ASA to FTD Migration Tool v1.1

Last Updated: 12-MAY-2017

About This Demonstration

The goal of this demonstration is to provide a guide and tool on how to convert an ASA configuration file into a format used in the Firepower Threat Defense (FTD) Next Generation Firewall (NGFW).

Though the output file generated using this dCloud demo could be used in a real world scenario it needs to be stressed that this is a demonstration of the tool and that its use should be limited to just that – a demonstration.

NOTE: PLEASE do not enable the interfaces on the provided FTD devices within the lab. Not only are they all cabled to the same network, which won't provide you any value in testing, they could also adversely affect your demo session by creating bridging loops.

The guide for this demonstration includes the following:

Requirements

The table below outlines the requirements for this preconfigured demonstration.

Table 1. Requirements

Required	Optional
• Laptop with Cisco AnyConnect® • A valid ASA configuration file.	• No optional requirements for this lab.

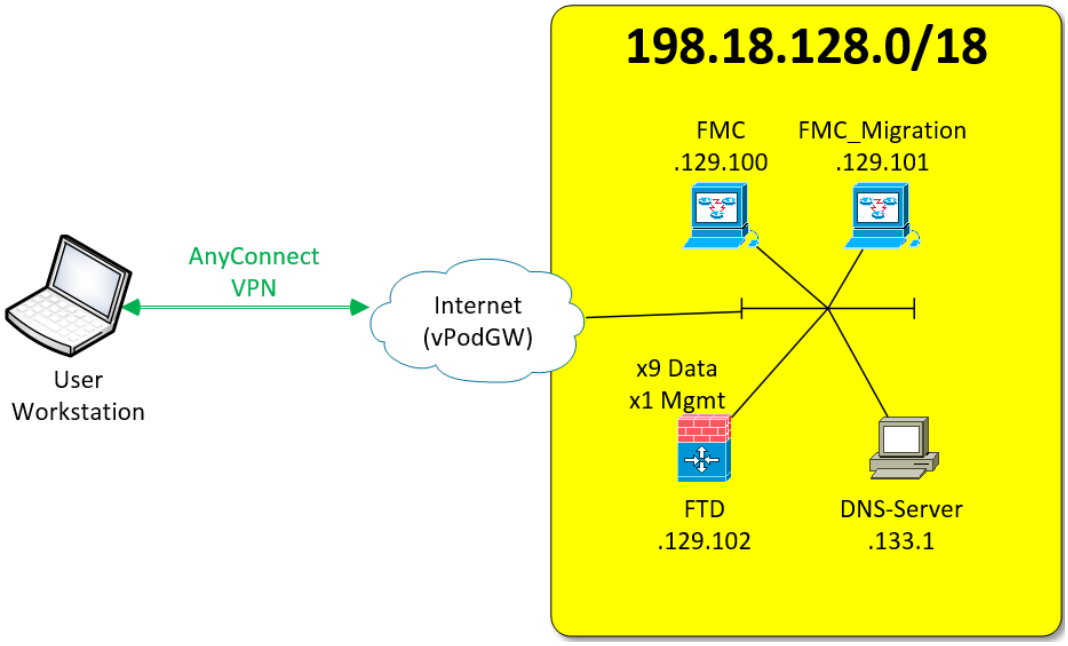
Topology

This topology does not indicate a mandatory configuration of the applications shown. The FMC and the Migration FMC can be on completely separate broadcast domains. The important thing to note is that you cannot use the “production” FMC for the migration – a separate, specially prepared FMC must be used.

The provided FTD device is available for testing the migrated configuration and not for actual data flow.

The DNS-Server is only there because the dCloud AnyConnect VPN sets your DNS server settings to point to this server. It is configured to allow you to connect to each of the devices within the topology via their FQDN but that is not mandatory.

Figure 1. Lab Topology



Scenario 1. Connecting to the Topology Environment

Scenario Description

This topology 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 then use a web browser to connect from your workstation to the FMC or FMC_Migration configuration GUIs.

VPN to the topology

1. Go to http://dcloud.cisco.com and log in using your Cisco CCO credentials.
2. Get your session'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 the IPs within the environment.

Access the FMC and FMC_Migration Web GUIs

6. Connect to the FMC and FMC_Migration GUIs using your local workstation's web browser.
    a. FMC: **https://198.18.129.100**, Username: **dcloud**, Password: **C1sco12345**.

NOTE: This FMC has a custom user account because it is associated with the dCloud Smart Licensing account. Therefore, this user does not have access to the Smart Licensing sections of the GUI. Please respect this and do not try to access this section as it could break all the dCloud labs using Smart Licensing.

    b. FMC_Migration: **https://198.18.129.101**, Username: **admin**, Password: **Admin123**

NOTE: The FMC and FMC_Migration VMs were deployed from the same source OVF file. Other than configuring different IPs for each, the only difference is a CLI command issued on the FMC_Migration VM to convert it to a specialized version of FMC that is dedicated to migrating ASA configuration files to FMC formatted files. You can learn more about how this VM was deployed in the Appendix A section of this guide.

Scenario Summary

This scenario connected your laptop/workstation to the dCloud session environment and ensured you could access both the FMC and FMC_Migration web GUIs.

Scenario 2. The ASA Configuration File

Scenario Description

This scenario discusses the requirements of the ASA configuration file, what commands are or are not supported for migration, and where in the FTD the supported commands will be imported.

Section 1: Supported Commands for Conversion

Not all commands within the ASA configuration are converted to the FTD. Many of the commands do not even have a corresponding equivalent! The main general categories for commands that are eligible for conversion are as follows:

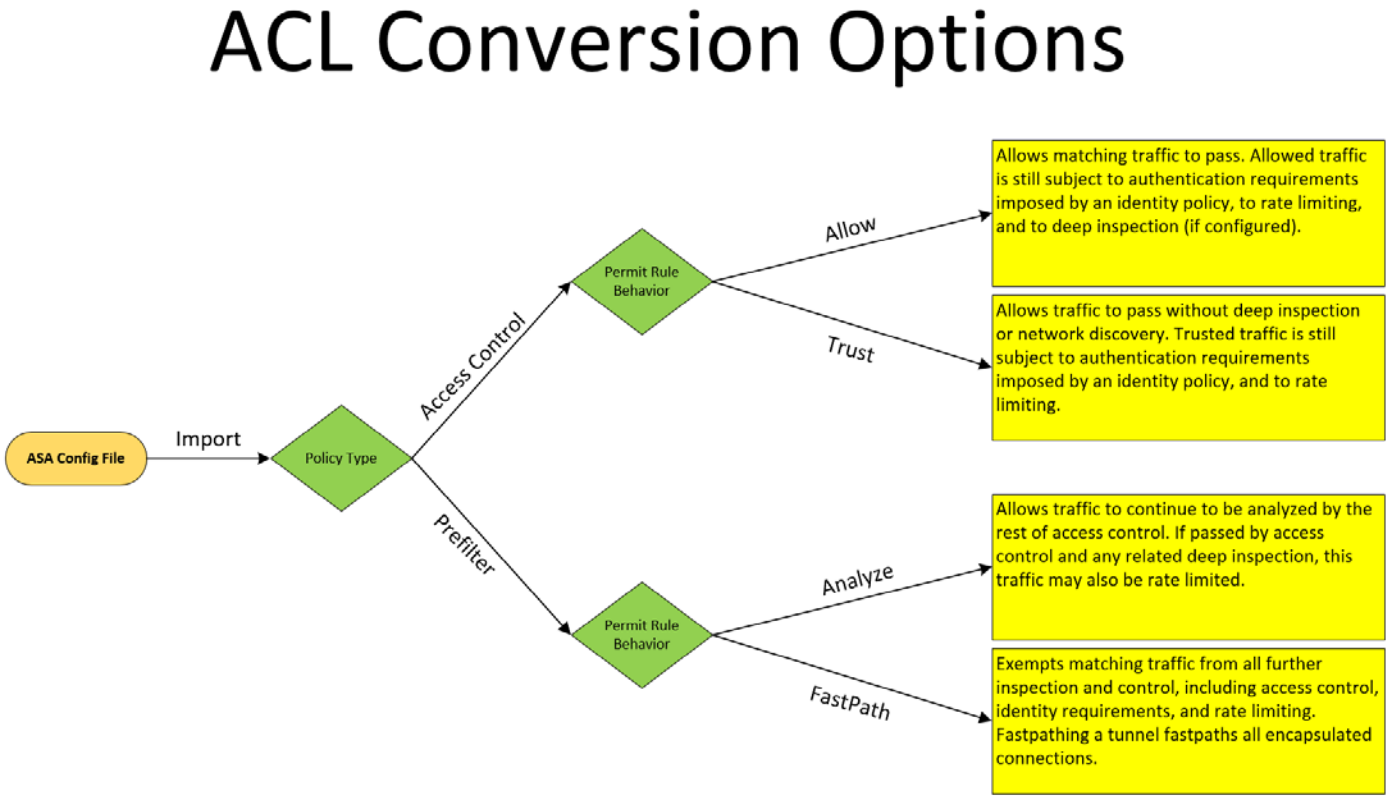
- Extended Access Control Rules
- NAT (Twice NAT and Object NAT)
- Any Network Object, Network Group Object, Service Object, Service Group Object associated with the above supported NAT and ACL rules.

Then each of these supported categories of commands have a list of caveats of what will or will not get converted. Check the **Cisco ASA to Firepower Threat Defense Migration Guide, Version 6.2** for more information on these caveats.

Section 2: ACL Conversion

When converting ASA Access Control List commands into a format that works in the FTD you will need to decide which “path” these rules will be imported. What is meant by that is there are two places in the FTD where Access Control type rules can be located. Either in the PreFilter Policy or the Access Control Policy sections. This demo focuses more on the mechanics of doing the conversion but here is a quick guide to your import options.

Figure 2. ACL Conversion Options



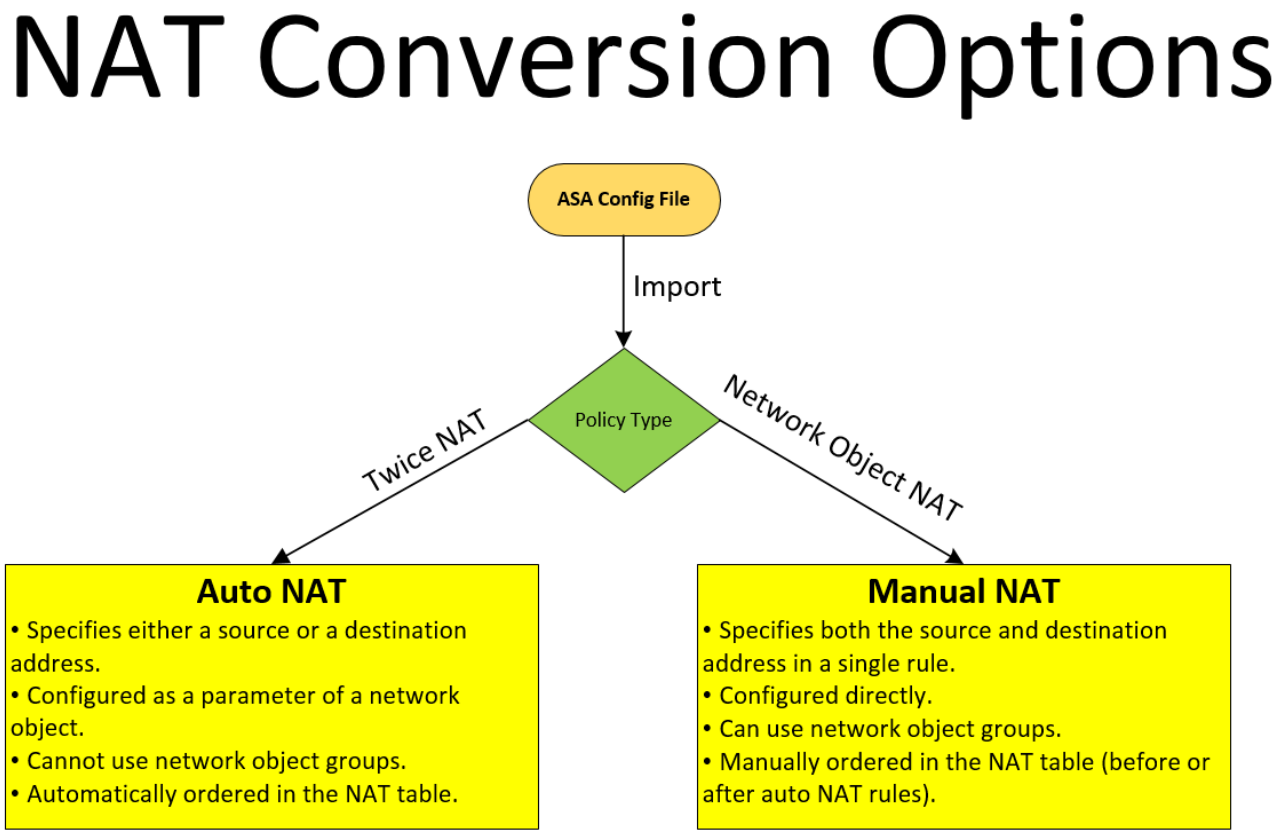
Access Control List commands that have unsupported features (like the time-based feature) can be imported along with the supported commands. However, they will be disabled by default so that you can evaluate how to deal with the issue of the unsupported feature.

Access Control Lists with logging enabled will have the option to enable logging “At the start of connection”, “At the end of connection”, or “Both”.

Section 3: NAT Conversion

The NAT conversion is more straightforward. Twice NAT rules become Manual NAT rules, Network Object NAT rules become Auto NAT rules.

Figure 3. NAT Conversion Options



NAT commands with unsupported features will not be converted and the conversion will fail.

Section 4: Network and Service Objects/Groups

The Network and Service Objects and Object Groups will only be converted when they are needed or associated with the Access Control Rules or NAT Rules that are being converted. Not all features within these features is supported in the FTD

Section 5: Other Important Information Regarding the ASA Configuration File:

Here are a list of other tidbits of important information regarding the ASA configuration file:

- The configuration file must be the plain text version of the configuration. This means a ".cfg" or ".txt" file.
- The file must have the ASA version command in it. Supported versions are 9.1 thru 9.6.
- The configuration must be in single context mode.
- The configuration must be from the Active ASA if from a failover pair.
- The configuration must be from the Master unit if from a cluster.

Scenario Summary

Though there were no "actions" to be done in this section within the demo environment it is important to know what type of ASA configuration file will be supported for the conversion as well as knowing what commands are supported. There is a lot more information about the details regarding these topics in the ASA to FTD Migration Tool Migration Guide.

Scenario 3. Perform ASA Configuration Conversion

Scenario Description

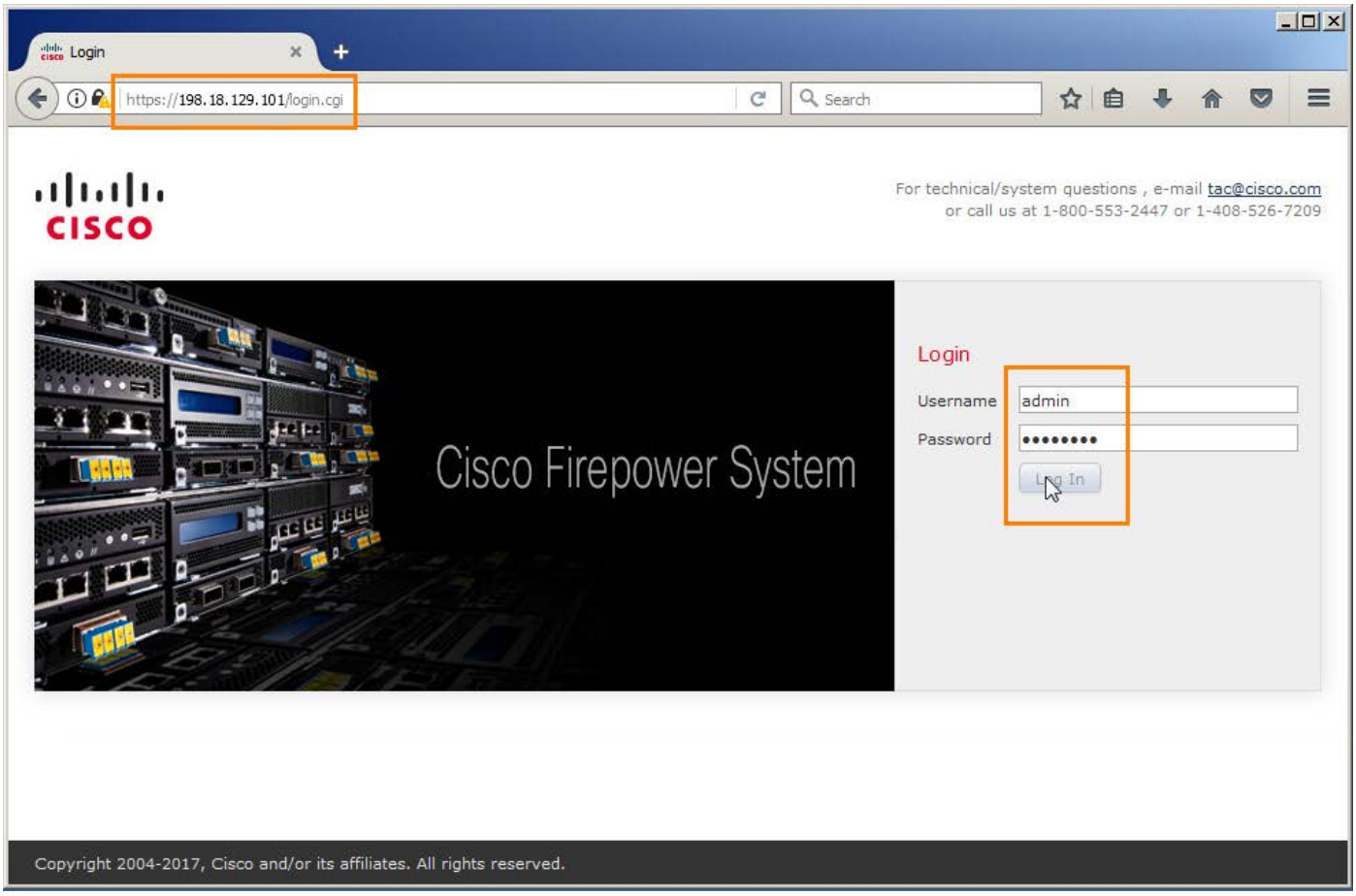
This scenario will walk you through the steps necessary to perform the conversion of the ASA configuration file a format supported by the FTD.

Section 1: Convert the ASA Configuration File

NOTE: This demo provides an ASA configuration file for conversion. However, the main goal is that this demo will be used either as a POV or as a tool to convert ASA configuration files into a format that is supported by FTD.

1. Once you have established your VPN into the demo (see Scenario 1 for more information) access the FMC_Migration web GUI by browsing to https://198.18.129.101. Log in as **admin** with a password of **Admin123**.

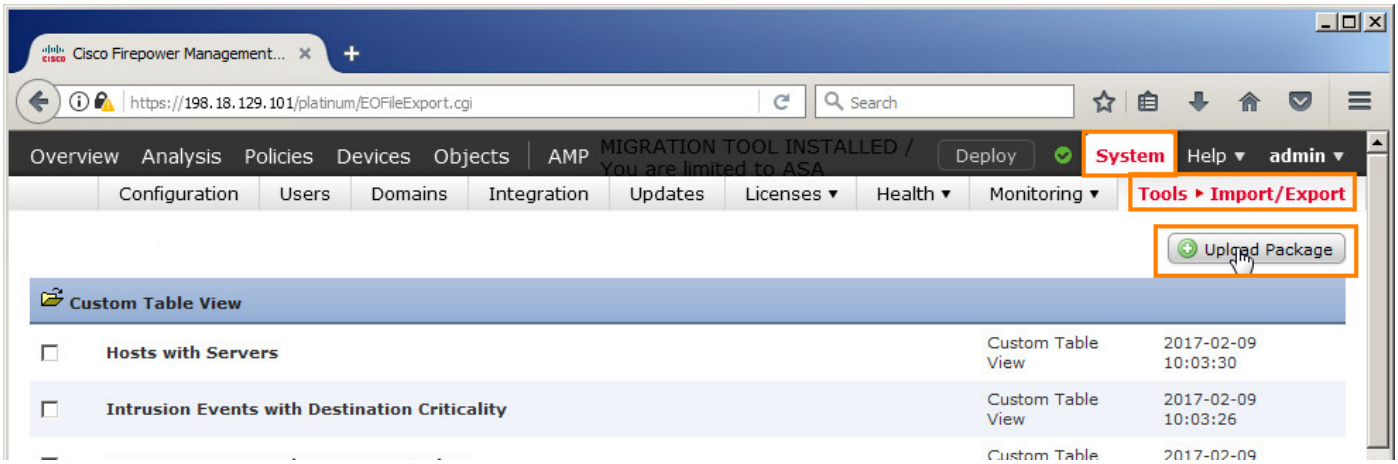
Figure 1. Log into Migration FMC



NOTE: This specially configured FMC has the sole purpose of converting ASA configuration files to a format that a standard FMC will support. You can see details on how this migration-enabled FMC was set up in Appendix A.

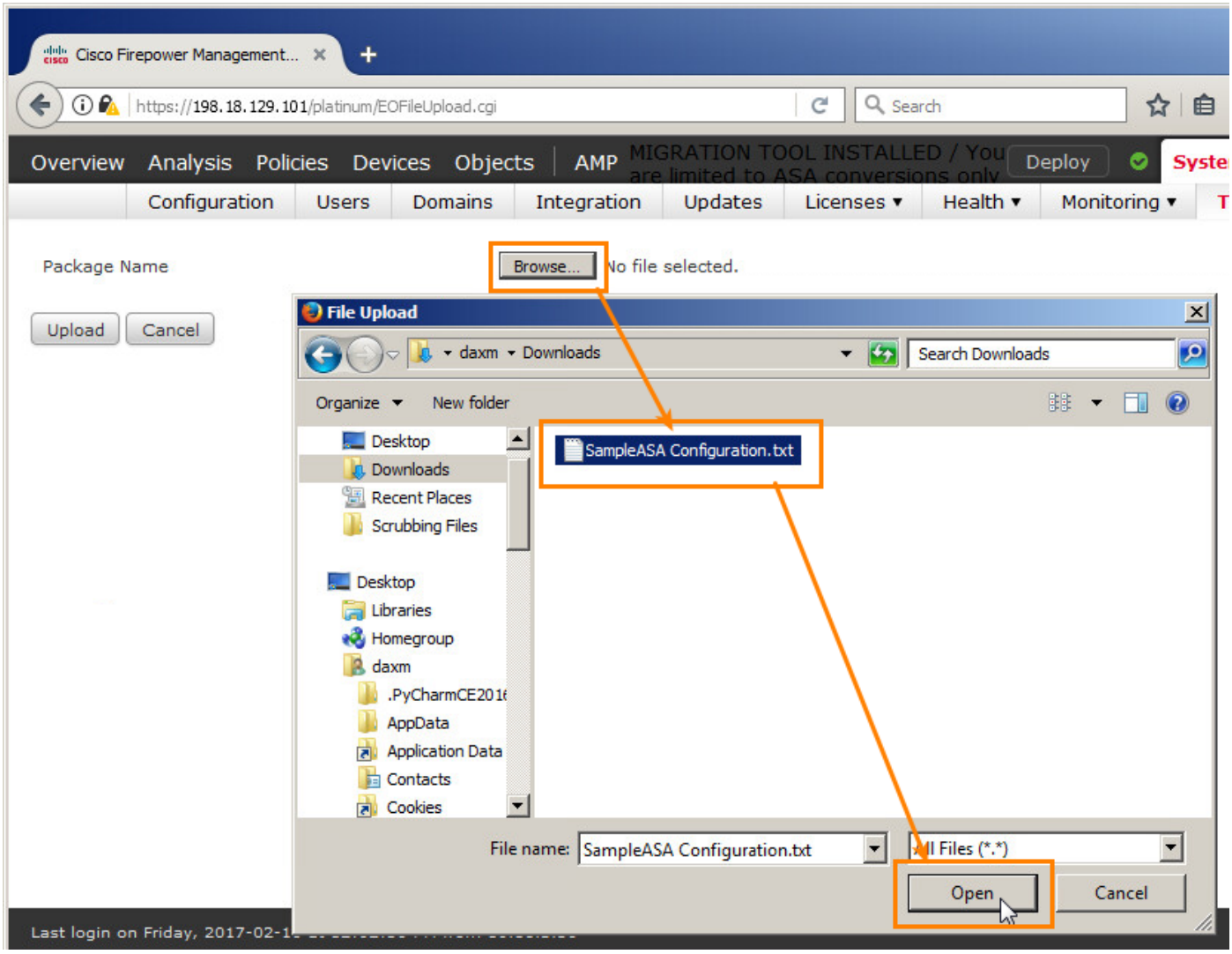
2. Navigate to **System > Tools > Import/Export** and then click **Upload Package**.

Figure 2. Navigate to Import/Export



3. Click **Browse…** to find and select your ASA configuration file. Once selected click **Open**.

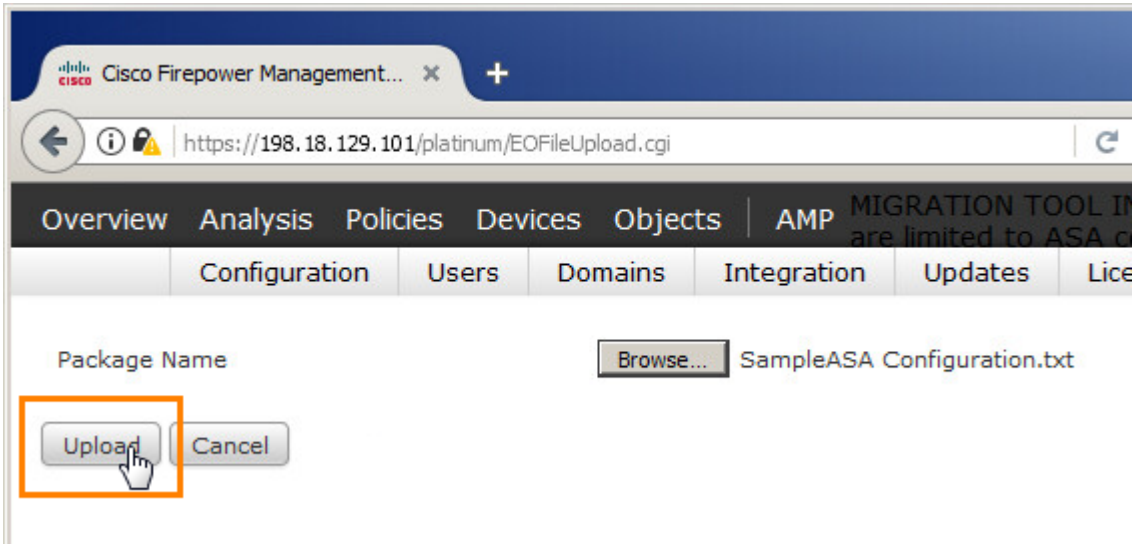
Figure 3. Find and Load ASA Configuration File



NOTE: The SampleASA Configuration.txt file is located in the **Resources** tab in your dCloud session for this lab.

4. Click **Upload** to load the ASA configuration file into the FMC Migration GUI.

Figure 4. Upload the File



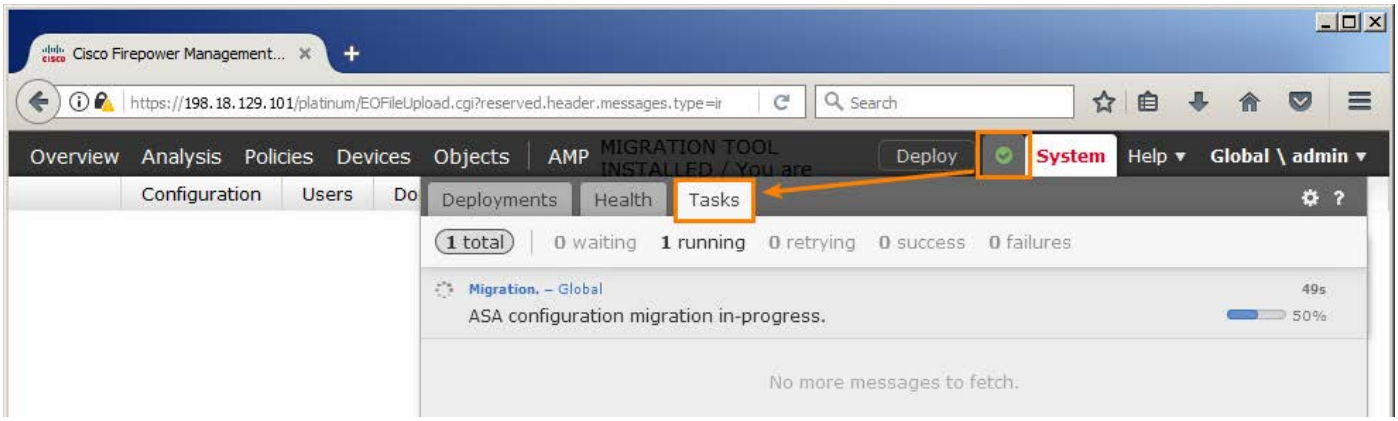
5. Now you will need to select the options you wish to use for the importation. For the purposes of this demo I've selected to use the **Prefilter Policy** and the **FastPath** action for any Access Control List statements with the Permit option. Select the combination that you prefer but take note that the further steps in this demonstration might differ from what you need if you choose a different combination. Click **OK** to continue.

Figure 5. Choose Migration Path and Start the Migration Process

NOTE: Do not click anywhere until the FMC notifies you to view the Task tab in Message Center. I've see this cause the import/conversion to fail.

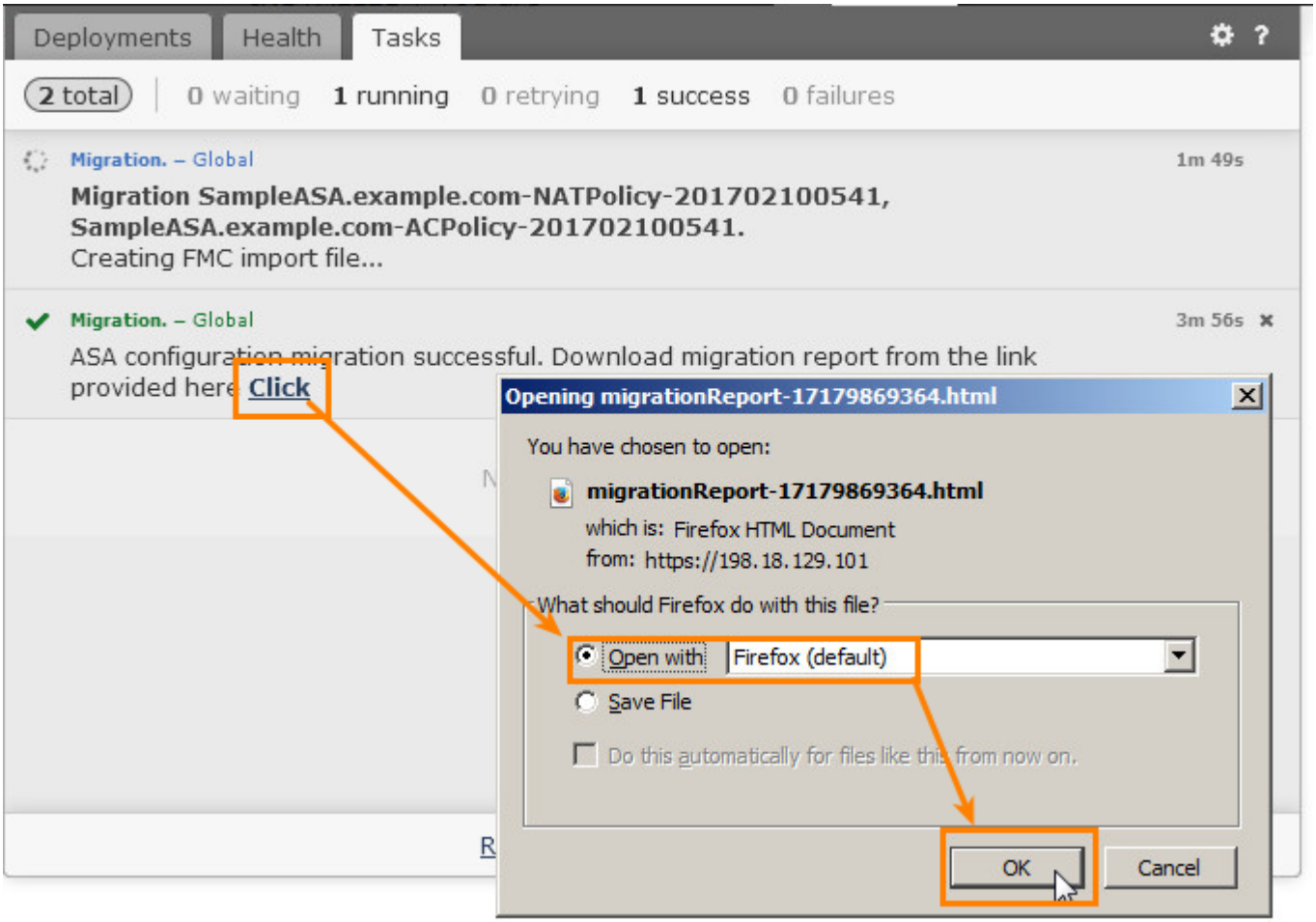
6. Under the Message Center's Tasks tab, you can watch the progression of the conversion. Navigate to the **Message Center's Tasks tab**.

Figure 6. Commence Navigation



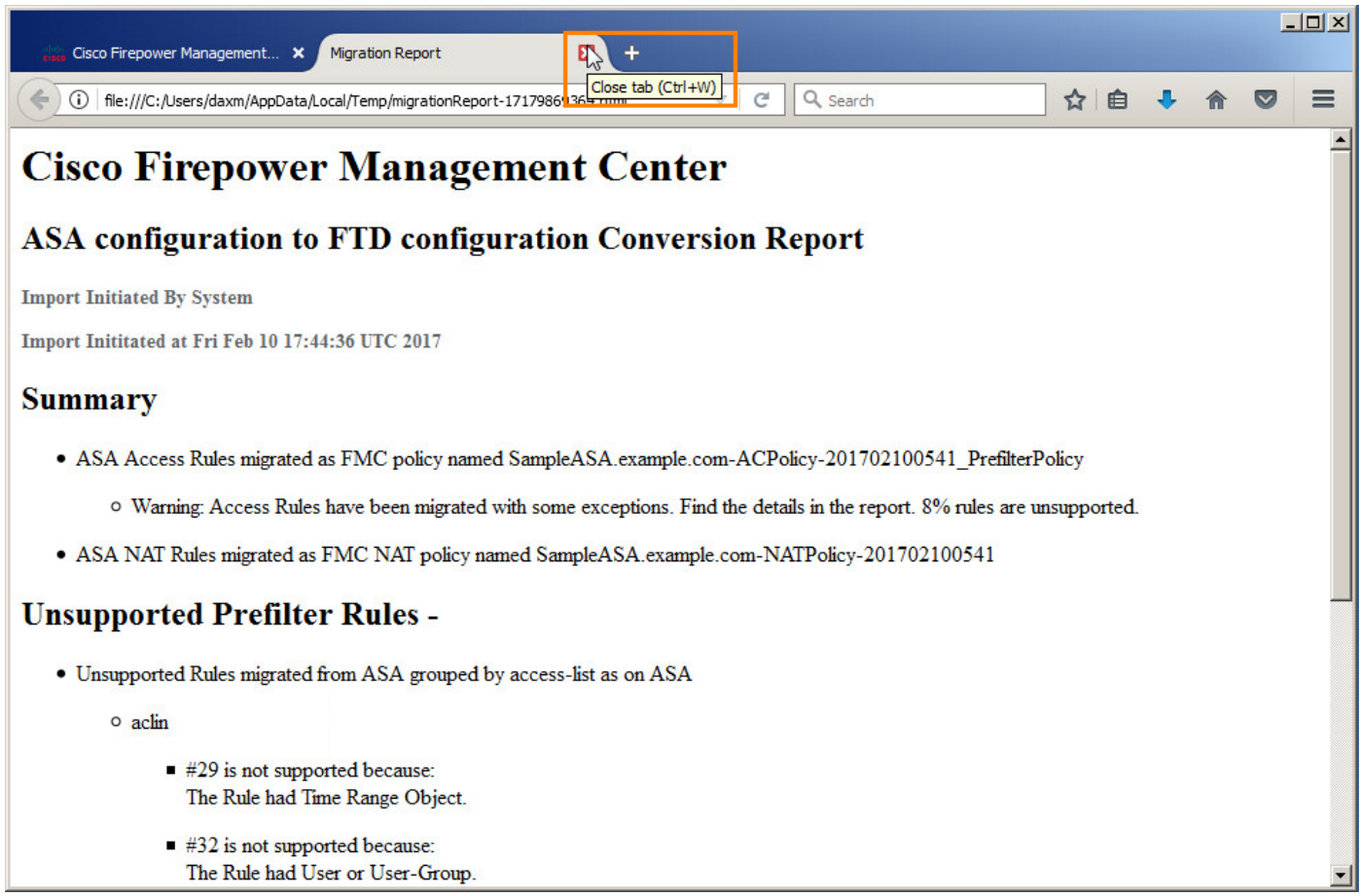
7. Once the FMC has parsed the whole ASA configuration file it will generate a report on what will or will not be converted. A link to this report will show up in the Task tab. Click on the **Click** link to download or view this report. I selected to **Open in Firefox** to view the report immediately.

Figure 7. Navigate to Message Center's Tasks tab



8. **Close** the report tab once you are done reviewing it.

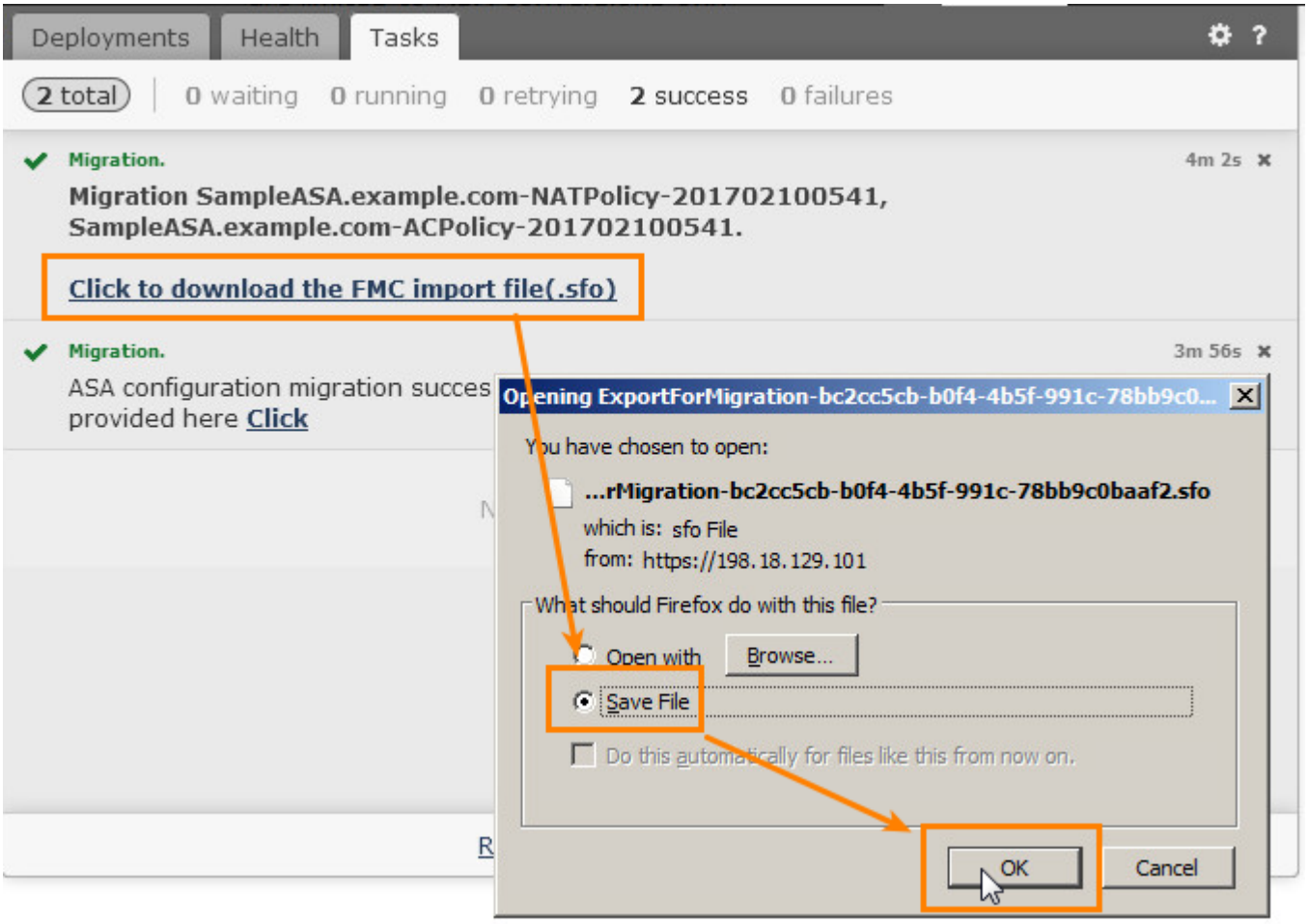
Figure 8. Close Browser Tab



NOTE: The conversion process can take some time, depending on the size of the ASA configuration file. Expect at least a 5 minute wait for the conversion.

9. Once the conversion is done, you will be given a link to download the converted file (in .sfo format). Click on the **Click to download the FMC import file(.sfo)** link to download the converted file. **Save** the file to your computer.

Figure 9. Download SFO File



NOTE: Multiple ASA configuration files can be converted using the same Migration FMC. There is no need to rebuild this server after each conversion.

Scenario Summary

This scenario translated the supported commands from an ASA configuration file into a format the Production FMC supports.

Scenario 4. Upload Converted File to FMC

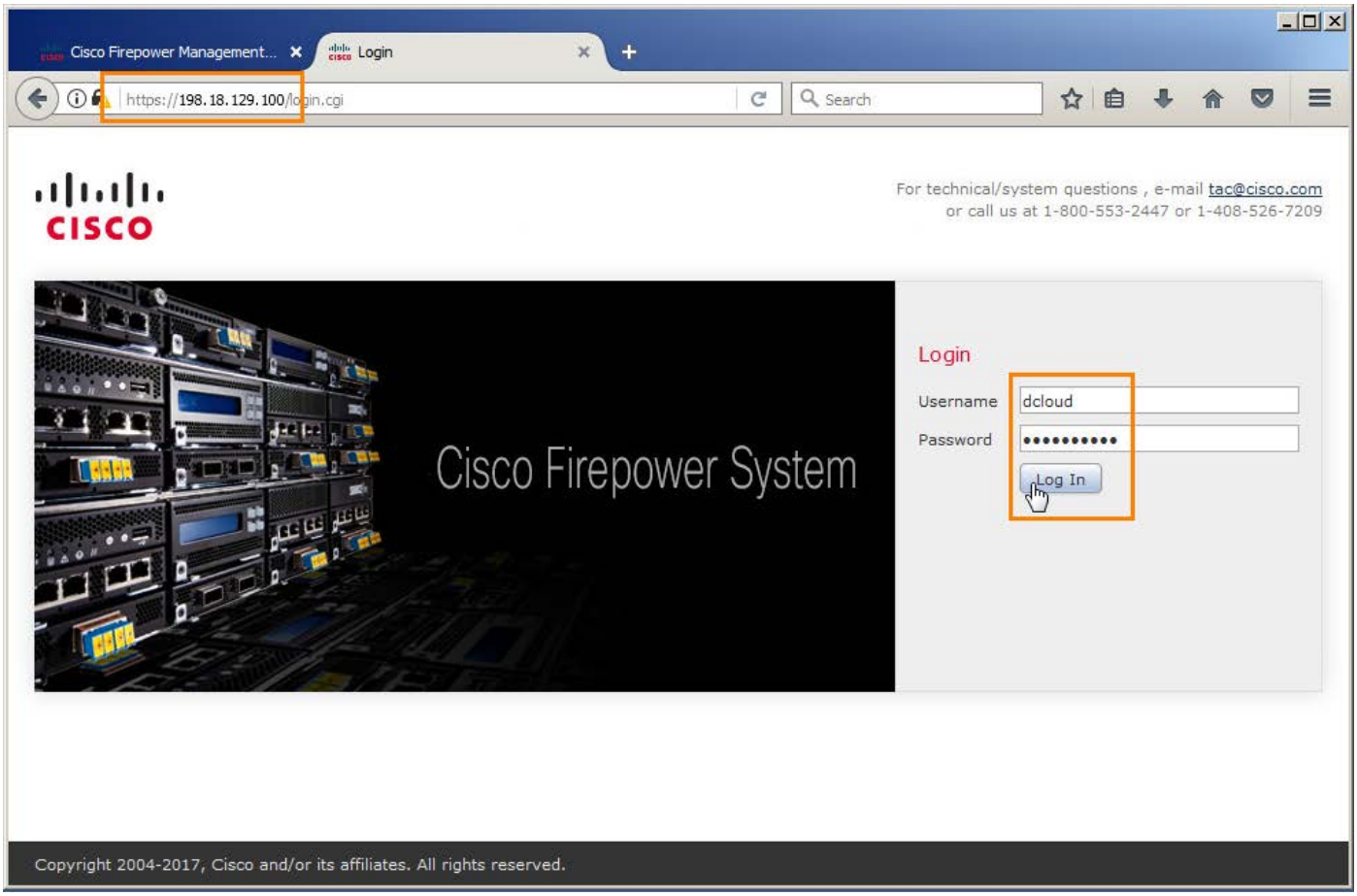
Scenario Description

Now that the Migration FMC has created the SFO file, it is time to upload it into the Production FMC. Once the upload is complete, we will review these new policies.

Section 1: Upload SFO File to Production FMC

1. Now that we have the converted file, it is time to import into the “production” FMC. Open a new tab in your browser and navigate to **https://198.18.129.100**. Log in as **dcloud/C1sco12345**.

Figure 1. Log into Production FMC



NOTE: This FMC is a “fresh” install with only minimal policies configured. This demo does not cover the issue of importing a file into an FMC that already has a complex set of policies configured. This may create conflicts that need resolved.

Here is what was done to this “freshly built” FMC:

Added “Sample Policy” Access Control Policy to be used as a placeholder for the managed FTD device.

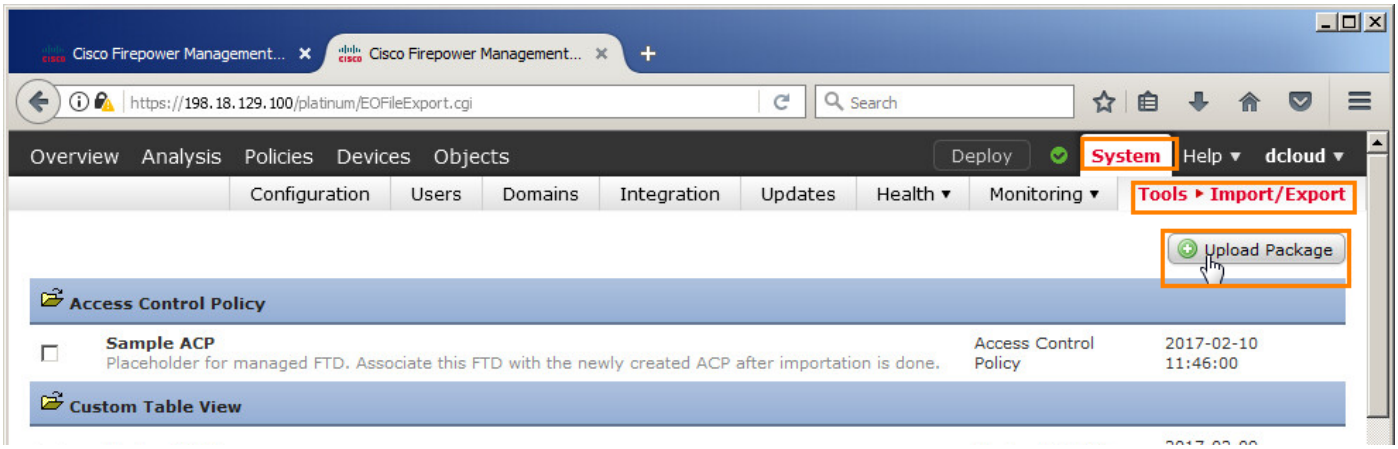
Added three Interface Groups (intgrpR_IN, intgrpR_OUT, intgrpR_DMZ) and associated three of the FTD’s interfaces with these groups.

Added three Security Zones (szR_IN, szR_OUT, szR_DMZ) and associated three of the FTD’s interfaces with these groups.

These modifications were done to easy the importation process. Feel free to create your own though.

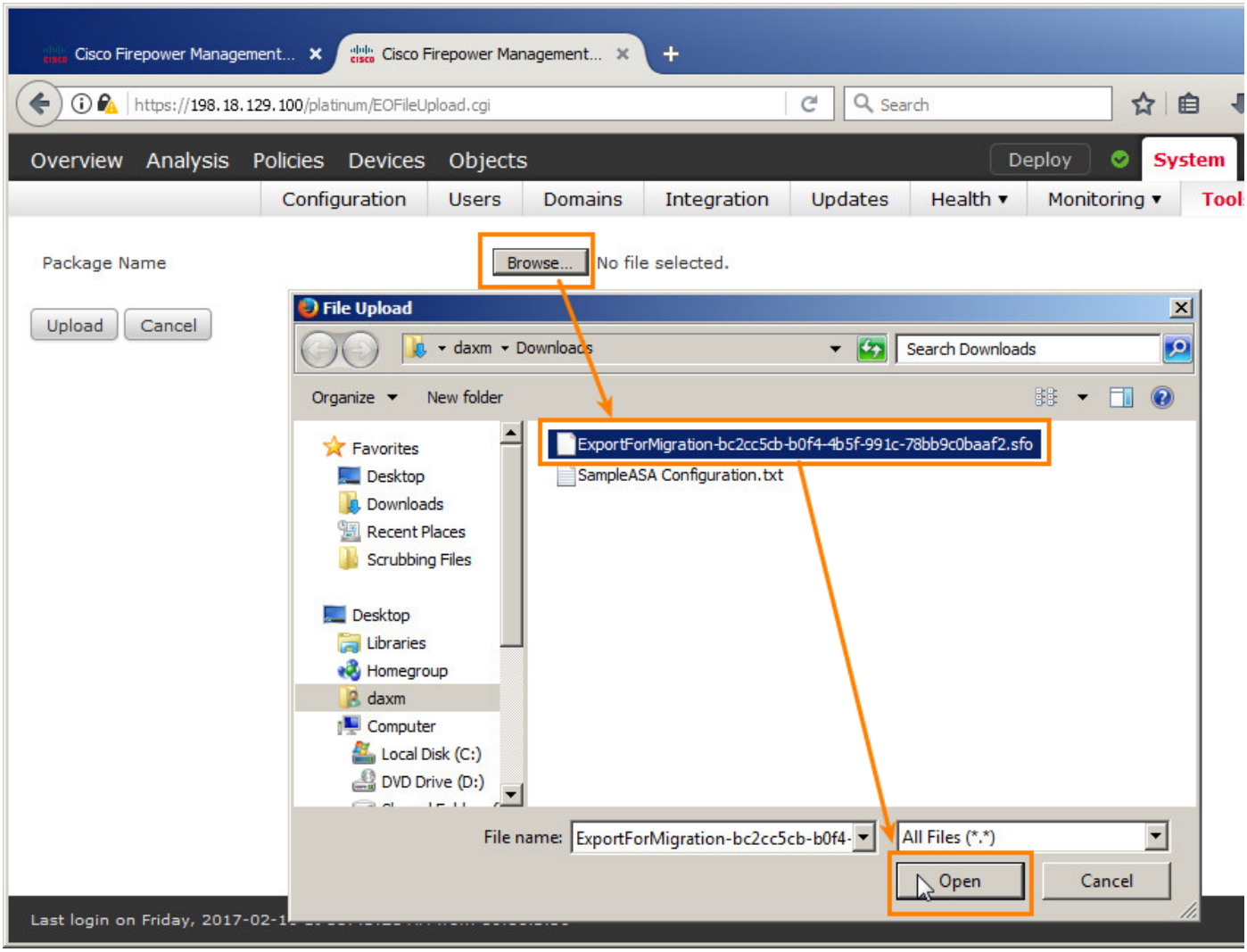
2. Navigate to **System > Tools > Import/Export** and click **Upload Package**.

Figure 2. Prepare to Upload SFO File



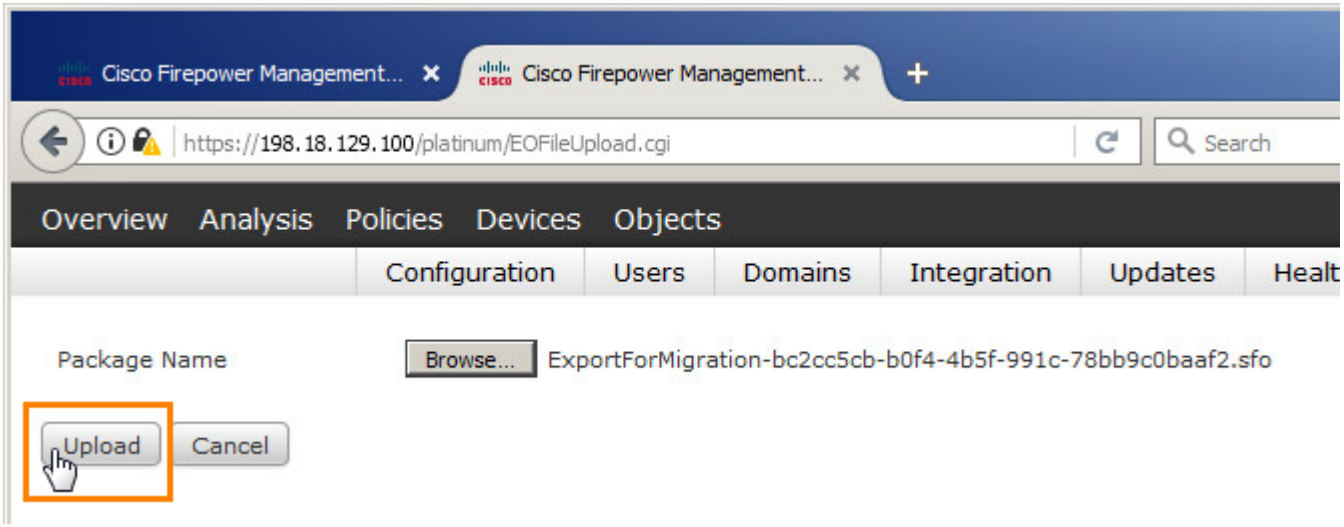
3. Click **Browse…** and **select** the converted configuration file. Click **Open**.

Figure 3. Select File for Import



4. Click **Upload** to load the file into the FMC.

Figure 4. Upload the File

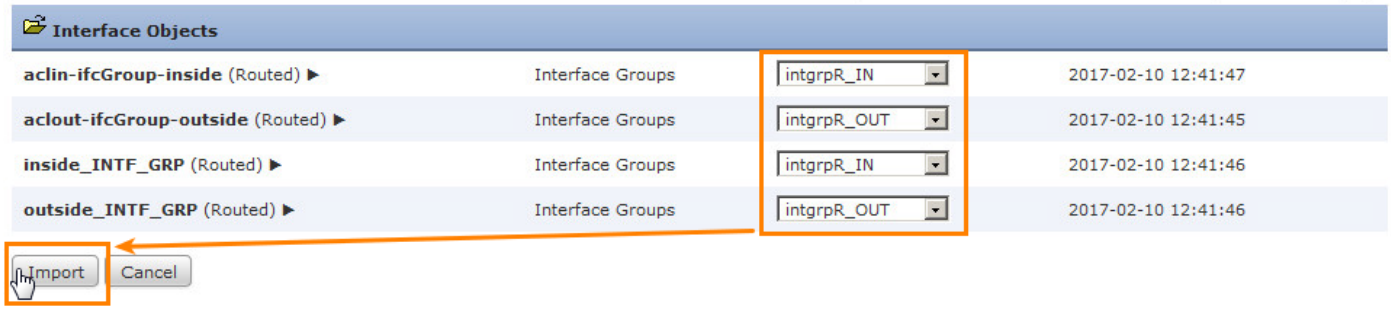


5. The policies should be already selected for you. If not, select the policies you wish to import. Click **Import** to continue.

Figure 5. Choose Policies

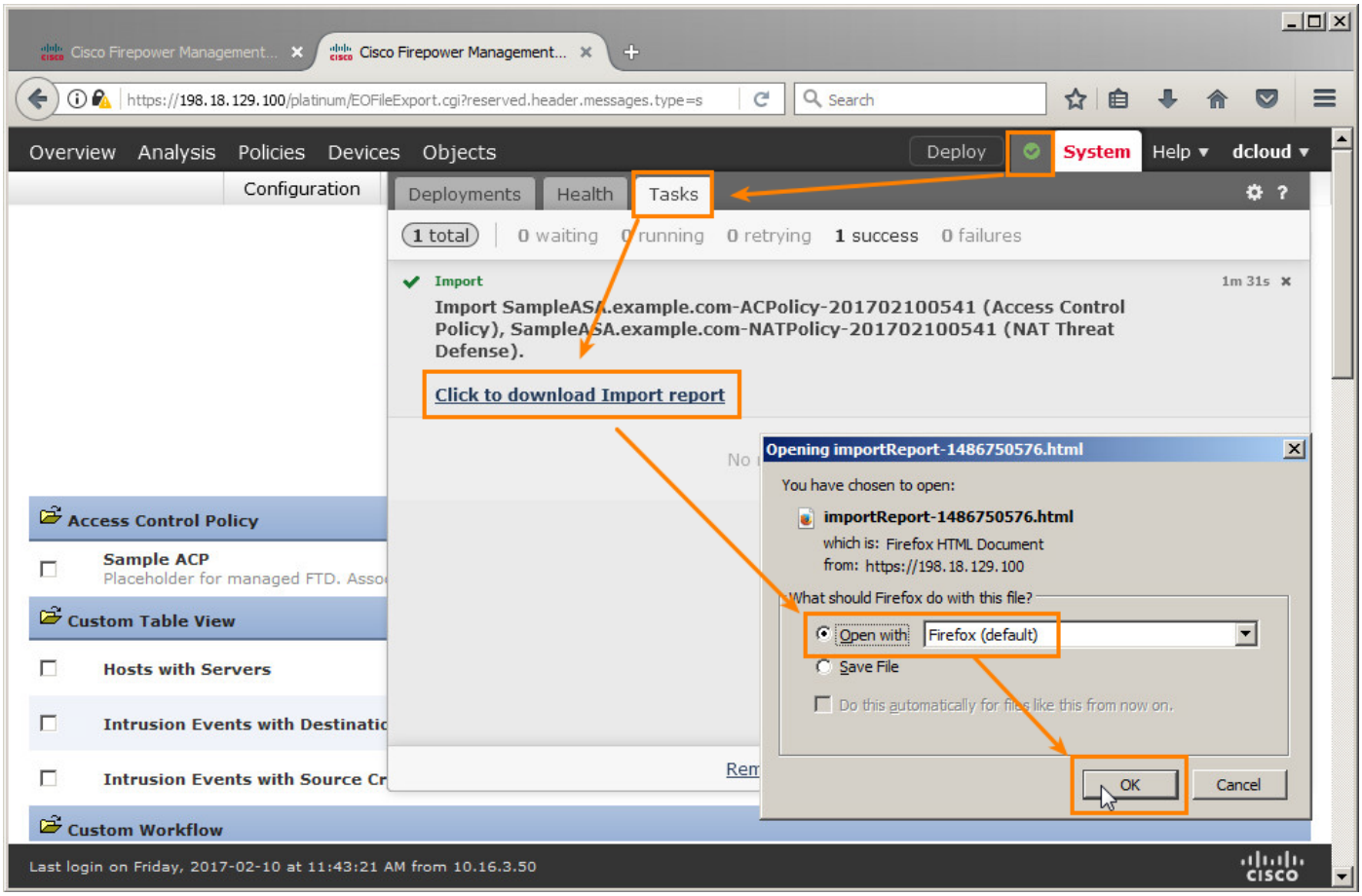
6. Map the “to be imported” objects to either new objects or to something already configured. I used the **intgrpR_IN** for the **aclin-ifcGroup-inside** and **inside_INTF_GRP** importing objects and **intgrpR_OUT** for the **aclout-ifcGroup-outside** and **outside_INTF_GRP** importing objects. Click **Import** when done.

Figure 6. Associate Import Objects to FMC Objects



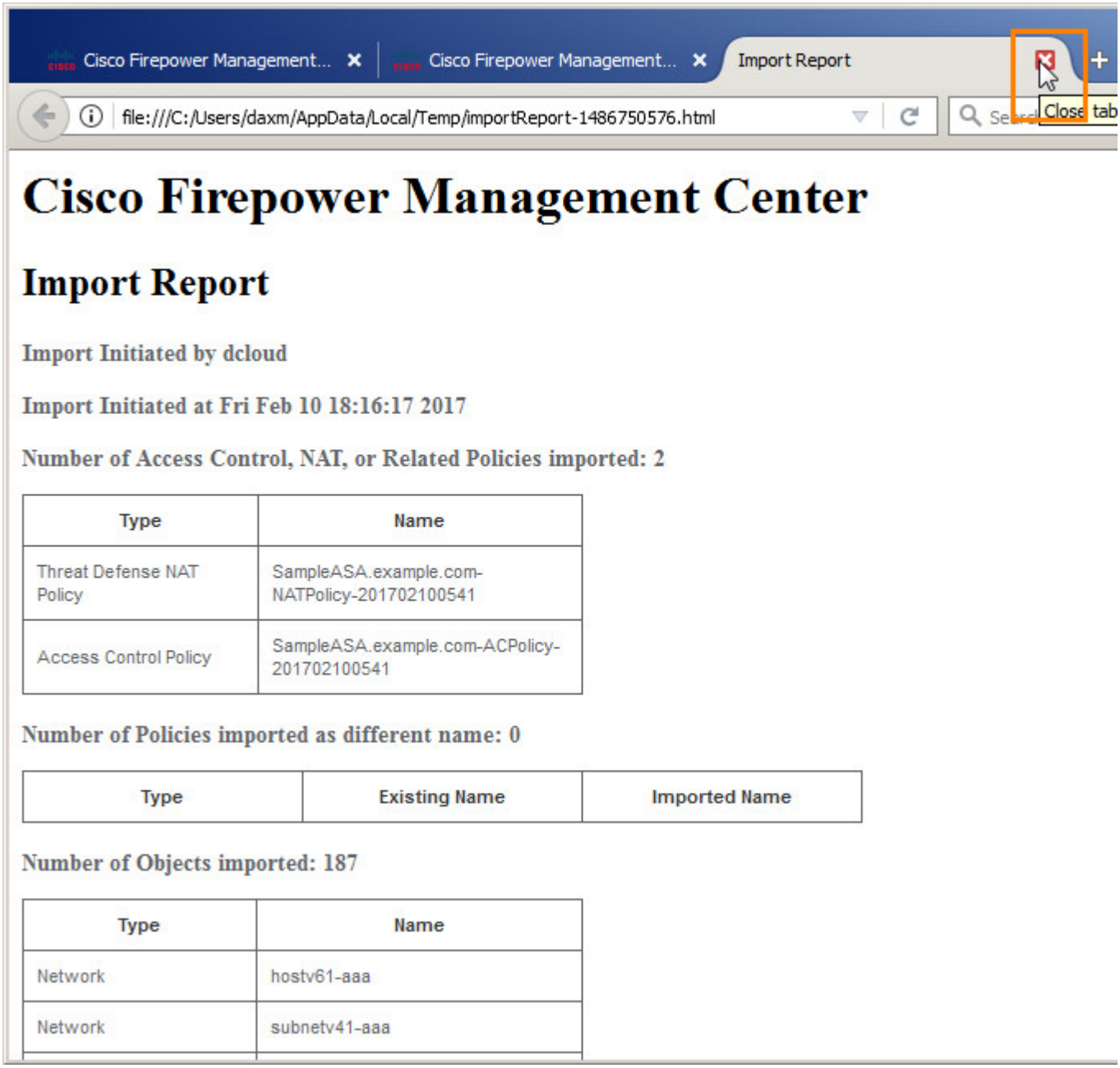
7. The FMC will now import the SFO file and make the new needed policies. This process can take some time. Watch the Message Center's Tasks tab for progress. Once the import is complete, a report will be available. **Click the Click to download Import report** link to view the report. When prompted select **"Open with Firefox"** and then click **OK** to view the report.

Figure 7. Open the Import Report



8. Review the import report and then **close the tab**.

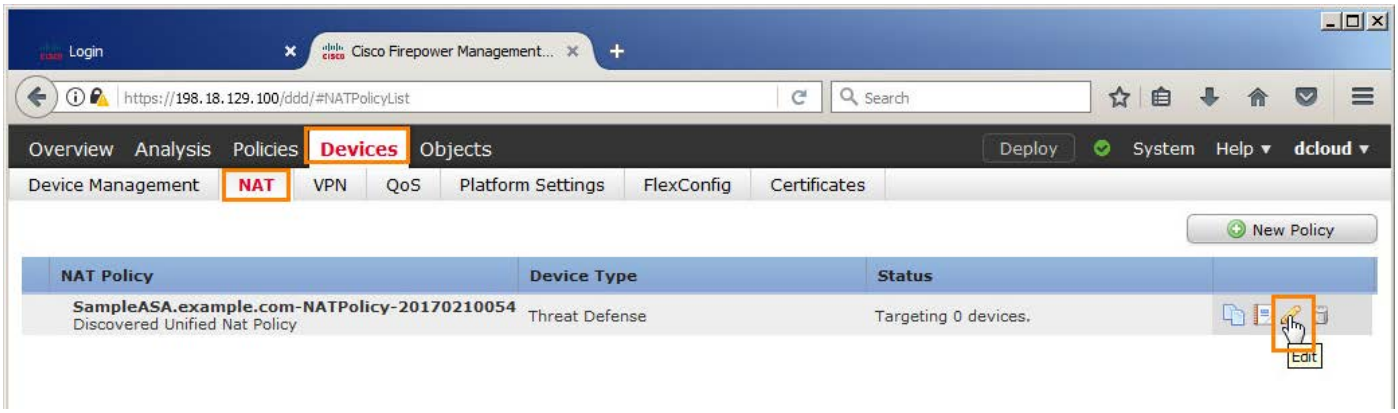
Figure 8. Review Import Report



Section 2: Review Newly Created Policies

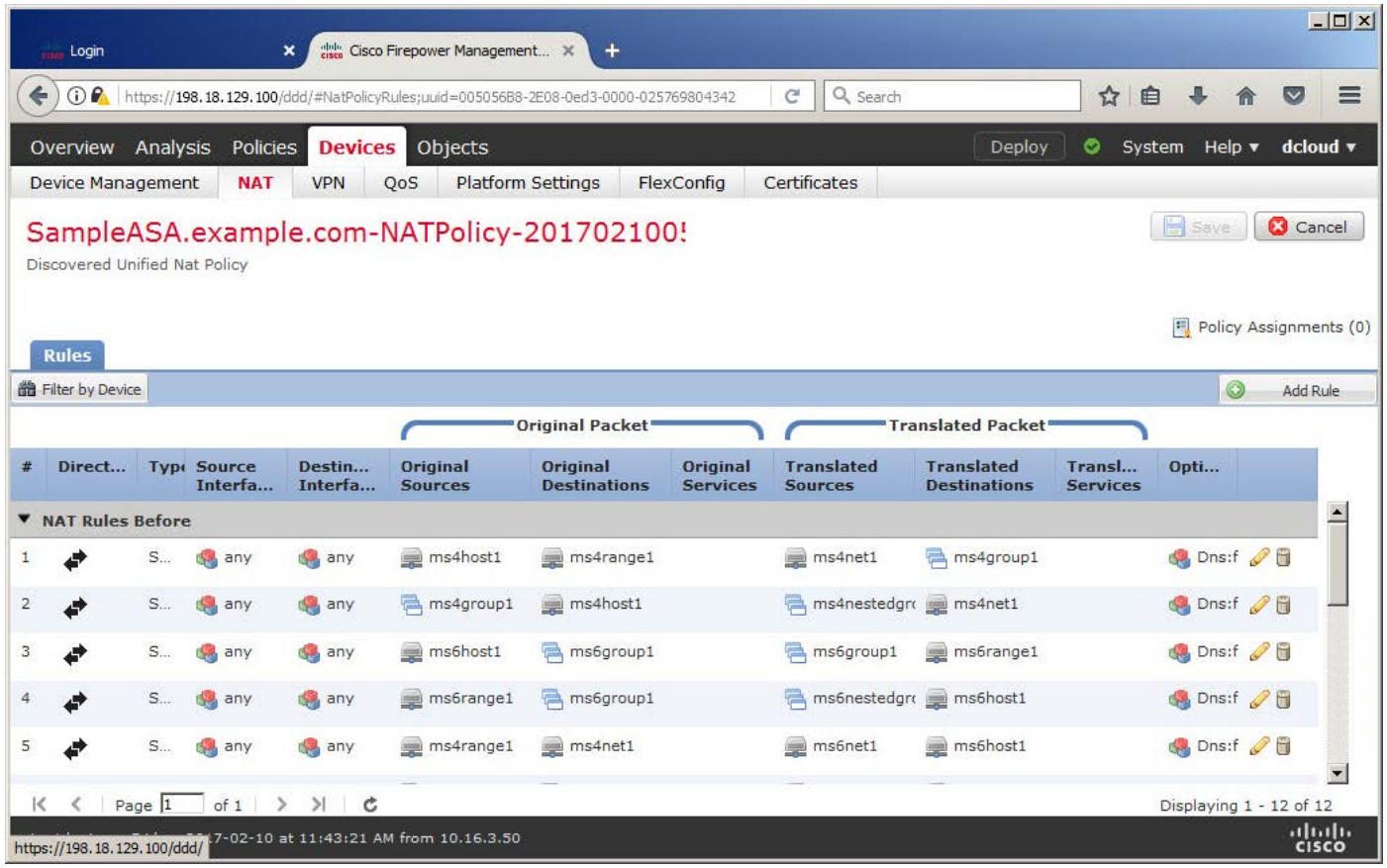
9. Now that the ASA configuration is imported review the imported policies. Navigate to **Devices > NAT** to view the newly imported NAT policy. Click the **Pencil icon** for this NAT policy to view this policy's rules.

Figure 9. Navigate to NAT



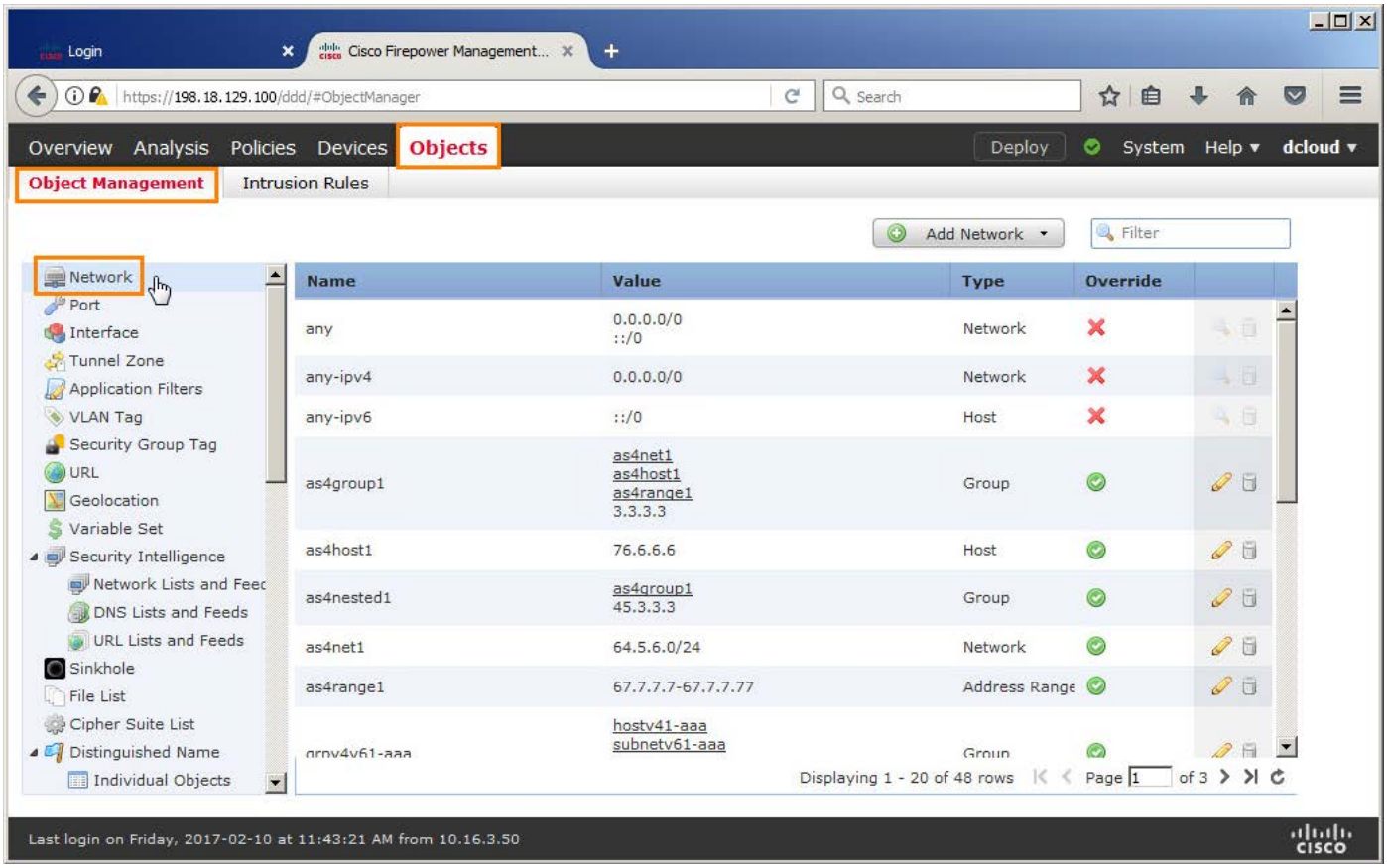
10. Browse the NAT rules. The ASA Twice NAT rules are the Manual NAT rules. The ASA Object NAT rules are the Auto NAT rules.

Figure 10. View NAT Rules



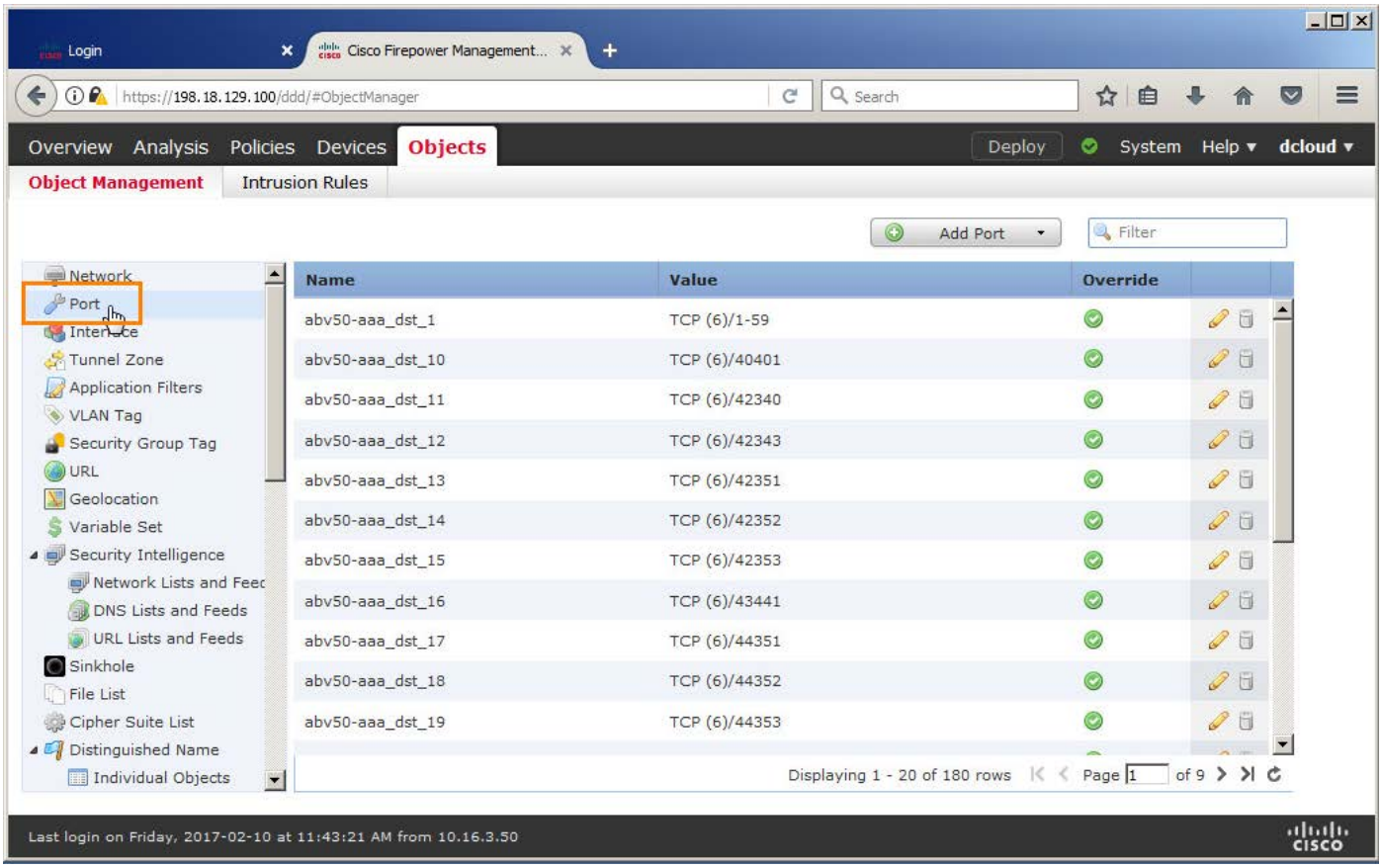
11. Navigate to **Objects > Object Management**. Click on **Network** from the list of options. Any imported Network Objects will be listed here.

Figure 11. View the Network Objects



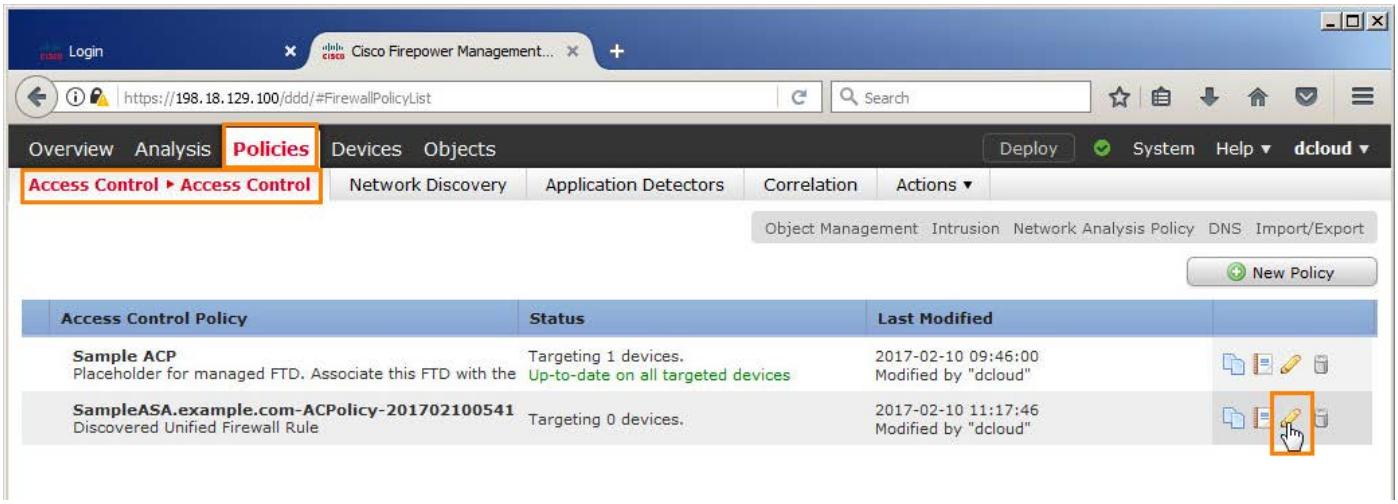
12. Click on the **Port** option to view imported Port Objects.

Figure 12. View Port Objects



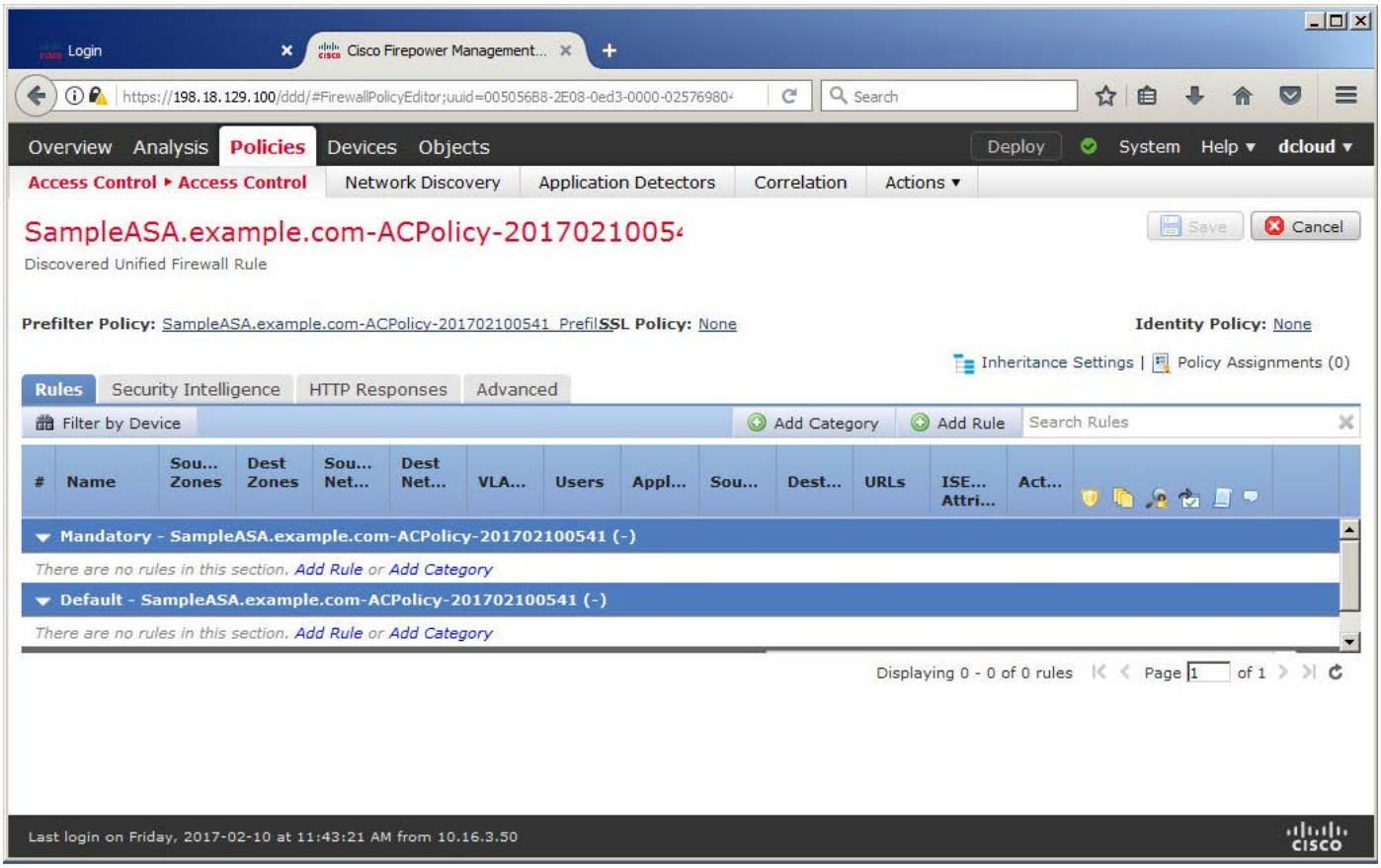
13. Navigate to **Policies > Access Control > Access Control** to view the newly created Access Control Policy. Click the **Pencil icon** for the created Access Control Policy to view any rules that were created.

Figure 13. View Access Control Policies



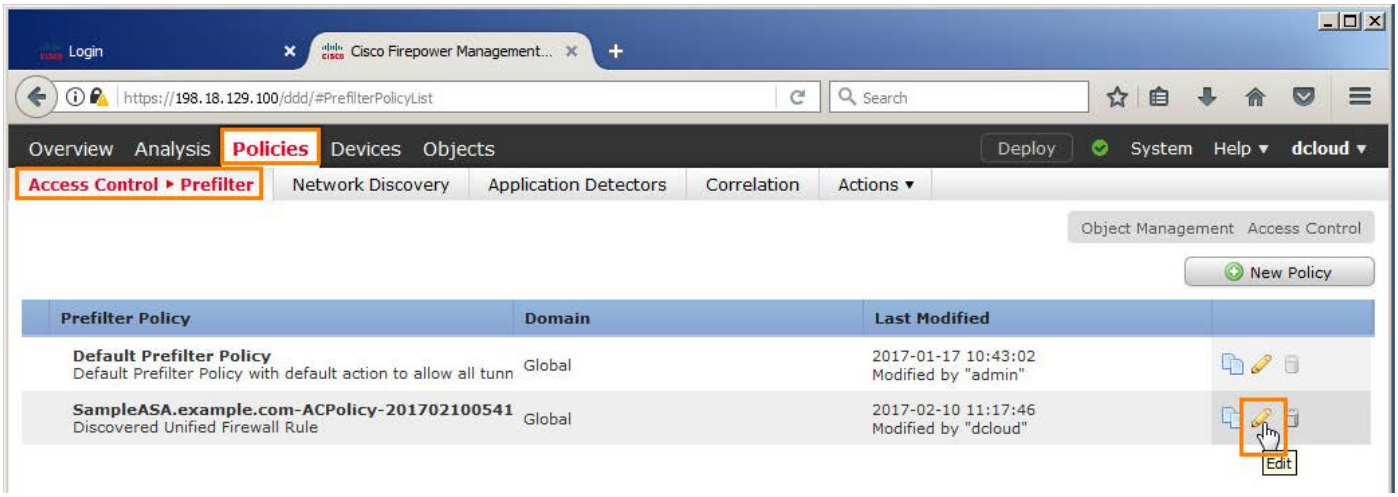
14. Since I choose to import the ASA Access Control Lists as PreFilter rules no rules will be shown here. However, note that the Prefilter Policy is set to a non-Default policy.

Figure 14. View ACP Rules and Settings



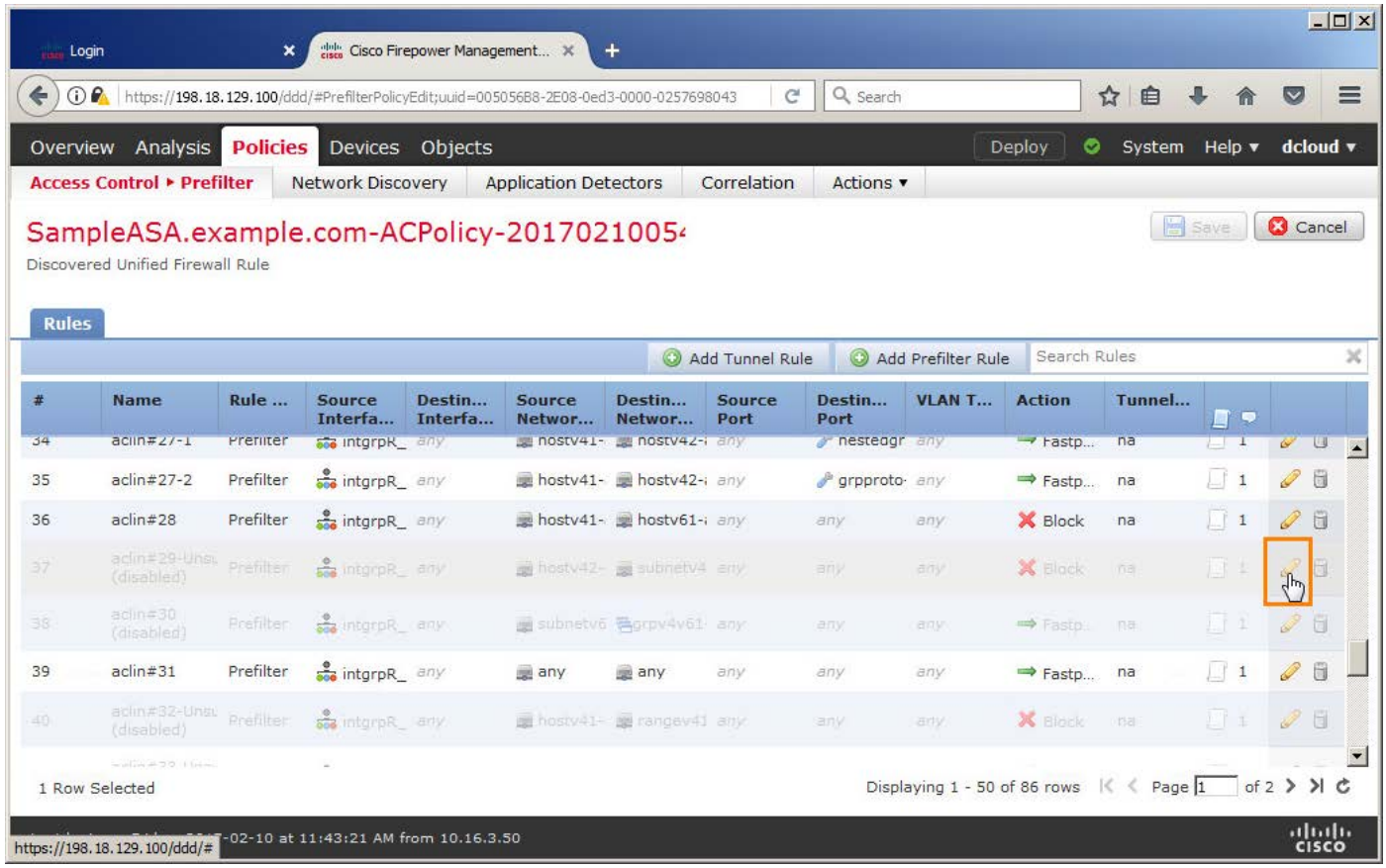
15. Navigate to **Policies > Access Control > Prefilter**. Since I choose to import the ASA Access Control Lists as Prefilter rules a new Prefilter Policy was created. Click the **Pencil icon** for this policy to view the rules.

Figure 15. Navigate to and Edit the Prefilter Policy



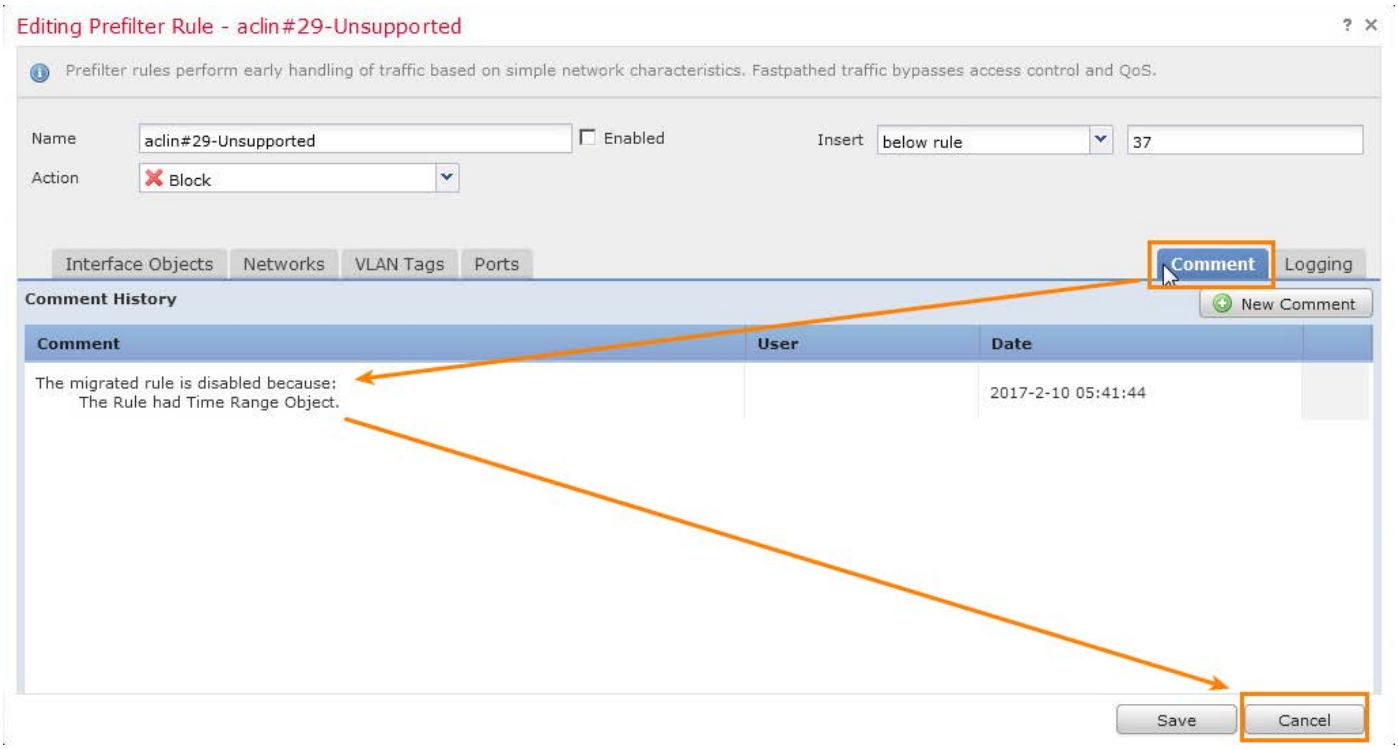
16. Scroll through the list of rules and notice the greyed out rules. These are the rules that were imported but had an issue with some unsupported feature. So, they are disabled by default. Edit one of these rules by clicking the **Pencil icon** on their row.

Figure 16. Edit a Disabled Rule



17. Click on the **Comment tab** to view a comment as to why this rule is disabled. Click **Cancel** when done viewing this rule.

Figure 17. View Disabled Reason



Scenario Summary

This scenario took the newly created SFO file and uploaded it into the Production FMC. From there, a quick review of the imported policies showed what was or was not imported.

Scenario 5. Deploy Configuration to FTD

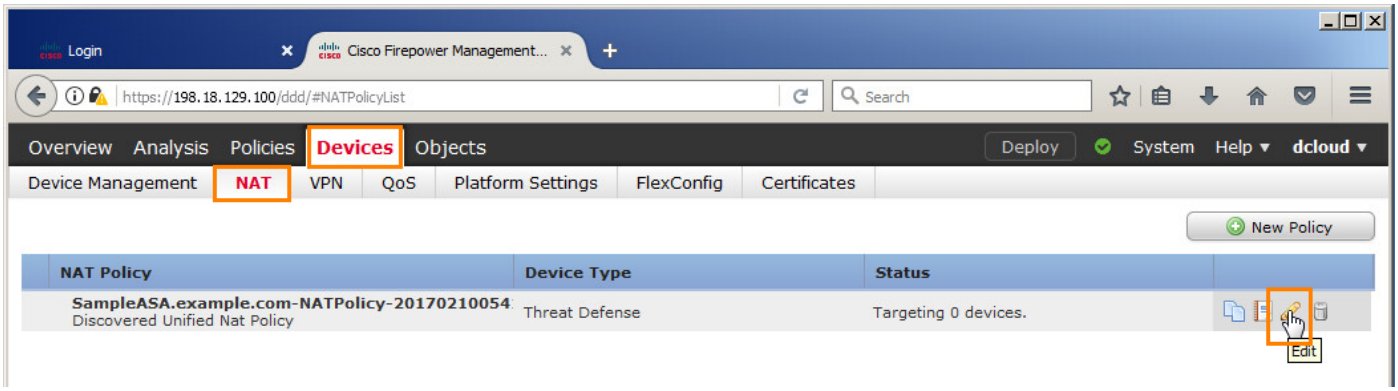
Scenario Description

This scenario will deploy the new policies to the provided FTD device. Bear in mind that this is for testing purposed only. We will NOT be able to send traffic through this FTD device. The goal is just to prove we can push the policies to an FTD device.

Section 1: Associate FTD with New Policies

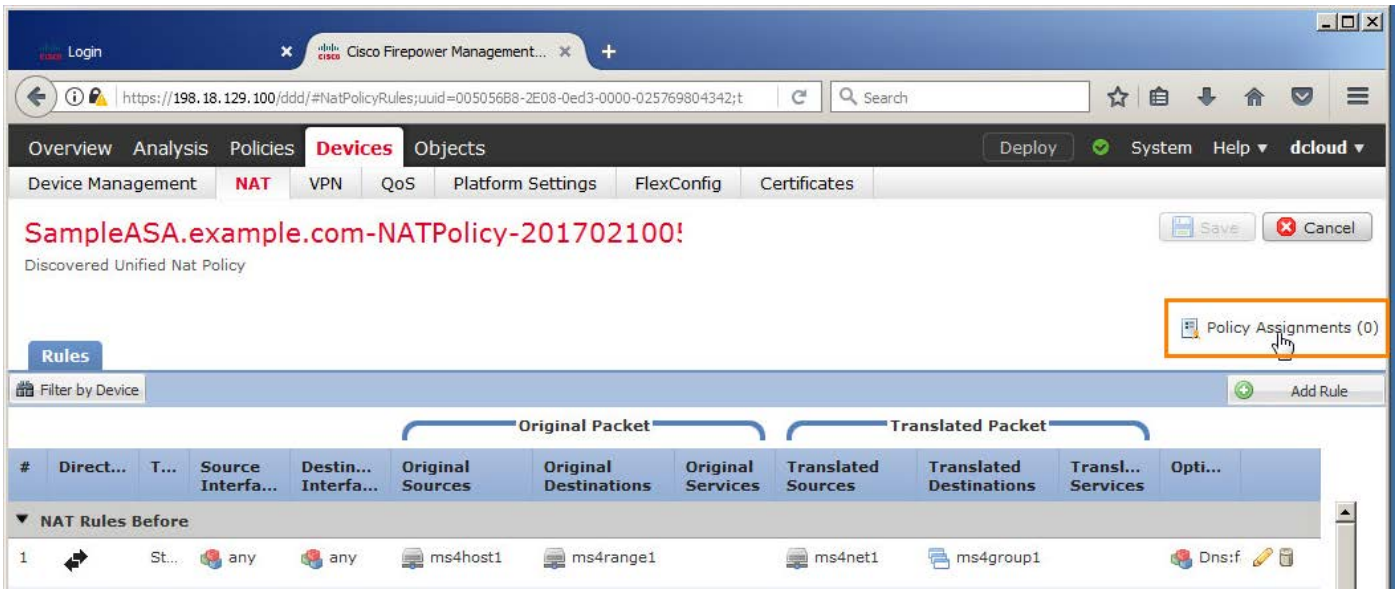
1. Since the import created new NAT, ACP, and Prefilter policies the FTD device needs to be moved from its currently associated policies to the new ones. Bear in mind that the current set up only had a Sample ACP just to “hold” the FTD until the new policies were created. Click **Devices > NAT** and then click the **Pencil icon** to edit the NAT policy.

Figure 1. Edit NAT Policy



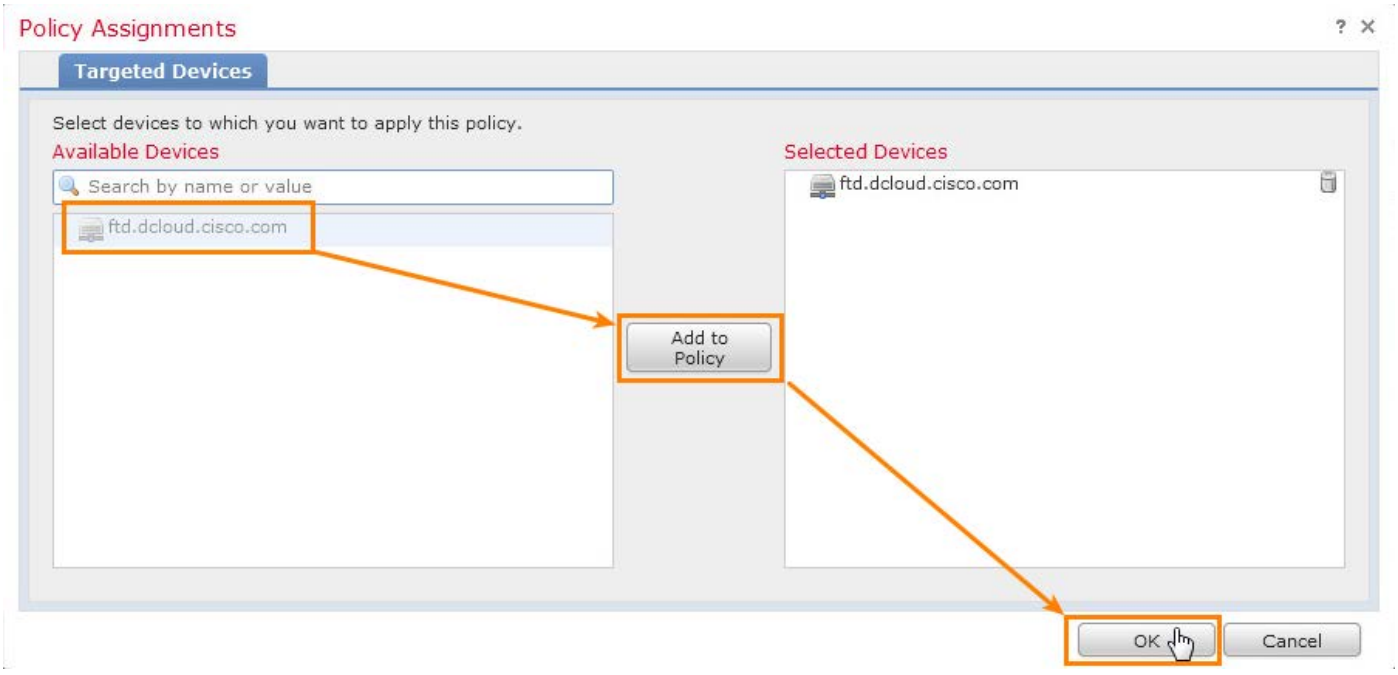
2. Click the **Policy Assignments** link.

Figure 2. Policy Assignments



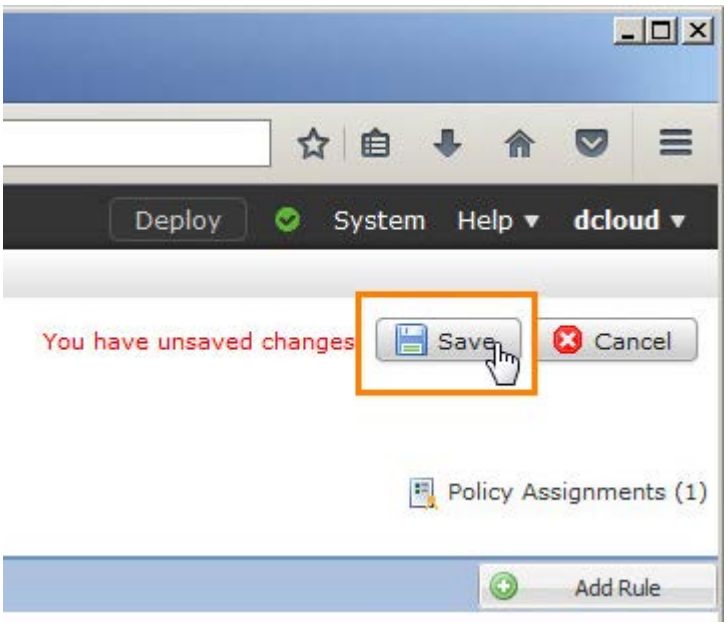
3. Select the **ftd.dcloud.cisco.com** device, click **Add to Policy**, and then click **OK**.

Figure 3. Add to Policy



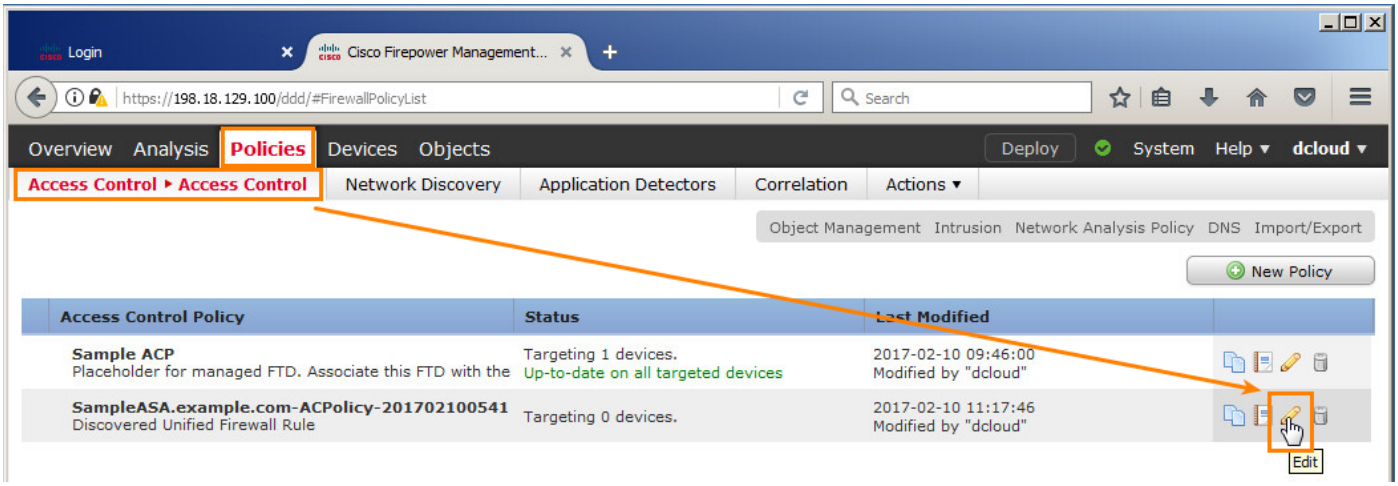
4. Click **Save** to commit these changes.

Figure 4. Save Changes



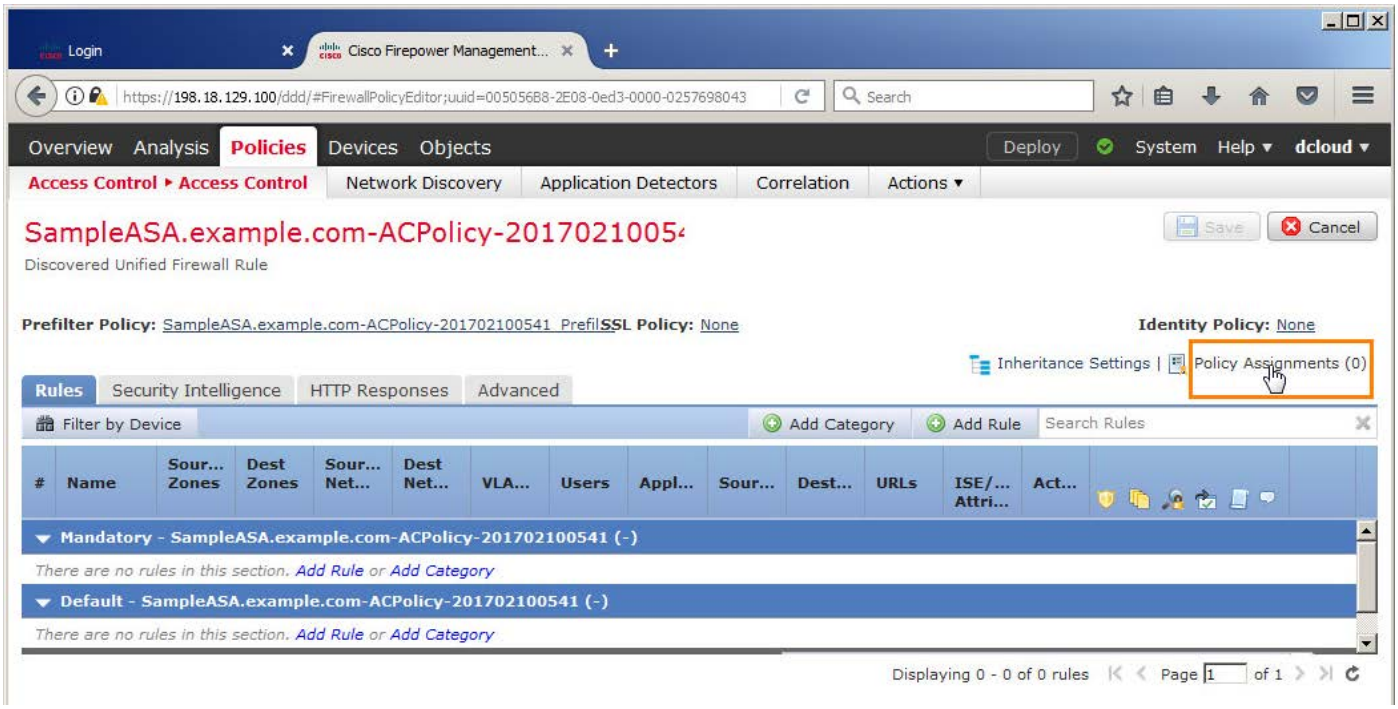
5. Navigate to **Policies > Access Control > Access Control** and **Edit** the new policy.

Figure 5. Edit ACP



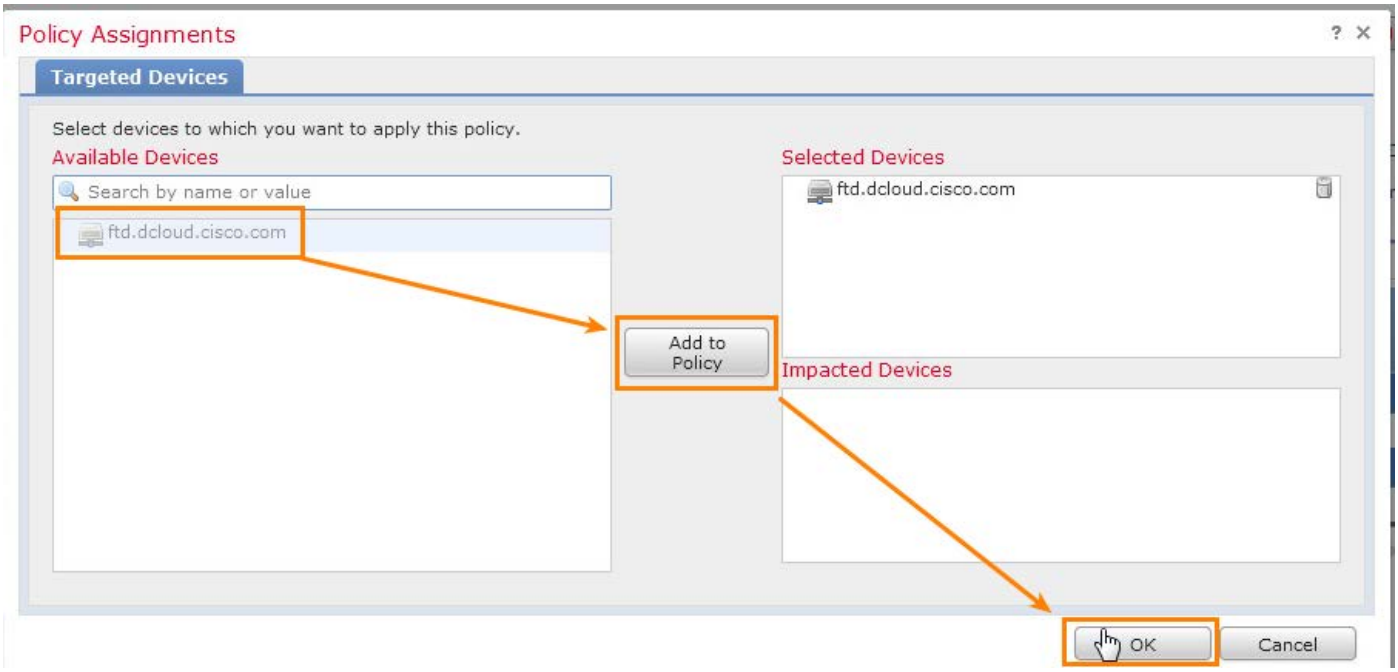
6. Click the **Policy Assignments** link.

Figure 6. Policy Assignments



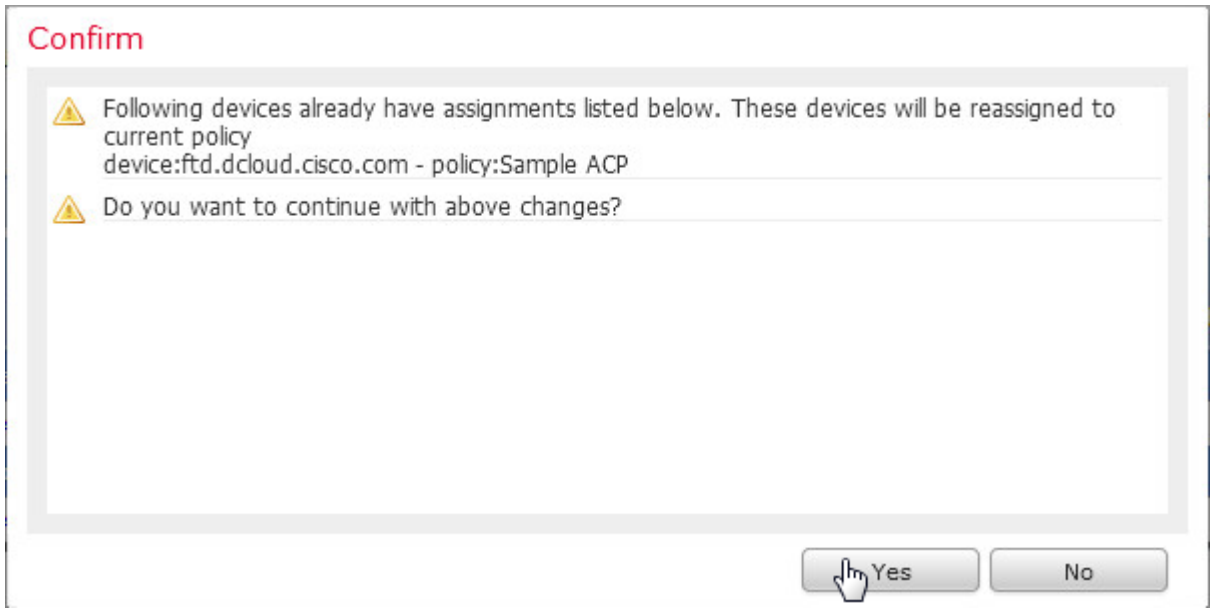
7. Select the **ftd.dcloud.cisco.com** device, click **Add to Policy**, and then click **OK**.

Figure 7. Add to Policy



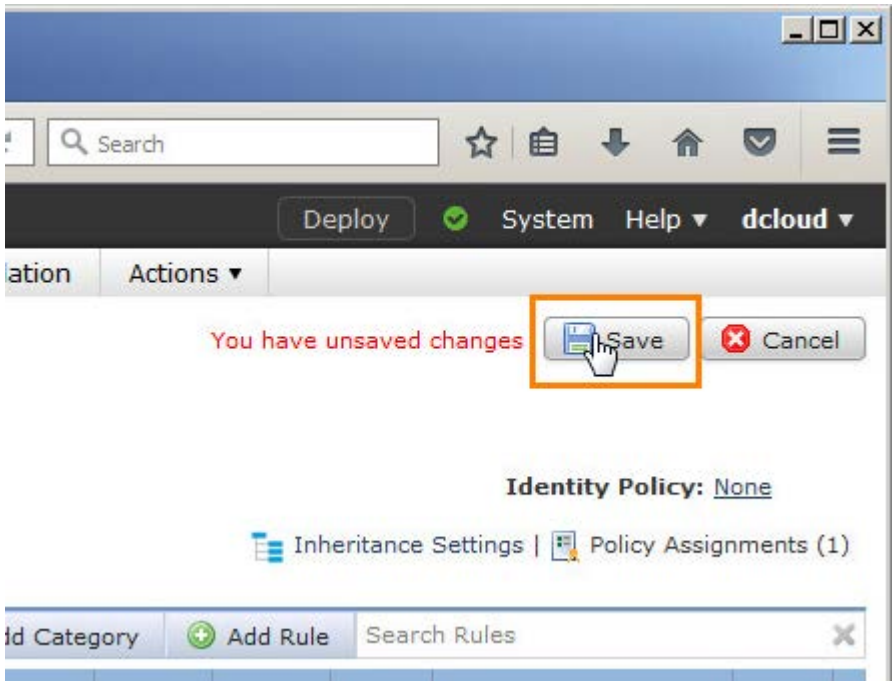
8. Since this FTD is already assigned to another ACP you need to confirm you want to move it. Click **Yes** to confirm.

Figure 8. Confirm Re-association



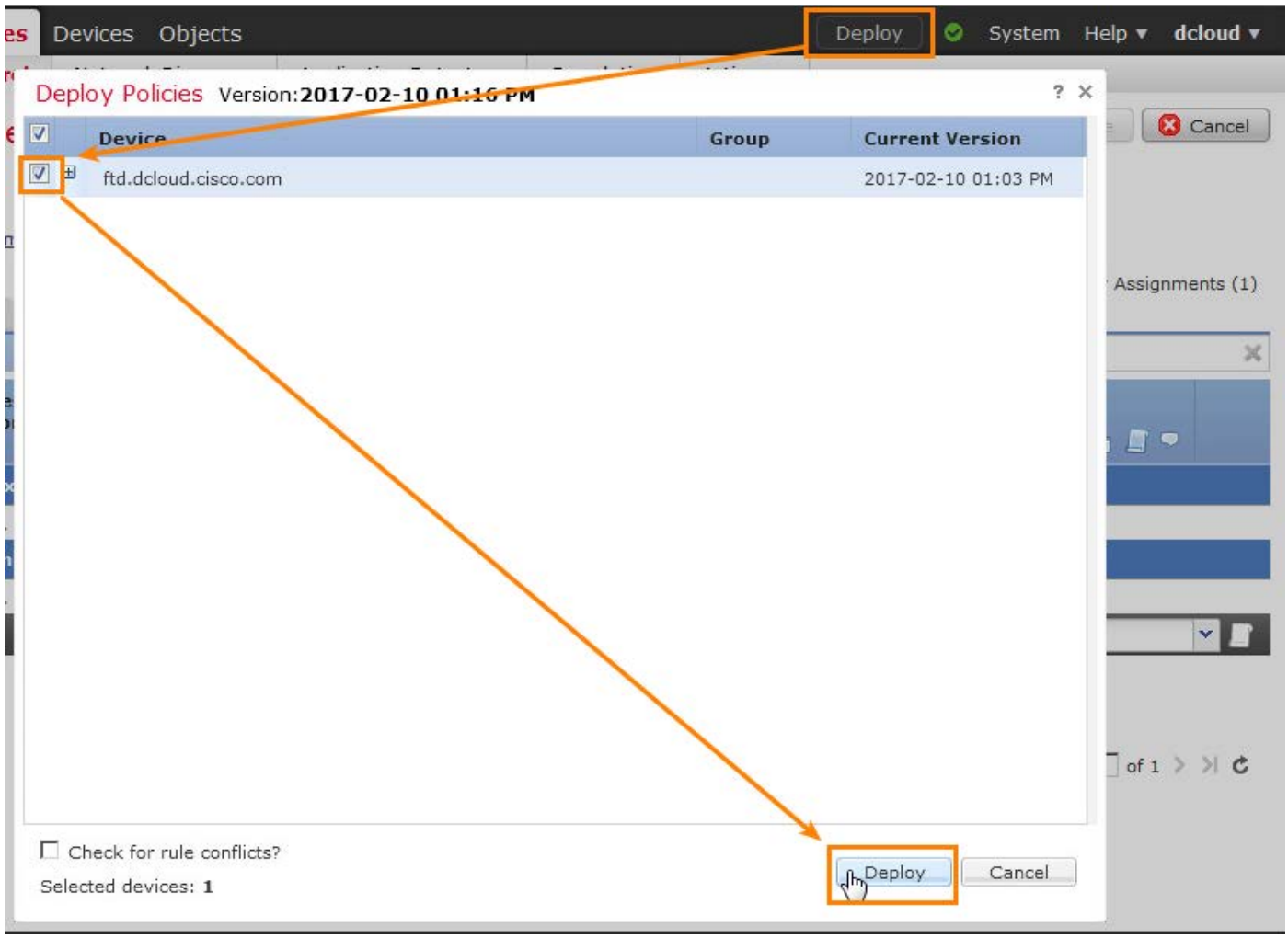
9. Click **Save** to commit these changes.

Figure 9. Save Changes



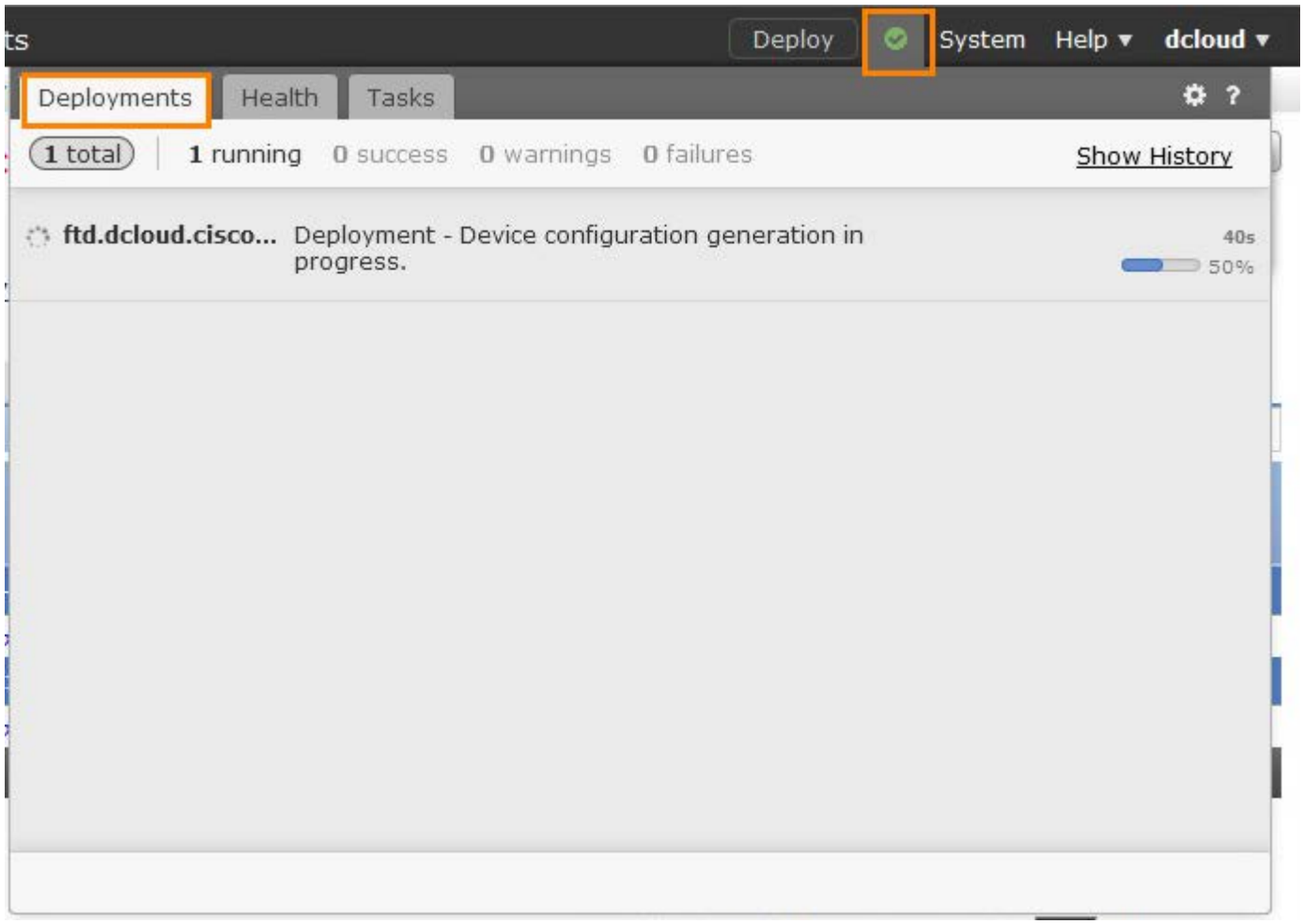
10. Finally, push these changes to the FTD. Click **Deploy**, **check the box** next to **ftd.dcloud.cisco.com** and then click **Deploy**.

Figure 10. Deploy Changes



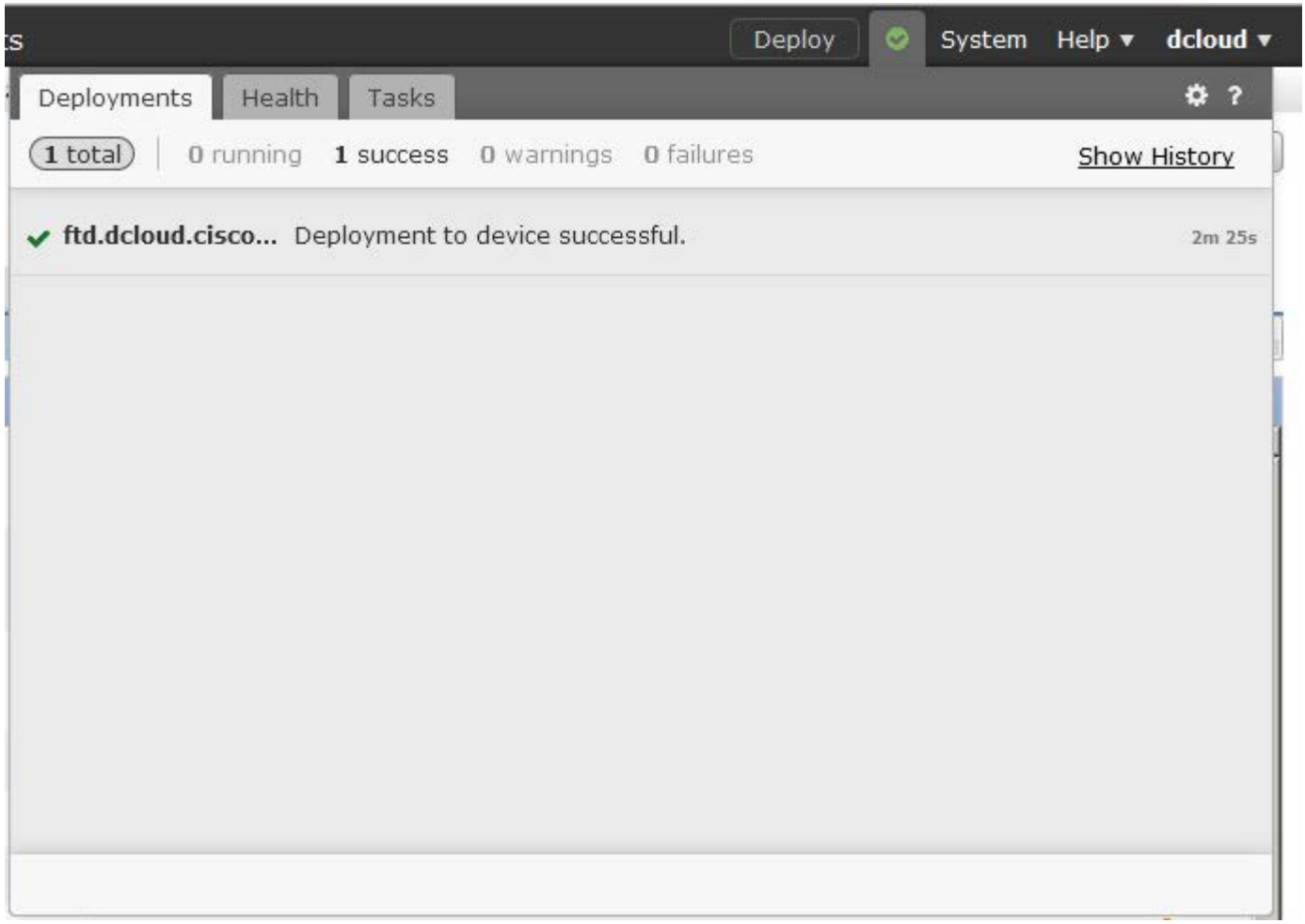
11. You can watch the progress of the deployment on the Message Center's Deployments tab.

Figure 11. View Deployment Progress



12. The Deployments tab will confirm when the configuration is complete.

Figure 12. Deployment is Complete



Scenario Summary

This scenario showed how to migrate an FTD device to the newly created policies.

Congratulations, you have completed the whole lab!!!

Appendix A. Convert Regular FMC to FMC Migration Tool

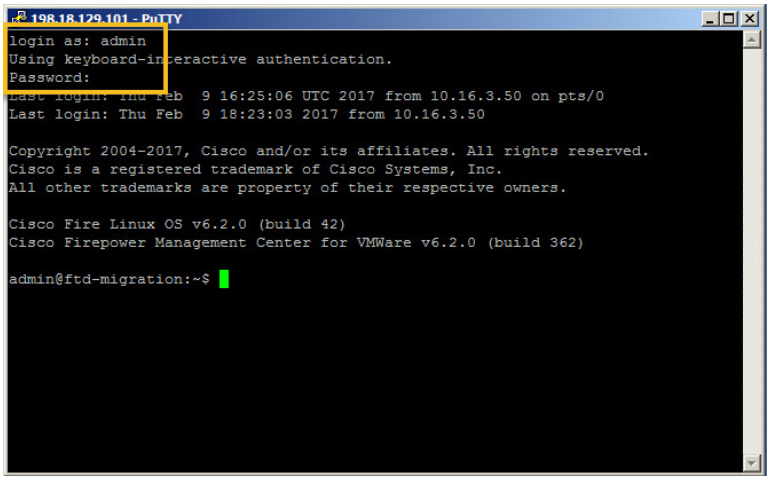
An FMC configured to convert ASA configuration files to FMC formatted files is exactly the same as a regular FMC, with one exception. There is a command that needs run on the CLI of the FMC that converts it to a “special” FMC, which is used for migration purposes only.

Here are the steps used to convert the FMC-Migration VM to that mode.

NOTE: These steps have already been done in this lab. Use the following steps just as a guideline on how you could create your own FMC Migration Tool VM.

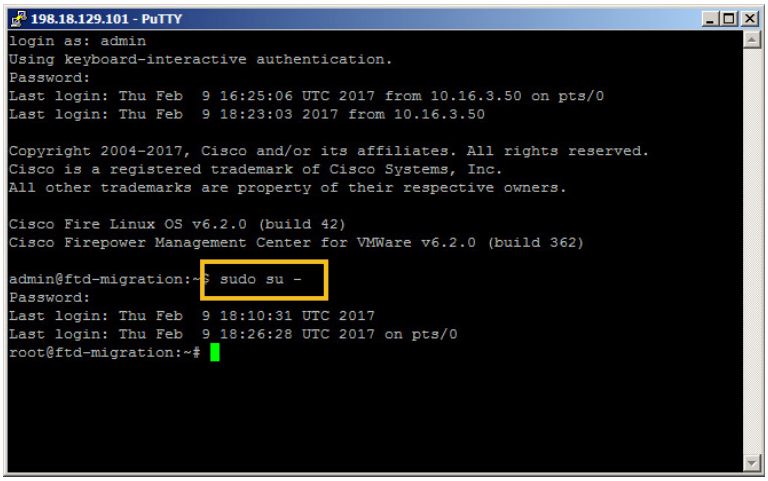
1. Deploy an FMC OVA just as you would normally. I do not show the steps for deployment here, as they are in the **Cisco Firepower Threat Defense v6.1 Basics Lab** lab guide available from dcloud.cisco.com.
2. Once the FMC has been deployed and booted up, **access the CLI**. In my case, I’ve used PuTTY to SSH to the FMC. **Log in** with an administrator level account. User **admin** with a password of **Admin123** is the default account available.

Figure 13. Log into FMC



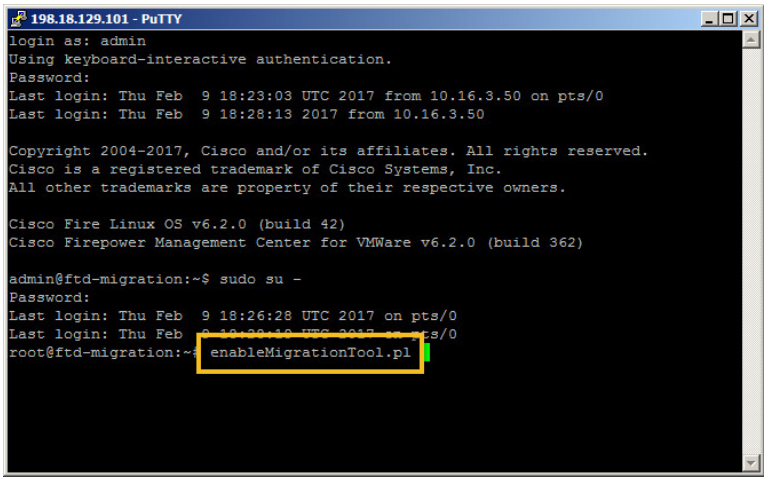
3. Issue the command **sudo su –** (a single dash) to instantiate a root level shell. Use your account's password (**Admin123**) when prompted.

Figure 14. Issue command



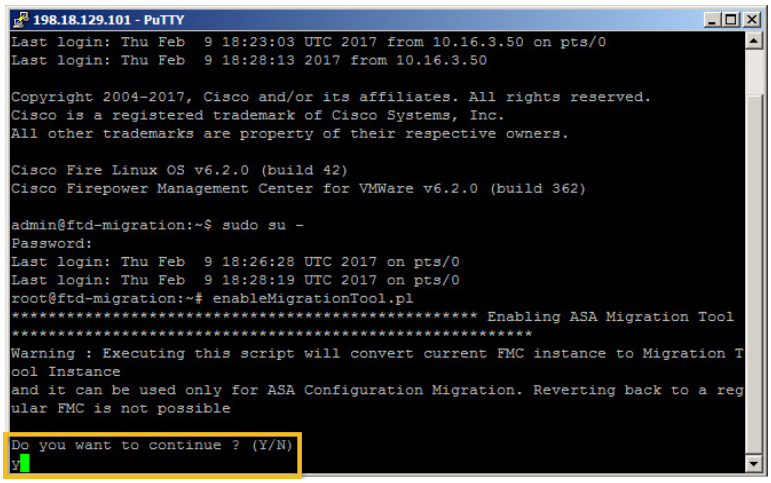
4. Issue the command **enableMigrationTool.pl**.

Figure 15. Issue command



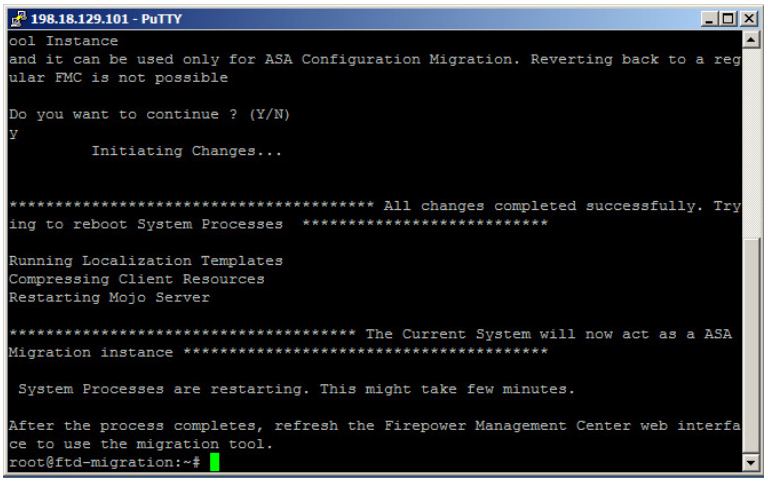
5. Type **y** when prompted to continue.

Figure 16. Issue command



6. This will change this FMC irrevocably into a special FMC whose sole purpose is to migrate ASA configurations into SFO formatted files.

Figure 17. Migration update complete



7. When the conversion is done, you'll be told to refresh the web GUI. From now on when you access this FMC you'll see an unmistakable message along the top telling you that this is a specially configure FMC.

Figure 18. Notification that this a special FMC