

CISCO *Live!*

ALL IN

#CiscoLiveAPJC

# Keeping Up on Network Security with Cisco Secure Firewall

Subtitle goes here

Andrew Ossipov  
Distinguished Engineer, Portfolio CTO  
BRKSEC-2236

# Cisco Webex App

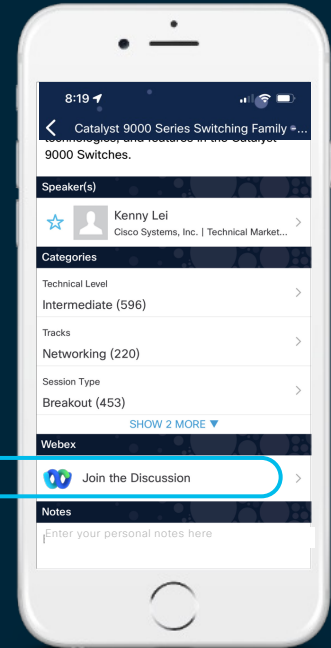
## Questions?

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](mailto:aeo@cisco.com)

Distinguished Engineer

Portfolio CTO for Cloud and Network Security

Firewall Architecture, Threat Visibility, Hybrid Cloud, SSE

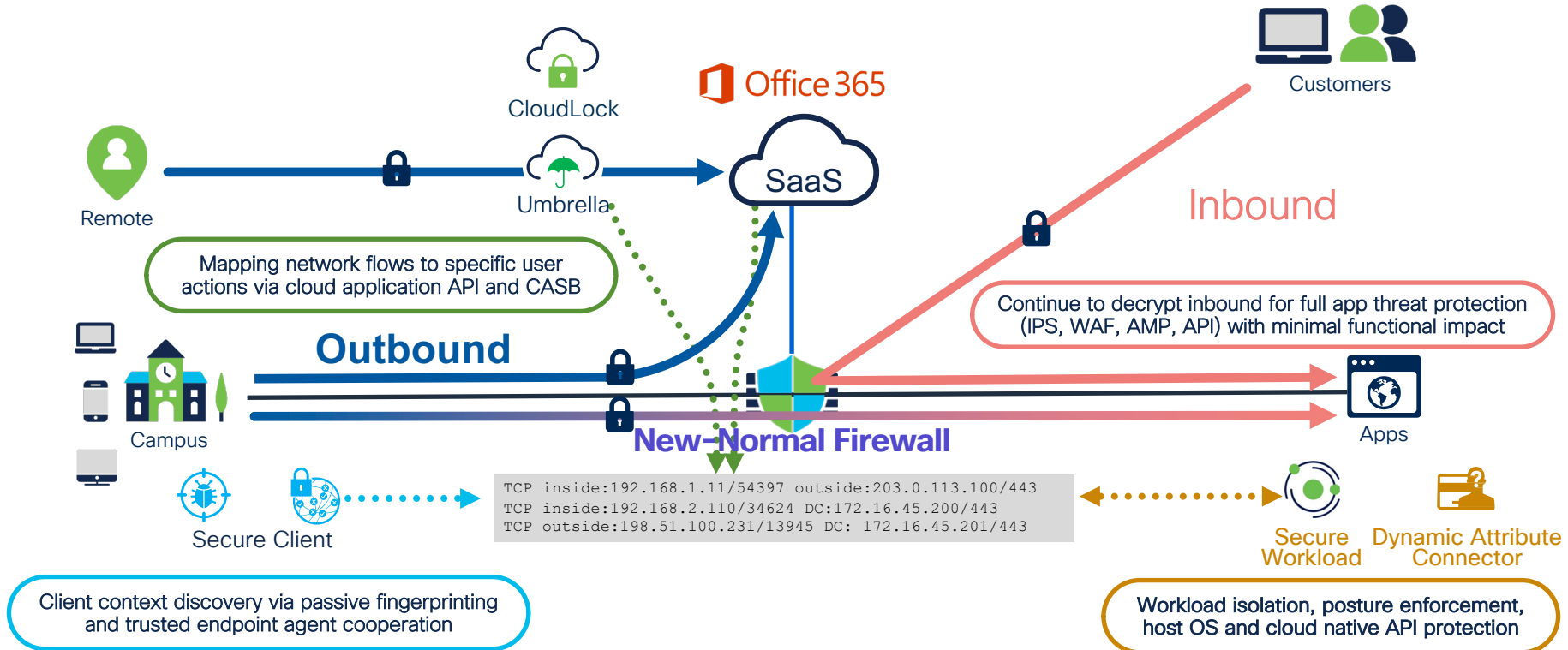




# Agenda

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

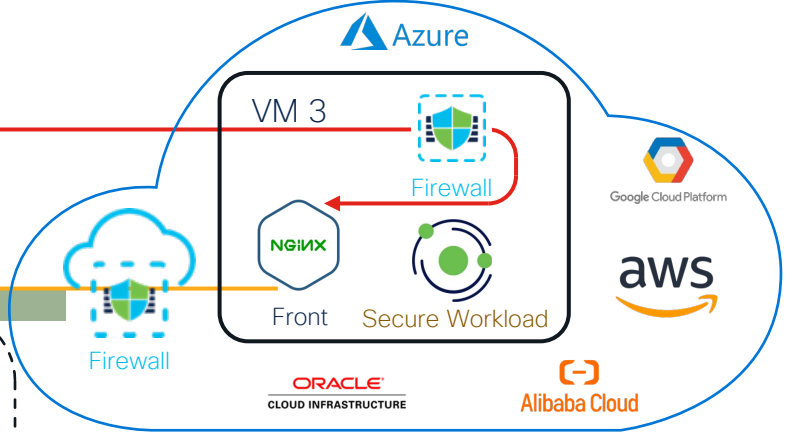
# Secure Firewall: Inspect, Infer, and Cooperate



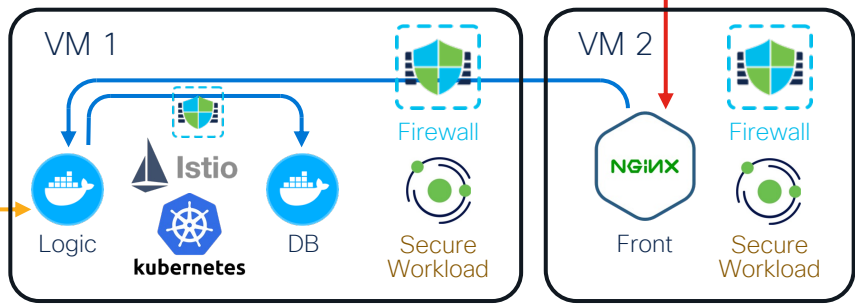
# Firewall Vision: Network, Workload, and Cloud

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

Private or cloud-delivered **Firewall** inspects application edge, implements Zero Trust Network Access (ZTNA), continuously applies full stack of inline security services.



## Private Cloud



**Secure Workload** protects host OS at process and file levels, selectively inspects network and service mesh traffic with inline **Firewall** and API controls, integrates with public cloud and cloud-native orchestrators for posture and policy, consumes policy as code from DevOps tools.

# Platforms



# Secure Firewall 3100 Overview

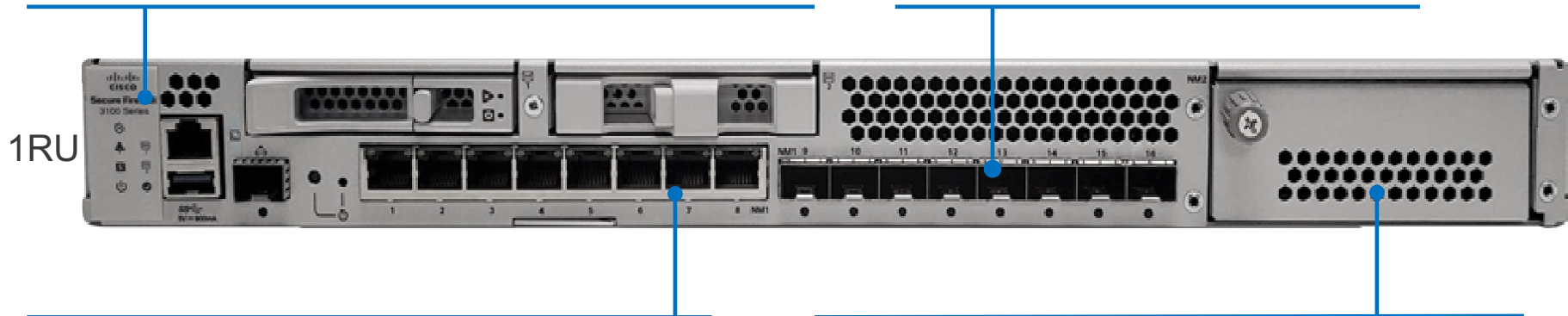


## Appliance-Mode Security Platform for FTD or ASA Application

- 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



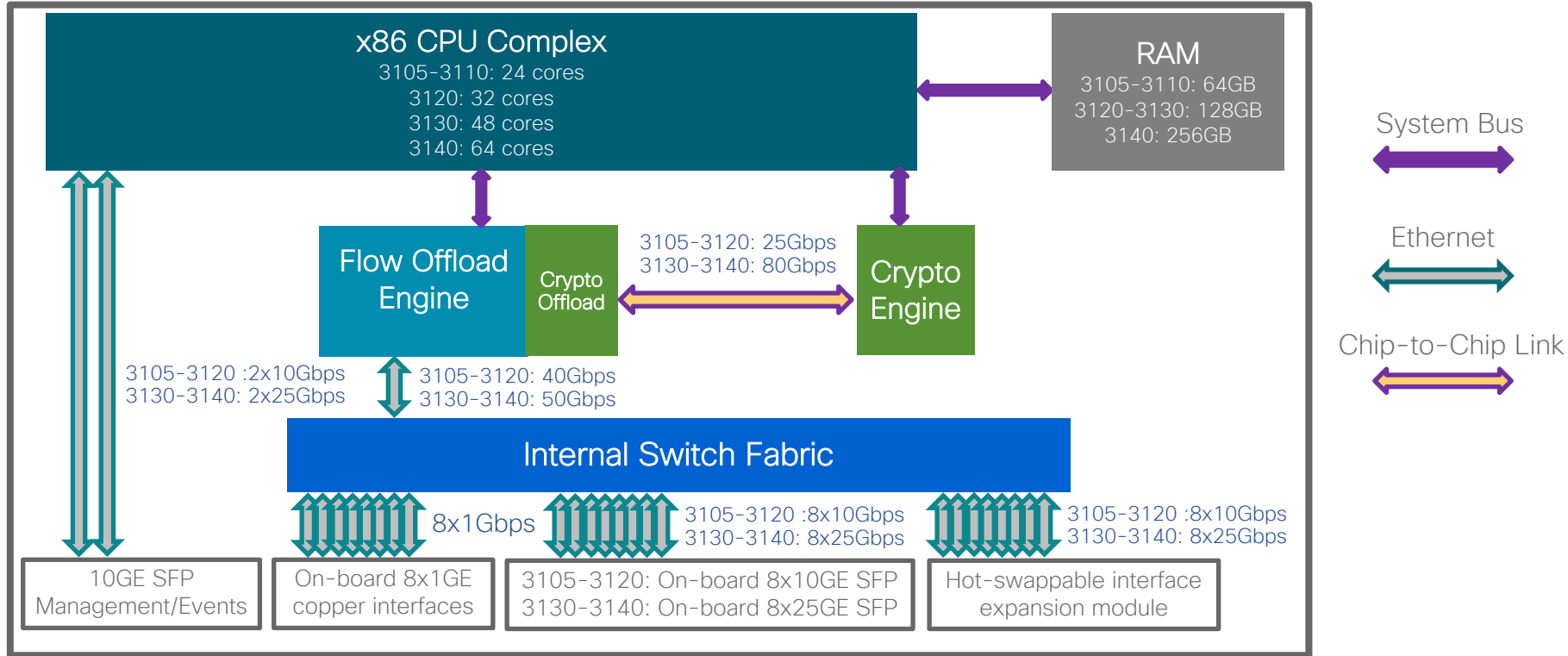
## Copper Data Interfaces

- 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






# Secure Firewall 3100 Performance



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

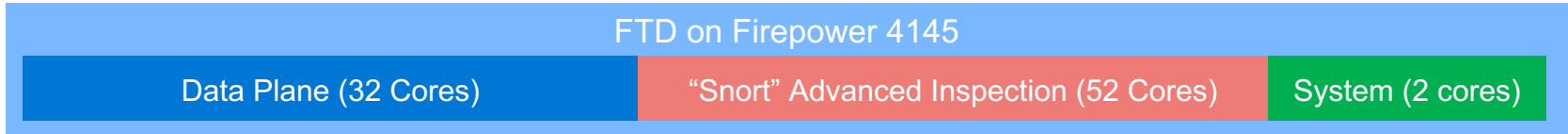
Up to <b>7x</b>  Boost in FW+AVC+IPS	Up to <b>17x</b>  Boost in IPsec VPN	Up to <b>14x</b>  Boost in TLS
---	---	---

\*Performance Estimates are subject to change in public release.



# Configurable CPU Core Allocation

- 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

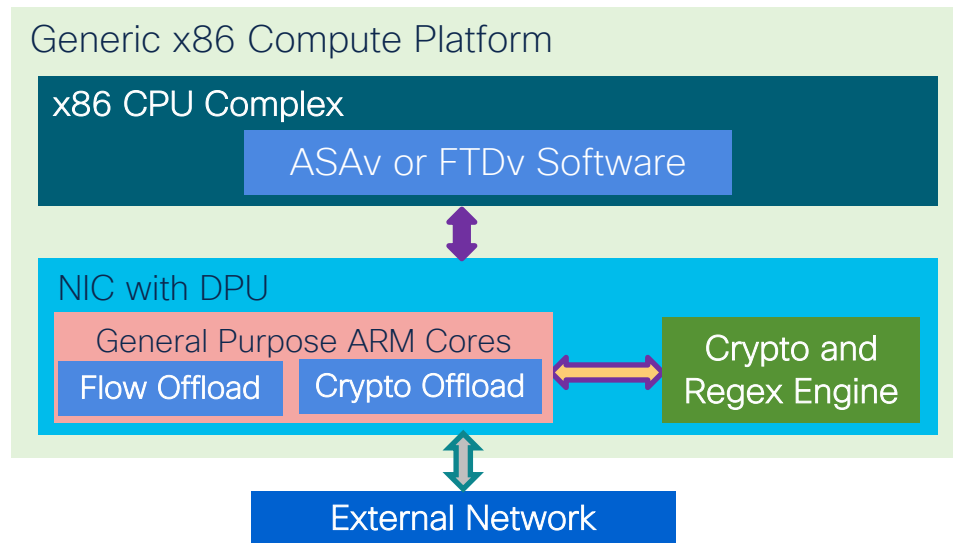
# Virtual Firewall with Data Processing Unit (DPU)

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.

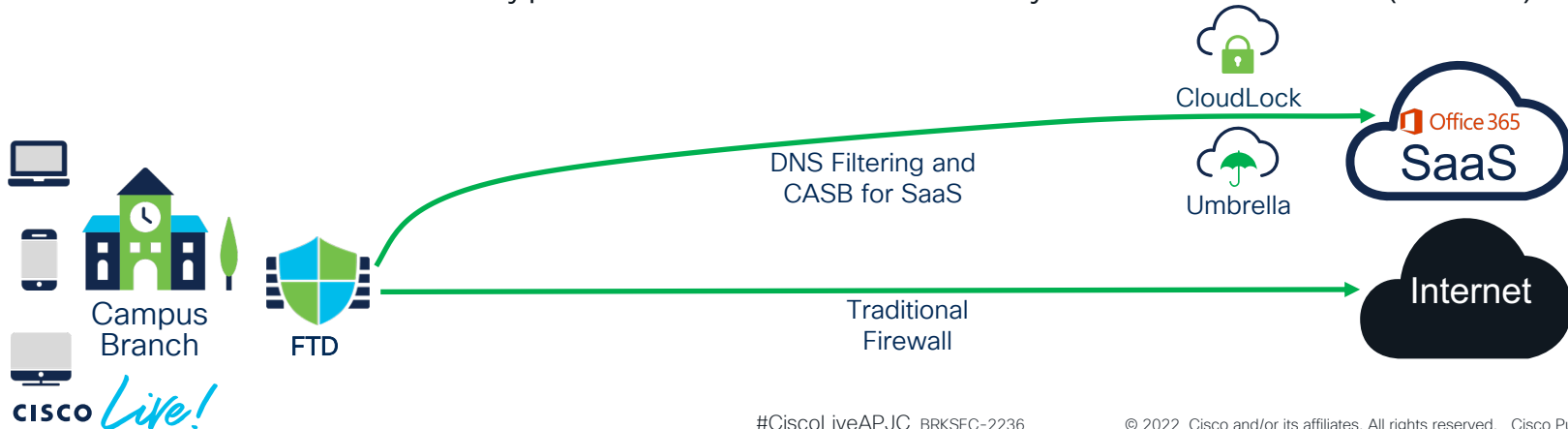


# Threat Protection



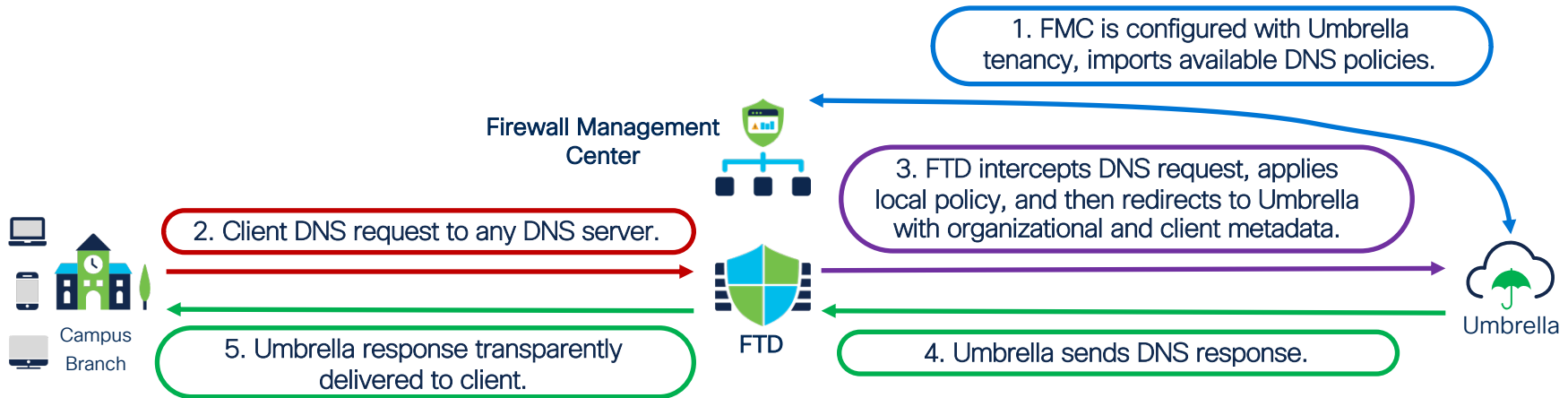
# Enhance Firewall with Umbrella Cloud Security

- 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

- 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

- 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

The screenshot shows the Fire Management Center interface for creating a SASE Topology. The 'Endpoints' tab is active, showing the configuration for the 'Umbrella Data Center' with the following details:

- Continent: Asia
- Data Center: Mumbai
- IP Address: 146.112.117.8

Below this, a table lists 'Threat Defense Nodes' with columns for Device, VPN Interface, and Local Tunnel ID:

Device	VPN Interface	Local Tunnel ID
chennai-bo-ftd-xyz.com	outside_static_vti_1	xyz11111111@*****.com
hyd-bo-ftd-xyz.com	out_static_vti_1	xyz111111112@*****.com
blr-bo-ftd-xyz.com	outside-airtel-blr_static_vti_1	xyz1212312@*****.com

A blue arrow points from the 'Local Tunnel ID' column to the 'Cisco Umbrella Configuration' panel on the right. This panel shows the configuration for the 'vpn-MumbaiUmbrella' topology:

- Topology Name: vpn-MumbaiUmbrella
- Primary Data Center: Asia-Mumbai
- DC IP Address: 146.112.117.8
- Start Time: Jul 13, 2022 11:29 AM
- Completion Time: Jul 13, 2022 11:29 AM

A progress bar indicates 100% completion with 3 successful configurations and 0 failures. Below this, the 'Tunnel Configuration Status' table shows the following results:

Device	Status	Transcript
✓ hyd-bo-ftd.xyz.com	SUCCESS	
✓ blr-bo-ftd.xyz.com	SUCCESS	
✓ chennai-bo-ftd.xyz.c...	SUCCESS	

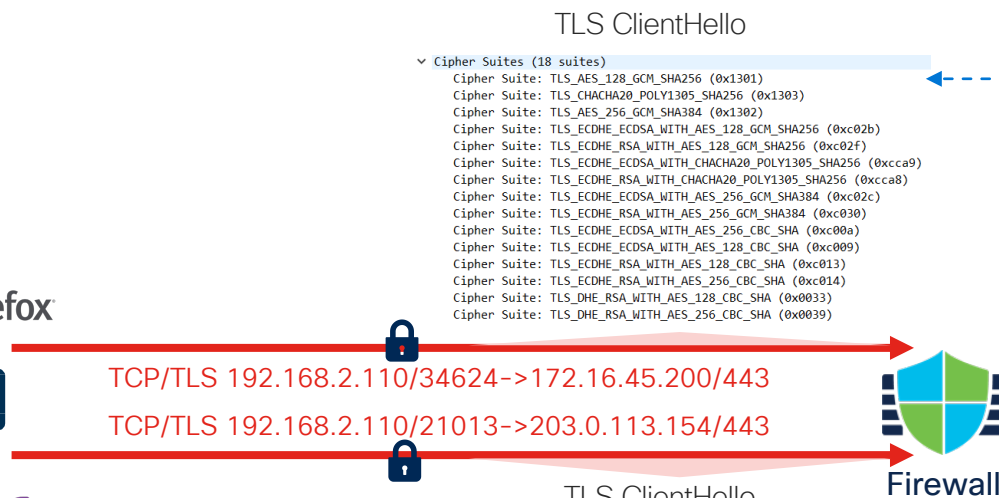


# Snort 3 IPS Engine



- 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)



TLS ClientHello

```

    Ciphers Suites (18 suites)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  
```

Confidence: 99.94%  
 Process: [firefox.exe](#)  
 Version: 76.0.1  
 Category: browser  
 OS: [Windows 10 19041.329](#)  
 Destination FQDN: [cisco.com](#)

Generate unique fingerprints for client applications based on outer packet fields; use for policy matching and context enrichment with TLS and QUIC.

TLS ClientHello

```

    Ciphers Suites (19 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
  
```

Confidence: 100%  
 Process: [tor.exe](#)  
 Version: 9.0.2  
 Category: anonymizer  
 OS: [Windows 10 19041.329](#)  
 Destination FQDN: [nksdilkoup.me](#)

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



# EVE-enriched Unified Events



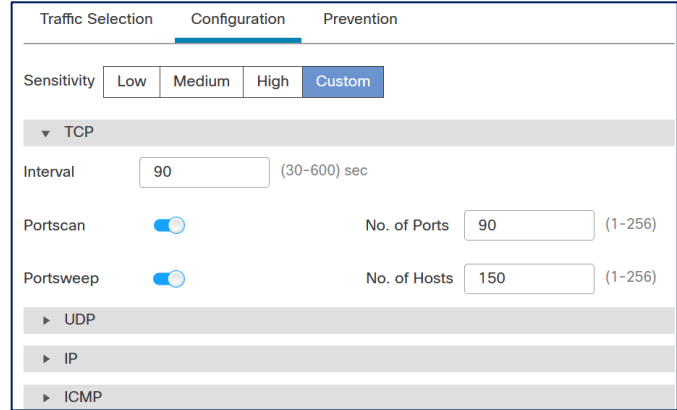
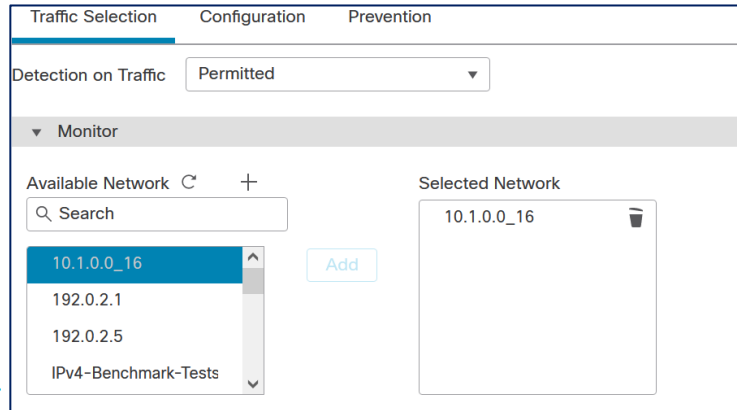
Client process name and detection confidence score; the name can be linked to a custom AppID for enforcement in FTD 7.2.

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 Unr)	3 (Port unreachable)	Passive	ICMP client	0%			0%

Inference-based threat alert and confidence level.

# 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





# 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 is supported
- 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. [Download](#)

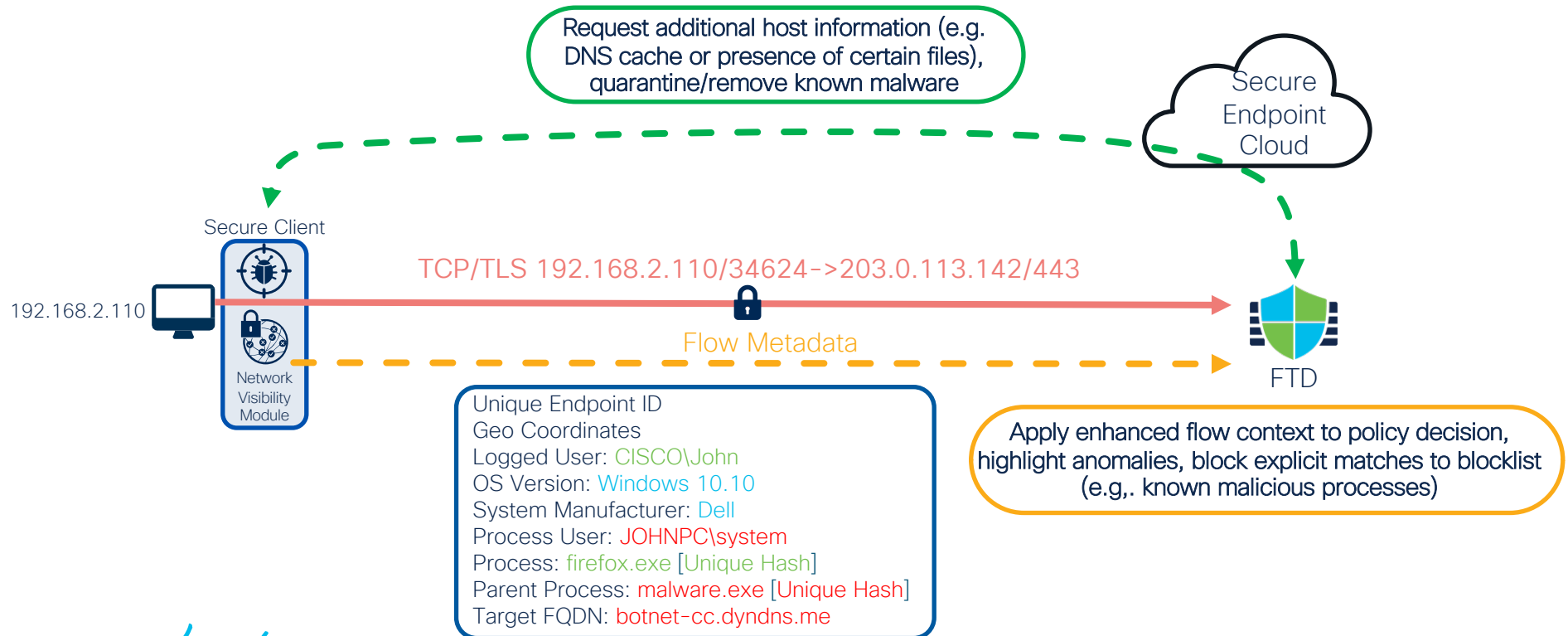
FMC\_Self    Associated: 2 Networks, 1 Port

[See how to configure](#)

Cancel    Save



# Real-time Flow Context via Endpoint Intelligence

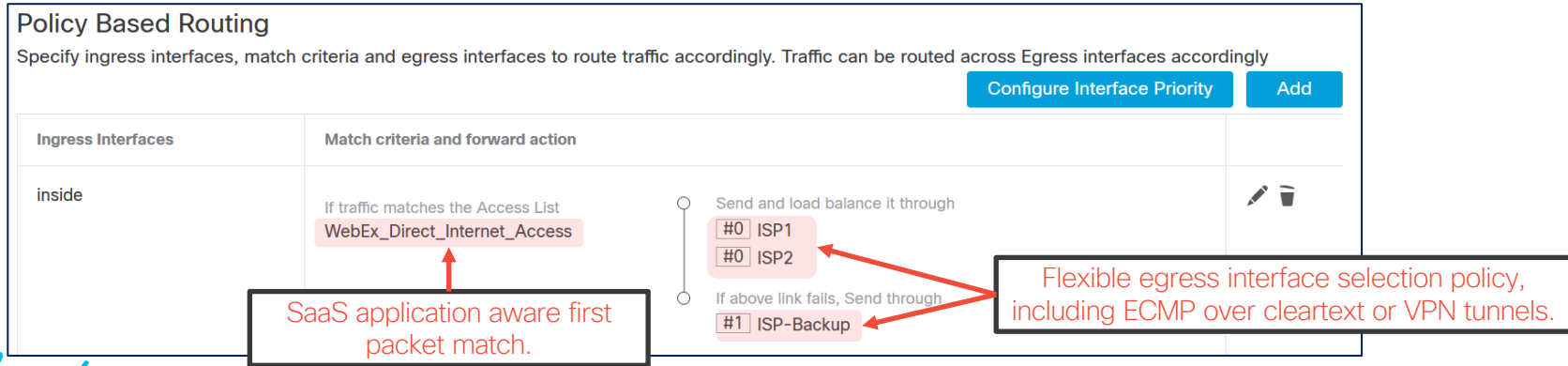


# Connectivity



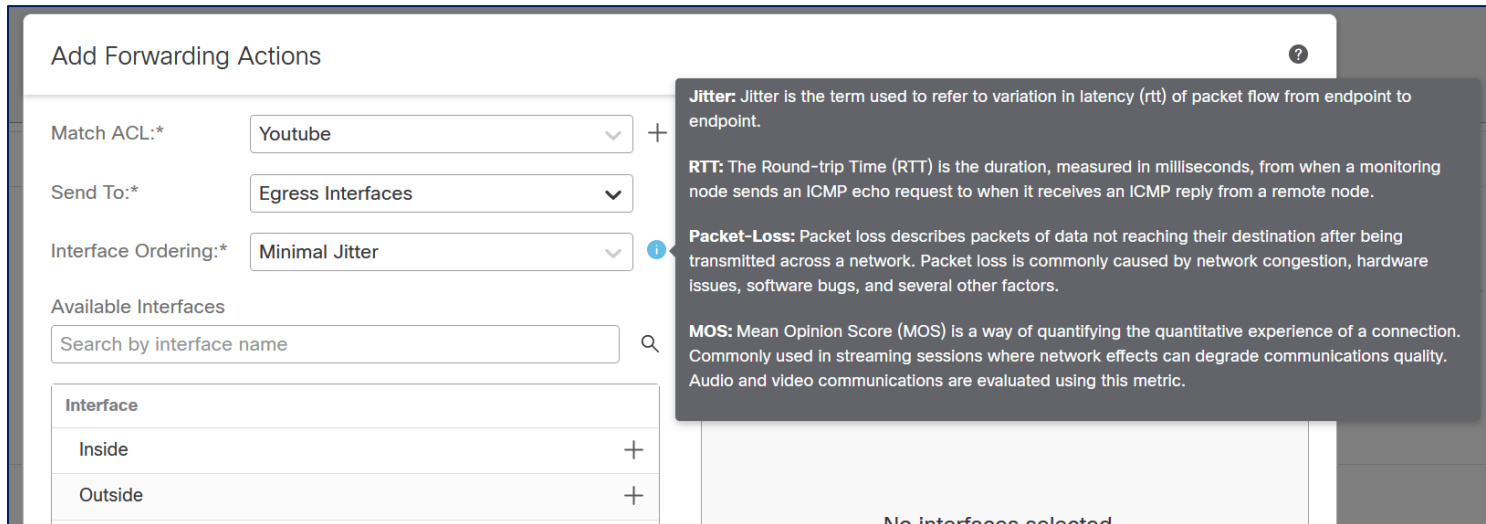
# Application-Aware Policy Routing

- 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



# Path Monitoring and Quality-Based Routing

- 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



**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 (rt) 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.

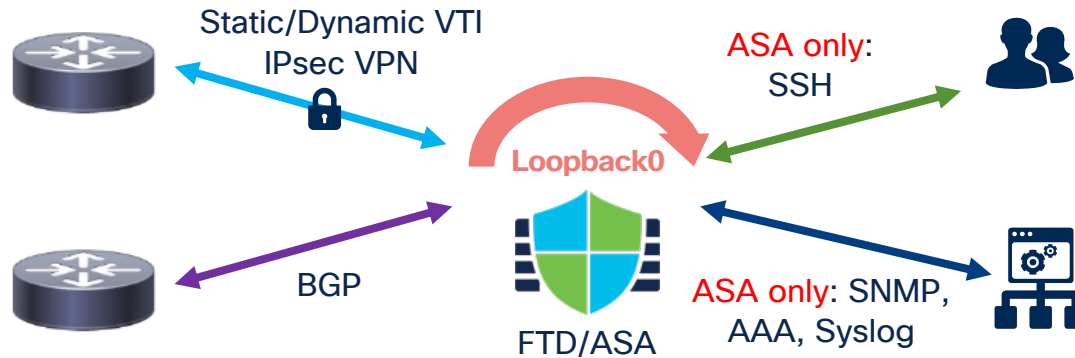
**Packet-Loss:** Packet loss describes packets of data not reaching their destination after being transmitted across a network. Packet loss is commonly caused by network congestion, hardware issues, software bugs, and several other factors.

**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.

# Loopback Interface



- 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

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

**Elephant Flow Settings** ?

**1** 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

Throughput threshold to qualify as an Elephant Flow

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

Optional flow remediation actions.



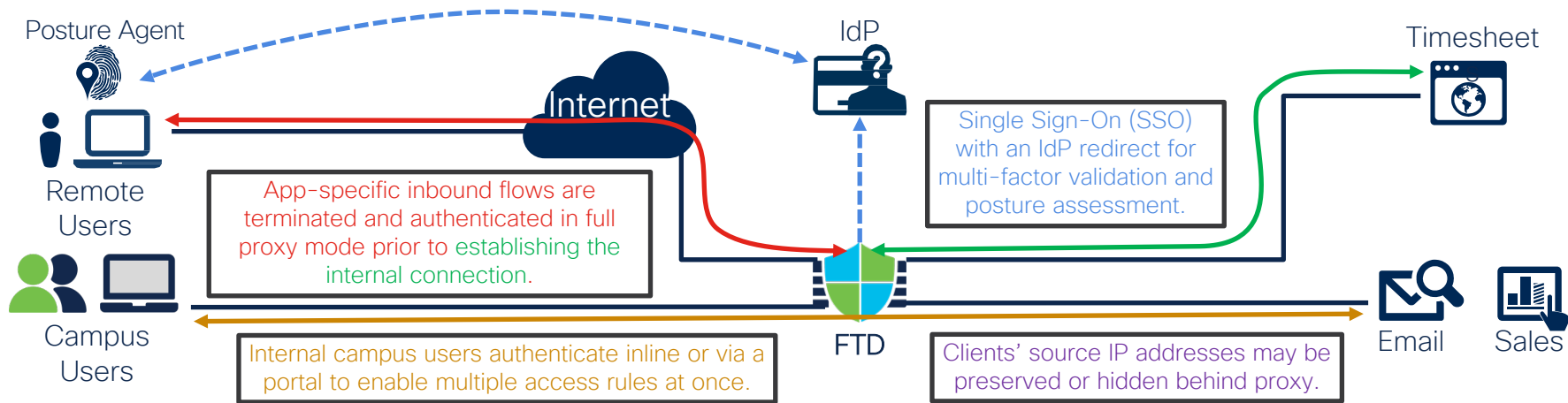
# Client Zero Trust Network Access (ZTNA)

- 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

- 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



## Private Cloud

Logos for HyperFlex, VMware ESXi, KVM, NUTANIX, and openstack.

## Public Cloud

Logos for Microsoft Azure, Google Cloud Platform, AWS, Rackspace Technology, Equinix, Oracle Cloud Infrastructure, Alibaba Cloud, and Alkira.

## 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

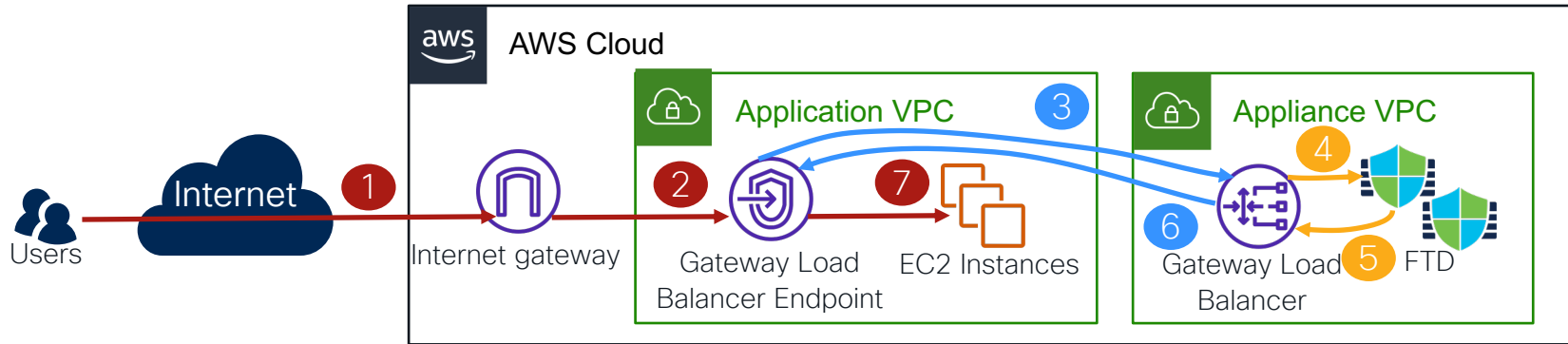


- Secure Firewall instantiation with public cloud templates   
- Declarative Terraform templates for ASA and FTD (via FMC) 
  - FTD Dynamic Object integration with HashiCorp Consul 
- Imperative Ansible tasks for ASA and FTD (FDM and now FMC) 
- Continuously updated Cisco DevNet repositories
  - <https://developer.cisco.com/secure-firewall/cloud-resources/>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

# Gateway Load-Balancer in AWS and Azure



- Network firewall service insertion for inbound and outbound flows
  - Redirection with GENEVE
  - Bring-your-own TLS decryption with available software capabilities

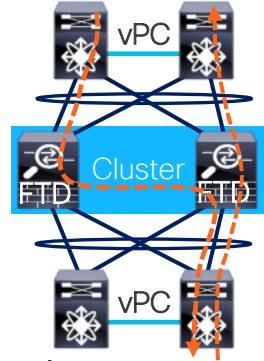


- Autoscale and snapshot-based instantiation in **FTD 7.2** and **ASA 9.18**

# Clustering for Virtual Firewalls



- 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

# Attribute-Based Policies



Custom Orchestrator

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



Dynamic Attribute Connector

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

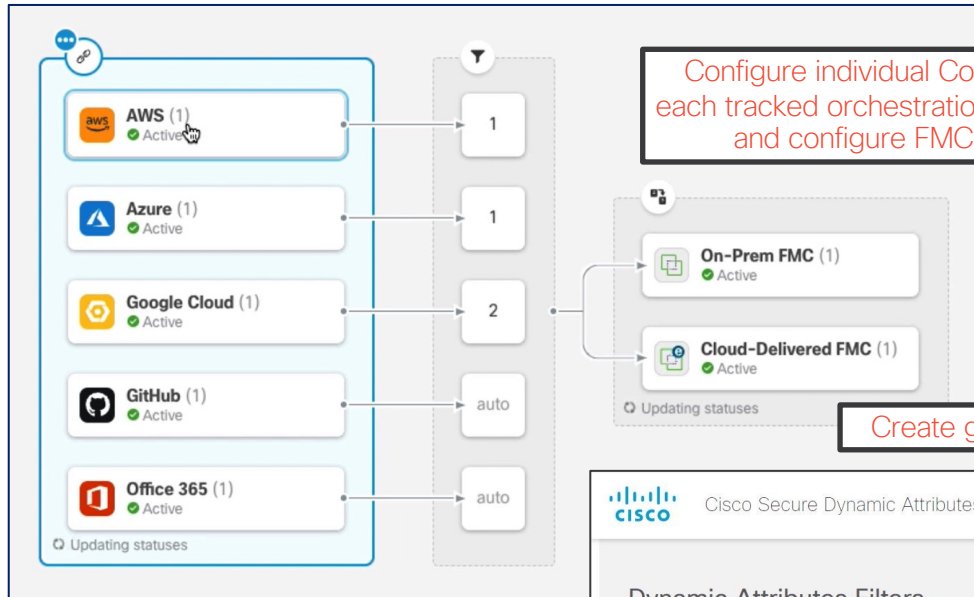
Name	Action	Source		Destination		Applications
		Networks	Dynamic Attributes	Networks	Dynamic Attributes	
Allow Windows Updates	➔ Allow	Any	Windows_OS	Any	Any	Windows Update
Allow WebApp to DB	➔ Allow	Any	WebApp_Logic	Any	DB_Cluster	Any

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.



# Dynamic Attributes Connector User Interface



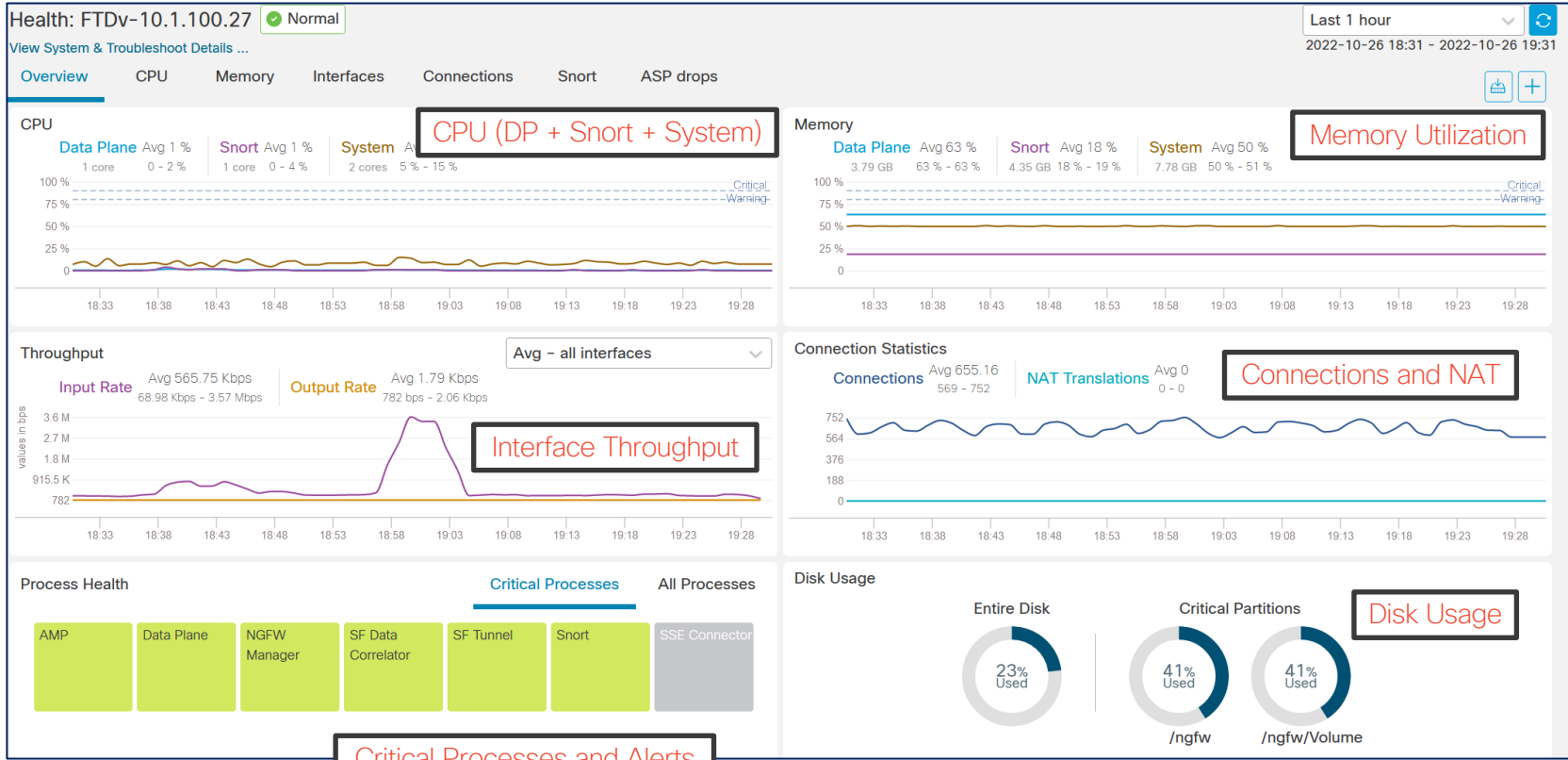
Create granular attribute filters to reduce noise.

#	Name	Connector	Query	Actions
1	Azure App	Azure	(Finance = 'App') AND (HR = 'App')	⋮
2	vCenter.os	vCenter	(os = 'Ubuntu Linux (64-bit)' OR os = 'CentOS 4/5 or later (64-bit)' OR os = 'FreeBSD Pre-11 versions (64-bit)') AND (network = 'u90c04p11-1511')	⋮
3	AWS App	AWS	(Sports = 'App') OR (News = 'App')	⋮

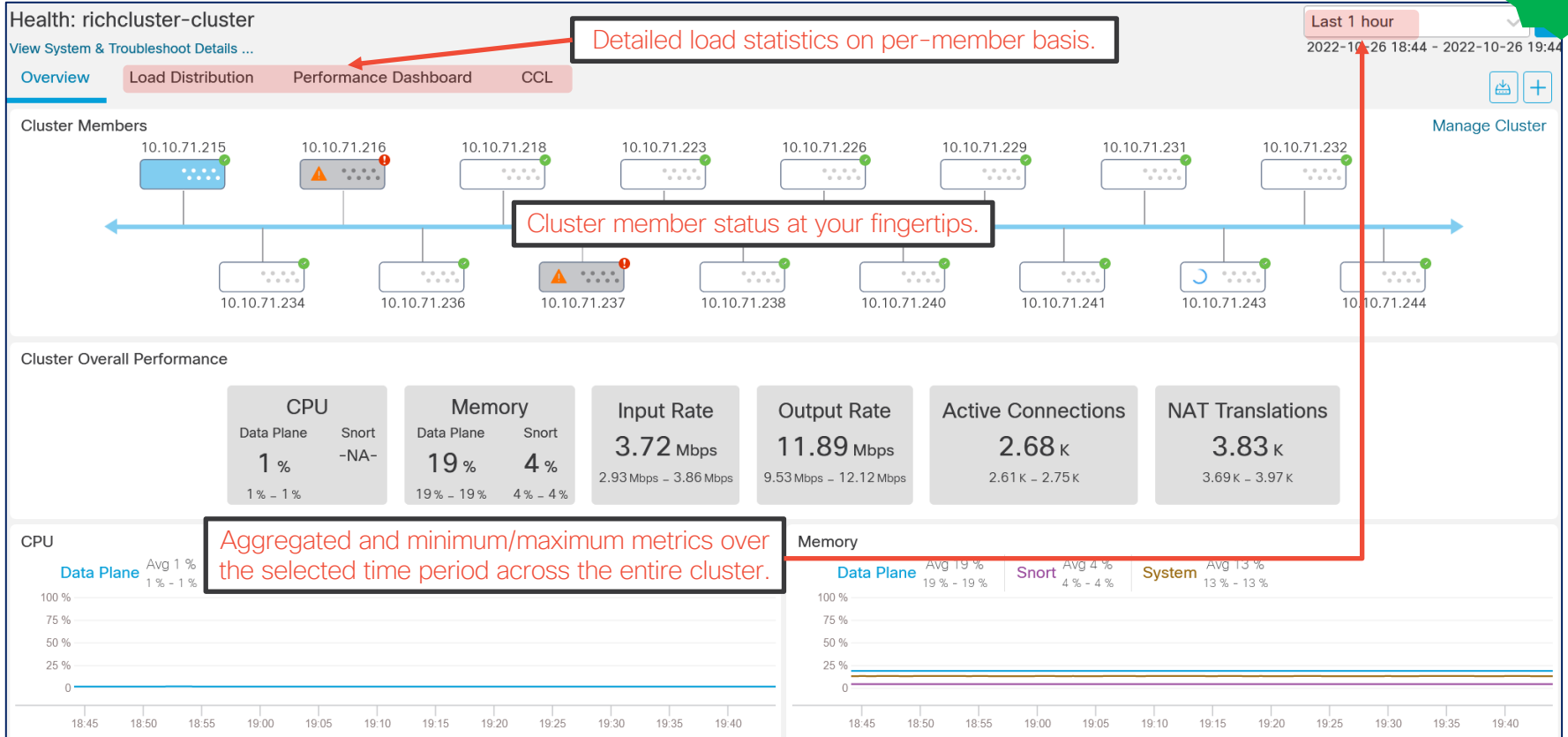
# Management



# FTD Health Dashboard



# Cluster Health Dashboard



# Unified Events with Live View



Firewall Management Center  
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? aossipov | Cisco SECURE

Q NAT Destination IP Select... Apply Cancel

Showing all 5,621 events (5,609 7 12) 2022-10-27 11:41:40 EDT → 2022-10-27 12:41:40 EDT Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule
2022-10-27 12:41:29	Connection	Allow		128.107.84.113	128.107.84.16	37420 / tcp	443 (https) / tcp	Cisco	Passive Inspect
		Allow		10.1.100.26	128.107.84.16	37420 / tcp	443 (https) / tcp	Cisco	Passive Inspect

Filter on any field and save commonly used search templates.

Switch to Live view for real-time event streaming..

Expand each event to see all connection fields.

**Decryption Rule:** Default Rule  
**SSL Flow Flags:** UNDECRYPTABLE, PRE\_DECISION\_ERRO...  
**Application Protocol:** HTTPS  
**Application Protocol Category:** network protocols/services  
**Client Application:** SSL client  
**Client Application Category:** web browser  
**Client Application Tag:** SSL protocol  
**Web Application:** Cisco  
**Web Application Category:** web services provider  
**Application Risk:** Medium

**Prefilter Policy:** Custom Prefilter  
**Domain:** Global  
**Device:** FTDv-10.1.100.27  
**Ingress Interface:** Passive-2  
**Initiator Packets:** 3  
**Responder Packets:** 2  
**QoS-Dropped Initiator Packets:** 0  
**QoS-Dropped Responder Packets:** 0  
**Initiator Bytes:** 7  
**Responder Bytes:** 1,185  
**QoS-Dropped Initiator Bytes:** 0  
**QoS-Dropped Responder Bytes:** 0

**Time:** 2022-10-27 12:41:29  
**Last Packet:** 2022-10-27 12:41:30  
**Action:** Allow  
**Source IP:** 10.1.100.26  
**Destination IP:** 128.107.84.16  
**Destination Continent:** North America  
**Destination Country:** USA  
**Ingress Security Zone:** Passive  
**Source Port / ICMP Type:** 37420 / tcp  
**Destination Port / ICMP Code:** 443 (https) / tcp  
**SSL Status:** Do Not Decrypt (Handshake Error)

2022-10-27 12:41:25	Connection	Allow		128.107.84.64	128.107.84.72	52411 / tcp	9080 / tcp		Passive Inspect
2022-10-27 12:41:19	Connection	Allow		10.1.100.26	128.107.84.16	37418 / tcp	443 (https) / tcp	Cisco	Passive Inspect



# 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
  - Ticket-based change commit mode is in the future

Legend: ■ Added ■ Edited ■ Removed

Changed Policies	Deployed Version	Pending Version
<b>Routing</b> <ul style="list-style-type: none"><li>Virtual Router (Global)<ul style="list-style-type: none"><li>OSPFv3 Process 1<ul style="list-style-type: none"><li>OSPFv3 Process Area</li><li>OSPFv3 Process</li></ul></li></ul></li></ul>	<b>Routing:</b> <b>Virtual Router: Virtual Router (Global)</b> <b>OSPFv3: OSPFv3 Process 1</b> Modified: 2020-04-23 11:37:34 Modified By: Firepower System	2020-05-13 16:58:37 admin
	<b>OSPFv3 Process Area:</b> 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	



# “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

# Simplified Access Control Policy (ACP) View



Global\_Policy  
Enter Description

Try New UI Layout  Show Warnings Analyze Hit Counts Save Cancel

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

Inheritance Settings | Policy Assignments (1)

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

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URL	Source Dynamic Attributes	Destinati... Dynamic Attributes	Action	Icons
Mandatory - Global_Policy (1-7)															
1	Block Non-Business Apps	inside	outside	Campus	Any	Any	Any	Risks: High, \	Any	Any	Any	Any	Any	Block	Icons
2	Block_Unauthorized_Wr	inside	outside	Campus	Any	Any	Any	Any	Any	Any	Adult Child Abuse Content Extreme Gambling Hate Speech	Any	Any	Interacti	Icons
3	Campus_File_Inspection	inside	outside	Campus	Any	Any	Any	HTTP HTTPS	Any	Any	Any	Any	Any	Allow	Icons

Global\_Policy

Show Warnings Analyze Hit Counts Discard Save

Packets → Prefilter Rules → SSL → Security Intelligence → Identity → **Access Control** → More Targeted: 1 device

Flow Total 7 rules Add Category Add Rule

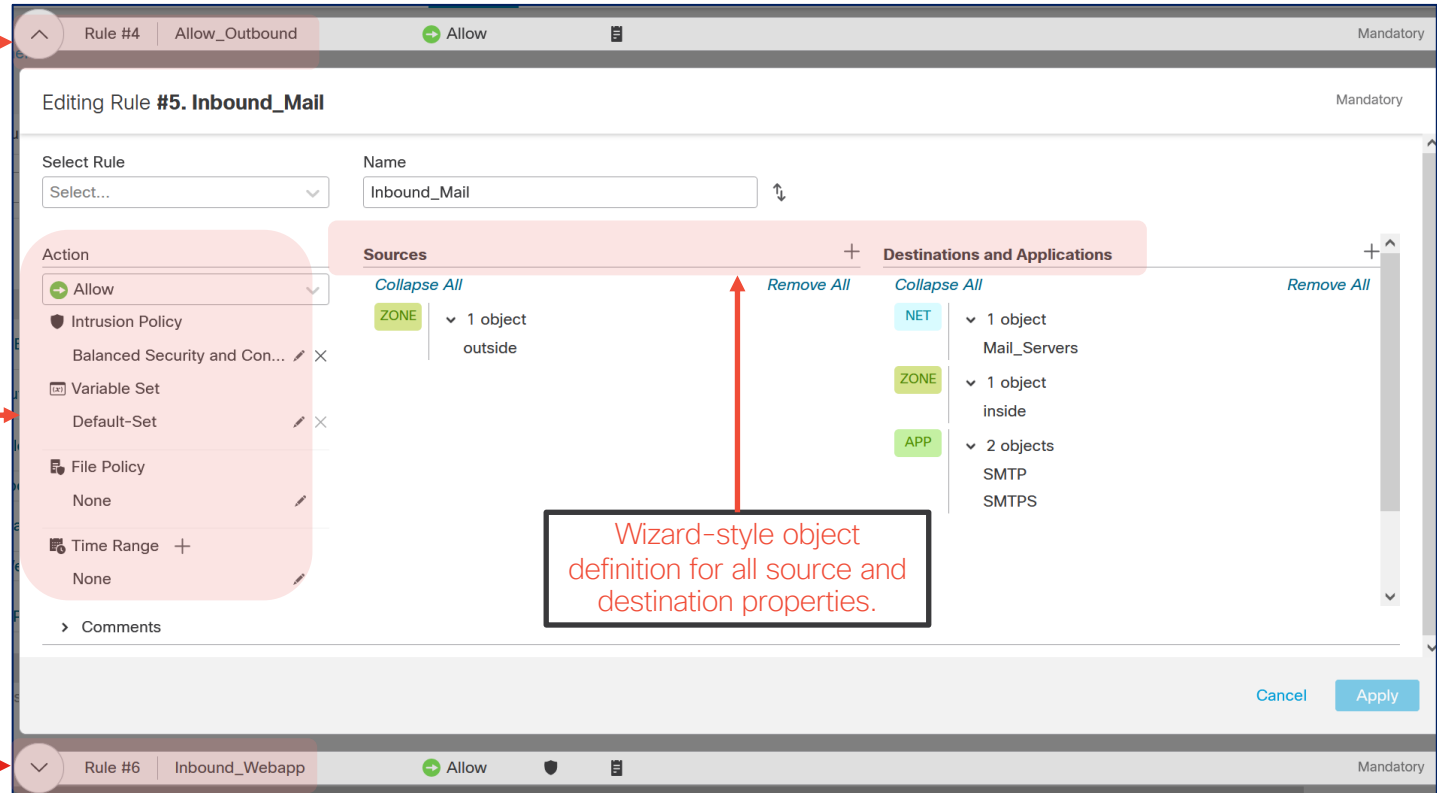
Name	Action	Source	Destinations and Applications
Mandatory (1 - 7)			
1 Block Non-Business Apps	Block	NET Campus	ZONE inside ZONE outside APP Risks: High Risks: Very High
2 Block_Unauthorized_Web	Interactive ...	NET Campus	ZONE inside ZONE outside URL Adult Child Abuse Content Extreme Gambling Hate Speech
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.



The screenshot shows the 'Editing Rule #5. Inbound\_Mail' interface. At the top, a breadcrumb trail shows 'Rule #4 | Allow\_Outbound' with a back arrow and 'Allow' status. The main area is titled 'Editing Rule #5. Inbound\_Mail' and includes a 'Mandatory' label. Below the title, there are fields for 'Select Rule' (a dropdown menu) and 'Name' (a text input containing 'Inbound\_Mail'). The interface is divided into three main sections: 'Action', 'Sources', and 'Destinations and Applications'. The 'Action' section on the left contains a list of actions: 'Allow' (selected), 'Intrusion Policy', 'Balanced Security and Con...', 'Variable Set', 'Default-Set', 'File Policy', 'None', and 'Time Range'. The 'Sources' section in the middle shows a 'Collapse All' button, a 'Remove All' button, and a list of objects: 'ZONE' (1 object, 'outside'). The 'Destinations and Applications' section on the right shows a 'Collapse All' button, a 'Remove All' button, and a list of objects: 'NET' (1 object, 'Mail\_Servers'), 'ZONE' (1 object, 'inside'), and 'APP' (2 objects, 'SMTP' and 'SMTPS'). At the bottom right, there are 'Cancel' and 'Apply' buttons. A footer bar at the very bottom shows 'Rule #6 | Inbound\_Webapp' with 'Allow' status and a shield icon.

# VPN Monitoring Dashboard

Firewall Management Center  
Overview / Dashboards / Remote Access VPN

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? BLR \ admin 🔒 cisco SECURE

**Sessions**

Select Type

By Device

FTD14 (250)

250 Total Sessions

**Active Sessions**

Headend session utilization heatmap to avoid oversubscription.

United States 50 Active Sessions

Reset

**Sessions**

- Less than 10
- 10 to 100
- 100 to 1000
- 1000 to 10000

**Device Identity Certificates**

2 Identity Certificates

- 1 certificate expiring in 1 to 30 days
- 1 certificate is expired

View Details

**Active Sessions (250)**

Select... Refresh

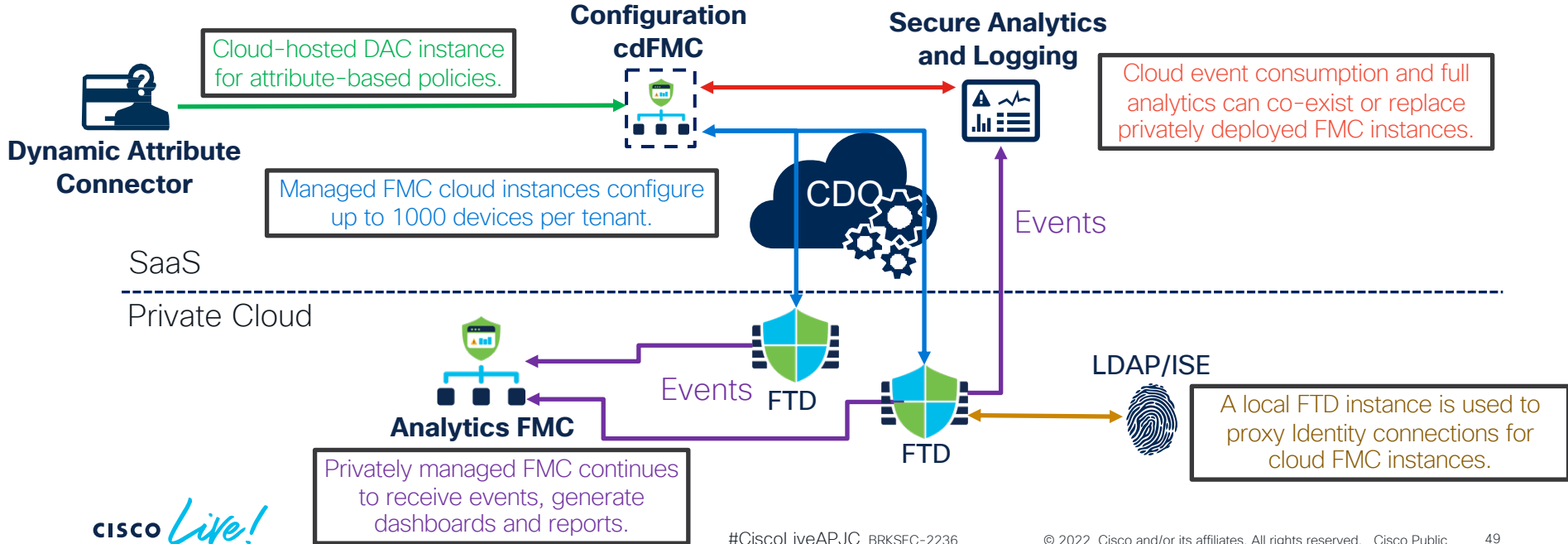
User Name	Assigned IP	Public IP	Login Time	Gateway	Client Application	Client OS	Connection Pro...	Group Policy	Actions
user998	192.168.111.52	202.12.1.115	2022-07-11 0...	FTD14	Cisco AnyConn...	win	BLR-VPN	DfltGrpPolicy	...
user527	192.168.114.251	202.12.101.28	2022-07-12 0...	FTD14		win	BLR-VPN	DfltGrpPolicy	...
user610	192.168.114.252	202.12.102.11	2022-07-12 0...	FTD14		win	BLR-VPN	DfltGrpPolicy	...
user829	192.168.115.87	202.12.27.30	2022-07-12 0...	FTD14					...
user833	192.168.115.88	202.12.27.34	2022-07-12 0...	FTD14					...
user823	192.168.115.89	202.12.27.24	2022-07-12 0...	FTD14					...
user837	192.168.115.90	202.12.27.38	2022-07-12 0...	FTD14		win	BLR-VPN	DfltGrpPolicy	...

Never miss headend identity certificate expiration again!

Active session list with ability to terminate a single session or all sessions for a user.

# Cloud-Delivered Firewall Management Center

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



# Cloud Analytics Dashboard



Defense Orchestrator
FTD Dashboard

product-tme-1  
aossipov@cisco.com

- Hide Menu
- Inventory
- Configuration
- Policies
- Objects
- VPN
- Events & Monitoring
- Analytics
- Change Log
- Jobs
- Tools & Services
- Settings

Overview | Threats | Network | Status

Last 1 year
Select devices...

### Network Activity

Egress  
 Ingress

### Top Intrusion Rules

Rule Message	Events
(stream_tcp) reset outside window (129:15:2)	188
BROWSER-OTHER HTTP characters prior to...	80
PUA-P2P Bittorrent uTP peer request (1:16...	32
(icmp4) ICMP ping Nmap (116:434:2)	14
BROWSER-IE Microsoft Internet Explorer lo...	12
PROTOCOL-DNS SPOOF query response wi...	11
PROTOCOL-SNMP request udp (1:1417:18)	11
PROTOCOL-SNMP trap udp (1:1419:18)	11

### Top Intrusion Targets

Responder IP	Events
::192.168.105.1	405
::1.3.42.61	192
::1.4.88.105	184
::1.3.15.231	184
::1.4.28.84	176
::1.4.39.40	172
::1.4.24.239	172
::1.4.2.137	172

### Top Intrusion Attackers

### Top Malware Signatures

Threat Name	Events
Xls.Exploit.Swfdrop::95.sbx.tg	68
Doc.Exploit.Mspoint::95.sbx.tg	19

### Top Malware Senders

Sending IP	Events
::192.168.104.245	77
::	4

CISCO Live!

#CiscoLiveAPJC BRKSEC-2236

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

50

# Simple Migration of FTD to Cloud Management

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

Inventory / Change FTD Manager

Change FTD Management  
Change FTD Manager from Firewall Management Center to CDO

1 Select FMC **FMC: 1771Fmc** Per-device co-management dispositions.

2 Select Devices

Select FTD devices to change management from FMC to CDO and specify an action in bulk or per device.

6 device(s) selected Multi-Device Action Multiple Actions Selected

✓	Name	IP Address	Domain	Action
✓	1771Fmc_10....	10.10.16.94:44	Global	Delete FTD from FMC
✓	1771Fmc_10....	10.10.16.87:44	Global	Delete FTD from FMC
✓	1771Fmc_10....	10.10.16.86:44	Global	Retain on FMC for Analytics
✓	1771Fmc_10....	10.10.16.70:44	Global	Retain on FMC for Analytics

Change FTD Management

After completing the change FTD manager process, you have up to 14 days to commit to CDO as your FTD manager or revert to FMC as your FTD manager.

After 14 days have passed, the actions you selected during this process will be automatically applied to your devices without further action from you. [Learn more.](#)

**Warning:** Deleting an FTD from FMC is final.

Migrations are reversible for 14 days.



# SecureX with Secure Firewall

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

**Incidents** | New Incident | MALWARE-CNC Win.Trojan.Ze...

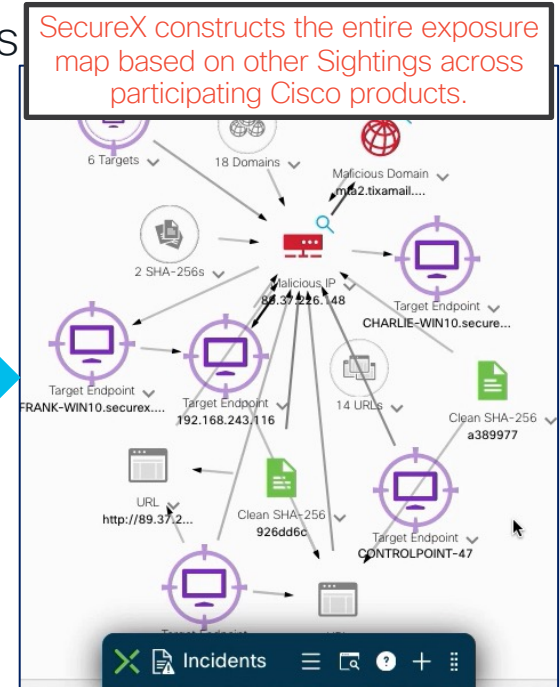
Search... | Assigned to me - Open (10) | Assigned to me - New (4)

**Intrusion event 1-48764-1** | NGFW Event Service | Mar 02, 2021

Summary | Observables | Timeline | Sightings | Linked References (0)

Incident Title	Intrusion event 1-48764-1
Urgency	High
Event Time	2021-03-02T22:54:41.000Z
Promoted At	2021-03-02T23:02:37.116Z
Reporting Device Type	NGFW
Reporting Device ID	ftd66-2.securex.local
Intrusion Rule Message	MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
Event Details	<a href="https://admin.sse.itd.cisco.com/events/show?id=5ee21992-b989-4af9-b609-7a6ca1a2faec">https://admin.sse.itd.cisco.com/events/show?id=5ee21992-b989-4af9-b609-7a6ca1a2faec</a>
Snort Rule	<a href="https://snort.org/rule-docs/1-48764">https://snort.org/rule-docs/1-48764</a>
Promotion Reason	intrusionRuleCategory,snortRuleImpact: impact_red





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



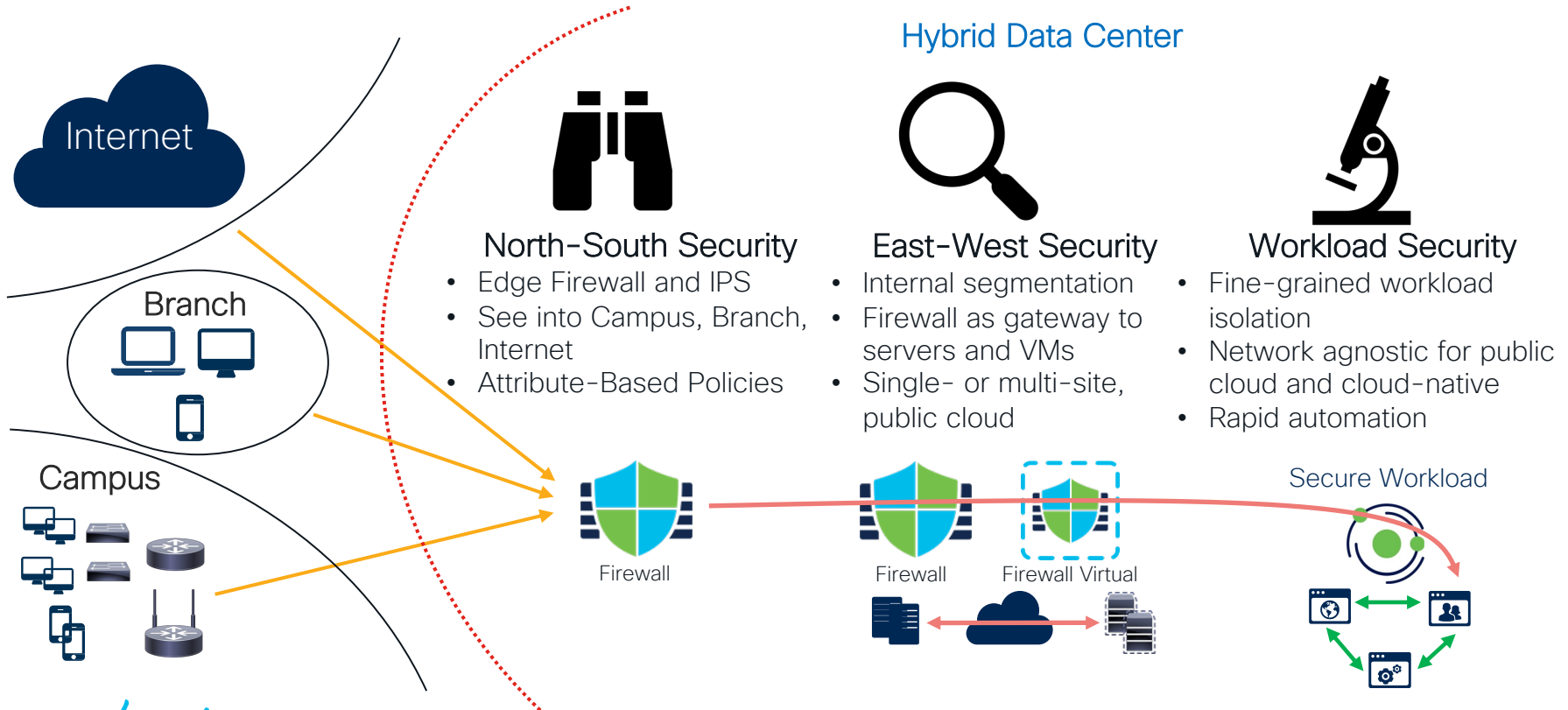
# Secure Workload



# Secure Workload Functional Overview

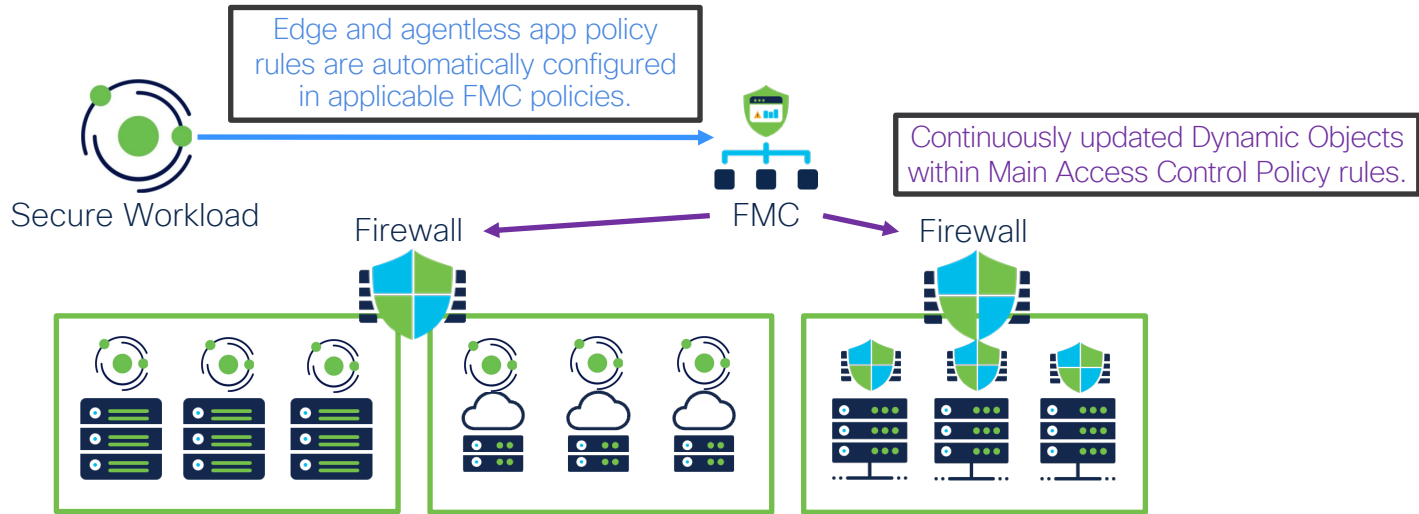
- Born for app visibility (Tetration), graduated to microsegmentation
  - Employs host OS agents for visibility and built-in firewalls for enforcement
- Ingests network telemetry from agents, Netflow/IPFIX, VPC flow logs
  - App flow discovery with Application Dependency Mapping (ADM)
  - Policy recommendation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

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



# Secure Workload Policy Orchestration in FMC



Firepower Management Center  
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects AMP

Deploy Search Settings Help DC-East-West | admin

### 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.

Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

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

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

#	Name	Source 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.



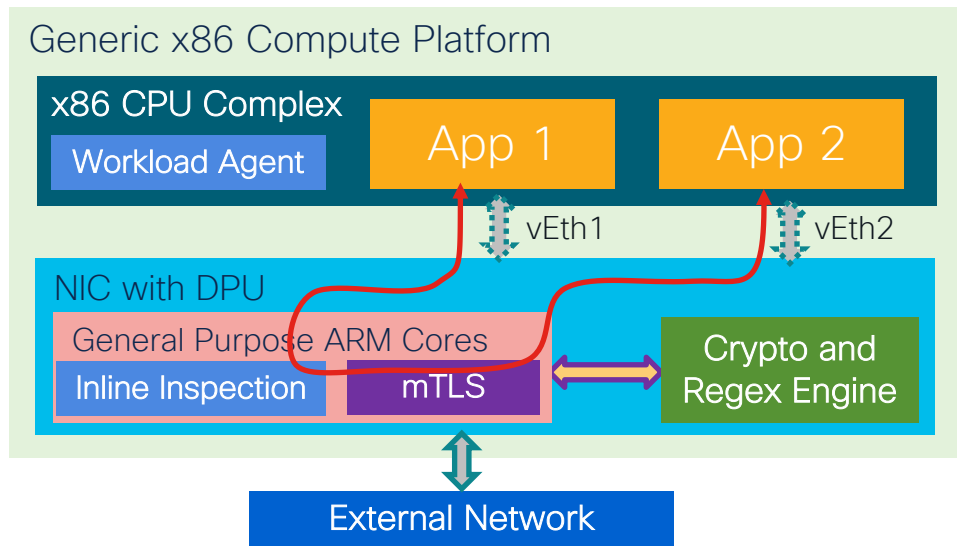


# Workload Segmentation with DPU

- 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](https://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](http://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

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

ALL IN

#CiscoLiveAPJC