Securing Networks with

Cisco Firepower

SNCF (300-710)

Mohsen Kheradmand

Topics

1- **Deployment**

- Implement NGFW modes
  - Routed mode
  - Transparent mode
- Implement NGIPS modes
  - Passive
  - Inline
- Implement high availability options
  - Link redundancy
  - Active/standby failover
  - Multi-instance
- Describe IRB configurations

2- **Configuration**

- Configure **system settings** in Cisco FMC
- Configure these **policies** in Cisco FMC
  - Access control
  - Intrusion
  - Malware and file
  - DNS
  - Identity
  - SSL
  - Prefilter
- Configure **features** using Cisco FMC
  - Network discovery
  - Application detectors (Open App-ID)
  - Correlation
  - Actions
- Configure **objects** using FMC
  - Object Management
  - Intrusion Rules
- Configure **devices** using FMC
  - Device Management
  - NAT
  - VPN
  - QoS
  - Platform Settings
  - Certificates

Topics

3- Management and Troubleshooting

- Troubleshoot with FMC CLI and GUI
- Configure dashboards and reporting in FMC
- Troubleshoot using packet capture procedures
- Analyze risk and standard reports

4- Integration

- Configure Cisco AMP for Networks in Firepower Management Center
- Configure Cisco AMP for Endpoints in Firepower Management Center
- Implement Threat Intelligence Director for third-party security intelligence feeds
- Describe using Cisco Threat Response for security investigations
- Describe Cisco FMC PxGrid Integration with Cisco Identify Services Engine (ISE)
- Describe Rapid Threat Containment (RTC) functionality within Firepower Management Center

Topics

- Introduction
- Basic configuration
  - FMC & FTD integration
  - Interface configuration
  - Zones
  - Routing (Static , RIPv2 , EIGRP , OSPF , BGP)
  - NAT
  - Access policies
- Advanced features
  - Geolocation filtering
  - URL filtering
  - Application Visibility and Control (AVC)
  - Intrusion Policies
  - Logging & Alerting
  - Network AMP / File Policies
- Transparent firewall
  - Initialization
  - Access policies
  - Ether type ACLs
- Redundancy
  - Multi-instance
  - High Availability

Firewalls

Stateless firewall (Packet filtering)

- Examines data packets without regard for the connection's context or state.

A stateful firewall (SPI)

- Monitors and regulates the status of network connections
- It keeps track of each connection's data, (the source and destination IP, port, and current state (open, closed, or in progress).

Next Generation Firewalls (DPI)

- NGFW has traditional firewall capabilities + new security features (IPS , application control, URL filtering, AMP and ….)
- NGFWs are designed to monitor network traffic at the application layer
- Making security decisions based on traffic content rather than IP addresses, ports, and protocols.

Unified Threat Management

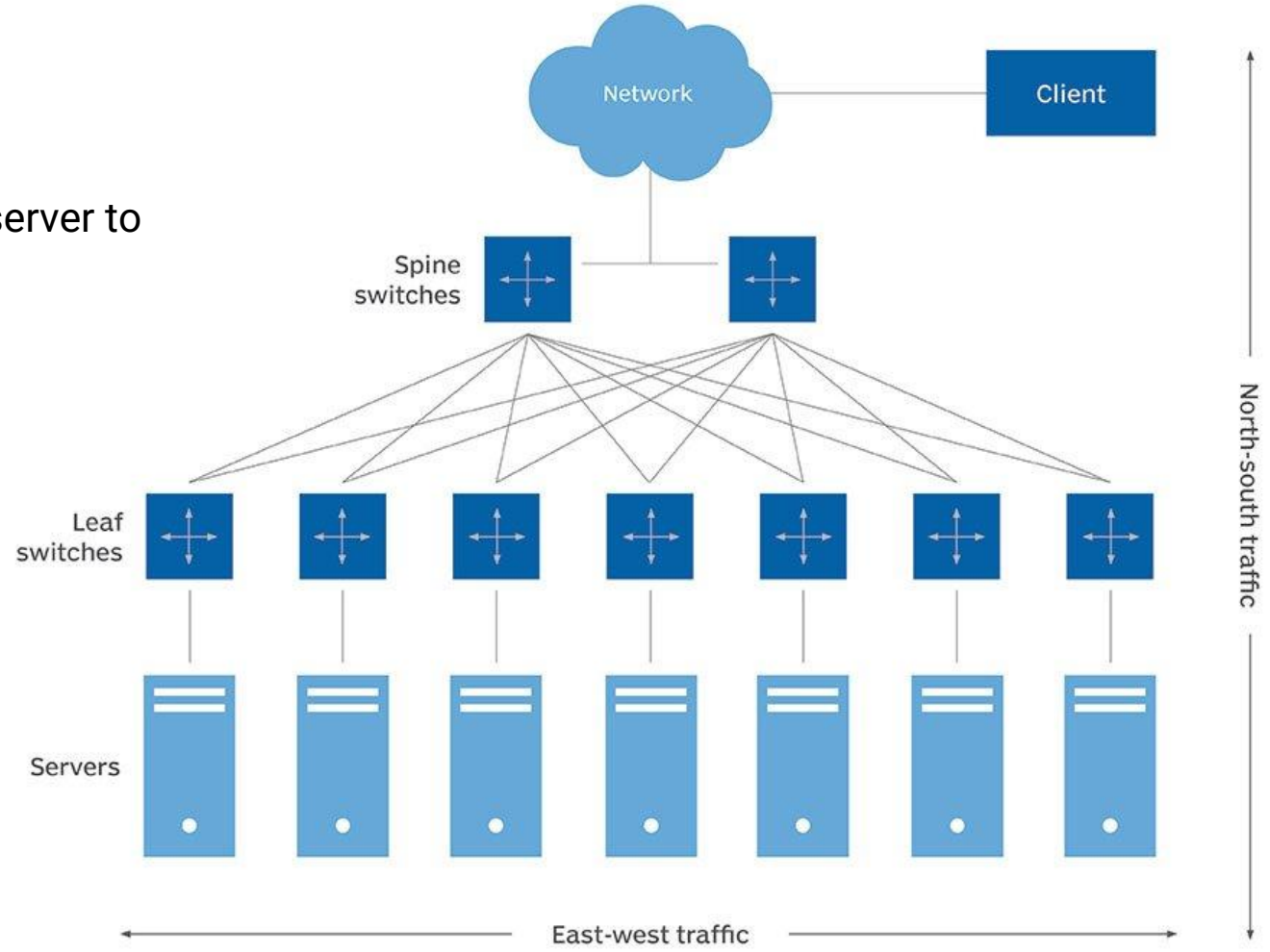
- A security system that unifies several security features such as firewall, IPS , anti-virus and anti-malware, content filtering, and VPN into a single platform

Firewalls

North-South and East-West traffic security

East-West traffic, is the transfer of data packets from server to server within a data center.

North-South traffic describes client-to-server traffic that moves between the data center and a location outside of the data center network



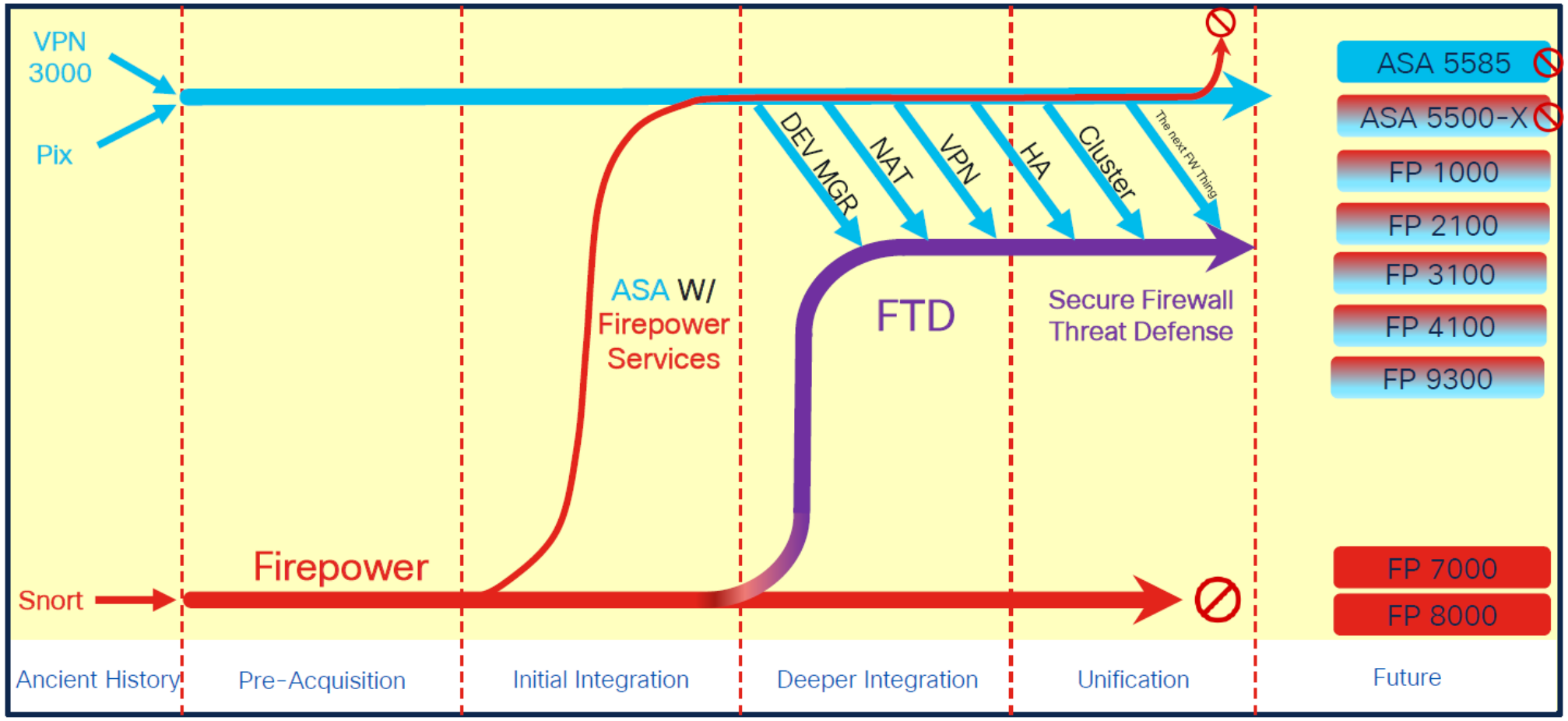
History of FTD

- The **PIX** firewall started back in 1994 (layer 4 firewall, with stateful inspection , ACL's, NAT/PAT)
- Cisco **Adaptive Security Appliance** (**ASA**) came about in 2005
- The ASA inherited the PIX OS, but moved it to a Linux based operating system(**Lina**)

- Martin Roesch in 1998 created a packet sniffer called **Snort** (an open source network-based IDS)
- In 2001 Martin founded a little company called Sourcefire.
- In 2007 Sourcefire acquired Clam Antivirus (Clam AV) creating the Sourcefire Vulnerability Research Team (**VRT**) and added malware scanning to Sourcefire appliances.

- Cisco acquired Sourcefire in 2013 for 2.7 billion and rebranded to **Firepower**
- Snort IPS replaced the ASA's IPS 4200, so (Lina & Snort) both ran in the same box for a while (ASA's with Firepower services)
- The Lina was handling the *routing*, *NAT*, *ACL's* & *VPN*, While the Snort (Sourcefire) handled *IPS* and *malware inspection*.
- It wasn't optimal. Packets had to switch back and forth between operating systems.
- So Cisco forked a new code base from the Sourcefire code and called it **Firepower Threat Defense (FTD).**

History of FTD



Snort

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection.

- Sniffer mode

  - The program will read network packets and display them on the console.

- Packet logger mode,

  - The program will log packets to the disk.

- Intrusion detection mode

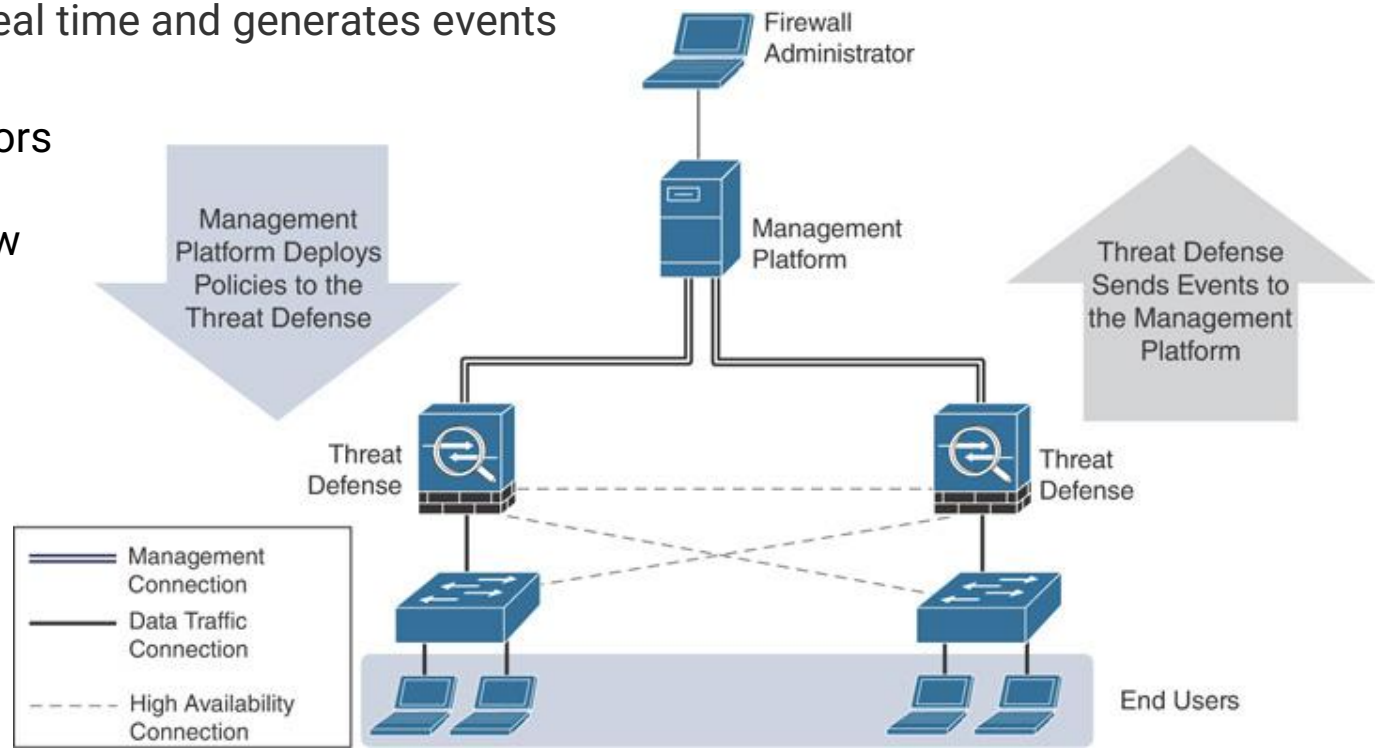
  - The program will monitor network traffic and analyze it against a rule set defined by the user.
  - The program will then perform a specific action based on what has been identified.

Cisco NGFW

The NGFW solution is composed of 2 components:

- **Manager :** to configure all the security policies and then deploy them to a **sensor**.
- **Sensor** : acts on inbound and outbound traffic in real time and generates events

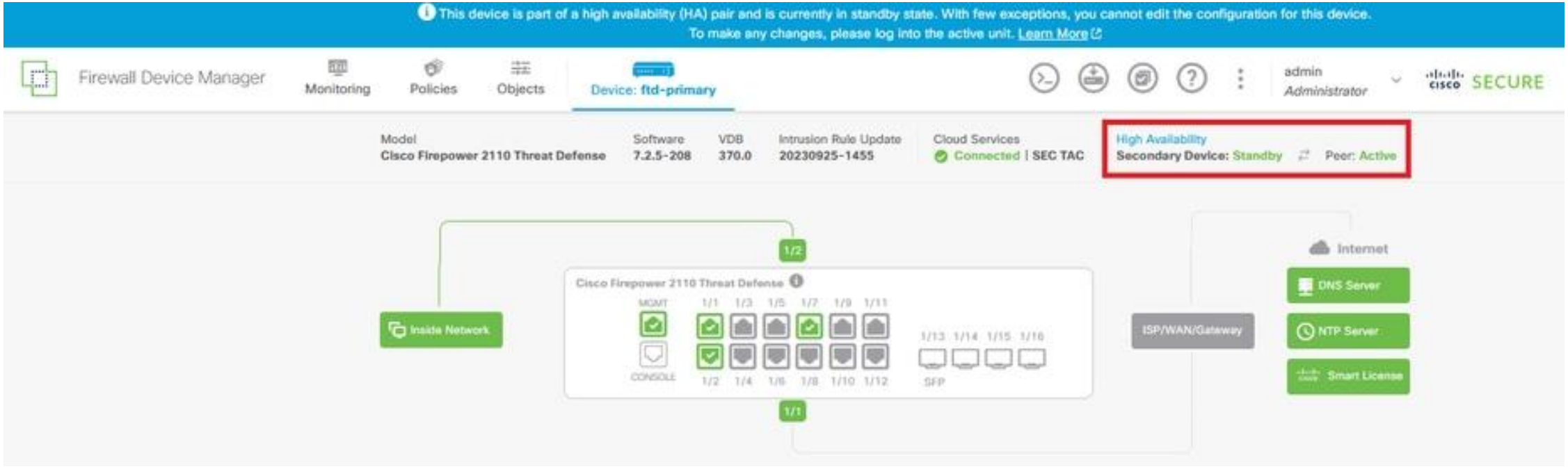
- A manager receives events from its managed sensors
- Correlates them with various contextual data
- And displays them in a (GUI) for an analyst to review



- Cisco Firepower Threat Defense (FTD) is a Sensor
- Cisco FDM , Cisco FMC , Cisco Defense Orchestrator and Adaptive Security Device Manager (ASDM) are the Managers

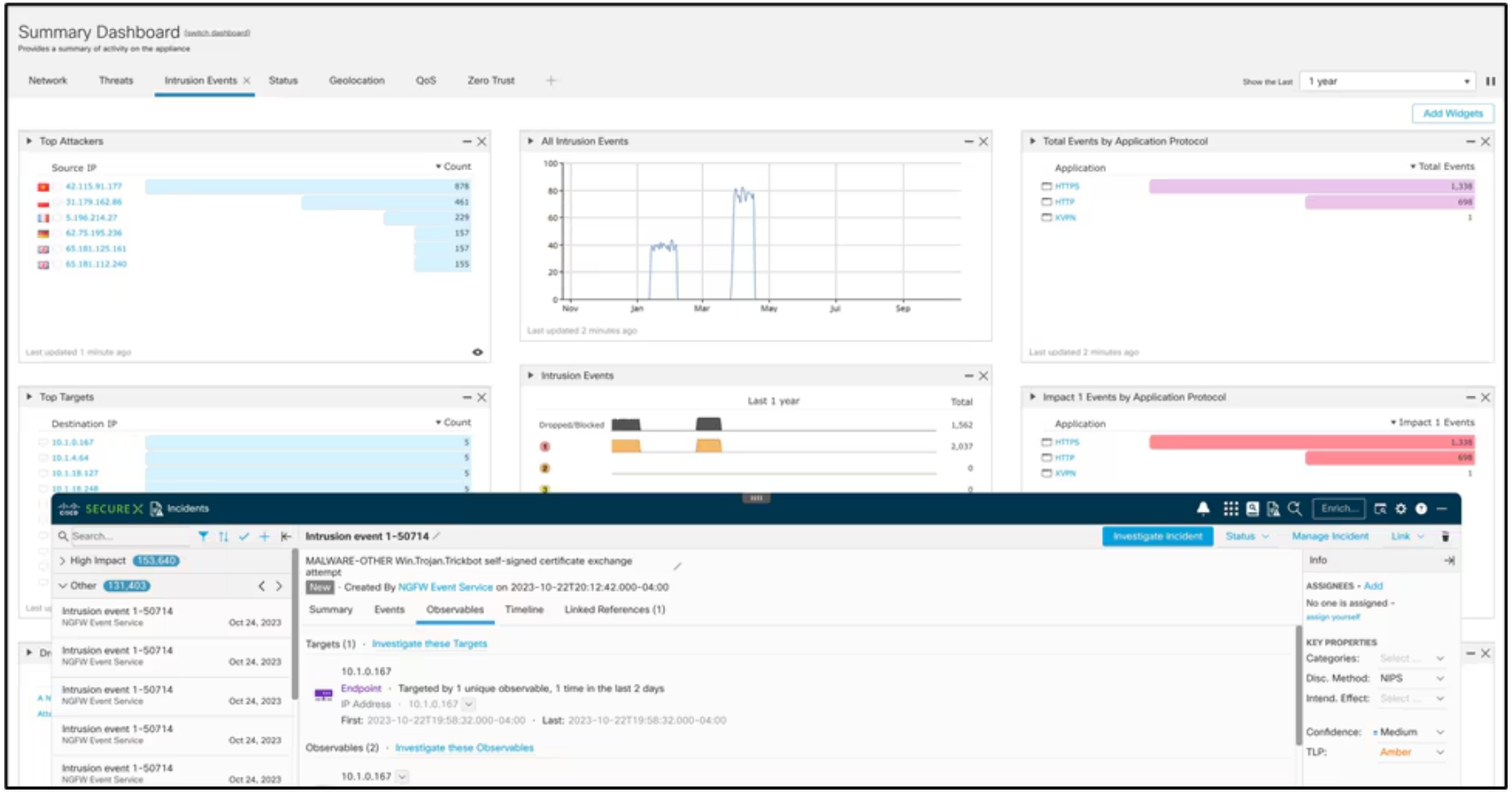
Firepower Device Manager (FDM)

This little power manager is used for SOHO environments or single-device configuration



Firepower Management Center (FMC)

Provides complete and unified management over firewalls, AVC, IPS/IDS , URL filtering, and AMP .



Firepower Management Center (FMC)

- FMC is sending the configuration and policies to the FTD devices
- If a Snort event occurs, the logging and the packets themselves will be sent to the FMC for analysis

- FMC can be deployed in both Hardware and Virtual Machine

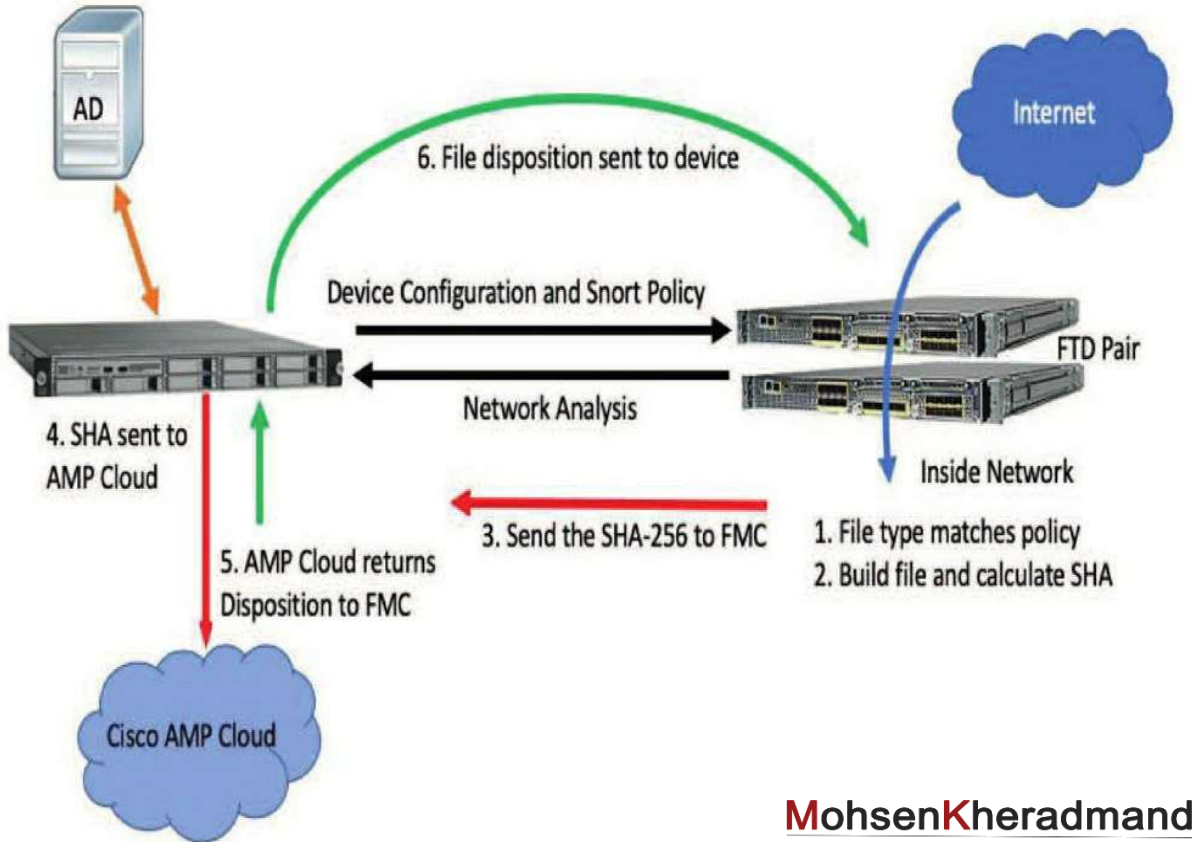
What If Your FMC Goes Down?

not much!

- You won't be getting network analysis and you won't be able to make any changes to the devices
- But the FTD will keep passing/dropping packets based on the configuration and policies it's already received from the FMC.

You lose access to :

1. File SHA-256 Hash checks
2. Any rule created using AD users and groups
   (AD integration only connects to the FMC)



Virtual FMCs

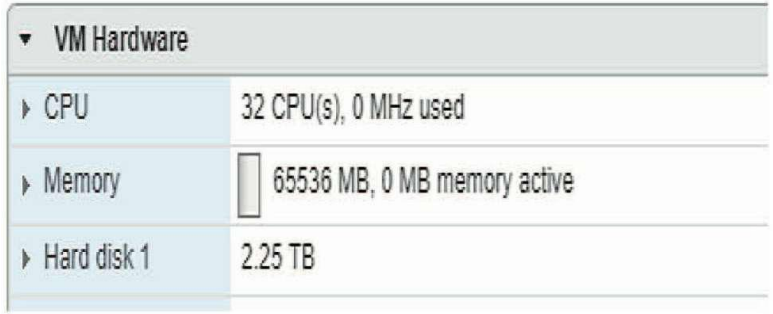
Cisco has 2 virtual FMCs on the market:

The original version

- managed up to 25 devices
- (Cheaper)
- 8 GB of RAM
- 4 cores of CPU
- 250 GB of disk space

New virtual FMC300

- managing up to 300 devices!
- (more expensive)
- 64 GB of RAM
- 32 core of CPUs
- A minimum 4.8 GB of disk space (thin provisioned).



Various hardware FMC's:

FMC1000/1600

- Up to 50 sensors managed
- 30 million maximum IPS events
- 90 million connection events
- 900 GB event storage
- 32 GB RAM
- Events per second: 12,000
- Network map up to 50K hosts, 50K users
- 1* Intel E5-2620 V4 CPU / 1* Intel Xeon 4110 processor
- 2* 900 GB SAS drives /2* 1.2 TB 10-K SAS HDDs RAID 1
- FA /GE/10GE Ethernet port

FMC2500/2600

- Up to 300 sensors managed
- 60 million maximum IPS events
- 300 million connection events
- 1.8 TB event storage
- 64 GB RAM
- Events per second: 12,000
- Network map up to 150K hosts, 150K users
- 2* Intel E5-2620 V4 / 2* Intel Xeon 4110 processors
- 4*600 GB SAS drives /4* 600 GB 10K SAS HDDs RAID 5
- FA /GE/10GE Ethernet port

Various hardware FMC's:

FMC4500/4600

- Up to 750 sensors managed
- 300 million maximum IPS events
- 1 billion connection events
- 3.2 TB event storage
- 128 GB RAM
- Events per second: 20,000
- Network map up to 600K hosts, 600K users
- 2* Intel E5-2640 V4 CPUs / 2* Intel Xeon 4116 processors
- 6* 800 GB SSDs /10* 1.2 TB SAS SSDs RAID 6
- FA /GE/10GE Ethernet port

FMC2500/2600

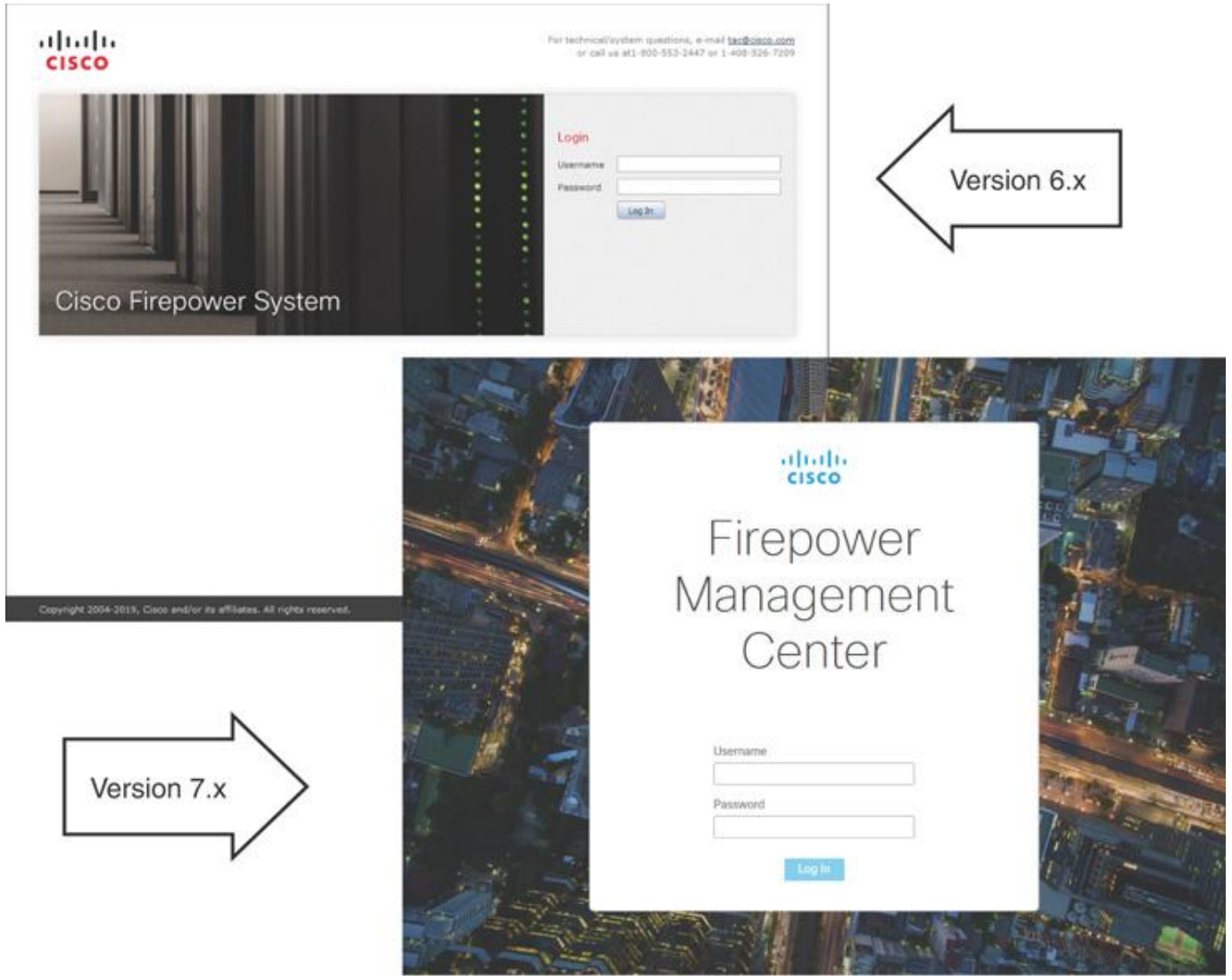
- Up to 300 sensors managed
- 60 million maximum IPS events
- 300 million connection events
- 1.8 TB event storage
- 64 GB RAM
- Events per second: 12,000
- Network map up to 150K hosts, 150K users
- 2* Intel E5-2620 V4 / 2* Intel Xeon 4110 processors
- 4*600 GB SAS drives /4* 600 GB 10K SAS HDDs RAID 5
- FA /GE/10GE Ethernet port

Product Evolution and Lifecycle

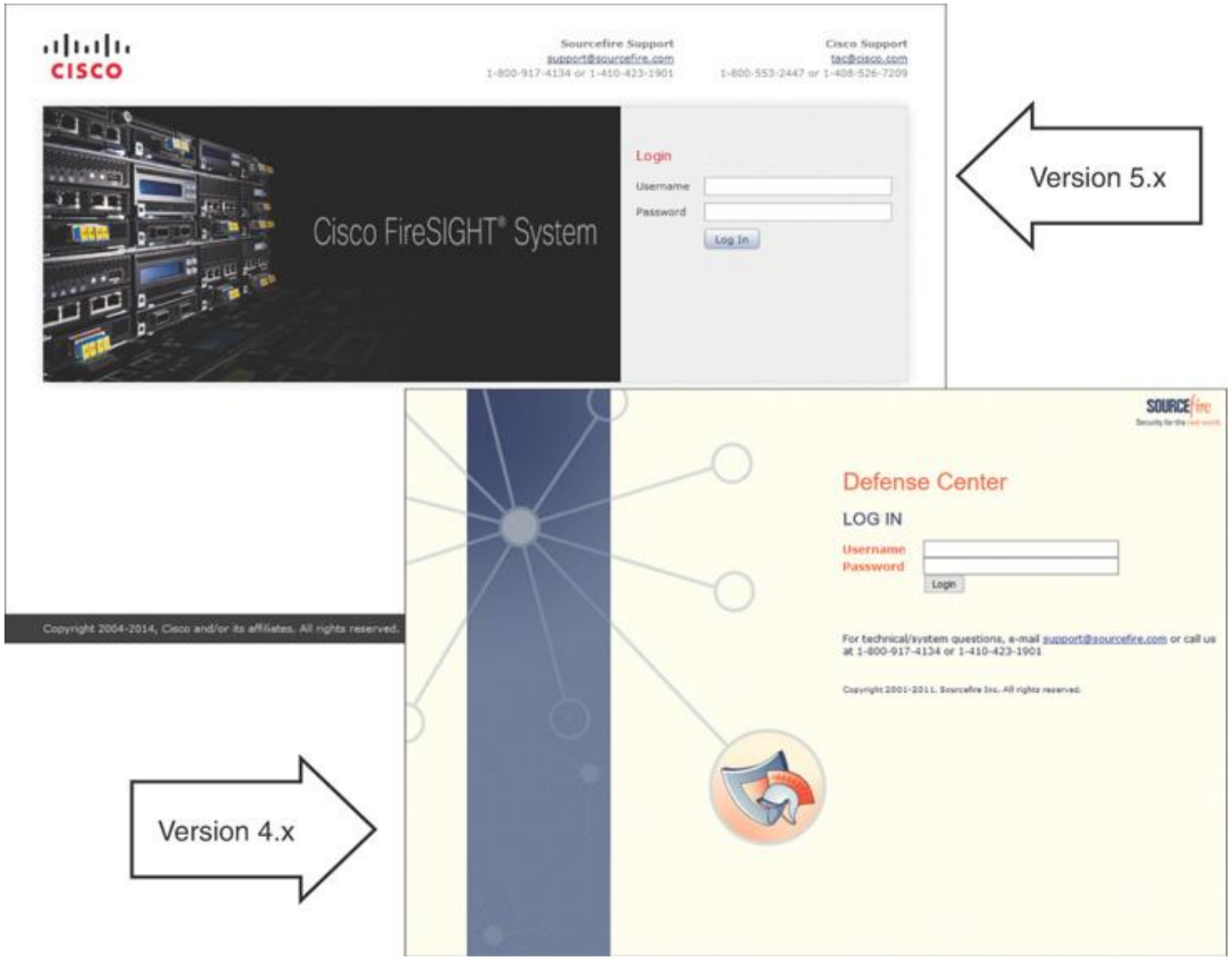
Version	Solution Name	Management Platform Name
Version 4.x	3D System	Defense Center
Version 5.x	FireSIGHT System	FireSIGHT Management Center
Version 6.x	Firepower System	Firepower Management Center
Version 7.x	Cisco Secure Firewall	Cisco Secure Firewall Management Center

- Version 4.x was primarily intended for **intrusion prevention system (IPS)** functionality
- Version 5.x was developed with the **next-generation firewall (NGFW)** features
- Version 6.x cisco renames and combined Lina and Snort to Firepower System
- In 2020, Cisco unified all the security product names with the Cisco Secure brand (Version 7.x)

Product Evolution and Lifecycle



Product Evolution and Lifecycle



SRT , LTR and XLTR

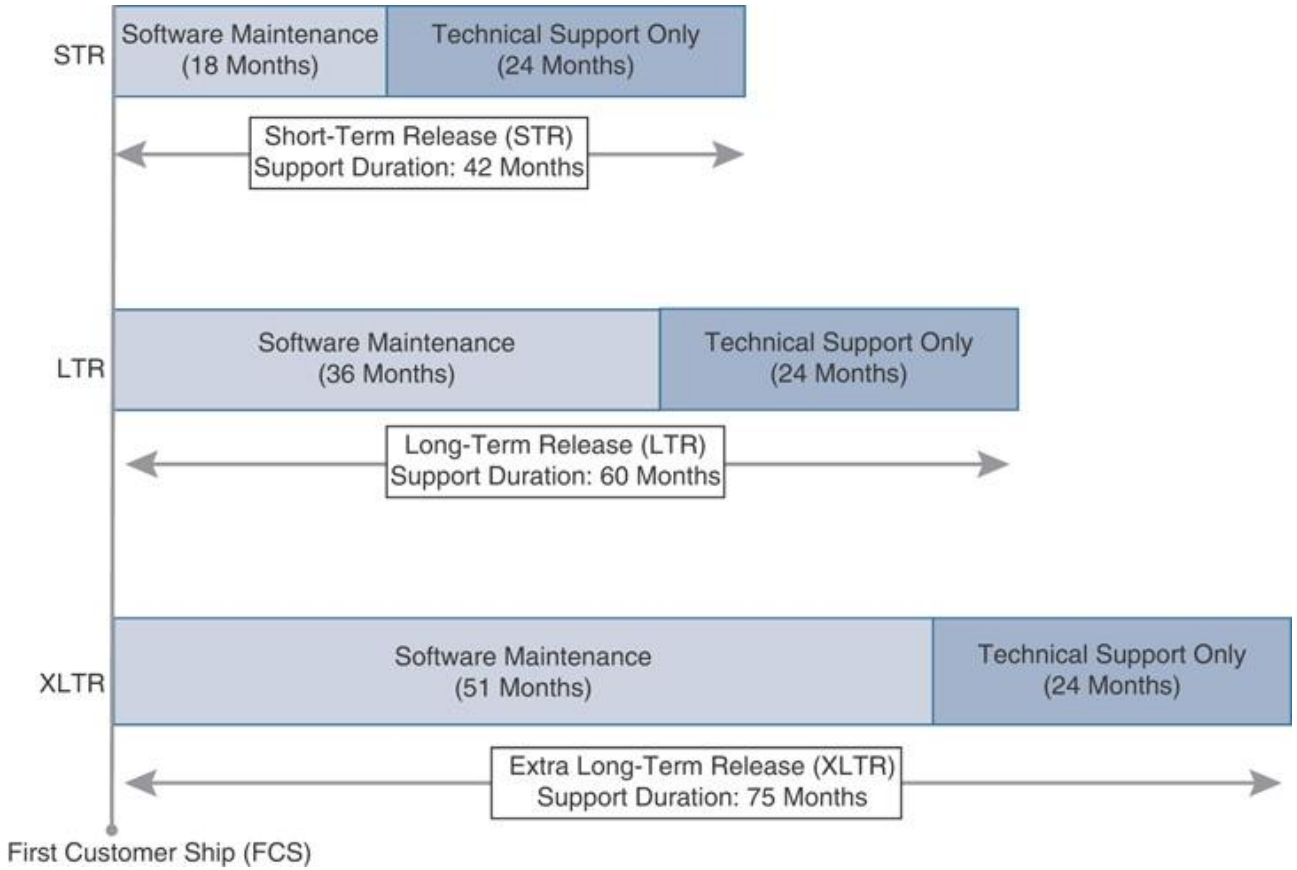
Cisco releases two software versions for Secure Firewall:

The Short-Term Release (STR)
Has a shorter lifecycle, but includes the latest feature set

The Long-Term Release (LTR)
provides a longer lifecycle (the latest features and longer support duration)

Extra Long-Term Release (XLTR) :
Every two years, Cisco releases an extended version of LTR (chosen for government certification)

✓ Cisco Secure Firewall Version 7.0, is an XLTR



Login to FMC

- The primary management port for all of the hardware FMCs is **eth0**
- You can use eth1, eth2, and eth3 as secondary management or event ports

There are 3 options to access the console:

(1) Connect a USB keyboard and VGA monitor.

(2) Connect to the serial console port.

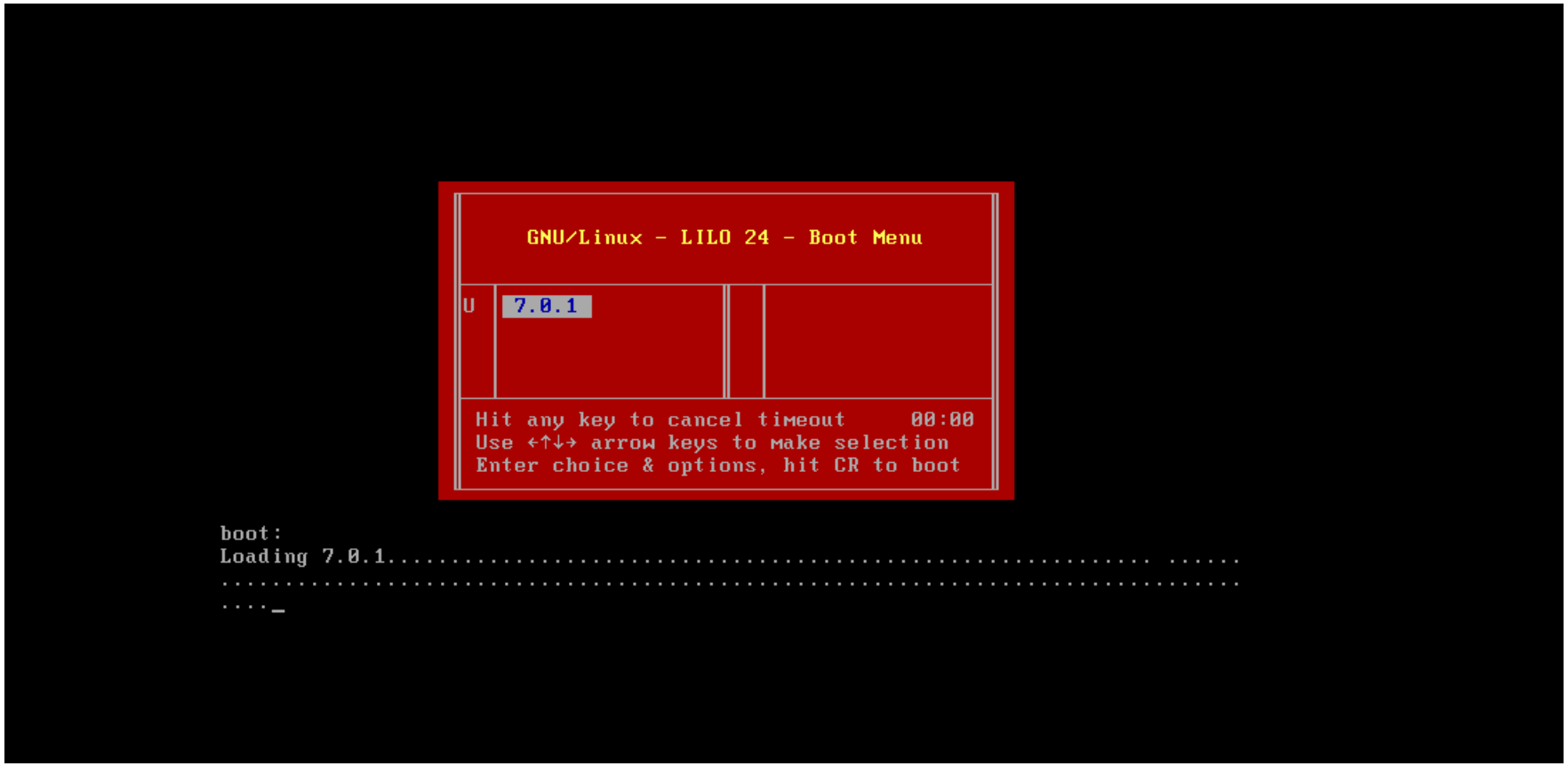
(3) Connect via SSH to the default IP address of 192.168.45.45.

✓ For virtual FMCs , access the console through vCenter or other virtual application

➢ Log in with the default credentials:

Username: admin
Password: Admin123

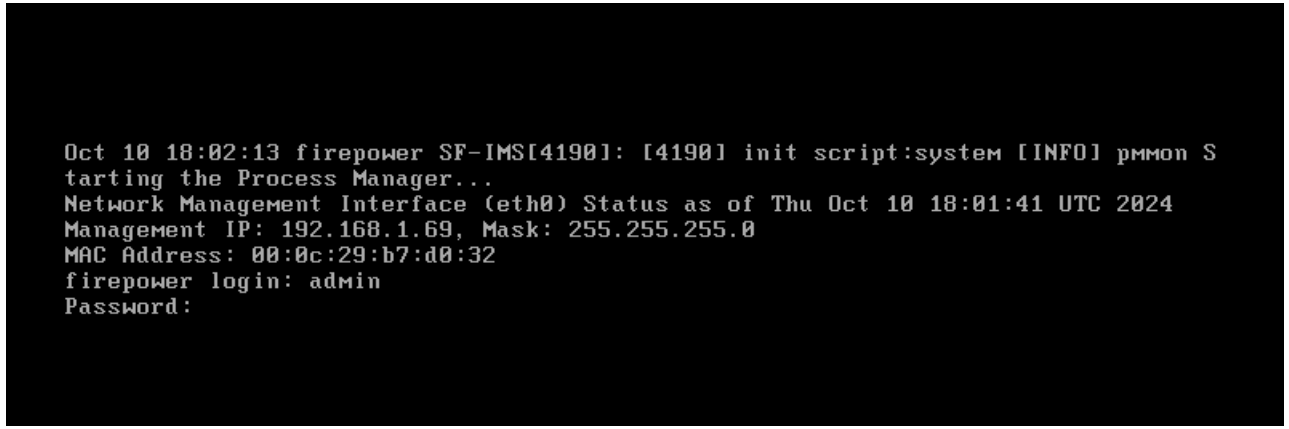
Login to FMC


GNU/Linux - LILO 24 - Boot Menu
U
7.0.1
Hit any key to cancel timeout 00:00
Use ←↑↓→ arrow keys to make selection
Enter choice & options, hit CR to boot
boot:
Loading 7.0.1.....

Login to FMC

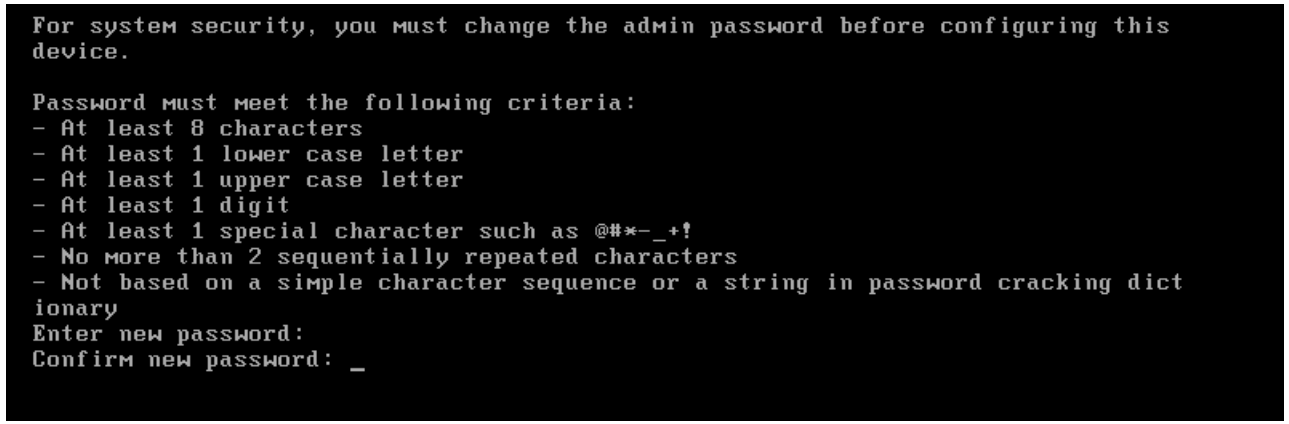
After the FMC boots up:

Enter default username and password



FMC will ask you to change password

Enter your new password



Login to FMC

Then enter TCP/IP setting

- Hostname:
- IPv4/v6 : (DHCP/manual)
- Subnet mask:
- Gateway:
- DNS:
- NTP:

to change FMC IP configuration :

- Expert
- Sudo SU
- (enter password)

```
Enter a hostname or fully qualified domain name for this system [firepower]: Con
figure IPv4 via DHCP or manually? (dhcp/manual) [dhcp]: Enter a comma-separated
list of DNS servers or 'none' [208.67.222.222,208.67.220.220]: Enter a comma-sep
arated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
]:
Hostname:             firepower
IPv4 configured via:  dhcp
DNS servers:          208.67.222.222,208.67.220.220
NTP servers:          0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org

Are these settings correct? (y/n) Are these settings correct? (y/n) n
Enter a hostname or fully qualified domain name for this system [firepower]: FMC
Configure IPv4 via DHCP or manually? (dhcp/manual) [dhcp]: manual
Enter an IPv4 address for the management interface [192.168.1.69]:
```

```
Hostname:                           FMC
IPv4 configured via:                manual configuration
Management interface IPv4 address:  192.168.1.250
Management interface IPv4 netmask:  255.255.255.0
Management interface IPv4 gateway:  192.168.1.1
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool
.ntp.org

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

```
admin@FMC:~$ sudo su
root@FMC:/Volume/home/admin# /usr/local/sf/bin/configure-network


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

Management IP address? [172.16.1.100] 192.168.10.200
Management netmask? [255.255.255.0] 255.255.255.0
Management default gateway? [172.16.1.1] 192
Management default gateway? [172.16.1.1] 192.168.10.1

Management IP address?          192.168.10.200
Management netmask?             255.255.255.0
Management default gateway?     192.168.10.1

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

MohsenKheradmand MK

Login to FMC

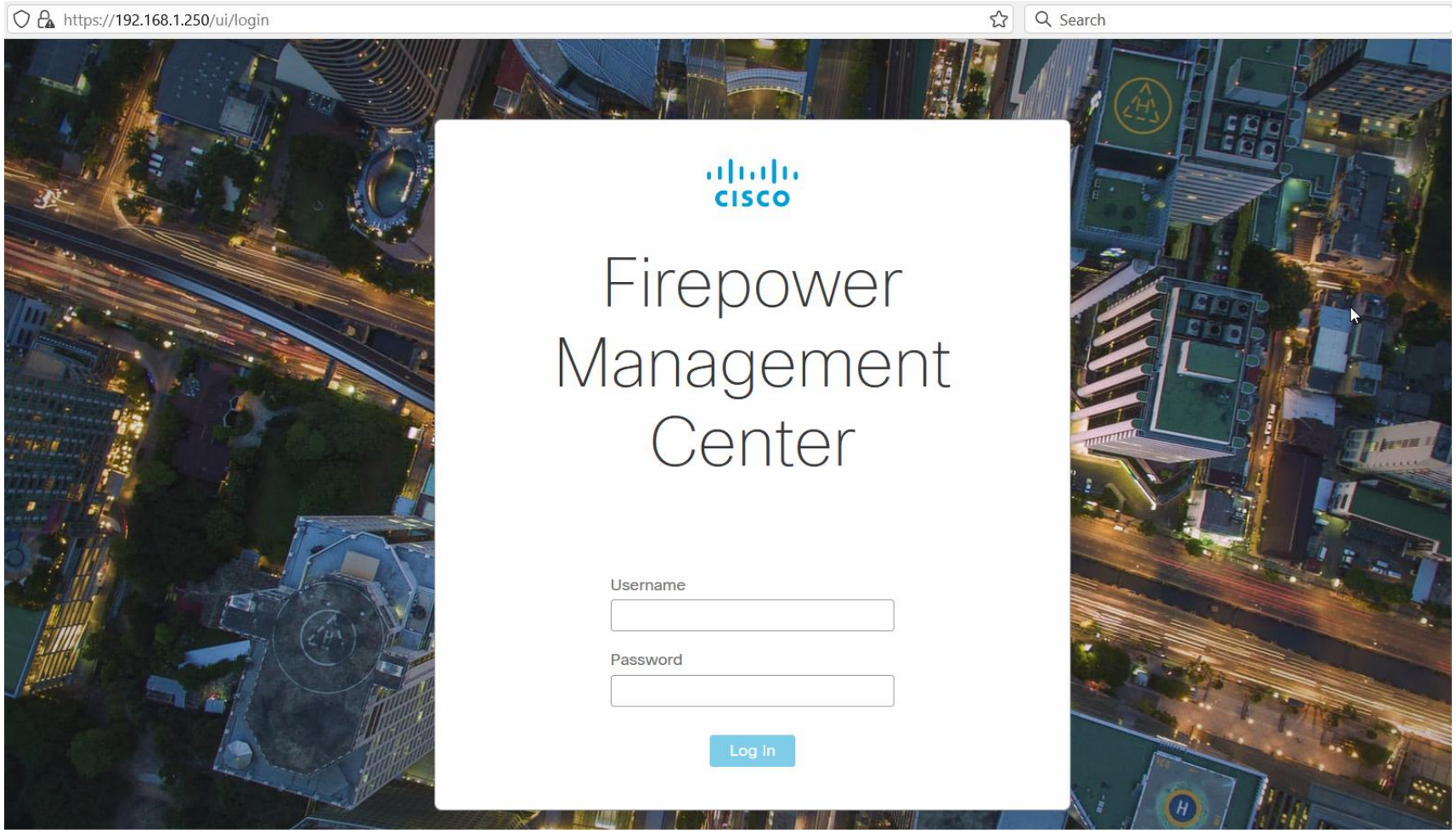
Open a web browser

Enter FMC IP address

example: HTTPS://192.168.1.250

Or : I.e. [*HTTPS://FMC.Local*](HTTPS://FMC.Local)

Enter username /password



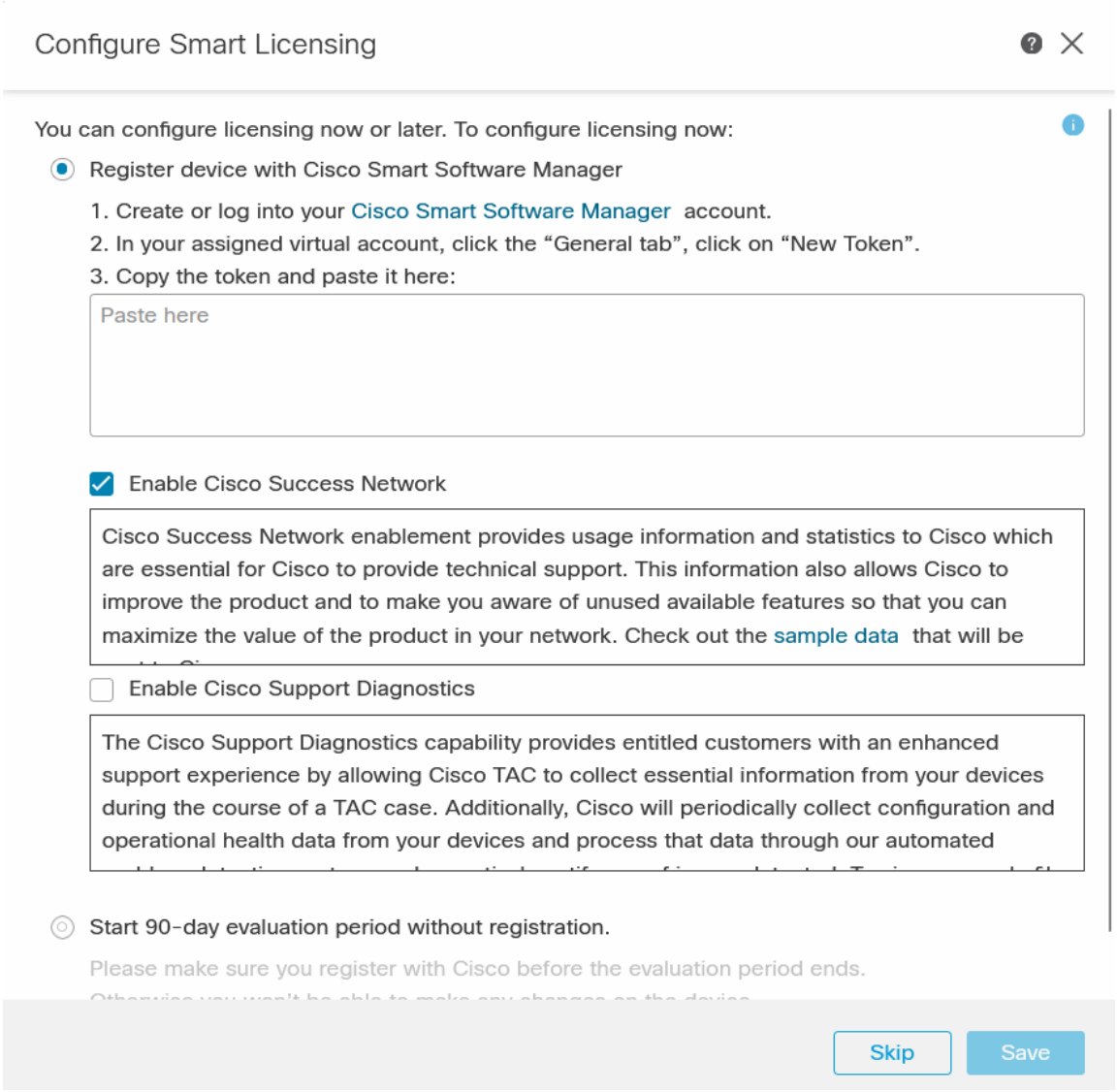
Login to FMC

Smart licensing will shows up

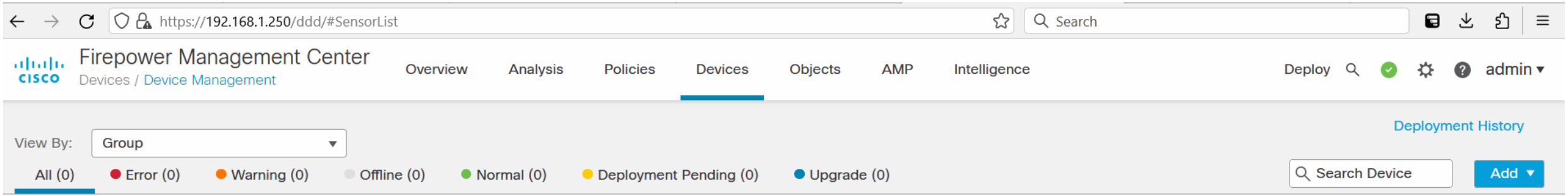
Choose trial 90-day

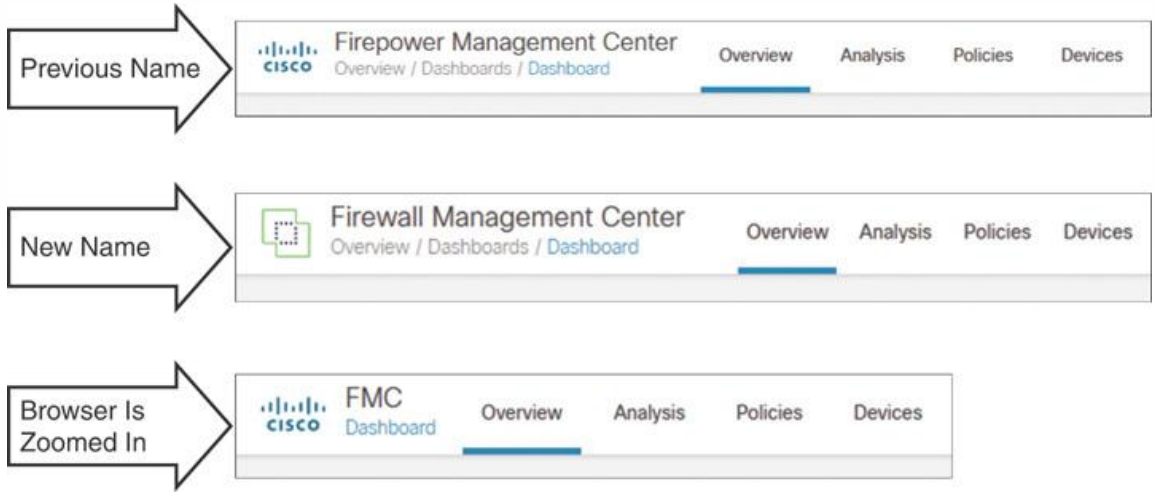
or enter the token you have got from Cisco

Trial supports everything, but can only use DES encryption for VPNs due to export laws.



Login to FMC

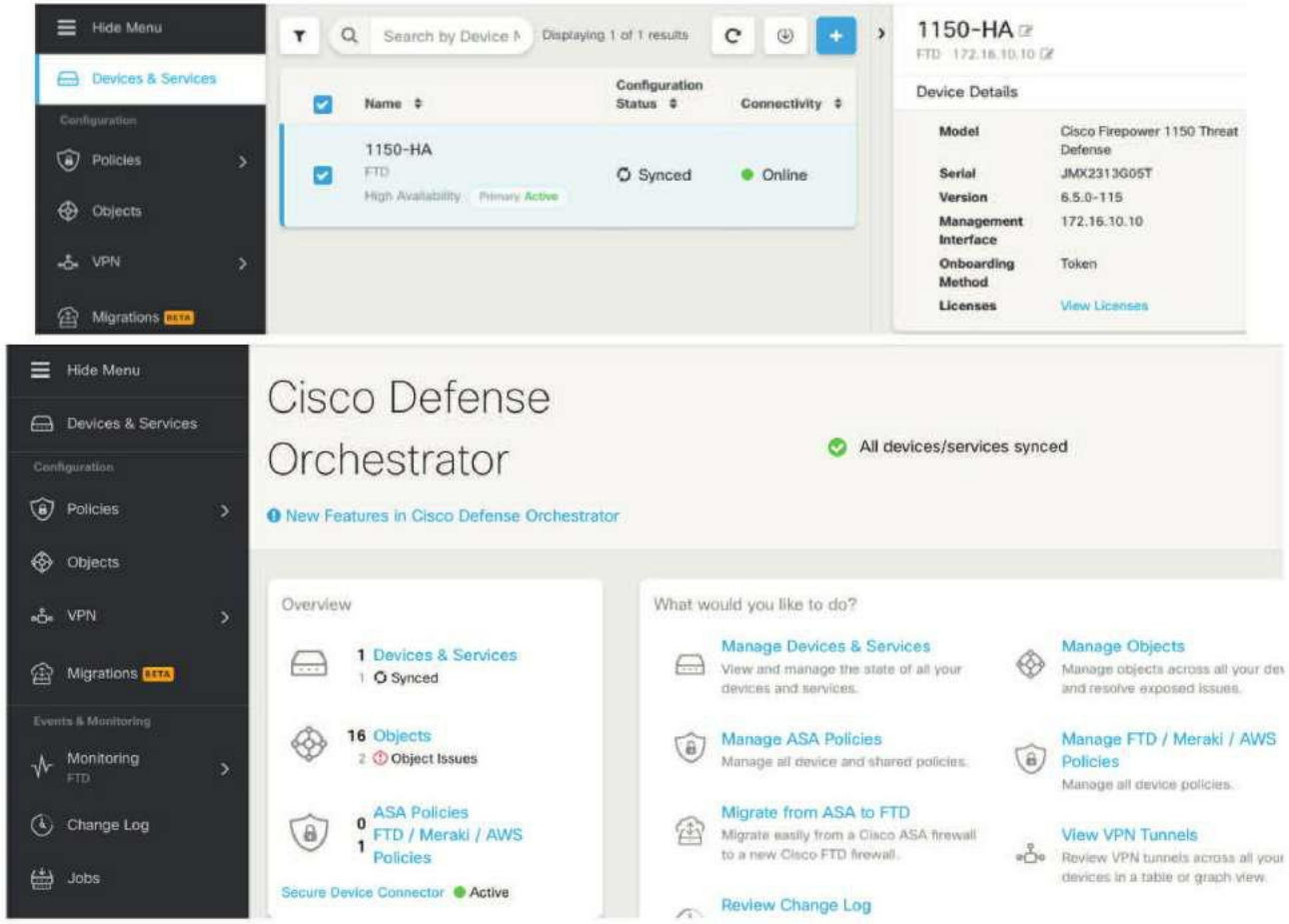




MohsenKheradmand MK

Cisco Defense Orchestrator (CDO)

- Cloud-based management system
- The future of managing Cisco security products like the ISE, Firepower, StealthWatch, AMP ASAs, and more:



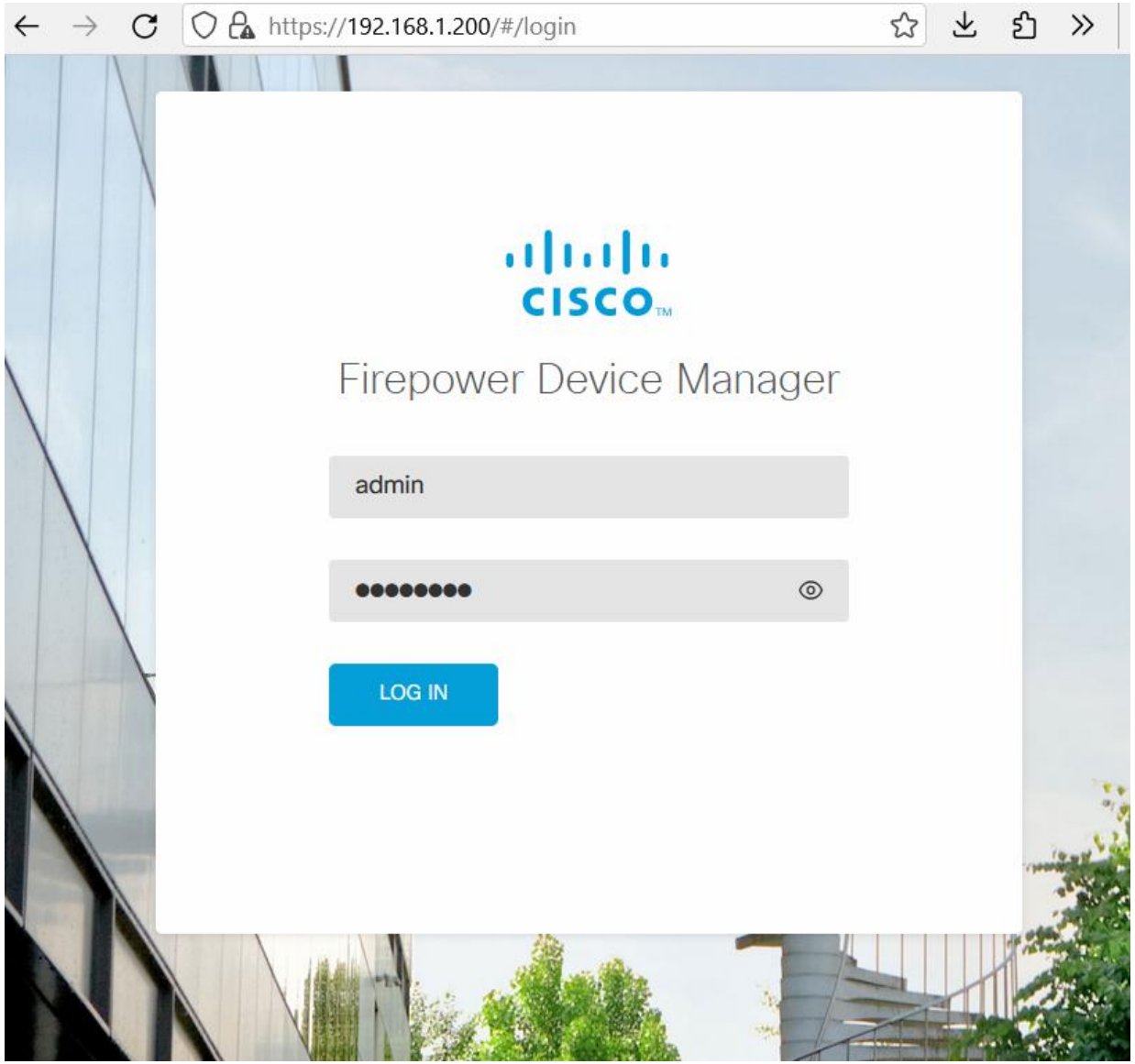
MohsenKheradmand MK

Adaptive Security Device Manager (ASDM)

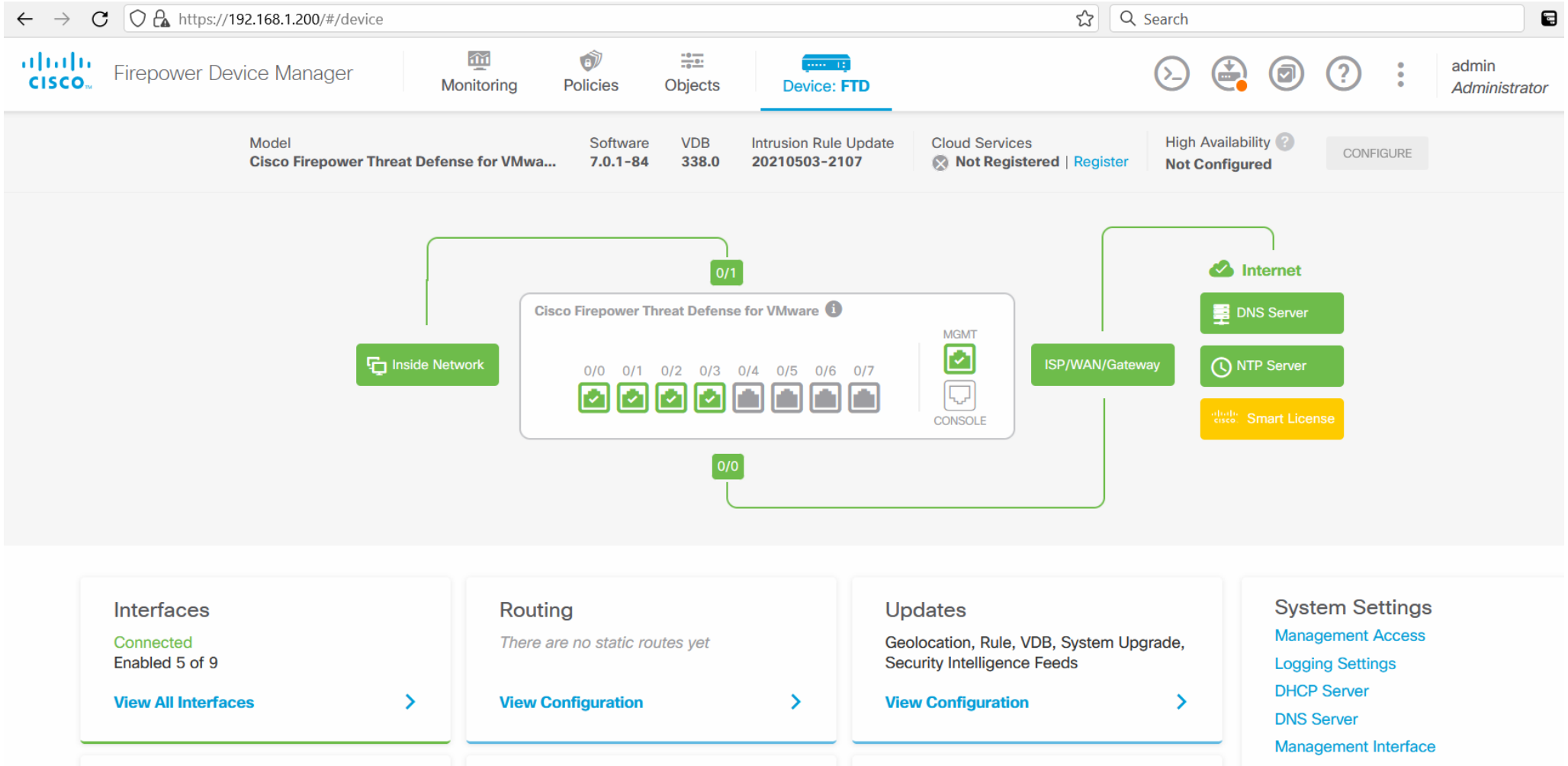
- Configure, manage, and troubleshoot small to large ASA deployments for more than a decade

Login to FDM

- After connecting to FTD
- Or after vFTD installation
- You must set TCP/IP setting in FTD CLI
- Then enter FTD IP address in browser
- And enter username/password



Login to FDM



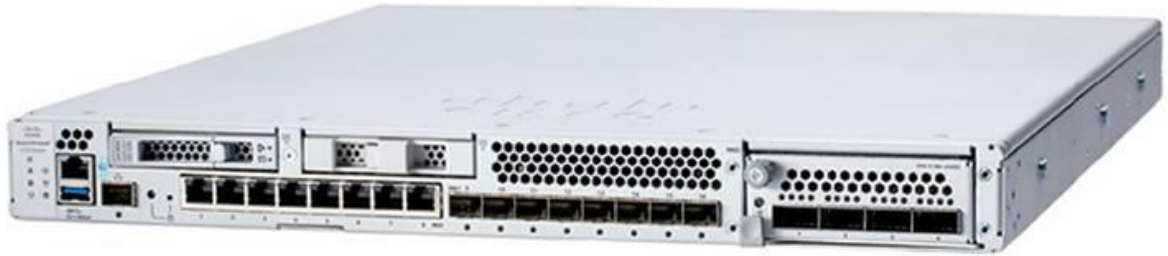
Cisco FTD devices

Cisco Firepower 1000 Series

Firepower 9300 Security Appliance

Firepower 2100 Series

Cisco Firepower 4100 Series

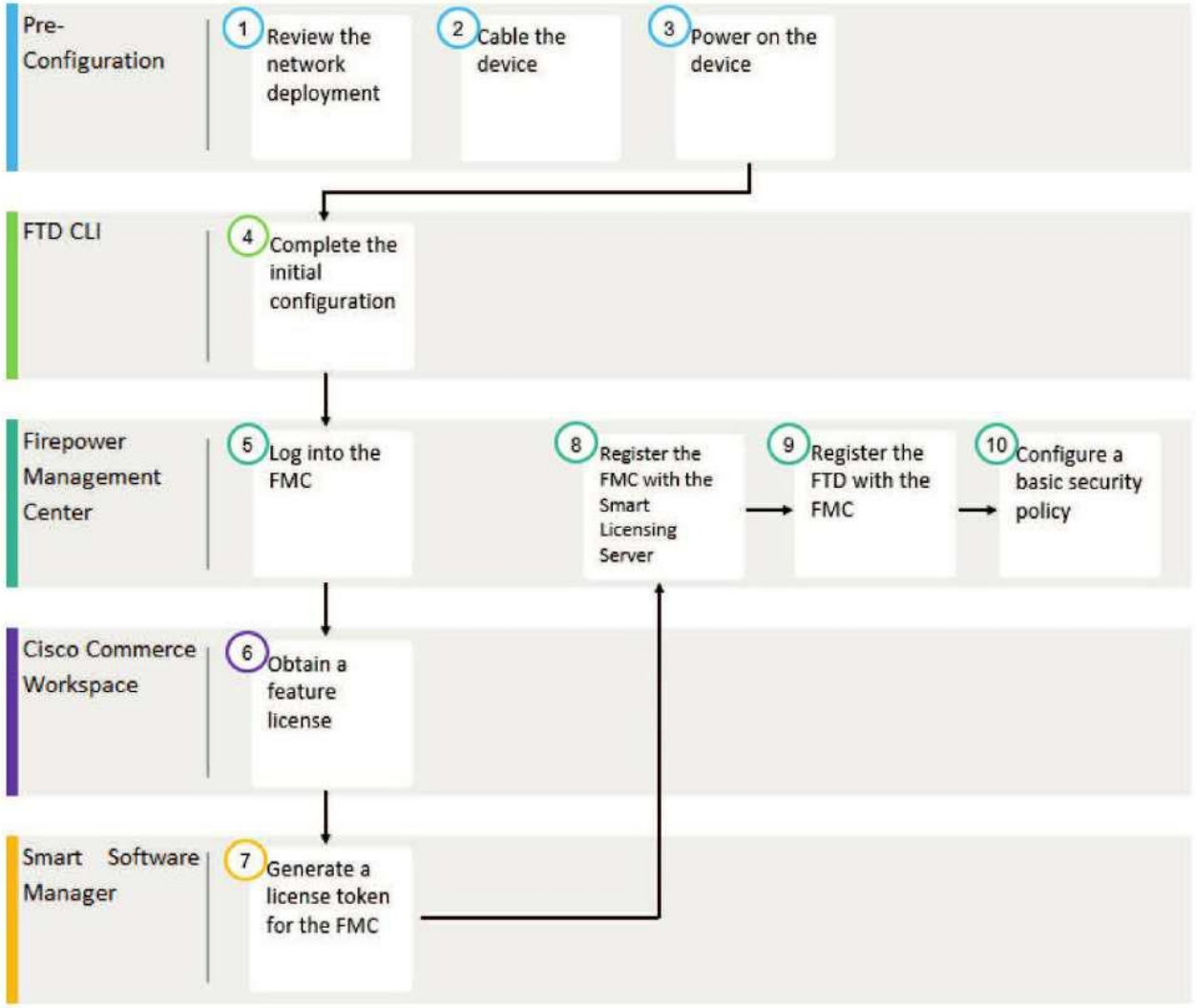


Cisco Secure Firewall 3100 Series

Cisco ASA 5500-X with FirePOWER Services

Cisco ASA 5500-X Series Firewalls

Deploying a Cisco Firepower Network



Deploying a Cisco Firepower Network