
cisco Live!
Let's go

The bridge to possible

Zero Trust

Securing the Evolving Workplace

Manfred Brabec, Principal Architect

cisco Live!

BRKSEC-2053

Agenda

- Cisco Live Housekeeping
- Introduction to Zero Trust
- Evolving Workplace Use Cases
- Securing the Workplace
- Summary

Abstract

- Cisco Zero Trust enables users to securely connect to your network from any device, anywhere while restricting access from non-compliant devices.
- Zero Trust – Securing the evolving workplace is focused on the workplace in offices/campuses. This session is focused on complimenting ZTNA with network zero trust.
- Our automated network-segmentation capabilities let you set micro-perimeters for users, devices, IoT and application traffic without requiring network redesign. Cisco Zero Trust for workplace will speak about how to accomplish:
  - Secure network access for network privacy and mitigating network attack
  - Network segmentation for controlled and uncontrolled endpoints
  - Dynamic visibility
  - Automated threat containment
  - Continuous Monitoring and Trust Analysis
- Cisco Zero Trust for the Workplace is a foundational pillar to enable any user and any device to access any application.

Objectives:
Understand Zero Trust Principles and their application to evolving workplace networks.

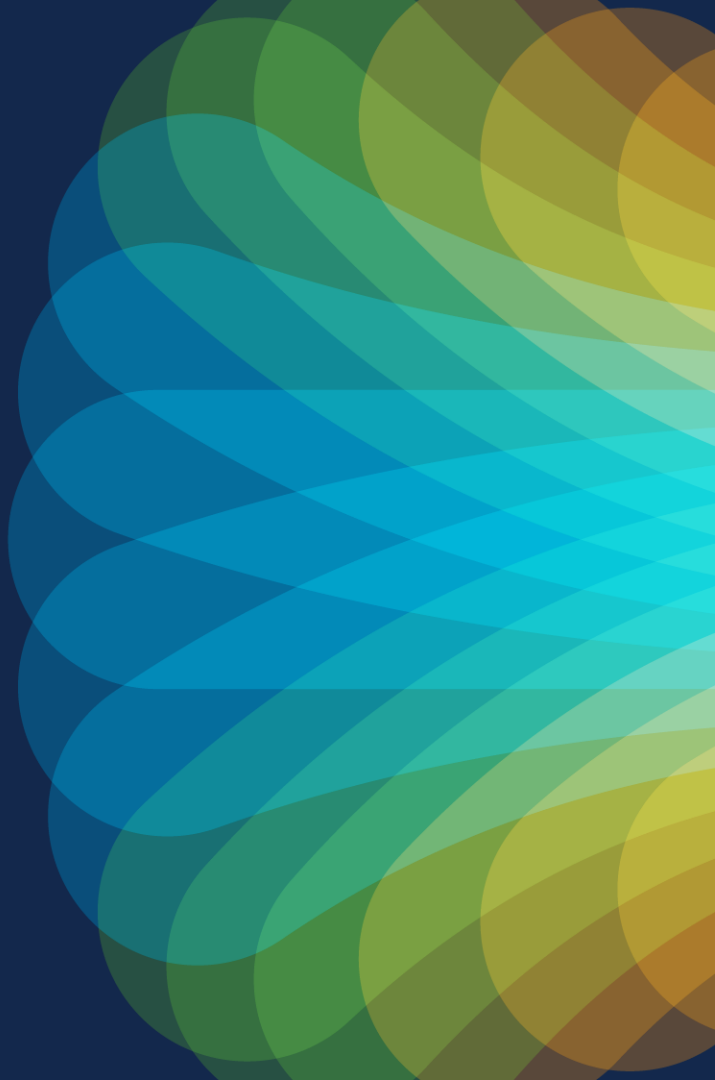
About Me

Manfred Brabec

- Principal Architect, acting as CTO for GSSO EMEA
- Focused on Security Architecture and Design
- BU Interlock to enhance our solutions
- 11+ years at Cisco
- 25+ years of Security & Network experience
- Outside work: family, nature, sports, home cinema, new technologies

CCIE Security #13180
CCDE #20130028

Introduction to Zero Trust



Zero Trust means different things to different people

It’s segmentation

It’s ZTNA

It’s endpoint security

It’s firewall

It’s identity

What Zero Trust Means to Us

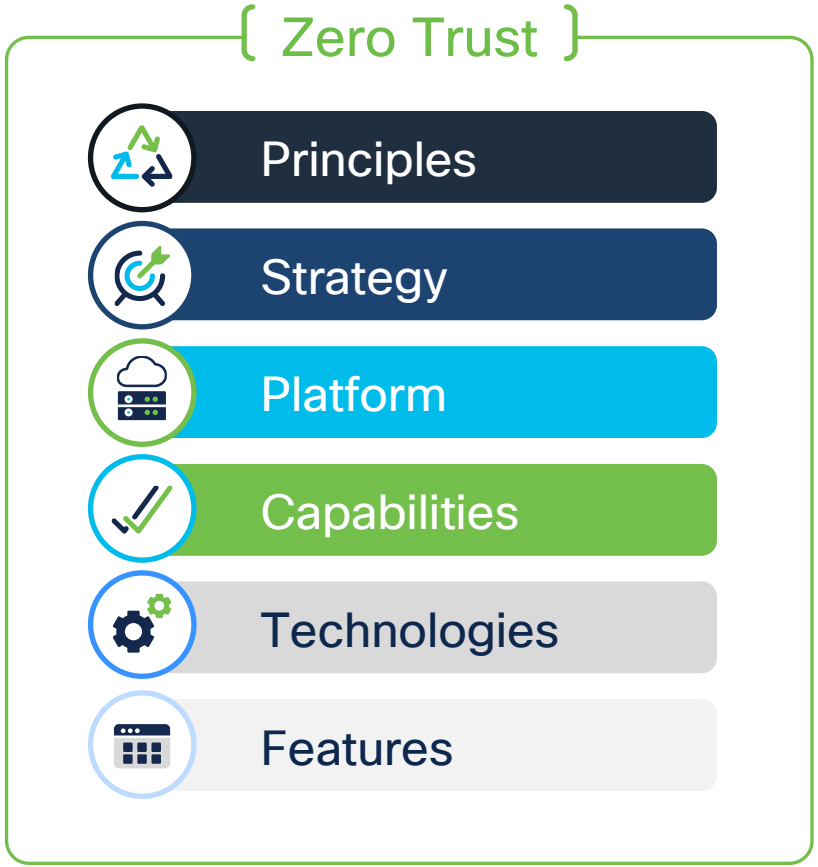
Improving the Nation's Cybersecurity

Executive Order (EO) 14028 - Sec. 10. Definitions

- *"Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment."*
- *"If a device is compromised, zero trust can ensure that the damage is contained."*

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

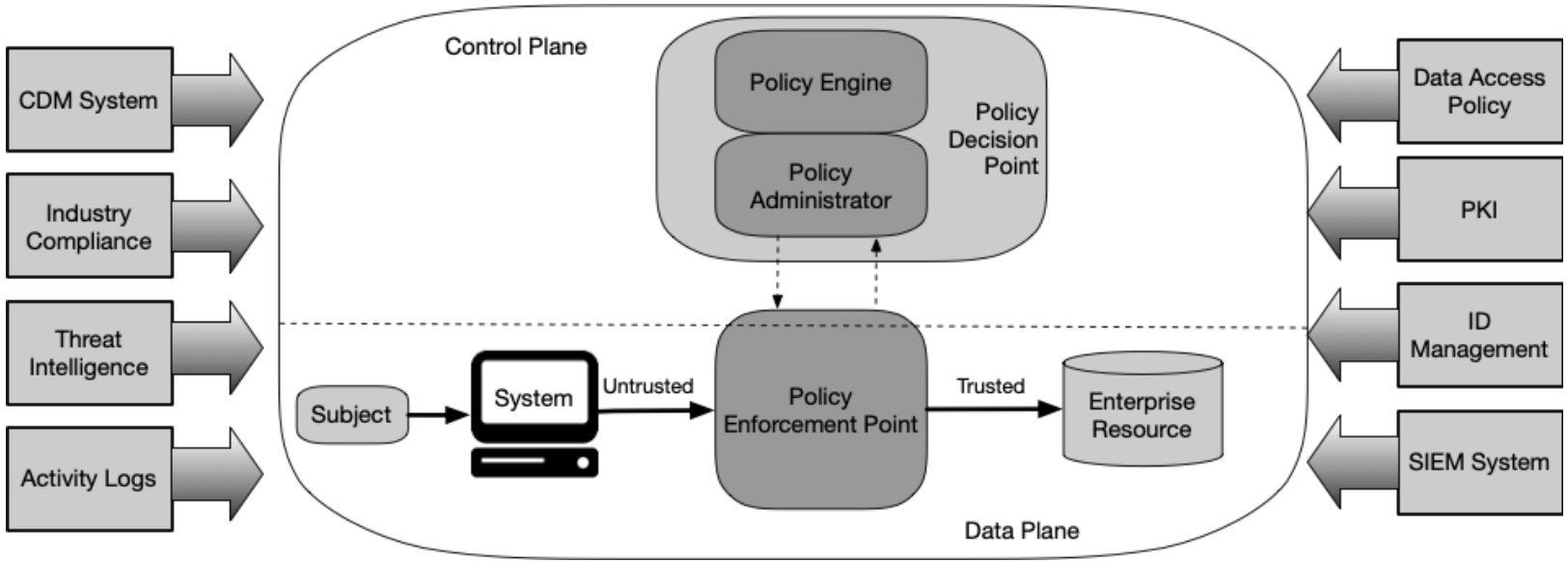
Cisco believes Zero Trust must be defined holistically



NIST Zero Trust Architecture SP 800-207

Core Zero Trust Logical Components

- **ZTA Using Micro-Segmentation:** *"In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) … to act as PEPs protecting each resource or small group of related resources."*



ISA-99/IEC-62443

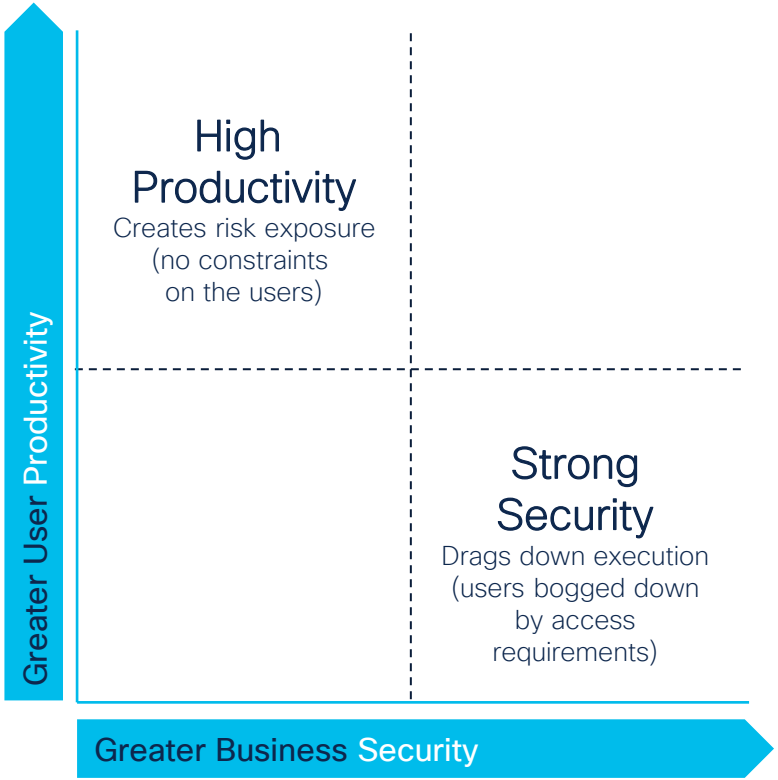
Optimal Segmentation

- After Completing the Detailed Risk Assessment (Cyber-PHA):

"Once the detailed risk assessment has been carried out, there will be an optimal segmentation of zones and conduits, together with an often-extensive list of recommendations and countermeasures. ***Simple segmentation is necessary, but in itself, it is not sufficient.*** *A series of recommendations must accompany the optimal segmentation. Each zone or conduit (node) will have an SL-T-required security level (Security Level Target), and an SL-A current security level (Security Level Achieved)—all without going into much technical detail."*

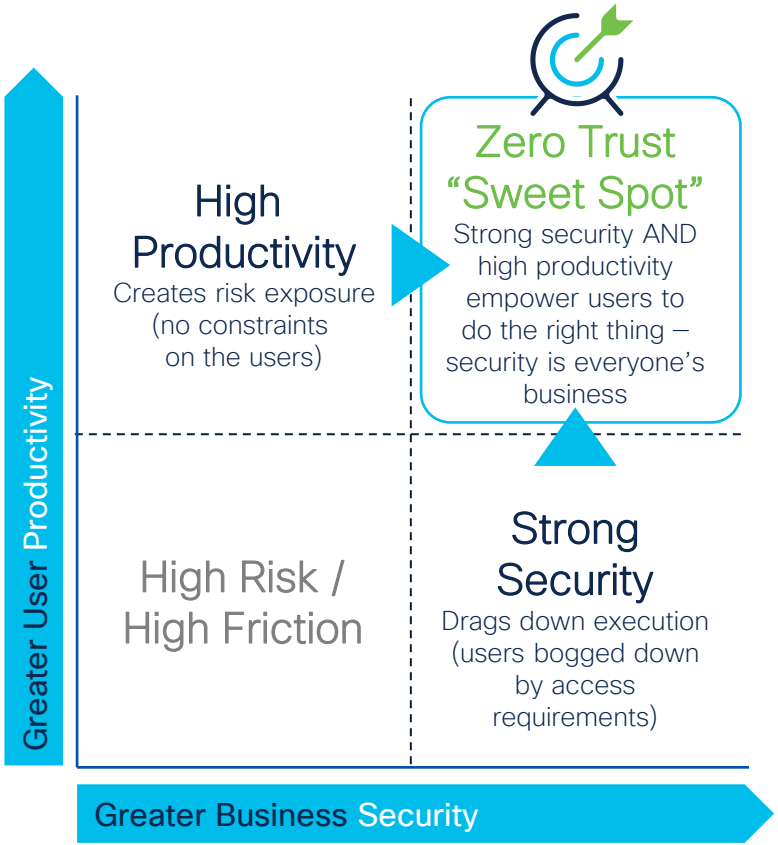
Today's trade-off is holding back Zero Trust

Security vs. productivity



Eliminate the trade-off

Frustrate attackers, not users



What it takes to get Zero Trust right

Zero Trust requirements

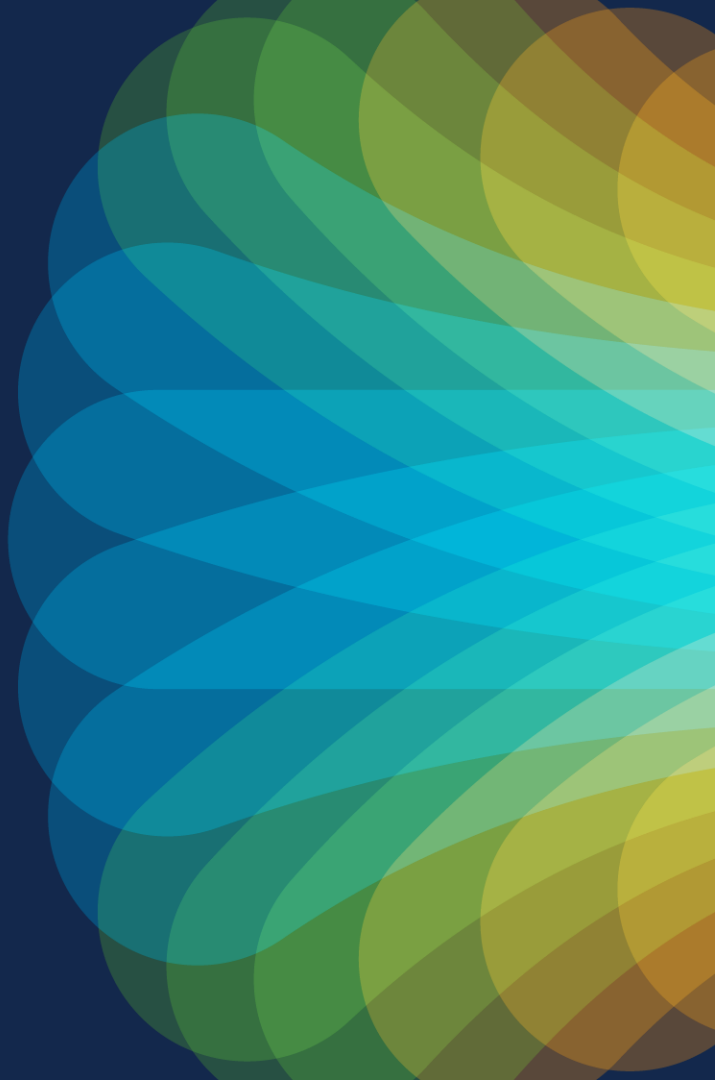
Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Respond to Change in Trust

Evolving Workplace Use Cases

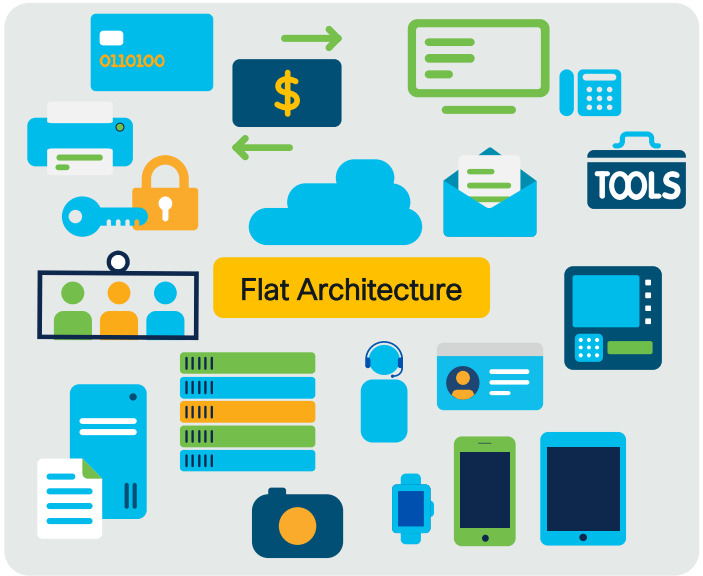


Major Shift in IT Landscape

Users, devices and apps are everywhere

Transition from Flat Network to Zero Trust Segmentation

Current State



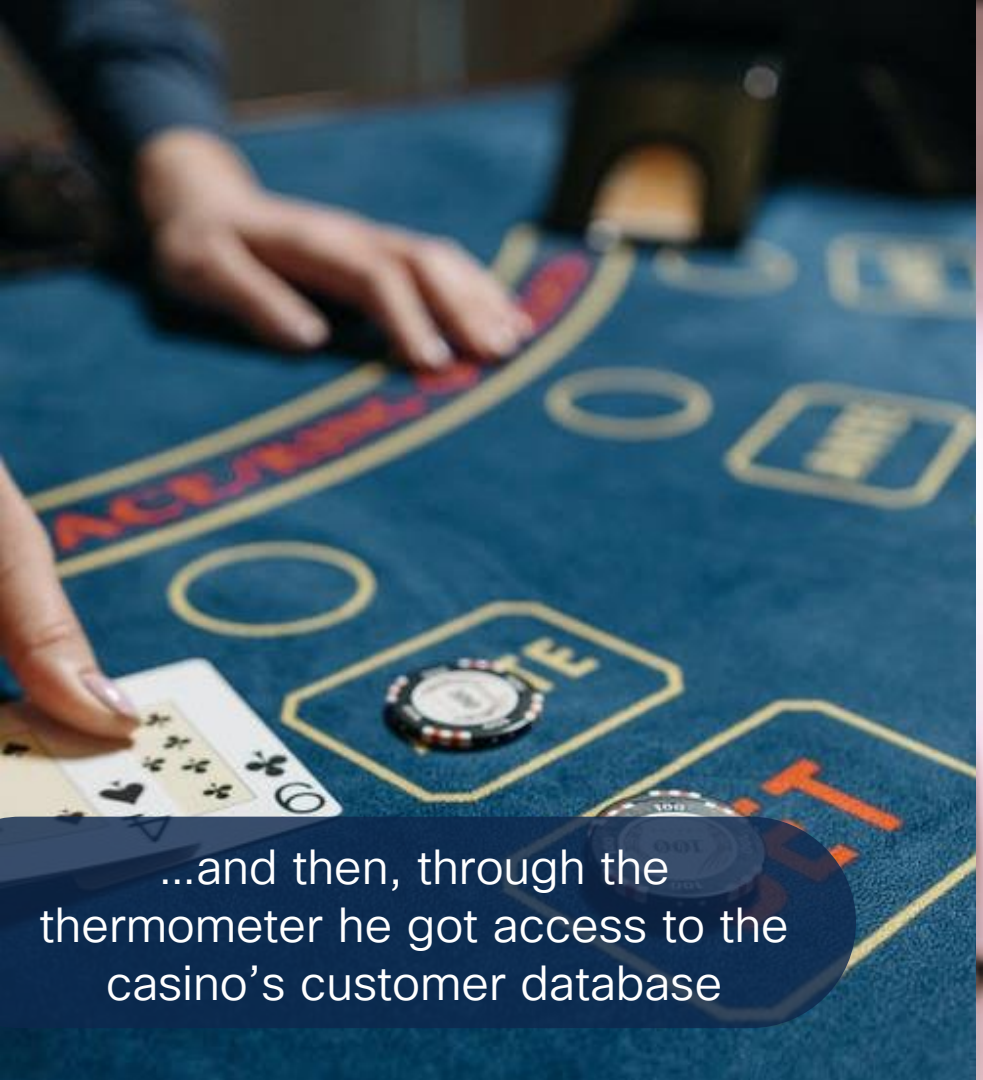
Zero Trust State

As Published by Cisco Press Book: “Zero Trust Architecture”

Let me tell you a story of a breach...

It’s about a Casino

A hacker noticed this networked thermometer



...and then, through the thermometer he got access to the casino's customer database

End of the story

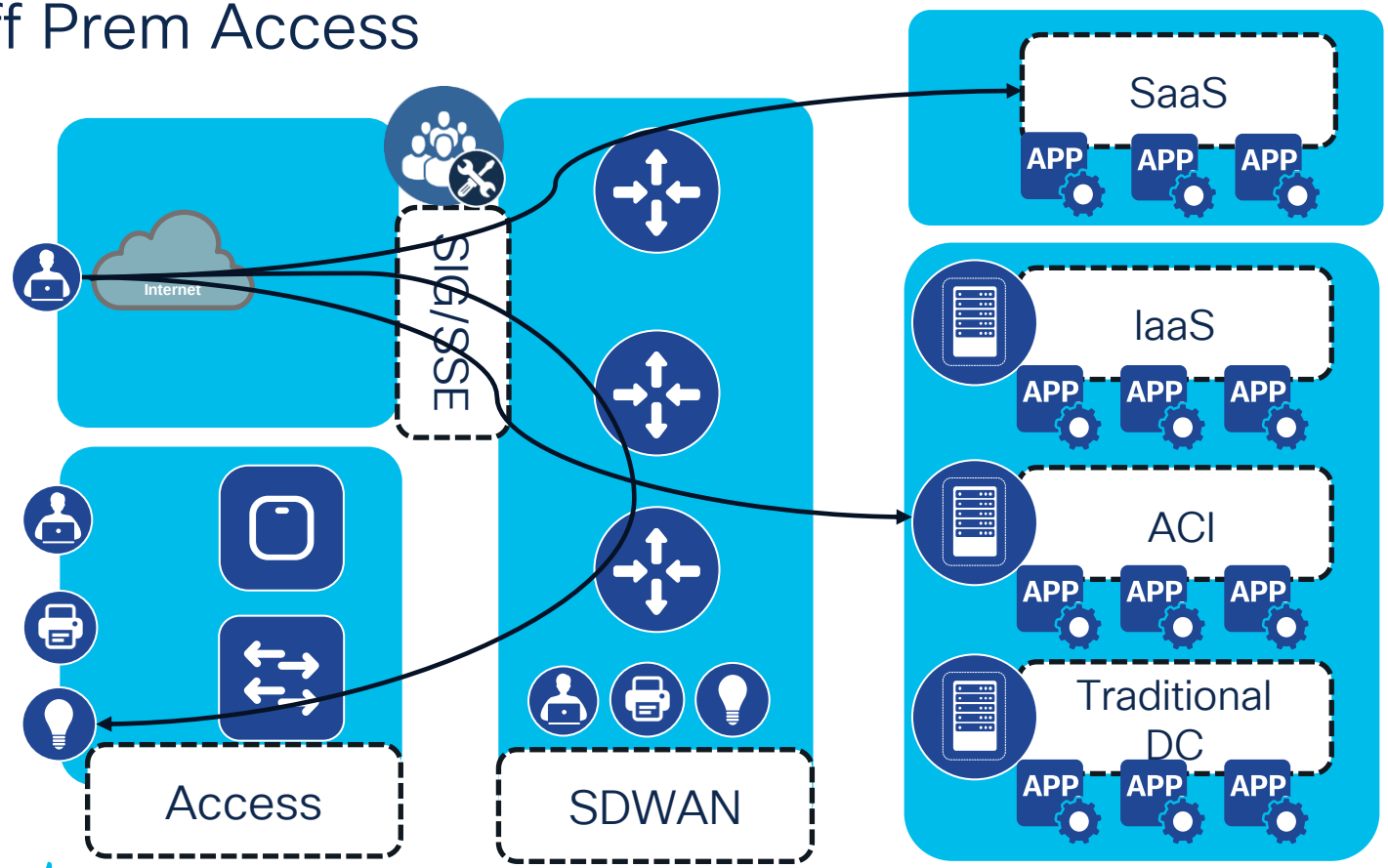
What is said about (ZT) – Making it reality

- Zero Trust Network Access (ZTNA) can remove all network controls
  - Assumes there is only a single use case to be solved. Users on smart devices accessing modern applications.
  - Company breakdown of users on smart devices and application infrastructure may or may not allow this
  - ZTNA can simplify network security
- I want a café like experience for all my users
  - Easier on boarding for devices
  - Seamless Wi-Fi experience.
  - Few have adopted unencrypted totally open networks

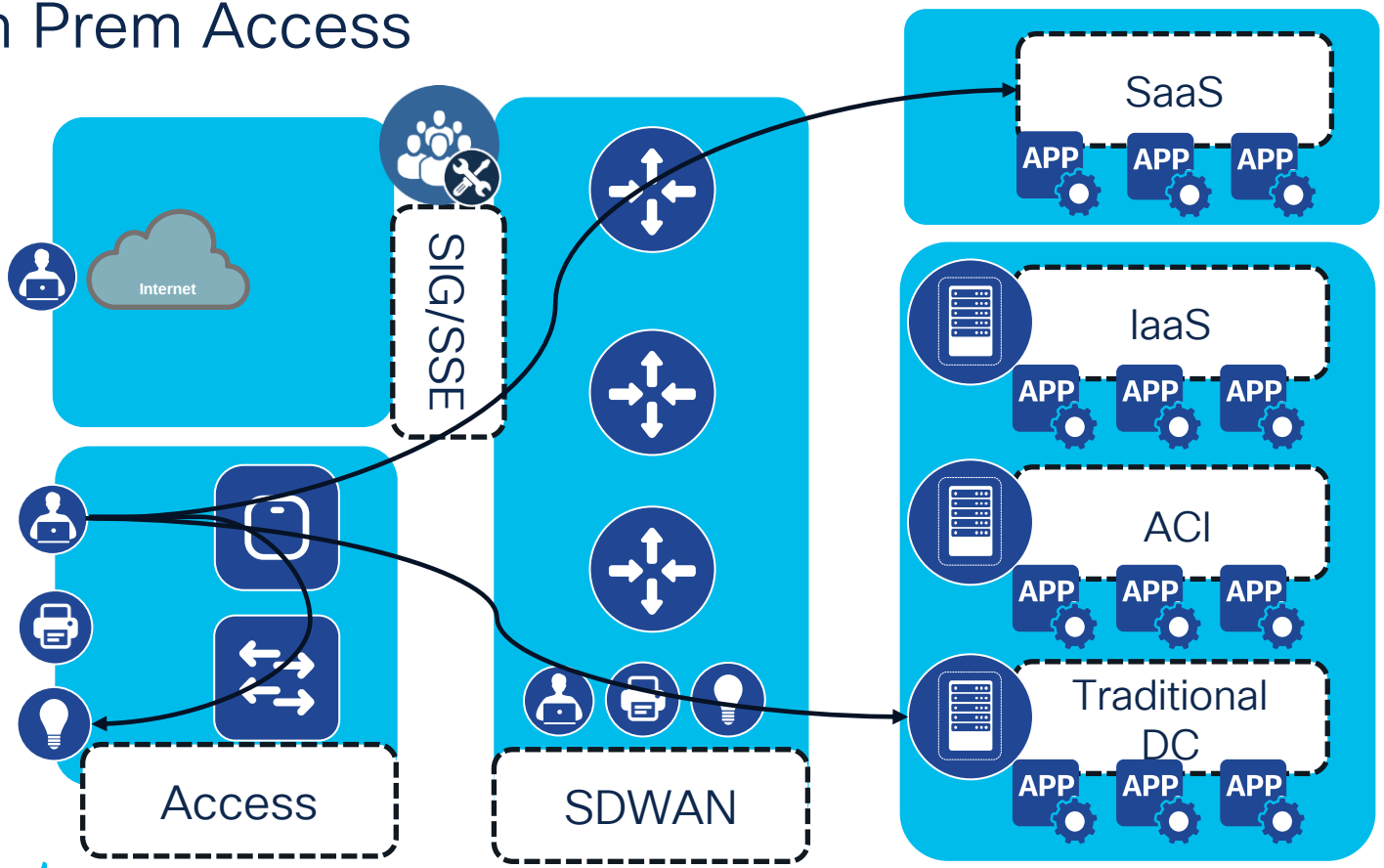
What is said about ZT – Making it reality

- Use the same user/device least privilege on prem as off prem
  - Depends on company and use cases
  - Application performance considerations depending on architecture.
    - Hair-pinning in Cloud
    - Latency sensitive applications
  - User interactions to non ZTNA capable device
- We can get rid of networks
  - Hybrid work may move cost of networking to the employee
  - Smaller offices may simplify what the Network does
  - Dramatic rise of IoT and Smart buildings might change primary focus of the network
- “Gartner: Zero Trust Is Not a Security Panacea” sdxcentral.com article January 25th 2023

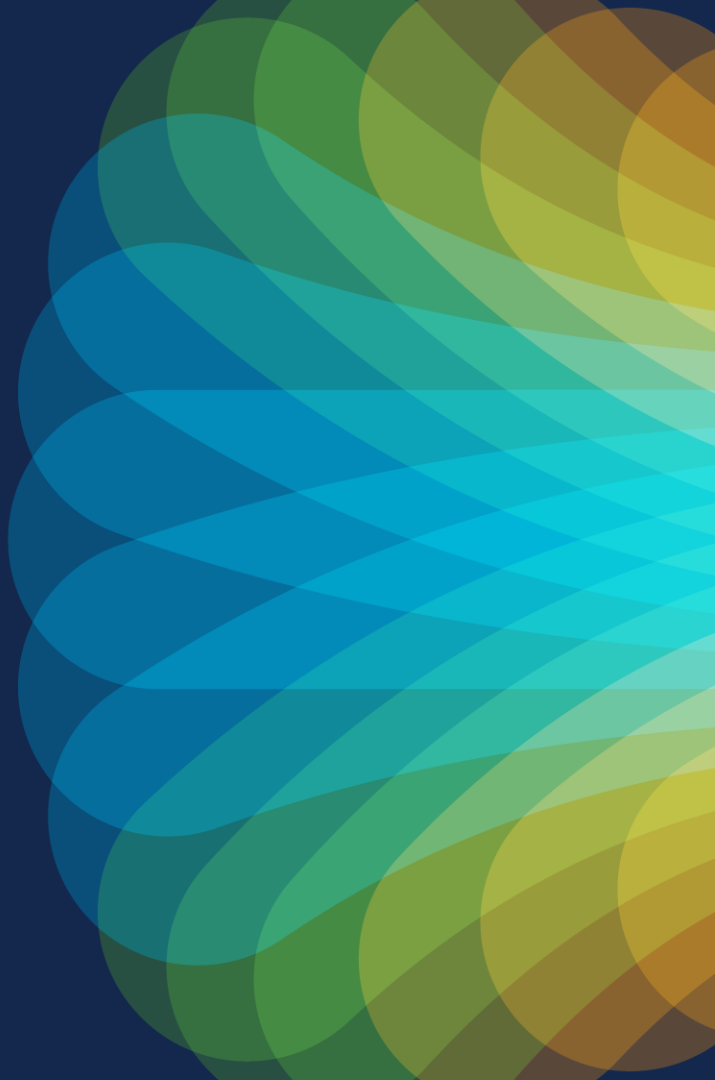
Off Prem Access



On Prem Access



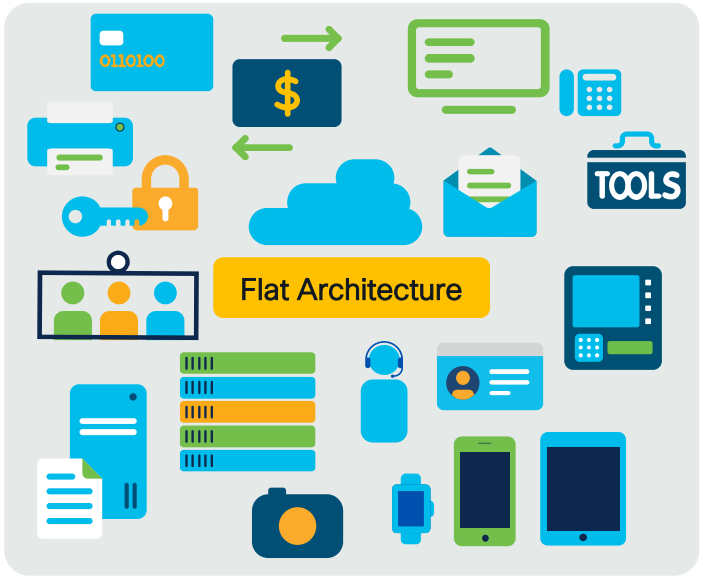
Securing the Workplace



cisco Live!

Transition from Flat Network to Zero Trust Segmentation

Current State



Zero Trust State

As Published by Cisco Press Book: "Zero Trust Architecture"

Zero Trust Success – More than Technology (Layer 8)

Service Owner
Application Owner

Security
Definition

"Policy Decision Maker"

- Approves and drives policy
- Gives the command to block communications
- Owns service impact

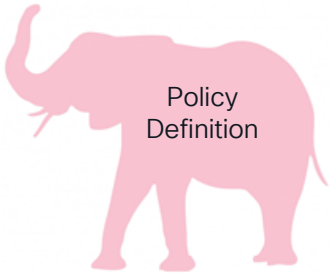
Infrastructure
Execution

Operational Needs

Policy

Audit & Compliance

Event Management



Policy
Definition

ITIL Management

Service Desk

Network Operations

Network Engineering

Users/Application / IoT Device

- What does it need to talk to?
- Where do endpoints and host reside?
- Availability/Business Continuance Requirements

Business Drivers

- Regulatory (Federal/Industry)
- Availability (Factories must run)
- Other Drivers?

Execution of Policy Rules

- Configuration of infrastructure to enforce the policy

Business Governance
And Executive Sponsorship

Cisco's Zero Trust capabilities

Establish Trust

- User / device / service identity
- Posture + context
- Risk-based authentication

Enforce Trust-Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Continuously Verify Trust

- Re-assessment of trust
- Indicators of compromise
- Shared signals
- Behavior monitoring – threat and non-threat activity
- Vulnerability management

Respond to Change in Trust

- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows

User & Device Security | Network & Cloud Security | Application & Data Security

Establish Trust

ISE Provides Zero Trust for the Workplace

Enterprise

Security

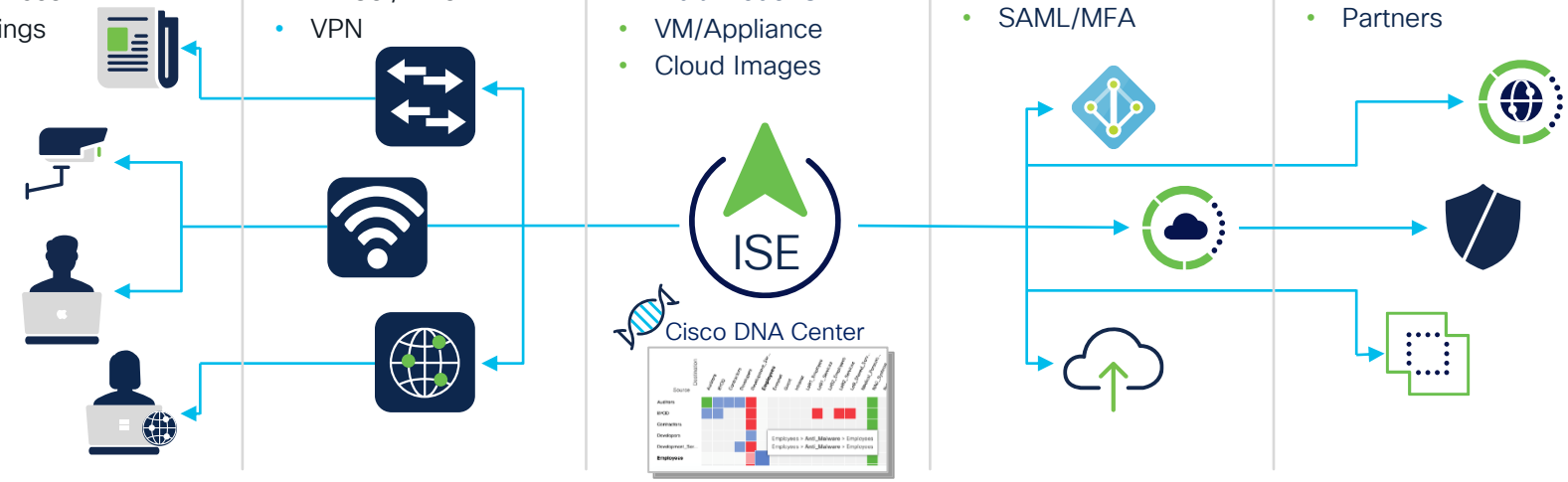
Endpoints
- Users
- Devices
- Things

Network Devices
- Switches
- WLCs / APs
- VPN

Cisco ISE
- Standalone ISE
- Multi-node ISE
- VM/Appliance
- Cloud Images

Identity Services
- Azure/AD/LDAP
- MDM
- SAML/MFA

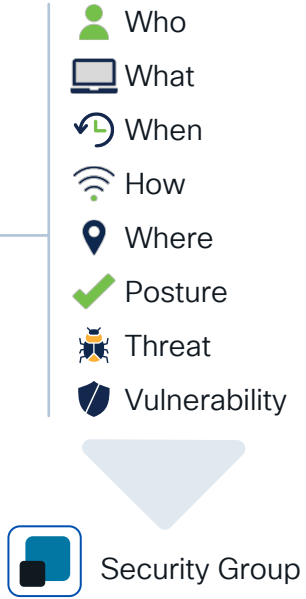
Security Services
- Network Analytics
- Secure Firewall
- Partners



Context Build, Summarize, Exchange

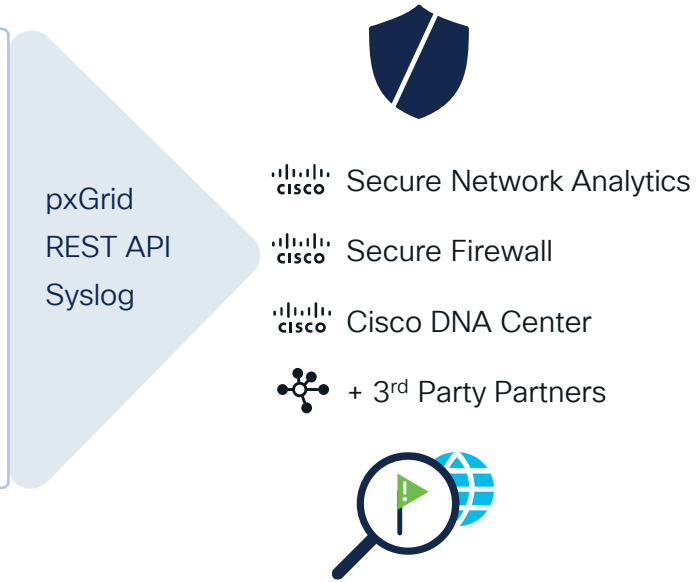
Visibility and Access Control

ISE builds context and applies access control restrictions to users and devices



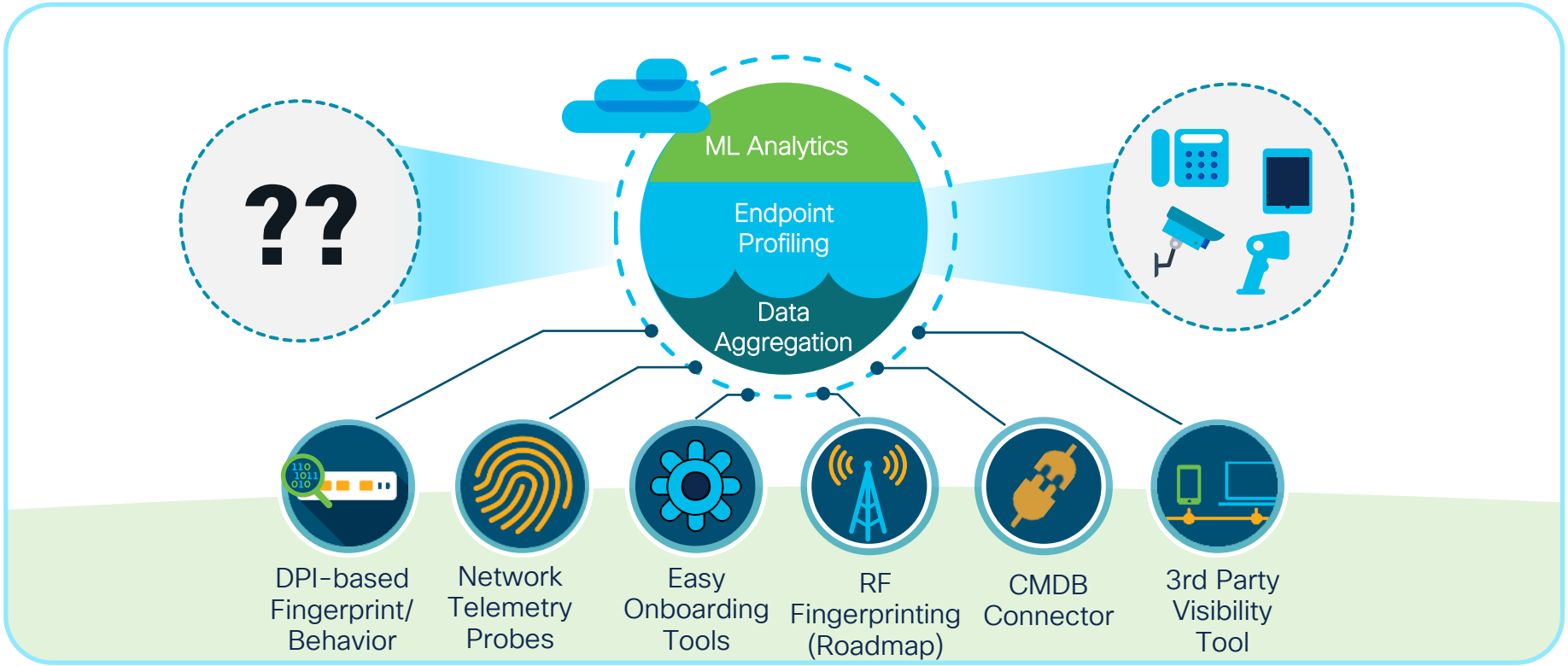
Context Reuse

by eco-system partners for analysis & control

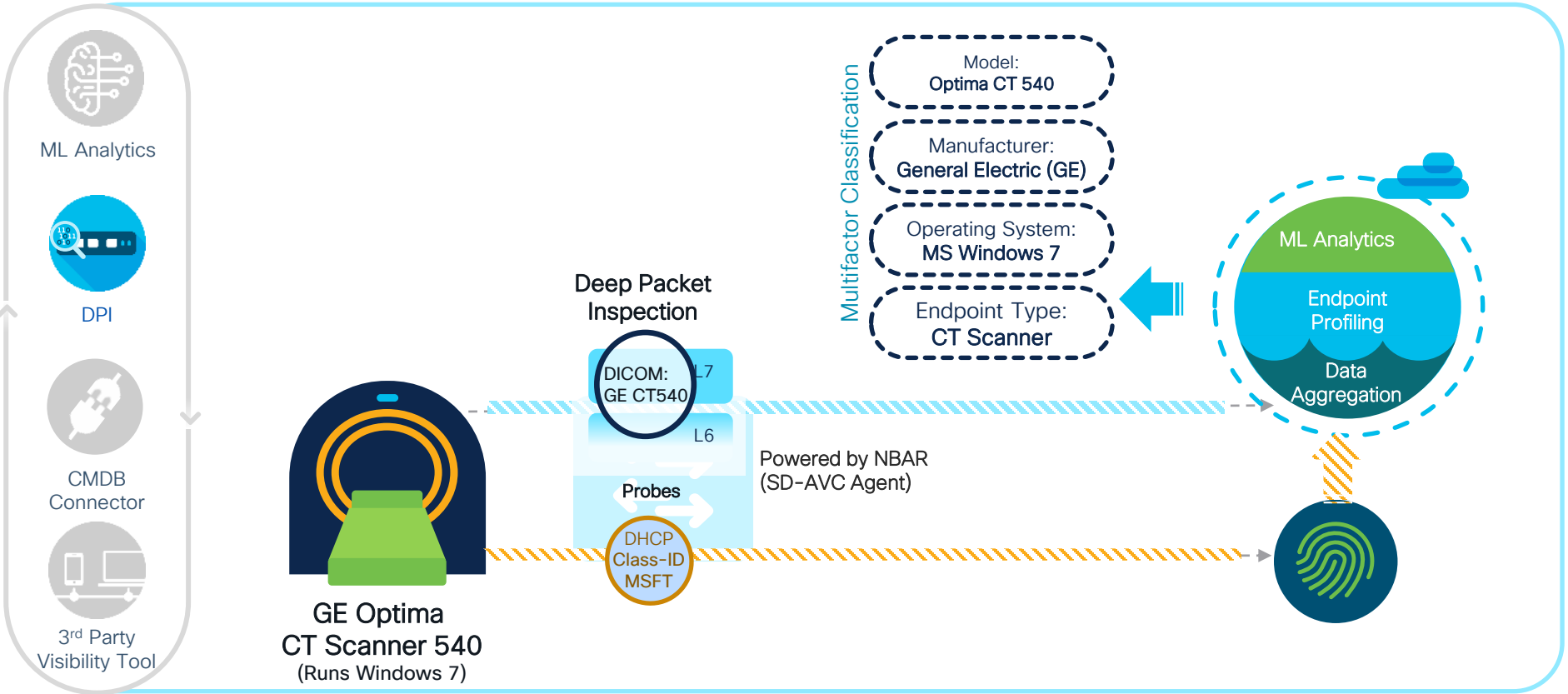


Improving Profiling – AI Endpoint Analytics on Cisco DNA Center (NetOps)

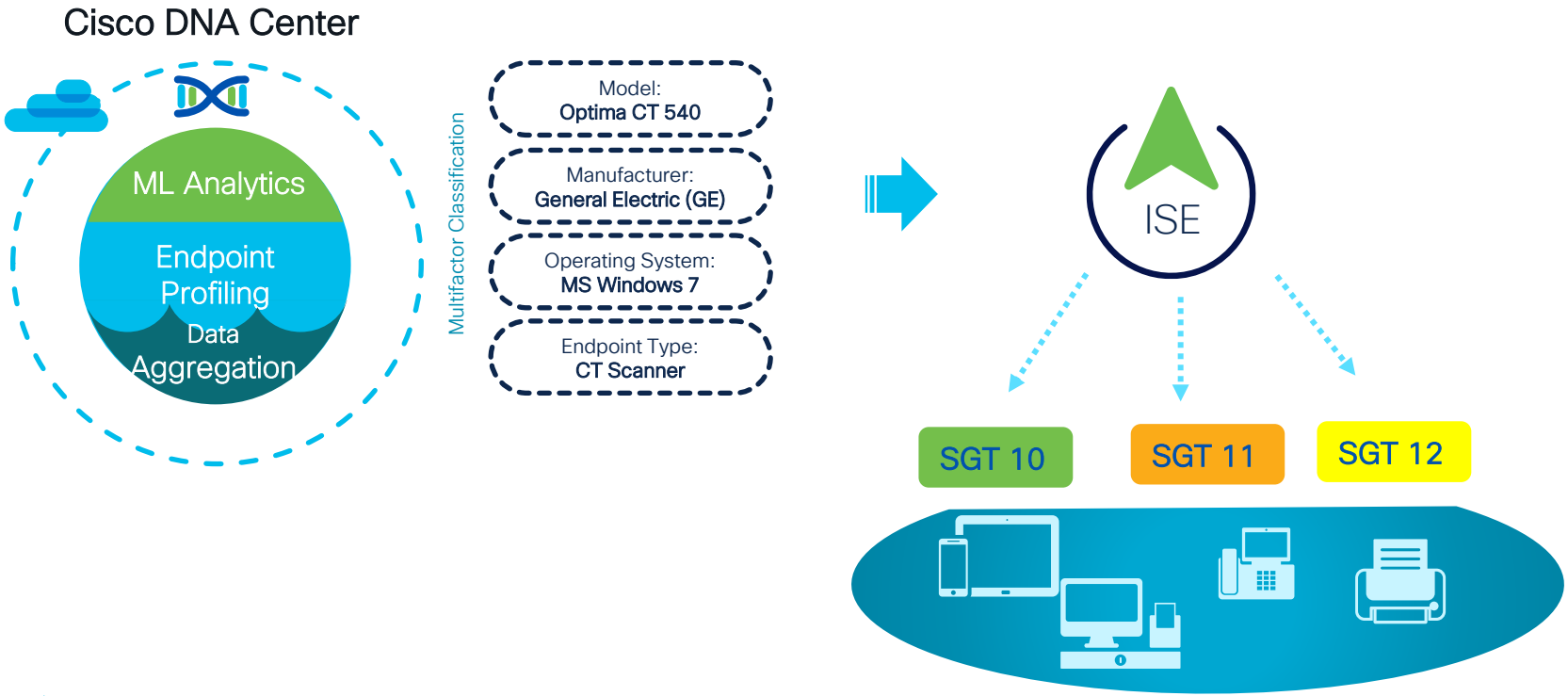
Rapidly reducing the unknowns to gain visibility on the pathway to Zero Trust



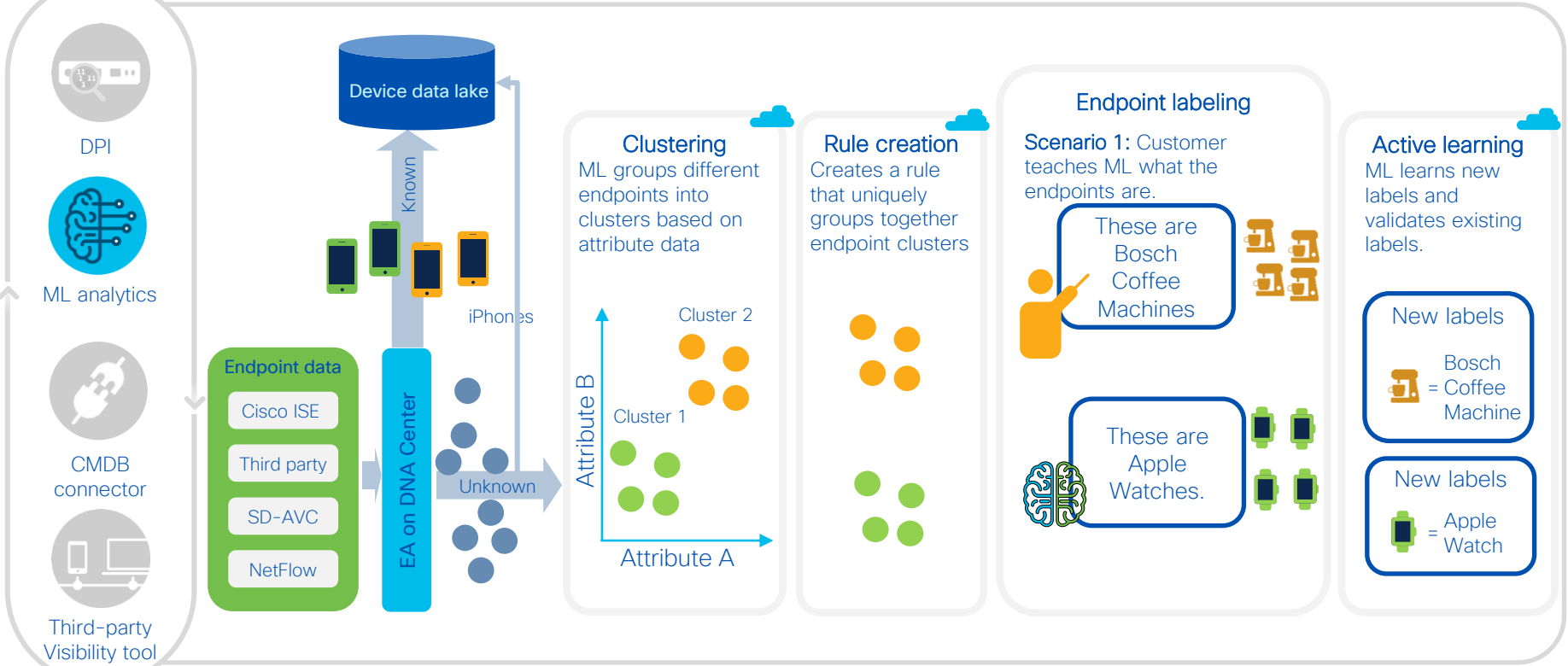
Classification based on Deep Packet Inspection



Better Classification reduces unauthorized access



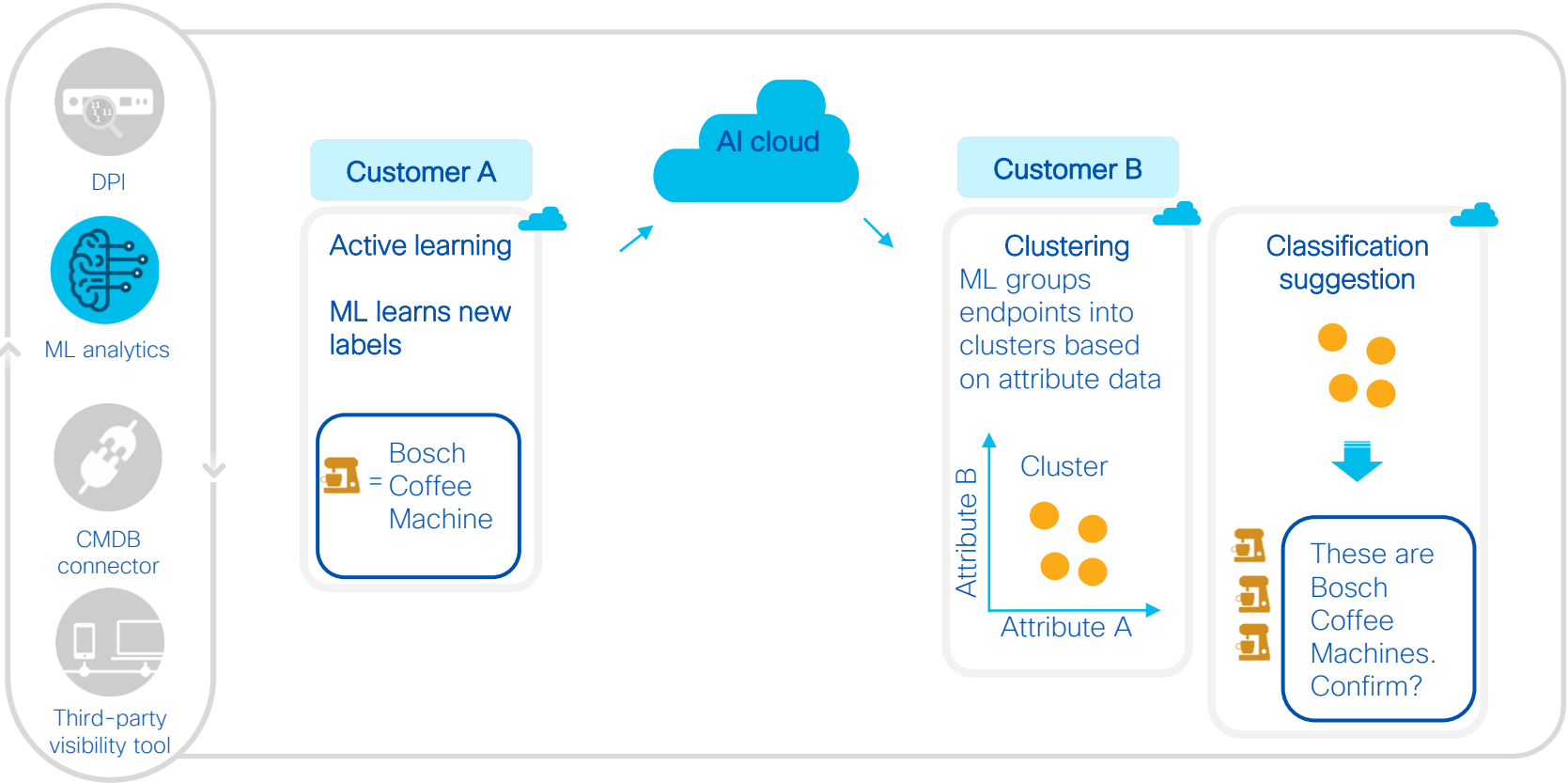
Reducing unknowns when using ML



= done in cloud

- Must forward endpoint attributes to ML cloud (available 3.2p1)
- Air gapped environments not supported

Crowdsourcing using ML



Multi-Factor Classification (MFC) on ISE 3.3 (NetSecOps)

Problem

Current endpoint profiles in ISE are simple strings, making it hard to filter endpoints on simple attributes and set consistent authorization policy

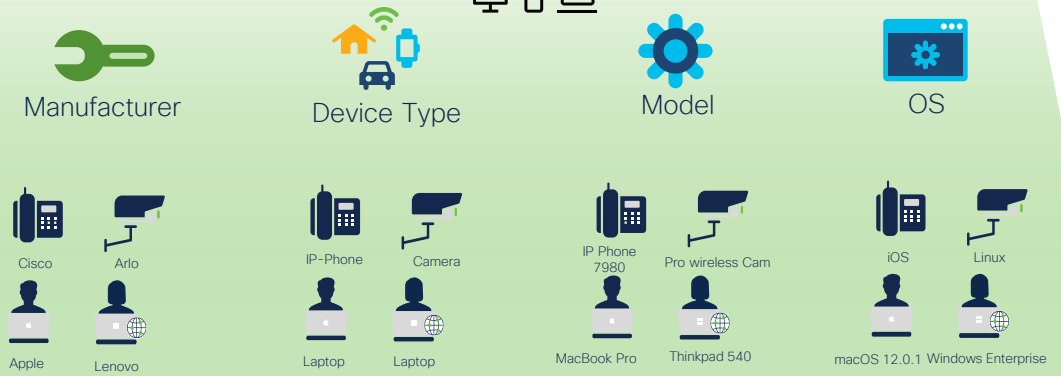
Solution

Profiles are now made up of four factors: MFC-Manufacturer, MFC-Model, MFC-OS, and MFC-Endpoint Type.

Benefits include easily setting policy based on these four MFC attributes, as well as compatibility with Cisco's AI/ML profiling engine

Caveats / Prerequisites

- Not turned on by default
- Does not work with current custom profiles



Use Wi-Fi Edge Analytics data for ISE 3.3

Problem

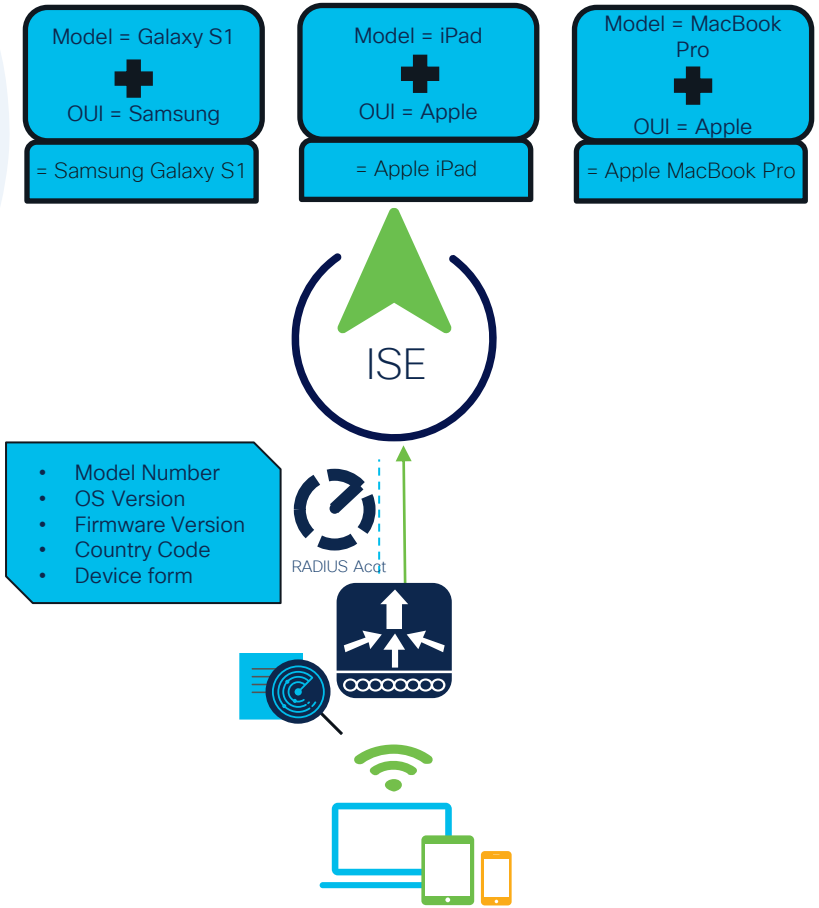
Apple, Samsung, and Intel devices are sharing rich data with WLCs that can improve profiling but was not usable in the past

Solution

9800 WLCs will now pass endpoint specific attributes to ISE, enabling for fast, accurate, and simple profiling of Samsung, Apple, and Intel devices

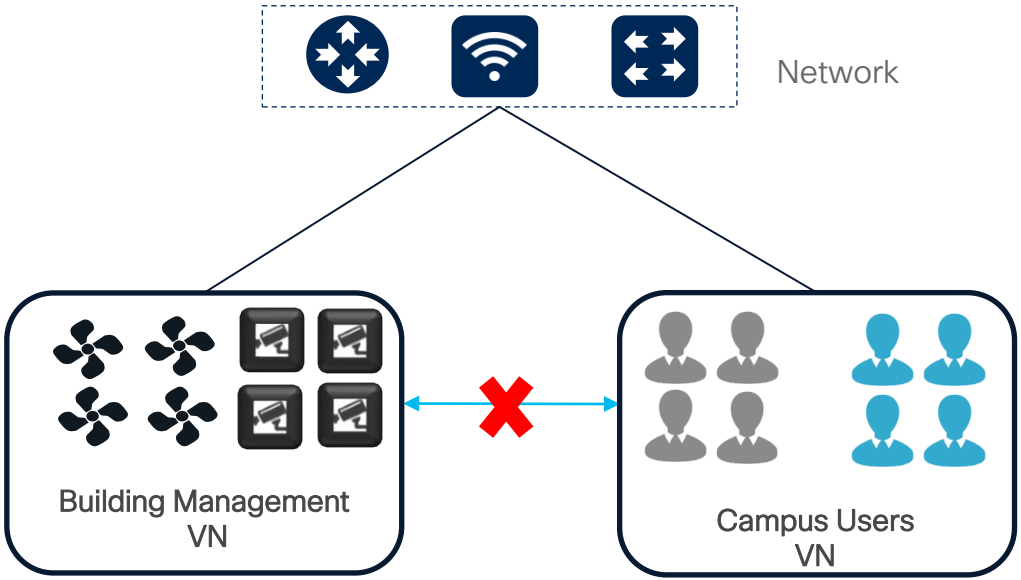
Caveats / Prerequisites

Must have 9800 WLCs
IOS-XE 17.10



Enforce Trust-Based Access

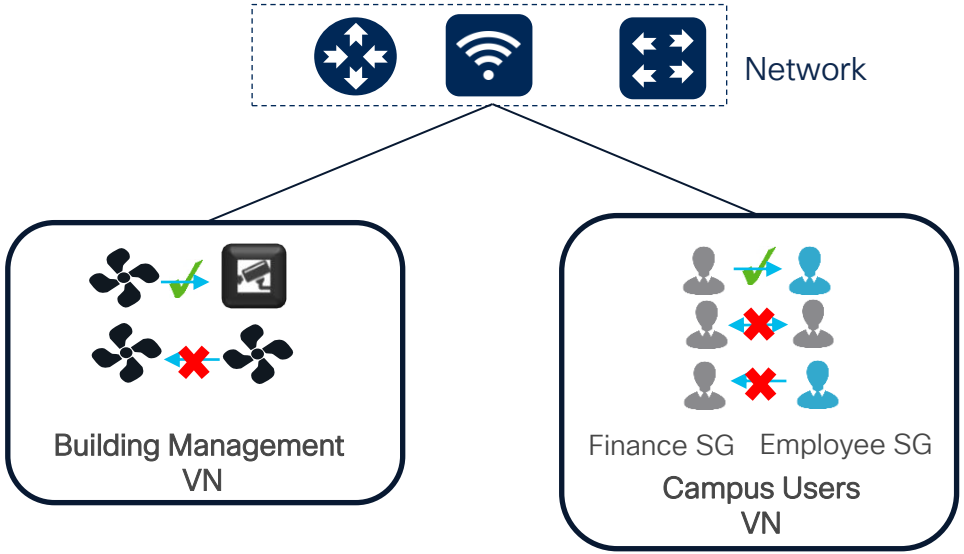
Two Level Hierarchy – Macro Level



Virtual Network (VN)/ Virtual Private Network (VPN)/ VRF/Zones

First level Segmentation that ensures **zero** communication between specific groups. Ability to consolidate multiple networks into one management plane.

Two Level Hierarchy – Micro Level



Group Based Policy (SGT)

Second level Segmentation **ensures role based access control** (least privilege) between two groups within or between Virtual Network(s). Provides the ability to segment the network into either line of businesses or functional blocks.

- SGT = Security Group Tag, Source Group Tag, Scalable Group Tag

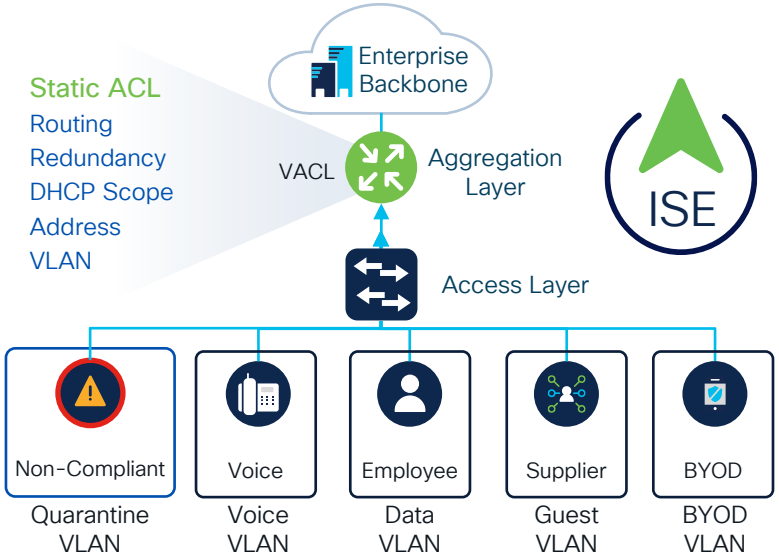
5 Security Group

5 Source Group

5 Scalable Group

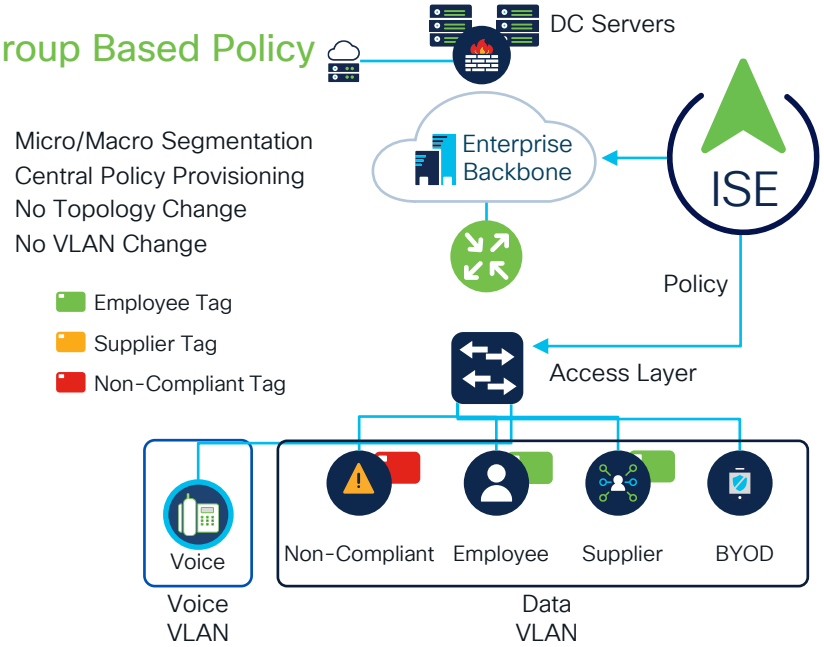
Group Based Policy Simplifies Trust Based Policy

Traditional Segmentation



Security Policy based on Topology
High cost and complex maintenance

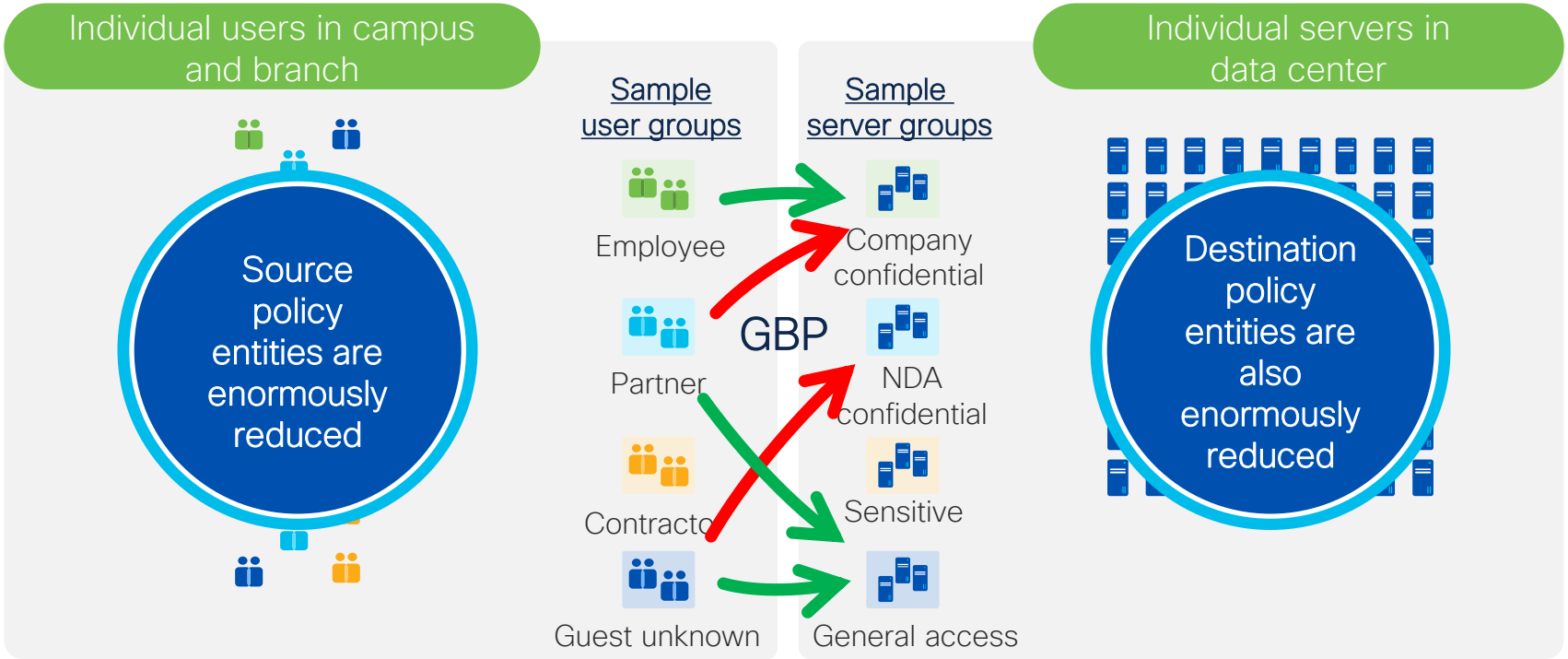
Group Based Policy



Use existing topology and automate
security policy to reduce OpEx

The Value of Group-Based Policies

Enhanced simplicity for better enforcement and management



Trust-Based Policy Workflow

View/Model Policy
Analyze the Network

- Visualize traffic flows
- Create groups
- Identify policies

Establish Policy
Establish the policies

- Establish Group-Based Segmentation Policy
- Trial/Monitor group-based policies
- Apply group-based Policy

Verify Policy
Continuous Trust Monitoring

- Monitor Policies effectiveness
- Detect Policy violations
- Deduce policy updates requirements

View/Model Policy

Group-Based Policy Analytics (GBPA)

Application on Cisco DNA Center (NetOps)

Policy Discovery

Policy Modeling

Policy Enforcement

ISE Scalable Groups and Profiles

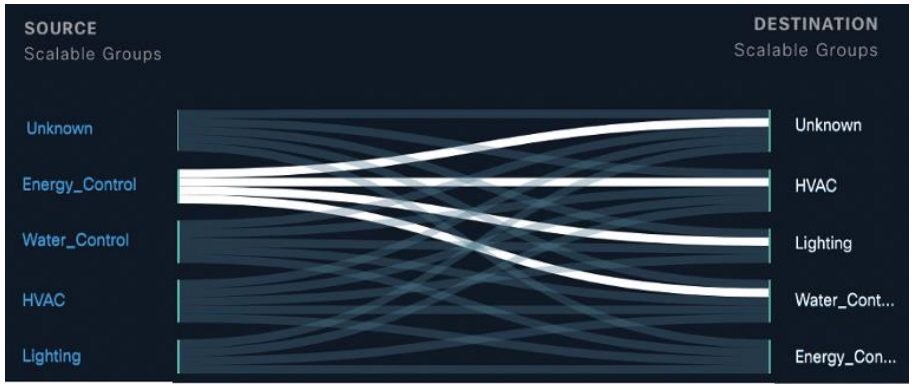
Endpoint Analytics MFC

Cisco DNA Center

Flow Info

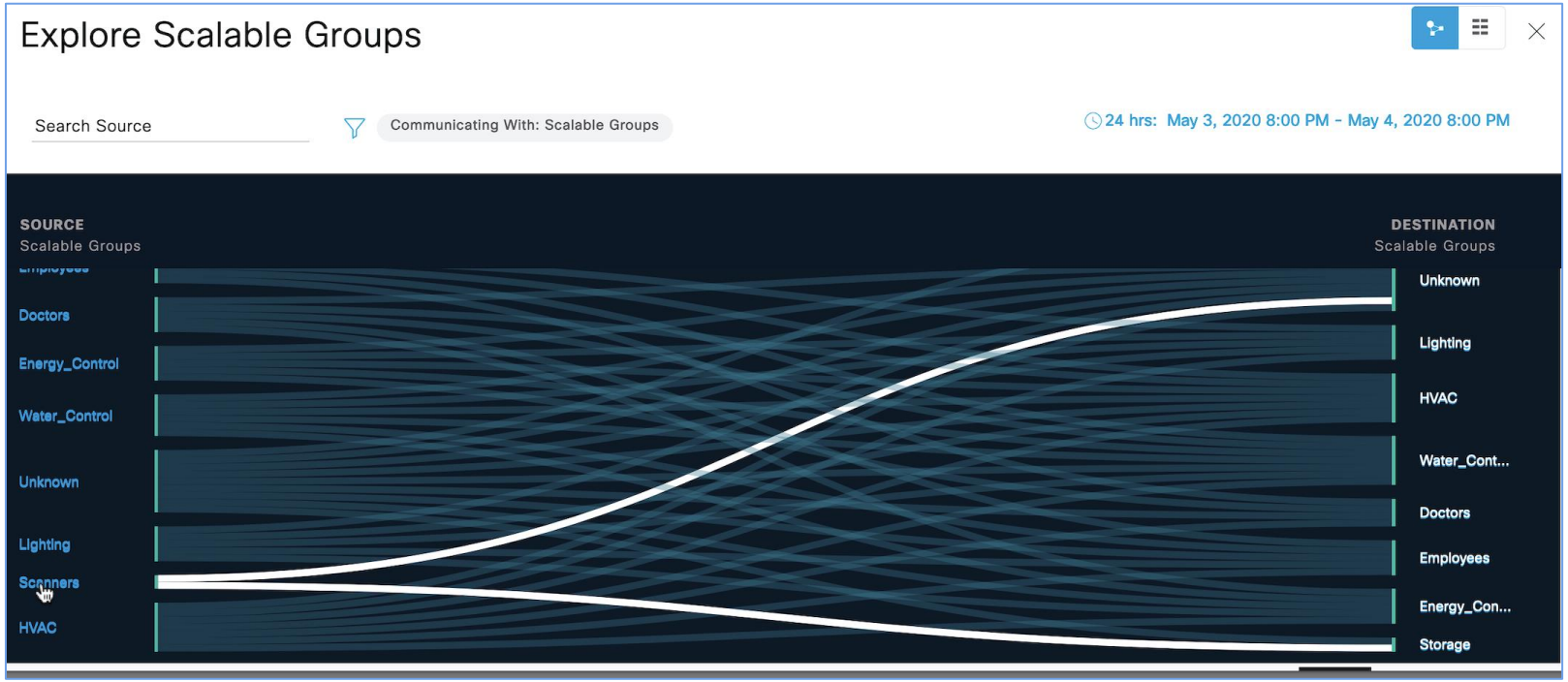
Secure Network Analytics Host Groups

Group-Group Activity



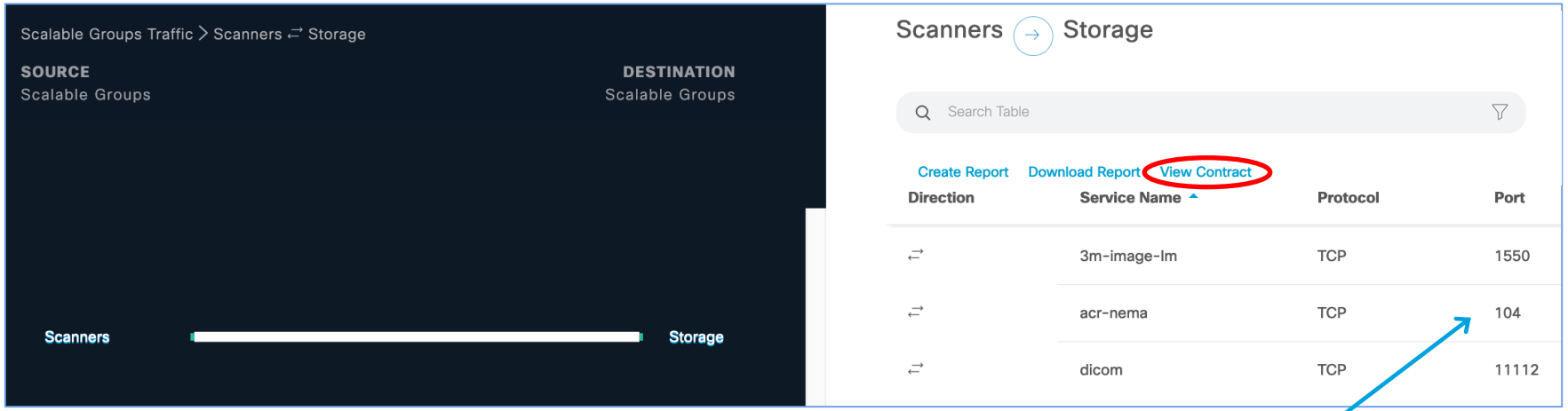
Direction	Service Name	Protocol	Port
⇄	3m-image-lm	TCP	1550
⇄	acr-nema	TCP	104
⇄	dicom	TCP	11112

Group to Group Activity
(GBPA App on Cisco DNA Center)



Detecting Ports/Protocols Between Groups

(GBPA App on Cisco DNA Center)



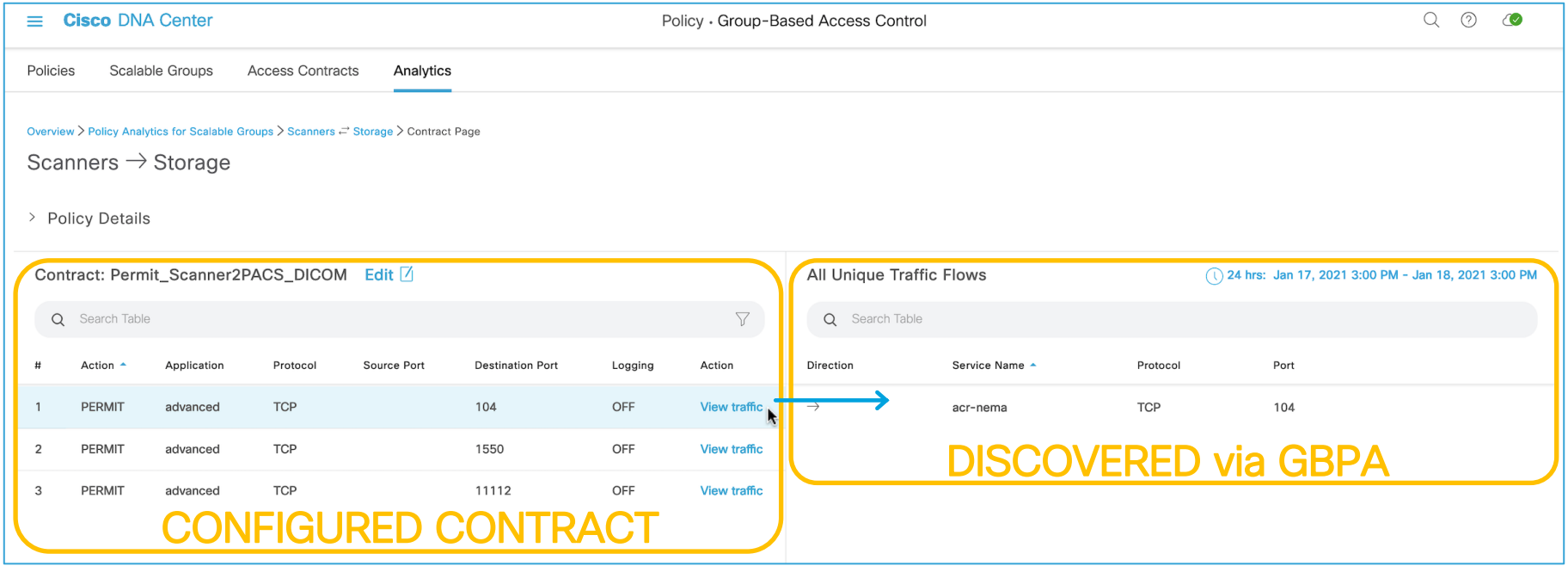
N.B. DICOM: Digital Imaging and Communications in Medicine

Ports 104, 1550 and 11112 detected between Scanners and Storage groups, all used for DICOM interaction

Identify the specific ports/protocols needed in access control policies

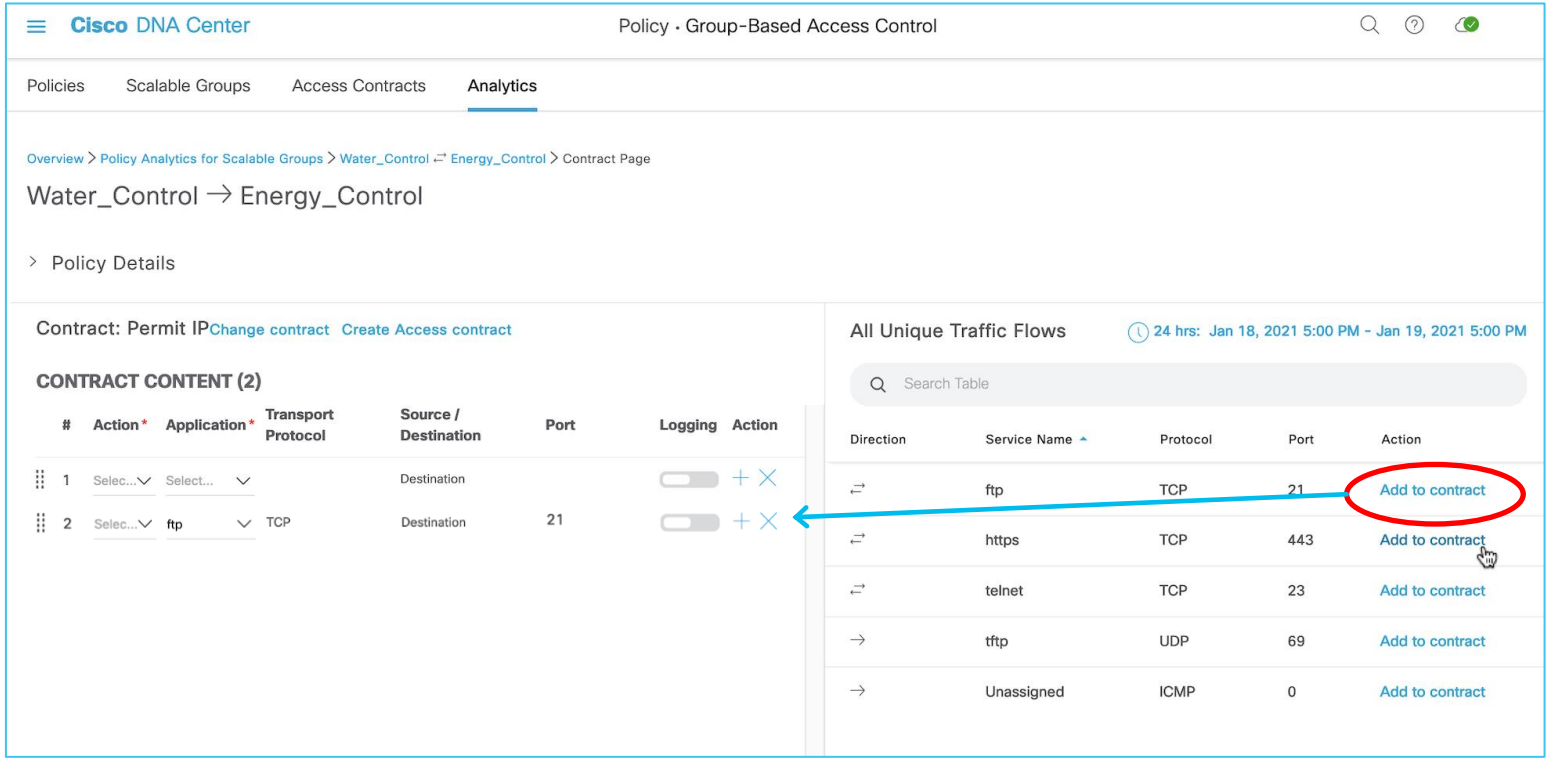
Contract and Discovered Information Side-by-Side

(GBPA App on Cisco DNA Center)



Create/Edit Contract Easily Based on Discovered Flows

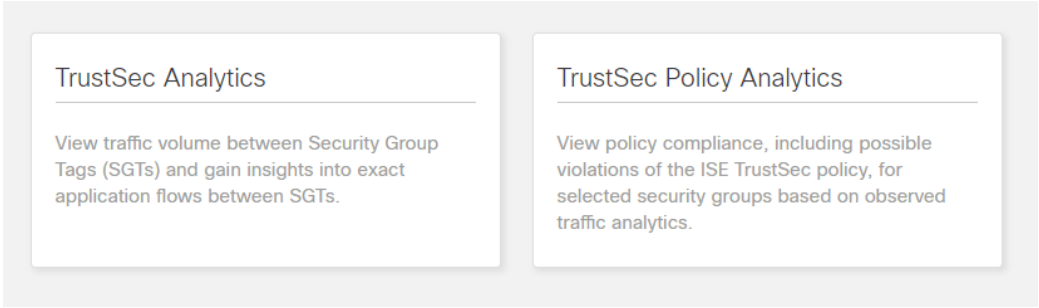
(GBPA App on Cisco DNA Center)

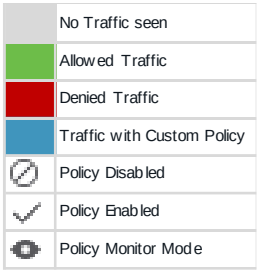


Secure Network Analytics (SNA)

Visualizing communications between SGTs (NetSecOps)

- Report on all observed SGT group communications
- Quickly see which SGTs are communicating
- Click on any cell to display the amount of data transmitted
- View up to 300 SGTs

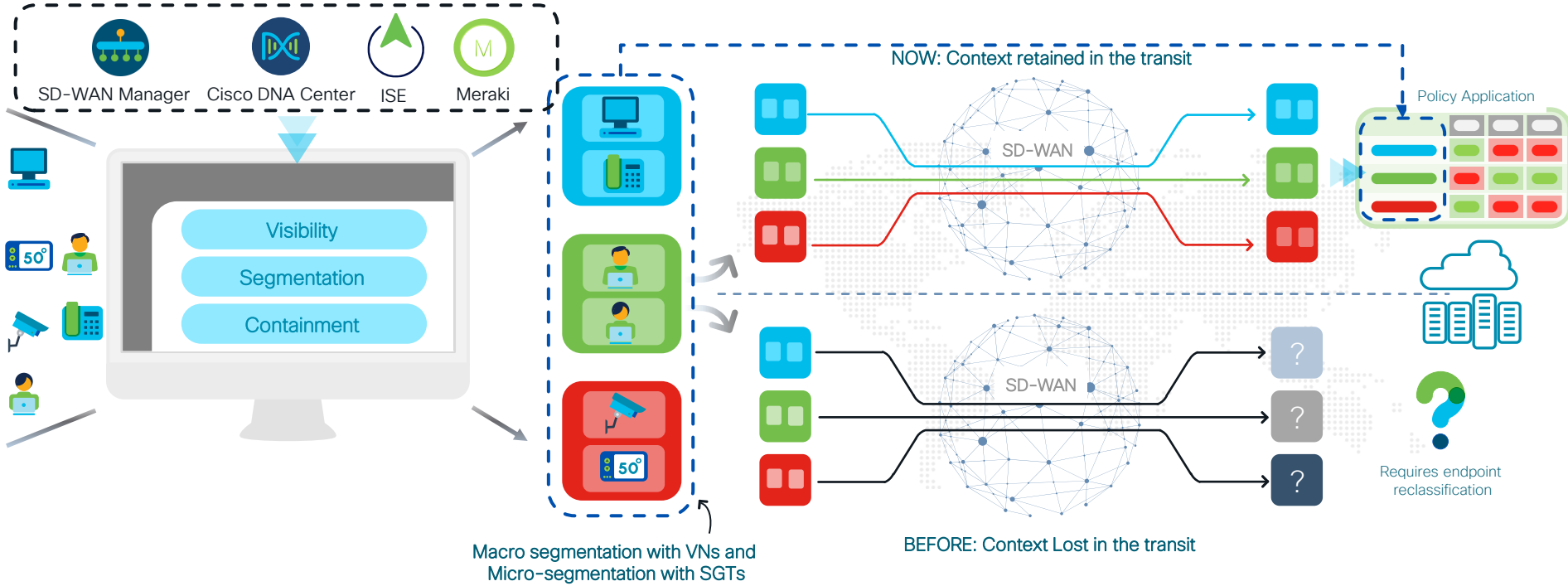




Establish Policy

Multidomain: Integration for Scaling

Connecting distributed trusted domains at scale



Retain policy context

Exchange the 'rich' context at scale across distributed trusted domains

Uniform security policy

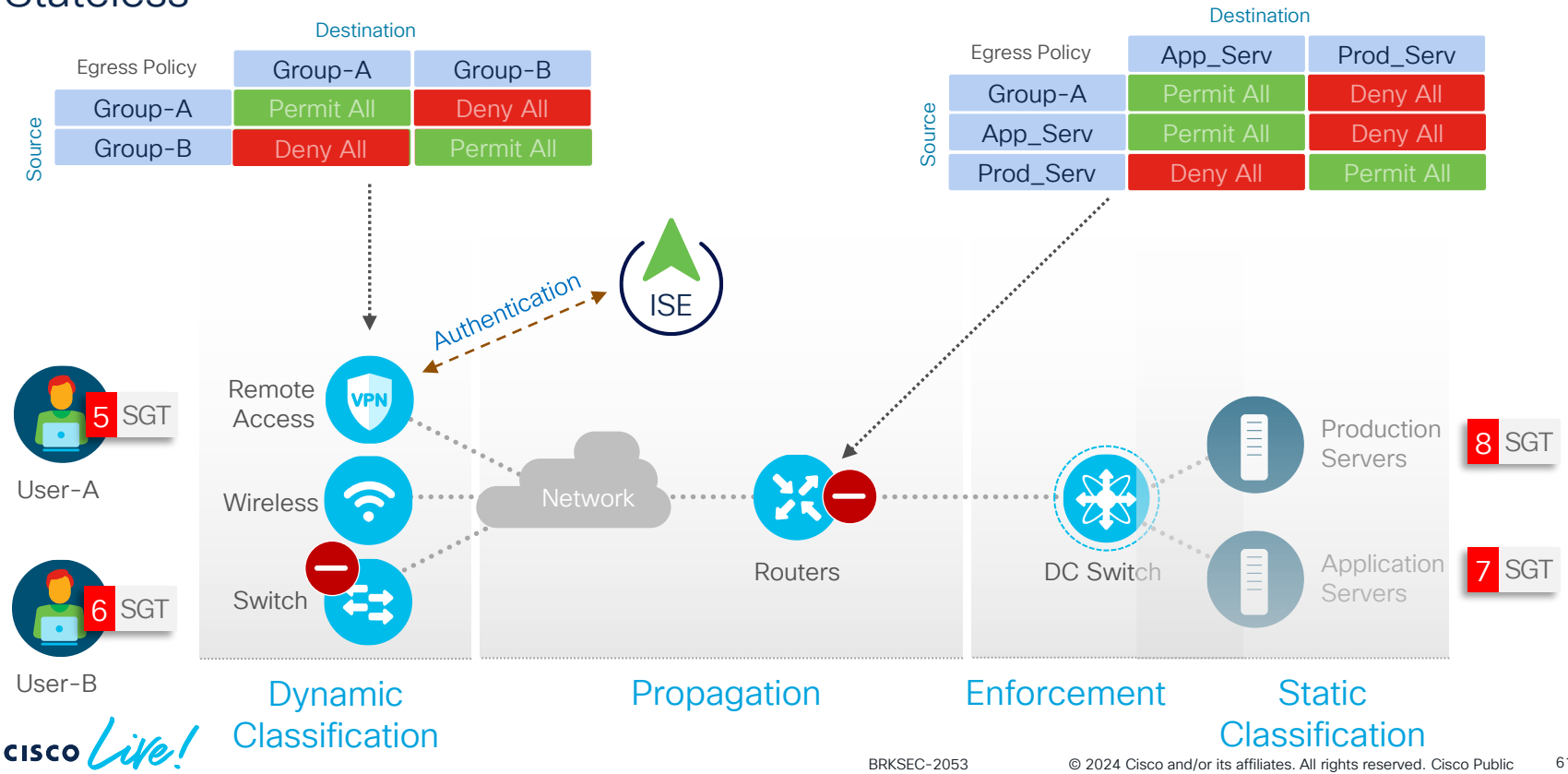
Having same rich context everywhere enables uniform policy application without having to reclassify endpoints

Controller Integration

Fully Automated, flexible deployment models between SDA and SD-WAN

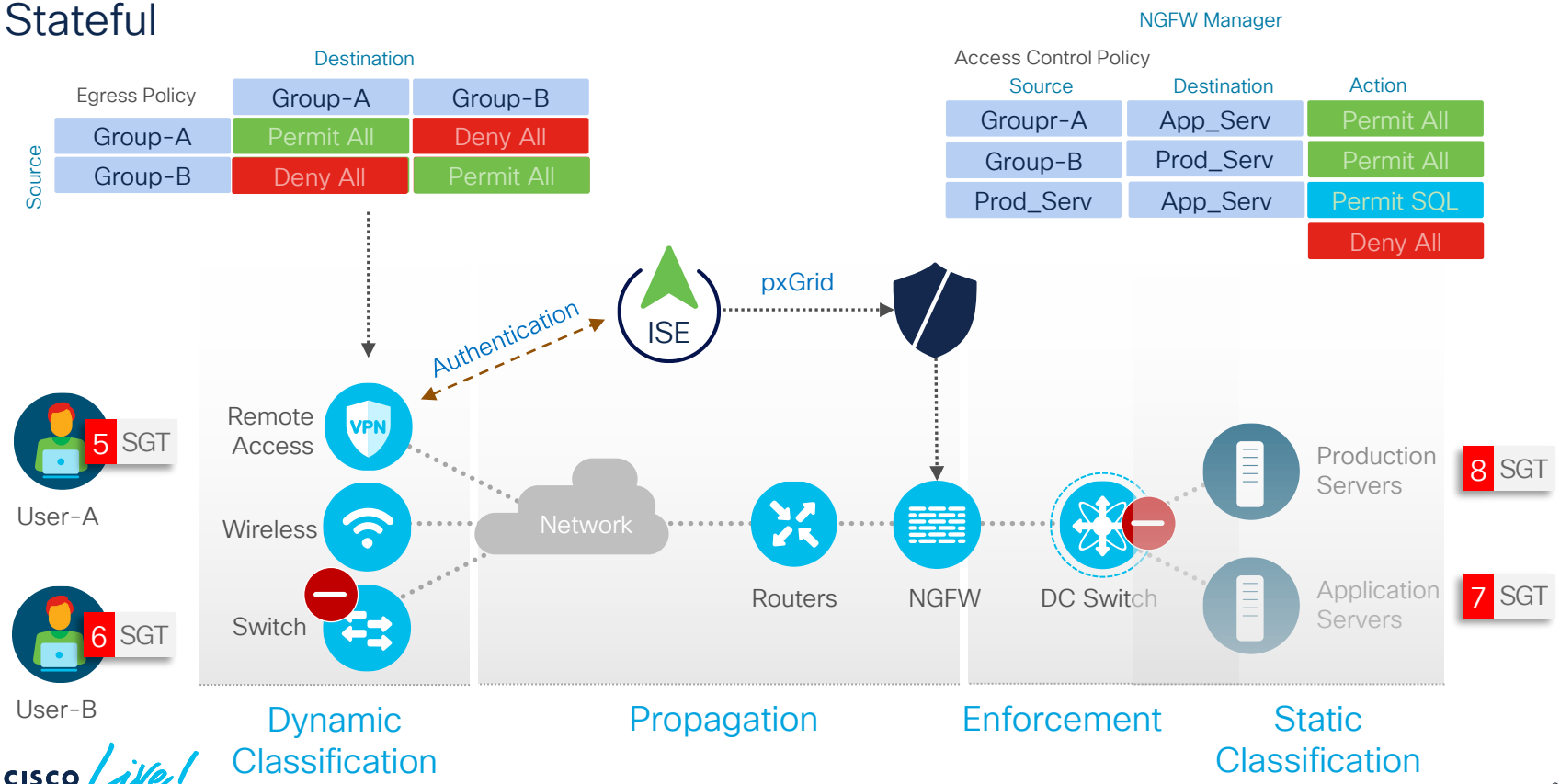
Group-Based Policy in Operation

Stateless



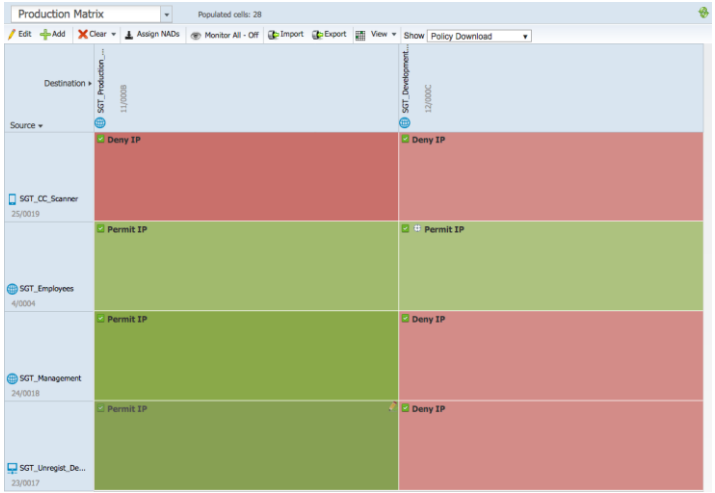
Group-Based Policy in Operation

Stateful



Enforcement of Group-Based Policies

- SGACL



- SGFW

Source			Destination			Action
IP	Group/User	Security Group	IP	Security Group	Port	Action
ANY	ANY	Employees on Corporate Assets	ANY	ACI_Intranet_Servers_EPG	Any tcp	Allow
ANY	ANY	Senior Execs on registered BYOD devices	ANY	ACI_Finance_Servers_EPG	http, https	Allow
ANY	ANY	Contractors on unmanaged devices	ANY	ACI_Citrix_VDI_EPG	RDP, ICA	Allow
ANY	ANY	Divested Business - Employees	ANY	Divested Business Servers	ANY	Allow
ANY	ANY	ANY	ANY	ANY	ANY	DENY

ISE Group policy management

NGFW Manager

ISE Group tag management

Group-Based Policy in Operation

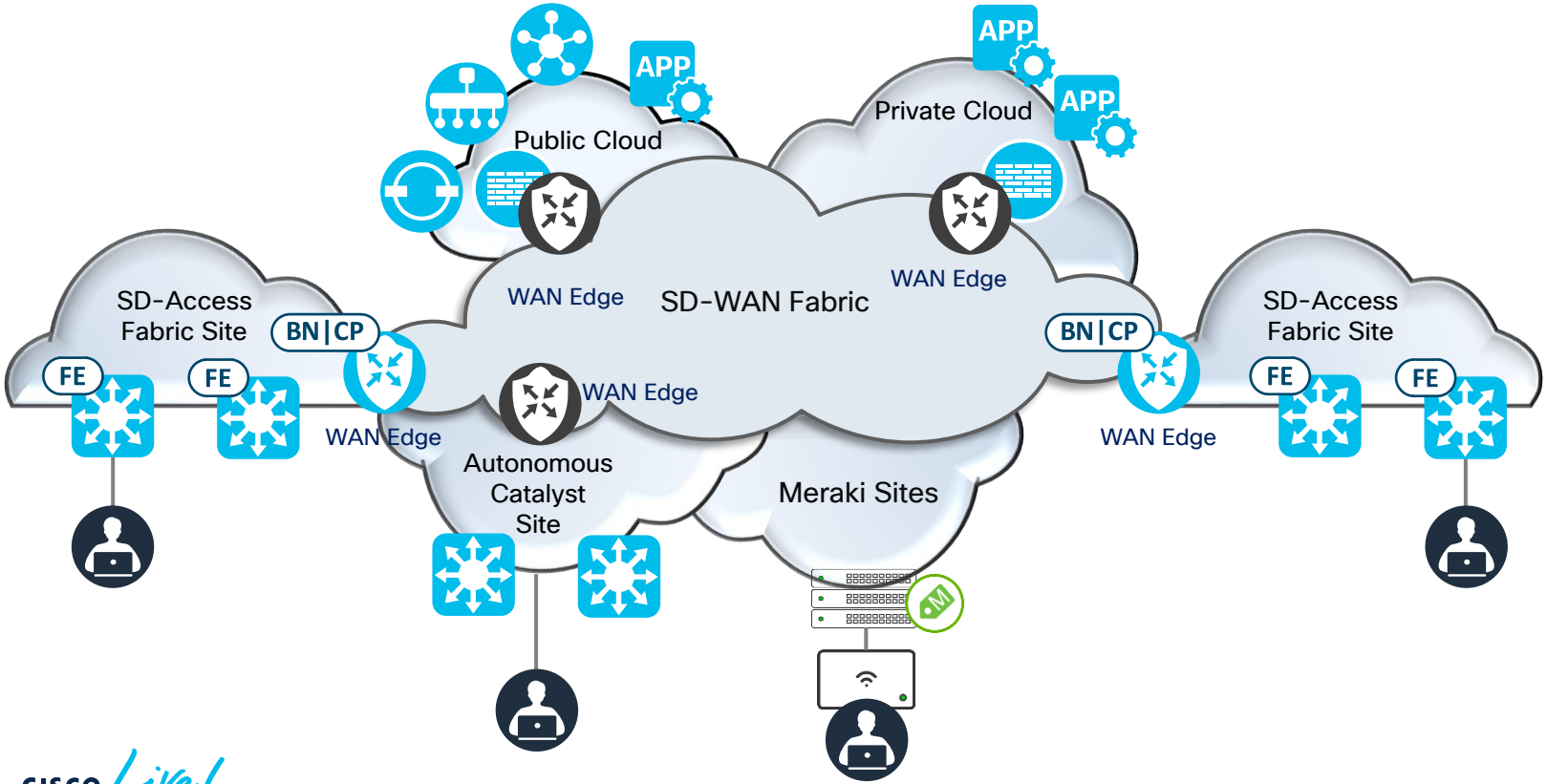
Use-case: Lateral movement

Destination

Egress Policy / Source	Employees	Contractors
Employees	Deny All	Deny All
PLCs	Permit All	Deny All
Contractors	Deny All	Permit All

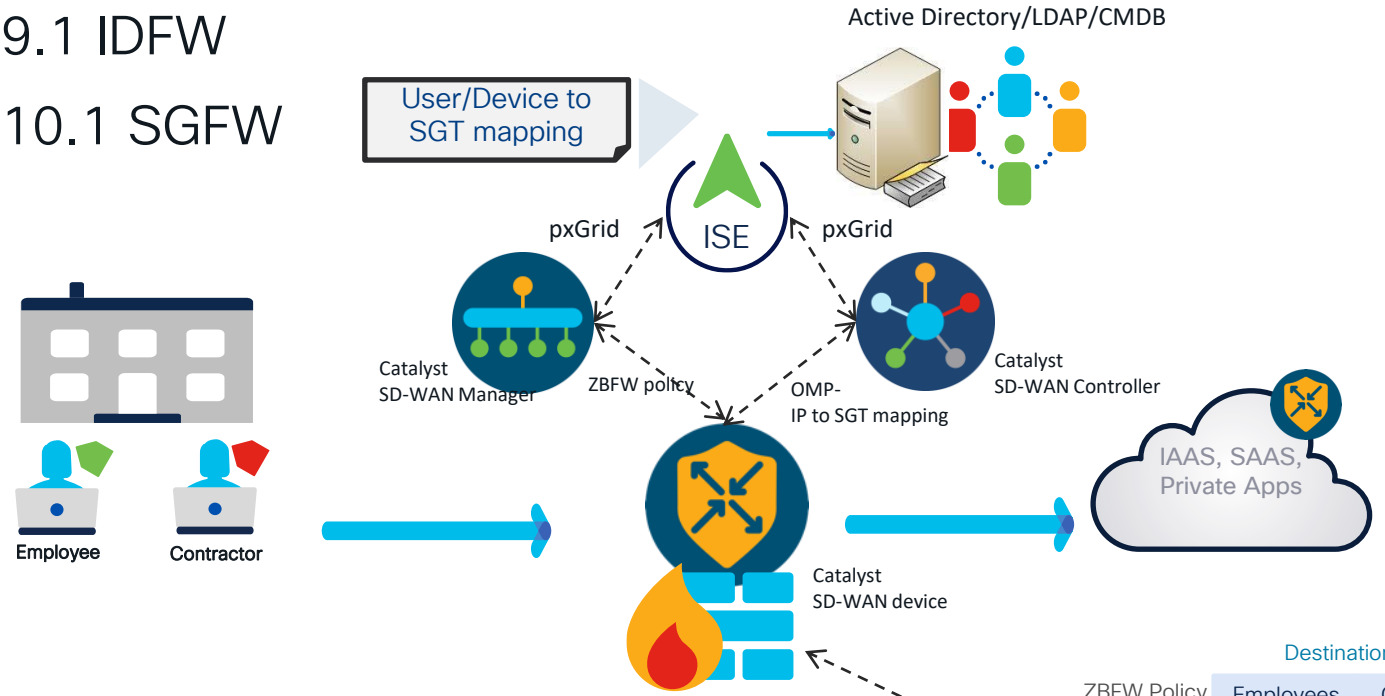
Group Based Policy Integrated Domains – Policy

Cisco Zero Trust Extension of Policy to Private/Public Clouds



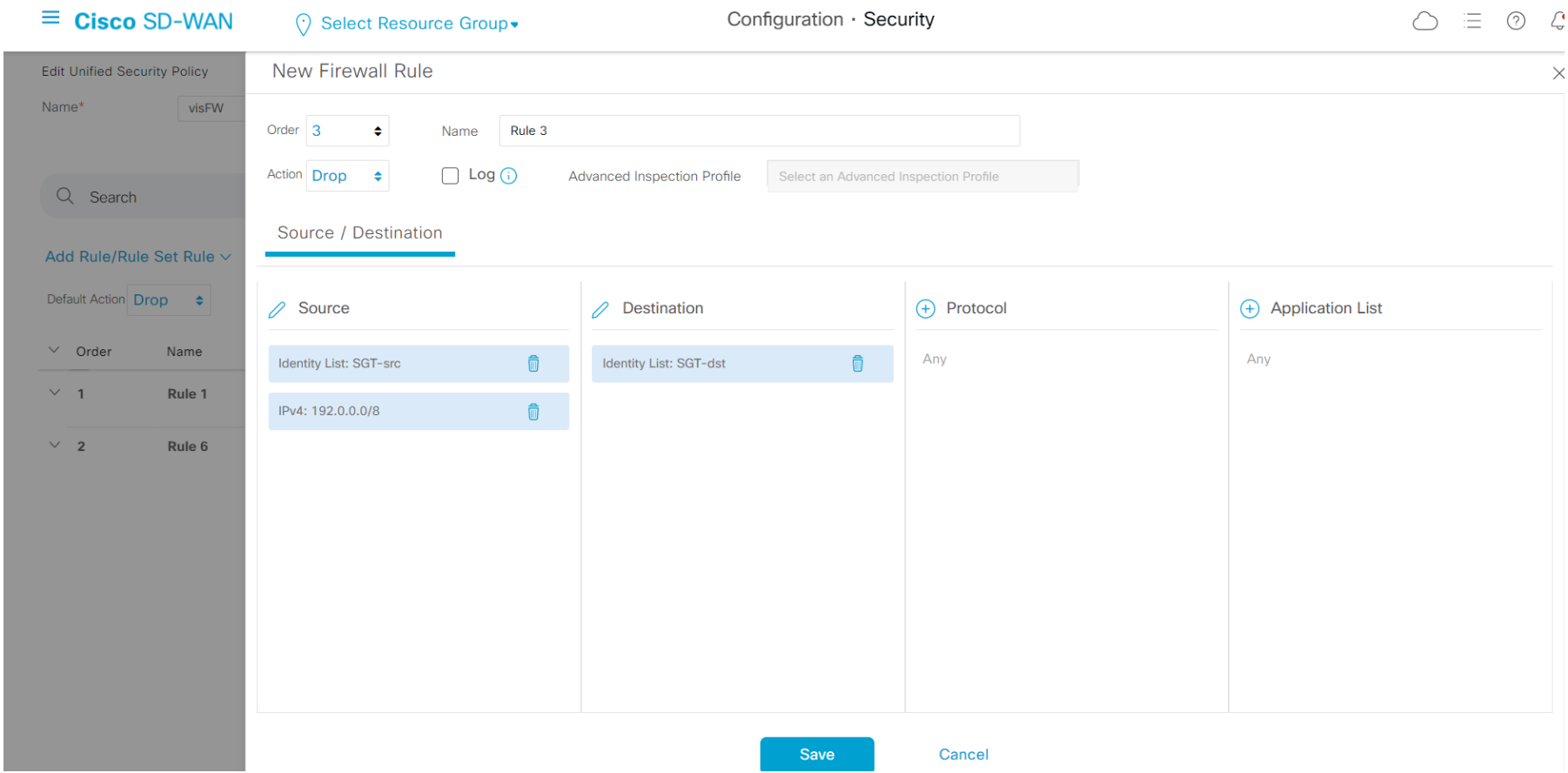
ISE/Cisco SD-WAN Integration

- 17.9.1 IDFW
- 17.10.1 SGFW

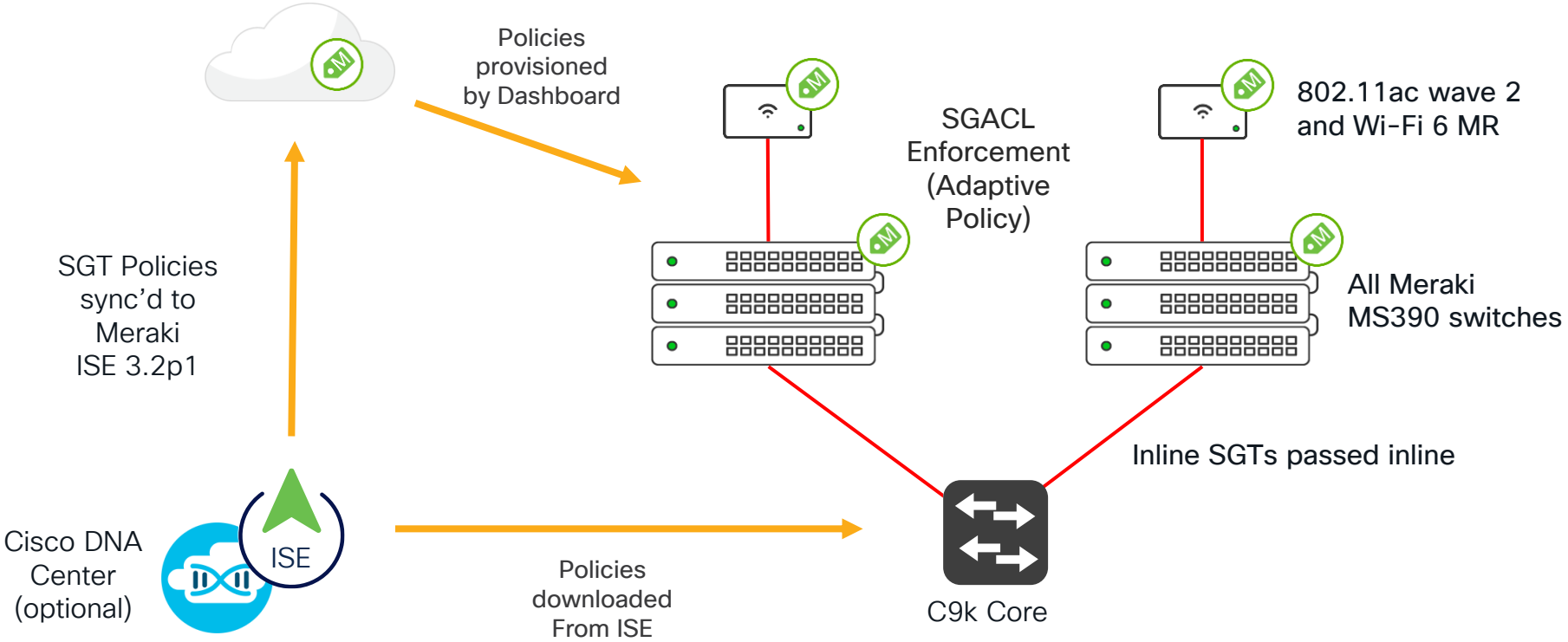


- Granular Security Control at User/Group Level
- Unified Security policy and intent

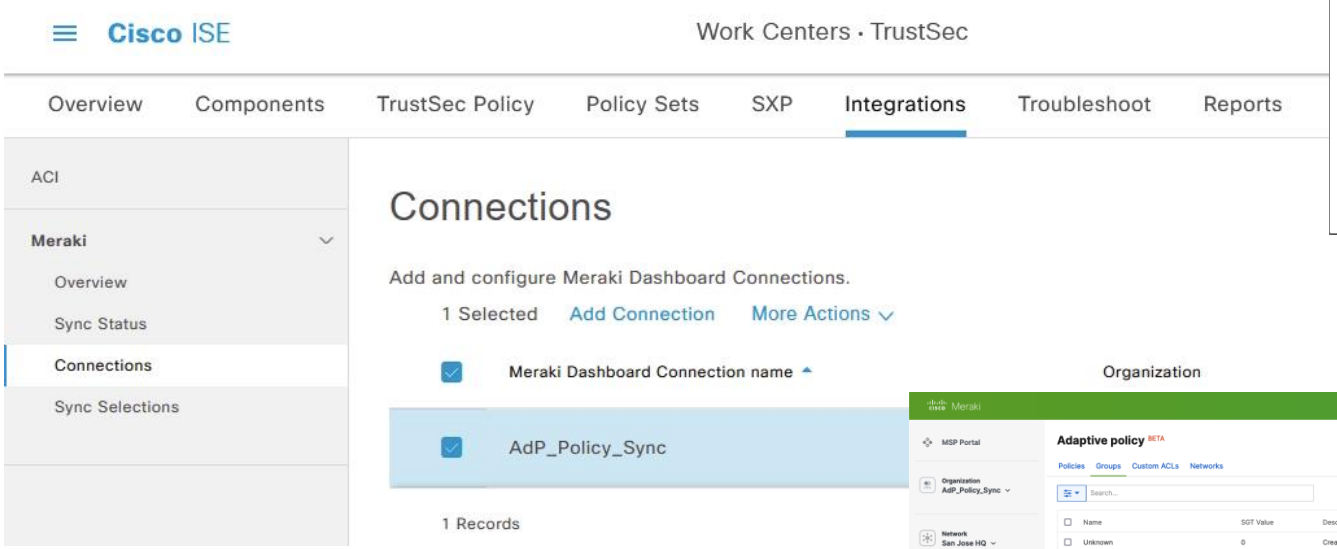
Grouped Based Policy – SD-WAN Group (SGT) Integration

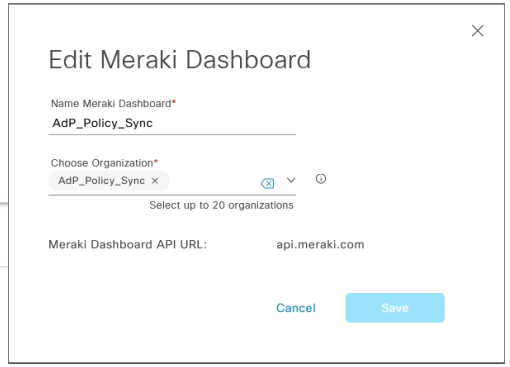


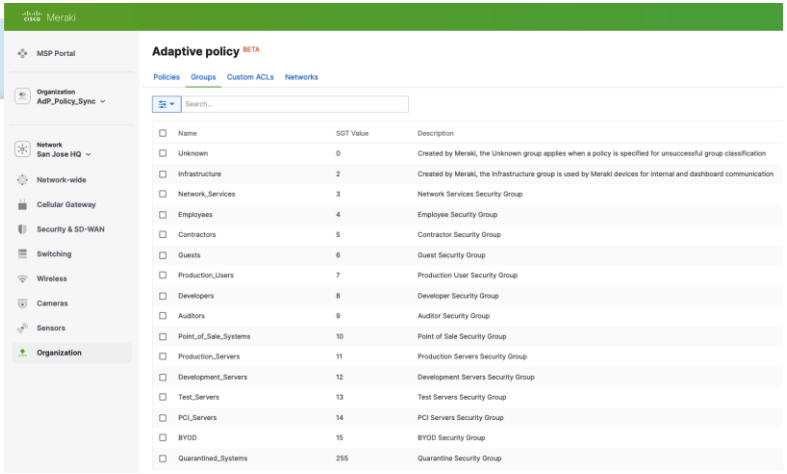
Meraki Adaptive Policy (SGT) and ISE Sync



ISE – Meraki Policy Sync







Open Implementations

- 3rd parties support SGTs via pxGrid - IETF proposal for Security Automation and Continuous Monitoring (SACM) – Check Point amongst others
- SXP published as an Informational Draft to the IETF, based on customer requests
  - shipping partner implementations
  - Open Source SXP Implementations – Java in OpenDaylight, C on github.com
- Includes the Cisco Meta Data (CMD) format for inclusion of the SGT with Ethernet frames (detailed on the next slides)
  - https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/
- All Major NGFW Vendors are interoperable via pxGrid
- SD-WAN competitors are interoperable via inline tagging and pxGrid
- Switching and Wireless Competitors have implemented SGT
- 3rd Party ASIC Vendors are publishing CMD/SGT support

Verify Policy

Policy Counters Cisco DNA Center (NetOps)

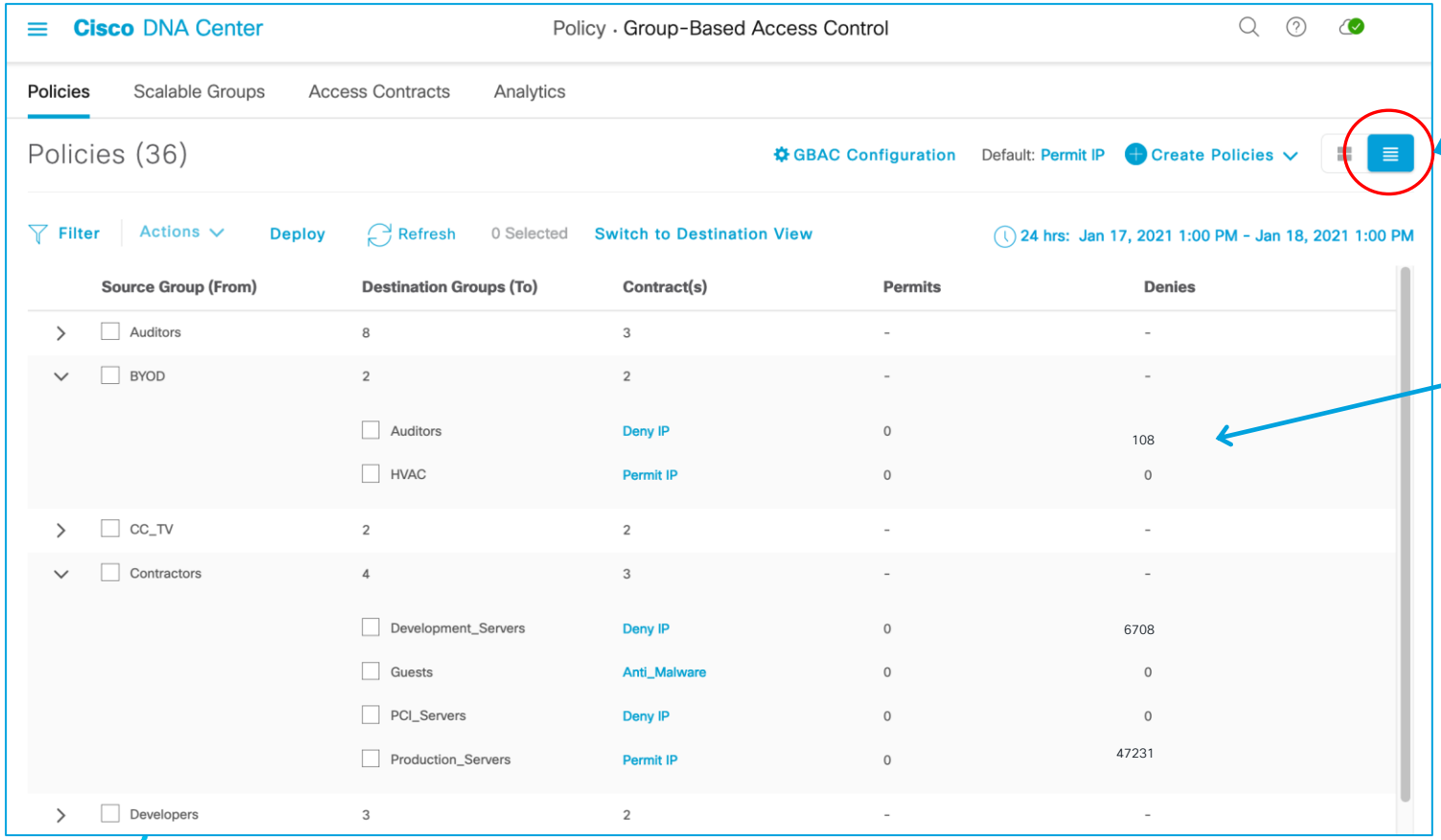


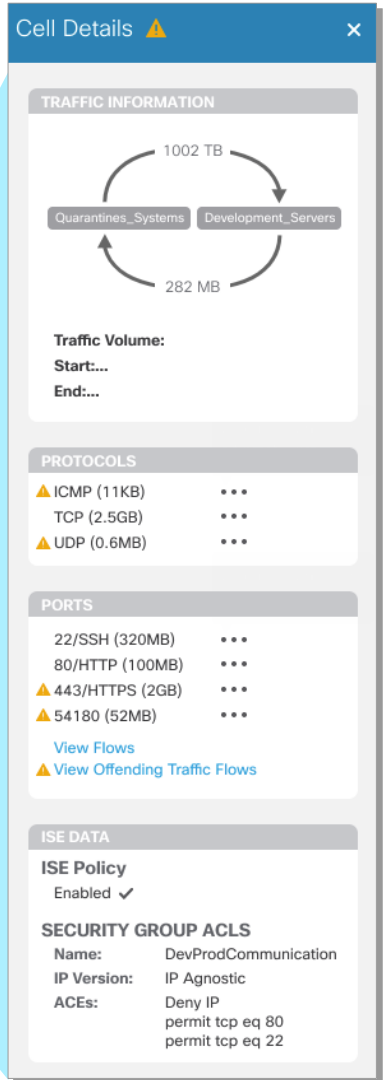
Table View

Permits and Denies per policy

SNA: Validate ISE policy is being observed

Near real time network telemetry (NetSecOps)

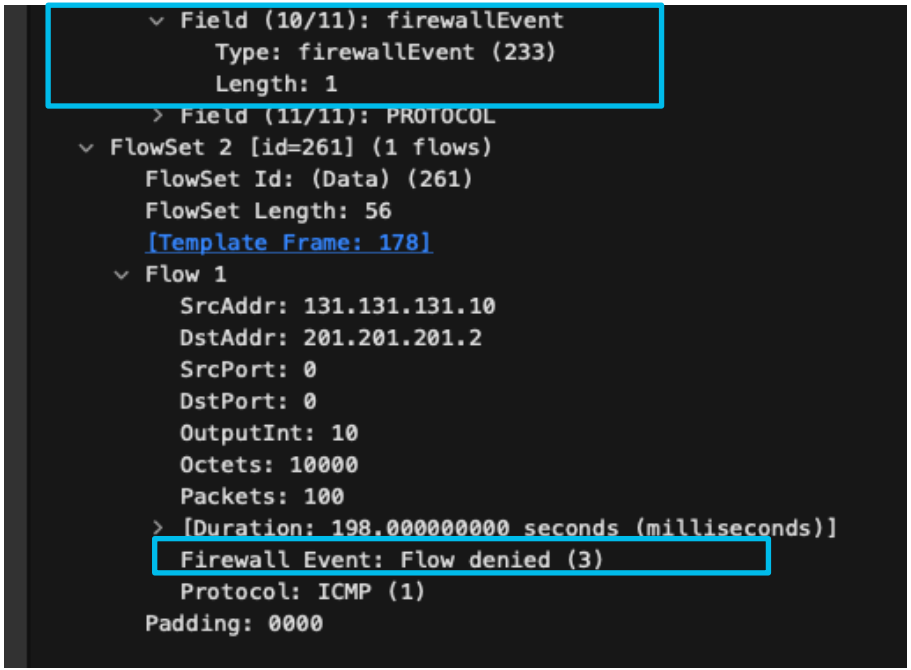
	No Traffic
	Allowed Traffic
	Denied Traffic
	Traffic with Custom Policy
	Policy Analysis Pending
	Policy Disabled
	Policy Enabled
	Policy Monitor Mode
	Possible Policy Violation
	Unknown

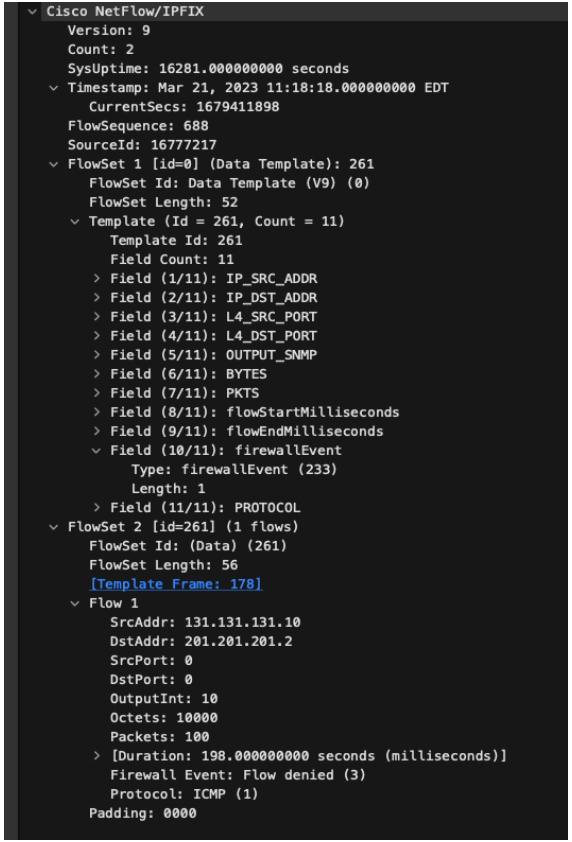


cisco Live!

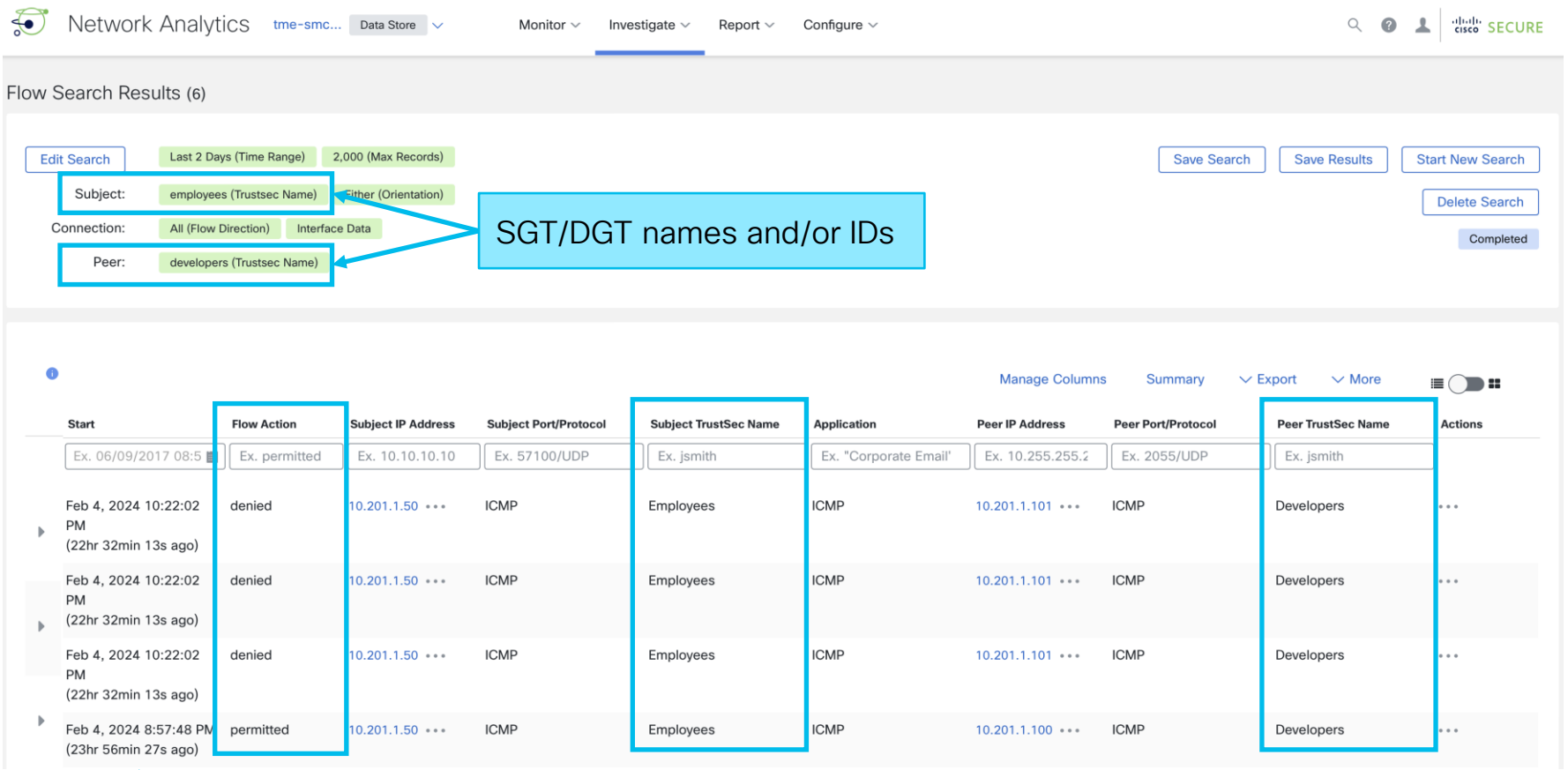
Flexible NetFlow Record for SGACL Permit and Deny

- 17.13.1 NetFlow Record for SGACL Deny





SNA: Flow Search based on SGTs (NetSecOps)



SGACL Logging – Open Telemetry

- 16.3 Initial support in C9k
- 17.3 Performance optimization for CPU protection

*Jan 27 13:33:43.355: %RBM-6-SGACLHIT: ingress_interface='GigabitEthernet1/0/24' sgacl_name='DenyIP_Log-01' action='Deny' protocol='tcp' src-vrf='default' src-ip='10.10.18.101' src-port='64382' dest-vrf='default' dest-ip='10.10.35.201' dest-port='80' sgt='4' dgt='4' logging_interval_hits='1'


```
{
      "logginghits" => "1",
         "protocol" => "tcp",
           "action" => "Permit",
           "srcvrf" => "default",
          "srcport" => "80",
         "destport" => "62700",
     "srcinterface" => "TenGigabitEthernet1/1/8",
        "timestamp" => "Jan 27 12:48:26.756",
            "sgacl" => "emp_dev_deny_log_copy-01",
              "sgt" => "4",
           "reason" => "%RBM-6-SGACLHIT",
      "received_at" => "2019-01-27T04:46:25.134Z",
          "message" => "<190>123319: Jan 27 12:48:26.756: %RBM-6-SGACLHIT: ingress_interface='TenGigabitEthernet1/1/8' s
gacl_name='emp_dev_deny_log_copy-01' action='Permit' protocol='tcp' src-vrf='default' src-ip='10.10.35.101' src-port='80
' dest-vrf='default' dest-ip='10.201.2.104' dest-port='62700' sgt='4' dgt='8' logging_interval_hits='1'",
    "received_from" => "10.99.100.1",
            "dstip" => "10.201.2.104",
             "host" => "10.99.100.1",
         "destvrf" => "default",
             "type" => "syslog",
         "@version" => "1",
       "@timestamp" => 2019-01-27T04:46:25.134Z,
              "dgt" => "8",
            "srcip" => "10.10.35.101"
}
```

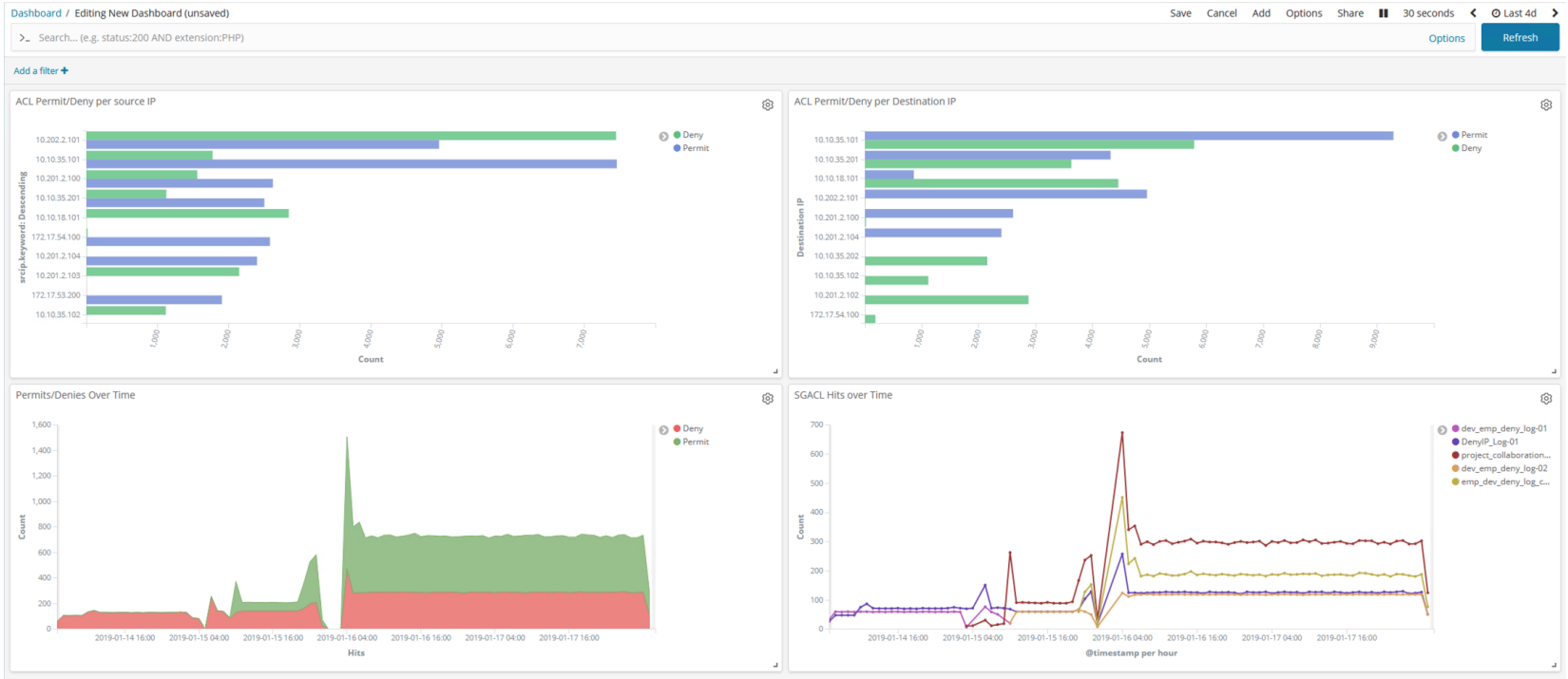
SGT/DGT Hit Counters via Open Telemetry

- NCC – open source NETCONF Client tools
  - https://github.com/CiscoDevNet/ncc
  - ./ncc-establish-subscription.py --host=172.23.41.129 -u cisco -p nbv_1234 -x /trustsec-state --period 50 --callback sample > trustsec-state.txt

```
Subscription Result : notif-bis:ok
Subscription Id     : 2147483648
-->>
Event time      : 2019-01-27 22:26:46.910000+00:00
Subscription Id : 2147483648
Type            : 1
Data            :
{
  "datastore-contents-xml": {
    "trustsec-state": {
      "cts-rolebased-policies": {
        "cts-rolebased-policy": [
```

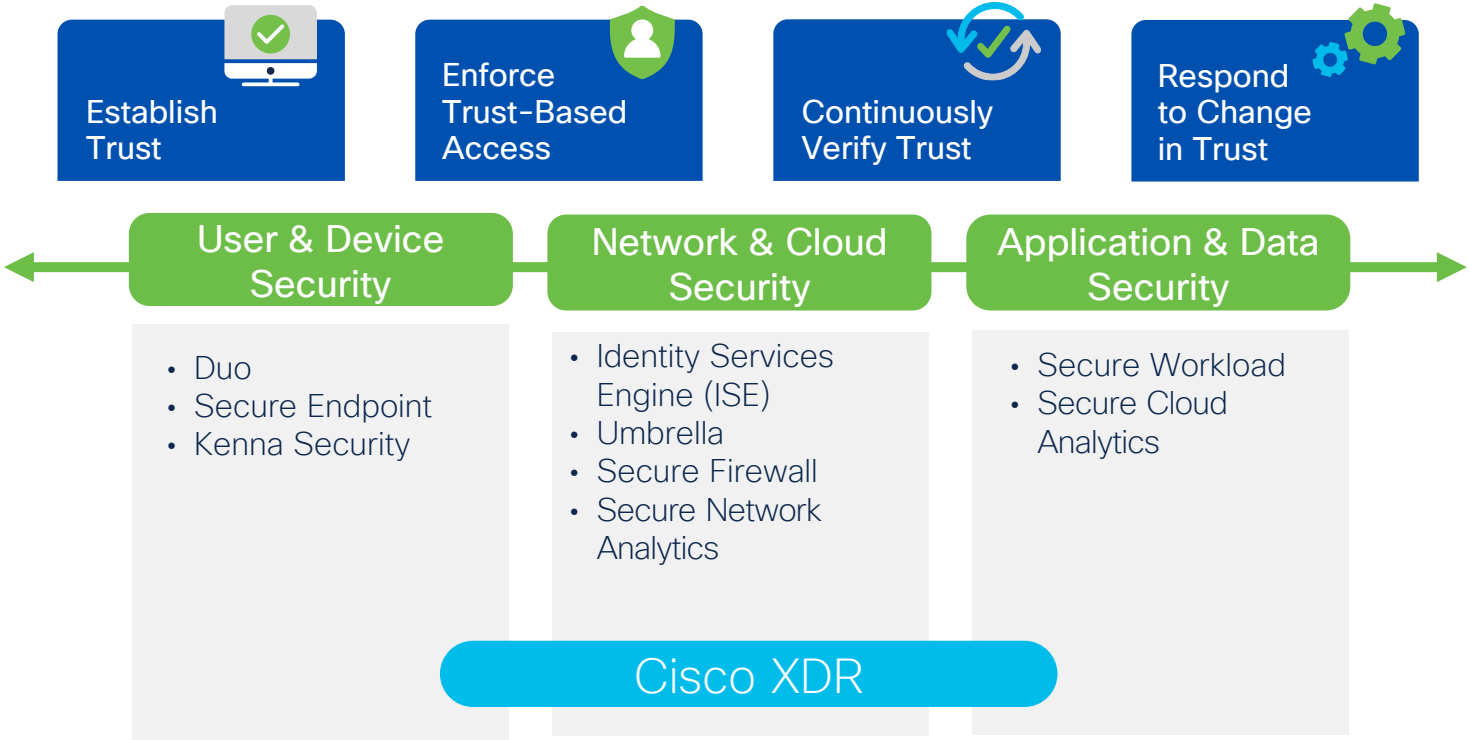
```
{
            "dst-sgt": "4",
            "hardware-deny-count": "145",
            "hardware-monitor-count": "0",
            "hardware-permit-count": "0",
            "last-updated-time": "1548631492542928",
            "monitor-mode": "false",
            "num-of-sgacl": "1",
            "policy-life-time": "86400",
            "sgacl-name": "dev_emp_deny_log-02;",
            "software-deny-count": "0",
            "software-monitor-count": "0",
            "software-permit-count": "0",
            "src-sgt": "8",
            "total-deny-count": "145",
            "total-permit-count": "0"
          },
```

Open Telemetry Example – SGACL Monitoring



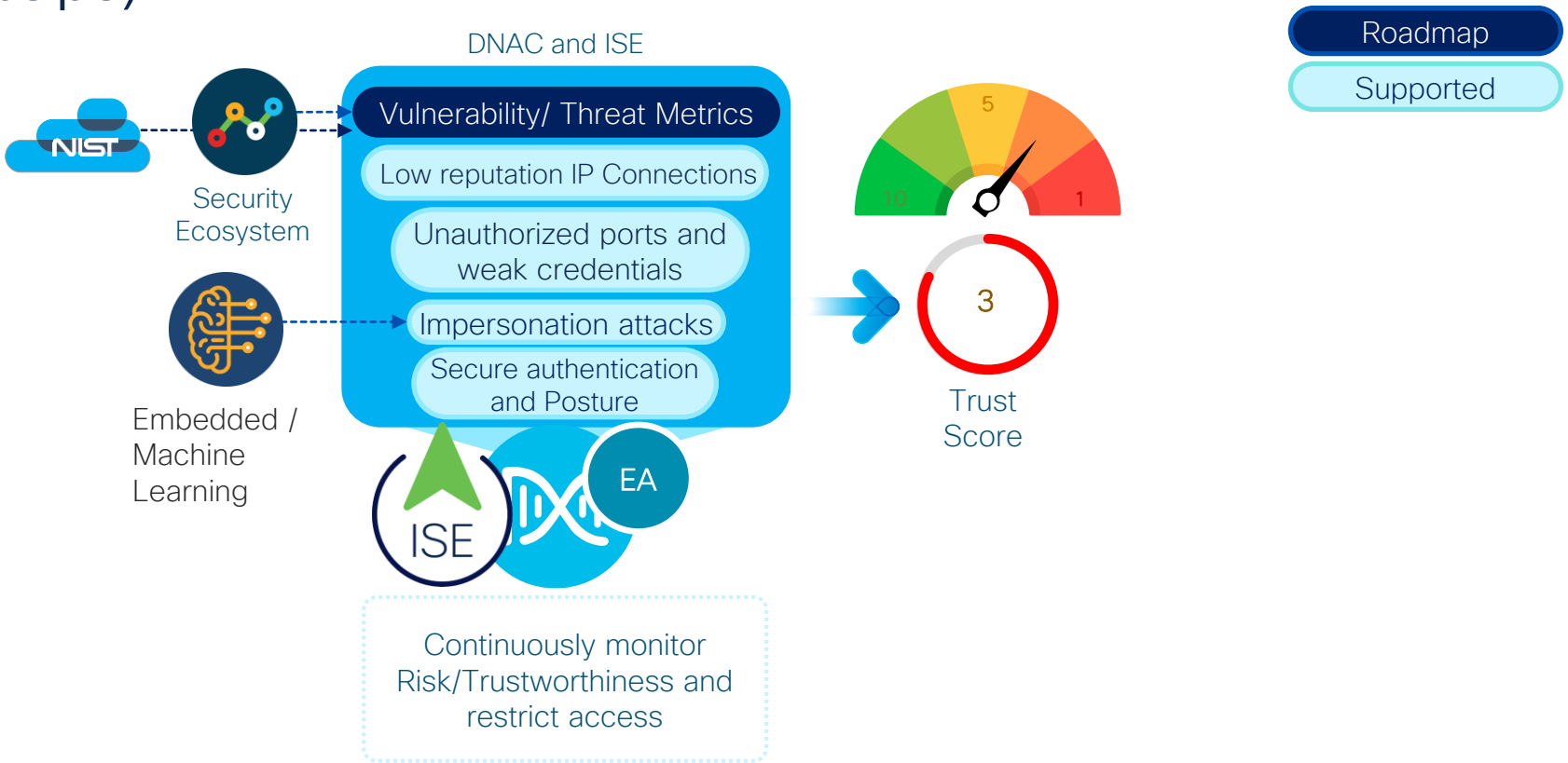
Continuously Verify

Sharing signals across all control points



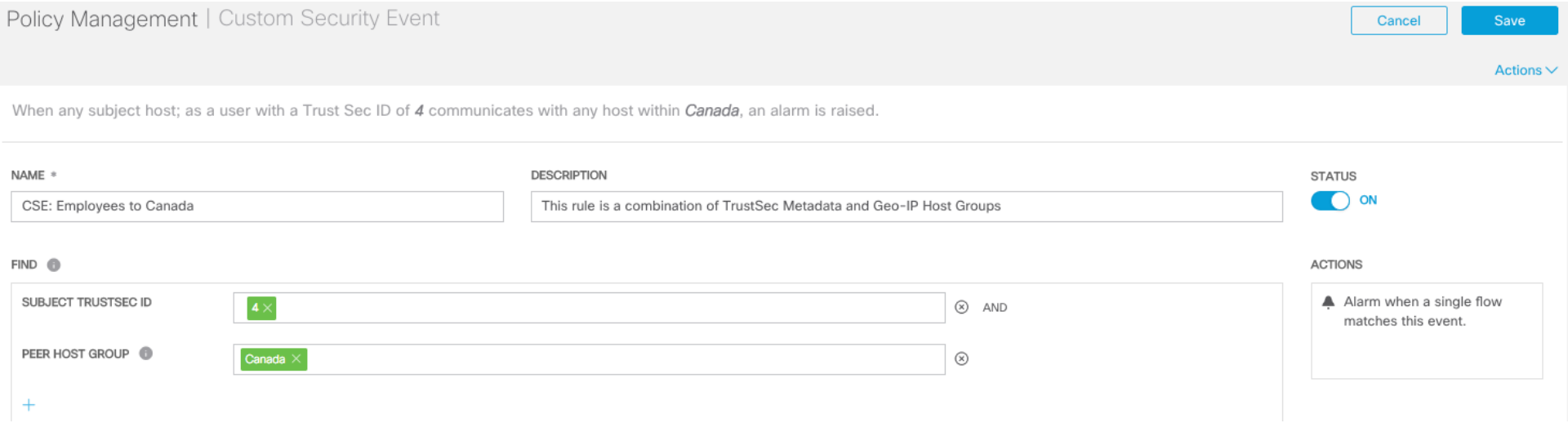
Enforce zero trust policies across the broadest set of control points

DNAC Trust Analytics: Continuous validation of endpoints (NetOps)



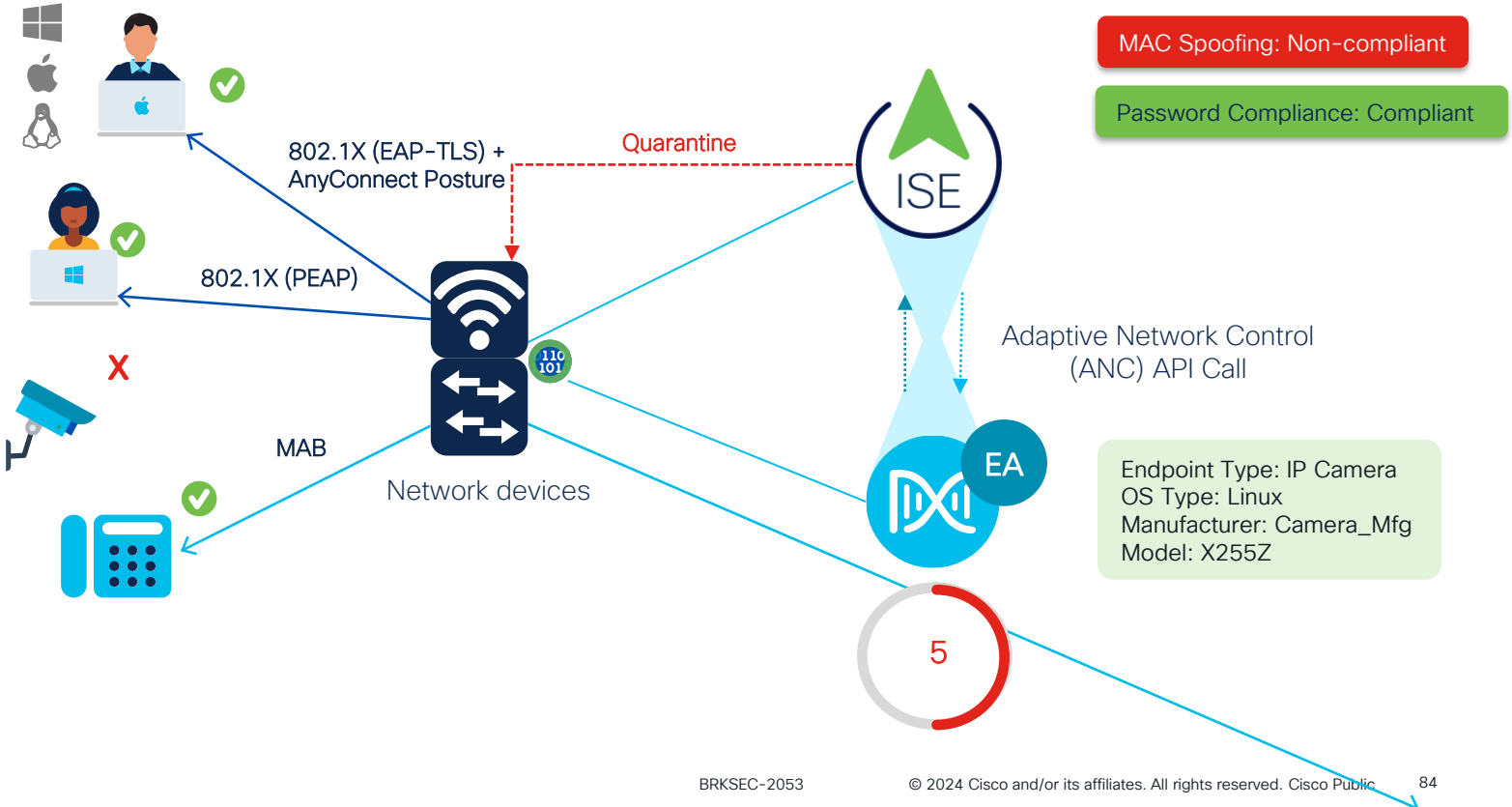
Secure Network Analytics (SNA) (NetSecOps)

Custom Security Event (CSE) using TrustSec (SGT) and Geo-IP Attributes

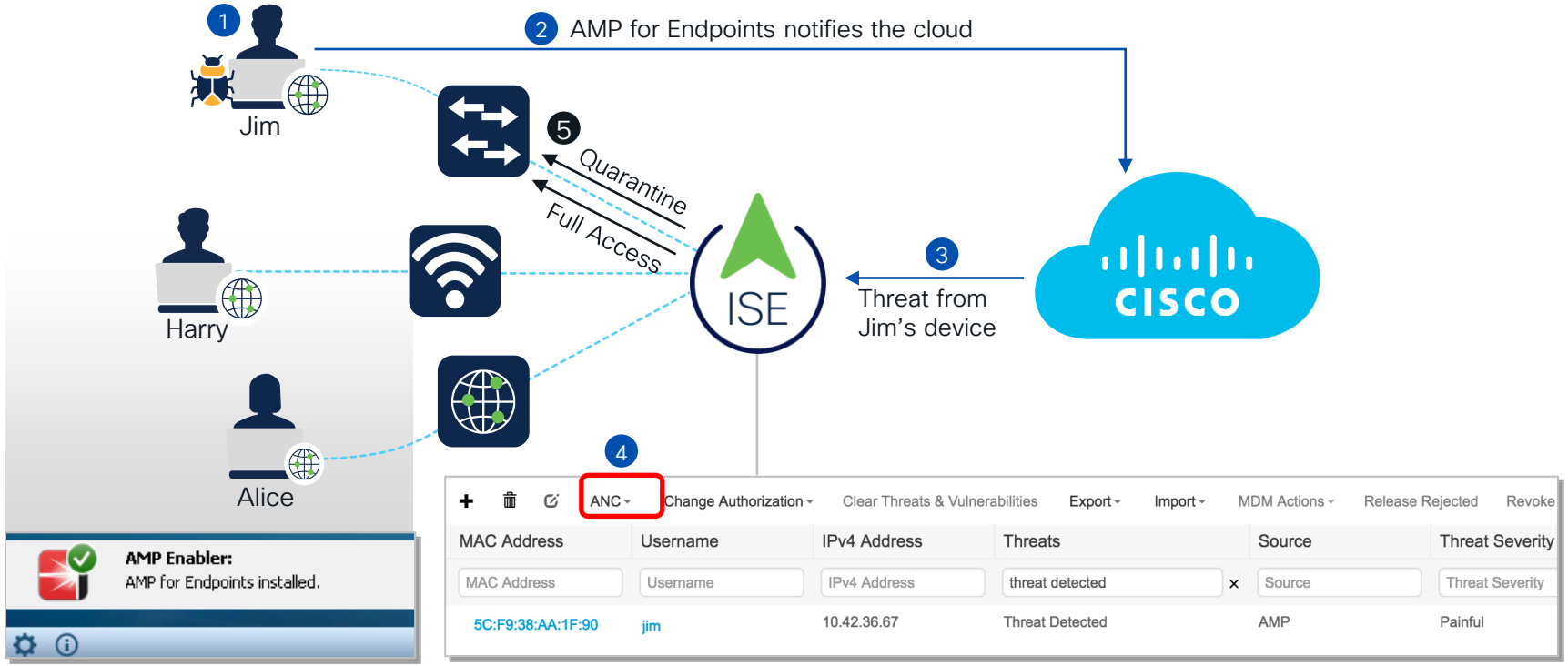


Respond to Trust

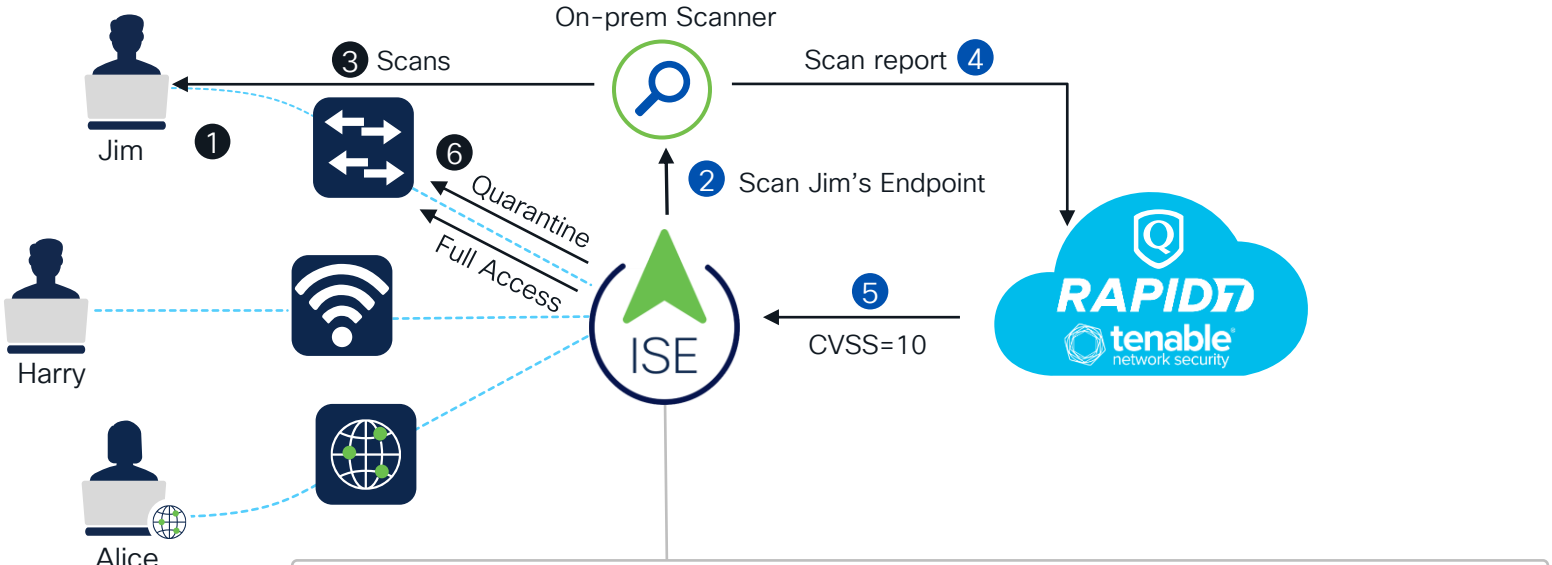
Endpoint Analytics: Trust Score after MAB



Threat Visibility Rapid Threat Containment (RTC)



Vulnerability Assessment (Threat-Centric NAC)



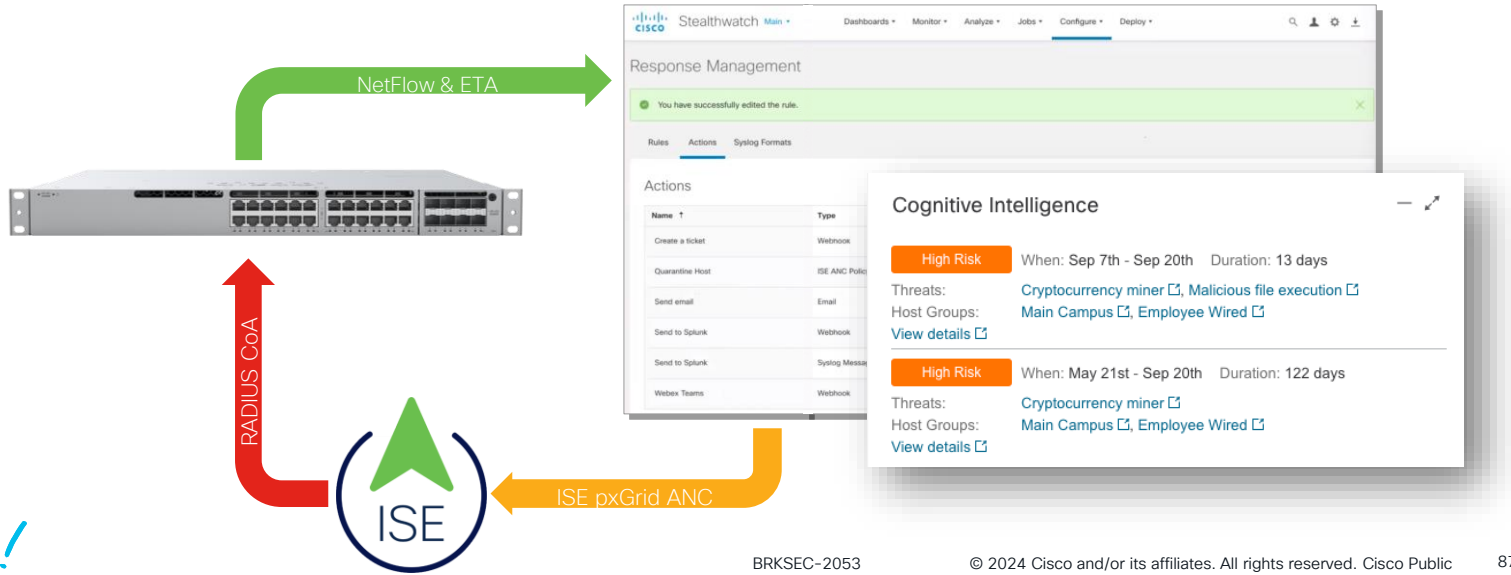
CVSS: Common Vulnerability Scoring System

Threat Detection and Response

Telemetry provided by **network devices** to Secure Network Analytics (SNA)

Flexible outcomes: Policy Violation

Trigger **CoA** via ISE



Response via API

Adaptive Network Control (ANC)

External RESTful Services (ERS) Online SDK

- Quick Reference
- API Documentation
  - ISE 3.3 Release Notes
  - ANC Endpoint
  - ANC Policy
  - Aci Bindings
  - Aci Settings
  - Active Directory
  - Admin User
  - Advanced Customization Global Set
  - Allowed Protocols
  - Authorization Profile
  - BYOD Portal
  - Certificate Template
  - CertificateProfile
  - Clear Threats and vulnerabilities
  - Downloadable ACL
  - Egress Matrix Cell
  - End Point
  - End Point Certificates
  - EndPoints Identity Group
  - External Radius Server
  - Filter Policy
  - Guest Location
  - Guest Smtp Notification Configurati
  - Guest Ssid
  - Guest Type
  - Guest User
  - Hotspot Portal
  - IP To SGT Mapping
  - IP To SGT Mapping Group
  - ISE Service Information
  - Identity Group
  - Identity Sequence
  - Internal User
  - Ldap
  - My Device Portal
  - Native Supplicant Profile
  - Network Device
  - Network Device Group
  - Node Details
  - PSN Node Details with Radius Servi
  - Portal
  - Portal Theme
  - Profiler Profile

ANC Endpoint

Overview

Adaptive Network Control (ANC) provides the ability to create network endpoint authorization controls based on ANC policies.

Please note that these examples are not meant to be used as is because they have references to DB data.
You should treat it as a basic template and edit it before sending to server.

Resource definition

Attribute	Type	Required	Default value	Description
name	String	Yes		Resource name
id	String	No		Resource UUID, mandatory for update
description	String	No		
macAddress	String	Yes		MAC address of the endpoint
policyName	String	Yes		Policy name for applying to the endpoint

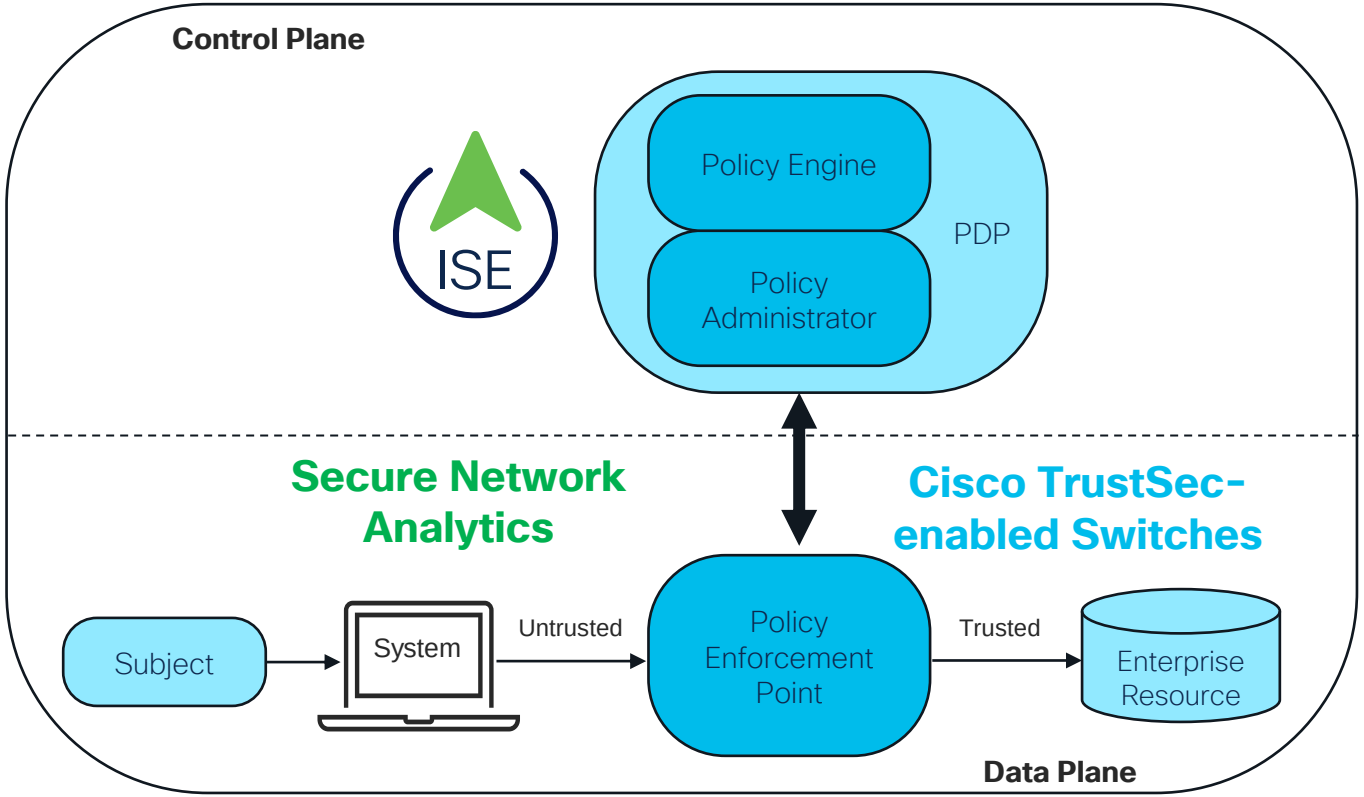
XML example:

```
1. XML
2. <?xml version="1.0" encoding="UTF-8"?>
3. <ns0:ancendpoint xmlns:ns0="anc.ers.ise.cisco.com" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com">
4.    <macAddress>00:11:22:33:44:55</macAddress>
5.    <policyName>policy1</policyName>
6. </ns0:ancendpoint>
7.
8. JSON
9. {
10.   "ErsAncEndpoint" : {
11.     "macAddress" : "00:11:22:33:44:55",
12.     "policyName" : "policy1"
13.   }
14. }
```

Implementation of a ZTA

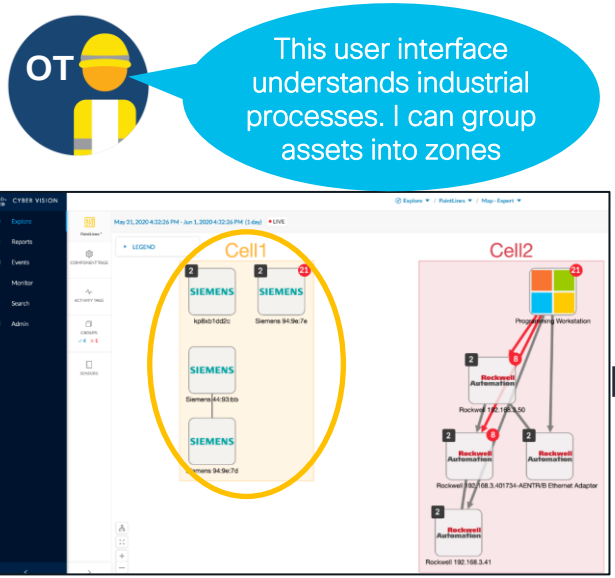
NIST Zero Trust Architecture SP 800-207

Implementing a ZTA using TrustSec-based Micro-segmentation

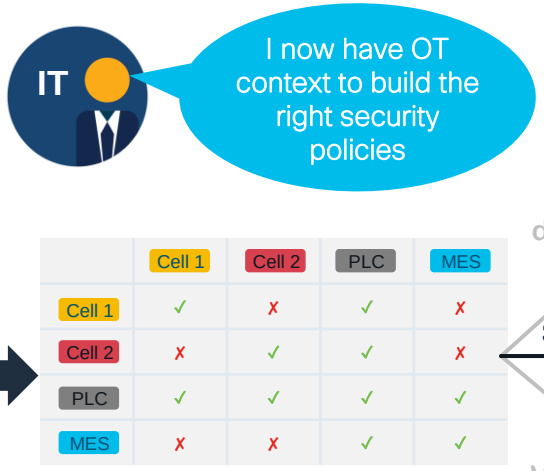


Optimal Segmentation in OT environments

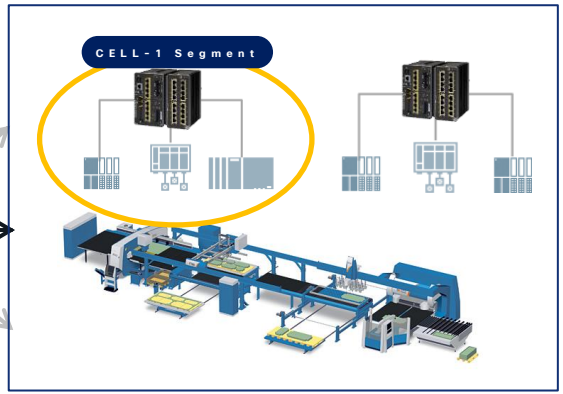
Aligned to NIST Zero Trust Architecture



Cyber Vision Map View

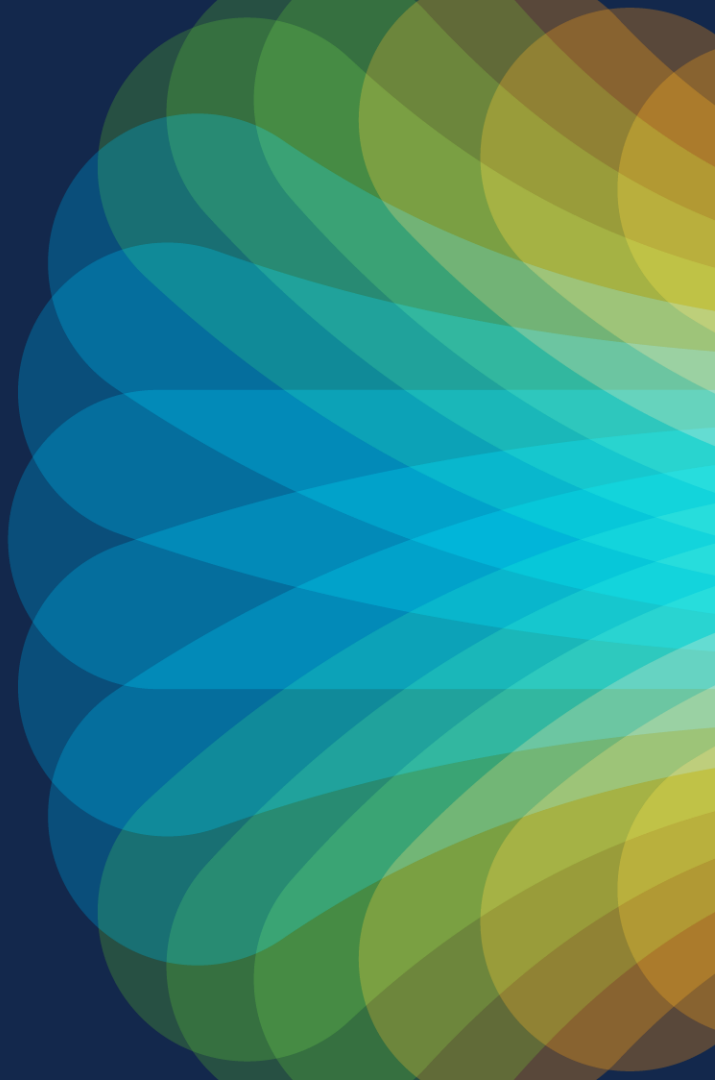


ISE



Dynamic segmentation of industrial network

Summary

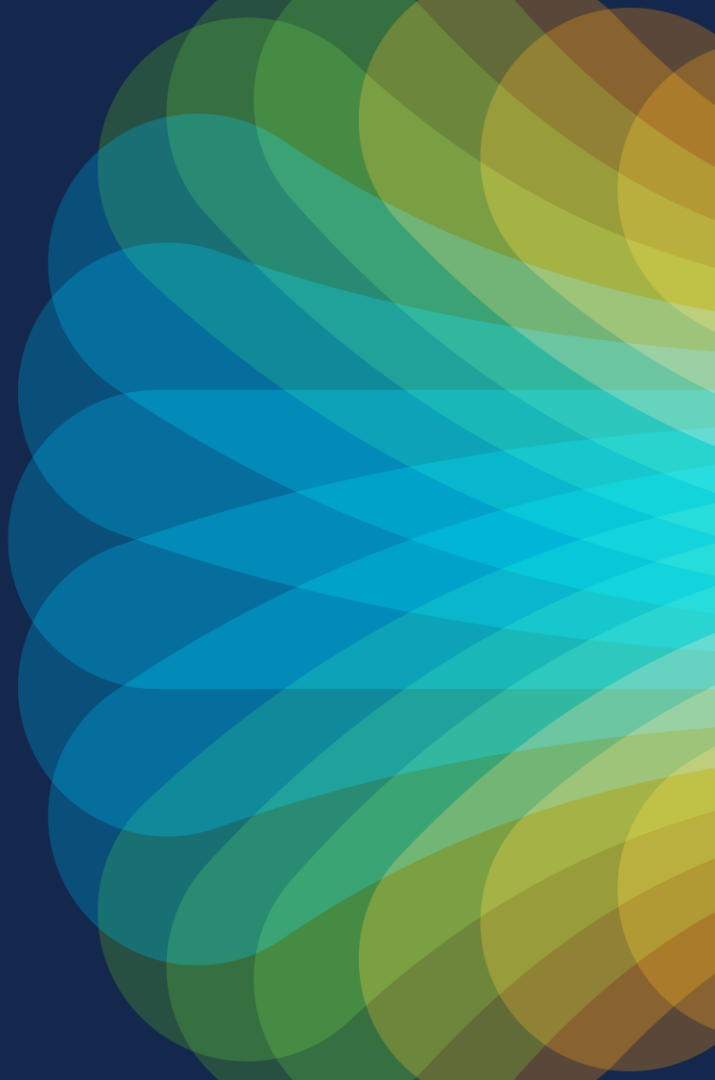


Summary

- Cisco's Zero Trust Architecture is a comprehensive approach to securing all access across your network, applications, and environment
- Cisco Zero Trust Architecture provides a scalable layered approach to Zero Trust that allows it to evolve with the customers needs
- As use cases evolve for Zero Trust, Cisco is innovating with products to provide least privilege access with Cisco Zero Trust for the workplace
- Cisco Zero Trust for the Workplace – provides unrivaled visibility, segmentation and containment

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go