TechClub

Firewall - back to basic

Jiří Tesař jitesar@cisco.com CCIE #14558
Cisco Solution Engineer - Security

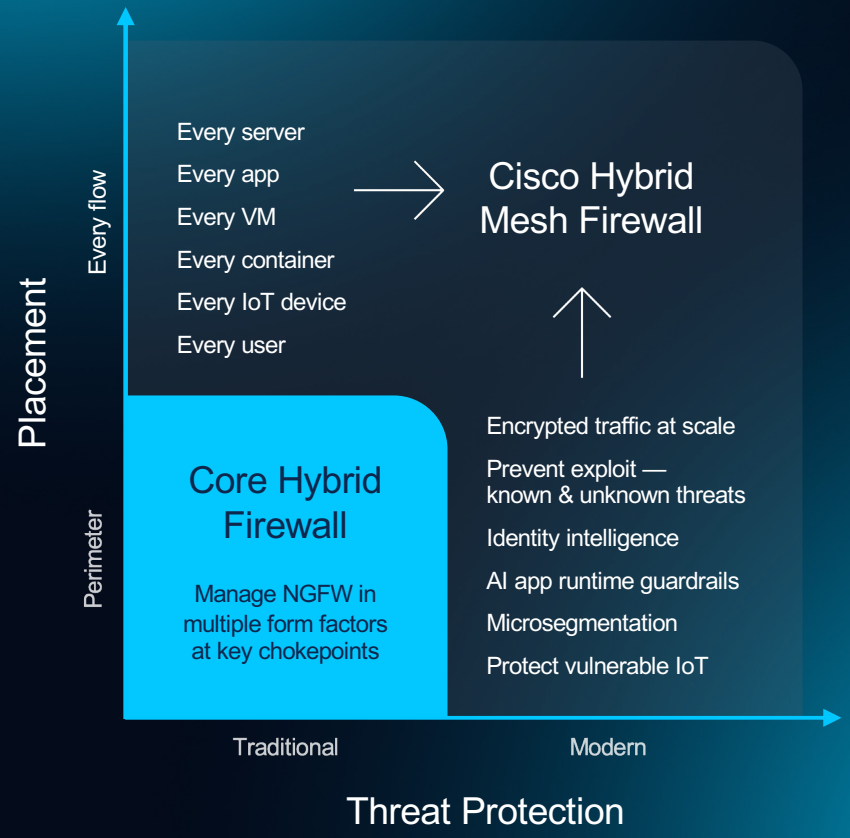
Firewalling needs to evolve to meet today's challenges

Our North Star

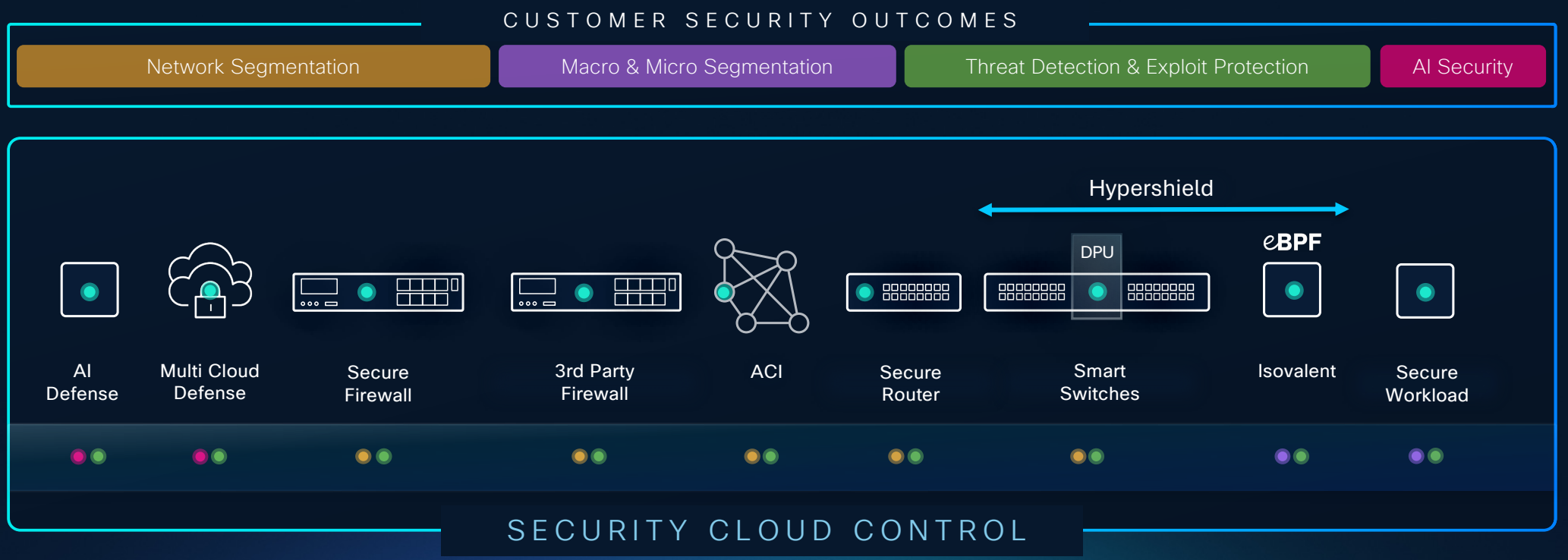
Make it easy for organizations to

- Reduce attack surface
- Prevent compromise
- Stop lateral movement

in the modern data center, cloud, campus, and factory



What is Cisco Hybrid Mesh Firewall

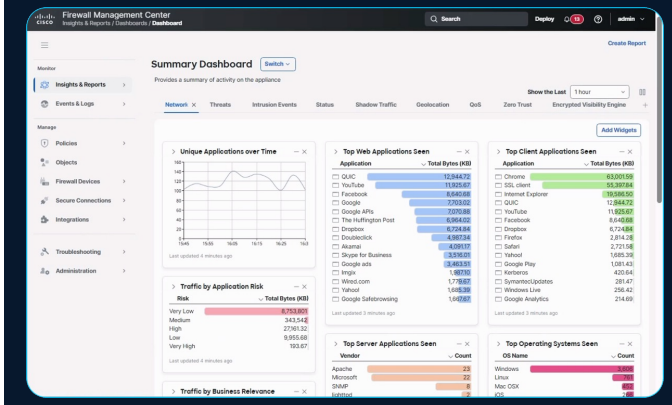


Write policy once, enforce across the mesh

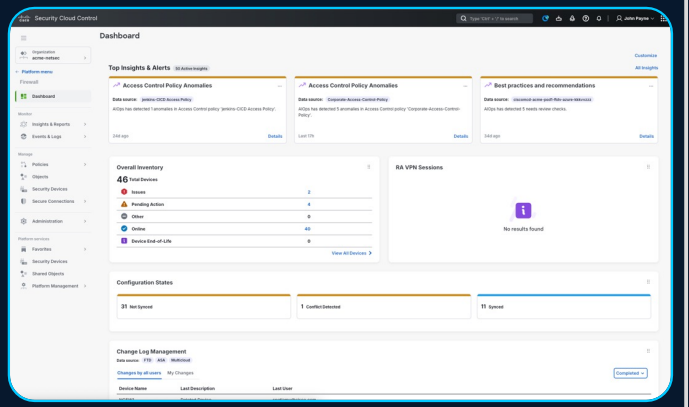
Management Designed for the User

Flexibility of cloud or on-premises options

Firewall Management Center

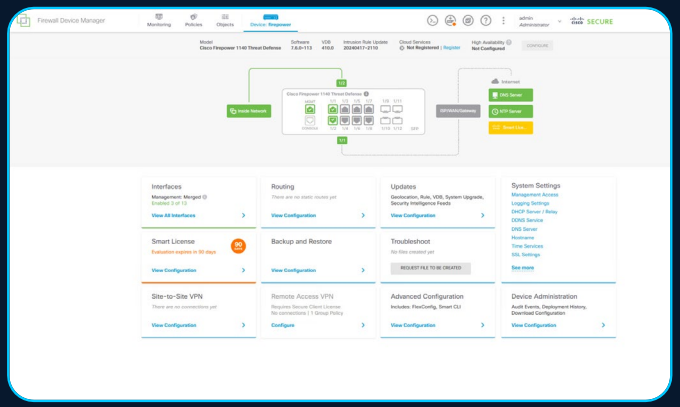


On-premise centralized manager



Cloud-delivered centralized manager via Security Cloud Control

Firewall Device Manager



On-box manager NetOps focused

Firewalls for every use case

ISA 3000 Series	200 Series	1010 & 1100 Series	1200 Compact Series	1200 Series	3100 Series	4200 Series	6100 Series
							
≦0.4Gbps NGFW	1.5Gbps NGFW	≦3Gbps NGFW	≦9Gbps NGFW	≦18Gbps NGFW	≦45Gbps NGFW 16x Clustering	≦145Gbps NGFW 16x Clustering	520-630Gbps NGFW 16x Clustering

IOT | Branch | Campus / Data Center

Private Cloud

HyperFlex
NUTANIX
KVM
openstack
VMware ESXi

Public Cloud

aws
Google Cloud Platform
Microsoft Azure
rackspace technology
ORACLE CLOUD INFRASTRUCTURE
EQUINIX
Alibaba Cloud
alkira

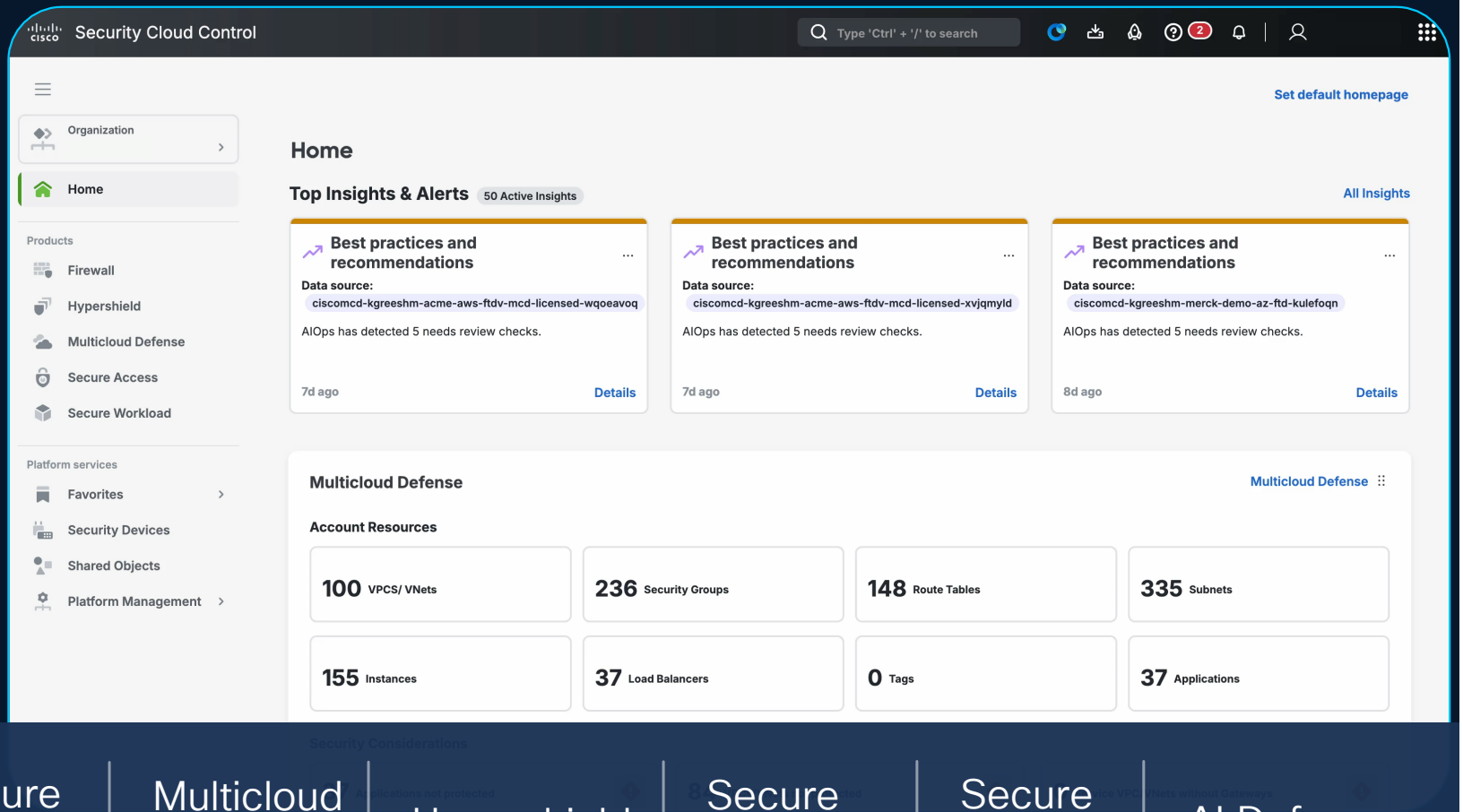
Gov/IC Cloud

aws
Google Cloud Platform

Security Cloud Control

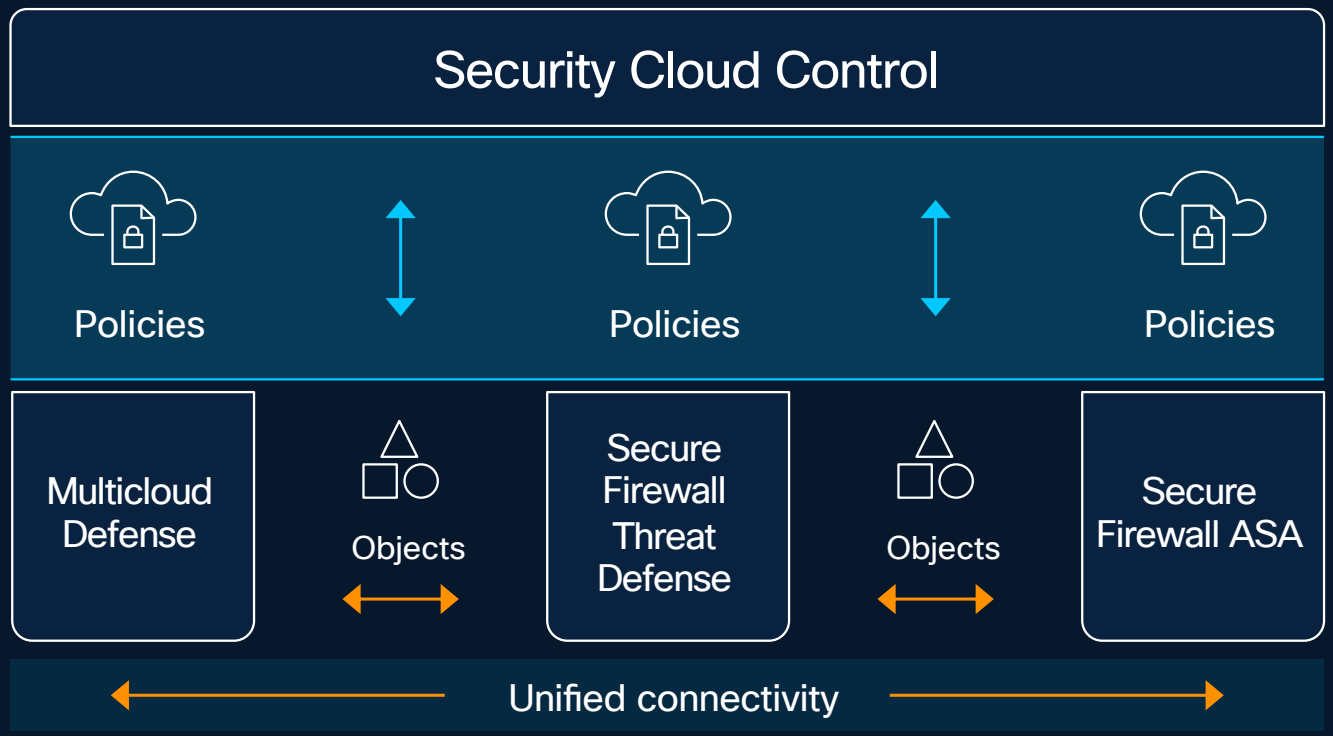
Security Cloud Control

- ✓ Define policy once and enforce everywhere
- ✓ AI-driven best practices
- ✓ Centralized visibility across solutions
- ✓ Consistent user experience



Secure Firewall | Multicloud Defense | Hypershield | Secure Workload | Secure Access | AI Defense

Streamline policy and device control



Centralize coordination of all ASA and FTD form factors
eliminating complexity across diverse environments

Ensure consistent security policies and compliance reducing misconfigurations

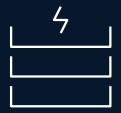
Automate object updates
saving time for strategic initiatives

Retain on-premises FMC or manage firewalls directly from Security Cloud Control
allowing you to migrate to the cloud at your own pace

Security Cloud Control Firewall Management

Cloud-based **firewall management** with policy configuration, cloud analytics, and logging

Same look and feel as on-premises FMC, no learning curve for existing users



Easy brownfield migration with support for up to 1200 firewalls

AI Assistant and AIOps

Cisco ensures uptime, patching, and updates. SOC2!

Secure Firewall

hybrid deployments

cisco

Simple onboarding experience for Secure Firewall

Registration key-based Onboarding

Use CLI Registration Key

Onboard a device using a registration key generated from SCC and applied on the device using the Command Line Interface. (FTD 7.0.3+ & 7.2+)

Zero-touch Provisioning using Serial Number

Use Serial Number

Onboard a factory-shipped FTD 7.2+ device to cdFMC or a 7.4+ On-Prem FMC using zero-touch provisioning.

Deploy FTDv to Public Cloud

Deploy an FTD to a cloud environment

Deploy a device to supported cloud platforms: AWS, GCP, and Azure.

Bulk Onboarding multiple devices using CSV file

Bulk Onboard using CSV File

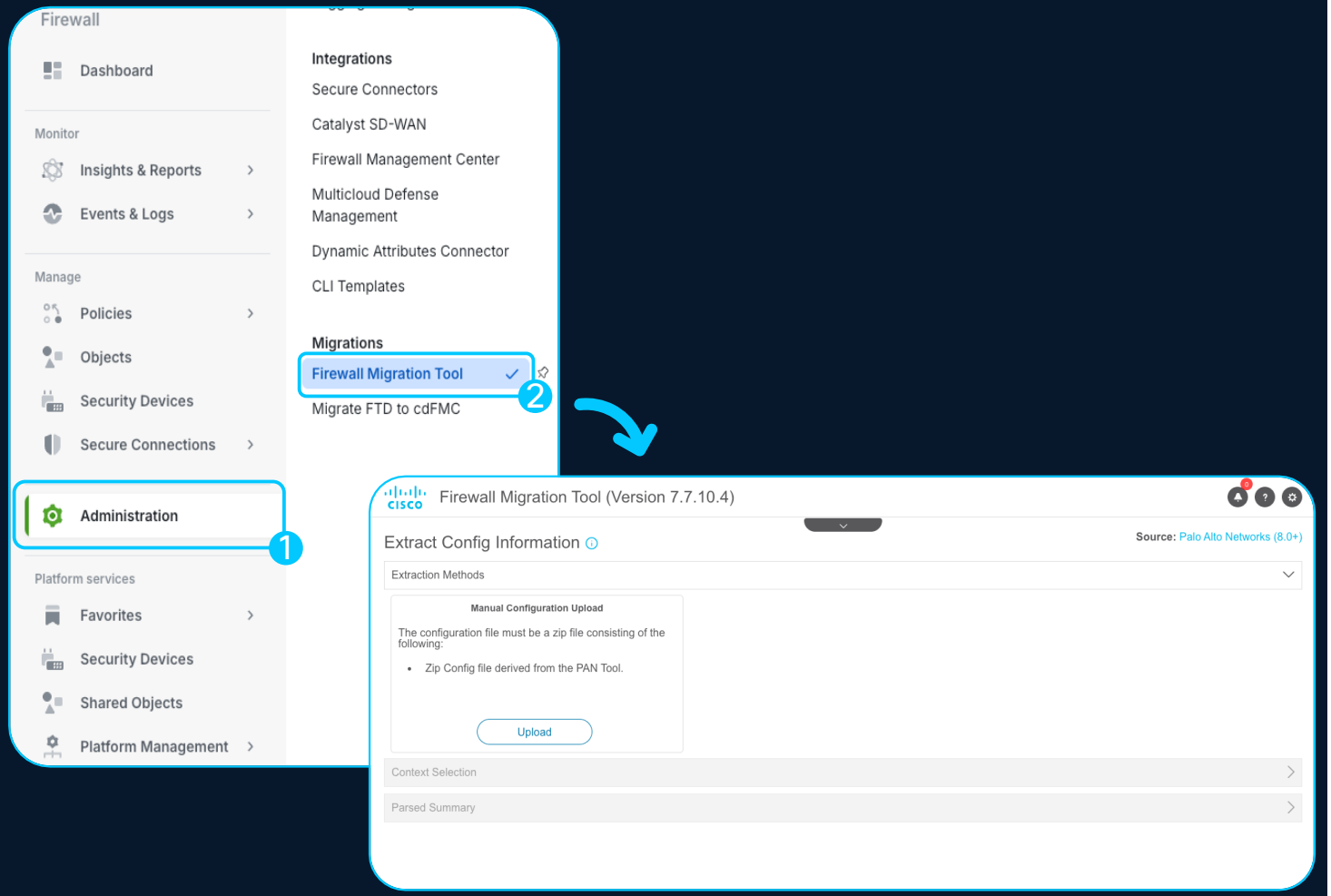
Use this method for adding multiple devices by uploading a .csv file, with template assignment. (FTD 7.4+)

SD-WAN Wizard - Simplification & Automation

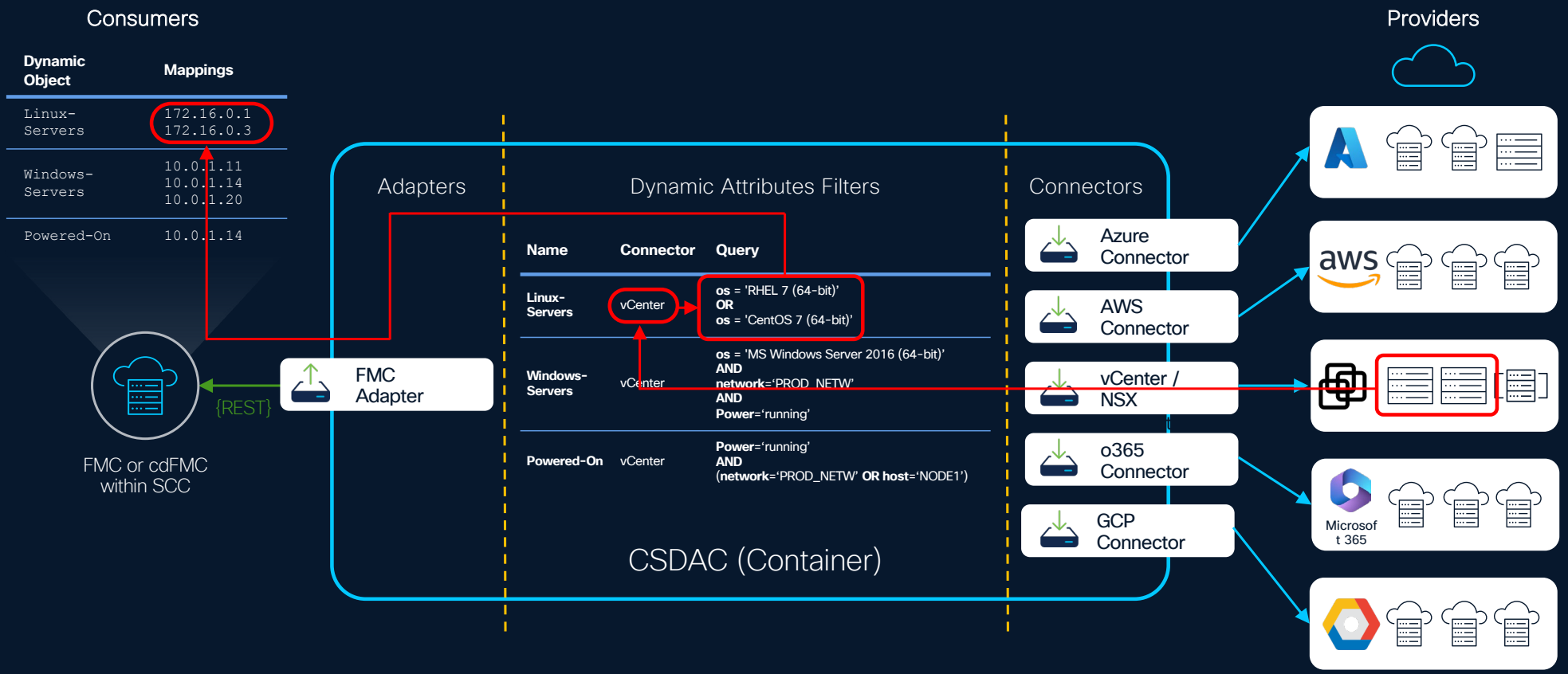
Steps	1. Hub	2. Spoke	3. Authentication	4. SD-WAN Settings
User Input	• Single / Dual Hub CSF device • DVTI Interface • IP Pool for Spoke Tunnels	• CSF Devices • VPN Interface Selection	• No input required • Can modify if required	• Security Zone for spoke tunnel interface • Overlay routing using BGP
Automated	• Auto population of dVTI Interface parameters • BGP Overlay Configuration	• Auto generate sVTI interface for each Hub • FMC assigns IP to sVTI interfaces • Bulk spoke addition • Auto generate Unique Local Tunnel ID for each spokes	• Auto generation of Pre-shared Key • Auto selection of IKE and IPsec policies	• Automatic addition of generated sVTI to Security Zone for easy AC policy rule update • Generate BGP neighbor and route map configuration for overlay interface and networks

Firewall 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



Architecture of the Dynamic Attributes Connector



Cisco Secure Dynamic Attributes Connectors – your bridge to dynamic data

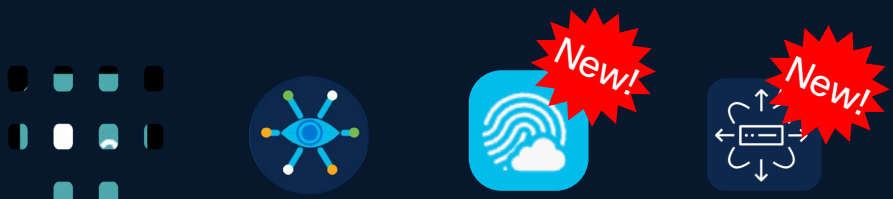
Cloud Connectors

AWS Azure GCP VMWare

Azure Service Tags | Security Groups | Service Tags | Multicloud Defense

Public Feeds and External Connectors

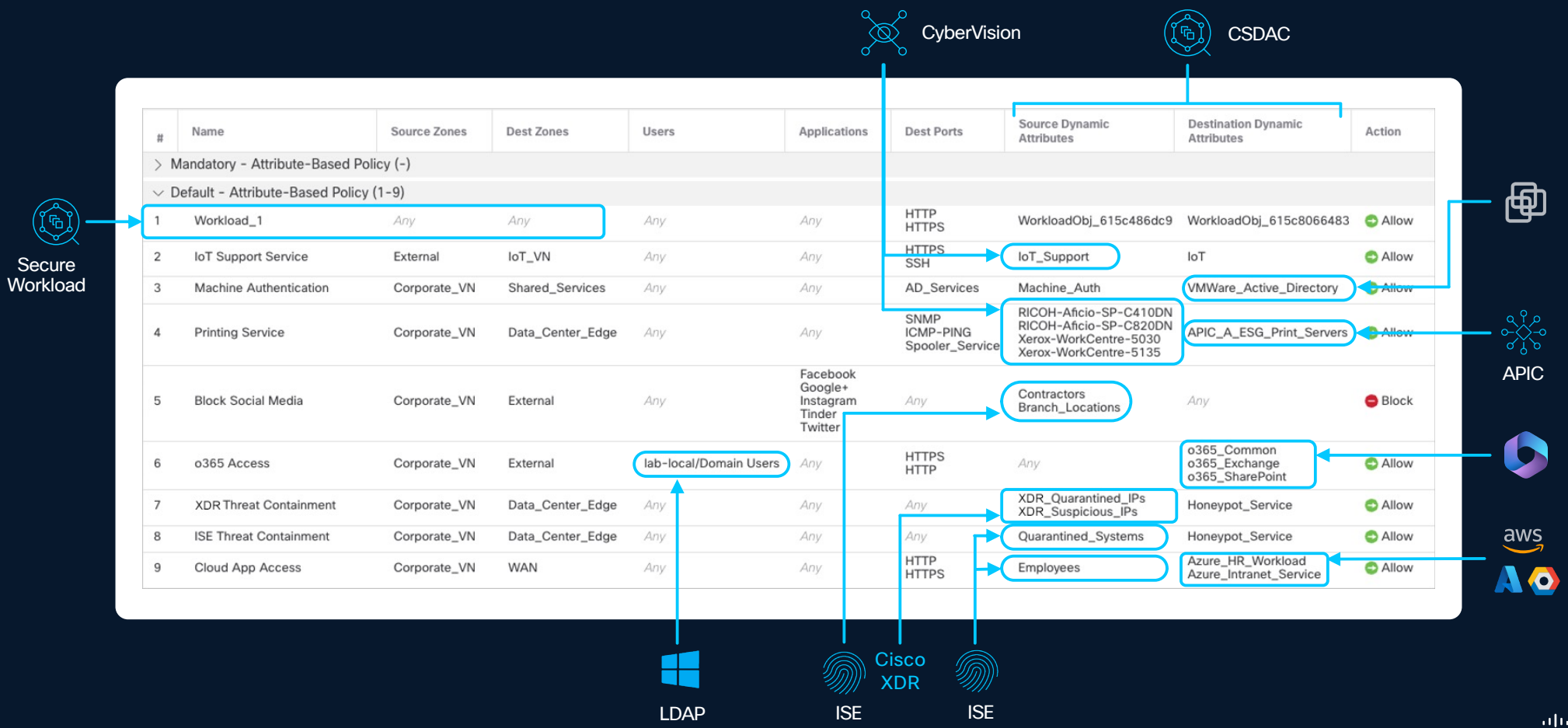
Office365 Webex Zoom GitHub



Generic Text | Cyber Vision | pxGrid Cloud | ACI

cisco

Attribute-based Policy with User and Server Identity

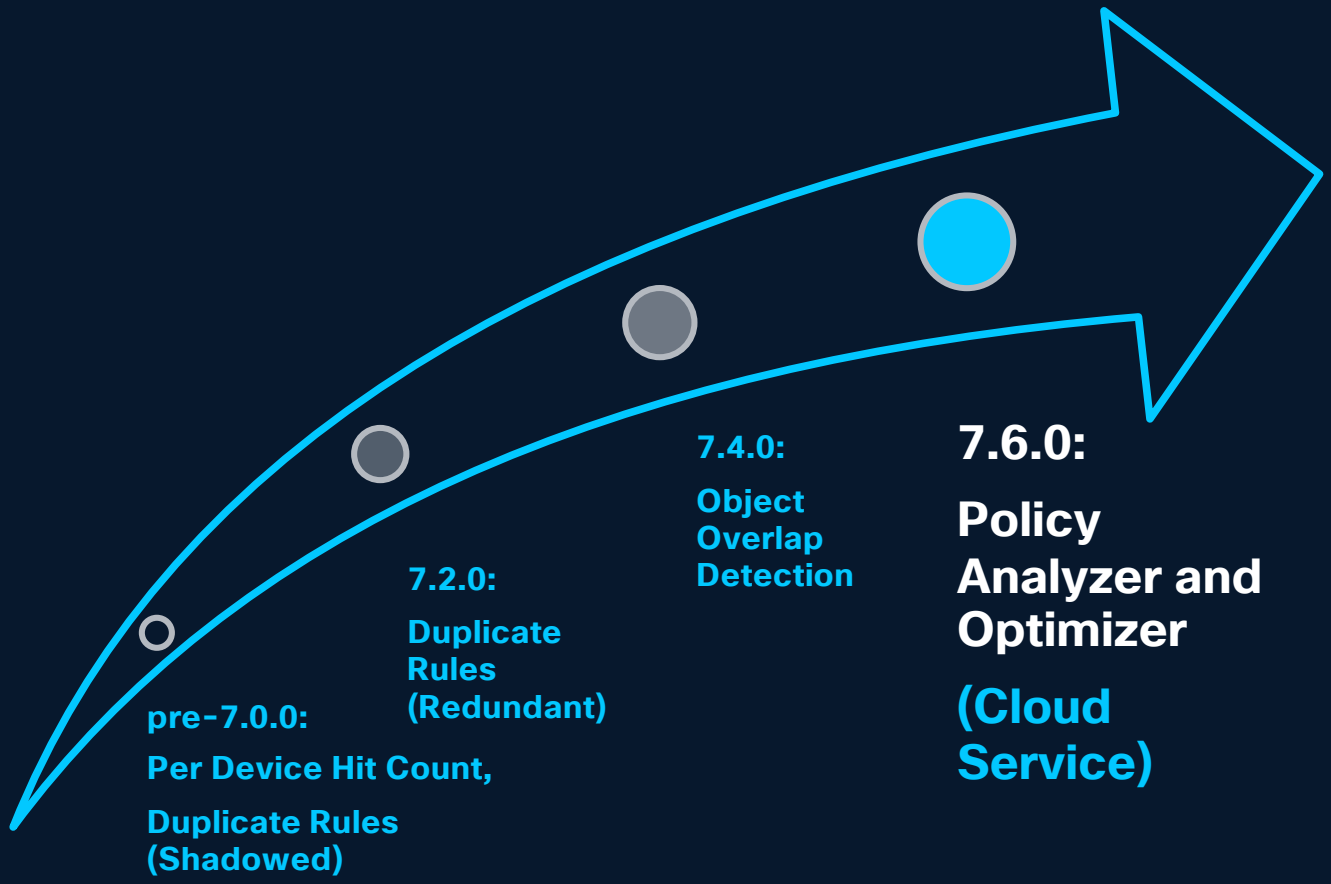


#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
>	Mandatory - Attribute-Based Policy (-)								
v	Default - Attribute-Based Policy (1-9)								
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	XDR Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	XDR_Quarantined_IPs XDR_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

AgenticOps

Policy Analyzer & Optimizer

The Road to Policy Analyzer & Optimizer (PAO)



The Policy Analyzer and Optimizer (PAO) provides:

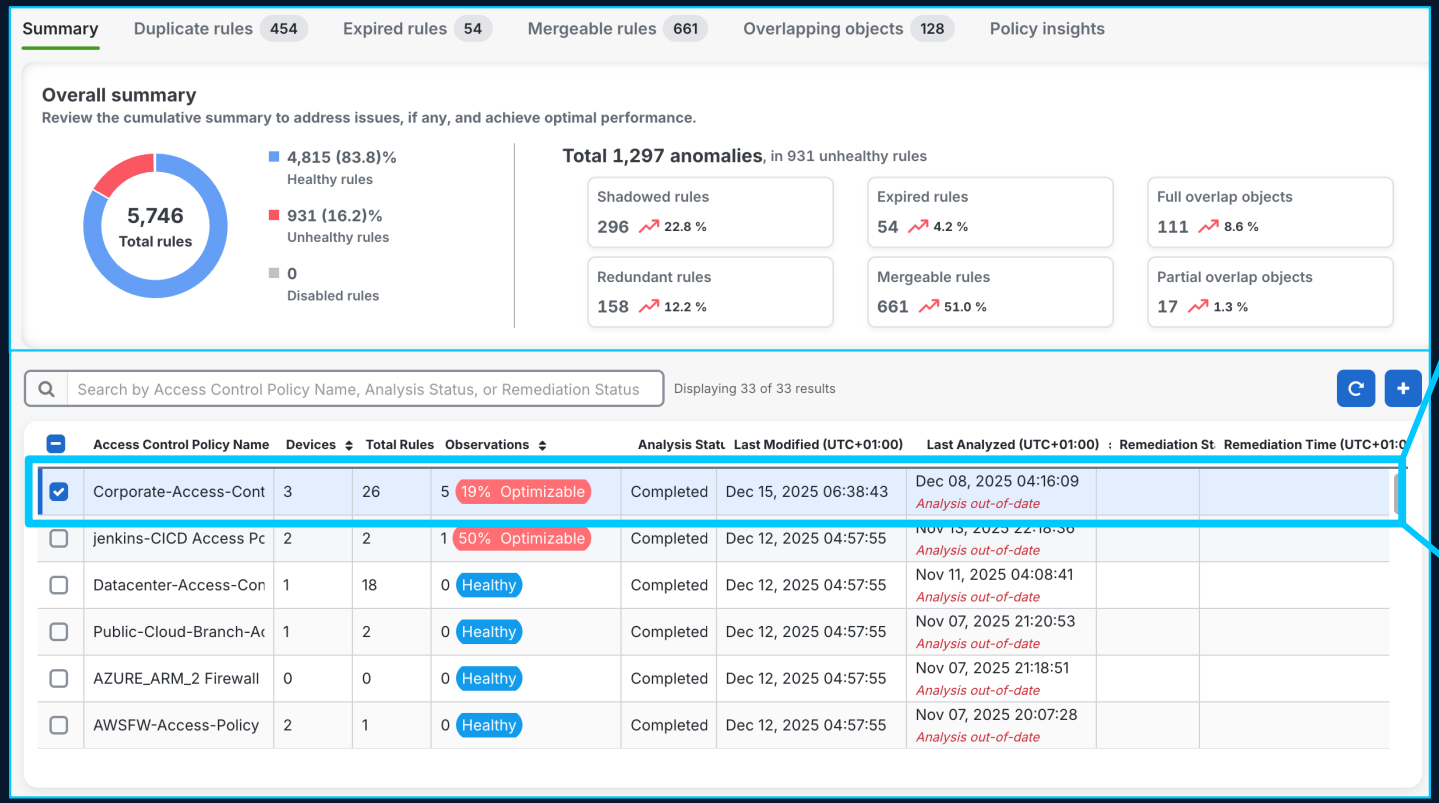
- Expiry Rule Detection
- Mergeable Rule Detection
- Hit Count Insights
- Remediation
- And is Version Agnostic

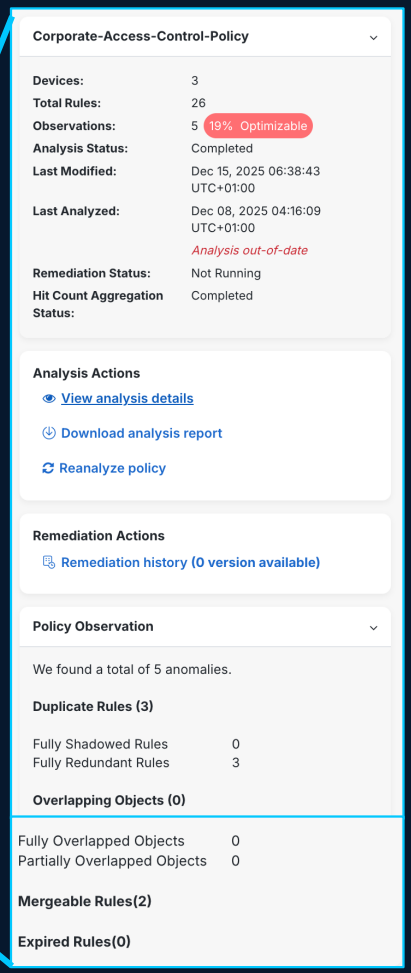
cisco

Policy Analyzer and Optimizer

Policy Validation

- Achieve proactive security policy validation:
  - Enhancing posture and hygiene
  - Optimizing resources





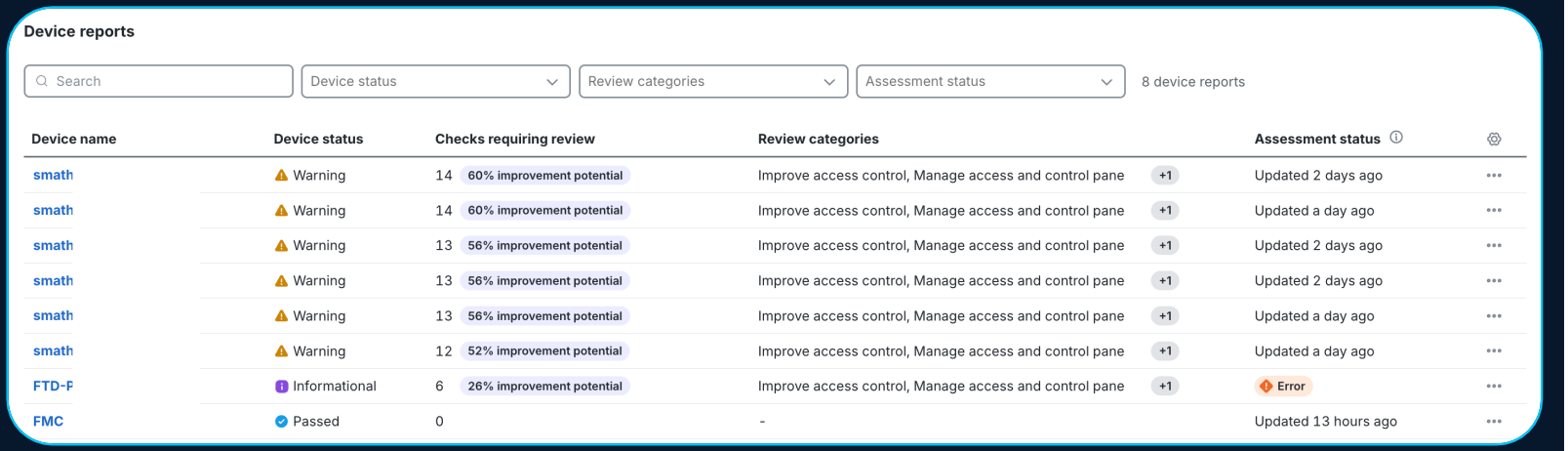
Best Practices & Recommendations

Best practices and recommendations

Technical Overview

The firewalls are evaluated against Cisco-defined best practices and then assigned a score to highlight their scope for improvement.

The list can be filtered by criticality and categories to assist with proper prioritization.



Device reports

Search | Device status | Review categories | Assessment status | 8 device reports

Device name	Device status	Checks requiring review	Review categories	Assessment status
smath	Warning	14 60% improvement potential	Improve access control, Manage access and control pane +1	Updated 2 days ago
smath	Warning	14 60% improvement potential	Improve access control, Manage access and control pane +1	Updated a day ago
smath	Warning	13 56% improvement potential	Improve access control, Manage access and control pane +1	Updated 2 days ago
smath	Warning	13 56% improvement potential	Improve access control, Manage access and control pane +1	Updated 2 days ago
smath	Warning	13 56% improvement potential	Improve access control, Manage access and control pane +1	Updated a day ago
smath	Warning	12 52% improvement potential	Improve access control, Manage access and control pane +1	Updated a day ago
FTD-F	Informational	6 26% improvement potential	Improve access control, Manage access and control pane +1	Error
FMC	Passed	0	-	Updated 13 hours ago

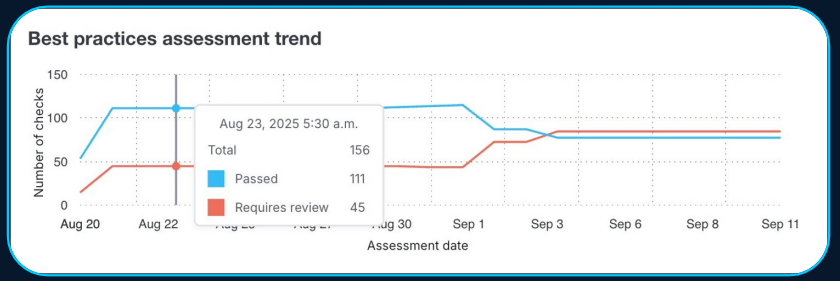
Best practices and recommendations

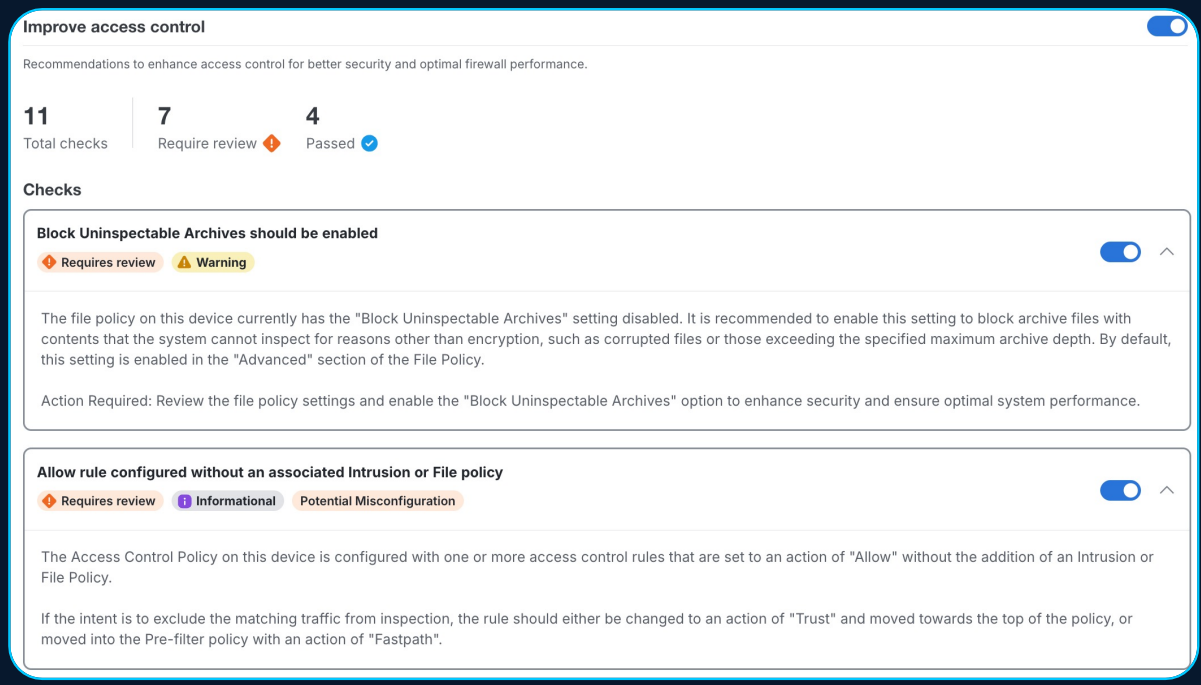
Technical Overview

Detailed insights into individual tests and the remediation steps are provided to assist in configuring the features according to best practices. The tests are tagged to prioritize critical configurations.

A trend graph is plotted to showcase the evolution of best practices in your configuration over time.

Detailed reports can be downloaded from the dashboard for the purpose of compliance monitoring



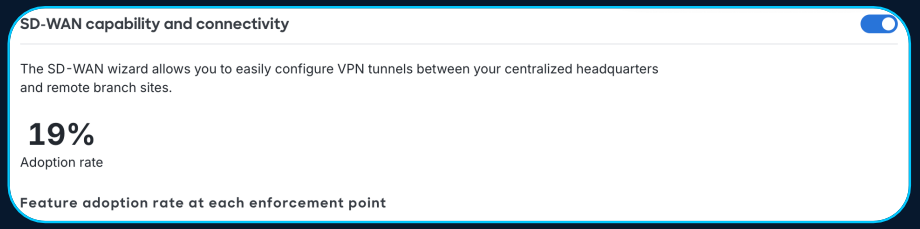


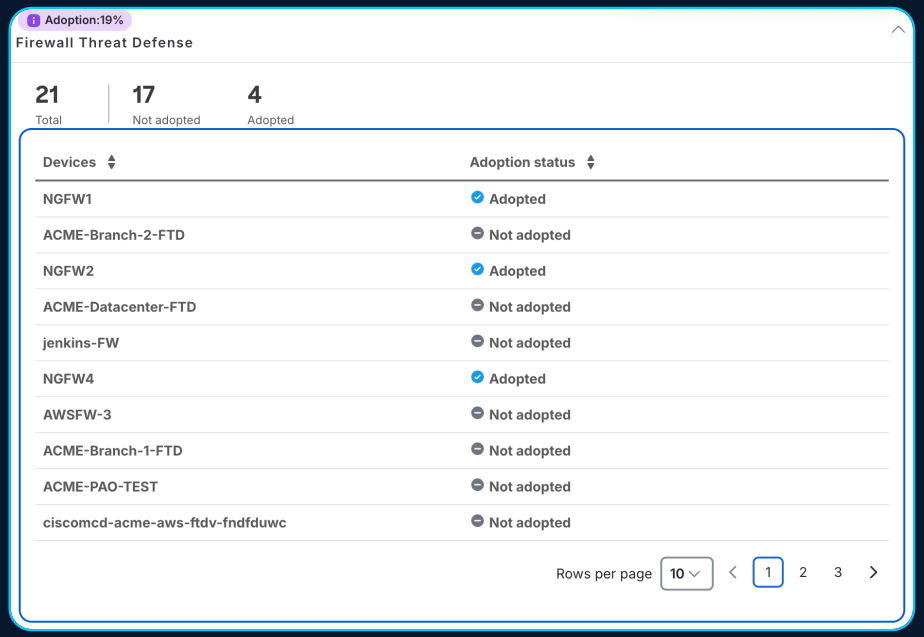
Feature Adoption

Feature adoption

Technical Overview

The dashboard provides quantitative insights into utilization of feature sets available for customers with adoption status highlighted for individual firewalls.





Feature adoption

Technical Overview

Get built in step-by-step guidance with video tutorials to help improve your feature adoption.

SD-WAN Capability and Connectivity Learn more

Software-Defined Wide Area Network (SD-WAN) VPN topology for Firewall Threat Defense devices

Steps to improve your feature adoption rate efficiency:

1) Create dynamic virtual tunnel interfaces in the devices.

   Go to **Device Management(Devices > Device Management)** page in Cloud-delivered FMC and edit the required devices to create dynamic virtual tunnel interfaces.

2) Go to **Site To Site(Devices > VPN > Site To Site)** page.

3) Launch the SD-WAN Wizard.

   Click Add, select SD-WAN Topology, and click Create.

4) Click Add Hub in the Hubs section.

   Choose a device, choose or create a dynamic virtual tunnel interface, enter a hub gateway IP address, and click Add.

5) Click on Add Spoke in the Spokes Section

   Choose a device and VPN interface, and click Add.

6) Click Next.

7) In the Authentication Settings section , configure the required settings, and click Next.

8) In the SD-WAN Settings section, choose the Spoke Tunnel Interface Security Zone, click Next, and click Finish.

cisco

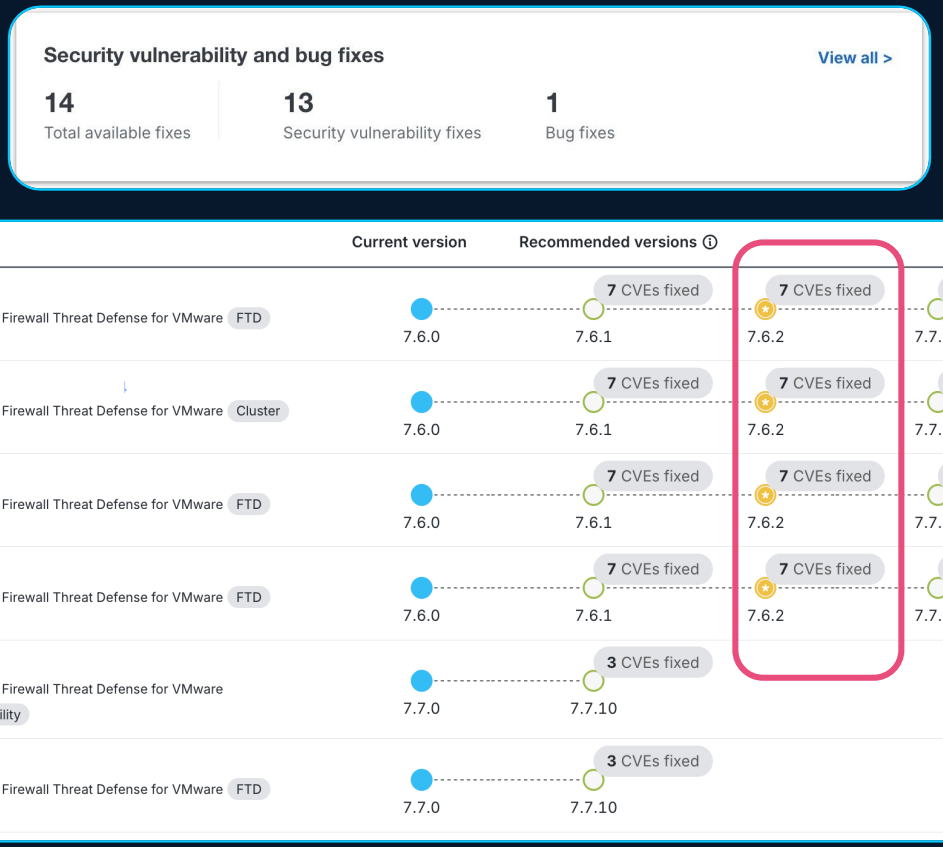
Software Upgrade Planner

Software upgrade planner

Technical Overview

The planner lets you compare the current version with the latest ones by showcasing CVE fixes and feature advancements.

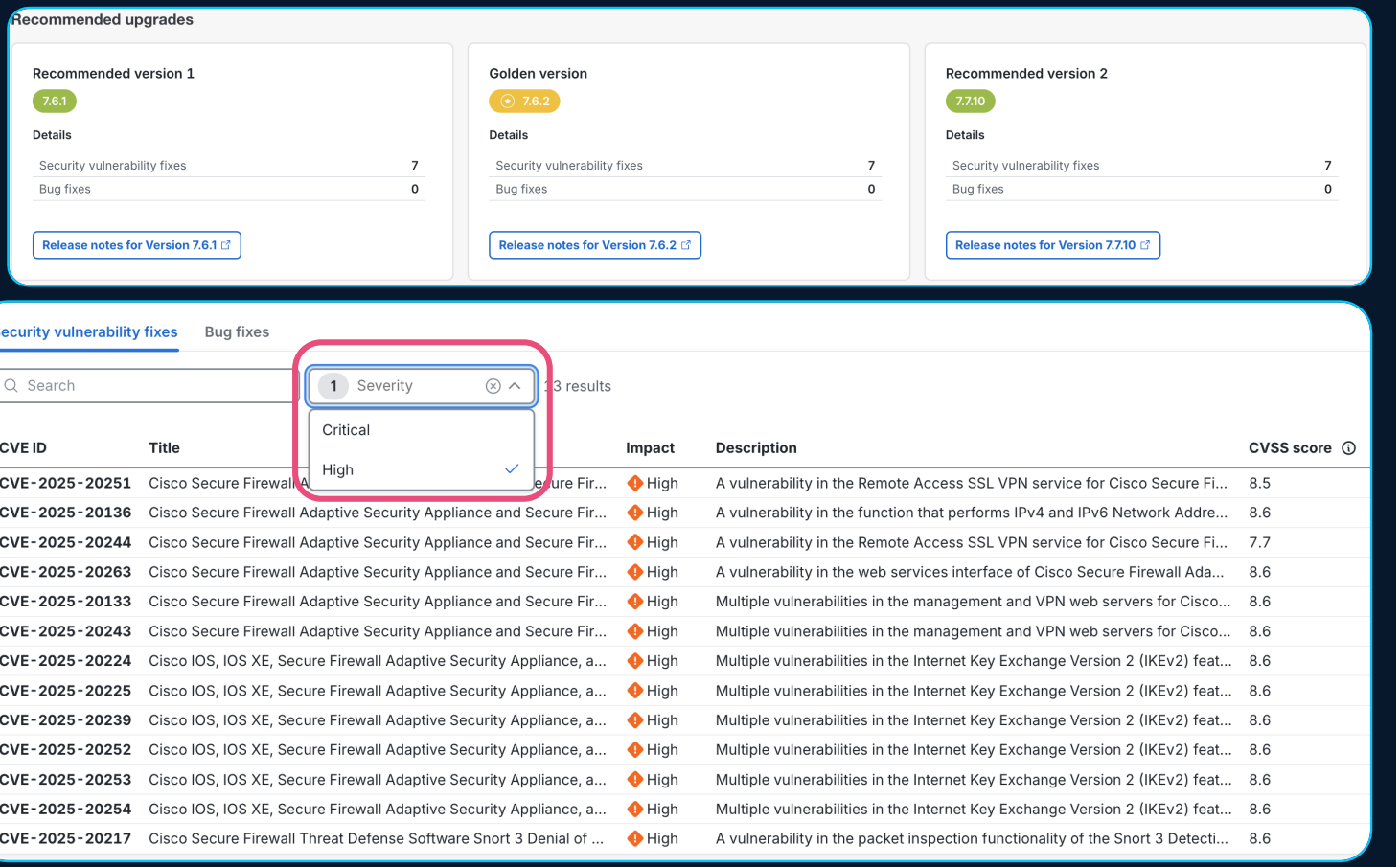
Cisco's recommended "Golden Image" is also highlighted here.



Software upgrade planner

Technical Overview

For each firewall, the dashboard also provides detailed insights into the CVE and bug fixes for the recommended updates, which can be sorted by severity level, allowing the security admin to make an informed decision.

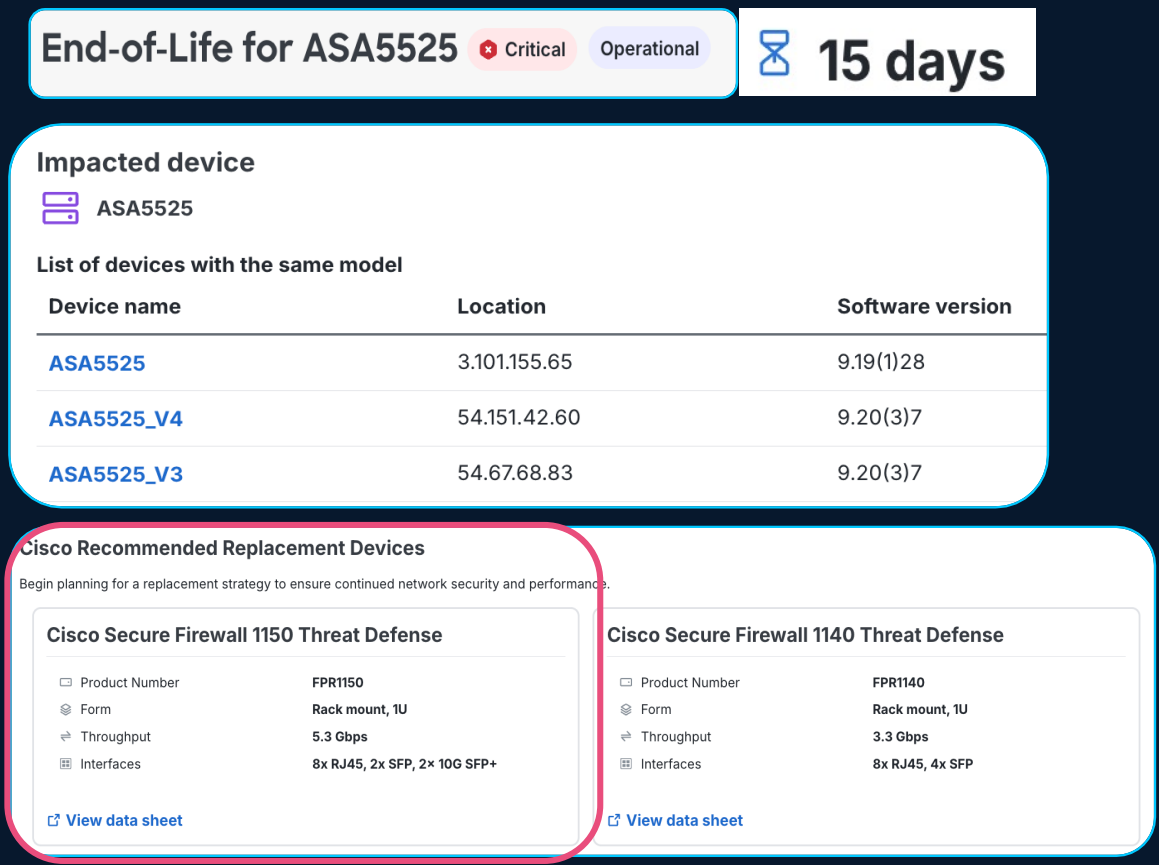


End of Life Planner

End of life planner

Technical Overview

The dashboard highlights the list of firewalls that are about to hit EOL with Cisco's recommended device for replacement.



Security Cloud Control

Define policy once and enforce anywhere

Cisco Firewalling | AI Defense | 3rd Party Firewalls

Secure Firewall | Secure Workload | Hypershield

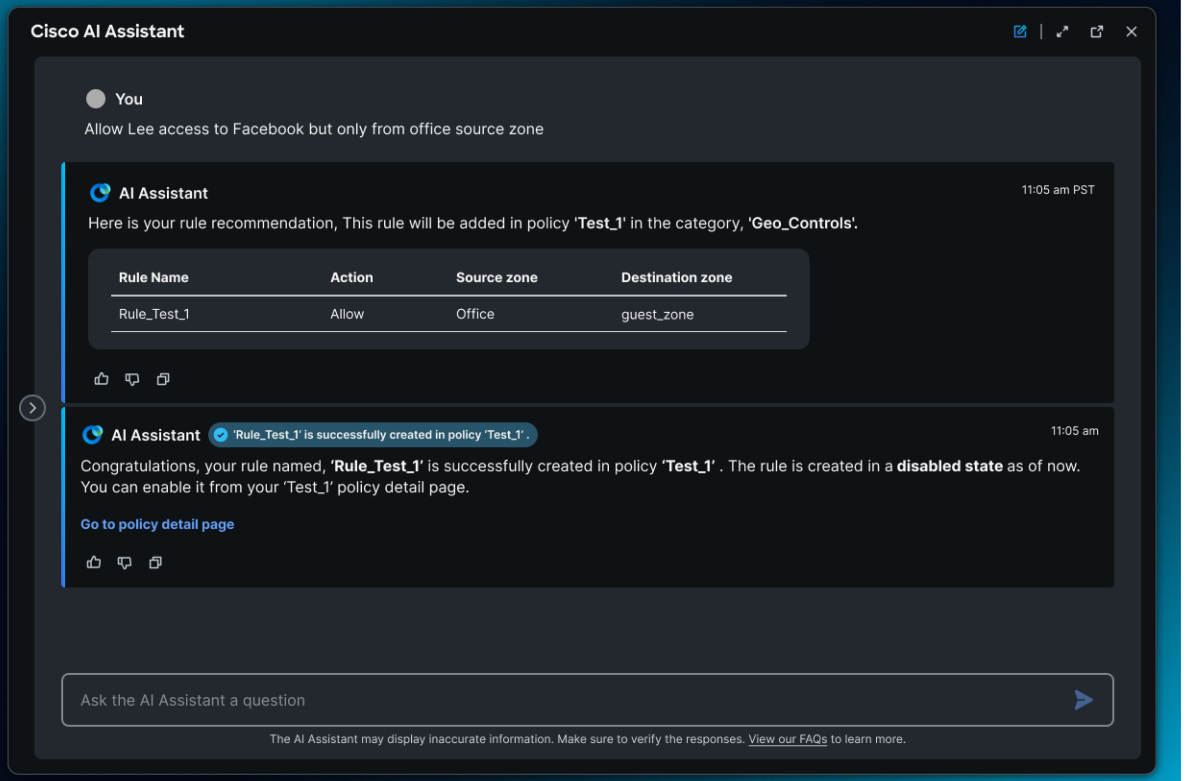
Secure Access (FW as a service) | Secure Router NGFW

Unified AI Assistant:
Simplify policy administration **by up to 70%**

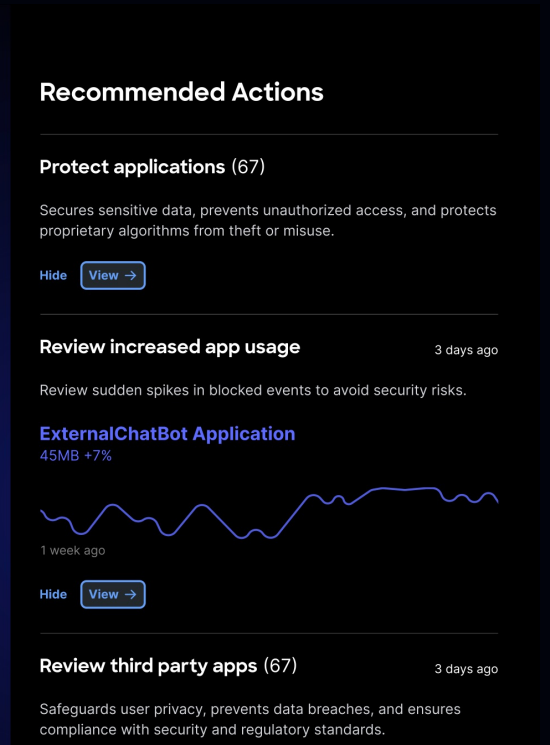
cisco

Reduce management overhead with AI Assistant

Assist	+ Policy configuration
Augment	+ Troubleshooting
Automate	+ Policy lifecycle management



AI Defense



Visibility of underlying models and data

Model Validation and guardrail recommendations

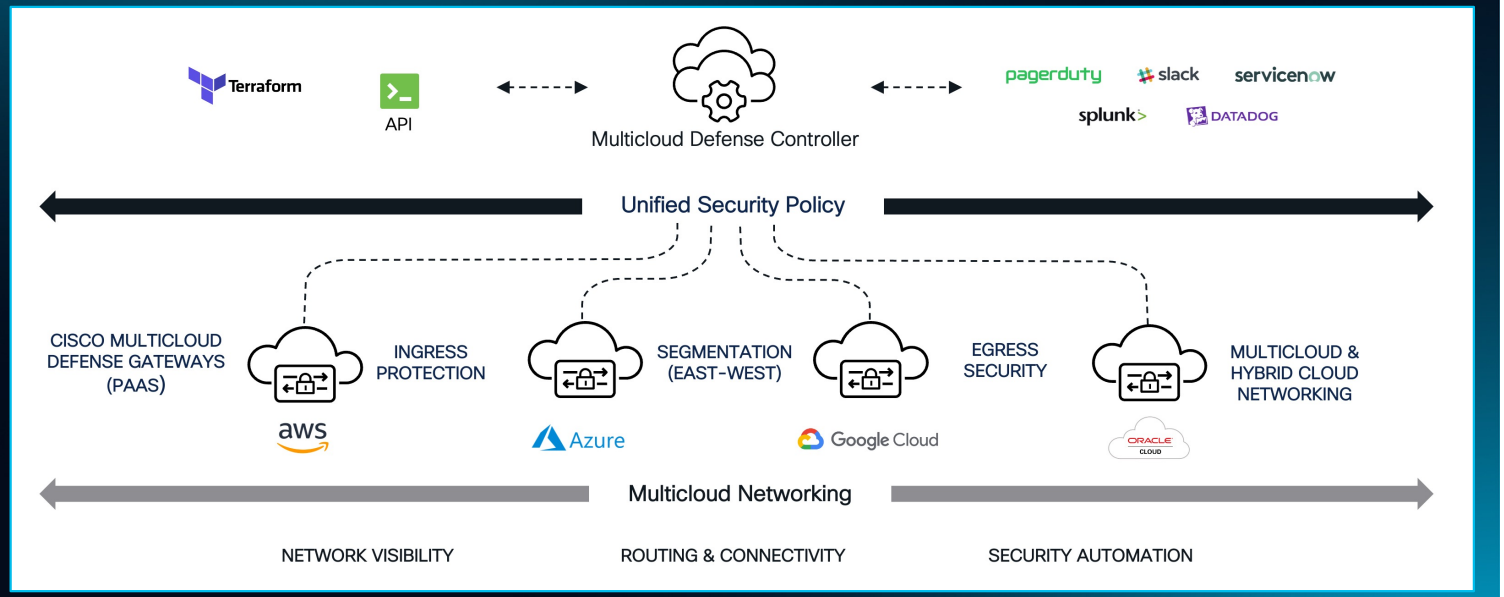
Runtime enforcement across public and private clouds

Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls

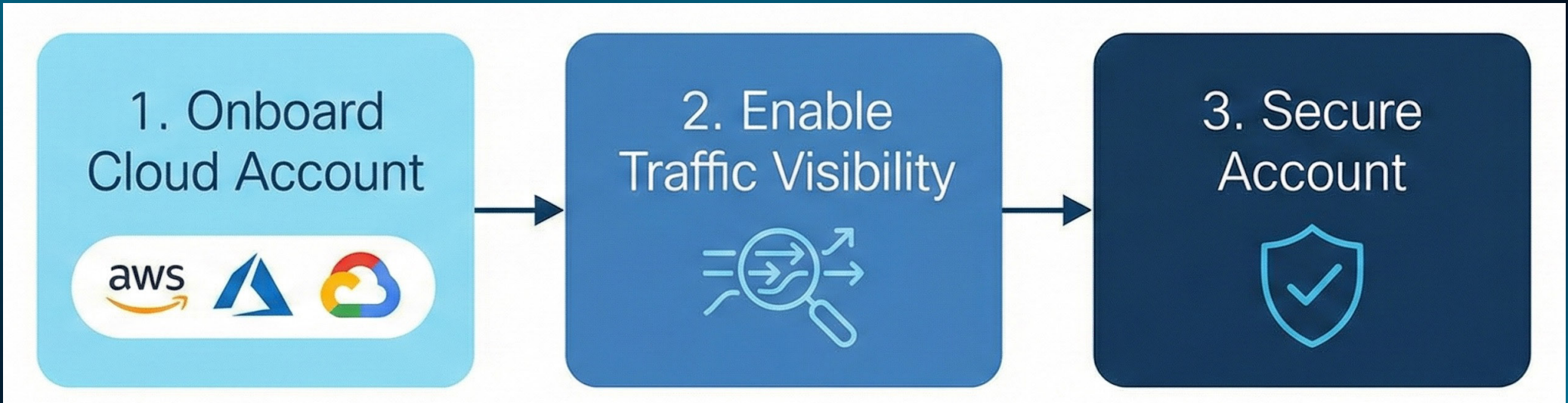
BRKSEC-2229

- Centralized Management
- Multi-region and Multi-AZ architecture
- Autoscale and Auto Heal
- Gateway lifecycle management
- Traffic engineering
- Unified dynamic policies



Cisco Multicloud Defense Workflow

Multicloud Defense Controller



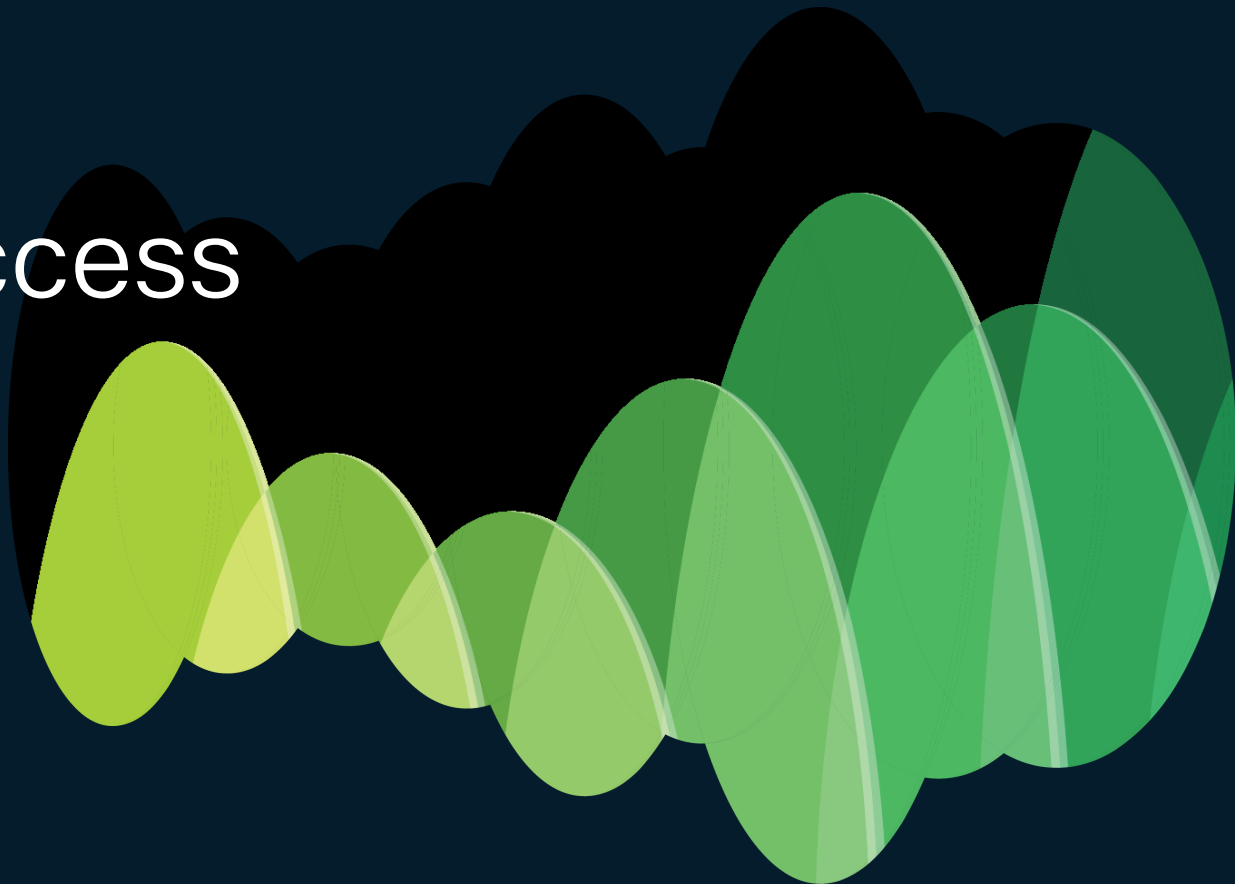
Securely onboard cloud accounts

Enable DNS query & VPC/NSG flow logs

Orchestration & Automation

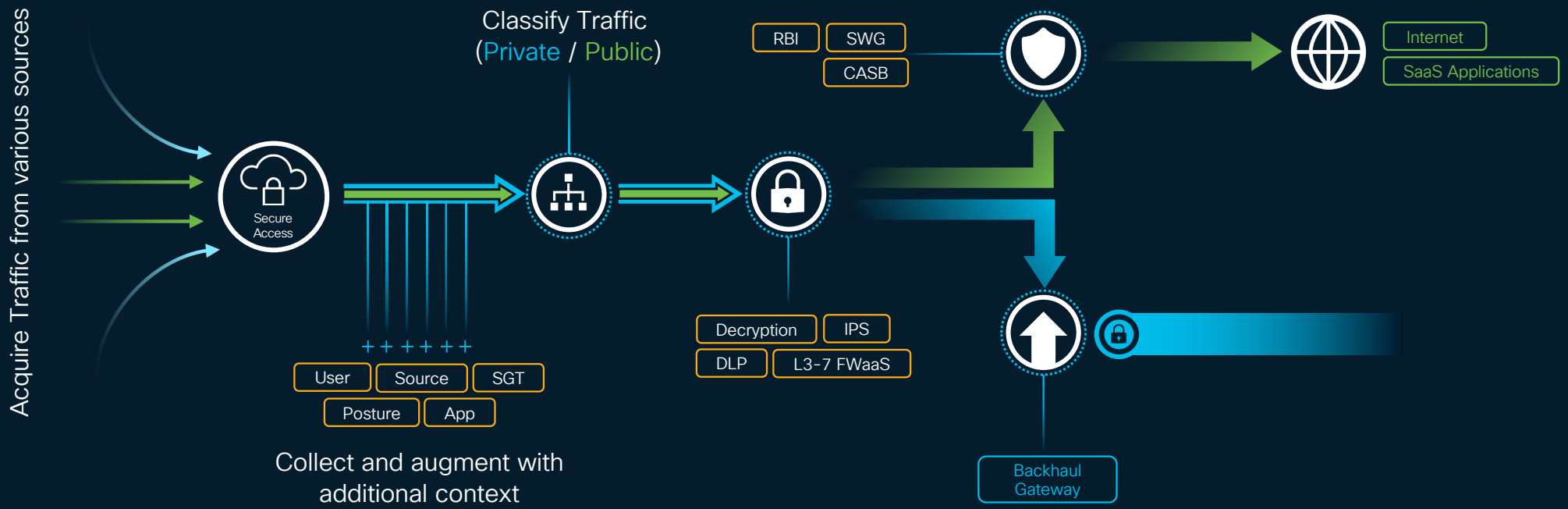
Orchestrate, manage, control, and secure cloud infrastructure using Multicloud Defense

Cisco Secure Access



Unified Cloud Architecture

Universal Traffic Acquisition & Single Data Path

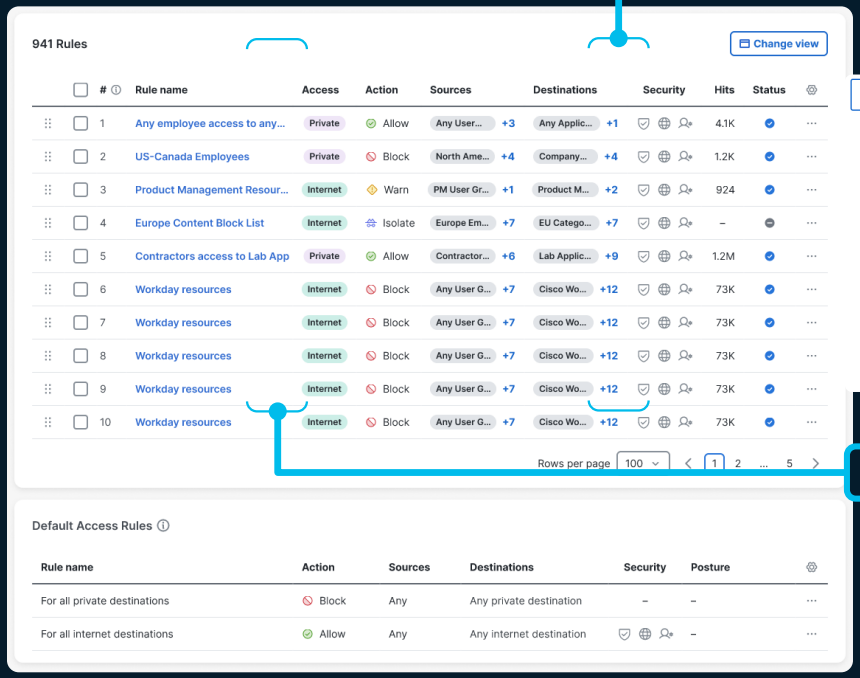


Unified Cloud Architecture

Consistent Policy & Security

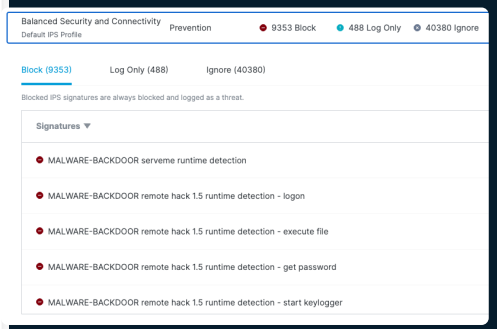
Secure Access

Unified Policy Evaluation



Consistent Security Enforcement

- Transit agnostic
- Private & Internet enforcement
- Per application / destination



Full IPS

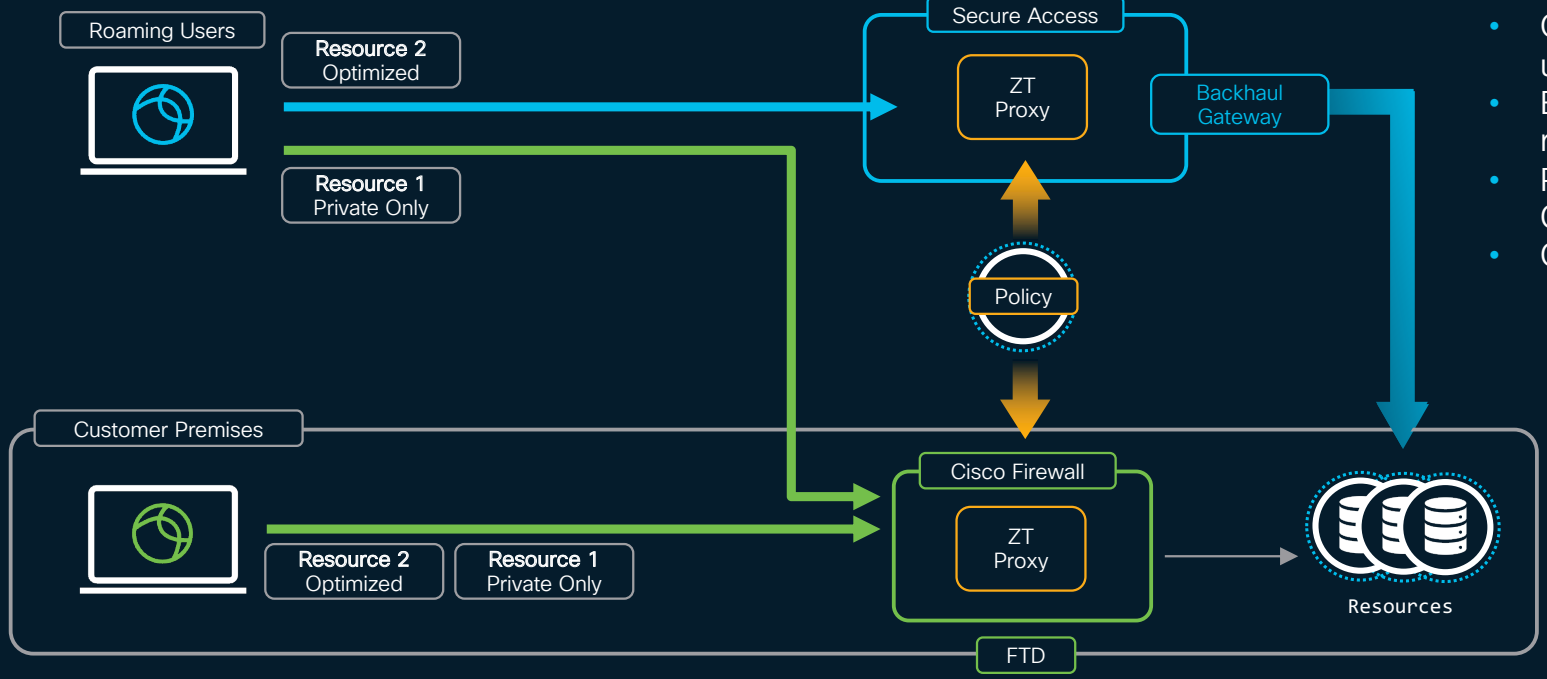
- Built on Snort 3.0
- Complete Signature Set
- TALOS updated

Unified Internet + Private Policy

- Single view of all access
- Filter and sort view
- No need to pivot

Universal ZTNA

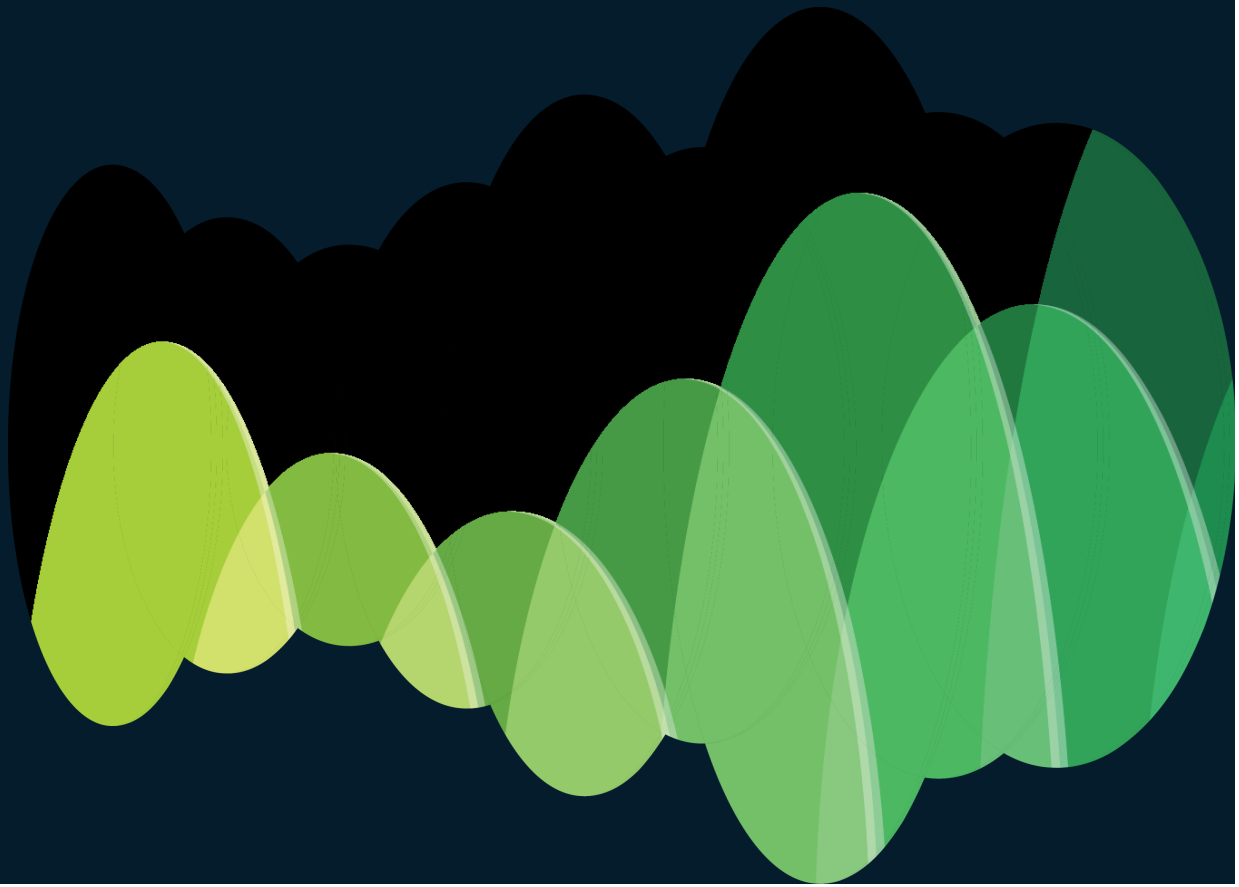
Single Policy, Distributed Enforcement (Overview)



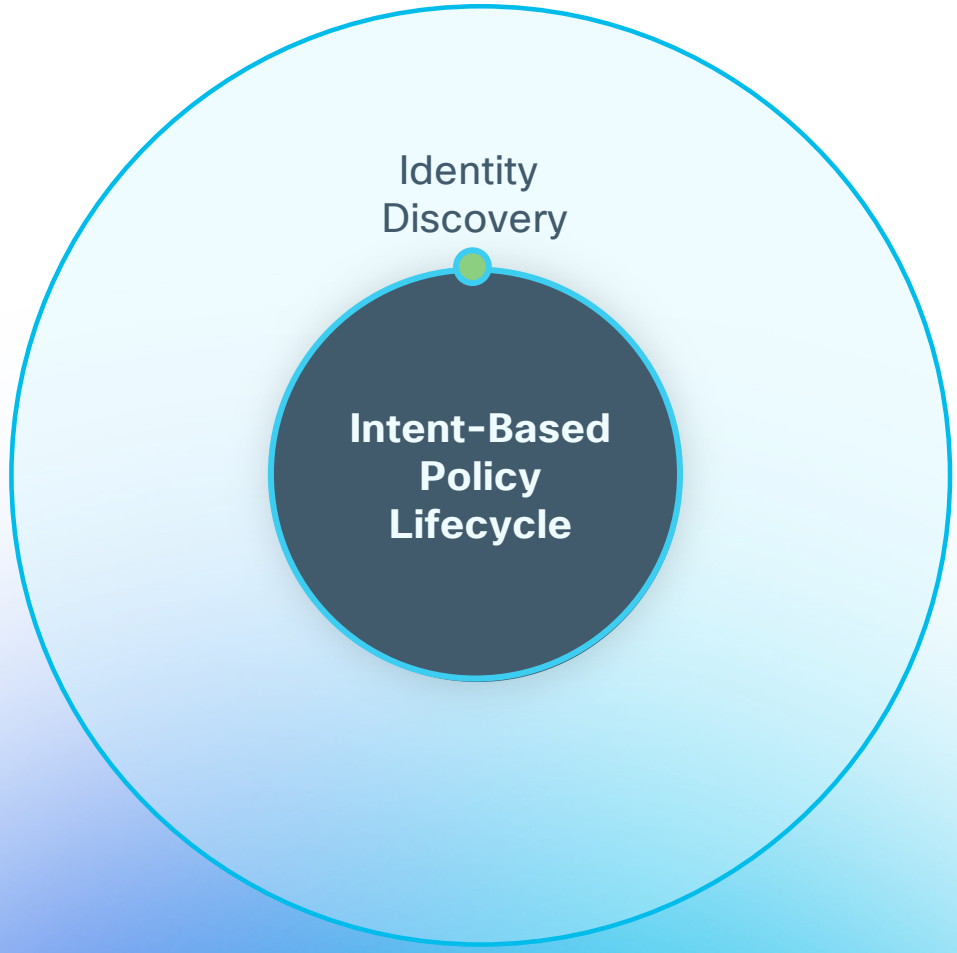
Distributed Enforcement

- Optimal connectivity based on user location
- Enterprise privacy for sensitive resources
- Resiliency in case of catastrophic Cloud Outage (Future)
- Central Management

Cisco Secure Firewall



Identity Discovery

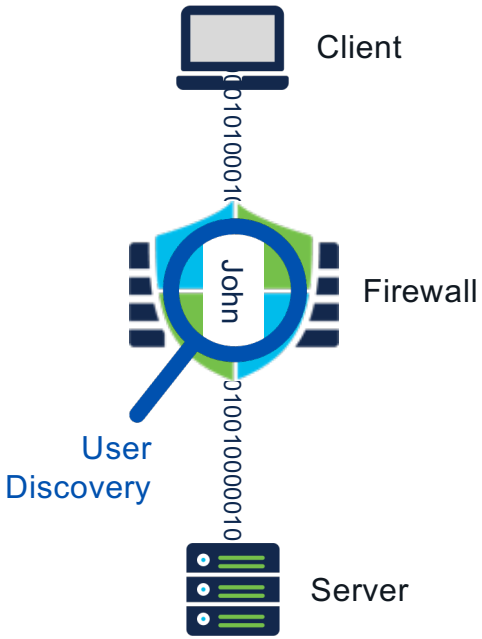


Network and Authentication-Based Discovery

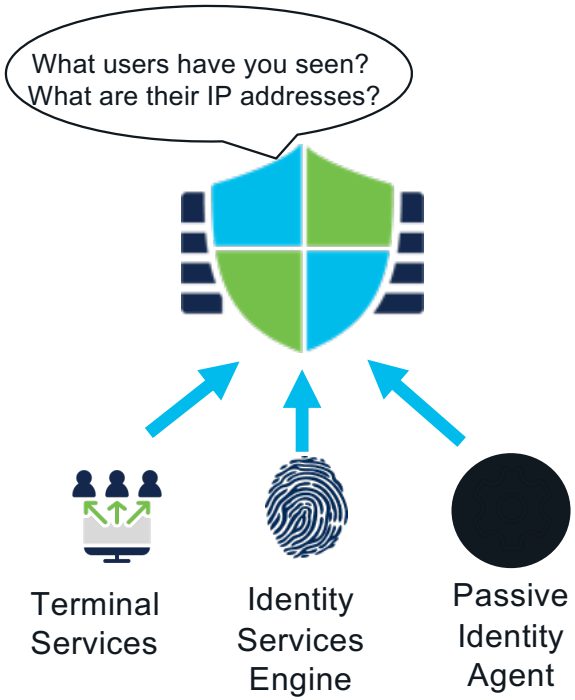
Identity Discovery

BRKSEC-2590

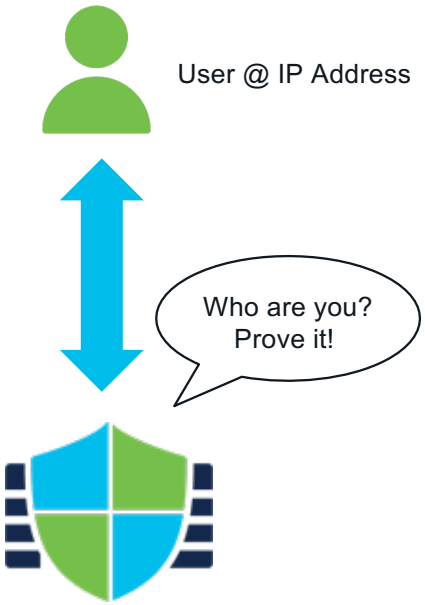
Network Discovery



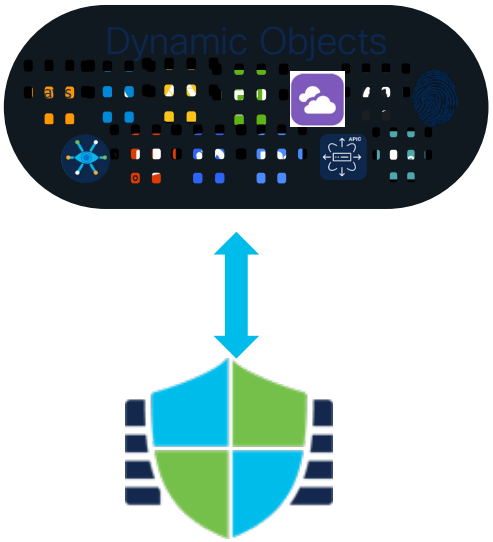
Passive Discovery



Active Discovery



External Integrations



Reference

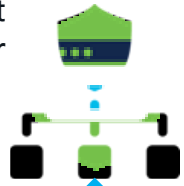
Passive Discovery from Events

User:	SGT:	IP:	Source:
-	10	172.16.0.4	TrustSec SXP
Lisa	30	172.16.0.22	AD Events Log, Syslog, REST API
Marge	15	172.19.1.13	RADIUS

Identity Services Engine

pxGrid

Management Center



What users have you seen?
What are their IP addresses?

User and Group check

Guest List	
Theodore Fairfax	VIP
Evelyn Harrington	VIP
Percival Whitmore	Ambassador
Serafina Beaumont	Host

Realms (Directories)

REST

API

REST

User:	IP:	Port Range
Burns	192.168.1.1	2024-2223

Terminal Services

Microsoft
Remote Desktop Services

citrix

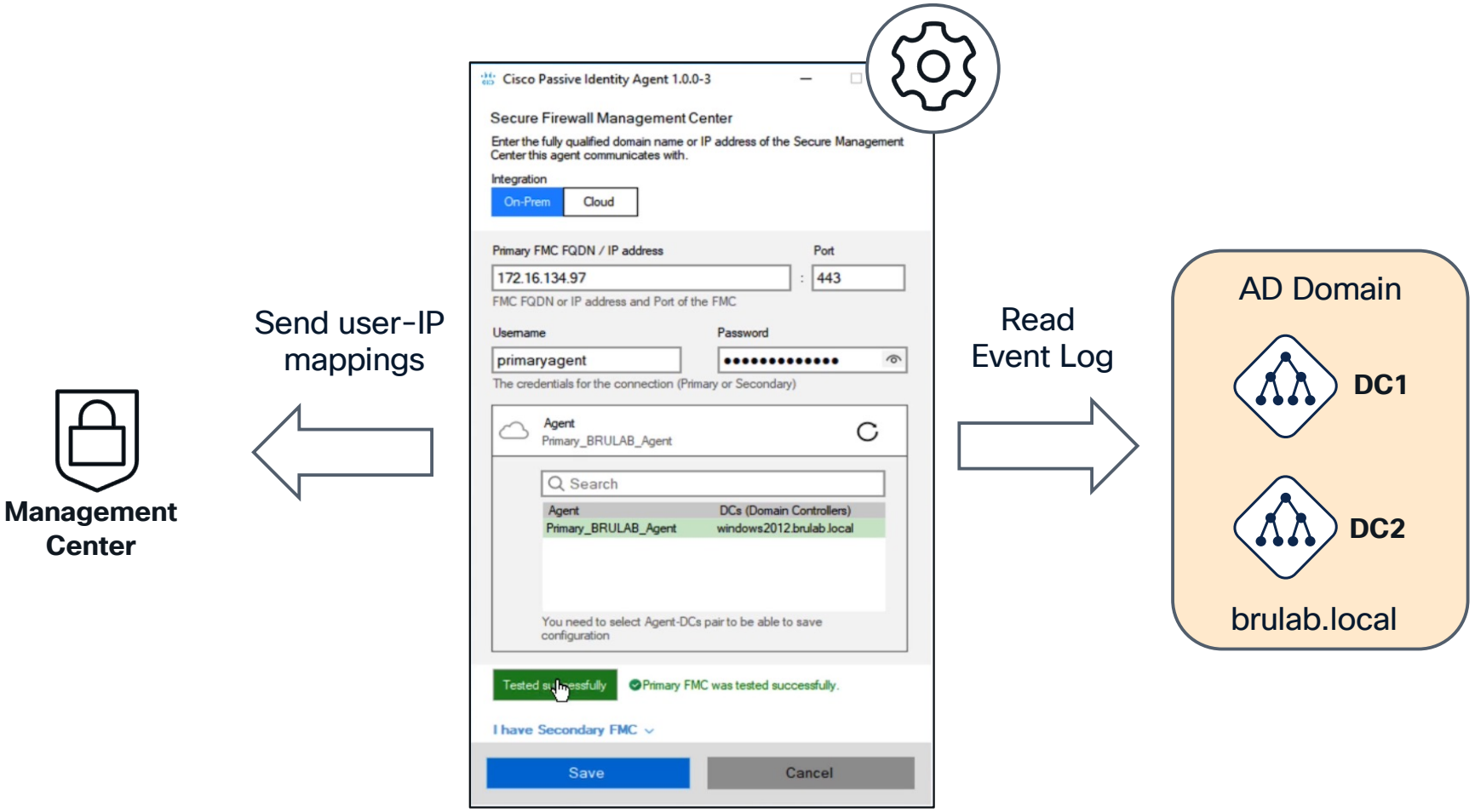
User:	IP:
Smithers	10.1.1.4

Passive Identity Agent

AD DC

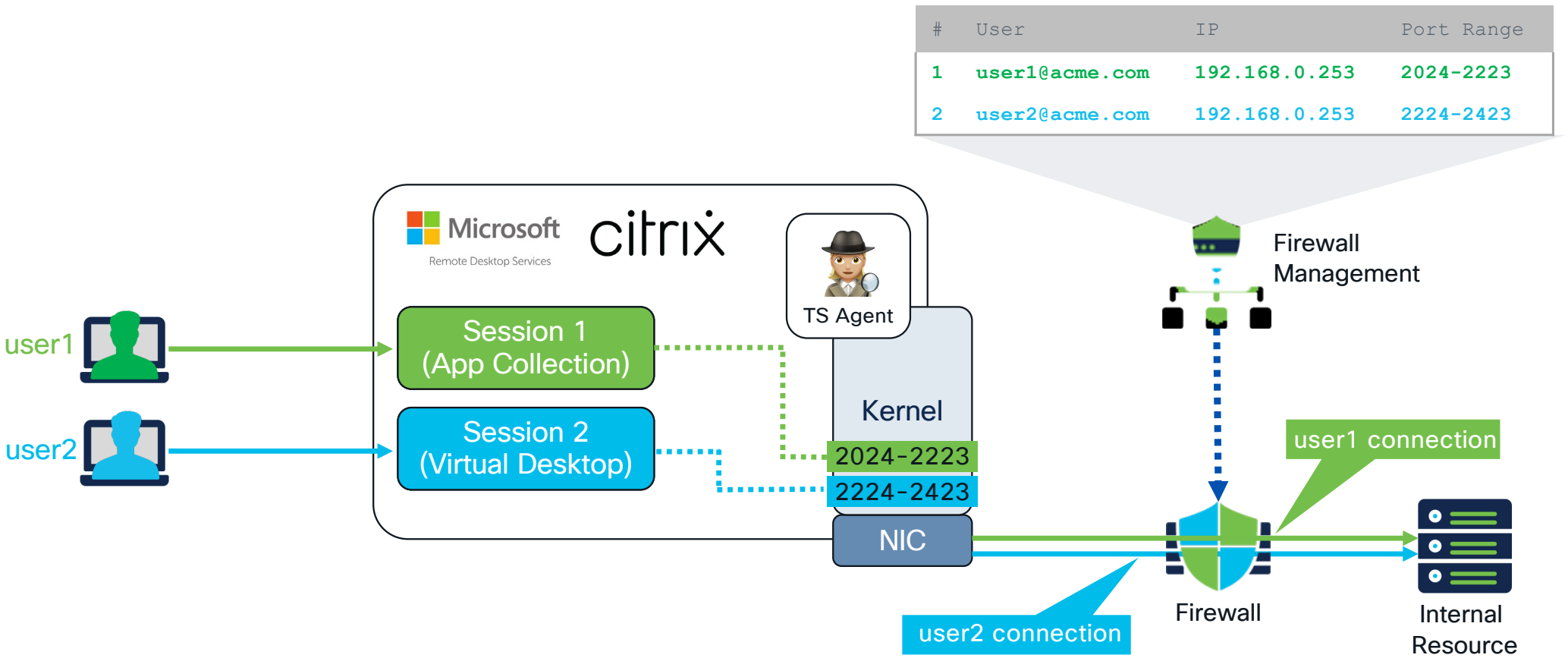
Reference

Passive Identity Agent



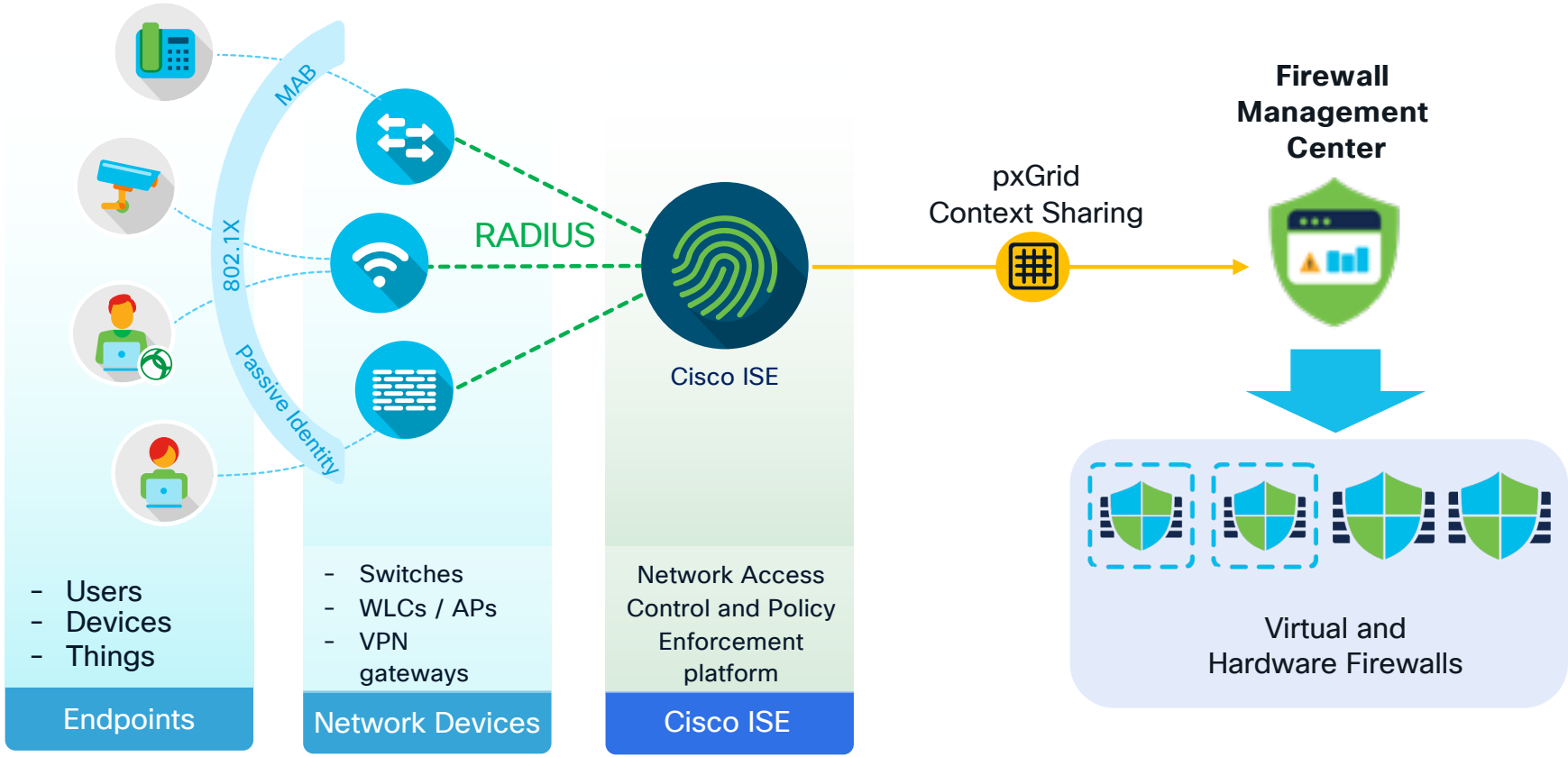
Identity Discovery

Terminal Services User Discovery



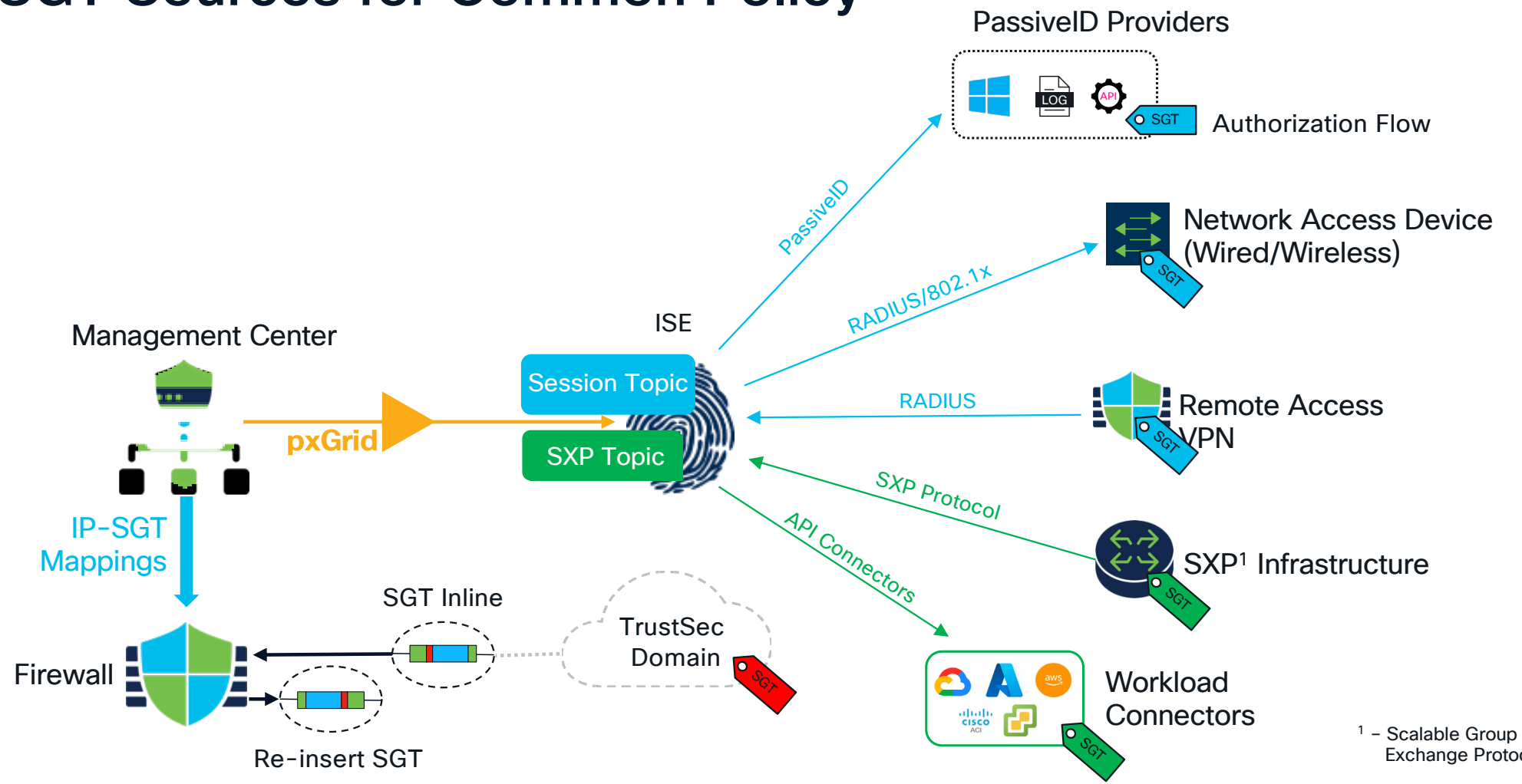
Reference

Identity Services Engine Integration



Identity Discovery

SGT Sources for Common Policy

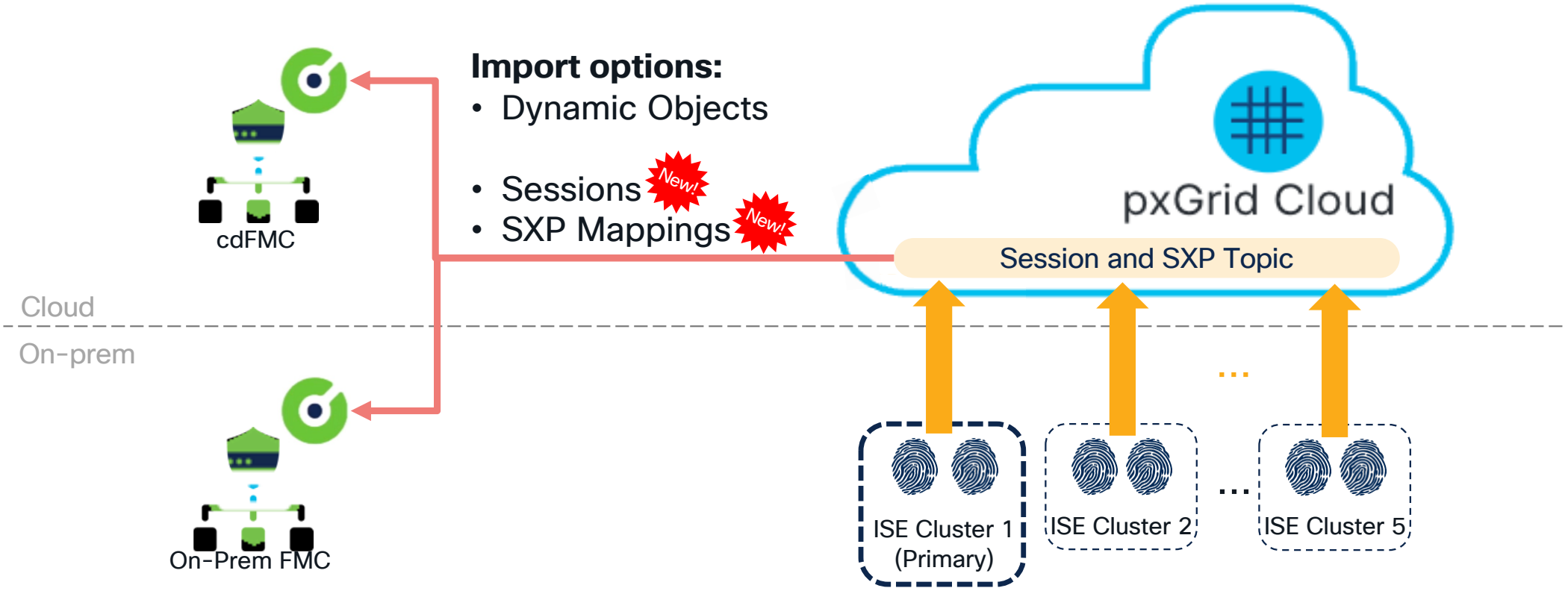


[1] – Scalable Group Tag (SGT) Exchange Protocol

cisco

Reference

Multiple ISE clusters and Session/SXP support



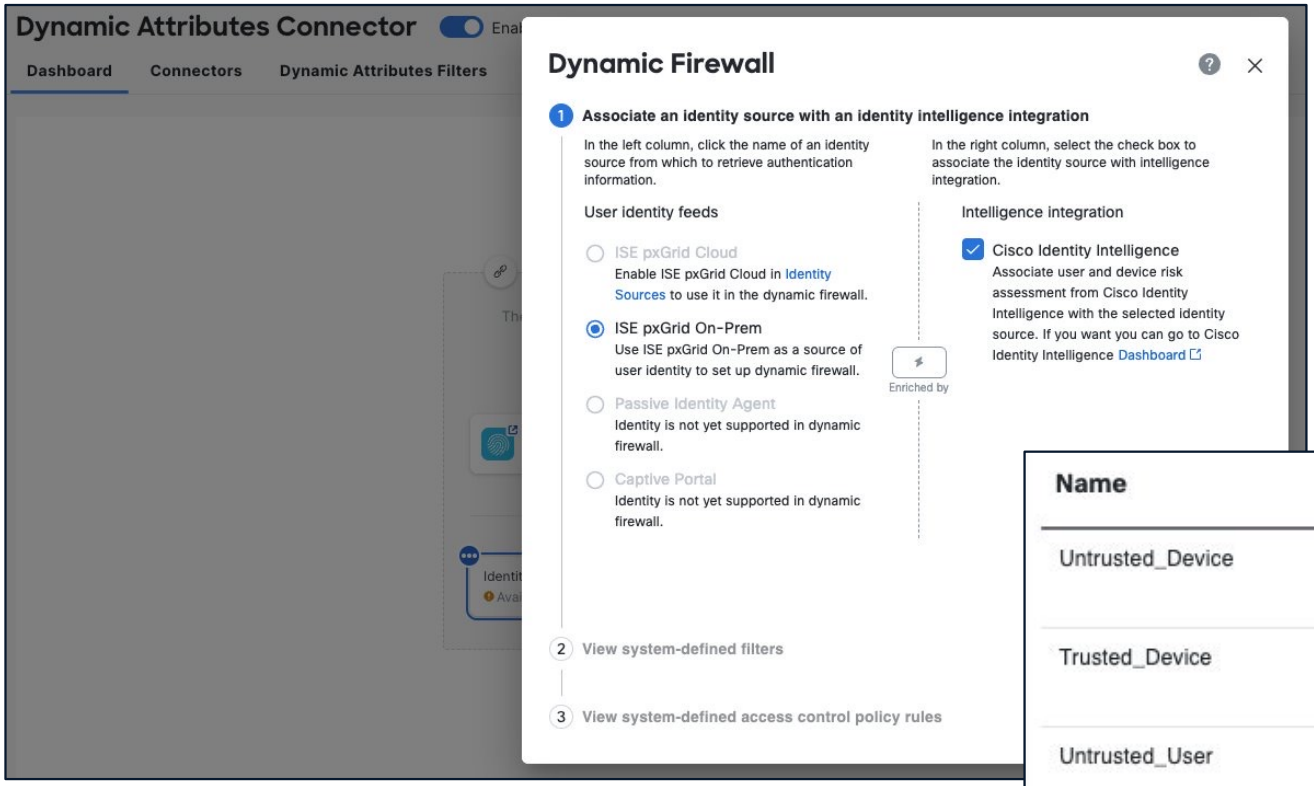
5 x ISE Cluster support New!

Reference

Cisco Identity Intelligence Integration

New!

FTD 10.0



Firewall policy learns IP addresses of:

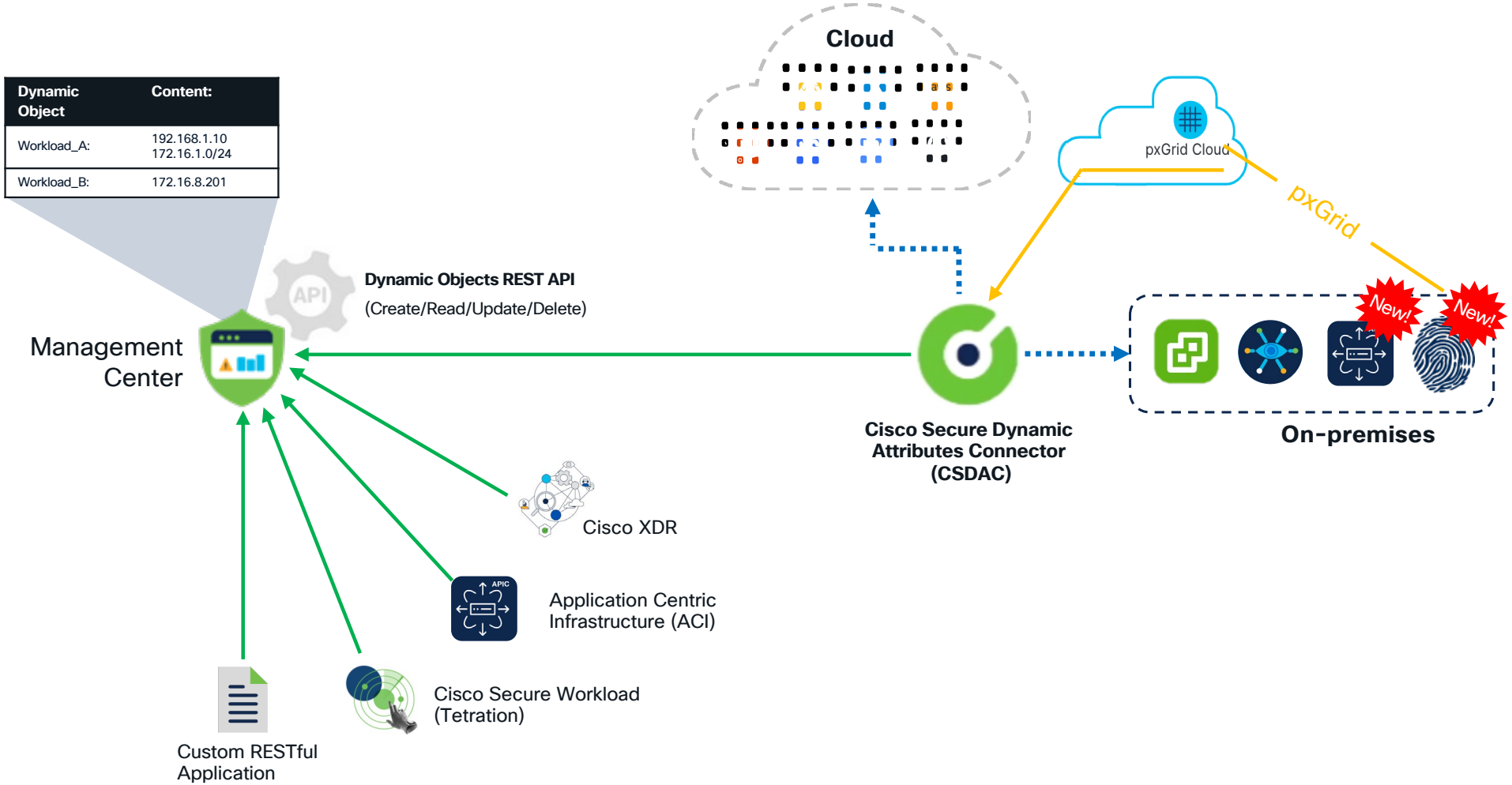
- **ISE** postured/non-compliant devices
- **CII** Untrusted and Questionable

Name	Query
Untrusted_Device	(**PostureStatus** eq 'NonCompliant') **OR** ((**MdmRegistered** eq 'true') **AND** (**MdmCo**...
Trusted_Device	(**PostureStatus** eq 'Compliant') **OR** ((**MdmRegistered** eq 'true') **AND** (**MdmCo**...
Untrusted_User	**TrustScore** eq 'UNTRUSTED'
Questionable_User	**TrustScore** eq 'QUESTIONABLE'

cisco

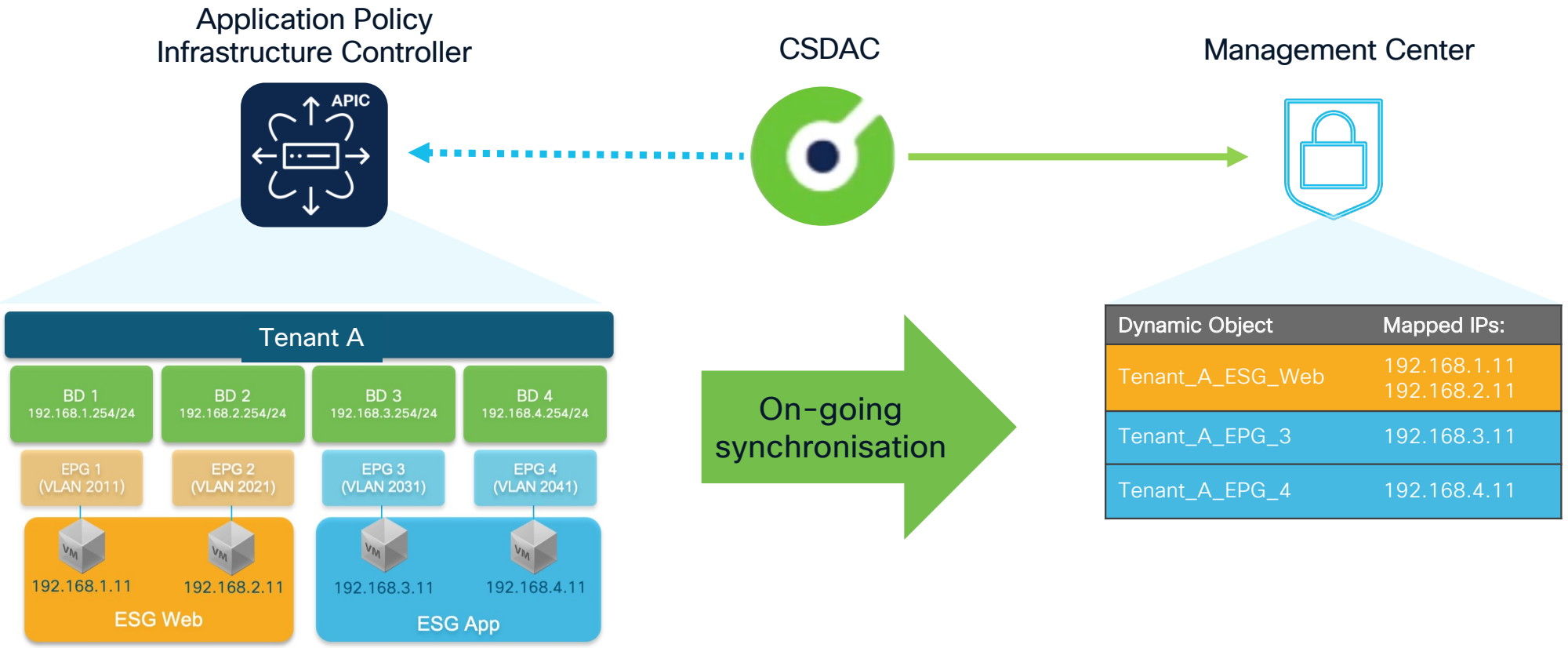
Identity Discovery

Dynamic Objects: adapting to a dynamic world



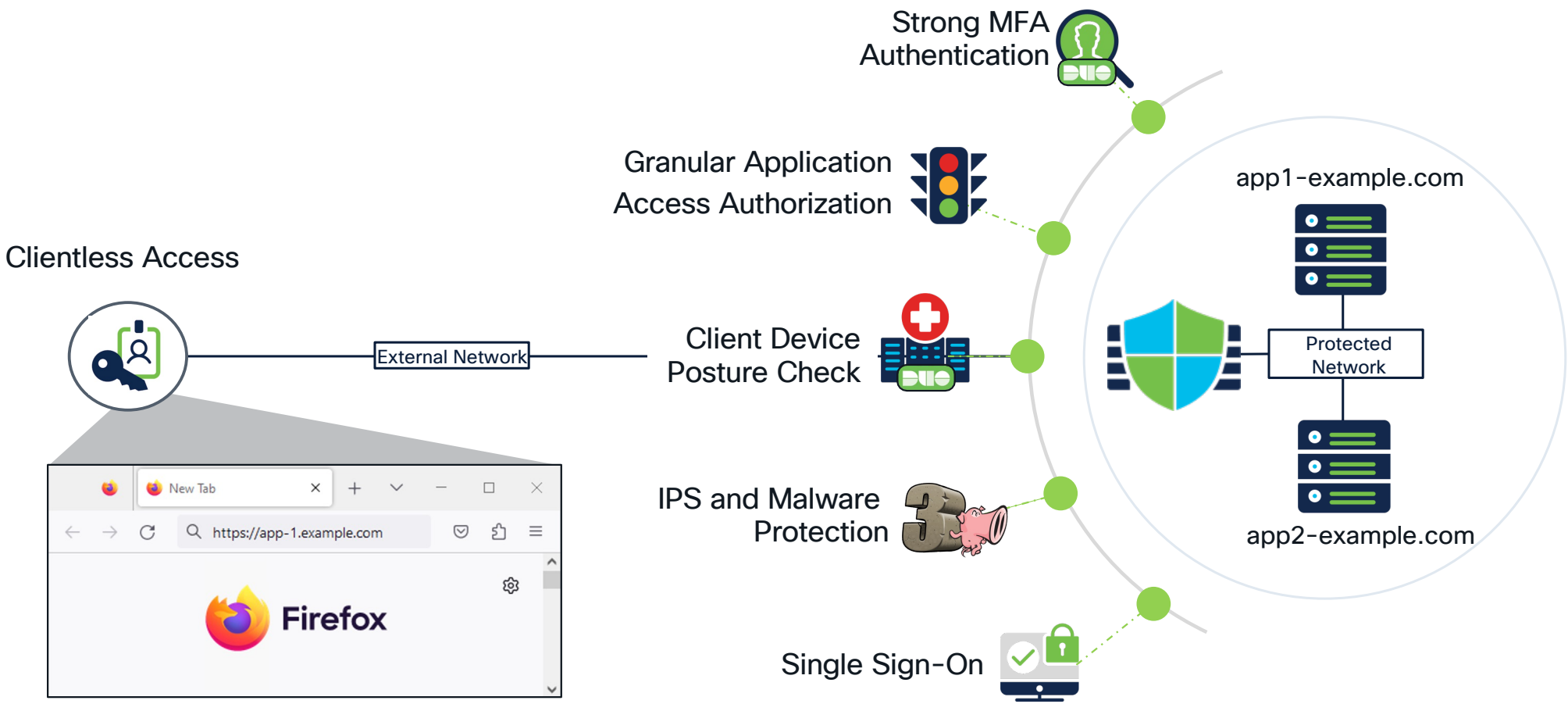
Reference

ACI Integration



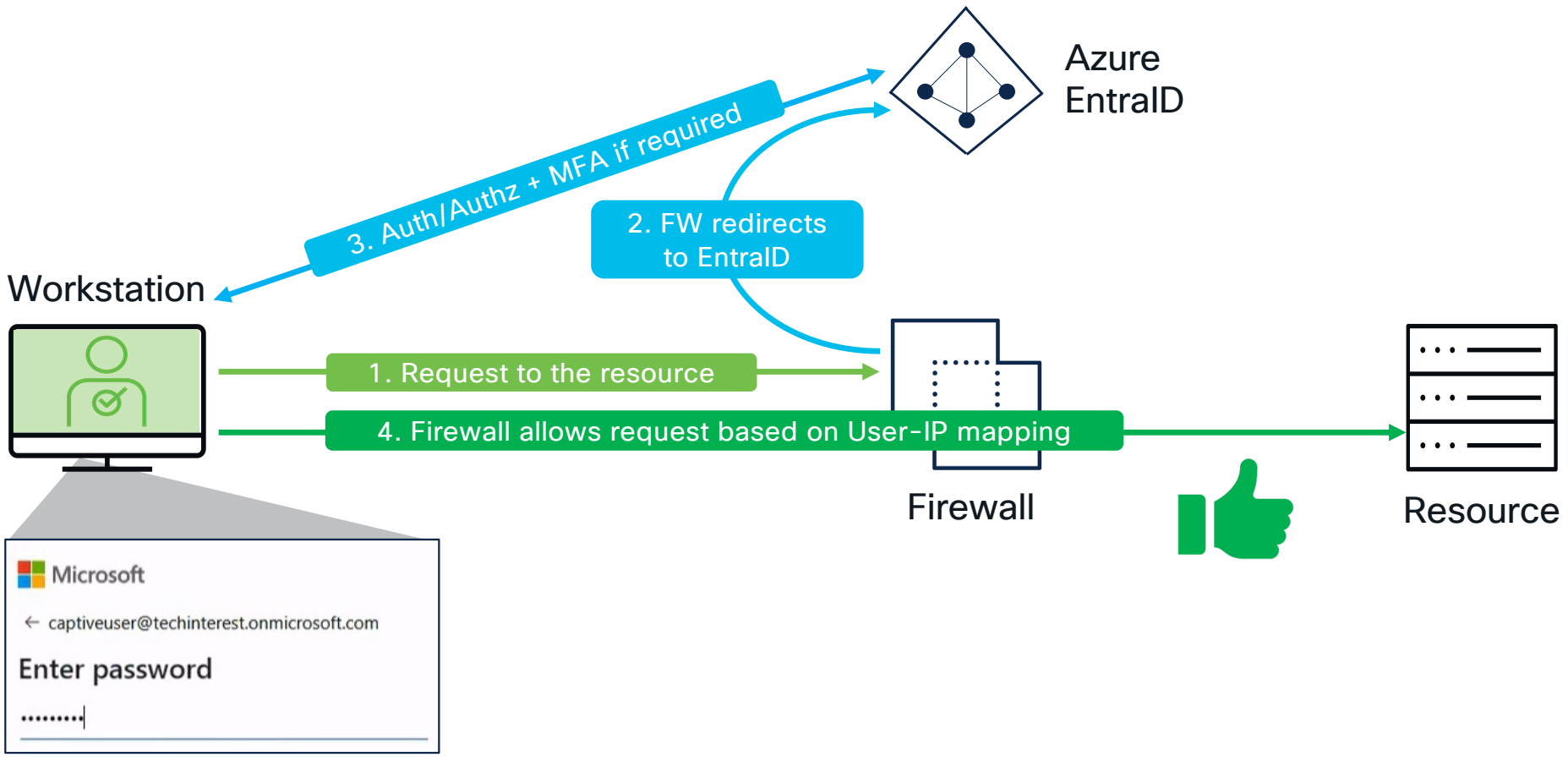
Zero Trust Network Access – User Discovery

Identity Discovery



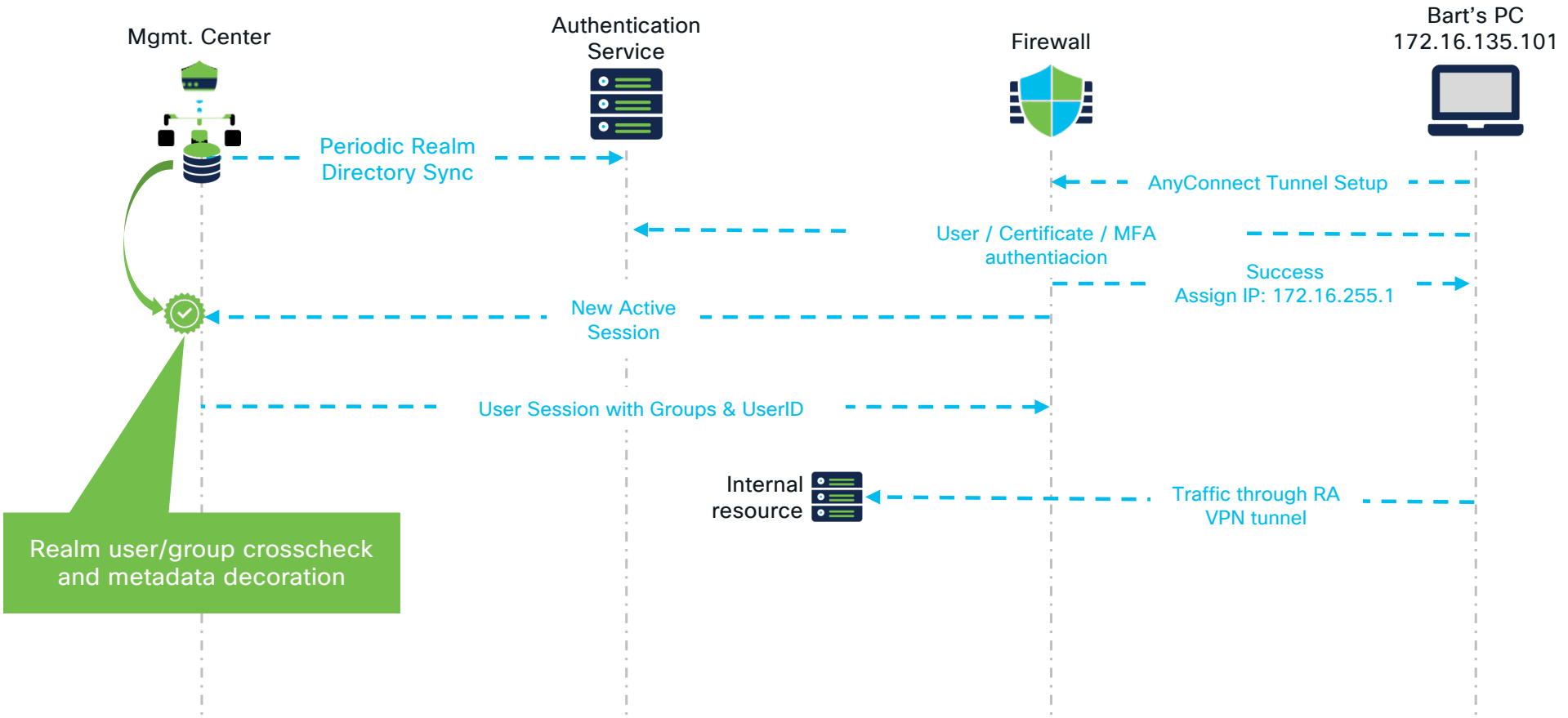
Reference

Captive Portal with EntraID

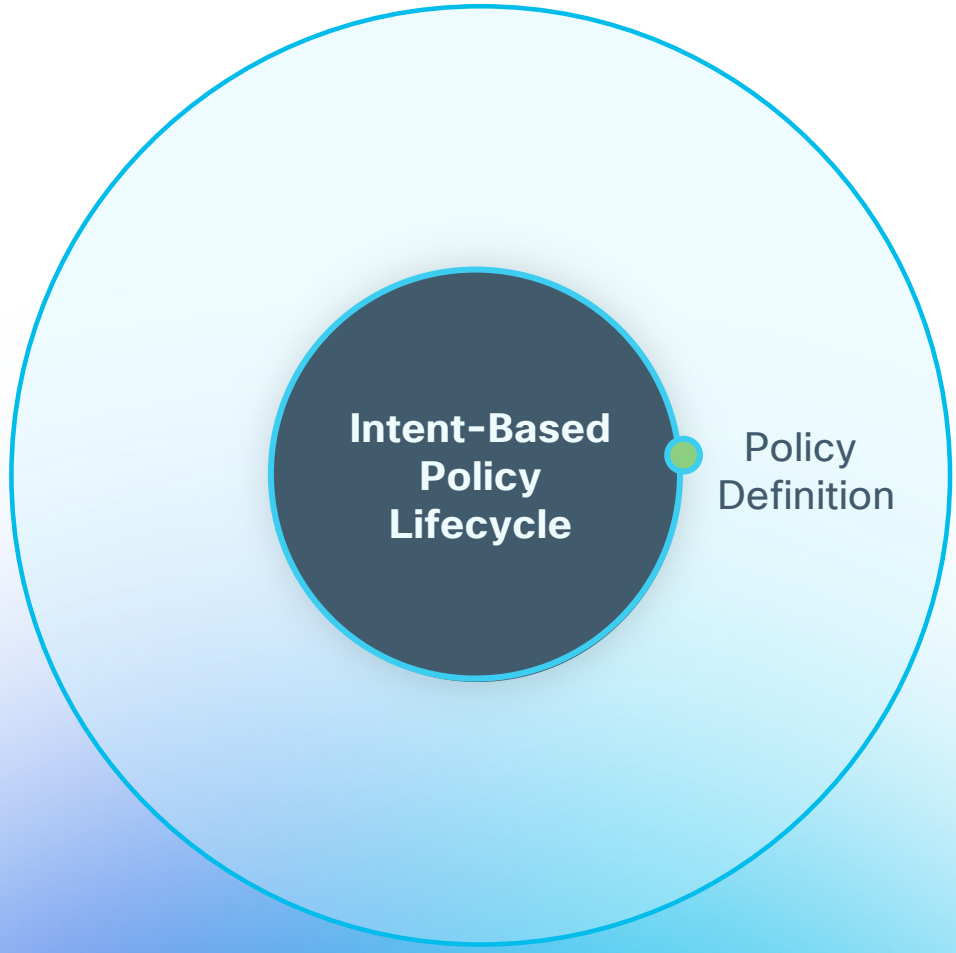


Reference

Remote Access VPN User Discovery (Active Discovery)



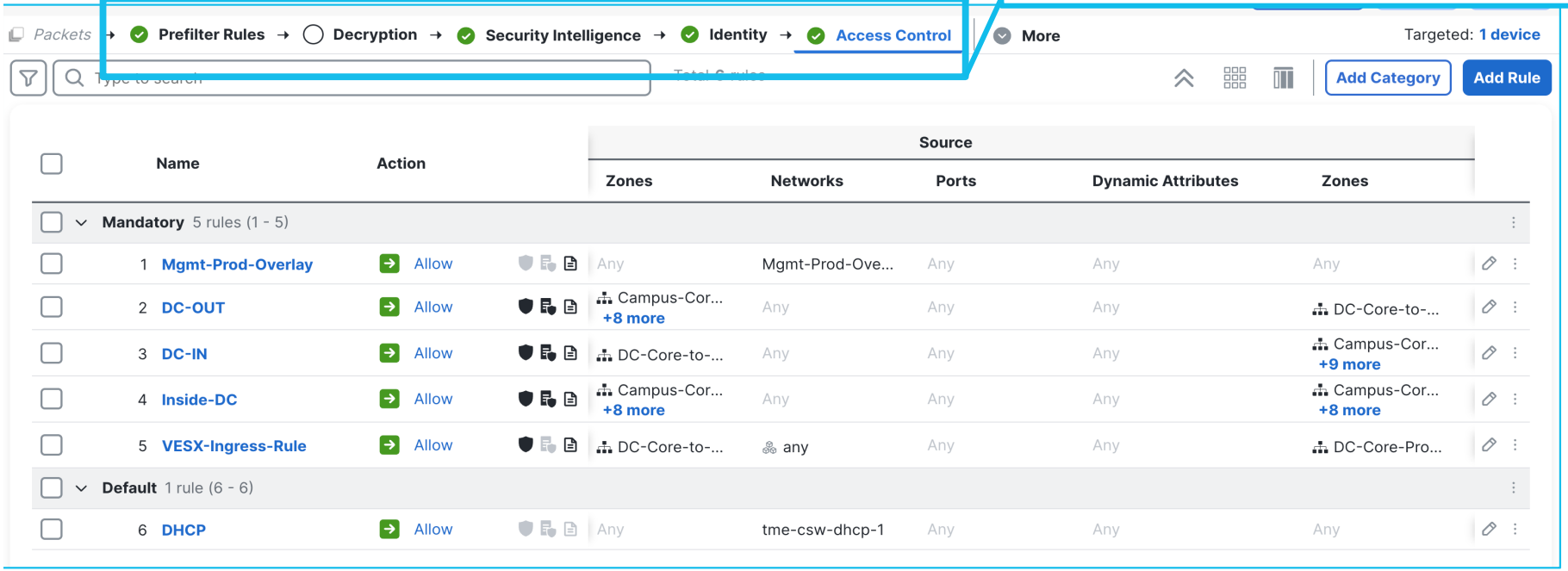
Policy Definition



Reference

Access Control Policy (ACP)

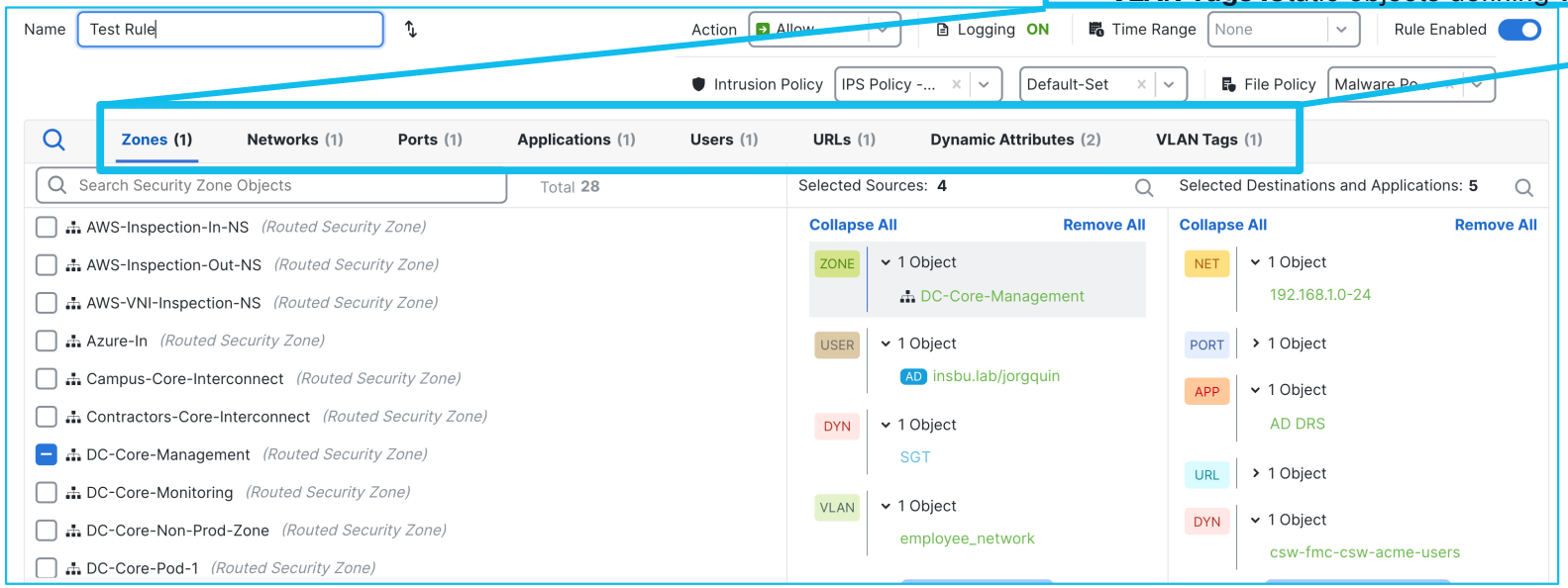
- **Access Control Associated Policies**
  - **Prefilter**: Fast forward or Fast Drop packtes without engaging inspection engine. Selects tunneled traffic for L7 inspection.
  - **Security Intelligence:** IP/DNS/URL threat intelligence feed
  - **Decryption:** Decrypts selected traffic for further inspection
  - **Identity:** Identity awareness from multiple identity sources for identity control



Reference

Access Control Policy (ACP)

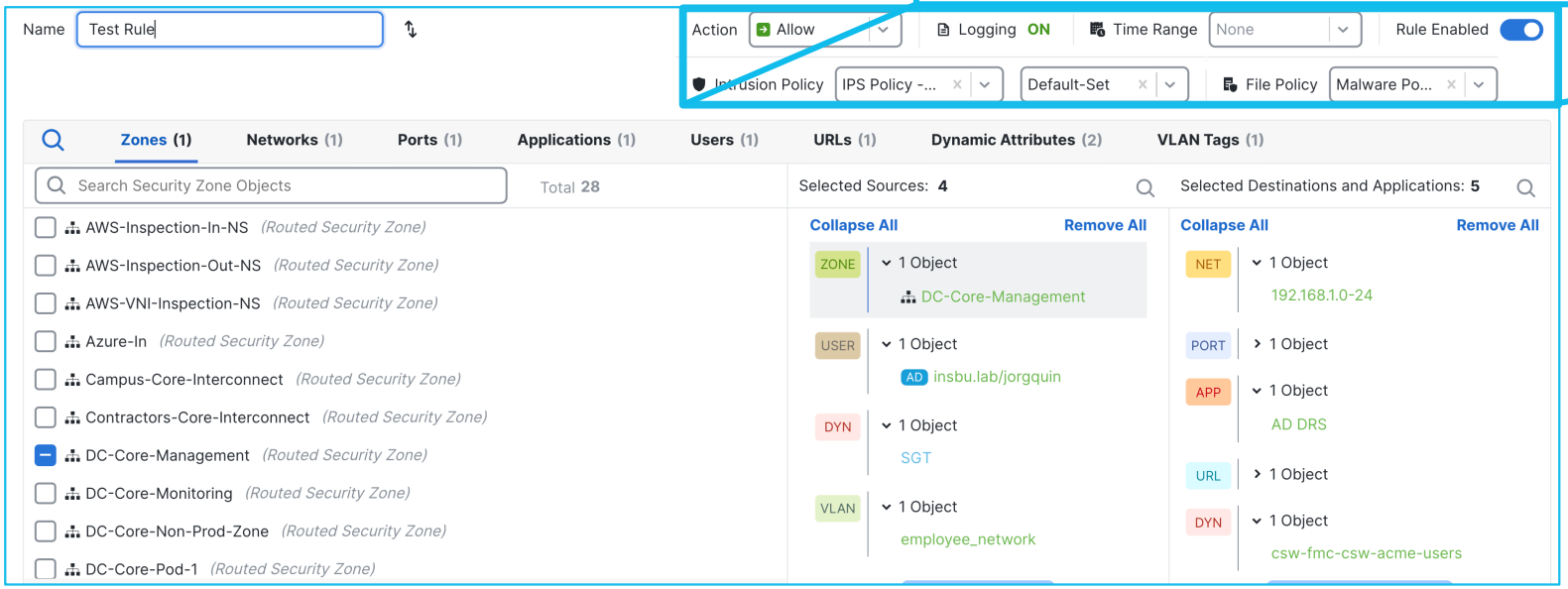
- **Policy Objects**
  - **Zones:** Object that groups interfaces
  - **Networks:** Static objects defining network/IPs
  - **Ports:** Static object defining ports
  - **Application:** AppIDs detectors objects
  - **Users:** Authoritative list of user group identity objects
  - **URL:** URL categories objects mapped to reputations
  - **Dynamic Attributes:** Dynamic objects and SGTs pulled from external systems
  - **VLAN Tags :**Static objects defining vlan tags



Reference

Access Control Policy (ACP)

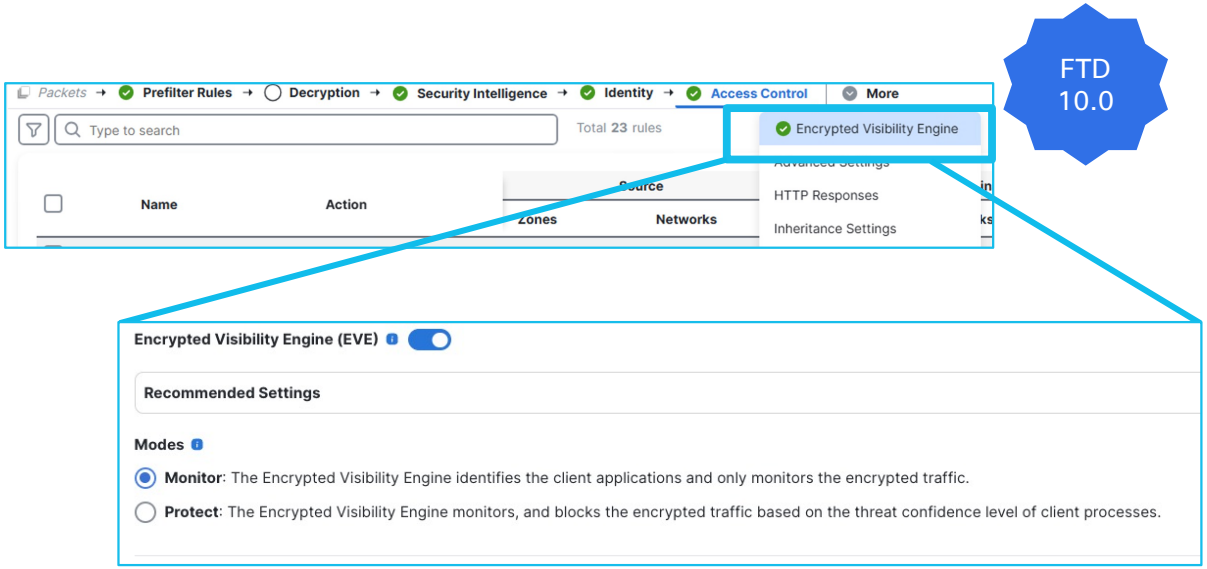
- **Additional Rule Configurations**
  - **Action:** Network control applied to traffic.
  - **Logging:** Log connection event for a network traffic rule.
  - **Time Range:** Duration or time frame for rule to be active.
  - **Rule Enabled:** Enable or disable rule.
  - **Intrusion Policy:** IPS policy inspection applied to the rule. This is an associated sub-policy.
  - **Variable Set:** Applies directionality of traffic flows to IPS rules.
  - **File Policy:** Malware detection and prevention inspection. This is an associated sub-policy.



Reference

Encrypted Visibility Engine

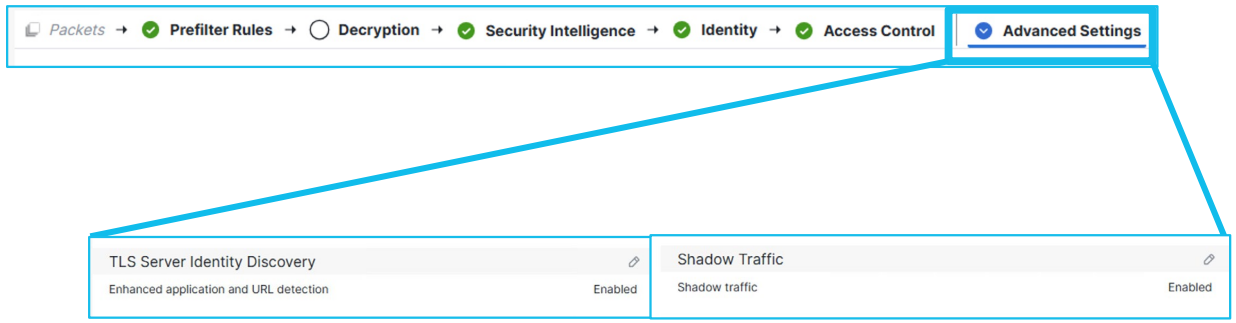
- Encrypted Visibility Engine
  - Available since 7.2
  - Detects and blocks malware in encrypted flows
  - Provides application and OS detection from a single TLS/QUIC packet – no decryption required
  - Minimal performance impact
  - Reduces performance utilization on decryption functions
  - Intelligent Decryption bypass with Client Threat Score + URL Reputations
  - NEW 10.0: Located under MORE options for quick configuration



Reference

Advanced Settings

- TLS Server Identity Discovery
  - Detect and decrypt TLS 1.3 without the need to engage full TLS 1.3.



- Shadow Traffic: Firewall detects and flags connections showing the signs of evasion in a new column
  - Evasive VPNs
  - Encrypted DNS
  - Domain Fronting
  - Multi-hop Proxies
  - Fake TLS

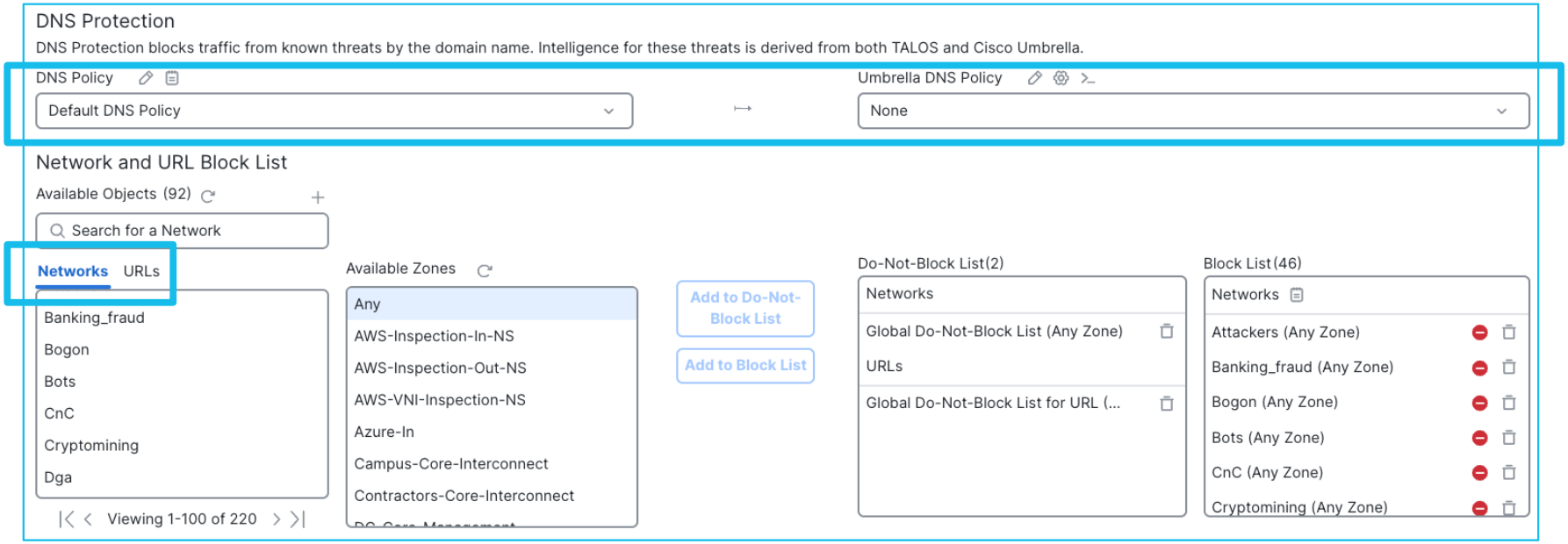
FTD 10.0

Event Type	Action	Client Application	Web Application	Destination IP	Destination Port / ICMP Code	Shadow Traffic Type	TLS Client SNI
Connection	Allow	SSL client	XVPN	35.205.176.240	**443** (https) / tcp	Evasive VPN	8v9m.com
Connection	Allow	X-VPN	Web Browsing	130.211.50.202	**20005** / tcp	Evasive VPN	
Connection	Allow	X-VPN	Web Browsing	35.205.250.171	**20005** / tcp	Evasive VPN	
Connection	Allow	Firefox	DNS over HTTPS	172.64.41.4	**443** (https) / tcp	Encrypted DNS	mozilla.cloudflare-dns.com
Connection	Allow	Firefox	DNS over HTTPS	172.64.41.4	**443** (https) / tcp	Encrypted DNS	mozilla.cloudflare-dns.com
Connection	Allow	Tor		185.220.101.192	**443** (https) / tcp	Evasive VPN, Multihop Proxy	www.4vg22c3cybm7v6bqyf...
Connection	Allow	Tor		64.65.0.11	**443** (https) / tcp	Evasive VPN, Multihop Proxy	www.sr33qfglszbztrvgyt3b...

Reference

Policy Definition – Security Intelligence

- Early defence policy mechanism with DNS policy and Threat-Intelligence Reputation
- Threat Intelligence from Talos updating in near real-time intelligence for well-known malicious actors
  - IP list
  - DNS list
  - URL list

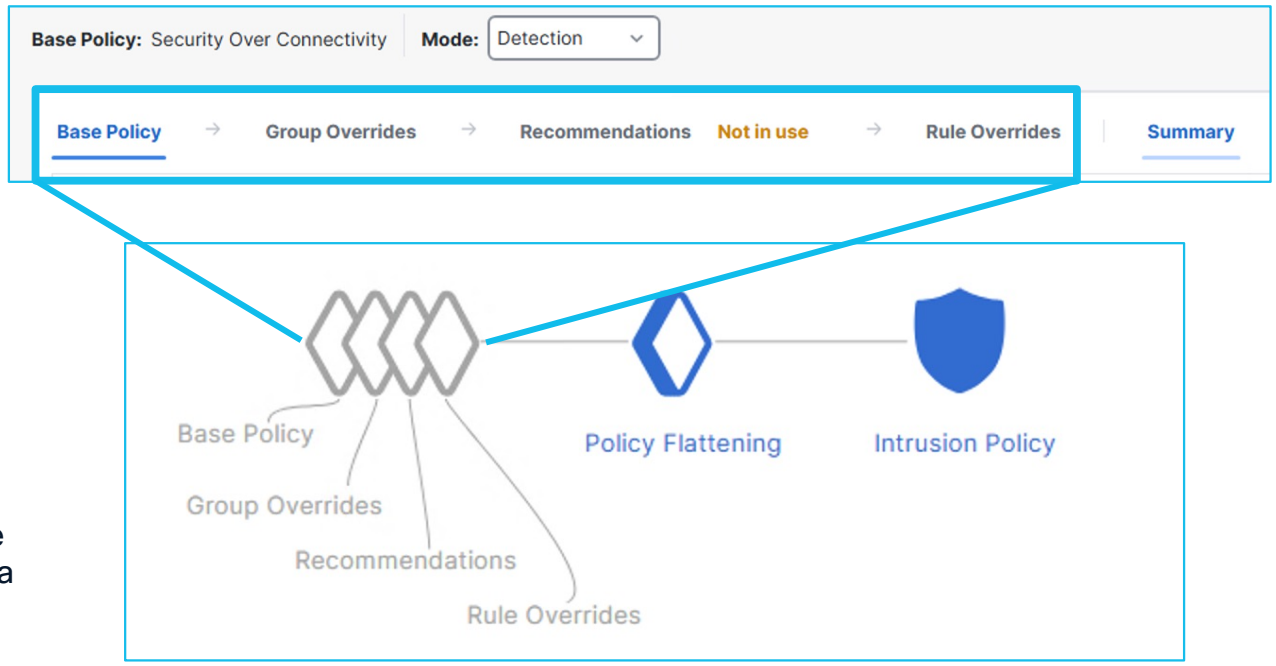


Reference

Policy Definition – IPS Associated Policy

BRKSEC-2861

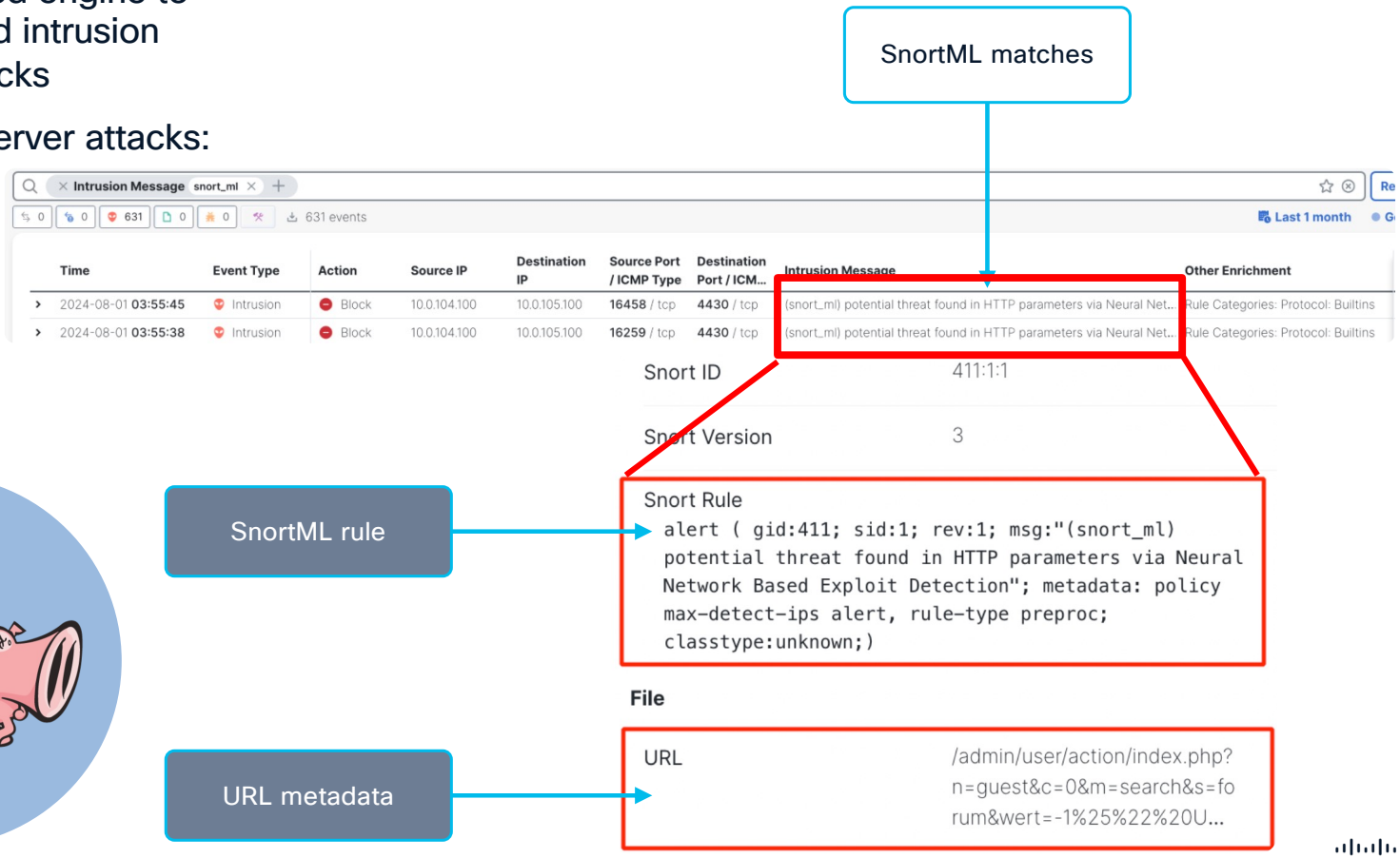
- IPS Policies consists of:
- A **base policy** (e.g Connectivity over Security, Balanced Security and Connectivity, Security Over Connectivity, Maximum Detection)
  - The higher the security level, more snort rules enabled by default
  - Base Layer on the policy
- **Group Overrides**: Group categories for rules
- **Cisco Recommendations**: Recommends rules based on discovered vulnerabilities on the network. Third layer on policy
- **Rule Overrides**: Are the top layer if specific rules are modified.
- Final step, policies get flattened
  - If there are conflicting rule verdicts, system will take most security-conscientious action, unless there is a manual rule override



Reference

SnortML - Neural Network-Based Exploit Detector

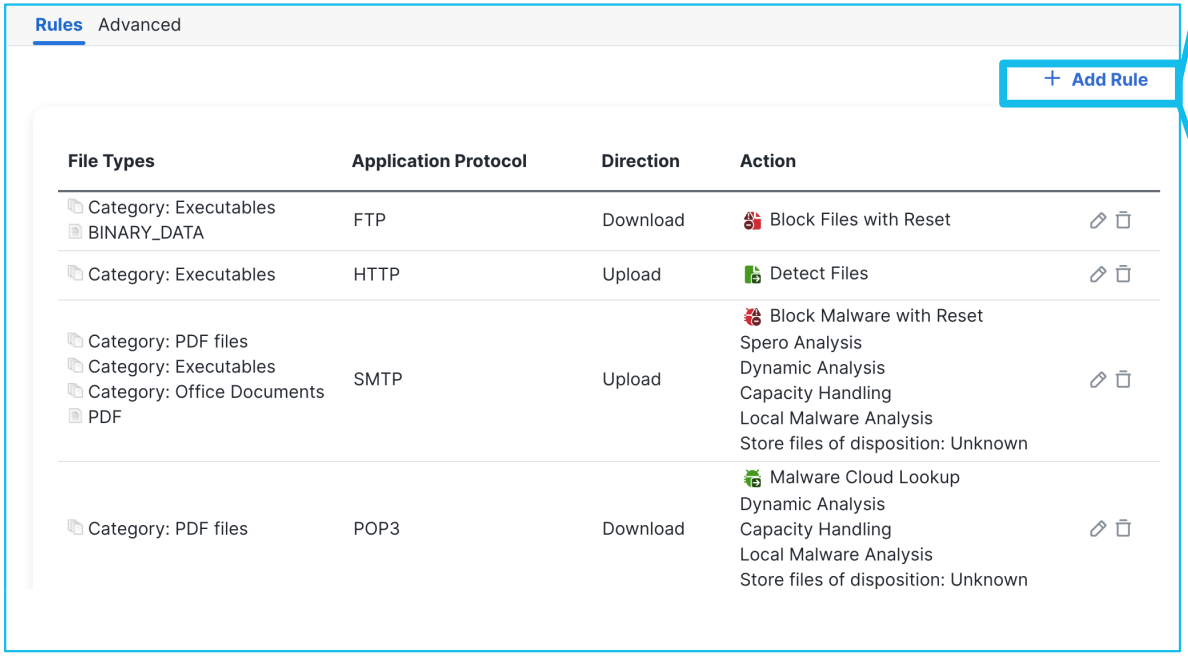
- **SnortML**: Machine Learning-based engine to augment traditional pattern-based intrusion protections against zero-day attacks
- SnortML protects against HTTP server attacks:
  - SQL Injection (7.6+)
  - HTTP command injection (10.0)

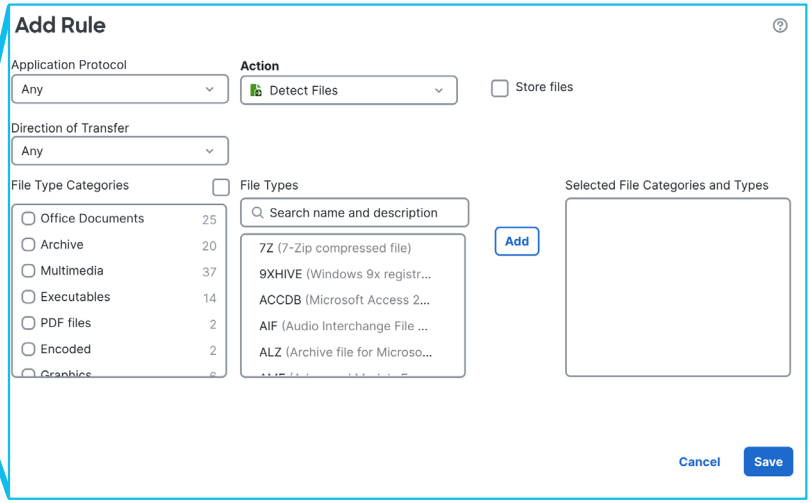


Reference

Policy Definition – File Associated Policy

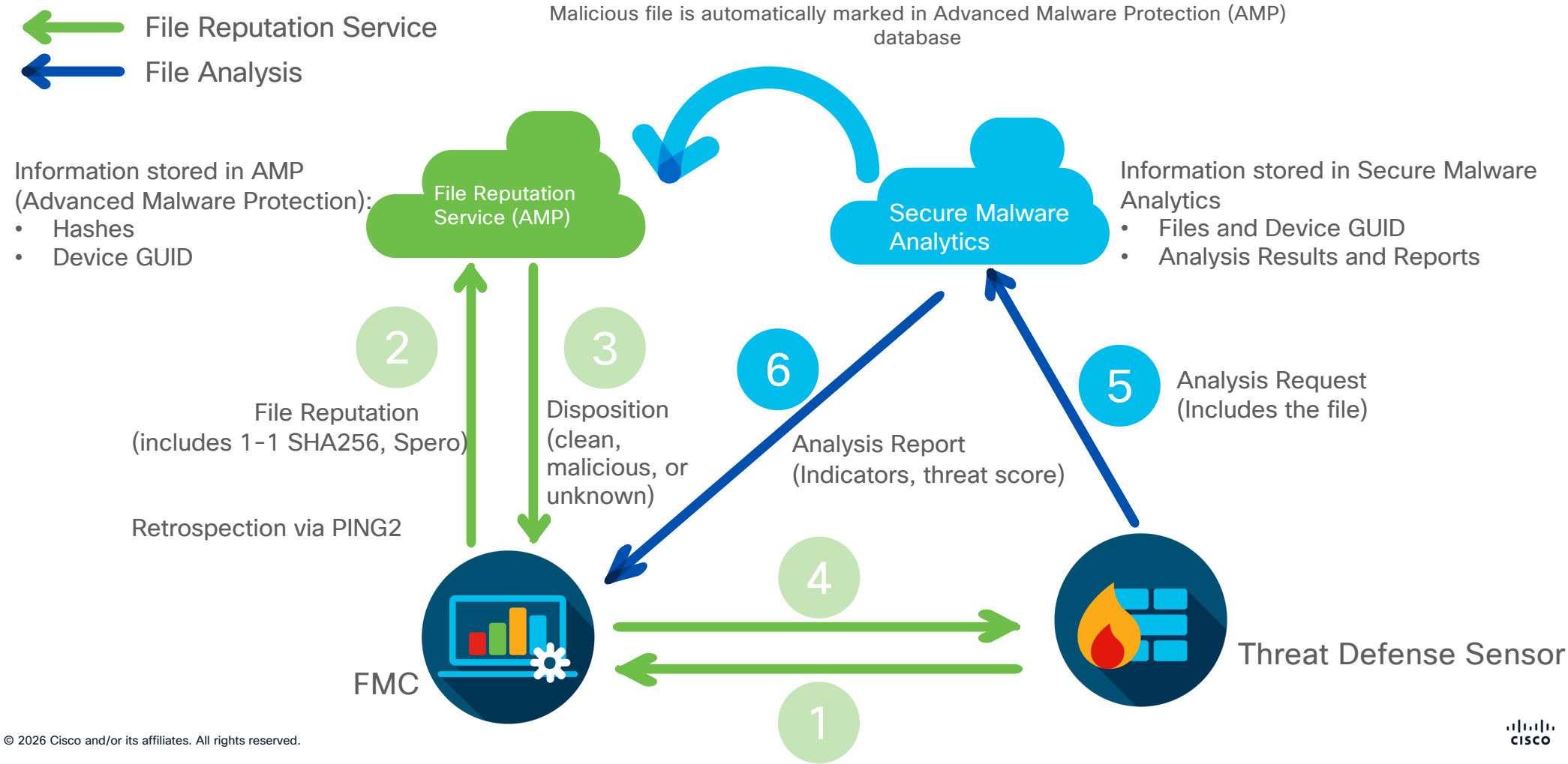
- File policy capabilities provide deep file inspection
  - Multi protocol file detection, tracking and storing
  - Dynamic analysis of files
  - Sandboxing for further disposition





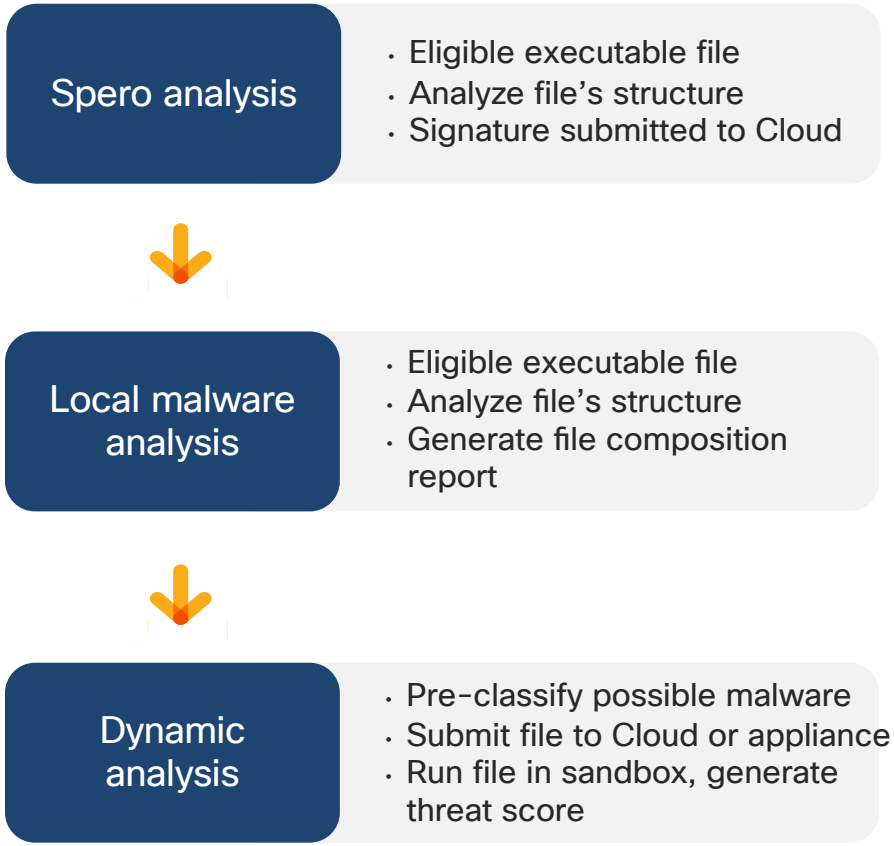
Reference

File Dispositions



Reference

Analysis Type

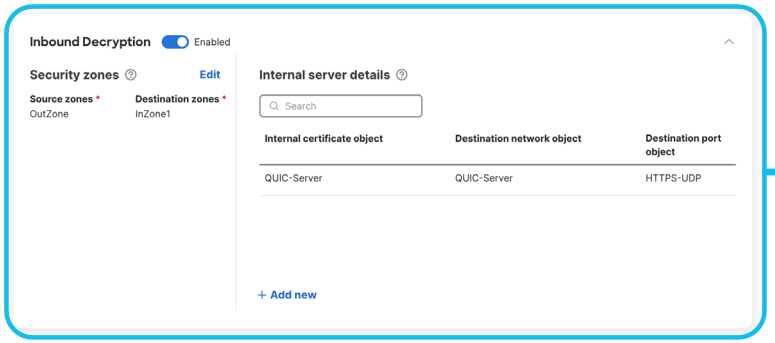


cisco

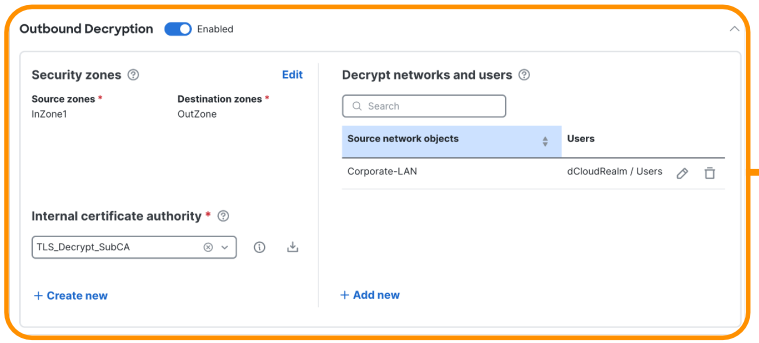
Reference

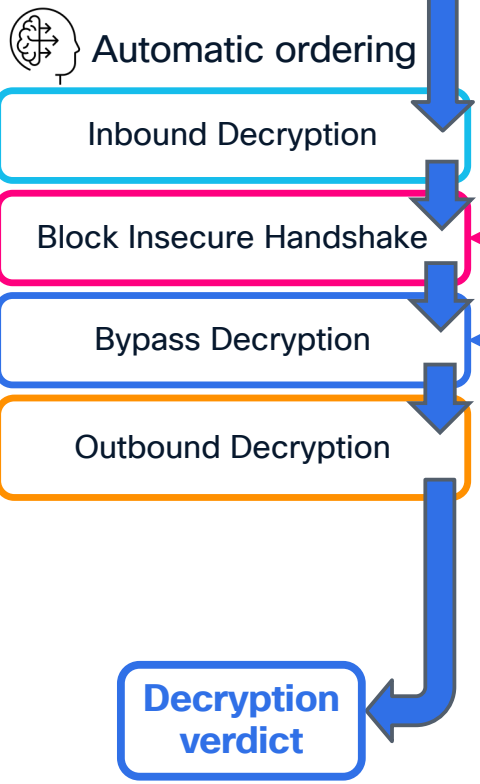
Policy Definition – Decryption Associated Policy

Step1: Specify your servers for decryption

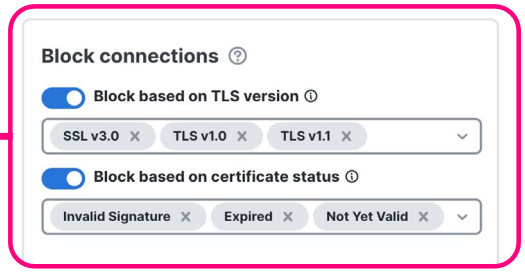


Step 2: Set protected networks and users

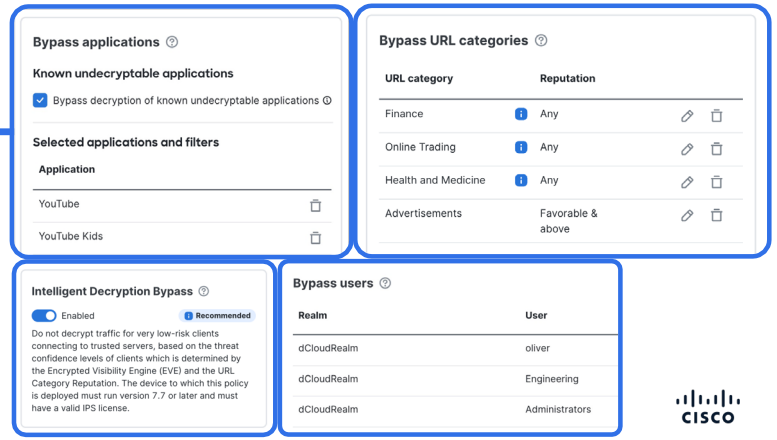




Step 4: Block weak ciphers and bad certificates



Step 3: Exempt Apps, URLs, Users etc...



Reference

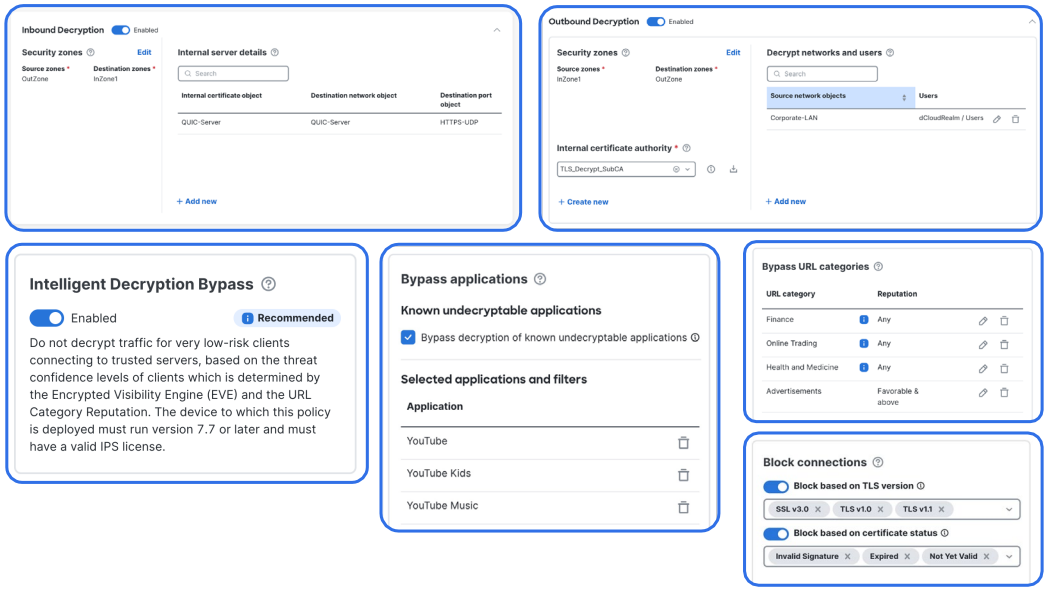
New Simplified Workflow

Convert Policy Mode

(one way road)

Standard Decryption Policy

- **Single-page** setup with a clear, **intuitive workflow**
- Organised, **tiled layout** for inbound, outbound, bypass, and block policies
- Rule order? Automatically managed – **focus on intent, not sequence**



Rule-based Decryption Policy

- Classic, granular rule-by-rule control
- Requires careful rule ordering to avoid decryption
- Recommended for complex and exceptional use-cases

Custom DND Exceptions for Inbound	(IP/Port based)
Known Key – Server Protection	(IP/Port based)
Custom DND Exceptions / Bypass for Outbound	(IP/Port based)
Custom DND Exceptions for Outbound (Specific: URLs, DNs, Applications)	
Do Not Decrypt (DND) Undecryptable, Pinned, Legaly Prohibited (URL Categories, Application Groups, DN Lists)	
Key Resign – Outbound Client Protection (URL Categories, Application Groups)	
Default Do Not Decrypt	

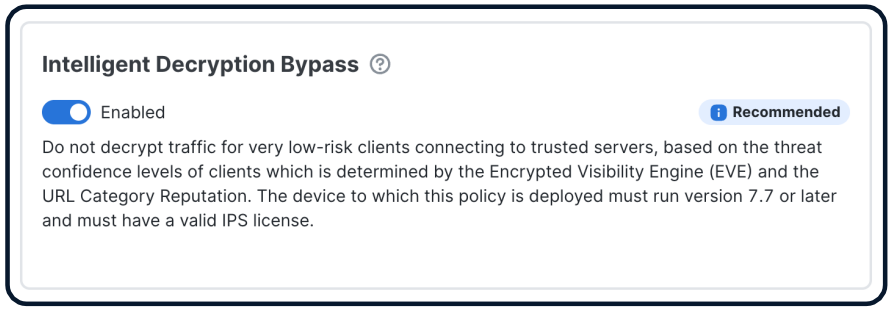
cisco

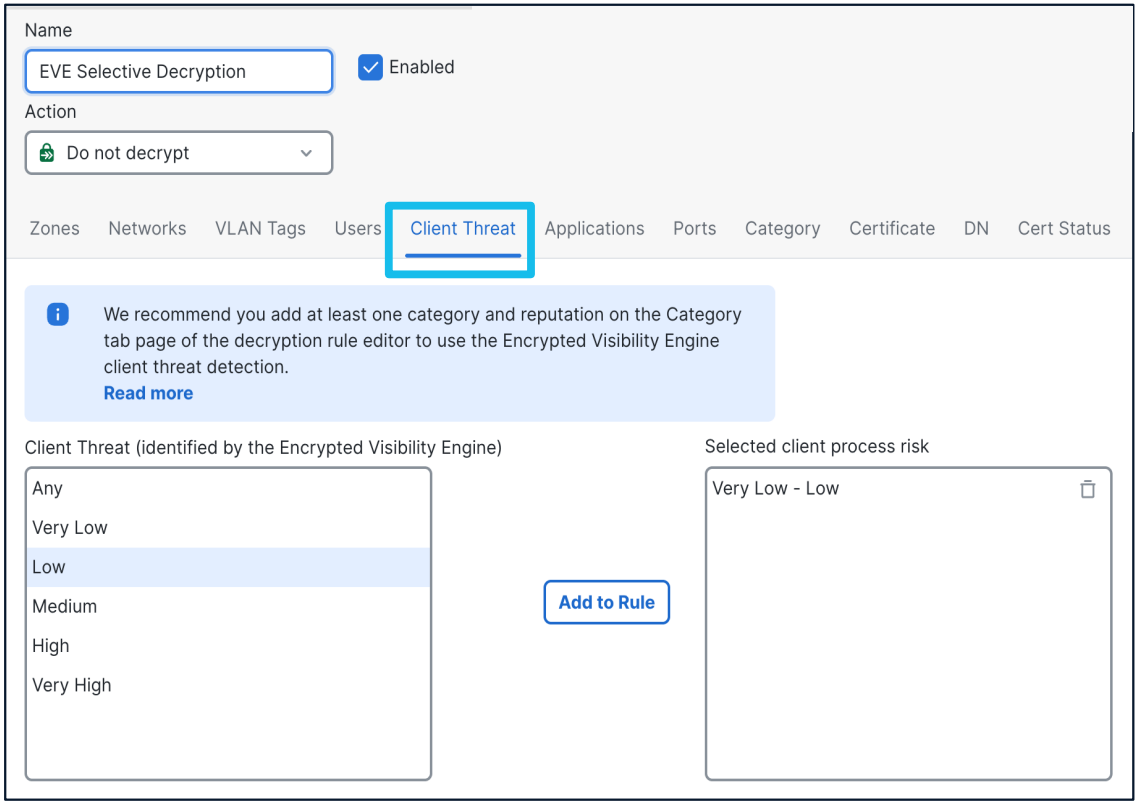
Reference

Intelligent/Selective Decryption – Client Threat Column

FTD 7.7

- Specify EVE derived client threat for TLS/QUIC decryption rules
- Strongly recommended to use in conjunction with URL risk/reputation categories

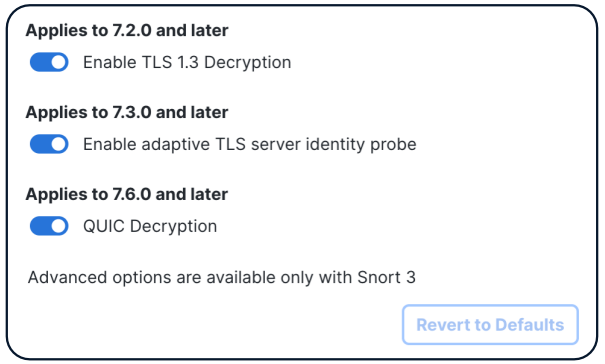


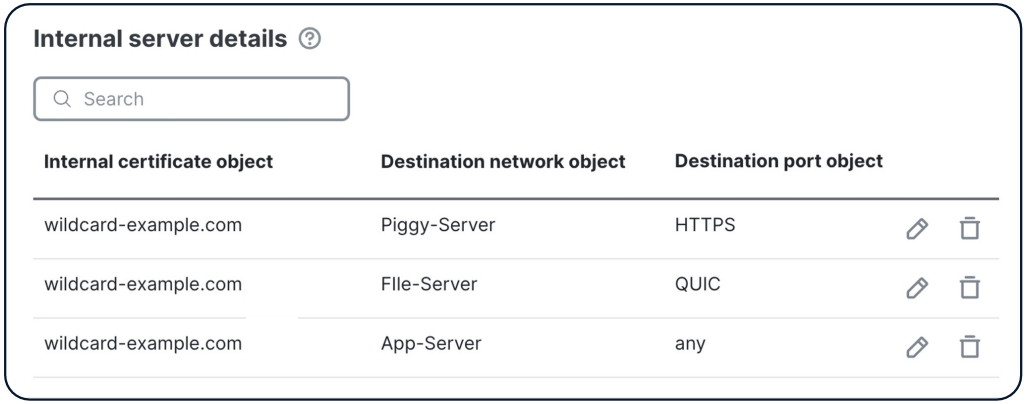


Reference

QUIC Decryption on Cisco Secure Firewall

- QUIC uses TLS 1.3 for negotiation – we follow the same decryption logic as with TLS
- QUIC is general availability – enabled by default when creating a new policy
- Seamless use in the decryption policy determined by selected port object:
  - UDP – matches QUIC connections only
  - TCP – matches TLS connections
  - Any – matches both QUIC and TLS connections
- Inbound decryption
  - Supported for all browsers
  - Tested webservers: NGINX, HA-Proxy, Caddy, OLS, H2O
  - Tested libraries: NGTCP/2, aioquic, quiche
- Outbound decryption supported on Firefox only
- Cluster and high availability – decrypted session states are not synchronized – existing flows must re-establish upon switchover (same behavior as with TLS)
- QUICv2 support planned in CY26



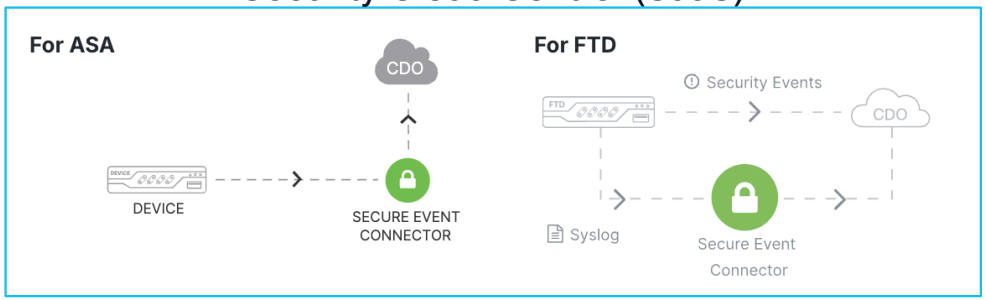


Policy Compliance

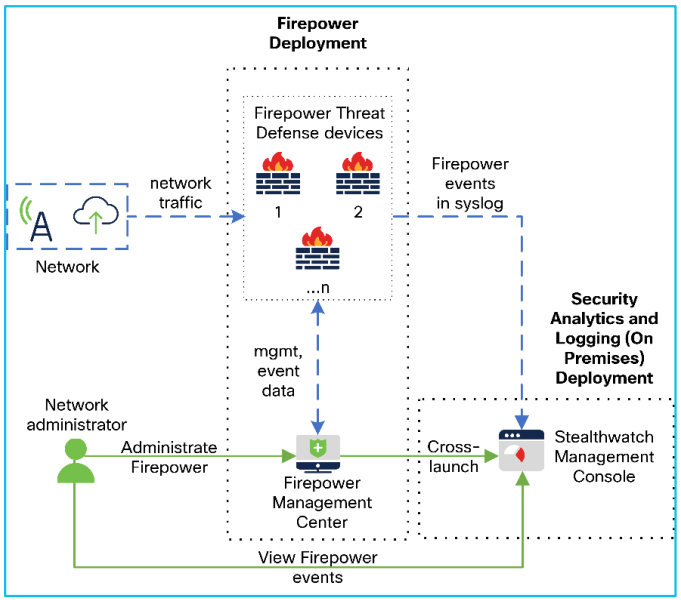
Security Analytics and Logging (SAL)

- 2 different flavors:
  - SaaS
  - On-Prem (through SNA)
- Unify Secure Firewall ASA and FTD logging
- Extends storage retention capacity and scalability

Security Cloud Control (SaaS)



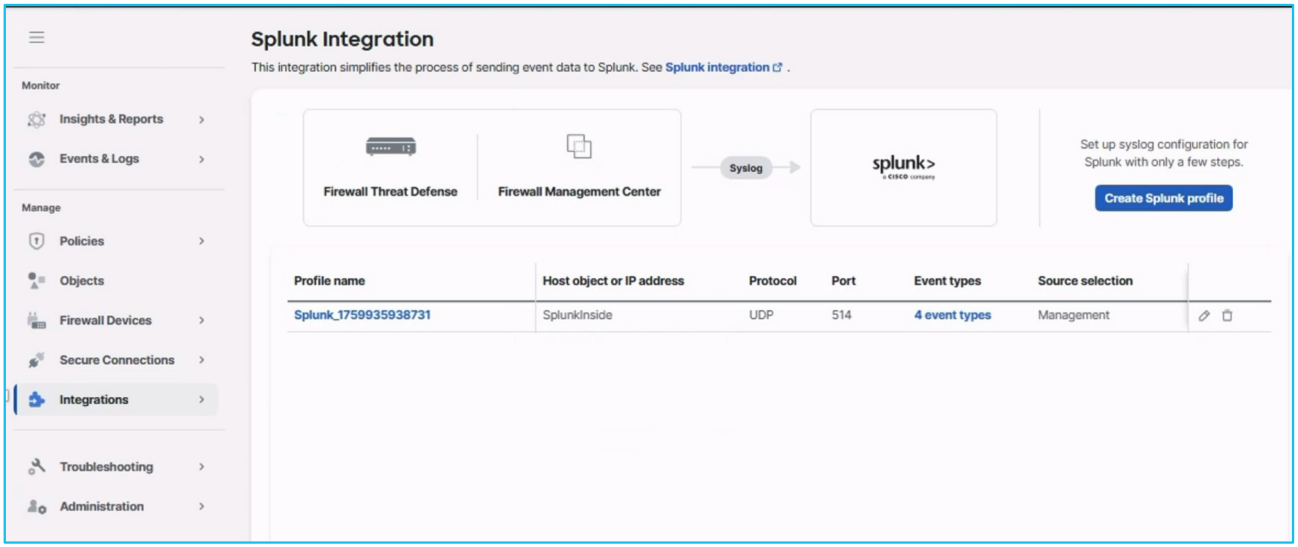
On-Prem



Policy Compliance

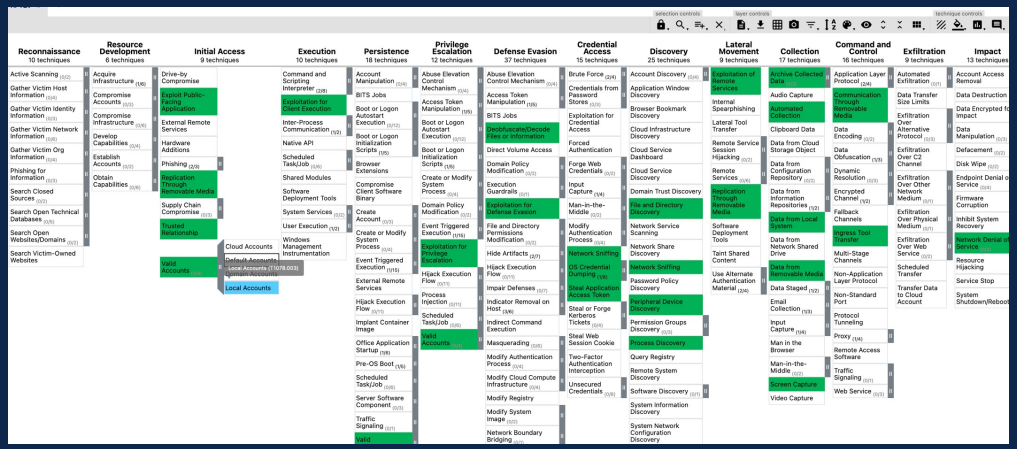
Splunk Integration

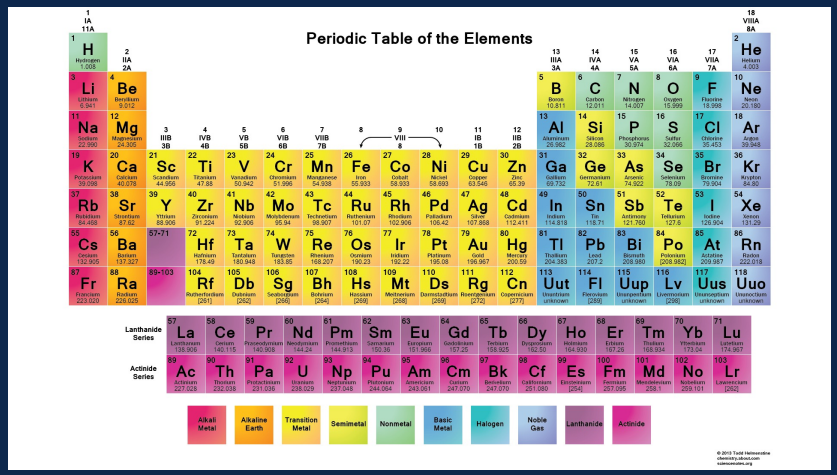
- FMC Wizard for easy integration
- Improved event options for syslog
  - Almost at par with eStremer
- UDP, TCP or TLS transport options



ATT&CK is Like a Periodic Table

The Table lists the atomic building blocks of Adversaries (Molecules)

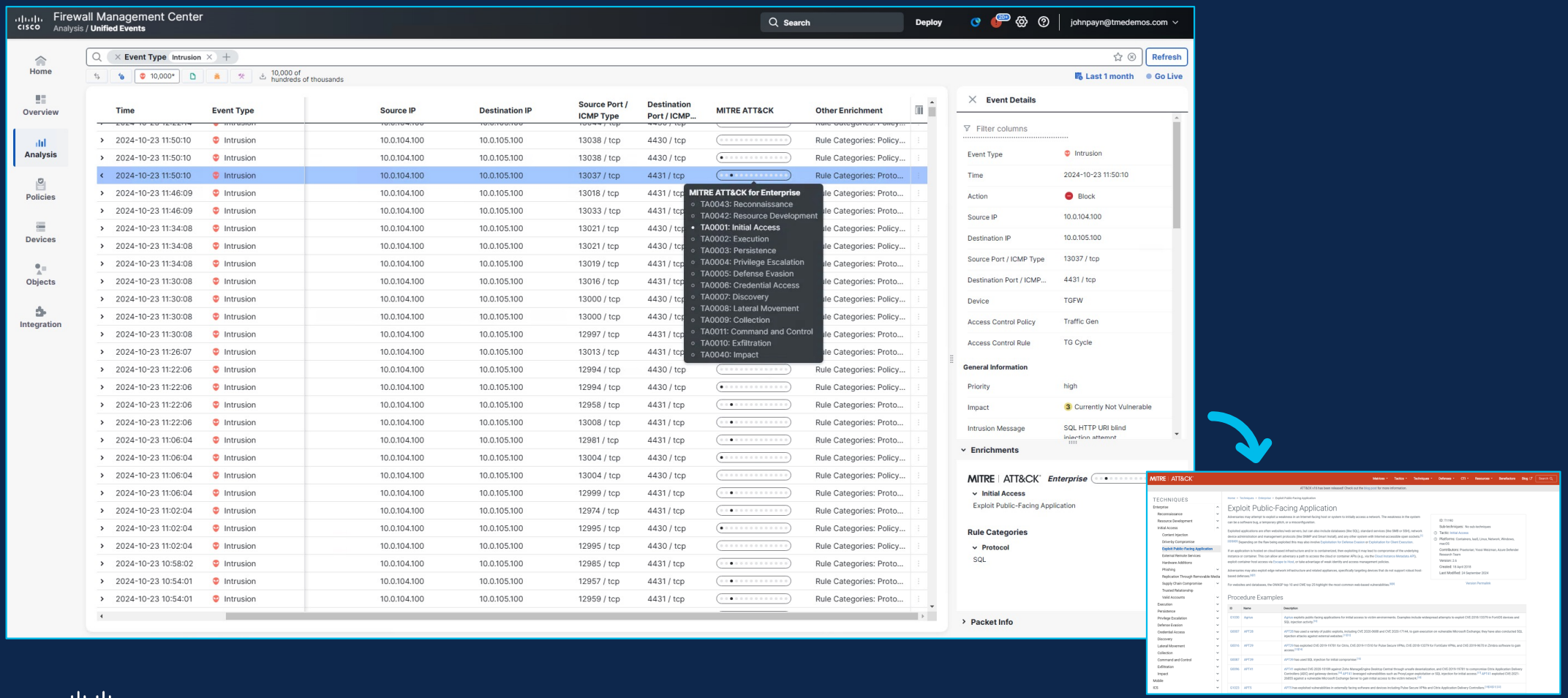




- Tactics (base on similar adversarial goals)
- Techniques and their Sub-Techniques
- Mitigations
- Adversaries

- Groups (based on similar behavior/valence band)
- Elements and their Isotopes
- MSDS Sheets
- Molecules

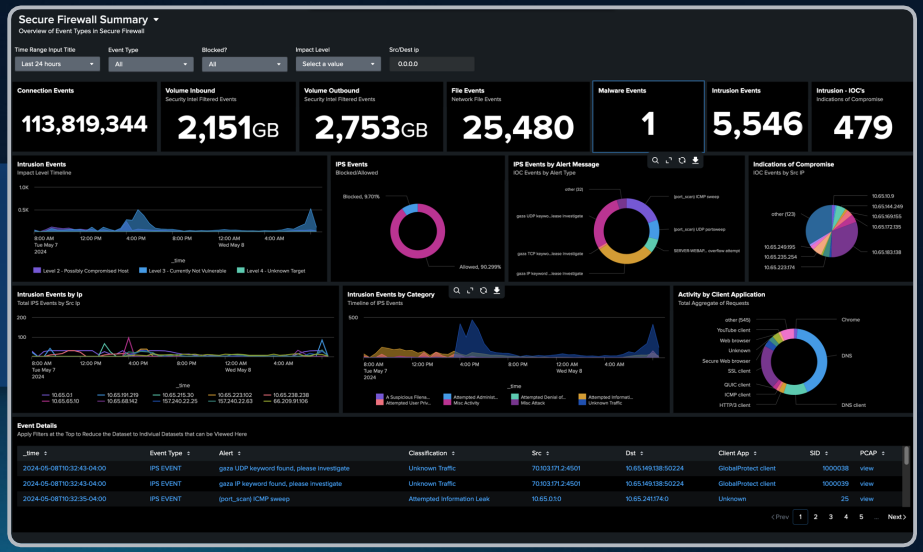
Security Content Enrichment Side Pane



Unlock insights from the network

Firewall Logs at no additional cost in Splunk*

Comprehensive TDIR + Unleash Network Insights + Bridging SecOps + NetOps



New detections | Automated response

*Cisco Secure Firewall (FTD) firewalls are entitled to 5GB of Splunk logging capacity per firewall, maxim of 1TB

Cisco AI Assistant for Security now on FMC

Assist

Policy and reporting

Find and report information on policies for faster queries, auditing, and reporting

Augment

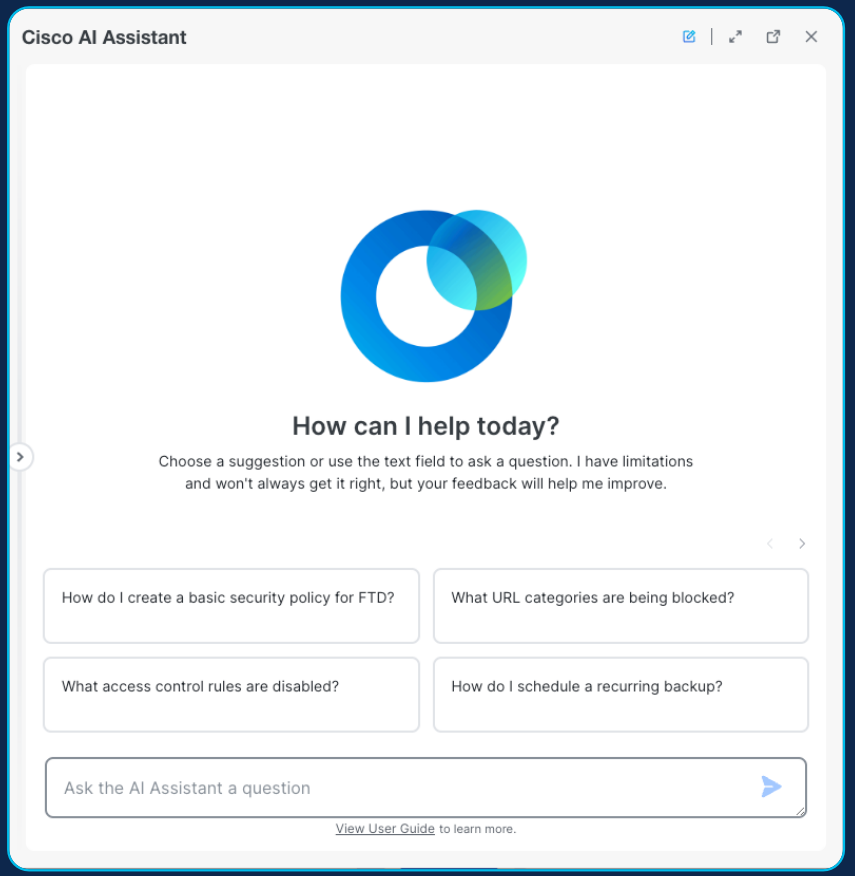
Troubleshooting and detection

Amalgamate all user guides for expedited resolution

Automate

Policy lifecycle management

Find and fix firewall rule misconfigurations for improved security and performance



Cisco Secure Firewall

DC Technology:

- Clustering (geo-clustering)
- ACI integration
- Virtual instances
- IPS/IDS/FW flexibility

Integration, Identity, Device, Health,...

- Integration with ISE, AMP, Vulnerability Scanners, Threat Director feeds...
- Dynamic Objects
- Secure Analytics and Logging (SAL)
- Application Detection (Cloud, AI, ... apps)

Talos

- Snort, MITRE
- EVE, AppID, Vulnerability DB
- Security Intelligence
- AMP

VPN

- Easy to install, also with virtual, multiplatform, Zero trust concept
- DUO MFA, Passwordless, Passport

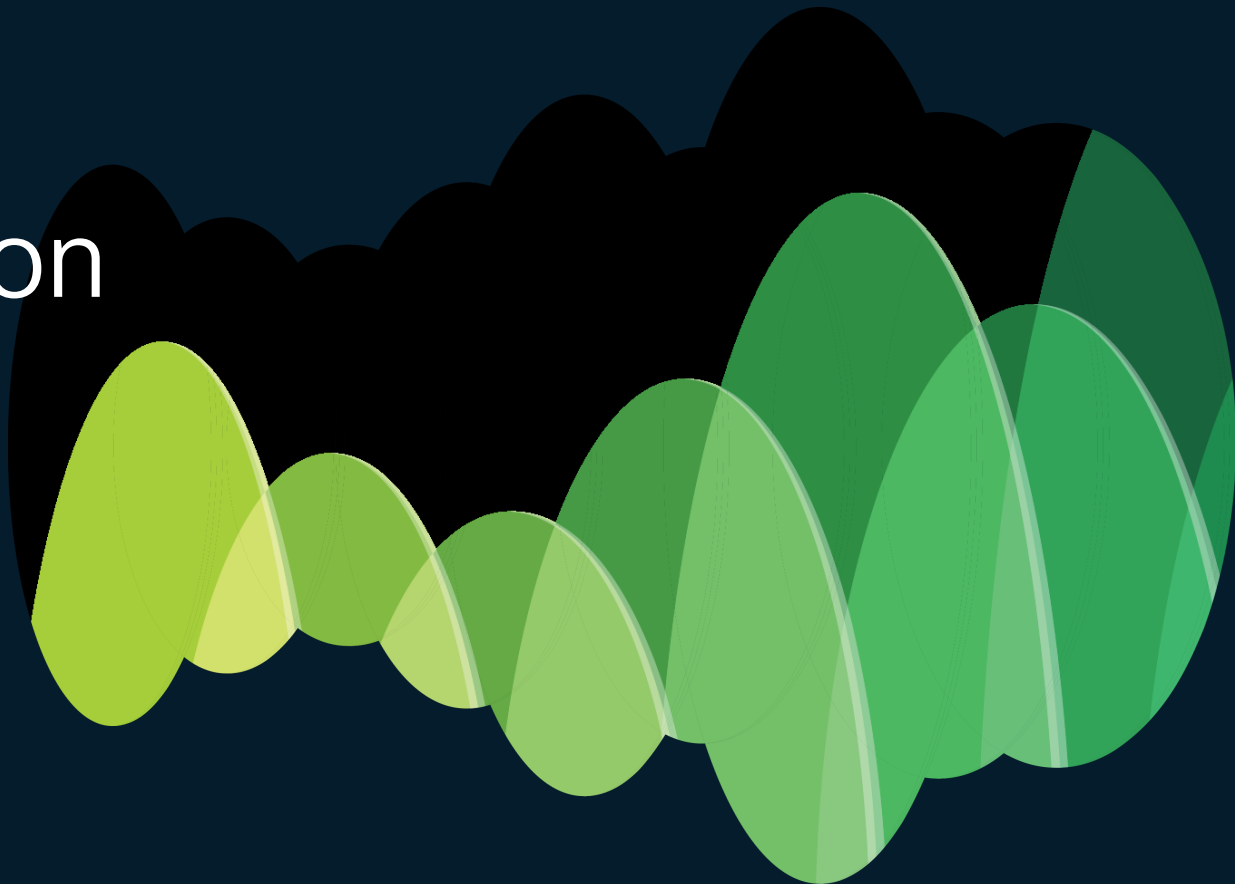
Encrypted traffic

- EVE, TLS 1.3, QUICK

Automation

- Correlation, Indication of compromise
- Network Discovery => Events Filtering & Priority, Signature Recommendation
- XDR integration
- API
- SD WAN

External Evaluation



FORRESTER WAVE LEADER 2024

Secure Firewall
Leader in Enterprise Firewall Solutions

Secure Workload
Leader in Microsegmentation

Secure Access
SSE Strong Performer

2022 FORTRESS CYBER SECURITY AWARD

Multicloud Defense
Finalist

The New York Times Wirecuter

Duo
Best 2FA App

Secure Access
Customer Value Leader

Email Security
Growth Leader -Email Radar 2024

NetSec OPEN

Firewall
Best Security Performance & Effectiveness

Gartner Magic Quadrant

Endpoint
Named a Visionary

Secure Access
Honorable Mention

TechRepublic

Duo
Best Robust Security Features

LEADERSHIP COMPASS 2022

Email Security
Recognized as Marketing champion

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

Secure Firewall
Cybersecurity Excellence Award

Secure Firewall
2024 Best Next Gen Firewall

SE Labs INTELLIGENCE-LED TESTING BEST Next Generation Firewall WINNER 2024

BEST IN KLAS SOFTWARE & SERVICES 2024

Duo
Best in KLAS: Software & Services

Secure Access
Leader in DNS

GIGAOM RADAR REPORT LEADER 2024

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2024

Secure Firewall
Global InfoSec Award

FAST COMPANY INNOVATION BY DESIGN WINNER: CISCO

XDR
Honorable Mention

Duo
Passwordless

TrustRadius Top Rated 2024

Duo
Authentication Winner

SC Awards WINNER 2024

Secure Access
Best SME Security Solution for Umbrella

Third-Party Security Reference Evaluations

WAVE LEADER 2024

Secure Firewall
Leader in enterprise Firewall

Secure Workload
Leader in Micro-segmentation

Secure Firewall
Cybersecurity Excellence Award

Secure Firewall
Global InfoSec Award

NetSecOPEN

University of New Hampshire InterOperability Laboratory

Secure Firewall
Best Price Performance

Secure Firewall
2023, 2024, 2025 Best Next Gen Firewall

Multi-cloud Defense
Finalist

cisco


cisco
Thank you