Let's go

The bridge to possible

Keeping Up on Network Security with Cisco Secure Firewall

Andrew Ossipov
Distinguished Engineer, Portfolio CTO

BRKSEC-2236

"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

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

Cisco Webex App

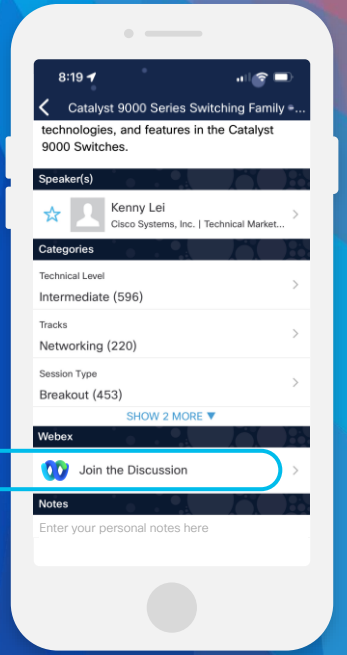
Questions?

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

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

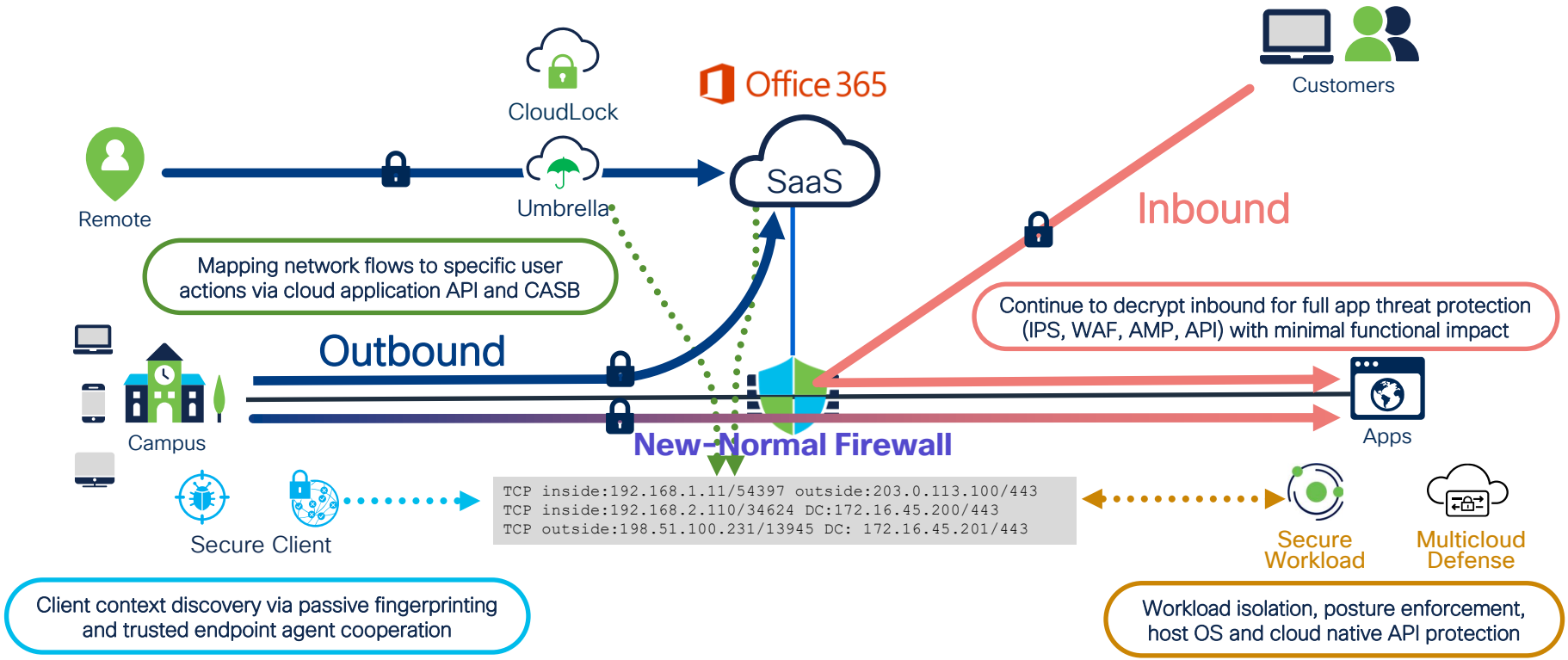
Agenda

FTD ASA

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

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

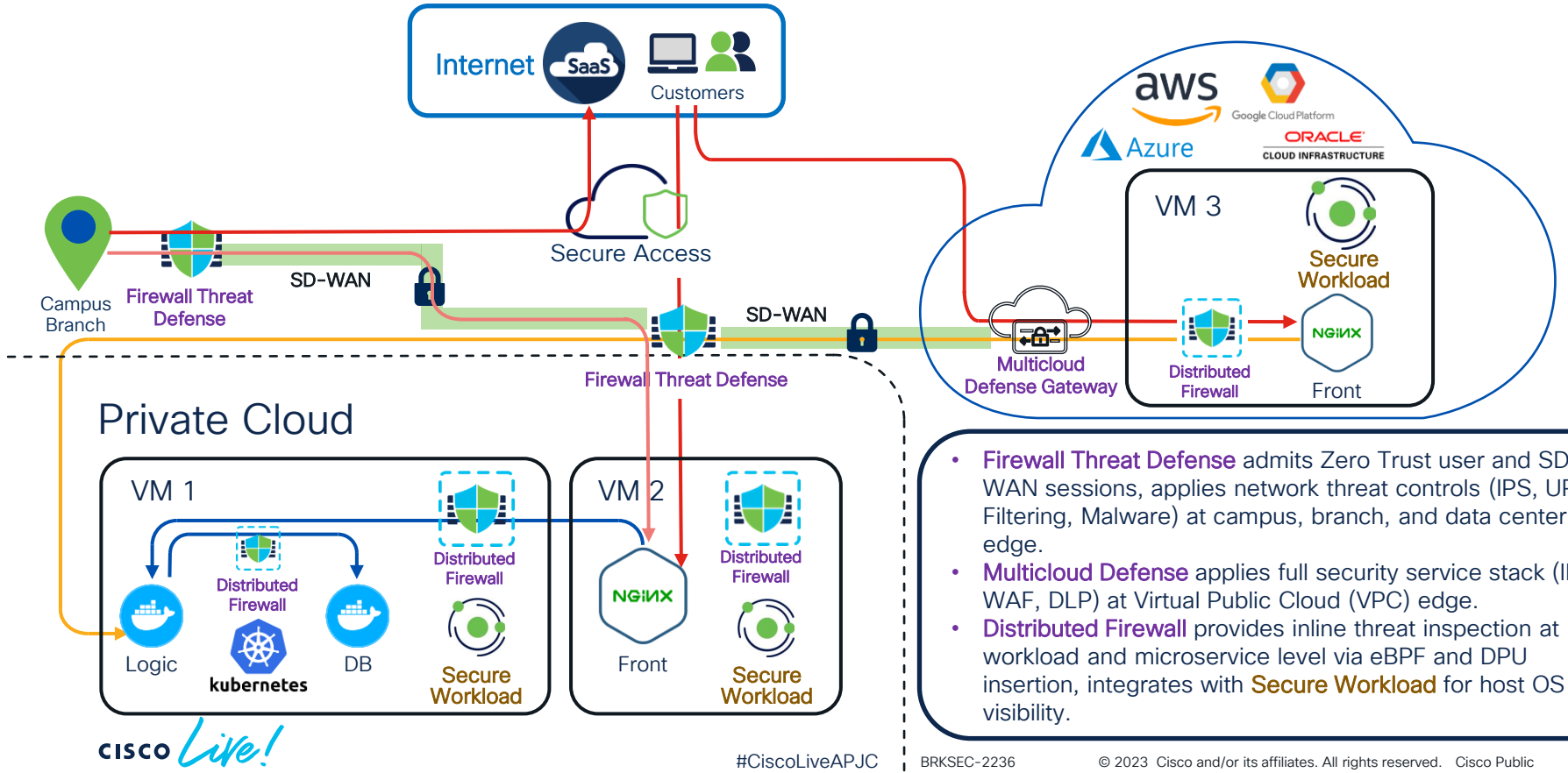
Secure Firewall: Inspect, Infer, and Cooperate



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

Firewall Vision: Network, Workload, and Cloud

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

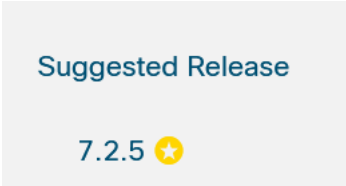


- Firewall Threat Defense admits Zero Trust user and SD-WAN sessions, applies network threat controls (IPS, URL Filtering, Malware) at campus, branch, and data center edge.
- Multicloud Defense applies full security service stack (IPS, WAF, DLP) at Virtual Public Cloud (VPC) edge.
- Distributed Firewall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

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

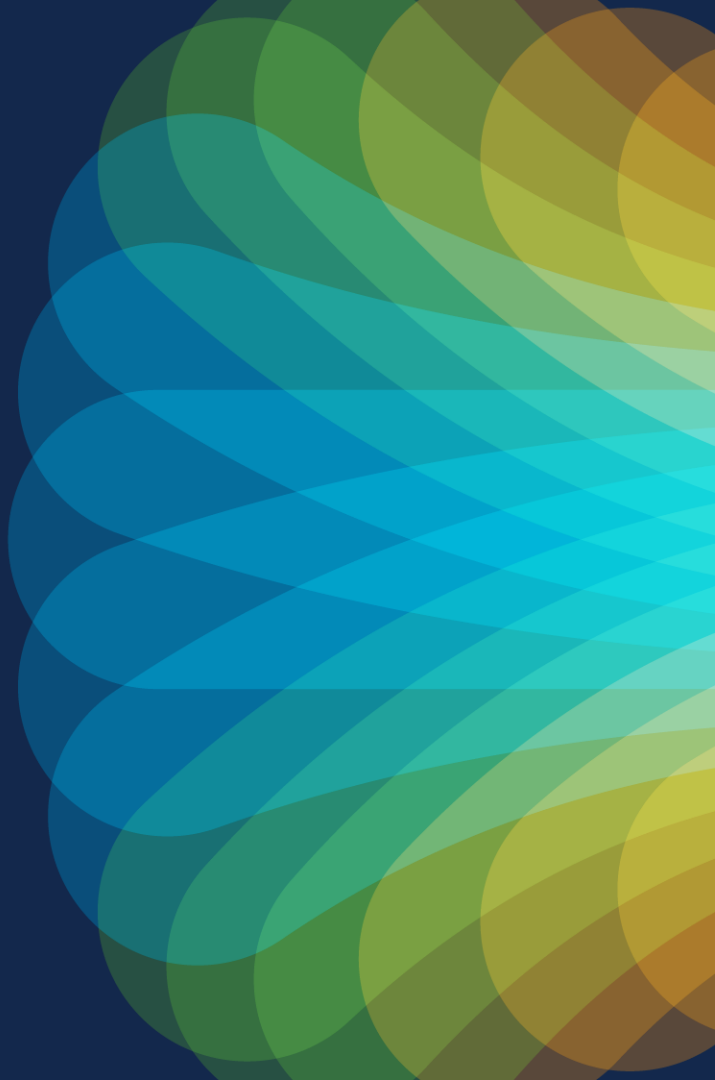
Firewall Threat Defense 7.2.4 Software

- 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



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

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

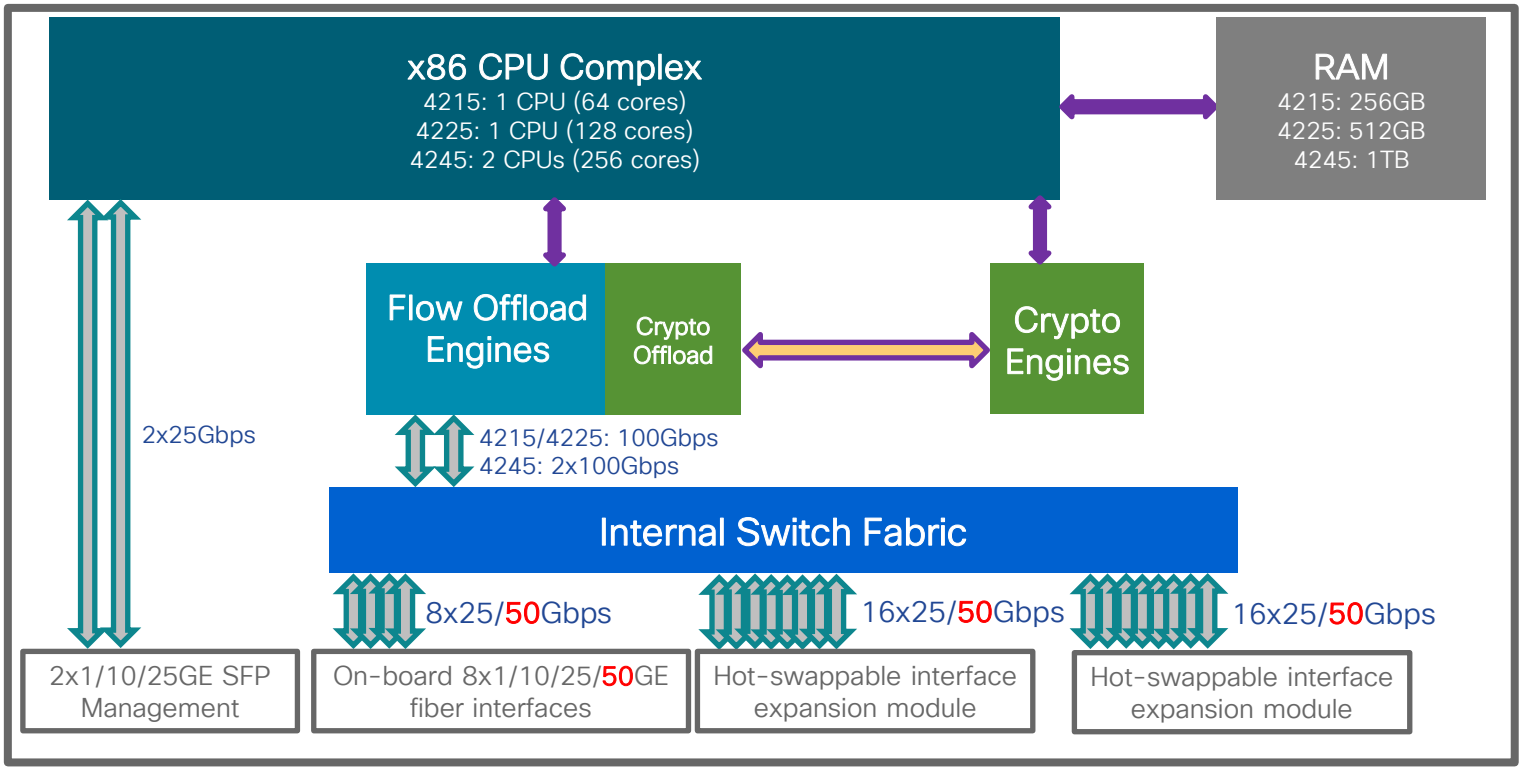
- Standard: 8x1/10GE, 8x1/10/25/50GE, 4x10/40GE, 2x100GE, 4x40/100/200GE, 2x200/400GE SFP+
- Fail-to-Wire: 8x1GE Copper; 6x10GE or 6x25GE SFP+ (SR and LR variants)

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

Secure Firewall 4200 Architecture

FTD 7.4

ASA 9.20



System Bus

Ethernet

Chip-to-Chip Link

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

Secure Firewall 4200 Performance

FTD 7.4

ASA 9.20

	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

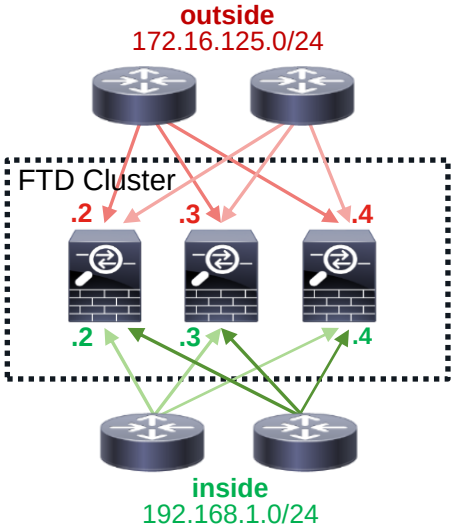
Up to 5x ↑ Boost in TLS Decrypt

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

Individual Mode Clustering

FTD 7.6

- 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



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

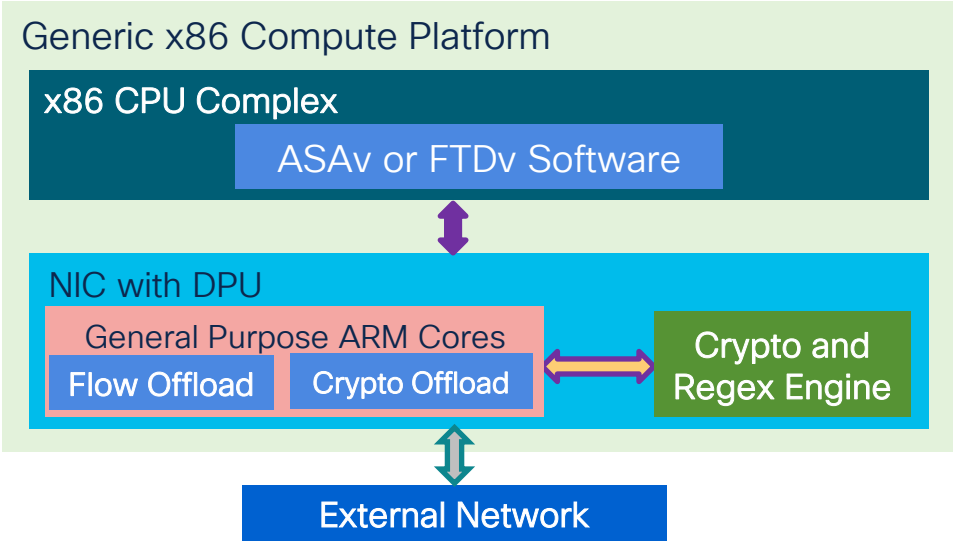
Data Processing Unit (DPU): Distributed Firewall

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

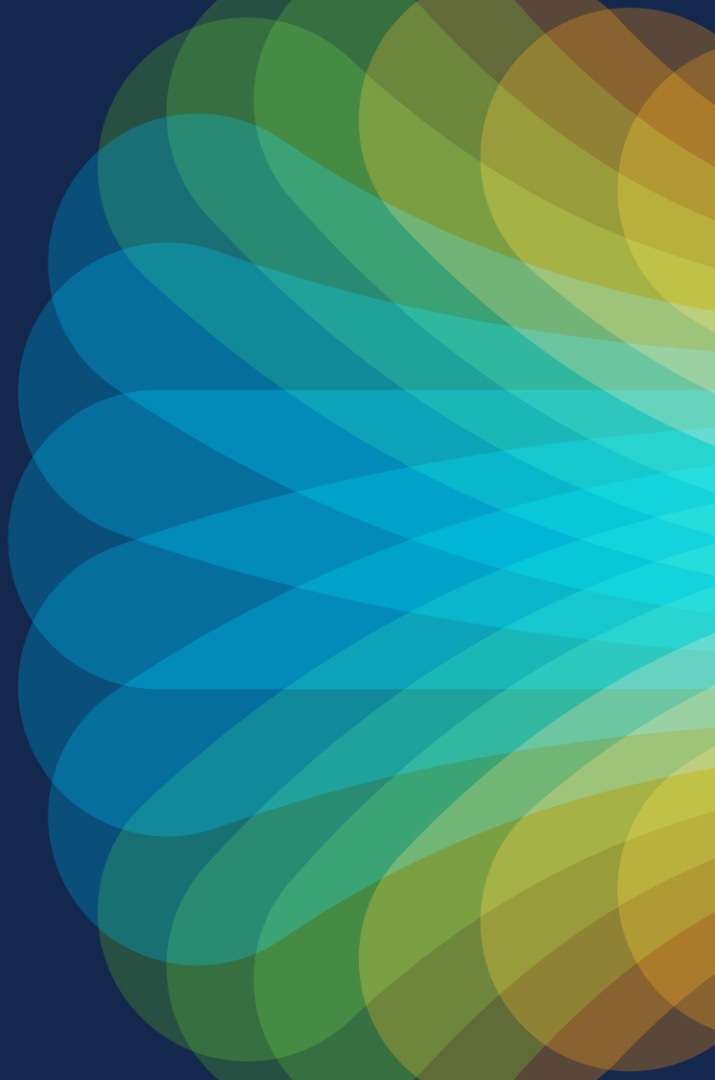
ASAv/FTDv software and Multicloud Defense is deployed on x86 CPU in generic private and public cloud environments.

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.



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

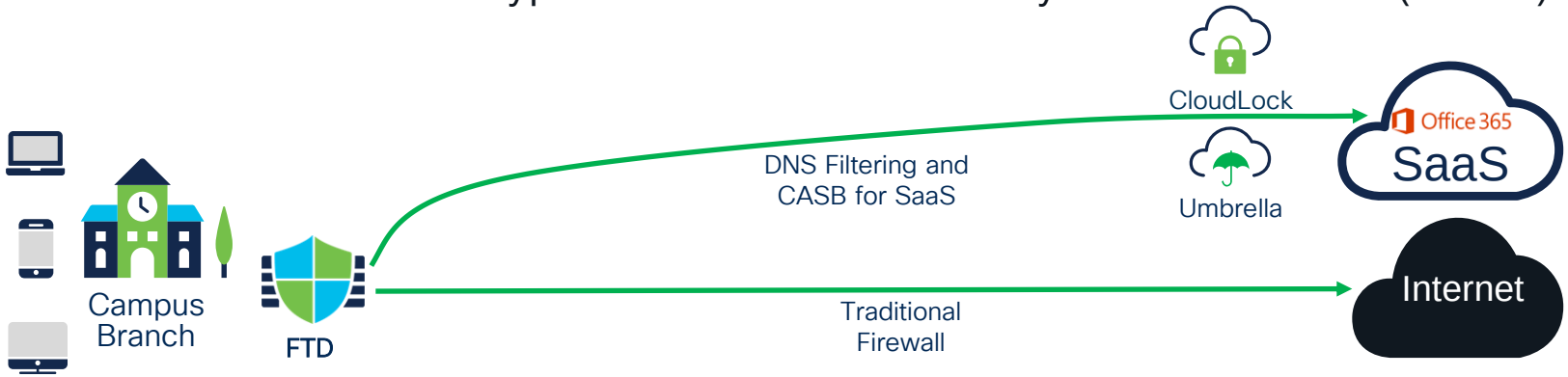
Threat Protection



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)

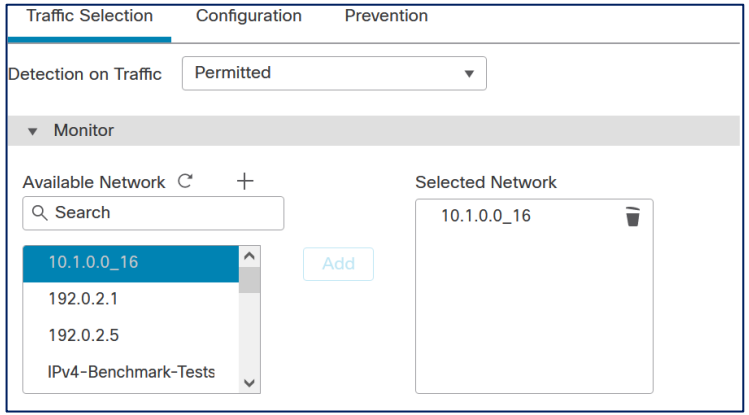


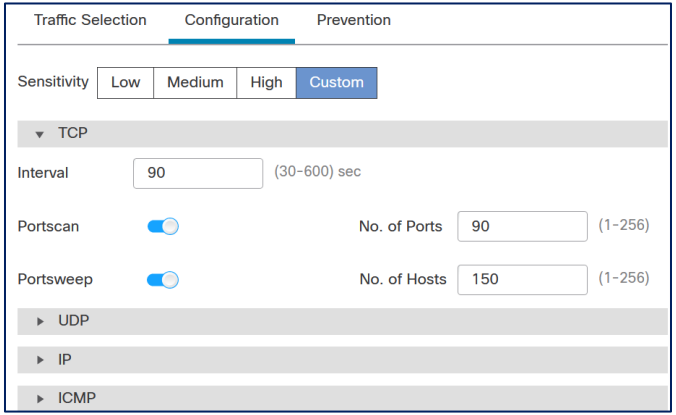
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Portscan Detection and Prevention

FTD 7.2

- 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

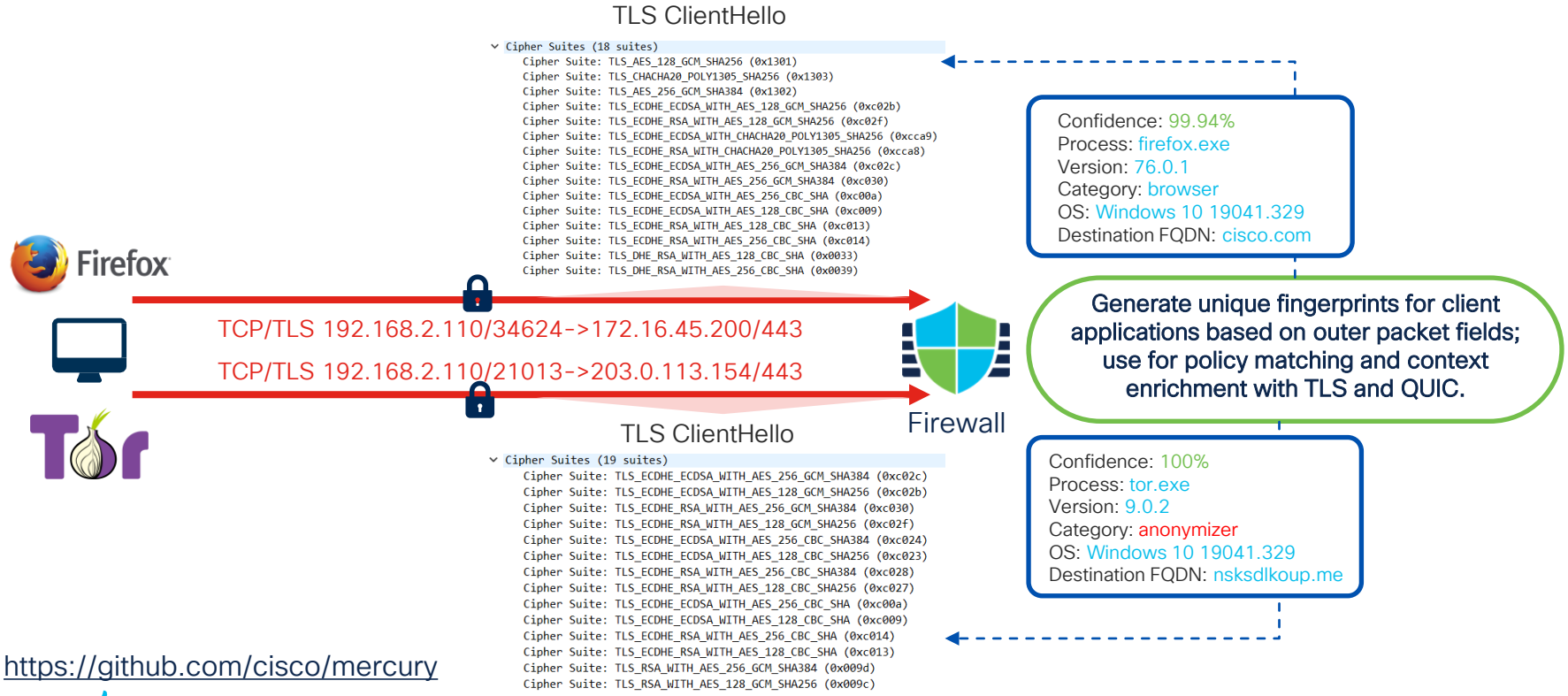




© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Encrypted Visibility Engine (EVE)

FTD 7.1



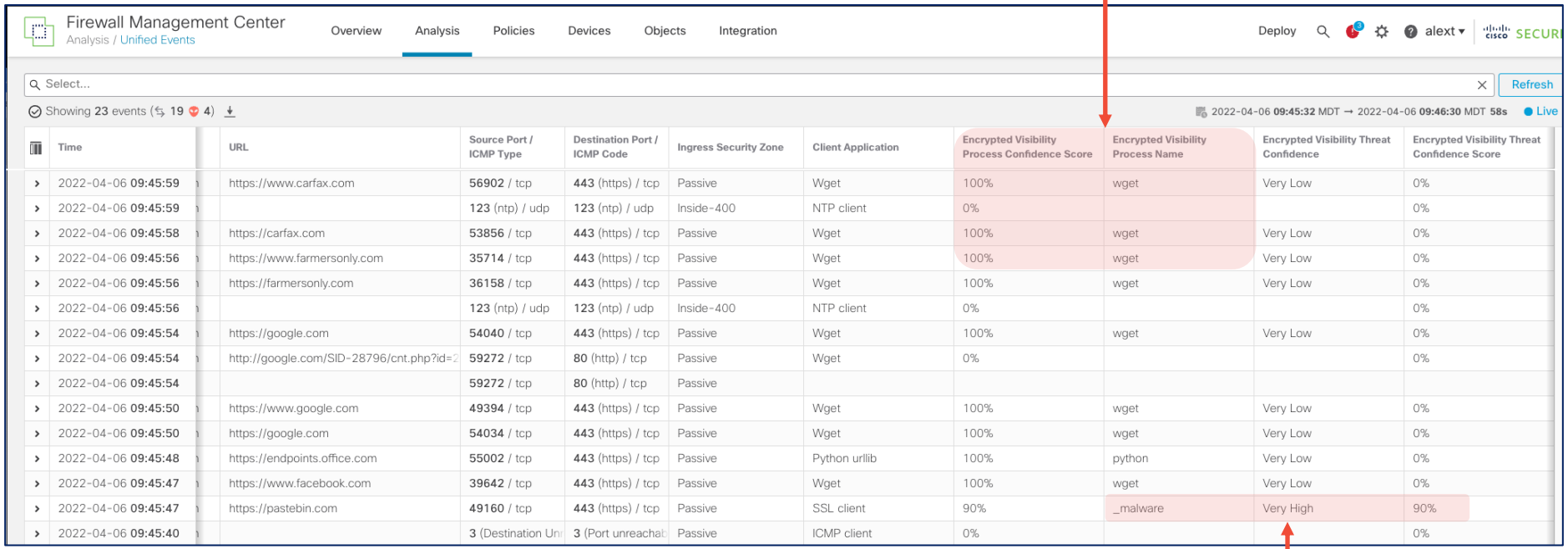
https://github.com/cisco/mercury

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

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.



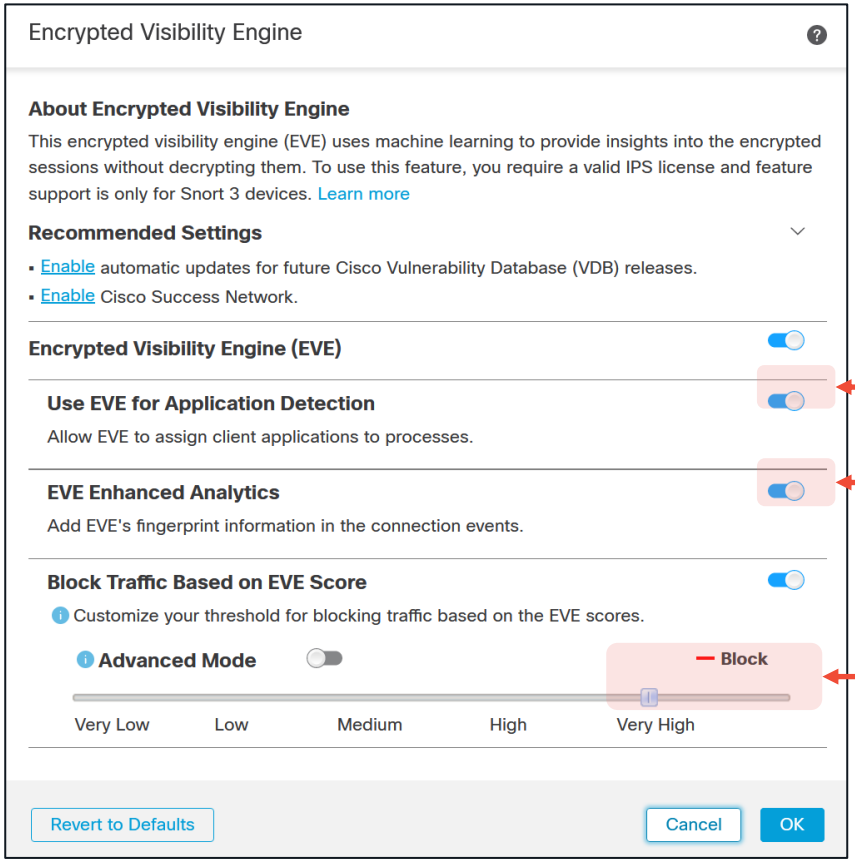
Time	URL	Source Port / ICMP Type	Destination Port / ICMP Code	Ingress Security Zone	Client Application	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
2022-04-06 09:45:59	https://www.carfax.com	56902 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:59		123 (ntp) / udp	123 (ntp) / udp	Inside-400	NTP client	0%			0%
2022-04-06 09:45:58	https://carfax.com	53856 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56	https://www.farmersonly.com	35714 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56	https://farmersonly.com	36158 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56		123 (ntp) / udp	123 (ntp) / udp	Inside-400	NTP client	0%			0%
2022-04-06 09:45:54	https://google.com	54040 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:54	http://google.com/SID-28796/cnt.php?id=2	59272 / tcp	80 (http) / tcp	Passive	Wget	0%			0%
2022-04-06 09:45:54		59272 / tcp	80 (http) / tcp	Passive					
2022-04-06 09:45:50	https://www.google.com	49394 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:50	https://google.com	54034 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:48	https://endpoints.office.com	55002 / tcp	443 (https) / tcp	Passive	Python urllib	100%	python	Very Low	0%
2022-04-06 09:45:47	https://www.facebook.com	39642 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:47	https://pastebin.com	49160 / tcp	443 (https) / tcp	Passive	SSL client	90%	_malware	Very High	90%
2022-04-06 09:45:40		3 (Destination Un	3 (Port unreachab	Passive	ICMP client	0%			0%

Inference-based threat alert and confidence level.

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

Encrypted Visibility Engine (EVE) 2.0

FTD 7.4



Inference-based AppID enrichment.

Detailed fingerprint data for third-party use.

Connection filtering based on malware confidence scores.

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

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

Now

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

https://appid.cisco.com/home

Search

Secure Firewall Application Detectors

Home | Release Notes | Support | Documentation | Resources | Feedback

ultrasurf

Search

Risk		Business Relevance	
Very Low	1,412	Very High	332
Low	891	High	976
Medium	1,353	Medium	2,411
High	1,630	Low	1,215
Very High	635	Very Low	987

Tags	
adds/installs other software	66
adult content	37
allows remote connect	90
allows remote control	52
antivirus	13

Categories	
active directory	8
ad portal	396
anonymizer/proxy	102
application development and testing	31
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 Vulnerability Database (VDB) Release Notes 365

365

(Type a VDB release between 343 - 365)

Encrypted Visibilty 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

  Threat Grid:
    total fingerprints: 801
    total connections:  3,041,256
```

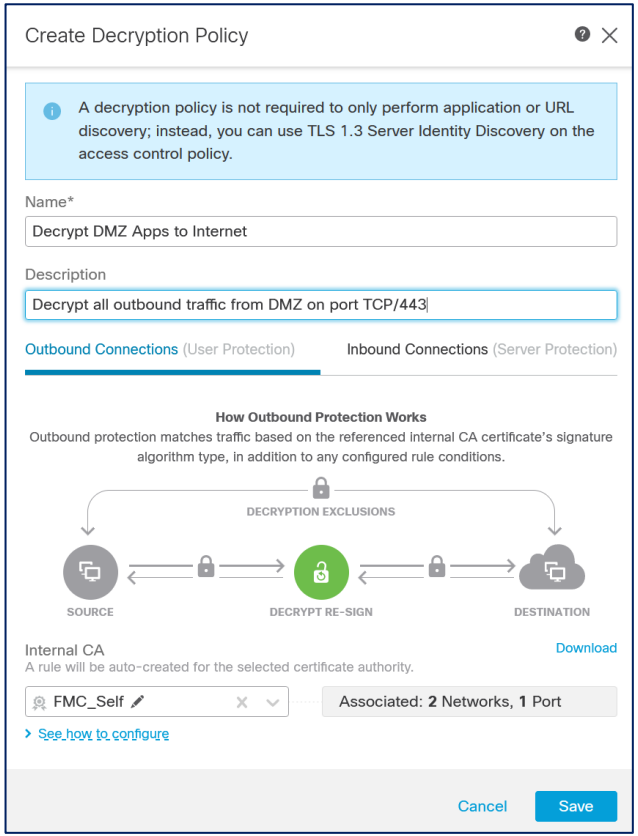
Full AppID database update information, including EVE fingerprint data.

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

Simplified TLS Decryption Policy

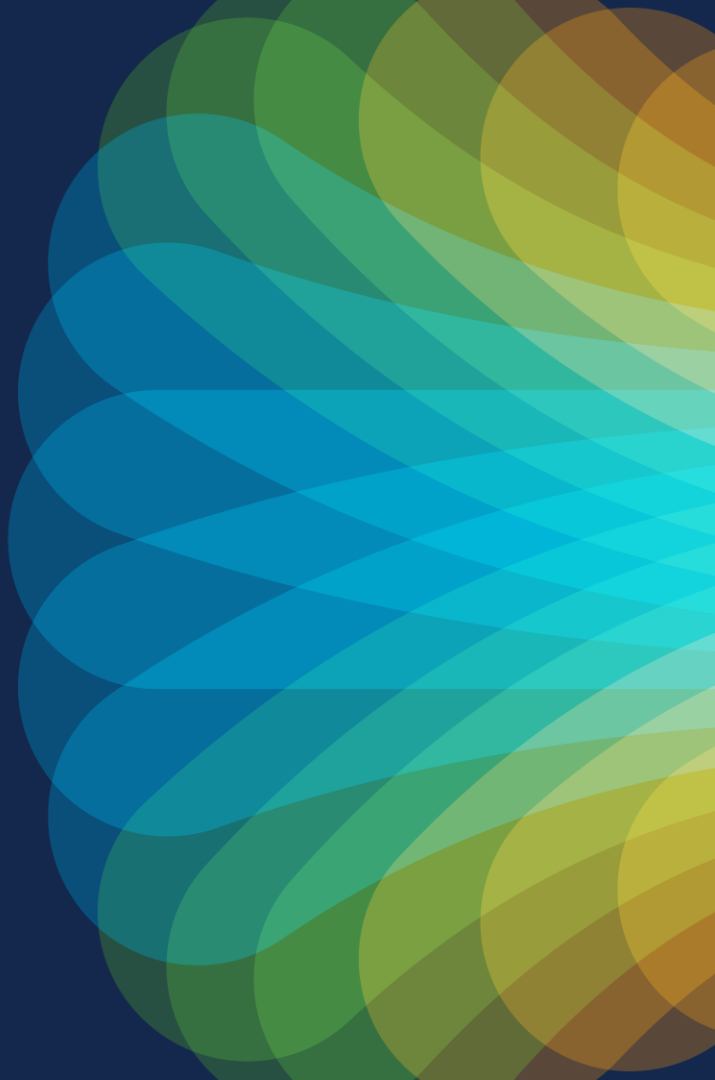
FTD 7.3

- 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



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

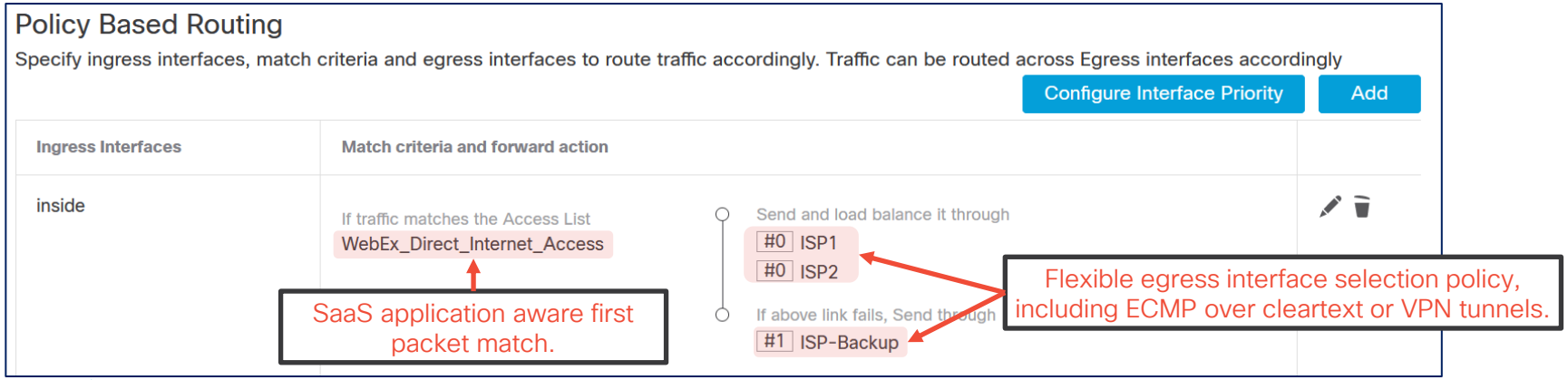
Connectivity



Application-Aware Policy Routing

FTD 7.1

- 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

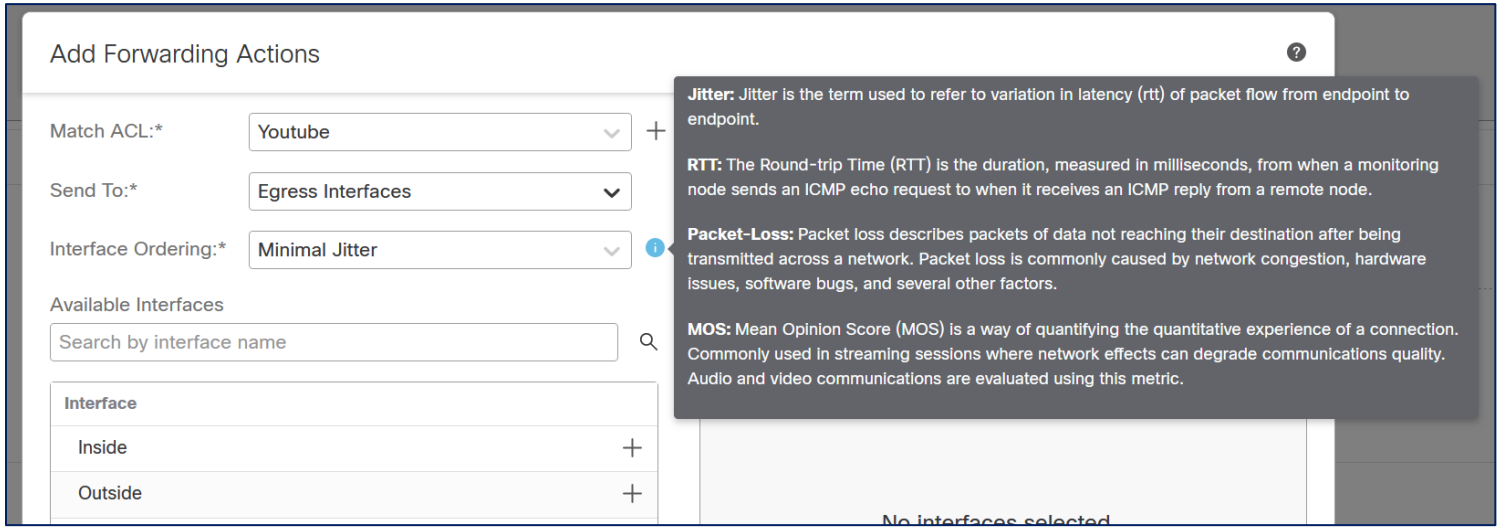


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Path Monitoring and Quality-Based Routing

FTD 7.2

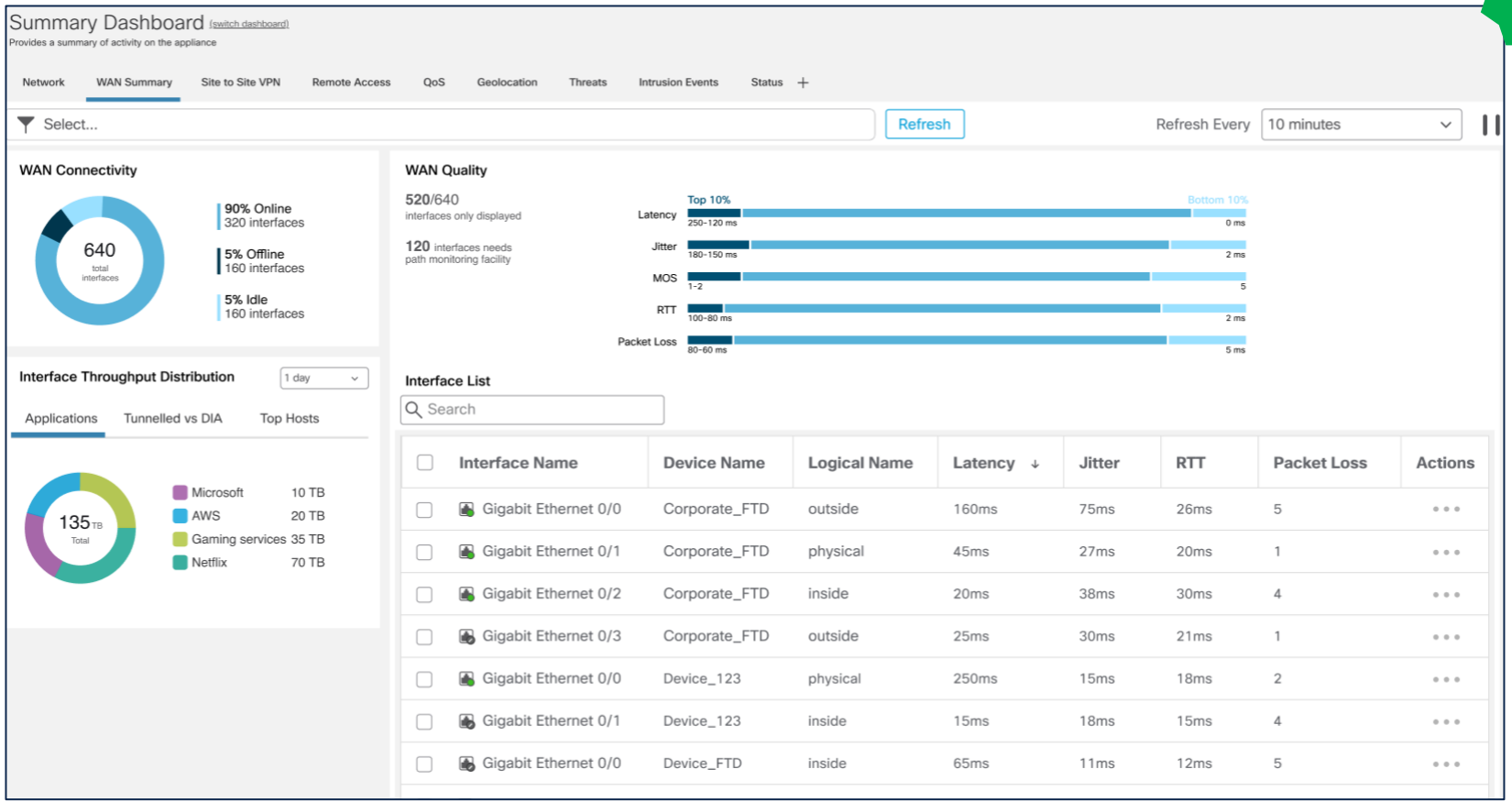
- Policy-based interface selection can be influenced by path quality
  - ICMP-based next-hop or external IP monitoring on each interface
  - HTTP(S)-based SaaS app tracking in FTD 7.4



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

SD-WAN Monitoring Dashboard

FTD 7.4



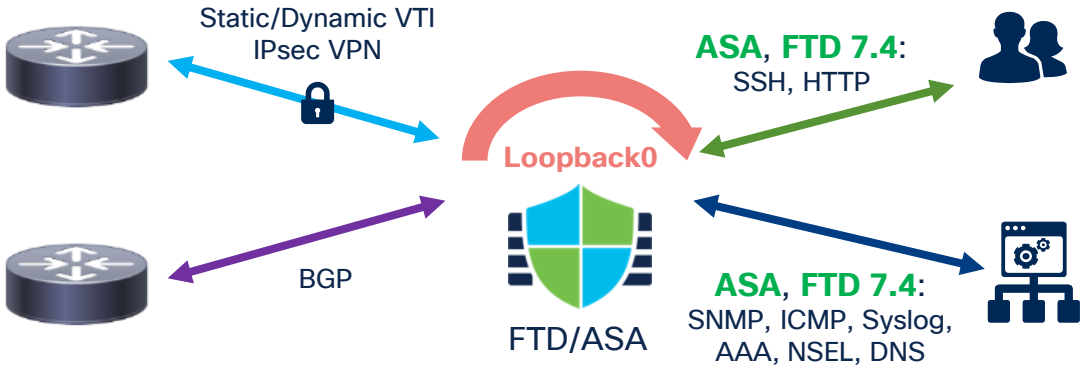
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Loopback Interface

FTD 7.3+

ASA 9.18.2

- 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

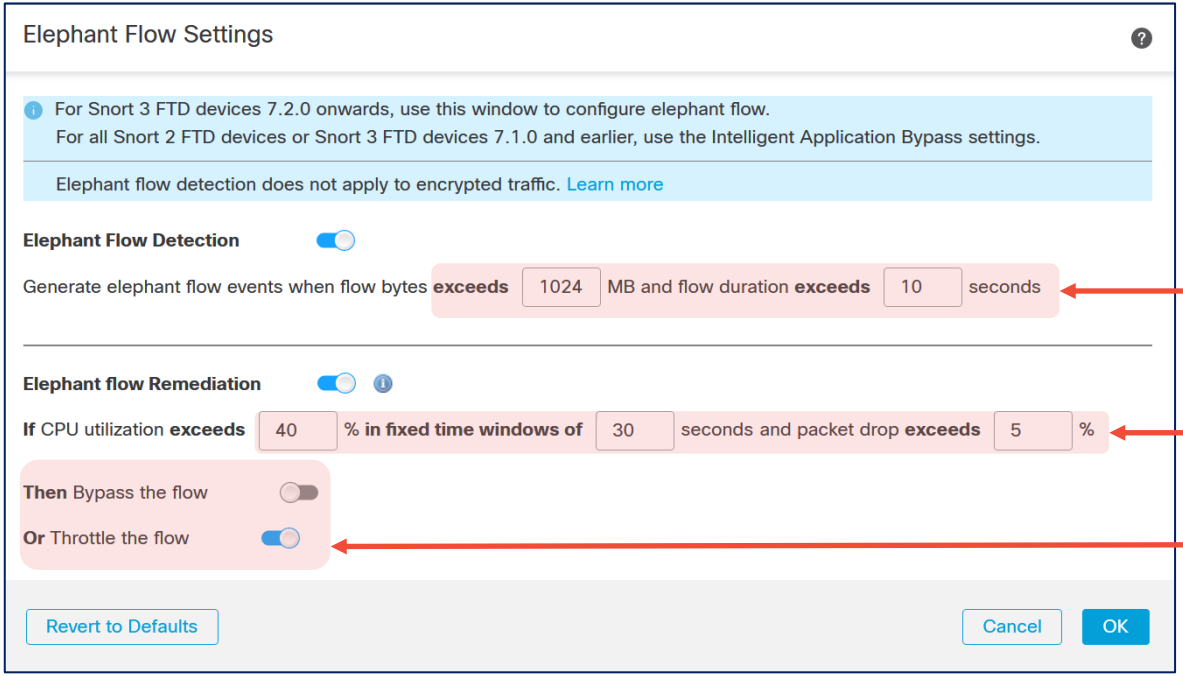


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Elephant Flow Detection

FTD 7.2

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



Throughput threshold to qualify as an Elephant Flow

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

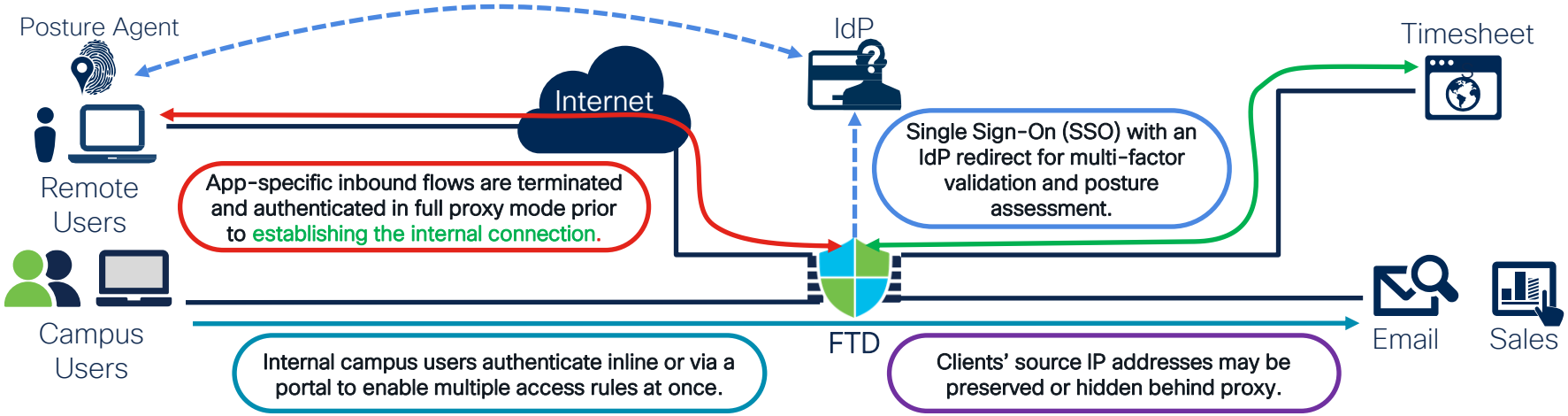
Optional flow remediation actions.

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

Clientless Zero Trust App Access (ZTAA)

FTD 7.4

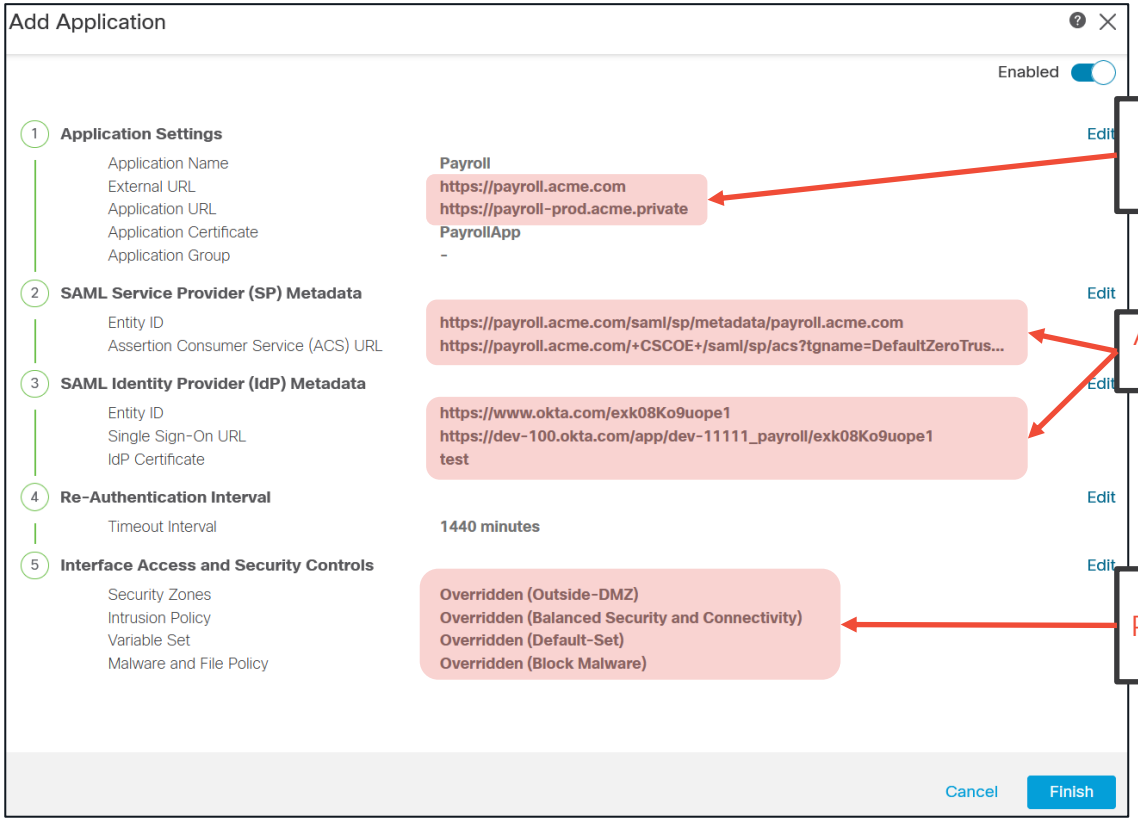
- Expand Captive Portal capabilities into a full reverse proxy
  - External Identity Provider (IdP) integration with posture assessment
  - Future support for internal (“BeyondCorp”) segmentation



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

Clientless ZTAA: App Definition

FTD 7.4



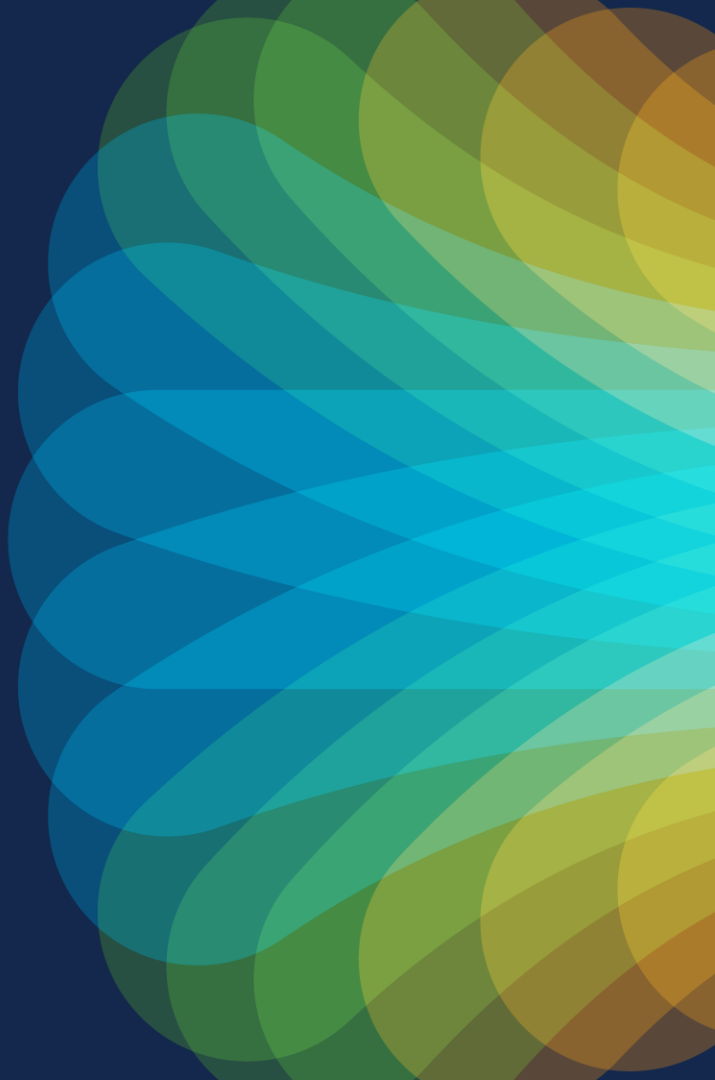
How the end user accesses the application (External URL) and how FTD makes the connection (Internal URL or IP).

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.

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

Hybrid Work



Consistent Protection in Hybrid Cloud

FTD 7.2

Secure Firewall Capabilities

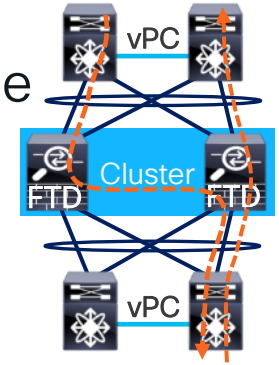
- Accelerated Networking
- Snapshot-Based Instantiation
- Gateway Load-Balancer insertion and FWaaS
- Clustering & Auto Scaling
- Infrastructure-as-Code and Automation for agility
- Integration with cloud services and management
- Dynamic Policy
- Smart & Tiered Licensing

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

Clustering for Virtual Firewalls

FTD 7.1+

ASA 9.17+



- 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
  - aws Google Cloud Platform Azure KVM vmware
  - 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

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

Automation with Infrastructure-as-Code

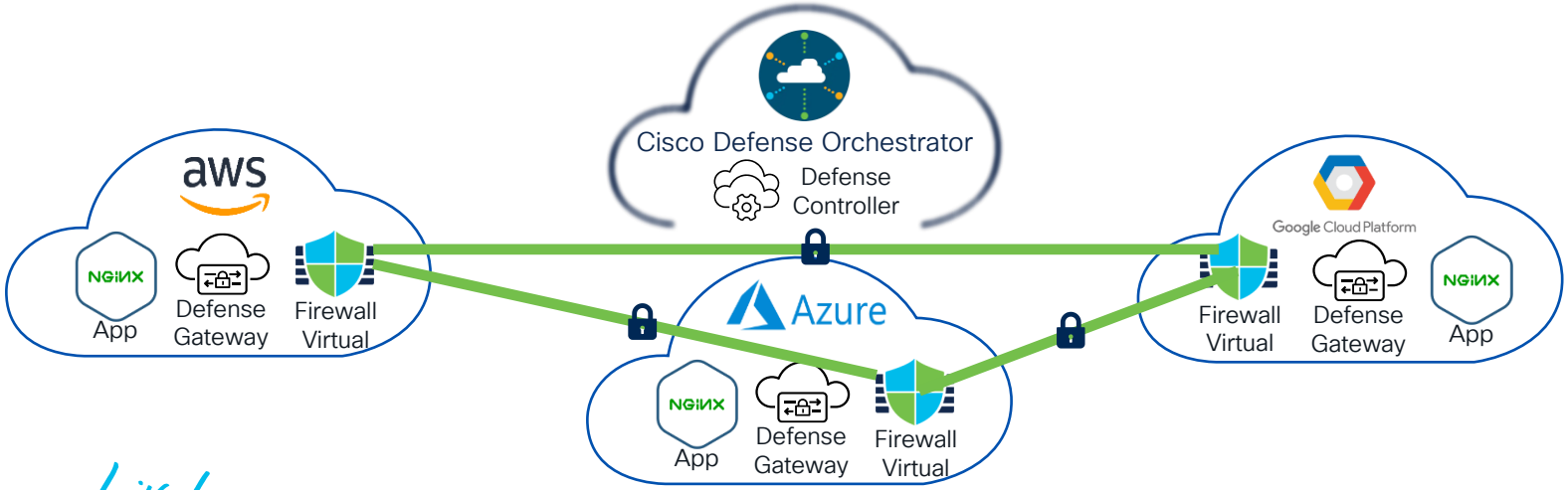
- Secure Firewall instantiation with public cloud templates
- Declarative Teraform templates for ASA and FTD (via FMC)
  - FTD Dynamic Object integration with HashiCorp Consul
- Imperative Ansible tasks for ASA and FTD (FDM and FMC)
- Continuously updated Cisco DevNet repositories
  - https://developer.cisco.com/secure-firewall/cloud-resources/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

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

Cisco Multicloud Defense

Now

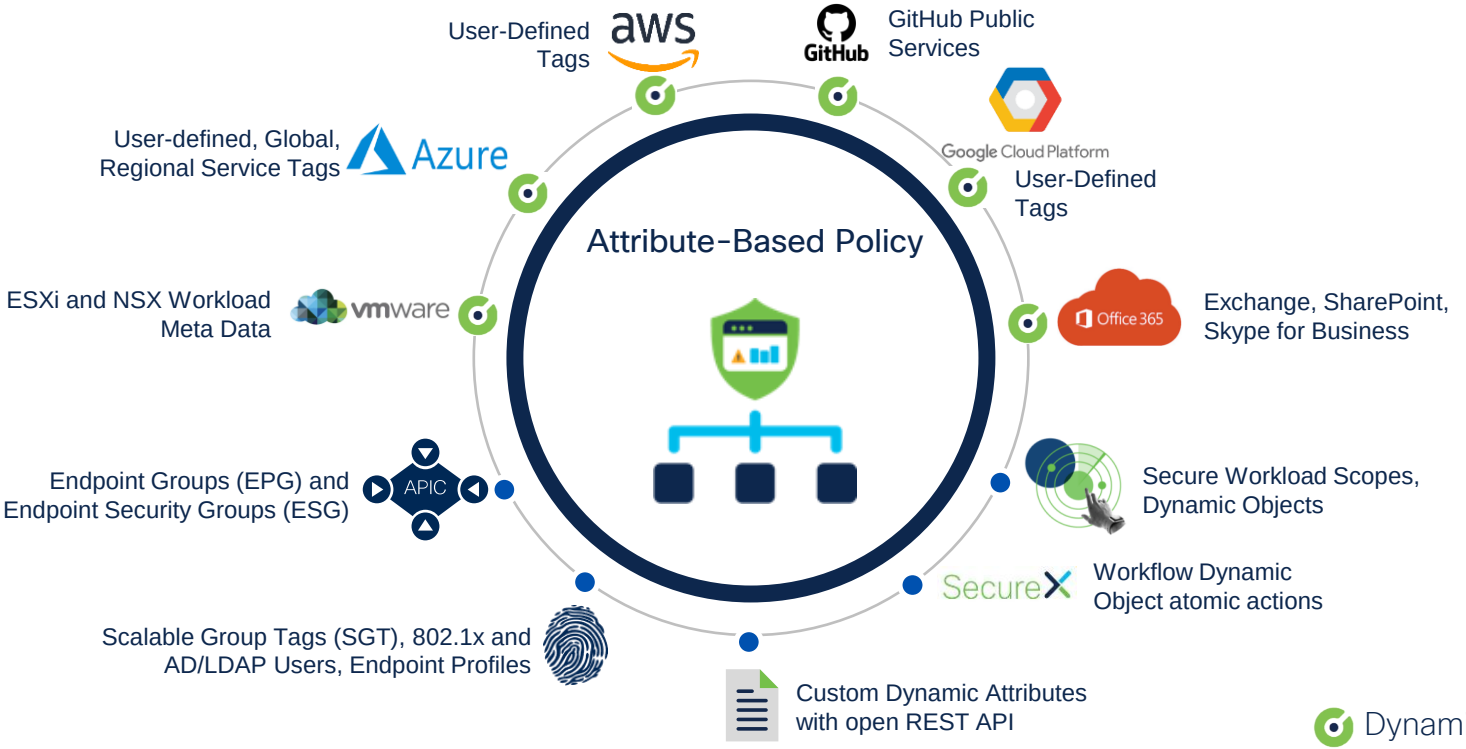
- Comprehensive and consistent VPC edge security in public clouds
  - Multicloud Defense Gateway: Firewall, IPS, WAF, DLP, reverse proxy
  - Inter-cloud and private cloud IPsec interconnect with ASAv/FTDv
  - Fully orchestrated by Multicloud Defense Controller in CDO



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

Firewall Policy Abstraction

FTD 7.0+



Dynamic Attribute Connector

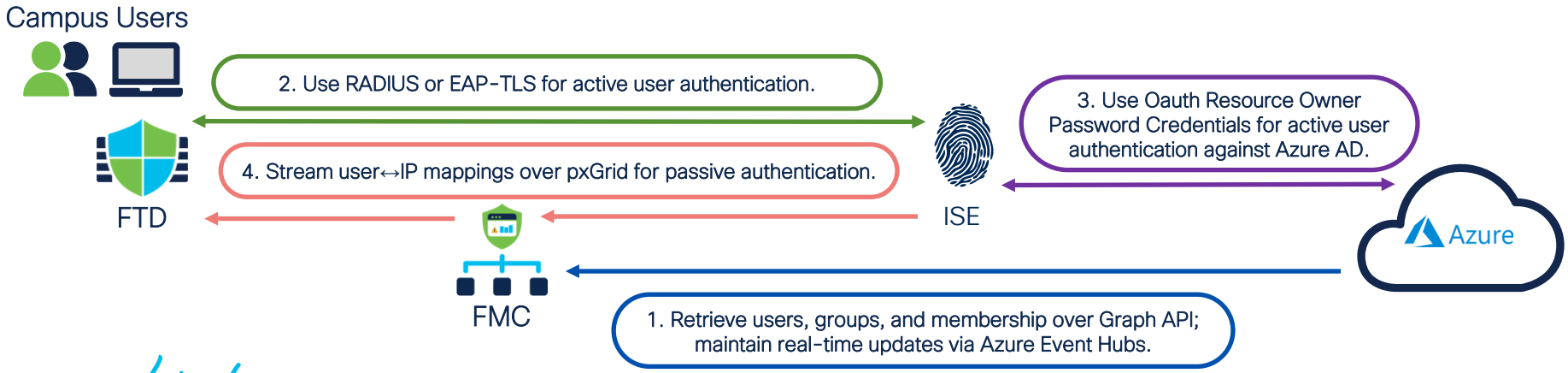
Firewall Management Center

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

User Identity from Azure AD with ISE

FTD 7.4

- 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



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

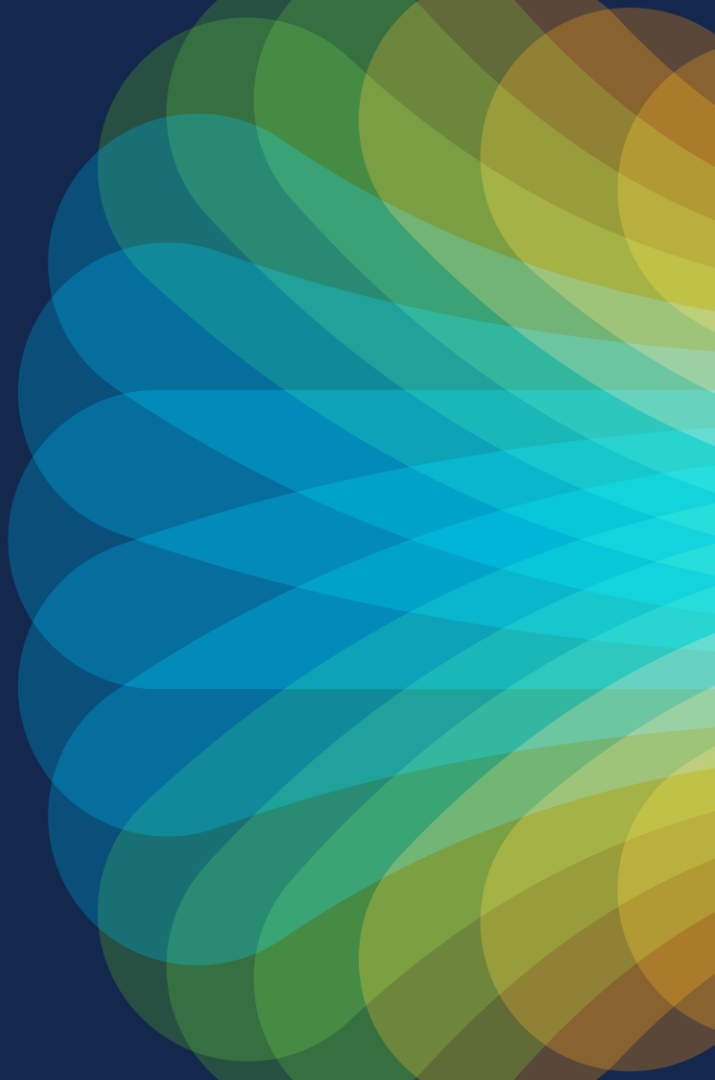
User Identity Beyond ISE

FTD 7.6

- 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

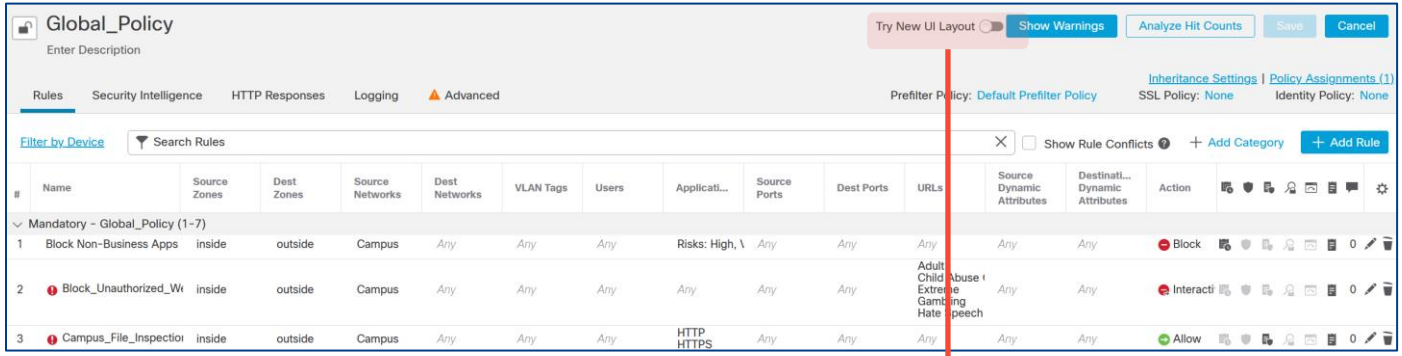
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

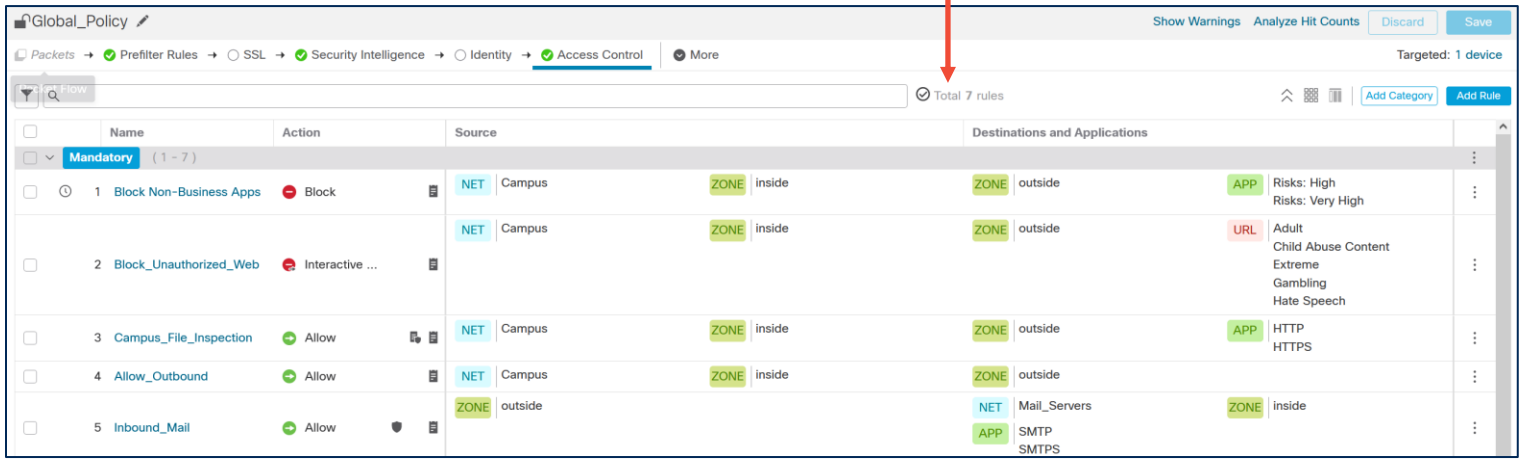
Management



Simplified Access Control Policy (ACP) View

FMC 7.2





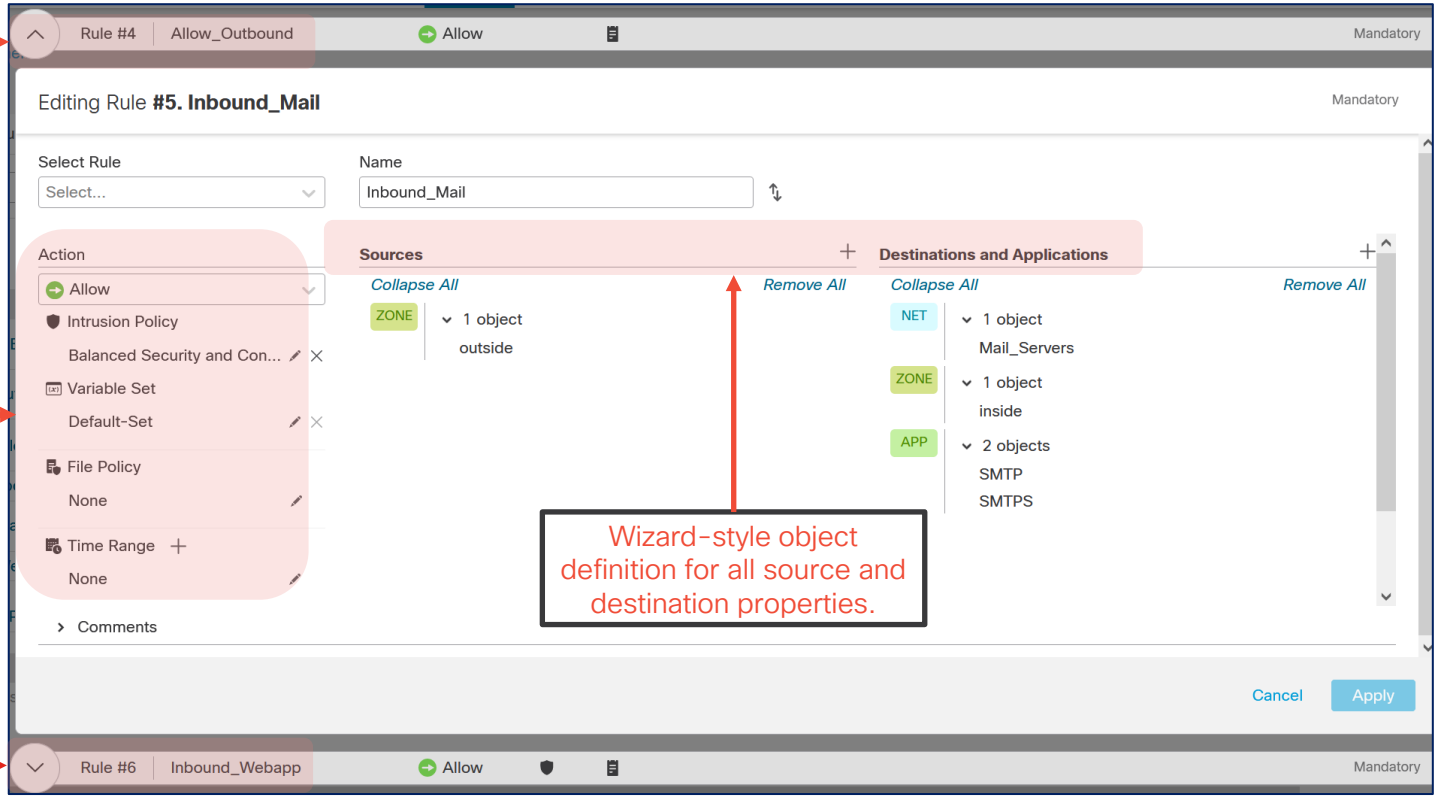
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Simplified ACP Rule Editor

FMC 7.2

Inline rule navigation.

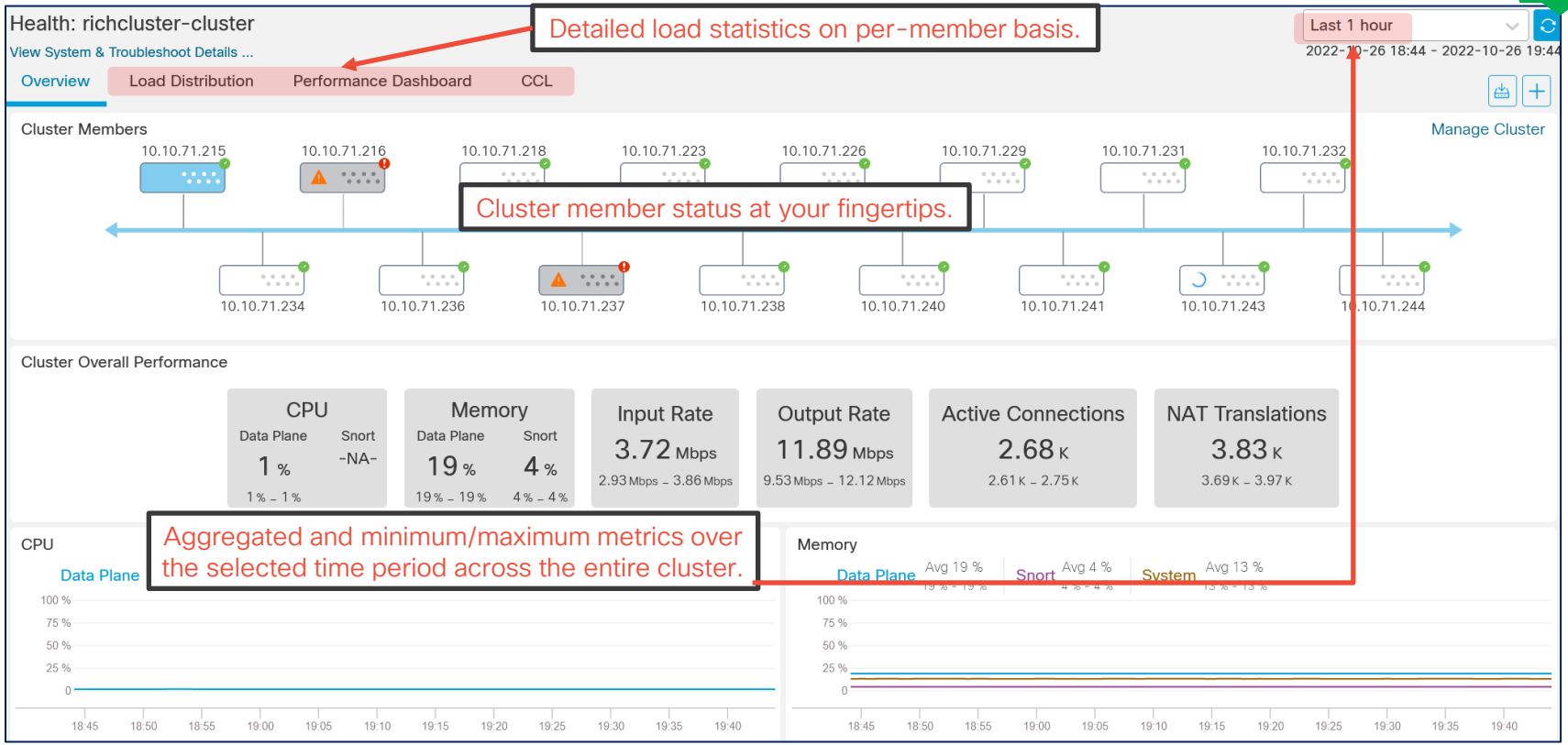
Direct access to all advanced actions.



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

Cluster Health Dashboard

FMC 7.3

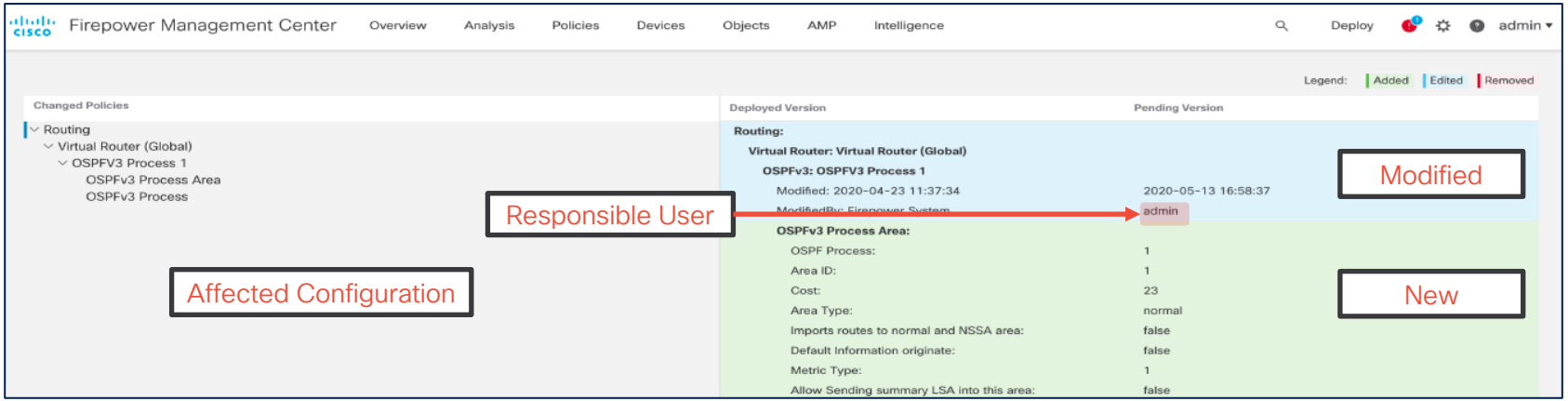


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Change Management

FMC 7.0+

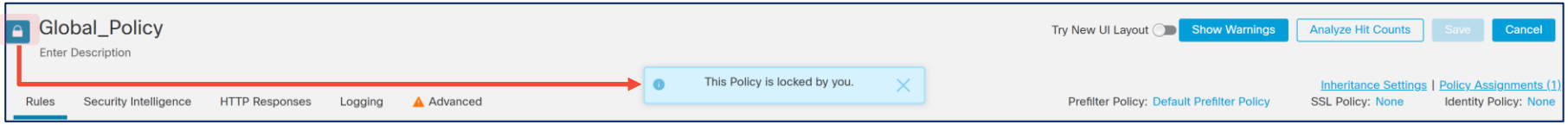
- Selective change deployment and detailed audit transcripts in FMC
  - Individual configuration changes can be filtered and deployed by user
  - Emergency rollback to one of 10 previous configuration versions
  - Separation of Access Rules, IPS, and File policy deployment in FTD 7.4

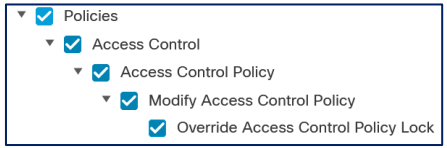


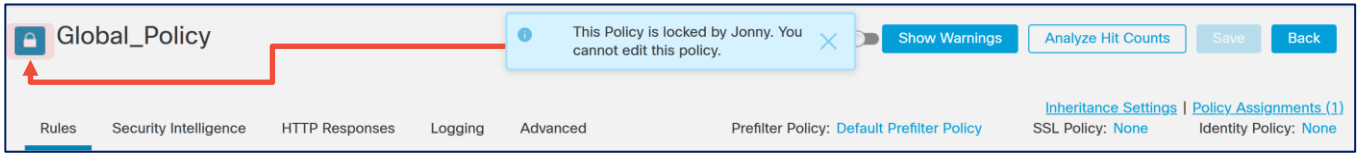
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

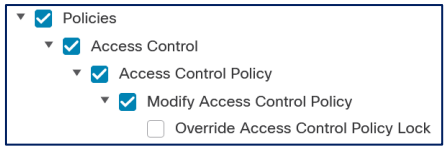
“Shallow” Access Policy Locking

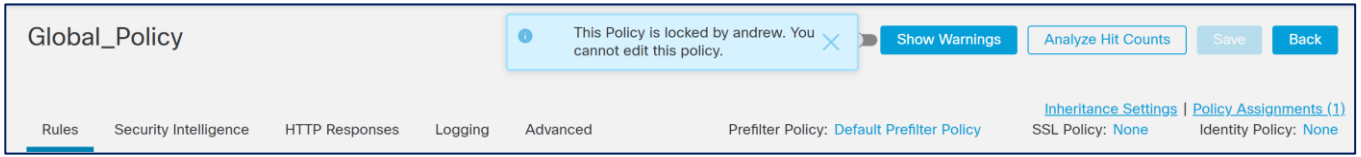
FMC 7.2











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

Workflow Mode and Change Logging

FMC 7.4+

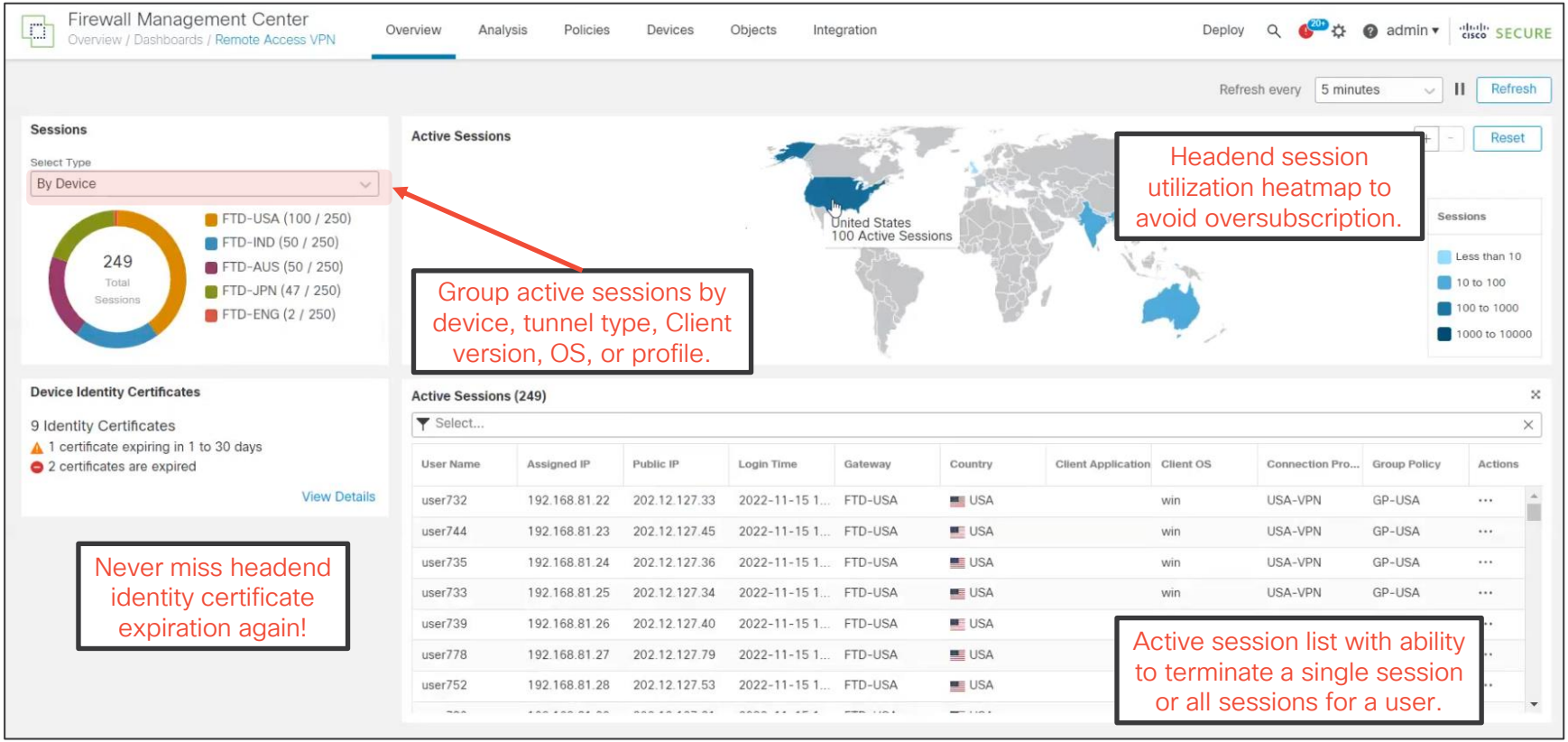
- Workflow Mode will require ticket approval for supported changes
  - Most policies and related objects are supported
  - Operator opens a change ticket before making changes
  - Ticket must be Rejected, Discarded, or Approved by an Approver
- Send configuration change syslogs with API link or full 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\"}],\"refe
rencesAddedList\":[],\"referencesDeletedList\":[],\"parentHierarchyList\":[],\"impactedDeviceList\":[],\"entityType\":\"Ser
viceObject\",\"entityName\":\"secure-sip-port\"}","parentUUid":"5e3fec7f-00a0-45fb-ac29-207b3d2af415","isGrouped":false}
```


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

VPN Monitoring Dashboard

FMC 7.3



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

Policy Analysis

FMC 7.4

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

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

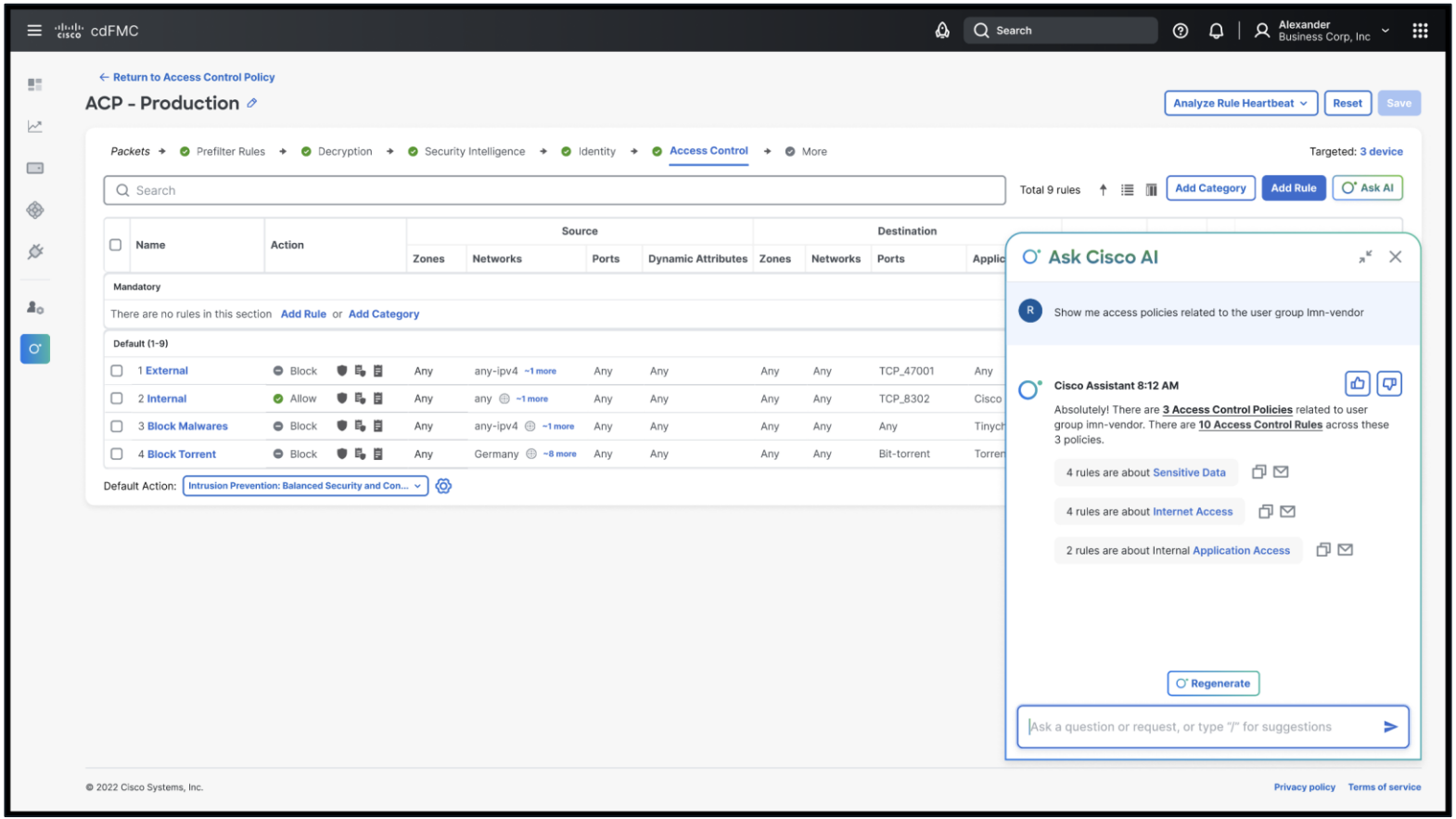
"Remove duplicate rules."

"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."

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

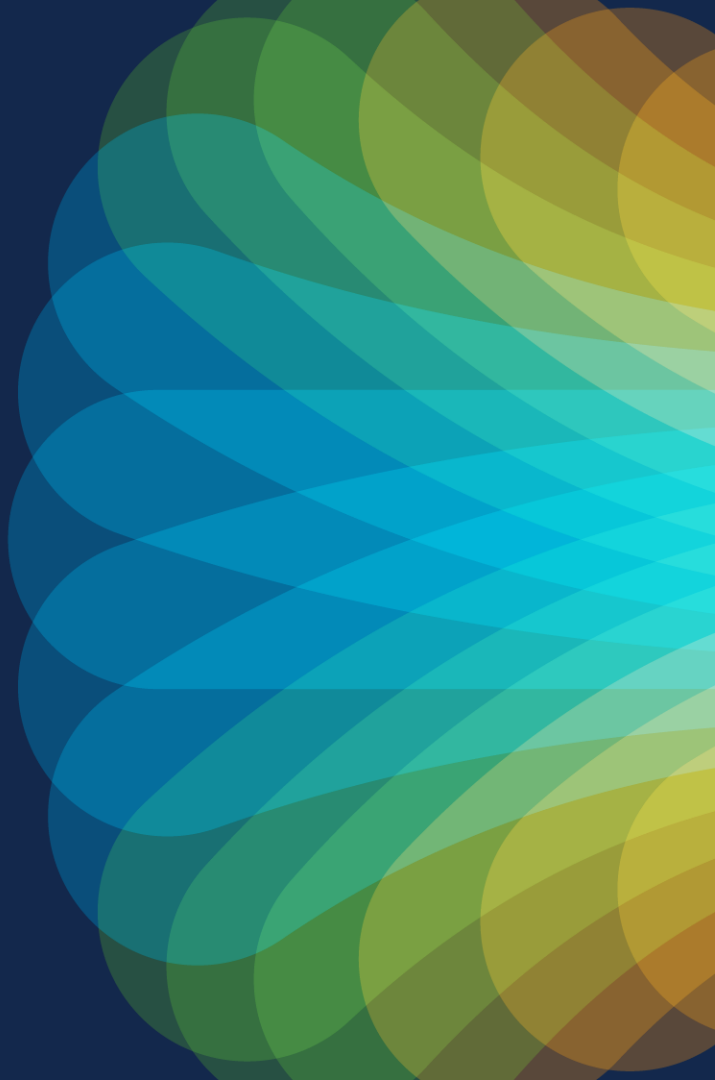
FMC View: AI Interactive Assistant

FMC 7.6



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

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 heterogenous enforcement points

Network Security (NetSecOps)

Secure Firewall

Secure Workload

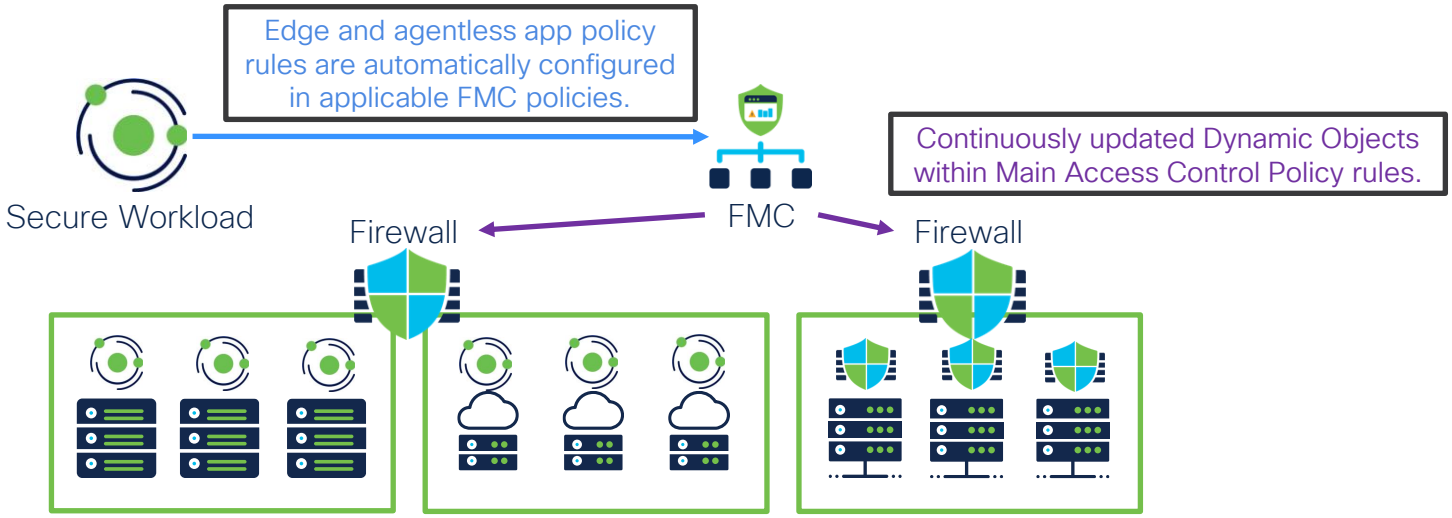
Distributed Firewall

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

Secure Workload Policy Extension to Firewall

Workload 3.6+

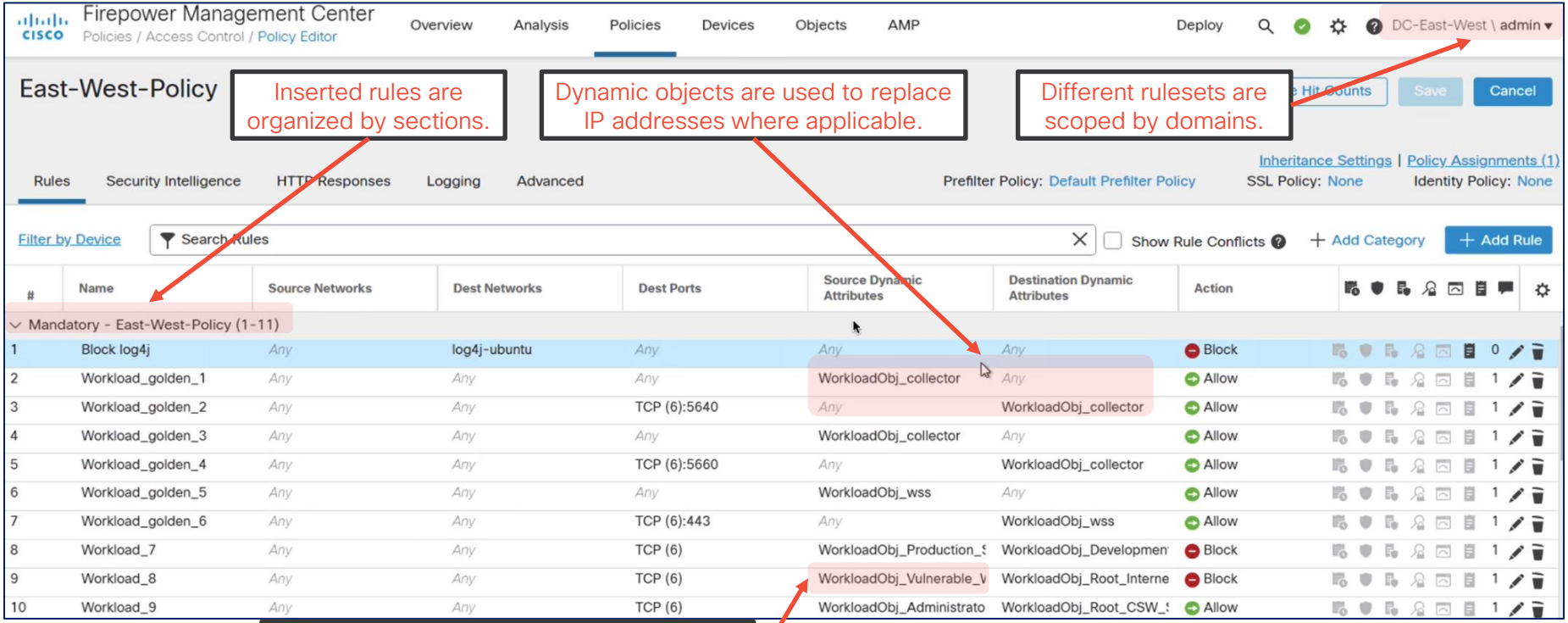
- Hybrid cloud microsegmentation with agents and network firewalls
  - North-South (edge) and East-West (lateral) policy enforcement



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

Secure Workload Policy Orchestration in FMC

Workload 3.6

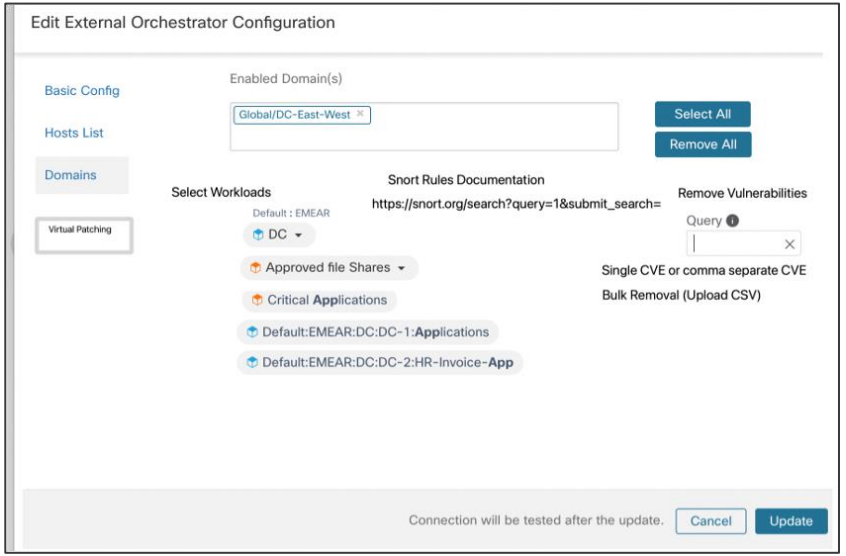


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Virtual Patching

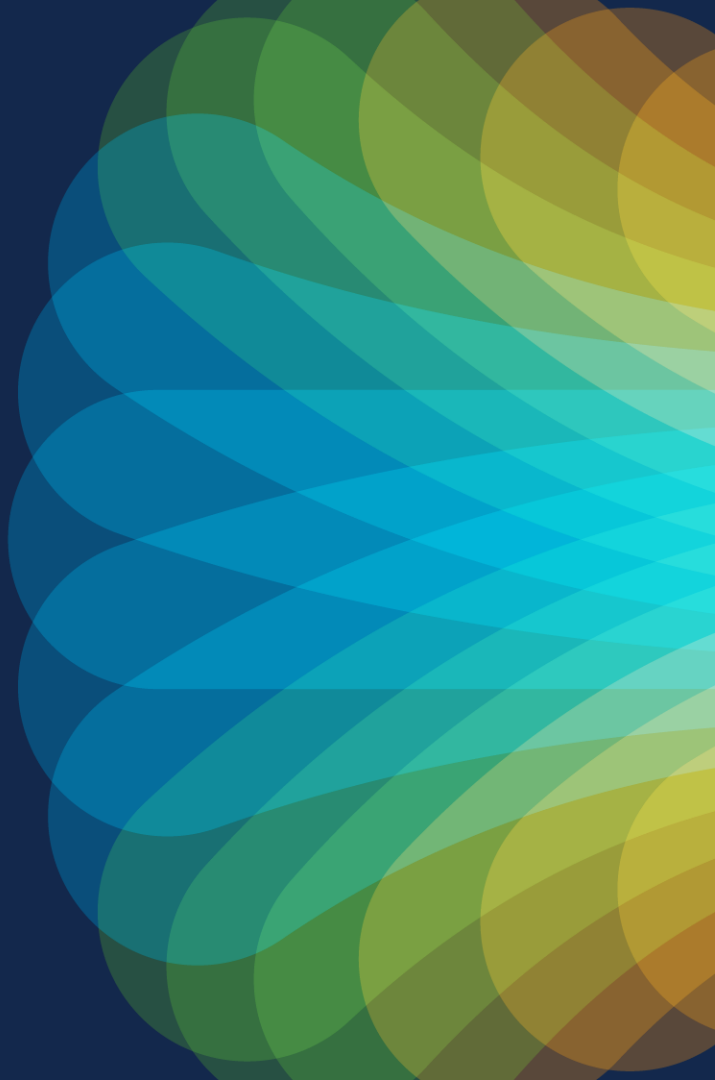
Workload 3.8

- 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



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

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

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

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!

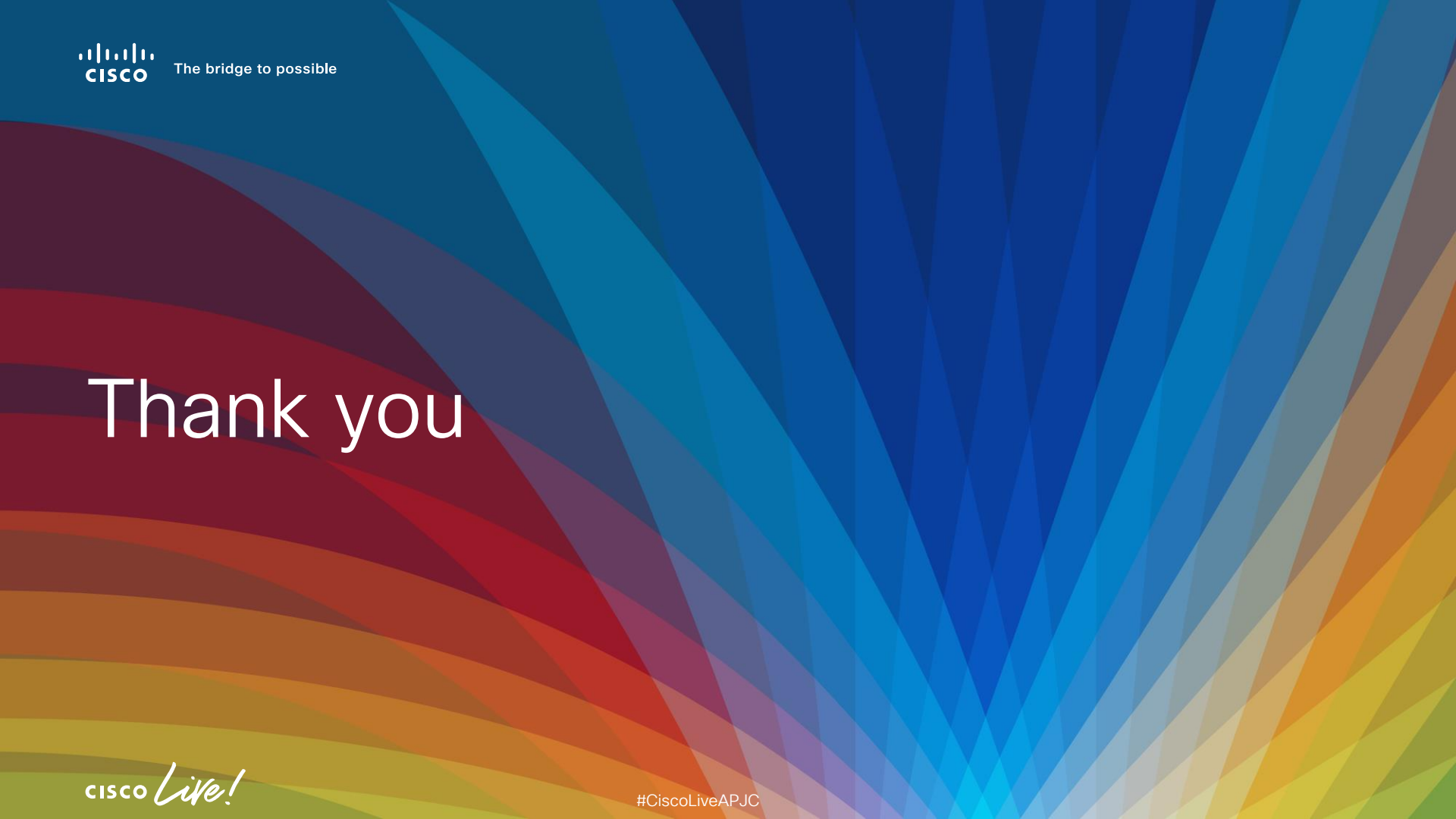
- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

© 2023 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 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

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


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC

cisco Live!

Let's go

#CiscoLiveAPJC