Practical segmentation strategies for every environment

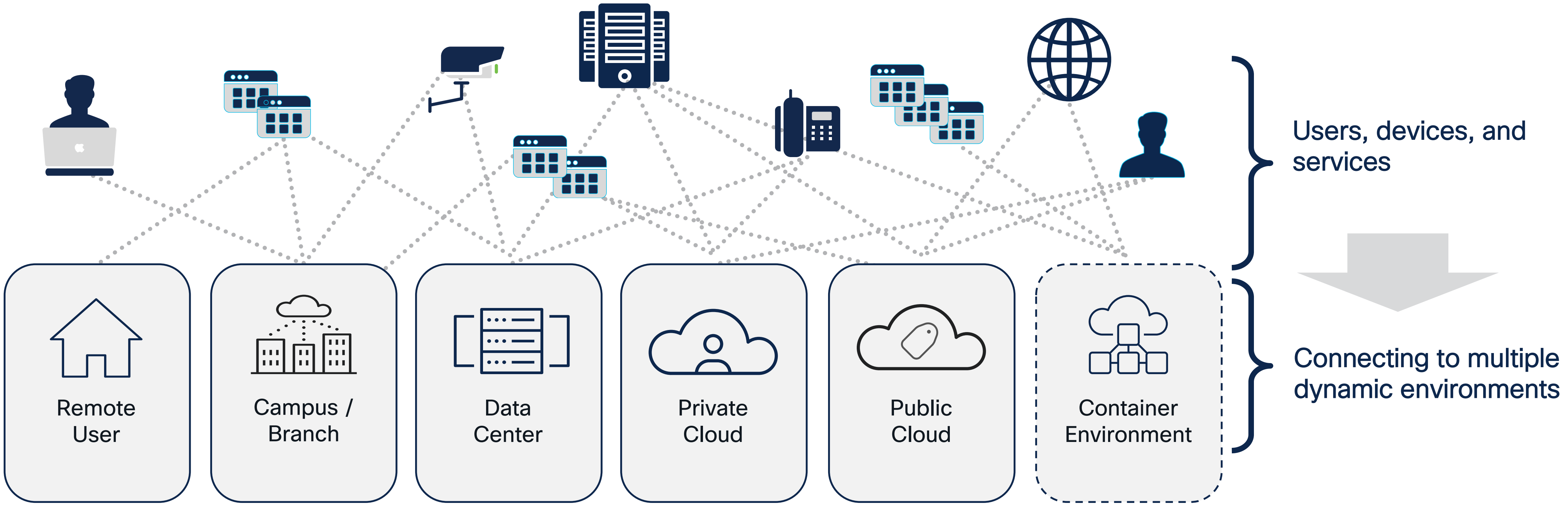
Waris Hussain – wahussai@cisco.com

Ryan Firth - ryfirth@cisco.com

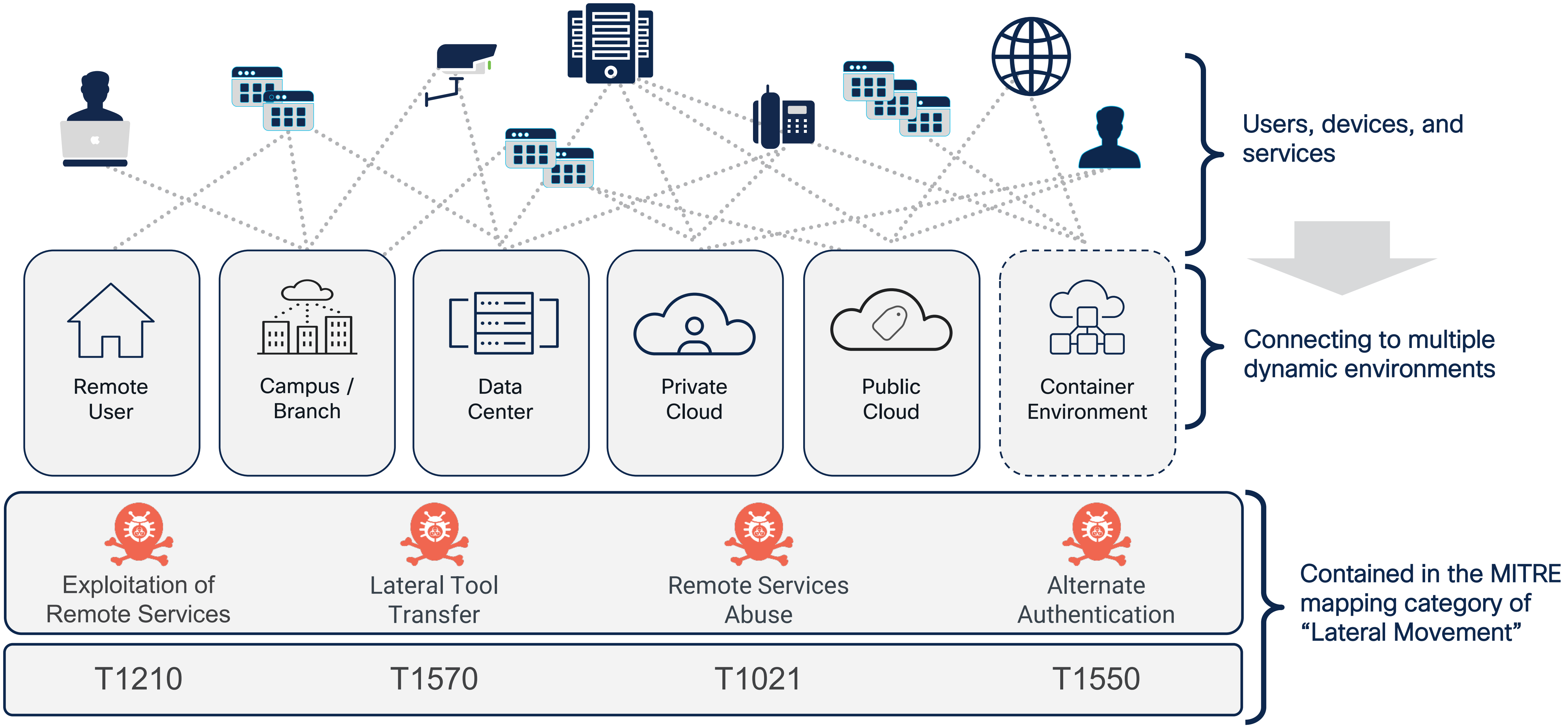
Technical Solutions Architects – US Commercial

December 3rd, 2024

Connectivity requirements today…



…introduce common “Lateral Movement” threats



Users, devices, and services

Remote User

Campus / Branch

Data Center

Private Cloud

Public Cloud

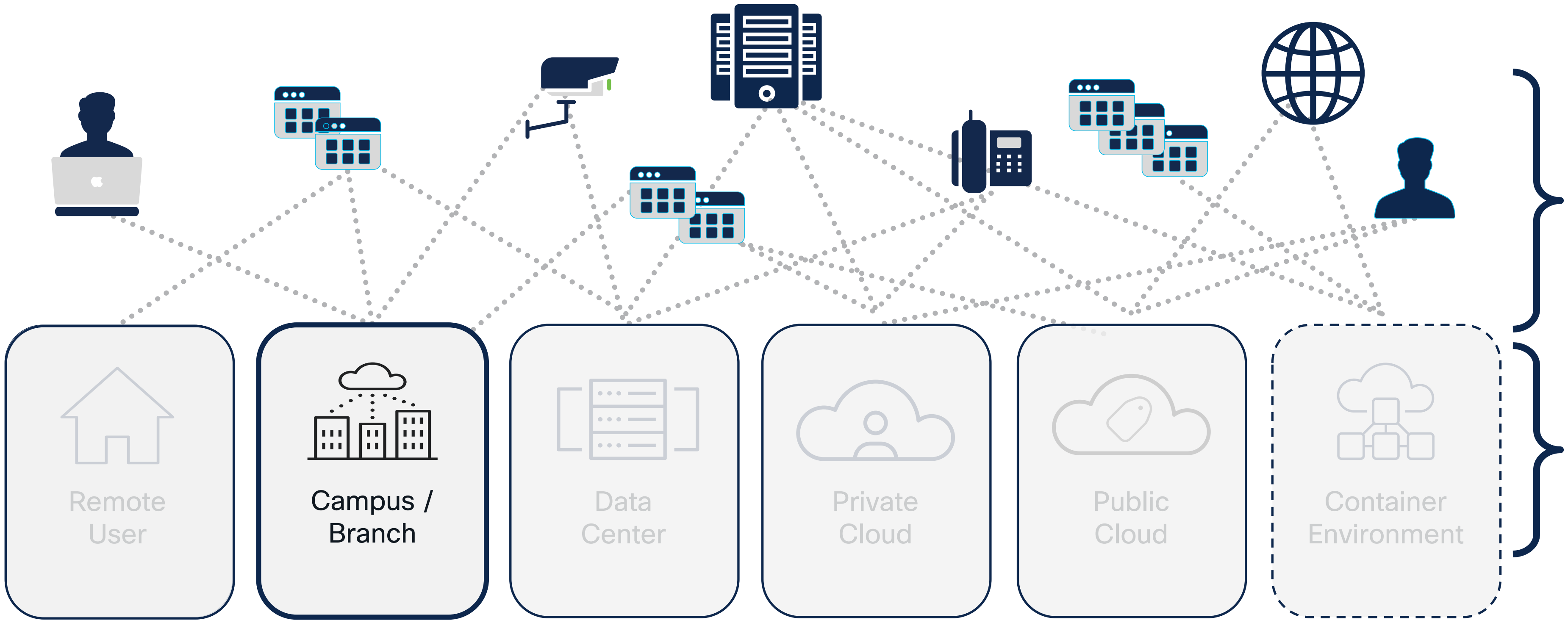
Container Environment

Connecting to multiple dynamic environments

Exploitation of Remote Services	Lateral Tool Transfer	Remote Services Abuse	Alternate Authentication
T1210	T1570	T1021	T1550

Contained in the MITRE mapping category of “Lateral Movement”

…introduce common “Lateral Movement” threats



Remote User

Campus / Branch

Data Center

Private Cloud

Public Cloud

Container Environment

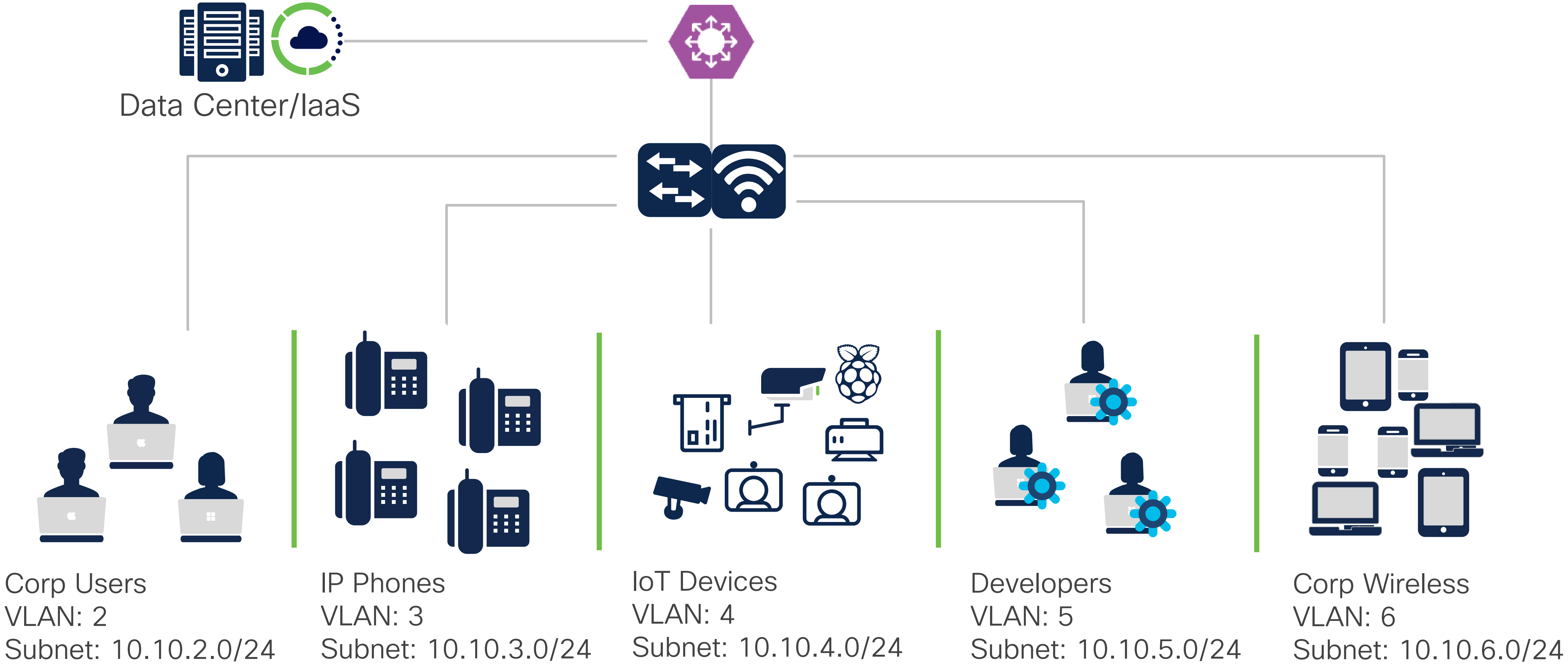
Users, devices, and services

Connecting to multiple dynamic environments

Exploitation of Remote Services	Lateral Tool Transfer	Remote Services Abuse	Alternate Authentication
T1210	T1570	T1021	T1550

Contained in the MITRE mapping category of “Lateral Movement”

Common campus segmentation



Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

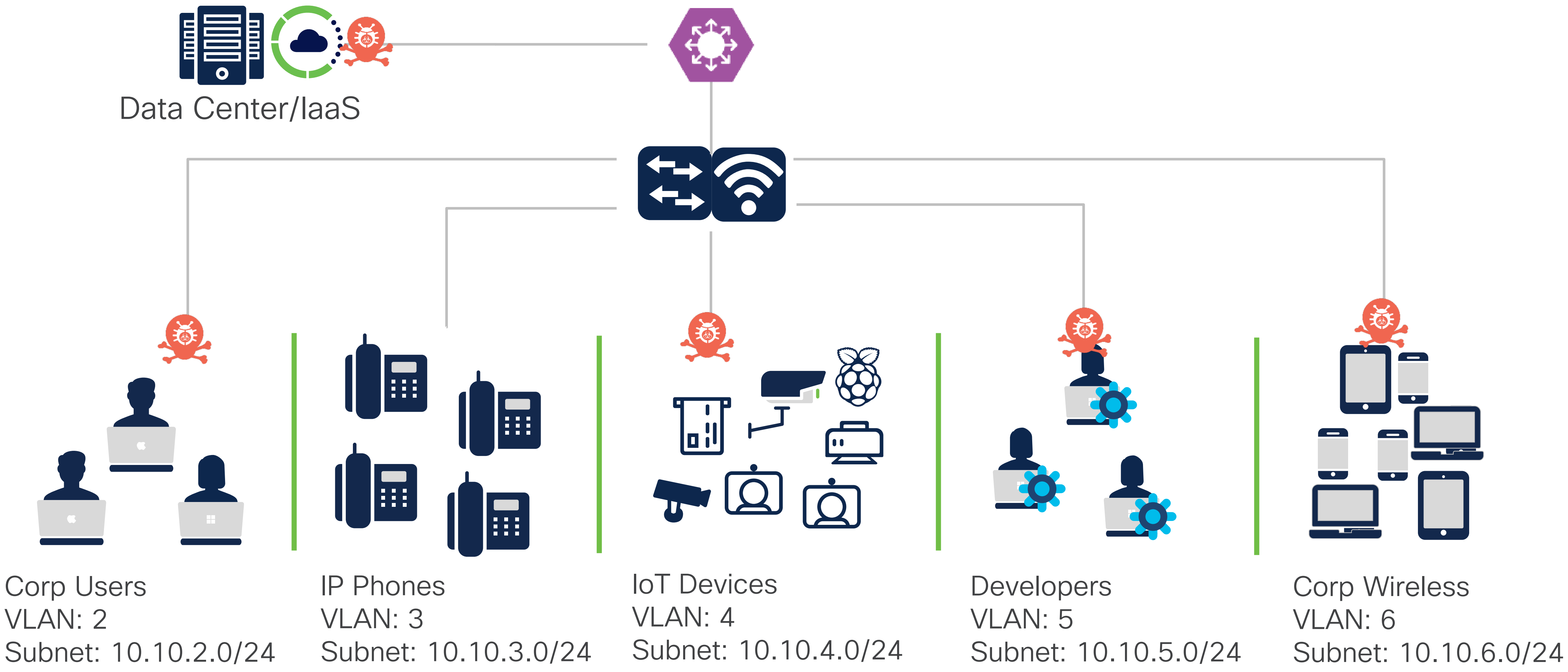
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Common campus segmentation



Data Center/IaaS

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

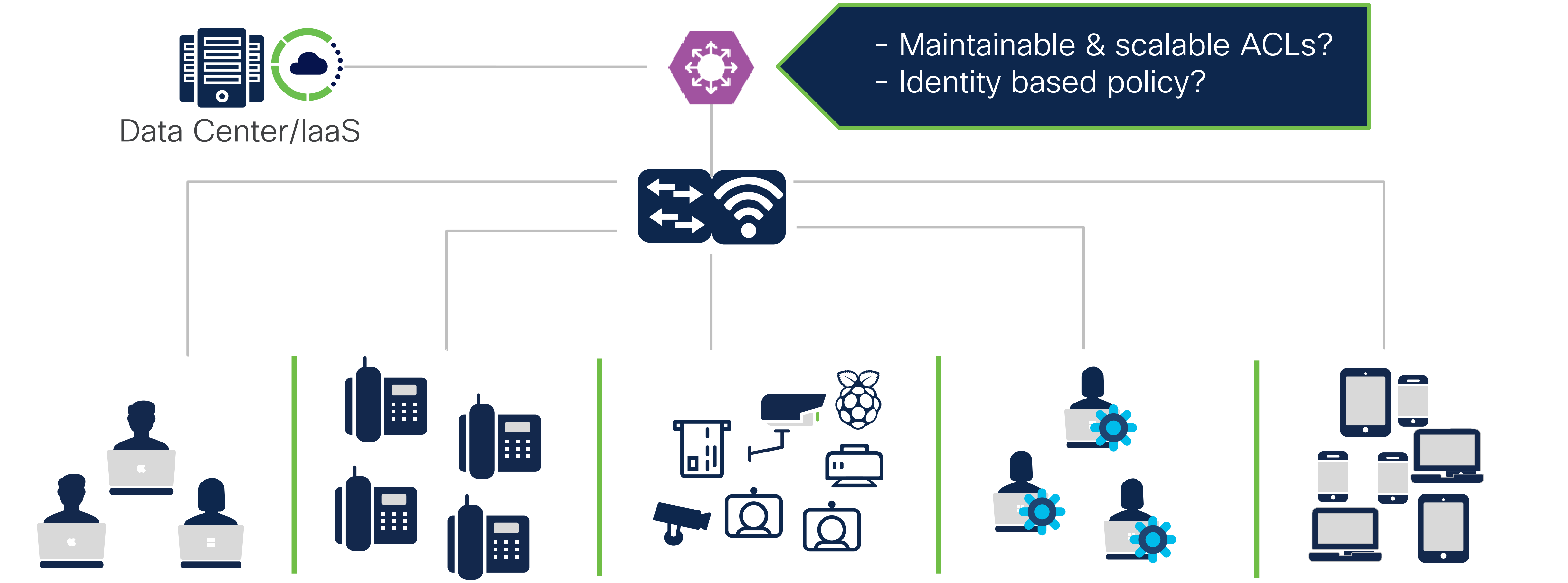
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Common campus segmentation



- Maintainable & scalable ACLs?
- Identity based policy?

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

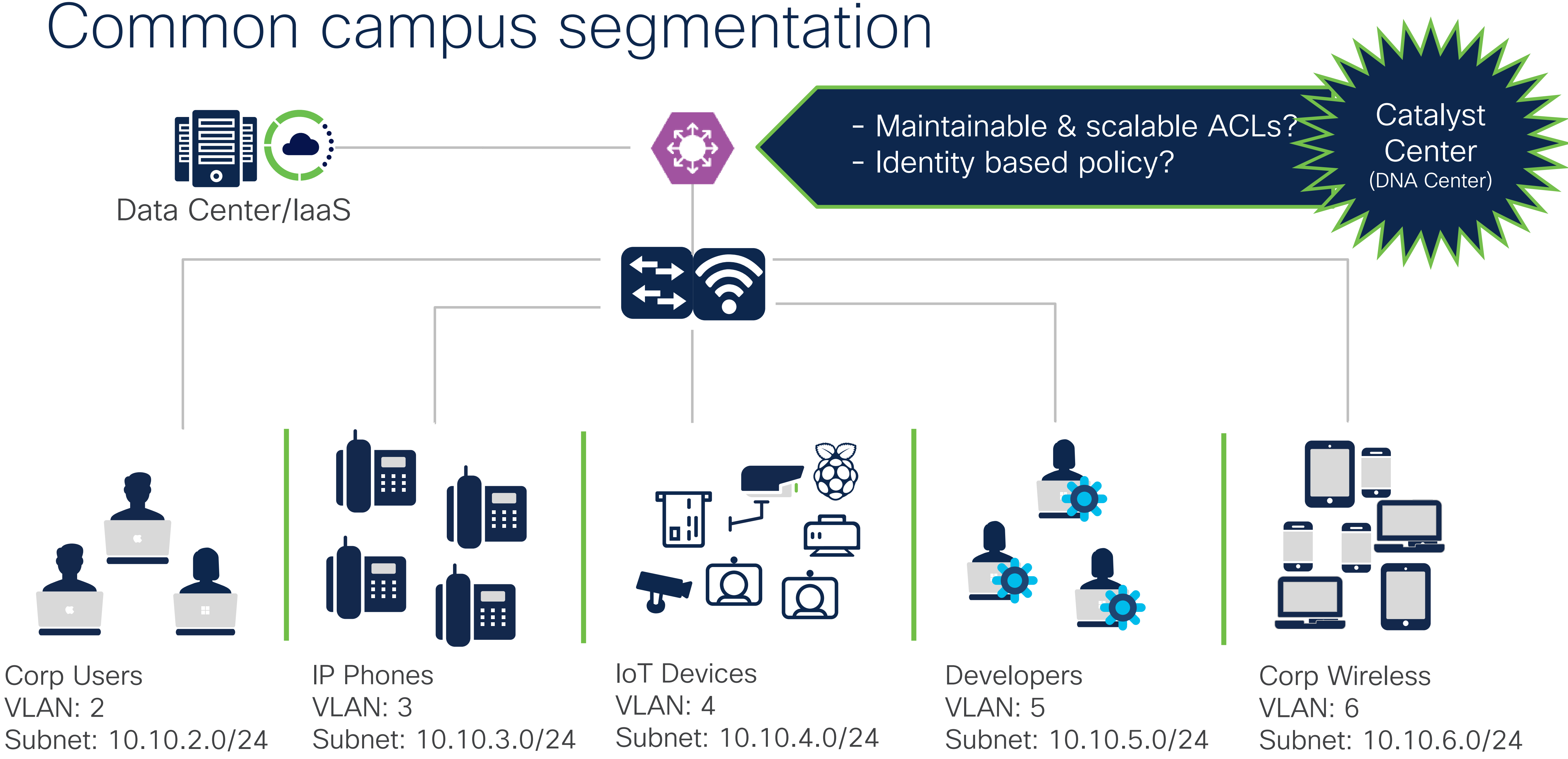
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Common campus segmentation



Data Center/IaaS

- Maintainable & scalable ACLs?
- Identity based policy?

Catalyst Center
(DNA Center)

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

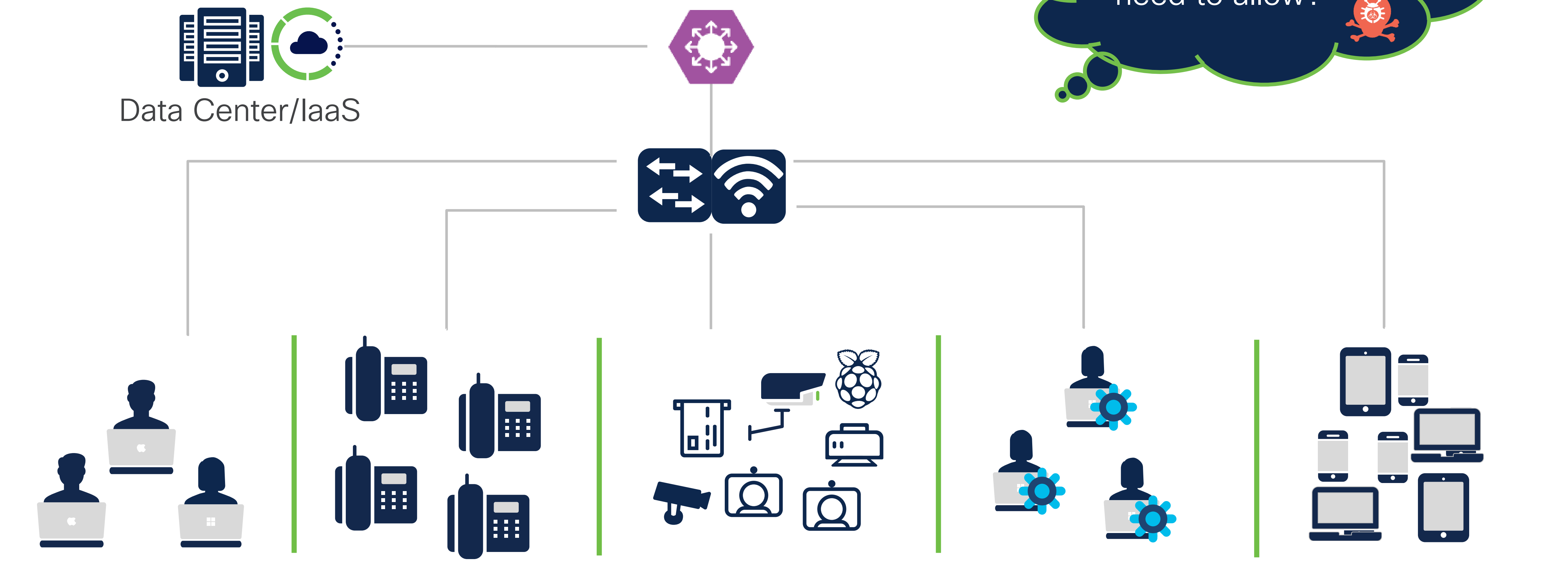
IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Common campus segmentation

What about traffic we need to allow?



Data Center/IaaS

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

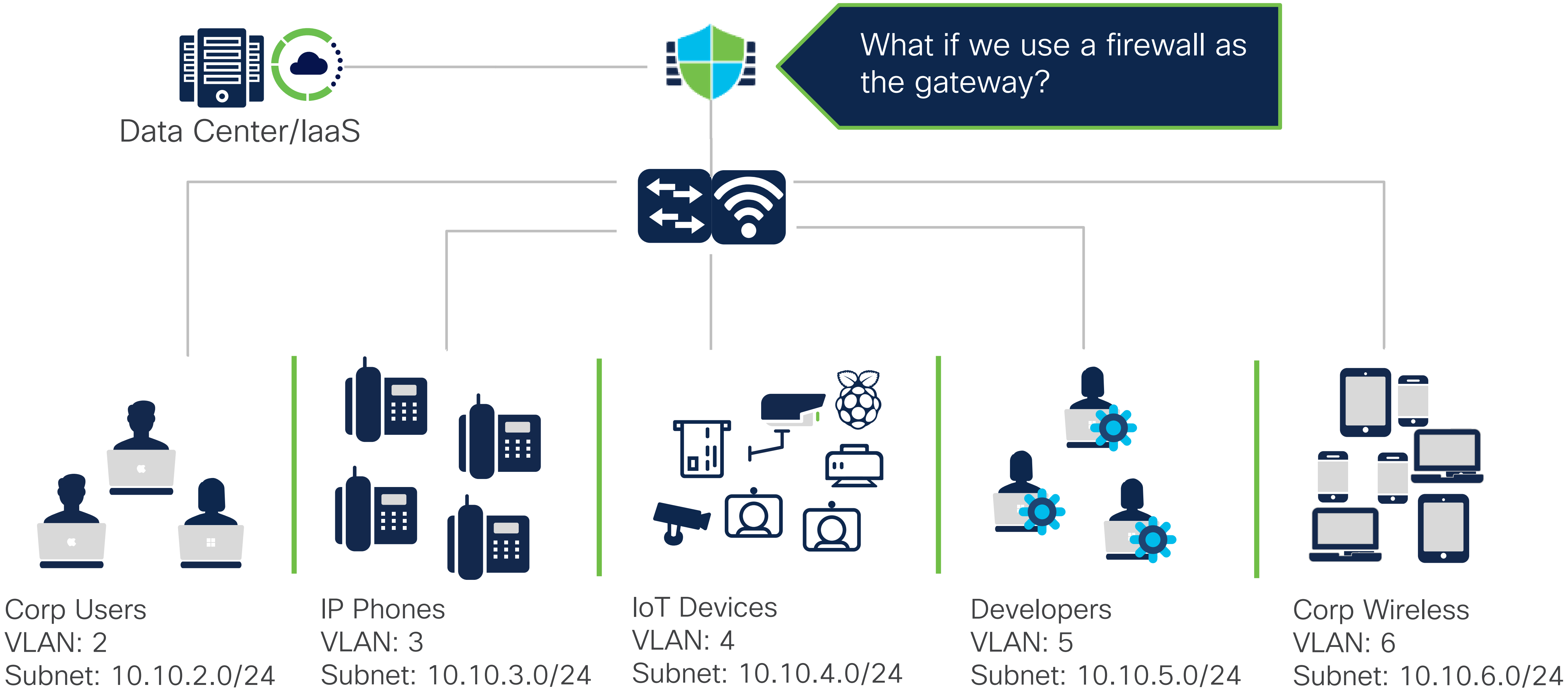
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Macro-segmentation



What if we use a firewall as the gateway?

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

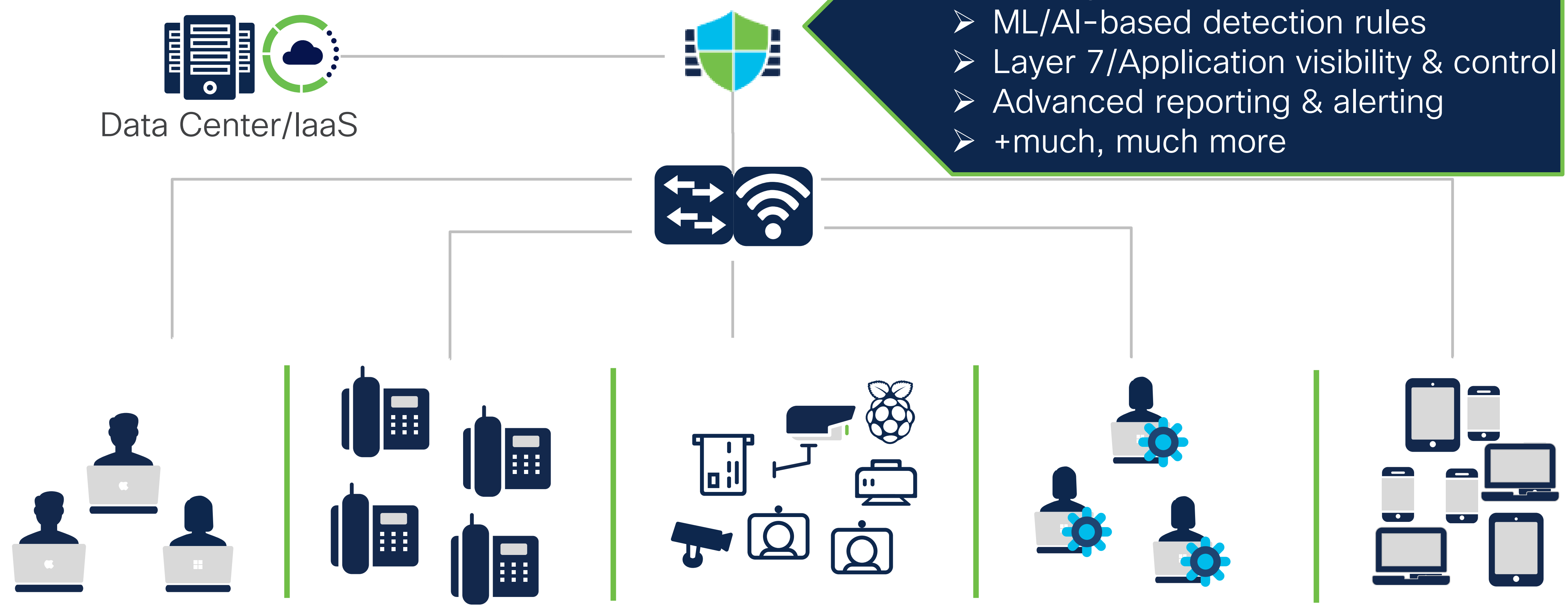
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Macro-segmentation



- ➢ Maintainable and scalable ACLs
- ➢ Identity-based policy
- ➢ IPS Signatures (50,000+)
- ➢ ML/AI-based detection rules
- ➢ Layer 7/Application visibility & control
- ➢ Advanced reporting & alerting
- ➢ +much, much more

Data Center/IaaS

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

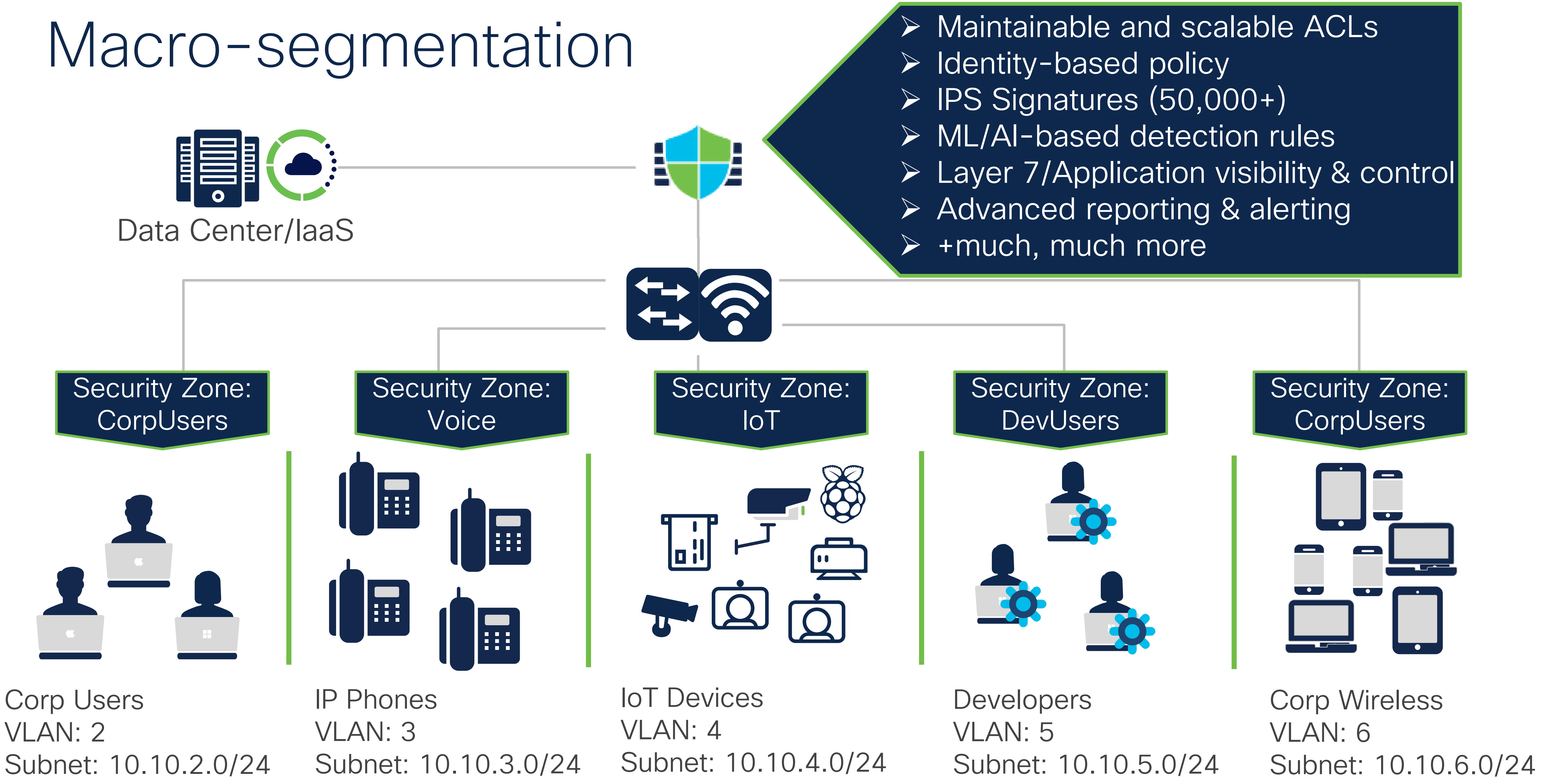
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Macro-segmentation



- Maintainable and scalable ACLs
- Identity-based policy
- IPS Signatures (50,000+)
- ML/AI-based detection rules
- Layer 7/Application visibility & control
- Advanced reporting & alerting
- +much, much more

Security Zone: CorpUsers

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

Security Zone: Voice

IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

Security Zone: IoT

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

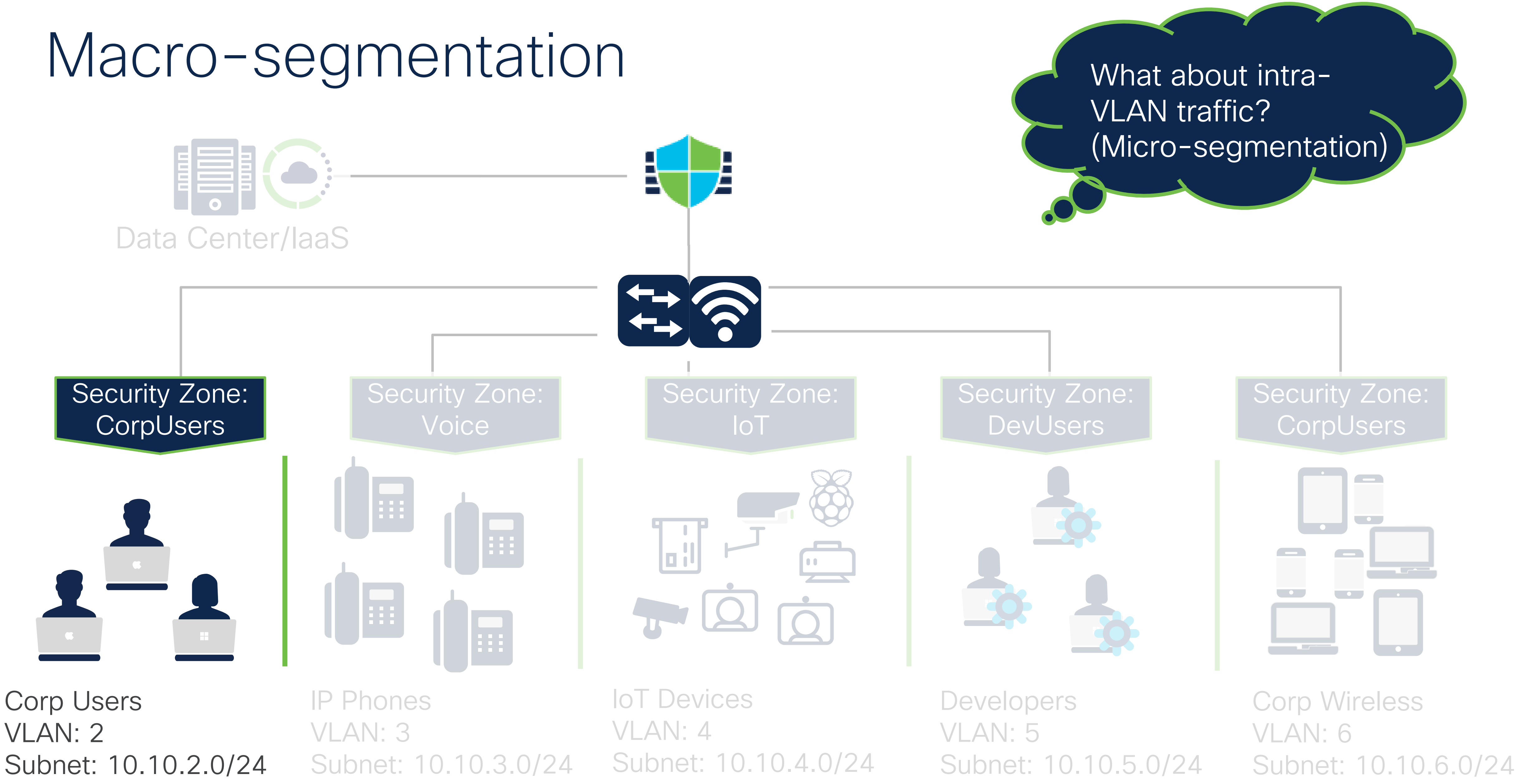
Security Zone: DevUsers

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Security Zone: CorpUsers

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Macro-segmentation



What about intra-VLAN traffic? (Micro-segmentation)

Data Center/IaaS

Security Zone: CorpUsers

Security Zone: Voice

Security Zone: IoT

Security Zone: DevUsers

Security Zone: CorpUsers

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

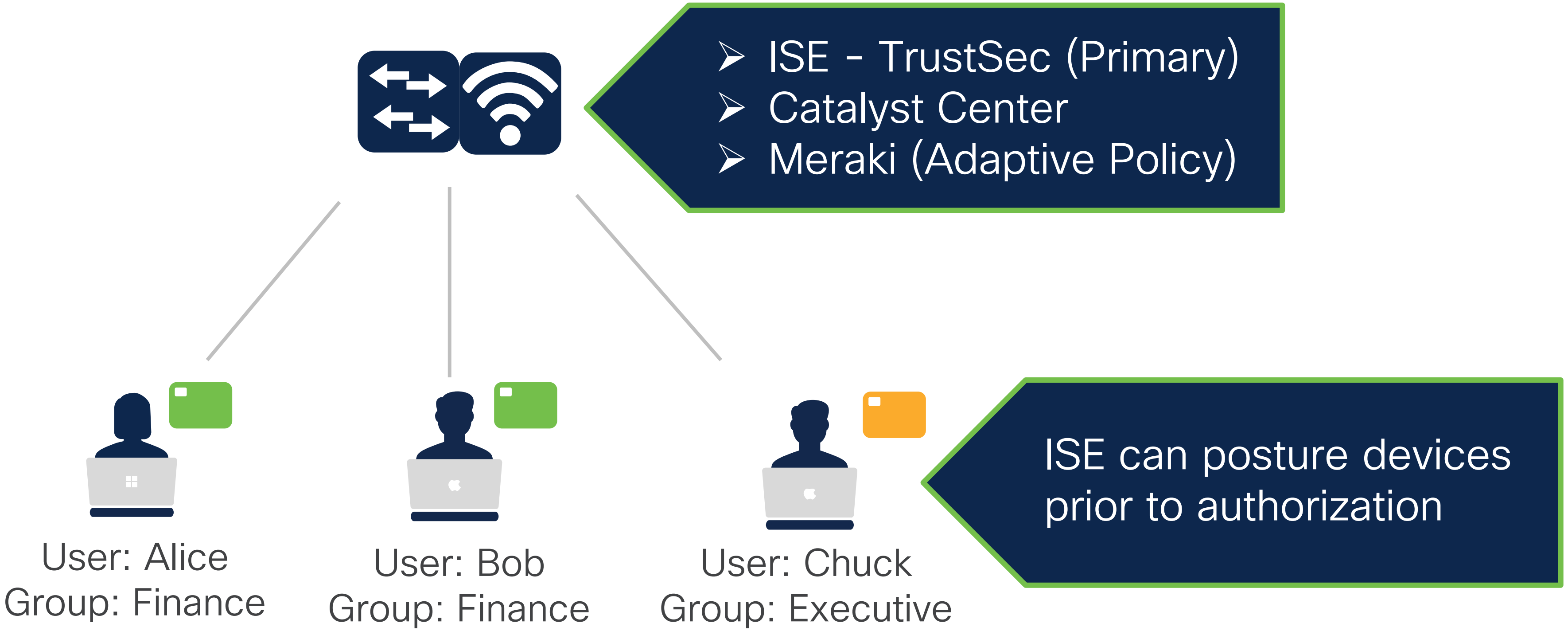
Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Micro-segmentation

🟩 Finance Tag

🟧 Executive Tag

🟥 Non-Compliant Tag



- ISE - TrustSec (Primary)
- Catalyst Center
- Meraki (Adaptive Policy)

User: Alice
Group: Finance

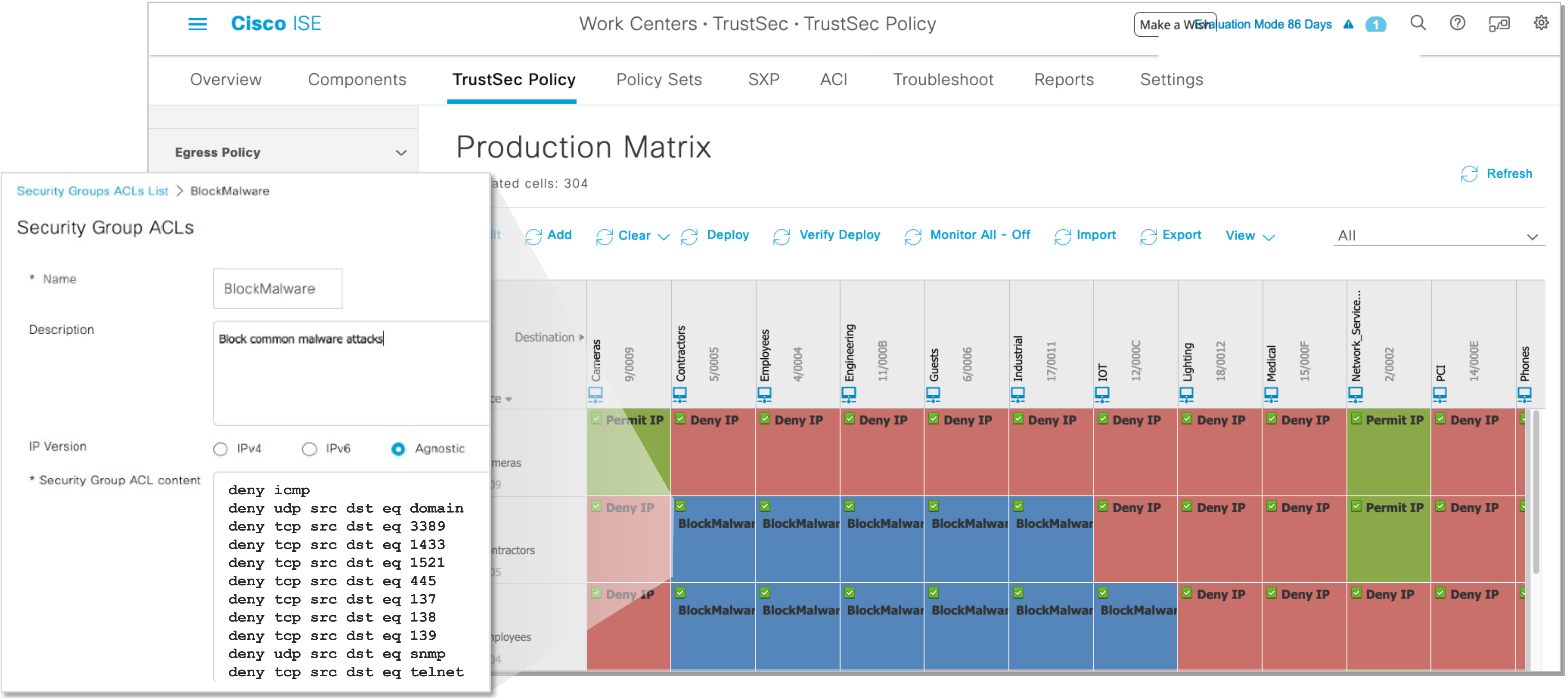
User: Bob
Group: Finance

User: Chuck
Group: Executive

ISE can posture devices prior to authorization

Corp Users
VLAN: 2 **(Auto-assigned)**
Subnet: 10.10.2.0/24

ISE TrustSec Policy



Production Matrix

ated cells: 304

	Cameras 9/0009	Contractors 5/0005	Employees 4/0004	Engineering 11/000B	Guests 6/0006	Industrial 17/0011	IOT 12/000C	Lighting 18/0012	Medical 15/000F	Network_Service... 2/0002	PCI 14/000E	Phones
meras 09	Permit IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	
ntractors 05	Deny IP	BlockMalwar	BlockMalwar	BlockMalwar	BlockMalwar	BlockMalwar	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	
ployees 04	Deny IP	BlockMalwar	BlockMalwar	BlockMalwar	BlockMalwar	BlockMalwar	BlockMalwar	Deny IP	Deny IP	Deny IP	Deny IP	

Security Groups ACLs List > BlockMalware

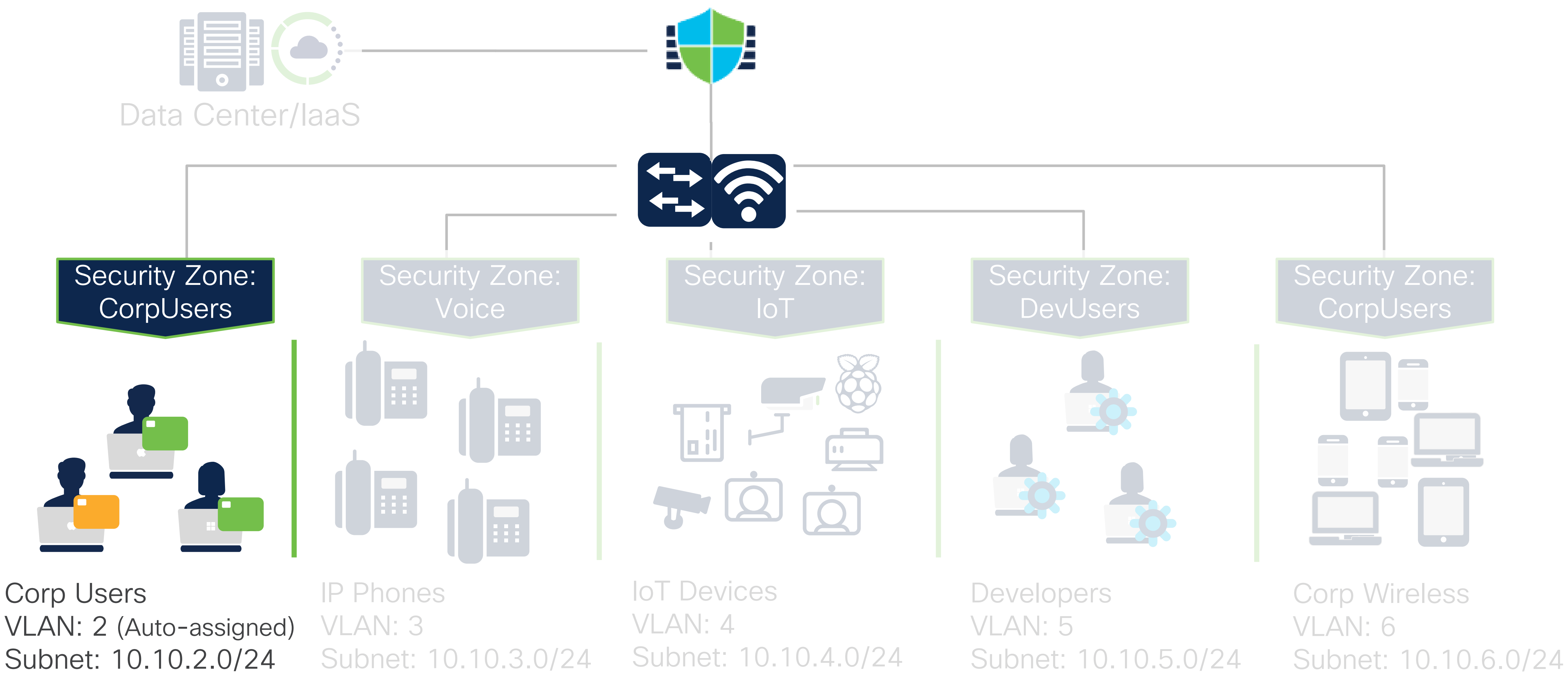
Security Group ACLs

* Name	BlockMalware
Description	Block common malware attacks
IP Version	○ IPv4 ○ IPv6 ● Agnostic

* Security Group ACL content

```
deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
```

Macro + Micro-segmentation



Corp Users
VLAN: 2 (Auto-assigned)
Subnet: 10.10.2.0/24

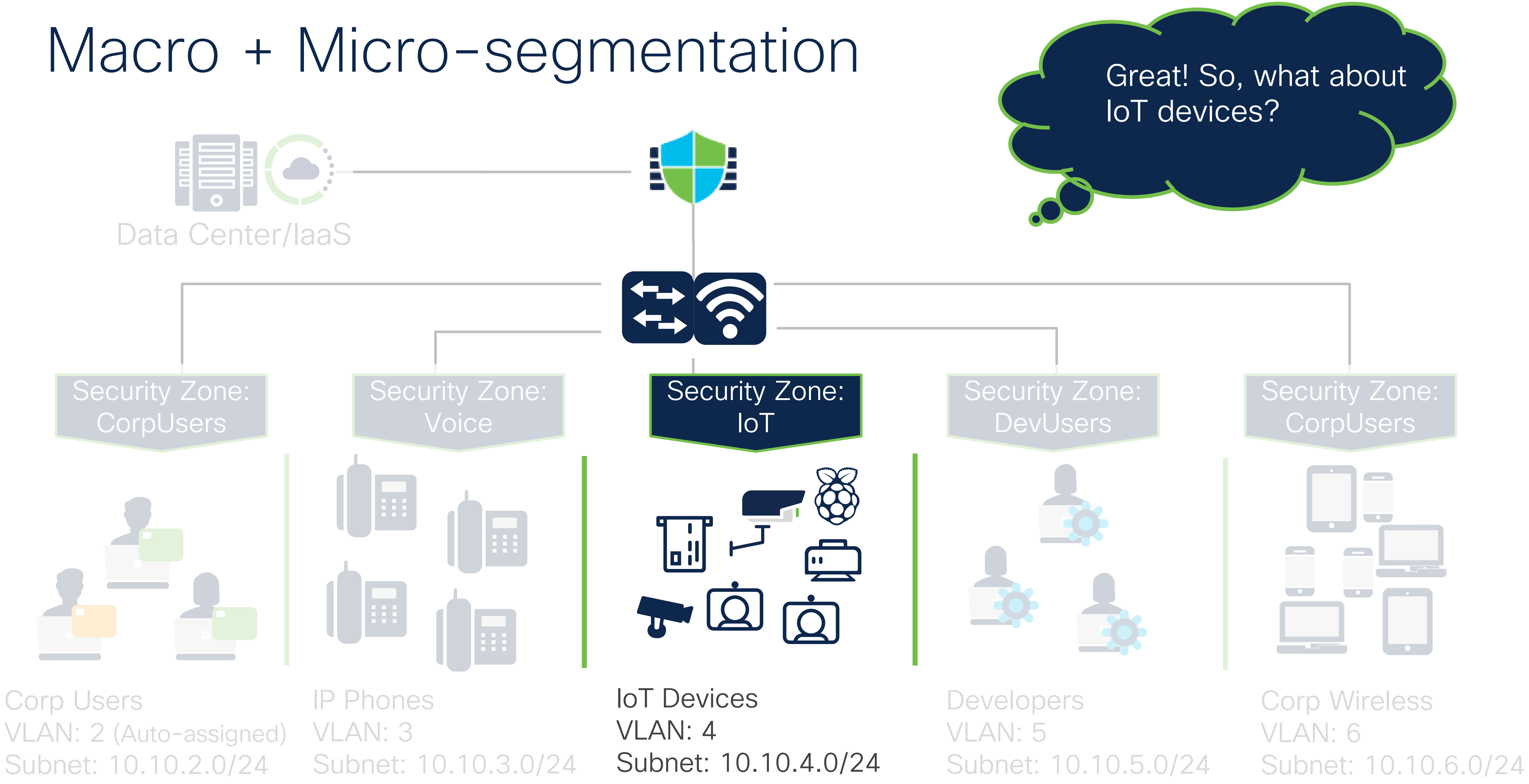
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

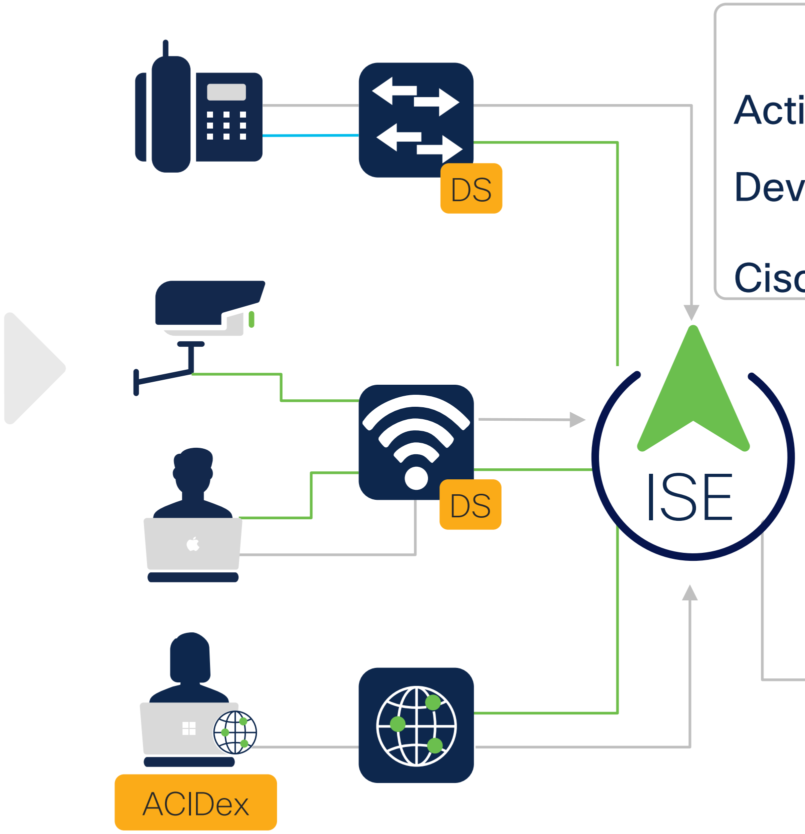
Macro + Micro-segmentation



ISE Endpoint Profiling

The profiling service in Cisco ISE identifies the devices that connect to your network

Endpoints send interesting data that reveal their device type

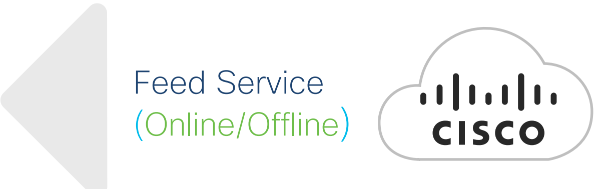


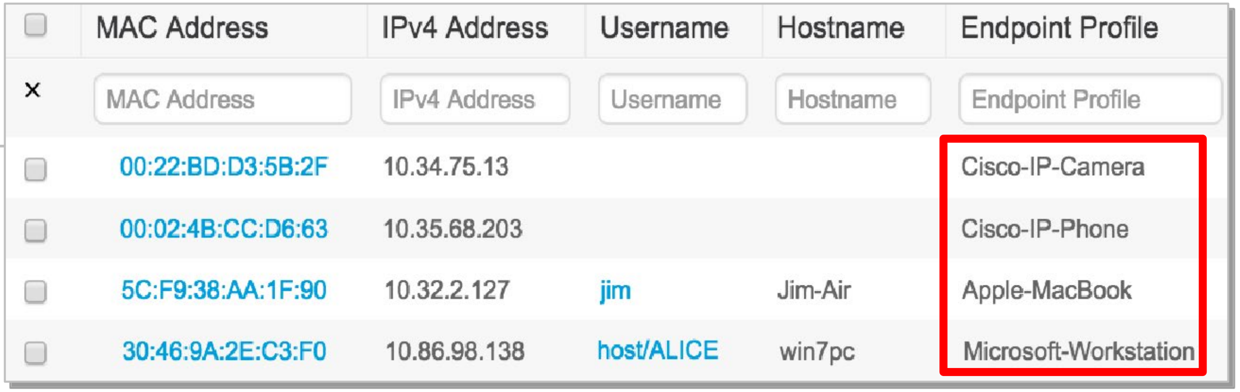
ISE Data Collection Methods for Device Profiling

Active Probes: NetFlow | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

Cisco Secure Client (formerly AnyConnect): ACIDex

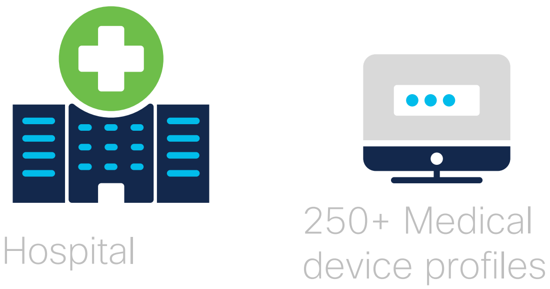


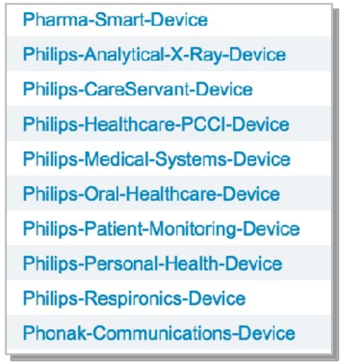


□	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
□	00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
□	00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
□	5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
□	30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

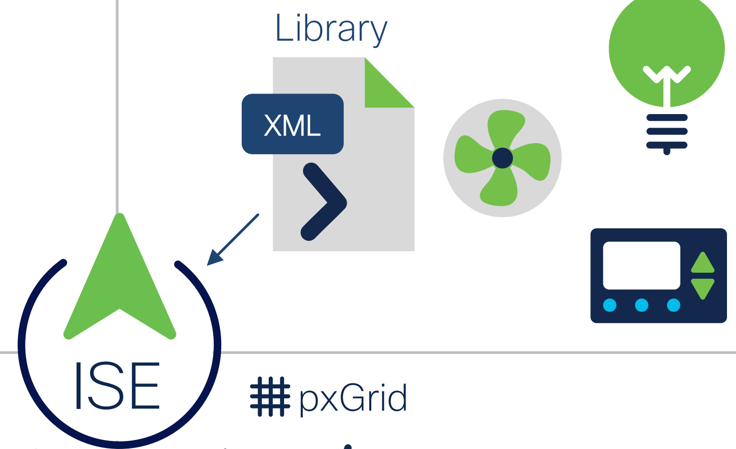
Profiling Packages and Integrations

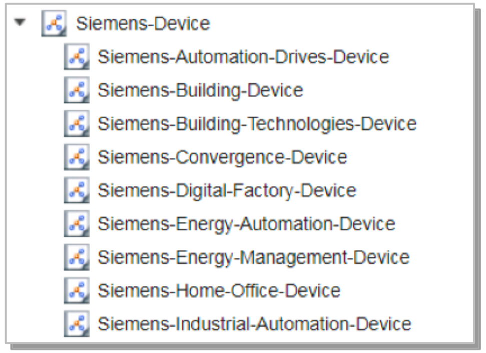
Medical Devices

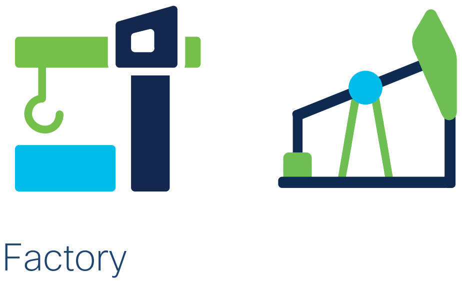



Pharma-Smart-Device
Philips-Analytical-X-Ray-Device
Philips-CareServant-Device
Philips-Healthcare-PCCI-Device
Philips-Medical-Systems-Device
Philips-Oral-Healthcare-Device
Philips-Patient-Monitoring-Device
Philips-Personal-Health-Device
Philips-Respironics-Device
Phonak-Communications-Device

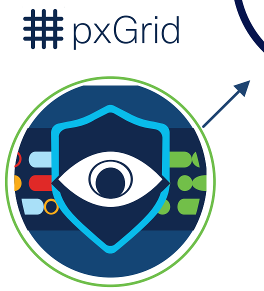
IOT Building & Automation



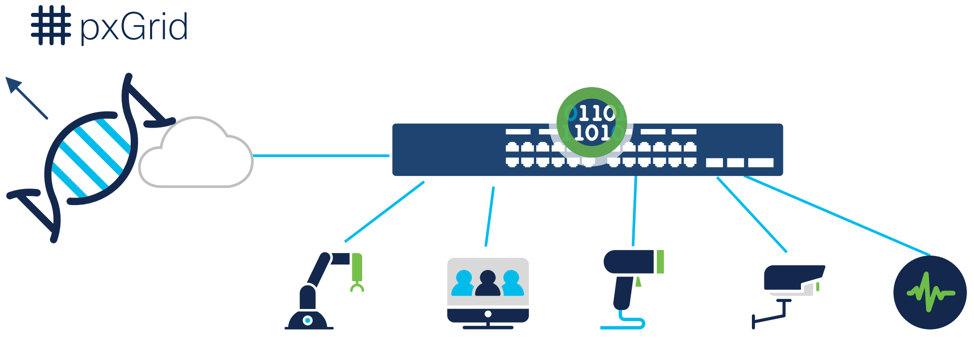

Siemens-Device
Siemens-Automation-Drives-Device
Siemens-Building-Device
Siemens-Building-Technologies-Device
Siemens-Convergence-Device
Siemens-Digital-Factory-Device
Siemens-Energy-Automation-Device
Siemens-Energy-Management-Device
Siemens-Home-Office-Device
Siemens-Industrial-Automation-Device



Industrial Devices



Cisco CyberVision

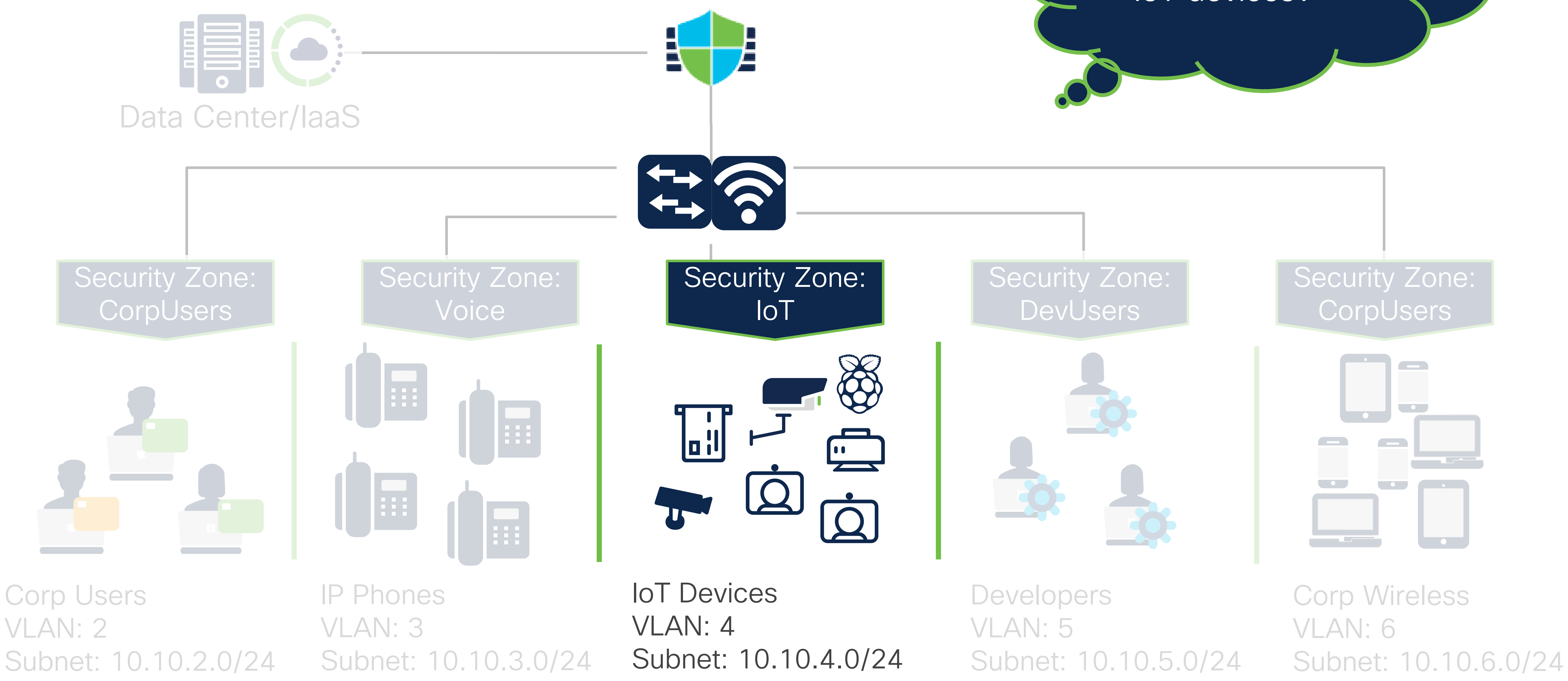


Cisco AI Endpoint Analytics

Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization

https://community.cisco.com/t5/tag/ise-endpoint-profile/tg-p/board-id/4561-docs-security

Macro + Micro-segmentation



Data Center/IaaS

OK, so what about our IoT devices?

Security Zone: CorpUsers

Security Zone: Voice

Security Zone: IoT

Security Zone: DevUsers

Security Zone: CorpUsers

Corp Users
VLAN: 2
Subnet: 10.10.2.0/24

IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

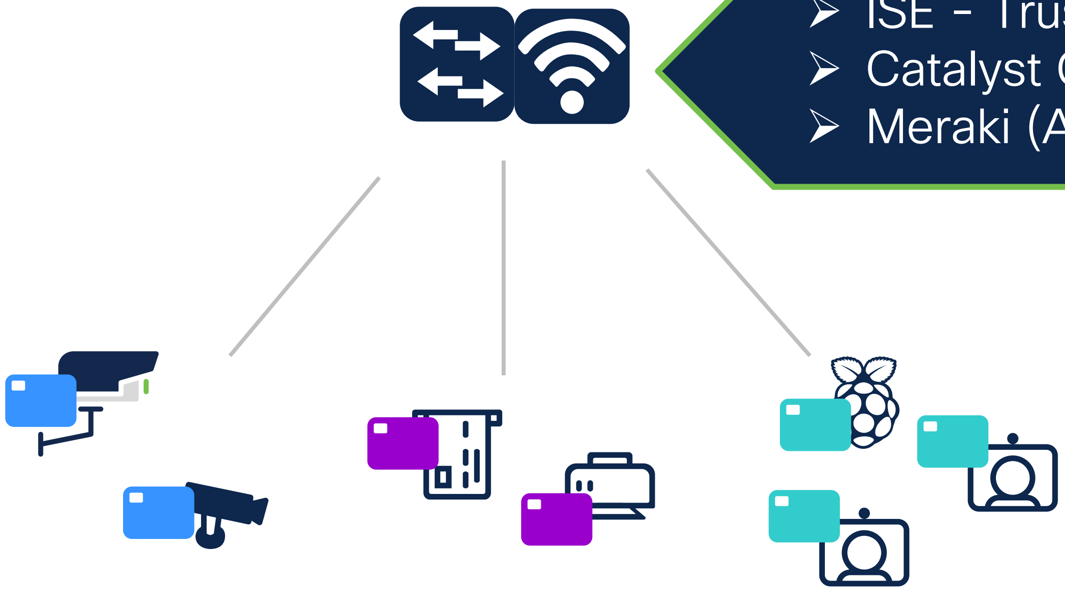
Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Micro-segmentation

🟦 Camera Tag

🟪 Printer Tag

🟩 Badge_Access Tag

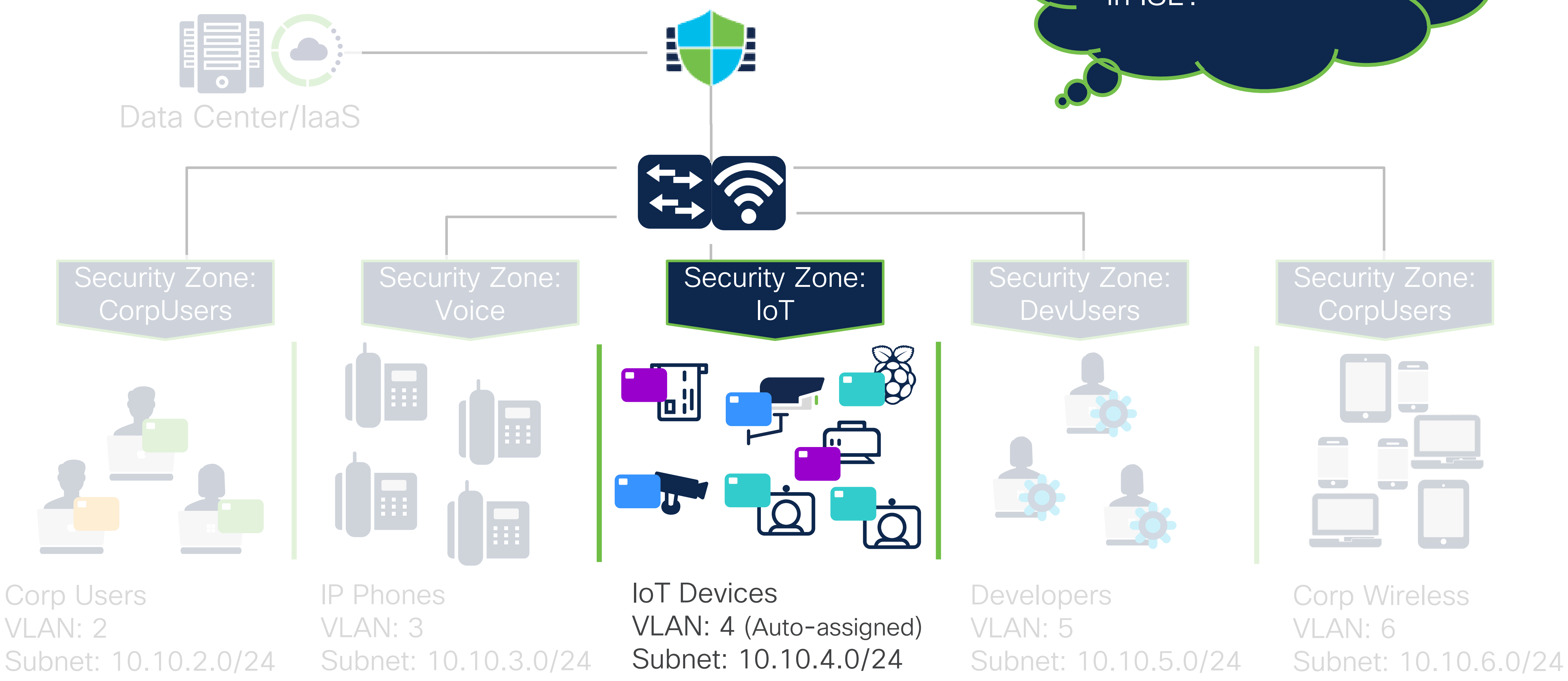


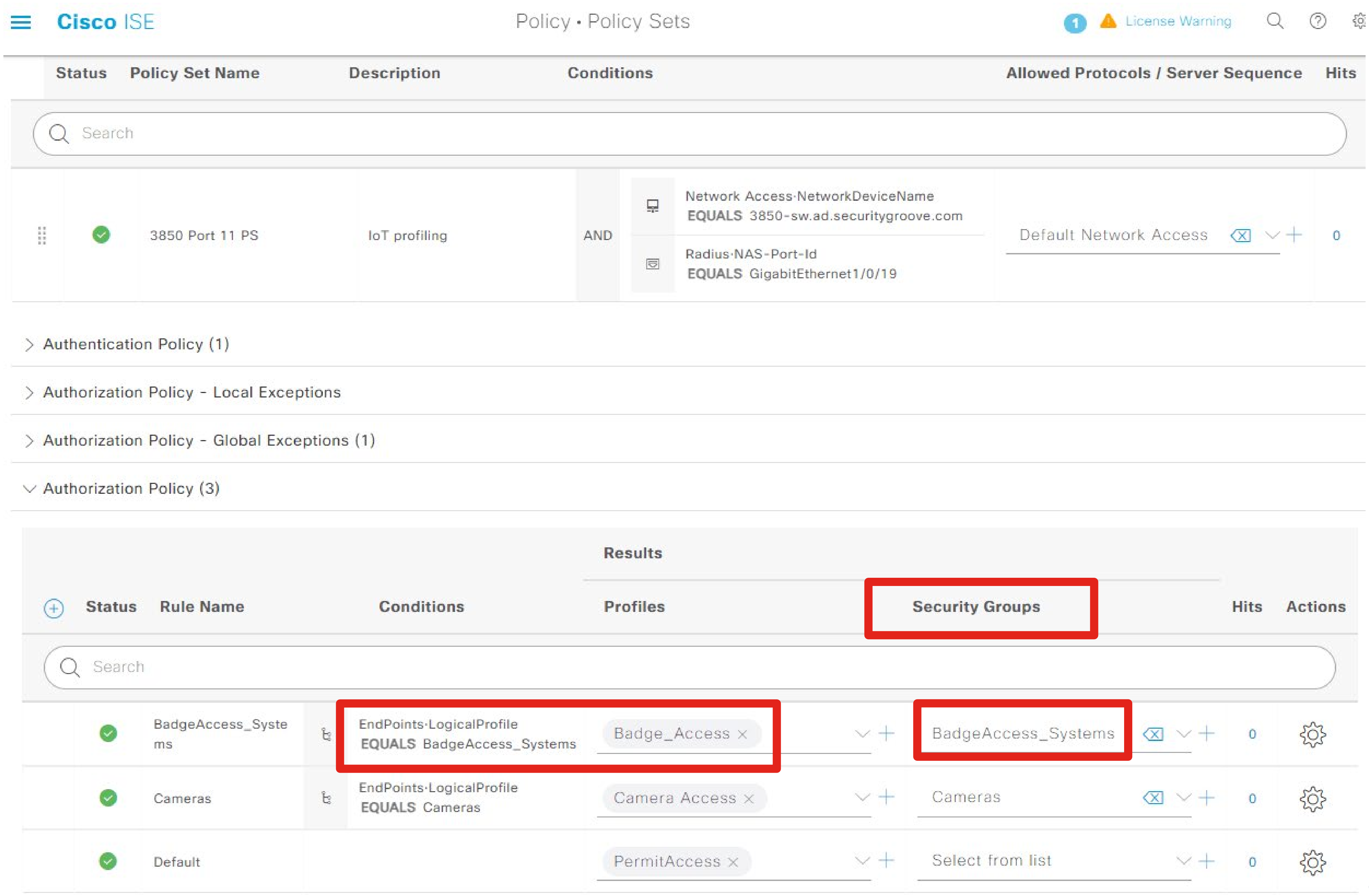
- ISE - TrustSec (Primary)
- Catalyst Center
- Meraki (Adaptive Policy)

IoT Devices
VLAN: 4 **(Auto-assigned)**
Subnet: 10.10.4.0/24

Macro + Micro-segmentation

How would this look in ISE?





Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search					
✓	3850 Port 11 PS	IoT profiling	AND Network Access·NetworkDeviceName **EQUALS** 3850-sw.ad.securitygroove.com Radius·NAS-Port-Id **EQUALS** GigabitEthernet1/0/19	Default Network Access	0

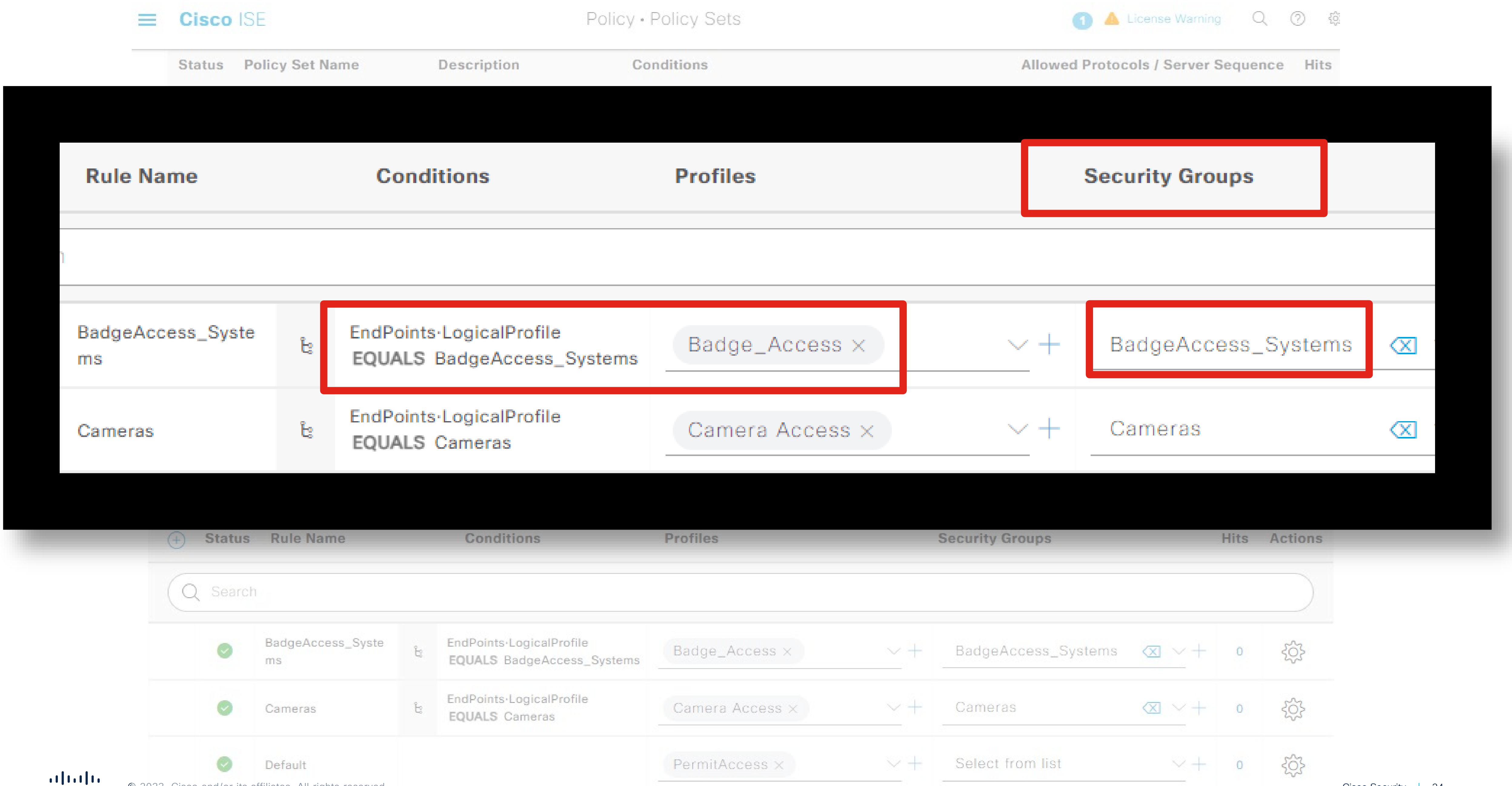
> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions (1)

∨ Authorization Policy (3)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search						
✓	BadgeAccess_Systems	EndPoints·LogicalProfile **EQUALS** BadgeAccess_Systems	Badge_Access ×	BadgeAccess_Systems	0	⚙
✓	Cameras	EndPoints·LogicalProfile **EQUALS** Cameras	Camera Access ×	Cameras	0	⚙
✓	Default		PermitAccess ×	Select from list	0	⚙



Cisco ISE — Policy · Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits

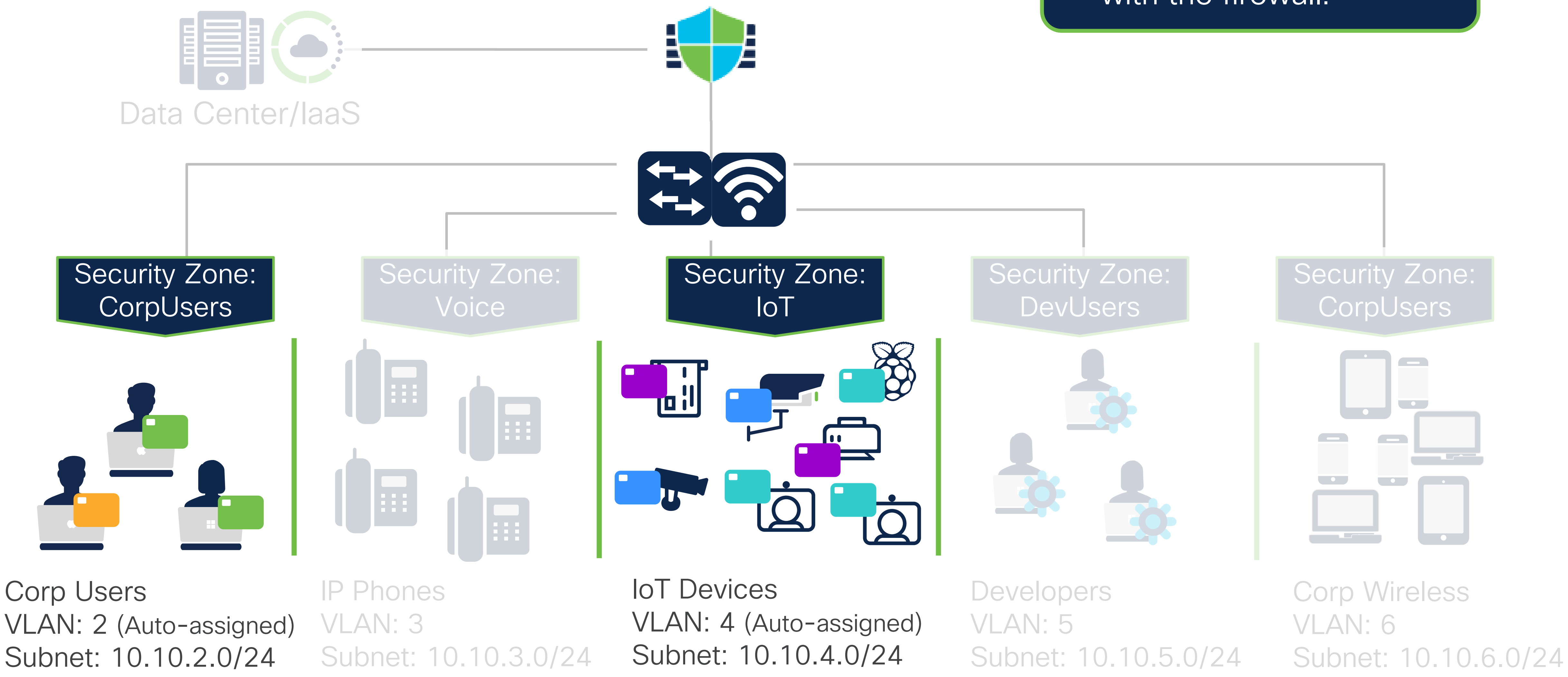
Rule Name	Conditions	Profiles	Security Groups
BadgeAccess_Systems	EndPoints·LogicalProfile EQUALS BadgeAccess_Systems	Badge_Access	BadgeAccess_Systems
Cameras	EndPoints·LogicalProfile EQUALS Cameras	Camera Access	Cameras

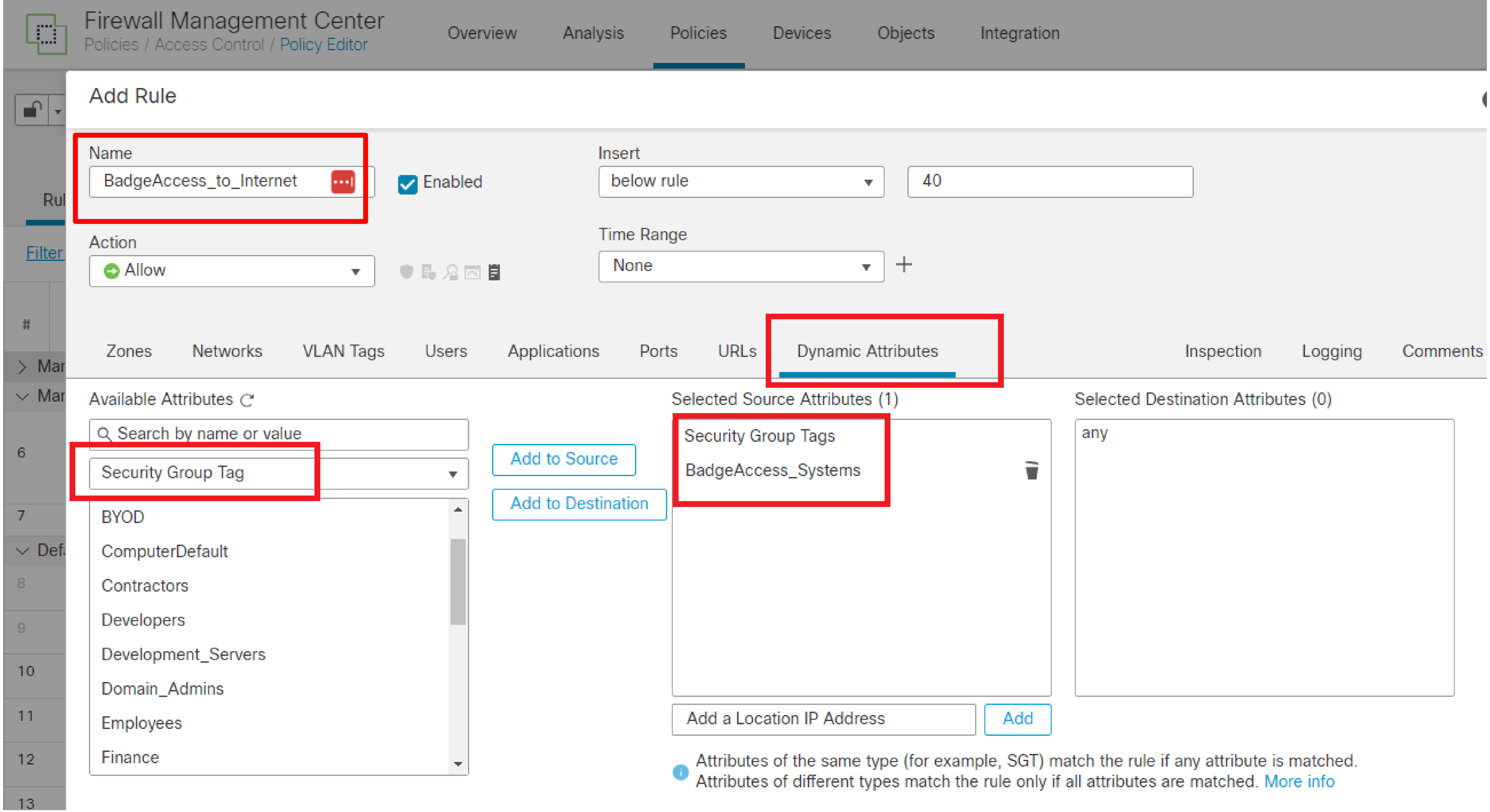
Search

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	BadgeAccess_Systems	EndPoints·LogicalProfile EQUALS BadgeAccess_Systems	Badge_Access	BadgeAccess_Systems	0	⚙
✓	Cameras	EndPoints·LogicalProfile EQUALS Cameras	Camera Access	Cameras	0	⚙
✓	Default		PermitAccess	Select from list	0	⚙

Macro + Micro-segmentation

Let’s pull this together with the firewall!




Firewall Management Center
Policies / Access Control / Policy Editor
Overview
Analysis
Policies
Devices
Objects
Integration

Add Rule

Name: BadgeAccess_to_Internet

☑ Enabled

Insert: below rule ▾ 40

Action: Allow ▾

Time Range: None ▾ +

Available Attributes

Search by name or value

Security Group Tag ▾

- BYOD
- ComputerDefault
- Contractors
- Developers
- Development_Servers
- Domain_Admins
- Employees
- Finance

Selected Source Attributes (1)

Security Group Tags

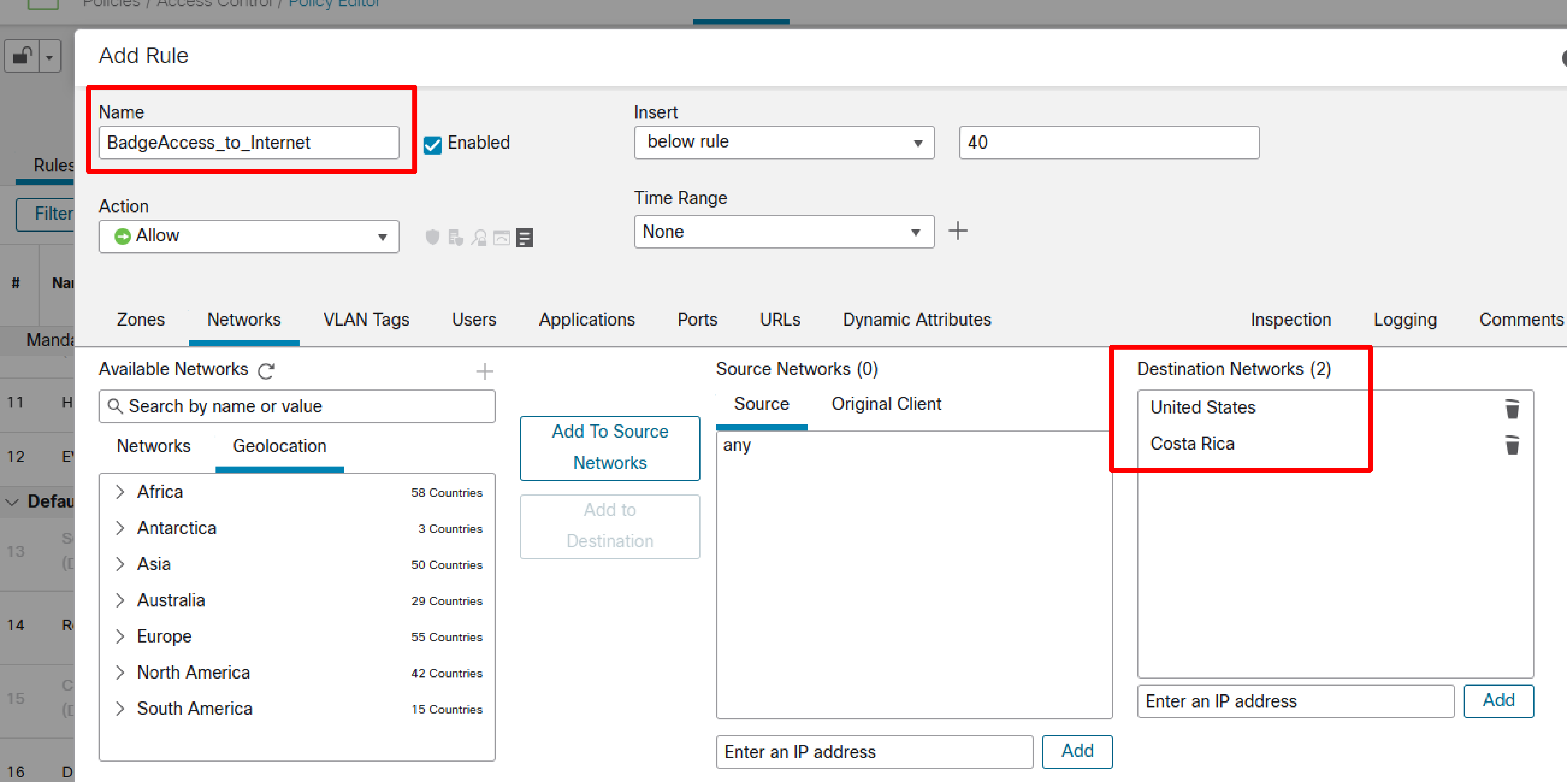
BadgeAccess_Systems

Selected Destination Attributes (0)

any

Add a Location IP Address Add

Attributes of the same type (for example, SGT) match the rule if any attribute is matched. Attributes of different types match the rule only if all attributes are matched. More info



Add Rule

Name: BadgeAccess_to_Internet

☑ Enabled

Insert: below rule 40

Action: Allow

Time Range: None

Available Networks

Africa	58 Countries
Antarctica	3 Countries
Asia	50 Countries
Australia	29 Countries
Europe	55 Countries
North America	42 Countries
South America	15 Countries

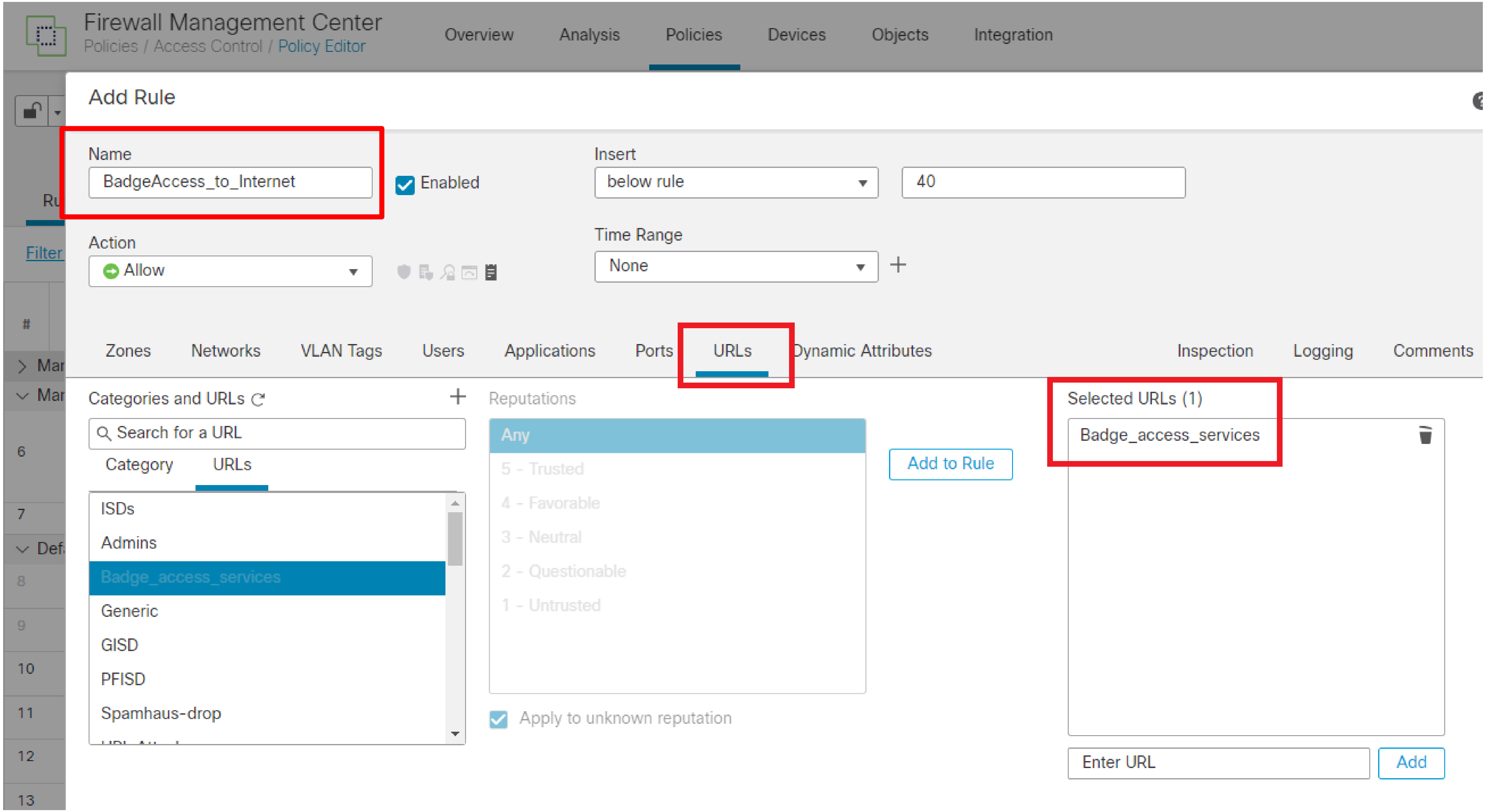
Source Networks (0)

any

Destination Networks (2)

United States

Costa Rica



Add Rule

Name: BadgeAccess_to_Internet

☑ Enabled

Insert: below rule 40

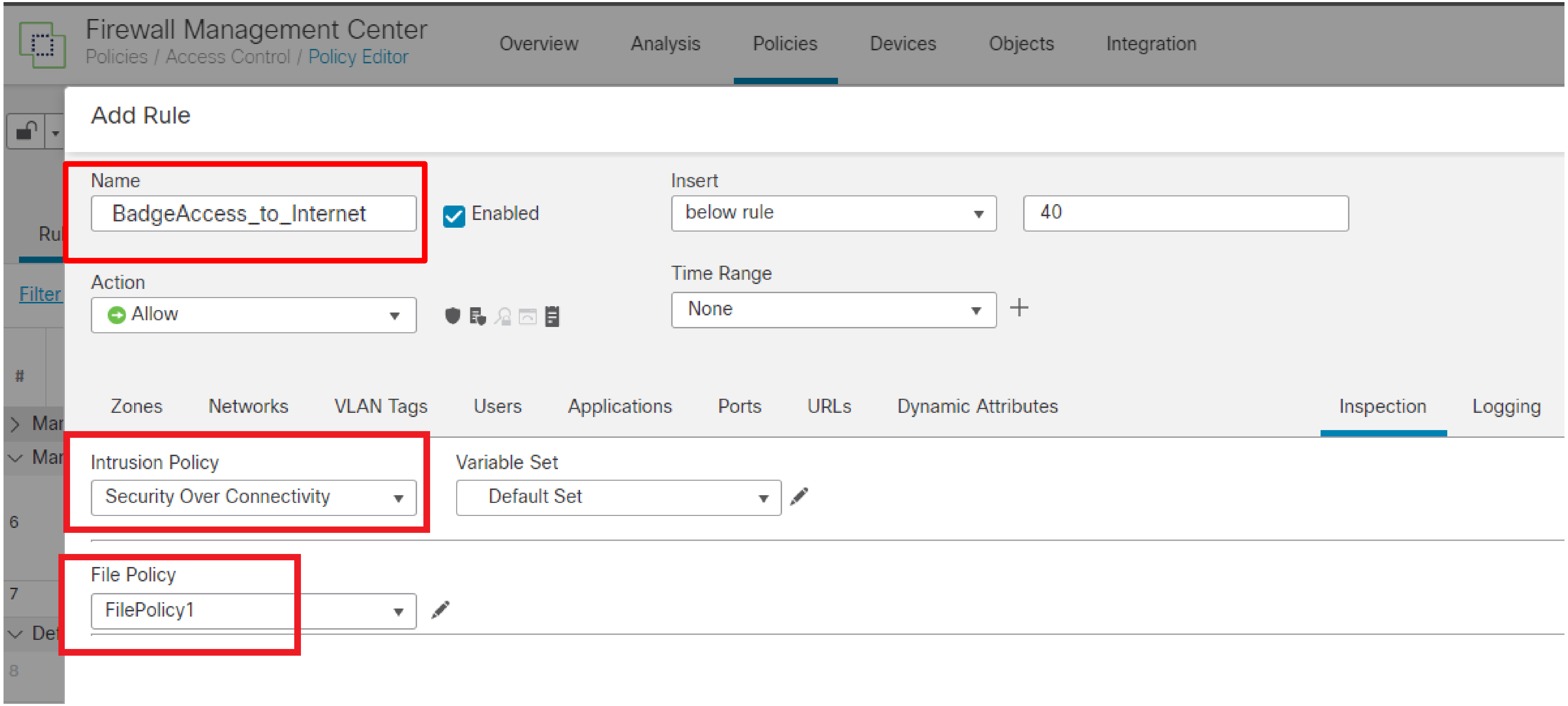
Action: Allow

Time Range: None

☑ Apply to unknown reputation

Selected URLs (1)

Badge_access_services



Add Rule

Name: BadgeAccess_to_Internet

☑ Enabled

Insert: below rule 40

Action: Allow

Time Range: None

Intrusion Policy: Security Over Connectivity

Variable Set: Default Set

File Policy: FilePolicy1

In summary...

Like using AD/EntraID groups for user-based firewall rules...

- Only members of the DevOps group may SSH or RDP to the DMZ.

- Only members of the IT and Dev groups may download executable files.

- Only members of the marketing and HR groups may access social media websites.

...use ISE Device Profiling Groups for device-based firewall rules

- IP surveillance cameras may only communicate with site abc-services.com

- Badge Access Systems are blocked from initiating connections internally, except to the building services subnets.

- Medical devices may only communicate to the Internet on the following domains...

Use AD/EntraID Groups OR SGTs for user-based firewall rules

+

Use ISE Device Profiling Groups for device-based firewall rules

- Only contractors in the ABC-Services group may connect to MRI machines.

- Only members of the Fabrication group may connect to 3D printers.

- Only members of the IT group may connect to an IoT device on a port other than 443. The exceptions are:
  - Users in the Graphics group connecting to Canon printers over TCP 9100.
  - Members of the Maintenance group connecting to HVAC systems.

FMC - Cisco Secure Dynamic Attribute Connector (CSDAC)

Cloud Connectors

Azure

Azure Service Tags

vCenter/ NSX-T

GCP

AWS

Public Feeds Connecors

O365

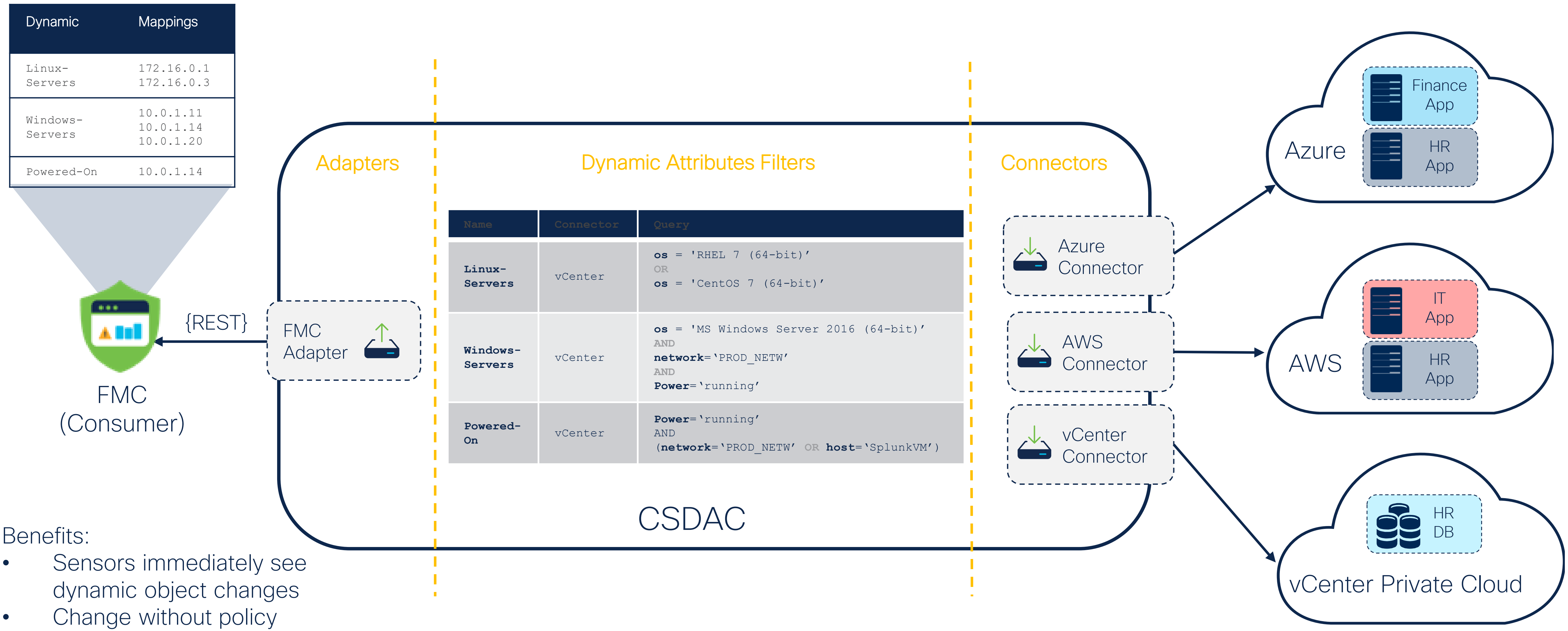
GitHub

Webex

Zoom

Generic TXT

FMC – Cisco Secure Dynamic Attributes Connector



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

Name	Connector	Query

Linux-Servers	vCenter	os = 'RHEL 7 (64-bit)’
		OR
		os = 'CentOS 7 (64-bit)’

Windows-Servers	vCenter	os = 'MS Windows Server 2016 (64-bit)’
		AND
		network=‘PROD_NETW’
		AND
		Power=‘running’

Powered-On	vCenter	Power=‘running’ AND (network=‘PROD_NETW’ OR host=‘SplunkVM’)

Benefits:

- Sensors immediately see dynamic object changes
- Change without policy deploy

FMC – Cisco Secure Dynamic Attributes Connector

Linux- Servers 172.16.0.1 172.16.0.3

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

Name (DAC)	Connector	Query
Linux-Servers	vCenter	**os** = 'RHEL 7 (64-bit)’ OR **os** = 'CentOS 7 (64-bit)’
Windows-Servers	vCenter	**os** = 'MS Windows Server 2016 (64-bit)’ AND **network**=‘PROD_NETW’ AND **Power**=‘running’
Powered-On	vCenter	**Power**=‘running’ AND (**network**=‘PROD_NETW’ OR **host**=‘SplunkVM’)

Benefits:

- Sensors immediately see dynamic object changes
- Change without policy deploy

Use AD/EntraID Groups OR SGTs for user-based firewall rules

+

Use ISE Device Profiling Groups for device-based firewall rules

+

Use Dynamic Attribute Connector for dynamic tag-based firewall rules

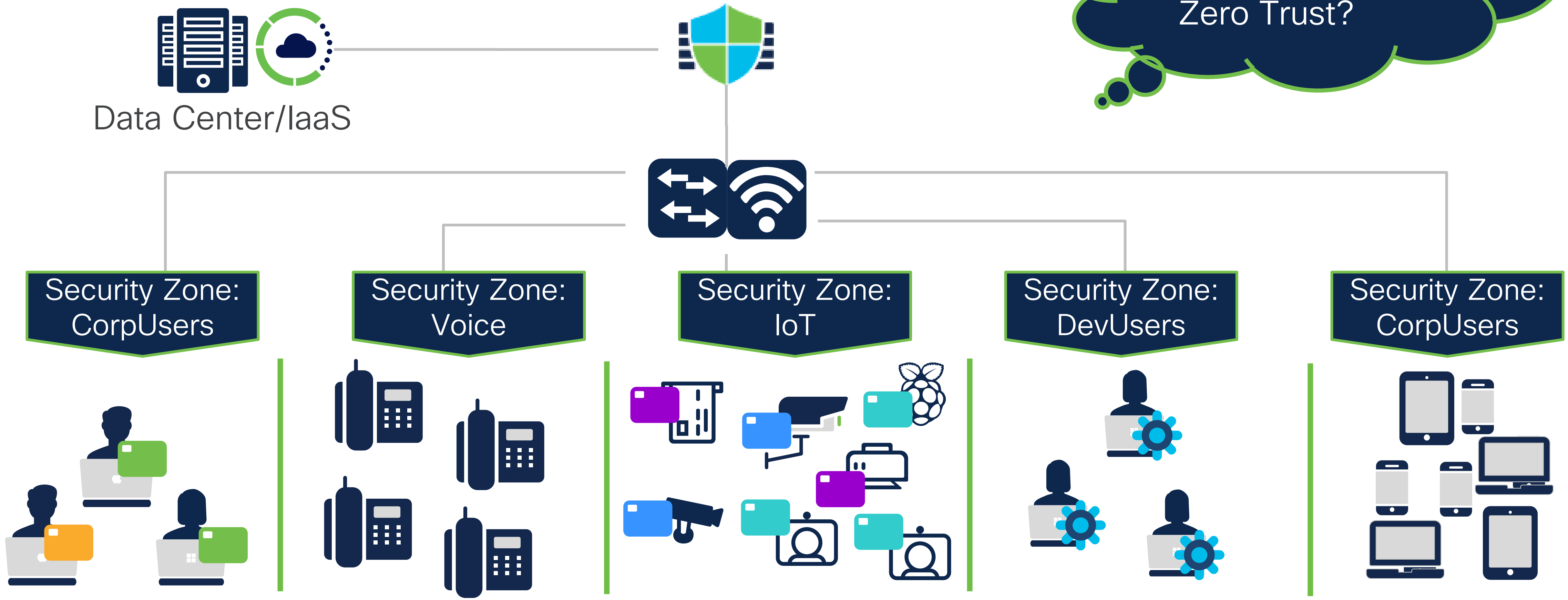
- Only Infusion Pumps and Vital Signs Monitors may connect to Lab-Systems-XYZ. (Which exist in Azure, AWS, and in VMware)

- Only Badge-Access-Devices may connect to Badge-Access-Systems.

- Only members of the WebDev group may connect to Dev-Systems on a port other than 443.

Macro + Micro-segmentation

What have we achieved toward Zero Trust?



Data Center/IaaS

Security Zone: CorpUsers

Security Zone: Voice

Security Zone: IoT

Security Zone: DevUsers

Security Zone: CorpUsers

Corp Users
VLAN: 2 (Auto-assigned)
Subnet: 10.10.2.0/24

IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4 (Auto-assigned)
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

Zero Trust Principles Covered

Segmentation

Identity-Based Access

Least Privilege

Visibility

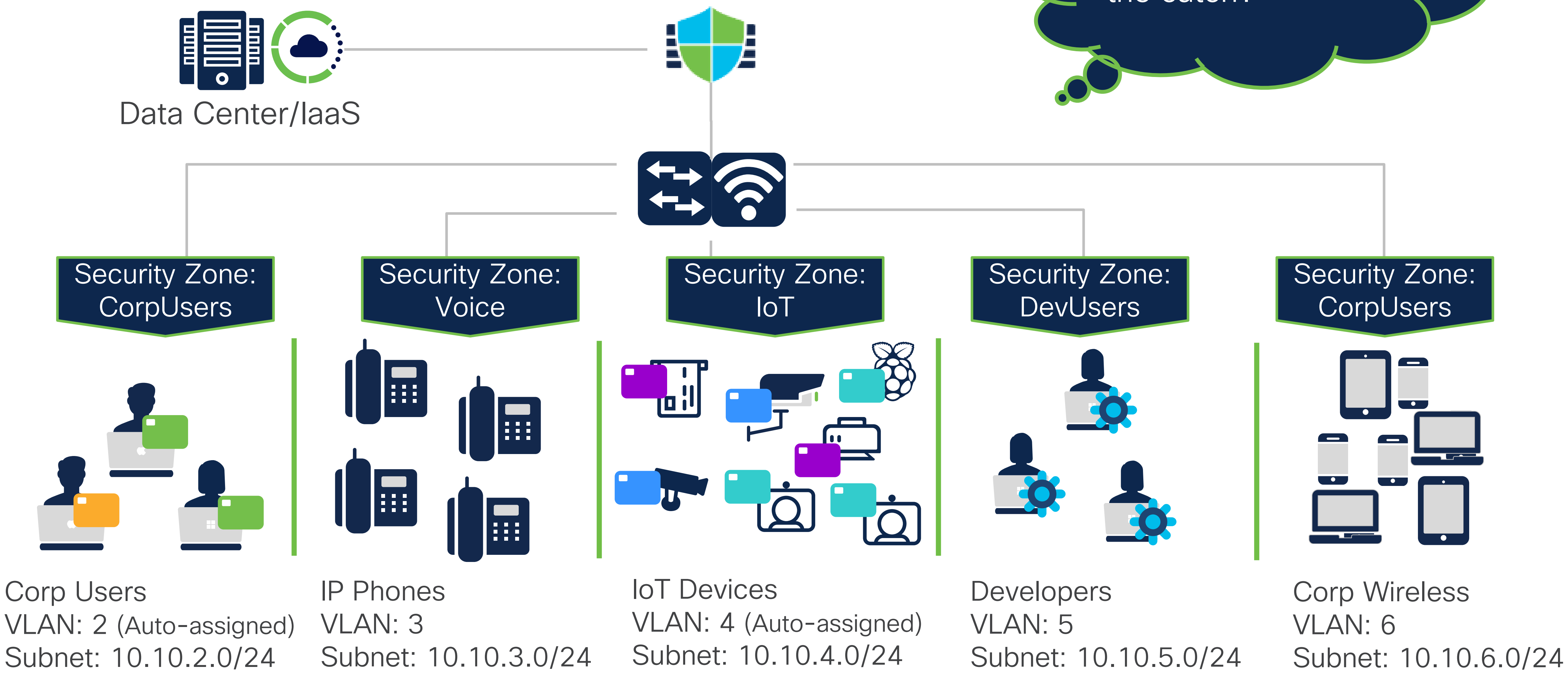
Lateral Movement Protection

Compliance Enforcement

Continuous Verification

Macro + Micro-segmentation

Great! Now what's the catch?



Data Center/IaaS

Security Zone: CorpUsers

Security Zone: Voice

Security Zone: IoT

Security Zone: DevUsers

Security Zone: CorpUsers

Corp Users
VLAN: 2 (Auto-assigned)
Subnet: 10.10.2.0/24

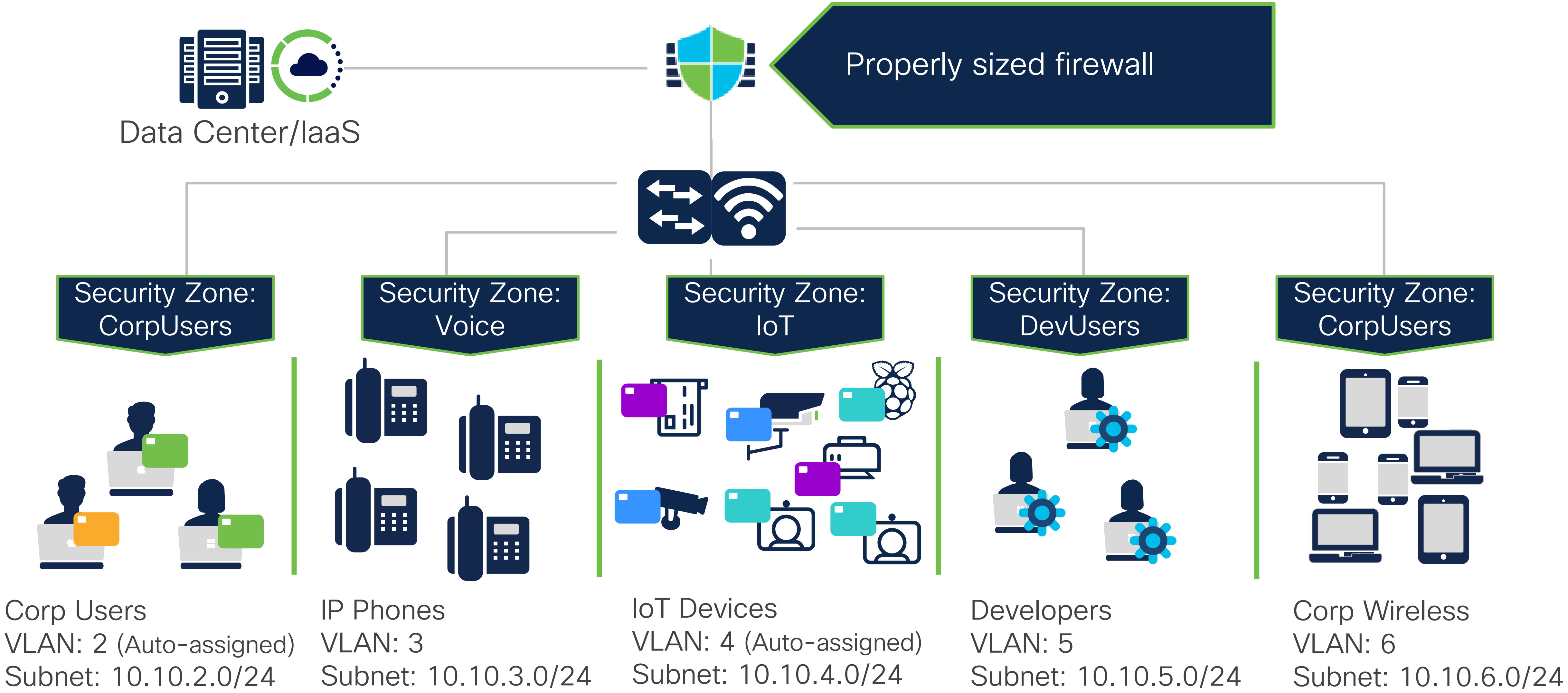
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4 (Auto-assigned)
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

The catch



Properly sized firewall

Data Center/IaaS

Security Zone: CorpUsers

Security Zone: Voice

Security Zone: IoT

Security Zone: DevUsers

Security Zone: CorpUsers

Corp Users
VLAN: 2 (Auto-assigned)
Subnet: 10.10.2.0/24

IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

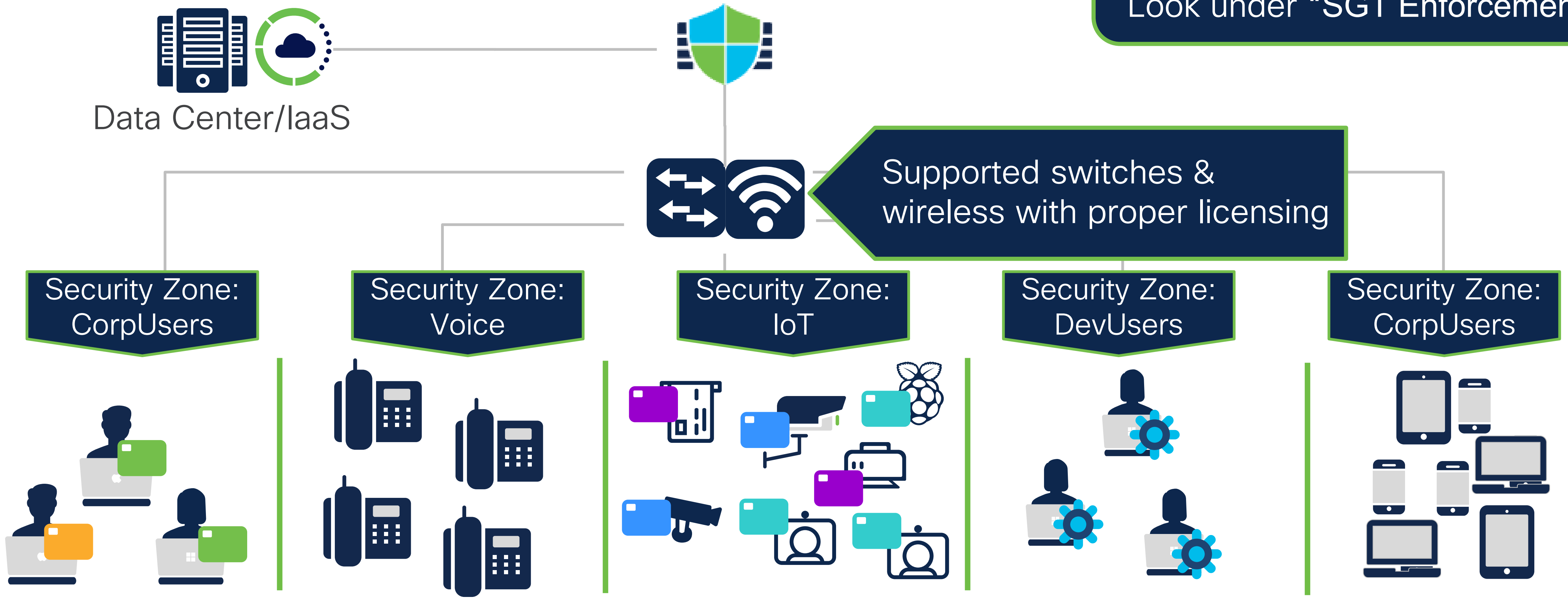
IoT Devices
VLAN: 4 (Auto-assigned)
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

The catch

Search:
TrustSec “capability matrix”
Look under “SGT Enforcement”



Data Center/IaaS

Supported switches & wireless with proper licensing

Security Zone: CorpUsers

Security Zone: Voice

Security Zone: IoT

Security Zone: DevUsers

Security Zone: CorpUsers

Corp Users
VLAN: 2 (Auto-assigned)
Subnet: 10.10.2.0/24

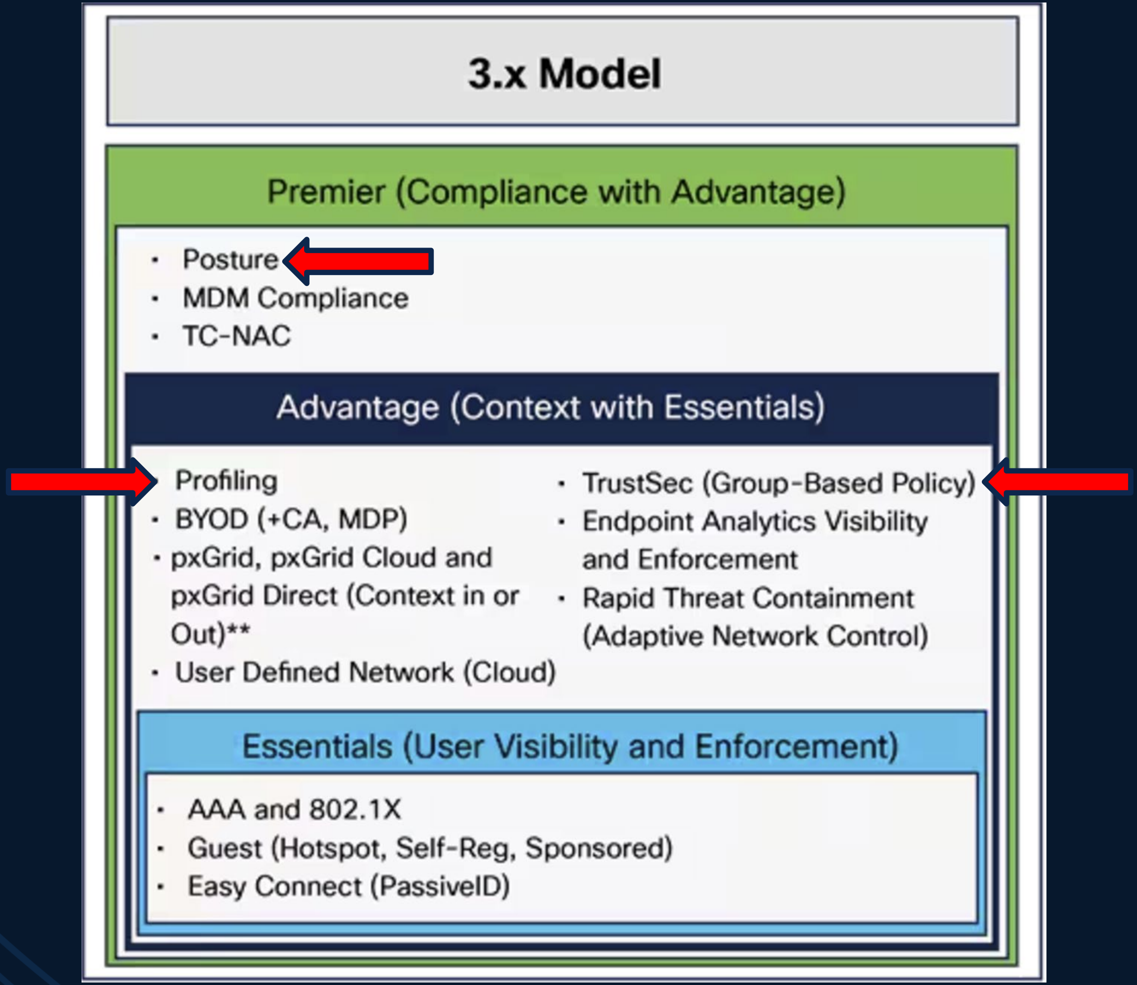
IP Phones
VLAN: 3
Subnet: 10.10.3.0/24

IoT Devices
VLAN: 4 (Auto-assigned)
Subnet: 10.10.4.0/24

Developers
VLAN: 5
Subnet: 10.10.5.0/24

Corp Wireless
VLAN: 6
Subnet: 10.10.6.0/24

ISE Licensing



3.x Model

Premier (Compliance with Advantage)

- Posture
- MDM Compliance
- TC-NAC

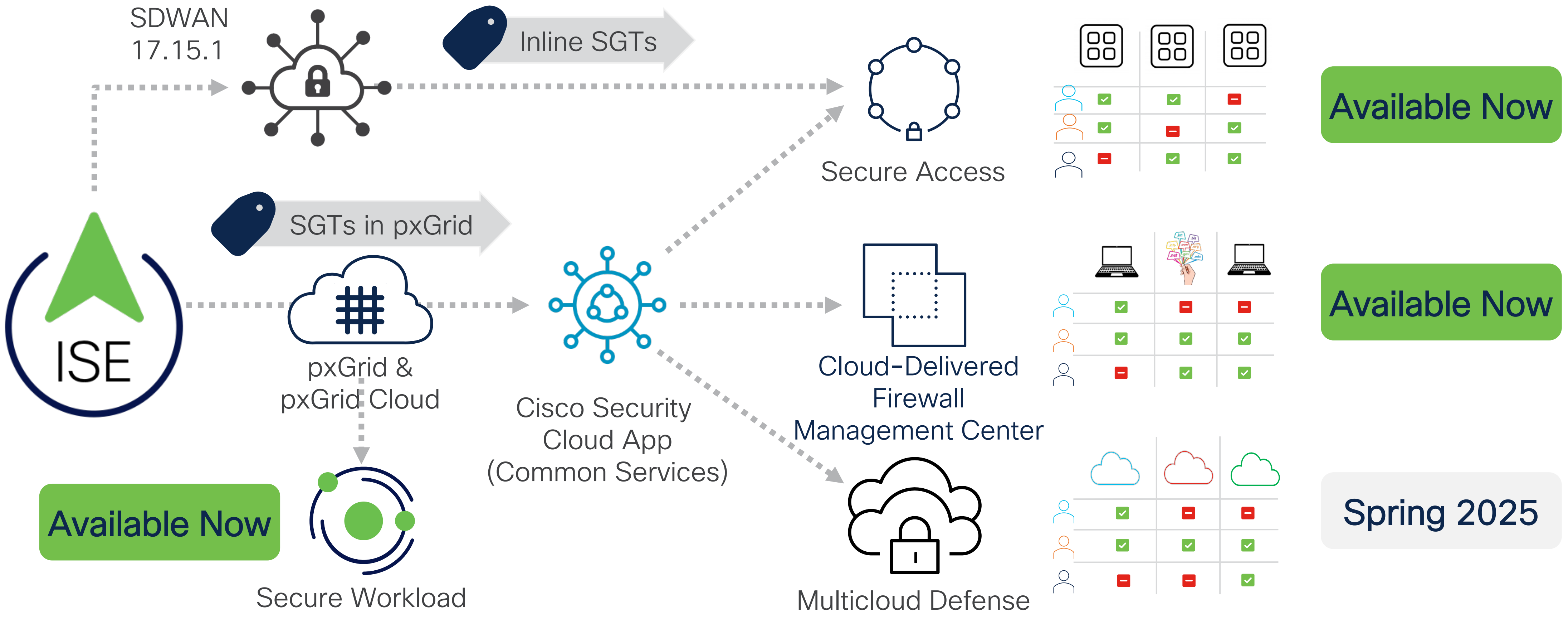
Advantage (Context with Essentials)

- Profiling
- BYOD (+CA, MDP)
- pxGrid, pxGrid Cloud and pxGrid Direct (Context in or Out)**
- User Defined Network (Cloud)
- TrustSec (Group-Based Policy)
- Endpoint Analytics Visibility and Enforcement
- Rapid Threat Containment (Adaptive Network Control)

Essentials (User Visibility and Enforcement)

- AAA and 802.1X
- Guest (Hotspot, Self-Reg, Sponsored)
- Easy Connect (PassiveID)

ISE for Cisco Security Cloud Services



Security Group Tags (SGTs) are the common language used across campus, remote, cloud, and firewall policies

Segmentation in Hybrid and Multi Cloud

Segmentation Journey and Challenges

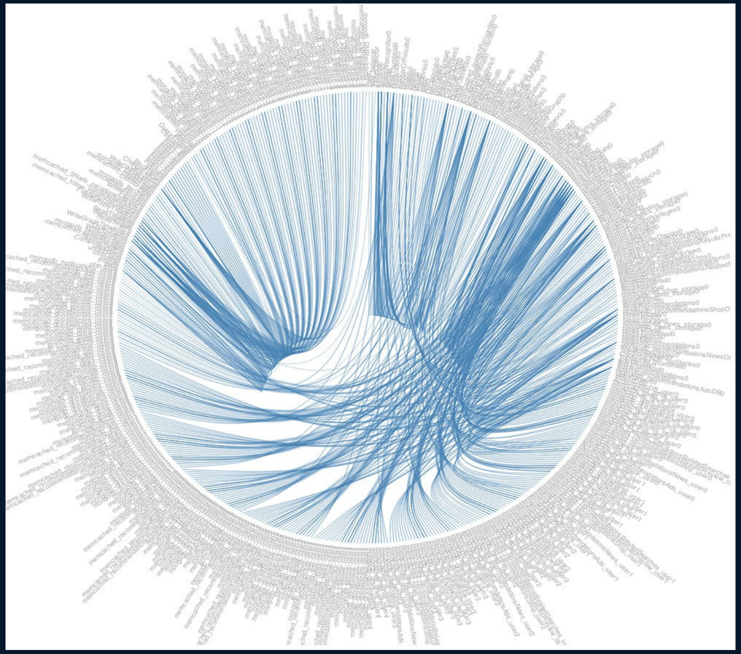
Multi-Cloud Defense

Secure Workload

Hyper Shield

Segmentation in Hybrid and Multi Cloud

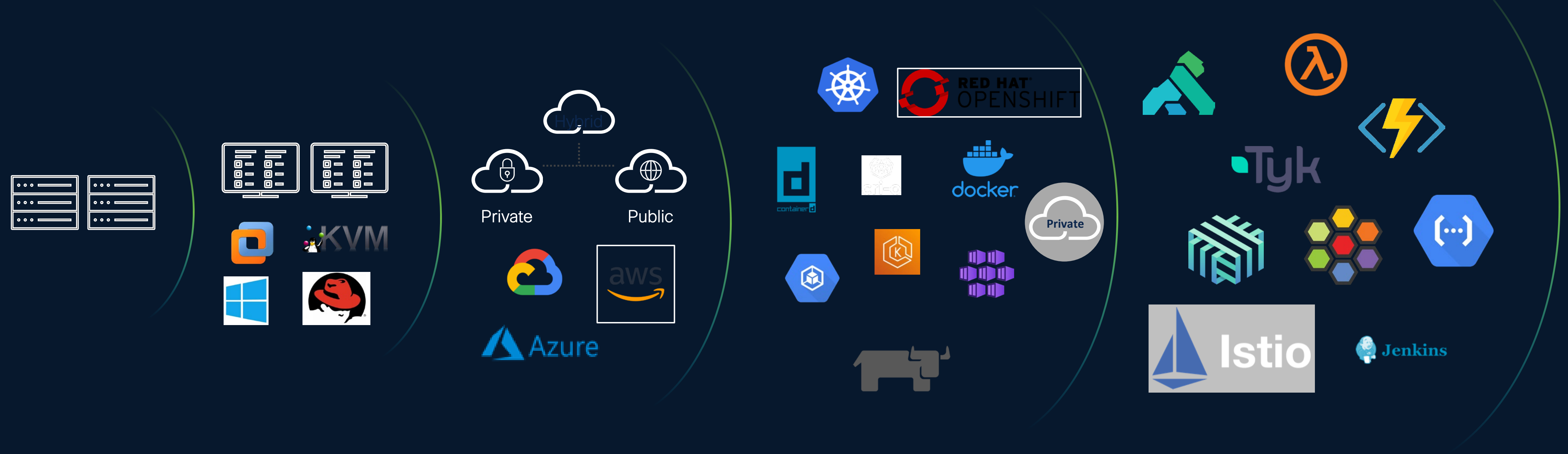
Applications are critical to modern businesses



Applications have dramatically evolved

Segmentation Journey and Challenges

Bare Metal | Virtualisation | Public Cloud pilot | Containers Pilot | K8s Full adoption | Embracing Cloud Native



System Admin | VM Admin | Cloud InfraOps | K8s Administrators | AppOps and DevOps

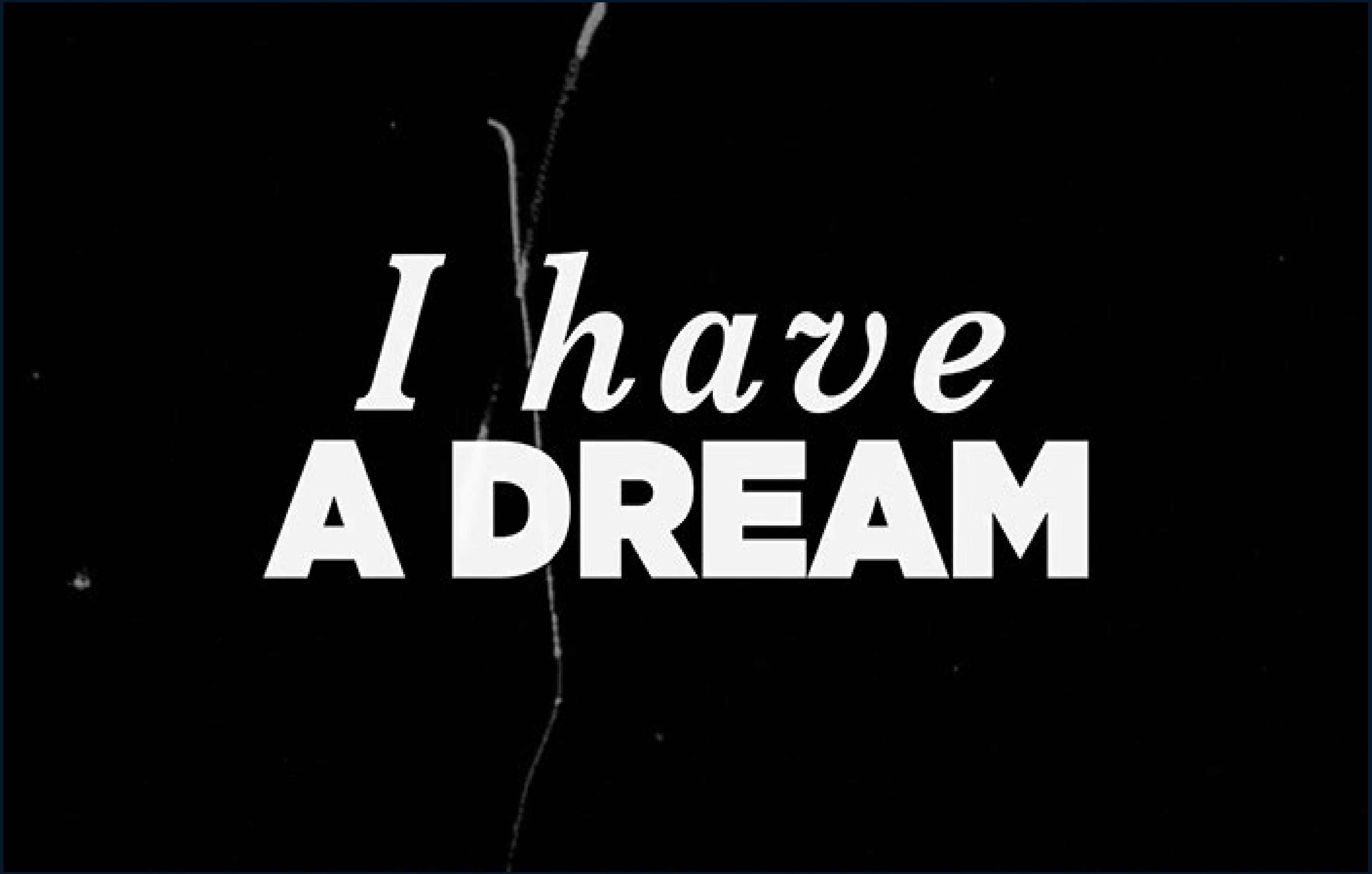
Segmentation Journey and Challenges

NetOps
SecOps
Cloud InfraOps
DevSecOps
K8 Admins

Some of the challenges

- Roles and responsabilities
- Understand the Applications behavior to build a policy
- Different security Domains (groups, objects, labels, Tags…)
- Speed of changes of applications
- Changing policy could break an application
- Several types of enforcement points
- …

Ideal Solution



Some ideas towards Ideal Solutions

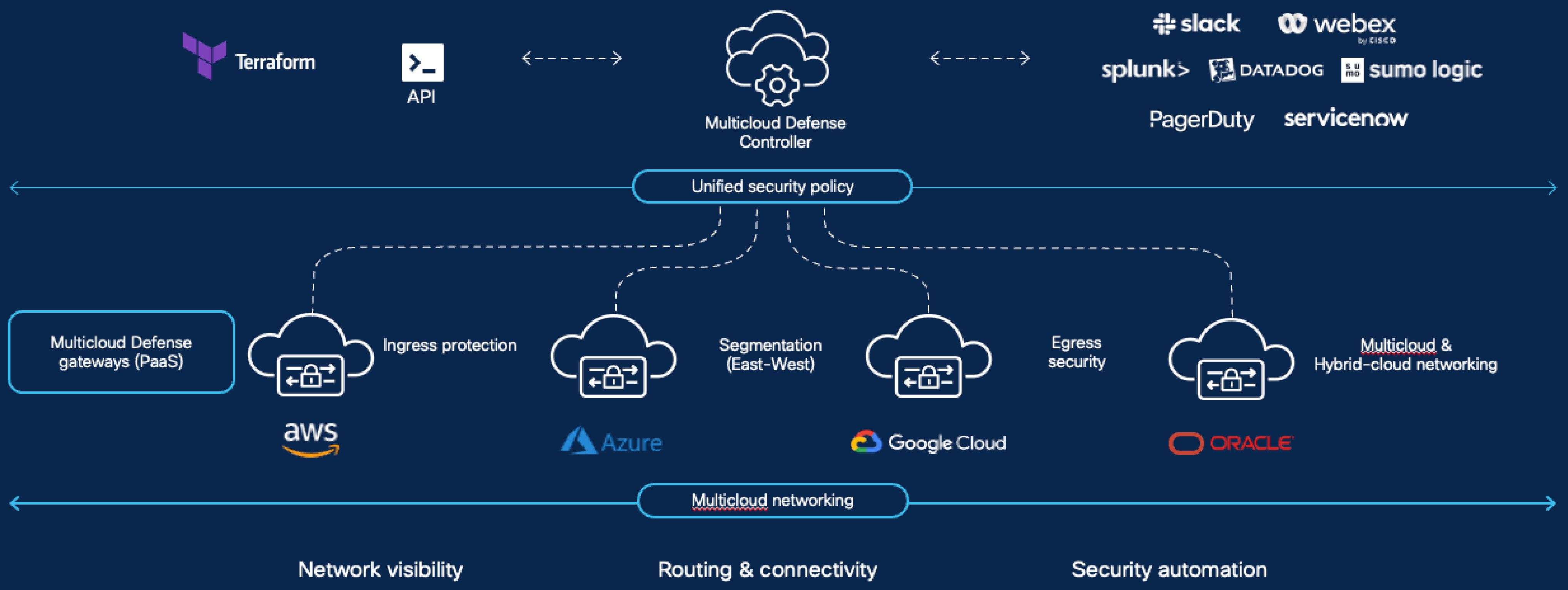
- Automatically discover new applications
- Understand the different way to identify applications
- Automatically map application behaviour to a Zero Trust policy
- Automatically adapt the policy when changes happen
- Test the policy before enforcing it
- Pick the best medium to enforce a policy
- ...

Agenda

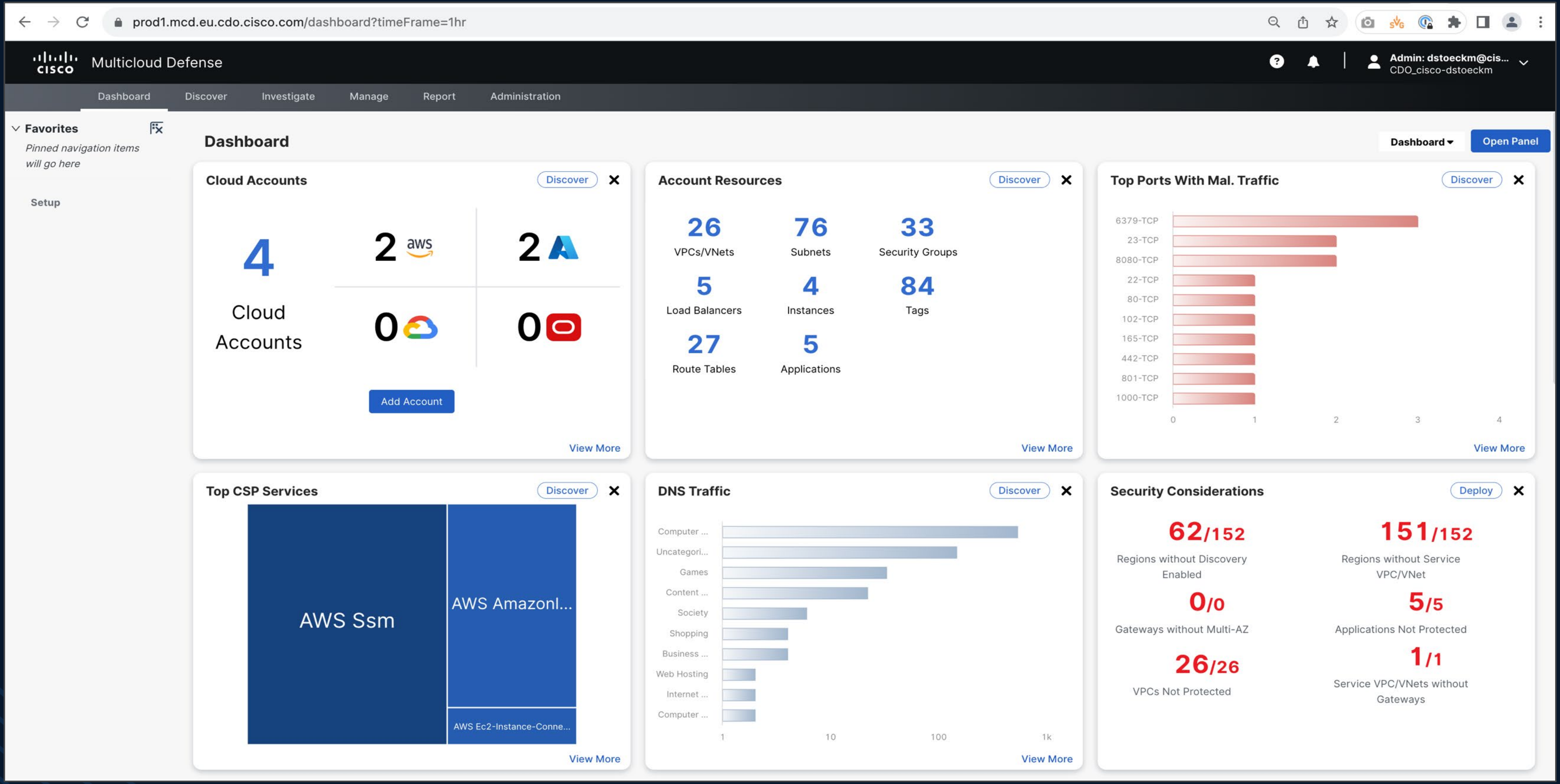
Cisco Multi-Cloud Defense

Cisco Multi-Cloud Defense

Combining multicloud networking, automation, and cloud native network security



Multi-Cloud Defense Asset Discovery & Visibility



Dashboard

Cloud Accounts

4 Cloud Accounts

2 aws

2 Azure

0 Google Cloud

0 Oracle

Account Resources

26 VPCs/VNets	76 Subnets	33 Security Groups
5 Load Balancers	4 Instances	84 Tags
27 Route Tables	5 Applications	

Top Ports With Mal. Traffic

Top CSP Services

DNS Traffic

Security Considerations

62/152 Regions without Discovery Enabled

151/152 Regions without Service VPC/VNet

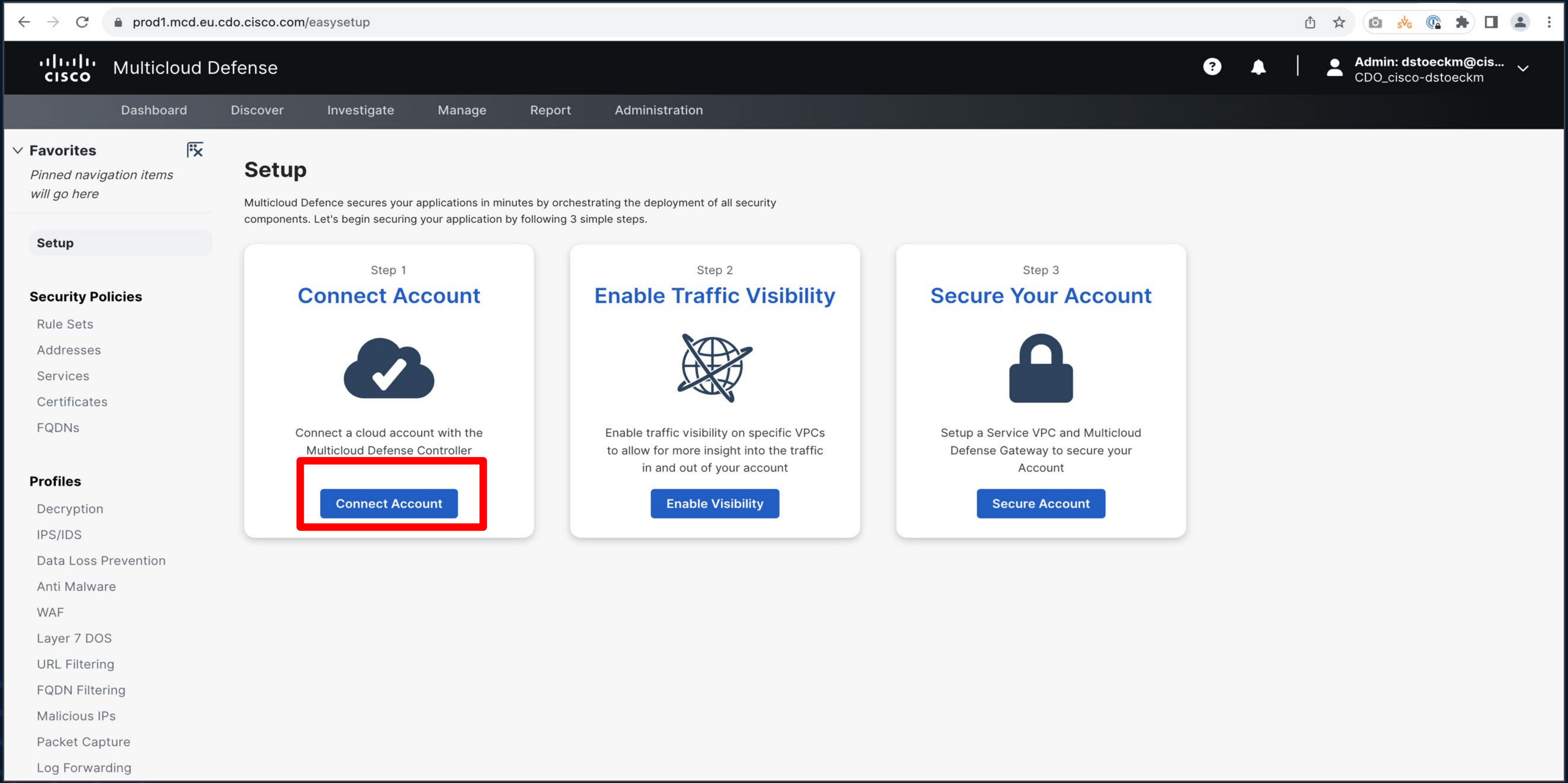
0/0 Gateways without Multi-AZ

5/5 Applications Not Protected

26/26 VPCs Not Protected

1/1 Service VPC/VNets without Gateways

Multi-Cloud Defense Asset Discovery & Visibility



Setup

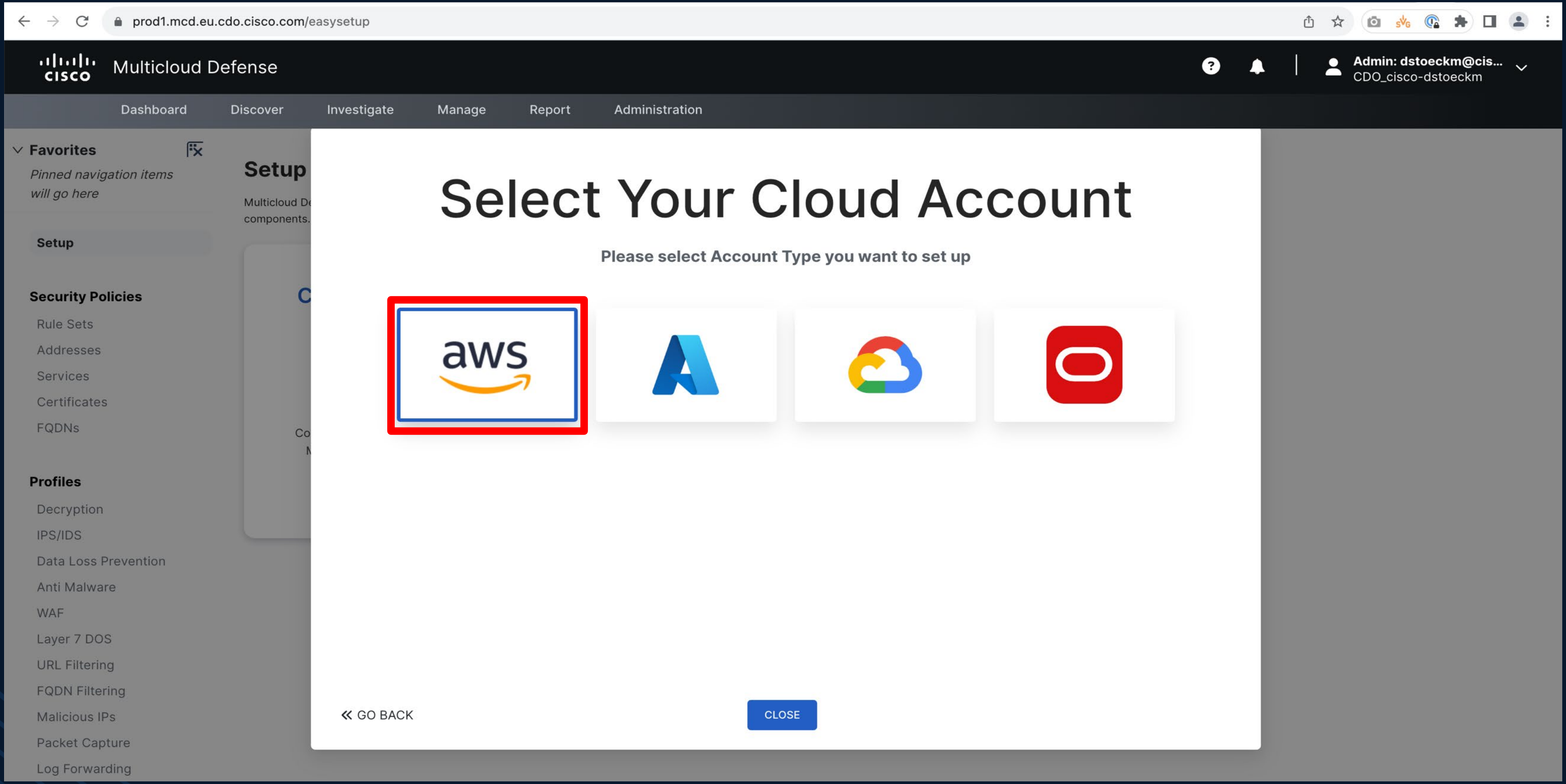
Multicloud Defence secures your applications in minutes by orchestrating the deployment of all security components. Let's begin securing your application by following 3 simple steps.

Step 1
Connect Account
Connect a cloud account with the Multicloud Defense Controller
Connect Account

Step 2
Enable Traffic Visibility
Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account
Enable Visibility

Step 3
Secure Your Account
Setup a Service VPC and Multicloud Defense Gateway to secure your Account
Secure Account

Multi-Cloud Defense Asset Discovery & Visibility



prod1.mcd.eu.cdo.cisco.com/easysetup

Multicloud Defense

Admin: dstoeckm@cis...
CDO_cisco-dstoeckm

Dashboard | Discover | Investigate | Manage | Report | Administration

Favorites

Pinned navigation items will go here

Setup

Security Policies
- Rule Sets
- Addresses
- Services
- Certificates
- FQDNs

Profiles
- Decryption
- IPS/IDS
- Data Loss Prevention
- Anti Malware
- WAF
- Layer 7 DOS
- URL Filtering
- FQDN Filtering
- Malicious IPs
- Packet Capture
- Log Forwarding

Setup

Multicloud De
components.

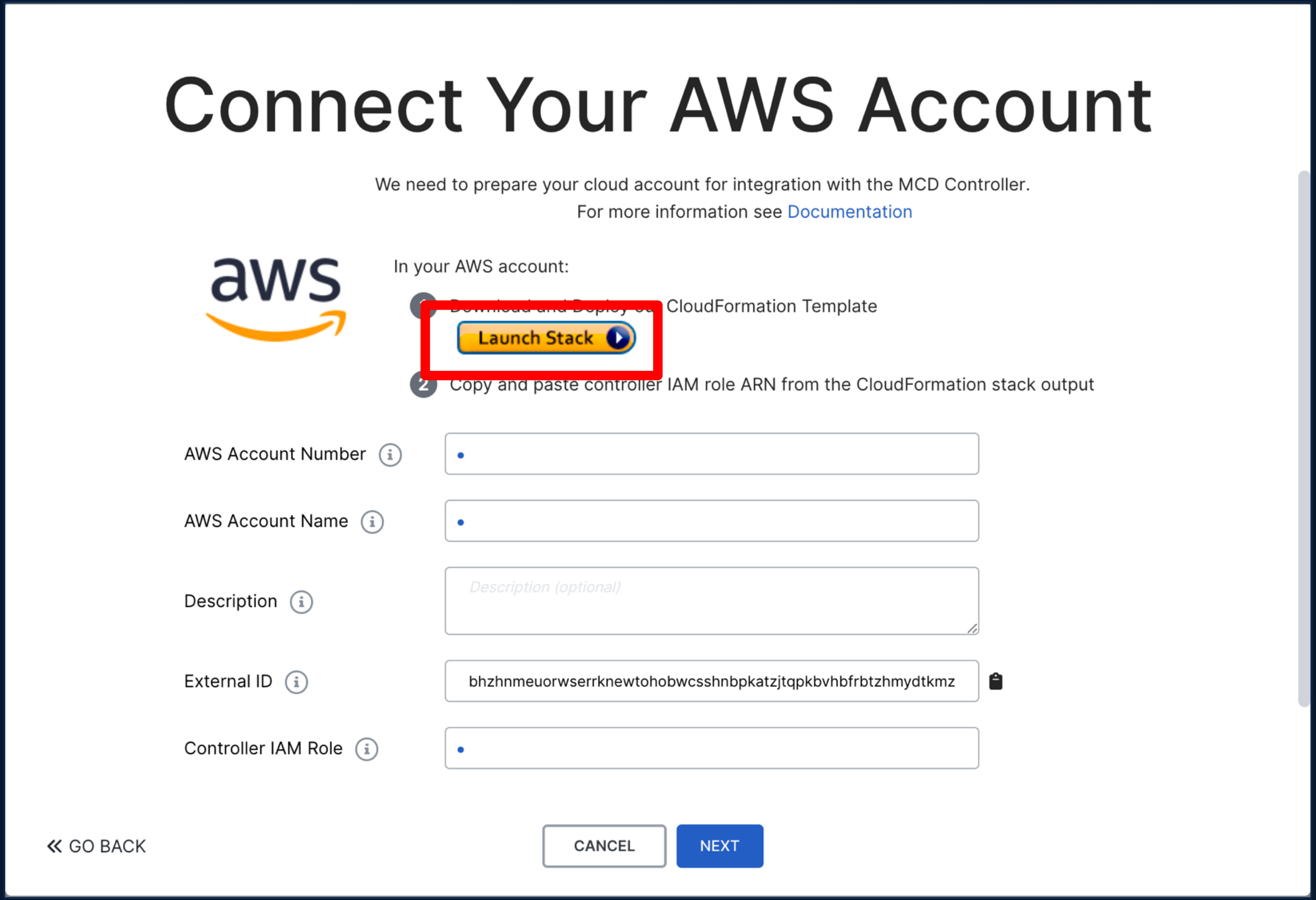
Select Your Cloud Account

Please select Account Type you want to set up

« GO BACK

CLOSE

Multi-Cloud Defense Asset Discovery & Visibility



Connect Your AWS Account

We need to prepare your cloud account for integration with the MCD Controller.
For more information see Documentation

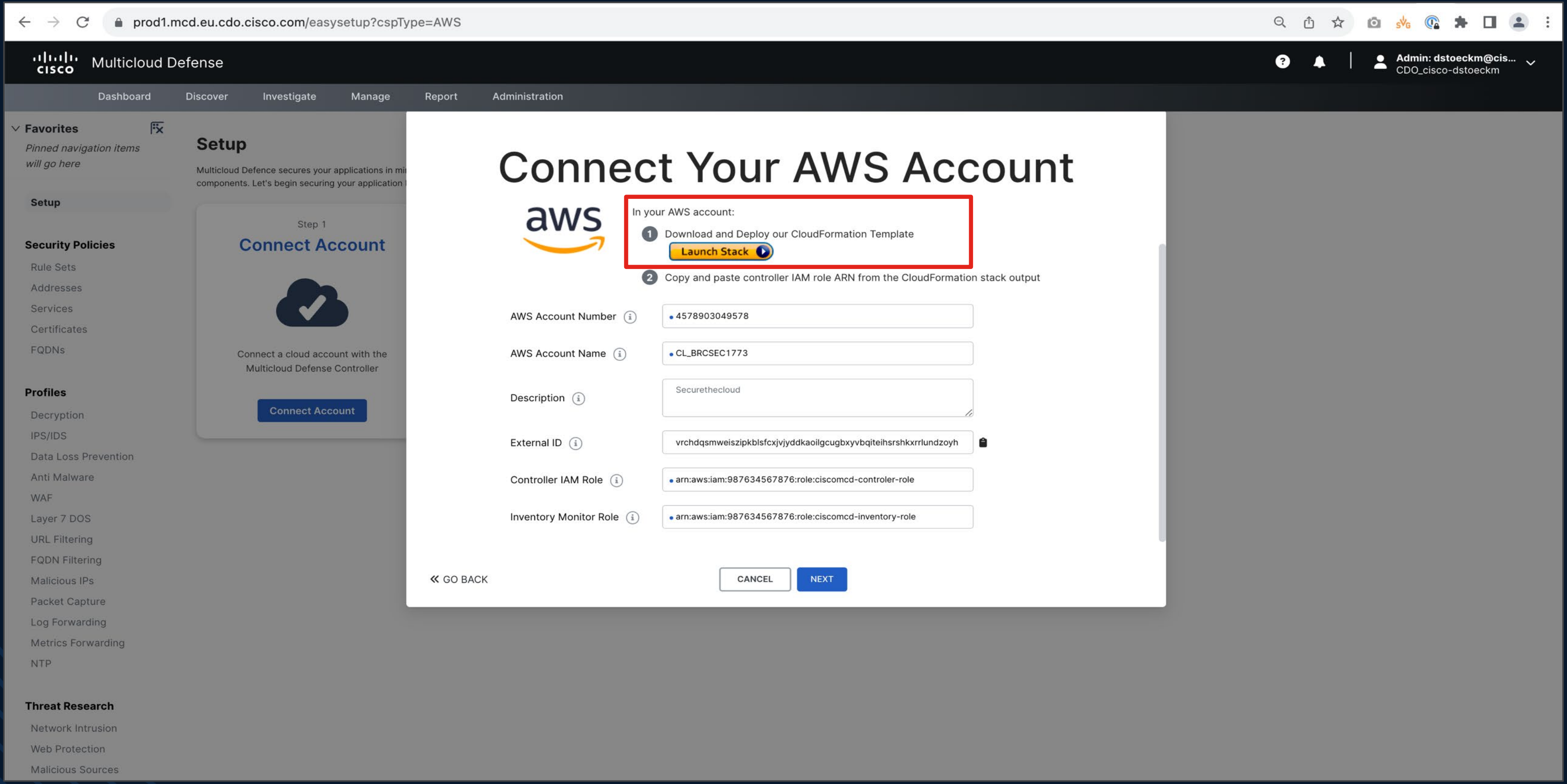
In your AWS account:

1 Download and Deploy our CloudFormation Template

2 Copy and paste controller IAM role ARN from the CloudFormation stack output

AWS Account Number ⓘ	•
AWS Account Name ⓘ	•
Description ⓘ	Description (optional)
External ID ⓘ	bhzhnmeuorwserrknewtohobwcsshnbpkatzjtqpkbvhbfrbtzhmydtkmz
Controller IAM Role ⓘ	•

Multi-Cloud Defense Asset Discovery & Visibility



Setup

Multicloud Defence secures your applications in mi
components. Let's begin securing your application

Step 1

Connect Account

Connect a cloud account with the Multicloud Defense Controller

Connect Your AWS Account

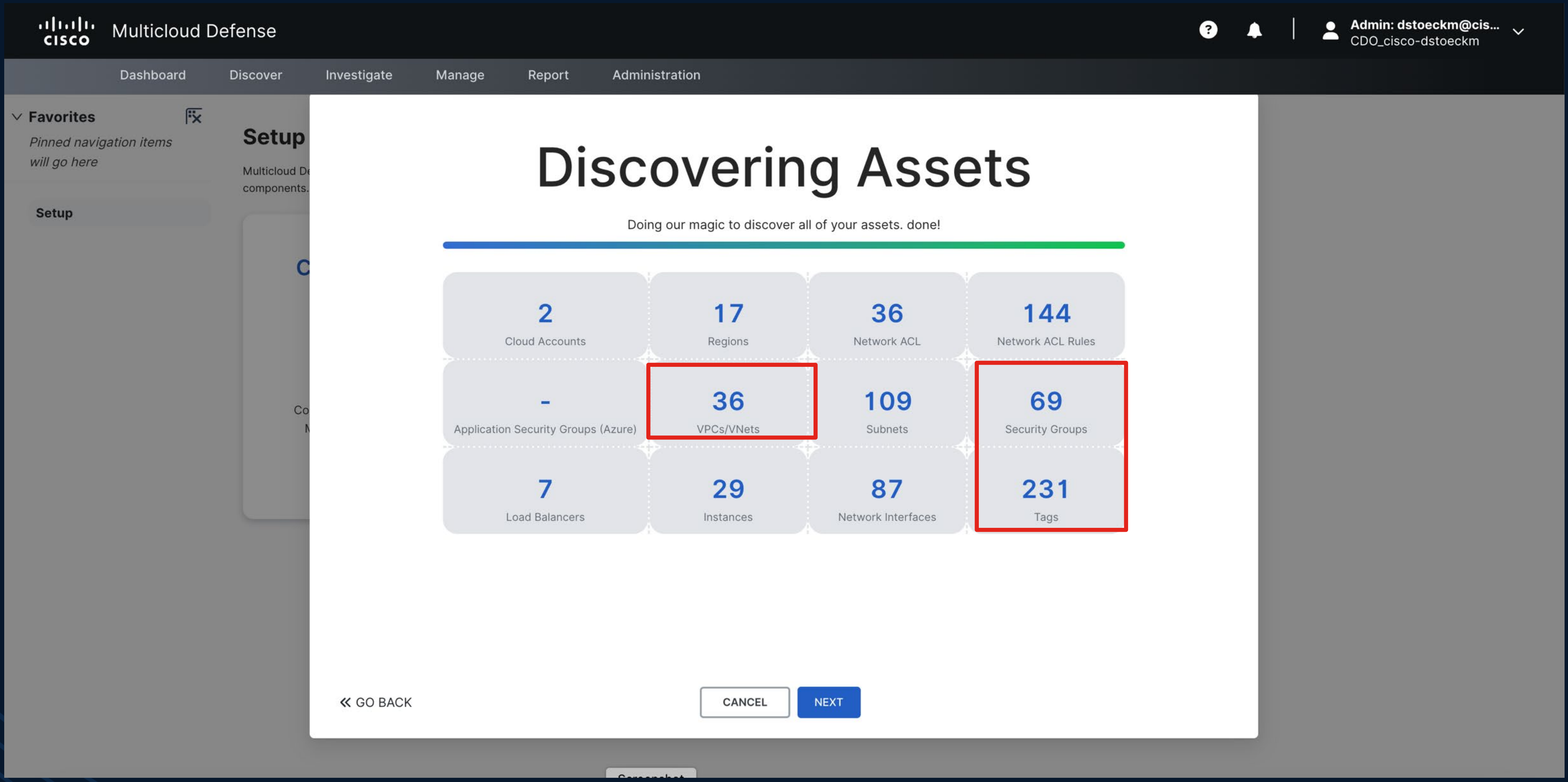
In your AWS account:

1. Download and Deploy our CloudFormation Template

2. Copy and paste controller IAM role ARN from the CloudFormation stack output

AWS Account Number	4578903049578
AWS Account Name	CL_BRCSEC1773
Description	Securethecloud
External ID	vrchdqsmweiszipkblsfcxjvjyddkaoilgcugbxyvbqiteihsrshkxrrlundzoyh
Controller IAM Role	arn:aws:iam:987634567876:role:ciscomcd-controler-role
Inventory Monitor Role	arn:aws:iam:987634567876:role:ciscomcd-inventory-role

Multi-Cloud Defense Asset Discovery & Visibility

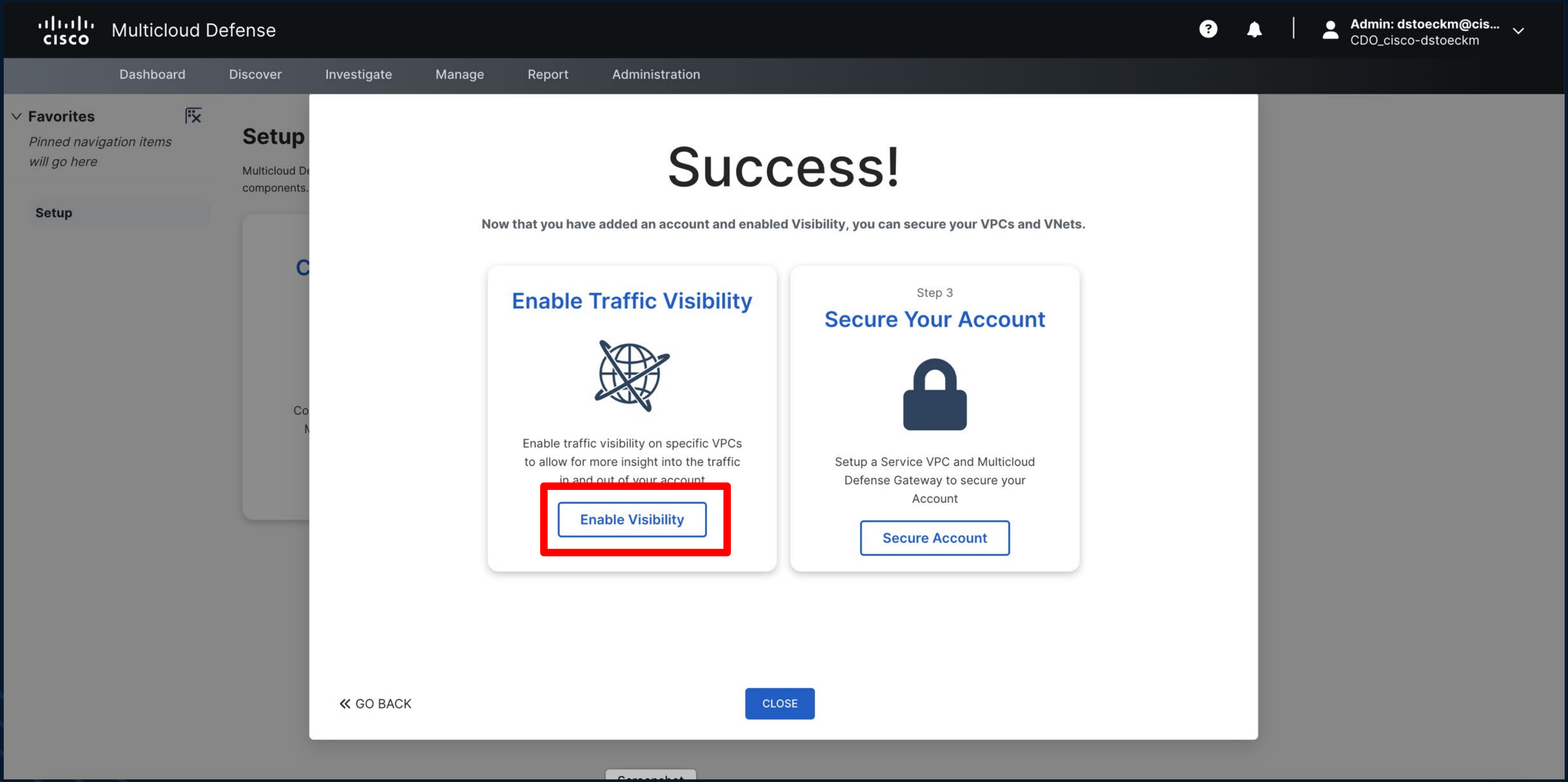


Discovering Assets

Doing our magic to discover all of your assets. done!

2 Cloud Accounts	17 Regions	36 Network ACL	144 Network ACL Rules
- Application Security Groups (Azure)	36 VPCs/VNets	109 Subnets	69 Security Groups
7 Load Balancers	29 Instances	87 Network Interfaces	231 Tags

Multi-Cloud Defense Asset Discovery & Visibility



Setup

Multicloud De components.

Success!

Now that you have added an account and enabled Visibility, you can secure your VPCs and VNets.

Enable Traffic Visibility

Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Enable Visibility

Step 3

Secure Your Account

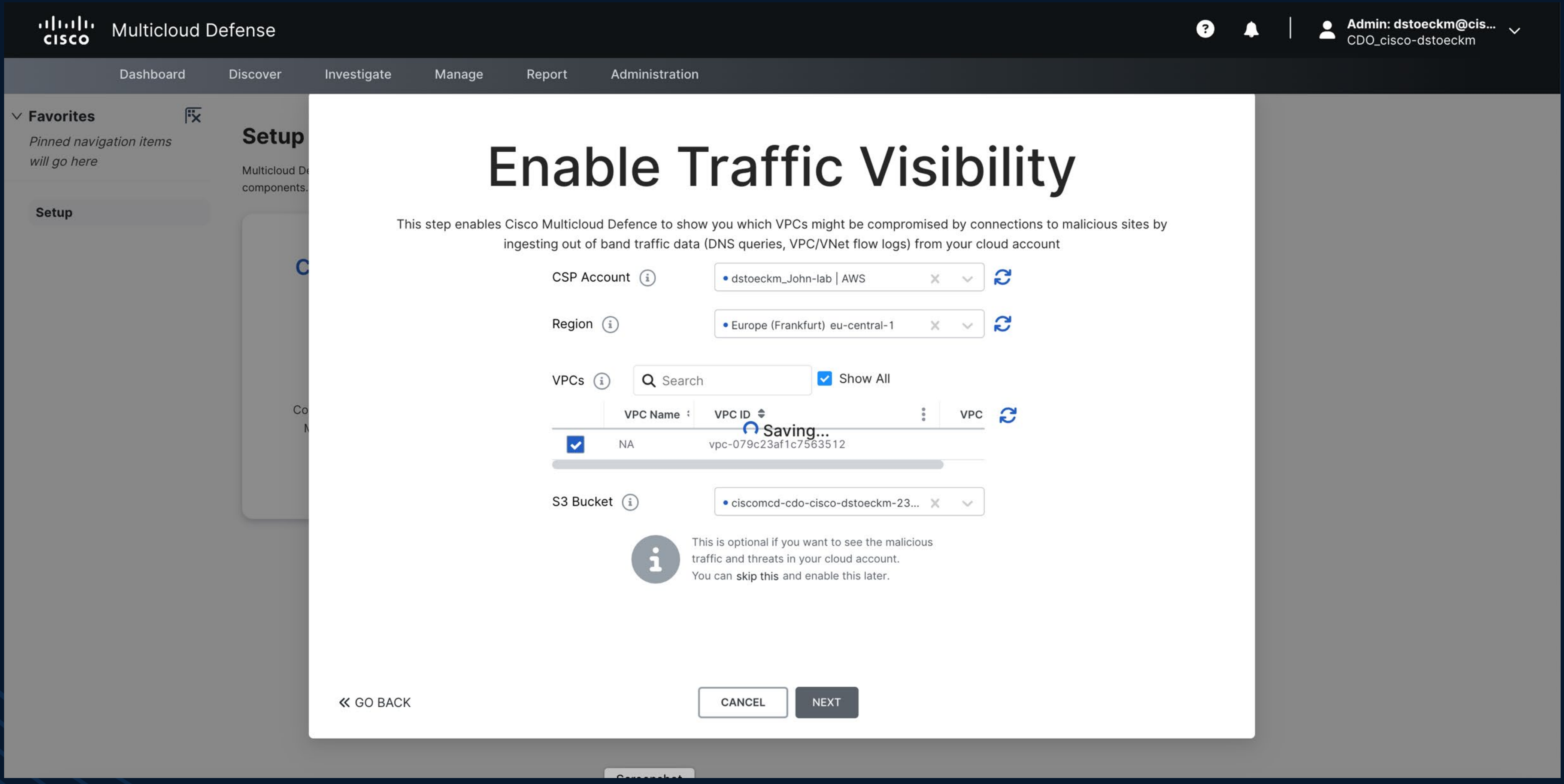
Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

« GO BACK

CLOSE

Multi-Cloud Defense Asset Discovery & Visibility



Enable Traffic Visibility

This step enables Cisco Multicloud Defence to show you which VPCs might be compromised by connections to malicious sites by ingesting out of band traffic data (DNS queries, VPC/VNet flow logs) from your cloud account

CSP Account: dstoeckm_John-lab | AWS

Region: Europe (Frankfurt) eu-central-1

VPCs: Search ☑ Show All

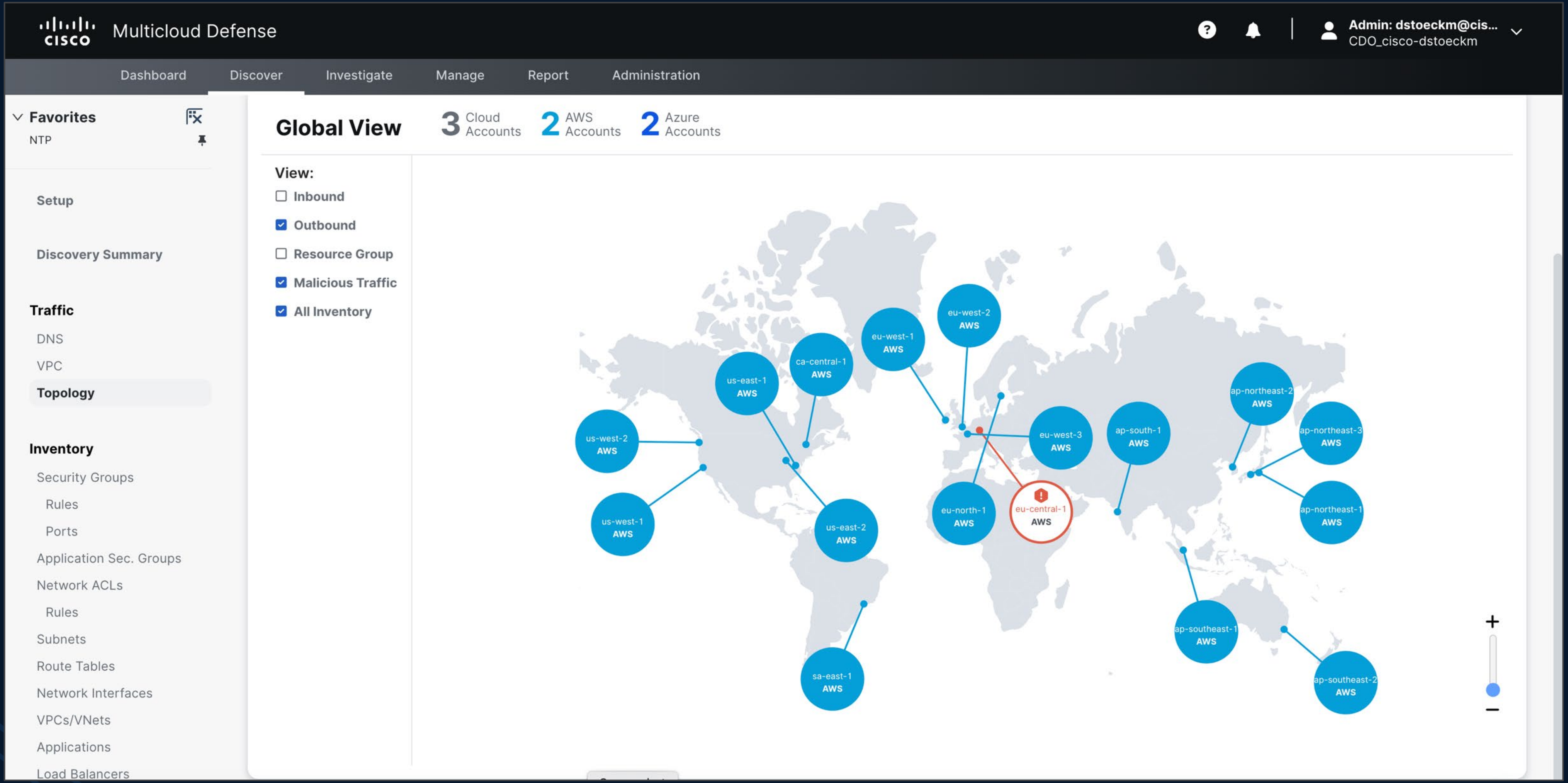
	VPC Name	VPC ID	VPC
☑	NA	vpc-079c23af1c7563512	

Saving...

S3 Bucket: ciscomcd-cdo-cisco-dstoeckm-23...

This is optional if you want to see the malicious traffic and threats in your cloud account. You can skip this and enable this later.

Multi-Cloud Defense Asset Discovery & Visibility



Global View

3 Cloud Accounts

2 AWS Accounts

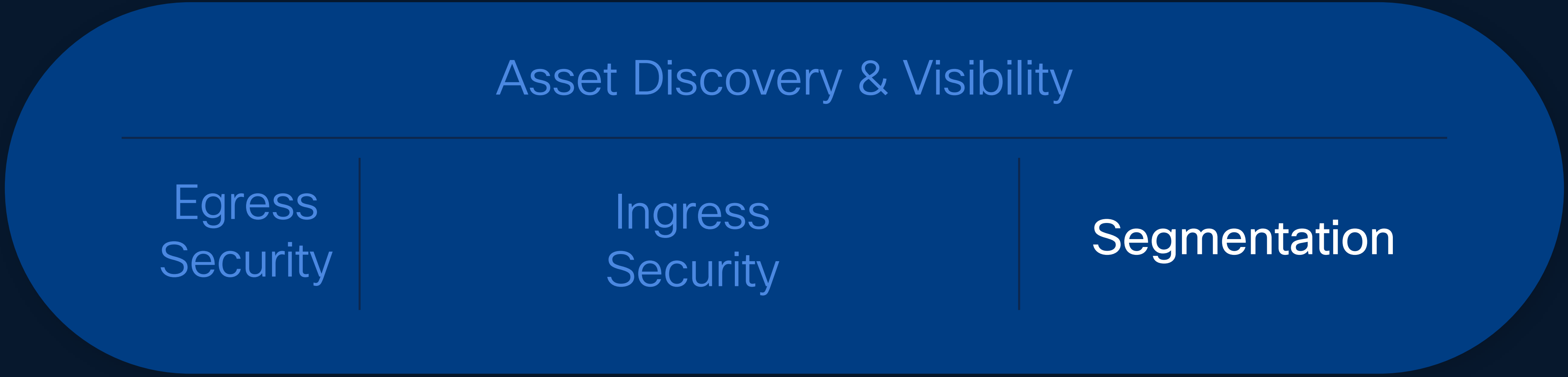
2 Azure Accounts

View:

- ☐ Inbound
- ☑ Outbound
- ☐ Resource Group
- ☑ Malicious Traffic
- ☑ All Inventory

Multi-Cloud Defense Asset Discovery & Visibility

Cisco Multicloud Defense



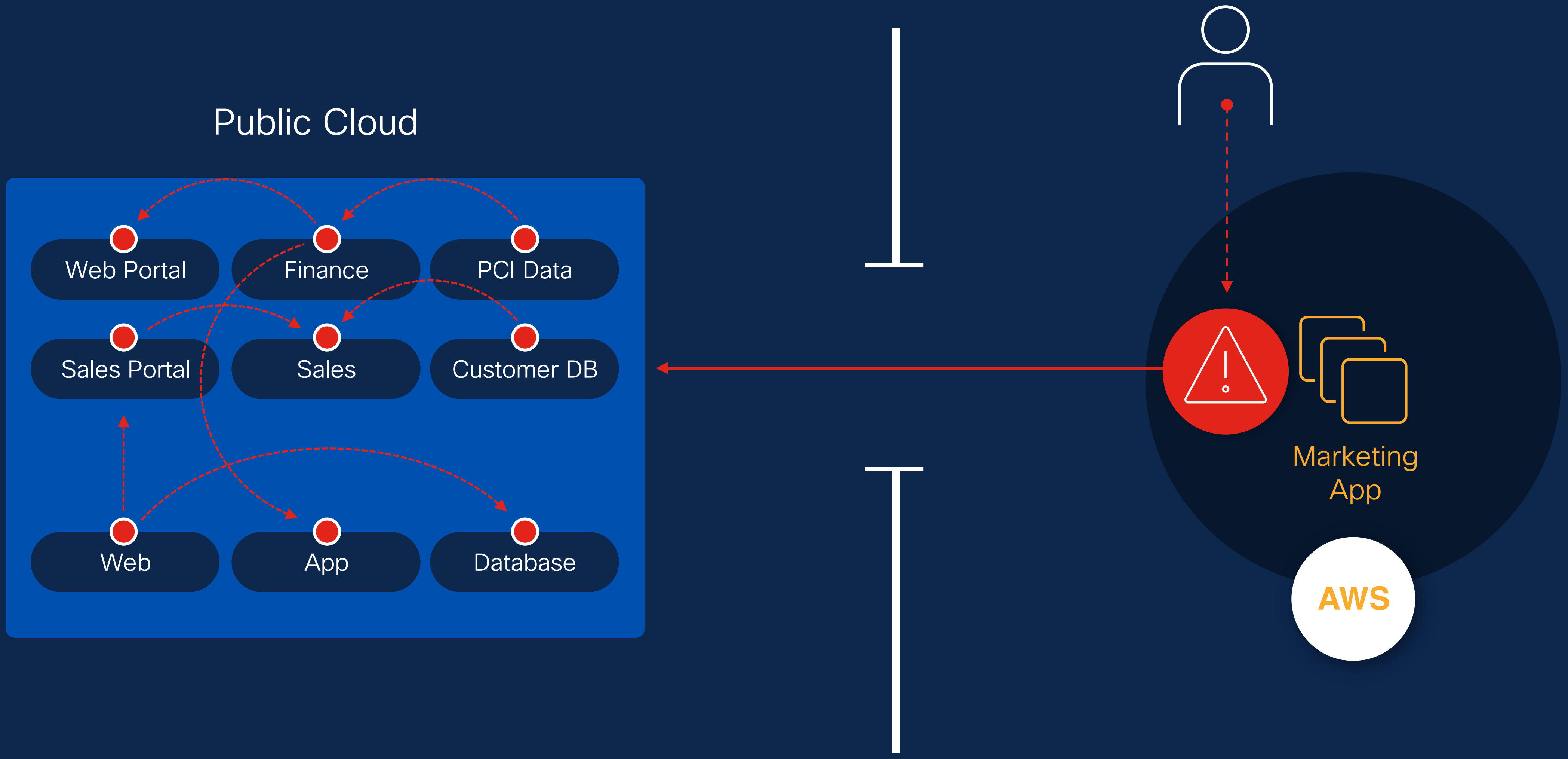
Asset Discovery & Visibility

Egress Security

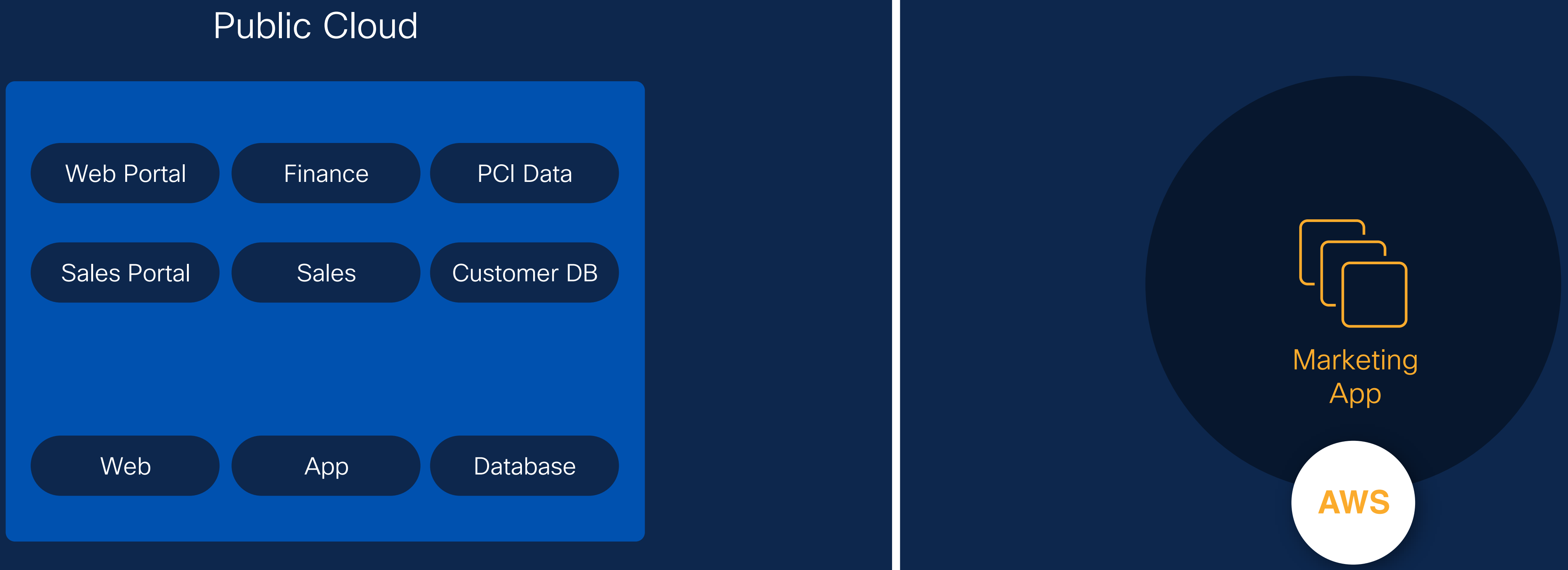
Ingress Security

Segmentation

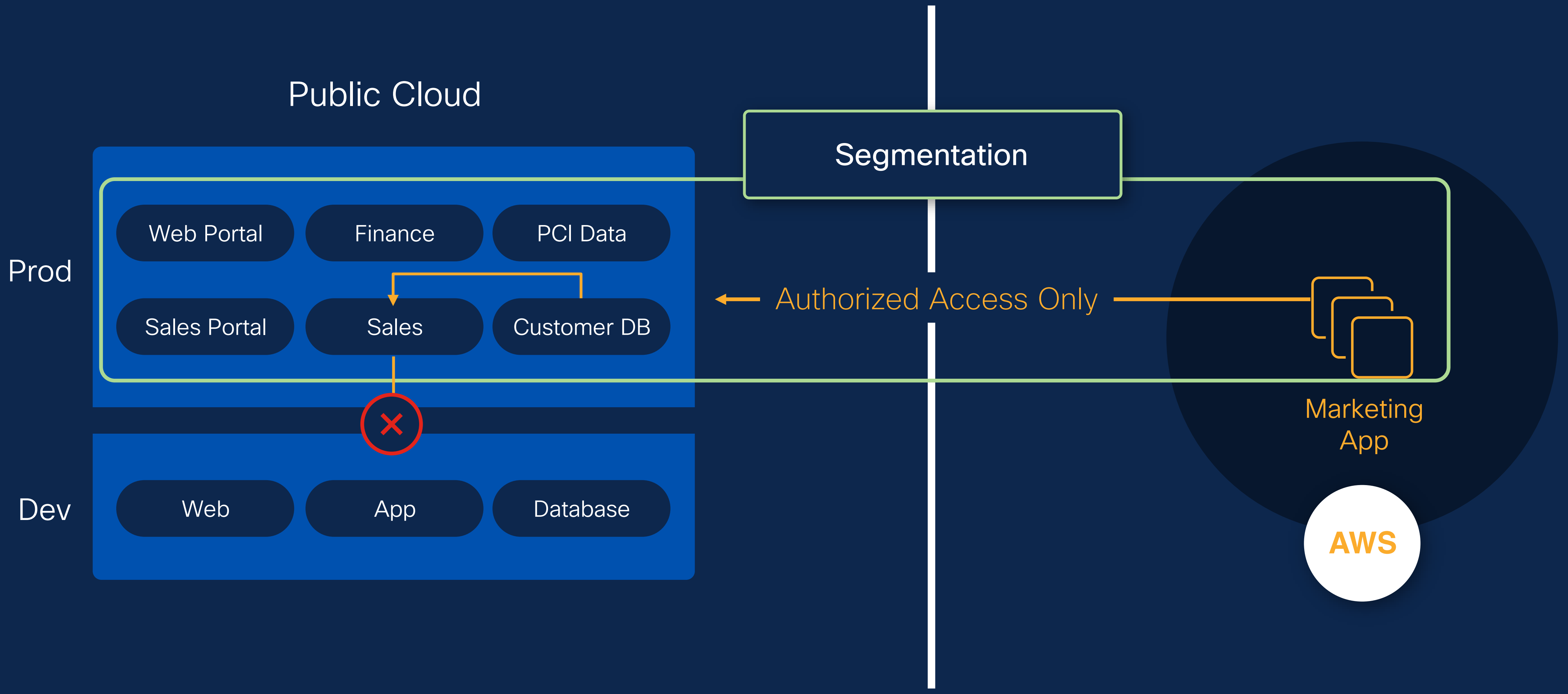
The exposure today



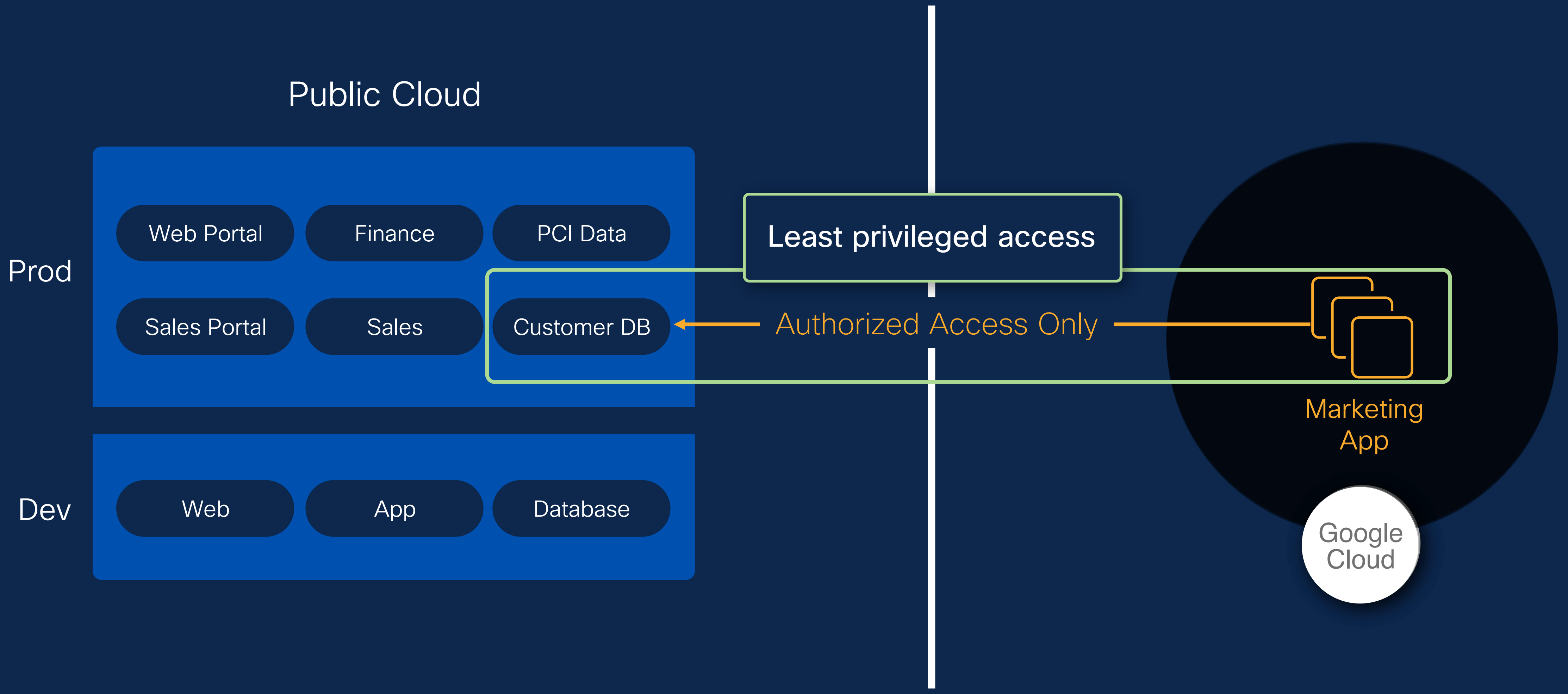
Lateral protection with segmentation



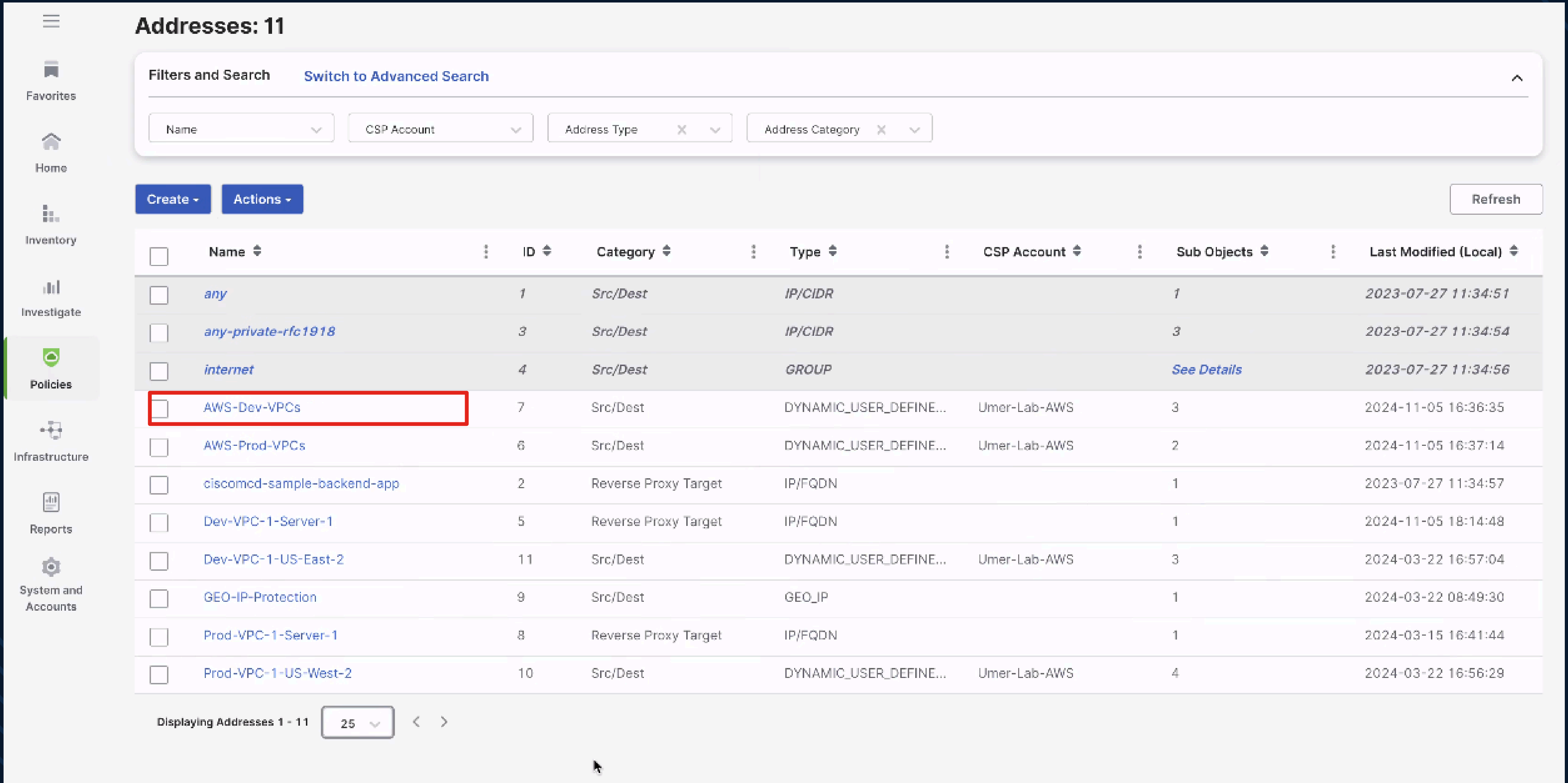
Lateral protection with segmentation



Lateral protection with segmentation



Segmentation in Multi-Cloud Defense



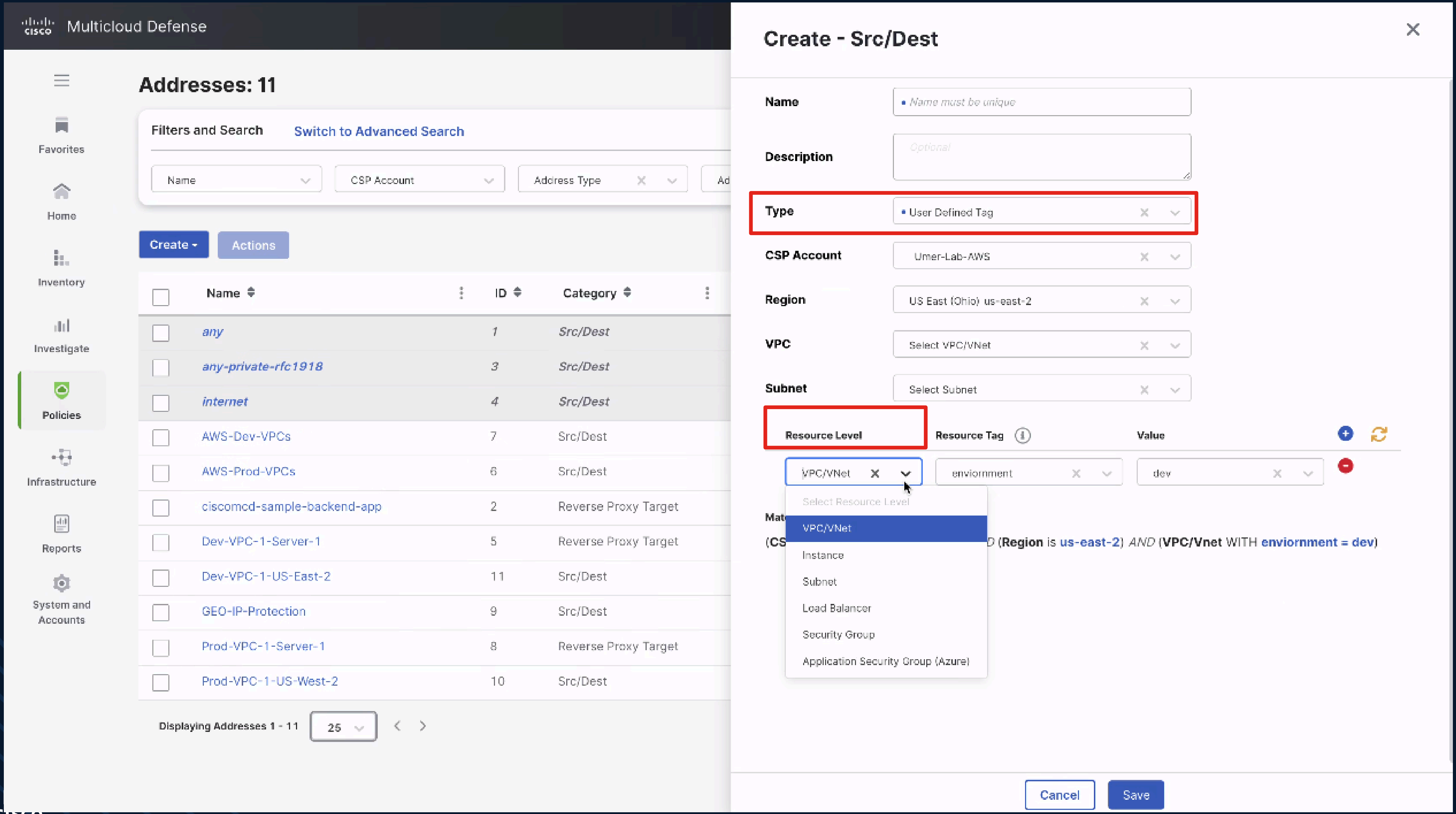
Addresses: 11

Filters and Search   Switch to Advanced Search

□	Name	ID	Category	Type	CSP Account	Sub Objects	Last Modified (Local)
□	*any*	*1*	*Src/Dest*	*IP/CIDR*		*1*	*2023-07-27 11:34:51*
□	*any-private-rfc1918*	*3*	*Src/Dest*	*IP/CIDR*		*3*	*2023-07-27 11:34:54*
□	*internet*	*4*	*Src/Dest*	*GROUP*		*See Details*	*2023-07-27 11:34:56*
□	AWS-Dev-VPCs	7	Src/Dest	DYNAMIC_USER_DEFINE...	Umer-Lab-AWS	3	2024-11-05 16:36:35
□	AWS-Prod-VPCs	6	Src/Dest	DYNAMIC_USER_DEFINE...	Umer-Lab-AWS	2	2024-11-05 16:37:14
□	ciscomcd-sample-backend-app	2	Reverse Proxy Target	IP/FQDN		1	2023-07-27 11:34:57
□	Dev-VPC-1-Server-1	5	Reverse Proxy Target	IP/FQDN		1	2024-11-05 18:14:48
□	Dev-VPC-1-US-East-2	11	Src/Dest	DYNAMIC_USER_DEFINE...	Umer-Lab-AWS	3	2024-03-22 16:57:04
□	GEO-IP-Protection	9	Src/Dest	GEO_IP		1	2024-03-22 08:49:30
□	Prod-VPC-1-Server-1	8	Reverse Proxy Target	IP/FQDN		1	2024-03-15 16:41:44
□	Prod-VPC-1-US-West-2	10	Src/Dest	DYNAMIC_USER_DEFINE...	Umer-Lab-AWS	4	2024-03-22 16:56:29

Displaying Addresses 1 - 11   25

Segmentation in Multi-Cloud Defense



Addresses: 11

Filters and Search Switch to Advanced Search

Name | CSP Account | Address Type | Ad

Create ▾ Actions

☐	Name	ID	Category
☐	*any*	*1*	*Src/Dest*
☐	*any-private-rfc1918*	*3*	*Src/Dest*
☐	*internet*	*4*	*Src/Dest*
☐	AWS-Dev-VPCs	7	Src/Dest
☐	AWS-Prod-VPCs	6	Src/Dest
☐	ciscomcd-sample-backend-app	2	Reverse Proxy Target
☐	Dev-VPC-1-Server-1	5	Reverse Proxy Target
☐	Dev-VPC-1-US-East-2	11	Src/Dest
☐	GEO-IP-Protection	9	Src/Dest
☐	Prod-VPC-1-Server-1	8	Reverse Proxy Target
☐	Prod-VPC-1-US-West-2	10	Src/Dest

Displaying Addresses 1 - 11 25 ‹ ›

Create - Src/Dest

Name	Name must be unique
Description	Optional
Type	User Defined Tag
CSP Account	Umer-Lab-AWS
Region	US East (Ohio) us-east-2
VPC	Select VPC/VNet
Subnet	Select Subnet

Resource Level	Resource Tag	Value
VPC/VNet	enviornment	dev

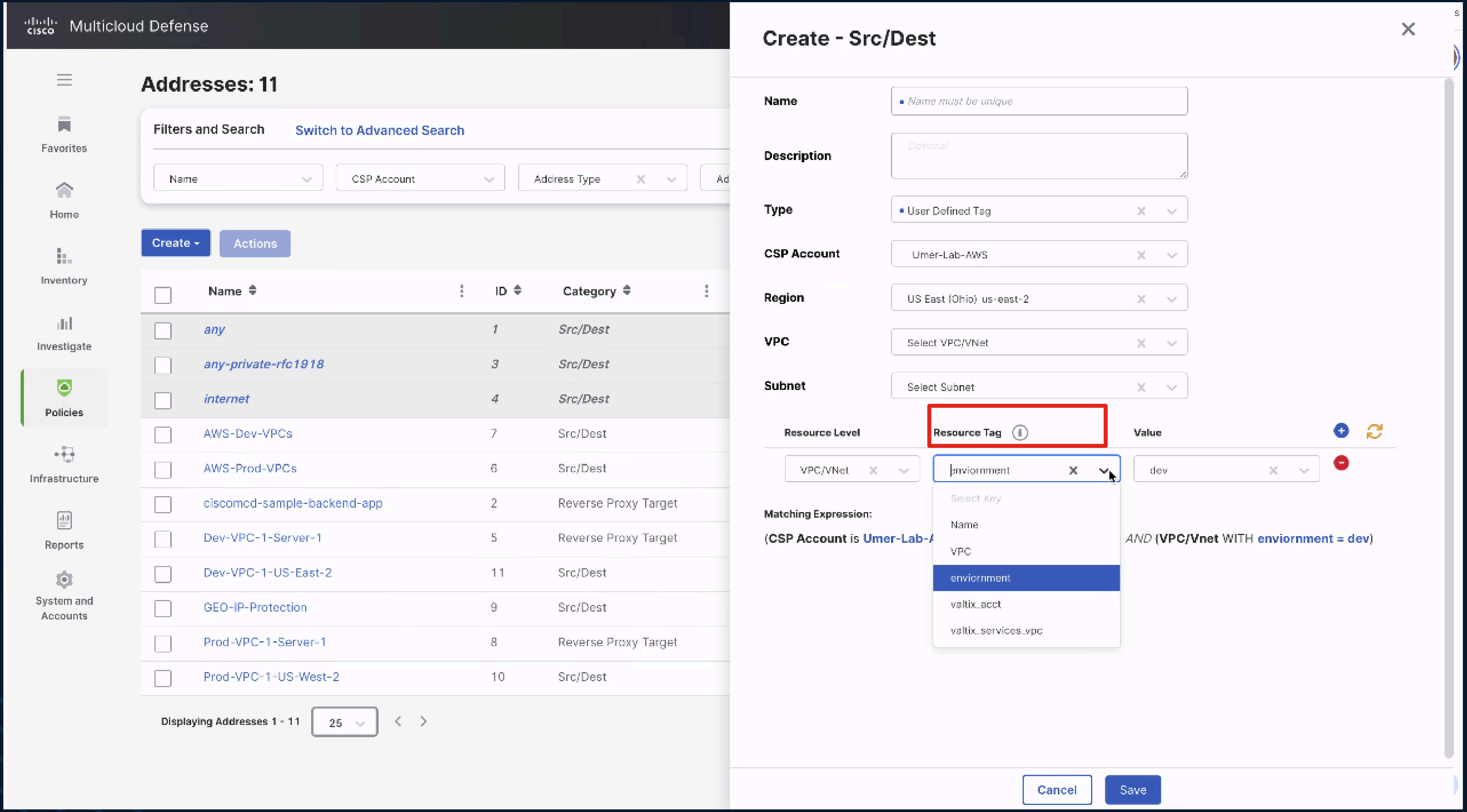
Select Resource Level
- VPC/VNet
- Instance
- Subnet
- Load Balancer
- Security Group
- Application Security Group (Azure)

Mat

(CS D (**Region** is us-east-2) *AND* (**VPC/Vnet** WITH enviornment = dev)

Cancel Save

Segmentation in Multi-Cloud Defense



Addresses: 11

Filters and Search | Switch to Advanced Search

Name | CSP Account | Address Type | Ad

Create | Actions

☐	Name	ID	Category
☐	*any*	*1*	*Src/Dest*
☐	*any-private-rfc1918*	*3*	*Src/Dest*
☐	*internet*	*4*	*Src/Dest*
☐	AWS-Dev-VPCs	7	Src/Dest
☐	AWS-Prod-VPCs	6	Src/Dest
☐	ciscomcd-sample-backend-app	2	Reverse Proxy Target
☐	Dev-VPC-1-Server-1	5	Reverse Proxy Target
☐	Dev-VPC-1-US-East-2	11	Src/Dest
☐	GEO-IP-Protection	9	Src/Dest
☐	Prod-VPC-1-Server-1	8	Reverse Proxy Target
☐	Prod-VPC-1-US-West-2	10	Src/Dest

Displaying Addresses 1 - 11 | 25

Create - Src/Dest

Name	Name must be unique
Description	Optional
Type	User Defined Tag
CSP Account	Umer-Lab-AWS
Region	US East (Ohio) us-east-2
VPC	Select VPC/VNet
Subnet	Select Subnet

Resource Level	Resource Tag	Value
VPC/VNet	enviornment	dev

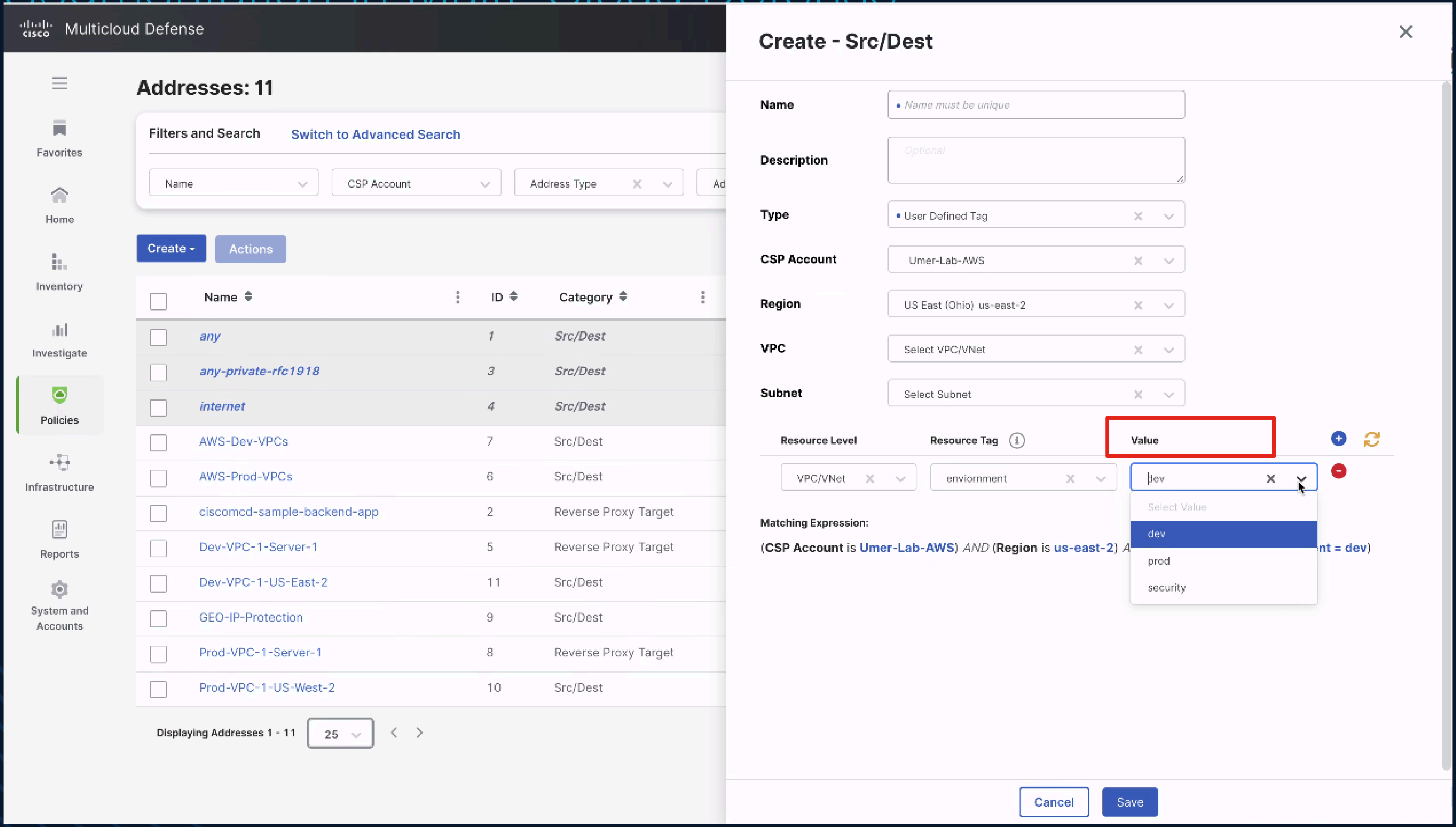
Select Key
- Name
- VPC
- enviornment
- valtix_acct
- valtix_services_vpc

Matching Expression:

(CSP Account is Umer-Lab-A AND (VPC/Vnet WITH enviornment = dev)

Cancel | Save

Segmentation in Multi-Cloud Defense



Multicloud Defense

Addresses: 11

Filters and Search Switch to Advanced Search

□	Name	ID	Category
□	*any*	*1*	*Src/Dest*
□	*any-private-rfc1918*	*3*	*Src/Dest*
□	*internet*	*4*	*Src/Dest*
□	AWS-Dev-VPCs	7	Src/Dest
□	AWS-Prod-VPCs	6	Src/Dest
□	ciscomcd-sample-backend-app	2	Reverse Proxy Target
□	Dev-VPC-1-Server-1	5	Reverse Proxy Target
□	Dev-VPC-1-US-East-2	11	Src/Dest
□	GEO-IP-Protection	9	Src/Dest
□	Prod-VPC-1-Server-1	8	Reverse Proxy Target
□	Prod-VPC-1-US-West-2	10	Src/Dest

Displaying Addresses 1 - 11 25

Create - Src/Dest

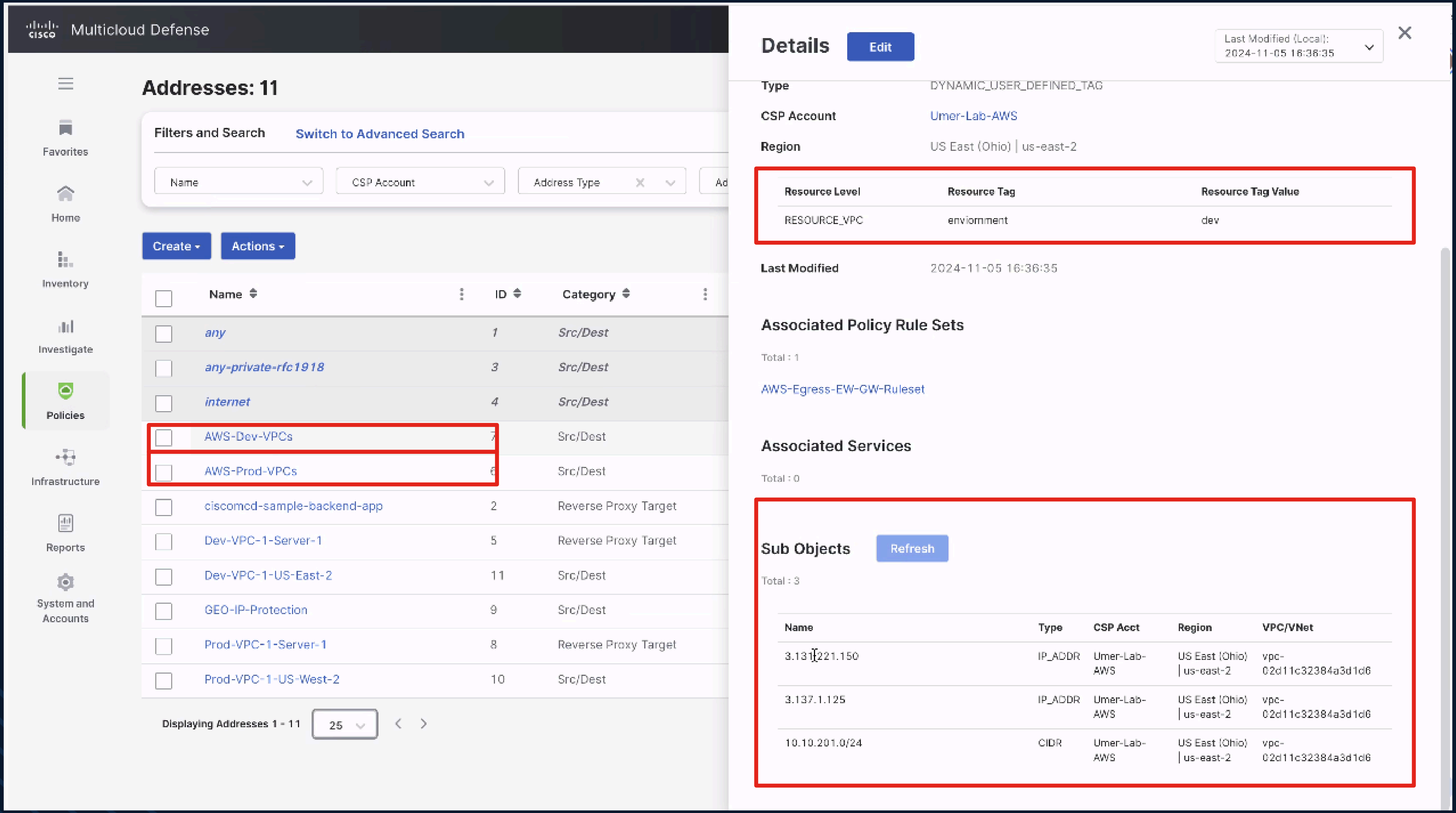
Name	• *Name must be unique*
Description	*Optional*
Type	• User Defined Tag
CSP Account	Umer-Lab-AWS
Region	US East (Ohio) us-east-2
VPC	Select VPC/VNet
Subnet	Select Subnet

Resource Level	Resource Tag	Value
VPC/VNet	enviornment	dev

Matching Expression:

(**CSP Account** is **Umer-Lab-AWS**) *AND* (**Region** is **us-east-2**) *A* **nt = dev**)

Segmentation in Multi-Cloud Defense



Addresses: 11

Filters and Search

Name | CSP Account | Address Type | Ad

Name	ID	Category
any	1	Src/Dest
any-private-rfc1918	3	Src/Dest
internet	4	Src/Dest
AWS-Dev-VPCs	7	Src/Dest
AWS-Prod-VPCs	6	Src/Dest
ciscomcd-sample-backend-app	2	Reverse Proxy Target
Dev-VPC-1-Server-1	5	Reverse Proxy Target
Dev-VPC-1-US-East-2	11	Src/Dest
GEO-IP-Protection	9	Src/Dest
Prod-VPC-1-Server-1	8	Reverse Proxy Target
Prod-VPC-1-US-West-2	10	Src/Dest

Displaying Addresses 1 - 11   25

Details

Last Modified (Local): 2024-11-05 16:36:35

Type	DYNAMIC_USER_DEFINED_TAG
CSP Account	Umer-Lab-AWS
Region	US East (Ohio) | us-east-2

Resource Level	Resource Tag	Resource Tag Value
RESOURCE_VPC	enviornment	dev

Last Modified 2024-11-05 16:36:35

Associated Policy Rule Sets

Total : 1

AWS-Egress-EW-GW-Ruleset

Associated Services

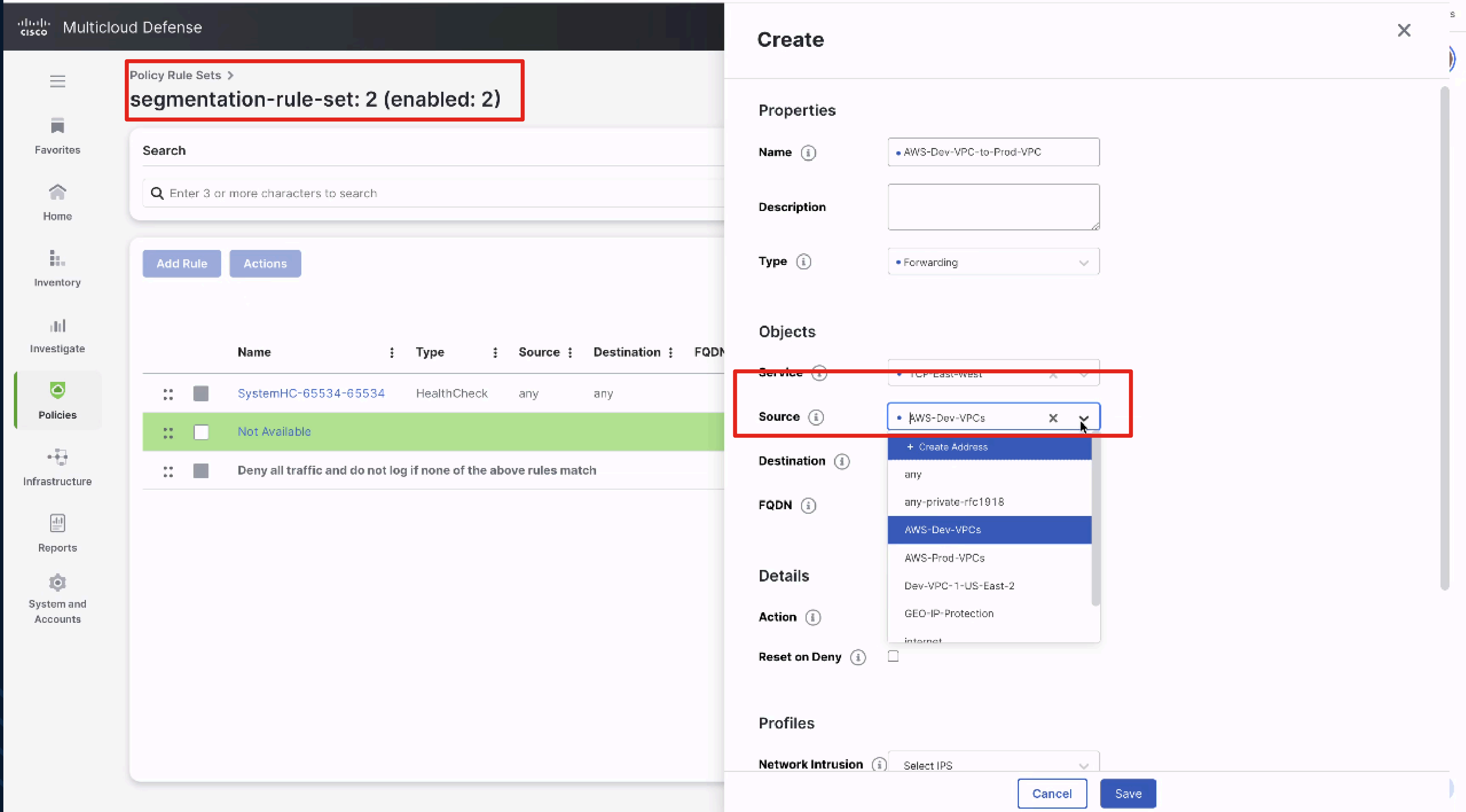
Total : 0

Sub Objects

Total : 3

Name	Type	CSP Acct	Region	VPC/VNet
3.131.221.150	IP_ADDR	Umer-Lab-AWS	US East (Ohio) | us-east-2	vpc-02d11c32384a3d1d6
3.137.1.125	IP_ADDR	Umer-Lab-AWS	US East (Ohio) | us-east-2	vpc-02d11c32384a3d1d6
10.10.201.0/24	CIDR	Umer-Lab-AWS	US East (Ohio) | us-east-2	vpc-02d11c32384a3d1d6

Segmentation in Multi-Cloud Defense



Policy Rule Sets >

segmentation-rule-set: 2 (enabled: 2)

Search

Enter 3 or more characters to search

	Name	Type	Source	Destination	FQDN
■	SystemHC-65534-65534	HealthCheck	any	any	
□	Not Available				
■	Deny all traffic and do not log if none of the above rules match				

Create

Properties

Name: AWS-Dev-VPC-to-Prod-VPC

Description:

Type: Forwarding

Objects

Service: TCP-East-West

Source: AWS-Dev-VPCs

- + Create Address
- any
- any-private-rfc1918
- AWS-Dev-VPCs
- AWS-Prod-VPCs
- Dev-VPC-1-US-East-2
- GEO-IP-Protection
- internet

Destination

FQDN

Details

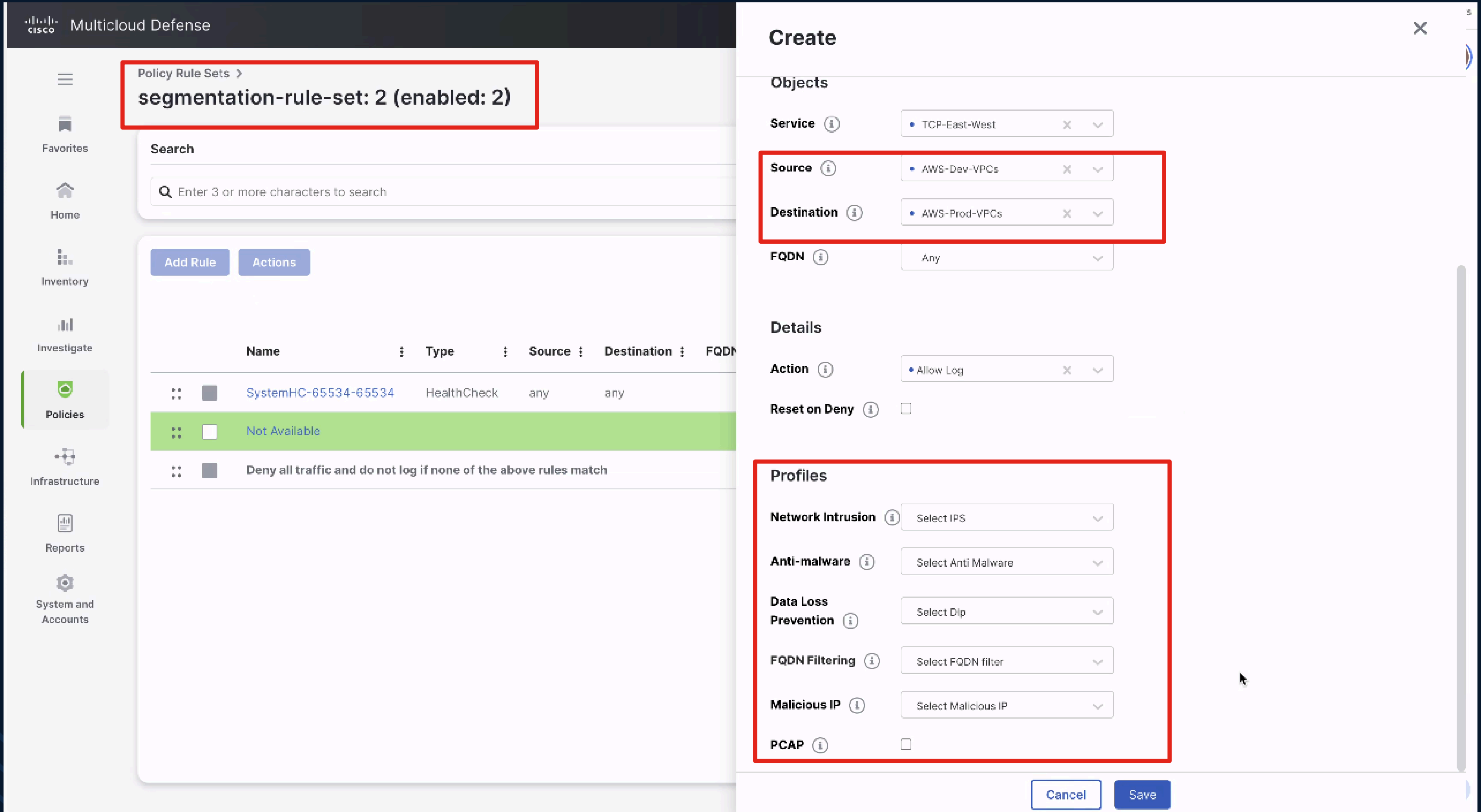
Action

Reset on Deny □

Profiles

Network Intrusion: Select IPS

Segmentation in Multi-Cloud Defense



Policy Rule Sets >

segmentation-rule-set: 2 (enabled: 2)

Search

Enter 3 or more characters to search

Name	Type	Source	Destination	FQDN
SystemHC-65534-65534	HealthCheck	any	any	
Not Available				
Deny all traffic and do not log if none of the above rules match				

Create

Objects

Service	TCP-East-West
Source	AWS-Dev-VPCs
Destination	AWS-Prod-VPCs
FQDN	Any

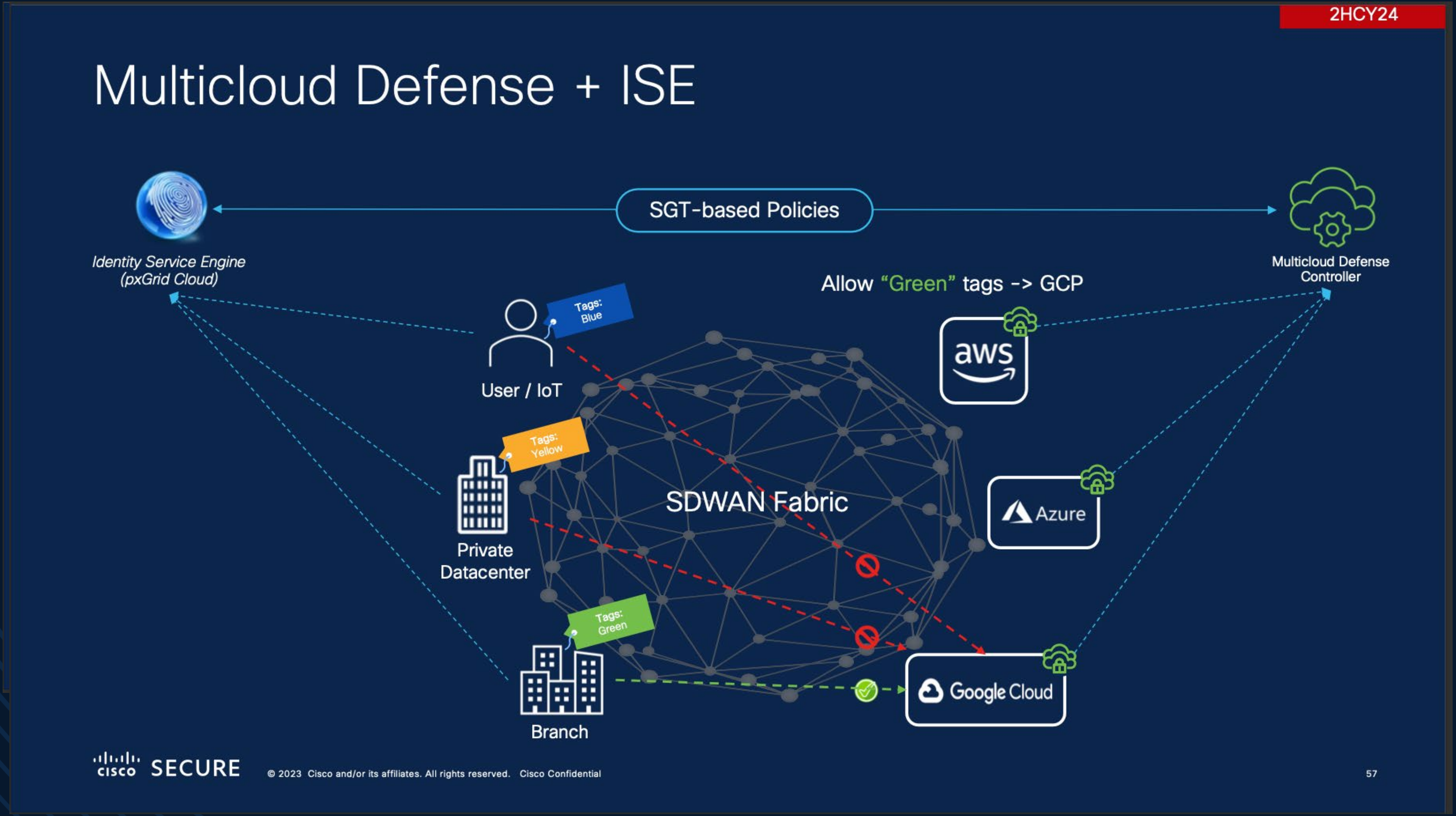
Details

Action	Allow Log
Reset on Deny	□

Profiles

Network Intrusion	Select IPS
Anti-malware	Select Anti Malware
Data Loss Prevention	Select Dlp
FQDN Filtering	Select FQDN filter
Malicious IP	Select Malicious IP
PCAP	□

Classifying Cloud Workflow



2HCY24

Multicloud Defense + ISE

SGT-based Policies

Identity Service Engine (pxGrid Cloud)

Multicloud Defense Controller

Allow “Green” tags -> GCP

User / IoT

Tags: Blue

Private Datacenter

Tags: Yellow

Branch

Tags: Green

SDWAN Fabric

aws

Azure

Google Cloud

SECURE

Segmentation in Multi-Cloud Defense

teradata.

> "Cisco enables us to do in minutes what previously took hours."

Dr. Stacy Lanier, Director of Cloud Engineering Teradata

35%

reduction in infrastructure cost through optimization

Minutes vs Hours

to deploy security across 100s of cloud sites

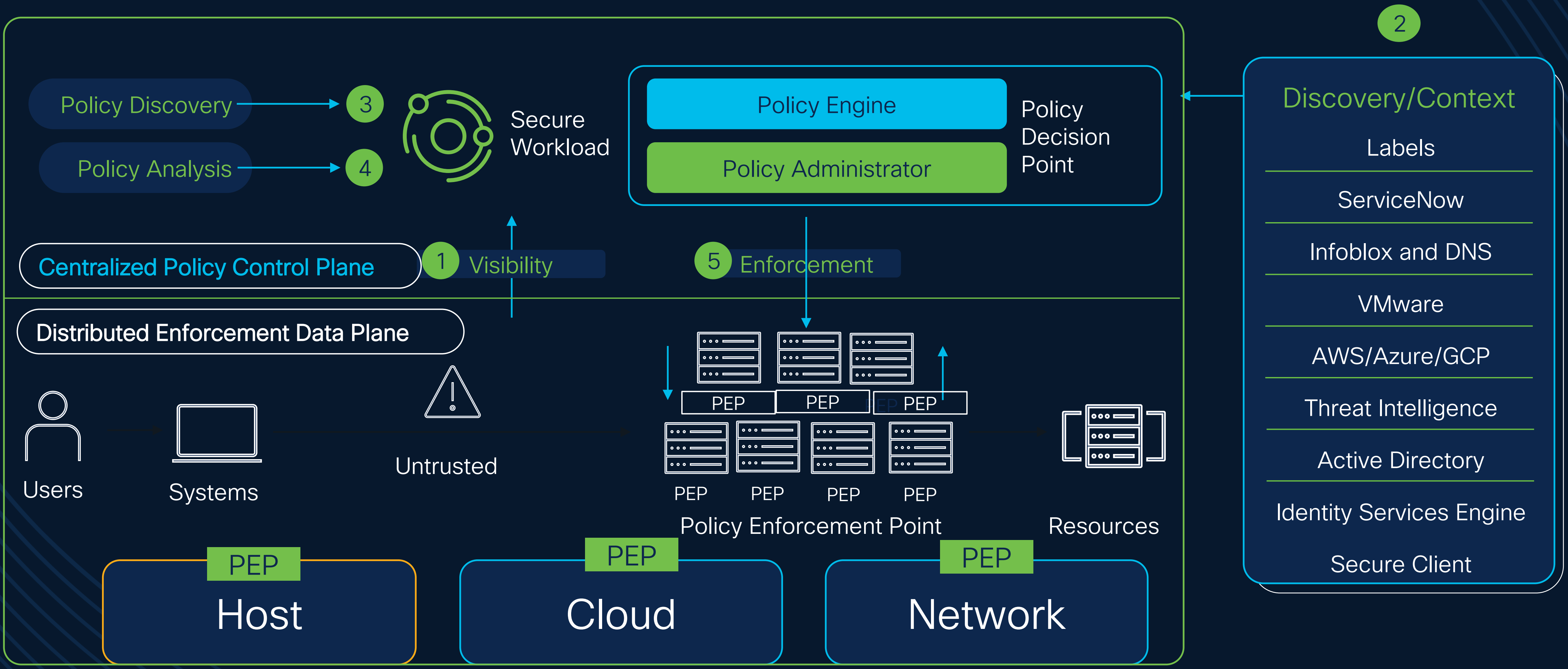
50%

reduction in gateway provisioning and upgrade time per site versus previous state

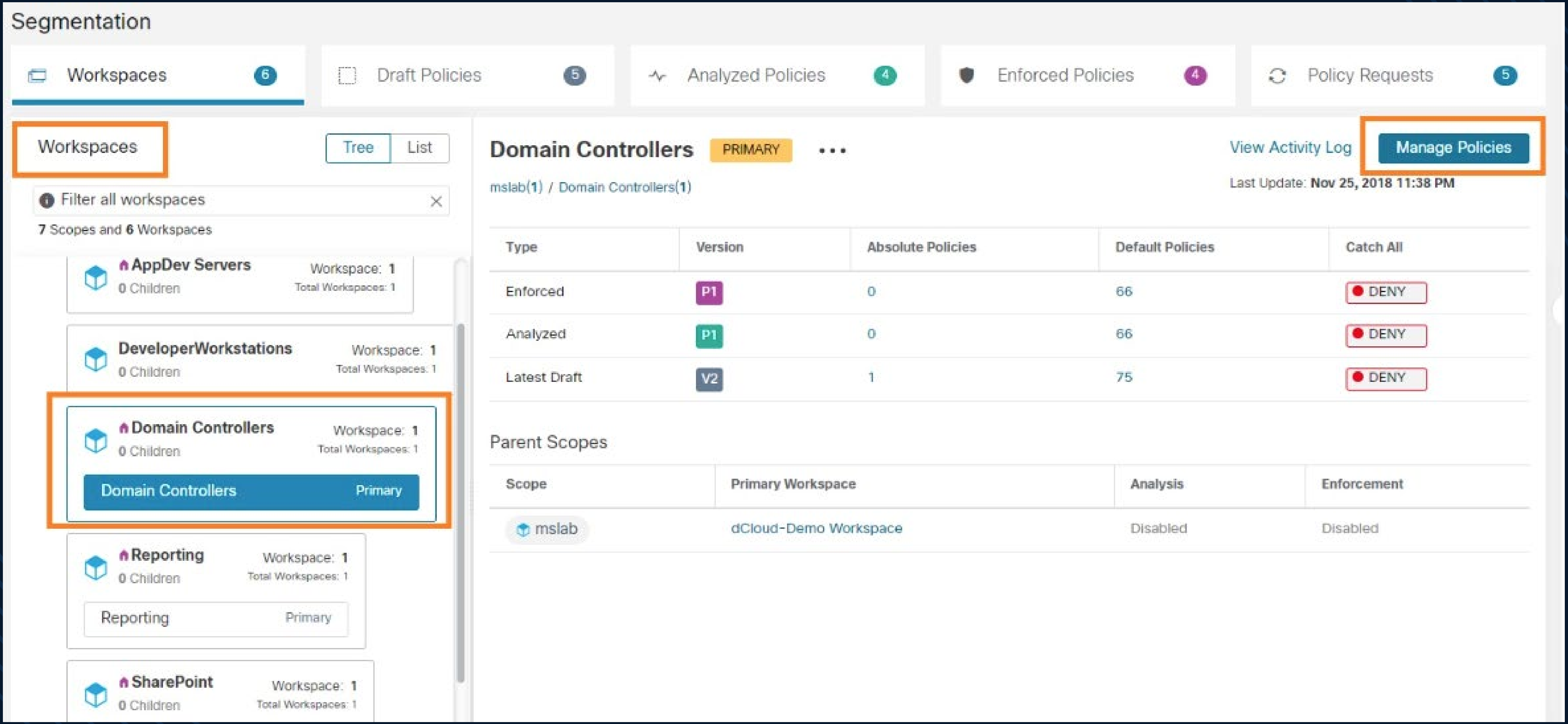
Agenda

Cisco Secure Workload

Secure Workload – Zero Trust Segmentation



Application Discovery Mechanism



Segmentation

Workspaces 6 | Draft Policies 5 | Analyzed Policies 4 | Enforced Policies 4 | Policy Requests 5

Workspaces

Tree | List

Filter all workspaces

7 Scopes and 6 Workspaces

Workspace	Children	Workspace	Total Workspaces
AppDev Servers	0 Children	Workspace: 1	Total Workspaces: 1
DeveloperWorkstations	0 Children	Workspace: 1	Total Workspaces: 1
Domain Controllers Domain Controllers Primary	0 Children	Workspace: 1	Total Workspaces: 1
Reporting Reporting Primary	0 Children	Workspace: 1	Total Workspaces: 1
SharePoint	0 Children	Workspace: 1	Total Workspaces: 1

Domain Controllers PRIMARY

View Activity Log | Manage Policies

mslab(1) / Domain Controllers(1)

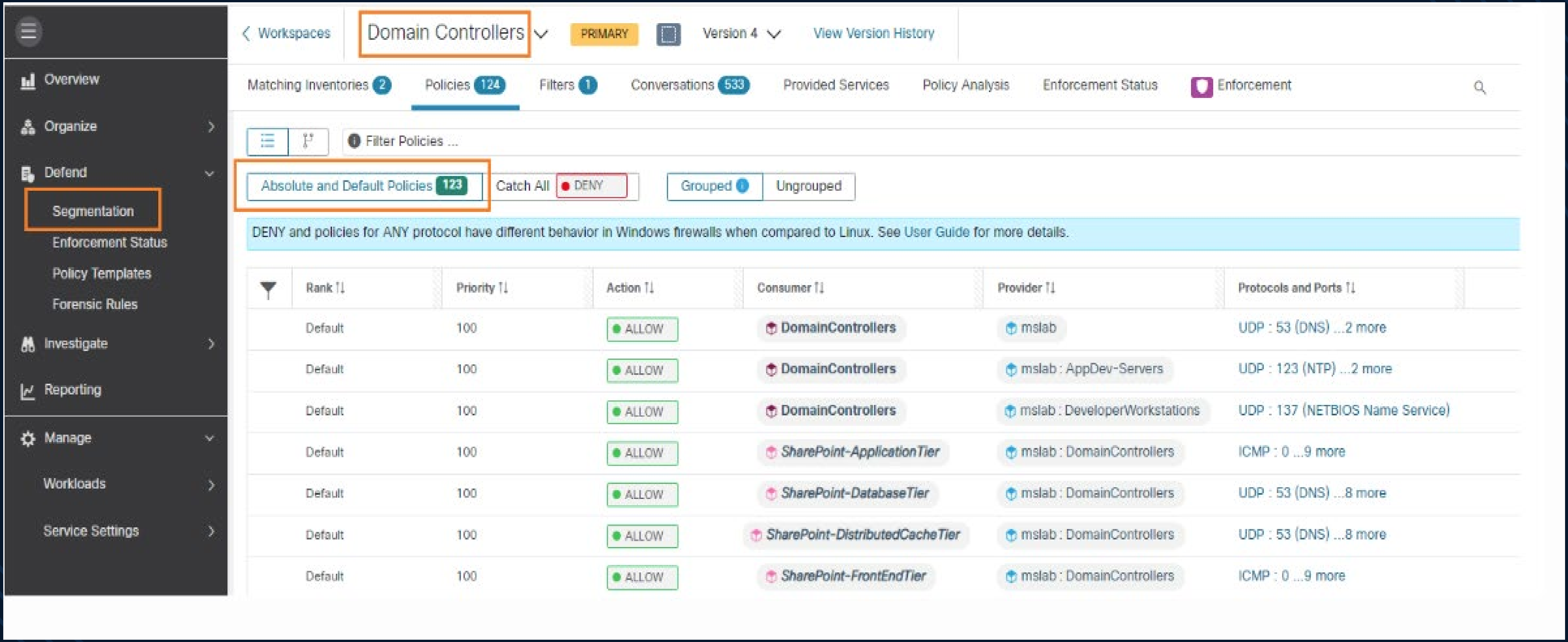
Last Update: Nov 25, 2018 11:38 PM

Type	Version	Absolute Policies	Default Policies	Catch All
Enforced	P1	0	66	● DENY
Analyzed	P1	0	66	● DENY
Latest Draft	V2	1	75	● DENY

Parent Scopes

Scope	Primary Workspace	Analysis	Enforcement
mslab	dCloud-Demo Workspace	Disabled	Disabled

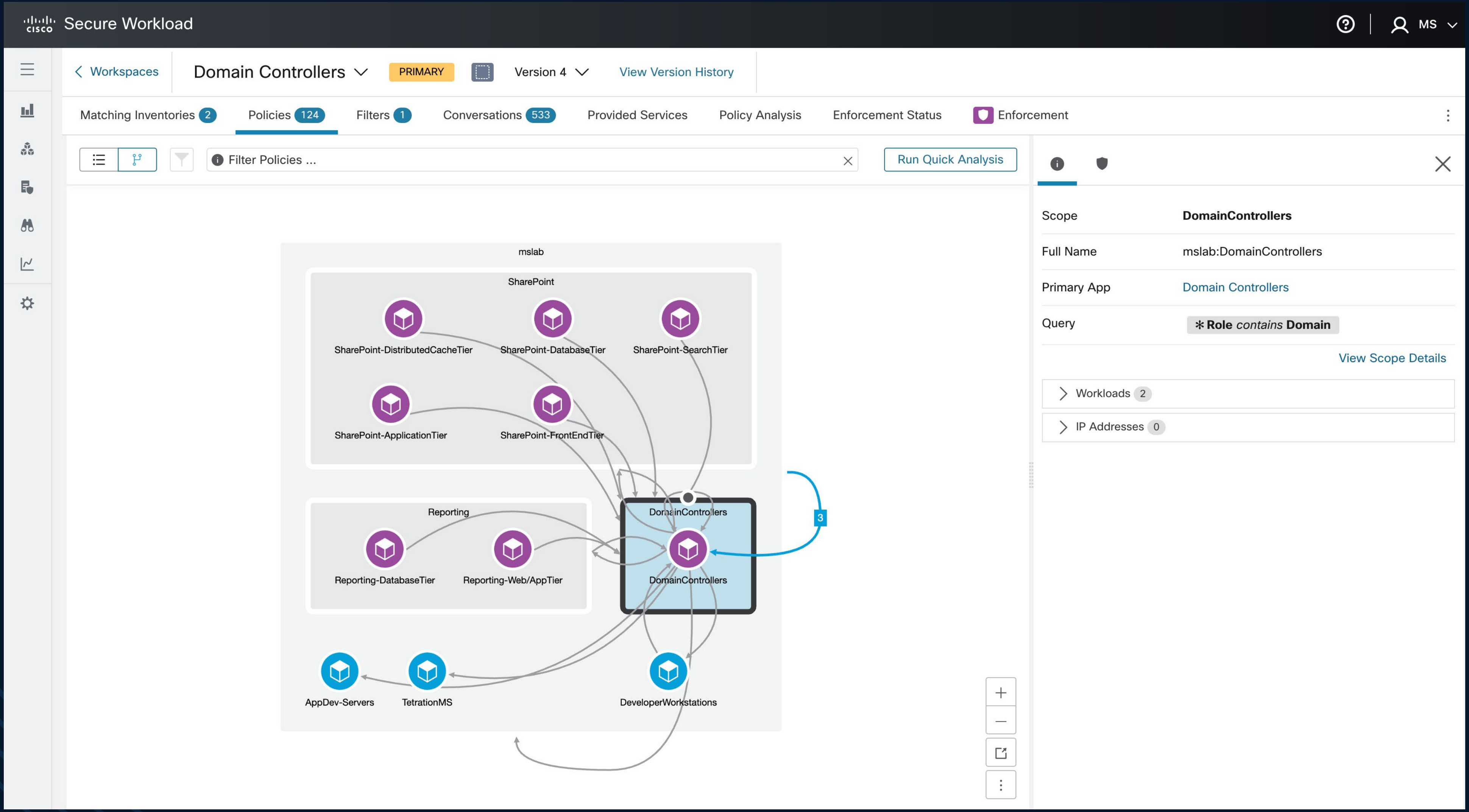
Application Micro Segmentation



DENY and policies for ANY protocol have different behavior in Windows firewalls when compared to Linux. See User Guide for more details.

Rank	Priority	Action	Consumer	Provider	Protocols and Ports
Default	100	ALLOW	DomainControllers	mslab	UDP : 53 (DNS) ...2 more
Default	100	ALLOW	DomainControllers	mslab : AppDev-Servers	UDP : 123 (NTP) ...2 more
Default	100	ALLOW	DomainControllers	mslab : DeveloperWorkstations	UDP : 137 (NETBIOS Name Service)
Default	100	ALLOW	SharePoint-ApplicationTier	mslab : DomainControllers	ICMP : 0 ...9 more
Default	100	ALLOW	SharePoint-DatabaseTier	mslab : DomainControllers	UDP : 53 (DNS) ...8 more
Default	100	ALLOW	SharePoint-DistributedCacheTier	mslab : DomainControllers	UDP : 53 (DNS) ...8 more
Default	100	ALLOW	SharePoint-FrontEndTier	mslab : DomainControllers	ICMP : 0 ...9 more

Application Discovery Mechanism



Scope: **DomainControllers**

Full Name: mslab:DomainControllers

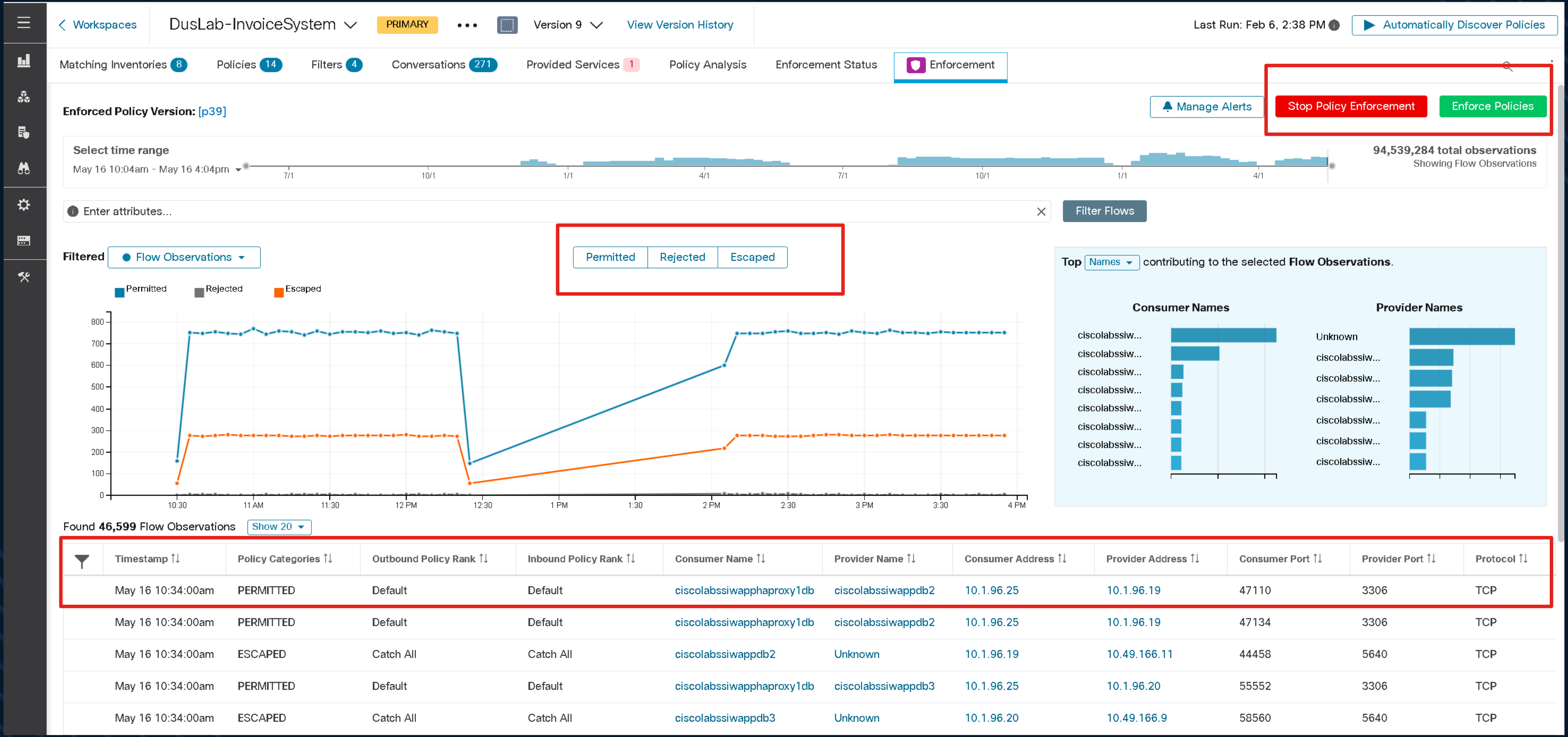
Primary App: Domain Controllers

Query: ✻ **Role** *contains* **Domain**

Application Micro Segmentation

One click away from testing and enforcement with Cisco Secure Workload

Policy ready to be enforced



Enforced Policy Version: [p39]

May 16 10:04am - May 16 4:04pm

94,539,284 total observations
Showing Flow Observations

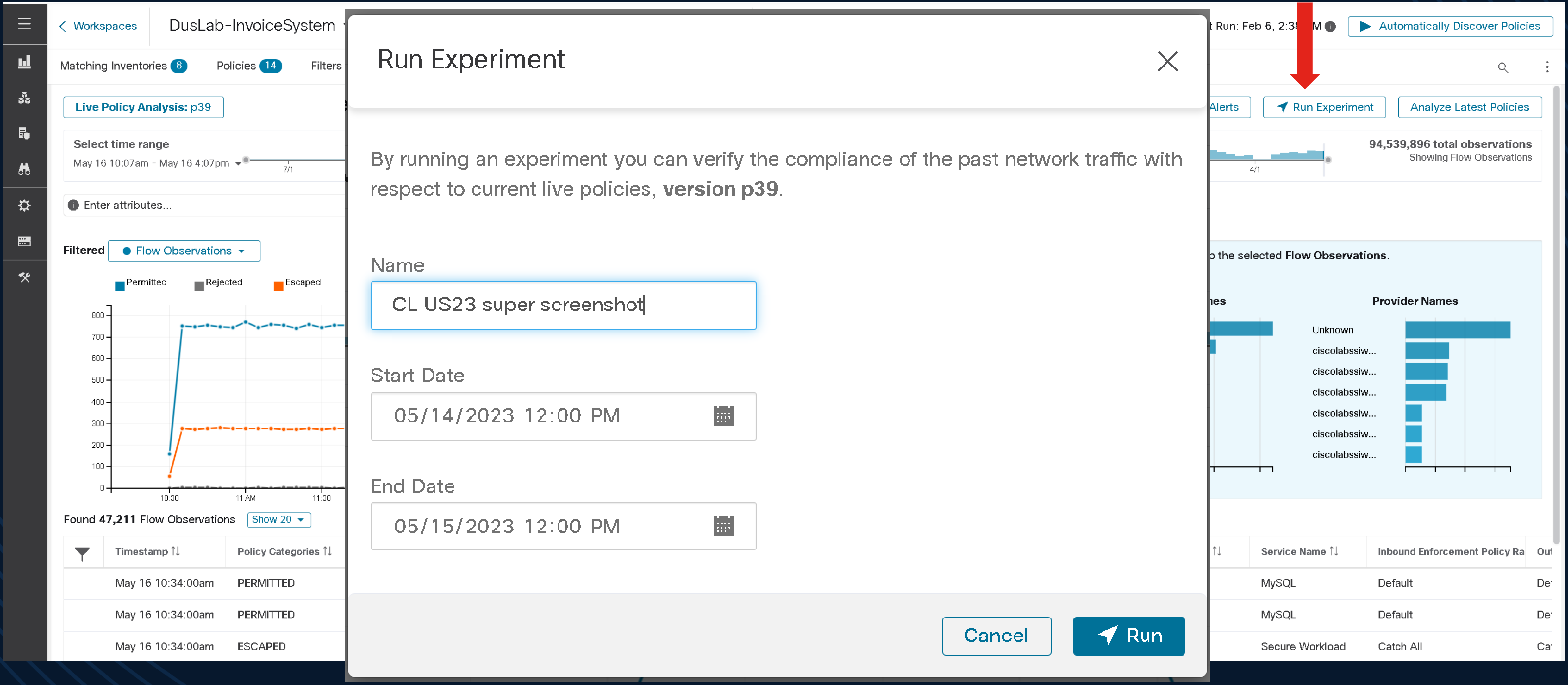
Enter attributes...

Top Names contributing to the selected **Flow Observations**.

Found **46,599** Flow Observations

Timestamp	Policy Categories	Outbound Policy Rank	Inbound Policy Rank	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol
May 16 10:34:00am	PERMITTED	Default	Default	ciscolabssiwapphaproxy1db	ciscolabssiwappdb2	10.1.96.25	10.1.96.19	47110	3306	TCP
May 16 10:34:00am	PERMITTED	Default	Default	ciscolabssiwapphaproxy1db	ciscolabssiwappdb2	10.1.96.25	10.1.96.19	47134	3306	TCP
May 16 10:34:00am	ESCAPED	Catch All	Catch All	ciscolabssiwappdb2	Unknown	10.1.96.19	10.49.166.11	44458	5640	TCP
May 16 10:34:00am	PERMITTED	Default	Default	ciscolabssiwapphaproxy1db	ciscolabssiwappdb3	10.1.96.25	10.1.96.20	55552	3306	TCP
May 16 10:34:00am	ESCAPED	Catch All	Catch All	ciscolabssiwappdb3	Unknown	10.1.96.20	10.49.166.9	58560	5640	TCP

Run Policy Experiment



Run Experiment

By running an experiment you can verify the compliance of the past network traffic with respect to current live policies, **version p39**.

Name: CL US23 super screenshot

Start Date: 05/14/2023 12:00 PM

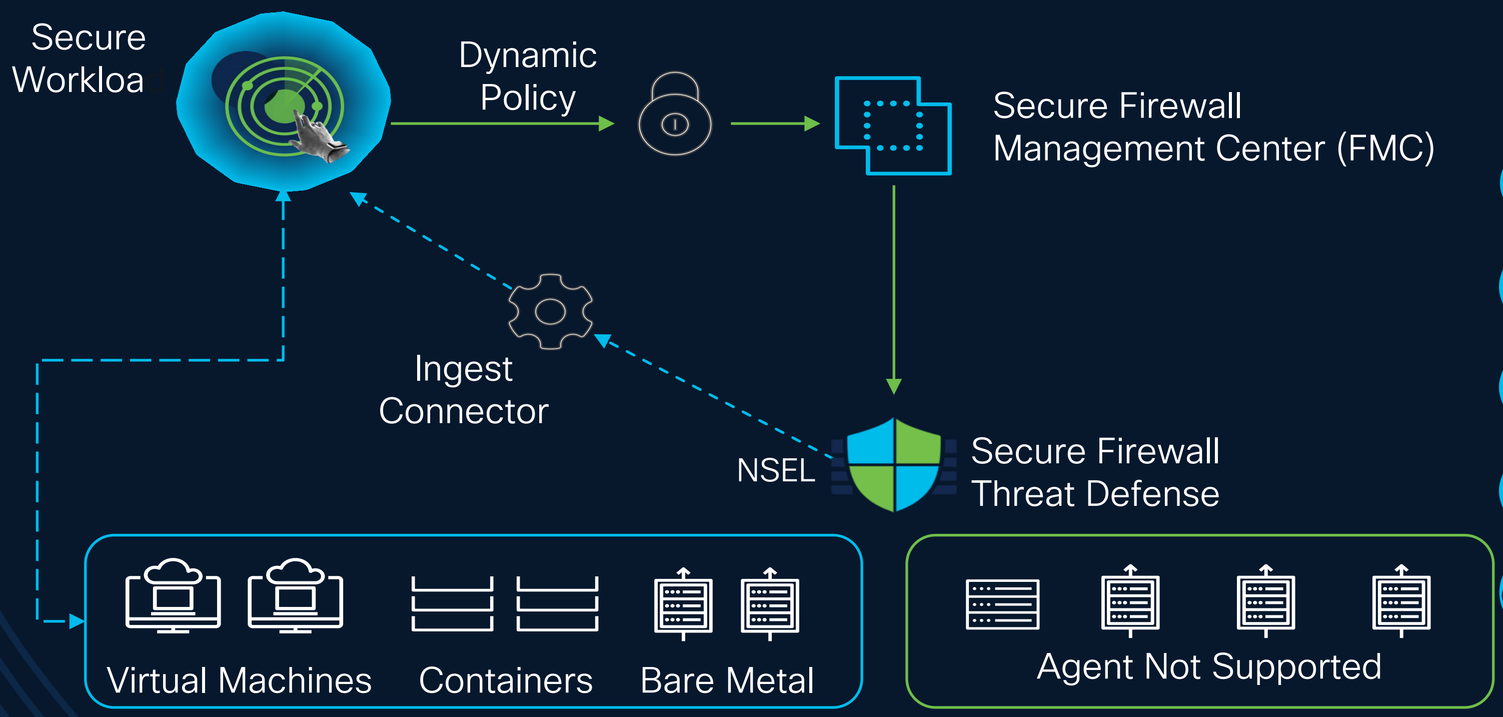
End Date: 05/15/2023 12:00 PM

Cancel | Run

Found 47,211 Flow Observations   Show 20

Timestamp	Policy Categories	Service Name	Inbound Enforcement Policy Ra	Out
May 16 10:34:00am	PERMITTED	MySQL	Default	De
May 16 10:34:00am	PERMITTED	MySQL	Default	De
May 16 10:34:00am	ESCAPED	Secure Workload	Catch All	Ca

Cisco Secure Workload Integration with FMC

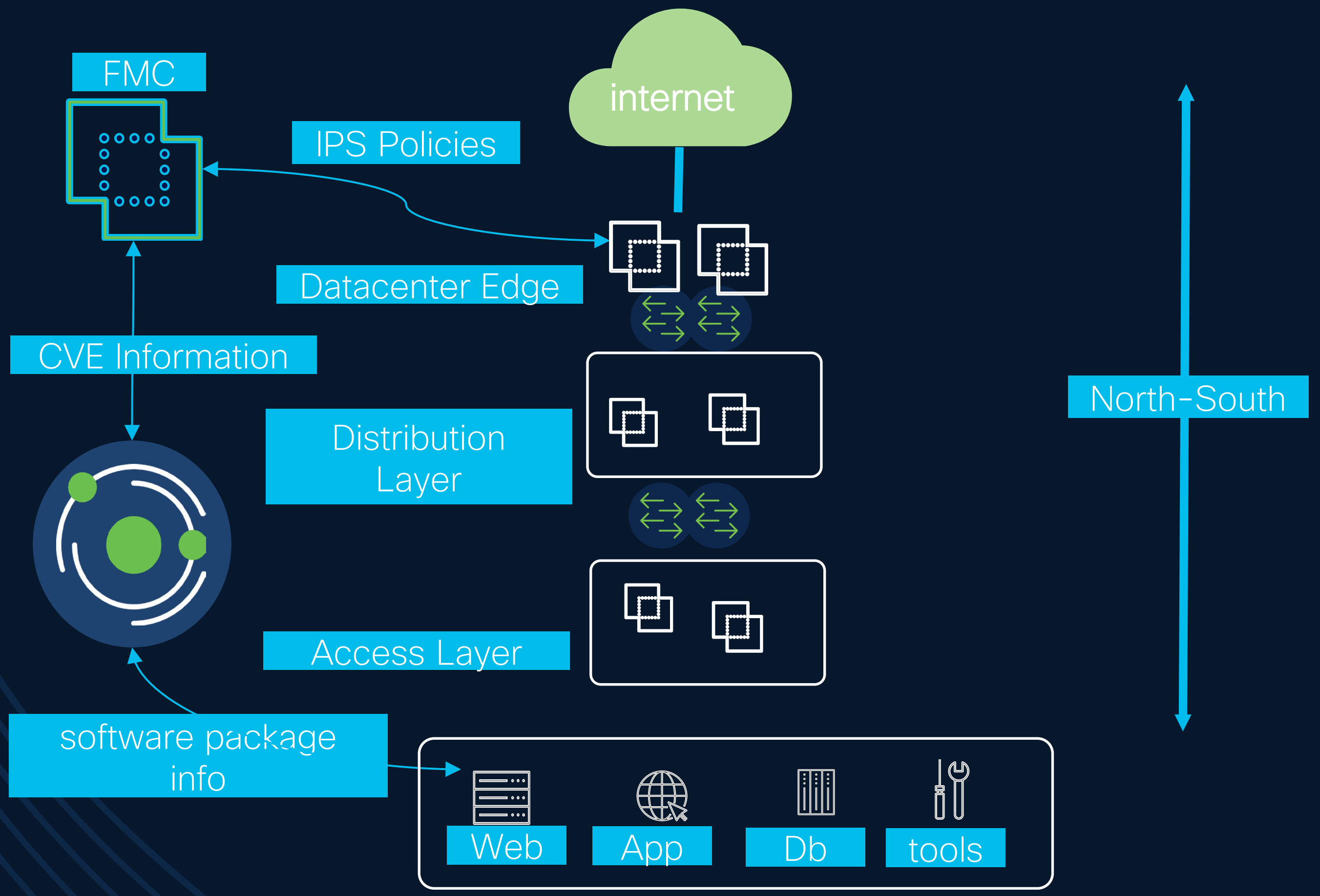


Segmentation policies enforcement
at workloads (agent-based deployment)

Segmentation policies enforcement
at firewall (agentless deployment

- Defense in depth
- Support access control policy and dynamic object
- Improved rule ordering
- FMC domain awareness
- Topology aware policy enforcement
- Support deployment across multicloud

Virtual patching - Cisco Secure Firewall



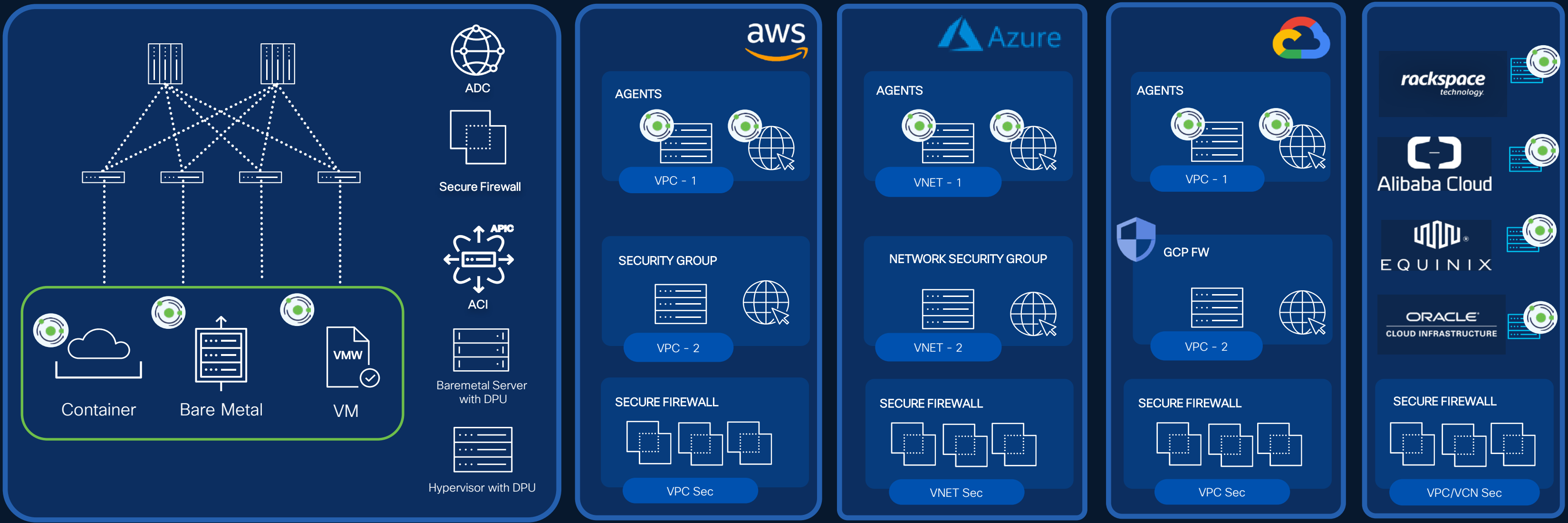
- Secure Workload agents collects CVE data from workloads
- Publish specific CVE data to Firepower Management Center
- Use Firepower recommendations to generate precise IPS policy
- Apply precise IPS policy to protect against CVE exploits

Big Picture

Agent

- Anywhere
- Windows Desktop
- Windows Server
- IBM AIX
- Oracle Solaris
- Oracle Linux
- Centos, Rocky, Alma Linux
- Ubuntu, Debian
- SUSE Linux
- RedHat Linux
- Amazon Linux
- OpenShift
- Kubernetes

Consistent microsegmentation from on-premises to the cloud



On Premise | Public Cloud

Bare Metal Servers | Virtual Machines | Containers

Agentless

- On-Prem
- Loadbalancer (ADC)
- Firewalls
- Data Center Fabric (SDN)
- NVIDIA Smart NIC (DPU)
- AWS, GCP, Azure
- Security Group
- Network Security Group
- Cloud Network Firewall
- Multicloud Defense*
- NVIDIA Smart NIC (DPU)

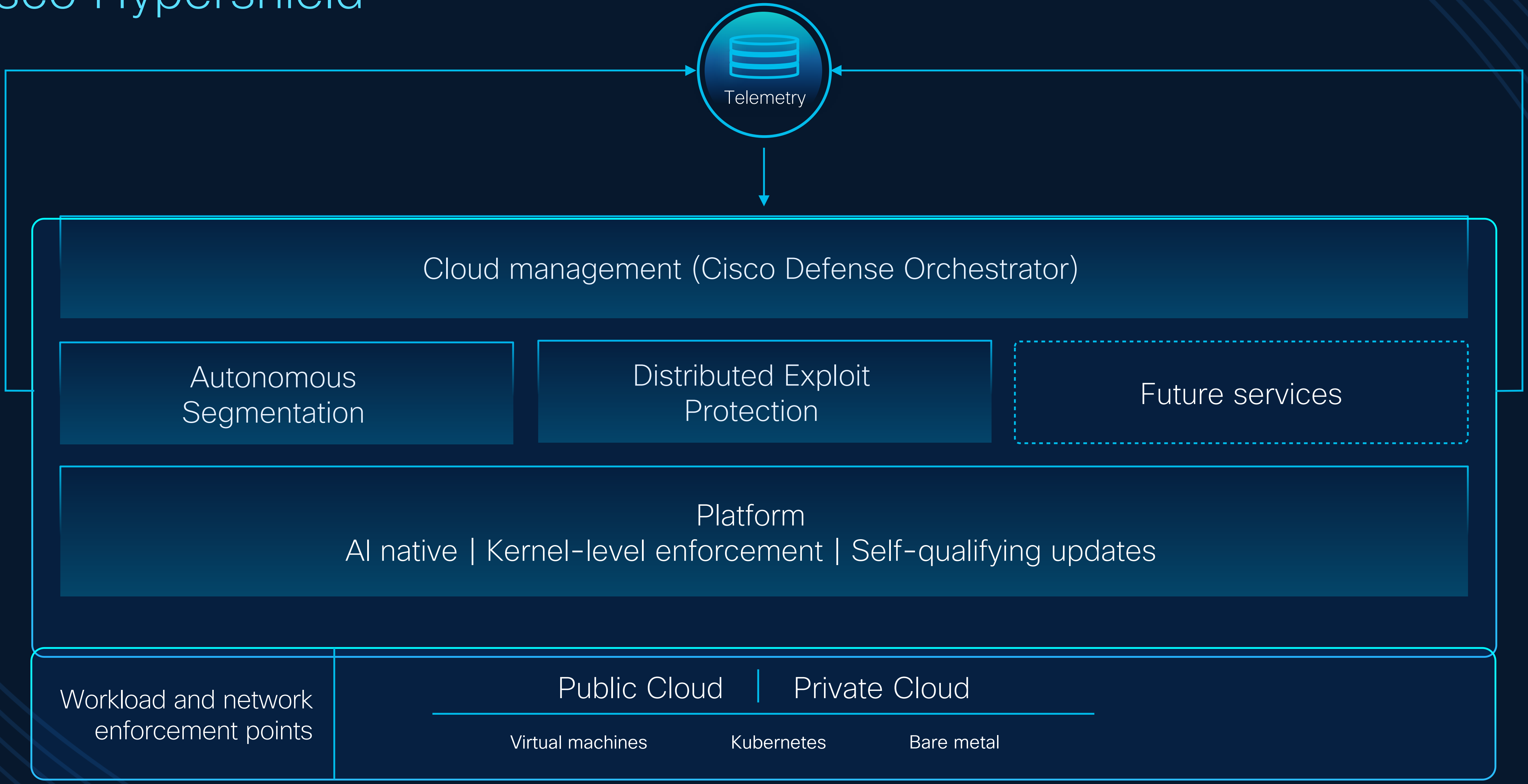
User Identity | Tags and Labels | Vulnerability

Threat Feed | Application Encryption | Domain/FQDN | Cisco Security Risk Score

Agenda

Cisco Hyper Shield

Cisco Hypershield



Telemetry

Cloud management (Cisco Defense Orchestrator)

Autonomous Segmentation

Distributed Exploit Protection

Future services

Platform
AI native | Kernel-level enforcement | Self-qualifying updates

Workload and network enforcement points

Public Cloud | Private Cloud

Virtual machines

Kubernetes

Bare metal

Core Technologies

eBPF

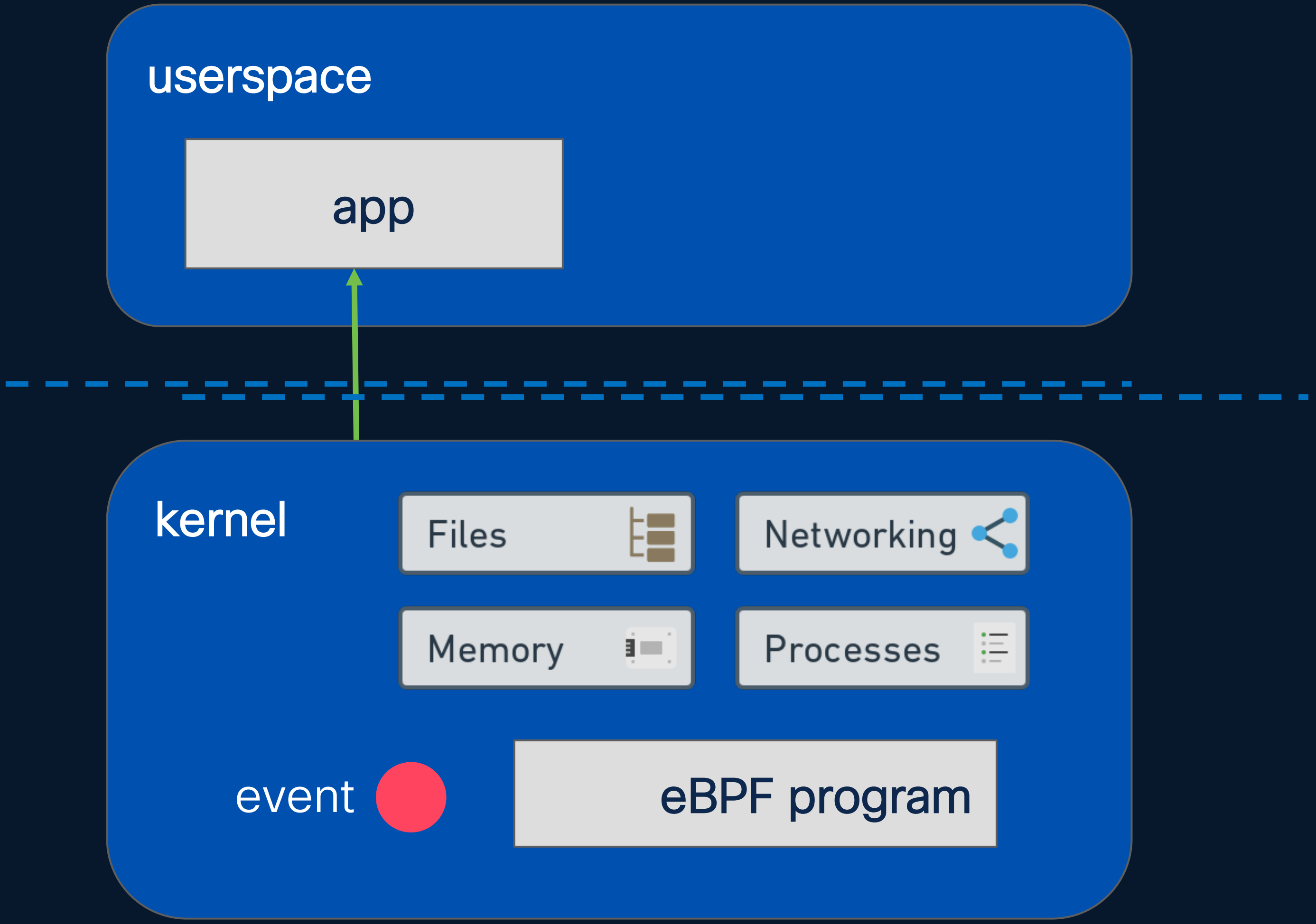
AI

Self-qualifying Updates

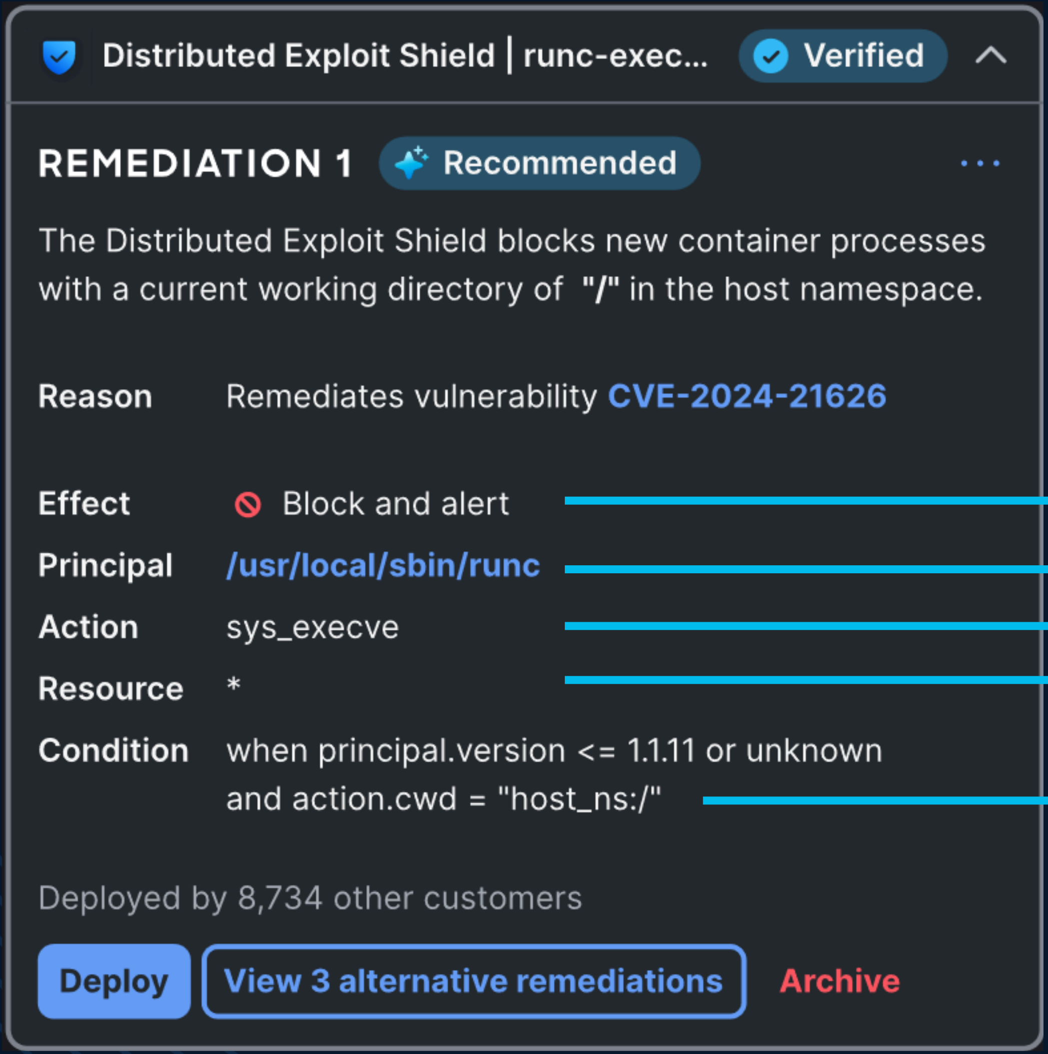
eBPF – extended Berkely Packet Filter

- Makes the Linux kernel programmable in a secure and efficient way

eBPF is to the kernel what Javascript is to the browser.



AI-Based Policy Engine – Building Trust



Distributed Exploit Shield | runc-exec... ✓ Verified

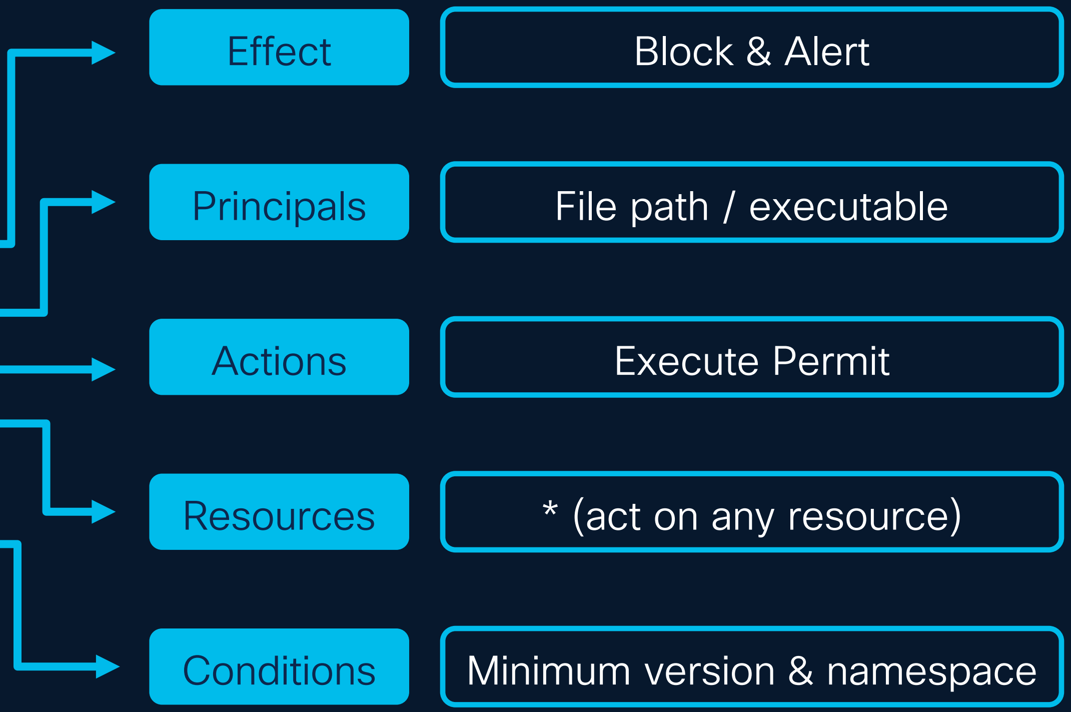
REMEDIATION 1 Recommended

The Distributed Exploit Shield blocks new container processes with a current working directory of **"/"** in the host namespace.

Reason	Remediates vulnerability **CVE-2024-21626**
Effect	🚫 Block and alert
Principal	**/usr/local/sbin/runc**
Action	sys_execve
Resource	*
Condition	when principal.version <= 1.1.11 or unknown and action.cwd = "host_ns:/"

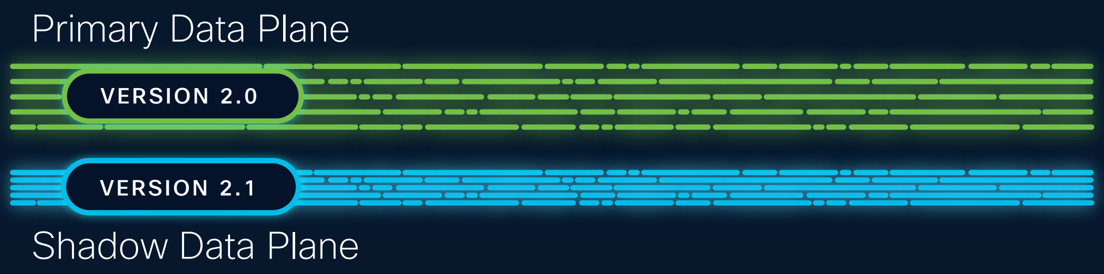
Deployed by 8,734 other customers

AI generated rule blocking a vulnerable container process



Effect	Block & Alert
Principals	File path / executable
Actions	Execute Permit
Resources	* (act on any resource)
Conditions	Minimum version & namespace

Dual Dataplane: Earning Your Trust

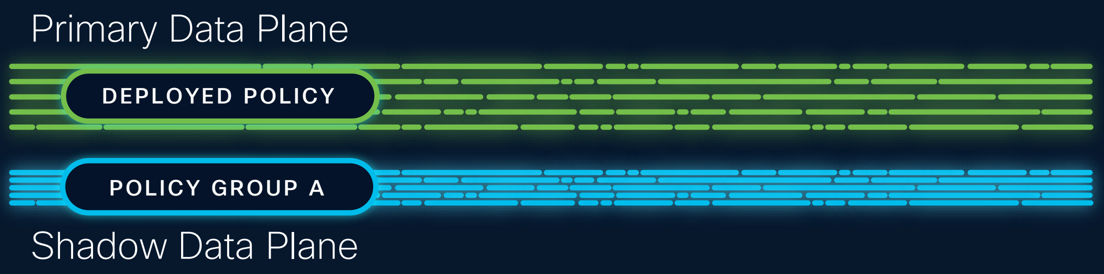


Primary Data Plane

VERSION 2.0

VERSION 2.1

Shadow Data Plane



Primary Data Plane

DEPLOYED POLICY

POLICY GROUP A

Shadow Data Plane

Self Qualifying SW updates

Policy Verification, Exploit Protection Test