The bridge to possible

Keeping Up on Network Security

with Cisco Secure Firewall

Luke Bromirski
BRKSEC-2236

mr0vka@infosec.exchange

@lbromirski

Cisco Webex App

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

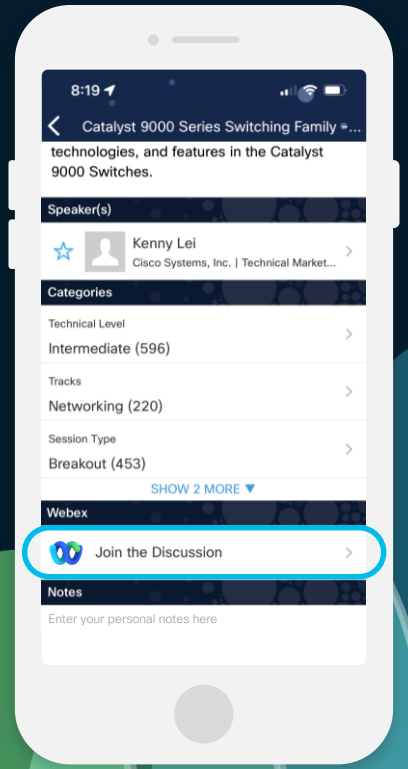
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

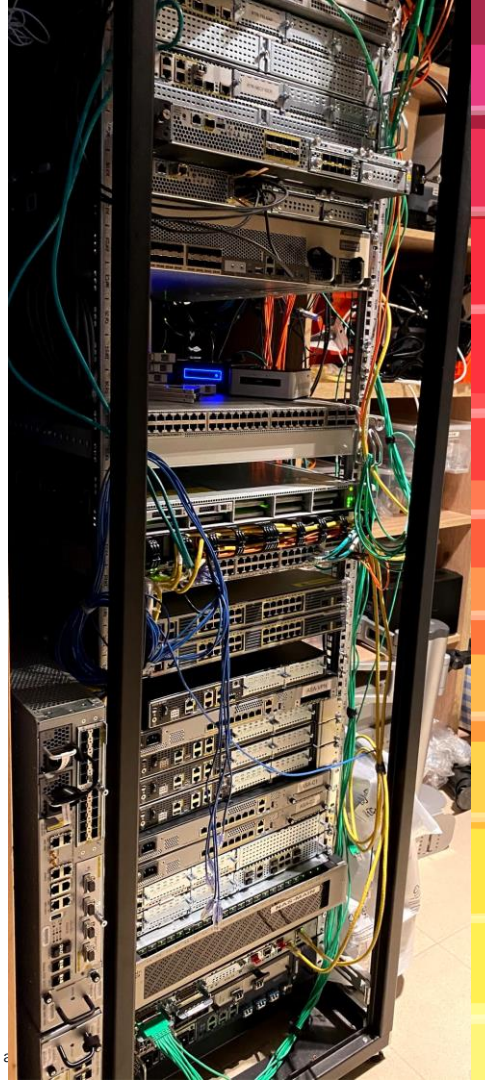
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the Firewall Platform Team until June 7, 2024.



Your Speaker

- CCIE #15929 (R&S/SP)
  CCDE #2012::17
- BGP Blackholing PL, AS 112 cluster in Poland, PLNOG co-founder
- https://lukasz.bromirski.net/
- Leading **Firewall Platform Team** at Cisco Security Business Group

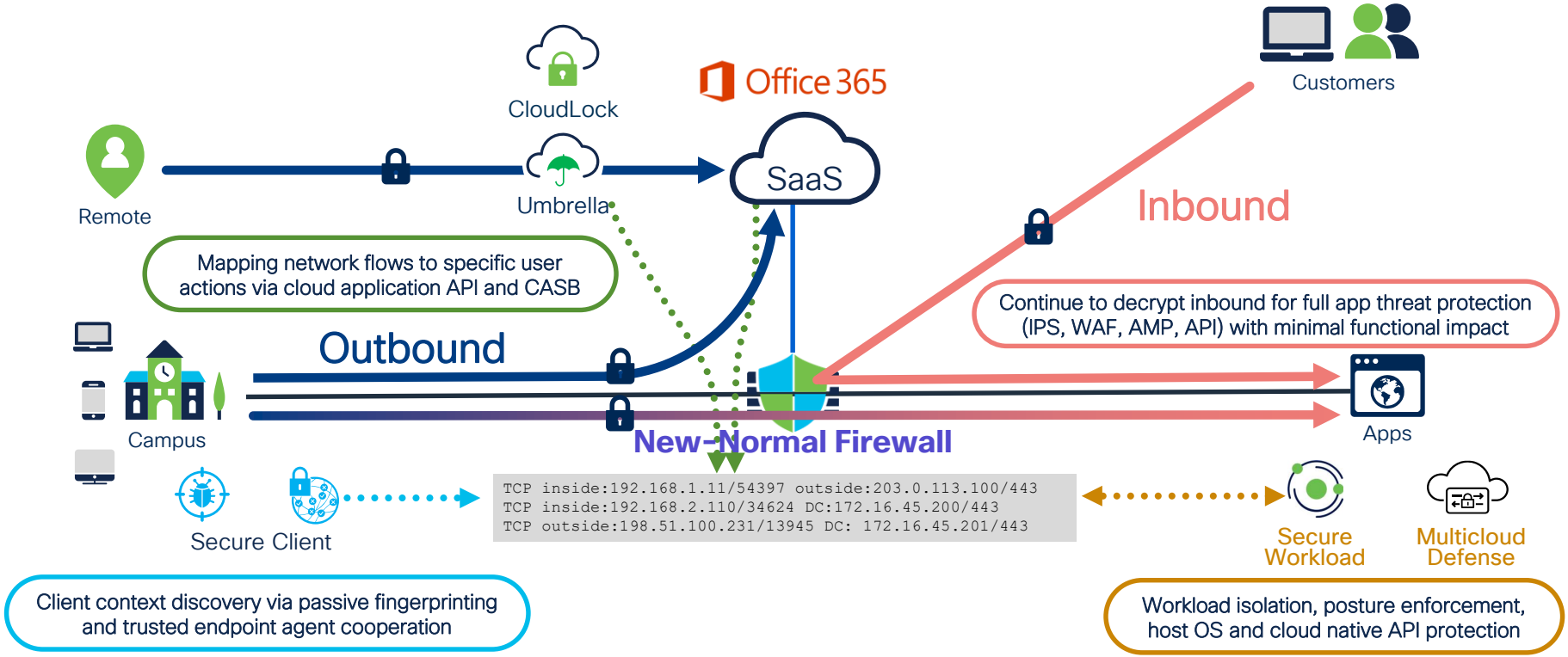


FTD ASA

Agenda

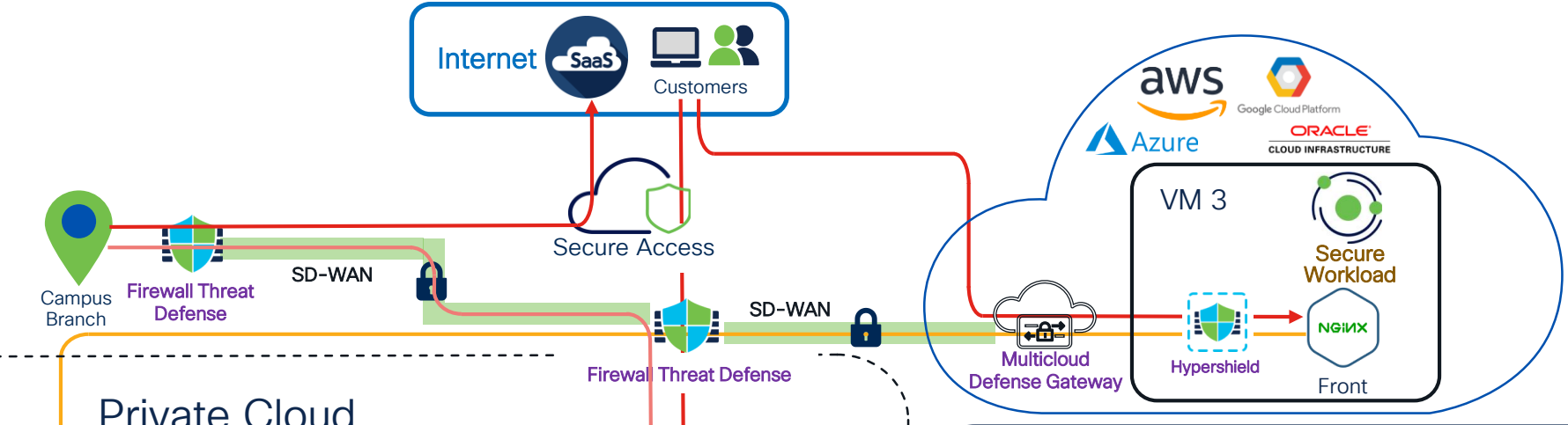
- Introduction
- Firewall
  - Platform
  - Threat Protection
  - Connectivity
  - Hybrid Work
  - Management
- Workload
- Conclusion

Secure Firewall: Inspect, Infer, and Cooperate



Firewall Vision: Network, Workload, and Cloud

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



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

Platforms

FTD 7.4

ASA 9.20

Secure Firewall 4200 Overview

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 (SED)
- Up to 2x1.8TB in RAID1 on 4245 (SED)

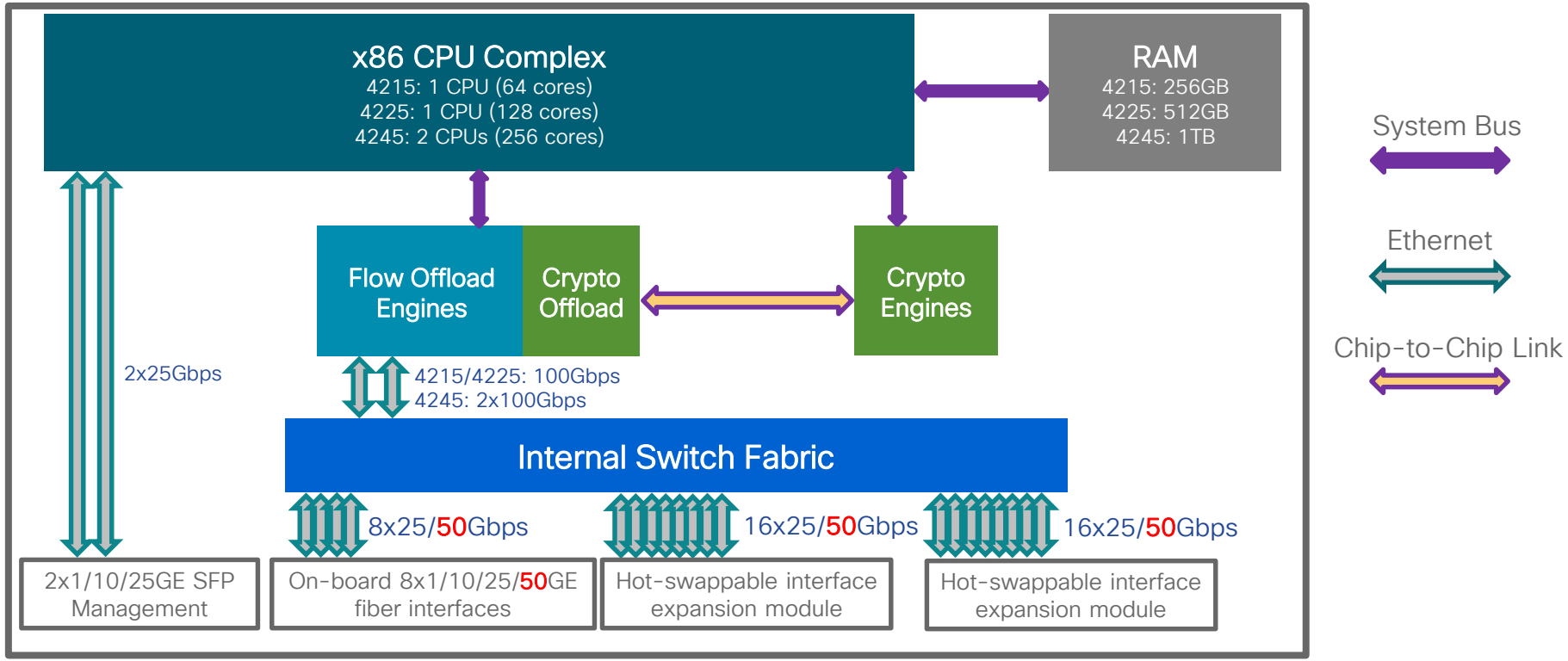
Expansion Network Modules

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

Secure Firewall 4200 Architecture

FTD 7.4

ASA 9.20



Secure Firewall 4200 Performance

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

Secure Firewall 1200C Series

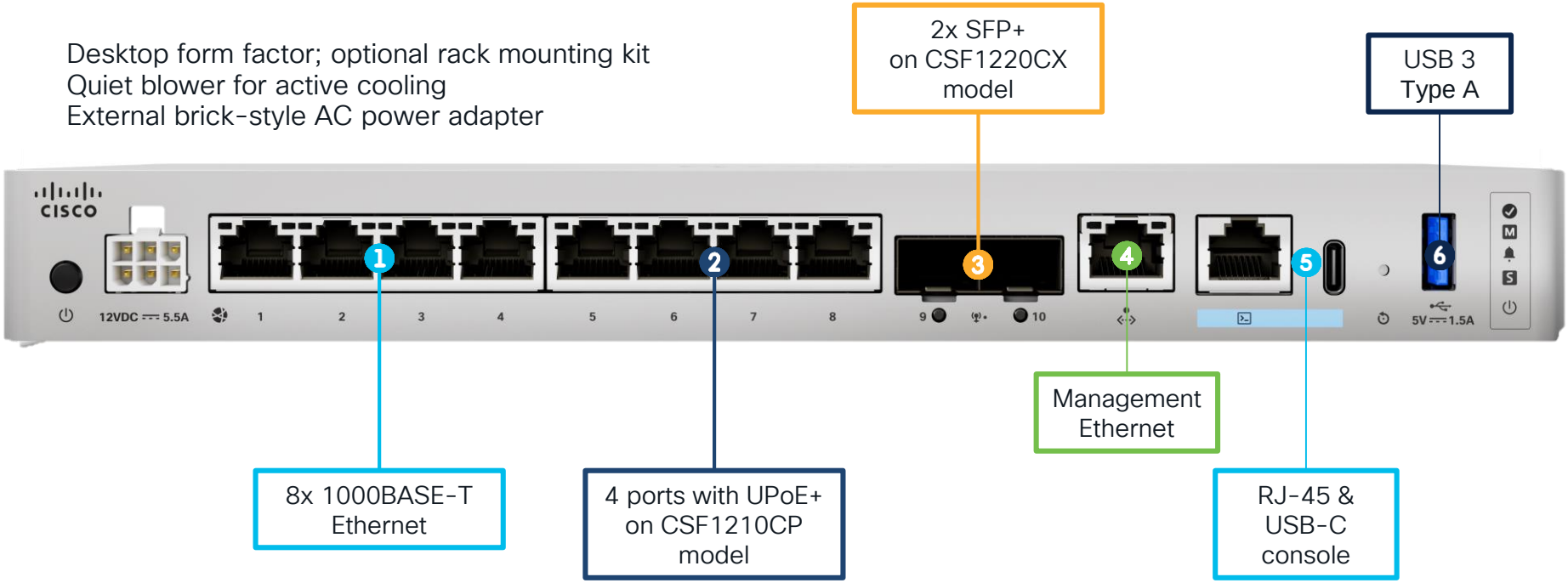
FTD 7.6

ASA 9.22

- 3 compact models – 1210CE, CP, 1220CX
  - 8 core SoC ARM design
  - 16GB of RAM
  - 240GB of NVMe storage
  - Fixed 8x1GE:
    - 1210CP - 4x1GE with UPoE+ support (120W total, max of 90W per port)
    - 1220CX - plus 2x 1/10G SFP+
- Multiple SoC-embedded accelerators
  - encryption/decryption
  - traffic processing
- Up to 2.6Gbps (450B) or up to 6Gbps (1024B) for NGFW traffic profiles (~10x over 1010, ~3x over 11xx)
- Up to 5Gbps for IPsec VPN, and up to 1.7Gbps for TLS 1.2/1.3

Secure Firewall 1200C Overview

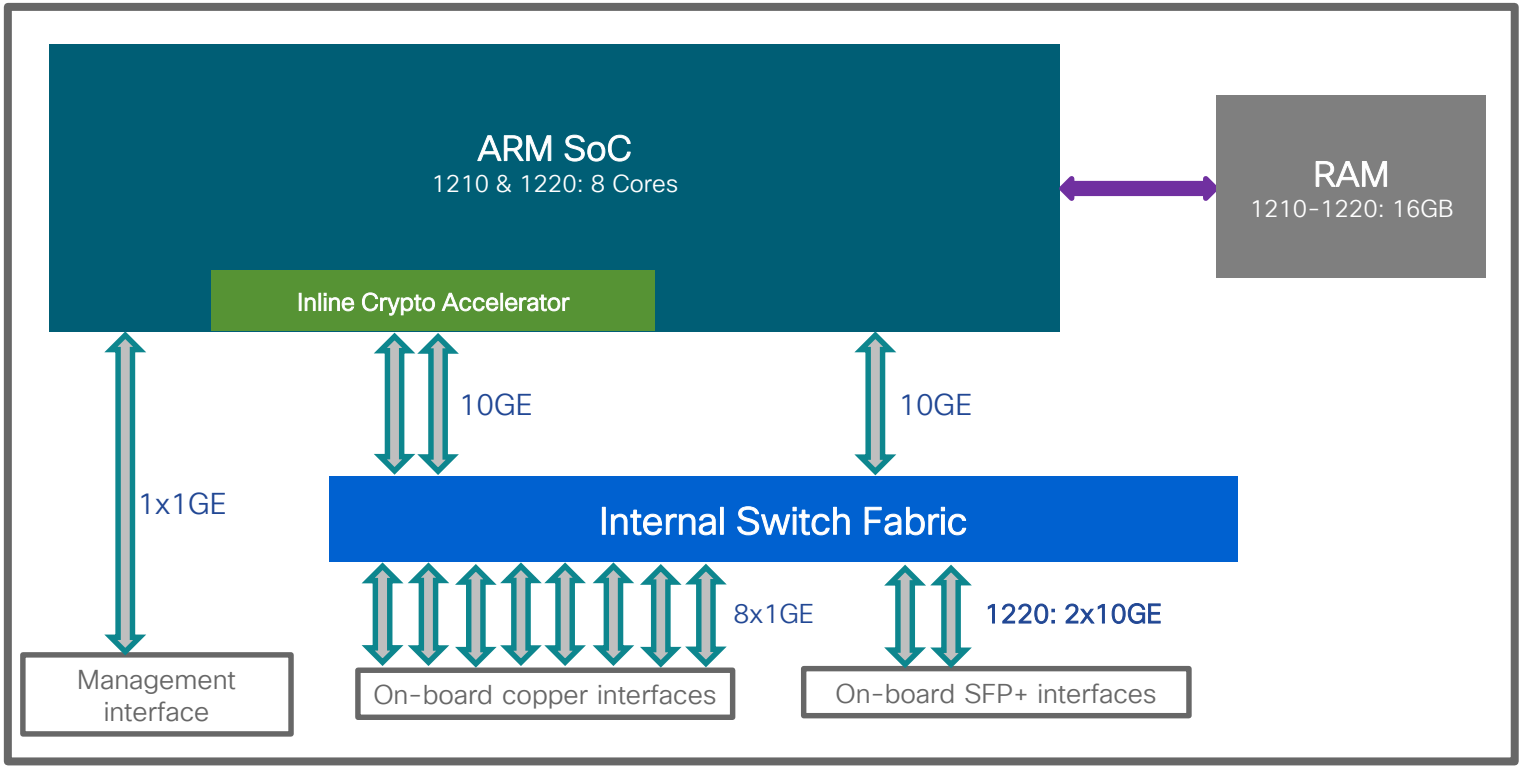
Desktop form factor; optional rack mounting kit
Quiet blower for active cooling
External brick-style AC power adapter



Secure Firewall 1200C Architecture

FTD 7.6+

ASA 9.22+



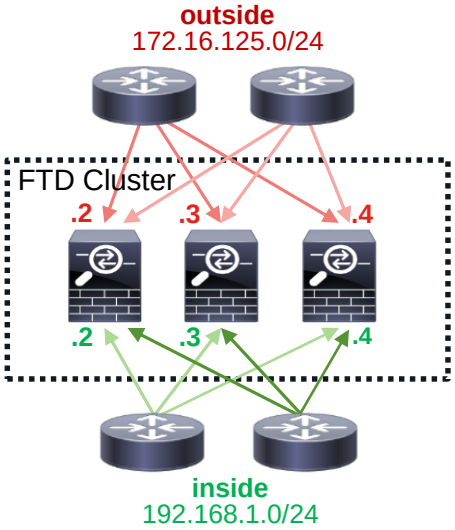
System Bus

Ethernet

FTD 7.6

Individual Mode Clustering

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



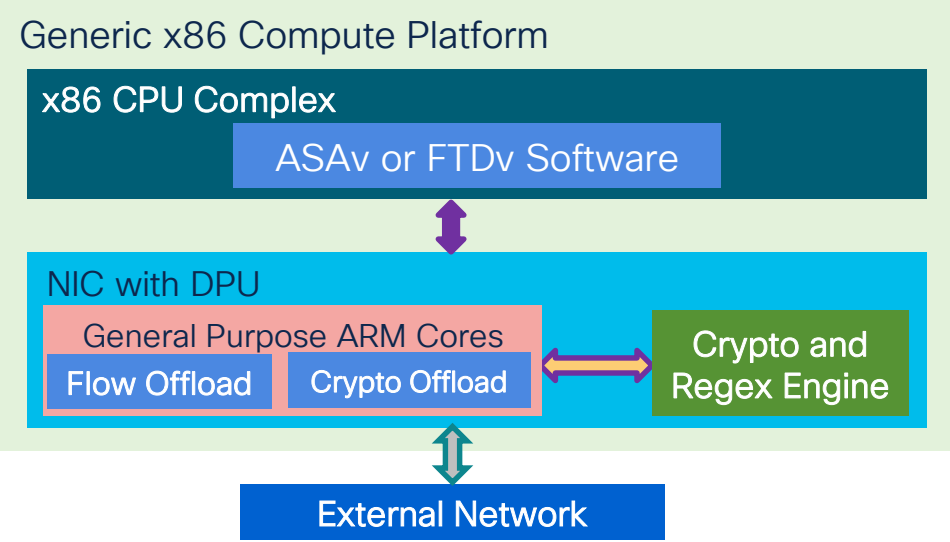
Future

Virtual Firewall on Data Processing Unit (DPU)

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

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

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

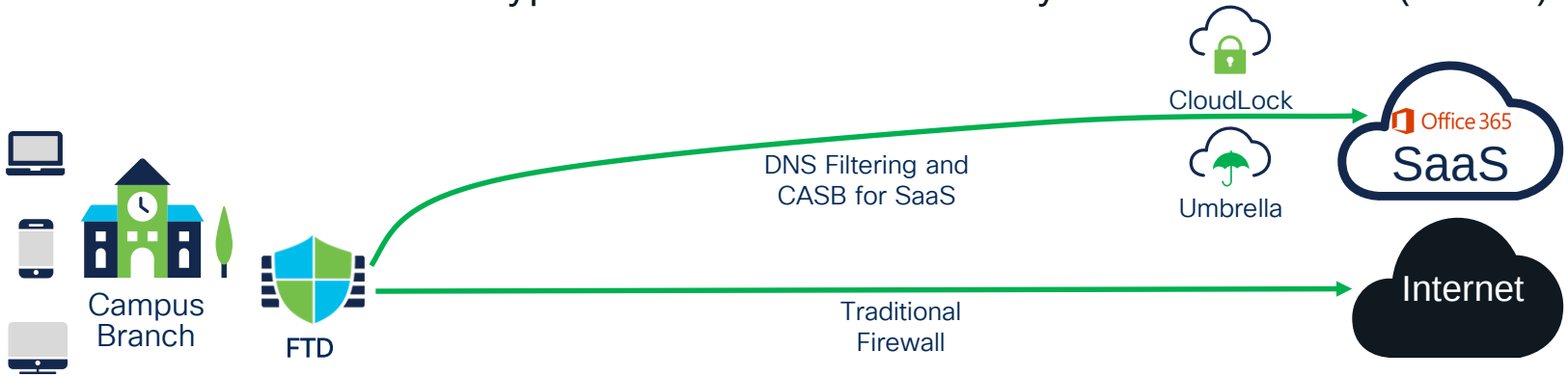


Threat Protection

FTD 7.2+

Enhance Firewall with Umbrella Cloud Security

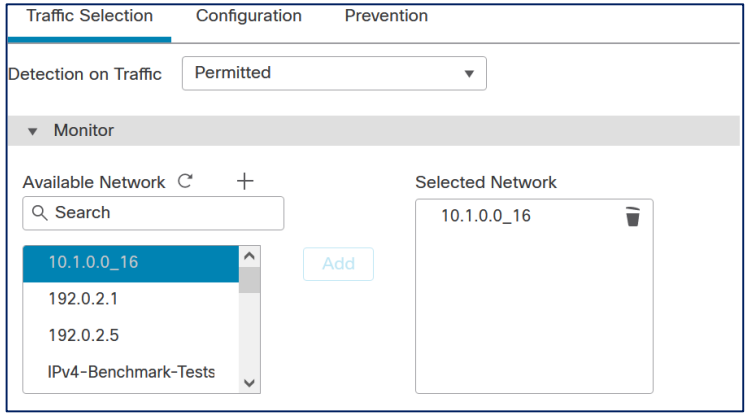
- Edge firewall is less effective against some outbound traffic
  - Dynamically changing DNS and undecryptable TLS connections
- Selectively redirect DNS, SaaS, and other traffic to Umbrella instead
  - Cloud-delivered DNS blocks most threats early with no local cycles spent
  - No SaaS traffic decryption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

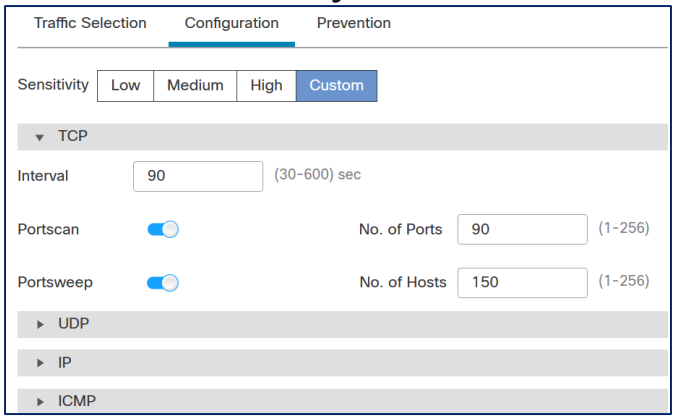


FTD 7.2

Portscan Detection and Prevention

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





Encrypted Visibility Engine (EVE)

FTD 7.1

TLS ClientHello

```
Cipher 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 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    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)
```

Firefox

TCP/TLS 192.168.2.110/34624->172.16.45.200/443

TCP/TLS 192.168.2.110/21013->203.0.113.154/443

Firewall

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

```
Cipher Suites (19 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    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: nsksdlkoup.me

https://github.com/cisco/mercury

EVE-enriched Unified Events

FTD 7.1

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

Firewall Management Center
Analysis / Unified Events

Overview | Analysis | Policies | Devices | Objects | Integration

Deploy | alext | SECURE

Select... | Refresh

Showing 23 events (19 4) | 2022-04-06 09:45:32 MDT → 2022-04-06 09:46:30 MDT 58s | Live

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.

Encrypted Visibility Engine (EVE) 2.0

FTD 7.4

Encrypted Visibility Engine

About Encrypted Visibility Engine

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

Recommended Settings

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

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

EVE Enhanced Analytics

Add EVE's fingerprint information in the connection events.

Block Traffic Based on EVE Score

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

Advanced Mode

Block

Very Low | Low | Medium | High | Very High

Revert to Defaults | Cancel | OK

Inference-based AppID enrichment.

Detailed fingerprint data for third-party use.

Connection filtering based on malware confidence scores.

Now

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

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

Secure Firewall Application Detectors

- Home
- Release Notes
- Support
- Documentation
- Resources
- Feedback

Risk		Business Relevance	
Very Low	1,478	Very High	345
Low	922	High	1,028
Medium	1,374	Medium	2,430
High	1,651	Low	1,259
Very High	638	Very Low	1,001

Tags	Show All Tags
adds/installs other software	66
adult content	37
allows remote connect	97
allows remote control	53
antivirus	13

Categories

- active directory
- ad portal
- anonymizer/proxy
- application development an
- backup and recovery

pplication Details (6,063)

Application Name	Description	Risk	Bus Rel
050plus	VoIP smartphone app.	Medium	
1&1 Internet	Internet and Domain name service provider.	Very Low	
1-800-Flowers	Online retailer of flowers and other gifts.	Low	
1.1.1.1 App	Offers a free app for mobile that makes internet private, safer and prevents anyone from snooping on the user.	High	
1000mercis	Advertising and analytics site.	Low	
1001.com	Provides online games.	High	

Secure Firewall Application Detectors

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: 2023.12.12

stats:
  general:
    total fingerprints:         10,000
    total labeled fingerprints: 5,405
    total connections:          4,085,565,284
    fingerprints per protocol:
```

Full AppID database update information, including EVE fingerprint data.

```
      tls: 2,470,673,413
     http: 1,518,166,983
     quic: 96,724,888

  Threat Grid:
    total fingerprints: 812
    total connections:  5,531,639
    fingerprints per protocol:
      http: 651
       tls: 161
    connections per protocol:
       tls: 3,895,992
      http: 1,635,647
```

FTD 7.6

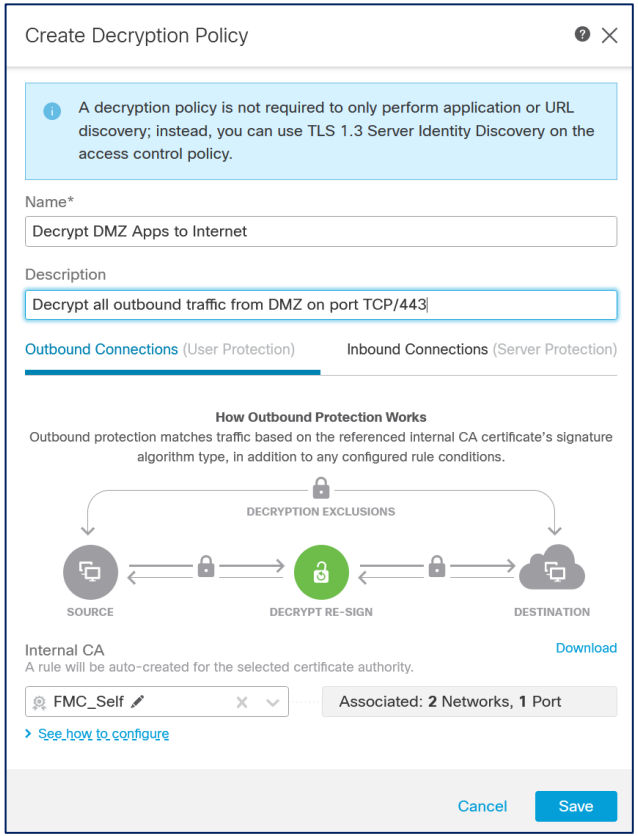
SnortML: Neural Exploit Engine

- Traditional IPS rules are based on known and fixed patterns
  - Slight changes to payload patterns can evade static signatures
  - Undisclosed or new vulnerabilities take time to become signatures
- Neural Detector uses Machine Learning to expand IPS capabilities
  - Trained on all known embodiments for a given vulnerability type
  - Detects new patterns for the vulnerability without a static signature
  - TLS or QUIC decryption is still required

FTD 7.3

Simplified TLS Decryption Policy

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

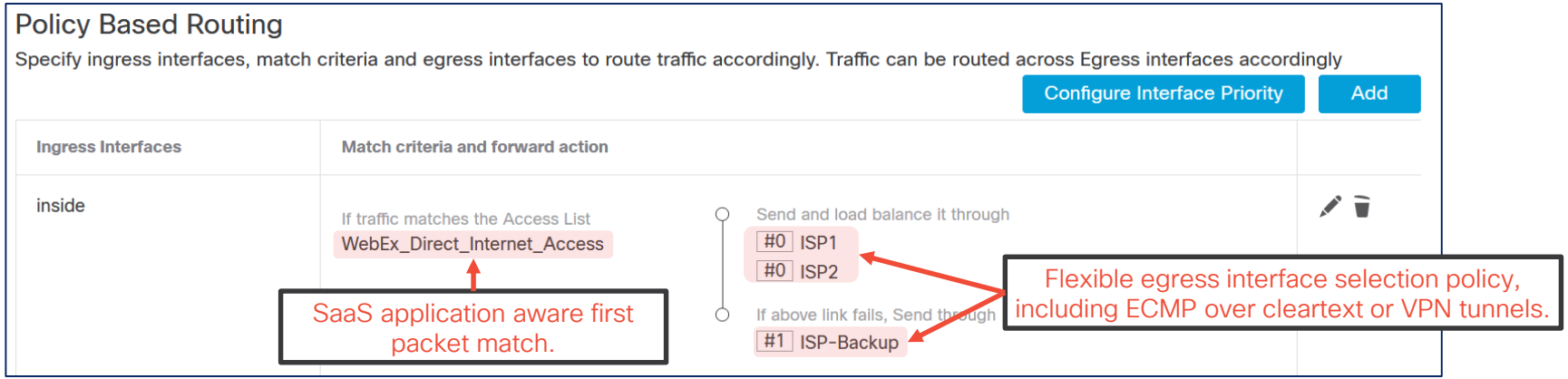


Connectivity

FTD 7.1

Application-Aware Policy Routing

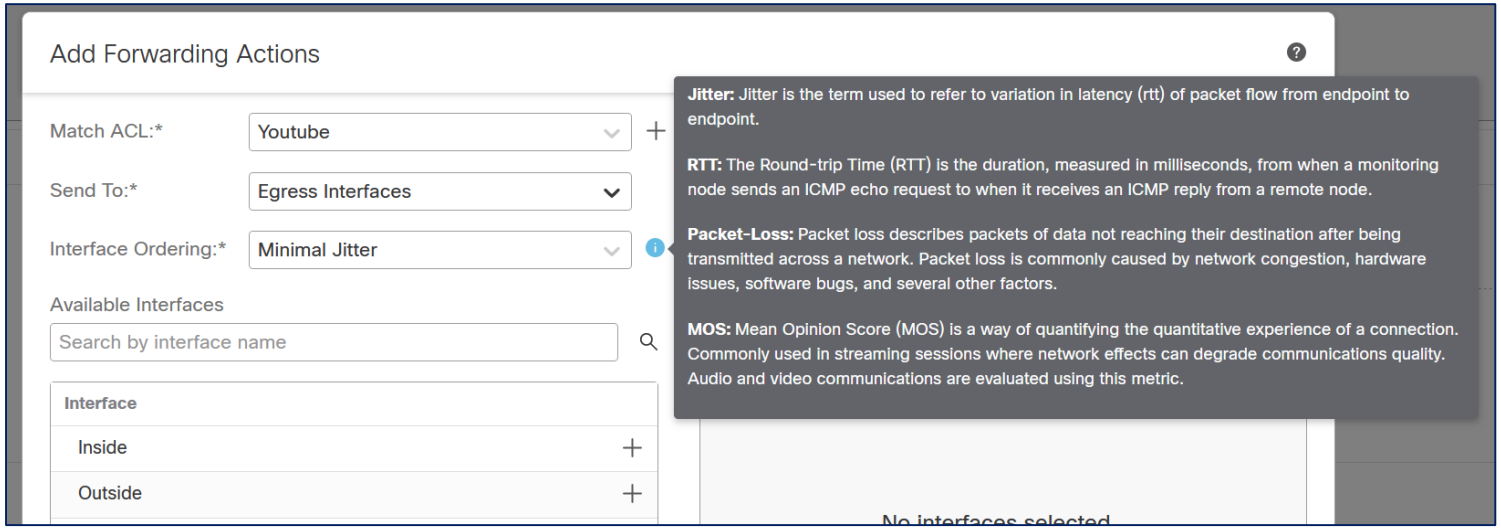
- Native support for Policy Based Routing configuration in FMC
  - Commonly used SaaS applications can be used as matching criteria
  - DNS snooping to Trusted Servers to support domain pattern matching
  - Data Plane maps app names to IP addresses with Network Service Groups
- Used in Direct Internet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



FTD 7.2

Path Monitoring and Quality-Based Routing

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



SD-WAN Monitoring Dashboard

FTD 7.4

Summary Dashboard (switch dashboard)

Provides a summary of activity on the appliance

Network | WAN Summary | Site to Site VPN | Remote Access | QoS | Geolocation | Threats | Intrusion Events | Status +

Select... | Refresh | Refresh Every 10 minutes

WAN Connectivity

640 total interfaces

- 90% Online 320 interfaces
- 5% Offline 160 interfaces
- 5% Idle 160 interfaces

WAN Quality

520/640 interfaces only displayed

120 interfaces needs path monitoring facility

	Top 10%	Bottom 10%
Latency	250-120 ms	0 ms
Jitter	180-150 ms	2 ms
MOS	1-2	5
RTT	100-80 ms	2 ms
Packet Loss	80-60 ms	5 ms

Interface Throughput Distribution 1 day

Applications | Tunnelled vs DIA | Top Hosts

135 TB Total

- Microsoft 10 TB
- AWS 20 TB
- Gaming services 35 TB
- Netflix 70 TB

Interface List

Search

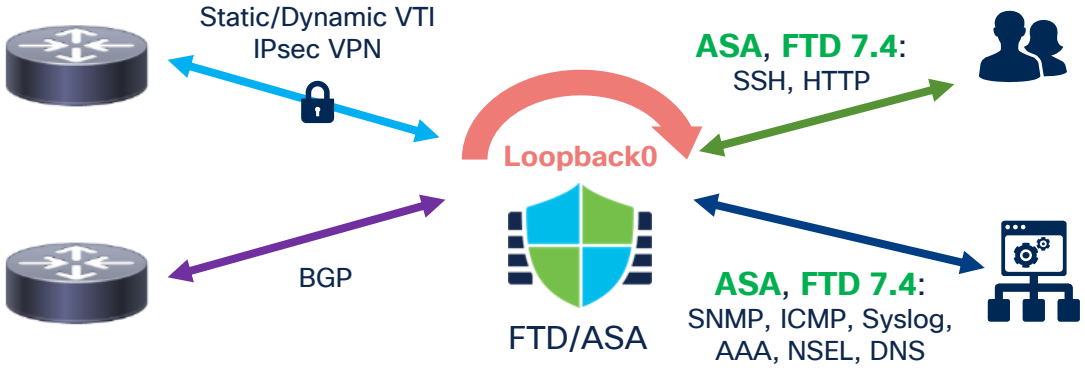
Interface Name	Device Name	Logical Name	Latency	Jitter	RTT	Packet Loss	Actions
Gigabit Ethernet 0/0	Corporate_FTD	outside	160ms	75ms	26ms	5	•••
Gigabit Ethernet 0/1	Corporate_FTD	physical	45ms	27ms	20ms	1	•••
Gigabit Ethernet 0/2	Corporate_FTD	inside	20ms	38ms	30ms	4	•••
Gigabit Ethernet 0/3	Corporate_FTD	outside	25ms	30ms	21ms	1	•••
Gigabit Ethernet 0/0	Device_123	physical	250ms	15ms	18ms	2	•••
Gigabit Ethernet 0/1	Device_123	inside	15ms	18ms	15ms	4	•••
Gigabit Ethernet 0/0	Device_FTD	inside	65ms	11ms	12ms	5	•••

FTD 7.3+

ASA 9.18.2

Loopback Interface

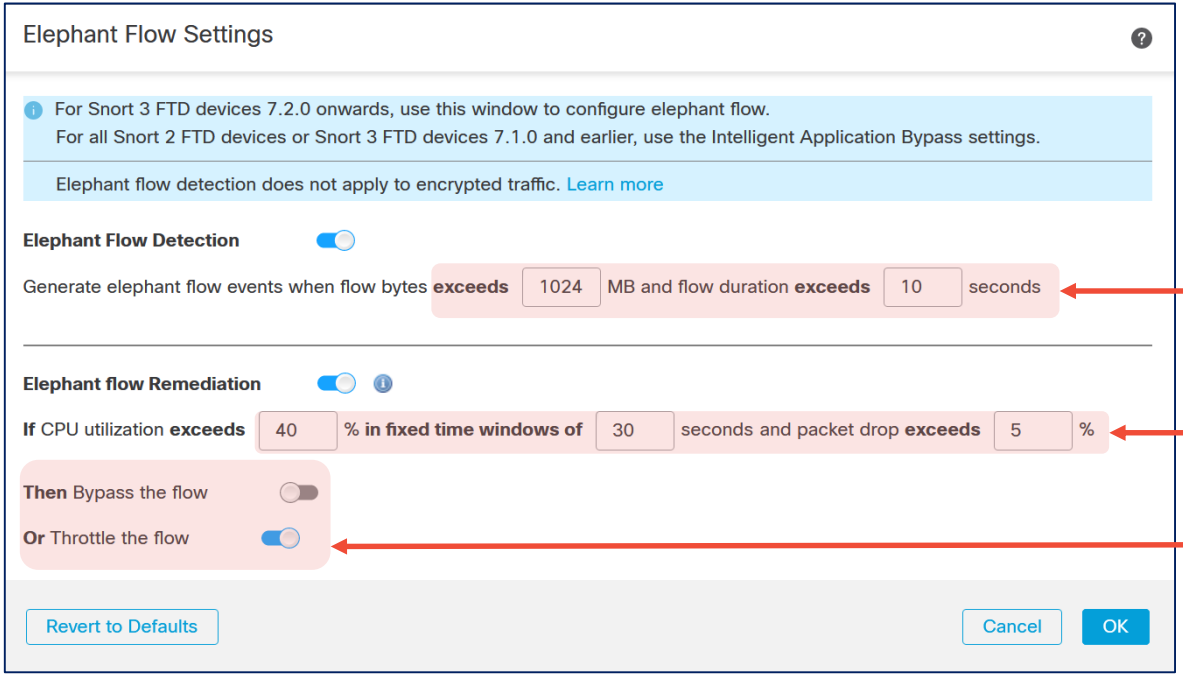
- Abstract to- and from-device connectivity from physical interfaces
  - IPv4/IPv6 addressing in routed and transparent (except for VTI) modes
  - HA/failover and clustering (except for VTI) support



FTD 7.2

Elephant Flow Detection

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



Throughput threshold to qualify as an Elephant Flow

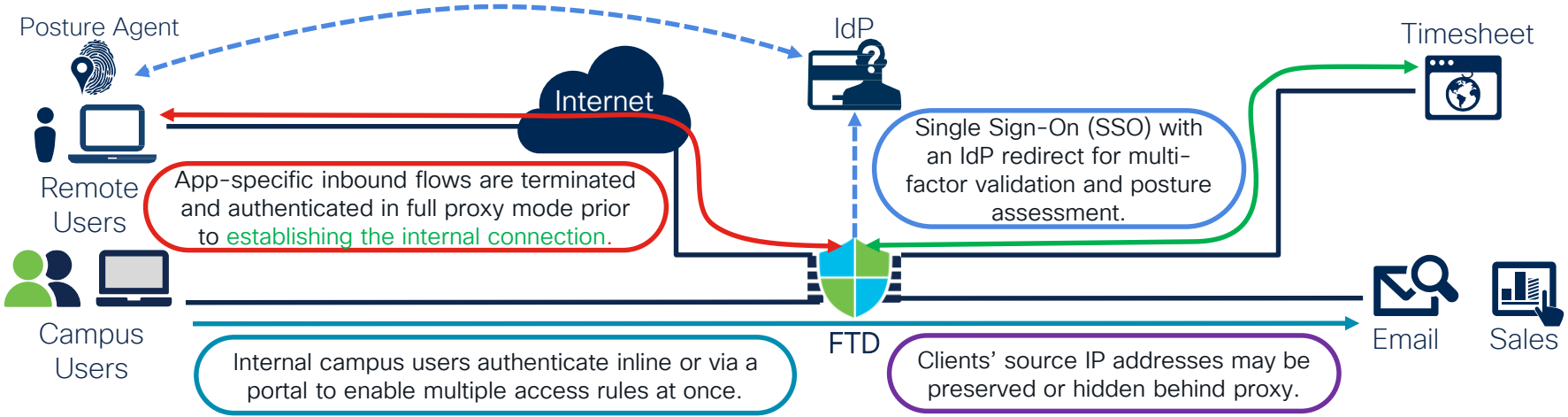
Optional flow-specific CPU resource consumption and packet drop thresholds for remediation.

Optional flow remediation actions.

FTD 7.4

Clientless Zero Trust App Access (ZTAA)

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



Clientless ZTAA: App Definition

FTD 7.4

Add Application

Enabled

1 **Application Settings** Edit

Application Name	Payroll
External URL	https://payroll.acme.com
Application URL	https://payroll-prod.acme.private
Application Certificate	PayrollApp
Application Group	-

2 **SAML Service Provider (SP) Metadata** Edit

Entity ID	https://payroll.acme.com/saml/sp/metadata/payroll.acme.com
Assertion Consumer Service (ACS) URL	https://payroll.acme.com/+CSCOE+/saml/sp/acs?tgname=DefaultZeroTrus...

3 **SAML Identity Provider (IdP) Metadata** Edit

Entity ID	https://www.okta.com/exk08Ko9uope1
Single Sign-On URL	https://dev-100.okta.com/app/dev-11111_payroll/exk08Ko9uope1
IdP Certificate	test

4 **Re-Authentication Interval** Edit

Timeout Interval	1440 minutes

5 **Interface Access and Security Controls** Edit

Security Zones	Overridden (Outside-DMZ)
Intrusion Policy	Overridden (Balanced Security and Connectivity)
Variable Set	Overridden (Default-Set)
Malware and File Policy	Overridden (Block Malware)

Cancel Finish

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

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

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

Hybrid Work

FTD 7.2

Consistent Protection in Hybrid Cloud

Private Cloud

HyperFlex

vmware ESXi

KVM

NUTANIX

openstack.

Public Cloud

Microsoft Azure

Google Cloud Platform

aws

rackspace technology.

EQUINIX

ORACLE CLOUD INFRASTRUCTURE

Alibaba Cloud

alkira

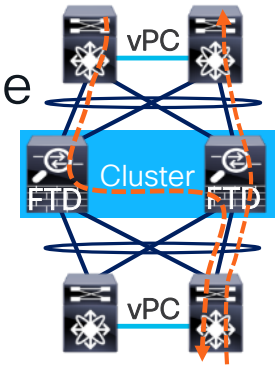
Secure Firewall Capabilities

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

FTD 7.1+

ASA 9.17+

Clustering for Virtual Firewalls

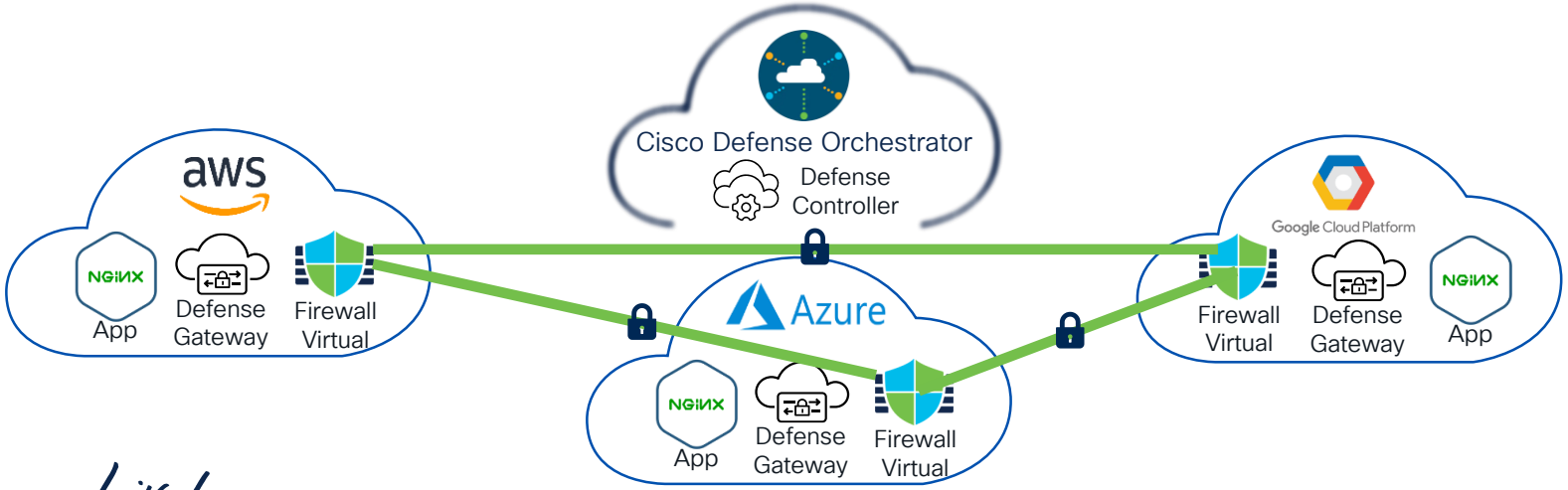


- Clustering combines multiple firewalls into one logical device
  - Seamless scalability up to 16 FTD units with no traffic disruption
  - Stateful handling of asymmetric traffic and failure recovery
  - Single point of management and unified reporting
- Better elasticity and failure handling in hybrid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

Now

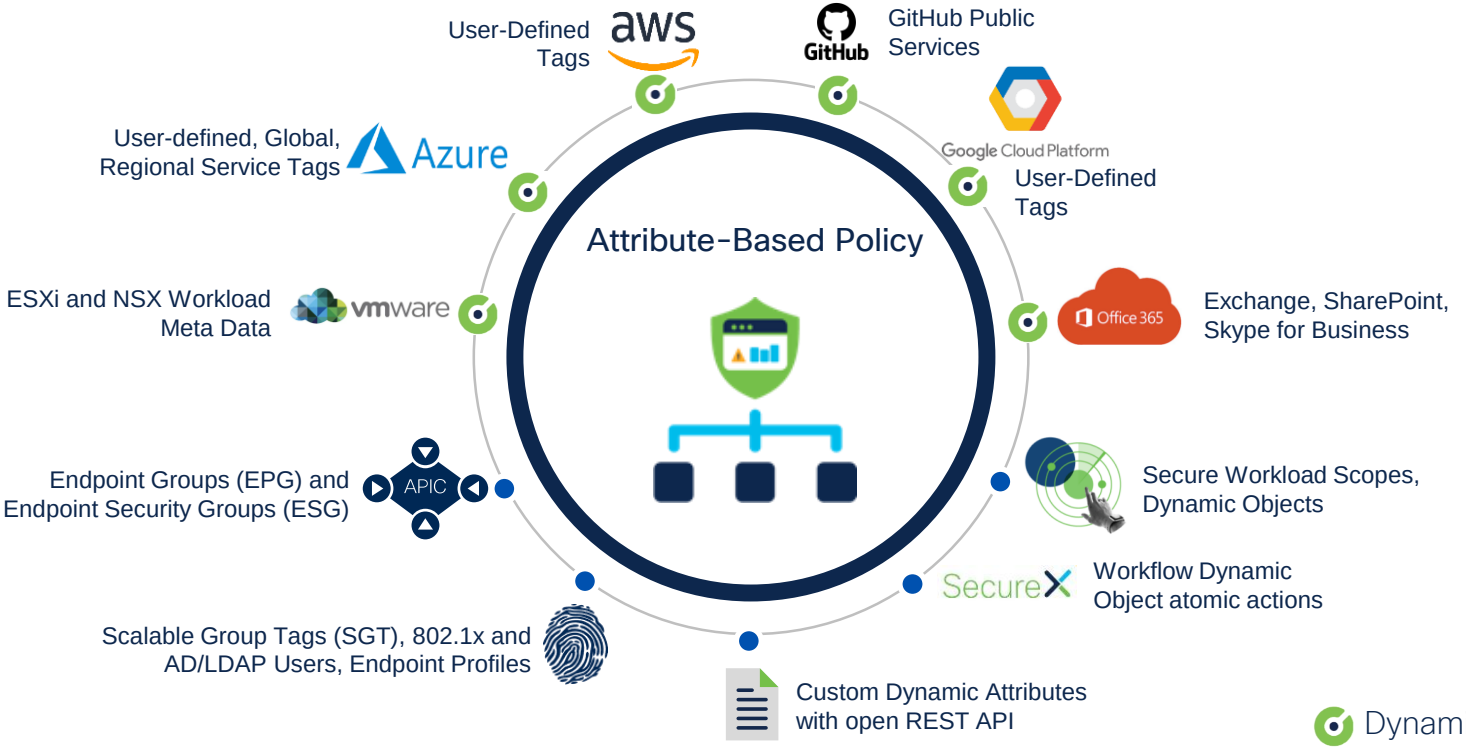
Cisco Multicloud Defense

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



Firewall Policy Abstraction

FTD 7.0+



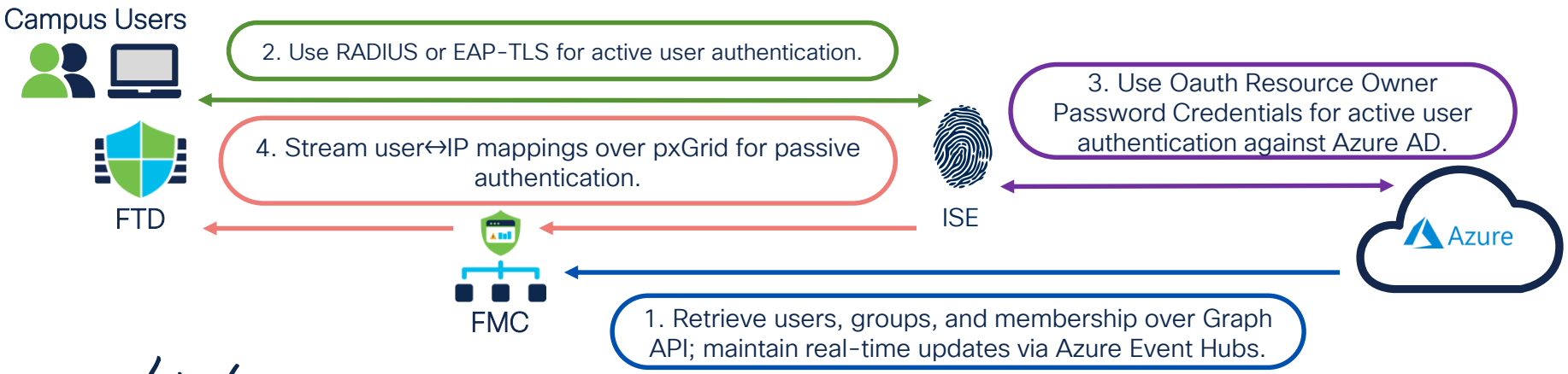
Dynamic Attribute Connector

Firewall Management Center

FTD 7.4

User Identity from Azure AD with ISE

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



FTD 7.6

User Identity Beyond ISE

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

Management

Simplified Access Control Policy (ACP) View

FMC 7.2

Global_Policy

Enter Description

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

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Inheritance Settings | Policy Assignments (1)

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

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

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

Global_Policy

Show Warnings | Analyze Hit Counts | Discard | Save

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

Targeted: 1 device

Total 7 rules | Add Category | Add Rule

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

Simplified ACP Rule Editor

FMC 7.2

Inline rule navigation.

Direct access to all advanced actions.

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

Rule #4 | Allow_Outbound | Allow | Mandatory

Editing Rule **#5. Inbound_Mail** | Mandatory

Select Rule: Select...

Name: Inbound_Mail

Action: Allow

Intrusion Policy: Balanced Security and Con...

Variable Set: Default-Set

File Policy: None

Time Range: None

Comments

Sources — Collapse All | Remove All

ZONE: 1 object — outside

Destinations and Applications — Collapse All | Remove All

NET: 1 object — Mail_Servers

ZONE: 1 object — inside

APP: 2 objects — SMTP, SMTPS

Cancel | Apply

Rule #6 | Inbound_Webapp | Allow | Mandatory

Cluster Health Dashboard

FMC 7.3

Health: richcluster-cluster

View System & Troubleshoot Details ...

Overview | Load Distribution | Performance Dashboard | CCL

Detailed load statistics on per-member basis.

Last 1 hour

2022-10-26 18:44 - 2022-10-26 19:44

Cluster Members

Manage Cluster

10.10.71.215 10.10.71.216 10.10.71.218 10.10.71.223 10.10.71.226 10.10.71.229 10.10.71.231 10.10.71.232

Cluster member status at your fingertips.

10.10.71.234 10.10.71.236 10.10.71.237 10.10.71.238 10.10.71.240 10.10.71.241 10.10.71.243 10.10.71.244

Cluster Overall Performance

CPU		Memory		Input Rate	Output Rate	Active Connections	NAT Translations
Data Plane	Snort	Data Plane	Snort				
1 %	-NA-	19 %	4 %	3.72 Mbps	11.89 Mbps	2.68 K	3.83 K
1 % – 1 %		19 % – 19 %	4 % – 4 %	2.93 Mbps – 3.86 Mbps	9.53 Mbps – 12.12 Mbps	2.61 K – 2.75 K	3.69 K – 3.97 K

Aggregated and minimum/maximum metrics over the selected time period across the entire cluster.

CPU

Data Plane

100 % 75 % 50 % 25 % 0

18:45 18:50 18:55 19:00 19:05 19:10 19:15 19:20 19:25 19:30 19:35 19:40

Memory

Data Plane Avg 19 % Snort Avg 4 % System Avg 13 %

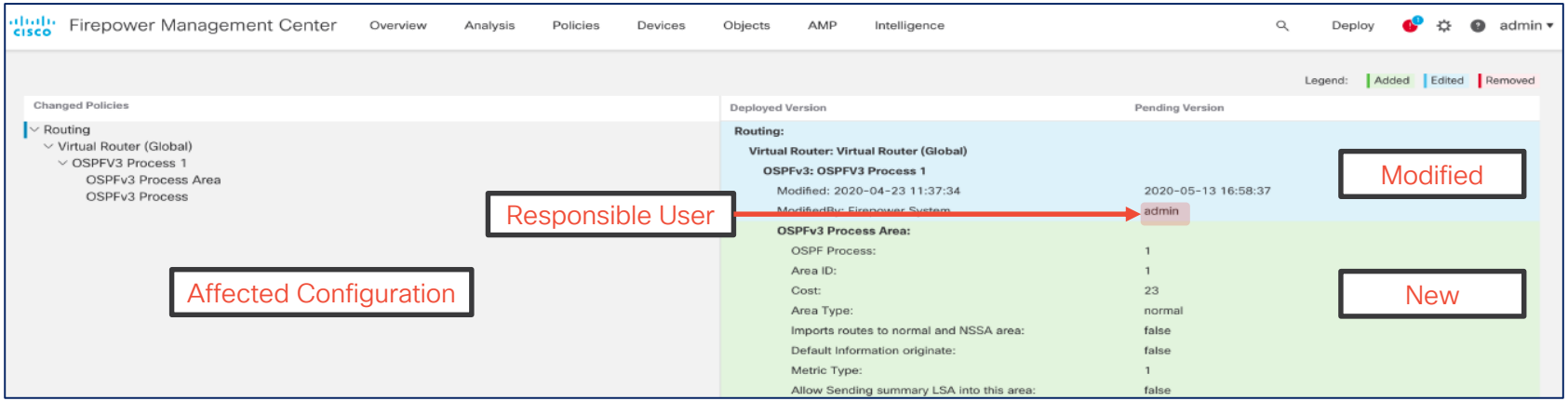
100 % 75 % 50 % 25 % 0

18:45 18:50 18:55 19:00 19:05 19:10 19:15 19:20 19:25 19:30 19:35 19:40

Change Management

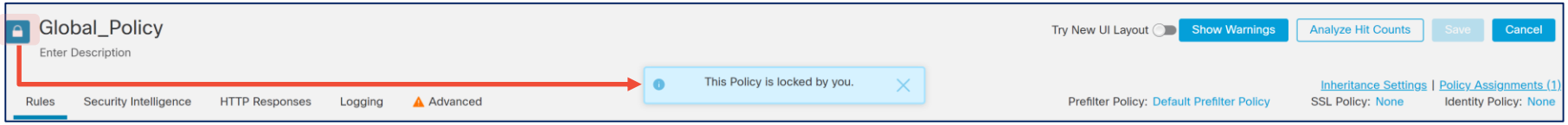
FMC 7.0+

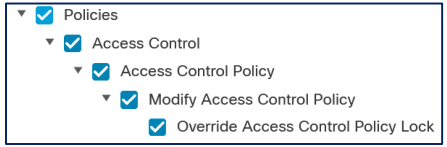
- Selective change deployment and detailed audit transcripts in FMC
  - Individual configuration changes can be filtered and deployed by user
  - Emergency rollback to one of 10 previous configuration versions
  - Separation of Access Rules, IPS, and File policy deployment in FTD 7.4

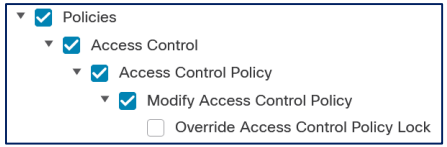


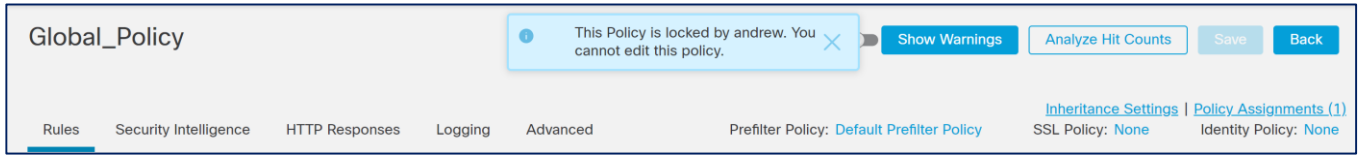
“Shallow” Access Policy Locking

FMC 7.2









FMC 7.4+

Workflow Mode and Change Logging

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


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

VPN Monitoring Dashboard

FMC 7.3

Firewall Management Center
Overview / Dashboards / Remote Access VPN

Overview | Analysis | Policies | Devices | Objects | Integration

Deploy | admin | cisco SECURE

Refresh every 5 minutes | Refresh

Sessions

Select Type: By Device

249 Total Sessions

- FTD-USA (100 / 250)
- FTD-IND (50 / 250)
- FTD-AUS (50 / 250)
- FTD-JPN (47 / 250)
- FTD-ENG (2 / 250)

Active Sessions

Reset

United States
100 Active Sessions

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

Device Identity Certificates

9 Identity Certificates
- 1 certificate expiring in 1 to 30 days
- 2 certificates are expired

View Details

Active Sessions (249)

Select...

User Name	Assigned IP	Public IP	Login Time	Gateway	Country	Client Application	Client OS	Connection Pro...	Group Policy	Actions
user732	192.168.81.22	202.12.127.33	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user744	192.168.81.23	202.12.127.45	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user735	192.168.81.24	202.12.127.36	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user733	192.168.81.25	202.12.127.34	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user739	192.168.81.26	202.12.127.40	2022-11-15 1...	FTD-USA	USA					...
user778	192.168.81.27	202.12.127.79	2022-11-15 1...	FTD-USA	USA					...
user752	192.168.81.28	202.12.127.53	2022-11-15 1...	FTD-USA	USA					...

Headend session utilization heatmap to avoid oversubscription.

Group active sessions by device, tunnel type, Client version, OS, or profile.

Never miss headend identity certificate expiration again!

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

Policy Analysis

FMC 7.4

Policy Analysis

Rule Warnings and Errors (0) | Policy Warnings (0) | Conflicts (3)

Total Conflicts: 3 | Shadowed: 1 | Object Overlap: 1 | Redundant: 1

Shadowed	3	Allow_Inside_DB_Acce...	This rule's match criteria are a subset of the criteria for rule Allow_Outbound_Internet. This rule will never be matched. Please evaluate the intended behavior and adjust the rule's location, match criteria, and action as needed, or you can delete the rule.
	2	Allow_Outbound_Inter...	
Object Overlap	4	Allow_Exec_Workstati...	FULL OVERLAPS (1): Source Network Overlaps: 192.168.1.5 fully overlaps with - [192.168.1.1-192.168.1.5]
	4	Allow_Exec_Workstati...	
Redundant	6	Allow_Outbound_Partn...	This rule is redundant to Allow_Outbound_Partner_HTTPS-11. You can delete this rule.
	8	Allow_Outbound_Partn...	

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

Close

AI Interactive Assistant

FMC 7.6

Improve visibility

+ Reduce effort to learn about the policies you have deployed

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

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

Speed up troubleshooting

+ Use knowledge base to autocomplete troubleshooting steps

"Have I enabled malware analysis on my access control policy?"

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

Act faster

+ Take actions to create new rules or block existing ones

"Remove duplicate rules."

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

FMC View: AI Interactive Assistant

FMC 7.6

cdFMC | Search | Alexander Business Corp, Inc

← Return to Access Control Policy

ACP - Production

Analyze Rule Heartbeat | Reset | Save

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

Targeted: 3 device

Search | Total 9 rules | Add Category | Add Rule | Ask AI

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

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

Ask Cisco AI

R: Show me access policies related to the user group Imn-vendor

Cisco Assistant 8:12 AM

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

- 4 rules are about Sensitive Data
- 4 rules are about Internet Access
- 2 rules are about Internal Application Access

Regenerate

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

© 2022 Cisco Systems, Inc. | Privacy policy | Terms of service

Secure Workload

Secure Workload as Policy Engine

Flow Telemetry Ingestion

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

Dependency Mapping

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

Policy Experiments

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

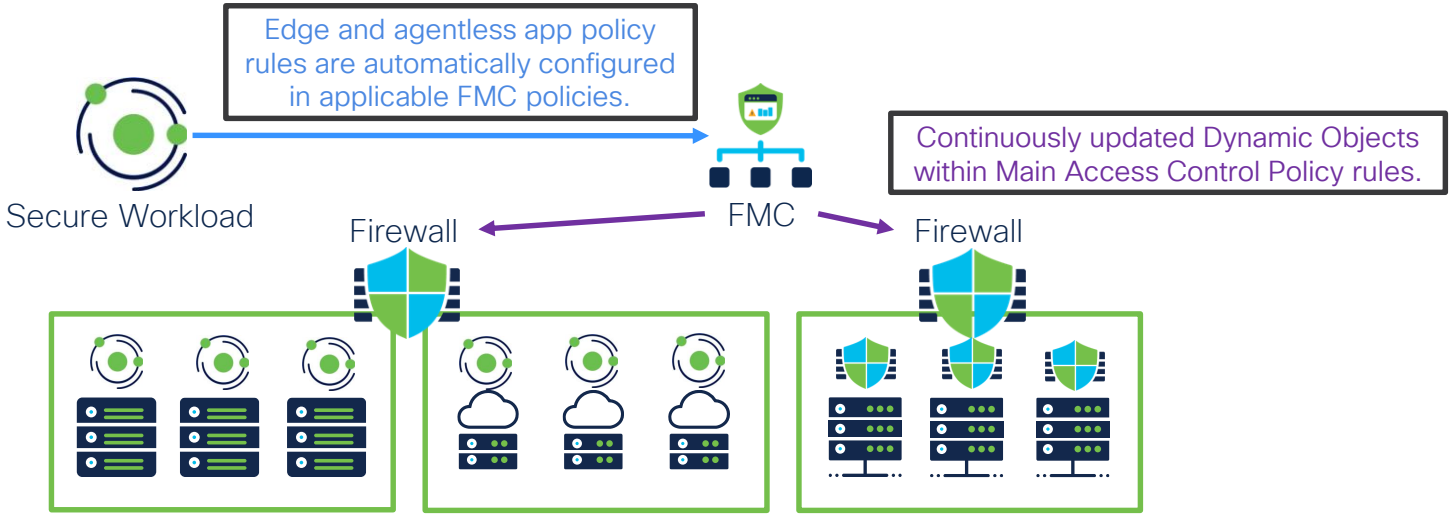
Network Security (NetSecOps)

Secure Firewall + Secure Workload + Distributed Firewall

Workload 3.6+

Secure Workload Policy Extension to Firewall

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



Secure Workload Policy Orchestration in FMC

Workload 3.6

Firepower Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Devices | Objects | AMP | Deploy | 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

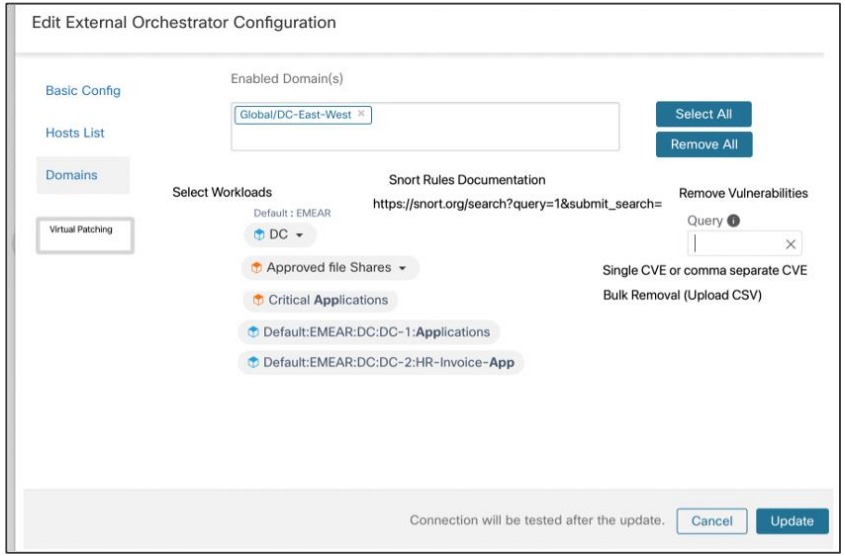
#	Name	Source Networks	Dest Networks	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action	
Mandatory - East-West-Policy (1-11)								
1	Block log4j	Any	log4j-ubuntu	Any	Any	Any	Block	0
2	Workload_golden_1	Any	Any	Any	WorkloadObj_collector	Any	Allow	1
3	Workload_golden_2	Any	Any	TCP (6):5640	Any	WorkloadObj_collector	Allow	1
4	Workload_golden_3	Any	Any	Any	WorkloadObj_collector	Any	Allow	1
5	Workload_golden_4	Any	Any	TCP (6):5660	Any	WorkloadObj_collector	Allow	1
6	Workload_golden_5	Any	Any	Any	WorkloadObj_wss	Any	Allow	1
7	Workload_golden_6	Any	Any	TCP (6):443	Any	WorkloadObj_wss	Allow	1
8	Workload_7	Any	Any	TCP (6)	WorkloadObj_Production_S	WorkloadObj_Developmen	Block	1
9	Workload_8	Any	Any	TCP (6)	WorkloadObj_Vulnerable_V	WorkloadObj_Root_Interne	Block	1
10	Workload_9	Any	Any	TCP (6)	WorkloadObj_Administrato	WorkloadObj_Root_CSW_S	Allow	1

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

Workload 3.8

Application Virtual Patching

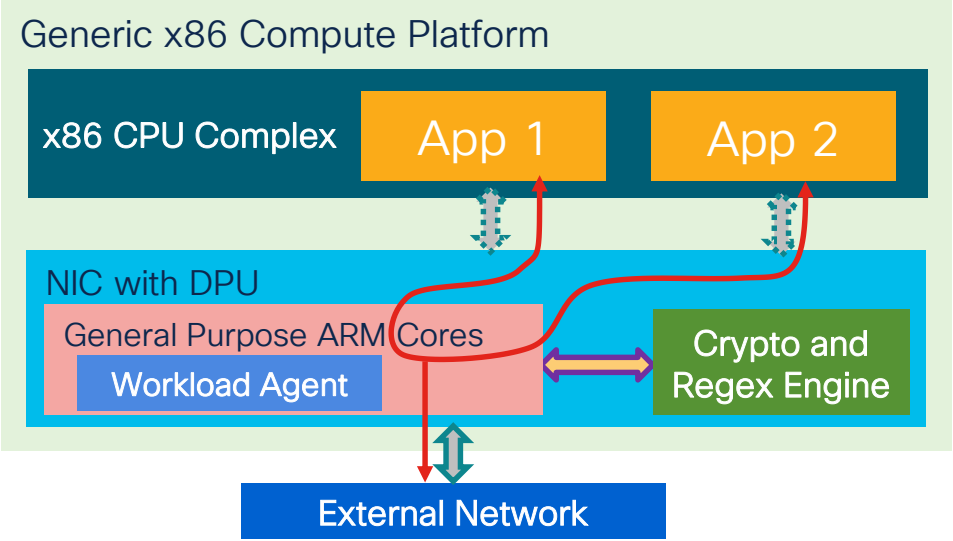
- Tailoring FTD IPS policy to specific apps improves performance
- Workload will import vulnerability information (CVE) into FMC
  - Leverage Network Discovery Policy
  - Update specific Host Profiles
  - Improve Firepower Recommendations



Workload 3.9

Workload Segmentation with Nvidia DPU

- Nvidia DPU adds advanced micro segmentation in hybrid cloud
  - Expanded inter-application visibility with a resident Workload agent
  - Future inline inspection and crypto acceleration capabilities



Cisco Hypershield

Near Future

App Dependency Mapping

Policy auto-reasoning

Auto-Compensating Controls

Management (Cisco Defense Orchestrator + Workload)

Every Network Port is an Advanced Firewall

In-Kernel with eBPF

DPU Server

DPU Smart Switch

Firewall Threat Defense

Cloud Agility

Dual Data Plane Architecture

Self-Qualifying Upgrades

Policy Modeling

Availability and Scalability

In-Kernel Application Runtime Controls

App1

App2

Web

App Runtime Fingerprinting

Auto-compensating controls

Hyper-distributed Architecture

Every physical, virtual, and cloud-native network interface becomes an advanced firewall. This is enabled by inline insertion with eBPF at host OS kernel level and by DPU-equipped servers and top-of-rack switches in the future.

Cloud Agility for Threat Protection

Dual data plane architecture enables self-qualifying upgrades, real-time policy modeling, and auto-scale-out use cases. It evolves from Workload agent visibility to advanced and flexible inline threat prevention.

AI-assisted Adaptive Runtime Policy

Expands on Workload visibility and policy modeling capabilities with runtime application fingerprinting and auto-compensating controls. Extends human language into security policy with generative AI capabilities.

Conclusion

Cisco Security Beta Programs

Influence product design
Design research participants shape the look, feel, & functionality of new product features and offerings

Attention to Feedback
Beta customer bugs and enhancements receive high visibility & priority

Top notch communication
Private conference calls with product team

Training
Customers receive early training & experience with new features

Customer Support
Feature experts will be on-hand & responsive to your issues

Sign Up Now: https://cs.co/security-beta

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you