

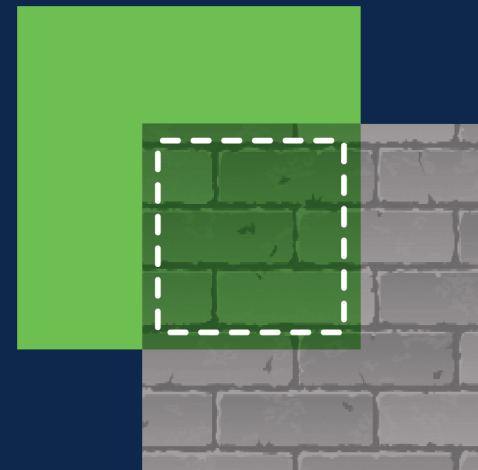
Cisco Secure Firewall

Netformers Firewall Roadshow

Przemysław Zawadzki przawadz@cisco.com

Channel Cybersecurity Technical Solutions Specialist

3rd October 2023

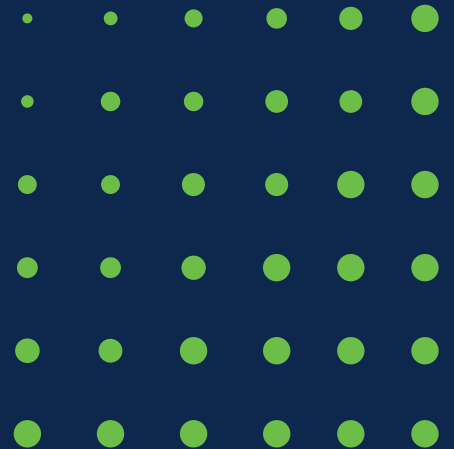


Agenda



- ▶ Overview
- ▶ Secure Firewall Physical Platforms
- ▶ Virtual Firewalls
- ▶ Secure Firewall Threat Defense (FTD)
- ▶ Consistent Policy and Visibility
- ▶ Secure Firewall Management Center (FMC)
- ▶ Cisco Defense Orchestrator (CDO)
- ▶ Security Analytics and Logging
- ▶ Integrated Security Portfolio
- ▶ Use Cases

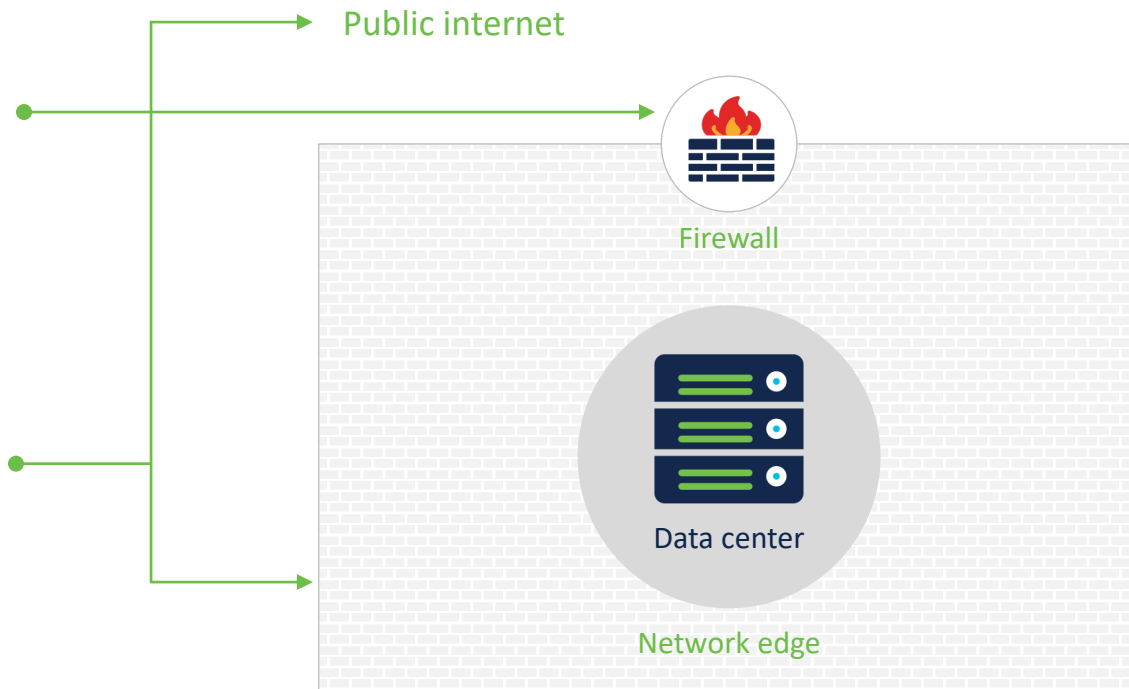
Overview



Traditional Network Security

One control point for all traffic

Internal traffic was considered trustworthy, and external traffic was untrustworthy



The New Reality

A one-size fits all approach has proved ineffective in today's landscape

Single control point is not adequate

Every environment needs its own micro-perimeter

Evolving form factor

Single control point replaced by multiple firewalls, both physical and virtual

Policy sprawl

Harmonizing policies across micro-perimeters is challenging



Management complexity

NetSec and IT use dozens of point products, each with its own management console

Evolving threat landscape

Security products need a continuous feed of threat intelligence to stay ahead of attackers

Firewall Validated Use Cases

Where can Cisco help?



Internet Edge



Data Center



Branch



Cloud/Virtual



Secure IPS



Remote
Access VPN

Why Cisco Secure Firewall?



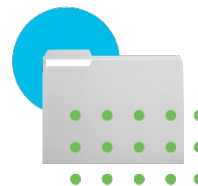
World-class security controls

Protect your workloads with a complete portfolio of Firewall solutions, backed by industry-leading threat intelligence.



Consistent policy and visibility

Streamline security policy and device management across your extended network and accelerate key security operations.



Integrated security portfolio

Extend network security beyond the firewall with malware protection, identity-based routing, multi-factor authentication, and more.

Cisco's Comprehensive Security Portfolio



World-class security controls

 Secure Firewall Threat Defense

 Secure Firewall ASA

 Talos



Consistent policies and visibility

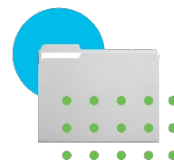
 Secure Firewall Management Center

 Secure Firewall Device Manager

 Cisco Defense Orchestrator

 SecureX threat response

 Secure Network Analytics



Integrated security portfolio

 Secure Workload

 Secure Access by Duo

 Secure Endpoint

 TrustSec

 Cisco Identity Services Engine

 Rapid Threat Containment

 Application Centric Infrastructure

World-Class Security Controls

Need: improve encrypted traffic performance and detect more sophisticated threats with a complete line of firewall solutions.



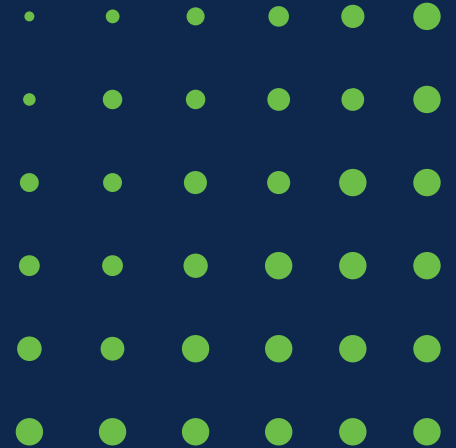
Cisco offering:

- **Stop more threats:** Contain known and unknown malware with leading Cisco® Advanced Malware Protection and sandboxing (Secure Malware Analytics).
- **Prioritize threats:** Gain superior visibility into your environment. Automate risk rankings and impact flags to quickly identify priorities.
- **Detect earlier, act faster:** Talos threat intelligence underpins the entire Cisco Secure ecosystem: if you own a Cisco Secure product, you're harnessing the power of Talos

Phasing Out FlexConfig

Firewall Management Center GUI Support (FlexConfig deprecated)	7.1	7.2	7.3	7.4
ECMP Zones	✓	✓	✓	✓
EIGRP, VXLAN Interfaces (VTEP/VNI)	-	✓	✓	✓
BFD for BGP, Cluster Health Settings, PBR Next-Hop Settings	-	-	✓	✓
FlexConfig Easy Migration to FMC for ECMP, EIGRP and VxLAN	-	-	✓	✓
NSEL (NetFlow Secure Event Logging)	-	-	-	✓

Secure Firewall Physical Platforms



Cisco Secure Firewall Hardware Portfolio

650 Mbps
AVC+IPS

1.5-2.2 Gbps AVC+IPS

2.3-20 Gbps
AVC+IPS

17-45 Gbps AVC+IPS
8 - 22.4 Gbps IPsec VPN
8 Node Cluster:
With 3140, up to
AVC+IPS(1024B) = 288 Gbps

Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS
Sixteen node cluster:
Up to 680 Gbps AVC
Up to 675 Gbps AVC+IPS

Stand-alone device:
70-150 Gbps AVC
70-145 Gbps AVC+IPS
Sixteen node cluster:
Up to 1.7 Tbps AVC
Up to 1.6 Tbps AVC+IPS

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS
Sixteen node cluster:
AVC+IPS
SM40*16n = 704 Gbps
SM48*16n = 830 Gbps
SM56*16n = 950 Gbps



1010



SMB



1120/40/50



Branch Office



2110/20/30/40



Mid Enterprise



3105/10/20/30/40



Large Enterprise



4112/15/25/45



Data Center



4215/25/45



Service Provider

NEW



9300 Series
SM-40
SM-48
SM-56

All appliances can run either ASA or FTD applications, FP9300 can run both on different SMs

Introducing the Cisco Secure Firewall 4200 Series



Superior Performance

- **Achieve High Performance Packet Processing** with powerful hardware, a wide range of high performing network interfaces with a 1 RU footprint.
- **Gain visibility** into encrypted traffic with crypto-accelerated architecture, speeding up TLS and IPsec decryption.

Outstanding ROI

- **Grow your security infrastructure** as your business grows with clustering capability of up to 16 firewall devices.
- **Ensure business uptime** with hot-swappable network modules, including fail-to-wire interfaces.

1RU, 16X clustering, 200G interface support, 2X interface module bays, dual SSD, dual mgt interface



Firepower Hardware Update

As the threat landscape evolves, our firewall portfolio does too. Gain more features and better performance at the same or lower price point.



Better performance

- Up to 3.5x boost in Firewall throughput
- Up to 5x boost in VPN throughput



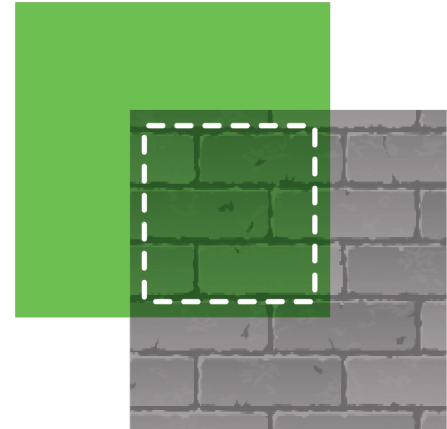
More connections

- Up to 2x more connections per second (CPS)



Improved encrypted traffic throughput

- Up to 3x boost in encrypted traffic performance



3100 and 4200 Series: Key Hardware Highlights



Crypto Acceleration

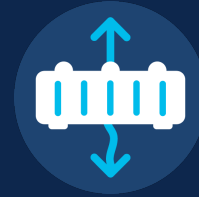
A specially built circuit to provide encryption/decryption acceleration

Crypto-acceleration using an FPGA (Field-programmable gate array)



Flow Offload

Flow offload engine processes packets in hardware up through layer 4



Interface Flexibility

Support for 1G,10G,25G,40G,100G,200G interfaces across 2 Network Modules



FIPS Compliance

Supports all FIPS 140-3 requirements

Firepower 1000 Series

Small business and branch office security with superior price/performance



Firepower 1010

- High-performance desktop firewall
- PoE, 8 10/100/1000 Base-T RJ45 switching ports
- Stateful firewall, AVC, NGIPS, AMP, URL filtering

650Mbps Firewall Throughput



Firepower 1120/40/50

- High-performance rackmount firewall
- 8 10/100/1000Base-T RJ45 switching ports, 4 1000Base-F SFP switching ports, 2 x 1/10Gbps SFP+ (1150)
- Stateful firewall, AVC, NGIPS, AMP, URL filtering

1120-1.5Gbps Firewall Throughput

1140-2.2Gbps Firewall Throughput

1150-3 Gbps Firewall Throughput

Cisco Secure Firewall 3100 Series

Make hybrid work and zero trust practical, with the flexibility to ensure strong return on investment

The new enterprise-class Cisco Secure Firewall 3100 Series supports your evolving world



Performance & Flexibility

Provide an exceptional hybrid work experience



Visibility & Enforcement

Keep the network from going dark and strengthen your zero-trust posture

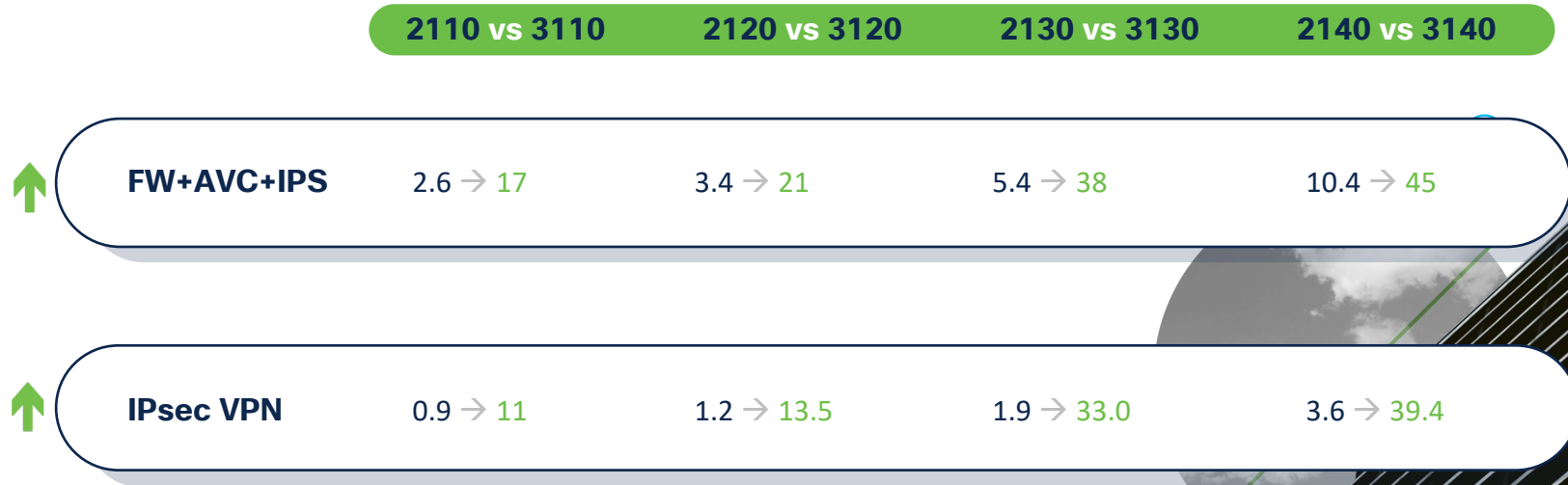


Efficiency & Simplicity

Advanced automation and integrations drive cost-savings for modern environments

Up to 3x performance boost

Secure Firewall 2100 Series vs. Firepower 3100



*Performance Estimates are in Gbps, subject to 1024B packet size, protocol type, and other networking variables.

IPSEC numbers for the Firepower 3100 series are with VPN Offload enabled.

Firepower 4100 Series

- Up to **50% performance improvement** over previous models
- Up to **44% higher TLS performance!**
- Supported software releases:
 - FTD 6.4+ – including multi-instance
 - ASA 9.12.1+
 - FXOS 2.6.1+

Enterprise and data center security with exceptional price/performance

Starting 7.3, 2X100G Netmod supported



Four new appliance models:
4112*, 4115, 4125, 4145
up to **47 Gbps** Firewall throughput**

* 4112 FXOS 2.8.1, FTD 6.6 or ASA 9.14.1

** 1024B FW+AVC+IPS

4200 Series Flexible Interface Architecture

- 2 x 1/10/25G Management Port
- 8 x built in 1/10/25 G SFP28 data ports
- 2 x netmod slots
 - Hot swappable
 - 1G, 10G, 25G, 40G,100G, 200G, 400G (Coming)
 - Fail to wire, standard



Firepower 9300 Service Modules

- Up to **80% performance boost** than previous generation SM
- Up to **33% higher TLS performance!**
- Supported software releases:
 - FTD 6.4+ – including multi-instance
 - ASA 9.12.1+
 - FXOS 2.6.1+



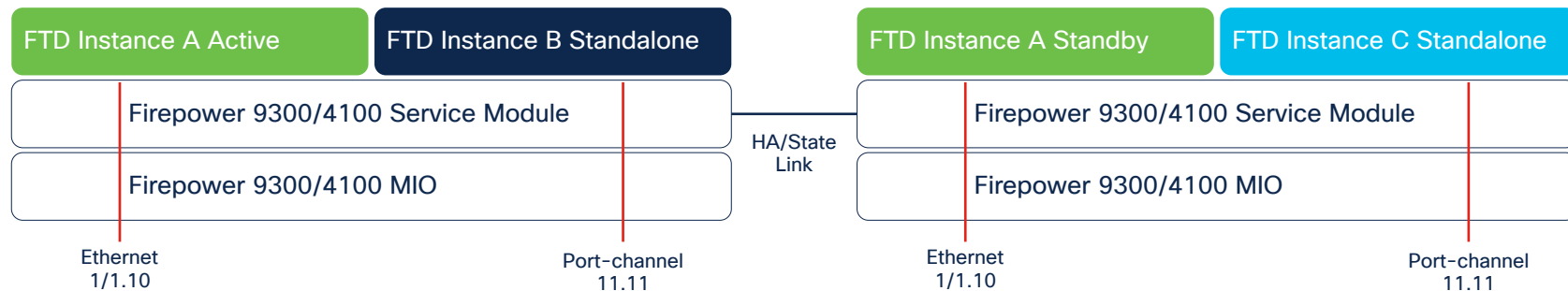
3 new 9300 SM models:
SM-40, SM-48, SM-56
up to **153 Gbps** Firewall throughput*

*1024B FW+AVC+IPS

Multi-Instance Expands Deployment Options

- Install multiple FTD logical devices on a single module or appliance
 - Container architecture
 - Instance failure does not affect other instances
- Allows tenant management separation, independent instance upgrade
- Supports HA between identical instances on different physical devices
- Example: 54 instances on a FPR9300 chassis with 3 x SM-56 modules
- Improved crypto acceleration in hardware

NEW

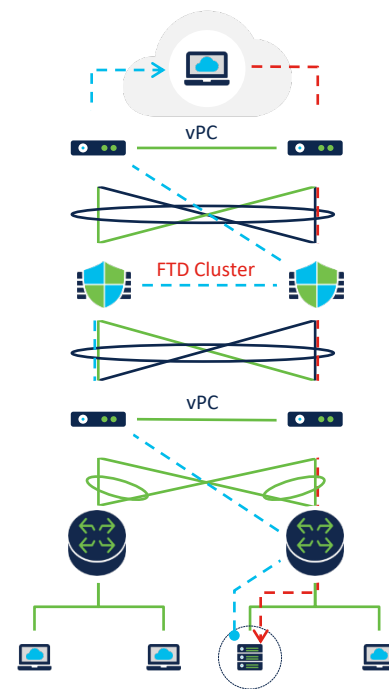


Clustering

Drive high return on investment while maintaining high availability

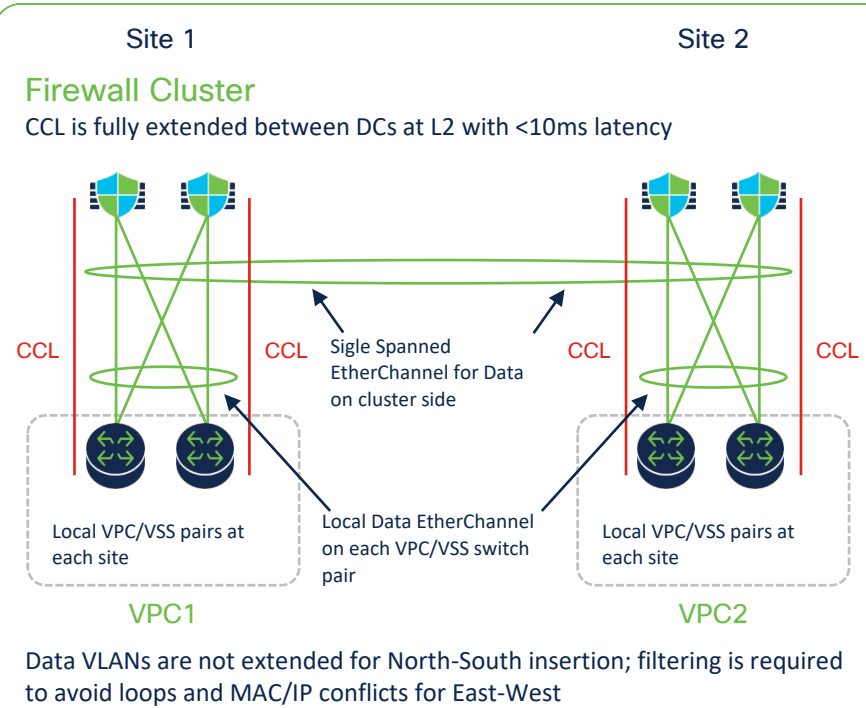
- Combine multiple devices to make a single scalable logical device
- Scale as you grow
 - Scale throughput, concurrent and new connection
 - Can span multiple datacenters
- N+1 resilience
- Handles asymmetric traffic seamlessly

Example: 16 node cluster
Upto 950 Gbps AVC+IPS

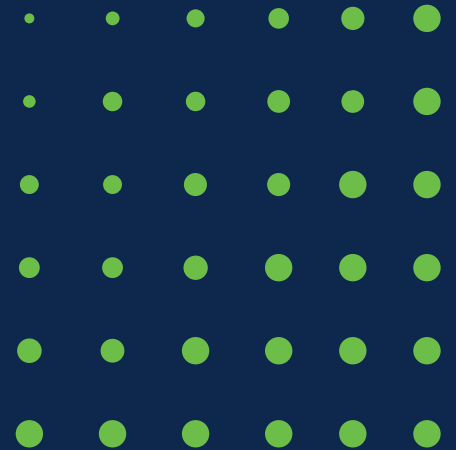


Multi-Site Data Center

- North-South insertion with LISP inspection and owner reassignment
- East-West insertion for first hop redundancy with VM mobility



Virtual Firewalls



Simplifying Multi-Cloud Environments

The image displays three panels representing different cloud environments supported by the product:

- Private Cloud:** Includes HyperFlex, NUTANIX, KVM, openstack, and vmware ESXi. A 'NEW' badge is present under NUTANIX.
- Public Cloud:** Includes aws, Google Cloud Platform, Microsoft Azure, rackspace technology, ORACLE CLOUD INFRASTRUCTURE, EQUINIX, Alibaba Cloud, and alkira. 'NEW' badges are present under EQUINIX, Alibaba Cloud, and alkira.
- Gov/IC Cloud:** Includes aws, Microsoft Azure, and Google Cloud Platform. A 'NEW' badge is present under Google Cloud Platform.

Virtual firewall performance-based licensing from 100Mbps up to 16Gbps

Cloud Leadership

Clustering & Auto Scaling

Integration with cloud native services & infrastructure

Accelerated Networking

Smart & Tiered Licensing

Dynamic Policy

Quickstarts, Infrastructure as Code and Automation

Gateway Load balancer integration

Snapshots

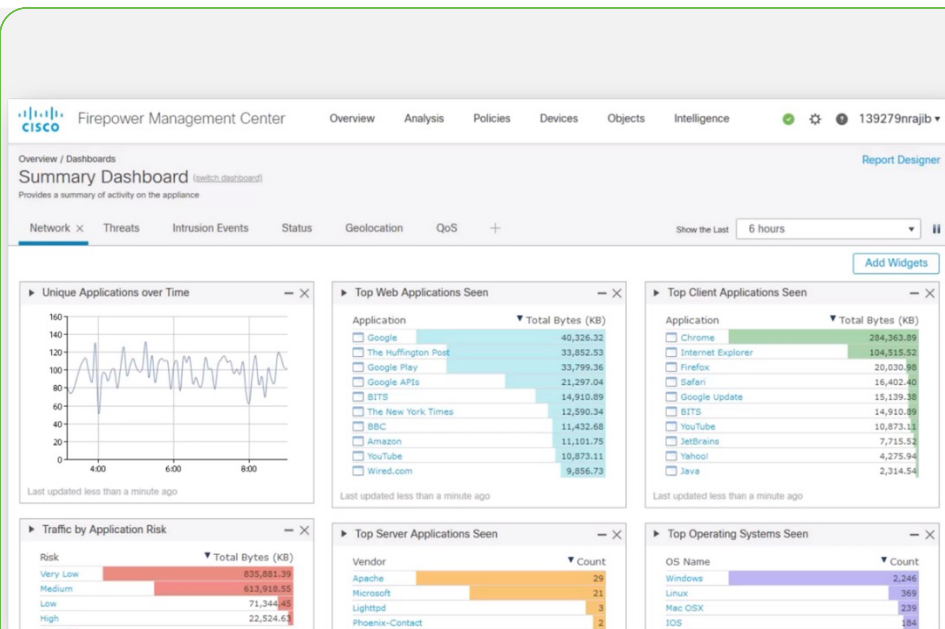
Smart Licensing Performance Tiers

- 7.0+ Evaluation mode and Smart License performance tiers
- Current perpetual BASE license moves to a subscription model

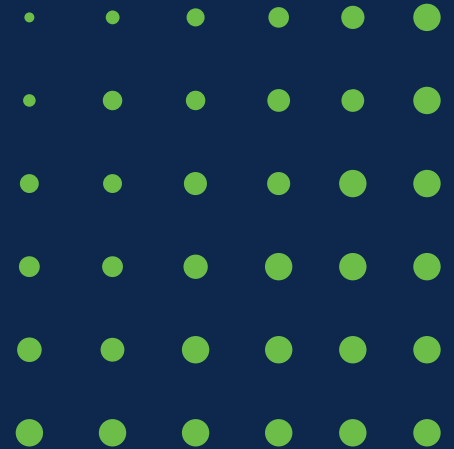
Performance Tier	Device Specifications	Rate Limit	RA VPN Session Limit
FTDv5	4 cores/8 GB	100Mbps	50
FTDv10	4 cores/8 GB	1Gbps	250
FTDv20	4 cores/8 GB	3Gbps	250
FTDv30	8 cores/16 GB	5Gbps	250
FTDv50	12 cores/24 GB	10Gbps	750
FTDv100	16 cores/32 GB	20Gbps	10000

FMC Virtual 300

- Up to **300 managed devices**
- **KVM and Azure support in 7.3**
- CPU: 2 x 8 cores, Memory: 64 GB, hard disk: 2.2 TB
- **Migrate easily** from one FMC model to another
- High Availability for on prem, AWS and OCI clouds – 7.1 or higher
- Supported software releases:
 - FTD 6.5 or higher – including multi-instance
 - FMC 6.5 or higher



Secure Firewall Threat Defense



What is Secure Firewall Threat Defense (FTD)?

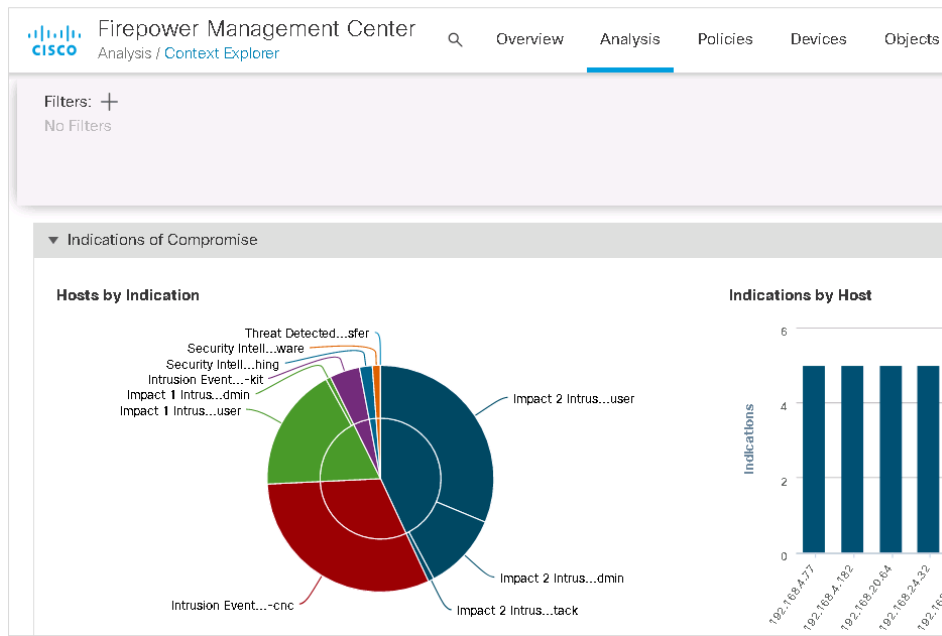
Delivers nearly 100% efficacy on blocking malicious flows and guards the network against threats

• Key Benefits

- Tenant management separation
- Scale as you grow
- Impact analysis
- Prioritize administration

• Features

- Firewall
- Intrusion Prevention
- Integrated TLS Decryption
- VPN
- Cisco Threat Intelligence Director
- Malware Continuous Analysis with Retrospection
- QUIC Fingerprinting



Release 7.3 Highlights

Threat Efficacy

- QUIC Fingerprinting
- MITRE support for Snort Rules
- Event Viewer shows MITRE ATT&CK Techniques

Device Management

- Improved Upgrade workflow
- Email Notification for Scheduled Jobs
- Dual ISP support for data interface management

Licensing

- Carrier License Support
- License Renaming [here](#)

SASE/Secure Access

- DVTI
- RAVPN Dashboard
- Umbrella Auto Tunnel Configuration
- Loopback Support for VTI and management services
- TLS 1.3 RAVPN

Virtual Deployment

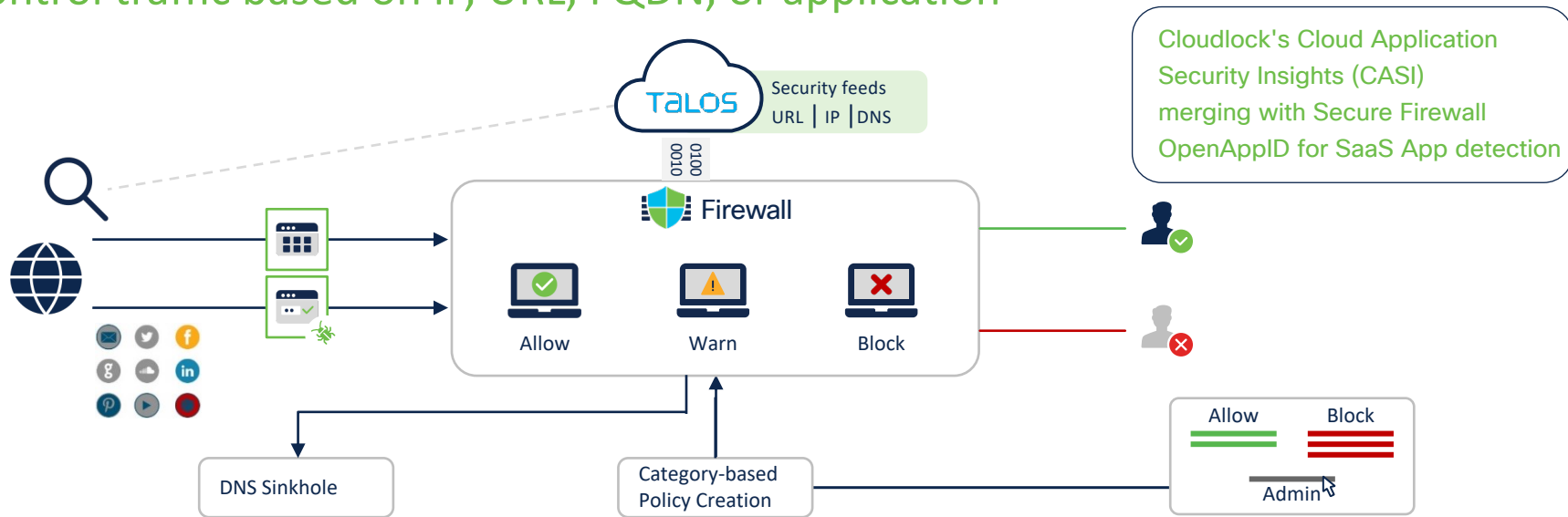
- Clustering Support with Gateway load balancer
- 6 node FTDv cluster in Azure
- IPv6 support validation for public and private cloud

Platform Updates

- Performance Profile for CPU Core allocation
- 3105 platform launch

Firewall Policy Powered by Talos and OpenAppID

Control traffic based on IP, URL, FQDN, or application



Security Intelligence:
Block latest malicious
IPs, URLs and FQDNs

AVC with OpenAppID:
Identify and control over
6,000+ pre-defined apps

AVC with OpenAppID:
Easily create custom
application detectors

URL Categories:
Classify **280M+** URLs
using **80+** categories




Secure IPS

Reduce the noise/volume of events and prioritize administration

Powered by Snort 3 – Best of breed, open source IPS

Firewall brings the power of context to IPS

Impact of IPS events can be deduced.

Impact flag	Administrator action	Why
1 	Act immediately, Vulnerable	Event Corresponds to vulnerability mapped to host
2 	Investigate, Potentially Vulnerable	Relevant port open or protocol in use but no vuln mapped
3 	Good to know, Currently Not available	Relevant port not open or protocol not in use
4 	Good to know, Unknown Target	Monitored network but unknown host
0 	Good to know, Unknown Network	Unmonitored network

Rule recommendation can tune IPS

Firepower Rule Recommendations

Security Level (Click tiles to select size)

Accept Recommendation to Disable Rules ⓘ

Increased Security - Enables additional rules that match potential vulnerabilities on discovered hosts based on the 'Security Over Connectivity' ruleset.

Protected Networks ⓘ

▼ Add +

Cancel Generate Generate and Apply

Snort 2 vs. Snort 3



	Snort 2	Snort 3
Multi-Threaded Architecture		✓
Capable of running multiple Snort Processes	✓	✓
Port Independent Protocol Inspection		✓
IPS Accelerators / Hyperscan Support		✓
Modularity – Easier TALOS contributions		✓
Scalable Memory Allocation		✓
Next Gen TALOS Rules – e.g., Regex/Rule Options/Sticky Buffers		✓
New and Improved HTTP Inspector – e.g., HTTP/2 support		✓
Lightweight content updates from TALOS		✓

Correlate Host Profile and IPS

Drive impact analysis and rule recommendations

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2020-04-07 13:51:40	2020-04-07 13:51:40



Impact flag	Administrator action	Why
1	Act immediately, Vulnerable	Event Corresponds to vulnerability mapped to host
2	Investigate, Potentially Vulnerable	Relevant port open or protocol in use but no vuln mapped
3	Good to know, Currently Not available	Relevant port not open or protocol not in use
4	Good to know, Unknown Target	Monitored network but unknown host
0	Good to know, Unknown Network	Unmonitored network

Firepower Rule Recommendations

Security Level (Click tiles to select size)

Accept Recommendation to Disable Rules

Increased Security - Enables additional rules that match potential vulnerabilities on discovered hosts based on the 'Security Over Connectivity' ruleset.

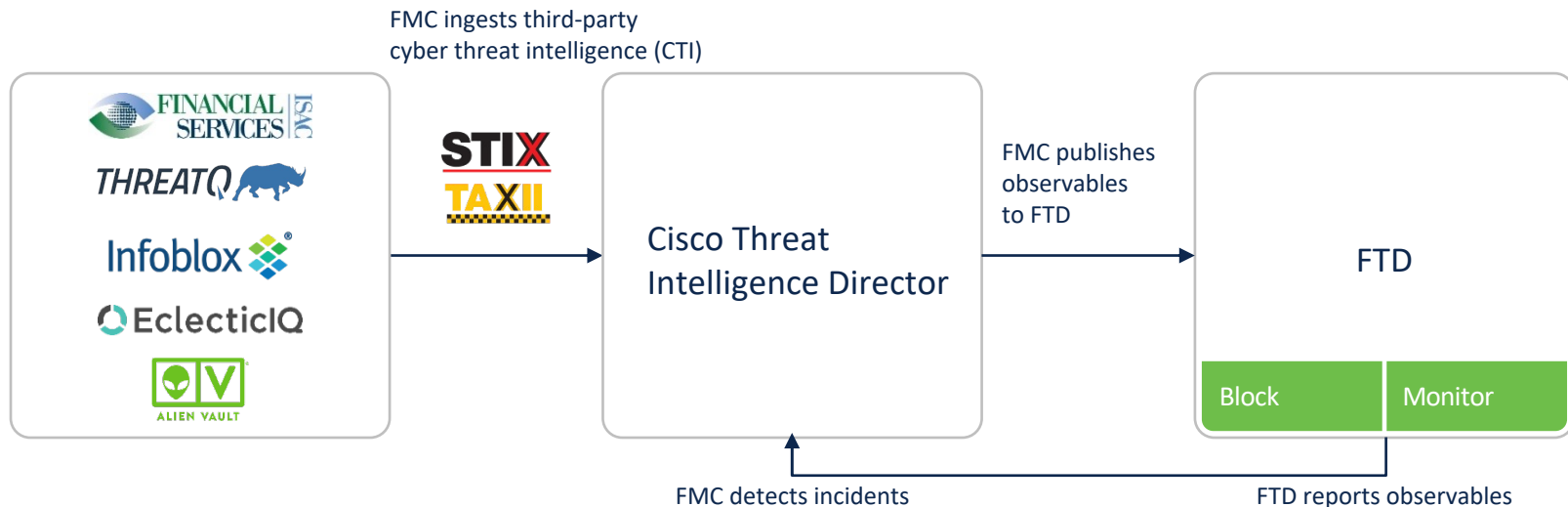
Protected Networks

Cancel Generate Generate and Apply

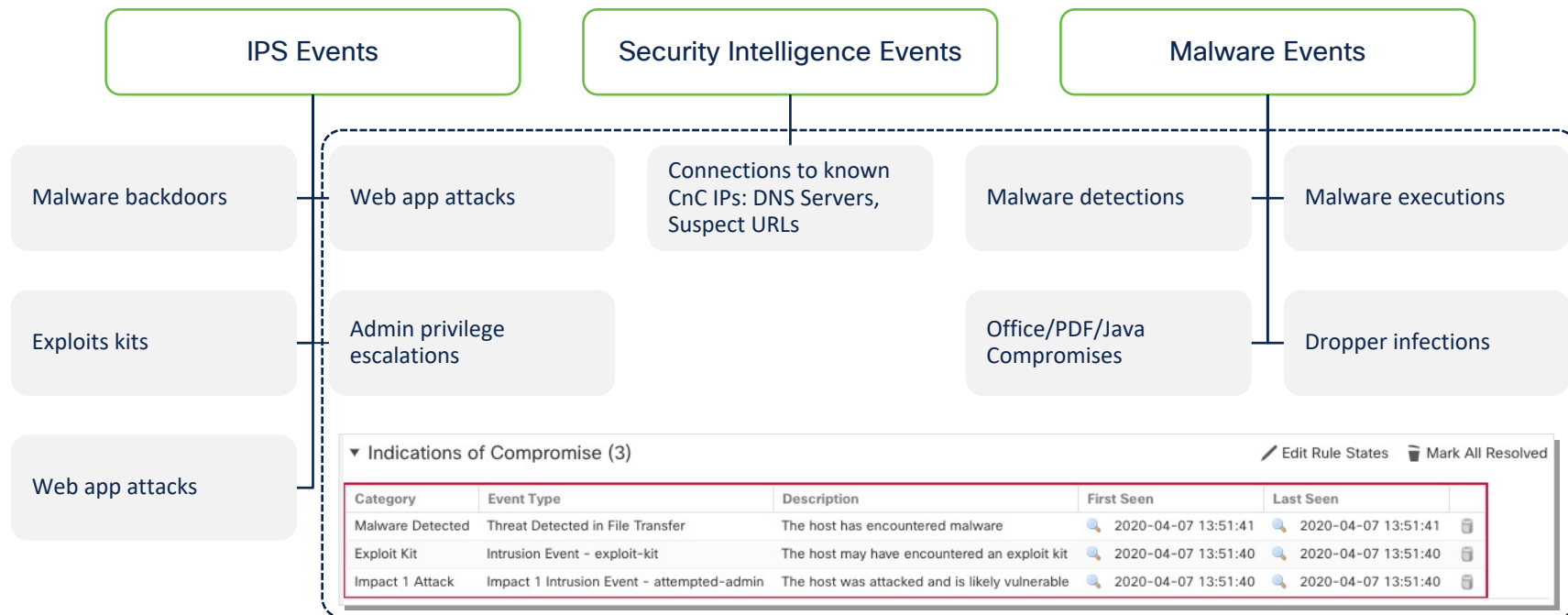
Cisco Threat Intelligence Director (CTID)

Support of open integration

- Extend Talos Security Intelligence with 3rd party cyber threat intelligence
- Parse and operationalize simple and complex threat indicators



Indications of Compromise (IoCs) Events

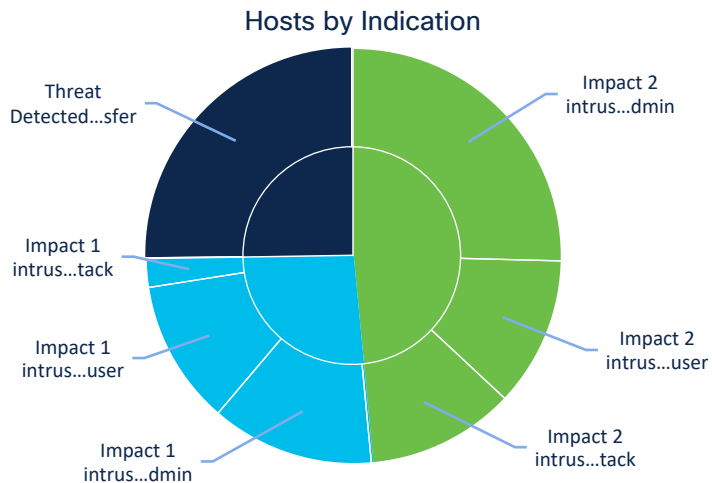


IoCs Facilitate Remediation

Facilitate understanding and remediation to reduce impact

- Identifies compromised and potentially compromised systems
- Take automatic action through **Cisco Rapid Threat Containment**

Indications of Compromise



The screenshot shows a "Host Profile" for IP 10.1.112.42. It includes details for NetBIOS Name, Device (FTD), MAC Addresses, Host Type, Last Seen, and Current User. Below this, a table titled "Indications of Compromise (3)" lists three events:

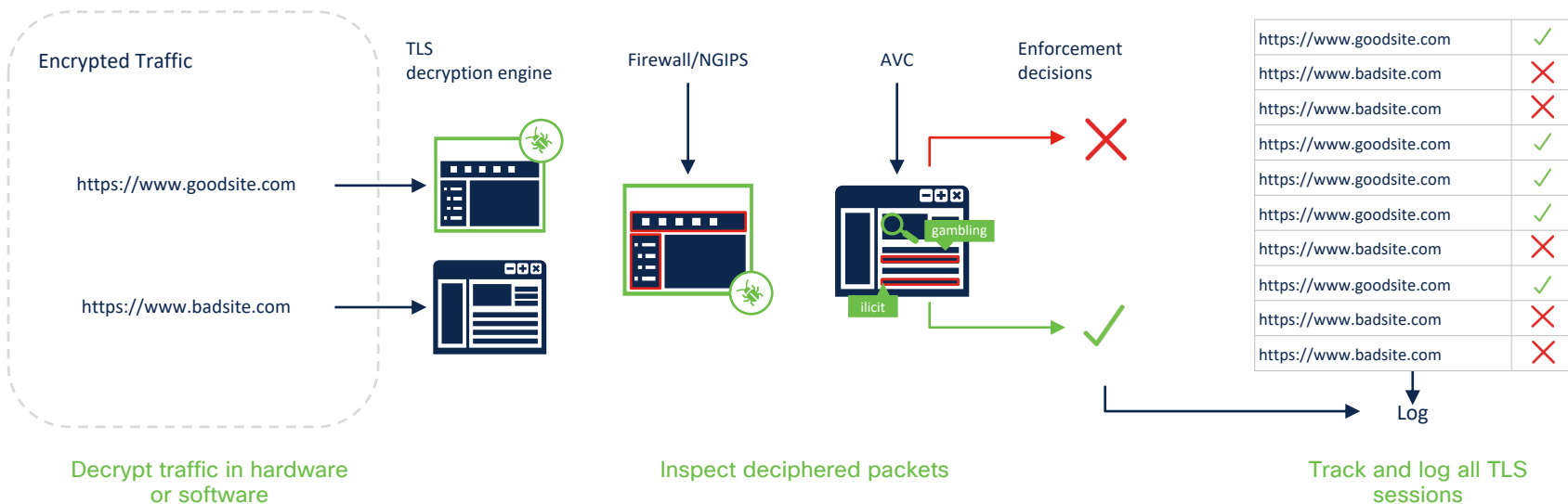
Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2020-04-07 13:51:40	2020-04-07 13:51:40

Below the table, the "Operating System" section shows: Vendor: Microsoft, Product: Windows, Version: Vista, 7, Server 2008, Source: Firepower. The "Applications (14)" section lists: BitTorrent, HTTP, and Internet Explorer.

Integrated TLS 1.3 Decryption

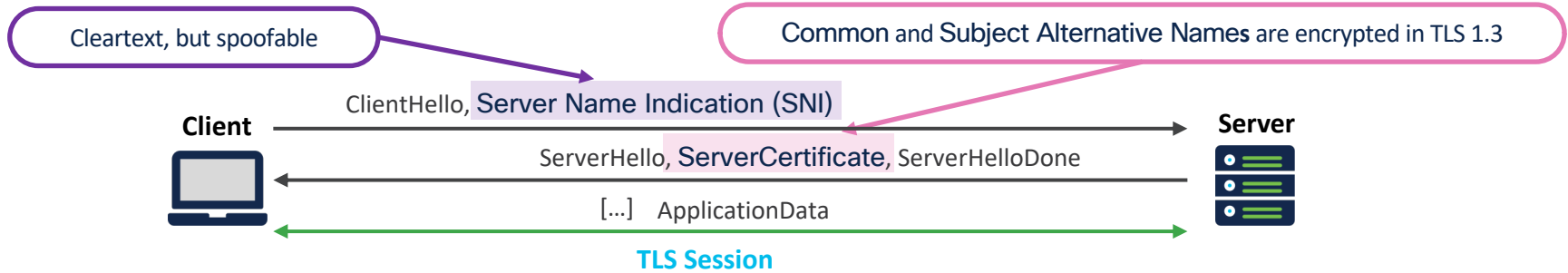
Finds encrypted threat while reducing performance impact

- TLS hardware acceleration delivers high-performance inspection of encrypted traffic
- Centralized enforcement of TLS certificate policies
 - Examples: Blocking self-signed encrypted traffic, specified TLS version, cypher suites

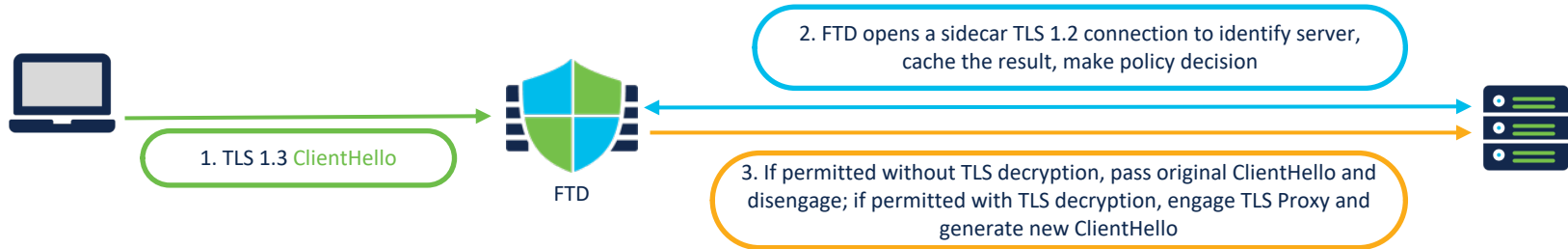


Fast App and URL Actions with TLS 1.3

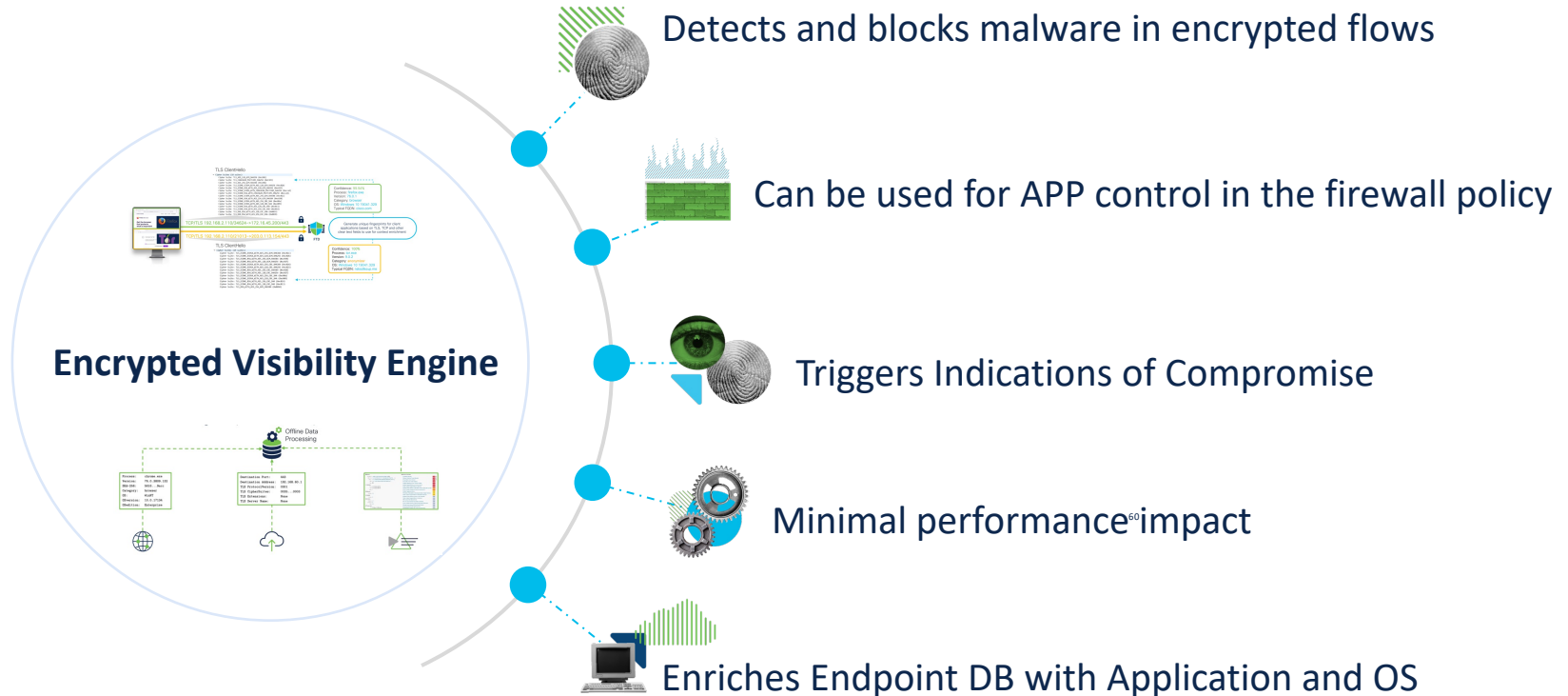
AVC, URL, and Decryption Policy decisions on pre-1.3 TLS header



TLS Server Identity Discovery without decryption since **FTD 6.7**

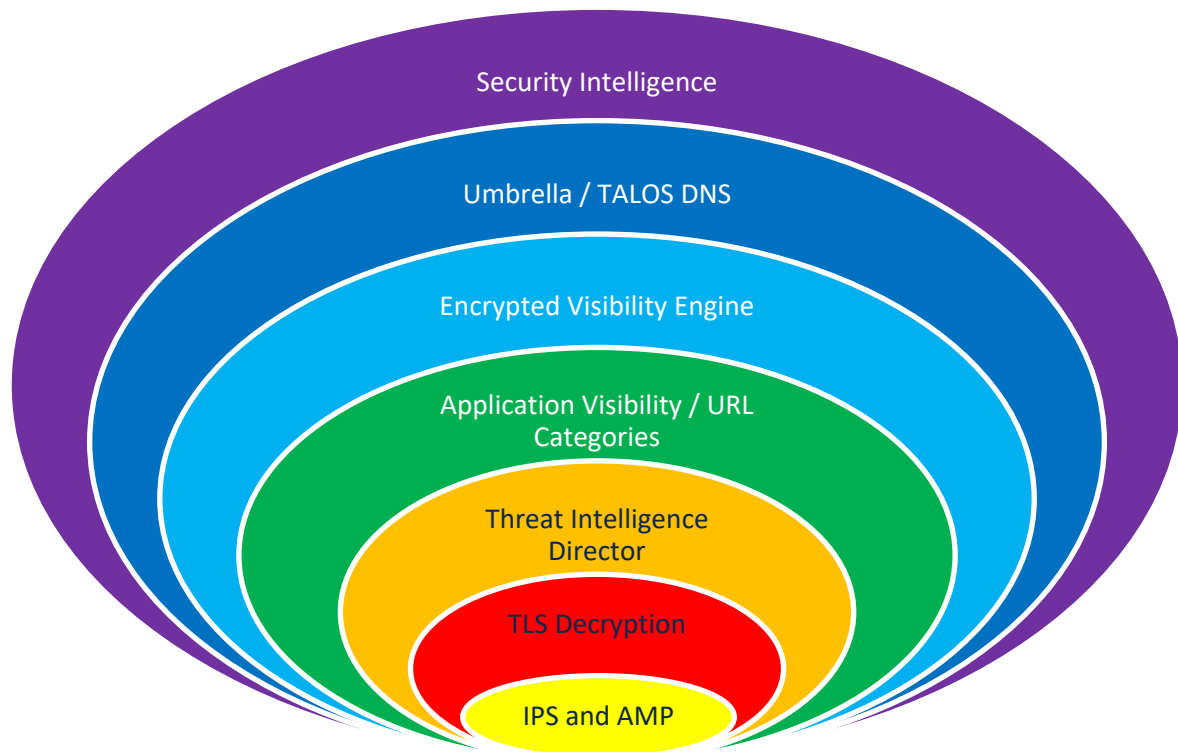


Encrypted Visibility Engine Benefits



EVE Empowers Defense-in-Depth with a New ML-Powered Line of Defense

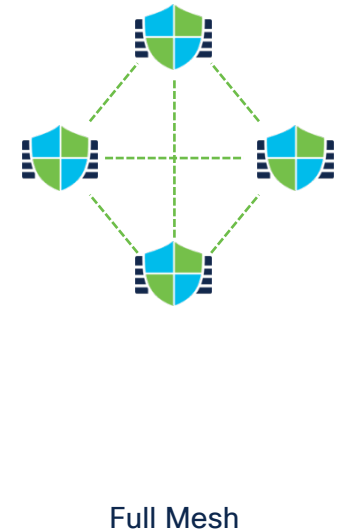
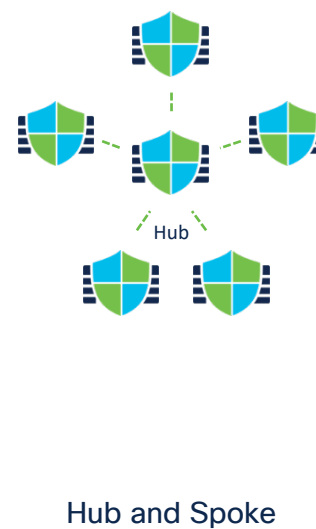
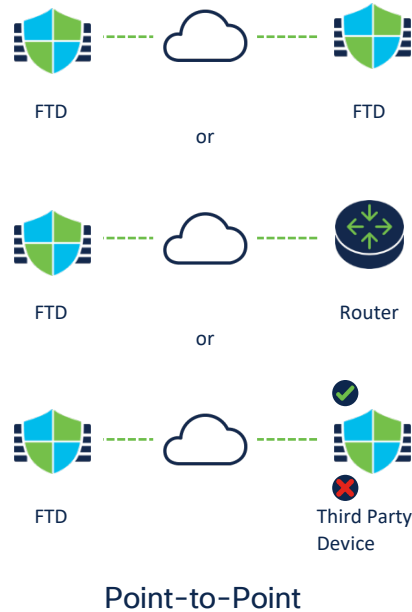
- EVE is a new player in the security features team
- Sifts out malware threats with minimal effort
- EVE reduce pressure on more resource-heavy functions
- It brings the best value when used as yet another layer of protection



Site-to-Site VPN

Easily and securely interconnect remote sites

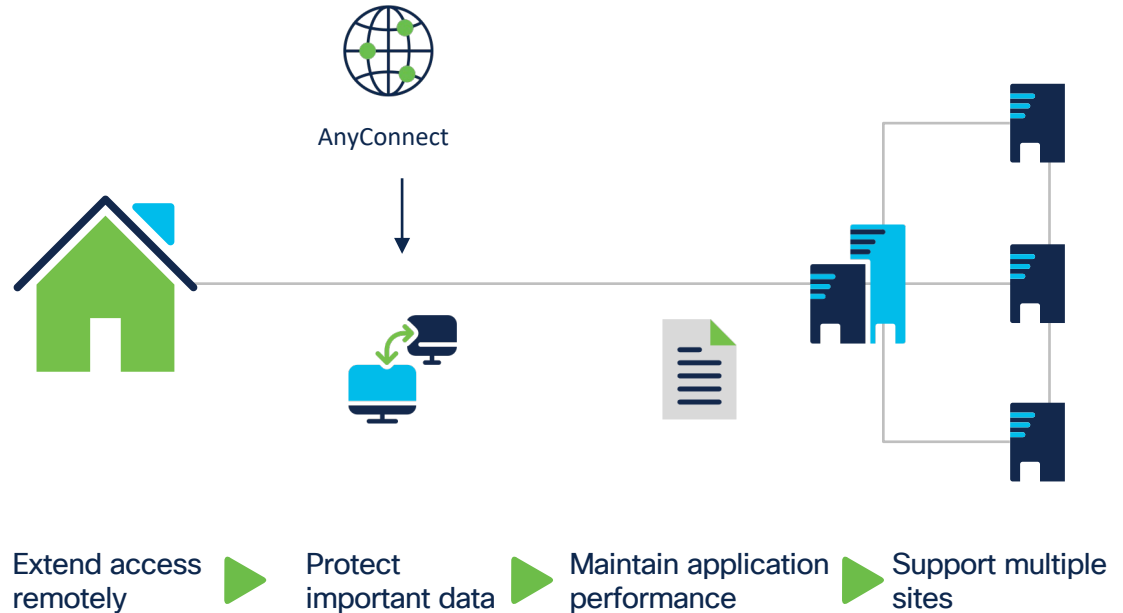
- IKEv1/IKEv2 policy-based VPN
- Easy topology-based management of VPN on multiple peers
 - Point-to-point
 - Hub and Spoke
 - Full Mesh
- Flexible authentication options – pre-shared key (automatic) and certificates



Remote Access VPN

Provide ubiquitous secure access from remote and roaming users

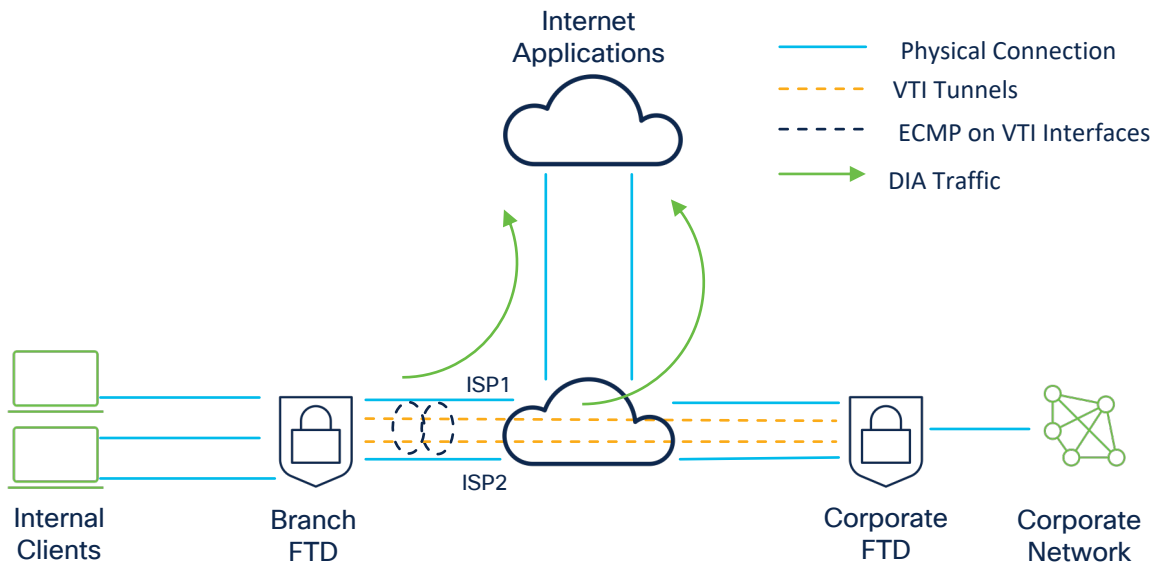
- Posture assessment
- Uses TLS, DTLS or IKEv2
- Easy wizard-based configuration
- Identity-based security policies
- Enhanced security with 2 FA/MFA provided by Secure Access (Duo)
- Passwordless Authentication
- Monitoring Dashboard
- TLS 1.3 support



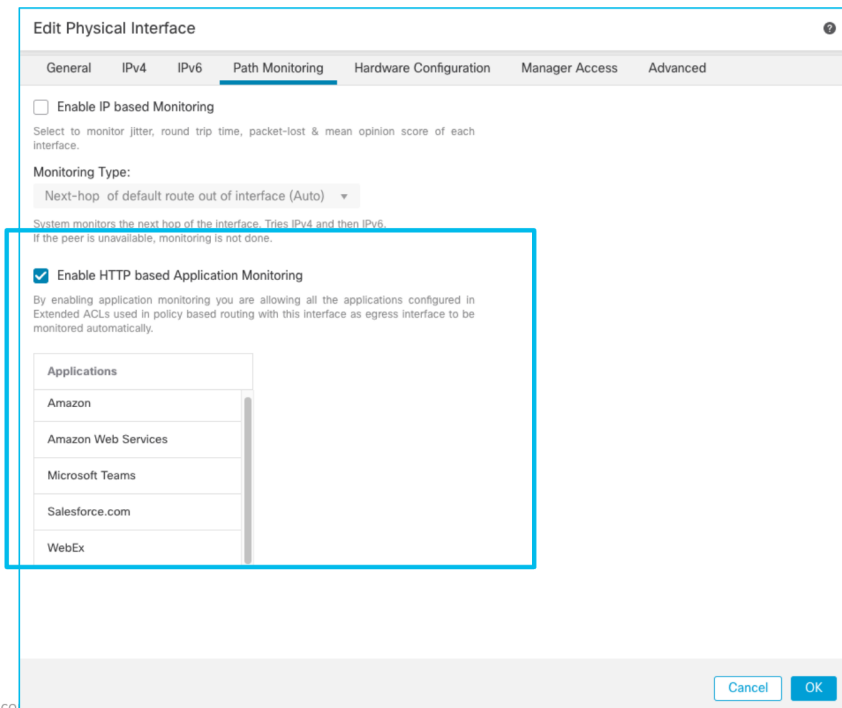
Simplified Branch

WAN Connect and Remote Branch Management

- Data Interface Management
- Intelligent Routing with Path Monitoring
- WAN PBR Path Monitoring
- Direct Internet Access
- Hub and Spoke DVTI
- Loopback Interface
- Auto-configuration rollback
- User Identity and SGT-based routing (in 7.4)



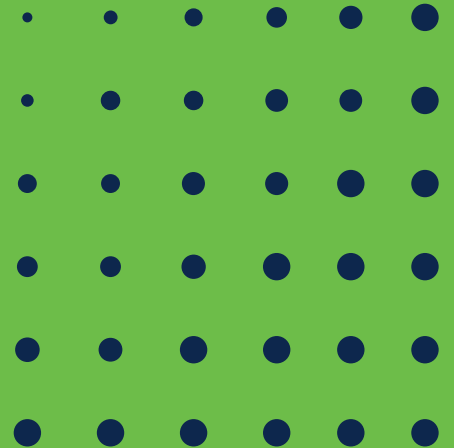
Enhanced Application Health Monitoring



- Under the Path Monitoring tab of Interface dialog, a new option to enable/disable HTTP-based Application Monitoring is added.
- A read-only view of the applications selected for Path Monitoring is also listed below the Enable option

FTD

New with 7.4



MITRE ATT&CK Support

- MITRE ATT&CK Tactics and Techniques provide a framework for descriptive categorization of IPS and Malware events.
- Snort3 Intrusion Policies include MITRE ATT&CK groups for signature tuning
- IPS and Local Malware Analysis events are now enriched with MITRE ATT&CK meta data making security incident investigation easier

Application Protocol ×	Client ×	Web Application ×	IOC ×	Detector ×	Message ×	File Policy ×	MITRE ×
Malware Detected by Local Malware Analysis						2 Techniques	
Malware Detected by Local Malware Analysis							
<input type="checkbox"/> HTTP	<input type="checkbox"/> Wget	<input type="checkbox"/> Cisco		SHA	Retrospective Event (Local Malware Analysis)	Block Malware	
<input type="checkbox"/> HTTP	<input type="checkbox"/> Wget	<input type="checkbox"/> Cisco		SHA, SPERO		Block Malware	
<input type="checkbox"/> HTTP	<input type="checkbox"/> Wget	<input type="checkbox"/> Cisco		SHA, SPERO		Block Malware	
<input type="checkbox"/> HTTP	<input type="checkbox"/> Wget	<input type="checkbox"/> Cisco		SHA, SPERO		Block Malware	
<input type="checkbox"/> HTTP	<input type="checkbox"/> Wget	<input type="checkbox"/> Cisco		SHA, SPERO		Block Malware	
<input type="checkbox"/> HTTP	<input type="checkbox"/> Wget	<input type="checkbox"/> Cisco		SHA, SPERO		Block Malware	
<input type="checkbox"/> HTTP	<input type="checkbox"/> Wget	<input type="checkbox"/> Cisco	Triggered	SHA		Block Malware	

MITRE Techniques

- ATT&CK Framework
 - Enterprise
 - Command and Control
 - Remote Access Software
 - Execution
 - User Execution
 - Malicious File

[Close](#)

The “Why” and “How” - MITRE ATT&CK Framework

Intrusion Prevention Group
(~1500 signatures)
reflecting **MITRE Framework**.

The “**Why**” – MITRE **Tactics**.

The “**How**” – MITRE **Techniques**.

The screenshot displays the Cisco Secure Firewall Management Center interface. On the left, the 'Group Overrides' section is visible, listing various MITRE ATT&CK Framework categories such as Execution, Exfiltration, Impact, Initial Access, Lateral Movement, Persistence, Privilege Escalation, Reconnaissance, and Resource Development. The 'Reconnaissance' group is highlighted in blue. A red dashed box highlights the 'Active Scanning' signature under the Reconnaissance group.

In the center, a text box states: "It is no longer only a signature **GID:SID 1:42785** – it tells you a “**story about the attack**”." A red arrow points from this text box to the 'Active Scanning' signature in the event log.

On the right, the 'Unified Events' section shows a table of events. The table has columns for 'MITRE ATT&CK' and 'Rule Group'. A red dashed box highlights the 'Active Scanning' technique under the 'Reconnaissance' tactic in the MITRE ATT&CK column.

Event ID	Time	Event Type	Source	Destination	MITRE ATT&CK	Rule Group
>	2022-06-10 15:02:32	Connection	security_intelligence	192.168.7.115		
>	2022-06-10 15:02:32	Intrusion	security_intelligence	192.168.7.115	1 Technique	1 Group
>	2022-06-10 15:02:32	Connection	security_intelligence	192.168.7.115	Enterprise	
>	2022-06-10 15:02:32	Connection	security_intelligence	192.168.7.115	Reconnaissance	
>	2022-06-10 15:02:32	Connection	security_intelligence	192.168.7.115	Active Scanning	1 Group
>	2022-06-10 15:02:32	Intrusion	security_intelligence	192.168.7.115		1 Group
>	2022-06-10 15:02:31	Connection	security_intelligence	192.168.7.115		
>	2022-06-10 15:02:31	Connection	security_intelligence	192.168.7.115		
>	2022-06-10 15:02:31	Intrusion	security_intelligence	192.168.7.115		1 Group

Encrypted Visibility Engine 7.4 Enhancements

The screenshot shows the configuration page for the Encrypted Visibility Engine (EVE). It includes several sections with toggle switches and a slider:

- Encrypted Visibility Engine (EVE)**: A toggle switch is turned on.
- Assign Client Applications to EVE-detected Processes**: A toggle switch is turned on. A red dashed box highlights this toggle.
- Enable Enhanced Analytics**: A toggle switch is turned on. A red dashed box highlights this toggle.
- Block Traffic Based on EVE Score**: A toggle switch is turned on. Below it is a sub-section for "Advanced Mode" with a toggle switch turned off. A slider is positioned between "High" and "Very High" on a scale from "Very Low" to "Very High". A red dashed box highlights the slider.

Red dashed boxes and arrows point from the callout boxes on the right to the corresponding configuration elements in the screenshot.

Decide if EVE engine be used for **client application detection**.

You can view **EVE fingerprints** in a new column Unified Event and cross-launch to appid.cisco.com for more details.

Specify acceptable EVE's confidence level for **blocking malware in encrypted flows**.

Viewing EVE Process Analysis

...and cross-launch to appid.cisco.com to check the **Process Analysis**.

You can view **EVE fingerprints** in a new column Unified Events...

Fingerprint **prevalance** across processes in EVE's dataset.

Destination context – SNI / IP / Port distribution in EVE's dataset.

Time	Event Type	Control Rule	Access Control Policy	Device	Encrypted Visibility Fingerprint	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
> 2023-05-22 10:05:43	↔ Connection	any Log	ACP	ftd.emelab.local	tls/1/(0303)(c02cc02bc030...	30%	microsoft networking	Medium	22%
> 2023-05-22 10:04:52	↔ Connection	any Log	ACP	ftd.emelab.local	https		code42 crashplan	Very Low	0%

Application Debug Log(Optional)

Server Name: v10.events.data.microsoft.com | IP Address: 20.42.65.84 | Port: 443

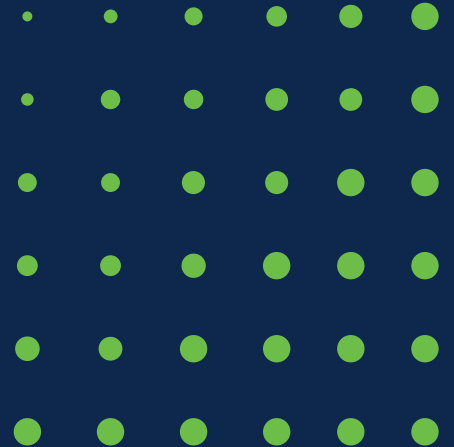
View Request To provide feedback about any of the processes from the list below, select the applicable entries and submit your request. If there are no results you can still submit your request.

Process Name	Prevalance	Server Name	IP Address	Port
<input type="checkbox"/> generic dmz process	0.4488	1.0000	0.8121	0.4545
<input type="checkbox"/> cisco amp for endpoints	0.2037	0.0000	0.0000	0.2086
<input type="checkbox"/> microsoft office	0.1388	0.0000	0.0029	0.1420
<input type="checkbox"/> microsoft networking	0.1382	0.0000	0.1846	0.1417
<input type="checkbox"/> cisco webex	0.0218	0.0000	0.0000	0.0224
<input type="checkbox"/> cisco anyconnect	0.0188	0.0000	0.0000	0.0000
<input type="checkbox"/> google services	0.0053	0.0000	0.0000	0.0054

Phasing Out FlexConfig

Firewall Management Center GUI Support (FlexConfig deprecated)	7.1	7.2	7.3	7.4
ECMP Zones	✓	✓	✓	✓
EIGRP, VXLAN Interfaces (VTEP/VNI)	-	✓	✓	✓
BFD for BGP, Cluster Health Settings, PBR Next-Hop Settings	-	-	✓	✓
FlexConfig Easy Migration to FMC for ECMP, EIGRP and VxLAN	-	-	✓	✓
NSEL (NetFlow Secure Event Logging)	-	-	-	✓

Consistent Policy and Visibility



Consistent Policy and Visibility

Need: stronger security policy management practices that can effectively protect the business at scale



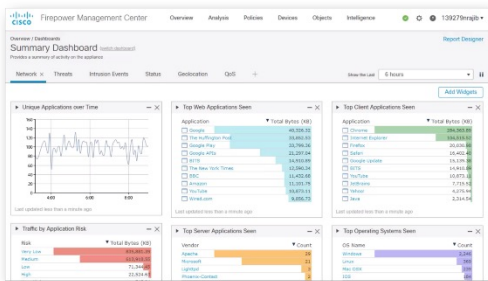
Cisco offering:

- **Maintain consistent policies:** Write a policy once and scale enforcement consistently across tens of thousands of security controls throughout your network.
- **Reduce complexity:** Get unified management and automated threat correlation across tightly integrated security functions, including application firewalling, NGIPS, and AMP.
- **Accelerate key security operations functions:** Leveraging existing resources and make the team more efficient by removing manual processes. Access security patches and new features faster by completing software image upgrades in a just a few clicks.

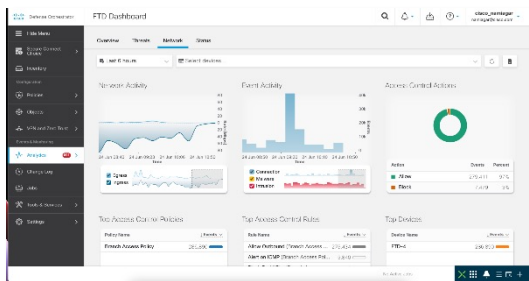
Management Designed for the User

Flexibility of cloud or on-premises options

Firewall Management
Center

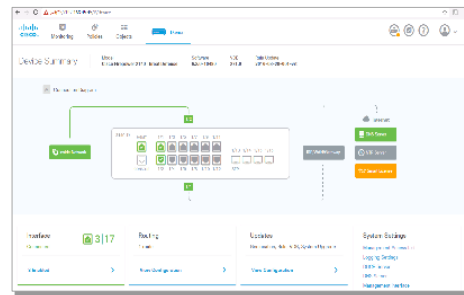


On premise centralized manager



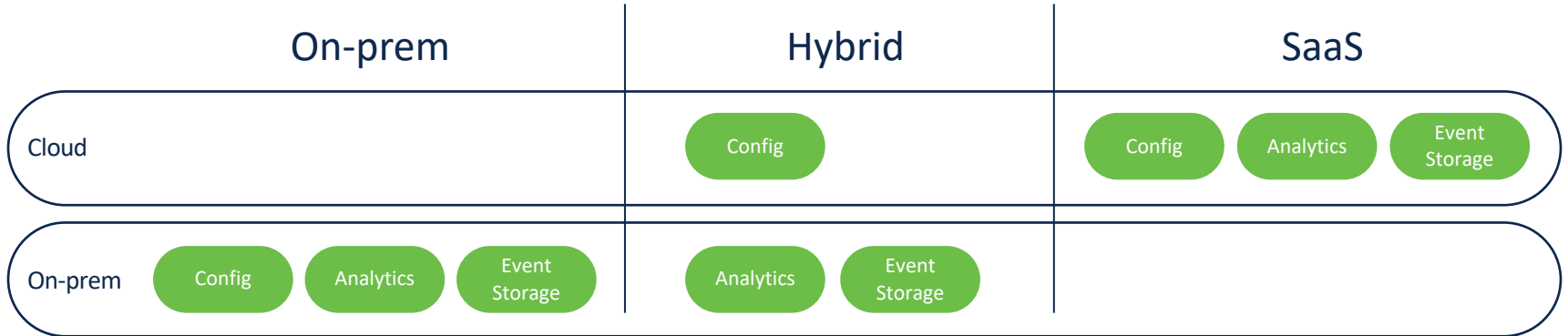
Cloud-delivered centralized manager via
Cisco Defense Orchestrator

Firewall Device Manager



On-box manager
NetOps focused

Flexibility of Management Consumption



- Driven by security concerns or regulatory compliance
- Government, financials

- Sensitivities around customer data
- Retail, financials

- Cloud-first approach
- Technology, startups

Increasing customer cloud acceptance



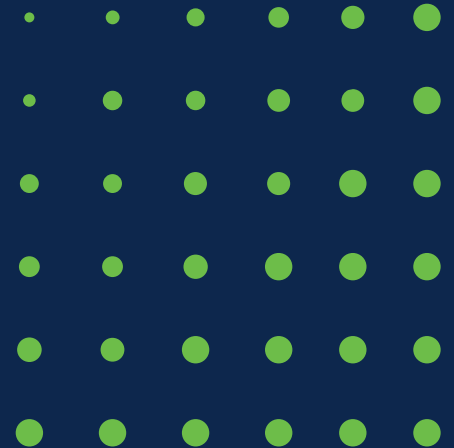
Management Platforms: When to Position?

Use case	Managers of choice	Details
Internet edge	Cloud-delivered or On-Prem FMC	<ul style="list-style-type: none">• Cloud-delivered for ease of use and netops users• FMC for advanced security analytics• Ask your customer about their priority
Enterprise branch	Cloud-delivered or On-Prem FMC	<ul style="list-style-type: none">• Choice of onboarding FTD through data interface or management interface• Low-touch onboarding
SMB / Small Business Edition	Cloud-delivered FMC	<ul style="list-style-type: none">• Cloud-delivered FMC eliminates the need for change management and update overhead• No rack space and utility bill, lowering operational cost
Data center Edge / Core	FMC	<ul style="list-style-type: none">• FMC supports clustering on 3100, 4100 and 9300, TrustSec
Campus fabric	FMC	<ul style="list-style-type: none">• FMC supports clustering on 3100 4100 and 9300, TrustSec
Firewall running in public cloud	Cloud-delivered or On-Prem FMC	<ul style="list-style-type: none">• FMC supports Firewalls running in public cloud
IPS only	Cloud-delivered or On-Prem FMC	<ul style="list-style-type: none">• FMC supports all the advanced IPS features and provides a separate interface from the Firewall

Logging Options: When to position?

Choice of Storage	Details	Benefits
Cloud	<ul style="list-style-type: none">• Available through an additional subscription of Security Analytics and Logging (SAL)• Unified Event Viewer and summary dashboard in Cisco Defense Orchestrator• Default storage of 90 days extendible up to 3 years• Additional Behavioral Analytics through the Security Analytics and Logging integration• Available in US, EMEA and APJC	<ul style="list-style-type: none">• Unified Event Viewer for ASA and FTD Events• Usage-based pricing• Correlate with telemetry from internal network and cloud logs in Secure Cloud Analytics• Higher storage capacity than on-prem storage• Can help reduce the cost of 3rd party logging solutions by sending only filtered or high-priority alerts from SAL
On-prem	<ul style="list-style-type: none">• Events sent from Secure Firewall to Management Center over sftunnel• Events are stored in FMC at no additional cost• Event Viewer and Analytics in FMC• Storage capacity dependent on the FMC model	<ul style="list-style-type: none">• Suitable for deployments with restrictions around storing data in the cloud• Familiar dashboard, reporting and workflows in FMC
Extended On-prem	<ul style="list-style-type: none">• Available through integration with Secure Network Analytics (SNA)• Events stored in FMC and SNA depending on retention configuration in FMC• Multiple storage capacity options using SNA clustered datastore• Event Viewer in FMC with easy configuration wizard and contextual cross launch from FMC	<ul style="list-style-type: none">• Unified log storage for ASA and FTD events• Exponentially higher on-prem storage capacity than the native storage capacity of FMC• Additional behavioural analytics powered by Secure Network Analytics• Correlate with telemetry from the internal network and on-prem sensor logs in Secure Network Analytics

Secure Firewall Management Center (FMC)



What is Firewall Management Center (FMC)?

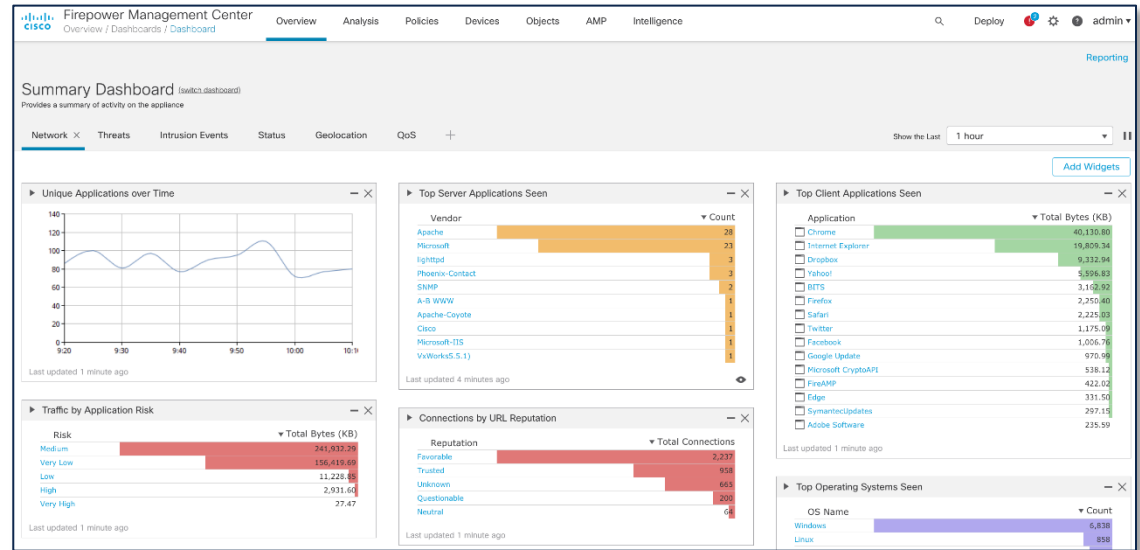
On-premise, centralized management for multi-site deployments

• Key Benefits

- Manage across many sites
- Control access and set policies
- Investigate incidents
- Prioritize response
- Available in physical and virtual options

• Features

- Multi-domain management
- Role-based access control
- High availability
- APIs and pxGrid integration
- Policy & device management
- Endpoint
- Security intelligence



Network Discovery

Provides the right data, at the right time, in the right format

- Discovers applications, users, and hosts through passive analysis of network traffic
- Provides context and helps determine the impact of attacks
- Tune IPS signature sets to devices discovered on the network
- Update host profiles with 3rd party vulnerability management integration

The screenshot displays the Cisco Secure Network Discovery interface, divided into several sections:

- Servers (3):** A table listing discovered servers with columns for Protocol, Port, Application Protocol, and Vendor and Version.

Protocol	Port	Application Protocol	Vendor and Version
tcp	139	pending	
udp	0	IGMP	
tcp	80	HTTP	
- Applications (1):** A table listing discovered applications with columns for Application Protocol, Client, Version, and Web Application.

Application Protocol	Client	Version	Web Application
NetBIOS-dgm	NetBIOS-dgm		
- User History:** A table listing discovered users with columns for Users and a date range (2020-01-12 11:31:21 to 2020-01-13 11:31:21).

Users	2020-01-12 11:31:21	2020-01-13 11:31:21
maik pennington (DCLLOUD-SOC\ypenn, LDAP)		
vicente vanbuskirk (DCLLOUD-SOC\pvamb, LDAP)		
maureen cepeda (DCLLOUD-SOC\iscepe, LDAP)		
diane tibbott (DCLLOUD-SOC\dtibbott, LDAP)		
chassidy francisco (DCLLOUD-SOC\mfran, LDAP)		
garth harrington (DCLLOUD-SOC\aharr, LDAP)		
eula gruber (DCLLOUD-SOC\egrub, LDAP)		
joy shanklin (DCLLOUD-SOC\jshah, LDAP)		
cherilyn spicer (DCLLOUD-SOC\lspic, LDAP)		
misty pagano (DCLLOUD-SOC\lpaga, LDAP)		
elmira ahih (DCLLOUD-SOC\cshih, LDAP)		
julian ibarra (DCLLOUD-SOC\oibarr, LDAP)		
laurine gibb (DCLLOUD-SOC\ygibb, LDAP)		
jaclyn parris (DCLLOUD-SOC\jparris, LDAP)		
takako collado (DCLLOUD-SOC\icoll, LDAP)		
collin carlson (DCLLOUD-SOC\lucarl, LDAP)		
lavenia cohn (DCLLOUD-SOC\lcohn, LDAP)		
rochell gaspar (DCLLOUD-SOC\rgasp, LDAP)		
- Host Profile:** A detailed view of a host profile with buttons for 'Scan Host' and 'Generate White List Profile'. It lists various attributes:
 - Domain: Global \ Cisco_Backend \ Cisco_SOC
 - IP Addresses: 10.0.10.151
 - NetBIOS Name: (empty)
 - Device (Hops): NGIPSv.dcloud.cisco.com (1), NGFWv.dcloud.cisco.com (128)
 - MAC Addresses (TTL): 00:0C:29:03:DF:AD (VMware, Inc.) (128), 00:0C:29:61:F5:5F (VMware, Inc.) (128), 00:10:45:CE:A7:2B (Nortel Networks) (128), ... (show all)
 - Host Type: Host
 - Last Seen: 2020-01-13 10:31:46
 - Current User: sean crowley (DCLLOUD-SOC\vcrow, LDAP)
 - View: [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)
- Indications of Compromise (1):** A table listing detected events with columns for Category, Event Type, Description, First Seen, and Last Seen.

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-01-13 07:39:38	2020-01-13 07:39:38
- Operating System:** A table listing discovered operating systems with columns for Vendor, Product, Version, and Source.

Vendor	Product	Version	Source
Microsoft	Windows	8.1	Firepower

Policy Management

Reduce complexity of policy maintenance

- Centralized on premise management across multiple Firewall platforms
- Integrates multiple security features into a single access policy
- Reduces manual configuration of policy through inheritance and template use.

The screenshot displays a web interface for managing network policies. The main title is 'Base_Policy'. At the top right, there are buttons for 'Analyze Hit Counts', 'Save', and 'Cancel'. Below the title, there are tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. The 'Rules' tab is active. The interface shows a search bar for 'Search Rules' and a 'Filter by Device' dropdown. A table lists several rules, each with columns for Name, Source Zone, Dest Zone, Source Network, Dest Network, VLAN Tags, Users, Applic..., Source Ports, Dest Ports, URLs, Source Set, Dest Set, and Action. The table contains 6 rows of rules, including 'Splunk Access', 'Block SSH for HR', 'Block Extranet11', 'Block ICMP Over GRE', 'Block Unaccept...', and 'Block Extra to In'. Each rule has a set of icons for actions like 'Trust', 'Block with...', and 'Add Rule'. At the bottom, there is a pagination control showing 'Displaying 1 - 11 of 11 rules' and 'Rules per page: 100'.

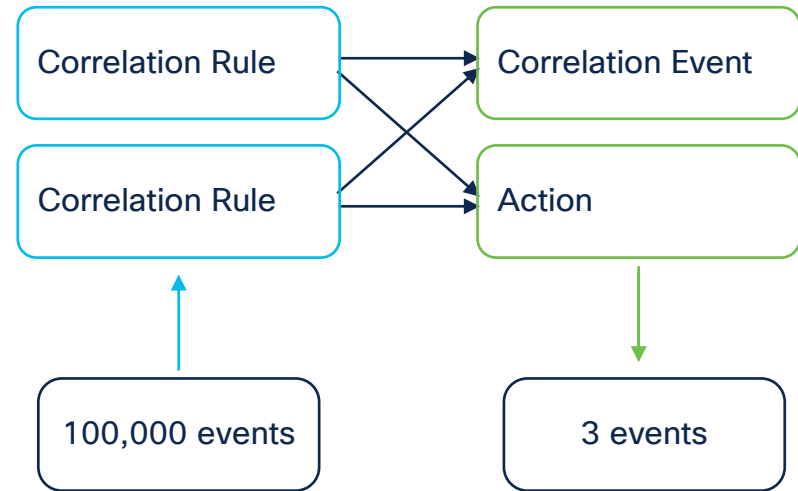
Name	Source Zone	Dest Zone	Source Network	Dest Network	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Set	Dest Set	Action
1 Splunk Access	OutZone	InZone	198.16.13	Splunknet	Any	Any	Any	UDP (172)8	Any	Any	Any	Any	Trust
2 Block SSH for HR	Any	Any	Any	Any	Any	dCloudRes	OpenSSH SSH	Any	Any	Any	Any	Any	Block with...
3 Block Extranet11	InZone	OutZone	Any	Extranet12	Any	Any	Any	Any	Any	Any	Any	Any	Block with...
4 Block ICMP Over GRE	GRE	Any	Any	Any	Any	Any	ICMP ICMP for IP	Any	Any	Any	Any	Any	Block with...
5 Block Unaccept...	Any	Any	Any	Any	Any	Any	Any	Any	Any	Pomograpl Adult (Any Gaming) Letters & Hate Sp...	Any	Any	Block with...
6 Block Extra to In	OutZone	InZone	Extranets	Infrastruct.	Any	Any	Any	Any	Any	Any	Any	Any	Block with...

FMC: Automate Security Response

Reduce the noise and connect the dots

- Correlate Security events
- Trigger automated response
 - Email
 - Syslog
 - SNMP
 - Remediation module
- Integration with Secure Network Access and other Cisco/3rd party products

Correlation Policy



Unified Event Viewer

The screenshot displays the Unified Event Viewer interface. At the top, it shows a search bar and a summary: "Showing 6,739 events (6,565 174)". The main table lists events with columns for Time, Event Type, Action, Reason, Source IP, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Code, and Web Application. An event at 2020-12-17 15:46:36 is highlighted in blue. A callout box labeled "1" points to this event, stating "True Correlation Clicking on the Intrusion Event highlights the associated Connection Event".

A second callout box labeled "2" points to a detailed view of the selected event. This view shows the following details:

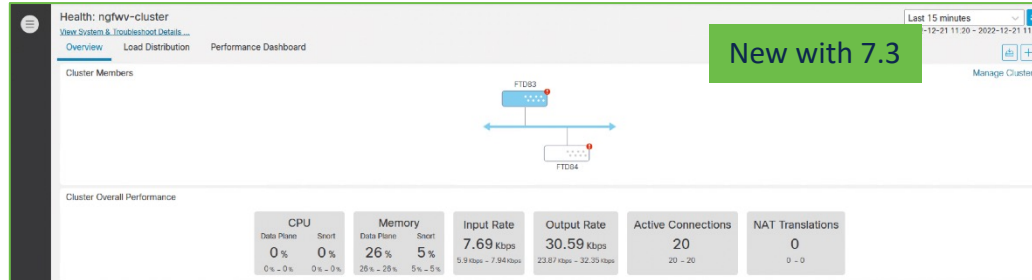
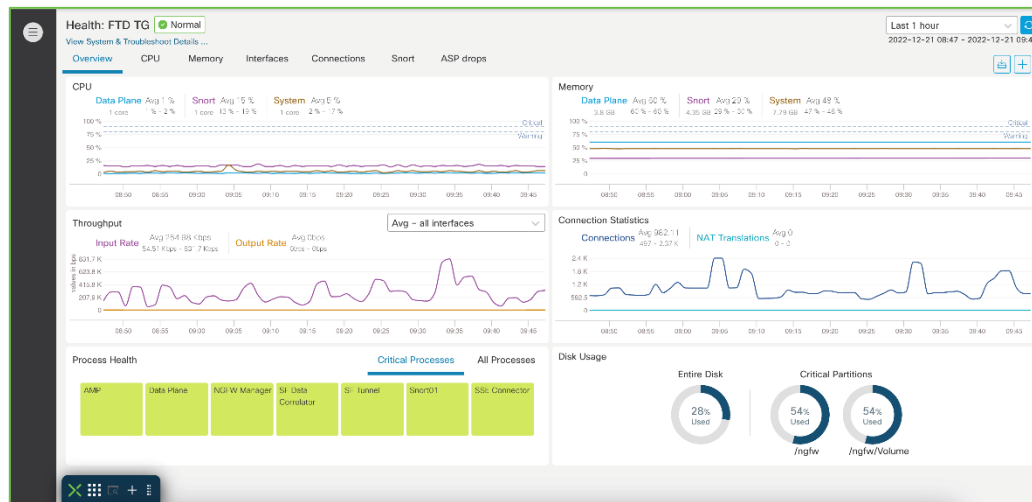
- Source IP: fe80::29b:47ff:fe21:c9d1
- Initiator User: Not Found
- Destination IP: ff02::16
- Ingress Security Zone: SZ_in
- Egress Security Zone: SZ_Out
- Source Port / ICMP Type: 143 (Multicast Listener Discovery v2 reports - RFC 3...
- Destination Port / ICMP Code: 0 / ipv6-icmp
- Application Protocol: ICMP for IPv6
- Application Protocol Category: network_protocols/services
- Client Application: ICMP for IPv6 client

The detailed view also shows a list of related connection events at the bottom, with a callout box labeled "2" pointing to the top row of this list, stating "Expand rows to view all details".

True Correlation
Clicking on the Intrusion Event highlights the associated Connection Event

Health Monitoring Dashboard

- FMC and Managed Firewalls
- All deployment modes – standalone, NGIPS, HA, Cluster
- Custom Health Stats
- Overall Cluster Stats added in 7.3
- Power Supply Monitoring for 4100/9300 in 7.3



VPN Monitoring Dashboard

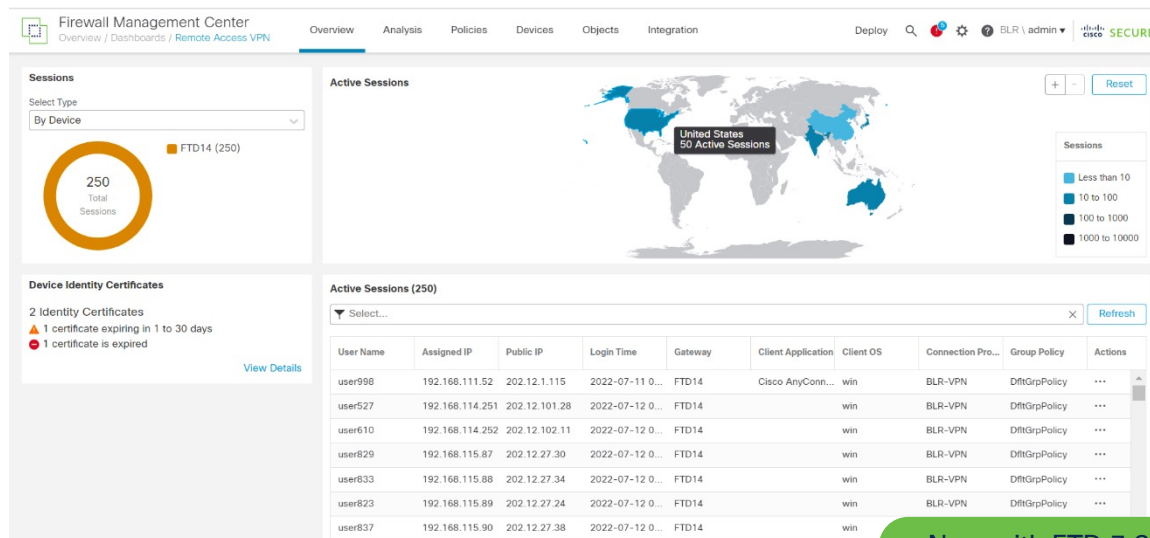
Application aware firewall policy enforcement, path selection, and decryption

DEPLOYMENT SCENARIO

- Mid to Large VPN deployment base
- Monitor user activity and session details
- Capacity Planning and availability statistics

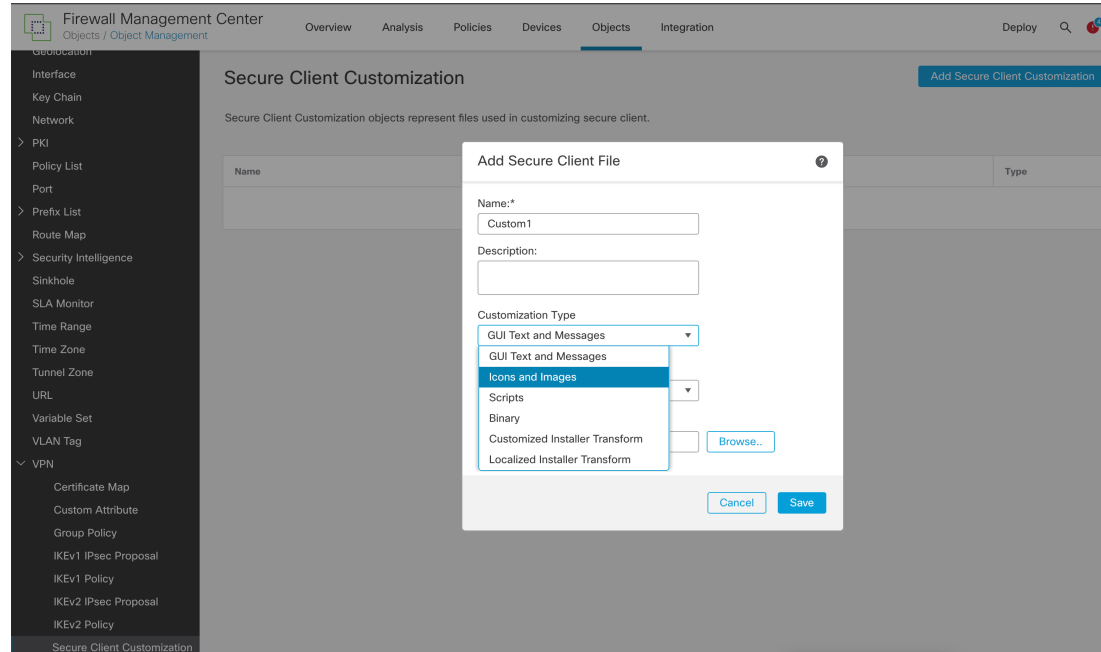
BENEFITS

- Consolidated Dashboard
- User Geolocation info
- Analytics for the deployment base, such as common workstation OS platforms
- Terminate one or all VPN sessions for upgrade planning



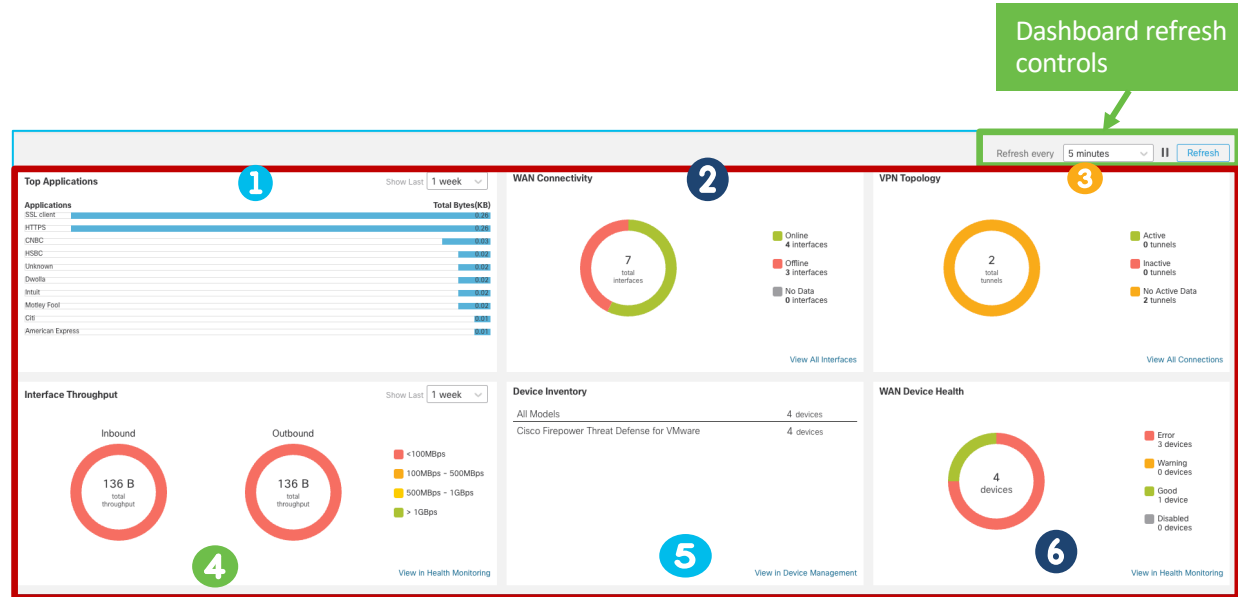
Anyconnect customization

- Customization of
 - GUI Text and messages
 - Icons and Images
 - OnConnect/Disconnect Scripts
- Works with Cisco Secure Client (Formerly AnyConnect)



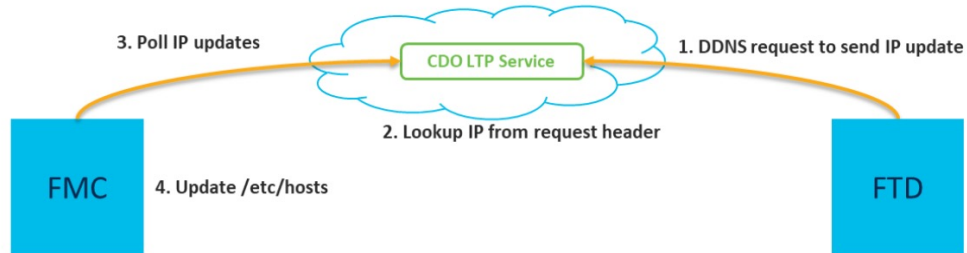
WAN Summary Dashboard

- The overall health of the Firewalls in WAN topology
- Application Bandwidth Consumption Data
- Inventory of Devices part of WAN topology
- Detailed View in Health Monitoring



WAN Summary Widgets

Low Touch Onboarding to On-prem FMC



Add Device ✕

Select the Provisioning Method

Registration Key
 Serial Number

Step 1 : Create SecureX and Cisco Defence Orchestrator (CDO) accounts
 SecureX and CDO are cloud services that are required for serial number onboarding. If you don't already have accounts, perform the following
 a. Create a SecureX user. [Learn more](#)
 b. Request a CDO tenant. [Learn more](#)

Step 2 : Integrate the management Center with SecureX
 SecureX Integration is required to add an on-prem management center to CDO. [Secure X Integration](#)

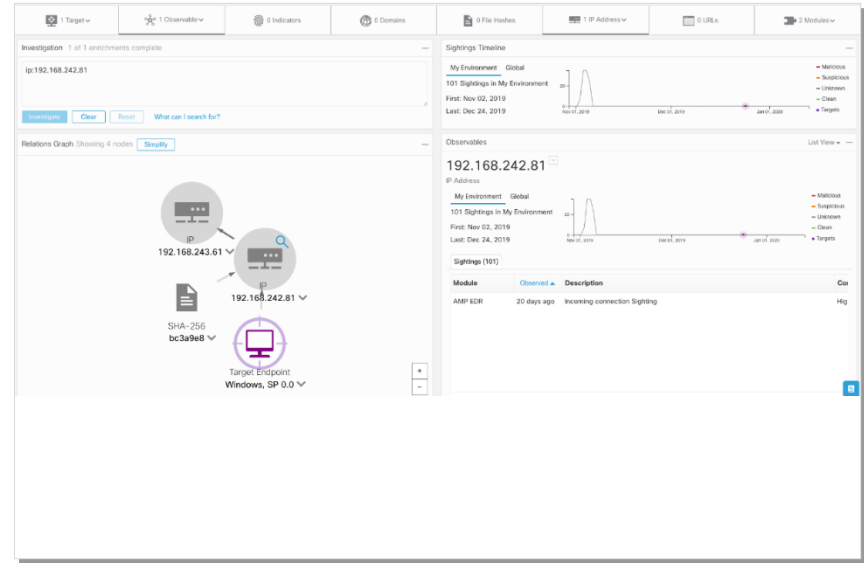
Prerequisites are complete. Click **Register** to launch CDO to register using the serial number

Cancel Register

FMC Integrations

Visibility and analytics beyond network discovery

- Close integration of FMC with Secure Endpoint
- Standards based threat indicators (STIX/TAXII)
 - Cisco Threat Intelligence Director (CTID)
- Drive down TTR with broad detection and collation
 - SecureX threat response
- Leverage other Cisco and 3rd party product to extend visibility
 - FMC external Cisco lookups
- Leverage SIEMs with Unified Events



Contextual cross-launch

Tight integration and pivoting to accelerate threat hunting

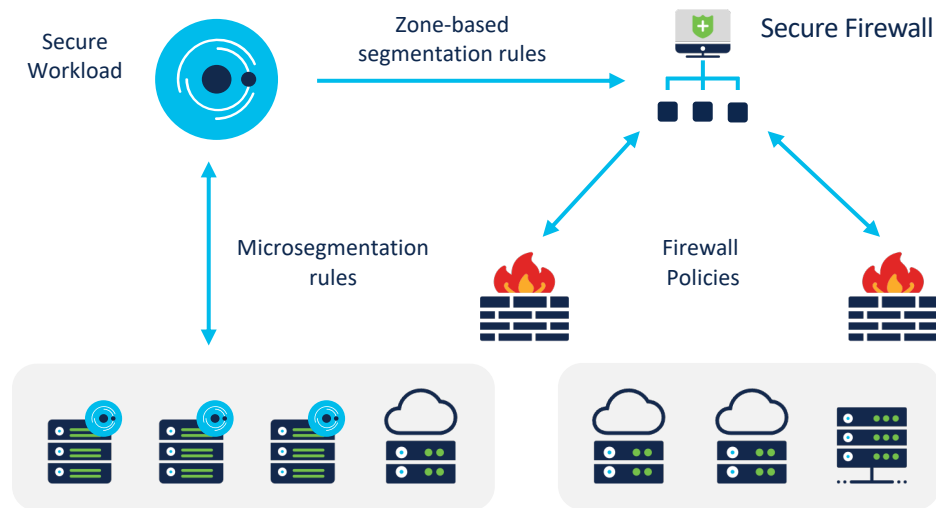
1 Right-click on an IP address

Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone
184.24.33.12	USA	InZone	OutZone
184.24.33.10	USA	InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone
52.8.		InZone	OutZone

2 Select Talos IP lookup

- Pivot directly to Cisco Architecture
- Pivot 3rd party tools
- Reduce time to analyze IoCs to drive down TTR
- Reduce complexity of integration

Dynamic Policy Across Multicloud Environments



Seamless Integration

Unified segmentation policy across Secure Firewall & Secure Workload



Dynamic Policies

Policy updated dynamically based on application communications information



Expanding to Cloud Providers

This fall, extending recommendation functionality to AWS and Azure security groups

“ Eagerly awaiting this! Integration across our multicloud controls will help drive better security in our distributed environment. ”

-- Global payments and fleet management enterprise

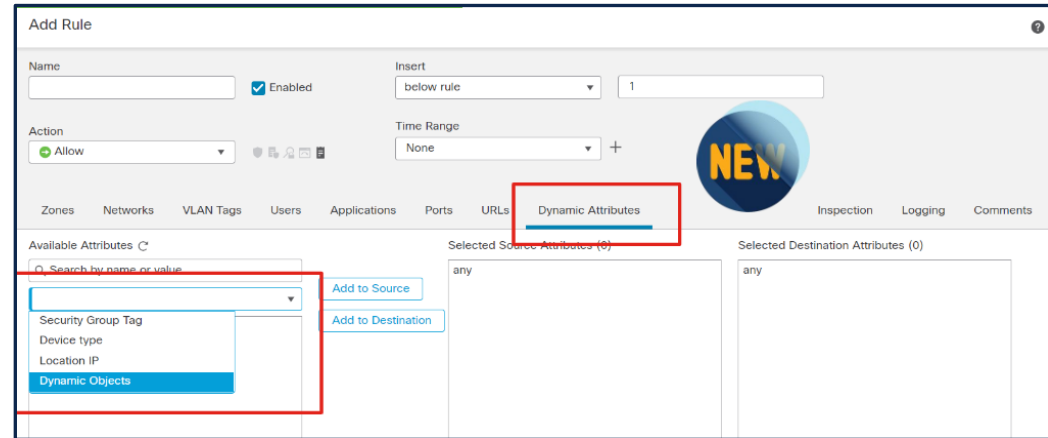
Cisco Secure Dynamic Attribute Connector



Problem: In a dynamic and multicloud world, admins struggle to keep up with ever changing object IPs as workloads are spun up, down and change.

Solution: Cisco provides a programmatic way to create, deploy and maintain dynamic objects.

Benefits: Dramatically reduces the admin overhead to keep security policies up to date, provides on demand updates without a deploy. Gain confident control of cloud services and other dynamic environments.



Cisco Secure Dynamic Attribute Connector

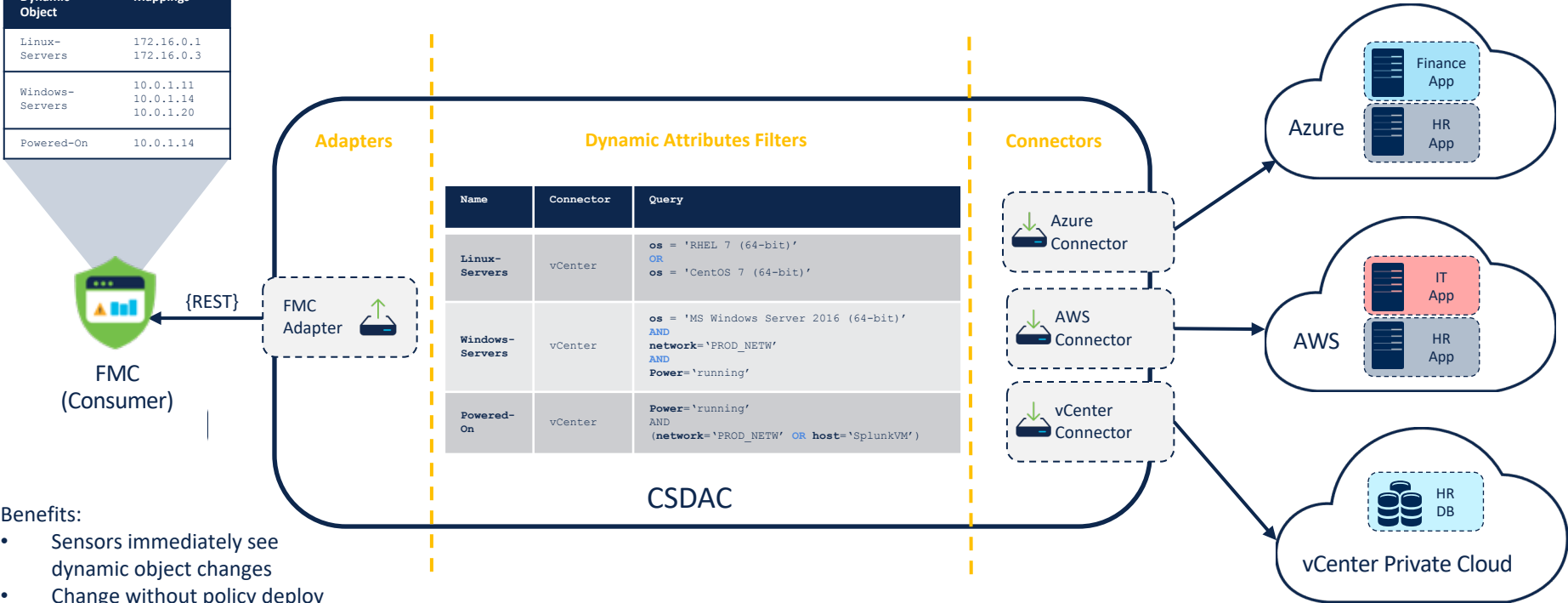


Integrations:

- AWS instances
- Azure instances
- Azure service tags
- VMware categories and tags managed by vCenter and NSX-T
- Google Cloud
- GitHub
- Office 365

Cisco Secure Dynamic Attributes Connector

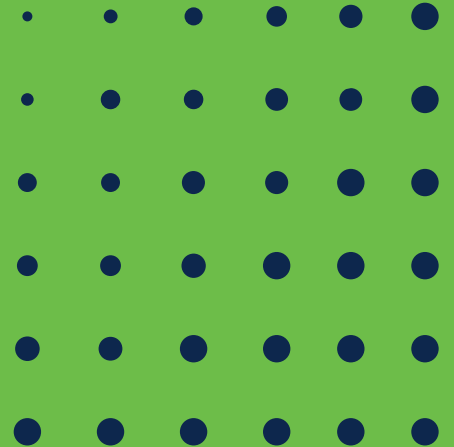
Dynamic Object	Mappings
Linux-Servers	172.16.0.1 172.16.0.3
Windows-Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14



- Benefits:**
- Sensors immediately see dynamic object changes
 - Change without policy deploy

FMC

New with 7.4



CSDAC in FMC



CSDAC
(Linux Machine)

Standalone

CSDAC in CDO's
Tools & Services

Cloud Delivered

CSDAC
in FMC

Built In

7.4 release

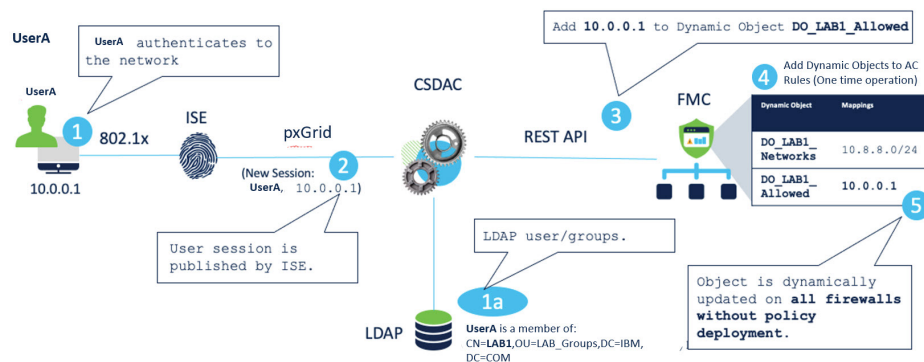
- You must configure
 - Connectors
 - Dynamic attribute filters
- You do not configure any adapters





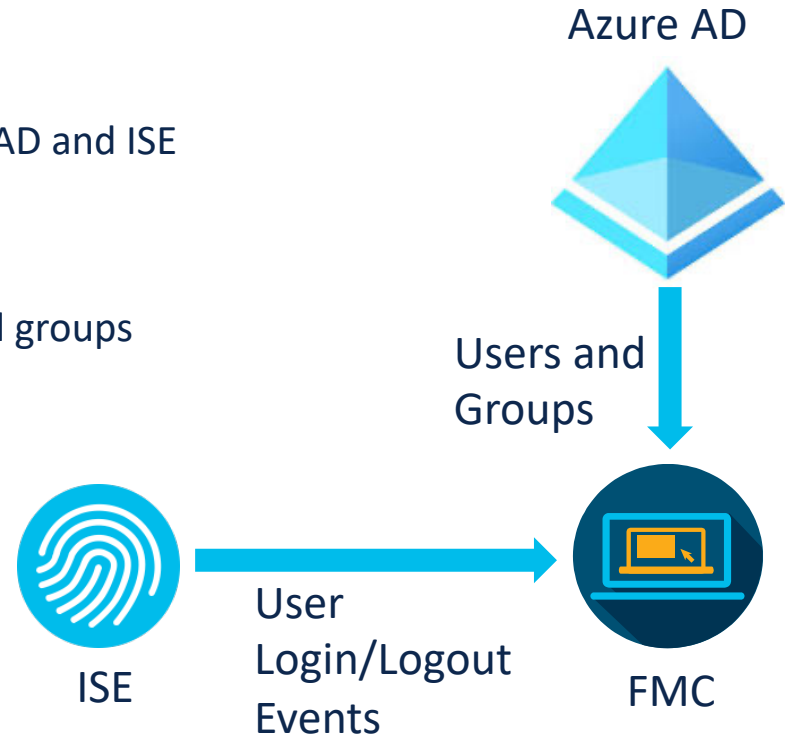
External User Identity with CSDAC

- Key motivation
 - Customers want to use Identity Services Engine (ISE) 802.1x Authentication with Lightweight Directory Access Protocol (LDAP)
 - FMC today does not support LDAP in Passive Authentication
- Three new connectors added to CSDAC
 - ISE Connector – creates IP-to-user mapping
 - LDAP Connector – creates user-to-groups mapping
 - Decorator – creates IP-user/groups mapping
- Adapter configuration has not changed

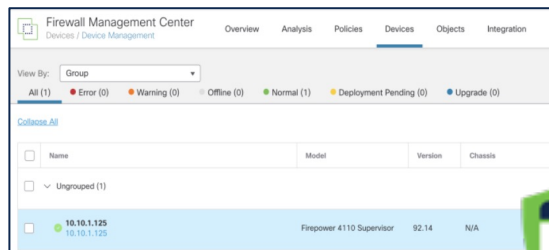


Azure AD Integration

- Objectives
 - Integrate Secure Firewall user identity with Azure AD and ISE
 - Receive Azure AD logins from ISE
 - Active authentication not supported in this release
 - Enforce access policy based on Azure AD users and groups
- Feature Overview
 - New Azure AD realm to get users, groups from Azure AD
 - Receive and process Azure AD user sessions from ISE
 - Stream real time user, group membership changes using Azure Event hub.
 - Revamped UI for User Analysis Screens



4100/9300 Chassis Registration to FMC



Firewall Management
Center

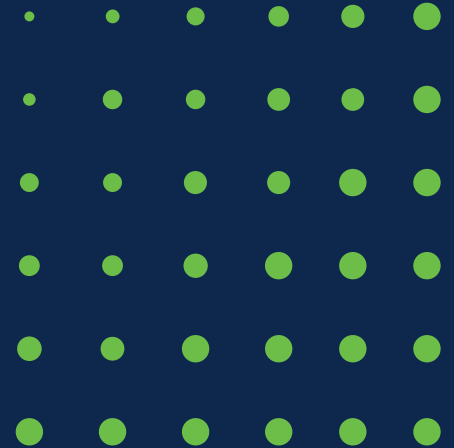
SFTunnel



FPR 4100/9300 Series
Chassis

- FMC have capability to register 4100/9300 chassis into device list
- FXOS faults (including HW bypass) collected by the FMC
- Chassis events available in UMS messages, Health Monitor and Events

Secure Firewall Device Manager (FDM)



What is Secure Firewall Device Manager (FDM)

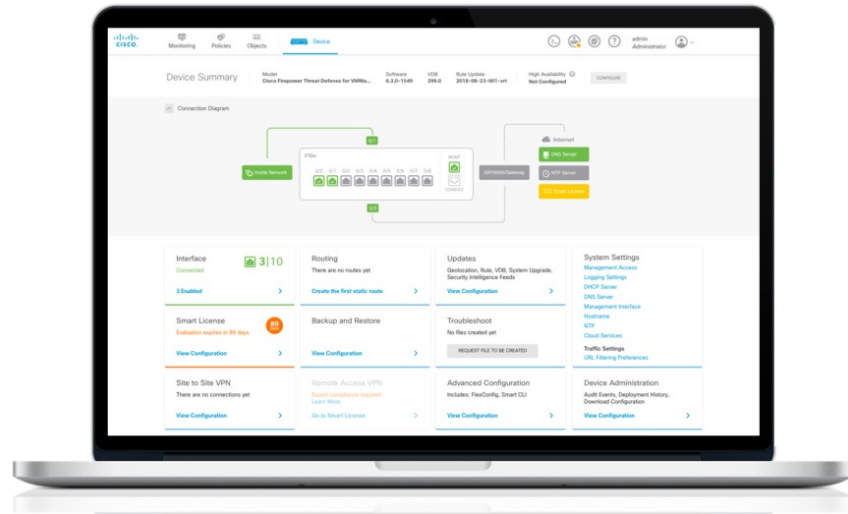
On-box manager and API platform

- **Key Benefits**

- Easy set up
- Control access and set policies
- Automate configuration
- Enhanced control

- **Features**

- Role-based access control
- High availability
- NAT and routing
- Intrusion and malware protection
- Device monitoring
- VPN support
- Support for Secure Firewall in GCP ^{New}



Simplified Firewall Management

Easy to setup, management, and monitoring

Manages Firepower Threat Defense on low-end and mid-range platforms



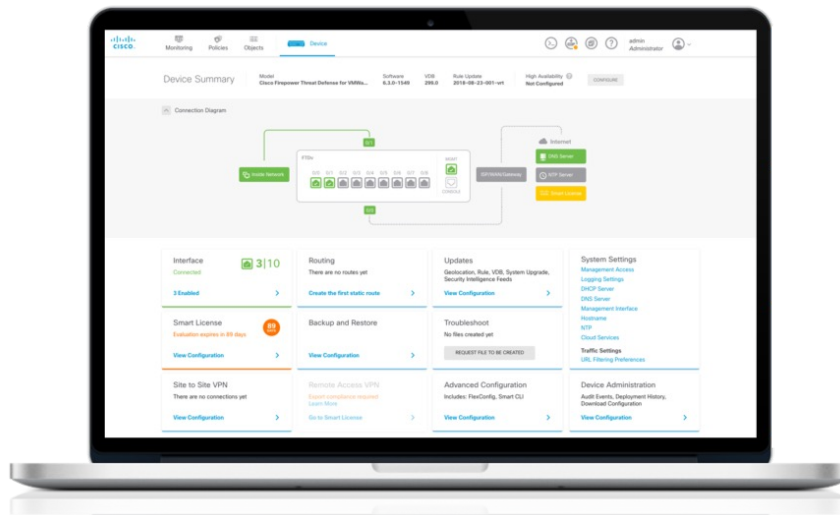
Wizard-based guided workflows



Predefined security policies for quick administration

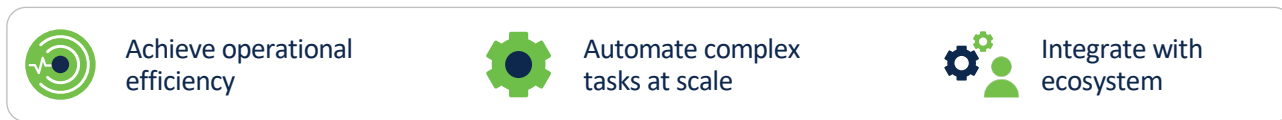


Built on FTD Device APIs



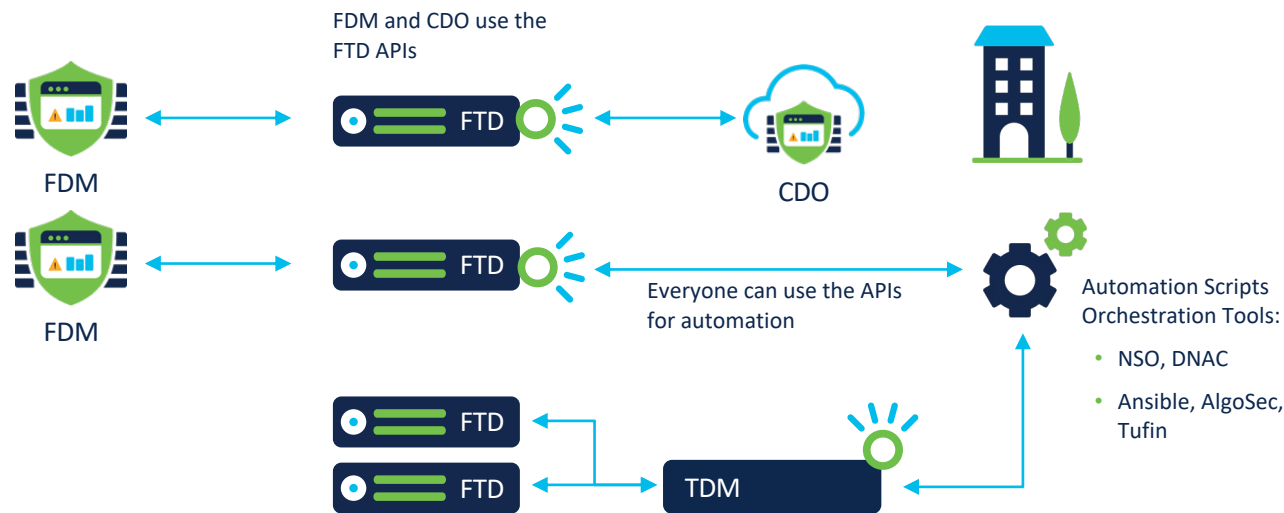
API-First Approach

An open, documented management and reporting architecture

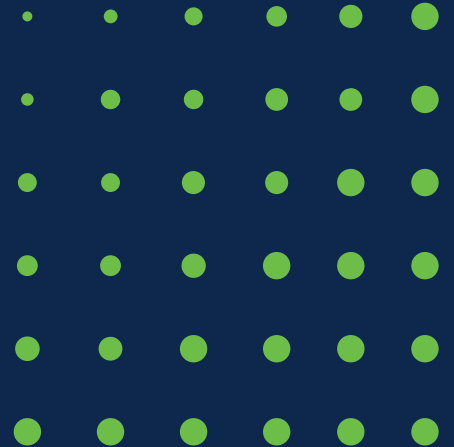


Key Features

- Day 0 Provisioning
- Day 1-2 Configuration Management
- Operations, Troubleshooting, Monitoring



Cisco Defense Orchestrator



Cisco Defense Orchestrator Overview

Consistently manage policies across your cisco security products.

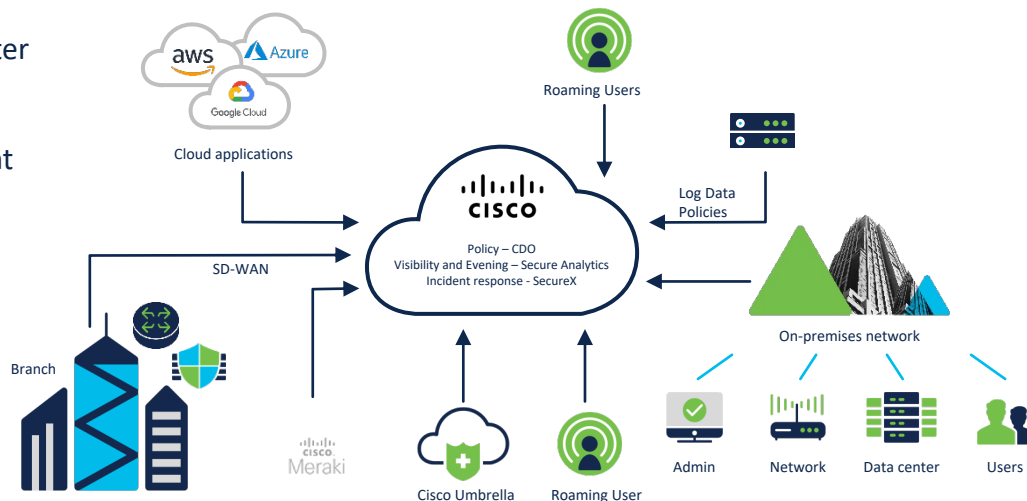
CDO is a Cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

Key Benefits

- Cloud-delivered Firewall Management Center
- Streamline security management
- Reduce time spent on security management tasks up to 90%
- Achieve better security while reducing complexity
- Prioritize response

Features

- Consistent policy enforcement
- Faster device deployments
- Configuration management



Cloud / SaaS Delivery Advantages

Highly available, full featured/managed cloud deployment

Global

- Connects to devices using device API with TLS v1.2
- Configuration encrypted at rest and in transit.
- CDO data center locations:
 - AWS – US
 - AWS – EU Central
 - AWS – APJC
- Secures management access using role-based access control with SAML-based two-factor authentication
- Allows multi-tenant management – full client separation

- Scalability / Flexibility
- No maintenance
- Faster feature delivery
- Low up-front cost
- Responsive to new requirements

99.999%

SLA Backed Uptime



Provision in
<1 day



Subscription pay
as you grow model



Low maintenance
costs

What's New? – CDO

NEW

June 2023

- Cisco Multicloud Defense (To be announced at Cisco Live)
- FTDv provisioning in the public cloud (Beta)
- Firepower Migration Tool cloud hosted (Beta)
- Consolidated Remote Access VPN Dashboard for ASA and FTD
- Improved Event Filtering

CDO is continually updated, [check here](#) for the latest information



Cisco Defense Orchestrator

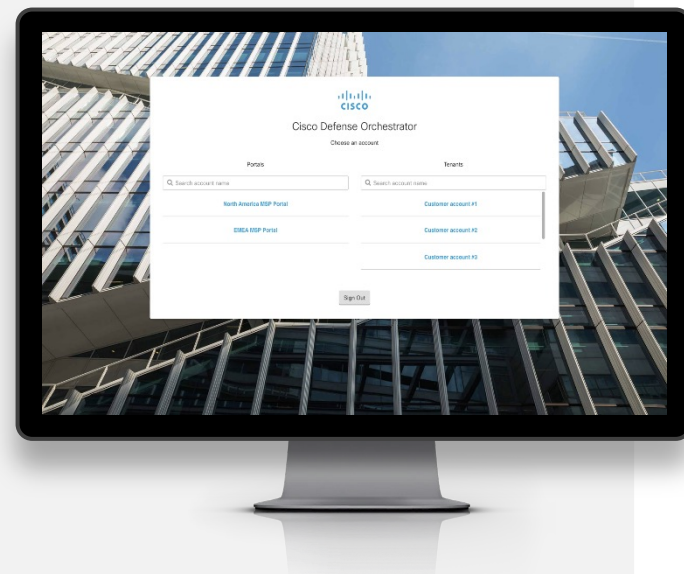
MSP Portal

- Use the CDO MSP portal to manage an unlimited number of customer accounts
- Easily view and search devices across all customer tenants
- Split customers across multiple MSP portals to limit admin access



Benefits

- Low Upfront Cost(s) – Pay As You Grow
- Minimized Deployment and Adoption Time
- Central Visibility with the MSP Portal
- Support for a Multi-Tenant Architecture
- Audit and Optimize
- Drive Automation Via API



Secure Services Edge Enablement

ASA to Umbrella SIG SASE Tunnels

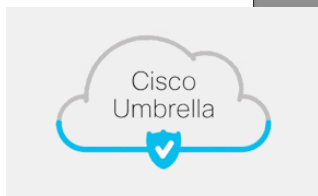
- Onboard Umbrella Organization
- View, Manage and Create SSE tunnels from Branch ASAs to Umbrella SIG
- Ensure consistency by leveraging Cross Launch into Umbrella Dashboard

The screenshot shows the 'Create SASE Tunnel' dialog box within the 'VPN Tunnels' management interface. The dialog is titled 'Create SASE Tunnel' and contains the following fields and options:

- Name ***: UmbrellaOrgbranch2montrealASA
- Umbrella Peer**:
 - Select Umbrella Organization *: Umbrella Org
 - Datcenter *: Toronto
- ASA Peer**:
 - Select ASA Device *: branch2-montreal-ASA
 - Public Facing Interface *: GigabitEthernet0/2 55.55.55.1
- LAN Interfaces ***: GigabitEthernet0/0 x
- Virtual Tunnel Interface (VTI) Address ***: 172.27.27.1
- Passphrase**:
 - Passphrase *: [Redacted]
 - Confirm Passphrase *: [Redacted]

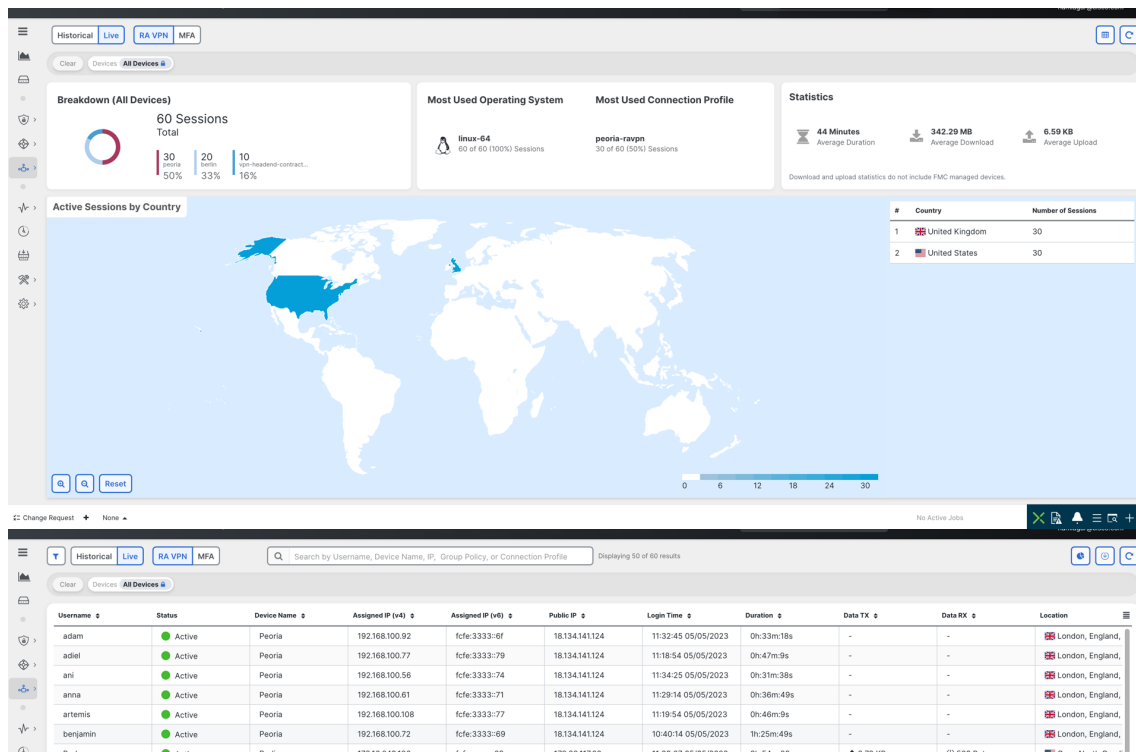
Below the passphrase fields, there is a note: "This passphrase must be between 16 and 64 characters long, include at least one upper case letter, one lower case letter, one number, and cannot contain any special characters."

At the bottom of the dialog, there is a checkbox labeled "Deploy changes to ASA immediately" which is checked. To the right of this checkbox are three buttons: "Cancel", "Save and Create Another", and "Save".



Consolidated RAVPN Monitoring Dashboard






- Consolidated RAVPN dashboard
 - Customers who have both ASA and FTD as VPN head-ends
 - Customers migrating their VPN deployment from ASA to FTD
- Filter, search and export the data
- Historical Reporting of VPN sessions
- Usage patterns
- Terminate sessions
- Same look and feel as the RAVPN dashboard in FMC



FTD provisioning in the public cloud using CDO

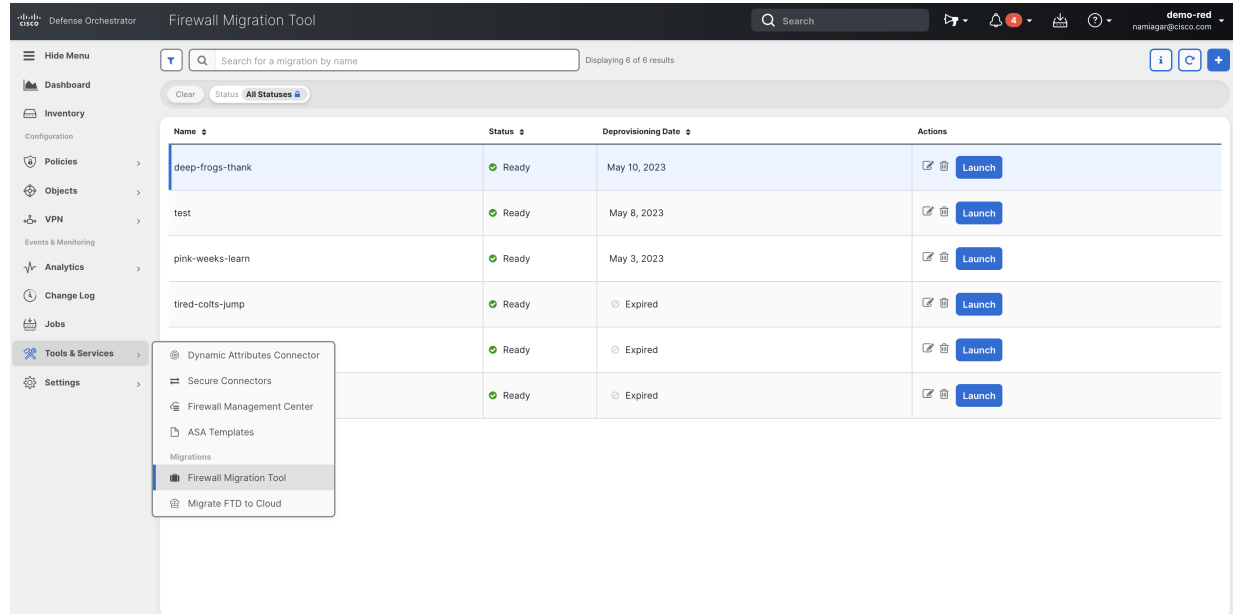
- Easy integration with multi-cloud environments
- Provision Firewall in any public cloud environment using a few clicks
- Combine with CSDAC available in CDO to enable automated policy deploy in multi-cloud environments

⚠ Important: After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure policies from CDO after onboarding. [Learn more](#)

 Use CLI Registration Key Onboard a device using a registration key generated from CDO and applied on the device using the Command Line	 Use Serial Number Use this method for low-touch provisioning or for onboarding configured devices using their serial number. (FTD 7.2+)	 Use AWS VPC Use this method for easy FTD provisioning to AWS and onboarding the device to CDO. (AWS VPC is required)	 Use Azure VNet Use this method for easy FTD provisioning to Azure and onboarding the device to CDO. (Azure VNet is required)	 Use GCP VPC Use this method for easy FTD provisioning to GCP and onboarding the device to CDO.
---	--	---	---	---

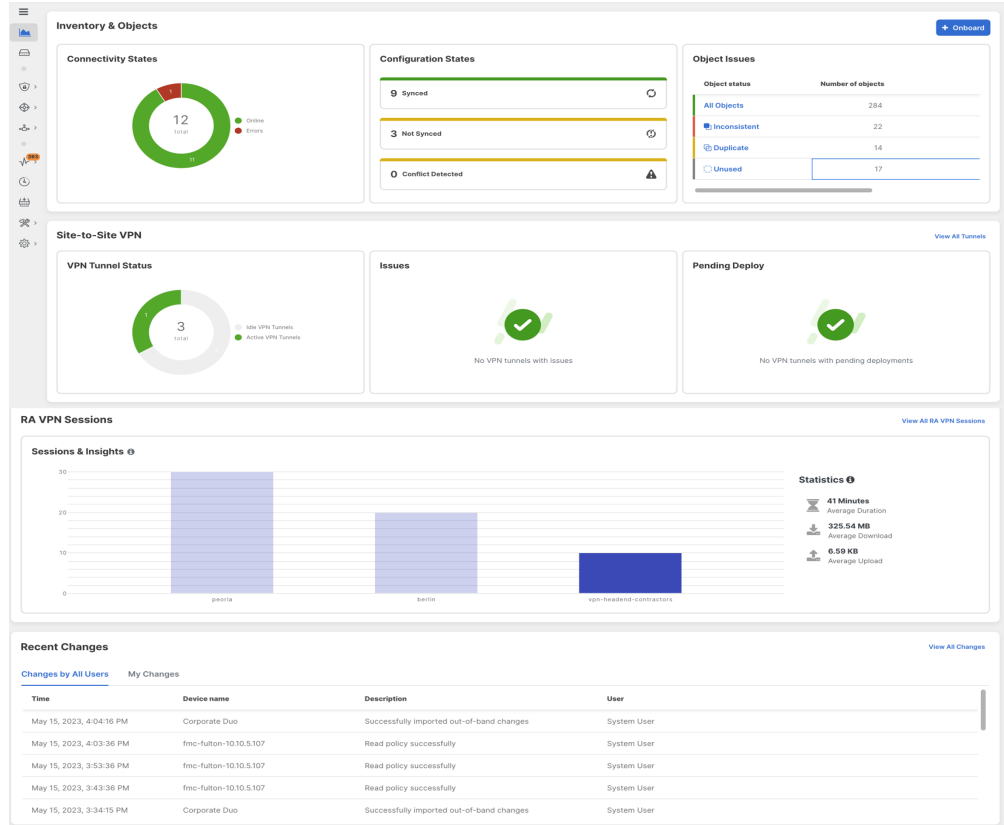
Firepower Migration Tool cloud-delivered

- Easily migrate from ASA or 3rd Party Firewalls to on-prem FMC or cloud-delivered FMC-managed FTDs
- No need for a desktop-based Migration tool as this is now cloud delivered as part of CDO



New Dashboard

- Actionable Insights about managed devices
 - Connectivity
 - Configuration state
- Tunnel Status
- Remote Access VPN Sessions
- Recent Configuration Changes

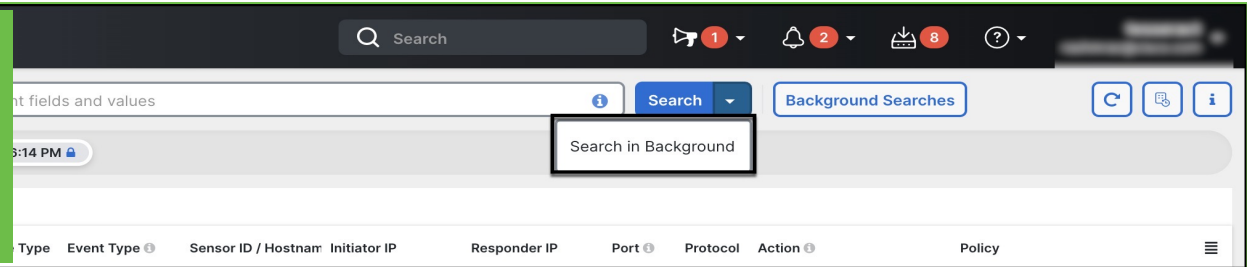


Improvements to Event Filtering

User can run search for events in the background

Continue with other tasks

Notification upon completion



Background Searches

Start a Background Search

View Notification Settings

Search Name	File Size	User	Status	Run Time	Actions
<input type="checkbox"/> Search_1679428080471	3.74 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:48:03 PM Completed in 2 seconds	View Download ...
<input type="checkbox"/> Search_1679428045727	3.74 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:47:27 PM Completed in 2 seconds	View Download ...
<input type="checkbox"/> Search_1679427993327	2.25 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:46:35 PM Completed in 2 seconds	View Download ...
<input type="checkbox"/> Search_167942230313	662 Bytes	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 1:58:39 PM Completed in 3 seconds	View Download ...
<input type="checkbox"/> Search_1679408015574	662 Bytes	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 10:13:44 AM Completed in 3 seconds	View Download ...

Revisit the background search page to view and download the results

Cloud-delivered Firewall Management Center

NEW

Now the new cloud-delivered Firewall Management Center boosts your productivity even further.



Eliminate change management and update overhead



Support at least 25% more firewalls per tenant



No rack space and utility bill, lowering operational cost







Cisco ensures uptime, increasing resiliency



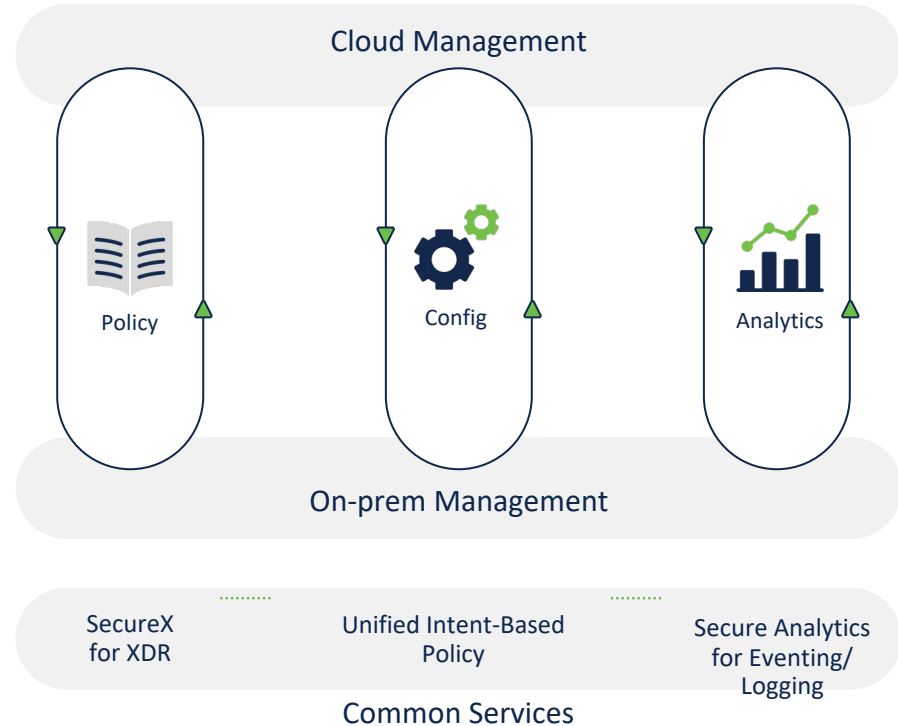
Same look and feel, no learning curve for existing users

Unifying Cloud and On-Prem Management

New Cloud-Delivered FMC

-  Simple and consistent UX
-  Easy migration from on-prem to cloud
-  Shared components for consistency
-  Common services for unified policy, XDR and logging

Re-use of components



Familiar User Experience

Defense Orchestrator
FMC / Policies / Access Control / Intrusion / Intrusion Policies

Analysis Policies Devices Objects Integration

Return Home Deploy Search Settings Profile namiagar@cisco.com

SECURE

Policies / Intrusion / Demo_IPS_Policy

Used by: 1 Access Control Policy | 1 Device

Mode: Prevention Base Policy: Balanced Security and Connectivity

Disabled 38106 Alert 470 Block 8899 Overridden 0 Rewrite 0 Pass 0 Drop 0 Reject 0

Base Policy → Group Overrides → Recommendations (Not in use) → Rule Overrides → Summary

Summary

50 items Filter Rule Group +

Rules

All rules assigned to current intrusion policy irrespective of rule group

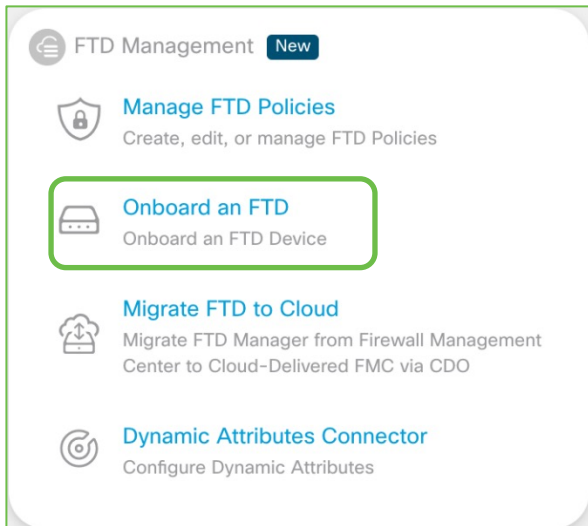
Rule Action Search by CVE, SID, Reference Info, or Rule Message

47,475 rules Preset Filters: 470 Alert rules | 8,899 Block rules | 38,106 Disabled rules | 0 Overridden rules | Advanced Filters

	GID:SID	Info	Rule Action	Assigned Groups
> Browser (6 groups)				
> Server (8 groups)				
> Policy (1 group)	> <input type="checkbox"/> 1:28496	BROWSER-IE Microsoft Internet Explorer createRange user after f...	Alert (Default)	Browser/Internet Explorer
> Indicator (4 groups)	> <input type="checkbox"/> 1:32478	BROWSER-IE Microsoft Internet Explorer CSecurityContext use af...	Alert (Default)	Browser/Internet Explorer
> Potentially Unwanted Applications (3 groups)	> <input type="checkbox"/> 1:32479	BROWSER-IE Microsoft Internet Explorer CSecurityContext use af...	Alert (Default)	Browser/Internet Explorer
> File (9 groups)	> <input type="checkbox"/> 1:26633	BROWSER-IE Microsoft Internet Explorer html reload loop attempt	Alert (Default)	Browser/Internet Explorer
> Malware (5 groups)	> <input type="checkbox"/> 1:31622	BROWSER-IE Microsoft Internet Explorer onreadystatechange us...	Alert (Default)	Browser/Internet Explorer
> Operating Systems (5 groups)	> <input type="checkbox"/> 1:31621	BROWSER-IE Microsoft Internet Explorer onreadystatechange us...	Alert (Default)	Browser/Internet Explorer
> Protocol (9 groups)	> <input type="checkbox"/> 1:27766	BROWSER-PLUGINS Oracle Java Security Slider feature bypass a...	Alert (Default)	Browser/Plugins
	> <input type="checkbox"/> 1:27110	EXPLOIT-KIT Blackholev2/Cool exploit kit outbound portable exe...	Alert (Default)	Malware/Exploit Kit
	> <input type="checkbox"/> 1:29165	EXPLOIT-KIT CritX exploit kit outbound jar request	Alert (Default)	Malware/Exploit Kit

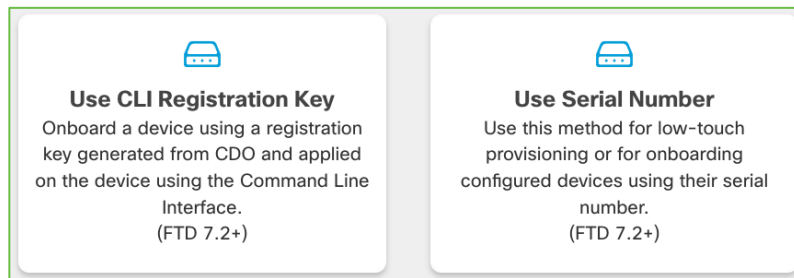
Simple Onboarding Experience

- Registration Key based Onboarding
- Zero Touch Provisioning using S/N



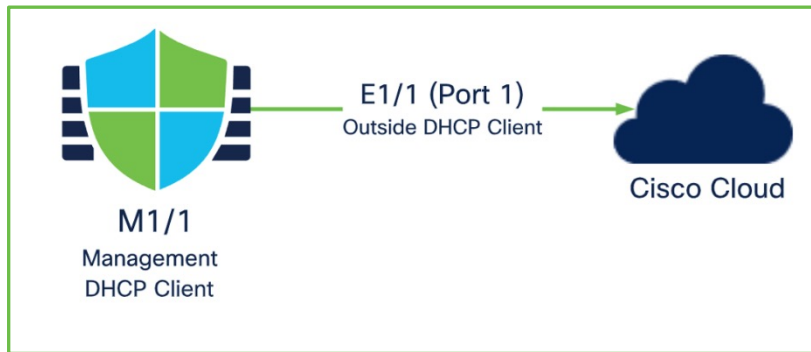
The screenshot shows the 'FTD Management' interface with a 'New' button. The main menu includes:

- Manage FTD Policies**: Create, edit, or manage FTD Policies
- Onboard an FTD**: Onboard an FTD Device (highlighted with a green border)
- Migrate FTD to Cloud**: Migrate FTD Manager from Firewall Management Center to Cloud-Delivered FMC via CDO
- Dynamic Attributes Connector**: Configure Dynamic Attributes

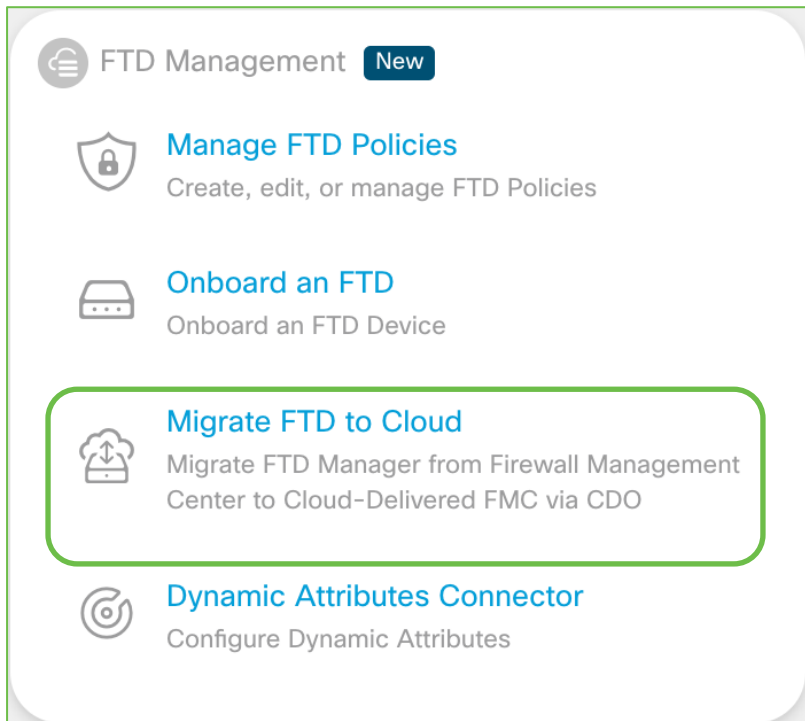


Two panels describe onboarding methods:





- Use CLI Registration Key**: Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface. (FTD 7.2+)
- Use Serial Number**: Use this method for low-touch provisioning or for onboarding configured devices using their serial number. (FTD 7.2+)



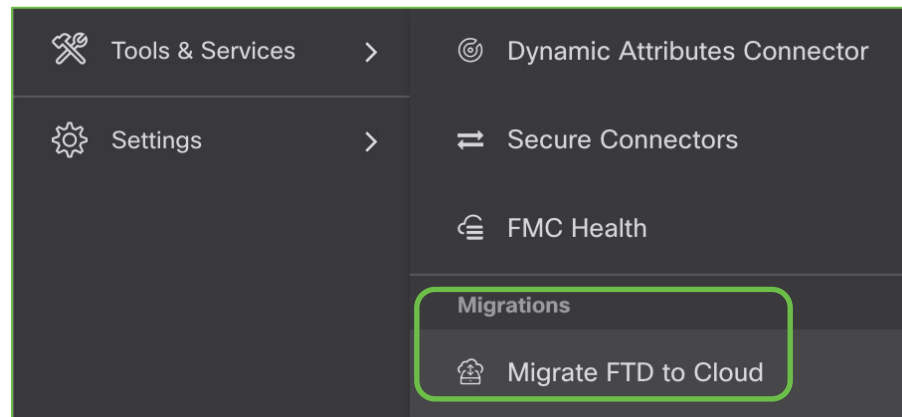
Easily migrate to Cloud-delivered management









FTD Management **New**

-  **Manage FTD Policies**
Create, edit, or manage FTD Policies
-  **Onboard an FTD**
Onboard an FTD Device
-  **Migrate FTD to Cloud**
Migrate FTD Manager from Firewall Management Center to Cloud-Delivered FMC via CDO
-  **Dynamic Attributes Connector**
Configure Dynamic Attributes

Easy Launch Points from Cisco Defense Orchestrator



-  Tools & Services >
 -  Dynamic Attributes Connector
 -  Secure Connectors
 -  FMC Health
 - Migrations**
 -  Migrate FTD to Cloud
-  Settings >

Easily migrate to Cloud-delivered management (Contd.)

Inventory / Migrate FTD to Cloud

Migrate FTD to Cloud
Migrate FTD from OnPrem FMC to cloud

1 Select OnPrem FMC **OnPrem FMC: fmc-namiagar.cisco.com**

2 Select Devices
Select FTD device(s) to migrate to cloud from OnPrem FMC and specify an action in bulk or per device.

Search: Name Multi-Device Action: Retain on OnPrem FMC for Analytics

Name	Domain	Action
<input type="checkbox"/> vancouver-branch-ftd	Global	Retain on OnPrem FMC for Analytics

0 device(s) selected Displaying 1 of 0 results

Migrate FTD to Cloud

3 Finish

Cancel

After completing the migration to cloud process, you have up to 14 days to try CDO as your FTD manager and commit or revert to OnPrem FMC as your FTD manager.

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

Please ensure DNS and other required configurations are correct so that the selected FTD(s) can reach CDO. [Learn more](#)

Onboard On-Prem FMC

Logging and Analytics – On Prem/Cloud

- Hide Menu
- Inventory
- Configuration
 - Policies >
 - Objects >
 - VPN >
- Events & Monitoring
 - Analytics **57782** >
 - Change Log
 - Jobs
- Tools & Services >
- Settings >

Migrate FTD to Cloud

Migrate FTD from OnPrem FMC to cloud

1 Select OnPrem FMC

OnPrem FMC: **fmc-namiagar.cisco.com**

2 Select Devices

Select FTD device(s) to migrate to cloud from OnPrem FMC and specify an action in bulk or per device.

After cor
FTD mar
After 14
applied t
Please c
can read

Search: Name

Multi-Device Action: Retain on OnPrem FMC for Analytics

<input checked="" type="checkbox"/>	Name	Domain	Action
<input checked="" type="checkbox"/>	vancouver-branch-ftd	Global	Retain on OnPrem FMC for Analytics

Retain on OnPrem FMC for Analytics
Delete FTD from OnPrem FMC

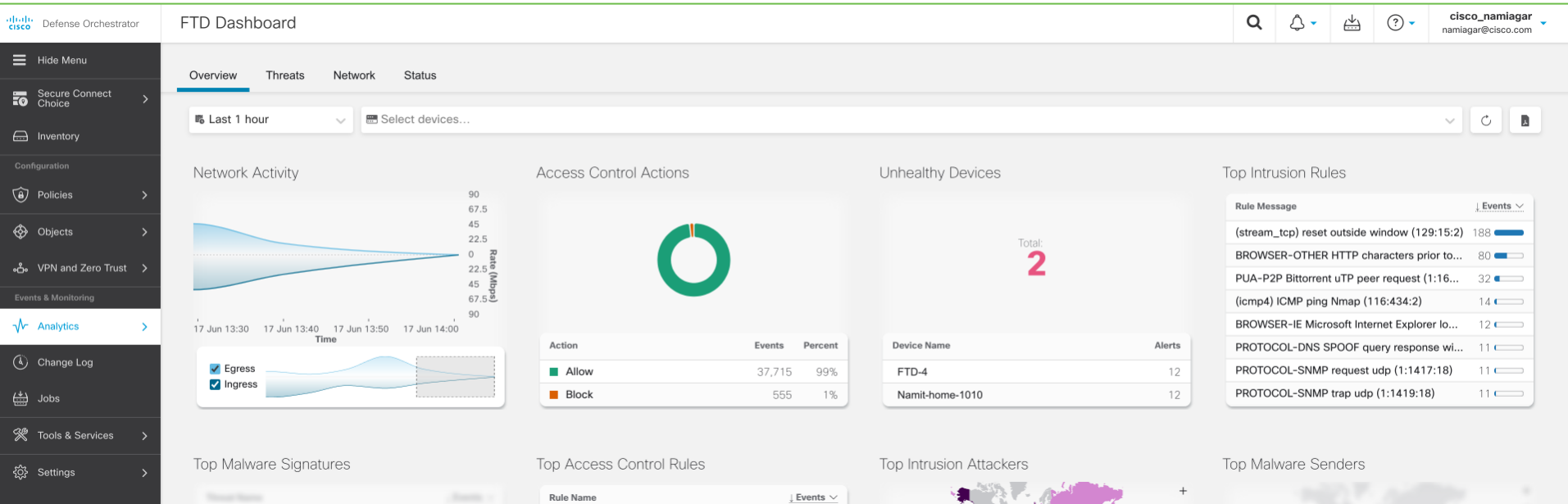
1 device(s) selected

Displaying 1 of 0 results

Migrate FTD to Cloud

3 Finish

Cloud Analytics Dashboard

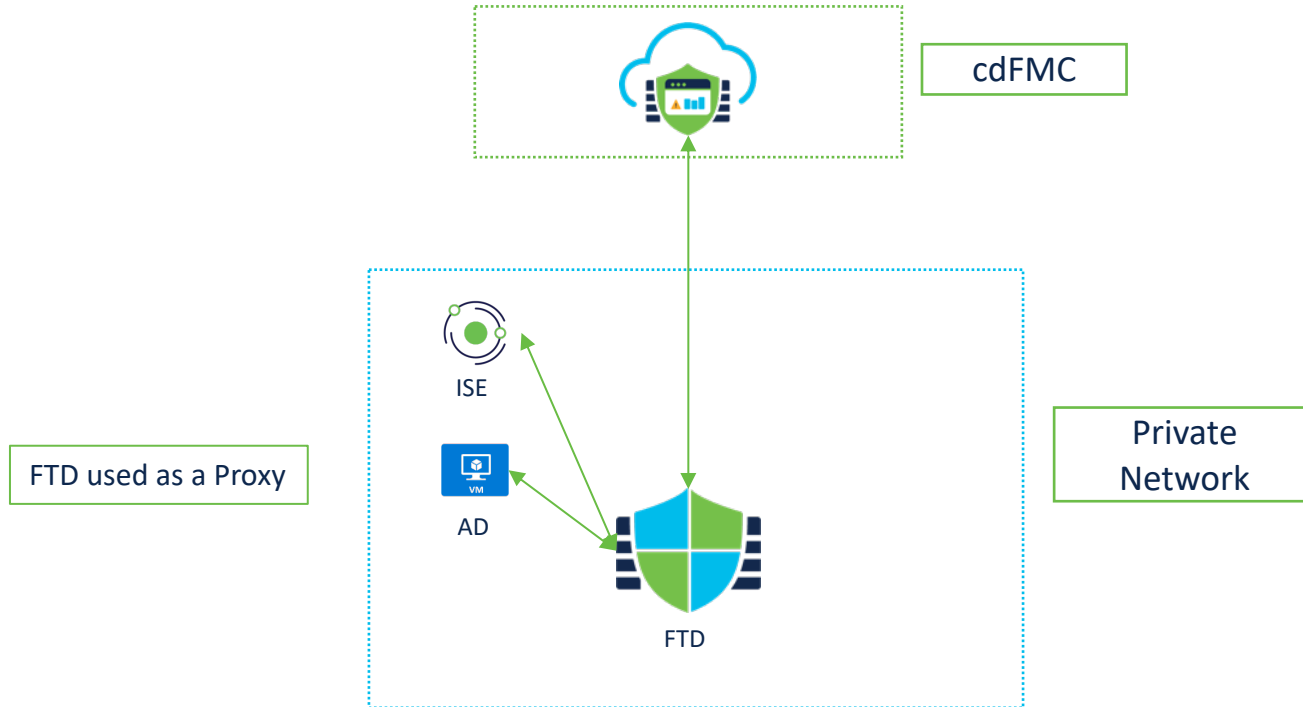


Cloud Delivered Dynamic Attributes Connector

- Update policy in real time using attributes from dynamically changing cloud environments
- Monitoring Dashboard
- Multi-tenant support
- Support for On-Prem and Cloud Delivered FMC

The screenshot shows the Cisco Defense Orchestrator interface for the Dynamic Attributes Connector. The left sidebar contains a navigation menu with sections: Configuration (Policies, Objects, VPN), Events & Monitoring (Analytics with 57782 items, Change Log, Jobs), Tools & Services (Dynamic Attributes Connector, Secure Connectors, FMC Health, Migrations, Migrate FTD to Cloud), and Settings. The main content area is titled 'Dynamic Attributes Connector' and 'Dashboard'. A central message states: 'There is nothing configured yet. You can start with any of the following actions:'. Below this, there are two columns of options. The first column, 'Create the first connector by clicking on the corresponding type:', includes icons for AWS, Azure, AST, and GCP, with a 'Go to Connectors' link below. The second column, 'Create the first adapter by clicking on the corresponding type:', includes icons for On-Prem FMC and Cloud-Delivered FMC, with an 'or' separator and a 'Go to Adapters' link below.

Connectivity Flow for AD/ISE



Secure Firewall support for Cisco Defense Orchestrator

Hardware

Minimum Software

Firepower 1000



FTD 7.2

Firepower 2100



FTD 7.2

Firepower 3100



FTD 7.2

Firepower 4100



FTD 7.2

Firepower 9300



FTD 7.2

Virtual – Private Cloud

KVM, VMWare

FTD 7.2

Virtual – Public Cloud

Alibaba,AWS, Azure, GCP, HyperFlex, Nutanix, OCI, OpenStack

FTD 7.2

ISA 3000

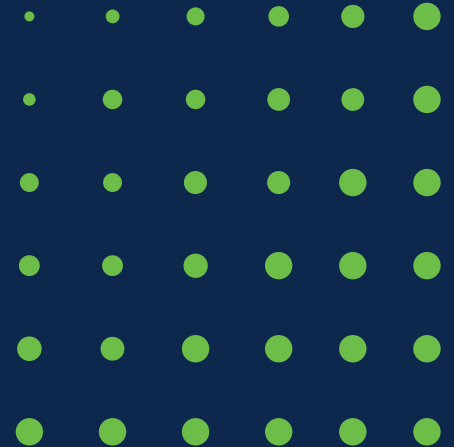
FTD 7.2

Meraki MX



Latest software update

Cisco Security Analytics and Logging



SAL (SaaS) Cloud Hosted Features



Cloud storage 90 days (default) up to 3 years, with viewing and download enabled within CDO



Supports **all** Cisco FTD & ASA devices. Direct-to-cloud option enabled for FMC 7.0+ managed devices



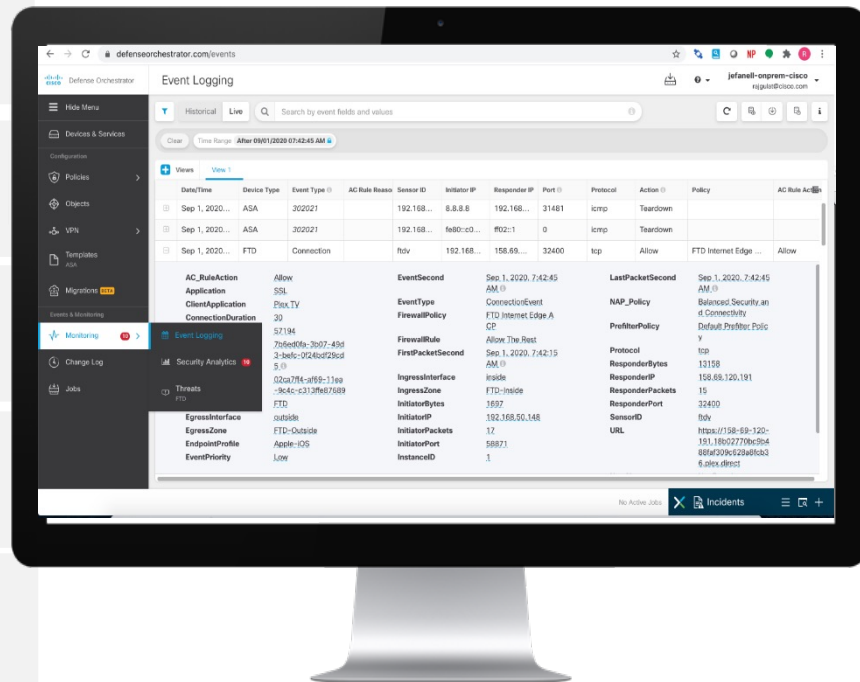
Firewall log analysis for advanced threat detections using Secure Cloud Analytics (SCA)



Correlation of firewall logs with internal network and cloud logs in SCA



Existing CTR-SecureX customers can opt-in to SAL logging easily by merging with their SecureX tenant



CDO: Cisco Security Analytics and Logging

Reduce complexity and logging event volume

DateTime	Event Type	Source IP	Destination IP	Port	Protocol	Detail
May 16, 2019 3:41:34 PM	File	22.4.0.231	2.253.0.231	25	tcp	
May 16, 2019 3:41:34 PM	Connection	22.4.0.229	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.227	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.230	2.253.0.230	25	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.227	2.253.0.221	21	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.202	2.253.0.12	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.202	2.253.0.12	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.207	2.253.0.17	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.200	2.253.0.10	443	tcp	Allow
May 16, 2019 3:41:34 PM	Connection	22.4.0.206	2.253.0.16	443	tcp	Allow



Store firewall and network logs securely in the cloud, accessible and searchable from CDO



Identify and enrich high fidelity alerts



Enable smarter response and reduce investigation times



Enhance breach detection capability using best-in-class security analytics

SAL On-Premise Features



FTD (including data plane logs) and ASA logging in a scalable data store hosted on-premises



Logging wizard in FMC 7.0+ simplifies on-premises and cloud logging configuration



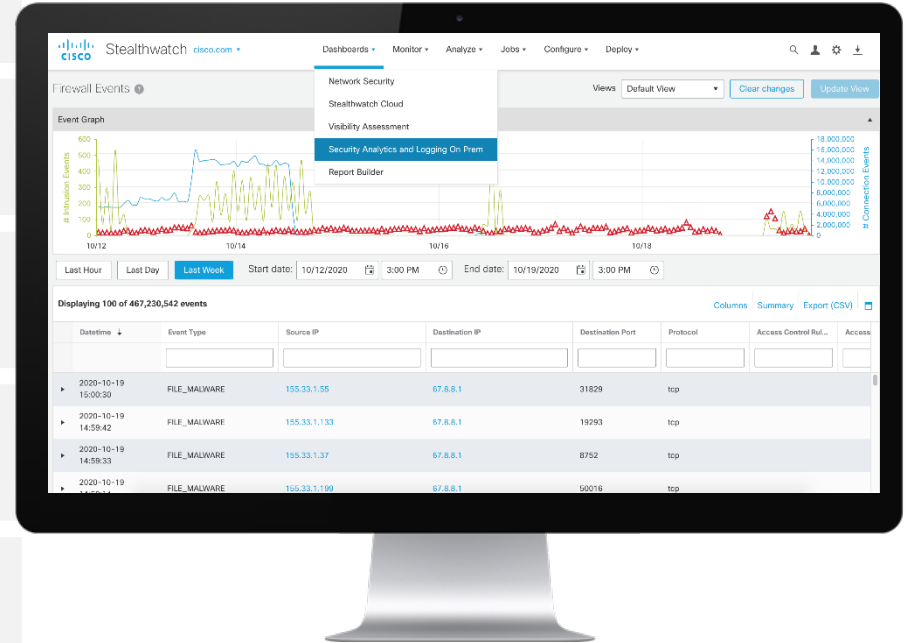
FMC 7.0+ logging and analytics scale drastically extended by a significant 300X magnitude via remote query of SAL/ SNA 7.3.2+



Context pivot to SAL's event viewer in Secure Network Analytics (SNA) for enhanced context



Multiple Flow Collector support with Firewall to Flow Collect mapping



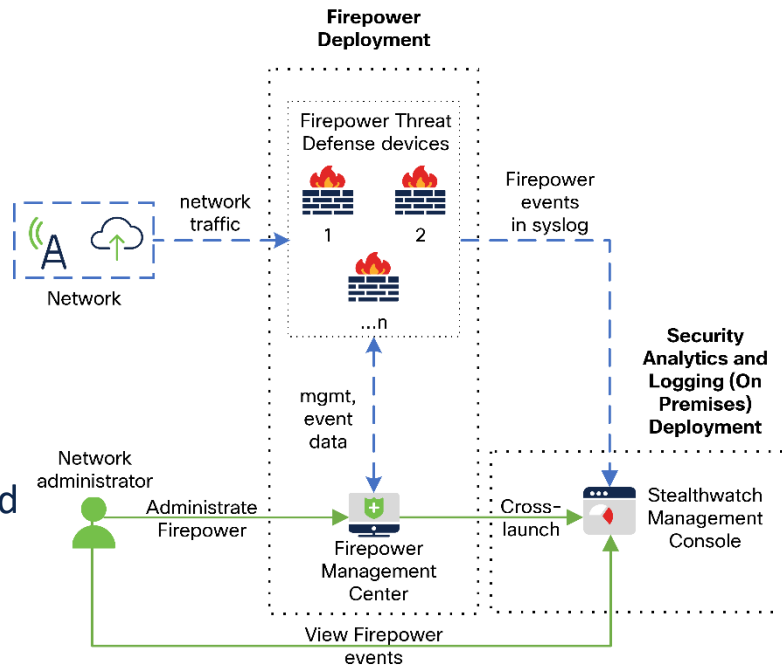
FMC Integration with Cisco Security Analytics and Logging (On-Prem)

Easy button for setup

- Setup FMC analytics cross launch links to the Secure Analytics console
- Setup remote query credentials from Secure Analytics datastore

Longer Event Retention and increased scale

- External Storage through Cisco Security Analytics and Logging On-Prem
- Auto select event source or manually specify
- Multiple Flow Collectors as event destination



Security Analytics and Logging Licenses

3 license tiers (nested)



Logging and Troubleshooting*

Scalable FTD and ASA event logging both in the cloud and on-premises, with API integration with Manager; CDO for cloud, and FMC for on premises stores



Logging Analytics and Detection

Firewall log data analysis using the behavior-based threat detections of Secure Cloud Analytics (SaaS)

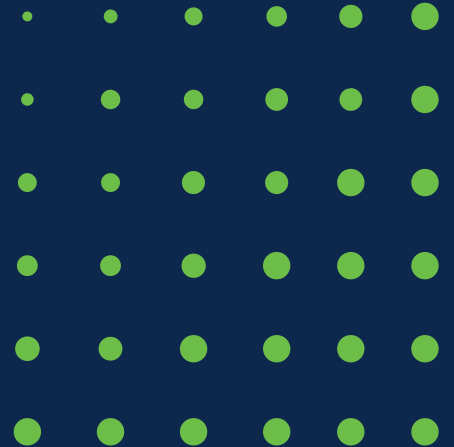


Total Network Analytics and Detection

Consolidated analysis run on combined dataset of firewall, internal and public cloud logs for comprehensive threat detection

*Security Analytics and Logging (On Premises) is currently only available with Logging and Troubleshooting License, which includes remote query by the FMC

Cisco Secure Firewall ASA



Adaptive Security Appliance (ASA)

Robust and effective firewall with stateful inspection and VPN functionality

ASA 5500X Series or Firewall hardware and ASA Stateful Firewall OS

- **Key Benefits**

- Basic inspection (L2-L4)
- Layer 7 Protocol Inspection
- Simple 5 tuple-based rules
- Multi-Context
- VPN load balancing

- **Features**

- Remote Access and Clientless VPN
- EzVPN, IKEv2/L2TP, DTSL1.2
- Site to Site VPN
- SSO with SAML, DAP
- Routing, CG NAT, QOS



ASA Software Provides

Robust, resilient stateful firewall and VPN concentrator



Rule

- Stateful controls
- Rules based on 5 Tuples only
- Allow or Block as two primary rule action



Feature

- VPN: Remote Access, Clientless, EzVPN, IKEv2/L2TP/3rd party Remote Access, Site-Site Route Based and Policy Based VPN, DTLS 1.2
- Routing and Quality of Service
- Carrier Grade NAT
- DAP
- SSO with SAML



Automate

- Leverage API's to integrate with SIEM
- API's to create enforcement based on 5 tuples



Security

- Packet Filtering and legacy Layer 2 to Layer 4 security and controls
- No advanced security controls like IPS, Endpoint, URL Filtering, Application control etc.

ASA Installation Modes




Platform Mode

- Provisioning and Initial configuration done from FXOS CLI or Firewall Chassis Manager
- Firewall 2100/4100/9300
- Default before 9.13.1, maintained on upgrading from lower releases to 9.13.1 or higher

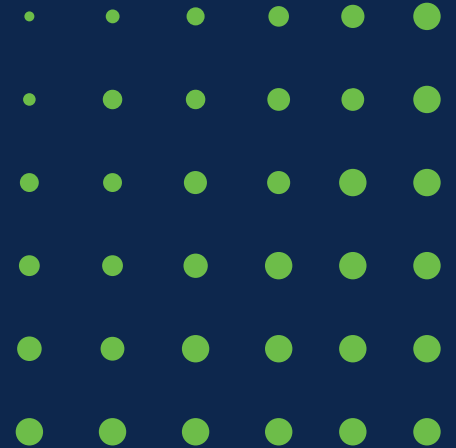
Appliance Mode

- Provisioning and initial configuration can be done from the ASA CLI or ASDM
- Firewall 1000/2100
- Default starting ASA 9.13.1 (fresh installation or reimage)
- FXOS CLI is used only for advanced troubleshooting

ASA Release 9.19.1 Highlights

 <p>Platform</p>	<ul style="list-style-type: none">• BGPv6 Graceful Restart• DHCPv6 Support• Flow Offload extended to non-IPSEC flows
 <p>VPN Management</p>	<ul style="list-style-type: none">• Loopback Interface for VTI and Management Services• Dynamic VTI• Dual Stack Support for IKEv2 Remote Access VPN• TLS 1.3 Remote Access VPN
 <p>Public Cloud</p>	<ul style="list-style-type: none">• Autoscale for Gateway Load Balancer in Azure• ASA v Clustering with AWS Gateway load balancer• IPv6 validation support in virtual deployments

Integrated Security Portfolio



Gain an Integrated Security Portfolio

Need: As IT infrastructure continues to become more diverse, the job of securing it becomes more dynamic. The perimeter becomes flexible, which requires a broader portfolio of security solutions.

Cisco offering:



Get more from your existing network

Tightly integrate existing investments, including Cisco Application-Centric Infrastructure (ACI) and Network Access with your Firewall solution.



Greater security control points

Enforce policies across your entire environment, including any device administered by the organization.



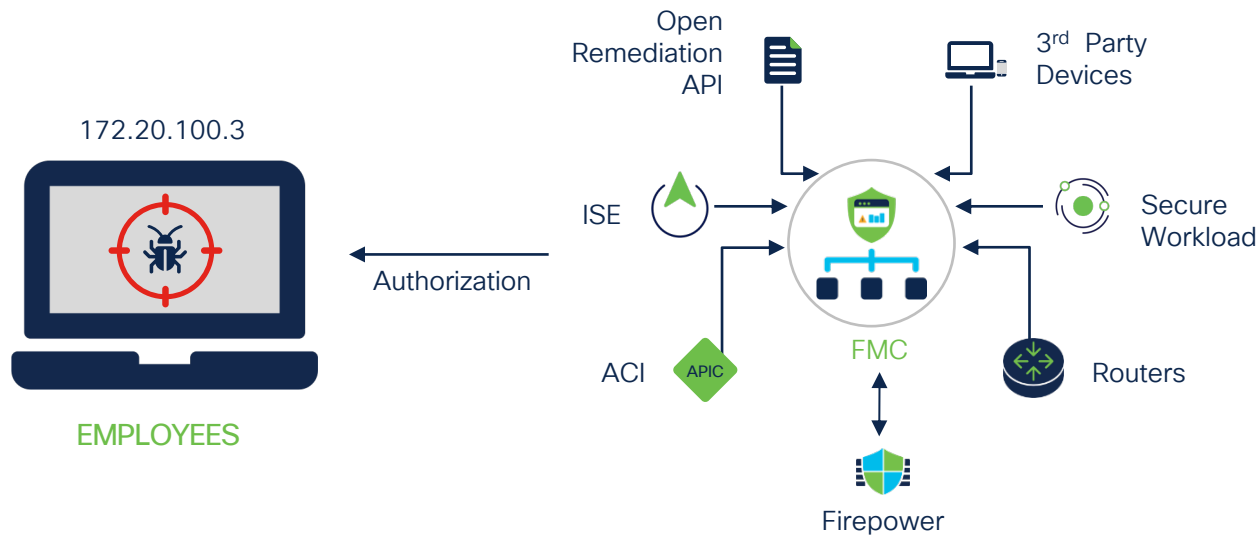
Extend protection

Remove blind spots, protect users anywhere they go and anywhere they access the internet.

Cisco Rapid Threat Containment

Proven approach to reduce time and impact of threat

- Automatic network threat containment using the network as an enforcer
- Threat-centric network access determines network access based on IoCs
- Richer visibility from bidirectional data sharing with the network access



Protect Your Network Using AMP

Understand the motion and behavior of files through network and endpoint visibility.

Breadth and Control points



Email



Endpoints



Web



Network



IPS



Devices

Threat Visibility



Retrospective
Detection



Behavioral
IoCs



File
Trajectory



Threat
Hunting

Telemetry Stream



File and Network I/O



Process Information

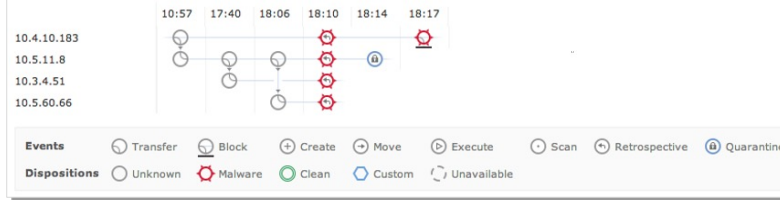


File Fingerprint and
Metadata



Talos and Malware Analytics
Intelligence

Trajectory



Application-Centric Infrastructure

Transparent policy-based security for both physical and virtual environments

- Link security to software defined networking
- Create identity-based policy with Application Policy Infrastructure Controller (APIC)
- Segment physical and virtual endpoints based on group policies with detailed and flexible segmentation

Configure Interface, PC, And VPC

Select Switches To Configure Interfaces: Quick Advanced

Switches: 101

Switch Profile Name: Switch101_Profile

Interface Type: Individual PC VPC

Interfaces:
Select interfaces by typing, e.g., 1/17-18

Interface Selector Name:

Interface Policy Group: Create One Choose One

Link Level Policy:

MCP Policy:

STP Interface Policy:

Storm Control Policy:

Attached Device Type: ESX Hosts

Domain Name:

vCenter Login Name:

Password:

vCenter/vShield:

CDP Policy:

LLDP Policy:

Monitoring Policy:

L2 Interface Policy:

VLAN Range:
Please use comma to separate VLANs.

Security Domains:

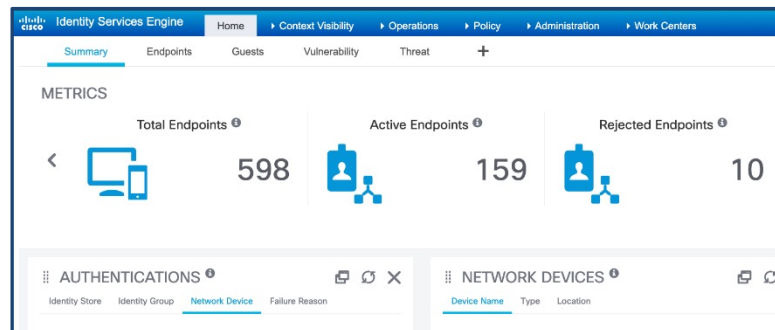
Confirm Password:

vSwitch Policy: MAC Pinning CDP LLDP

SAVE CANCEL

Control Traffic Based on User Awareness

- Use Active Directory users and groups in policy configuration
- Use Cisco Identity Services Engine to provide identity
 - TrustSec Security Group Tag (SGT)
 - Device type (endpoint profiles) and location
 - Identity Mapping Propagation & device level filtering
- Examples
 - Block HR users from using personal iPads
 - Create rules for quarantined iPhones



The screenshot shows the Cisco Firepower Management Center (FMC) Policy Editor. The main title is 'Branch Access Control Policy'. The 'Rules' tab is selected, and a search filter 'Filter by Device' is applied. The table below lists the rules for this policy.

#	Name	Source SGT	Dest SGT	Action
>	Mandatory - Branch Access Control Policy (-)			
✓	Default - Branch Access Control Policy (1-2)			
1	block quarantined hosts	Quarantined_Systems	ANY	Block with reset

Simplify Security Management with TrustSec

Leverage the network and investment

- Scalable and agile segmentation technology in over 40 different Cisco product families
- Enables dynamic, role-based policy enforcement anywhere on your network
- Extend TrustSec policies over Firepower Threat Defense with SRC & DST SGT matching



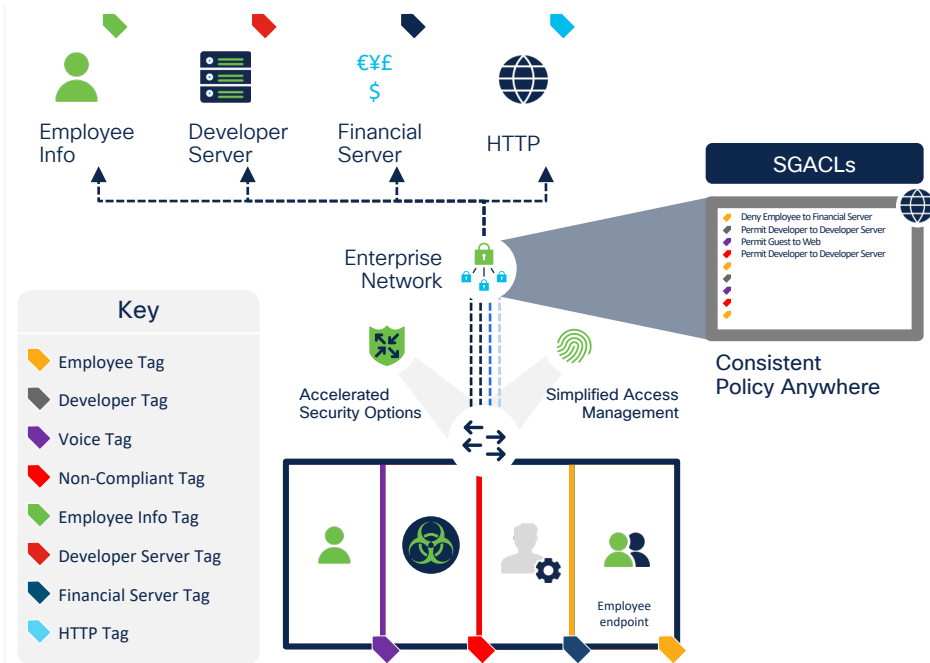
Simplified Access Management
Manage policies using plain language and maintain compliance by regulating access based on business role



Rapid Security Administration
Speed-up adds, moves, and changes, simplifying firewall administration to speed up server onboarding



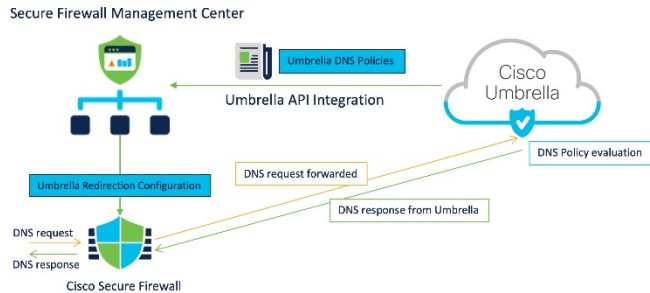
Consistent Policy Anywhere
Control all network segments centrally, regardless of whether devices are wired, wireless or on VPN



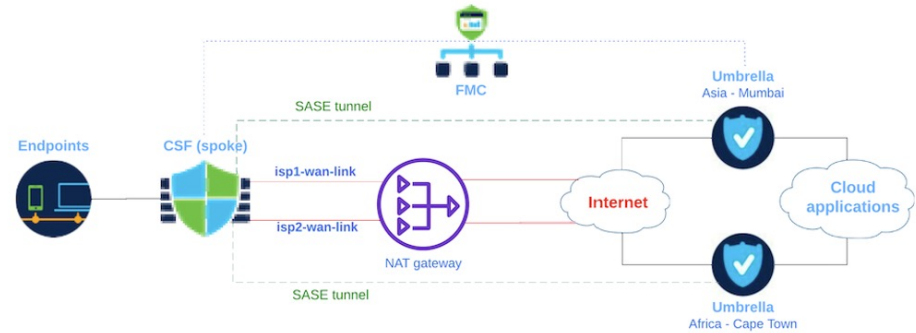
Umbrella Integration

SASE Deployments Auto Tunnel and Common DNS Security Policy

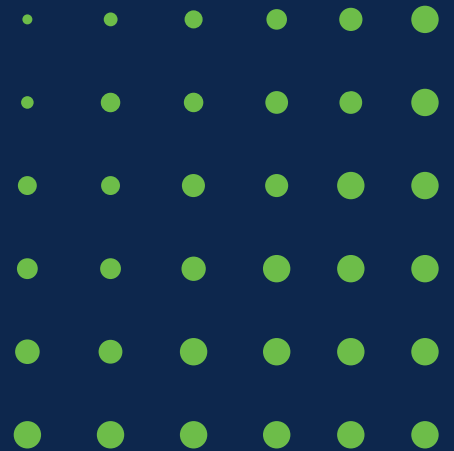
- Common Security Policies for all branches
- Multi-layered DNS Security
- Faster Protection
- Improved Internet Performance
- Uniform Security policy for Hybrid workers



- SASE use case
- Umbrella SIG – Cloud-delivered Firewall
- Auto-generation and deployment of configuration on Firewall and Umbrella

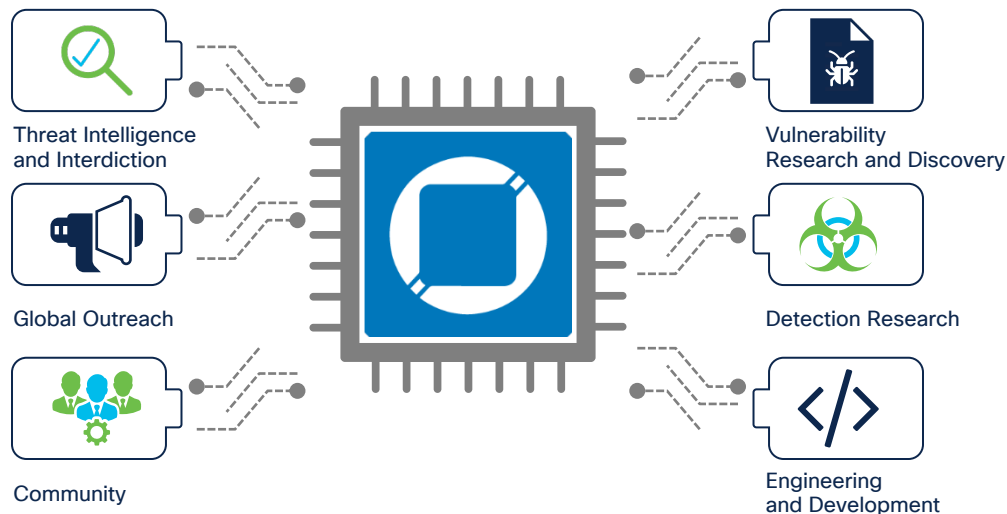


Talos



What is Talos?

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



From Unknown to Understood

Product Telemetry



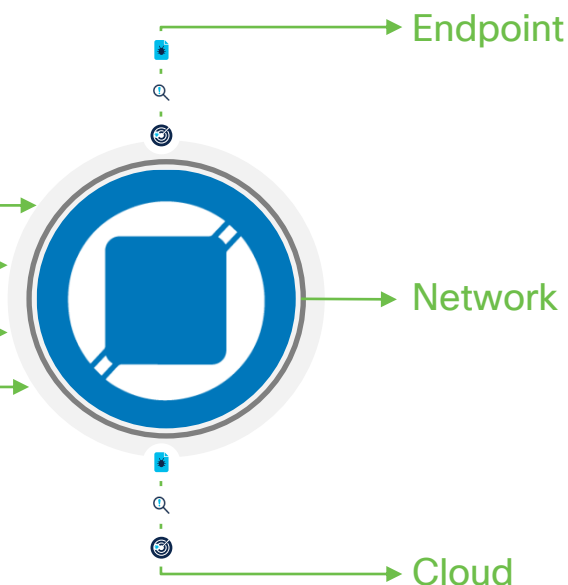
Data Sharing



Vulnerability Discovery



Threat Traps



Endpoint

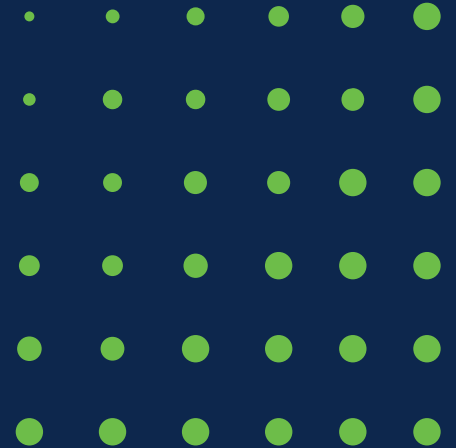
Network

Cloud



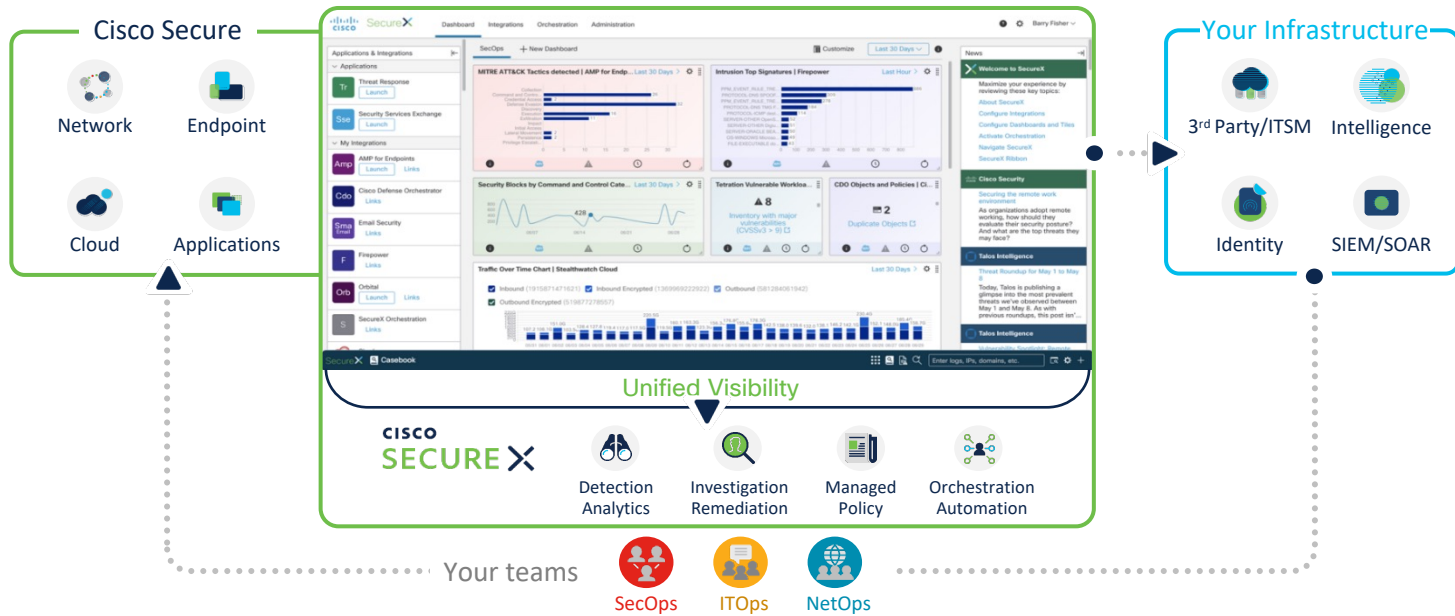
- Endpoint Detection and Response
- Mobile Security
- Multi-factor authentication
- Firewall
- Intrusion Prevention
- Web Security
- SD Segmentation
- Behavioral Analytics
- Security Internet Gateway
- DNS Security
- Secure Email

SecureX and Cisco XDR



Cisco SecureX

A cloud-native, built-in platform experience within our portfolio



integrations
built-in, pre-built
or custom

ribbon & sign-on
never leaves you
maintains context

dashboard
customizable for what
matters to you

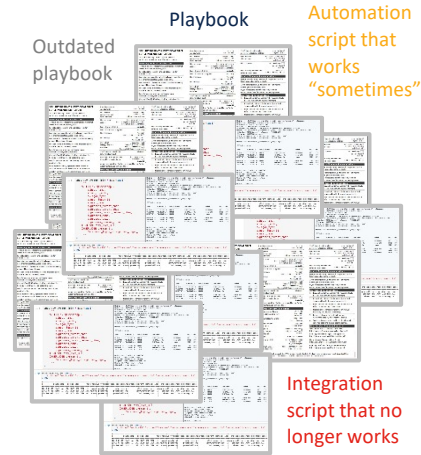
threat response
is at the core
of the platform

orchestration
drag-drop GUI
for no/low code

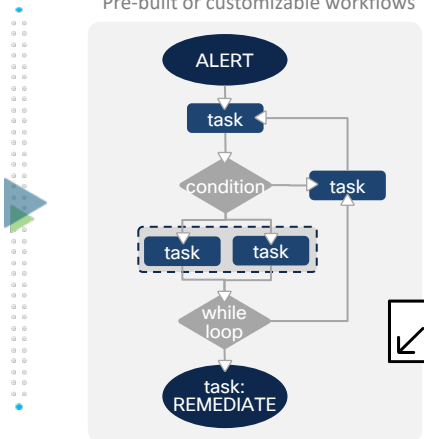
device insights
device inventory
with the contextual
awareness

Maximizing operational efficiency

BEFORE: Repetitive, human-powered tasks



SOLUTION:
Orchestrating security across the full lifecycle



Cisco or non-Cisco infrastructure

AFTER: "I combined 9 tasks across 3 security tools, 2 infrastructure systems, and 3 teams in one keystroke!"

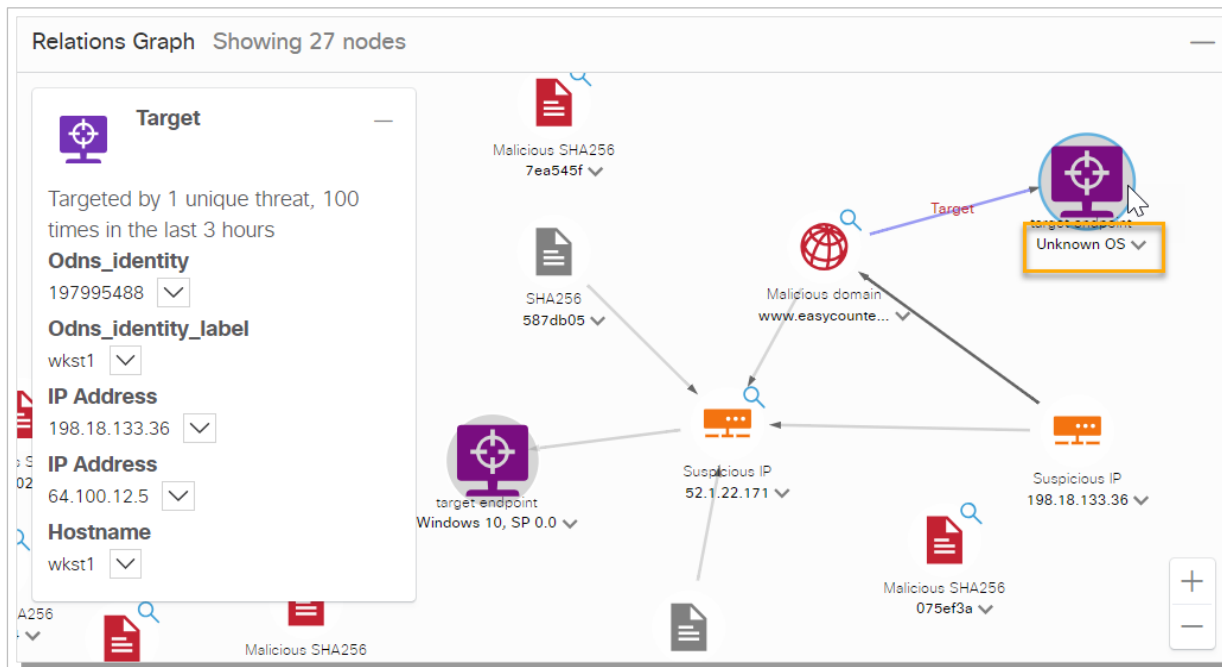
"We have never communicated faster: Our approvals are automated"

"I make automated playbook changes in minutes with a drag-drop interface"

"My top 5 most frustrating tasks have all been automated"

Investigate Any Item: Endpoint

Reduce complexity and time needed for threat hunting



Leverage a Seamless Workflow

FTD supplies security events to SecureX threat response

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and 'admin'. The main content area is titled 'Events By Priority and Classification' and shows a table of security events. The table has columns for Message, Priority, Classification, and Count. The events listed include various malware and trojan detections, such as 'EXPLOIT-KIT Rig Exploit Kit URL outbound communication' and 'MALWARE-CNC Win.Trojan.Cryptowall variant outbound connection'. Below the table are buttons for 'View', 'Copy', 'Delete', 'Review', and 'Download Packets'.

Message	Priority	Classification	Count
EXPLOIT-KIT Rig Exploit Kit URL outbound communication [1:42808:3]	high	Attempted User Privilege Gain	1
MALWARE-CNC Win.Trojan.Cryptowall variant outbound connection [1:34318:4]	high	A Network Trojan was Detected	3
MALWARE-CNC Win.Trojan.Ukranif variant outbound connection attempt [1:42894:4]	high	A Network Trojan was Detected	1
MALWARE-CNC DNS asspionkus_bit_top_dns_query [1:42841:8]	high	A Network Trojan was Detected	1
MALWARE-CNC Win.Trojan.Kpot variant outbound connection [1:50125:1]	high	A Network Trojan was Detected	1
MALWARE-CNC Win.Trojan.Livedid variant certificate exchange attempt [1:49552:1]	high	A Network Trojan was Detected	1
MALWARE-CNC Win.Trojan.TesaaCrypt server reply [1:38917:1]	low	Misc Activity	1

The screenshot shows the Cisco Threat Response interface. The top navigation bar includes 'Investigate', 'Suspicion', 'Intelligence', and 'Modules'. The main content area is titled 'Threat Response' and shows a detailed investigation of a security event. The event is identified as 'Win.Trojan.Miley-6735960-0' with a 'Risk: High'. The interface displays a 'Relations Graph' showing 27 nodes and a 'Signage Timeline' showing 104 sightings in the environment. Below the graph are several 'Observables' cards, each displaying a target and a number of sightings, such as 'www.easycount...' with 1 target and 102 sightings.

- Limited data is stored in cloud
- FMC can send IPS events to SecureX threat response
- Any IP, domain, file hash or IoC seen in FMC can queried in SecureX threat response, reducing complexity and time for threat hunting
- Continuous analysis with retrospection facilitates remediation and enhances forensics

Firewall and SecureX are better together

New Features Save Time and Effort



Simplified smart licensing allows users to have a seamless integration in 3 steps



Onboard entire suite of FMC API's directly to the cloud



Save time by importing workflows with minimal configuration



Access orchestration capabilities at no additional cost



New Workflows Simplify Administration



Proactively monitor the health of Firewall deployment



Streamline PSIRT impact and patch management processes



Automate policy management of time-based rules



FMC SecureX Ribbon Expanded

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intelligence

Deploy 🔍 🟢 ⚙️ ⓘ admin ▾

Network

Add Network ▾ 🔍 Filter

Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Value	Type	Override	
any	0.0.0.0/0 ::/0	Group		🔍 🗑️ 👤
any-ipv4	0.0.0.0/0	Network		🔍 🗑️ 👤

SecureX Home 🔍 Enter logs, IPs, domains, etc. ⚙️ ⓘ —

SecureX Ribbon

- Casebook 🔍
- Incidents 📄
- Orbital 🔍
- Settings ⚙️

Applications

- SecureX [Launch](#)
- PM-NAM-AMP [Launch](#)
- Security Services Exchange [Launch](#)
- TG via SecureX-NAM Org [Launch](#)
- Threat Grid [Launch](#)
- Threat Response [Launch](#)

My Account

Kishore Chakraborty
kischakr+platform@cisco.com
admin
IROH Testing
Logged in with Cisco Security Account

SecureX threat response and CDO Integration

Pivot to threat response from CDO using the event viewer

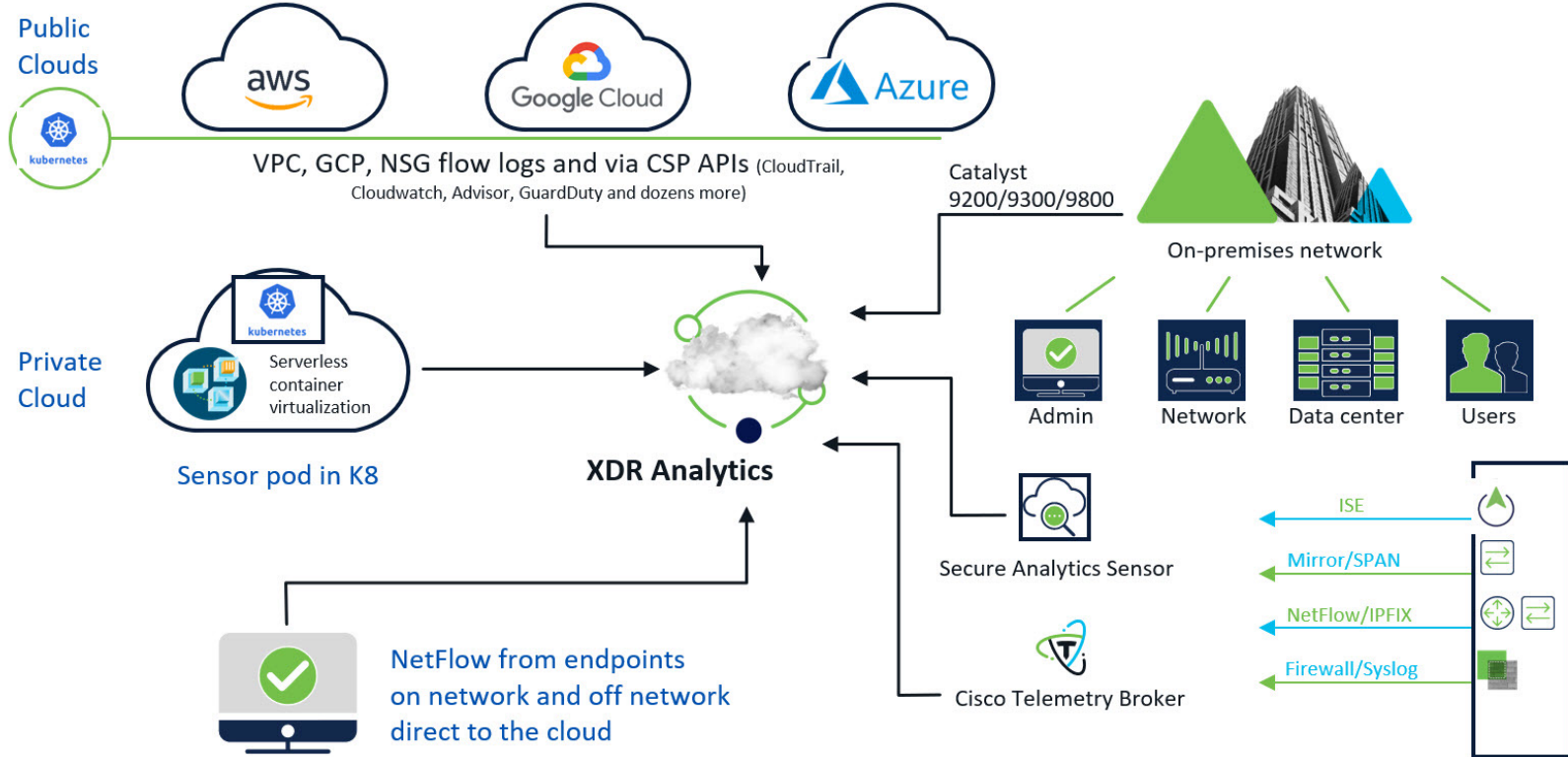
The screenshot displays the Cisco SecureX Defense Orchestrator interface. The main window shows the 'Events' section with a search bar and filters. The event viewer is set to 'Historical' and shows a list of events. The selected event is a 'MalwareEvent' from May 5, 2019, at 5:00:09 PM, originating from IP 192.168.242.220. The event details are expanded to show various attributes:

Attribute	Value
Application	HTTP
ArchiveFileName	28930249_3cdc7f1cbabaa4769c47541beaa7e353bb1eef2d.cab
ArchiveFileStatus	Extracted
ClientApplication	Windows Update
EventSecond	1557090008
EventType	MalwareEvent
FileAction	Malware Cloud Lookup
FileDirection	Download
FileName	28930249_3cdc7f1cbabaa4769c47541beaa7e353bb1eef2d.cab
FilePolicy	CTRNetworkAMPPolicy
FileSHA256	5bda9a35ab2b5eb7fca011140e0ef0d8db372d88e84b7a14a036278ed7937fb
FileSize	7299
FileStorageStatus	Not St (Dispo)
FileType	MSCAF
FirstPacketSecond	155701
InitiatorIP	192.16
InitiatorPort	54389
LastPacketSecond	155701
Protocol	tcp
ResponderIP	205.18
ResponderPort	80
SHA_Disposition	Unavail

A pop-up window titled '8 new observables were found' is overlaid on the right side of the interface. It shows a list of observables with columns for 'Clean' (1) and 'Unknown' (7). The observables include:

- http://download.windowsupdate.com/d/msdownload/update/...
- 28930249_3cdc7f1cbabaa4769c47541beaa7e353bb1eef2d.cab
- 192.168.242.23
- 192.168.242.220
- 205.185.216.42
- 192.168.242.220
- download.windowsupdate.com
- 5bda9a35ab2b5eb7fca011140e0ef0d8db372d88e84b7a14a036278ed7937fb
- 72.21.81.240

Cisco XDR for Dynamic Environments



Benefits of Cisco XDR

Where are we **most exposed** to risk? How good are we at detecting attacks **early**?

Detect Sooner

Prioritize by Impact

Are we **prioritizing the attacks** that represent the largest **material impacts** to our business?

How quickly are we able to understand the **full scope** and **entry vectors** of attacks?

Reduce Investigation Time

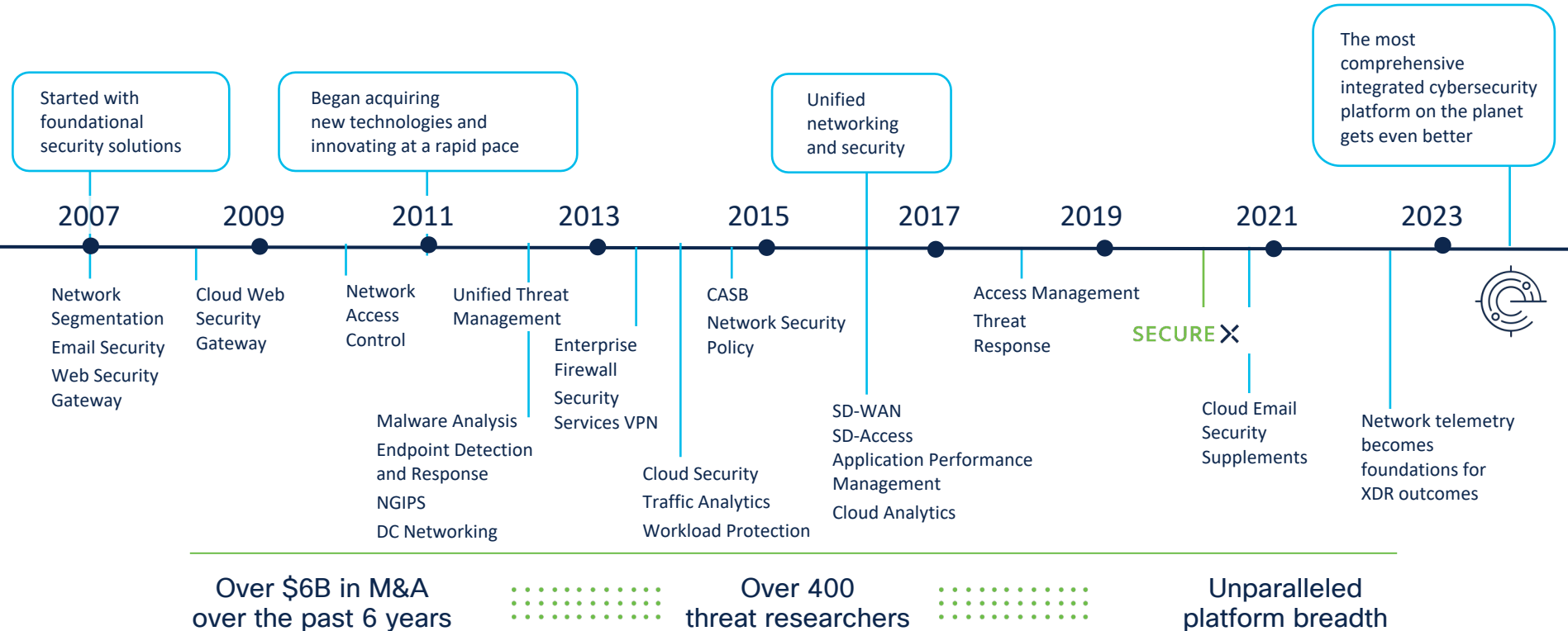
Accelerate Response

How fast can we **confidently respond**? How much can SecOps **automate**? Are we **improving our time to respond**?

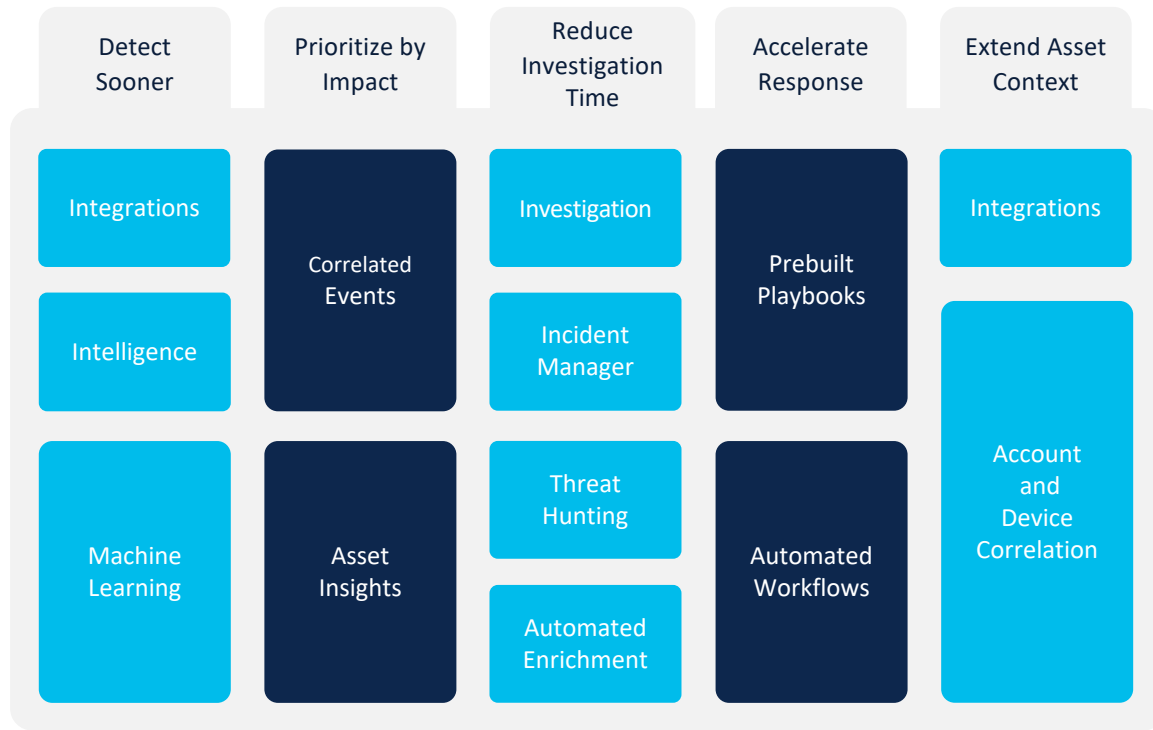
Do we have **full visibility** into all our assets? Can we **reliably identify** a device and who uses it?

Extend Asset Context

Building Cisco XDR



XDR Components



Analytics
Detections based on raw telemetry

Incidents
Security alerts, correlated, prioritized and enriched

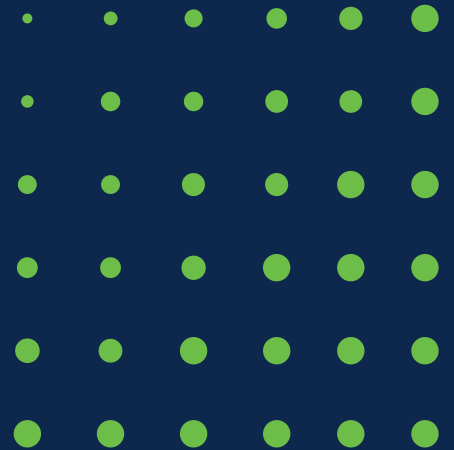
Integrations
built-in, pre-built or custom

Investigate
is at the core of the platform

Automate
drag-drop GUI for no/low code

Devices
device inventory with the contextual awareness

Use Cases



Common and Unique Requirements for Secure Firewall



Internet Edge

- High availability and redundancy
- Dynamic routing and address translation
- Integration with end point security
- Integration with NAC network access control



Data Center

- High availability
- Scalability
- Very high bandwidth, very low latency
- Cloud scale
- Hyper-density and high performing volts
- DDoS
- IPS capability
- Multi-instance



Branch

- Site to site VPN
- High availability
- Dynamic routing
- Application visibility and control
- Breach detection
- Threat intelligence
- Incident response
- Dual-WAN
- Application Aware Intelligent Routing(DIA)



Cloud/Virtual

- High availability
- Support for DPDK and SRIOV
- Internet edge or VPN gateway
- SD-WAN backhaul
- NSEW inspection
- Inbound inspection
- Device acting as edge



Secure IPS

- Separation of duties
- IPS capability
- Superior threat efficacy
- Threat intelligence
- TLS decryption
- Mirror traffic and deploy in active, inline, or passive mode
- Network reliability
- Scalability



Remote Access

- Cisco VPN and third-party VPN clients
- Integration with end point security
- Authentication, Authorization, Accounting
- Zero Trust Clientless access to private applications

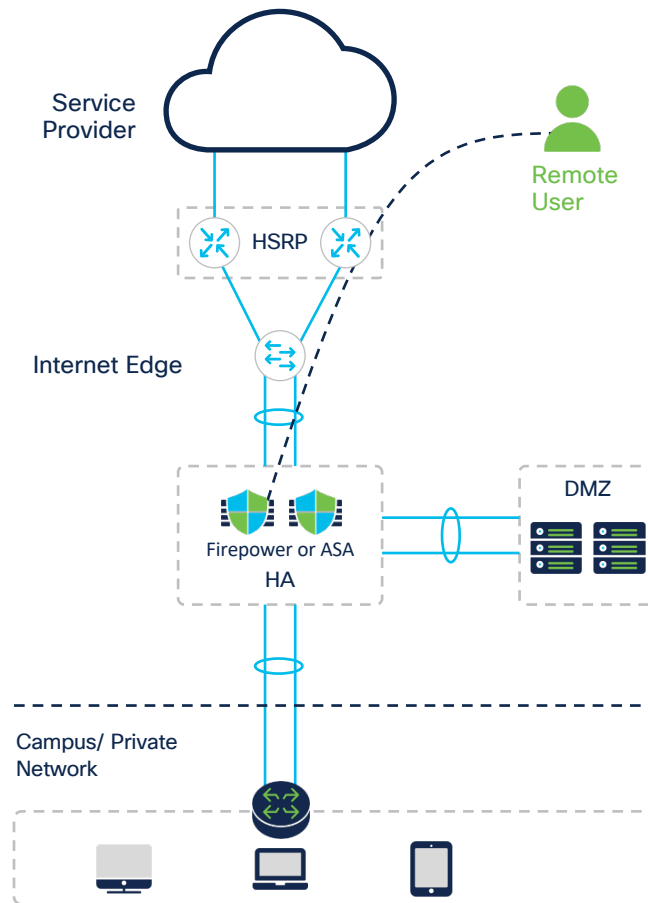
Internet Edge

Key Functions

- Resilience (and scalability)
- Advanced Access Control
- Block access to malicious IP's, URL's, DNS
- Dynamic NAT/PAT and Static NAT
- Remote Access VPN
- Site to Site VPN
- Detecting malicious network traffic
- Visibility and tracking of file transfers, Blocking of malicious files
- Dynamic analysis of unknown files

Key Capabilities

- VPN load balancing
- Applications, URLs, Users, and TrustSec Policy using SGTs
- Talos Security Intelligence
- Carrier Grade NAT
- Cisco Secure VPN
- Point to Point, Hub and Spoke, Full mesh
- Snort IPS
- Advanced Malware Protection
- Malware Analytics Integration



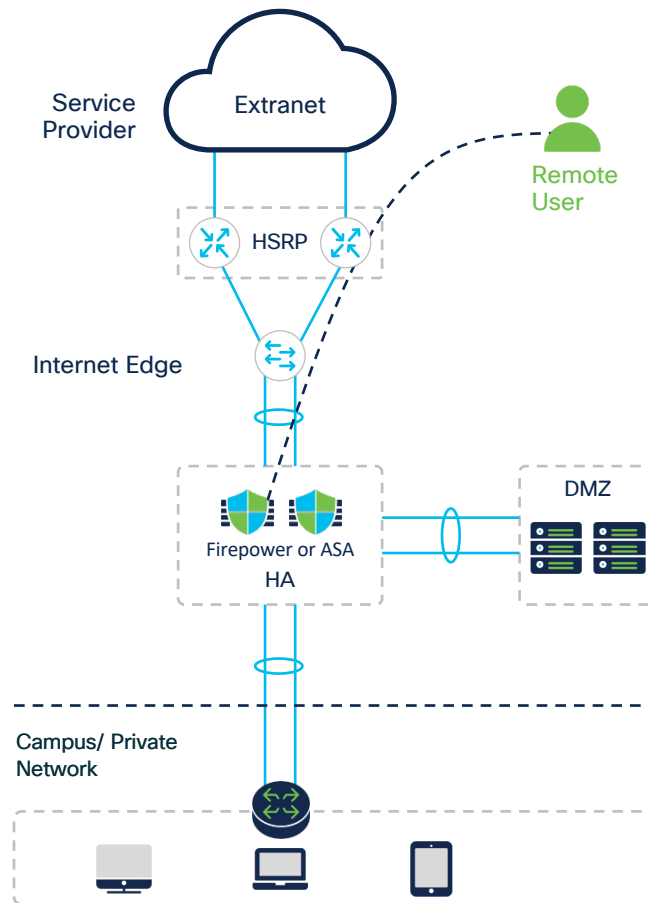
Remote Access VPN (RA VPN)

Key Functions

- Resilience (and scalability)
- Advanced Access Control
- Block access to malicious IP's, URL's, DNS
- Dynamic NAT/PAT and Static NAT
- Remote Access VPN
- Site to Site VPN
- Detecting malicious network traffic
- Visibility and tracking of file transfers, Blocking of malicious files
- Dynamic analysis of unknown files
- Access to private applications

Key Capabilities

- VPN load balancing
- IPSEC and SSL
- Talos Security Intelligence
- AD, LDAP and Radius
- IKEv2
- RADIUS CoA
- Snort IPS
- Advanced Malware Protection
- Malware Analytics Integration
- Zero Trust application Access



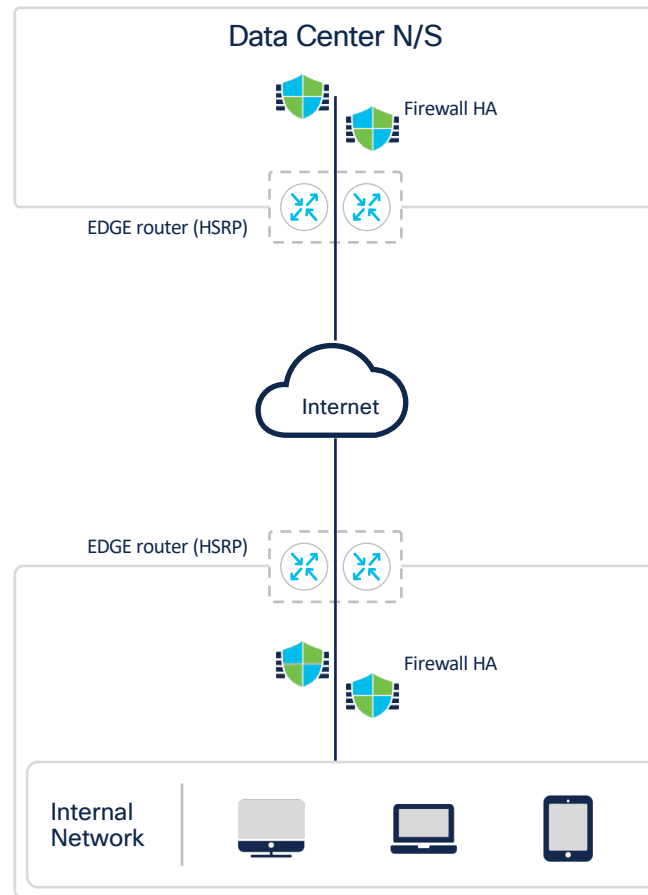
Branch

Key Functions

- Advanced access control options
- Remote Access VPN
- Site to site VPN
- Dual ISP Support
- Block access to malicious IP's, URL's, DNS
- Block traffic to 3rd party lists
- Detecting malicious network traffic
- Visibility and tracking of file transfers, Blocking of malicious files, Dynamic analysis of unknown files
- Application Aware Intelligent Routing (Direct Internet Access)

Key Capabilities

- Applications, URLs, Users, and TrustSec Policy using SGTs
- Cisco Secure VPN
- Route Based VPN
- IP SLA or Traffic Zones
- Talos Security Intelligence
- Threat Intelligence Director
- Snort IPS
- Advanced Malware Protection
- Malware Analytics Integration



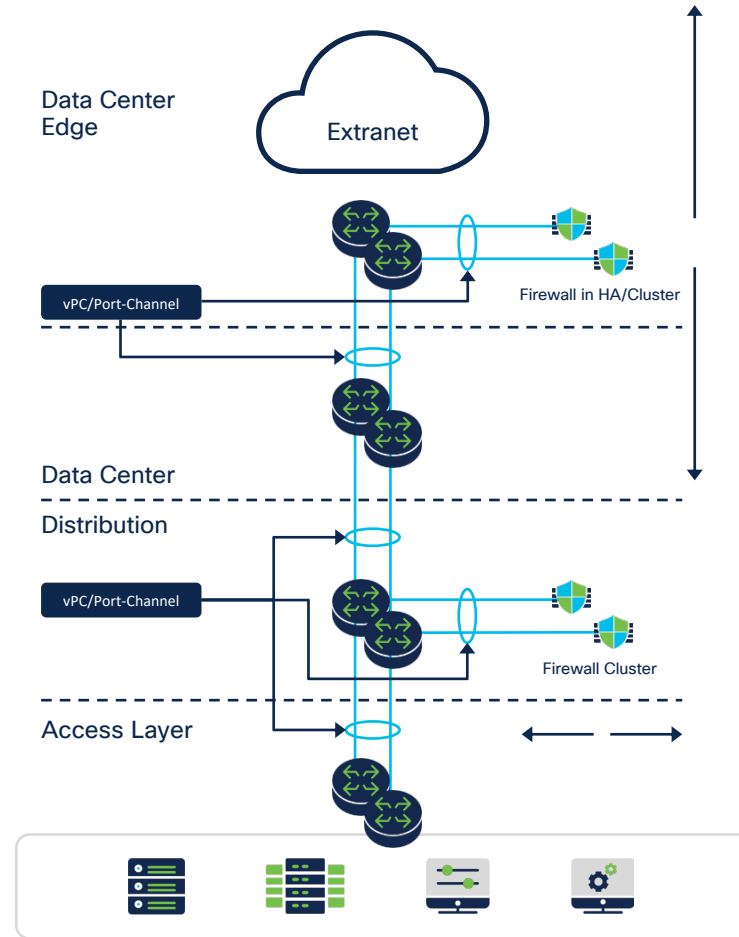
Data Center

Key Functions

- Advanced Access Control
- Low Latency Capabilities
- Scalability and Resilience
- Geographic DC Separation
- Detecting malicious network traffic
- Visibility and tracking of file transfers, Blocking of malicious files
- Dynamic analysis of unknown files
- Firewall Segmentation

Key Capabilities

- TrustSec Policy using SGTs, ACI Policy Control with EPGs
- Hardware Flow Offload
- HA or Clustering
- Inter-site Clustering
- Snort IPS
- Advanced Malware Protection
- Malware Analytics Integration
- Multi-Instance



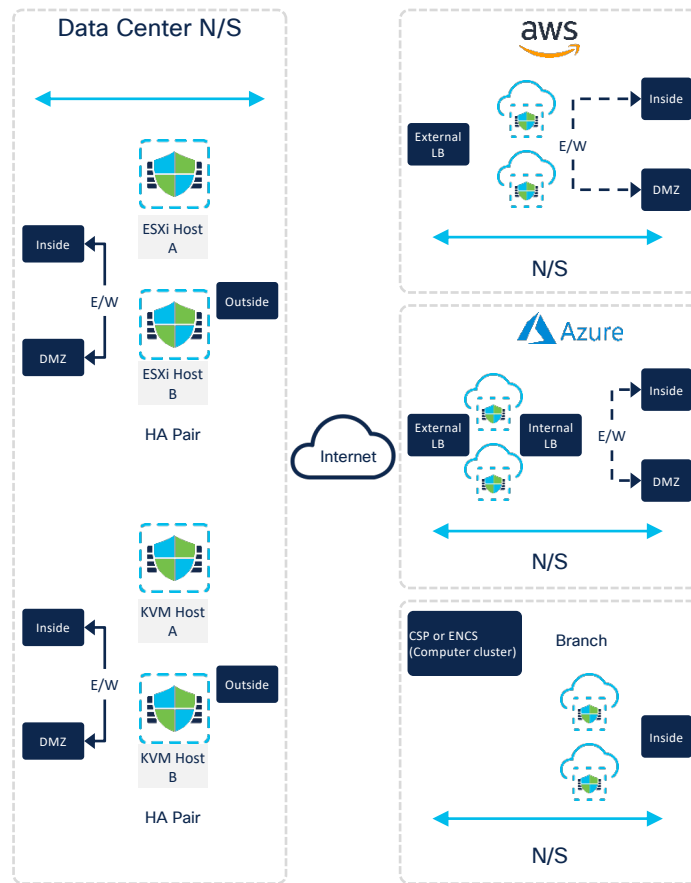
Cloud/Virtual

Key Functions

- Advanced Access Control options
- Remote
- Site to Site VPN
- Block access to malicious IP's, URL's, DNS
- Block traffic to 3rd party lists
- Detecting malicious network traffic
- Visibility and tracking of file transfers, blocking of malicious files
- Dynamic analysis of unknown files

Key Capabilities

- Applications, URLs, Users, and TrustSec Policy using SGTs/CCP
- VPN
- Route Based VPN (ASA) and Policy Based VPN
- Talos Security Intelligence
- Threat Intelligence Director
- Snort IPS
- Advanced Malware Protection
- Malware Analytics Integration



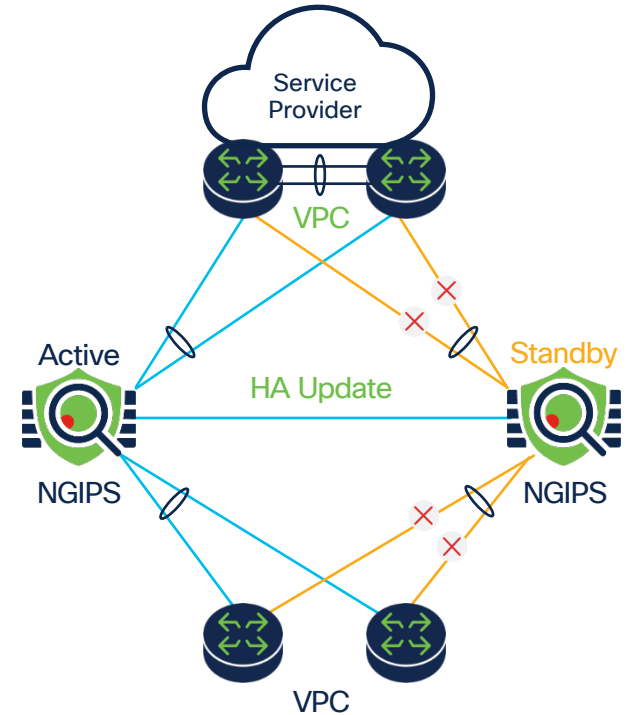
NGIPS

Key Functions

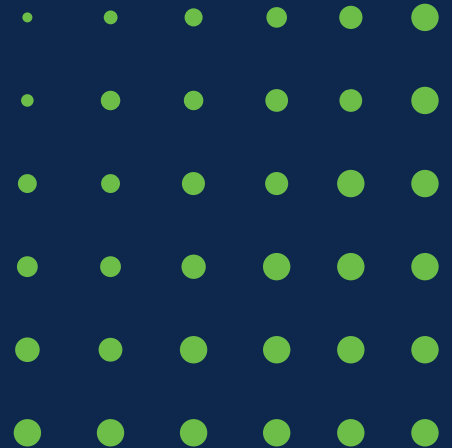
- Advanced access control options
- Block access to malicious IP's, URL's, DNS
- Block traffic to 3rd party lists
- Detecting malicious network traffic
- Visibility and tracking of file transfers, Blocking of malicious files
- Dynamic analysis of unknown files

Key Capabilities

- Applications, URLs, Users, and TrustSec Policy using SGTs
- Talos Security Intelligence
- Threat Intelligence Director
- Snort IPS
- Advanced Malware Protection
- Malware Analytics Integration



Dostęp do labów:
http://cs.co/FTD_NEFO





SECURE