

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

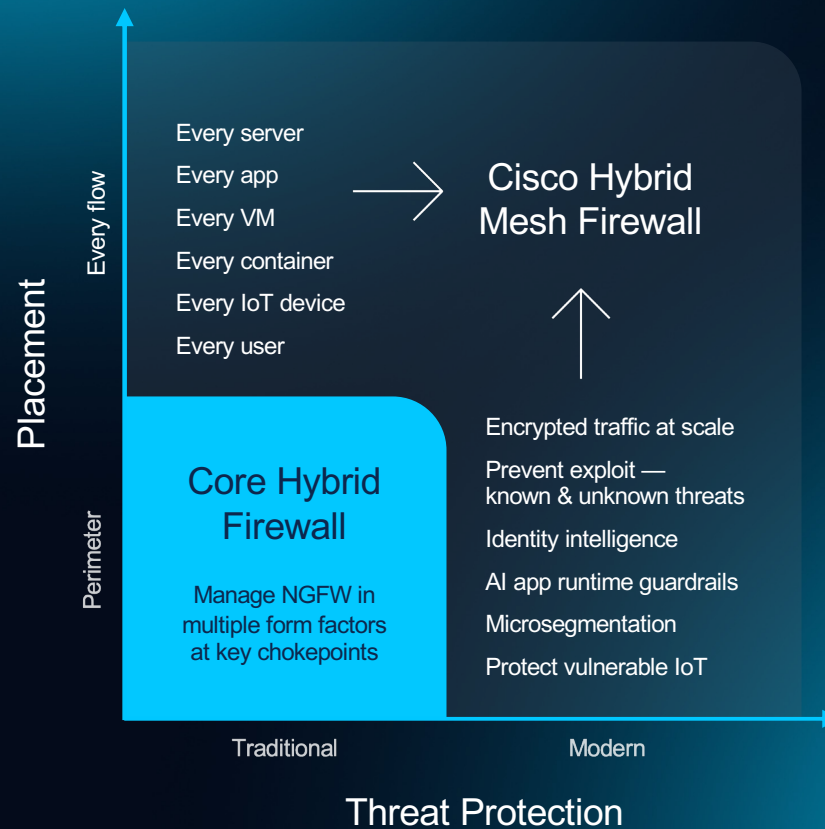
Make it easy for organizations to

Reduce attack surface

Prevent compromise

Stop lateral movement

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



What is Cisco Hybrid Mesh Firewall

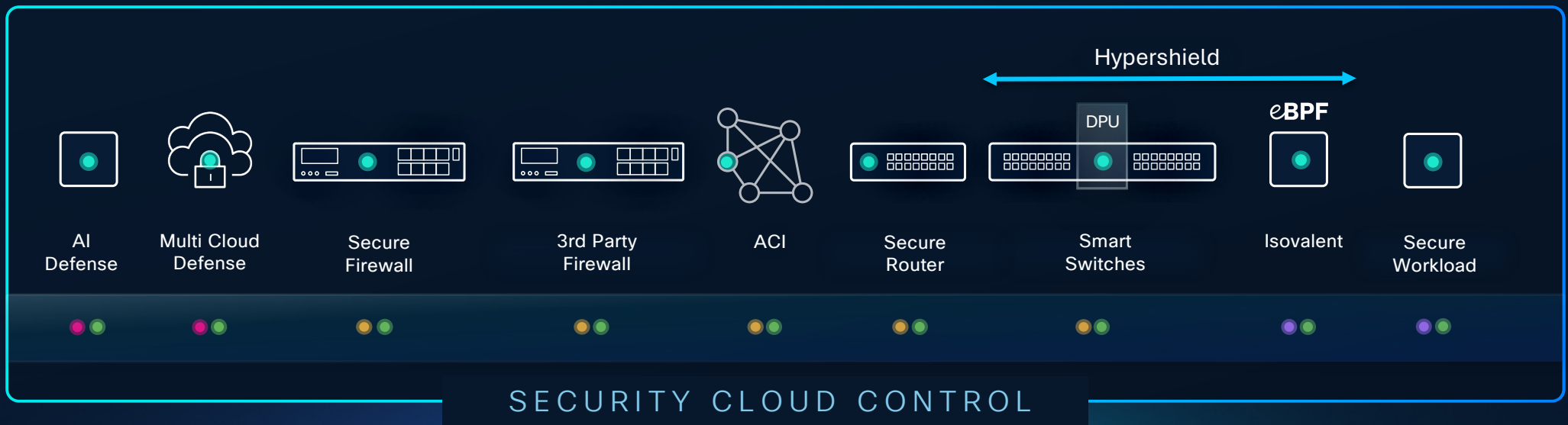
CUSTOMER SECURITY OUTCOMES

Network Segmentation

Macro & Micro Segmentation

Threat Detection & Exploit Protection

AI Security

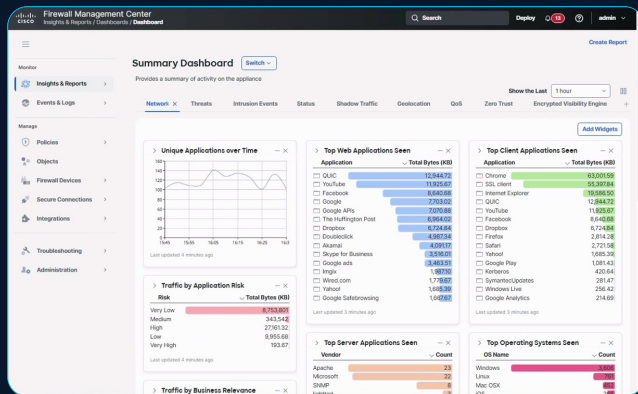


Write policy once, enforce across the mesh

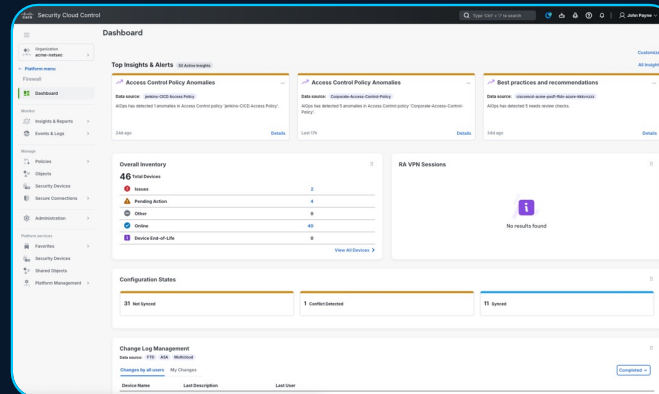
Management Designed for the User

Flexibility of cloud or on-premises options

Firewall Management Center

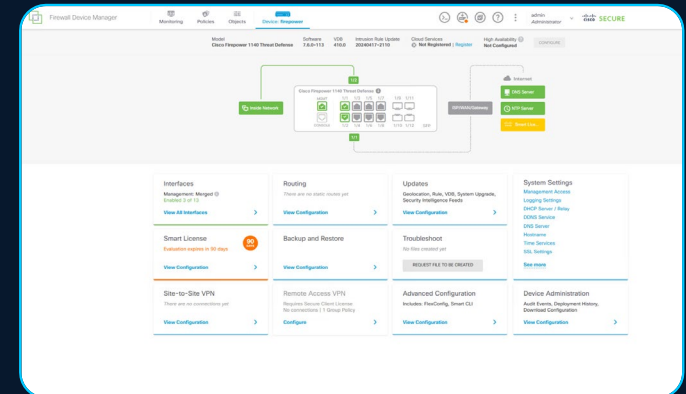


On-premise centralized manager



Cloud-delivered centralized manager via Security Cloud Control

Firewall Device Manager



On-box manager NetOps focused

Firewalls for every use case

ISA 3000 Series



≤0.4Gbps NGFW

200 Series



1.5Gbps NGFW

1010 & 1100 Series



≤3Gbps NGFW

1200 Compact Series



≤9Gbps NGFW

1200 Series



≤18Gbps NGFW

3100 Series



≤45Gbps NGFW
16x Clustering

4200 Series



≤145Gbps NGFW
16x Clustering

6100 Series



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

Organization

Home

Products

- Firewall
- Hypershield
- Multicloud Defense
- Secure Access
- Secure Workload

Platform services

- Favorites
- Security Devices
- Shared Objects
- Platform Management

Home

Top Insights & Alerts 50 Active Insights

Best practices and recommendations

Data source: ciscomcd-kgreeshm-acme-aws-ftdv-mcd-licensed-wqoeavog

AI Ops has detected 5 needs review checks.

7d ago [Details](#)

Best practices and recommendations

Data source: ciscomcd-kgreeshm-acme-aws-ftdv-mcd-licensed-xvjgmyld

AI Ops has detected 5 needs review checks.

7d ago [Details](#)

Best practices and recommendations

Data source: ciscomcd-kgreeshm-merck-demo-az-ftd-kulefoqn

AI Ops has detected 5 needs review checks.

8d ago [Details](#)

Multicloud Defense

Account Resources

100 VPCS/ VNets	236 Security Groups	148 Route Tables	335 Subnets
155 Instances	37 Load Balancers	0 Tags	37 Applications



Secure Firewall

Multicloud Defense

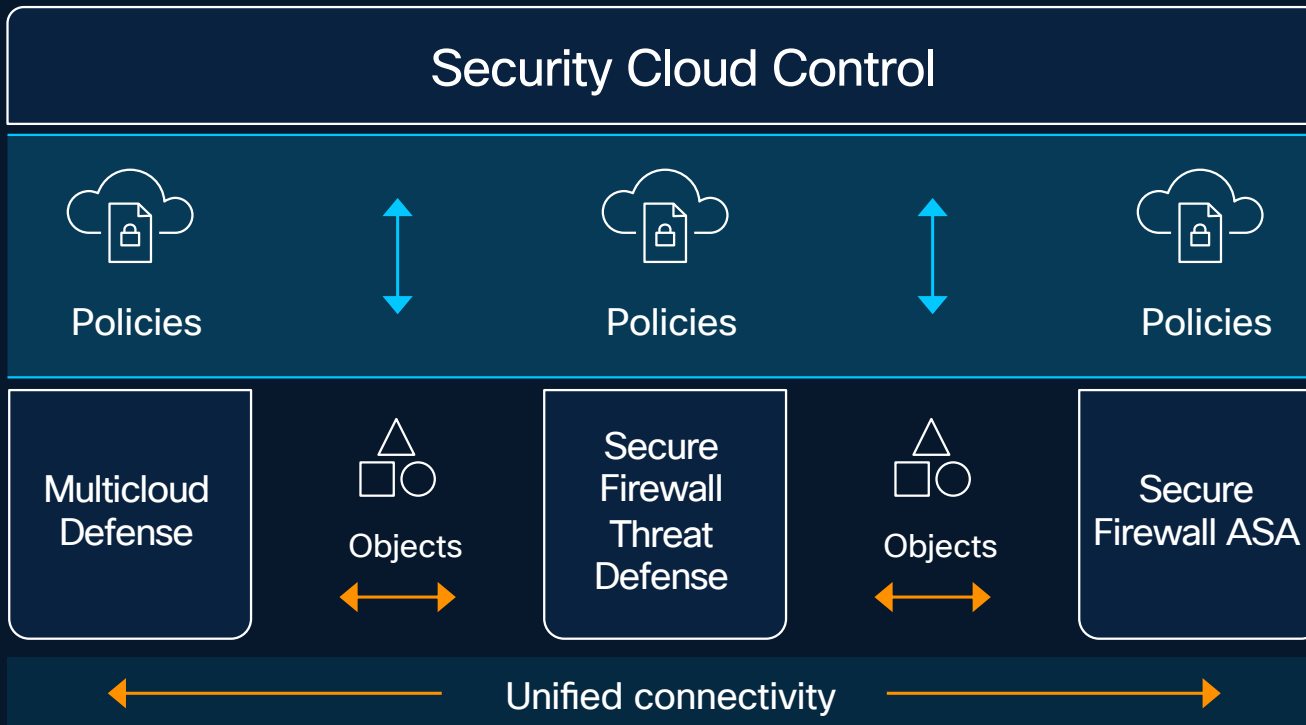
Hypershield

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

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.

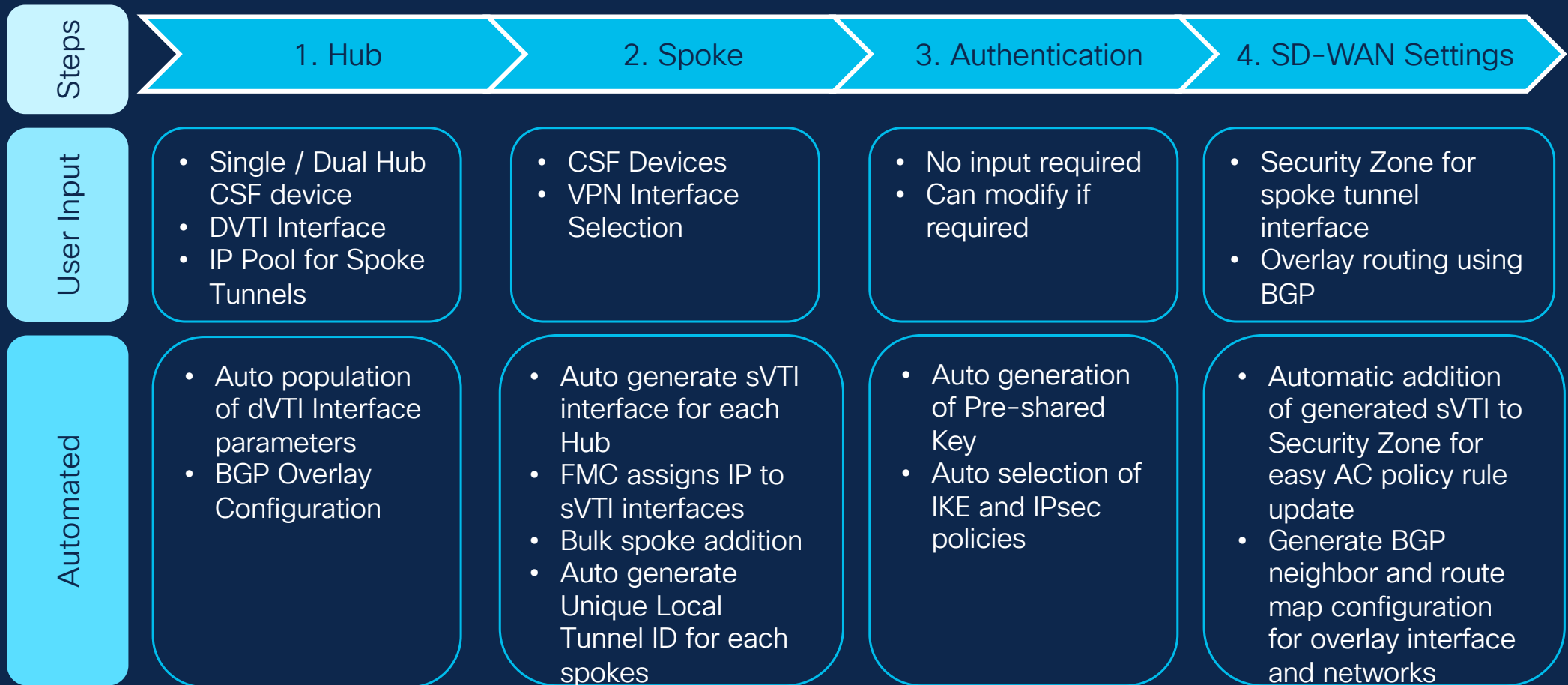
Bulk Onboarding multiple devices using CSV file



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



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

The image displays two screenshots of the Cisco Firewall Migration Tool interface. The top screenshot shows the main navigation menu with the 'Migrations' section highlighted, and the 'Firewall Migration Tool' option selected. A blue arrow points from this option to the bottom screenshot. The bottom screenshot shows the 'Manual Configuration Upload' screen, which includes instructions for the configuration file format and an 'Upload' button.

Firewall Migration Tool (Version 7.7.10.4)

Extract Config Information ⓘ Source: Palo Alto Networks (8.0+)

Extraction Methods

Manual Configuration Upload

The configuration file must be a zip file consisting of the following:

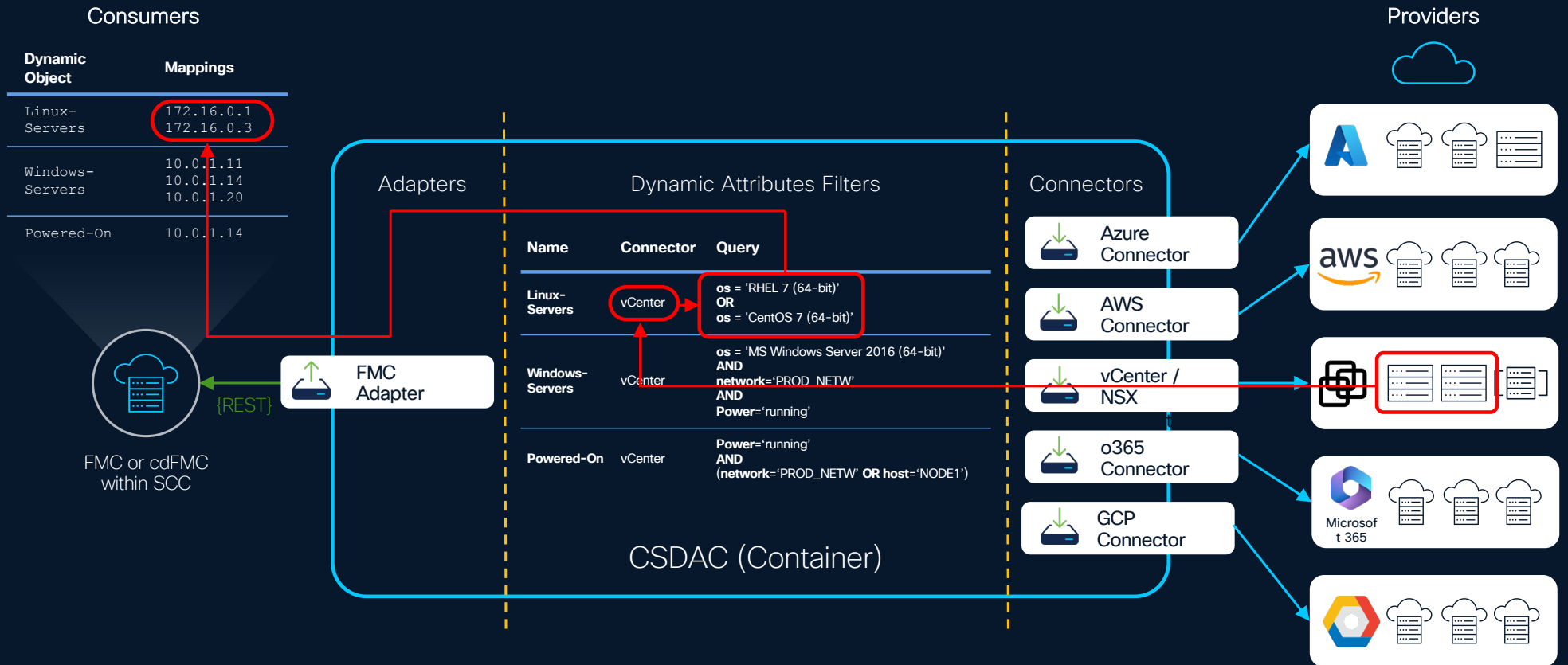
- Zip Config file derived from the PAN Tool.

Upload

Context Selection >

Parsed Summary >

Architecture of the Dynamic Attributes Connector



Cisco Secure Dynamic Attributes Connectors – your bridge to dynamic data

Cloud Connectors

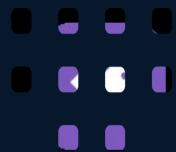


AWS

Azure

GCP

VMWare



Azure Service
Tags



Security
Groups



Service
Tags

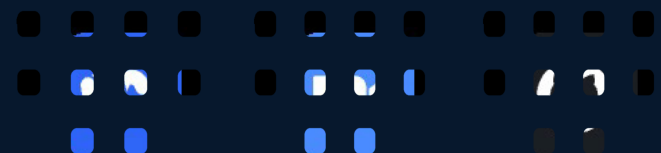


Multicloud
Defense

Public Feeds and External Connectors



Office365



Webex

Zoom

GitHub



Generic
Text



Cyber
Vision



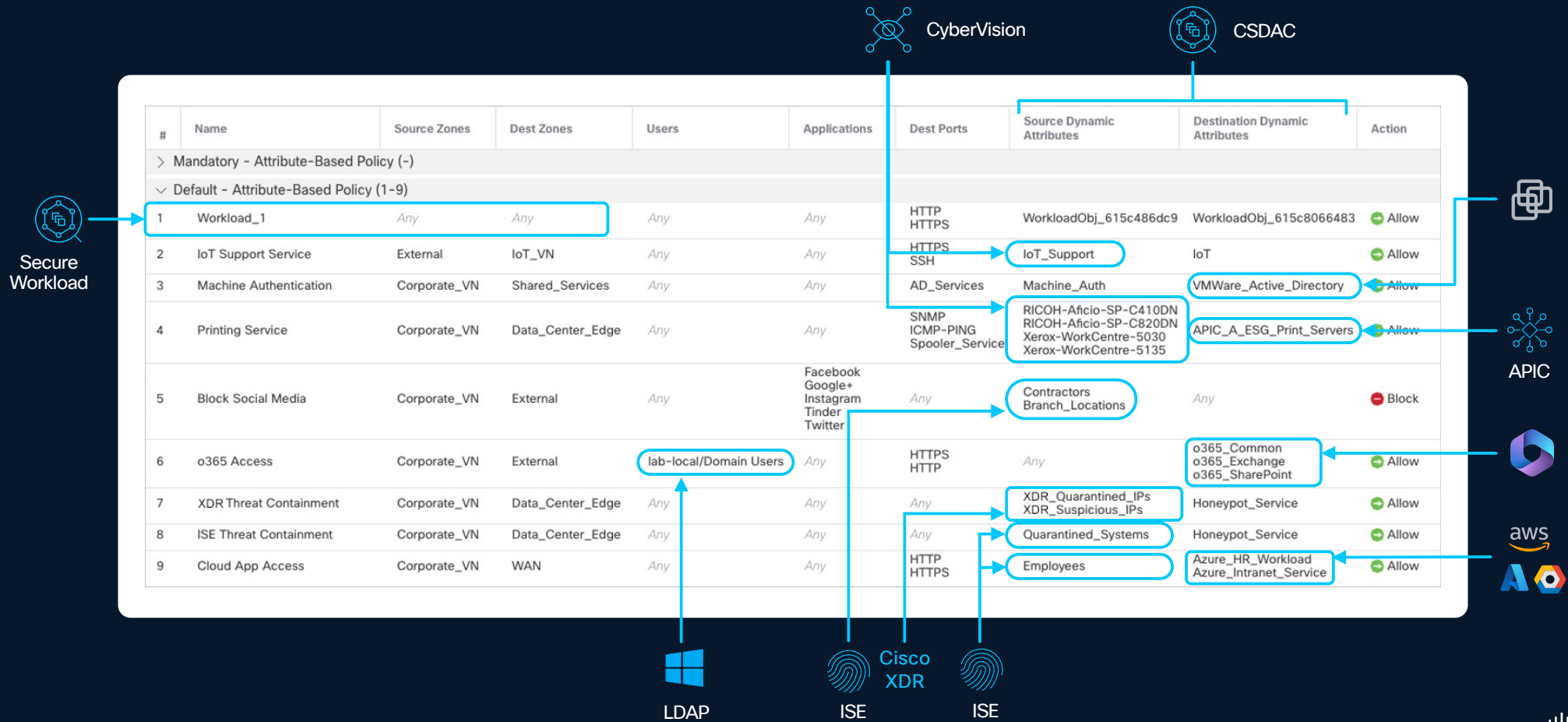
pxGrid
Cloud



ACI



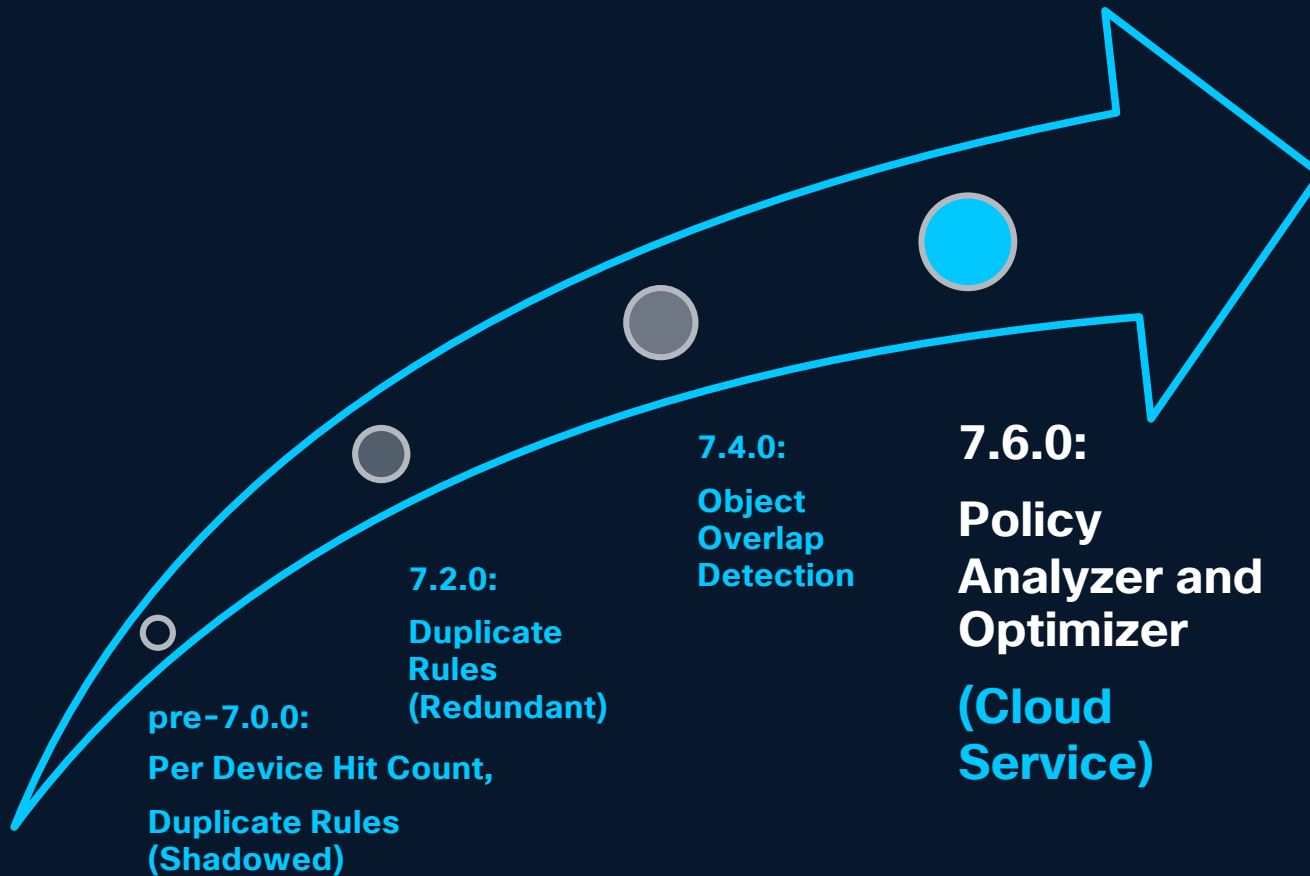
Attribute-based Policy with User and Server Identity



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

Policy Analyzer and Optimizer

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

Summary Duplicate rules 454 Expired rules 54 Mergeable rules 661 Overlapping objects 128 Policy insights

Overall summary
Review the cumulative summary to address issues, if any, and achieve optimal performance.

4,815 (83.8%)
Healthy rules

931 (16.2%)
Unhealthy rules

0
Disabled rules

Total 1,297 anomalies, in 931 unhealthy rules

Shadowed rules
296 ↗ 22.8%

Expired rules
54 ↗ 4.2%

Full overlap objects
111 ↗ 8.6%

Redundant rules
158 ↗ 12.2%

Mergeable rules
661 ↗ 51.0%

Partial overlap objects
17 ↗ 1.3%

Search by Access Control Policy Name, Analysis Status, or Remediation Status Displaying 33 of 33 results

Access Control Policy Name	Devices	Total Rules	Observations	Analysis Status	Last Modified (UTC+01:00)	Last Analyzed (UTC+01:00)	Remediation Status	Remediation Time (UTC+01:00)
<input checked="" type="checkbox"/> Corporate-Access-Cont	3	26	5 19% Optimizable	Completed	Dec 15, 2025 06:38:43	Dec 08, 2025 04:16:09 Analysis out-of-date		
<input type="checkbox"/> jenkins-CICD Access Pc	2	2	1 50% Optimizable	Completed	Dec 12, 2025 04:57:55	Nov 13, 2025 22:18:38 Analysis out-of-date		
<input type="checkbox"/> Datacenter-Access-Con	1	18	0 Healthy	Completed	Dec 12, 2025 04:57:55	Nov 11, 2025 04:08:41 Analysis out-of-date		
<input type="checkbox"/> Public-Cloud-Branch-Ac	1	2	0 Healthy	Completed	Dec 12, 2025 04:57:55	Nov 07, 2025 21:20:53 Analysis out-of-date		
<input type="checkbox"/> AZURE_ARM_2 Firewall	0	0	0 Healthy	Completed	Dec 12, 2025 04:57:55	Nov 07, 2025 21:18:51 Analysis out-of-date		
<input type="checkbox"/> AWSFW-Access-Policy	2	1	0 Healthy	Completed	Dec 12, 2025 04:57:55	Nov 07, 2025 20:07:28 Analysis out-of-date		

Corporate-Access-Control-Policy

Devices: 3
Total Rules: 26
Observations: 5 19% Optimizable
Analysis Status: Completed
Last Modified: Dec 15, 2025 06:38:43 UTC+01:00
Last Analyzed: Dec 08, 2025 04:16:09 UTC+01:00
Analysis out-of-date
Remediation Status: Not Running
Hit Count Aggregation: Completed
Status:

Analysis Actions
[View analysis details](#)
[Download analysis report](#)
[Reanalyze policy](#)

Remediation Actions
[Remediation history \(0 version available\)](#)

Policy Observation
We found a total of 5 anomalies.

Duplicate Rules (3)
Fully Shadowed Rules: 0
Fully Redundant Rules: 3

Overlapping Objects (0)
Fully Overlapped Objects: 0
Partially Overlapped Objects: 0

Mergeable Rules(2)
Expired Rules(0)

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	...

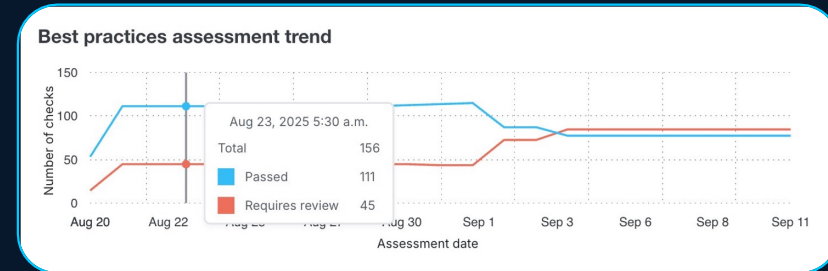
Best practices and recommendations

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



Improve access control

Recommendations to enhance access control for better security and optimal firewall performance.

11 Total checks | **7** Require review | **4** Passed

Checks

Block Uninspectable Archives should be enabled

Requires review Warning

The file policy on this device currently has the "Block Uninspectable Archives" setting disabled. It is recommended to enable this setting to block archive files with contents that the system cannot inspect for reasons other than encryption, such as corrupted files or those exceeding the specified maximum archive depth. By default, this setting is enabled in the "Advanced" section of the File Policy.

Action Required: Review the file policy settings and enable the "Block Uninspectable Archives" option to enhance security and ensure optimal system performance.

Allow rule configured without an associated Intrusion or File policy

Requires review Informational Potential Misconfiguration

The Access Control Policy on this device is configured with one or more access control rules that are set to an action of "Allow" without the addition of an Intrusion or File Policy.

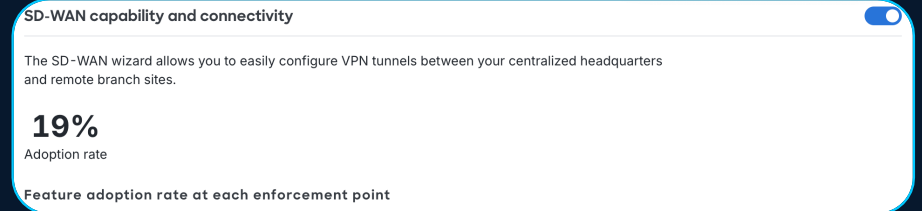
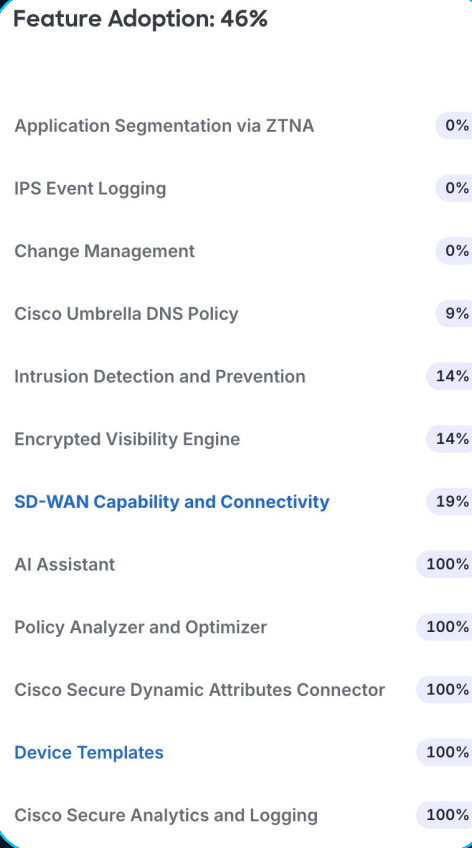
If the intent is to exclude the matching traffic from inspection, the rule should either be changed to an action of "Trust" and moved towards the top of the policy, or moved into the Pre-filter policy with an action of "Fastpath".

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.



Adoption: 19%

Firewall Threat Defense

Devices	Adoption status
NGFW1	Adopted
ACME-Branch-2-FTD	Not adopted
NGFW2	Adopted
ACME-Datacenter-FTD	Not adopted
jenkins-FW	Not adopted
NGFW4	Adopted
AWSFW-3	Not adopted
ACME-Branch-1-FTD	Not adopted
ACME-PAO-TEST	Not adopted
ciscomcd-acme-aws-ftdv-fndfduwcc	Not adopted

21 Total | 17 Not adopted | 4 Adopted

Rows per page: 10 | 1 | 2 | 3

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

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

[Learn more](#)

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.

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.

Security vulnerability and bug fixes [View all >](#)

14 Total available fixes	13 Security vulnerability fixes	1 Bug fixes
------------------------------------	---	-----------------------

Device	Current version	Recommended versions ⓘ
smal Cisco Secure Firewall Threat Defense for VMware FTD	7.6.0	7.6.1 (7 CVEs fixed) → 7.6.2 (7 CVEs fixed) → 7.7.10 (7 CVEs fixed)
> smath Cisco Secure Firewall Threat Defense for VMware Cluster	7.6.0	7.6.1 (7 CVEs fixed) → 7.6.2 (7 CVEs fixed) → 7.7.10 (7 CVEs fixed)
smal Cisco Secure Firewall Threat Defense for VMware FTD	7.6.0	7.6.1 (7 CVEs fixed) → 7.6.2 (7 CVEs fixed) → 7.7.10 (7 CVEs fixed)
FTD-Pu Cisco Secure Firewall Threat Defense for VMware FTD	7.6.0	7.6.1 (7 CVEs fixed) → 7.6.2 (7 CVEs fixed) → 7.7.10 (7 CVEs fixed)
> FTDHA Cisco Secure Firewall Threat Defense for VMware High Availability	7.7.0	7.7.10 (3 CVEs fixed)
smal Cisco Secure Firewall Threat Defense for VMware FTD	7.7.0	7.7.10 (3 CVEs fixed)

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.

Recommended upgrades

Recommended version 1
7.6.1
Details
Security vulnerability fixes: 7
Bug fixes: 0
[Release notes for Version 7.6.1](#)

Golden version
7.6.2
Details
Security vulnerability fixes: 7
Bug fixes: 0
[Release notes for Version 7.6.2](#)

Recommended version 2
7.7.10
Details
Security vulnerability fixes: 7
Bug fixes: 0
[Release notes for Version 7.7.10](#)

Security vulnerability fixes Bug fixes

Search: [] 13 results

Severity: 1
Critical
High

CVE ID	Title	Impact	Description	CVSS score
CVE-2025-20251	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall...	High	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Fi...	8.5
CVE-2025-20136	Cisco Secure Firewall Adaptive Security Appliance and Secure Fir...	High	A vulnerability in the function that performs IPv4 and IPv6 Network Adre...	8.6
CVE-2025-20244	Cisco Secure Firewall Adaptive Security Appliance and Secure Fir...	High	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Fi...	7.7
CVE-2025-20263	Cisco Secure Firewall Adaptive Security Appliance and Secure Fir...	High	A vulnerability in the web services interface of Cisco Secure Firewall Ada...	8.6
CVE-2025-20133	Cisco Secure Firewall Adaptive Security Appliance and Secure Fir...	High	Multiple vulnerabilities in the management and VPN web servers for Cisco...	8.6
CVE-2025-20243	Cisco Secure Firewall Adaptive Security Appliance and Secure Fir...	High	Multiple vulnerabilities in the management and VPN web servers for Cisco...	8.6
CVE-2025-20224	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, a...	High	Multiple vulnerabilities in the Internet Key Exchange Version 2 (IKEv2) feat...	8.6
CVE-2025-20225	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, a...	High	Multiple vulnerabilities in the Internet Key Exchange Version 2 (IKEv2) feat...	8.6
CVE-2025-20239	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, a...	High	Multiple vulnerabilities in the Internet Key Exchange Version 2 (IKEv2) feat...	8.6
CVE-2025-20252	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, a...	High	Multiple vulnerabilities in the Internet Key Exchange Version 2 (IKEv2) feat...	8.6
CVE-2025-20253	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, a...	High	Multiple vulnerabilities in the Internet Key Exchange Version 2 (IKEv2) feat...	8.6
CVE-2025-20254	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, a...	High	Multiple vulnerabilities in the Internet Key Exchange Version 2 (IKEv2) feat...	8.6
CVE-2025-20217	Cisco Secure Firewall Threat Defense Software Snort 3 Denial of ...	High	A vulnerability in the packet inspection functionality of the Snort 3 Detecti...	8.6

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.

End-of-Life for ASA5525

Critical

Operational



15 days

Impacted device



ASA5525

List of devices with the same model

Device name	Location	Software version
ASA5525	3.101.155.65	9.19(1)28
ASA5525_V4	54.151.42.60	9.20(3)7
ASA5525_V3	54.67.68.83	9.20(3)7

Cisco Recommended Replacement Devices

Begin planning for a replacement strategy to ensure continued network security and performance.

Cisco Secure Firewall 1150 Threat Defense

Product Number	FPR1150
Form	Rack mount, 1U
Throughput	5.3 Gbps
Interfaces	8x RJ45, 2x SFP, 2x 10G SFP+

[View data sheet](#)

Cisco Secure Firewall 1140 Threat Defense

Product Number	FPR1140
Form	Rack mount, 1U
Throughput	3.3 Gbps
Interfaces	8x RJ45, 4x SFP

[View data sheet](#)

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%**

Reduce management overhead with AI Assistant

Assist

+ Policy configuration

Augment

+ Troubleshooting

Automate

+ Policy lifecycle management

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

Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

Below the table, the AI Assistant confirms: "'Rule_Test_1' is successfully created in policy 'Test_1'". It then states: "Congratulations, your rule named, 'Rule_Test_1' is successfully created in policy 'Test_1'. The rule is created in a **disabled state** as of now. You can enable it from your 'Test_1' policy detail page." A link "Go to policy detail page" is provided. At the bottom, there is a text input field "Ask the AI Assistant a question" and a disclaimer: "The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more."

AI Defense



Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Recommended Actions

Protect applications (67)

Secures sensitive data, prevents unauthorized access, and protects proprietary algorithms from theft or misuse.

Hide [View →](#)

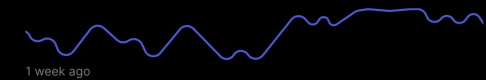
Review increased app usage

3 days ago

Review sudden spikes in blocked events to avoid security risks.

ExternalChatBot Application

45MB +7%



Hide [View →](#)

Review third party apps (67)

3 days ago

Safeguards user privacy, prevents data breaches, and ensures compliance with security and regulatory standards.

Cisco Multicloud Defense

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

BRKSEC-2229

Centralized Management

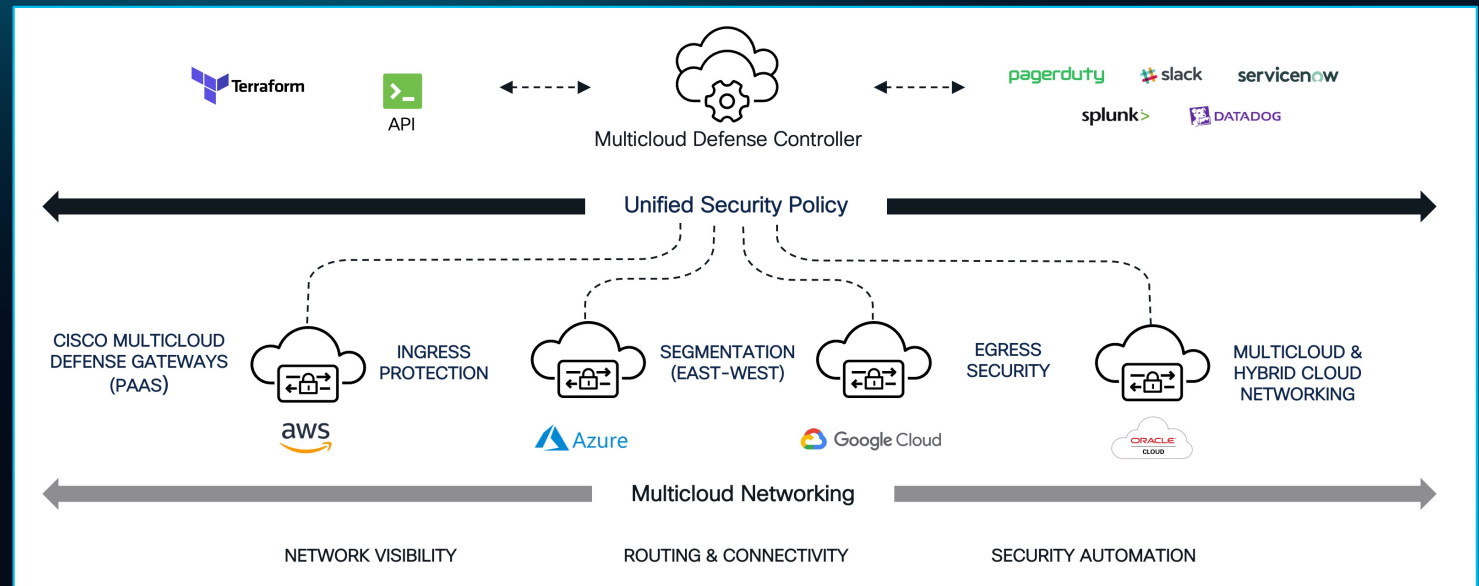
Multi-region and Multi-AZ architecture

Autoscale and Auto Heal

Gateway lifecycle management

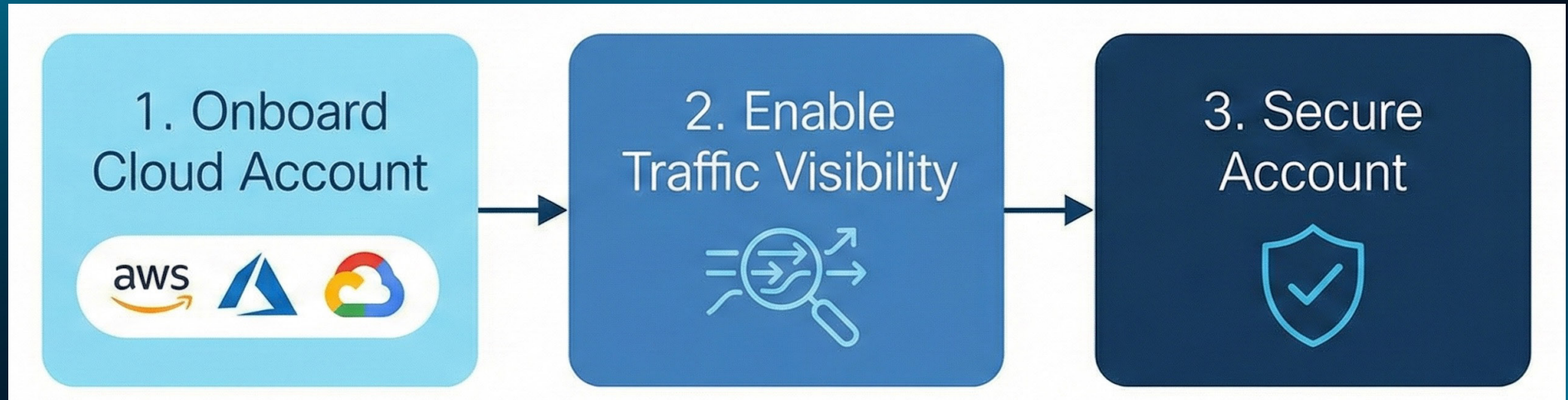
Traffic engineering

Unified dynamic policies



Cisco Multicloud Defense Workflow

Multicloud Defense Controller



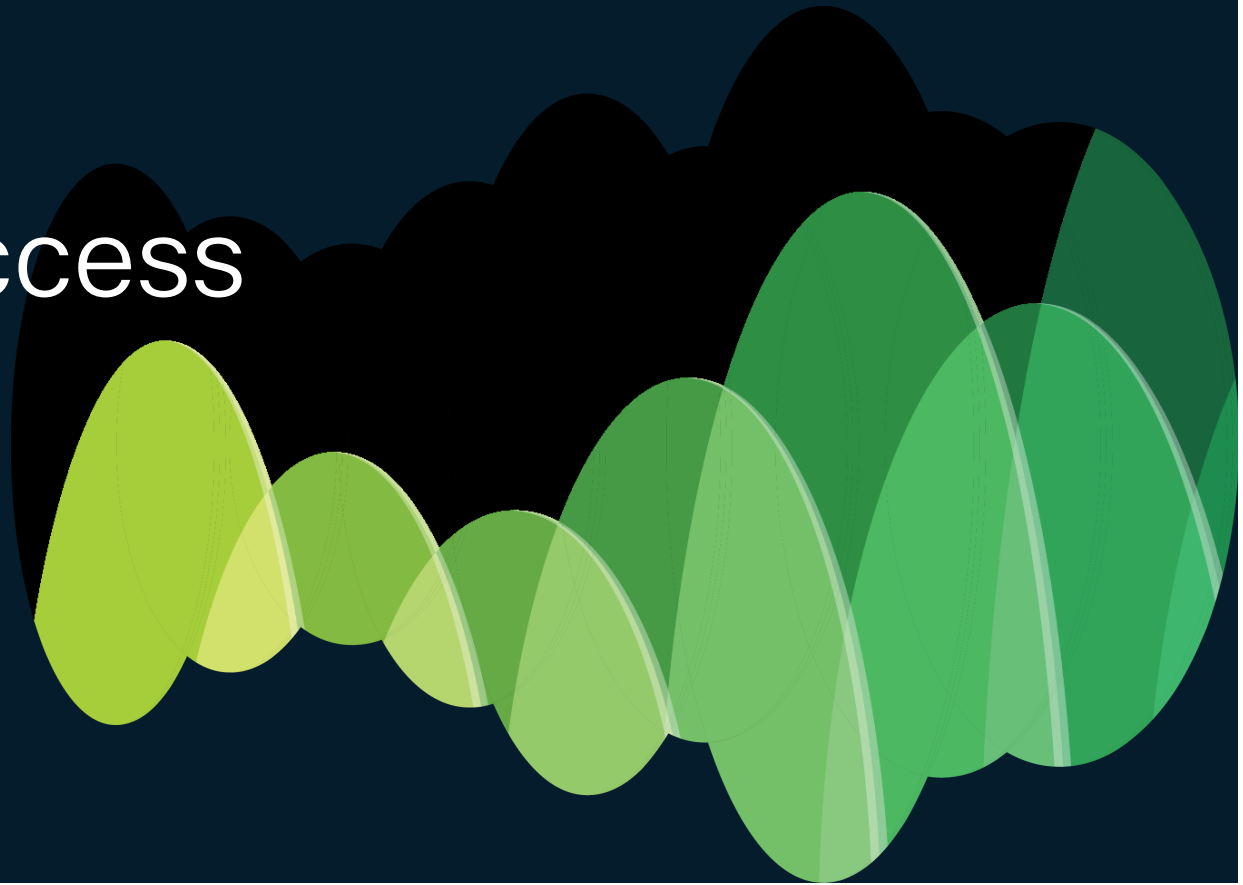
Securely onboard cloud accounts

Enable DNS query & VPC/NSG flow logs

Orchestration & Automation

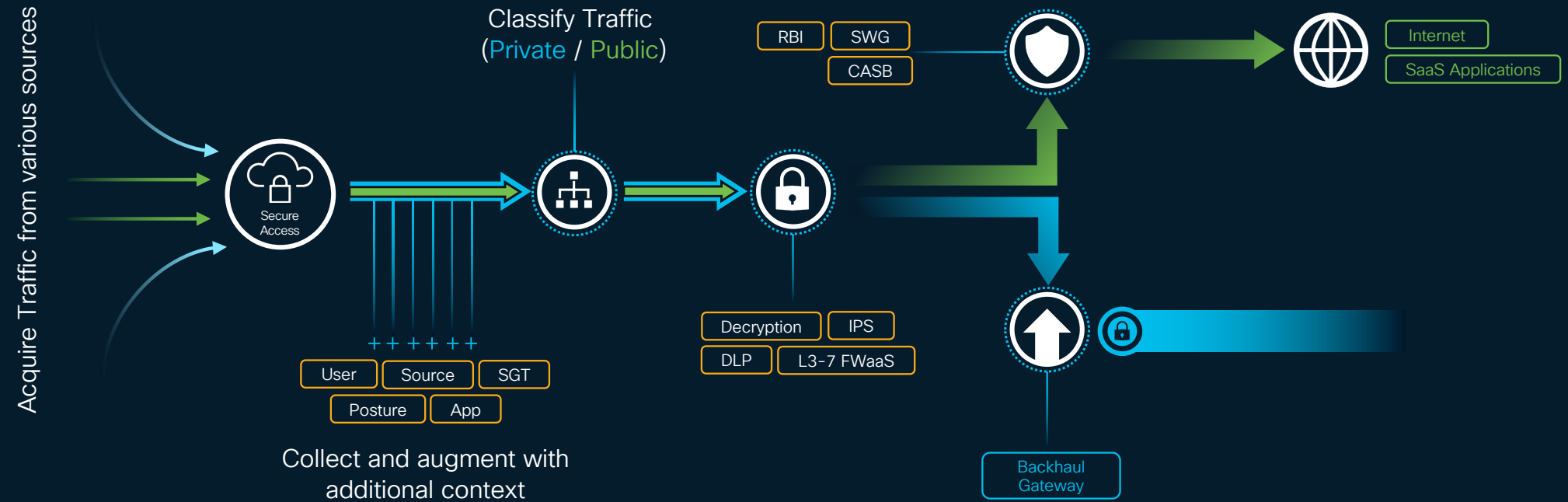
Orchestrate, manage, control, and secure cloud infrastructure using Multicloud Defense

Cisco Secure Access



Unified Cloud Architecture

Universal Traffic Acquisition & Single Data Path



Unified Cloud Architecture

Consistent Policy & Security



Secure Access

Unified Policy Evaluation

941 Rules Change view

#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1	Any employee access to any...	Private	Allow	Any User... +3	Any Applic... +1		4.1K	
2	US-Canada Employees	Private	Block	North Ame... +4	Company... +4		1.2K	
3	Product Management Resour...	Internet	Warn	PM User Gr... +1	Product M... +2		924	
4	Europe Content Block List	Internet	Isolate	Europe Em... +7	EU Catego... +7		-	
5	Contractors access to Lab App	Private	Allow	Contractor... +6	Lab Applic... +9		1.2M	
6	Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
7	Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
8	Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
9	Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
10	Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	

Rows per page: 100

Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private destinations	Block	Any	Any private destination	-	-
For all internet destinations	Allow	Any	Any internet destination		-

Consistent Security Enforcement

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

Full IPS

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

Balanced Security and Connectivity
Default IPS Profile

Prevention 9353 Block 488 Log Only 40380 Ignore

Block (9353) Log Only (488) Ignore (40380)

Blocked IPS signatures are always blocked and logged as a threat.

Signatures

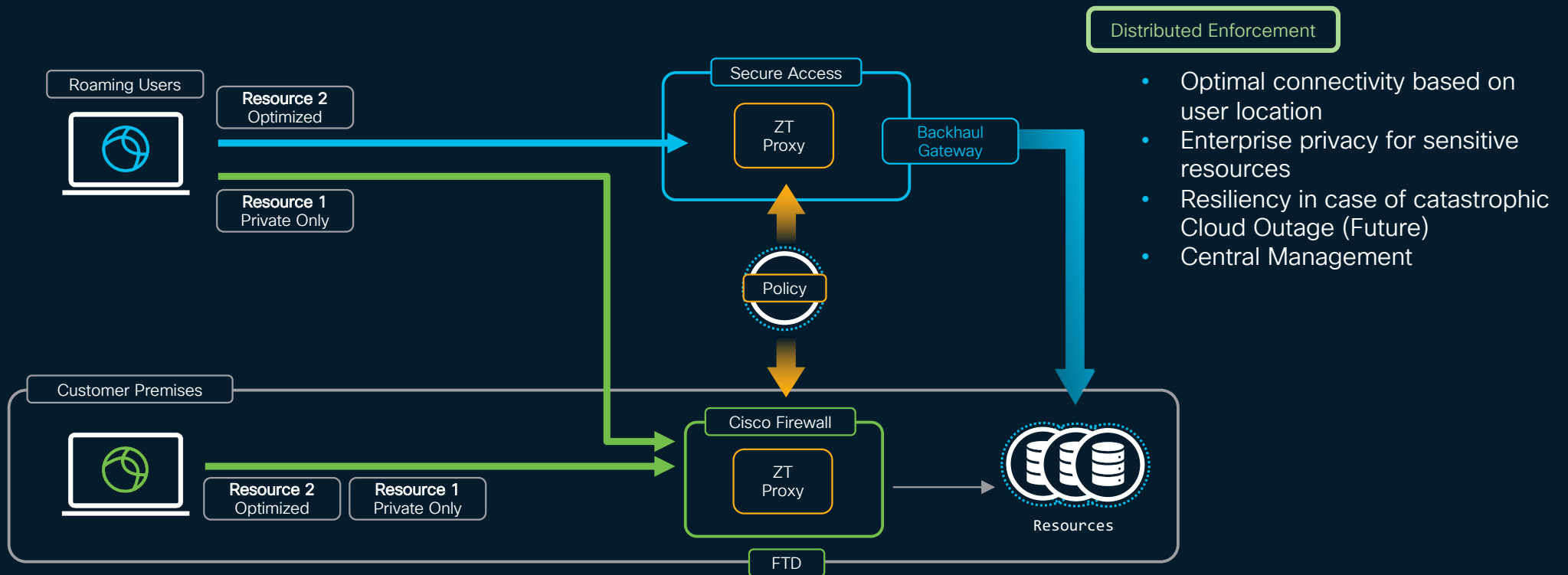
- MALWARE-BACKDOOR serveme runtime detection
- MALWARE-BACKDOOR remote hack 1.5 runtime detection - logon
- MALWARE-BACKDOOR remote hack 1.5 runtime detection - execute file
- MALWARE-BACKDOOR remote hack 1.5 runtime detection - get password
- MALWARE-BACKDOOR remote hack 1.5 runtime detection - start keylogger

Unified Internet + Private Policy

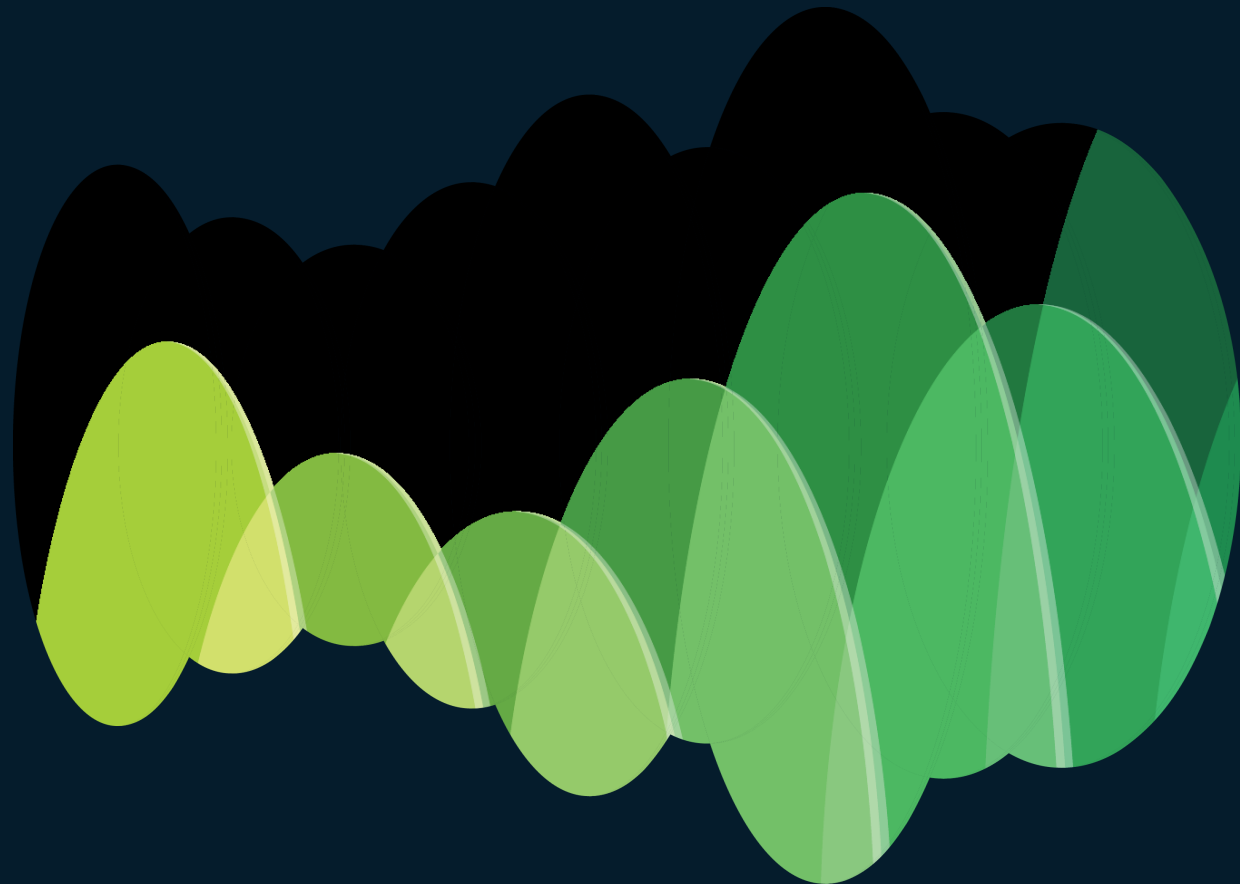
- Single view of all access
- Filter and sort view
- No need to pivot

Universal ZTNA

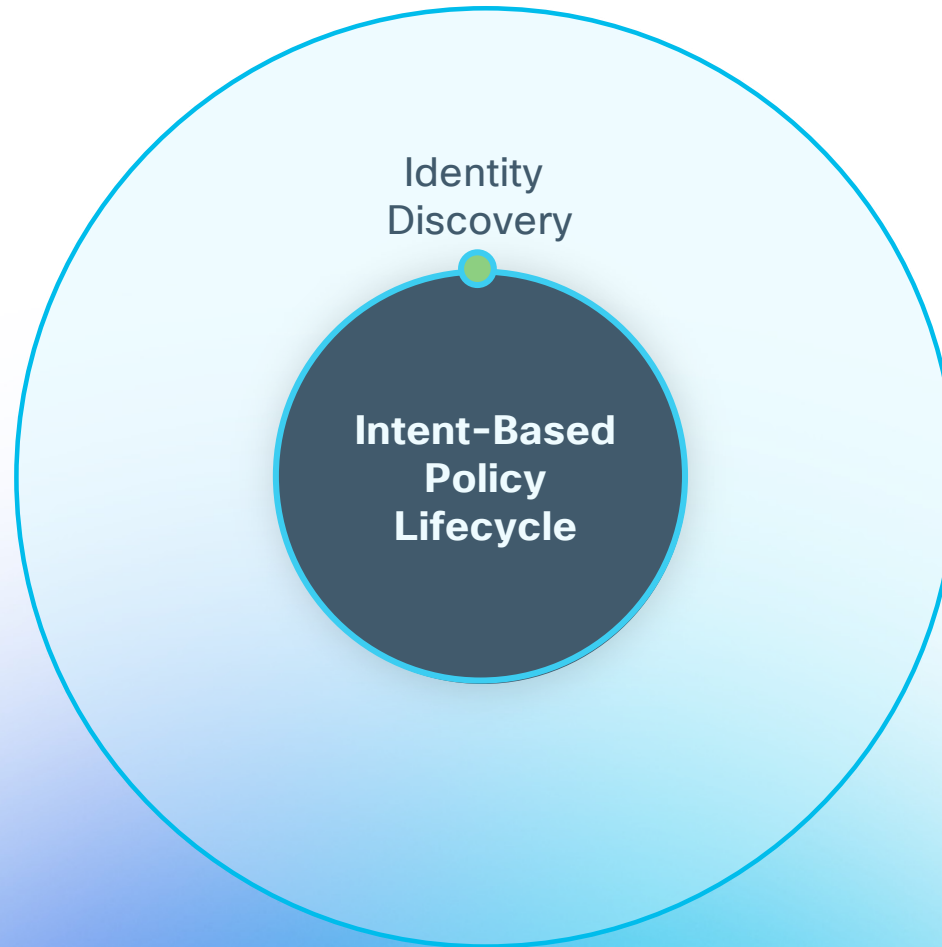
Single Policy, Distributed Enforcement (Overview)



Cisco Secure Firewall



Identity Discovery

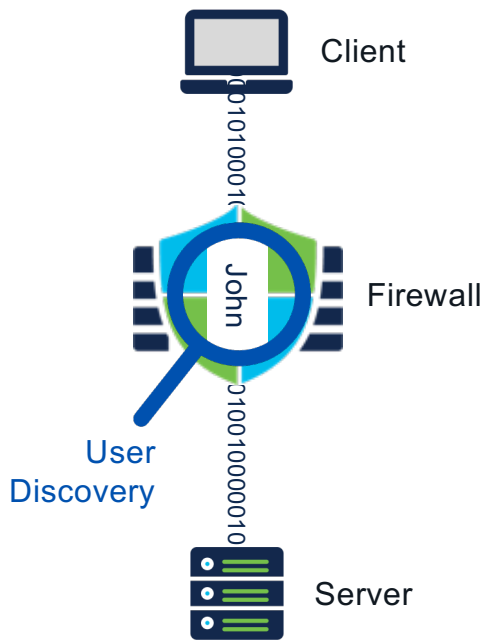


Network and Authentication-Based Discovery

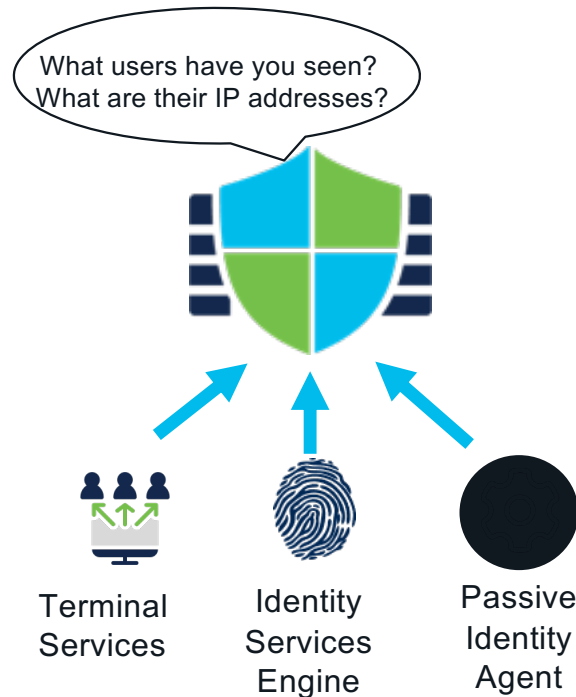
Identity Discovery

BRKSEC-2590

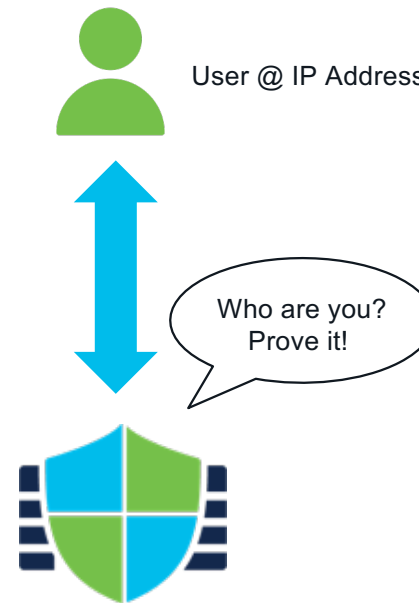
Network Discovery



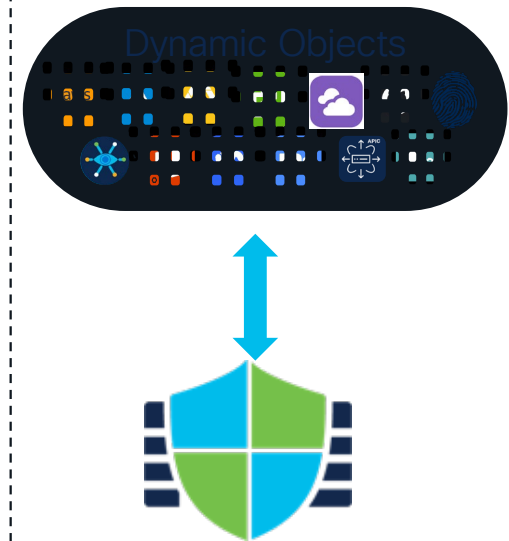
Passive Discovery



Active Discovery



External Integrations



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

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

User:	IP:	Port Range
Burns	192.168.1.1	2024-2223



Terminal Services



REST



Identity Services Engine

pxGrid

Management Center



User and Group check

User:	IP:
Smithers	10.1.1.4



Passive Identity Agent



AD DC

REST

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

Realms (Directories)

Passive Identity Agent



Send user-IP mappings

Cisco Passive Identity Agent 1.0.0-3

Secure Firewall Management Center

Enter the fully qualified domain name or IP address of the Secure Management Center this agent communicates with.

Integration

On-Prem Cloud

Primary FMC FQDN / IP address Port

172.16.134.97 : 443

FMC FQDN or IP address and Port of the FMC

Username Password

primaryagent

The credentials for the connection (Primary or Secondary)

Agent Primary_BRULAB_Agent

Agent	DCs (Domain Controllers)
Primary_BRULAB_Agent	windows2012.brulab.local

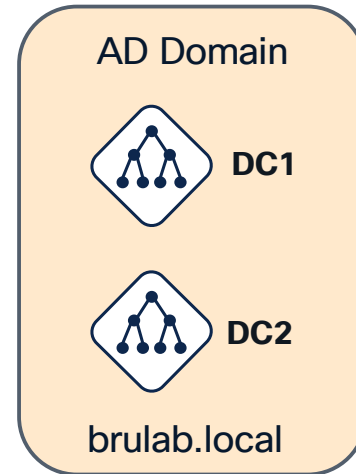
You need to select Agent-DCs pair to be able to save configuration

Tested successfully Primary FMC was tested successfully.

I have Secondary FMC

Save Cancel

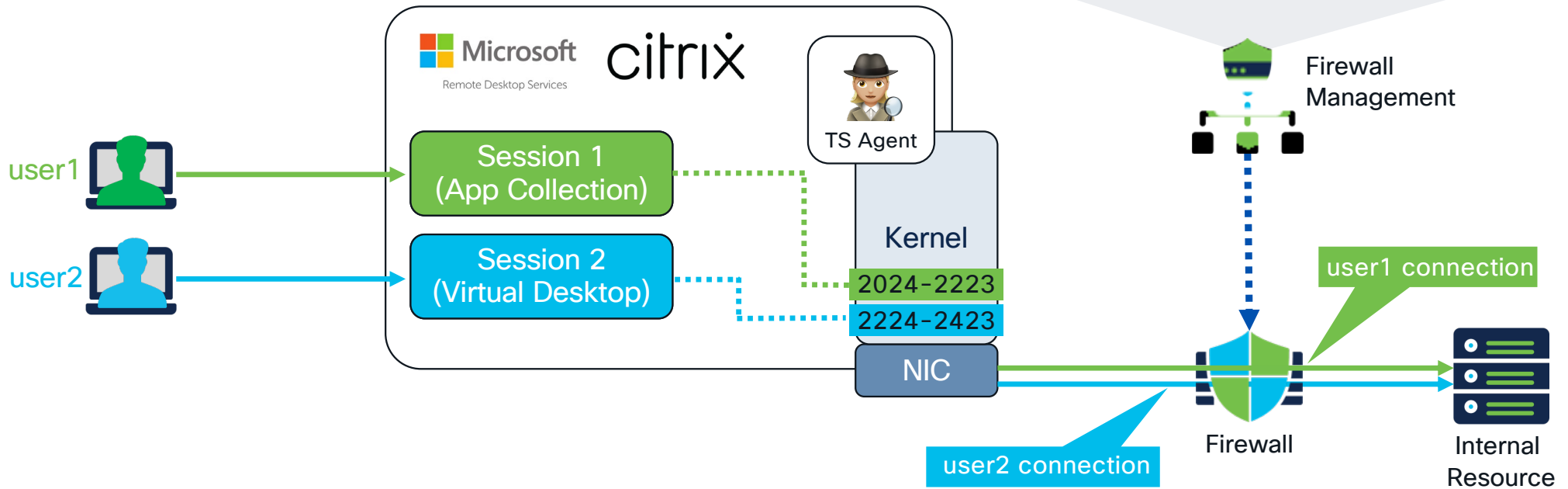
Read Event Log



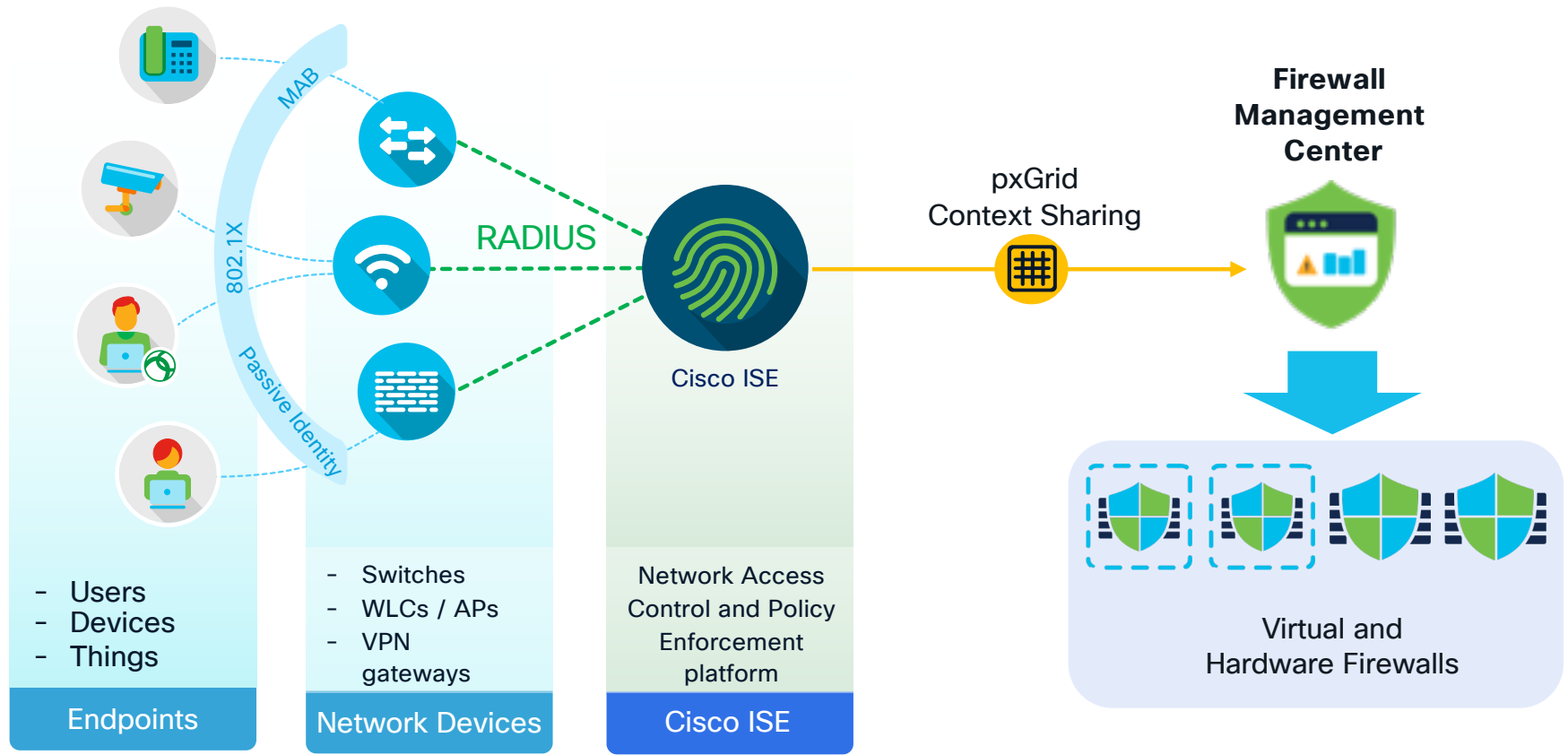
Terminal Services User Discovery

Identity Discovery

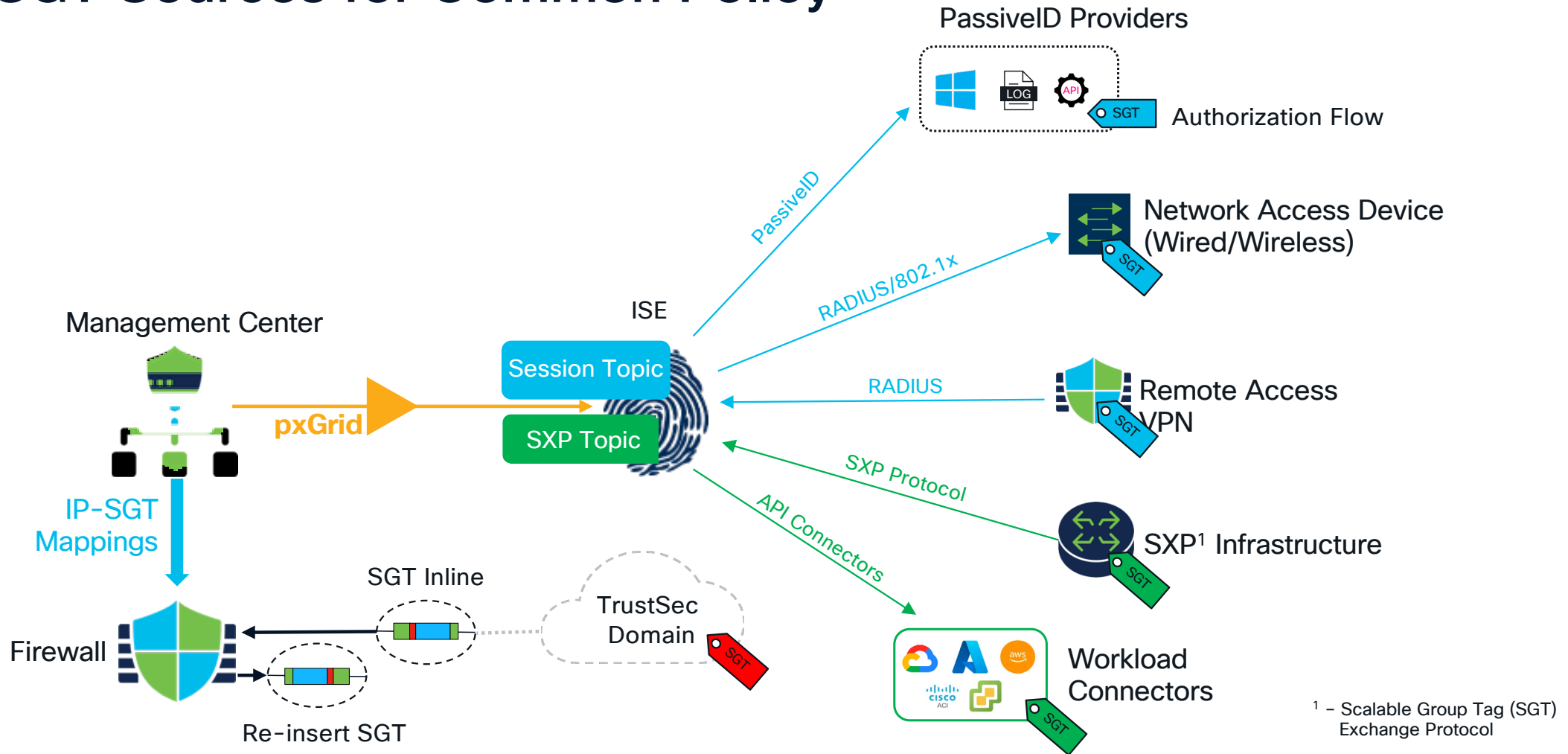
#	User	IP	Port Range
1	user1@acme.com	192.168.0.253	2024-2223
2	user2@acme.com	192.168.0.253	2224-2423



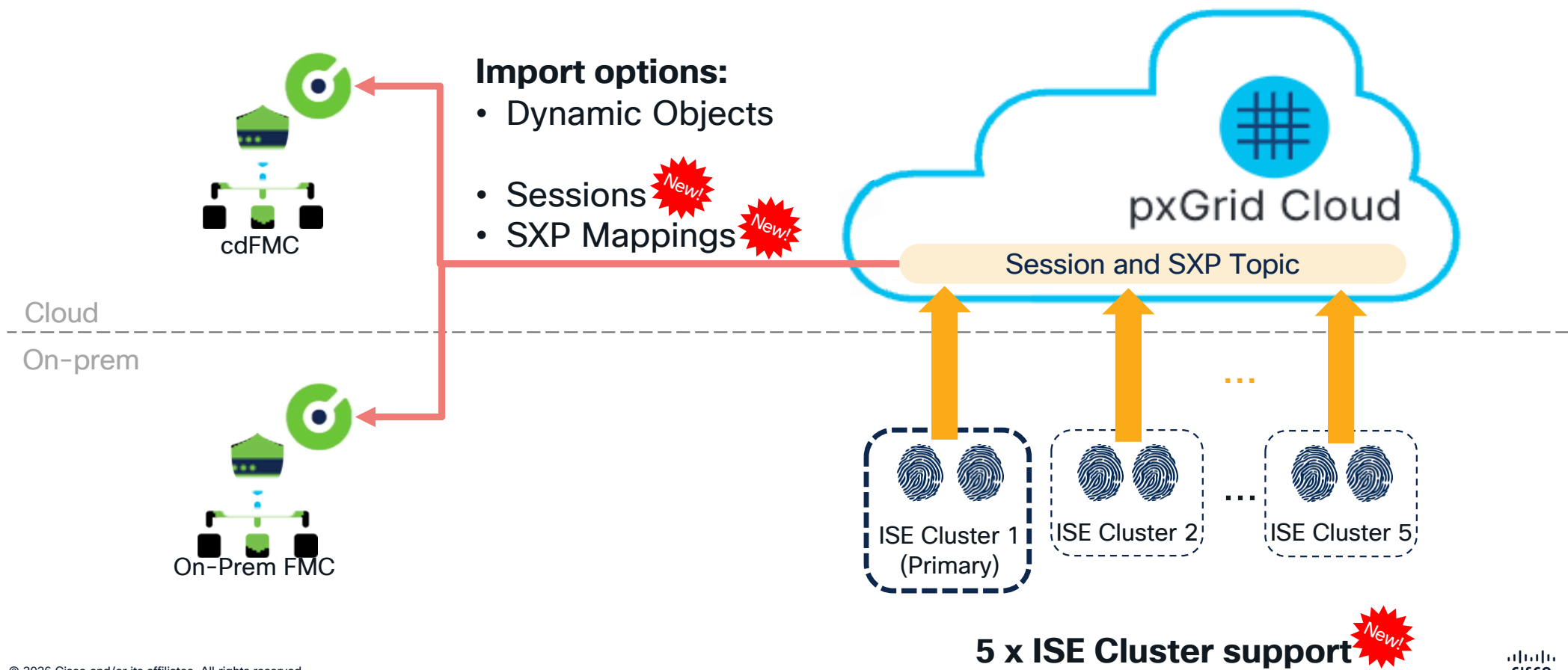
Identity Services Engine Integration



SGT Sources for Common Policy



Multiple ISE clusters and Session/SXP support



Cisco Identity Intelligence Integration



Dynamic Attributes Connector Enabled

Dashboard Connectors Dynamic Attributes Filters

Dynamic Firewall

1 Associate an identity source with an identity intelligence integration

In the left column, click the name of an identity source from which to retrieve authentication information.

In the right column, select the check box to associate the identity source with intelligence integration.

User identity feeds

- ISE pxGrid Cloud
Enable ISE pxGrid Cloud in [Identity Sources](#) to use it in the dynamic firewall.
- ISE pxGrid On-Prem
Use ISE pxGrid On-Prem as a source of user identity to set up dynamic firewall.
- Passive Identity Agent
Identity is not yet supported in dynamic firewall.
- Captive Portal
Identity is not yet supported in dynamic firewall.

Intelligence integration

- Cisco Identity Intelligence
Associate user and device risk assessment from Cisco Identity Intelligence with the selected identity source. If you want you can go to Cisco Identity Intelligence [Dashboard](#)

Enriched by

2 View system-defined filters

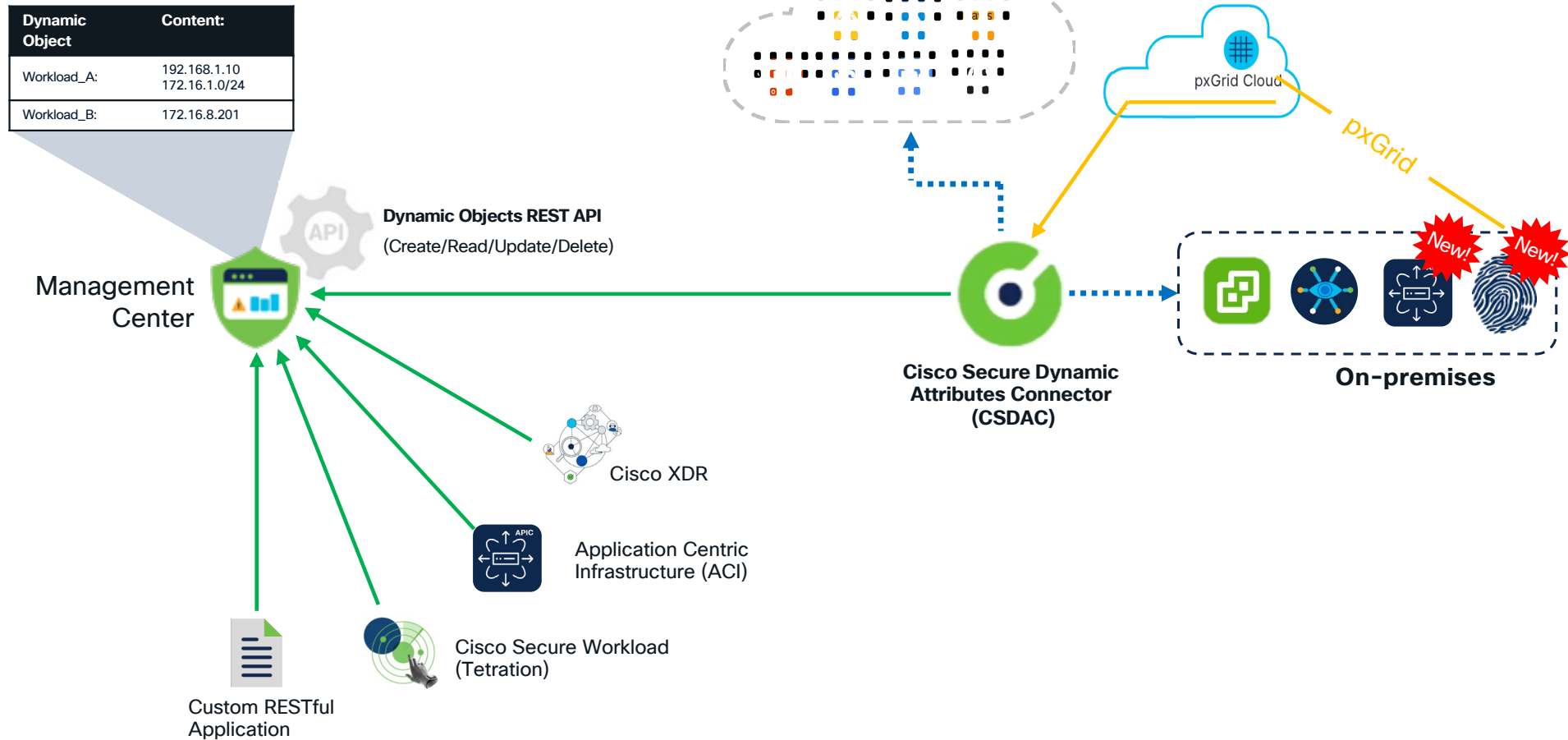
3 View system-defined access control policy rules

Firewall policy learns IP addresses of:

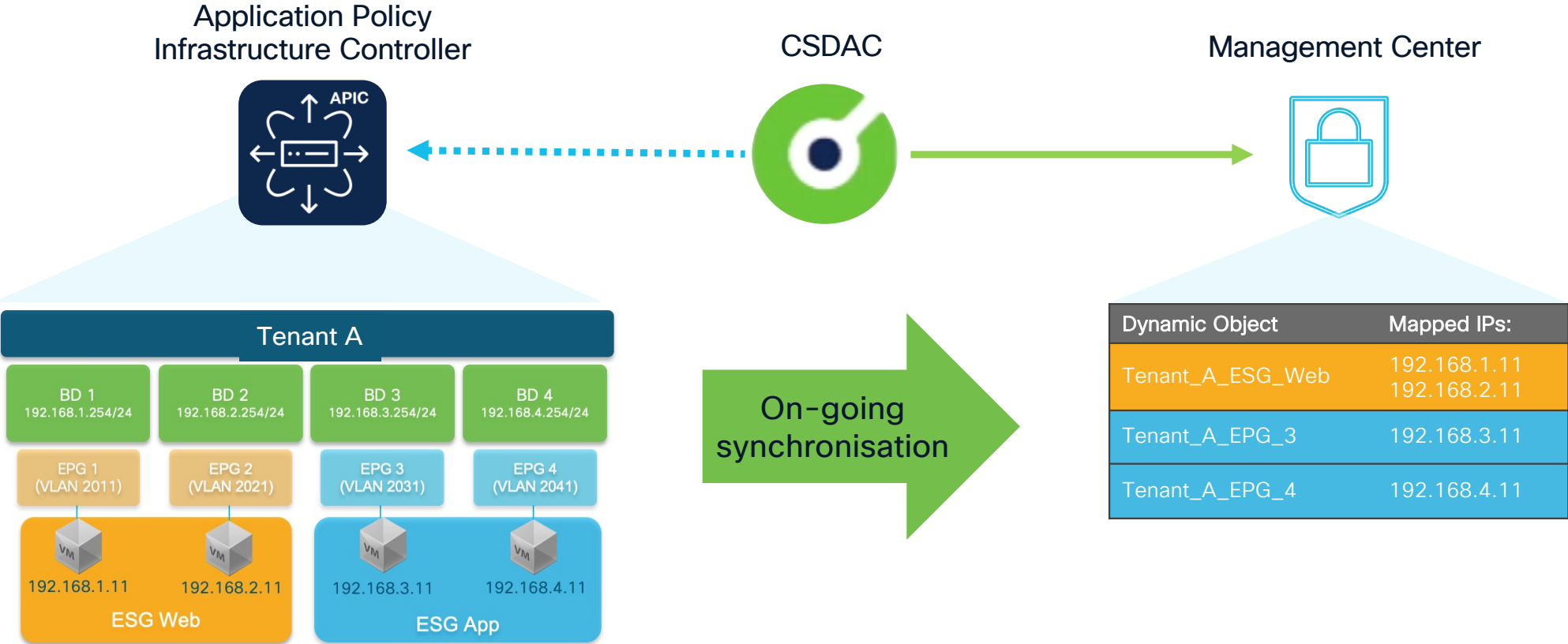
- ISE postured/non-compliant devices
- CII Untrusted and Questionable

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'

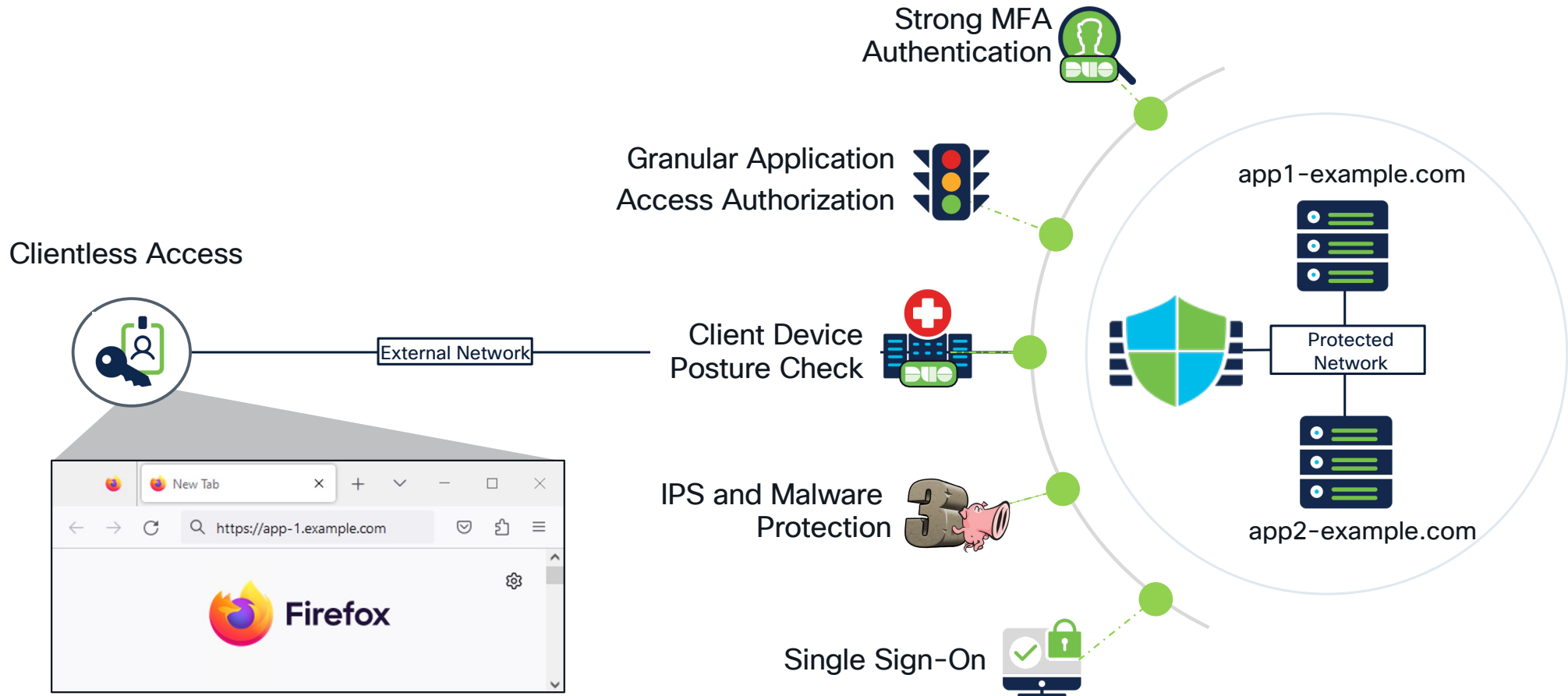
Dynamic Objects: adapting to a dynamic world



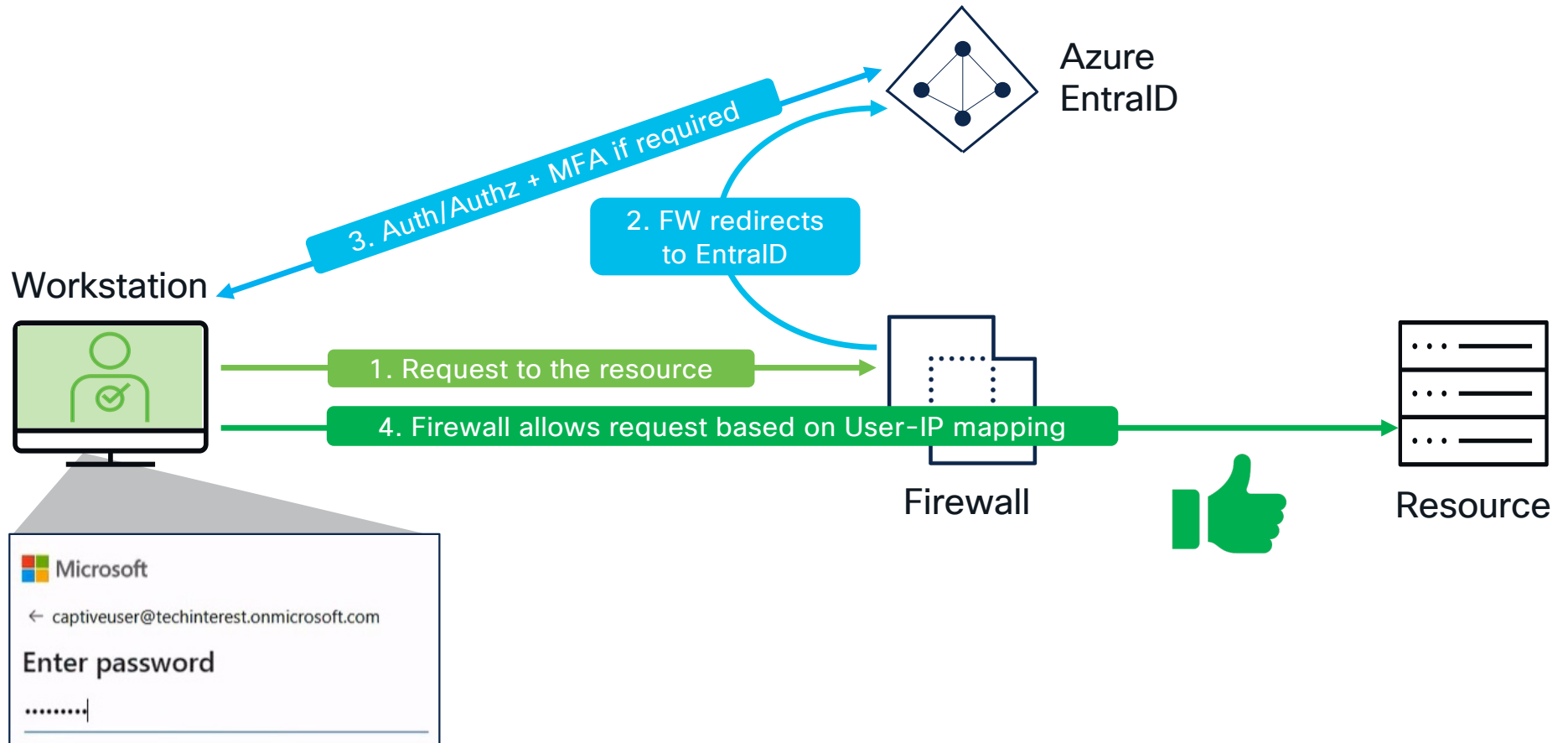
ACI Integration



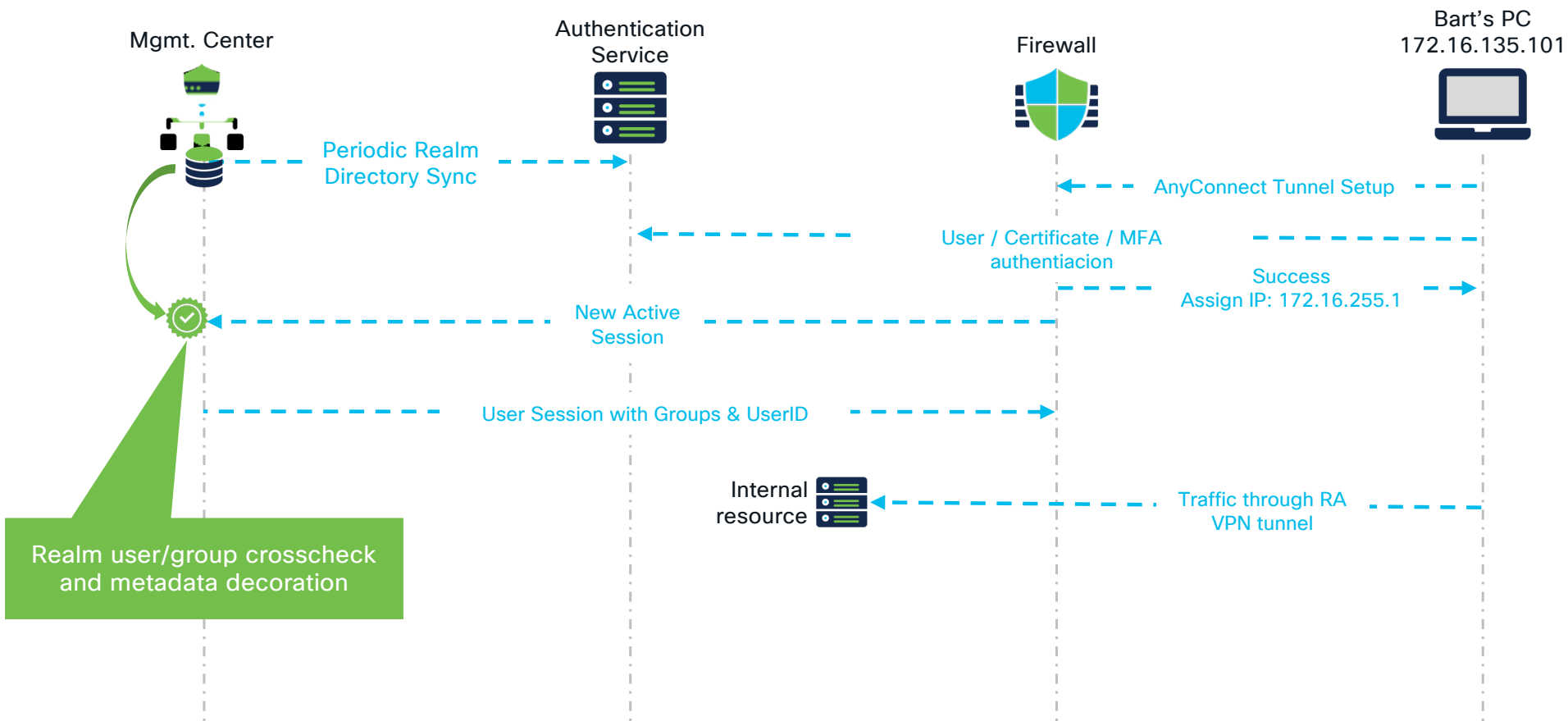
Zero Trust Network Access – User Discovery



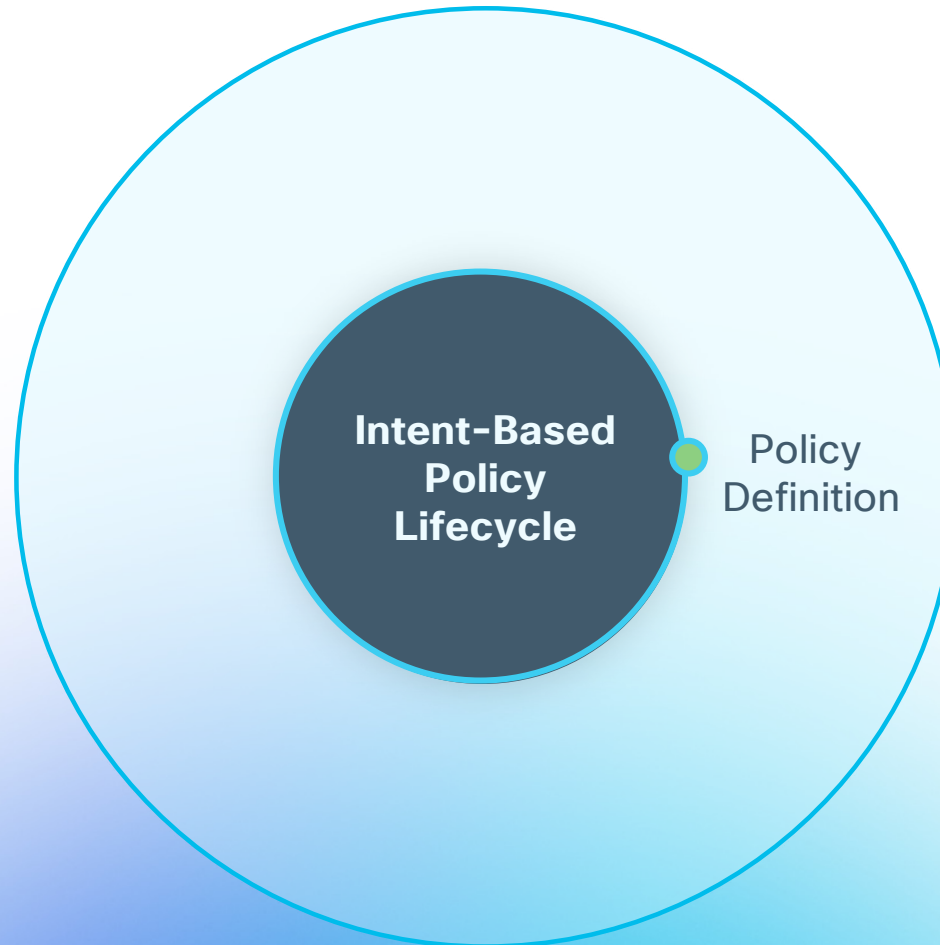
Captive Portal with EntraID



Remote Access VPN User Discovery (Active Discovery)



Policy Definition



Access Control Policy (ACP)

- **Access Control Associated Policies**
 - **Prefilter:** Fast forward or Fast Drop packets 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

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More Targeted: 1 device

Type to search

	Name	Action	Source					
			Zones	Networks	Ports	Dynamic Attributes	Zones	
<input type="checkbox"/> Mandatory 5 rules (1 - 5)								
<input type="checkbox"/> 1	Mgmt-Prod-Overlay	→ Allow	Any	Mgmt-Prod-Ove...	Any	Any	Any	
<input type="checkbox"/> 2	DC-OUT	→ Allow	Campus-Cor... +8 more	Any	Any	Any	DC-Core-to-...	
<input type="checkbox"/> 3	DC-IN	→ Allow	DC-Core-to-...	Any	Any	Any	Campus-Cor... +9 more	
<input type="checkbox"/> 4	Inside-DC	→ Allow	Campus-Cor... +8 more	Any	Any	Any	Campus-Cor... +8 more	
<input type="checkbox"/> 5	VESX-Ingress-Rule	→ Allow	DC-Core-to-...	any	Any	Any	DC-Core-Pro...	
<input type="checkbox"/> Default 1 rule (6 - 6)								
<input type="checkbox"/> 6	DHCP	→ Allow	Any	tme-csw-dhcp-1	Any	Any	Any	

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

Name: Test Rule | Action: Allow | Logging: ON | Time Range: None | Rule Enabled: ON

Intrusion Policy: IPS Policy -... | Default-Set: | File Policy: Malware Po...

Search Security Zone Objects | Total 28 | Selected Sources: 4 | Selected Destinations and Applications: 5

Zones (1) | Networks (1) | Ports (1) | Applications (1) | Users (1) | URLs (1) | Dynamic Attributes (2) | VLAN Tags (1)

Zone Name	Type
AWS-Inspection-In-NS	Routed Security Zone
AWS-Inspection-Out-NS	Routed Security Zone
AWS-VNI-Inspection-NS	Routed Security Zone
Azure-In	Routed Security Zone
Campus-Core-Interconnect	Routed Security Zone
Contractors-Core-Interconnect	Routed Security Zone
DC-Core-Management	Routed Security Zone
DC-Core-Monitoring	Routed Security Zone
DC-Core-Non-Prod-Zone	Routed Security Zone
DC-Core-Pod-1	Routed Security Zone

Selected Source: DC-Core-Management

Object Type	Object Name
ZONE	1 Object: DC-Core-Management
USER	insbu.lab/jorgquin
DYN	SGT
VLAN	employee_network

Selected Destinations and Applications:

Object Type	Object Name
NET	192.168.1.0-24
PORT	> 1 Object
APP	AD DRS
URL	> 1 Object
DYN	csw-fmc-csw-acme-users

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.

Name:

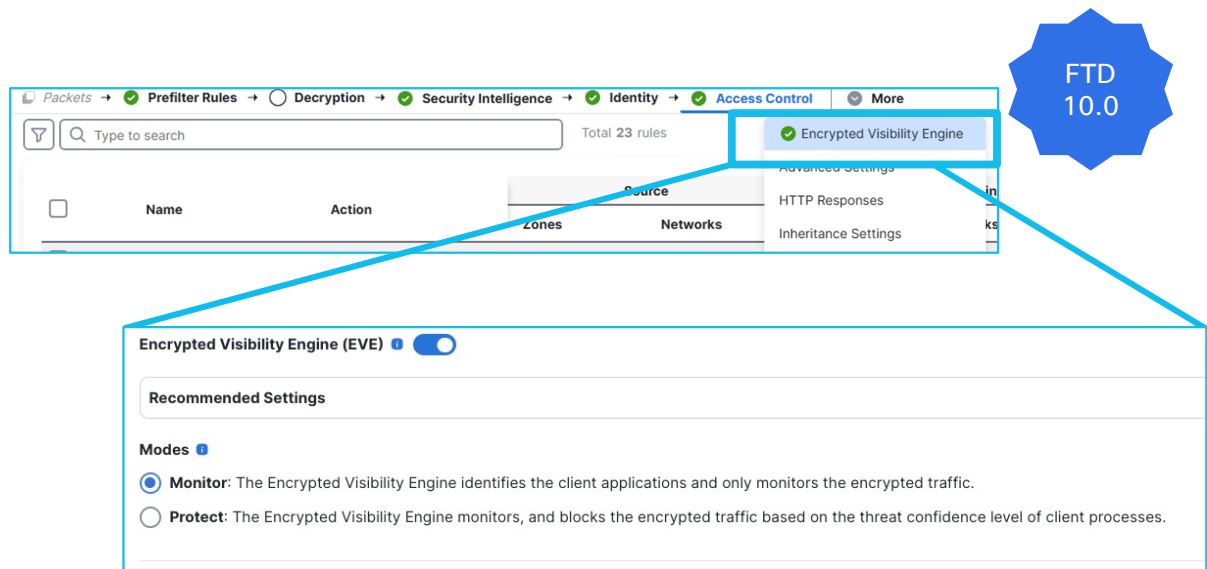
Action: Logging: ON Time Range: Rule Enabled:

Intrusion Policy: Default-Set: File Policy:

Search Security Zone Objects	Total 28	Selected Sources: 4	Selected Destinations and Applications: 5
<input type="checkbox"/> AWS-Inspection-In-NS (Routed Security Zone)		Collapse All Remove All	Collapse All Remove All
<input type="checkbox"/> AWS-Inspection-Out-NS (Routed Security Zone)		ZONE 1 Object DC-Core-Management	NET 1 Object 192.168.1.0-24
<input type="checkbox"/> AWS-VNI-Inspection-NS (Routed Security Zone)		USER 1 Object insbu.lab/jorgquin	PORT 1 Object
<input type="checkbox"/> Azure-In (Routed Security Zone)		DYN 1 Object SGT	APP 1 Object AD DRS
<input type="checkbox"/> Campus-Core-Interconnect (Routed Security Zone)		VLAN 1 Object employee_network	URL 1 Object
<input checked="" type="checkbox"/> DC-Core-Management (Routed Security Zone)			DYN 1 Object csw-fmc-csw-acme-users
<input type="checkbox"/> DC-Core-Monitoring (Routed Security Zone)			
<input type="checkbox"/> DC-Core-Non-Prod-Zone (Routed Security Zone)			
<input type="checkbox"/> DC-Core-Pod-1 (Routed Security Zone)			

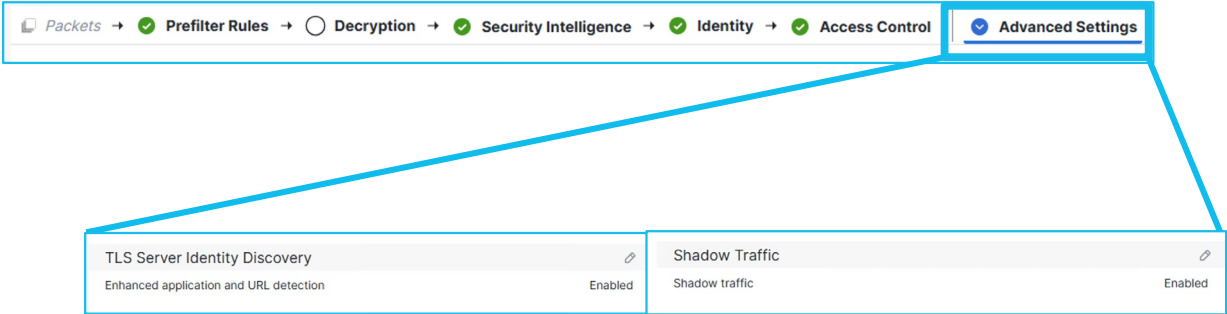
Encrypted Visibility Engine

- 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



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



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.sr33qfglszbztrvrgyt3b...

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

DNS Protection
DNS Protection blocks traffic from known threats by the domain name. Intelligence for these threats is derived from both TALOS and Cisco Umbrella.

DNS Policy Umbrella DNS Policy

Default DNS Policy → None

Network and URL Block List

Available Objects (92)

Networks URLs

Banking_fraud
Bogon
Bots
CnC
Cryptomining
Dga

Available Zones

Any
AWS-Inspection-In-NS
AWS-Inspection-Out-NS
AWS-VNI-Inspection-NS
Azure-In
Campus-Core-Interconnect
Contractors-Core-Interconnect

Do-Not-Block List(2)

Networks

Global Do-Not-Block List (Any Zone)

URLs

Global Do-Not-Block List for URL (...

Block List(46)

Networks

Attackers (Any Zone)

Banking_fraud (Any Zone)

Bogon (Any Zone)

Bots (Any Zone)

CnC (Any Zone)

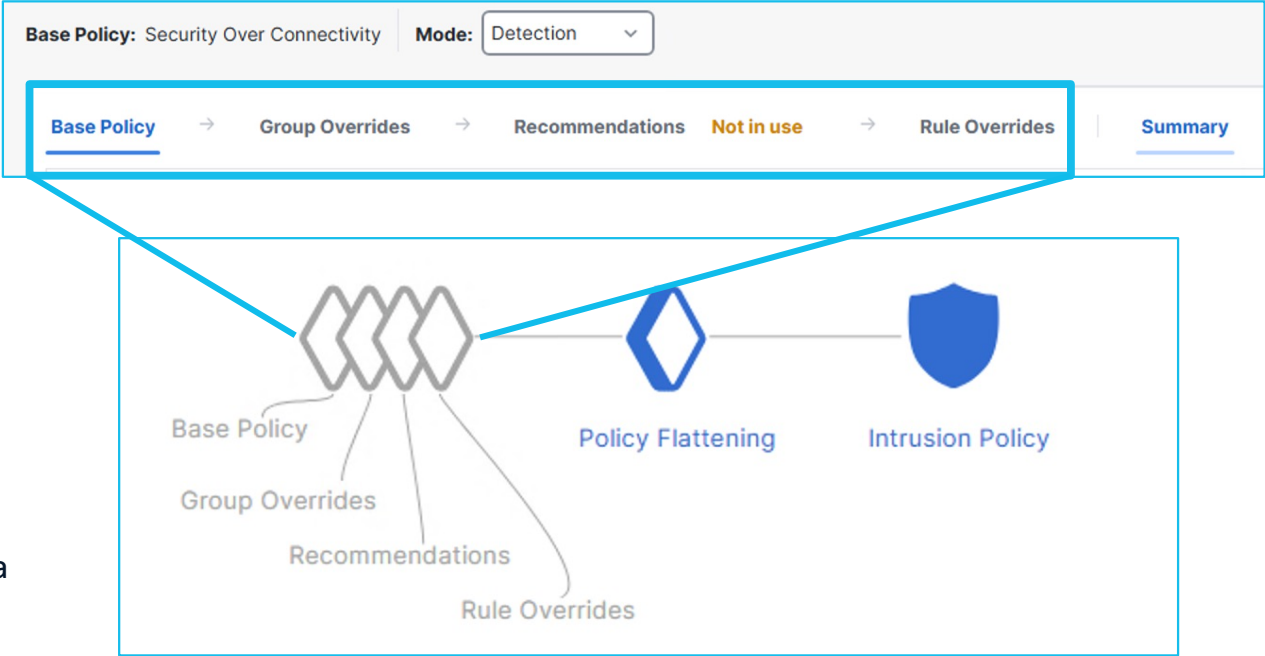
Cryptomining (Any Zone)

|< < Viewing 1-100 of 220 > >|

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-conscious action, unless there is a manual rule override



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)

SnortML matches

Time	Event Type	Action	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Intrusion Message	Other Enrichment
> 2024-08-01 03:55:45	Intrusion	Block	10.0.104.100	10.0.105.100	16458 / tcp	4430 / tcp	(snort_ml) potential threat found in HTTP parameters via Neural Net...	Rule Categories: Protocol: Builtins
> 2024-08-01 03:55:38	Intrusion	Block	10.0.104.100	10.0.105.100	16259 / tcp	4430 / tcp	(snort_ml) potential threat found in HTTP parameters via Neural Net...	Rule Categories: Protocol: Builtins



SnortML rule

URL metadata

Snort ID 411:1:1
Snort Version 3

```
Snort Rule
alert ( gid:411; sid:1; rev:1; msg:"(snort_ml)
potential threat found in HTTP parameters via Neural
Network Based Exploit Detection"; metadata: policy
max-detect-ips alert, rule-type preproc;
classtype:unknown;)
```

```
File
URL /admin/user/action/index.php?
n=guest&c=0&m=search&s=fo
rum&wert=-1%25%22%20U...
```

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

Rules Advanced

+ Add Rule

File Types	Application Protocol	Direction	Action
Category: Executables BINARY_DATA	FTP	Download	Block Files with Reset
Category: Executables	HTTP	Upload	Detect Files
Category: PDF files Category: Executables Category: Office Documents PDF	SMTP	Upload	Block Malware with Reset Spero Analysis Dynamic Analysis Capacity Handling Local Malware Analysis Store files of disposition: Unknown
Category: PDF files	POP3	Download	Malware Cloud Lookup Dynamic Analysis Capacity Handling Local Malware Analysis Store files of disposition: Unknown

Add Rule

Application Protocol: Any

Action: Detect Files Store files

Direction of Transfer: Any

File Type Categories: File Types

- Office Documents: 25
- Archive: 20
- Multimedia: 37
- Executables: 14
- PDF files: 2
- Encoded: 2
- Graphics: 6

Search name and description

- 7Z (7-Zip compressed file)
- 9XHIVE (Windows 9x registr...
- ACCDB (Microsoft Access 2...
- AIF (Audio Interchange File ...)
- ALZ (Archive file for Microso...

Selected File Categories and Types

Add

Cancel Save

File Dispositions

- ← File Reputation Service
- ← File Analysis

Malicious file is automatically marked in Advanced Malware Protection (AMP) database

Information stored in AMP (Advanced Malware Protection):

- Hashes
- Device GUID



Information stored in Secure Malware Analytics

- Files and Device GUID
- Analysis Results and Reports

2 File Reputation (includes 1-1 SHA256, Spero)

3 Disposition (clean, malicious, or unknown)

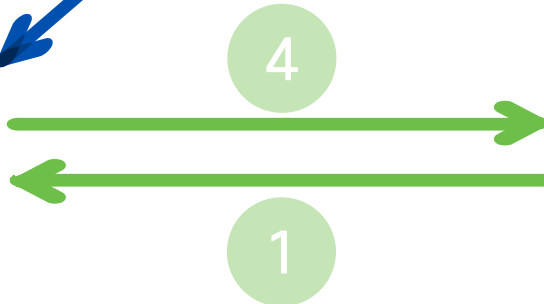
6 Analysis Report (Indicators, threat score)

5 Analysis Request (Includes the file)

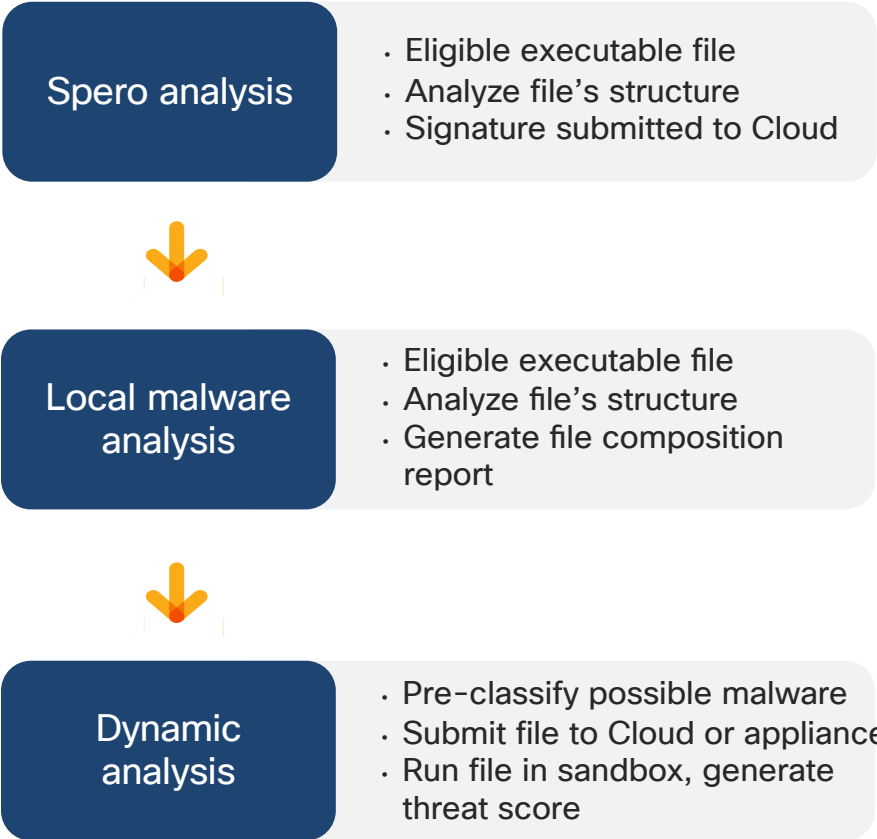
Retrospection via PING2



Threat Defense Sensor

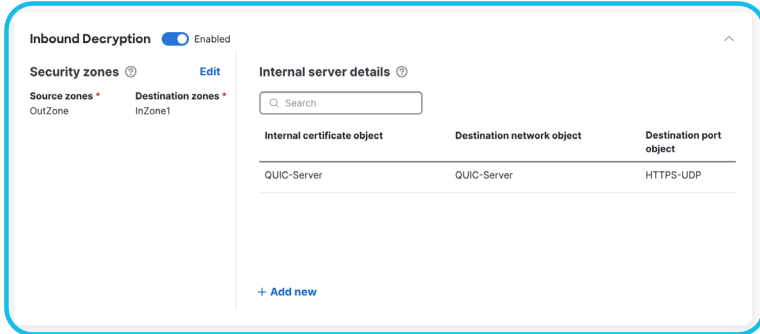


Analysis Type



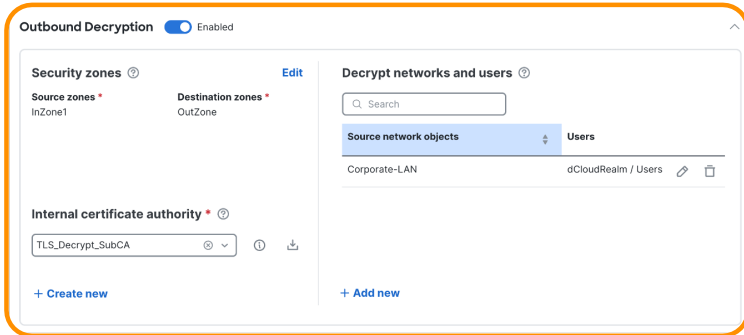
Policy Definition – Decryption Associated Policy

Step 1: Specify your servers for decryption



The screenshot shows the 'Inbound Decryption' configuration page. It includes a toggle for 'Inbound Decryption' which is 'Enabled'. Under 'Security zones', there are 'Source zones' (OutZone) and 'Destination zones' (InZone1). The 'Internal server details' section has a search bar and a table with columns: 'Internal certificate object', 'Destination network object', and 'Destination port object'. The table contains one entry: 'QUIC-Server', 'QUIC-Server', and 'HTTPS-UDP'. There is an '+ Add new' button at the bottom.

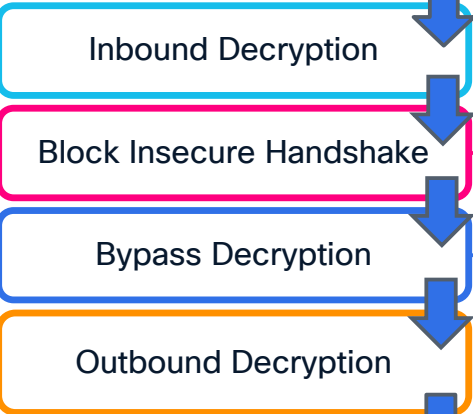
Step 2: Set protected networks and users



The screenshot shows the 'Outbound Decryption' configuration page. It includes a toggle for 'Outbound Decryption' which is 'Enabled'. Under 'Security zones', there are 'Source zones' (InZone1) and 'Destination zones' (OutZone). The 'Decrypt networks and users' section has a search bar and two tabs: 'Source network objects' and 'Users'. The 'Users' tab is active, showing a table with columns for 'Source network objects' and 'Users'. One entry is visible: 'Corporate-LAN' and 'dCloudRealm / Users'. There is an '+ Add new' button at the bottom.

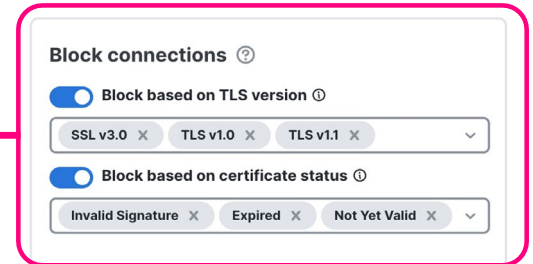


Automatic ordering



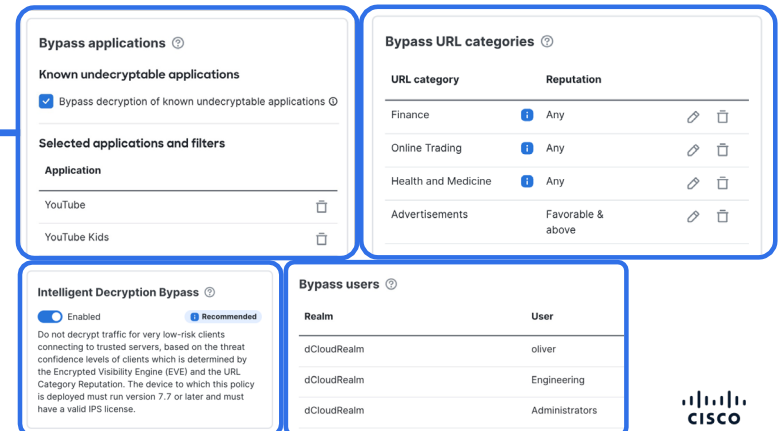
TLS Handshake

Step 4: Block weak ciphers and bad certificates



The screenshot shows the 'Block connections' configuration page. It includes a toggle for 'Block based on TLS version' which is 'Enabled'. Below it are three buttons: 'SSL v3.0', 'TLS v1.0', and 'TLS v1.1'. There is a dropdown menu. Below that is a toggle for 'Block based on certificate status' which is 'Enabled'. Below it are three buttons: 'Invalid Signature', 'Expired', and 'Not Yet Valid'. There is a dropdown menu.

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



This block contains four sub-screenshots:

- Bypass applications:** Shows 'Known undecryptable applications' with a checked box for 'Bypass decryption of known undecryptable applications'. Under 'Selected applications and filters', there is a table with columns 'Application' and 'Bypass'. Applications listed include YouTube and YouTube Kids.
- Bypass URL categories:** Shows a table with columns 'URL category' and 'Reputation'. Categories include Finance, Online Trading, Health and Medicine, and Advertisements.
- Intelligent Decryption Bypass:** Shows a toggle for 'Intelligent Decryption Bypass' which is 'Enabled'. A note below states: 'Do not decrypt traffic for very low-risk clients connecting to trusted servers, based on the threat confidence levels of clients which is determined by the Encrypted Visibility Engine (EVE) and the URL Category Reputation. The device to which this policy is deployed must run version 7.7 or later and must have a valid IPS license.'
- Bypass users:** Shows a table with columns 'Realm' and 'User'. Users listed include oliver, Engineering, and Administrators.

New Simplified Workflow



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**

Inbound Decryption (Enabled)

Outbound Decryption (Enabled)

Intelligent Decryption Bypass (Enabled, Recommended)

Bypass applications

Bypass URL categories

Block connections

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, Legally Prohibited (URL Categories, Application Groups, DN Lists)	
Key Resign – Outbound Client Protection (URL Categories, Application Groups)	
Default Do Not Decrypt	



Intelligent/Selective Decryption – Client Threat Column

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

Name: EVE Selective Decryption Enabled

Action: Do not decrypt

Zones Networks VLAN Tags Users **Client Threat** Applications Ports Category Certificate DN Cert Status

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

Client Threat (identified by the Encrypted Visibility Engine)

- Any
- Very Low
- Low**
- Medium
- High
- Very High

Selected client process risk: Very Low - Low

[Add to Rule](#)

Intelligent Decryption Bypass ?

Enabled **i** Recommended

Do not decrypt traffic for very low-risk clients connecting to trusted servers, based on the threat confidence levels of clients which is determined by the Encrypted Visibility Engine (EVE) and the URL Category Reputation. The device to which this policy is deployed must run version 7.7 or later and must have a valid IPS license.

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

Applies to 7.2.0 and later
 Enable TLS 1.3 Decryption

Applies to 7.3.0 and later
 Enable adaptive TLS server identity probe

Applies to 7.6.0 and later
 QUIC Decryption

Advanced options are available only with Snort 3

[Revert to Defaults](#)

Internal server details ⓘ

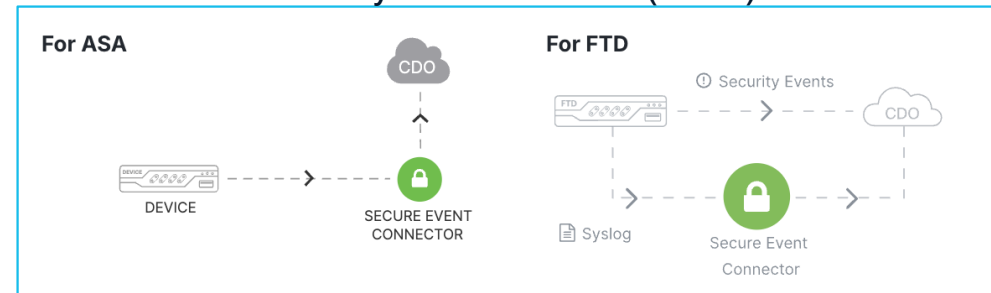
🔍 Search

Internal certificate object	Destination network object	Destination port object		
wildcard-example.com	Piggy-Server	HTTPS		
wildcard-example.com	File-Server	QUIC		
wildcard-example.com	App-Server	any		

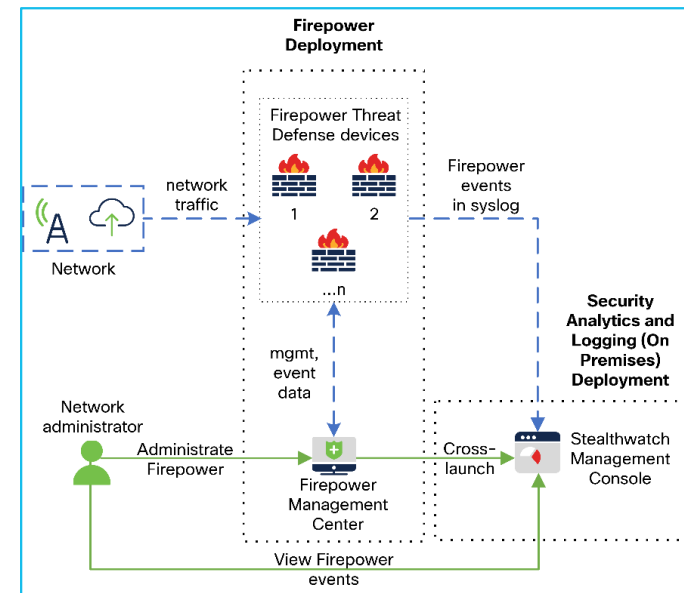
Security Analytics and Logging (SAL)

- 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



Splunk Integration

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

Splunk Integration
This integration simplifies the process of sending event data to Splunk. See [Splunk integration](#).

Monitor

- Insights & Reports >
- Events & Logs >

Manage

- Policies >
- Objects >
- Firewall Devices >
- Secure Connections >
- Integrations >**
- Troubleshooting >
- Administration >

Firewall Threat Defense | Firewall Management Center → Syslog → splunk>

Set up syslog configuration for Splunk with only a few steps. [Create Splunk profile](#)

Profile name	Host object or IP address	Protocol	Port	Event types	Source selection	
Splunk_1759935938731	Splunkinside	UDP	514	4 event types	Management	edit delete

ATT&CK is Like a Periodic Table

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

The image shows a screenshot of the MITRE ATT&CK framework table. The table is organized into columns representing different stages of an attack, such as Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Each column contains a list of specific techniques, often with a small icon and a reference number. The table is presented in a grid-like format, similar to a periodic table of elements.

The image shows a standard periodic table of elements. The table is organized into rows and columns, with elements grouped by their chemical properties. The elements are color-coded into groups such as Alkali Metal, Alkaline Earth, Transition Metal, Semimetal, Nonmetal, Basic Metal, Halogen, Noble Gas, Lanthanide, and Actinide. The table includes the element symbol, atomic number, and name for each element.

- 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

Unlock insights from the network

Firewall Logs at no additional cost in Splunk*

Comprehensive
TDIR



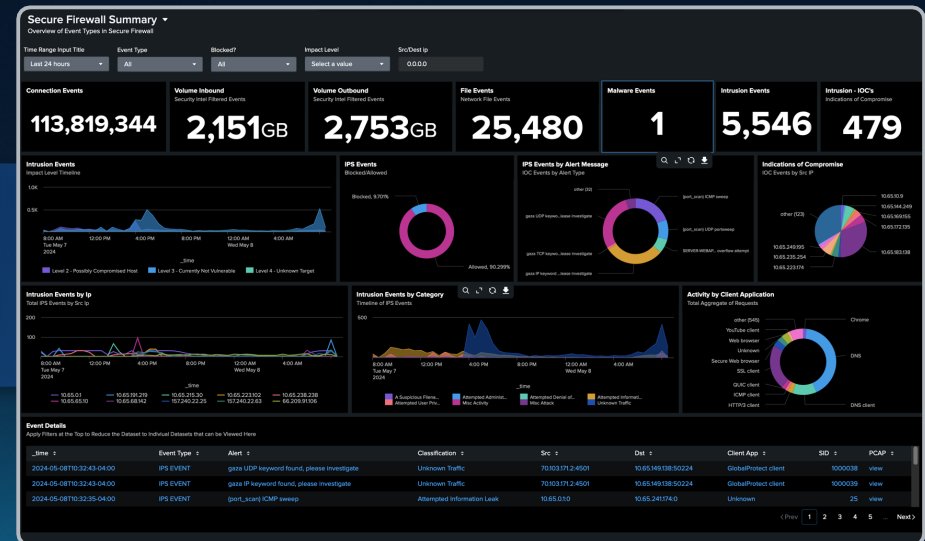
Unleash
Network Insights



Bridging
SecOps + NetOps



New detections | Automated response



Cisco AI Assistant for Security now on FMC

Assist

Policy and reporting

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

Augment

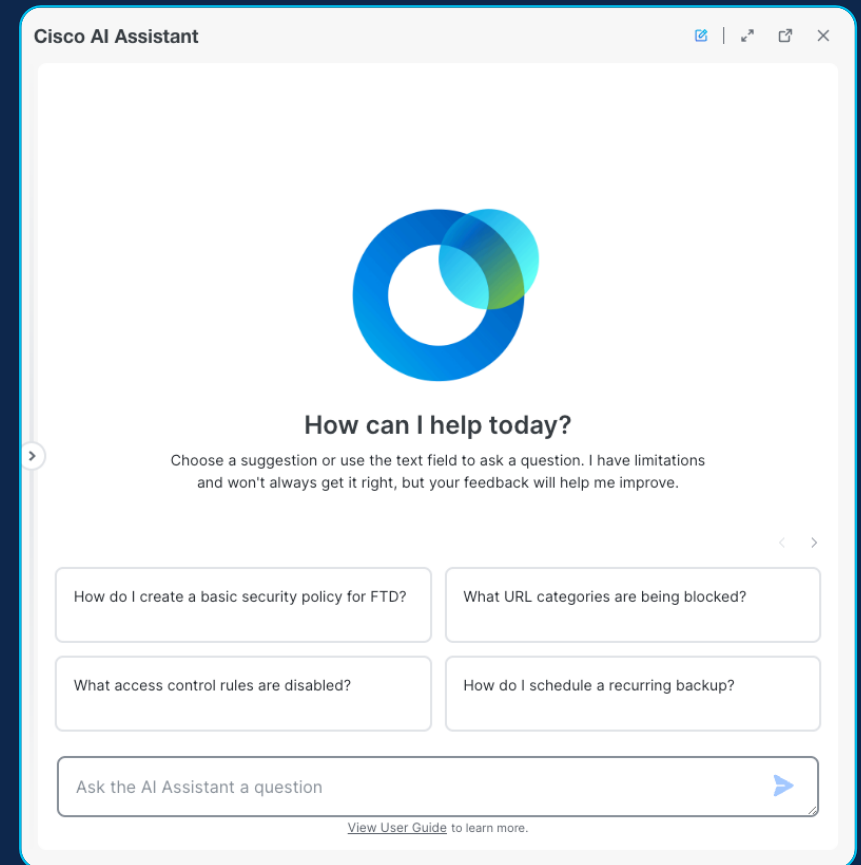
Troubleshooting and detection

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

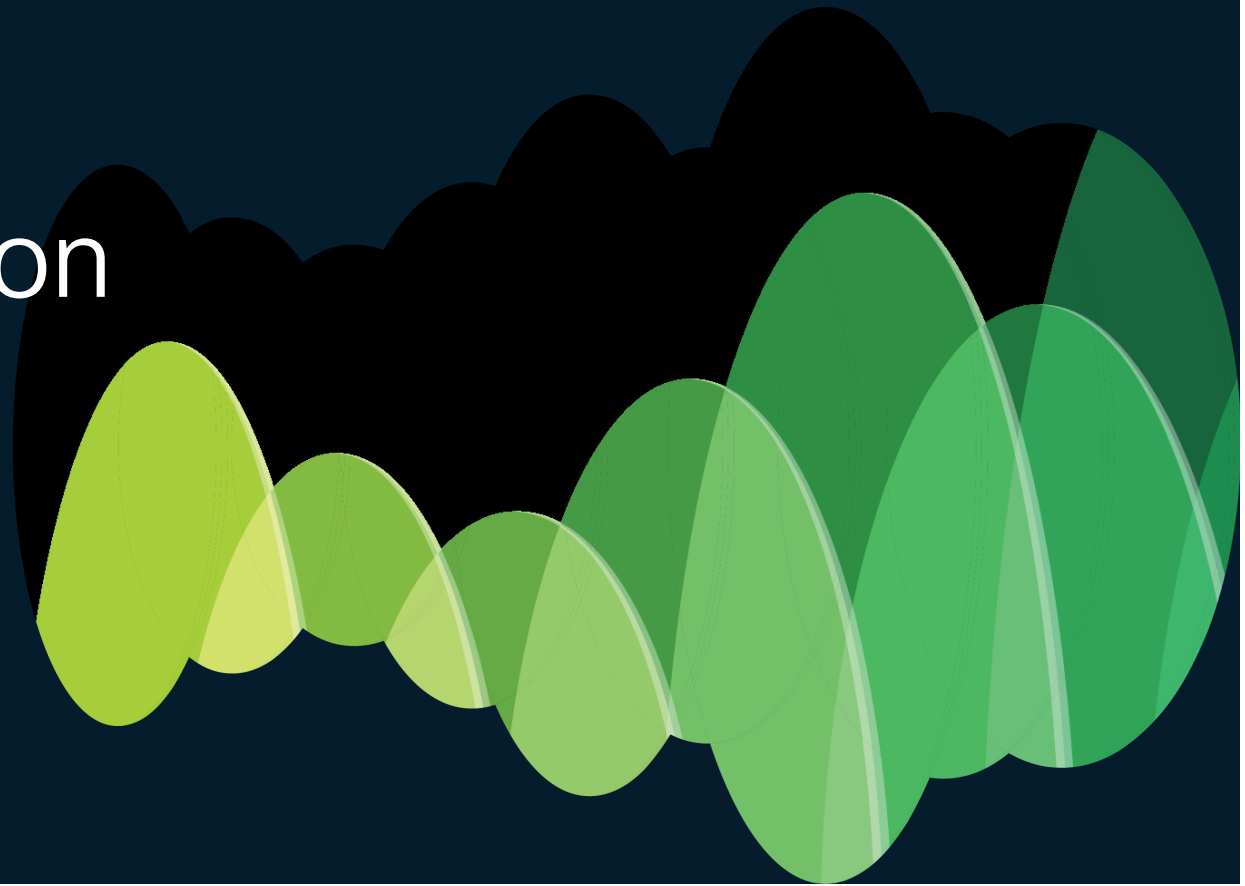
Encrypted traffic

- 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



Multicloud Defense

Finalist



Duo

Best 2FA App

Secure Access

Customer Value Leader

Email Security

Growth Leader -Email Radar 2024

NetSec OPEN

Firewall

Best Security Performance
& Effectiveness



Magic Quadrant

Endpoint

Named a Visionary

Secure Access

Honorable Mention



Duo

Best Robust Security Features



Email Security

Recognized as
Marketing
champion



Secure Firewall

Cybersecurity
Excellence Award

Secure Firewall

2024 Best
Next Gen
Firewall



Duo

Best in KLAS:
Software &
Services

Secure Access

Leader in DNS



Secure Firewall

Global InfoSec
Award



XDR

Honorable Mention

Duo

Passwordless



Duo

Authentication
Winner



Secure Access

Best SME
Security Solution
for Umbrella

Third-Party Security Reference Evaluations

FORRESTER WAVE LEADER 2024

Secure Firewall
Leader in enterprise Firewall

FORRESTER WAVE LEADER 2024
Enterprise Firewall Solutions

FORRESTER WAVE LEADER 2024
Microsegmentation Solutions

Secure Workload
Leader in Micro-segmentation

Secure Firewall
Cybersecurity Excellence Award

2024 WINNER

CYBER SECURITY
EXCELLENCE AWARDS

Secure Firewall
Global InfoSec Award

GLOBAL INFOSEC AWARDS WINNERS
CYBER DEFENSE MAGAZINE
2024

NetSec OPEN

 University of New Hampshire InterOperability Laboratory

Secure Firewall
Best Price Performance

Secure Firewall
2023, 2024, 2025 Best Next Gen Firewall

Advanced Security Test Award
The following product wins the SE Labs award:

SE LABS
AAA
FEBRUARY 2025
Advanced Security NDR Protection
Cisco
Secure Firewall 4225

Multi-cloud Defense
Finalist

2022
FORTRESS
CYBER SECURITY
AWARD



Thank you