

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright white sunburst graphic that radiates across the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

Keeping Up on Network Security with Cisco Secure Firewall

Andrew Ossipov
Distinguished Engineer, Portfolio CTO
BRKSEC-2236

CISCO *Live!*

#CiscoLiveAPJC



“Reconciliation”- Dustin Koa Art

Your Speaker

Andrew Ossipov

aeo@cisco.com

Distinguished Engineer

Portfolio CTO for Cloud and Network Security

Firewall Architecture, Threat Visibility, Hybrid Cloud



Cisco Webex App

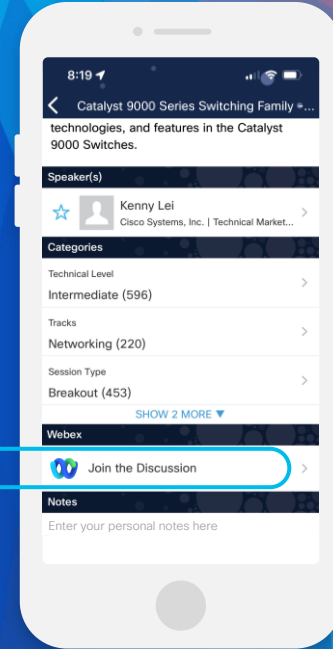
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2236>

Agenda

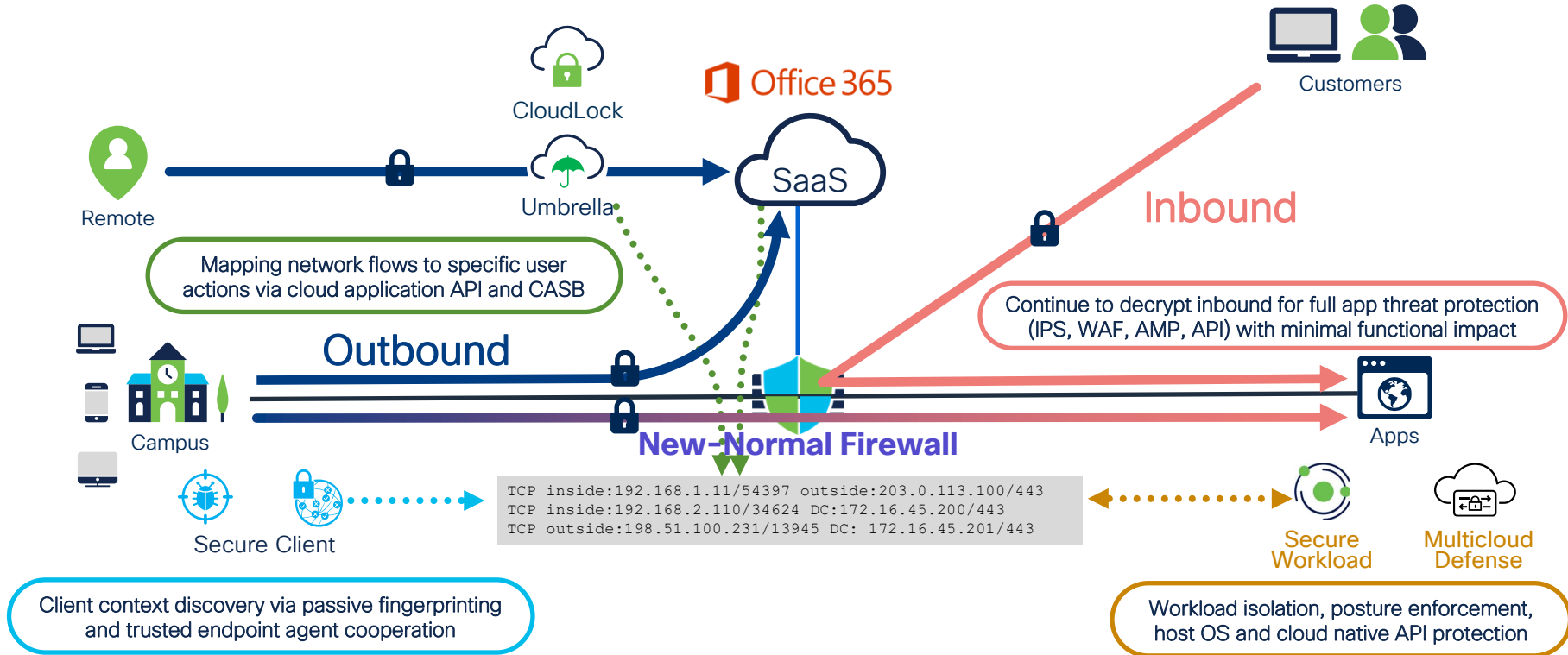
CISCO *Live!*



- Introduction
- Firewall
 - Platform
 - Threat Protection
 - Connectivity
 - Hybrid Work
 - Management
- Workload
- Conclusion

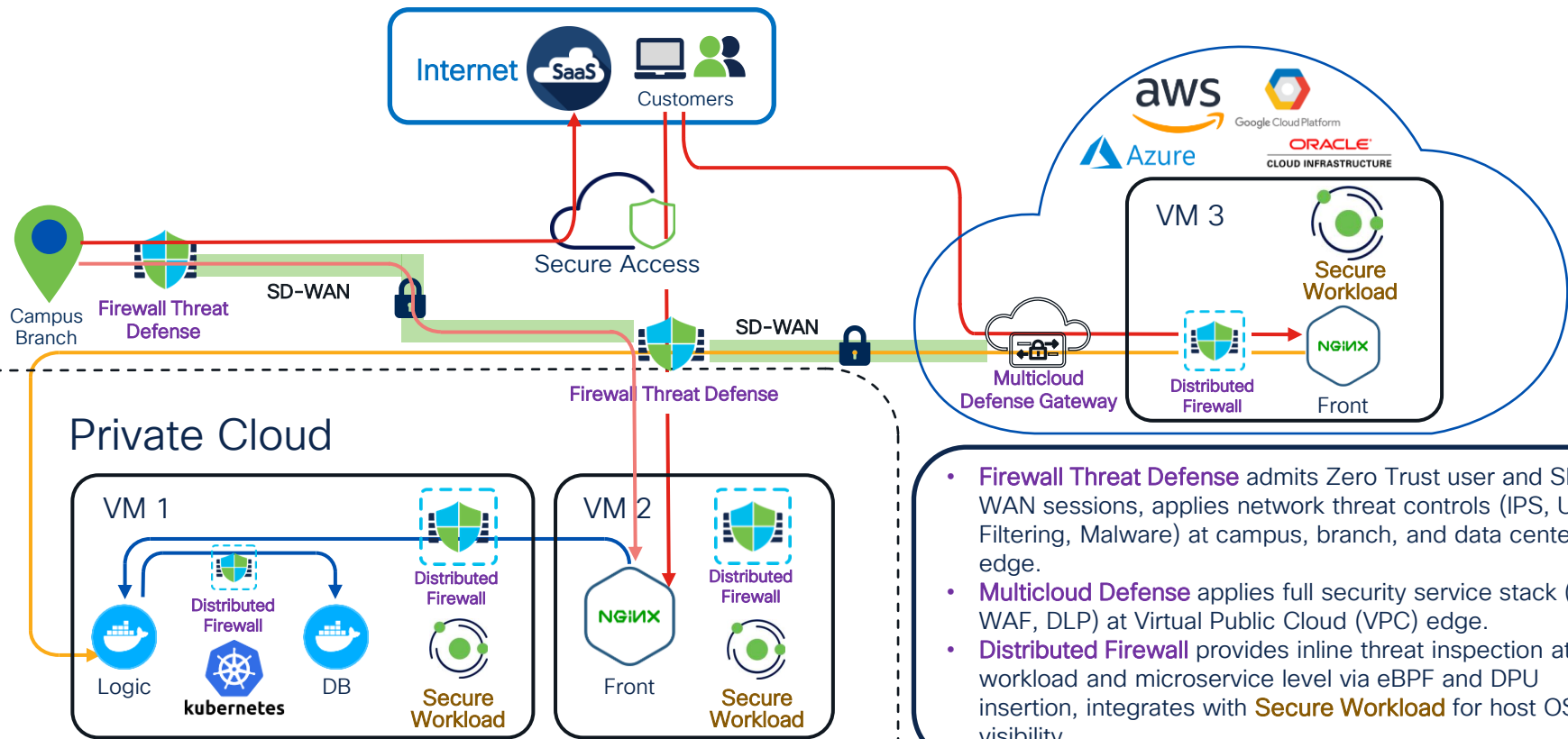


Secure Firewall: Inspect, Infer, and Cooperate



Firewall Vision: Network, Workload, and Cloud

Cisco Defense Orchestrator abstracts end-to-end policy intent from enforcement point specific configuration.



- **Firewall Threat Defense** admits Zero Trust user and SD-WAN sessions, applies network threat controls (IPS, URL Filtering, Malware) at campus, branch, and data center edge.
- **Multicloud Defense** applies full security service stack (IPS, WAF, DLP) at Virtual Public Cloud (VPC) edge.
- **Distributed Firewall** provides inline threat inspection at workload and microservice level via eBPF and DPU insertion, integrates with **Secure Workload** for host OS visibility.

Firewall Threat Defense 7.2.4 Software

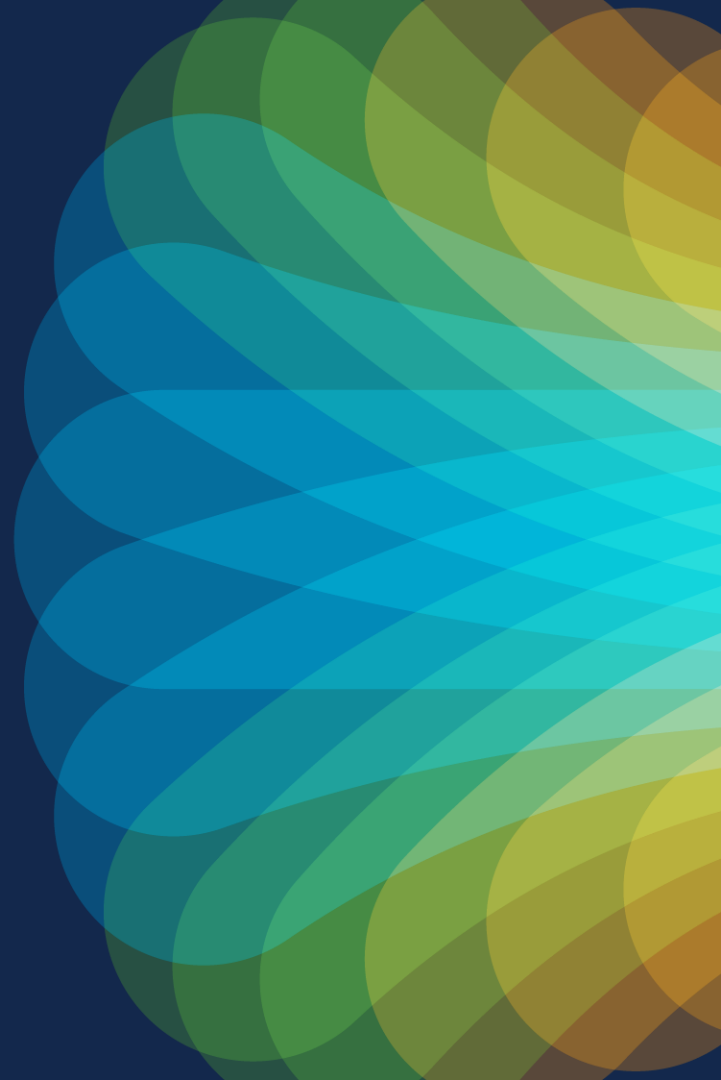


- Deliberate quality checkpoint in FTD 7.2 feature train
 - Database engine hardening across FTD and FMC
 - Resolve remaining Snort 3 operational issues
 - Tripled automated system test cases and resolved defects
- Intense focus on customer experience and outcomes
 - Validated against 100+ actual production deployments
 - Select enhancements to improve deployment times and scale
- Backport to 7.0.x and baseline for 7.4.x release trains

Suggested Release

7.2.5 ★

Platforms



Secure Firewall 4200 Overview

FTD
7.4

ASA
9.20

Appliance-Mode Security Platform for FTD or ASA Application

- Fixed configurations: 4215, 4225, 4245
- Lightweight virtual Supervisor module w/**Multi-Instance** and Clustering
- Integrated Datapath FPGA w/Flow Offload and Crypto Engine
- Rear dual redundant power supplies and triple fan trays

SFP Data Interfaces

- 8x1/10/25GE/**50GE**

1RU



NVMe Drives

- Up to 2x900GB in RAID1 on 4215/4225
- Up to 2x1.8TB in RAID1 on 4245

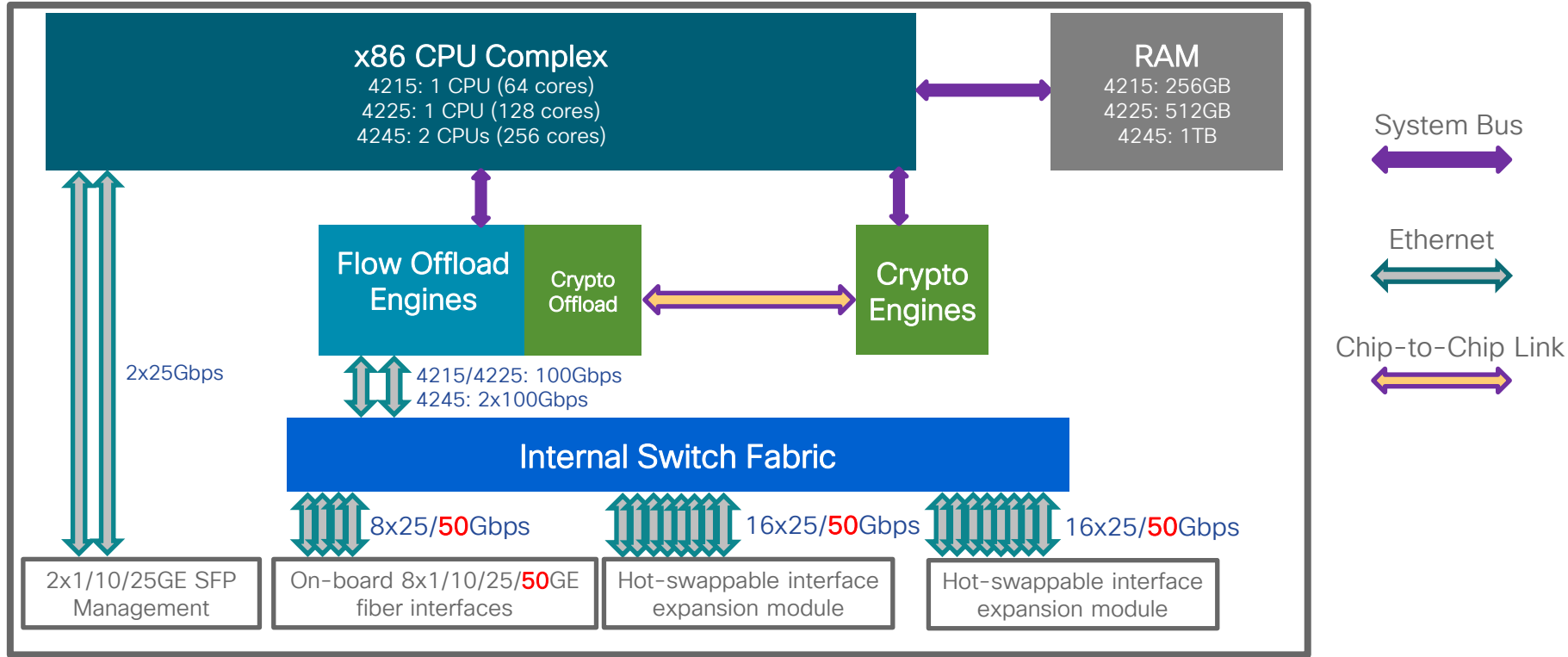
Expansion Network Modules

- Standard: 8x1/10GE, 8x1/10/25/**50GE**, 4x10/40GE, 2x100GE, 4x40/100/200GE, **2x200/400GE** SFP+
- Fail-to-Wire: 8x1GE Copper; 6x10GE or 6x25GE SFP+ (SR and LR variants)

Secure Firewall 4200 Architecture

FTD
7.4

ASA
9.20



Secure Firewall 4200 Performance



	4215	4225	4245
FW+AVC+IPS HTTP 1024B Avg Packet	65Gbps	85Gbps	145Gbps
IPsec VPN HTTP 1024B Avg Packet	45Gbps (45Gbps per tunnel)	80Gbps (57Gbps per tunnel)	140Gbps (57Gbps per tunnel)
TLS Decryption HTTP 1024B Avg Packet 50% Flows Decrypted	20Gbps	30Gbps	45Gbps

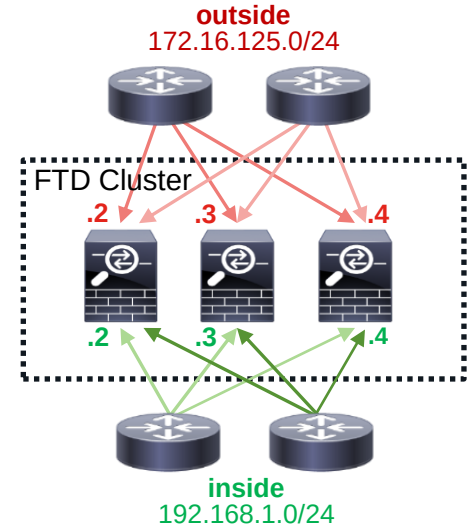
Up to **3x**  Boost in
FW+AVC+IPS

Up to **6x**  Boost in
IPsec VPN

Up to **5x**  Boost in
TLS Decrypt

Individual Mode Clustering

- Hybrid cloud is driving Layer 3 centric data center topologies
 - No Layer 2 Port Channels in public cloud
 - Equal Cost Multi-Path (ECMP) with dynamic routing
- Clusters can use individual data interfaces
 - Already supported on ASAv/FTDv for hybrid cloud
 - Each data interface has its own IP address
 - Each unit runs an independent routing instance



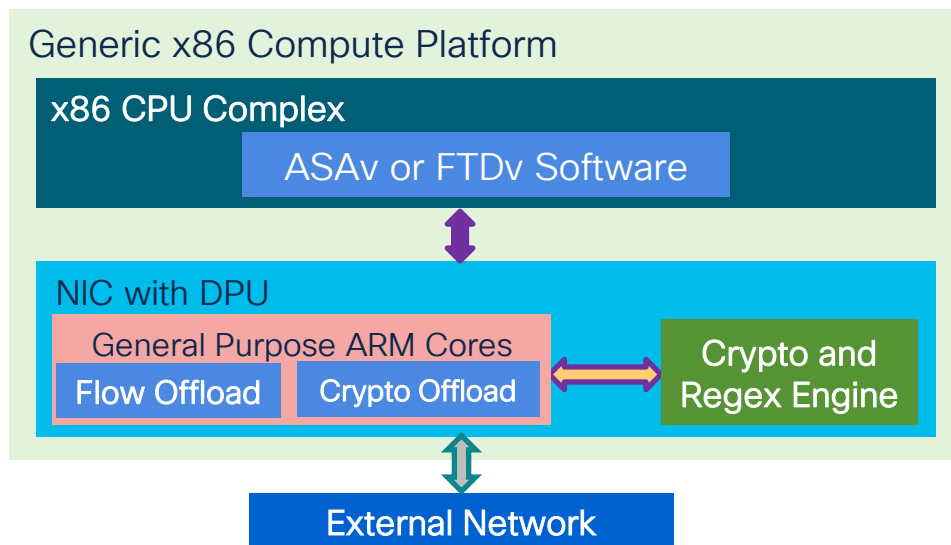
Data Processing Unit (DPU): Distributed Firewall

Future

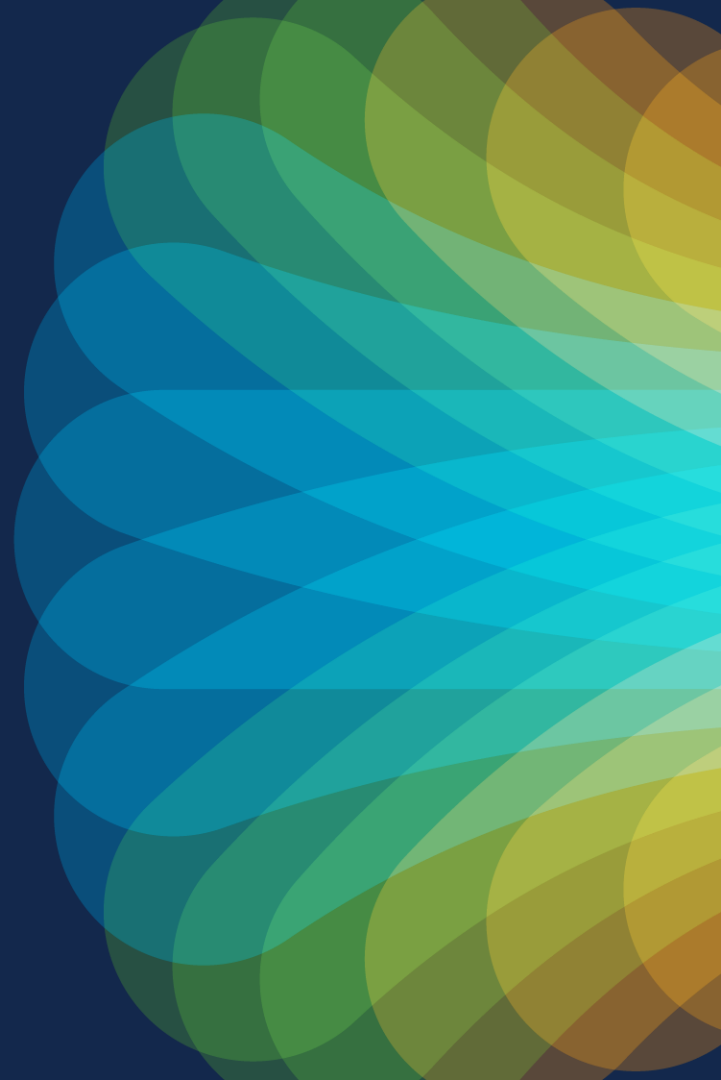
- Network Interface Controller (NIC) with a DPU in a server or switch
 - Inline hardware acceleration for broad packet processing functionality
 - Perfect opportunity to accelerate and scale firewall in hybrid data centers

ASAv/FTDv software and Multicloud Defense is deployed on x86 CPU in generic private and public cloud environments.

If a DPU is present, additional ARM software components program inline acceleration of flow processing, IPsec and (D)TLS encryption, Regex matching, and other capabilities.



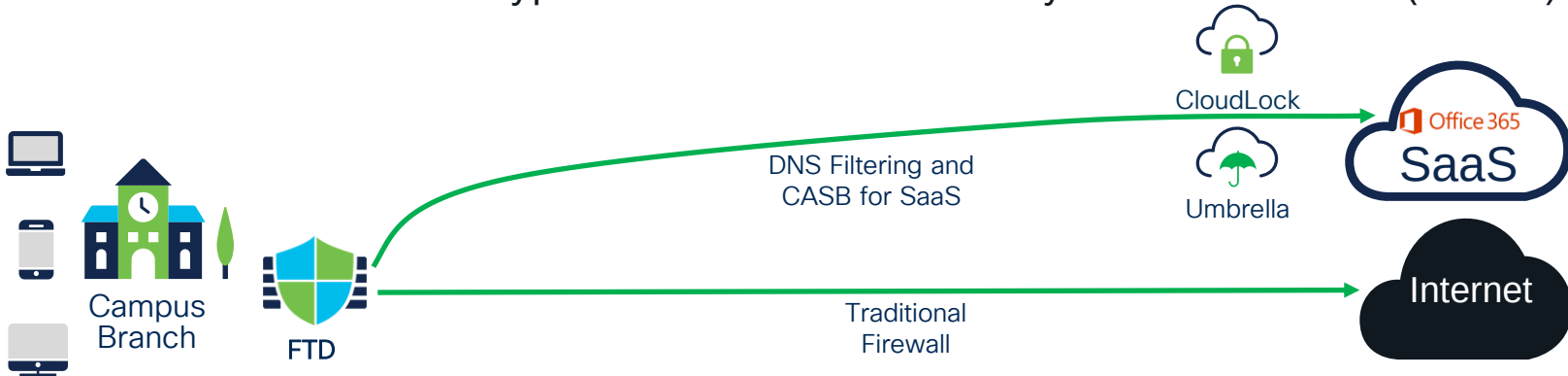
Threat Protection



Enhance Firewall with Umbrella Cloud Security

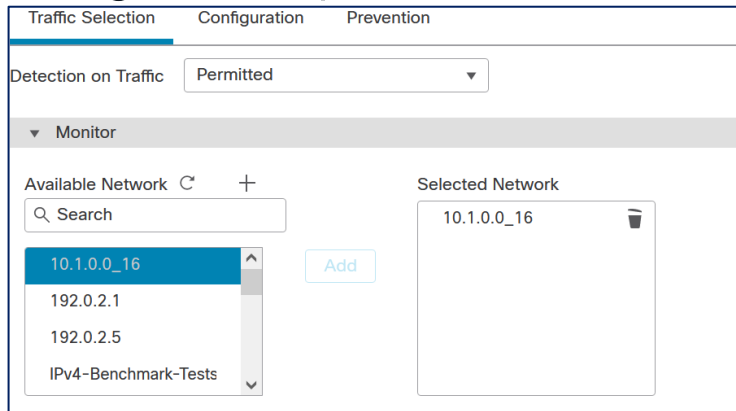
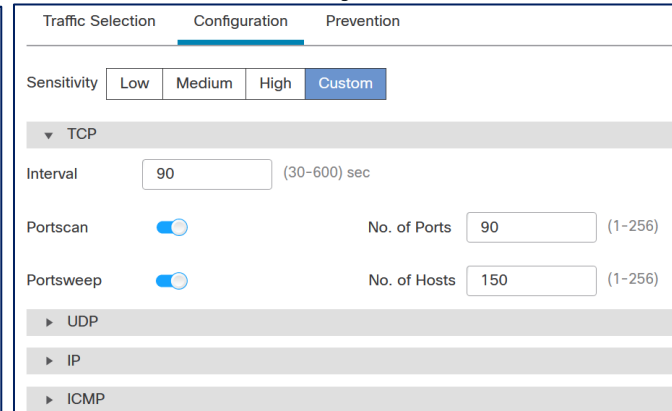
FTD
7.2+

- Edge firewall is less effective against some outbound traffic
 - Dynamically changing DNS and undecryptable TLS connections
- Selectively redirect DNS, SaaS, and other traffic to Umbrella instead
 - Cloud-delivered DNS blocks most threats early with no local cycles spent
 - No SaaS traffic decryption with Cloud Security Access Broker (CASB)

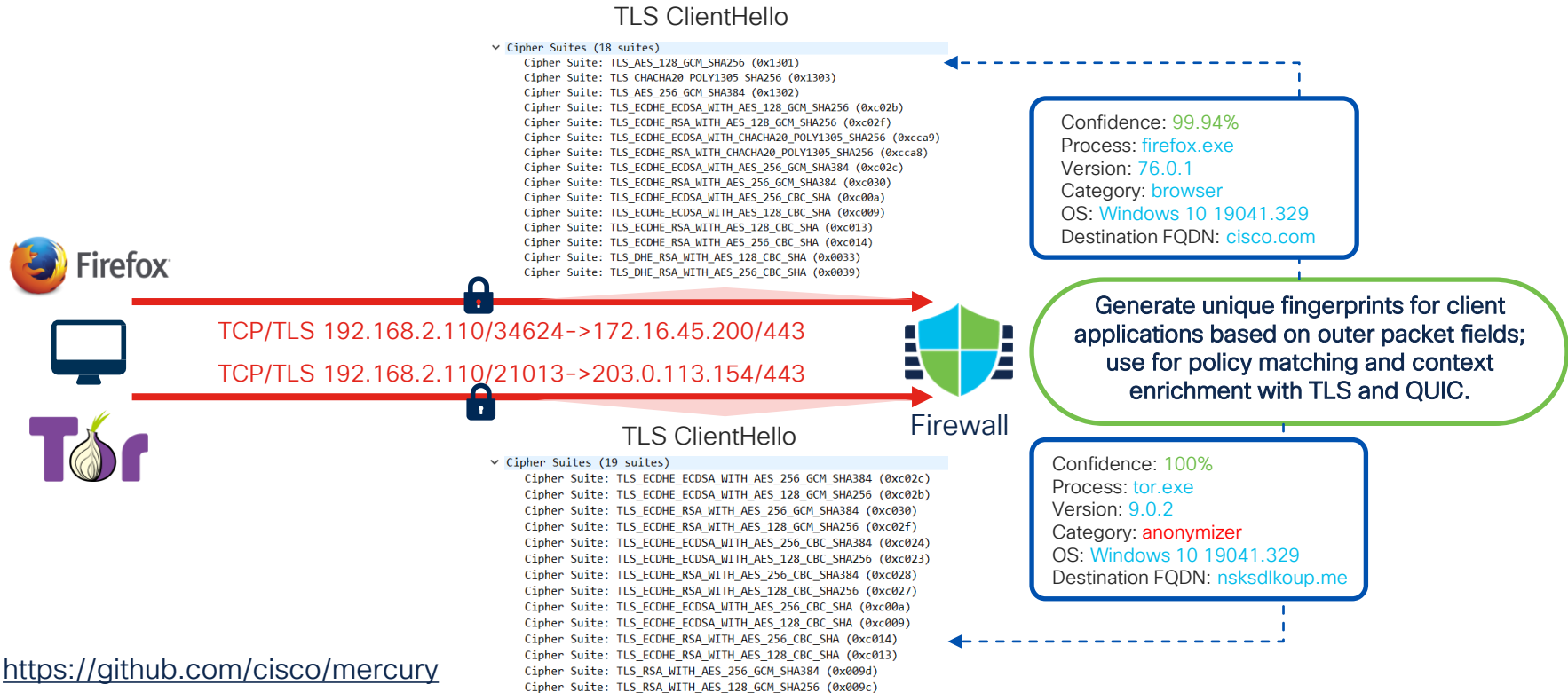


Portscan Detection and Prevention

- Evolved Portscan protection engine directly within Data Plane
 - Much higher performance and detection efficacy
 - Recognizes single-host, decoy-based, distributed, and port sweep scans
 - Optional time-based blocking of potential attackers
- Granular configuration profiles at Access Control Policy level



Encrypted Visibility Engine (EVE)



<https://github.com/cisco/mercury>

EVE-enriched Unified Events

FTD
7.1

Client process name and detection confidence score; the name can be linked to a custom AppID for enforcement in FTD 7.2.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

alex

Inference-based threat alert and confidence level.

Encrypted Visibility Engine (EVE) 2.0

FTD
7.4

Encrypted Visibility Engine

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. [Learn more](#)

Recommended Settings

- [Enable](#) automatic updates for future Cisco Vulnerability Database (VDB) releases.
- [Enable](#) Cisco Success Network.

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

EVE Enhanced Analytics

Add EVE's fingerprint information in the connection events.

Block Traffic Based on EVE Score

Customize your threshold for blocking traffic based on the EVE scores.

Advanced Mode

Very Low

Low

Medium

High

Very High

Block

Revert to Defaults

Cancel

OK

Inference-based AppID enrichment.

Detailed fingerprint data for third-party use.

Connection filtering based on malware confidence scores.

AppID Portal: <https://appid.cisco.com>

Now

Mirrors full AppID information that is available in Firewall Management Center.

Cisco Vulnerability Database (VDB) Release Notes 365

Q 365

(Type a VDB release between 343 - 365)

Encrypted Visibility Engine Reference Details:

```
/*
 disclaimer: EVE resource files are automatically generated with
 real-world data. Older, less-relevant data is aged out, which
 leads to natural churn and can result in some month-to-month
 variations in the data.
*/
```

resources version: 2023.05.18

stats:

general:

total fingerprints: 39,860
total labeled fingerprints: 6,930
total connections: 2,680,300,185
fingerprints per protocol:
http: 3,677
tls: 3,130
quic: 123

Full AppID database update information,
including EVE fingerprint data.

Threat Grid:

total fingerprints: 801
total connections: 3,041,256

Secure Firewall Application Detectors

Home Release Notes Support Documentation Resources Feedback

Search ultrasurf X Search

Risk	Business Relevance	Tags	Categories
Very Low	1,412 Very High 332	adds/installs other software 66	active directory 8
Low	891 High 976	adult content 37	ad portal 396
Medium	1,353 Medium 2,411	allows remote connect 90	anonymizer/proxy 102
High	1,630 Low 1,215	allows remote control 52	application development and testing 31
Very High	635 Very Low 987	antivirus 13	backup and recovery 9

Application Details (1) Release Notes (Ultrasurf): 354 349 348 347 346 345 343

Application Name	Description	Risk	Business Relevance
Ultrasurf	Freeware anti-censorship proxy.	Very High	Low

Tags: evasive, SSL protocol, encrypts communications, tunnels, NSG, encrypted visibility engine
Categories: vpn/tunnel, network protocols/services
Protocol: TCP
Request Application Support

CISCO Live!

Simplified TLS Decryption Policy

- Decryption is not required for all visibility
 - URL Filtering and some AppID work without
 - IPS and File/Malware policies imply full decryption
- Native TLS 1.2 and 1.3 decryption
- Wizard-style flow for Decryption policy
 - **Outbound** is ineffective for most SaaS apps
 - **Inbound** gives full control with access to app server

Create Decryption Policy

1 A decryption policy is not required to only perform application or URL discovery; instead, you can use TLS 1.3 Server Identity Discovery on the access control policy.

Name*
Decrypt DMZ Apps to Internet

Description
Decrypt all outbound traffic from DMZ on port TCP/443

Outbound Connections (User Protection) Inbound Connections (Server Protection)

How Outbound Protection Works
Outbound protection matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions.

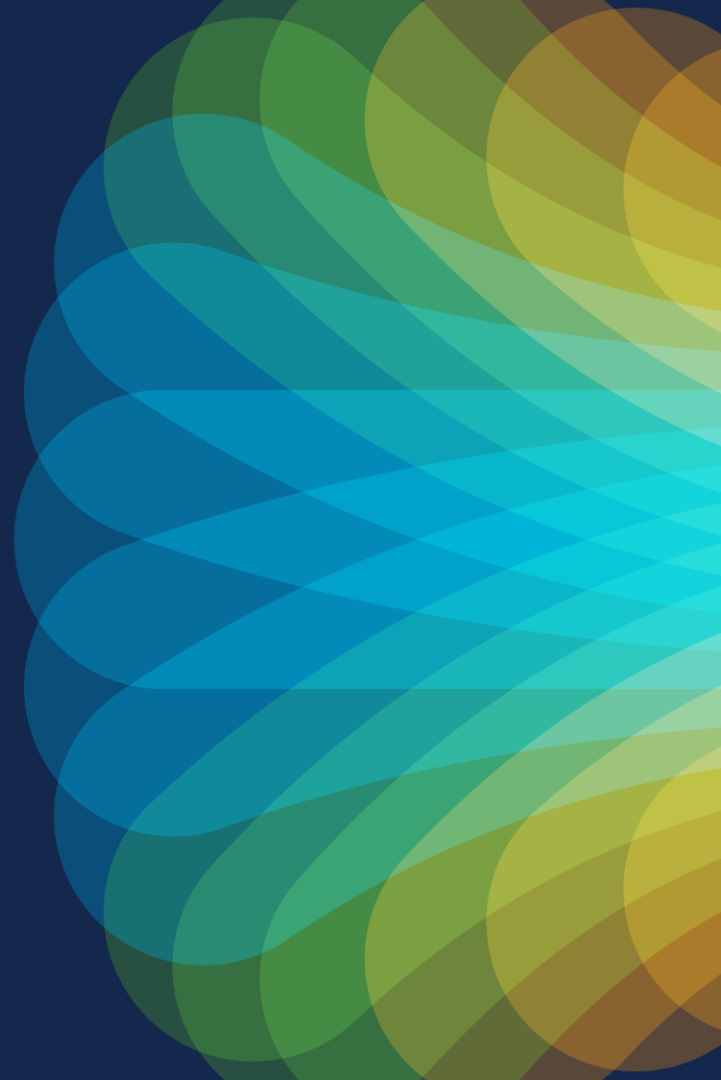
Internal CA
A rule will be auto-created for the selected certificate authority.

FMC_Self Associated: 2 Networks, 1 Port

[See how to configure](#)

Cancel Save

Connectivity



Application-Aware Policy Routing

- Native support for Policy Based Routing configuration in FMC
 - Commonly used SaaS applications can be used as matching criteria
 - DNS snooping to Trusted Servers to support domain pattern matching
 - Data Plane maps app names to IP addresses with Network Service Groups
- Used in Direct Internet Access (DIA) breakout in WAN deployments

Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

[Configure Interface Priority](#) [Add](#)

Ingress Interfaces	Match criteria and forward action	
inside	<p>If traffic matches the Access List WebEx_Direct_Internet_Access</p> <p>SaaS application aware first packet match.</p> <p>Send and load balance it through</p> <ul style="list-style-type: none">#0 ISP1#0 ISP2 <p>If above link fails, Send through</p> <ul style="list-style-type: none">#1 ISP-Backup <p>Flexible egress interface selection policy, including ECMP over cleartext or VPN tunnels.</p>	

Path Monitoring and Quality-Based Routing

- Policy-based interface selection can be influenced by path quality
 - ICMP-based next-hop or external IP monitoring on each interface
 - HTTP(S)-based SaaS app tracking in **FTD 7.4**

Add Forwarding Actions

Match ACL:* Youtube +

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter ⓘ

Available Interfaces

Search by interface name 🔍

Interface	
Inside	+
Outside	+

No interfaces selected

Jitter: Jitter is the term used to refer to variation in latency (rtt) of packet flow from endpoint to endpoint.

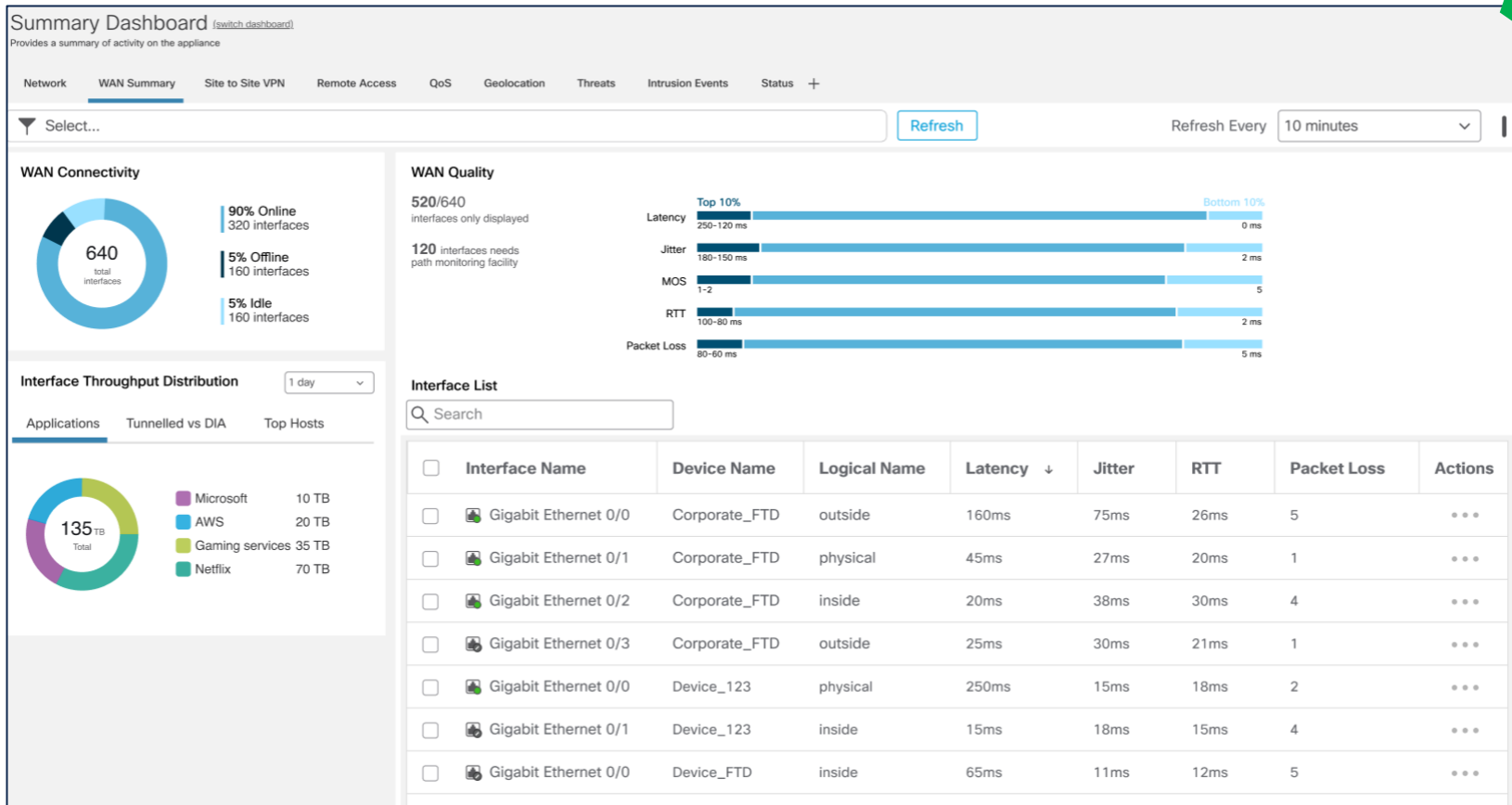
RTT: The Round-trip Time (RTT) is the duration, measured in milliseconds, from when a monitoring node sends an ICMP echo request to when it receives an ICMP reply from a remote node.

Packet-Loss: Packet loss describes packets of data not reaching their destination after being transmitted across a network. Packet loss is commonly caused by network congestion, hardware issues, software bugs, and several other factors.

MOS: Mean Opinion Score (MOS) is a way of quantifying the quantitative experience of a connection. Commonly used in streaming sessions where network effects can degrade communications quality. Audio and video communications are evaluated using this metric.

SD-WAN Monitoring Dashboard

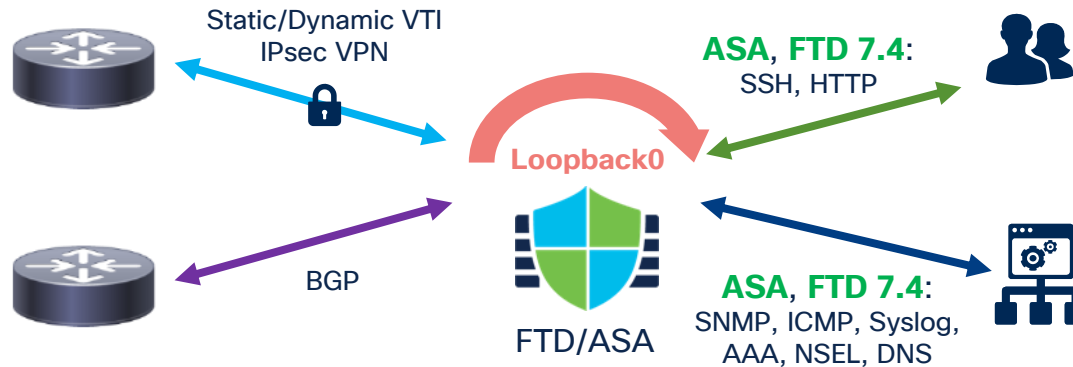
FTD
7.4



Loopback Interface



- Abstract to- and from-device connectivity from physical interfaces
 - IPv4/IPv6 addressing in routed and transparent (except for VTI) modes
 - HA/failover and clustering (except for VTI) support



Elephant Flow Detection

- Per-flow tracking replaces Intelligent Application Bypass (IAB)

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** MB and flow duration **exceeds** seconds

Elephant flow Remediation ☒ ?

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

Then Bypass the flow ☐

Or Throttle the flow ☒

[Revert to Defaults](#) [Cancel](#) [OK](#)

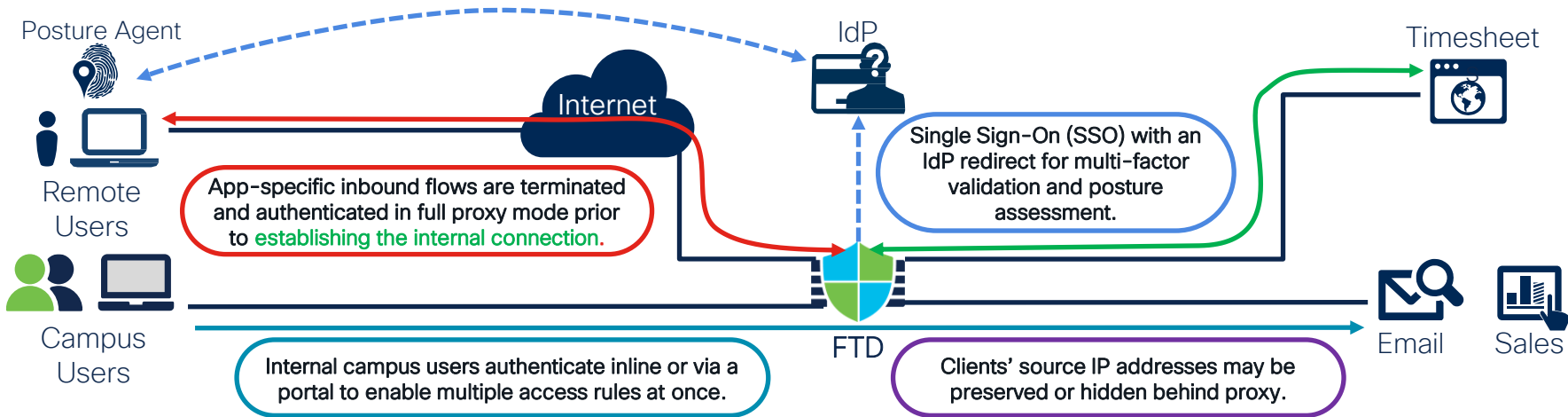
Throughput threshold to qualify as an Elephant Flow

Optional flow-specific CPU resource consumption and packet drop thresholds for remediation.

Optional flow remediation actions.

Clientless Zero Trust App Access (ZTAA)

- Expand Captive Portal capabilities into a full reverse proxy
 - External Identity Provider (IdP) integration with posture assessment
 - Future support for internal (“BeyondCorp”) segmentation



Clientless ZTAA: App Definition

Add Application

Enabled ☒

1 Application Settings

Application Name
External URL
Application URL
Application Certificate
Application Group

2 SAML Service Provider (SP) Metadata

Entity ID
Assertion Consumer Service (ACS) URL

3 SAML Identity Provider (IdP) Metadata

Entity ID
Single Sign-On URL
IdP Certificate

4 Re-Authentication Interval

Timeout Interval
1440 minutes

5 Interface Access and Security Controls

Security Zones
Intrusion Policy
Variable Set
Malware and File Policy

Payroll

<https://payroll.acme.com>
<https://payroll-prod.acme.private>
PayrollApp
-

<https://payroll.acme.com/saml/sp/metadata/payroll.acme.com>
<https://payroll.acme.com/+CSCOE+/saml/sp/acs?tname=DefaultZeroTrus...>

<https://www.okta.com/exk08Ko9uope1>
https://dev-100.okta.com/app/dev-11111_payroll/exk08Ko9uope1
test

Overridden (Outside-DMZ)
Overridden (Balanced Security and Connectivity)
Overridden (Default-Set)
Overridden (Block Malware)

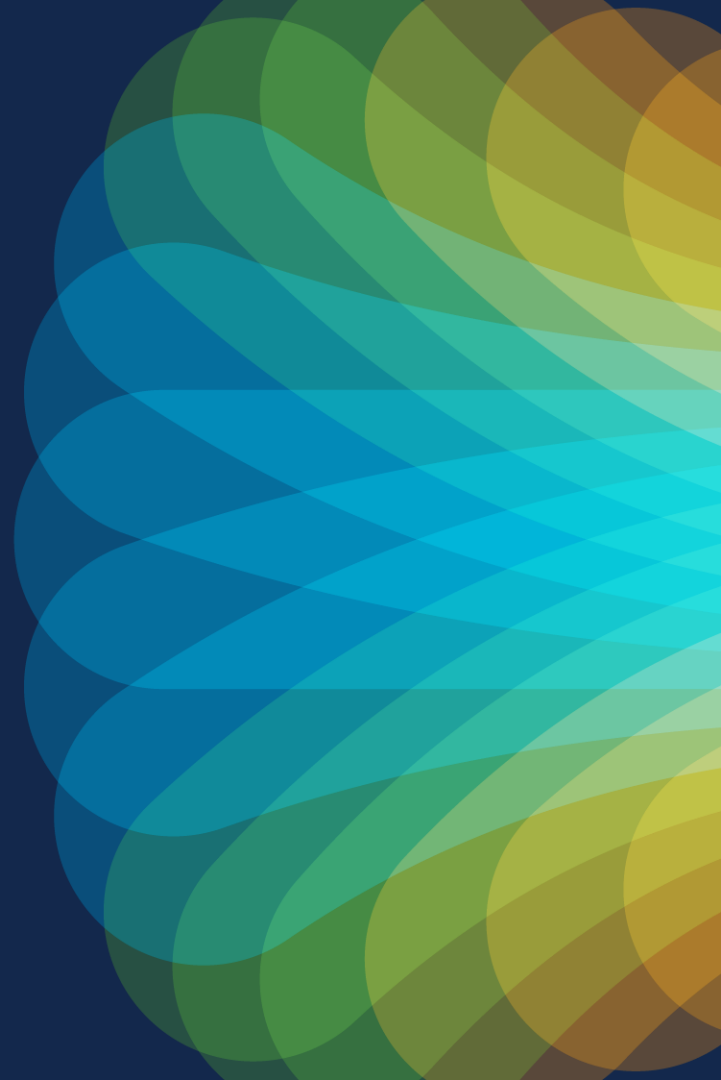
Cancel Finish

How the end user accesses the application (External URL) and how FTD makes the connection (Internal URL or IP).

Any SAML-enabled IdP can be used for any individual application.

Application-specific or default IPS and File Policies apply; positive access control policy verdict and full TLS decryption are implied.

Hybrid Work



Consistent Protection in Hybrid Cloud

Private Cloud



HyperFlex



NUTANIX



Public Cloud

Microsoft
Azure

Google Cloud Platform

rackspace
technology

EQUINIX

ORACLE
CLOUD INFRASTRUCTURE

Alibaba Cloud

alkira

Secure Firewall Capabilities

Accelerated Networking

Snapshot-Based Instantiation

Gateway Load-Balancer
insertion and FWaaS

Clustering & Auto Scaling

Infrastructure-as-Code and
Automation for agilityIntegration with cloud services
and management

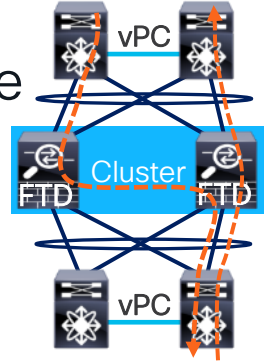
Dynamic Policy

Smart & Tiered Licensing

Clustering for Virtual Firewalls



- Clustering combines multiple firewalls into one logical device
 - Seamless scalability up to 16 FTD units with no traffic disruption
 - Stateful handling of asymmetric traffic and failure recovery
 - Single point of management and unified reporting
- Better elasticity and failure handling in hybrid cloud with clustering



- Individual data interface IP addresses instead of a single Port-channel
- VxLAN-based Cluster Control Link for unicast control plane
- No source NAT requirement for handling traffic asymmetry
- Existing flow re-hosting on failure in supported environments

Automation with Infrastructure-as-Code

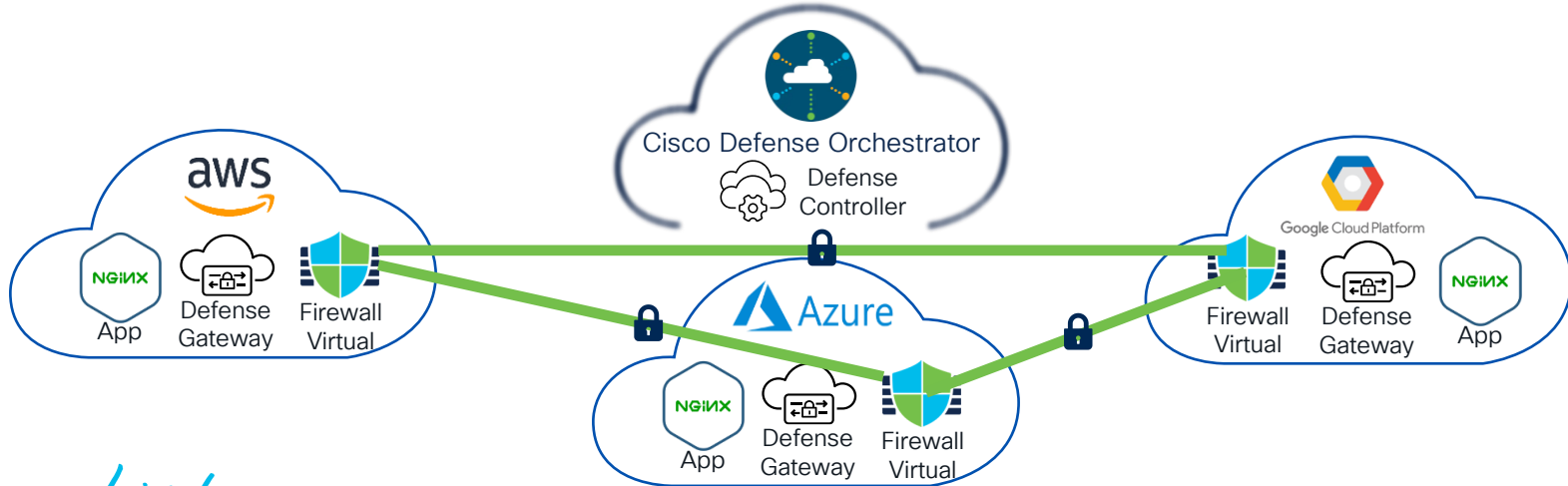


- Secure Firewall instantiation with public cloud templates
- Declarative Teraform templates for ASA and FTD (via FMC)
 - FTD Dynamic Object integration with HashiCorp Consul
- Imperative Ansible tasks for ASA and FTD (FDM and FMC)
- Continuously updated Cisco DevNet repositories
 - <https://developer.cisco.com/secure-firewall/cloud-resources/>
 - <https://github.com/CiscoDevNet/secure-firewall>
 - <https://github.com/CiscoDevNet/FMCAnsible>

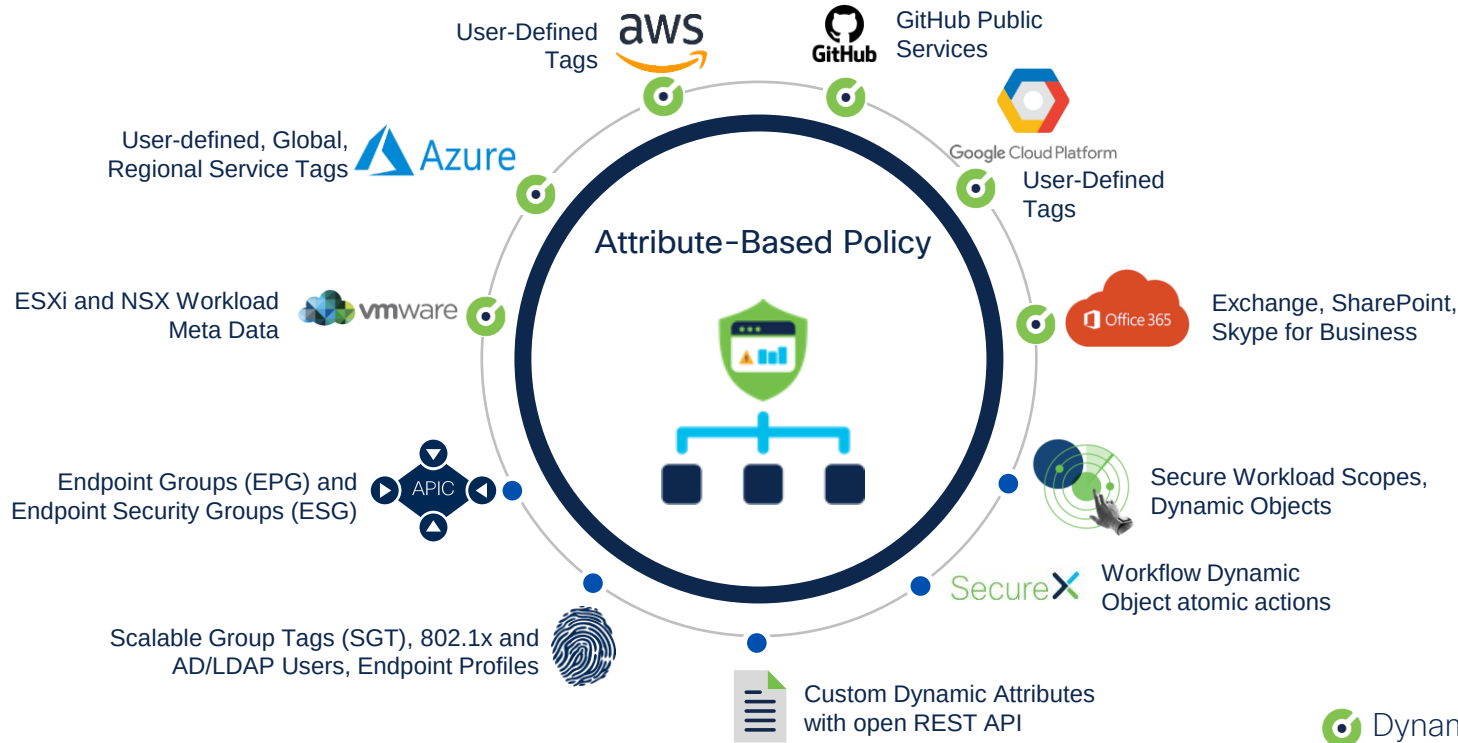


Cisco Multicloud Defense

- Comprehensive and consistent VPC edge security in public clouds
 - Multicloud Defense Gateway: Firewall, IPS, WAF, DLP, reverse proxy
 - Inter-cloud and private cloud IPsec interconnect with ASA/FTDv
 - Fully orchestrated by Multicloud Defense Controller in CDO



Firewall Policy Abstraction

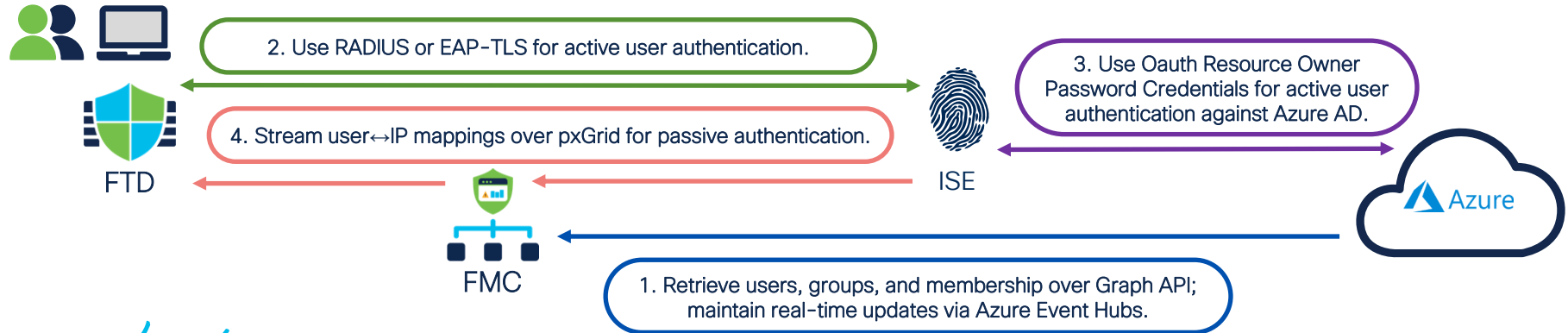


Dynamic Attribute Connector
 Firewall Management Center

User Identity from Azure AD with ISE

- A *very* different experience from Active Directory
- Passive user identity discovery in Access Control Policy
 - TLS Decryption and QoS support is **in the future**
 - No explicit Identity policy is required

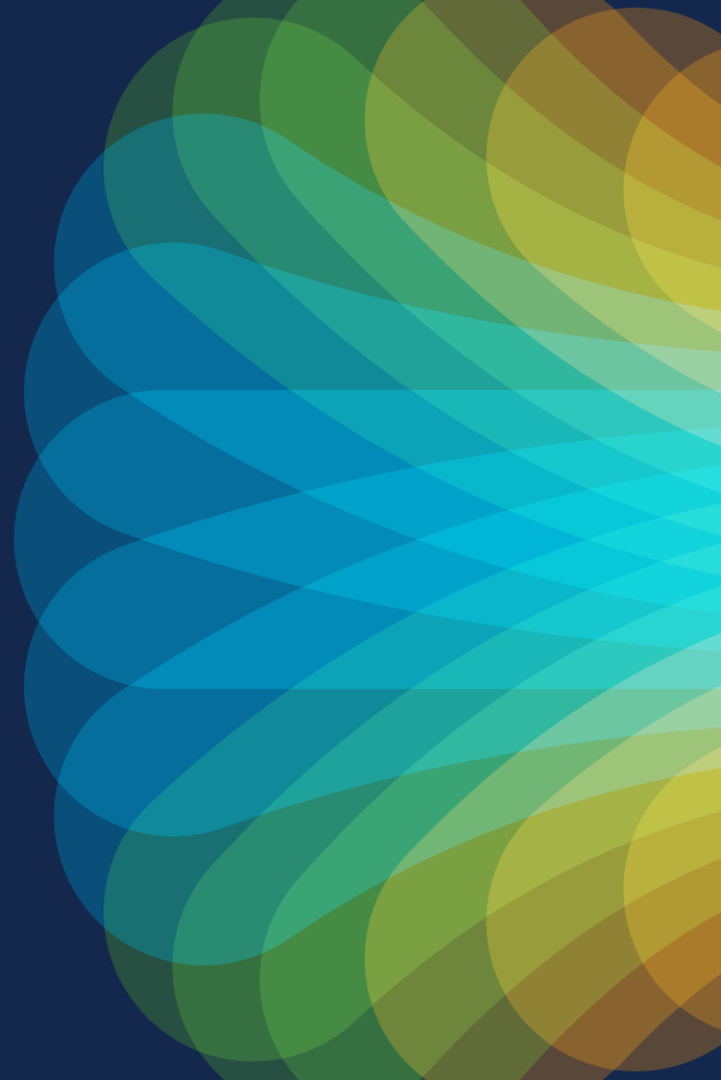
Campus Users



User Identity Beyond ISE

- Captive Portal support for active Azure AD user authentication
 - “BeyondCorp” use case for internal campus segmentation
 - Direct SAML integration with Azure AD or via Duo Single Sign-On
- Built-in FMC passive user identity discovery agent
 - Support all private Active Directory and LDAP deployments
 - Simplified feature set without full ISE or ISE-PIC integration

Management



Simplified Access Control Policy (ACP) View



Global_Policy

Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Search Rules

Try New UI Layout Show Warnings Analyze Hit Counts Save Cancel

Prefilter Policy: Default Prefilter Policy Inheritance Settings Policy Assignments (1) SSL Policy: None Identity Policy: None

Show Rule Conflicts Add Category Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action	Icons	0	Icons
Mandatory - Global_Policy (1-7)																	
1	Block Non-Business Apps	inside	outside	Campus	Any	Any	Any	Risks: High, V	Any	Any	Any	Any	Any	Block	Icons	0	Icons
2	Block_Unauthorized_Wi	inside	outside	Campus	Any	Any	Any	Any	Any	Any	Any	Any	Any	Interacti	Icons	0	Icons
3	Campus_File_Inspection	inside	outside	Campus	Any	Any	Any	HTTP HTTPS	Any	Any	Any	Any	Any	Allow	Icons	0	Icons

Global_Policy

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

Targeted: 1 device

Total 7 rules

Add Category Add Rule

	Name	Action	Source	Destinations and Applications
Mandatory (1-7)				
1	Block Non-Business Apps	Block	NET Campus	ZONE inside ZONE outside APP Risks: High Risks: Very High
2	Block_Unauthorized_Web	Interactive ...	NET Campus	ZONE inside ZONE outside URL Adult Child Abuse Content Extreme Gambling Hate Speech
3	Campus_File_Inspection	Allow	NET Campus	ZONE inside ZONE outside APP HTTP HTTPS
4	Allow_Outbound	Allow	NET Campus	ZONE inside ZONE outside
5	Inbound_Mail	Allow	ZONE outside	NET Mail_Servers ZONE inside APP SMTP SMTPS

Simplified ACP Rule Editor

Inline rule navigation.

Direct access to all advanced actions.

Wizard-style object definition for all source and destination properties.

Editing Rule #5. Inbound_Mail

Select Rule: Select... Name: Inbound_Mail

Action: Allow

Sources: Collapse All Remove All

- ZONE 1 object outside

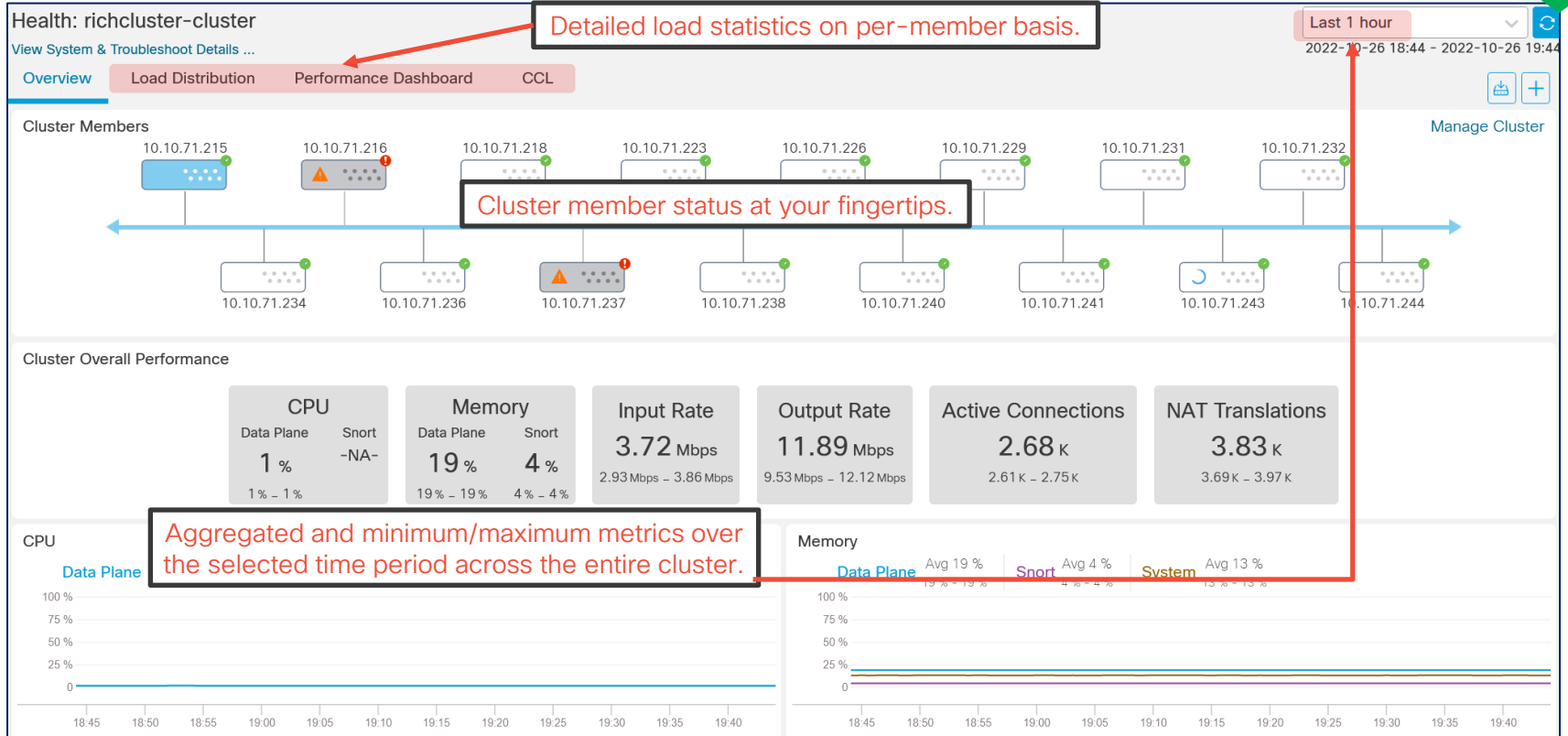
Destinations and Applications: Collapse All Remove All

- NET 1 object Mail_Servers
- ZONE 1 object inside
- APP 2 objects SMTP SMTPS

Cancel Apply

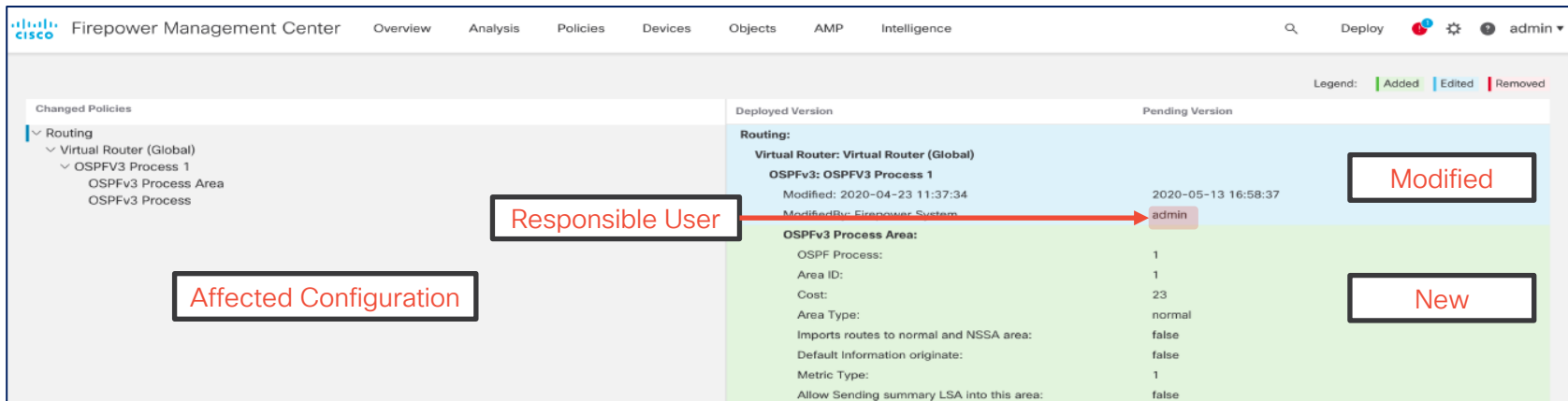
Cluster Health Dashboard

FMC
7.3



Change Management

- Selective change deployment and detailed audit transcripts in FMC
 - Individual configuration changes can be filtered and deployed by user
 - Emergency rollback to one of 10 previous configuration versions
 - Separation of Access Rules, IPS, and File policy deployment in **FTD 7.4**



Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

Legend: Added Edited Removed

Changed Policies	Deployed Version	Pending Version
Routing <ul style="list-style-type: none"> Virtual Router (Global) OSPFv3 Process 1 <ul style="list-style-type: none"> OSPFv3 Process Area OSPFv3 Process 	Routing: Virtual Router: Virtual Router (Global) OSPFv3: OSPFv3 Process 1 Modified: 2020-04-23 11:37:34 ModifiedBy: Firepower System	2020-05-13 16:58:37 admin Modified
	OSPFv3 Process Area: OSPF Process: 1 Area ID: 1 Cost: 23 Area Type: normal Imports routes to normal and NSSA area: false Default information originate: false Metric Type: 1 Allow Sending summary LSA into this area: false	New

Responsible User

Affected Configuration

“Shallow” Access Policy Locking

Global_Policy

Enter Description

Try New UI Layout ☐ Show Warnings Analyze Hit Counts Save Cancel

Rules Security Intelligence HTTP Responses Logging **Advanced**

This Policy is locked by you.

Prefilter Policy: Default Prefilter Policy Inheritance Settings Policy Assignments (1)
SSL Policy: None Identity Policy: None

☒ Policies

- ☒ Access Control
 - ☒ Access Control Policy
 - ☒ Modify Access Control Policy
 - ☒ Override Access Control Policy Lock

Global_Policy

This Policy is locked by Jonny. You cannot edit this policy.

Show Warnings Analyze Hit Counts Save Back

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: Default Prefilter Policy Inheritance Settings Policy Assignments (1)
SSL Policy: None Identity Policy: None

☒ Policies

- ☒ Access Control
 - ☒ Access Control Policy
 - ☒ Modify Access Control Policy
 - ☐ Override Access Control Policy Lock

Global_Policy

This Policy is locked by andrew. You cannot edit this policy.

Show Warnings Analyze Hit Counts Save Back

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: Default Prefilter Policy Inheritance Settings Policy Assignments (1)
SSL Policy: None Identity Policy: None

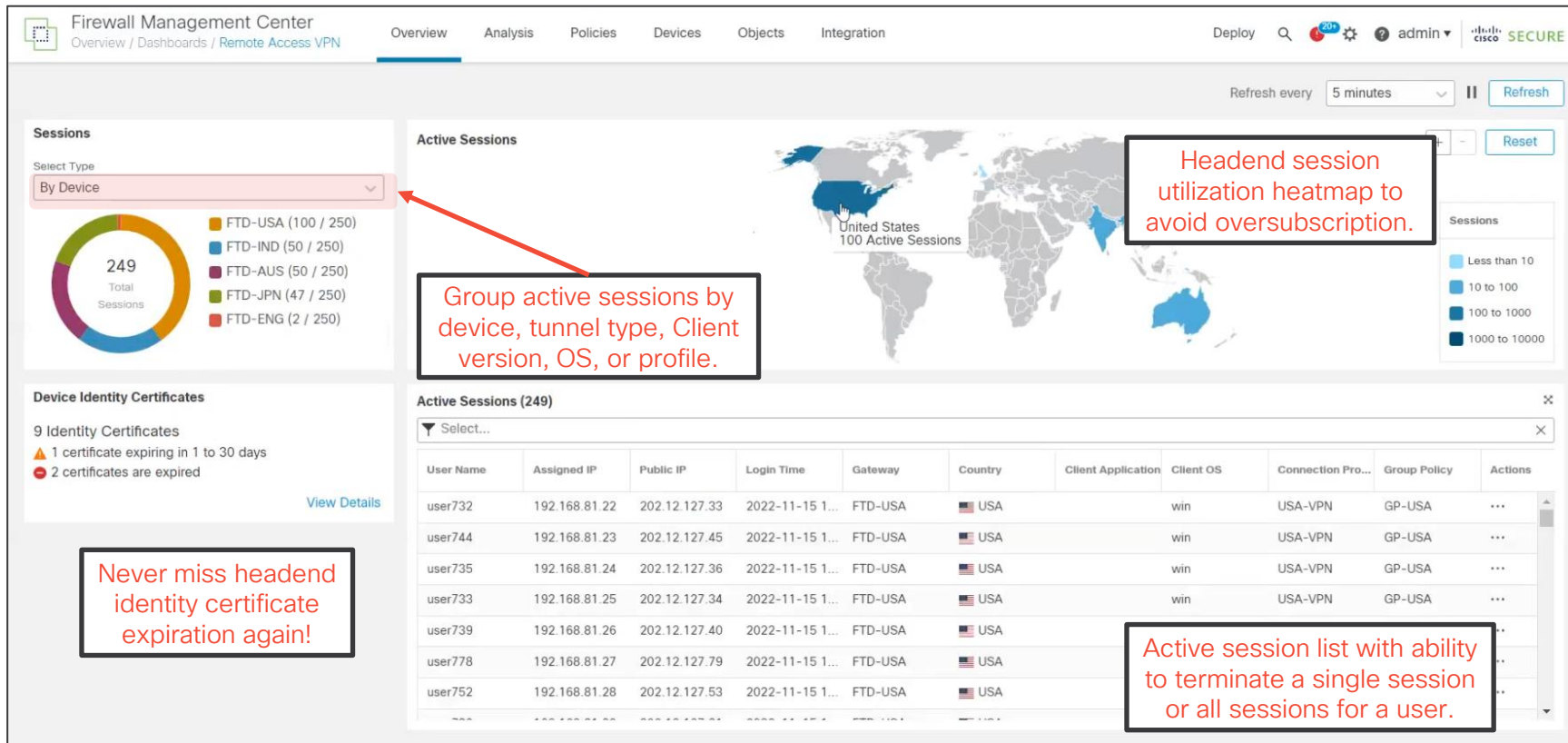
Workflow Mode and Change Logging

- Workflow Mode will require ticket approval for supported changes
 - Most policies and related objects are supported
 - Operator opens a change ticket before making changes
 - Ticket must be Rejected, Discarded, or Approved by an Approver
- Send configuration change syslogs with API link or full JSON

```
Jan 9 17:01:32 FTDv audit-syslog[169]:[auditLog@169 username="andrew" ip="192.0.2.12"
 subsystem="Objects>ObjectManagement>ServiceObject"] [{"policyDiffDataId":0,"policyDiffId":0,"objectUUid":"00000000-0000-
0ed3-0000-008589935118","type":"ServiceObject","diffData":{"entityUUid":"00000000-0000-0ed3-0000-
008589935118","userList":[],"parentUUid":"5e3fec7f-00a0-45fb-ac29-
207b3d2af415","valuesDeletedList":[],"valuesAddedList":[],"valuesUpdatedList":[{"oldValue":"","newValue":"202
3-01-09 17:01:32","fieldName":"Modified"}, {"oldValue":"","newValue":"secure-sip-
port","fieldName":"Name"}, {"oldValue":"","newValue":"Port","fieldName":"Type"}, {"oldValue":"","newVal
ue":"","fieldName":""}, {"oldValue":"","newValue":"TCP","fieldName":"Protocol"}, {"oldValue":"","newV
alue":"5061","fieldName":"Port"}, {"oldValue":"","newValue":"false","fieldName":"AllowOverrides"}], "refer
encesAddedList":[],"referencesDeletedList":[],"parentHierarchyList":[],"impactedDeviceList":[],"entityType":"Ser
viceObject","entityName":"secure-sip-port"},"parentUUid":"5e3fec7f-00a0-45fb-ac29-207b3d2af415","isGrouped":false}
```

VPN Monitoring Dashboard

FMC
7.3



Policy Analysis



Policy Analysis

Rule Warnings and Errors (0)

Policy Warnings (0)

Conflicts (3)

⚠ Total Conflicts: 3

Shadowed: 1

Object Overlap: 1

Redundant: 1

Shadowed

3

Allow_Inside_DB_Acce...

This rule's match criteria are a subset of the criteria for rule Allow_Outbound_Internet. This rule will never be matched. Please evaluate the intended behavior and adjust the rule's location, match criteria, and action as needed, or you can delete the rule.

2

Allow_Outbound_Inter...

Object Overlap

4

Allow_Exec_Workstati...

FULL OVERLAPS (1): Source Network Overlaps: 192.168.1.5 fully overlaps with - [192.168.1.1-192.168.1.5]

4

Allow_Exec_Workstati...

Redundant

6

Allow_Outbound_Partn...

This rule is redundant to Allow_Outbound_Partner_HTTPS-11. You can delete this rule.

8

Allow_Outbound_Partn...

"Shadow" typically refers to a rule that is at least partially rendered ineffective by another higher-priority rule.

Close

CISCO *Live!*

#CiscoLiveAPJC

BRKSEC-2236

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

48

AI Interactive Assistant

FMC
7.6

Improve
visibility



Reduce effort to learn about the policies you have deployed

“What are the rules in my #campus-fw policy?”

“This policy contains a total of 2,500 rules. About 1,500 rules are set to 'allow' action, while approximately 1,000 are set to 'block'.”

Speed up
troubleshooting



Use knowledge base to autocomplete troubleshooting steps

“Have I enabled malware analysis on my access control policy?”

“Yes. You currently have malware analysis enabled on 120 rules out of 700.”

Act faster



Take actions to create new rules or block existing ones

“Remove duplicate rules.”

“Calling services to check and remove duplicates. We found 300 duplicate rules. Please confirm if you would like to delete these rules. You can restore the config file should anything fail.”

FMC View: AI Interactive Assistant



cdFMC

Search

Alexander Business Corp, Inc

Return to Access Control Policy

ACP - Production

Analyze Rule Heartbeat Reset Save

Packets Prefilter Rules Decryption Security Intelligence Identity Access Control More

Targeted: 3 device

Search

Total 9 rules

Add Category Add Rule Ask AI

	Name	Action	Source				Destination			
			Zones	Networks	Ports	Dynamic Attributes	Zones	Networks	Ports	Applications
Mandatory										
There are no rules in this section Add Rule or Add Category										
Default (1-9)										
☐	1 External	Block	Any	any-ipv4	-1 more	Any	Any	TCP_47001	Any	
☐	2 Internal	Allow	Any	any	-1 more	Any	Any	TCP_8302	Cisco	
☐	3 Block Malwares	Block	Any	any-ipv4	-1 more	Any	Any	Any	Tiny	
☐	4 Block Torrent	Block	Any	Germany	-8 more	Any	Any	Bit-torrent	Torren	

Default Action: Intrusion Prevention: Balanced Security and Con...

Ask Cisco AI

Show me access policies related to the user group Inn-vendor

Cisco Assistant 8:12 AM

Absolutely! There are **3 Access Control Policies** related to user group inn-vendor. There are **10 Access Control Rules** across these 3 policies.

4 rules are about Sensitive Data

4 rules are about Internet Access

2 rules are about Internal Application Access

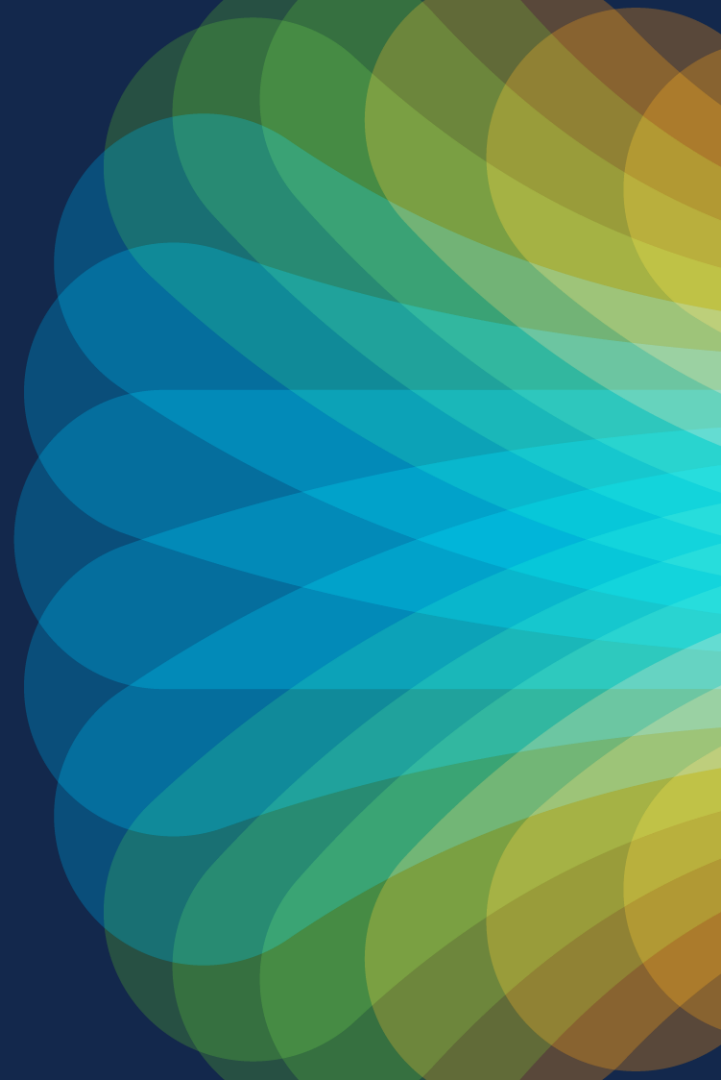
Regenerate

Ask a question or request, or type "/" for suggestions

© 2022 Cisco Systems, Inc.

Privacy policy Terms of service

Secure Workload



Secure Workload as Policy Engine

Flow Telemetry Ingestion

- Switch and Router flows (Netflow)
- Firewall flows (NSEL)
- Public cloud Flow Logs
- Secure Client metadata
- 2M+ artifacts per second

Dependency Mapping

- Access policy baseline and continuous updates
- Non-compliant communication
- Logical topology visualization
- Connectivity troubleshooting

Policy Experiments

- Prevent costly outages by planning ahead
- Optimize and prune stale access rules
- More complex modeling across heterogeneous enforcement points

Network Security (NetSecOps)



Secure Firewall



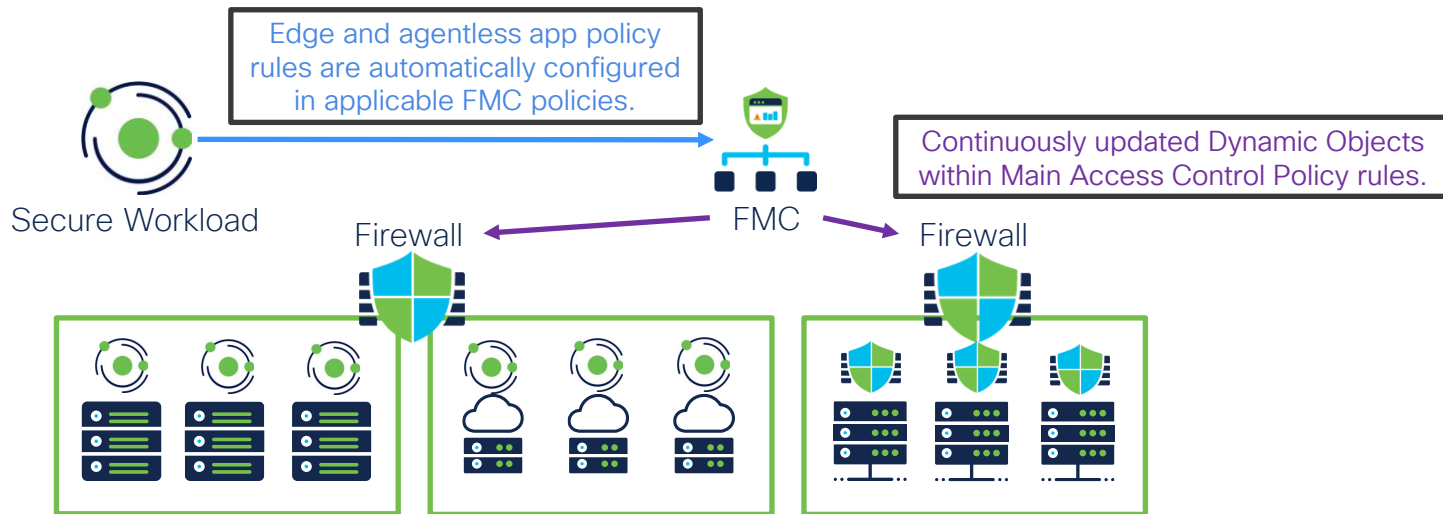
Secure Workload



Distributed Firewall

Secure Workload Policy Extension to Firewall

- Hybrid cloud microsegmentation with agents and network firewalls
 - North-South (edge) and East-West (lateral) policy enforcement



Secure Workload Policy Orchestration in FMC

Workload
3.6

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects AMP Deploy

East-West-Policy

Inserted rules are organized by sections.

Dynamic objects are used to replace IP addresses where applicable.

Different rulesets are scoped by domains.

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Search Rules

Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

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

Show Rule Conflicts Add Category Add Rule

#	Name	Source Networks	Dest Networks	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action	
Mandatory - East-West-Policy (1-11)								
1	Block log4j	Any	log4j-ubuntu	Any	Any	Any	Block	
2	Workload_golden_1	Any	Any	Any	WorkloadObj_collector	Any	Allow	
3	Workload_golden_2	Any	Any	TCP (6):5640	Any	WorkloadObj_collector	Allow	
4	Workload_golden_3	Any	Any	Any	WorkloadObj_collector	Any	Allow	
5	Workload_golden_4	Any	Any	TCP (6):5660	Any	WorkloadObj_collector	Allow	
6	Workload_golden_5	Any	Any	Any	WorkloadObj_wss	Any	Allow	
7	Workload_golden_6	Any	Any	TCP (6):443	Any	WorkloadObj_wss	Allow	
8	Workload_7	Any	Any	TCP (6)	WorkloadObj_Production_5	WorkloadObj_Developmen	Block	
9	Workload_8	Any	Any	TCP (6)	WorkloadObj_Vulnerable_V	WorkloadObj_Root_Interne	Block	
10	Workload_9	Any	Any	TCP (6)	WorkloadObj_Administrato	WorkloadObj_Root_CSW_5	Allow	

Outside access from workloads with known vulnerabilities based on version and CVE data can be blocked automatically.

Application Virtual Patching

- Tailoring FTD IPS policy to specific apps improves performance
- Workload will import vulnerability information (CVE) into FMC
 - Leverage Network Discovery Policy
 - Update specific Host Profiles
 - Improve Firepower Recommendations

Edit External Orchestrator Configuration

Basic Config

Hosts List

Domains

Virtual Patching

Enabled Domain(s)

Global/DC-East-West ✕

Select All

Remove All

Select Workloads

Default : EMEAR

DC ▾

Approved file Shares ▾

Critical Applications

Default:EMEAR:DC:DC-1:Applications

Default:EMEAR:DC:DC-2:HR-Invoice-App

Snort Rules Documentation

https://snort.org/search?query=1&submit_search=

Remove Vulnerabilities

Query ⓘ

Single CVE or comma separate CVE

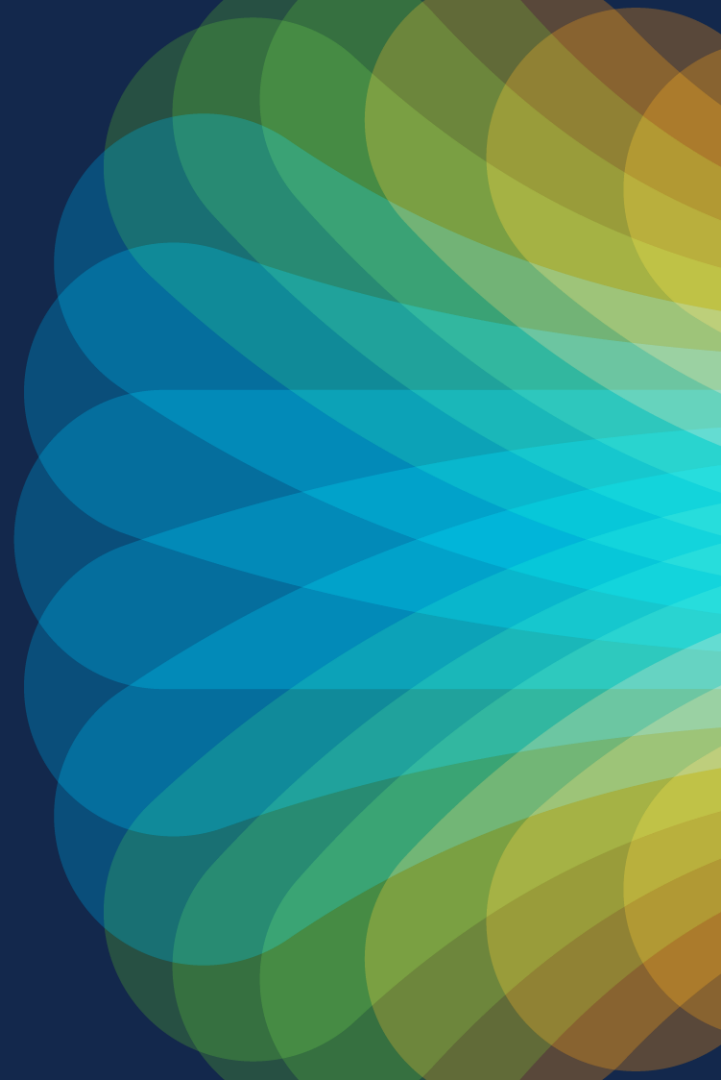
Bulk Removal (Upload CSV)

Connection will be tested after the update.

Cancel

Update

Conclusion



Cisco Security Beta Programs



Sign-Up Now:

<https://cs.co/security-beta-nomination>

"I've been involved in many beta programs...I must say that this one has been the best organized. This beta takes a very active, hands-on approach."

Higher-Ed Beta Customer



**Early Feedback
Programs**



**Beta Software
Access**



**Product
Training**



**Influence
Product Roadmap**



Presented by Security Customer Insights

CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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!*

#CiscoLiveAPJC

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, script font.

CISCO *Live!*

The text "Let's go" in a dark blue, sans-serif font, positioned to the left of a bright, multi-colored sunburst graphic that radiates from the right side of the image.

Let's go

#CiscoLiveAPJC