cisco Live!

#CiscoLive

The bridge to possible

Firepower NGFW in the DC and Enterprise

Deployment Tips and New Features

Steven Chimes, Technical Solutions Architect

BRKSEC-2828

Cisco Webex App

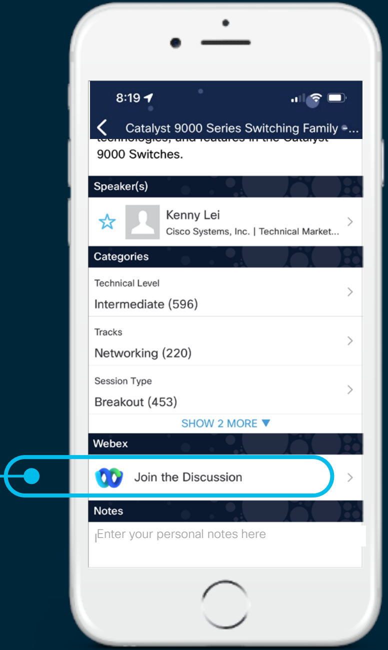
Questions?

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 17, 2022.



8:19

Catalyst 9000 Series Switching Family -...

9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

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

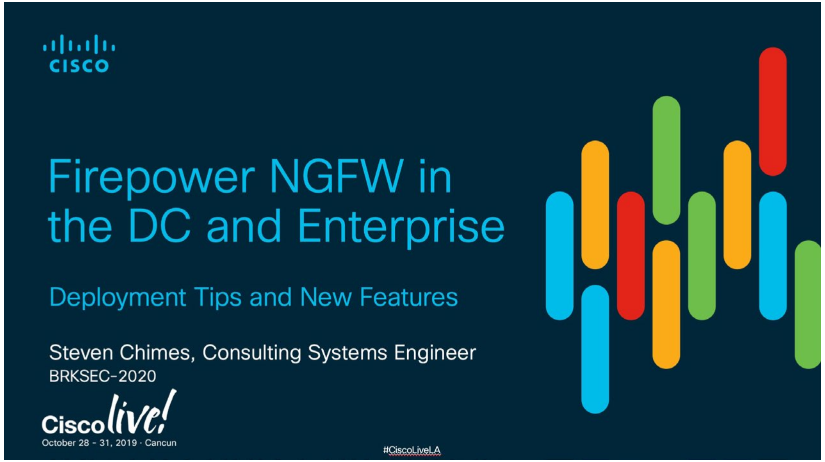
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Frequently Asked Questions
- Logging at Scale
- New Features
- Clustering Improvements
- Dynamic Objects
- Closing

Background Useful for this Session

Check out BRKSEC-2020, which includes other useful best practices



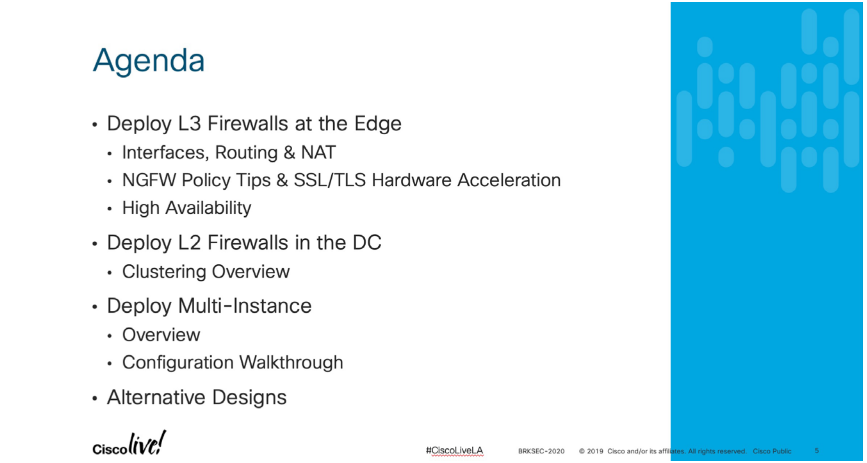
Firepower NGFW in the DC and Enterprise

Deployment Tips and New Features

Steven Chimes, Consulting Systems Engineer
BRKSEC-2020

Cisco live!
October 28 - 31, 2019 · Cancun

#CiscoLiveLA



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

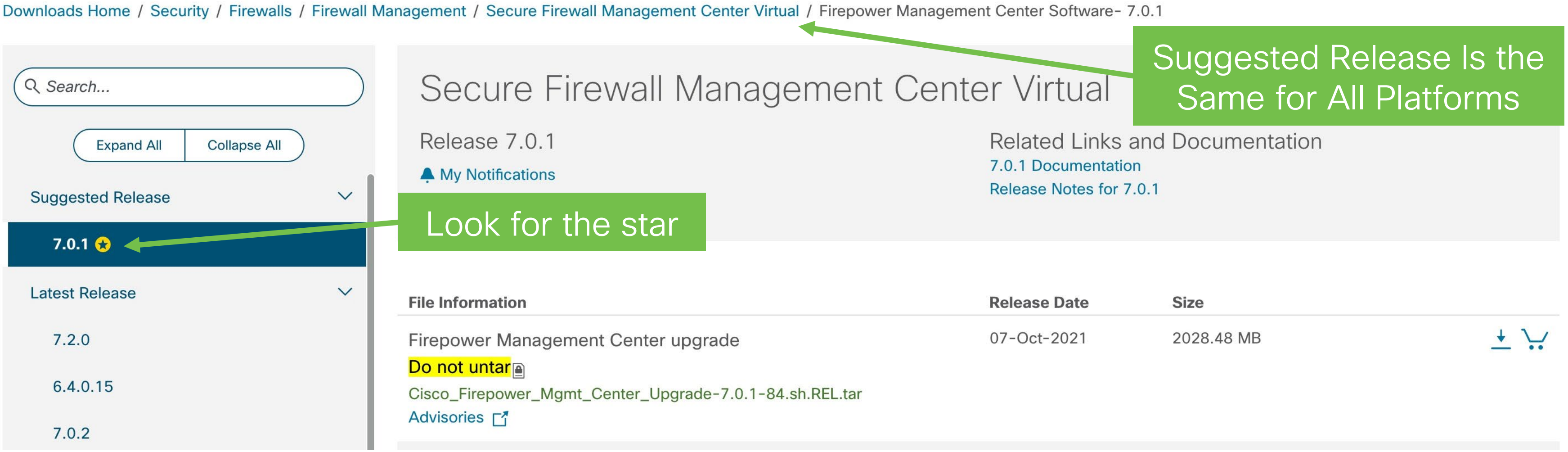
Cisco live! #CiscoLiveLA BRKSEC-2020 © 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public 5

https://www.ciscolive.com/on-demand/on-demand-library.html?#/session/1636060029985001 7Qsx

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 Virtual / Firepower Management Center Software- 7.0.1

Suggested Release Is the Same for All Platforms

Search...

Expand All | Collapse All

Suggested Release

- 7.0.1 ★

Latest Release

- 7.2.0
- 6.4.0.15
- 7.0.2

Look for the star

Secure Firewall Management Center Virtual

Release 7.0.1

My Notifications

Related Links and Documentation

7.0.1 Documentation

Release Notes for 7.0.1

File Information	Release Date	Size
Firepower Management Center upgrade Do not untar Cisco_Firepower_Mgmt_Center_Upgrade-7.0.1-84.sh.REL.tar Advisories	07-Oct-2021	2028.48 MB

+

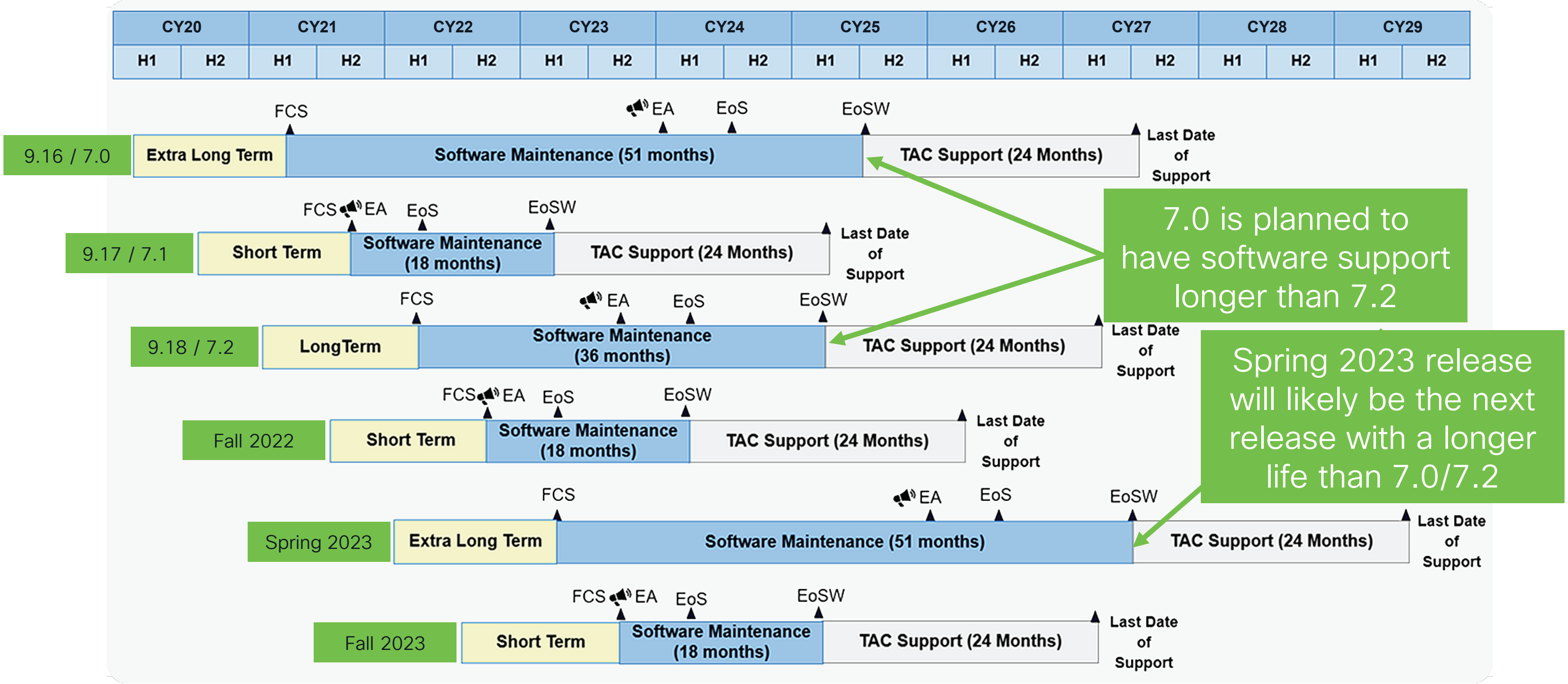
For the 4100/9300 Only - Latest Compatible FXOS Version, Currently 2.10(1.159)+

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

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

FAQ - What Version Do I Run Next?

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



CY20 | CY21 | CY22 | CY23 | CY24 | CY25 | CY26 | CY27 | CY28 | CY29

H1 H2 (each year)

9.16 / 7.0 — Extra Long Term — FCS — Software Maintenance (51 months) — EA — EoS — EoSW — TAC Support (24 Months) — Last Date of Support

9.17 / 7.1 — Short Term — FCS — EA — Software Maintenance (18 months) — EoS — EoSW — TAC Support (24 Months) — Last Date of Support

9.18 / 7.2 — LongTerm — FCS — Software Maintenance (36 months) — EA — EoS — EoSW — TAC Support (24 Months) — Last Date of Support

Fall 2022 — Short Term — FCS — EA — Software Maintenance (18 months) — EoS — EoSW — TAC Support (24 Months) — Last Date of Support

Spring 2023 — Extra Long Term — FCS — Software Maintenance (51 months) — EA — EoS — EoSW — TAC Support (24 Months) — Last Date of Support

Fall 2023 — Short Term — FCS — EA — Software Maintenance (18 months) — EoS — EoSW — TAC Support (24 Months) — Last Date of Support

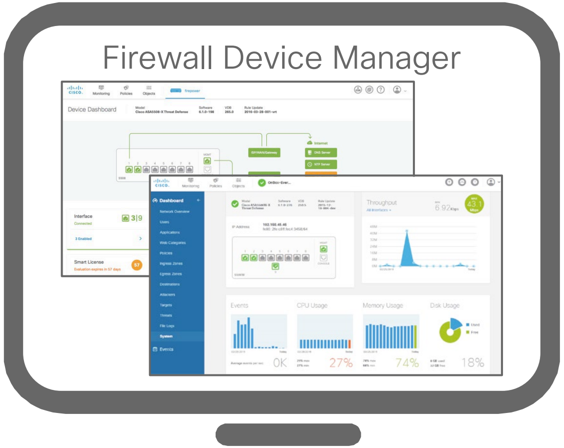
7.0 is planned to have software support longer than 7.2

Spring 2023 release will likely be the next release with a longer life than 7.0/7.2

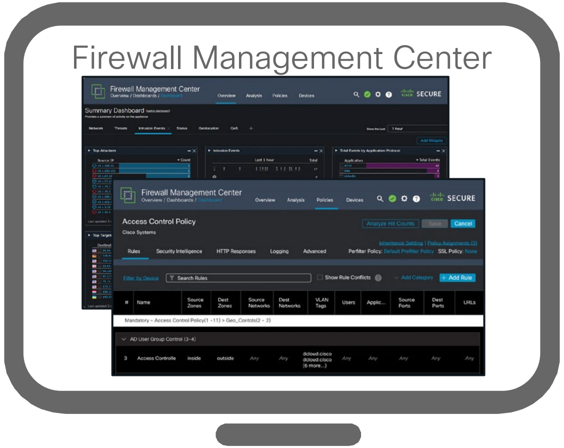
Cisco's NGFW Product Line Software Release and Sustaining Bulletin:
https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html

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

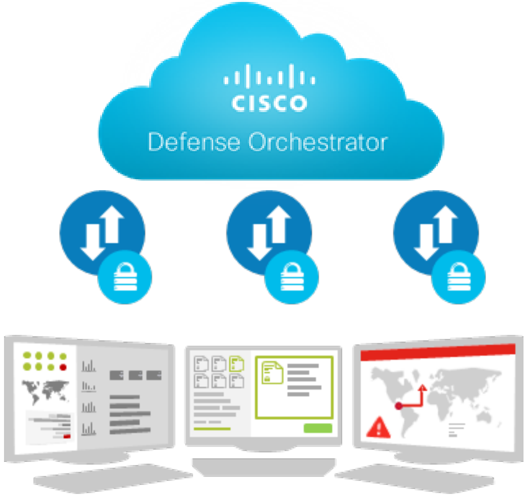
FAQ – What Firewall Manager Do I Use?



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



- Management appliance
- Manages Secure Firewall
- Supports full FTD feature set including analytics and firewall clustering



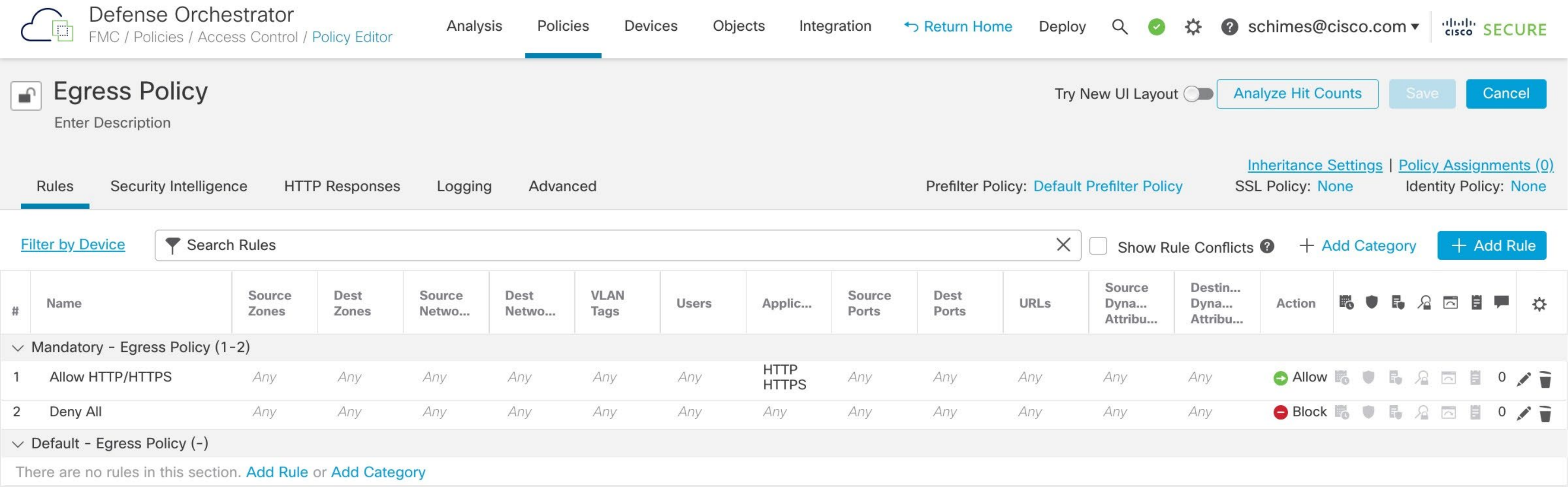
- Centralized cloud manager
- Manages Secure Firewall, ASA, Meraki MX and Umbrella SASE
- Near feature parity with FMC

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

7.2

Cloud Delivered Firewall Management Center

Almost complete feature parity with On-Premises FMC



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

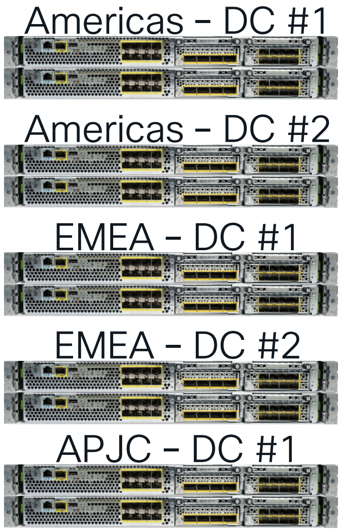
Note for DC/Enterprise Deployments - No support (today) for clustering

cisco Live!

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

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

- Logs stored on physical or FMC virtual appliance
- Logs sent via sftunnel
- View logs in FMC

Best for small FMC managed deployments

Security Analytics and Logging (On-Premises)

- 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

Best for larger FMC managed deployments

Security Analytics and Logging (SaaS)

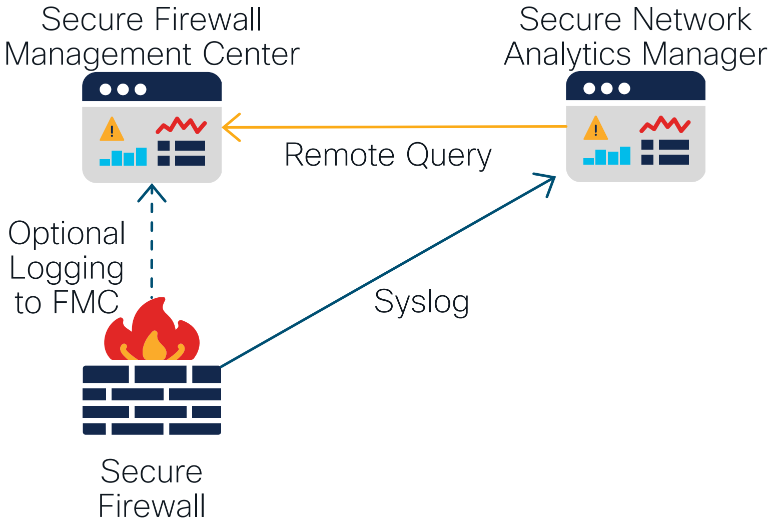
- Logs stored in SAL cloud
- Logs sent via built-in Secure Services Exchange (SSE) connector or via syslog to the Secure Event Connector (SEC)
- View logs in CDO

Best for CDO managed deployments

7.0

Security Analytics and Logging (On-Premises)

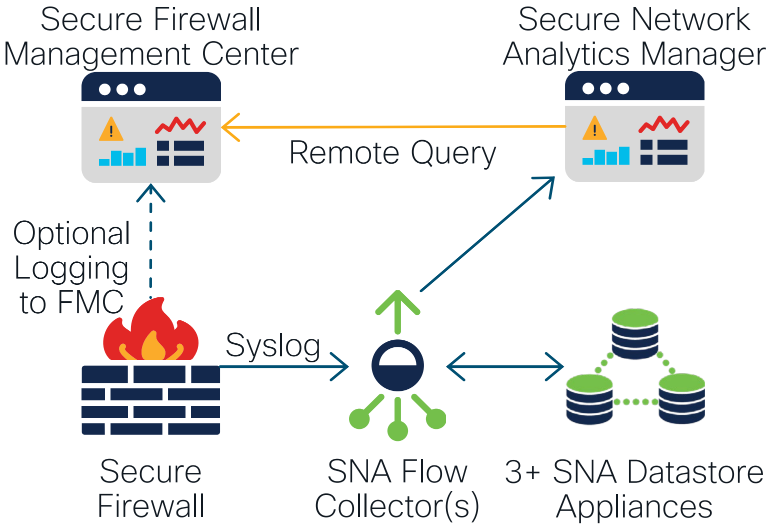
Single Node



Secure Firewall Management Center
Secure Network Analytics Manager
Remote Query
Optional Logging to FMC
Syslog
Secure Firewall

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

Multi-Node



Secure Firewall Management Center
Secure Network Analytics Manager
Remote Query
Optional Logging to FMC
Syslog
Secure Firewall
SNA Flow Collector(s)
3+ SNA Datastore Appliances

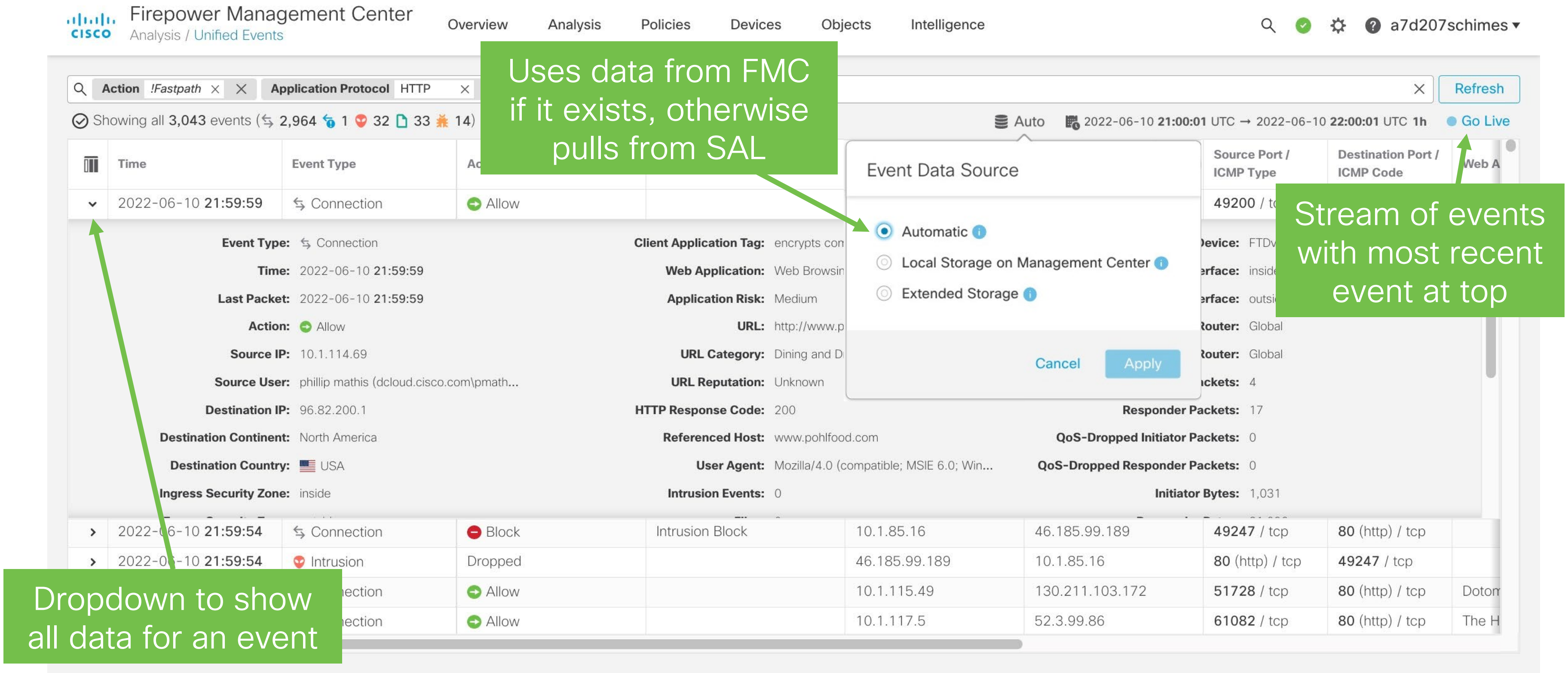
Scales to 100k+ EPS (sustained)
Retention of 600+ days @ 5k EPS

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

7.0

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

Time	Event Type	Ac				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	
	ection	Allow		10.1.115.49	130.211.103.172	51728 / tcp	80 (http) / tcp	Dotom
	ection	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

evice: FTDv
erface: inside
erface: outsi
Router: Global
Router: Global
ckets: 4
Responder Packets: 17
QoS-Dropped Initiator Packets: 0
QoS-Dropped Responder Packets: 0
Initiator Bytes: 1,031

Event Data Source
◉ Automatic
○ Local Storage on Management Center
○ Extended Storage
Cancel Apply

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

Stream of events with most recent event at top

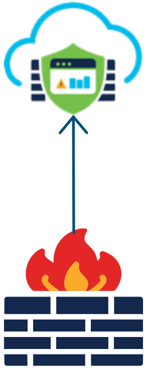
Dropdown to show all data for an event

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

7.0

Security Analytics and Logging (SaaS)

Direct to Cloud

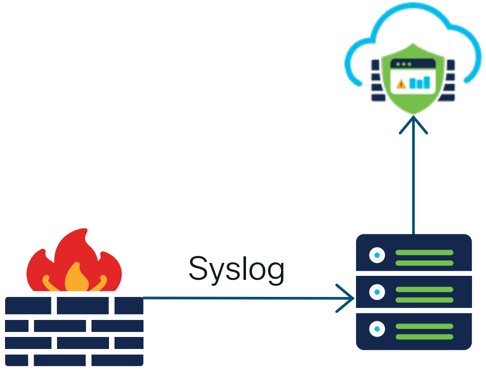


Cisco Defense Orchestrator

Secure Firewall

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

via CDO Secure Event Connector



Cisco Defense Orchestrator

Syslog

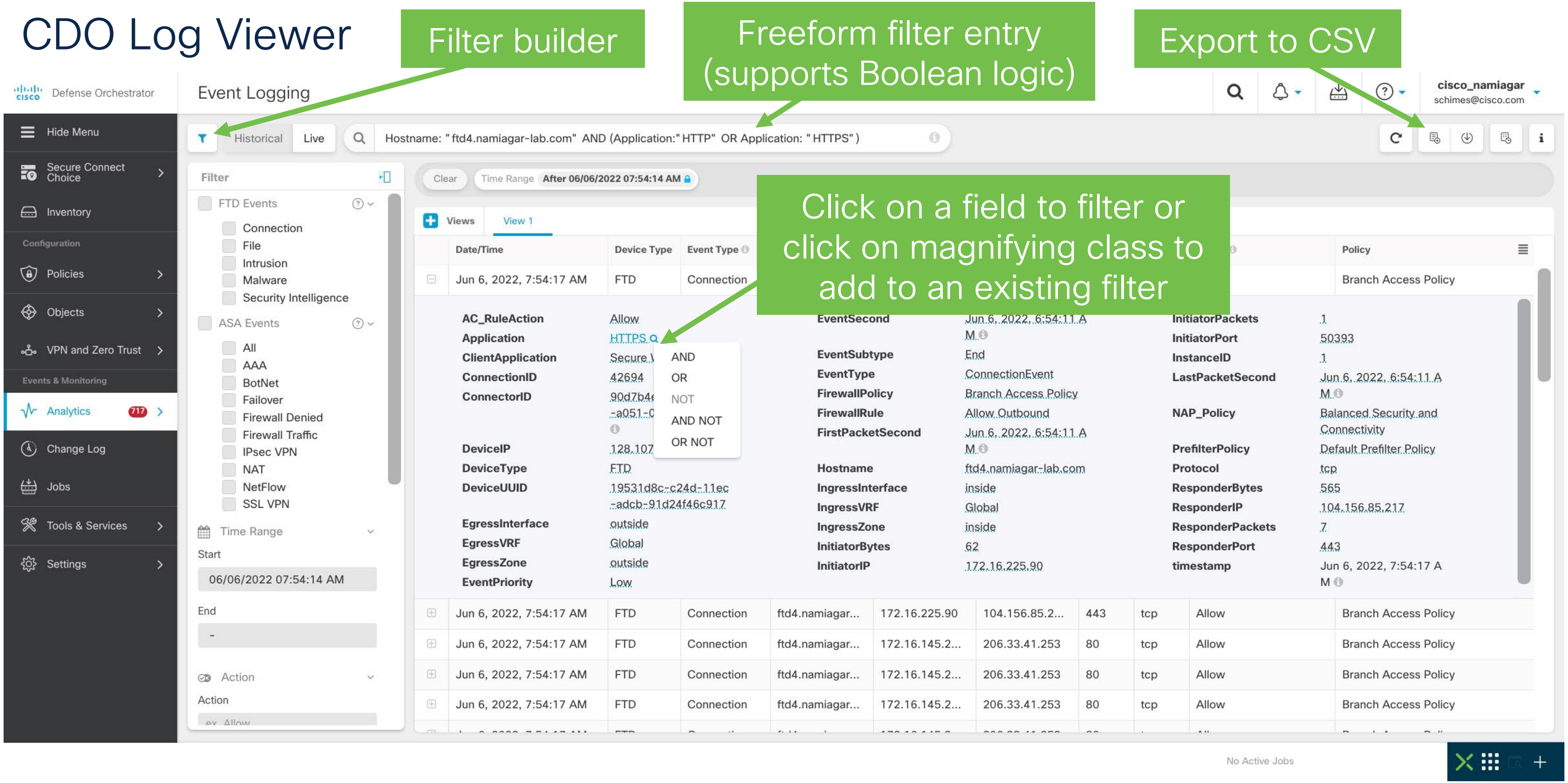
Secure Firewall

CDO Secure Event Connector(s)

Unlimited Scale
Retention Up to 3 Years

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

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

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

Start: 06/06/2022 07:54:14 AM

End: -

Date/Time	Device Type	Event Type							Policy
Jun 6, 2022, 7:54:17 AM	FTD	Connection							Branch Access Policy

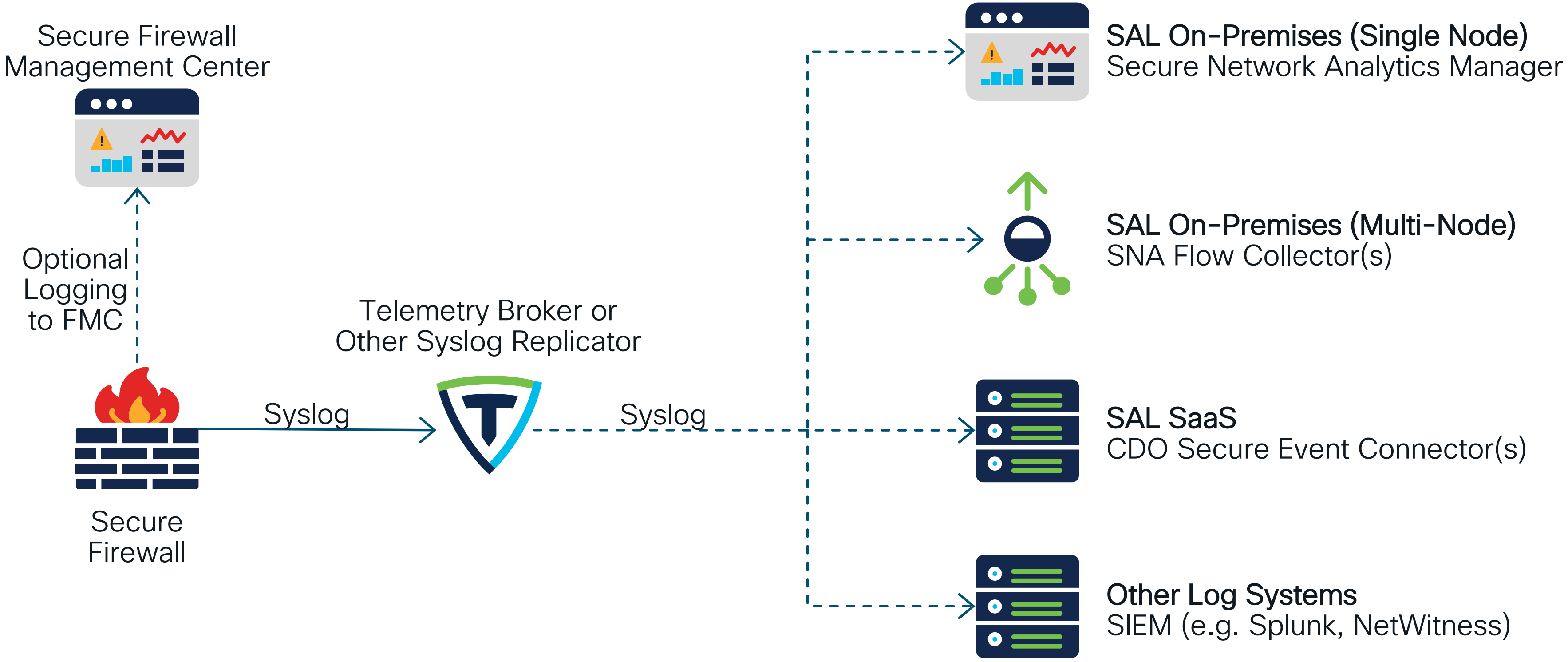
AC_RuleAction: Allow
Application: HTTPS
ClientApplication: Secure \
ConnectionID: 42694
ConnectorID: 90d7b4e -a051-0
DeviceIP: 128.107
DeviceType: FTD
DeviceUUID: 19531d8c-c24d-11ec -adcb-91d24f46c917
EgressInterface: outside
EgressVRF: Global
EgressZone: outside
EventPriority: Low
EventSecond: Jun 6,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

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

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

For Best Performance, Send Logs Only Once

Use Telemetry Broker to Send Logs to Multiple Destinations



Secure Firewall Management Center

Optional Logging to FMC

Secure Firewall

Syslog

Telemetry Broker or Other Syslog Replicator

Syslog

SAL On-Premises (Single Node)
Secure Network Analytics Manager

SAL On-Premises (Multi-Node)
SNA Flow Collector(s)

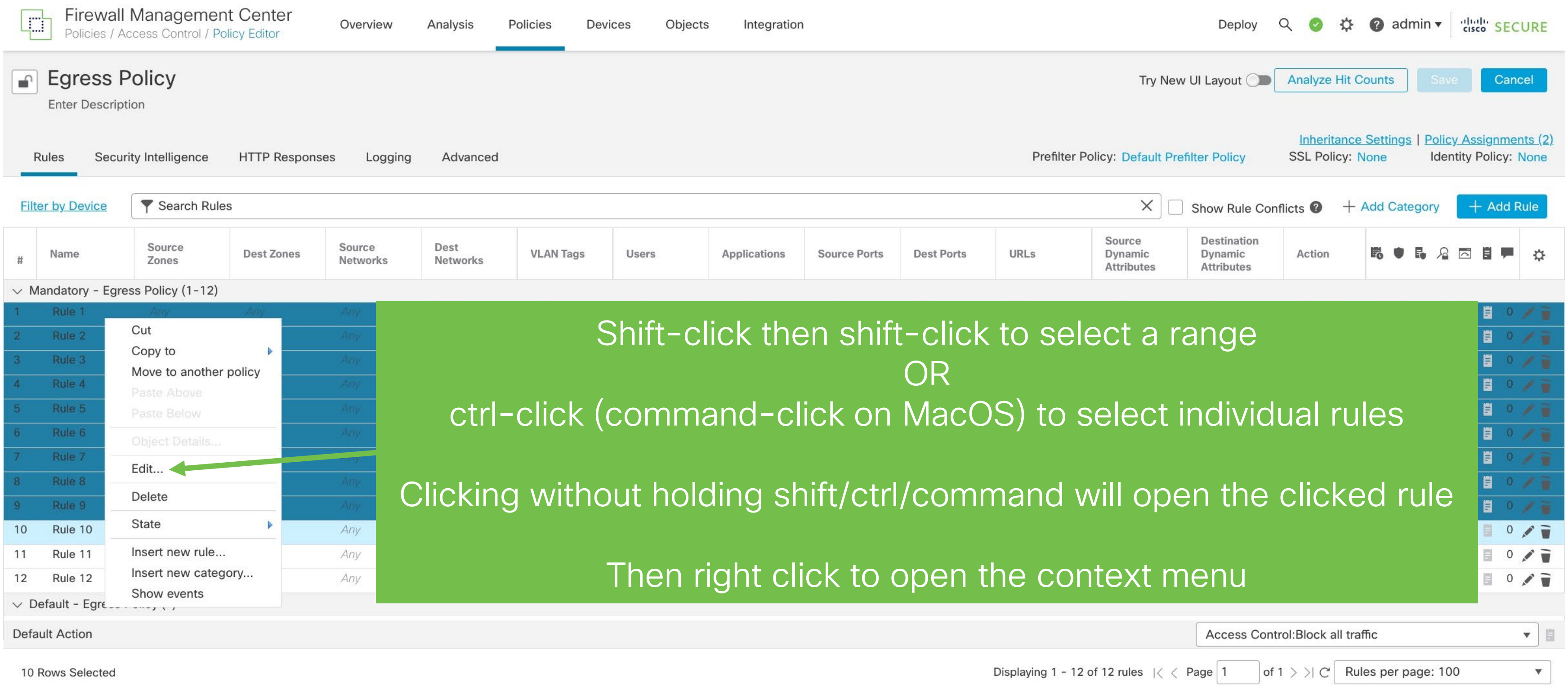
SAL SaaS
CDO Secure Event Connector(s)

Other Log Systems
SIEM (e.g. Splunk, NetWitness)

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

New Features

Access Control Policy – Bulk Edit



Egress Policy

Enter Description

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

Identity Policy: None

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

Default Action: Access Control:Block all traffic

10 Rows Selected

Displaying 1 - 12 of 12 rules   Page 1 of 1   Rules per page: 100

Shift-click then shift-click to select a range
OR
ctrl-click (command-click on MacOS) to select individual rules

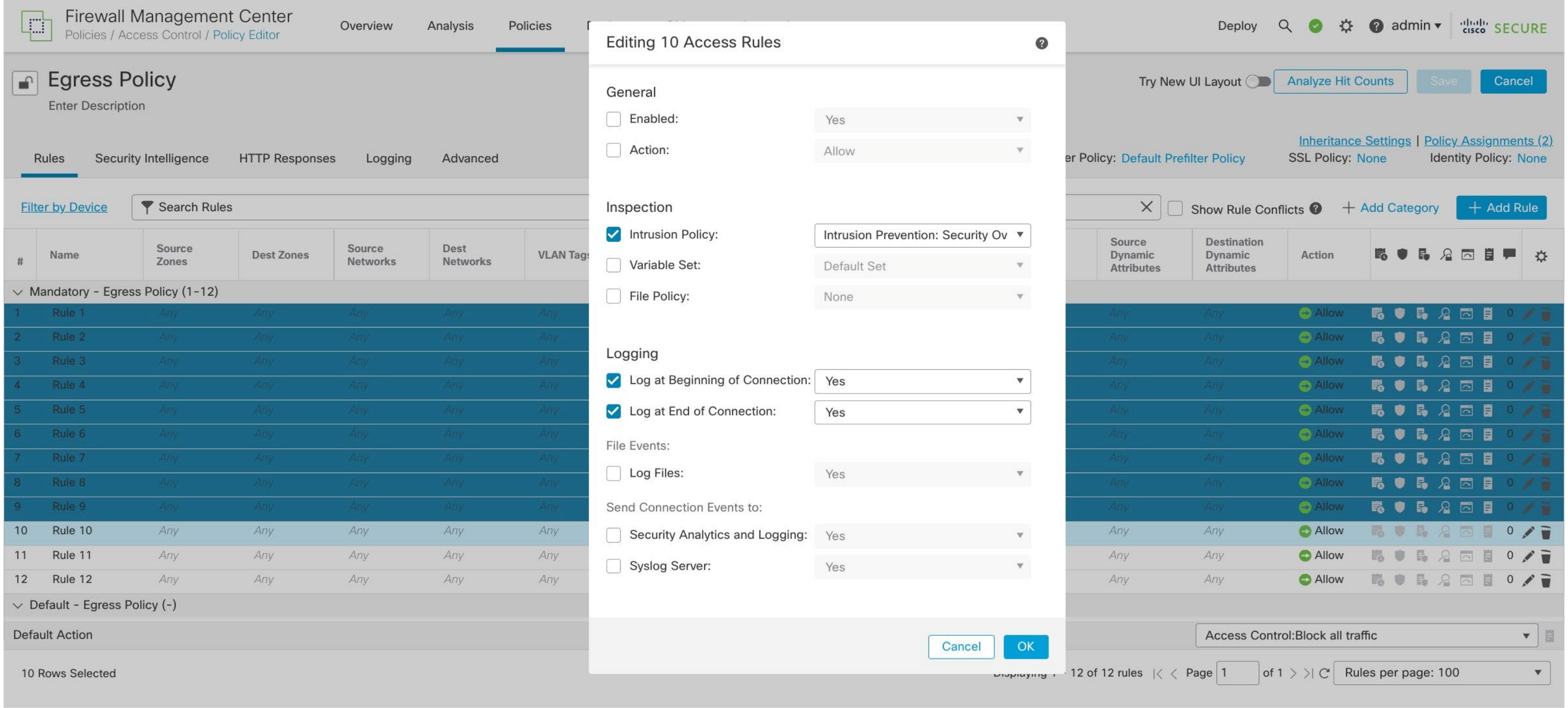
Clicking without holding shift/ctrl/command will open the clicked rule

Then right click to open the context menu

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

6.6

Access Control Policy – Bulk Edit



Firewall Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Deploy | admin | SECURE

Egress Policy

Enter Description

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

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

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

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	0
2	Rule 2	Any	Any	Any	Any	Any	Any	Any	Allow	0
3	Rule 3	Any	Any	Any	Any	Any	Any	Any	Allow	0
4	Rule 4	Any	Any	Any	Any	Any	Any	Any	Allow	0
5	Rule 5	Any	Any	Any	Any	Any	Any	Any	Allow	0
6	Rule 6	Any	Any	Any	Any	Any	Any	Any	Allow	0
7	Rule 7	Any	Any	Any	Any	Any	Any	Any	Allow	0
8	Rule 8	Any	Any	Any	Any	Any	Any	Any	Allow	0
9	Rule 9	Any	Any	Any	Any	Any	Any	Any	Allow	0
10	Rule 10	Any	Any	Any	Any	Any	Any	Any	Allow	0
11	Rule 11	Any	Any	Any	Any	Any	Any	Any	Allow	0
12	Rule 12	Any	Any	Any	Any	Any	Any	Any	Allow	0
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

- ☑ 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:

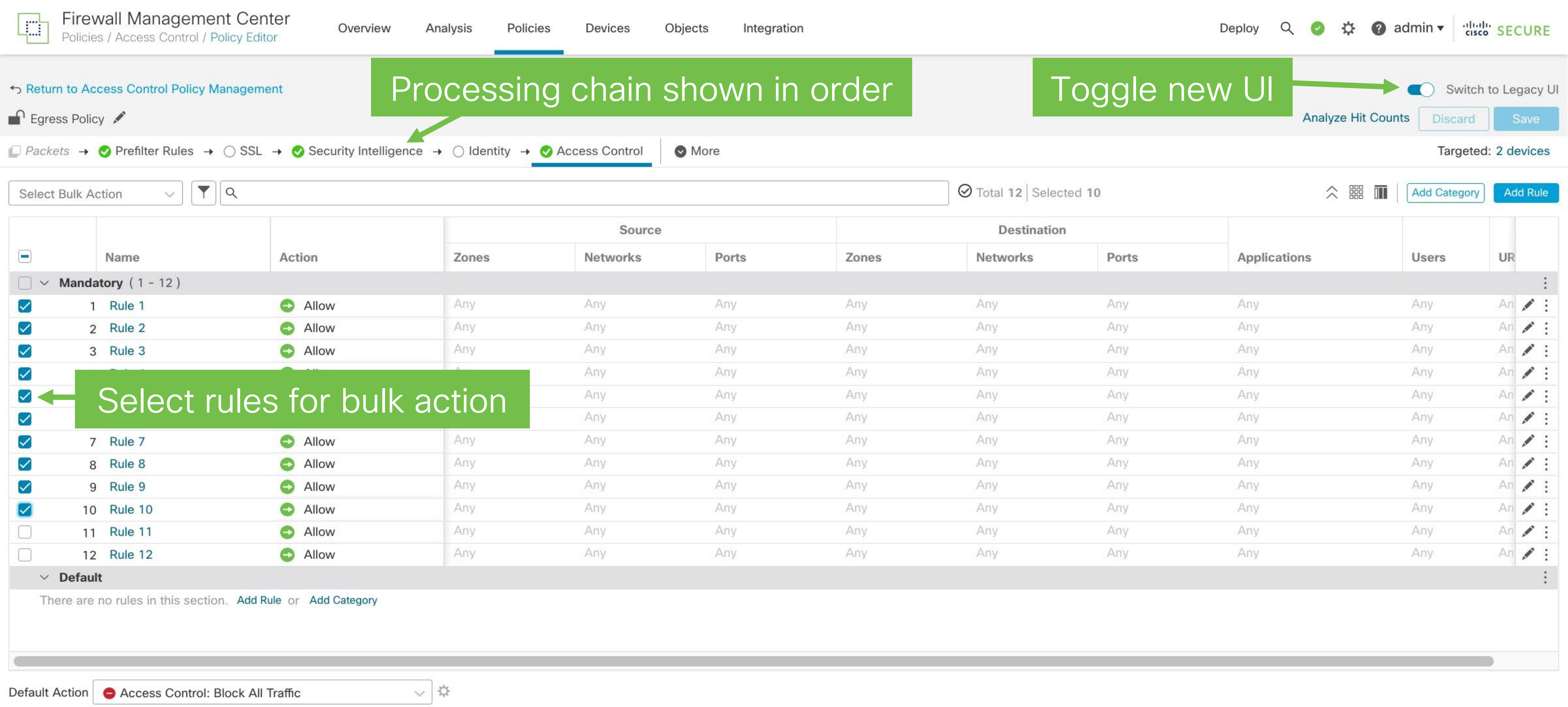
- □ Log Files: Yes

Send Connection Events to:

- □ Security Analytics and Logging: Yes
- □ Syslog Server: Yes

Cancel | OK

Access Control Policy – New UI



Processing chain shown in order

Toggle new UI

Select rules for bulk action

Egress Policy

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

Targeted: 2 devices

Total 12 | Selected 10

		Name	Action	Source			Destination			Applications	Users	UR
				Zones	Networks	Ports	Zones	Networks	Ports			
□		**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

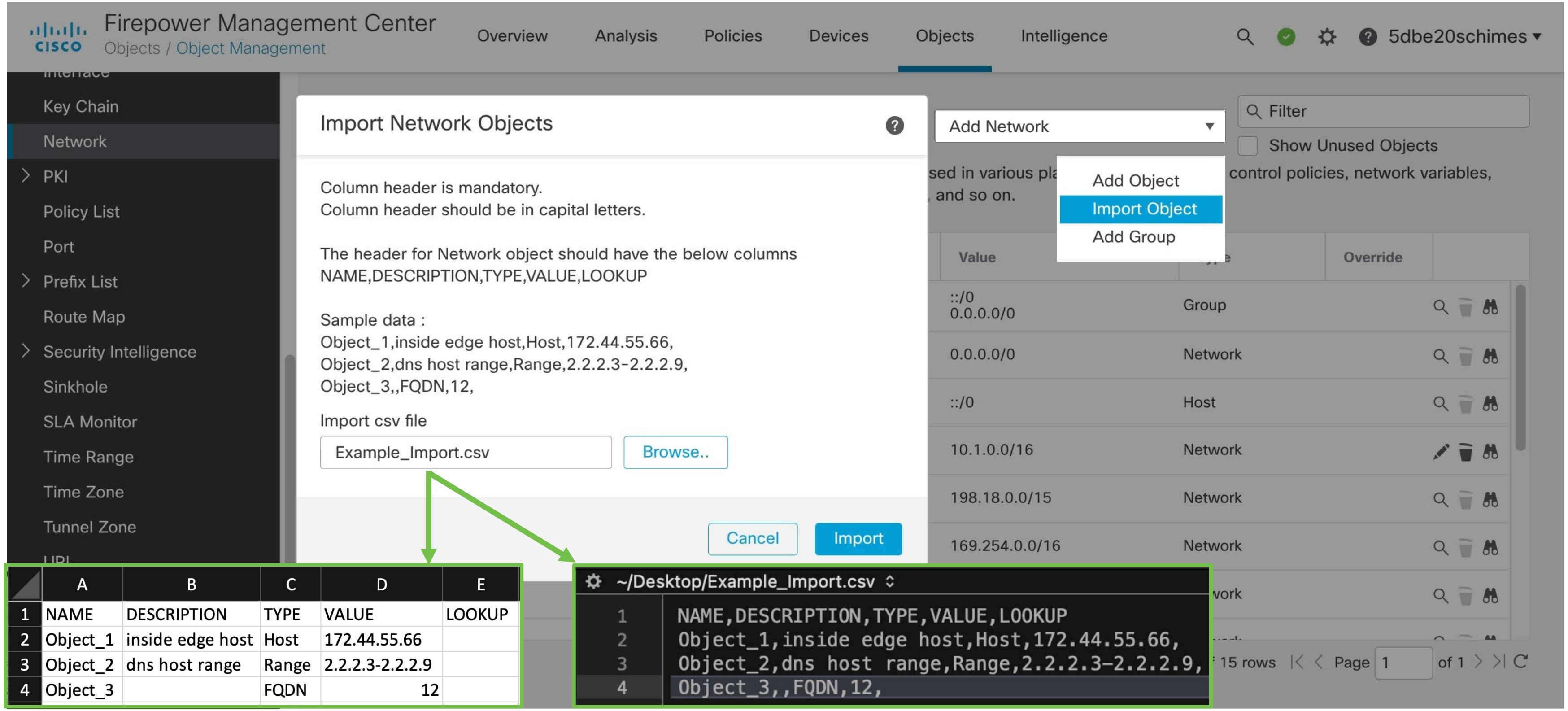
Default Action: Access Control: Block All Traffic

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

6.7

Bulk Import of Objects

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



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]

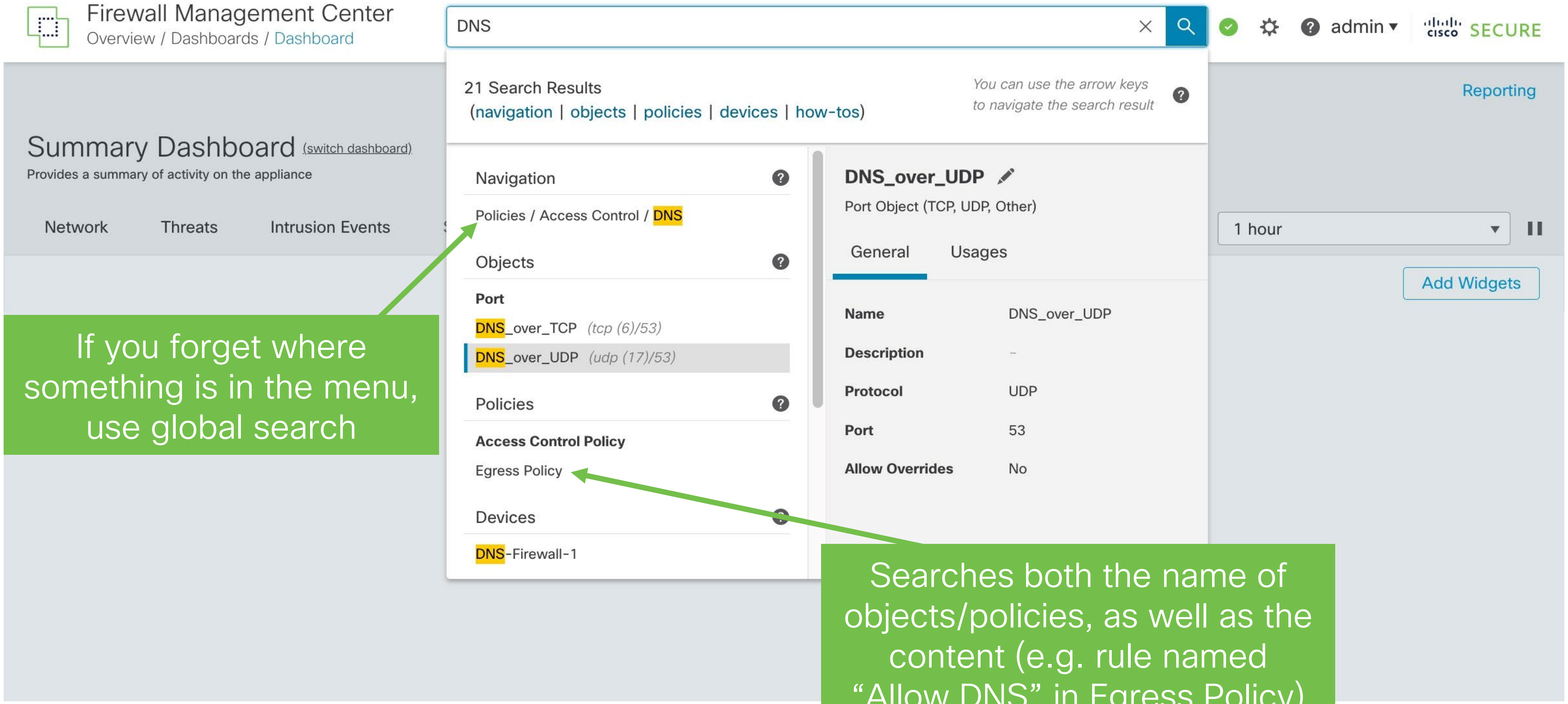
	A	B	C	D	E
1	NAME	DESCRIPTION	TYPE	VALUE	LOOKUP
2	Object_1	inside edge host	Host	172.44.55.66	
3	Object_2	dns host range	Range	2.2.2.3-2.2.2.9	
4	Object_3		FQDN	12	

~/Desktop/Example_Import.csv

```
NAME,DESCRIPTION,TYPE,VALUE,LOOKUP
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,
```

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

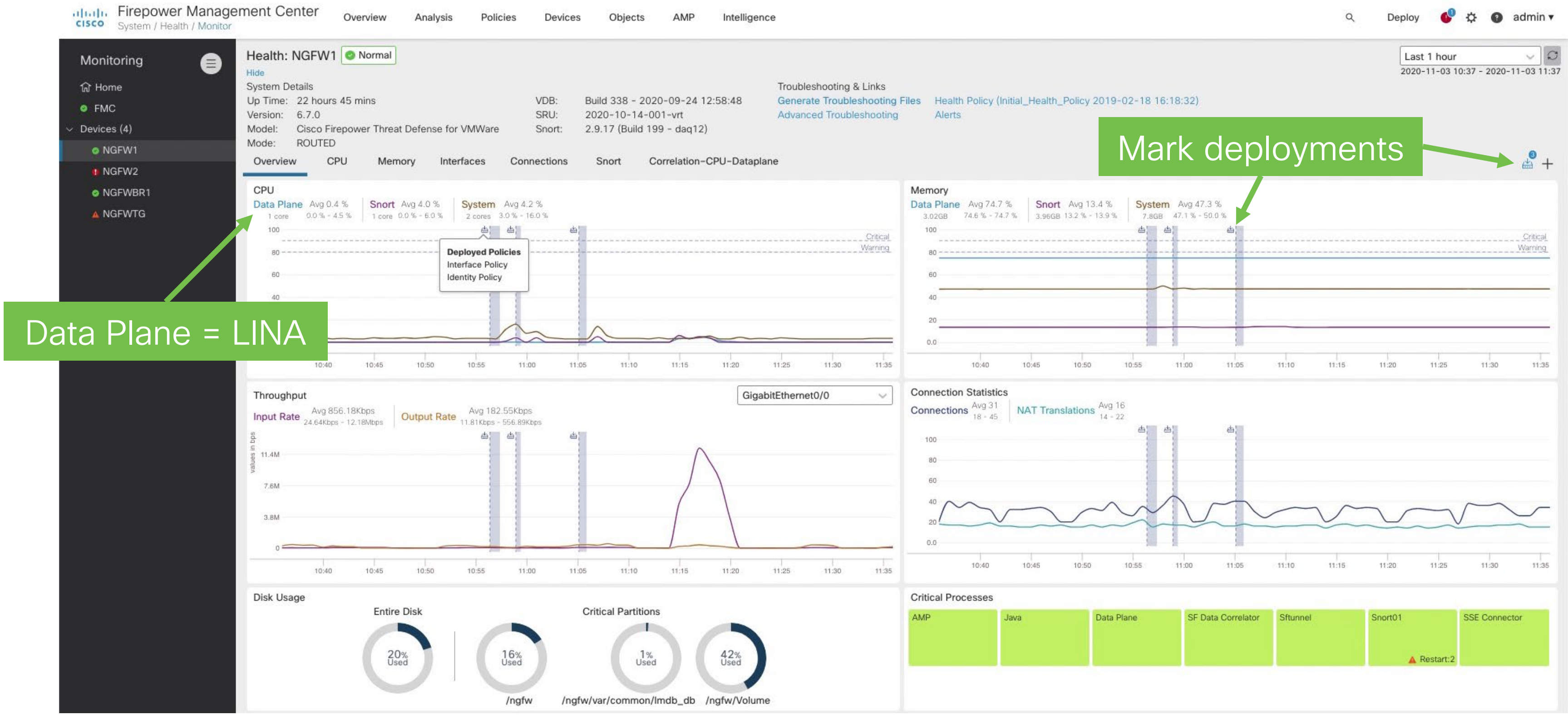
If you forget where something is in the menu, use global search

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

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

Device Health Monitoring Dashboard

No more going to the CLI for basic performance troubleshooting!



Firepower Management Center
System / Health / Monitor

Health: NGFW1 Normal

Hide

System Details
Up Time: 22 hours 45 mins
Version: 6.7.0
Model: Cisco Firepower Threat Defense for VMWare
Mode: ROUTED
VDB: Build 338 - 2020-09-24 12:58:48
SRU: 2020-10-14-001-vrt
Snort: 2.9.17 (Build 199 - daq12)

Troubleshooting & Links
Generate Troubleshooting Files
Advanced Troubleshooting
Health Policy (Initial_Health_Policy 2019-02-18 16:18:32)
Alerts

Last 1 hour
2020-11-03 10:37 - 2020-11-03 11:37

CPU
Data Plane Avg 0.4 % 1 core 0.0 % - 4.5 %
Snort Avg 4.0 % 1 core 0.0 % - 6.0 %
System Avg 4.2 % 2 cores 3.0 % - 16.0 %

Deployed Policies
Interface Policy
Identity Policy

Memory
Data Plane Avg 74.7 % 3.02GB 74.6 % - 74.7 %
Snort Avg 13.4 % 3.96GB 13.2 % - 13.9 %
System Avg 47.3 % 7.8GB 47.1 % - 50.0 %

Throughput
GigabitEthernet0/0
Input Rate Avg 856.18Kbps 24.64Kbps - 12.18Mbps
Output Rate Avg 182.55Kbps 11.81Kbps - 556.89Kbps

Connection Statistics
Connections Avg 31 18 - 45
NAT Translations Avg 16 14 - 22

Disk Usage
Entire Disk: 20% Used; 16% Used /ngfw
Critical Partitions: 1% Used /ngfw/var/common/lmdb_db; 42% Used /ngfw/Volume

Critical Processes
AMP
Java
Data Plane
SF Data Correlator
Sftunnel
Snort01 Restart:2
SSE Connector

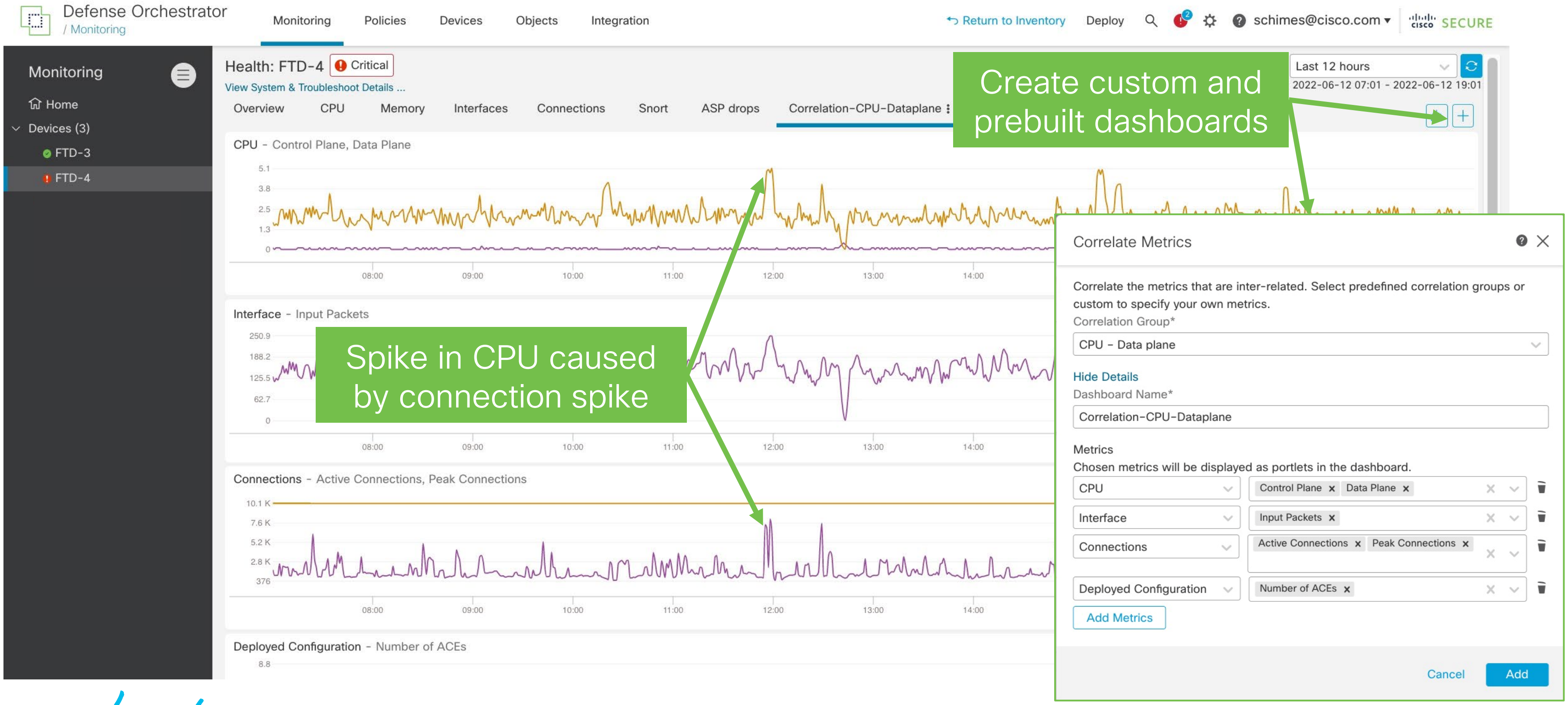
Mark deployments

Data Plane = LINA

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

Device Health Monitoring Dashboard

Use Correlated Dashboards for Easy Troubleshooting



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.

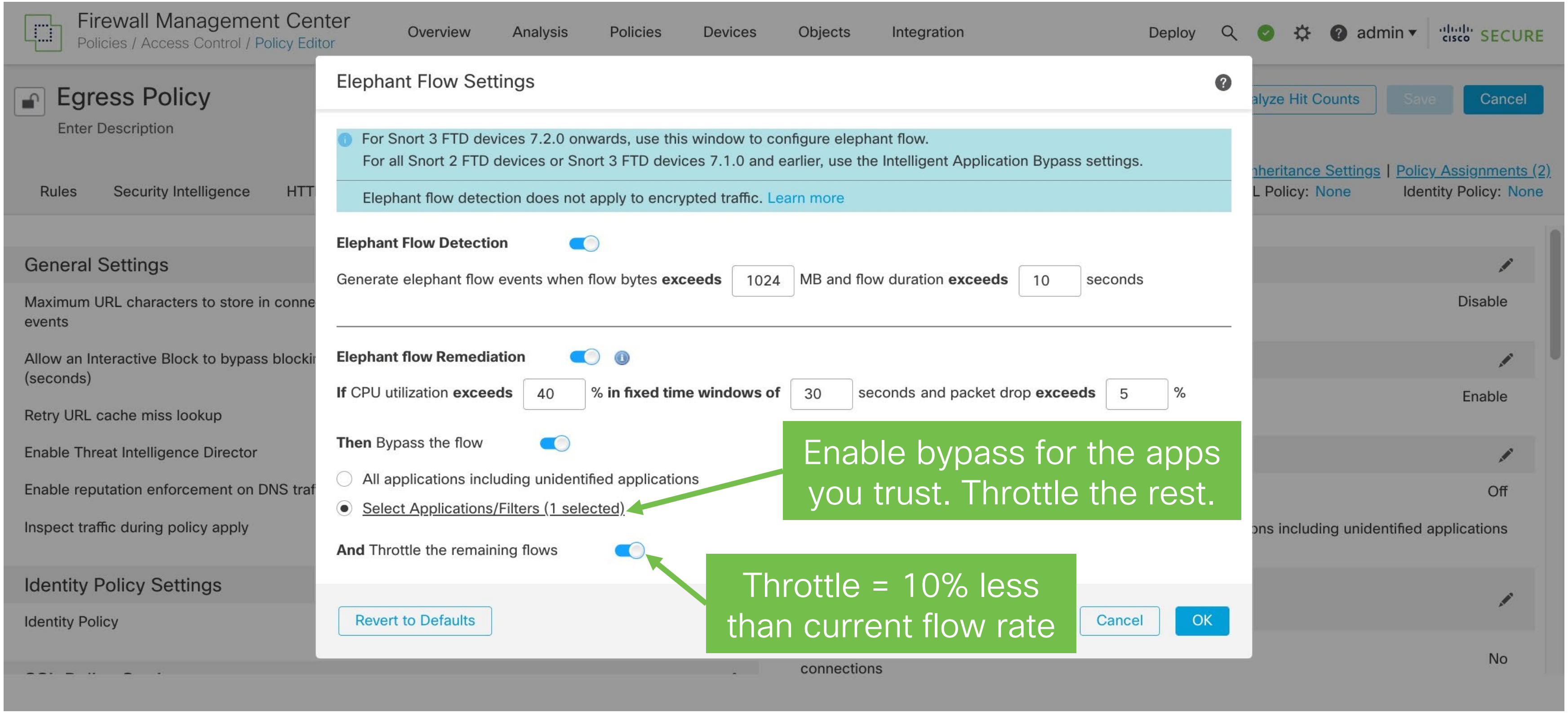
CPU	Control Plane × Data Plane ×
Interface	Input Packets ×
Connections	Active Connections × Peak Connections ×
Deployed Configuration	Number of ACEs ×

Add Metrics

Cancel   Add

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

Elephant Flow Remediation



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
General Settings
Maximum URL characters to store in conne events
Allow an Interactive Block to bypass blocki (seconds)
Retry URL cache miss lookup
Enable Threat Intelligence Director
Enable reputation enforcement on DNS traf
Inspect traffic during policy apply
Identity Policy Settings
Identity Policy
alyze Hit Counts
Save
Cancel
nheritance Settings | Policy Assignments (2)
L Policy: None
Identity Policy: None
Disable
Enable
Off
ons including unidentified applications
No
connections

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 ●

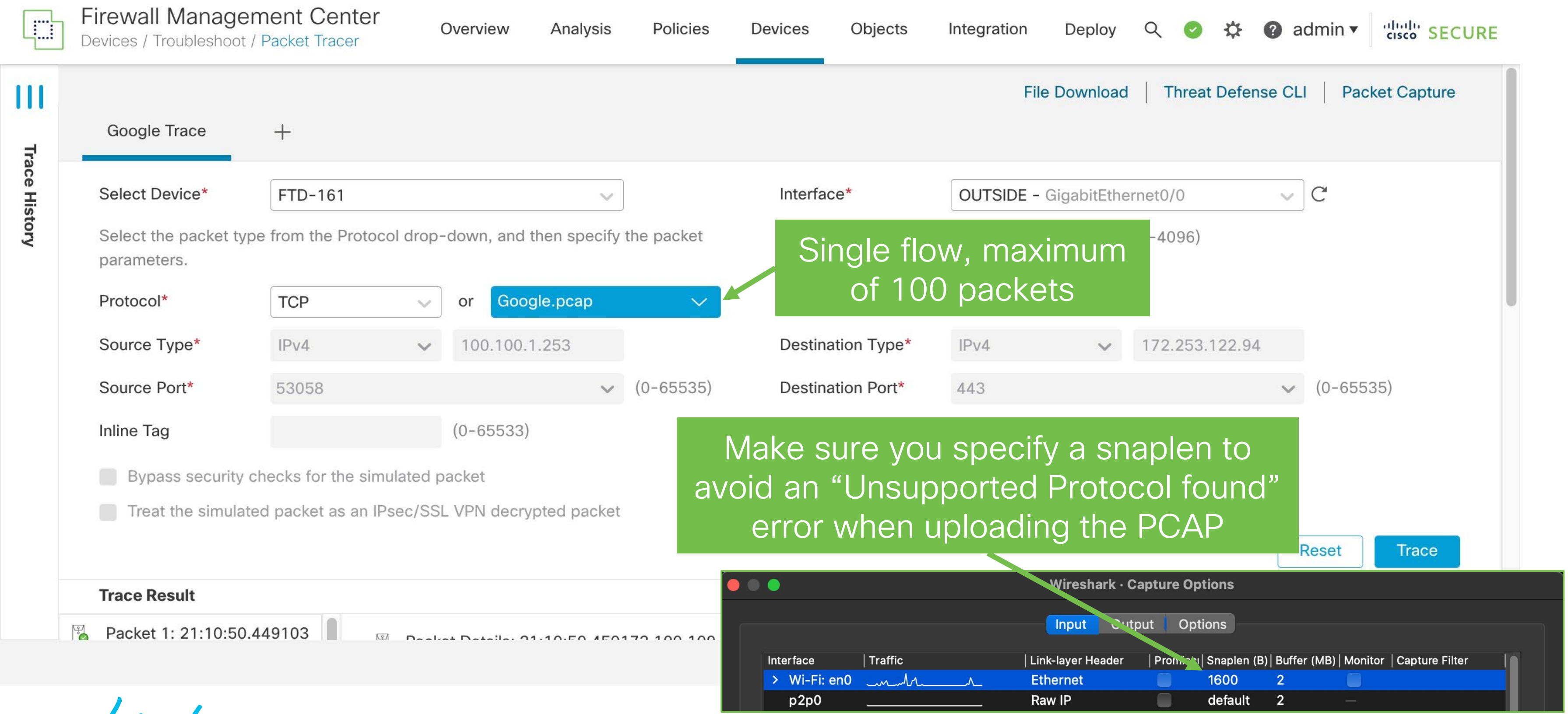
Revert to Defaults | Cancel | OK

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

Throttle = 10% less than current flow rate

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

Packet Tracer PCAP Upload



Select Device*: FTD-161

Interface*: OUTSIDE - GigabitEthernet0/0

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

-4096)

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

Trace Result

Packet 1: 21:10:50.449103

Packet Details: 21:10:50.450172 100.100

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

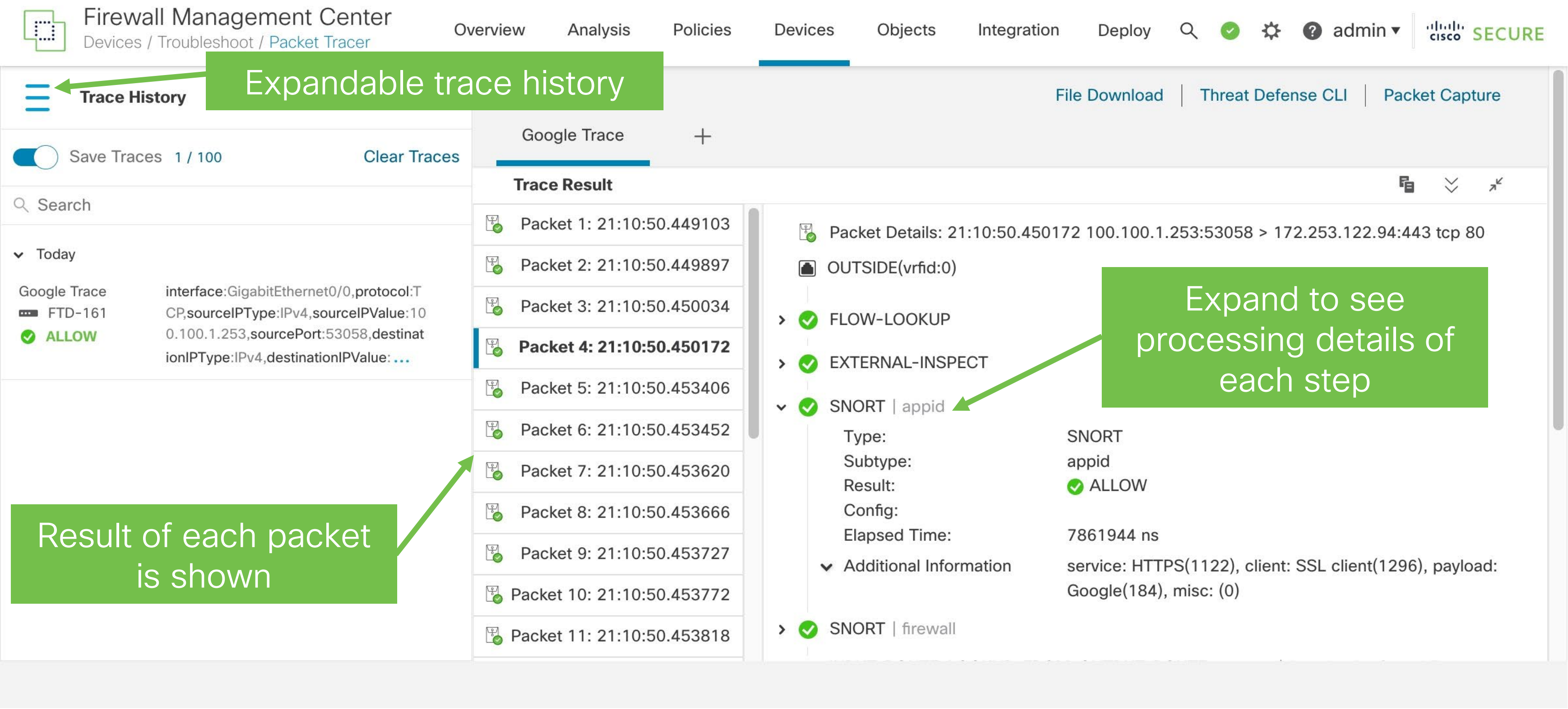
Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
› Wi-Fi: en0		Ethernet	□	1600	2	□	
p2p0		Raw IP	□	default	2	—	

cisco Live!

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

7.1

Packet Tracer PCAP Upload



Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Trace History

File Download | Threat Defense CLI | Packet Capture

Save Traces 1 / 100 Clear Traces

Search

Today

Google Trace
FTD-161
✓ ALLOW

interface:GigabitEthernet0/0,protocol:TCP,sourceIPType:IPv4,sourceIPValue:100.100.1.253,sourcePort:53058,destinationIPType:IPv4,destinationIPValue: ...

Google Trace +

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

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

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

Expandable trace history

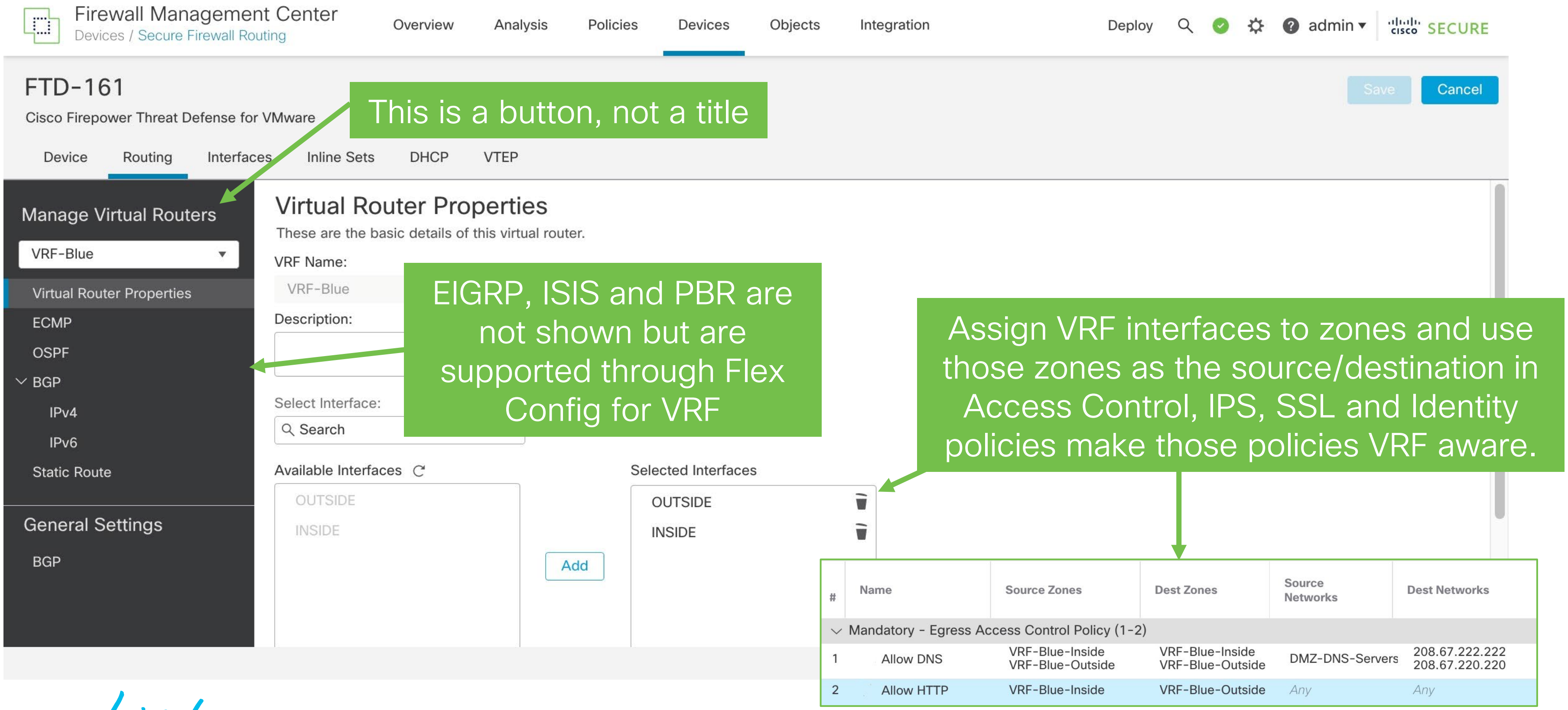
Expand to see processing details of each step

Result of each packet is shown

cisco Live!

6.6

Virtual Routing and Forwarding



Firewall Management Center
Devices / Secure Firewall Routing

FTD-161
Cisco Firepower Threat Defense for VMware

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name: VRF-Blue

Description:

Select Interface:

Search

Available Interfaces: OUTSIDE, INSIDE

Selected Interfaces: OUTSIDE, INSIDE

This is a button, not a title

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

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

Clustering Improvements

7.2

Cisco Clustering Support

Physical Cluster

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

Virtual Cluster

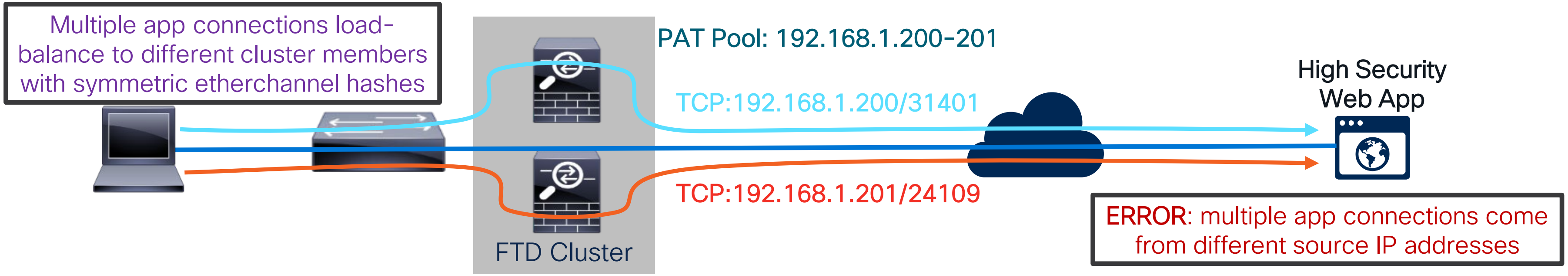
- ASAv
  - Already released (9.17.1)
  - Private cloud (VMware and KVM)
- FTDv
  - FMC managed nodes, running 7.2
    - Private cloud (VMware and KVM)
    - Public cloud (AWS and GCP)
  - Minimum 1 node; maximum 16 nodes
  - All nodes require 5 interfaces (with CCL)
    - AWS cluster behind GWLB can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

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

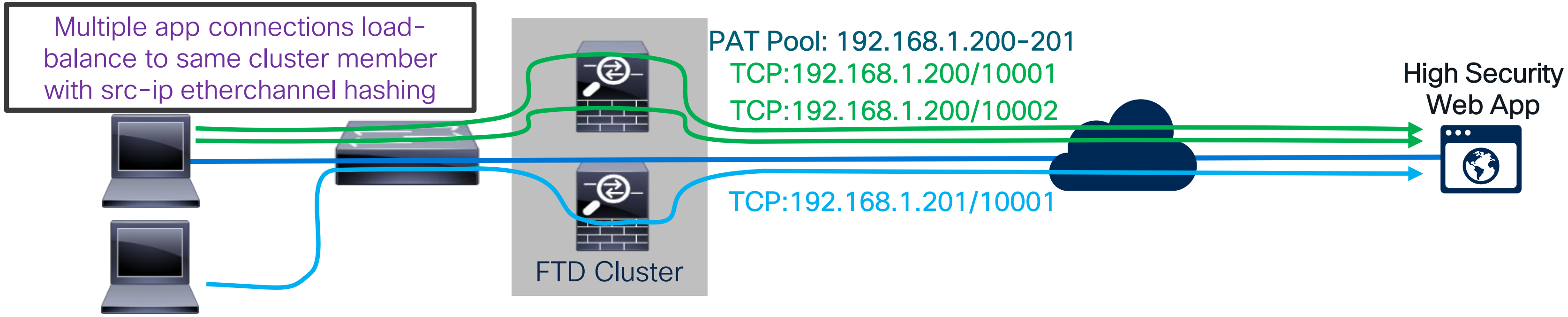
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

PAT in Clustering for Internet Egress (6.6 or Lower)

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


Multiple app connections load-balance to different cluster members with symmetric etherchannel hashes
PAT Pool: 192.168.1.200-201
TCP:192.168.1.200/31401
TCP:192.168.1.201/24109
FTD Cluster
High Security Web App
ERROR: multiple app connections come from different source IP addresses

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

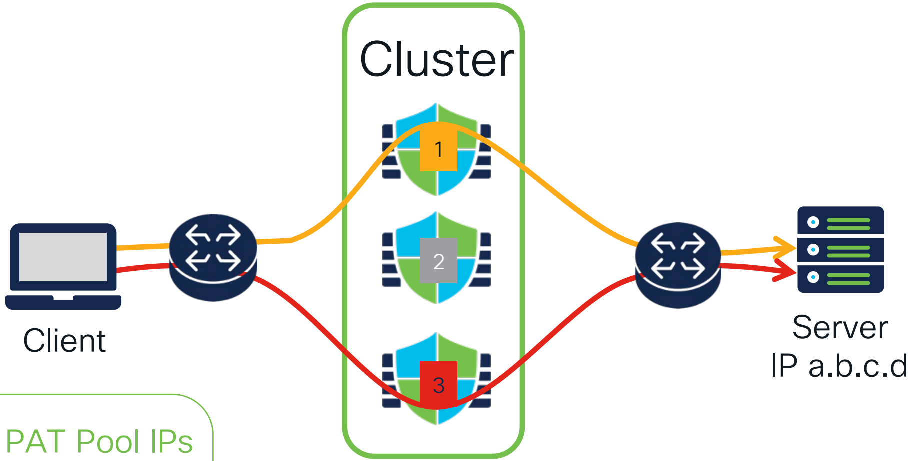

Multiple app connections load-balance to same cluster member with src-ip etherchannel hashing
PAT Pool: 192.168.1.200-201
TCP:192.168.1.200/10001
TCP:192.168.1.200/10002
TCP:192.168.1.201/10001
FTD Cluster
High Security Web App

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

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

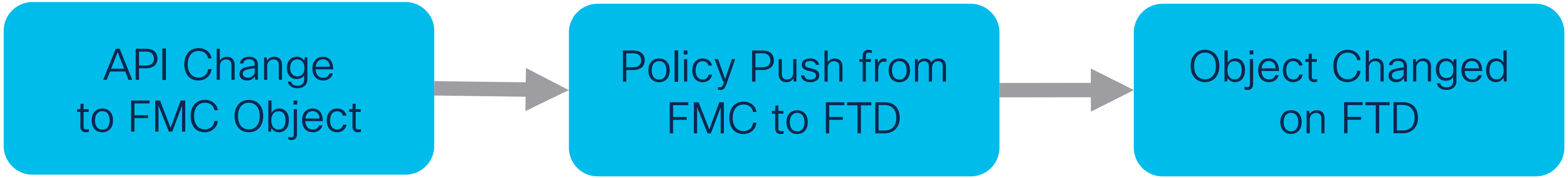
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dynamic Objects

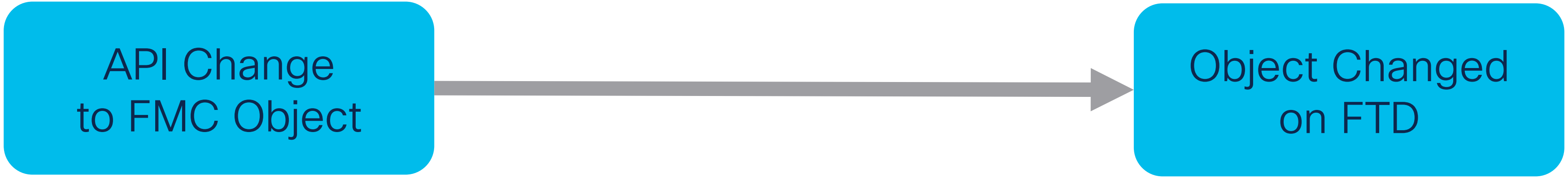
7.0

Dynamic Objects

Without Dynamic Objects:



With Dynamic Objects:

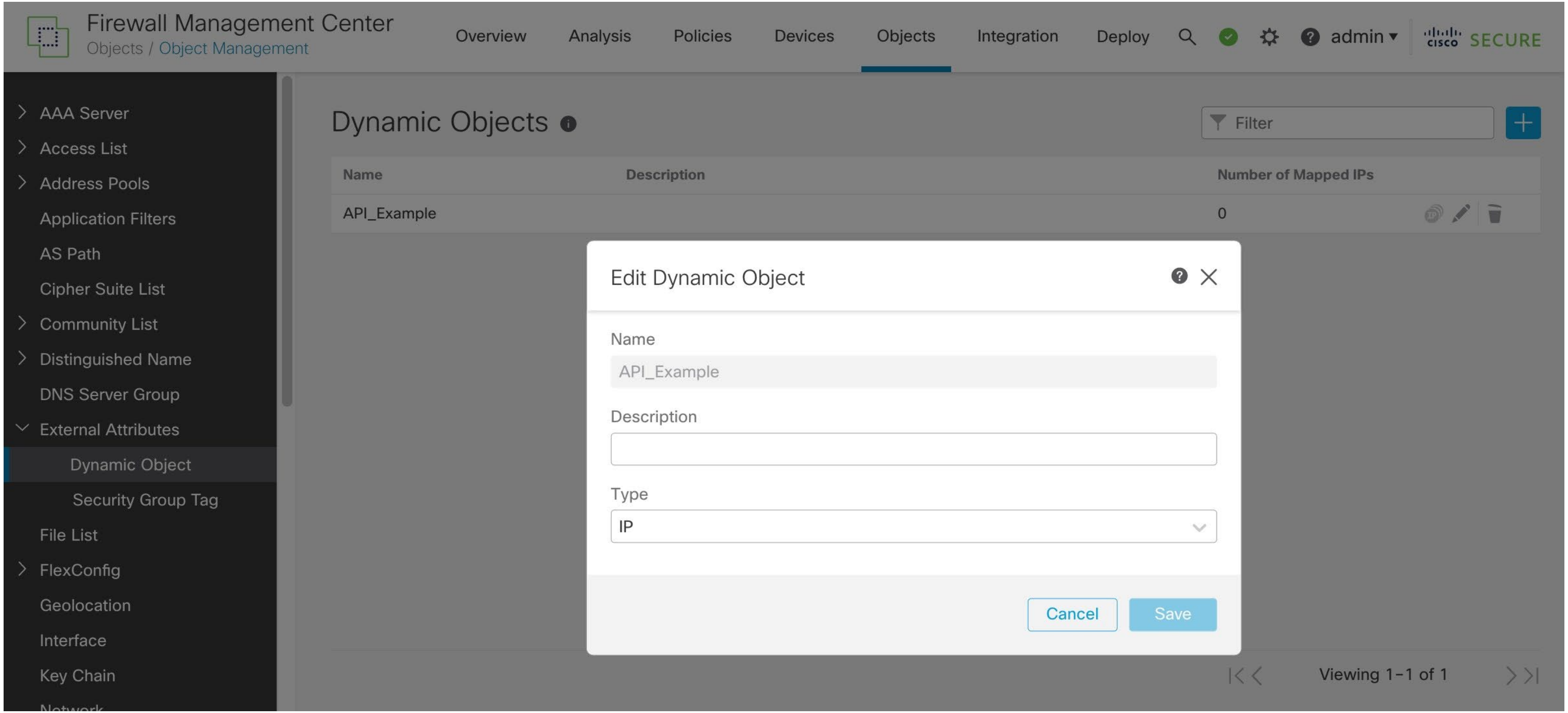


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dynamic Objects API Demo

Demo Setup

Create Dynamic Object (Can Also Be Done via API)



Dynamic Objects

Name	Description	Number of Mapped IPs
API_Example		0

Edit Dynamic Object

Name: API_Example

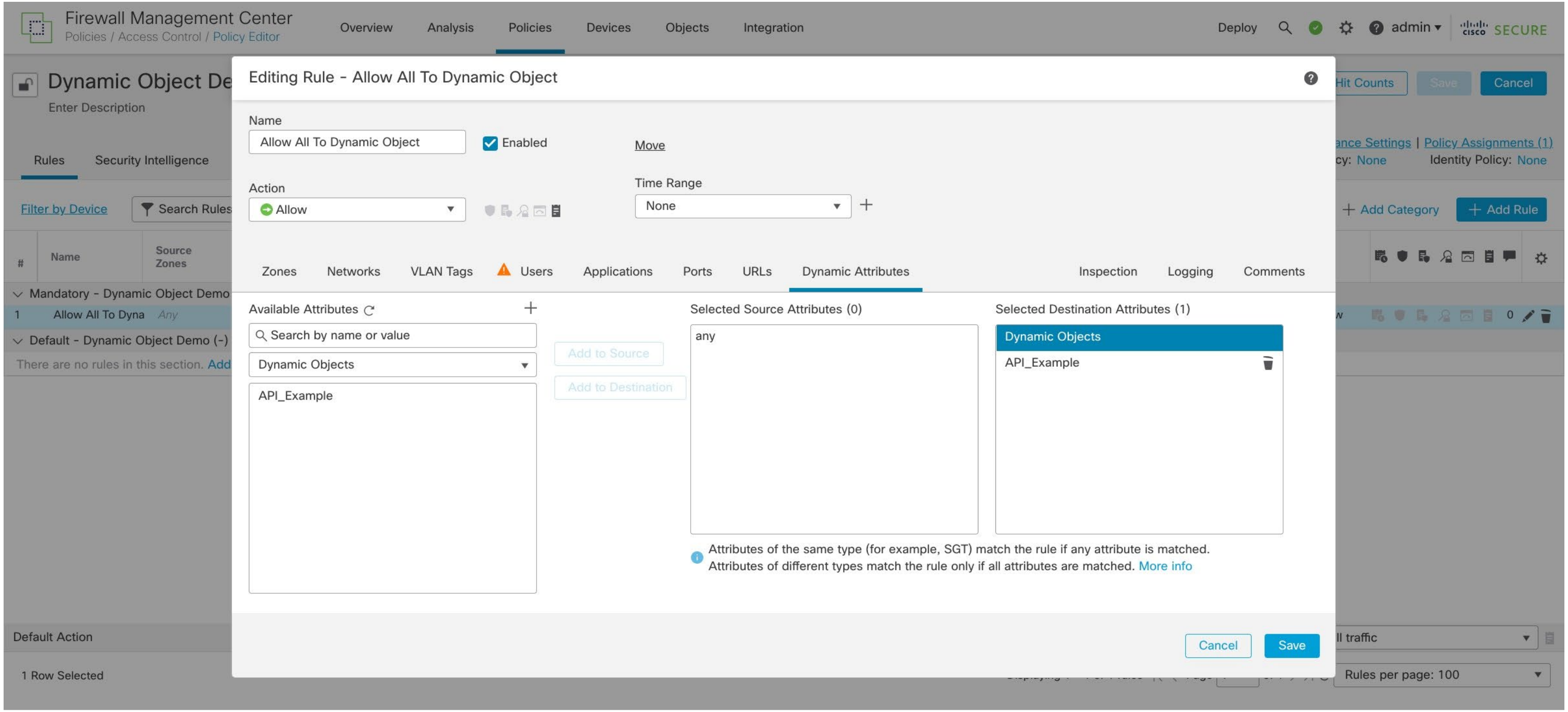
Description:

Type: IP

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

Demo Setup

Apply Dynamic Object to Access Control Policy



Editing Rule - Allow All To Dynamic Object

Name: Allow All To Dynamic Object

☑ Enabled

Action: Allow

Time Range: None

Available Attributes

Dynamic Objects

API_Example

Selected Source Attributes (0)

any

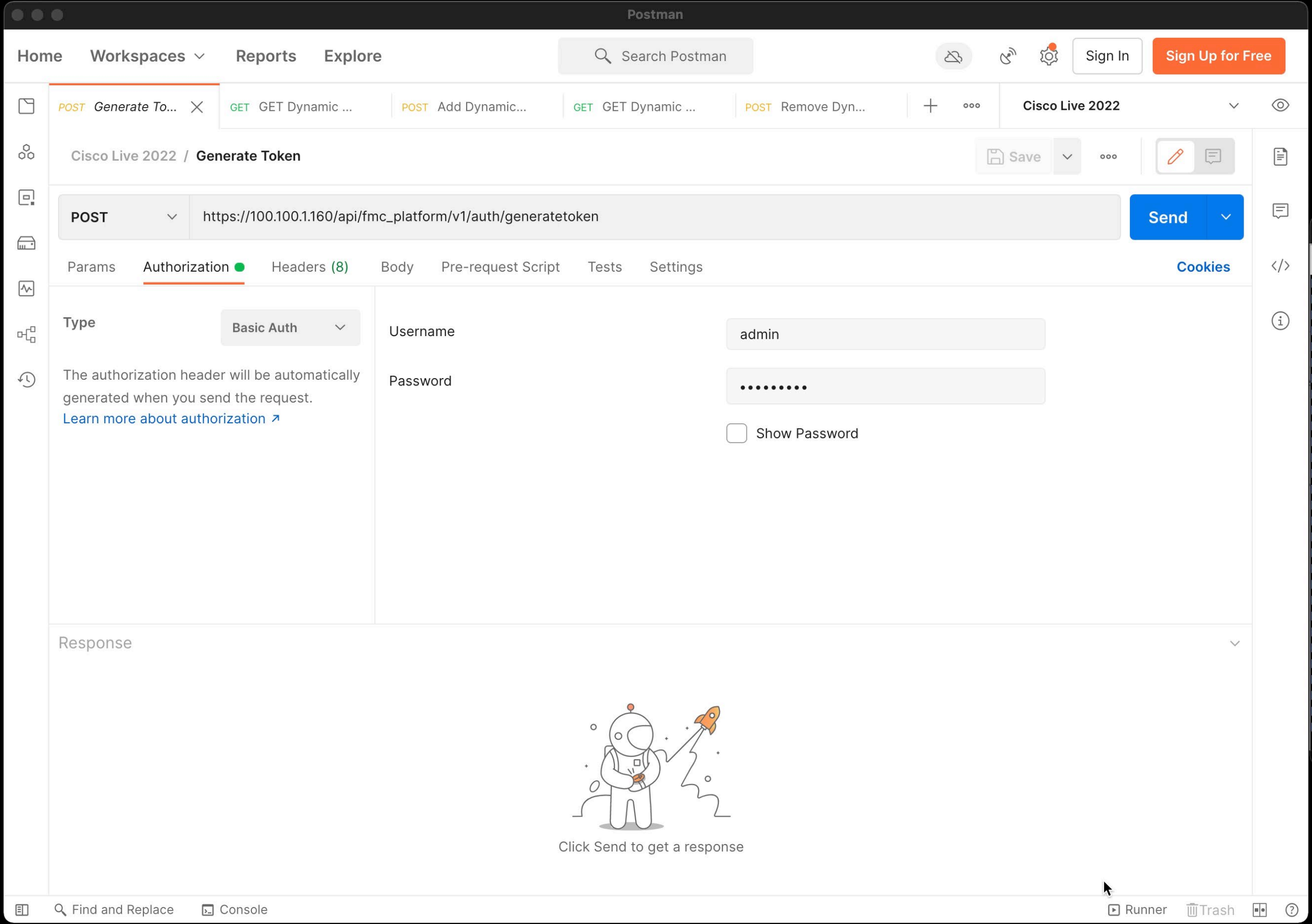
Selected Destination Attributes (1)

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

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



Cisco Live 2022 / Generate Token

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

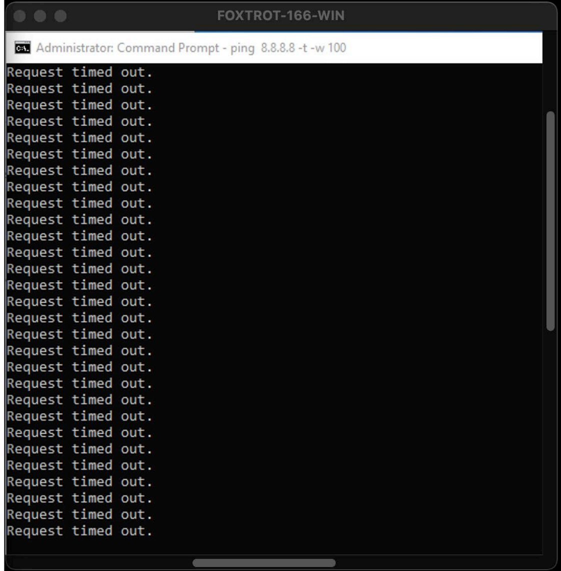
Type: Basic Auth

The authorization header will be automatically generated when you send the request.

Username: admin

Password: ••••••••••

□ Show Password



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.
```

7.0

Options for Implementing Dynamic Attributes

🟦 Admin Handled / 🟩 System Handled or Assisted

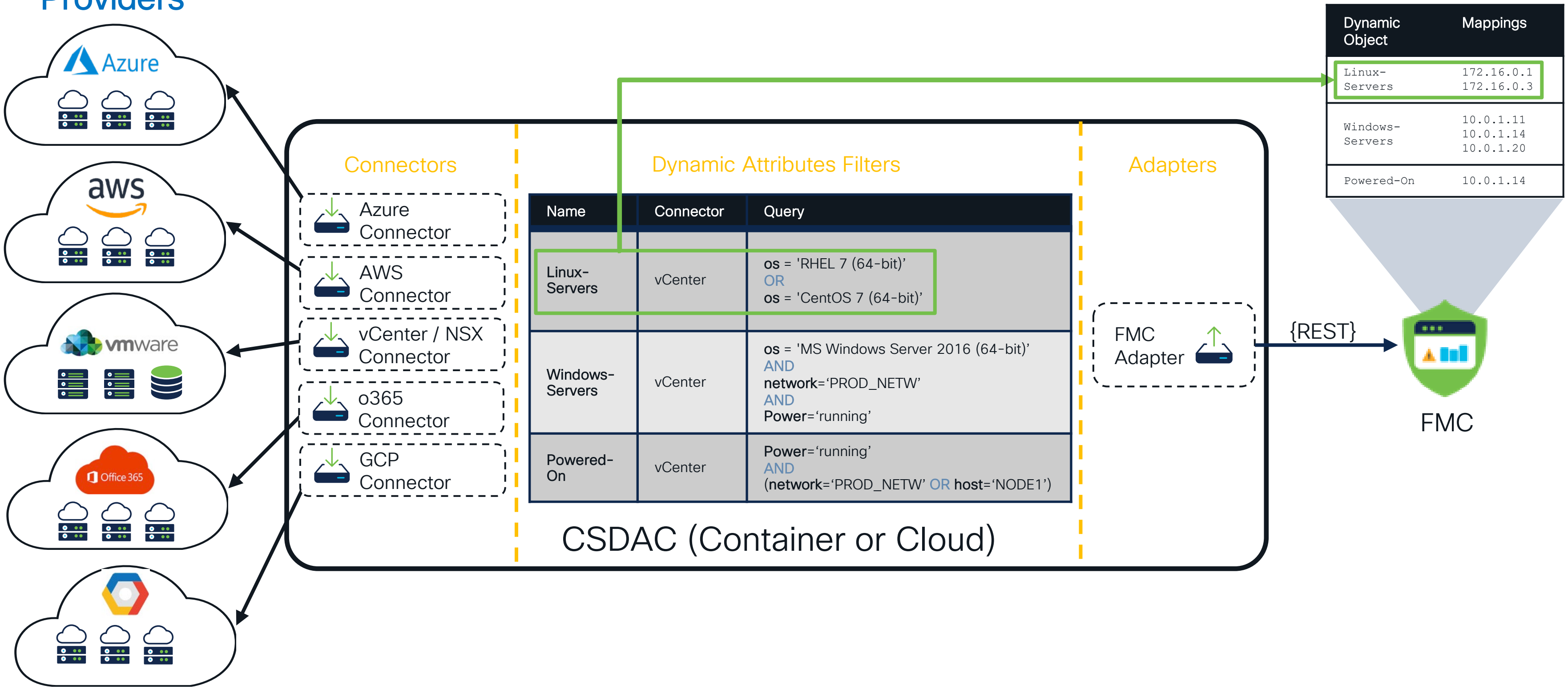
Dynamic Attribute FMC API	Cisco Secure Attribute Connector (CSDAC)	Cisco Secure Workload
🟦 Define Policy	🟦 Define Policy	🟩 Define Policy
🟦 Define Dynamic Objects	🟦 Define Dynamic Objects	🟩 Define Dynamic Objects
🟦 Interact w/ Upstream API(s)	🟩 Interact w/ Upstream API(s)	🟩 Interact w/ Upstream API(s)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

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

7.0

Cisco Secure Dynamic Attributes Connector

Providers



Name	Connector	Query

Linux-Servers	vCenter	os = 'RHEL 7 (64-bit)'
		OR
		os = 'CentOS 7 (64-bit)'

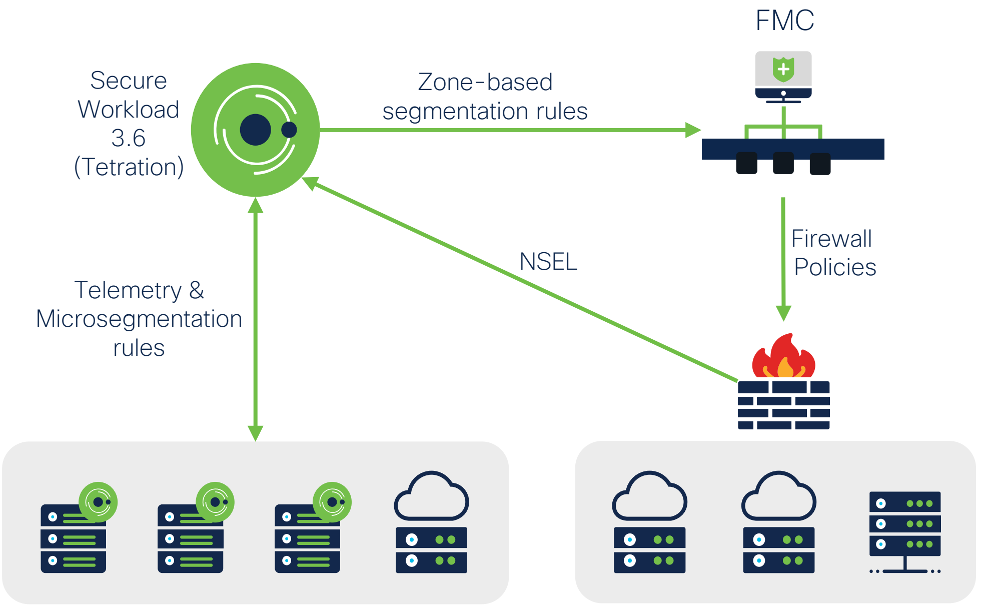
Windows-Servers	vCenter	os = 'MS Windows Server 2016 (64-bit)'
		AND
		network='PROD_NETW'
		AND
		Power='running'

Powered-On	vCenter	Power='running' AND (network='PROD_NETW' OR host='NODE1')

Dynamic Object	Mappings
Linux-Servers	172.16.0.1 172.16.0.3
Windows-Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14

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

Secure Workload Dynamic Policy Integration


FMC
Secure Workload 3.6 (Tetration)
Zone-based segmentation rules
NSEL
Firewall Policies
Telemetry & Microsegmentation rules

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.

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

Technical Session Surveys

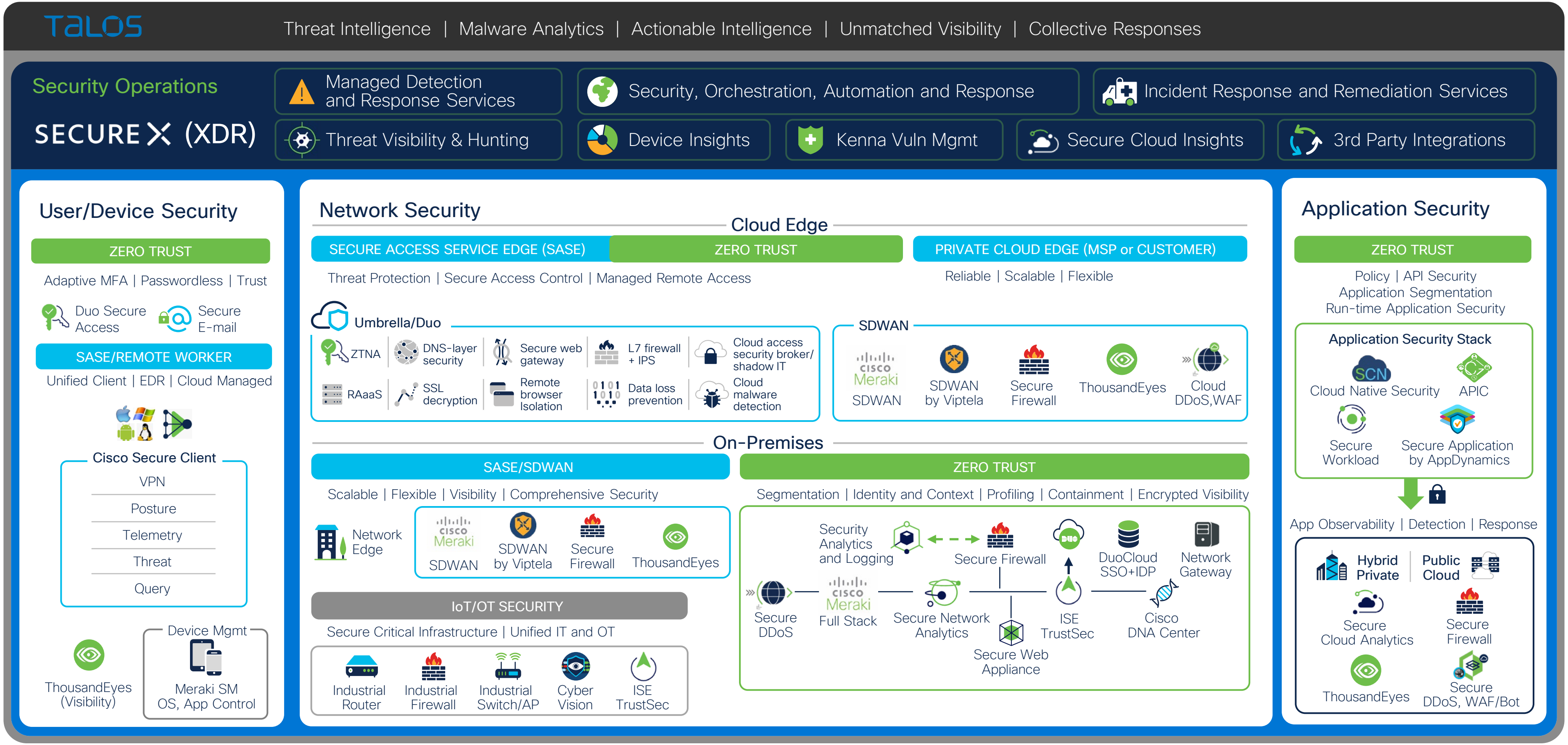
- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

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

CISCO SECURE

Security Reference Architecture



Talos

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN

- Cisco Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Cisco Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DUO
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Cisco Meraki Full Stack
- Secure Network Analytics
- ISE TrustSec
- Cisco DNA Center
- Secure Web Appliance

Application Security

ZERO TRUST

Policy | API Security

Application Segmentation

Run-time Application Security

Application Security Stack

- SCN Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

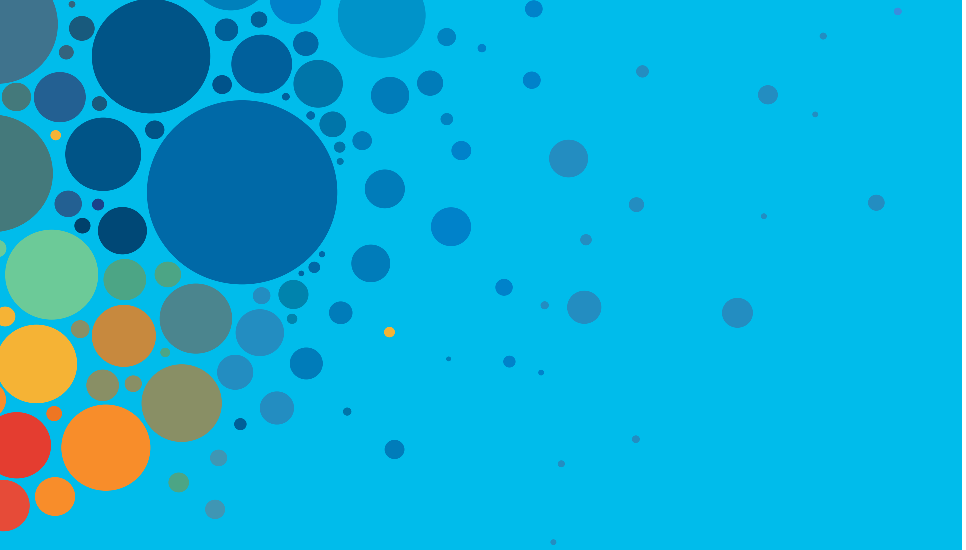
Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at The Learning and Certifications lounge at the World of Solutions

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



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

The bridge to possible

Thank you

cisco Live!

#CiscoLive