



Fire Jumper Academy

FTD for FE's

Ed Finger
edfinge@cisco.com





Consistent, predictable and measurable enablement methodology for internal and partner Cybersecurity Sales Reps, SEs, and FEs.





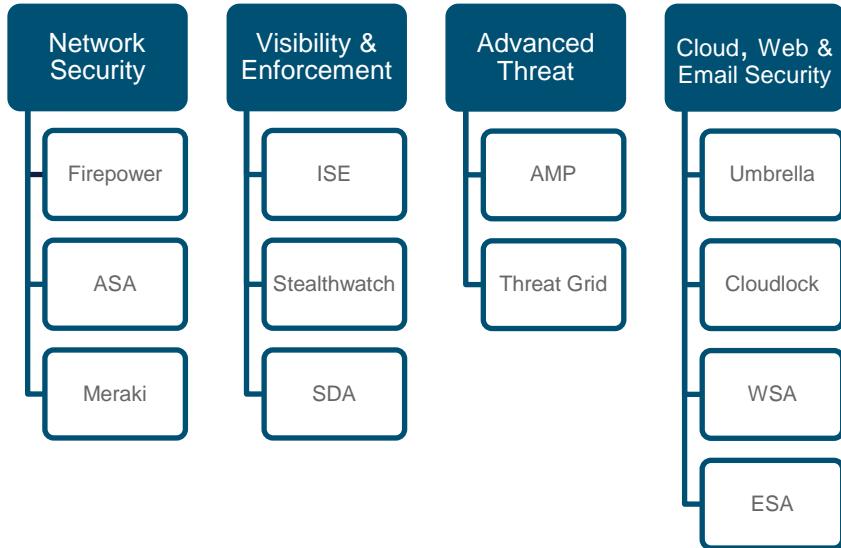
	Network Security	Visibility & Enforcement	Advanced Threat	Cloud, Web & Email Security
Stage 1: Recruit	Registration			
Stage 2: Recruit	Product Fundamentals (Tech Talks) – COLT Exam Per Competency			
Stage 3: Recruit	Deep Dive, Live Class w/ Lab – Challenge Exercise			
Stage 4: Specialist	CCNP Security Course – CCNP Exam			
Continuing Education	SEVT, PVT, TechTalk, Workshops, NPI, etc. – Aligned to Stages			



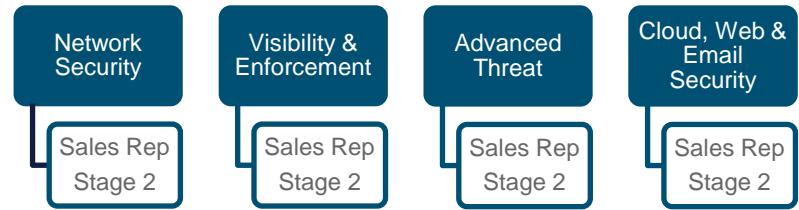
Individual Development Plans

Role-based mapping of competency areas & stages

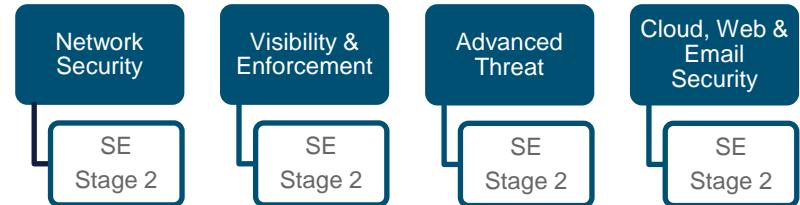
- Competency Areas



- Account Manager (Generalist)



- Systems Engineer (Generalist)





Stage 3 Field Engineer Roadshow Format

- Two Day ILT
- Product Focused, Competency Area Aligned
 - Firewall Threat Defense
 - AMP For Endpoints
 - Stealthwatch
 - ESA & WSA
 - Identity Service Engine
- Installation & Configuration
- Challenge Exercise



Resources

- Fire Jumper Academy for FEs
 - <https://communities.cisco.com/docs/DOC-64625>
 - <https://community.cisco.com/t5/security-documents/fire-jumper-academy-for-field-engineers/ta-p/3630112>
- dCloud Labs
 - <https://dCloud.cisco.com>



Black Belt Partner Academy Security *Powered By Fire Jumper* – Alignment for Deployment

Field Engineer- Deployment			Black Belt Partner Academy Security <i>Powered by Fire Jumper</i>		
Fire Jumper Academy			Stage	Content	Assessment
Stage	Content	Assessment	Stage	Content	Assessment
1	Registration	Form	1	Learning Map	Quiz
2	Learning Map	Quiz	2	Learning Map	Quiz ----- Deal Id or Cisco SO#*
3	Advanced Training	Challenge Lab	3	Advanced Training Learning Map	Quiz Challenge Lab Certificate
4	Cisco Certification	Certificate		Programmability Mission Stages 1-3 Learning Maps	Programmability Mission Stages 1-3 Quizzes* Cisco SO#*

***REQUIRED for Black Belt ONLY**

- *The same Cisco SO# submitted in Stage 2 can be used for Stage 3 certification as well. The participants will not be required to provide a different Cisco SO#. The Cisco SO# is not required to achieve Fire Jumper status.



Agenda Day 1



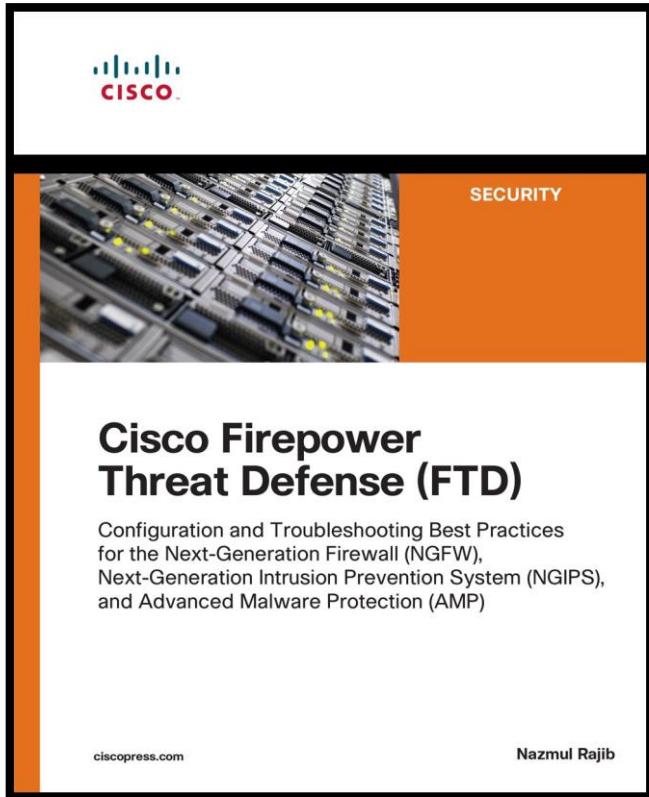
- Solutions Portfolio
- Operational Modes
- Architecture
- Basic Configuration
- Network Discovery Policy
- FlexConfig
- NAT and Routing
- Prefilter Packet Processing
- File and Malware Policy
- NAP and Intrusion Policy

Agenda Day 2

- High Availability and Resiliency
- Application Programming Interface (API)
- Virtual Private Networks RAVPN and Site-to-Site
- Operation Monitoring and Troubleshooting
- TLS/SSL Decryption
- Cisco Threat Intelligence Director (CTID)
- Upgrade FMC, FTD and FXOS
- ISE Integration
- Firewall Migrations

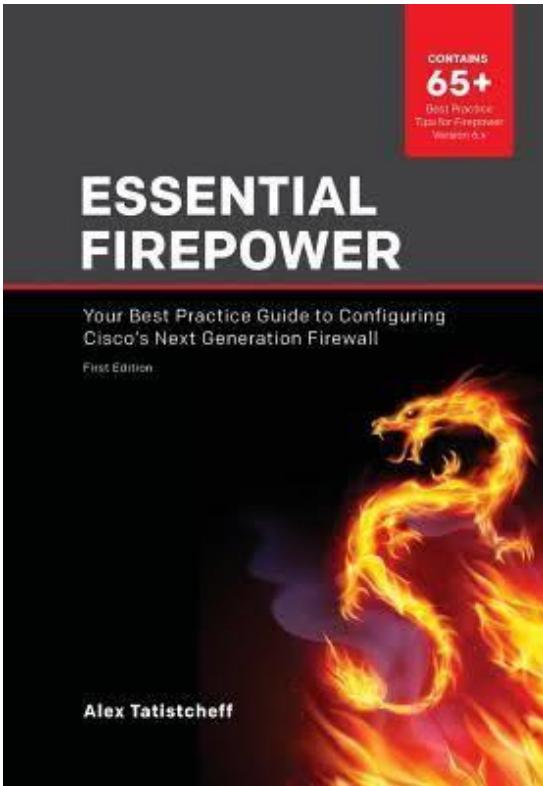


Training Resource for this Class



amazon.com/dp/1587144808
ciscopress.com/title/9781587144806

Training Resource for this Class



[Available at Amazon](#)

Firewall Solutions Portfolio



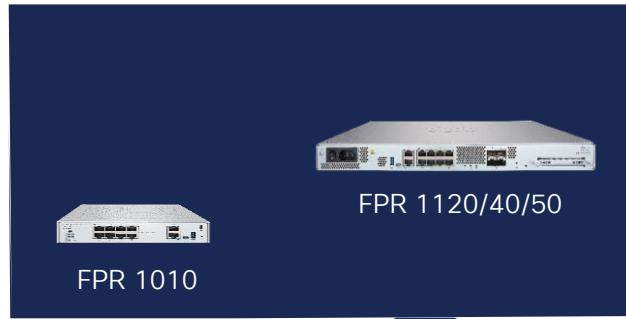
Brand Naming Changes in 7.0

Firepower Management Center (FMC)	→	Cisco Secure Firewall Management Center (FMC)
Firepower Threat Defense (FTD)	→	Cisco Secure Firewall Threat Defense (FTD)
Adaptive Security Appliance (ASA)	→	Cisco Secure Firewall ASA
Firepower Hardware Appliance	→	Cisco Secure Firewall 2100 Series
Firepower Threat Defense Virtual / NGFWv	→	Cisco Secure Firewall Threat Defense Virtual (FTDv)



Cisco Secure Firewall Hardware Portfolio

Next Generation Hardware available in any size



FPR 1120/40/50

FPR 1010



FPR 4115/25/45

FPR 4110/20/40/50



FPR 9300 Series
SM-24 SM-40
SM-36 SM-48
SM-44 SM-56



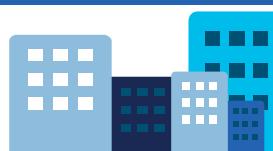
650 Mbps AVC or AVC+IPS



1.5-3 Gbps AVC or
AVC+IPS



2-8.5 Gbps AVC or AVC IPS



Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS 6

Six node cluster:
Up to 254 Gbps AVC
Up to 226 Gbps AVC+IPS



One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS

Six node (2 chassis) cluster:
Up to 336 Gbps AVC
Up to 307 Gbps AVC+IPS



Branch
Office

Mid-Size
Enterprise

Large
Enterprise

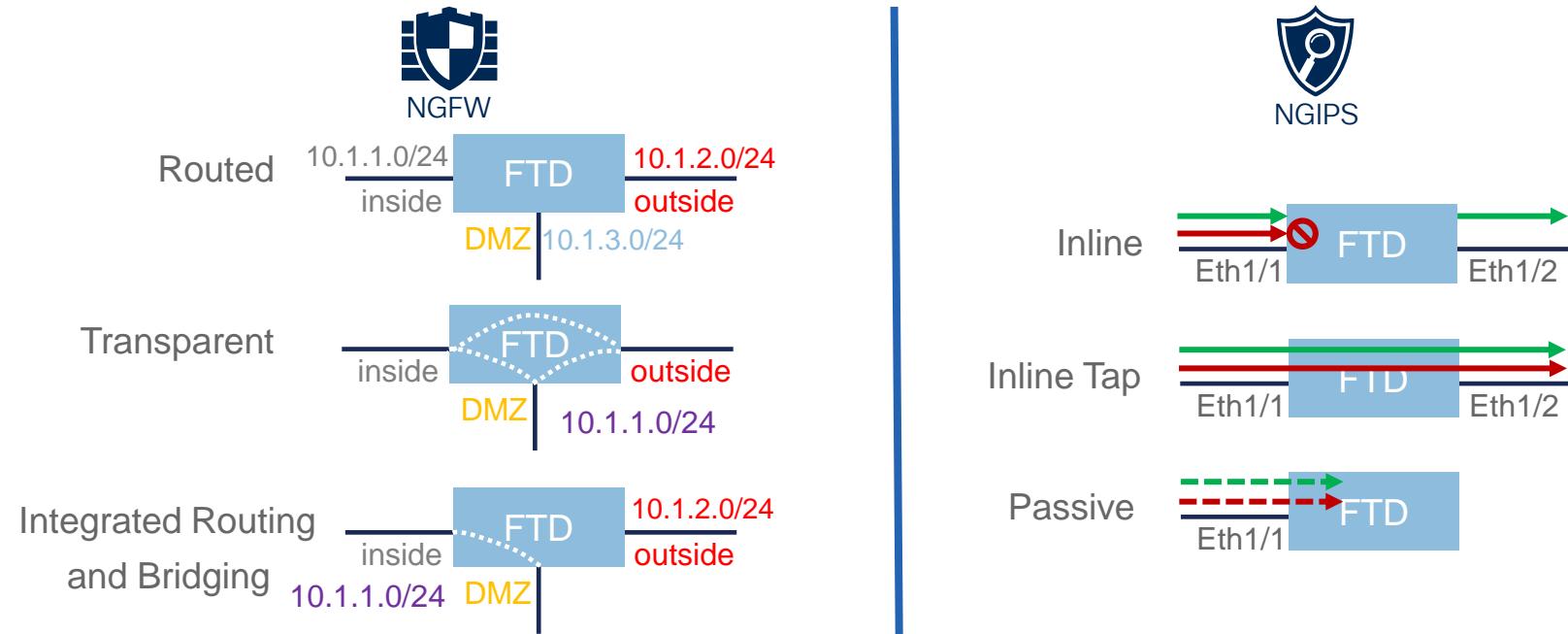
Data
Center

Service
Provider

Operational Modes



FTD Deployment Modes



Mode of Operation – IPS Only



▪ **Passive Mode**

- Detection only mode. Does not interrupt network traffic flow.
- Support physical interfaces and Ether Channels only.

Sensor sits between two physical ports on a switch or two different switches

▪ **Inline Mode**

- Blocks malicious traffic in real time.
- Support physical interfaces and Ether Channels only
- Cannot use redundant interfaces, VLANs, and sub-interfaces



Transparent Interfaces
Sensor is Layer 2 Bridge

▪ **Inline-Tap**

- Cabling is like the Inline mode, but act like the Passive mode.
- Switch between inline and inline-tap modes is done simply in the GUI.

Deployment Options



Feature	VMware	KVM	AWS	Azure
Routed Mode	✓	✓	✓	✓
Transparent Mode	✓	✓		
Inline Pair	✓	✓		
Inline TAP	✓	✓		
Passive	✓	✓	✓	
High Availability	✓	✓		



Appliance Mode (ASA Software Only)

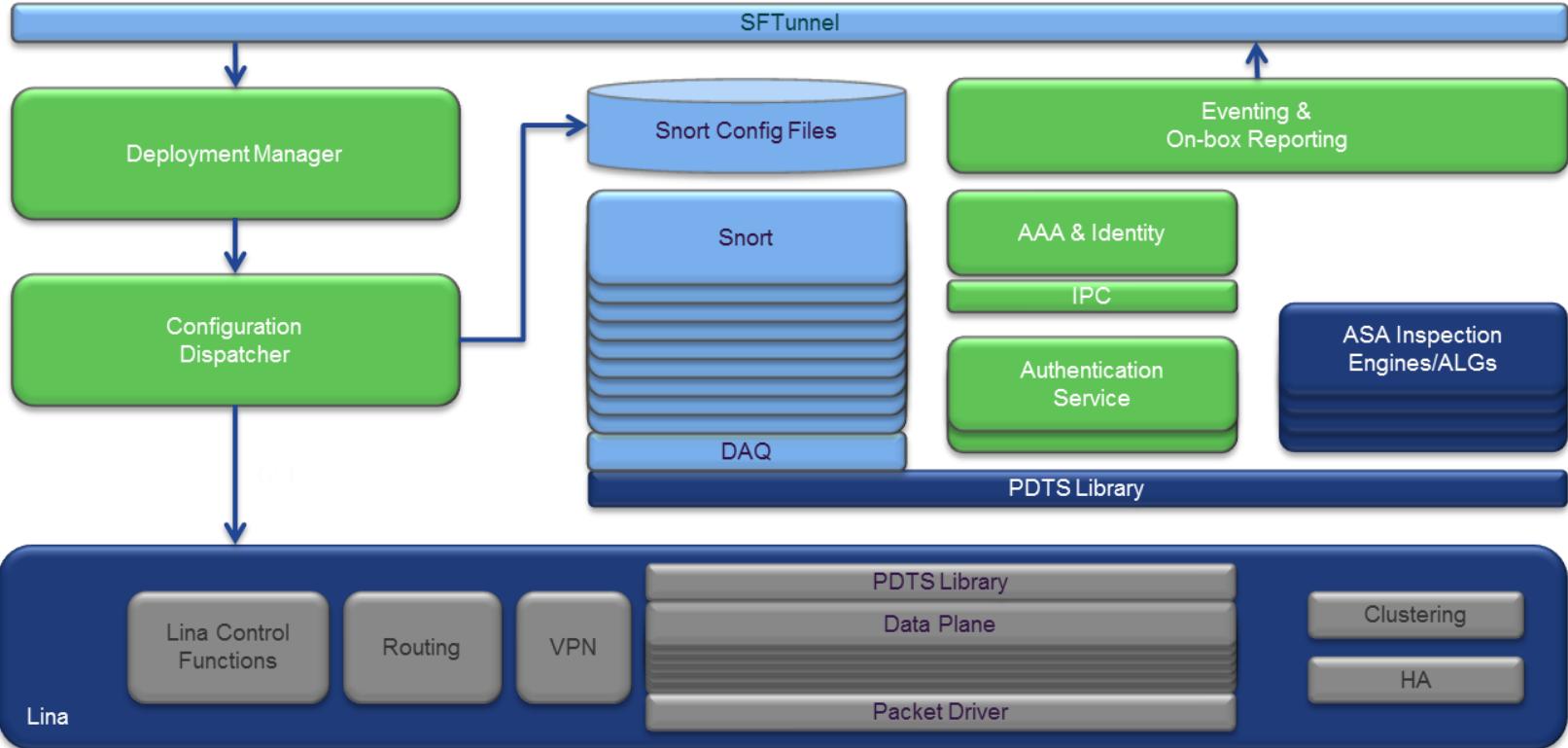
- Provides traditional ASA interfaces.
- Applies to the ASA software, not to the FTD software.

Mode	1000	2100	4100	9300
Appliance Mode	✓	✓		
Platform Mode		✓		

Architecture

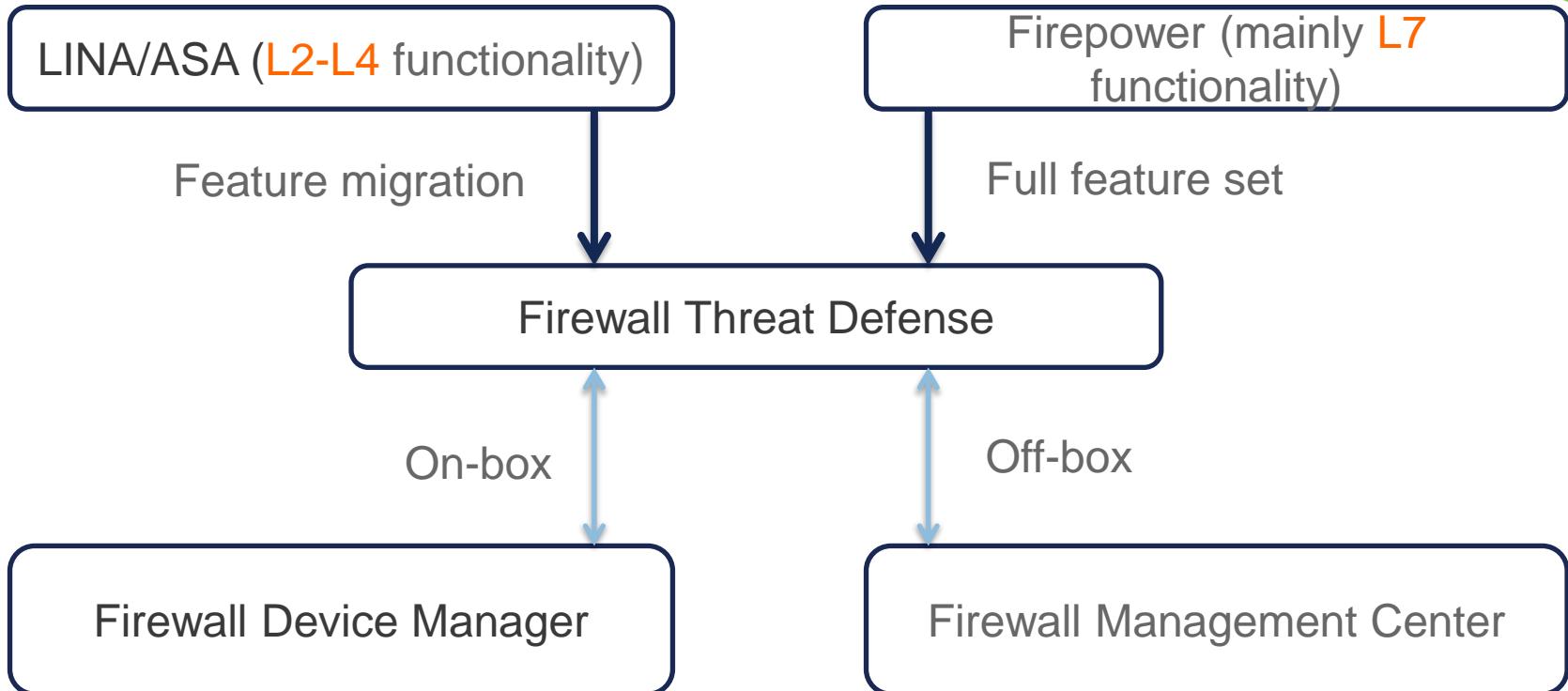


Architecture Diagram

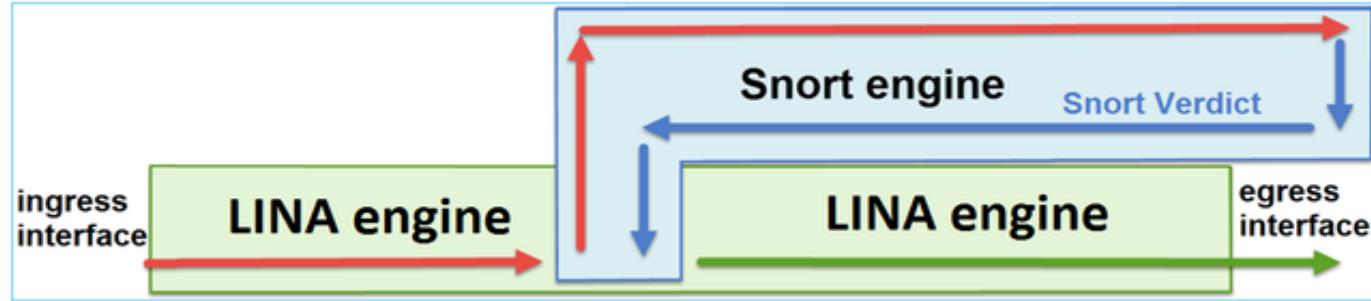




Firewall Threat Defense Introduction



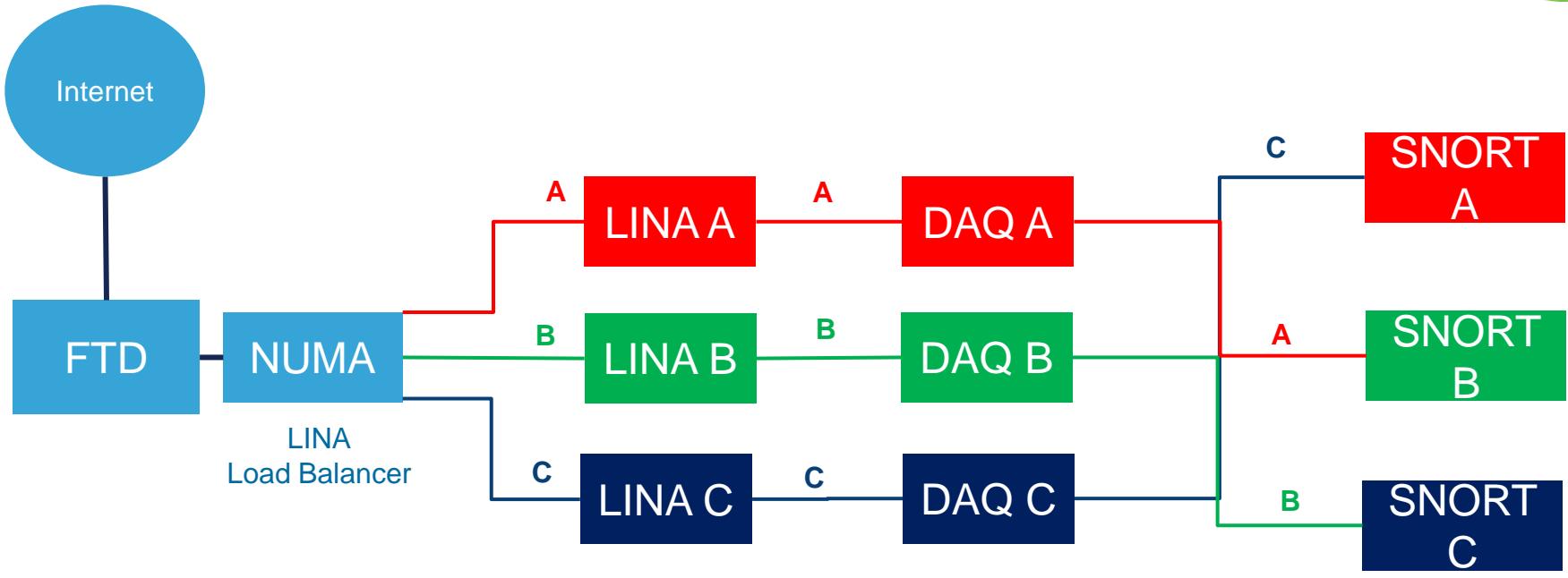
FTD Software Architecture – The Big Picture



- **LINA engine** (multiple instances of Data Path) - Focused on **L2-L4** functionality
 - **Snort engine** (multiple instances of Snort) - Focused on **L7** functionality
1. A packet enters the ingress interface, and it is **handled by the LINA engine**
 2. If the policy dictates so the packet is **inspected by the Snort engine**
 3. Snort engine **returns a verdict** (allow or block) for the packet
 4. The **LINA engine drops or forwards** the packet based on Snort's verdict



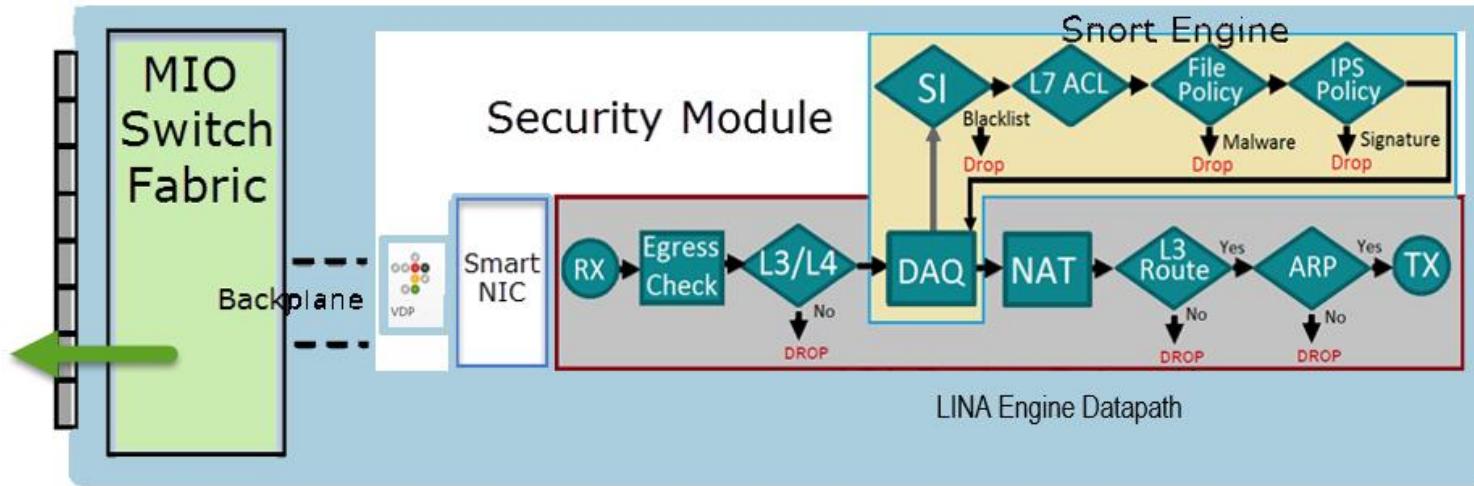
FTD Flow Load Balancing



DAQ Initiates Flows to SNORT Instance



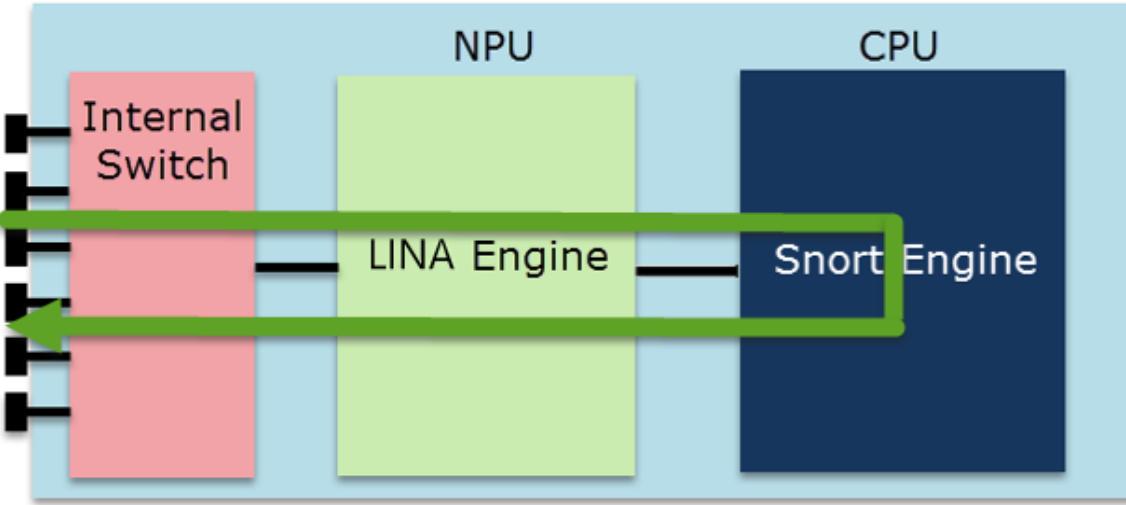
FXOS Architecture and Packet Flow



1. MIO receives the packet on physical port
2. MIO sends the packet to Decorator (DDoS - vDP Radware)
3. MIO receives the packet from Decorator (DDoS - vDP Radware)
4. MIO sends the packet to the Security Module (FTD). If there is FTD Clustering the MIO will get the packet back and send it to the peer unit
5. FTD sends the packet back to MIO
6. MIO sends the packet to the egress physical port

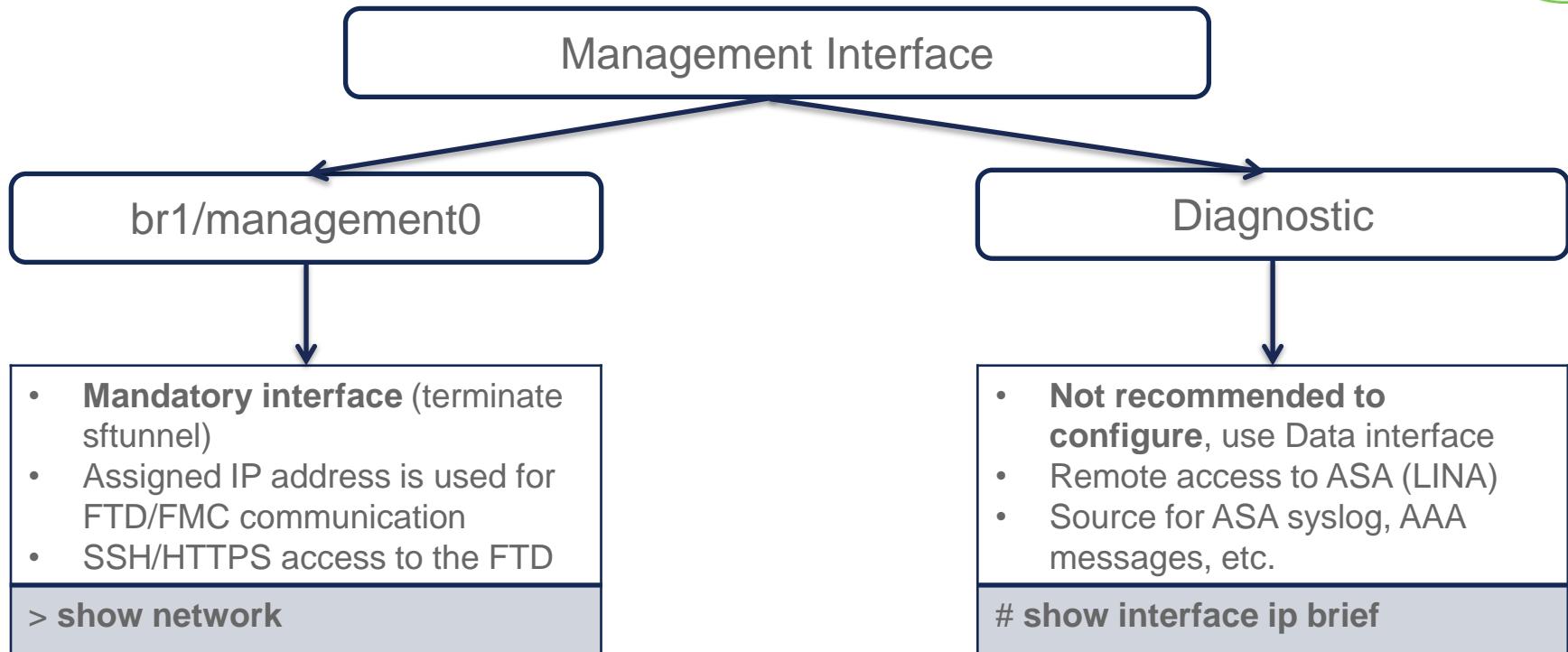
Packet Flow on FP2100

FTD on FP2100



1. The packet arrives on the Internal Switch
2. Internal Switch forwards the packet to the LINA (ASA) Engine (Network Processing Unit - NPU)
3. LINA (ASA) Engine forwards the packet to Snort Engine (CPU)
4. Snort Engine forwards the packet back to LINA (ASA) Engine (NPU)
5. LINA (ASA) Engine forwards the packet to the Internal Switch
6. The Internal Switch sends the packet back to physical network

FTD Diagnostic vs. Management Interface





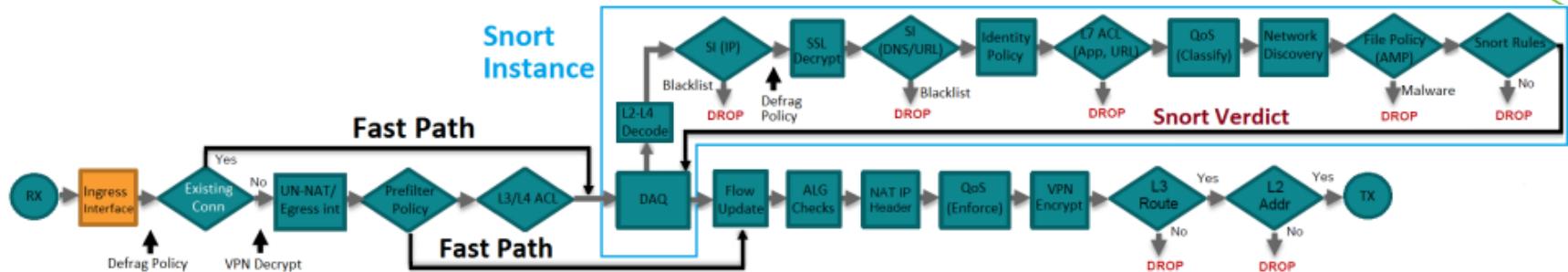
FTD Management Interface

- Firepower 1000/2000, ASA-5500-X
 - Defaults to DHCP
- 4100/9300, FTDv, ISA 3000
 - Default to DHCP NOT SUPPORTED



Packet Processing

FTD Packet Processing: Ingress Interface



- Packet arrives on ingress interface.
- Input counters are incremented by NIC and periodically retrieved by CPU
- Similar to classic ASA, input queue (RX ring) is an indicator of packet load

```
> show interface g1/2 detail
```

```
Interface GigabitEthernet1/2 "inside", is up, line protocol is up
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
```

```
IPS Interface-Mode: inline-tap, Inline-Set: Set1
```

```
47770671 packets input, 7620806887 bytes, 0 no buffer
```

```
Received 23734506 broadcasts, 0 runts, 0 giants
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
input queue (blocks free curr/low): hardware (1008/800)
```

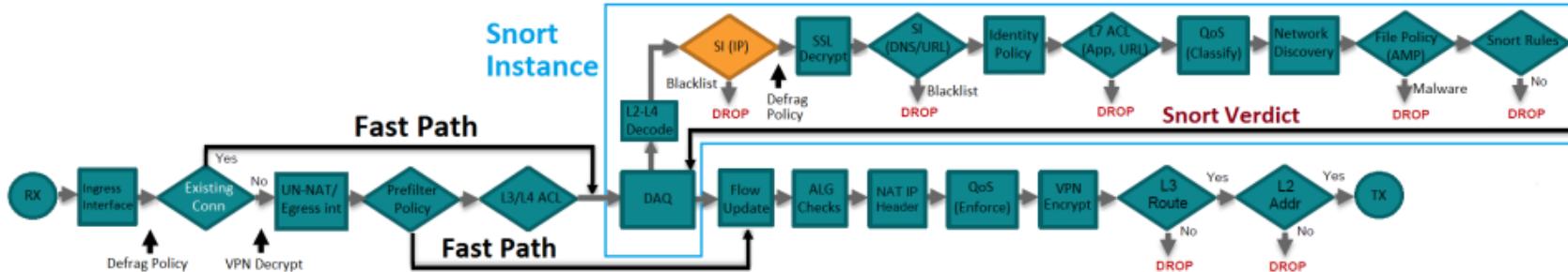
```
output queue (blocks free curr/low): hardware (1023/985)
```



Packet Processing Policy Tuning



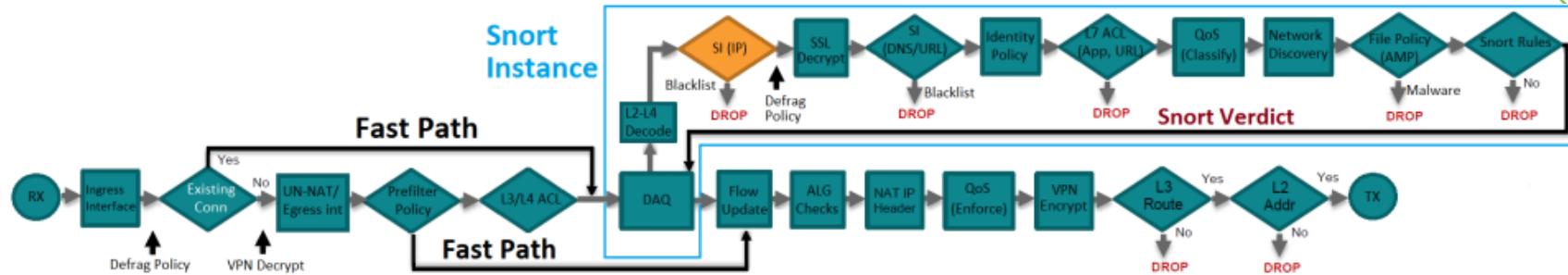
FTD Packet Processing: SI (IP)



- Security Intelligence (SI) can Drop or Allow IP addresses early in the packet processing lifetime within the Snort engine
- Do-Not-Block-List overwrites the Block-List
- The Blocklist can be populated in 2 ways:
 - Manually by the FMC administrator
 - Automatically by Intelligence Feed (Talos or custom) or List
- Snort returns to LINA a verdict about a packet being blocked

	Date	Time	Action	Source IP	Dest IP	Protocol	Port	Service	Protocol	Client Type	URL			
✓	2021-06-25 11:29:34	2021-06-25 11:29:34	Allow	192.168.26.54	128.8.10.99	USA	InZone	OutZone	32789 / udp	S3 (binary) / udp	DNS	dns client		
✓	2021-06-25 11:29:33	2021-06-25 11:29:33	Allow	192.168.24.2	188.125.82.68	IRL	InZone	OutZone	57122 / tcp	80 (http) / tcp	HTTP	Web browser		
✓	2021-06-25 11:29:33	2021-06-25 11:29:33	Allow	192.168.24.2	188.125.83.68	... (redacted)	InZone	OutZone	57962 / tcp	80 (http) / tcp	HTTP	Web browser		
✓	2021-06-25 11:29:33	2021-06-25 11:29:33	Allow	192.168.24.2	188.125.83.68	... (redacted)	InZone	OutZone	23.238	Open in New Window	pre_62795 / tcp	80 (http) / tcp	HTTP	Internet Explorer
✓	2021-06-25 11:29:23	2021-06-25 11:29:23	Allow	192.168.52.48	72.162	Exclude	pre_58115 / udp	53 (domain) / udp	DNS	dns client				
✓	2021-06-25 11:29:23	2021-06-25 11:29:23	Allow	192.168.10.100	72.162	Exclude	pre_58115 / udp	53 (domain) / udp	DNS	dns client				
✓	2021-06-25 11:29:23	2021-06-25 11:29:23	Allow	192.168.10.100	206.25	Open in Context Explorer	pre_58606 / udp	53 (domain) / udp	DNS	dns client				
✓	2021-06-25 11:29:23	2021-06-25 11:29:23	Allow	192.168.10.100	190.26	Whois	pre_57991 / udp	53 (domain) / udp	DNS	dns client				
✓	2021-06-25 11:29:23	2021-06-25 11:29:23	Allow	192.168.10.100	206.25	View Host Profile	pre_57619 / udp	53 (domain) / udp	DNS	dns client				
✓	2021-06-25 11:29:23	2021-06-25 11:29:23	Allow	192.168.10.100	56.031	Exclude	pre_56031 / udp	53 (domain) / udp	DNS	dns client				
✓	2021-06-25 11:29:20	2021-06-25 11:29:20	Allow	192.168.10.102	52.70	Add IP to Block List	pre_42778 / tcp	443 (https) / tcp	HTTPS	ssl client				
✓	2021-06-25 11:29:20	2021-06-25 11:29:20	Allow	192.168.24.173	91.198	Add IP to Do-Not-Block List	pre_49169 / tcp	12350 / tcp	Skype Auth	Skype Auth client				
✓	2021-06-25 11:29:20	2021-06-25 11:29:20	Allow	192.168.24.207	212.58	AlienVault IP	pre_53483 / tcp	80 (http) / tcp	HTTP	Chrome	... (redacted)	http://www.abuseipdb.com/reports/1142		
✓	2021-06-25 11:29:20	2021-06-25 11:29:20	Allow	192.168.22.89	75.101	IBM X-Force Exchange IP	pre_49490 / tcp	80 (http) / tcp	HTTP	Chrome	... (redacted)	http://edge.abuseipdb.com/events/14		
✓	2021-06-25 11:29:20	2021-06-25 11:29:20	Allow	192.168.22.89	75.101.145.202	USA	InZone	OutZone	49491 / tcp	80 (http) / tcp	HTTP	Chrome		
✓	2021-06-25 11:29:20	2021-06-25 11:29:20	Allow	192.168.16.236	172.241.249.145	GBR	InZone	OutZone	49473 / tcp	443 (https) / tcp	HTTPS	ssl client		
✓	2021-06-25 11:29:20	2021-06-25 11:29:20	Allow	192.168.16.236	172.241.249.145	GBR	InZone	OutZone	49473 / tcp	443 (https) / tcp	HTTPS	OpenX		

FTD Packet Processing: SI (IP)



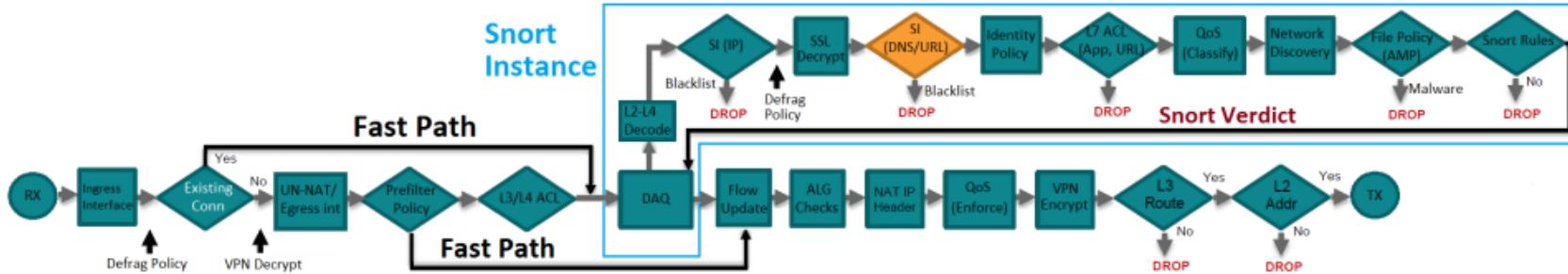
- The files containing the IPs from Talos SI Feed are in [/ngfw/var/sf/ipmap_download](#) directory

```
root@NGFW1:/ngfw/var/sf/ipmap_download# ls -alt | grep blf
-rw-r--r-- 1 root root 1252278 Jun 12 16:06 3e2af68e-5fc8-4b1c-b5bc-b4e7cab598ba.blf
-rw-r--r-- 1 root root 227696 Jun 12 16:05 032ba433-c295-11e4-a919-d4ae5275a468.blf
```

- If a packet is being dropped by Snort SI the LINA capture trace shows the Verdict

```
> show capture CAPI packet-number 1 trace
1: 16:07:45.147743      192.168.75.14 > 38.229.186.248: icmp: echo request
Phase: 14
Type: SNORT
Subtype:
Result: DROP
Additional Information:
Snort Verdict: (black-list) black list this flow
```

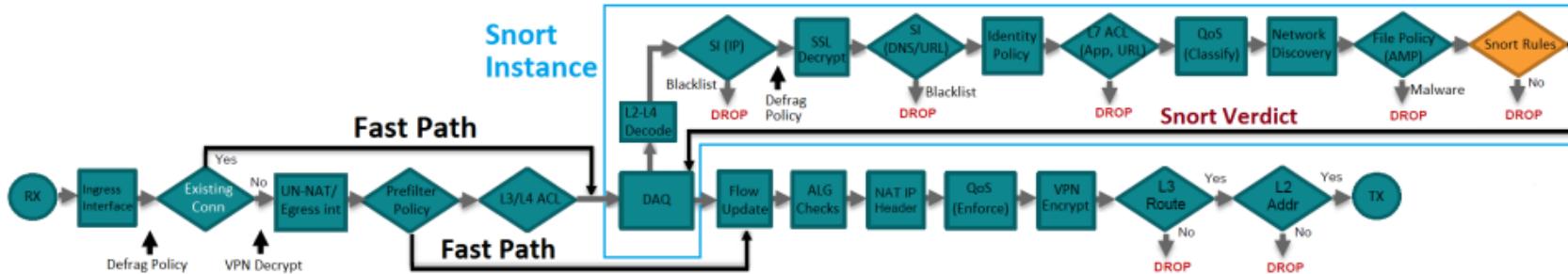
FTD Packet Processing: SI (DNS/URL)



Security Intelligence (URL)

- Works similarly to IP Security Intelligence and provides 3 actions
 1. Allow (Do-Not-Block-List)
 2. Block (Block-List)
 3. Monitor (Block-List)
- In case Talos URL Feed is used part of the db is stored locally and updated daily
- For non-cached URLs a Cloud lookup is done

FTD Packet Processing: Intrusion Policy



- Tracing a real packet shows the Snort engine verdict when a Snort Rule is being matched

```
> show capture CAPO packet-number 2 trace
2: 12:16:09.232776      192.168.77.40 > 192.168.75.39: icmp: echo reply
Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Verdict: (black-list) black list this flow
..
Result:
input-interface: outside
input-status: up
input-line-status: up
Action: drop
Drop-reason: (snort-drop) Snort requested to drop the frame
```

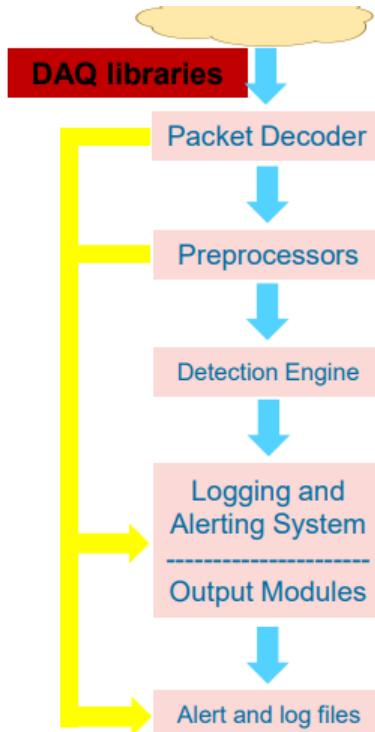
SNORT Architecture and Policies



SNORT 2 Architecture

Snort Architecture

- **Packet Decoder**
 - Packets are read using the Data AcQuisition library (DAQ)
(e.g. afpacket)
 - Decodes datalink protocols
 - Decodes network protocols
 - Decodes transport protocols
- **Preprocessors**
 - Examine packets
 - Modify packets
 - Normalize traffic
- **Detection Engine**
 - Uses Snort rules to create signatures for threats
 - Wide range of detection capabilities
 - Modular detection elements





SNORT 2 Architecture

Preprocessors

Handle the task of presenting packets and packet data in a contextually relevant way to the detection engine.

For example: HTTP header seen on non-standard port

Packet
fragment
reassembly

Maintaining
TCP state

TCP Stream
reassemble

Protocol
normalization

Frag(x)

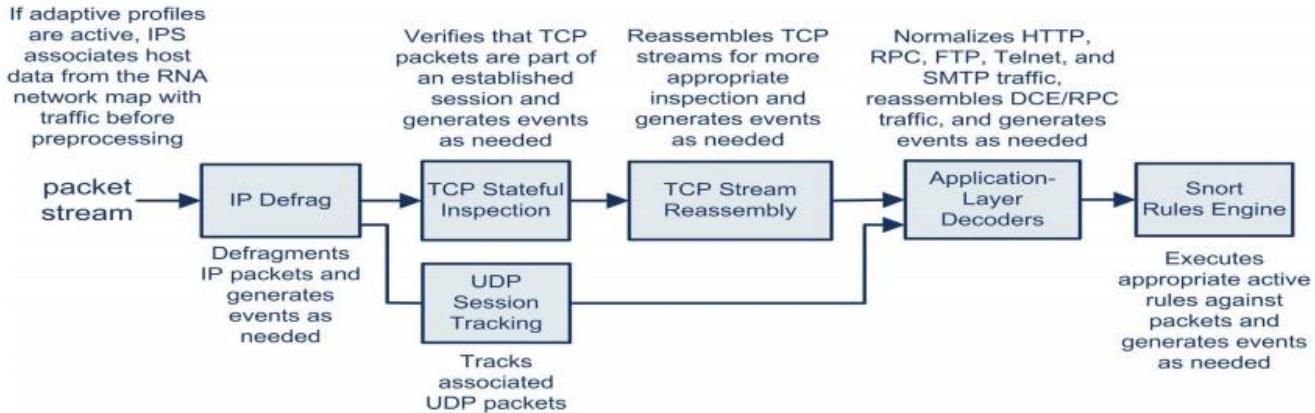
Stream(x)

8080, 8000, 8180, etc.



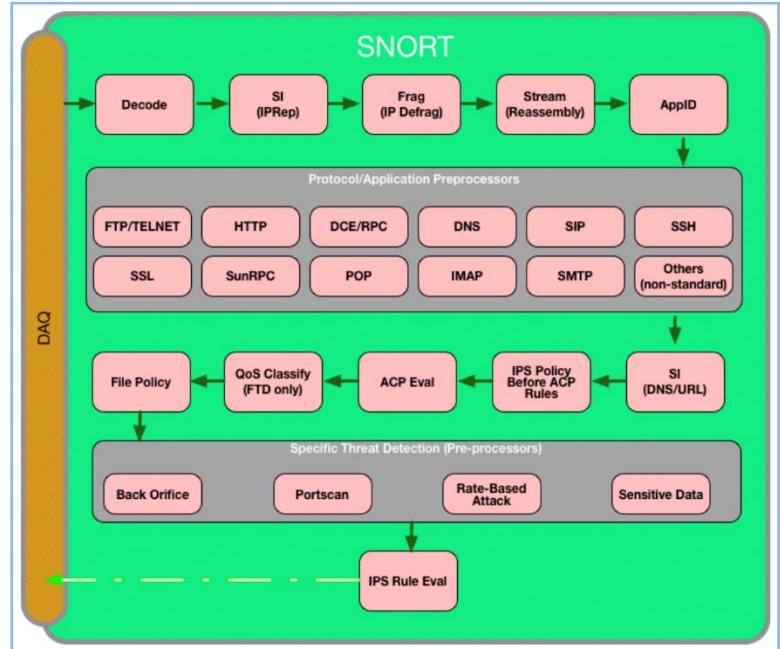
SNORT 2 Architecture

Preprocessors – Execution Order



SNORT 2 Components Supported

acl	AC policies in the packet path
pdt	Communication path between Lina and Snort
daq	Data Acquisition Layer for accepting the packet into SNORT
Snort-engine	Snort Generic Component
Snort-file processor	Snort File Processor Component
Snort-firewall	Snort Component responsible for enforcing Access Control Policy (AC Policy)





Snort 3 - Overview

- Snort 3 is now supported with FMC as well as FDM
- Snort 3 Device Management
 - Ability to toggle device Snort versions (Snort 2<->Snort 3) from FMC device management
- Upgrade / Migration Changes
 - Simplified Migration of Snort 2 to Snort 3 policies after upgrading to FP 7.0
 - Support for synchronizing common intrusion policies between Snort 2 and Snort 3 versions



Snort 3 Primer

- **Inspectors** replace preprocessors
- Event driven **Plugins** accomplish much of the processing objectives:
 - Codec - to decode and encode packets
 - Inspector - replaces Snort 2 preprocessors, for normalization, etc.
 - IpsOption - for detection in Snort rules
 - IpsAction - for custom actions
 - Logger - for handling events
 - Mpse - for fast pattern matching
 - So - for dynamic rules
- **Lightweight Security Package(LSP)** is the new release manager for Snort 3, replacing Security Rule Updates (SRU) – fast, smaller, higher frequency

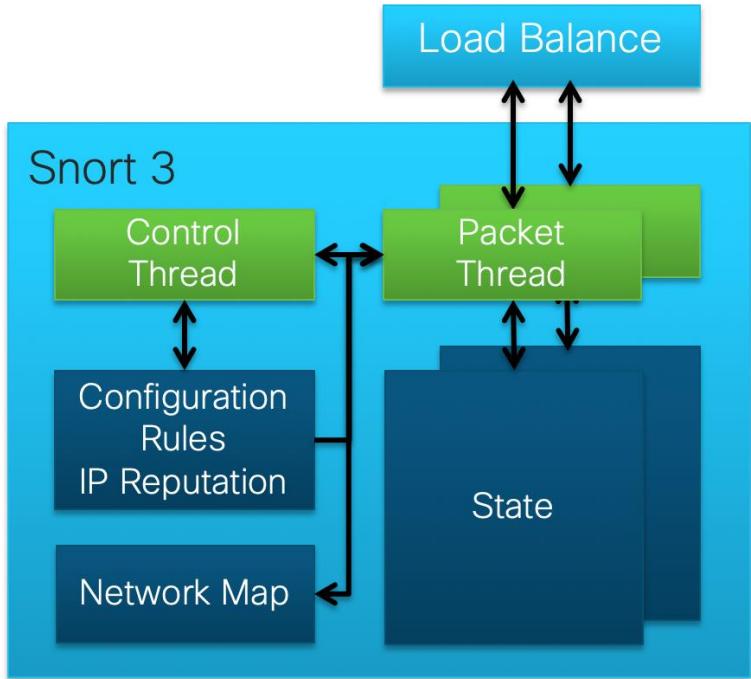


Snort 3 – Benefits

- Much more efficient memory utilization and faster reload times from multi-threaded architecture
- Faster/deeper pattern lookups with HyperScan for higher efficacy
- Improved human-readable signature language
- LSP Light Weight Security Package – Smaller and Faster
- Event-driven plugins replace preprocessors for quicker verdicts

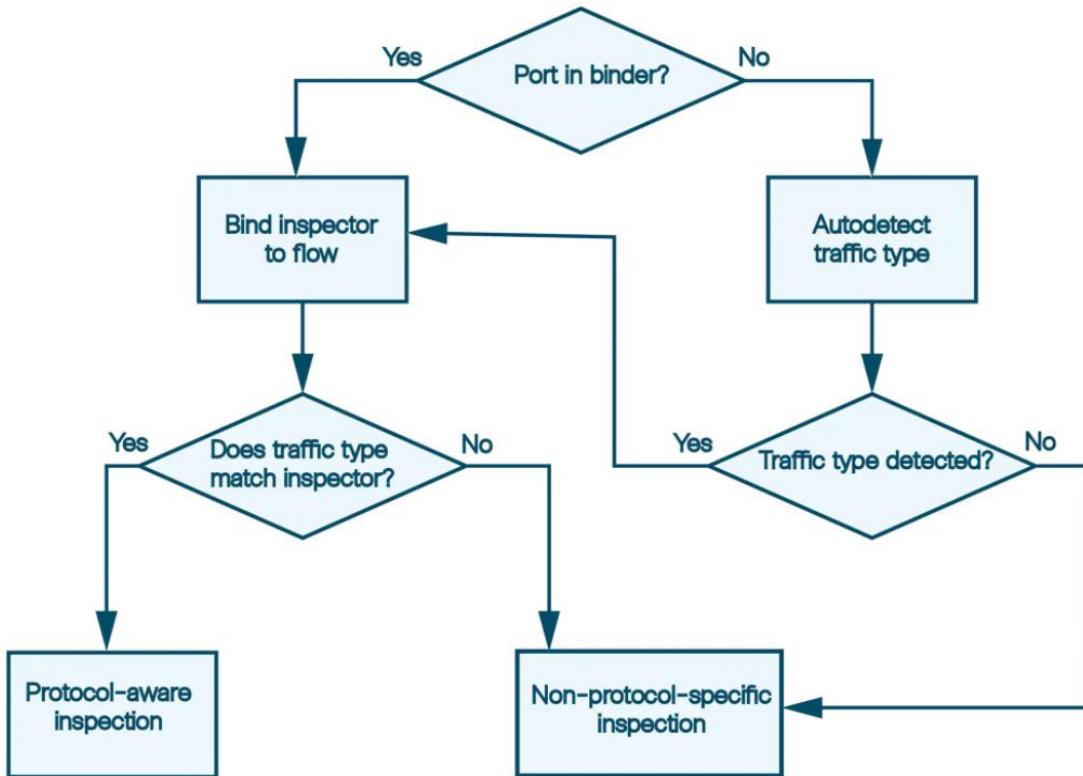
Snort 3.0 Architecture

- Threaded to utilize multiple cores
 - 1 control thread (main)
 - N packet threads per process
 - Reloads faster (1 vs N)
- A single config and network map
 - Uses less memory
 - Supports more IPS rules and larger netmap
- Rules written in text like Snort 2
 - More uniform syntax in Snort 3
 - Easier to read, write, and verify
 - “Snort2lua” converts 2.9 IPS rules to 3.0 format
 - LuaJIT will be added later by TALOS





Snort 3 Traffic Inspection





Custom Intrusion Rules

- Users can upload custom intrusion rules, written in Snort 3 rule syntax
- snort2lua tool on the FMC can be used to convert Snort 2 rules to Snort 3 syntax
- Each custom rule must have a SID (>1000000) and REV information
- GID need not be provided by the user
 - GID will be auto-generated per domain as in case of Snort 2
 - Auto generated GID will be different from Snort 2 GID to avoid SID collision`



Snort 3 – Changes in IPS Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BLACKLIST URI request for known malicious URI"; flow:established,to_server; content:"/setup_b.asp?prj="; nocase; http_uri; content:"&pid="; nocase; http_uri; content:"&mac="; nocase; http_uri; pcre:"/\setup_b\.asp\?prj=\d\x26pid=[^\r\n]*\x26mac=/Ui"; metadata:service http; sid:19626; rev:2;)
```



```
alert http
(
    msg:"BLACKLIST URI request for known malicious URI";
    flow:established,to_server;
    http_uri;
    regex:"/setup_b.asp\?prj=\d&pid=.*&mac=", nocase, fast_pattern;
    sid:19626; rev:4;
)
```

Basic Configuration



Basic Configuration

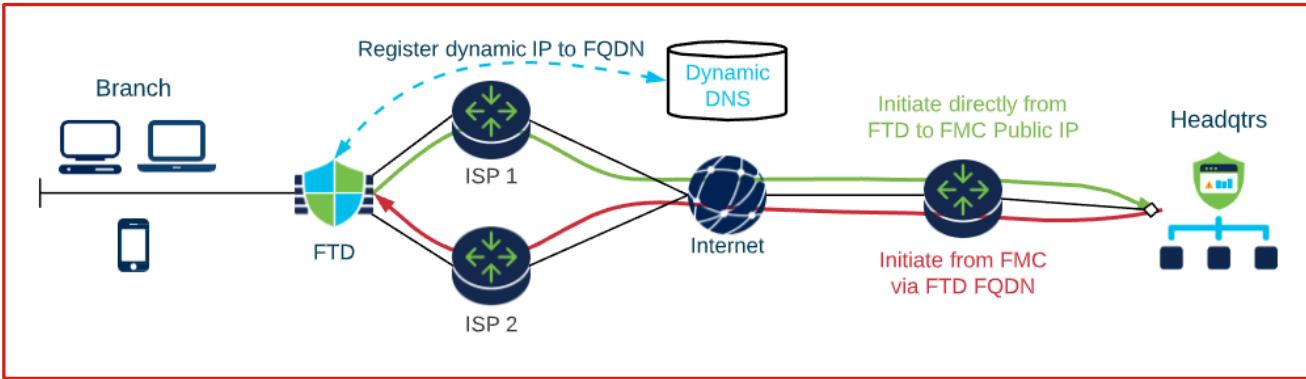
- Deploy physical or virtual appliance according to documentation
- First login Username: admin Password: Admin123
- Lab Login Username: admin Password: C1sco12345
- Check time zone
- Check licensing
- Configure FMC
- Register devices
- Configure Access Control Policies
- Deploy Configuration changes



FMC Remote Deployment

Remote Deployment

FMC management over one or more data interfaces for non-VPN use case



- Initial outside interface configuration through a CLI wizard
- Restore connectivity with FMC using CLI (Network Triggered or Policy Triggered)

Remote Deployment Bootstrap

Initial Bootstrap using FTD CLI

- CLI Wizard after the box is powered on
- FMC connection not required
- Command `configure network management-data-interface`

Configure FMC as manager on the FTD

- Existing command to configure FMC as manager on FTD
- FMC and FTD need connectivity over the data interface

Register the FTD on FMC

- Existing workflow of registering FTD on FMC
- FMC will discover the data interface used for management and display in UI



Device Access on FMC

NGFW1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP

General

Name:	NGFW1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

Inspection Engine

Inspection Engine:	Snort 2
--------------------	---------

NEW Upgrade to our new and improved Snort 3

Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Threat Defense devices. With significant improvements to performance and security efficacy, there is a lot to be excited about! [Learn more](#)

⚠️ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

FMC Access Interface

This is an advanced setting and need to be configured only if needed. Review documentation guide for more details.

Manage device by

Data Interface
Management Interface
Data Interface

Management to Data Interface causes the device to deploy, pick a data interface and enable it for FMC Access. See the [online help](#) for detailed steps.

System

Model:	Cisco Firepower Threat Defense for VMware
Serial:	9A3AELLN75A
Time:	2021-10-25 17:53:52
Time Zone:	UTC (UTC+0:00)
Version:	7.0.0
Time Zone setting for Time based Rules:	UTC (UTC+0:00)

Management

Host:	ngfw1.ddcloud.local
Status:	✓
FMC Access Interface:	Management Interface



Device Access Info on FMC

Firepower Management Center Devices / NGFW Interfaces Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin Save Cancel

kochi.ath.cx Cisco Firepower Threat Defense for VMWare Device Routing Interfaces Inline Sets DHCP

Interface	Logical Name	Type
Diagnostic0/0	diagnostic	Physical
GigabitEthernet0/0 (FMC Access)	outside	Physical
GigabitEthernet0/1		Physical
GigabitEthernet0/2		Physical
GigabitEthernet0/3		Physical
GigabitEthernet0/4		Physical
GigabitEthernet0/5		Physical

Manage Virtual Routers Global Virtual Router Properties OSPF OSPFv3 RIP BGP IPv4 IPv6 Static Route Multicast Routing IGMP PIM Multicast Routes Multicast Boundary Filter

Save Cancel

Firepower Management Center Devices / NGFW Routing Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin Save Cancel

kochi.ath.cx Cisco Firepower Threat Defense for VMWare Device Routing Interfaces Inline Sets DHCP

+ Add Route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Any-IPv4	outside (FMC Access)	Global	gw	false	1	
IPv4-Private-10.0.0.0-8	diagnostic	Global	gwnetworking	false	1	
IPv4-Private-172.16.0.0-12	diagnostic	Global	gwnetworking	false	1	

How To

Data Interface for FMC access highlighted along with the static routes

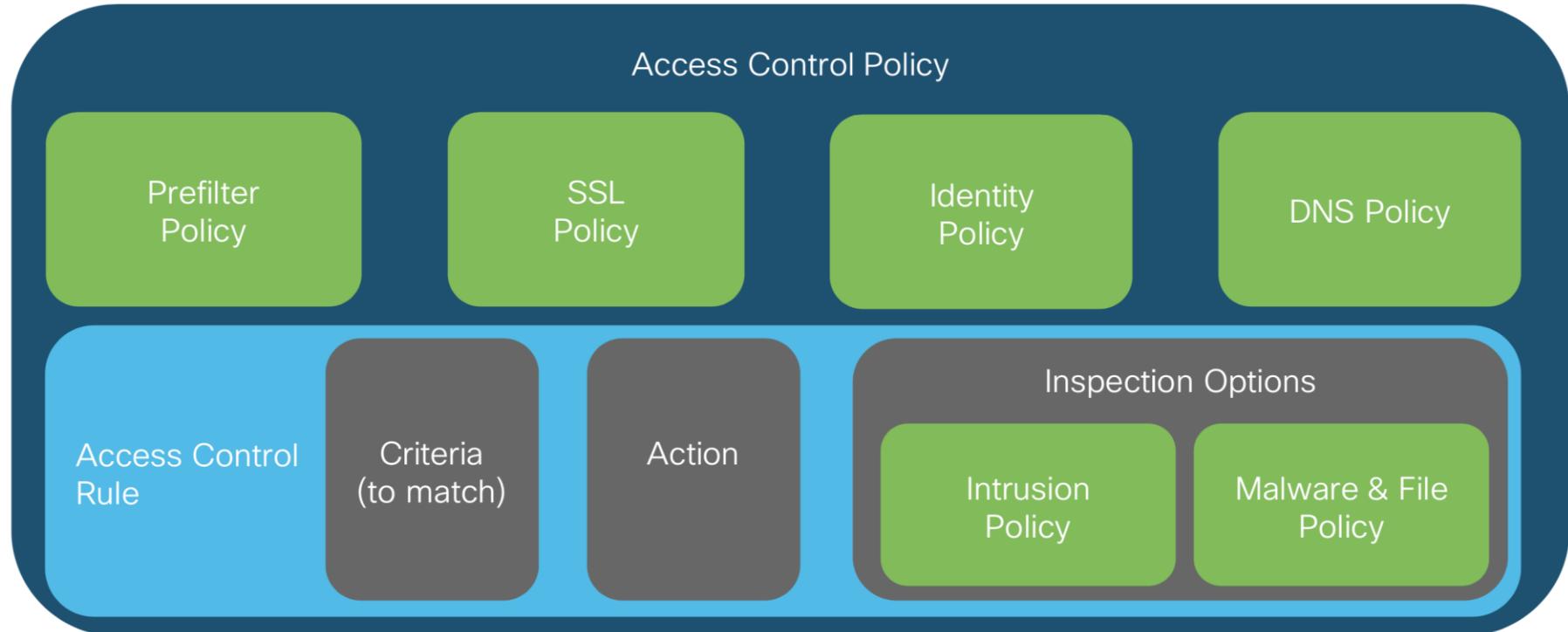




Packet Processing Policy Enforcement with ACLs



Access Control Policy Components





Access Control Policy – Overview

- Central location to invoke all security policies
- Defines “what & how” traffic is allowed, blocked, inspected and logged
- Provide granular criteria to handle traffic, such as,
 - Zones
 - Networks
 - VLAN Tags
 - Applications
 - Ports
 - URLs
 - Users
 - Identity Attributes

Add Rule

Name	<input type="text" value="AC Rule"/>	<input checked="" type="checkbox"/> Enabled	Insert	<input type="text" value="into Mandatory"/>
Action	<input checked="" type="radio"/> Allow			
Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes				



ACP Invokes All Policies

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin ▾

AC Policy

Enter Description

Show Warnings Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

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

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device

Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	Shield	Globe	Lock	Document	Comment	Settings
▼	Mandatory - AC Policy (-)																			
There are no rules in this section. Add Rule or Add Category																				
▼	Default - AC Policy (-)																			
There are no rules in this section. Add Rule or Add Category																				
Default Action																				
Intrusion Prevention: Balanced Si																				





ACP Invokes All Policies cont'd

Add Rule

Name: AC Rule Enabled: Insert: into Mandatory

Action: Allow

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Intrusion Policy: IPS/IDS Policy Variable Set: Default Set

File: File Policy

Cancel Add



FMC: Policy deployment delta preview

A screenshot of the Cisco Firepower Management Center (FMC) Deployment page. The page title is "Deployment" and it says "Select the device to deploy to". On the left, there's a tree view of policy groups under "vklaузов-demo-2": "Access Policy Group" containing "Access Control Policy: demo", "File Policy: File-detection-home", and "Intrusion Policy: IPS-home"; and "Device Configurations" containing "Interface Policy" and "Routing Group". On the right, there's a table with columns: Inspect Interruption, Type, Group, and Last Modified. There are two rows: one for a Sensor (FTD) and one for a FTD. At the bottom right, a large orange circle highlights a button labeled "Preview the changes" with a cursor icon pointing to it.

Inspect Interruption	Type	Group	Last Modified
–	Sensor	M	10/17/2023
No	FTD	Peno	10/17/2023



FMC: Selective policy deployment

Deployment

Select the devices to deploy policy changes

Search using device name, type, or version

Device

vklauzov-demo-1

Access Policy Group

Show or hide policy selection

Policy: demo ● ●

Prefilter Policy: custom-prefilter ●

File Policy: File-detection-home ●

Intrusion Policy: IPS-SIP-inspect ●

NAT Group

Manual NAT Rules: NAT

Deployment

Select the devices to deploy policy changes

Search using device name, type, or version

Device

vklauzov-demo-1

Access Policy Group

Access Control Policy: demo ● ●

Prefilter Policy: custom-prefilter ●

File Policy: File-detection-home ●

Intrusion Policy: IPS-SIP-inspect ●

NAT Group

Manual NAT Rules: NAT



Selective Policy Deployment

Firepower Management Center Deploy / Deployment

Overview Analysis Policies Devices Objects Deploy sec-ops ▾

3 devices selected Deploy time: Estimate Deploy

Search using device name, type, domain, group or status	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> Device						
<input checked="" type="checkbox"/> NGFWBR1		FTD		Nov 3, 2020 1:37 AM		Pending
<input checked="" type="checkbox"/> Access Control Group						
<input checked="" type="checkbox"/> NGFWTG		FTD		Nov 3, 2020 1:37 AM		Pending
<input checked="" type="checkbox"/> Access Control Group						
<input checked="" type="checkbox"/> NGFW1		FTD		Nov 3, 2020 1:39 AM		Pending
<input checked="" type="checkbox"/> Access Control Group						

**IPS Policy Allowed to deploy Selectively
(Unrelated changes)**

The diagram shows a blue rectangular box highlighting the "Access Control Group" section for the NGFW1 device. An arrow points from this highlighted area to a callout box containing the text "IPS Policy Allowed to deploy Selectively (Unrelated changes)".



Time-based rules in ACP and pre-filter policies

- Enables administrator to:
 - Configure time-based URL filtering, content inspection
 - Define a time range object that can be "absolute" or "periodic" and includes time zone
- Standalone / HA / Cluster supported
- No additional licensing required
- FMC - UI and APIs, FDM – only APIs

Firepower Management Center Objects / Object Management

Time Range Time Zone

Name	Effective Dates	Time
tr-abs1	Started to Never End	
tr-abs2	2020-01-16, 09:00 to 2020-01-23, 17:00	
tr-rec1-daily	2020-01-16, 09:00 to 2020-01-31, 17:00	Daily Interval: Weekdays, 09:00 to 17:00
tr-rec2-range	2020-01-16, 09:00 to 2020-01-31, 17:00	Range: Mon 09:00 to Tue 17:00
tr-rec3-range-daily	2020-01-16, 09:00 to 2020-01-31, 17:00	Daily Interval: Weekend, 09:00 to 17:00 Range: Mon 09:00 to Tue 17:00

Name	Time Zone	Day Light Saving
EST-no-DST	(UTC-05:00) Canada/Eastern	No Daylight Savings
EST-with-DST	(UTC-05:00) Canada/Eastern	02:00, 08/03/2020 to 02:00, 01/11/2020
test	(UTC-12:00) Etc/GMT+12	No Daylight Savings

Add Rule

Name: test Enabled:

Action: Allow

Insert: below rule

Time Range: tr-abs1

Zones: inside, outside

Networks:

VLAN Tags:

Users:

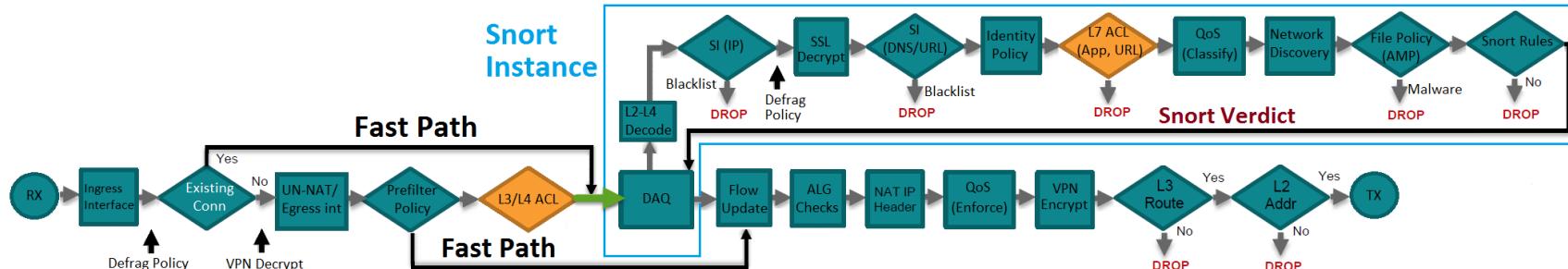
Applications:

Available Zones: Search by name: inside, outside

Add to Source, Add to Destination



FTD Packet Processing: ACL best practices



- Use Prefilter Policy Fastpath rules for big ‘fat’ flows
- Place more specific rules at the top of the Access Control Policy
- Place rules that require Snort inspection at the bottom of the policy
- Avoid excessive logging
- Be aware of rule expansion

```
> show access-list | include elements
access-list CSM_FW_ACL_; 7 elements; name hash: 0x4a69e3f3
```

```
admin@NGFW1$ cat /var/sf/detection_engines/UUID/ngfw.rules | grep "Start of AC rule" -A 10000000 | grep -v " of AC rule." | wc -l
```

32



Best Practice: Block Sooner then Later

- Any rules that drop traffic based on only IP address or port number should come as early as possible.
- Prefilter is the optimal choice in this case.

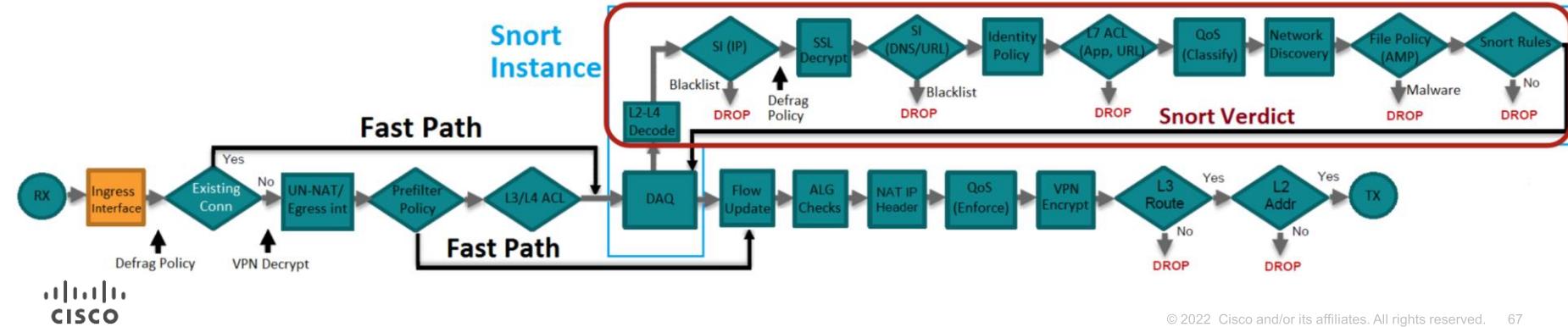
Add Prefilter Rule

Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpath traffic bypasses access control and QoS.

Name: Prefilter Rule Insert: below rule 0

Block

Interface Objects (highlighted with a red box) Networks VLAN Tags Ports





Best Practice: Specific Rule Comes First

- Specific rules should come before general rules, especially when the specific rules are exceptions to general rules.
- Put specific drop rules near the top of the policy. This ensures the earliest possible decision on undesirable traffic.

Screenshot of the Firepower Management Center showing the AC Policy configuration screen. The policy has two rules defined:

Name	Sour... Zones	Dest Zо...	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
1 Block 10 Exception	Any	Any	10.1.1.1	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block
2 Allow 10 Network	Any	Any	IPv4-Private-10.0.0.0-8	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

The first rule, "Block 10 Exception", is highlighted with a red box. The second rule, "Allow 10 Network", is also highlighted with a red box. The "Action" column for the second rule shows the "Allow" button, which is also highlighted with a red box.



Best Practice: Avoid Rules Conflicts

Identify the duplicate or shadow rules when adding new access rules

Screenshot of the Cisco Firepower Management Center interface showing the Policies tab for an AC Policy.

The interface includes:

- Top navigation bar: Overview, Analysis, Policies (selected), Devices, Objects, AMP, Intelligence, Deploy, Notifications (2), Settings, Help, and admin.
- AC Policy title and description input field.
- Buttons: Analyze Hit Counts, Save, Cancel.
- Policy settings: Inheritance Settings, Prefilter Policy (Default Prefilter Policy), SSL Policy (None), Identity Policy (None).
- Tab navigation: Rules (selected), Security Intelligence, HTTP Responses, Logging, Advanced.
- Rules section: Filter by Device, Show Rule Conflicts checkbox (highlighted with a red box), Add Category, Add Rule, Search Rules.
- Table header: Name, Source Zones, Dest Zones, Source Netw..., Dest Netw..., VLAN Tags, Users, Appli..., Source Ports, Dest Ports, URLs, Source SGT, Dest SGT, Act... (with icons for shield, file, lock, etc.).
- Table body: ▼ Mandatory - AC Policy (-)



Best Practice: Logging for Security Incidents

- Disable “per rule logging” where not needed
- When logging is required, enable it at the End of Connection

Add Rule

Name: AC Rule Insert: into Mandatory

Action: Allow

Enabled:

Logging: Log at Beginning of Connection Log at End of Connection

File Events: Log Files

Send Connection Events to:

Event Viewer

Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides

SNMP Trap Select an SNMP Alert Configuration +

Cancel Add



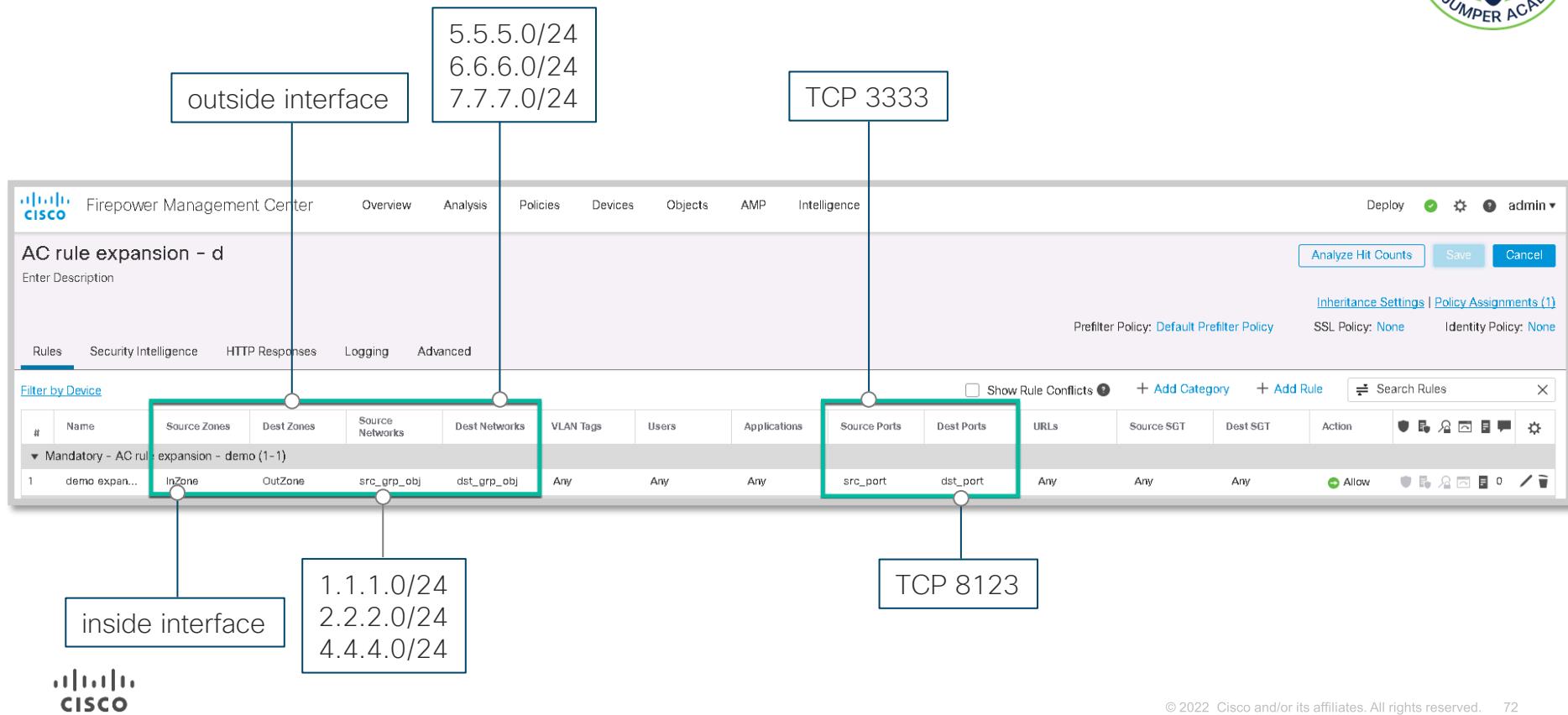


Access Rule Expansion

- Access Control rules in the GUI gets expanded to multiple Access Control elements once it's deployed to FTD
- There are limitations for the number of expanded rules for each platform (depending on the amount of available memory) and other factors



Example: Access Rule Expansion



```
access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in object-group src_grp_obj object-group src_port ifc out object-group dst_grp_obj object-group dst_port rule-id 268434508 (hitcnt=0) 0xf3aaacc3

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 1.1.1.0 255.255.255.0 eq 3333 ifc out 7.7.7.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0xb4439cd3

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 1.1.1.0 255.255.255.0 eq 3333 ifc out 6.6.6.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0xeb2e68f7

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 1.1.1.0 255.255.255.0 eq 3333 ifc out 5.5.5.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0x8c62bd17

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 2.2.2.0 255.255.255.0 eq 3333 ifc out 7.7.7.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0xdbc1fa4c

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 2.2.2.0 255.255.255.0 eq 3333 ifc out 6.6.6.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0xbcef694a

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 2.2.2.0 255.255.255.0 eq 3333 ifc out 5.5.5.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0x906459c7

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 4.4.4.0 255.255.255.0 eq 3333 ifc out 7.7.7.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0x2dd6c9d9

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 4.4.4.0 255.255.255.0 eq 3333 ifc out 6.6.6.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0x7c918805

access-list CSM_FW_ACL_ line 13 advanced permit tcp ifc in 4.4.4.0 255.255.255.0 eq 3333 ifc out 5.5.5.0 255.255.255.0 eq 8123 rule-id 268434508 (hitcnt=0) 0xaee562c3
```

each SRC and DST network group-object contains 3 objects/elements
both SRC and DST ports includes each 1 element/object
and SRC and DST zones includes each 1 interface

The expanded rule element written down to LINA is a multiplier of all objects: **1x1x3x3x1x1=9**

Sizing Recommendation Based on AC Rule Element



Platform	Max Recommended AC elements on LINA
FPR 2120	75,000
FRP 2140	375,000
FPR 4110	2,250,000
FPR 4120	2,250,000
FPR 4140	2,250,000
FPR 4150	3,000,000
FPR 9300 with 1x SM-24	2,250,000
FPR 9300 with 1x SM-36	2,250,000
FPR 9300 with 1x SM-44	3,000,000
FPR 9300 with 3 clustered SM-44	3,000,000



When to implement Object Group Search (OGS)

- FMC provides **health warning** when the **number of Access Control Entries (ACEs)** reaches the limit of recommended entries per platform basis; then it suggests enabling OGS
- Feature is applicable for **Standalone**, **High-Availability**, and **Clustering** deployments from **6.6 release onwards**
- Expensive operation / CPU intense during packet processing process
- Should be **implemented** when **device is running low on memory**



FMC configuration - OGS

Firepower Management Center
Devices / NGFW Device Summary

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

FTD-66

Cisco Firepower Threat Defense for VMWare

Device Routing Interfaces Inline Sets DHCP

Storage:	NA
Chassis Url:	NA
Chassis Serial Number:	NA
Chassis Module Number:	NA
Chassis Module Serial Number:	NA

Applied Policies

Access Control Policy: empty

Prefilter Policy: Default Prefilter Policy

SSL Policy:

DNS Policy: Default DNS Policy

Advanced Settings

Application Bypass: No

Bypass Threshold: 3000 ms

Object Group Search: Enabled

OGS





Illustrative example – Access control policy rules

Rules	Security Intelligence	HTTP Responses	Logging	Advanced Settings				
Filter by Device <input type="button" value="Search Rules"/>								
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports
▼ Mandatory - empty (1-1)								
AC rule expansion example	Any	Any	1.1.1.1 2.2.2.2	3.3.3.3 4.4.4.4	Any	Any	Any	Any



Object Group Search OGS disabled

```
# show run object-group-search
#
# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip object-group FMC_INLINE_src_rule_268434433 object-group
FMC_INLINE_dst_rule_268434433 rule-id 268434433 (hitcnt=0) 0xeb692b0
access-list CSM_FW_ACL_ line 10 advanced permit ip host 1.1.1.1 host 3.3.3.3 rule-id 268434433 (hitcnt=0) 0xa866baa3
access-list CSM_FW_ACL_ line 10 advanced permit ip host 1.1.1.1 host 4.4.4.4 rule-id 268434433 (hitcnt=0) 0x1f2904fd
access-list CSM_FW_ACL_ line 10 advanced permit ip host 2.2.2.2 host 3.3.3.3 rule-id 268434433 (hitcnt=0) 0x7cbde7d7
access-list CSM_FW_ACL_ line 10 advanced permit ip host 2.2.2.2 host 4.4.4.4 rule-id 268434433 (hitcnt=0) 0x64d8a459
```

4 elements

Object Group Search OGS enabled

```
# show run object-group-search
object-group-search access-control
#
# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip object-group FMC_INLINE_src_rule_268434433 object-group
FMC_INLINE_dst_rule_268434433 rule-id 268434433 (hitcnt=0) 0xeb692b0
access-list CSM_FW_ACL_ line 10 advanced permit ip v4-object-group FMC_INLINE_src_rule_268434433(2147483648) v4-object-group
FMC_INLINE_dst_rule_268434433(2147483649) rule-id 268434433 (hitcnt=0) 0xe88cf0c7
```

1 element



Interface Object Optimization

Firepower Management Center Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy admin ▾

NGFW1 Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP

Inspection Engine: Snort 2
NEW Upgrade to our new and improved Snort 3
Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Threat Defense devices. With significant improvements to performance and security efficacy, there is a lot to be excited about! [Learn more](#)
⚠️ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.
Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.
[Upgrade](#)

Status: Policy: Initial_Health_Policy 2020-11-20 21:02:54 Advanced Settings
Host: ngfw1.ccloud.local Status:
Management Interface:

Automatic Application Bypass:
Bypass Threshold (ms): 3000
Object Group Search:
Interface Object Optimization:

Cancel Save Base_Policy
Prefilter Policy: Default Prefilter Policy
SSL Policy: Default SSL Policy
DNS Policy: Default DNS Policy
Identity Policy: NGFWIdentityPolicy

Advanced Settings
Application Bypass: No
Bypass Threshold: 3000 ms
Object Group Search: Disabled
Interface Object Optimization: Disabled





Interface Object Optimization

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports
▼ Mandatory - nsz (1-2)										
1	allow-egress	inside-zone	outside-zone	inside-hosts	Any	Any	Any	Any	Any	Any
2	allow-ingress	outside-zone	inside-zone	outside-host	Any	Any	Any	Any	Any	Any
▼ Default - nsz (-)										

Disabled

```
> show running-config access-list
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268437508: ACCESS POLICY: nsz - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268437508: L7 RULE: allow-egress
access-list CSM_FW_ACL_ advanced permit ip ifc interface1 object inside-hosts ifc interface3 any rule-id 268437508
access-list CSM_FW_ACL_ advanced permit ip ifc interface1 object inside-hosts ifc interface4 any rule-id 268437508
access-list CSM_FW_ACL_ advanced permit ip ifc interface2 object inside-hosts ifc interface3 any rule-id 268437508
access-list CSM_FW_ACL_ advanced permit ip ifc interface2 object inside-hosts ifc interface4 any rule-id 268437508
access-list CSM_FW_ACL_ remark rule-id 268437509: ACCESS POLICY: nsz - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268437509: L7 RULE: allow-ingress
access-list CSM_FW_ACL_ advanced permit ip ifc interface3 object outside-host ifc interface1 any rule-id 268437509
access-list CSM_FW_ACL_ advanced permit ip ifc interface3 object outside-host ifc interface2 any rule-id 268437509
access-list CSM_FW_ACL_ advanced permit ip ifc interface4 object outside-host ifc interface1 any rule-id 268437509
access-list CSM_FW_ACL_ advanced permit ip ifc interface4 object outside-host ifc interface2 any rule-id 268437509
access-list CSM_FW_ACL_ remark rule-id 268437507: ACCESS POLICY: nsz - Default
```

Enabled

```
> show running-config access-list
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: nsz - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434433: L7 RULE: allow-egress
access-list CSM_FW_ACL_ advanced permit ip object-group-ifc inside-zone object-group inside-hosts object-group-ifc outside-zone any
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: nsz - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434434: L7 RULE: allow-ingress
access-list CSM_FW_ACL_ advanced permit ip object-group-ifc outside-zone object-group outside-hosts object-group-ifc inside-zone any
```

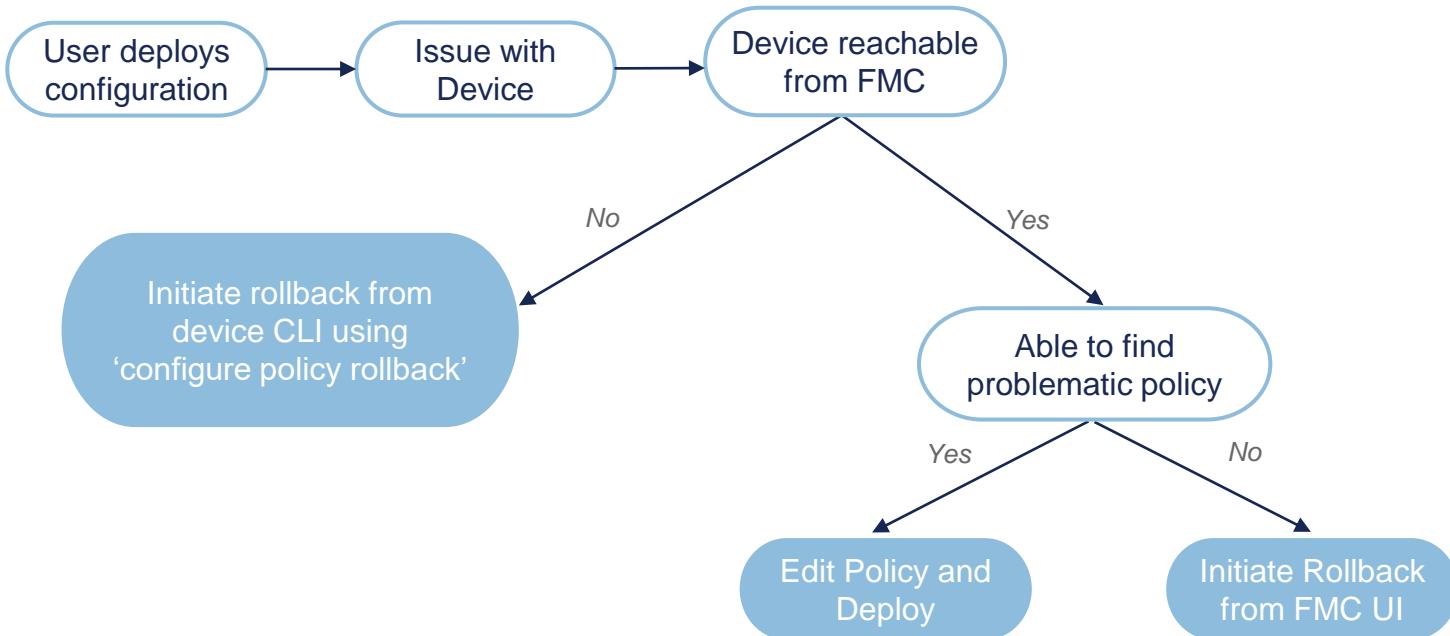


Rollback Feature Overview

- Can rollback to one of last 10 successful deployment configurations
- Rollback Preview - compare deployed configuration and the configuration selected for rollback
- Rollback support for
 - HA/Cluster
 - Bulk rollback of multiple devices
- Ability to add custom deploy notes as part of every deployment
- Deployment history with search bar



Device Configuration Rollback - Workflow



Unified Event Viewer



Unified Event Viewer with the following new capabilities

- Unified view
 - Connection, File, Malware, and Intrusion events are in a single page
- Simplified searching
 - Search bar on top of page rather than a completely different page
- Real time mode
 - Automatically loads new events into the view
- View full event details inline
- Updated UX/UI
- Supports querying events stored locally as well as remotely (using Cisco Security Analytics and Logging On Prem)

7.0 Walkthrough



Modify event filters

Shrink/Expand the time window
...or use real-time view

2020-12-15 13:38:35 - 2020-12-15 14:38:35 / 1h Real-time

Fixed Time Range Sliding Time Range

Start time: 2020-12-15 End time: 2020-12-15

Select last: 1 hour, 6 hours, 1 day, 2 weeks, 1 month

< December 2020 >

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5		
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

1h selected

CISCO

Firepower Management Center
Overview / Dashboards / Dashboard

Overview Analysis Policies Devices

Context Explorer

Unified Events

Summary Dashboard (switch_dashboard)

Event Type Connection × × Source IP 128.2.10.163. × 10.1.1.1/8 × × Destination IP 72.163.4.161 × ×

Search

Show/Hide specific event columns

Search column

Select all

First Packet Second

Last Packet Second

Event Type

Initiator IP

Initiator Country Code

Expand rows to view all details of specific events

2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
Source IP:	fe80::25ff:ff8bc9:3f18	
Initiator User:	Not Found	
Destination IP:	f02::16	
Ingress Security Zone:	SZ_In	
Egress Security Zone:	SZ_Out	
Source Port / ICMP Type:	143 (Multicast Listener Discovery v2 reports - RFC 3...	
Destination Port / ICMP Code:	0 / ipv6-icmp	
Application Protocol:	ICMP for IPv6	
Application Protocol Category:	network protocols/services	
Client Application:	ICMP for IPv6 client	
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow
2020-12-16 10:28:17	<input type="checkbox"/> Connection	<input checked="" type="checkbox"/> Allow



Unified Events

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

Deploy Refresh admin ▾

Showing all 9,404 events (🕒 9,300 🛡 6 🔍 98) 2021-10-27 03:01:44 EDT → 2021-10-27 04:01:44 EDT 1h Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy	
2021-10-27 04:01:33	Connection	Allow		192.168.19.234	23.67.242.10	50388 / tcp	80 (http) / tcp	WIX	Allow Outbound	TG Access Control Policy	
Event Type: Connection				Client Application Category: web browser				Network Analysis Policy: Balanced Security and Connectivity			
Time: 2021-10-27 04:01:33				Client Application Tag: encrypts communications, recent vulnerabilities, SSL pr...				Prefilter Policy: Default Prefilter Policy			
Last Packet: 2021-10-27 04:01:33				Web Application: WIX				Domain: Global			
Action: Allow				Web Application Category: web services provider				Device: NGFW/TG			
Source IP: 192.168.19.234				Web Application Tag: encrypts communications				Ingress Interface: inside			
Destination IP: 23.67.242.10				Application Risk: Medium				Egress Interface: outside			
Destination Continent: North America				Business Relevance: Very Low				Ingress Virtual Router: Global			
Destination Country: USA				URL: http://static.wix.com/client/js/facebook.js?cacheKiller=v...				Egress Virtual Router: Global			
Ingress Security Zone: InZone				URL Category: Web Hosting				Initiator Packets: 6			
Egress Security Zone: OutZone				URL Reputation: Favorable				Responder Packets: 4			
> 2021-10-27 04:01:33	Connection	Allow		192.168.19.234	23.67.242.10	50387 / tcp	80 (http) / tcp	WIX	Allow Outbound	TG Access Control Policy	
> 2021-10-27 04:01:33	Connection	Allow		192.168.19.234	23.67.242.10	50386 / tcp	80 (http) / tcp	WIX	Allow Outbound	TG Access Control Policy	
> 2021-10-27 04:01:33	Connection	Allow		192.168.19.234	23.67.242.10	50385 / tcp	80 (http) / tcp	WIX	Allow Outbound	TG Access Control Policy	



Network Discovery Policy

Network Discovery Policy



Network Discovery policy allows you to:

- Collects metadata on network assets
- Monitors network segments and ports

Discovery data is most valuable when:

- Intrusion policy can leverage them
- Build a network map of your network
- FMC can correlate the data to identify the most vulnerable hosts



Best Practice: Do Not Use the Default Rule

Firepower Management Center Overview Analysis Policies **Policies** Devices Objects AMP Intelligence Deploy ⓘ² ⚙️ ⓘ admin ▾

Custom Operating Systems | Custom Topology
Snort3 is not supported Up to date on all targeted devices.

+ Add Rule

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action	
0.0.0.0/0 ::/0	any	none	none	Discover: Hosts, Users, Applications	

Best Practice: Discover YOUR Internal Network Only



Edit Rule

Discover

Hosts Users Applications

Networks Zones Port Exclusions

Available Networks

IPv4-Private-All-RFC1918

any-ipv4
any-ipv6
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12

Enter network address

IPv4-Private-All-RFC1918

Enter network address



Best Practice: Use Exclusions

Exclude the following devices from discovery:

- Load balancers
- NAT devices
- Proxies

Consequences for not using exclusion:

- Create excessive events
- Trigger misleading events
- Fill the database quickly
- Exceed Licensed Hosts limit of the FMC
- Inaccurate Firepower Recommendation

A screenshot of the Firepower Management Center (FMC) interface. The title bar says 'Add Rule'. Below it is a dropdown menu set to 'Exclude'. There are three tabs: 'Networks' (selected), 'Zones', and 'Port Exclusions'. Under 'Available Networks', there is a search bar and a list of network types: IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16, IPv6-IPv4-Mapped, IPv6-Link-Local, IPv6-Private-Unique-Local-Addresses, and IPv6-to-IPv4-Relay-Anycast. The entry 'Load_Balancers' is highlighted with a blue selection bar. To the right, under 'Networks', 'Load_Balancers' is listed in a table with a delete icon. At the bottom, there is an 'Enter network address' input field and an 'Add' button.

FlexConfig



FlexConfig

- To configure ASA features that cannot be configured from FMC
- Provides a work-around to configure features not exposed directly by FMC
- Examples
 - Policy Based Routing (PBR)
 - EIGRP
 - Ethertype ACLs
 - Application Layer Gateways (ALGs)
 - Virtual Extensible LAN (VxLAN)
 - Web Cache Communication Protocol (WCCP)
 - Platform sysopt commands



FlexConfig Objects

- To view ASA current ASA version running on FTD
 - **Show version system:** look for ASA software version number
 - **Show running-config**
 - **Show running-config all**
- System > Health > Monitor
 - Click on device targeted by FlexConfig policy
 - Choose **Advance Troubleshooting**
 - Choose **Threat Defense CLI**
 - Choose **show version**
 - Click **Execute**



FlexConfig Objects

- Sample FlexConfig Objects
 - DNS_Configure dnsNameServerList, dnsParameters
 - Default_Inspection_Protocol_Disable disableInspectProtocolList
 - Default_Inspection_Protocol_Enable enableInspectProtocolList
 - Eigrp_Interface_Configure eigrpIntList,eigrpAS, eigrpDisableSplitHorizon
 - ISIS_Configure isISNet, isISAddressFamily, isISType
- Sample Predefined Text Objects
 - dnsNameServerList DNS_Configure
 - dnsParameters DNS_Configure
 - eigrpDisableSplitHorizon Eigrp_Interface_Configure
 - netflow_Destination Netflow_Add_Destination

NAT and Routing



NAT

- Auto NAT
 - Rule becomes a parameter for the network object
 - IP address serves as the original (real) address
- Manual NAT
 - Identify a network object or group for both the real and mapped address
 - Is more scalable than Auto NAT
- NAT rules stored in single table with 3 sections
 - Section 1 Manual NAT
 - First Match Basis order they appear in configuration
 - Section 2 Auto NAT
 - If match not found Section 1
 - Static rules
 - Dynamic rules
 - Section 3 Manual NAT
 - Rules applied on a first match basis in the order they appear in the configuration

NAT



- NAT is supported in routed and transparent firewall mode
- Bridge Virtual Interface (BVI)
 - Must specify the member interface cannot configure NAT for bridge group interface
 - Must specify real and mapped addresses
 - Cannot configure PAT when mapped address is a bridge group member
 - No translation between IPv4 and IPv6 networks when source and destination interfaces are members of the same bridge group



NAT and Routing

- Firewall Threat Defense device receives traffic for a mapped address then the FTD device un-translates the destination address according to the NAT rule.
 - BVI Transparent mode
 - FTD determines the egress interface for the real address by using the NAT rule; you must specify the source and destination bridge group member interfaces as part of the NAT rule
 - Regular interfaces Routed mode
 - FTD determines the egress interface
 - FTD devices uses the NAT rule to determine the egress interface
 - FTD if you do not configure the interface NAT rule then the FTD uses route lookup to determine the egress interface

Prefilter Packet Processing



Prefilter

- Prefilter and access control policies both allow you to block and trust traffic, though the prefiltering "trust" functionality is called "fastpathing" because it skips more inspection.
- Bypass capability Fastpath rule action
 - Fastpathing traffic in the prefilter stage bypasses all further inspection and handling, including:
 - Security Intelligence
 - authentication requirements imposed by an identity policy
 - SSL decryption
 - access control rules
 - deep inspection of packet payloads
 - Discovery
 - rate limiting

Best Practice: Use Prefilter Rule to Bypass Inspection



For highly trusted traffic, prefer a *Fastpath* action over a *Trust* action

Add Prefilter Rule

Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: Prefilter Rule, Enabled: Insert: below rule, 0

Action: Fastpath

Interface Objects (selected), Networks, VLAN Tags, Ports

Add Rule

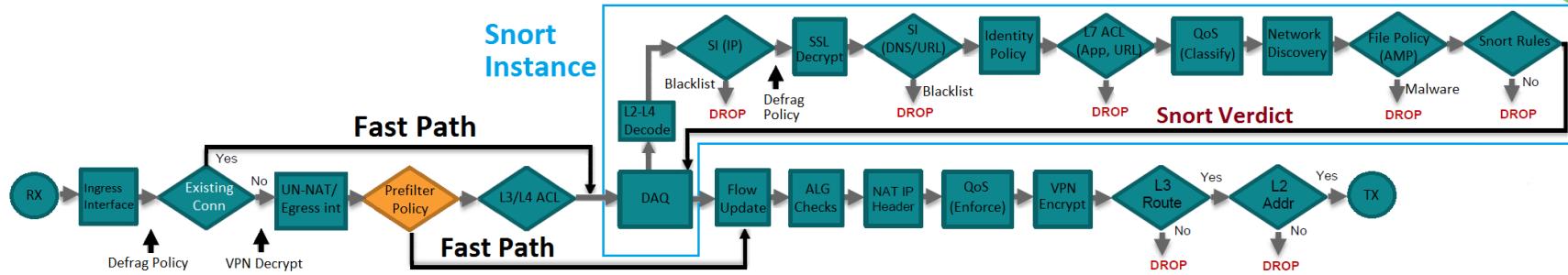
Name: AC Rule, Enabled: Insert: into Mandatory

Action: Trust

Icons: shield, file, lock, user, application, port

Zones (selected), Networks, VLAN Tags, Users, Applications, Ports, URLs, SGT/ISE Attributes

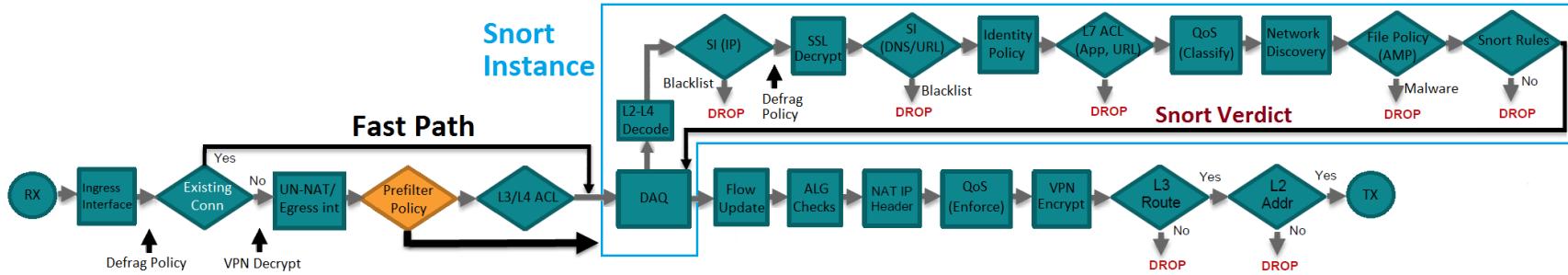
FTD Packet Processing: Prefilter Policy



- Prefilter Policy got introduced in 6.1 version
- Serves 2 main purposes
 1. Adds additional flexibility when it comes to handling tunneled traffic:
 - GRE
 - IP-in-IP
 - IPv6-in-IP
 - Teredo Port 3544
 2. Provides Early Access Control (EAC) which allows a flow to bypass completely the Snort engine

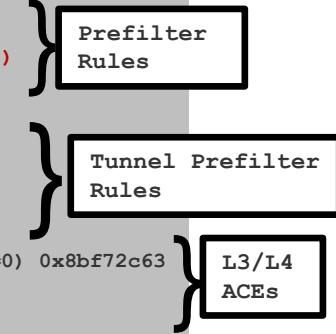


FTD Packet Processing: Prefilter Policy



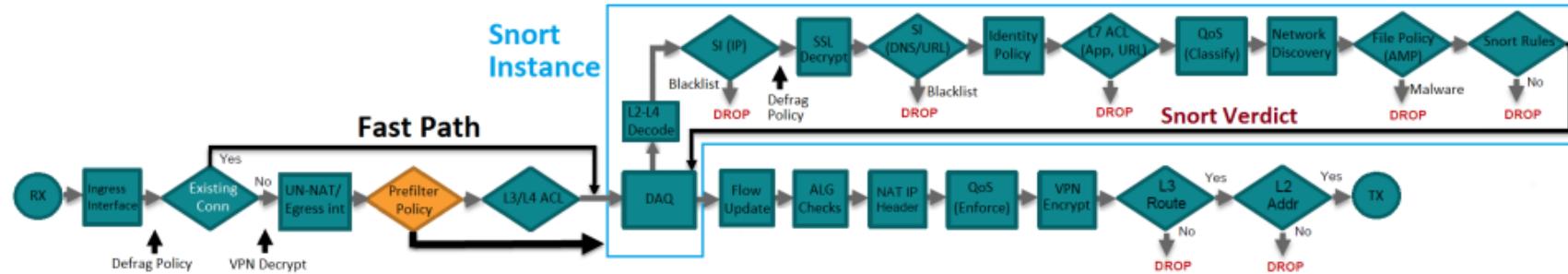
Prefilter Rules are deployed to LINA as L3/L4 ACEs and are placed **above** the normal L3/L4 ACEs

```
firepower# show access-list
access-list CSM_FW_ACL line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL line 10 remark rule-id 268434445: ACCESS POLICY: NGFW1 - Mandatory/1
access-list CSM_FW_ACL line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xa1d3780e
```



..|.|.|.|. Prefilter vs ACP rules = **first match** is applied
CISCO

FTD Packet Processing: Prefilter Policy (tunneled)

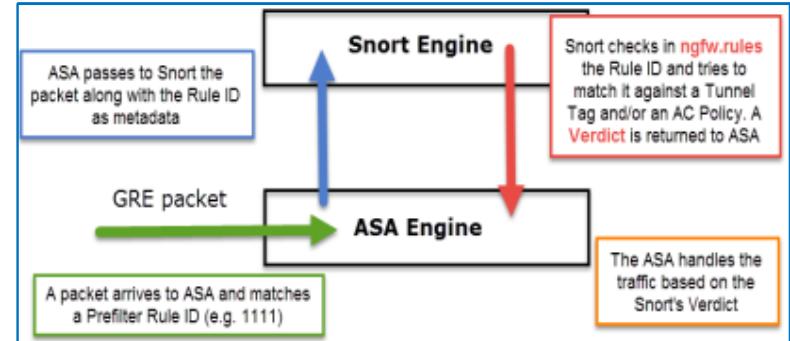


- How works the **analyze** action:

```
firepower# show access-list
access-list CSM_FW_ACL_ line 5 remark rule-id 268435473: RULE: Tunnel_Rule1
access-list CSM_FW_ACL_ line 6 advanced permit gre any any rule-id 268435473
```

```
root@NGFW1:/var/sf/detection_engine/001d# cat ngfw.rules
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used ..
268435473 allow any any any any any any 47 (tunnel 2)
268434456 allow any any any any any any 41 (tunnel -1)
268434456 allow any any any any any any 41 (tunnel -1)
# End of tunnel and priority rules.

# Start of AC rule.
268435474 allow 2 any any any any any
268435468 allow any any any any any any (log dcforward) #
End of AC rule.
```



File and Malware Policy



Malware & File Policy Overview

- Controls what and how files are allowed, blocked and inspected
- Inspection includes:
 - static analysis of the file (via Spero)
 - dynamic analysis (via AMP Threat Grid)
 - local analysis (via ClamAV)
- Complex policies can include different actions and levels of inspections for different application protocols, directions and file types.



Malware & File Policy Actions

Simple policy applies the same action (e.g. Block Malware) to all files.
Actions are:

- **Detect Files** – Detect and log the file transfer, perform no inspection
- **Block Files** – Block and log the file transfer, perform no inspection
- **Malware Cloud Lookup** – Inspect the file to determine disposition (Malware, Unknown or Clean) and log
- **Block Malware** – Inspect the file to determine disposition, log and block if Malware



Application Protocols for Detection

Add Rule

Application Protocol

-
-
-
-
-
-
-
-

Action

Detect Files

Store files

File Types

Search name and description

- 7Z (7-Zip compressed file)
- 9XHIVE (Windows 9x registry...)
- ACCDB (Microsoft Access 20...)
- AMF (Advanced Module For...)
- AMR (Adaptive Multi-Rate Co...)
- ARJ (Compressed archive file)

Add

Selected File Categories and Types

Cancel Save



Malware & File Policy Best Practices

Add Rule

Application Protocol: Any | Action: Block Malware

Direction of Transfer: Download | Action: Block Malware

Action Options:

- Spero Analysis for MSEXE
- Dynamic Analysis
- Capacity Handling ⓘ
- Local Malware Analysis
- Reset Connection

Store Files:

- Malware
- Unknown
- Clean
- Custom

File Type Categories:

Category	Count
Office Documents	15
Archive	17
Multimedia	2
Executables	9
PDF files	1
Encoded	0
Graphics	0

File Types:

- NEW_OFFICE (Microsoft Offic...)
- OLD_TAR (Pre-POSIX Tape A...)
- PDF (PDF file)
- POSIX_TAR (POSIX Tape Arc...)
- PST (Microsoft Outlook Perso...)
- RAR (WinRAR compressed ar...

Selected File Categories and Types:

- MSEXE (Windows/DOS exec...)
- PDF (PDF file)

Buttons: Cancel, Save

Don't store clean files

Select the file types that are important



Malware & File Policy Enablement

Add Rule

Name: AC Rule Insert: below rule, 1

Action: Allow

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Intrusion Policy: Balanced Security and Connectiv Variable Set: Default Set

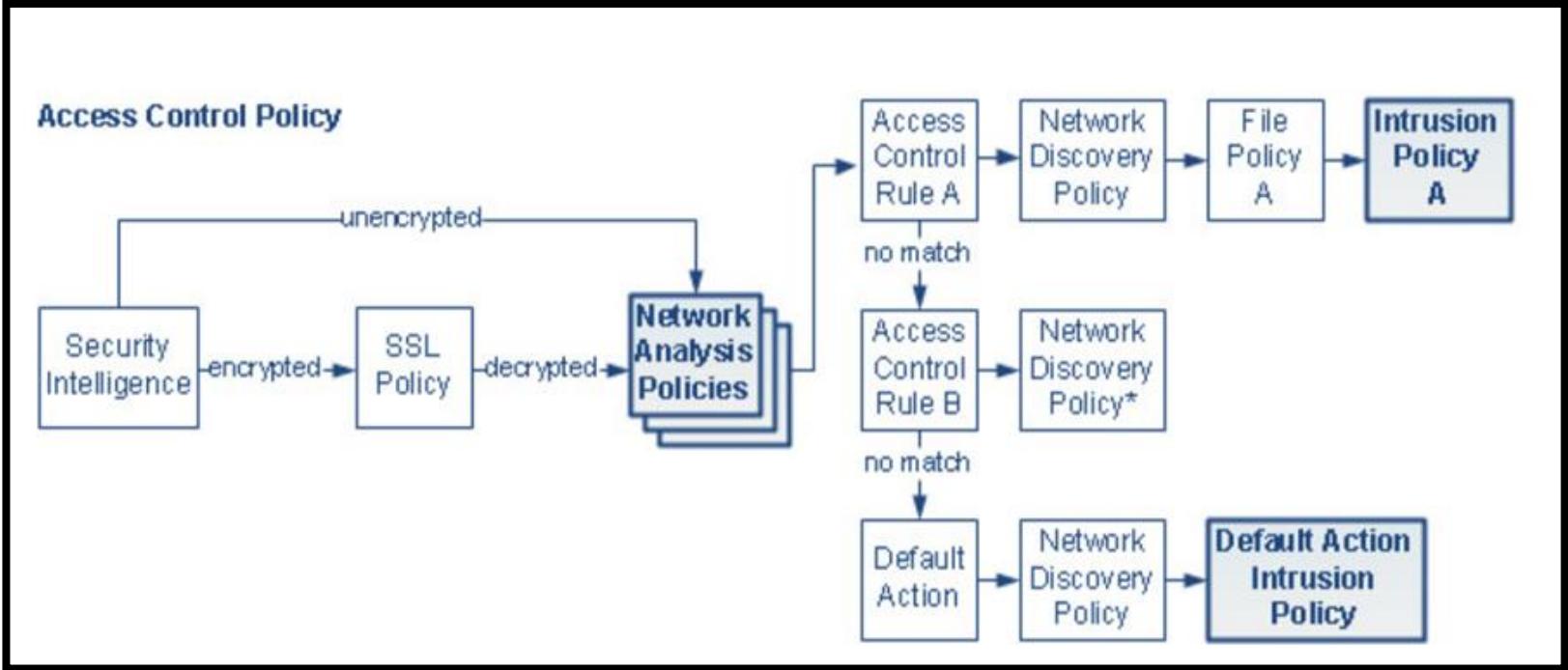
File: File Policy (selected), None, File Policy

Must select the desired file policy in the access rule

Cancel Add

NAP and Intrusion Policy

Network Analysis Policies NAP





Network Analysis Policies NAP

- NAP control traffic preprocessing
- Occurs after SI drops and SSL decryption
 - But before access control and intrusion or file inspection
- Default Balanced Security and Connectivity
 - The system will apply different NAP's based on which intrusion policies you select in access control rules
- NAP do not have the same traffic matching criteria that are available in access control rules, so you can get mismatched policies



NAP cont'd

- NAP rules based on Security Zone and Network specifications **only**
 - For each access control rule that include intrusion policy:
 - System creates a NAP rule that applies the same-named NAP to same Source/destination security zone and network
 - Ports, URL, user, and application criteria are ignored
- Different intrusion policies based on L4-7 criteria have no impact on NAP

NAP Policy Rule Selection Example



- Access rule 1
 - Action: Allow
 - Source zone: Inside_Zone
 - Source network: any
 - Destination zone: Outside_Zone
 - Destination network: any
 - **Intrusion policy: Security over Connectivity**
- Access rule 2
 - Action: Allow
 - Source zone: Inside_Zone
 - Source network: any
 - Destination zone: Outside_Zone
 - Destination network: any
 - **Intrusion policy: Balanced Security and Connectivity**
- Two NAP rules will be created but because both NAP rules have the same match criteria system will apply the **Security over Connectivity** to traffic matching Access rule 1 or 2



Intrusion Policy

- Intrusion Policy uses intrusion and preprocessor rules (collectively known as intrusion rules) to examine the **decoded** packets for attacks based on patterns.
 - Rules can:
 - Prevent (drop) threatening traffic and generate an event
 - Detect (alert) threatening traffic and generate an event only
 - Intrusion rules subdivided into shared object and standard text rules
 - Preprocessor rules are associated with preprocessors and packet decoder detection options in the network analysis policy (NAP)

Intrusion Rule Attributes



- Intrusion rule Attributes:
- Signature Description- The description is the actual code used by the Snort inspection engine to match traffic against the rule
- GID- This number indicates which system component evaluates the rule and generate results
 - 1 indicates a standard text intrusion rule
 - 3 indicates a shared object intrusion rule
 - SNORT 3 supports some but not all shared object intrusion rules
- SID- Snort Identifier lower than 1,000,000 were created by Talos
- Action- Alert, Drop, Disabled
- Status- Overridden
- Message- The name of the rule which also appears in events triggered by the rule.



Intrusion Rule Attribute cont'd Snort 2

Filter:

Category:"protocol-ftp"

0 selected rules of 112

Rule State ▾ Event Filtering ▾ Dynamic State ▾ Alerting ▾ Comments ▾ Layer: My Changes

GID	SID ↑	Message
1	144	PROTOCOL-FTP ADMw0rm ftp login attempt

[Hide details](#) [Above](#) [Below](#)

Dynamic Details ▾

> Alerts (0)

> Comments (0)

Documentation

rule alert tcp \$EXTERNAL_NET any -> \$HOME_NET 21 (msg:"PROTOCOL-FTP CWD ~root attempt"; flowto_server,established; content:"CWD"; nocase;; content:"~root"; distance:1; nocase;; pcre:"/^CWD\s+~root/smi"; metadata:ruleset community, service ftp; reference:cve,1999-0082; classtype:bad-unknown; sid:336; rev:17; gid:1;)

References

[Rule Documentation](#)

[CVE: 1999-0082](#)

SRU

[Snort Rule Update 2020 08 18 001 vrt](#)

[Isp rel 20210503 2107](#)

1 of 3 < >

Add SNMP Alert

Add



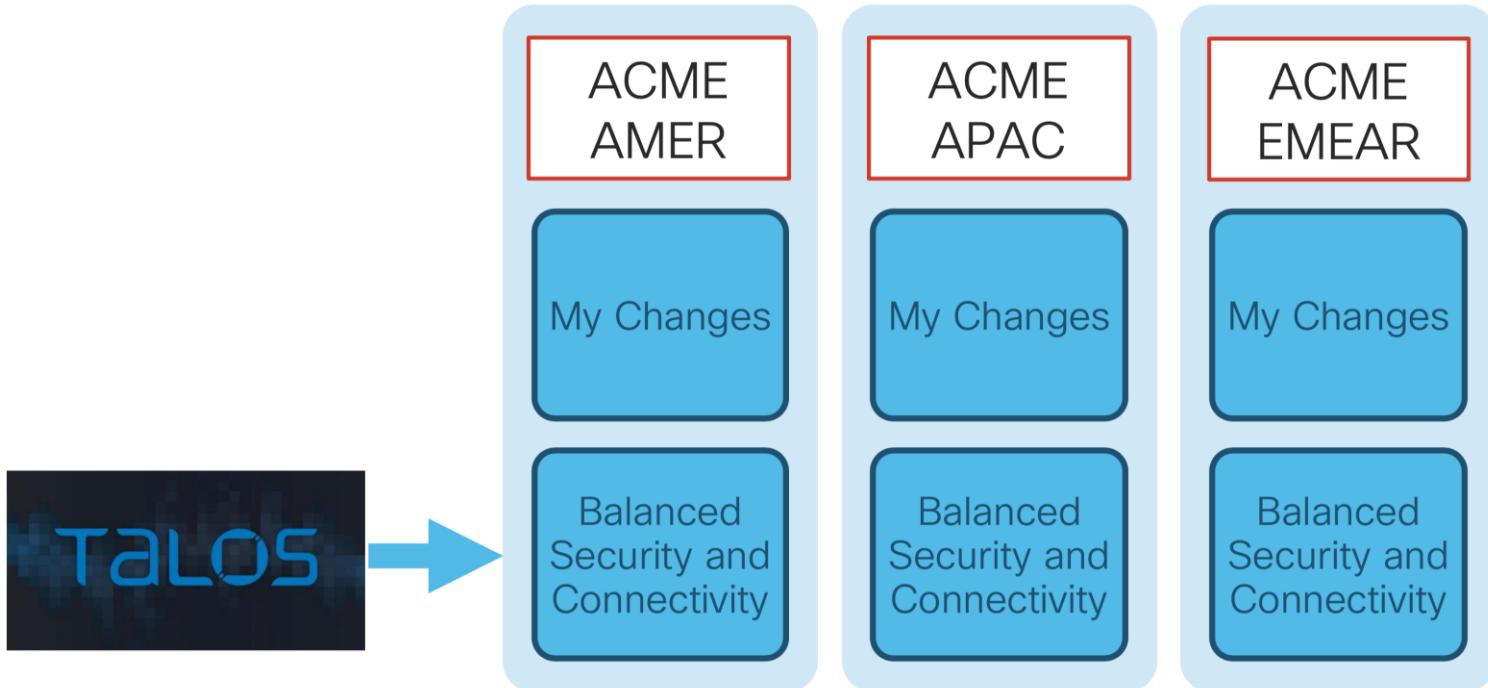
Inheritance

- Every user-created policy depends on another policy as its “Base”
- All policies trace their roots back to a TALOS base policy
 - Connectivity Over Security
 - **Balanced Security and Connectivity**
 - Security Over Connectivity
 - No Rules Active (*For troubleshooting*)
 - Maximum Detection (*For testing only*)



Typical Flat Design

Three Regions, Three Different Policies





Intrusion Policy Viewed from FMC

Firepower Management Center Overview Analysis Policies **Policies** Devices Objects AMP Intelligence Deploy ! ? admin ▾

Policy Information
Rules
Firepower Recommendations
Advanced Settings
Policy Layers
My Changes
Balanced Security and Conn

Policy Layers

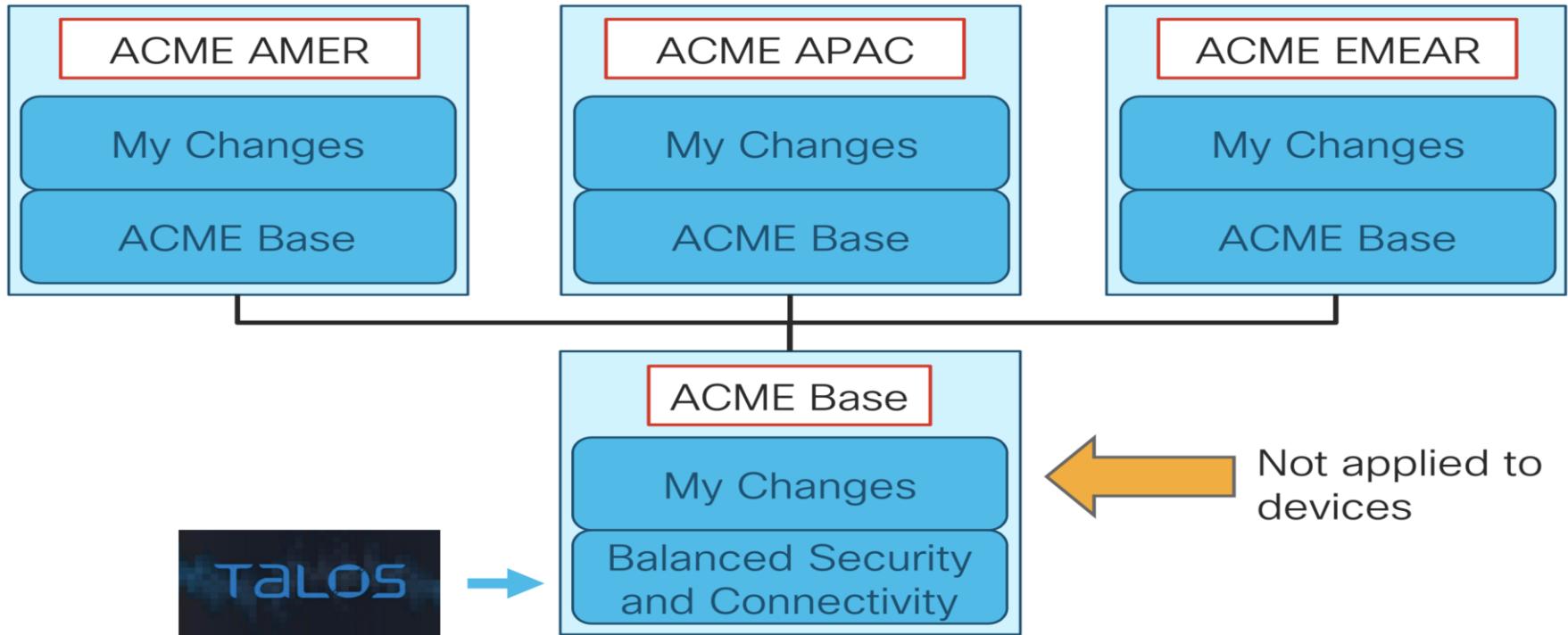
< Back

Policy Summary	Rules (11023)	0 10929 rules drop and generate events → 94 rules generate events	Global Rule Thresholding
	Enabled Advanced Settings		
User Layers	+ Add Shared Layer + Add Layer		
My Changes	Rules (0)	0 0 rules drop and generate events → 0 rules generate events	→ 0 rules disabled
	Advanced Settings		
Built-in Layers			
Balanced Security and Connectivity	Rules (11023)	0 10929 rules drop and generate events → 94 rules generate events	
	Advanced Settings	Global Rule Thresholding, SNMP Alerting, Sensitive Data, Syslog Alerting	





Hierarchical Design



Performance Impact on Different Base Policy



Base Policy

Security Over Connectivity ▾

✓ The base policy is up to date (Rule Update 2019-08-12-001-vrt)

This policy has 16278 enabled rules

→ 123 rules generate events

✗ 16155 rules drop and generate events

Base Policy

Balanced Security and Connect ▾

✓ The base policy is up to date (Rule Update 2019-08-12-001-vrt)

This policy has 11023 enabled rules

→ 94 rules generate events

✗ 10929 rules drop and generate events

Base Policy

Connectivity Over Security ▾

✓ The base policy is up to date (Rule Update 2019-08-12-001-vrt)

This policy has 509 enabled rules

→ 10 rules generate events

✗ 499 rules drop and generate events

Default Variable Set

Edit Variable Set Default-Set

Name:

Default-Set

Description:

This Variable Set is system-provid

Add

Variable Name	Type	Value	
---------------	------	-------	--

Customized Variables

This category is empty

Default Variables

DNS_SERVERS	Network	HOME_NET	/C
EXTERNAL_NET	Network	any	/C
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	/C
FTP_PORTS	Port	[21, 2100, 3535]	/C
GTP_PORTS	Port	[3386, 2123, 2152]	/C
HOME_NET	Network	any	/C

Cancel

Save

Importance of Variables for IPS



- Contains Snort variables
- Increases inspection efficiency, reduces false positives
- Can impact detection if not configured, potential to blind IPS
- Find it under *Objects > Variable Set*

A screenshot of the Cisco Firepower Management Center web interface. The top navigation bar includes tabs for Analysis, Policies, Devices, Objects (which is highlighted with a blue underline), AMP, Intelligence, Deploy, and user authentication. Below the navigation is a search bar labeled "Variable Set" and a "Filter" button. A descriptive text block explains that variables represent values used in intrusion rules to identify source and destination IP addresses and ports. It also mentions their use in policies for rule suppressions, adaptive profile updates, and dynamic rule states. A table displays a single entry: "Default-Set" in the Name column and "This Variable Set is system-provided." in the Description column. To the right of the table are edit and delete icons.

Name	Description
Default-Set	This Variable Set is system-provided.

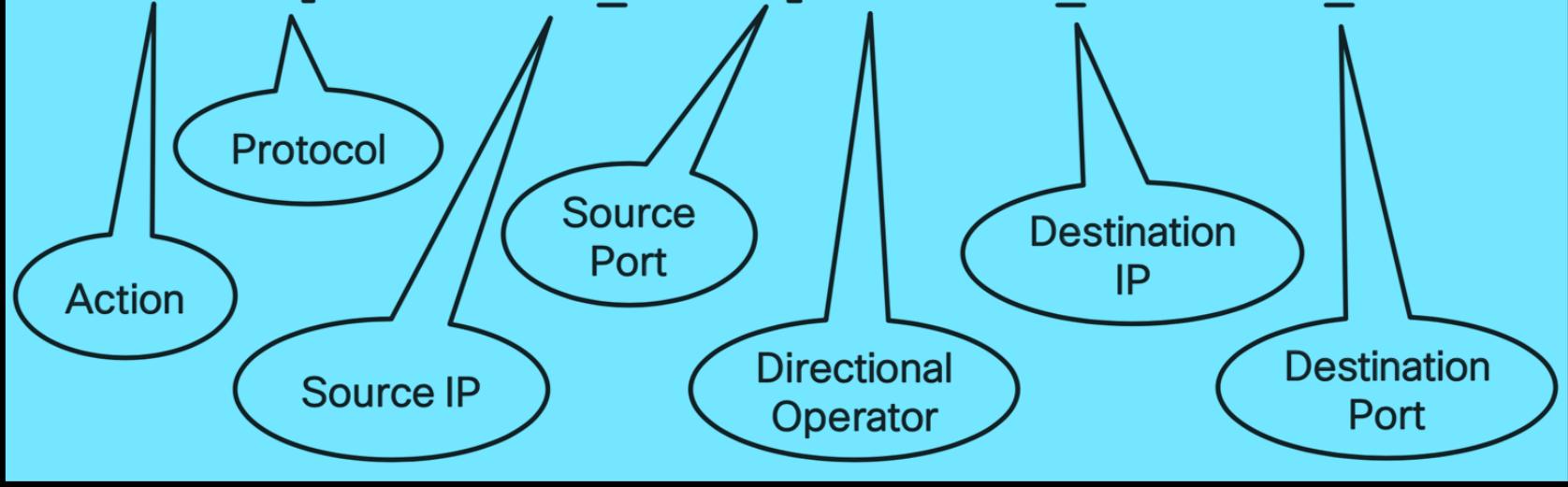


Variable Set Use Case Scenarios

- **North/South Traffic Only**
 - Define \$HOME_NET
 - \$EXTERNAL_NET = !\$HOME_NET is ok
- **Just East/West Traffic (or Combination of Both)**
 - Define \$HOME_NET
 - \$EXTERNAL_NET = default “any”

Variable Sets within a Snort Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
```



- \$HOME_NET = Protected network
- \$EXTERNAL_NET = Potential attack sources



Variable Set

Filter:

Category:"protocol-ftp"



1 selected rule of 112

Rule State ▾ Event Filtering ▾ Dynamic State ▾ Alerting ▾ Comments ▾

Policy

<input type="checkbox"/>	GID	SID	Message	→					
--------------------------	-----	-----	---------	---	--	--	--	--	--

[Hide details](#)

◀ ▶ 1 of 3 ▷ ▸

Add

Comments (0)

Documentation

rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"PROTOCOL-FTP CWD ~root attempt"; flow:to_server,established; content:"CWD"; nocase;; content:"~root"; distance:1; nocase;; pcre:"/^CWD\$\s+~root\$/smi"; metadata:ruleset community, service ftp; reference:cve,1999-0082; classtype:bad-unknown; sid:336; rev:17; gid:1; )
```

References

- [Rule Documentation](#)
- [CVE: 1999-0082](#)

SRU

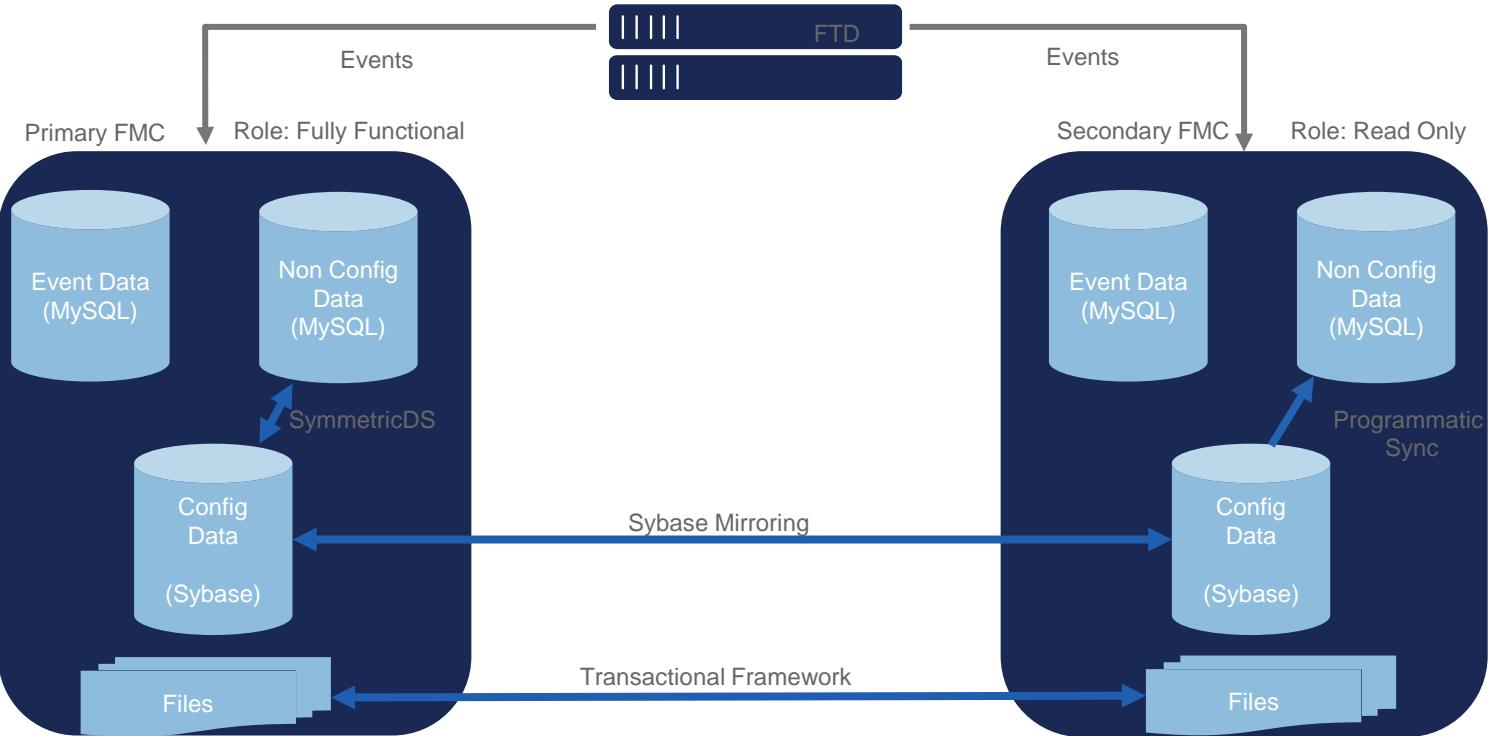
- [Snort Rule Update 2018 08 23 001 vrt](#)



High Availability and Resiliency



FMC High Availability





FMC HA Requirements

Hardware Requirements

- FMC devices should be of same hardware model
- Backup from primary FMC should not be restored to secondary
- There must be at least 5Mbps bandwidth between the two FMC

Software Requirements

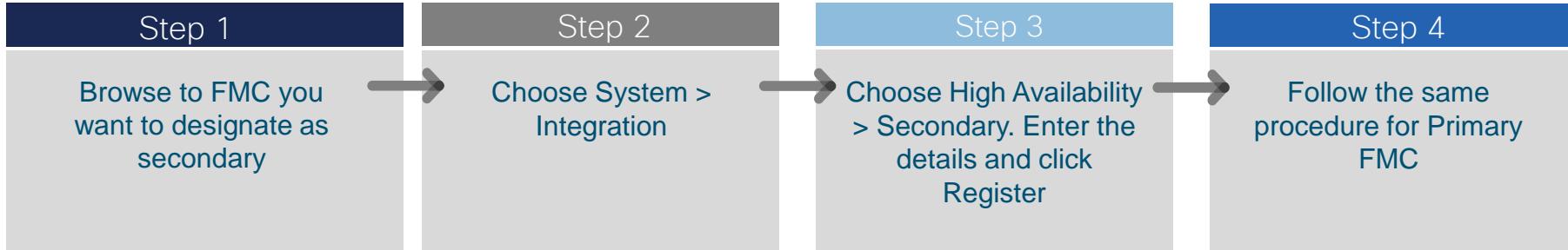
- The two FMC in HA must have same major (first number), minor (second number), and maintenance (third number) software version.
- Both should have same version of intrusion rule update and vdb update installed.

License Requirements

- No license is required to establish HA



FMC HA Configuration



In order to verify the status of HA, Use either of the two options the

- Browse to System > Integration > High Availability to check the status
- SSH to Primary/Secondary FMC and elevate to root and execute `/Volume/home/admin# manage_HADC.pl`

Important Troubleshoot files

- **`/var/log/action_queue.log`:** Establish HA, Switch Roles and Resume (Rebuild) Mirror are AQ transactions.
- **`/var/log/messages`:** Processes like vmsDbEngine start and stop failures are available in this log file.
- **`/var/opt/symmetric/logs/symmetric.log`:** This log file helps us debugging any issue with SymmetricDS.
- **`/var/log/syncd.log`:** Any issues related to periodic sync is shown here.
- **`/var/log/mojo.log` and `/var/log/mojo/mojo.log`:** To track UI logs for HA operations.



FTD High Availability

FTD HA is build upon stateful failover capabilities of ASA and supports Active/Standby configuration and appliances assume the role of

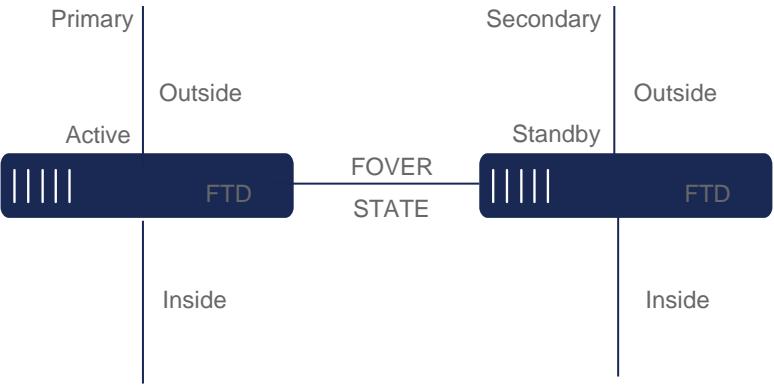
- Primary Firewall – Active unit in the HA Pair
- Secondary Firewall – Standby unit in the HA Pair

FTD HA can be configured for both FMC and FDM managed firewall pairs.

HA is supported in both routed and transparent mode of firewall operation

Following features support stateful failover

- NAT translation table
- TCP/UDP connection replication
- SNORT connection state
- SNORT inspection for pinhole information
- Strict TCP enforcement so that mid-flow session are permitted
- ARP Table
- L2 Bridging table
- Routing: Static routes, RIP, OSPF, OSPV3, BGP IPv4 and IPv6
- NGFW Features URL, Geo Location, URL DB, Passive Identity
- IP Reputation based Security Intelligence





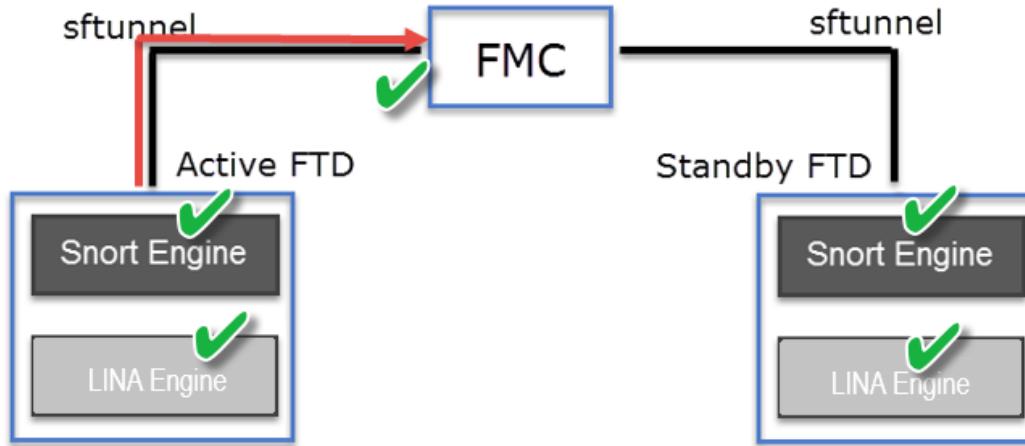
HA Requirements

To build an HA pair between 2 FTD devices the following requirements should be met:

- Same model
- Same version (FXOS and FTD)
- Same number and type of interfaces
- Both devices are in the same group/domain in FMC
- Identical NTP configuration
- No uncommitted changes on FMC
- The same FTD mode: routed or transparent
- No DHCP/PPPoE configured on any of interfaces
- Different hostname (FQDN) for both chassis:



Policy Deployment in HA (Prior to 6.6)



1. Start Deployment request initiated from FMC comes to Active FTD
2. **Snort-side configuration** is applied on Active FTD
3. LINA process on Active unit will send snort-side config to Standby node
4. **Lina configuration** applied on Active unit
5. LINA process on Active unit takes care of syncing lina configurations to Standby node
6. Deployment Status with SUCCESS or FAILURE is sent back to FMC with all the information



FMC: Policy deployment improvements

Parallel
Policy apply
for HA

Parallel
Policy for
Cluster

Delta Apply
for Pre-filter
Rules

- 30-40% reduction in deployment time
- Deployment time reduced drastically *for cluster with more than two nodes having large configuration*
- ~20-30% Reduction in deployment time for configurations with large pre-filter rules



High Availability Actions

The screenshot shows a network management interface with a tree view on the left. Under the "HA Test" node, there is a "High Availability" section. It lists two nodes:

Node	Type	Software Version	Policy
NGFW1(Primary, Standby) 198.19.10.81 - Routed	FTDv for VMware	7.0.0	N/A
NGFW3(Secondary, Active) 198.19.10.83 - Routed	FTDv for VMware	7.0.0	N/A

A context menu is open over the NGFW3 row. The menu items are: Switch Active Peer, Break, Force refresh node status, and Delete. The "Break" option is highlighted with a red arrow pointing to it from the top right.

1. Switching Failover Roles
2. Breaking the HA pair
3. Disabling the HA pair



FTD HA Quick Tips

Create HA

- No Pending deployment on FMC
- Devices should be connected either directly or using a switch in between them
- Turn On monitoring for interfaces
- Configure failover MAC along with Standby IP
- Configure the failover timers as needed if not an expert do not change the defaults

Switch Active/Standby Firewalls Manually

- No deployment should be in progress
- Switch Operation is triggered only on Active unit
- System icons will display the active unit and show the progress of failover

Break HA

- Break an HA Pair when it is desired to manage the devices in the pair individually
- The former Active FTD unit will continue to keep the active IP addresses for all interfaces and continues to pass traffic. It will retain the policy assigned to the HA-pair
- The former Standby unit will also keep the policy assigned to the HA-pair. However, its interface configuration will revert back to factory defaults.
- On the former Standby, only physical interfaces will be retained and all interfaces except the management interface will be shutdown. All other configuration on the physical interfaces will be lost



FTD HA Requirements

Licensing

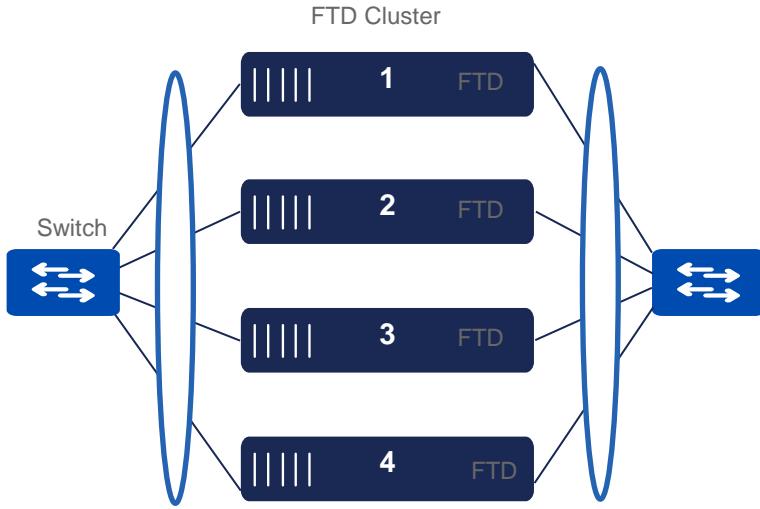
- All Licenses held by the FTD selected as the primary are retained by the primary.
- All Licenses held by the FTD selected as the secondary are released by the secondary and all licenses held by the primary are requested for the secondary FTD.
- From an FMC stand point, when forming an FTD HA pair, 2 standalone licenses are consumed under the hood.



FTD Clustering

Clustering allows multiple firewalls to be clustered into a single unit in order to provide Active/Active Load balancing between them and is supported on following FMC managed platforms only

- 41xx
- 9300 with SM xx
- 6 SMs (2 chassis)as of FTD v6.5





FTD Clustering

Intra-chassis cluster

This is used for a 9300 cluster where cluster is formed within the 3 security modules of a Chassis. Here a cluster port-channel should be present in cluster logical device but it must not have any member interface.

Inter-chassis cluster

This is used when cluster is formed either between 2 or more 9300s or 2 or more 4100. Here, the cluster port-channel must be present in the logical device and it must have a member interface assigned. On both the chassis, same member interface must be assigned.

Inter-site cluster

This is used when cluster members are spread across different sites. Each cluster member can have a different Site-ID assigned from Chassis manager.



FTD Clustering

- Up to 6 identical Firewall appliances/SMs combine in one traffic processing system
- Preserve the benefits of failover
 - Virtual IP and MAC addresses for first-hop redundancy
 - Centralized configuration mirrored to all members
 - Connection state preserved after a single member failure
- Implement true scalability in addition to high availability
 - Stateless load-balancing via Spanned EtherChannel with LACP
 - Out-of-band Cluster Control Link to compensate for external asymmetry
 - Elastic scaling of throughput and maximum concurrent connections

Multi-Instance on FTD



Full management separation



Policy management separation



Routing separation, resource separation (CPU, RAM, Disk)



Traffic processing isolation



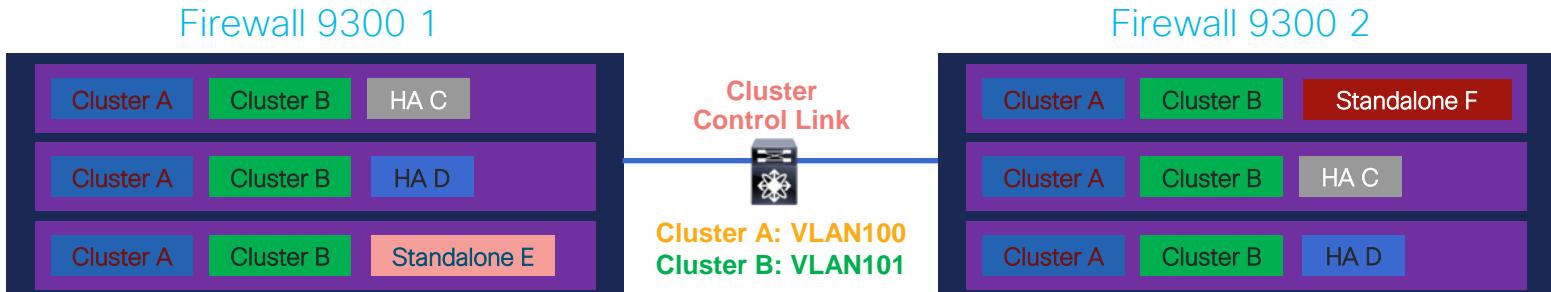
Multi-Instance cluster overview

- Multi-Instance (MI) clustering connects multiple FTD instances across multiple units to form a single firewall
- It offers linear scalability and active/active High Availability
- Maximum supported cluster size is six nodes
- There are three types of MI cluster deployments:
 - Intra-Chassis Cluster (FPR 9300 only)
 - Inter-Chassis Cluster (FPR 9300 or FPR 4100)
 - Combination of Inter-(or intra)-Chassis Clustering, HA, or Standalone FTD instances



Multi-Instance clustering

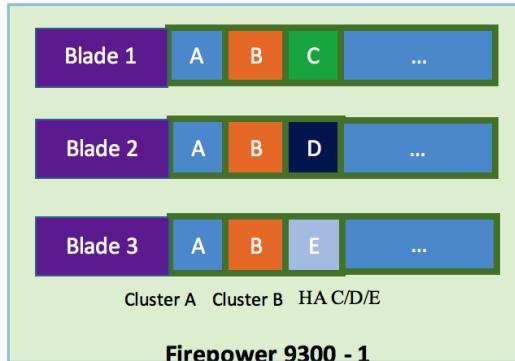
- Requires FTD 6.6 and FXOS 2.8(1):
 - Instance-level clustering with one cluster member instance per module
 - Shared CCL, but no shared data interfaces between instance clusters
 - Unused resources can be used for standalone or HA instances



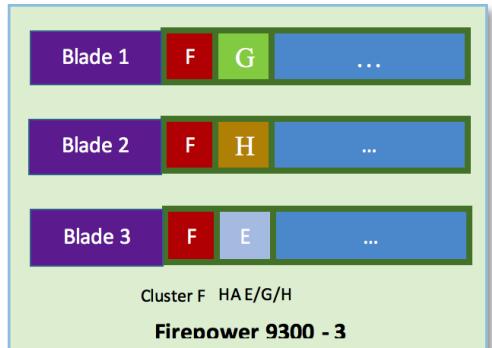
- Mixed hardware in a cluster for container instances only:
 - For example, Firewall 4120 and 4145, Firewall 9300 SM-24 and SM-44

FTD MI clustering – Deployment scenario

- MI Clustering combined with HA and standalone deployment with FP9300



Clusters: A, B, F
HA Pairs: C, D, E, G, H

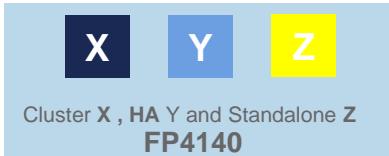




FTD MI clustering – Deployment scenario

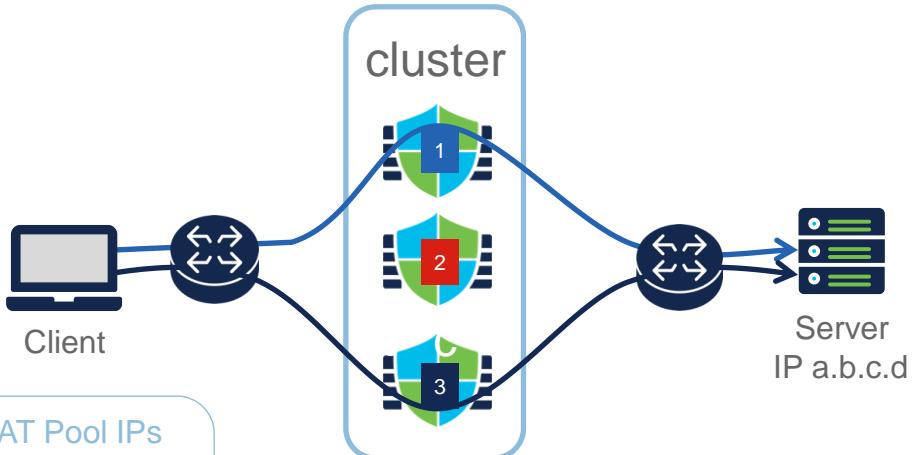
- MI clustering combined with HA and standalone deployment with FP4100

*Clusters: x
HA Pair: Y
Standalone: Z, W*



PAT Pool Improvements

- Port Address Translation is distributed in cluster
- PAT Pool IPs distributed and owned by cluster nodes
- Multiple Connections to a server from the same host can be load balanced across different nodes, each using its own PAT Pool IP for translating those connections



- This feature introduces port block based distribution of PAT Pool IPs
- Cluster members now own a port block from the same PAT address
- Multiple Connections from the same host are translated using the same IP address, even if load balanced across different members

Application Programming Interface

API on FMC

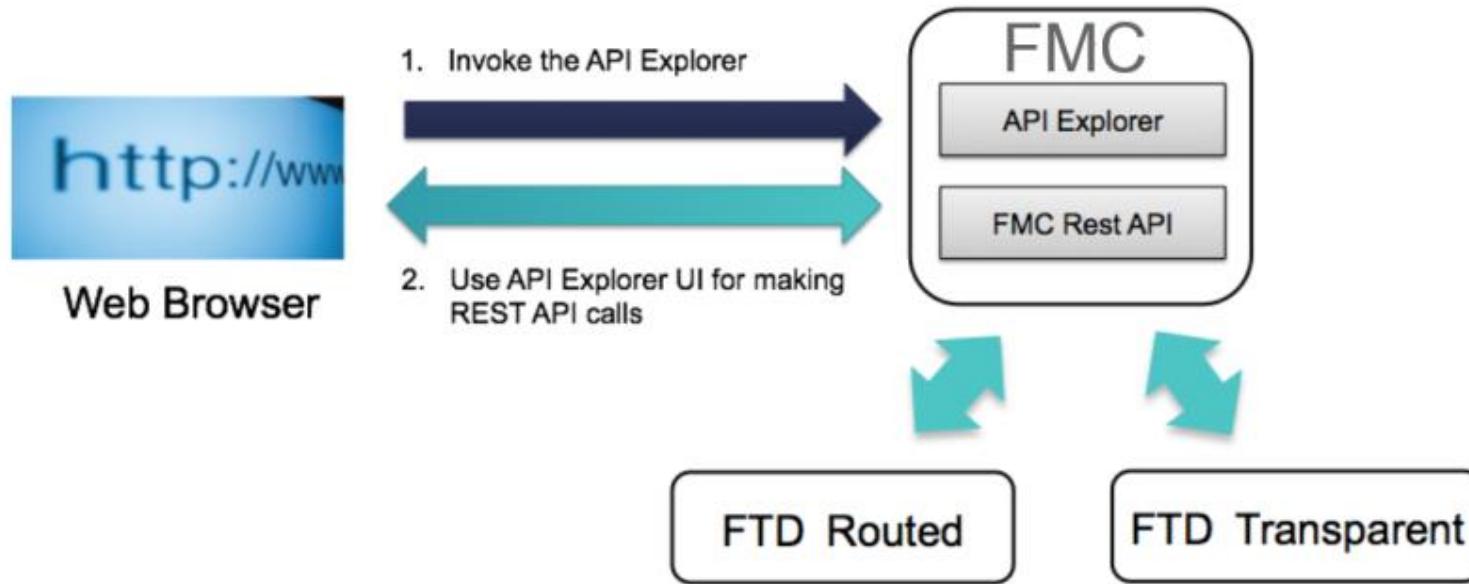


- REST API provides a lightweight interface for 3rd party applications
- FMC allows requests from application using REST API by default (can configure to block)
- Issue API calls to FMC
 - API-Explorer
 - External script (python, perl)
- Cannot “push” to FTD (yet)
- Good for regular/mass repetitive changes (PUT or POST or DELETE)
- Great for regularly retrieving JSON formatted information (GET)
- Use to update 3rd party and/or in-house external monitoring tools
- A username can only uniquely log into FMC via HTTPS once. If that username attempts to log in a 2nd time their 1st connection will be logged out.
- Creation of a special “API User” might be best to avoid HTTPS access collisions since API calls and web page calls are treated the same.



REST API: Architecture

- REST API does not communicate with FTD directly.
- REST API communicates with FMC. FMC pushes changes to FTD.





REST API v6.1 for FTD 7.0

- REST API is used to interact with the FTD through a client program.
- Starting with FTD 6.4, you can use **latest** instead of the v element in the path.
 - For example, <https://ftd.example.com/api/fdm/latest/>.
 - The **latest** alias resolves to the most recent API version supported by the device
- With 6.7, the API is backward compatible. Calls from previous versions should work without change in the v6 API
- 6.1 URL does not change from 6.0



REST API Best Practices

- Keep UI users and script users separate. Especially do not use the admin account as an API user.
- Do not give script users more privilege than needed.
- Always validate the content coming from the server.
- Validate/sanitize JSON content, as it may include embedded executable code.

API Explorer

https://<fmc IP>/api/api-explorer



Screenshot of the Cisco Firepower Management Center API Explorer interface:

The URL in the browser is <https://fmc.dcloud.local/api/api-explorer/>.

The page title is "Cisco Firepower Management Center".

The page header includes links for NGFW2 (FDM), NGFW2 (API Explorer), NGFW3 (FDM), NGFW3 (API Explorer), Splunk, and Unquarantine.

A message at the top states: "Specifies the REST URLs and methods supported in the Cisco Firepower Management Center API. Refer to the version specific [REST API Quick Start Guide](#) for additional information." It also includes links for Cisco Technical Assistance Center (TAC) - Website, Send email to Cisco Technical Assistance Center (TAC), and Cisco Firepower Management Center Licensing.

The main content area shows a list of API endpoints under the heading "Domain: Global":

- Devices >
- Policy Assignments >
- Device HA Pairs >
- Updates >
- Intelligence >
- Audit >
- Device Groups >
- Integration >
- Status >
- Device Clusters >

API Explorer (cont.)



Devices

1

POST /api/fmc_config/v1/domain/{domainUUID}/devices/copyconfigrequests

GET /api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords

2

Retrieves or modifies the device record associated with the specified ID. Registers or unregisters a device. If no ID is specified for a GET, retrieves list of all device records.

Parameters

3 Try it out

Name	Description
domainUUID * required string (path)	Domain UUID e276abec-e0f2-11e3-8169-6d9ed49b625f
offset integer (query)	Index of first item to return. offset - Index of first item to return.
limit integer (query)	Number of items to return. limit - Number of items to return.
expanded boolean (query)	If set to true, the GET response displays a list of objects with additional attributes. --

Exporting a Generic Script (Legacy Explorer)



Export operation in python language

Cut & paste below script in the appropriately typed file

To execute the script type in following in a terminal by passing in FMC username and password as parameters:

```
python script.py <username> <password>
```

```
# Generated FMC REST API sample script

import json
import sys
import requests

server = "https://172.16.100.100"

username = "admin"
if len(sys.argv) > 1:
    username = sys.argv[1]
password = "sf"
if len(sys.argv) > 2:
    password = sys.argv[2]

r = None
headers = {'Content-Type': 'application/json'}
api_auth_path = "/api/fmc_platform/v1/auth/generatetoken"
auth_url = server + api_auth_path
try:
    # 2 ways of making a REST call are provided:
    # One with "SSL verification turned off" and the other with "SSL verification turned on"
    # The one with "SSL verification turned off" is commented out. If you like to use that
    # uncomment the line where verify=False and comment the line with =verify='/path/to/ssl'
    # REST call with SSL verification turned off:
    # r = requests.post(auth_url, headers=headers, auth=requests.auth.HTTPBasicAuth(username,
    # REST call with SSL verification turned on: Download SSL certificates from your FMC fi
    r = requests.post(auth_url, headers=headers, auth=requests.auth.HTTPBasicAuth(username,
    auth_headers = r.headers
    auth_token = auth_headers.get('X-auth-access-token', default=None)
    if auth token == None:
        raise Exception("Authentication failed")
```

Domains Global

Devices/devicerecords

DELETE PUT POST GET

Registers or unregisters a device. If

Examples

Type	Data Type
path	string
query	integer
query	integer

Constraints

None

None

None

API CONSOLE

api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
devices/devicerecords

objectid

Identifier for a device.

+ query parameter

Content-Type Header application/json

Accept Header application/json

GET Success!

Response Text Response Info Request Info

```
{ "links": { "self": "https://172.16.100.100/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords?offset=0&limit=3" }, "items": [ { "id": "16ble756-5e3b-11e6-aed9-a32bf906c3e9", "type": "Device", "name": { } } ] }
```

Export operation in... ▾

Python script

Perl script



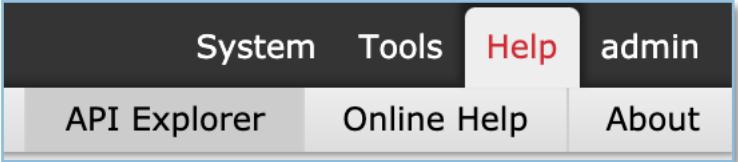
Documentation

- *Firepower REST API Quick Start Guide, Version 7.0*
- Inline information provided by the API Explorer
 - Legacy API Explorer is set to be removed in future releases



FXOS improvements

- REST API explorer on 4100/9300 for chassis management



API Explorer
/api/api-explorer/index.html

CISCO

FXOS REST API Explorer

You can use the following Firepower eXtensible Operating System (FXOS) REST API objects to programmatically access and configure your Firepower device. To use this Explorer:

- Click a listed object to view its supported methods.
- Click a displayed object method to view information about that method, including parameters and responses.
- Within a method description, for both Parameters and Responses, you can toggle between Example Value and Model views for detailed information about the object.
- You can directly test each method: click the Try It Out button, edit the parameters in the Edit Value box, and then click Execute.

FXOS Object Model

FXOS uses a hierarchical, tree-like structure to link objects. Each object may contain child objects. Every object retrieved through the REST API includes the property *dn*, or "distinguished name." The *dn* property uniquely identifies the object in the FXOS object tree. Children of an object contain the *m* property, or "relative name." The *m* property uniquely identifies a child object in the context of its parent.

HTTP Methods Supported

GET – Retrieves objects. The query is submitted in the URL and the output is contained in the response body.

PATCH – Partially updates objects.

POST – Creates objects.

PUT – Updates objects completely. Read-only properties are ignored, and writable properties, if not specified in the request body, are set to default values. Child objects are deleted if they are not specified (except for automatically created objects).

DELETE – Deletes the object (and its children) specified in the URL.

For the PATCH, POST and PUT methods, the object being modified must be present in the request body. Also, the object must include the "dn" property, and its children must include the "m" property.

Authentication

The REST API uses the HTTP "TOKEN" header from a REST client in order to authenticate each request. The `login` object (below) has more information on generating an authentication token.





7.0 FMC VPN API

- FMC RAVPN REST APIs delivered in 7.0:
 - FMC Get APIs for RAVPN Objects
 - FMC Get APIs for RAVPN Policies
 - Existing Policy Assignment's GET APIs enhanced to return RAVPN Policy Assignments
- These REST APIs are not being used by the FMC UI itself
- FMC only feature
 - FTD can be on older release

Virtual Private Network



Purpose of VPN Technology



VPN provides secure connectivity for traffic over an unsecured network



Provides access for Remote users to connect securely from any location



IKEv1, IKEv2, SSL protocols supported



Remote Access VPN



DTLS 1.2 support for Remote Access VPN

- FMC UI and FDM API support
- Configurable from Platform Settings
- Cisco AnyConnect Secure Mobility Client version 4.7 or higher

A screenshot of the Fireware Management Center (FMC) user interface. On the left, a sidebar lists various security protocols: ARP Inspection, Banner, DNS, External Authentication, Fragment Settings, HTTP, ICMP, Secure Shell, SMTP Server, SNMP, and SSL. The SSL option is highlighted with a blue selection bar. To the right, a main configuration panel is titled "Minimum SSL Version as Server:". It contains four dropdown menus:

- TLS Version: TLSv1.2
- DTLS Version: DTLSv1
- Diffie-Hellman Group: DTLSv1 (Bit Modulus)
- Elliptical Curve Diffie-Hellman group: group 19 (256 Bit)

A table below shows the "Protocol Version" and "Security Level" for different cipher suites. The first row is visible, showing "Protocol Version" and "Security Level".

Protocol Version	Security Level



RA VPN Components

Access interfaces – determine interfaces to be used by RA VPN

- SSL settings, such as access ports
- IKEv2 settings such as certificate
- AnyConnect image – client package to be installed on the endpoint
- AnyConnect client profile – XML can be uploaded into the FMC as file object.
 - Referenced in the group policy and downloaded to the endpoint while the VPN connection is initiating
 - Includes many parameters for the AnyConnect client.
- Connection profiles – determine how authentication is performed
- Group policies -- a set of user-oriented attribute/value pairs for RA VPN users
 - DNS/WINS, SSL/DTLS, timeouts, client bypass protocol and DHCP network scope
 - Split tunnel and split DNS configuration
 - VPN filter , egress VLAN and client firewall rules
 - AnyConnect client profile, SSL/DTLS settings and connection settings



Objects Associated with RA VPN

Firepower Management Center Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy admin ▾

Objects / Object Management

Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
RADIUS Server Group
Route Map
Security Group Tag
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone

Group Policy

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Name: DftGrpPolicy

Add Group Policy Filter

The screenshot shows the Firepower Management Center interface, specifically the "Objects / Object Management" section under the "Objects" tab. On the left is a navigation sidebar with various objects like Interface, Key Chain, Network, PKI, and Security Intelligence. The main area displays a "Group Policy" configuration page with a single input field named "Name" containing "DftGrpPolicy". There are buttons for "Add Group Policy" and "Filter".





Remote Access VPN

- Monitoring Remote Access VPN
 - Show vpn-sessiondb
 - Clear vpn-sessiondb
 - Show webvpn
 - Show aaa

RA VPN FMC Configuration Wizard



Remote Access VPN Policy Wizard

① Policy Assignment > ② Connection Profile > ③ AnyConnect > ④ Access & Certificate > ⑤ Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	NGFW1
Connection Profile:	RAVPN
Connection Alias:	RAVPN
AAA:	
Authentication Method:	Client Certificate & AAA
Username From Certificate:	CN (Common Name) & OU (Organisational Unit)
Authentication Server:	ISE_RADIUS
Authorization Server:	ISE_RADIUS
Accounting Server:	ISE_RADIUS
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	VPNPool
Address Pools (IPv6):	-
Group Policy:	DfitGrpPolicy
AnyConnect Images:	anyconnect-win-4.7.01076-webdeploy-k9.pkg
Interface Objects:	OutZone
Device Certificates:	NGFW1_Outside

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- ① **Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- ② **NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- ③ **DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- ④ **Port Configuration**
SSL will be enabled on port 443.
Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- ⚠ Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'OutZone'

Firewall RA integrations and Features



- ISE Integration
- Duo Integration
- Always-On
- SSL/IKEv2 VPN
- Radius/AAA-server integrations
- Posture
- Load Balancing
- Local Authentication
- Dynamic access policies
- Multi-certificate authentication
- AnyConnect custom attributes
- Selectively deploy RA policies



Remote Access VPN Enhancements



SAML Authentication for Remote Access VPN

- Introduced in 6.7
- SAML 2.0 Authentication Support with DUO as the Identity Provider for federated identity management with 2-factor authentication
 - FMC and FDM UI along with FTD API
- User Identity based Security Policy Enforcement
 - Adding the AD behind Identity Provider as Realm
- Untrusted SAML Server certificates not allowed in embedded browser for authentication

New Single Sign-on Server

Name*	SAML_IdP
Identity Provider Entity ID*	http://saml.lab.local/adfs/services,
SSO URL*	https://saml.lab.local:444/adfs/ls/
Logout URL	https://saml.lab.local:444/adfs/ls/
Base URL	https://ftd.lab.local
Identity Provider Certificate*	SAML_IdP
Service Provider Certificate	SSL_Wildcard.lab.local
Request Signature	--No Signature--
Request Timeout	Use the timeout set by the provider seconds (1-7200)



AnyConnect Management Tunnel

- Provides connectivity to the corporate network whenever the remote worker machine is powered up
- The management tunnel automatically disconnects when the VPN tunnel is established
- This release introduces Management Tunnel Profile in the Group Policy for FMC managed FTDs
- Uses machine certificate for authentication

Edit Group Policy

Name: * GP-MGMT

Description:

General AnyConnect Advanced

Profile Management Profile

Client Modules
SSL Settings
Connection Settings

A **Management VPN Tunnel** ensures connectivity to the corporate network whenever the endpoint is powered up, even if end-user does not connect over VPN.

The **Management Profile** file contains settings for enabling and establishing Management VPN Tunnel on endpoint automatically. Standalone Management VPN Tunnel profile editor can be used to create a new or modify existing profile file. You can download the profile editor from [Cisco Software Download Center](#)

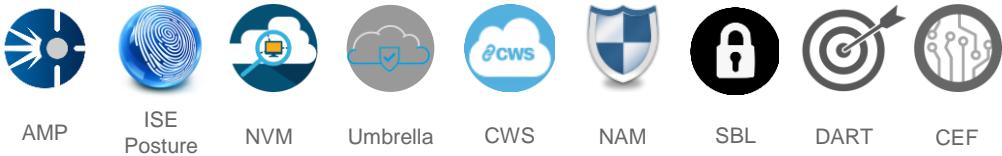
Management VPN Profile: +
VPN_MgmtTunnel_26

Additional configuration:
1. Configure authentication method as 'Client Certificate Only' in the Connection Profile used for Management VPN tunnel. On the Client configure a valid/trusted machine certificate for authentication.
2. Configure Split Tunnel to include only specified network(s) in the associated Group Policy.
3. Enable Client Bypass Protocol in the associated Group Policy.

AnyConnect Modules and Profile Distribution



- FMC UI and FTD Rest API support added for managing and distributing Anyconnect Modules and the Profiles
- Modules and Profiles can be associated to the group policy in VPN Wizard
- Profile Editor not available in FMC



Add Client Module

Client Module

- AMP Enabler
- DART
- FeedBack
- ISE Posture
- Network Access Manager
- Network Visibility
- Start Before Login
- Umbrella Roaming Security
- Web Security

Cancel Add

Add Group Policy

Name: * GRP_POLICY_FINANCE

Description:

General AnyConnect Advanced

Profile Client Modules

Download optional client modules to the endpoint. AnyConnect client requests download from the FTD of only the modules that are configured here.

Client Module	Profile	Download
AMP Enabler	ampEnabler.asp	✓
DART	Not Applicable	✓
FeedBack	feedback.fsp	✗
ISE Posture	iseposture.isp	✓
Network Access Man...	nam.nsp	✓
Network Visibility	networkvisibility...	✓

Cancel Save



7.0 AnyConnect Custom Attributes



7.0 What's New

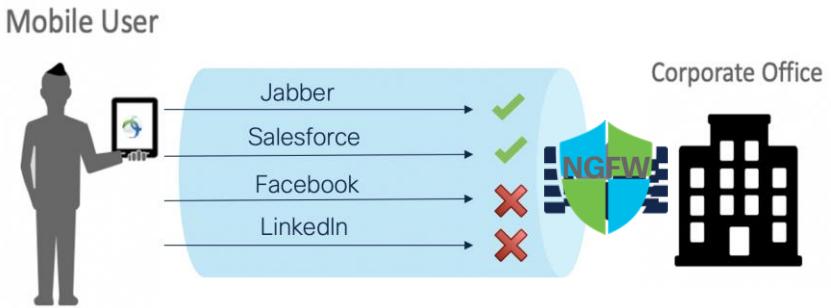
- In 7.0, FMC will support a user-friendly way to configure the Anyconnect Custom Attributes
 - Per App VPN on mobile devices with AnyConnect
 - Dynamic Split Tunneling
 - AnyConnect Defer Update
- FMC 7.0 builds the framework for flexibility to configure other custom attributes in addition to the above-mentioned ones. This will allow user to configure other existing and new AnyConnect features
- Custom attribute provides a generic infrastructure to configure AnyConnect client features without adding hard-coded support for these features on the FTD and FMC UI

Per Application VPN on Mobile devices

- Allows for tunneling specified subset of apps through one AnyConnect tunnel.

For example:

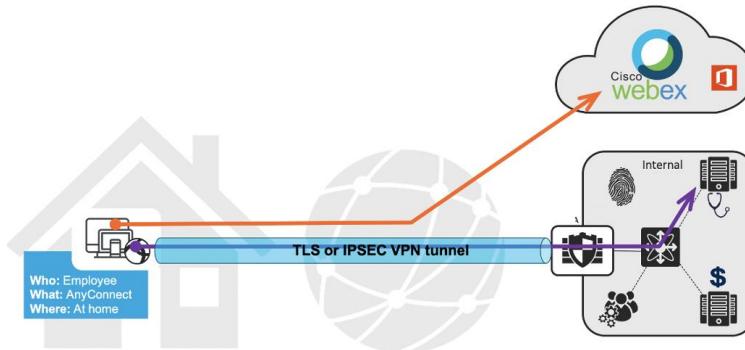
- Save resources: don't Netflix over VPN tunnel
- Security: don't allow non enterprise apps on enterprise network
- Avoiding tunneling trusted cloud applications (to minimize latency)
- PerApp VPN must be configured via Mobile Device Manager (MDM) and each device must be enrolled to the MDM server





Dynamic Split Tunneling

- Static split tunneling involves defining the IP addresses of hosts and networks that should be included in or excluded from the remote access VPN tunnel.
- Dynamic Split tunnel with AnyConnect was introduced to dynamically provision split include/exclude tunneling after tunnel establishment based on the host DNS domain name.
- Dynamic Split tunneling can be provisioned using
 - Dynamic Split Exclude
 - Dynamic Split Include





Defer Update

- Defer Update allows the user to delay update of the AnyConnect client
- When a client update is available, AnyConnect opens a dialog asking the user if they would like to update or defer the update





Local User Authentication for AnyConnect VPN users

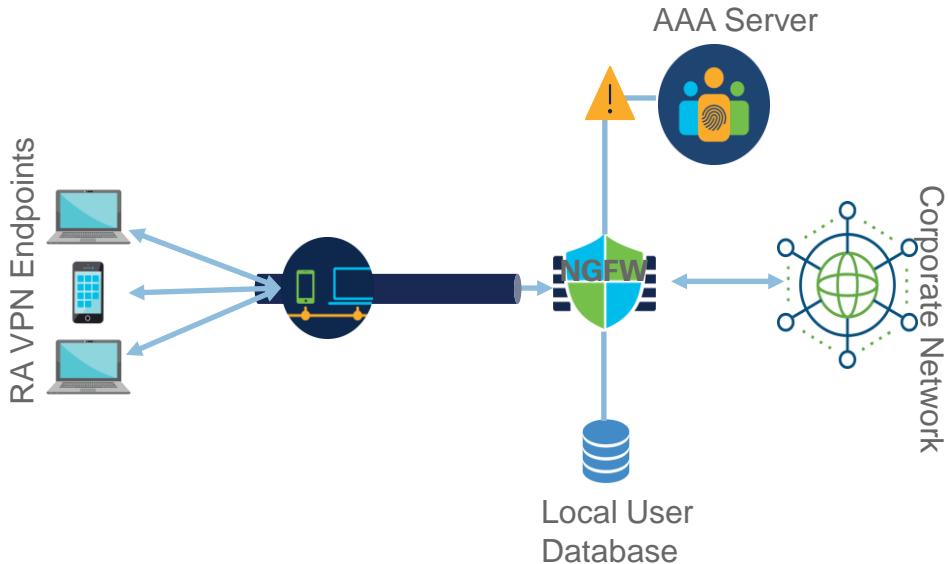


7.0 What's New

- FMC introduces the ability to configure and deploy Local Users to FTD via GUI and REST API
- When a RADIUS/LDAP/AD Server used for RA VPN Authentication fails, a fallback to authenticate to the Corporate Network through RA VPN and fix the issue
- Need a quick way to setup RA VPN for a quick demo/test
- Use cases where the authentication requests cannot go outside of FTD to an external AAA server for reasons of securing data in transit and data at rest
- It is already supported with FDM management

Local Authentication Feature Overview

- Local User Database can be used for VPN
 - Primary Authentication
 - Secondary Authentication
 - Fallback for Primary Authentication
 - Fallback for Secondary Authentication
- Local Users database configured as Realm (like AD/LDAP implementation)
 - Can be reused or shared across VPN configurations on multiple FTDs





Remote Access VPN Load Balancing

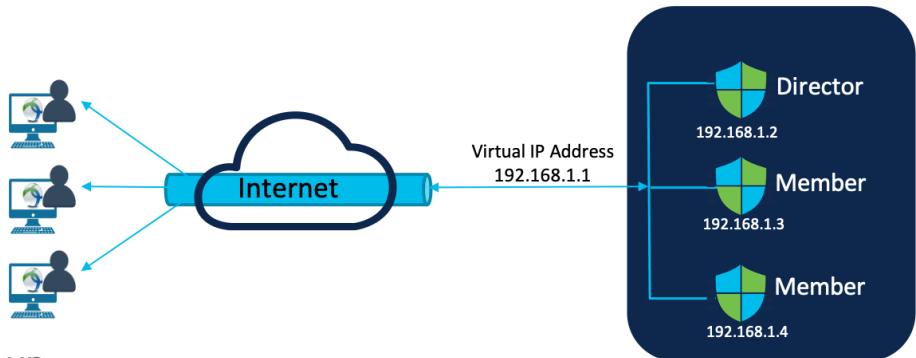


Remote Load Balancing

- This release adds support for
 - configuring and deploying two or more FTDs in a logical group for Load Balancing the Remote Access VPN sessions
 - share the Load Balancing configuration among multiple devices
- VPN Scalability combined with increased availability
 - Different from FTD Clustering or FTD High Availability
 - FTD Standalone or High Availability pair can be added as part of the Load Balancing group

Remote Load Balancing

- AnyConnect VPN session shared among devices
- Two or more devices virtually grouped to form a Load Balancing Group
- Members
 - FTDs participating in Load Balancing Group
 - Share the VPN connections
- Director
 - One FTD acts as a director
 - Distributes the load to other members in the group
 - Also participates in serving VPN sessions





VPN PKI Enhancements



Enrollment over Secure Transport (EST)

- A new enrollment type - Enrollment over Secure Transport (EST) supported in this release.
 - EST is the successor to the Simple Certificate Enrollment Protocol (SCEP)
 - EST uses TLS for the secure transport of messages.
 - In EST, the certificate signing request (CSR) can be tied to a requestor that is already trusted and authenticated with TLS.
- EST is described in RFC 7030



Site to Site VPN



S2S VPN Capabilities

IKE Protocol

IKEv1 & IKEv2

Authentication

Pre-Share Key & PKI

IP Version

IPv4 & IPv6. All combinations of inside and outside protocols supported, provided the protected networks have matching addressing schemes

Interface Types

Static and Dynamic IP

FMC/FTD HA

VPN is supported for both FTD and FMC HA environments

Topology

Point to Point
Hub & Spoke
Full mesh



Site to Site VPN

- Monitoring Commands
 - Show crypto ipsec sa
 - Clear crypto ipsec sa counters
 - Show crypto ipsec
 - df-bit
 - Fragmentation
 - Policy
 - Sa
 - stats
 - Show crypto isakmp



VPN on FTD

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A:

Device Name	VPN Interface	Protected Networks
NGFW1	outside/198.18.133.81	MainOfficeNetworks

Node B:

Device Name	VPN Interface	Protected Networks
NGFWBR1	outside/198.18.128.81	Branch1Office

● Ensure the protected networks are allowed by access control policy of each device.



Point to Point Example



Edit Endpoint

Device:*

Interface:*

IP Address:*

This IP is Private

Connection Type:

Certificate Map:
 +

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)

MainOfficeNetworks
+

Edit VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version: IKEv1 IKEv2

Endpoints

Node A:

Device Name	VPN Interface	Protected Networks
NGFW1	outside/198.18.133.81	MainOfficeNetworks <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Node B:

Device Name	VPN Interface	Protected Networks
NGFWBR1	outside/198.18.128.81	Branch1 Office <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Ensure the protected networks are allowed by access control policy of each device.



Virtual Tunnel Interface (VTI)

- Support for Route Based VPN
 - FMC, FDM, FTD API
- Static Virtual Tunnel Interface (VTI)
- Simple VPN Wizard with recommended default settings
- VTI interface can be used in Security Zone and Access Control Policy
- Static Routes or BGP used to define the VPN traffic
- Easy Configuration Wizard

VTI Requirements and Support



- Supports IPsec only, GRE is not supported
- No support for Dynamic VTI
- Supports only IPv4 interfaces as well as IPv4 protected networks or VPN payload
- IPv6 addressing on Static Virtual Tunnel Interface
- Static routing and BGP Dynamic Routing protocol is supported for VTI interfaces for classifying traffic for VPN\\
 - No Support for routing protocols like OSPF, RIP etc
- Not supported on FTD Cluster
- 1024 VTIs per interface
- Ability to configure backup VTI interfaces natively from FMC
- Adds support for ASA and CSM UI as well



Dynamic Reverse Route Injection

- This release introduces the support for Dynamic Reverse Route injection for FMC managed devices
- FMC UI and FMC API supported in 6.7
- FTD API already supports this starting 6.5
- Supported only with IKEv2 based static crypto maps
- VPN wizard adds an endpoint specific option to enable this feature

Add Endpoint

Device:^{*}
NGFW1

Interface:^{*}

IP Address:^{*}

This IP is Private

Connection Type:
Bidirectional

Certificate Map:
 +

Protected Networks:^{*}
 Subnet / IP Address (Network) Access List (Extended)
+

▼ Advance Settings

Enable Dynamic Reverse Route Injection



VPN Troubleshooting

- System Messages
- VPN Logging Settings (Can adjust Platform Settings > Syslog > Logging Setup)
- VPN syslogs are automatically enabled to be sent to the Firewall Management Center by default whenever a device is configured with site-to-site or remote access VPNs.
- Debug Commands

```
debug webvpn condition {group |p-ipaddress[{subnet|prefix}]} reset | user
```

```
debug aaa
```

```
debug crypto
```

```
debug ldap
```

```
debug ssl
```



FMC VPN Monitoring



FMC – RA VPN Monitoring

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

No Search Constraints ([Edit Search](#))

[Table View of Active Sessions](#) [Active Sessions](#)

Jump to...

	Login Time X	Last Seen X	User X
▼	2020-05-07 10:13:55	2020-05-07 10:13:55	Discovered Identity
▼	2020-05-06 07:52:27	2020-05-06 07:52:27	Discovered Identity
▼	2020-05-06 07:32:11	2020-05-06 07:32:11	Discovered Identity
▼	2020-05-06 06:55:23	2020-05-06 06:55:23	Discovered Identity
▼	2020-05-06 06:25:37	2020-05-06 06:25:37	Discovered Identity
▼	2020-05-06 06:18:20	2020-05-06 06:18:20	Discovered Identity
▼	2020-05-06 06:07:13	2020-05-06 06:07:13	Discovered Identity
▼	2020-05-06 05:57:46	2020-05-06 05:57:46	Discovered Identity
▼	2020-05-06 05:50:08	2020-05-06 05:50:08	Discovered Identity
▼	2020-05-06 05:49:17	2020-05-06 05:49:17	Discovered Identity\carlos.danger (LDAP)
▼	2020-05-06 05:47:40	2020-05-06 05:47:40	Discovered Identity\conception.varner (LDAP)
▼	2020-05-06 05:30:26	2020-05-06 05:30:26	Discovered Identity\judson.rigsby (LDAP)
▼	2020-05-06 05:07:47	2020-05-06 05:07:47	Discovered Identity\lyndon.russ (LDAP)
▼	2020-05-06 04:54:03	2020-05-06 04:54:03	Discovered Identity\adriana.breaux (LDAP)
▼	2020-05-06 04:59:46	2020-05-06 04:59:46	Discovered Identity\jermija.lyakh (LDAP)
▼	2020-05-06 04:57:03	2020-05-06 04:57:03	Discovered Identity\elmer.blanco (LDAP)
▼	2020-05-06 04:37:52	2020-05-06 04:37:52	Discovered Identity\faithe.hoffman (LDAP)
▼	2020-05-06 04:36:53	2020-05-06 04:36:53	Discovered Identity\bobby.tiger (LDAP)

Context Explorer Hosts Correlation

Connections Hosts Correlation Events

Events Indications of Compromise White List Events

Security Intelligence Events Applications White List Violations

Intrusions Servers Status

Events Host Attributes Advanced

Reviewed Events Discovery Events Custom Workflows

Clipboard Vulnerabilities Custom Tables

Incidents Third-Party Vulnerabilities Geolocation

Files Users Contextual Cross-launch

Malware Events Active Sessions Search

File Events Users

Captured Files User Activity

Network File Trajectory Indications of Compromise

Bookmark This Page | Report Designer | Dashboard | View Bookmarks | Search | [Predefined Searches](#)

First Name X	Last Name X	E-Mail X	Department X	Phone X	Discovery Application X	Device X
jon.russ					<input type="checkbox"/> LDAP	NGFWTG
abod.crane					<input type="checkbox"/> LDAP	NGFWTG
eva.underwood					<input type="checkbox"/> LDAP	NGFWTG
thijs.devries					<input type="checkbox"/> LDAP	NGFWTG
nald.chandler					<input type="checkbox"/> LDAP	NGFWTG
ll.palumbo					<input type="checkbox"/> LDAP	NGFWTG
go.almeida					<input type="checkbox"/> LDAP	NGFWTG
uko.overton					<input type="checkbox"/> LDAP	NGFWTG
emelda.goodson					<input type="checkbox"/> LDAP	NGFWTG
carlos.danger					<input type="checkbox"/> LDAP	NGFWTG
conception.varner					<input type="checkbox"/> LDAP	NGFWTG
judson.rigsby					<input type="checkbox"/> LDAP	NGFWTG
lyndon.russ					<input type="checkbox"/> LDAP	NGFWTG
adriana.breaux					<input type="checkbox"/> LDAP	NGFWTG
jermija.lyakh					<input type="checkbox"/> LDAP	NGFWTG
elmer.blanco					<input type="checkbox"/> LDAP	NGFWTG
faithe.hoffman					<input type="checkbox"/> LDAP	NGFWTG
bobby.tiger					<input type="checkbox"/> LDAP	NGFWTG



FMC – RA VPN Troubleshooting



Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin ▾

Devices / VPN / Troubleshooting

No Search Constraints ([Edit Search](#))

Bookmark This Page | Report Designer | Dashboard | View Bookmarks | Search

2021-04-28 10:32:00 - 2021-05-28 10:37:27 Expanding

Table View of VPN Troubleshooting

<input type="checkbox"/>	Time	Severity	Message	Message Class	Username	Device
<input type="checkbox"/>	2021-05-16 19:02:12	Critical	Error activating tunnel-group scripts	User Authentication		NGFW1
<input type="checkbox"/>	2021-05-12 18:24:58	Critical	Error activating tunnel-group scripts	User Authentication		NGFW1

< Page 1 of 1 > | Displaying rows 1–2 of 2 rows

[View](#) [Delete](#)
[View All](#) [Delete All](#)

Operations Monitoring and Troubleshooting



Operations



Get knowing the tools

Logging utilities

- FTD ASA Engine logs
- FTD Snort Engine logs
- FXOS logs

Debug utilities

- FTD ASA Engine Debugs
- FTD Snort Engine Debugs
- FXOS Cisco Interactive Debug (TAC only)

Tracing utilities

- FTD Packet-Tracer
- FTD ASA Engine Capture w/Trace

Capture utilities

- FTD ASA Engine Capture
- FTD Snort Engine Capture
- FXOS internal switch Capture



FXOS Logging

- FXOS syslog messages can be sent to local or remote destinations

The screenshot shows the FXOS Platform Settings interface with the 'Remote Destinations' tab selected. On the left, a sidebar lists various system components: NTP, SSH, SNMP, HTTPS, AAA, Syslog (which is highlighted in red), DNS, FIPS and Common Criteria, and Access List. The main configuration area for 'Server 1' includes fields for Admin State (checked), Level (set to 'debugging'), Hostname/IP Address (10.229.24.27), and Facility (local7). Another 'Server 2' entry is partially visible below.

- Use 'show tech-support' to generate 3 different log bundles for TAC analysis

```
FPR4140-A# connect local-mgmt
FPR4140-A(local-mgmt) # show tech-support fprm detail
FPR4140-A(local-mgmt) # show tech-support chassis 1 detail
FPR4140-A(local-mgmt) # show tech-support module 1 detail
FPR4140-A(local-mgmt) # dir techsupport/
1 15595520 Apr 09 17:29:10 2017 20170409172722_FPR4140_FPRM.tar
1 962560 Apr 09 17:32:20 2017 20170409172916_FPR4140_BC1_all.tar
1 7014400 Apr 09 18:06:25 2017 Firepower-Module1_04_09_2017_18_05_59.tar
FPR4140-A(local-mgmt) # copy workspace:///techsupport/20170409172722_FPR4140_FPRM.tar
ftp|tftp|scp|sftp://username@192.168.0.1/
```

FP2100 has only fprm bundle

Generate the bundles

Check the filenames

Export the files



FXOS improvements

- Combines tech support files from various FXOS components into one troubleshooting bundle file
- Prior to this, FXOS CLI/GUI supported separate options to collect these tech support outputs
- Reduces duration for collection of troubleshooting logs
- Frequently, customers would collect just one of these, leading to incomplete troubleshooting information

Screenshot of the FXOS Tools > Troubleshooting Logs interface:

System Tools Help admin

Packet Capture Troubleshooting Logs

Overview Interfaces Logical Devices Security Engine Platform Settings

Create and Download a Tech Support File

Generate troubleshooting files at the Chassis, Module and Firmware level.

✓ Log generation status for Chassis: Success

Chassis Generate Log

Chassis: Click the File explorer after the job is successfully completed. Generated files are located under the techsupport folder.

Module 1

Expand All Collapse All Refresh

File Name	Last Updated On	Size(in KB)
diagnostics	Sun Jan 01 11:10:50 GMT-500 2012	
bladelog	Sun Jan 01 11:10:11 GMT-500 2012	
techsupport	Fri Apr 24 15:40:22 GMT-400 2020	
debug_plugin	Sun Jan 01 11:15:41 GMT-500 2012	
packet-capture	Wed Jan 08 21:51:23 GMT-500 2020	
cores	Sun Jan 01 11:10:13 GMT-500 2012	
blade_debug_plugin	Sun Jan 01 11:10:11 GMT-500 2012	
lost+found	Sun Dec 22 21:59:54 GMT-500 2019	



Configure Syslog for FXOS

- Firepower eXtensible Operating System (FXOS) has its own Syslog messages
 - Configured through the Firepower Chassis Manager (FCM)
 - For the 4100/9300 Platforms

The screenshot shows the 'Platform Settings' tab selected in the navigation bar. On the left, a sidebar lists various system components: NTP, SSH, SNMP, HTTPS, AAA, Syslog (which is currently selected), DNS, FIPS and Common Criteria, and Access List. The main panel is titled 'Local Destinations' and contains two sections: 'Console' and 'Monitor'. In the 'Console' section, 'Admin State' is set to 'Enable' (unchecked) and 'Level' is set to 'Critical' (selected). In the 'Monitor' section, 'Admin State' is set to 'Enable' (unchecked) and 'Level' is set to 'critical' (selected). At the bottom are 'Save' and 'Cancel' buttons.



FTD Logging – ASA-level logs

ASA-level logs provide information about the FTD LINA Engine

Screenshot of the Cisco ASA configuration interface showing the Syslog Servers tab and command-line output.

Syslog Servers Tab:

Interface	IP Address	Protocol	Port	EMBLEM	SECURE
inside	10.10.10.32	UDP	514	false	false

Command-line Output:

```
> show running-config logging
> show logging
Apr 23 2017 11:11:45: %ASA-7-609002: Teardown local-host nlp_int_tap:ff02::1 duration 0:00:02
```

Remote Syslog server
which receives the logs

Same as on classic ASA



FTD Logging – Snort-level logs

Connection Events provide information about Snort Data-Plane

Connection Events ([switch workflow](#))

No Search Constraints ([Edit Search](#))

Connections with Application Details Table View of Connection Events Jump to...

II 2021-10-25 18:57:50 - 2021-10-25 19:57:50 Expanding

	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	Client	Web Application	URL
▼	2021-10-25 19:57:41	2021-10-25 19:57:42	Allow		192.168.16.182	IRL	54.76.114.37	IRL	InZone	OutZone	65287 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	https://gwa.lphbs.com
▼	2021-10-25 19:57:41	2021-10-25 19:57:41	Allow		192.168.16.182	IRL	54.76.114.37	IRL	InZone	OutZone	57383 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	https://gwa.lphbs.com
▼	2021-10-25 19:57:41	2021-10-25 19:57:41	Allow		192.168.16.182	IRL	54.76.114.37	IRL	InZone	OutZone	65240 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	https://gwa.lphbs.com
▼	2021-10-25 19:57:41	2021-10-25 19:57:41	Allow		192.168.16.182	IRL	54.76.114.37	IRL	InZone	OutZone	57384 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	https://gwa.lphbs.com
▼	2021-10-25 19:57:41	2021-10-25 19:57:41	Allow		192.168.16.182	IRL	54.76.114.37	IRL	InZone	OutZone	57382 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	https://gwa.lphbs.com
▼	2021-10-25 19:57:40	2021-10-25 19:57:41	Allow		192.168.22.141	USA	34.202.139.1	USA	InZone	OutZone	49795 / tcp	443 (https) / tcp				
▼	2021-10-25 19:57:40	2021-10-25 19:57:41	Allow		192.168.22.141	USA	34.202.139.1	USA	InZone	OutZone	49793 / tcp	443 (https) / tcp				
▼	2021-10-25 19:57:40	2021-10-25 19:57:41	Allow		192.168.22.141	USA	34.202.139.1	USA	InZone	OutZone	49794 / tcp	443 (https) / tcp				

Table View provides flexibility – allows addition/removal of columns

On FTD the Connection Events are stored in:

```
ngfw/var/sf/detection_engines/UUID/instance-X/unified_events-2.logXXX
```

When they get archived, they go to:

```
ngfw/var/sf/detection_engines/UUID/instance-X/backup/unified_events-2.logXXX
```





FTD Logging – System logs

- Files like **/ngfw/var/log/messages** contain valuable information about FTD Control and Data-Plane status
- You can use '**system support view-files**' command from CLISH to see the contents of files under **/ngfw/var/log** directory

```
> system support view-files
====View Logs====
=====
Directory: /ngfw/var/log
-----sub-dirs-----
packages
removed_packages
...
-----files-----
2017-04-23 13:09:14.360532 | 3148401    | messages
([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s
Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> messages
Apr 23 04:02:14 Firepower-module1 CROND[54253]: pam_unix(crond:session): session closed
```

Type 's' to select a file

Specify the file name



Simple Network Management Protocol (SNMP)



SNMP: What & Why



Monitor health and status of managed devices centrally



Devices can send TRAPS or provide READ access



FTD supports SNMP versions 1, 2c and 3



Your organization's security and compliance needs should determine your SNMP configuration.

SNMP support over management interface

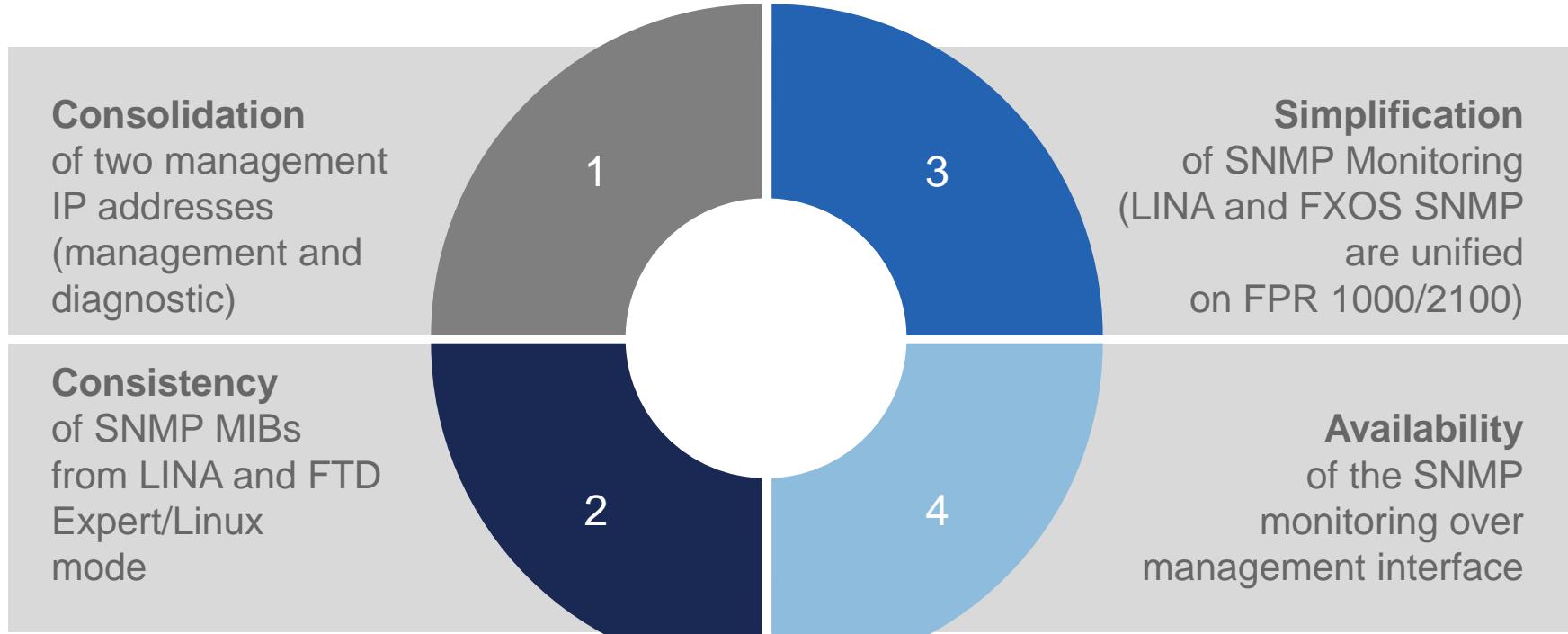


- Prior to 6.6 release, the SNMP monitoring was available over (LINA) Data or Diagnostic type interfaces
- With the 6.6 release, SNMP LINA and FXOS polling and traps are available over the FTD Management Interface

SNMP Monitoring	FTD LINA MIBS	FXOS MIBS
Platforms	FPR 1000, 2100, 4100, 9300, FTDv, ASA 5500-x platforms	FPR 1000 and 2100 series
Configuration	Platform Settings > SNMP	Devices > Device Management > SNMP

No longer required

SNMP support over management interface



Benefits of Enabling SNMP on Firepower



Monitor Health of Devices

Generate alerts based on system or connection events

Centralize network monitoring

Troubleshooting



Firepower & SNMP

- SNMP can be used to monitor the status and health of your Firepower devices.
- SNMP can also be used as a method to deliver alerts generated by the system or security policies.
- Both FTD & FXOS can be monitored using SNMP

Note:

The recommended method of monitoring the health of a Firepower deployment is to use the built-in Health Monitoring feature.

SNMP Use Cases

- 1 CPU Monitoring
- 2 Memory Monitoring
- 3 Interface Monitoring





SNMP Use Case: CPU Monitoring

FXOS	<ul style="list-style-type: none">Provides average CPU utilization for 1 and 5 minute intervalsAverage is calculated for ALL CPU cores, irrespective of process running on a specific coreMultiple cores will have DATA PLANE threads, SNORT instances and Management processesDATA PLANE continuously queries interface buffers for incoming packets so cores running DATA PLANE threads will likely always show almost 100% utilizationThis could result in FXOS reporting high CPU utilization even when the appliance is idle
FTD	<ul style="list-style-type: none">SNMP queries to FTD reports CPU statistics only when the data plane has something to processThis makes for a more accurate report on CPU utilization compared to FXOSThis however, does not include statistics for processes handling Snort instances



SNMP Use Case: Memory Monitoring

FXOS/FTD

- As with CPU monitoring, memory usage can be tracked using SNMP
- SNMP monitoring returns information from the DATA PLANE threads
- FMC Health Policies also support monitoring of device memory utilization and is the recommended method



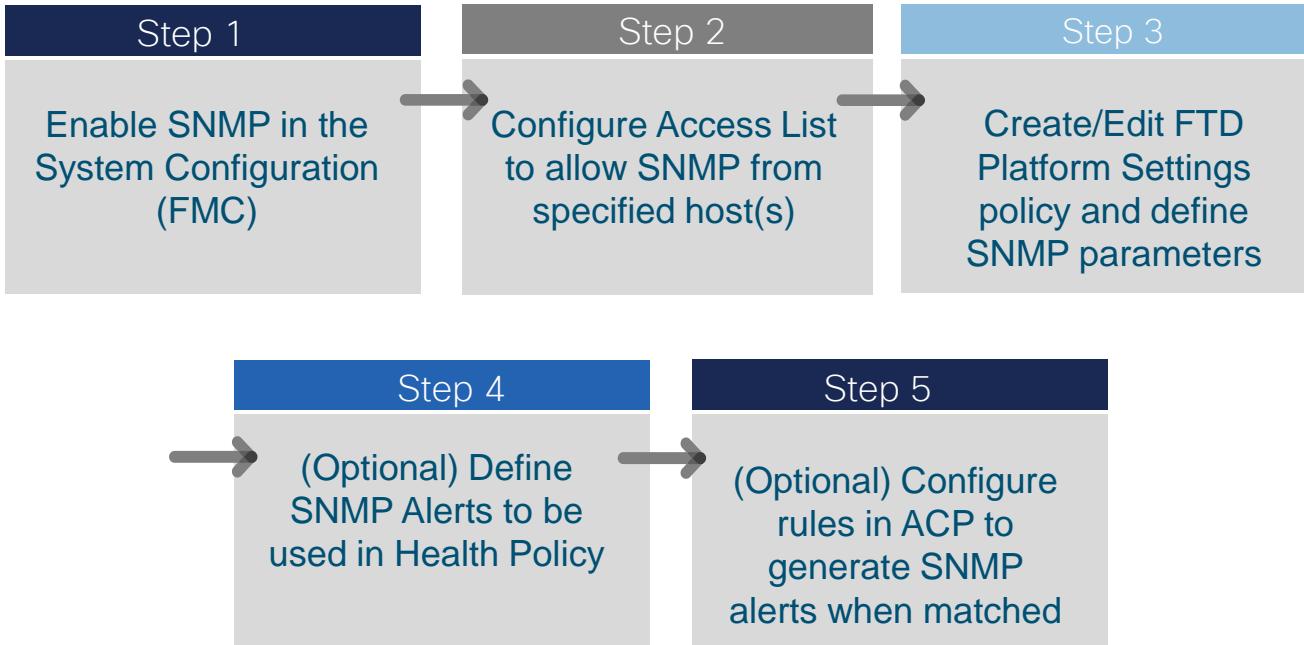
SNMP Use Case: Interface Monitoring

FXOS/FTD

- Both FXOS and FTD support monitoring of interfaces via SNMP
- Shared interfaces in FXOS will return cumulative statistics when monitored
- Recommendation is to monitor interfaces via FTD for individual interface statistics



SNMP - Configuration Steps





Configuring SNMP – Configuration Settings

The screenshot shows the FMC configuration interface. On the left, a sidebar lists various configuration options, with "SNMP" highlighted by a red arrow. The main pane displays two configuration fields: "SNMP Version" set to "Version 2" and "Community String" set to "EXAMPLE". A large red oval highlights these two fields. The FMC header includes the Cisco logo and navigation tabs: Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence.

- Enable SNMP in FMC
- Select Version (1,2c or 3)
- Define Community String





Configuring SNMP – Configuration Settings

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

Access List **Add Rules**

Host	Port	Actions
any	443	edit
any	22	edit
192.168.100.50	161	edit

Edit Access List and add the required SNMP server(s)

IP Address

Port SSH HTTPS SNMP





Configuring SNMP – Platform Settings

FTD_Platform_Policy

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP

ICMP

Secure Shell

SMTP Server

SNMP

SSL

Syslog

Enable SNMP Servers

Read Community String
.....

Confirm*
.....

System Administrator Name
FTD-Admin

Location
A galaxy far, far away.....

Port
161
(1 - 65535)



Create/Edit an FTD Platform Settings policy

- Select *SNMP*
- *Enable SNMP*
- *Enter the:*
 - *Community String*
 - *Admin Name*
 - *Location*
 - *Port*



Configuring SNMP – Platform Settings

FTD_Platform_Policy

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP

ICMP

Secure Shell

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Hosts

Interface

+ Add

Reachable By:

Device Management Interface (Applicable from v6.6.0 and above)

Security Zones or Named Interface

Add SNMP Management Hosts

IP Address*
SNMP_Server +

SNMP Version
2c

Username

Community String

Confirm

Location

Poll

Trap

Port
161
(1 - 65535)

Port
162
(1 - 65535)

You have unsaved changes **Save** **Cancel**

Policy Assignments (0)





Configuring SNMP – Alerts

The screenshot shows the Firepower Management Center interface. The top navigation bar includes links for Policies, Devices, Objects, AMP, and Intelligence, along with a Deploy button and user admin. Below the navigation is a secondary menu with links for Policies, Intrusion Rules, White List, Traffic Profiles, Alerts, Remediations, Groups, and Monitor Alerts. The main content area has tabs for Alerts, Impact Flag Alerts, Discovery Event Alerts, and Advanced Malware Protection Alerts. The 'Alerts' tab is selected and highlighted with a red circle. A modal window titled 'Edit SNMP Alert Configuration' is open in the center. This modal contains fields for Name (set to 'Example_Alert'), Trap Server (set to '192.168.100.50'), Version (set to 'v2'), and Community String (set to 'example'). On the right side of the modal, there is a 'Create Alert' dropdown menu with three options: 'Create Email Alert', 'Create SNMP Alert', and 'Create Syslog Alert'. The 'Create SNMP Alert' option is highlighted with a red box and a red arrow pointing to it from the bottom right. The bottom right corner of the modal has 'Cancel' and 'Save' buttons.

Multiple custom alerts can be created for use in Access Control or Health Policies

The Cisco logo, which consists of a series of vertical bars of increasing height followed by the word "CISCO".

© 2022 Cisco and/or its affiliates. All rights reserved. 223



Configuring SNMP – Using Alerts in ACP

Editing Rule - Web Access

Name: Web Access Enabled: Move

Action: Allow Time Range:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Log at Beginning of Connection
 Log at End of Connection

File Events:
 Log Files

Send Connection Events to:
 Event Viewer
 Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)
 SNMP Trap

Select the SNMP alert created previously from the drop down list or create a new Alert using the "+" button

Cancel Save

Configuring SNMP – Using Alerts in Health Policy



The screenshot shows the 'Configure Health Alerts' interface in the Firepower Management Center. On the left, a sidebar lists 'Active Health Alerts' with one entry: 'Monitor CPU'. In the center, the 'Configure Health Alerts' form is displayed:

- Health Alert Name:** Monitor CPU (highlighted by a red arrow)
- Severity:** Warning (highlighted by a red arrow)
- Module:** CPU Usage (highlighted by a red arrow)
- Alert:** Example_Alert (SNMP) (highlighted by a red arrow)
- Threshold Timeout (Optional):** (in minutes) (empty input field)

At the bottom right of the form is a blue 'Save' button.

Navigate to:
System – Health – Monitor Alerts

Give the alert a name

Select the Severity to be alerted on

Select the Module to alert on

Assign the alert (created earlier)

Save (alert appears in Active Health Alerts window on left)

Best Practices for SNMP



-  Use FMC Health Monitor for monitoring your deployment
 -  Use SNMP Alerts to trigger notifications of critical events
 -  (Optional) Use SNMP alerts in access rules to be notified of critical
 -  network events
-  © 2022 Cisco and/or its affiliates. All rights reserved. 226

Device Health Monitoring – SNMP Unification



7.0

- FXOS stats available as part of the Unified SNMP infrastructure
- Improved Metrics over API

6.7

- Integrated SNMP stats for Snort and Data plane over data and management interface
- HA and Cluster status available over SNMP

6.6

- Added Support for SNMP polling over FTD management interface



Easy and Flexible Unified Monitoring of Device Health





FTD CPU usage

FTD provides 2 levels of CPU usage:

- **System level**

```
> system support utilization
top - 13:00:15 up 2 days, 3 min, 0 users, load average: 24.29, 24.17, 24.15
Tasks: 719 total, 1 running, 717 sleeping, 0 stopped, 1 zombie
Cpu(s): 29.8%us, 4.9%sy, 0.0%ni, 65.2%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
...
    PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+   COMMAND
13672 root      0 -20 27.2g 2.5g 2.0g S 1794  1.0  51978:46 lina ←
13863 root      20   0 5778m 72m 15m S     2  0.0  49:11.73 SFDataCorrelator
> show cpu system
Time          CPU      %usr      %nice      %sys %iowait      %irq      %soft      %steal      %guest      %gnice      %idle
19:53:46      all    29.79      0.00      4.92      0.04      0.00      0.01      0.00      0.00      0.00      0.00      65.24
```

Expected behavior!

- **LINA engine level**

```
> show cpu usage
CPU utilization for 5 seconds = 2%; 1 minute: 1%; 5 minutes: 0%

> show processes cpu-usage sorted non-zero
PC                  Thread          5Sec      1Min      5Min    Process
-                   -            0.1%      0.1%      0.1%  DATAPATH-0-5729
```



CPU and Memory Usage

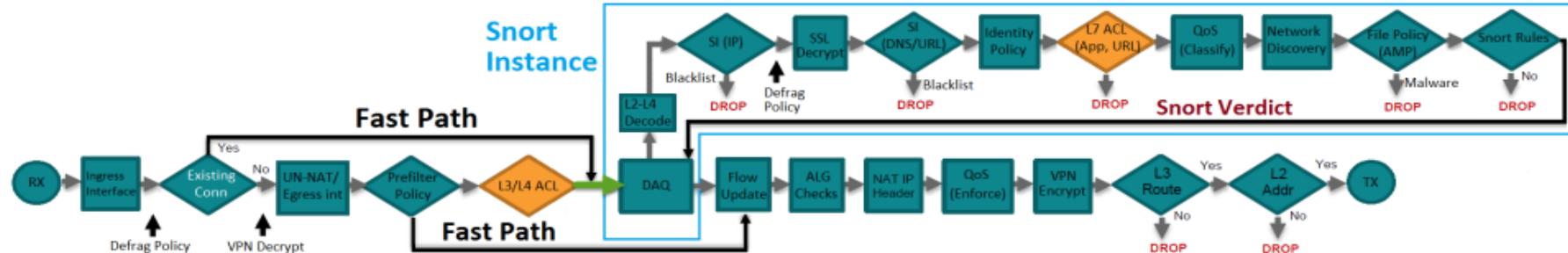


FTD CPU usage



- Baseline your total CPU utilization
- Alerts about High CPU don't necessarily indicate a problem unless there is also latency and/or packet loss
- Bypass flows that don't need Snort Inspection using Prefilter Policy Fastpath
 - a) Big/fat flows (e.g backups, file transfers)
 - b) Encrypted traffic that you don't decrypt (e.g. IPSec, SSH)
- Intrusion Policy tuning and poorly-written Snort rules can affect performance. Try "Connectivity over Security" to narrow down

FTD Packet Processing: L3/L4 ACL - Allow



- 'Allow' action will forward **all** packets to Snort engine.
- In **show snort statistics** output the packets will be shown as **Passed Packets**

```
> show snort statistics

Packet Counters:
  Passed Packets          18446306
  Blocked Packets         53799
  Injected Packets        312
  Packets bypassed (Snort Down) 0
  Packets bypassed (Snort Busy) 0

Flow Counters:
  Fast-Forwarded Flows    79915
  Blacklisted Flows       542777

Miscellaneous Counters:
  Start-of-Flow events    0
  End-of-Flow events      299039
  Denied flow events      0
  Frames forwarded to Snort before drop 0
  Inject packets dropped 0
  TCP Ack bypass Packets 0
  TCP Meta-Ack Packets   0
>
```



FTD Memory usage

FTD provides 2 levels of memory usage:

- **System level**

```
> system support utilization
...
Mem: 8184696k total, 3583248k used, 2991088k free, 171812k buffers
Swap: 3998716k total, 4920k used, 3993796k free, 1438548k cached
```

total = used + free + buffers + cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
13672	root		0	-20	27.2g	2.5g	2.0g	S	1794	1.0	51978:46 lina

```
> show memory system
      total        used         free        shared        buffers        cached
Mem: 8184696  3582772  2992228          0  171828  1437868
-/+ buffers/cache: 3582772  4601924
Swap: 3998716   4920  3993796
```

free + buffers + cached

- **LINA engine level**

```
> show memory [detail]
Free memory: 2645848803 bytes (57%)
Used memory: 1985224704 bytes (43%)
-----
Total memory: 4631073507 bytes (100%)
```

Least free memory: 131126033472 bytes (92%)
Most used memory: 11392566208 bytes (8%)





FTD Logging – System logs

pigtail is an FMC and FTD CLI tool that parses, reformats, and displays contents of several log files as the files are written

```
> pigtail
Pigtail selection of feature logs  Select feature log type (ALL/Deploy/UI/captive-portal)

root@NGFW1:~# pigtail

** Displaying logs: CPER MOJO MSGS TCAT SOUT NGFW SYDB HTTP TAPP CPAC SERR SSEC CPLG DCSM NGUI DMSG VMSB TCLG VMSS DEPL USMS AUTD ACTQ ****
*****
***** SERR: 10-26 07:58:08 NGFW1 Pruner[3256]: find: '/ngfw/var/log/deploy_ts': No such file or directory
***** SERR: 10-26 19:58:57 NGFW1 Pruner[3256]: find: '/ngfw/var/log/deploy_ts': No such file or directory
***** SERR: 10-27 07:59:46 NGFW1 Pruner[3256]: find: '/ngfw/var/log/deploy_ts': No such file or directory
***** SERR: 10-27 20:00:34 NGFW1 Pruner[3256]: find: '/ngfw/var/log/deploy_ts': No such file or directory
***** SERR: 10-28 08:01:22 NGFW1 Pruner[3256]: find: '/ngfw/var/log/deploy_ts': No such file or directory
***** NGUI: 10-28 08:06:19 com.cisco.smx.eventing.event.capture.EventCaptureServer.run(EventCaptureServer.java:111)
***** NGUI: 10-28 08:06:19 java.lang.Thread.run(Thread.java:748)
***** NGUI: 01-05 18:51:23 SEVERE [localhost-startStop-2] org.apache.catalina.loader.WebappClassLoaderBase.checkThreadLocalMapForLeaks The web application key of type [java.lang.ThreadLocal$SuppliedThreadLocal] (value [java.lang.ThreadLocal$SuppliedThreadLocal@47f0fe73]) and a value of type [org.neo4j.io.pageCursorTracer] (value [org.neo4j.io.pagecache.tracing.cursor.DefaultPageCursorTracer@363ea076]) but failed to remove it when the web application was renewed over time to try and avoid a probable memory leak.
***** NGUI: 01-05 18:51:23 INFO [Thread-38] org.apache.coyote.AbstractProtocol.stop Stopping ProtocolHandler ["ajp-nio-8009"]
***** NGUI: 01-05 18:51:23 INFO [Thread-38] org.apache.coyote.AbstractProtocol.destroy Destroying ProtocolHandler ["ajp-nio-8009"]
***** SOUT: 10-28 07:45:51 NGFW1 run_hm[13094]: DOMAIN: Global
***** SOUT: 10-28 07:50:52 NGFW1 run_hm[13094]: DOMAIN: Global
***** SOUT: 10-28 07:55:52 NGFW1 run_hm[13094]: DOMAIN: Global
***** SOUT: 10-28 08:00:54 NGFW1 run_hm[13094]: DOMAIN: Global
***** SOUT: 10-28 08:05:55 NGFW1 run_hm[13094]: DOMAIN: Global
***** DMSG: 07-08 20:15:01 [Thu 2021] sync_fs (17405): drop_caches: 1
***** DMSG: 07-08 20:25:00 [Thu 2021] sync_fs (21152): drop_caches: 1
***** DMSG: 07-08 20:29:31 [Thu 2021] brl: port 3(tap5) entered disabled state
***** DMSG: 07-08 20:29:31 [Thu 2021] brl: port 1(tap2) entered disabled state
***** DMSG: 07-08 20:29:31 [Thu 2021] br0: port 1(tap1) entered disabled state
***** False [] range "\w+" in regex; marked by <-- HERE in m/(?: \w+ <-- HERE .)+ ActionQueueScrape.pl\\((\\d+)\\))/ at /ngfw/usr/local/sf/bin/pigtail line 1
***** DEPL: 10-28 08:01:22 NGFW1 Pruner.pl[3256]: > SF::UMPD::DataStore::getPolicies start (144.21M)
***** DEPL: 10-28 08:01:22 NGFW1 Pruner.pl[3256]: Generating revision UUID from Version 00000000-0000-0000-0000-00006177222a
***** DEPL: 10-28 08:01:22 NGFW1 Pruner.pl[3256]: < SF::UMPD::DataStore::getPolicies end (144.21M, 0.019(sec))
***** DEPL: 10-28 08:01:41 pid=3257 > main::_ANON start - Memory Check - executeTask (26.91M)
***** DEPL: 10-28 08:01:41 pid=3257 < main::_ANON end - Memory Check - executeTask (26.91M, 0.024(sec))
***** MMSG: 10-28 08:05:30 NGFW1 SF-IMS[2807]: [2807] sfifd::config [ERROR] Failed to get interface index for 'eth0'.
***** MMSG: 10-28 08:05:54 NGFW1 SF-IMS[2933]: [2933] pm:control [INFO] ControlHandler auditing message: ProcessHealthPurge, socket 70, user '', cmd '/usr/bin/hm.pl --persistent', pid 13094 (uid 0, gid 0)
```



FTD Logging – System logs

- Use the 'pigtail --help' from root to get additional information about usage

```
These are the keywords and associated log files that pigtail supports:
ACTQ /var/log/action_queue.log
AUTD /var/log/auth-daemon.log
CPAC /var/log/idhttpsd/access_log
CPER /var/log/idhttpsd/error_log
CPLG /var/log/captive_portal.log
DCSM /var/log/mojo.log
DEPL /var/log/sf/policy_deployment.log
DMSG /var/log/dmesg.log
HTTP /var/log/httpd/httpsd_error_log
MOJO /var/log/mojo/mojo.log
MSGS /var/log/messages
NGFW /var/log/ngfwManager.log
NGUI /var/log/cisco/ngfw-onbox.log
SERR /var/log/process_stderr.log
SOUT /var/log/process_stdout.log
SSEC /var/log/connector/connector.log
SYDB /opt/CSCOpX/MDC/log/operation/sydb.out
TAPP /var/log/SSE/sse_telemetry.log
TCAT /opt/CSCOpX/MDC/tomcat/logs/stdout.logs
TCLG /opt/CSCOpX/MDC/log/operation/sftunnel-javaclient.log
USMS /opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log
VMSB /opt/CSCOpX/MDC/log/operation/vmsbesvcs.log
VMSS /opt/CSCOpX/MDC/log/operation/vmssharedsvcs.log

pigtail has several presets built in for feature-specific debugging. You can use a preset name in lieu of specifying
the log keywords. Using a preset will always create an output file with the name 'pigtail-<preset>-<timestamp>.log'.
The following presets are supported:
captiveportal CPLG CPAC CPER
deploy ACTQ DEPL NGFW NGUI USMS VMSB VMSS TCLG
ui DCSM HTTP MOJO NGUI TCAT
all ACTQ AUTD CPAC CPER CPLG DCSM DEPL DMSG HTTP MOJO MSGS NGFW NGUI SERR SOUT SSEC SYDB TAPP TCLG USMS VMSB VMSS
```

- Run pigtail over an SSH connection to avoid console delay



Firepower Recommendations

Use Firepower Recommendation to:

- Associate the operating systems, servers, and client application protocols detected on network.
- Tailor your intrusion policy to the specific needs of your monitored network.



Firepower Recommendations

Firepower Management Center Overview Analysis Policies **Policies** Devices Objects AMP Intelligence Deploy ! 2 admin ▾

Policy Information

Rules

Firepower Recommendations (selected)

> Advanced Settings

> Policy Layers

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

Generate Recommendations **Generate and Use Recommendations**





Troubleshooting



Get knowing the tools

Logging utilities

- FTD ASA Engine logs
- FTD Snort Engine logs
- FXOS logs

Debug utilities

- FTD ASA Engine Debugs
- FTD Snort Engine Debugs
- FXOS Cisco Interactive Debug (TAC only)

Tracing utilities

- FTD Packet-Tracer
- FTD ASA Engine Capture w/Trace

Capture utilities

- FTD ASA Engine Capture
- FTD Snort Engine Capture
- FXOS internal switch Capture



Get knowing the tools

Logging utilities

- FTD ASA Engine logs
- FTD Snort Engine logs
- FXOS logs

Debug utilities

- FTD ASA Engine Debugs
- FTD Snort Engine Debugs
- FXOS Cisco Interactive Debug (TAC only)

Tracing utilities

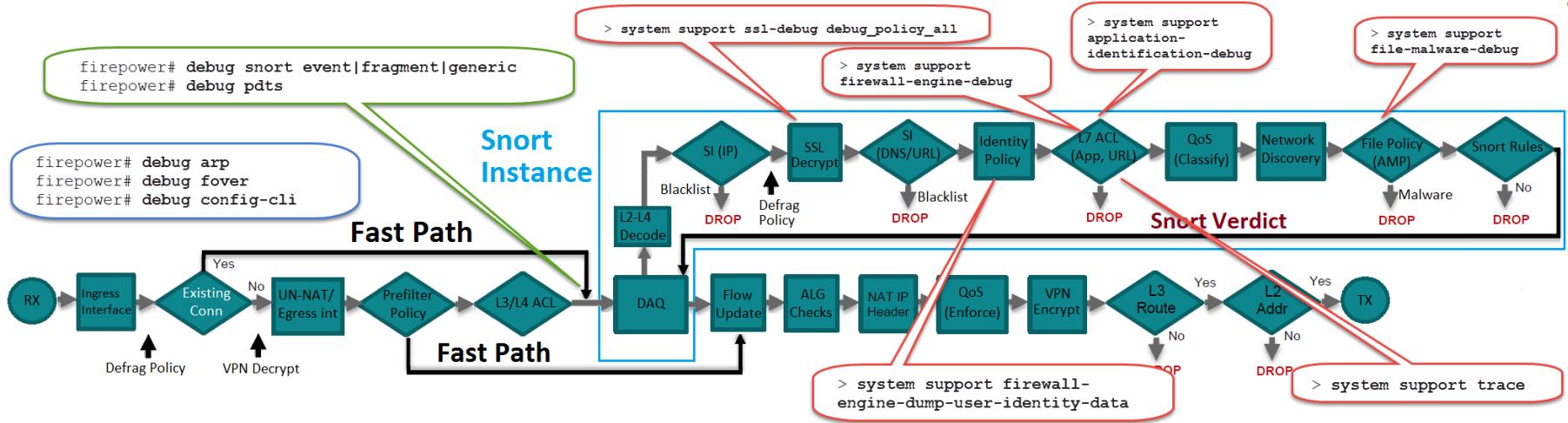
- FTD Packet-Tracer
- FTD ASA Engine Capture w/Trace

Capture utilities

- FTD ASA Engine Capture
- FTD Snort Engine Capture
- FXOS internal switch Capture



FTD Debugs



- FTD debugs can be categorized in 3 types
 1. LINA Engine Control-Plane debugs
 2. LINA Engine Data-Plane debugs
 3. Snort Engine Data-Plane debugs



Get knowing the tools

Logging utilities

- FTD ASA Engine logs
- FTD Snort Engine logs
- FXOS logs

Debug utilities

- FTD ASA Engine Debugs
- FTD Snort Engine Debugs
- FXOS Cisco Interactive Debug (TAC only)

Tracing utilities

- FTD Packet-Tracer
- FTD ASA Engine Capture w/Trace

Capture utilities

- FTD ASA Engine Capture
- FTD Snort Engine Capture
- FXOS internal switch Capture

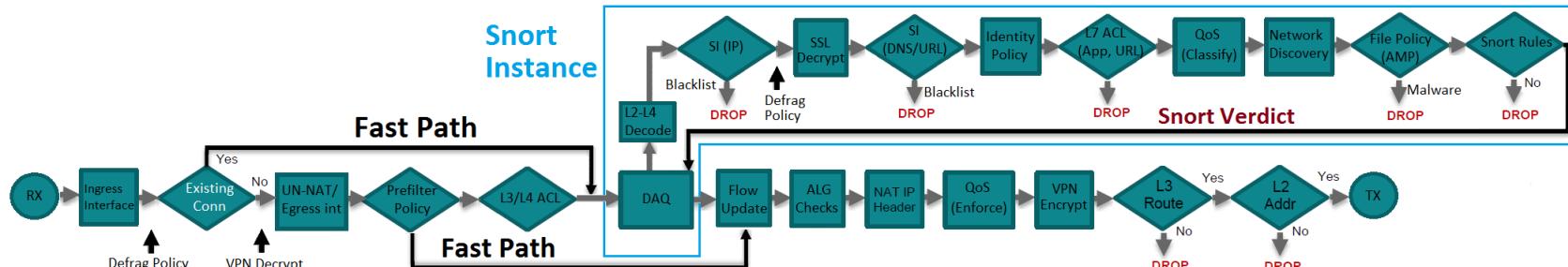


Packet Tracer

- Test policy configuration by modeling a packet based on source/destination address and protocol characteristics.
- Policy lookup to test:
 - access rules
 - NAT
 - Routing
 - Access policies
 - Rate limiting
- Packet flow based on:
 - Interfaces
 - SA/DA
 - Ports and protocols



FTD Data-Plane - Packet-Tracer



- Packet-tracer shows the LINA Engine Datapath checks done on a virtual packet

Advanced Troubleshooting

NGFW1

File Download Threat Defense CLI Packet Tracer Capture w/Trace

Select the packet type and supply the packet parameters. Click start to trace the packet.

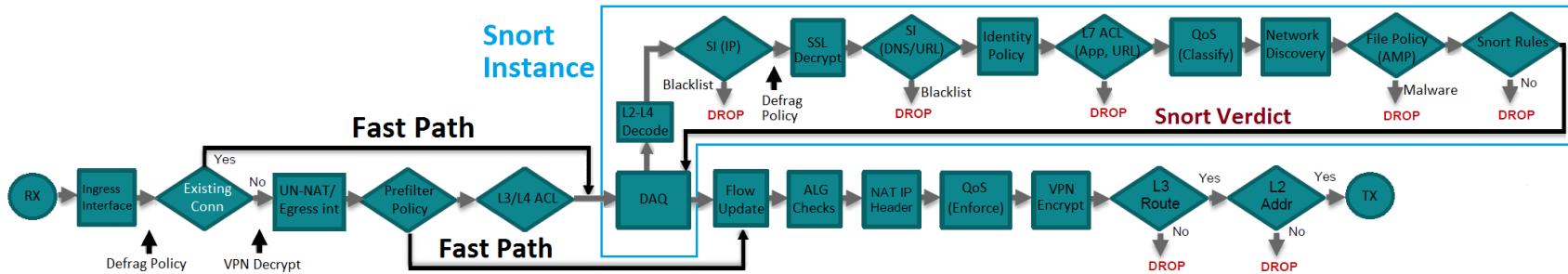
Packet type:	TCP	Interface*:	In10
Source*:	IP address (IPv4)	Source Port*:	Select or enter...
Destination*:	IP address (IPv4)	Destination Port*:	Select or enter...
SGT number:	SGT number... (0-65535)	VLAN ID:	VLAN ID... (1-4096)
Output Format:	summary	Destination MAC Address: 000C.0000.0000	

Source interface

summary, detailed or xml format

Clear Start

FTD Data-Plane - Packet-Tracer



When to use Packet-Tracer:

- To verify if traffic to a specific port is allowed by LINA Engine Data-path and Snort

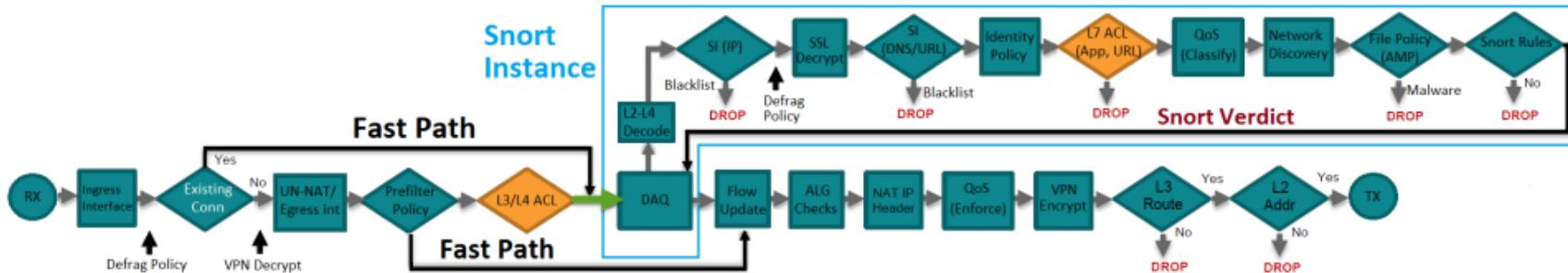
Examples of Snort features that **can be verified** by Packet-Tracer:

- Security Intelligence (IP Reputation)
- L3/L4 IPS Intrusion Rules

Examples of Snort features that currently **cannot** be verified by Packet-Tracer:

- L7-related (SI DNS/URL, App ID, File Policy, L7 IPS Intrusion Rules)
- Identity-based rules

FTD Packet Processing: L3/L4 ACL - Allow



- packet-tracer shows that LINA engine will send the packet to Snort engine for a Verdict

```
> packet-tracer input inside icmp 1.1.1.1 8 0 2.2.2.2

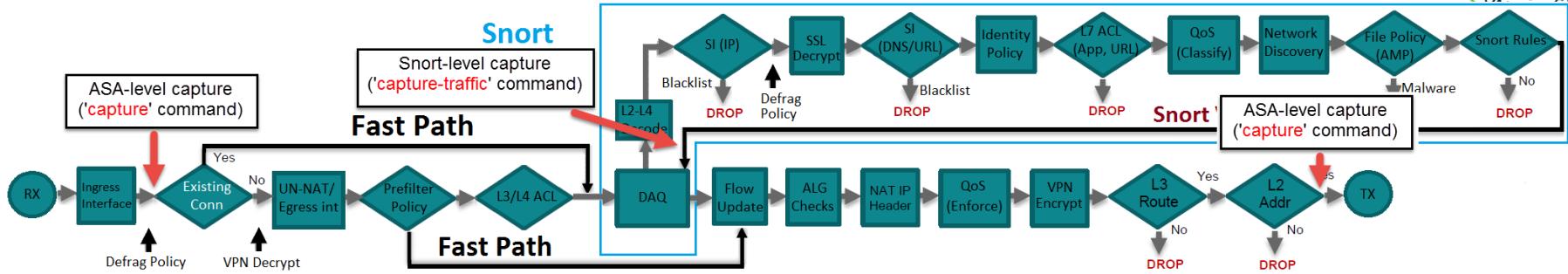
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 1.1.1.1 host 2.2.2.2 rule-id 268435456
access-list CSM_FW_ACL_ remark rule-id 268435456: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268435456: L7 RULE: ACP_Rule1_Allow_ICMP_App
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
```



Packet Capture

- Allows Real packets that are captured on ingress interface to be traced through the system
- Includes information from Snort and preprocessors about verdicts and actions
- Multiple packet captures are possible at a time
- Can modify, delete, clear and save captures
- Traffic data can be downloaded in pcap or ASCII format

FTD Captures



- FTD provides 2 types of captures
 1. LINA-level capture – ‘**capture**’ command
 2. Snort-level capture – ‘**capture-traffic**’ command
- Where do these captures take place?
- capture-traffic** command can be also used to capture FTD **control-plane** traffic (br1, management0)



FTD Data-Plane – Capture + Capture w/Trace

Add Capture

Name: CAPI Interface: in10

Match Criteria:

Protocol: IP

Source Host: 198.19.10.200 Source Netmask: 255.255.255.255

Destination Host: 198.18.133.200 Destination Netmask: 255.255.255.255

SGT number: 0 (0-65535)

Circular buffer

Buffer:

Packet Size: 1518 14-1522 bytes

Buff. Size: 524288 1534-33554432 bytes

Continuous Capture

Stop when full

Trace

Trace Count: 128

Cancel Save

Source interface

IP Protocol

Trace ingress packets

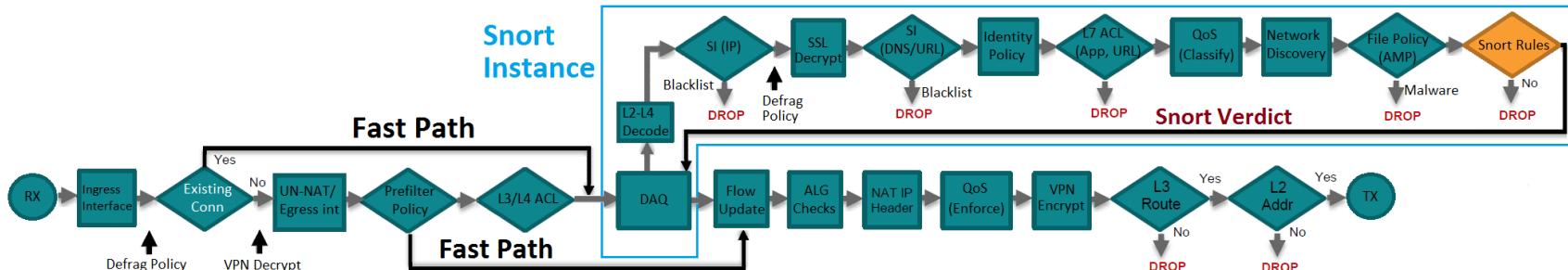
Current GUI limitations

- Cannot specify Src and Dst ports
- Only basic IP Protocols can be matched
- Cannot enable capture for LINA Engine ASP Drops

Workaround – Use the FTD CLI



FTD Packet Processing: Intrusion Policy



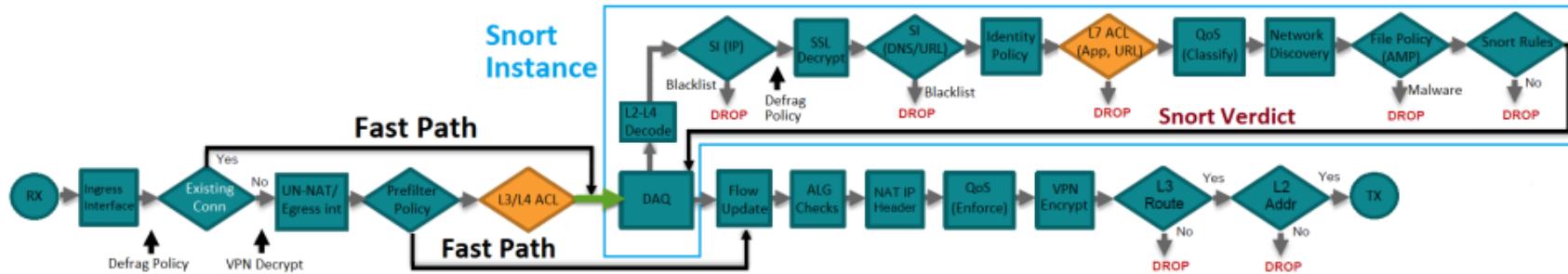
- Intrusion Policy (Snort Rules) is the same as on classic Firepower devices
- Packets marked as dropped by a Snort Rule (Signature) can be tracked by:
 1. FMC GUI (Connection Events, Intrusion Events)
 2. Capture with Trace:

```
> show cap CAPI%intf=INSIDE% trace | in Drop
Drop-reason: (ips) Blocked or blacklisted by the IPS preprocessor
```

3. From CLISH mode using 'system support trace'

```
> system support trace
192.168.0.10-45988 > 192.168.2.10-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.0.10-45988 > 192.168.2.10-80 6 AS 1 I 12 Deleting session
192.168.0.10-45988 > 192.168.2.10-80 6 NAP id 2, IPS id 1, Verdict BLACKLIST
192.168.0.10-45988 > 192.168.2.10-80 6 ===> Blocked by IPS
```

FTD Packet Processing: L3/L4 ACL - Allow



- Tracing a real packet will show the Snort Verdict

```
> show capture CAPI packet-number 1 trace
1: 09:17:18.996149      1.1.1.1 > 2.2.2.2: icmp: echo request
!
Phase: 4
Type: ACCESS-LIST
...
This packet will be sent to snort for additional processing where a verdict will be reached
!
Phase: 13
Type: EXTERNAL-INSPECT
...
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
...
Snort Verdict: (pass-packet) allow this packet
```



FTD Data-Plane – Capture + Capture w/Trace

As from 6.2 release the capture can **trace Snort** features known as **preprocessors** and get the verdict:

```
> show capture CAPI packet-number 6 trace
..
Type: SNORT
Result: DROP
Additional Information:
Packet: TCP, ACK, seq 157078375, ack 664745083
AppID: service HTTP (676), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 655
username 'No Authentication Required', , url http://192.168.2.10/image.bmp
Firewall: block rule, 'Rule1' , drop
Snort: processed decoder alerts or actions queue, drop
NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow..
..
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor
```

The Snort ACP Rule that triggered the Drop Verdict

The Snort Verdict

The Drop Reason



FTD Data-Plane – Capture w/Trace

Snort Verdicts of Capture w/Trace and possible Root Causes

Drop Reason	Possible Root Cause
(firewall) Blocked by the firewall preprocessor	The packet is dropped by Snort ACL Block rule. Check 'system support firewall-engine-debug' to confirm this
(ips) Blocked the IPS preprocessor	The packet is dropped by a Signature from the Snort Intrusion Policy
(file-process) Blocked by the file process preprocessor	The packet is dropped by Snort File Policy
(reputation) Blocked by the reputation preprocessor	The packet is dropped by the Snort Security Intelligence (SI)
(snort-drop) Snort requested to drop the frame	The packet matches an existing LINA Engine flow. Check the first packet of the flow that was blocked to see the full verdict

ACP L7 Rule

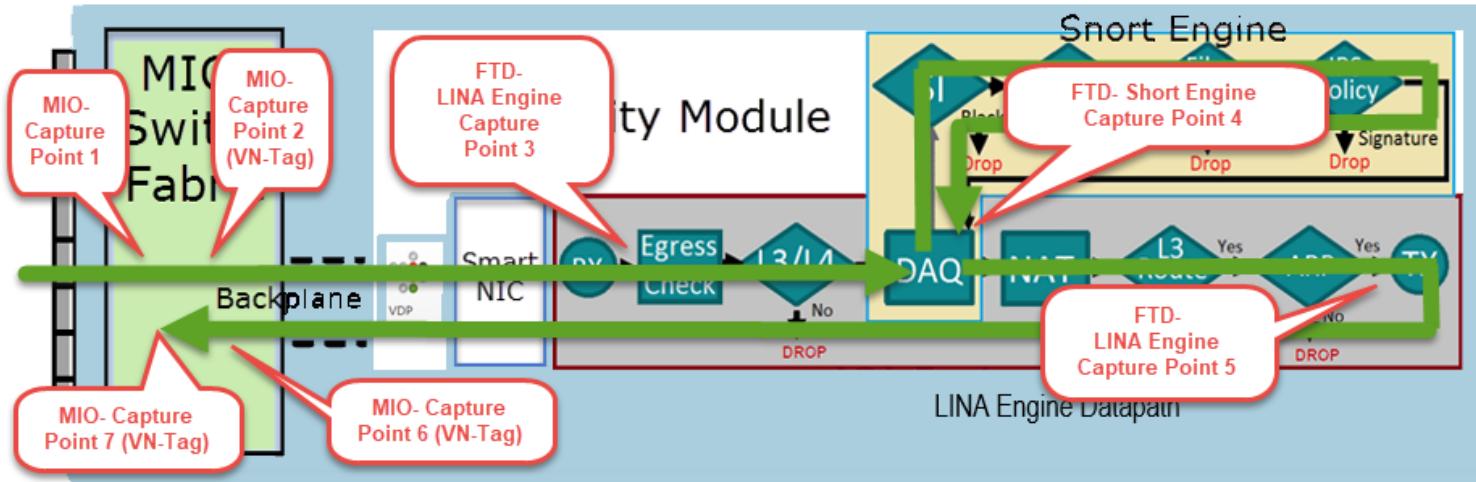
Intrusion Policy

File Policy

SI (IP reputation)

Existing
LINA Engine
flow

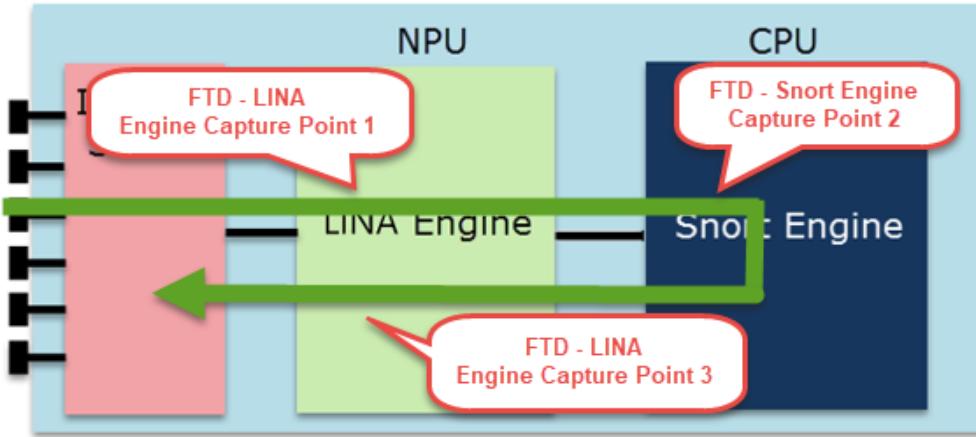
FXOS and FTD Capture Points



1. MIO – Ingress Capture Point 1 – The packet doesn't have any VN-Tag
2. MIO – Ingress Capture Point 2 – The packet has a VN-Tag
3. FTD – Ingress Capture Point 3 – The LINA Engine receives the packet
4. FTD – Capture Point 4 – The Snort Engine processes the packet
5. FTD – Egress Capture Point 5 – On LINA Engine egress interface
6. MIO – Capture Point 6 – The MIO Backplane receives the packet (Ingress)
7. MIO – Capture Point 7 – The MIO processes the packet (Ingress)

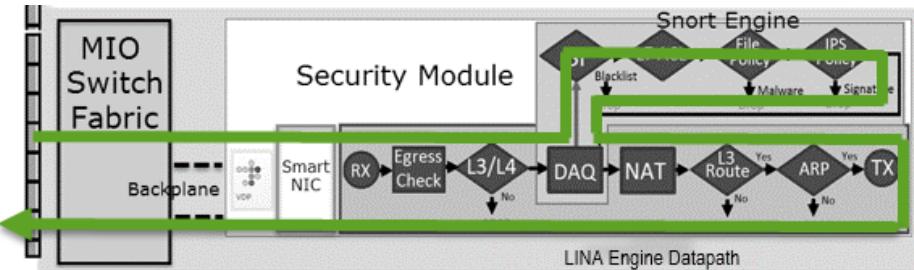
FTD Capture Points on FP2100

FTD on FP2100



1. The packet arrives on the Internal Switch – no Capture capabilities
2. FTD – Ingress Capture Point 1 – The LINA Engine receives the packet
3. FTD – Capture Point 2 – The Snort Engine processes the packet
4. FTD – Egress Capture Point 3 – On LINA Engine egress interface
5. The packet arrives on the Internal Switch – no Capture capabilities

FTD-FXOS Data-Plane – Troubleshooting Check List



#	TSHOOT Check	Result
Check 1	Ingress traffic reaches the FXOS chassis (MIO switch fabric)?	✓
Check 2	Traffic reaches the FTD ingress interface?	✓
Check 3	Problems in the LINA Engine Datapath (before Snort Inspection)?	✓
Check 4	Traffic requires Snort inspection?	✓
Check 5	Traffic reaches the Snort Engine?	✓
Check 6	Snort Verdict to LINA Engine Datapath?	✓
Check 7	Problems in the LINA Engine Datapath (after Snort Inspection)?	✓
Check 8	Traffic exits the FTD LINA Engine Datapath?	✓
Check 9	Egress traffic reaches the FXOS chassis (MIO switch fabric)?	✓
Check 10	Traffic exits the FXOS chassis?	✓

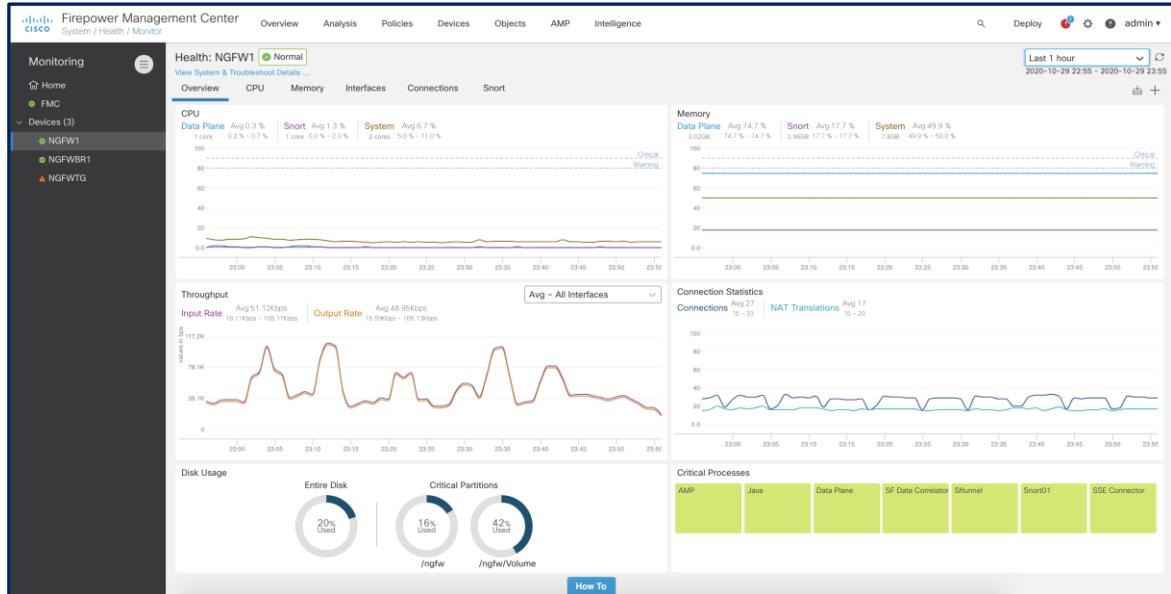
Health Monitoring Dashboard



Unified Stats from the device sub-systems and critical processes

Features

- Trend charts, overlays and custom dashboards
- Enhanced Live monitoring including failover and cluster status
- Unified Dataplane & Snort Metrics (E.g. CPU, Memory)
- Snort, Configuration, Connection & Process statistics reporting
- Available over API



Health Monitor Reports for Troubleshooting



This option...	Reports...
Snort Performance and Configuration	data and configuration settings related to Snort on the appliance
Hardware Performance and Logs	data and logs related to the performance of the appliance hardware
System Configuration, Policy, and Logs	configuration settings, data, and logs related to the current system configuration of the appliance
Detection Configuration, Policy, and Logs	configuration settings, data, and logs related to detection on the appliance
Interface and Network Related Data	configuration settings, data, and logs related to inline sets and network configuration of the appliance
Discovery, Awareness, VDB Data, and Logs	configuration settings, data, and logs related to the current discovery and awareness configuration on the appliance
Upgrade Data and Logs	data and logs related to prior upgrades of the appliance
All Database Data	all database-related data that is included in a troubleshoot report
All Log Data	all logs collected by the appliance database
Network Map Information	current network topology data



Operations System User Management

- Firepower System lets you allocate user privileges based on user roles.
- Predefined roles
- Custom user roles with custom access privileges

Operations System User Management



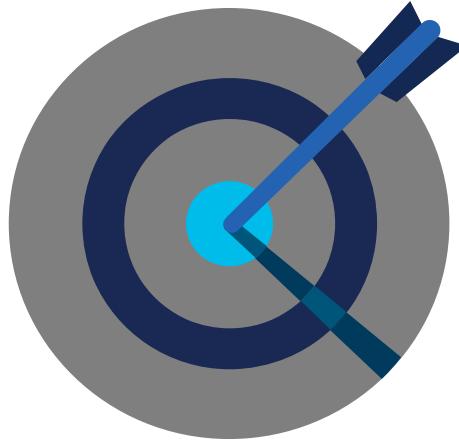
- **Predefined User Roles**
 - Access Admin
 - Administrator
 - Discovery Admin
 - External Database User
 - Intrusion Admin
 - Maintenance User
 - Network Admin
 - Security Analyst and Security Analyst (Read Only)
 - Security Approver
 - Threat Intelligence Director (TID) User
- **Custom User Roles can be made using any set of menu-based and system permissions**

TLS/SSL Decryption



Be Selective

- Reduced firewall throughput
- Many applications can break:
 - Public Key Pinning
 - Client certificate authentication
- Clients without Enterprise Certificate Authority trust will get browser errors
- Do not decrypt rules may require breaking sessions (client reset)





What not to Decrypt ?

- Enterprise SaaS applications
 - Office 365, Cloud Backups, etc
 - Cloud Infrastructure Services
 - Apple / Azure / AWS / GCP
- Traffic from personal devices on guest / segregated networks
- Trusted source networks
- Trusted / managed devices



Un-decryptable traffic types

Type	Description	Default Action	Available Action
Compressed Session	SSL session applies a data compression method	Inherit default action	DND, Block, BwR, Inherit Default
SSLv2 Session	Session is encrypted with SSL version 2	Inherit default action	DND, Block, BwR, Inherit Default
Unknown Cipher Suite	System does not recognize the cipher suite	Inherit default action	DND, Block, BwR, Inherit Default
Unsupported Cipher Suite	System does not support decryption based on the detected cipher suite	Inherit default action	DND, Block, BwR, Inherit Default
Session not Cached	Session has session reuse enabled. Client and Server reestablished with the session ID but system did not cache that Session ID	Inherit default action	DND, Block, BwR, Inherit Default
Handshake Errors	An error occurred during SSL handshake negotiation	Inherit default action	DND, Block, BwR, Inherit Default



Optimum Order of SSL policy rules evaluation

Monitor	Block/BwR	Do Not Decrypt	Decrypt Known Key	Decrypt with Resign
Phase 1 Rules that log matching connections, but take no other action on traffic	Phase 2 Rules that block traffic without further inspection.	Phase 3 Rules that do not decrypt encrypted traffic, passing the encrypted session to access control rules. The payloads of these sessions are not subject to deep inspection	Phase 4 Rules that decrypt incoming traffic with a known private key.	Phase 5 Rules that decrypt outgoing traffic by re-signing the server certificate.



Choosing the right decryption strategy

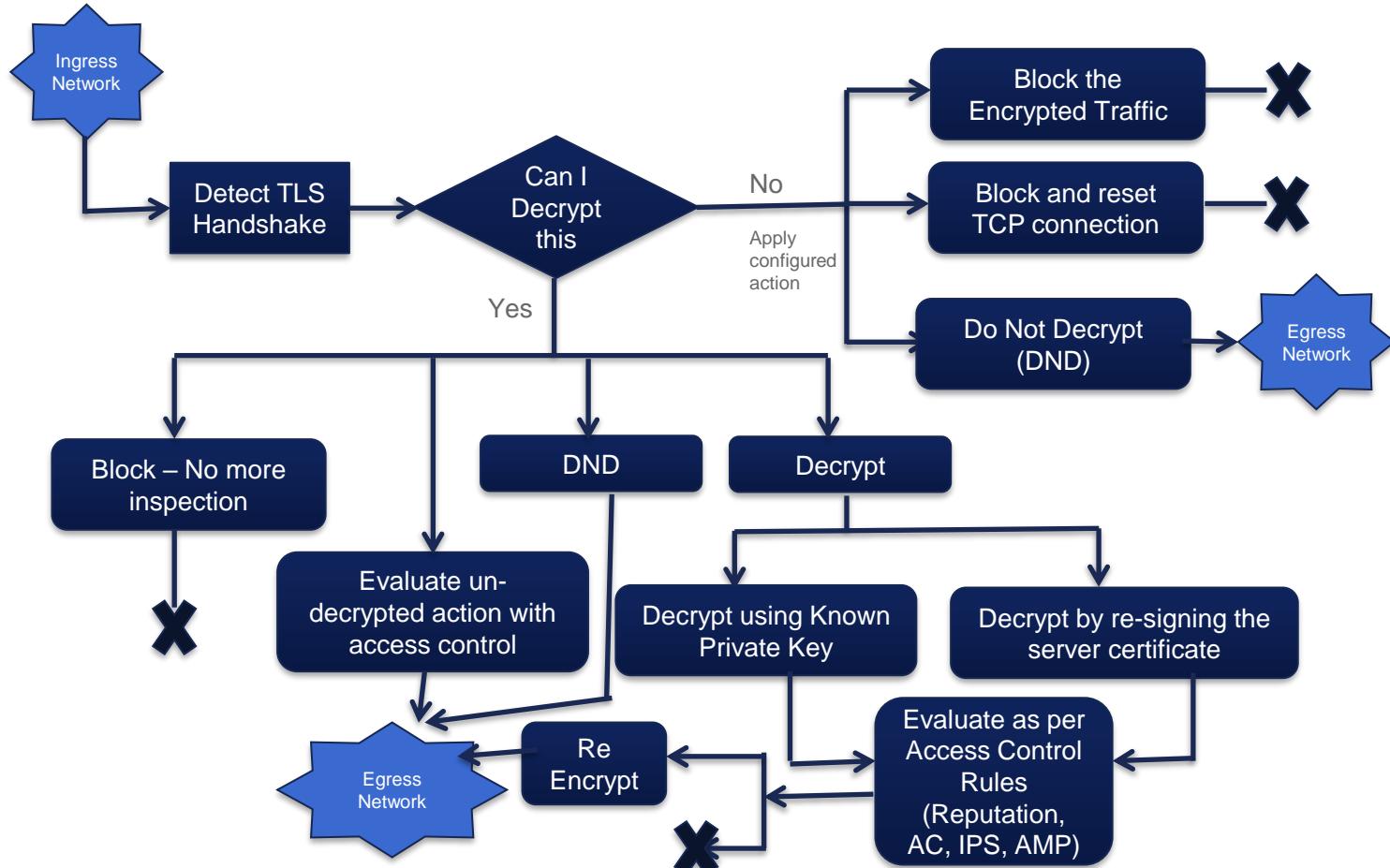
Decrypt with Known Key

- Protect the network from threats from remote TLS servers
- Rules that decrypt incoming traffic with a known private key
- Internal certificate object using the server's certificate file and paired private key file

Decrypt with Resign

- Protect the network from attacks on internal TLS servers
- Rules that decrypt outgoing traffic by re-signing the server certificate
- Internal Certificate Authority (CA) certificate and private key
- Client Hello modifications

SSL Flowchart





TLS 1.3 Server Identity Discovery

Over 90% of Internet traffic being encrypted with Transport Layer Security (TLS)

Mobile app and SaaS flows are not decryptable



TLS 1.3 encrypts Server Certificate Information

Effective Security Policy Evaluation relies on Server Name Indication and Server Certificate

TLS decryption has a steep performance impact

TLS 1.3 Server Identity Discovery

Server Identity Discovery makes Server Certificate Information available without performing decryption

More effective and reliable match for the TLS policy evaluation

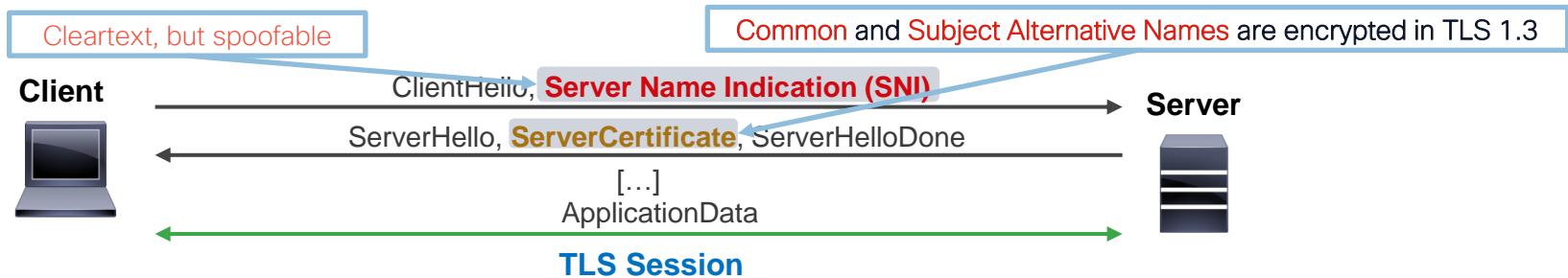
Detect and Block SNI Spoofing

Enhanced control and increased visibility into encrypted flows

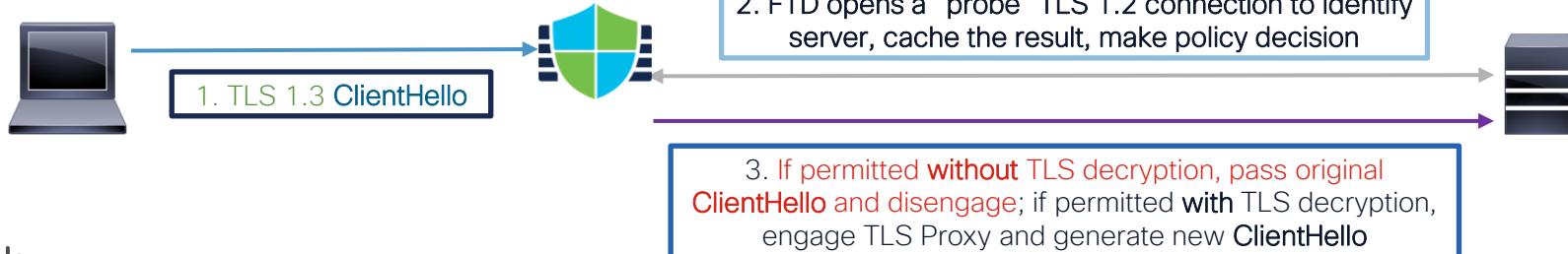


TLS 1.3 Server Identity Discovery How it works

- FTD makes AVC, URL, and “SSL” Policy decisions on pre-1.3 TLS header



- FTD can identify TLS 1.3 servers without decryption



Cisco Threat Intelligence Director (CTID)

Cisco Threat Intelligence Director on FTD



Helps to aggregate intelligence data



Additional line of defense against threats



Provides granular control of filtering actions



Changes don't require redeployment of policy



Benefits of Enabling CTID on FTD

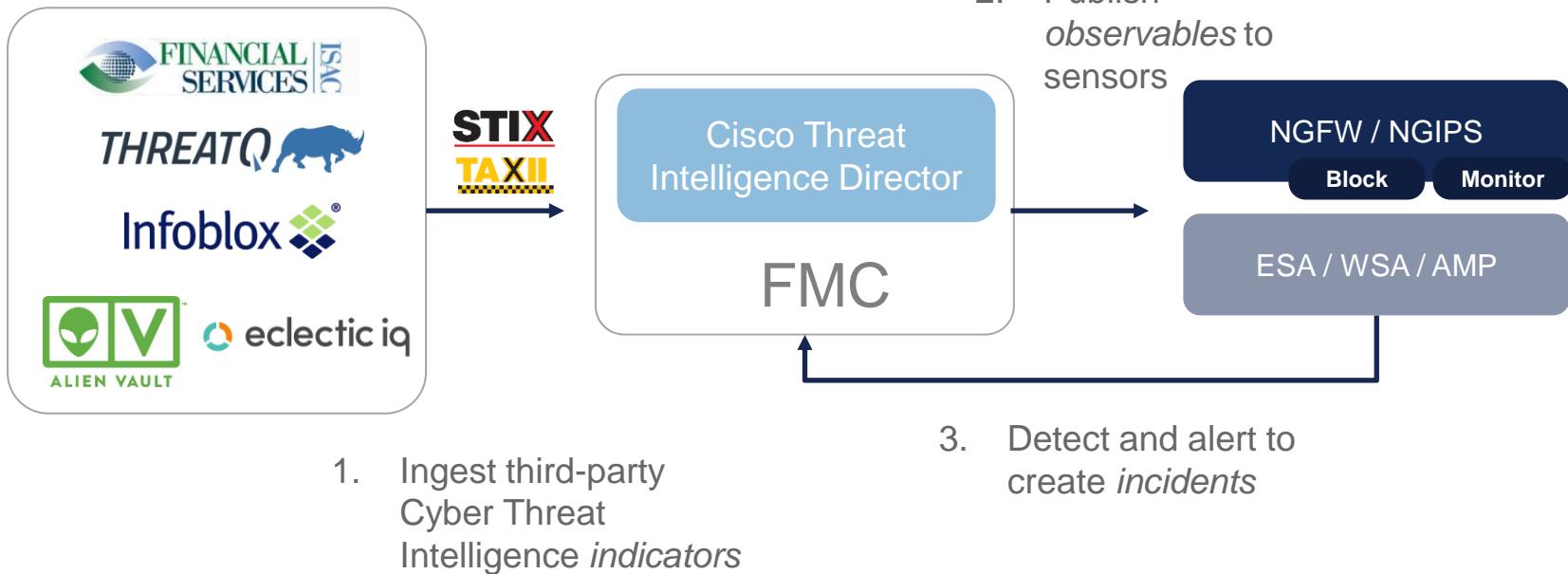
CTID adds support for filtering on SHA-256 hash values

TID can retrieve and ingest intelligence provided in Structured Threat Information eXpression (STIX™)

With TID, you can configure filtering actions for individual criteria (that is, simple indicators or individual observables)

You can configure sources, indicators, and observables without redeploying, and the system automatically publishes new TID data to the devices

Cisco Threat Intelligence Director (CTID)



CTID

Indicator 1: Simple Indicator

Observable A

Indicator 2: Complex Indicator, One Operator

Observable A

Observable B

AND

Indicator 3: Complex Indicator, Two Operators

Observable A

Observable B

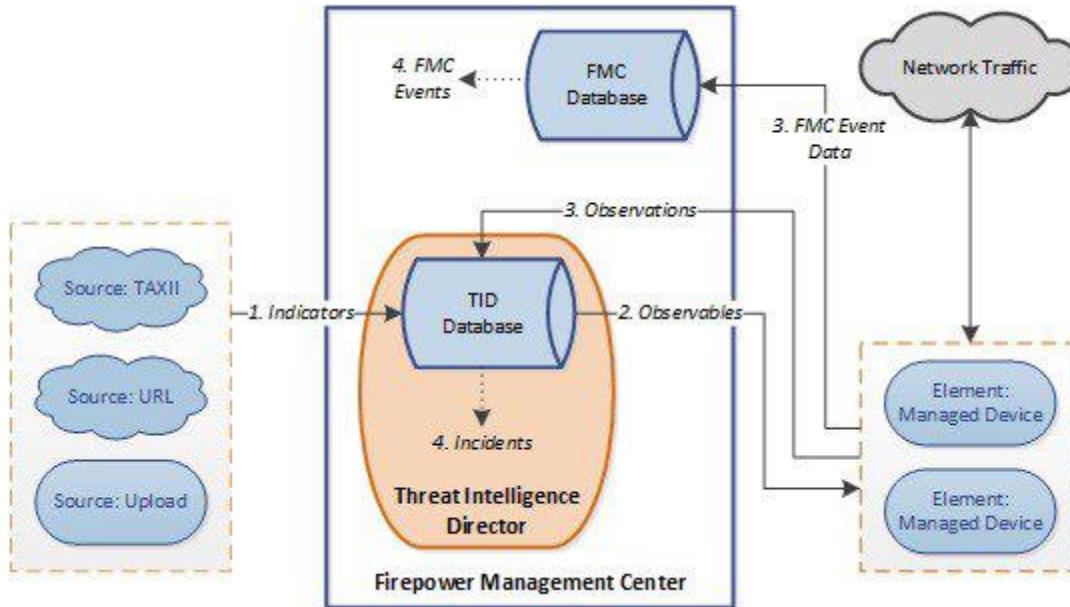
Observable C

OR

AND



CTID FMC Data Flow



Trusted Automated eXchange of Indicator Information (TAXII™)



- Transport mechanism for STIX
- Standardizes the automated exchange of cyber threat information
- Free
- Open Source



Hail a TAXII !!



- Free source of TAXII feeds
- Website URL: <http://hailataxii.com>
- Multiple feeds
- To configure the TAXII intelligence source
 - URL: <http://hailataxii.com/taxii-discovery-service>
 - USERNAME: guest
 - PASSWORD: guest



The screenshot shows the homepage of the Hail a TAXII website. At the top, there is a large yellow banner with the text "HAIL A TAXII" in white, surrounded by red flame-like graphics. Below the banner, the text "Poll to Start." is visible. The main content area has a white background. It includes sections titled "WHAT IS IT?", "AVAILABLE FEEDS", "HOW TO CONNECT", and "CONTACT US".

WHAT IS IT?
Hail a TAXII.com is a repository of Open Source Cyber Threat Intelligence feeds in STIX format. There are currently 727165 indicators, last updated Wed Jan 11 16:25:00 2017 UTC.

AVAILABLE FEEDS

```
guest Abuse_ch  
guest CyberCrime_Tracker  
guest EmergingThreats_rules  
guest Lehigh_edu  
guest MalwareDomainList_Hostlist  
guest blutmagie_de_torExits  
guest dataForLast_7daysOnly  
guest dshield_Blocklist  
guest phishtank_com
```

HOW TO CONNECT
Our data is accessible via the TAXII-HTTP Message Protocol. (1.0 & 1.1)
The discovery service is located at <http://hailataxii.com/taxii-discovery-service>
Anonymous connections are accepted.
Clients that require login details can use HTTP-Basic user=guest, password=guest.

CONTACT US
For questions or comments, please contact us using info@hailataxii.com.

TID Common Issues

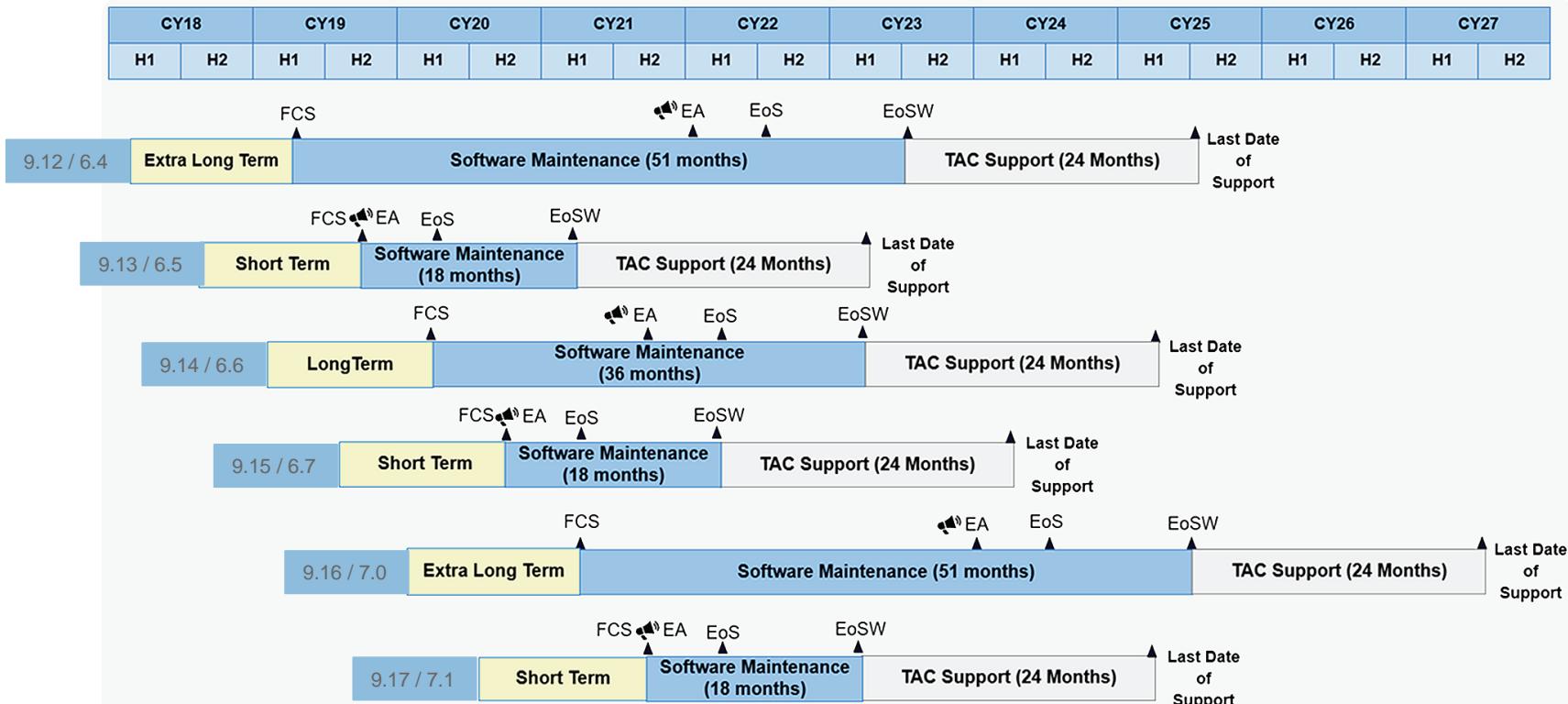


- Fetching or uploading flat file sources generates an error
- TAXII or URL source update generates an error
- TID table views return “No results”
- System is experiencing slowness or decreased performance
- FMC table views do not show TID data
- One or more elements are overwhelmed by TID data
- System is performing a Malware Cloud Lookup instead of a TID block
- System is performing a Security Intelligence or DNS Policy action instead of a TID action
- REST API is disabled
- TID is disabled

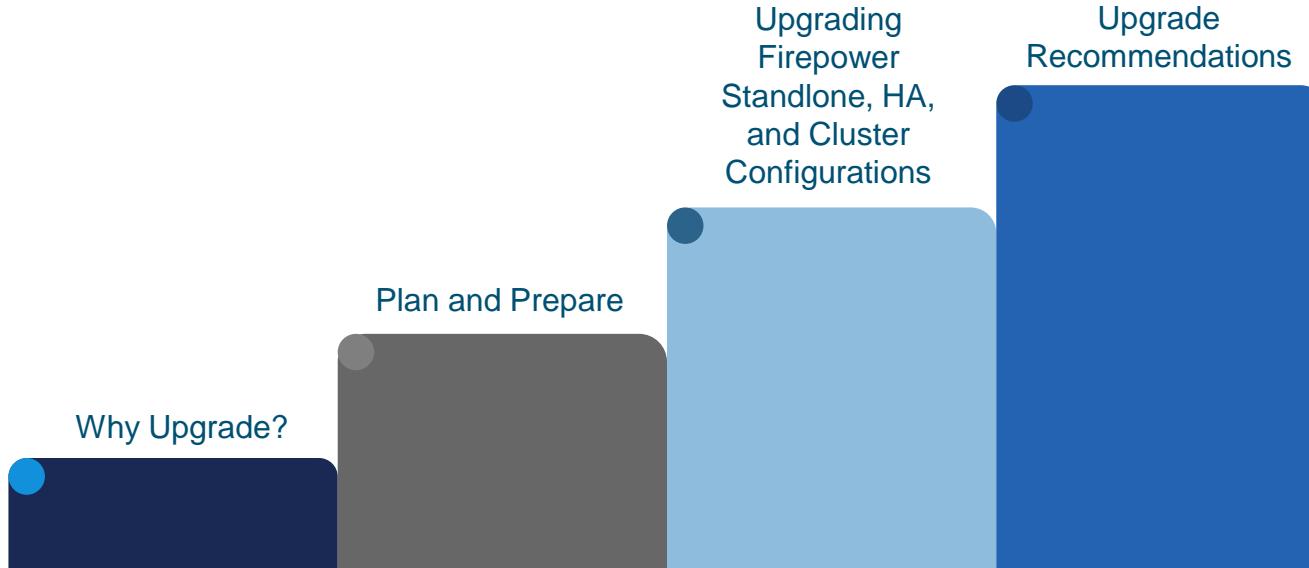
Upgrade FMC, FTD, and FXOS



ASA/FTD Release Lifecycle



What you'll learn today to help you on your NGFW upgrade journey





FMC: Software upgrade improvements

Estimated Time For Upgrade

for upgrades to major releases

FTD can pull updates from specific URL

- No need for FMC to download update
- Only for updates for 6.6 and above

The screenshot shows the FMC interface with the following details:

- Header:** Deploy, admin, Show Notifications (on).
- Task Overview:** Deployments, Health, Tasks (selected). 1 total, 0 waiting, 1 running, 0 retrying, 0 success, 0 failures.
- Task Details:** Local Install, Installing Cisco Firepower Mgmt Center Upgrade version: 6.6.0-68, [3%] [44 mins to go for reboot], Running script 000_start/101_run_pruning.pl... (status bar shows 2m 28s).
- Message:** No more older tasks.
- Bottom Panel:** System / Updates, Product Updates (selected), Rule Updates, Geolocation Updates. Currently running software version: 6.6.0. Updates section: Action (radio buttons for Upload local software update package and Specify software update source (FTD devices only) (selected)), Source URL: http://web-server.cisco.com/Cisco, CA Certificate(s) (required for HTTPS) (empty field).



Firepower Software Upgrade Types



Major updates



Minor updates



Hotfixes

Major upgrades



- New features and functionality
- Changes the first, second, or third digit of the version number
- Can be freshly installed / restored
- Likely to have companion operating system upgrades
- Cannot be uninstalled
- Will require a reboot

File Information	Release Date	Size	
Firepower Threat Defense upgrade Do not untar Cisco_FTD_SSP_FP2K_Upgrade-7.0.0-94.sh.REL.tar Advisories	26-May-2021	898.63 MB	





Minor upgrades/patches



- ✓ Limited range of fixes
- ✓ Changes the fourth digit of the version number
- ✓ Can be uninstalled
- ✗ Cannot be freshly installed (install previous major patch first)
- ✗ Will require a reboot

File Information	Release Date	Size	
Firepower Threat Defense Patch 6.7.0.2 Do not untar	11-May-2021	655.45 MB	

[Cisco_FTD_SSP_FP2K_Patch-6.7.0.2-24.sh.REL.tar](#)
[Advisories](#)





Hotfixes



- ✓ Urgent updates released outside the patch release cycle
- ✓ Addresses one specific problem
- ✓ May not require a reboot.

File Information

Release Date

Size

Firepower Threat Defense Hotfix 6.5.0 O
Do not untar

06-Aug-2020

46.18 MB



Cisco_FTD_SSP_FP2K_Hotfix_O-6.5.0.5-3.sh.REL.tar
Advisories ↗





FTD Upgrade



Why Upgrade to FTD 7.0

- FMCv, FTDv, NGIPSV, support for VMware vSphere ESXi 7.0 (Vmware 6.0 discontinued)
- FMCv, FTDv, support Cisco HyperFlex, OpenStack, Nutanix Enterprise Cloud
- FTDv support performance-tiered Smart Licensing
- RA VPN Load balancing
- Backup VTI (Virtual Tunnel Interface) for site-to-site VPN
- Snort 3 for FTD for FMC is default
- Dynamic Objects
- Unified Event Viewer



Why Upgrade to FTD 7.0

- Improved upgrade performance and status reporting
- Upgrade Wizard
- Upgrade more devices at once recommendation was 5 in 6.6
- Selectively deploy RA and site-to-site VPN policies
- New Health Modules
- New default password for AWS
- Search for policies and objects by name
- Hardware crypto acceleration of FTDv using Intel QuickAssist Technology (QAT)



Why Upgrade to 7.0 FDM

- Custom intrusion rules for Snort 3
- Snort 3 new features for FDM
- DNS request filtering based on URL category and reputation
- SSL cipher setting for RA VPN
- VTI (Virtual Tunnel Interface) increased to 1024
- Equal-Cost Multi-Path routing (ECMP)
- New default inside IP address: 192.168.95.1
- Performance-Tiered Licensing
- Faster bootstrap processing and early login to FDM
- Upgrade readiness check for FDM Managed devices

Upgrading NGFW

Plan & Prepare

Upgrade

Deployment Assessment | Compatibility Checks |
Pre-Upgrade Activities



Deployment Assessment



Questions to ask before you begin

What appliances and Firepower versions do I have?

What version do I want to run and does it require a separate OS upgrade?

Am I using a standalone Firepower Management Center (FMC), or a pair in high availability (HA)?

Are my managed devices standalone, clusters, and/or HA pairs of devices?

Are my devices deployed passively, as an intrusion prevention system (IPS inline), or as a firewall?



Compatibility Checks (7.0.x)

Supported Hardware



Firepower 21xx
Firepower 1020 /1120 /1140/1150
Firepower 4100/9300 (2.8.1.105+*)
ASA 5508-X /5516-X
ISA 3000

Management



FMC->FTD (Covered In Detail)

FMC Physical :

FMC 1600/2600/4600
FMC 1000/2500/4500
ASDM 7.14.1 > ASA Firepower module



Supported Virtual Environments



MC / FTD

- VMware ESXi 6.5-7.0
- AWS/KVM/Azure

Compatibility with Other Product



ISE 3.0/2.7 patch 2+

ISE PIC 3.0/2.7 patch 2+

Cisco Defense Orchestrator (CDO)

Cisco Threat Response (CTR)

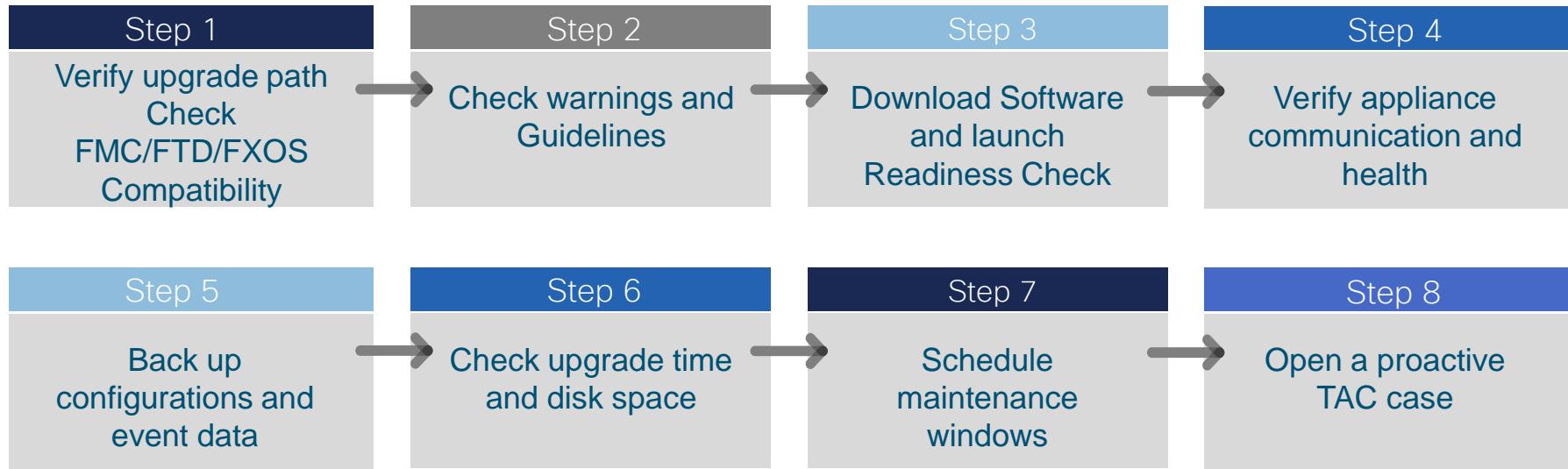


FMC and Device version Compatibility

FMC Version	Can Manage: Device Version										
	7.0.x	6.7.x	6.6.x	6.5.0	6.4.0	6.3.0	6.2.3	6.2.2	6.2.1	6.2.0	6.1.0
7.0.x	YES	YES	YES	YES	YES	–	–	–	–	–	–
6.7.x	–	YES	YES	YES	YES	YES	–	–	–	–	–
6.6.x	–	–	YES	YES	YES	YES	YES	–	–	–	–
6.5.0	–	–	–	YES	YES	YES	YES	–	–	–	–
6.4.0	–	–	–	–	YES						
6.3.0	–	–	–	–	–	YES	YES	YES	YES	YES	YES
6.2.3	–	–	–	–	–	–	YES	YES	YES	YES	YES



Pre-Upgrade Activities for NGFW & FMC





Step 1 : Verify Upgrade path – 7.x

Table 2. Minimum Version to Upgrade to Version 7.0.0/7.0.x

Platform	Minimum Version
FMC	6.4.0
FTD	6.4.0 FXOS 2.10.1.159 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1) .
ASA with FirePOWER Services	6.4.0 ASA 9.5(2) through 9.16(x) is required. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the Cisco ASA Release Notes .
NGIPSV	6.4.0



FMC Recommended Upgrade Paths

Table 2. Minimum Version to Upgrade to Version 7.0.0/7.0.x

Platform	Minimum Version
FMC	6.4.0
FTD	6.4.0 <p>FXOS 2.10.1.159 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1).</p>
ASA with FirePOWER Services	6.4.0 <p>ASA 9.5(2) through 9.16(x) is required. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the Cisco ASA Release Notes.</p>
NGIPSV	6.4.0



Step 2: Check Warnings and Guidelines

Table 5. FMCv Memory Requirements for Version 6.6.0+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.
AWS	Resize instances: <ul style="list-style-type: none">• From c3.xlarge to c3.4xlarge.• From c3.2.xlarge to c3.4xlarge.• From c4.xlarge to c4.4xlarge.• From c4.2xlarge to c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.
Azure	Resize instances: <ul style="list-style-type: none">• From Standard_D3_v2 to Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

Step 3: Download Software



File Information

	Release Date	Size	
Firepower NGFW Virtual v7.0.0 on Azure	06-Jul-2021	918.97 MB	
Cisco_Firepower_Threat_Defense_Virtual-7.0.0-94.vhd.bz2			
Advisories			
Firepower Threat Defense upgrade	26-May-2021	969.18 MB	
Do not update			
Cisco_FTD_Upgrade-7.0.0-94.sh.REL.tar			
Advisories			
FTDv: KVM install package	26-May-2021	1046.13 MB	
Cisco_Firepower_Threat_Defense_Virtual-7.0.0-94.qcow2			
Advisories			
FTDv: VMware install package for ESXi 6.5, 6.7, or 7.0	26-May-2021	1029.40 MB	
Cisco_Firepower_Threat_Defense_Virtual-7.0.0-94.tar.gz			
Advisories			

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.0.0
Currently Installed VDB version: build 344 (2021-07-01 01:57:30)

[Download Updates](#) [Upload Updates](#)

Type	Version	Date	Reboot	
Cisco Vulnerability And Fingerprint Database Updates	348	Tue Oct 12 12:58:46 UTC 2021	No	
Cisco Vulnerability And Fingerprint Database Updates	344	Thu Jul 1 01:58:54 UTC 2021	No	
Cisco Firepower Mgmt Center Upgrade	7.0.1-84	Tue Oct 5 03:37:31 UTC 2021	Yes	
Cisco FTD Upgrade	7.0.1-84	Tue Oct 5 04:14:09 UTC 2021	Yes	
Cisco FTD Upgrade	7.0.0-94	Tue May 25 19:14:06 UTC 2021	Yes	

<https://www.cisco.com/go/ftd-software>



Step 3: Download Software & launch Readiness Check

FMC Upgrade

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.0.0

Selected Update

Type	Cisco Firepower Mgmt Center Upgrade
Version	7.0.1-84
Date	Tue Oct 5 03:37:31 UTC 2021
Reboot	Yes

By Group

Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time	
<input checked="" type="checkbox"/> Ungrouped (1 total)	<div style="background-color: #e0f2e0; padding: 5px;">Compatibility check passed. Proceed with readiness check.</div>		28 min	
<input checked="" type="checkbox"/> fmc.deloud.local 192.168.10.120 - Cisco Firepower Management Center for VMware v7.0.0				

[Back](#) [Check Readiness](#) [Install](#)





Step 3: Download Software & launch Readiness Check

FMC Upgrade

The screenshot shows the FMC Tasks page. At the top, there are tabs for Deployments, Upgrades, Health, and Tasks, with Tasks selected. Below the tabs, a summary shows 1 total task, 0 waiting, 1 running, 0 retrying, 0 success, and 0 failures. A 'Show Notifications' toggle switch is on. A search bar with a 'Filter' placeholder is also present. The main area displays a single task card:

Local Install	Installing Cisco Firepower Mgmt Center Upgrade version: 7.0.1-84 Installing Cisco Firepower Mgmt Center Upgrade version: 7.0.1-84	1m 6s
---------------	--	-------

Below the task card, a message says "No more older tasks". At the bottom of the page is a button labeled "Remove completed tasks".





Step 3: Download Software & launch Readiness Check

FMC Upgrade

Logout

 Upgrade Status

Current Version: 7.0.0
Upgrade Version: 7.0.1
Elapsed Time: 7 minutes
Estimated Time Remaining: 22 mins to go for reboot

21 %

Running script 300_os/070_setup_partition.sh...
(show log for current script)

Step 3: Download Software & launch Readiness Check



<https://www.cisco.com/go/ftd-software>

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.0.0

Currently Installed VDB version: build 344 (2021-07-01 01:57:30)

Download Updates Upload Update

Available Updates Readiness History

Type	Version	Date	Reboot	
Cisco Vulnerability And Fingerprint Database Updates	348	Tue Oct 12 12:59:46 UTC 2021	No	
Cisco Vulnerability And Fingerprint Database Updates	344	Thu Jul 1 01:58:54 UTC 2021	No	
Cisco Firepower Mgmt Center Upgrade	7.0.1-84	Tue Oct 5 03:37:31 UTC 2021	Yes	
Cisco FTD Upgrade	7.0.1-84	Tue Oct 5 04:14:09 UTC 2021	Yes	
Cisco FTD Upgrade	7.0.0-94	Tue May 25 19:14:06 UTC 2021	Yes	

- Copies an upgrade package to managed devices
- Recommended to do it prior the upgrade
- Reduces upgrade time



Step 3: Download Software & launch Readiness Check

FTD Upgrade

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.0.1

Selected Update

Type: Cisco FTD Upgrade
Version: 7.0.1-84
Date: Tue Oct 5 04:14:09 UTC 2021
Reboot: Yes

Dismiss all notifications

Process Status - NGFWTG
The data correlator process exited 1 time(s).

By Group	
Ungrouped (3 total)	Compatibility Check
<input checked="" type="checkbox"/> HA_Test Cisco Firepower Threat Defense for VMware Cluster	Compatibility check passed. Proceed with readiness check. 10 min
<input checked="" type="checkbox"/> NGFW1 (active) 198.19.10.81 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check. 10 min
<input checked="" type="checkbox"/> NGFW3 198.19.10.83 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check. 10 min
<input type="checkbox"/> NGFWBR1 198.18.133.42 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check. 10 min
<input type="checkbox"/> NGFWTG 198.18.133.11 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check. 10 min

Back Push





Step 3: Download Software & launch Readiness Check

FTD Upgrade

A screenshot of the Cisco Firepower Threat Defense (FTD) interface. The top navigation bar includes tabs for Deployments, Upgrades, Health (with a red dot), and Tasks. The Tasks tab is selected, showing 14 total tasks. Below the tabs, there are four status indicators: 14 total, 1 waiting, 1 running, 0 retrying, 12 success, and 0 failures. A search bar labeled "Filter" is also present. Two tasks are listed under the "Tasks" section: "Push to NGFW1" (status: Pushing upgrade..., duration: 19s) and "Push to NGFW3" (status: Pushing upgrade..., duration: 19s). Both tasks are preceded by a blue circular icon with a white question mark.

A screenshot of the Cisco FTD interface showing the same view as the previous screenshot, but with completed tasks. The "Push to NGFW3" task is now listed as "Complete" with a green checkmark icon and a duration of 58s. The "Push to NGFW1" task is also listed as "Complete" with a green checkmark icon and a duration of 32s. Both completed tasks are highlighted with a red rectangular box.



Step 3: Download Software & launch Readiness Check

FTD Upgrade

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.0.1

Selected Update

Type	Cisco FTD Upgrade
Version	7.0.1-84
Date	Tue Oct 5 04:14:09 UTC 2021
Reboot	Yes

Automatically cancel on upgrade failure and roll back to the previous version (Applies to individual units in HA or Clusters)

	Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time	
<input type="checkbox"/> Ungrouped (3 total)					
<input checked="" type="checkbox"/> HA_Test Cisco Firepower Threat Defense for VMware Cluster	● Compatibility check passed. Proceed with readiness check.			10 min	█
<input checked="" type="checkbox"/> NGFW1 (active) 198.19.10.81 - Cisco Firepower Threat Defense for VMware v7.0.0	● Compatibility check passed. Proceed with readiness check.			10 min	█
<input checked="" type="checkbox"/> NGFW3 198.19.10.83 - Cisco Firepower Threat Defense for VMware v7.0.0	● Compatibility check passed. Proceed with readiness check.			10 min	█
<input type="checkbox"/> NGFWR1 198.18.133.42 - Cisco Firepower Threat Defense for VMware v7.0.0	● Compatibility check passed. Proceed with readiness check.			10 min	█
<input type="checkbox"/> NGFWTG 198.18.133.11 - Cisco Firepower Threat Defense for VMware v7.0.0	● Compatibility check passed. Proceed with readiness check.			10 min	█

Back Check Readiness Install

Step 3: Download Software & launch Readiness Check



FTD Upgrade

By Group				
	Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time
<input type="checkbox"/> <input type="checkbox"/> Ungrouped (3 total)				
<input type="checkbox"/> <input checked="" type="checkbox"/> HA_Test Cisco Firepower Threat Defense for VMware Cluster				
<input type="checkbox"/> NGFW1 (active) 198.19.10.81 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check.	<div style="border: 2px solid red; padding: 2px;">In-progress</div>		10 min
<input type="checkbox"/> NGFW3 198.19.10.83 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check.	<div style="border: 2px solid red; padding: 2px;">In-progress</div>		10 min

Step 3: Download Software & launch Readiness Check



FTD Upgrade

Firepower Management Center
System / Updates / [Upload Update](#)

Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🔍⚙️👤 admin ▾

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.0.1

Selected Update

Type	Cisco FTD Upgrade
Version	7.0.1-84
Date	Tue Oct 5 04:14:09 UTC 2021
Reboot	Yes

Automatically cancel on upgrade failure and roll back to the previous version (Applies to individual units in HA or Clusters)

Process Status – NGFW3
The synchronization daemon exited 1 time(s).

By Group					
Ungrouped (3 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time	Actions
<input type="checkbox"/> HA_Test	Compatibility check passed. Proceed with readiness check.	<div style="border: 1px solid red; padding: 2px;">Success</div>	2021-10-28 06:57:53	10 min	
<input checked="" type="checkbox"/> NGFW1 (active) 198.19.10.81 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check.	Success	2021-10-28 06:57:53	10 min	
<input checked="" type="checkbox"/> NGFW3 198.19.10.83 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check.	Success	2021-10-28 06:57:53	10 min	
<input type="checkbox"/> NGFWBR1 198.18.133.42 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check.			10 min	
<input type="checkbox"/> NGRWTG 198.18.133.11 - Cisco Firepower Threat Defense for VMware v7.0.0	Compatibility check passed. Proceed with readiness check.			10 min	

[Back](#) [Check Readiness](#) [Install](#)



Step 4: Verify Appliance Communication and Health



System > Health > Monitor

A screenshot of a web-based monitoring interface. At the top, there are tabs for "Deployments", "Upgrades", "Health" (which is highlighted with a red dot), and "Tasks". To the right of the tabs is a toggle switch for "Show Notifications" which is turned on. Below the tabs, a summary bar shows "3 total" items, with 0 warnings, 1 critical, and 0 errors. There is also a "Filter" search bar. The main content area displays a single critical alert: "Appliance Heartbeat" for device "fmc.dcloud.local". The alert message states: "Appliance NGFWBR1 is not sending heartbeats." and "Appliance NGFWTG is not sending heartbeats.".

Example of poor device health

A screenshot of a Cisco device configuration or status page. At the top, it shows a table with columns for "Name", "IP Address", "Software Version", "Status", and "Policy". The first row shows "NGFWTG" with IP "198.18.133.11 - Routed", software version "7.0.0", and status "N/A". The "Policy" column shows "Base, Threat (2 more...)" and a link to "TG Access Control Policy". Below the table, there is a progress bar consisting of several small circles, and the Cisco logo at the bottom left.



Step 5: Backup

System > Tools > Backup/Restore

Remote Storage

Backup Management Backup Profiles

Firepower Management Backups

<input type="checkbox"/> System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
Storage Location: /var/sf/backup/ (Disk Usage: 13%)								

Create Backup

Name

Storage Location

Back Up Configuration

Back Up Events

Back Up Threat Intelligence Director

Email *Not available. You must set up your mail relay host.*

Copy when complete

Managed Device Backup

NGFWBR1
NGFWTG

Managed Devices

Retrieve to Management Center

Storage Location: /var/sf/remote-backup

Note: Backup the Firepower 9300/4100 chassis configuration before initiating a backup of the logical Threat Defense devices configured on it.



Step 6: Check Time And Disk Space

Table 15. Version 7.0.0 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time	Reboot Time
FMC	14 GB 70 MB	in /Volume in /	—	41 min	7 min
FMCv	16 GB 72 MB	in /Volume in /	—	28 min	4 min
Firepower 1000 series	420 MB 7.6 GB	in /ngfw/var	890 MB	12 min	14 min
Firepower 2100 series	480 MB 7.7 GB	in /ngfw/Volume in /ngfw	950 MB	11 min	13 min
Firepower 9300	45 MB 11.1 GB	in /ngfw/Volume in /ngfw	830 MB	11 min	11 min
Firepower 4100 series	40 MB 8.4 GB	in /ngfw/Volume in /ngfw	830 MB	8 min	9 min
Firepower 4100 series container instance	36 MB 9.7 GB	in /ngfw/Volume in /ngfw	830 MB	8 min	7 min
ASA 5500-X series with FTD	5.3 GB 95 KB	in /ngfw/Volume in /ngfw	1.1 GB	25 min	12 min
FTDv	6.6 GB 23 KB	in /ngfw/Volume in /ngfw	1.1 GB	11 min	6 min
ASA FirePOWER	9.5 GB 64 MB	in /var in /	1.1 GB	69 min	8 min
NGIPSv	5 GB 54 MB	in /var in /	720 MB	8 min	4 min

Step 7: Schedule Maintenance Window



Use maintenance windows for updates and upgrades



Communicate about possible downtime



Schedule more time than you think

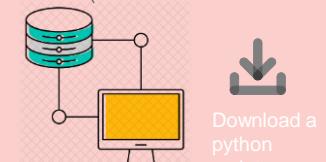
Step 8: Open A Proactive TAC Case



A large blue arrow points from the 'Support Case Manager' screenshot to the right towards the case creation form.



Cisco First Responder
...Please run the commands on the devices in question...



Cisco Customer eXperience Drive (CXD)

Run commands on FMC/FTD  

Download a python script.  

Upload troubleshoot file & Core Files generated in the past 30 days to the case 

Upgrading NGFW

Plan & Prepare

Upgrade

Upgrade Order | FMC Stand alone & HA|

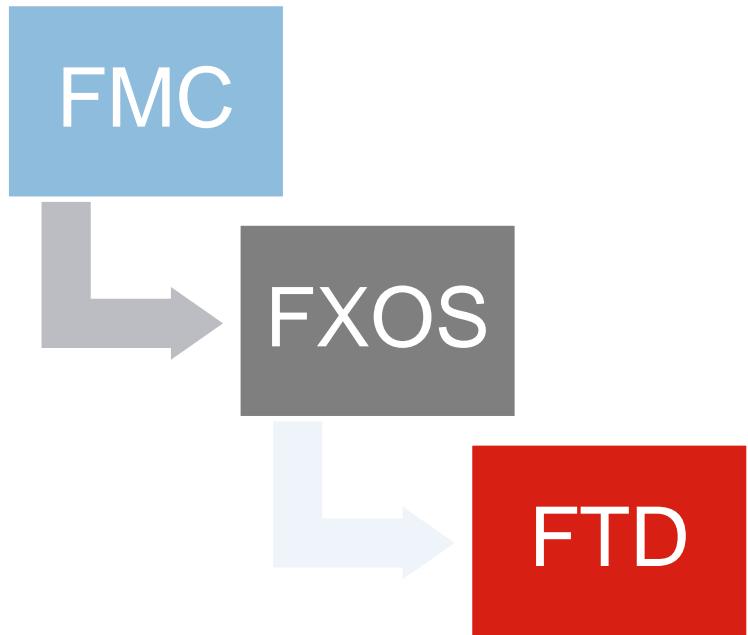
vFTD/2100/1100 standalone & HA| 4100s & 9300s

Standalone, HA, & Cluster





Upgrade Order





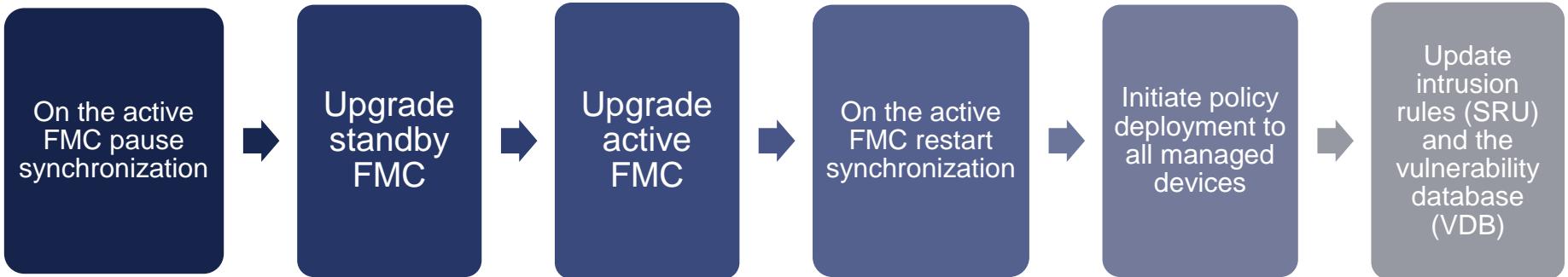
FMC Standalone



Do not make configuration changes or deploy to any device while the FMC is upgrading. do *not* restart the upgrade or reboot the FMC.

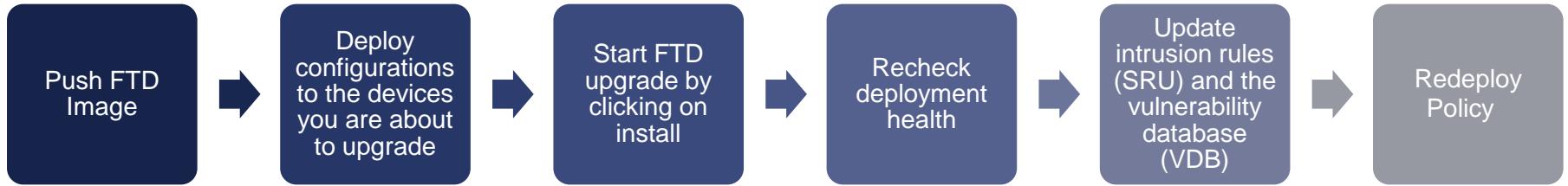


FMC HA





vFTD/2100/1100 Standalone & HA



We strongly recommend upgrading no more than five devices simultaneously!



Firepower 4100s & 9300s Standalone

Firepower Version	FXOS Version	Firepower 9300		Firepower 4100 Series			
		SM-26	SM-40	4110	4150	4112	4115
6.6.x	2.8.1.105+	YES	YES	YES	YES	YES	YES
		SM-36	SM-48	4120		4125	
		SM-44	SM-56	4140		4145	

- Upgrade the FXOS separately from the Firepower software
- Upgrade the FXOS on each chassis independently
- FXOS upgrade it if required for your sensors before upgrading the FTD version



Traffic Flow Impact During Upgrade

Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	Best Practice: Update FXOS on the standby, switch active peers, upgrade the new standby.
	Dropped until one peer is online.	Upgrade FXOS on the active peer before the standby is finished upgrading.
Inter-chassis cluster	Unaffected.	Best Practice: Upgrade one chassis at a time so at least one module is always online.
	Dropped until at least one module is online.	Upgrade chassis at the same time, so all modules are down at some point.
Intra-chassis cluster (Firepower 9300 only)	Passed without inspection.	Hardware bypass enabled: Bypass: Standby or Bypass-Force .
	Dropped until at least one module is online.	Hardware bypass disabled: Bypass: Disabled .
	Dropped until at least one module is online.	No hardware bypass module.



Traffic Flow Impact During Upgrade

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, hardware bypass force-enabled: Bypass: Force	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: Bypass: Standby	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: Bypass: Disabled	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.



Upgrade Recommendation

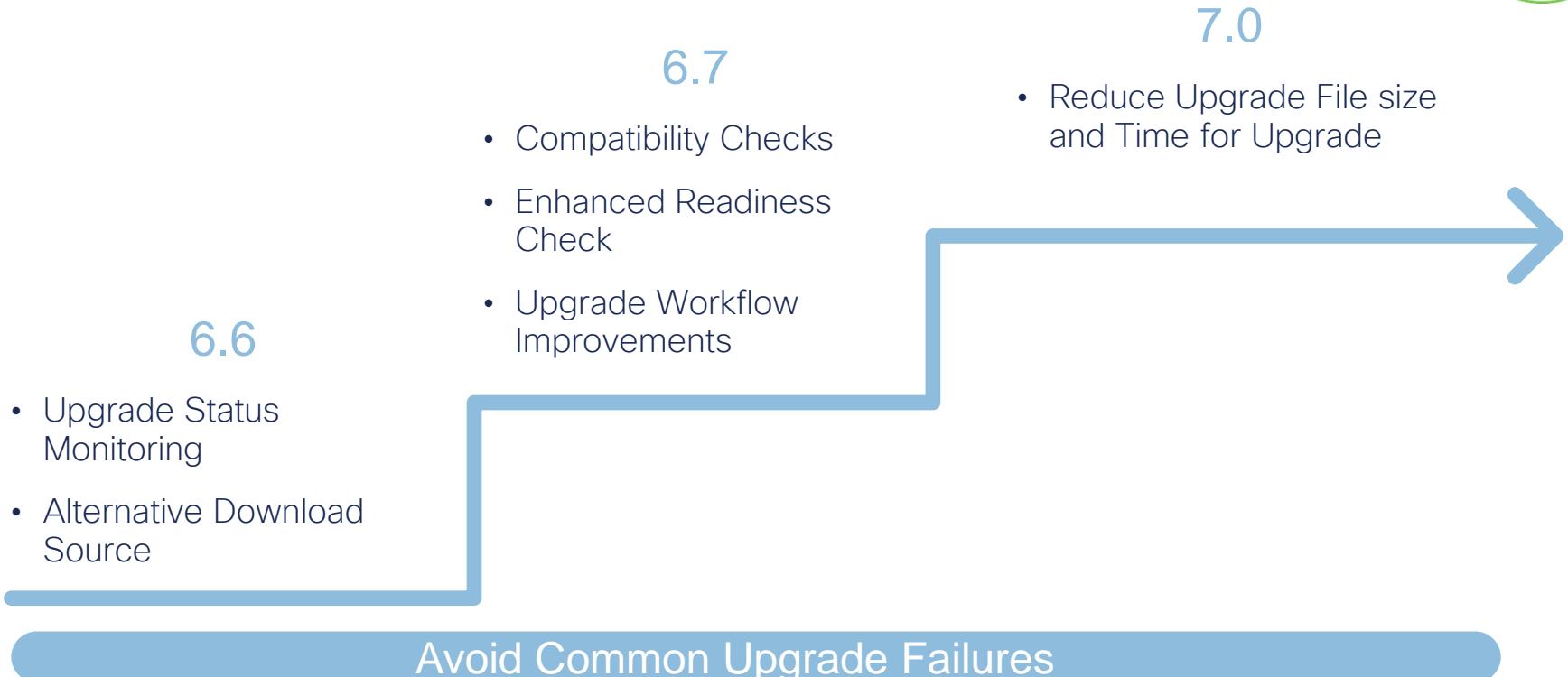


www.cisco.com/go/ftd-software

- ✖ DO NOT stop an upgrade in process on any appliance.
- ✓ Check the FMC UI for the cause of a failed upgrade.
- ✓ Ensure there is nothing in the deploy queue prior to an upgrade.
- ✓ Upgrade FMC to a higher version first, then its sensors.
- ✓ Update to the most recent maintenance release on your current branch.
- ✓ Upgrade major branches only if a newly released feature is needed.

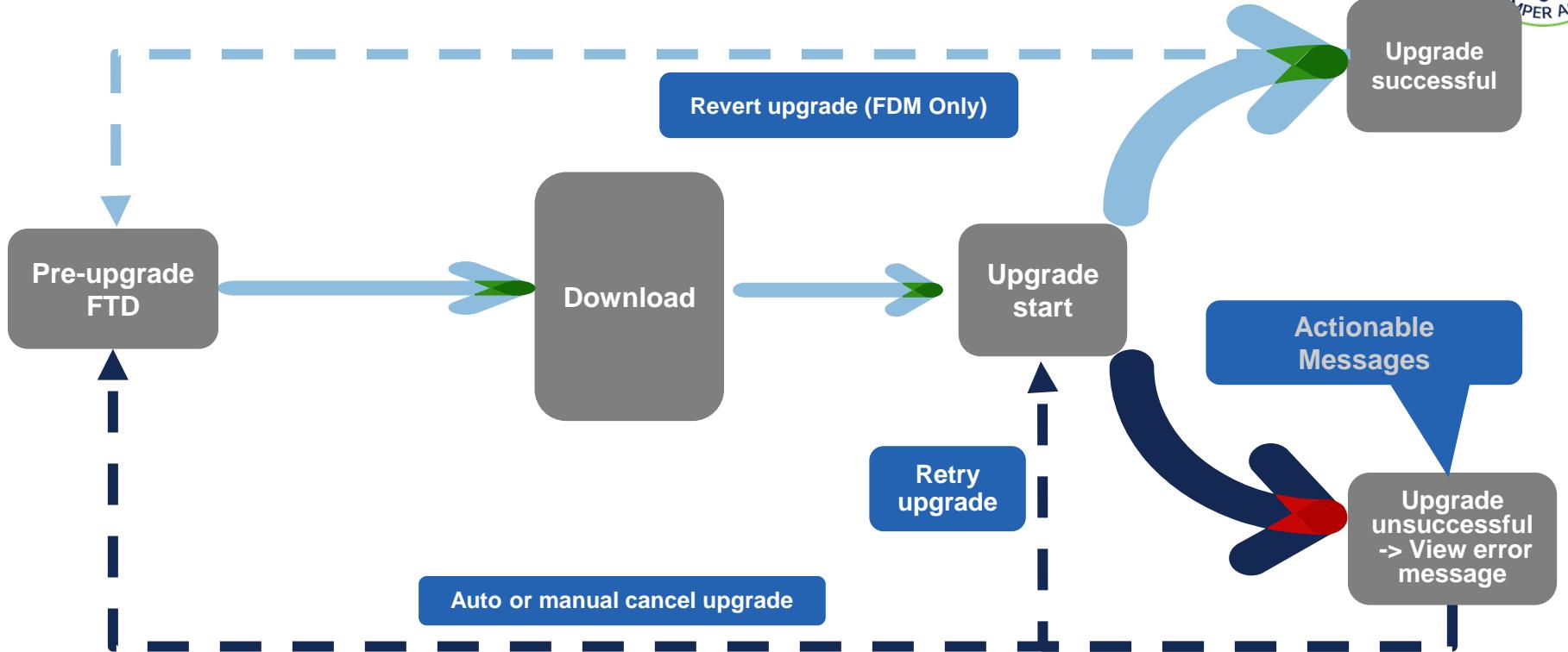


Upgrade Improvements - Timeline





New Upgrade Workflow





Upgrade Workflow Improvements

Upgrade Status Reporting

- Enhanced error reporting with failure reason and actionable recovery steps
- Live upgrade status UI

Device Installation Retry

- Auto-retry FTD image installation, if a new installation is interrupted (e.g. power failure)
- Firepower 1000 and 2100 series

New Upgrade Recovery Options

- Revert after Successful Upgrade
(FMC will be supported in future release)
- Manual/Auto-cancel Major Upgrade upon failure
- Retry Major Upgrade



Compatibility Checks

- FXOS version is not compatible with the target FTD version
 - on a FPR9300 or FPR4100 Series
- Pending deployment
- Weak ciphers in use
 - Applicable for 6.7 release only
- FMC only

Upgrade Type	FXOS Validation	Pending deployment
FMC upgrade	Not applicable	Supported (Minimum FMC version 6.7.0)
FTD Upgrade	Supported (FTD upgraded to 6.7.0 or later and FMC running 6.7.0 or above)	Supported (Minimum FTD version must be 6.3 and FMC running 6.7.0)

Avoid Common Upgrade Failures



Readiness Check Improvements

- Increased performance (~2min)
- HA & Clusters supported
- Enhanced logs & messages
- Displayed on Updates page
- Consolidated view across multiple devices
- Upgrade ETA displayed
- API support

- FMC version 6.7.0 and above
 - FMC managed FTD major, maintenance or patch upgrade
 - New “Readiness Check Results” column on Updates page
 - New consolidated view with “readiness checks” tab
 - Run Readiness Checks on HA/Cluster devices
 - Downloadable “Readiness Check” results available in Task manager

Avoid Common Upgrade Failures

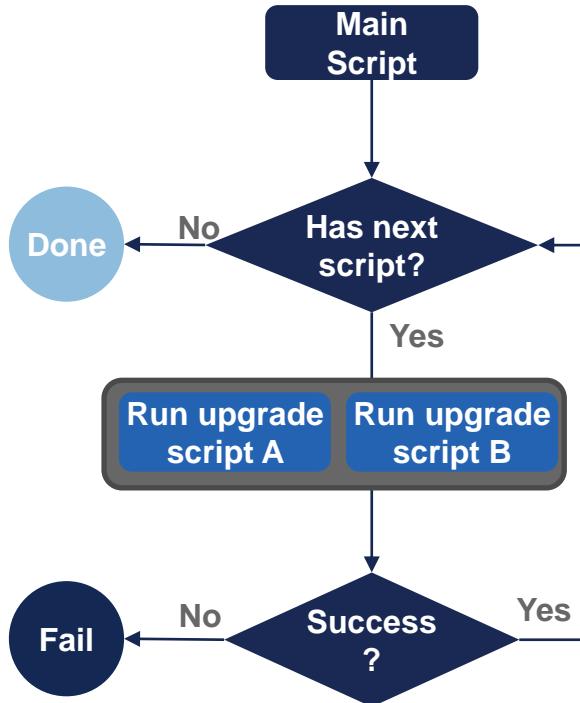


7.0 Install and Upgrade Improvements



Faster Upgrades

- Reduced FTD upgrade time
 - Optimize the number of system operations
 - Smaller upgrade package file
 - Parallel execution of upgrade tasks
 - Both FMC and FDM managed
 - Faster file transfer from FMC to FTD





Fleet Upgrades

- Increase number of concurrent upgrades of FMC managed FTDs
- Decrease the time to upgrade deployment with more than 15 devices
- Stacks/Clusters and HA are supported
- Faster upgrade times with release 7.0

Firepower Management Center
Devices / Device Management

Overview Policies Devices Objects AMP Intelligence Deploy Search Device Add Deployment History

View By: Group All (4) Error (0) Warning (0) Offline (0) Normal (4) Deployment Pending (0) Upgrade (2)

Collapse All 4 Visible Devices Selected (Select all 4 Devices) Select Bulk Action

Name	Chassis	Licenses	Access Control Policy
10.10.1.38	FTD on VMWare	6.7.0 N/A	Base acp
10.10.1.46	FTD on VMWare	6.7.0 N/A	Base acp
10.10.1.52	FTD on VMWare	6.7.0 N/A	Base acp
10.10.1.58	FTD on VMWare	6.7.0 N/A	Base acp

Upgrade Firepower Software



FTD Upgrade

FTD Upgrade

Deployments Upgrades Health Tasks

Show Notifications

1 total 0 waiting 1 running 0 retrying 0 success 0 failures Filter

🕒 Remote Install

Apply Cisco FTD Upgrade 7.0.1-84 to HA_Test 28s

Initializing

No more older tasks



FTD Upgrade

FTD Upgrade

Upgrade in Progress

... NGFW3
198.19.10.83
Cisco Firepower Threat Defense for VMware (Version: 7.0.0)

Version: 7.0.1 | Size: 970.54 MB | Build Date: Oct 5, 2021 4:14 AM UTC
Initiated By: admin | Initiated At: Oct 28, 2021 7:02 AM EDT

FTD → FTD

0% Completed (14 minutes left)

Upgrade In Progress...

Checking device readiness... (000_start/400_run_troubleshoot.sh)

Upgrade will automatically cancel on failure and roll back to the previous version.

Log Details

Upgrade logs:

```
Thu Oct 28 11:01:51 UTC 2021 0% Running script 000_start/000_00_run_c11_kick_start.sh... 14 m
Thu Oct 28 11:01:52 UTC 2021 0% Running script 000_start/000_0_start_upgrade_status_api_stack
Thu Oct 28 11:01:53 UTC 2021 0% Running script 000_start/000_check_platform_support.sh... 14 m
Thu Oct 28 11:01:53 UTC 2021 0% Running script 000_start/000_check_update.sh... 14 mins remai
Thu Oct 28 11:01:53 UTC 2021 0% Running script 000_start/100_start_messages.sh... 14 mins remai
Thu Oct 28 11:01:54 UTC 2021 0% Running script 000_start/181_run_pruning.pl... 14 mins remain
Thu Oct 28 11:02:29 UTC 2021 0% Running script 000_start/105_check_model_number.sh... 14 mins remai
Thu Oct 28 11:02:29 UTC 2021 0% Running script 000_start/107_version_check.sh... 14 mins remai
Thu Oct 28 11:02:29 UTC 2021 0% Running script 000_start/107_version_check.sh... 14 mins remai
```

Cancel Upgrade Close





FTD Upgrade HA

FTD Upgrade

✓ Upgrade Completed

NGFW3
198.19.10.83
Cisco Firepower Threat Defense for VMware (Version: 7.0.0)

Version: 7.0.1 | **Size:** 970.54 MB | **Build Date:** Oct 5, 2021 4:14 AM UTC
Initiated By: admin | Initiated At: Oct 28, 2021 7:16 AM EDT

→

Upgrade to version 7.0.1 Completed

● Upgrade will automatically cancel on failure and roll back to the previous version.

▼ Log Details

Upgrade logs:

```
Thu Oct 28 11:01:51 UTC 2021 0% Running script 000_start/000_00_run_cli_kick_start.sh... 14 n
Thu Oct 28 11:01:52 UTC 2021 0% Running script 000_start/000_0_start_upgrade_status_api_stack
Thu Oct 28 11:01:53 UTC 2021 0% Running script 000_start/000_check_platform_support.sh... 14
Thu Oct 28 11:01:53 UTC 2021 0% Running script 000_start/000_check_update.sh... 14 mins remai
Thu Oct 28 11:01:53 UTC 2021 0% Running script 000_start/100_start_messages.sh... 14 mins rem
Thu Oct 28 11:01:53 UTC 2021 0% Running script 000_start/101_run_pruning.pl... 14 mins remai
Thu Oct 28 11:02:29 UTC 2021 0% Running script 000_start/105_check_model_number.sh... 14 mins
Thu Oct 28 11:02:29 UTC 2021 0% Running script 000_start/107_version_check.sh... 14 mins rema
Thu Oct 28 11:02:29 UTC 2021 0% Running script 000_start/110_interpreter_check.sh... 14 mins rem
```

Close

✗ Upgrade in Progress

NGFW1
198.19.10.81
Cisco Firepower Threat Defense for VMware (Version: 7.0.0)

Version: 7.0.1 | **Size:** 970.54 MB | **Build Date:** Oct 5, 2021 4:14 AM UTC
Initiated By: admin | Initiated At: Oct 28, 2021 7:27 AM EDT

→

7% Completed (13 minutes left)
Upgrade In Progress...
Preparing to upgrade... (200_pre/200_enable_maintenance_mode.pl)

● Upgrade will automatically cancel on failure and roll back to the previous version.

▼ Log Details

Upgrade logs:

```
Thu Oct 28 11:25:04 UTC 2021 0% Running script 000_start/000_00_run_cli_kick_start.sh... 14 n
Thu Oct 28 11:25:06 UTC 2021 0% Running script 000_start/000_0_start_upgrade_status_api_stack
Thu Oct 28 11:25:07 UTC 2021 0% Running script 000_start/000_check_platform_support.sh... 14
Thu Oct 28 11:25:07 UTC 2021 0% Running script 000_start/000_check_update.sh... 14 mins remai
Thu Oct 28 11:25:07 UTC 2021 0% Running script 000_start/100_start_messages.sh... 14 mins rem
Thu Oct 28 11:25:07 UTC 2021 0% Running script 000_start/101_run_pruning.pl... 14 mins remai
Thu Oct 28 11:25:43 UTC 2021 0% Running script 000_start/105_check_model_number.sh... 14 mins
Thu Oct 28 11:25:43 UTC 2021 0% Running script 000_start/107_version_check.sh... 14 mins rem
```

Cancel Upgrade **Close**





Improved Error Messaging Example

Error message for base version less than 7.0.0

Cisco Firepower Management Center for VMWare 6.6.1 Build 91 (firepower) - admin – Mozilla Firefox

://10.10.2.90/admin/update.cgi?no_mojo=1

Firepower Manager Cisco Firepower Manager +

Overview Analysis Policies Devices Objects AMP Intelligence

Application Updates Deployments 0 Health 0 Tasks

20+ total | 0 waiting 0 running 0 retrying 2

Task Notification Message Center Tasks Tab queued

Remote Install Apply to 10.10.2.67 Update Install failed

No error message displayed

Error message for base version >= 7.0.0

Upgrade Failed

vfdt2 10.10.1.83 Cisco Firepower Threat Defense for VMWare (Version: 7.0.0)

Version: | Size: 0 B | Build Date: Jan 1, 1970 12:00 AM UTC
Initiated At: Dec 11, 2020 7:45 PM EST

FTD FTD

Upgrade to version 7.0.0 Failed

Upgrade package signature verification failed

Log Details Download Logs Close

ISE Integration

Benefits of integrating NGFW with ISE



-  Improves Access Control Policy Abstraction
-  Unlocks Path to SDA Integration
-  Adds Security Group TAG eXchange Protocol (SXP) Support for Trustsec Only Use Cases
-  Allows customers to define policies which identifies devices by TAGs

Benefits of NGFW integration with ISE



Ability to use combination of source and destination SGT's in access control rules for segregating network access

Ability to subscribe to SXP mappings from ISE, that address multiple use cases such as VPN / non-VPN traffic flow handling, SDA integration, maps EPGs to SGTs in ACI DC environment

Minimize Access Control Rule Expansion

Remediation module allows Firepower system to use ISE Adaptive Network Control (ANC) and automate quarantine/blocking of attackers on the network



Firepower Management Center

Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin ▾

NETSEC.LOCAL
FMC and ISE Integration

Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

Prefilter Policy: Demo Prefilter Policy SSL Policy: None Identity Policy: NGFWIdentityPolicy

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Application...	Source Ports	Dest Ports
▼ Mandatory - NETSEC.LOCAL (1-6)									
1 users to webservers	Any	Any	Any	Any	Any	Any	Any	Any	Any
2 Block SSH for HR	Any	Any	Any	Any	Any	dCloudRe...	OpenSSH SSH	Any	Any
3 Block Extranet129	InZone	OutZone	Any	Extranet129	Any	Any	Any	Any	Any
4 Block ICMP Over GRE	GRE	Any	Any	Any	Any	Any	ICMP ICMP for I...	Any	Any
5 Block Unacceptable Content	Any	Any	Any	Any	Any	Any	Any	Any	Any
6 Block Extra to Infra	OutZone	InZone	Extranets	Infrastruct...	Any	Any	Any	Any	Any
▼ Default - NETSEC.LOCAL (7-10)									
7 Web Server Access	OutZone	InZone	Any	www:in	Any	Any	Any	Any	Any

Source SGT Dest SGT Action

Users WebServer Block with reset

Displaying 1 - 10 of 10 rules Page 1 of 1 Rules per page: 100





Analysis

/ Connections

[Bookmark This Page](#) | [Report Designer](#) | [Dashboard](#) | [View Bookmarks](#) | [Search](#)[Custom Searches](#)

II 2019-12-11 17:36:10 - 2019-12-11 18:53:50

Expanding

Disabled Columns

Connection Events (switch workflow)▶ Search Constraints ([Edit Search](#) [Save Search](#))[Connections with Application Details](#)[Table View of Connection Events](#)

Jump to...

<input type="checkbox"/>	First Packet x	Action x	Initiator IP x	Responder IP x	Source Port / ICMP Type x	Destination Port / ICMP Code x	Access Control Policy x	Access Control Rule x	Source SGT x	Destination SGT x	De x	Ingress Interface x	Egress Interface x	Initiator Packets x	Responder Packets x	Initiator Bytes x	Responder Bytes x
▼	2019-12-11 18:53:34	Block with reset	198.19.10.201	198.18.133.201	51408 / tcp	80 (http) / tcp	NETSEC.LOCAL	users to users	Users	WebServer	NC			1	0	74	0
▼	2019-12-11 18:53:33	Block with reset	198.19.10.201	198.18.133.201	50919 / tcp	80 (http) / tcp	NETSEC.LOCAL	users to users	Users	WebServer	NC			1	0	74	0
▼	2019-12-11 18:53:33	Block with reset	198.19.10.201	198.18.133.201	51316 / tcp	80 (http) / tcp	NETSEC.LOCAL	users to users	Users	WebServer	NC			1	0	74	0
▼	2019-12-11 18:53:31	Block with reset	198.19.10.201	198.18.133.201	39591 / tcp	80 (http) / tcp	NETSEC.LOCAL	users to users	Users	WebServer	NC			1	0	74	0
▼	2019-12-11 18:50:19	Block with reset	198.19.10.201	198.18.133.201	35361 / tcp	80 (http) / tcp	NETSEC.LOCAL	users to users	Users	WebServer	NC			1	0	74	0





Destination SGTs



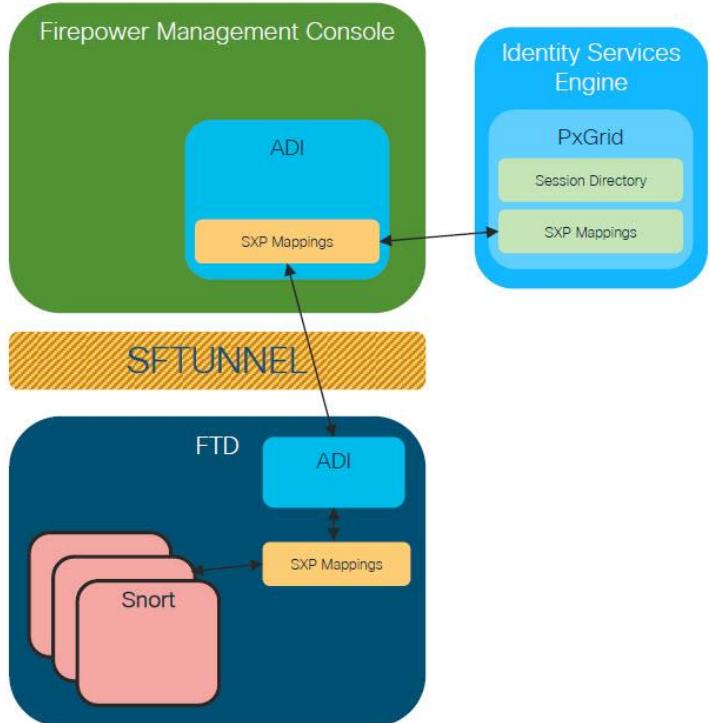
Destination Security Group Tags (DGTs)

- Prior to 6.5, only Source SGTs could be used in access control policy rules.
- Access control policy rules can use both source SGTs and DGTs as rule matching criteria
- Unlike source SGTs, DGTs are *never* embedded in frames.
 - DGTs must be learned out of band. FMC uses pxGrid to learn IP-to-SGT mappings from ISE.



Flow

- ADI subscribes to PxGrid on the FMC, and transfers SXP mappings to its counterpart on the FTD which delivers them to Snort
- Session Directory delivers User-IP-SGT mappings via a similar mechanism not shown here.



Max. Recommended Number of Bindings*

Virtual FTD
KVM, VMWare, AWS, Azure



ASA 5500-X
5508, 5516, 5525, 5545, 5555



Firepower 1010, 1120, 1140, 1150



Firepower 2110, 2120, 2130



Firepower 4110



Firepower 2140, 4115, 4120, 4125



150K

Firepower 9300 and 4100
4140, 4145, 4150, SM-24, 36, 40, 44, 48, 56



300K



*Scale is limited by the smallest device connected to the FMC e.g. FMC managing both Firepower 1010 and Firepower 9300 will be limited to 64k.

Best Practices for NGFW DST TAGs Feature



-  Resilient deployment: FMC and ISE nodes in High Availability mode
-  Enable Health Policy ISE Connection Monitor Module
-  Use suggested ISE release 2.7+ or above
-  Enable PxGrid service under ISE node deployment
-  Define on ISE an SXP device configuration to publish IP-SXP bindings
-  Do Not Forget to Enable “Publish SXP Bindings on PxGrid” option on ISE



Identity Passive Connector (ISE-PIC)

- The Cisco ISE Passive Identity Connector is a subset of functionality offered with Cisco Identity Service Engine
- Supports only passive ID functionality
- ISE-PIC provides 2 license models
 - 3,000 users
 - 300,000 users
- Supports up to 100 domains
- FMC allows 1 ISE-PIC connection that is HA capable

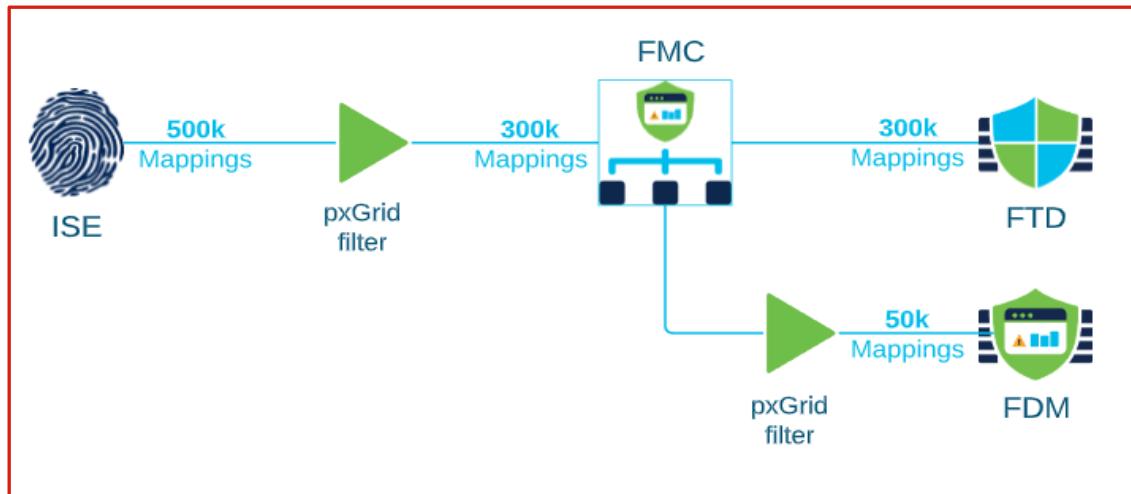
FMC Integration to Identity Services Engine Passive Identity Connector



- Cisco has announced End of FMC Support for User Agent 6.7 removed
- Cisco recommends stopping the use of User Agent and migrating to Cisco Identity Services Engine (ISE) / Passive Identity Connector (ISE-PIC)
- Benefits of using ISE-PIC in comparison to User Agent:
 - Support for Microsoft Active Directory up to version 2016
 - Gathers authentication data from up to 10 Microsoft Active Directory domain controllers
 - Gathers Active Directory authentication data from switches supporting Kerberos SPAN
 - Supports passive/active redundancy
 - Supports KVM, VMware, Hyper-V hypervisors
- ISE-PIC Entitlements w/FMC PIDs:
 - ISE Passive Identity Connector for Firepower Management Center

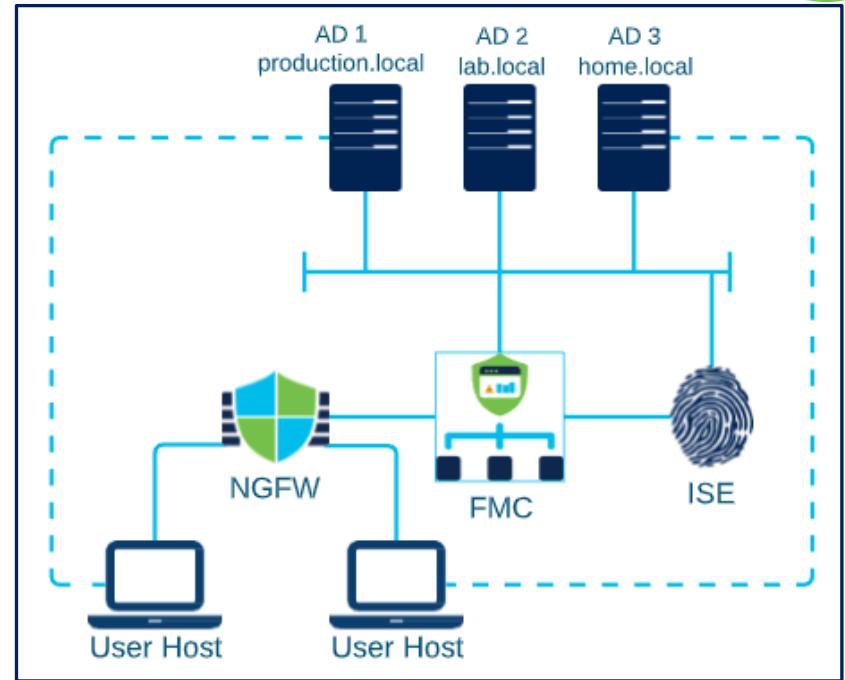
FMC pxGrid 2.0 Integration

- Adaptive Network Control (ANC) remediation module replaces Endpoint Protection Services (the conversion is not automated)
- ISE improves scale and supports HA for pxGrid 2.0
- **Move to ISE/ISE-PIC**



Active Directory Realm Sequence

- Allows users from different AD domains on the same network
- Introduces the concept of “Realm Sequence”
- A Realm Sequence is a collection of ordered Active Directory realms
- FMC/FDM UI and API





Active Directory Realm Sequence

FDM UI

Click Objects -> Identity Sources -> Realm Sequence

Add AD Realm Sequence

Name: Bombay_Network_Lookup

Description: Look under these realms when a user is visiting Bombay office

AD Realms:

- + Movies
- Soccer
- ntd

Drag and drop to order your realms

CANCEL OK

FMC UI

Click Integration -> Sequences -> Add Sequences

Add Realm Sequence

Name*: Geographic_Sequence

Description: Realm Sequence by Geography

Realms

+ Austin (AD)

India (AD)

Germany (AD)

Drag and drop to order your realms

Save

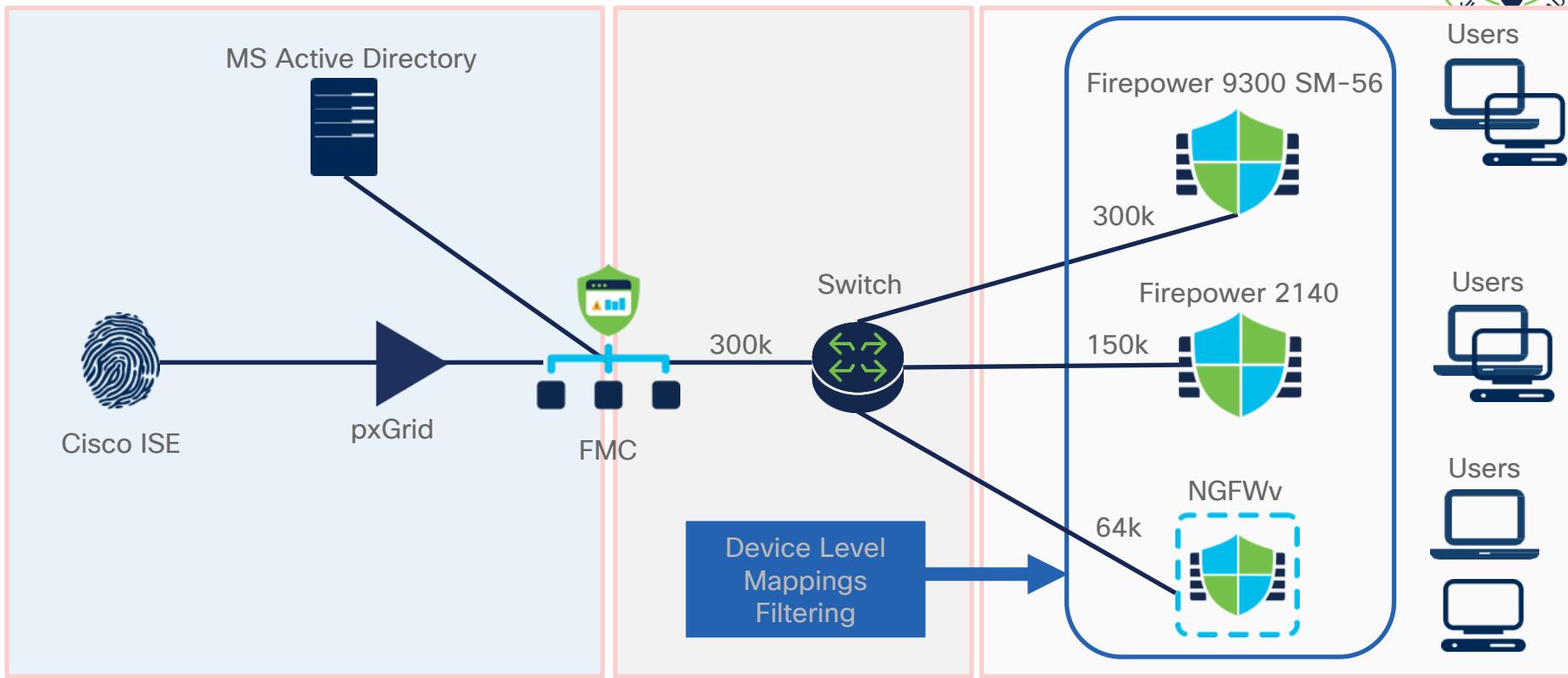




7.0 Subnet Filter for Identity Policy Mappings



Where does Identity Filter takes place?





FMC UI Configuration

New Identity Source tab in the Identity Policy Editor

Firepower Management Center Policies / Access Control / [Identity Policy Editor](#) Overview Analysis Policies Devices Objects AMP Intelligence

Identity Mapping Filter on Identity Policy

Enter Description

Rules Active Authen. **Identity Source**

Identity Mapping Filter + ←

Identity Mapping Filter Settings!
Allows to create or select existing Network Object or Group as the filter criteria.

6.7 added support for this feature in FTD CLI



How Identity Device Filter helps?

! Snort Identity Memory Usage

250.4% of 15.0M used [see less](#)

Total Usage : 250.4%(37.6M / 15.0M)

Memory Usage Detail

Memory Usage Detail 37.5M

Host Cache 32B

User Group Mapping 65.7K

Binding Detail

Current 265983 / 64000

Host 265983

Subnet 0

User Group Mapping Detail

User Group Mapping 0

Group used in policy 0 / 128

Total number of identity bindings/mappings
(combined User-IP,SGT-IP,Dynamic Object Mappings)
on the selected FTD is currently over 265k.

No Identity Device Filter applied.



How Identity Device Filter helps?

Snort Identity Memory Usage

63.1% of 15.0M used [see less](#)

Total Usage : 63.1%(9.5M / 15.0M)

Memory Usage Detail

Memory Usage Detail 9.4M

Host Cache 32B

User Group Mapping 65.7K

Binding Detail

Current 65280 / 64000

Host 65280

Subnet 0

User Group Mapping Detail

User Group Mapping 0

Group used in policy 0 / 128

Total number of identity bindings/mappings
(combined User-IP,SGT-IP,Dynamic Object Mappings)
on the selected FTD has been reduced down to 65k
after Identity Device Filter has been applied!



Benefits of Identity Mapping Subnet Filter Feature

- Lower usage of Snort Identity Memory
 - by ignoring identity mappings from subnets that are not being monitored by the managed device (FTD)
 - only required Identity Mappings (User-IP, SGT-IP, Dynamic Object Mappings) are loaded to the Snort memory on the managed device/s (FTD)
- Ability to manage all type of managed devices (low/mid/high-end) by single management platform (FMC)
- Control total number of user identity mappings (through subnet filter)
 - per device based on total amount of recommended bindings for the platform

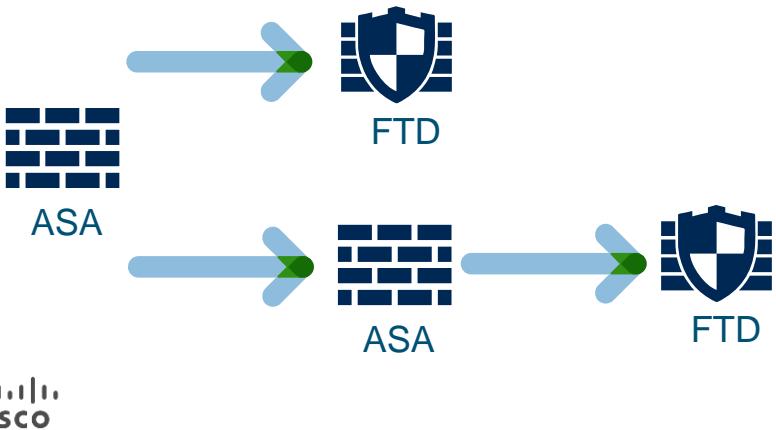
Firepower Migrations



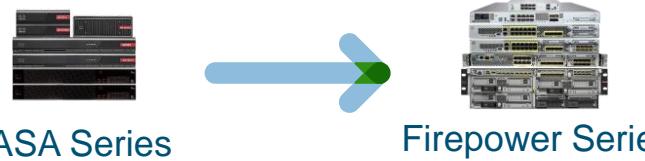
What are my migration options?



Software OS: ASA or FTD



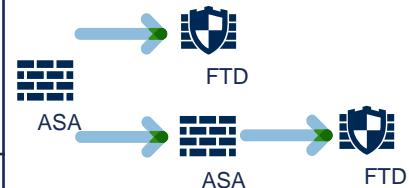
Hardware: Platform





ASA or FTD OS Software

From OS	To OS	Level	Details
ASA	ASA	Easy	Upgrade hardware only. Keep ASA OS and re-use existing configuration Easier migration to FTD later on
ASA	FTD	Complex	Available Migration Tools and resources.
FTD	ASA	N/A	Not Supported



Single or Two Steps process from ASA to FTD

ASA to Firepower hardware

*Recommended Hardware Platform Migration Options



From ASA 5500-X Series	To Firepower FPR Series
ASA 5505 / ASA 5506-X	Firepower FPR 1010
ASA 5508-X	Firepower FPR 1120
ASA 5516-X	Firepower FPR 1140
ASA 5525-X	Firepower FPR 1150/FPR 2110
ASA 5545-X	Firepower FPR 2120
ASA 5555-X	Firepower FPR 2130
ASA 5585-X SSP-10	Firepower FPR 2140/ FPR 4115
ASA 5585-X SSP-20	Firepower FPR 4115
ASA 5585-X SSP-40	Firepower FPR 4125
ASA 5585-X SSP-60	Firepower FPR 4145





Cisco Firepower Migration Tool (FMT)



Cisco Firepower Migration Tool

Reporting



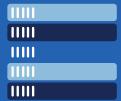
- Pre- and Post- Migration reports
- Ability to edit the configuration being migrated
- Live running logs, graceful error handling and resume from failure
- Object conflict detection and resolution

Automation



- ACL, NAT, Object, Interface, FQDN migration
- Multi Context to Multi Instance
- Selective migration and optimizations such as object re-use
- Auto-mapping of interfaces

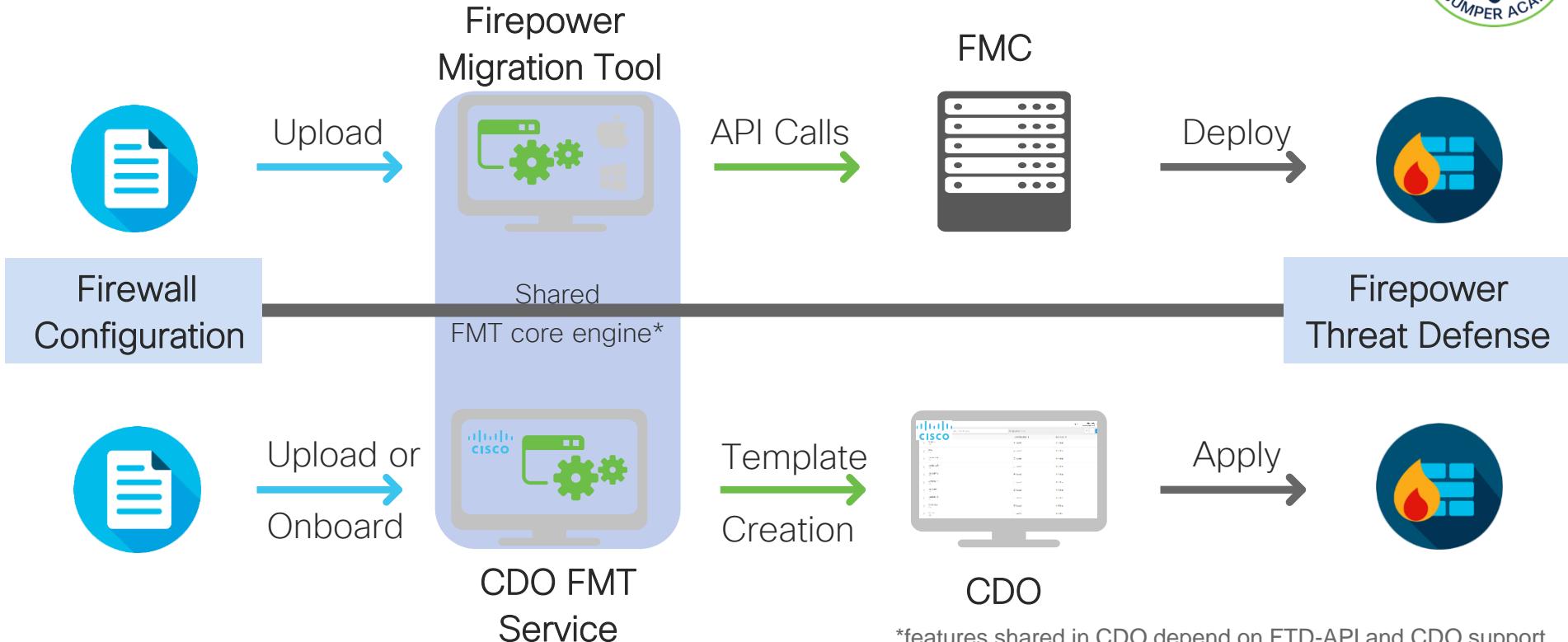
Scale



- Supports migration of features supported in FMC REST API
- Runs on Windows or Mac through Chrome browser
- CDO integration* to leverage orchestration benefits
- Programmability* through tool APIs



Firepower Migration Tool (Firewall to FTD)





Firepower Migration Tool Options

	FMT Desktop	FMT in CDO
FMT Client	Windows10 or Mac Chrome Browser No Internet Connectivity Required	CDO-Compatible Browser Internet Connectivity
FMT Authentication	Local or Cisco ID	CDO ID
Minimum Firepower Version	FP 6.2.3.0 ...FP 6.5	FP 6.4.0.x
FTD Manager	FMC	CDO (FDM)
ASA 8.4+ to FTD	Yes	Yes
Migration Target	Push to FMC for later deploy to FTD	Push to Live CDO managed FTD or create template in CDO for reuse
Reporting	Yes	Yes



Technical Online Resources

<http://www.cisco.com/go/support>

Tools

Bug Search Tool

Find software bugs based on product, release and keyword

Register & Manage Software Licenses

Product License Registration Tool

Software Research

View Cisco suggestions for supported products

Collaboration Solutions Analyzer

Suite of tools to assist you in the day to day operations of your Collaboration infrastructure.

Cisco CLI Analyzer

The Cisco CLI Analyzer (formerly ASA CLI Analyzer) is a smart SSH client with internal TAC tools and knowledge integrated. It is designed to help troubleshoot and check the overall health of your Cisco supported software.

[View All Tools](#)

Support Resources

Security Advisories

Field Notices

Cisco Cloud Status (New!)

Contacts / Support Cases

[Open New Case](#)

To open or view cases, you need a [Service Contract](#)

Manage Support Cases

Contact TAC by Phone

Enterprise and Service Provider Products

US/Canada 800-553-2447

Worldwide Phone Numbers

Small Business Products

US/Canada 866-606-1866

Worldwide Phone Numbers

Returns

Returns Portal

We've simplified RMAs. [Learn How](#) New!

Cisco Community

My Notifications

Small Business Product Support (New!)

Support forums



*Events, Webinars
Influencer Hub
(podcasts)*

Newsroom

Events

Blogs

Community



TAC Severity Definition

Severity 1	Severity 2
<ul style="list-style-type: none">• Production network down• Critical impact to business operations• 24-hour Cisco and customer commitment	<ul style="list-style-type: none">• Network severely degraded• Significant impact to business• Cisco and customer committed during business hours
Severity 3	Severity 4
<ul style="list-style-type: none">• Network functionality degraded• Business operations noticeably impaired• Cisco and customer in frequent contact	<ul style="list-style-type: none">• General assistance• Installation, upgrade, or configuration assistance• General product information

[Cisco TAC Severity and Escalation Guidelines](#)

Additional Post-Sales Support Resources



- Partner Self Service portal: www.cisco.com/go/pss
- Cisco Account Profile Manager (contract association):
https://tools.cisco.com/RPFA/profile/profile_management.do
- Support Case Manager:
<https://tools.cisco.com/ServiceRequestTool/scm/manager/case>
- Technical Services Quick Start Guide:
[http://www.cisco.com/web/partners/services/resources/tsquickstart/downloads/Global Technical Services Quick Start Guide.pdf](http://www.cisco.com/web/partners/services/resources/tsquickstart/downloads/Global%20Technical%20Services%20Quick%20Start%20Guide.pdf)

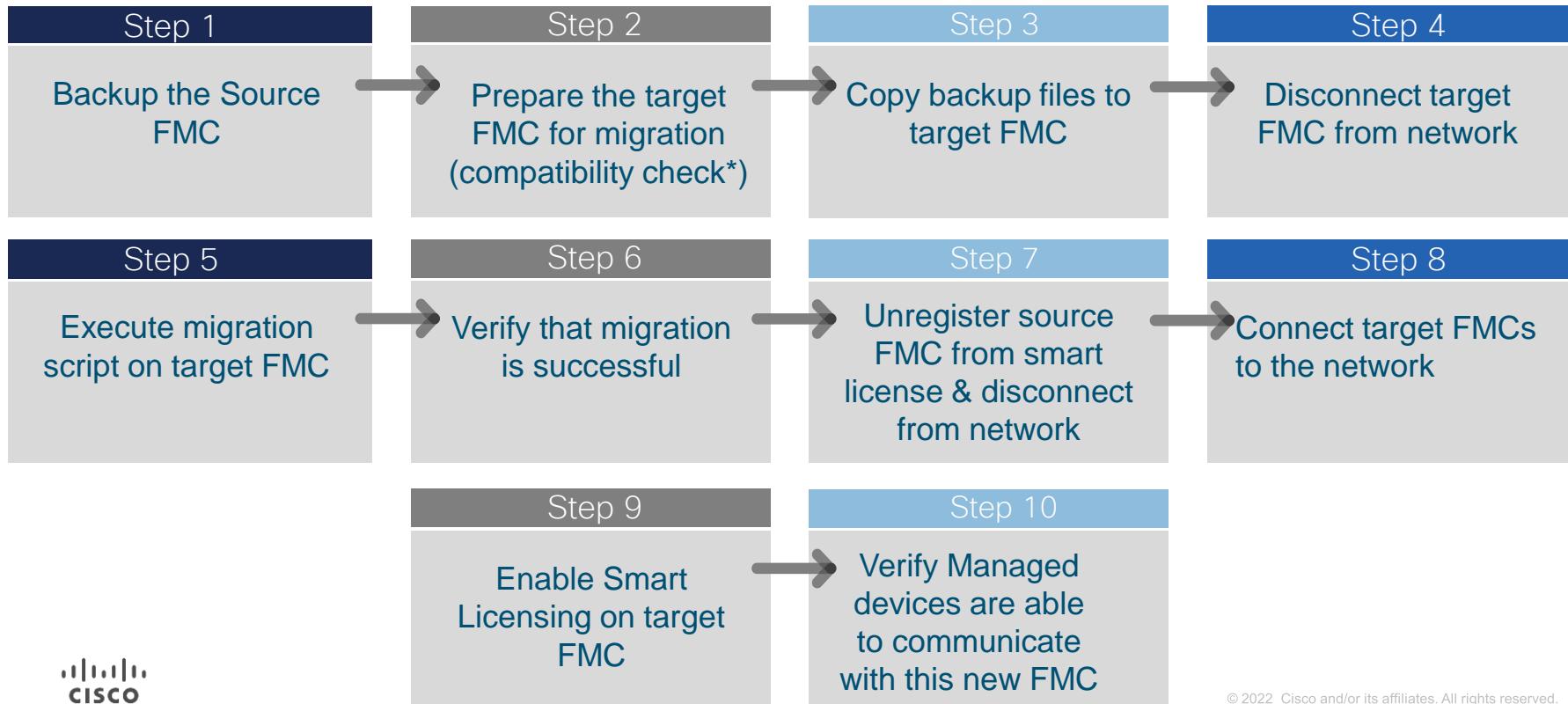


FMC Model Migration

- Move from lower to equivalent or to higher capacity FMC model
- based on existing FMC backup and restore flow
- Supported 6.5 onwards
- FMC managing any type of device
- All licensing model supported
- Licenses need to be removed from old FMC
- KVM and Azure not supported
- NAT between FTD and FMC must reflect the change in FMC IP, if any
- Version parity ((including patch, VDB, and SRU)
- Match number of interfaces



FMC Model Migration Workflow



*Compatibility Check - Supported model, management interfaces, IP address assignment, version parity including (patch, VDB, and SRU)

Thank You