Cisco Firepower Threat Defense 6.4 Proof of Value v1.6

Last Updated: 12-June-2019

About This Demonstration

The Cisco dCloud is pleased to announce the Firepower Threat Defense (FTD) Proof of Value (POV). This document provides information on the POV process, training, software download, installation, licensing, initial configuration, customer deployment, risk report generation, and device sanitization.

This guide covers the most common deployment type and provides necessary information for successful POVs. For different deployment options or additional details, you can review additional POV materials here: https://communities.cisco.com/docs/DOC-65405.

This guide for the preconfigured demonstration includes:

Requirements

The table below outlines the requirements for this preconfigured demonstration.

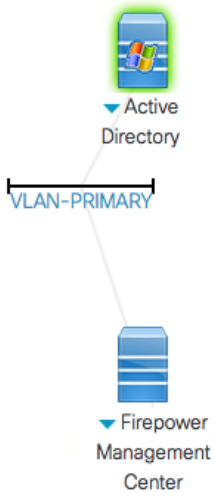
Table 1. Requirements

Required	Optional
Laptop	Cisco AnyConnect®

Topology

This content includes preconfigured users and components to illustrate the scripted scenarios and features of the solution. Most components are fully configurable with predefined administrative user accounts. You can see the IP address and user account credentials to use to access a component by clicking the component icon in the **Topology** menu of your active session and in the scenario steps that require their use.

Figure 1. dCloud Topology



Get Started

BEFORE PRESENTING

Cisco dCloud strongly recommends that you perform the tasks in this document with an active session before presenting in front of a live audience. This will allow you to become familiar with the structure of the document and content.

It may be necessary to schedule a new session after following this guide in order to reset the environment to its original configuration.

PREPARATION IS KEY TO A SUCCESSFUL PRESENTATION.

Follow the steps to schedule a session of the content and configure your presentation environment.

1. Initiate your dCloud session. [Show Me How]

NOTE: It may take up to 10 minutes for your session to become active.

2. For best performance, connect to the Active Directory with Cisco AnyConnect VPN [Show Me How] and the local RDP client on your laptop [Show Me How]
    - Active Directory: **198.18.133.36**, Username: **administrator**, Password: **C1sco12345**

NOTE: You can also connect to the active directory using the Cisco dCloud Remote Desktop client [Show Me How]. The dCloud Remote Desktop client works best for accessing an active session with minimal interaction. However, many users experience connection and performance issues with this method.

POV Process

A POV is a customer engagement that demonstrates unique business value during an on-site engagement. The POV process requires proper scoping to identify customer win criteria. Win criteria are used to focus the on-site engagements on the solution elements that are most important to a particular customer. Appendix A includes scoping questions to help establish win criteria for FTD POVs.

Most partner-executed POVs will be tactical leveraging FTD and dCloud hosted Firepower Management Centers (FMCs). All customer configurations should be implemented prior to arriving on site based on pre-defined customer evaluation data including network, management, span port, and power. A worksheet to collect this information is available in Appendix B.

The following sections cover system installation and configuration steps for a partner executed POV. All items must be completed together for the system to work properly during the customer engagement. After the POV, completing the POV Outcome worksheet in Appendix C will help to track POV information and lead to effective POV decision-making and increased win rates. Follow the instructions below carefully and submit any feedback to asa-assess@external.cisco.com.

Training

Cisco offers the Fire Jumper program that develops partner pre-sales security SEs to lead customer engagements from sizing, scoping, and design through demonstration and proof-of-value. Prior to delivering a customer FTD POV, we recommend that partners achieve Stage 4 of the Fire Jumper program for the NGFW & NGIPS competency area. Program and training information is through the following Security Partner Community posts.

- Fire Jumper Program
  https://communities.cisco.com/docs/DOC-55046
- NGFW & NGIPS Competency Area
  https://communities.cisco.com/docs/DOC-57815

Deployment

The majority of tactical POVs will leverage Cisco ASAs running FTD. To minimize risk or disruption to the customer environment while providing the most value, passive deployments are recommended. This can be accomplished by configuring a span port on a Cisco switch in the customer environment and configuring a passive interface on the FTD.

There are multiple options to send traffic to the FTD and the best deployment is one that gives visibility of both internet facing and internal segments. For tactical POVs, we recommend configuring multiple SPAN ports on a customer switches to capture both internet and internal traffic. Please refer to the SPAN configuration examples here that match your customer's switch type: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html.

For tactical POVs, we recommend that partners leverage the Cisco Firepower Management Center Proof of Value available at https://dcloud.cisco.com. When using dCloud, installation options for dCloud include Endpoint Router and FTD or Standalone FTD. This guide will present the standalone FTD option.

Scenario 1. POV Preparation

VALUE PROPOSITION: The instructions that follow show how to download required software for an ASA 5515-X. As of the writing of this document, the recommended FTD version is 6.4. Verify the current supported version by checking the name of the dCloud Firepower Management Center Proof of Value. The information below serves as an example of a common POV configuration. Adjust the process as required to match your hardware specifications.

If you are unable to access any software due to entitlement, engage with your Cisco alliance manager to associate your CCO account with your company to grant partner-level CCO access. If you are still unable to access the software, follow the process at this link to request access from partner help through the special file publish process: **https://communities.cisco.com/docs/DOC-55301**. Use of Firepower Threat Defense software on the device is strongly encouraged.

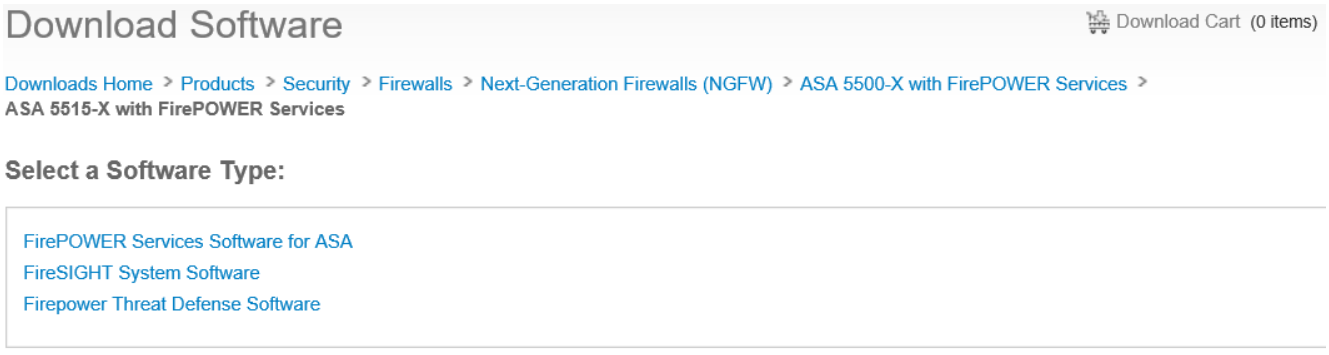
For additional information on migration paths and upgrade dependencies, please refer to the following link: **http://www.cisco.com/c/en/us/td/docs/security/asa/asa95/upgrade/upgrade95.html**.

Steps

NOTE: Instructions to download required software for an ASA 5515-X and use for POV preparation can be used for other ASA models as needed.

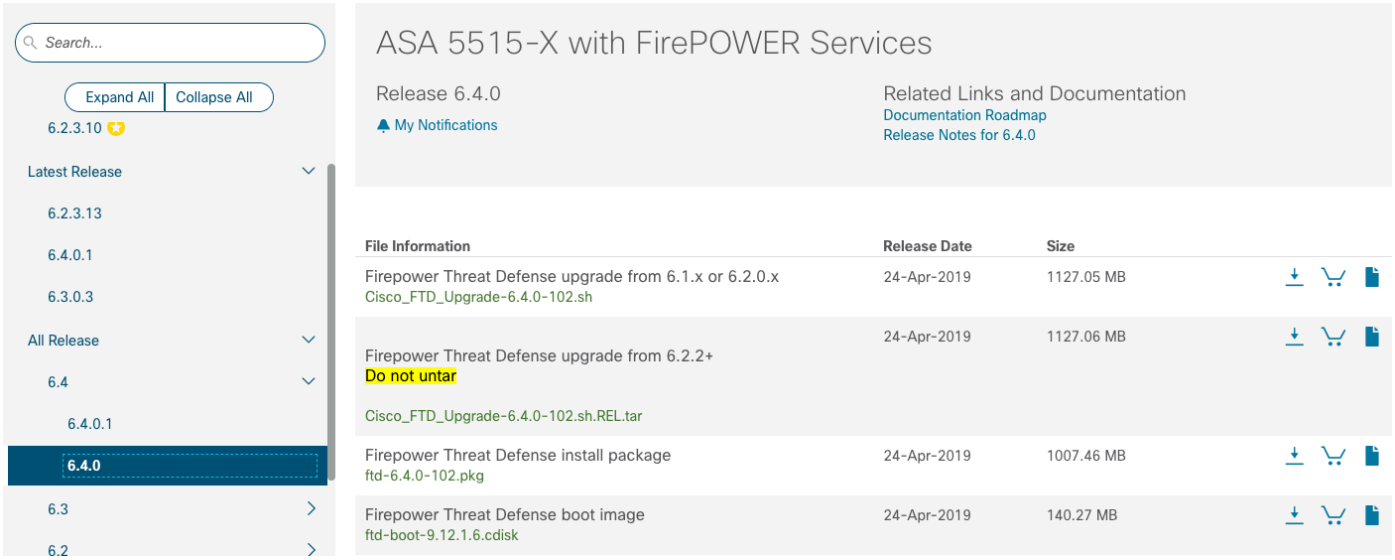
1. To download the FTD software, go to **http://software.cisco.com/download/navigator.html**.
2. This displays the **Downloads Home > Products** pane.
3. Continue to navigate to Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > ASA 5500-X with FirePOWER Services > ASA 5515-X with FirePOWER Services > Firepower Threat Defense Software.

Figure 2. Download Software



4. Select the following options and download the versions listed below or later.
   - Firepower Threat Defense for ASA 55XX series v6.4 (ftd-6.4.0-102.pkg)
   - Firepower Threat Defense v6.4 boot image for ASA 5512/5515/5525/5545/5555 devices (ftd-boot-9.12.1.6.cdisk)

Figure 3. ASA 5515-X with FirePOWER Services



NOTE: The ASA5585-X platforms will not support the FTD software.

Installation

Confirm Health of Solid State Drive (SSD)

Prior to installation, confirm the health of the solid state drive (SSD) within your 5515-X.

1. Power on the ASA and access the command line. Enter the **show inventory** command and confirm the presence of the SSD storage device.

```
ciscoasa# show inventory
Name: "Chassis", DESCR: "ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC"
PID: ASA5515           , VID: V01     , SN: FGH123456A1

Name: "Storage Device 1", DESCR: "Unigen 128 GB SSD MLC, Model Number: Micron_M550_MTFDDAK123MAY"
PID: N/A               , VID: N/A     , SN: 12345678900
```

2. If the SSD is not recognized, consider the following:

- The SSD drive may not be inserted properly. Ensure the SSD drive is properly inserted and secured via the handle. With the ASA powered off, pull the SSD drive out and re-insert it.
- The SSD drive may have failed. A healthy SSD drive will show a solid green LED next to the SSD. In the event of a failure, contact Cisco TAC for a replacement

Uninstalling Existing Firepower Services, IPS, or CX Software (If Required)

If your ASA is running legacy Firepower Services, IPS or CX on the ASA, you need to uninstall the old service before installing FTD.

1. Access the ASA command line and follow the procedures below. The commands below will shut down the sfr module, uninstall the SFR software, and then reload the ASA. If you need to remove IPS or CX, follow the same steps, but use ips or csc in each command instead of sfr.

```
ciscoasa# sw-module module sfr shutdown
ciscoasa# sw-module module sfr uninstall
ciscoasa# reload
```

Verify and Upgrade the ROMMON Image (If Required)

For the ASA 5506-X series, ASA 5508-X, and ASA 5516-X models only, the ROMMON version on your system must be 1.1.8 or later to reimage to the Firepower Threat Defense software. Follow the steps below to verify the ROMMON version and, if necessary, upgrade the ROMMON image.

1. Access the command line and enter the **show module** command. Note the Fw Version in the output for Mod 1 in the MAC Address Table.

```
ciscoasa# show module
Name: "Chassis", DESCR: "ASA 5506-X with SW, 6 GE Data, 1 GE Mgmt, AC"
[…]
Mod  MAC Address Range          Hw Version Fw Version Sw Version
---- -------------------------- ---------- ---------- ----------
1    7426.aceb.ccea to 7426.aceb.ccf2   1.0  1.1.1      9.3(2)2
sfr 7426.aceb.cce9 to 7426.aceb.cce9   N/A  N/A
```

NOTE: The Example ASA5506-X has an Fw Version of 1.1.1 and needs to be upgraded.

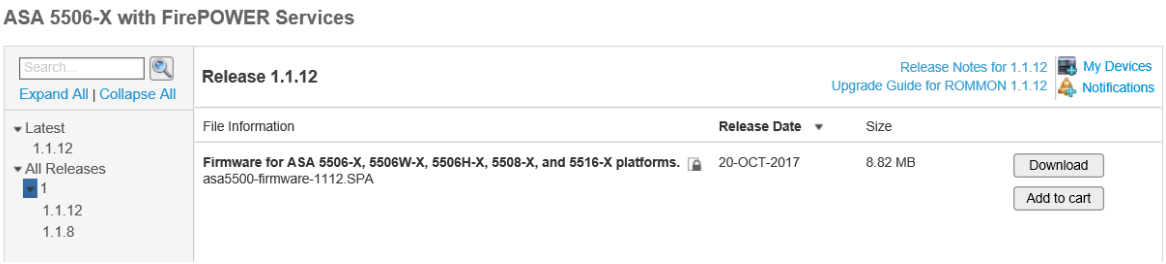
If the Fw Version of your ASA 5506-X series, ASA 5508-X, or ASA 5516-X is not 1.1.1 or greater, follow the steps below to upgrade the ROMMON. The example that follows is for the ASA5506-X, but the same firmware also works for ASA5508-X and ASA5516-X platforms.

2. To download the ROMMON software, go to http://software.cisco.com/download/navigator.html. This will present the Downloads Home > Products pane. Continue to navigate to Downloads Home > Products > Security > Firewalls > Next-Generation Firewall (NGFW) > ASA 5500-X with FirePOWER Services > ASA 5506-X with FirePOWER Services > ASA Rommon Software.

Figure 4. Download Software

3. Select the following options and download the versions listed below or later.
   - ASA Rommon Software (asa5500-firmware-1112.SPA)

Figure 5. ASA 5506-X with Firepower Services



4. To upgrade the ASA ROMMON, connect to the ASA and escalate to configuration mode. Configure the management1/1 interface with an IP address with connectivity to a TFTP server that can source the required ROMMON software. Use the **ping** command to confirm connectivity.

```
ciscoasa# config t
ciscoasa (config)# interface management1/1
ciscoasa (config)# ip address 10.10.200.3 255.255.255.0
ciscoasa (config)# ping 10.10.200.2
```

5. Copy the ROMMON image to ASA flash memory with the **copy** command. Upgrade the ROMMON image with the **upgrade rommon** command. Save the configuration and confirm for the ASA to upgrade the ROMMON image and reload when complete.

```
ciscoasa (config)# copy tftp://10.10.200.2:/asa5500-firmware-1112.SPA disk0:asa5500-firmware-1112.SPA
Address or name of remote host [10.10.200.2]?
Source filename [asa5500-firmware-1112.SPA]?
Destination filename [asa5500-firmware-1112.SPA]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[…]
!!!!!!!!!!!!!!!!!!!
9241408 bytes copied in 11.218 secs (9241408 bytes/sec)
ciscoasa (config)# upgrade rommon disk0:asa5500-firmware-1112.SPA
Computed Hash SHA2: 0809c2851ead97a1a327bfceb3f04ed6
[…]
Verification successful.
System config has been modified. Save? [Y]es/[N]o: Y
Cyrptochecksum: c0048ee4 bca79091 de890268 d5f5010b

92100 bytes copied in 0.270 secs
Proceed with reload? [confirm]
```

6. After system reload, access the command line and enter the **show module** command. Note the Fw Version in the output for Mod 1 in the MAC Address Table. This should match the ROMMON version loaded 1.1.12 or greater.

```
ciscoasa# show module
Name: "Chassis", DESCR: "ASA 5506-X with SW, 6 GE Data, 1 GE Mgmt, AC"
[…]
Mod MAC Address Range Hw Version Fw Version Sw Version ---- --------------------------- ---------- ------
---- ----------1 7426.aceb.ccea to 7426.aceb.ccf2 1.0 1.1.12 9.9(1)
sfr 7426.aceb.cce9 to 7426.aceb.cce9 N/A N/A
```

Install Firepower Threat Defense

To install the FTD software, you must access the ROMMON prompt. The boot image can then download the FTD system software install package using HTTP or FTP.

1. Copy the previously downloaded FTD boot image to a device running a TFTP server accessible by the ASA management interface.
2. Copy the previously downloaded FTD system software to a device running an FTP or HTTP server accessible by the ASA management interface.
3. From the console port, reload the ASA by issuing the **reload** command.
4. Press **Esc** during startup when prompted to reach the ROMMON prompt. If you see the message **Launching BootLoader...** then you waited too long and must reload the ASA again after it finishes booting.

```
ciscoasa# reload
System config has been modified. Save? [Y]es/[N]o: N
Proceed with reload? [confirm]
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
[…]
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
[…]
Booting from ROMMON
[…]
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
Link is DOWN
MAC Address: a0ec.f938.fdac

Use ? for help.
rommon #0>
```

5. From ROMMON, configure the Management IP address, Default Gateway, TFTP server, and TFTP path, and file name.
   - ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X
     - Use interface management 0/0
     - Boot image file extension is .cdisk
   - ASA 5506-X Series, 5508-X, and 5516-X
     - Use **interface management 1/1** by default and do not require the **interface** command
     - Boot image file extension is .lfbff

NOTE: These Use the **set** command to verify settings and the **sync** command to save the configuration for later use. Commands may vary by ROMMON version so adjust as required.

```
rommon #0> interface management0/0
rommon #1> address 10.10.200.3
rommon #2> server 10.10.200.2
rommon #3> gateway 10.10.200.1
rommon #4> file ftd-boot-9.12.1.6.cdisk
rommon #5> set
ROMMON Variable Settings:
ADDRESS=10.10.200.2
SERVER=10.10.200.3
GATEWAY=10.10.200.1
PORT=Management0/0
VLAN=untagged
IMAGE=ftd-boot-9.12.1.6.cdisk
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20
rommon #5> sync
Updating NVRAM Parameters...
```

6. Use the **ping** command to confirm connectivity to the TFTP server. Then, enter **tftpdnld** to load the boot image. The image can take a number of minutes to download so please be patient. You can monitor the download status in most TFTP server software.

```
rommon #6> ping 10.10.200.2
Sending 20, 100-byte ICMP Echoes to 10.10.200.2, timeout is 4 seconds:
?!!!!!!!!!!!!!!!!!!!
Success rate is 95 percent (19/20)
rommon #7> tftpdnld
ROMMON Variable Settings:
 ADDRESS=10.10.200.2
 SERVER=10.10.200.3
 GATEWAY=10.10.200.2
 PORT=Management0/0
 VLAN=untagged
 IMAGE=ftd-boot-9.12.1.6.cdisk
 CONFIG=
 LINKTIMEOUT=20
 PKTTIMEOUT=4
 RETRY=20


tftp ftd-boot-9.12.1.6.cdisk@10.10.200.2 via 10.10.200.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[…]
Received 101173248 bytes
[…]
Launching TFTP Image...
[…]
ciscoasa-boot>
```

7. Type **setup** and configure network settings for the Management interface to establish temporary connectivity to the HTTP or FTP server so that you can download and install the system software.

```
ciscoasa-boot> setup
Welcome to Cisco FTD Setup
[hit Ctrl-C to abort]
Default values are inside []

Enter a hostname [ciscoasa]: <FTD Hostname>
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: <FTD Sensor Management IP>
Enter the netmask [255.255.255.0]: <Netmask>
Enter the gateway [192.168.8.1]: <Default Gateway>
Do you want to configure static IPv6 address on management interface?(y/n) [N]: N
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: <DNS Server>
Do you want to configure Secondary DNS Server? (y/n) [n]: N
Do you want to configure Local Domain Name? (y/n) [n]: N
Do you want to configure Search domains? (y/n) [n]: N
Do you want to enable the NTP service? [Y]: Y
Enter the NTP servers separated by commas: <NTP Server>
Do you want to enable the NTP symmetric key authentication? [N]: N
Please review the final configuration:
Hostname:               ftd
Management Interface Configuration

IPv4 Configuration:     static
        IP Address:     10.10.200.3
        Netmask:        255.255.255.0
        Gateway:        10.10.200.1
IPv6 Configuration:     Stateless autoconfiguration
DNS Configuration:
        DNS Server:     208.67.222.222
[…]

Apply the changes?(y,n) [Y]: y
Configuration saved successfully!
Applying...
Restarting network services...
Done.
```

8. Type **system install** followed by the path to the FTD system software. HTTP and FTP are supported and the example below shows an FTP installation. When installation is complete, enter **y** to continue with the upgrade. When prompted, press **Enter** to reboot the system. The initial reboot after installing FTD on an ASA make take 30 minutes or longer.

```
ciscoasa-boot>system install ftp://10.10.200.2/ftd-6.4.0-102.pkg

######################### WARNING ############################
# The content of disk0: will be erased during installation! #
##############################################################

Do you want to continue? [y/N]: Y
Erasing disk0 ...
Verifying

Enter credentials to authenticate with ftp server
```

```
Username: admin
Password:

Enter credentials to authenticate with ftp server
Username: admin
Password:
Verifying
Downloading...
Extracting
Package Detail
Description:              Cisco ASA-FTD 6.4.0-102 System Install
Requires reboot:   Yes

Do you want to continue with upgrade? [y]: Y
Warning: Please do not interrupt the process or turn off the system. Doing so might leave system in
unusable state.

Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

NOTE: See the Reimage the Cisco ASA or Firepower Threat Defense Device document for additional details:

http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/reimage/asa-ftd-reimage.html

Bootstrap Firepower Threat Defense

When the reboot is complete, login to the FTD CLI with the default username: **admin** and password: **Admin123**.

Accept the EULA, change the password, and enter bootstrap information based on the Data Collection Worksheet. Ensure that you select **no** when asked if you would like to manage the device locally. Risk Reports are not supported in the on-box Manager, Firepower Device Manager.

```
Cisco ASA5515-X Threat Defense v6.4.0 (build 102)
firepower login: admin
Password: Admin123
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
[…]
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: Y
Do you want to configure IPv6? (y/n) [n]: N
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]:
<FTD Management IP>
Enter an IPv4 netmask for the management interface [255.255.255.0]: <Netmask>
Enter the IPv4 default gateway for the management interface [192.168.45.1]: <Default Gateway>
Enter a fully qualified hostname for this system [firepower]: <hostname>
Enter a comma-separated list of DNS servers or 'none' []: <dns servers>
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
Manage the device locally? (yes/no) [yes]: <no>
Configure firewall mode? (routed/transparent) [routed]: <transparent>
Configuring firewall mode ...
[…]
>
```

1. If you need to adjust the management IP after completing the bootstrapping wizard, enter the **configure network** command from the CLI. You can verify the configuration with the **show network** command.

- configure network ipv4 manual *X.X.X.X X.X.X.X X.X.X.X*
- show network

Scenario 2. FMC Configuration

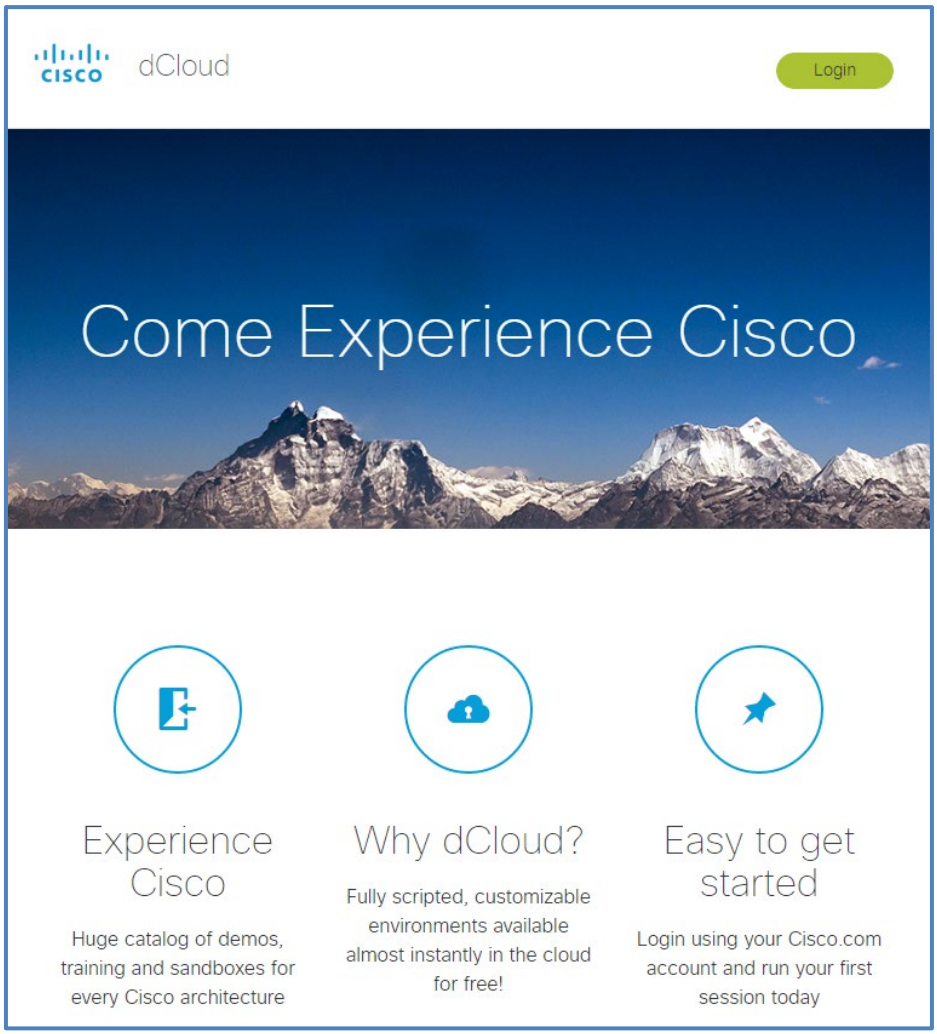
VALUE PROPOSITION: The FTD supplies NGFW and NGIPS services such as Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP). A FMC is optional to configure FTD, but required to generate Risk Reports. dCloud provides a hosted and pre-configured FMC that follows POV best practices and includes customized dashboards optimized for POVs.

Steps

Schedule dCloud POV

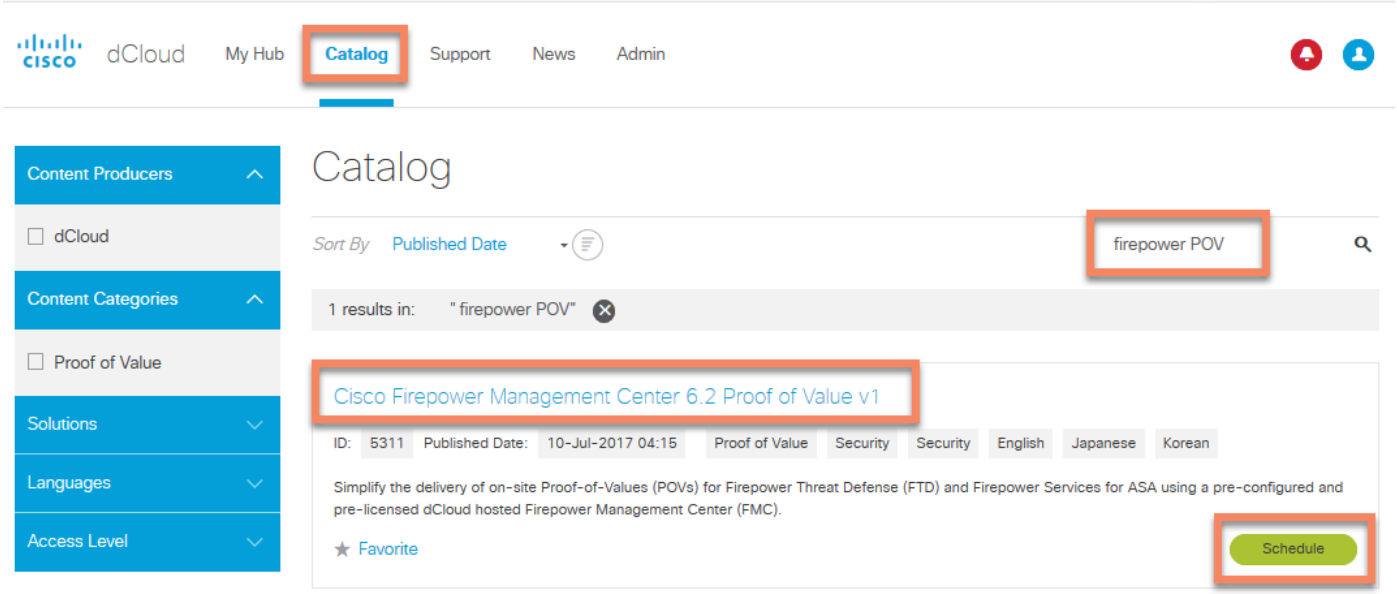
1. To schedule a dCloud POV, browse to http://dcloud.cisco.com and login with your CCO credentials. If prompted, select the region closest to you to set your default data center.

Figure 6. Cisco dCloud



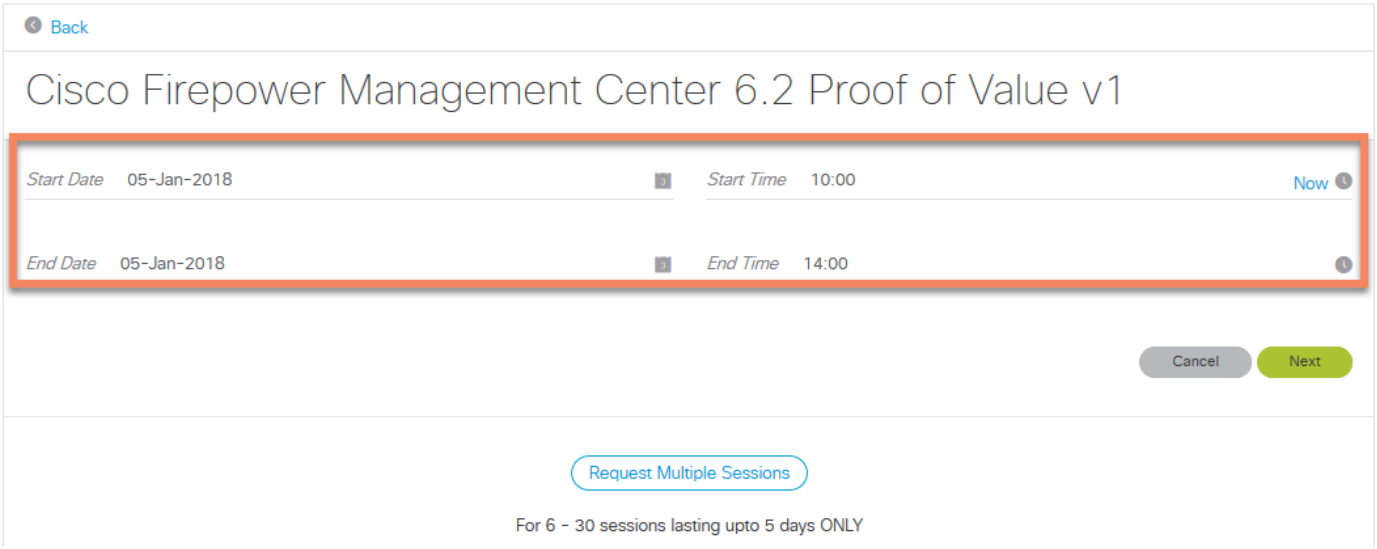
2. Select **Catalog** from the toolbar and search for **Firepower POV.** Find the appropriate catalog item and click **Schedule** to setup the dCloud POV Session. Image below may not match exactly but may be a later version.

Figure 7. Catalog



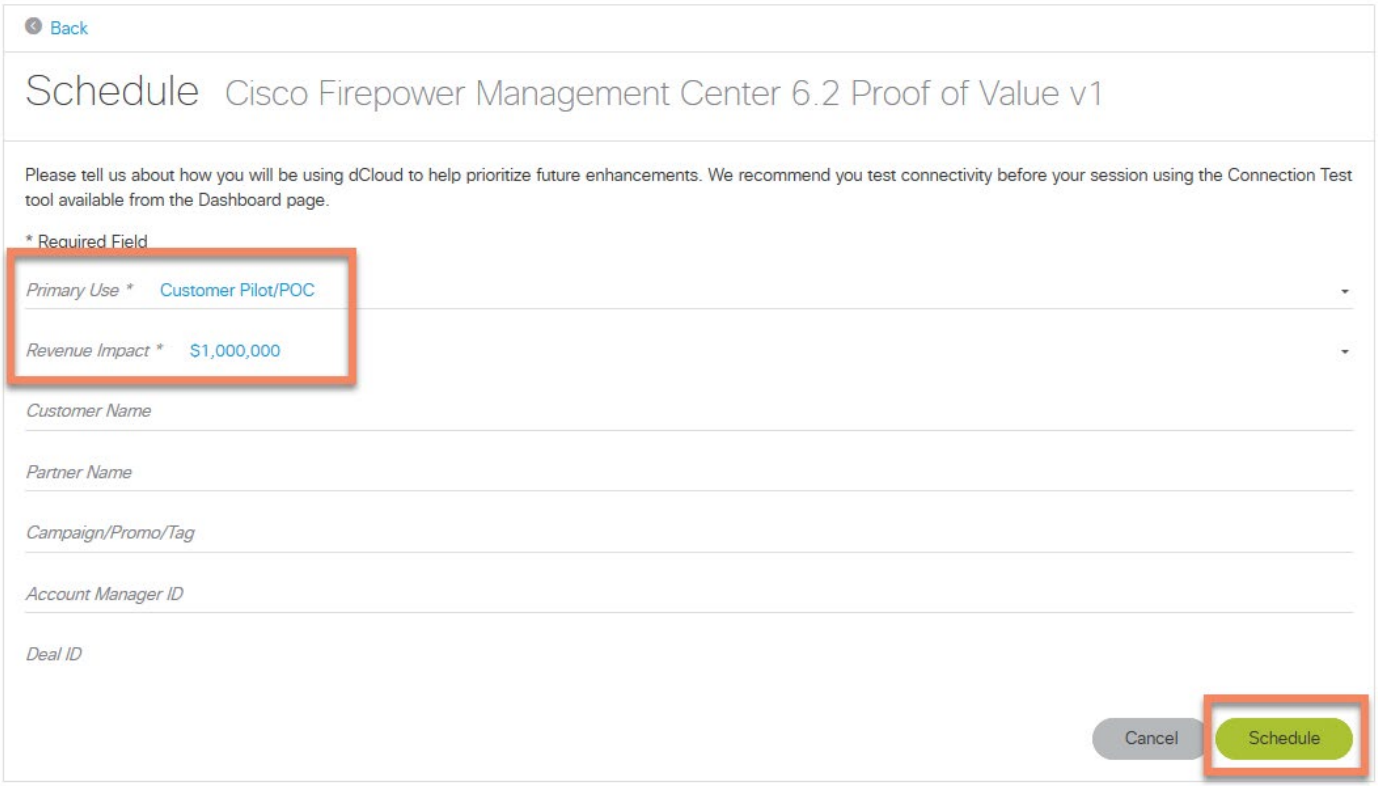
3. Enter the POV timeframe and click **Next**. Note that dcloud POVs are limited to 5-days by default. Extensions of up to 30 days are available by contacting support. Extensions beyond 30-days are handled on a case-by-case basis and require additional customer opportunity information. Risk Reports are based on 5-days of customer traffic and additional time should only be used as required to troubleshoot receiving network traffic or other items.

Figure 8. Schedule your Session



4. Enter **Customer Pilot/POC** for Primary Use, select the Revenue Impact, and provide relevant customer and partner information. When finished, click **Schedule**.

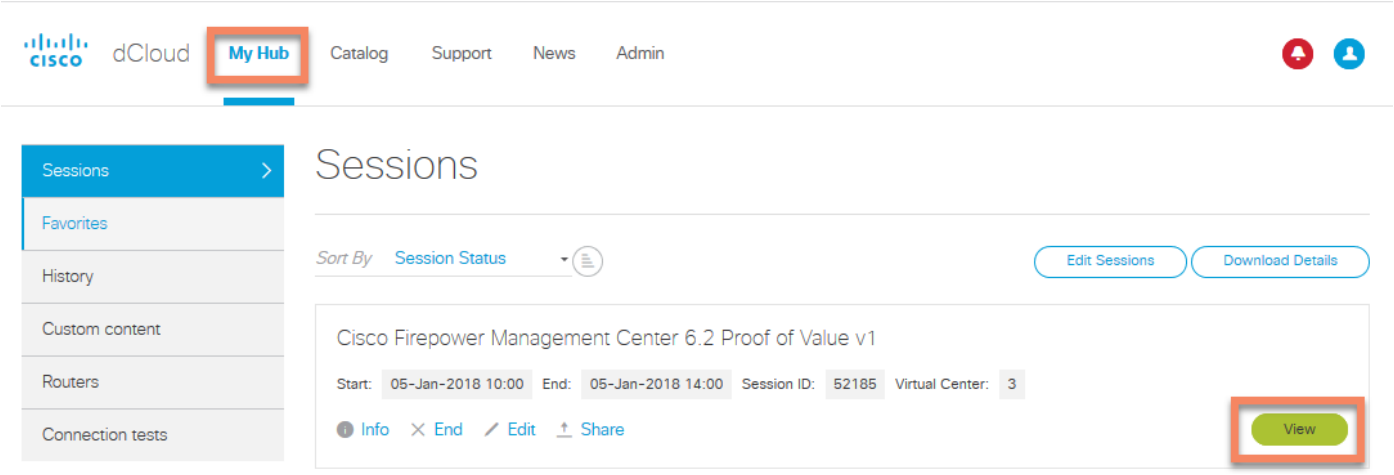
Figure 9. Primary Use and Revenue Impact



Connect FTD to FMC

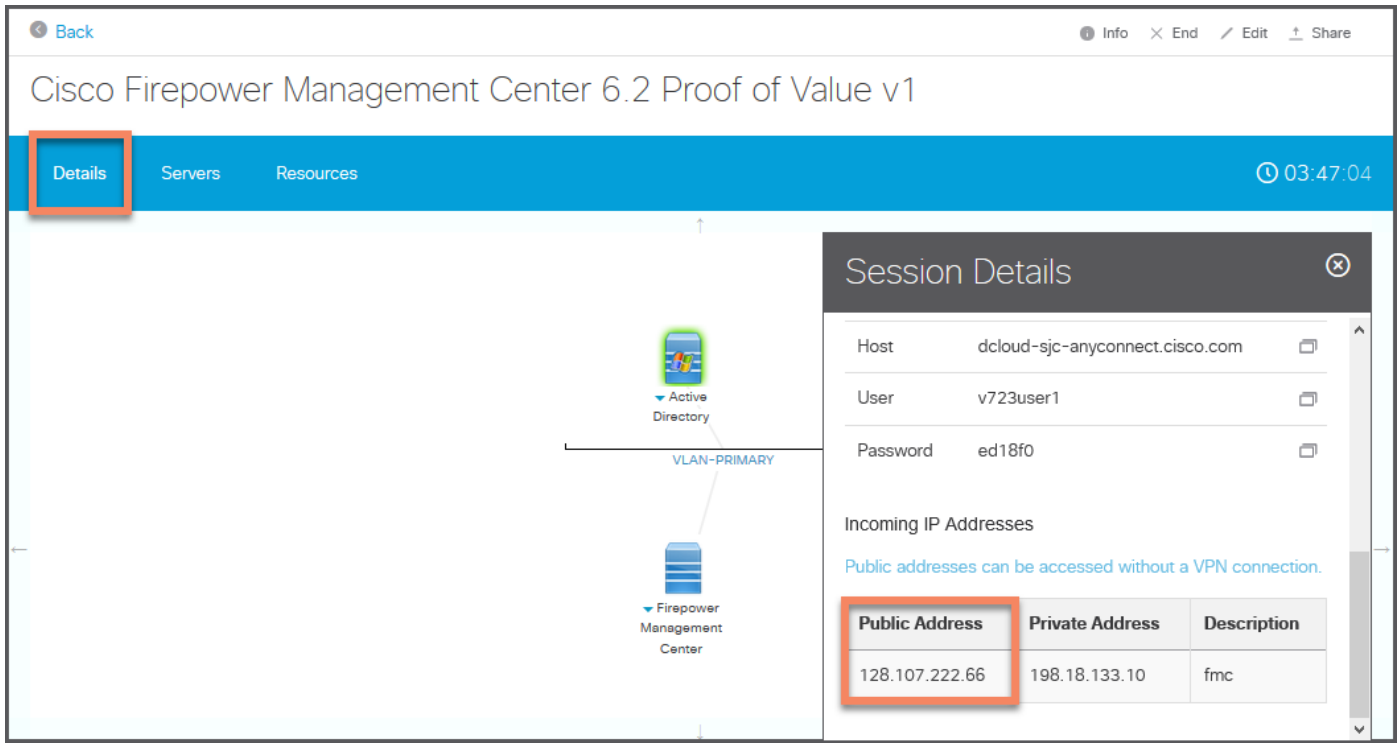
1. Access dCloud and select **Dashboard**, which will reflect the current scheduled sessions. Select **View** for the **Firepower POV.**

Figure 10. Dashboard > My Sessions



2. Select **Details** and note the **Public Address** for the FMC**.**

Figure 11. Public Address



3. Return to the FTD CLI and complete the configuration by identifying the FMC that will manage the sensor. When using FMC hosted on dCloud, the network management-port must be changed to **8443**. The Public Address from the dCloud session details will be the Firepower MC IP, the default registration key is **C1sco12345**, and the default nat-id is **12345**. The registration key and nat-id are arbitrary, but must match the key that will be created during FMC setup. Management port can be confirmed with '`show network`' command.

```
> configure network management-port 8443
Management port changed to 8443.

> configure manager add <FMC Public IP> <Registration Key> <nad-id>
Manager successfully configured.
> show network
===============[ System Information ]===============
Hostname                : vftd.dcloud.cisco.com
Domains                 : dcloud.cisco.com
DNS Servers             : 8.8.8.8
                          8.8.4.4
                          198.18.133.1
Management port         : 8443
IPv4 Default route
  Gateway               : 198.18.128.1

=====================[ br1 ]=====================
State                   : Enabled
Channels                : Management & Events
Mode                    : Non-Autonegotiation
```

```
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:50:5A:FA:CE:01
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 198.18.133.10
Netmask                   : 255.255.192.0
Broadcast                 : 198.18.191.255
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

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

>
```

Licensing

FMCs use Smart Licensing for sensors running 6.0 software or later for FTD devices. This dCloud FMC comes with a built-in Smart License account pre-installed. Running Firepower Threat Defense software will thus have the license installed directly from FMC on connection. Cisco strongly recommends FTD, but if you do require classic licenses for NGIPS or Firepower on ASA devices please use links below.

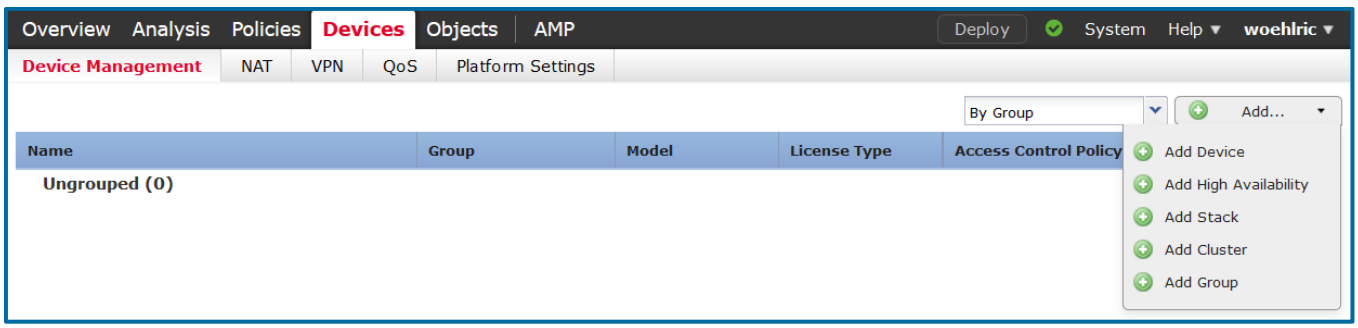
1. **Cisco Internal employee classic licensing**
2. **Cisco Partners/Customers**

Connect FMC to FTD

NOTE: The credentials for the FMC are Username and Session ID from dCloud for password. The username **dcloud** and the unique Session ID from dCloud for password can also be used. e.g. dcloud/55123

1. To add your FTD to the FMC, navigate to **Devices > Device Management**. Select **Add > Add Device** from the top right.

Figure 12. Devices > Device Management

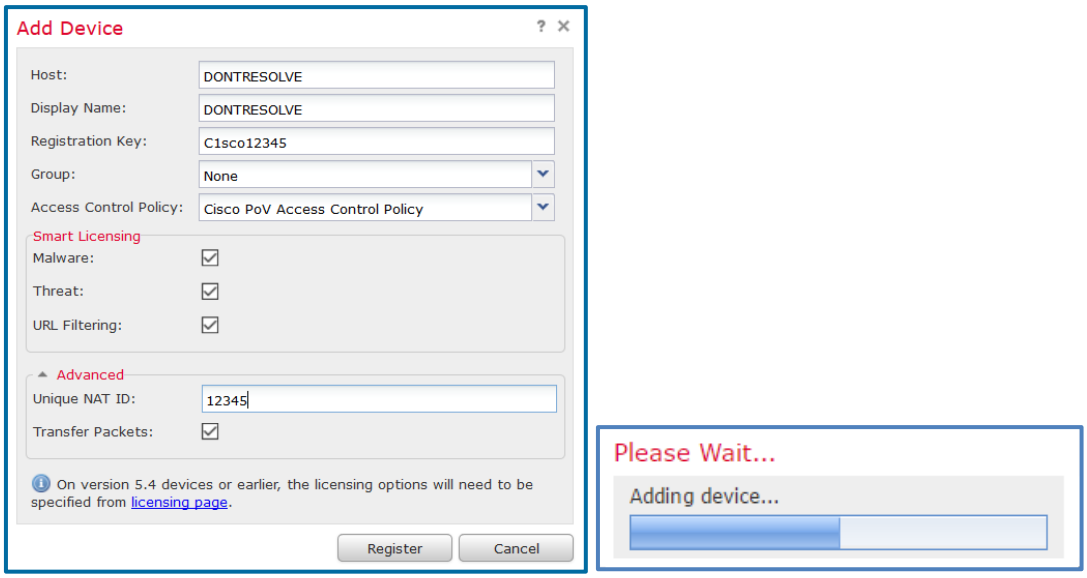


2. When adding a device from dCloud, use the Host of **DONTRESOLVE**, the Registration Key of **C1sco12345**, and select **Cisco PoV Access Control Policy** from the Access Control Policy drop-down.

NOTE: If you already registered one device with the FMC you must use a different name for subsequent devices such as **DONTRESOLVE2**. When connecting more than one device to the FMC, make sure to complete one setup first before continuing to other devices as to verify the FMC is building the correct connection to the correct device.

3. Select the **Malware, Threat,** and **URL Filtering** Licensing options. Expand the advanced settings and enter a Unique NAT ID of **12345**. When complete, click **Register**.

Figure 13. Add Device



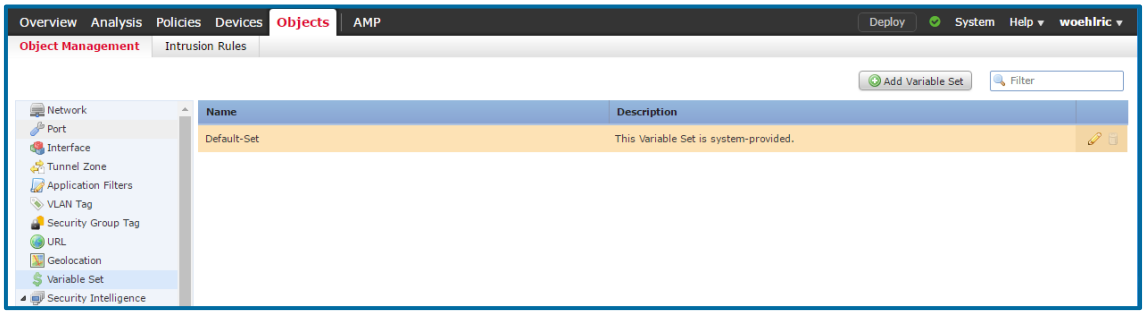
4. The FMC will contact your FTD and add it as a managed device. If the device is not added successfully, confirm that the registration keys match, the software versions are compatible, and that a network device is not blocking the connection. The **show managers** command from the FTD CLI will confirm the FMC IP address and view the current status.

5. To further troubleshoot the FTD to FMC connection, enter **expert** mode from the CLI and use **sudo pigtail** to review debugging information. Open a TAC POV case through your Cisco GSSO CSE as required. dCloud support can also assist directly and connect you with TAC as needed.

Initial Configuration

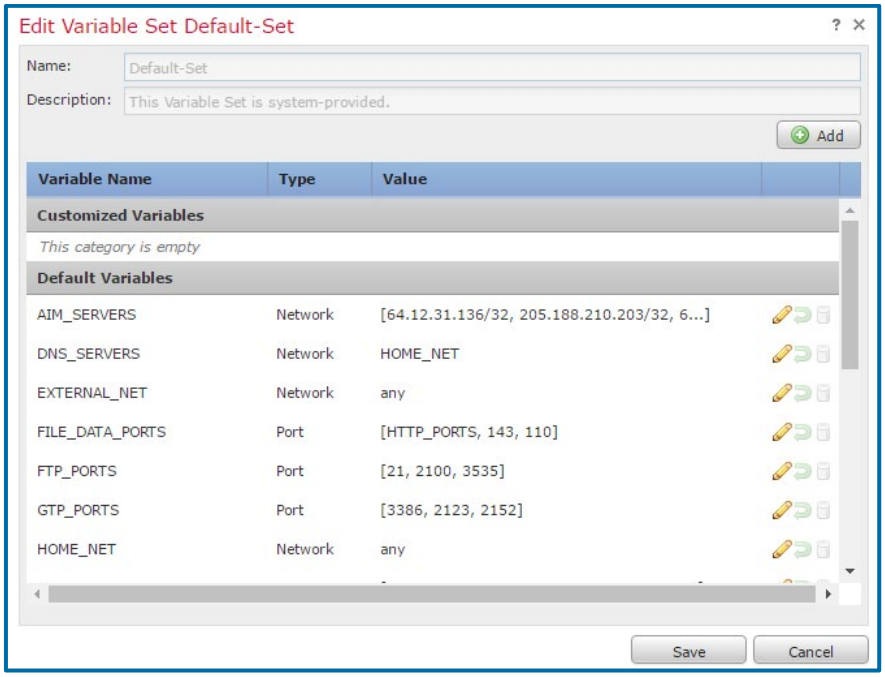
Object Management

1. The variable set should be adjusted to match the monitored network. In the FMC browse to **Objects > Object Management**. Select the **Variable Set** on the left hand side and select to edit the Default-Set.



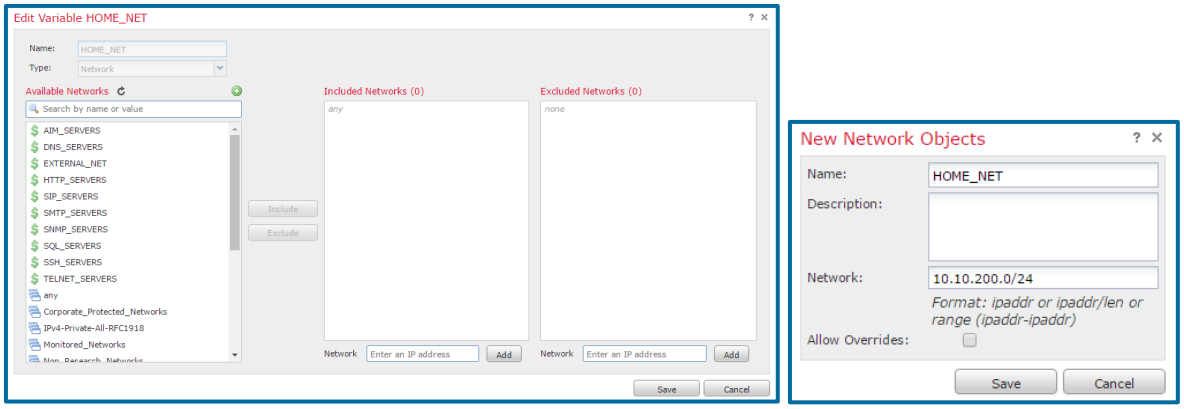
2. Select next to **HOME_NET.**

Figure 14. Edit Variable Set



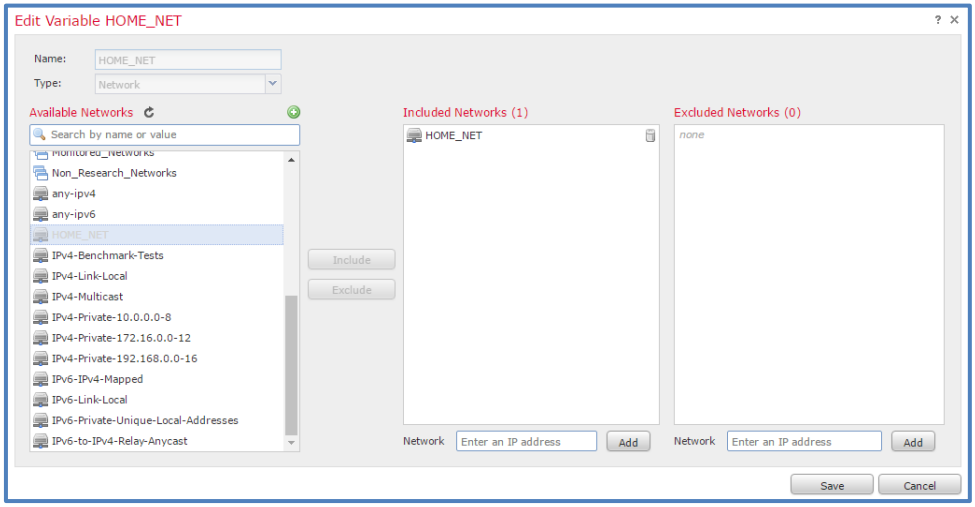
3. Click  to create a new Network Object. Provide a Name and enter Network information that matches the customer environment. Click **Save** when complete.

Figure 15. Create a New Network Object



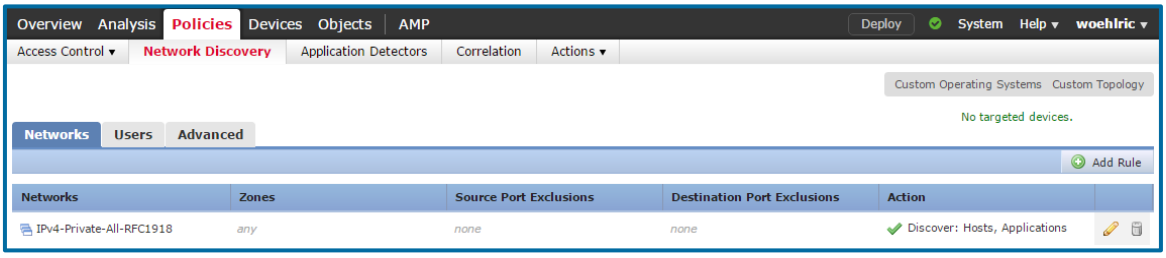
4. Click **Include** to add the New Network Object in the **HOME_NET** Variable. Continue by clicking **Save, Save, Yes.**

Figure 16. Edit Variable



5. Browse to **Policies > Network Discovery**. Select  to delete the IPv4-Private-All-RFC1918. Click **Yes** to confirm.

Figure 17. Policies > Network Discovery

1. 

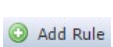
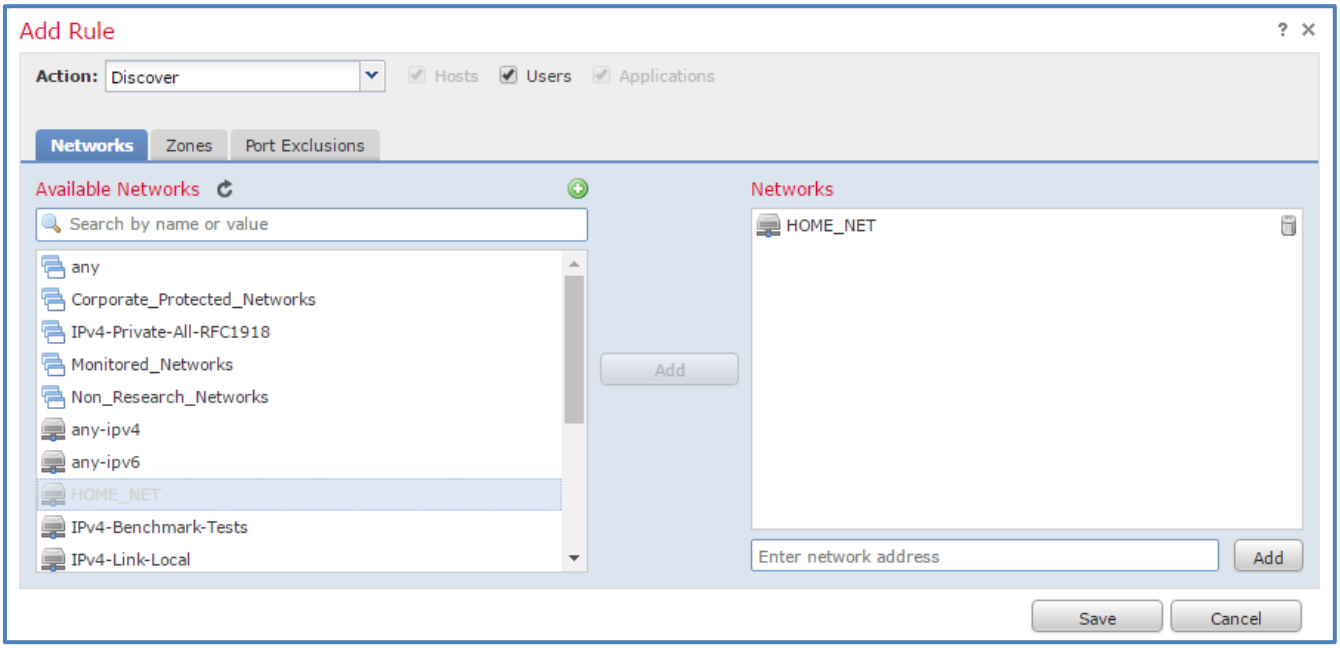
6. Select  to add a new rule. Select the **Users** checkbox. Add the newly created **HOME_NET** variable to the right hand pane. Click **Save**.

Figure 18. Add Rule Window

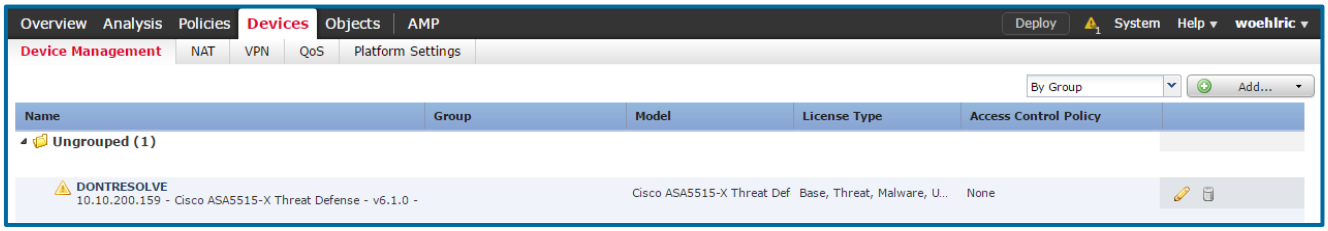
2. 

Passive Interface

A passive interface needs to be configured for the FTD to accept traffic from the SPAN port or tap on the customer network.

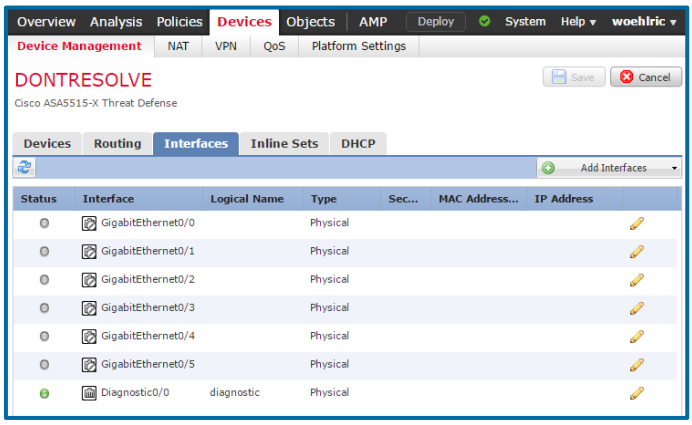
1. Navigate to **Devices > Device Management** and select ✎ to edit the FTD.

Figure 19. Devices > Device Management



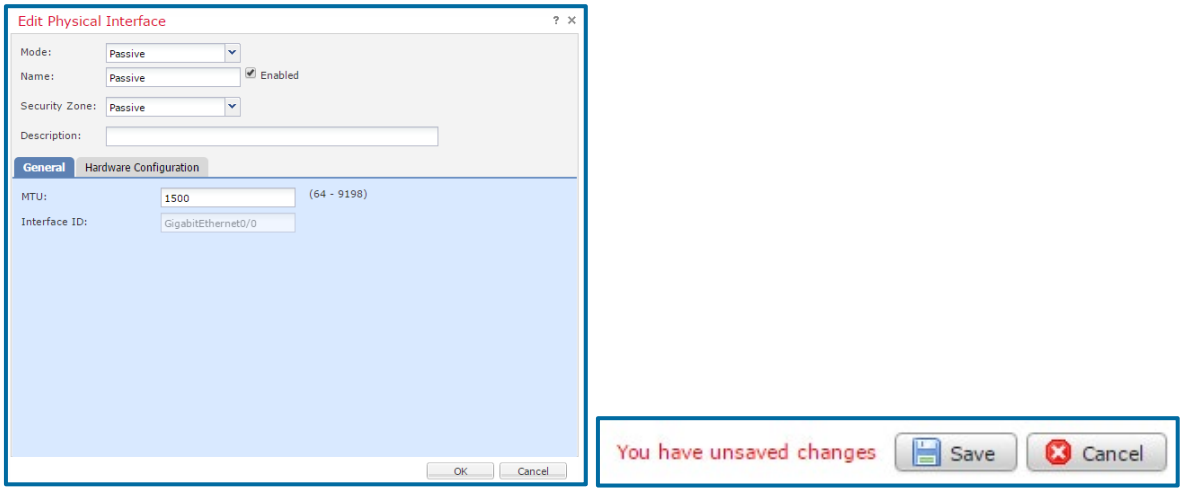
2. Select next to the interface connected to the evaluation network.

Figure 20. Evaluation Network



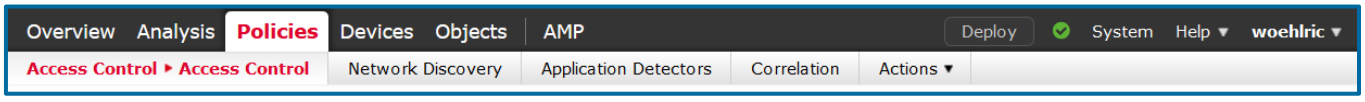
3. Set the interface Mode to **Passive**. Provide a Name and check the box to Enable the interface. Then, define a new Security Zone named **Passive**. Click **OK** and then **Save.**

Figure 21. Edit Physical Interface



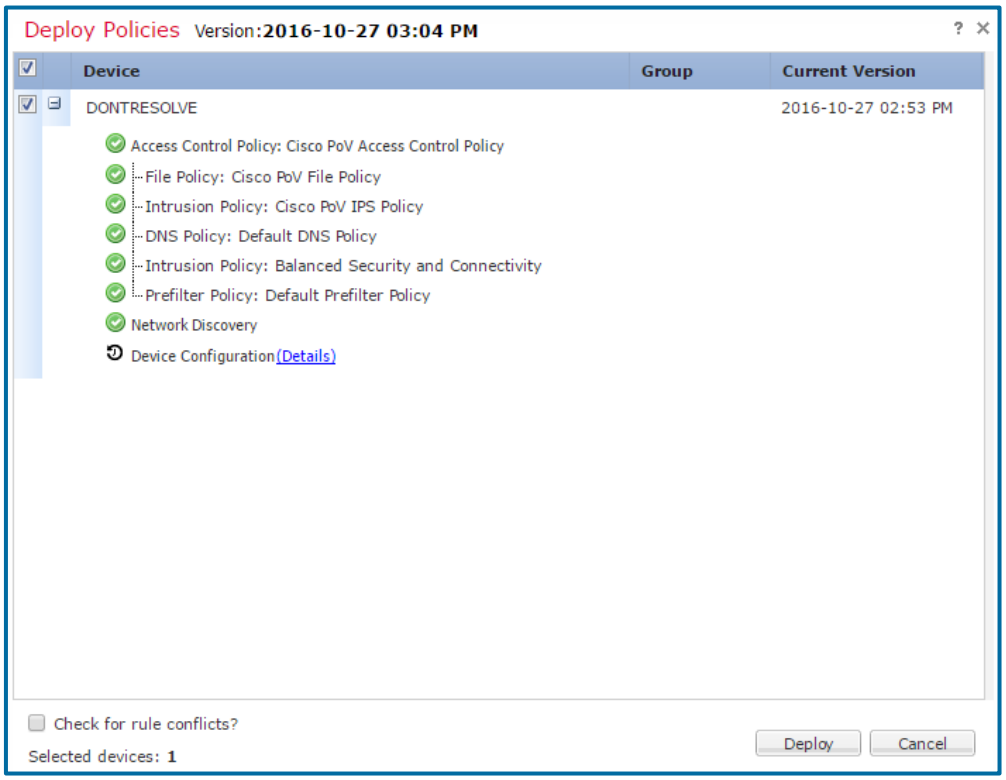
4. Click the **Deploy** button at the top right to push the interface configuration to the FTD.

Figure 22. Deploy



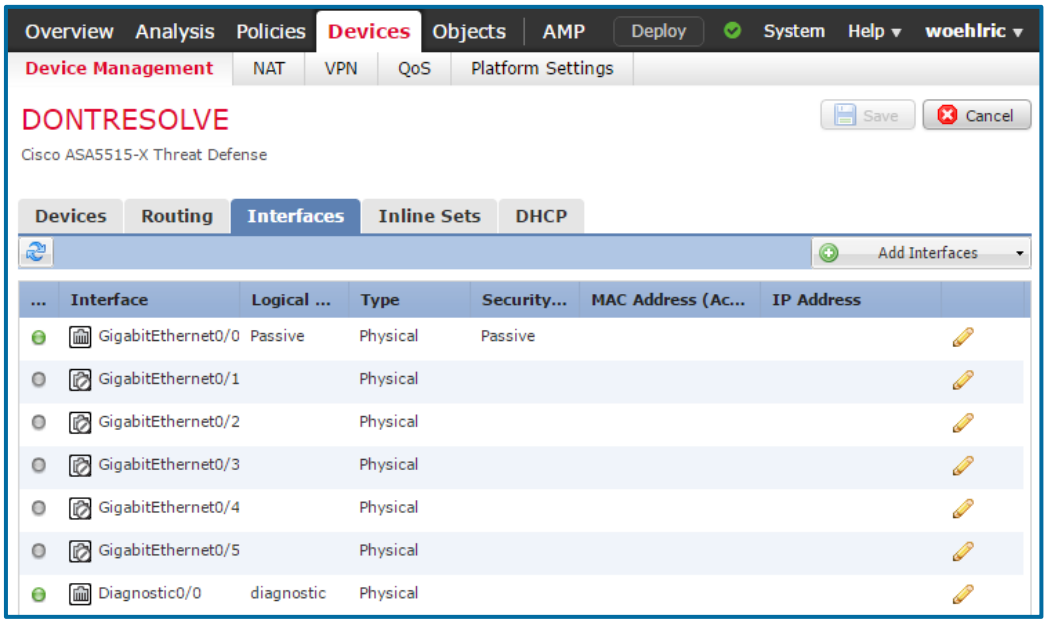
5. Select the checkbox by your FTD and click **Deploy.**

Figure 23. Deploy Policies



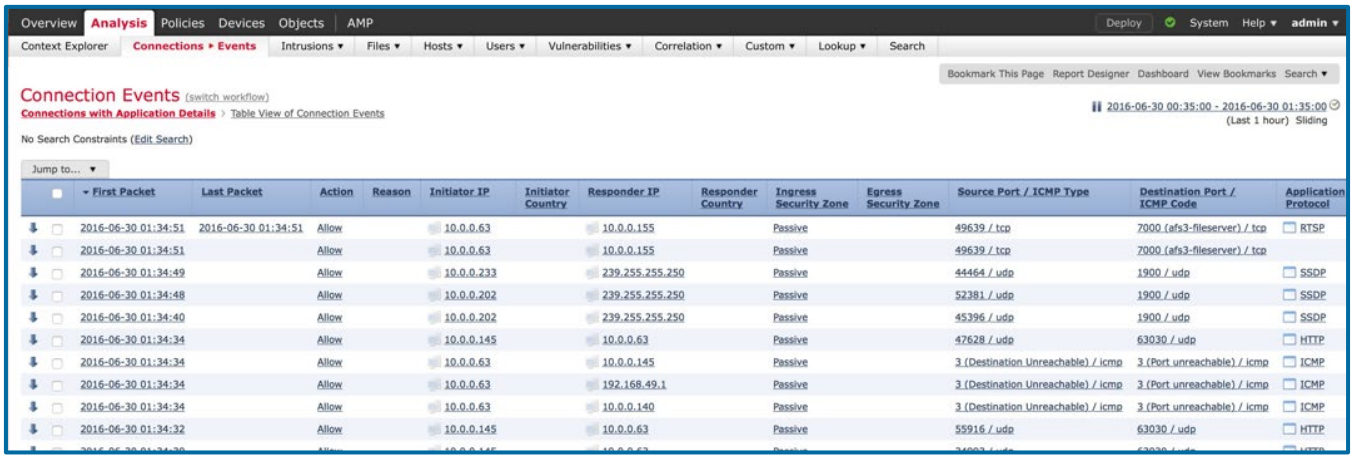
6. When the deployment completes, the interface status for the passive interface should turn green.

Figure 24. Interface Status



7. Browse to **Analysis > Connections > Events**. If events are not populating, verify that interfaces are connected, enabled, and the SPAN port or tap is functional.

Figure 25. Analysis > Connections > Events



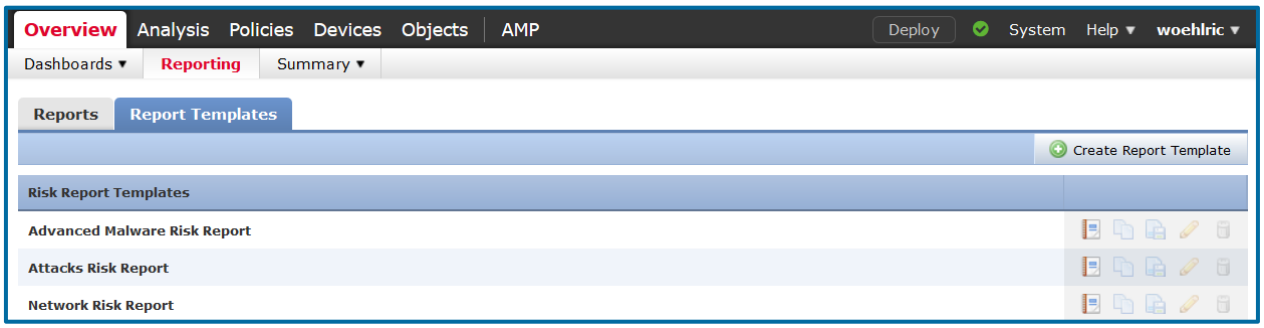
Scenario 3. Risk Report Generation

VALUE PROPOSITION: After allowing the system to collect customer data for at least five days, you can generate the Risk Reports. As of FMC 6.1, Risk Reports are now integrated into the FMC.

Steps

1. To generate the reports navigate to **Overview > Reporting** and select the **Report Templates** tab.
2. Then generate the Advanced Malware, Attacks, and Network Risk Reports. These will provide actionable information based on the customers traffic.

Figure 26. Report Templates



Once complete, you can access these PDF reports in the FMC and transfer them to your local system using any cloud based storage solution or email client. Share these reports and your findings with the customer at the POV close-out meeting. During the meeting focus on the win criteria established upfront and the differentiating value of the Cisco solution. Provide a bill of materials that positions the appropriate FTD licensed features

3. When complete, submit the POV for the company incentive through SIRE if supported in your location: www.cisco-sire.com. Note that the required proof-of-performance items are:

- Win Criteria: Appendix A in POV Best Practices Guides
- Data Collection Worksheet: Appendix B in POV Best Practices Guide
- POV Outcome: Appendix C in POV Best Practices Guide
- Risk Reports or Customer Facing Reports based on POV Best Practices Guide
- Bill of Materials (Microsoft Excel Format): Note that there is a $10k minimum opportunity to qualify for the program

Review the Cisco Funded Network Assessment Post for more information: https://communities.cisco.com/docs/DOC-65405.

Device Sanitization

After a successful partner executed POV, you will need to purge the customer data to prepare for the next POV. dCloud will automatically delete the FMC VM and any customer information.

1. The customer data on the FTD is deleted when you erase and reformat the file system. Enter the following command to complete the process.

```
> erase /noconfirm disk0:
```

2. To prepare for your next POV, re-install the FTD software as described in section 6.

Appendix A. Win Criteria

Customer Name	

Win criteria needs to be defined before a partner executed POV begins so that you are able to quickly demonstrate unique business value to the customer during the on-site engagement. This process focuses the engagement on the solution elements that are most important to the customer. The worksheet below serves as a starting point to develop win criteria for a Tactical Partner Executed POV and can be adjusted as required based on dialogue with your customer.

Prioritize each Win Criteria in order from 1 – 8 with one being most important and eight being least important based on your customer's priorities.

Visibility
Do you want to have a better understanding of the types of devices on your network and the applications they are running?

Threat
Are you concerned about bad actors in your environment and the threat that they pose to other internal systems?

Automation
Would you like to reduce the strain on your security analysts while arrive at a faster resolution of intrusion information?

Reputation
Do you value a robust reputation service that helps to limit traffic to known bad websites and actors on the Internet?

Malware Detection
Would you like to implement network malware detection with file reputation, sandboxing, and retrospection?

File Blocking
Do you value visibility of file types entering your environment with the capability to block files before an attack by type, protocol, or transfer direction?

Application Control
Are you interested in granular control of applications that helps maximize productivity and reduce the attack surface?

Cross product integration
Would you be interested in using the eStreamer API to share host and event data with third partner applications such as SIEM and integrate with systems such as Cisco ISE?

What compelling factors are driving this engagement?

Appendix B. Data Collection Worksheet

Customer Name	

Thank you for giving Cisco the opportunity to demonstrate the security posture of your network using Firepower Threat Defense. Please provide the following information to prepare for the evaluation.

Network Range(s)

1. Network ranges to be part of the evaluation: Please provide the smallest NETMASKs possible in CIDR format (e.g. 10.100.0.0/16 – instead of 10.100.1.0/24, 10.100.2.0/24, etc.)

2. Networks within these ranges that should be excluded from the above. (Note that this is a non-intrusive observatory system and will not footprint any of your hosts.)

Time Zone

3. Local Time Zone	

IP Addresses for POV

4. All should be on the same local subnet.	Format: **x.x.x.x**
Management IP for POV Firepower Threat Defense Sensor	
Netmask	
Default Gateway	
DNS Servers	
(Optional) Management IP for POV Firepower MC	
(Optional) Management IP for POV ESXi Server	

SPAN Port configuration

5. Is there a SPAN already set up that can see the traffic from the evaluated networks?
☐ Yes ☐ No Which port?

What type of switch will the system collect SPAN traffic from? (Cisco 3850, Cisco Catalyst 4K, etc.)

SPAN will be configured using Source Interface or Source VLANs. List sources below (VLAN 10, 20, etc.)

Length of Evaluation

6. Desired Length of Evaluation	

Appendix C. POV Outcome

POV Outcome	
Partner SE Name	
Partner SE Email	
Partner Fire Jumper	
Compelling Event	
Competitors	
POV Duration	
Technical Win or Loss	
Reason for Technical Decision	
Business Win or Loss	
Reason for Business Decision	
Cisco Deal ID	
Cisco PO or SO #	
Cisco Security Revenue	
Comments	

What's Next?

This completes the Cisco FTD POV Guide. For additional support, send requests to asa-assess@external.cisco.com.

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.**