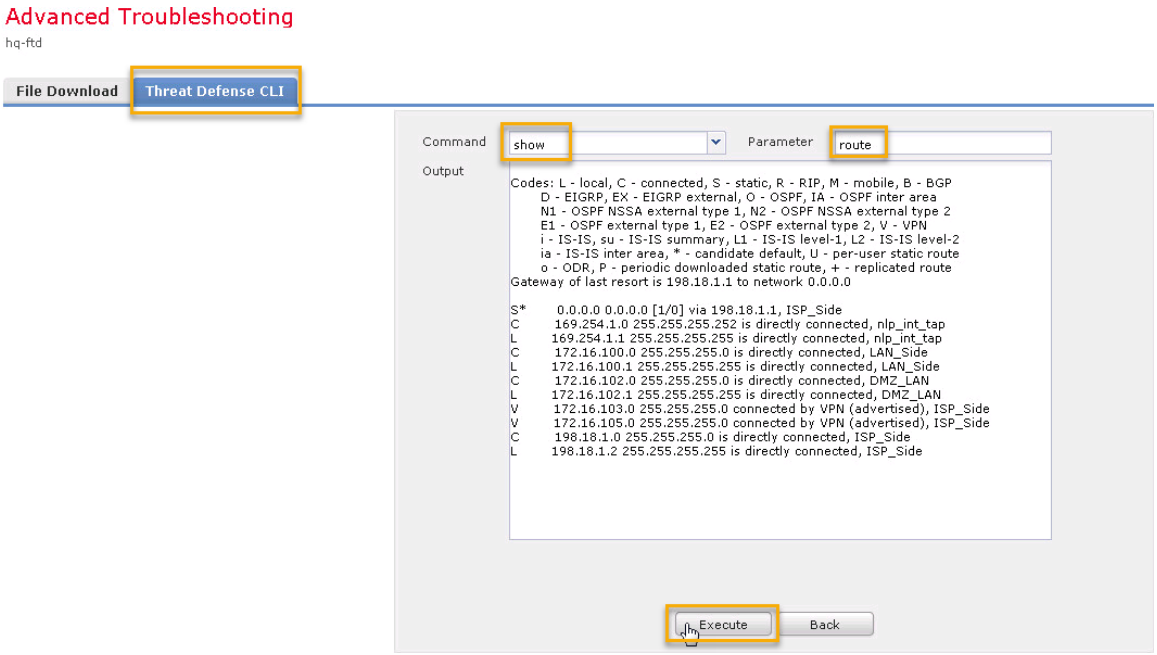
Figure 473. File Download tab



372. 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 474. Show route CLI

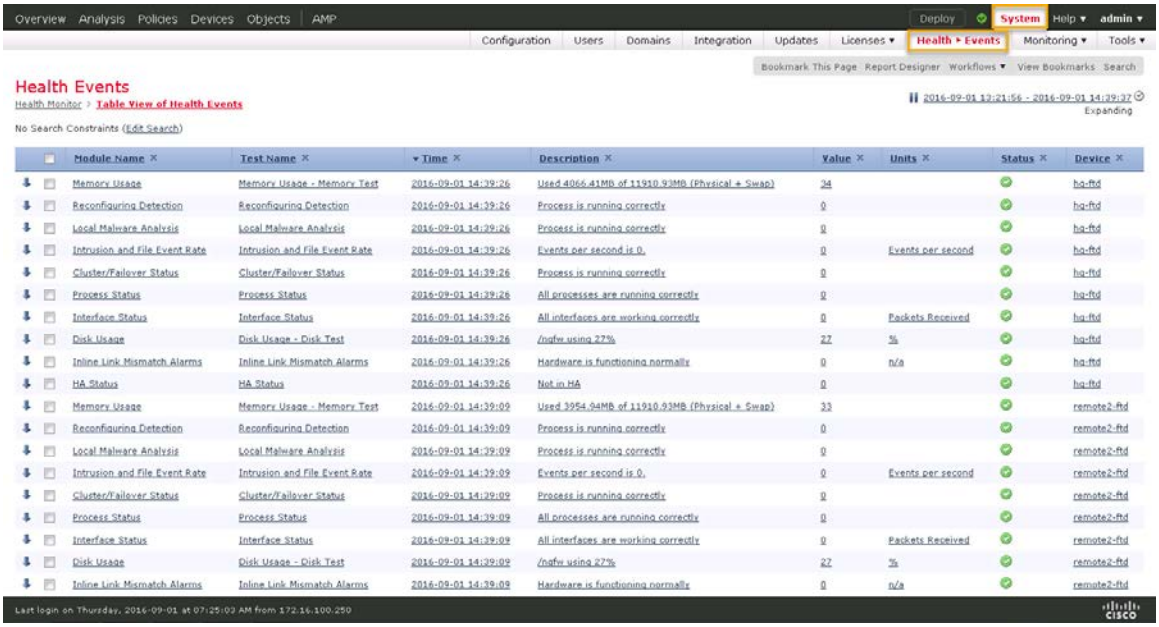


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

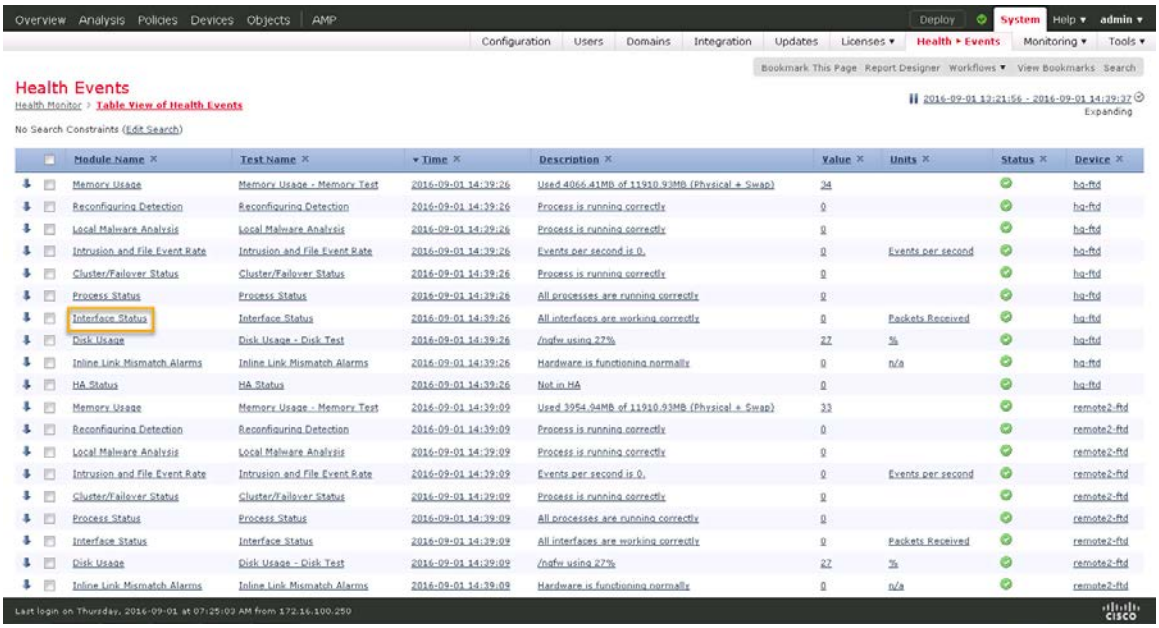
373. Skipping the Policy page for now, navigate to **System > Health > Events**. This page is a tabular history of modules and tests that are running against each FMC managed device on a regular basis. You can use this to drill into specific problems you might be seeing to figure out how long that issue has been ongoing and whether it is an intermittent problem.

Figure 475. Health Events



374. Click on the **Interface Status** link in the Module Name column.

Figure 476. Interface Status



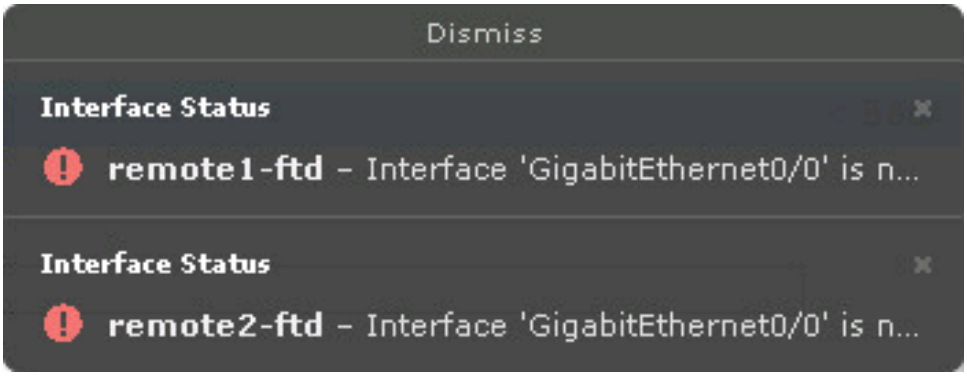
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

375. 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.

376. Throughout the lab, have you been getting several popup indicators telling you that your FTD management interfaces are not receiving any packets?

Figure 477. Annoying Error Message



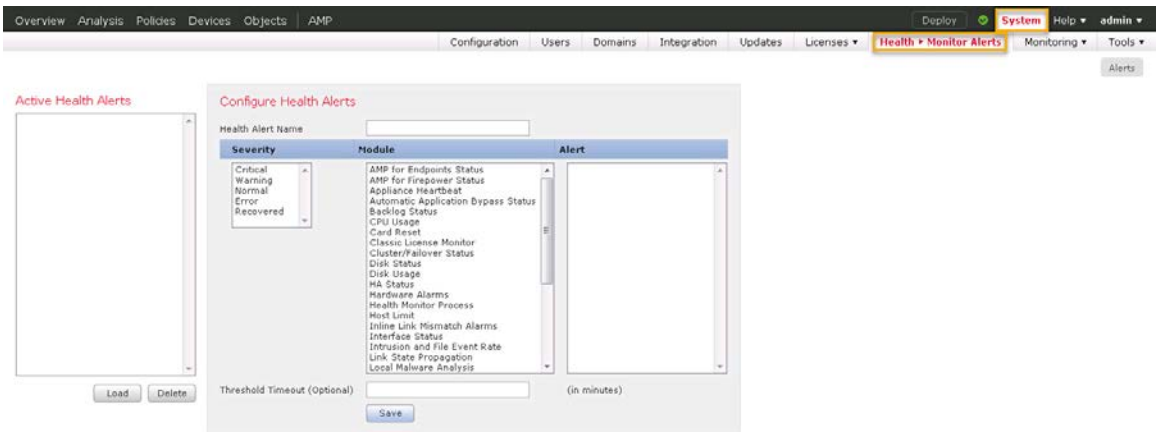
377. It might take some looking throughout the history of this particular test but you should find some failures.

Figure 478. Interface Status test failures



378. 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 479. Monitors Alerts page



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

379. Finally let's go to **System > Health > Policy**. This is the heart of the whole System Health configuration.

380. **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 480. Edit Health Policy



381. Click the **Interface Status** link.

    a. Click the **Off** radio button.

Figure 481. Turn off Interface Status testing



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

382. Scroll down and click **Save Policy and Exit**.

Figure 482. Save and Exit



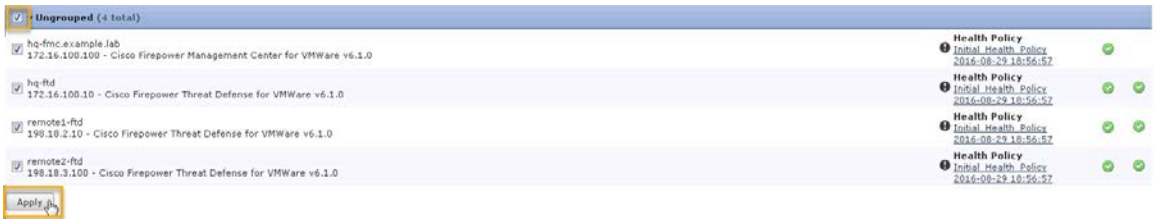
383. Click the **green checkmark** (the apply button) on the **Initial Health Policy** policy row.

Figure 483. Click green checkmark



384. Check the boxes next to **all the devices** and click **Apply**. (No more erroneous nagging messages about interfaces not receiving packets. YAY!)

Figure 484. Free of the tyranny of Interface Status warnings



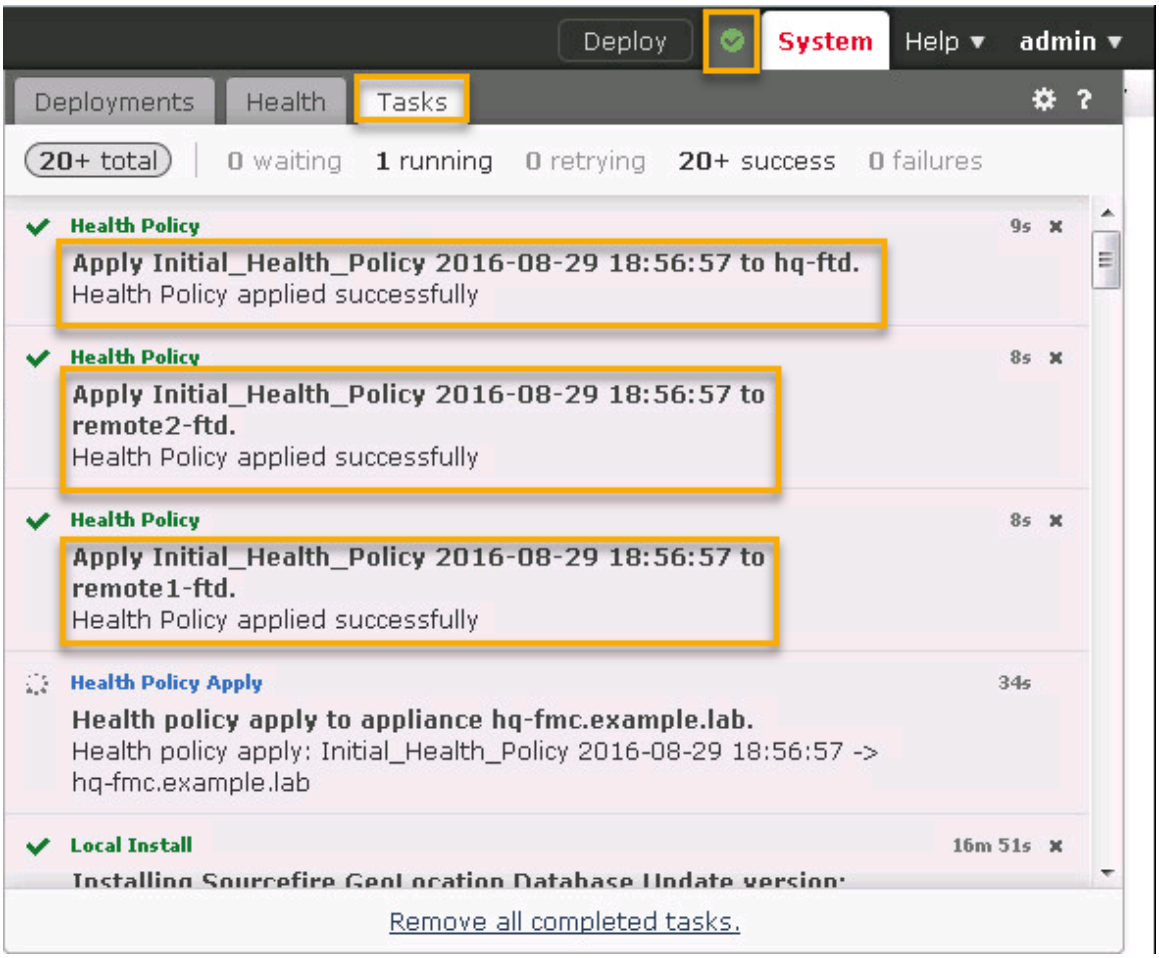
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

385. Once the deployment is complete the Message Center's Health tab should no longer show warnings/errors regarding interfaces not receiving packets.

Figure 485. Health Policy Updated on all Devices



386. 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 486. Task Notification



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

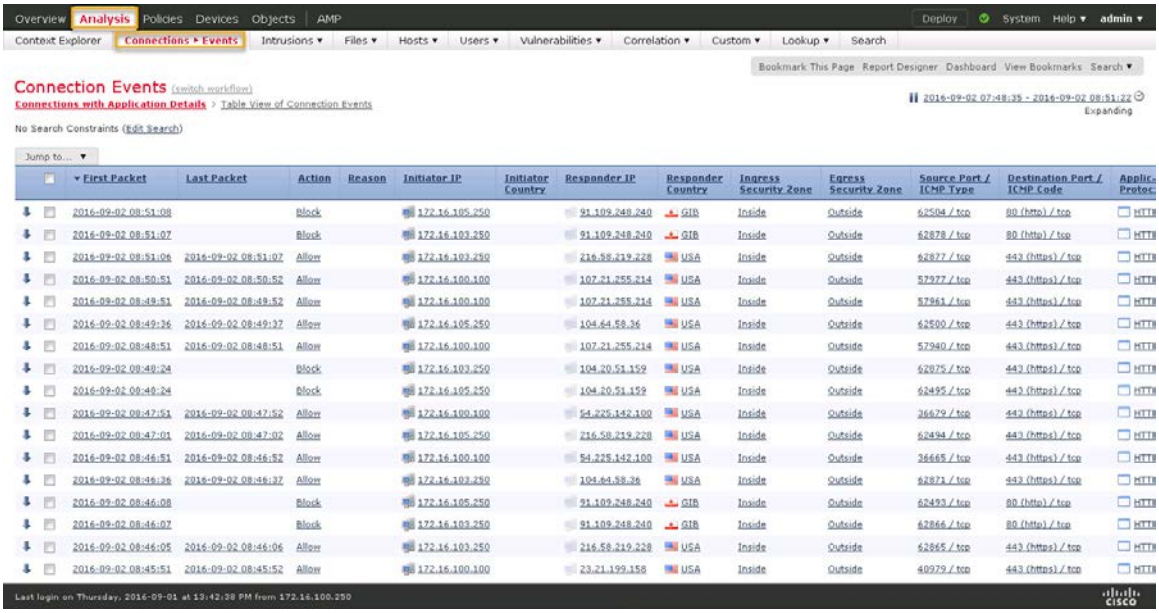
In this scenario you will explore the Connection Events, File Events, and the Host's Network Map features.

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.

387. 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 487. Connection Events

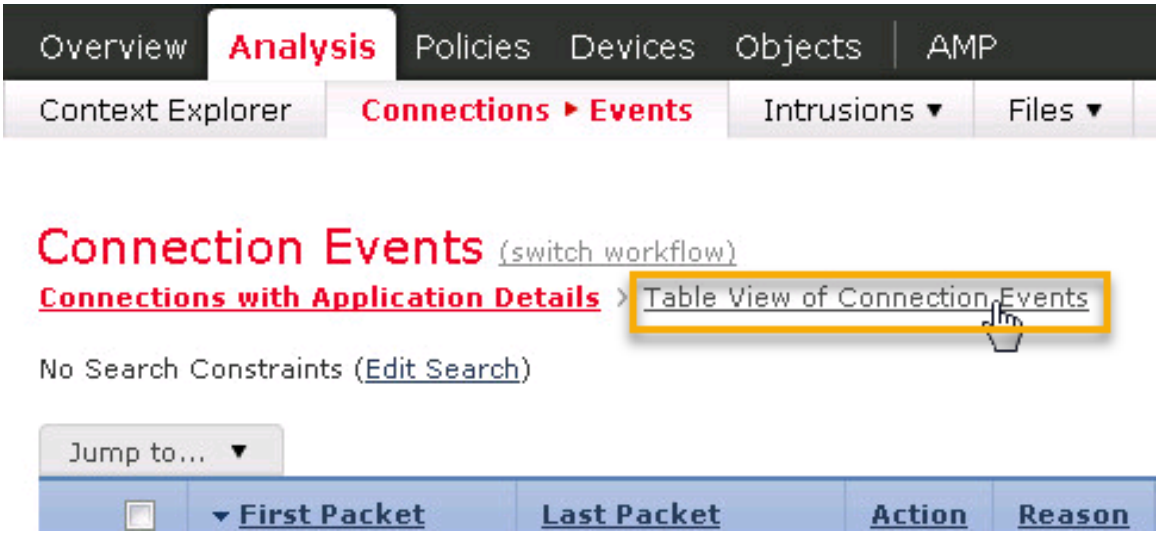


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

388. This page is just the “summary” page though. To get additional detail about each entry click the **Table View of Connection Events** link.

Figure 488. Click link

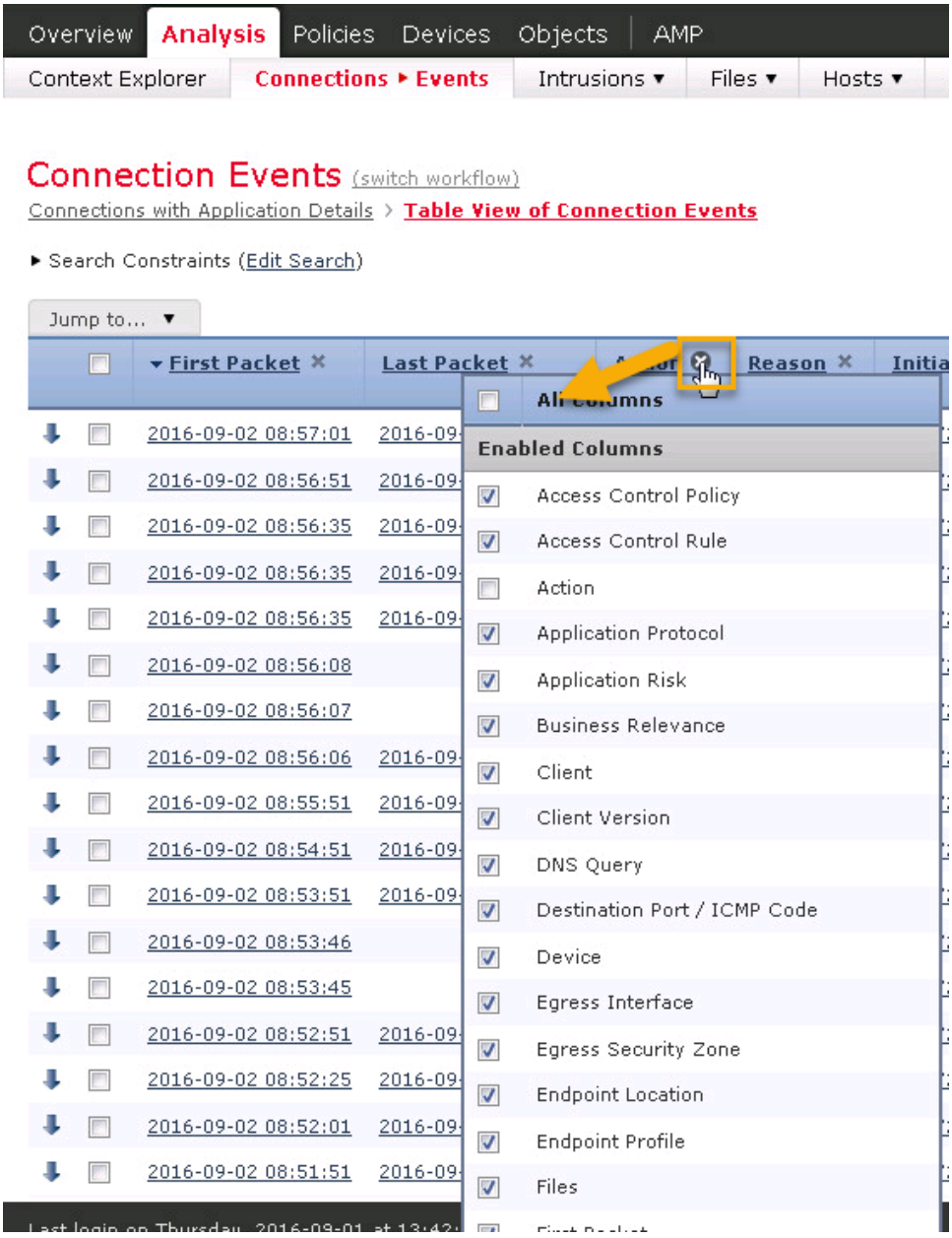


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

389. 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 489. Selecting Columns



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

390. 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 490. Click Cancel

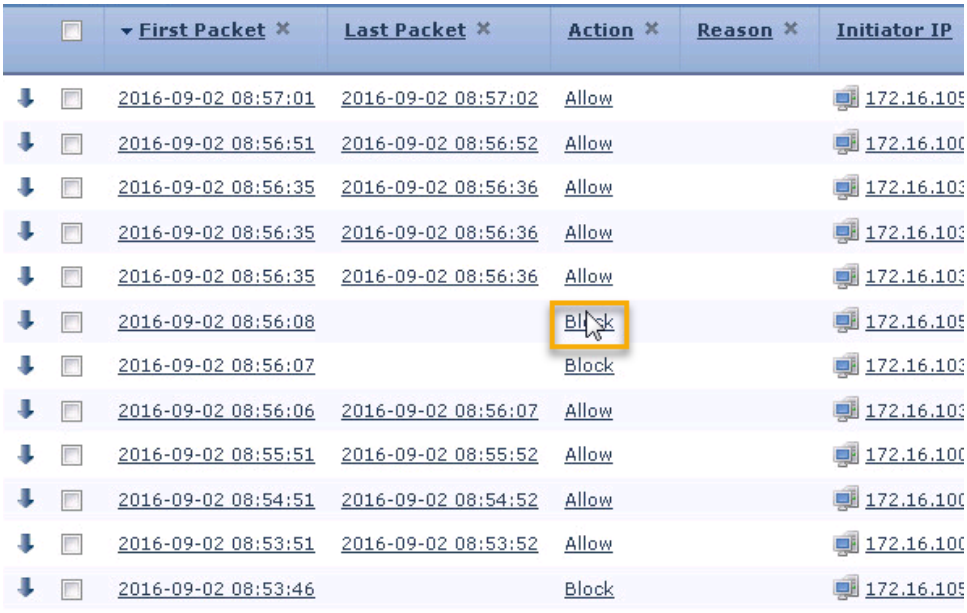


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

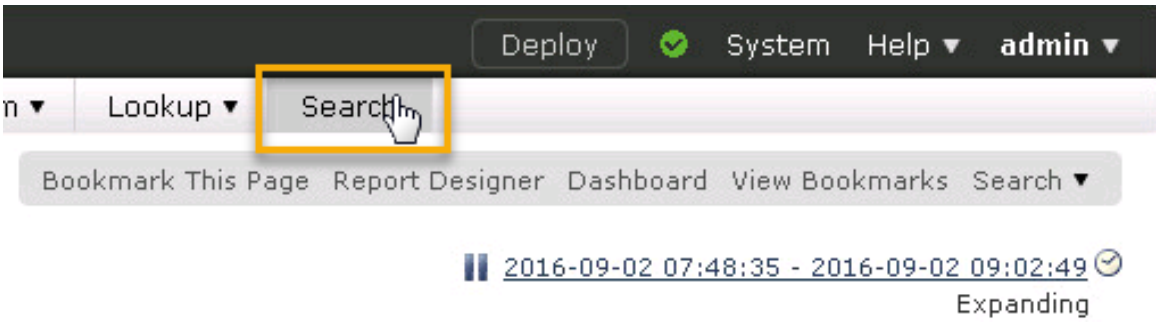
391. Clicking on any link from this list of events (such as the **Block link in the Action column**) you will be filtering this list to only events that have this particular feature.

Figure 491. Filter by Block Action



392. 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 492. Click the Search button



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

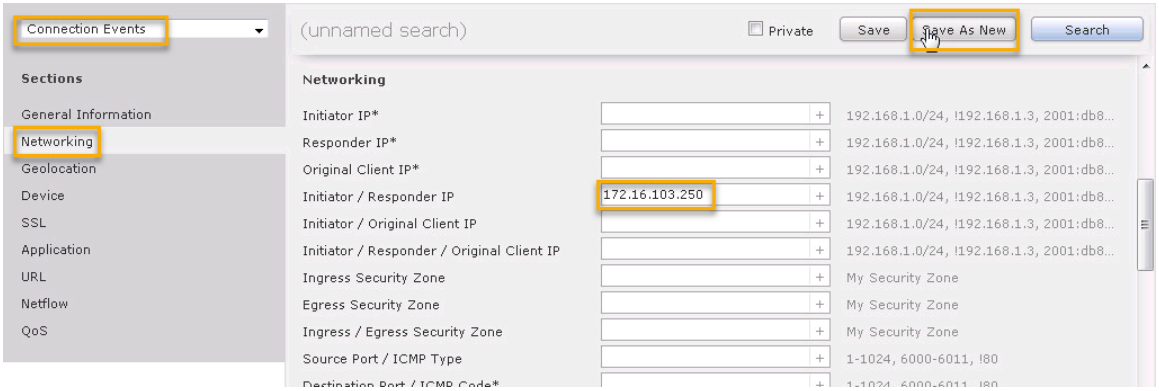
393. On the search tab you can create a custom search for any of the Analysis event logs. Select **Connection Events** from the dropdown list to change the view to only list the variables related to the Connection Events.

394. 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.

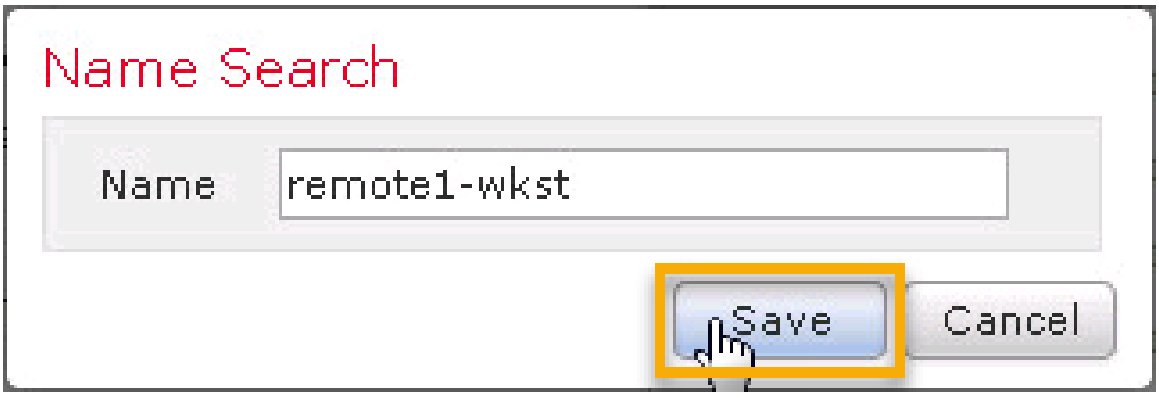
395. Click **Save As New**.

Figure 493. Build a filter



396. In the Name Search popup use **remote1-wkst** for the Name and then click **Save**.

Figure 494. Name and save



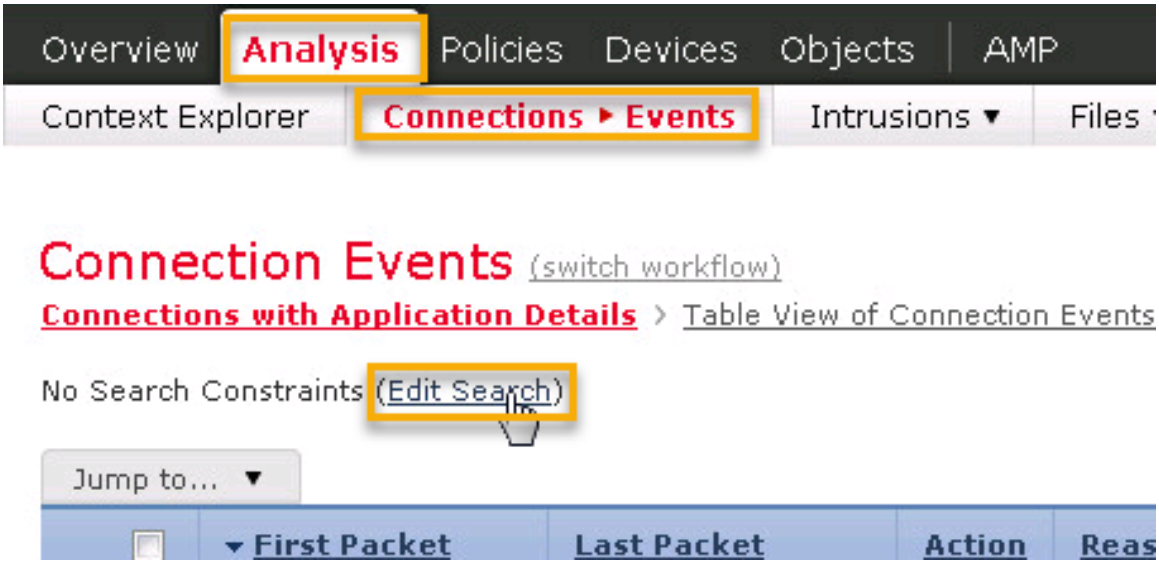
397. Navigate to **Analysis > Connections > Events** again.

398. Click the **Edit Search** link.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

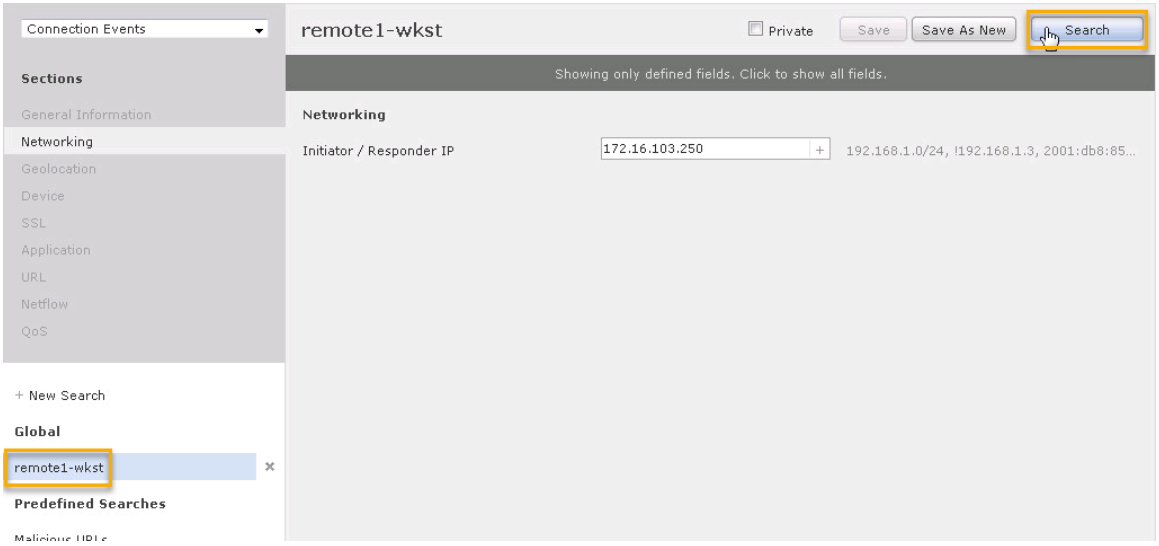
https://t.me/learningnets

Figure 495. Filter by Search



399. 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 496. Filter by saved search

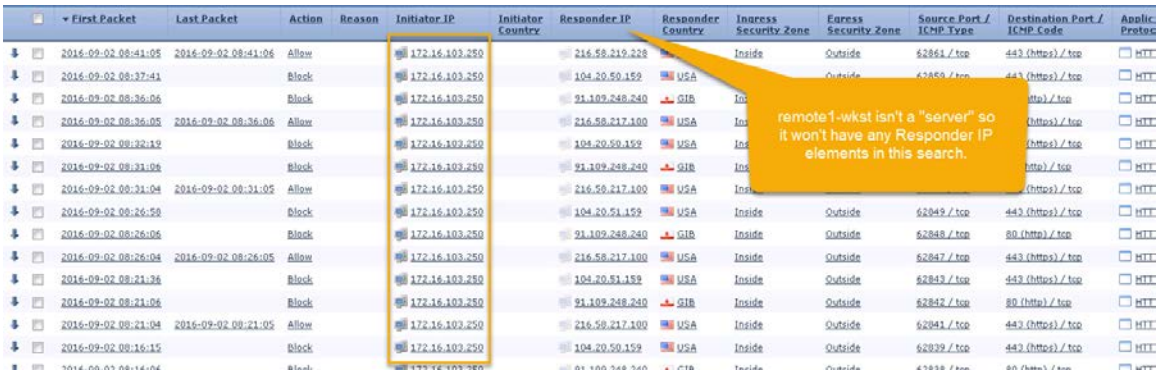


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

400. Now the Connection Events are filtered based on any traffic to/from remote1-wkst.

Figure 497. Filtered Connection Events

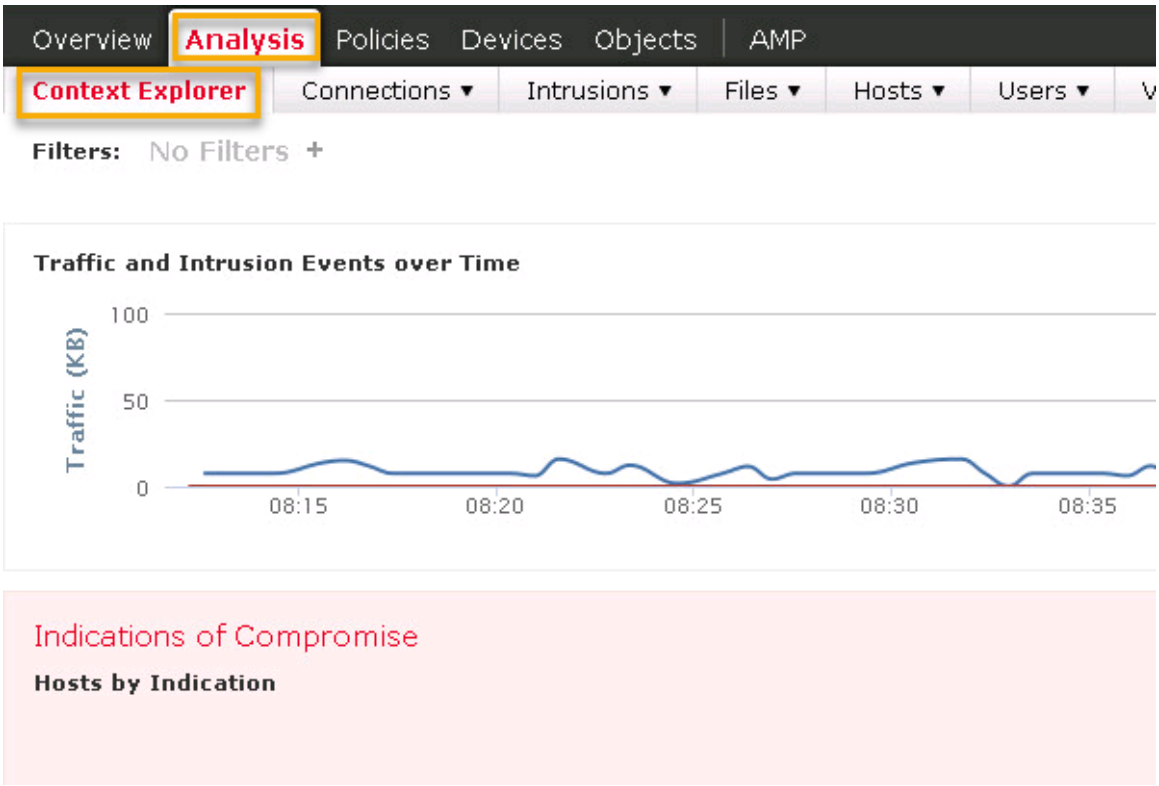


The Context Explorer

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.

401. To view what this page looks like navigate to **Analysis > Context Explorer**.

Figure 498. Context Explorer



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

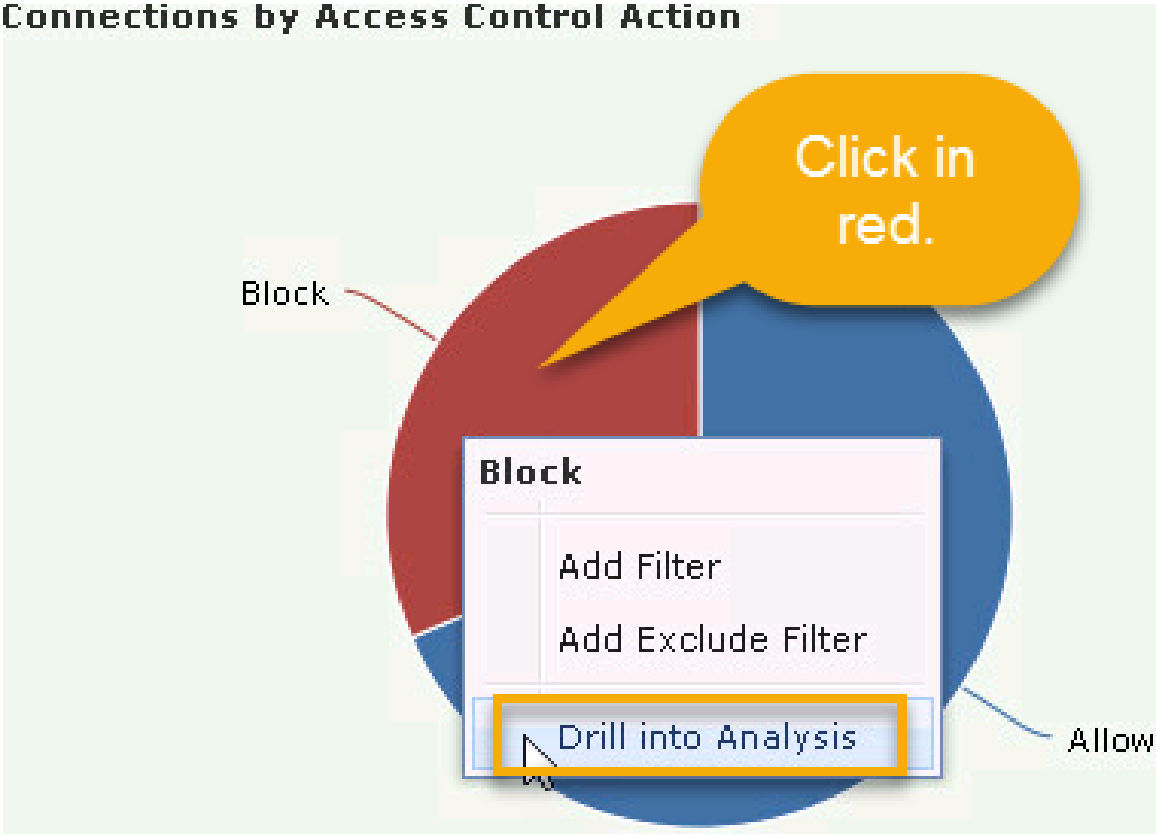
https://t.me/learningnets

402. Scroll down and view the type of information that is gathered so far and at your disposal.

403. Find the **Connections by Access Control Action** section and click on the **red slice** of the pie chart.

404. From the list of actions click **Drill into Analysis**.

Figure 499. Drill into Analysis



405. This is a quick way to see what Block actions have been taken by Access Control Policies.

Figure 500. Results



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

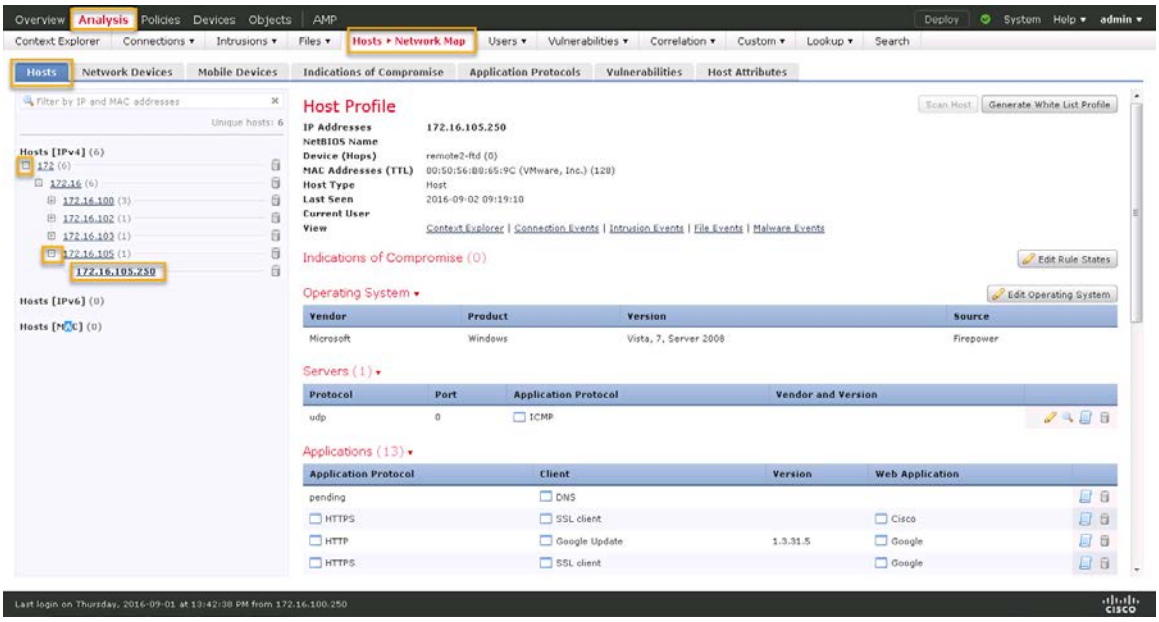
406. Navigate to **Analysis > Hosts > Network Map**. Each tab on this page correlates to some sort of analysis of the type of hosts, devices, and applications running on the Example Corp network.

407. 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 501. Details of a Host



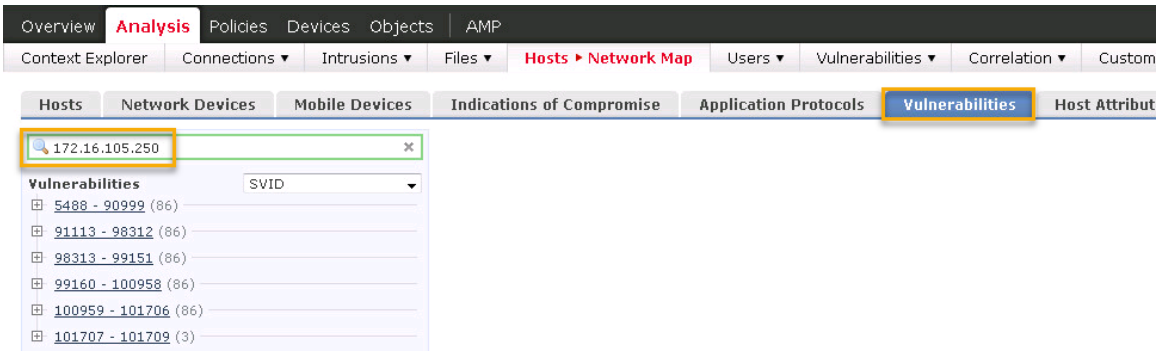
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

408. 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.

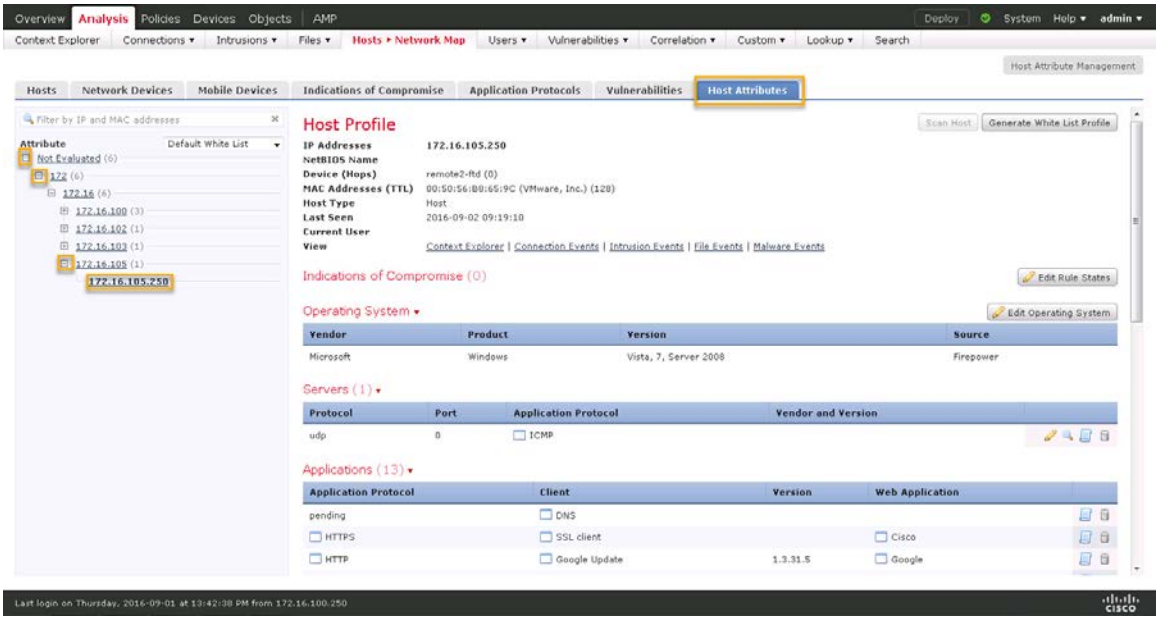
Figure 502. Filter Vulnerabilities by a particular discovered host



409. 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 503. More details about remote2-wkst



410. 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

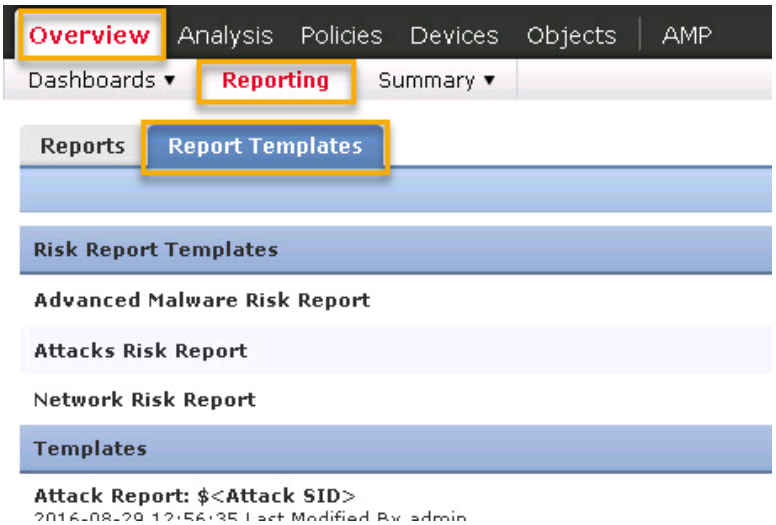
https://t.me/learningnets

Risk Reports

411. Navigate to Overview > Reporting and click on the Report Templates tab.

412. Notice the three prebuilt Risk Report Templates. Click the **Generate Report** link for the **Network Risk Report** row.

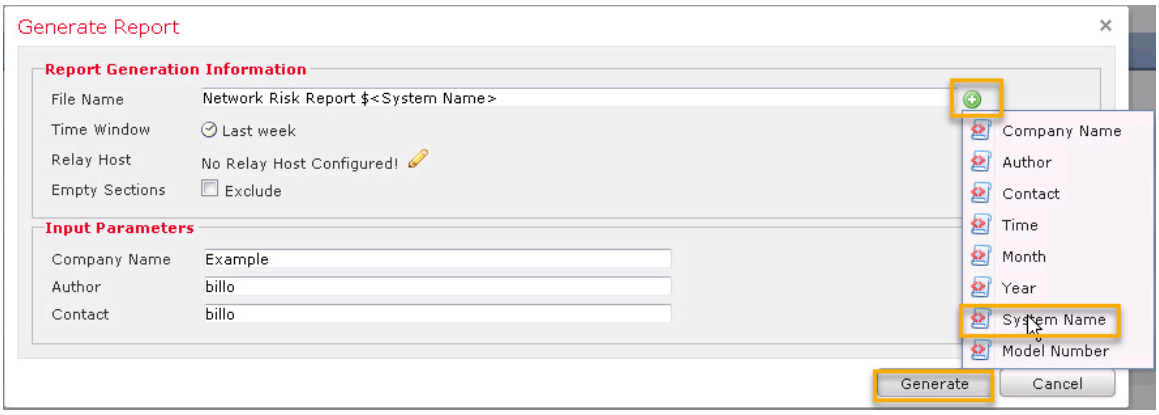
Figure 504. Navigate to Risk Reports



413. Click the **green plus icon** on the **File Name** row. Notice how you can add addition information to customize the report. Select **System Name**.

414. Click **Generate** to create this report.

Figure 505. Generate report



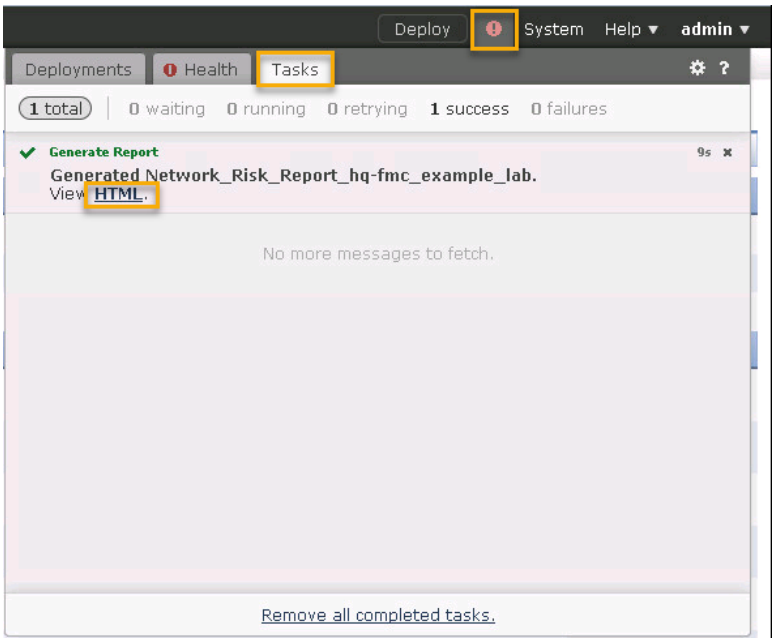
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

415. You can view the progress of the generation of this report in the **Message Center > Tasks tab**.

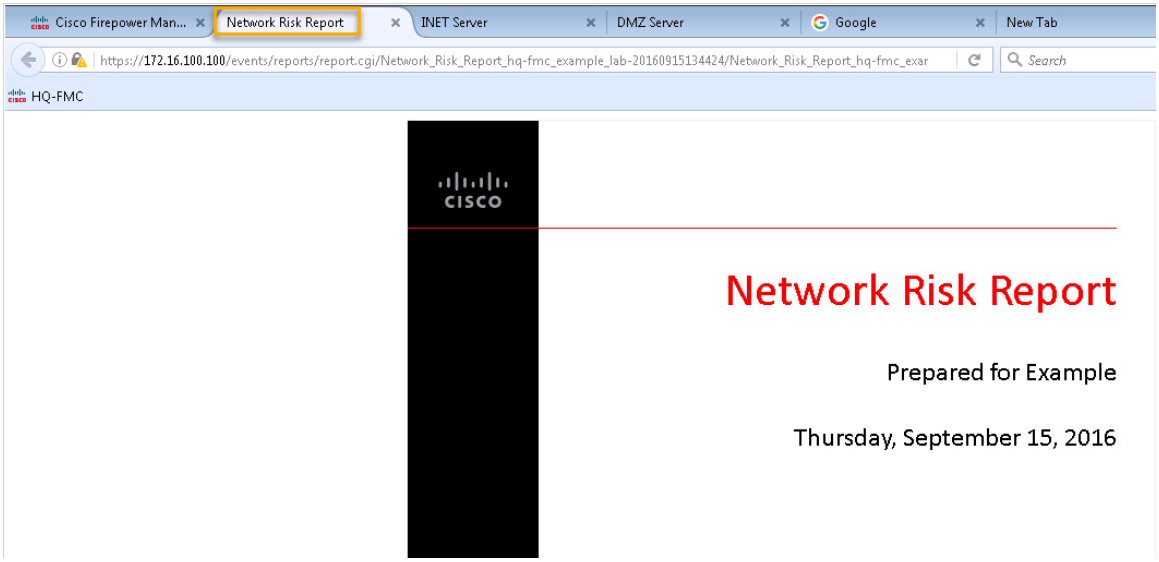
416. Once the report is generated click the HTML link or navigate to **Overview > Reporting > Reports** and click on the report. A new browser tab will load the report for viewing.

Figure 506. Message Center Tasks



417. 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 507. Risk Report



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**.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

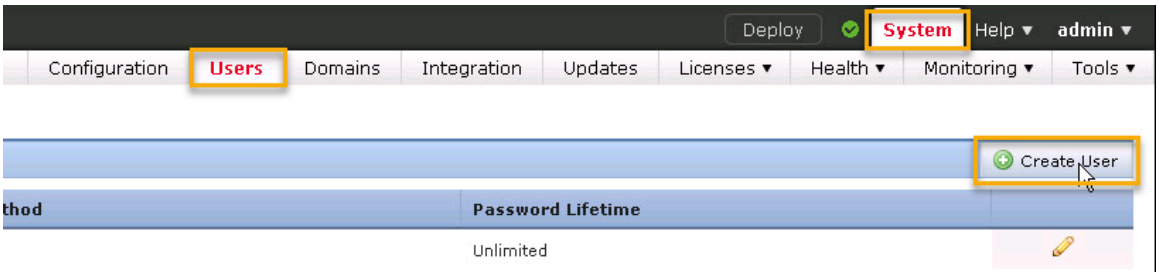
In this scenario you will learn how to send API requests to the FMC and how to interpret the results returned.

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.

418. On hq-wkst in the FMC GUI navigate to **System > Users** and click the **Create User** button.

Figure 508. Users



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

419. 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.)

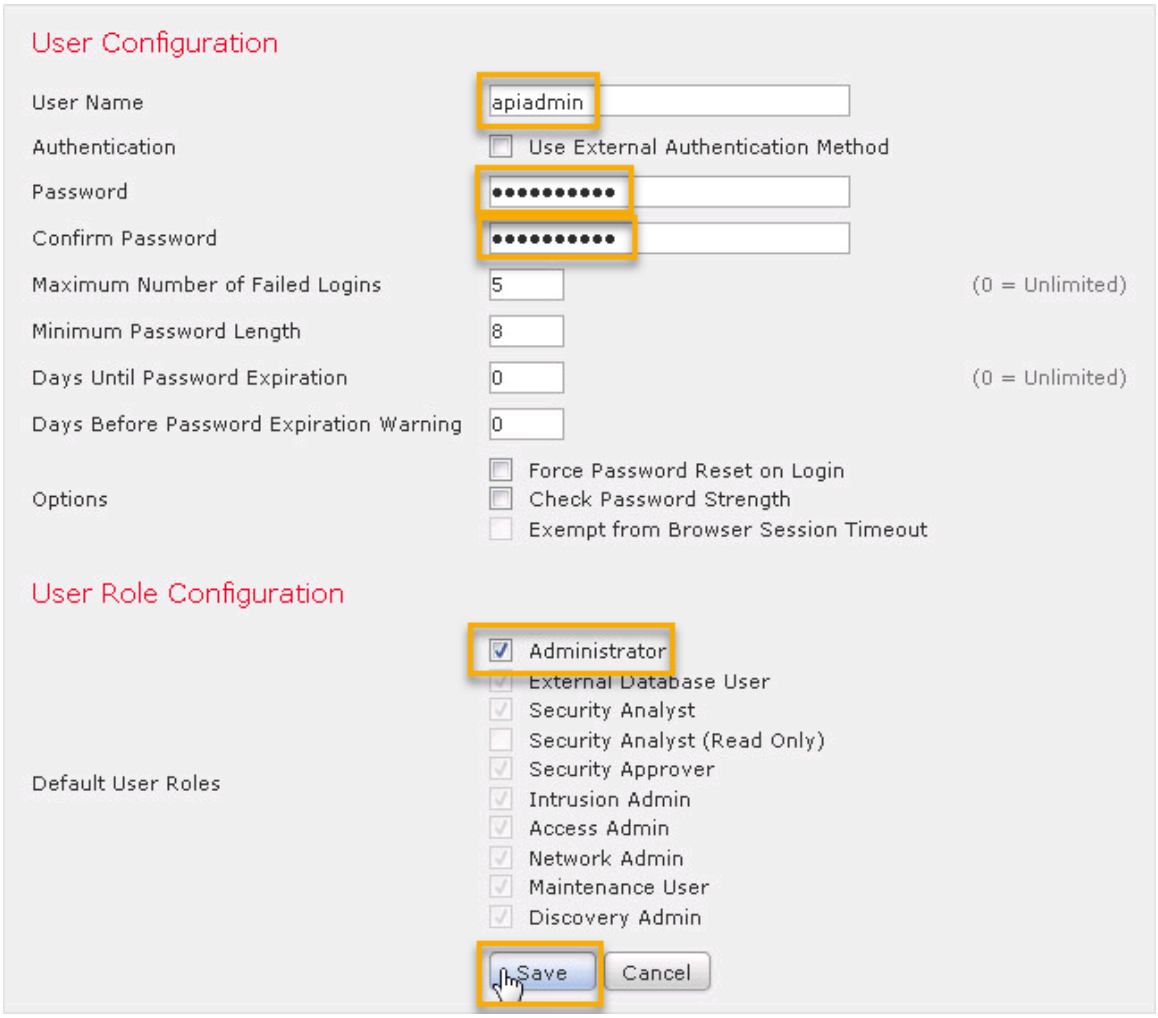
b. Password: **C1sco12345**

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 509. Create new User



Notice that you are not going to “Save and Deploy”. This user account is related to accessing the FMC.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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.

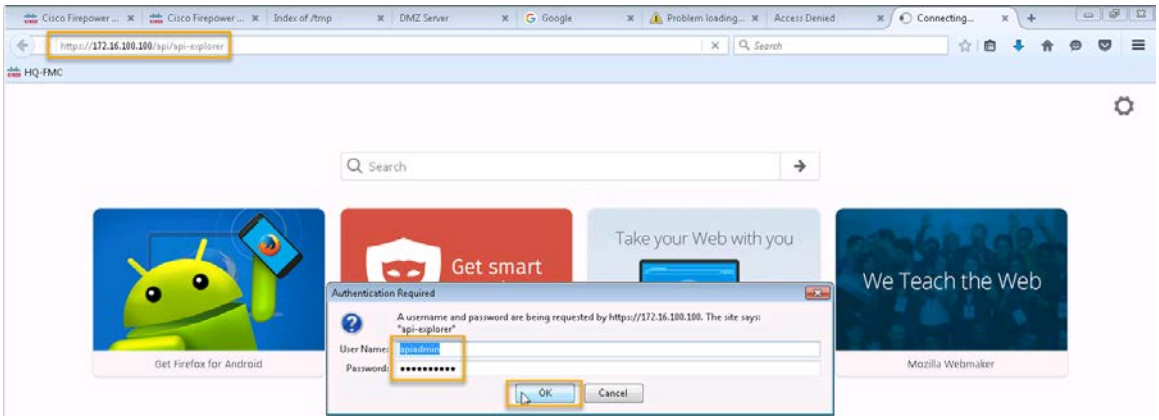
420. On hq-wkst, within **FireFox**, open a **new tab** and go to **https://172.16.100.100/api/api-explorer**.

421. In the Authentication Required popup windows log in using the new user credentials:

   a. User Name: **apiadmin**

   b. Password: **C1sco12345**

Figure 510. Log into API Explorer



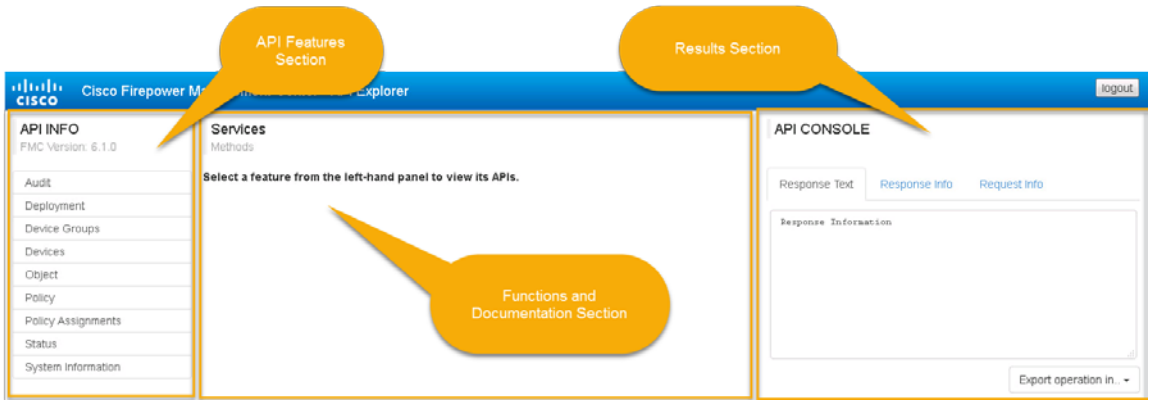
422. This page is broken into 3 parts, or columns:

   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 511. API Explorer GUI Layout



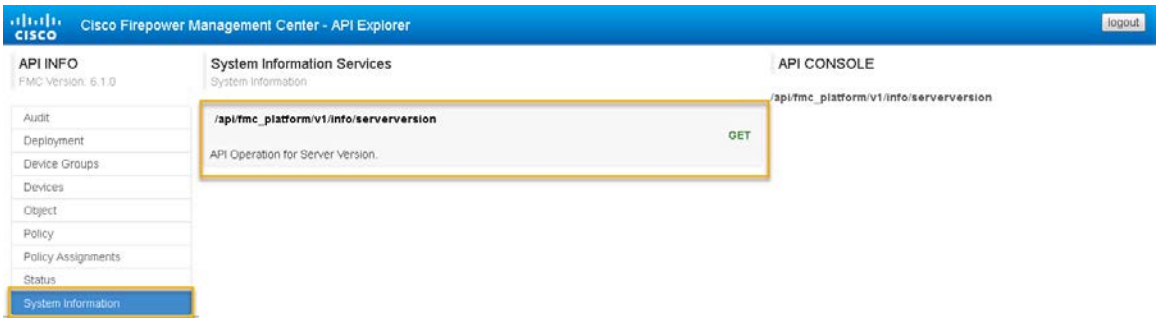
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

423. From the left column click the **System Information** link.

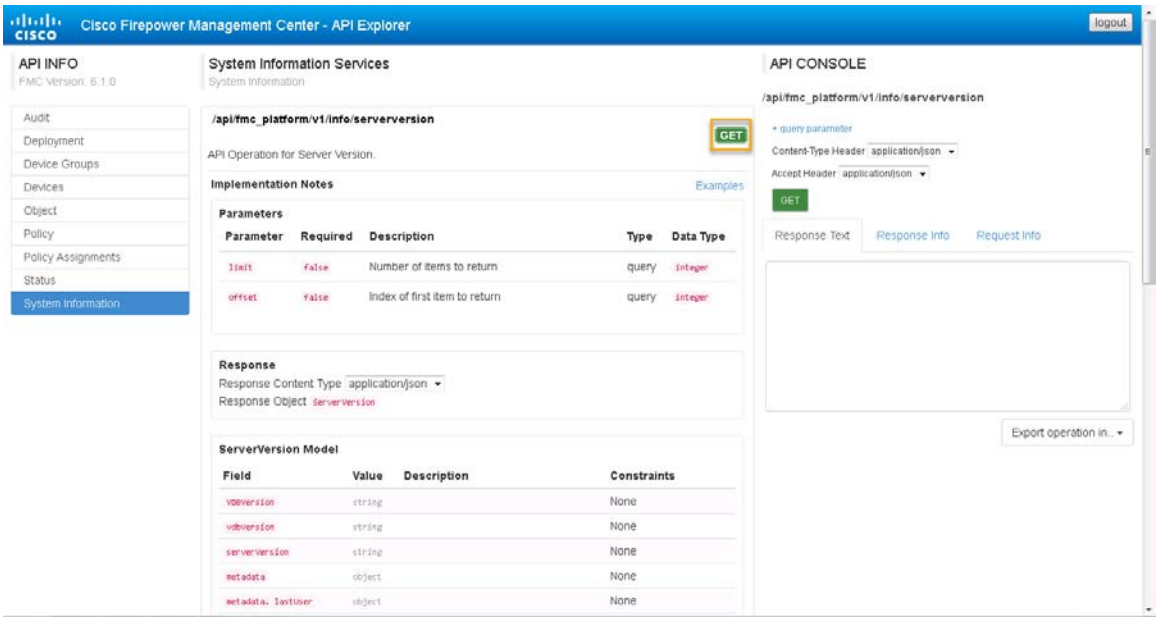
a. Notice how the middle column is now populated with all the API functions related to System Information feature. In this case there is only one function: The Server Version function.

Figure 512. Functions for System Information Features



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 513. Documentation and Functions for Server Version



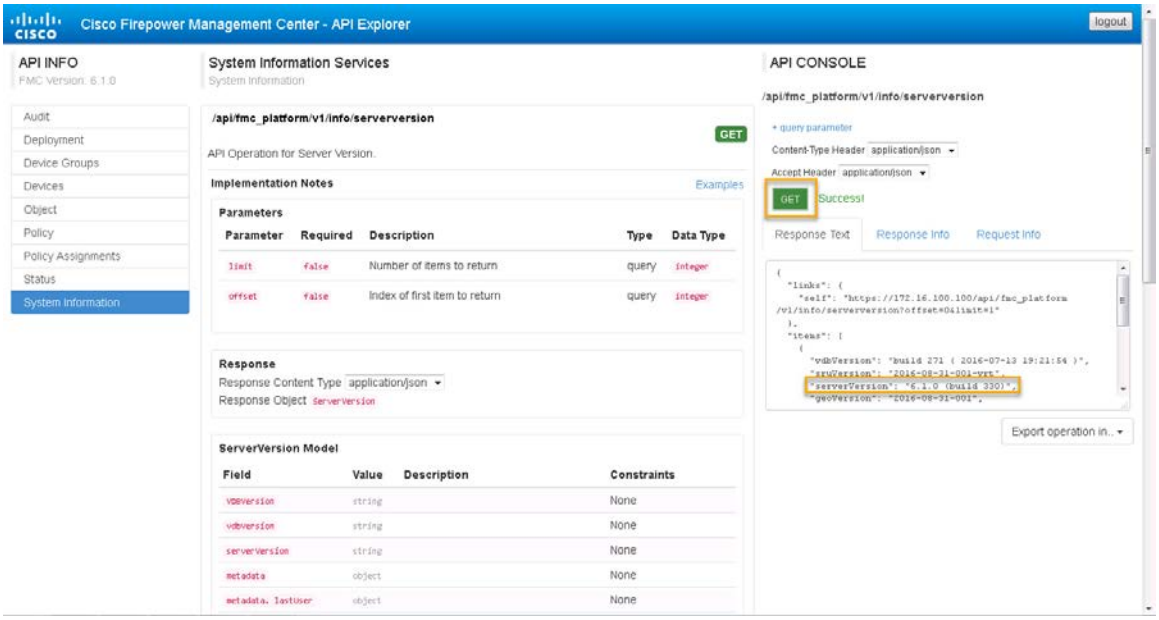
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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).

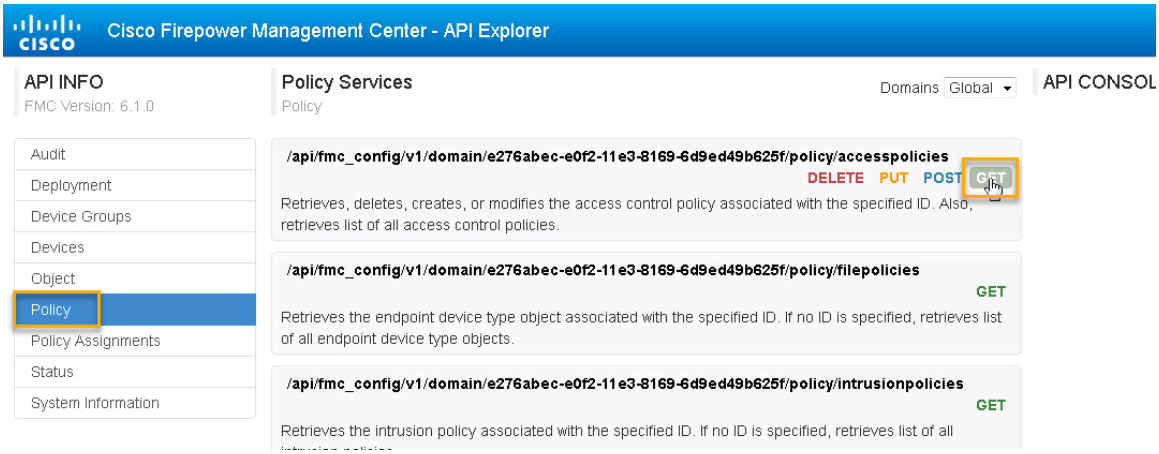
Figure 514. GET Server Version JSON



424. 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 515. GET Access Policies



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

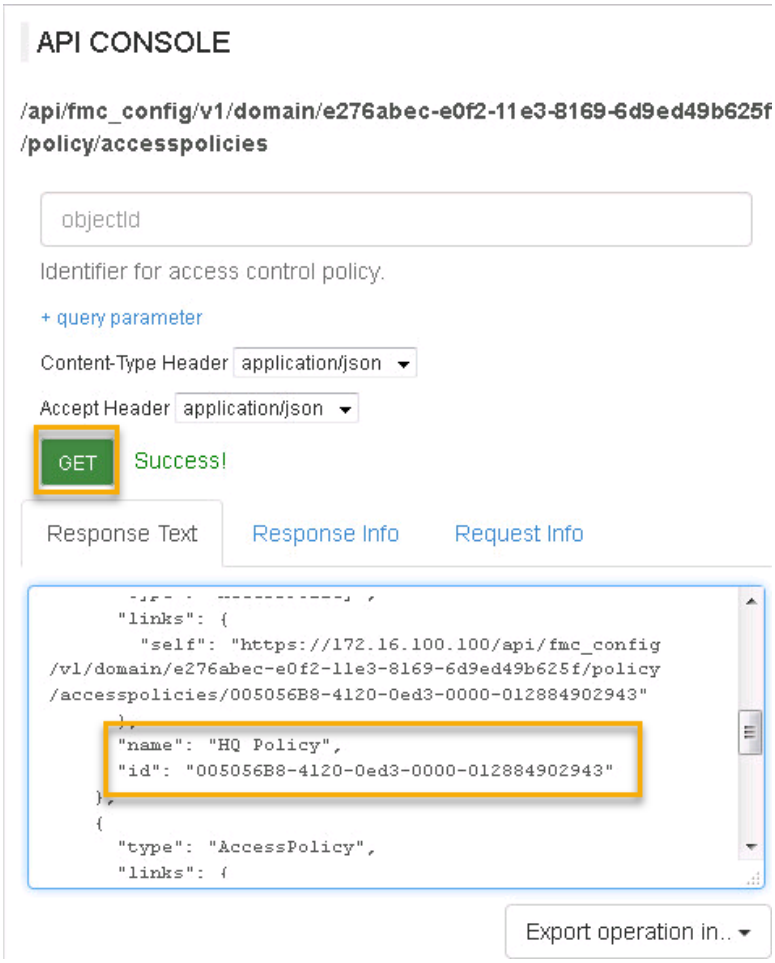
https://t.me/learningnets

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 516. GET Access Policies Results

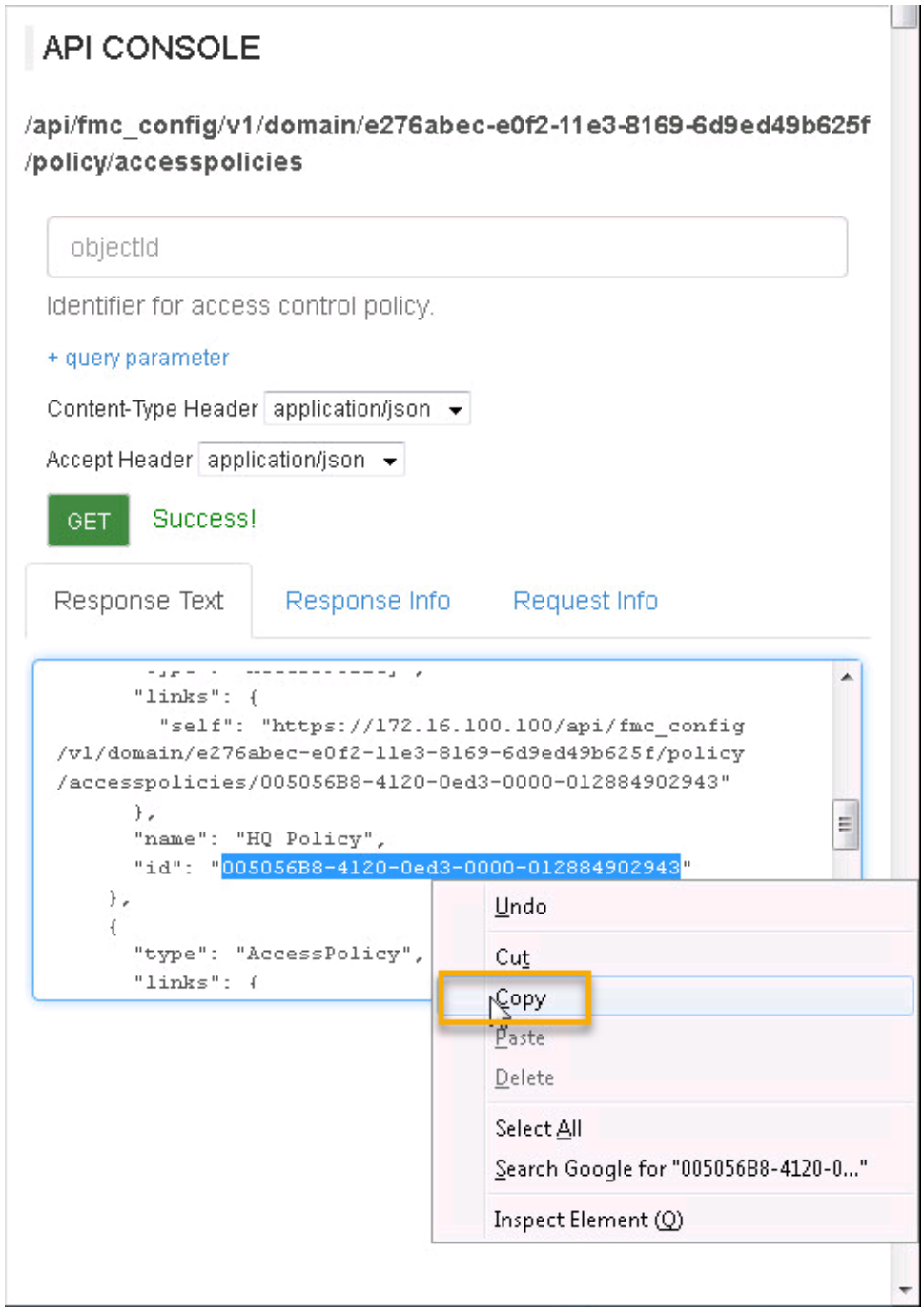


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

e. Copy the HQ Policy's ID value.

Figure 517. Copy HQ Policy ID

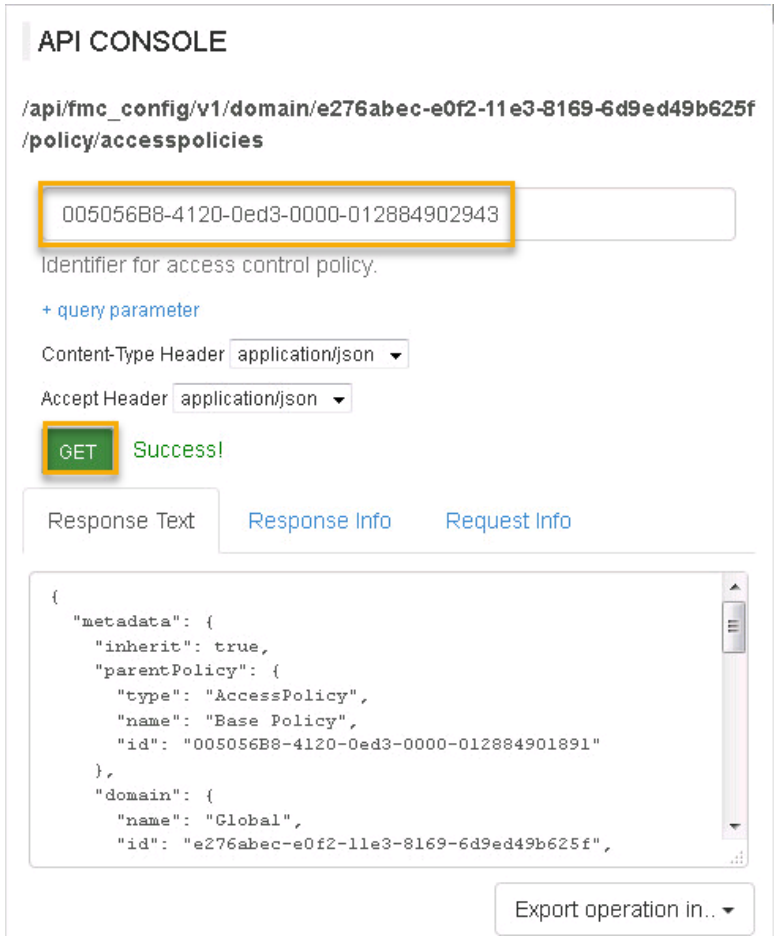


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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 518. Paste into Field and GET again



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

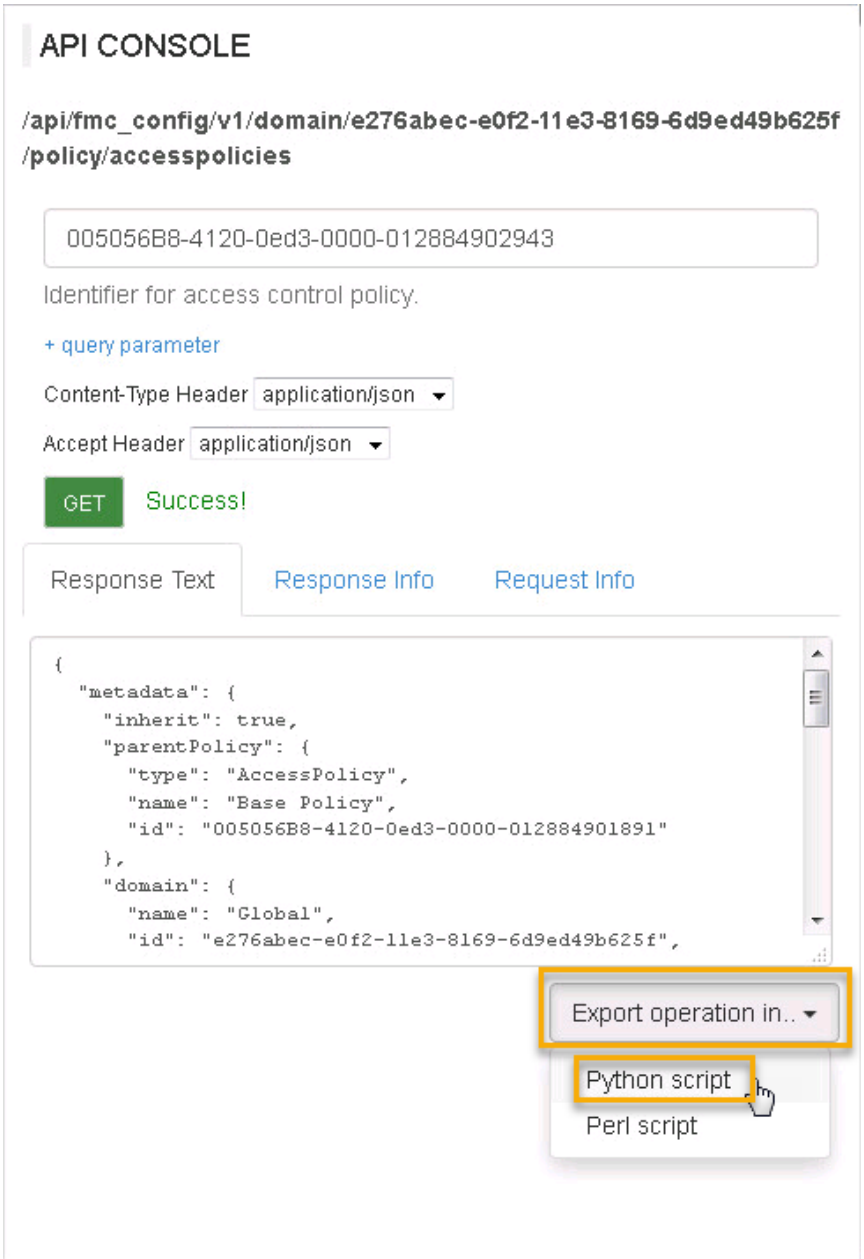
https://t.me/learningnets

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.

425. Click the **Export operation in…** link at the bottom of the right column. Select **Python script** from the dropdown list.

Figure 519. Export Python Script

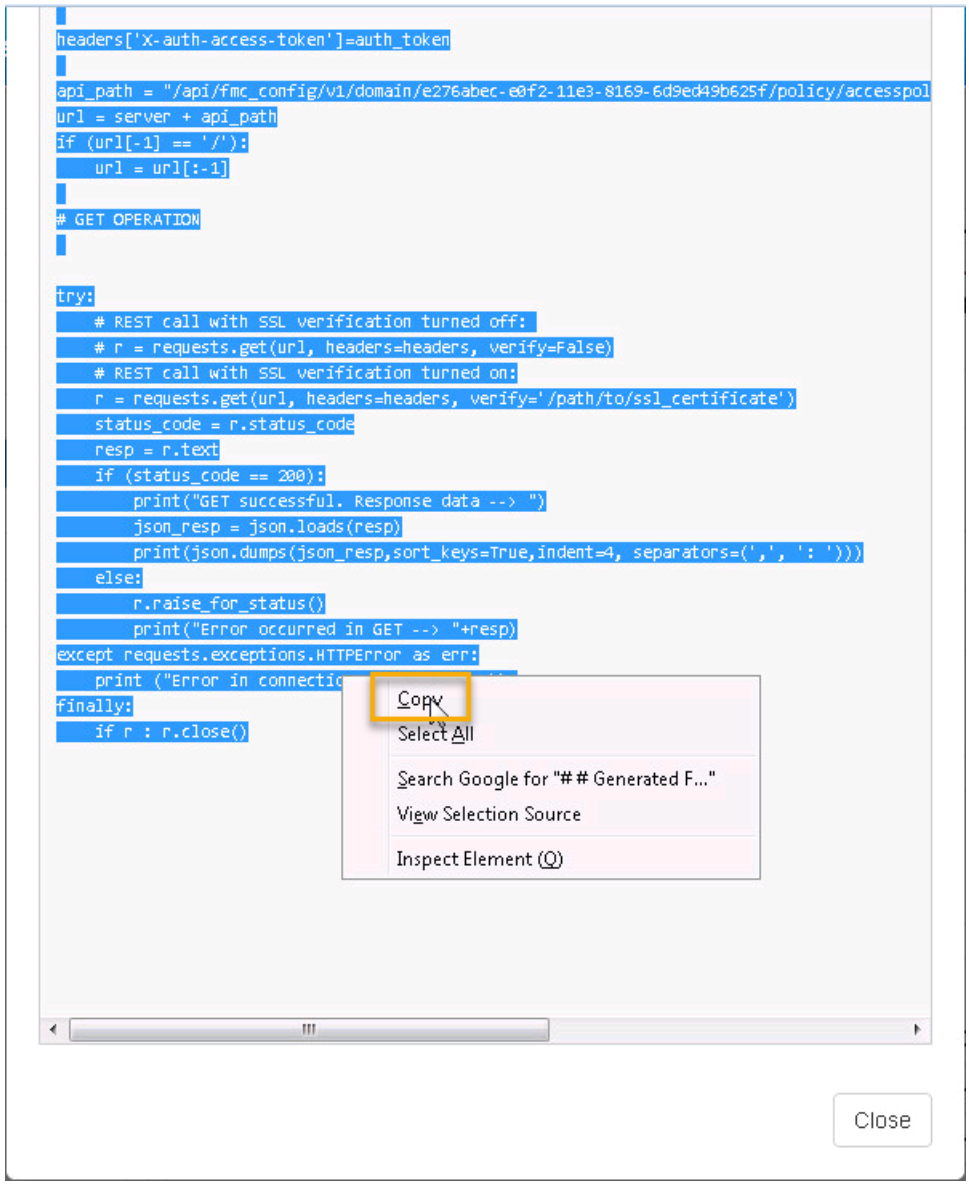


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

426. 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 520. Copy python script text

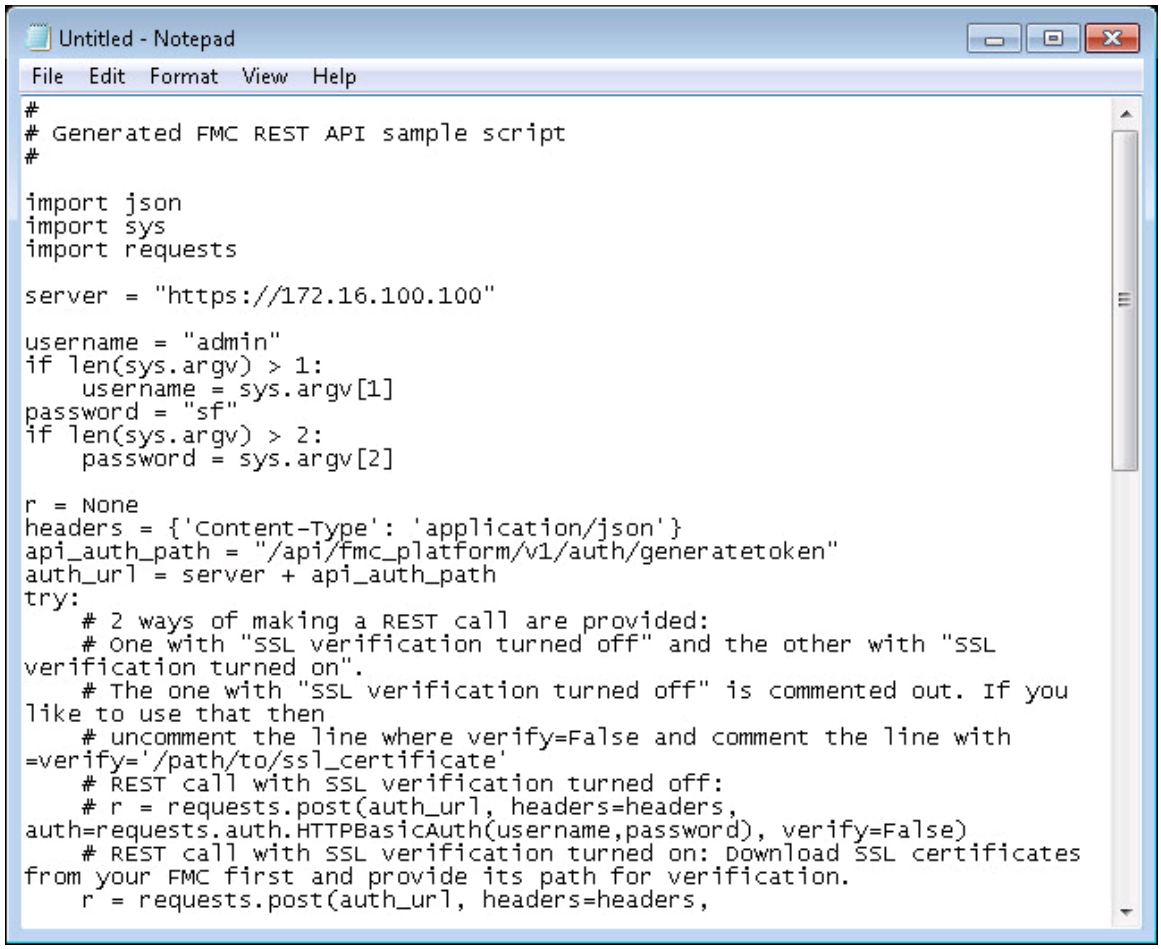


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

427.**Paste** it into a **notepad** file.

Figure 521. Open Notepad and paste text into it.

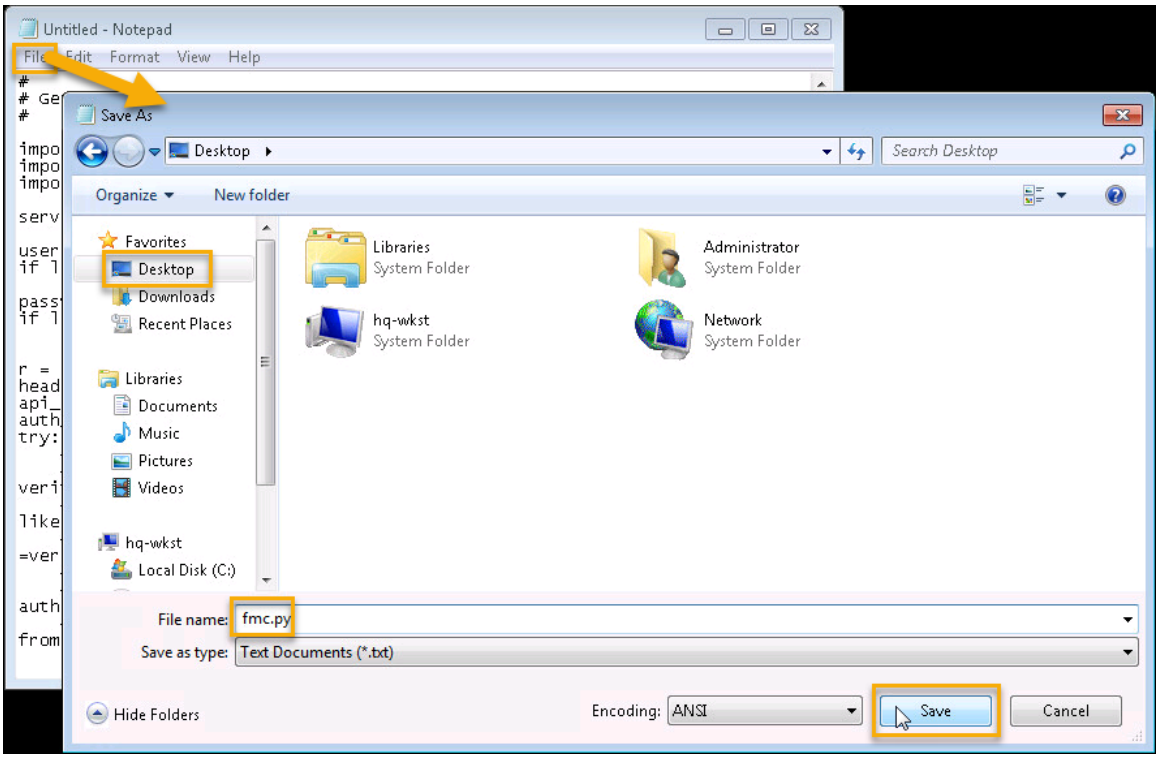


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

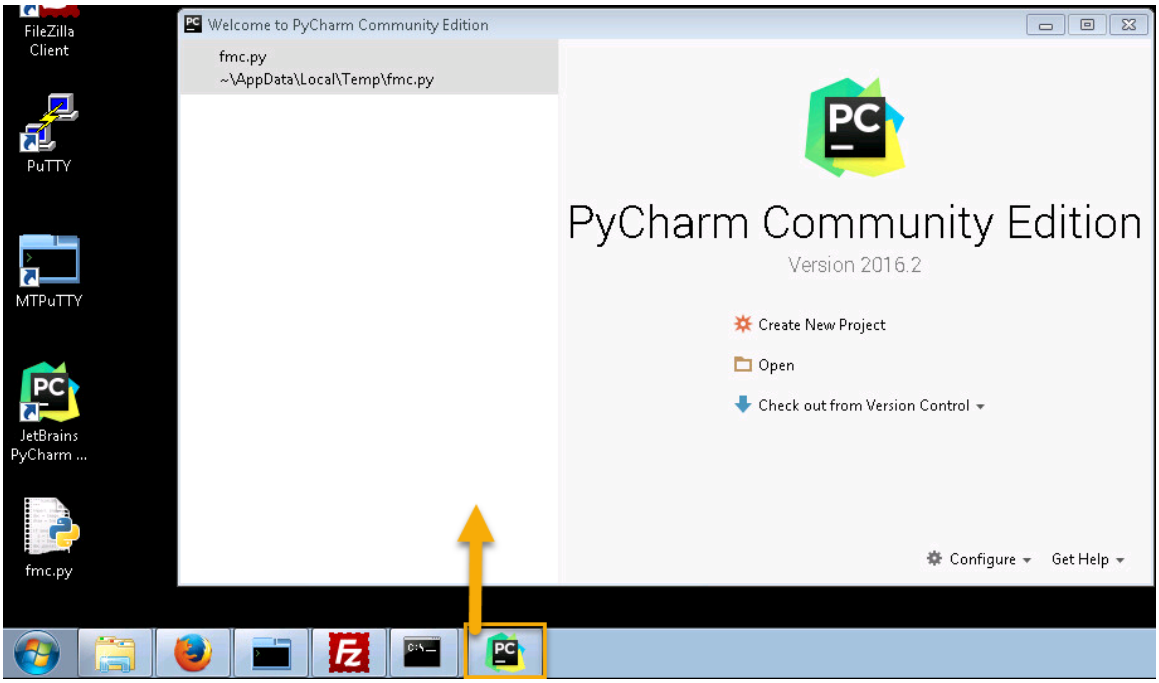
428. **Save** that notepad file as **fmc.py** to the **Desktop**.

Figure 522. Save the file



429. 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.

Figure 523. Open PyCharm

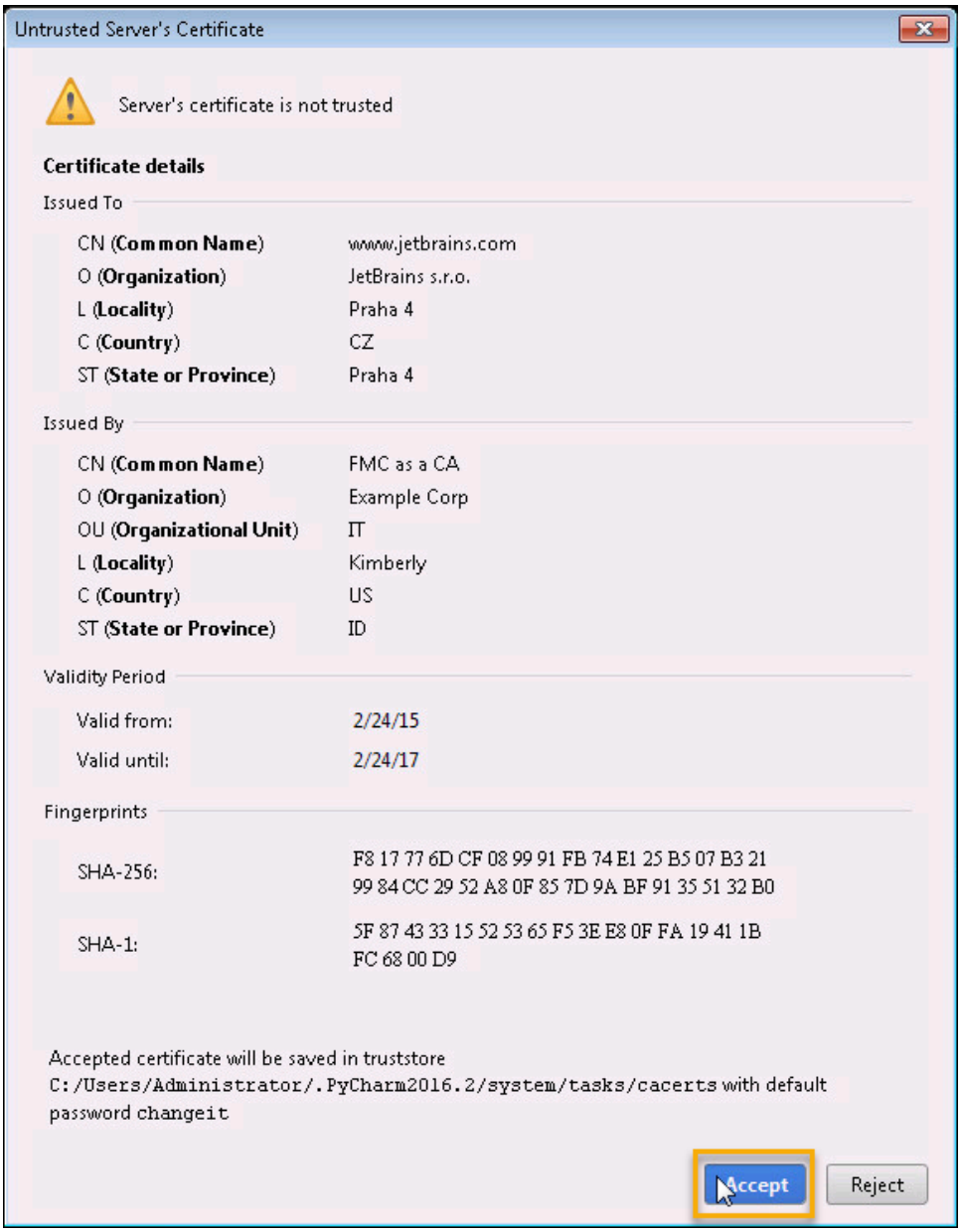


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

430. Looks like the SSL Policy is still working. **Accept** the certificate when prompted.

Figure 524. Accept certificate

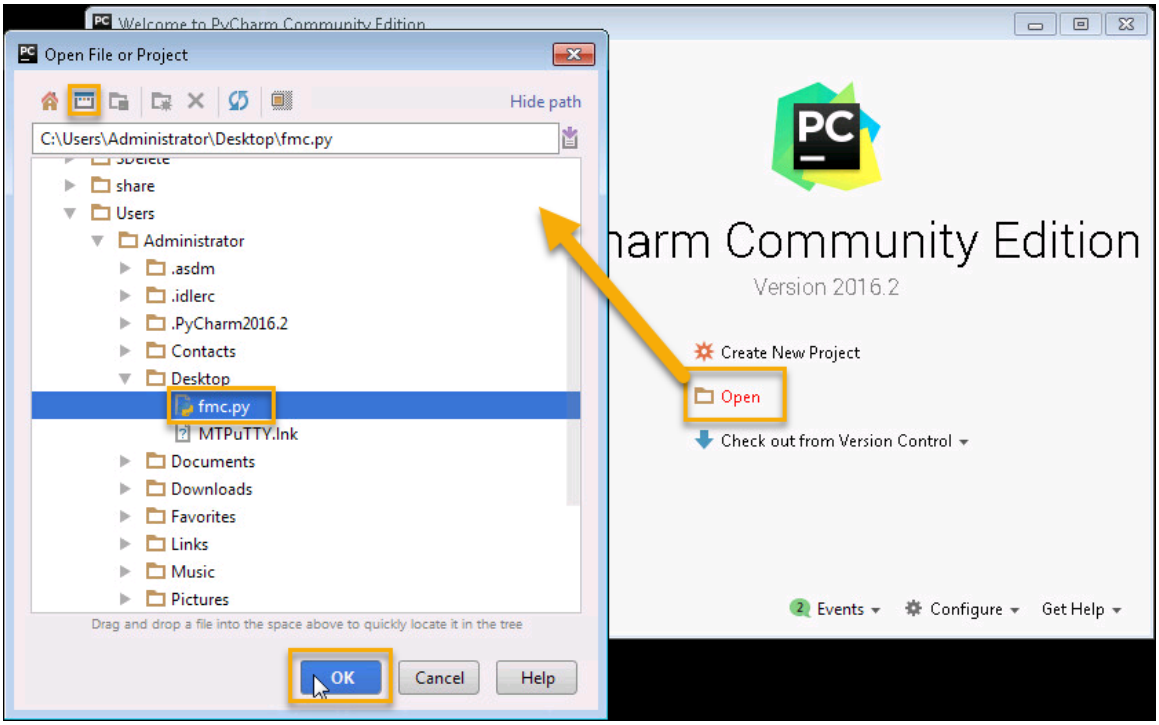


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

431. 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 525. Open fmc.py



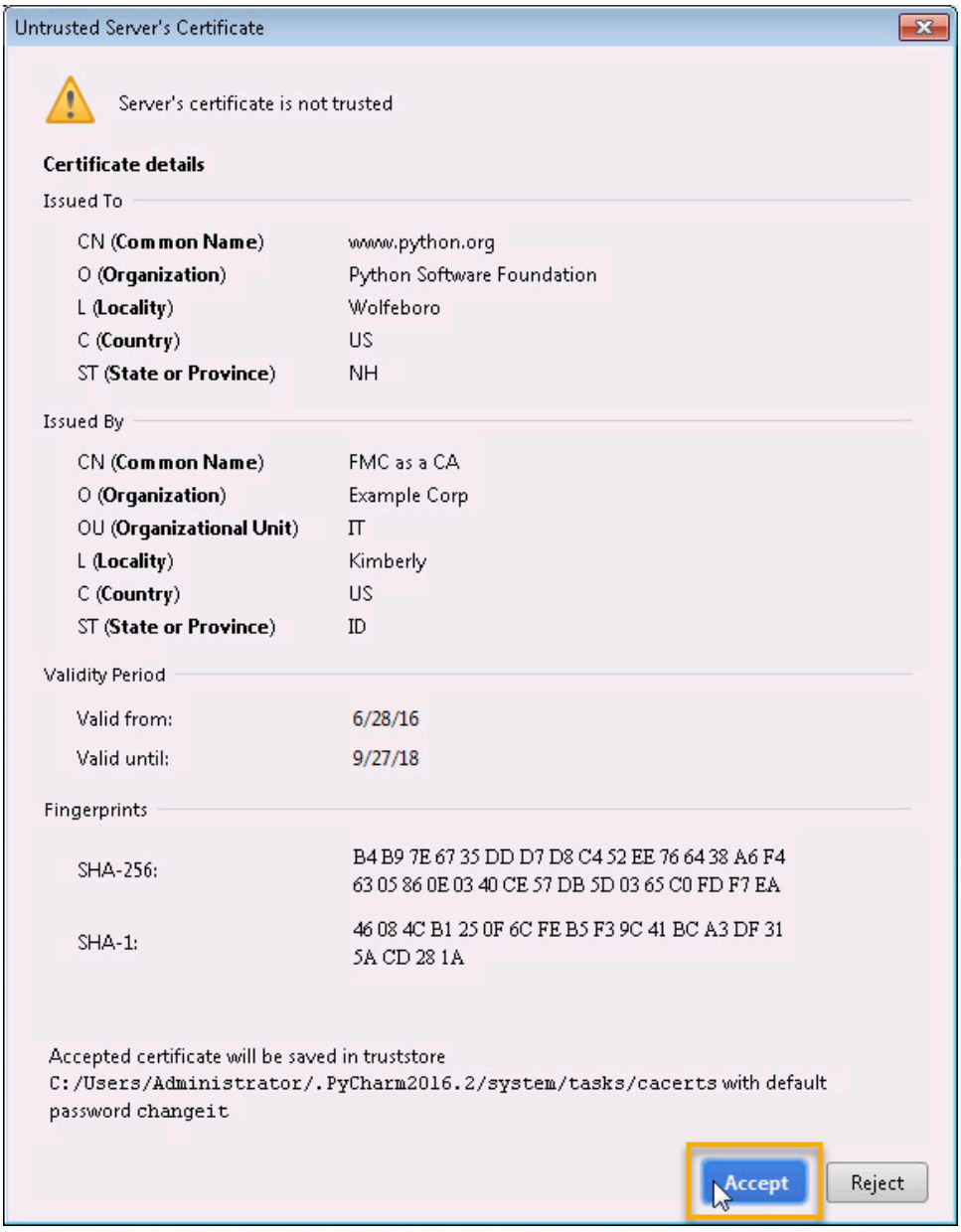
The following changes are by no means the “best practices” that a normal programmer would use. These changes are to get the script to run as quickly as possible to show you that it works. Typically, you would not want to statically assign the username and password in the file. Nor would you disable the certificate process.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

432.I'm not sure what PyCharm is doing but **Accept** the certificates to continue.

Figure 526. Accept certificate again



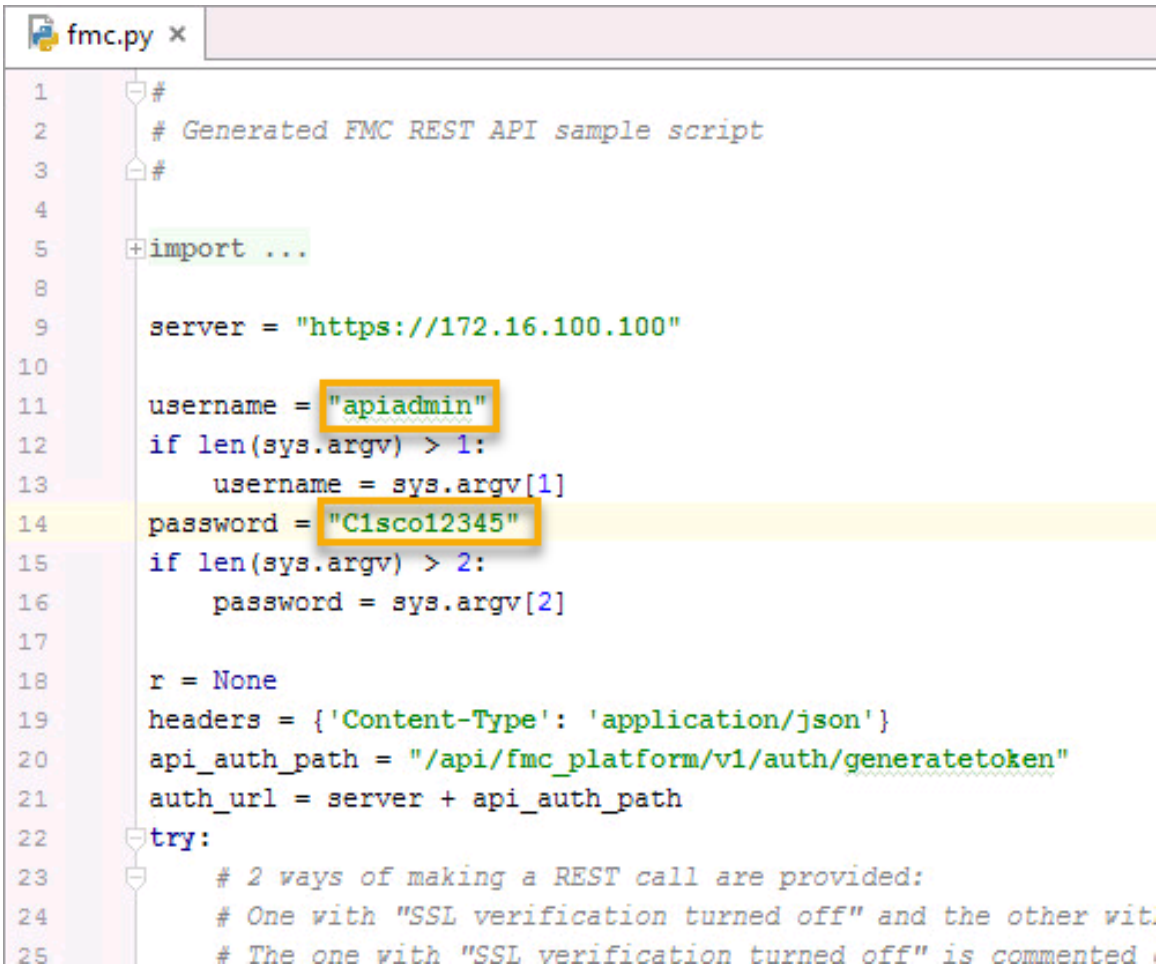
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

433. Find the **username variable** and change its value to **apiadmin**. (Around line 11.)

434. Find the **password variable** and change its value to **C1sco12345**. (Around line 14.)

Figure 527. Set username/password in script



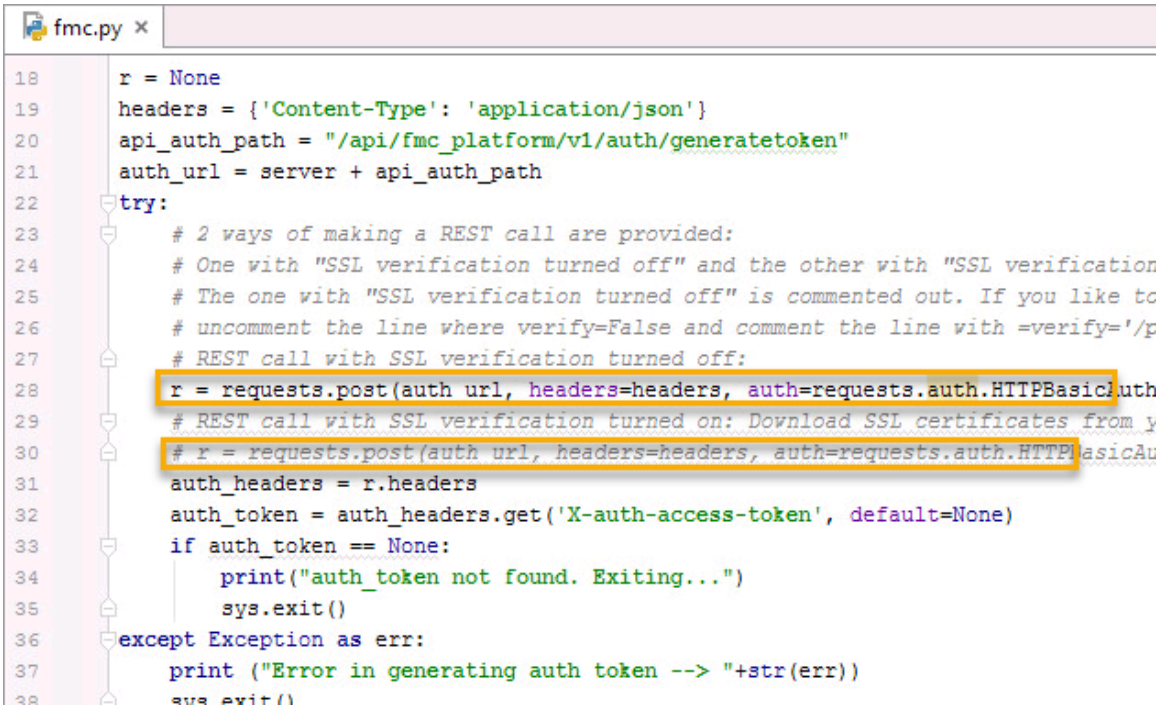
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

435. 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.

436. 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 528. Turn off certs for this script



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

437. Around line 54 find the **r= requests.get(url,…** line and **comment it out**.

438. Around line 52 find the **# r = requests.get(url,…** line and **uncomment it**.

Figure 529. 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).

439. 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 530. Finding the api_path variable

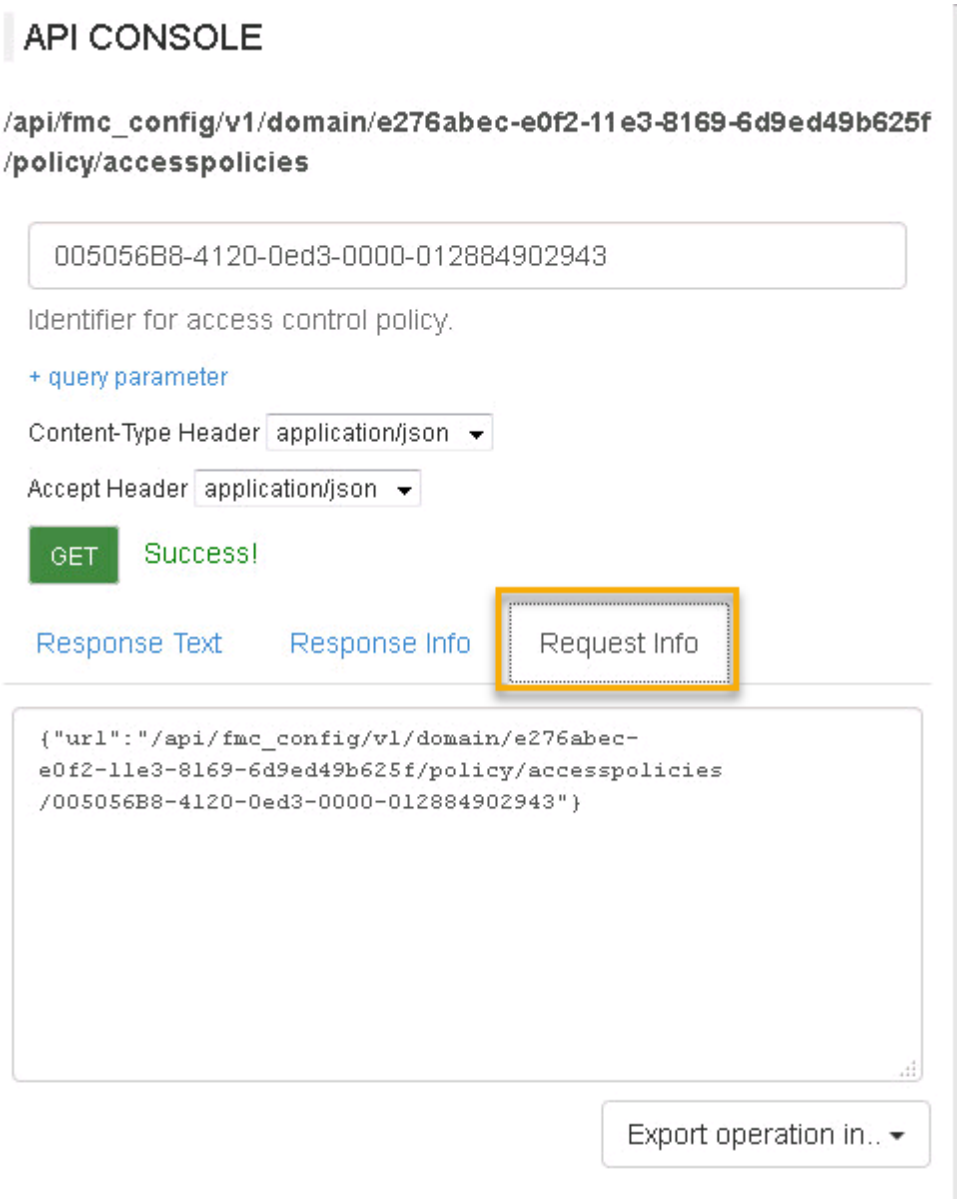
```
40  headers['X-auth-access-token']=auth_token
41
42  api_path = "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/005056B8-4120-0ed3-0000-012884902943"
43  url = server + api_path
44  if (url[-1] == '/'):
45      url = url[:-1]
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

440. 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 531. Value for api_path variable

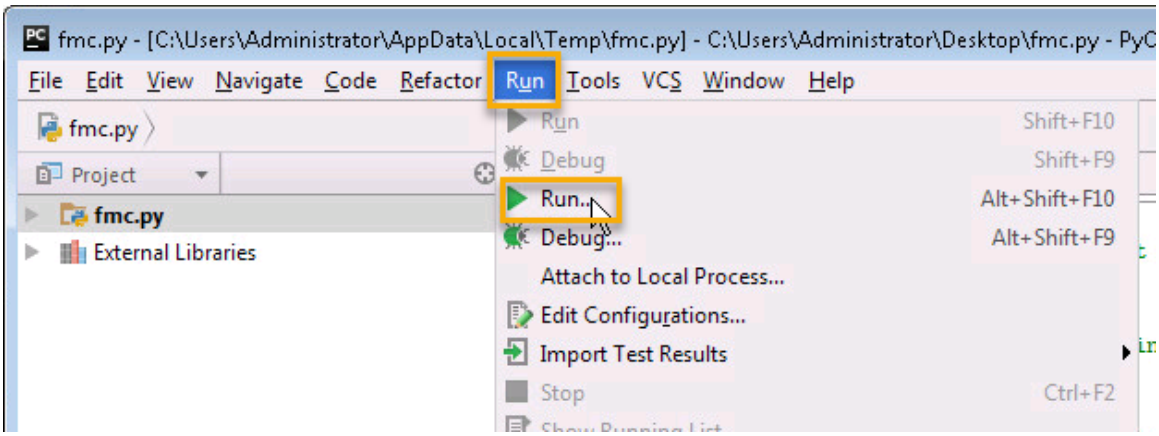


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

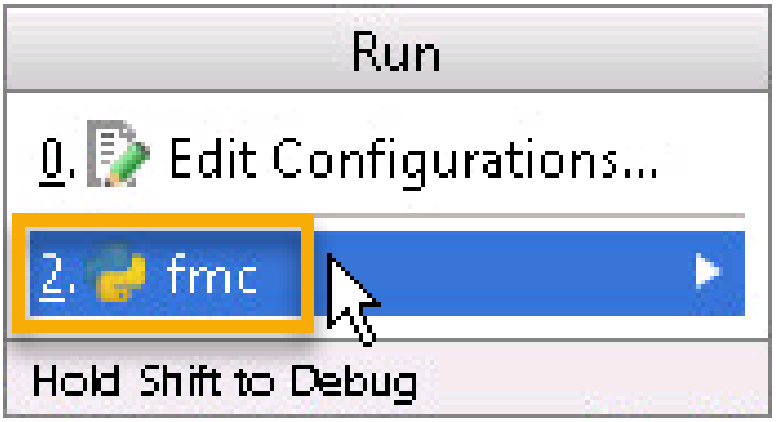
441. From the **PyCharm** menu select **Run > Run**.

Figure 532. Select Run



442. In the Run popup window select **fmc**.

Figure 533. Run fmc.py



443. The python script will now be run and the output will be displayed at the bottom of the PyCharm application.

Figure 534. Results of running fmc.py script



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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!!!

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

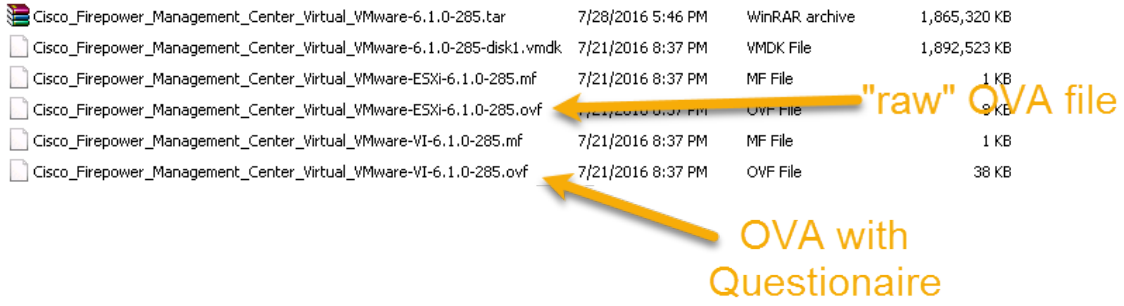
https://t.me/learningnets

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.

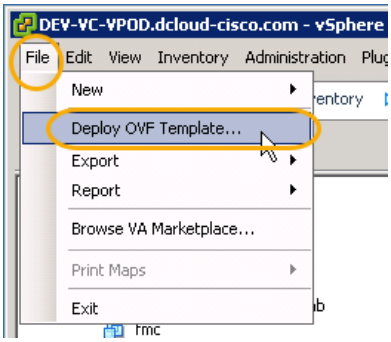
Figure 1. Listing of files in OVA zip.



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

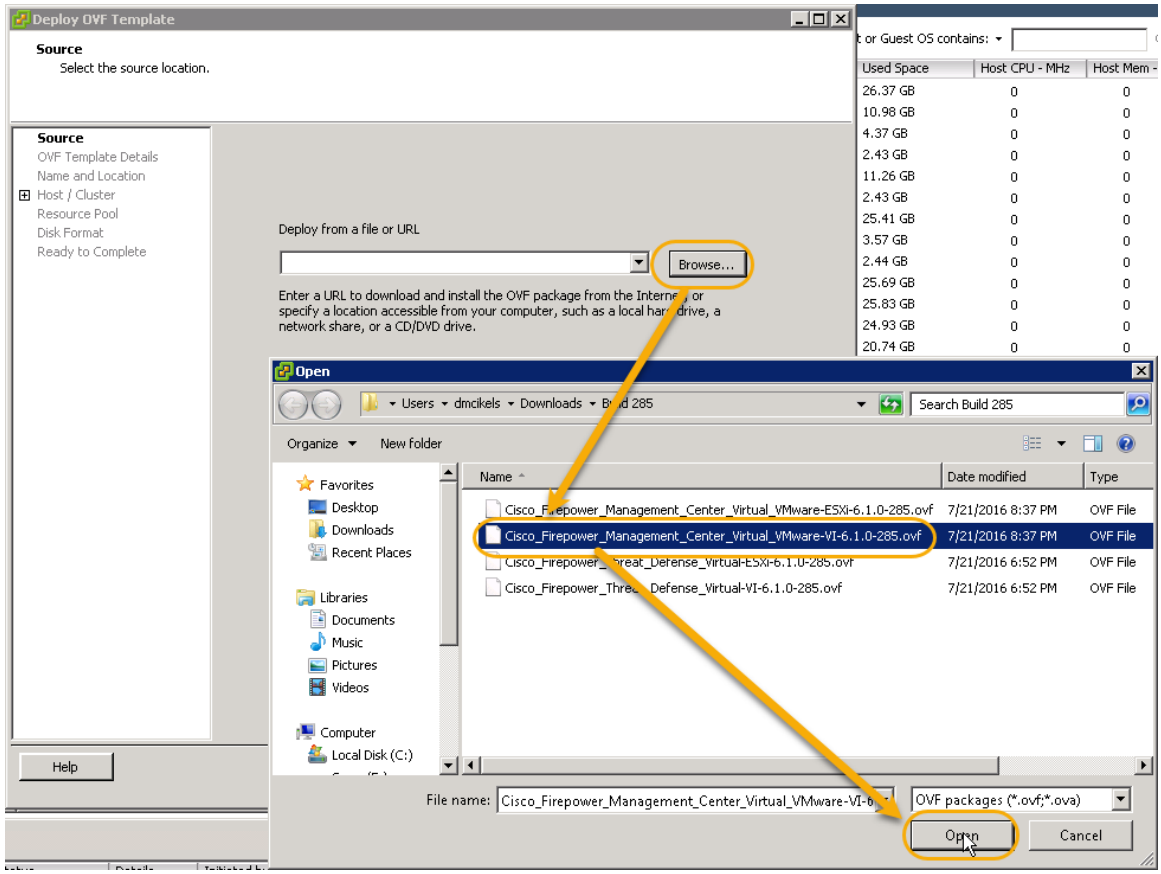


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

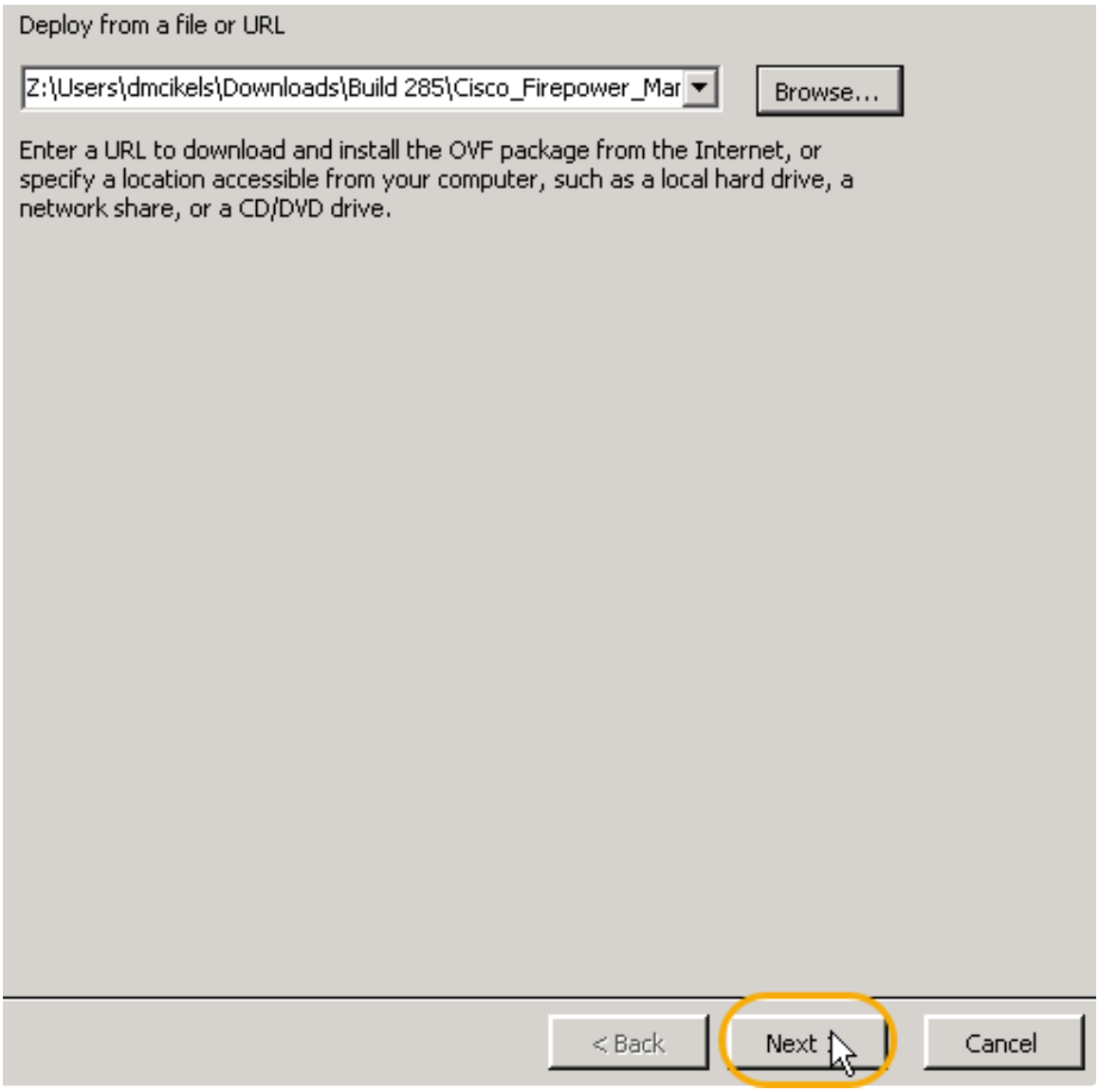


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

3. With the proper file selected click **Next >**.

Figure 4. Select file

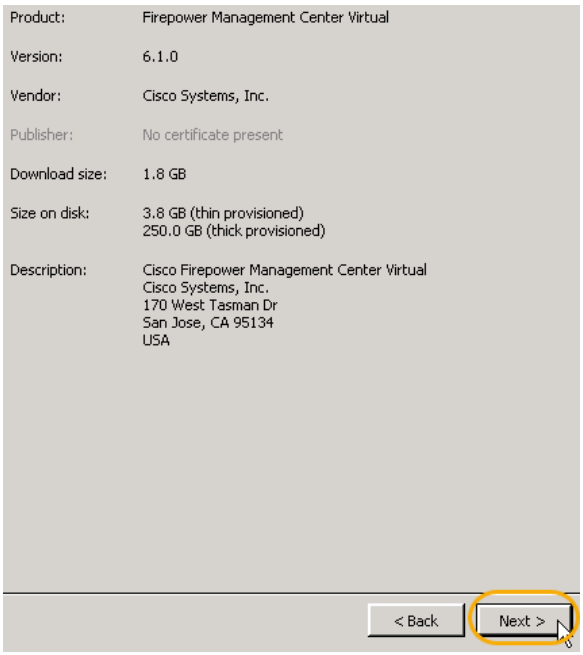


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

4. The next page will display some basic details of this OVA file. Click **Next >** to continue.

Figure 5. Click Next



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

5. **Accept** the EULA and click **Next >**.

Figure 6. Accept the EULA



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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**

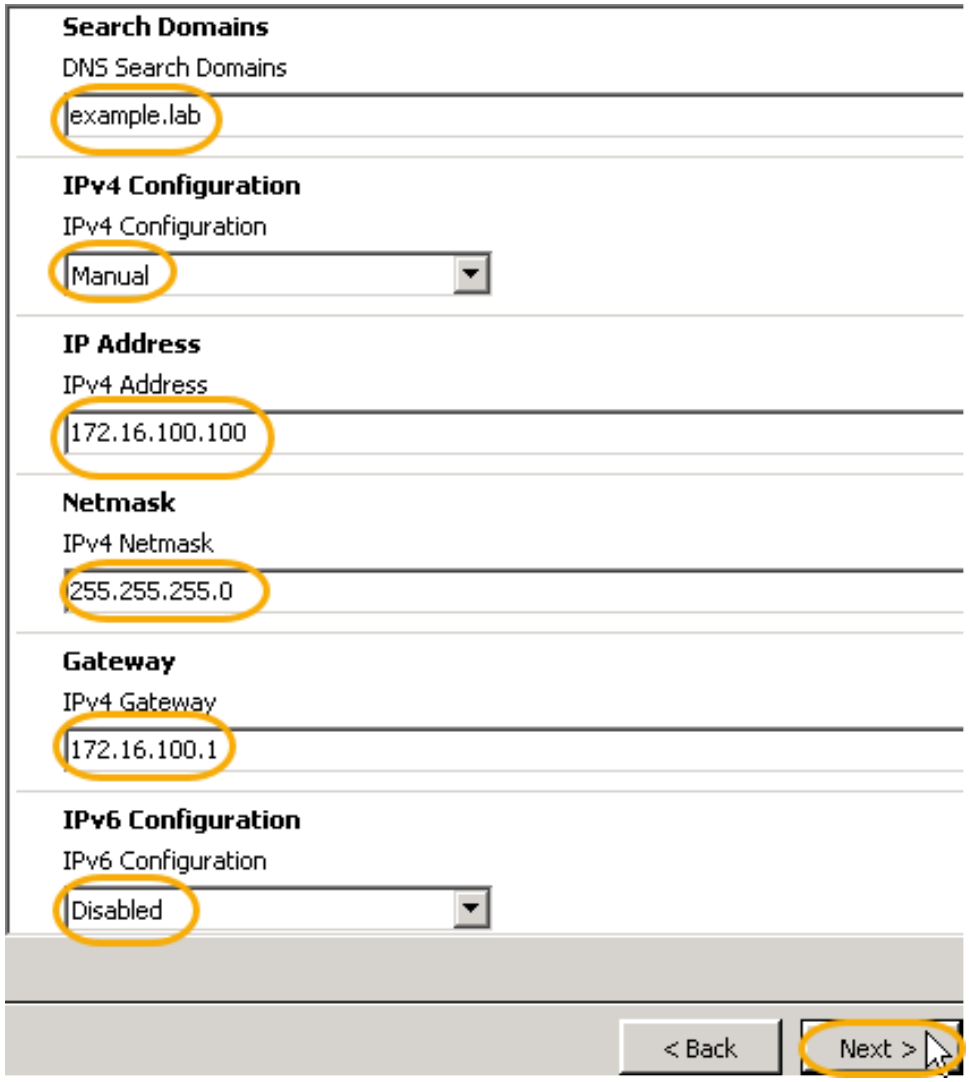
    f. IPv4 Address: **172.16.100.100**

    g. IPv4 Netmask: **255.255.255.0**

    h. IPv4 Gateway: **172.16.100.1**

    i. IPv6 Configuration: **Disabled**

Figure 7. Fill out Wizard



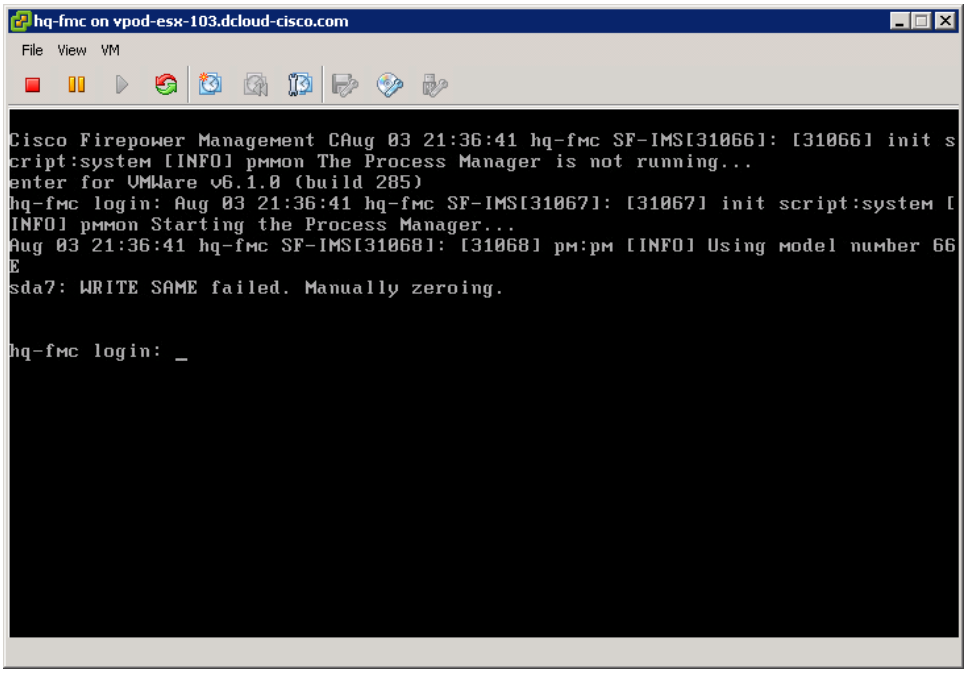
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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



Congratulations! You have deployed the FMC VM! Return to Scenario 1 to learn how to configure it from here.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Appendix B. FTD OVA Deployment

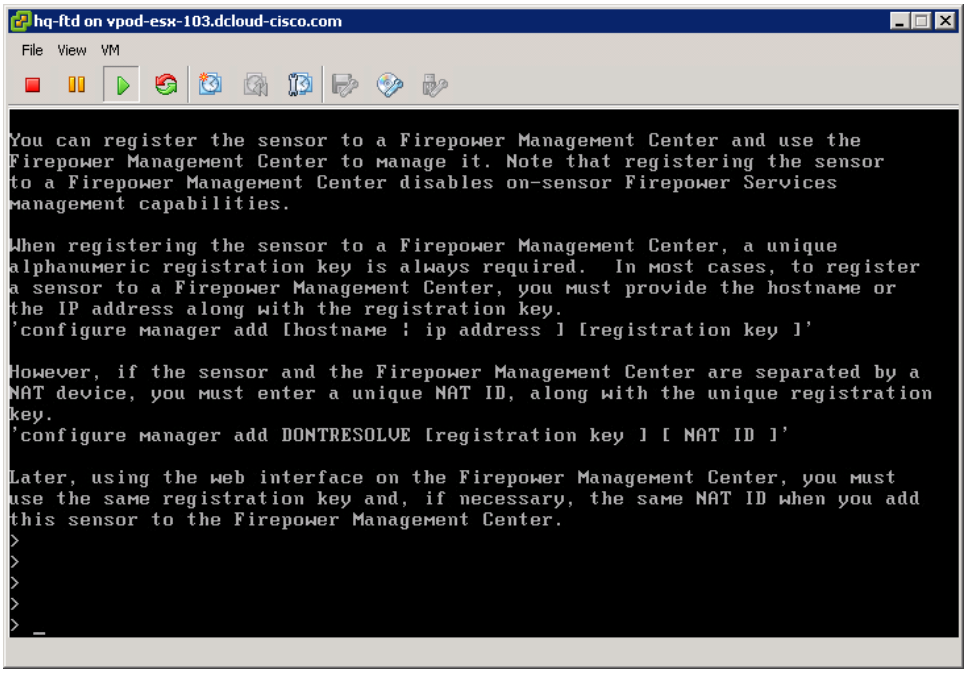
Deploying the FTD OVA file is very similar to how to deploy the FMC OVA as shown in Appendix A. Instead of duplicating all the steps I'll start with the questionnaire.

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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**

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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



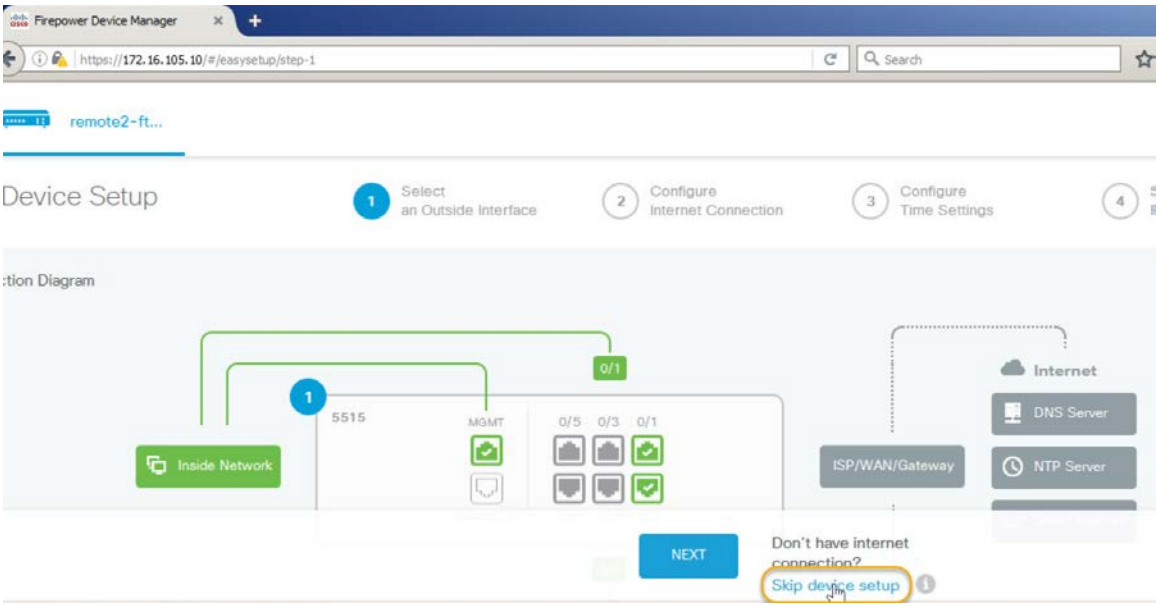
The initial screen shows a "wiring diagram" of how the FTD device is cabled and to which zone each cable is connected. By default, the Mgmt and 0/1 interfaces are connected to the "inside Network" and interface 0/0 is connected to the "Outside Network". If you were able to cable the device such that 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

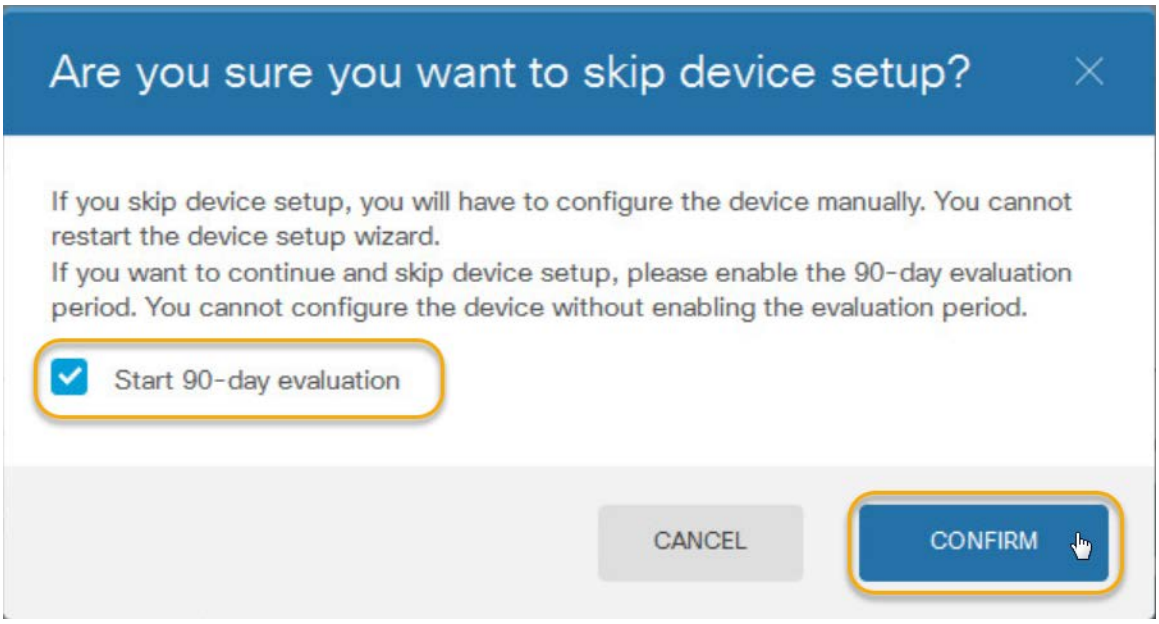
5. Click **Skip device setup** link.

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

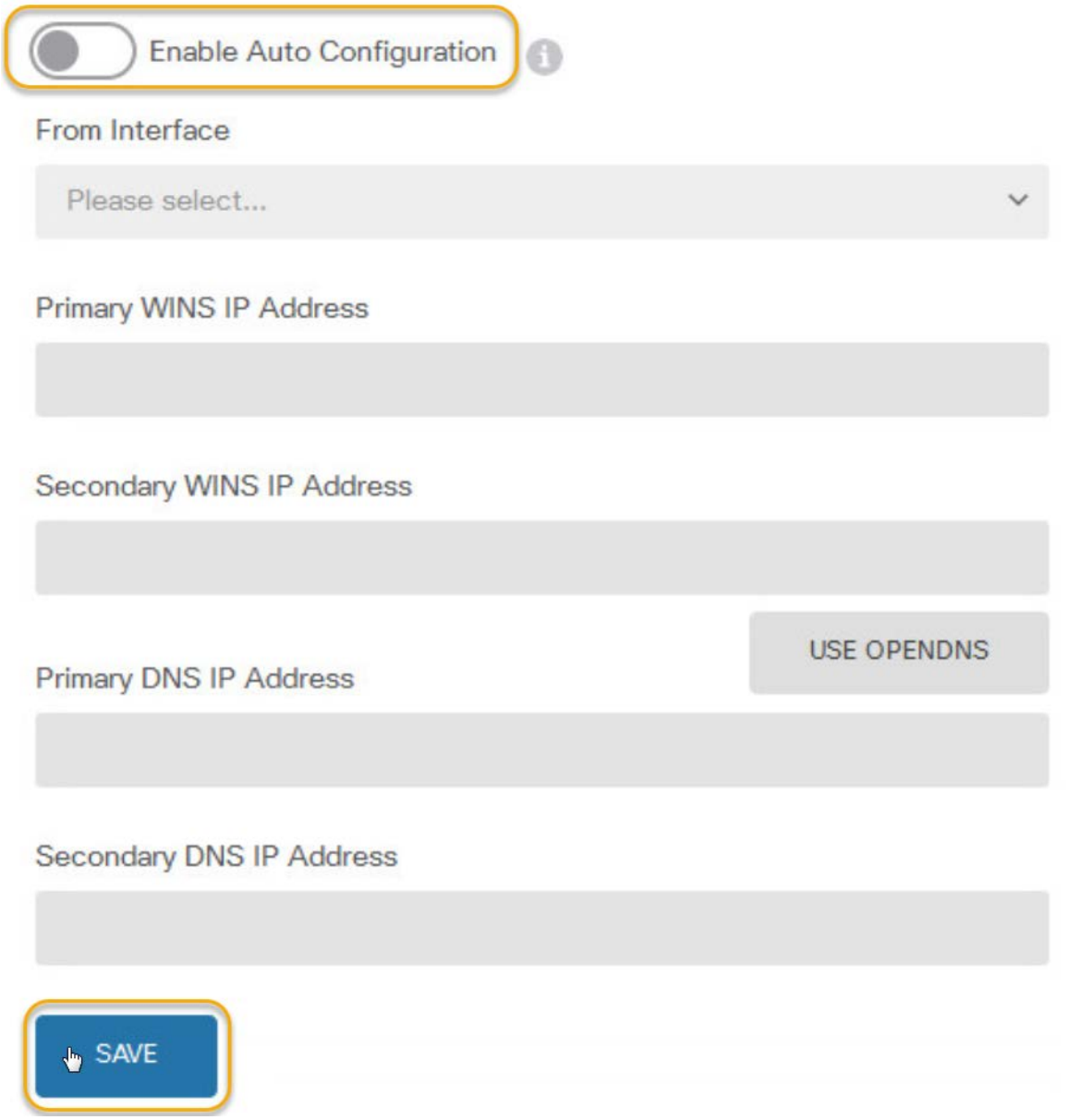


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

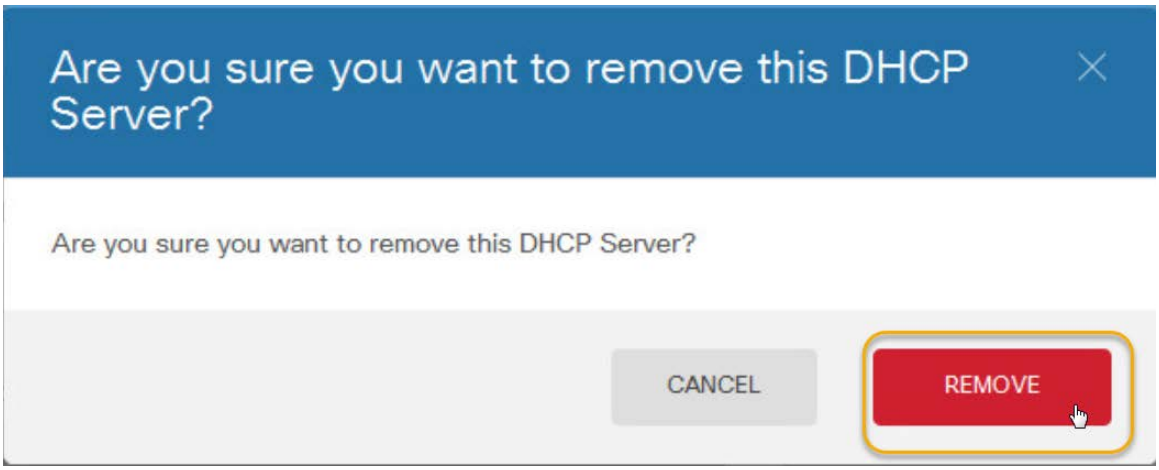


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

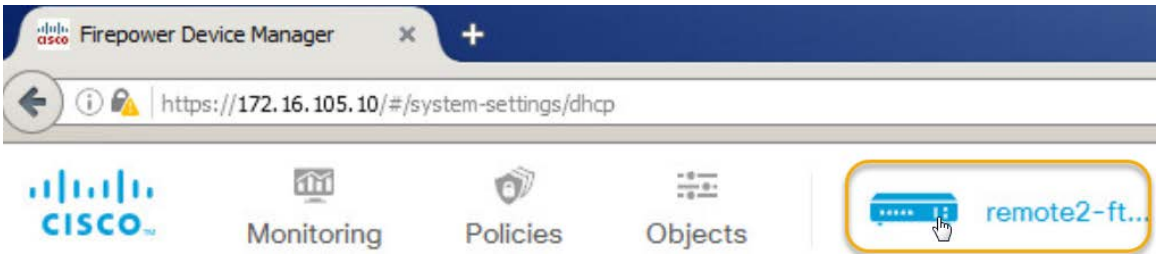
12. Click **Remove** from the popup window.

Figure 16. Confirm removal of DHCP Pool



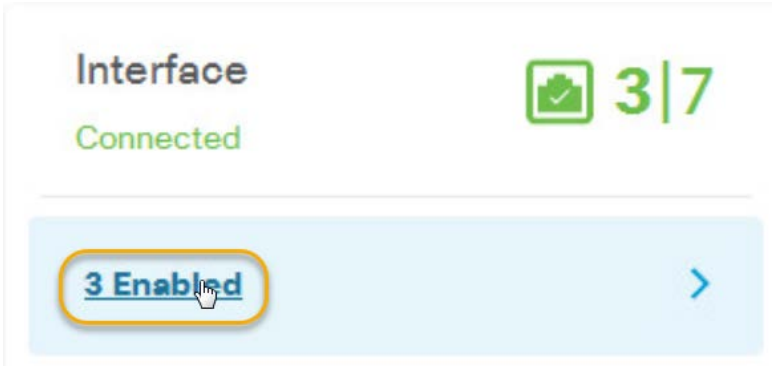
13. With the DHCP server configuration disabled and the DHCP address pool deleted you can now configure your interfaces in the right order and with the correct IP addressing. Return to the dashboard page by clicking the **remote2-ftd** menu button along the top of the page.

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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



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



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

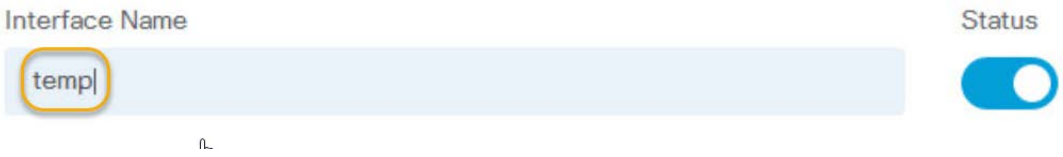


Figure 22. Click Save



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

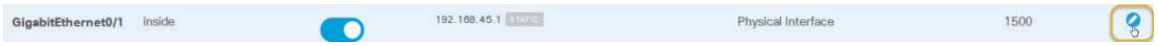
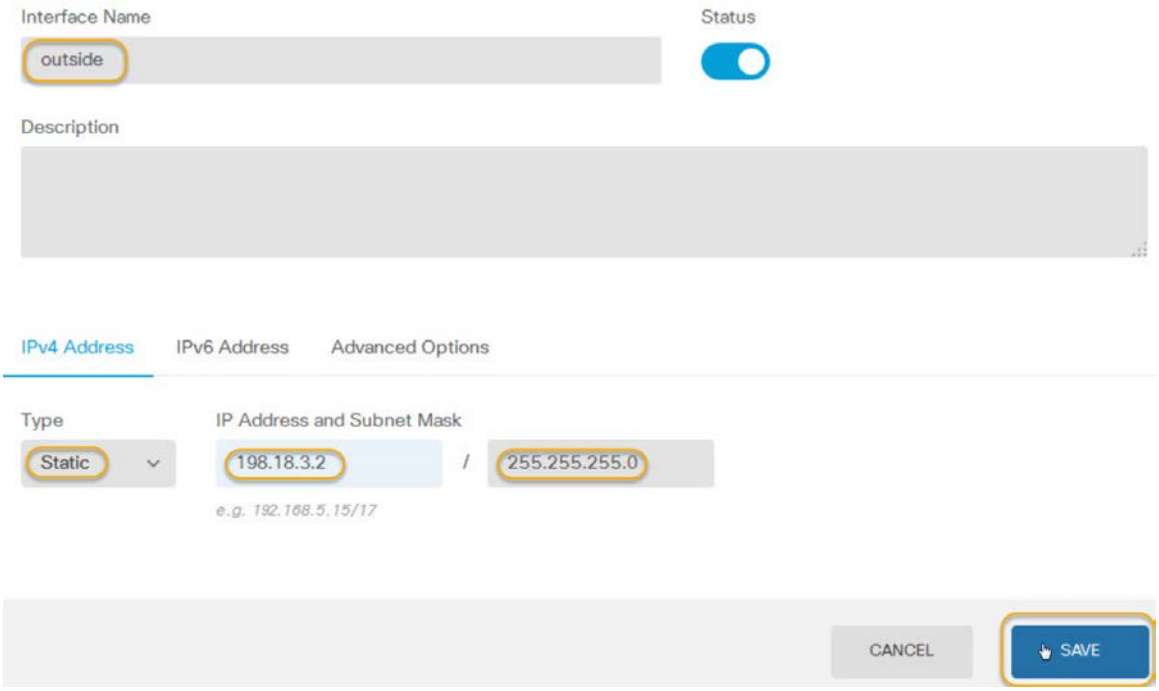
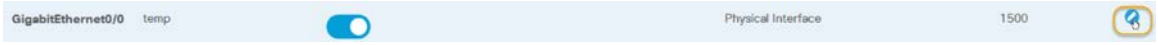


Figure 24. Configure g0/1



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**.

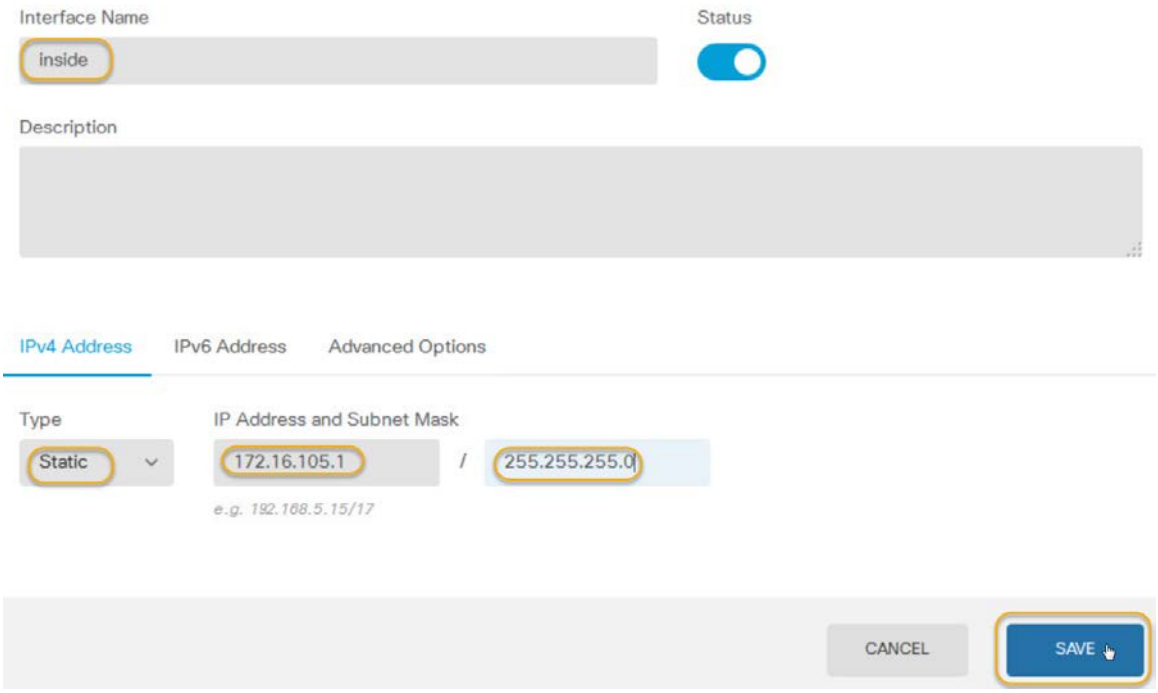
Figure 25. Edit g0/0



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

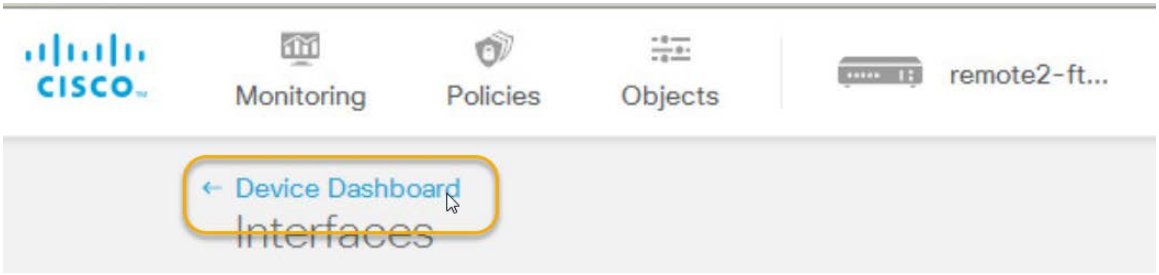
https://t.me/learningnets

Figure 26. Configure g0/0



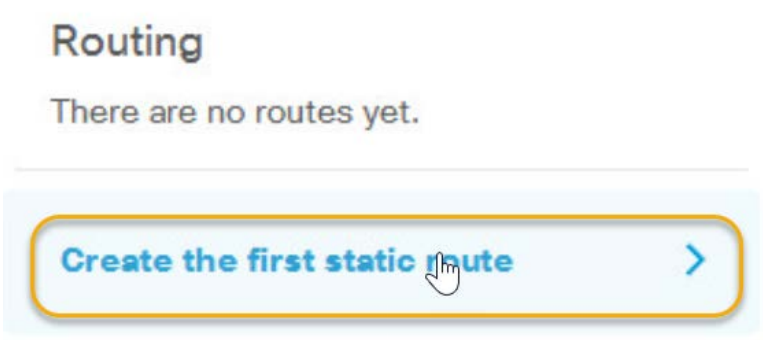
19. Return to the Dashboard page by clicking the **Device Dashboard** link in the upper-left section of this page or by clicking the remote2-ftd menu item along the top of the page.

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

22. Click the **plus icon** in the upper right corner of this page and then use the following to fill out the needed information:

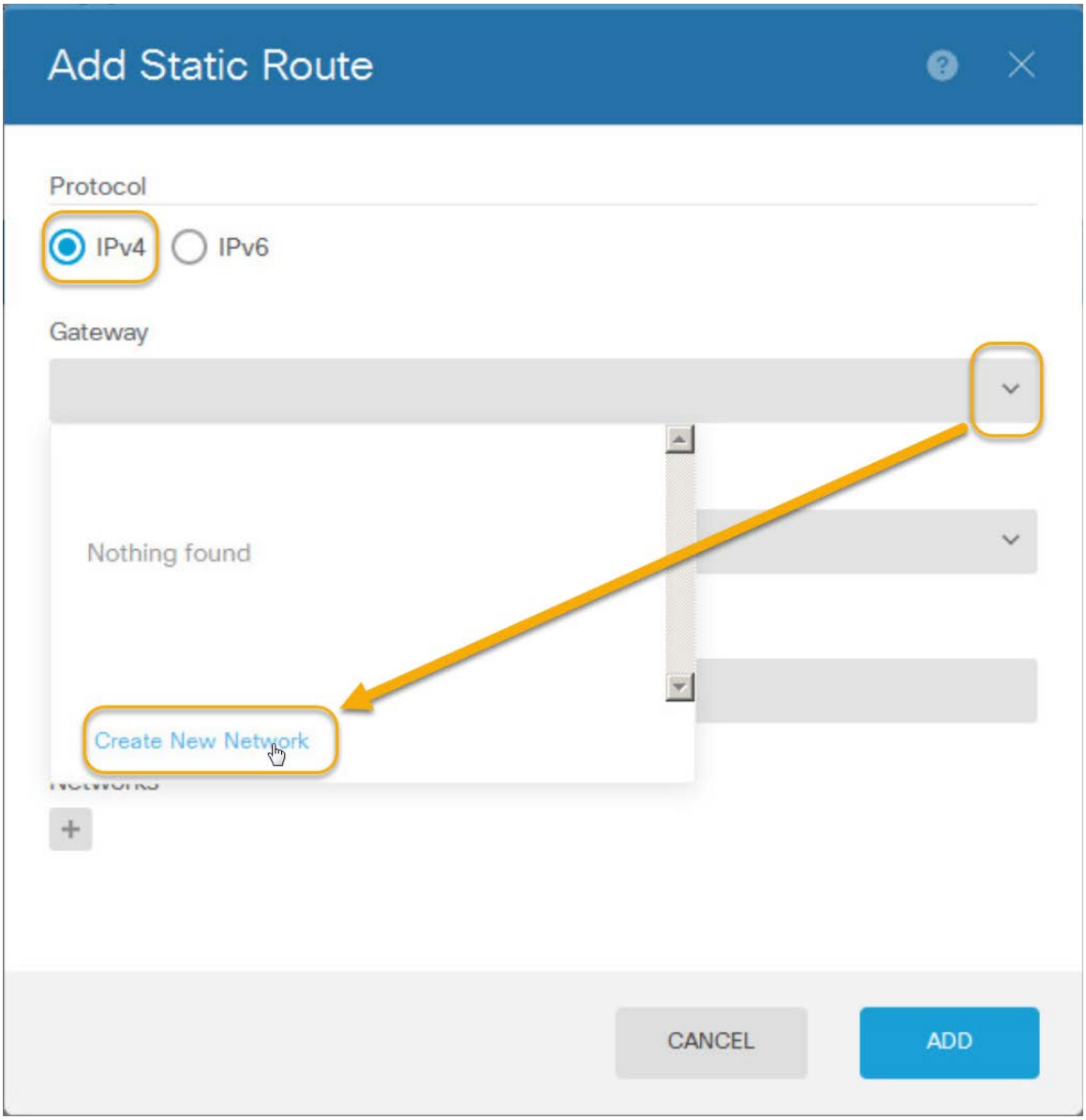
Figure 29. Add a route



a. Select **IPv4**.

b. From the dropdown menu for Gateway select **Create New Network**.

Figure 30. Configure the static route



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

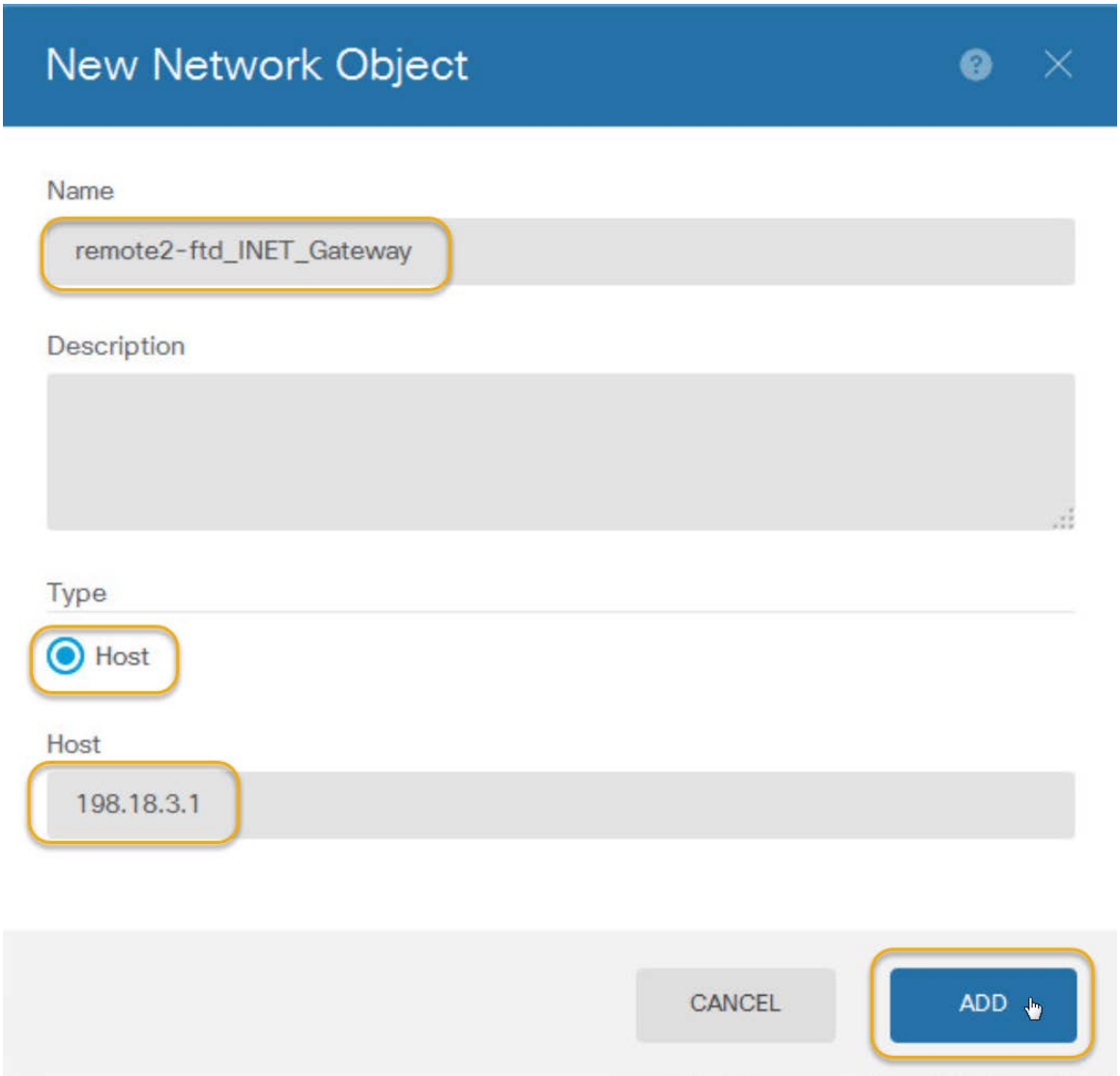
c. Use the following to fill out the needed information for the New Network Object popup window:

   i. Name: **remote2-ftd_INET_Gateway**

   ii. Host: **198.18.3.1**

   iii. Click **Add**.

Figure 31. Create a network object



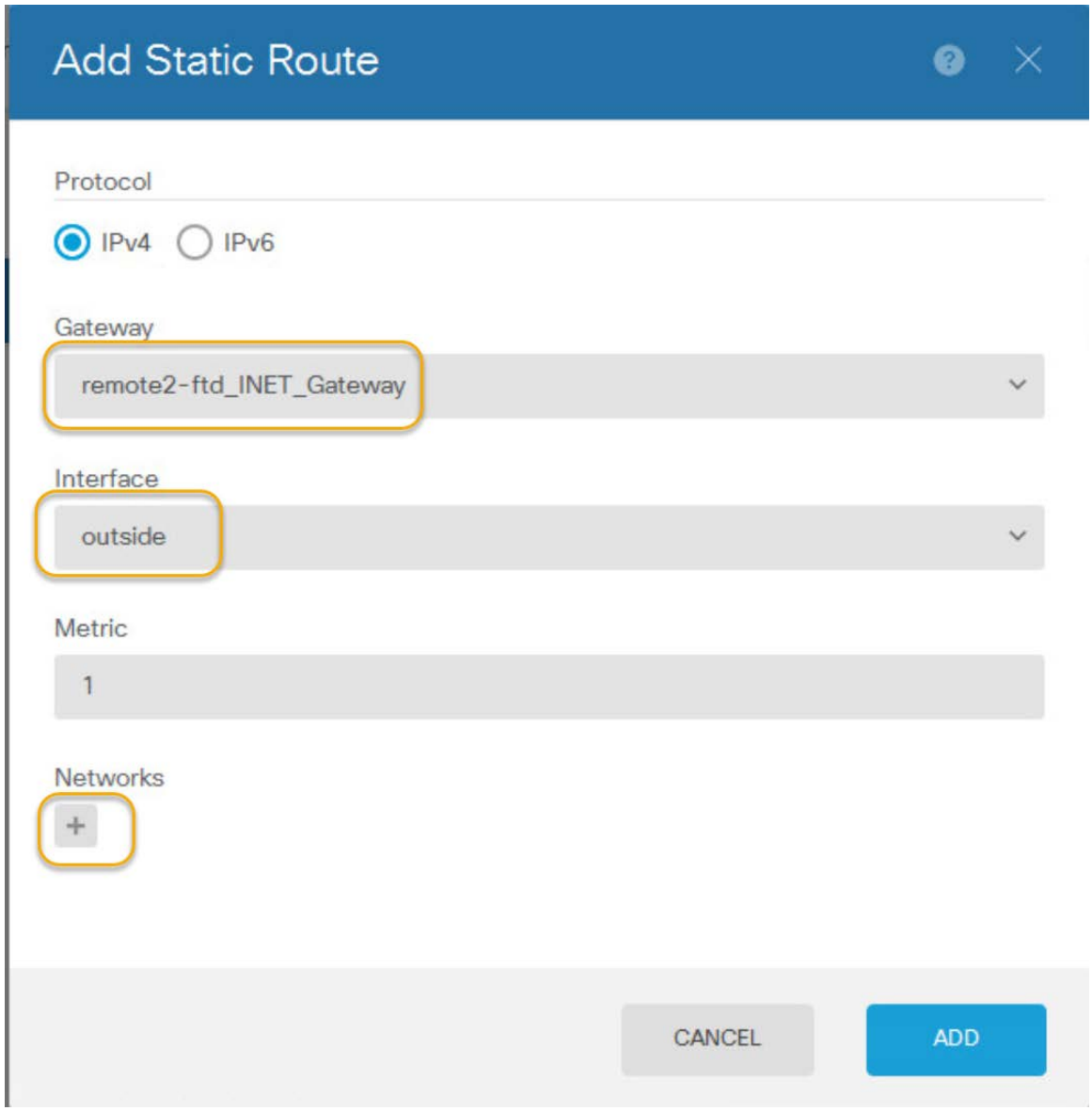
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

d. Gateway: **remote2-ftd_INET_Gateway**

e. Interface: **outside**

Figure 32. Continue filling out static route

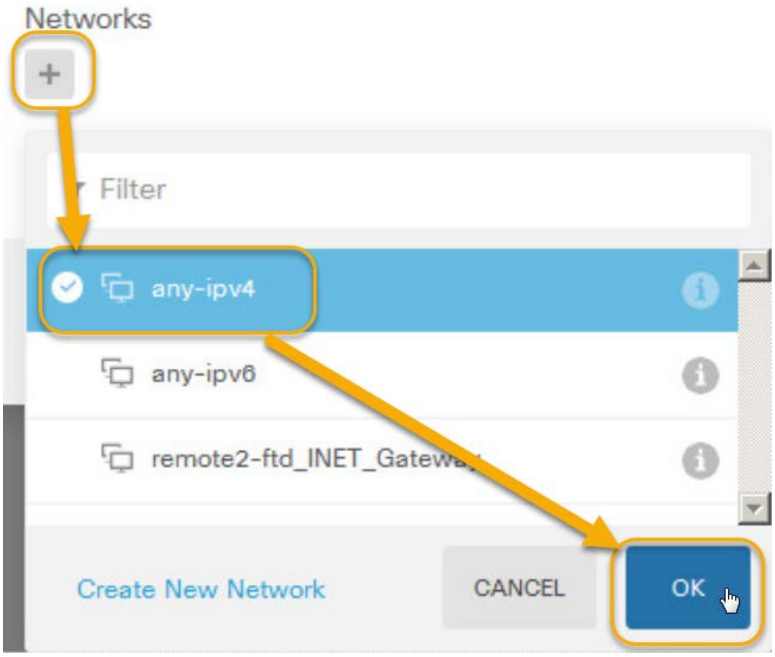


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

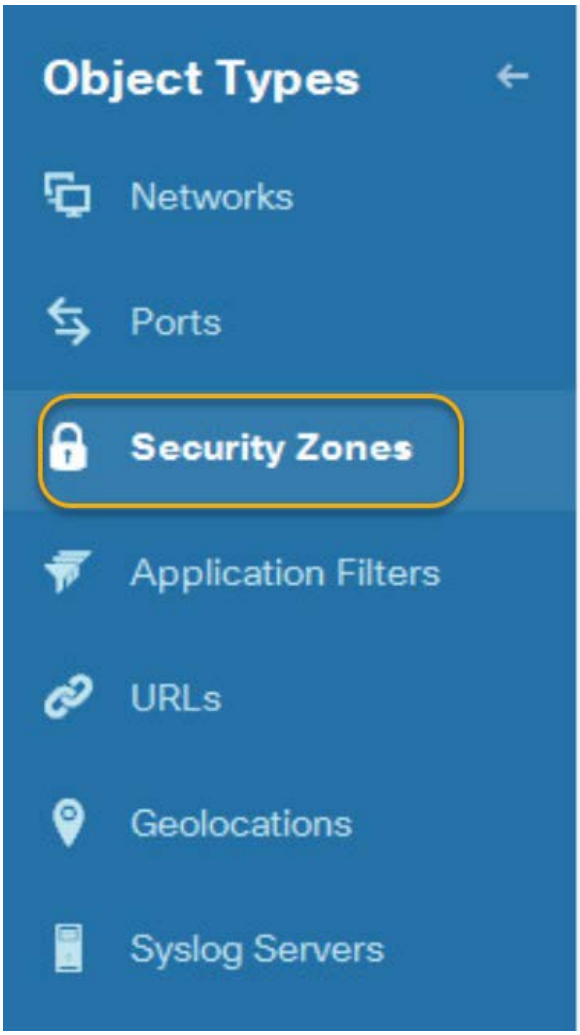


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

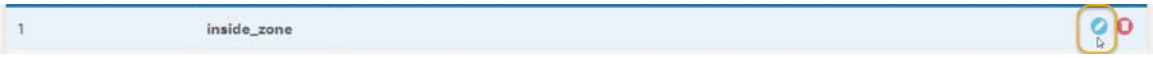
24. From the Object Types menu along the left of the page select **Security Zones**.

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

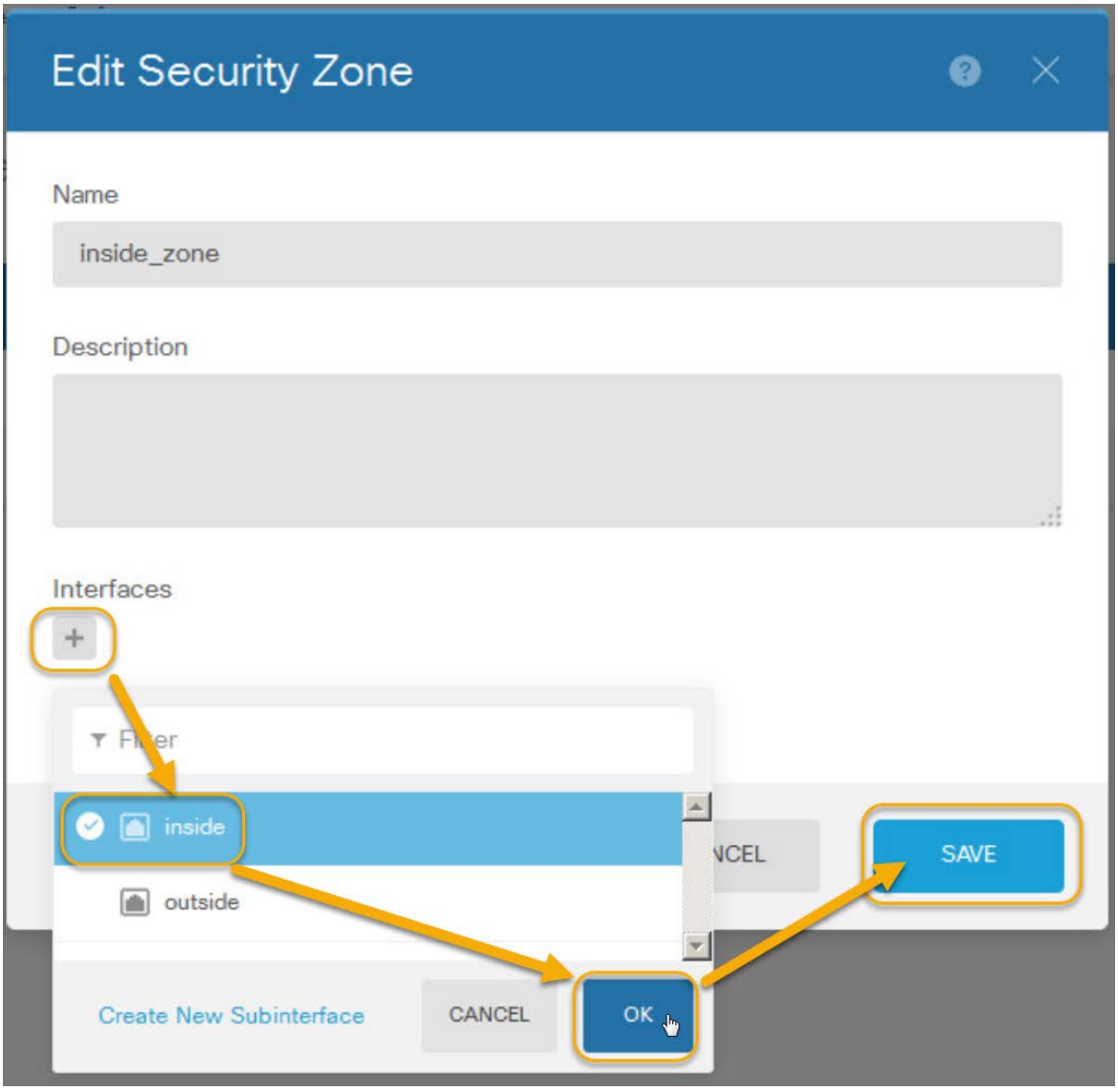
https://t.me/learningnets

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.

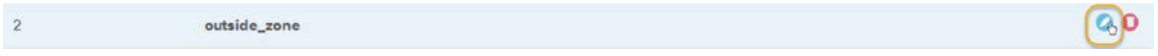
c. Click **SAVE**.

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

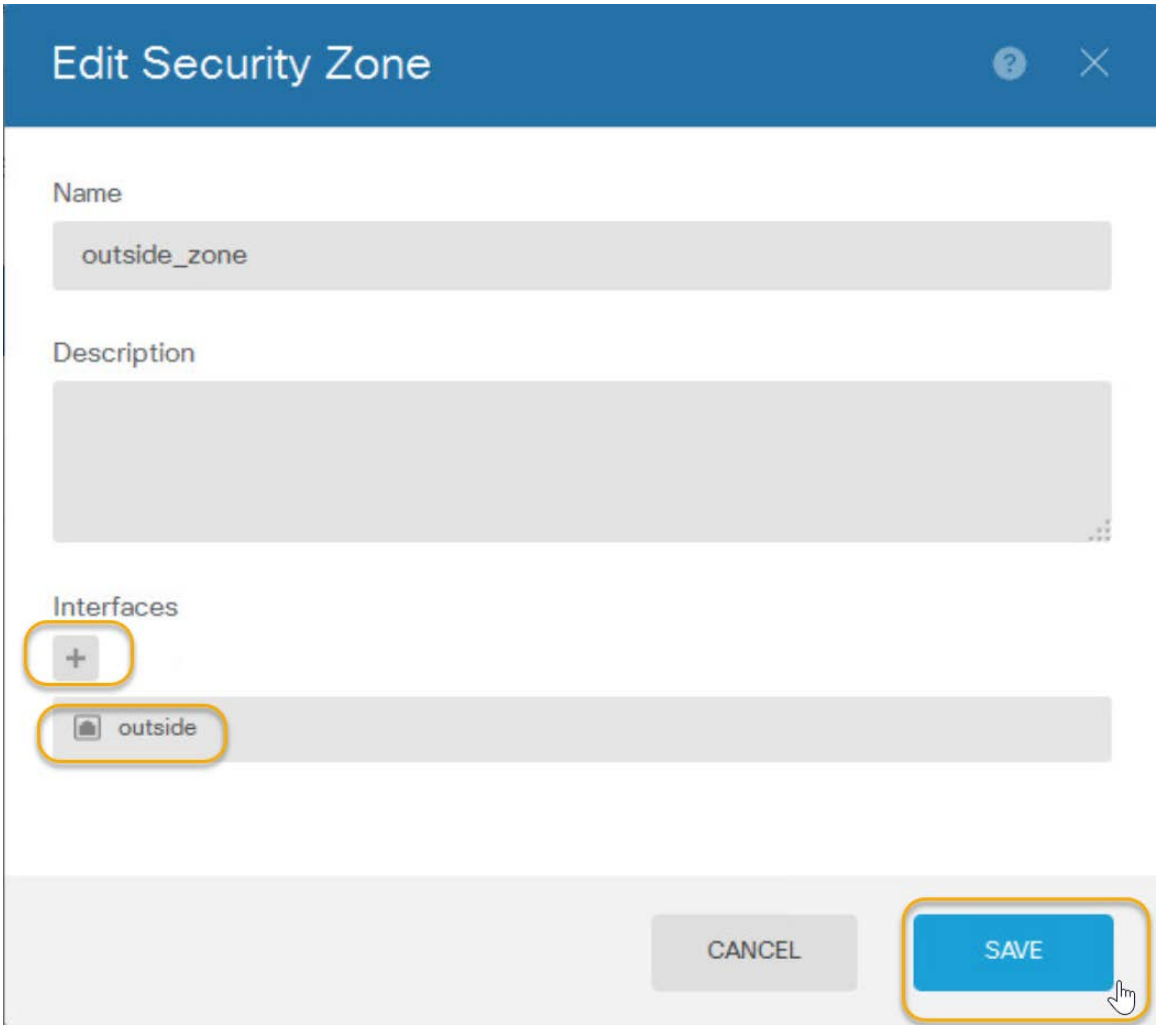
https://t.me/learningnets

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



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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

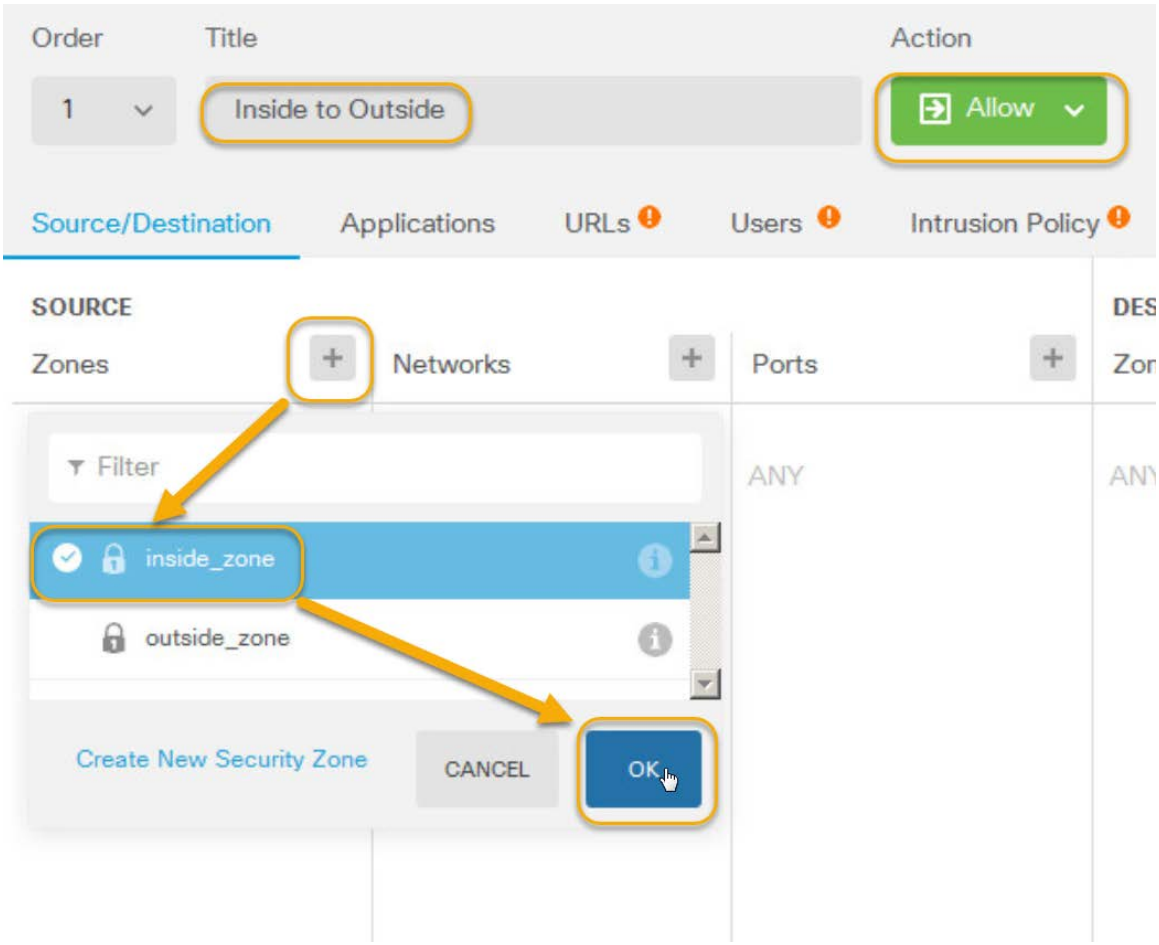


a. Title: **Inside to Outside**

b. Action: **Allow**

c. Source Zones: Click the **plus icon** and select **inside_zone**.

Figure 43. Configure Access Policy

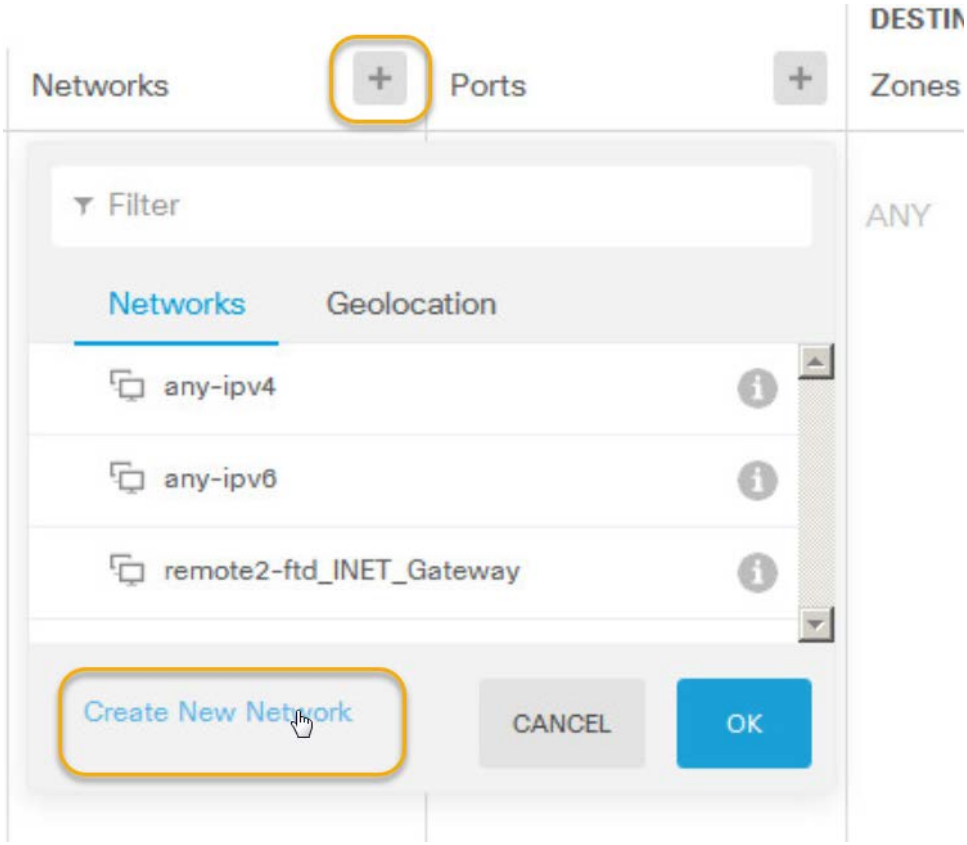


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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



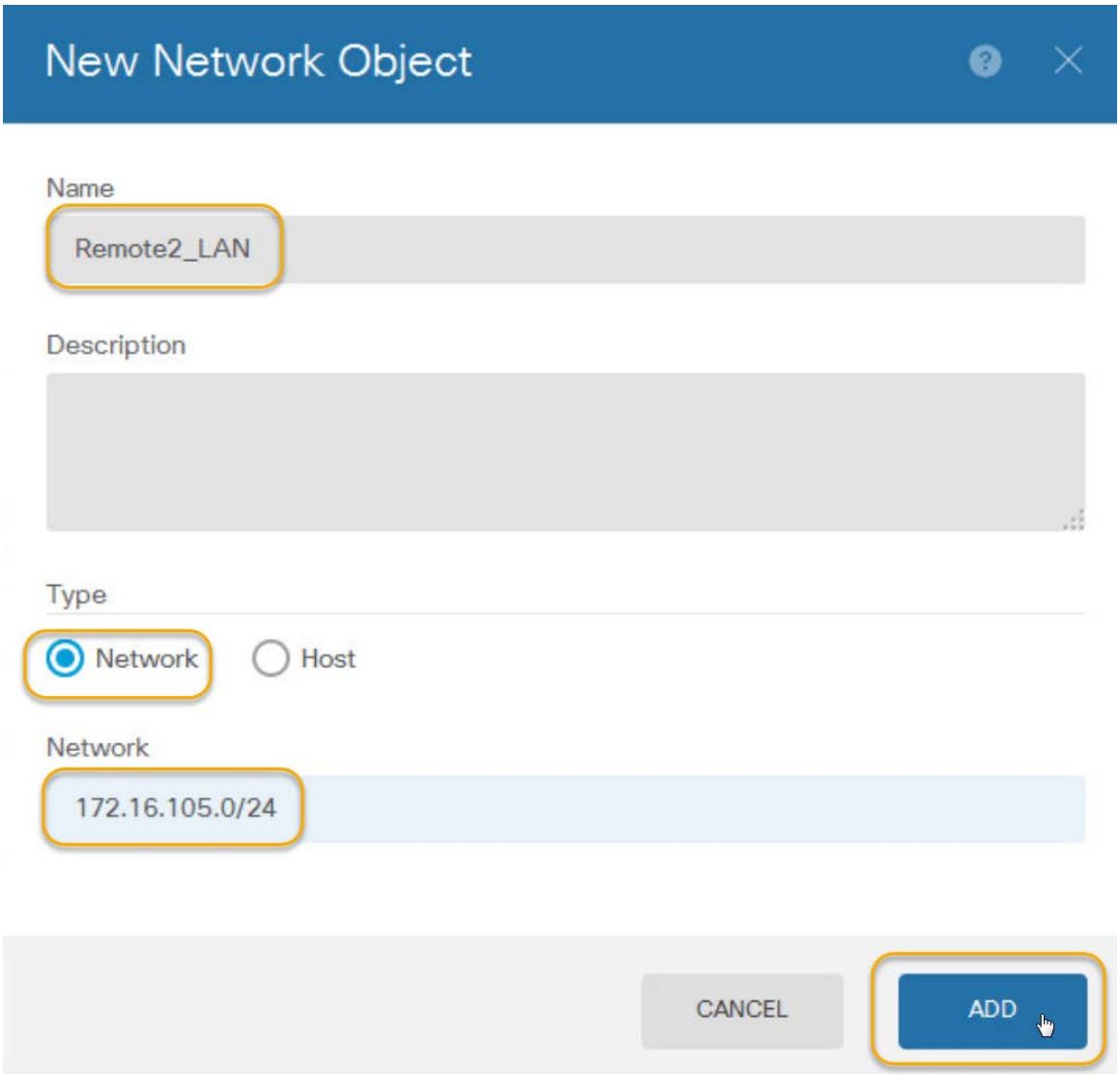
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

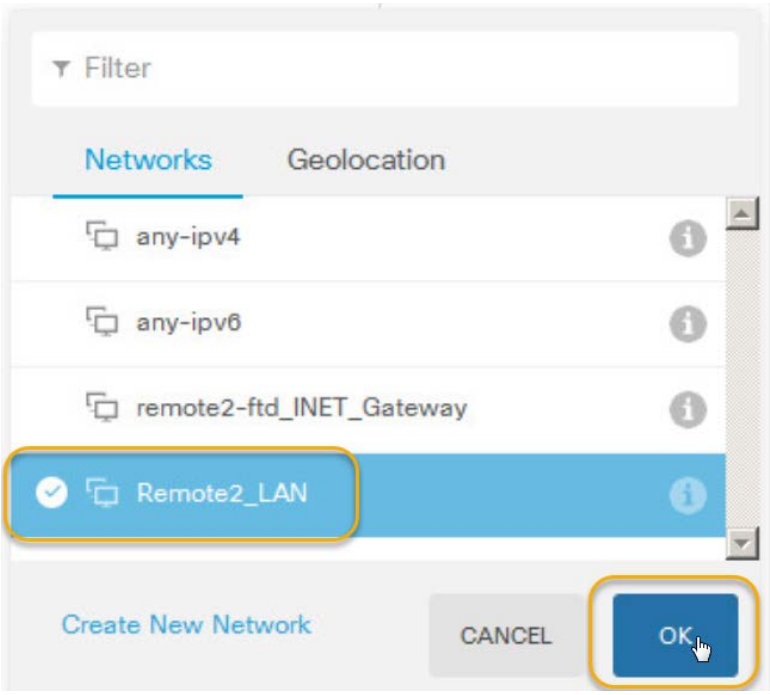


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

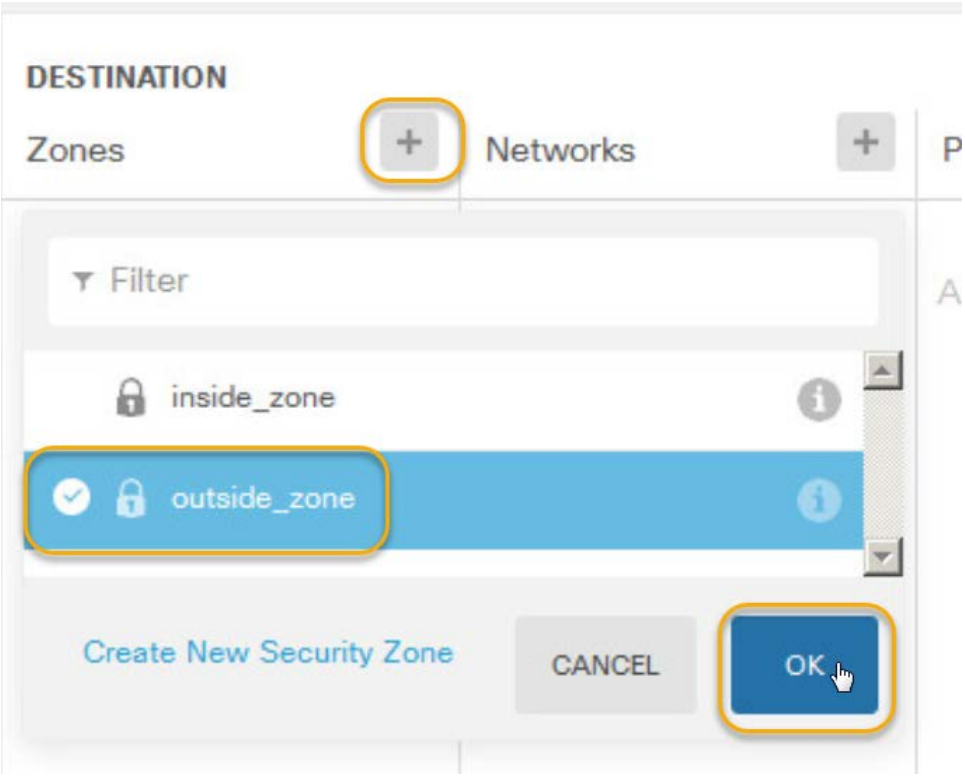
ii. Select the **Remote2_LAN** from the list of networks and click **OK**.

Figure 46. Select the Remote2_LAN object



e. Destination Zones: outside_zone

Figure 47. Select outside_zon for the destination



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

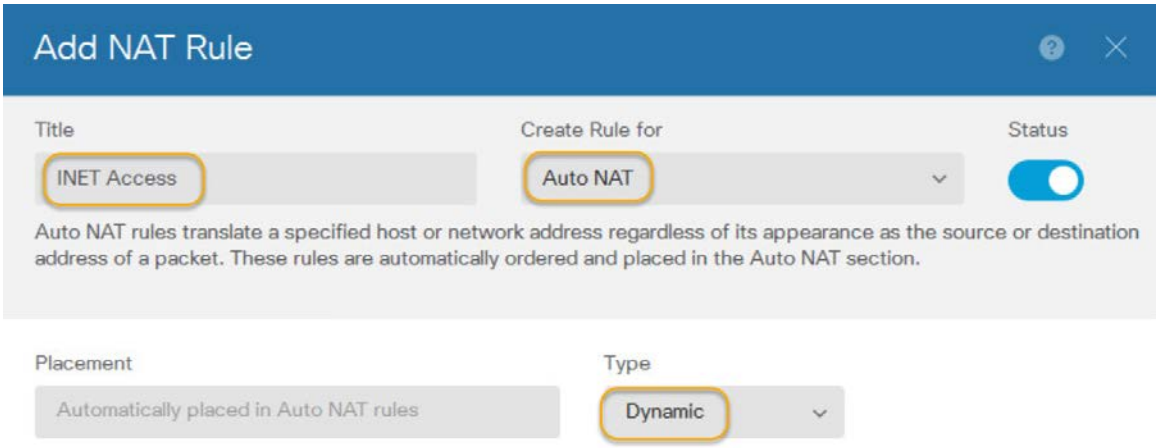
https://t.me/learningnets

a. Title: **INET Access**

b. Create Rule for: **Auto NAT**

c. Type: **Dynamic**

Figure 52. Configure NAT rule



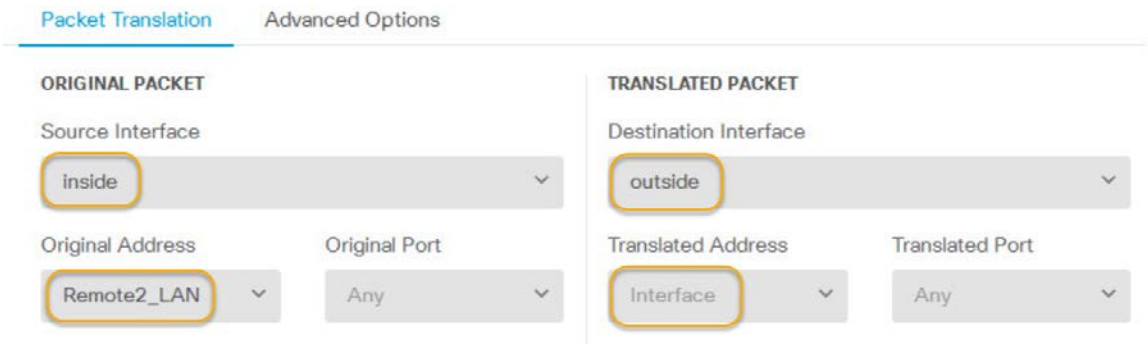
d. Source Interface: **inside**

e. Original Address: **Remote2_LAN**

f. Destination Interface: **outside**

g. Translated Address: **Interface**

Figure 53. Continue filling out NAT rule

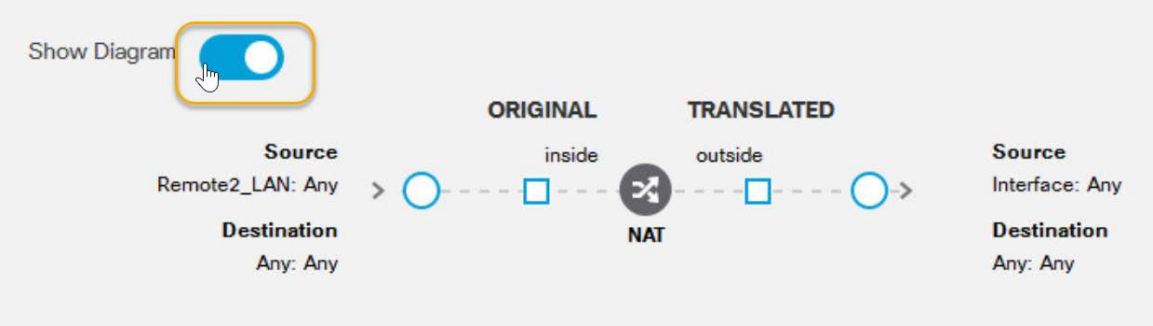


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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



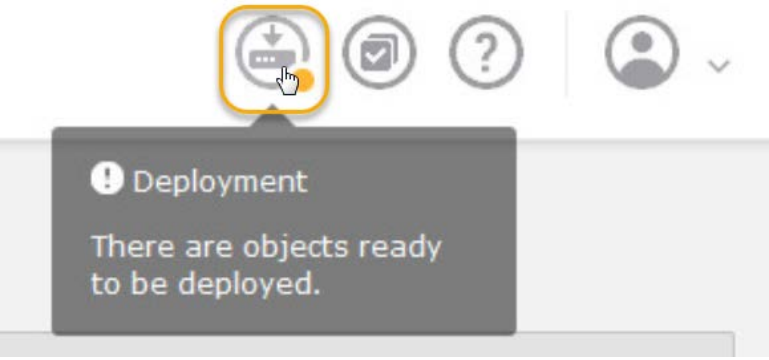
i. Click **OK** to create the NAT policy.

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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

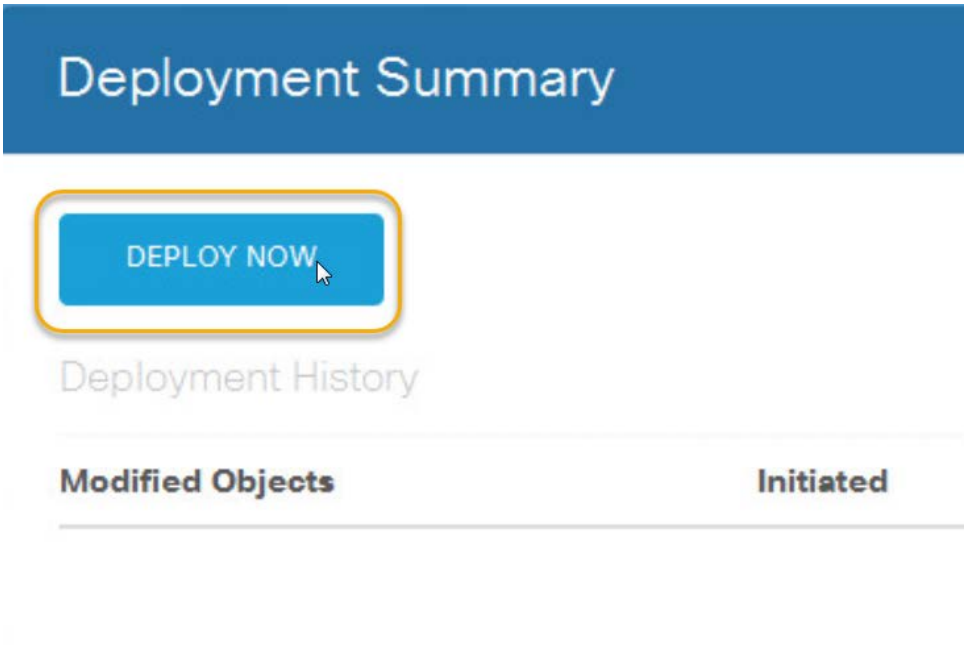
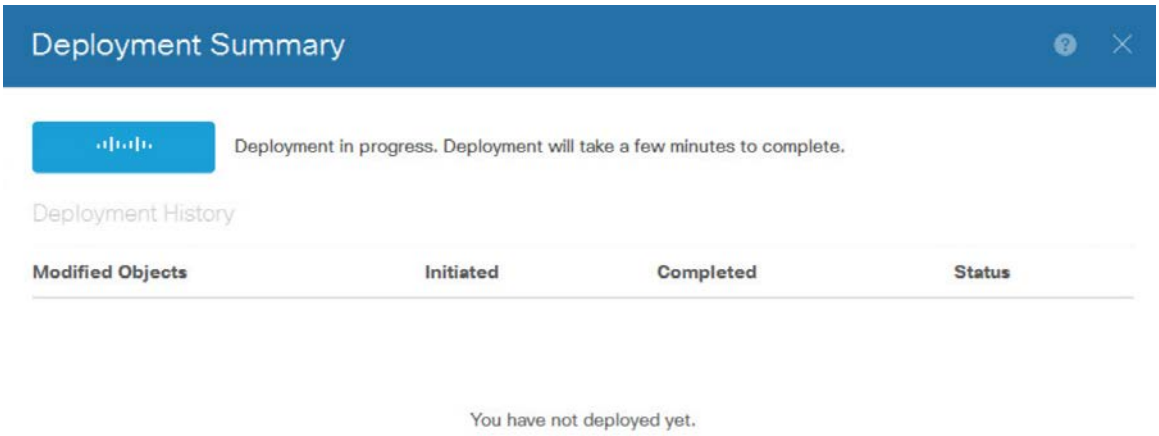


Figure 58. More confirm deployment

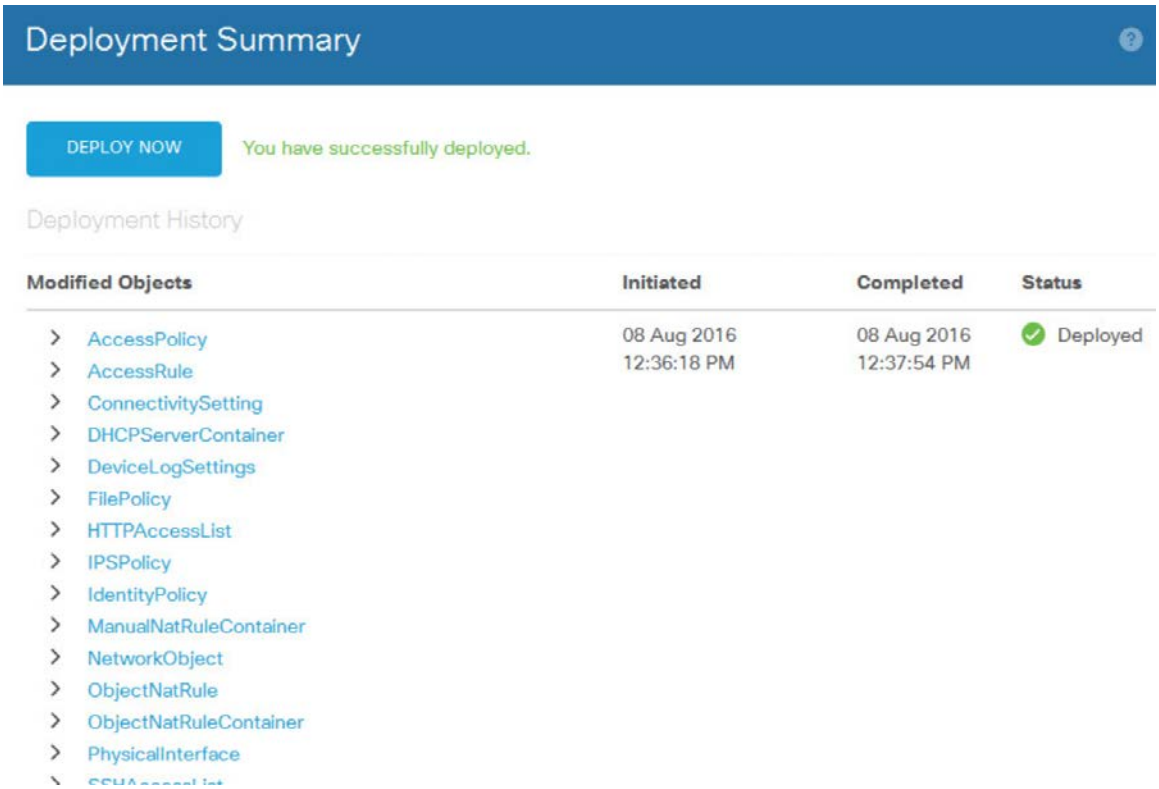


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

33. Once the Deployment Summary window show that the deployment is done close that popup window.

Figure 59. Successful deployment



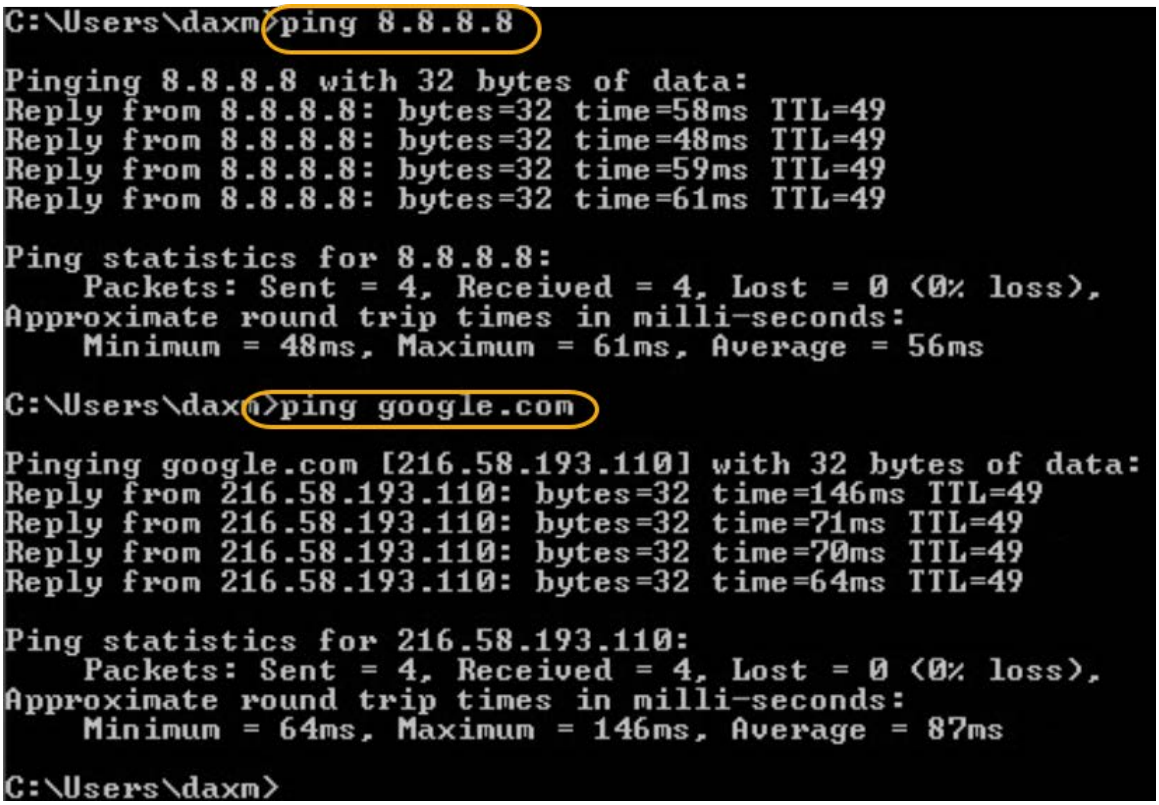
© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

Testing Remote2-FTD Configuration

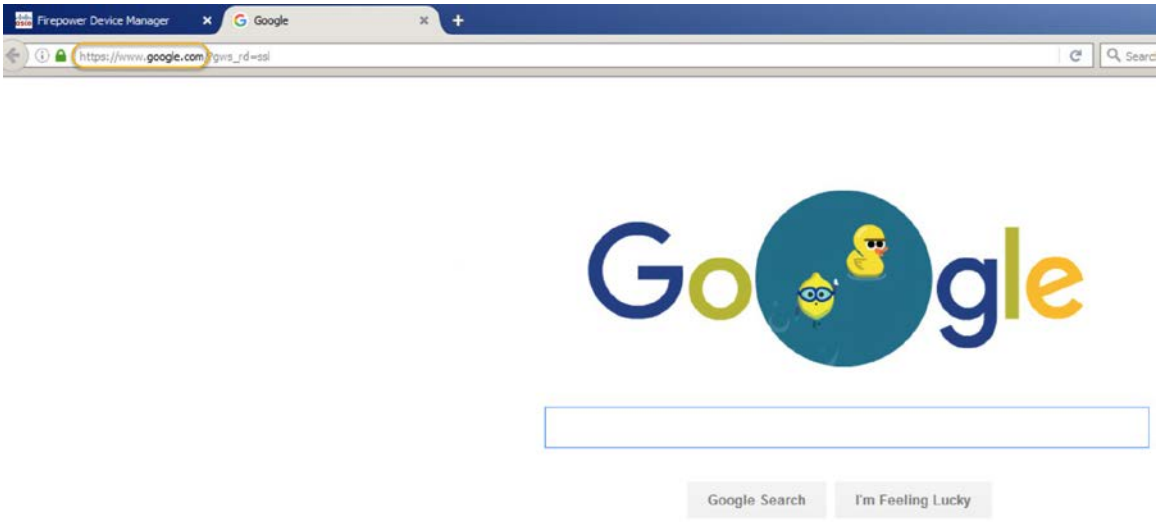
34. On **remote2-wkst** open up a **CMD prompt** and type **ping 8.8.8.8** as an initial test. This should succeed. A further test would be to ping google.com to ensure DNS resolution works too.

Figure 60. Ping test on remote2-wkst



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



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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).

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

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

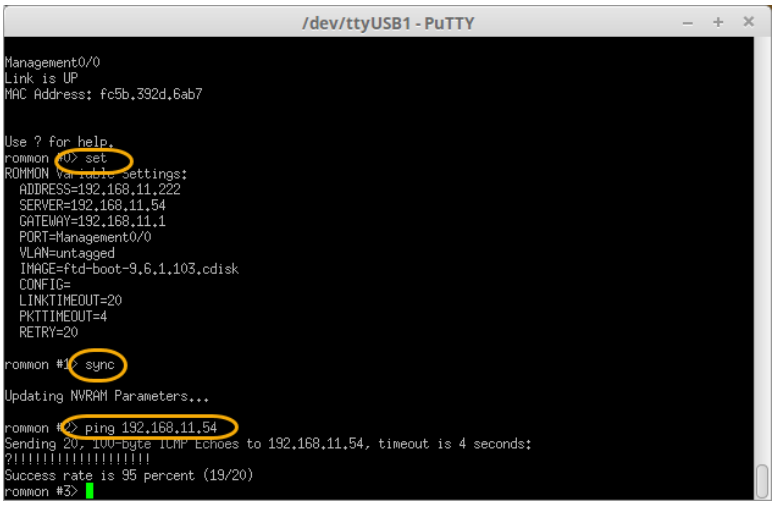
The boot image is a very simple operating system that is designed to boot your ASA NOT using the local hard drive. Think of this much like “booting from CD” when installing a new operating system on your PC. Use the following steps to install and boot the boot image.

1. **Power on your ASA** and break the normal boot process to enter ROMMON mode by pressing **ESC** when prompted.
2. 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.

3. Once the variables are correct use the **sync** command to ensure they are save in ROMMON.
4. **Ping** your **tftp server** to ensure you have access.

Figure 62. Prepare for tftpdnld

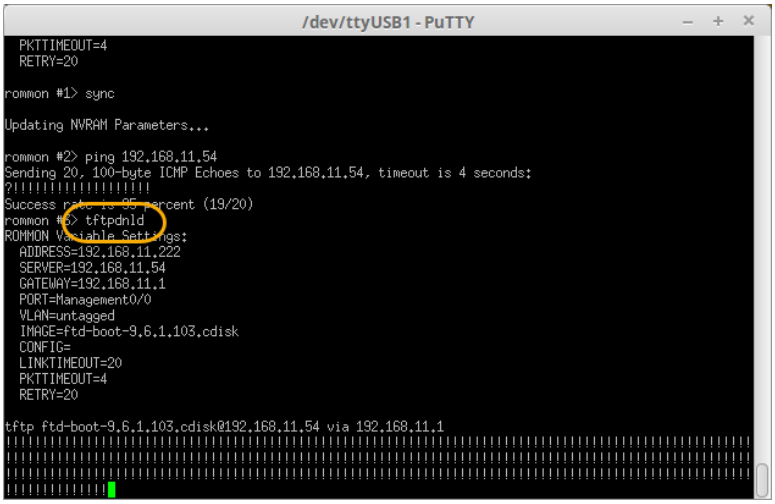


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

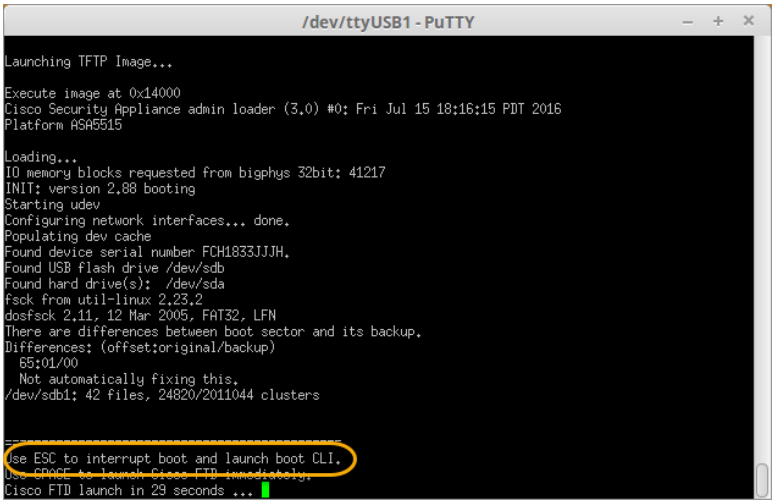
5. Use the **tftpdnld** command to start the tftp download process. Once the download is complete the system will reboot and you HAVE to break the normal boot process again in order to load the boot image or your ASA will just boot to its normal ASA code. This is probably the hardest part of this process 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



6. Press **ESC** to load the boot image when prompted.

Figure 64. Press ESC



© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

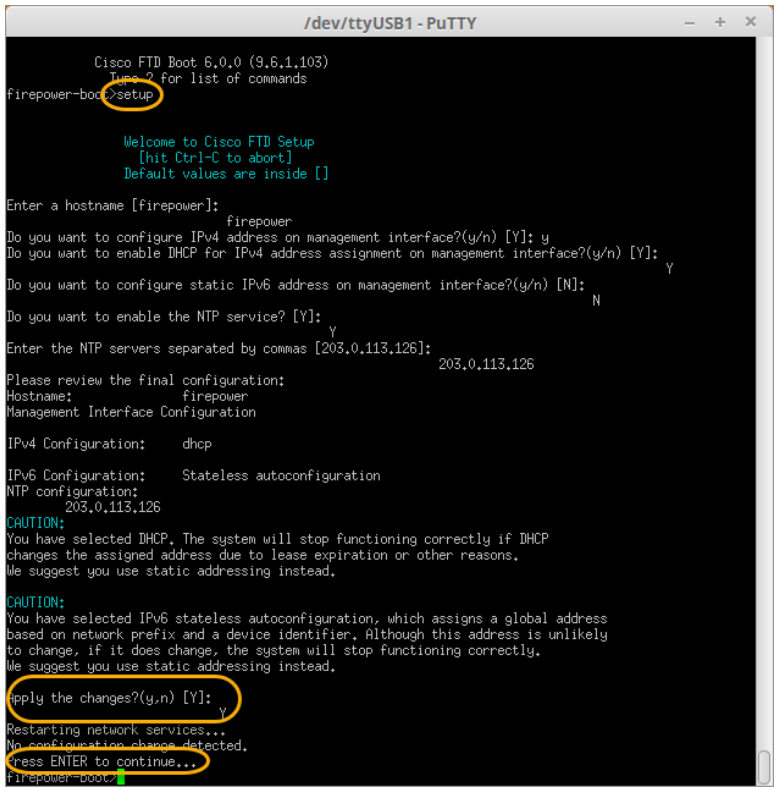
https://t.me/learningnets

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.

7. 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

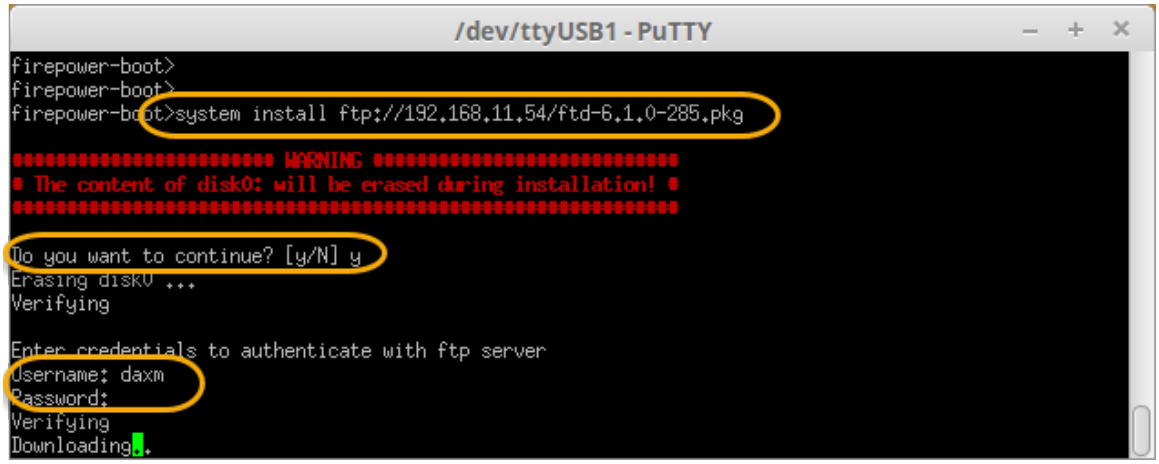


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets

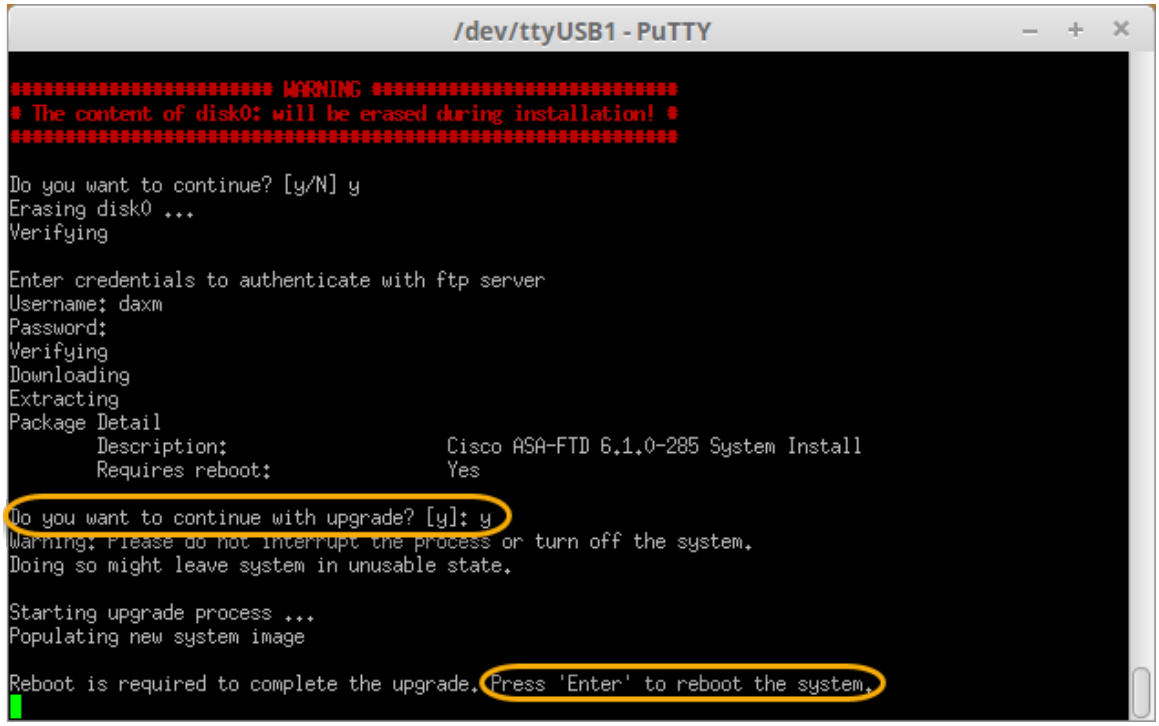
8. Unlike downloading the boot image file you must use http, https, or ftp to download the FTD code package file. Issue the command **system install** to download the package file.

Figure 66. Download pkg file



9. 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



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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

https://t.me/learningnets