

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





SSE, XDR, ZTNA, SD-WAN

How NGFW continues to play a pivotal role

Anshul Kaushik, Technical Solutions Architect, Distinguished Speaker
Dinesh Moudgil, Technical Marketing Leader, Distinguished Speaker
BRKSEC-2706

Your Speaker

Anshul Kaushik

- ankaushi@cisco.com
- CCIE Security #23790
- 21 Years in Industry, 19 with Cisco
- TAC – Presales – Channels
- Drive end to end Security Enablement
- Lives in Melbourne and like outdoors

cisco *Live!*



Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

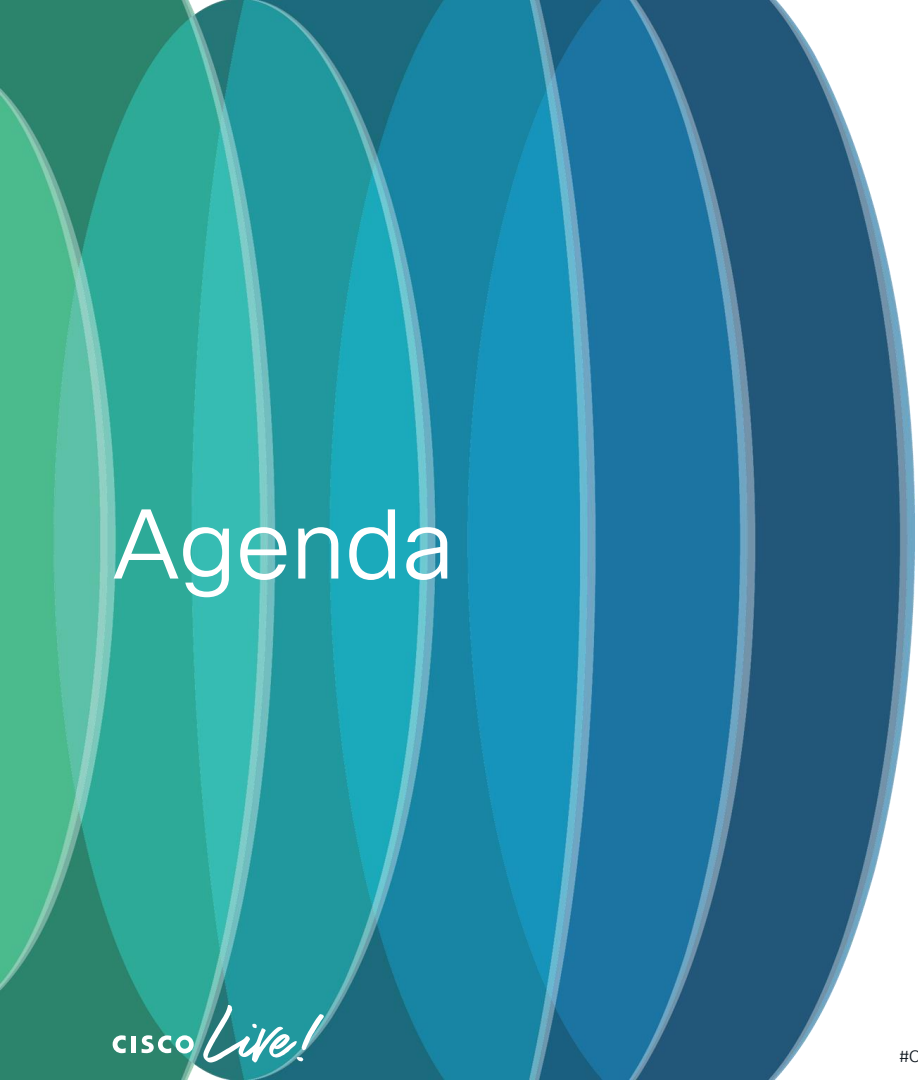
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2706>





Agenda

- Customer Challenges
- Cisco Security Overview
- Addressing Challenges via
 - XDR
 - SSE
 - ZTNA
 - SD-WAN
- Conclusion

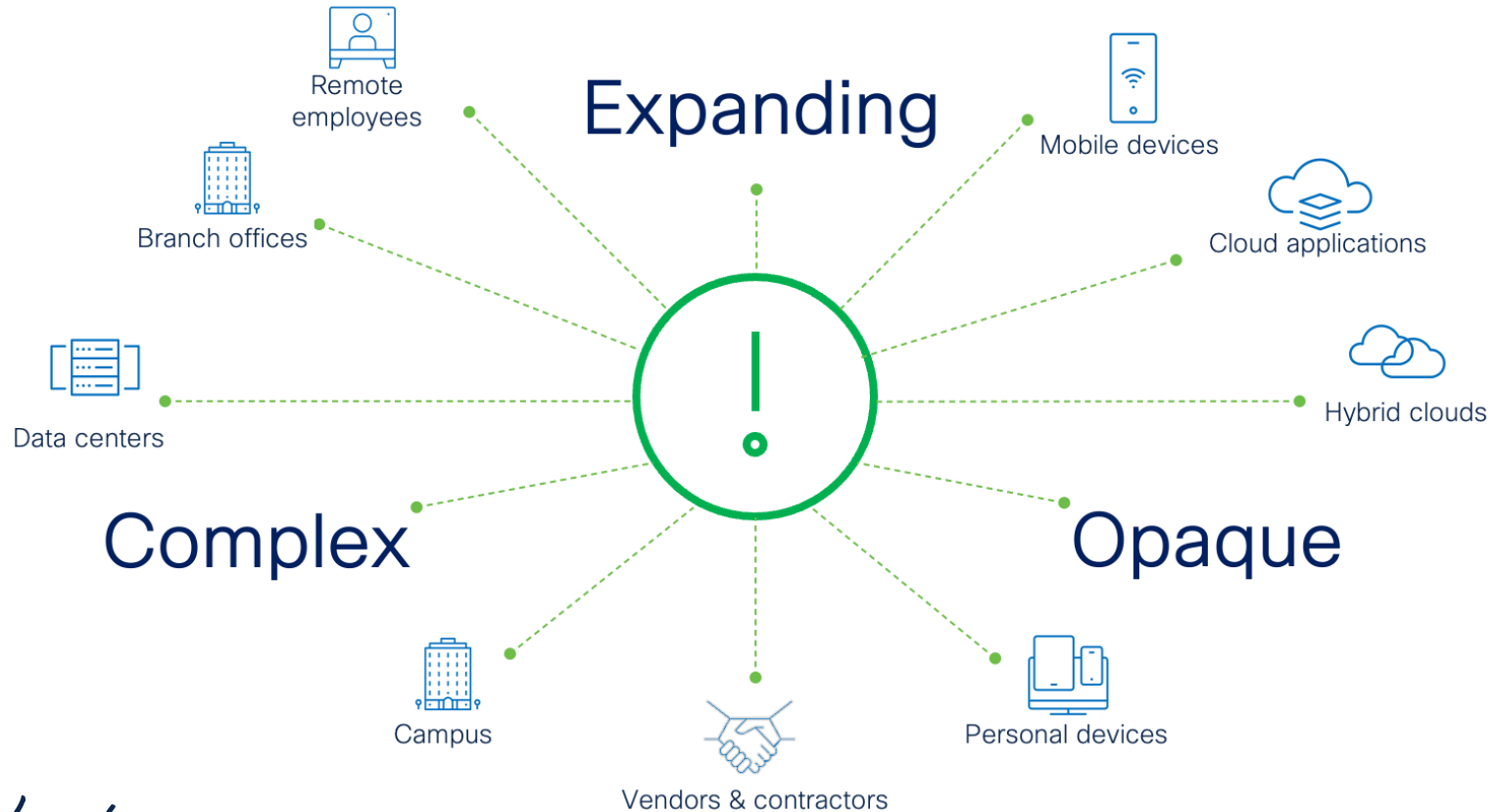
The world has changed.
Distributed users are
connecting to **distributed**
applications...



and there's a potential
threat behind every
connection.



Network attack surfaces are increasingly...



This highly distributed landscape makes secure connectivity challenging

41%

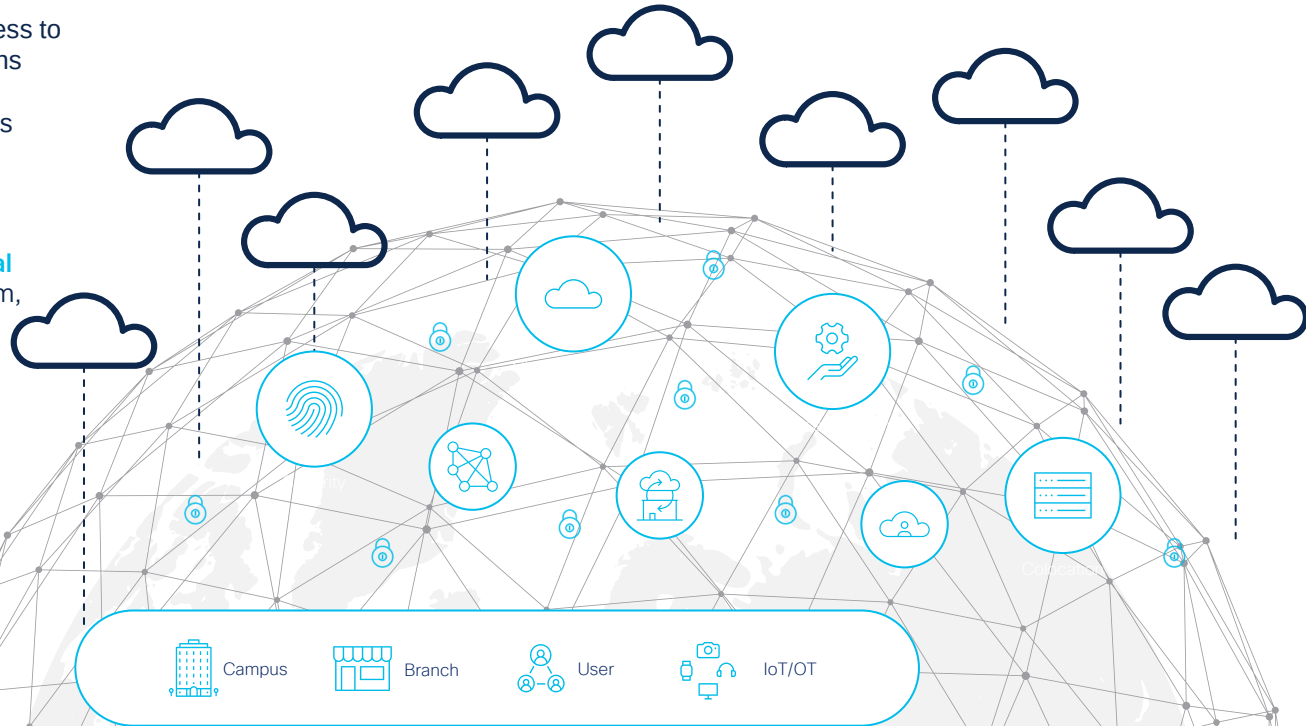
Say securing user access to cloud-based applications and mobile devices or cloud-based solutions is their biggest obstacle

86%

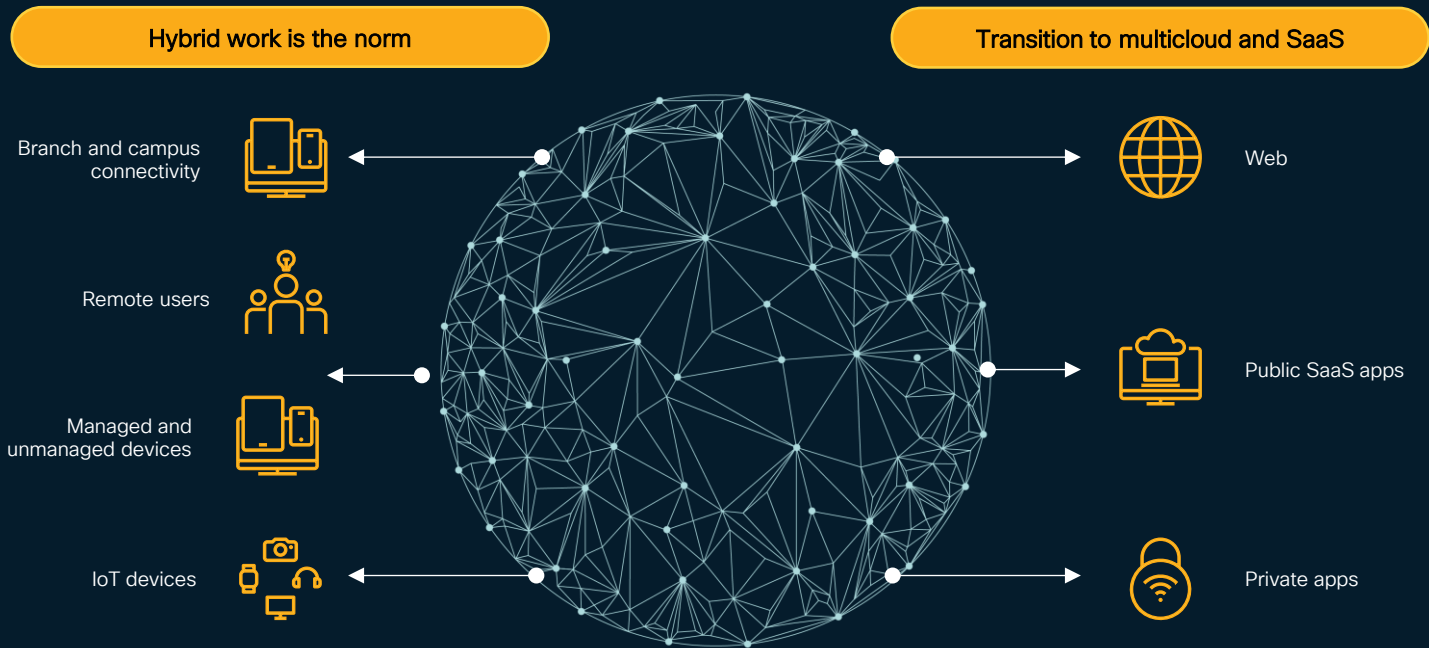
See having a **consistent operational model** across on-prem, private cloud, public cloud, and SaaS as important

85%

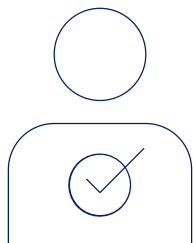
Say they value **simplicity** when it comes to technology management



Connectivity and security are fundamental for every experience



Our customers tell us that they need...



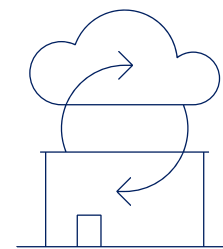
Complete visibility

of diverse attack surfaces and security compliance state



Comprehensive threat protection

that scales with their increasing network traffic and business needs



Easy deployment, management

and operations for their hybrid cloud and on-prem networks

Simplifying security,
your intent,
translated into action



Imagine
harmonizing
your security

Regaining visibility
across your networks
and applications



**Your teams
operating as
one,** driving
efficiency at
scale

Addressing the challenges

- XDR
- SSE
- ZTNA
- SD-WAN

Extended Detection and Response (XDR)

What SecOps wants



“I need my alerts to be correlated and prioritized to focus on what’s important.”

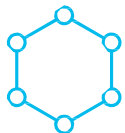


“I want my team to remediate threats with guidance from automated playbooks.”



“I need AI to help me work with speed, accuracy, and confidence.”

What is XDR?



Collection of telemetry from multiple security tools



Application of analytics to the collected and homogenized data to arrive at a detection of maliciousness

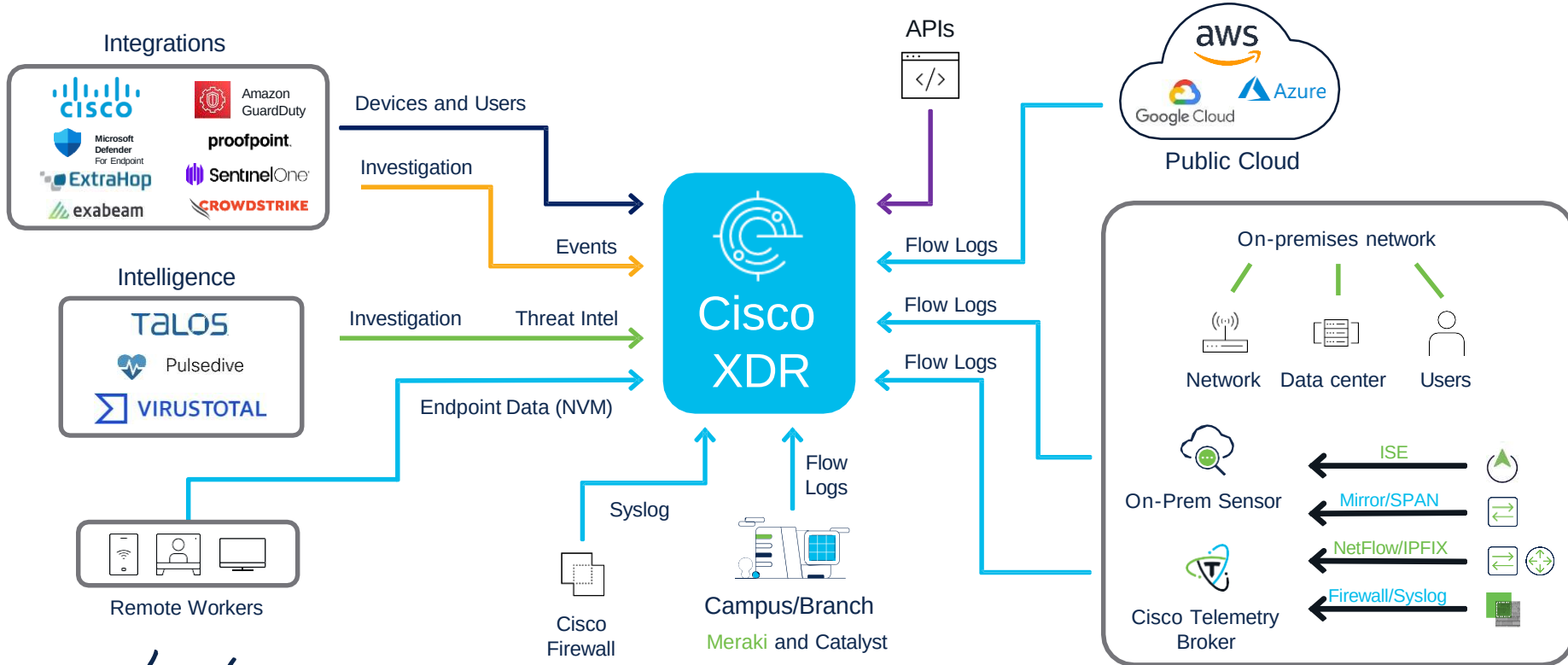


Response and remediation of that maliciousness

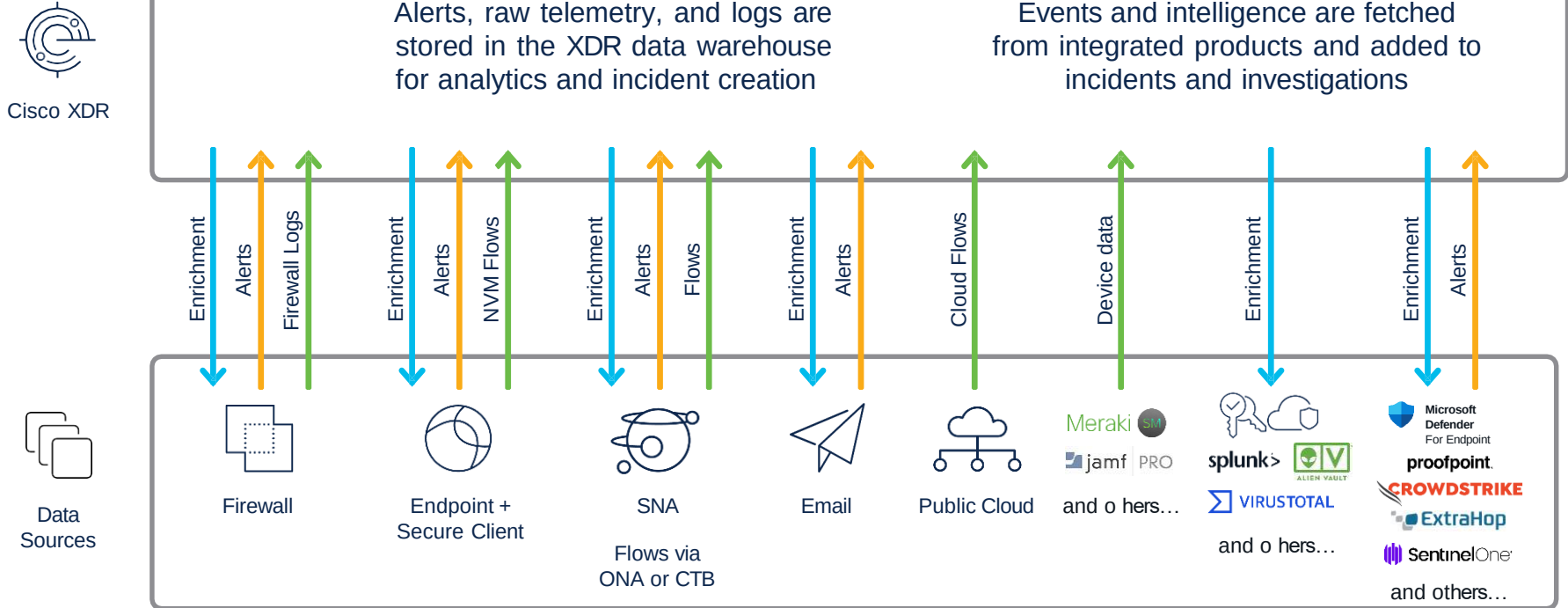


Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



Telemetry and enrichment



Cisco XDR Focuses on outcomes

Detect sooner

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

Speed up investigations

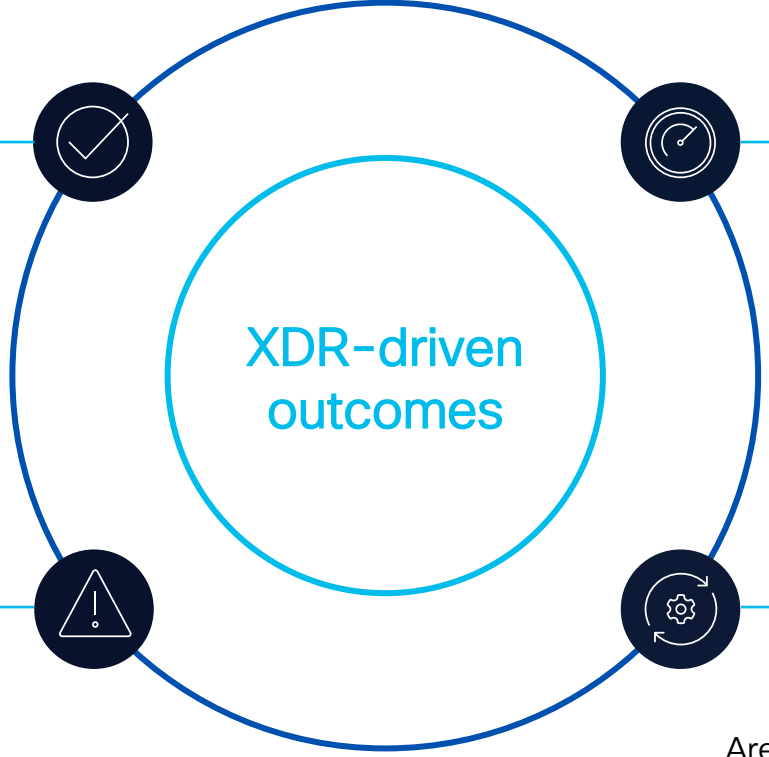
How quickly are we able to understand the full scope and entry vectors of attacks?

Prioritize by impact

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

Accelerate response

How fast can we respond?
How much can we automate?
Are we quantifiably getting better?



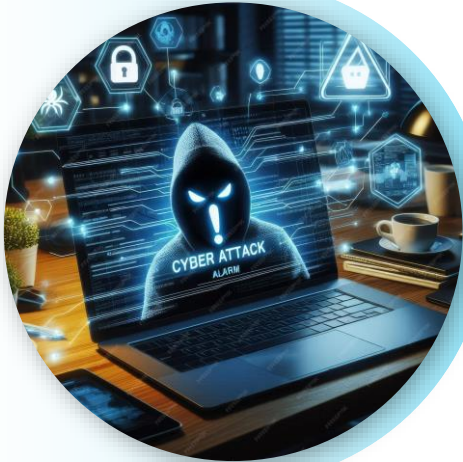
XDR-driven
outcomes

XDR Analytics detection and incident creation path



XDR Analytics covers end-to-end from raw telemetry to correlated, prioritized incidents which are enriched with context

Top use cases for Cisco XDR with network



Early Warning of Advanced Threats in Real-time



Visibility into Encrypted Traffic and Lateral Movement



AI-Powered Prioritization, Investigation, & Response

Advantages of Firewall integration with Cisco XDR

Security Operations Center (SOC)



Network telemetry is foundational
XDR
Associate disparate security
Discover and track lateral movement
and traffic anomalies

Network Operations Center (NOC)



Reduced network outages through
early warning of developing
Advanced threat detection/NDR overlay
on top of network security

Security & Network Operations Center (SNOC)



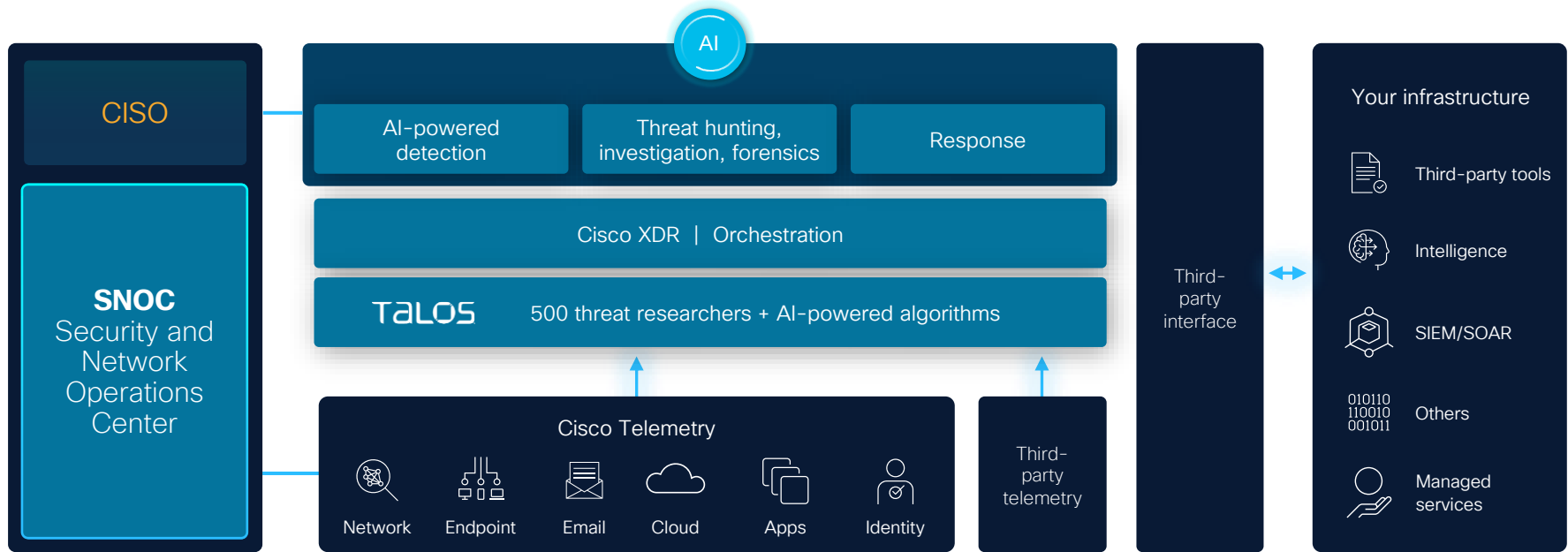
Align Security, Network, and IT teams
Realize efficiency with tool consolidation

Business Stakeholders



Enhanced business continuity
reduced risk
Greater synergy between CTO/CIO and
CISO

Cisco XDR: AI driven acceleration of the SNOCC

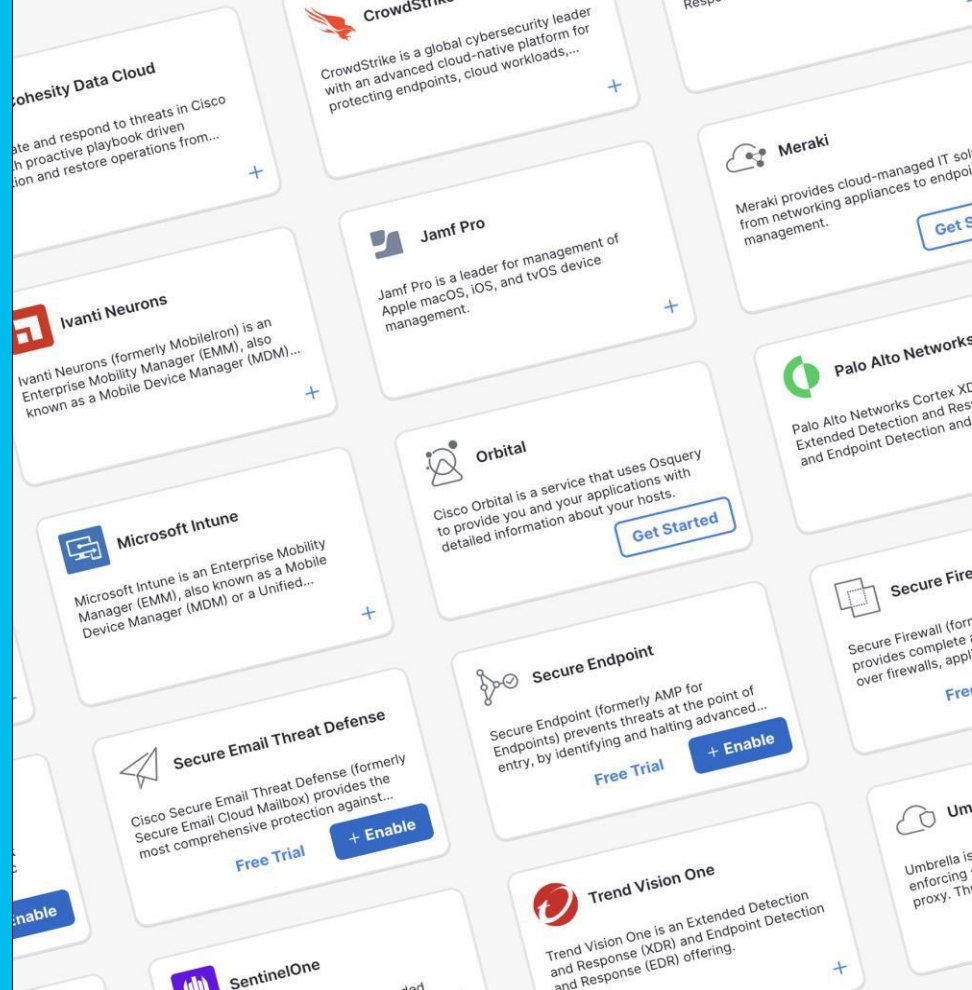


Real-time attack chain detection for the most common attacks
with curated integrations and response guidance

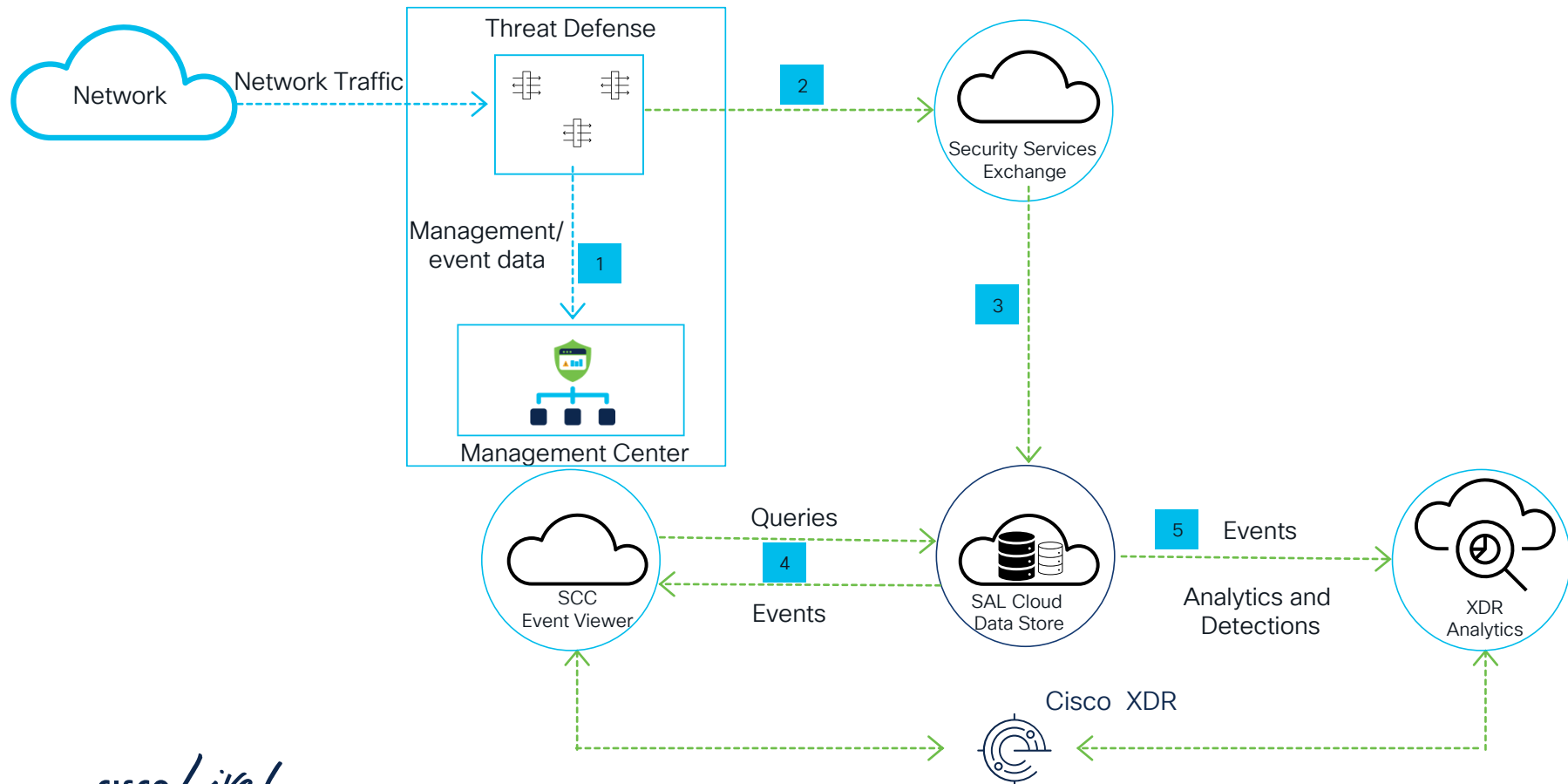
We have over 90 integrations built-in



<http://cs.co/9001pQZLV>

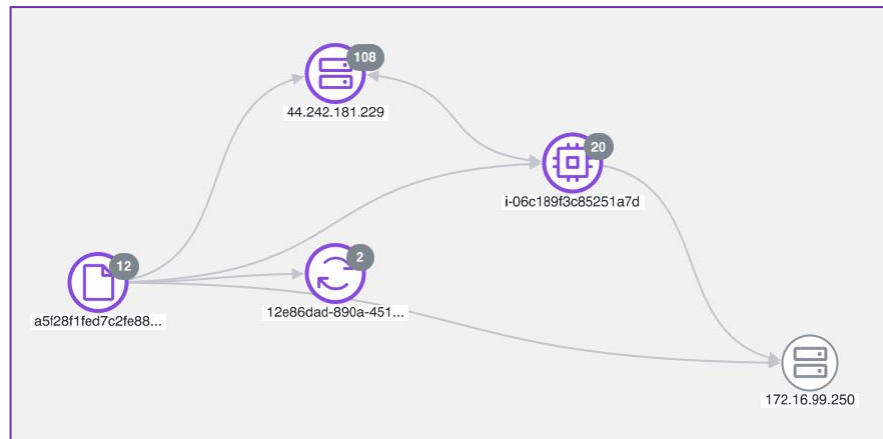


Eventing High Level Flow



Reduce investigation time

- Interactive, visual representations of incidents
- Event correlation and incident chaining to group related intelligence
- Automated enrichment for the most critical incidents, ensuring intelligence is gathered immediately



Distinct Alert Types / MITRE Tactic		Zoom	1d	3d	7d	1y	All	15-May-2023	24-May-2023
								2023	May
Internal Port Scanner	#11916	Discovery							Created: 2023-05-15 11:19 EDT
Potential Data Exfiltration	#11917	Exfiltration							Created: 2023-05-16 08:31 EDT
Outbound SMB Connection Spike	#11920	Reconnaissance							Created: 2023-05-17 16:50 EDT
DNS Abuse	#11918	Exfiltration							Created: 2023-05-17 17:02 EDT
New Unusual DNS Resolver	#11919	Command And Control							Created: 2023-05-18 12:48 EDT
Outbound Traffic Spike	#11921	Exfiltration							Created: 2023-05-19 17:37 EDT
Country Set Deviation	#11922	Initial Access							Created: 2023-05-22 09:55 EDT
Malicious Process Detected	#11924	Execution							Created: 2023-05-22 17:55 EDT
Suspicious Process Path	#11925	Defense Evasion							Created: 2023-05-22 18:01 EDT
LDAP Connection from Suspicious Process	#11926	Credential Access							Created: 2023-05-22 18:32 EDT
Suspected Malicious URL	#11923	Initial Access							Created: 2023-05-23 12:34 EDT
Suspected Cryptocurrency Activity	#11927	Impact							Created: 2023-05-24 23:25 EDT

Configure the integration on Firewall

- 1 Enable XDR
- 2 Enable XDR Automation
- 3 Select a user role for XDR workflows
- 4 Save the configuration

Cisco Security Cloud Integration

This feature enables Cisco Secure Firewall Management Center to integrate with Cisco cloud services. If you don't have a Cisco Security Cloud Sign On account, create an account [here](#) and integrate the management center with security cloud to use the cloud services. If you are using Cisco Security Cloud services prior to Release 7.6, note that you can continue to send events to the cloud. However, to use the new cloud features such as AI Assistant and PAO, you must enable Cisco Security Cloud. [Learn more](#)

Integration

Cisco Security Cloud: Enabled Current Cloud Region: us-east-1 (US Region) Security Services Exchange Tenant: cisco-kgreeshm-cdo-tenant_sdtzgt Cloud Onboarding Status: Not Available

[Disable Cisco Security Cloud](#)

Settings

Event Configuration

☒ Send events to the cloud [View your Cisco Cloud configuration](#)
☐ Intrusion events [View your Events in Cisco Security Cloud](#)
☐ File and malware events
☒ Connection events
☐ Security
☒ All

Cisco AI Assistant for Security

Powered by generative artificial intelligence and natural language processing, Cisco AI Assistant for Security is your virtual companion, assisting you in efficiently managing the Secure Firewall Threat Defense devices in your network. The AI Assistant helps you understand and create firewall policy rules and configurations, and generates custom guides to walk you through common administration tasks. [Learn more](#)

☒ Enable Cisco AI Assistant for Security

Policy Analyzer and Optimizer

Policy Analyzer & Optimizer is a Firewall refers to the process of reviewing and organizing firewall rules, analyzing the security and performance of the firewall. This can include removing redundant or unnecessary rules, consolidating rules, and reordering rules to reduce the number of rule evaluations required for each packet.

☒ Enable Policy Analyzer and Optimizer

Cisco Security Cloud Support

Cisco cloud support services provide an enhanced support experience and maximize the value of the Cisco products. The management center establishes and maintains a secure connection to Cisco cloud to participate in additional service offerings from Cisco.

☐ Enable Cisco Success Network
☐ Enable Cisco Support Diagnostics

Cisco XDR Automation

Enable Cisco XDR Automation to allow Cisco XDR user to build automated work flows that interact with various resources in the Secure Firewall Management Center.

Note that Cisco XDR, which integrates with the broad Cisco security portfolio to provide extended detection and accelerated response capabilities, is a licensed product. [Learn more](#)

☒ Enable Cisco XDR Automation

Specify the Firewall Management Center user role that you want to assign to the Cisco XDR Automation workflows.

Assigned Role: Access Admin

Local Provisioning (LTP)

The LTP method enables you to provision multiple devices simultaneously using serial numbers and a device template.

☒ Enable Low-Touch Provisioning

[Save](#)

Configure the integration on XDR

Secure Email Threat Defense Formerly Secure Email Cloud Mailbox

Cisco Secure Email Threat Defense (formerly Secure Email Cloud Mailbox) provides the most comprehensive protection against damaging and...



+ Enable

Secure Email and Web Manager Formerly SMA Email

Cisco Secure Email and Web Manager (formerly SMA Email) centralizes management and reporting functions across multiple Cisco email and web...



Secure Malware Analytics Formerly Threat Grid

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protec...



Secure Firewall Formerly Firepower

Secure Firewall (formerly Firepower) provides complete and unified management for firewall application control, intrusion prevention, URL fil...



ADD INTEGRATION

Integration Module Name

Secure Firewall

Manage Devices

Check for New Devices

Name	Version	Status	Description	IP Address
atl-tme-fmc	7.2.0	Registered	10.90.12.219 atl-tme-fmc	10.90.12.219
atl-tme-fmc-log.cisco.com	7.2.3	Registered	10.90.12.236 atl-tme-fmc-log.cisco.com	10.90.12.236
atl-tme-fp4100-1	7.2.0	Registered	10.90.12.210 atl-tme-fp4100-1 (FMC managed)	10.90.12.210
atl-tme-fp4100-2	7.2.0	Registered	10.90.12.220 atl-tme-fp4100-2 (FMC managed)	10.90.12.220
atl-tme-ftd-log	7.2.3	Registered	10.90.12.237 atl-tme-ftd-log (FMC managed)	10.90.12.237

5 per page 1-5 of 5 < > 1 / 1 >>

☒ Create Dashboard

Create a dashboard of the tiles associated with this integration module, which can be shared by all members of your organization.

Save

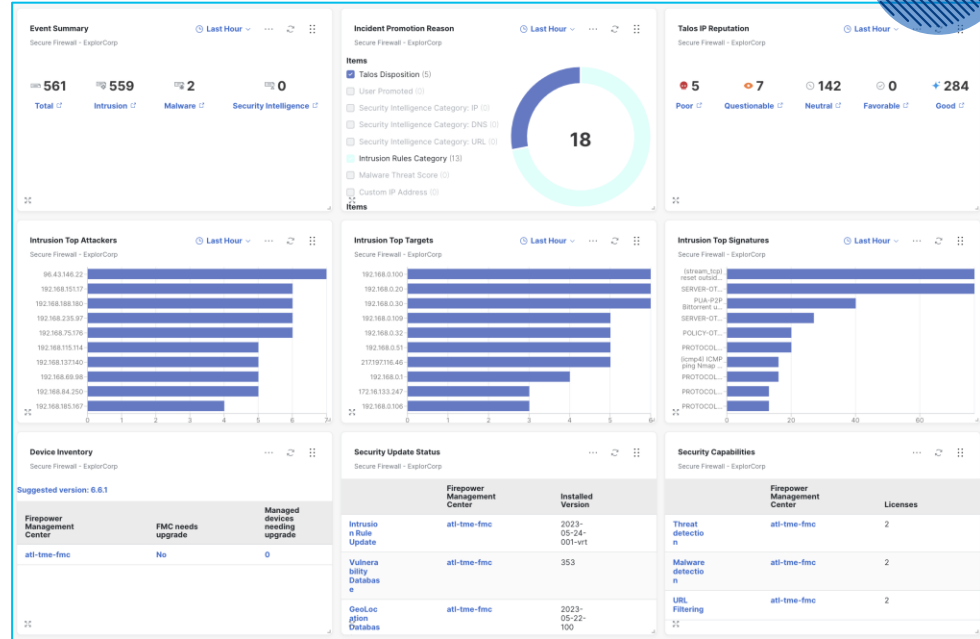
1 Add Firewall module

2 Save the module

Secure Firewall

Dashboard tiles

- Raw event summary
- Incident promotion reason
- Talos IP reputation
- Intrusion top attackers
- Intrusion top targets
- Intrusion top signatures
- Security Capabilities (FMC)
- Security Update Status (FMC)
- Device Inventory(FMC)

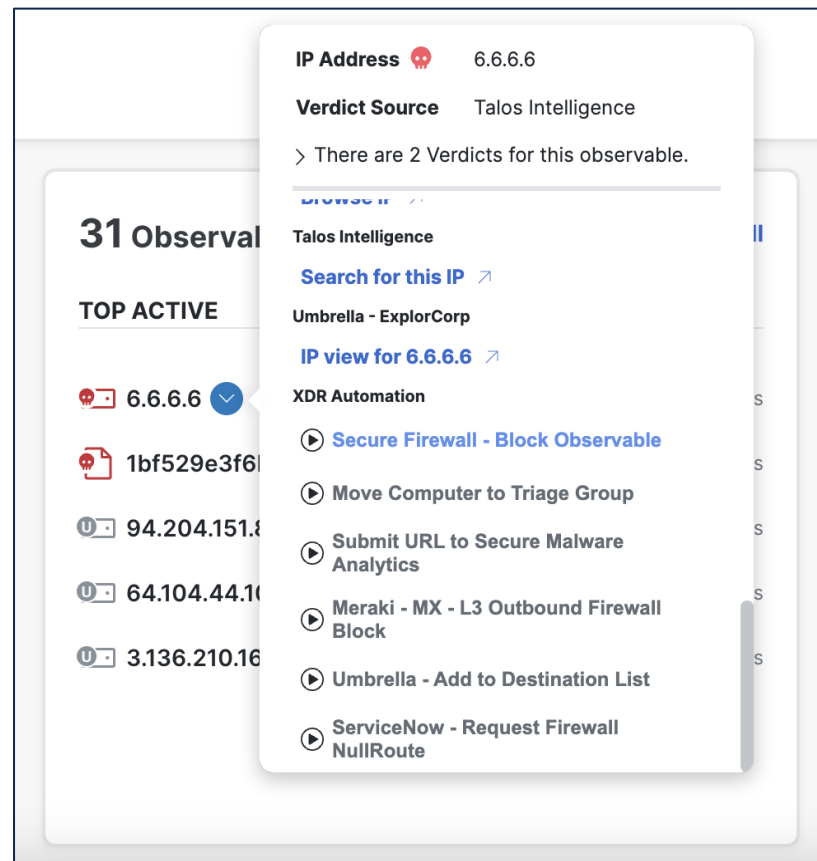


Use Cases

Use Case : Block Observables on Firewall

Problem: Adam the analyst, is reviewing an endpoint alert. He notices an unknown IP address related to a compromise on the endpoint. Adam wants to act by blocking this IP address on the firewall, but he doesn't have access to Firepower Management Center.

Solution: Using the pivot menu Adam can block the IP address at the click of a button from anywhere.



Demo



Firewall Threat Defense 7.4.2 is available.

recommends upgrading to the suggested

Remind Me 

Access Control Policy	Status	Last Modified	Lock Status	
AccessPolicy1	Targeting 0 device(s)	2024-10-18 14:50:53 Modified by "Firepower System"		
AustinLabPolicy Default Access Control Policy with default action block	Targeting 1 device(s) <i>Out-of-date on 1 targeted devices</i>	2024-10-18 14:50:53 Modified by "Firepower System"		
Default Access Control Policy Default Access Control Policy with default action block	Targeting 0 device(s)	2024-10-18 14:50:53 Modified by "Firepower System"		
Global APJC Parent Common APJC Policy Settings	Targeting 0 device(s)	2024-10-18 14:50:53 Modified by "Firepower System"		
GCP-BR-FTD1	Targeting 1 device(s) <i>Out-of-date on 1 targeted devices</i>	2024-10-18 14:50:53 Modified by "Firepower System"		
Global Pseudo-AI Parent Pseudo-AI Parent Policy	Targeting 0 device(s)	2024-10-18 14:50:53 Modified by "Firepower System"		
RTP-BR-FTDv-003-Robotics	Targeting 1 device(s) <i>Up-to-date on all targeted devices</i>	2024-10-22 21:31:27 Modified by "thiachan@cisco.com"		
ibm-cloud-acp	Targeting 1 device(s) <i>Out-of-date on 1 targeted devices</i>	2024-10-18 14:50:53 Modified by "Firepower System"		
ibm-cloud-nlb-acl	Targeting 0 device(s)	2024-10-18 14:50:53 Modified by "Firepower System"		
IZ-T-TestPolicy	Targeting 1 device(s) <i>Out-of-date on 1 targeted devices</i>	2024-10-18 14:50:53 Modified by "Firepower System"		
RTP-DMZ-POLICY	Targeting 1 device(s) <i>Out-of-date on 1 targeted devices</i>	2024-10-18 14:50:53 Modified by "Firepower System"		
RTPLab-Default-Policy Default Policy	Targeting 0 device(s)	2024-10-18 14:50:53 Modified by "Firepower System"		
RTPLab-Regional-Block-Policy RTP Regional Block Policy	Targeting 0 device(s)	2024-10-18 14:50:53 Modified by "Firepower System"		

Use Case: PSIRT Impact Monitoring

Problem: A network administrator is continuously monitoring for new PSIRT announcements and checking to see if their devices are vulnerable

Solution: This orchestration workflow will check for new PSIRTs then compare your devices version and notify you if any vulnerable devices were found.

SXO-WF QA 3:05 PM

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

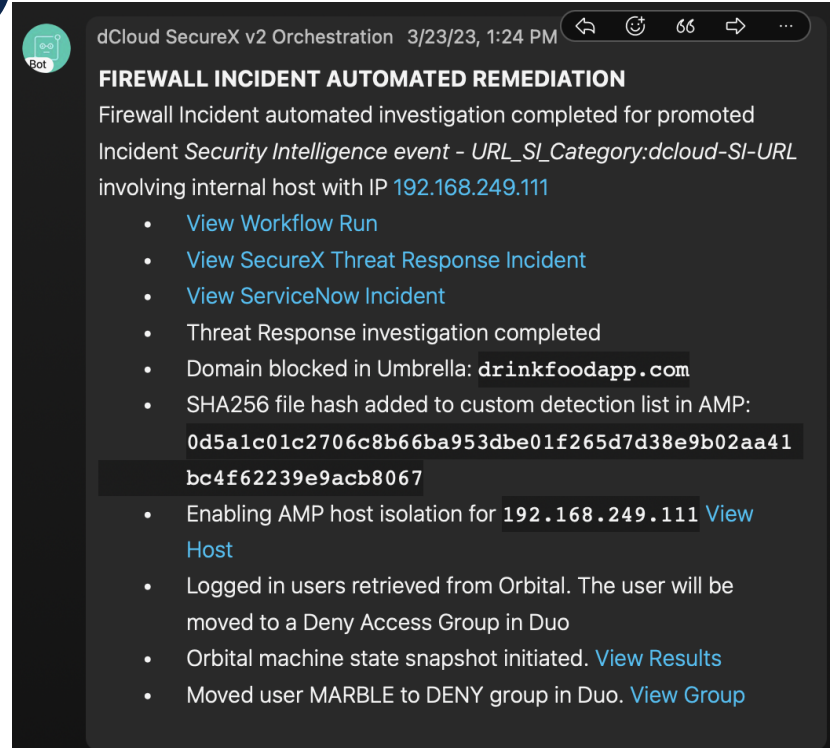
One or more devices managed by Secure Firewall Manager require software updates due to a Medium PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.
2 | FTD-test (ASA) at 127.0.0.1 is running software version 9.14.4 and needs to be upgraded.
3

Use Case: Impact RED Remediation

Problem: A high priority intrusion event is detected by the Firewall. Adam, the analyst, needs to remediate quickly across multiple technologies.

Solution: An XDR orchestration workflow investigates the event and waits for approval. Once approval is granted, automated remediation at the DNS, application, and endpoint level are taken.



The screenshot shows a notification from 'dCloud SecureX v2 Orchestration' dated '3/23/23, 1:24 PM'. It features a 'Bot' icon and standard notification controls. The main heading is 'FIREWALL INCIDENT AUTOMATED REMEDIATION'. The body text states: 'Firewall Incident automated investigation completed for promoted Incident *Security Intelligence* event - *URL_SI_Category:dcloud-SI-URL* involving internal host with IP **192.168.249.111**'. A bulleted list follows, detailing the remediation steps: 'View Workflow Run', 'View SecureX Threat Response Incident', 'View ServiceNow Incident', 'Threat Response investigation completed', 'Domain blocked in Umbrella: **drinkfoodapp.com**', 'SHA256 file hash added to custom detection list in AMP: **0d5a1c01c2706c8b66ba953dbe01f265d7d38e9b02aa41bc4f62239e9acb8067**', 'Enabling AMP host isolation for **192.168.249.111** View Host', 'Logged in users retrieved from Orbital. The user will be moved to a Deny Access Group in Duo', 'Orbital machine state snapshot initiated. View Results', and 'Moved user MARBLE to DENY group in Duo. View Group'.

dCloud SecureX v2 Orchestration 3/23/23, 1:24 PM

FIREWALL INCIDENT AUTOMATED REMEDIATION

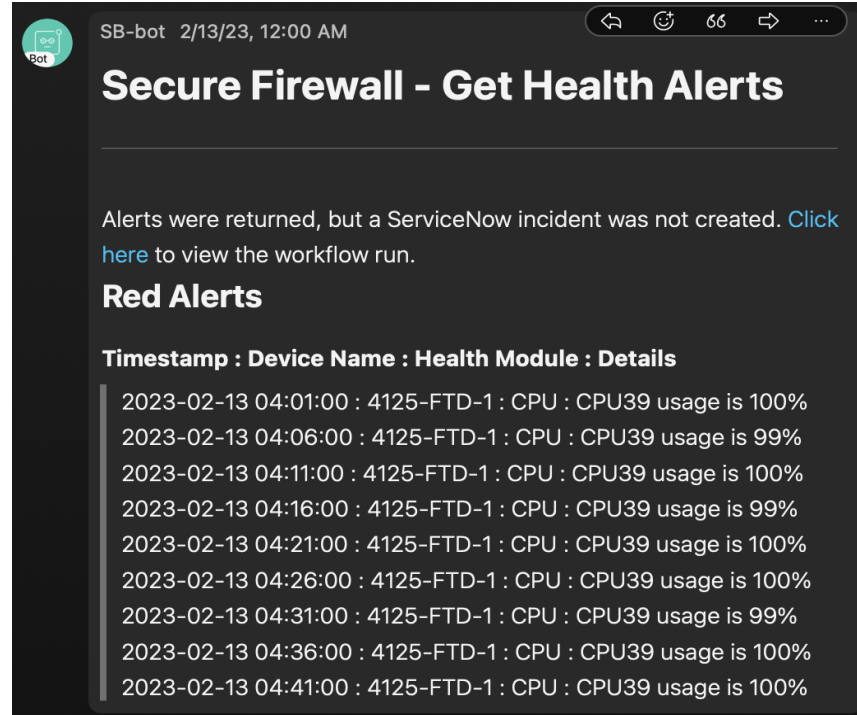
Firewall Incident automated investigation completed for promoted Incident *Security Intelligence* event - *URL_SI_Category:dcloud-SI-URL* involving internal host with IP **192.168.249.111**

- [View Workflow Run](#)
- [View SecureX Threat Response Incident](#)
- [View ServiceNow Incident](#)
- Threat Response investigation completed
- Domain blocked in Umbrella: **drinkfoodapp.com**
- SHA256 file hash added to custom detection list in AMP: **0d5a1c01c2706c8b66ba953dbe01f265d7d38e9b02aa41bc4f62239e9acb8067**
- Enabling AMP host isolation for **192.168.249.111** [View Host](#)
- Logged in users retrieved from Orbital. The user will be moved to a Deny Access Group in Duo
- Orbital machine state snapshot initiated. [View Results](#)
- Moved user MARBLE to DENY group in Duo. [View Group](#)

Use Case: Firewall Health Monitoring

Problem: A network administrator is trying to maintain a healthy network but sometimes a device gets into an unhealthy state. It can take time to react these issue the network administrator is not aware.

Solution: This orchestration workflow will check for health alerts from your devices and proactively notify via Webex teams, Slack, or email.



SB-bot 2/13/23, 12:00 AM

Secure Firewall - Get Health Alerts

Alerts were returned, but a ServiceNow incident was not created. [Click here](#) to view the workflow run.

Red Alerts

Timestamp	Device Name	Health Module	Details
2023-02-13 04:01:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:06:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:11:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:16:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:21:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:26:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:31:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:36:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:41:00	4125-FTD-1	CPU	CPU39 usage is 100%

Use Case: Expiring Time-based Objects

Problem: As a network administrator it is always challenging to manage your policies. Some rules in the policy may not be active due to an expired time range and finding expired rules can be time consuming.

Solution: This orchestration workflow will check rules that have already expired or will expire soon and proactively notify you of which rules to review.



SXO-WF QA 4:10 PM

Time-based rules set to expire

An audit of Secure Firewall has uncovered one or more policies with time-based rules set to expire within the next 30 days

Policy: Block All Traffic

- Allow Apple has a time-based object titled 2-28 which expired -77 days ago

Policy: Default

- Allow Apple has a time-based object titled 2-28 which expired -77 days ago

Policy: SecureX Policy

- end_of_april_rule has a time-based object titled end_of_april which expired -16 days ago
- end_of_may_rule has a time-based object titled end_of_may which is set to expire in 14 days
- 5/15 end has a time-based object titled 5-15 which expired -1 days ago

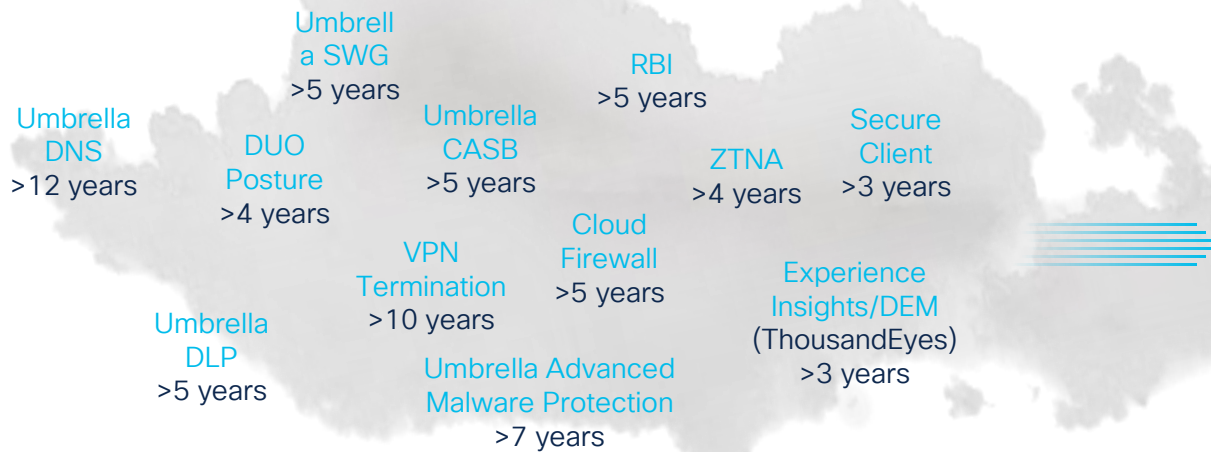
Key Takeaways

- Automated Threat Intelligence Sharing
- Simplified Security Operations
- Real-time Threat Mitigation

Cisco Secure Access - Security Service Edge (SSE)

Introducing Cisco Secure Access

Proven cloud-native security converged into one service

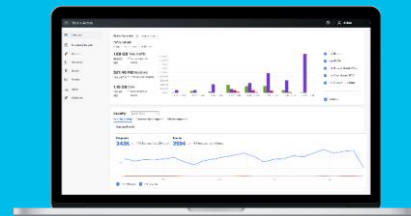


Protecting 70,000+ customers

More than 220M endpoints

CISCO *Live!*

Cisco Secure Access



- Single Console
- Single Client
- Unified Policies

Cisco Secure Access

Industry-leading
Security Service Edge

Unified console,
policies, and client

Advanced levels of
zero trust protection

Exceptional
experience
for users

Simplified IT
Operations

Secure Internet Access

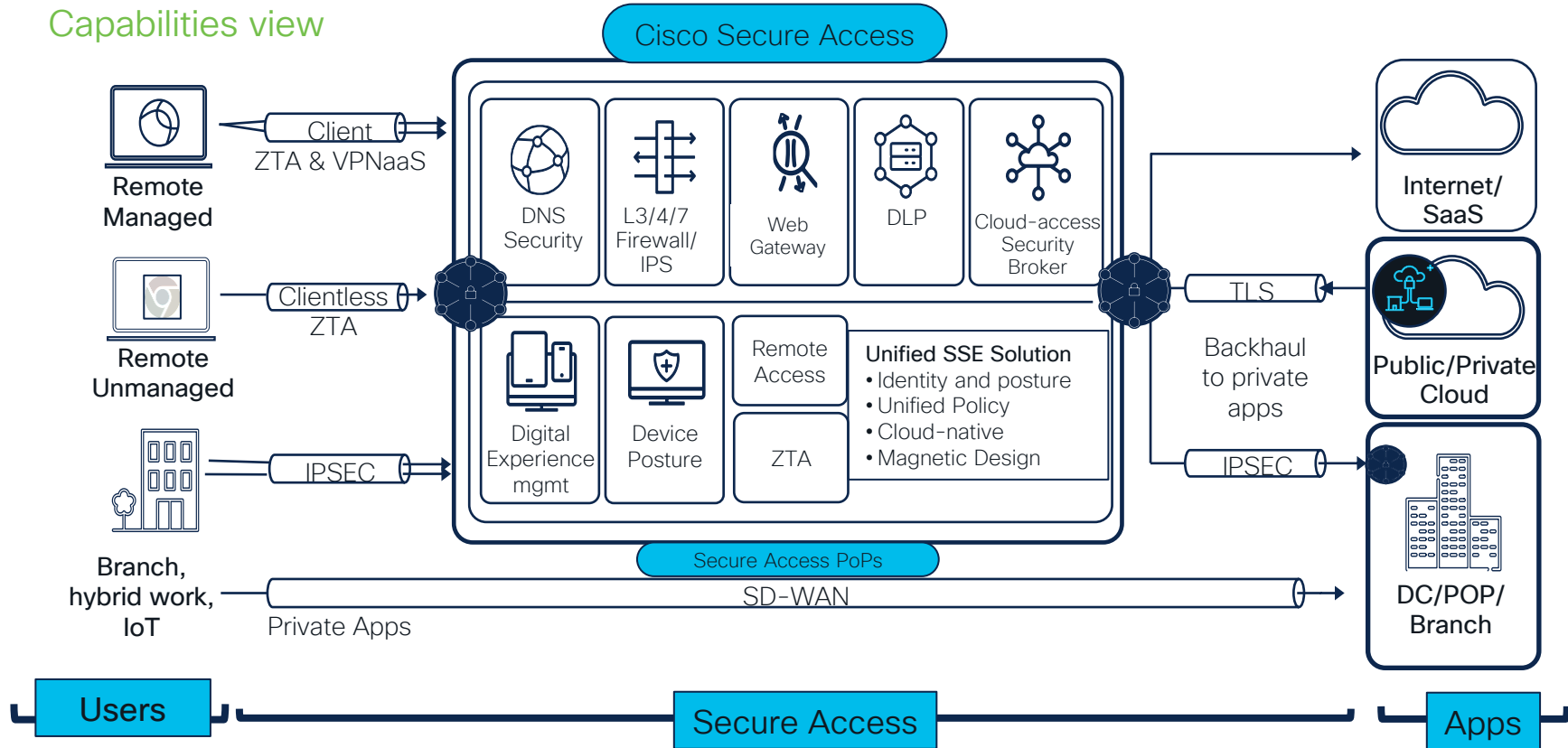
Secure Private Access

Gen AI threat defense
and administration

cisco *Live!*

Cisco Secure Access

Capabilities view



Cisco Secure Client

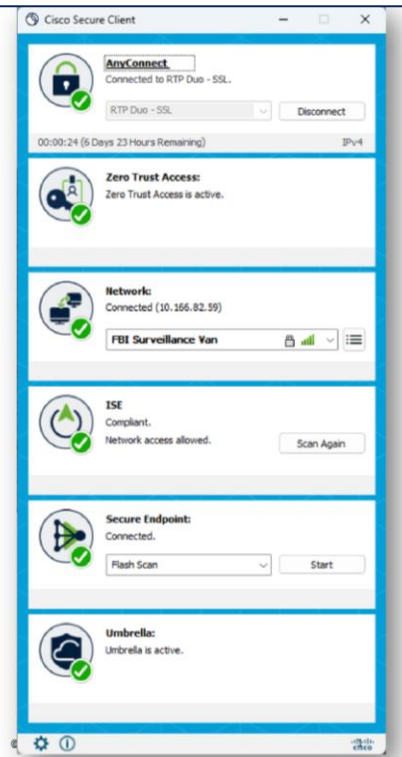
Suite of security service enablement modules



Cisco Secure Client

Suite of security service enablement modules

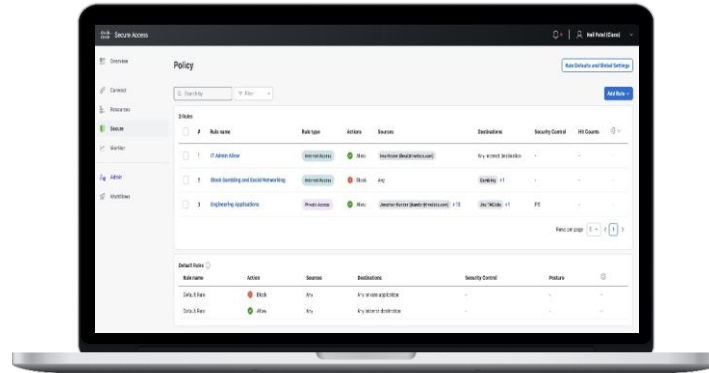
- AnyConnect VPN (Core)
- Zero Trust Access (Cisco Secure Access)
- Network Access Manager (NAM)
- ISE Posture
- Secure Firewall Posture (aka: HostScan) (No UI)
- Secure Endpoint (AMP)
- Umbrella Module
- Cloud Management Module (No UI)
- Network Visibility Module (NVM) (No UI)
- Diagnostics and Reporting Tool (DART)
- Thousand Eyes (new) (No UI)



Simply see traffic, analyse risk, manage access

Unified Policy Management
Holistic Threat Visibility
Aggregated reporting

Seamless user experience
Faster onboarding
Streamlined maintenance



Vendor/License consolidation
Deployment optimization
Cost efficiencies

Converged cloud security for lower cost and improved efficiencies

Cisco Secure Access – User Anywhere

STEP 1
Authenticate

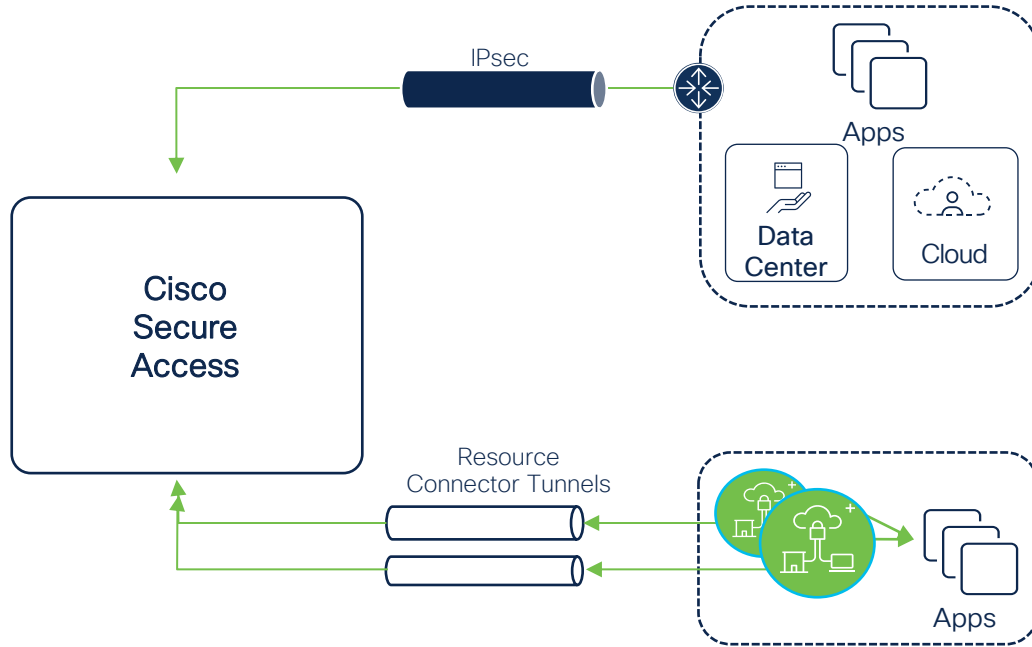
STEP 2
Go to Work



Use Cases



Apps: Private Applications



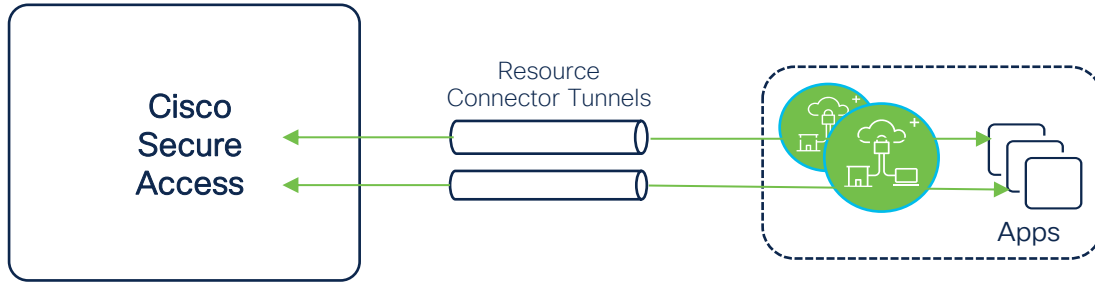
Site-to-site Tunnels with IPsec

- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Fallback for resource connectors

Resource Connectors

- Lightweight VM for AWS and ESXi
- All traffic egresses from Resource Connector IP
- Access applications with overlapping IPs
- Outbound connection / no firewall holes required
- No routing configuration required
- Auto failover / load balancing

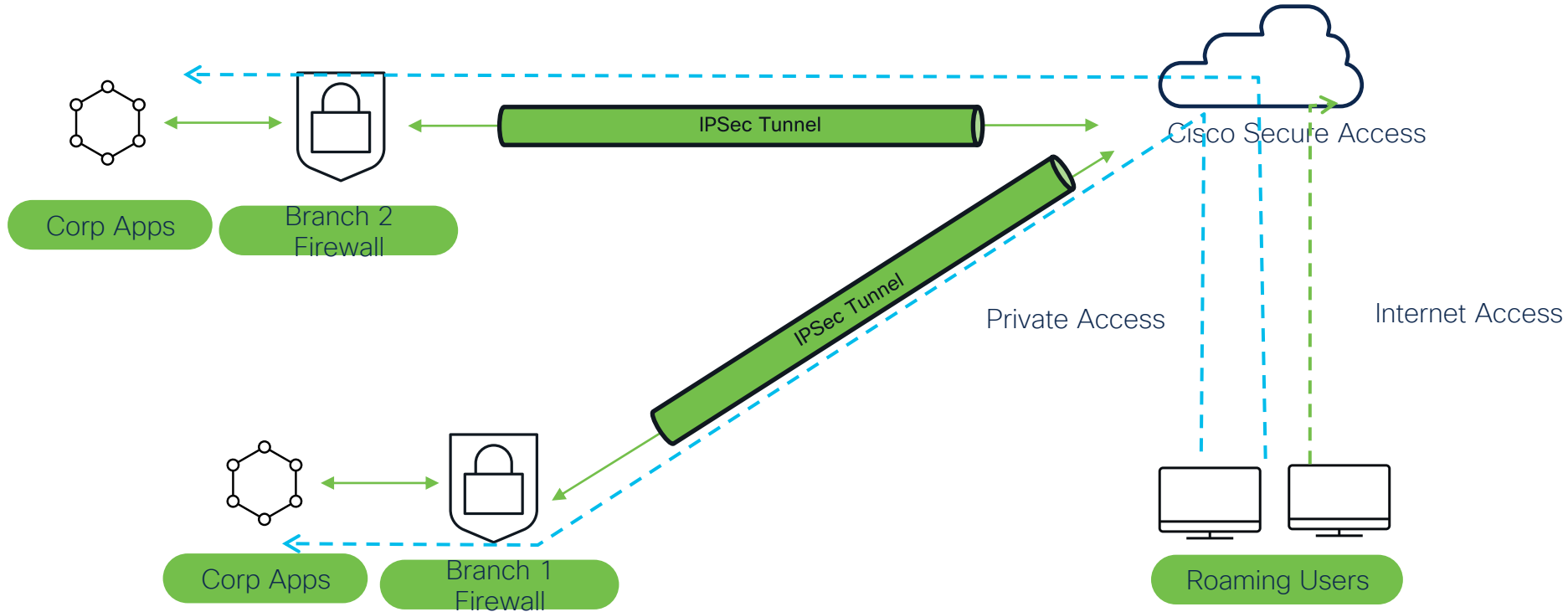
Apps: Internet/SaaS Applications



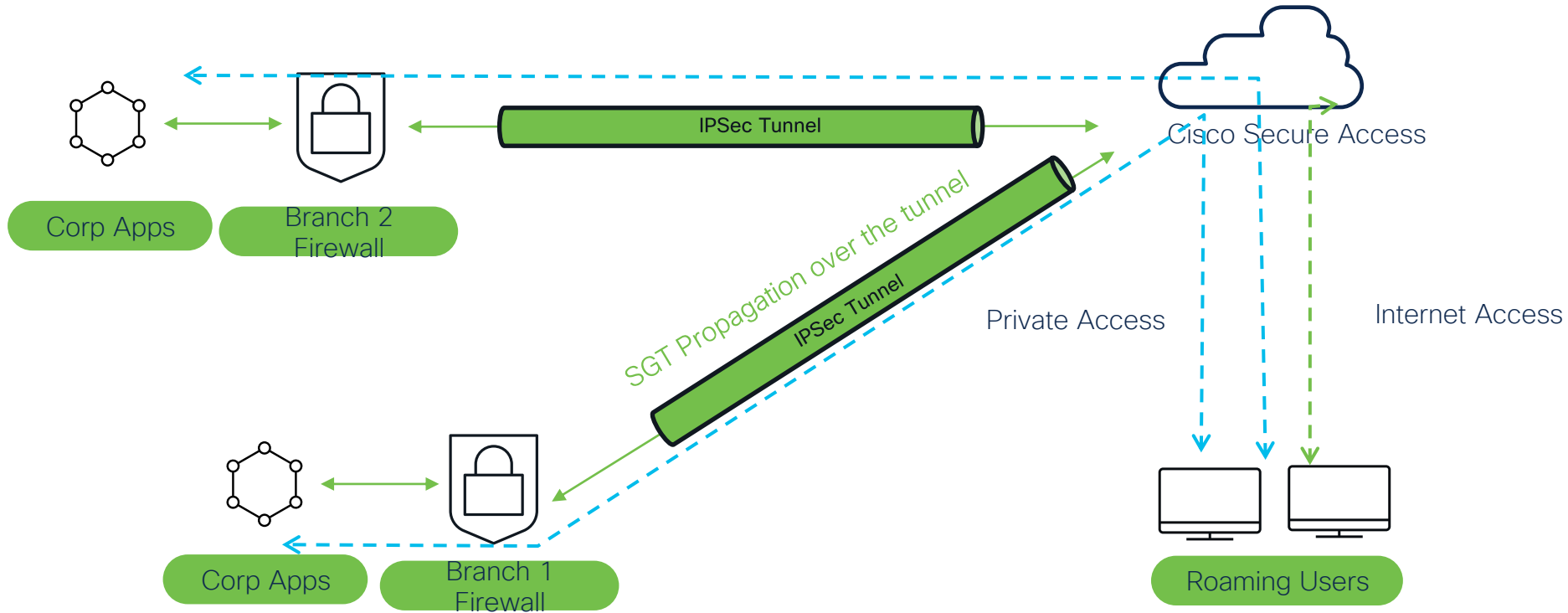
Resource Connectors

- Lightweight VM for AWS and ESXi
- All traffic egresses from Resource Connector IP
- Access applications with overlapping IPs
- Outbound connection / no firewall holes required
- No routing configuration required
- Auto failover / load balancing

Secure Firewall Integration

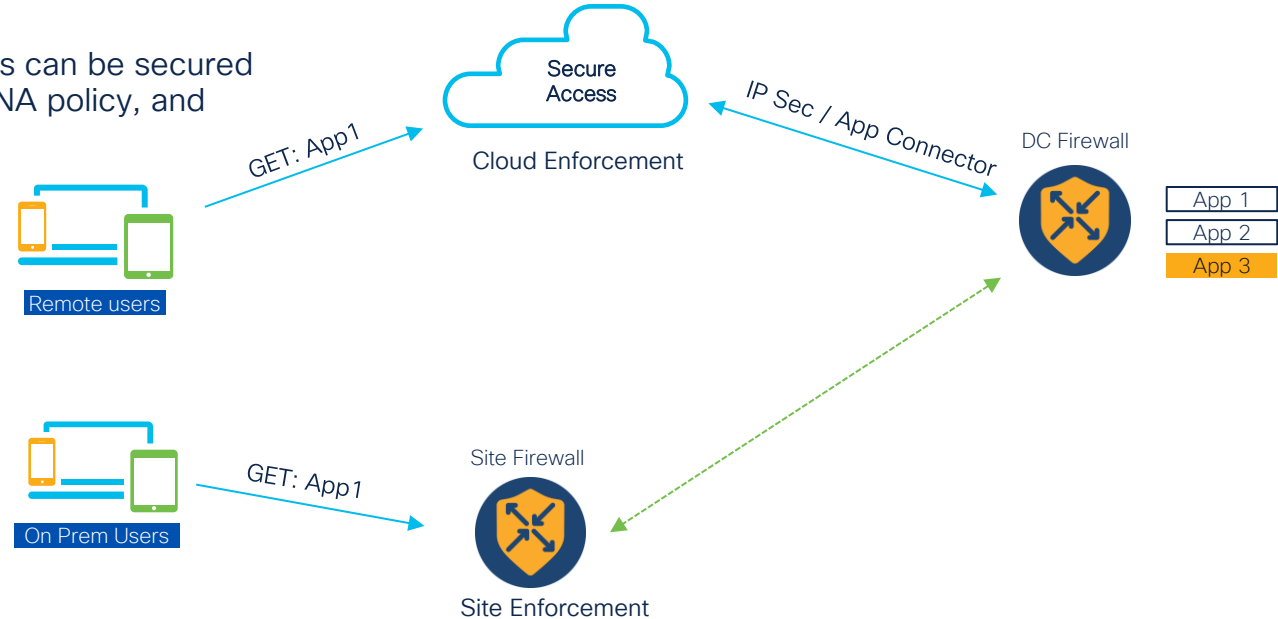


Cisco Secure Access Enhancements



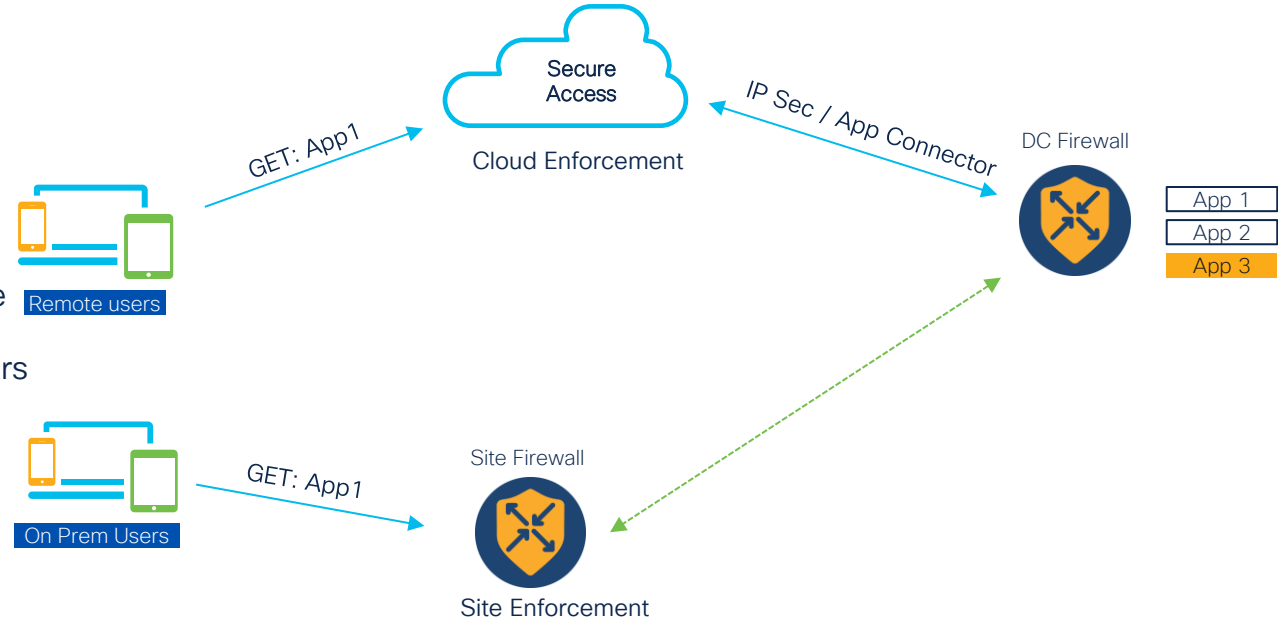
Secure Firewall + SSE = Future

- Admin has Central Policy Configuration – Secure Access
- Users On network clients can be secured in branch with same ZTNA policy, and identity



Secure Firewall + SSE = Future

- User network has no direct routes to application network
- User Performance improvements
- Cost optimisation – No need to massively scale internet pipe for large number of users in branch

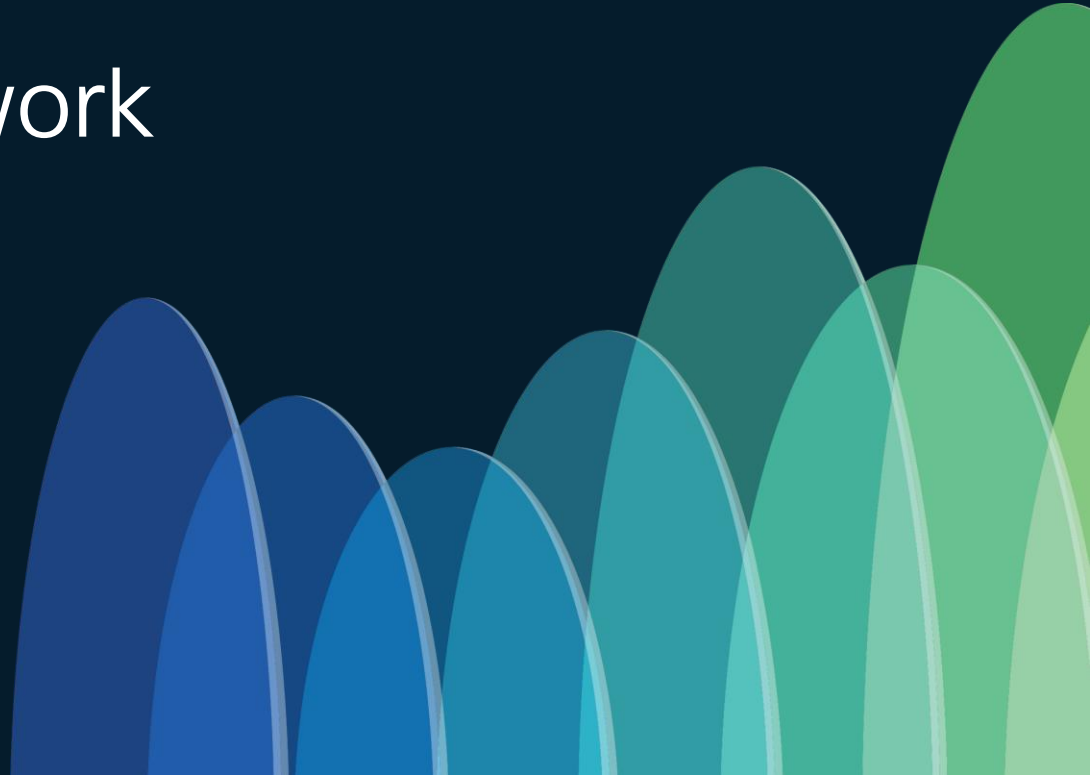


Key Takeaways

Cisco Secure Access + Firewall integration provides:

- Unified Security Policy Management
- Enhanced User Experience with Optimized Access
- Cost Efficiency and Scalability

Zero Trust Network Access (ZTNA)



Your Speaker

Dinesh Moudgil



- dmoudgil@cisco.com
- From Chandigarh, India
- CCIE Security #58881
- 12 Years in Industry, 9 with Cisco
- TAC - HTTS - TME Leader
- Lead Management & SD-WAN
- Like outdoors and guitar



What is Zero Trust Network Access?

- Zero Trust Network Access (ZTNA) means different things to different organisations.
- Granting USERS access to APPLICATIONS and doing so only after the relevant criteria are met.
- The “Network Access” part of ZTNA is not Network Access as we typically understand it.
- Users should not need access at the network level to access a specific application (i.e., they do not need an IP on the network).
- ZTNA does not just apply to remote access, access from inside the network should also be covered by the same protections.

Zero Trust Application Access

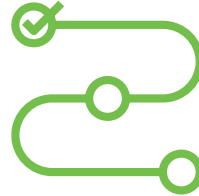
Securely and Simply Connect Users to Private Applications

Zero trust application access (ZTAA) moves beyond traditional “authorize then ignore” ZTNA models by adding complete threat inspection and policy for each individual application



Limit who is allowed

Per application access with clientless SAML, Azure AD, ISE, and Duo



Limit where they can go

Reduce access to specific apps to limit attack surface and lateral spread of threats

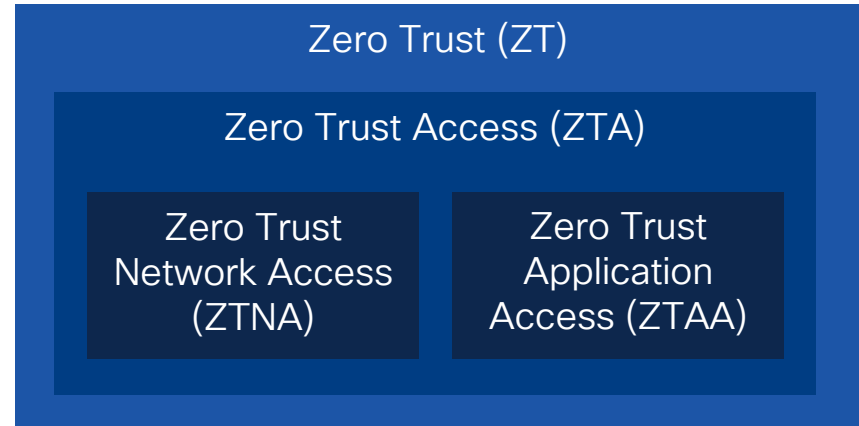


Limit threats they may bring

Go beyond traditional ZTNA by continuously inspecting allowed traffic/behaviors with IPS/malware protection

ZT vs. ZTA vs. ZTNA vs. ZTAA

- Zero Trust
 - A comprehensive security framework that prioritizes least privilege, strict access controls, and continuous monitoring to mitigate risks and protect resources.
- Zero Trust **Access**
 - A specific aspect of Zero Trust that **focuses on managing and enforcing access** to resources
- Zero Trust **Network** Access (ZTNA)
 - A subset of Zero Trust Access that focuses on secure **access to networks**.
- Zero Trust **Application** Access (ZTAA)
 - A subset of Zero Trust Access that focuses on secure **access to individual applications**.



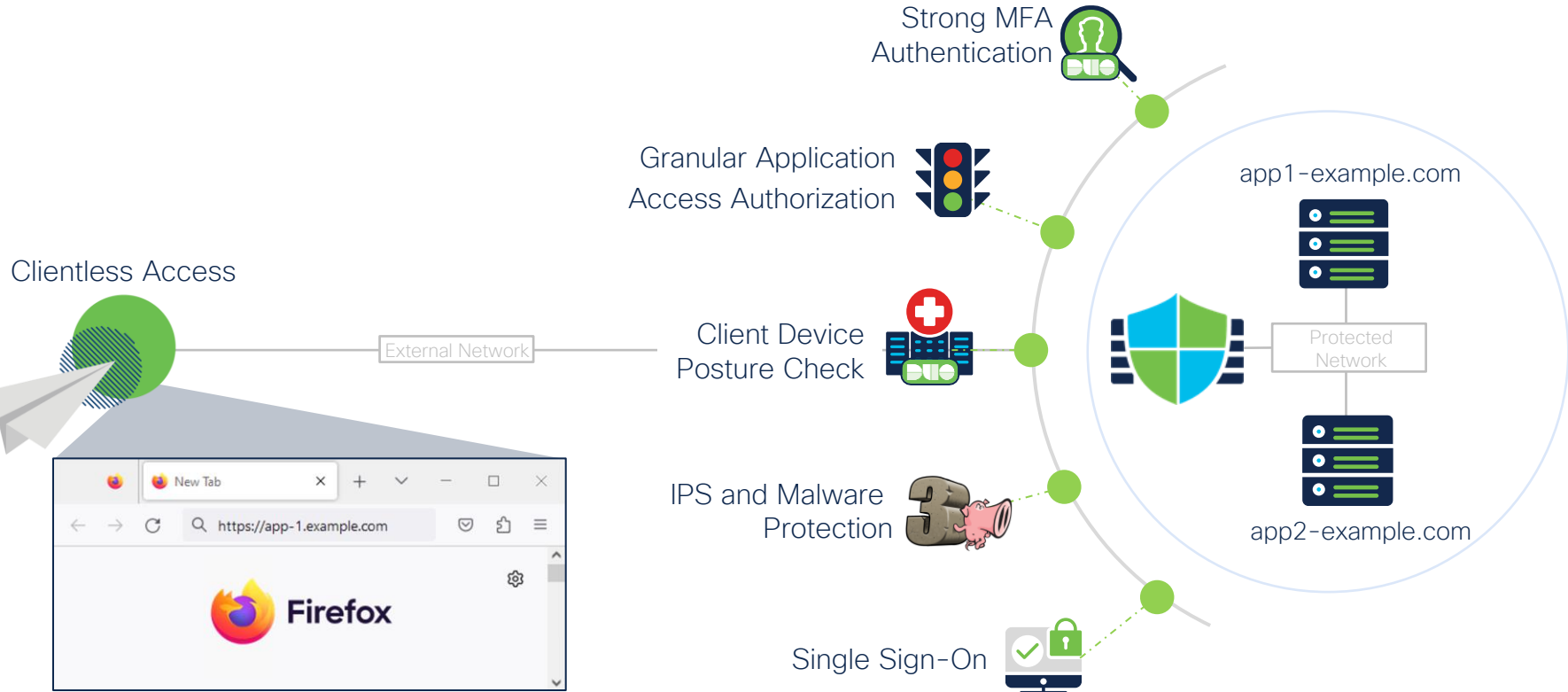
RAVPN vs ZTNA

	Remote Access VPN	Zero Trust Network Access
Access Granted	Access to full network or network segment	Access to specific resource/application
Network	Client gets IP address on the network	No specific IP address assigned to the client for access
Posture	Posture assessed once at VPN Authentication	Posture assessed at each application access with Continuous Trusted Access
Headend	1:1 Client-to-Headend relationship	Client can connect to different headends per application

Clientless and Client-Based ZTNA

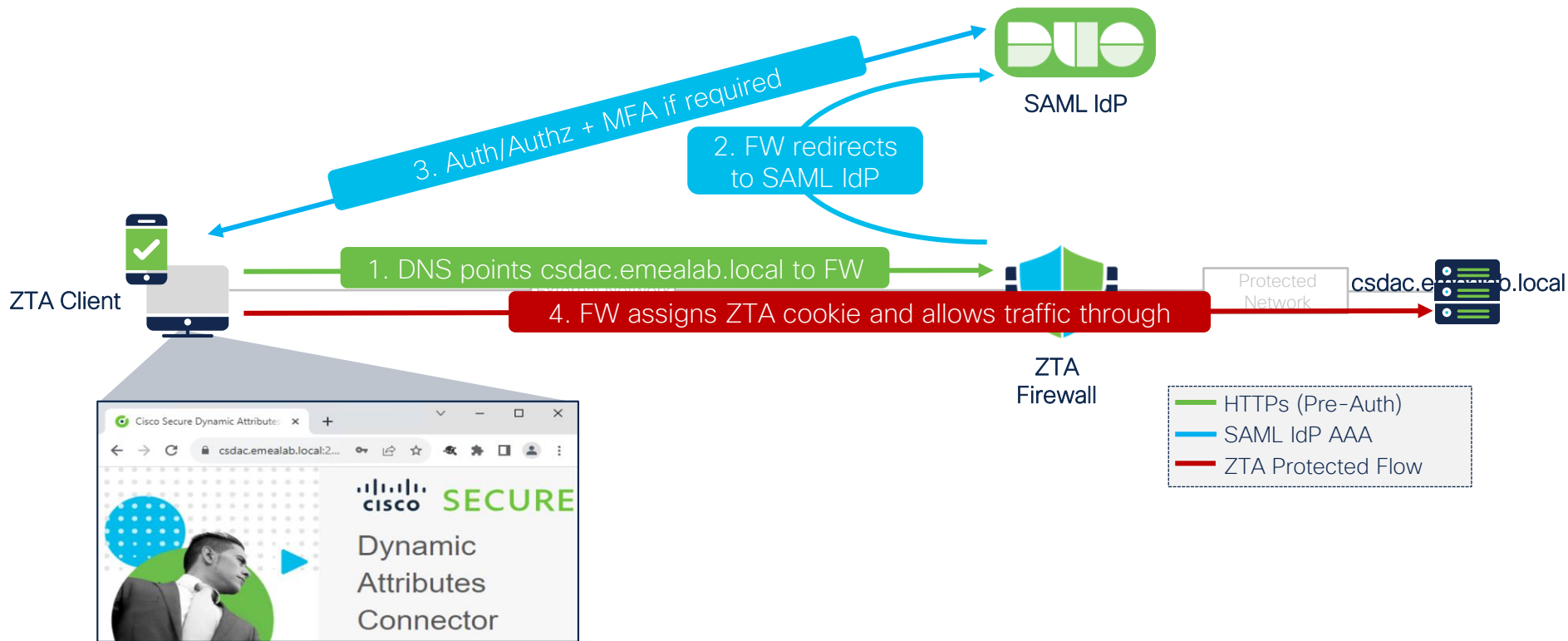
	Clientless ZTNA	Client-Based ZTNA
Endpoint Presence	No client application required on endpoint device	Client software required to be installed on endpoint device
Access Type	Can only be accessed through a web browser	Client software handles traffic transparent to the user
Application Type	Only browser-based web applications	Supports all applications on different ports and protocols
Posture Type	Posture only available through authentication flow (e.g. Duo Health or Intune)	Client software handles posture based on policy (similar to HostScan or ISE Posture)
User Types	Can be used for Contractor/3 rd Party clients as well as internal users on personal devices	Generally restricted to customers owned and managed devices due to client requirement.

Zero Trust Access - Overview



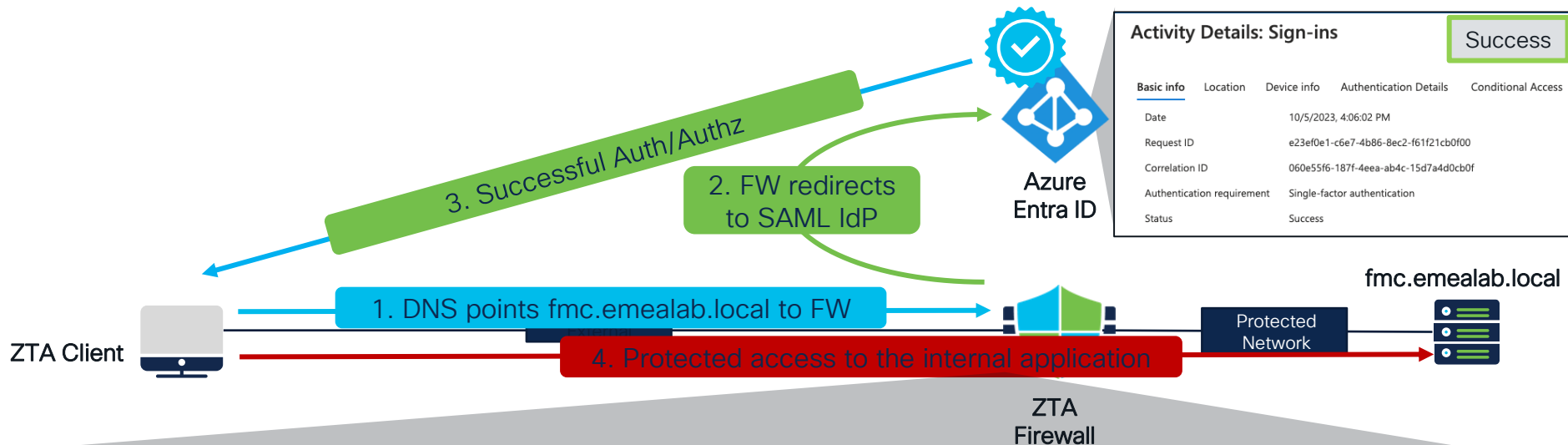


Zero Trust Access – Basic Flow





Zero Trust Access – Successful Auth/Authz



Activity Details: Sign-ins

Success

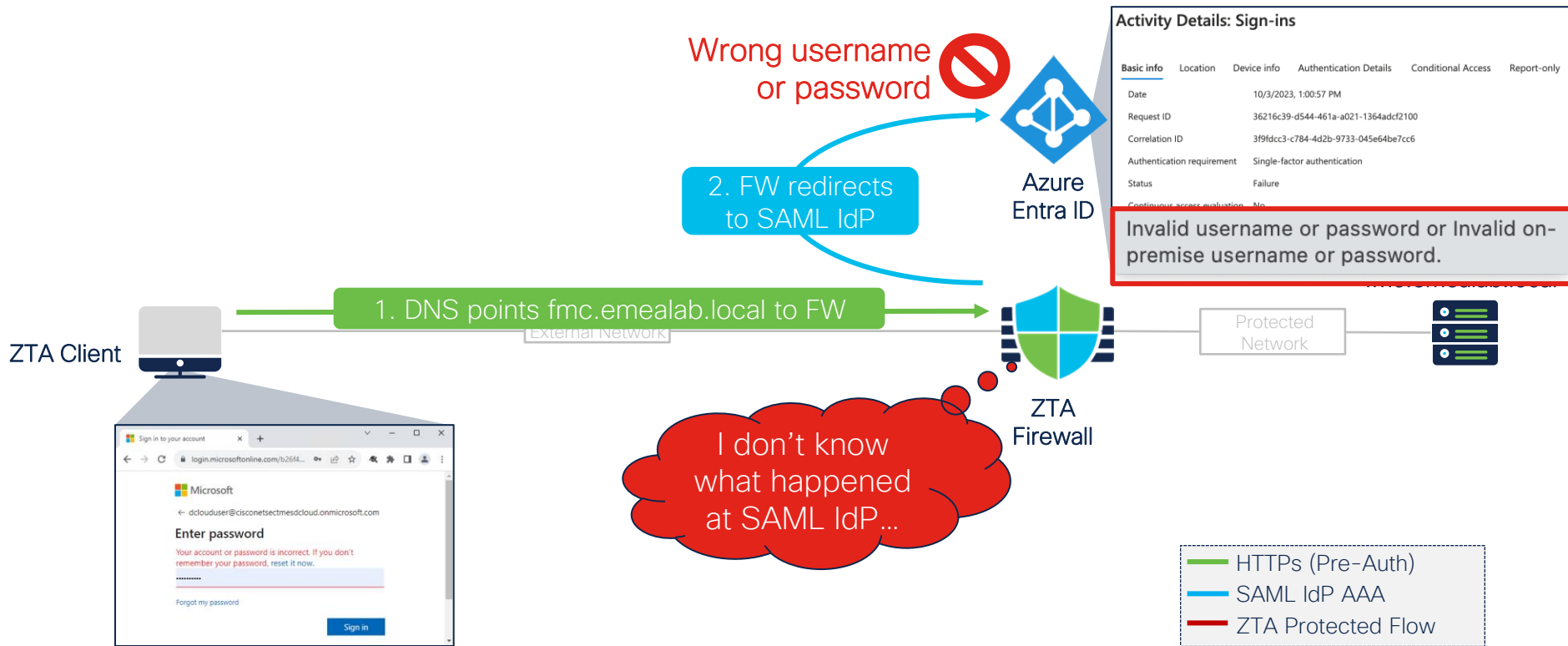
Basic info	Location	Device info	Authentication Details	Conditional Access
Date		10/5/2023, 4:06:02 PM		
Request ID		e23ef0e1-c6e7-4b86-8ec2-f61f21cb0f00		
Correlation ID		060e55f6-187f-4eea-ab4c-15d7a4d0cb0f		
Authentication requirement		Single-factor authentication		
Status		Success		

Firewall Management Center Analysis / Unified Events										
Overview Analysis Policies Devices Objects Integration										
Zero Trust Application N/A										
Showing all 4 events (4)										
Time	Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	Zero Trust Application	Zero Trust Application Group	Zero Trust Application Policy	Source User	
2023-10-06 13:31:48	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@ciconetsectmesdcloud.onmicrosoft.com	
2023-10-06 13:26:20	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@ciconetsectmesdcloud.onmicrosoft.com	
2023-10-06 13:21:37	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@ciconetsectmesdcloud.onmicrosoft.com	
2023-10-06 13:16:29	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@ciconetsectmesdcloud.onmicrosoft.com	

cisco Live!

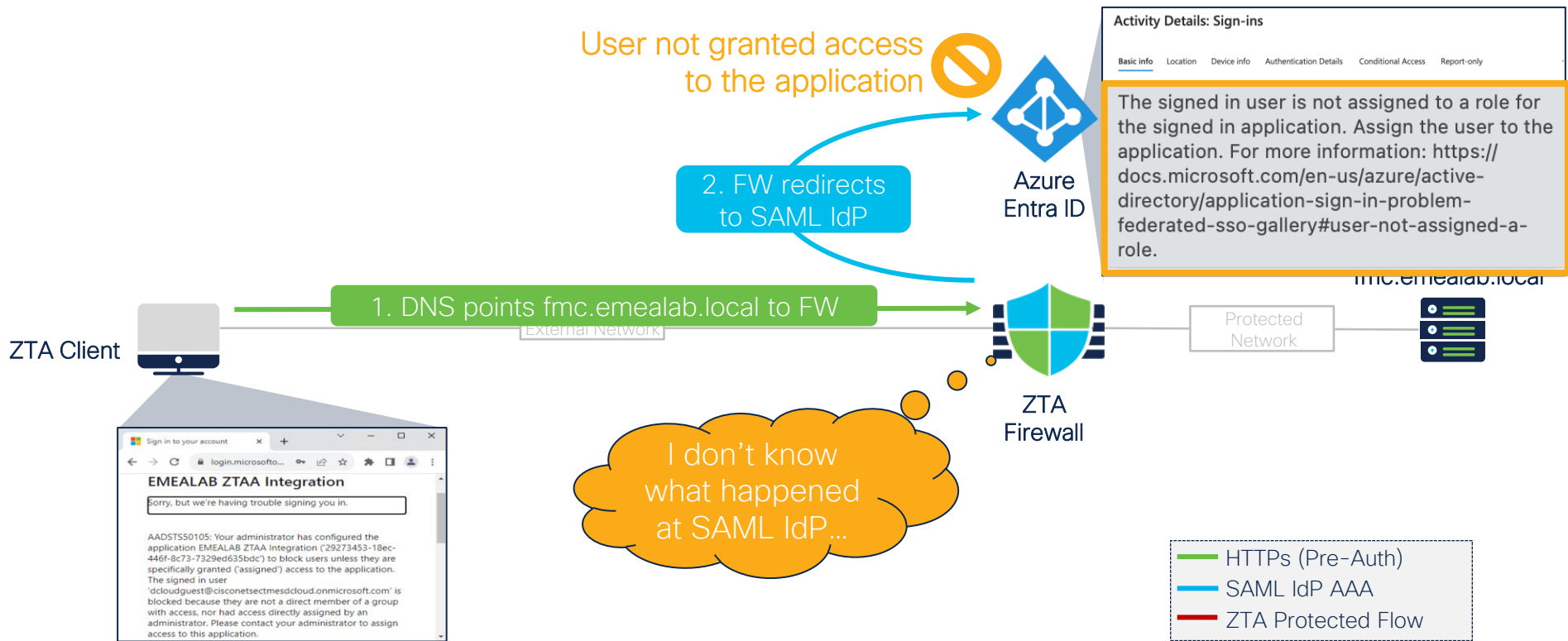


Zero Trust Access – Failed Authentication

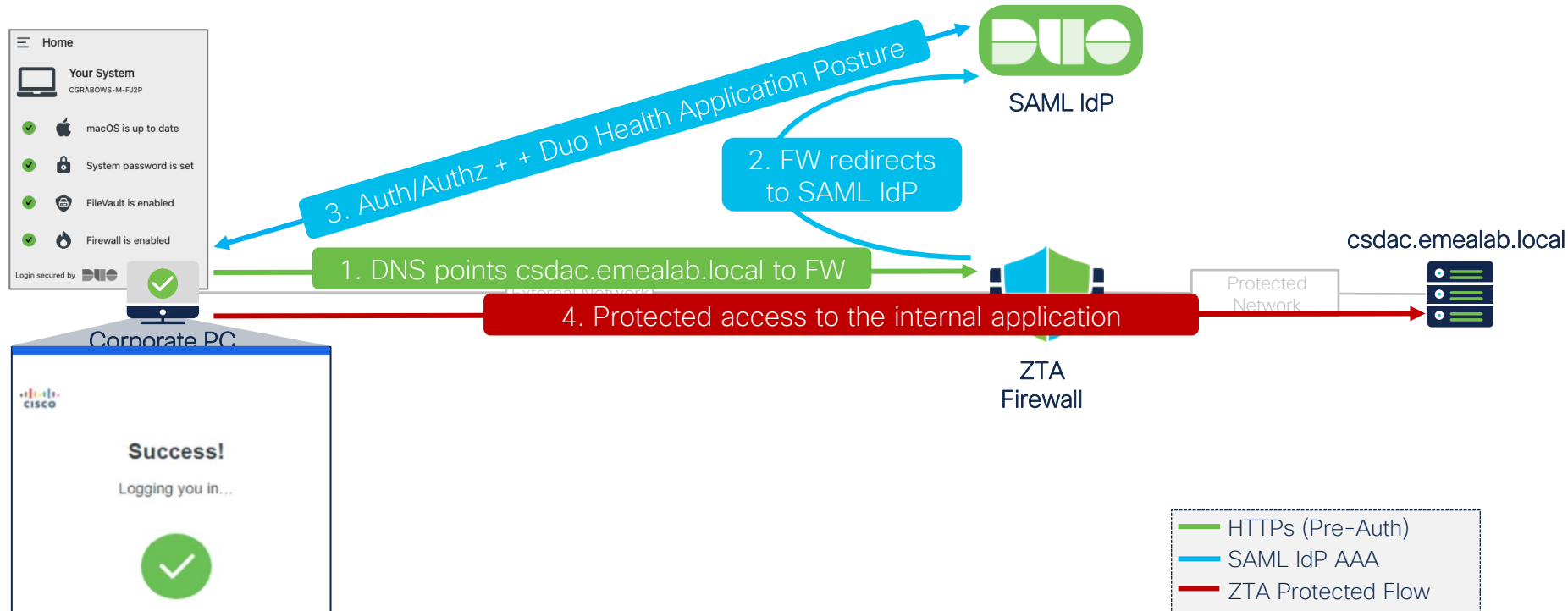




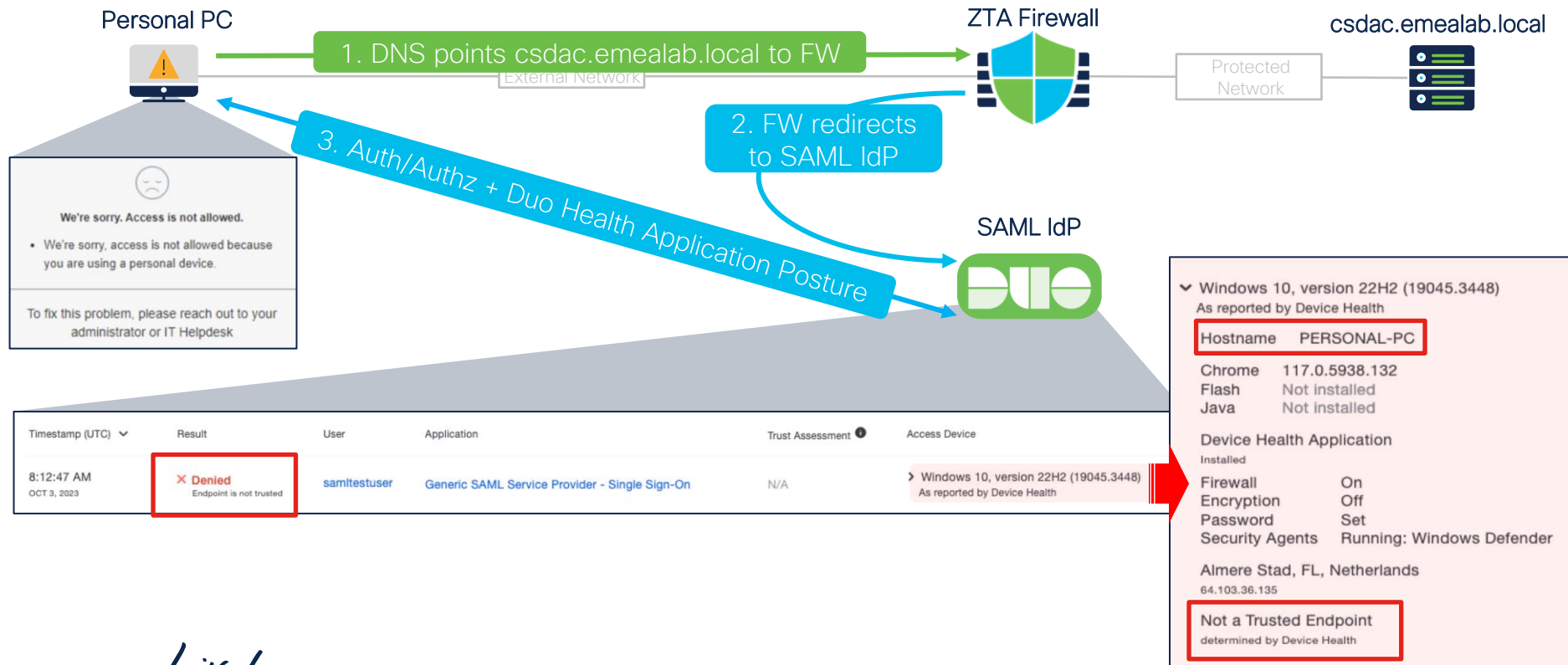
Zero Trust Access – Failed Authorization



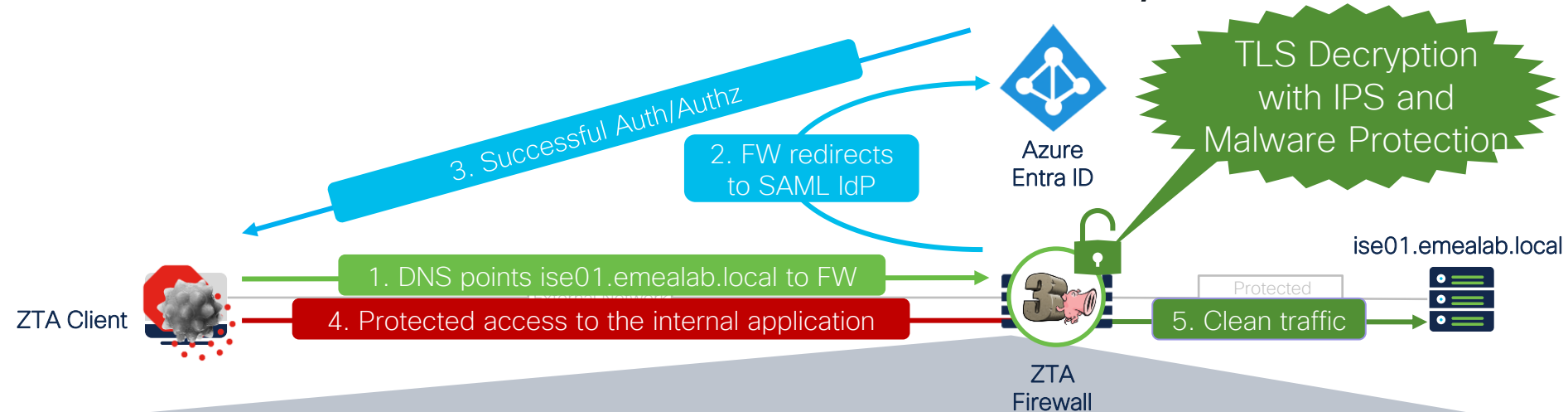
Zero Trust Access – Compliant Endpoint



Zero Trust Access – Non-Compliant Endpoint



Zero Trust Access – Successful Auth/Authz



Firewall Management Center
Analysis / Unified Events

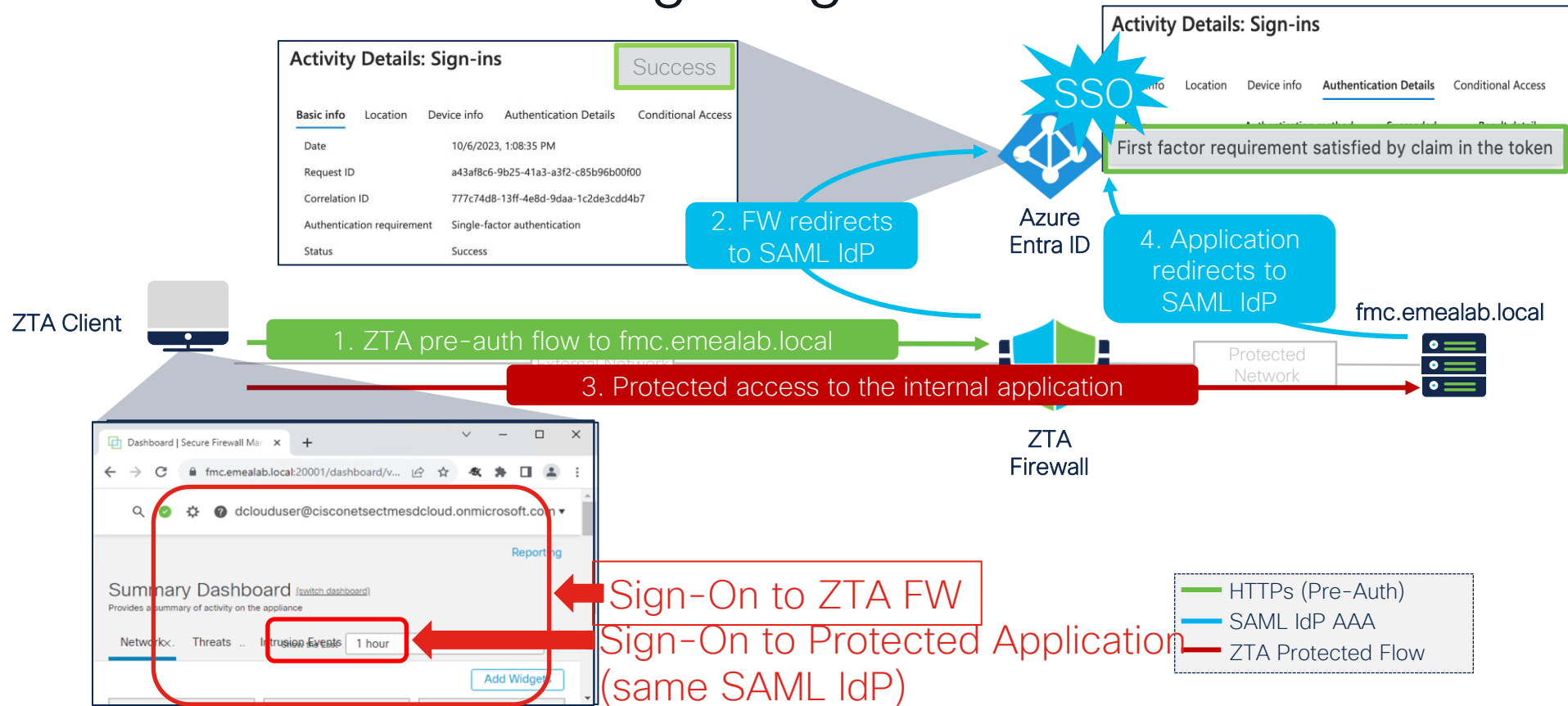
Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin ▾ cisco SECURE

🔍 Event Type Intrusion x Malware x +

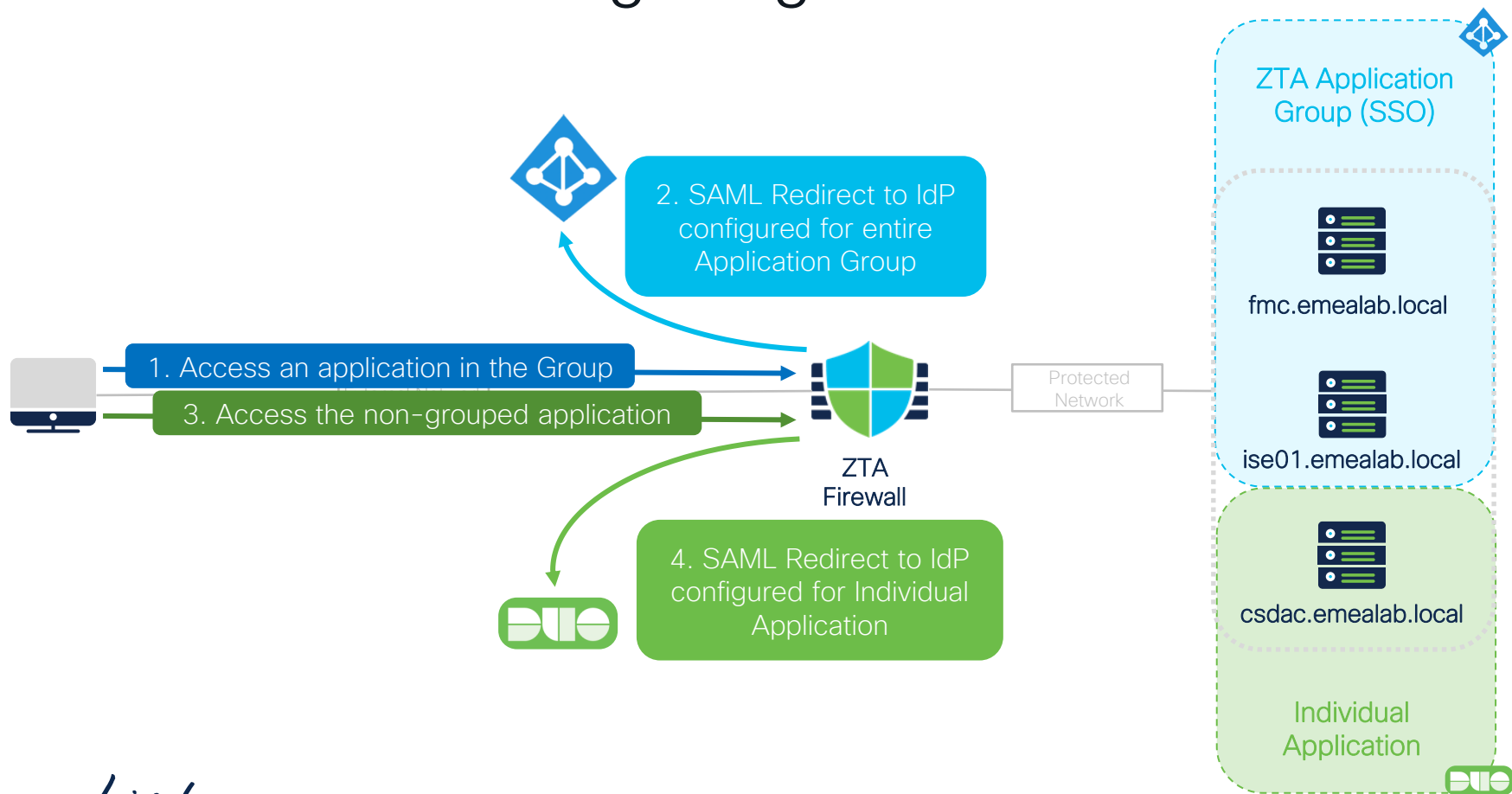
📌 Showing all 27 events (🔴 8 🟡 19) ⬇️ Last 1 month 🟢 Go Live

Time	Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	Source User	
2023-10-03 09:59:30	Malware	Malware Block	172.16.135.101	172.16.134.96	443 (https) / tcp	dclouduser@cisconetsectmesdcloud.onmicrosoft.com	⋮
2023-10-03 09:59:28	Intrusion	Alert	172.16.135.101	172.16.134.96	443 (https) / tcp	dclouduser@cisconetsectmesdcloud.onmicrosoft.com	⋮

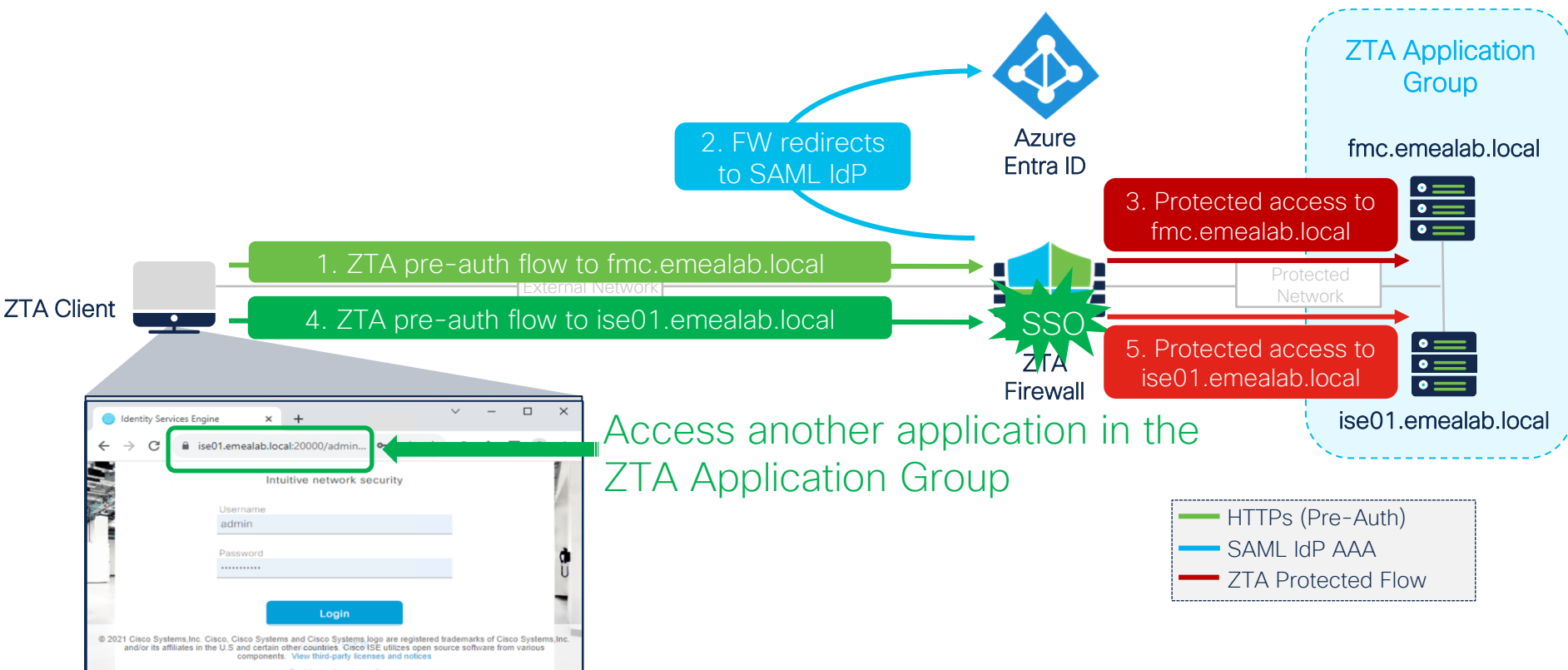
ZTA Clientless - Single Sign-On Flow



ZTA Clientless - Single Sign-On Flow



ZTA Application Group Flow



Zero Trust Access Enhancements in 7.4.1

1. Troubleshoot the zero trust configuration issues using the diagnostics tool

The screenshot displays the Cisco Duo Zero Trust console interface. At the top, there are tabs for 'Applications' and 'Settings'. Below the tabs, there's a 'Bulk Actions' dropdown and a search bar labeled 'Filter by Name, IdP SAML missing, Enabled/Disabled'. To the right of the search bar are two buttons: 'Add Application Group' and 'Add Application'.

The main content area shows a table of applications. The table has columns: Name, External URL, Application URL, SAML Entity ID, Security Zones, Intrusion Policy, Malware and File Policy, and Policy. The applications listed are:

- engineering** (1): External URL: http://www..., Security Zones: BulkZone5 (Inh..., Intrusion Policy: None (Inheri..., Malware and File Policy: None (Inheri...
- wiki**: External URL: https://wiki.acme.com, Application URL: https://internal-..., Security Zones: BulkZone5 (Inh..., Intrusion Policy: None (Inheri..., Malware and File Policy: None (Inheri..., Policy: True
- Un grouped** (2 A):
- concur**: External URL: https://concur.acme.co, Application URL: https...
- payroll**: External URL: https://payroll.acme.co, Application URL: https...

Each application row has a checkbox on the left and a set of icons (refresh, edit, delete) on the right. A green box highlights the 'Diagnostics' button in the top right corner of the application list.

Below the application list, there's a 'Diagnostics: File-Upload' modal window. It has a 'Select Device' dropdown menu with 'CorpHQ-FW' selected. To the right of the dropdown is a 'Run' button. Below the dropdown, there are tabs for 'Report' and 'Logs'. The 'Report' tab is active, showing a green checkmark and the text 'Application Specific Validation' and 'All Checks Passed'.

Zero Trust Access Enhancements in 7.4.1

2. Ability to configure source NAT for an application

Edit Application

Enabled ☒

1 Application Settings

Application Name *

File-Upload

External URL * ⓘ

https://fileupload.tmedemos.com

Application URL (FQDN or Network IP) *

https://fileupload.tmedemos.com

☒ Use External URL as Application URL

By default, External URL is used as Application URL. Uncheck the checkbox to specify a different URL. For e.g., https://10.72.34.57:8443

Application Certificate * ⓘ

tmedemos_ZTNA_App_Cert

IPv4 Source Translation * ⓘ

Ignore source translation

RDApp1

RDApp2

RDSQLServer1

Cancel

Finish

Zero Trust Access - Recommendations

- Only SAML IdPs are supported e.g. Azure AD, Duo, Ping ID, One Login, Okta
- DNS needs to be configured to attract application traffic to the ZTA firewall's interface.
- ZTA application protection supported for Internet and internal access use-case (with proper DNS configuration)
- ZTA is supported on routed mode in HA/Cluster*/Multi-Instance deployments
- License requirements:
 - Essentials license for basic ZTA access
 - IPS and/or Malware Defense for application traffic inspection
 - ZTA does not work in evaluation mode
- ZTA traffic is not subjected to Access Control Policy (ZTA policy takes precedence)

Zero Trust Access - Recommendations

- Supports HTTPs applications only (HTTP, RDP, SSH not supported)
- ZTA supports interactive web applications (requires user SAML login)
- ZTA is not a reverse-proxy:
 - Firewall does not rewrite HTTP requests
 - The flow is based on HTTP redirects
 - TLS decryption is mandatory – Snort validates ZTA HTTP cookie in the HTTP request
- ZTA will not work for non-HTTP traffic tunneled through TCP 443 interface.
- ZTA preserves original client IP address – ensure symmetric traffic between client and application through the firewall (superseded by Source-NAT in 7.4.1)
- A pre-auth certificate matching FQDNs of protected applications is required
- Not supported if protected application redirects between ports or does strict HTTP Host Header validation

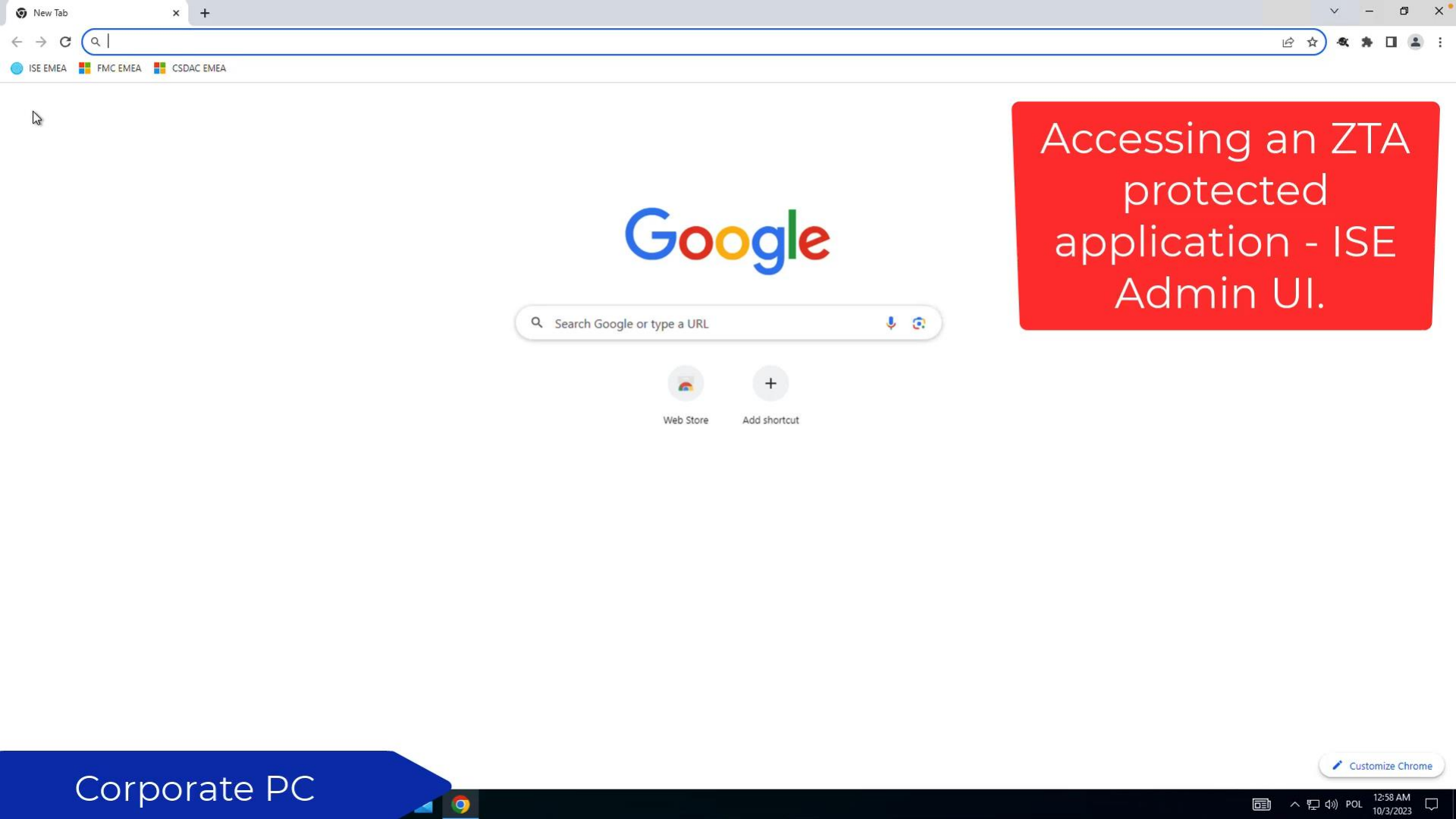
Demo





Corporate PC

Successful Authentication and Authorization



Accessing an ZTA
protected
application - ISE
Admin UI.

Google

Search Google or type a URL



Web Store

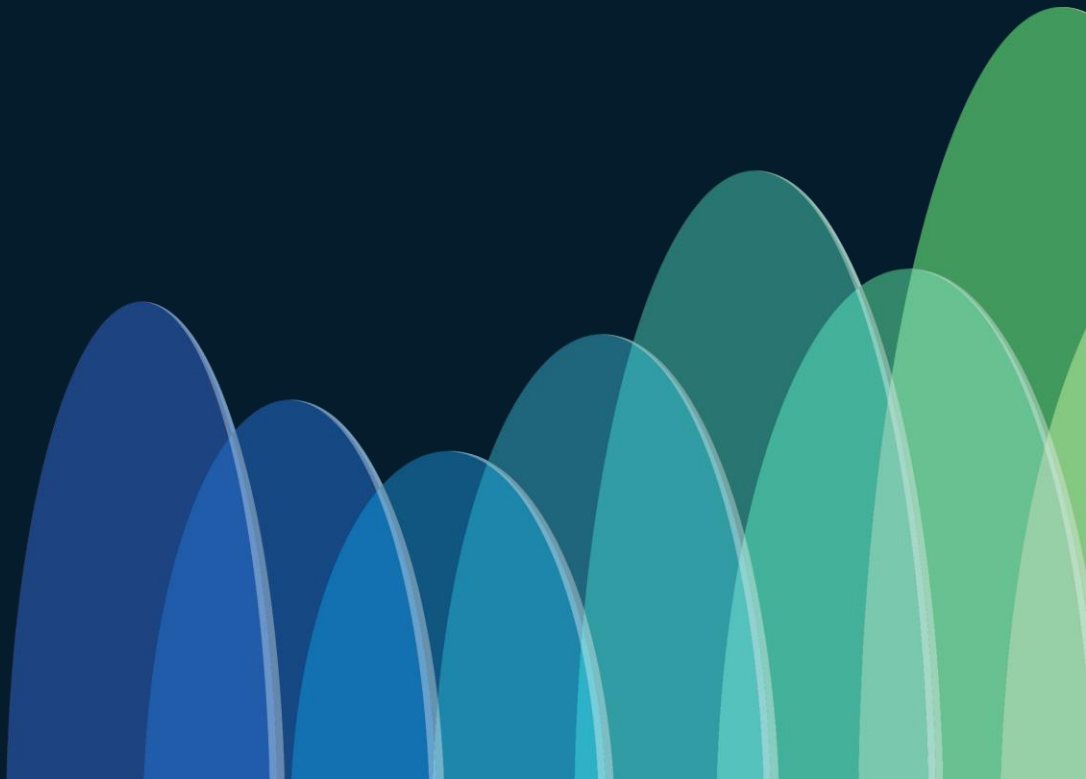


Add shortcut

Corporate PC

Customize Chrome

SD-WAN



SD-WAN Definition

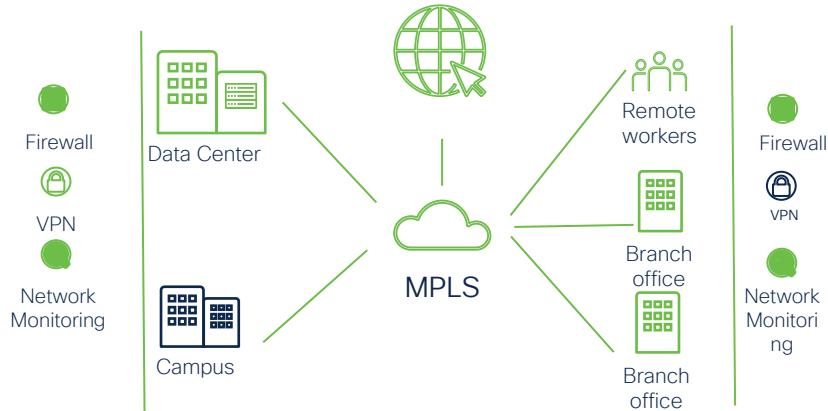
SD-WAN solutions provide a replacement for traditional WAN routers and are agnostic to WAN transport technologies.

SD-WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.

Source: Gartner

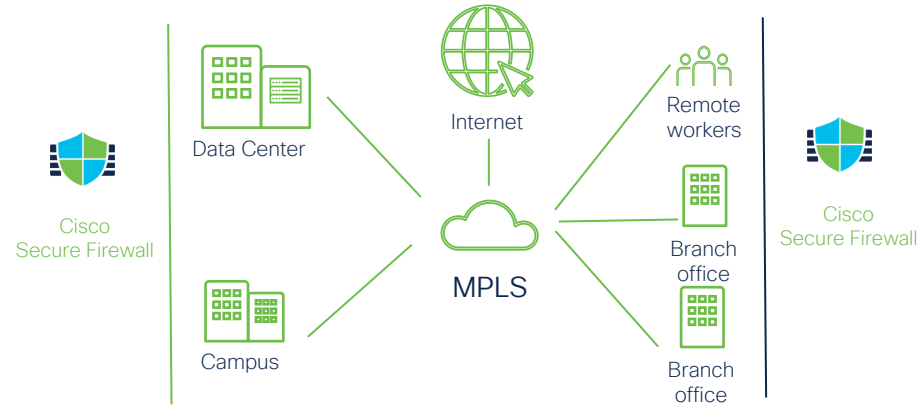
One-box for security and connectivity with SD-WAN

Today



- Direct access to the internet needed for SaaS/cloud apps
- Extensive MPLS circuits, network monitoring tools
- Collapsing appliances & infrastructure at branch for security & routing

1-Box & Management for connectivity and security



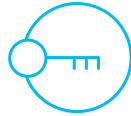
- Direct internet access with advanced threat prevention
- Low-touch central provisioning
- Central dashboard to view statuses, health, and performance

Simplifying Branch Deployments



Secure Elastic Connectivity

- Configure Route-based VPN VTI tunnels between branches (Spokes) to headquarters (Hubs)
- IPv6 VTI with BGP
- BGPv6 over VTI
- EIGRP and OSPF over VTI
- DVTI Support DHCP



High availability with near-Zero Network Down time / WAN Optimization

- Dual ISP configuration
- Active-Standby Backup VTI tunnel configuration with SLA Monitoring
- Optimal Path Selection based on interface monitoring



Increased Usable Bandwidth

- ECMP Support for load-balancing across multiple ISPs
- ECMP Support for VTI
- Application based load balancing using PBR



Direct Internet Access for Public Cloud and Guest Traffic

- SaaS Application detection (First Packet using AVC)
- DNS Snooping using trusted DNS servers
- Policy Based Routing using Application as matching criteria
- Local tunnel ID Support for Umbrella



Simplified Management

- Data Interface Management
- Auto Config Rollback
- SASE: Umbrella Auto-tunnel deployment
- DVTI Hub and Spoke topology simplification
- WAN Monitoring Dashboard

Secure Firewall SD-WAN Features

Feature	Version Introduced
Static Virtual Tunnel Interface (SVTI)	6.7
Backup SVTI	7.0
Direct Internet Access (DIA)/ Policy Based Routing	7.1
ECMP with WAN Interfaces	7.1
ECMP with VTI Interfaces	7.1
Route based VPN with Hub and Spoke Topology	7.2
Support for IPv4 and IPv6 BGP, IPv4 and IPv6 OSPFv2/v3, and IPv4 EIGRP for VTIs	7.2
Direct Internet Access (DIA) with Path Monitoring	7.2
Dynamic Virtual Tunnel Interface (DVTI)	7.3
Umbrella Auto Tunnel	7.3
Loopback interface support for VTI	7.3
Policy-based routing using HTTP path monitoring	7.4
Policy-based routing with user identity and SGTs	7.4
SD-WAN Summary Dashboard	7.4
SD-WAN Configuration Wizard	7.6
Device Templates	7.6
Bulk Preprovisioning using Templates	7.6



No Additional
License

Common Branch Challenges



Complex Deployment



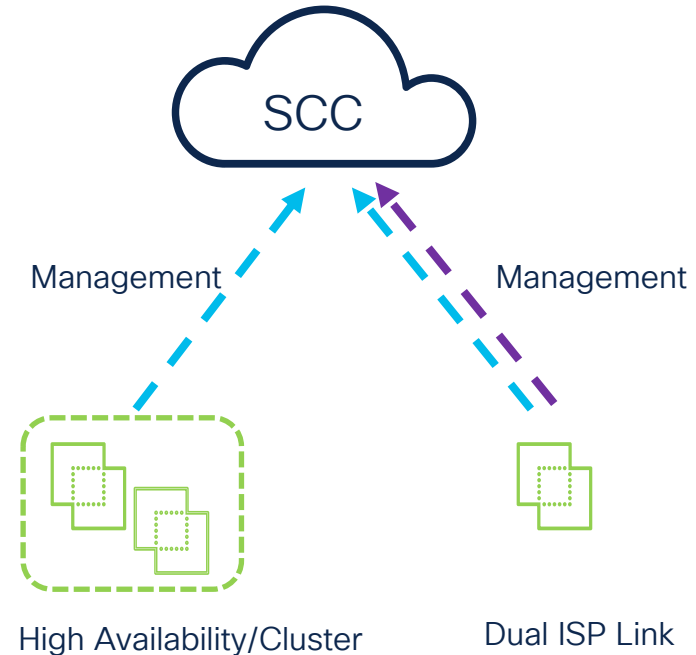
Skilled person on site



Expensive

Cloud-Delivered Firewall Management Center

- Familiar User Experience for existing FMC customers
- Complete feature parity with on-prem FMC's policy management capabilities
- Easy Configuration Migration including Licenses
- Cloud Logging
- Firewall Initiates Management Tunnel over Internet
- CLI and API access
- Ideal for Remote Branches



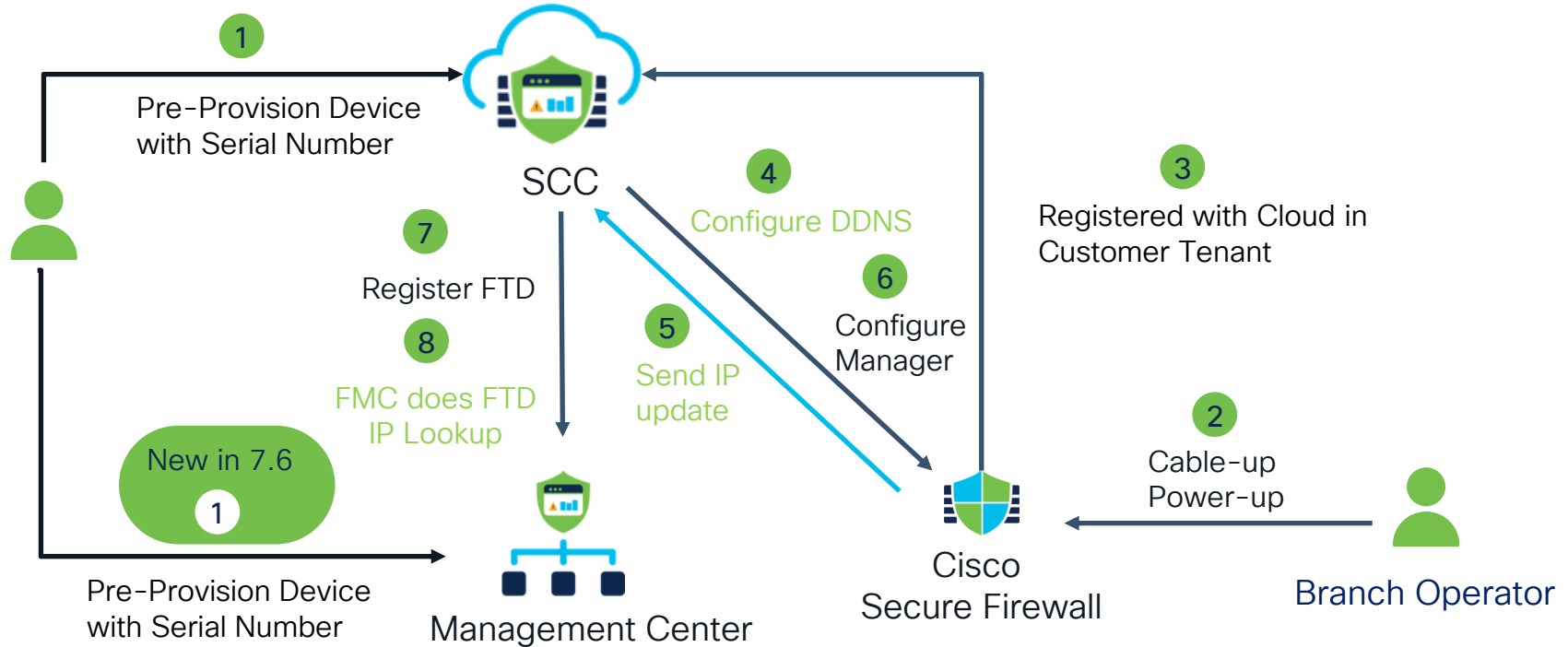
Zero Touch Provisioning Flow

Extend the existing cdFMC LTP workflow to on-prem FMC.

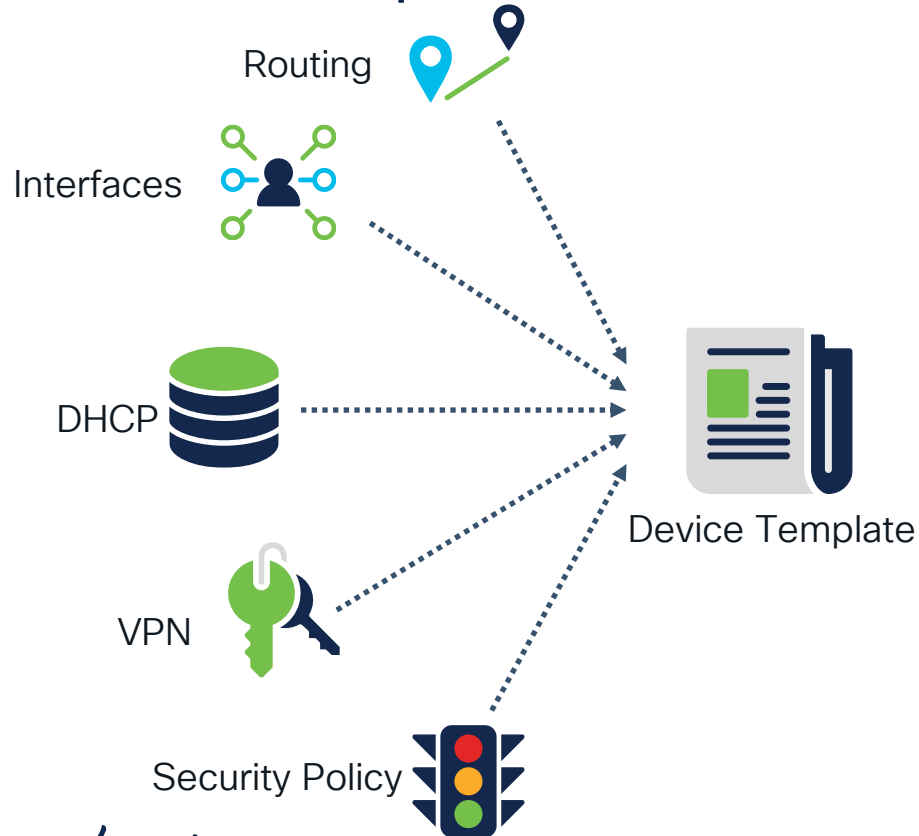


- SCC acts as an orchestrator between FMC and FTD
- FTD configured to update SCC as the provider with any address change
- SCC updates FMC with IP address mapping for its associated FTDs

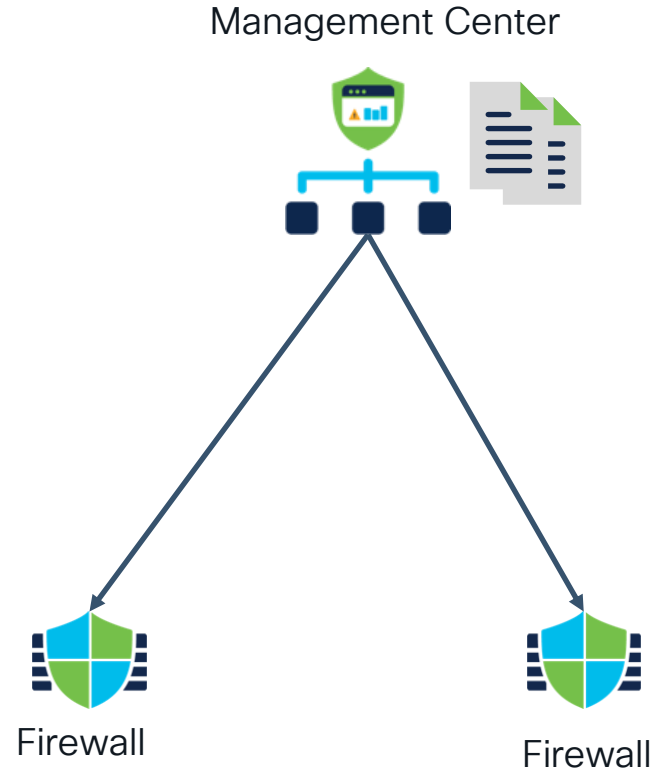
High Level Workflow



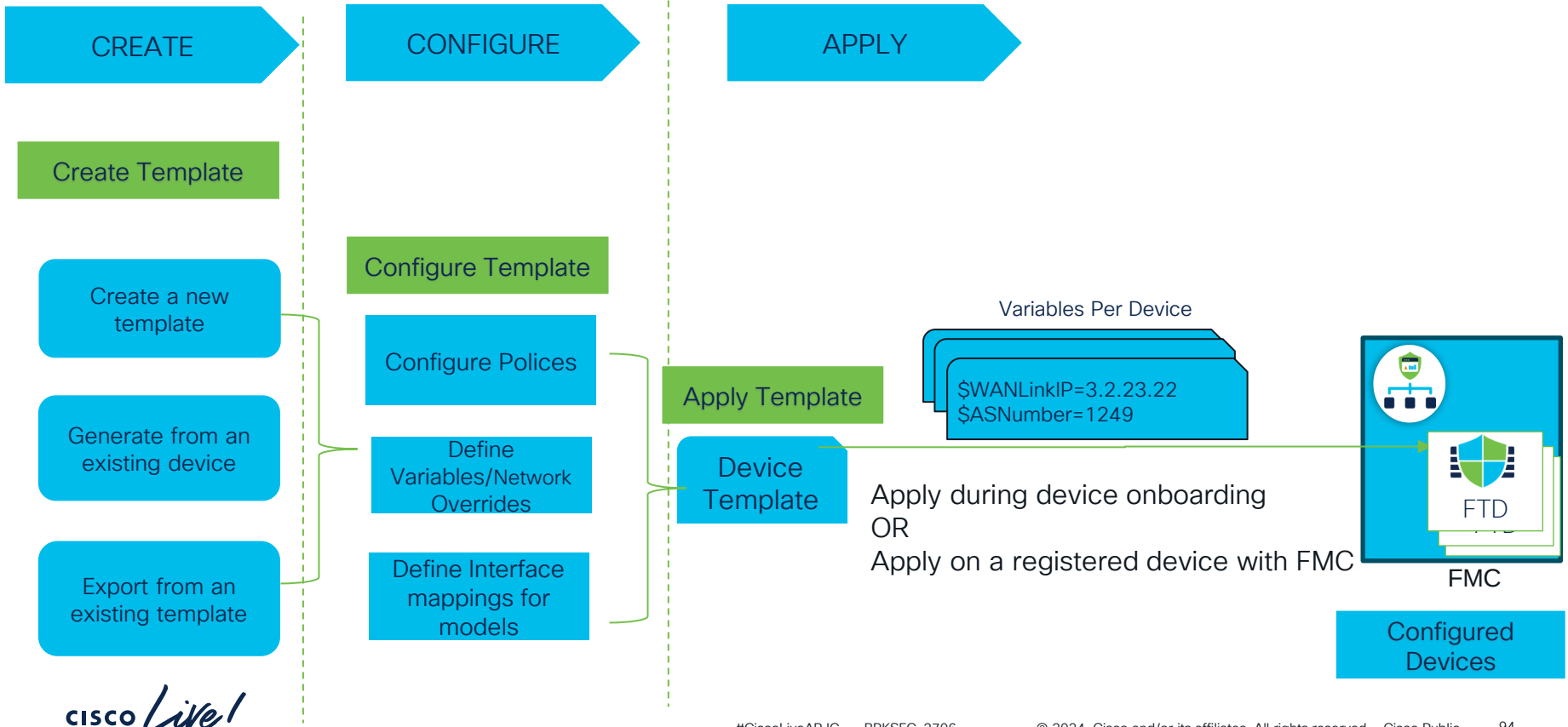
Device Templates



CISCO *Live!*

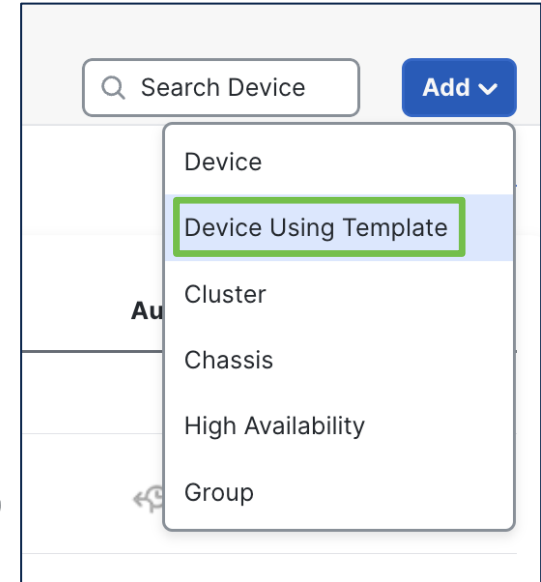


Device Template Workflow

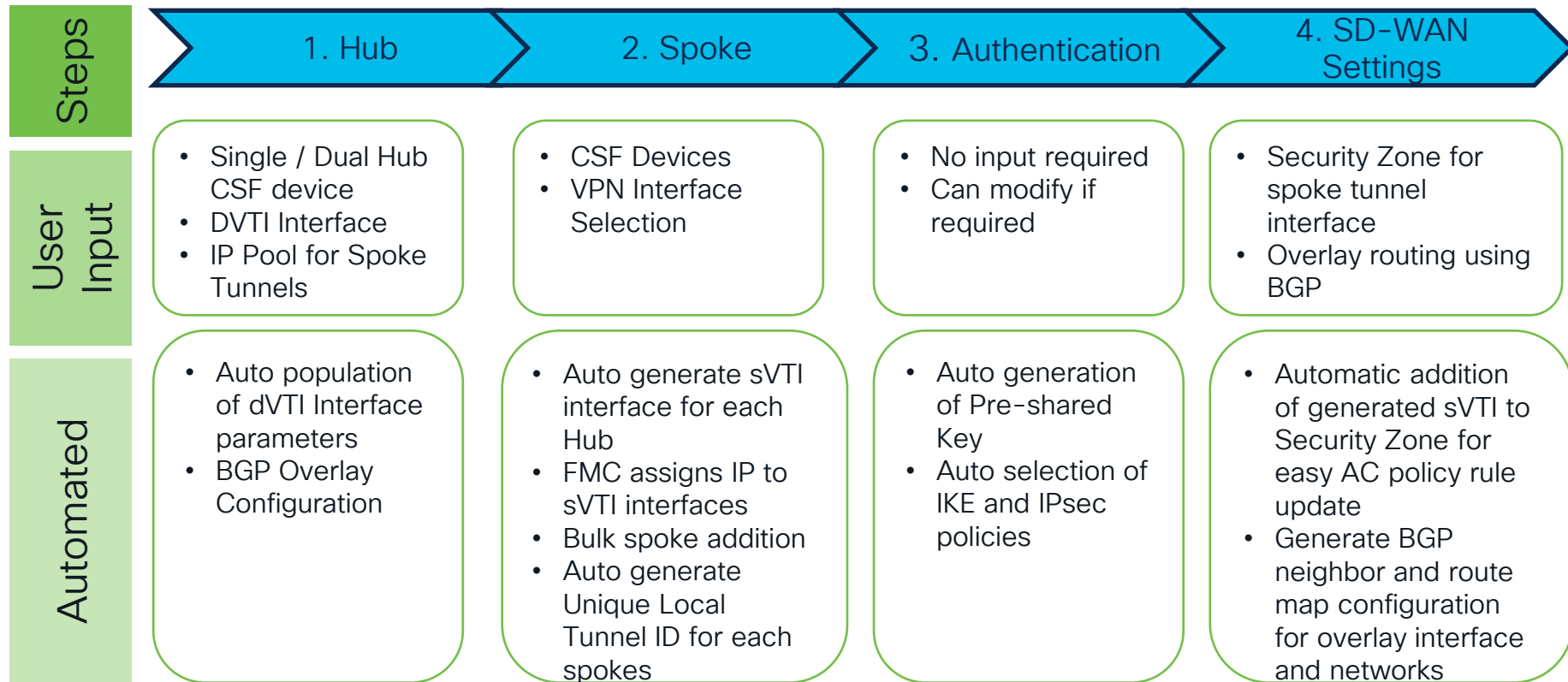


Bulk Pre-Provisioning

- Choose the “Device Using Template” option from ”Add” dropdown in Device Management
- 4 Steps
 - Device Registration Method Selection
 - Domain Selection
 - Template / Access Policy Selection
 - File Upload (for Serial number with template) / Connection Step (for SN with access policy)



SD-WAN Wizard



Create VPN Topology

After clicking Add, a popup dialog, “Create VPN Topology”, appears which simplifies the selection of Topology which user intends to create

- Options:
 - New** SD-WAN Wizard for SD-WAN Topology
 - Route-Based or Policy-Based VPN (launches existing wizard)
 - A SASE Topology (tunnel to Umbrella)
- This dialog validates pre-requisites:
 - Smart License with Export-Control is required for SD-WAN Topology
 - Umbrella Connection Configuration is required for SASE Topology

Create VPN Topology ⓘ

Topology Name *

VPN Type

- ☒ **SD-WAN Topology** New
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
☒ Hub and Spoke
[Prerequisites](#)
- ☐ **Route-Based VPN**
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
- ☐ **Policy-Based VPN**
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
☐ Full Mesh
- ☐ **SASE Topology**

You cannot configure a SASE topology without configuring Umbrella connection settings. [More info](#) [Configure Umbrella Connector](#)

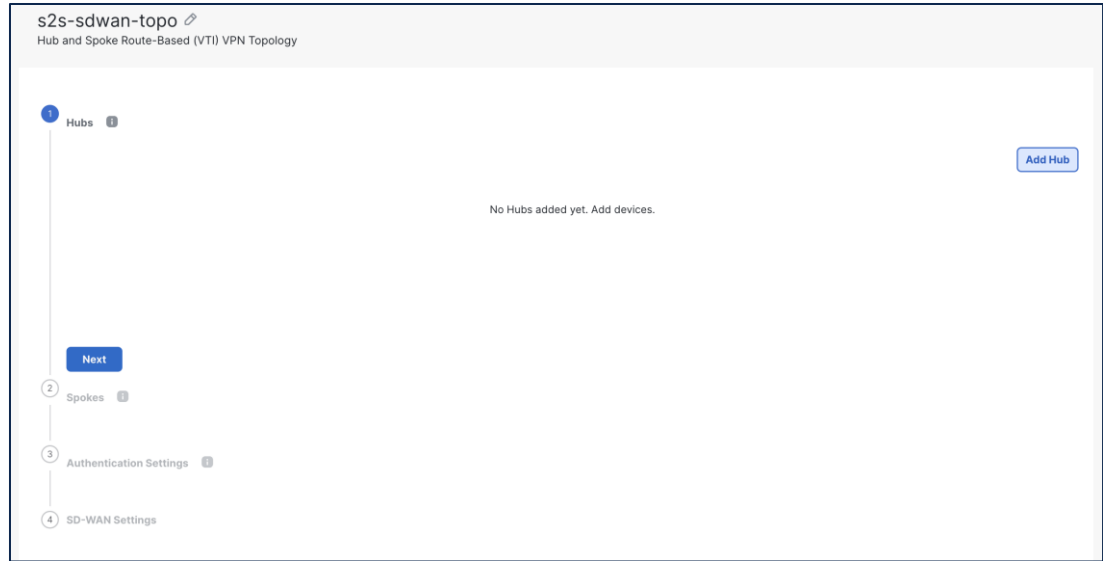
[Refresh](#)

[Cancel](#) [Create](#)

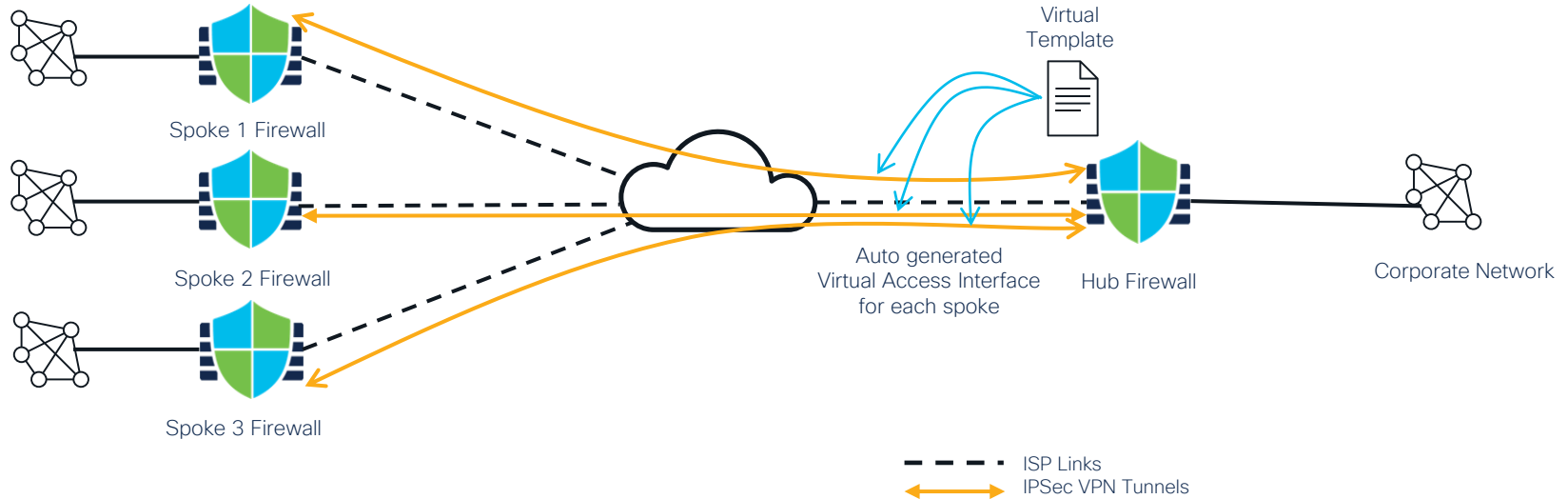
SD-WAN Wizard - Steps

It is a four-step guided Wizard:

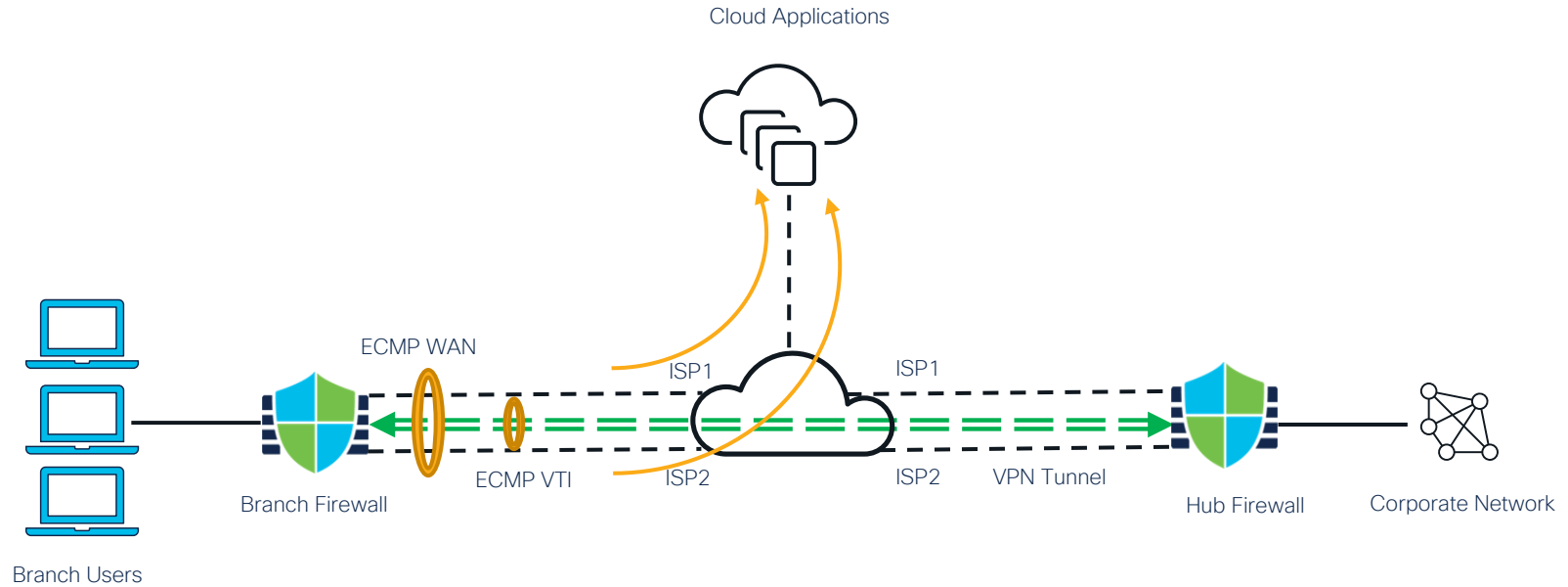
1. Hub Configuration
2. Spoke Configuration
3. Authentication Settings
4. SD-WAN Settings



Simplifying Branch to Hub Communication using Dynamic Virtual Tunnel Interface (DVTI)



Direct Internet Access



- ISP links from Branch FTD to Service Provider
- ↔ VPN Tunnel between Branch and Corporate FTD
- Direct Internet Access Path for Cloud applications

Direct Internet Access

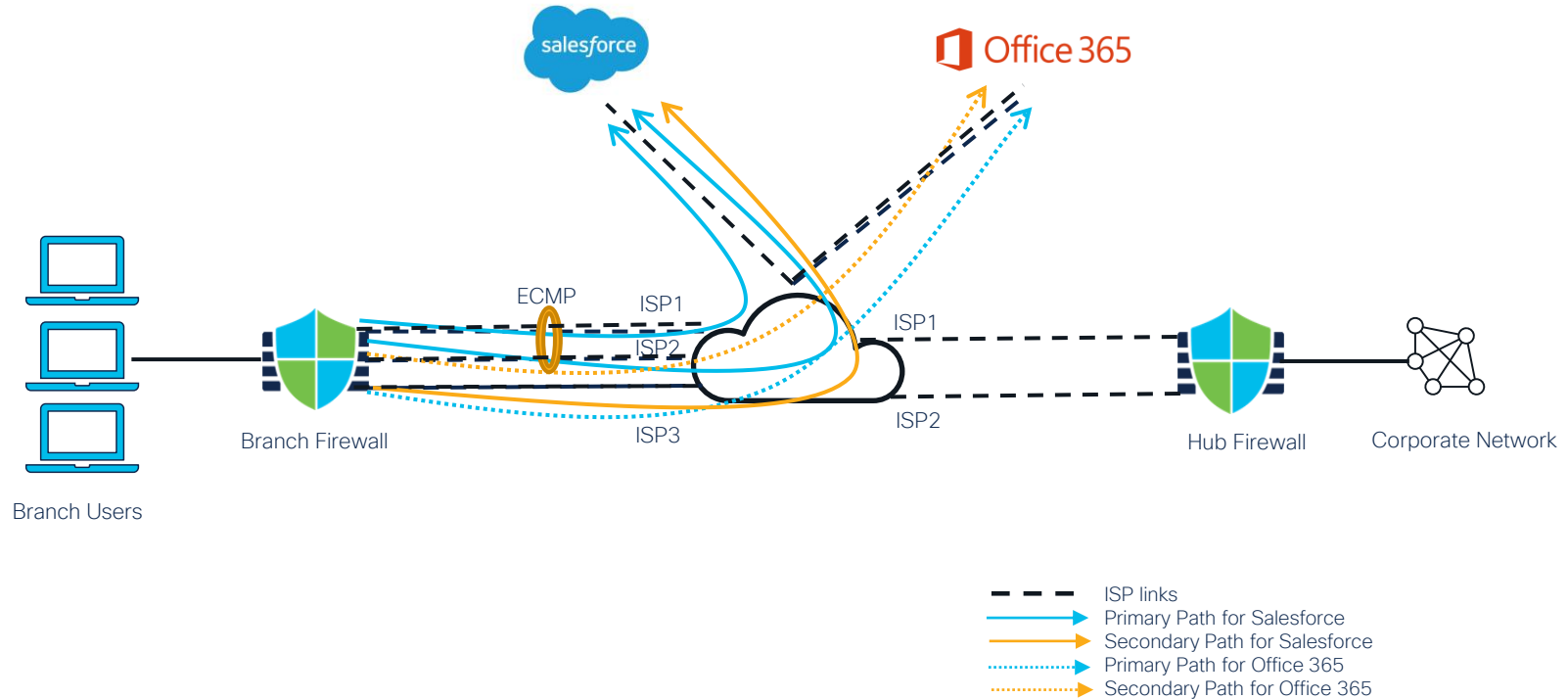
Feature Description

- Routing application traffic directly out to the Internet
- Supporting all SaaS applications
- Traffic steering based on specific applications or networks or users

Benefits

- Cost-effective: reduces bandwidth usage
- Improved branch office user experience
- Simplify network management

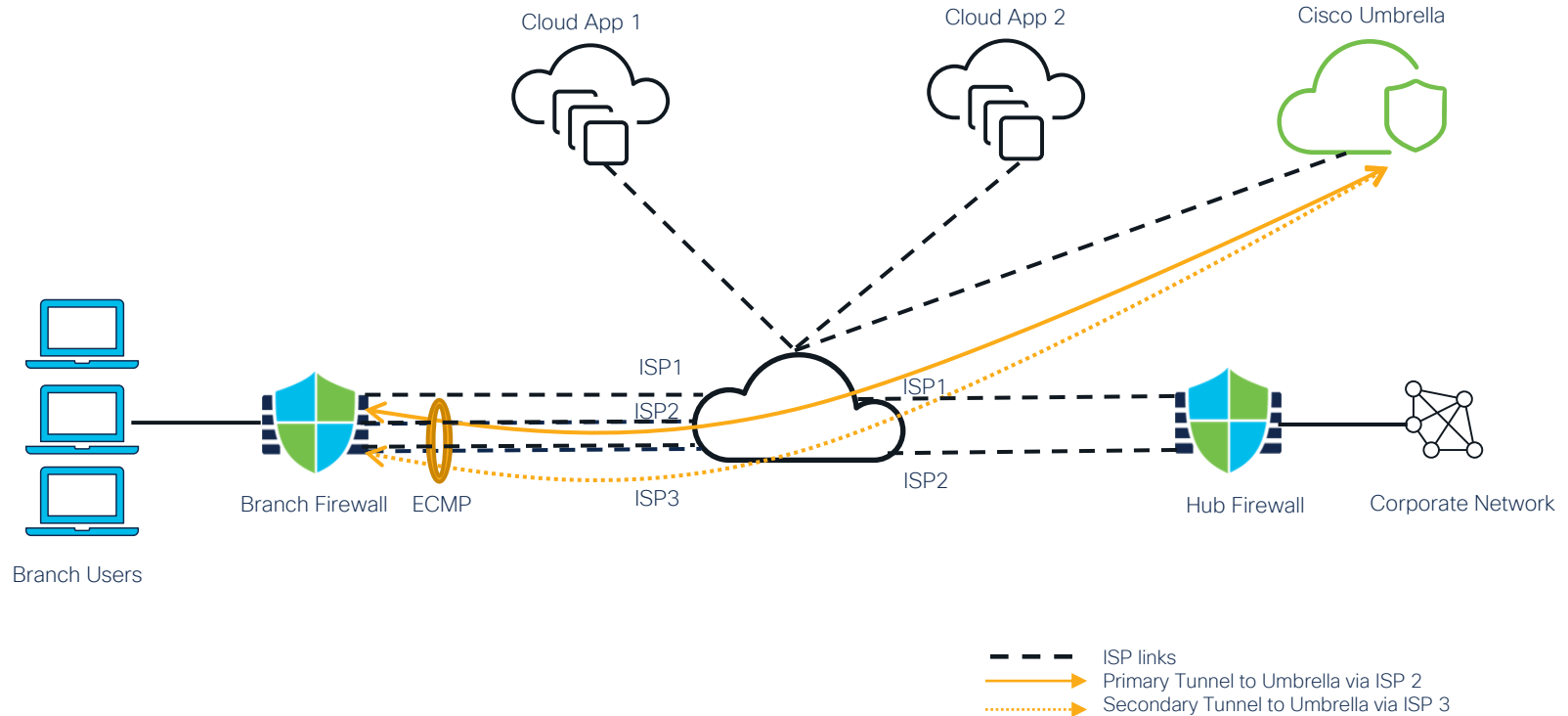
Direct Internet Access with Path Monitoring



Direct Internet Access with Path Monitoring

- Best egress path guaranteed without manual intervention
 - ICMP probes (every 1 seconds)
 - HTTP probes (every 10 seconds)
- Traffic steering based on dynamically monitored metrics
 - Round Trip Time (RTT)
 - Jitter
 - Packet Loss
 - Mean Opinion Score (MOS)
- Path monitoring based on
 - Next-hop (Auto, Auto IPv4, Auto IPv6)
 - An explicit user-configured IP address (Peer-IPv4, Peer-IPv6)

Umbrella SASE Auto Tunnel



Umbrella SASE Auto Tunnel

Feature Description

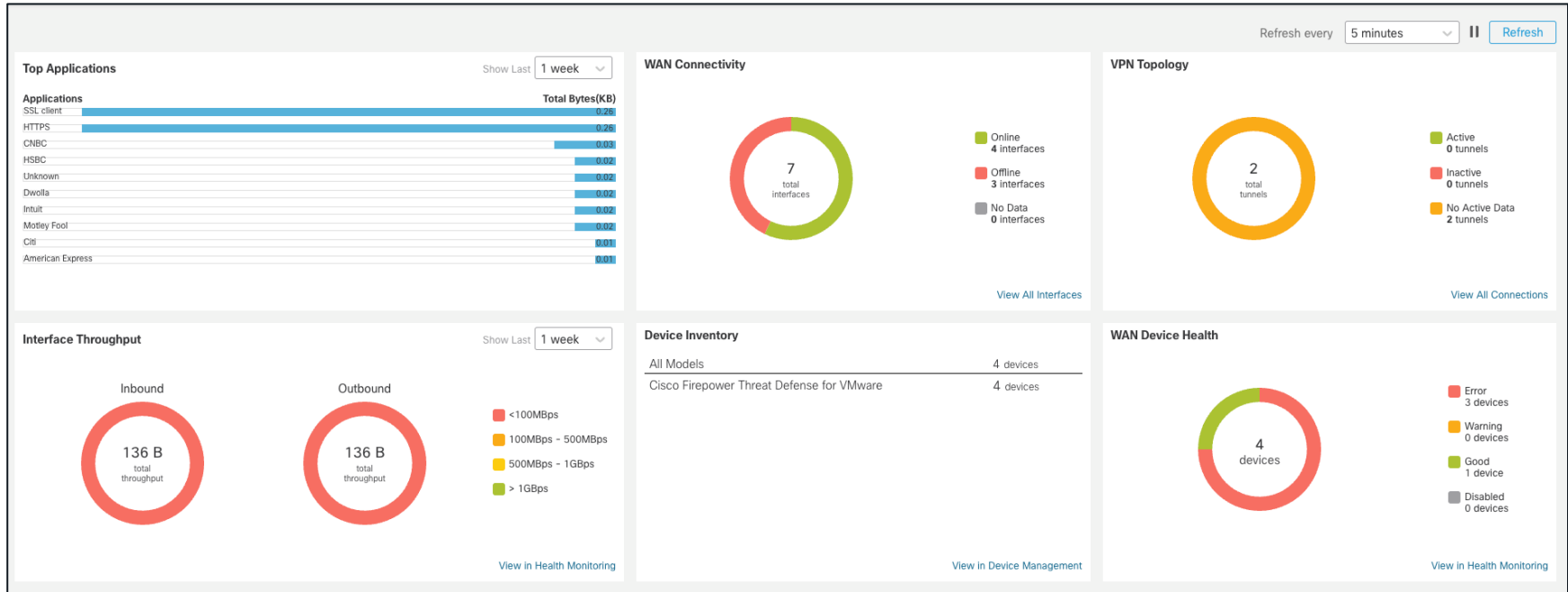
- Simplified workflow for the tunnel between Secure Firewall and Umbrella
- Secures DNS and Web Traffic
- Auto configuration on Cisco Umbrella from Firewall Management Center

Benefits

- Uniform Security policy for branch and hybrid workers
- Improved internet performance
- Reduces configuration overhead

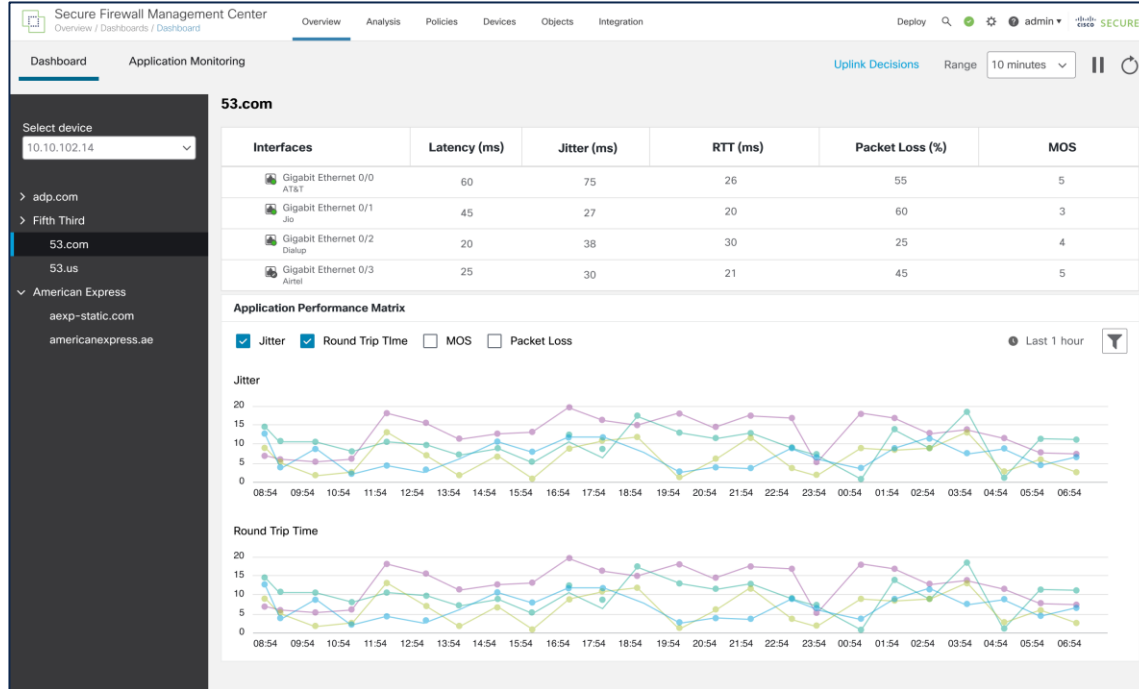
SD-WAN Summary Dashboard

Holistic Overview of Threat Defense Devices part of WAN Deployments



SD-WAN Summary Dashboard

- Application visibility with 7.4.1
- Drill down application performance over a period of time



Key Takeaways

- One box solution for security and connectivity
- Easy onboarding, configuration and management
- Leverage Secure Firewall's advanced security features

Demo



Conclusion

- Firewall is key component of the puzzle in securing the networks
- Supports various integrations with Cisco/3rd party devices
- Provides centralized management with integrated security and threat protection

Cisco Secure Firewall YouTube Channel

[Cisco Secure Firewall YouTube Channel](https://www.youtube.com/@CiscoNetSec)

[Security Cloud Control Playlist on Cisco Secure Firewall YouTube Channel](https://www.youtube.com/@CiscoNetSec)

The screenshot shows the YouTube channel page for Cisco Secure Firewall. At the top, the browser address bar displays the URL <https://www.youtube.com/@CiscoNetSec>. Below the address bar is a search bar and navigation icons. The channel banner features the Cisco Secure Firewall logo on the left and a Cisco Firepower 1000 Series firewall unit on the right. To the right of the banner is a 'NetSec Community' button. Below the banner, the channel name 'Cisco Secure Firewall' is displayed along with the handle '@CiscoNetSec' and '4.78K subscribers'. A 'Subscribed' button is visible on the right. The navigation menu includes links for HOME, VIDEOS, LIVE, PLAYLISTS, COMMUNITY, CHANNELS, and ABOUT. The first video in the 'VIDEOS' section is titled 'Cisco Secure Firewall - 7.3 Release Overview', showing a thumbnail with a man's face and the text 'CISCO SECURE FIREWALL 7.3 OVERVIEW'. The video description states: 'Cisco Secure Firewall • 647 views • 5 days ago. In this video, Alan will walk you through Cisco Secure Firewalls latest release, 7.3, and review some of the highlights. Timestamps: 1:01 - QUIC Fingerprinting (EVE Enhancement) 2:23 -...'

Reference Session

FULL CONFERENCE

IT LEADERSHIP

FULL CONFERENCE PLUS

Keeping Up on Network Security with Cisco Secure Firewall [BRKSEC-2236]



Schedule

Thursday, Nov 14 | 8:30 AM - 10:00 AM AEDT | Room 212

[Andrew Ossipov](#), Distinguished Engineer, Portfolio CTO, Cisco

The network security death rumors are highly exaggerated, and Cisco Secure Firewall is the best proof of all. Whether you are an experienced Firepower aficionado, or someone who is open to trying something new, this session will get you the fix. From a completely transformed management experience, to blazing-fast new hardware platforms, to supporting insertion into complex LAN and WAN topologies, to maintaining visibility in the world of pervasive TLS encryption, there is something for everyone to get at least a little excited about.

Session Type: Breakout

Technical Level: Intermediate

Technology: Security

Session Track: Security

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



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



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



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC