



You make **possible**



Firepower NGFW in the DC and Enterprise

Deployment Tips and New Features

Wissam El Charif, Technical Solutions Architect

BRKSEC-2020

CISCO *Live!*

Barcelona | January 27-31, 2020



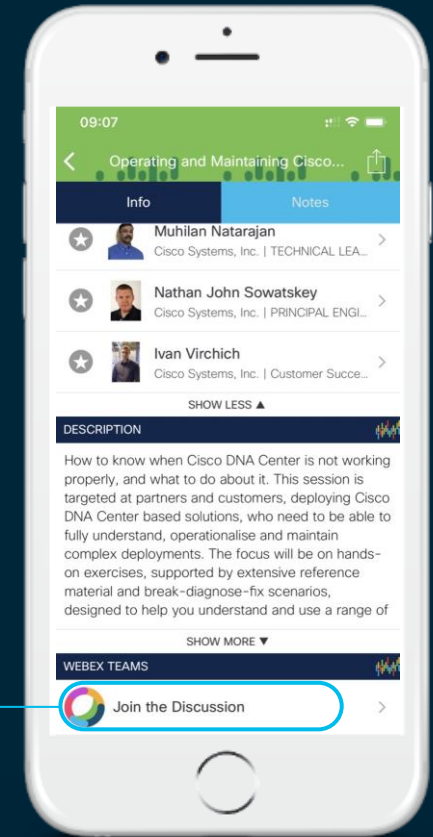
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



Agenda

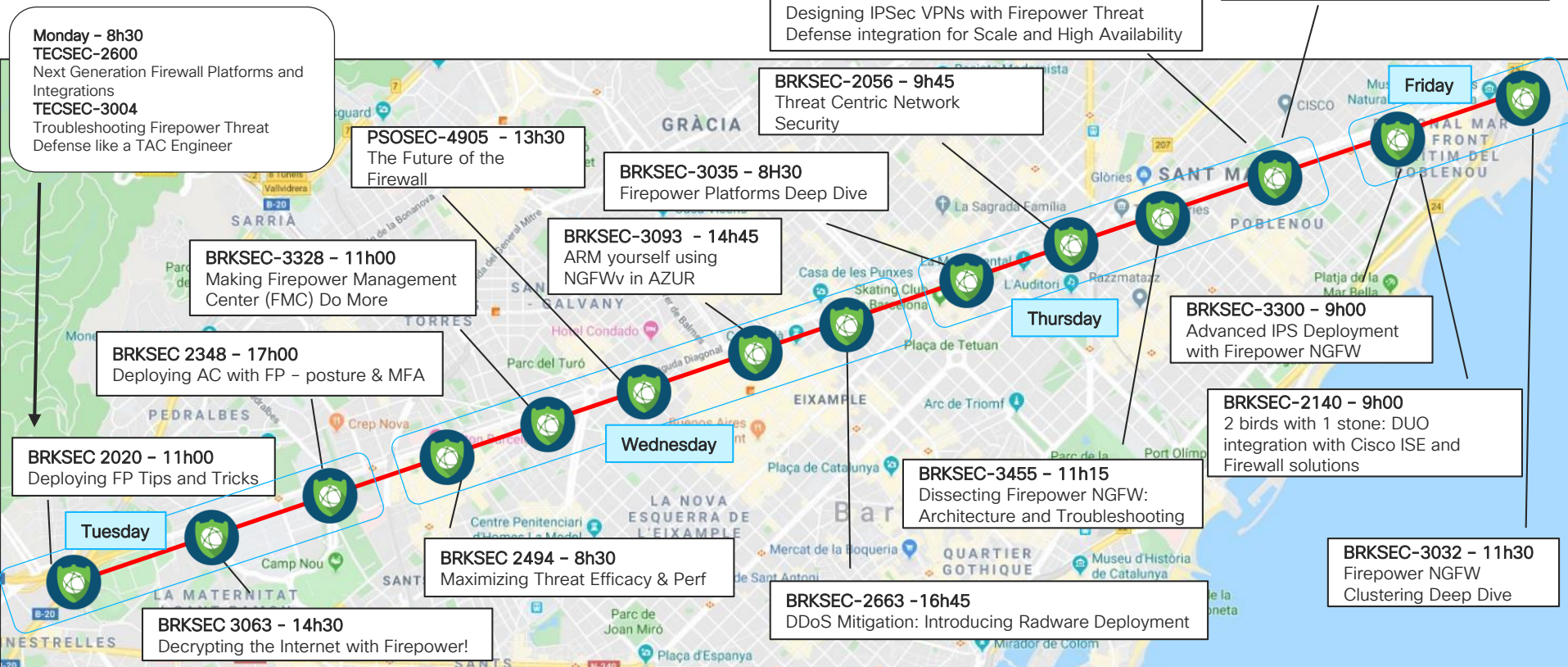
- Deploy L3 Firewalls at the Edge
 - Interfaces, Routing & NAT
 - NGFW Policy Tips & SSL/TLS Hardware Acceleration
 - High Availability
- Deploy L2 Firewalls in the DC
 - Clustering Overview
- Deploy Multi-Instance
 - Overview
 - Configuration Walkthrough
- Alternative Designs

Your Speaker

- Security Architect providing consultancy and technical sales support for Qatar.
- Deployed the first firepower and end-end Cisco security architecture in UAE.
- 13 years in the industry as a technical trainer, in operations/implementation and now Cisco



Firepower Diagonal Learning Map







Whisper Suites



After the Session
or MTE

CLINET (clinet.com)

Cisco LIVE Information Networking Company

- CLINET (clinet.com) is a fictional company created for understanding use cases in FTD firewall deployment.
- CLINET has embarked on a network/security deployment project entitled “The Security 20/20 Project” which serves as the basis for the use case.
- Company requirements and configuration examples are based upon real-life customer conversations and deployments.

There are ~100 slides we will not cover today

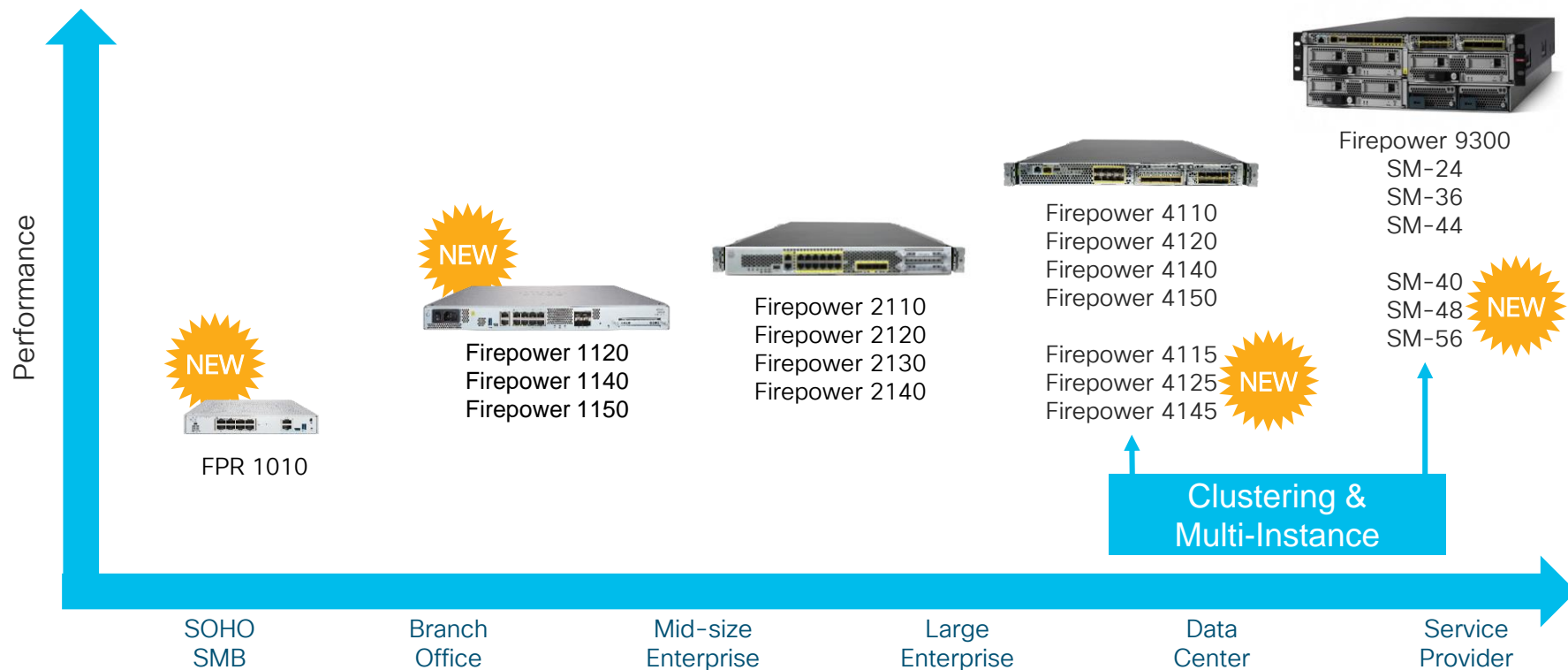
They are included for additional detail
and reference back at home

An abstract graphic at the top of the slide consists of numerous vertical bars of varying heights and small circles, all in a dark blue color, creating a rhythmic, barcode-like pattern.

Cisco Firepower NGFW

Cisco NGFW portfolio

Running Firepower Threat Defense (FTD)

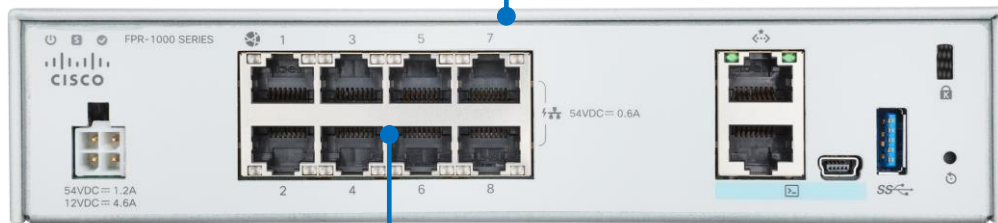


Firepower 1010 Overview

Integrated Security Appliance with ASA or FTD

- Embedded x86 CPU with QuickAssist Crypto Acceleration
- Fixed non-modular configuration

Desktop



Copper Data Interfaces

- 8x1GE Ethernet
- Built-in Layer 2 switch **new**
- Power over Ethernet (PoE) on ports 7 and 8 **new**

Firepower 1100 Overview

Integrated Security Appliance with ASA or FTD

- Embedded x86 CPU with QuickAssist Crypto Acceleration
- Fixed non-modular configurations (1120, 1140, 1150^{new})

SFP Data Interfaces

- 4x1GE on 1120 and 1140
- 2x1GE, 2x10GE on 1150^{new}

1RU



Copper Data Interfaces

- 8x1GE Ethernet

Field Replaceable SSD

Cisco NGFW Management Options



- On-box management
- Manages single deployment
- Simplified management / feature set

cisco *Live!*



- Centralized cloud manager
- Manages FTD, ASA, Meraki, Umbrella and AWS
- Rapidly evolving feature set



- Management appliance
- Supports full FTD feature set

Session Focus – Firepower Management Center

Firepower Management Center



Multi-Instance

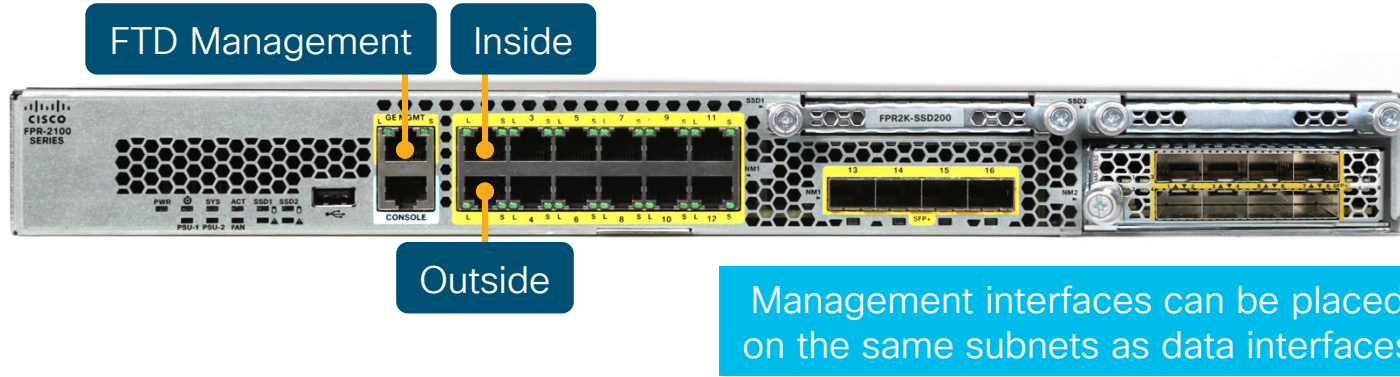
Clustering



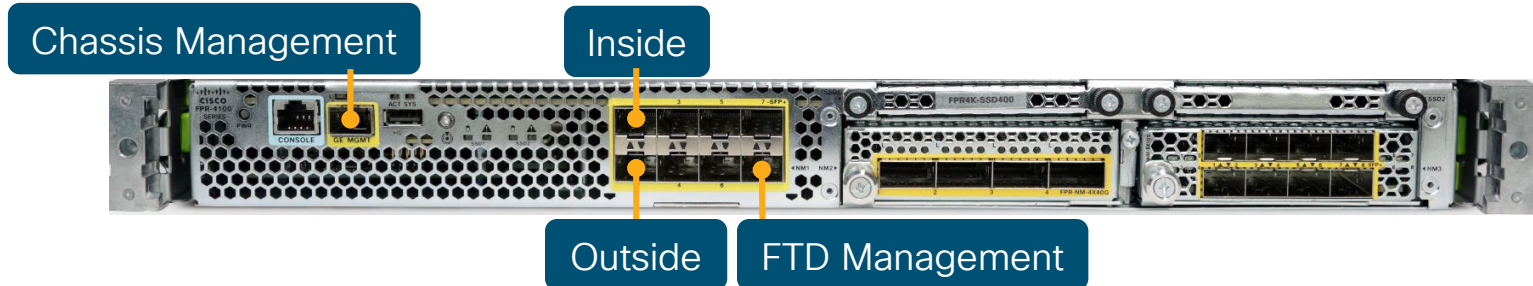
FTD Initial Setup

Management Connections

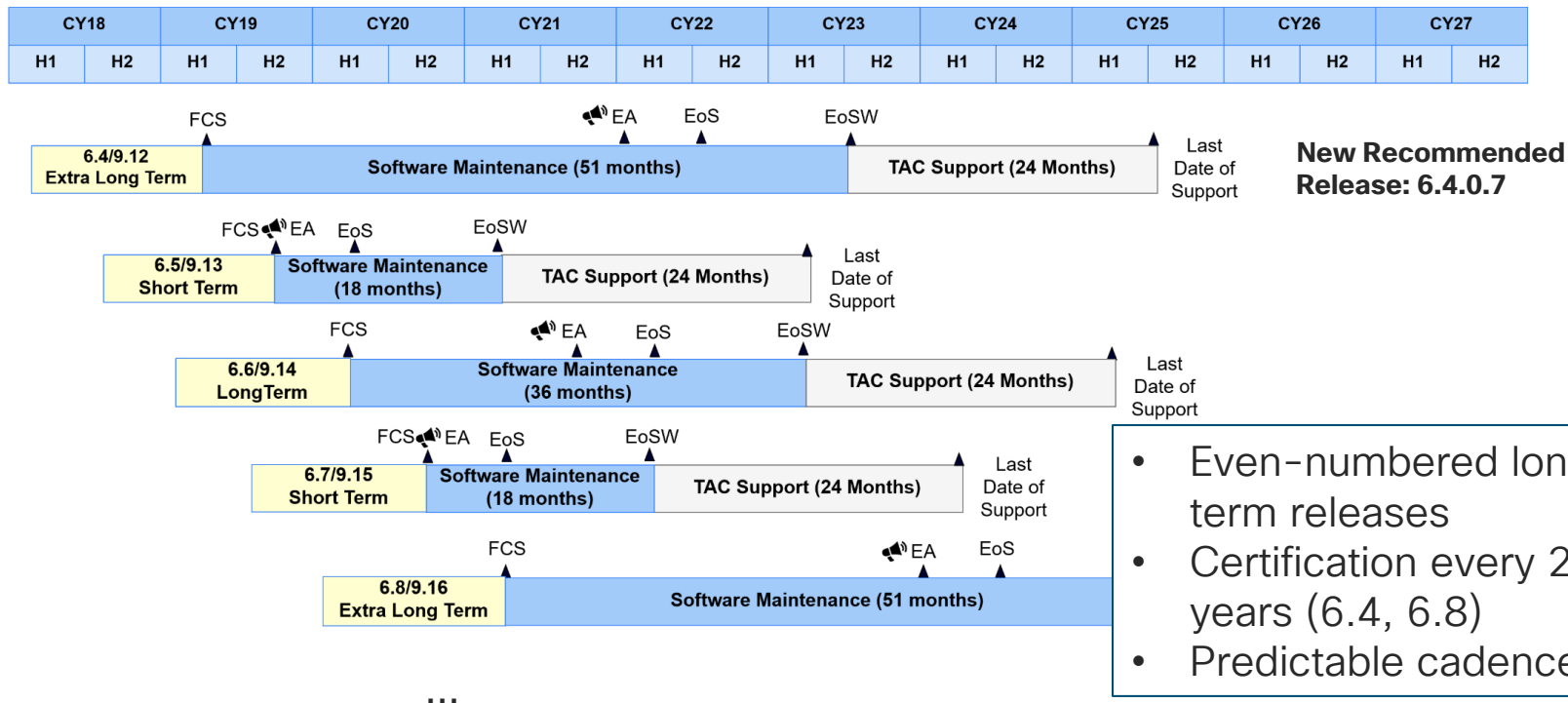
FPR1000 / FPR2100 (1 Management)



FPR4100 / FPR9300 (2 Management)



New Software Lifecycle Policy



Generally Suggested Version: FTD 6.4.0.7

Software Download Page on cisco.com Has Latest Recommendation

[Downloads Home](#) / [Security](#) / [Firewalls](#) / [Next-Generation Firewalls \(NGFW\)](#) / [Firepower 4100 Series](#) / [Firepower 4115 Security Appliance](#) / [Firepower Threat Defense \(FTD\) Software- 6.4.0.7](#)

Expand All Collapse All

Suggested Release

6.4.0.7 ★

Latest Release

6.4.0.7 ★
6.5.0.2

All Release

Firepower 4115 Security Appliance

Release 6.4.0.7

▲ My Notifications

Related Links and Documentation
[Release Notes for 6.4.0.7](#)
[Documentation Roadmap](#)

File Information	Release Date	Size
Firepower Threat Defense SSP Patch 6.4.0.7 Do not untar Cisco_FTD_SSP_Patch-6.4.0.7-53.sh.REL.tar	19-Dec-2019	302.76 MB

Look for the star



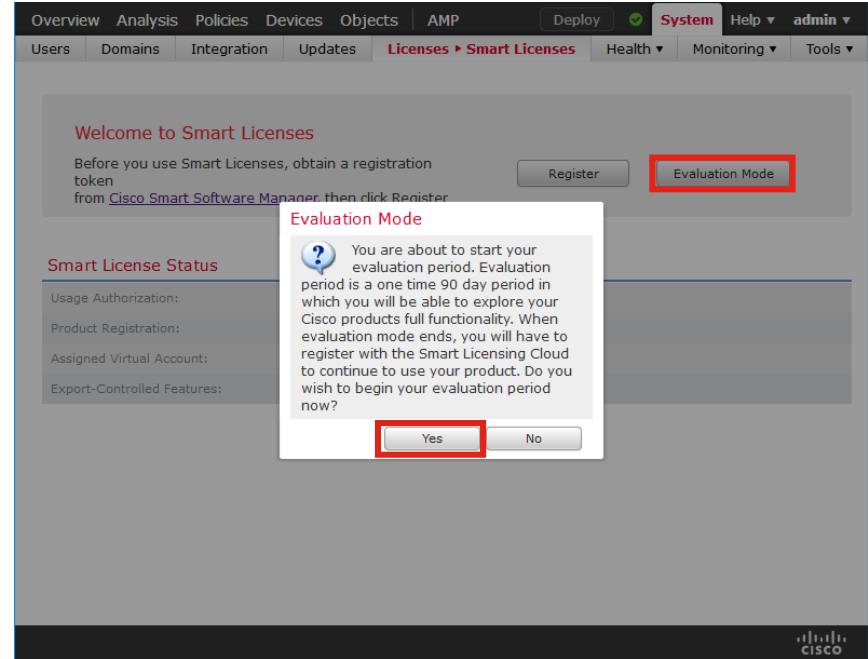
Latest Compatible FXOS Version (now 2.6.1.174)



Cisco FXOS Compatibility: <https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html>

FTD Licensing Tips

- All licensing for FTD are installed and enforced on the Firepower Management Center via Smart Licensing(PLR & SLR available)*
- Licenses are transferrable between firewalls of the same model
- Licensing is enforced when the policy is pushed
- 90 day “Evaluation Mode” applies to all FTD devices managed by that FMC



PLR: Permanent License Reservation for Air gapped environments
SLR: Specific License Reservation for Highly secure environments

Deploying Changes

Changes don't take effect until you deploy the policy

The screenshot shows the Cisco FPR4K web interface. The 'Policies' tab is active, and the 'Deploy' button in the top right is highlighted with a red box. A 'Deploy Policies' dialog box is open, showing a table of policies for device 'FPR4K'. The dialog box title is 'Deploy Policies Version: 2018-03-05 01:43 AM'. The table has columns: Device, Type, Group, and Current Version. The 'FPR4K' device is selected, and its policies are listed with green checkmarks indicating they are deployed. The 'Deploy' button at the bottom right of the dialog box is also highlighted with a red box.

Device	Type	Group	Current Version
<input checked="" type="checkbox"/> FPR4K	FTD		2018-03-05 01:35 AM

- Access Control Policy: FPR4K
- SSL Policy: Cisco - Decrypt
- Intrusion Policy: Balanced Security and Connectivity
- Intrusion Policy: No Rules Active
- DNS Policy: Default DNS Policy
- Prefilter Policy: Default Prefilter Policy
- Network Discovery
- Device Configuration (Details)
- Rule Update (2017-09-13-001-vrt)
- VD6 (Build 290 - 2017-09-20 18:50:28)
- Snort Version 2.9.12 (Build 1092 - daq7)

Selected devices: 1

Deploy Cancel

Deploying Changes

Changes don't take effect until you deploy the policy

The screenshot shows the Cisco FPR4K configuration interface. The 'Policies' tab is active, and the 'Deploy' button in the top right is highlighted with a red box. A 'Deploy Policies' dialog box is open, showing a table of policies. The 'Inspect Interruption' column for the 'FPR4K' policy is highlighted with a red box and labeled 'No'. A blue arrow points from a text box to this 'No' value. Another blue arrow points from the same text box to the 'Inspect Interruption' checkbox in the 'Columns' menu, which is also highlighted with a red box. The 'Deploy' button at the bottom of the dialog is also highlighted with a red box. A list of policy components is shown on the left, including Access Control Policy, SSL Policy, Intrusion Policy, DNS Policy, Prefilter Policy, Network Discovery, Device Configuration, Rule Update, VDB, and Snort Version.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control Access Control Network Discovery Application Detectors Correlation Actions

FPR4K

Prefilter Policy: Default Prefilter Policy

Rules Security Intelligence HTTP Responses

Filter by Device

#	Name	Source Zones	Dest Zones
Mandatory - FPR4K (1-2)			
1	Allow All URLs	Any	Any
2	Allow All	Any	Any
Default - FPR4K (-)			
There are no rules in this section. Add Rule or Add Category			

Default Action

Deploy Policies Version: 2018-03-05 01:43 AM

Device	Inspect Interruption	Type	Group	Current Version
<input checked="" type="checkbox"/> FPR4K	No	FTD		2018-03-05 01:35 AM

Columns: ☒ Device ☒ Inspect Interruption ☒ Type ☒ Domain ☒ Group ☒ Current Version

Selected devices: 1

Deploy Cancel

Displaying 1 - 2 of 2 rules | Page 1 of 1

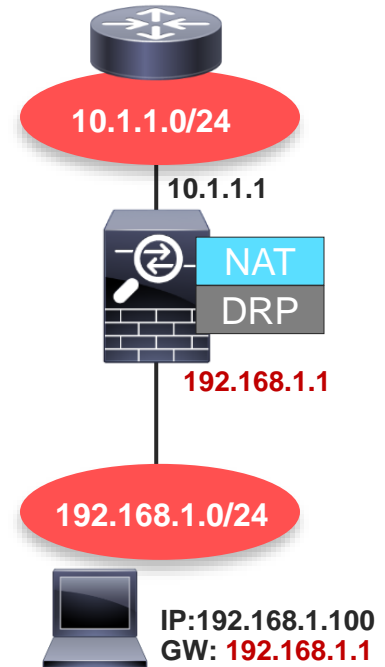
Enable to add column to show if traffic interruption will occur during policy deploy



Firewall Deployment Mode & Interfaces

Firewall Design: Modes of Operation

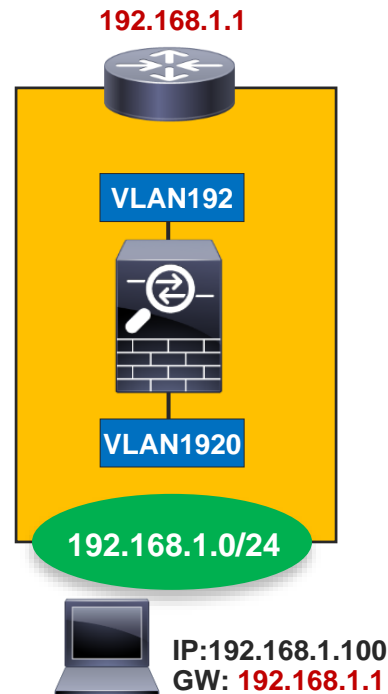
- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts.



DRP: Dynamic
Routing Protocol

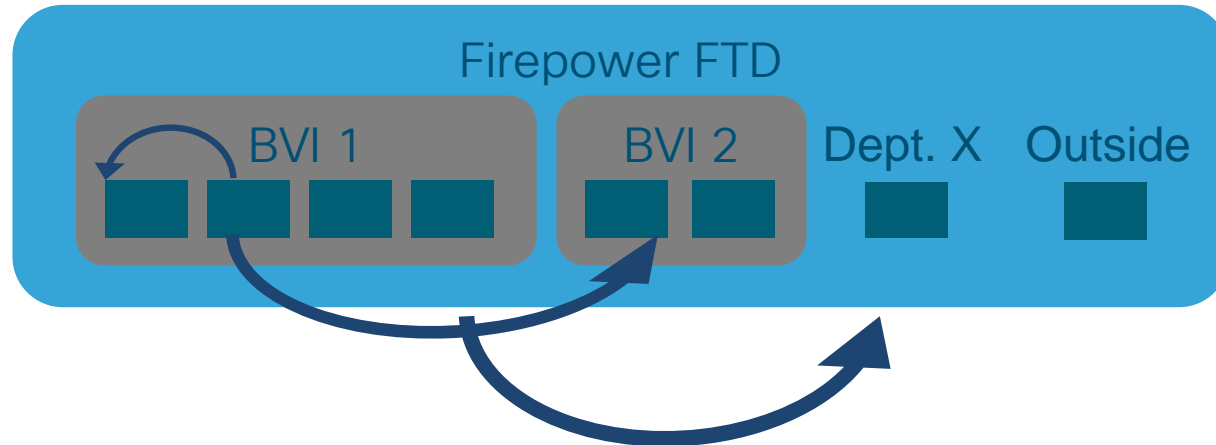
Firewall Design: Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts.
- **Transparent Mode** is where the firewall acts as a bridge functioning at L2.
 - Transparent mode firewall offers some unique benefits in the DC.
 - Transparent deployment is tightly integrated with our ‘best practice’ data center designs.
- **Integrated Routing and Bridging (IRB)** allows a firewall to both route and bridge for the same subnet.
 - Available in Routed Mode when standalone or HA pair
 - Not currently supported with Clustering
 - Useful for micro-segmentation and switching between interfaces


















Integrated Routing and Bridging

- Allows configuration of bridges in routed firewall mode
- Regular routed interfaces can now co-exist with BVI interfaces and interfaces that are members of bridge groups.



FTD Security Zones

- True zone based firewall
- Security Zones are collections of interfaces or sub-interfaces
- Policy rules can apply to source and/or destination security zones
- ASA Interface Security levels are not available

Name ^	Type	Interface Type	
 dmz1	Security Zone	Routed	 
 Edge-FW1			
 dmz1			
 inside	Security Zone	Routed	 
 Edge-FW1			
 inside			
 outside	Security Zone	Routed	 
 Edge-FW1			
 outside			

Routed/Transparent Interface Types

Standalone Interface



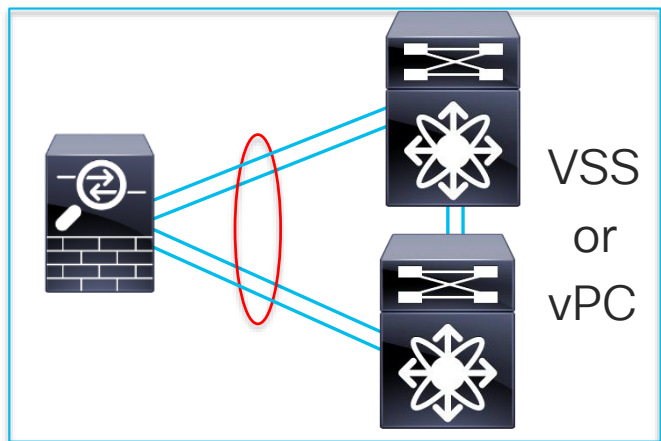
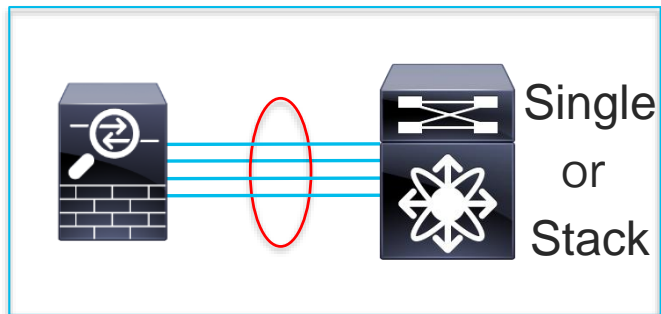
- All platforms
- No redundancy
- Simple

EtherChannel Interface



- All platforms
- Up to 16 active links
- Requires stack, VSS or vPC when connected to multiple switches

EtherChannel on FTD



- Supports 802.3ad and LACP standards
 - Direct support for vPC/VSS
 - FPR2100/FPR4100/FPR9300 require LACP w/ 6.2.3
 - FPR4100/9300 support EtherChannel "On" mode w/ 6.3
- Up to 16 active links
 - 100Mb, 1Gb, 10Gb, 40Gb are all supported – must match
- Supported in all modes (transparent and routed)
- FXOS EtherChannels have the LACP rate set to fast by default.
 - Recommended to change to fast on switch interfaces when clustering
 - <https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html>



Routing on FTD

Routing on FTD

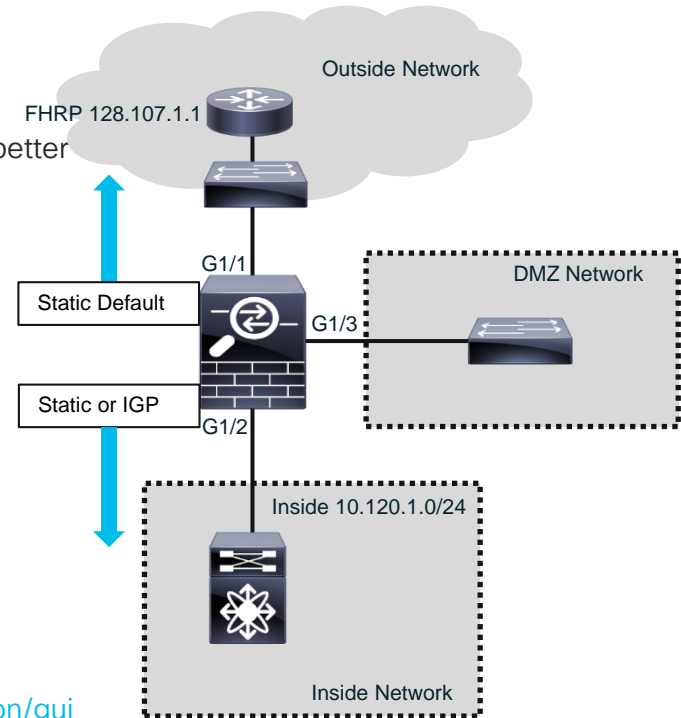
- FTD performs L3 route lookup as part of its normal packet processing flow
 - FTD is optimized as a flow-based inspection device
 - For smaller deployments, FTD is perfectly acceptable as the router
 - For larger deployments, a dedicated router (ISR, ASR, Nexus) is a much better option.
 - For SD WAN deployments, Viptela is a much better option.
 - FTD may originate routes depending on the network design

- FTD Supports static routing and most IGP routing protocols:

- BGP-4 with IPv4 & IPv6 (aka BGPv4 & BGPv6)
- OSPFv2 & OSPFv3 (IPv6)
- RIP v1/v2
- Multicast
- EIGRP (via FlexConfig)
- PBR(via FlexConfig)

- Complete IP Routing config:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/routing_overview_for_firepower_threat_defense.pdf



FHRP: First Hop Redundancy Protocol

A decorative pattern at the top of the slide consisting of numerous vertical bars of varying heights and small circles, all in a dark blue color, set against a lighter blue background.

NAT on FTD

NAT on FTD

- NAT on FTD is built around objects, with two types of NAT:
 - **Auto NAT** – Only source is used as a match criteria
 - Only used for static or dynamic NAT
 - When configuring, it is configured within a network object (internally)
 - Device automatically orders the rules for processing:
 - Static over dynamic
 - Quantity of real IP addresses – from smallest to largest
 - IP address – from lowest to highest
 - Name of network object – in alphabetical order
 - **Manual NAT** – Source (and possibly destination) is used as a match criteria
 - More flexibility in NAT rules (one-to-one, one-to-many, many-to-many, many-to-one)
 - Supports NAT of the source and destination in a single rule
 - Only the order matters for processing

NAT on FTD Processing

- Single NAT rule table (matching on a first match basis).
- Uses a simplified “Original Packet” to “Translated Packet” approach:

		Original Packet				Translated Packet					
#	Direction	Type	Source Interface Obj...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1	↔	Static	inside	outside	IPv4-Host-192.168.1.10	IPv4-Host-192.168.1.155		IPv4-Host-128.107.1.242	IPv4-Host-128.107.1.155		Dns:false
2	↔	Static	inside	pubdmz	IPv4-10.1.2.0-24			IPv4-10.120.1.0-24			Dns:false
3	↔	Static	inside	pubdmz	IPv4-Host-10.120.2.100			IPv4-Host-10.120.2.100			Dns:false
▼ Auto NAT Rules											
#	→	Dyna...	inside	outside	IPv4-10.120.1.0-24			Interface			Dns:false
#	↔	Static	inside	outside	IPv4-Host-172.16.25.200			IPv4-Host-128.107.1.200			Dns:false
▼ NAT Rules After											

Manual NAT

- NAT is ordered within 3 sections.
 - Section 1 – NAT Rules Before (Manual NAT)
 - Section 2 – Auto NAT Rules (Object NAT)
 - Section 3 – NAT Rules After (Manual NAT – Not Typically Used)

Manual NAT Use Case

Static NAT 192.168.1.10 → 192.168.1.155 to 128.107.1.242 → 128.107.1.155

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static ☒ Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- outside
- prtdmz
- pubdmz
- inside
- diversion
- byod

Source Interface Objects (1) inside

Destination Interface Objects (1) outside

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static ☒ Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* IPv4-Host-192.168.1.10

Original Destination: Address

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address

Translated Destination: IPv4-Host-128.107.1.155

Translated Source Port:

Translated Destination Port:

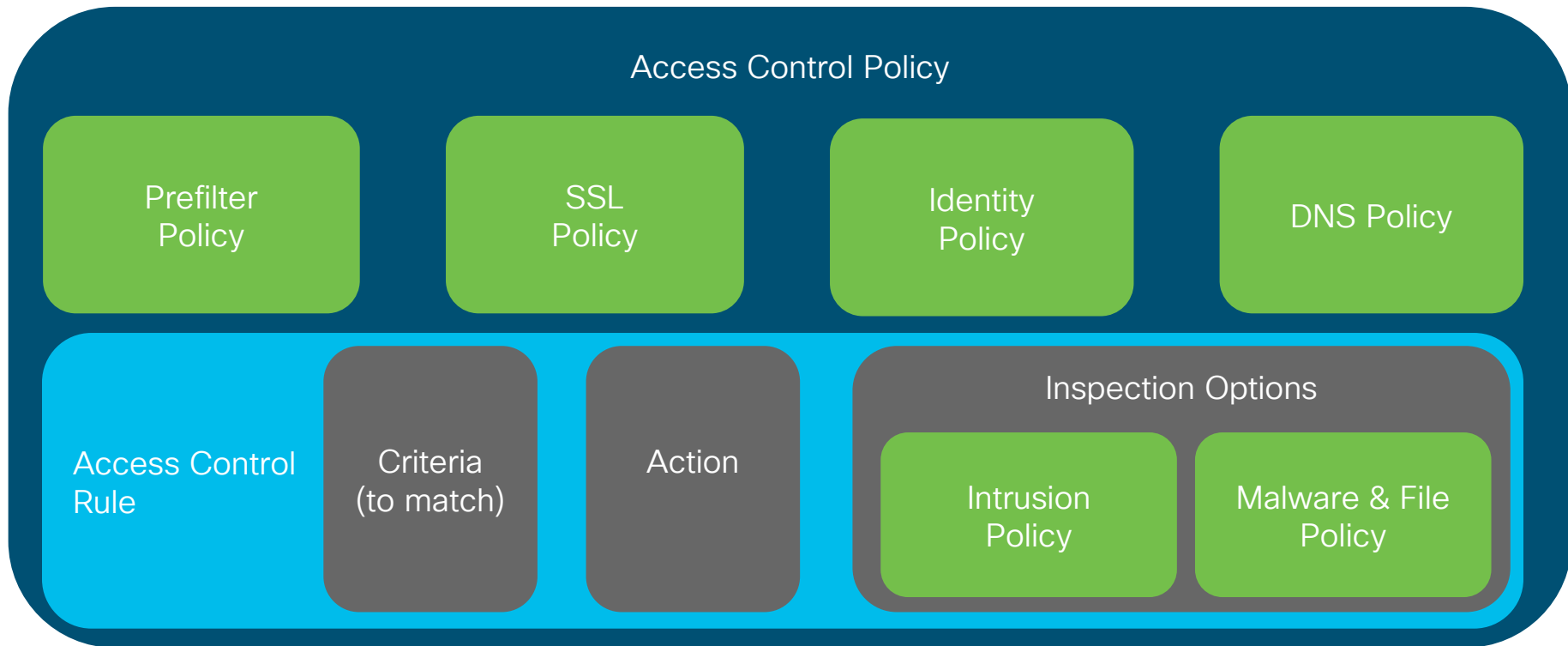
OK Cancel



FTD NGFW Policy Tips

Access Control Policy

The glue that ties everything together



NGFW Policy Types in FTD

Policy Type	Function
Access Control	Specify, inspect and log network traffic
Intrusion	Inspect traffic for security violations (including block or alter)
Malware & File	Detect and inspect files for malware (including block)
SSL	Inspect encrypted traffic (including decrypt and block)
DNS	Controls whitelisting or blacklisting of traffic based on domain
Identity	Collect identity information via captive portal
Prefilter	Early handling of traffic based L1-L4 criteria

URL Policy: It is configured within the ACR

Access Control Policy Overview

- Controls what and how traffic is allowed, blocked, inspected and logged
- Simplest policy contains only default action:
 - Block All Traffic
 - Trust All Traffic – Does not pass through Intrusion and Malware & File inspection
 - Network Discovery – Discovery applications, users and devices on the network only
 - Intrusion Prevention – Using a specific intrusion policy
- Criteria can includes zones, networks, VLAN tags, applications, ports, URLs and SGT/ISE attributes
- The same Access Control Policy can be applied to one or more device
- Complex policies can contain multiple rules, inherit settings from other access control policies and specify other policy types that should be used for inspection

Access Control Policy Use Case #1 – Logging Tab

Allow MS SQL from inside to pubdmz

Add Rule

Name: Allow MS SQL to pubdmz ☒ Enabled Insert: into Default

Action: ☒ Allow

Logging Tab:

- ☒ Log at Beginning of Connection
- ☐ Log at End of Connection

File Events:

- ☐ Log Files

Send Connection Events to:

- ☒ Event Viewer
- ☐ Syslog - ☐ SNMP Trap

Log at Beginning of Connection and Send Connection Events to: Event Viewer are highlighted with red boxes.

Logging will increase the number of events the FMC must handle. Be sure to consider your logging requirements before logging connection events to the FMC

Logging Considerations for Large Deployments

Americas - DC #1



Americas - DC #2



EMEA - DC #1



EMEA - DC #2



APJC - DC #1



Total = 10x FP4150s

1 FP4150 = 200K CPS

Policy With Full Logging:
10x FP4150s = 2M EPS



1x FMC4600
Rated for 20K EPS

Logging Design for Large Deployments

6.3+
Example

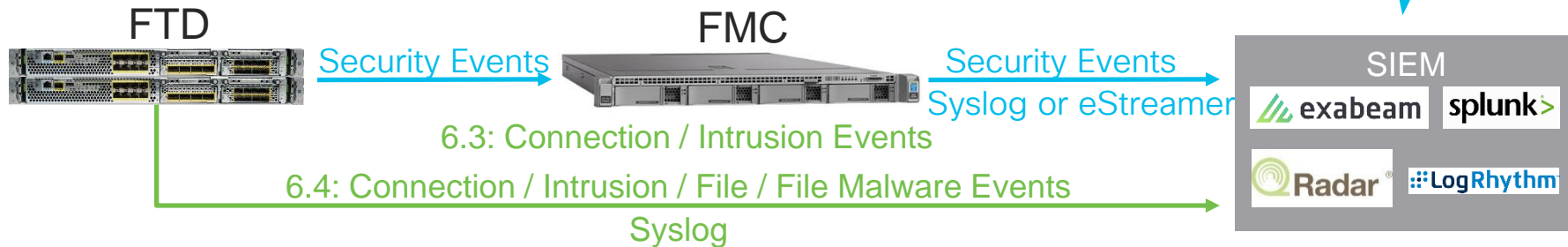


Diagram illustrating the configuration of logging settings in the Cisco FTD GUI, specifically the **Logging** tab.

The configuration shows the following settings:

- ☒ 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

Annotations:

- Uncheck – Even when unchecked, security events and security related connection events are always sent to FMC
- Check to enable syslog directly from FTD

FTD 6.3+ – Logging Tab in Access Control Policy

Allows more global control of syslog and more flexible syslog settings

Rules **Security Intelligence** **HTTP Responses** **Logging** **Advanced**

Default Syslog Settings:

The following configuration will be used for all syslog destinations in this AC policy and all included SSL, Prefilter and Intrusion policies unless explicitly overridden.

☒ Send using specific syslog alert

Syslog Alert:

☐ FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device

Syslog Severity:

File and Malware Settings

☐ Send Syslog messages for File and Malware events

Default syslog settings configured above are used for syslog destinations for File and Malware events [Show Overrides](#)

Summary

FTD Version 6.3 and later
Send using syslog alert 'SIEM'

All other devices
Send using syslog alert 'SIEM'

Applies to all devices. Syslog connection log format will change after FTD (not FMC) is upgraded from pre-6.2.3 to 6.3+

Allows you to have different syslog servers per region (NAM, EU, APJC) but still use the same policy

SSL Policy Overview

- Controls how and what encrypted traffic is inspected and decrypted
- Simple policy blocks all encrypted traffic that uses a self-signed certificate
- Actions are:
 - Decrypt - Resign - Used for SSL decryption of public services (Google, Facebook, etc.)
 - Decrypt - Known Key - Used when you have the certificate's private key
 - Do not decrypt
 - Block
 - Block with reset
 - Monitor
- Many actions can be taken on encrypted traffic without decryption by inspecting the certificate, distinguished name (DN), certificate status, cipher suite and version (all supported by FTD)

Setting Up an SSL Policy

Step #1 – Import Root or Certificates (If Doing Decryption)

Overview Analysis Policies Devices **Objects** Deploy System Help Cisco_Backend \ Cisco_SOC \ schimes

Object Management Intrusion Rules

Internal CA certs w/ private key that can be used to spoof resign public certificates. Used for “Decrypt – Resign”.

Internal CAs

Name	Domain	Value
Cisco_dCloud_Root_CA_1	Global	CN=Cisco dCloud Class 3 Root CA 1

Trusted CAs

CAs that are trusted. SSL policy can specify clients can only connect to sites signed by these CAs

External Certs

Internal Certs

Certs that are trusted. SSL policy can specify clients can only connect to sites with these certs

Cert Enrollment

Internal CA Groups

Trusted CA Groups

Internal Cert Groups

External Cert Groups

Internal certs w/ private key that can be used for decryption without resigning. Used for “Decrypt – Known Key”.

Setting Up an SSL Policy

Example: Create the SSL Rule

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The 'Policies' tab is active, and the 'Access Control > SSL' sub-tab is selected. The 'Add Rule' dialog is open, showing the configuration for a new SSL rule. The 'Name' field is 'Block Self Signed Certificates'. The 'Action' dropdown is set to 'Do not decrypt'. The 'Zone' dropdown is set to 'Block'. The 'Source Zones (0)' and 'Destination Zones (0)' fields are empty. The 'Add to Source' and 'Add to Destination' buttons are visible. The background shows the 'Policies' tab with 'Access Control > SSL' selected.

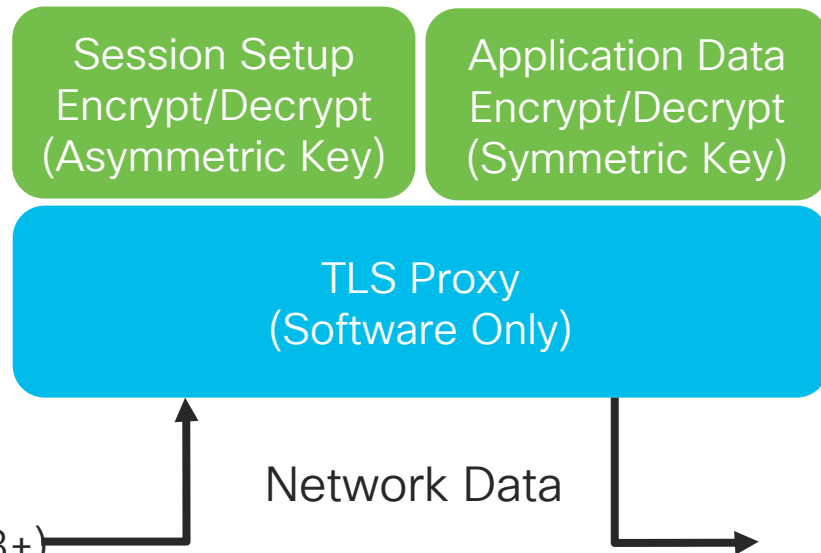
For public servers (you don't control)

For servers you control

SSL/TLS Hardware Acceleration

Technically always TLS, but is called SSL in pre-6.4 versions

- TLS hardware acceleration consists of three components (simplistically):
 - TLS Proxy
 - Session Setup Encrypt/Decrypt (Asymmetric Key)
 - Application Data Encrypt/Decrypt (Symmetric Key)
- TLS Proxy is always done in software
- Encrypt/Decrypt can be done in hardware on:
 - Firepower 4100/9300 series (6.2.3+)
 - Firepower 1000 (6.4+) & 2100 series (6.3+)



NTP Config #1 – FXOS

A leading cause of “no events are showing up in my FMC”...

Overview Interfaces Logical Devices Security Engine **Platform Settings** System Tools Help admin

► **NTP**

- SSH
- SNMP
- HTTPS
- AAA
- Syslog
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- Resource Profiles
- Chassis URL

Time Synchronization Current Time

Set Time Source

☐ Set Time Manually

Date: (mm/dd/yyyy)

Time: PM (hh:mm)

NTP Server Authentication: ☐ Enable

☒ **Use NTP Server**

FXOS does not sync time from FMC. Use the same NTP servers as FMC

NTP Server	Server Status	Actions
172.18.108.15	Candidate	
172.18.108.14	Synchronized	

Ensure the Server Status is Synchronized

1 Use same settings on Firepower Management Center managing this application in case you are running a Firepower Threat Defense Device.

NTP Config #2 – FMC for Non-FXOS Devices

A leading cause of “no events are showing up in my FMC”...

The screenshot shows the Cisco FMC interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices' (selected), 'Objects', 'AMP', and 'Intelligence'. Below this, there are tabs for 'Device Management', 'NAT', 'VPN', 'QoS', 'Platform Settings' (selected), 'FlexConfig', and 'Certificates'. The main content area is titled 'Threat Defense Policy' with a sub-header 'Enter Description'. On the left, a sidebar lists various settings: ARP Inspection, Banner, DNS, External Authentication, Fragment Settings, HTTP, ICMP, Secure Shell, SMTP Server, SNMP, SSL, Syslog, Timeouts, **Time Synchronization** (highlighted with a red arrow), and UCAPL/CC Compliance. The 'Time Synchronization' section contains two radio buttons: 'Via NTP from Management Center' (selected and highlighted with a red box) and 'Via NTP from' (with an empty text field below it). A blue callout box points to the 'Via NTP from Management Center' option with the text: 'For FTD, defined in a Threat Defense policy. For legacy Firepower, defined in a Firepower policy'. Another blue callout box points to the 'Policy Assignments (6)' link in the top right corner with the text: 'Ensure all the necessary/new devices are added'. A third blue callout box points to the 'Via NTP from Management Center' option with the text: 'Using “Via NTP from the Management Center” is the default and general best practice for non-FXOS devices (e.g. FPR2100)'. The bottom of the page features the Cisco Live! logo and a footer with the text 'BRKSEC-2020 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public 111'.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS **Platform Settings** FlexConfig Certificates

Threat Defense Policy
Enter Description

Save Cancel

Policy Assignments (6)

Set My Clock

☒ Via NTP from Management Center

☐ Via NTP from

This setting is unsupported on firepower 9300 and Firepower 4100 platforms. Please use Firepower Chassis Manager instead to set NTP time synchronization.

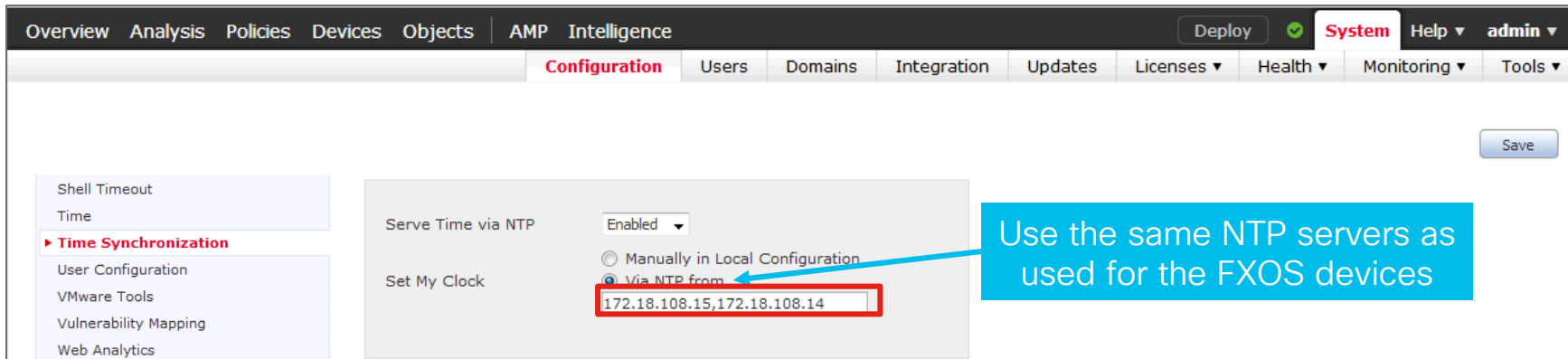
Using “Via NTP from the Management Center” is the default and general best practice for non-FXOS devices (e.g. FPR2100)

Ensure all the necessary/new devices are added

For FTD, defined in a Threat Defense policy
For legacy Firepower, defined in a Firepower policy

NTP Config #3 – FMC Itself

A leading cause of “no events are showing up in my FMC”...



The screenshot shows the Cisco FMC web interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Configuration' tab is active, showing sub-tabs for Users, Domains, Integration, Updates, Licenses, Health, Monitoring, and Tools. The left sidebar lists configuration categories: Shell Timeout, Time, Time Synchronization (highlighted), User Configuration, VMware Tools, Vulnerability Mapping, and Web Analytics. The main content area shows the 'Time Synchronization' configuration. Under 'Serve Time via NTP', the status is 'Enabled'. Under 'Set My Clock', the option 'Via NTP from' is selected, and the IP addresses '172.18.108.15,172.18.108.14' are entered in the text field. A blue callout box with an arrow points to the IP addresses, stating: 'Use the same NTP servers as used for the FXOS devices'. A 'Save' button is located in the top right corner of the configuration area.



Organizing Access Control Rules

Policy Management – Categories

- All access control policies contain two categories – Mandatory and Default
- Customer categories can be created to further organize rules
- Note – After you create a category, you cannot move it. You can delete it, rename it, and move rules into, out of, within, and around it

The screenshot displays the Cisco Policy Manager interface. At the top is a table with columns: #, Name, So... Zo..., Dest Zo..., So... Ne..., Dest Ne..., VL..., Us..., Ap..., So..., De..., URLs, IS... Att..., A..., and a set of icons. Below the table, a list of policy categories is shown. The first two categories, 'Mandatory - Europe Data Center Policy (-)' and 'Default - Europe Data Center Policy (-)', are highlighted with a red box. A blue callout box with an arrow points to the 'Default' category, containing the text 'Present by default, can't be deleted'. Below these are three user-created categories: 'Blanket Rules (-)', 'SAP Rules (-)', and 'Active Directory Rules (-)', which are also highlighted with a red box. A blue callout box with an arrow points to this group, containing the text 'User created categories'. At the bottom, the 'Default Action' is set to 'Access Control: Block All Traffic'.

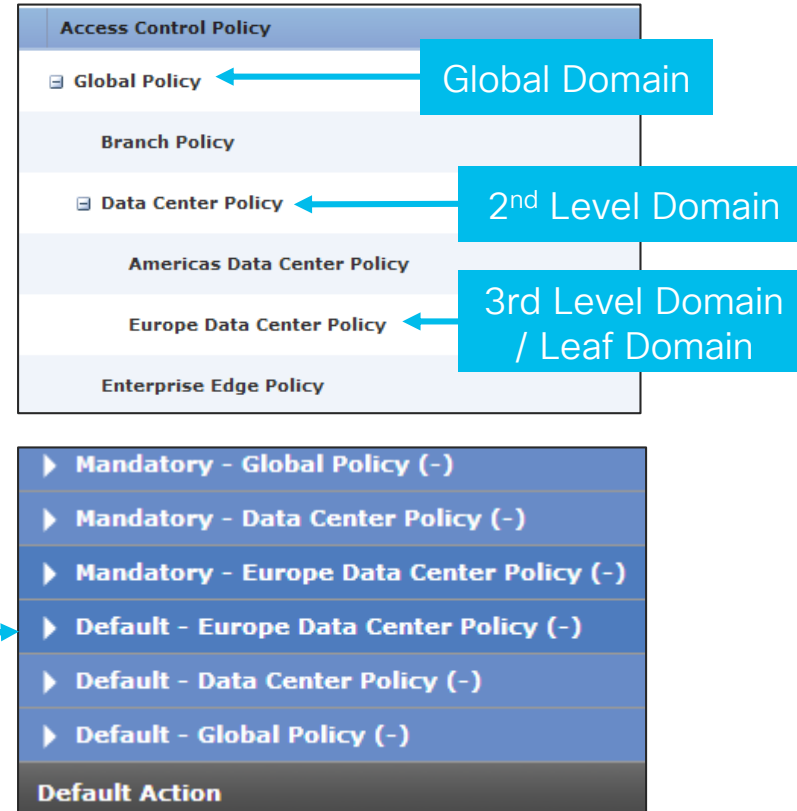
#	Name	So... Zo...	Dest Zo...	So... Ne...	Dest Ne...	VL...	Us...	Ap...	So...	De...	URLs	IS... Att...	A...	Icons
▶	Mandatory - Europe Data Center Policy (-)													
▼	Default - Europe Data Center Policy (-)													
▶	Blanket Rules (-)													✎ 🗑
▶	SAP Rules (-)													✎ 🗑
▶	Active Directory Rules (-)													✎ 🗑

Default Action: Access Control: Block All Traffic

Policy Management – Inheritance

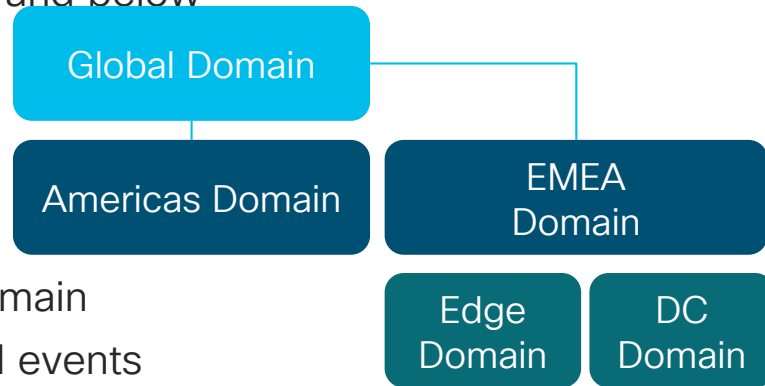
- Allows an access control policy to inherit the access control rules from another policy.
- Two types of sections in an policy:
 - Mandatory – Processed before any rules in a child policy
 - Default – Processed after all mandatory rules and after any default rules from child policies

Example of what the Europe Data Center Policy will look like in the Access Control Policy Editor



Policy Management – Multi-Domain Management

- Multitenancy for the Firepower management console
 - Maximum of 50 (6.0+), 100 (6.5+) or 1024 domains (via expert mode in 6.5+)
 - Maximum of 3 levels deep (2 child domains)
 - Segments user access to devices, configurations and events
 - Users can administer devices in that domain and below
 - Devices are assigned to a domain



- Uses in the Enterprise:
 - Force a policy to apply to all firewalls in a domain
 - Limit user visibility to only select devices and events
 - Delegate admin control while maintaining global visibility/control

Policy Management – Object Overrides

- Allows an object to be reused on multiple firewalls, but with different meanings
- Networks, Ports, VLAN Tags and URLs all support overrides

Example use cases:

- Selectively override an object on the few devices that need a different value
- Create an empty object, so that an override is required for every firewall
- Create a default value in the global domain, but allow subdomain administrators to override the default value

New Network Objects

Name:

Description:

Network:

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides: ☒

Override (2)

Override On	Content	Type	
FP2130-1	203.0.113.0/24	Network	
ASA5515-FTD-1	198.51.100.0/24	Network	

Annotations:

- Default value, can be left empty (points to Network field)
- Enable overrides (points to Allow Overrides checkbox)
- Overridden values (points to the Override table)

Designing Your Access Control Policy

Prefilter Policy (no AVC/IPS/AMP)

Layer 1-4 block rules
and/or

Layer 1-4 allow rules for medium/long* lived flows (e.g. allow backups)

Access Control Policy

Layer 1-4 block rules
and/or

Layer 1-4 allow rules for short lived** flows (e.g. allow Umbrella DNS)

Layer 5 block rules (e.g. block servers with self signed certificates)
and/or

Layer 7 URL block rules (e.g. block URL category Adult)

Layer 7 application block rules (e.g. block Office 365)

Targeted layer 7 allow rules (e.g. allow HTTP with tailored AMP policy)

Generic layer 7 allow rules (e.g. allow all traffic with generic IPS policy)

- Prefilter rules are the fastest
- Any rules that are layer 1-4 based and traffic that does not need security inspection (e.g. backup traffic) should be placed in the prefilter policy for best performance
- Rule order in Access Control Policy is not strictly required
- Leads to the fastest blocking with the fewest number of transmitted packets

*length of flow does not matter on ASA/FPR1000/FPR2100

**length of flow only matters on FPR4100/FPR9300

Best Practices Docs

Cisco Firepower Threat Defense Policy Management Common Practices

NGFW Basic Policy Creation for Firepower



Basic Policy Creation for Firepower

First Published: May 25, 2018
Last Updated: January 30, 2019



Table of Contents

Document Scope: 4

Traffic Flow Overview: 4


Security Intelligence: 4

Access Control Policy: 4

Building an access control policy: 4

Adding Rules to Access Control Policy: 4

NGFW Policy Order of Operations



NGFW Policy Order of Operations

First Published: May 22, 2018
Last Updated: May 22, 2018

Table of Contents

Policy Order of Operations..... 2

Introduction: Purpose..... 2

Policy Firewall: Funnel Approach (Threat tornado) 2

Common Misconceptions: 3

Firewall Funnel Model: 3

Order of Operations Best Practices..... 4

Path of the packet and policy checkpoints: 6

Best practices for policy ordering: 7

Policy Inheritance: 7

Policy Management Table of Contents:

1. Access Policies

- Rationalizing
- Connection Logging
- Defining Flows
- Blocking Bad Traffic
- Determining What Needs Encryption

2. IPS Policies

- Testing Policies
- Leveraging Firepower Recommendations
- Deploying Strict Controls
- Leverage X-Forwarding
- Fine-Tuning Rules

3. Malware Policies

4. SSL Policies

5. Identity Policies

6. Network Analysis Policies

https://explore.cisco.com/ngfw_ftd_common-practices/ngfw-ftd-policy-mgmt

https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/Basic_Policy_Creation_on_Cisco_Firepower_Devices.pdf

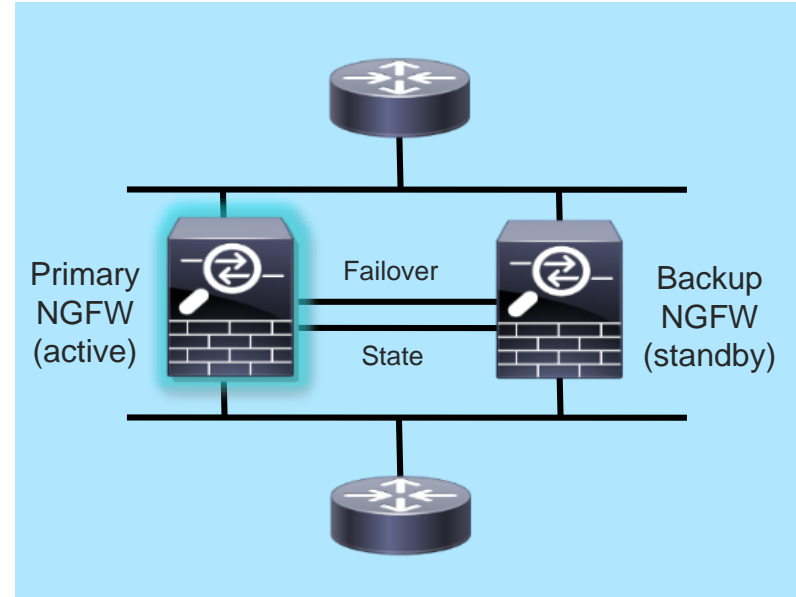
https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/NGFW_Policy_Order_of_Operations.pdf



FTD High Availability

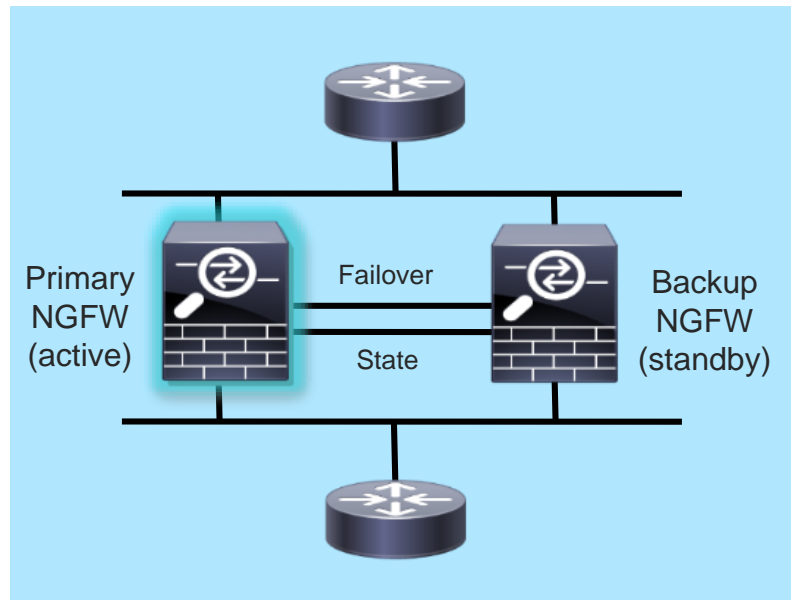
Firepower Threat Defense High Availability

- Supported on all physical models and ESXi
- Stateful Active/Standby failover only
- All features are supported with failover
- Both NGFWs in pair must be identical in software, memory, interfaces and mode
- On FPR9300, failover is only supported
 - Across blades in different chassis
 - In non-cluster mode
- Long distance LAN failover is supported if latency is less than 250 ms



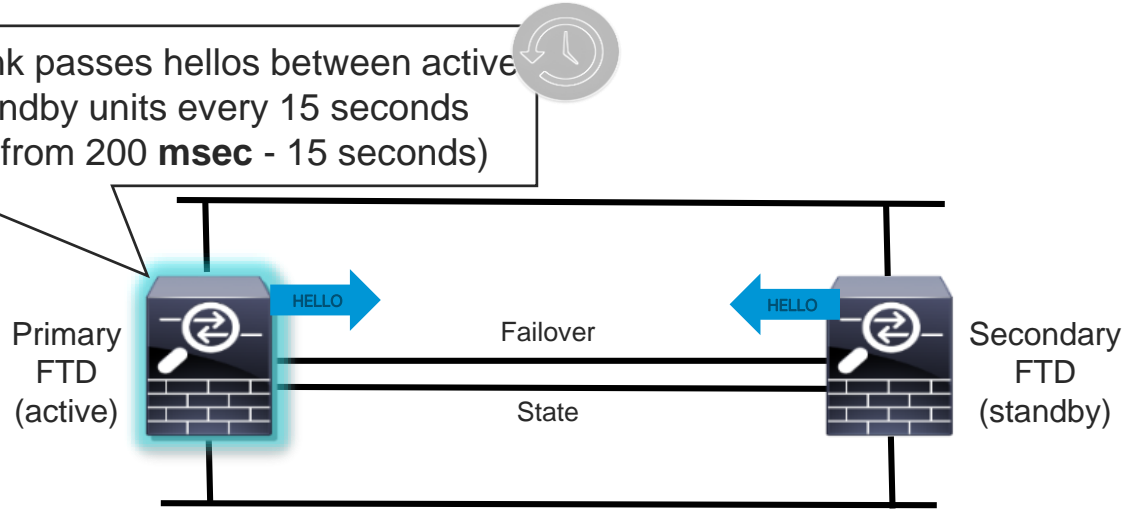
Firepower Threat Defense High Availability (Part 2)

- Two nodes connected by one or two dedicated connections called “failover links”
 - Failover and state
 - Can use the same link for both
 - Best practice is to use a dedicated link for each if possible
- When first configured, Primary’s policies are synchronized to Secondary
- Configuration/policy updates are sent to current active node by FMC
- Active unit replicates policies to standby

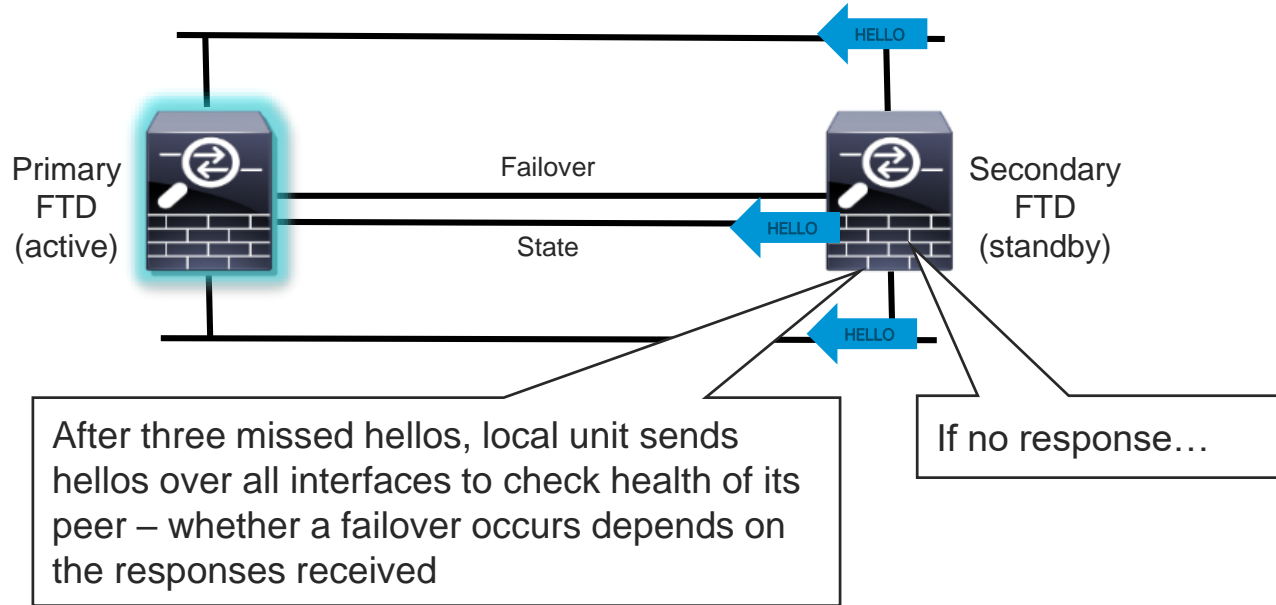


How Failover Works

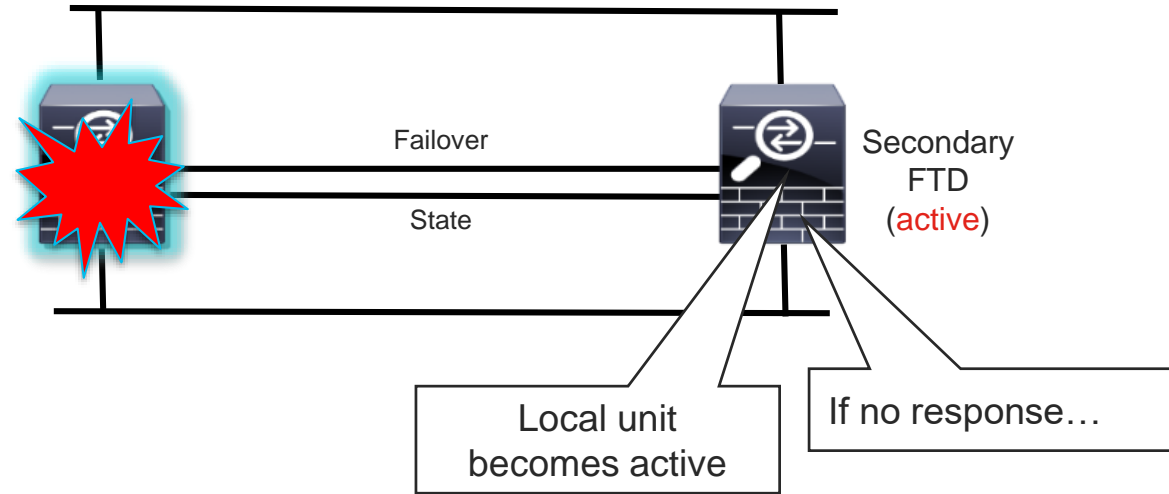
Failover link passes hellos between active and standby units every 15 seconds (tunable from 200 msec - 15 seconds)



How Failover Works

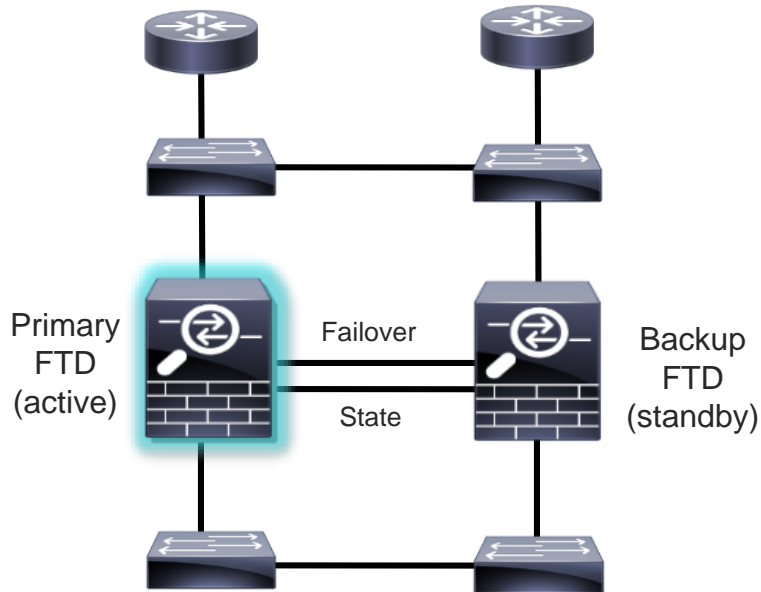


How Failover Works

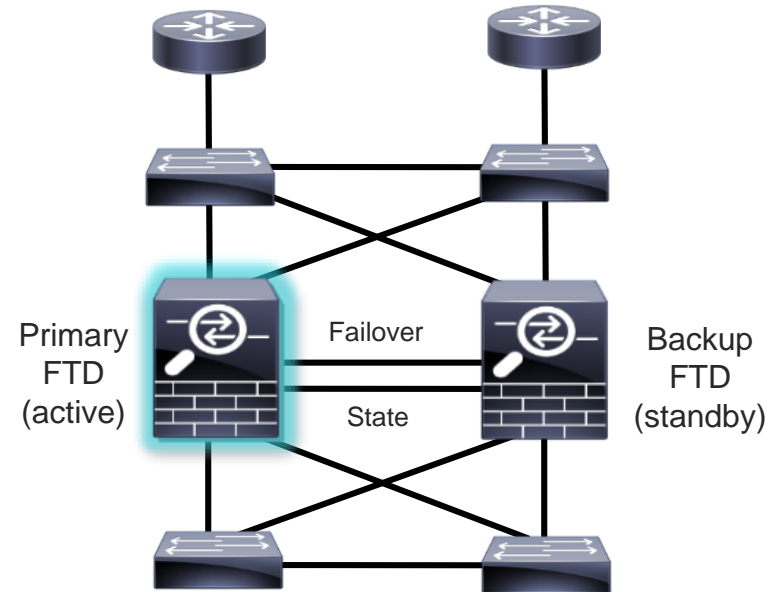


HA with Interface Redundancy

Before...

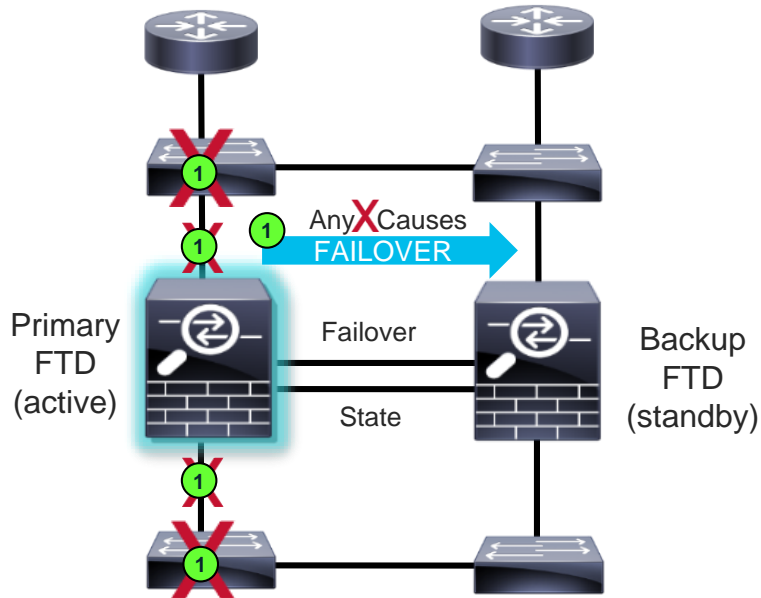


After with redundant interfaces

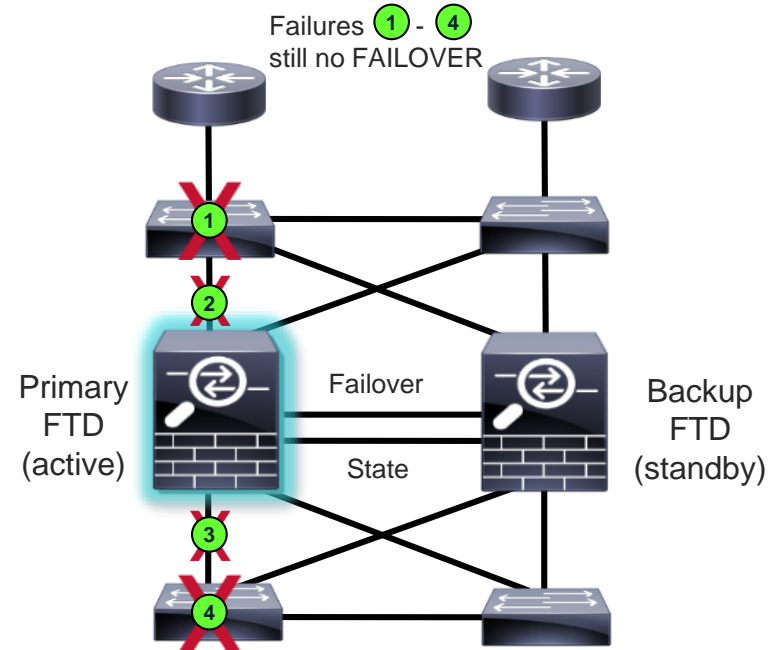


HA with Interface Redundancy

Before...



After with redundant interfaces



Port Channel feature makes this concept somewhat obsolete if switches support VSS/vPC

Deploying Active/Standby Failover – Secondary IPs

Required to send hellos between data interfaces

Overview Analysis Policies Devices Objects AMP

Edge-FW Cisco ASA5506W-X Threat Defense

Summary High Availability Devices Routing Interfaces Inline Sets DHCP

High Availability Configuration

High Availability Link

Interface

Logical Name

Primary IP

Secondary IP

Subnet Mask

IPsec Encryption

Monitored Interfaces

Interface Name Active IPv4 Standby IPv4 Act

Interface Name	Active IPv4	Standby IPv4	Act
byod	10.255.255.254		
redundant2			
prtdmz	10.151.100.254		
outside	128.107.1.128		
diversion	10.2.1.254		
pubdmz	10.150.1.254		

Edit byod

☒ Monitor this interface for failures

IPv4 IPv6

Interface Name: byod

Active IP Address: 10.255.255.254

Mask: 24

Standby IP Address: 10.255.255.253

OK Cancel

Edit interfaces to add standby IP addresses for better interface monitoring

172.31.1.6

255.255.255.252

Standby Link-Local IPv6 Monitoring

Deploying Active/Standby Failover – MAC Address

For stability, set virtual MAC address

Edit Sub Interface ? X

Name: ☒ Enabled ☐ Management Only

Security Zone: ▼

Description:

General IPv4 IPv6 **Advanced**

Information ARP Security Configuration

Active Mac Address:

Standby Mac Address:

DNS Lookup: ☐

OK Cancel

Not required functionally, but best set for stability

Why? Traffic disruption due to MAC address changes:

- If the secondary unit boots without detecting the primary unit, the secondary unit becomes the active unit and uses its own MAC addresses. When the primary unit becomes available, the secondary (active) unit changes the MAC addresses to those of the primary.
- If the primary unit is replaced with new hardware, the MAC addresses from the new primary are used.



FTD Clustering Overview

FTD Clustering Basics

- Designed to solve two critical issues with firewall HA:
 - Aggregates firewall capacities for DC environments (bandwidth, connections/sec, etc.)
 - Provides dynamic N+1 stateful redundancy with zero packet loss
- Two types of clustering:
 - Intra-chassis clustering – Supported (9300 only)
 - Inter-chassis clustering – Supported (4100 or 9300)

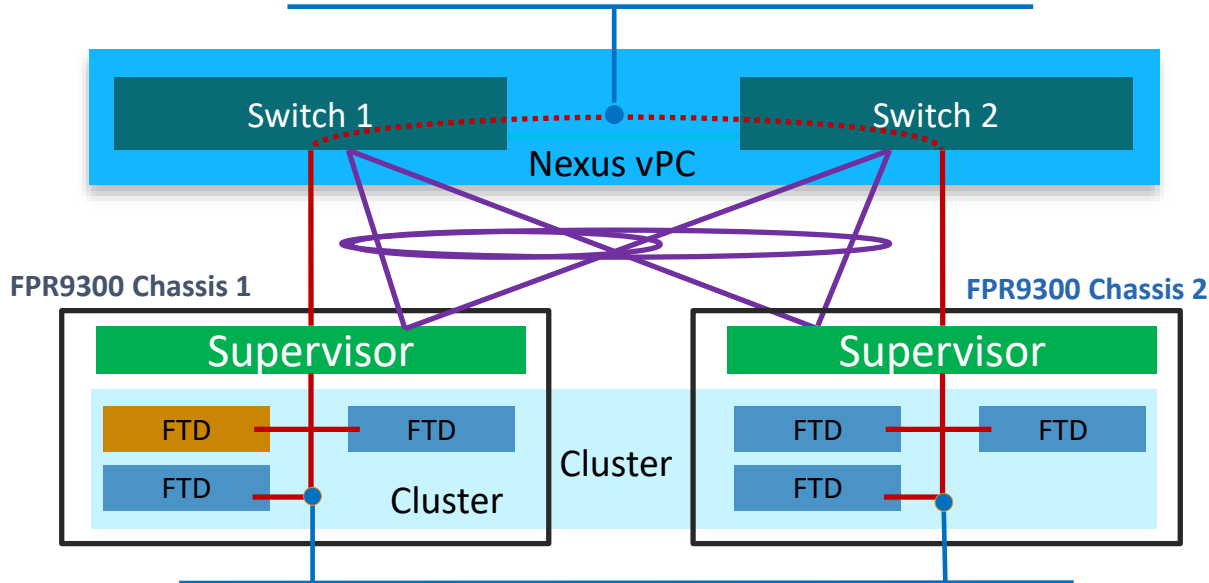
Highly Reliable
Scalable
Available



FTD Clustering Types with FP9300

FTD Inter-Chassis Cluster

- Cluster of up to 6 modules (across 2 – 6 chassis)
- Off-chassis flow backup for complete redundancy

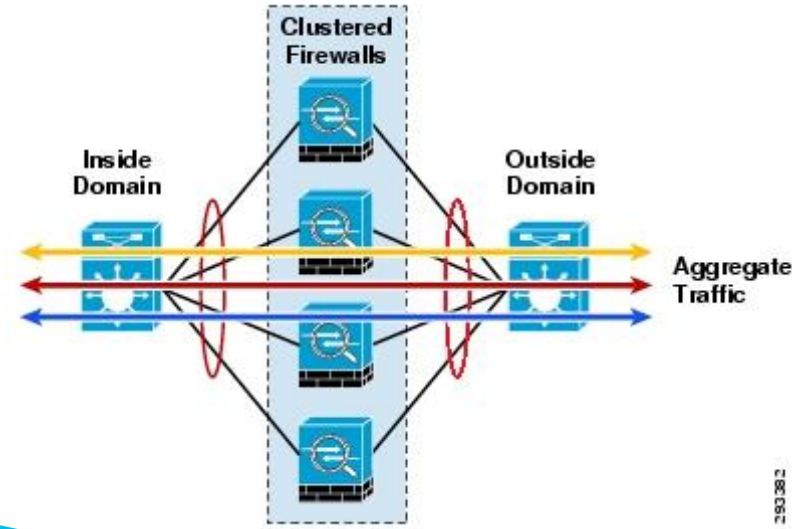


FTD Intra-Chassis Cluster

- Modules can be clustered within chassis
- Bootstrap configuration is applied by Supervisor

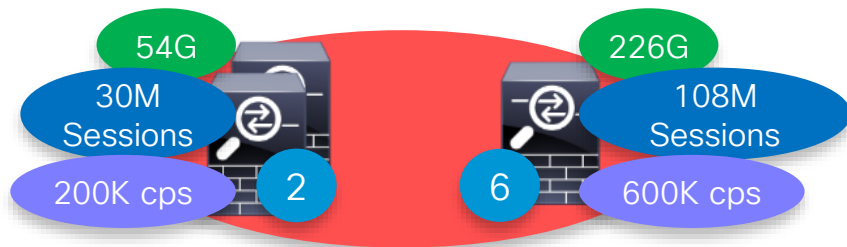
Inter-Chassis Clustering

- All NGFWs in cluster must be identical:
 - 9300 – modules must be the same type. Ex: SM40 with SM48
 - 4100 – chassis must be the same model
- Only Spanned EtherChannel mode (L2) is supported
- Equal-Cost Multi-Path (ECMP) mode (L3) is **not** supported
- Requires at least FXOS 2.1.1 and FTD 6.2
- Not yet supported with Multi-Instance. Targeting **FTD 6.6** and **FXOS 2.8.1** releases



For practical purposes, use
FXOS 2.6.x and FTD 6.4.0.x

Cluster Scalability – FTD 6.4.0.7 Example



Bandwidth

70% Avg.



100% with no
Asymmetry*

Example

2 Firepower 9300s w/ 6 Total SM-44 Modules at 54 Gbps → 226 Gbps of throughput

Concurrent Sessions

60%

Example

2 Firepower 9300s w/ 6 Total SM-44 Modules at 30M → 108M concurrent sessions

New Connection Rate

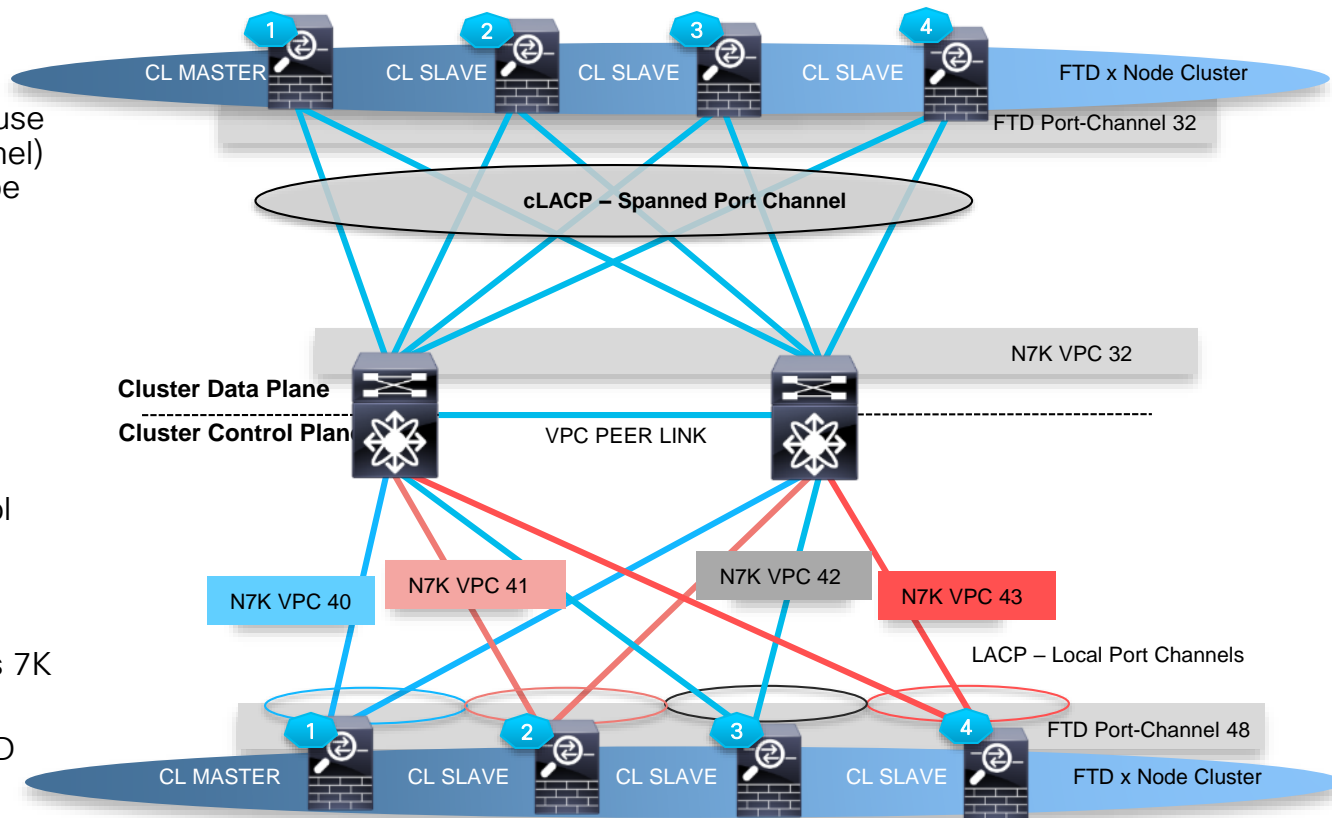
50%

Example

2 Firepower 9300s w/ 6 Total SM-44 Modules at 300K → 900K connections/sec

Correct Use of EtherChannels When Clustering with VPCs

- **Data Plane** of Cluster MUST use cLACP (Spanned Port-Channel)
VPC Identifier on N7K must be the same for channel consistency
- **Control Plane** [Cluster Control Link] of Cluster MUST use standard LACP (Local Port-Channel)
- Each VPC Identifier on Nexus 7K is unique
- Port Channel Identifier on FTD defaults to 48



Data Center – Cluster Connectivity Preferences

Firewall on a Stick



#1
Choice

- Single EtherChannel for the inside and outside

Same Model Switches



#2
Choice

- Two EtherChannels to different switch pairs
- Same model switch

Different Model Switches



#3
Choice

- Two EtherChannels to different switch pairs
- Different model switches

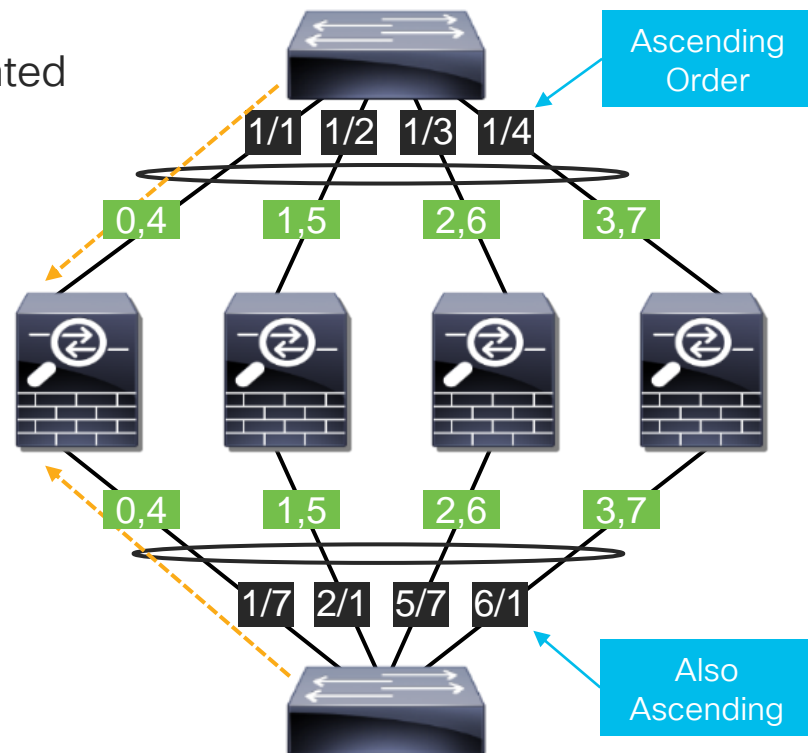
Data Center - Using 2 Different Switches

Switch Port Numbers Matter

EtherChannel **RBH values** are sequentially allocated in ascending order starting from the lowest numeric line card and port ID.

For best cluster performance, keep traffic symmetric and off the CCL:

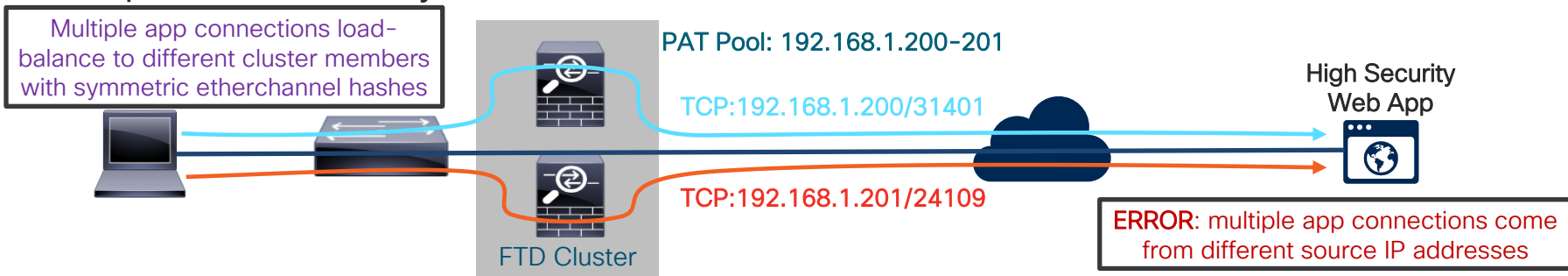
- Use a symmetric hashing algorithm
- Use fixed RBH allocation for EtherChannels
e.g. `port-channel hash-distribution fixed` on Nexus 7K and Catalyst 6500
- Links should be connected in matching ascending order on each switch



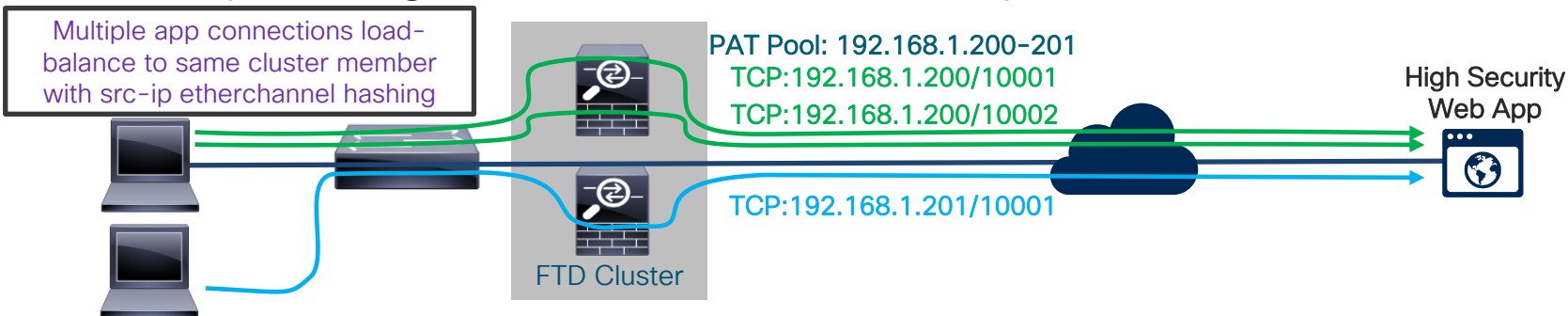
Configuring Load Balancing Using Port Channels in Nexus 7000 Series NX-OS Interfaces Configuration Guide:
<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/interfaces/configuration/guide/b-Cisco-Nexus-7000-Series-NX-OS-Interfaces-Configuration-Guide-Book/configuring-port-channels.html>

PAT in Clustering for Internet Egress

PAT pool is uniformly distributed to all cluster members at IP level



Use src-ip hashing on client side switch to keep NAT IPs consistent



Other PAT with Cluster Best Practices

- Ensure there are as many or more IPs in the PAT pool as there are cluster members or required for translations
 - 4 cluster members = 4+ IPs in PAT pool, 8+ is ideal
 - 250k translations = 4+ IPs in PAT pool, 8+ is deal
- Use flat port range option
 - Stops FTD from prematurely moving to next PAT IP due to high low port range usage
 - Helps keep PAT IP pool IP distribution even across the cluster members (each unit owns one or more IP)

Original Src Port	Translated Src Port	Translated Src Port (flat)
1-511	1-511	1024-65535
512-1023	512-1023	1024-65535
1024-65535	1024-65535	1024-65535

Edit NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category

Type: Dynamic ☒ Enable

Description:

Interface Objects Translation **PAT Pool** Advanced

☒ Enable PAT Pool

PAT: Address Cluster-PAT-Pool

☐ Use Round Robin Allocation

☐ Extended PAT Table

☒ Flat Port Range

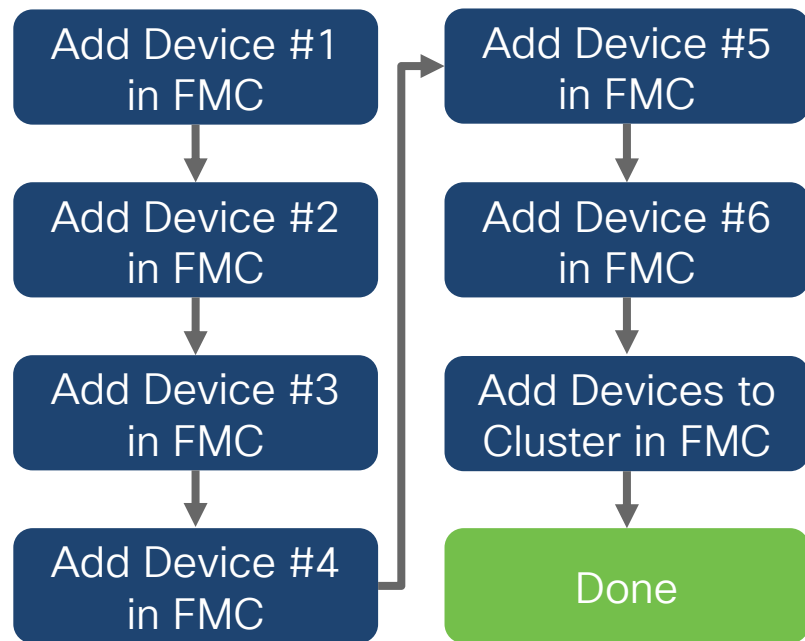
☐ Include Reserve Ports

These ranges can fill up quickly if NTP, NETBIOS, etc. is allowed

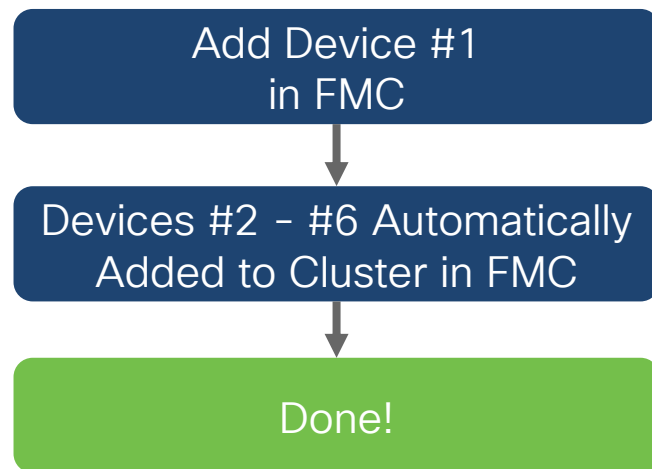
FMC Clustering Improvements with FTD 6.3

Discovery of cluster nodes is now automatic in FMC

FTD 6.2.3 – 6 Node Cluster Setup



FTD 6.3+ – 6 Node Cluster Setup



Automatic discovery of nodes applies to both initial setup and additions

Set Cluster Control Link (CCL) MTU

Avoids fragmentation after encapsulation on CCL

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The left sidebar displays the 'Device Management' section for a Cisco Firepower 4110 Threat Defense device, with tabs for Cluster, Device, Routing, Interfaces, and Inline. The 'Interfaces' tab is active, showing a list of interfaces including Ethernet1/7, Port-channel3, Port-channel3.30, Port-channel4, Port-channel4.10, and Port-channel48. The 'Port-channel48' interface is highlighted in orange.

The main area displays the 'Edit Ether Channel Interface' dialog box. The 'General' tab is selected, showing the following fields:

- Mode: None
- Name: (empty)
- Security Zone: (empty)
- Description: Clustering Interface
- MTU: 1600 (164 - 9184)
- Ether Channel ID *: 48 (1 - 48)

The MTU value of 1600 is highlighted with a red box. A blue arrow points from a text box to the MTU field. The text box contains the following text:

Set MTU at 100 bytes above highest data MTU

The right sidebar shows the 'IP Address' section with a table of IP addresses:

IP Address	Actions
30.0.0.2/16(Static)	[Edit] [Delete]
10.0.0.2/16(Static)	[Edit] [Delete]

Pro-Tip – Set Virtual MAC Addresses

For stability, set Active Mac address, especially if using non-interface NAT IPs

Edit Sub Interface

Name: ☒ Enabled ☐ Management Only

Security Zone:

Description:

General IPv4 IPv6 **Advanced**

Information ARP Security Configuration

Active Mac Address:

Standby Mac Address:

DNS Lookup: ☐

Not required, but more stable if set. For clustering, only Active Mac Address needs to be set.

OK Cancel

Why? Traffic disruption due to MAC address changes:

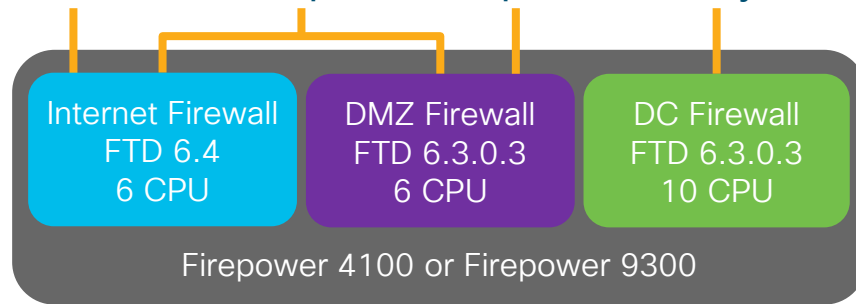
- On boot, the MAC addresses of the master unit are used across the cluster. If the master unit becomes unavailable, the MAC addresses of the new master unit are used across the cluster.
- Gratuitous ARP for interface IPs partially mitigates this, but has no effect on NAT IPs.



FTD Multi-Instance Overview

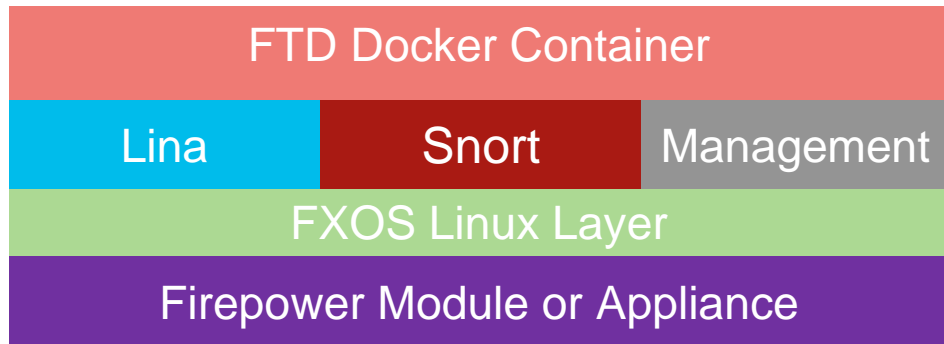
FTD Multi-Instance Intro

- Next generation replacement for ASA Multiple Context Mode
- Create multiple logical devices on a single module or appliance
 - Instances are truly virtual (unlike ASA contexts), leveraging Docker containers
 - Dedicated resources allows for traffic processing and management isolation
- Each container instance runs its own FTD software version
- Physical, logical and VLAN separation provided by chassis supervisor



FTD Multi-Instance Key Details

- Requires FTD 6.3+
- Supported on Firepower 4100 and 9300 hardware only
- Supports inter-chassis HA for high availability only
- Supports hardware crypto:
 - 1 instance/module (FTD 6.4+)
 - 16 instances/modules (FTD 6.5+)
- Maximum of 54 instances per chassis
- Not yet supported, but planned:
 - Clustering
 - Flow Offload
 - Overlapping IP addresses across instances managed by a single FMC



Instance Counts by Platform

Model	Max Cores Per Instance	Max Instances Per Chassis
4110	22	3
4120	46	3
4140	70	7
4150	86	7
9300 w/ 1 x SM-24	46	7
9300 w/ 1 x SM-36	70	11
9300 w/ 1 x SM-44	86	14
9300 w/ 3 x SM-24	46	21
9300 w/ 3 x SM-36	70	33
9300 w/ 3 x SM-44	86	42



Model	Max Cores Per Instance	Max Instances Per Chassis
4115	46	7
4125	62	10
4145	78	13
9300 w/ 1 x SM-40	78	13
9300 w/ 1 x SM-48	94	15
9300 w/ 1 x SM-56	110	18
9300 w/ 3 x SM-40	78	39
9300 w/ 3 x SM-48	94	45
9300 w/ 3 x SM-56	110	54

Network Interfaces

- Supervisor assigns physical, EtherChannel, and VLAN subinterfaces
 - FXOS supports up to 500 total VLAN subinterfaces
 - FTD can create VLAN subinterfaces on physical/Etherchannel interfaces
- Each instance can have a combination of different interface types

Data (Dedicated)



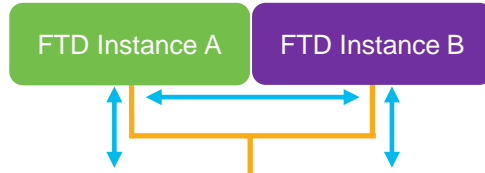
Supported Firewall Modes:

Routed, Transparent

Supported Usage:

Routed, Transparent, Inline, Passive, HA

Data-Sharing (Shared)



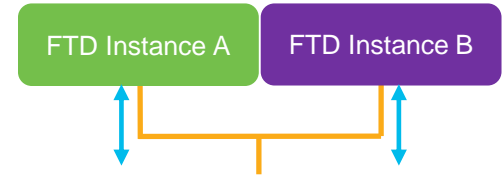
Supported Firewall Modes:

Routed

Supported Interface Usage:

Routed (no BVI members), HA

Mgmt/Firepower-Eventing



Supported Firewall Modes:

Routed, Transparent

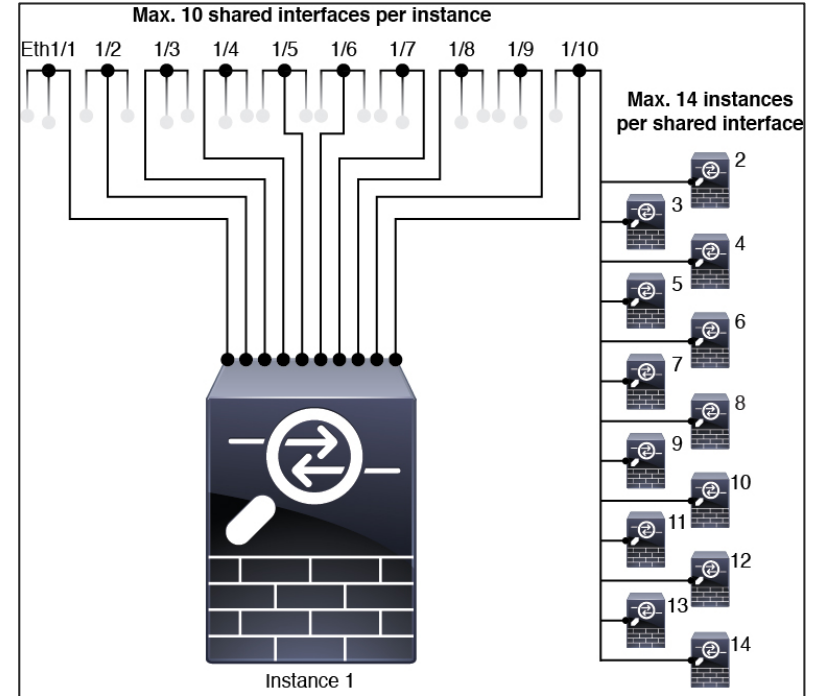
Supported Interface Usage:

Management, Eventing

Interface Scalability Best Practices

In order of preference:

- Use non-shared interfaces or subinterfaces
- Share subinterfaces instead of physical/port-channel interfaces
 - e.g. Po1.100, Po2.200, Po3.300 instead of Po1, Po2 and Po3
- Share subinterfaces under a single physical/port-channel interface
 - e.g. Share Po4.100, Po4.200, Po4.300 instead of Po1, Po2 and Po3
- Share physical ports or port-channels



Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/instance261/cli-guide/b_CLI_ConfigGuide_FXOS_261/interface_management.html



Alternatives to Multi-Instance

Use Cases for Multi-Tenancy

Routing Table Separation

Independent and/or overlapping IP spaces

Resource Sharing

Oversubscription of firewall resources

Traffic Processing Isolation

Compliance separation and tenant resource overflow protection

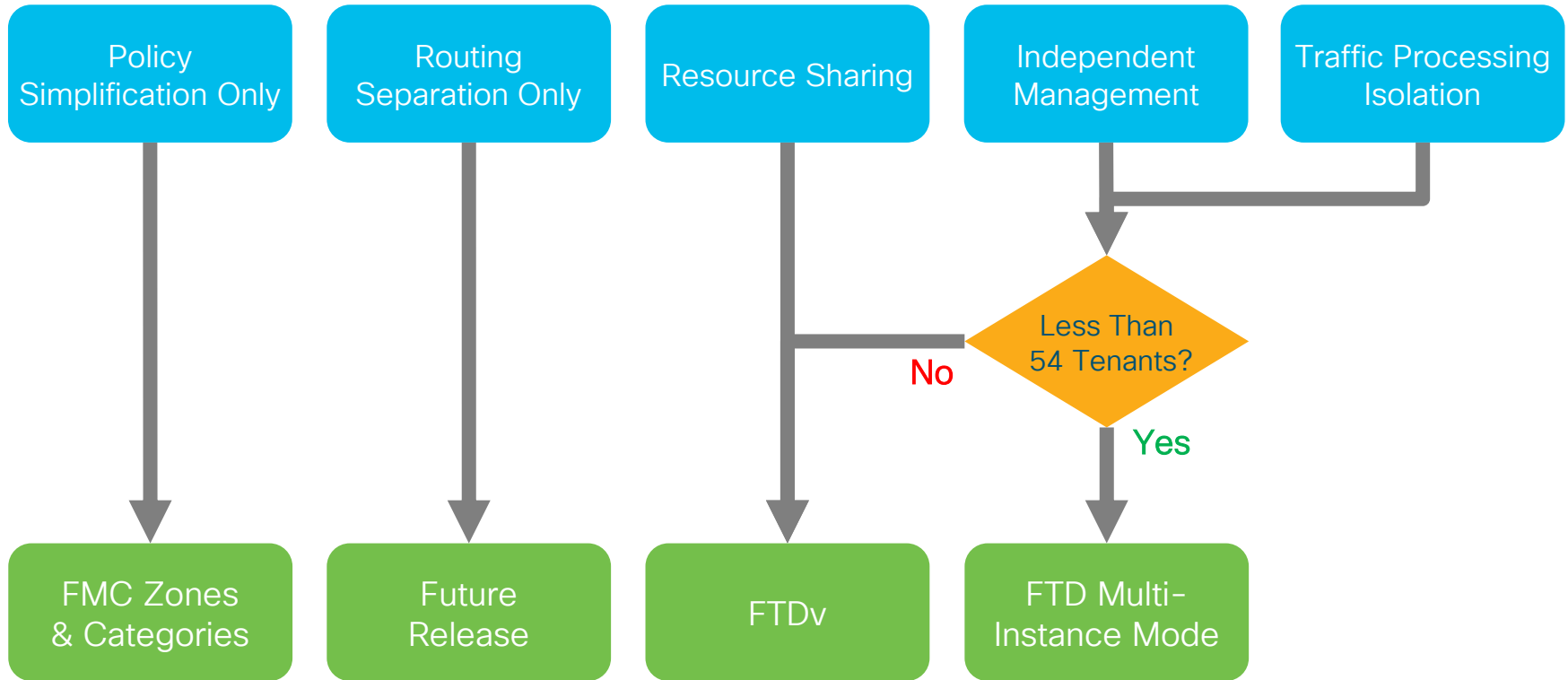
Policy Management Simplification

Smaller policy views that are managed by a single administrator

Management Separation

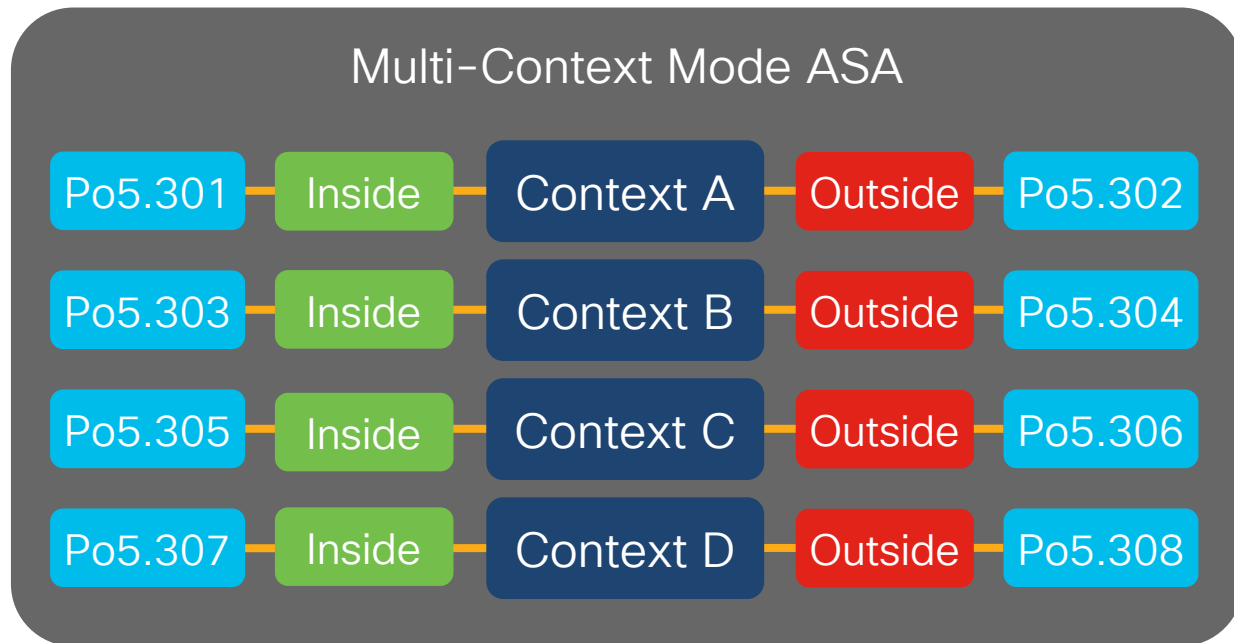
Independent management of firewall partitions

Multi-Tenancy Use Case Mapping to FTD



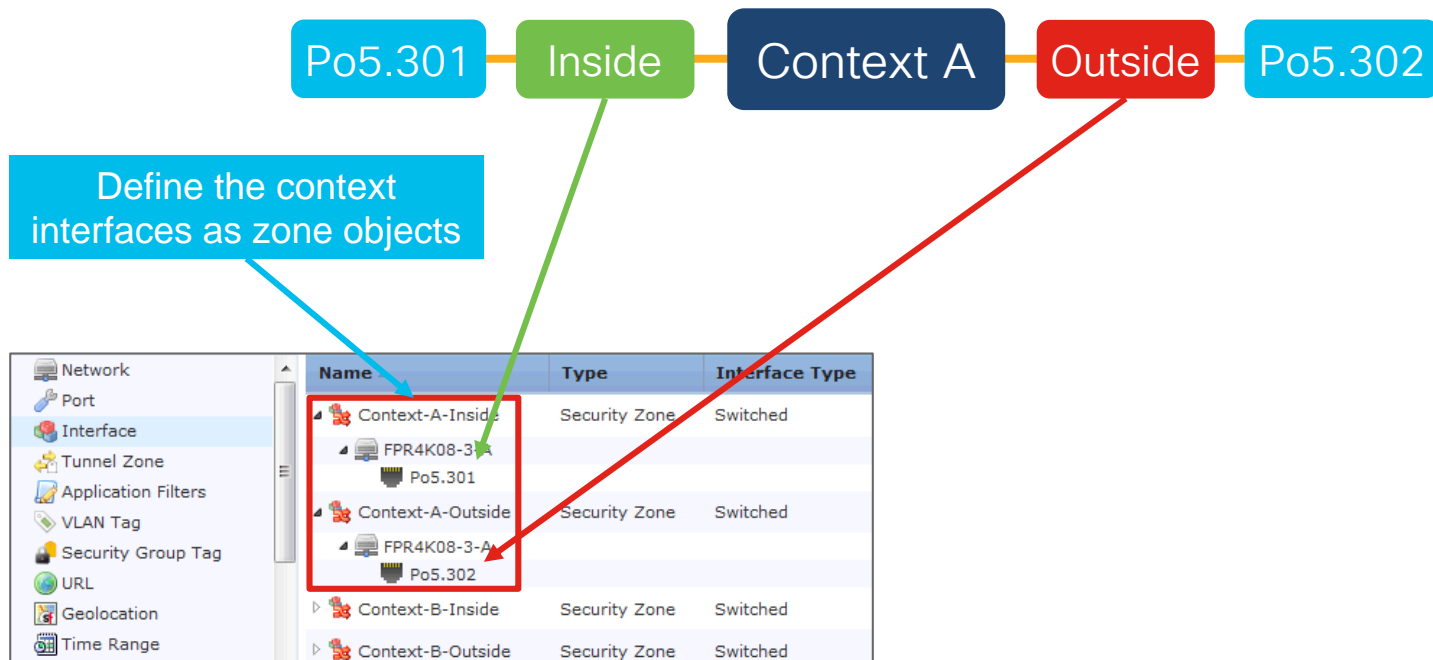
Zones and Categories for Policy Management

Migrate ASA contexts to FTD, without FTD Multi-Instance



Zones and Categories for Policy Management

Migrate ASA contexts to FTD, without FTD Multi-Instance



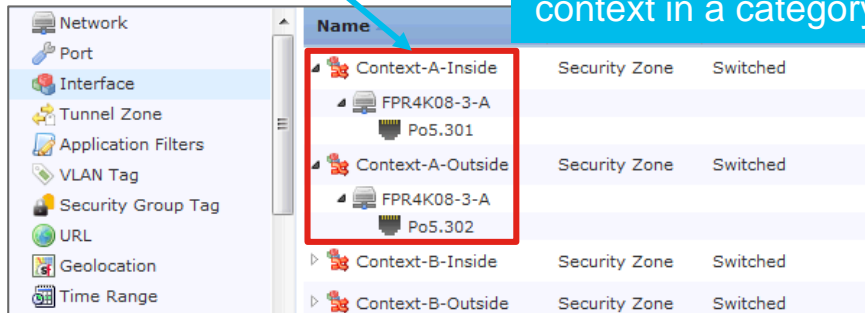
Zones and Categories for Policy Management

Migrate ASA contexts to FTD, without FTD Multi-Instance



Define the context interfaces as zone objects

Group the rules that were in an ASA context in a category



Rules

Security Intelligence

HTTP Responses

Logging

Advanced

Filter by Device

#	Name	Source Zones	Dest Zones	Sour...	Dest...
Mandatory - Context Like Management (1-3)					
Context A (1-2)					
1	Permit HTTP	Context-A-Inside	Context-A-Outside	Any	Any
2	Deny Any	Context-A-Inside	Context-A-Outside	Any	Any
Context B (3-3)					
3	Permit All	Context-B-Inside	Context-B-Outside	Any	Any
Context C (-)					
Context D (-)					

Zones and Categories for Policy Management

Migrate ASA contexts to FTD, without FTD Multi-Instance

Po5.301

Inside

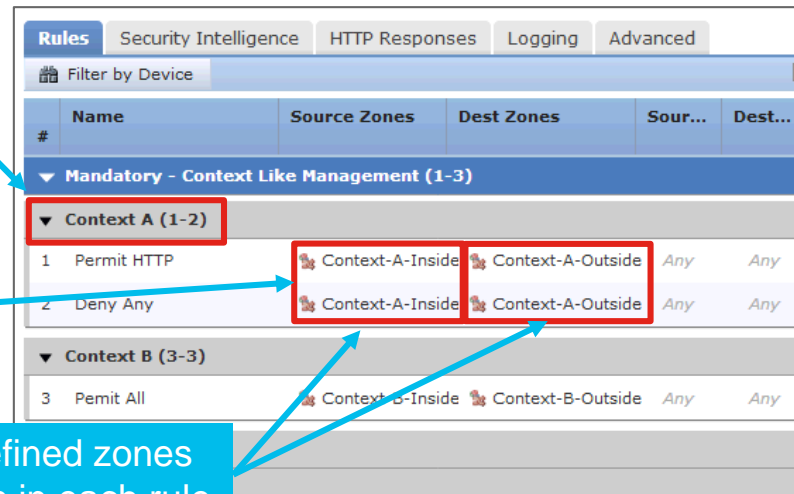
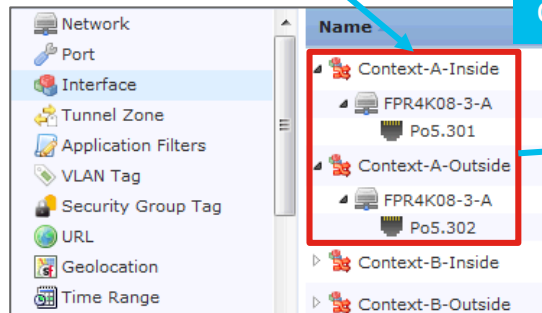
Context A

Outside

Po5.302

Define the context interfaces as zone objects

Group the rules that were in an ASA context in a category

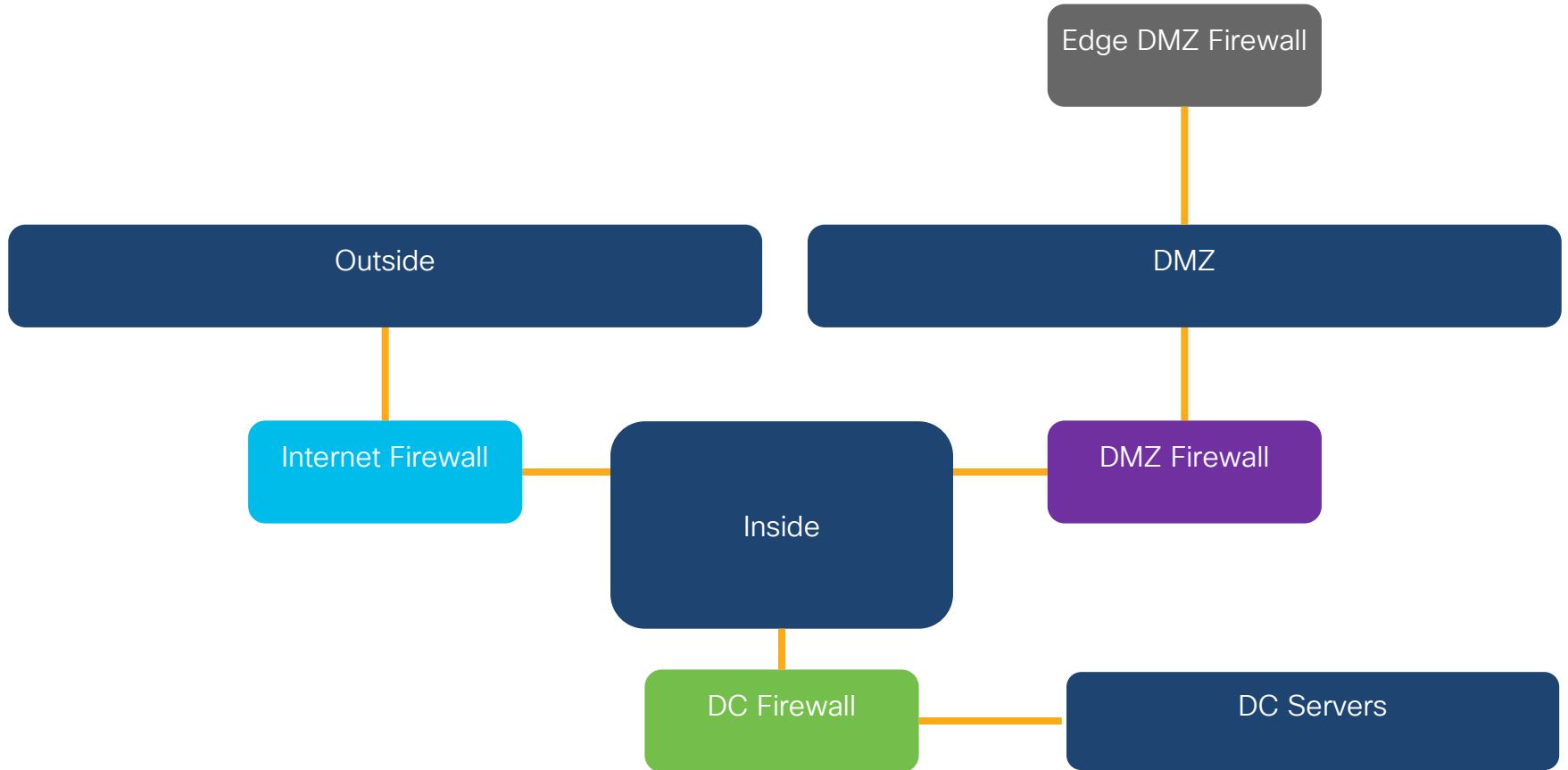


Use the previously defined zones as a source/destination in each rule

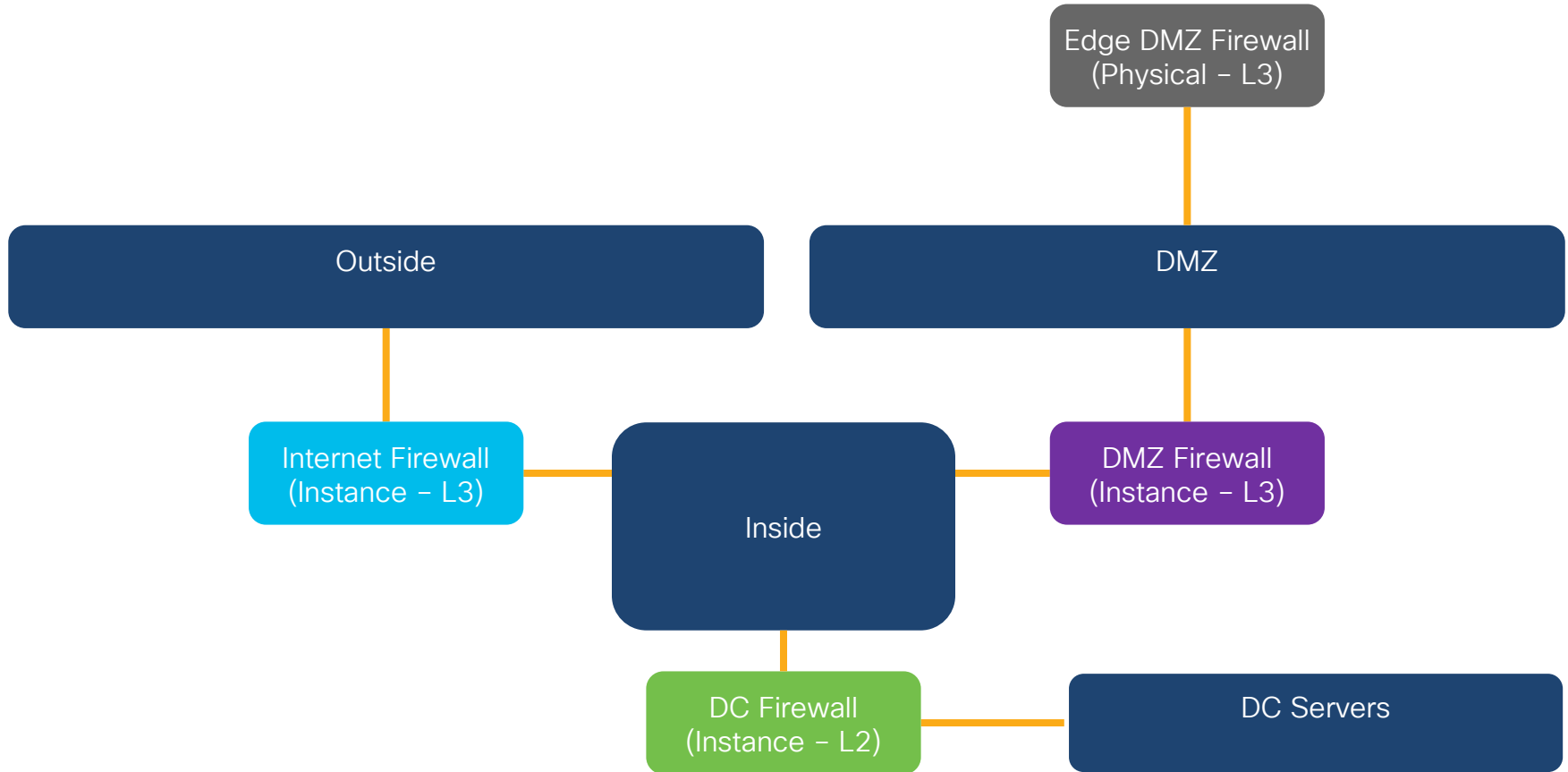


Multi-Instance Configuration Walkthrough

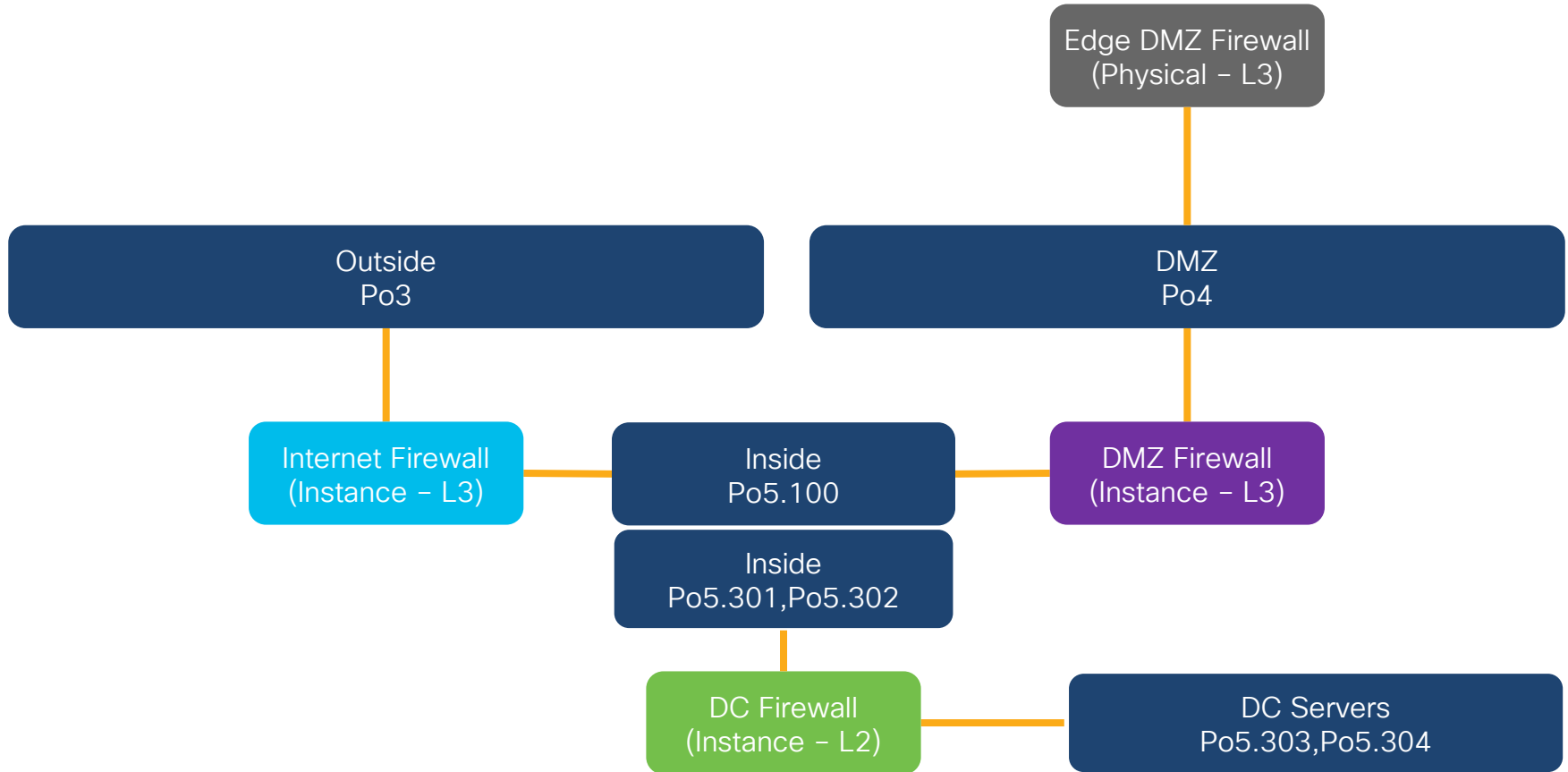
Demo Scenario Logical Design



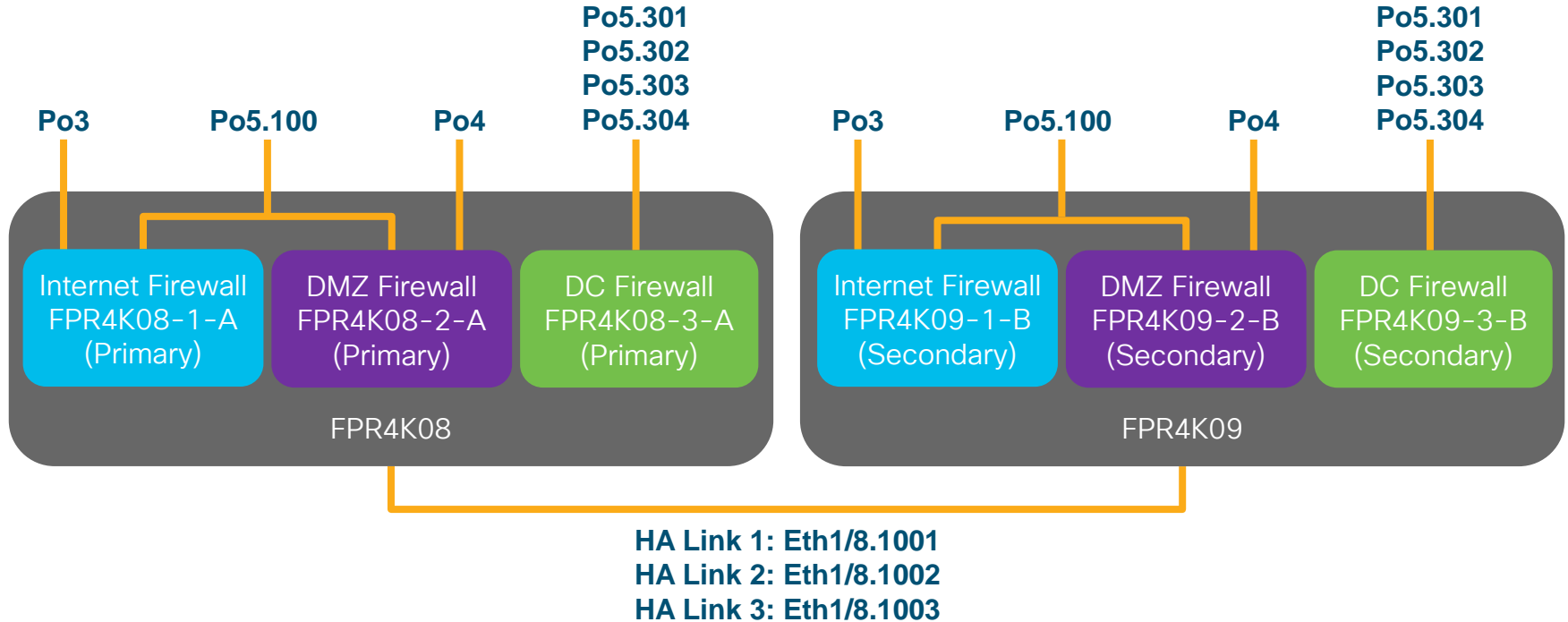
Demo Scenario Logical Design



Demo Scenario Logical Design



Demo Scenario Multi-Instance Design



Steps Involved in Bringing up a Multi-Instance



Multi-Instance Setup – FXOS Upgrade

Upload and upgrade FXOS to 2.4.1+

Available Updates

Image Name	Type	Version	Status	Build Date	Image Integrity
fxos-k9.2.3.1.130.SPA	platform-bundle	2.3(1.130)	Installed	12/14/2018	✓ Verified - Mon 28 Jan 2019, 01...
cisco-ftd.6.2.3.83.csp	ftd	6.2.3.83	Not-Installed	04/01/2018	
cisco-ftd.6.3.0.83.csp	ftd	6.3.0.83	Not-Installed	12/01/2018	

Upload Image

Uploading **fxos-k9.2.4.1.214.SPA...**

Upload Close

FXOS file on local machine previously downloaded from Cisco website

The file is big (~1 GB) with no status bar. If you can, upload from a local machine.

Pressing Close and staying on the page does not stop the upload. It will continue in the background.

Multi-Instance Setup – FXOS Upgrade

Upload and upgrade FXOS to 2.4.1+

Available Updates

If you uploaded via the CLI, use Refresh to repoll for images

Refresh Upload Image Filter..

Image Name	Type	Version	Status	Build Date	Image Integrity
fxos-k9.2.4.1.214.SPA	platform-bundle	2.4(1.214)	Not-Installed	11/21/2018	✓ Verified - Mon 28 Jan 2019, 02...
fxos-k9.2.3.1.130.SPA	platform-bundle	2.3(1.130)	Installed	12/14/2018	✓ Verified - Mon 28 Jan 2019, 01...
cisco-ftd.6.2.3.83.csp	ftd	6.2.3.83	Not-Installed	04/01/2018	
cisco-ftd.6.3.0.83.csp	ftd	6.3.0.83			

Success

fxos-k9.2.4.1.214.SPA
Successfully Uploaded

OK

Message will always appear when upload is complete, even if you pressed Close on the upload dialog

Multi-Instance Setup – FXOS Upgrade

Upload and upgrade FXOS to 2.4.1+

Available Updates

Upgrade/downgrade FXOS button

Image Name	Type	Version	Status	Build Date	Image Integrity
fxos-k9.2.4.1.214.SPA	platform-bundle	2.4(1.214)	Not-Installed	11/21/2018	✓ Verified - Mon 28 Jan 2019, 02...
fxos-k9.2.3.1.130.SPA	platform-bundle	2.3(1.130)			✓ Verified - Mon 28 Jan 2019, 01...
cisco-ftd.6.2.3.83.csp	ftd	6.2.3.83			✓
cisco-ftd.6.3.0.83.csp	ftd	6.3.0.83			✓

Update Bundle Image

Please ensure Application configuration is saved. All existing sessions will be terminated and FCM will not be accessible during the process. It may take several minutes. Chassis will reboot after upgrade, please re-login to FCM after upgrade completes.

Selected version 2.4(1.214) will be installed. Do you want to proceed?

Yes No

Verify image integrity button

After pressing Yes the upgrade process takes a while (~15 min). Be patient and leave this page open.

Multi-Instance Setup – FXOS Upgrade

Upload and upgrade FXOS to 2.4.1+ – If you are impatient

The screenshot displays the Cisco Firepower 4110 Security Appliance management interface. The top navigation bar includes 'Overview' (selected), 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings'. The right side of the bar contains 'System', 'Tools', 'Help', and 'admin'.

Key information at the top:

- Device ID: F241TS-24-08-FPR4110-1
- IP Address: 14.2.185.12
- Model: Cisco Firepower 4110 Security Appliance
- Version: 2.3(1.130) (highlighted with a red box and a blue arrow pointing to a text box)
- Operational State: Power-problem
- Chassis Uptime: 00:00:56:49

A blue text box with a white border contains the text: "Expected version if you refresh the page before the upgrade restart occurs".

Below the top bar, there are status indicators for Console, MGMT, and USB. Power status shows Power 1 as 'Running' and Power 2 as 'Unknown'. A network module diagram shows 8 ports, with ports 1, 3, 5, and 7 highlighted in red.

The 'FAULTS' section shows 0(0) CRITICAL and 18(18) MAJOR faults. Below this, a table lists the faults:

Severity	Description	Cause	Occure...	Time	Acknowl...
MAJOR	Power state on chassis 1 is redundancy-failed	power-problem	1	2018-01-25T20:39:51.821	no
MAJOR	Ian port-channel 4 on fabric interconnect A oper state: failed, reason: No operational mem...	operational-state-down	1	2019-01-26T22:17:32.651	no
MAJOR	Ian port-channel 5 on fabric interconnect A oper state: failed, reason: No operational mem...	operational-state-down	3	2019-01-28T12:43:35.987	no
MAJOR	Ian Member 1/6 of Port-Channel 5 on fabric interconnect A is down, membership: suspend...	membership-down	3	2019-01-28T12:44:29.727	no

Multi-Instance Setup – FXOS Upgrade

Upload and upgrade FXOS to 2.4.1+ – If you are impatient

The screenshot shows the Cisco NX-OS GUI with the 'Overview' tab selected. The top navigation bar includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', 'Platform Settings', 'System', 'Tools', 'Help', and 'admin'. The main content area displays the device's operational state, including Model, Version, and Operational State. Below this, there are sections for 'CONSOLE', 'MGMT', and 'USB' ports, and 'Power' buttons. A 'Validation Error' dialog box is overlaid on the screen, displaying a yellow warning icon and the text 'Error communicating with SSP Backend'. A blue arrow points from the dialog box to a blue text box that says 'Expected message if you refresh the page before the upgrade is complete'. The bottom of the screen shows a table with columns for Severity, Description, Cause, Occurrence, Time, and Acknowledged.

Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin

Model: | Version: | Operational State: | Chassis Uptime ⓘ

CONSOLE MGMT USB

Power - Power -

Network Module 1

1 3 5 7

2 4 6 8

Network Module 2 Network Module 3

Validation Error

! Error communicating with SSP Backend

OK

Expected message if you refresh the page before the upgrade is complete

FAULTS

0(0) 0(0)

CRITICAL MAJOR

INTERFACES

0 0

DOWN UP

Select All Faults Cancel Selected Faults Acknowledge

INVENTORY

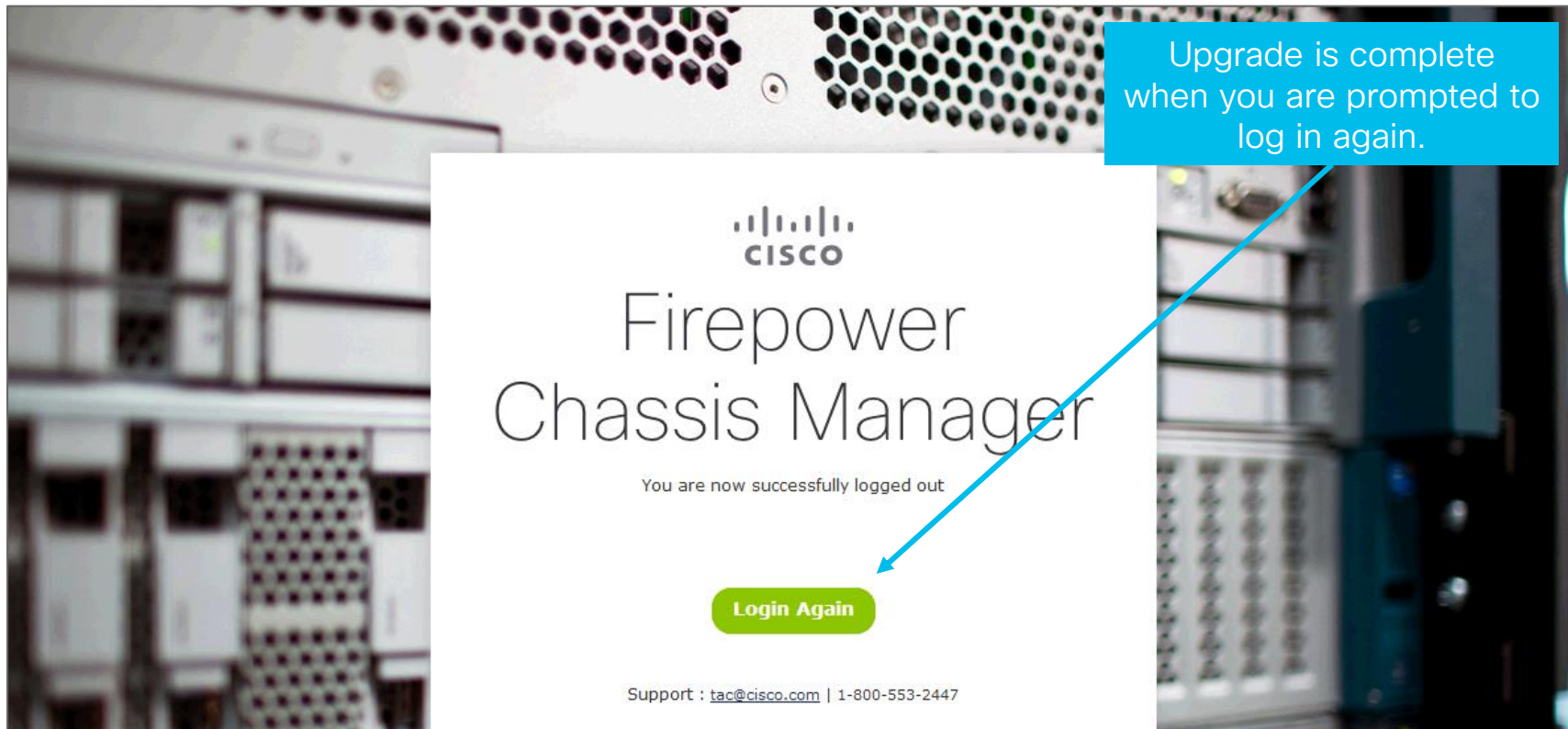
0 0 0

Security Engine Fans Power Supplies

Severity	Description	Cause	Occurrence	Time	Acknowledged
----------	-------------	-------	------------	------	--------------

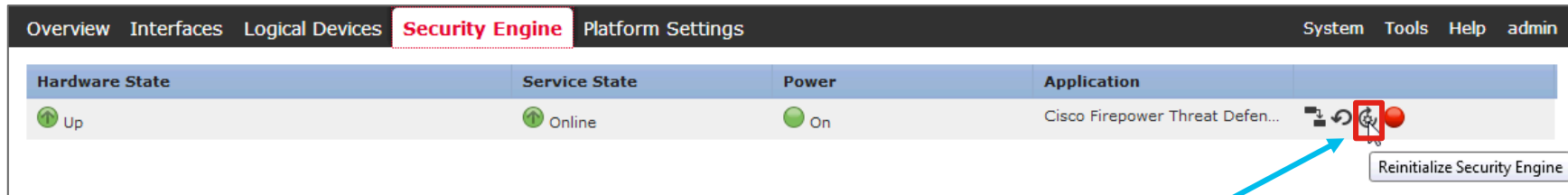
Multi-Instance Setup – FXOS Upgrade

Upload and upgrade FXOS to 2.4.1+






Multi-Instance Setup – Module Reinitialization

Required to support Container instances



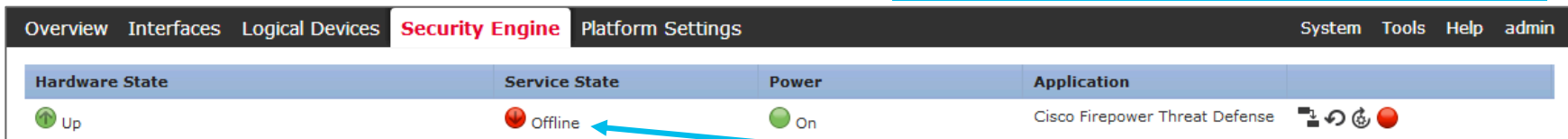
Overview Interfaces Logical Devices **Security Engine** Platform Settings System Tools Help admin

Hardware State	Service State	Power	Application
Up	Online	On	Cisco Firepower Threat Defen...   




Reinitialize Security Engine



Reinitialization required after FXOS upgrade to support Multi-Instance.



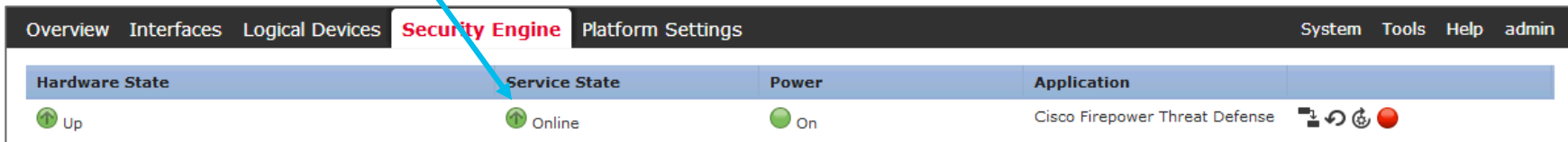
Overview Interfaces Logical Devices **Security Engine** Platform Settings System Tools Help admin

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




Module is Multi-Instance ready when you Service State returns to Online



Reinitialization typically takes ~5 minutes



Overview Interfaces Logical Devices **Security Engine** Platform Settings System Tools Help admin

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

Multi-Instance Setup – Configuring Interfaces

Adding Data-Sharing Interface for FPR4K08-1-A and FPR4K08-2-A

The screenshot shows the Cisco IOS XE GUI with the 'Interfaces' tab selected. A modal window titled 'Add Subinterface' is open, showing the following fields:

- Type: Data
- Interface: Data
- Subinterface ID: Data-sharing
- VLAN ID: (empty)

Buttons 'OK' and 'Cancel' are at the bottom of the modal. In the background, a table lists interfaces:

Interface	Type	Speed	Duplex	Mode
MGMT	data	10gbps	10gbps	
Port-channel3	data	10gbps	10gbps	
Eth1/0/23	data	10gbps	10gbps	
Eth1/0/24	data	10gbps	10gbps	
Eth1/0/25	data	10gbps	10gbps	
Eth1/0/26	data	10gbps	10gbps	
Eth1/0/27	data	10gbps	10gbps	
Eth1/0/28	data	10gbps	10gbps	
Eth1/0/29	data	10gbps	10gbps	
Eth1/0/30	data	10gbps	10gbps	
Eth1/0/31	data	10gbps	10gbps	
Ethernet1/6	mgmt	1gbps	1gbps	
Ethernet1/7	mgmt	1gbps	1gbps	
Ethernet1/8	data	10gbps	10gbps	

On the right, a table shows the 'Add New' button and a 'Filter..' dropdown. Below it, a table shows the 'Add New' button and a 'Filter..' dropdown.

Annotations:

- Data interfaces can be used by a single instance
- Data-Sharing interfaces can be shared across interfaces. Physical interfaces, port-channels and subinterfaces can all be set to Data-Sharing
- New in 6.3 is the option to add subinterfaces

Multi-Instance Setup – Configuring Interfaces

Adding Data-Sharing Interface for FPR4K08-1-A and FPR4K08-2-A

Physical interface for the subinterface

Subinterface ID used by FXOS and FMC

External VLAN. Does not need to match Subinterface ID.

Add Subinterface

Type: Data-sharing

Interface: Port-channel5

Subinterface ID: 100

VLAN ID: 100

OK Cancel

Interface	Mode	Speed	Full Duplex	Admin State	Operation State
MGMT					
Port-channel3	data	10gbps		failed	suspended
Port-channel4	data	10gbps		failed	suspended
Ethernet1/6				failed	suspended
Ethernet1/7	mgmt	1gbps	Full Duplex	up	up
Ethernet1/8	data	10gbps	Full Duplex	up	up

Multi-Instance Setup – Configuring Interfaces

Completed Interface Configuration

Overview Interfaces Logical Devices Security Engine Platform Settings				System Tools Help admin		
Interface	Type	Admin Sp...	Operational		Operation St...	Admin State
MGMT	Management					
Port-channel3	data	10gbps	10gbps	Dedicated port-channel to be used on FPR4K08-1-A	failed	<input checked="" type="checkbox"/>
Port-channel4	data	10gbps	10gbps	Dedicated port-channel to be used on FPR4K08-2-A	failed	<input checked="" type="checkbox"/>
Port-channel5	data	10gbps	10gbps		failed	<input checked="" type="checkbox"/>
Port-channel5.100	data-sharing					
Port-channel5.301	data			Shared subinterface to be used on FPR4K08-1-A and FPR4K08-2-A		
Port-channel5.302	data					
Port-channel5.303	data					
Port-channel5.304	data					
Ethernet1/5					suspended	
Ethernet1/6					suspended	
Ethernet1/7	mgmt	1gbps	1gbps	Dedicated subinterfaces to be used on FPR4K08-3-A	up	<input checked="" type="checkbox"/>
Ethernet1/8	data	10gbps	10gbps	Semi-shared interface for management of all instances	up	<input checked="" type="checkbox"/>
Ethernet1/8.1001	data			Dedicated subinterfaces for HA link for each instance		
Ethernet1/8.1002	data					
Ethernet1/8.1003	data					

Multi-Instance Setup – First Instance Creation

The screenshot shows the Cisco FXOS configuration interface. The 'Logical Devices' tab is selected. A message states: 'No logical devices available. Click on Add Device to add a new logical device.' An 'Add Device' dialog box is open, showing the following fields:

- Device Name: FPR4K08-1-A
- Template: Cisco Firepower Threat Defense
- Image Version: 6.3.0.83
- Instance Type: Native
- Usage: Container

Annotations on the left side of the image provide context for the values:

- Device name used locally within FXOS. Best practice to match FMC name.
- Native for standalone
- Containers for Multi-Instance

Multi-Instance Setup – First Instance Creation

FPR4K08-1-A

Provisioning - FPR4K08-1-A
Standalone | Cisco Firepower

Data Ports

- Ethernet1/8
 - Ethernet1/8.1001
 - Ethernet1/8.1002
 - Ethernet1/8.1003
- Port-channel3
 - Port-channel3
 - Port-channel4
- Port-channel5
 - Port-channel5.100
 - Port-channel5.301
 - Port-channel5.302
 - Port-channel5.303
 - Port-channel5.304

Interfaces assigned to instance by clicking

Dark grey text indicates the interface is assigned

These are the untagged (no VLAN tag) interfaces. Light grey indicates the interface is not assigned to the instance.

Application	Version	Resource Profile	Management IP	Gateway
FTD	6.3.0.83		14.2.185.37	14.2.185.1

Interface Name

- Ethernet1/8.1001
- Port-channel3
- Port-channel5.100

Type

- data
- data
- data-sharing

Multi-Instance Setup – First Instance Creation

FPR4K08-1-A

Provisioning - FPR4K08-1-A
Standalone | Cisco Firepower Threat Defense | 6.3.0.83

Data Ports

- Ethernet1/8
- Ethernet1/8.1001
- Ethernet1/8.1002
- Ethernet1/8.1003
- Port-channel3
- Port-channel4
- Port-channel5
- Port-channel5.100
- Port-channel5.301
- Port-channel5.302
- Port-channel5.303
- Port-channel5.304

Application | **Version** | **Resource**

Application	Version	Resource
FTD	6.3.0.83	

Interface Name

- Ethernet1/8.1001
- Port-channel3
- Port-channel5.100

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information | Settings | Agreement

SM 1 - 22 Cores Available

Resource Profile: **Default-Small**

Interface Information

Management Interface: **Ethernet1/7**

Management

Address Type: **IPv4 only**

IPv4

Management IP: **14.2.185.37**

Network Mask: **255.255.255.0**

Network Gateway: **14.2.185.1**

OK | Cancel

Controls the number of CPUs assigned to the instance. Default-Small is 6 CPUs.

Semi-shared management interface. If empty, check that interfaces of type Management are defined under Interfaces.

Unique management IP for the instance. Must be reachable from the FMC.

Multi-Instance Setup – First Instance Creation

FPR4K08-1-A

Registration Key:
Confirm Registration Key:
Password:
Confirm Password:

Firepower Management Center IP: 14.2.185.40

Permit Expert mode for FTD SSH sessions: no

Search domains: zulu.biglab.co

Firewall Mode: Routed

DNS Servers: 18.108.43,172.18.108.34

Firepower Management Center NAT ID:

Fully Qualified Hostname: fpr4k08-1-a.zulu.biglab.co

Eventing Interface:

Registration key used only once when pairing with FMC. Doesn't need to be complex.

Admin password for FTD, not the password for FMC

Controls whether entering expert mode (Linux shell) is allowed via SSH.

Transparent or Routed

Alphanumeric string to assist setup w/ NAT. Must be unique across all devices in FMC.

If a dedicated event interface is desired

Multi-Instance Setup – First Instance Creation

FPR4K08-1-A

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List

If the Status is install-failed, the module was not reinitialized. Fix is to reinitialize the module.

Refresh Add Device

FPR4K08-1-A		Standalone	Status:ok			
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.83	Default-Small	14.2.185.37	14.2.185.1	Ethernet1/7	install-failed

Assuming everything is okay, Status should move to installing within ~1 min

FPR4K08-1-A		Standalone	Status:ok			
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.83	Default-Small	14.2.185.37	14.2.185.1	Ethernet1/7	installing

Multi-Instance Setup – Modify Resource Profile

FPR4K08-3-A

The screenshot displays the 'Logical Devices' tab in the Cisco FTD configuration interface. At the top, a summary bar indicates '(3 instances) 19% (4 of 22) Cores Available'. Below this, a table lists three logical devices: FPR4K08-1-A, FPR4K08-2-A, and FPR4K08-3-A. Each device has a table of applications (FTD) with columns for Version, Resource Profile, Management IP, Gateway, Management Port, and Status. Annotations with blue arrows point to specific elements: one points to the summary bar, another to the 'FPR4K08-2-A' device name, and a third to the 'FPR4K08-3-A' device name. A fourth annotation points to the 'started' status of the FTD application in the FPR4K08-3-A device table. A fifth annotation points to the 'started' status of the FTD application in the FPR4K08-2-A device table. A sixth annotation points to the 'started' status of the FTD application in the FPR4K08-1-A device table.

Overview Interfaces **Logical Devices** Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates User Management Refresh Add Device

Logical Device List (3 instances) 19% (4 of 22) Cores Available

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FPR4K08-1-A Standalone Status:ok						
FTD	6.3.0.83	Default-Small	14.2.185.37	14.2.185.1	Ethernet1/7	online
FPR4K08-2-A Standalone Status:ok						
FTD	6.3.0.83	Default-Small	14.2.185.65	14.2.185.1	Ethernet1/7	started
FPR4K08-3-A Standalone Status:ok						
FTD	6.3.0.83	Default-Small	14.2.185.67	14.2.185.1	Ethernet1/7	started

In some cases, the Default-Small profile may not consume all the cores

Additional instances configured. Steps in the hidden slides.

Setup still running

Multi-Instance Setup – Modify Resource Profile

FPR4K08-3-A

The screenshot displays the Cisco IOS XE Platform Settings interface. The left sidebar shows the navigation menu with 'Resource Profiles' selected. The main area shows a table of resource profiles. The 'Default-Small' profile is highlighted with a red box and an annotation: 'Default profile of 6 CPUs'. A modal window titled 'Add Resource Profile' is open, showing a new profile named 'Medium' with 10 cores. The 'Number of Cores' field is highlighted with a red box and an annotation: 'New profile to unused CPU capacity'. The 'Number of Cores' field also has a red box around the value '10' and an annotation: 'Multiples of 2, excluding 8. (e.g. 6, 10, 12, 14, 16)'. The modal window also includes a description field, a range indicator '[6 to 22]', and a note: 'Specify even value for number of cores.'.

Name	Description	Cores
Default-Small	Auto-created application resource-profile with 6 cpu-cores	6

Add Resource Profile

Name: * Medium

Description:

Number of Cores: * 10 Range : [6 to 22]

Specify even value for number of cores.

OK Cancel

Multi-Instance Setup – Modify Resource Profile

FPR4K08-3-A

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information Settings Agreement

SM 1 - 4 Cores Available

Resource Profile: **Default-Small** (dropdown menu showing **Medium** as an option)

Interface Information

Management Interface: **Ethernet1/7** (dropdown menu)

Management

Address Type: **IPv4 only** (dropdown menu)

IPv4

Management IP: **14.2.185.67**

Network Mask: **255.255.255.0**

Network Gateway: **14.2.185.1**

OK Cancel

Provisioning - FPR4K08-3-A

Standalone | Cisco Firepower Threat Defense | 6.3.0.83

Data Ports

- + Ethernet1/8
- + Port-channel5

Application	Version	Resource
FTD	6.3.0.83	

Interface Name

- Port-channel5.301
- Port-channel5.302
- Port-channel5.303

Port Status

Ethernet1/7
Click to configure

Save Cancel

If previously created, the profile could have been selected during setup. It can be changed after setup.

Multi-Instance Setup – Modify Resource Profile

FPR4K08-3-A

Alert

Changing the resource profile will cause the instance to restart.

If new resource profile does not allocate enough resources for current policies to function, there may be deployment or operational issues.

OK

With HA and increasing resources, stateful failover is supported.

With HA and decreasing resource, stateful failover is not guaranteed.

Multi-Instance Setup – Completed FXOS Setup

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (3 instances) 0% (0 of 22) Cores Available 100% of CPU resources now consumed

Refresh Add Device

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FPR4K08-1-A Standalone Status:ok						
FTD	6.3.0.83	Default-Small	14.2.185.37	14.2.185.1	Ethernet1/7	online
FPR4K08-2-A Standalone Status:ok						
FTD	6.3.0.83	Default-Small			1/7	
FPR4K08-3-A Standalone Status:ok						
FTD	6.3.0.83	Medium	14.2.185.67	14.2.185.1	Ethernet1/7	online

Complete the same steps for FPR4K09, using different names/IPs

Multi-Instance Setup – FMC Setup

Adding devices

The screenshot shows the Cisco FMC web interface. The top navigation bar includes tabs for Overview, Analysis, Policies, **Devices**, Objects, AMP, and Intelligence. Below this, there's a sub-navigation bar with links like Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates. The main content area is titled 'Device Management' and shows a list of devices. A modal dialog box titled 'Add Device' is open in the center, with a red border. The dialog contains fields for Host, Display Name, Registration Key, Group, and Access Control Policy. It also has sections for Smart Licensing (Malware, Threat, URL Filtering) and Advanced settings (Unique NAT ID, Transfer Packets). At the bottom of the dialog are 'Register' and 'Cancel' buttons. A blue arrow points from a text box at the bottom left to the 'Add Device' dialog.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center

View By: Group All (0) Error (0)

Name	Model
Ungrouped (0)	

Add Device

Host: 14.2.185.37

Display Name: FPR4K08-1-A

Registration Key: ABC123

Group: None

Access Control Policy: Internet

Smart Licensing

Malware: ☒

Threat: ☒

URL Filtering: ☒

Advanced

Unique NAT ID:

Transfer Packets: ☒

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from [smart license page](#)

Register Cancel

Search Device Add

Access Control Poli...

Adding an Instance to FMC is no different than adding a physical firewall

Multi-Instance Setup – FMC Setup

Adding devices

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By: Group All (6) Error (0) Warning (0) Offline (0) Normal (6) Deployment Pending (0) Search Device Add

Name	Model	Versi...	Chassis	Licenses	Access Control Poli...
Ungrouped (6)					
✓ FPR4K08-1-A 14.2.185.37 - Routed	FTD on Firepower 4110	6.3.0	fpr4k08.zulu.biglab.co Security Module - 1 (Container)	Base, Threat (2 more...)	Internet DMZ
✓ FPR4K08-2-A 14.2.185.65 - Routed	FTD on Firepower 4110	6.5.0	fpr4k08.zulu.biglab.co Security Module - 1 (Container)	Base, Threat (2 more...)	
✓ FPR4K08-3-A 14.2.185.67 - Transparent	FTD on Firepower 4110	6.3.0	fpr4k08.zulu.biglab.co Security Module - 1 (Container)	Base, Threat (2 more...)	Data Center
✓ FPR4K09-1-B 14.2.185.38 - Routed	FTD on Firepower 4110	6.3.0	fpr4k09.zulu.biglab.co Security Module - 1 (Container)		
✓ FPR4K09-2-B 14.2.185.66 - Routed	FTD on Firepower 4110	6.5.0	fpr4k09.zulu.biglab.co Security Module - 1 (Container)		
✓ FPR4K09-3-B 14.2.185.68 - Transparent	FTD on Firepower 4110	6.3.0	fpr4k09.zulu.biglab.co Security Module - 1 (Container)		

Each Instance must be added individually. Device name defined in FMC.

Separate versions, upgrades, policies per instance

Chassis name defined in FXOS

Chassis Details

Specify the name and URL that Firepower Management Center should display for this device.

Chassis Name: FPR4K08

Chassis URL: https://fpr4k08.zulu.biglab.co/

Platform Settings

Overview Interfaces Logical Devices Security Engine Platform Settings

NTP
SSH
SNMP
HTTPS
AAA
Syslog
DNS
FIPS and Common Criteria
Access List
MAC Pool
Resource Profiles
Chassis URL

cisco Live!

BRKSEC-2020 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public 237

Multi-Instance Licensing

The screenshot shows the Cisco FMC interface with the 'Licenses > Smart Licenses' tab selected. The table displays various licenses, with a red box highlighting six container instances of the URL Filtering feature. Annotations explain that these six instances share only two licenses because they are managed by the same FMC.

License Type/Device Name	License Status	Device Type	Domain	Group
Base (2)	✓			
Malware (2)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
FPR4K08-1-A (Container Instance; Security Module:1)(FLM2145057L) 14.2.185.37 - Cisco Firepower 4110 Threat Defense - v6.3.0	✓	Cisco Firepower 4110 Threat Defense	Global	N/A
FPR4K08-2-A (Container Instance; Security Module:1)(FLM2145057L) 14.2.185.65 - Cisco Firepower 4110 Threat Defense - v6.3.0	✓	Cisco Firepower 4110 Threat Defense	Global	N/A
FPR4K08-3-A (Container Instance; Security Module:1)(FLM2145057L) 14.2.185.67 - Cisco Firepower 4110 Threat Defense - v6.3.0	✓	Cisco Firepower 4110 Threat Defense	Global	N/A
FPR4K09-1-B (Container Instance; Security Module:1)(FLM214505KD) 14.2.185.38 - Cisco Firepower 4110 Threat Defense - v6.3.0	✓	Cisco Firepower 4110 Threat Defense	Global	N/A
FPR4K09-2-B (Container Instance; Security Module:1)(FLM214505KD) 14.2.185.66 - Cisco Firepower 4110 Threat Defense - v6.3.0	✓	Cisco Firepower 4110 Threat Defense	Global	N/A
FPR4K09-3-B (Container Instance; Security Module:1)(FLM214505KD) 14.2.185.68 - Cisco Firepower 4110 Threat Defense - v6.3.0	✓	Cisco Firepower 4110 Threat Defense	Global	N/A

Note: Container Instances of same blade share feature licenses

No new feature license for Multi-Instance features

URL Filtering license #1

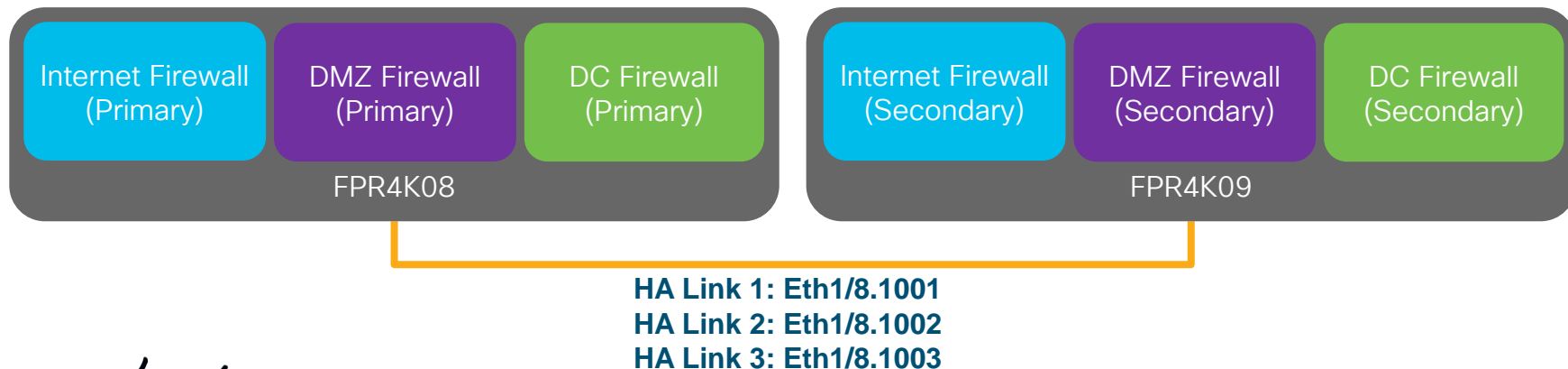
URL Filtering license #2

Instances on the same module share a feature license when managed by the same FMC.

6 instances on 2 modules requires only 2 licenses

Multi-Instance High Availability

- Container instances only support inter-chassis HA
 - Configured exactly as you would physical appliances
 - Multiple instances can share one HA Link, using one VLAN per instance
- An HA pair allows differently sized instances for seamless resizing
 - Stateful HA is supported but not guaranteed when downsizing



Multi-Instance Hardware Crypto Acceleration

- Applies to VPN (IPSec/SSL) and TLS HW decryption
- In FP 6.4, only one instance could use crypto hardware
 - Manually enabled via CLI
- In FP 6.5, up to 16 instances can share crypto hardware
 - Enabled by default for new instances
 - Must be manually enabled for existing instance after upgrade
 - Can be disabled by editing the instance – will cause instance reboot

The image displays two side-by-side screenshots of the Cisco Firepower Threat Defense - Bootstrap Configuration window, specifically the 'Settings' tab. Both windows show the same configuration fields: Firepower Management Center IP, Permit Expert mode for FTD SSH sessions, Search domains, Firewall Mode, DNS Servers, Firepower Management Center NAT ID, Fully Qualified Hostname, Registration Key, Confirm Registration Key, Password, Confirm Password, and Eventing Interface. In the left window, a red box highlights the 'Hardware Crypto' field, which is currently set to 'Disabled'. A blue arrow points from the text 'New instance' to this field. In the right window, the 'Hardware Crypto' dropdown menu is open, showing 'Enabled' as the selected option. A blue arrow points from the text 'Existing instance' to this dropdown menu. The 'OK' and 'Cancel' buttons are visible at the bottom of both windows.

Managed Just Like A Physical Firewall

HA, Policies, Eventing, etc.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FPR4K08-1-A Cisco Firepower 4110 Threat Defense

Device Routing **Interfaces** Inline Sets

Interface Ethernet1/7 Ethernet1/8.1001 Port-channel3 Port-channel5.100

Edit Sub Interface

General IPv4 IPv6 Advanced

Name: ☒ Enabled

Description:

Security Zone:

MTU: (64 - 9184)

Interface *:

Sub-Interface ID *: (1 - 4294967295)

VLAN ID: (1 - 4094)

OK Cancel

Subinterfaces are managed within FXOS

Everything else, except for subinterfaces, is managed just like a physical firewall



Alternative Designs

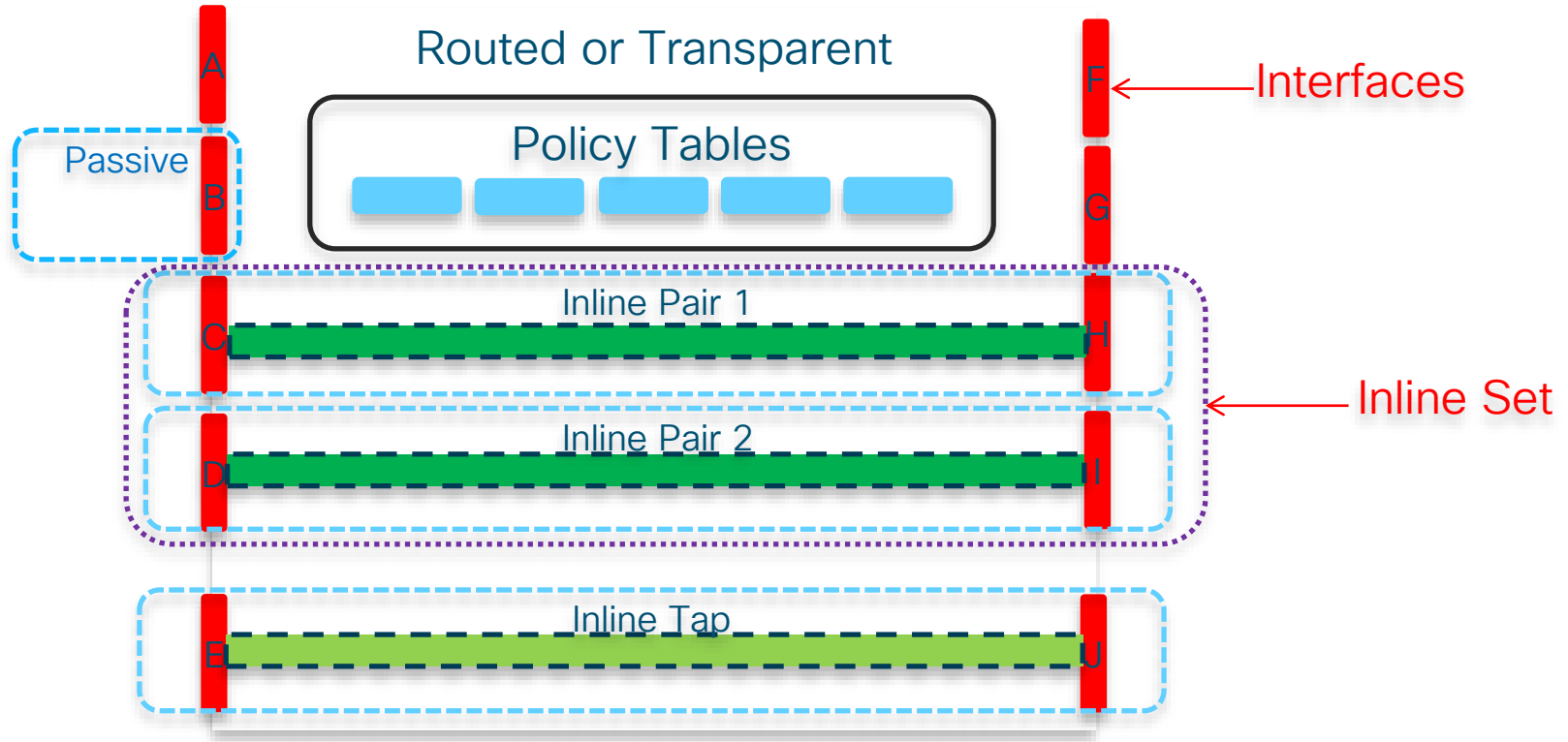
Interfaces Revisited: Optional Interface Modes

- By default, all interfaces are firewall interfaces (routed or transparent)
- Optionally, specific interfaces can be configured for use as IDS or IPS
- IDS Mode
 - Inline Tap
 - Passive
 - ERSPAN
- IPS Mode
 - Inline Pair

Edit Physical Interface

Mode:	<div>None</div>	<input checked="" type="checkbox"/> Enabled
Name:	<div>Passive</div>	
Security Zone:	<div>None</div>	
	<div>Erspar</div>	

Optional FTD Interface Modes



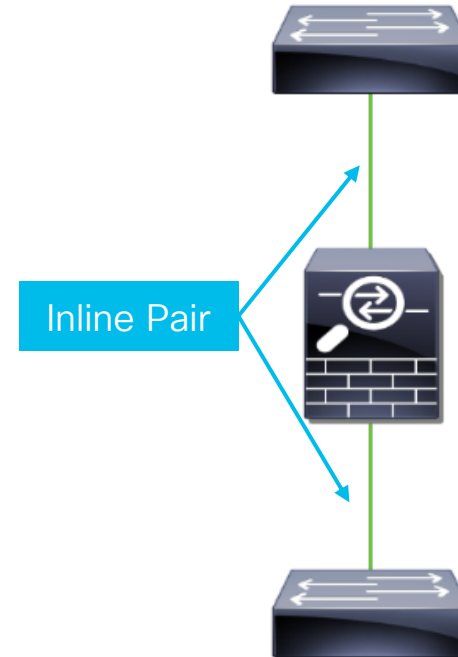
Inline NGFW

Firewall without Routing or Bridging Interfaces

- Although not a “Firewall” interface, L3/L4/L7 rules can be enforced when using “IPS” interface types
- Useful when Routed or Transparent aren’t possible/feasible
- No subinterfaces required for trunks, use “VLAN Tags” in ACP instead:



- Caveats:
 - No NAT / No Routing
 - No strict TCP state tracking



Configuration: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html>

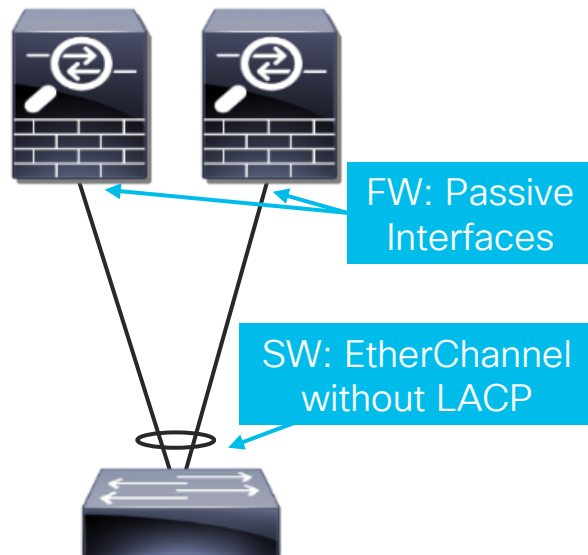
Out-of-Band IDS - Multichassis SPAN

When a single Firepower appliance is not enough

- Each device configured as a standalone device
- On switch, SPAN destination configured as EtherChannel
 - EtherChannel set to mode of “On”
- On firewall, each port configured as Passive interface:
- EtherChannel load balancing distributes traffic to different Firepower chassis

Edit Physical Interface

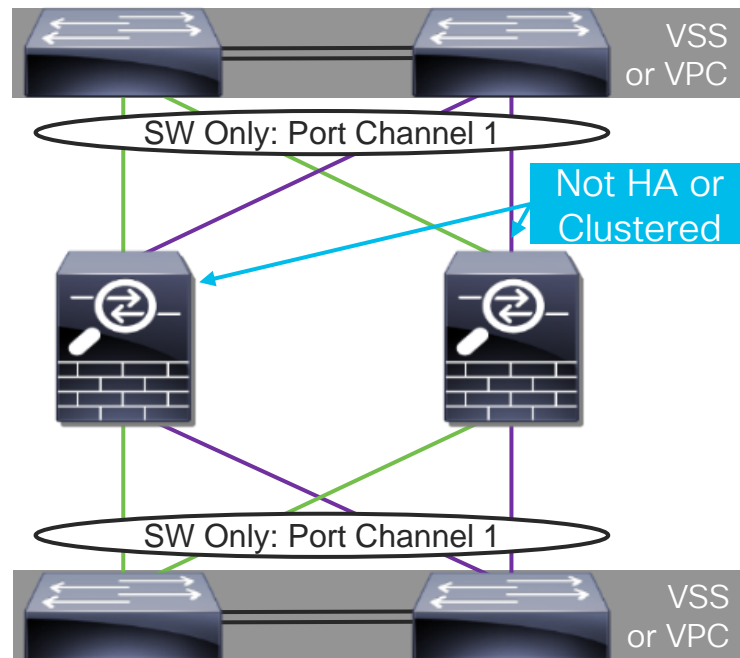
Mode: ▼



Inline IPS – Passthrough EtherChannel w/o HA

LACP EtherChannel through FTD

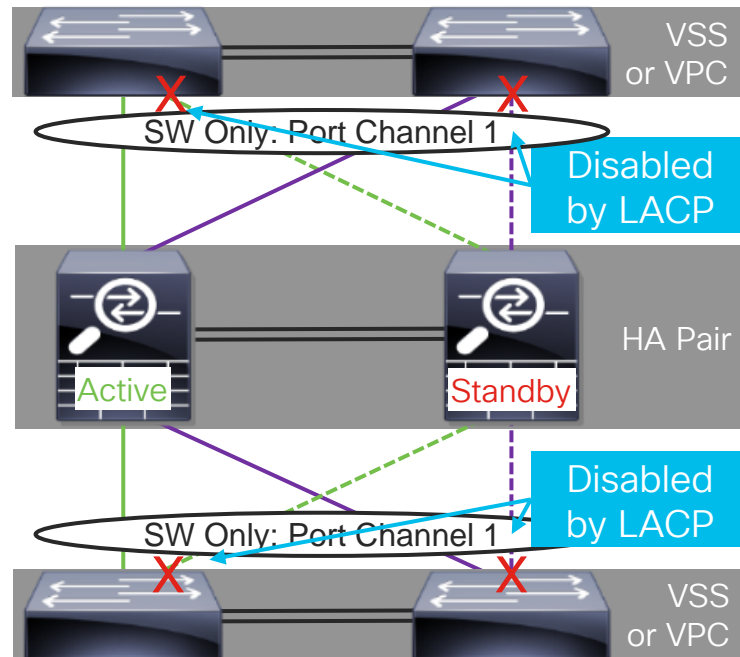
- Useful for scaling IPS without Clustering or scaling IPS with total fault isolation
- LACP EtherChannel formed between switches on either side of FTD
 - FTD has no knowledge of EtherChannel
 - Interfaces configured as Inline Pair on FW
 - Enable link state propagation on NGIPS inline pairs
- Each FTD appliance configured as standalone device in FMC
- Failover of FTD handled by LACP on SW
- EtherChannel MUST deliver symmetric traffic for effective security



Inline IPS – Passthrough EtherChannel w/ HA

LACP EtherChannel through FTD w/o Symmetric Traffic

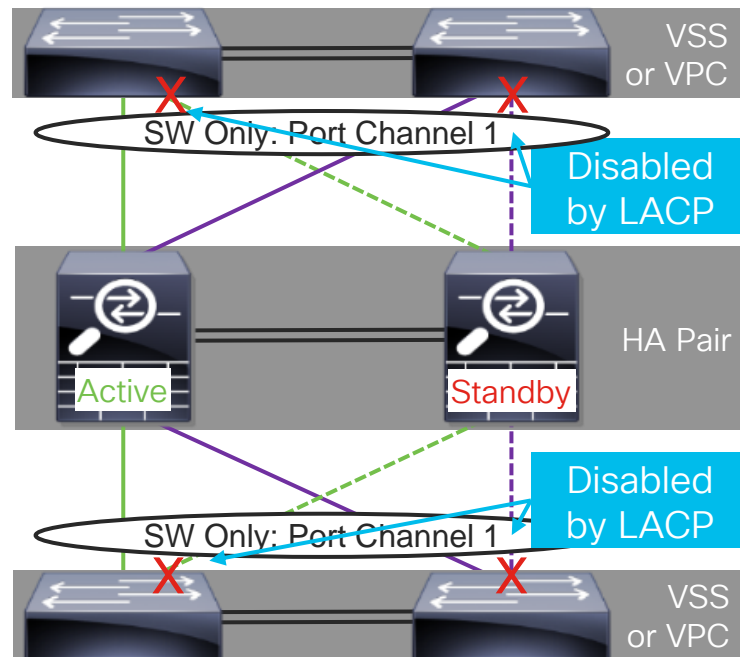
- Useful for IPS HA without Clustering
- Same interface configuration as Passthrough EtherChannel w/o HA
 - Traffic is automatically symmetric through FTD, since only 1 unit is ever active
- Inline pair interfaces on Standby HA unit are forced down when not active
- On failure of Active unit, LACP on SW:



Inline IPS – Passthrough EtherChannel w/ HA

LACP EtherChannel through FTD w/o Symmetric Traffic

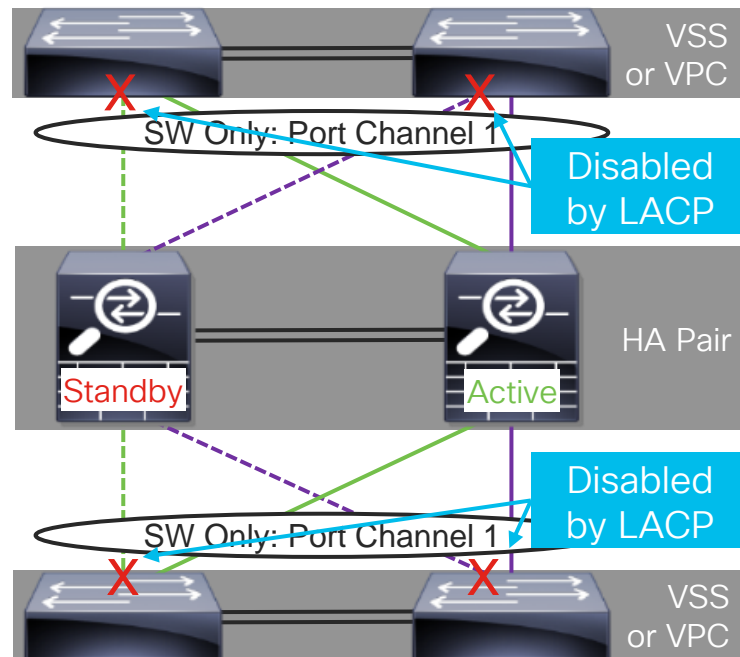
- Useful for IPS HA without Clustering
- Same interface configuration as Passthrough EtherChannel w/o HA
 - Traffic is automatically symmetric through FTD, since only 1 unit is ever active
- Inline pair interfaces on Standby HA unit are forced down when not active
- On failure of Active unit, LACP on SW:
 - Detects links on old Active unit are down and removes those ports from use in EtherChannel
 - Detects links to new Active unit are now up and starts sending traffic across those links



Inline IPS – Passthrough EtherChannel w/ HA

LACP EtherChannel through FTD w/o Symmetric Traffic

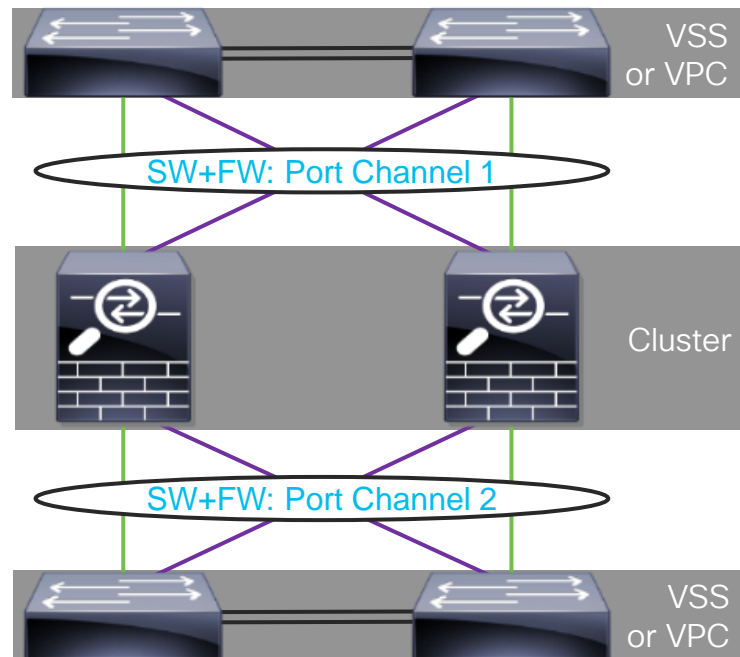
- Useful for IPS HA without Clustering
- Same interface configuration as Passthrough EtherChannel w/o HA
 - Traffic is automatically symmetric through FTD, since only 1 unit is ever active
- Inline pair interfaces on Standby HA unit are forced down when not active
- On failure of Active unit, LACP on SW:
 - Detects links on old Active unit are down and removes those ports from use in EtherChannel
 - Detects links to new Active unit are now up and starts sending traffic across those links



Inline IPS – EtherChannel Termination w/ Cluster

LACP EtherChannel to FTD

- Preferred method of scaling IPS w/ FTD
- Unlike previous designs, LACP EtherChannel terminates on FTD
 - Traffic is automatically symmetric through FTD, since Cluster handles any asymmetry
- Physical ports for both PC1 and PC2 configured in FXOS FCM
- PC1 and PC2 configured as Inline Pair within FMC



Continuing the Discussion – It's All About You

1 hour for questions
after the session

Ask question in the
WebEx Teams Room

Email me at
welchari@cisco.com

Cisco Firepower Sessions: Focus Blocks



Tuesday

11:00

BRKSEC-2020

Firepower NGFW in
DC and Enterprise

14:30

BRKSEC-3063

Decrypting the
Internet with
Firepower!

Wednesday

08:30

BRKSEC-2494

Maximizing Threat
Efficacy &
Performance

11:00

BRKSEC-3328

Making FMC do
more

Thursday

08:30

BRKSEC-3035

FP platforms deep
dive

11:15

BRKSEC-3455

Dissecting FP
NGFW: Architecture
& Troubleshooting

Friday

09:00

BRKSEC-3300

Adv. Firepower IPS
Deployment with FP
NGFW

11:30

BRKSEC-3032

FP NGFW
Clustering Deep
Dive

Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



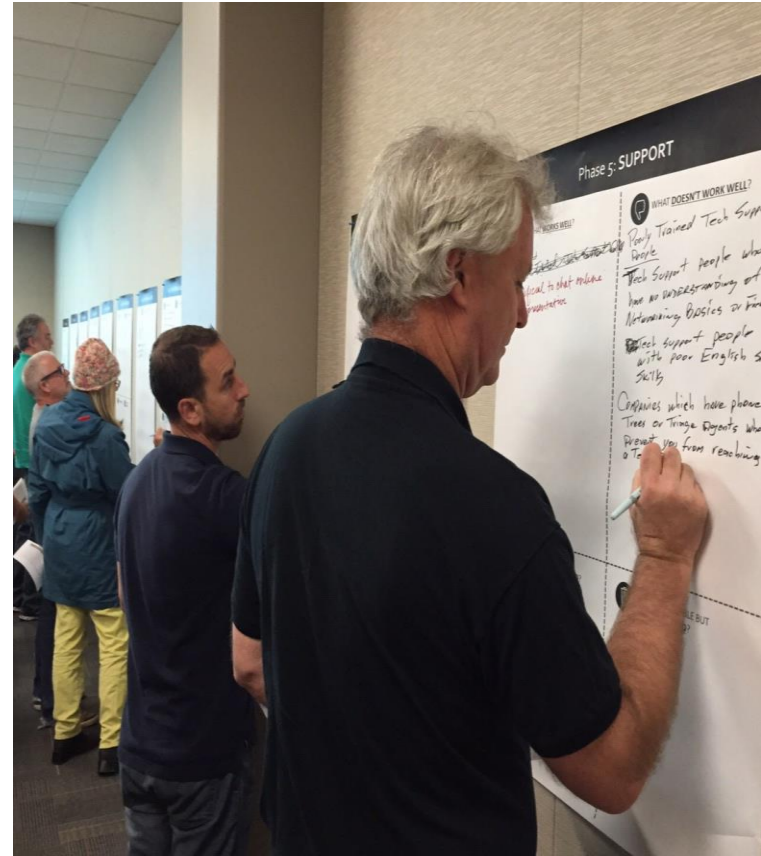
Meet the Engineer
1:1 meetings



Related sessions

SBG's User Experience (UX) team is running collaborative Design Thinking Sessions at Cisco Live!

Your ideas →
Sharpies + Inner Picasso
→
Product Improvements!



Do you:

- ✓ use our NextGen FireWall product(s)?
- ✓ wonder who you can bring your experience **pain points** to?
- ✓ have **ideas** that keep you up at night?
- ✓ want to improve product experience for yourself?

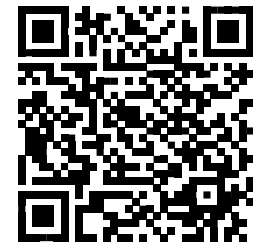
Come talk to Security User Experience (UX) Team!!

1



Come join our Design Thinking session on Tuesday or Thursday! Signup using QR code 1 (above).

2



Don't have time at Cisco Live? Join our UX participant database and we'll be in touch to showcase upcoming features and get your feedback! Signup using QR code 2.



Thank you





You make **possible**