

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





Keeping Up on Network Security with Cisco Secure Firewall

Andrew Ossipov
Distinguished Engineer, Portfolio CTO
BRKSEC-2236

CISCO *Live!*

#CiscoLiveAPJC



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 November 15, 2024.



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



Agenda



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



Your Speaker

Andrew Ossipov

aeo@cisco.com

Distinguished Engineer

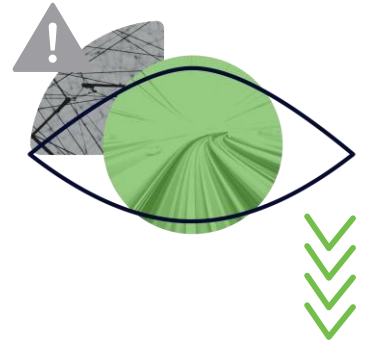
Portfolio CTO for Cloud and Network Security

Firewall Architecture, Threat Visibility, Hybrid Cloud

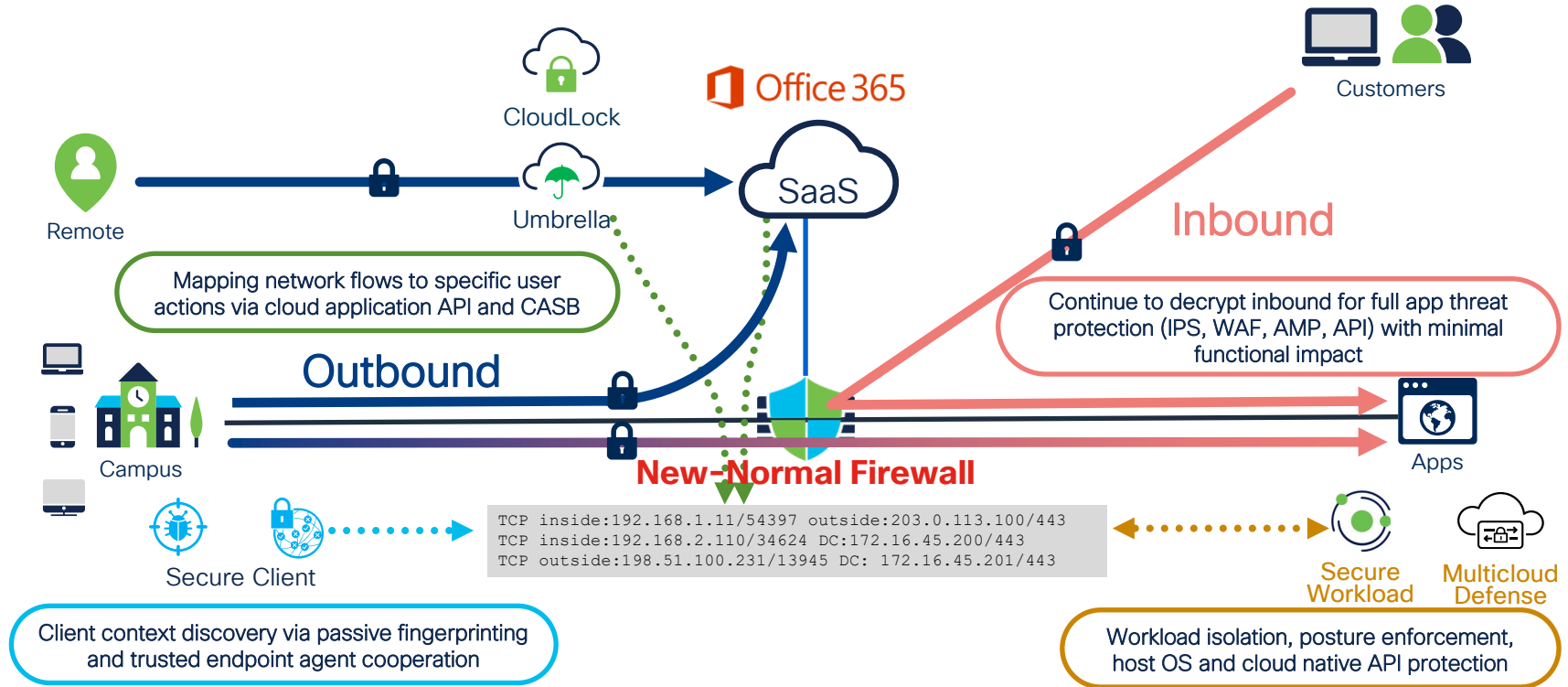


Traditional “Next-Gen” Firewall is Struggling

- Pervasive traffic encryption against deep inspection
 - TLS 1.3, DNS-over-HTTPS, QUIC (HTTP/3)
- New protocols with single-flow throughput constraints
 - Stream multiplexing in HTTP/2 and QUIC
- Roaming endpoints with multiple network interfaces
 - App connection abstraction with Multipath TCP and QUIC
- Evasive network attachment point in hybrid cloud
 - Cloud native, public cloud, serverless

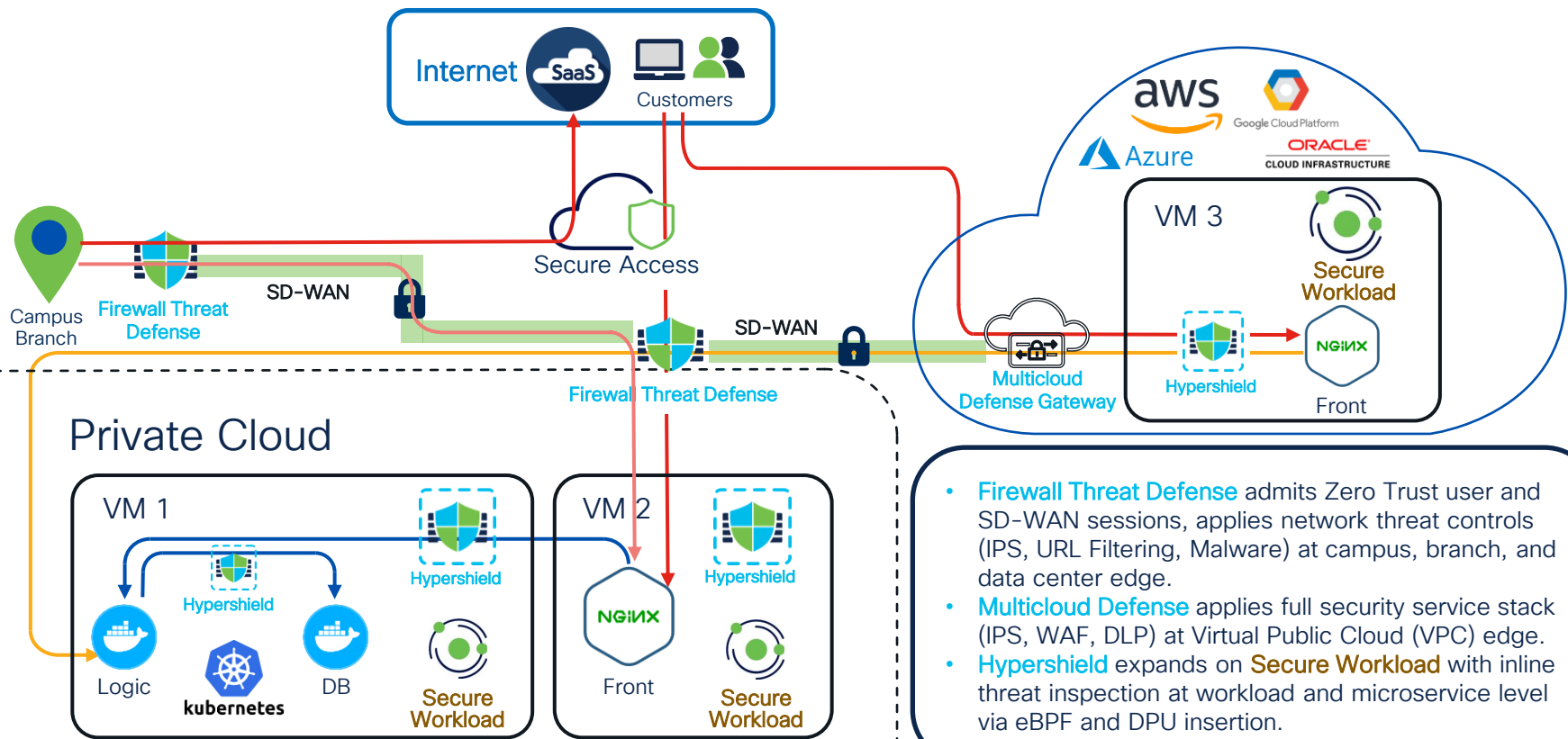


Secure Firewall: Inspect, Infer, and Cooperate



Firewall Vision: Network, Workload, and Cloud

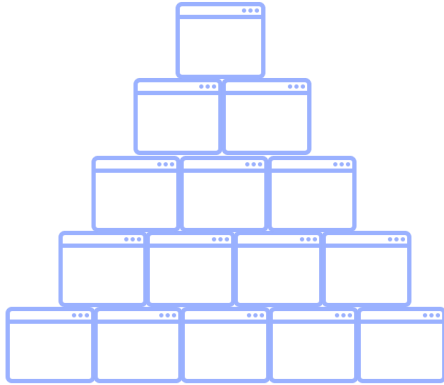
Cisco Security Cloud Control abstracts end-to-end policy intent from enforcement point specific configuration.



- **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.

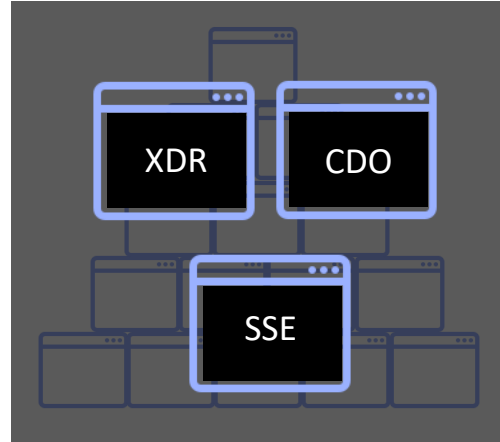
Security Cloud Control

Historically



20+ Product Consoles

Right Now



Platform Experiences have formed

defenseorchestrator.com

xdr.cisco.com

sse.cisco.com

Emerging



security.cisco.com

Security Cloud Control Outcomes



One Experience

- Common User experience across products
- Centralized onboarding and provisioning
- End-to-end product interactions (e.g. Hybrid ZTNA)



Simplified Tenancy

- Cross-product trust – no manual integrations
- Extends to MSPs who don't want to provision and manage individual products



Role-Based Access

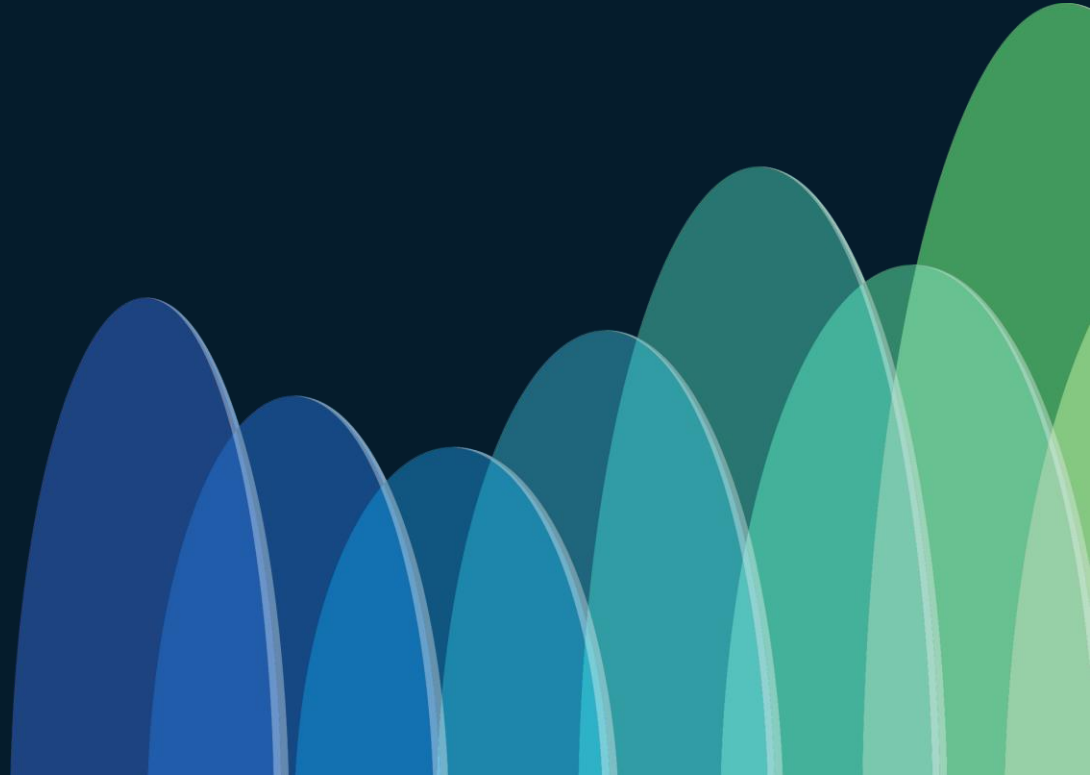
- Configure permissions once per user
- Manage access control/compliance auditing centrally, reduce potential for misconfiguration
- Take advantage of IDP integration and group mapping



Shared Services

- Portfolio convergence around identity and subscription concepts
- Enables common frameworks for hybrid deployment (Policy, network, posture)
- Common services (search, notifications, AI) extend across all products

Platforms



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 **or** 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/**50**GE

1RU



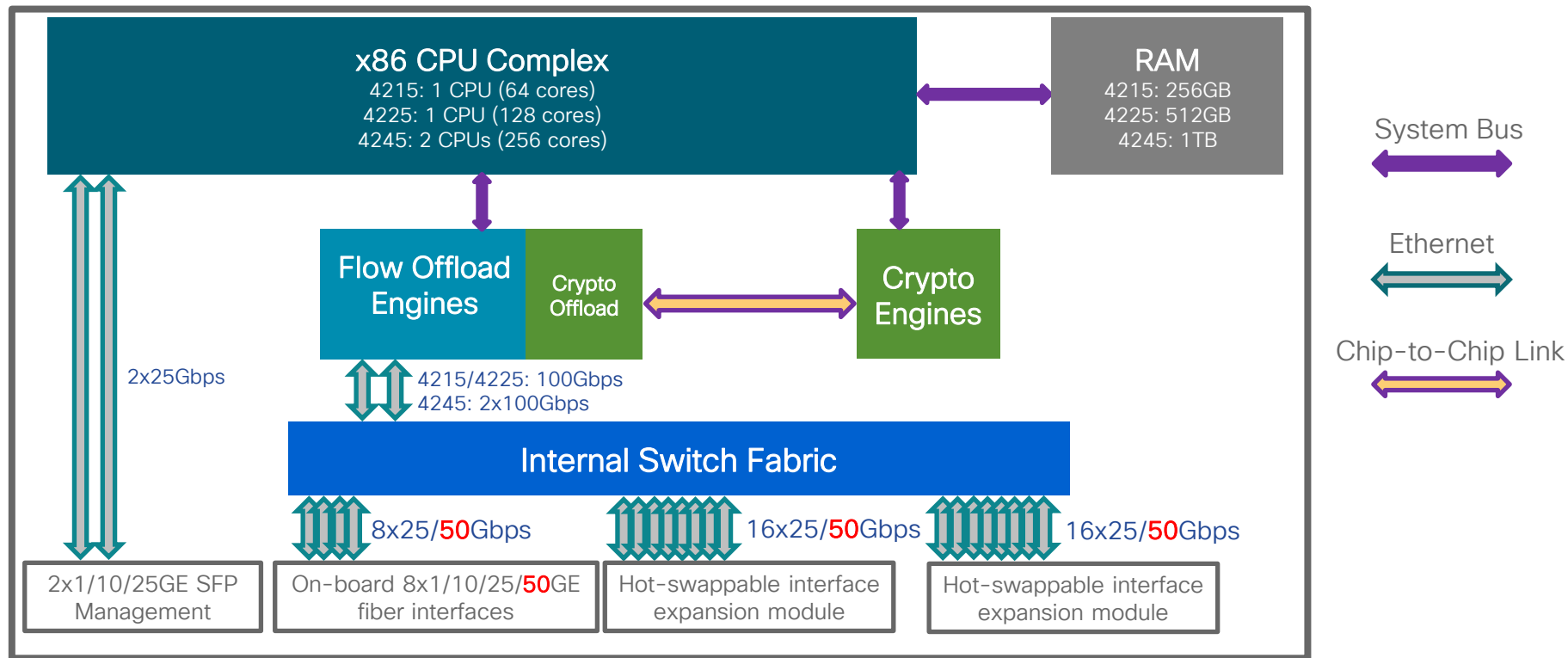
NVMe Drives

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

Expansion Network Modules

- Standard: 8x1/10GE, 8x1/10/25/**50**GE, 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



Multi-Instance Mode

- Full migration and configuration support in FMC for 3100 and 4200

Multi-instance Mode Conversion ×

1 Selected Devices — 2 Readiness Check — 3 Convert to Multi-instance

1 Multi-instance convergence process will take 15-20 minutes for completion. To get the latest status of your device, check the task notifications.

Search devices

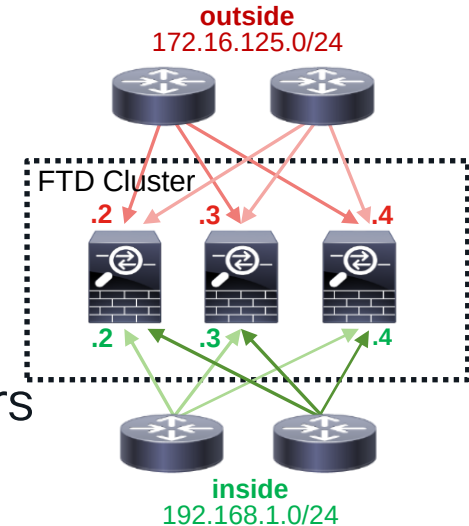
☐	Device Name	IP	Version	Model	Status	Action
☐	10.10.5.24	10.10.5.24	7.4.0	Firewall 3120 Threat Defence	In Progress...(15 minutes)	

- Expanded instance count with 4200 appliances

Platform	Maximum Instance Count
Secure Firewall 4215	10
Secure Firewall 4225	15
Secure Firewall 4245	34

Individual Mode Clustering on 3100/4200

- 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
- Powerful design option for multi-site data centers



Secure Firewall 1200 Overview

Appliance-Mode Security Platform for FTD or ASA Application

- Desktop (1210CE/CP and 1220CX) or Rack-Mount (1230, 1240, and 1250)
- Fully integrated System-on-a Chip (SOC) for crypto acceleration
- No multi-instance or Clustering support, Failover only

SFP Data Interfaces

- 1220CX: 2x1GE/10GE SFP+
- 1230 and 1240: 4x1GE/10GE SFP+
- 1250: 4x1GE/10GE (future 2x25GE)

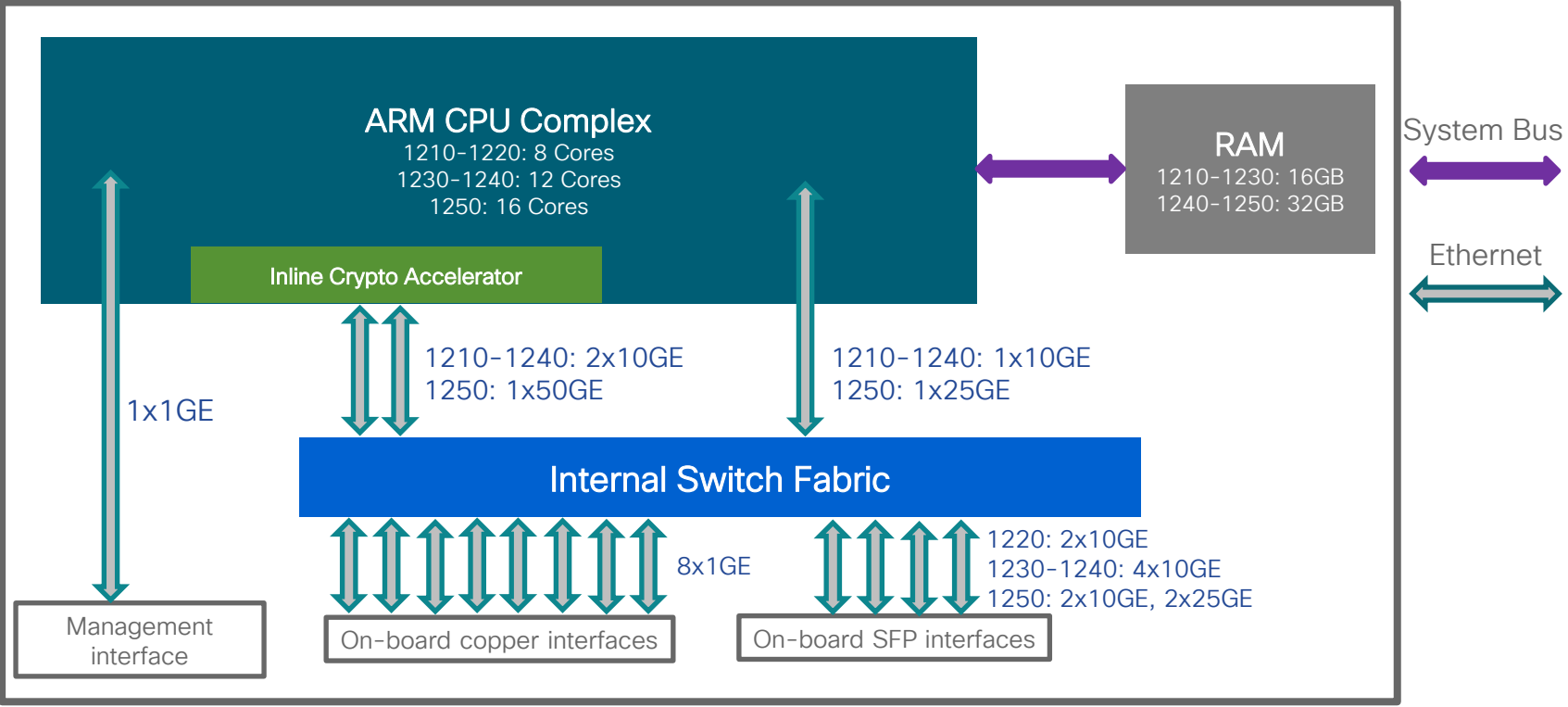
1RU



Copper Data Interfaces

- 1210-1240: 8x1GE (4xPoE on 1210CP only)
- 1250: 8x1GE/2.5GE

Secure Firewall 1200 Architecture



Secure Firewall 1200 Performance



	1210CE/CP	1220CX	1230	1240	1250
FTD AVC+IPS HTTP 450B Avg Packet	1.7Gbps	2.7Gbps	3.6Gbps	4.3Gbps	5.5Gbps
ASA TCP 450B Avg Packet	8Gbps	18Gbps	20Gbps	20Gbps	20Gbps
IPsec VPN UDP 450B Avg Packet	2Gbps	6.7Gbps	6.9Gbps	7Gbps	7.5Gbps

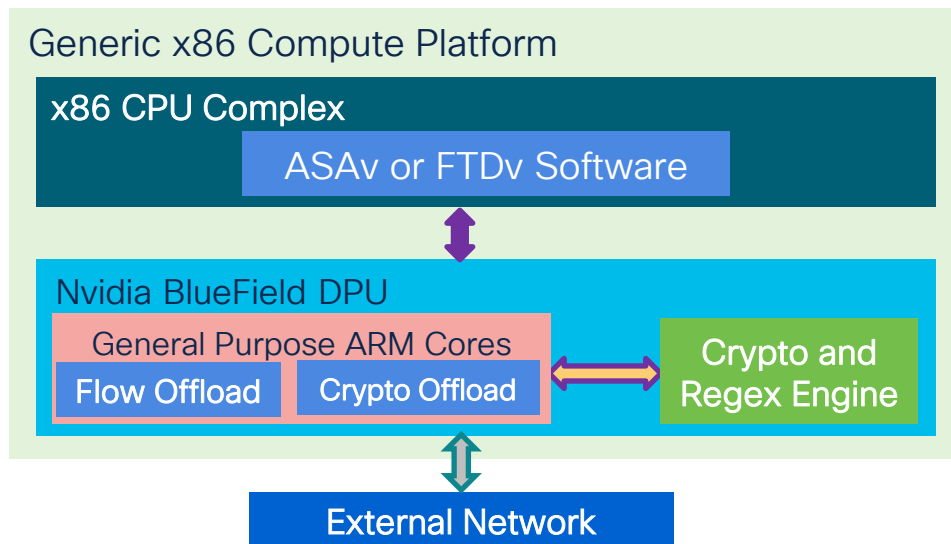
All performance estimates are subject to change in public release.

Virtual Firewall on Nvidia BlueField DPU

- Data Processing Unit (DPU) is a next-generation x86 NIC
 - Inline hardware acceleration for broad packet processing functionality
 - Perfect opportunity to accelerate and scale firewall in hybrid data centers

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

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

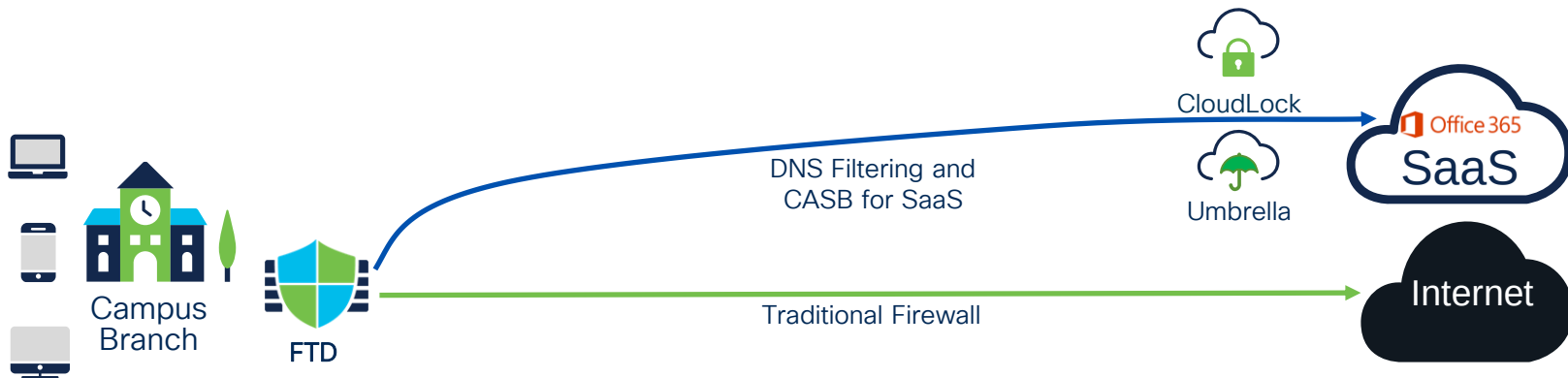


Threat Protection

Enhance Firewall with Umbrella Cloud Security

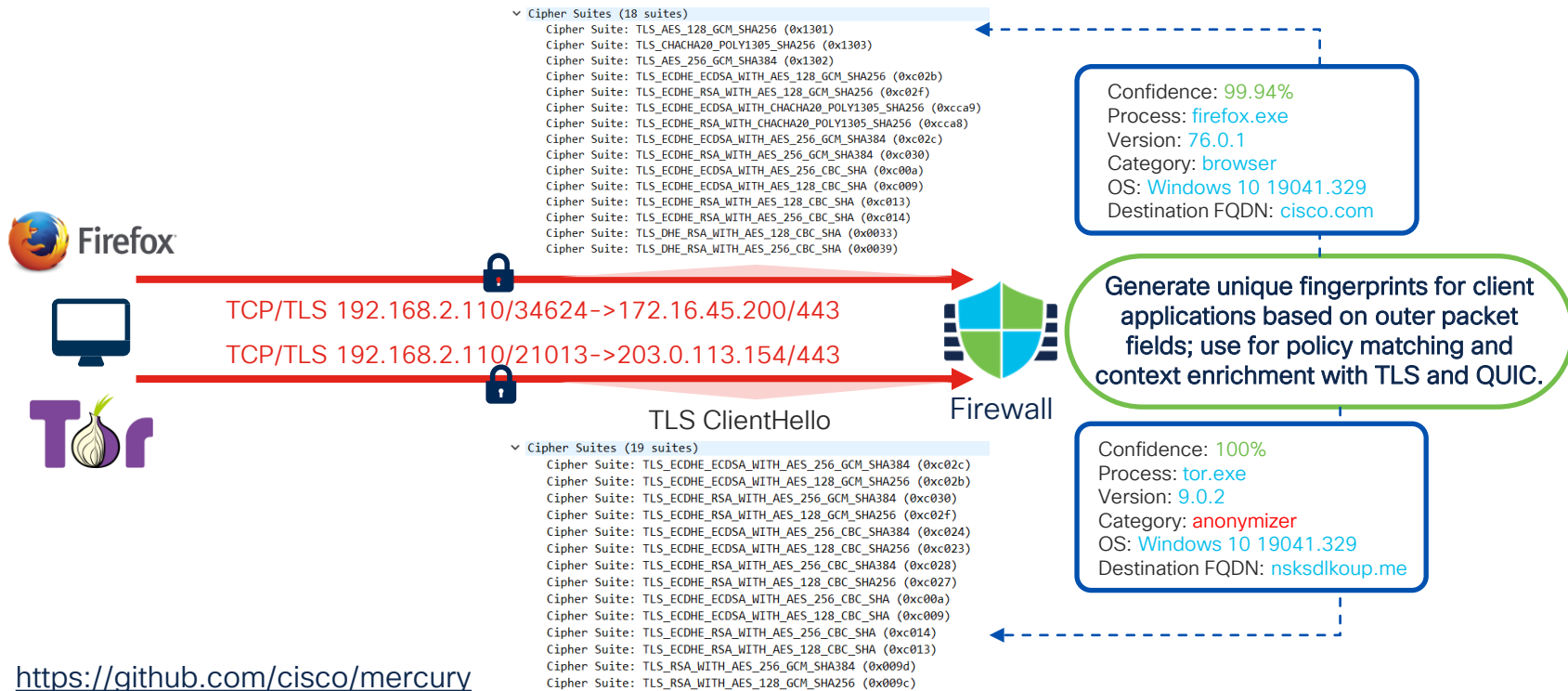
FTD
7.2+

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



Encrypted Visibility Engine (EVE)

TLS ClientHello



EVE-enriched Unified Events

FTD
7.1

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

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ alexx | cisco 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 Unr)	3 (Port unreachable)	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

Very Low

Low

Medium

High

Very High

Block

Revert to Defaults

Cancel

OK

Inference-based AppID enrichment.

Detailed fingerprint data for third-party use.

Connection filtering based on malware confidence scores.

Simplified TLS Decryption Policy

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

Create Decryption Policy

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

Name*
Decrypt DMZ Apps to Internet

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

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

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

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

FMC_Self Associated: 2 Networks, 1 Port

[See how to configure](#)

Cancel Save

QUIC Decryption and Inspection

- QUIC (HTTP/3) uses UDP with modified TLS 1.3 for encryption



- All firewall vendors require downgrade to HTTP/2 for inspection
- Some browsers ignore Enterprise CA in local trust store for decryption
- Encrypted Visibility Engine supported QUIC apps since **FTD 7.3**
- Full QUIC decryption and inspection is supported in **FTD 7.6**

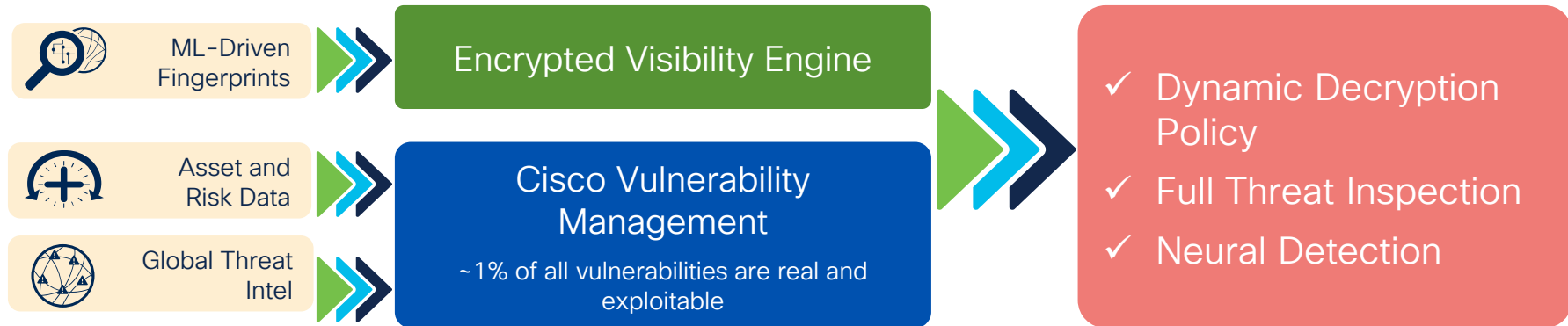
SnortML: Neural Exploit Detector

- 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
- SnortML 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

Selective Traffic Decryption



- Effective threat protection requires some traffic to be decrypted
 - Decrypting everything will degrade performance even with fast hardware
 - Difficult to predict what to decrypt with static policies
- Goal: classify 90% traffic as benign, inspect remaining 10%



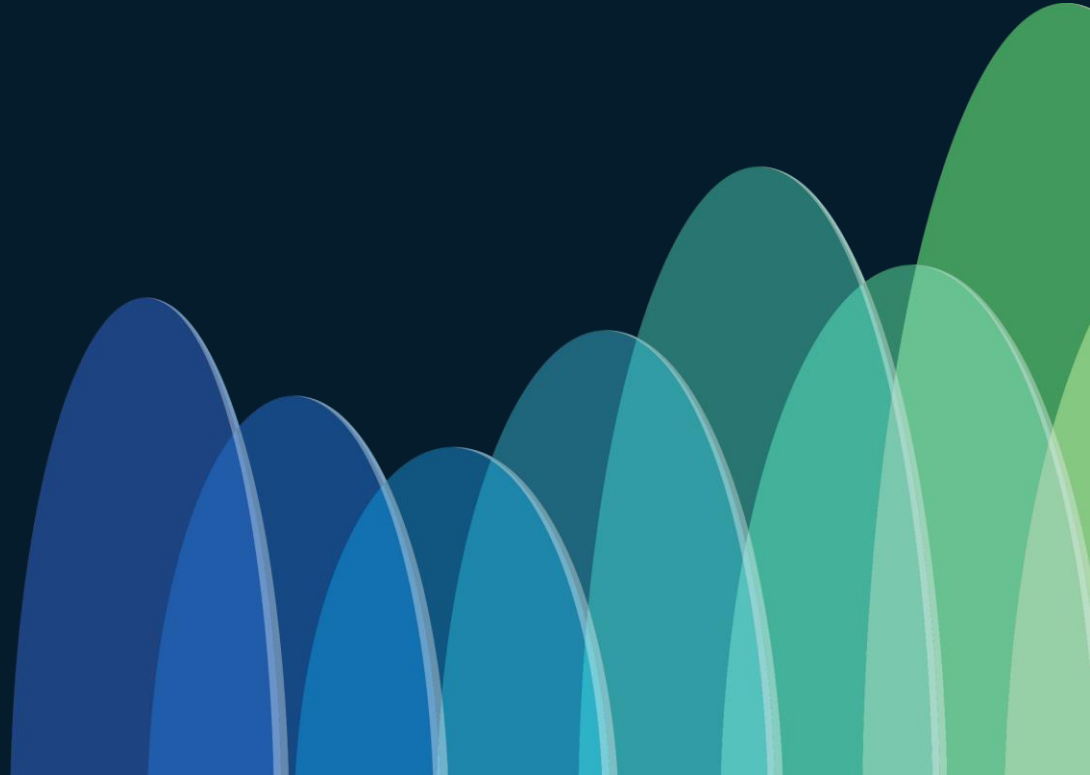
Intelligent Decryption Bypass

☒ **Bypass decryption for very low-risk connections** New

Bypass decryption for very low-risk clients connecting to trusted servers.

Note: **The access control policy associated with this decryption policy must have the Encrypted Visibility Engine (EVE) enabled. The device to which the policy is deployed must run version 7.7 or later and have a valid IPS license.**

Connectivity



Application-Aware Policy Routing



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

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

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

Ingress Interfaces	Match criteria and forward action	
inside	<p>If traffic matches the Access List WebEx_Direct_Internet_Access</p> <p>SaaS application aware first packet match.</p> <p>Send and load balance it through #0 ISP1 #0 ISP2</p> <p>If above link fails, Send through #1 ISP-Backup</p> <p>Flexible egress interface selection policy, including ECMP over cleartext or VPN tunnels.</p>	 

Path Monitoring and Quality-Based Routing

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

Add Forwarding Actions

Match ACL:* Youtube +

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter ⓘ

Available Interfaces

Search by interface name 🔍

Interface
Inside +
Outside +

No interfaces selected

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

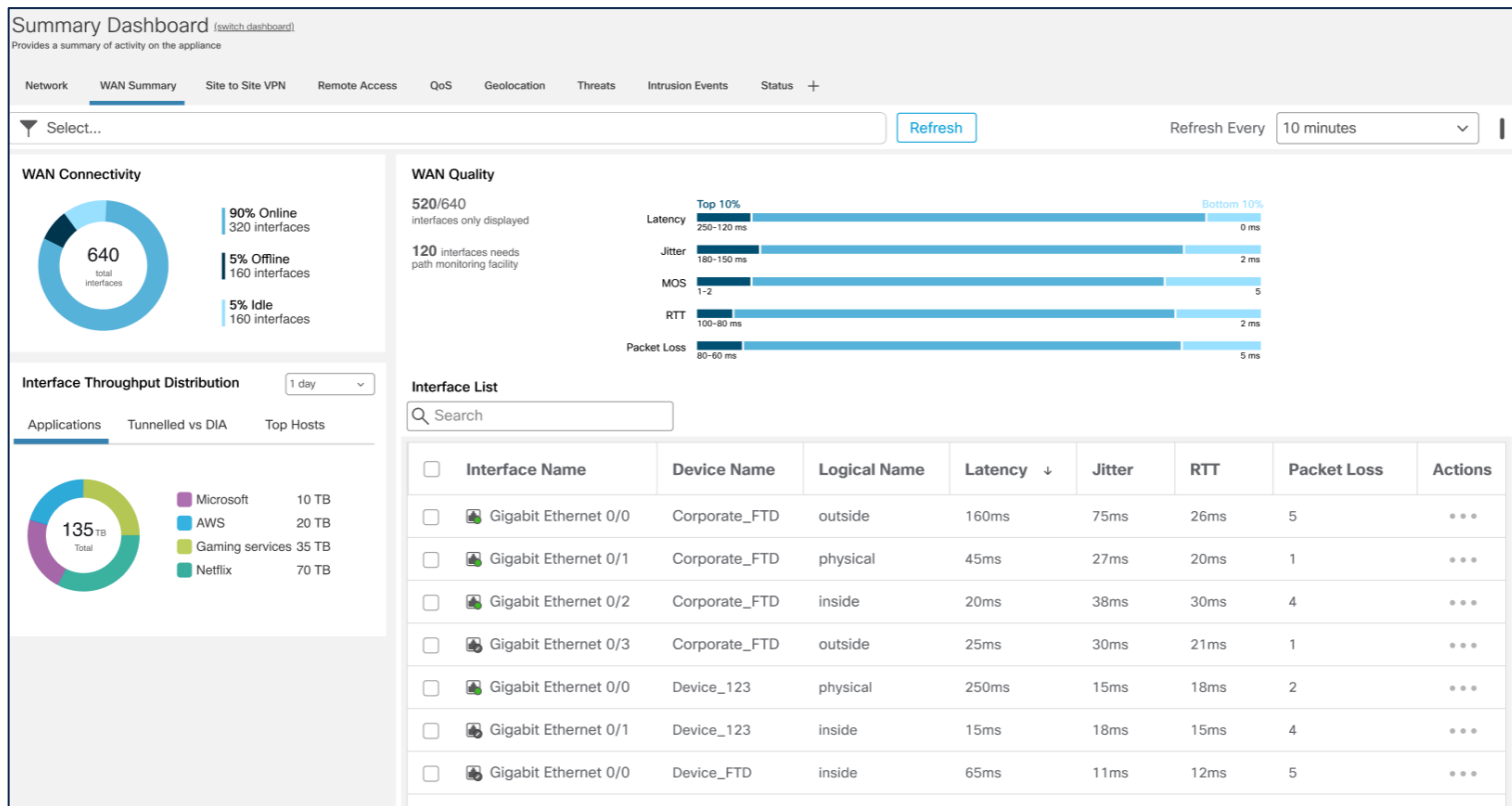
RTT: The Round-trip Time (RTT) is the duration, measured in milliseconds, from when a monitoring node sends an ICMP echo request to when it receives an ICMP reply from a remote node.

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

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

SD-WAN Monitoring Dashboard

FTD
7.4



Simplified SD-WAN Setup Wizard

- Assisted creation of SD-WAN Hub-and-Spoke topology
 - Single or multiple interconnected hubs in Regions
 - Simplified Spoke addition without impacting existing devices
- Multiple configuration elements are automatically generated
 - Dynamic VTI interfaces and Security Zone assignment on Hub
 - Static VTI interfaces on Spokes with interface redundancy
 - Preshared tunnel keys and IKE/IPsec profiles
 - BGP overlay for Spoke-to-Hub and Hub-to-Hub connectivity

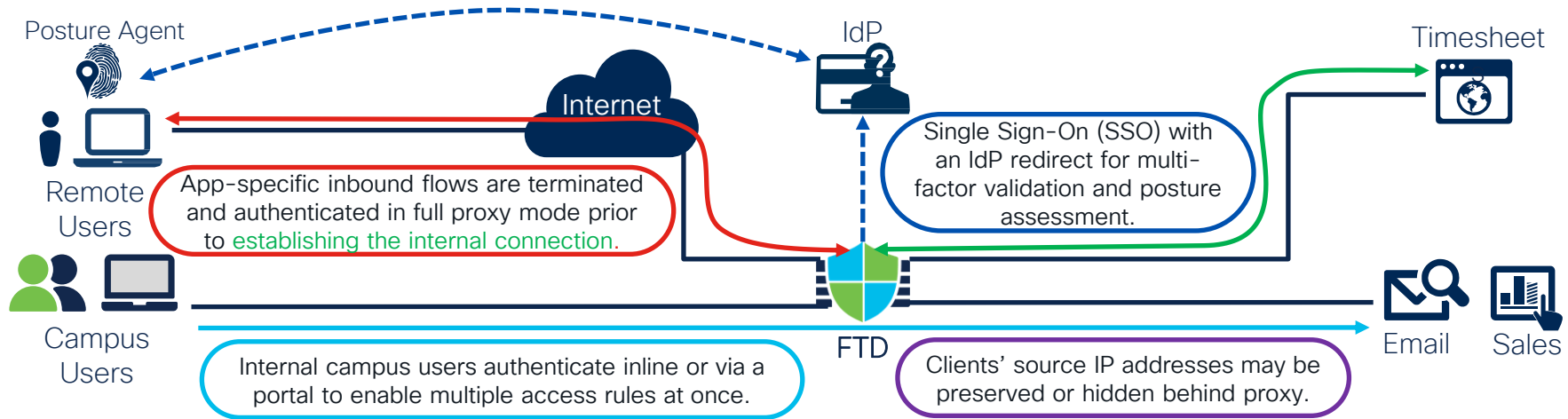
Device Configuration Templates

- Reusable configuration templates for bulk device provisioning
 - Supported with 1x00, 2100, and 3100 appliances on **FTD 7.4** and above
- Device Templates have shared and device-specific configurations
 - Shared: Access Policies, NAT, Platform Settings, Health Policy, QoS, VPN
 - Device: Interfaces, Static and Dynamic Routing, PBR
 - Logical-to-physical interface mapping and Variables for abstraction

Template Name	Domain	Variables ⓘ	Access Control Policy*	Model Interface Mapping ⓘ	Last edited
Retail Branch Template A1 Routed 0 Associated Devices	Sub-Global	3 variable objects 4 Network objects overrides	Branch Access Policy	● Firepower NGFW 2100 ● Firepower NGFW 2100, +3 more	10:30:23 12/21/2022

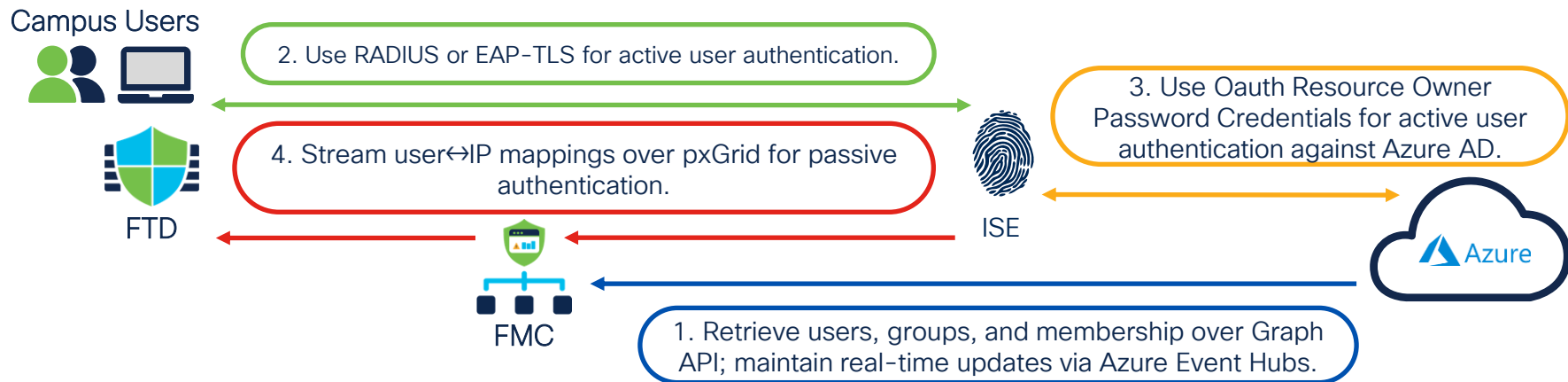
Clientless Zero Trust App Access (ZTAA)

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



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



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 Identity Agent
 - Support all private Active Directory and LDAP deployments
 - Simplified feature set without full ISE or ISE-PIC integration

Hybrid Zero Trust Network Access (ZTNA)

2. **Secure Client** creates a control connection to **Secure Access**. It is used to authenticate and authorize application access, and select the appropriate edge device based on policy or proximity.

Remote User



Secure Client

3. Per-application tunnels to public apps or private apps requiring advanced inspection features (e.g. DLP) go through **Secure Access** and **App Connectors**.

4. Eligible per-application tunnels to private apps are automatically directed to closest edge **Firewall Threat Defense** instance for full threat inspection.

Secure Access

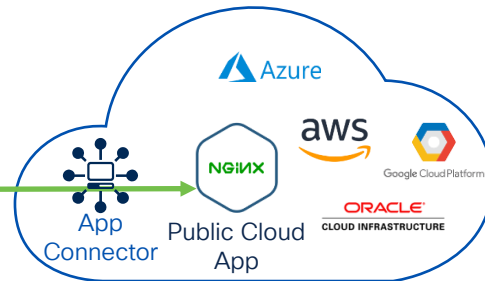
1. **Secure Access** provisions private Firewall instances with appropriate private application access policies.

Firewall Threat Defense

Firewall Management Center

Private Cloud App

Private Cloud



Management

FMC 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 content

```
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":{"oldValue":"","newValue":"00000000-0000-0ed3-0000-
008589935118"},"parentUUID":{"oldValue":"","newValue":"5e3fec7f-00a0-45fb-ac29-
207b3d2af415"},"valuesDeletedList":[],"valuesAddedList":[],"valuesUpdatedList":[{"oldValue":"","newValue":"2023-01-09
17:01:32"},"fieldName":{"oldValue":"","newValue":"secure-sip-
port"},"fieldName":{"oldValue":"","newValue":"Port"},"fieldName":{"oldValue":"","newValue":"Type"},"fieldName":{"oldValue":"","newValue":""},
{"oldValue":"","newValue":"TCP"},"fieldName":{"oldValue":"","newValue":"5061"},
{"oldValue":"","newValue":"Port"},"fieldName":{"oldValue":"","newValue":"false"},"fieldName":{"oldValue":"","newValue":"AllowOverrides"}],
"referencesAddedList":[],"referencesDeletedList":[],"parentHierarchyList":[],"impactedDeviceList":[],"entityType":{"oldValue":"","newValue":"ServiceObject"},"entityName":{"oldValue":"","newValue":"secure-sip-port"},"parentUUID":"5e3fec7f-00a0-45fb-ac29-207b3d2af415","isGrouped":false}]
```

Policy Analysis

Policy Analysis

Rule Warnings and Errors (0)

Policy Warnings (0)

Conflicts (3)

Total Conflicts: 3

Shadowed: 1

Object Overlap: 1

Redundant: 1

Shadowed

3

Allow_Inside_DB_Acce...

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

2

Allow_Outbound_Inter...

Object Overlap

4

Allow_Exec_Workstati...

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

4

Allow_Exec_Workstati...

Redundant

6

Allow_Outbound_Partn...

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

8

Allow_Outbound_Partn...

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

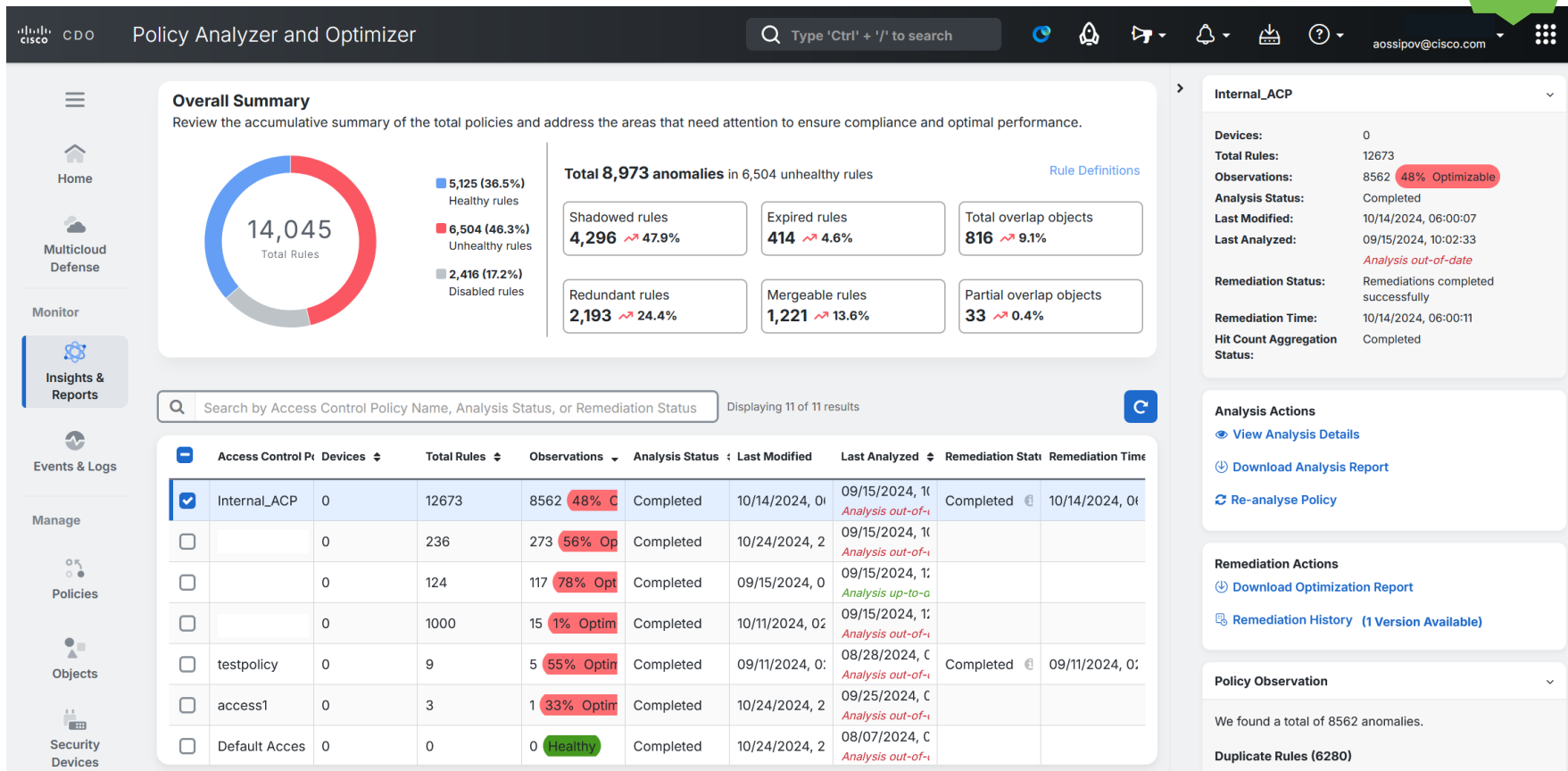
Close

Policy Analyzer and Optimizer

- Provided in CDO for Cloud-Delivered and private onboarded FMC
- Expanded set of rule conflict and anomaly detection
 - Partially overlapping (Shadowed) and fully Redundant objects and rules
 - Expired time-based and unused (by Hitcount) rules
 - Identify mergeable rules
- All conflicts allow for user-supervised automated remediation
 - Remove fully redundant objects and rules
 - Remove unused and expired rules
 - Merge similar adjacent rules into one

Policy Analyzer and Optimizer Dashboard

FMC
7.6+



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.”

CISCO *Live!*

FMC View: AI Interactive Assistant

FMC
7.6

The screenshot displays the Cisco FMC 7.6 user interface. At the top, the navigation bar includes the Cisco logo, 'cdFMC', a search bar, and user information for 'Alexander Business Corp, Inc'. The main content area is titled 'ACP - Production' and shows a breadcrumb trail: Packets > Prefilter Rules > Decryption > Security Intelligence > Identity > Access Control > More. A table lists access control rules with columns for Name, Action, Source (Zones, Networks, Ports, Dynamic Attributes), and Destination (Zones, Networks, Ports, Applications). The table shows four rules: 1 External (Block), 2 Internal (Allow), 3 Block Malwares (Block), and 4 Block Torrent (Block). A 'Default Action' dropdown is set to 'Intrusion Prevention: Balanced Security and Con...'. An 'Ask Cisco AI' overlay is open on the right, displaying a query: 'Show me access policies related to the user group imm-vendor'. The assistant responds with a summary of 3 Access Control Policies and 10 Access Control Rules, categorized by Sensitive Data (4 rules), Internet Access (4 rules), and Internal Application Access (2 rules). A 'Regenerate' button and a text input field for further queries are at the bottom of the overlay.

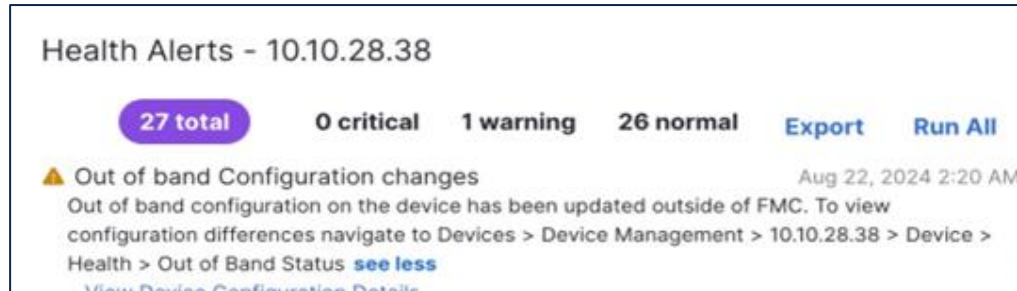
© 2022 Cisco Systems, Inc.

Privacy policy Terms of service

Local Configuration Changes



- Limited Command Line Interface for FTD configuration changes
 - Always available, but intended for FMC-down emergencies only
 - Interfaces, static and dynamic routing, S2S VPN, and Prefilter commands
- Out-of-band changes must be reconciled by FMC
 - Periodic assurance checking and pre-deployment validation
 - Audit transcript lists any detected changes
 - New deployments are blocked until the changes are acknowledged

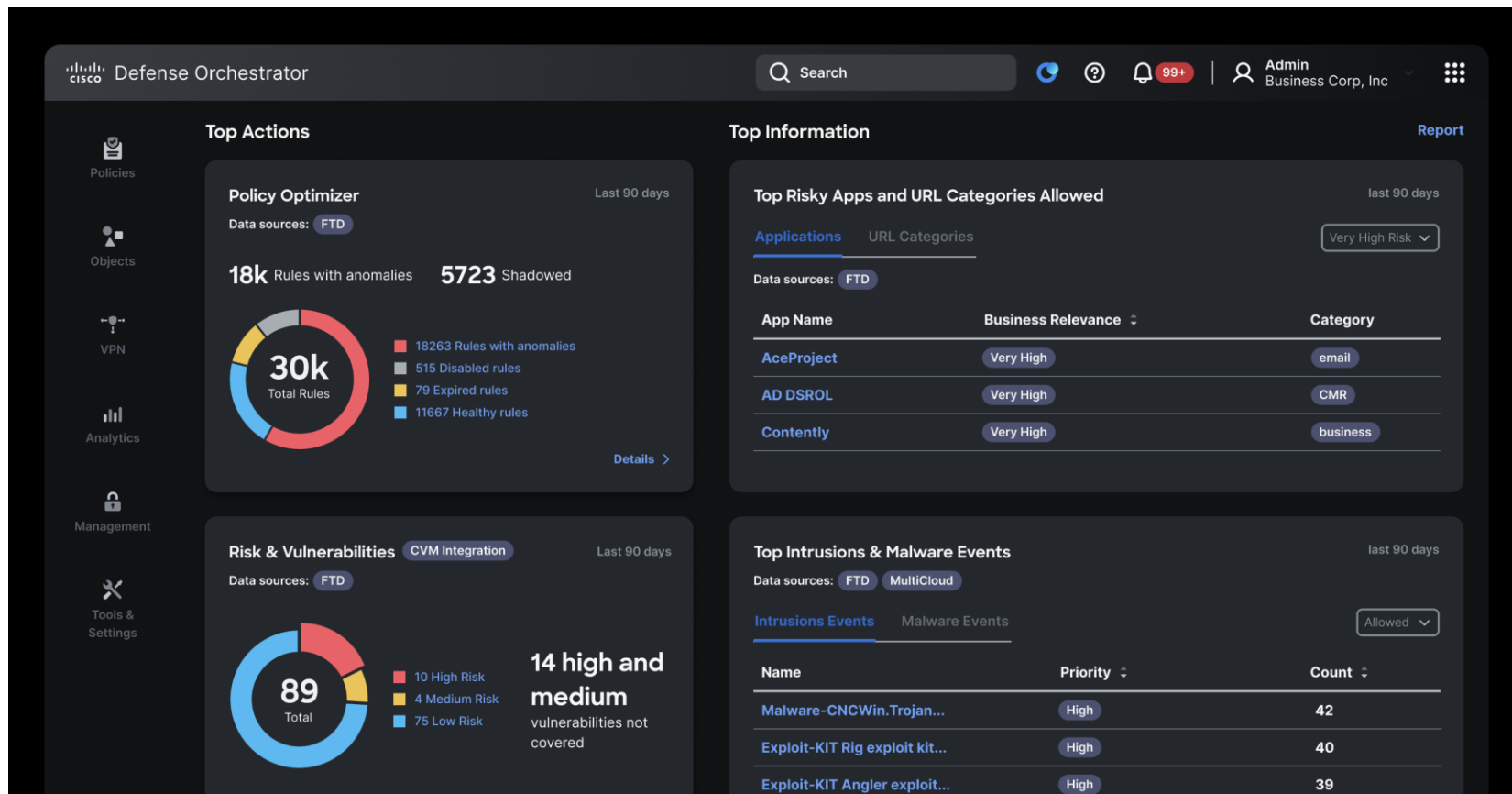


Security Cloud Control: AIOps Tools

- Use Generative AI to simplify firewall management and monitoring
 - Predict network and security events from historical and real-time events
 - Identify, predict, and reduce performance bottlenecks from live traffic
 - Continuously analyze and optimize security policy rules
- Cisco Defense Orchestrator enables backend for private FMC
- Initial focus on capacity planning and monitoring
 - Proactively identify applications that generate Elephant Flows
 - Estimate immediate and future cluster scale to match bandwidth trends
 - Identify unnecessary IPS rules with high processing impact

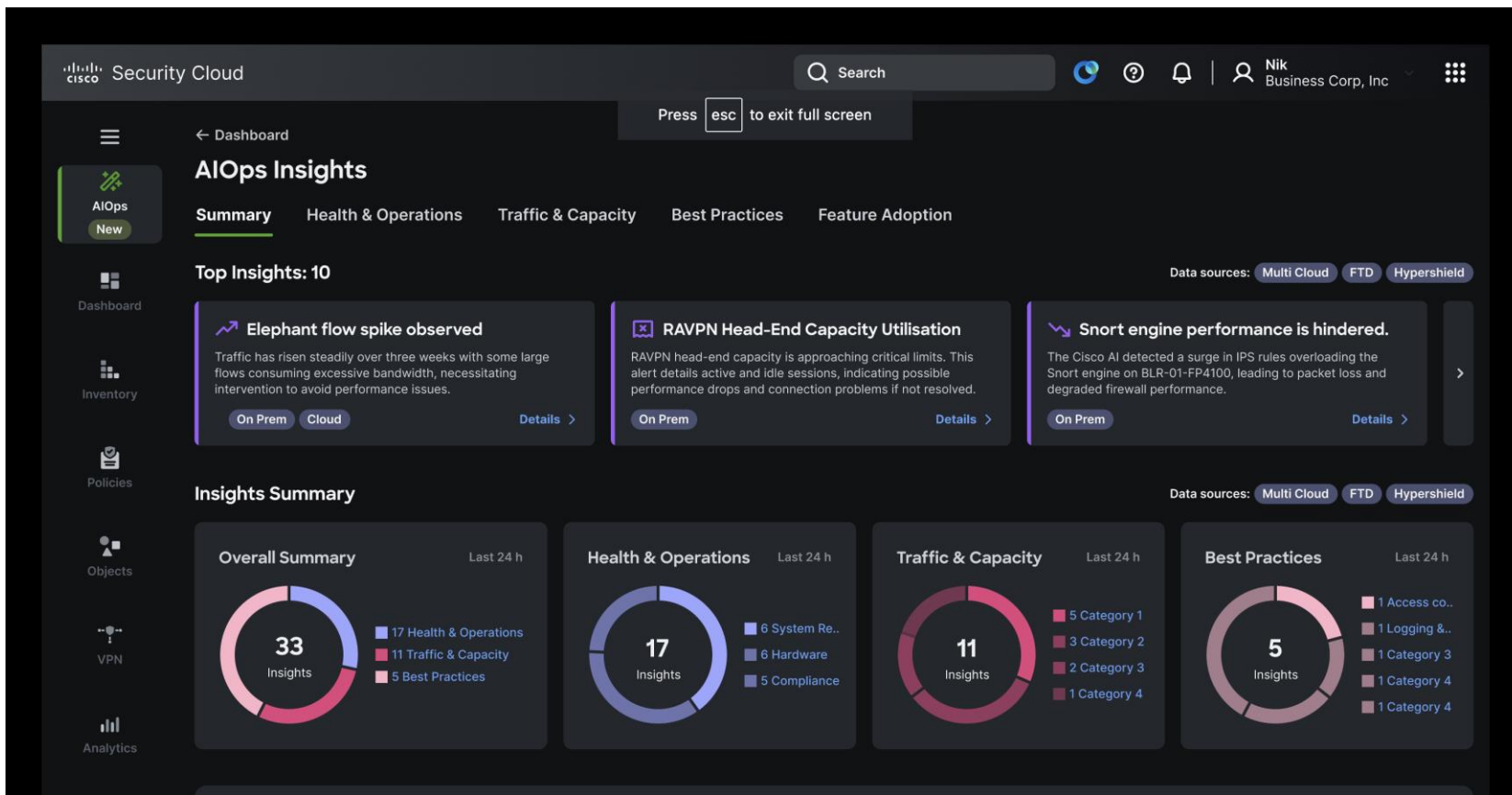
Security Cloud Control: Risks and Policy

Near
Future



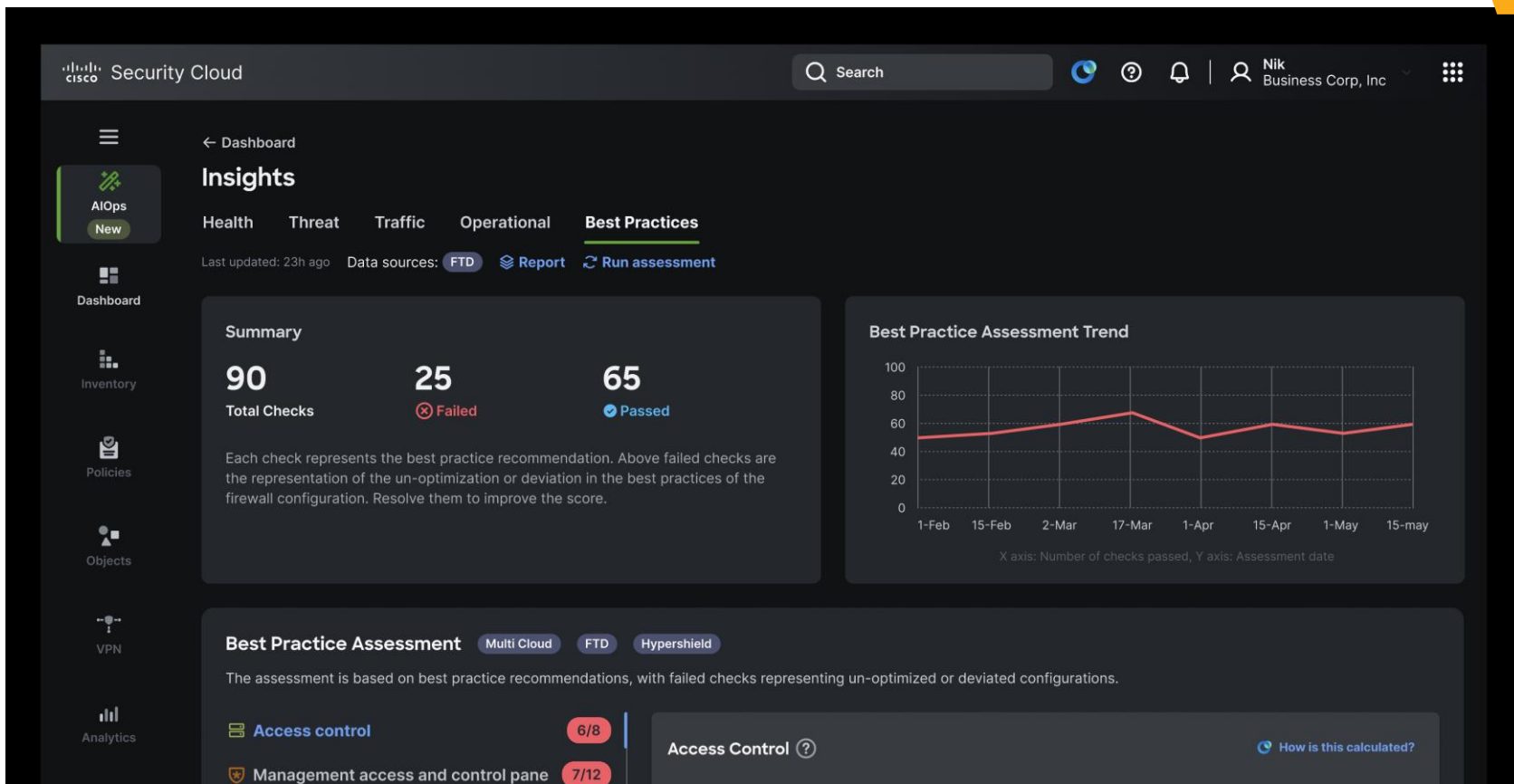
Security Cloud Control: Insights

Near
Future



Security Cloud Control: Best Practices

Near
Future



Multicloud Defense Orchestrator

- 10+ steps to deploy FTDv in a public cloud
- Each cloud is just a little different
- Defense Orchestrator dramatically simplifies FTDv insertion



Secure Workload

Secure Workload as Policy Engine

Flow Telemetry Ingestion

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

Dependency Mapping

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

Policy Experiments

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

Network Security (NetSecOps)



Secure Firewall



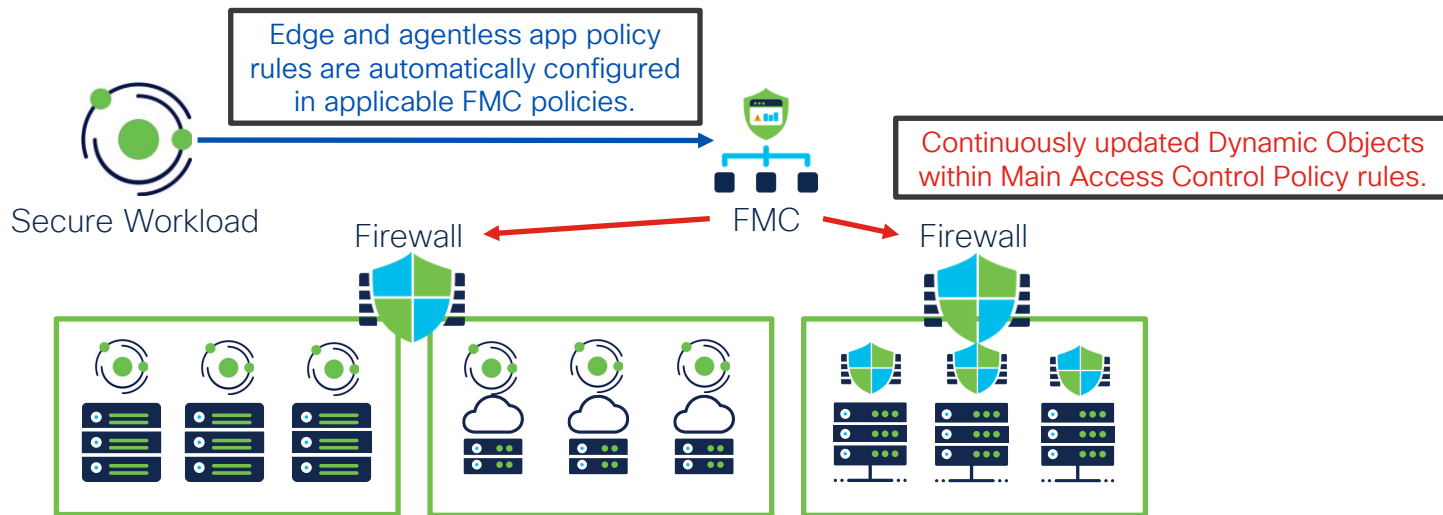
Secure Workload



Hypershield

Secure Workload Policy Extension to Firewall

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



Secure Workload Policy Orchestration in FMC

Workload
3.6

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects AMP Deploy

East-West-Pol

Inserted rules are organized by sections.

Dynamic objects are used to replace IP addresses where applicable.

Different rulesets are scoped by domains.

Rules Security Intelligence HTTP Responses Logging Advanced

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

Filter by Device Search Rules

#	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_!	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_CS	Allow

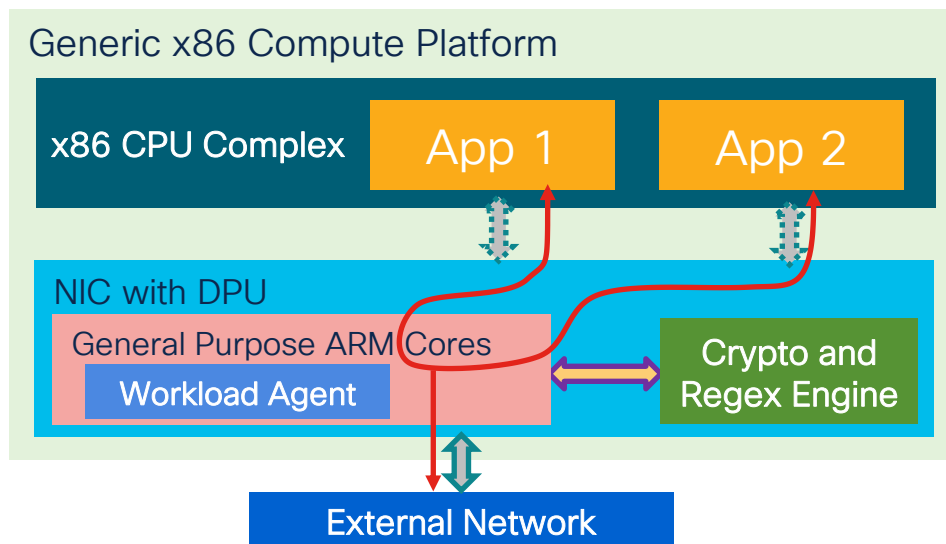
Outside access from workloads with known vulnerabilities based on version and CVE data can be blocked automatically.

Application Virtual Patching

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

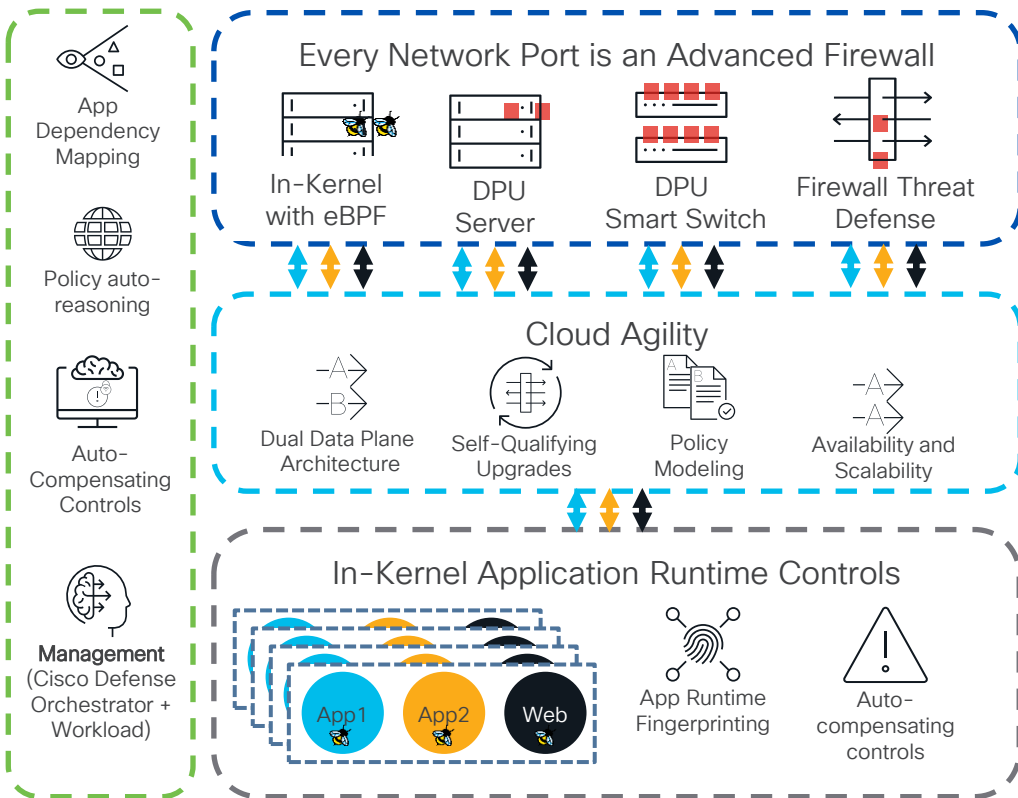
Workload Segmentation with Nvidia DPU

- 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

Now



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

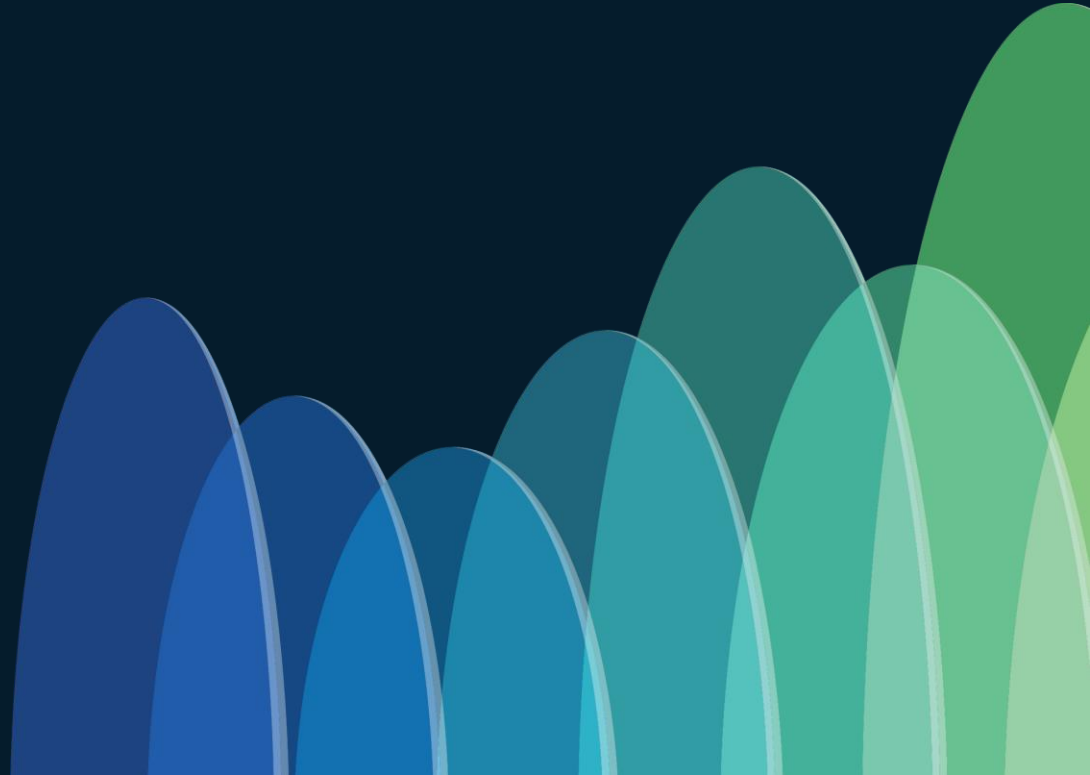
Dual data plane architecture enables self-qualifying upgrades, real-time policy modeling, and auto-scale-out use cases. It evolves from Workload agent visibility to advanced and flexible inline threat prevention.



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 claim a **Cisco Live T-Shirt**.



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



Continue your education

- Visit the Cisco Stand 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

Contact me at: aossipov@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC