cisco Live!

Let's go

The bridge to possible

Secure Firewall in the DC and Enterprise

Deployment Tips and New Features

Steven Chimes, Technical Solutions Architect

BRKSEC-2828

About Your Speaker

- Security Architect focused on global financials and global life sciences customers
- 15 years in industry including higher ed, manufacturing and 10 years at Cisco
- Author of CCNP Security Virtual Private Networks SVPN 300-730 Official Cert Guide

Agenda

- Frequently Asked Questions
- Hardware Selection
- Logging at Scale
- Useful Features
- Access Control Policy Tips
- HA and Clustering
- Dynamic Objects

Cisco Webex App

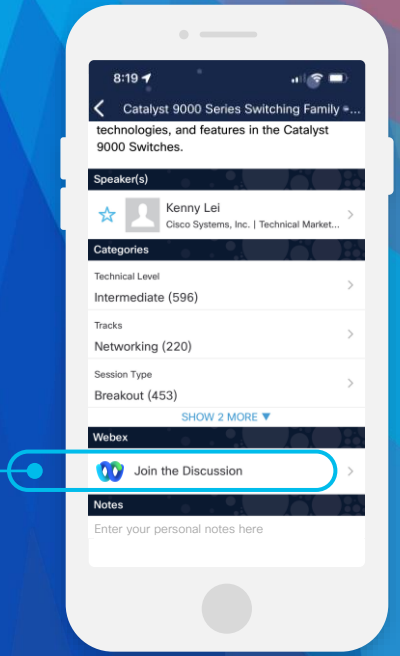
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2828

Frequently Asked Questions

FAQ - What Version Should I Be Running?

Software Download Page on cisco.com Has Latest Suggested Release

Downloads Home / Security / Firewalls / Firewall Management / Secure Firewall Management Center / Firepower Management Center 4600 / Firepower Management Center Software- 7.2.4

Search...

Expand All | Collapse All

Suggested Release

7.2.4

Latest Release

7.2.4

7.1.0.3

7.3.1

6.6.7.1

All Release

Firepower Management Center 4600

Release 7.2.4

My Notifications

Related Links and Documentation

Documentation for 7.2.4

Release Notes for 7.2.4

Hotfix Release Notes

File Information	Release Date	Size
Firepower Management Center 7.2.4 Hotfix AN Do not untar Cisco_Secure_FW_Mgmt_Center_Hotfix_AN-7.2.4.1-2.sh.REL.tar Advisories	11-May-2023	9.95 MB
Firepower Management Center install package Cisco_Secure_FW_Mgmt_Center-7.2.4-169-Restore.iso Advisories	10-May-2023	2017.56 MB

Suggested Release Is the Same for All Platforms

Look for the star

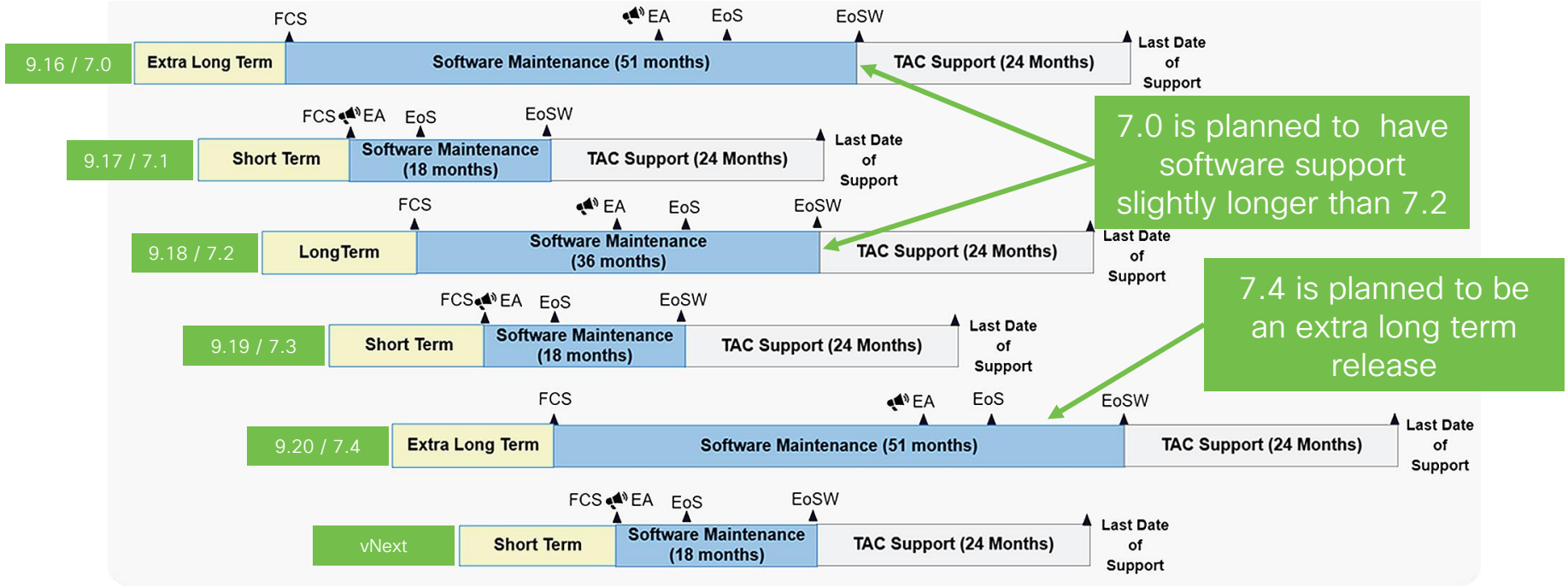
+

For the 4100/9300 Only - Latest Compatible FXOS Version, Currently 2.12(0.31)+

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

FAQ - What Version Do I Run Next?

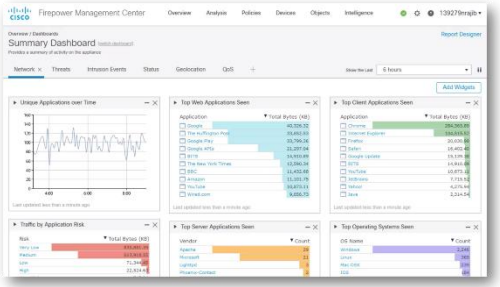
Note - These are only estimates, plans can/do change



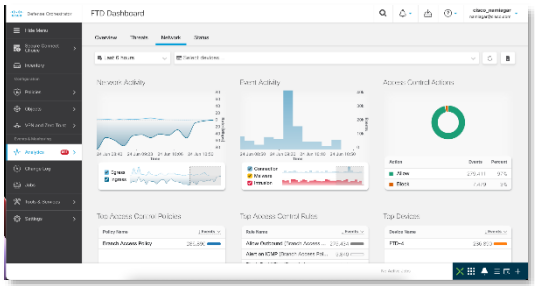
Cisco's NGFW Product Line Software Release and Sustaining Bulletin:
https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html

FAQ – What Firewall Manager Do I Use?

Firewall Management Center

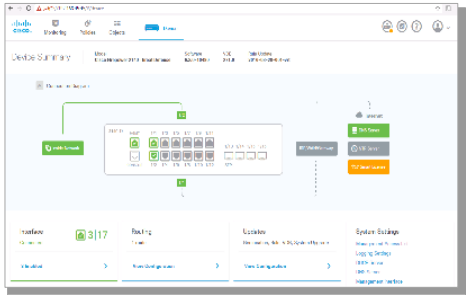


On premise centralized manager



Cloud-delivered centralized manager via Cisco Defense Orchestrator

Firewall Device Manager



On-box manager NetOps focused

Cloud Delivered Firewall Management Center

Defense Orchestrator
FMC / Policies / Access Control / Policy Editor

Analysis | Policies | Devices | Objects | Integration | Return Home | Deploy | schimes@cisco.com | SECURE

Egress Policy

Enter Description

Try New UI Layout | Analyze Hit Counts | Save | Cancel

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Inheritance Settings | Policy Assignments (0)

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

Filter by Device | Search Rules | Show Rule Conflicts | + Add Category | + Add Rule

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Dyna... Attribu...	Destin... Dyna... Attribu...	Action
Mandatory - Egress Policy (1-2)														
1	Allow HTTP/HTTPS	Any	Any	Any	Any	Any	Any	HTTP HTTPS	Any	Any	Any	Any	Any	Allow 0
2	Deny All	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block 0
Default - Egress Policy (-)														
There are no rules in this section. Add Rule or Add Category														

Clustered firewalls must be running 7.3 to be onboarded to cdFMC or running 7.4 to be migrated from FMC to cdFMC

Hardware Selection

Cisco Secure Firewall Hardware Portfolio

1010	1120/40/50	2110/20/30/40	3105/10/20/30/40	4112/15/25/45	4215/25/45 (NEW)	9300 Series SM-40 SM-48 SM-56
650 Mbps AVC+IPS	1.5-2.2 Gbps AVC+IPS	2.3-20 Gbps AVC+IPS	17-45 Gbps AVC+IPS 8 - 22.4 Gbps IPsec VPN 8 Node Cluster: With 3140, up to AVC+IPS(1024B) = 288 Gbps	Stand-alone device: 12-53 Gbps AVC 10-47 Gbps AVC+IPS Sixteen node cluster: Up to 680 Gbps AVC Up to 675 Gbps AVC+IPS	Stand-alone device: 70-150 Gbps AVC 70-145 Gbps AVC+IPS Sixteen node cluster: Up to 1.7 Tbps AVC Up to 1.6 Tbps AVC+IPS	One Module: 30-70 Gbps AVC 24-64 Gbps AVC+IPS Sixteen node cluster: AVC+IPS SM40*16n = 704 Gbps SM48*16n = 830 Gbps SM56*16n = 950 Gbps
SMB	Branch Office	Mid Enterprise	Large Enterprise	Data Center	Service Provider	

All appliances can run either ASA or FTD applications, FP9300 can run both on different SMs

Cisco Secure Firewall 4200 Series

Superior Performance

- Achieve High Performance Packet Processing with powerful hardware, a wide range of high performing network interfaces with a 1 RU footprint.
- Gain visibility into encrypted traffic with crypto-accelerated architecture, speeding up TLS and IPsec decryption.

Outstanding ROI

- Grow your security infrastructure as your business grows with clustering capability of up to 16 firewall devices.
- Ensure business uptime with hot-swappable network modules, including fail-to-wire interfaces.

1RU, 16X clustering, 200G interface support, 2X interface module bays, dual SSD, dual mgt interface

Cisco Secure Firewall 4200 Series

Crypto Acceleration

A specially built circuit to provide encryption/decryption acceleration

Crypto-acceleration using an FPGA (Field-programmable gate array)

Interface Flexibility

Support for 1G,10G,25G,40G,100G,200G interfaces across 2 Network Modules

Flow Offload

Flow offload engine processes packets in hardware up through layer 4

FIPS Compliance

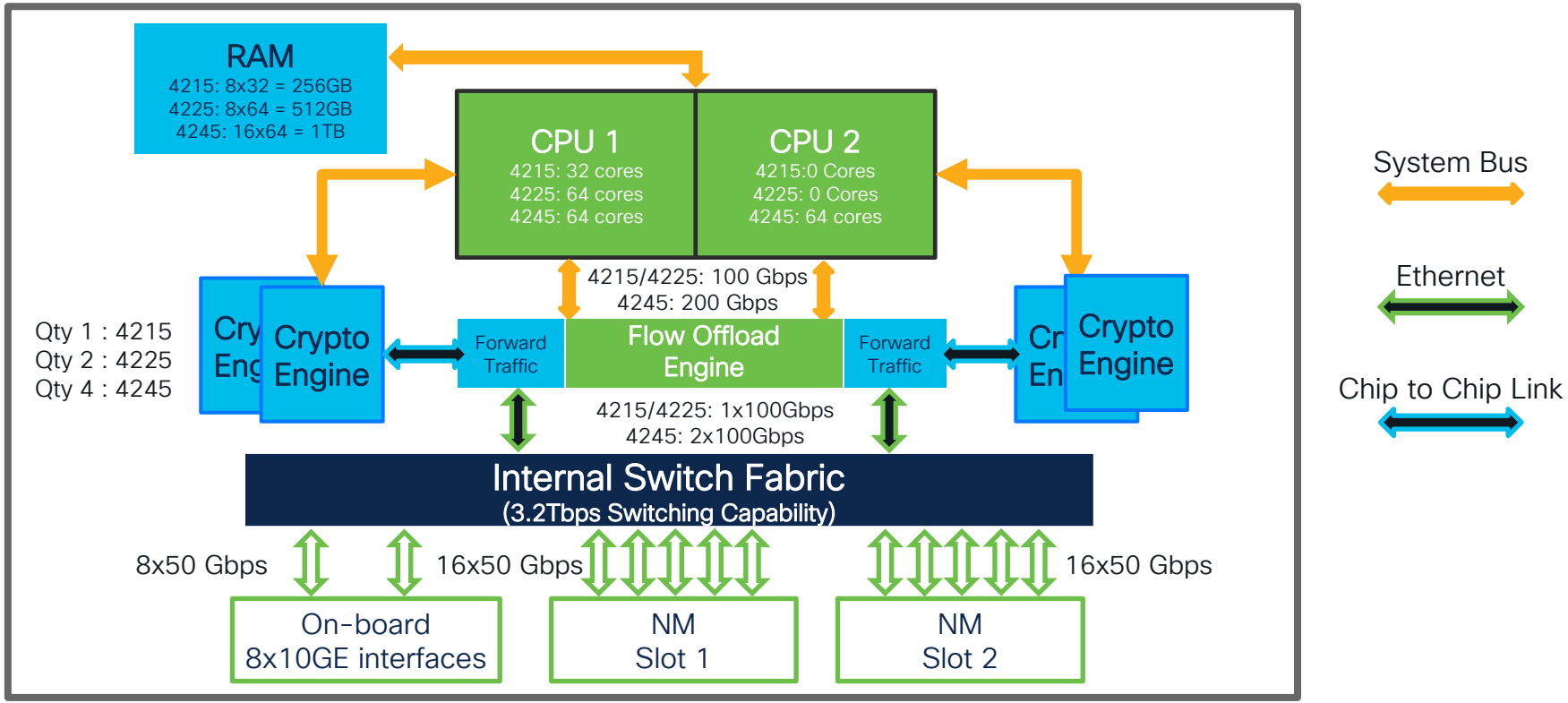
Supports all FIPS 140-3 requirements

Performance Metrics

Metric	4215	4225	4245
Throughput* FW+AVC+IPS	71 Gbps	89 Gbps	149 Gbps
Throughput* IPsec VPN (Fastpath)	51 Gbps	86 Gbps	96 Gbps
Maximum number of VPN peers	20000	25000	30000
Maximum concurrent connections with AVC	15 M	30 M	60 M
Maximum new connections per second (ASA code)	1.5 M	1.8 M	2.1 M

* Stateful Inspection 1024 Byte Packets

High-Level Hardware Architecture



Flexible Interface Architecture

- 2 x 1/10/25 G Management Port
- 8 x built in 1/10/25 G SFP28 data ports
- 2 x netmod slots
  - Hot swappable
  - 1G, 10G, 25G, 40G,100G, 200G, 400G (Coming)
  - Fail to wire, standard

High Performance Packet Processing
Flow Offload and Dynamic Flow Offload

- All 4200s include specialized hardware capable of stateful flow processing up through layer 4
  - Flow does not need to transit the system bus or engage the CPU complex
  - Flow offload engine supports up to 32M concurrent flows for IPv4 and 12M for IPv6
  - Example: the 4245 can do up to 125Gbps in a single TCP flow
- Static flow offload
  - Trusted flows can be specified by the administrator (using prefilter policies for FTD or service-policy for ASA)
- Dynamic flow offload
  - Snort deep packet inspection does not always require to inspection of the entire flow
  - Flows can be dynamically offloaded once inspection is completed

Hardware Crypto Acceleration

- Hardware Crypto Accelerator chips can perform IPsec Encryption/Decryption in hardware
  - 4215 – Nitrox V
  - 4225 – 2 x Nitrox V
  - 4245 – 4 x Nitrox V
- Dedicate inter-chip links between the crypto acceleration chip and the flow offload engine
  - Allows traffic to be decrypted and encrypted without adding traffic to the system bus.
- 4200 series includes support for full-stack TLS decryption including TLS 1.3

Logging at Scale

Logging Considerations for Large Deployments

Americas – DC #1

Americas – DC #2

EMEA – DC #1

EMEA – DC #2

APJC – DC #1

Total = 10x FP4145s

1x FP4145 = 365K CPS

Policy With Full Logging:
10x FP4145s = 3.6M EPS

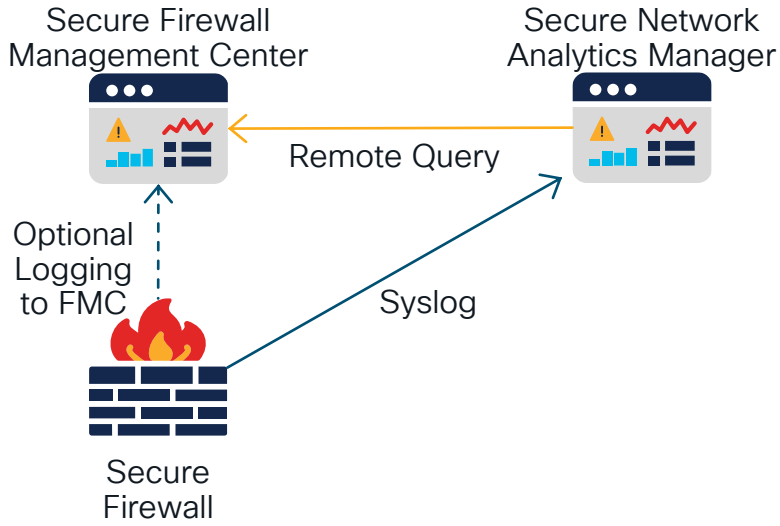
1x FMC4600
Rated for 20K EPS

Cisco Secure Firewall Logging Options

Firewall Management Center	Security Analytics and Logging (On-Premises)	Security Analytics and Logging (SaaS)
• Logs stored on physical or FMC virtual appliance • Logs sent via sftunnel • View logs in FMC	• Log stored on physical or virtual Secure Networks Analytics (SNA) appliance(s) • Logs sent via syslog • View logs in FMC w/ Unified Event View or on SNA Manager	• Logs stored in SAL cloud • Logs sent via built-in Secure Services Exchange (SSE) connector or via syslog to the Secure Event Connector (SEC) • View logs in CDO
Best for small FMC managed deployments	Best for larger FMC managed deployments	Best for CDO managed deployments

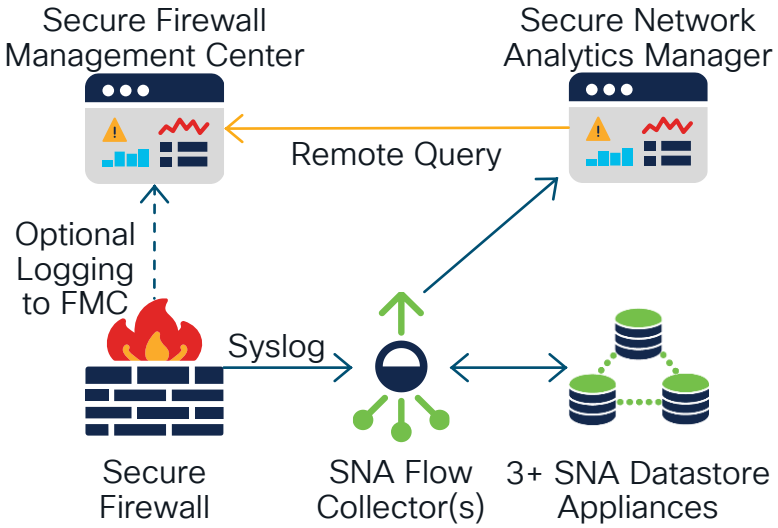
Security Analytics and Logging (On-Premises)

Single Node



Scales to 20k EPS (sustained)
Retention of 200 days @ 5k EPS

Multi-Node



Scales to 100k+ EPS (sustained)
Retention of 600+ days @ 5k EPS

Best for Larger FMC Managed Deployments

Unified Event Viewer

Connection, Security Intelligence, Intrusion, File & Malware Events

Firepower Management Center
Analysis / Unified Events

Overview | Analysis | Policies | Devices | Objects | Intelligence | a7d207schimes

Action !Fastpath | Application Protocol HTTP | Refresh

Showing all 3,043 events (2,964 1 32 33 14) | Auto | 2022-06-10 21:00:01 UTC → 2022-06-10 22:00:01 UTC 1h | Go Live

Uses data from FMC if it exists, otherwise pulls from SAL

Stream of events with most recent event at top

Event Data Source
- Automatic
- Local Storage on Management Center
- Extended Storage

Cancel | Apply

Time	Event Type	Action				Source Port / ICMP Type	Destination Port / ICMP Code	Web A
2022-06-10 21:59:59	Connection	Allow				49200 / t		
2022-06-10 21:59:54	Connection	Block	Intrusion Block	10.1.85.16	46.185.99.189	49247 / tcp	80 (http) / tcp	
2022-06-10 21:59:54	Intrusion	Dropped		46.185.99.189	10.1.85.16	80 (http) / tcp	49247 / tcp	
	Connection	Allow		10.1.115.49	130.211.103.172	51728 / tcp	80 (http) / tcp	Dotom
	Connection	Allow		10.1.117.5	52.3.99.86	61082 / tcp	80 (http) / tcp	The H

Event Type: Connection
Time: 2022-06-10 21:59:59
Last Packet: 2022-06-10 21:59:59
Action: Allow
Source IP: 10.1.114.69
Source User: phillip mathis (dcloud.cisco.com\pmath...
Destination IP: 96.82.200.1
Destination Continent: North America
Destination Country: USA
Ingress Security Zone: inside

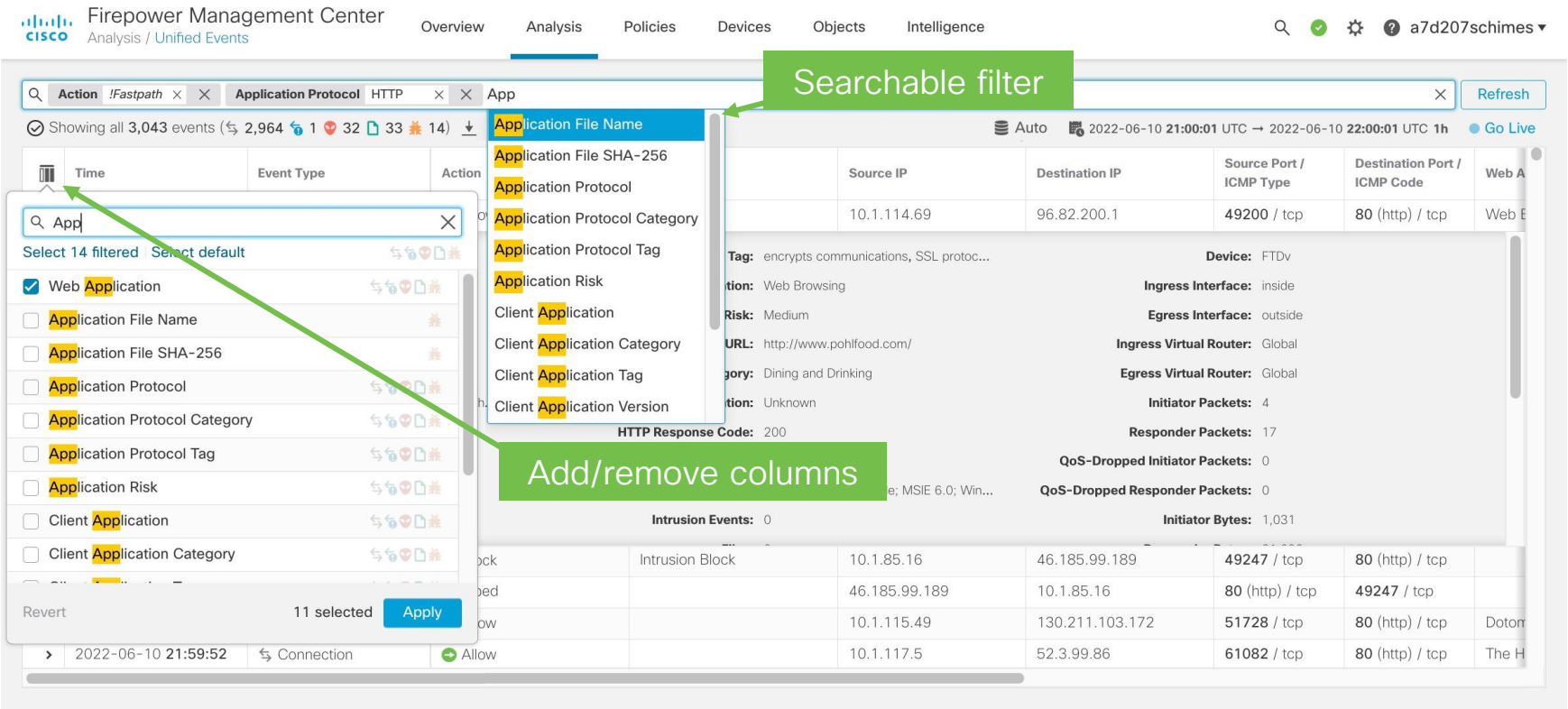
Client Application Tag: encrypts con
Web Application: Web Browsin
Application Risk: Medium
URL: http://www.p
URL Category: Dining and D
URL Reputation: Unknown
HTTP Response Code: 200
Referenced Host: www.pohlfood.com
User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win...
Intrusion Events: 0

Responder Packets: 17
QoS-Dropped Initiator Packets: 0
QoS-Dropped Responder Packets: 0
Initiator Bytes: 1,031

Dropdown to show all data for an event

Unified Event Viewer

Connection, Security Intelligence, Intrusion, File & Malware Events

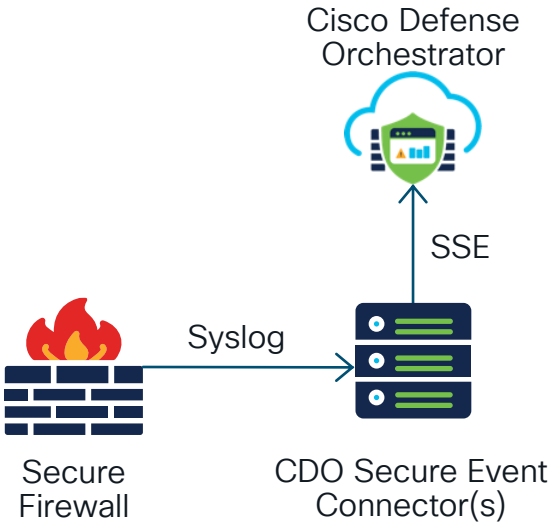


Security Analytics and Logging (SaaS)

Direct to Cloud

Scales to 8.5k EPS/FW
Retention Up to 3 Years

via CDO Secure Event Connector



Unlimited Scale
Retention Up to 3 Years

Best for Larger CDO Managed Deployments

Security Analytics and Logging (SaaS)

CDO Log Viewer

Filter builder

Freeform filter entry (supports Boolean logic)

Export to CSV

Click on a field to filter or click on magnifying class to add to an existing filter

Defense Orchestrator | Event Logging | cisco_namiagar schimes@cisco.com

Hide Menu
Secure Connect Choice
Inventory
Configuration
Policies
Objects
VPN and Zero Trust
Events & Monitoring
Analytics 717
Change Log
Jobs
Tools & Services
Settings

Historical | Live | Hostname: "ftd4.namiagar-lab.com" AND (Application:"HTTP" OR Application: "HTTPS")

Filter
FTD Events: Connection, File, Intrusion, Malware, Security Intelligence
ASA Events: All, AAA, BotNet, Failover, Firewall Denied, Firewall Traffic, IPsec VPN, NAT, NetFlow, SSL VPN
Time Range
Start: 06/06/2022 07:54:14 AM
End: -
Action
Action: ex. Allow

Clear | Time Range After 06/06/2022 07:54:14 AM

Views | View 1

Date/Time	Device Type	Event Type							Policy
Jun 6, 2022, 7:54:17 AM	FTD	Connection							Branch Access Policy
Jun 6, 2022, 7:54:17 AM	FTD	Connection	ftd4.namiagar...	172.16.225.90	104.156.85.2...	443	tcp	Allow	Branch Access Policy
Jun 6, 2022, 7:54:17 AM	FTD	Connection	ftd4.namiagar...	172.16.145.2...	206.33.41.253	80	tcp	Allow	Branch Access Policy
Jun 6, 2022, 7:54:17 AM	FTD	Connection	ftd4.namiagar...	172.16.145.2...	206.33.41.253	80	tcp	Allow	Branch Access Policy
Jun 6, 2022, 7:54:17 AM	FTD	Connection	ftd4.namiagar...	172.16.145.2...	206.33.41.253	80	tcp	Allow	Branch Access Policy

AC_RuleAction	Allow	EventSecond	Jun 6, 2022, 6:54:11 AM	InitiatorPackets	1
Application	HTTPS	EventSubtype	End	InitiatorPort	50393
ClientApplication	Secure	EventType	ConnectionEvent	InstanceID	1
ConnectionID	42694	FirewallPolicy	Branch Access Policy	LastPacketSecond	Jun 6, 2022, 6:54:11 AM
ConnectorID	90d7b4e-a051-0	FirewallRule	Allow Outbound	NAP_Policy	Balanced Security and Connectivity
		FirstPacketSecond	Jun 6, 2022, 6:54:11 AM	PrefilterPolicy	Default Prefilter Policy
DeviceIP	128.107	Hostname	ftd4.namiagar-lab.com	Protocol	tcp
DeviceType	FTD	IngressInterface	inside	ResponderBytes	565
DeviceUUID	19531d8c-c24d-11ec-adcb-91d24f46c917	IngressVRF	Global	ResponderIP	104.156.85.217
EgressInterface	outside	IngressZone	inside	ResponderPackets	7
EgressVRF	Global	InitiatorBytes	62	ResponderPort	443
EgressZone	outside	InitiatorIP	172.16.225.90	timestamp	Jun 6, 2022, 7:54:17 AM
EventPriority	Low				

AND
OR
NOT
AND NOT
OR NOT

No Active Jobs

SAL Log Data Retention Matrix

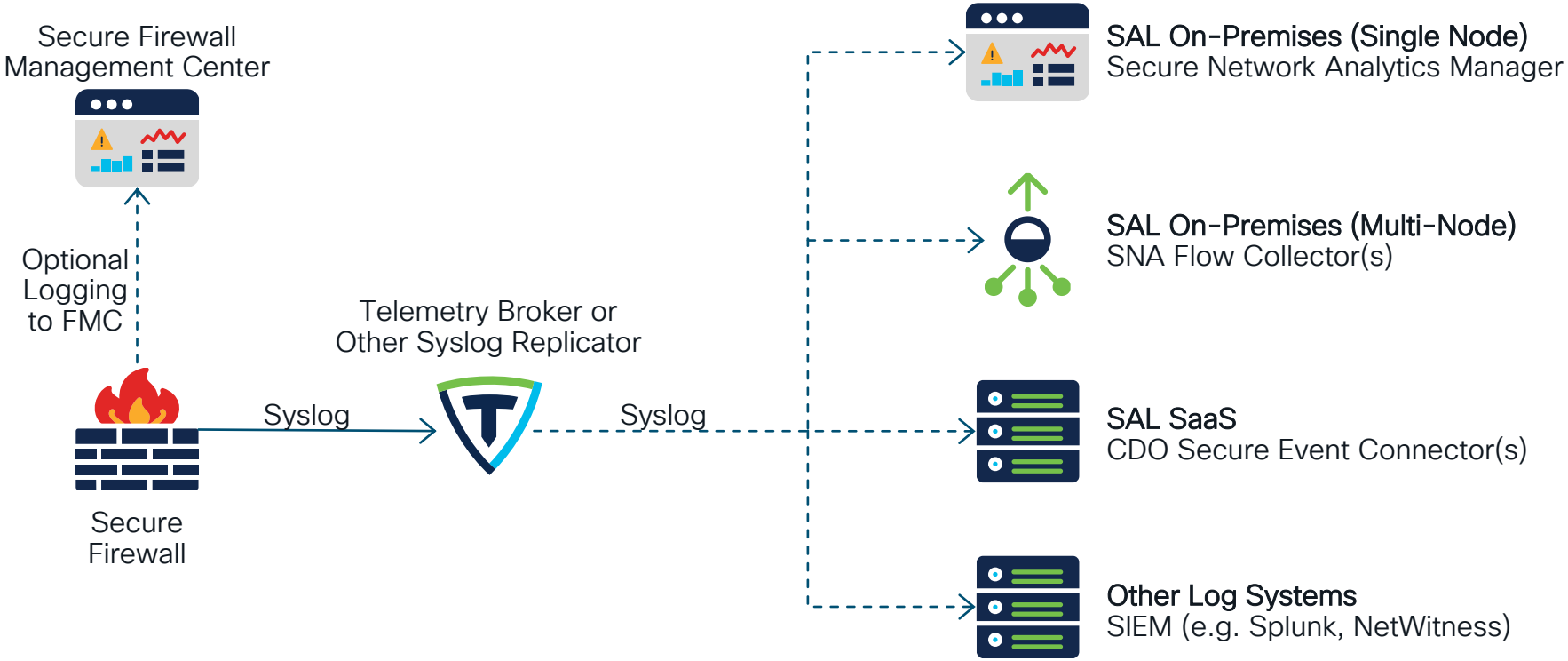
Sustained Firewall Events per Second (EPS)	Equivalent GB/day	On-premises					Cloud		
		Single Node* 1TB Storage	Single Node* 2TB Storage	Single Node* 4TB Storage	Multi-Node** Virtual	Multi-node** HW	Single SEC	Multi-SEC	Direct-to-Cloud
		Expected Retention period in days (under average deployment conditions)							
5,000	562	50	100	200	300	600	Up to 3 years	Up to 3 years	Up to 3 years Not suggested when individual device's logging rate exceeds 8,500 eps
10,000	1,123	25	50	100	150	300			
20,000	2,246	12.5	25	50	75	150***			
50,000	5,616	NA	NA	NA	30	60			
75,000	8,424	NA	NA	NA	NA	40			
100,000	11,232	NA	NA	NA	NA	30			
200,000	22,464	NA	NA	NA	NA	NA	NA		

Note: The on-premises log retention in days above are based on average deployment conditions, and may vary materially in different production environments

* Single-node = Repurposed SMC 2210 (HW or Virtual) ** Multi-node = SMC 2210 + FC 4210 + 3 x DS 6200 (All appliances HW or Virtual)
*** Compare FMC native logs retention ½ day @ 20,000 peak EPS

For Best Performance, Send Logs Only Once

Use Telemetry Broker to Send Logs to Multiple Destinations



Useful Features You May Not Know About

4100/9300 Chassis Registration to FMC

- FMC have capability to register 4100/9300 chassis into device list
- FXOS faults (including HW bypass) collected by the FMC
- Chassis events available in Health Monitor and Events

Access Control Policy – Bulk Edit

Shift-click then shift-click to select a range
OR
ctrl/command-click to select individual rules.

Then right click to open the bulk edit menu.

Clicking without holding shift/ctrl/command will immediately open the clicked rule

Firewall Management Center
Policies / Access Control / Policy Editor

Deploy admin SECURE

Egress Policy
Enter Description

Try New UI Layout | Analyze Hit Counts | Save | Cancel

Rules | Security Intelligence | HTTP Respon

Filter by Device | Search Rules

#	Name	Source Zones	Dest Zones
Mandatory - Egress Policy (1-12)			
1	Rule 1	Any	Any
2	Rule 2	Any	Any
3	Rule 3	Any	Any
4	Rule 4	Any	Any
5	Rule 5	Any	Any
6	Rule 6	Any	Any
7	Rule 7	Any	Any
8	Rule 8	Any	Any
9	Rule 9	Any	Any
10	Rule 10	Any	Any
11	Rule 11	Any	Any
12	Rule 12	Any	Any
Default - Egre			
Default Action			

Cut
Copy to
Move to another policy
Paste Above
Paste Below
Object Details...
Edit...
Delete
State
Insert new rule...
Insert new category...
Show events

10 Rows Selected

Displaying 1 - 12 of 12 rul

Editing 10 Access Rules

General
- Enabled: Yes
- Action: Allow

Inspection
- Intrusion Policy: Intrusion Prevention: Security Ov
- Variable Set: Default Set
- File Policy: None

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

File Events:
- Log Files: Yes

Send Connection Events to:
- Security Analytics and Logging: Yes
- Syslog Server: Yes

Cancel | OK

Access Control Policy – Bulk Edit

Firewall Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Deploy | admin | cisco SECURE

Egress Policy

Enter Description

Try New UI Layout | Analyze Hit Counts | Save | Cancel

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Inheritance Settings | Policy Assignments (2)

er Policy: Default Prefilter Policy | SSL Policy: None | Identity Policy: None

Filter by Device | Search Rules | Show Rule Conflicts | + Add Category | + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Dynamic Attributes	Destination Dynamic Attributes	Action
Mandatory - Egress Policy (1-12)									
1	Rule 1	Any	Any	Any	Any	Any	Any	Any	Allow
2	Rule 2	Any	Any	Any	Any	Any	Any	Any	Allow
3	Rule 3	Any	Any	Any	Any	Any	Any	Any	Allow
4	Rule 4	Any	Any	Any	Any	Any	Any	Any	Allow
5	Rule 5	Any	Any	Any	Any	Any	Any	Any	Allow
6	Rule 6	Any	Any	Any	Any	Any	Any	Any	Allow
7	Rule 7	Any	Any	Any	Any	Any	Any	Any	Allow
8	Rule 8	Any	Any	Any	Any	Any	Any	Any	Allow
9	Rule 9	Any	Any	Any	Any	Any	Any	Any	Allow
10	Rule 10	Any	Any	Any	Any	Any	Any	Any	Allow
11	Rule 11	Any	Any	Any	Any	Any	Any	Any	Allow
12	Rule 12	Any	Any	Any	Any	Any	Any	Any	Allow
Default - Egress Policy (-)									

Default Action: Access Control:Block all traffic

10 Rows Selected | Displaying 1 - 12 of 12 rules | Page 1 of 1 | Rules per page: 100

Editing 10 Access Rules

General

- [ ] Enabled: Yes
- [ ] Action: Allow

Inspection

- [x] Intrusion Policy: Intrusion Prevention: Security Ov
- [ ] Variable Set: Default Set
- [ ] File Policy: None

Logging

- [x] Log at Beginning of Connection: Yes
- [x] Log at End of Connection: Yes

File Events:

- [ ] Log Files: Yes

Send Connection Events to:

- [ ] Security Analytics and Logging: Yes
- [ ] Syslog Server: Yes

Cancel | OK

Access Control Policy – New UI

Firewall Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Devices | Objects | Integration

Deploy | admin | SECURE

Return to Access Control Policy Management

Egress Policy

Processing chain shown in order

Toggle new UI

Switch to Legacy UI

Analyze Hit Counts | Discard | Save

Packets → Prefilter Rules → SSL → Security Intelligence → Identity → Access Control | More

Targeted: 2 devices

Select Bulk Action

Bulk actions

Total 12 | Selected 10

Add Category | Add Rule

Select rules for bulk action

		Name		Source Zones	Source Networks	Source Ports	Destination Zones	Destination Networks	Destination Ports	Applications	Users	URL
		Mandatory (1 - 12)										
☑	1	Rule 1	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☑	2	Rule 2	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☑	3	Rule 3	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☑					Any	Any	Any	Any	Any	Any	Any	An
☑					Any	Any	Any	Any	Any	Any	Any	An
☑					Any	Any	Any	Any	Any	Any	Any	An
☑	7	Rule 7	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☑	8	Rule 8	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☑	9	Rule 9	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☑	10	Rule 10	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☐	11	Rule 11	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
☐	12	Rule 12	Allow	Any	Any	Any	Any	Any	Any	Any	Any	An
		Default										

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

Default Action | Access Control: Block All Traffic

Access Control Policy – New UI / Bulk Edit

Firewall Management Center
Objects / Object Management

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

- AAA Server
- Access List
- Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- Distinguished Name
- DNS Server Group
- External Attributes
- File List
- FlexConfig
- Geolocation
- Interface
- Key Chain
- Network
- PKI
- Policy List

Network

Add Network

Filter

Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various pla control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

- Add Object
- Import Object
- Add Group

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	::/0	Host	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	

Displaying 1 - 14 of 14 rows | Page 1 of 1

Bulk Import of Objects

Available for DN, Network, Port, URL & VLAN objects

Firepower Management Center
Objects / Object Management

Overview | Analysis | Policies | Devices | Objects | Intelligence | 5dbe20schimes

- Key Chain
- Network
- PKI
- Policy List
- Port
- Prefix List
- Route Map
- Security Intelligence
- Sinkhole
- SLA Monitor
- Time Range
- Time Zone
- Tunnel Zone

Import Network Objects

Column header is mandatory.
Column header should be in capital letters.

The header for Network object should have the below columns
NAME,DESCRIPTION,TYPE,VALUE,LOOKUP

Sample data :
Object_1,inside edge host,Host,172.44.55.66,
Object_2,dns host range,Range,2.2.2.3-2.2.2.9,
Object_3,,FQDN,12,

Import csv file
Example_Import.csv | Browse..

Cancel | Import

Add Network
- Add Object
- Import Object
- Add Group

Filter
Show Unused Objects

sed in various pla control policies, network variables, , and so on.

Value	Type	Override
::/0 0.0.0.0/0	Group	
0.0.0.0/0	Network	
::/0	Host	
10.1.0.0/16	Network	
198.18.0.0/15	Network	
169.254.0.0/16	Network	

15 rows | Page 1 of 1

	A	B	C	D	E
1	NAME	DESCRIPTION	TYPE	VALUE	LOOKUP
2	Object_1	inside edge host	Host	172.44.55.66	
3	Object_2	dns host range	Range	2.2.2.3-2.2.2.9	
4	Object_3		FQDN	12	

~/Desktop/Example_Import.csv

```
1 NAME,DESCRIPTION,TYPE,VALUE,LOOKUP
2 Object_1,inside edge host,Host,172.44.55.66,
3 Object_2,dns host range,Range,2.2.2.3-2.2.2.9,
4 Object_3,,FQDN,12,
```

Bulk Import of Objects

Available for DN, Network, Port, URL & VLAN objects

Object Type	Rules
Individual object	• The file must have the columns headers: NAME, DN • Both NAME and DN column entries are mandatory to import an entry. • You can import individual objects directly into an existing distinguished name object group.
Network object	• The file must have the columns headers: NAME, DESCRIPTION, TYPE, VALUE, LOOKUP • The NAME and VALUE column entries are mandatory to import an entry of host, range, or network object type. • For an FQDN object, the TYPE column entry must mention 'fqdn,' and the LOOKUP column entry must be specified as 'ipv4,' 'ipv6,' or 'ipv4_ipv6.' • If no content is provided in the LOOKUP column entry for the FQDN object, then the object is saved with the ipv4_ipv6 field value.
Port	• The file must have the columns headers: NAME, PROTOCOL, PORT, ICMPCODE, ICMPTYPE • The NAME column entry is mandatory. • For 'tcp' and 'udp' protocol types, the PORT column entry is mandatory. • For 'icmp' and 'icmp6' protocol types, the ICMPCODE and ICMPTYPE column entries are mandatory.
URL	• The file must have the columns headers: NAME, DESCRIPTION, URL • The NAME and URL column entries are mandatory to import an entry.
VLAN Tag	• The file must have the following columns headers: NAME, DESCRIPTION, TAG • The NAME and TAG column entries are mandatory to import an entry.

The column header is required and must be in capital letters.

Global Search

Easily Find Navigation Pages, Policies, Objects by Name or Values (e.g. IP)

Firewall Management Center
Overview / Dashboards / Dashboard

DNS

admin ▾ SECURE

21 Search Results
(navigation | objects | policies | devices | how-tos)

You can use the arrow keys to navigate the search result

Reporting

Summary Dashboard (switch dashboard)
Provides a summary of activity on the appliance

Network Threats Intrusion Events

1 hour

Add Widgets

Navigation

Policies / Access Control / DNS

Objects

Port

DNS_over_TCP *(tcp (6)/53)*

DNS_over_UDP *(udp (17)/53)*

Policies

Access Control Policy

Egress Policy

Devices

DNS-Firewall-1

DNS_over_UDP

Port Object (TCP, UDP, Other)

General Usages

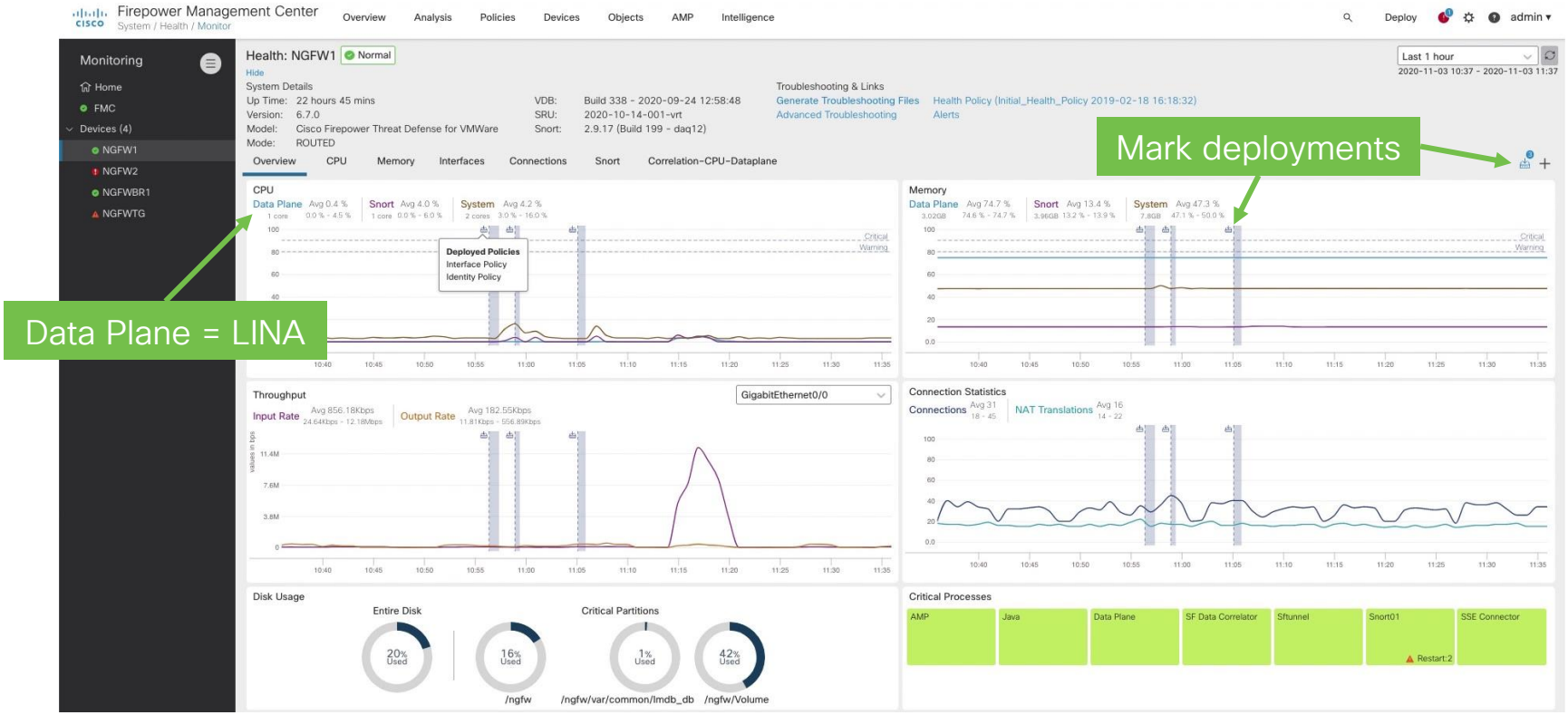
Name	DNS_over_UDP
Description	–
Protocol	UDP
Port	53
Allow Overrides	No

If you forget where something is in the menu, use global search

Searches both the name of objects/policies, as well as the content (e.g. rule named “Allow DNS” in Egress Policy)

Device Health Monitoring Dashboard

No more going to the CLI for basic performance troubleshooting!



Device Health Monitoring Dashboard

Use Correlated Dashboards for Easy Troubleshooting

Defense Orchestrator / Monitoring

Monitoring | Policies | Devices | Objects | Integration

Return to Inventory | Deploy | schimes@cisco.com | SECURE

Monitoring
- Home
- Devices (3)
  - FTD-3
  - FTD-4

Health: FTD-4 Critical

View System & Troubleshoot Details ...

Overview | CPU | Memory | Interfaces | Connections | Snort | ASP drops | Correlation-CPU-Dataplane

Last 12 hours
2022-06-12 07:01 - 2022-06-12 19:01

CPU - Control Plane, Data Plane

Interface - Input Packets

Connections - Active Connections, Peak Connections

Deployed Configuration - Number of ACEs

Create custom and prebuilt dashboards

Spike in CPU caused by connection spike

Correlate Metrics

Correlate the metrics that are inter-related. Select predefined correlation groups or custom to specify your own metrics.

Correlation Group*
CPU - Data plane

Hide Details

Dashboard Name*
Correlation-CPU-Dataplane

Metrics
Chosen metrics will be displayed as portlets in the dashboard.

CPU	Control Plane × Data Plane ×
Interface	Input Packets ×
Connections	Active Connections × Peak Connections ×
Deployed Configuration	Number of ACEs ×

Add Metrics

Cancel | Add

Elephant Flow Remediation

Firewall Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

Egress Policy

Enter Description

Try New UI Layout | Analyze Hit Counts | Save | Cancel

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Inheritance Settings | Policy Assignments (2)

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

General Settings

Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
Retry URL cache miss lookup	Yes
Enable Threat Intelligence Director	Yes
Enable reputation enforcement on DNS traffic	Yes
Inspect traffic during policy apply	Yes

Identity Policy Settings

Identity Policy	None

Threat Detection

Portscan Mode	Disable

Elephant Flow Settings

Generate Elephant Flow Events	Enable

Intelligent Application Bypass Settings

Intelligent Application Bypass Settings	Off
Total Apps and Filters Configured	All applications including unidentified applications

Transport/Network Layer Preprocessor Settings

Ignore the VLAN header when tracking connections	No

Elephant Flow Remediation

Available with Snort 3 Running 7.2 or Higher

Firewall Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

Egress Policy
Enter Description

Rules | Security Intelligence | HTT

Analyze Hit Counts | Save | Cancel

Inheritance Settings | Policy Assignments (2)
SSL Policy: None | Identity Policy: None

General Settings

Maximum URL characters to store in connection events — Disable

Allow an Interactive Block to bypass blocking (seconds)

Retry URL cache miss lookup — Enable

Enable Threat Intelligence Director

Enable reputation enforcement on DNS traffic — Off

Inspect traffic during policy apply — ...ons including unidentified applications

Identity Policy Settings

Identity Policy

Logging Connections — No

Elephant Flow Settings

For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass settings.

Elephant flow detection does not apply to encrypted traffic. Learn more

Elephant Flow Detection

Generate elephant flow events when flow bytes **exceeds** 1024 MB and flow duration **exceeds** 10 seconds

Elephant flow Remediation

If CPU utilization **exceeds** 40 **% in fixed time windows of** 30 seconds and packet drop **exceeds** 5 %

Then Bypass the flow

All applications including unidentified applications

Select Applications/Filters (1 selected)

And Throttle the remaining flows

Revert to Defaults | Cancel | OK

Enable bypass for the apps you trust. Throttle the rest.

Throttle = 10% less than current flow rate

Packet Tracer PCAP Upload

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

File Download | Threat Defense CLI | Packet Capture

Trace History

Google Trace +

Select Device* FTD-161

Interface* OUTSIDE - GigabitEthernet0/0

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

Protocol* TCP or Google.pcap

Source Type* IPv4 100.100.1.253

Destination Type* IPv4 172.253.122.94

Source Port* 53058 (0-65535)

Destination Port* 443 (0-65535)

Inline Tag (0-65533)

Bypass security checks for the simulated packet

Treat the simulated packet as an IPsec/SSL VPN decrypted packet

Reset | Trace

Trace Result

Packet 1: 21:10:50.449103

Single flow, maximum of 100 packets

Make sure you specify a snaplen to avoid an “Unsupported Protocol found” error when uploading the PCAP

Wireshark · Capture Options

Input | Output | Options

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
Wi-Fi: en0		Ethernet		1600	2		
p2p0		Raw IP		default	2		

Packet Tracer PCAP Upload

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

Expandable trace history

Trace History

File Download | Threat Defense CLI | Packet Capture

Save Traces 1 / 100 | Clear Traces

Google Trace

Search

Today

Google Trace
FTD-161
ALLOW
interface:GigabitEthernet0/0,protocol:TCP,sourceIPType:IPv4,sourceIPValue:100.100.1.253,sourcePort:53058,destinationIPType:IPv4,destinationIPValue: ...

Trace Result

Packet 1: 21:10:50.449103
Packet 2: 21:10:50.449897
Packet 3: 21:10:50.450034
Packet 4: 21:10:50.450172
Packet 5: 21:10:50.453406
Packet 6: 21:10:50.453452
Packet 7: 21:10:50.453620
Packet 8: 21:10:50.453666
Packet 9: 21:10:50.453727
Packet 10: 21:10:50.453772
Packet 11: 21:10:50.453818

Result of each packet is shown

Packet Details: 21:10:50.450172 100.100.1.253:53058 > 172.253.122.94:443 tcp 80

OUTSIDE(vrfid:0)

FLOW-LOOKUP

EXTERNAL-INSPECT

SNORT | appid

Expand to see processing details of each step

Type:	SNORT
Subtype:	appid
Result:	ALLOW
Config:	
Elapsed Time:	7861944 ns
Additional Information	service: HTTPS(1122), client: SSL client(1296), payload: Google(184), misc: (0)

SNORT | firewall

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

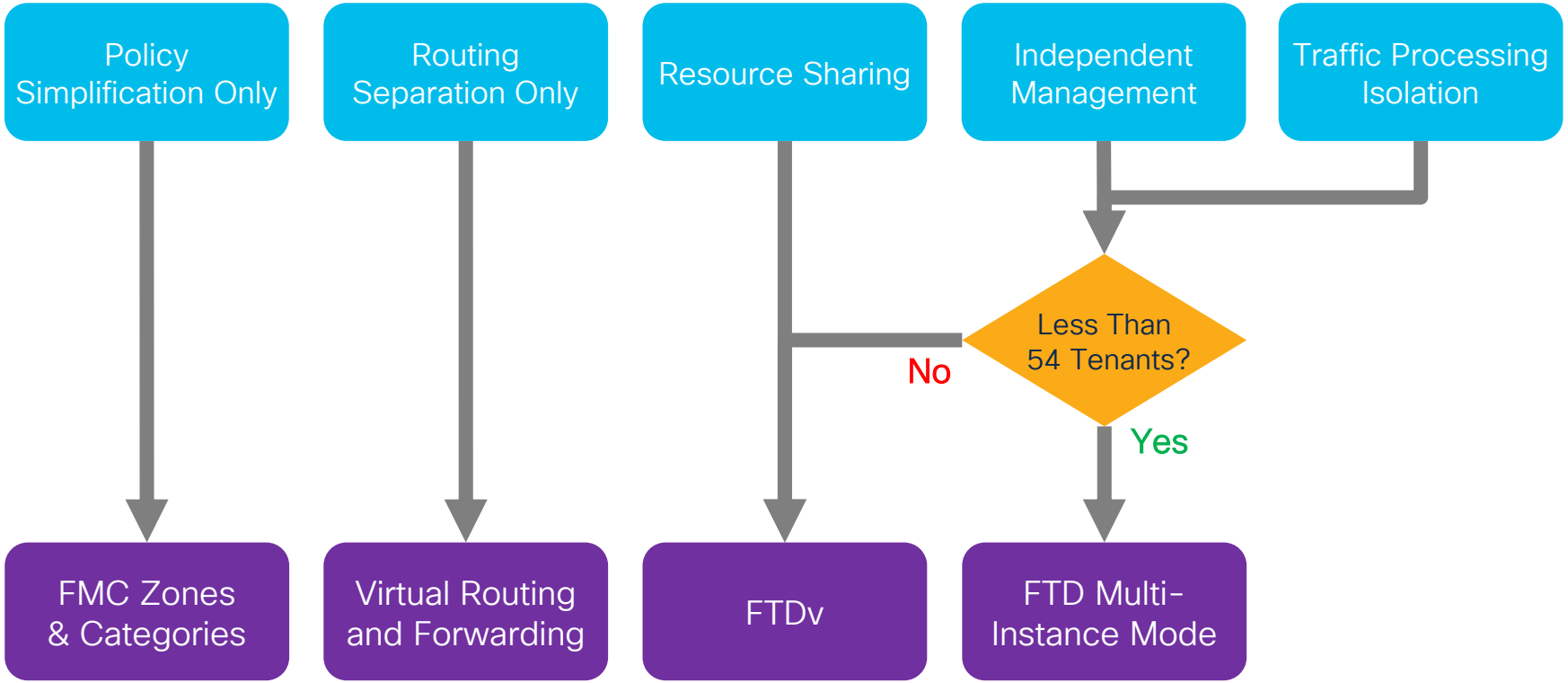
Policy Management Simplification

Smaller policy views that are managed by a single administrator

Management Separation

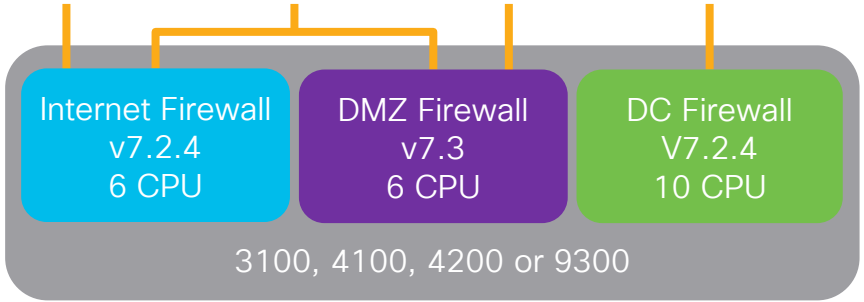
Independent management of firewall partitions

Multi-Tenancy Use Case Mapping



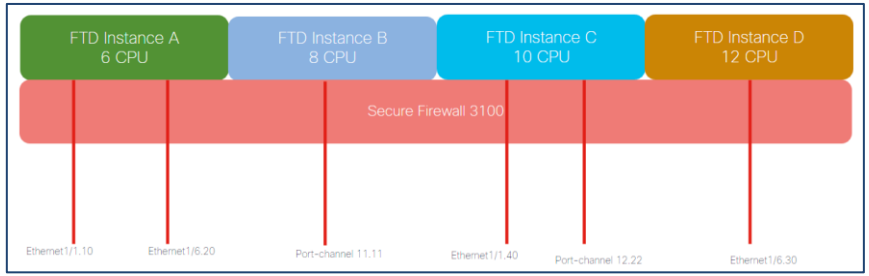
Secure Firewall Multi-Instance Intro

- 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 Secure Firewall software version
- Physical, logical and VLAN separation provided by chassis supervisor



Multi-Instance on 3100

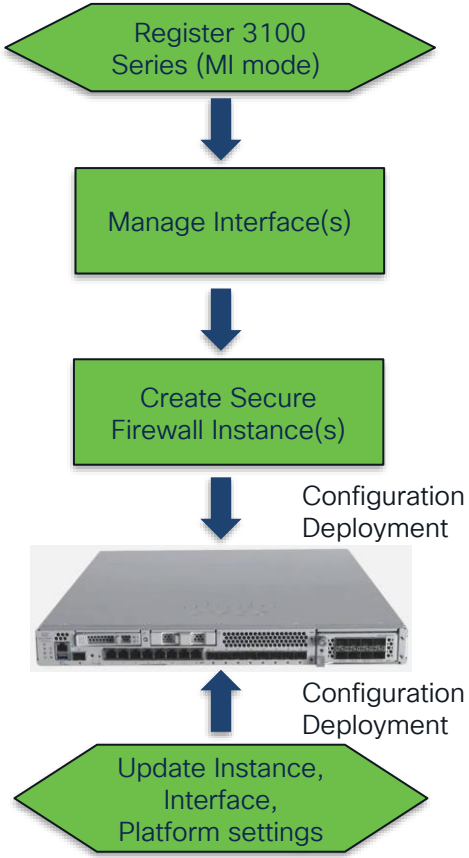
- 31xx series Multi-Instance feature functionality is identical to the Firepower 4100 series, but it differs in the number of instances supported:
  - 3105 supports no (0) Instances
  - CSF 3110 supports up to 3 Instances max
  - CSF 3120 supports up to 5 Instances max
  - CSF 3130 supports up to 7 Instances max
  - CSF 3140 supports up to 10 Instances max



- All Multi-Instance configuration is only through FMC.
- Multi-Instance configuration is not supported via CLI. However, changing from Native to Container Mode is supported in the CLI.

Multi-Instance on 3100 Config

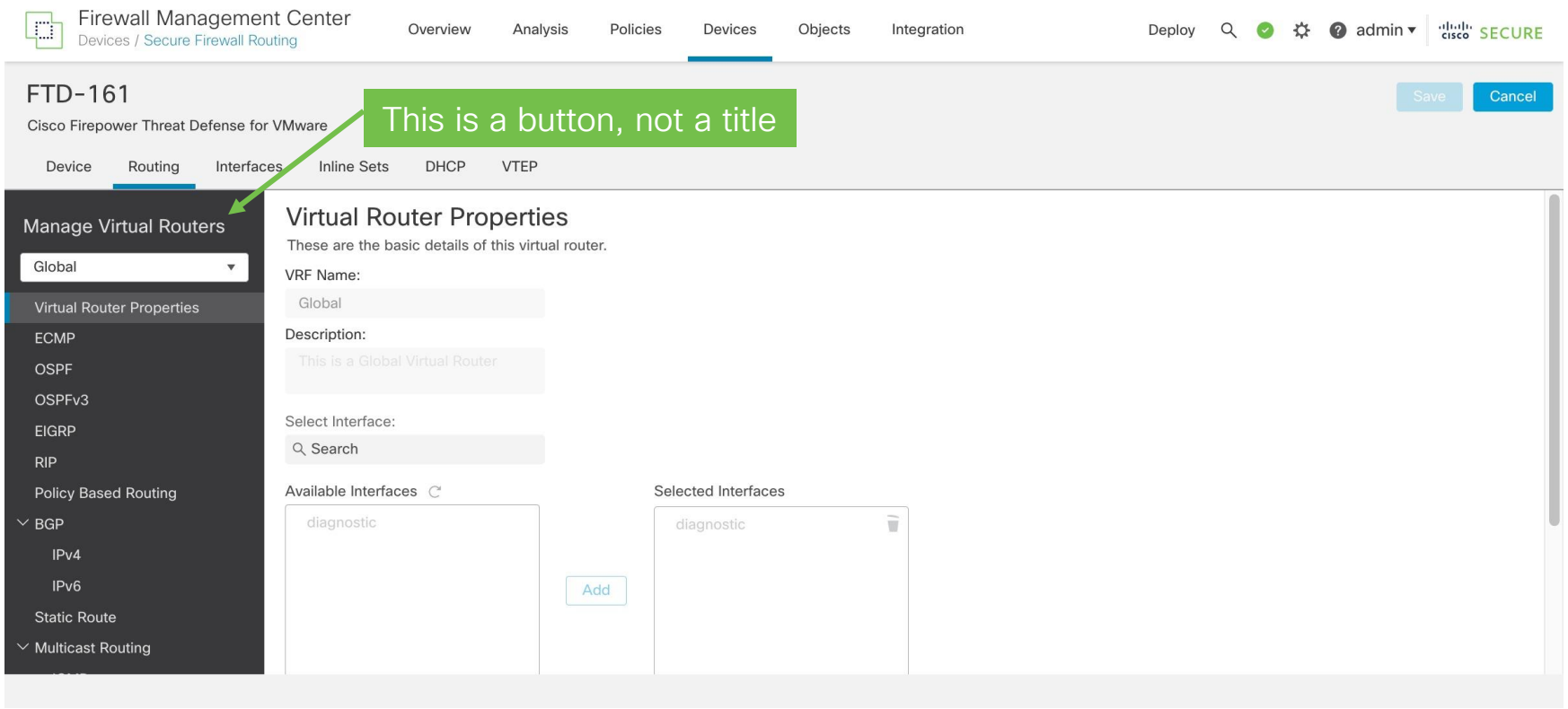
1. Run CLI to enable FMC as MI manager and Register 3100 Series (MI mode) device in FMC.
2. Update Physical Interface(s)
3. Create Secure Firewall instance(s) and assign interface(s)
4. Create/Update/Delete Port channel and subinterfaces from FMC
5. Configure platform settings
6. Deploy configuration changes to device
7. Secure Firewall instance(s) auto registers to FMC.



Limitations

- Secure Firewall is the only application to support Multi-Instance (no ASA)
- Mixing Native and Multi-Instance on the same 3100 Series chassis is not supported
- Native Secure Firewall applications cannot be converted or migrated into Multi-Instance Secure Firewall applications or vice versa
- The Secure Firewall applications will have to be reinstalled, with all configuration lost, to switch between the two modes
- Clustering, HW Crypto, Flow offload/redirect is not supported in the initial release
- All assigned resources are dedicated to an instance. Oversubscription is not supported.

Virtual Routing and Forwarding



Virtual Routing and Forwarding

Firewall Management Center
Devices / Secure Firewall Routing

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

FTD-161

Cisco Firepower Threat Defense for VMware

Save | Cancel

Device | Routing | Interfaces | Inline Sets | DHCP | VTEP

Manage Virtual Routers

Select

Virtual Routers

Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) network routers that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices.

Total Virtual Router Configured : (3)

Search Virtual Router or Interface

+ Add Virtual Route

Virtual Router	Interfaces	Show/TroubleShoot
Global	diagnostic	>_ Routes >_ IPv6 Routes >_ BGP Summary >_ OSPF Summary
VRF-Blue	OUTSIDE, INSIDE	>_ Routes >_ IPv6 Routes >_ BGP Summary >_ OSPF Summary
VRF-Red		>_ Routes >_ IPv6 Routes >_ BGP Summary >_ OSPF Summary

Virtual Routing and Forwarding

Firewall Management Center
Devices / Secure Firewall Routing

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

FTD-161
Cisco Firepower Threat Defense for VMware

Save | Cancel

Device | Routing | Interfaces | Inline Sets | DHCP | VTEP

This is a button, not a title

Manage Virtual Routers
VRF-Blue
- Virtual Router Properties
- ECMP
- OSPF
- BGP
  - IPv4
  - IPv6
- Static Route

General Settings
- BGP

Virtual Router Properties
These are the basic details of this virtual router.

VRF Name: VRF-Blue

Description:

Select Interface: Search

Available Interfaces: OUTSIDE, INSIDE

Add

Selected Interfaces: OUTSIDE, INSIDE

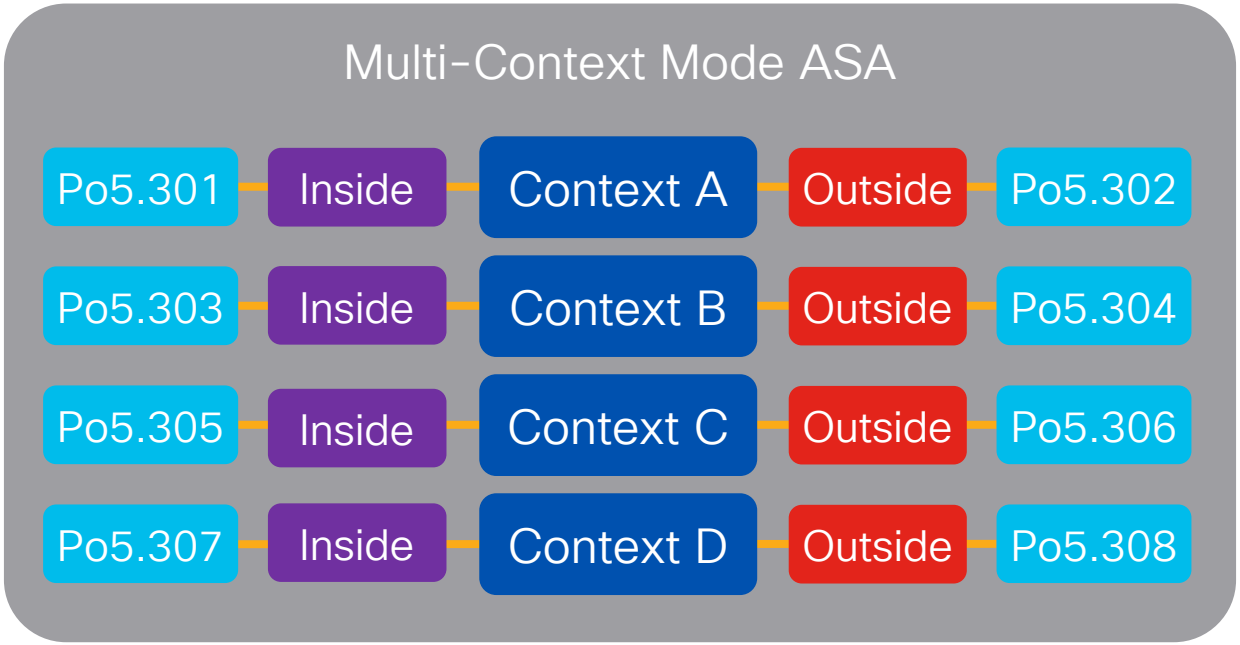
EIGRP, ISIS and PBR are not shown but are supported through Flex Config for VRF

Assign VRF interfaces to zones and use those zones as the source/destination in Access Control, IPS, SSL and Identity policies make those policies VRF aware.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - Egress Access Control Policy (1-2)					
1	Allow DNS	VRF-Blue-Inside VRF-Blue-Outside	VRF-Blue-Inside VRF-Blue-Outside	DMZ-DNS-Servers	208.67.222.222 208.67.220.220
2	Allow HTTP	VRF-Blue-Inside	VRF-Blue-Outside	Any	Any

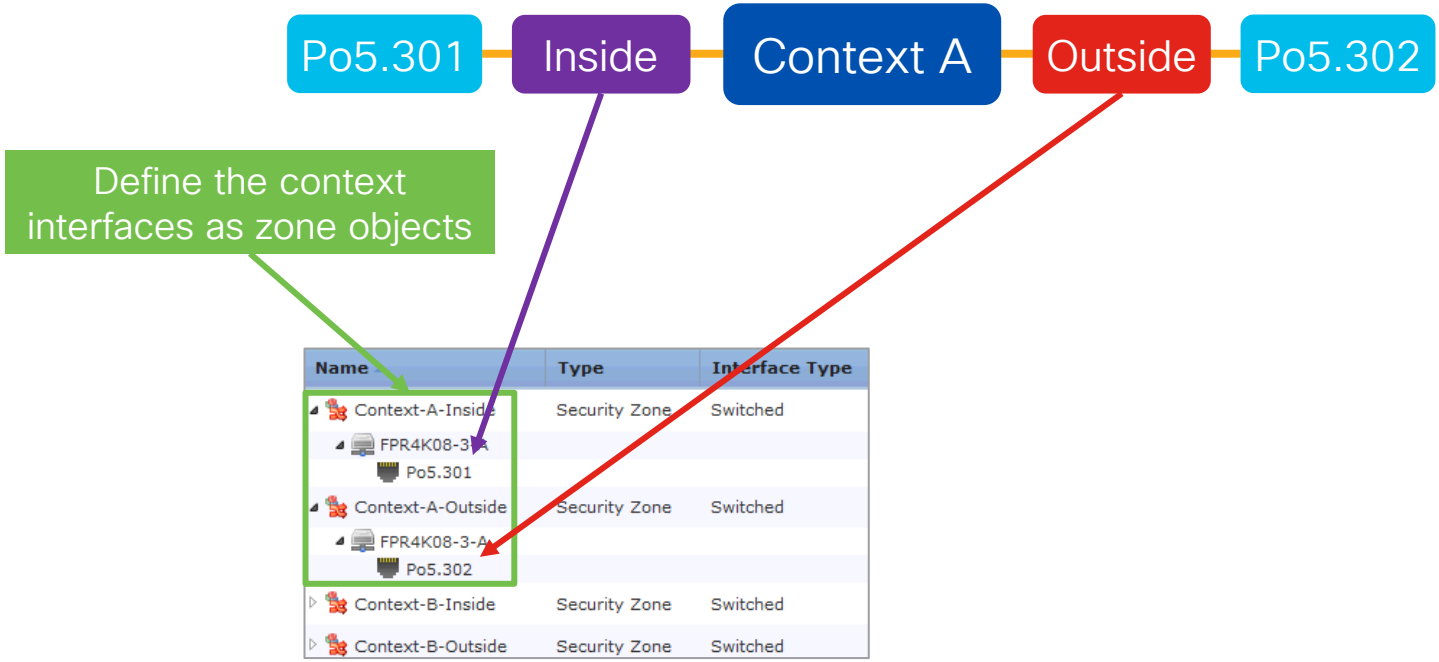
Zones and Categories for Policy Management

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

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

Name		
Context-A-Inside	Security Zone	Switched
FPR4K08-3-A		
Po5.301		
Context-A-Outside	Security Zone	Switched
FPR4K08-3-A		
Po5.302		
Context-B-Inside	Security Zone	Switched
Context-B-Outside	Security Zone	Switched

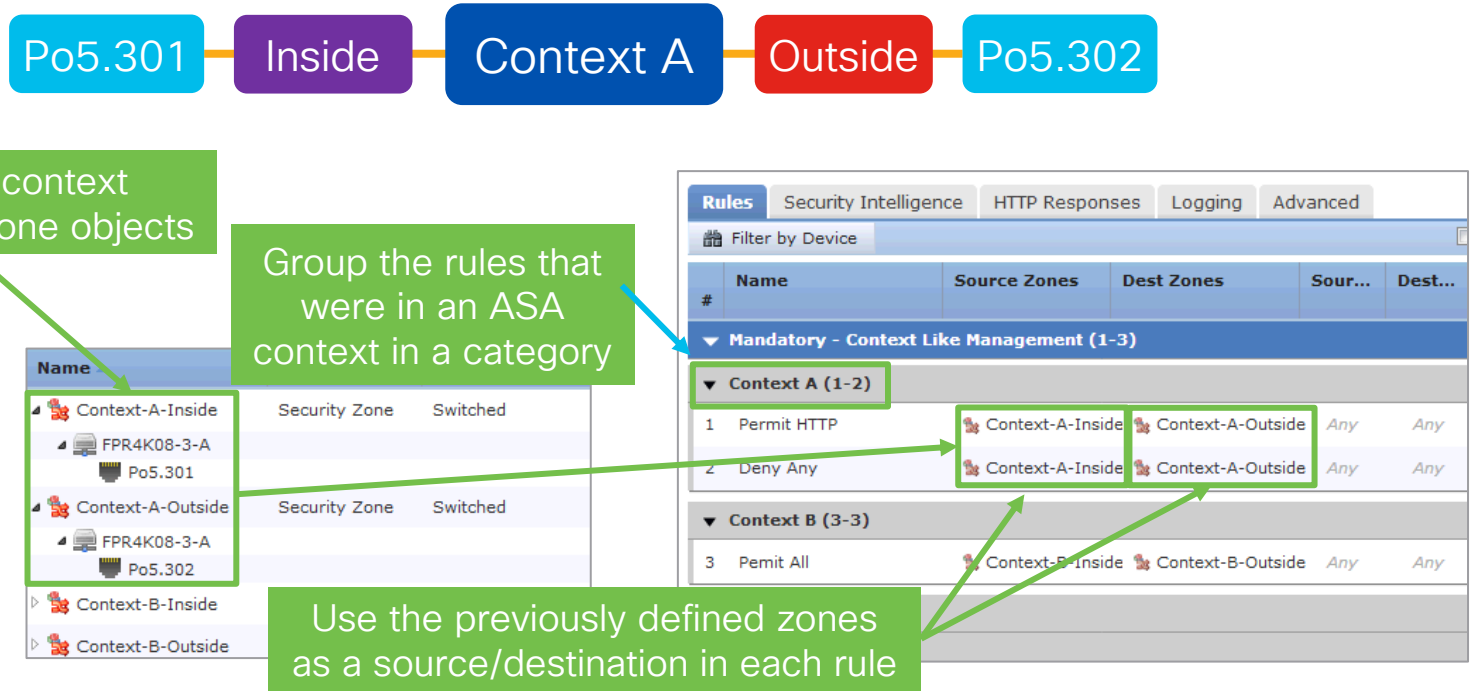
Rules | Security Intelligence | HTTP Responses | Logging | Advanced

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	Pemit 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



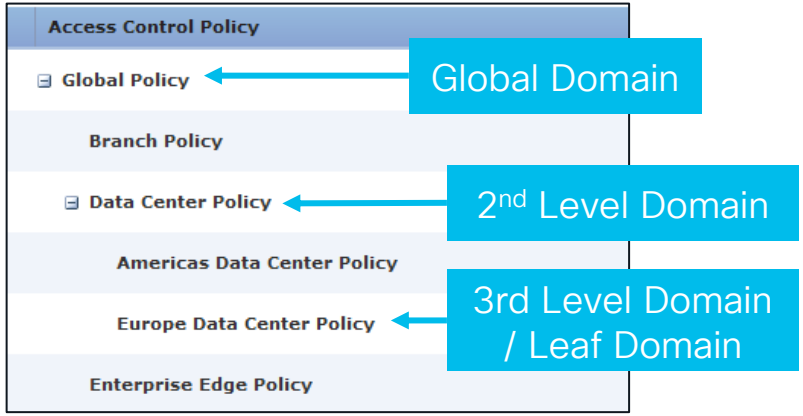
Phasing Out FlexConfig

Firewall Management Center GUI Support (FlexConfig depricated)	7.1	7.2	7.3	7.4
ECMP Zones	✓	✓	✓	✓
EIGRP, VXLAN Interfaces (VTEP/VNI)	-	✓	✓	✓
BFD for BGP, Cluster Health Settings, PBR Next-Hop Settings	-	-	✓	✓
FlexConfig Easy Migration to FMC for ECMP, EIGRP and VxLAN	-	-	✓	✓
NSEL (NetFlow Secure Event Logging)	-	-	-	✓

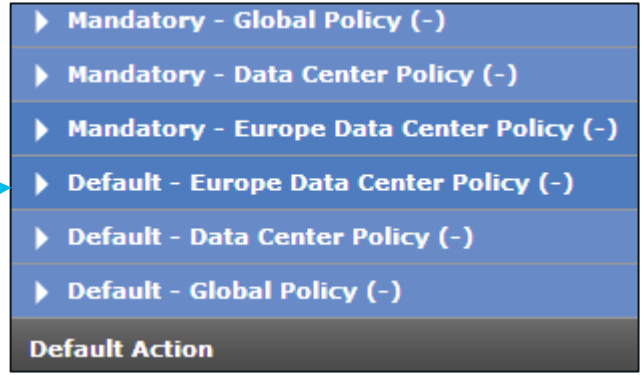
Access Control Policy Tips

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

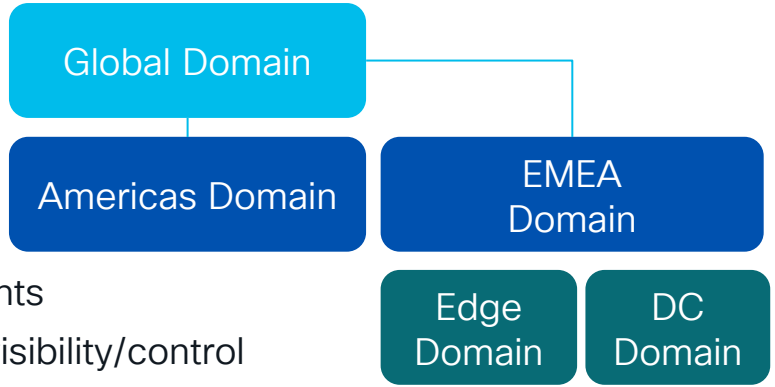


Example of what the Europe Data Center Policy will look like in the Access Control Policy Editor



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
  - Primarily for MSPs



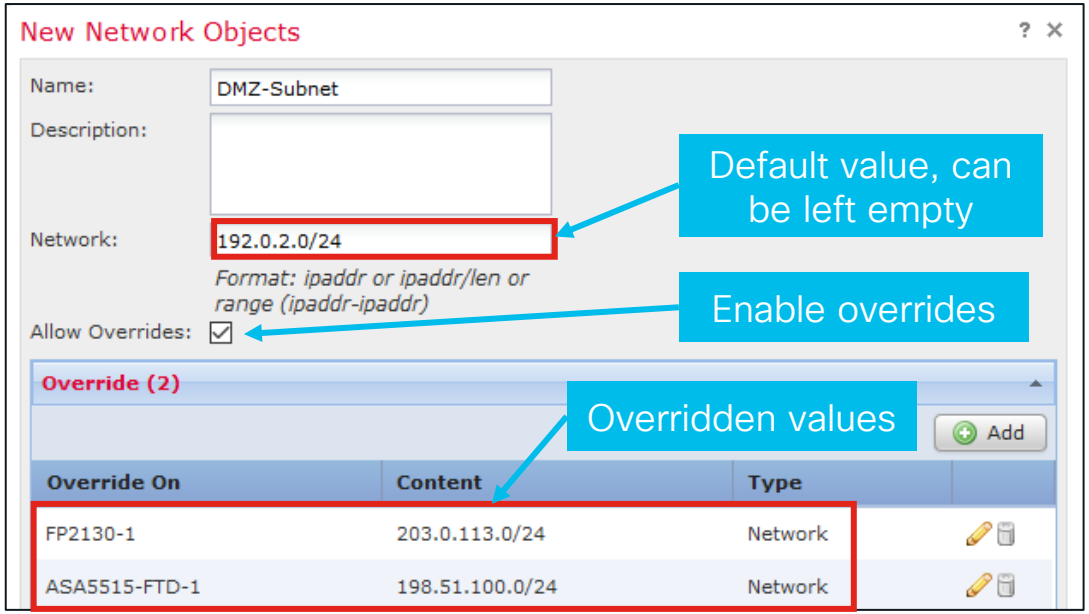
- Uses in the Enterprise:
  - Force a policy to apply to all firewalls in a domain
  - Limit user visibility to only select devices and events
  - Delegate admin control while maintaining global visibility/control

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



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 1000/21000

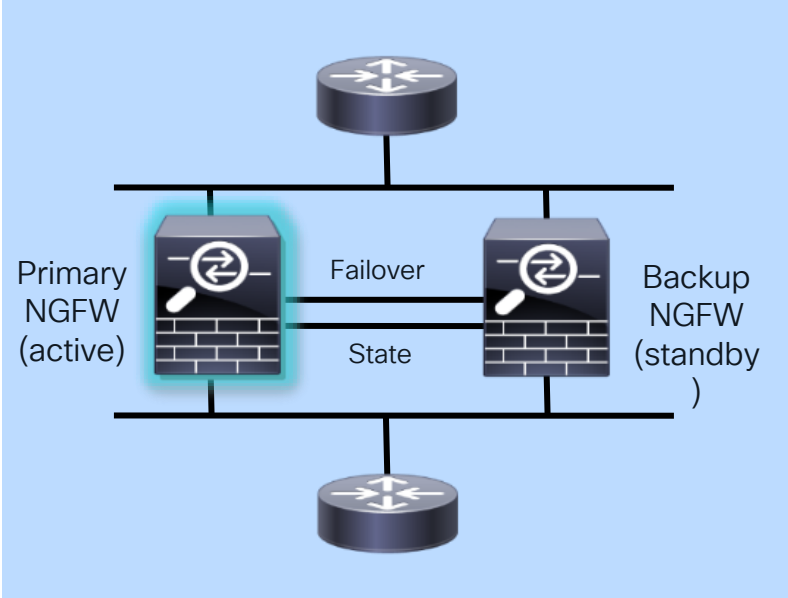
**length of flow only matters on 3100/4100/4200/9300

HA and Clustering

Secure Firewall High Availability

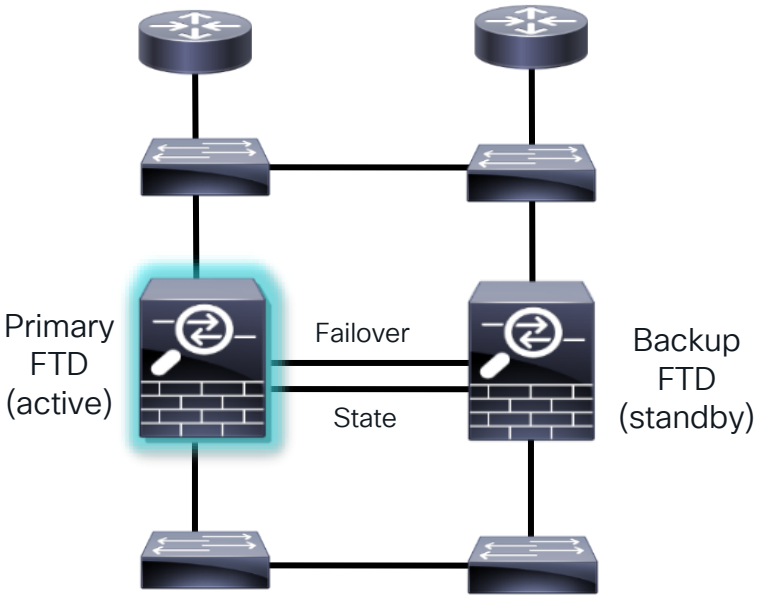
- Two nodes connected by one or two dedicated connections called “failover links”
  - Failover and state
  - Can use the same link for both
  - Best practice is to use a dedicated link for each if possible (cross-over or VLAN)

- 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

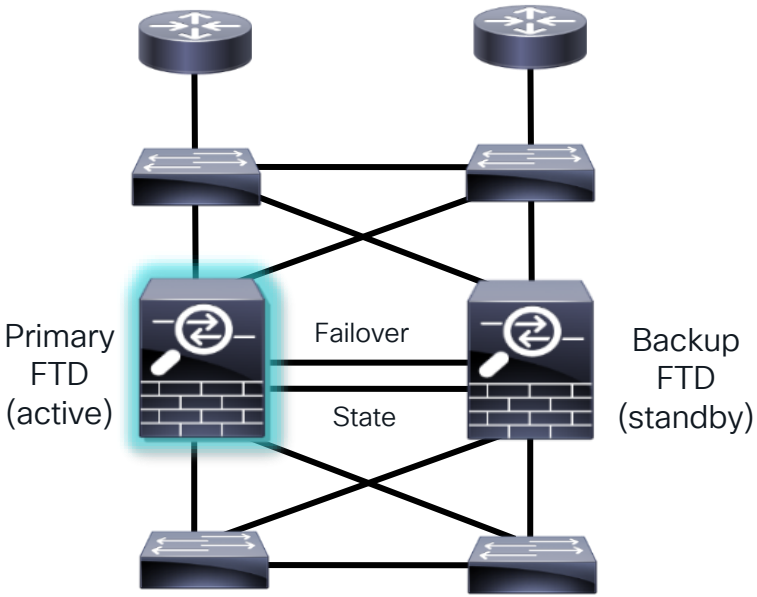


HA with Interface Redundancy

Before…

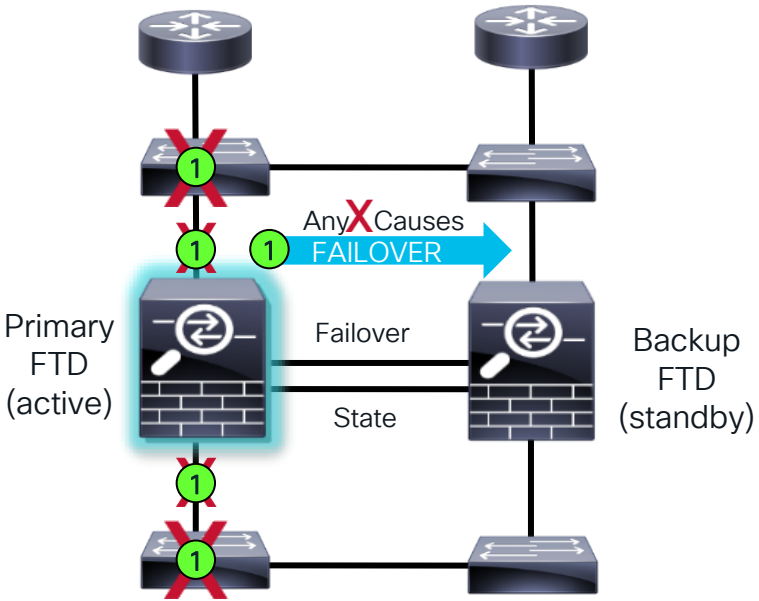


After with redundant interfaces

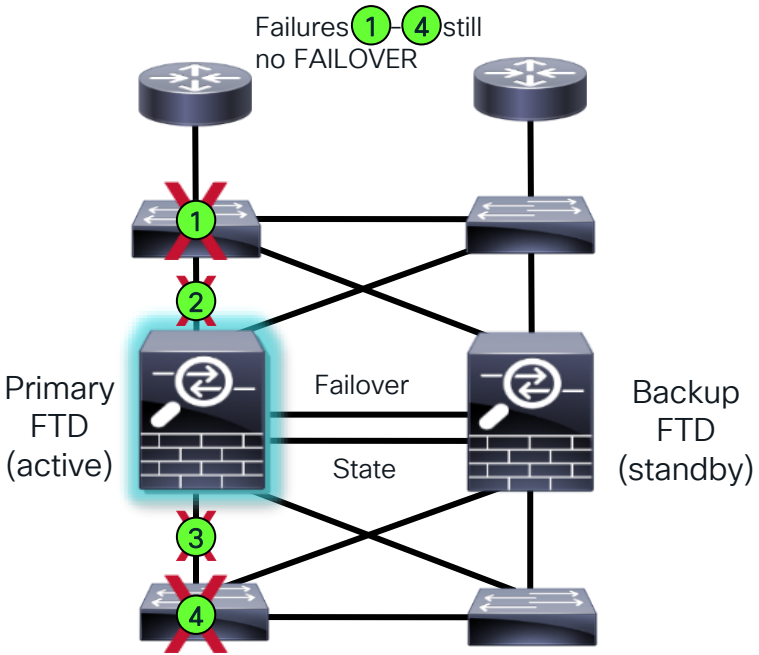


HA with Interface Redundancy

Before…

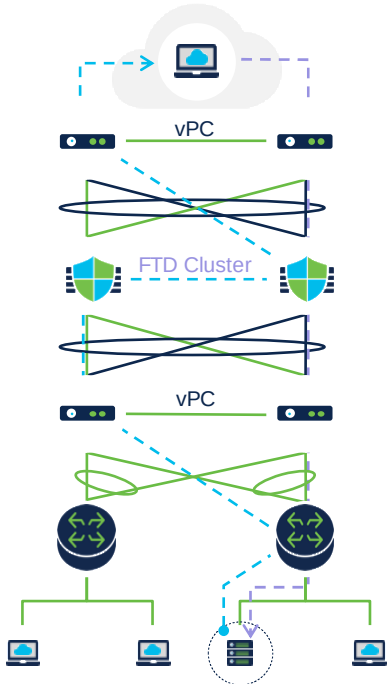


After with redundant interfaces



Clustering Concepts – Physical and Virtual

- Cluster roles
  - Control Node – synchronizes cluster configuration
  - Flow Director (deterministic) – keeps track of owner
  - Flow Owner (nondeterministic) – receiver of first packet of flow
- Cluster Control Link (CCL)
  - Internode communication
  - Asymmetric traffic redirection to flow owner
- State sharing
  - Cluster nodes share connection state
    - Each connection state is stored on two nodes
  - Cluster nodes do not share IPS state

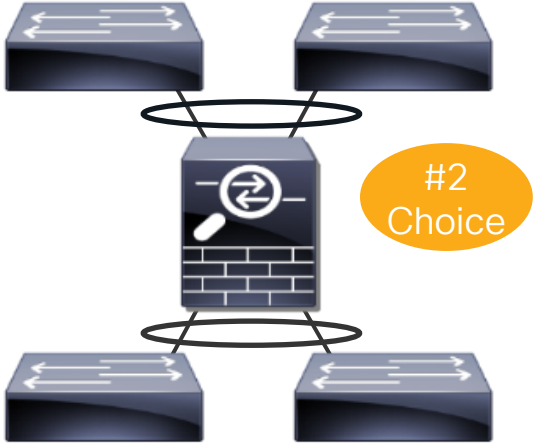


Data Center - Cluster Connectivity Preferences

Firewall on a Stick

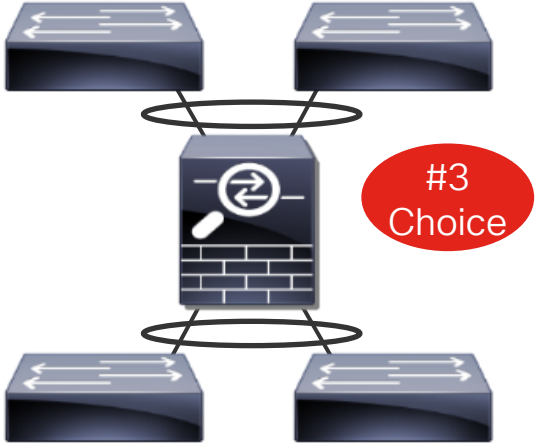
- Single EtherChannel for the inside and outside

Same Model Switches



- Two EtherChannels to different switch pairs
- Same model switch

Different Model Switches



- Two EtherChannels to different switch pairs
- Different model switches

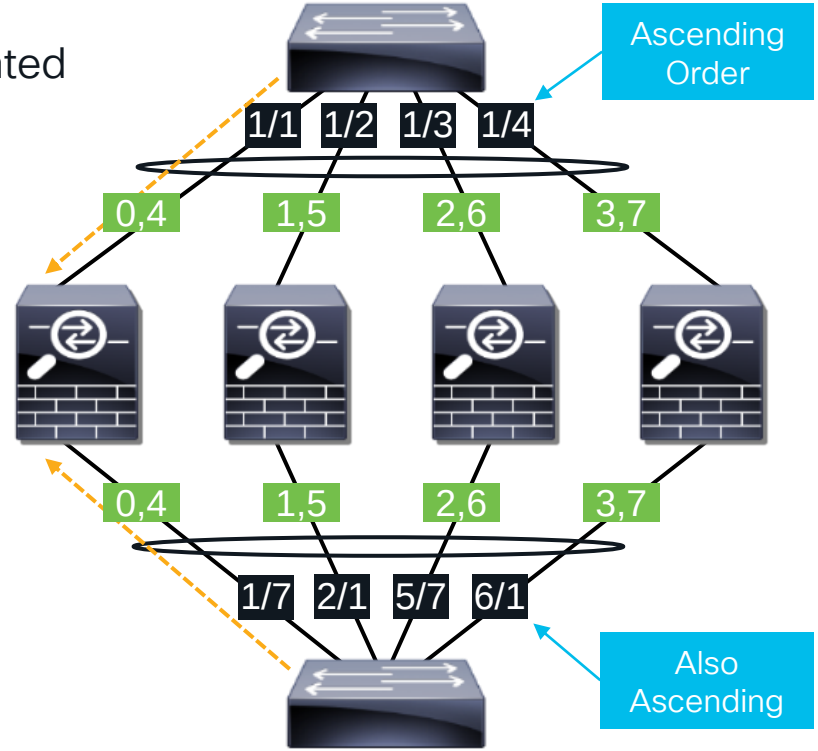
Data Center - Using 2 Different Switches

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`
- Links should be connected in matching ascending order on each switch



Set Cluster Control Link (CCL) MTU

Avoids fragmentation after encapsulation on CCL

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Pla

FPR4K

Cisco Firepower 4110 Threat Defense

Save Cancel

Cluster Device Routing Interfaces Inline

Sync Device Add Interfaces

Status	Interface	Log	IP Address
	Ethernet1/7	diag	
	Port-channel3		
	Port-channel3.30	OUT	30.0.0.2/16(Static)
	Port-channel4		
	Port-channel4.10	INS	10.0.0.2/16(Static)
	Port-channel48		

1-6 of 6 interfaces Page 1 of 1

Edit Ether Channel Interface

Mode: None

Name: Enabled Management Only

Security Zone:

Description: Clustering Interface

General IPv4 IPv6

MTU: 1600 (164 - 9184)

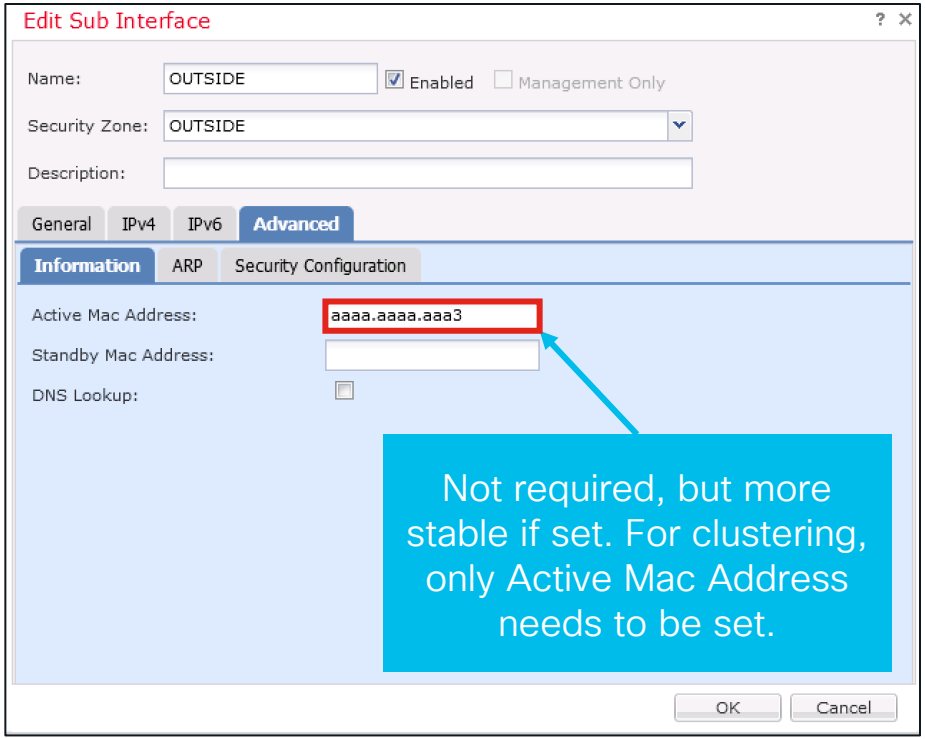
Ether Channel ID *: 48 (1 - 48)

Set MTU at 100 bytes above highest data MTU

OK Close

Pro-Tip – Set Virtual MAC Addresses

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



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.

Cisco Clustering Support

Physical Cluster

- ASA
  - 3100 (min 1 node; max 8 nodes)
  - 4100/4200 (min 1 node; max 16 nodes)
  - 9300 (min 1 node; max 16 nodes)
- FTD
  - 3100 (min 1 node; max 8 nodes)
  - 4100/4200 (min 1 node; max 16 nodes)
  - 9300 (min 1 node; max 16 nodes)

Virtual Cluster

- ASAv
  - Already released (9.17.1)
  - Private cloud (VMware and KVM)
- FTDv
  - FMC managed nodes, running 7.2
    - Private cloud (VMware and KVM)
    - Public cloud (AWS and GCP)
  - Minimum 1 node; maximum 16 nodes
  - All nodes require 5 interfaces (with CCL)
    - AWS cluster behind GWLB can have 4 interfaces

Use 90 day FMC trial to license FMC and FTDv appliances and learn/experiment with clustering for free.

Porting Cisco Clustering to the Public Cloud

Physical Cluster

- Data interfaces have two modes
  - Individual interface mode (different IP addresses on different nodes)
  - Spanned interface mode (uses EtherChannel)
- CCL uses proprietary protocol over IP (no transport layer protocol)
- CCL uses broadcast for internode communication
  - Dynamic node discovery

Virtual Cluster

- Data interfaces on each node use different IP addresses
- CCL uses VXLAN over UDP
- CCL uses unicast
  - Cluster requires static peer list

Cluster Configuration

Physical Cluster

- Cluster configuration and management requires two steps
  - Cluster bootstrapping with Chassis Manager (of FXOS)
  - Registering a cluster node to FMC
    - Other cluster nodes are discovered
    - FMC automatically register remaining nodes*
    - FMC provides remaining configuration

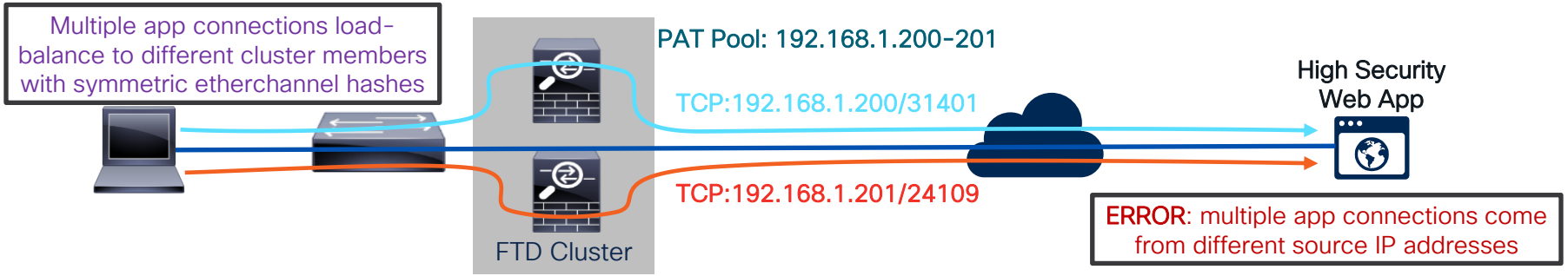
Virtual Cluster

- AWS and GCP
  - Cluster bootstrapping with day0 config
  - Registering a cluster node to FMC
    - Other cluster nodes are discovered
    - FMC automatically registers remaining nodes*
    - FMC provides remaining configuration
- VMware and KVM
  - FMC performs all cluster configuration

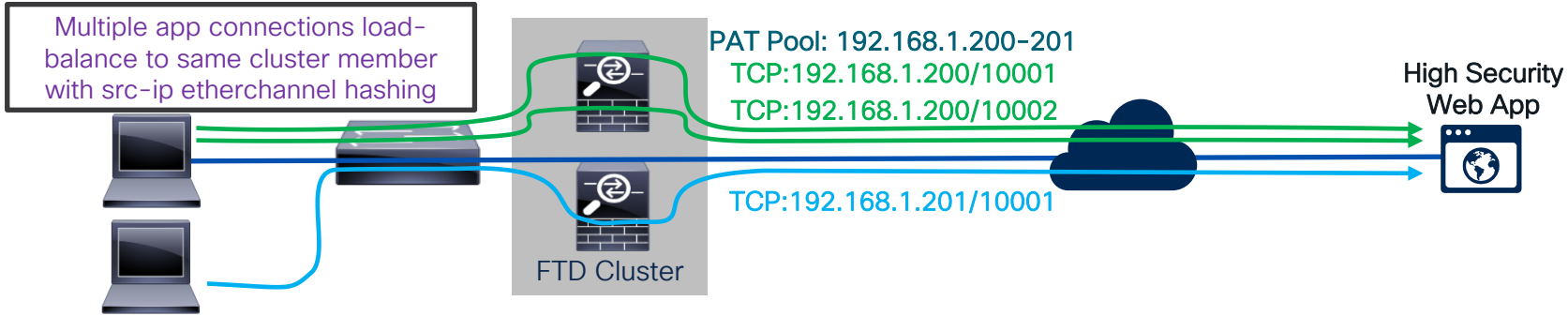
* This process is known as **Auto-Registration**

PAT in Clustering for Internet Egress (6.6 or Lower)

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

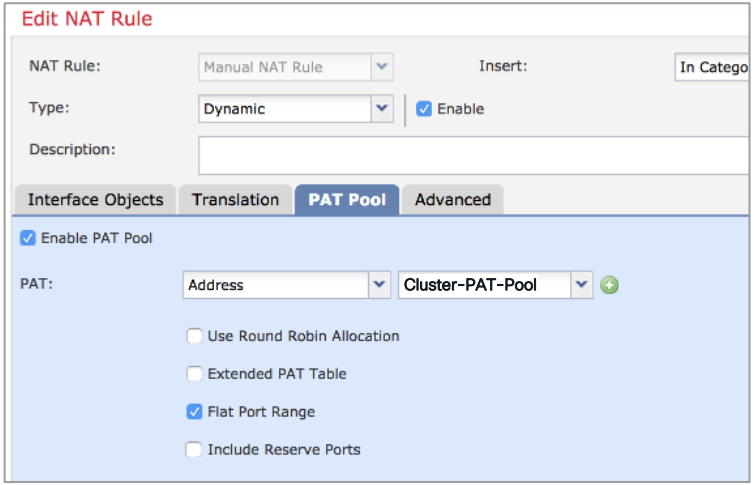


Use src-ip hashing on client side switch to keep NAT IPs consistent



PAT with Cluster Best Practices (6.6 or Lower)

- 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)



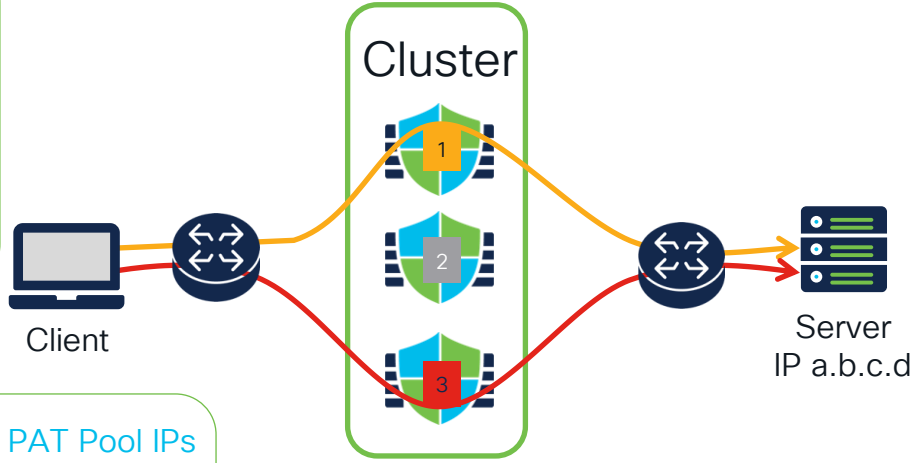
Original Src Port	Translated Src Port	Translated Src Port (flat)
1-511	1-511	1024-65535
512-1023	512-1023	1024-65535
1024-65535	1024-65535	1024-65535

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

NAT Details: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/network_address_translation__nat__for_firepower_threat_defense.html

Cluster PAT Pool Improvements

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



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

a.b.c.d port x
a.b.c.d port y

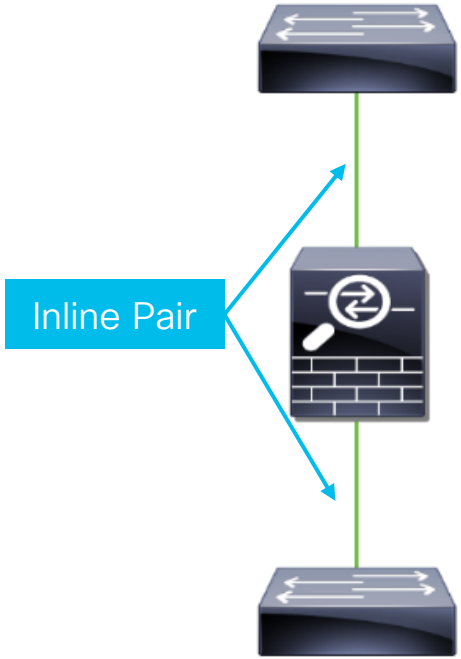
Alternative Designs

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:

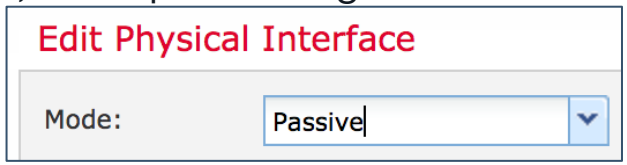
- Caveats:
  - No NAT / No Routing
  - No strict TCP state tracking



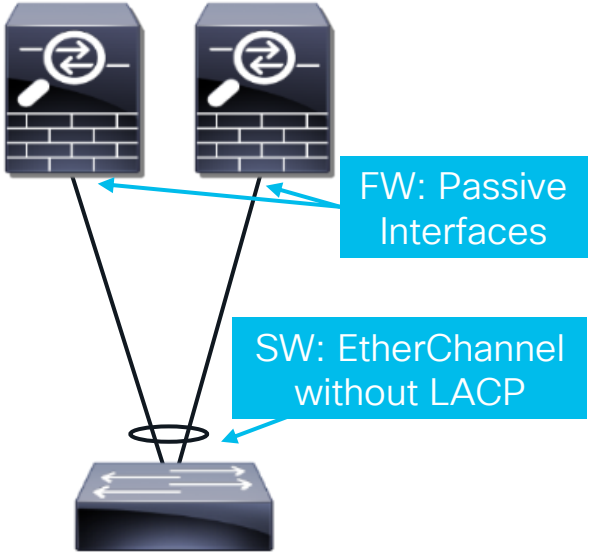
Out-of-Band IDS - Multichassis SPAN

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:



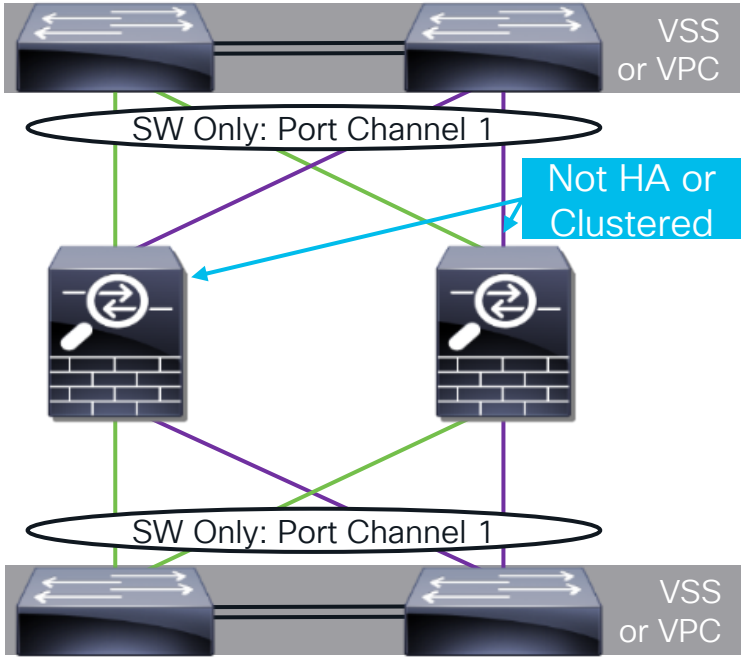
- EtherChannel load balancing distributes traffic to different Firepower chassis



Inline IPS – Passthrough EtherChannel w/o HA

LACP EtherChannel through FTD

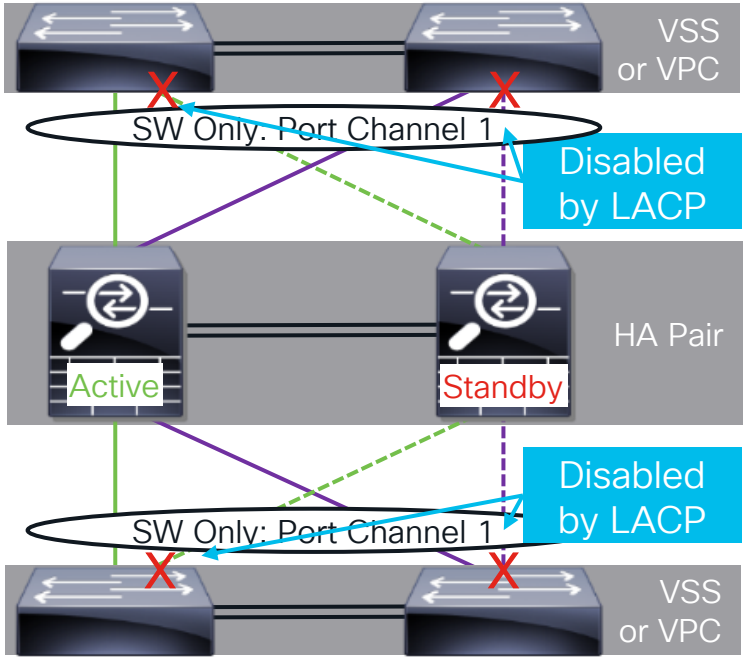
- Useful for scaling IPS without Clustering or scaling IPS with total fault isolation
- LACP EtherChannel formed between switches on either side of FTD
  - FTD has no knowledge of EtherChannel
  - Interfaces configured as Inline Pair on FW
- Each FTD appliance configured as standalone device in FMC
- 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

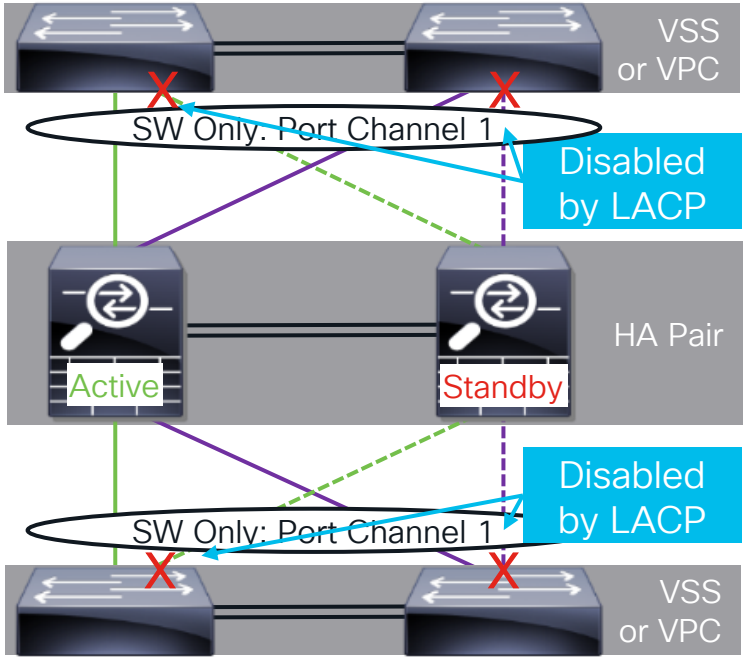
- Useful for IPS HA without Clustering
- Same interface configuration as Passthrough EtherChannel w/o HA
  - Traffic is automatically symmetric through FTD, since only 1 unit is ever active
- Inline pair interfaces on Standby HA unit are forced down when not active
- On failure of Active unit, LACP on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



Inline IPS – Passthrough EtherChannel w/ HA

LACP EtherChannel through FTD w/o Symmetric Traffic

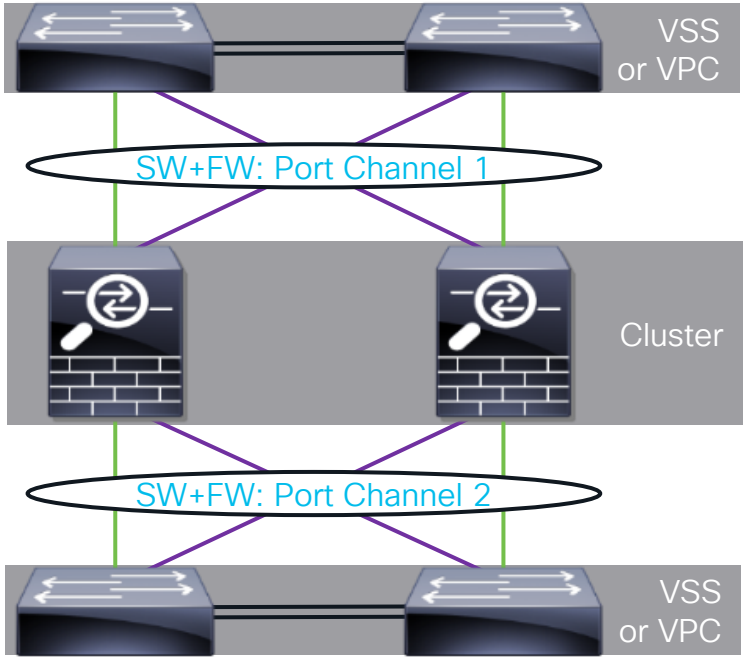
- Useful for IPS HA without Clustering
- Same interface configuration as Passthrough EtherChannel w/o HA
  - Traffic is automatically symmetric through FTD, since only 1 unit is ever active
- Inline pair interfaces on Standby HA unit are forced down when not active
- On failure of Active unit, LACP on 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 – 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 PC1and PC2 configured in FXOS FCM
- PC1 and PC2 configured as Inline Pair within FMC



Dynamic Objects

Dynamic Objects

Without Dynamic Objects:

API Change to FMC Object → Policy Push from FMC to FTD → Object Changed on FTD

With Dynamic Objects:

API Change to FMC Object → Object Changed on FTD

Dynamic Objects REST API

Connect to your FMC at ”https://<FMC IP>/api/api-explorer” to browse the REST API documentations

GET	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects**	Retrieves the list of all Dynamic Objects or creates a new Dynamic Object.
POST	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects**	
GET	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}**	Retrieves, deletes or modifies an existing Dynamic Object with the specified ID.
PUT	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}**	
DELETE	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}**	
GET	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}/mappings**	Retrieves, adds or removes IP addresses mapped to an existing Dynamic Object with the specified ID.
PUT	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}/mappings**	
POST	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjectmappings**	Adds or removes IP addresses mapped to existing Dynamic Objects in bulk.

Updating Dynamic Object with REST API

Environment Variables:

X-auth-access-token =
c830333c-614e-44a7-b6ca-dca7b8be605d

Domain UUID =
e276abec-e0f2-11e3-8169-6d9ed49b625f

Workload_A Object ID =
005056AF-6E04-0ed3-0000-021474843199

POST /api/fmc_platform/v1/auth/**generatetoken**

HEADER Authorization : Basic cnWzdFAcdDovcW86RFfTMU==

Status: 204

HEADER X-auth-access-token : c8303…605d
Domain_UUID : e276abec…b625f

GET /api/fmc_platform/v1/domain/e276abec…b625f/object/**dynamicobject**

HEADER X-auth-access-token : c830333c-614e-44a7-b6ca-dca7b8be605d

Status: 200

BODY

```
[…]
"id": "005056AF…199",
"name": "Workload_A",
"type": "DynamicObject",
[…]
```

POST /api/fmc_platform/v1/domain/e276abec…b625f/object/**dynamicobjectmappings**

HEADER X-auth-access-token : c830333c-614e-44a7-b6ca-dca7b8be605d

BODY

```
{
    "add": [
        {
          "mappings": [
             "172.16.11.100"
             ],
             "dynamicObject": {
                    "id": "005056AF-6E04-0ed3-0000-021474843199"

             }
        }
    ]
}
```

Status: 201

FMC

Dynamic Object	Content:
Workload_A:	172.16.11.100

Dynamic Objects API Demo

Demo Setup

Create Dynamic Object (Can Also Be Done via API)

Firewall Management Center
Objects / Object Management

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

- AAA Server
- Access List
- Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- Distinguished Name
- DNS Server Group
- External Attributes
  - Dynamic Object
  - Security Group Tag
- File List
- FlexConfig
- Geolocation
- Interface
- Key Chain
- Network

Dynamic Objects

Filter

Name	Description	Number of Mapped IPs
API_Example		0

Viewing 1-1 of 1

Edit Dynamic Object

Name
API_Example

Description

Type
IP

Cancel | Save

Demo Setup

Apply Dynamic Object to Access Control Policy

Firewall Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Devices | Objects | Integration

Deploy | admin | SECURE

Dynamic Object De
Enter Description

Rules | Security Intelligence

Filter by Device | Search Rules

| Name | Source Zones

Mandatory - Dynamic Object Demo
1 Allow All To Dyna Any
Default - Dynamic Object Demo (-)
There are no rules in this section. Add

Default Action

1 Row Selected

Hit Counts | Save | Cancel

ance Settings | Policy Assignments (1)
cy: None | Identity Policy: None

+ Add Category | + Add Rule

ll traffic

Rules per page: 100

Editing Rule - Allow All To Dynamic Object

Name: Allow All To Dynamic Object
Enabled
Move

Action: Allow

Time Range: None

Zones | Networks | VLAN Tags | Users | Applications | Ports | URLs | Dynamic Attributes | Inspection | Logging | Comments

Available Attributes
Search by name or value
Dynamic Objects
API_Example

Add to Source
Add to Destination

Selected Source Attributes (0)
any

Selected Destination Attributes (1)
Dynamic Objects
API_Example

Attributes of the same type (for example, SGT) match the rule if any attribute is matched.
Attributes of different types match the rule only if all attributes are matched. More info

Cancel | Save

Postman

Home | Workspaces | Reports | Explore | Search Postman | Sign In | Sign Up for Free

POST Generate To... | GET GET Dynamic ... | POST Add Dynamic... | GET GET Dynamic ... | POST Remove Dyn...

Cisco Live 2022

Cisco Live 2022 / **Generate Token**

Save

POST https://100.100.1.160/api/fmc_platform/v1/auth/generatetoken Send

Params | Authorization | Headers (8) | Body | Pre-request Script | Tests | Settings | Cookies

Type: Basic Auth

The authorization header will be automatically generated when you send the request.
Learn more about authorization ↗

Username: admin

Password: ••••••••••

Show Password

Response

Click Send to get a response

Find and Replace | Console | Runner | Trash

FOXTROT-166-WIN

Administrator: Command Prompt - ping 8.8.8.8 -t -w 100

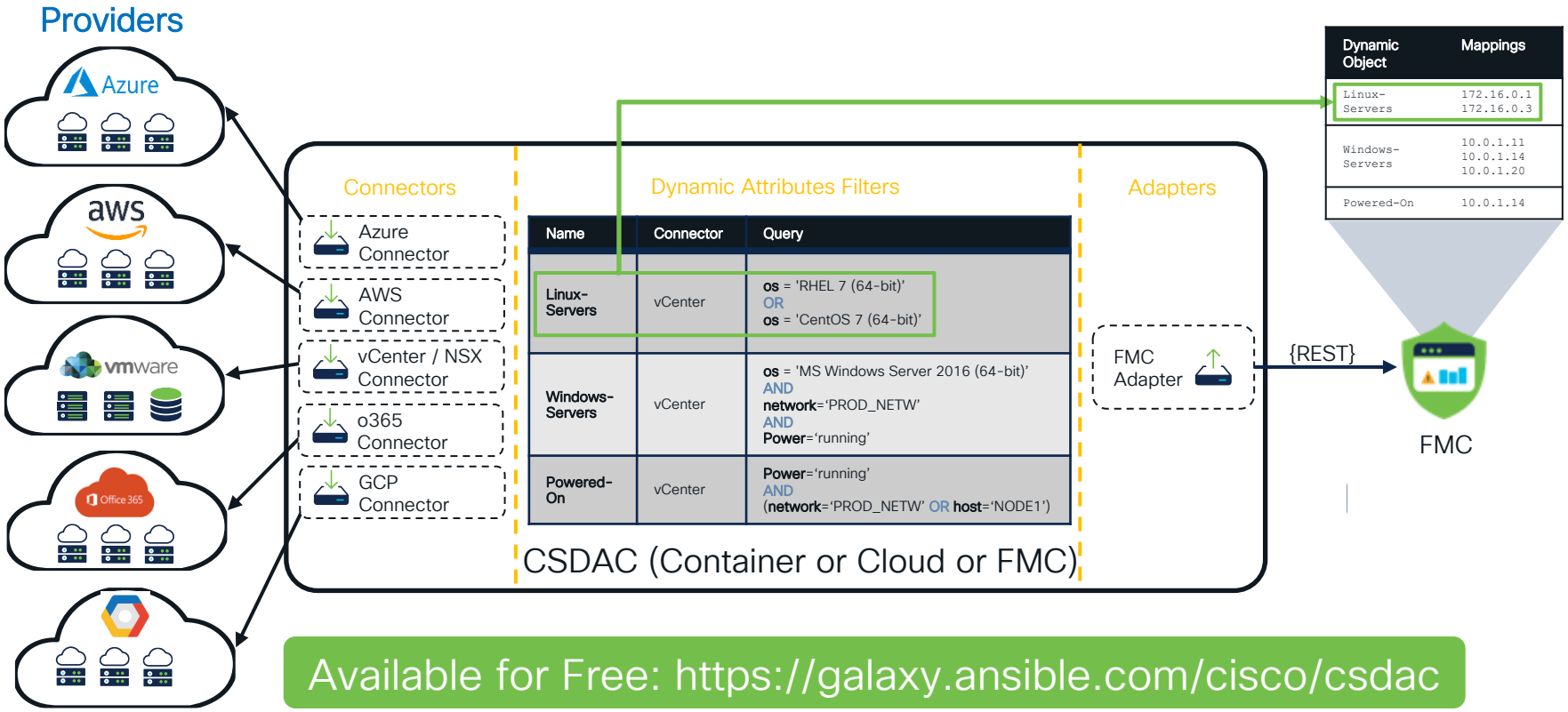
```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Options for Implementing Dynamic Attributes

Admin Handled / System Handled or Assisted

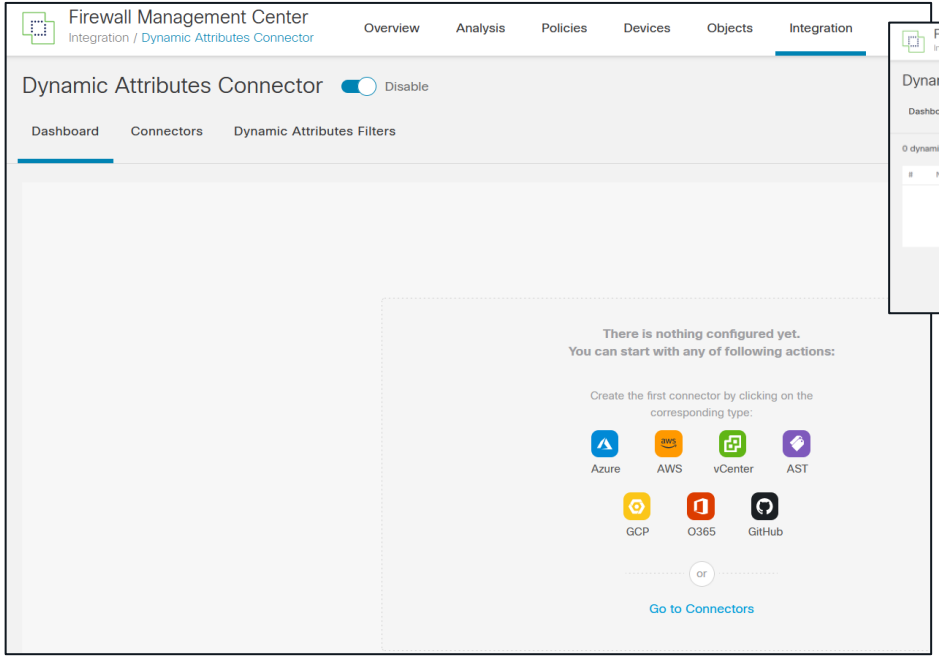
Dynamic Attribute FMC API	Cisco Secure Dynamic Attribute Connector (CSDAC)	Cisco Secure Workload
Define Policy	Define Policy	Define Policy
Define Dynamic Objects	Define Dynamic Objects	Define Dynamic Objects
Interact w/ Upstream API(s)	Interact w/ Upstream API(s)	Interact w/ Upstream API(s)
Interact w/ FMC API	Interact w/ FMC API	Interact w/ FMC API

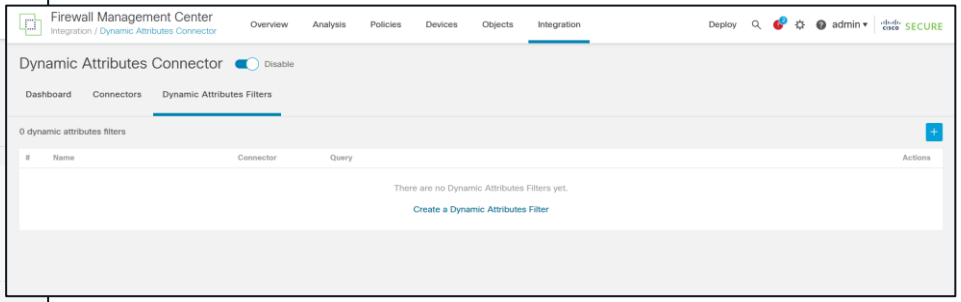
Cisco Secure Dynamic Attributes Connector



Available for Free: https://galaxy.ansible.com/cisco/csdac

CSDAC in FMC



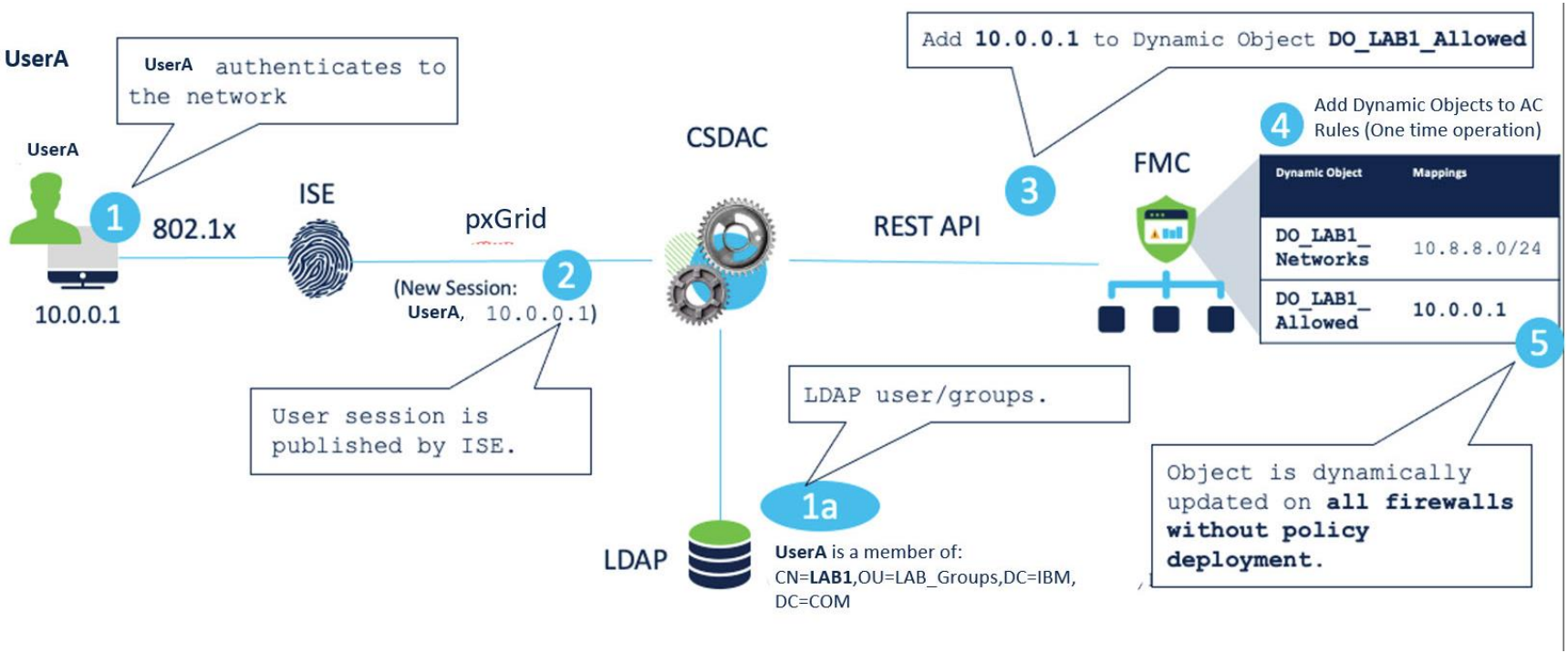


- You must configure
  - Connectors
  - Dynamic attribute filters
- You do not configure any adapters

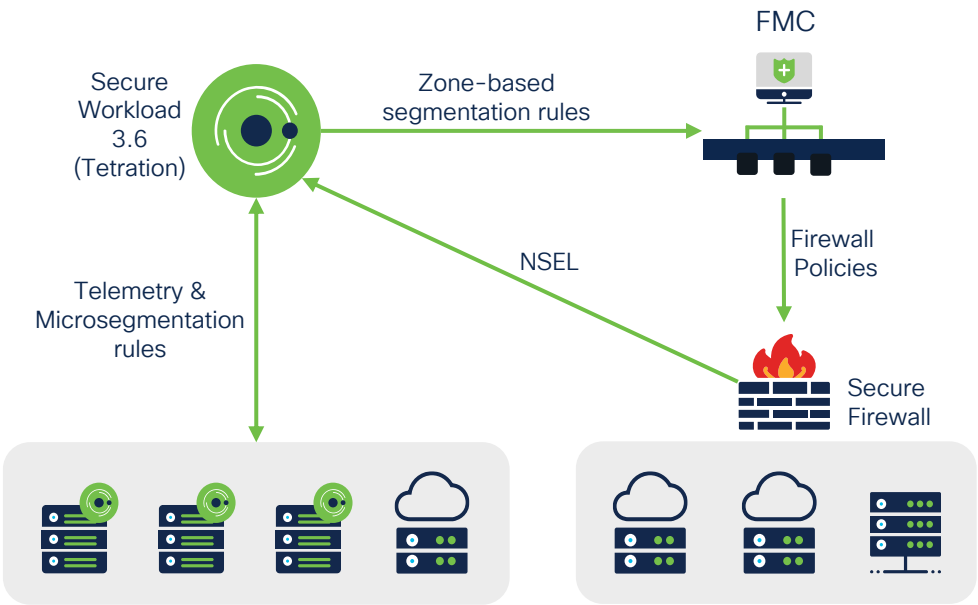
External User Identity with CSDAC

- Enables Identity Services Engine (ISE) 802.1x Authentication with Lightweight Directory Access Protocol (LDAP)
- FMC today does not support LDAP with Passive Authentication
- Three new connectors added to CSDAC
  - ISE Connector – creates IP-to-user mapping
  - LDAP Connector – creates user-to-groups mapping
  - Decorator – creates IP-user/groups mapping

External User Identity with CSDAC



Secure Workload Dynamic Policy Integration



Secure Workload and Secure Firewall integration walkthrough:
https://www.youtube.com/watch?v=xpbg3s0vrcl

Integrate with FMC

Create the FMC external orchestrator in Secure Workload

Create Segmentation Policies

- Define scopes, filters and clusters.
- Define consumers and providers.

Push Dynamic Policies

Segmentation Policy pushed to FMC as access control rules with Dynamic Objects

Monitor and Auto-Update

Secure Workload continuously checks for changes and automatically pushes updates every 5 seconds.

Secure Workload / Secure Firewall Integration

Using Dynamic Objects

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

- AAA Server
- Access List
- Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- Distinguished Name
- DNS Server Group
- External Attributes
  - Dynamic Object
  - Security Group Tag

Dynamic Objects

Add Dynamic Object | Filter

A dynamic object represents one or more attributes which can be dynamically mapped to the object.
You can use dynamic objects in access control policies.

Name	Description	Number of Mapped IPs
WorkloadObj_612e0db4497d4f69ba32dd8f	Internet	31
WorkloadObj_615acfaf755f026e6f621609	AD-DNS-Internal	1
WorkloadObj_615c76fe497d4f0d09d1b093	Default:EMEAR:DC:DC-1:Applications:Prod	6
WorkloadObj_615c8055755f020e377c5201	Default:EMEAR:DC:DC-1:Applications:Prod:Invo	
WorkloadObj_615c8409497d4f0d0ad1b0d8	Developers	
WorkloadObj_615c847b755f020e357c51b8	Contractors	
WorkloadObj_615f3ec5755f020e367c5525	db-tier-aws	
WorkloadObj_615f3f39755f020e347c5535	app-tier-aws	
WorkloadObj_615f4f00497d4f0d0cd1b41f	CVE-2020-0646-SQL	
WorkloadObj_615f58cf497d4f0d0cd1b434	IOT-Branch-Devices	

East-West Policy

Analyze Hit Counts | Save | Cancel

Inheritance Settings | Policy Assignments (1)

Rules | Security Intelligence | HTTP Responses | Logging | Advanced | Prefilter Policy: Default Prefilter Policy_1 | SSL Policy: None | Identity Policy: None

Filter by Device | Search Rules

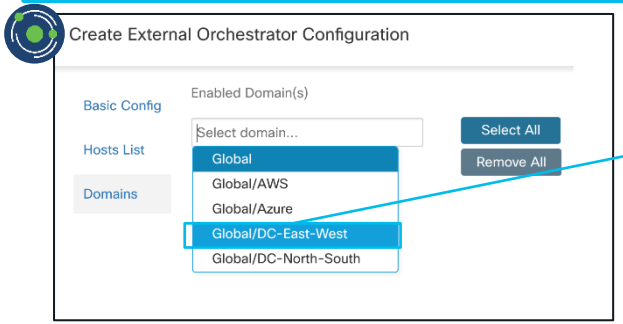
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action
4	Workload_gold	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):5660	Any	Any	WorkloadObj_	Allow
5	Workload_gold	Any	Any	Any	Any	Any	Any	Any	TCP (6):443	Any	Any	WorkloadObj_	Any	Allow
6	Workload_gold	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):443	Any	Any	WorkloadObj_	Allow
7	Workload_7	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):8080	Any	WorkloadObj_	WorkloadObj_	Block
8	Workload_8	Any	Any	Any	Any	Any	Any	Any	Any	ICMP (1)	Any	WorkloadObj_	WorkloadObj_	Block
9	Workload_9	Any	Any	Any	Any	Any	Any	Any	Any	UDP (17)	Any	WorkloadObj_	WorkloadObj_	Block
10	Workload_10	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6)	Any	WorkloadObj_	WorkloadObj_	Block
11	Workload_11	Any	Any	Any	Any	Any	Any	Any	Any	ICMP (1)	Any	WorkloadObj_	WorkloadObj_	Block
12	Workload_12	Any	Any	Any	Any	Any	Any	Any	Any	UDP (17)	Any	WorkloadObj_	WorkloadObj_	Block
13	Workload_13	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6)	Any	WorkloadObj_	WorkloadObj_	Block
14	Workload_14	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):3306	Any	WorkloadObj_	WorkloadObj_	Allow
15	Workload_15	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):22 TCP (6):80	Any	WorkloadObj_	WorkloadObj_	Allow

Secure Workload / Secure Firewall Integration

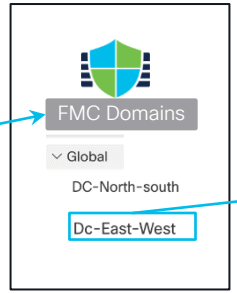
FMC Domain Selection

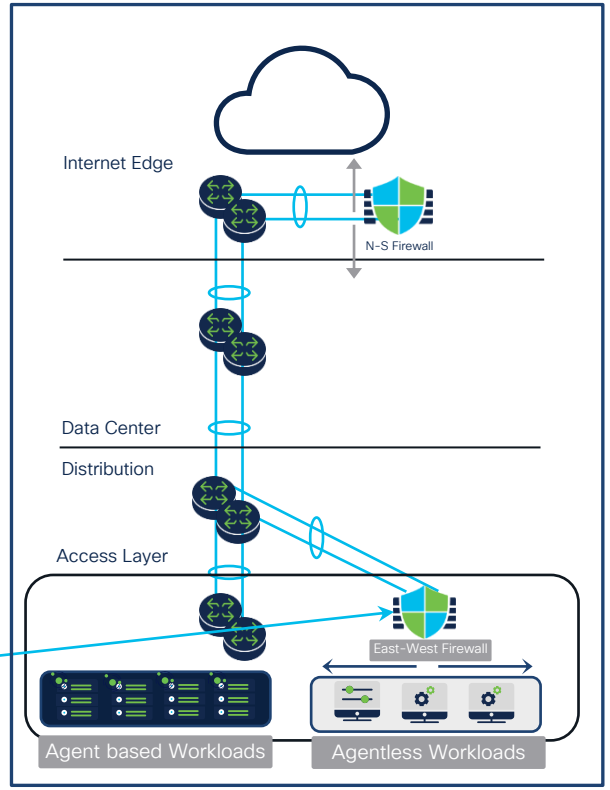
- FMC orchestrator now allows the ability to select specific FMC domains for enforcement (Starting 3.6-Patch3)
- Policies are pushed only to FTDs within the selected FMC domains.

CSW: Manage > External Orchestrator > FMC > Domains



FMC: Domains



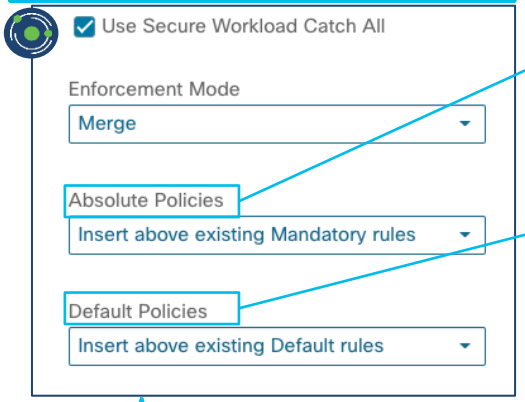


Secure Workload / Secure Firewall Integration

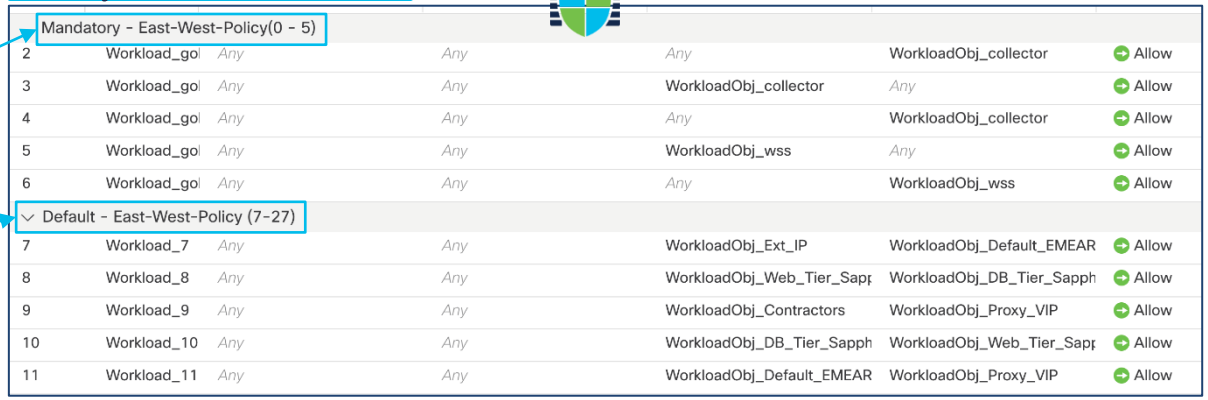
Rule Ordering

- Absolute policies from Secure Workload map to mandatory rules in FMC access control policy.
- Default policies from Secure Workload map to default rules in FMC access control policy.
- Absolute and default policies from Secure Workload can be inserted at the top or bottom of the mandatory and default rules in the FMC access control policy.

CSW UI: Manage > External Orchestrator > FMC



FMC UI: Access Control Policy



Secure Workload / Secure Firewall Integration

Better Object Naming

- Dynamic objects now have meaningful names on the Firewall Management Center.
- Simplifies the identification and mapping of the policies on Secure Workload and FMC.
- Naming Format – WorkloadObj_<CSW Inventory_filter_name>

CSW: Organize > Inventory Filters

Inventory Filters

Name *contains* **logic** Filter

Total matching filters: **2**

Name	Query	Ownership Scope
AppLogic1-WP-Cluster	✻ Service = Wordpress	...:Datacenter:Development:eCommerce-Dev
AppLogic2-OC-Cluster	✻ Service = OC	...:Datacenter:Development:eCommerce-Dev

FMC: Objects > Object Management > External Attributes > Dynamic Objects

Dynamic Objects

A dynamic object represents one or more attributes which can be dynamically mapped to the control policies.

Name	Description
WorkloadObj_3k0cD8oUvyG843sWBbmqTg	3k0cD8oUvyG843sWBbmqTg
WorkloadObj_AD_DNS	627218b2755f0229eb06f484
WorkloadObj_Administrator	6332ebc8755f02217db9eee7
WorkloadObj_AppLogic1_WP_Cluster	6332bd26497d4f1edbb54670
WorkloadObj_AppLogic2_OC_Cluster	62b37a8f497d4f622a226709
WorkloadObj_Back_End	62b37afc755f02181d51c4e0
WorkloadObj_collector	collector
WorkloadObj_Contractor_Bob	6332ec05755f0221bfba320f
WorkloadObj_Front_End	62b37ae3755f027a2e51ec81
WorkloadObj_NFS	62b37b1b497d4f622a22670c
WorkloadObj_NTP	627218db755f02214406957d
WorkloadObj_OCI_DB_Workload	6315fb9e755f0272cab9f2cf
WorkloadObj_Redis	62b37ac5497d4f75f5226614
WorkloadObj_SQL_Cluster	62b37aaf755f027a2e51ec7e

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

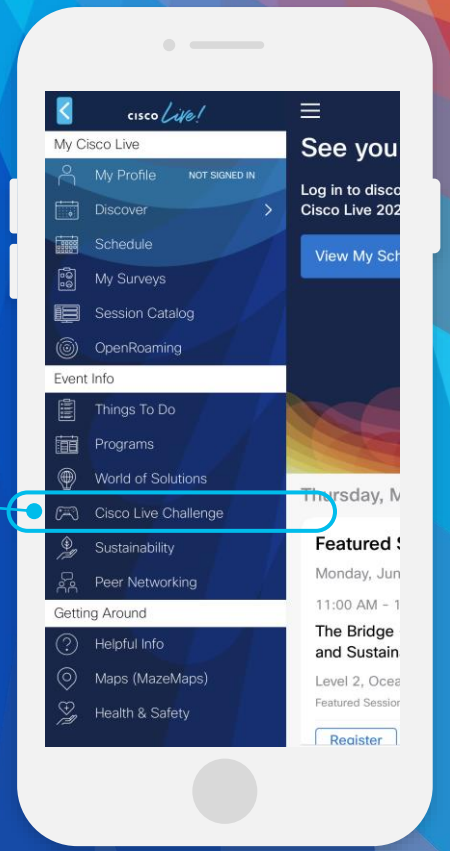
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

Let's go