FTD Basic POV Guide:

6.1 Software

Jerry Lin, Consulting Systems Engineer

Joey Muniz, Technical Solutions Architect

Alex Kirk, Consulting Systems Engineer

Security SEVT, October 2016

Purpose Of Creating This Class

1. Walk the SE or CSE through a successful installation of Firepower Management Console (FMC) and Firepower Threat Defense (FTD).

2. Configure a Passive Interface or an Inline TAP Interface Set.

   These interface types are used because they inspect copies of traffic. In a traditional POV, we do not want to interrupt production traffic.

3. Create an initial set of policies.

Exercise great care if a customer insists on deploying in any other mode if the appliance is interacting with production traffic. TAC me be required to troubleshoot

Why Are **YOU** Here?

The Sales Process 101

- L d with “Workshop”
  - e Dcloud and slides to showcase a working environment
- O r Gold Lab / Contained Demo (example CTR)
  - duces unknown r
  - l it ou would
    re u will see the worst day scenario and how this works within it.
- Offer Passive!
  - uce risk of impacting live users.
  - esn’t require TAC
- All else fails, inline / live PoV

= More Time To Close

What To Avoid

“Can I turn FirePOWER on my existing edge ASA?”

“I just want to try it out for a while”

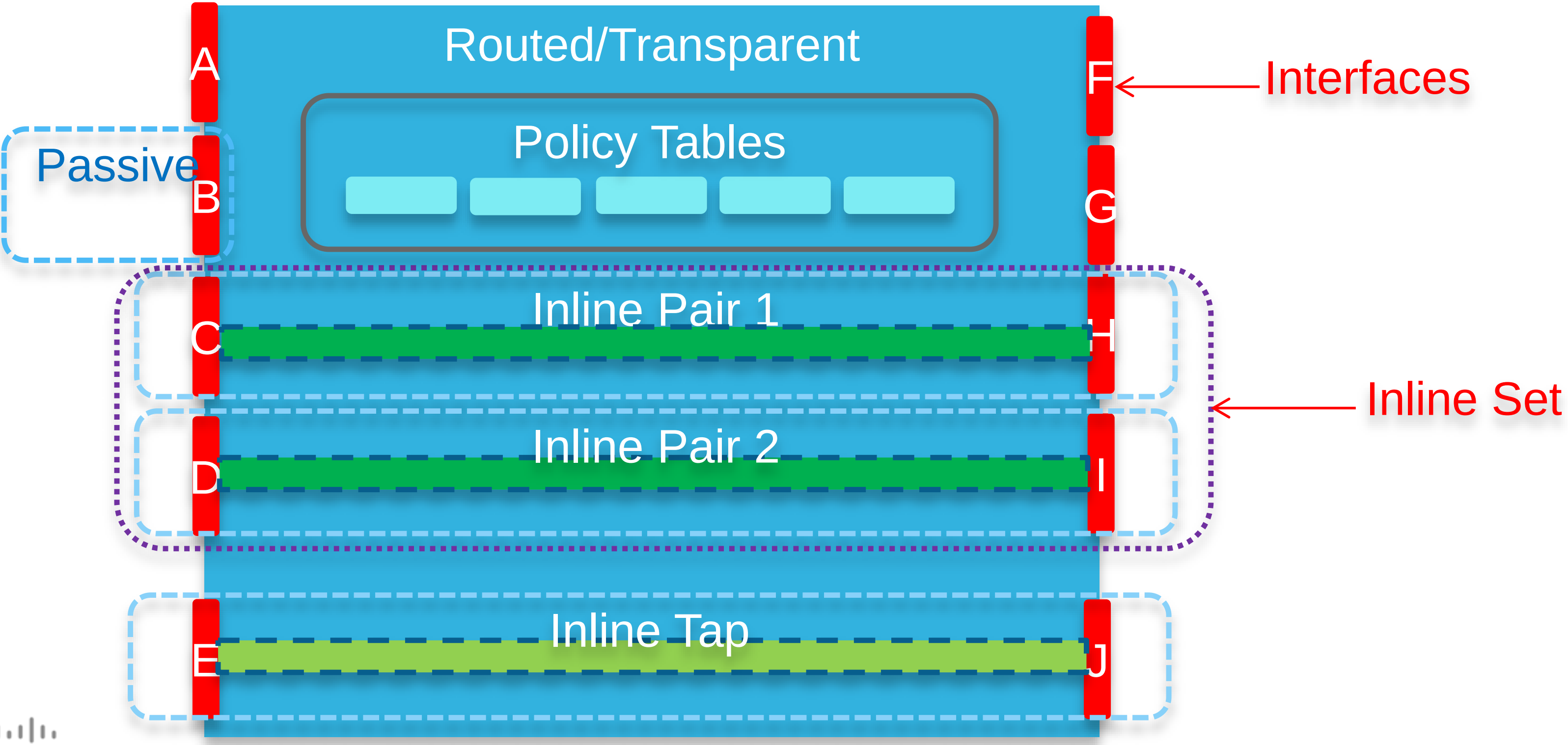
“We don’t need a presentation, lets just get to the technology”

“We can install it ourselves, just give us the software and install guide”

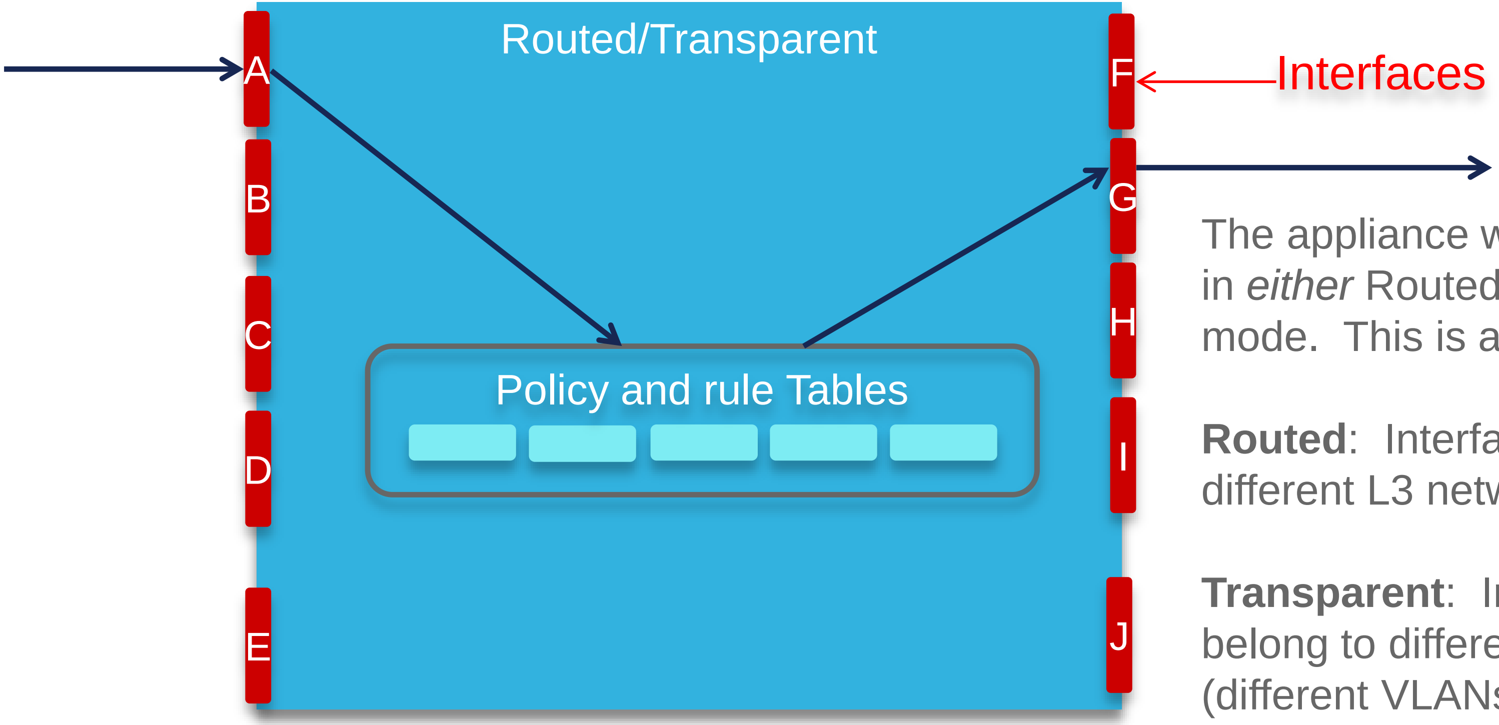
When to use which option

- **Cloud** – Dcloud runs the FMC, you deploy FirePOWER solution
  - Quickest deployment however must be open to their data in Cloud
- **Virtual FMC and FirePOWER solution**
  - 2nd quickest deployment however requires virtual environment to support VMs and permit traffic
- **Physical FMC and FirePOWER solution**
  - Slowest due to hardware requirements but least amount of customer dependencies.

FTD Interface Modes



FTD Interface Modes, continued…



The appliance will be installed in *either* Routed or Transparent mode. This is a global setting.

Routed: Interfaces belong to different L3 networks.

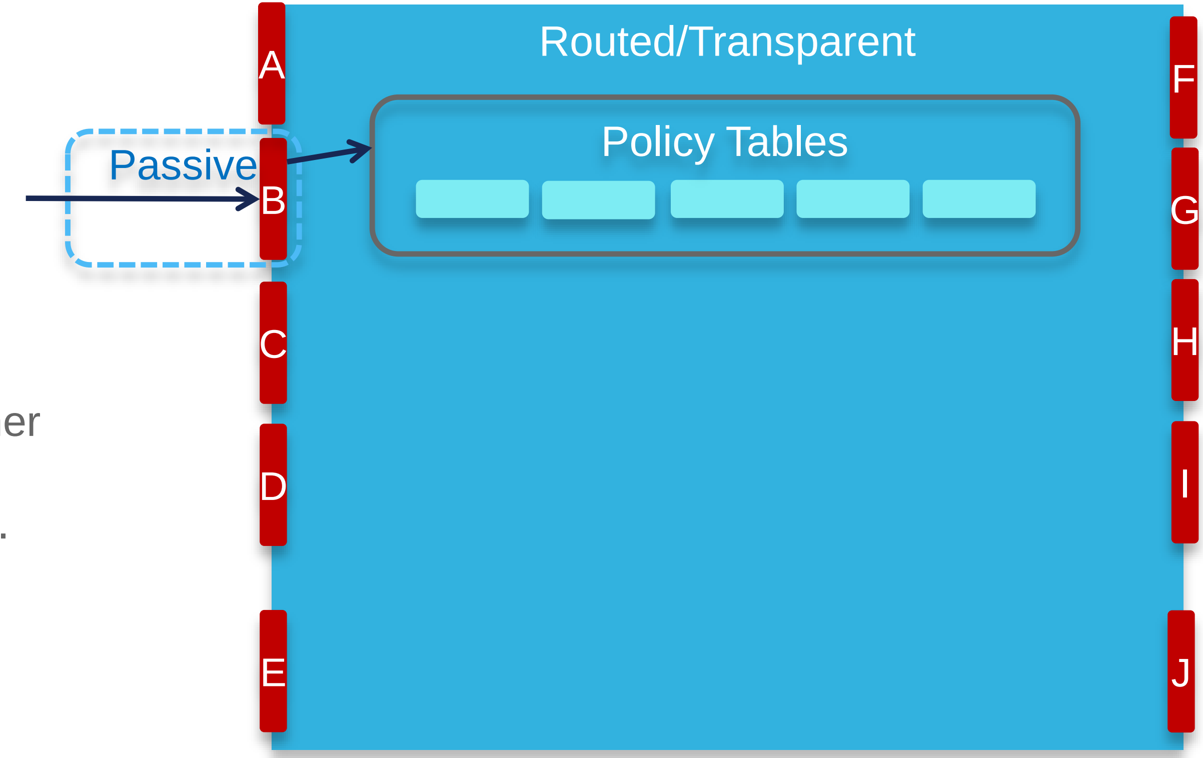
Transparent: Interfaces belong to different L2 networks (different VLANs).

FTD Interface Modes, continued…

Passive: A Promiscuous Interface receives copies of traffic from a SPAN port or TAP.

Passive interfaces are available regardless of whether the appliance is installed in Transparent or Routed mode.

Good POV Candidate!

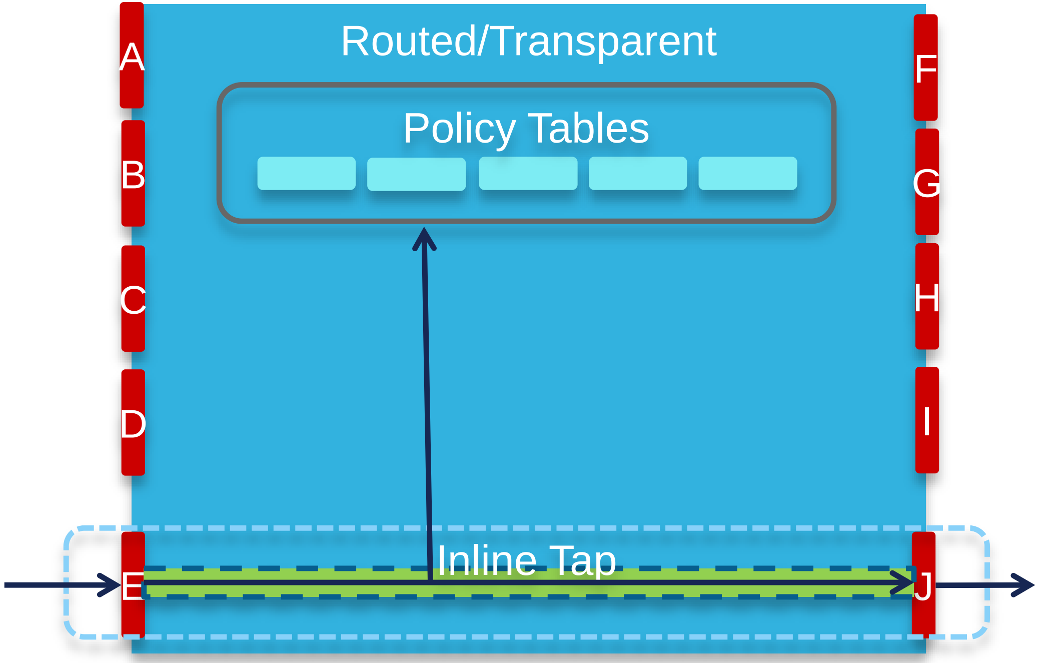


Firepower Threat Defense interface modes: Inline pair with tap

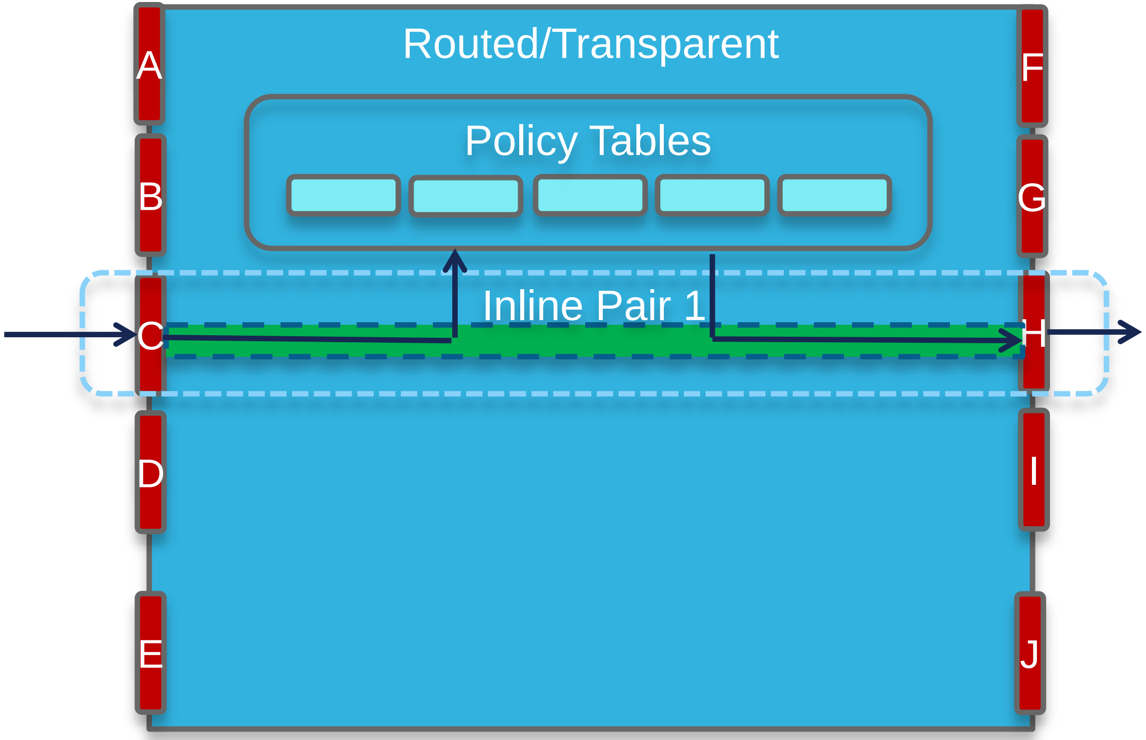
Inline TAP: Traffic passes from one member interface to another, without changing either VLAN or L3 network. As traffic passed, it is copied to the inspection engine, so traffic cannot be blocked.

Inline Pairs are available regardless of whether the appliance is installed in Transparent or Routed mode.

Good POV Candidate!



FTD Interface Modes, continued…

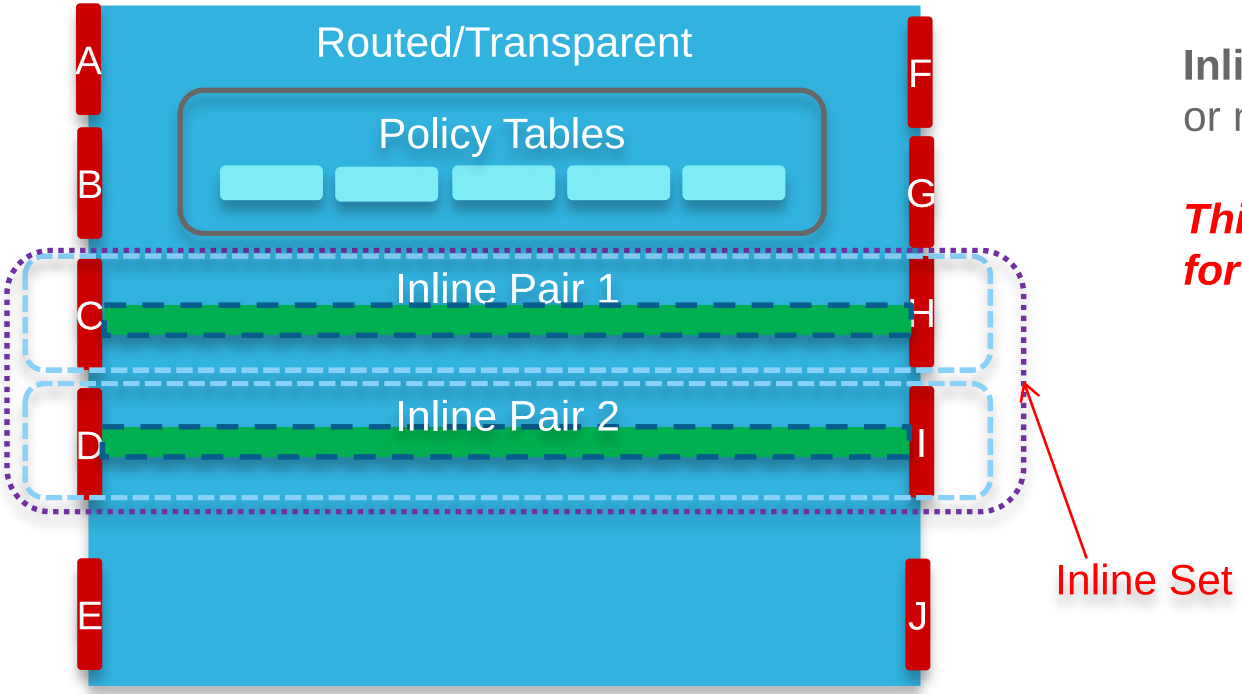


Inline Pair: Traffic passes from one member interface to another, without changing either VLAN or L3 network. It functions as a smart wire.

Inline Pairs are available regardless of whether the appliance is installed in Transparent or Routed mode.

This is not a good candidate for most POVs. – TAC!

FTD Interface Modes, continued…



Inline Set: A grouping of two or more Inline Pairs.

This is not a good candidate for most POVs.

Prerequisites

Hardware Prerequisites

1. Firepower Management Console (FMC) hardware or ESXi server for virtual Management Center. Another alternative for FMC is using dCloud. Just be aware that dCloud is a shared resource, and likely will perform slower than a virtual or physical appliance.

2. Hardware ASA or Firepower appliance for FTD (or ESXi server for virtual)

- ASA 5506-X, 5508-S, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X, or 5555-X
- FP-4110, 4120, 4140, or 4150
- FP-9300 with at least one Security Module

Have your customer setup the FirePOWER manager prior to showing up on site to avoid delays from provisioning IT resources.

Other Prerequisites

- One (1) IP address for FMC
- One (1) IP address for FTD
- Default Gateway
- Netmask
- Domain Name
- DNS Information
- SMTP Gateway
- NTP (unless using the default external NTP servers)

Optional Prerequisites

LDAP Connection (from FMC):

- 1-2 AD Service IP addresses or hostnames
- Username and Password to pull AD information
- Context where users are located (via DN)

User Agent:

- Windows system to install user agent
- Username and Password with privileges to access Security Logs

ISE:

- ISE 2.0 or 2.1 can be used as an alternate identity source instead of User Agent.

Qualify if you need this! Many PoVs do not and it reduces risk without this!

Login Information

Default Username and Password for FTD is:

- Username – admin
- Password - Admin123

You will change these during the installation. Make sure you record the new password!

Traffic Prerequisites

Required Ports for Cloud Connectivity and Automatic Updates

-	443	HTTPS/AMPQ	TCP	Outbound
-	80	HTTP	TCP	Outbound
-	32137	AMP	TCP	Outbound (Optional port. Default is now 443)
-	123	NTP	UDP	Outbound
-	443	URL Database Updates	TCP	Outbound to database.brightcloud.com
-	80	URL Unknown Lookups	TCP	Outbound to service.brightcloud.com

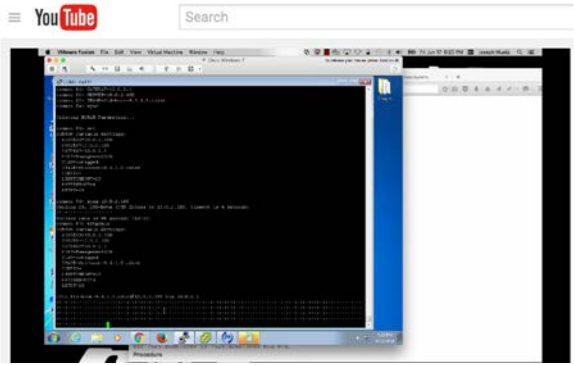
Required Ports for Internal Connectivity

-	8305	Sensor Comm.	TCP	Bidirectional
-	53	DNS	TCP/UDP	Outbound
-	22	SSH	TCP	Bidirectional
-	514	Syslog	UDP	Outbound
-	3306	User Agent	TCP	Bidirectional
-	443	HTTPS	TCP	Bidirectional
-	25	SMTP	TCP	Outbound
-	8302	eStreamer	TCP	Bidirectional

PoV Prerequisites Best Practices Summary

- First provide a demo aka “workshop”.
- Delivery a BOM to assure budget.
- Develop list of what still needs to be proved.
- Commit that if you prove, they buy
- If onsite, send information to setup FMC and publish FMC software
- Gather expected IP info / open firewall ports
- Pre-installation setup – Install software to point of requesting IP info
- Go onsite

PoV Documentation and VoDs



Everything you need for PoVs

https://communities.cisco.com/docs/DOC-65405

How to setup FirePOWER manager using ESXI

http://www.thesecurityblogger.com/installing-cisco-sourcefire-firesight-defense-center-on-esxi/

Solution PoVs + Other Uses

- **FirePOWER + ISE/Stealthwatch** = Add an additional VM(s) to include the better together story
- **FirePOWER security assessment** = Goal to deliver “risk report” to show current threats and areas of concern. **Free security assessment!**

Install
Firepower Management Console (FMC)

Install FMC

Ideally, you will already have the FMC software installed on the hardware or virtual appliance. If not, follow the instructions in the Installation Guide to install on ESXi.

Please note FMC needs to be at a software version equal or greater than the version of FTD you'll be installing on the appliance.

Instructions provided here use the Virtual FMC as the example.

Install FMC, continued…

1. Download the Installation File. It will be large (greater than 1.7GB).

2. Extract the file, and deploy the OVF. This will take about 5-20 minutes, depending on the server.

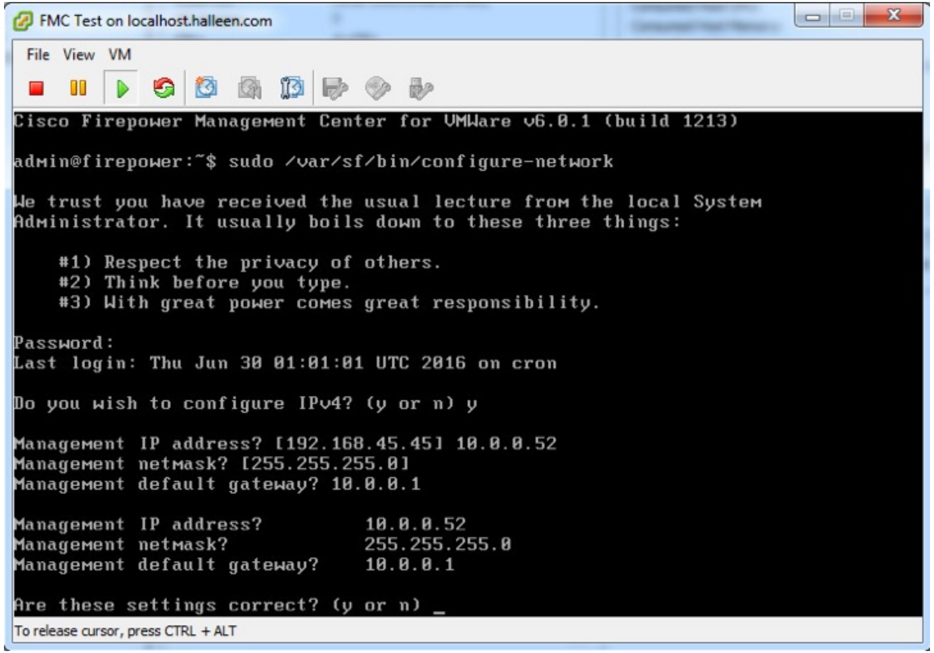
3. Start the new FMC virtual machine, and open a console. This part of the installation will take a long time - possibly more than 1 hour. It would be good to go through the first three steps prior to beginning the POV.

Install FMC, continued…

4. At the command prompt, login as “admin”. The default password is “Admin123”

5. Configure the network settings by entering:

```
sudo /var/sf/bin/configure-network
```



```
Cisco Firepower Management Center for VMWare v6.0.1 (build 1213)

admin@firepower:~$ sudo /var/sf/bin/configure-network

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
Last login: Thu Jun 30 01:01:01 UTC 2016 on cron

Do you wish to configure IPv4? (y or n) y

Management IP address? [192.168.45.45] 10.0.0.52
Management netmask? [255.255.255.0]
Management default gateway? 10.0.0.1

Management IP address?          10.0.0.52
Management netmask?             255.255.255.0
Management default gateway?     10.0.0.1

Are these settings correct? (y or n) _
```

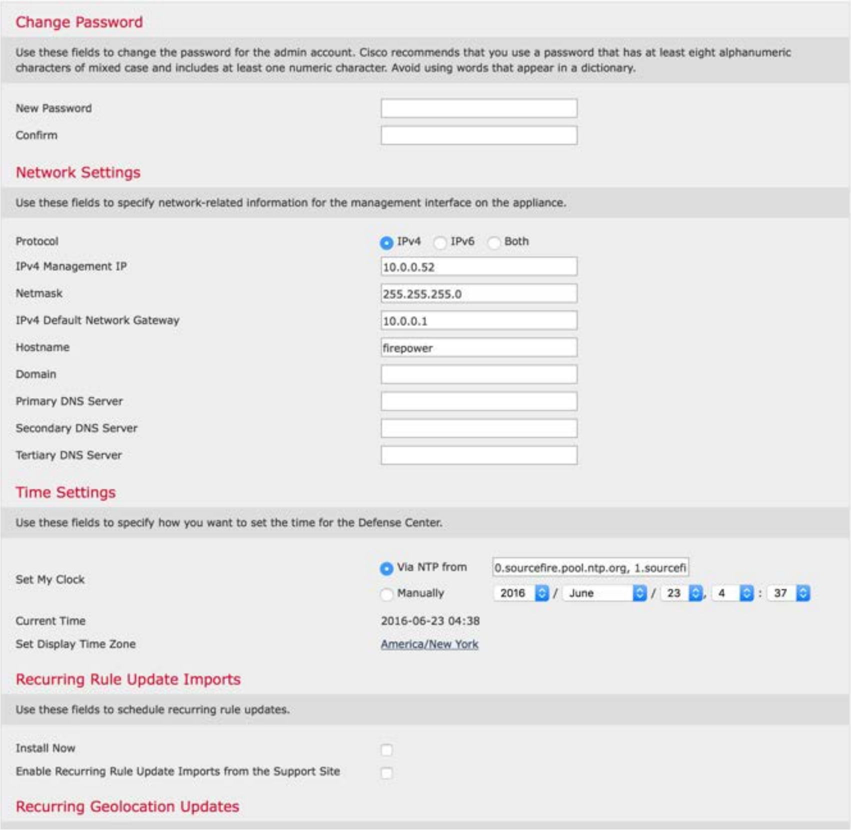
To release cursor, press CTRL + ALT

Install FMC, continued…

6. Login to the FMC using a web browser by going to:
   https://[ip address of FMC]

7. Change the admin user password and complete the network settings. Remember to also change the time zone.

8. You do NOT need to configure any of the updates at this time, and you also do not need a license key beginning with FMC 6.0.



Change Password

Use these fields to change the password for the admin account. Cisco recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password	
Confirm	

Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

Protocol	● IPv4 ○ IPv6 ○ Both
IPv4 Management IP	10.0.0.52
Netmask	255.255.255.0
IPv4 Default Network Gateway	10.0.0.1
Hostname	firepower
Domain	
Primary DNS Server	
Secondary DNS Server	
Tertiary DNS Server	

Time Settings

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock	● Via NTP from 0.sourcefire.pool.ntp.org, 1.sourcefi ○ Manually 2016 / June / 23, 4 : 37
Current Time	2016-06-23 04:38
Set Display Time Zone	America/New York

Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

Install Now	□
Enable Recurring Rule Update Imports from the Support Site	□

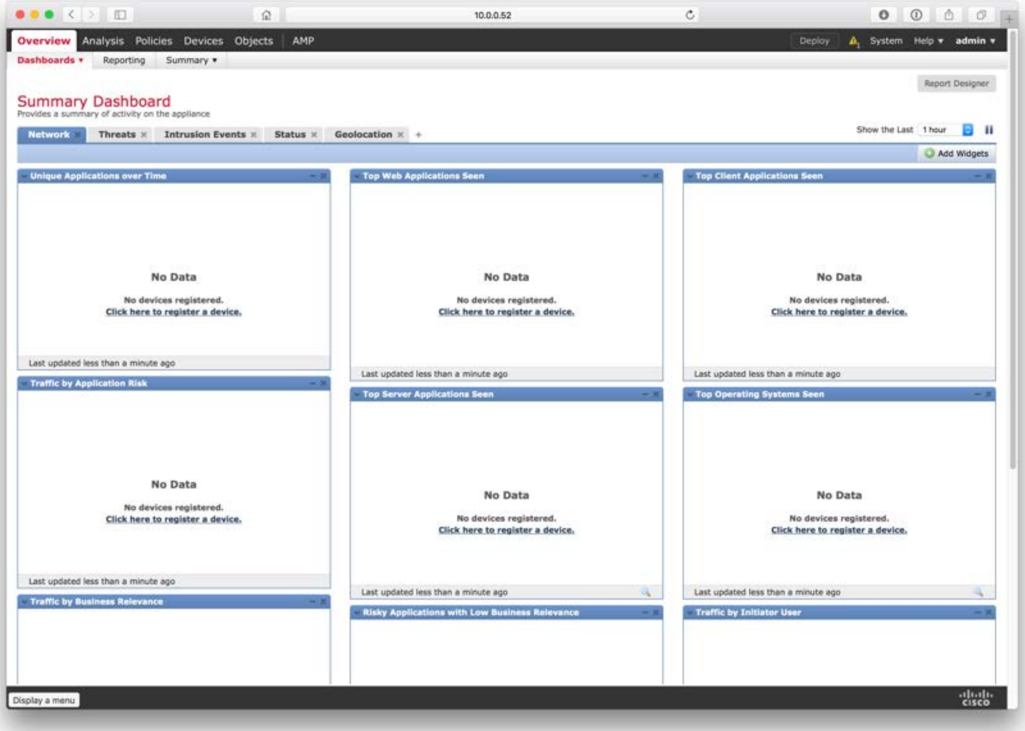
Recurring Geolocation Updates

Install FMC, continued…

7. You should be redirected after a few moments to the FMC Dashboard page. It should look like this.

8. Update FMC software to the latest patch, if one is available.

9. Now it is time to install the FTD appliance.



Summary Dashboard
Provides a summary of activity on the appliance

Unique Applications over Time No Data No devices registered. Click here to register a device. Last updated less than a minute ago	Top Web Applications Seen No Data No devices registered. Click here to register a device. Last updated less than a minute ago	Top Client Applications Seen No Data No devices registered. Click here to register a device. Last updated less than a minute ago
Traffic by Application Risk No Data No devices registered. Click here to register a device. Last updated less than a minute ago	Top Server Applications Seen No Data No devices registered. Click here to register a device. Last updated less than a minute ago	Top Operating Systems Seen No Data No devices registered. Click here to register a device. Last updated less than a minute ago
Traffic by Business Relevance	Risky Applications with Low Business Relevance	Traffic by Initiator User

FMC VM Performance Tips

The OVF file allocates 8GB of RAM and 4 CPUs for FMC, but this is not an optimal level for the best demo performance.

If your VMWare system has the resources to spare, the POV will perform better if you increase the values as below:

CPU: Change from 4 Virtual Sockets, 1 Core per Socket, to
4 Virtual Sockets, 2 Cores per Socket.

RAM: Change from 8GB, to 16GB or more.

Install FTD

FTD Device Requirements

ASA-5512, 5515, 5525:

These devices need to have one SSD-120 installed. Newer appliances have these by default, but older ones will not.

ASA-5545 and 5555:

The devices need to have two SSD-120 installed. Newer appliances will have these by default, but older ones will not.

ASA-5506, 5508, 5516:

These devices need to have ROMMON 1.1.8 or later installed prior to installing any FTD software. Earlier versions of ROMMON are not able to boot into FTD. *These models must have the Management interface connected to the network.*

FTD Device Requirements, continued

FP-4100 and 9300:

These devices require FXOS 2.0.1 to be installed prior to installing FTD 6.1 software. FXOS is the software image used to configure that hardware platform itself. FTD is the security image that runs on top of it.

Verifying or Installing SSD

ASA-5512, 5515, 5525, 5545, and 5555 only

Verify SSDs are Installed

From the CLI on the ASA, execute the ‘show inventory’ command.

```
asafirewall# show inventory
Name: "Chassis", DESCR: "ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC"
PID: ASA5515           , VID: V03     , SN: FTX18451114

Name: "Storage Device 1", DESCR: "Model Number: Micron_M550_MTFDDAK128MAY"
PID: N/A               , VID: N/A     , SN: MXA183701NW
```

If you do not see the 128 GB SSD installed (2 required for ASA-5545/5555), check to see if the SSD are installed by looking at the front of the ASA.

If it appears to be installed, but not showing on the screen, power off the ASA. Then pull the drive out and reinsert it. If it still does not show up, you’ll need to contact TAC.

Updating ROMMON

if necessary – ASA-5506, 5508, 5516 only

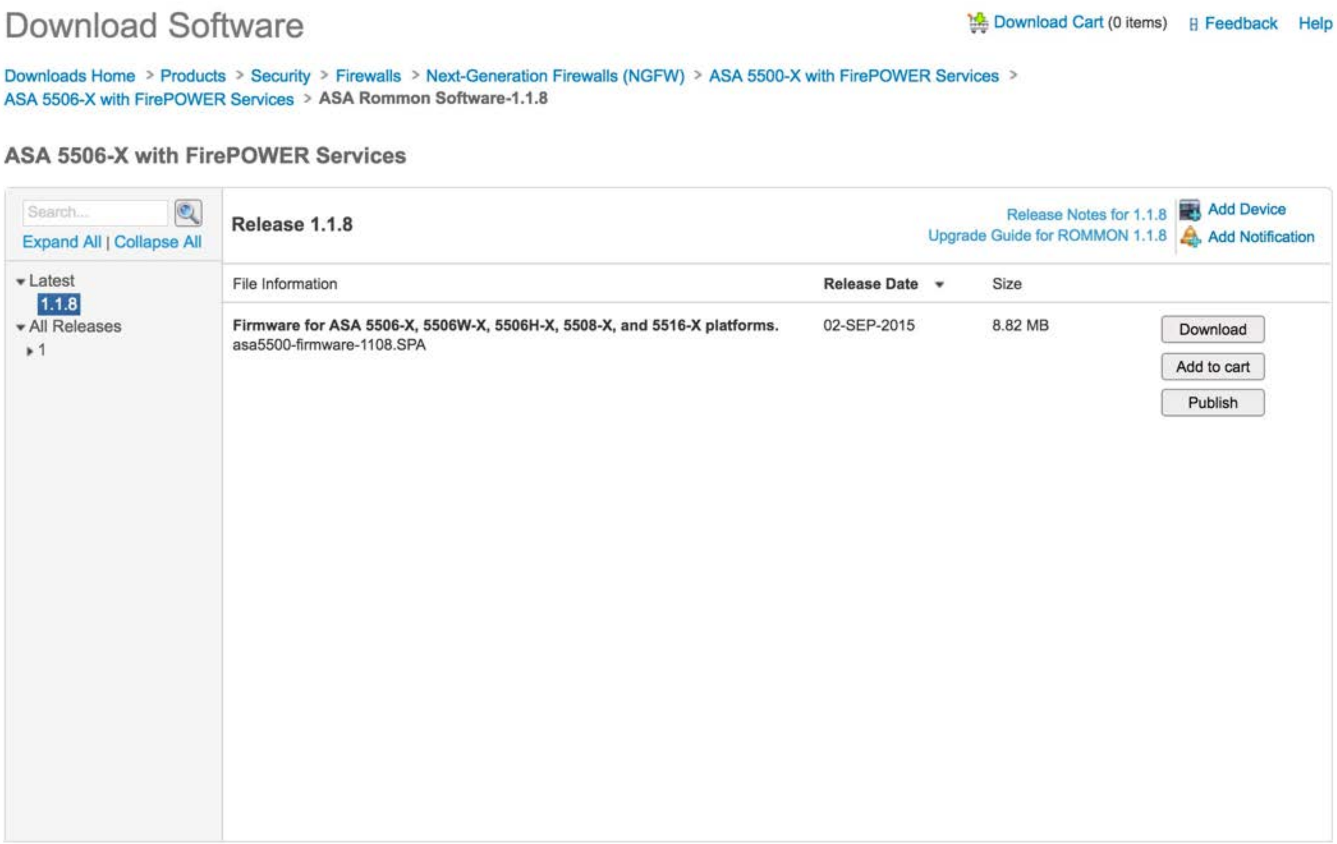
Verify ROMMON Version

From the CLI, execute the ‘show module’ command.

```
ciscoasa# show module
[...]
Mod MAC Address Range Hw Version Fw Version Sw Version
---- --------------------------------- ------------ ----------- ---------------
1 7426.aceb.ccea to 7426.aceb.ccf2 0.3 1.1.2 9.6(1)
sfr 7426.aceb.cce9 to 7426.aceb.cce9 N/A N/A
```

If the version show less than 1.1.8, you need to upgrade the ROMMON.

Download ROMMON



Download Software

Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > ASA 5500-X with FirePOWER Services > ASA 5506-X with FirePOWER Services > ASA Rommon Software-1.1.8

ASA 5506-X with FirePOWER Services

Release 1.1.8

File Information	Release Date	Size
Firmware for ASA 5506-X, 5506W-X, 5506H-X, 5508-X, and 5516-X platforms. asa5500-firmware-1108.SPA	02-SEP-2015	8.82 MB

Upgrade ROMMON

Copy the new ROMMON file to the ASA using the 'copy' command. Here is an example using FTP (but other protocols, like TFTP or HTTP can also be used):

```
ciscoasa# copy ftp://admin:test@10.0.0.6/asa5500-firmware-1108.SPA disk0:asa5500-
firmware-1108.SPA
```

Perform the upgrade:

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
```

Reboot is required afterward. Verify the ASA is now using the correct ROMMON.

Installing FTD on ASA Appliances

Installation Notes:

These steps are applicable in each of these conditions:

- New ASA
- Existing ASA with IPS, CX, or SFR virtual module

Please note, if installing on customer-owned ASA or ASA+SFR that FTD is a destructive installation. All existing configuration information, images, and licenses will be overwritten.

ASAs with IPS, CX, or SFR virtual modules do **not** need the modules to be uninstalled first. However the FTD installation will remove them.

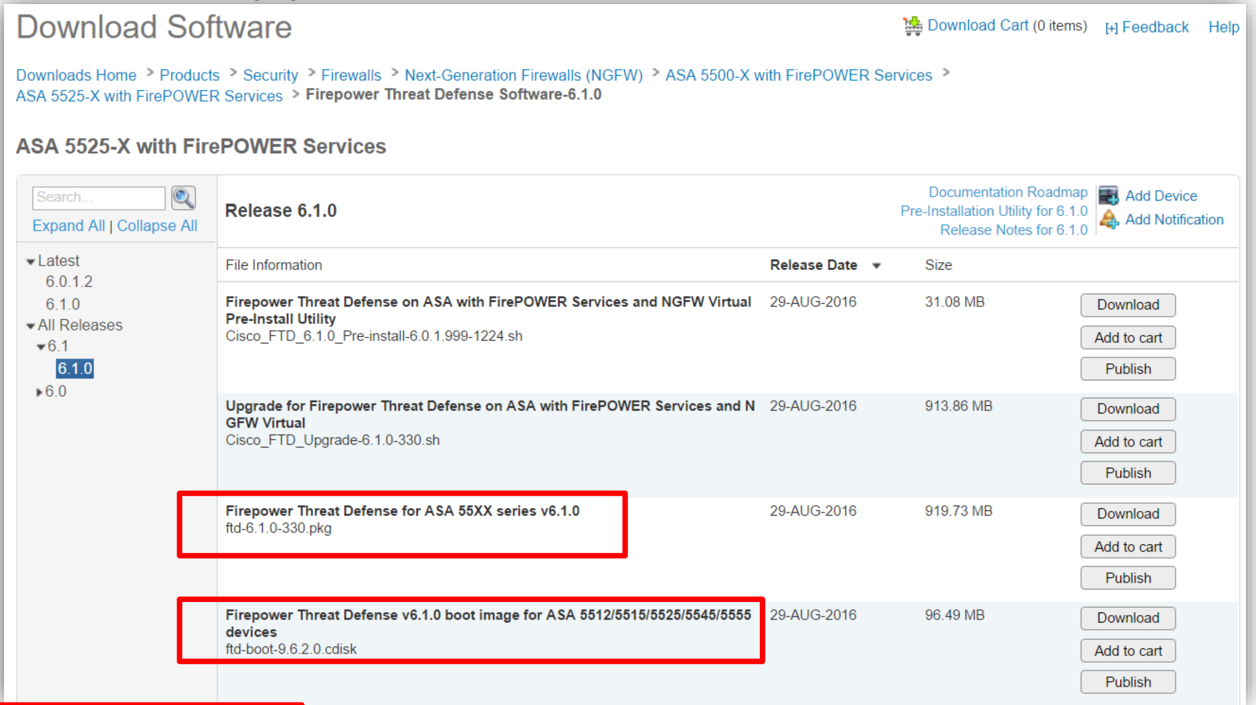
Download Boot and System Images

Installation of FTD on an ASA is a two-step process.

1. Install Boot Image
2. Install System Image

The Boot Image will need to be on a TFTP Server.

The System Image will need to be on a HTTP or FTP Server.



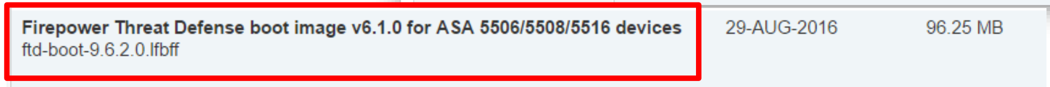
Download Software

Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > ASA 5500-X with FirePOWER Services > ASA 5525-X with FirePOWER Services > **Firepower Threat Defense Software-6.1.0**

ASA 5525-X with FirePOWER Services

Release 6.1.0

File Information	Release Date	Size
Firepower Threat Defense on ASA with FirePOWER Services and NGFW Virtual Pre-Install Utility Cisco_FTD_6.1.0_Pre-install-6.0.1.999-1224.sh	29-AUG-2016	31.08 MB
Upgrade for Firepower Threat Defense on ASA with FirePOWER Services and NGFW Virtual Cisco_FTD_Upgrade-6.1.0-330.sh	29-AUG-2016	913.86 MB
Firepower Threat Defense for ASA 55XX series v6.1.0 ftd-6.1.0-330.pkg	29-AUG-2016	919.73 MB
Firepower Threat Defense v6.1.0 boot image for ASA 5512/5515/5525/5545/5555 devices ftd-boot-9.6.2.0.cdisk	29-AUG-2016	96.49 MB



Firepower Threat Defense boot image v6.1.0 for ASA 5506/5508/5516 devices ftd-boot-9.6.2.0.lfbff	29-AUG-2016	96.25 MB

Install Boot Image

Copy the boot image to the ASA.

1. Reboot the ASA, and interrupt the boot by hitting BREAK or ESC.

2. Connect an interface to the network. On ASA-5506/5508/5516, this must be the Management interface. On other ASA models, it can be any interface.

Install Boot Image, continued…

3. From ROMMON mode, install the Boot Image:

```
rommon #0> address 10.0.0.7
rommon #1> server 10.0.0.60
rommon #2> file ftd-boot-96.x.x.x.cdisk
rommon #3> ping 10.0.0.60
Sending 20, 100-byte ICMP Echoes to 10.0.0.60, timeout is 4
seconds:
?!!!!!!!!!!!!!!!!!!!
Success rate is 95 percent (19/20)
rommon #4> set
ROMMON Variable Settings:
  ADDRESS=10.0.0.7
  SERVER=10.0.0.60
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=ftd-boot-96.x.x.x.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #5> sync

Updating NVRAM Parameters...

rommon #6> tftp
```

‘interface’ is not required on ASA-5506/5508/5516
‘address’ is the temporary IP address of the ASA.
’server’ should be your TFTP Server, containing the boot image.
‘gateway’ is only needed if the ASA and TFTP server are on different networks.
‘file’ is the FTD Boot Image you downloaded from CCO.

On the ASA-5506/5508/5516, the boot file will end with .lfbff
On other ASA-5500-X, the boot file will end with .cdisk

When you type ‘tftp’, you file will copy from your server to the ASA and then you will reboot and wait for the boot image to load.

Install the System Image

After the ASA boots into the Boot Image, from CLI, type:

```
> setup
```

Follow the setup script:

```
 Cisco FTD Boot 6.0.0 (96.2.2.11)
              Type ? for list of commands
firepower-boot>setup


                Welcome to Cisco FTD Setup
                  [hit Ctrl-C to abort]
                Default values are inside []

Enter a hostname [firepower]: ftd-5506
Do you want to configure IPv4 address on management interface?(y/n) [Y]:
```

Install the System Image, continued…

Install the System Image:

```
firepower-boot>system install noconfirm http://10.0.0.129/ftd-6.1.0-xxx.pkg

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

Do you want to continue? [y/N] y
Erasing disk0 ...
Verifying
Downloading ...
```

If you don’t add ‘noconfirm’ the install will timeout unless you are watching the console and answer the prompt (about 5-10 minutes into the installation):

```
Package Detail
        Description:                    Cisco ASA-FTD 6.1.0-xxx System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]:
```

Install the System Image, continued…

Login, Accept the EULA:

```
firepower login: admin
Password:
You must accept the EULA to continue.
Press <ENTER> to display the EULA:

(press the spacebar 17 times to scroll through 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:
```

Remember, the default login/password is admin/Admin123

OR, press “Q” to jump to end of EULA

Create a new password now.

Install the System Image, continued…

Setup Script launches automatically:

```
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]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.0.0.6
Enter an IPv4 netmask for the management interface [255.255.255.0]:
Enter the IPv4 default gateway for the management interface [192.168.45.1]: 10.0.0.1
Enter a fully qualified hostname for this system [firepower]: ftd-5506
Enter a comma-separated list of DNS servers or 'none' []: 10.0.0.114,10.0.0.115,10.0.0.116
Enter a comma-separated list of search domains or 'none' []: example.com
If your networking information has changed, you will need to reconnect.
```

Install the System Image, continued…

Finalize installation:

```
Manage the device locally? (yes/no) [yes]:
Configuring firewall mode to routed
```

In most POVs, you will not want to manage the device locally, and will want to use FMC instead.

Local Management is used mainly for small-customer firewall deployments where simplicity is more important than visibility, and where IPS or AMP is **not** a focus.

In POV deployments, using SPAN and Inline-TAP modes, it doesn’t matter whether the firewall is configured in Routed or Transparent mode. Routed is the default.

Installing FTD on FP-4100 or 9300

Installation Notes:

These steps are applicable in each of these conditions:

- New 4100 or 9300
- Existing 4100 or 9300 with no images assigned to security modules

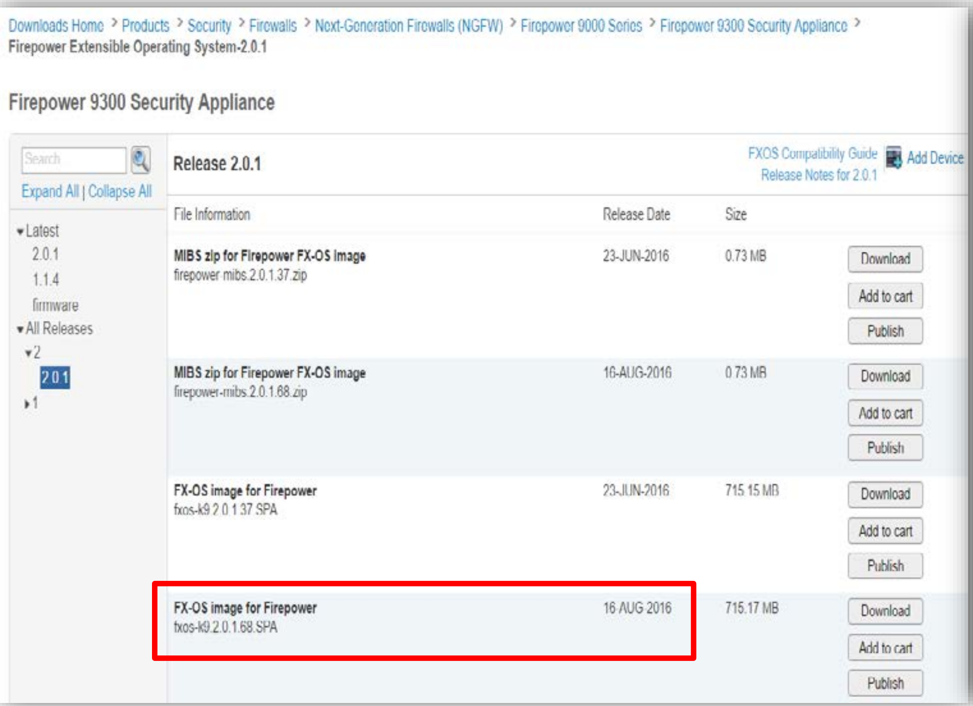
The initial configuration steps performed via the console will allow for access into the Firepower Chassis Manager GUI.

Firepower Chassis Manager is used for the management of the FX-OS supervisor and well as the orchestration of the security module(s), including interface allocation as well as image assignment (ASA or FTD).

If Password Recovery is needed for FX-OS, please follow the TechZone article here.

Download FX-OS and FTD images for 9300

FX-OS 2.0.1 is needed for compatibility with FTD 6.1.



Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 9000 Series > Firepower 9300 Security Appliance >
Firepower Extensible Operating System-2.0.1

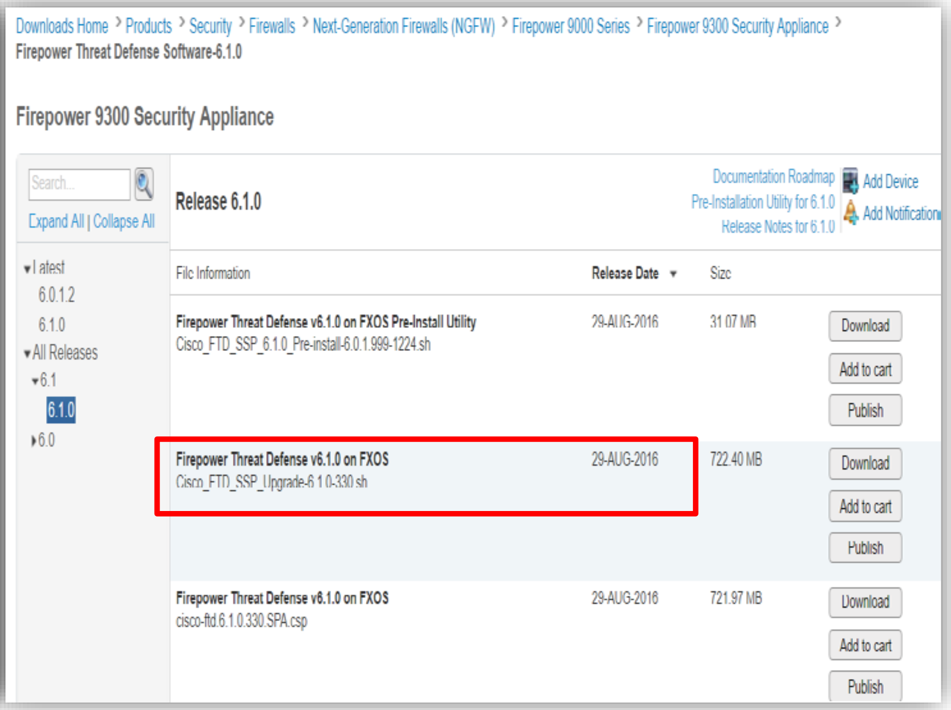
Firepower 9300 Security Appliance

- Latest
  - 2.0.1
  - 1.1.4
  - firmware
- All Releases
  - 2
    - 2.0.1
  - 1

Release 2.0.1

FXOS Compatibility Guide
Release Notes for 2.0.1

File Information	Release Date	Size
MIBS zip for Firepower FX-OS Image firepower-mibs.2.0.1.37.zip	23-JUN-2016	0.73 MB
MIBS zip for Firepower FX-OS image firepower-mibs.2.0.1.68.zip	16-AUG-2016	0.73 MB
FX-OS image for Firepower fxos-k9.2.0.1.37.SPA	23-JUN-2016	715.15 MB
FX-OS image for Firepower fxos-k9.2.0.1.68.SPA	16-AUG-2016	715.17 MB



Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 9000 Series > Firepower 9300 Security Appliance >
Firepower Threat Defense Software-6.1.0

Firepower 9300 Security Appliance

- Latest
  - 6.0.1.2
  - 6.1.0
- All Releases
  - 6.1
    - 6.1.0
  - 6.0

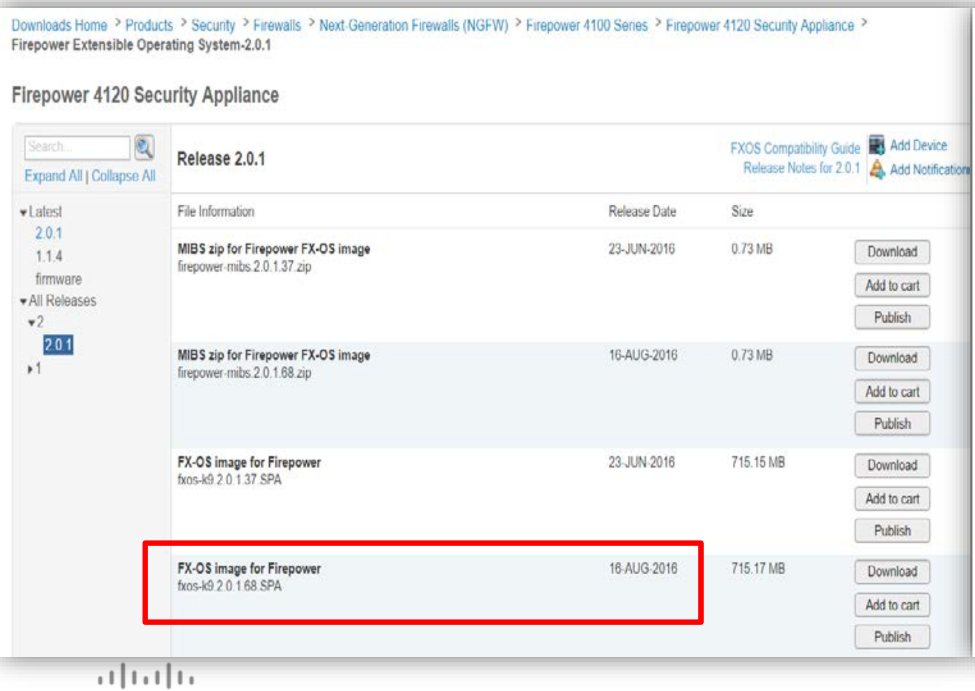
Release 6.1.0

Documentation Roadmap
Pre-Installation Utility for 6.1.0
Release Notes for 6.1.0

File Information	Release Date	Size
Firepower Threat Defense v6.1.0 on FXOS Pre-Install Utility Cisco_FTD_SSP_6.1.0_Pre-install-6.0.1.999-1224.sh	29-AUG-2016	31.07 MB
Firepower Threat Defense v6.1.0 on FXOS Cisco_FTD_SSP_Upgrade-6.1.0-330.sh	29-AUG-2016	722.40 MB
Firepower Threat Defense v6.1.0 on FXOS cisco-ftd.6.1.0.330.SPA.csp	29-AUG-2016	721.97 MB

Download FX-OS and FTD images for 4100 Series

FX-OS 2.0.1 is needed for compatibility with FTD 6.1.



Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 4100 Series > Firepower 4120 Security Appliance >
Firepower Extensible Operating System-2.0.1

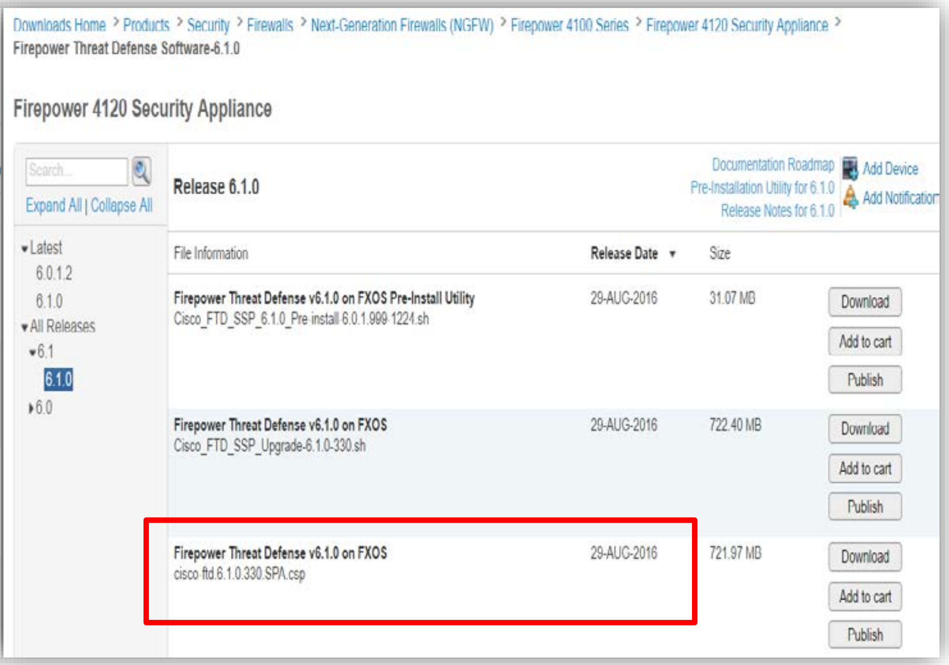
Firepower 4120 Security Appliance

Release 2.0.1

FXOS Compatibility Guide
Release Notes for 2.0.1

- Latest
  - 2.0.1
  - 1.1.4
  - firmware
- All Releases
  - 2
    - 2.0.1
  - 1

File Information	Release Date	Size
MIBS zip for Firepower FX-OS image firepower-mibs.2.0.1.37.zip	23-JUN-2016	0.73 MB
MIBS zip for Firepower FX-OS image firepower-mibs.2.0.1.68.zip	16-AUG-2016	0.73 MB
FX-OS image for Firepower fxos-k9.2.0.1.37.SPA	23-JUN-2016	715.15 MB
FX-OS image for Firepower fxos-k9.2.0.1.68.SPA	16-AUG-2016	715.17 MB



Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 4100 Series > Firepower 4120 Security Appliance >
Firepower Threat Defense Software-6.1.0

Firepower 4120 Security Appliance

Release 6.1.0

Documentation Roadmap
Pre-Installation Utility for 6.1.0
Release Notes for 6.1.0

- Latest
  - 6.0.1.2
  - 6.1.0
- All Releases
  - 6.1
    - 6.1.0
  - 6.0

File Information	Release Date ▼	Size
Firepower Threat Defense v6.1.0 on FXOS Pre-Install Utility Cisco_FTD_SSP_6.1.0_Pre-install-6.0.1.999-1224.sh	29-AUG-2016	31.07 MB
Firepower Threat Defense v6.1.0 on FXOS Cisco_FTD_SSP_Upgrade-6.1.0-330.sh	29-AUG-2016	722.40 MB
Firepower Threat Defense v6.1.0 on FXOS cisco-ftd.6.1.0.330.SPA.csp	29-AUG-2016	721.97 MB

Initial configuration of FX-OS on new 4100/9300

Verify the following physical connections on the FXOS chassis:

–The console port is physically connected to a computer terminal or console server.
–The 1Gbps Ethernet management port is connected

Connect to the console port and power on FX-OS chassis. When an unconfigured system boots, a Setup Wizard prompt is presented requesting for information needed to manage the chassis.

*Detailed steps outlined in the FX-OS 2.x Configuration Guide here.

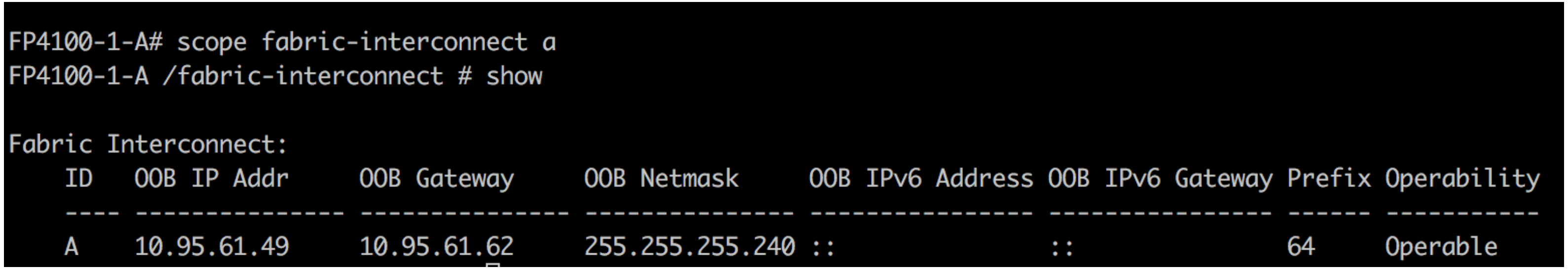
Initial configuration of FX-OS Example

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": <newpassword>
Confirm the password for "admin": <newpassword>
Enter the system name: FP4100-1
Physical Switch Mgmt0 IP address : 10.95.61.49
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.240
IPv4 address of the default gateway: 10.95.61.62
Configure the DNS Server IP address? (yes/no) [n]: yes
DNS IP address: 171.70.168.183
Configure the default domain name? (yes/no) [n]: yes
Default domain name: IrvineLab.demo

Following configurations will be applied:
Switch Fabric=A
System Name=FP4100-a
Enforce Strong Password=no
Physical Switch Mgmt0 IP Address=10.95.61.49
Physical Switch Mgmt0 IP Netmask=255.255.255.240
Default Gateway=10.95.61.62
IPv6 value=0
DNS Server=171.70.168.183
Domain Name=IrvineLab.demo
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

View Management IP of 4100/9300 Chassis

To view the current IPv4 management IP address:

- Set the scope for fabric-interconnect a:
- FP4100-1-A# **scope fabric-interconnect a**
- View the IP:
- FP4100-1-A /fabric-interconnect # **show**



```
FP4100-1-A# scope fabric-interconnect a
FP4100-1-A /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ---------------- ------ -----------
    A    10.95.61.49     10.95.61.62     255.255.255.240 ::               ::               64     Operable
```

Change Management IP of 4100/9300 Chassis

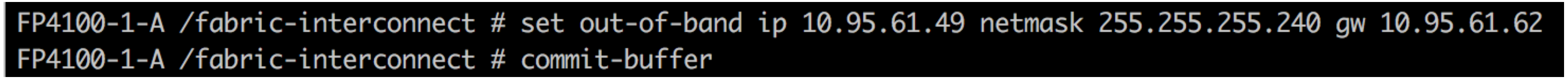
If the chassis was previously configured, the Setup wizard will not be displayed. The management IP address will need to be manually changed.

Enter the following command to configure a new management IP address and gateway:

FP4100-1-A /fabric-interconnect # **set out-of-band ip** <ip_address> **netmask** <network_mask> **gw** <gateway_ip_address>

Commit the transaction to the system configuration:

FP4100-1-A /fabric-interconnect # **commit-buffer**



```
FP4100-1-A /fabric-interconnect # set out-of-band ip 10.95.61.49 netmask 255.255.255.240 gw 10.95.61.62
FP4100-1-A /fabric-interconnect # commit-buffer
```

*Information about viewing and changing management IP available in FX-OS 2.x Configuration Guide here.

Access Firepower Chassis Manager

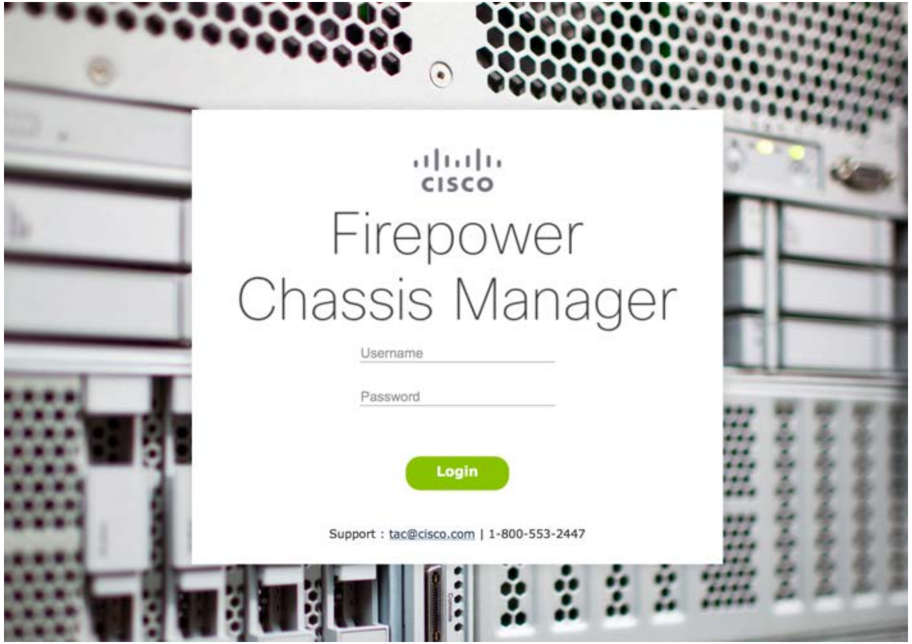
With Management IP defined, we will be using the Firepower Chassis Manager GUI to finish the configuration. Using a supported browser:

Mozilla Firefox – Version 42 and later
Google Chrome – Version 47 and later

enter the following URL in the address bar:

https://<*chassis_mgmt_ip_address*>

where <*chassis_mgmt_ip_address*> is the IP address of the FXOS chassis that you entered during initial configuration.

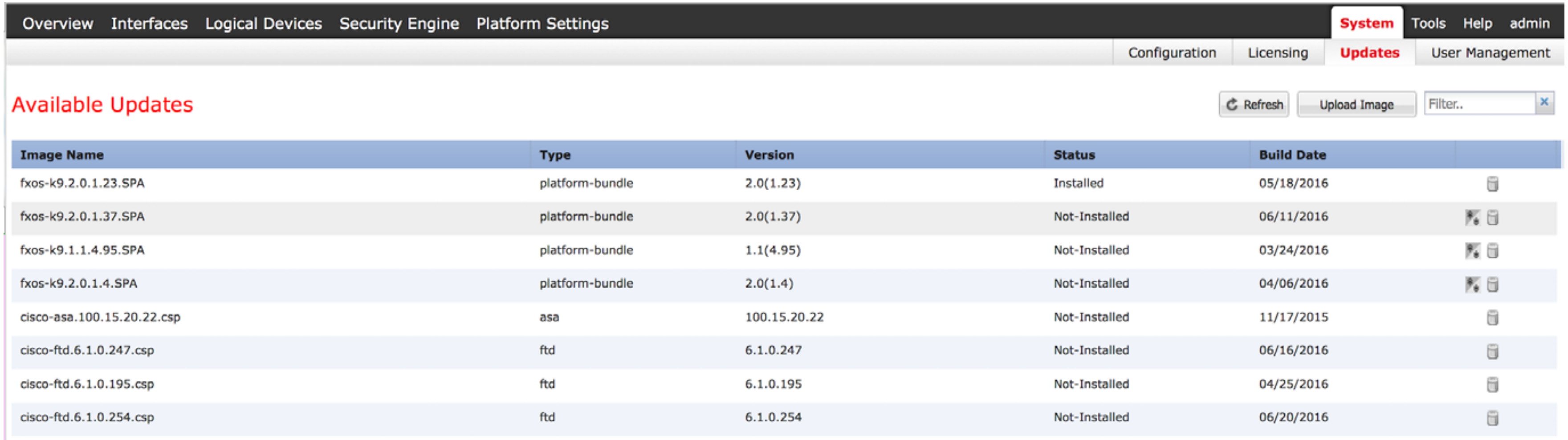


Firepower Chassis Manager

Support : tac@cisco.com | 1-800-553-2447

Upload FX-OS and FTD Images to FCM

From the FCM interface, go to System>Updates:

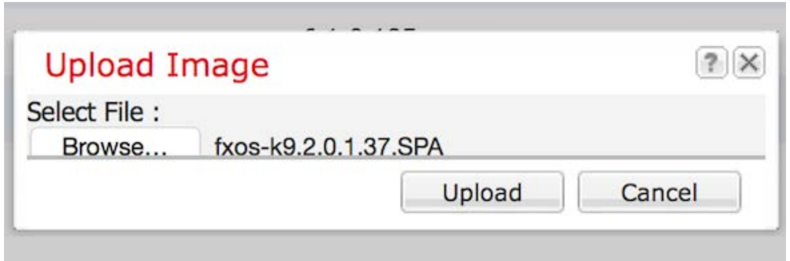


Available Updates

Image Name	Type	Version	Status	Build Date
fxos-k9.2.0.1.23.SPA	platform-bundle	2.0(1.23)	Installed	05/18/2016
fxos-k9.2.0.1.37.SPA	platform-bundle	2.0(1.37)	Not-Installed	06/11/2016
fxos-k9.1.1.4.95.SPA	platform-bundle	1.1(4.95)	Not-Installed	03/24/2016
fxos-k9.2.0.1.4.SPA	platform-bundle	2.0(1.4)	Not-Installed	04/06/2016
cisco-asa.100.15.20.22.csp	asa	100.15.20.22	Not-Installed	11/17/2015
cisco-ftd.6.1.0.247.csp	ftd	6.1.0.247	Not-Installed	06/16/2016
cisco-ftd.6.1.0.195.csp	ftd	6.1.0.195	Not-Installed	04/25/2016
cisco-ftd.6.1.0.254.csp	ftd	6.1.0.254	Not-Installed	06/20/2016

Upload FX-OS and FTD Images to FCM Cont’d

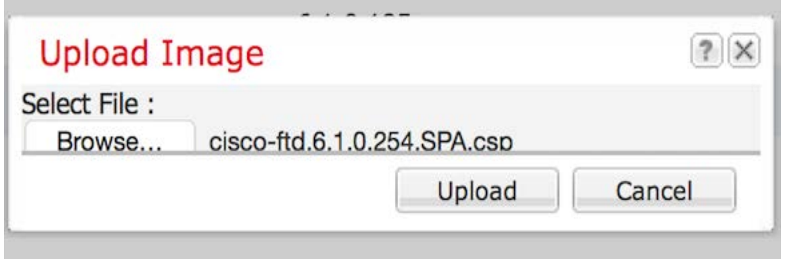
Click Upload Image, individually upload the FX-OS and FTD images



Upload Image

Select File :

fxos-k9.2.0.1.37.SPA



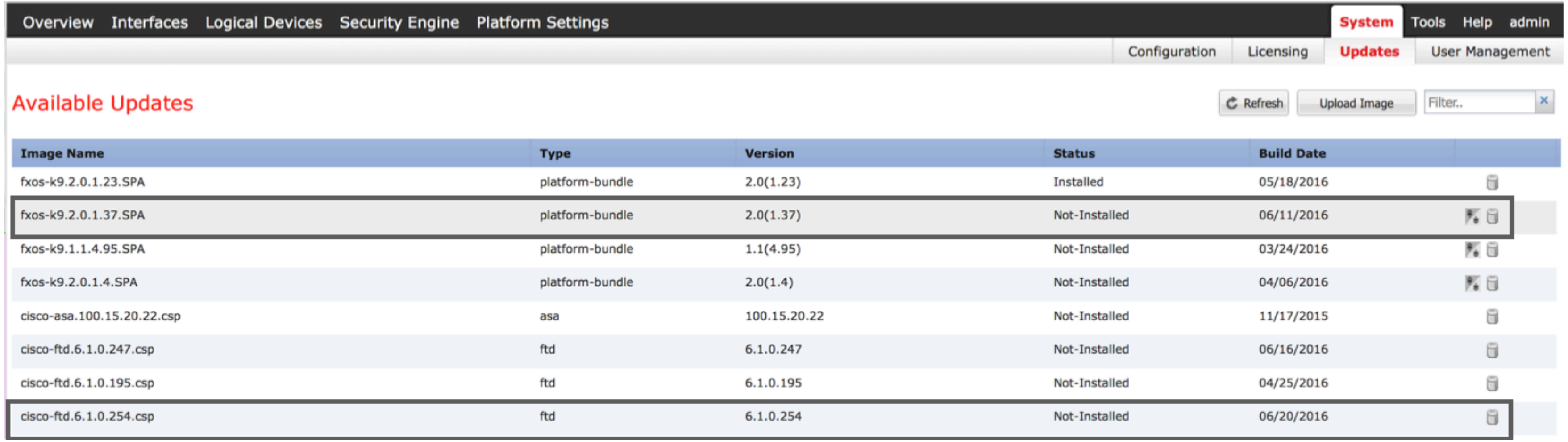
Upload Image

Select File :

cisco-ftd.6.1.0.254.SPA.csp

Upload FX-OS and FTD Images to FCM

Both images should now exist in FCM.

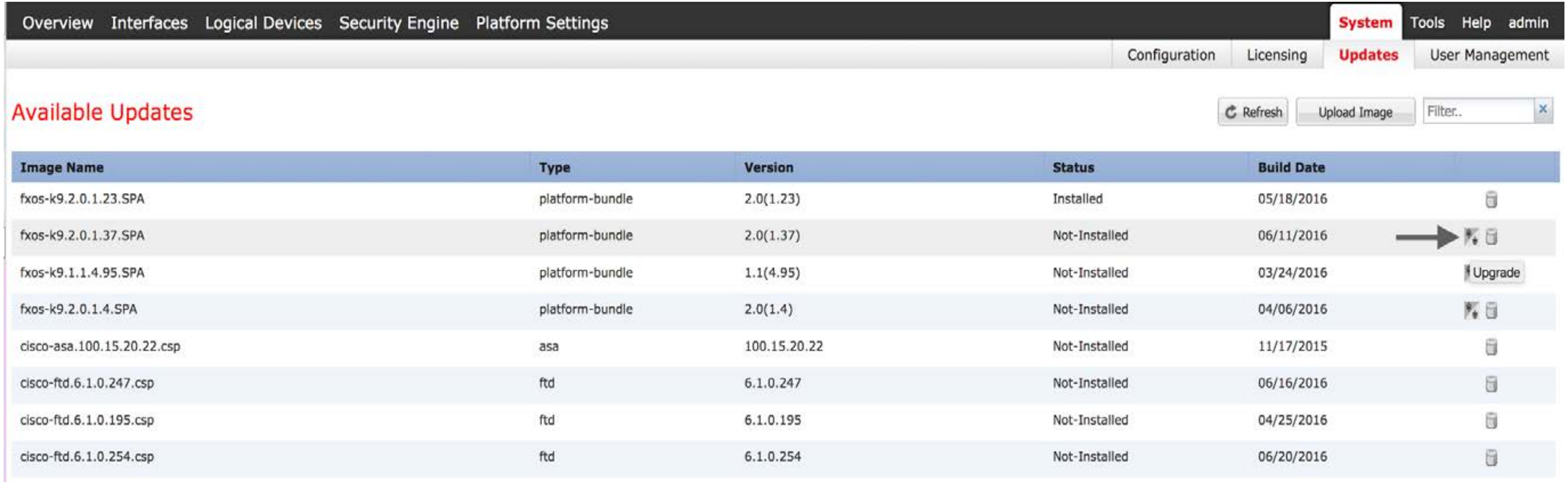


Available Updates

Image Name	Type	Version	Status	Build Date
fxos-k9.2.0.1.23.SPA	platform-bundle	2.0(1.23)	Installed	05/18/2016
fxos-k9.2.0.1.37.SPA	platform-bundle	2.0(1.37)	Not-Installed	06/11/2016
fxos-k9.1.1.4.95.SPA	platform-bundle	1.1(4.95)	Not-Installed	03/24/2016
fxos-k9.2.0.1.4.SPA	platform-bundle	2.0(1.4)	Not-Installed	04/06/2016
cisco-asa.100.15.20.22.csp	asa	100.15.20.22	Not-Installed	11/17/2015
cisco-ftd.6.1.0.247.csp	ftd	6.1.0.247	Not-Installed	06/16/2016
cisco-ftd.6.1.0.195.csp	ftd	6.1.0.195	Not-Installed	04/25/2016
cisco-ftd.6.1.0.254.csp	ftd	6.1.0.254	Not-Installed	06/20/2016

Upgrade FX-OS Image

2.0(1.23) is currently installed, we will upgrade to 2.0(1.37). Click the Upgrade icon next to the correct image.

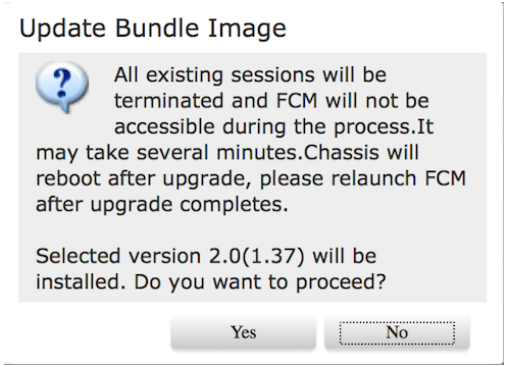


Available Updates

Image Name	Type	Version	Status	Build Date
fxos-k9.2.0.1.23.SPA	platform-bundle	2.0(1.23)	Installed	05/18/2016
fxos-k9.2.0.1.37.SPA	platform-bundle	2.0(1.37)	Not-Installed	06/11/2016
fxos-k9.1.1.4.95.SPA	platform-bundle	1.1(4.95)	Not-Installed	03/24/2016
fxos-k9.2.0.1.4.SPA	platform-bundle	2.0(1.4)	Not-Installed	04/06/2016
cisco-asa.100.15.20.22.csp	asa	100.15.20.22	Not-Installed	11/17/2015
cisco-ftd.6.1.0.247.csp	ftd	6.1.0.247	Not-Installed	06/16/2016
cisco-ftd.6.1.0.195.csp	ftd	6.1.0.195	Not-Installed	04/25/2016
cisco-ftd.6.1.0.254.csp	ftd	6.1.0.254	Not-Installed	06/20/2016

Upgrade FX-OS image Cont'd

Accept warning message.



Update Bundle Image

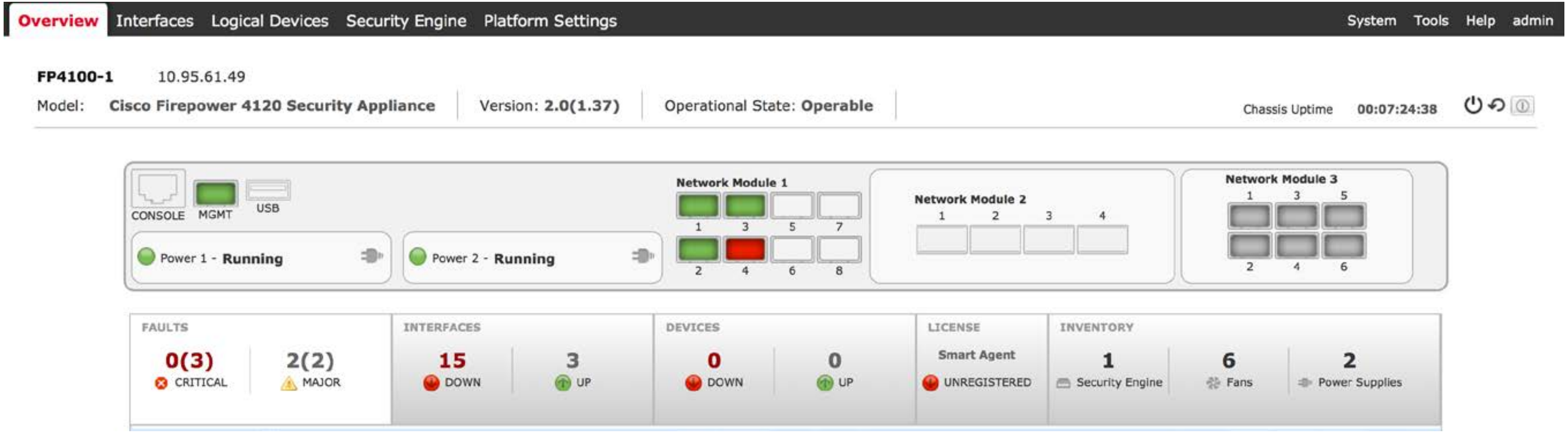
All existing sessions will be terminated and FCM will not be accessible during the process.It may take several minutes.Chassis will reboot after upgrade, please relaunch FCM after upgrade completes.

Selected version 2.0(1.37) will be installed. Do you want to proceed?

Upgrade might take a little time, so be patient.

FX-OS Upgrade Completed

The chassis will reboot to finish the upgrade. The Overview dashboard should now indicate the new FX-OS image version after logging back into FCM after the reboot.



FP4100-1 10.95.61.49

Model: Cisco Firepower 4120 Security Appliance | Version: 2.0(1.37) | Operational State: Operable

Chassis Uptime 00:07:24:38

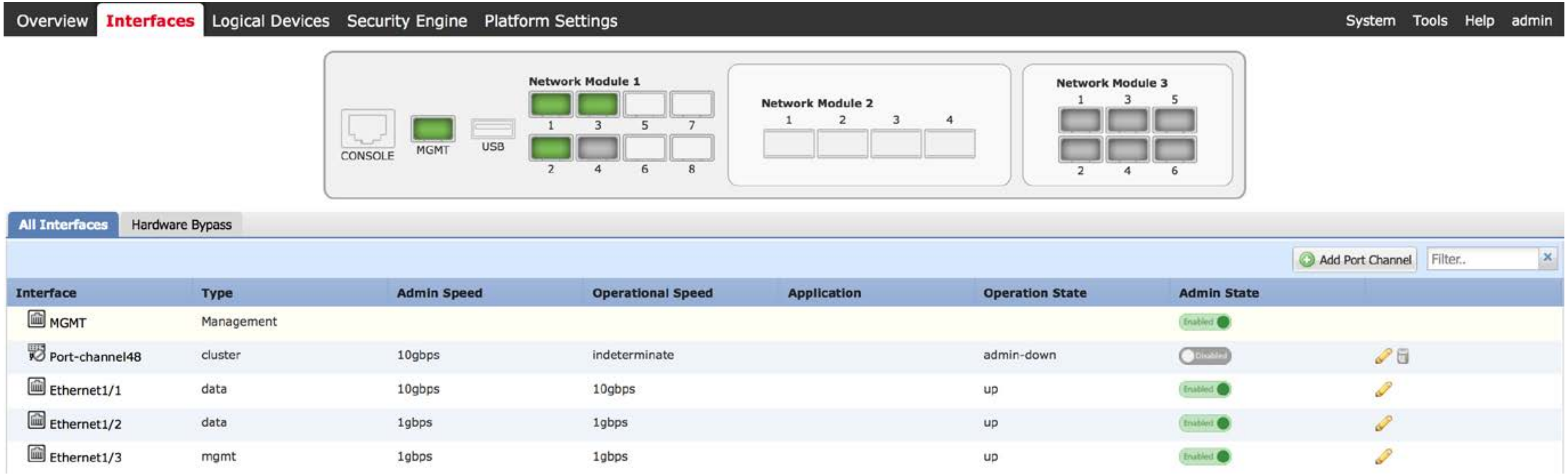
Power 1 - Running

Power 2 - Running

FAULTS		INTERFACES		DEVICES		LICENSE	INVENTORY		
0(3)	2(2)	15	3	0	0	Smart Agent	1	6	2
CRITICAL	MAJOR	DOWN	UP	DOWN	UP	UNREGISTERED	Security Engine	Fans	Power Supplies

Enable Interfaces that will be Assigned to FTD

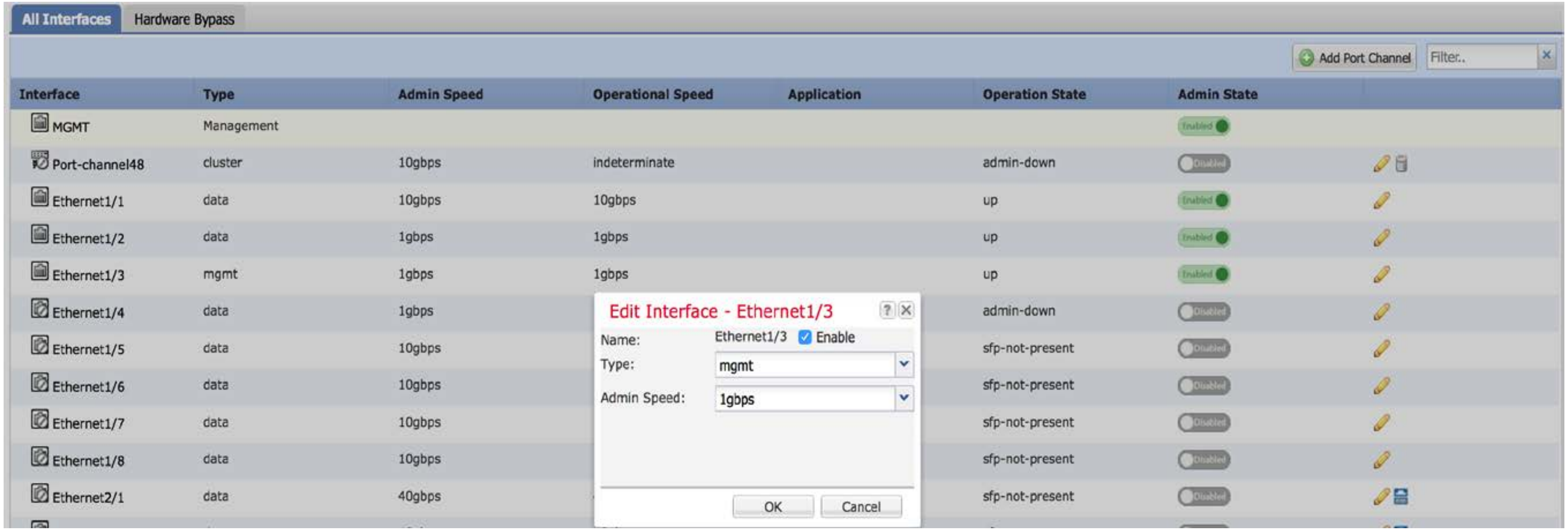
Under Interfaces, enable the interfaces that will be assigned to FTD. In this example, we will assign interfaces Ethernet 1/1 – 1/3 to FTD.



Interface	Type	Admin Speed	Operational Speed	Application	Operation State	Admin State
MGMT	Management					Enabled
Port-channel48	cluster	10gbps	indeterminate		admin-down	Disabled
Ethernet1/1	data	10gbps	10gbps		up	Enabled
Ethernet1/2	data	1gbps	1gbps		up	Enabled
Ethernet1/3	mgmt	1gbps	1gbps		up	Enabled

Configure interfaces, define one interface for FTD MGMT

Edit the interfaces to modify the speed and type of interface. One interface MUST be defined as MGMT for FTD (in this example Ethernet 1/3).



Interface	Type	Admin Speed	Operational Speed	Application	Operation State	Admin State
MGMT	Management					Enabled
Port-channel48	cluster	10gbps	indeterminate		admin-down	Disabled
Ethernet1/1	data	10gbps	10gbps		up	Enabled
Ethernet1/2	data	1gbps	1gbps		up	Enabled
Ethernet1/3	mgmt	1gbps	1gbps		up	Enabled
Ethernet1/4	data	1gbps			admin-down	Disabled
Ethernet1/5	data	10gbps			sfp-not-present	Disabled
Ethernet1/6	data	10gbps			sfp-not-present	Disabled
Ethernet1/7	data	10gbps			sfp-not-present	Disabled
Ethernet1/8	data	10gbps			sfp-not-present	Disabled
Ethernet2/1	data	40gbps			sfp-not-present	Disabled

Edit Interface - Ethernet1/3

Name: Ethernet1/3 ☑ Enable

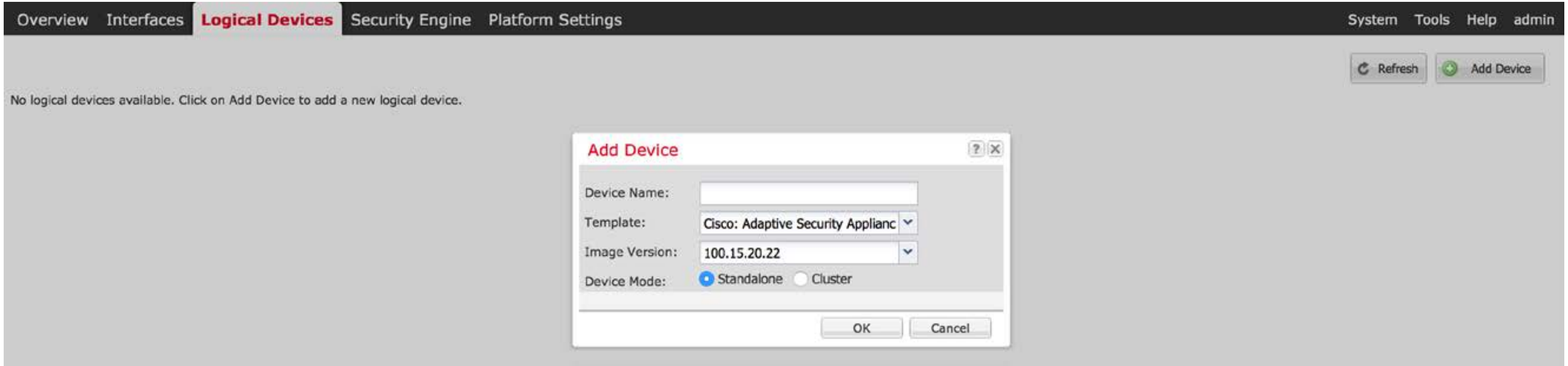
Type: mgmt

Admin Speed: 1gbps

OK Cancel

Assign FTD Image to the Security Module

Go to Logical Devices, click Add Device.



No logical devices available. Click on Add Device to add a new logical device.

Add Device

Device Name:

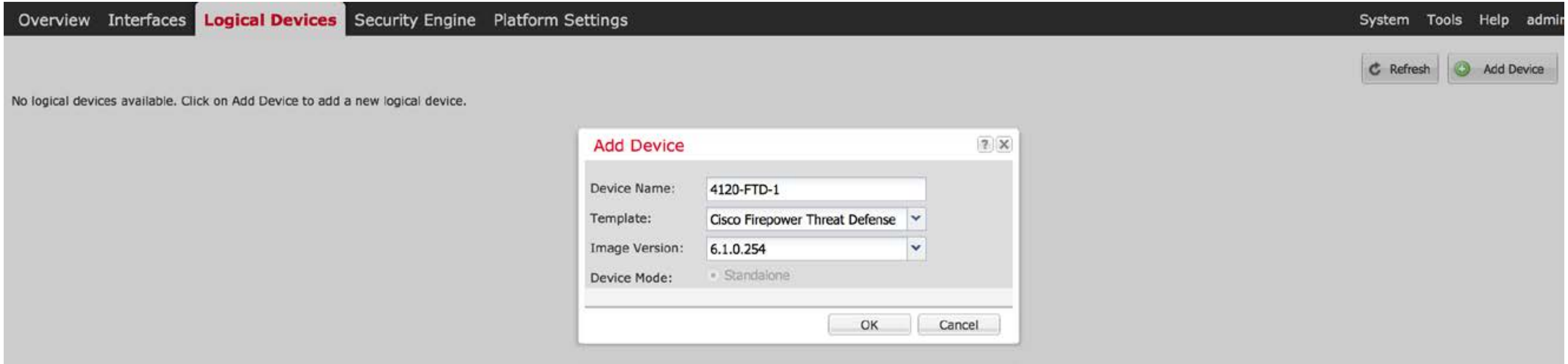
Template: Cisco: Adaptive Security Applianc

Image Version: 100.15.20.22

Device Mode: ● Standalone ○ Cluster

Assign FTD Image to the Security Module Cont’d

Assign a Device Name, choose Firepower Threat Defense as the Template, and select the FTD image version that was previously uploaded. Click OK, which will lead you to the Provisioning page.



No logical devices available. Click on Add Device to add a new logical device.

Add Device

Device Name: 4120-FTD-1

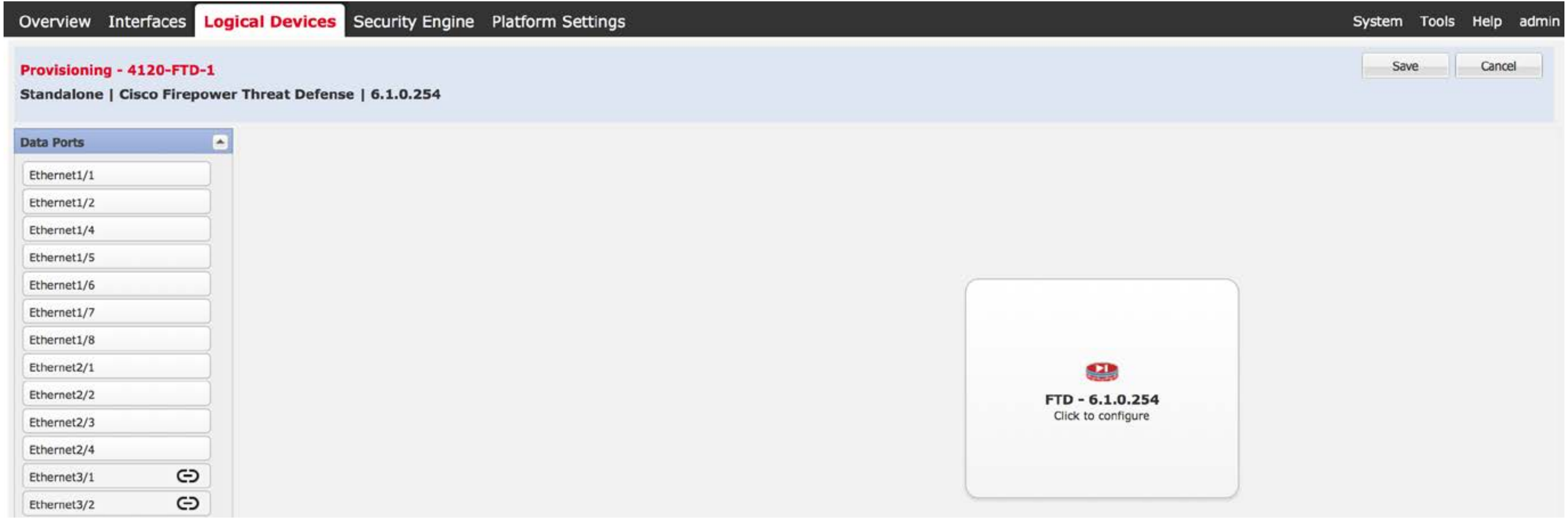
Template: Cisco Firepower Threat Defense

Image Version: 6.1.0.254

Device Mode: ○ Standalone

Assign Data Interfaces to the Security Module

In the Logical Devices Provisioning page, select interfaces under Data Ports to assign to this FTD instance. Notice that Ethernet1/3 is missing in this example, as it was previously changed from the default interface type of DATA to MGMT.



Provisioning - 4120-FTD-1

Standalone | Cisco Firepower Threat Defense | 6.1.0.254

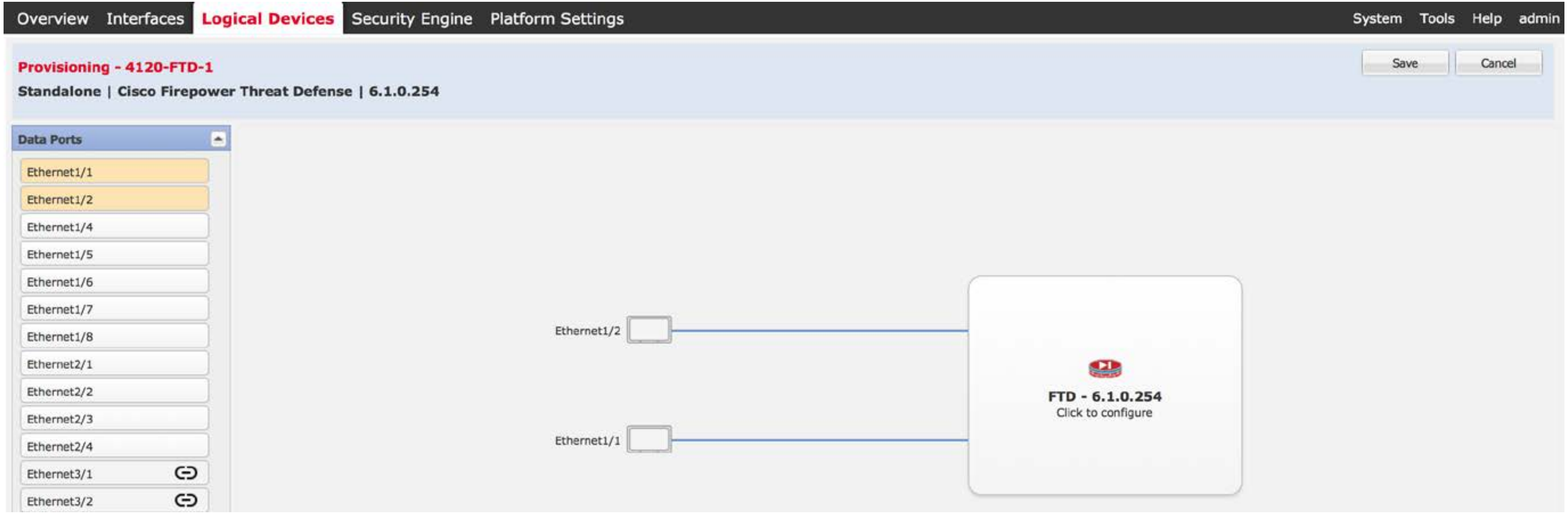
Data Ports

- Ethernet1/1
- Ethernet1/2
- Ethernet1/4
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet2/1
- Ethernet2/2
- Ethernet2/3
- Ethernet2/4
- Ethernet3/1
- Ethernet3/2

FTD - 6.1.0.254
Click to configure

Assign Data Interfaces to the Security Module Cont’d

Data Interfaces assigned (Ethernet 1/1 and 1/2).

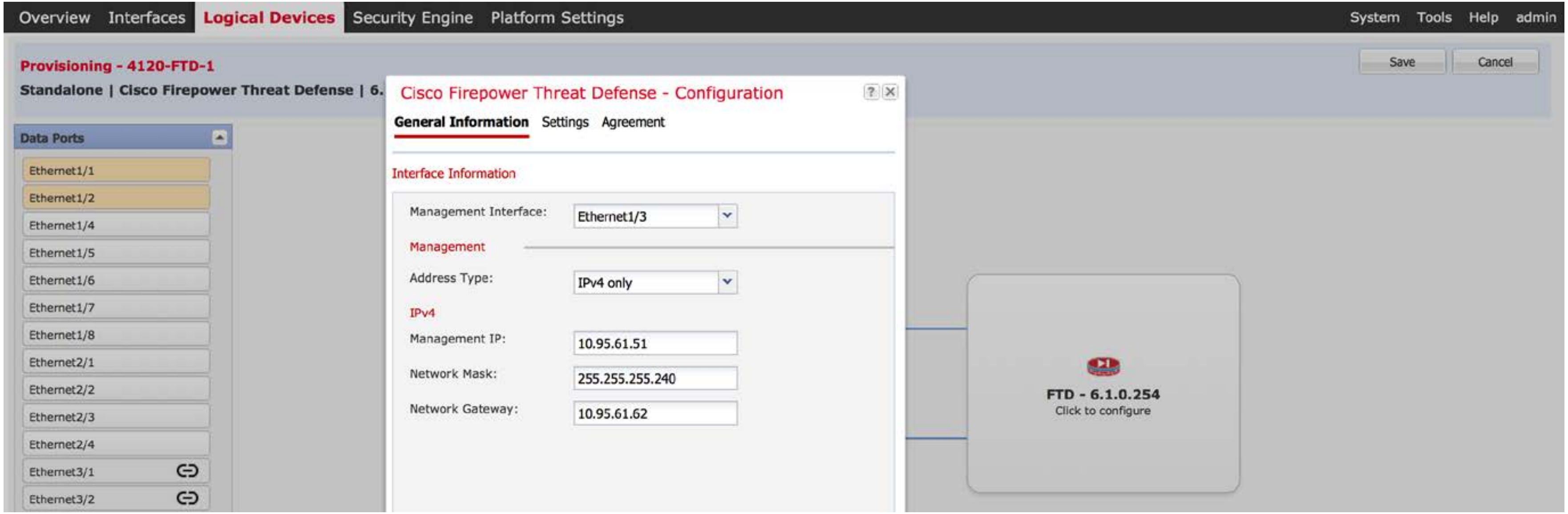


Provisioning - 4120-FTD-1

Standalone | Cisco Firepower Threat Defense | 6.1.0.254

Configure FTD Instance

Click on the FTD instance to configure the Management Interface as well as other settings. Under General Information, assign IP information to the Management Interface.



Provisioning - 4120-FTD-1

Standalone | Cisco Firepower Threat Defense | 6.

Cisco Firepower Threat Defense - Configuration

General Information | Settings | Agreement

Interface Information

Management Interface: Ethernet1/3

Management

Address Type: IPv4 only

IPv4

Management IP: 10.95.61.51

Network Mask: 255.255.255.240

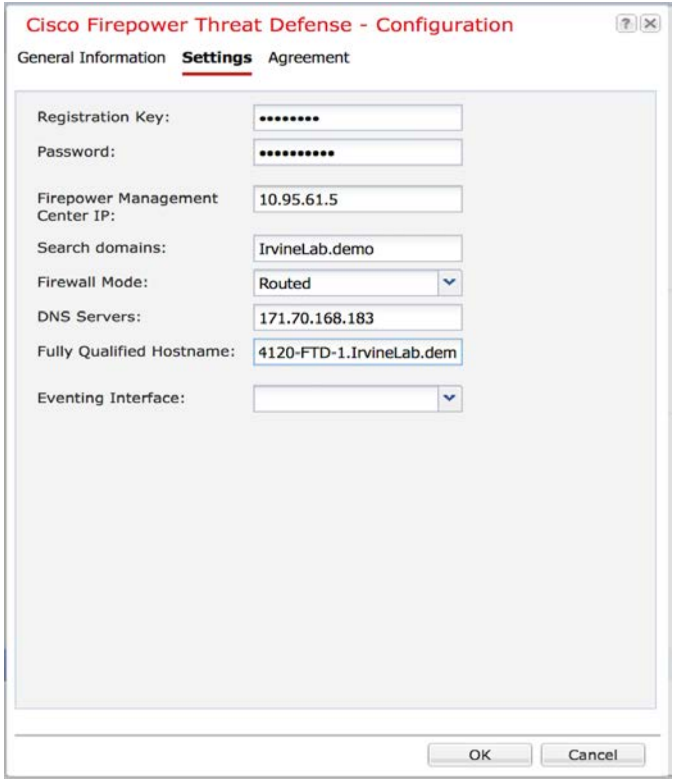
Network Gateway: 10.95.61.62

Configure FTD Instance Cont'd

Under Settings, enter the Firepower Management Center information along with other network settings and firewall mode.

Registration Key—user-defined shared key between FTD and FMC to establish connectivity. The same key needs to be used in FMC under Devices>Device Management when adding FTD.

Password—assign admin password for FTD



Cisco Firepower Threat Defense - Configuration

Registration Key: ••••••••••

Password: •••••••••••••

Firepower Management Center IP: 10.95.61.5

Search domains: IrvineLab.demo

Firewall Mode: Routed

DNS Servers: 171.70.168.183

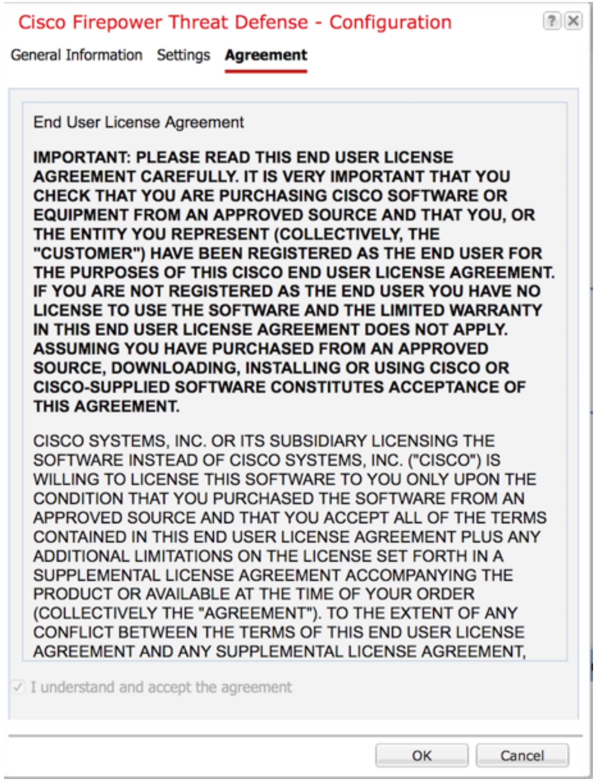
Fully Qualified Hostname: 4120-FTD-1.IrvineLab.dem

Eventing Interface:

Configure FTD Instance Cont’d

Under Agreement, the FTD EULA will be displayed. The agreement is automatically accepted (grayed out).

Click OK.



End User License Agreement

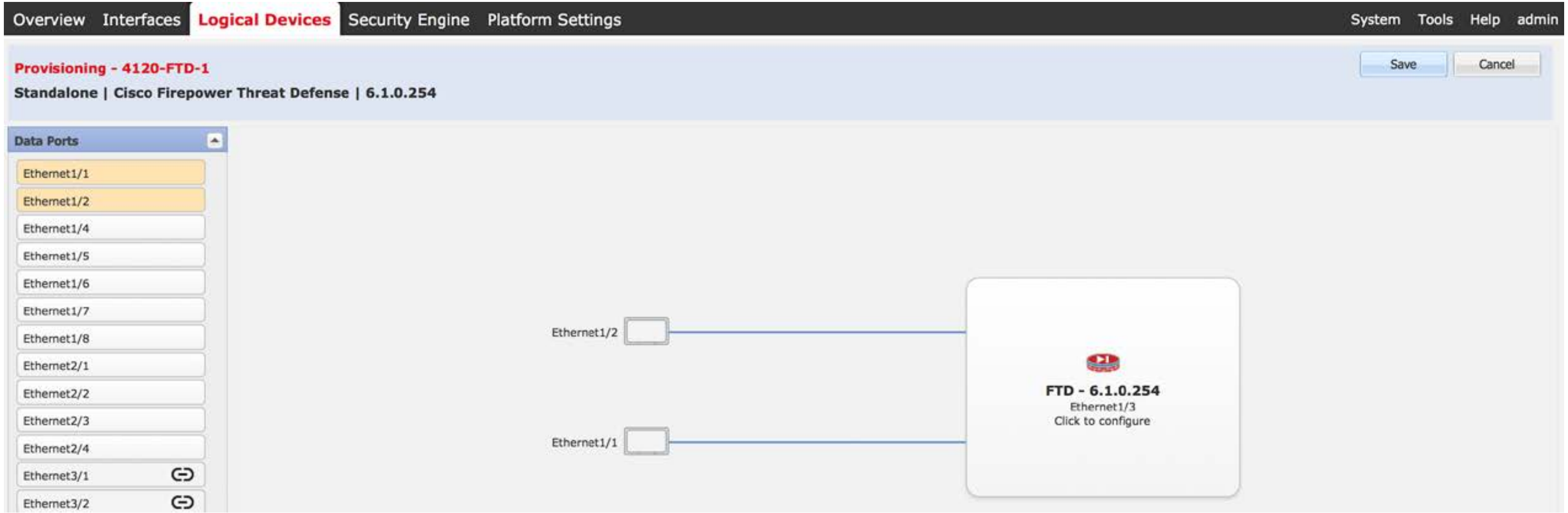
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT,

☑ I understand and accept the agreement

Completed FTD Instance Configuration

FTD Instance is completed. Click Save.

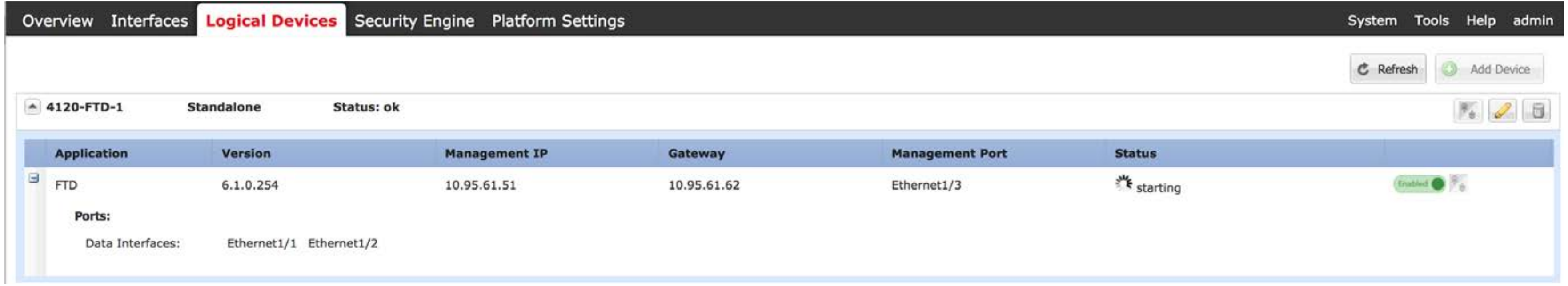


Provisioning - 4120-FTD-1

Standalone | Cisco Firepower Threat Defense | 6.1.0.254

FTD Configuration Pushed to Security Module

Status will change from Starting…



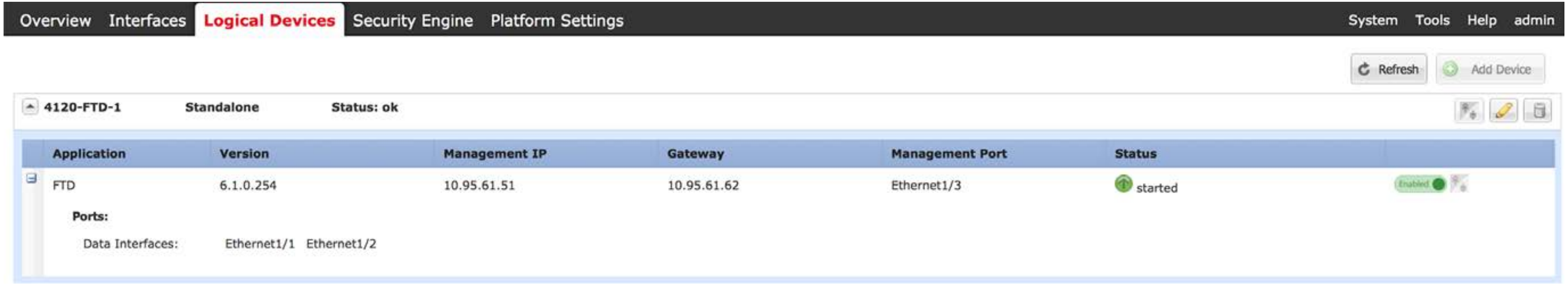
4120-FTD-1 Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.254	10.95.61.51	10.95.61.62	Ethernet1/3	starting

Ports:

Data Interfaces: Ethernet1/1 Ethernet1/2

To Started…



4120-FTD-1 Standalone Status: ok

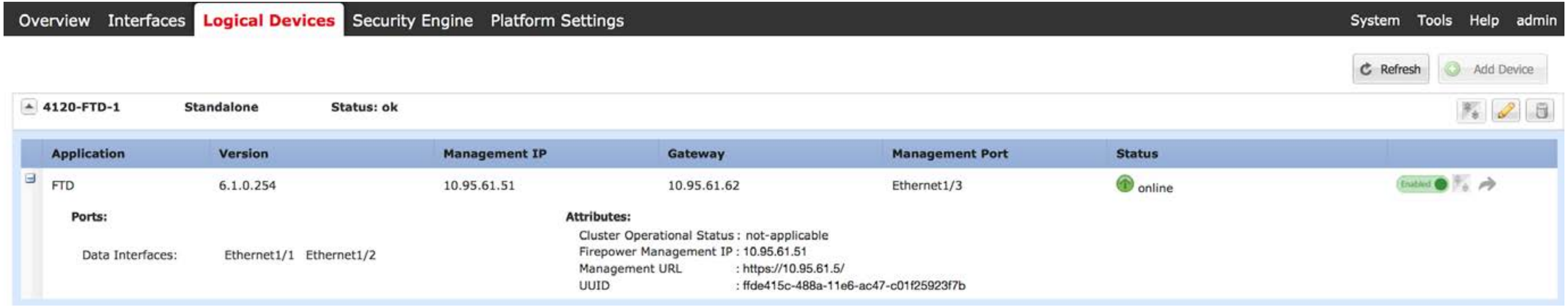
Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.254	10.95.61.51	10.95.61.62	Ethernet1/3	started

Ports:

Data Interfaces: Ethernet1/1 Ethernet1/2

Successful FTD Instantiation

To finally Online! Installation of FTD on the security module is now complete.



4120-FTD-1 Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.254	10.95.61.51	10.95.61.62	Ethernet1/3	online

Ports:

Data Interfaces: Ethernet1/1 Ethernet1/2

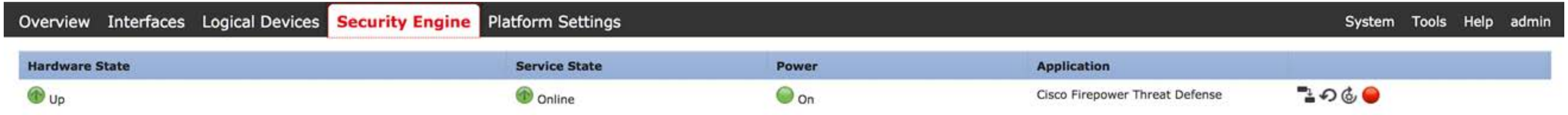
Attributes:

```
Cluster Operational Status : not-applicable
Firepower Management IP : 10.95.61.51
Management URL          : https://10.95.61.5/
UUID                    : ffde415c-488a-11e6-ac47-c01f25923f7b
```

Successful FTD Instantiation Con’d

Verify under Security Engine for status and application of the security module.

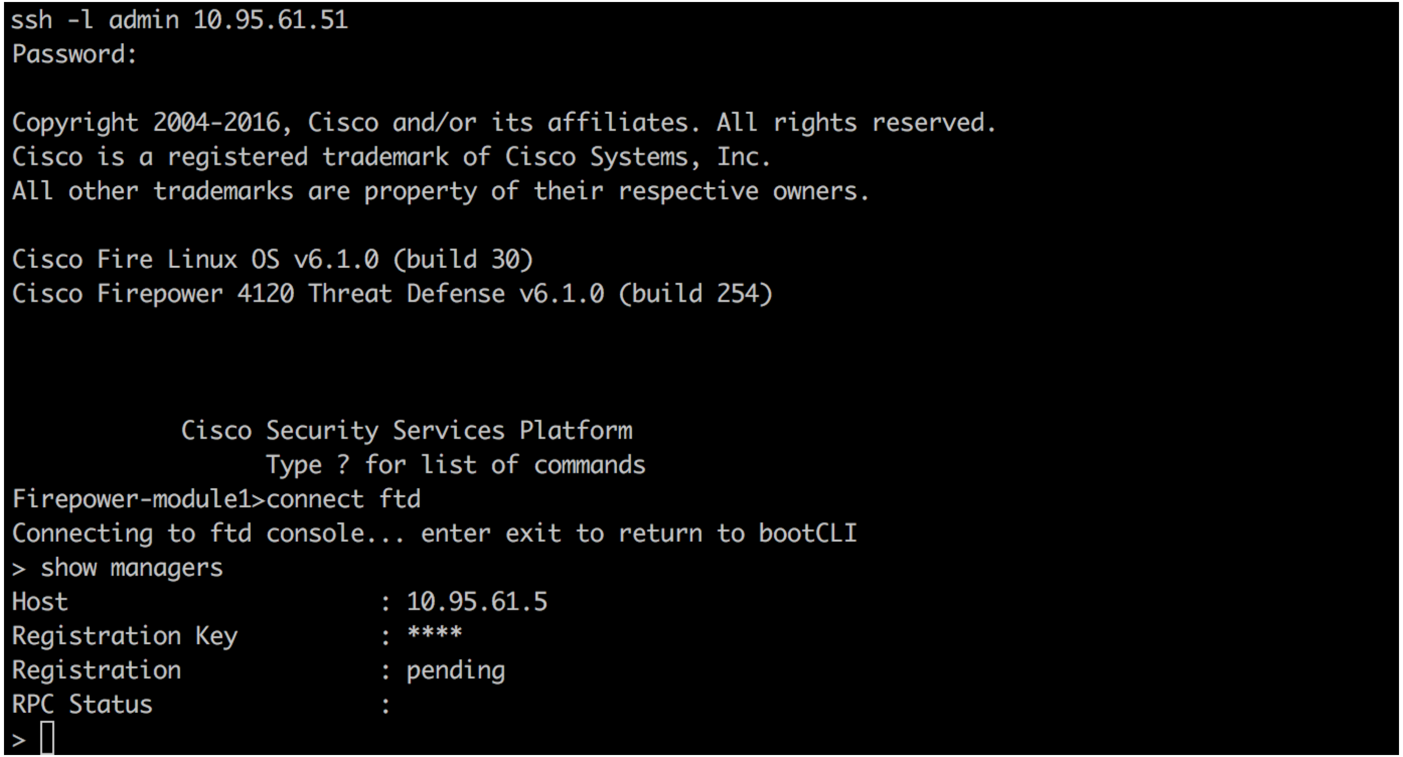
Hardware State—Up
Service State—Online
Power—On
Application—Cisco Firepower Threat Defense



Hardware State	Service State	Power	Application	
Up	Online	On	Cisco Firepower Threat Defense	

FTD should now be ready to be added into Firepower Management Center.

Use CLI to Verify that FTD is ready to be added into FMC



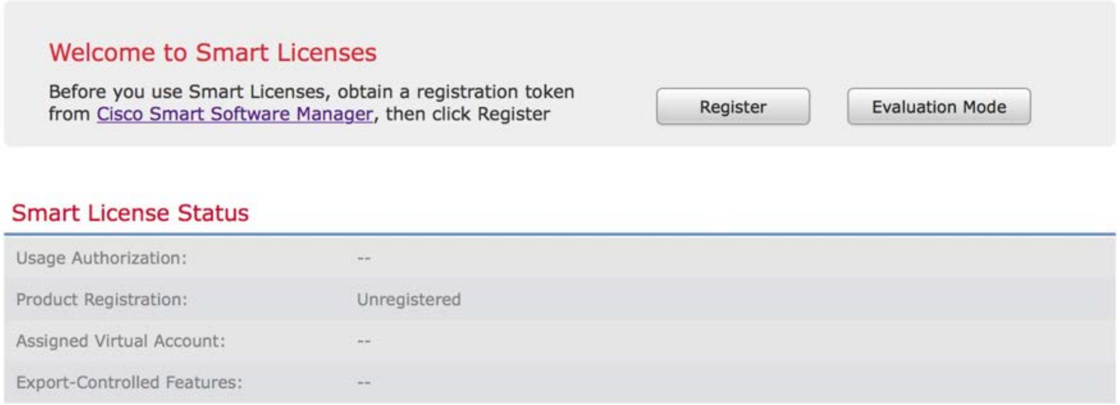
```
ssh -l admin 10.95.61.51
Password:

Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.1.0 (build 30)
Cisco Firepower 4120 Threat Defense v6.1.0 (build 254)



            Cisco Security Services Platform
                  Type ? for list of commands
Firepower-module1>connect ftd
Connecting to ftd console... enter exit to return to bootCLI
> show managers
Host                      : 10.95.61.5
Registration Key          : ****
Registration              : pending
RPC Status                :
> 
```

Add FTD Appliance to FMC

Enable Smart Licenses

From the FMC Web Interface, click on System -> Licenses -> Smart Licenses.

Select “Evaluation Mode”. This will enable all licenses for a 90-day period.



Welcome to Smart Licenses

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

Smart License Status

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

Add FTD to FMC

From the FTD CLI, define the FMC:

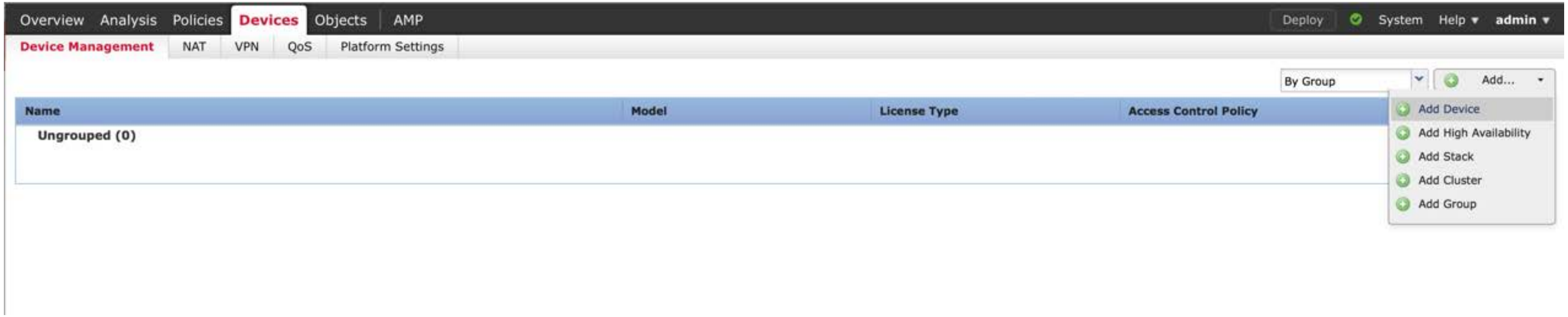
```
> configure manager add 10.0.0.52 randomword
```

Whichever phrase you choose here instead of “randomword” will also need to be entered on the FMC.

Add FTD to FMC, continued…

On the FMC web interface, click anywhere you see the link:
Click here to register a device.

If you don't see the link, click on the Devices tab, and then the Add button on the right side of the screen.

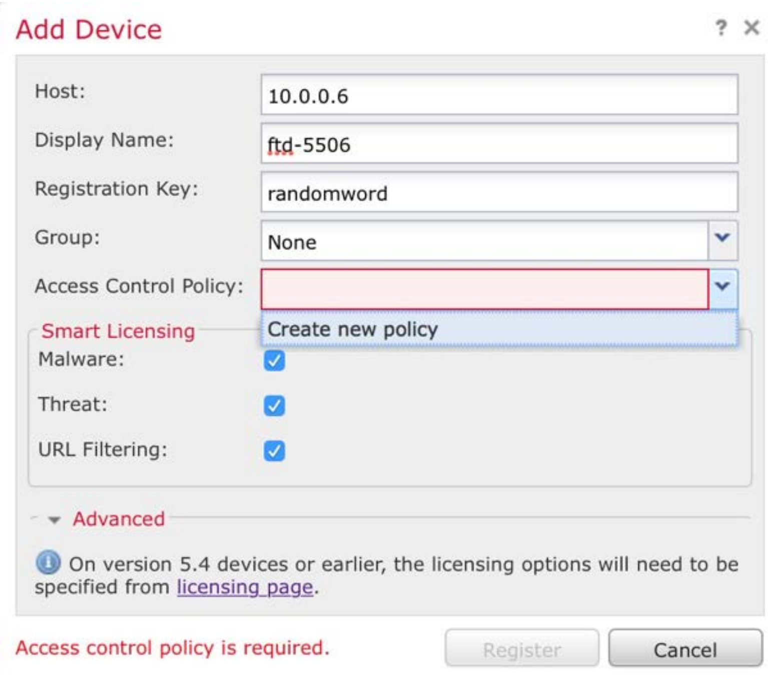


Name	Model	License Type	Access Control Policy
Ungrouped (0)			

Add FTD to FMC, continued…

Enter the IP address, Display Name, and Registration Key.

Select all of the licenses, and then click on the pulldown for Access Control Policy, and select Create new policy.



Add Device

Host: 10.0.0.6

Display Name: ftd-5506

Registration Key: randomword

Group: None

Access Control Policy:

Create new policy

Smart Licensing

Malware: ☑

Threat: ☑

URL Filtering: ☑

Advanced

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

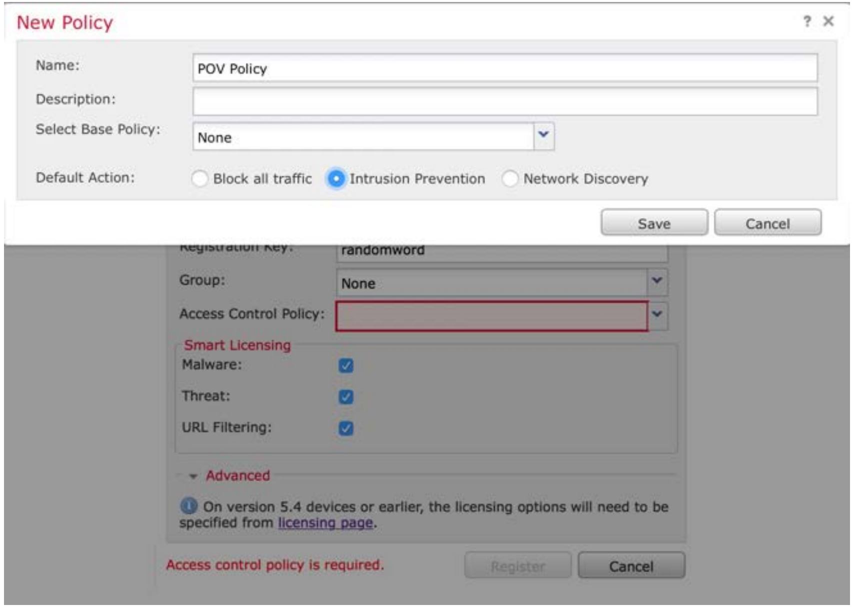
Access control policy is required.

Add FTD to FMC, continued…

Provide a name for this Access Control Policy, and select Intrusion Prevention for the Default Action.

Click Save

Click Register



New Policy

Name: POV Policy

Description:

Select Base Policy: None

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

Registration Key: randomword

Group: None

Access Control Policy:

Smart Licensing

Malware: ☑

Threat: ☑

URL Filtering: ☑

Advanced

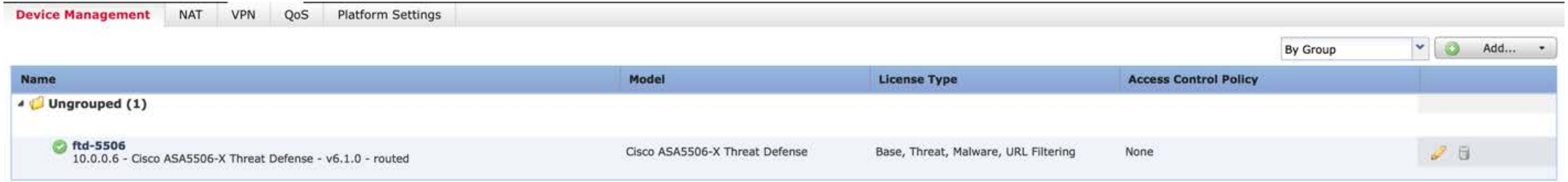
On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.

Access control policy is required.

Device Configuration

Configure Passive Interface

Click on Device Name to edit it. Alternatively, click on the pencil icon.



Name	Model	License Type	Access Control Policy	
Ungrouped (1)				
ftd-5506 10.0.0.6 - Cisco ASA5506-X Threat Defense - v6.1.0 - routed	Cisco ASA5506-X Threat Defense	Base, Threat, Malware, URL Filtering	None	✎ 🗑

Then, select an interface and edit it by clicking on the pencil icon next to the interface name.

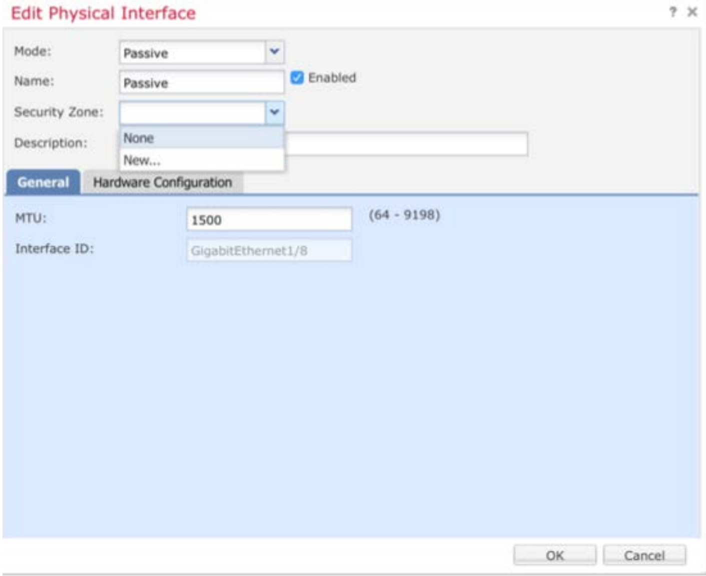
Configure Passive Interface, continued…

If connecting FTD to a SPAN port or TAP, you'll need a Passive interface.

Set Interface to Passive Mode.
Give it a name.   (Passive is fine)
Define a new Security Zone. (Passive is fine)

Click OK

Click Save



Edit Physical Interface

Mode: Passive

Name: Passive ☑ Enabled

Security Zone:

Description:

MTU: 1500 (64 - 9198)

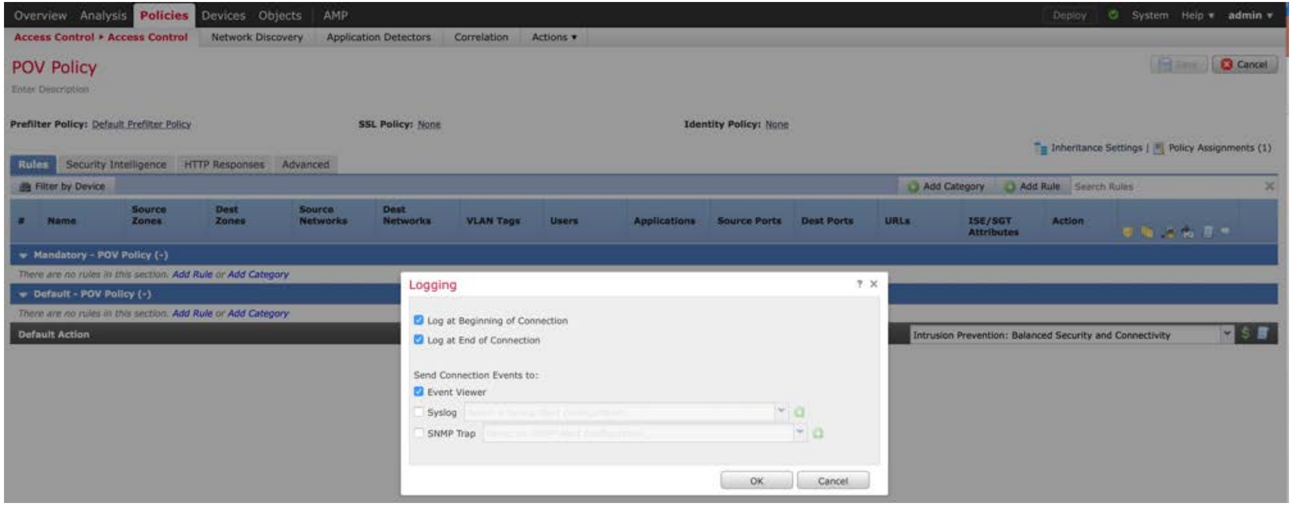
Interface ID: GigabitEthernet1/8

Configure Passive Interface, continued…

Click on Policies, and then select the POV Policy.

Click the paper icon by the Intrusion Policy at the bottom right.

Enable Logging, and click OK.



POV Policy

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

Identity Policy: None

Mandatory - POV Policy (-)

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

Default - POV Policy (-)

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

Default Action: Intrusion Prevention: Balanced Security and Connectivity

Logging

☑ Log at Beginning of Connection

☑ Log at End of Connection

Send Connection Events to:

☑ Event Viewer

□ Syslog

□ SNMP Trap

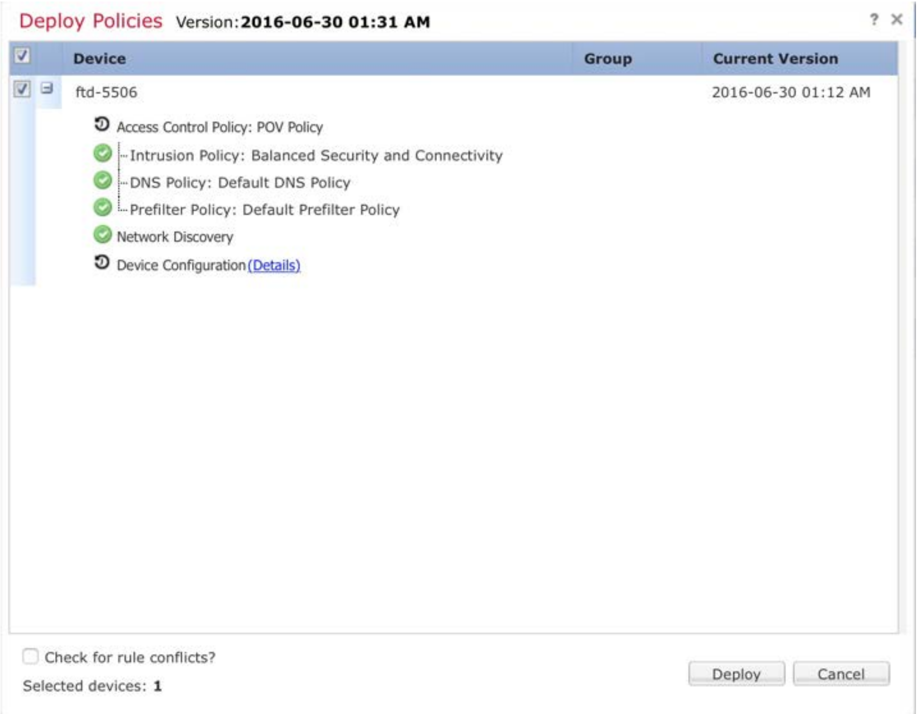
OK Cancel

Configure Passive Interface, continued…

Click the Deploy button at top right of screen.

Select the checkbox by your FTD device.

Click Deploy



Deploy Policies Version:**2016-06-30 01:31 AM**

☑	Device	Group	Current Version
☑	ftd-5506		2016-06-30 01:12 AM

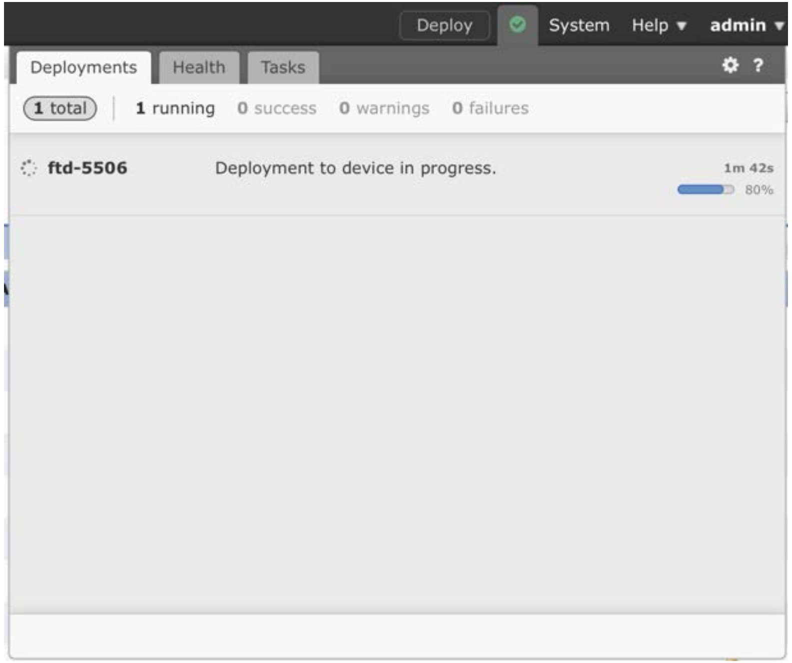
- Access Control Policy: POV Policy
  - ✓ Intrusion Policy: Balanced Security and Connectivity
  - ✓ DNS Policy: Default DNS Policy
  - ✓ Prefilter Policy: Default Prefilter Policy
- ✓ Network Discovery
- Device Configuration (Details)

□ Check for rule conflicts?

Selected devices: **1**

Deployment Status

Note: You can view the status of a Deploy by clicking the Green checkmark icon.

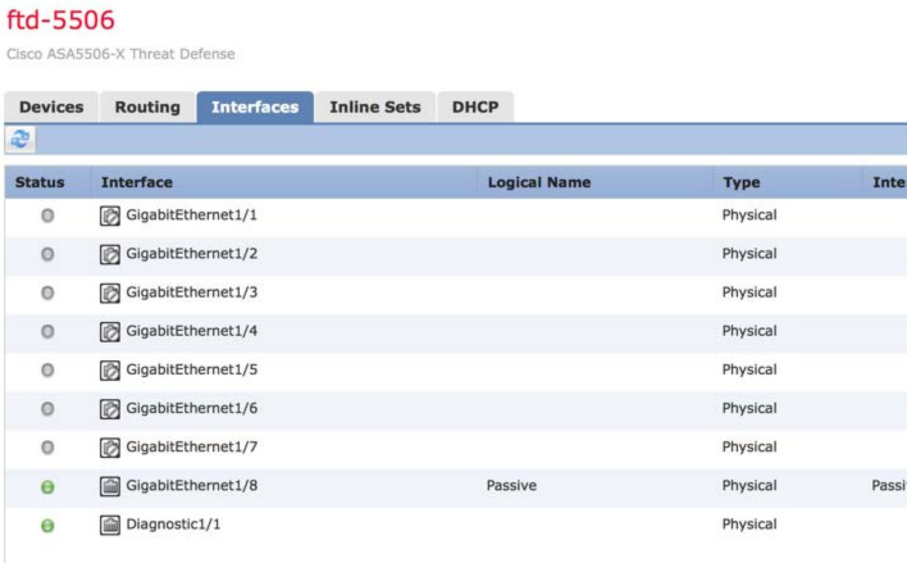


1 total | 1 running 0 success 0 warnings 0 failures

ftd-5506 Deployment to device in progress. 1m 42s 80%

Configure Passive Interface, continued…

When the deployment completes, the interface Status for the Passive interface should turn green.



ftd-5506

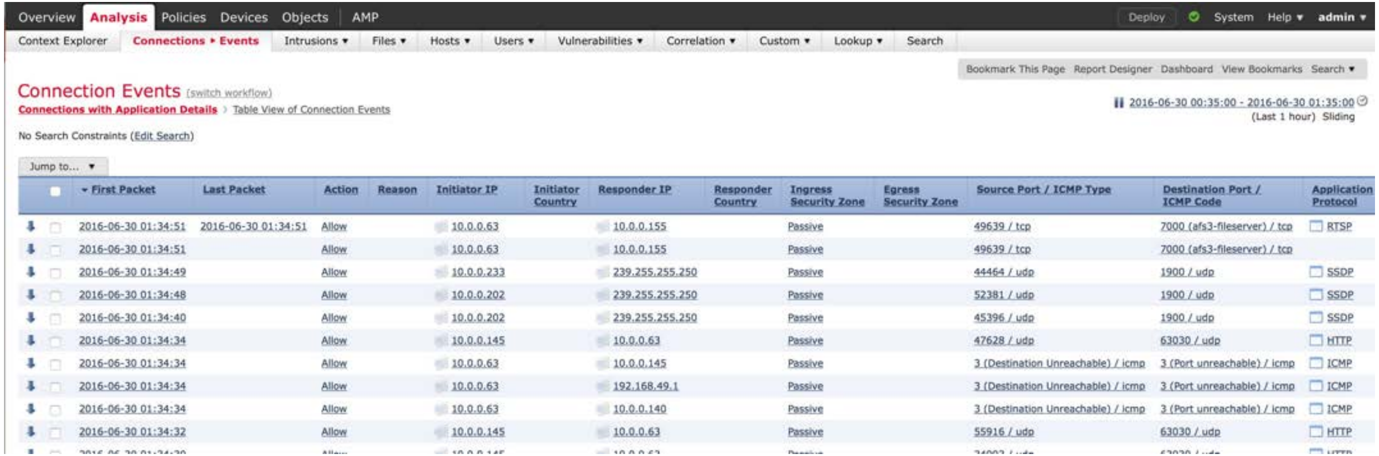
Cisco ASA5506-X Threat Defense

Status	Interface	Logical Name	Type	Inte
○	GigabitEthernet1/1		Physical	
○	GigabitEthernet1/2		Physical	
○	GigabitEthernet1/3		Physical	
○	GigabitEthernet1/4		Physical	
○	GigabitEthernet1/5		Physical	
○	GigabitEthernet1/6		Physical	
○	GigabitEthernet1/7		Physical	
●	GigabitEthernet1/8	Passive	Physical	Passi
●	Diagnostic1/1		Physical	

Check Traffic

Click on ‘Analysis’ -> ‘Connections’ -> ‘Events’.

You should see traffic passing the device. If you don’t, verify interfaces are connected, enabled, and the SPAN port is functional.



Connection Events (switch workflow)

Connections with Application Details › Table View of Connection Events

2016-06-30 00:35:00 - 2016-06-30 01:35:00
(Last 1 hour) Sliding

No Search Constraints (Edit Search)

□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol
□	2016-06-30 01:34:51	2016-06-30 01:34:51	Allow		10.0.0.63		10.0.0.155		Passive		49639 / tcp	7000 (afs3-fileserver) / tcp	RTSP
□	2016-06-30 01:34:51		Allow		10.0.0.63		10.0.0.155		Passive		49639 / tcp	7000 (afs3-fileserver) / tcp	
□	2016-06-30 01:34:49		Allow		10.0.0.233		239.255.255.250		Passive		44464 / udp	1900 / udp	SSDP
□	2016-06-30 01:34:48		Allow		10.0.0.202		239.255.255.250		Passive		52381 / udp	1900 / udp	SSDP
□	2016-06-30 01:34:40		Allow		10.0.0.202		239.255.255.250		Passive		45396 / udp	1900 / udp	SSDP
□	2016-06-30 01:34:34		Allow		10.0.0.145		10.0.0.63		Passive		47628 / udp	63030 / udp	HTTP
□	2016-06-30 01:34:34		Allow		10.0.0.63		10.0.0.145		Passive		3 (Destination Unreachable) / icmp	3 (Port unreachable) / icmp	ICMP
□	2016-06-30 01:34:34		Allow		10.0.0.63		192.168.49.1		Passive		3 (Destination Unreachable) / icmp	3 (Port unreachable) / icmp	ICMP
□	2016-06-30 01:34:34		Allow		10.0.0.63		10.0.0.140		Passive		3 (Destination Unreachable) / icmp	3 (Port unreachable) / icmp	ICMP
□	2016-06-30 01:34:32		Allow		10.0.0.145		10.0.0.63		Passive		55916 / udp	63030 / udp	HTTP

Helpful Tips

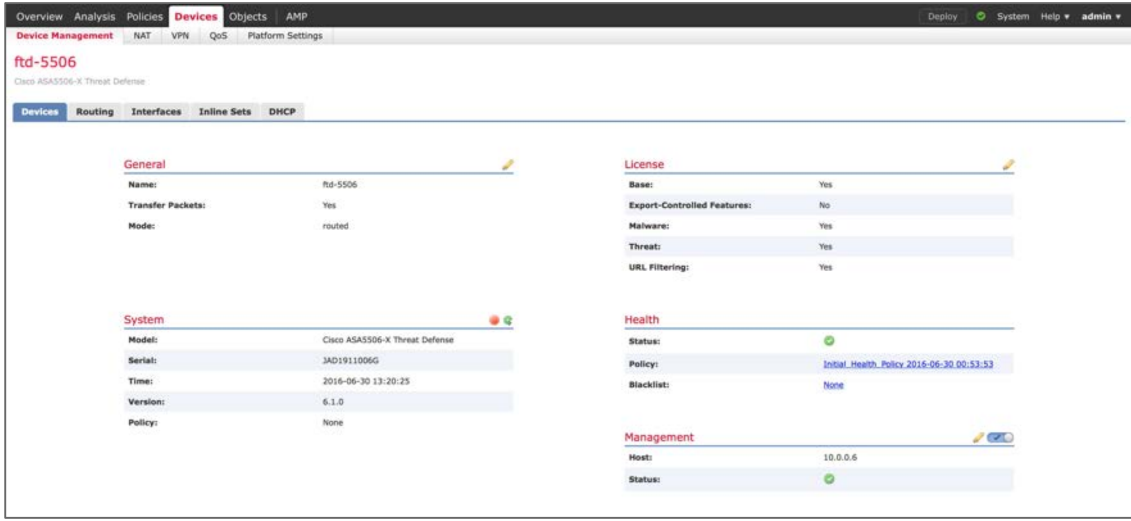
FTD should not be powered off with a switch or by pulling a power cord. Disk corruption can occur, and can cause problems with deploying policies or upgrades later.

To power off an FTD device (Option 1):

Devices -> Device Management
Select your device
Click on Devices
Click on the Red Stop symbol

To power off an FTD device (Option 2):

From CLI, type: `shutdown`



ftd-5506

Cisco ASA5506-X Threat Defense

General

Name:	ftd-5506
Transfer Packets:	Yes
Mode:	routed

System

Model:	Cisco ASA5506-X Threat Defense
Serial:	JAD1911006G
Time:	2016-06-30 13:20:25
Version:	6.1.0
Policy:	None

License

Base:	Yes
Export-Controlled Features:	No
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes

Health

Status:	✓
Policy:	Initial_Health_Policy 2016-06-30 00:53:53
Blacklist:	None

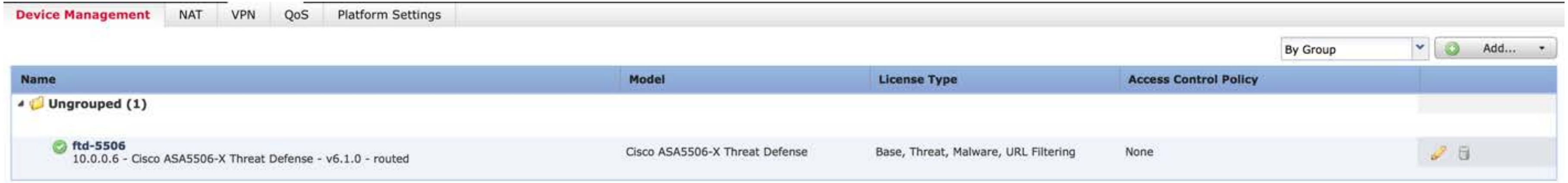
Management

Host:	10.0.0.6
Status:	✓

Alternate Device Configuration for Inline TAP

Alternate: Configure Inline TAP

Click on Device Name to edit it. Alternatively, click on the pencil icon.



Name	Model	License Type	Access Control Policy
Ungrouped (1)			
ftd-5506 10.0.0.6 - Cisco ASA5506-X Threat Defense - v6.1.0 - routed	Cisco ASA5506-X Threat Defense	Base, Threat, Malware, URL Filtering	None

Click one of the interfaces that will be sending/receiving traffic and edit it by clicking on the pencil icon next to the interface name.

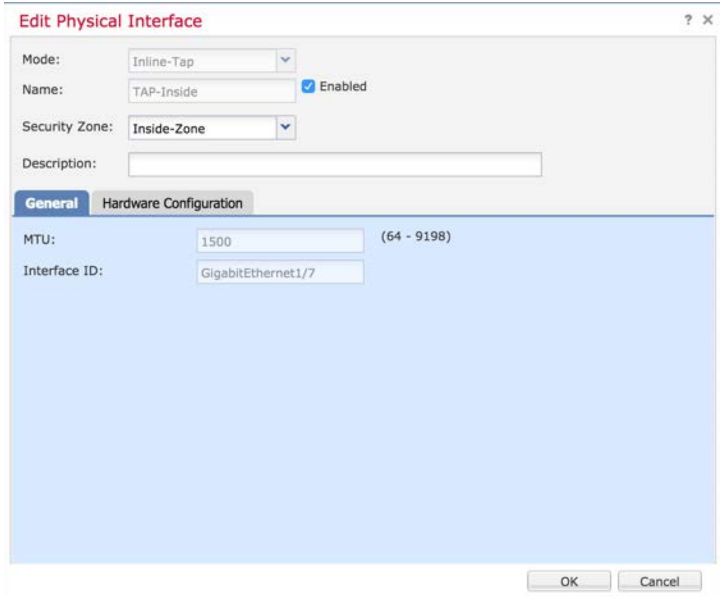
Alternate: Configure Inline TAP, continued…

Remember, an Inline TAP will pass all traffic through to the other member of the Set, and copy packets for inspection, but not interrupt traffic flow.

1. Leave Interface Mode as ‘None’.
2. Enable the Interface.
3. Give it a name.   (TAP-Inside is fine)
4. Define a new Security Zone. (Inside-Zone is fine)

Click OK

Click Save


Edit Physical Interface

Mode: Inline-Tap

Name: TAP-Inside ☑ Enabled

Security Zone: Inside-Zone

Description:

MTU: 1500 (64 - 9198)

Interface ID: GigabitEthernet1/7

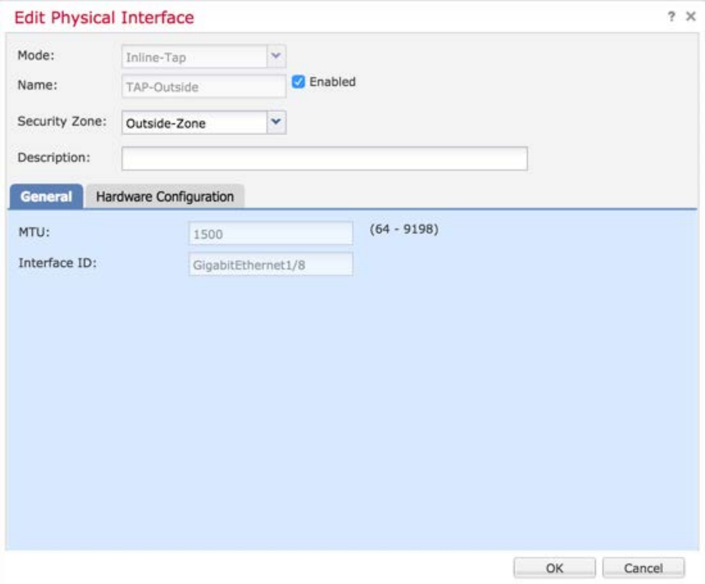
Alternate: Configure Inline TAP, continued…

Repeat the process for the other Set member.

1. Leave Interface Mode as ‘None’.
2. Enable the Interface.
3. Give it a name. (TAP-Outside is fine)
4. Define a new Security Zone. (Outside-Zone is fine)

Click OK

Click Save


Edit Physical Interface

Mode: Inline-Tap

Name: TAP-Outside ☑ Enabled

Security Zone: Outside-Zone

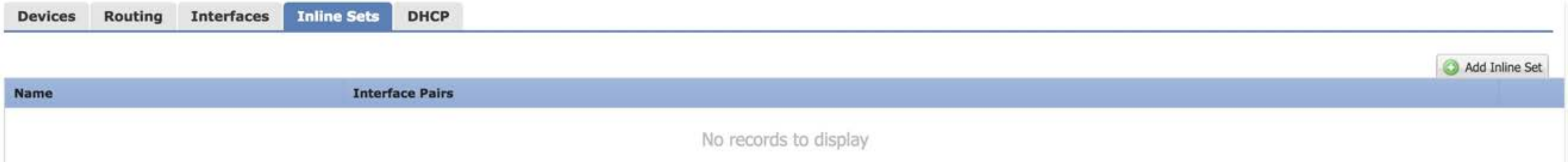
Description:

MTU: 1500 (64 - 9198)

Interface ID: GigabitEthernet1/8

Alternate: Configure Inline TAP, continued…

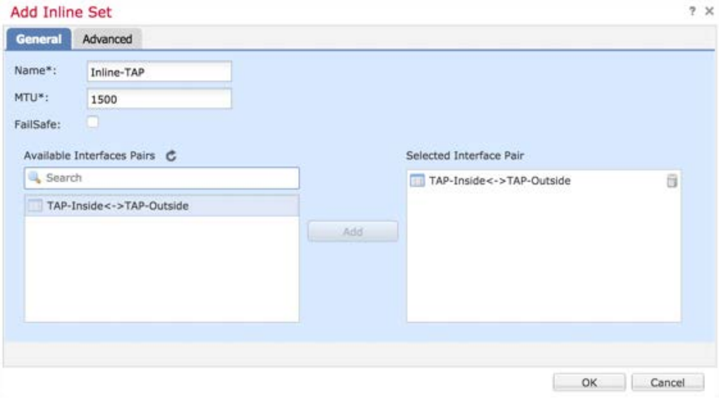
Click on ‘Inline Sets’, and then on ‘Add Inline Set’ button.



Name	Interface Pairs
No records to display	

Give the Inline Set a name (like Inline-TAP), and add the available Interface Pairs.

Click on ‘Advanced’.



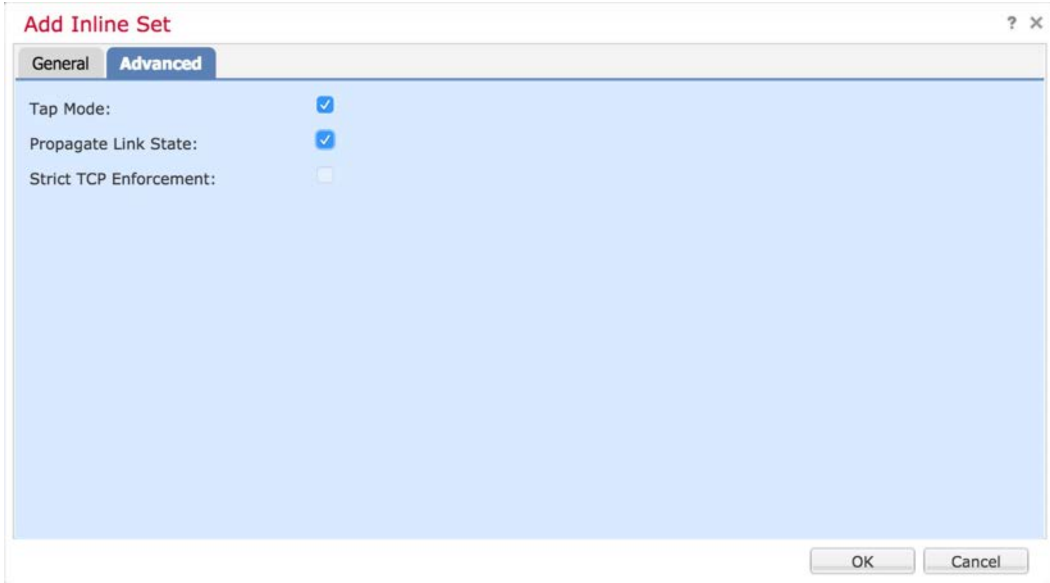
Name*: Inline-TAP
MTU*: 1500
FailSafe: □
TAP-Inside<->TAP-Outside
TAP-Inside<->TAP-Outside

Alternate: Configure Inline TAP, continued…

Click the options to enable ‘Tap Mode’, and also to ‘Propagate Link State’.

If you do not put it in Tap Mode, you will potentially block customer’s traffic, depending on the policy configurations, and whether or not the appliance detects an attack or Security Intelligence hits.

Remember Inline Sets and Inline Taps are different than Transparent mode in that the same VLAN exists on both sides.



Add Inline Set

Tap Mode: ☑

Propagate Link State: ☑

Strict TCP Enforcement: □

User Agent Configuration (optional)

About Identity

There are currently three ways to authenticate users against Microsoft Active Directory.

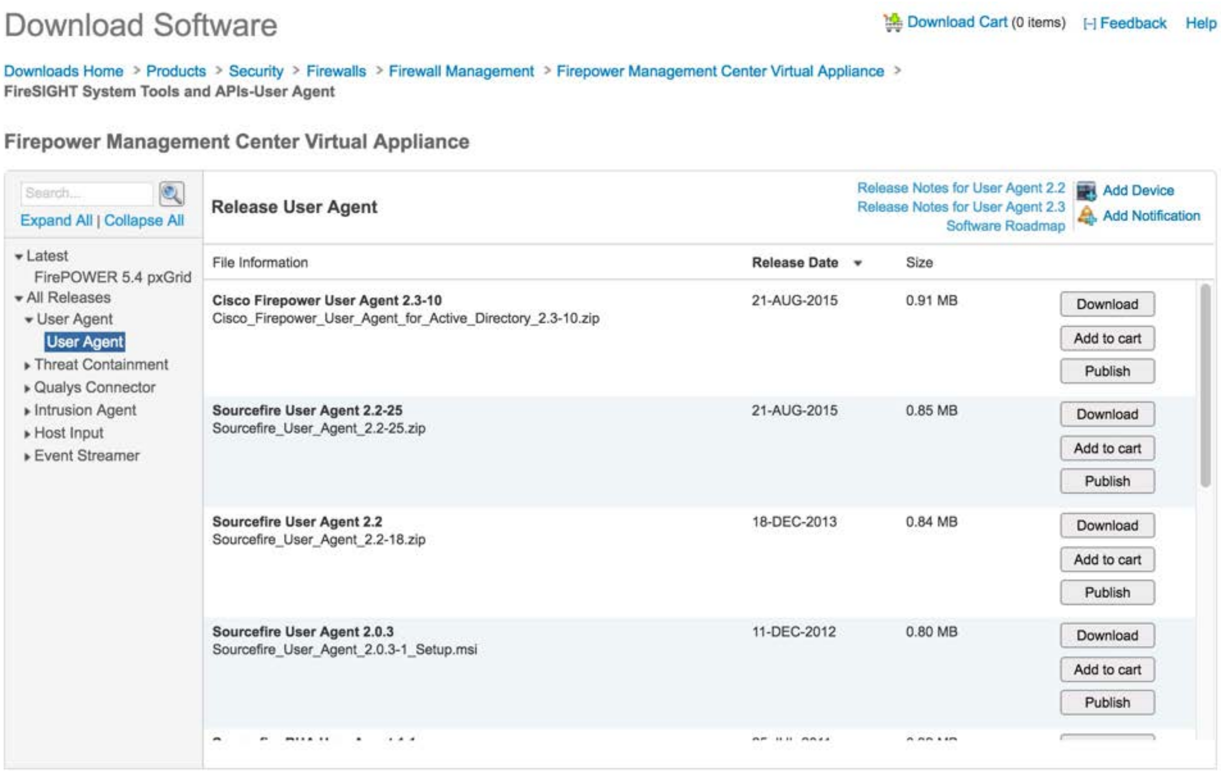
1. The Sourcefire User Agent passively watched Active Directory authentications and allows FTD to enforce policy based on username or group membership.

2. Identity Services Engine uses the 802.1x authentication used to access the wired or wireless network and makes the information available to FTD.

3. Web Authentication prompts each user to authenticate via web page.

Sourcefire User Agent is likely the easiest to deploy during a POV.

Download Sourcefire User Agent (SFUA)



Download Software

Downloads Home > Products > Security > Firewalls > Firewall Management > Firepower Management Center Virtual Appliance > FireSIGHT System Tools and APIs-User Agent

Firepower Management Center Virtual Appliance

- Latest
  - FirePOWER 5.4 pxGrid
- All Releases
  - User Agent
    - User Agent
  - Threat Containment
  - Qualys Connector
  - Intrusion Agent
  - Host Input
  - Event Streamer

Release User Agent

File Information	Release Date	Size
Cisco Firepower User Agent 2.3-10 Cisco_Firepower_User_Agent_for_Active_Directory_2.3-10.zip	21-AUG-2015	0.91 MB
Sourcefire User Agent 2.2-25 Sourcefire_User_Agent_2.2-25.zip	21-AUG-2015	0.85 MB
Sourcefire User Agent 2.2 Sourcefire_User_Agent_2.2-18.zip	18-DEC-2013	0.84 MB
Sourcefire User Agent 2.0.3 Sourcefire_User_Agent_2.0.3-1_Setup.msi	11-DEC-2012	0.80 MB

User Agent Information

How difficult is it to setup?

In most cases, it is easy to setup and configure. It should only take a few minutes.

How does it work?

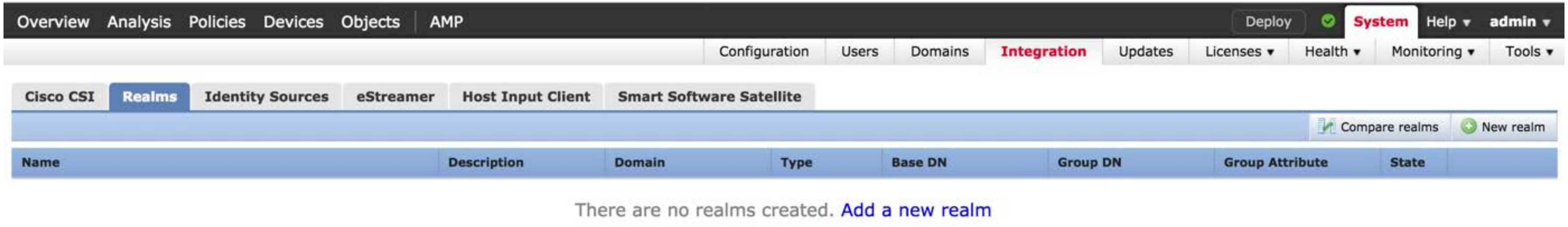
SFUA will monitor the security logs in Active Directory, making login/logout information to FMC. FMC will query AD via LDAP for group memership information.

Install on a Windows Server. It should not be the AD Server.

Create Realm

Click on ’System’ -> ‘Integration’ -> ‘Realms’

Select ’Add a new realm’



There are no realms created. Add a new realm

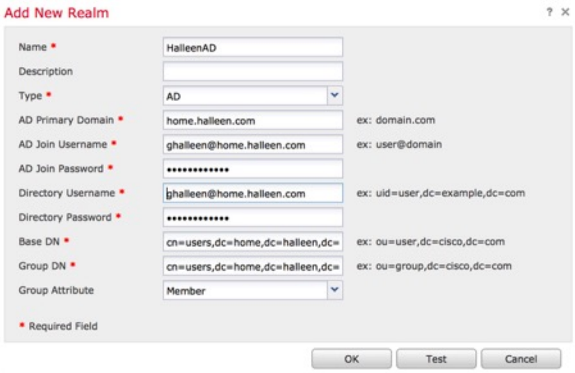
Create Realm, continued…

Enter the relevant information for the customer’s Active Directory.

An LDAP browser, like Softerra LDAP Browser for Windows, can help if you have problems with syntax.

http://www.ldapadministrator.com/download.htm

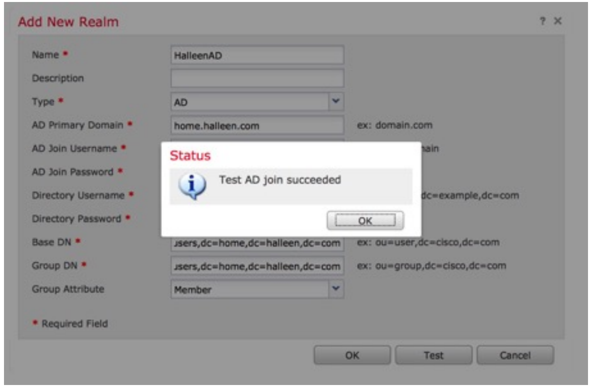
Click ‘Test’ when finished, and then ‘OK’.



Add New Realm

Name *	HalleenAD	
Description		
Type *	AD	
AD Primary Domain *	home.halleen.com	ex: domain.com
AD Join Username *	ghalleen@home.halleen.com	ex: user@domain
AD Join Password *	•••••••••••••	
Directory Username *	ghalleen@home.halleen.com	ex: uid=user,dc=example,dc=com
Directory Password *	•••••••••••••	
Base DN *	cn=users,dc=home,dc=halleen,dc=	ex: ou=user,dc=cisco,dc=com
Group DN *	cn=users,dc=home,dc=halleen,dc=	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

* Required Field



Add New Realm

Name *	HalleenAD	
Description		
Type *	AD	
AD Primary Domain *	home.halleen.com	ex: domain.com
AD Join Username *		ain
AD Join Password *		
Directory Username *		dc=example,dc=com
Directory Password *		
Base DN *	ısers,dc=home,dc=halleen,dc=com	ex: ou=user,dc=cisco,dc=com
Group DN *	ısers,dc=home,dc=halleen,dc=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

* Required Field

Status

Test AD join succeeded

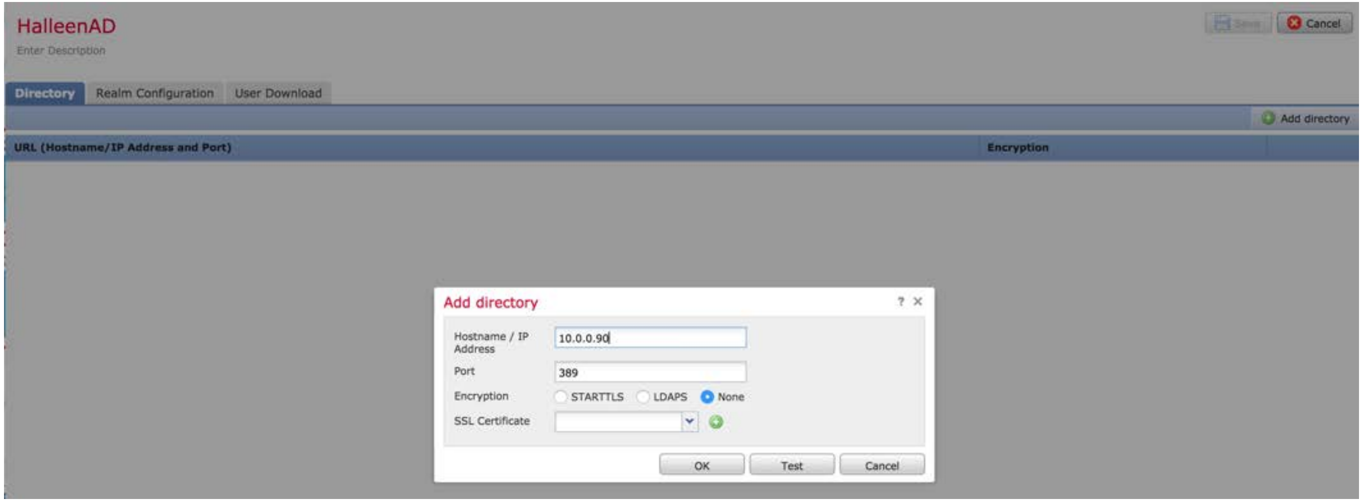
Create Realm, continued…

Click on ‘Directory’

Select ’Add directory’ and enter relevant information.

Click ‘Test’

Click ‘OK’



Hostname / IP Address: 10.0.0.90

Port: 389

Encryption: ○ STARTTLS ○ LDAPS ● None

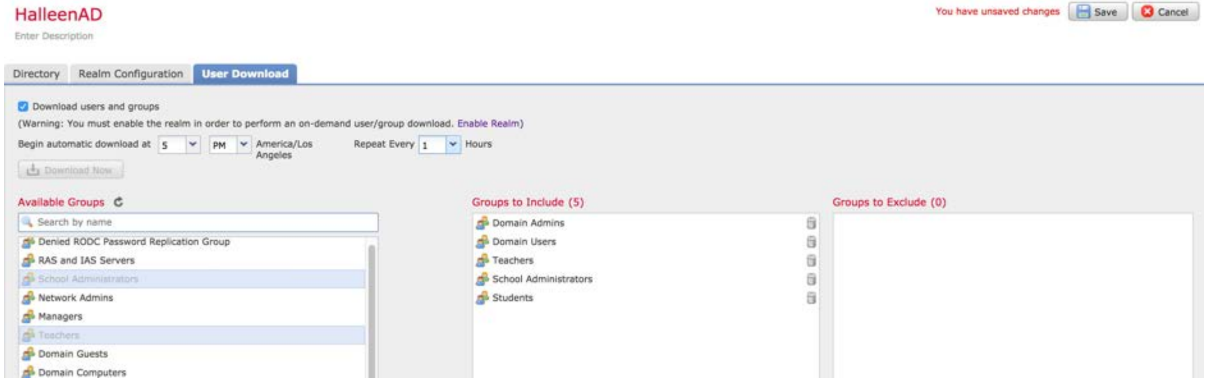
SSL Certificate:

Create Realm, continued…

Click on ‘User Download’

Click ‘Download users and groups’, and configure a download frequency.

Either Include the AD groups your customers wants to include in policy decisions, or Exclude those they don’t want, and Save.



HalleenAD

Enter Description

You have unsaved changes

☑ Download users and groups

(Warning: You must enable the realm in order to perform an on-demand user/group download. Enable Realm)

Begin automatic download at 5 PM America/Los Angeles Repeat Every 1 Hours

Available Groups

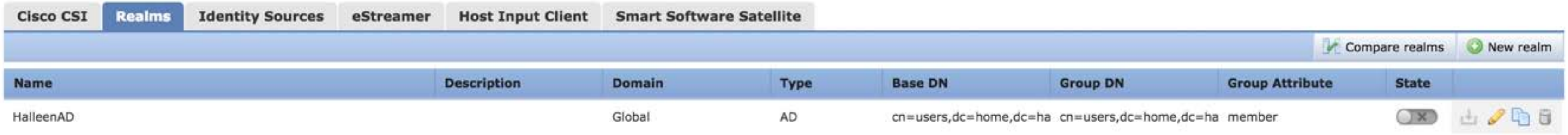
- Denied RODC Password Replication Group
- RAS and IAS Servers
- School Administrators
- Network Admins
- Managers
- Teachers
- Domain Guests
- Domain Computers

Groups to Include (5)

- Domain Admins
- Domain Users
- Teachers
- School Administrators
- Students

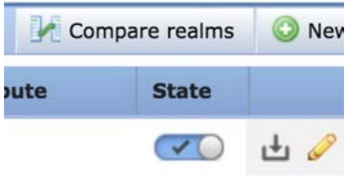
Groups to Exclude (0)

Create Realm, continued…



Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
HalleenAD		Global	AD	cn=users,dc=home,dc=ha	cn=users,dc=home,dc=ha	member	✗

Activate the Realm by clicking the slider.



User Agent Information

How difficult is it to setup?

> In most cases, it is easy to setup and configure. It should only take a few minutes.

How does it work?

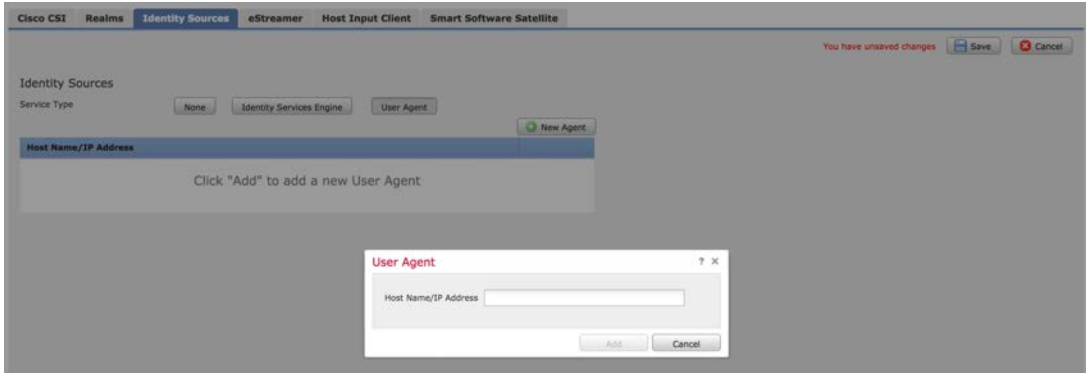
> SFUA will monitor the security logs in Active Directory, making login/logout information to FMC. FMC will query AD via LDAP for group memership information.

Install on a Windows Server. It should not be the AD Server.

Associate User Agent…

Click ‘Identity Source’, and then click ‘User Agent’

Enter the IP address or hostname of the Windows server you installed the User Agent on.

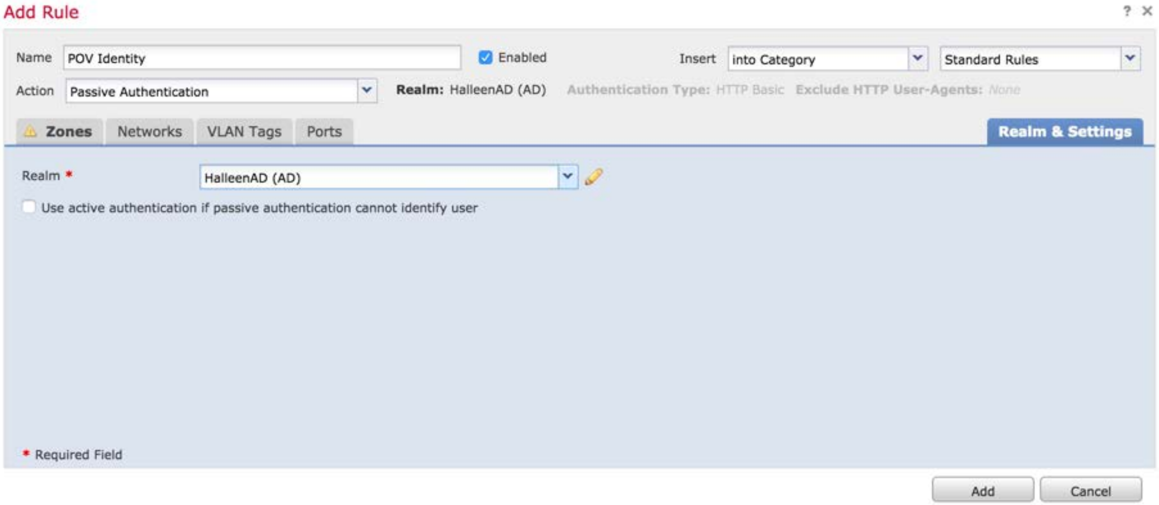


Create Identity Policy

Click on ‘Policies’ -> ‘Identity’, and Create an Identity Policy

For a Passive deployment, you only need a single rule, but if your customer wants to enforce policy, and wants Active Directory to be used in the policy, you’ll need to define which traffic has Identity enabled.

Note: Active Authentication requires Routed interfaces, but is not required in a standard POV.



Add Rule

Name: POV Identity

☑ Enabled

Insert: into Category

Standard Rules

Action: Passive Authentication

Realm: HalleenAD (AD)   Authentication Type: HTTP Basic   Exclude HTTP User-Agents: None

Realm *: HalleenAD (AD)

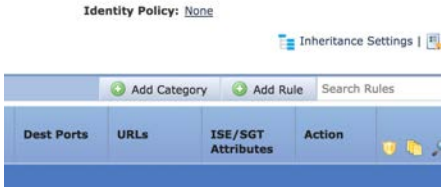
☐ Use active authentication if passive authentication cannot identify user

* Required Field

Add Identity to the Access Control Policy

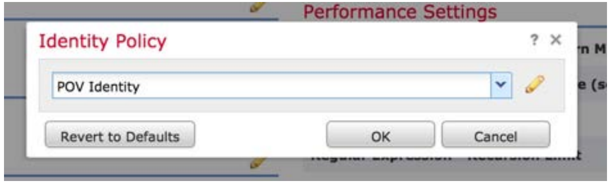
Click on ‘Policies’ -> ‘Access Control’, and edit your Access Control Policy.

In the top right, click on the Identity Policy: None link.



Identity Policy: None

Select the POV Identity Policy.



Identity Policy

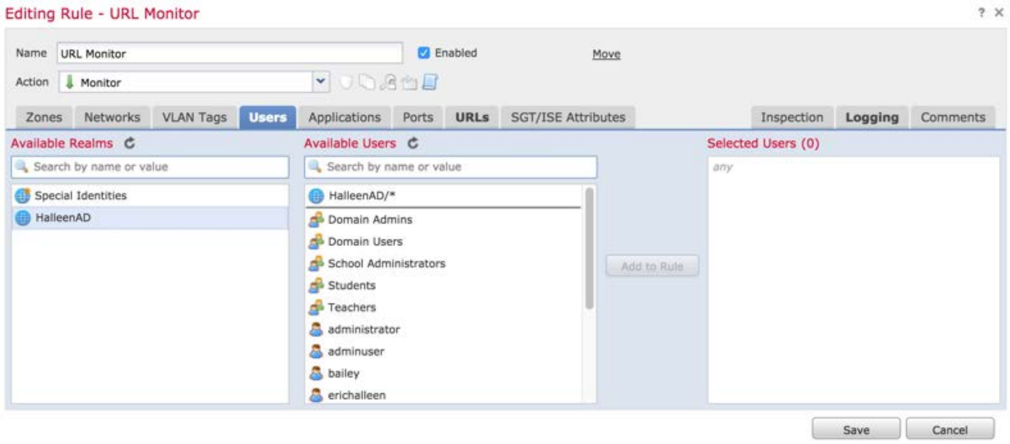
POV Identity

Add Identity Policy, continued…

Edit any Access Control rule, or create a new rule, and click on ‘Users’ to verify you are seeing user and group information.

If you don’t see any users or groups, make sure you’ve downloaded users and groups from the Identity Policy at least once.

Hit Cancel on the rule change, and then Save and Deploy your changes.



Editing Rule - URL Monitor

Name: URL Monitor

☑ Enabled

Action: Monitor

Available Realms

- Special Identities
- HalleenAD

Available Users

- HalleenAD/*
- Domain Admins
- Domain Users
- School Administrators
- Students
- Teachers
- administrator
- adminuser
- bailey
- erichalleen

Selected Users (0)

any

Initial Policy Configuration

Policy Overview

FMC has several different policies, but most are not used except for initial configuration.

Frequently:

- Access Control
- Intrusion
- File & Malware

Occasionally or only on Initial Setup:

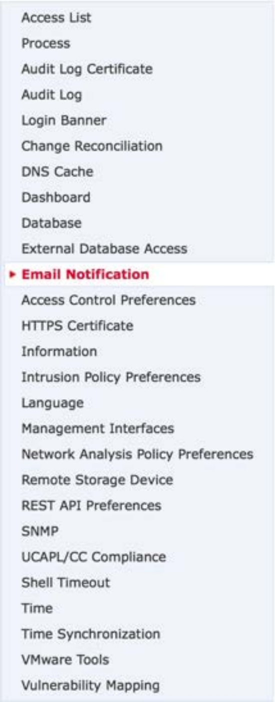
- Network Discovery
- Health
- Correlation
- DNS
- Identity
- SSL
- Prefilter
- Network Analysis

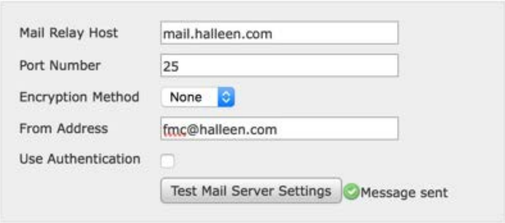
System Configuration

Click on ‘System’. Very little should be modified here. The focus will be on Email Notification and Time Synchronization.

1. Define the customer’s SMTP Relay.

2. Click the ‘Test Mail Server Settings’ to send a test email.





Mail Relay Host: mail.halleen.com

Port Number: 25

Encryption Method: None

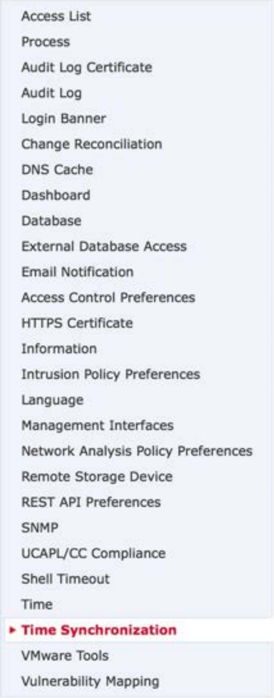
From Address: fmc@halleen.com

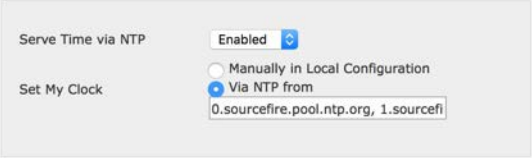
Use Authentication: □

Message sent

System Configuration, continued…

3. Verify the NTP settings are correct.




Serve Time via NTP: Enabled

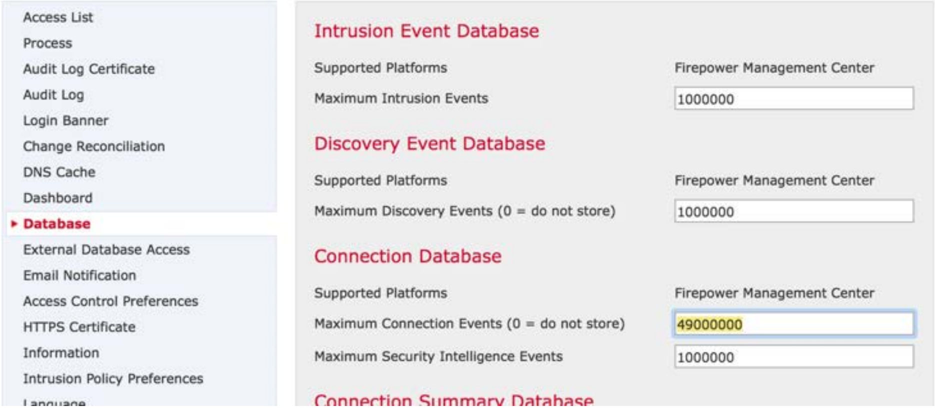
Set My Clock:
○ Manually in Local Configuration
● Via NTP from
0.sourcefire.pool.ntp.org, 1.sourcefi

System Configuration, continued…

Optional Setting: The Virtual FMC has a default size of 1,000,000 events in the Connection Database. Hardware FMC has a much larger size. Depending on the logging you enable, and the amount of traffic being monitored, you will exceed 1,000,000 events in hours or just a couple days.

4. Increase the Maximum Connection Events to NO MORE than 49,000,000. *(A smaller value will improve performance, so I typically start with 10,000,000 instead.)*

5. Click ‘Save’



Intrusion Event Database

Supported Platforms	Firepower Management Center
Maximum Intrusion Events	1000000

Discovery Event Database

Supported Platforms	Firepower Management Center
Maximum Discovery Events (0 = do not store)	1000000

Connection Database

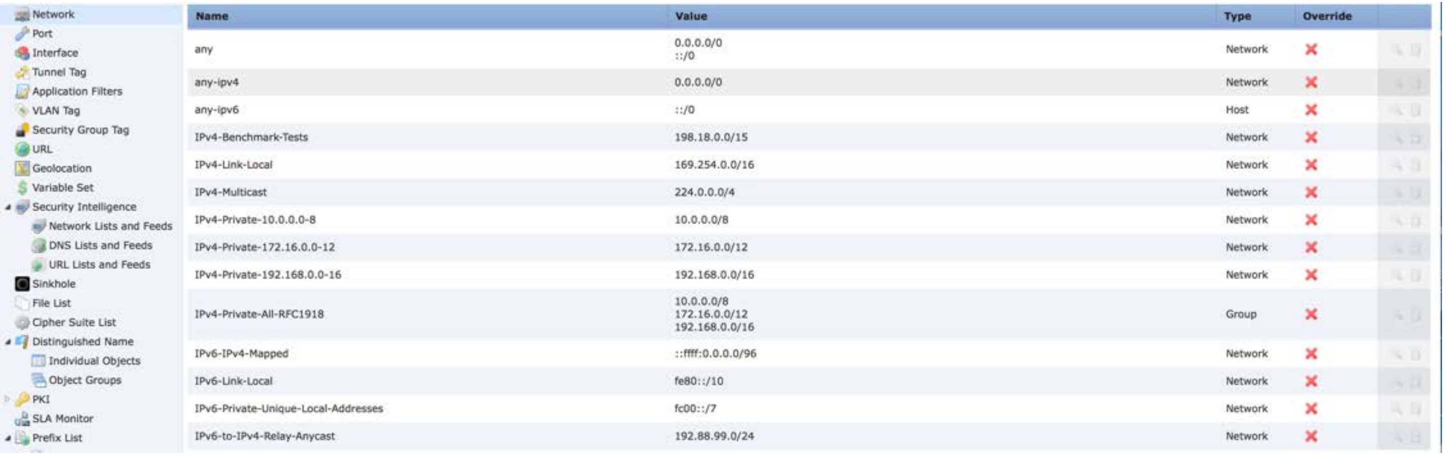
Supported Platforms	Firepower Management Center
Maximum Connection Events (0 = do not store)	49000000
Maximum Security Intelligence Events	1000000

Connection Summary Database

Network Objects

Network Objects can be used in many places to simplify rules, searches, and reports. However, this step can be considered optional unless there are segmented networks that might need special attention.

To add objects, click ‘Objects’.



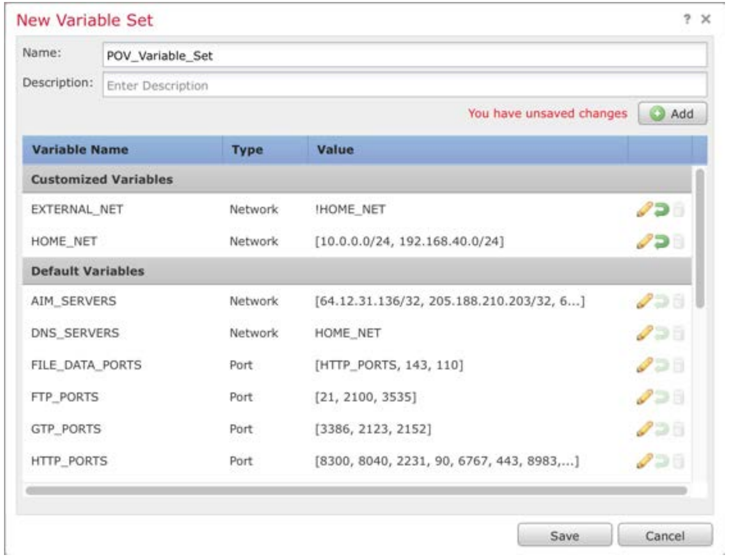
Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Network	✕
any-ipv4	0.0.0.0/0	Network	✕
any-ipv6	::/0	Host	✕
IPv4-Benchmark-Tests	198.18.0.0/15	Network	✕
IPv4-Link-Local	169.254.0.0/16	Network	✕
IPv4-Multicast	224.0.0.0/4	Network	✕
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	✕
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	✕
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	✕
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	✕
IPv6-IPv4-Mapped	::ffff:0.0.0.0/96	Network	✕
IPv6-Link-Local	fe80::/10	Network	✕
IPv6-Private-Unique-Local-Addresses	fc00::/7	Network	✕
IPv6-to-IPv4-Relay-Anycast	192.88.99.0/24	Network	✕

Variable Sets

Variable Sets are used to define ports and networks for use throughout the product. The POV will provide better results if the variables are customized.

Click ‘Objects’ -> ‘Variable Set’, and then click ‘Add Variable Set’.

1. Give your Variable Set a name (cannot use spaces).
2. Define HOME_NET as the IP addresses the customer uses.
3. Define EXTERNAL_NET as *excluding* the IP addresses the customer uses.



New Variable Set

Name: POV_Variable_Set

Description: Enter Description

You have unsaved changes

Variable Name	Type	Value
Customized Variables		
EXTERNAL_NET	Network	!HOME_NET
HOME_NET	Network	[10.0.0.0/24, 192.168.40.0/24]
Default Variables		
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]

Security Intelligence

Security Intelligence is the ability to Block or Monitor traffic to/from hosts that are known to participate in different types of unwanted behavior. For example, you likely do not want hosts that are know to attack other networks, or who participate in Botnets to communicate with your hosts.

Firepower 6.1 supports both IP address lists, as well as DNS and URL. In order to take advantage of these feeds, you need to initially Update the Feeds.

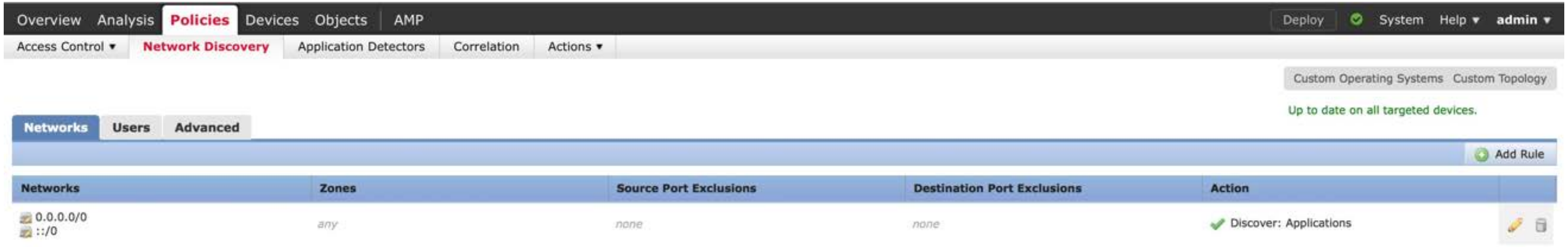
Click ‘Objects’ -> ‘Security Intelligence’ -> ’Network Lists and Feeds’, and then click the ‘Update Feeds’ button.

Network Discovery Policy

The Network Discovery Policy defines which areas of the network you’d like FMC to learn about hosts, users, and applications. In general, this should be ALL of the IP addresses used by the customer.

By default, FMC is set to learn Applications from the entire world.

1. Delete the default entry (0.0.0.0/0) by clicking on the Trash icon.



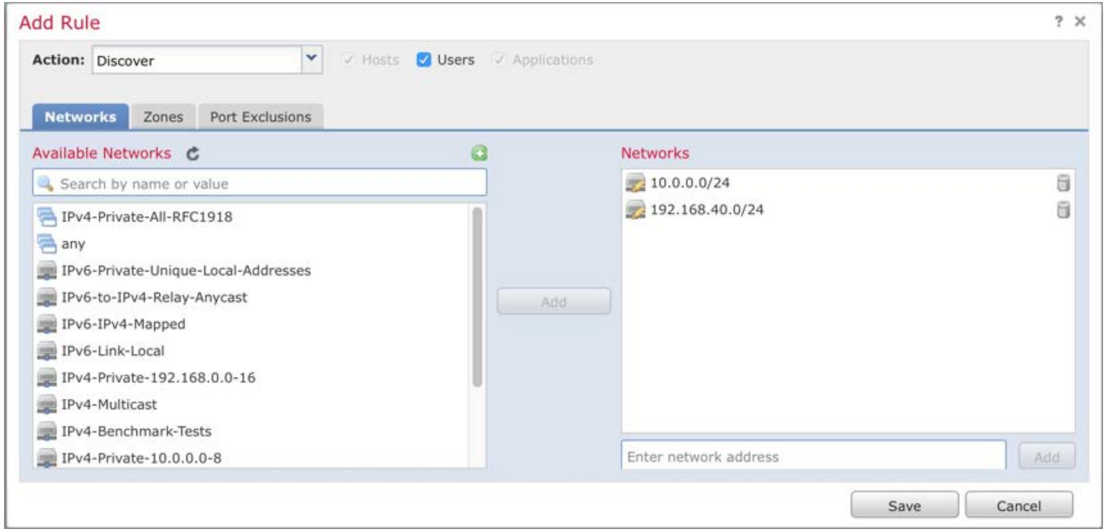
Up to date on all targeted devices.

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

Network Discovery Policy, continued…

2. Click ‘Add Rule’ and add the customer’s networks. *(you can use Network Objects if they were defined earlier)*

3. Click ‘Save’.



Add Rule

Action: Discover

✓ Hosts ☑ Users ✓ Applications

Available Networks

- IPv4-Private-All-RFC1918
- any
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast
- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv4-Private-192.168.0.0-16
- IPv4-Multicast
- IPv4-Benchmark-Tests
- IPv4-Private-10.0.0.0-8

Networks

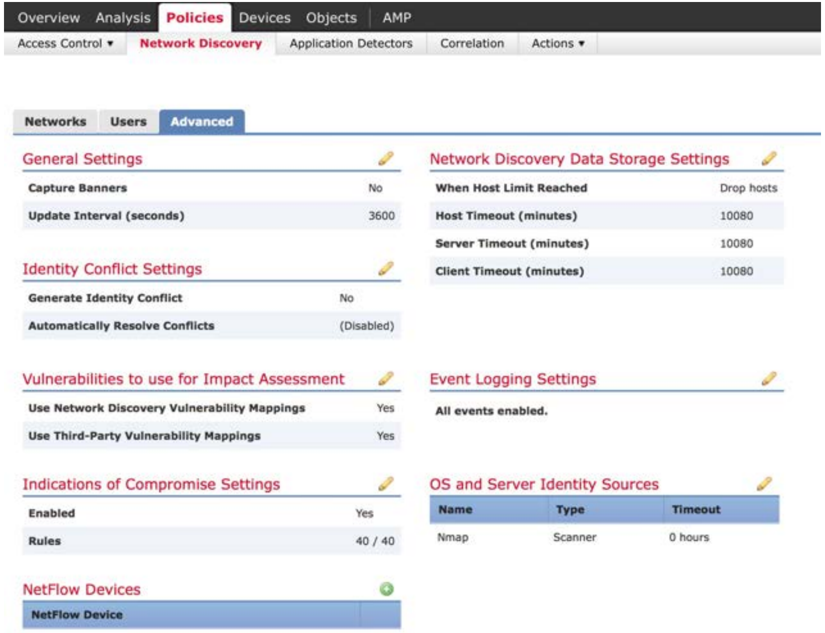
- 10.0.0.0/24
- 192.168.40.0/24

Network Discovery Policy, continued…

4. Click the ‘Advanced’ tab.

5. Set “Capture Banners” to Yes.
   This setting improves the accuracy of the application detection capability.

6. Click the ‘Deploy’ button.



General Settings

Capture Banners	No
Update Interval (seconds)	3600

Identity Conflict Settings

Generate Identity Conflict	No
Automatically Resolve Conflicts	(Disabled)

Vulnerabilities to use for Impact Assessment

Use Network Discovery Vulnerability Mappings	Yes
Use Third-Party Vulnerability Mappings	Yes

Indications of Compromise Settings

Enabled	Yes
Rules	40 / 40

NetFlow Devices

NetFlow Device

Network Discovery Data Storage Settings

When Host Limit Reached	Drop hosts
Host Timeout (minutes)	10080
Server Timeout (minutes)	10080
Client Timeout (minutes)	10080

Event Logging Settings

All events enabled.

OS and Server Identity Sources

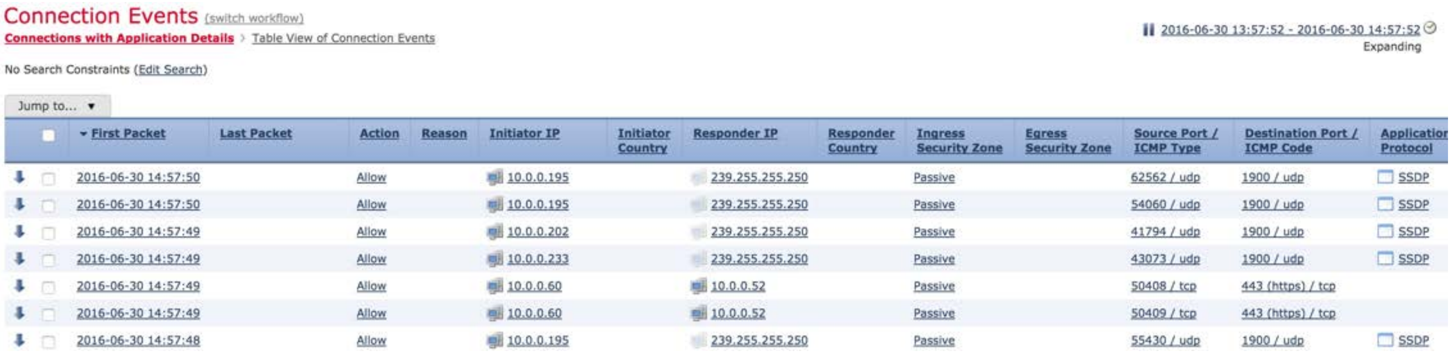
Name	Type	Timeout
Nmap	Scanner	0 hours

Check Traffic

Click on ‘Analysis’ -> ‘Connections’ -> ‘Events’.

You should notice the colors of the computer icons have changed in many cases.

Blue – Host on Customer’s Network.
Grey – Host not on Customer’s Network.
Red – Host with IoC (Indicator of Compromise) on Customer’s Network.



Connection Events (switch workflow)
Connections with Application Details > Table View of Connection Events

2016-06-30 13:57:52 - 2016-06-30 14:57:52
Expanding

No Search Constraints (Edit Search)

Jump to... ▾

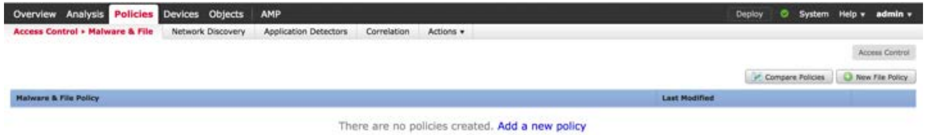
	□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Applicatior Protocol
⬇	□	2016-06-30 14:57:50		Allow		10.0.0.195		239.255.255.250		Passive		62562 / udp	1900 / udp	SSDP
⬇	□	2016-06-30 14:57:50		Allow		10.0.0.195		239.255.255.250		Passive		54060 / udp	1900 / udp	SSDP
⬇	□	2016-06-30 14:57:49		Allow		10.0.0.202		239.255.255.250		Passive		41794 / udp	1900 / udp	SSDP
⬇	□	2016-06-30 14:57:49		Allow		10.0.0.233		239.255.255.250		Passive		43073 / udp	1900 / udp	SSDP
⬇	□	2016-06-30 14:57:49		Allow		10.0.0.60		10.0.0.52		Passive		50408 / tcp	443 (https) / tcp	
⬇	□	2016-06-30 14:57:49		Allow		10.0.0.60		10.0.0.52		Passive		50409 / tcp	443 (https) / tcp	
⬇	□	2016-06-30 14:57:48		Allow		10.0.0.195		239.255.255.250		Passive		55430 / udp	1900 / udp	SSDP

File Policy

In a POV, we want a File Policy that only Monitors for Visibility Purposes

Malware & File Policy

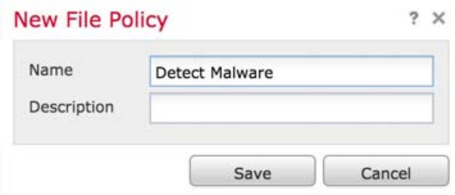
1. Select ‘Policies’ -> ‘Access Control’ -> ‘Malware & File’



Malware & File Policy	Last Modified

There are no policies created. Add a new policy

2. New File Policy



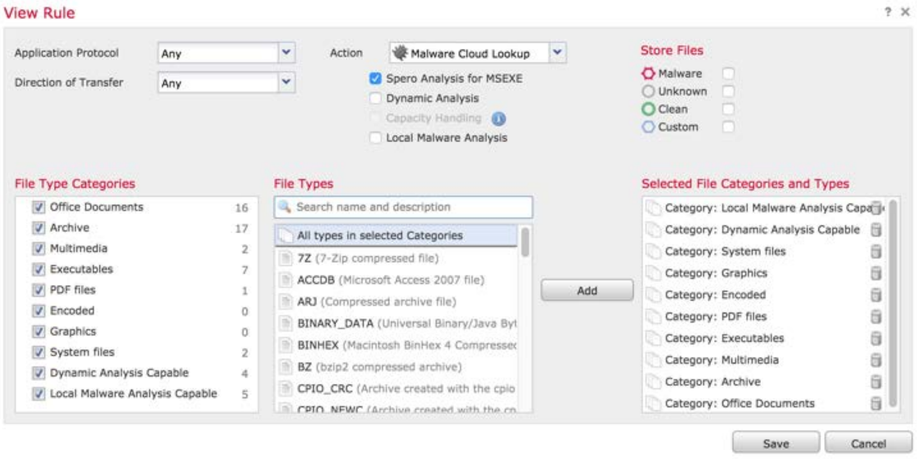
Name: Detect Malware

Description:

3. Add Rule

4. Select All File Categories, and Spero Analysis for MSEXE

5. Save



Application Protocol: Any

Direction of Transfer: Any

Action: Malware Cloud Lookup

☑ Spero Analysis for MSEXE
☐ Dynamic Analysis
☐ Capacity Handling
☐ Local Malware Analysis

Store Files

Malware	☐
Unknown	☐
Clean	☐
Custom	☐

File Type Categories

☑ Office Documents	16
☑ Archive	17
☑ Multimedia	2
☑ Executables	7
☑ PDF files	1
☑ Encoded	0
☑ Graphics	0
☑ System files	2
☑ Dynamic Analysis Capable	4
☑ Local Malware Analysis Capable	5

File Types

Search name and description

- All types in selected Categories
- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY_DATA (Universal Binary/Java Byt
- BINHEX (Macintosh BinHex 4 Compressec
- BZ (bzip2 compressed archive)
- CPIO_CRC (Archive created with the cpio
- CPIO_NEWC (Archive created with the cp

Selected File Categories and Types

- Category: Local Malware Analysis Capa
- Category: Dynamic Analysis Capable
- Category: System files
- Category: Graphics
- Category: Encoded
- Category: PDF files
- Category: Executables
- Category: Multimedia
- Category: Archive
- Category: Office Documents

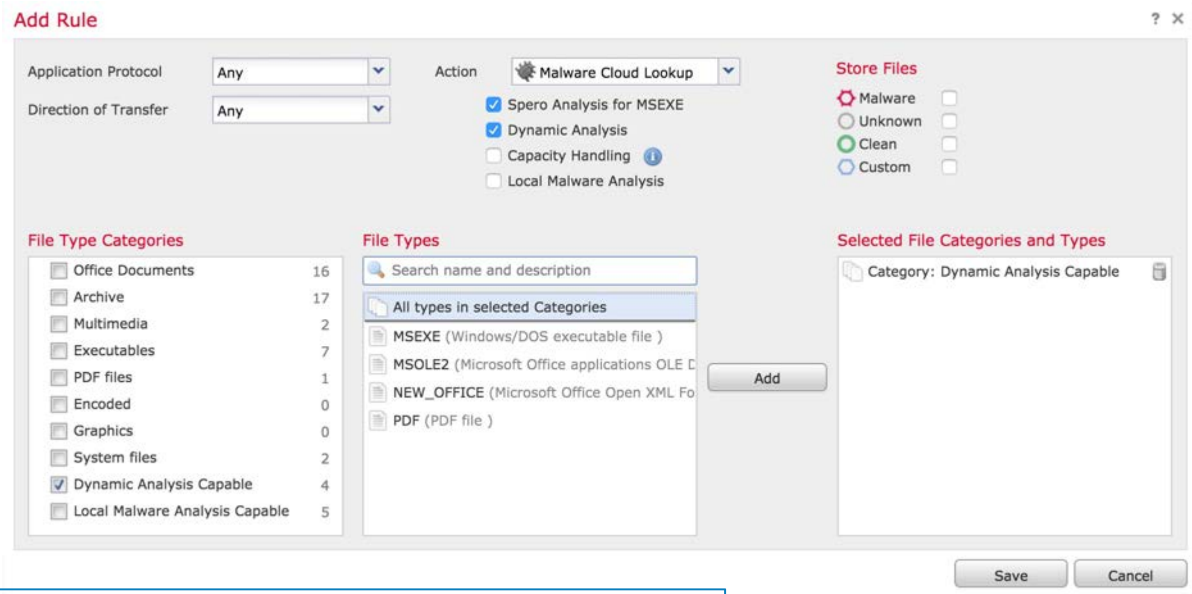
Malware & File Policy, continued…

6. Add another Rule

7. Select 'Dynamic Analysis Capable' as well as 'Spero Analysis for MSEXE'

8. Save

9. Save Policy



Add Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Malware Cloud Lookup

☑ Spero Analysis for MSEXE
☑ Dynamic Analysis
☐ Capacity Handling
☐ Local Malware Analysis

Store Files

- Malware ☐
- Unknown ☐
- Clean ☐
- Custom ☐

File Type Categories

☐ Office Documents	16
☐ Archive	17
☐ Multimedia	2
☐ Executables	7
☐ PDF files	1
☐ Encoded	0
☐ Graphics	0
☐ System files	2
☑ Dynamic Analysis Capable	4
☐ Local Malware Analysis Capable	5

File Types

Search name and description

- All types in selected Categories
- MSEXE (Windows/DOS executable file)
- MSOLE2 (Microsoft Office applications OLE D
- NEW_OFFICE (Microsoft Office Open XML Fo
- PDF (PDF file)

Selected File Categories and Types

Category: Dynamic Analysis Capable

Note: Dynamic Analysis will transmit Unknown files to the Talos cloud for analysis. If the customer is sensitive to this, skip this second rule. Optionally, you could exclude NEW_OFFICE and PDF from the included file types to reduce the chance of sending sensitive data.

Intrusion Policy

Intrusion Policy

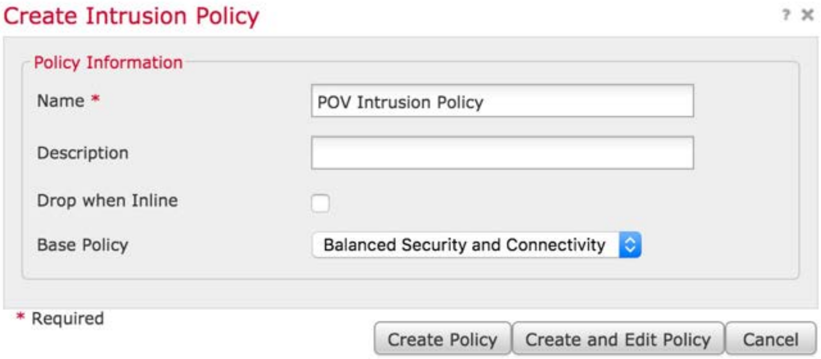
1. Select ‘Policies’ -> ‘Access Control’ -> ‘Intrusion’

2. Create a New Policy

3. Uncheck ‘Drop when Inline’

4. The ‘Balanced Security and Connectivity’ base policy is usually a good policy to start with.

5. Click ‘Create and Edit Policy’



Create Intrusion Policy

Policy Information

Name * POV Intrusion Policy

Description

Drop when Inline □

Base Policy Balanced Security and Connectivity

* Required

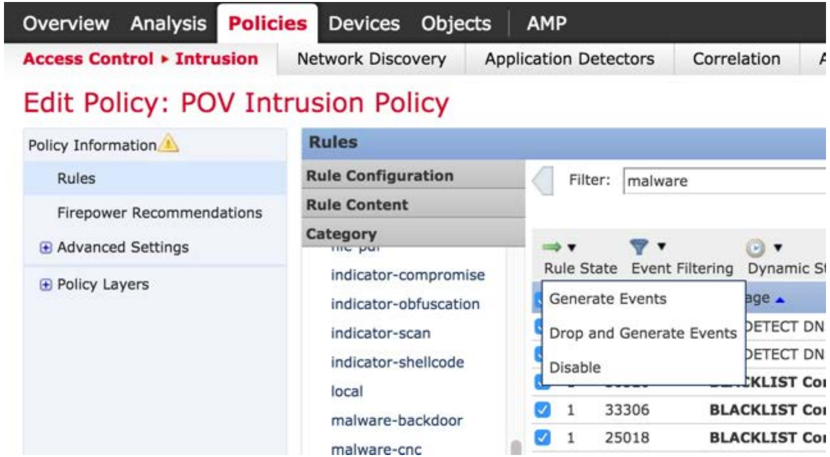
Intrusion Policy, continued…

6. Type “malware” in the Filter line and press ENTER.

7. Check the checkbox on the blue line to select all rules.

8. Click on ‘Rule State’ and select ’Drop and Generate’.

9. Clear the filter, and then click on ’Exploit Kit’ in the Category list. Select these, as well, and set them to ‘Drop and Generate’.



Edit Policy: POV Intrusion Policy

Filter: malware

indicator-compromise
indicator-obfuscation
indicator-scan
indicator-shellcode
local
malware-backdoor
malware-cnc

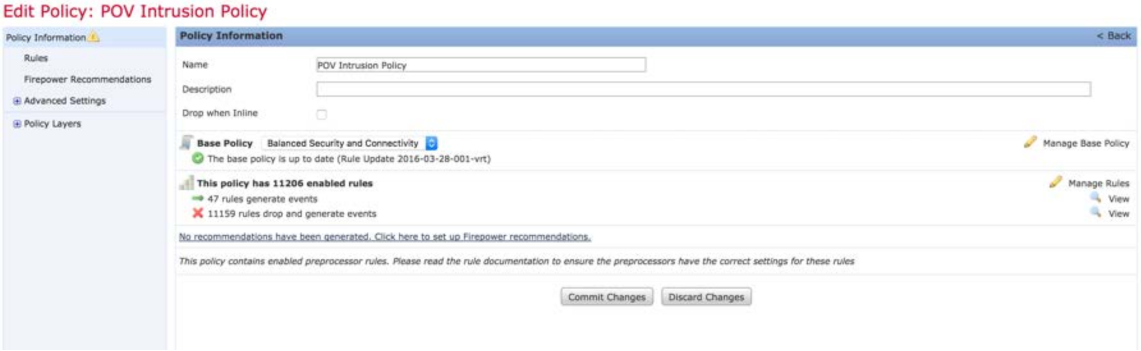
☑	1	33306	BLACKLIST Co
☑	1	25018	BLACKLIST Co

Intrusion Policy, continued…

10. Consider looking at other Categories, as well.
    - Blacklist
    - PUA

11. Click on ‘Policy Information’.

12. Click on ‘Commit Changes’.



Edit Policy: POV Intrusion Policy

Policy Information

Name: POV Intrusion Policy

Description:

Drop when Inline: □

Base Policy: Balanced Security and Connectivity

The base policy is up to date (Rule Update 2016-03-28-001-vrt)

This policy has 11206 enabled rules

47 rules generate events

11159 rules drop and generate events

No recommendations have been generated. Click here to set up Firepower recommendations.

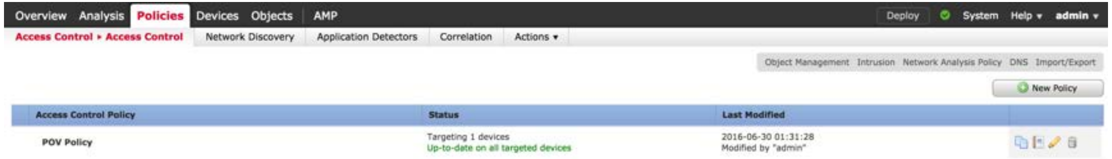
This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules

Access Control Policy

Access Control Policy

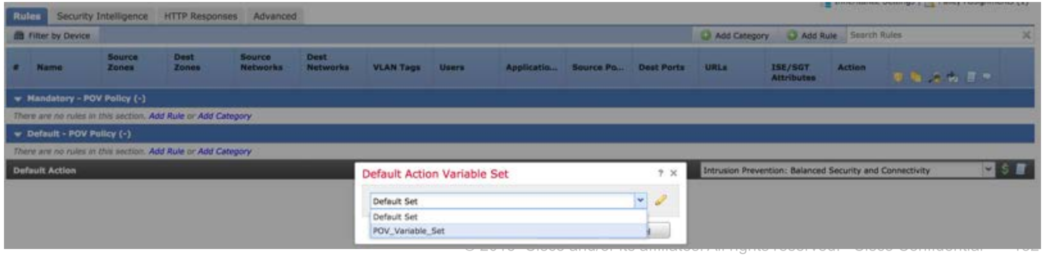
1. Click ‘Policies’ *(or you can click ‘Policies’ -> ‘Access Control’)*

2. Select your Access Control Policy. To edit it, you can click the name of the policy, or click the pencil icon.



Access Control Policy	Status	Last Modified
POV Policy	Targeting 1 devices Up-to-date on all targeted devices	2016-06-30 01:31:28 Modified by "admin"

3. Click the Green $ sign on the bottom of the page and select the POV Variable Set you created earlier.



▾ Mandatory - POV Policy (-)

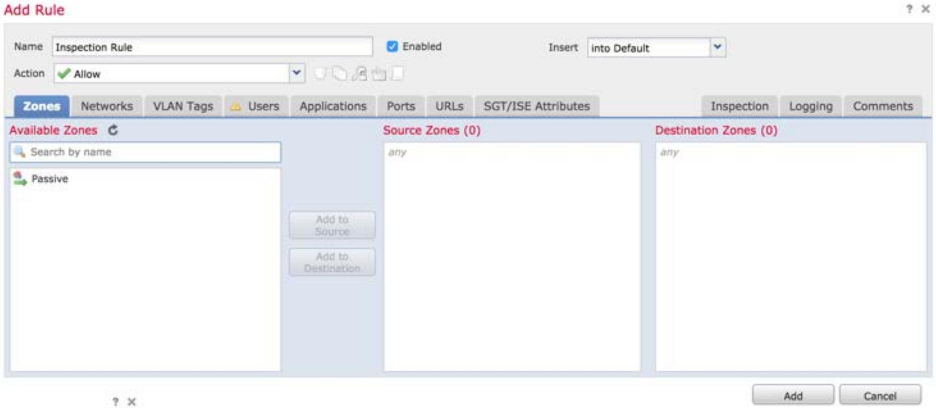
There are no rules in this section. Add Rule *or* Add Category

▾ Default - POV Policy (-)

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

Access Control Policy, continued…

4. Click ‘Add Rule’.
   Name – Inspection Rule
   Action – Allow
   Insert – into Default



Add Rule

Name: Inspection Rule ☑ Enabled Insert: into Default

Action: ✓ Allow

Available Zones

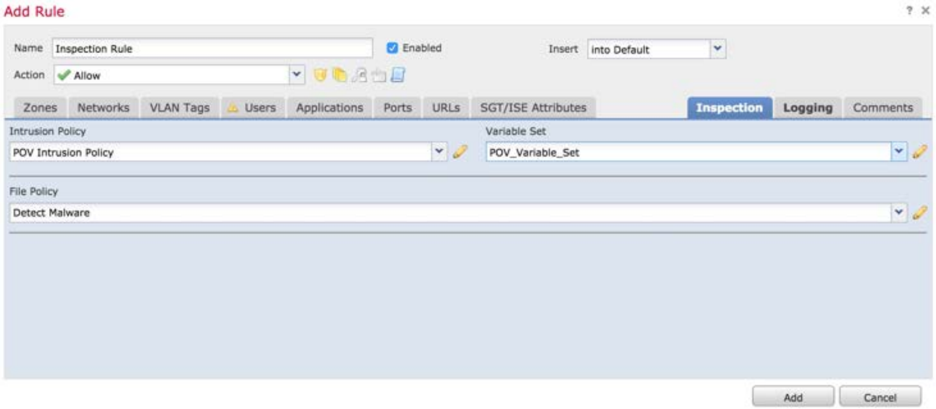
Passive

Source Zones (0)

any

Destination Zones (0)

any



Add Rule

Name: Inspection Rule ☑ Enabled Insert: into Default

Action: ✓ Allow

Intrusion Policy: POV Intrusion Policy

Variable Set: POV_Variable_Set

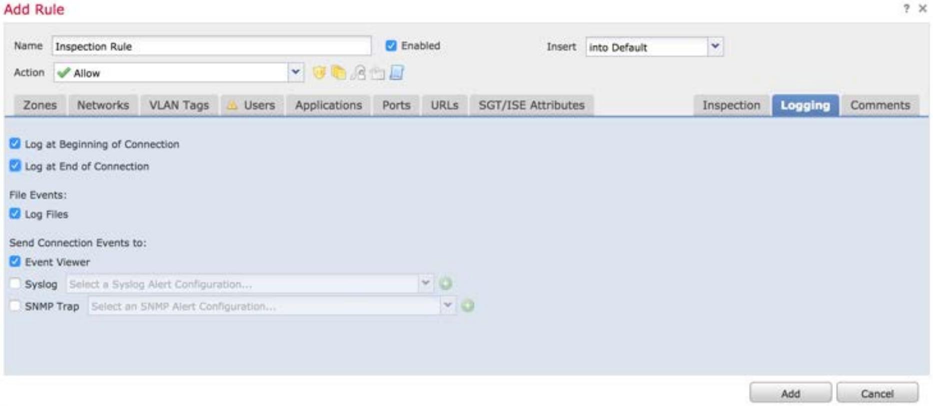
File Policy: Detect Malware

5. Click ‘Inspection’
   Intrusion Policy – POV Policy
   File Policy – Detect Malware
   Variable Set – POV Variable Set

Access Control Policy, continued…

4. Click ‘Logging’.
   Log at Beginning and End

5. Click ‘Add’.



Add Rule

Name: Inspection Rule

☑ Enabled

Insert: into Default

Action: ✓ Allow

☑ Log at Beginning of Connection

☑ Log at End of Connection

File Events:

☑ Log Files

Send Connection Events to:

☑ Event Viewer

□ Syslog: Select a Syslog Alert Configuration...

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

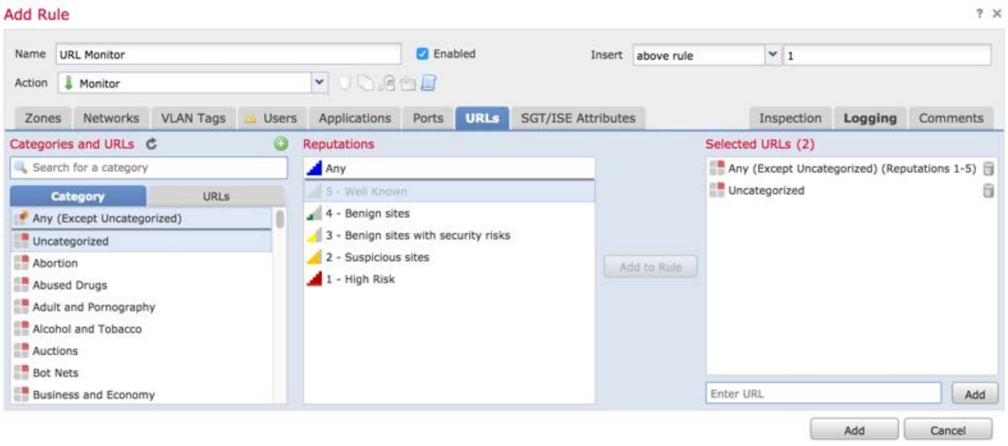
Access Control Policy, continued…

6. Recommended URL Monitoring
   Create ”URL Monitor” rule, inserting it ABOVE Rule 1.

7. Click ‘URLs’

8. Select ‘Any (Except Uncategorized)’, as well as ’Uncategorized’, in the first box.

9. Select ‘5 – Well Known’, and click ‘Add to Rule’



Add Rule

Name: URL Monitor ☑ Enabled Insert: above rule 1

Action: Monitor

Categories and URLs

- Any (Except Uncategorized)
- Uncategorized
- Abortion
- Abused Drugs
- Adult and Pornography
- Alcohol and Tobacco
- Auctions
- Bot Nets
- Business and Economy

Reputations

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

Selected URLs (2)

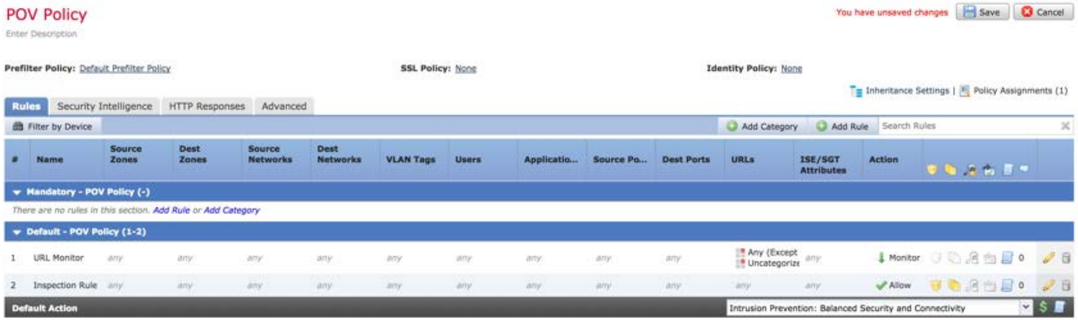
- Any (Except Uncategorized) (Reputations 1-5)
- Uncategorized

10. Enable Logging, and Click ‘Add’.

Access Control Policy, continued…

11. Policy should look like this.

12. Click on ‘Security Intelligence’.



POV Policy

Enter Description

You have unsaved changes Save Cancel

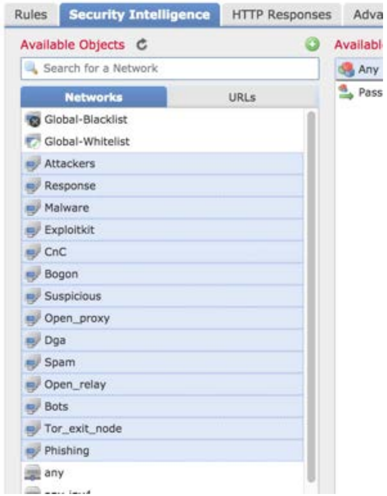
Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

Inheritance Settings | Policy Assignments (1)

Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Po...	Dest Ports	URLs	ISE/SGT Attributes	Action	
Mandatory - POV Policy (-)														
There are no rules in this section. Add Rule or Add Category														
Default - POV Policy (1-2)														
1	URL Monitor	any	any	any	any	any	any	any	any	any	Any (Except Uncategorize	any	Monitor	0
2	Inspection Rule	any	any	any	any	any	any	any	any	any	any	any	✓ Allow	0
Default Action													Intrusion Prevention: Balanced Security and Connectivity	



Rules | **Security Intelligence** | HTTP Responses | Adva

Available Objects Availabl

Search for a Network

Networks | URLs

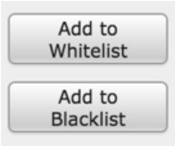
- Global-Blacklist
- Global-Whitelist
- Attackers
- Response
- Malware
- Exploitkit
- CnC
- Bogon
- Suspicious
- Open_proxy
- Dga
- Spam
- Open_relay
- Bots
- Tor_exit_node
- Phishing
- any

Any

Pass

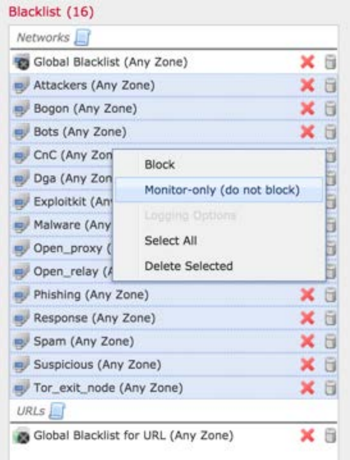
13. Select ‘Attackers’ thru ‘Phishing’.

14. Click ‘Add to Blacklist’.



Access Control Policy, continued…

15. Select the objects in the Blacklist box, and right-click to set to ’Monitor-only’.



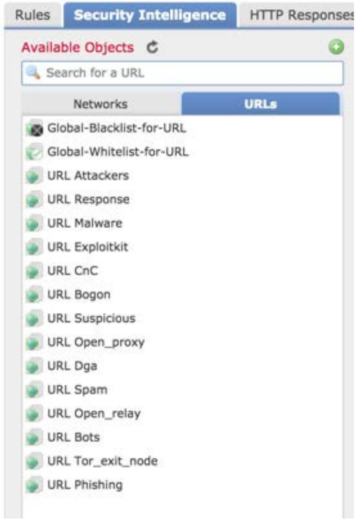
Blacklist (16)

Networks

- Global Blacklist (Any Zone)
- Attackers (Any Zone)
- Bogon (Any Zone)
- Bots (Any Zone)
- CnC (Any Zon
- Dga (Any Zon
- Exploitkit (An
- Malware (Any
- Open_proxy (
- Open_relay (A
- Phishing (Any Zone)
- Response (Any Zone)
- Spam (Any Zone)
- Suspicious (Any Zone)
- Tor_exit_node (Any Zone)

URLs

- Global Blacklist for URL (Any Zone)



Available Objects

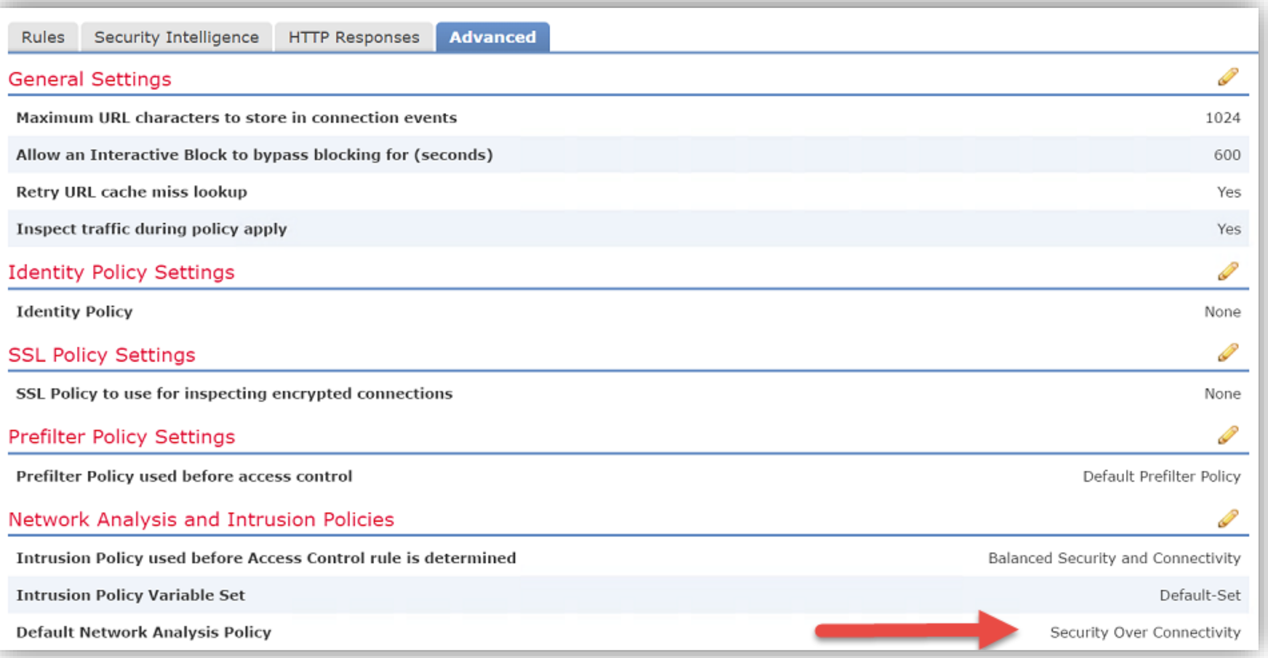
Search for a URL

- Global-Blacklist-for-URL
- Global-Whitelist-for-URL
- URL Attackers
- URL Response
- URL Malware
- URL Exploitkit
- URL CnC
- URL Bogon
- URL Suspicious
- URL Open_proxy
- URL Dga
- URL Spam
- URL Open_relay
- URL Bots
- URL Tor_exit_node
- URL Phishing

16. Click the ‘URLs’ tab and repeat the same settings.

17. Click ‘Save’ and then Deploy the settings.

Advanced Tab: Default Network Analysis Policy



General Settings

Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
Retry URL cache miss lookup	Yes
Inspect traffic during policy apply	Yes

Identity Policy Settings

Identity Policy	None

SSL Policy Settings

SSL Policy to use for inspecting encrypted connections	None

Prefilter Policy Settings

Prefilter Policy used before access control	Default Prefilter Policy

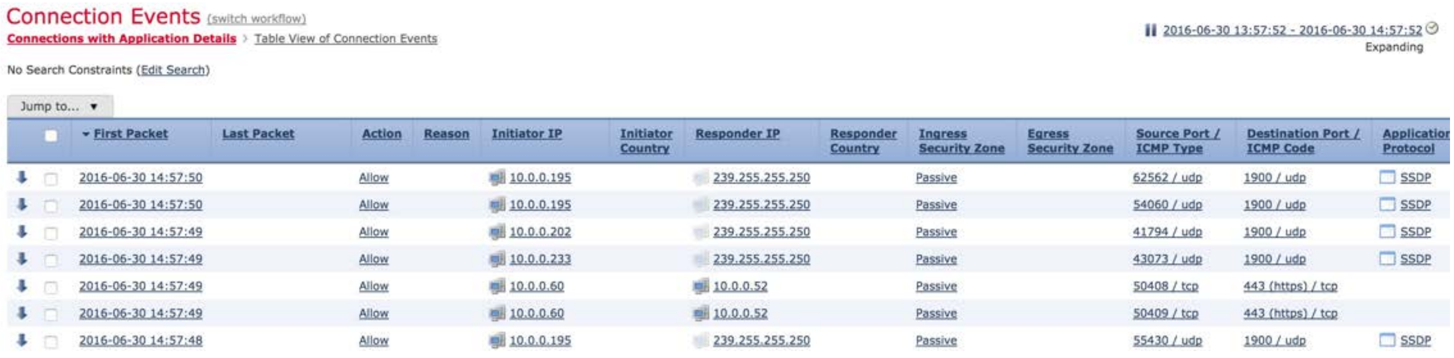
Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined	Balanced Security and Connectivity
Intrusion Policy Variable Set	Default-Set
Default Network Analysis Policy	Security Over Connectivity

Break or Lunch Time

Check Traffic

Click on ‘Analysis’ -> ‘Connections’ -> ‘Events’.



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

2016-06-30 13:57:52 - 2016-06-30 14:57:52

Expanding

Jump to... ▼

	☐	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Applicatior Protocol
⬇	☐	2016-06-30 14:57:50		Allow		10.0.0.195		239.255.255.250		Passive		62562 / udp	1900 / udp	SSDP
⬇	☐	2016-06-30 14:57:50		Allow		10.0.0.195		239.255.255.250		Passive		54060 / udp	1900 / udp	SSDP
⬇	☐	2016-06-30 14:57:49		Allow		10.0.0.202		239.255.255.250		Passive		41794 / udp	1900 / udp	SSDP
⬇	☐	2016-06-30 14:57:49		Allow		10.0.0.233		239.255.255.250		Passive		43073 / udp	1900 / udp	SSDP
⬇	☐	2016-06-30 14:57:49		Allow		10.0.0.60		10.0.0.52		Passive		50408 / tcp	443 (https) / tcp	
⬇	☐	2016-06-30 14:57:49		Allow		10.0.0.60		10.0.0.52		Passive		50409 / tcp	443 (https) / tcp	
⬇	☐	2016-06-30 14:57:48		Allow		10.0.0.195		239.255.255.250		Passive		55430 / udp	1900 / udp	SSDP

Ideally, FMC will need a couple hours to “learn” the network now. This is a good time to go to lunch, take a long break, or stop for the day.

All initial setup steps have been completed.

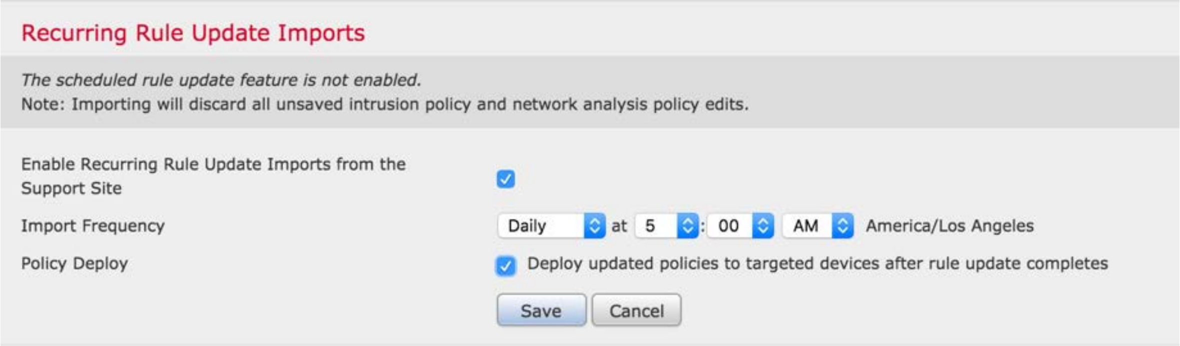
Post-Install Steps

Configure Updates

Rule and Geolocation Updates

Click on ‘System’ -> ‘Updates’, and then click on ‘Rule Updates’.

Enable Recurring Updates. It’s a good idea to also manually update everywhere, as well.



Recurring Rule Update Imports

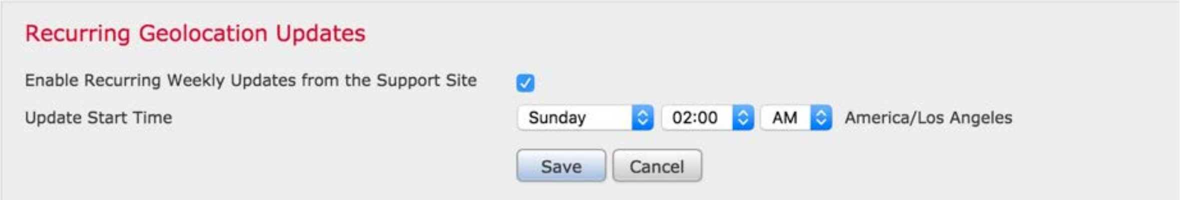
The scheduled rule update feature is not enabled.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site ☑

Import Frequency: Daily at 5 : 00 AM America/Los Angeles

Policy Deploy: ☑ Deploy updated policies to targeted devices after rule update completes

Click on ‘Geolocation Updates’ and enable recurring updates, as well.



Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site ☑

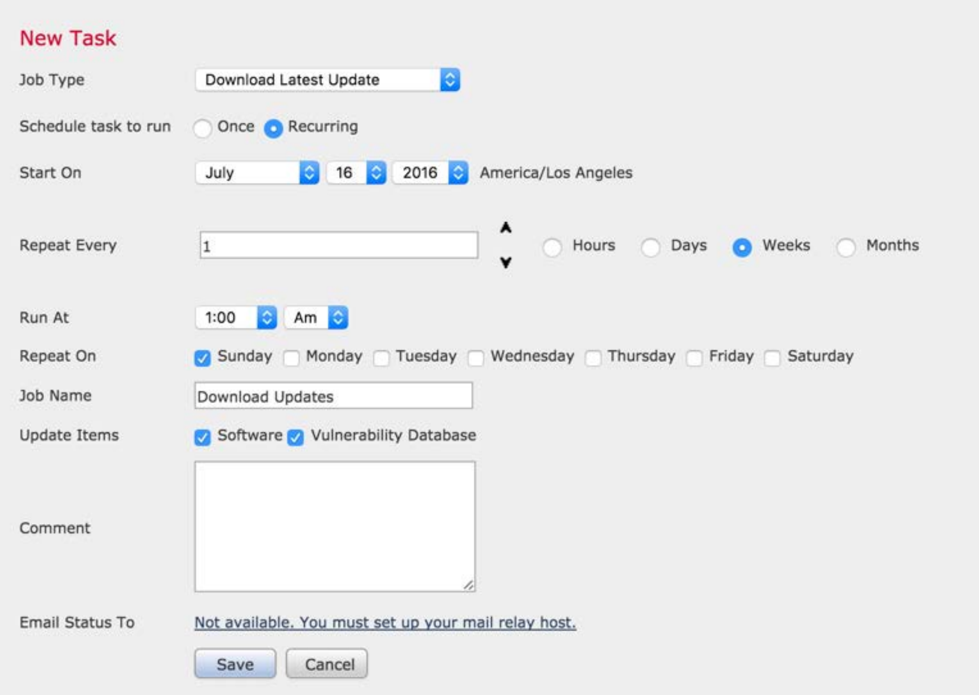
Update Start Time: Sunday 02:00 AM America/Los Angeles

Vulnerability Database and System Software

Click on ‘System’ -> ‘Scheduling’, and then click on ‘Add Task’.

Create a Task to Download Latest Update on a scheduled basis.

When creating Recurring Tasks, make sure you select Tomorrow’s date as the Start On. Otherwise, you’ll get an error later.



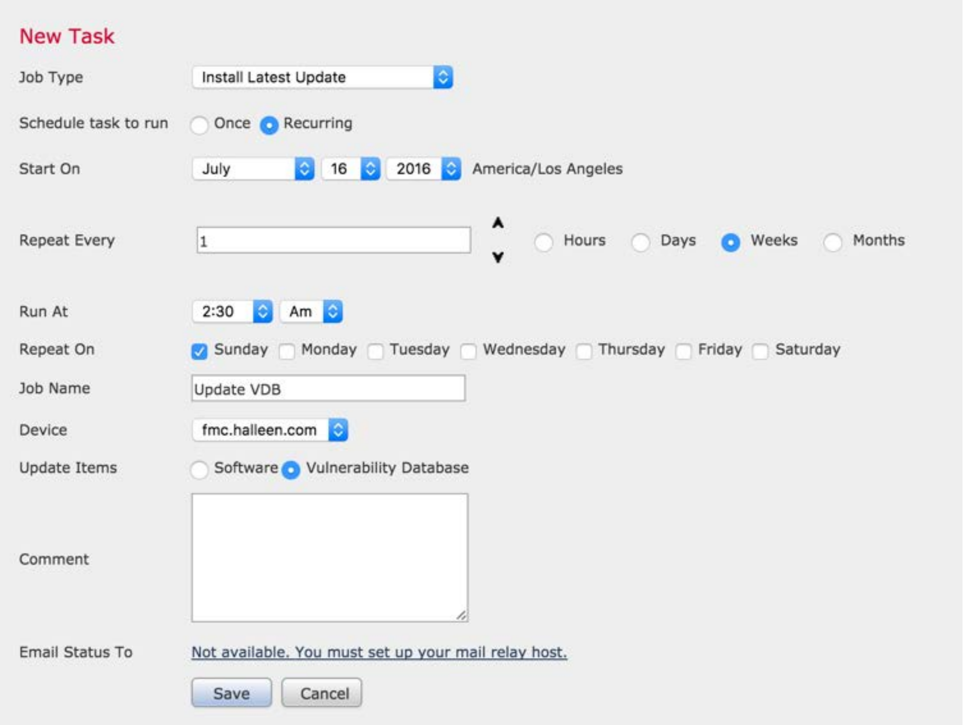
New Task

Job Type	Download Latest Update
Schedule task to run	○ Once ● Recurring
Start On	July 16 2016 America/Los Angeles
Repeat Every	1 ○ Hours ○ Days ● Weeks ○ Months
Run At	1:00 Am
Repeat On	☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
Job Name	Download Updates
Update Items	☑ Software ☑ Vulnerability Database
Comment	
Email Status To	Not available. You must set up your mail relay host.

Vulnerability Database and System Software

Create another Task to Update the Vulnerability Database.

We strongly recommend against automatically updating Software, but the Vulnerability Database is good to update.



New Task

Job Type: Install Latest Update

Schedule task to run: ○ Once ● Recurring

Start On: July 16 2016 America/Los Angeles

Repeat Every: 1 ○ Hours ○ Days ● Weeks ○ Months

Run At: 2:30 Am

Repeat On: ☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Job Name: Update VDB

Device: fmc.halleen.com

Update Items: ○ Software ● Vulnerability Database

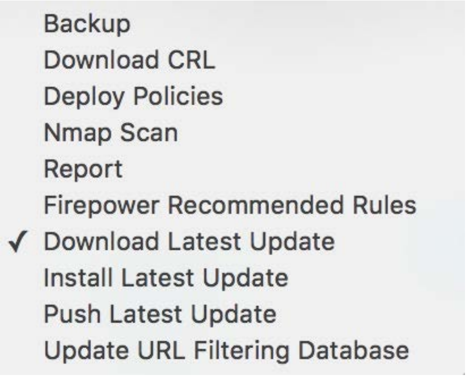
Comment:

Email Status To: Not available. You must set up your mail relay host.

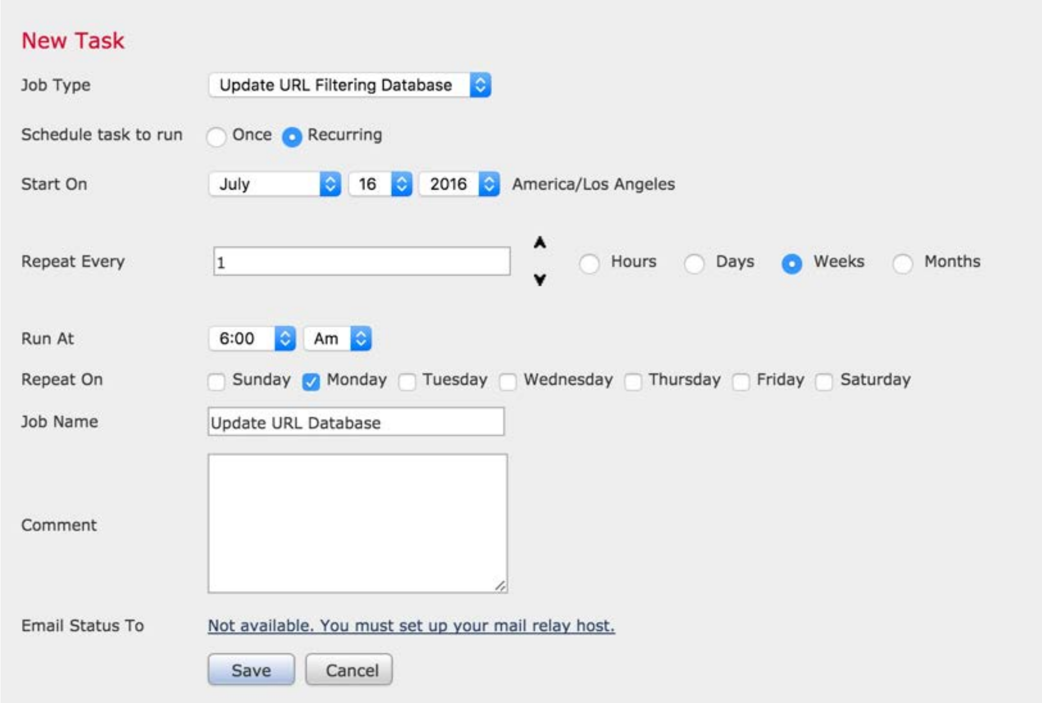
Update URL Database

Create a Task to update the URL database.

See this list to understand what other types of tasks you can create, if needed:



Backup
Download CRL
Deploy Policies
Nmap Scan
Report
Firepower Recommended Rules
✓ Download Latest Update
Install Latest Update
Push Latest Update
Update URL Filtering Database



New Task

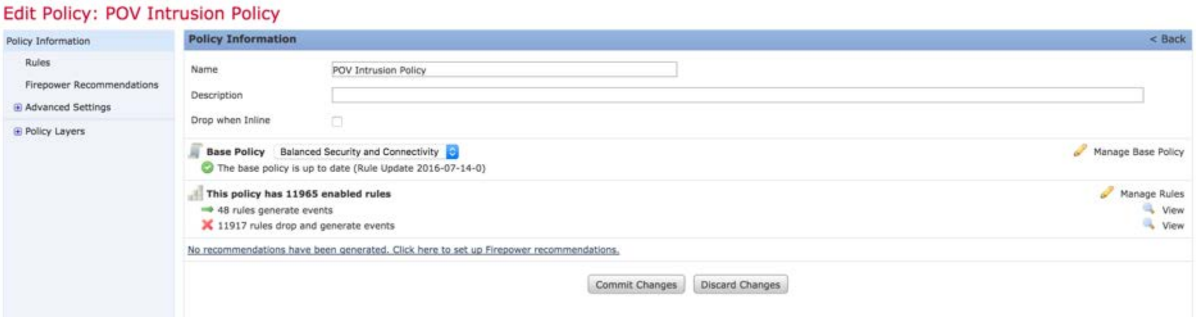
Job Type	Update URL Filtering Database
Schedule task to run	○ Once ● Recurring
Start On	July 16 2016 America/Los Angeles
Repeat Every	1 ○ Hours ○ Days ● Weeks ○ Months
Run At	6:00 Am
Repeat On	□ Sunday ☑ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
Job Name	Update URL Database
Comment	
Email Status To	Not available. You must set up your mail relay host.

Firesight Recommendations

Enable Firesight Recommendations

Click on ‘Policies’ -> ‘Intrusion’, and then edit the intrusion policy you created earlier.

Firesight Recommendations are useful for automatically tuning the IPS policy for your customer’s environment. It is most effective after the system has had a minimum of several hours to “learn” the network.



Edit Policy: POV Intrusion Policy

Policy Information

Name: POV Intrusion Policy

Description:

Drop when Inline: □

Base Policy: Balanced Security and Connectivity

The base policy is up to date (Rule Update 2016-07-14-0)

This policy has 11965 enabled rules

48 rules generate events

11917 rules drop and generate events

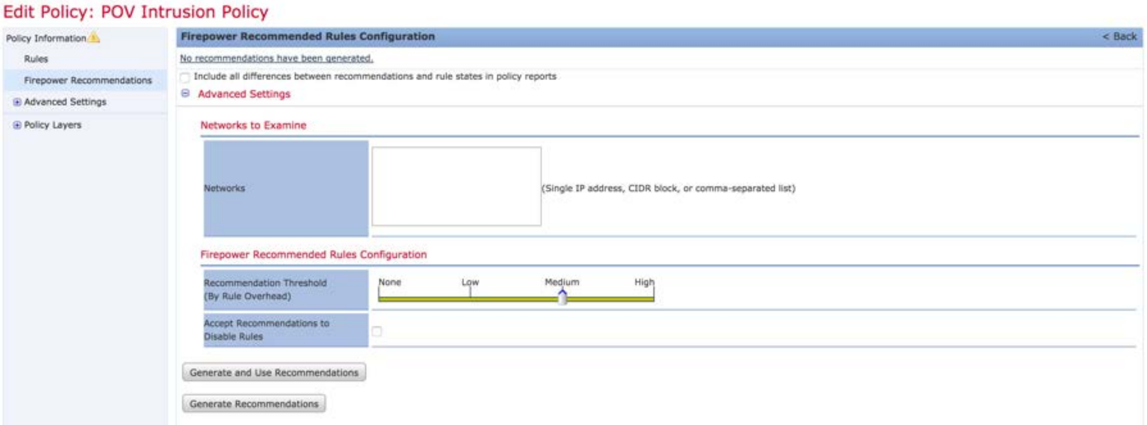
No recommendations have been generated. Click here to set up Firepower recommendations.

Enable Firesight Recommendations, cont…

Click on ‘Advanced Settings’, and Uncheck the option to Disable Rules.

In production deployments, customers will often leave this setting Checked, but in a POV, it is best to Uncheck it and leave more rules enabled.

Click ‘Generate and Use Recommendations’.



Edit Policy: POV Intrusion Policy

Firepower Recommended Rules Configuration

No recommendations have been generated.

□ Include all differences between recommendations and rule states in policy reports

⊖ Advanced Settings

Networks to Examine

Networks: (Single IP address, CIDR block, or comma-separated list)

Firepower Recommended Rules Configuration

Recommendation Threshold (By Rule Overhead): None Low Medium High

Accept Recommendations to Disable Rules: □

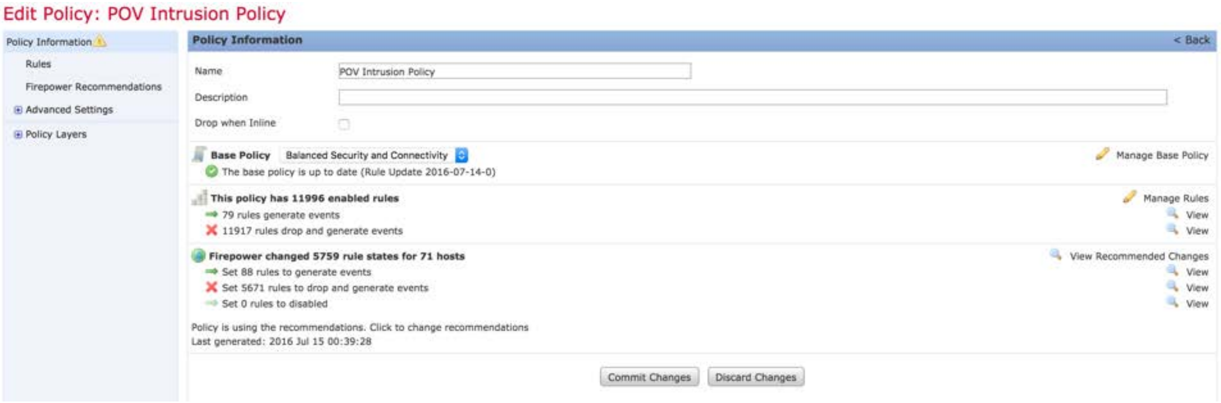
Enable Firesight Recommendations, cont…

Click on ‘Policy Information’

Verify Firepower is changing several rule states, and leaving most enabled.

Click ‘Commit Changes’

Deploy Changes.



Edit Policy: POV Intrusion Policy

Policy Information

Name: POV Intrusion Policy

Description:

Drop when Inline: □

Base Policy Balanced Security and Connectivity

The base policy is up to date (Rule Update 2016-07-14-0)

This policy has 11996 enabled rules

79 rules generate events

11917 rules drop and generate events

Firepower changed 5759 rule states for 71 hosts

Set 88 rules to generate events

Set 5671 rules to drop and generate events

Set 0 rules to disabled

Policy is using the recommendations. Click to change recommendations

Last generated: 2016 Jul 15 00:39:28

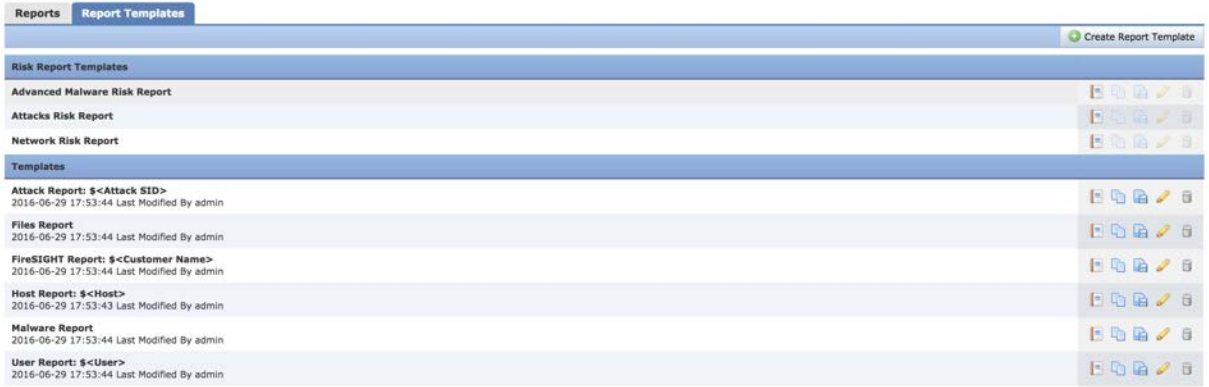
Risk Reports

Risk Reports

Click on ‘Overview’ -> ‘Reporting’ -> ‘Report Templates’

Risk Reports are executive-style reports, and are integrated into the 6.1 FMC release.

These reports should be run near the end of the POV rather than at the beginning. It is recommended to wait a minimum of one week before running them.



Risk Report Templates

Advanced Malware Risk Report

Attacks Risk Report

Network Risk Report

Templates

Attack Report: $<Attack SID>
2016-06-29 17:53:44 Last Modified By admin

Files Report
2016-06-29 17:53:44 Last Modified By admin

FireSIGHT Report: $<Customer Name>
2016-06-29 17:53:44 Last Modified By admin

Host Report: $<Host>
2016-06-29 17:53:43 Last Modified By admin

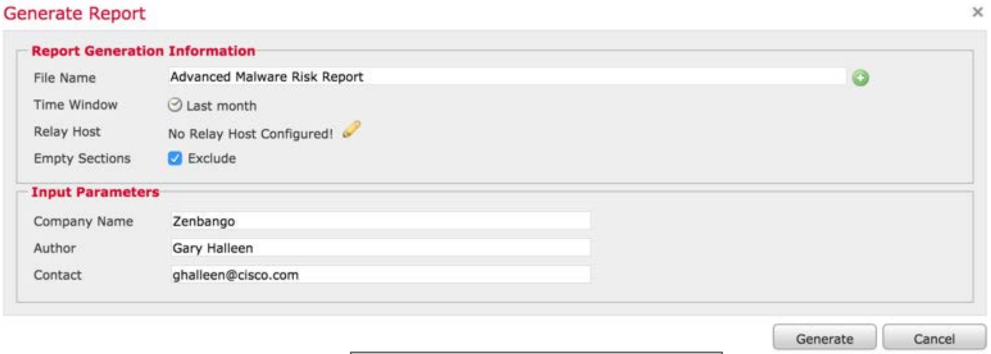
Malware Report
2016-06-29 17:53:44 Last Modified By admin

User Report: $<User>
2016-06-29 17:53:44 Last Modified By admin

Risk Reports, continued…

Click on the “Generate” icon:

Complete the Input Parameters, and select the time period.



Generate Report

Report Generation Information

File Name: Advanced Malware Risk Report

Time Window: Last month

Relay Host: No Relay Host Configured!

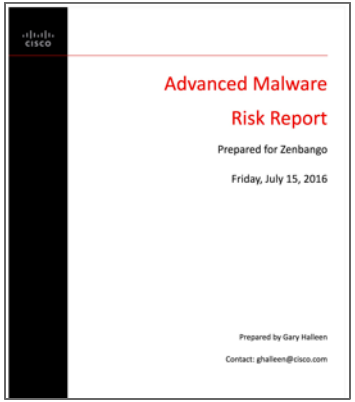
Empty Sections: ☑ Exclude

Input Parameters

Company Name: Zenbango

Author: Gary Halleen

Contact: ghalleen@cisco.com



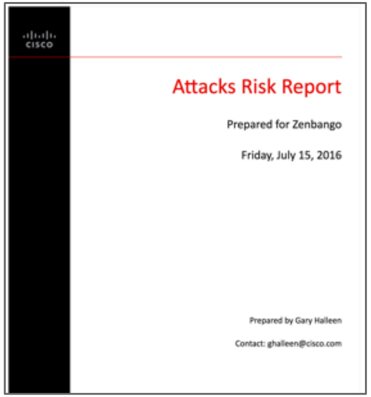
Advanced Malware Risk Report

Prepared for Zenbango

Friday, July 15, 2016

Prepared by Gary Halleen

Contact: ghalleen@cisco.com



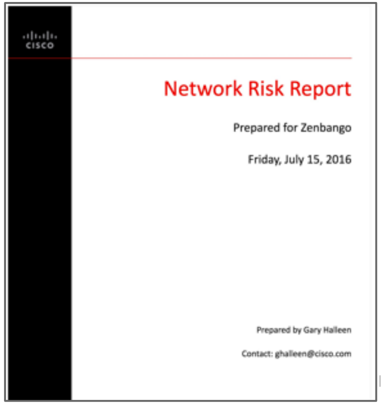
Attacks Risk Report

Prepared for Zenbango

Friday, July 15, 2016

Prepared by Gary Halleen

Contact: ghalleen@cisco.com



Network Risk Report

Prepared for Zenbango

Friday, July 15, 2016

Prepared by Gary Halleen

Contact: ghalleen@cisco.com

TOMORROW starts here.