

Keeping Up on Network Security with Cisco Secure Firewall

CISCO Live !

Jeff Fanelli
Distinguished Engineer, Cisco Systems, Inc.

Agenda

- 01 Versions and numbering
- 02 Firewall Platforms
- 03 Threat Protection
- 04 SD-WAN Capabilities
- 05 Management & AI Ops
- 06 Hybrid Mesh Firewall
- 07 Conclusions

New Firewall Release Numbering

Simplified release structure with consistent support and certification across all releases

Each major release is now broken into two minor releases (eg. 10.0.0, 10.5.0)

Example:

10 - Major version that is specified by the first digit and indicates a series of releases

10.0 - Initial minor version delivering new features/improvements

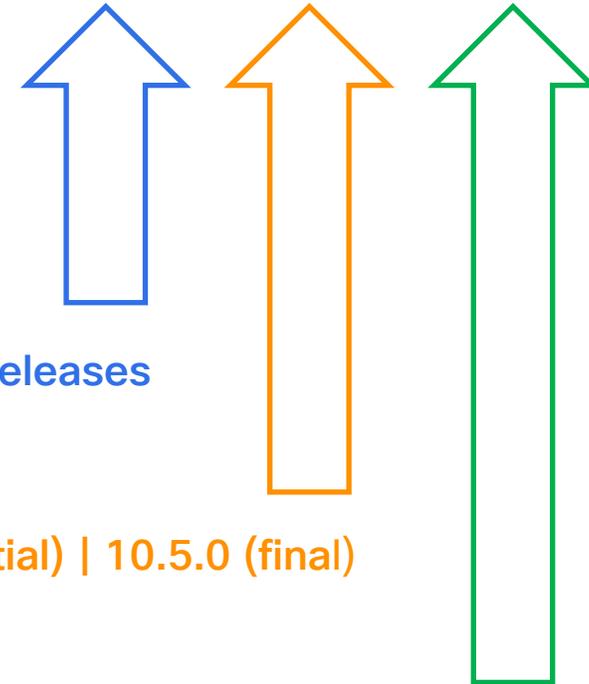
10.5 - Final minor version delivering new features/improvements. Submitted for government certification.

10.0.2 - Maintenance version that provides bug fixes and vulnerability protection on top of major version.

10.5.2 - Maintenance version that provides bug fixes and vulnerability protection for the final minor version only and for all 10.x.x.x customers to move to for sustaining support.

10.5.5 - Vulnerability Release based on the 10.5.5 Maintenance release.

10.0.0



Major Version - Series of releases

Minor Version - 10.0.0 (initial) | 10.5.0 (final)

Maintenance Release

Supported Upgrades

From 7.3.x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<ul style="list-style-type: none">• The install and upgrades file is the same same for Secure Firewall 1200.• Upgrade is only supported from 7.6.x to higher for 1200 Compact and from 7.7.x for 1200 Rackmount.• The install and upgrade file for the 3100 Series is the same file, as opposed to separate files.• The install and upgrade file is same for 4200 and Upgrade is only supported from 7.4 to higher versions.
From 7.4.x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
From 7.6.x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
From 7.7.x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

- Always upgrade FXOS before FTD on Firepower 4100 & 9300 Series
- For 10.0, the minimum version supported is 7.3 and 7.3 / 7.4 / 7.6 / 7.7 to 10.0 upgrades are supported

Where are we now?

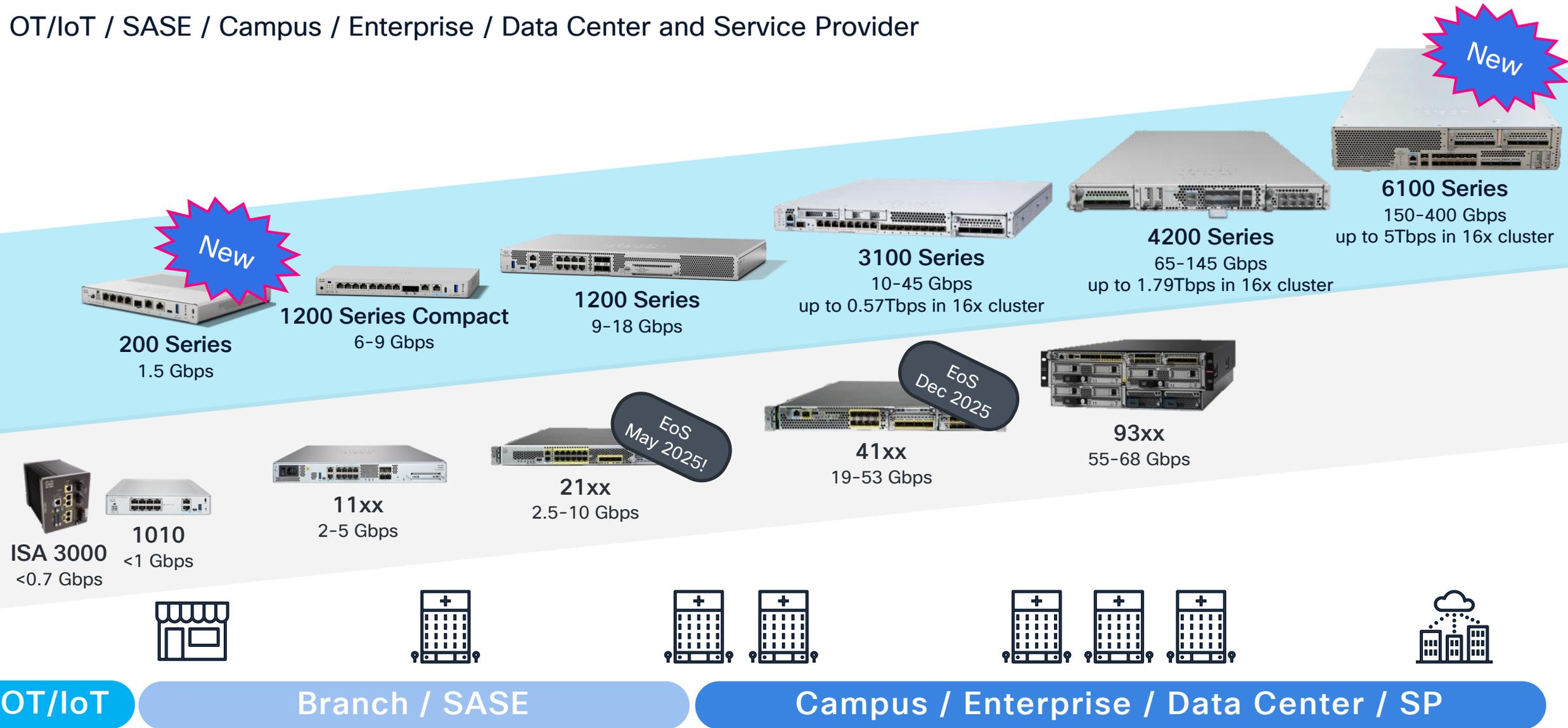
Major releases and dates for Firewall Threat Defense



Firewall Platforms

Cisco Secure Firewall Portfolio

OT/IoT / SASE / Campus / Enterprise / Data Center and Service Provider



Secure Firewall 220

FTD
10.0

ASA
9.24

PQC
Ready

- One Model
- Flexibility to address all modern use cases
- Network/Security SoC with 4 ARM cores
- SoC-embedded accelerators for encryption and traffic processing
- Up to 1.5Gbps (1024B) for NGFW traffic profiles
- Up to 1 Gbps for IPsec VPN, and up to 0.5 Gbps for TLS 1.2/1.3



AVAILABLE DEC 2025

Secure Firewall 1200 Overview

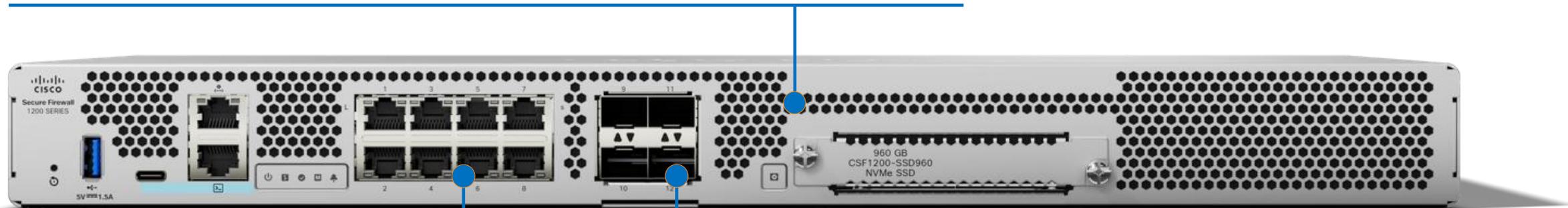
FTD
7.6+

ASA
9.21+

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

1RU



Copper Data Interfaces

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

SFP Data Interfaces

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

Cisco Secure Firewall 6100 Series

FTD
10.0+

ASA
9.24+

PQC
Ready

- Flexibility to address all modern NGFW use cases
 - Two CPUs with 192-256 physical cores (384-512 with HT)
 - 12x 1/10/25/50GE (SFP56) and 4x 40/100/200GE QSFP56 interfaces built in plus two Network Module bays
 - 1.5-2.3TB of RAM
 - Two NVMe slots, up to 7.2TB of RAID1 protected space
 - HVAC/HVDC/DC redundant PS
- Advanced FPGAs and one or two dedicated cryptographic hardware accelerators
- Clustering support on all models, up to 16x nodes
- Up to 400 Gbps for NGFW traffic profiles
 - up to 140 Gbps with 50% of TLS 1.2/1.3 mix
 - up to 350 Gbps for IPsec traffic



AVAILABLE DEC 2025

A high-performing firewall for every use case

Cisco Secure Firewall family performance at-a-Glance



Branch

Campus

Datacenter

Cloud



200 Series

1 Model

Firewalling+IPS

1.5 Gbps

IPSec VPN

1 Gbps

TLS Decryption

0.75 Gbps



1200 Series

5 Models

Firewalling+IPS

6-24 Gbps

IPSec VPN

5-22 Gbps

TLS Decryption

1-4.1 Gbps



3100 Series

5 Models

Firewalling+IPS

10-45 Gbps

IPSec VPN

5.5-39.4 Gbps

TLS Decryption

3.2-11.5 Gbps



4200 Series

3 Models

Firewalling+IPS

71-149 Gbps

IPSec VPN

51-148 Gbps

TLS Decryption

20-45 Gbps



6100 Series

2 Models

Firewalling+IPS

280-400 Gbps

IPSec VPN

280-350 Gbps

TLS Decryption

90-120 Gbps



Public/Private

20+ cloud variants

Public & Private Cloud

- ASA v support for Clustering & Autoscale in GCP
- ARM-based Instance Support for FTDv & ASA v in OCI
- FTDvU Form Factor for VMWare & KVM

GCP Clustering with Autoscale



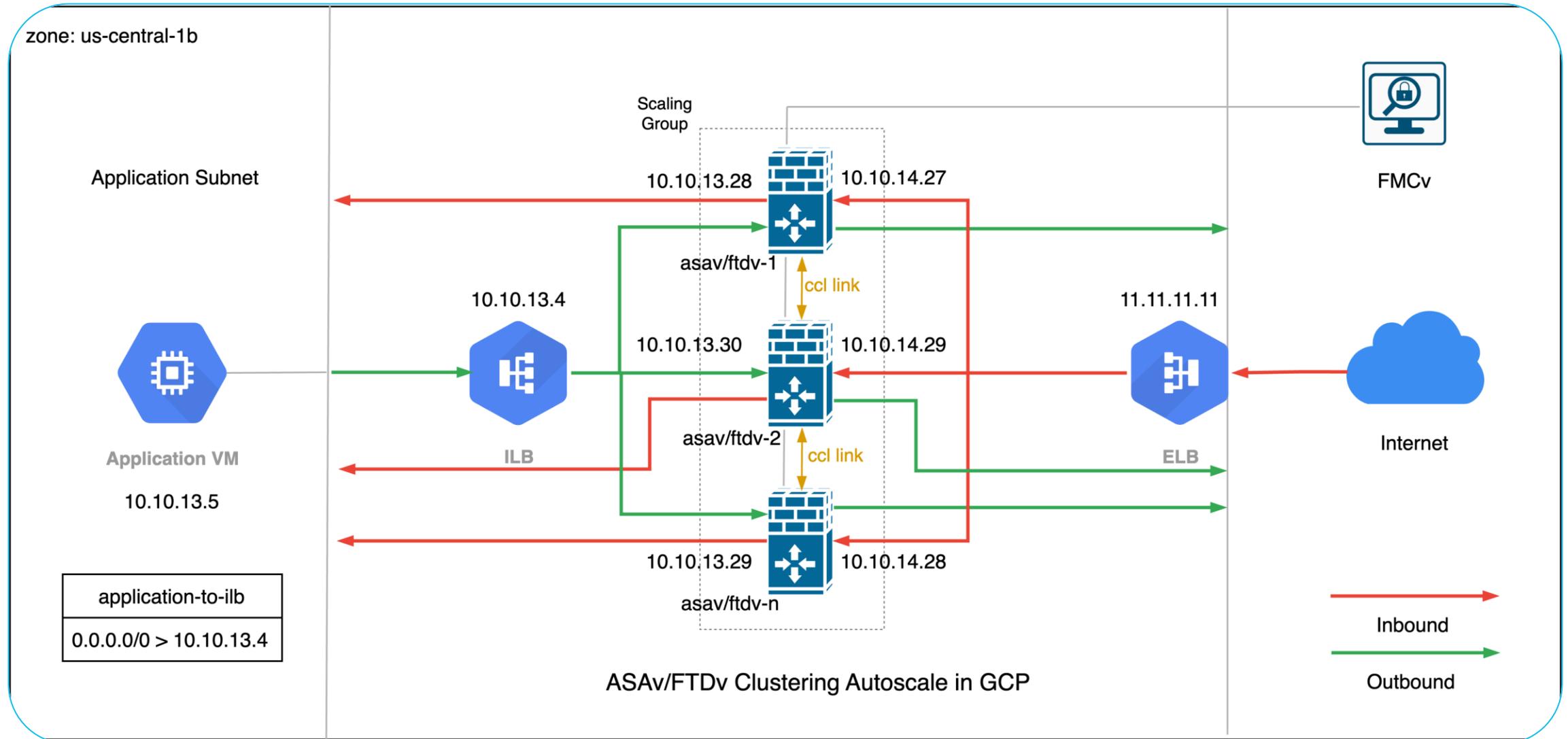
Challenge:

- GCP cluster deployments do not support dynamic scaling (increasing or decreasing cluster nodes) based on load(cpu/memory)

What's New:

- Added Clustering with dynamic scaling on GCP for ASA v
- FTDv Updated existing fixed-node Clustering with dynamic scaling capabilities on GCP.

Deployment Example - Clustering Autoscale in GCP



OCI ARM Instance Support



Background:

- Today, ASAv and TDv are x86 based OCI instances.
- While Cisco has ARM based ASA and Threat Defense hardware appliances, no support for virtual form factor based on ARM architecture.

What's New:

- ARM based ASAv and Threat Defense virtual instance support on OCI.
- Supported ARM instances: VM.Standard.A1.Flex and VM.Standard.A2.Flex types.
- Flexible configurations with 4, 8, 12, or 16 Oracle CPUs (OCPU) for ASAv and FTDv instances.
- Only BYOL (Bring Your Own License) is supported.

Instance Types: ASAv

Instance Type	CPU Cores	RAM	Max. Interfaces Supported	Recommended Throughput/License Type
A1.Flex	4	8	4	1G/ASAv_10
	8	16	8	2G/ASAv_30
	12	24	10	10G/ASAv_50
	16	32	10	20G/ASAv_100
A2.Flex	4	8	4	1G/ASAv_10
	8	16	8	2G/ASAv_30
	12	24	10	10G/ASAv_50
	16	32	10	20G/ASAv_100

Device Support

Features supported on ARM instances		Features supported on ARM instances	
FTDv		ASAv	
Minimum Licenses Required	Essentials	Minimum Licenses Required	Essentials
Works in Evaluation Mode	Yes	Works without Licensing	Yes
IP Addressing	IPv4 IPv6	IP Addressing	IPv4 IPv6
Multi-instances supported?	No	Multiple context supported?	No
Supported with HA'd devices	No	Supported with HA'd devices	No
Supported with clustered devices?	No	Supported with L3 clustered devices?	No
Other (only routed mode transparent mode), etc.	Only routed mode only	Supported with L2 clustered devices?	No

Device Registration in FMC

- Prior to the 10.0.0 release, FTDv was constrained to a maximum of 16 virtual CPU cores.
- FTDvU – Unlimited new tier license

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

- FTDv5 - 100 Mbps
- FTDv10 - 1 Gbps
- FTDv20 - 3 Gbps
- FTDv30 - 5 Gbps
- FTDv50 - 10 Gbps
- FTDv100 - 16 Gbps
- FTDvU - Unlimited**
- FTDv - Variable

Threat Protection

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 via access to app server

Create Decryption Policy

1 Policy Details — 2 Blocking — 3 Decryption Exclusions

Enter name, description, choose policy type and certificates. (Optional) Configure blocking based on TLS version and certificate status. (Optional) Configure exclusions for outbound connections.

Decryption Exclusions

Bypass decryption for sensitive URL categories

In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.
Note: URL License is Required

URL Categories: Health and Medicine × Finance × Online Trading × [+ Add](#)

Bypass decryption for undecryptable distinguished names

Bypass decryption based on Cisco's list of known undecryptable distinguished names.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.

56 Distinguished names included

Bypass decryption for undecryptable applications

Certain enterprise applications are not supported for decryption due to a variety of reasons (Certificate Pinning, Client Certificate Authentication, etc.). Bypass decryption based on Cisco's list of known undecryptable applications.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.

56 Applications included

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 this policy is deployed must run version 7.7 or later and must have a valid IPS license.

[Cancel](#) [Back](#) [Create Policy](#)

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
 - Supports Command and SQL Injection and HTTP command injection (10.0), with more coverage coming soon.

Intelligent Decryption Bypass



- Build into Decryption Policy creation wizard
 - Utilized by EVE and URL Category Reputation
 - Creates and enables a Do Not Decrypt Rule

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.**

[Cancel](#) [Back](#) [Create Policy](#)

Rule Level Configuration of Intelligent Decryption Bypass

- New **Client Threat** tab in the Decryption Rule Editor
- Client Threat – Identified by EVE
- Threat Levels – Very Low to Very High (Or Any)
- For traffic originating from clients identified by EVE as Very Low, decryption is bypassed.
- Recommended to add a URL Category and Reputation filter.

Editing Rule - New_Rule

Name Enabled [Move](#)

Action

Zones
Networks
VLAN Tags
Users
Client Threat
Applications
Ports
Category
Certificate
DN
Cer

i We recommend you add at least one category and reputation on the Category tab page of the decryption rule to use EVE threat detection. [Read more](#)

Client Threat (as identified by EVE)

Any

Very Low

Low

Medium

High

Very High

Selected client process risk

Very Low - Low

[Add to Rule](#)

Block Insecure TLS Versions & Certificate Statuses



Build into Decryption Policy creation wizard

Create Decryption Policy

1 Policy Details | **2 Blocking** | 3 Decryption Exclusions

Block connections based on TLS version NEW

We recommend blocking the following because they are not secure.

SSL v3.0 x TLS v1.0 x TLS v1.1 x

- SSL v3.0
- TLS v1.0
- TLS v1.1
- TLS v1.2
- TLS v1.3

Reset to default

Cancel Back Next



Create Decryption Policy

1 Policy Details | **2 Blocking** | 3 Decryption Exclusions

Block connections based on server certificate status NEW

We recommend blocking the following because they are not secure.

Invalid Signature x Expired x Not Yet Valid x

Invalid Certificate x

- Self Signed
- Invalid Signature
- Expired
- Not Yet Valid
- Invalid Certificate
- Invalid CRL

Reset to default

Cancel Back Next

Decryption Policy with Auto Generated Rules



Rules for Certificate Status/TLS Versions

Rule for Intelligent Decryption Bypass (EVE)

Standard Rules									
1	Auto-Rule-Certificate-Status	<i>an, an, any, an, any, an, any</i>	<i>any, any, any</i>	4 Cert Status selections	Block with reset				
2	Auto-Rule-TLS-Versions	<i>an</i>	<i>any, any, any</i>	3 Protocol Versions	Block with reset				
3	Auto-Rule-Undecryptable-DNs	<i>an</i>	<i>any, any, any</i>	1 DN selection	Do not decrypt				
4	Auto-Rule-Low-Risk-Connections	<i>an, an, any, an, any, an, any</i>	<i>any, any</i> Any (Except Uncategorized) (Reputation 5)	1 Client Threat selection	Do not decrypt				
5	Auto-Rule-URL-Categories (Disabled)	<i>an, an, any, an, any, an, any</i>	<i>any, any</i> Finance (Any reputation) Health and Medicine (Any reputation) Online Trading (Any reputation)	<i>any</i>	Do not decrypt				
6	Auto-Rule-Undecryptable-Apps	<i>an, an, any, an, any, an</i> Tags: undecryptable	<i>any, any, any</i>	<i>any</i>	Do not decrypt				
7	Auto-Rule-internal_ca	<i>an, an, any, an, any, an, any</i>	<i>any, any, any</i>	<i>any</i>	Decrypt - Resign				

Simplifying EVE

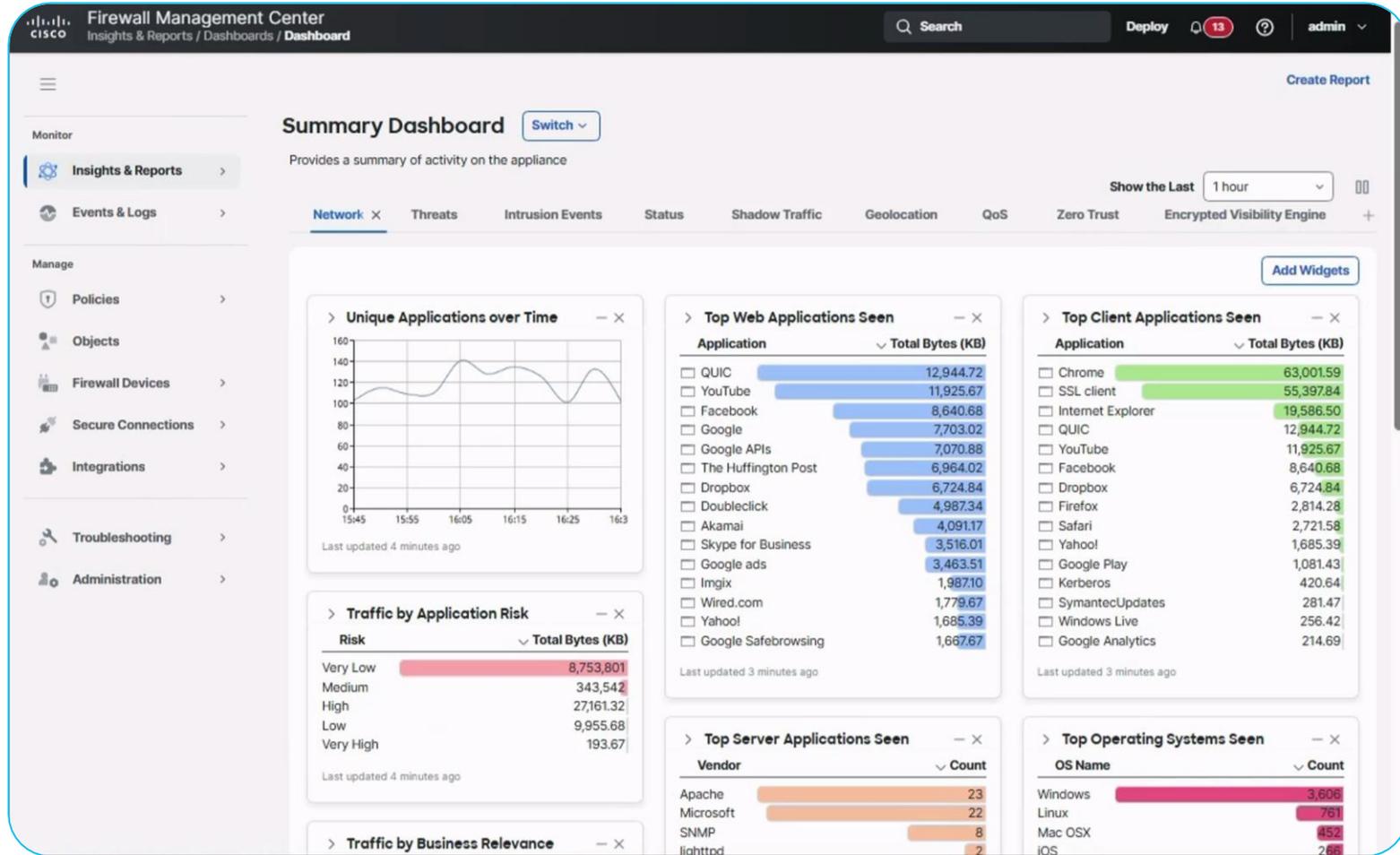
New Dashboard/Widgets

Introduction of two modes: Monitor and Protect.

Protect: EVE **monitors and blocks** malicious connections based on the Block Threshold Level configured.

If EVE is enabled, it is now automatically used for client **application detection**.

Simplified Block Threshold Configuration



Simplifying the Decryption Policy

Simplified decryption policy workflow

Option for Selective Decryption.

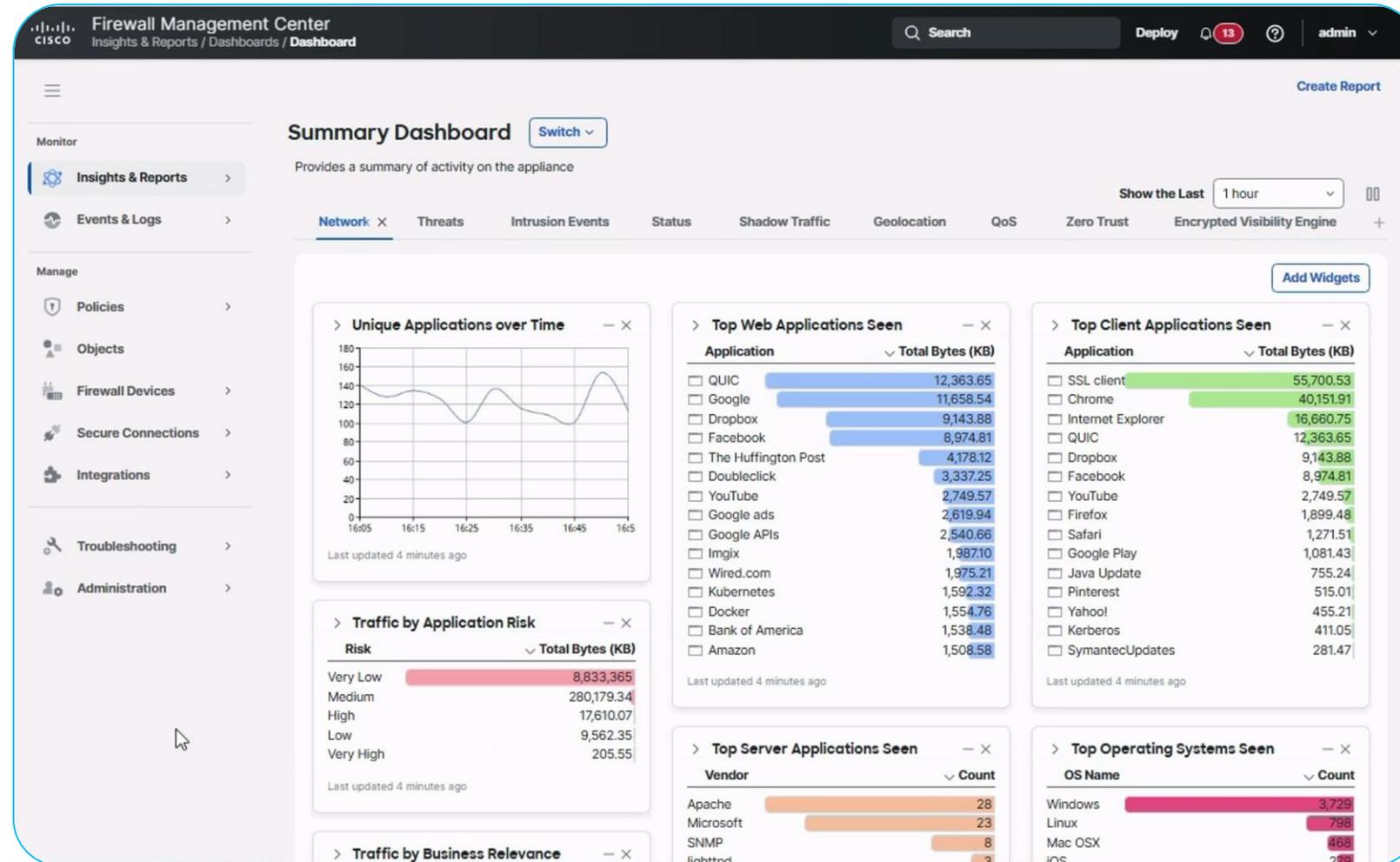
Enhanced **certificate management** directly from the Decryption Policy creation page.

Two policy modes:

Standard – Policies created and modified using the new interface. Default policy mode in 10.0

Legacy – Policies created and modified using the editor in 7.7 or lower.

QUIC Decryption no longer experimental.



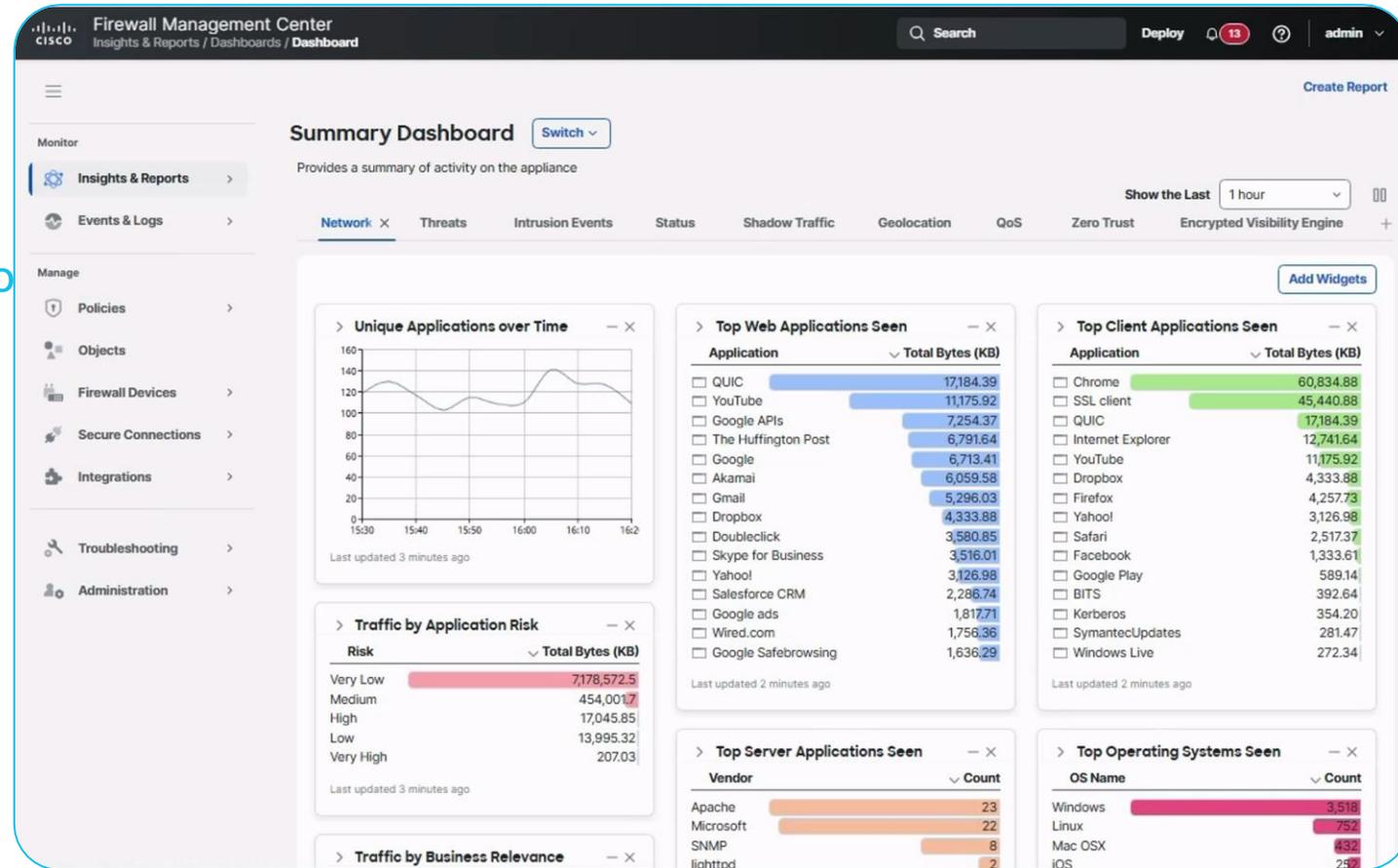
AppID Default Port Specification



- AppID provides the ability to detect and control access to resources based on application type.
- However, for many applications, customers are unlikely to know which default ports are even associated with an application (e.g., do you know which ports the gaming app Steam uses?).
- **New in 10.0.0:**
 - When adding Applications to Access Control rules, default ports will be enforced as standard behavior.
 - If multiple Applications are added to a single rule, each application will match only against its specific default ports (e.g., in the same rule, SSH only matches on TCP/22 while HTTP matches only on TCP/80).

What is Dynamic Firewall?

- The Dynamic Firewall feature helps associate an identity source (ISE or pxGrid Cloud) with identity intelligence like Cisco Identity Intelligence (CII) for user trust scores.
- Cisco Identity Intelligence (CII) – Collects user information from different identity sources (Duo or Entra ID) and classifies user patterns into five trust levels:
 1. Trusted
 2. Favorable
 3. Neutral
 4. Questionable
 5. Untrusted
- FMC can get the Untrusted and Questionable levels from CII and apply it to logins received from ISE or pxGrid Cloud.



SDWAN Capabilities

Simplifying Branch Deployments

FMC
7.0+



Secure Elastic Connectivity

- Configure route-based VPN VTI tunnels between branches (Spokes) to headquarters (Hubs)
- IPv6 overlay support
- BGPv6 over VTI
- EIGRP, OSPF and BGP over VTI
- DVTI supports DHCP (spokes)

High availability with near-zero network down time / WAN optimization

- Multi-ISP configuration
- Active-standby backup VTI tunnel configuration with SLA monitoring
- Optimal path selection based on interface monitoring
- HA Management with Dual WAN links via Data Interface

Increased Usable Bandwidth

- ECMP support for load-balancing across multiple ISPs
- ECMP support for VTI
- Application based load balancing using policy-based routing
- SDWAN Monitoring Dashboard with Application performance

Direct internet access for public cloud and guest traffic

- SaaS application detection (First Packet using DNS snooping)
- Policy-based routing using application, user and SGT as matching criteria
- Local tunnel ID support for Umbrella
- BGP AS Override

Simplified Management

- Zero Touch Provisioning
- Data interface management
- Auto config rollback
- Bulk pre-provisioning with device templates
- Umbrella SASE auto-tunnel deployment
- Simplified branch to hub communication using SD-WAN Wizard

Secure Firewall 7.6 Topology Wizard

Firewall Management Center
Site To Site

Overview Analysis Policies Devices Objects Integration Deploy

admin

Create VPN Topology

Topology Name *

Hub-Spoke-VPN

VPN Type

- SD-WAN Topology** New
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology
 Hub and Spoke
[Prerequisites](#)
- Route-Based VPN**
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology
 Hub and Spoke
 Peer to Peer
- Policy-Based VPN**
Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology
 Hub and Spoke
 Peer to Peer
 Full Mesh
- SASE Topology**
Simplifies and orchestrates the auto tunnel configuration between the threat defense device and the Umbrella SIG gateway.

Select VPN Topology
 Hub and Spoke

Cancel Create

Full automated VPN deployment!



View By: Group

All (6) Error (0) Warning (0) Offline (0) Normal (6) Deployment Pending (6) Upgrade (0) Snort 3 (6)

[Add](#)

[Collapse All](#)

[Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (6) <ul style="list-style-type: none"> <input type="checkbox"/> ftdv-test-11 Snort 3 10.101.128.211 - Routed <input type="checkbox"/> ftdv-test-12 Snort 3 10.101.128.212 - Routed <input type="checkbox"/> ftdv-test-13 Snort 3 10.101.128.213 - Routed <input type="checkbox"/> ftdv-test-14 Snort 3 10.101.128.214 - Routed <input type="checkbox"/> ftdv-test-15 Snort 3 10.101.128.215 - Routed 	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
<input type="checkbox"/>	<ul style="list-style-type: none"> <input type="checkbox"/> ftdv-test-12 Snort 3 10.101.128.212 - Routed 	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
<input type="checkbox"/>	<ul style="list-style-type: none"> <input type="checkbox"/> ftdv-test-13 Snort 3 10.101.128.213 - Routed 	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
<input type="checkbox"/>	<ul style="list-style-type: none"> <input type="checkbox"/> ftdv-test-14 Snort 3 10.101.128.214 - Routed 	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
<input type="checkbox"/>	<ul style="list-style-type: none"> <input type="checkbox"/> ftdv-test-15 Snort 3 10.101.128.215 - Routed 	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	Edge Access Policy		
<input type="checkbox"/>					Essentials, IPS (2 more...)	Edge Access Policy		



Carry SGT Across VTI-based Site-to-Site Tunnels



A need exists for carrying encrypted Security Group Tags across SD-WAN fabric



DVTI's & SVTI's can receive and propagate SGT's



Outer ESP inline tagging supported



Point-to-Point or Hub-and-Spoke and ASA and FTD topologies supported

ECMP & BFD Fault Detection for VTIs



Challenge: Only traffic initiated from spoke to hub can be load balanced, whereas hub to spoke cannot be load balanced. VPN path failures also need to be detected faster.



Multiple DVTI interfaces can be part of an ECMP zone & BFD link detection is faster within a few mili/microseconds.



Spoke-bound traffic can now be load balanced.



ECMP & BFD configurations for hub are visible after upgrade to 10.0.0

Enable ECMP on DVTI in SD-WAN Topology

Firewall Management Center
Devices / VPN / Site To Site

SDWAN-BFD-Topology-V4-1
Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP
HA-1 Threat Defense	Virtual-Template1 (outside_dynamic_vti_1) Source:Ethernet0/0 (outside)	192.172.100.187	BFD-IPV4-Pool- Range: 10.10.10.1

Next

2 Spokes ⓘ

Device	VPN Interface
10.10.9.150	outside-IS
10.10.9.189	outside-IS

3 Authentication Settings ⓘ

Enables ECMP on dynamic VTI of hub devices with Version 7.8 or later. All virtual access interfaces generated on the hub that connect to the same spoke are added to an ECMP zone.

- Select the checkbox to enable ECMP on the dynamic VTI of the Hub.
- This feature is supported on devices running version 10.0.0 or later.
- Note: This option enables ECMP only for the Hub. For spoke SVTI, configure it through the device routing page.

Universal 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.

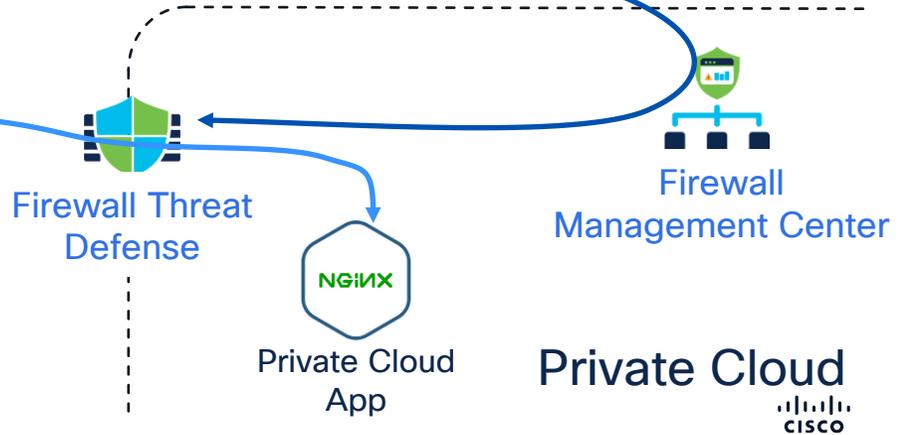
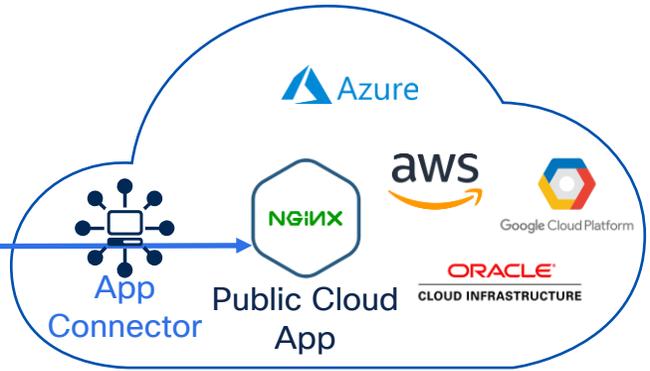


3. Per-application tunnels to public apps or private apps requiring advanced inspection features (e.g. DLP) go through **Secure Access** and **App Connectors**.

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



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



Consistent Zero Trust Access – Hybrid Private Access

- Unified management and distributed enforcement for cloud and on-premises
- Dynamic steering of traffic through the nearest enforcement point via Trusted Network Detection (TND).
- Protect your existing firewall investments while moving towards Zero Trust model.

The screenshot displays the Cisco Firewall Management Center (FMC) interface for Zero Trust Access. The top navigation bar includes the Cisco logo, 'Firewall Management Center', 'Policies > Zero trust access', a search bar, and a 'Deploy' button. A blue starburst in the top right corner indicates the version 'FTD 7.7.1'. The left sidebar contains navigation options: Home, Overviews, Analysis, Policies (highlighted), Devices, Objects, and Integration.

Zero Trust Access

Clientless **Hybrid**

Hybrid zero trust access (Client based)

Zero Trust Access Policy protects private applications with identity based access, intrusion protection, and malware and file inspection for the remote end users and on-prem end users. You can protect your private resources (application) using on-cloud enforcements or

How it works?

Policies created in Secure Access to protect the private resources (applications) will be deployed to devices managed by FMC.

Steps to follow:

- Secure Firewall Management Center**
- Secure Access**
- Secure Firewall Management Center**

- Step 1**
Go to **Integration > Cisco Secure Cloud Integrations** page and **Enable Cisco Security Cloud**.
- Step 2**
Here on Hybrid ZTA Page > Device Configuration and configure devices for Hybrid ZTNA. These devices will be visible in **Secure Access**.
- Step 3**
Go to **Devices** and Select the devices which are required for **Hybrid ZTA policy enforcement**.
- Step 4**
Go to **Private Resources** and define the private resources (application) and associate the **FTD devices** with them.
- Step 5**
Go to **Access Policy** and create a **rule with private resources (application)** to provide access to specific end user. Enforce the policy for further deployment.
- Step 6**
Go to **Deployment** and deploy the policies enforced from **Secure Access**.
- Step 7**
Go to **Hybrid ZTA Policy** page and check the **deployment status**.

[Device configuration](#)

[Hybrid zero trust access policy](#)

Optimized Zero-Touch Provisioning (ZTP)

6.7 - LTP to FDM in Cisco Defense Orchestrator (CDO)

- ✓ Low Touch Provisioning claim with serial number was supported in CDO for FDM managed FTD.

7.2+ Low Touch Provisioning for Cloud and on-prem FMC managed FTD

- ✓ 7.2 added LTP support in cdFMC.
- ✓ 7.4.1 extended LTP support for On-Prem FMC using cloud.
- ✓ 7.6 enhanced LTP to Zero-touch Provisioning
- ✓ 7.6 ZTP Bulk Registration to on-prem FMC + Pre-provisioning using Templates.

New! 10.0.0 - ZTP Lite

- ✓ 10.0.0 introduces ZTP Lite - Optimized ZTP backend on FTD by removing dependency on FDM.

Recovery CLI Example

- Emergency Local Configuration Changes When Management Connectivity is not available
- Always available, but intended for FMC-down emergencies only
- Currently Supports CLI Configuration changes for:
 - Static Routes
 - Dynamic Routing (BGP and OSPF)
 - PreFilters
 - Site-to-Site VPN
 - Interface Configurations
- Manual Reconciliation once the firewall is connected to the central manager

The image shows a screenshot of the Cisco Firewall Management Center (FMC) interface. A blue starburst in the top right corner indicates 'FMC 7.7'. The main window displays 'Out-of-band configuration details (10.10.28.38)' with a warning: 'The configuration on the device is different from the management center. Review the differential and acknowledge. Manually make changes in the management center before deploying.' Below this, there are two columns of configuration text: 'Last-deployed configuration' and 'Configuration on device (10.10.28.38)'. A modal dialog box is open, titled 'Acknowledge out-of-band configuration differential', with the text: 'Manually make changes in the management center before deploying. The management center configuration will overwrite the configuration on the device. To acknowledge, click Yes.' The dialog has 'No' and 'Yes' buttons.

Below the FMC screenshot, there is a detailed view of 'Out of Band Configuration Details (172.16.0.100)'. It shows a comparison between 'Last deployed Configuration from Manager/FMC' and 'Configuration on Device'. The configurations are listed in a table format with line numbers.

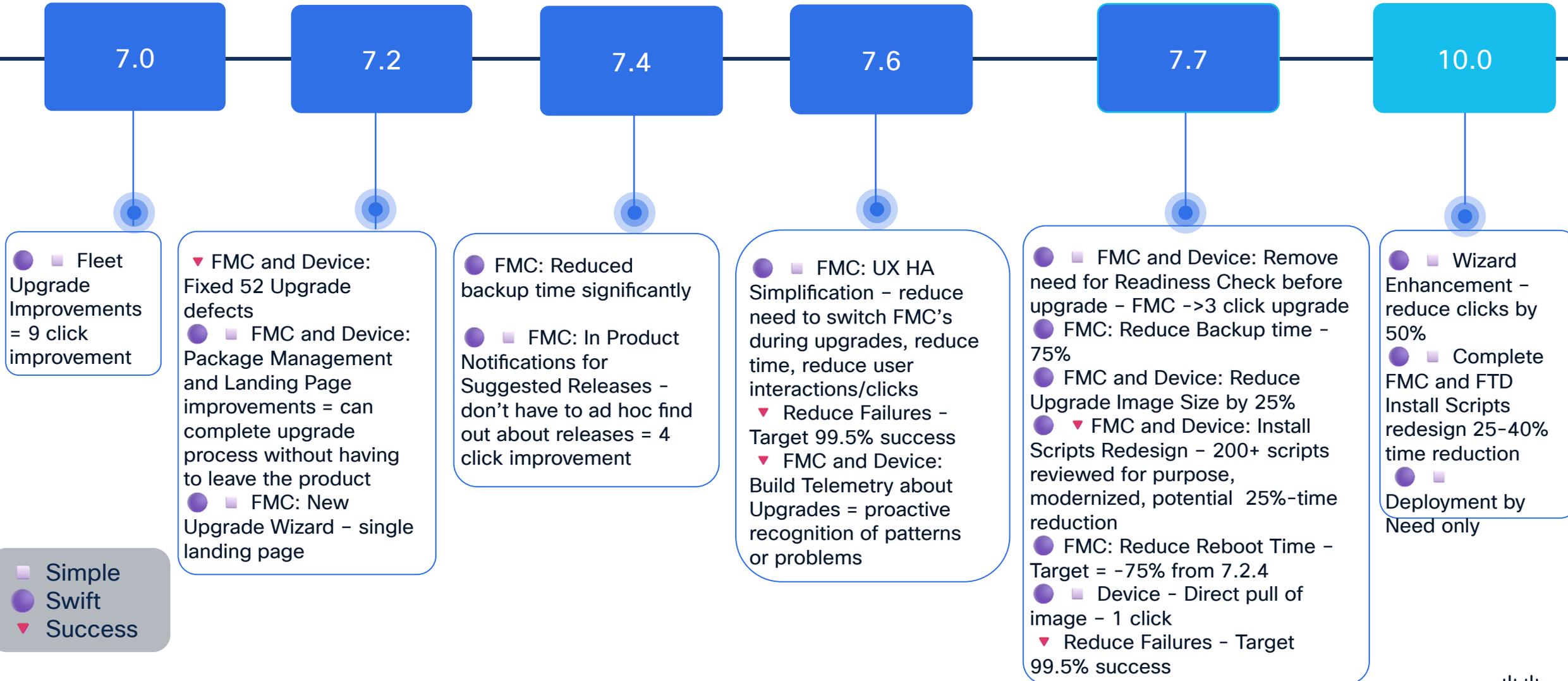
Line	Last deployed Configuration from Manager/FMC	Configuration on Device
1	hostname ciscoasa	hostname ciscoasa
2	passwd new ciscoasa	passwd new ciscoasa
3	enable password ***** p8k#f2	enable password ***** p8k#f2
4	filec enable	filec enable
5	interface Ethernet1/1	interface Ethernet1/1
6	nameif outside	nameif outside
7	cts manual	cts manual
8	security-level 90	security-level 90
9	ip address 172.16.0.6 255.255.255.0	ip address 172.16.0.6 255.255.255.0
10	ispd address 2000:1:854	ispd address 2000:1:854
11	ispd enable	ispd enable
12	!	!
13	interface Ethernet1/2	interface Ethernet1/2
14	nameif inside	nameif inside
15	security-level 100	security-level 100
16	ip address 4.4.4.6 255.255.255.0	ip address 4.4.4.6 255.255.255.0
17	!	!
18	interface Ethernet1/3	interface Ethernet1/3
19	shutdown	shutdown
20	no nameif	no nameif
21	no security-level	no security-level
22	no ip address	no ip address
23	!	!
24	interface Ethernet1/4	interface Ethernet1/4
25	shutdown	shutdown
26	no nameif	no nameif
27	no security-level	no security-level
28	no ip address	no ip address
29	!	!
30	interface Ethernet1/5	interface Ethernet1/5
31	shutdown	shutdown
32	no nameif	nameif test
33	no security-level	security-level 1
34	no ip address	no ip address
35	!	!

Management

Firewall Upgrade Improvements over Releases

Progress: Achieving 80% of North Star with 7.7, targeting complete realization with 7.8

Future



Upgrade Workflow Layout – Step Navigation

The screenshot shows the 'Threat Defense Upgrade' page in the Cisco Firewall Management Center. The page features a top navigation bar with the Cisco logo, 'Firewall Management Center', and 'Devices / Upgrade / Threat Defense Upgrade'. A search bar and 'Deploy' button are also present. The main content area includes a progress indicator with four steps: 1. Select Devices, 2. Prepare for Upgrade, 3. Start Upgrade, and 4. Monitor Upgrade. The current step is 'Prepare for Upgrade', which is highlighted in blue. Below the progress indicator, there are tabs for 'Check for Compatibility and Readiness (1 + 1)', 'In Progress (1 + 1)', and 'Ready to Upgrade (0)'. The 'In Progress' tab is selected. A table lists the devices being upgraded, including their names, versions, models, and details. The table has columns for 'Device', 'Version', 'Model', and 'Details'. The devices listed are 'auto_bwasniak_ftd', 'HA2025 High Availability', 'auto_bwasniak_ftd2 (Primary)', and 'auto_bwasniak_ftd3 (Secondary - Active)'. The details for each device indicate that the readiness check is in progress. A sidebar on the left contains navigation options: Home, Overview, Analysis, Devices, Objects, and Integration. The 'Devices' option is selected. At the bottom of the page, there are 'Reset', 'Previous', and 'Next' buttons.

Upgrade Step

Filter Tabs

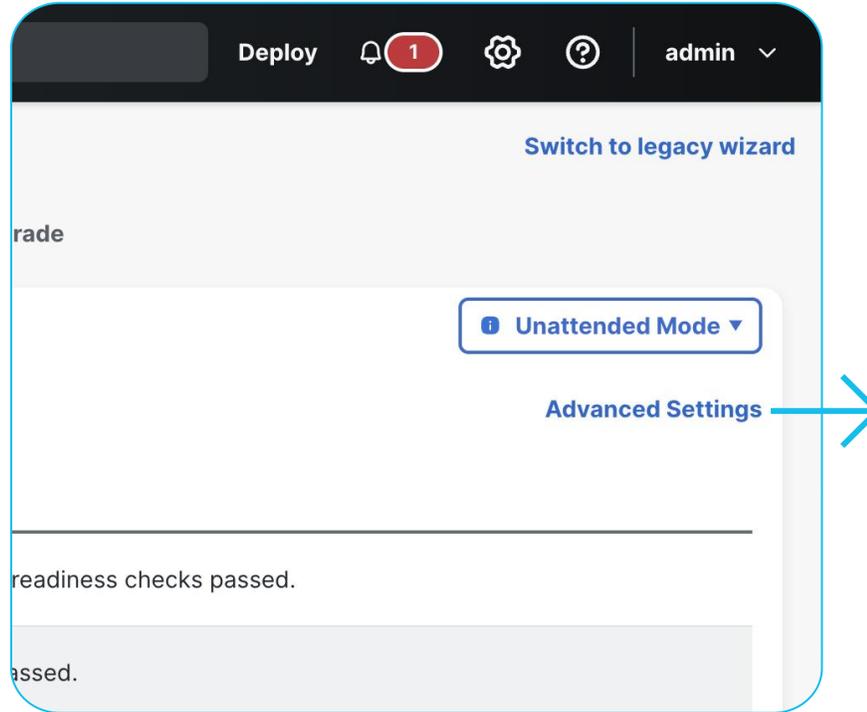
Selected Devices

Device Details

Device	Version	Model	Details
auto_bwasniak_ftd	7.4.1	Firewall Threat Defense for VMware	Not ready for upgrade. Compatibility check passed. Readiness check in progress.
HA2025 High Availability			
1 auto_bwasniak_ftd2 (Primary)	7.4.1	Firewall Threat Defense for VMware	Not ready for upgrade. Compatibility check passed. Readiness check in progress. High availability status: Standby.
2 auto_bwasniak_ftd3 (Secondary - Active)	7.4.1	Firewall Threat Defense for VMware	Not ready for upgrade. Compatibility check passed. Readiness check in progress. High availability status: Active.

Upgrade Workflows - Advanced Settings

Control compatibility checks



Advanced Settings

Compatibility and Readiness Checks

- Require passing compatibility and readiness checks.

Upgrade Failure

- Automatically cancel on upgrade failure and roll back to the previous version.

Enable Revert ⚠

- Enable revert after successful upgrade. ⓘ

Upgrade Snort ⚠

- Convert eligible devices from Snort 2 to Snort 3. ⓘ

Upgrading FTDs – Monitor Upgrade

Firewall Management Center
Devices / Upgrade / Threat Defense Upgrade

Search Deploy 1 admin

Threat Defense Upgrade

Switch to legacy wizard

1 Select Devices — 2 Prepare for Upgrade — 3 Start Upgrade — 4 Monitor Upgrade

i Upgrade of selected devices started 2025-03-24 18:10:33 EDT.
Use the [Message Center](#) to view overall upgrade status. This page (until you clear it) and [Device Management](#) have detailed upgrade status. [Clear Upgrade Information](#)

Upgrade to: **7.7.0-89**

[Upgrade Initiated \(1 + 1\)](#) [In Progress \(1 + 1\)](#)

Device	Version	Model	Status
auto_bwasniak_ftd	7.4.1	Firewall Threat Defense for VMware	In progress <div style="width: 14%;"></div> 14% Detailed Status Preparing to upgrade...
HA2025 High Availability			
1 auto_bwasniak_ftd3 (Secondary)	7.4.1	Firewall Threat Defense for VMware	In progress <div style="width: 14%;"></div> 14% Detailed Status Preparing to upgrade...
2 auto_bwasniak_ftd2 (Primary – Active)	7.4.1	Firewall Threat Defense for VMware	Pending Detailed Status Waiting to start...

Upgrade initiated for 1 + 1 devices.

[Reset](#) [Previous](#)

Monitor Device Upgrades from Single-pane

Additional Device Model Migration Support

- Ability to migrate device specific configurations from Firepower 1010, 1100, 2100, 4100, or 9300 Series to Secure Firewall 1200, 3100 or 4200 Series:
 - Firepower 4100 Support: 4112, 4115, 4125, 4145
 - Firepower 9300 SM Support: SM40, SM48, SM56
- Built-in FTD Model Migration Wizard with FMC 10.0.0 now allows administrators to:
 - Choose a source device (Firepower 1000/2100/4100/9300 Series)
 - Choose a target device (Secure Firewall 1200, 3100 or 4200 Series)
- Ability to migrate:
 - Interface configurations
 - Inline sets
 - Routing configurations
 - DHCP
 - Virtual router configurations
 - Objects



Any 1100,
2100, 4100,
9300 Series
FTD on 7.3+

3100 or
4200
Series FTD
on 7.4.1+

Note: Device Model Migration for 4110, 4120, 4140, 4150, SM24, SM36, & SM44 on 7.2.x is supported with FMC 7.6.1.

Policy Analyzer and Optimizer



- Security Cloud Control capability for cloud or on-prem FMC managed firewalls
- Expanded set of rule conflict and anomaly detection
 - Partially overlapping (Shadowed) and fully Redundant objects and rules
 - Expired time-based and unused (by hit count) 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



- Home
- Multicloud Defense
- Monitor
- Insights & Reports**
- Events & Logs
- Manage
- Policies
- Objects
- Security Devices

Overall Summary

Review the accumulative summary of the total policies and address the areas that need attention to ensure compliance and optimal performance.

14,045
Total Rules

Total 8,973 anomalies in 6,504 unhealthy rules [Rule Definitions](#)

Shadowed rules
4,296 ↗ 47.9%

Expired rules
414 ↗ 4.6%

Total overlap objects
816 ↗ 9.1%

Redundant rules
2,193 ↗ 24.4%

Mergeable rules
1,221 ↗ 13.6%

Partial overlap objects
33 ↗ 0.4%

Displaying 11 of 11 results Refresh

<input type="checkbox"/>	Access Control Policy	Devices	Total Rules	Observations	Analysis Status	Last Modified	Last Analyzed	Remediation Status	Remediation Time
<input checked="" type="checkbox"/>	Internal_ACP	0	12673	8562 48% C	Completed	10/14/2024, 06:00:07	09/15/2024, 10:02:33 Analysis out-of-date	Completed	10/14/2024, 06:00:11
<input type="checkbox"/>	[Redacted]	0	236	273 56% Op	Completed	10/24/2024, 2	09/15/2024, 10:02:33 Analysis out-of-date		
<input type="checkbox"/>	[Redacted]	0	124	117 78% Opt	Completed	09/15/2024, 0	09/15/2024, 10:02:33 Analysis up-to-date		
<input type="checkbox"/>	[Redacted]	0	1000	15 1% Optim	Completed	10/11/2024, 02	09/15/2024, 10:02:33 Analysis out-of-date		
<input type="checkbox"/>	testpolicy	0	9	5 55% Optim	Completed	09/11/2024, 0:	08/28/2024, 08:00:00 Analysis out-of-date	Completed	09/11/2024, 0:
<input type="checkbox"/>	access1	0	3	1 33% Optim	Completed	10/24/2024, 2	09/25/2024, 08:00:00 Analysis out-of-date		
<input type="checkbox"/>	Default Acces	0	0	0 Healthy	Completed	10/24/2024, 2	08/07/2024, 08:00:00 Analysis out-of-date		

Internal_ACP

Devices: 0

Total Rules: 12673

Observations: 8562 48% Optimizable

Analysis Status: Completed

Last Modified: 10/14/2024, 06:00:07

Last Analyzed: 09/15/2024, 10:02:33
Analysis out-of-date

Remediation Status: Remediations completed successfully

Remediation Time: 10/14/2024, 06:00:11

Hit Count Aggregation Status: Completed

Analysis Actions

- [View Analysis Details](#)
- [Download Analysis Report](#)
- [Re-analyse Policy](#)

Remediation Actions

- [Download Optimization Report](#)
- [Remediation History \(1 Version Available\)](#)

Policy Observation

We found a total of 8562 anomalies.

Duplicate Rules (6280)

FMC View: AI Interactive Assistant



The screenshot displays the Cisco Firewall Management Center (FMC) interface with the AI Assistant overlay. The background shows the 'Policy Editor' for an 'AC Policy' with a 'Prefilter Rules' tab selected. The AI Assistant window contains two interactions:

Interaction 1:
User: What airflow Secure Firewalls support?
AI Assistant (Today at 11:42 AM): Cisco Secure Firewalls (formerly known as Cisco ASA appliances) have standard airflow direction from front to back for cooling. This is the case across various hardware series including Firepower Series, Secure Firewall 3100 Series and the newly introduced Secure Firewall 1200. [1]
However, please verify this with the specific model documentation as it may vary. Information you should look for include the placement of air inlets and exhausts, the temperature operating range, and any specific environment requirements. [1]
Sources: 1. Secure Firewall Solutions
How this response was generated

Interaction 2:
User: How do I configure dVTI?
AI Assistant (Today at 11:43 AM): You can configure Dynamic Virtual Tunnel Interface (DVTI) by primarily creating a VTI interface on your Secure Firewall device. This can be done through the following procedure:
Step 1: Choose Devices > Device Management.
Step 2: Click the Edit icon next to the device on which you want to create a VTI interface.
Step 3: Choose Add Interfaces > Virtual Tunnel Interface.
Step 4: Select the Tunnel Type as Dynamic.
Step 5: Enter the name and description for the interface. By default, the interface is enabled. Ensure that you specify a name that is not longer than 28 characters.

At the bottom of the AI Assistant window, there is a text input field with the placeholder 'Ask the AI Assistant a question' and a blue arrow button. A link 'View User Guide to learn more.' is located below the input field.

Reduce Management Overhead with Cisco AI Assistant

Assist

+ Policy configuration

Augment

+ Troubleshooting

Automate

+ Policy lifecycle management

The screenshot displays the Cisco AI Assistant interface. At the top, it says "Cisco AI Assistant". Below that, a user message reads: "Allow Lee access to Facebook but only from office source zone". The AI Assistant responds at 11:05 am PST: "Here is your rule recommendation, This rule will be added in policy 'Test_1' in the category, 'Geo_Controls'". A table is shown with the following data:

Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

Below the table, there are icons for thumbs up, thumbs down, and a copy icon. The AI Assistant then sends a confirmation message at 11:05 am: "'Rule_Test_1' is successfully created in policy 'Test_1'". The message continues: "Congratulations, your rule named, 'Rule_Test_1' is successfully created in policy 'Test_1'. The rule is created in a **disabled state** as of now. You can enable it from your 'Test_1' policy detail page." A link "Go to policy detail page" is provided. At the bottom, there is a text input field "Ask the AI Assistant a question" with a blue arrow button to the right. A disclaimer at the very bottom reads: "The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more."

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
- Security Cloud Control 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: AI Ops and Insights

Shipping!

Capacity Planning of RAVPN

Predictable headend capacity that will stop capacity issues before they happen

Apply Best Practice Recommendations

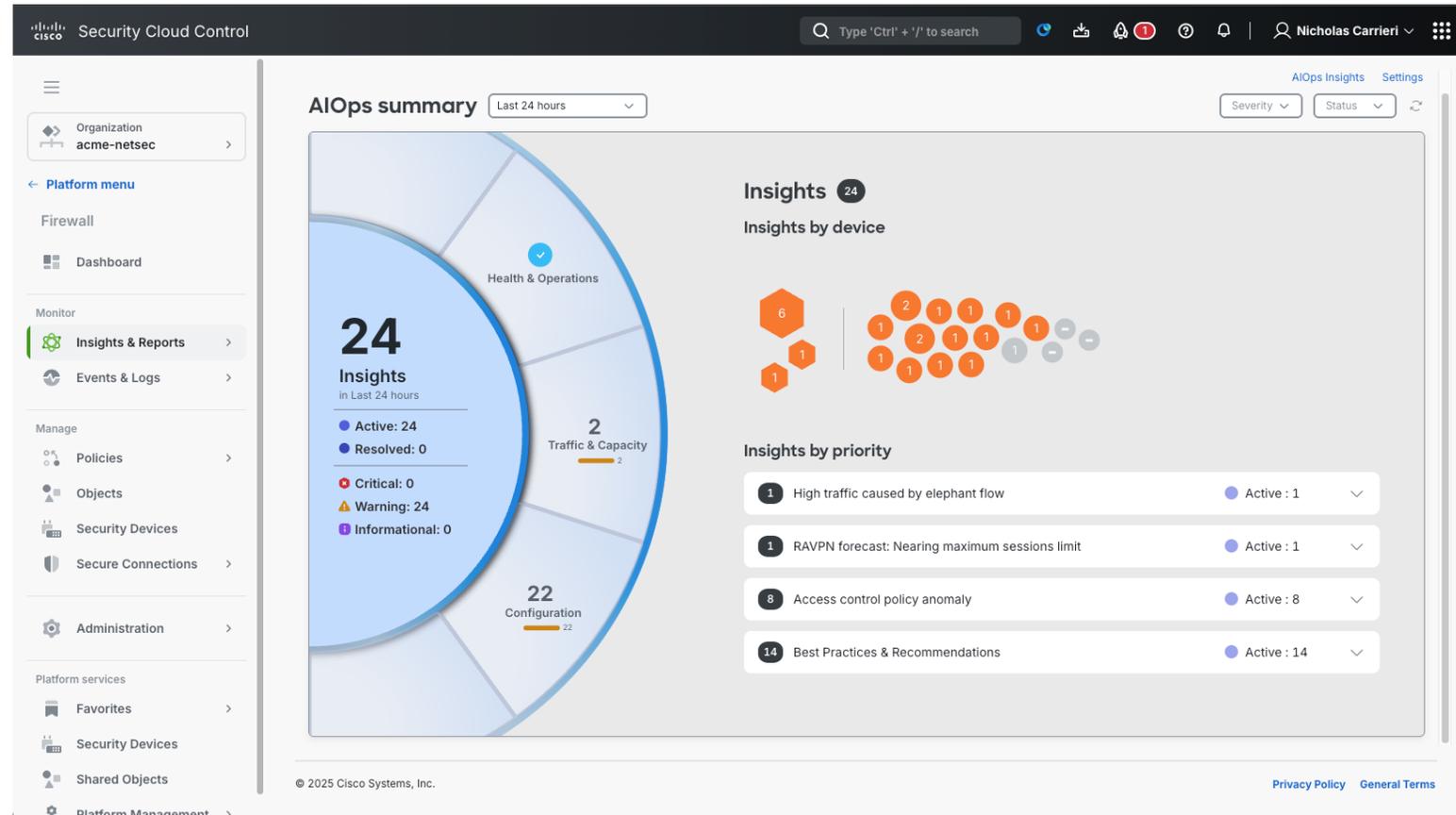
Hundreds of best practices applied in real time to your configuration from our TAC database

Gamify Feature Adoption

Easily adopt new features with guided walk throughs and a security posture score

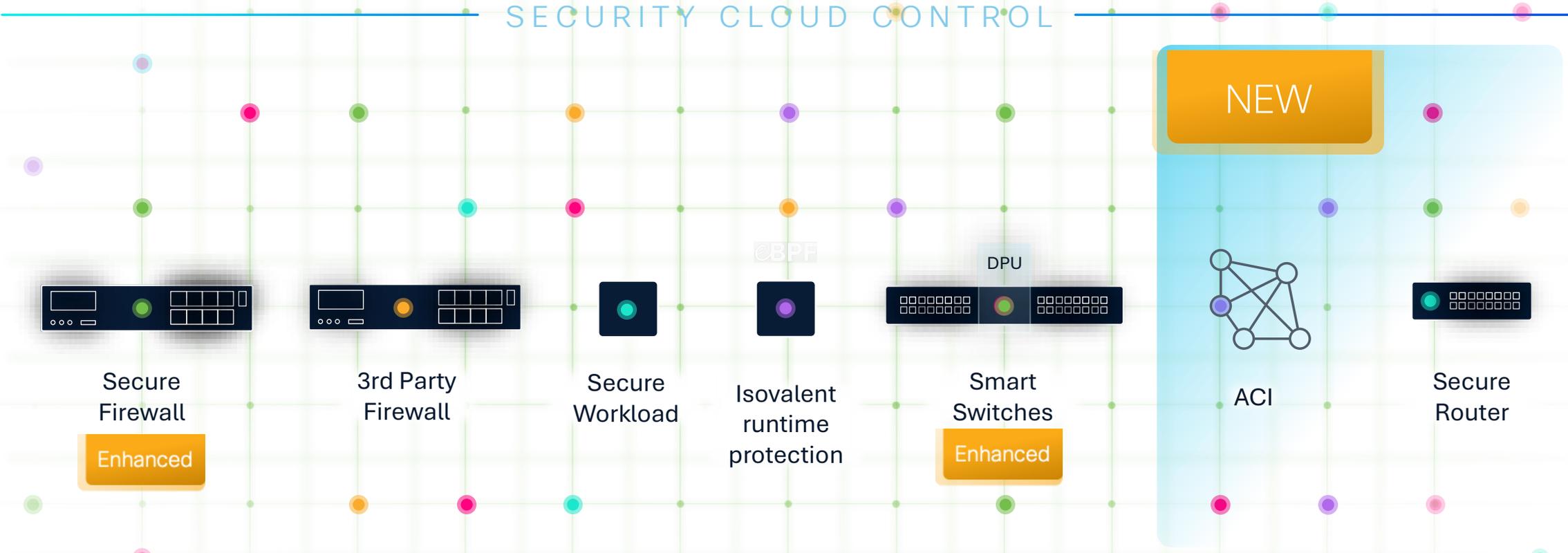
Reduce manual effort by 90%

Guided workflows ensuring a seamless upgrade experience



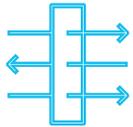
Workload

Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

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

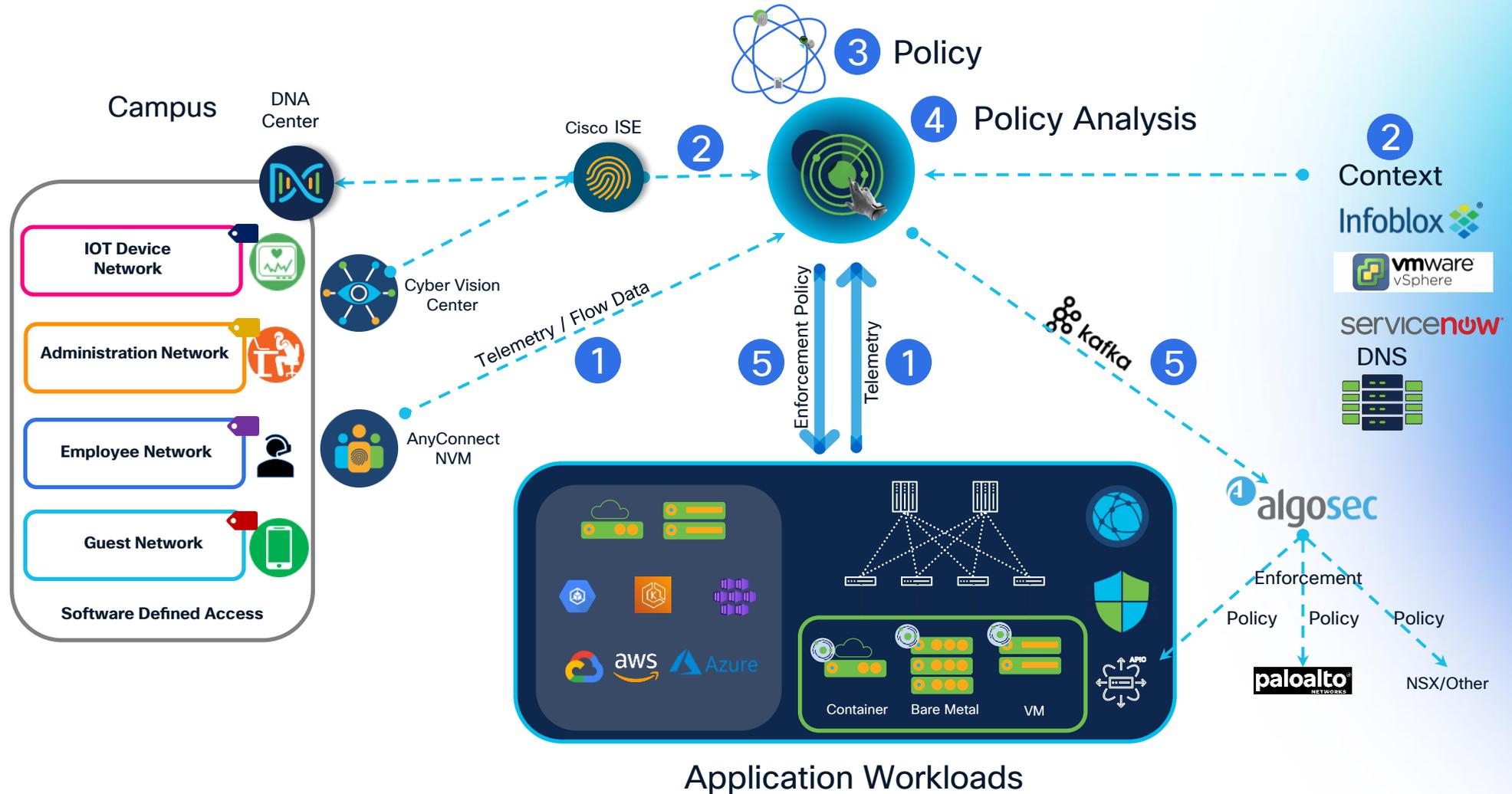
- Configure permissions once per user
- Manage access control/compliance auditing centrally, reduce potential for misconfiguration
- Take advantage of IDP integration and group mapping



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

Secure Workload Architecture



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

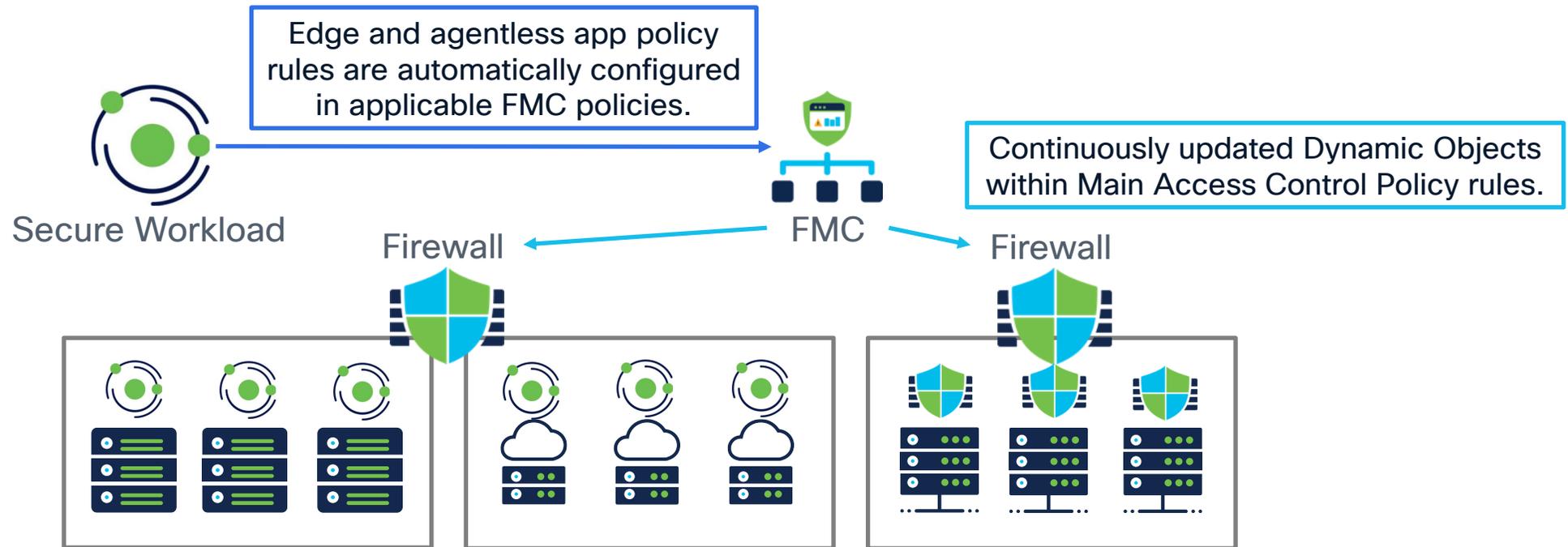


Hypershield

Secure Workload Policy Extension to Firewall

Workload
3.6+

- Hybrid cloud micro segmentation 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

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_	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_!	Allow

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

Application Virtual Patching

Workload
3.8

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

Edit External Orchestrator Configuration

Basic Config

Hosts List

Domains

Virtual Patching

Enabled Domain(s)

Global/DC-East-West

Select All

Remove All

Select Workloads

Default : EMEAR

DC

Approved file Shares

Critical Applications

Default:EMEAR:DC:DC-1:Applications

Default:EMEAR:DC:DC-2:HR-Invoice-App

Snort Rules Documentation

https://snort.org/search?query=1&submit_search=

Remove Vulnerabilities

Query

Single CVE or comma separate CVE

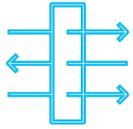
Bulk Removal (Upload CSV)

Connection will be tested after the update.

Cancel

Update

Better outcomes with Firewall Threat Defense



Better management

- Cloud or on-premises
- Tightly integrated with Cisco Security Portfolio
- SD-WAN Workflows
- AI Ops



Platform innovations

- Refresh of platforms across entire portfolio (low to high)
- Best in class performance
- Built for decryption



Best in class Threat Protection

- Simplified TLS Decryption
- QUIC Decryption and Inspection
- Snort ML
- Encrypted Visibility Engine



Hybrid Mesh Firewall Architecture

- Protection across physical, virtual, cloud and workloads
- Policy integrations across enforcement points
- Security Cloud Control central management

Conclusion

Cisco Security Beta Programs



Sign Up Now:

<https://cs.co/security-beta-nomination>

“I've been involved in many beta programs...I must say that this one has been the best organized. This beta takes a very active, hands-on approach.”

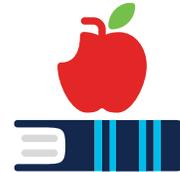
Higher-Ed Beta Customer



Early Feedback Programs



Beta Software Access



Product Training



Influence Product Roadmap



Presented by Security Customer Insights

Join our Security Research Community

Participating in design research gives you a place to share your thoughts and experiences to influence the future of Cisco Security Products.



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events 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

Contact me at: Insert preferred comms method

Thank you

CISCO Live !

