#CiscoLiveAPJC

The bridge to possible

Keeping Up on Network Security with Cisco Secure Firewall

Subtitle goes here

Andrew Ossipov
Distinguished Engineer, Portfolio CTO

BRKSEC-2236

Cisco Webex App

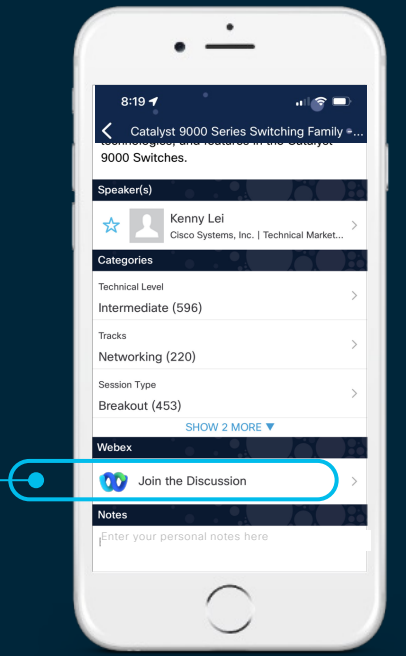
Questions?

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 Thursday 22 December, 2022.



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

Your Speaker

Andrew Ossipov

aeo@cisco.com

Distinguished Engineer

Portfolio CTO for Cloud and Network Security

Firewall Architecture, Threat Visibility, Hybrid Cloud, SSE

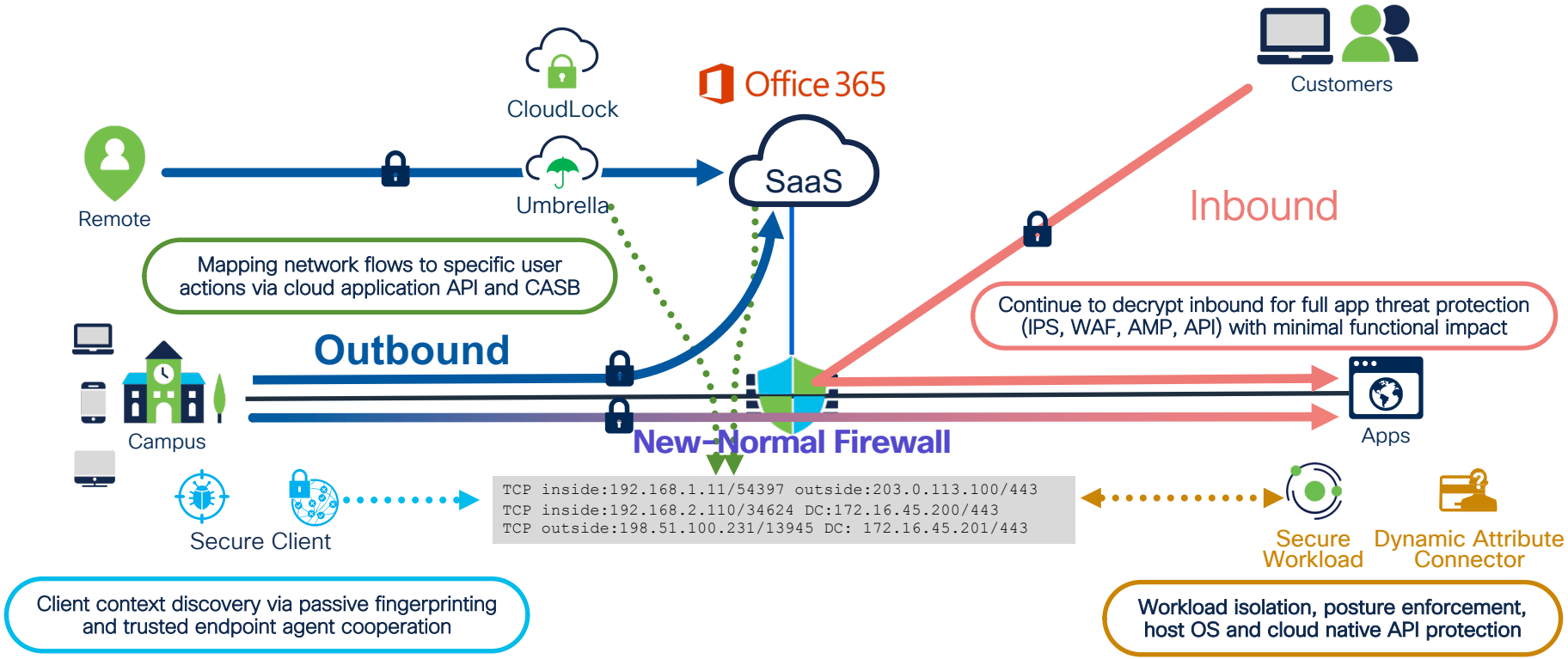
FTD

ASA

Agenda

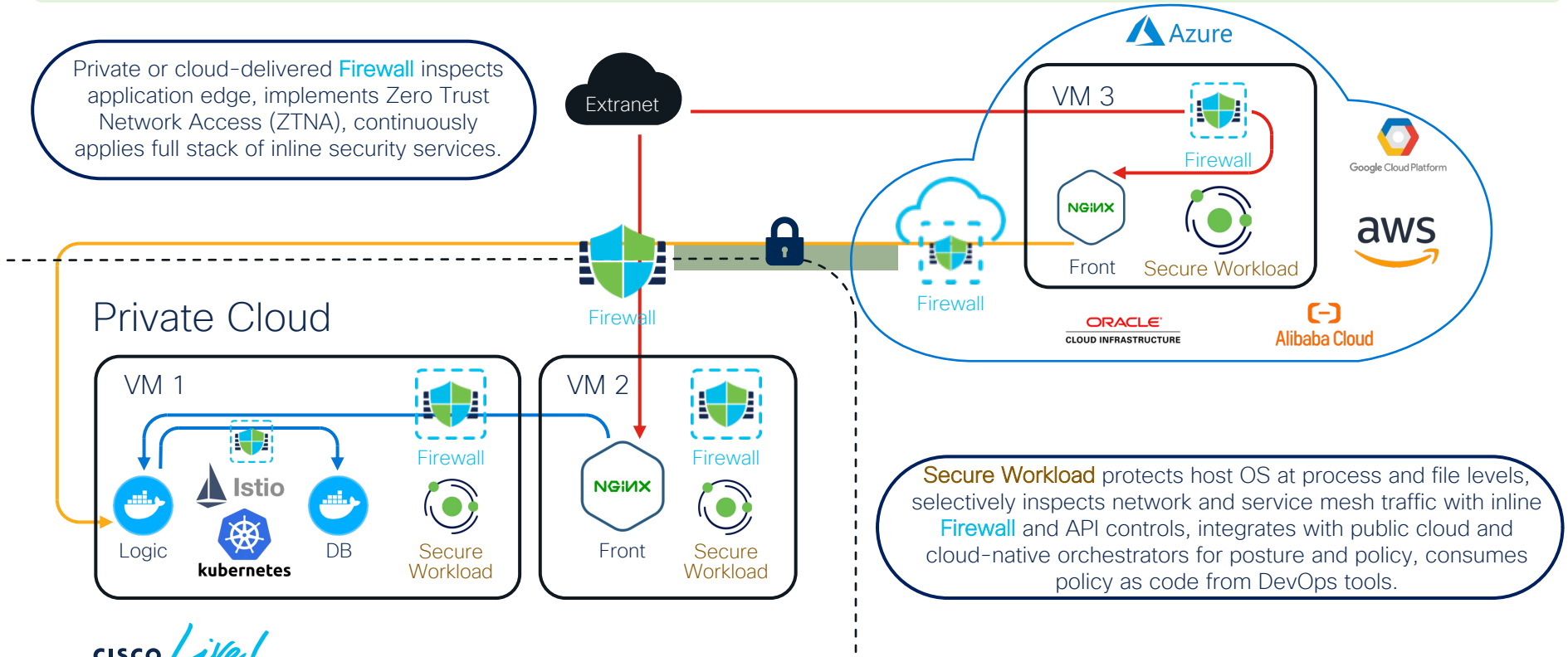
- Introduction
- Platforms
- Threat Prevention
- Connectivity
- Private and Public Cloud
- Management
- Secure Workload
- Conclusion

Secure Firewall: Inspect, Infer, and Cooperate



Firewall Vision: Network, Workload, and Cloud

Single security management plane to abstract end-to-end policy intent from enforcement point specific configuration.



Platforms

Secure Firewall 3100 Overview

FTD 7.1

ASA 9.17

Appliance-Mode Security Platform for FTD or ASA Application

- Fixed configurations: 3105, 3110, 3120, 3130, 3140
- Lightweight virtual Supervisor module w/Multi-Instance and Clustering
- Integrated Datapath FPGA w/Flow Offload and Crypto Engine
- Rear dual redundant power supplies and fan trays

SFP Data Interfaces

- 8x1/10GE on Firepower 3105-3120
- 8x1/10/25GE on Firepower 3130-3140

1RU

Copper Data Interfaces

- 8x10M/100M/1GE Ethernet

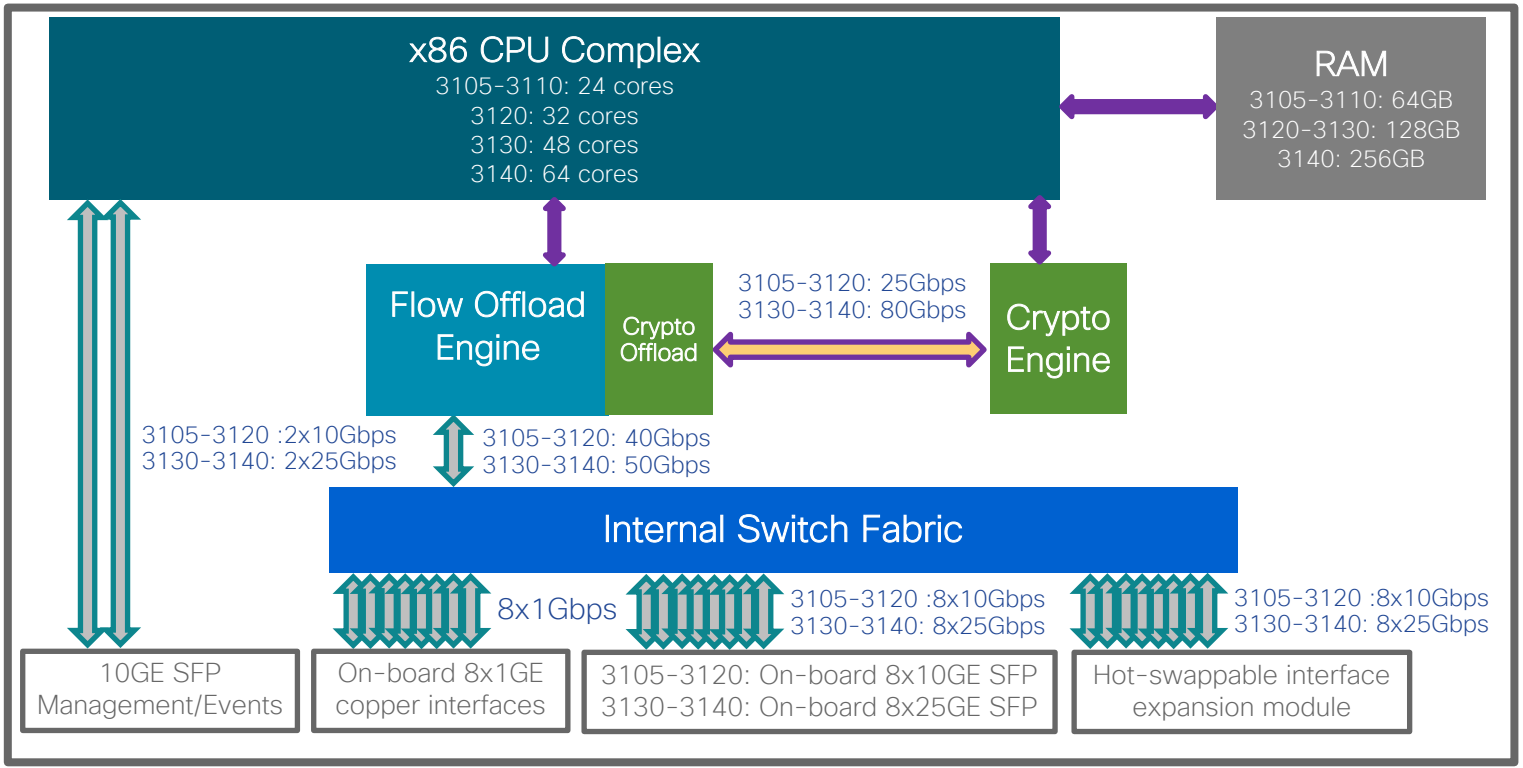
Network Module

- 8x1/10/25GE or 6x10/25GE FTW on Firepower 3105-3120
- 4x40GE or 2x40GE FTW on Firepower 3130-3140

Secure Firewall 3100 Architecture

FTD 7.1

ASA 9.17



System Bus

Ethernet

Chip-to-Chip Link

Secure Firewall 3100 Performance

FTD 7.2

ASA 9.18

	3110	3120	3130	3140
FW+AVC+IPS 1024B Avg Packet	17Gbps (6Gbps with 450B)	21Gbps (8Gbps with 450B)	38Gbps (11.5Gbps with 450B)	45Gbps (14Gbps with 450B)
IPsec VPN 1024B Avg Packet	11Gbps (11Gbps per tunnel)	13.5Gbps (13.5Gbps per tunnel)	33Gbps (30Gbps per tunnel)	39Gbps (31Gbps per tunnel)

Up to 7x Boost in FW+AVC+IPS

Up to 17x Boost in IPsec VPN

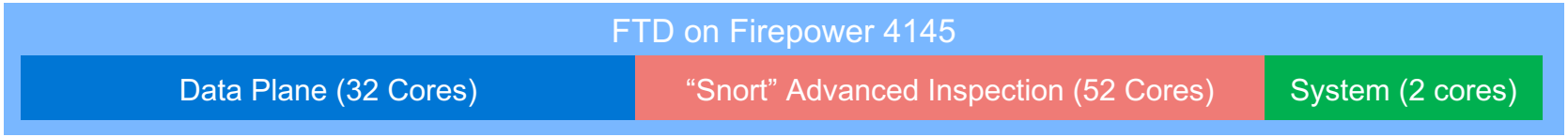
Up to 14x Boost in TLS

*Performance Estimates are subject to change in public release.

Configurable CPU Core Allocation

FTD 7.3

- FTD uses a static CPU core allocation between Data Plane and Snort



- Tailor FTD to a specific use case with a configurable allocation
  - Select from a few templates in FTD 7.3; dynamic in the future
  - VPN headend or basic stateful firewall would use more Data Plane cores
  - Heavy IPS and file inspection would bias toward more “Snort” cores

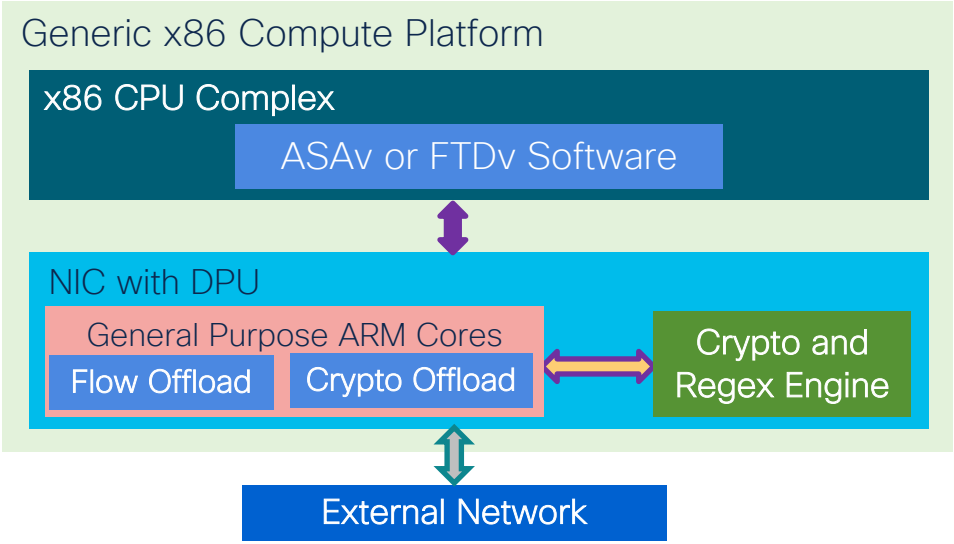
Virtual Firewall with Data Processing Unit (DPU)

Future

- Network Interface Controller (NIC) with a DPU on a generic server
  - Inline hardware acceleration for broad packet processing functionality
  - Perfect opportunity to accelerate virtual firewalls in hybrid data centers

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

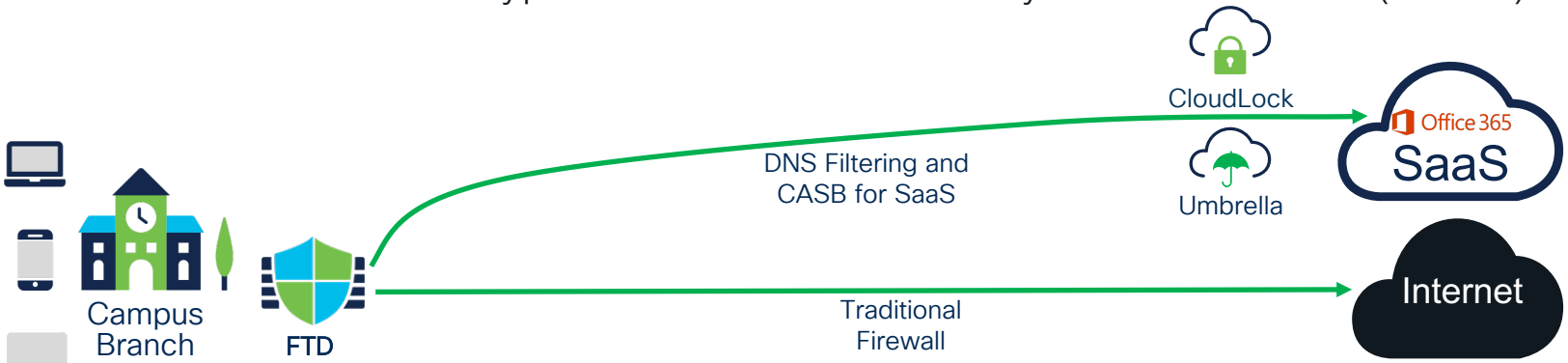
If a DPU is present, main ASAv or FTDv software deploys ARM software components to program inline acceleration of flow processing, IPsec and (D)TLS encryption, Regex matching, and other capabilities.



Threat Protection

Enhance Firewall with Umbrella Cloud Security

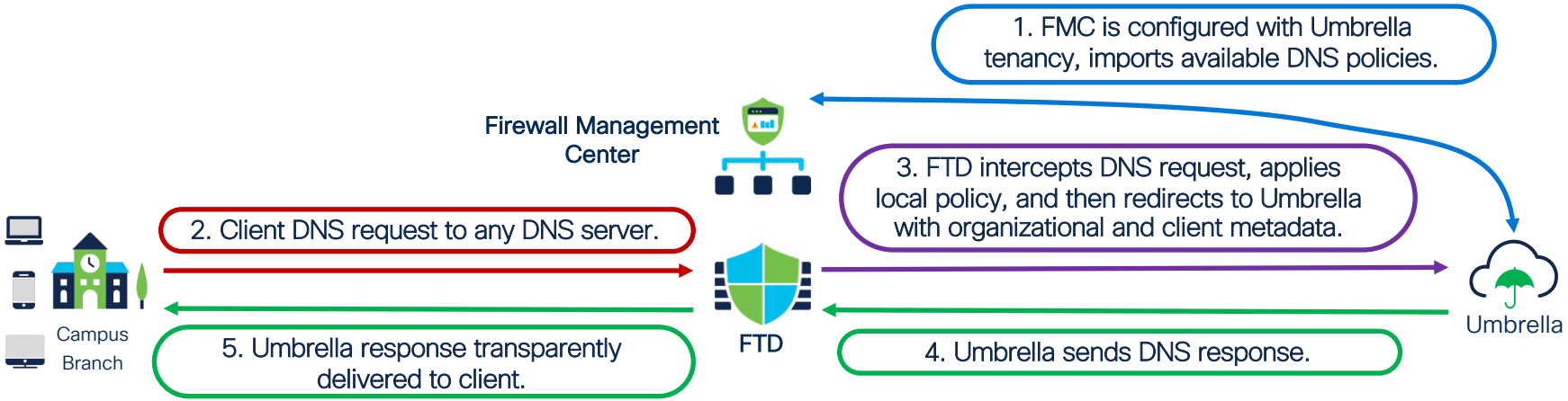
- Edge firewall is less effective against some outbound traffic
  - Dynamically changing DNS and undecryptable TLS connections
- Selectively redirect DNS, SaaS, and other traffic to Umbrella instead
  - Cloud-delivered DNS blocks most threats early with no local cycles spent
  - No SaaS traffic decryption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



DNS Redirection to Umbrella

FTD 7.2

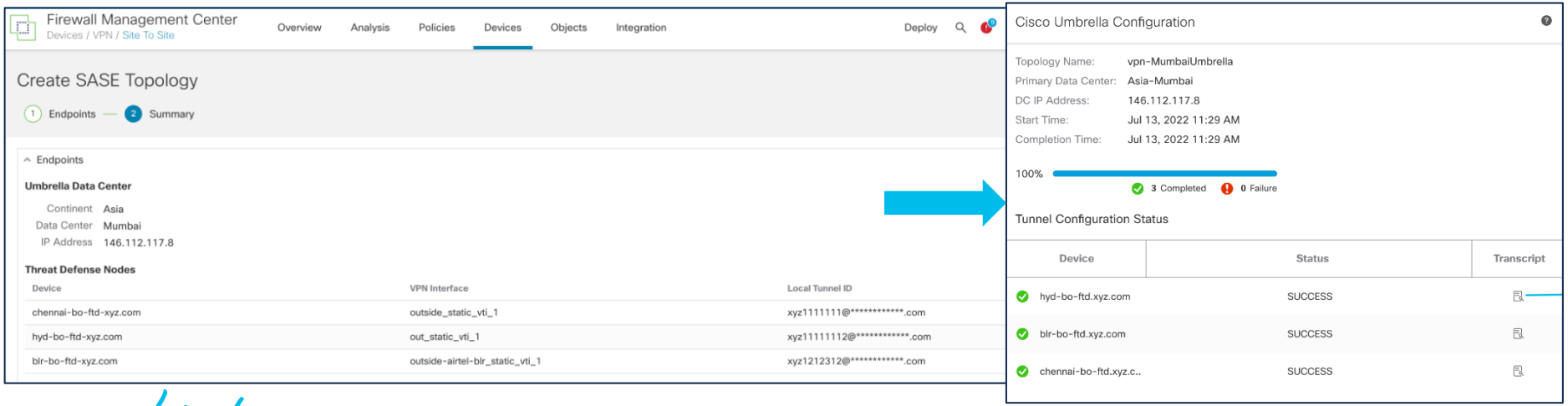
- FMC registered with Umbrella for bi-directional integration
  - Umbrella DNS policies can be attached to FTD Access Control Policy
  - FTD includes inline organization and device identifiers, original client IP



Automatic Umbrella Tunnel for SASE

FTD 7.3

- New SASE Topology in FMC redirects all-port traffic to Umbrella SIG
  - Builds on DNS Connector feature to simplify bi-directional provisioning
  - Modeled as a Virtual Tunnel Interface (VTI) for policy-based redirection
  - Load-balancing across multiple tunnels with per-tunnel custom IKE ID



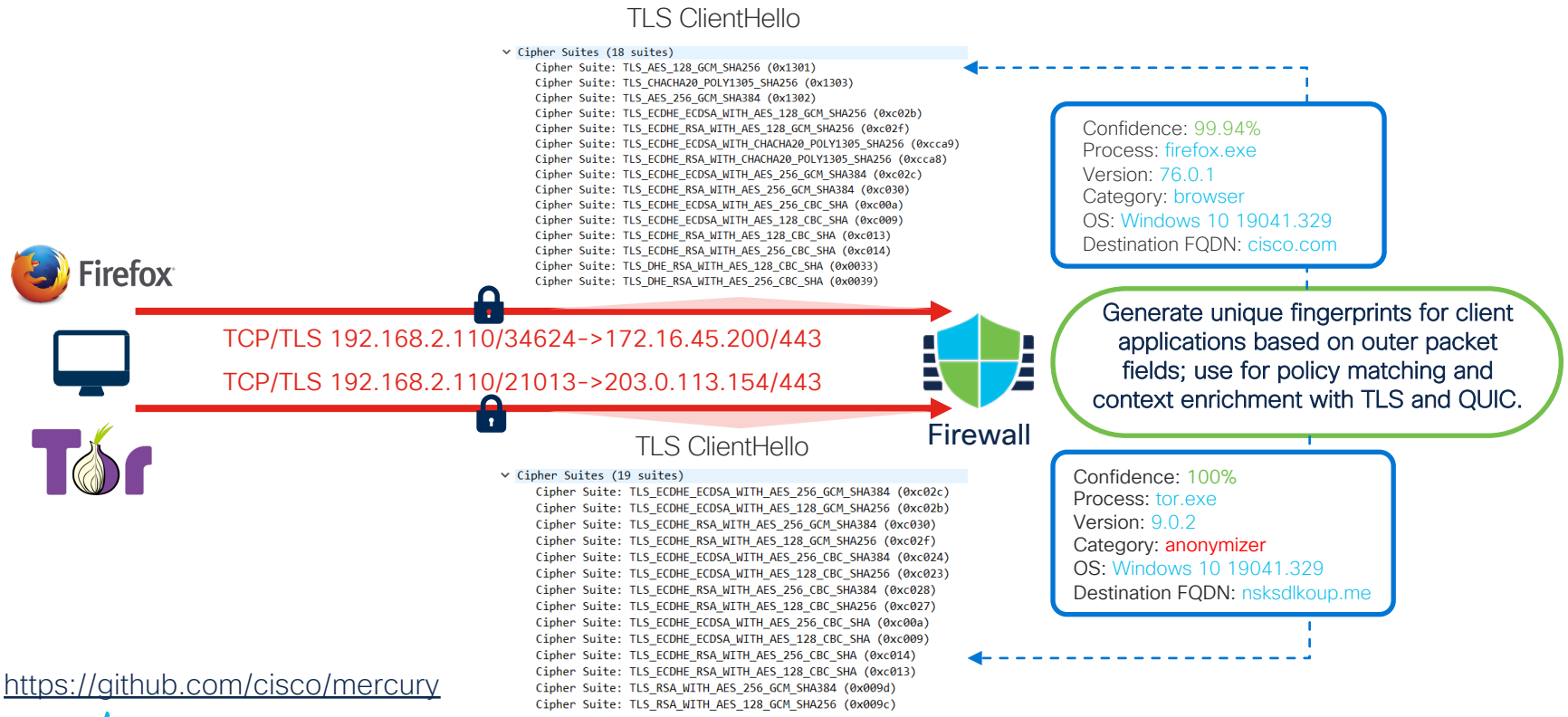
Snort 3 IPS Engine

FTD 7.0+

- Thwart modern threats with the trusted NGIPS engine update
  - Much higher efficacy and performance with a multi-threaded architecture
  - Native support for modern protocols, such as HTTP/2 and QUIC
  - Improved human-readable signature language
  - Tunable inspection level within a single policy with Rule Groups
- Multiple must-have new capabilities require Snort 3
  - Encrypted Visibility Engine (EVE) for ML-enabled security
  - Comprehensive Portscan attack detection and prevention
  - Native TLS 1.3 Decryption
  - Elephant Flow detection and impact mitigation

Encrypted Visibility Engine (EVE)

FTD 7.1

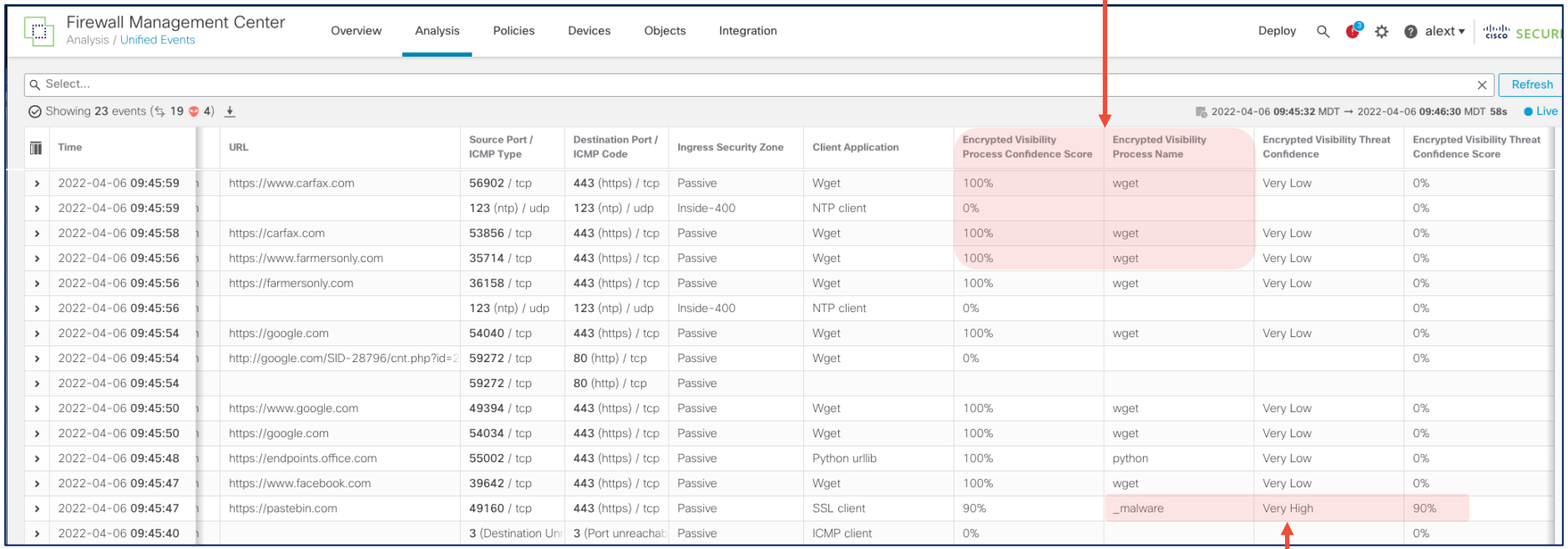


https://github.com/cisco/mercury

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.



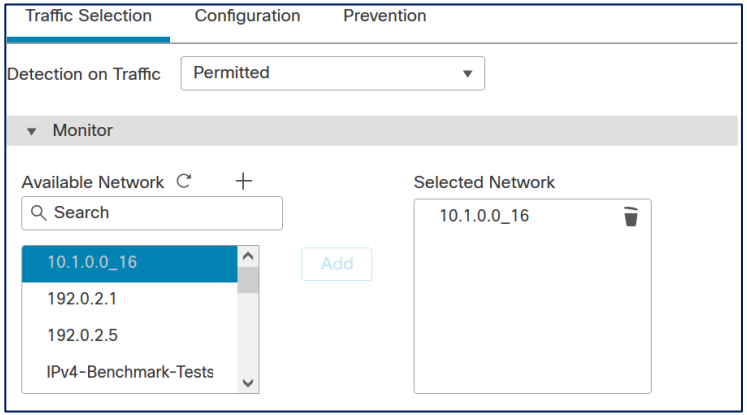
Time	URL	Source Port / ICMP Type	Destination Port / ICMP Code	Ingress Security Zone	Client Application	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
2022-04-06 09:45:59	https://www.carfax.com	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%

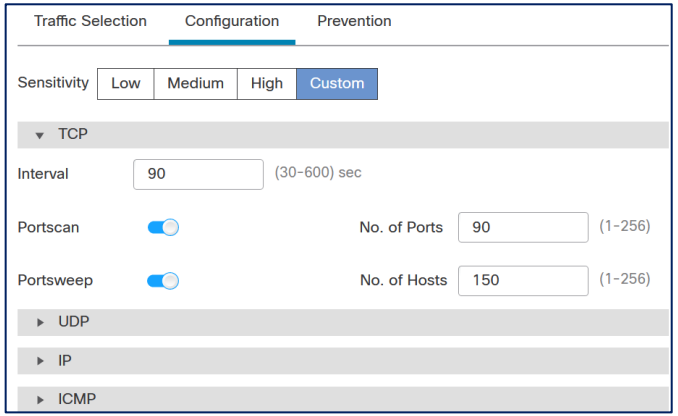
Inference-based threat alert and confidence level.

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

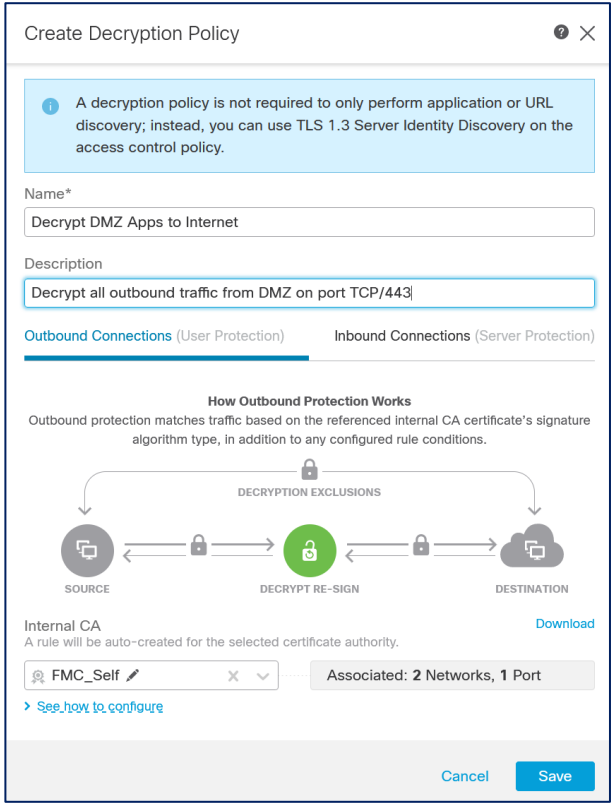




Simplified TLS Decryption Policy

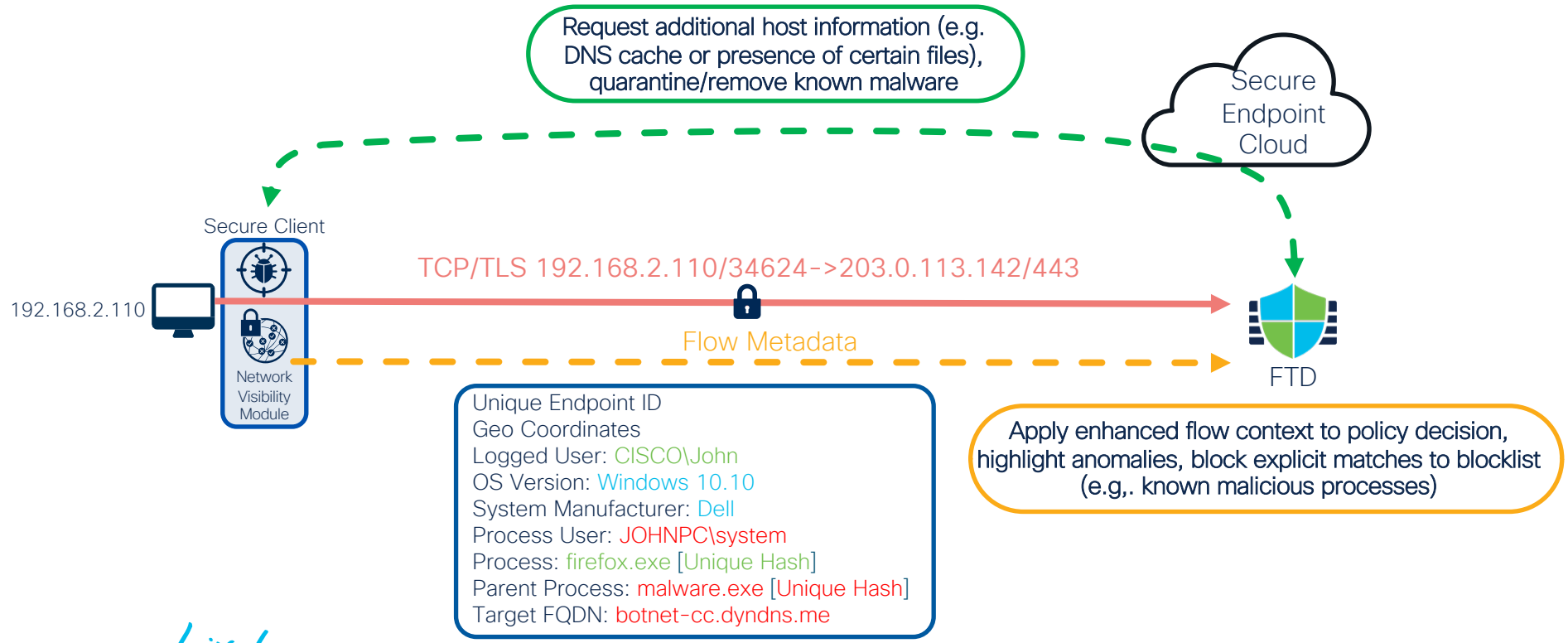
FTD 7.3

- 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 is supported
- Wizard-style flow for Decryption policy
  - Outbound is ineffective for most SaaS apps
  - Inbound gives full control with access to app server



Real-time Flow Context via Endpoint Intelligence

Future

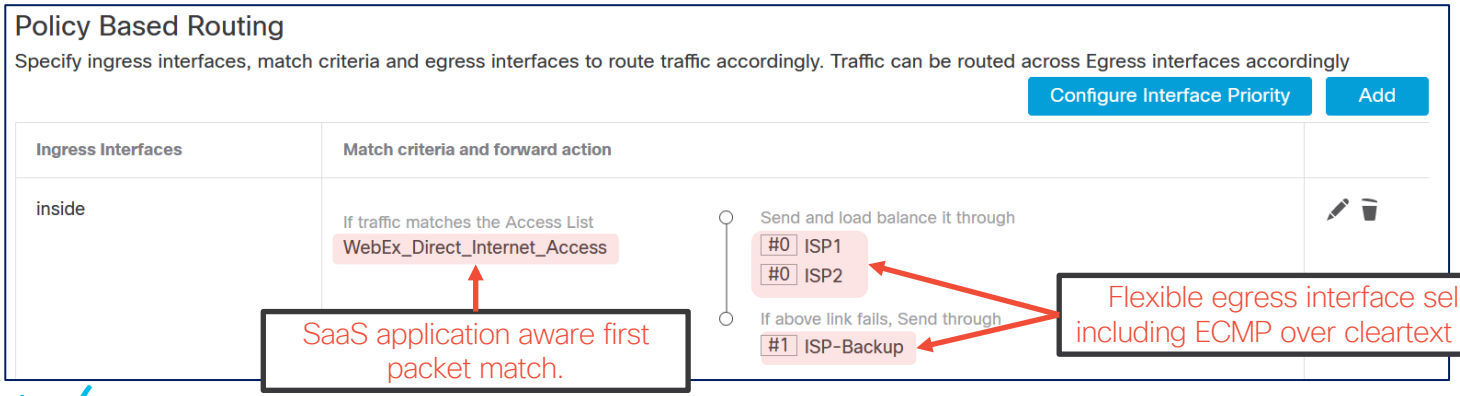


Connectivity

Application-Aware Policy Routing

FTD 7.1

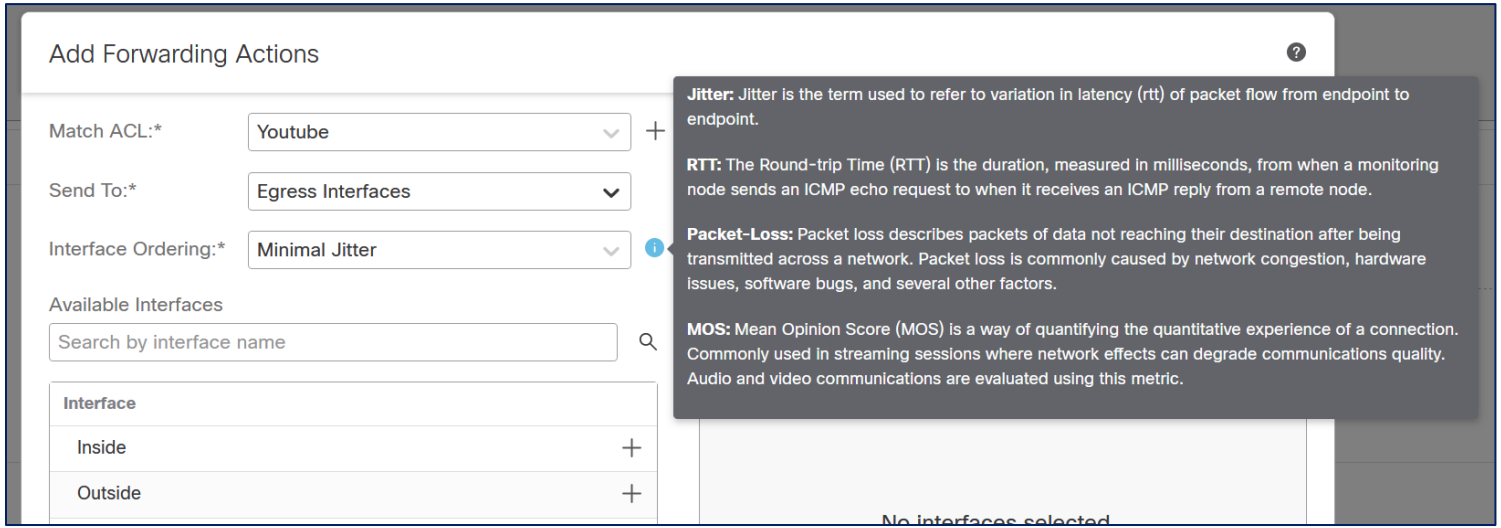
- Native support for Policy Based Routing configuration in FMC
  - Commonly used SaaS applications can be used as matching criteria
  - DNS snooping to Trusted Servers to support domain pattern matching
  - Data Plane maps app names to IP addresses with Network Service Groups
- Used in Direct Internet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



Path Monitoring and Quality-Based Routing

FTD 7.2

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

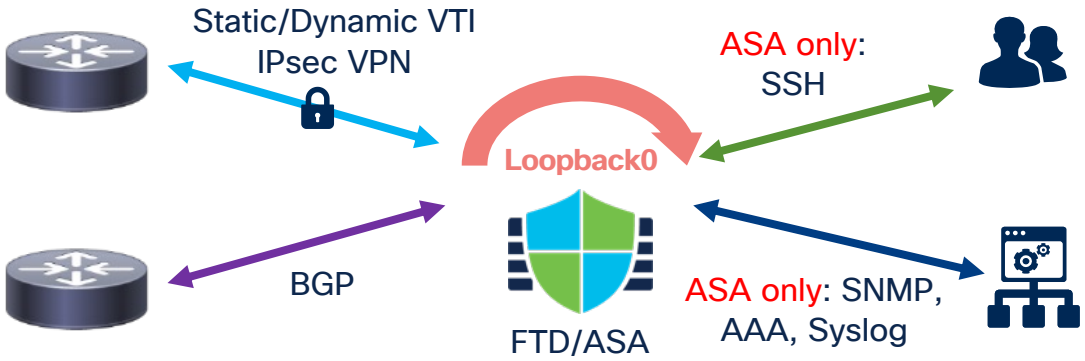


Loopback Interface

FTD 7.3

ASA 9.18.2

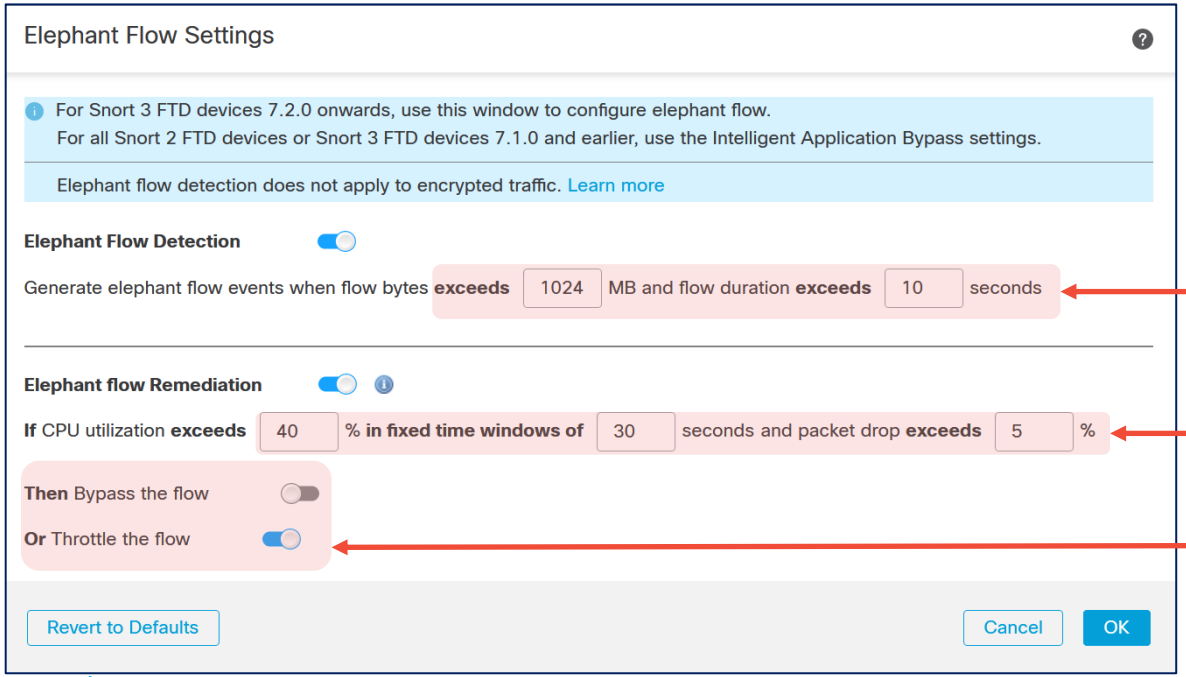
- Abstract to- and from-device connectivity from physical interfaces
  - IPv4 and IPv6 addressing in routed and transparent (except for VTI) modes
  - HA/failover and clustering (except for VTI) support



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.

Client Zero Trust Network Access (ZTNA)

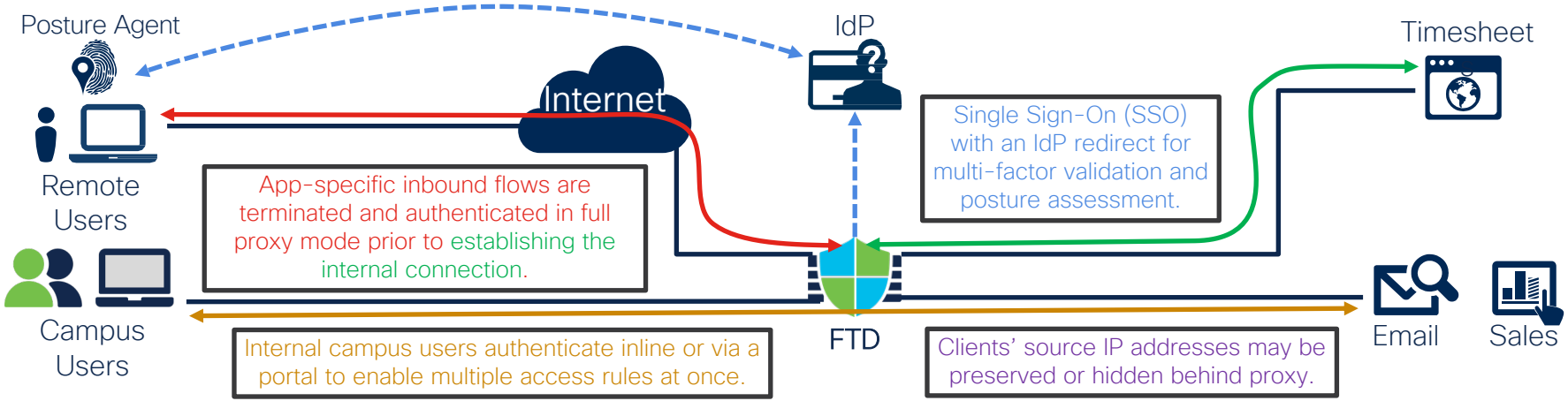
FTD 7.2

- ZTNA expands beyond network admission control alone
  - User activity must be continuously tracked throughout the app session
  - Firewall, TLS Decryption, IPS, and File/Malware protection are critical
- Secure Client (formerly AnyConnect) delivers ZTNA with Firewall
  - Dynamic Policies and Access Lists for granular posture-driven app access
  - Single Sign-On (SSO) with SAML for unified authentication
  - Certificate-based and Duo Passwordless authentication for ease of use
  - Load-Balancing across physical and virtual appliances for scalable access
  - Client profile management and distribution with SecureX Device Insights

Clientless ZTNA

Future

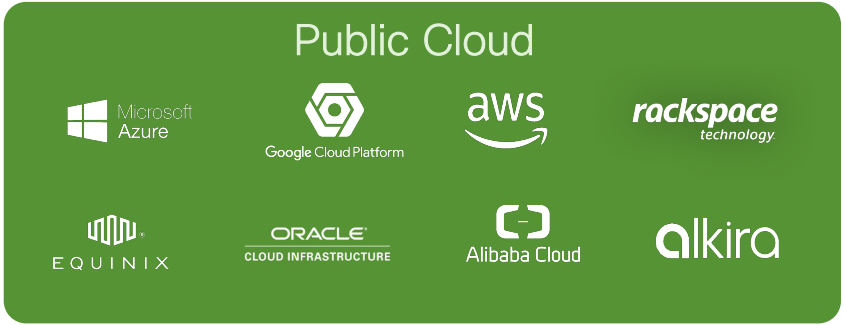
- Expand Captive Portal capabilities into a full ZTNA proxy
  - External Identity Provider (IdP) integration with posture assessment
  - Support both inbound and internal (“BeyondCorp”) segmentation



Private and Public Cloud

Consistent Security in Multi-Cloud Deployments

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

Automation with Infrastructure-as-Code

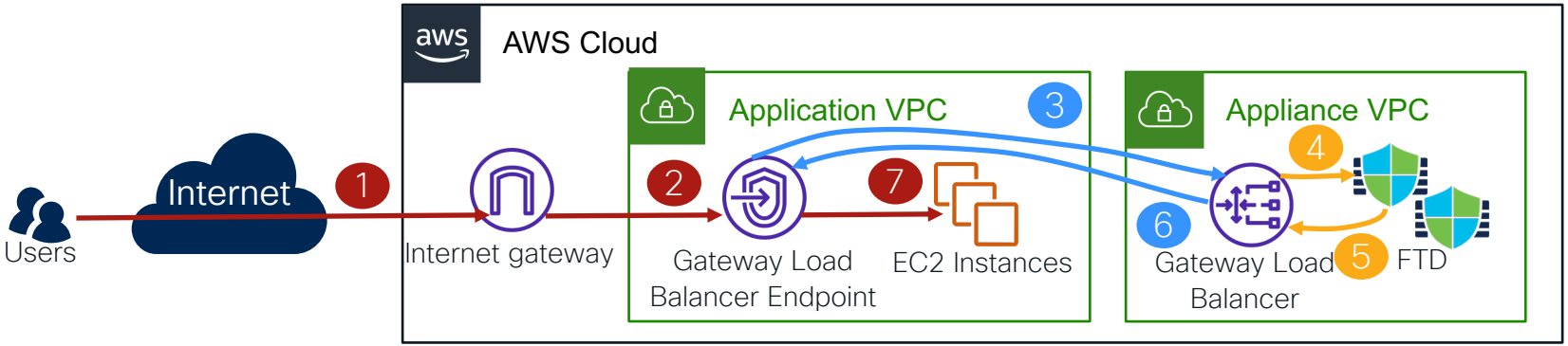
- Secure Firewall instantiation with public cloud templates
- Declarative Teraform templates for ASA and FTD (via FMC)
  - FTD Dynamic Object integration with HashiCorp Consul
- Imperative Ansible tasks for ASA and FTD (FDM and now FMC)
- Continuously updated Cisco DevNet repositories
  - https://developer.cisco.com/secure-firewall/cloud-resources/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

Gateway Load-Balancer in AWS and Azure

FTD 7.1+

ASA 9.17+

- Network firewall service insertion for inbound and outbound flows
  - Redirection with GEneric NEtwork Virtualization Encapsulation (GENEVE)
  - Bring-your-own TLS decryption with available software capabilities

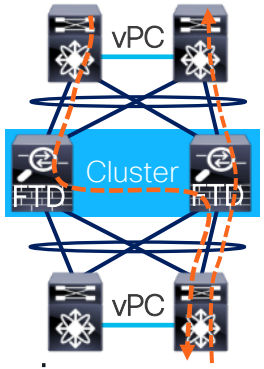


- Autoscale and snapshot-based instantiation in FTD 7.2 and ASA 9.18

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

Attribute-Based Policies

FTD 7.0+

Custom Orchestrator

Push Model: FMC REST API for populating/updating attribute mappings synchronously.

Name	Action	Source		Destination		Applications
		Networks	Dynamic Attributes	Networks	Dynamic Attributes	
Allow Windows Updates	Allow	Any	Windows_OS	Any	Any	Windows Update
Allow WebApp to DB	Allow	Any	WebApp_Logic	Any	DB_Cluster	Any

vmware aws Azure Office 365 GitHub

Dynamic Attribute Connector

Pull Model: Orchestrator-specific Connectors for subscribing to near-real-time updates.

FMC

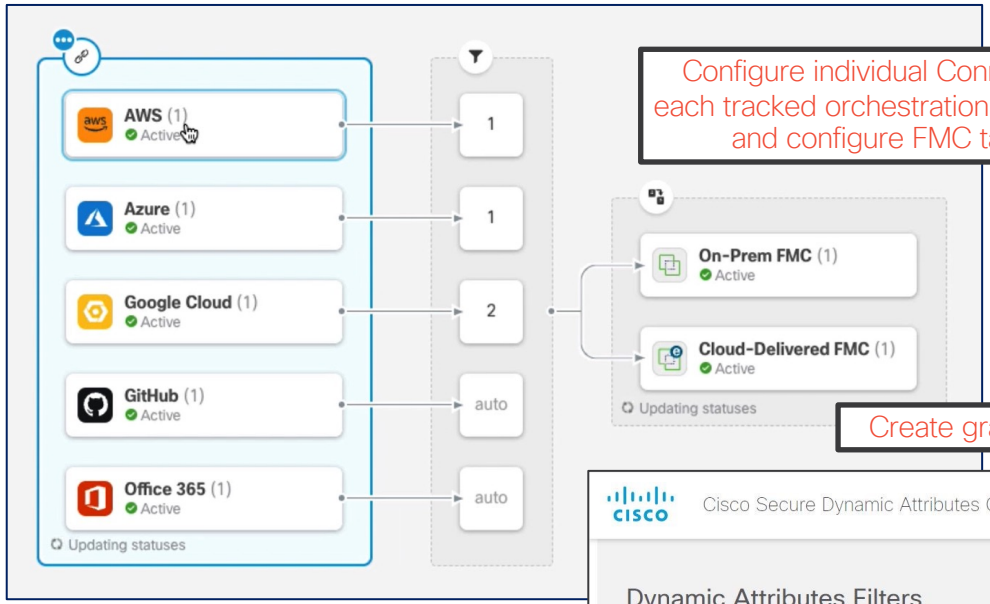
Label	IP Address
WebApp_Logic	192.168.1.151
Windows_OS	192.168.1.120-130
DB_Cluster	172.16.45.90

Real-time mapping updates without a full configuration deployment.

FTD FTD FTD

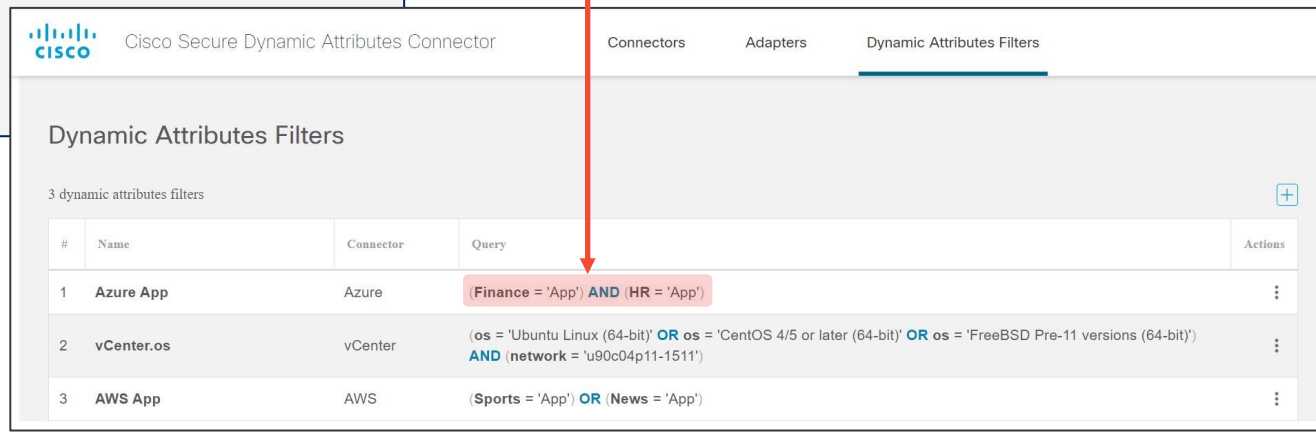
Dynamic Attributes Connector User Interface

FTD 7.0+



Configure individual Connectors for each tracked orchestration environment and configure FMC targets.

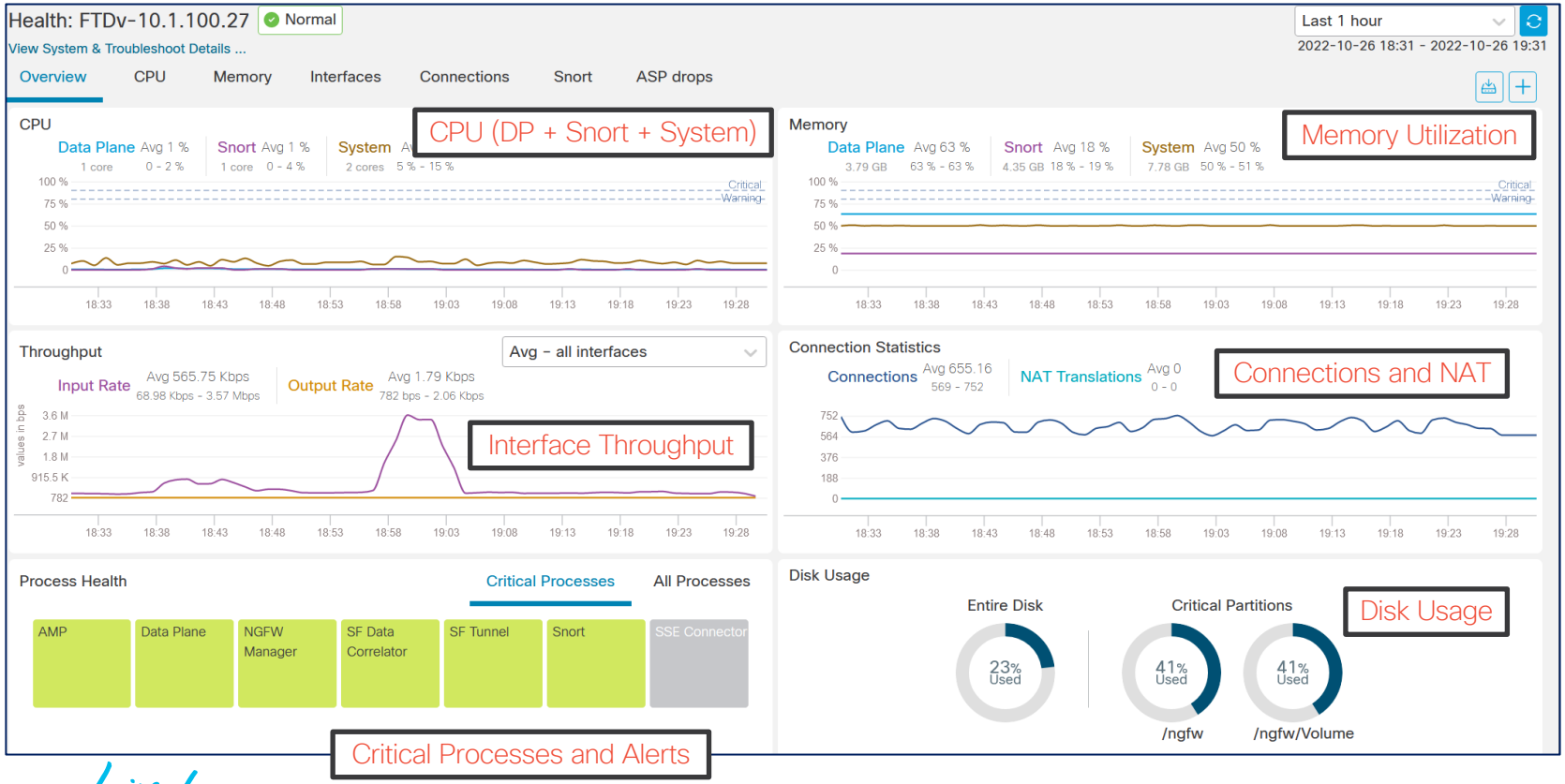
Create granular attribute filters to reduce noise.



Management

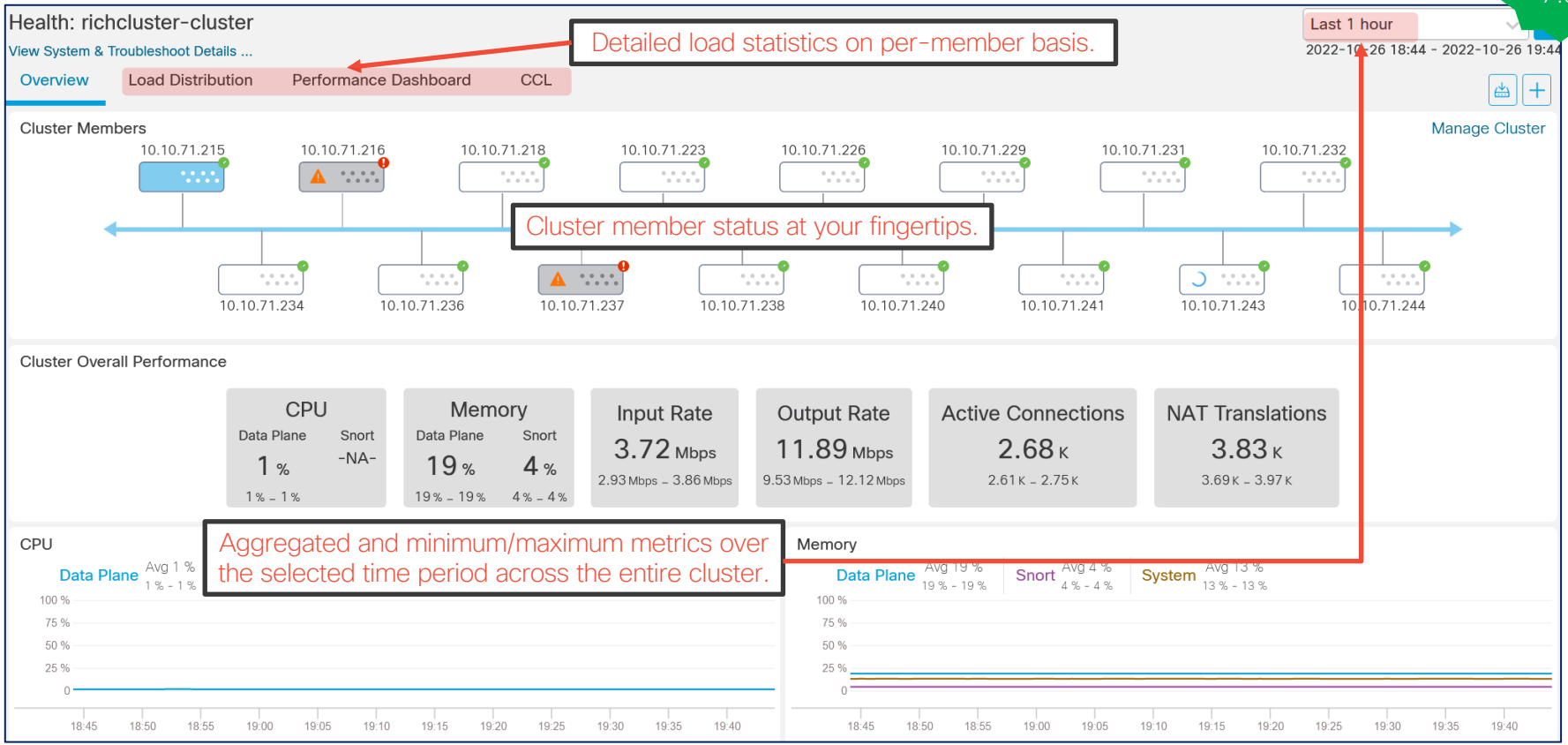
FTD Health Dashboard

FMC 6.7+



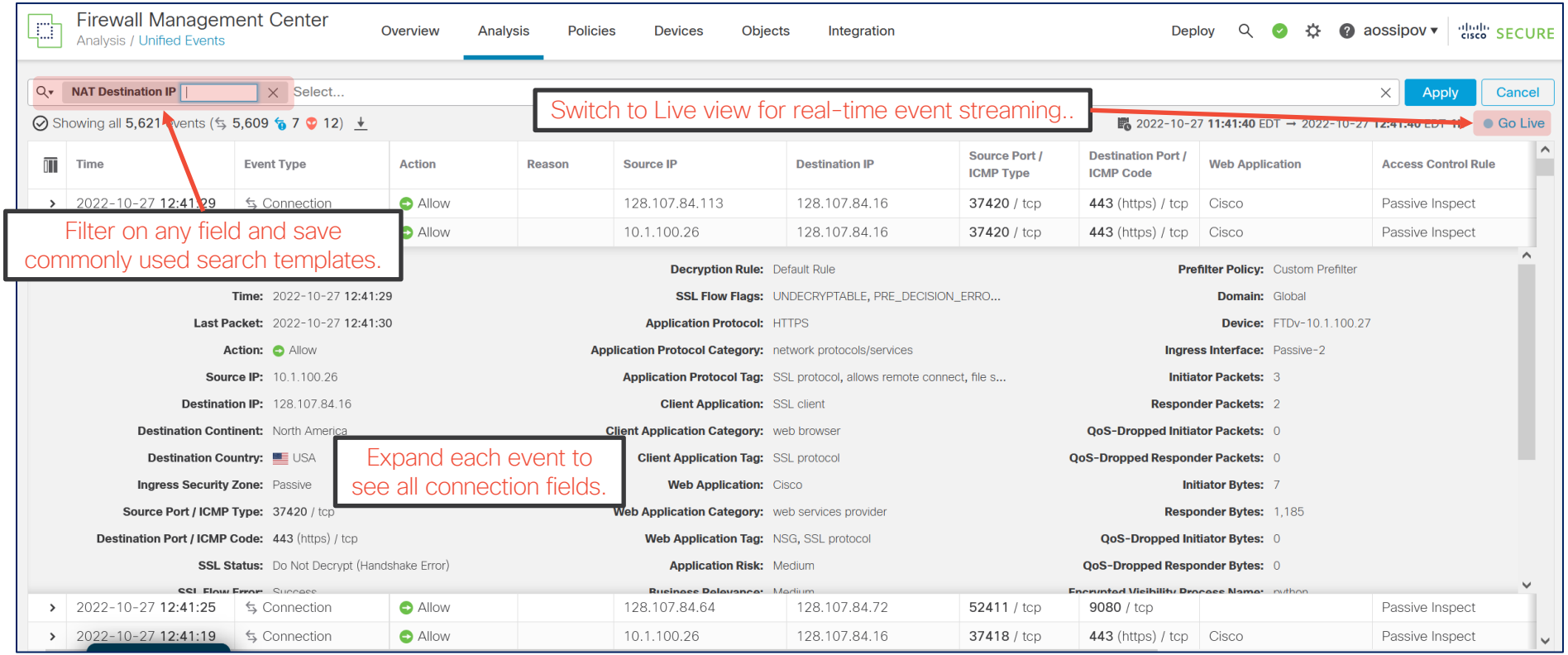
Cluster Health Dashboard

FMC 7.3



Unified Events with Live View

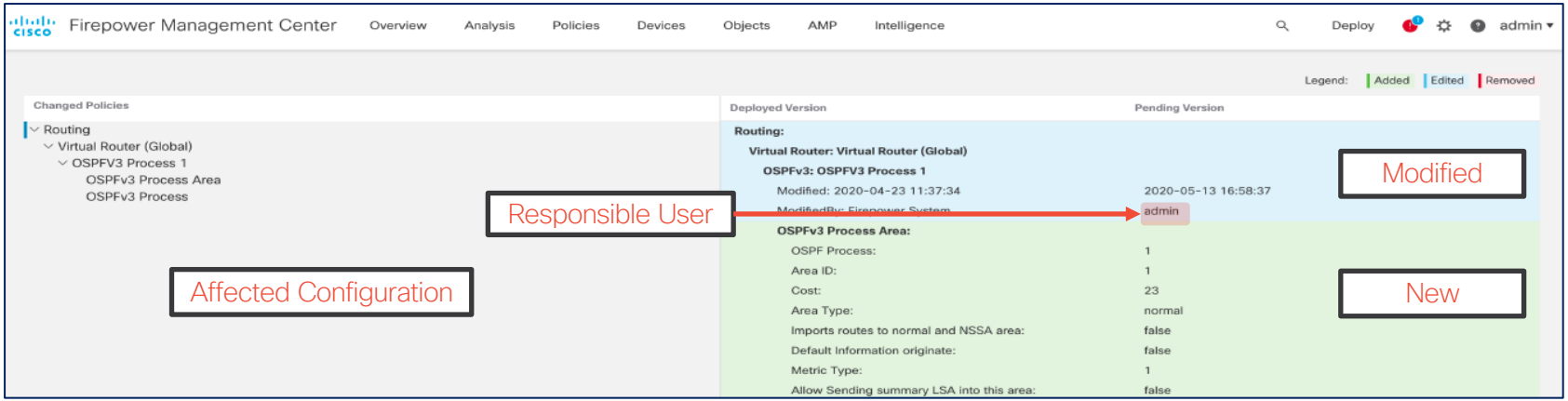
FMC 7.0



Change Management

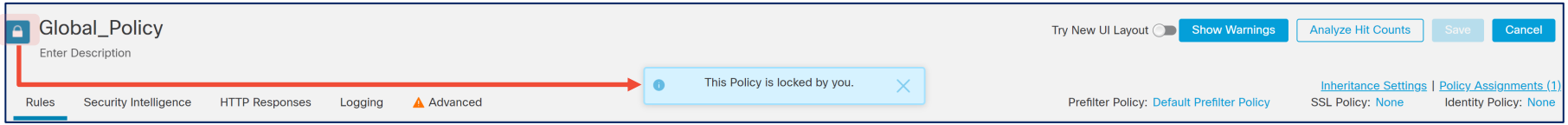
FMC 7.0

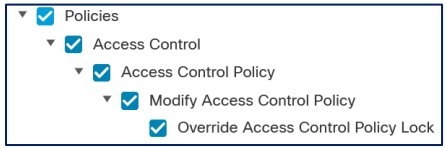
- Selective change deployment and detailed audit transcripts in FMC
  - Individual configuration changes can be filtered and deployed by user
  - Emergency rollback to one of 10 previous configuration versions
  - Ticket-based change commit mode is in the future

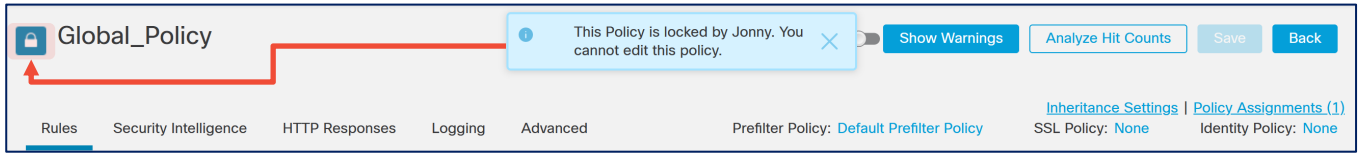


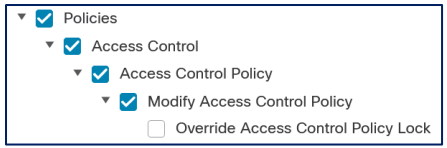
“Shallow” Access Policy Locking

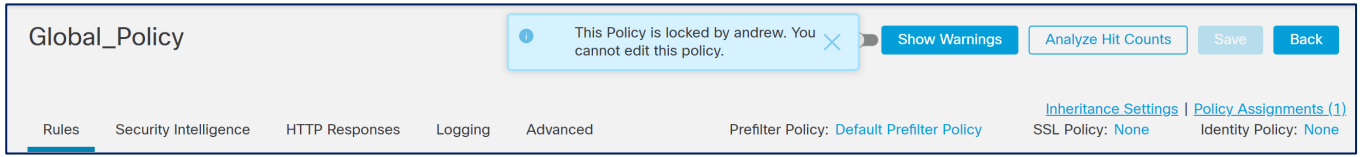
FMC 7.2





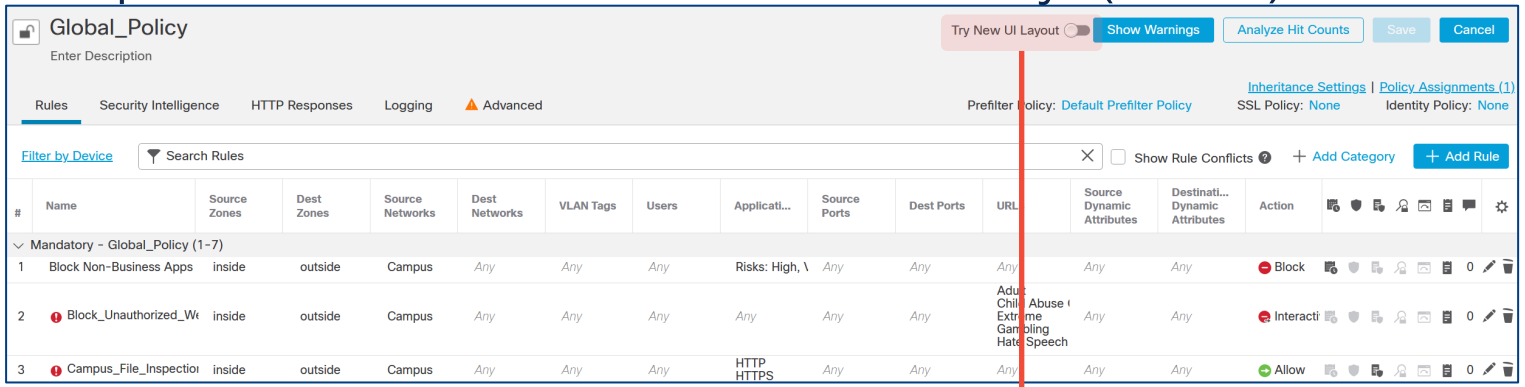


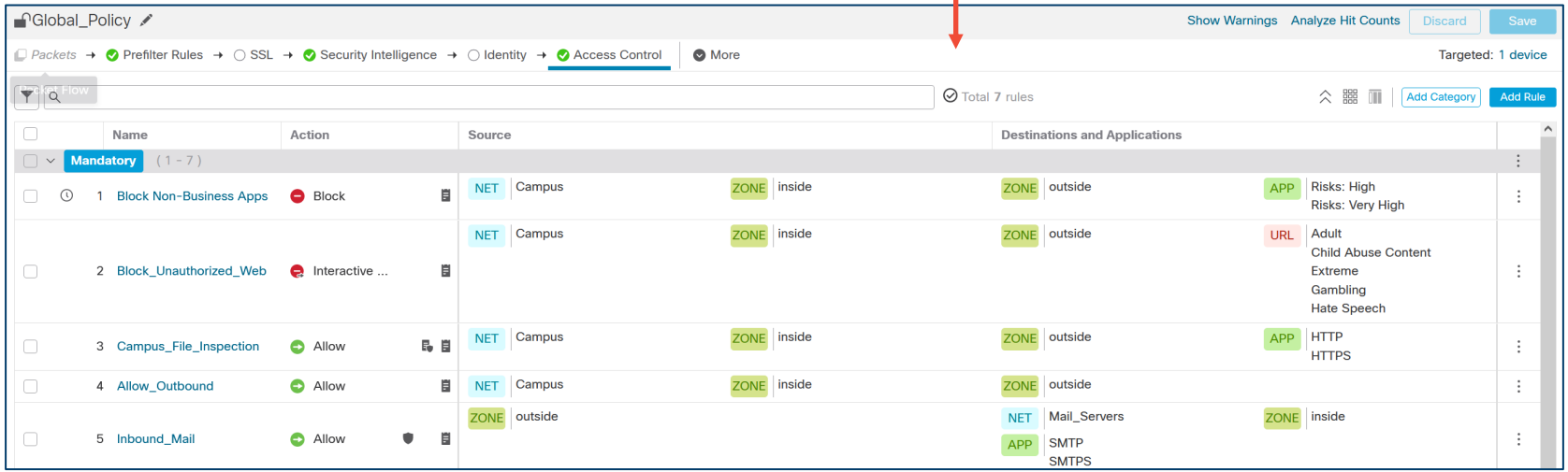




Simplified Access Control Policy (ACP) View

FMC 7.2



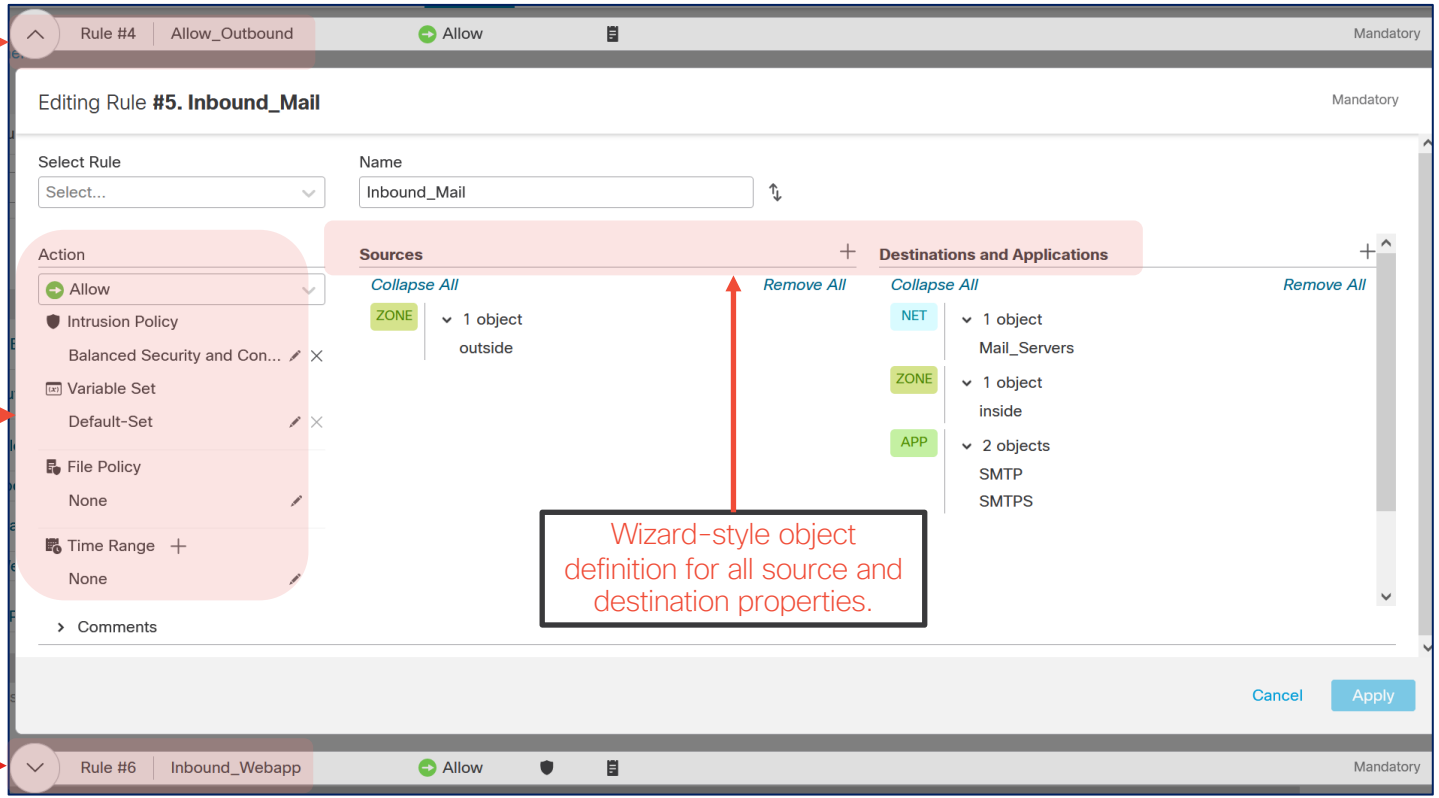


Simplified ACP Rule Editor

FMC 7.2

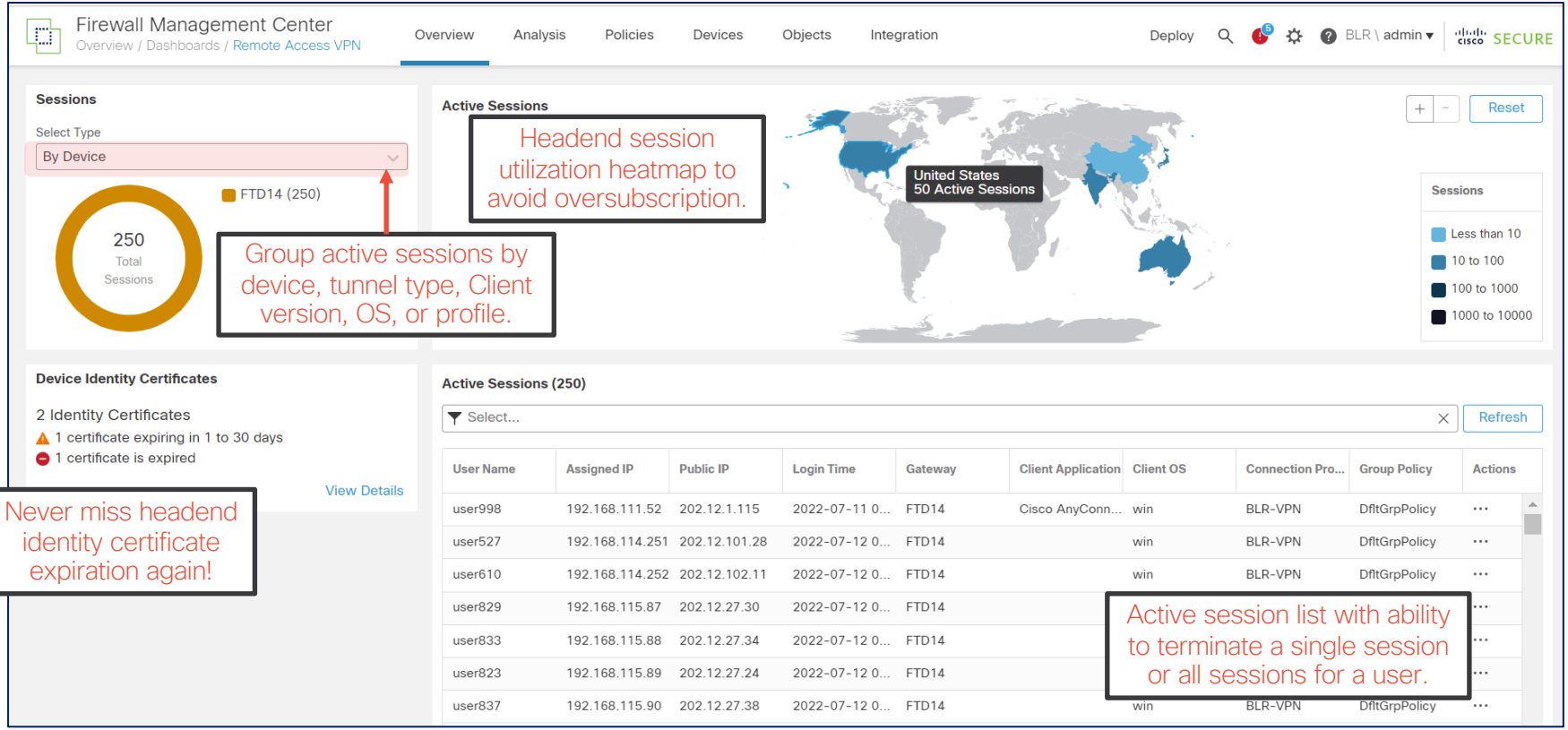
Inline rule navigation.

Direct access to all advanced actions.



VPN Monitoring Dashboard

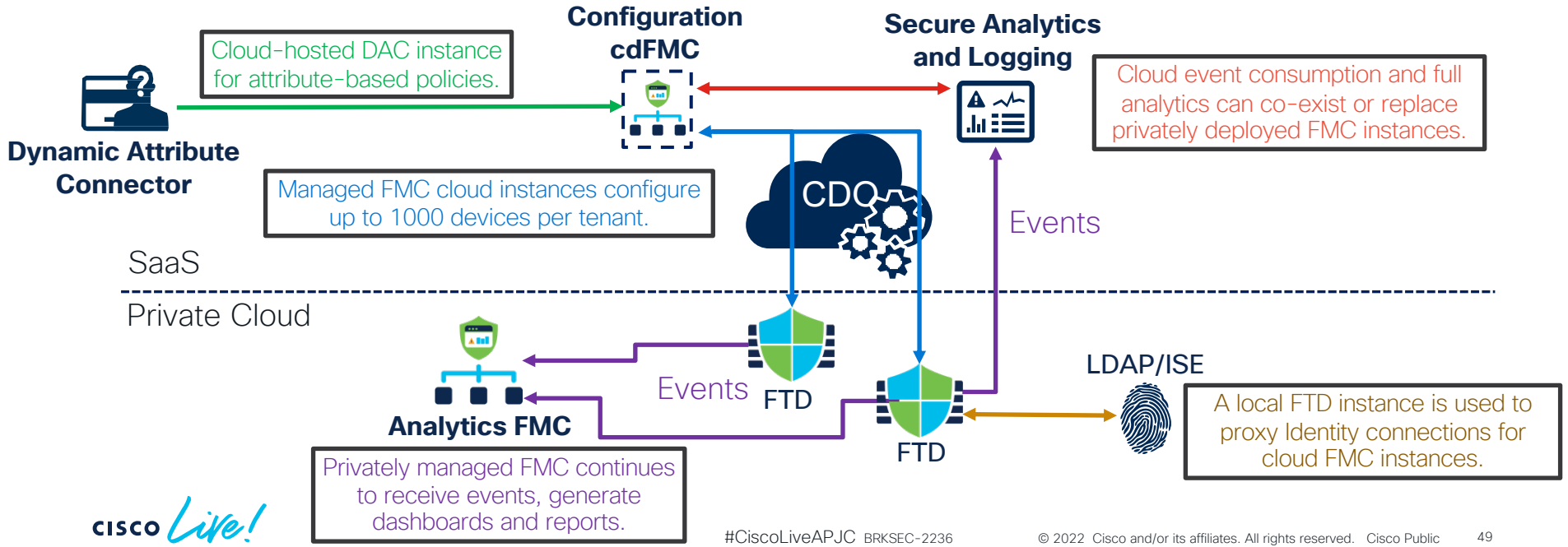
FMC 7.3



Cloud-Delivered Firewall Management Center

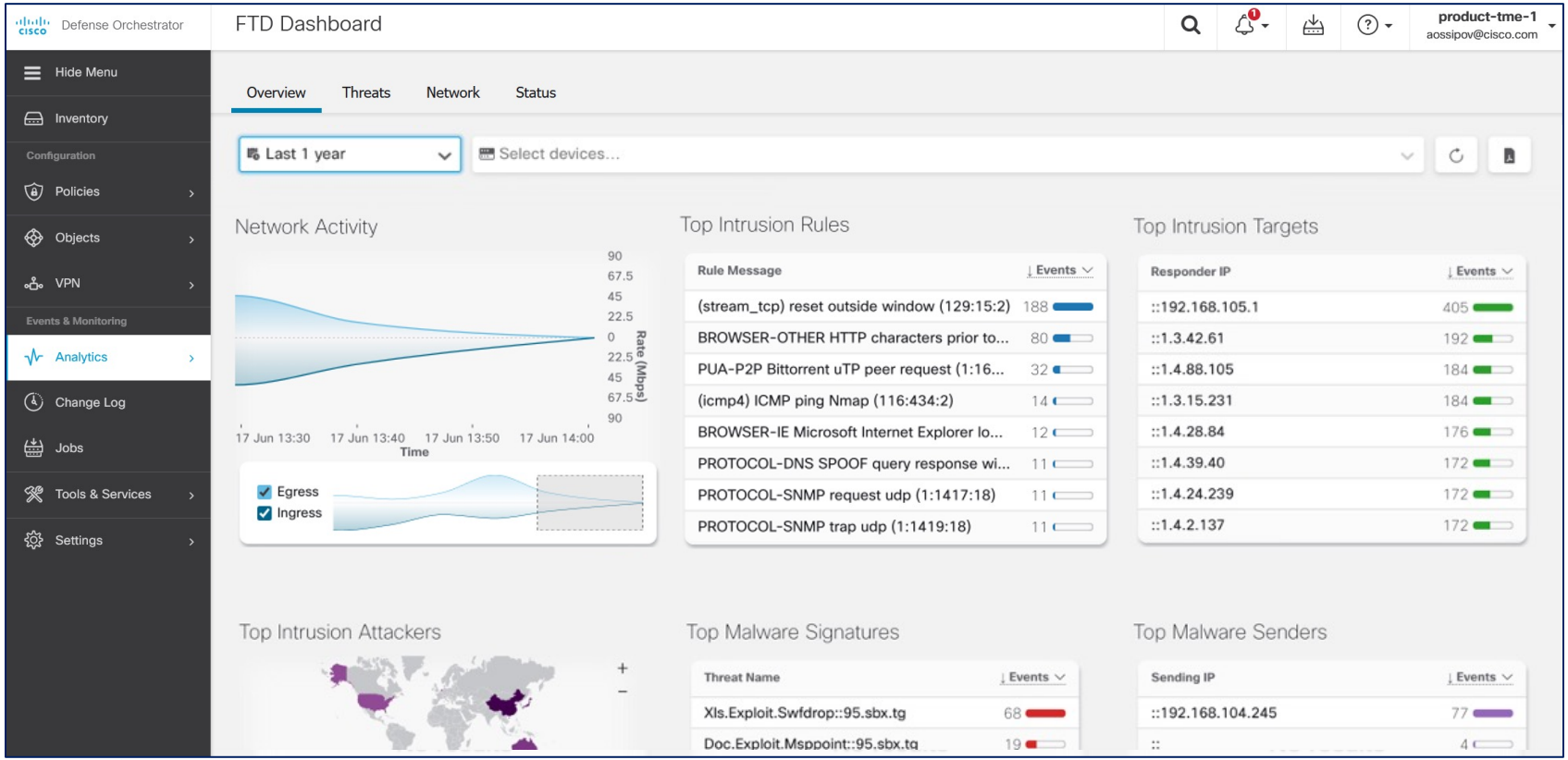
FMC 7.2

- Fully-featured FMC experience within Cisco Defense Orchestrator
  - Managed backend from platform upgrades to configuration backup



Cloud Analytics Dashboard

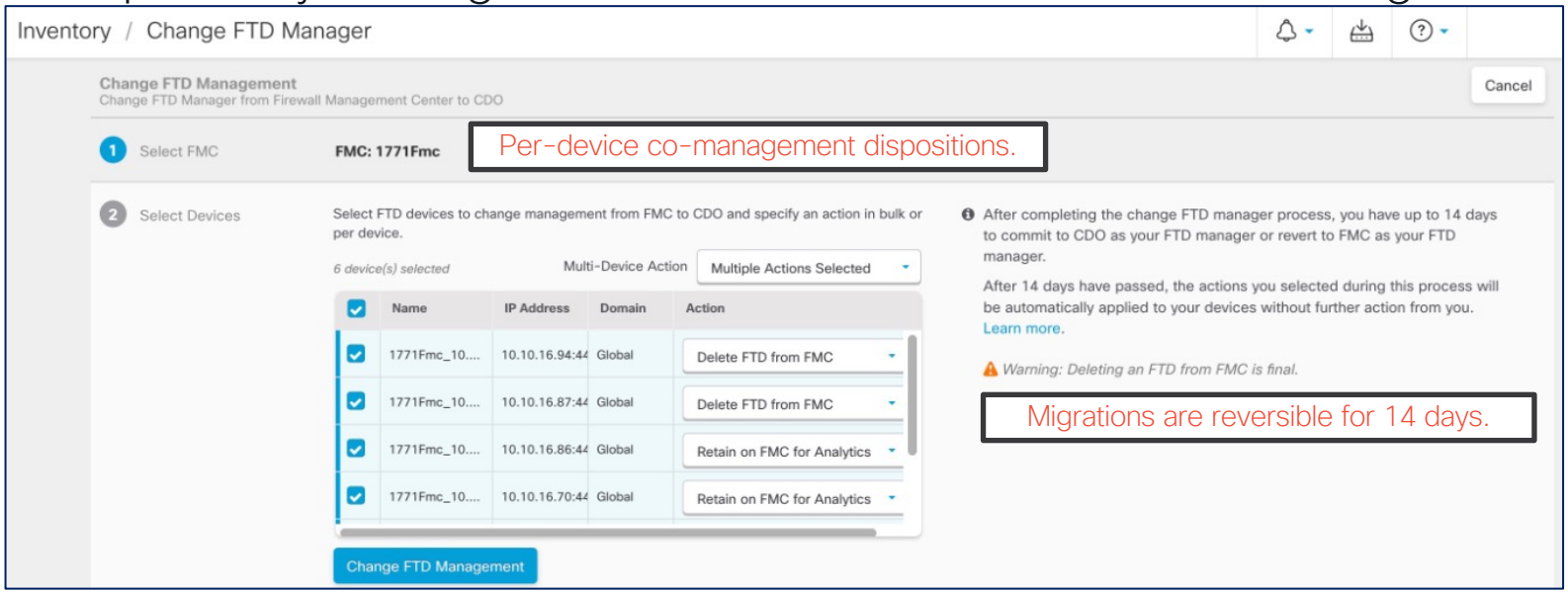
cdFMC 7.2



Simple Migration of FTD to Cloud Management

FMC 7.2

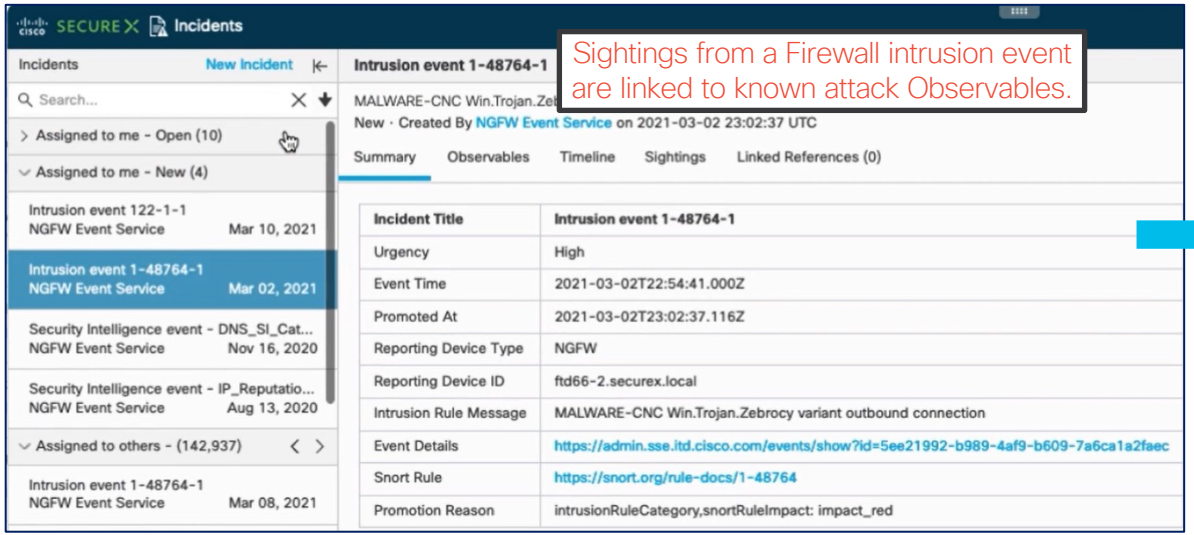
- New devices can be easily on-boarded by serial number
- Add privately managed FMC instances to CDO for fleet migrations



SecureX with Secure Firewall

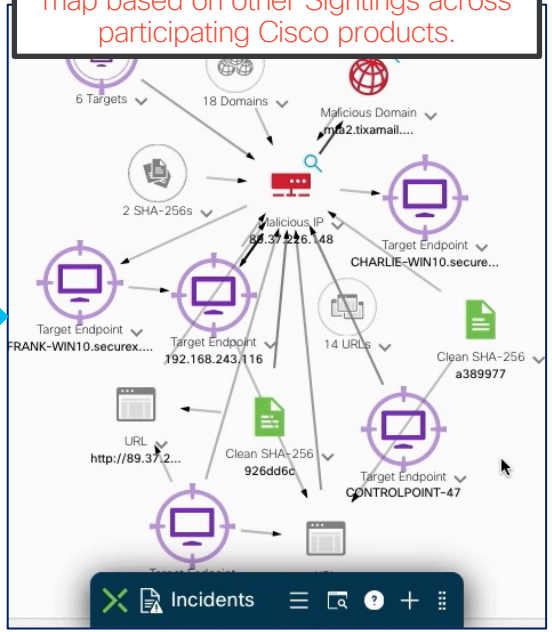
FMC 6.5+

- Coordinated incident response with an FMC SecureX Ribbon
  - Send promoted high-priority File and Intrusion events
  - Automated response and remediation via FMC API



Sightings from a Firewall intrusion event are linked to known attack Observables.

SecureX constructs the entire exposure map based on other Sightings across participating Cisco products.



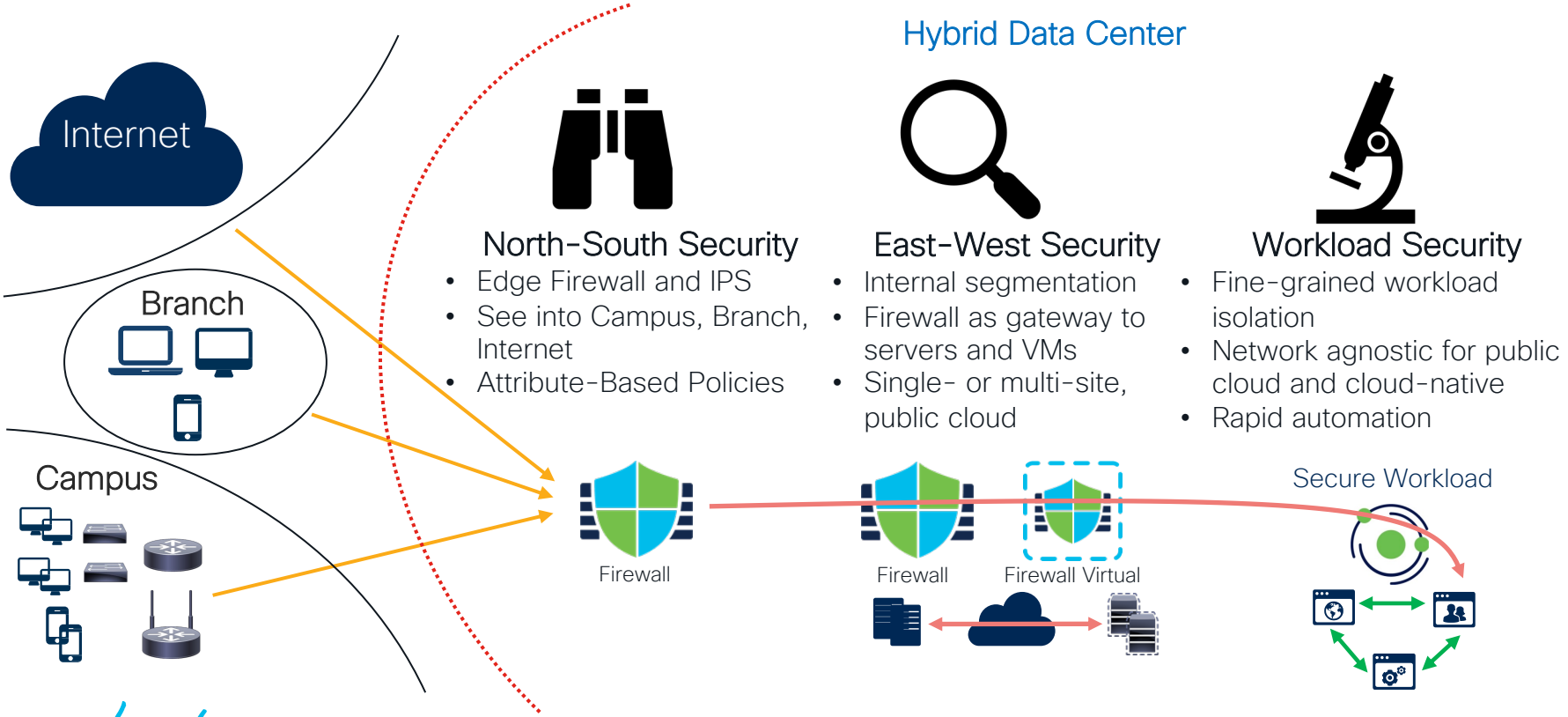
Secure Workload

Secure Workload Functional Overview

- Born for app visibility (Tetration), graduated to microsegmentation
  - Employs host OS agents for visibility and built-in firewalls for enforcement
- Ingests network telemetry from agents, Netflow/IPFIX, VPC flow logs
  - App flow discovery with Application Dependency Mapping (ADM)
  - Policy recommendation based on observed communication patterns
  - Policy impact prediction on existing flows to reduce business impact
- Numerous integrations to enrich endpoint context
  - Workload attributes 

  - User context: Secure Client (formerly AnyConnect), ISE/pxGrid
  - Cisco Secure Firewall, F5, Citrix for enforcement

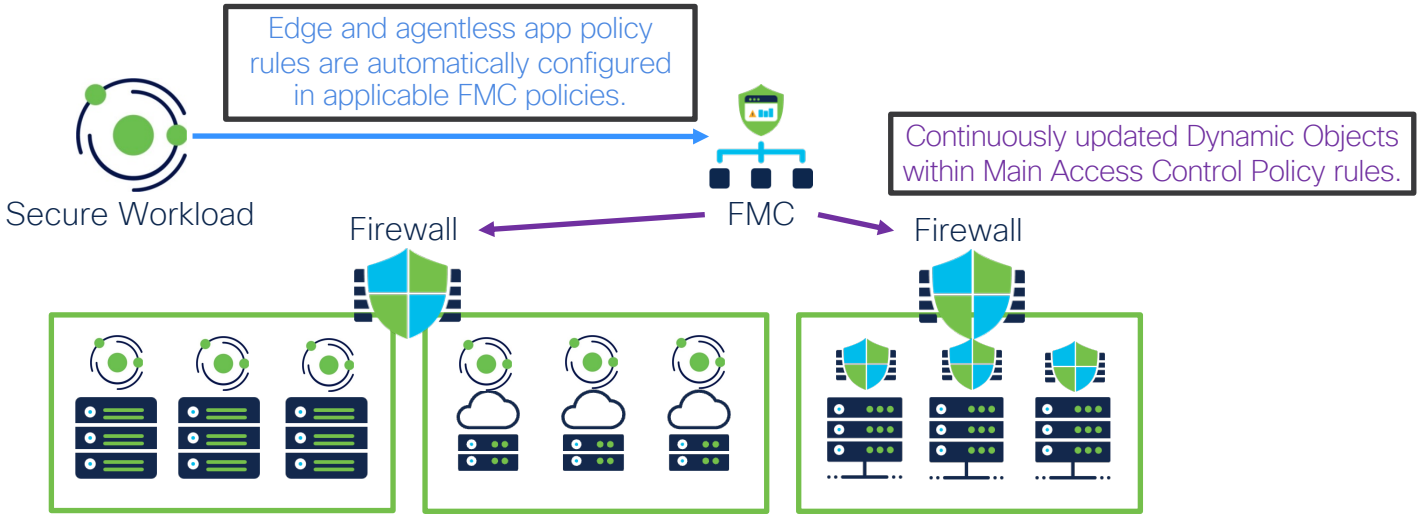
End-to-End Application Protection



Secure Workload Policy Extension to Firewall

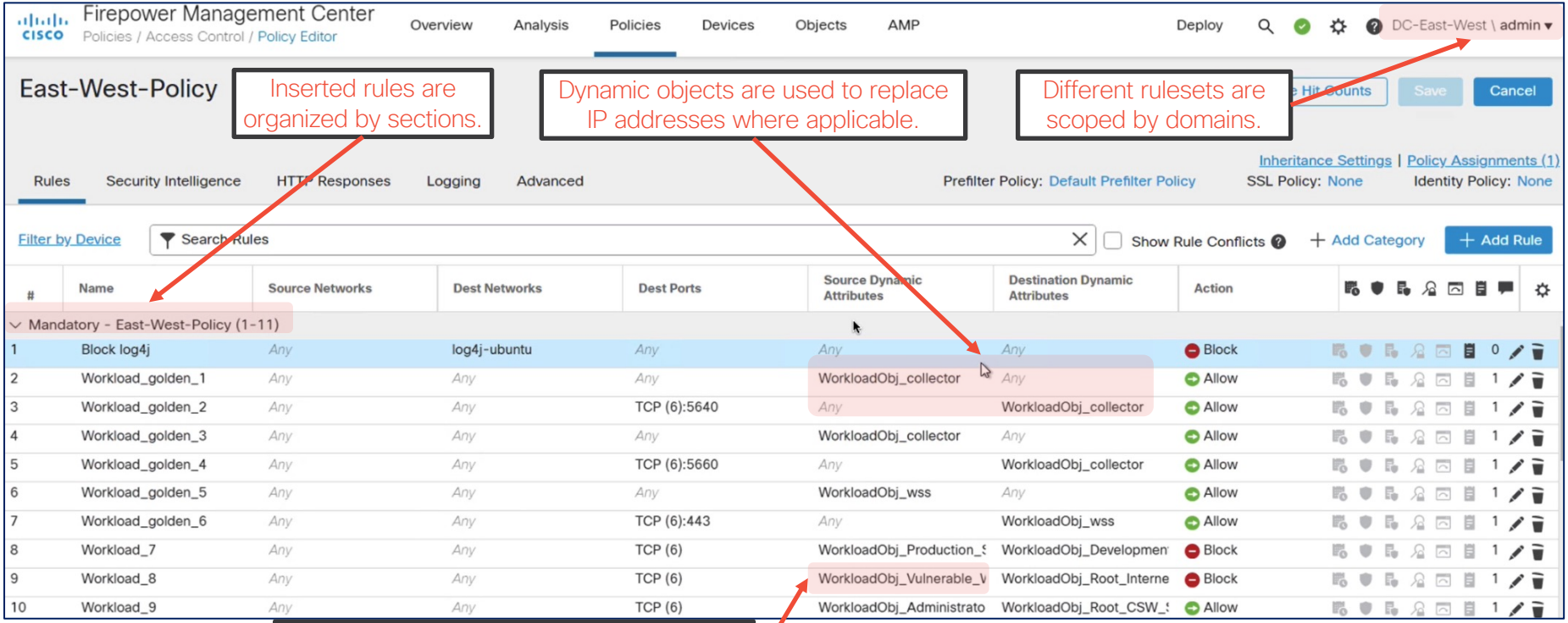
Workload 3.6

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



Secure Workload Policy Orchestration in FMC

Workload 3.6



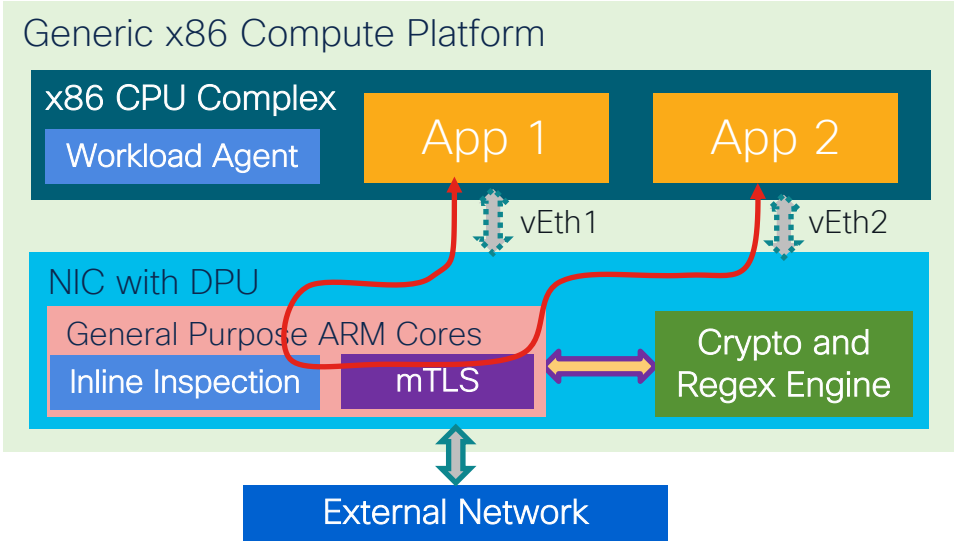
Workload Segmentation with DPU

Future

- NIC with DPU enables advanced micro segmentation in hybrid cloud
  - Expanded inter-application isolation and inline inspection with Workload
  - Real-time anomaly detection with add-on hardware inference engines

Workload Agent continues to provide application visibility at host OS, container, and cloud API levels. All external application communication and mutual TLS (mTLS) encryption is handled through Virtual Ethernet instances.

Resident DPU inspection component exposes isolated Virtual Ethernet interface to individual applications, provides targeted inline virtual patching, and leverages on-board mTLS offload to inspect above encryption layer.



Cisco Security Beta Programs

Sign-Up Now:
http://cs.co/clive-security-beta

"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

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

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

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

The bridge to possible

Thank you

#CiscoLiveAPJC