Zero Trust Workplace with Cisco DNA

Santa Monica Networks Security Day

Taras Dmytriv
Systems Engineer
November 2022

Taras Dmytriv

- Helping customers to transform their network infrastructure with Cisco Solutions
- Background in Advanced Services and Customer Success roles
- Coffee, sci-fi, and eSports enthusiast

Helsinki, Finland

Session Objective

- Inform
- Educate
- Inspire

Agenda

1. Cisco Digital Network Architecture
2. Cisco Continuous Trust Overview
3. Cisco Segmented Access Overview

What is Cisco DNA?

Cisco Digital Network Architecture

Begins with 3 pillars for secure, agile networking

Software Defined and Systems Thinking

Cisco DNA Center

Digital-Ready Infrastructure

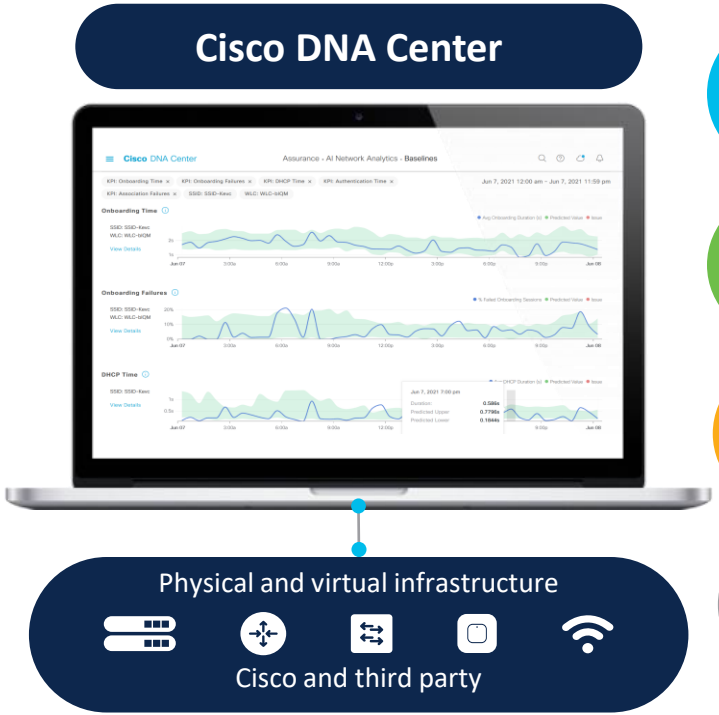
Catalyst 9000 Family

Catalyst 8000 Family

Zero Trust Security Model

Cisco DNA Center is a foundational platform technology

Command and control center for Cisco Catalyst



Automation

Automation and workflows simplify building and maintaining large scale networks. AI/MR streamlines and simplifies complex tasks

Analytics

AI/ML and insights to ensure the health, performance and reliability of applications and infrastructures

Security

AI/ML and DPI Identify and classify endpoints, enforce security policies and mitigate threats for a complete workplace zero trust solution

Programmability

Mature APIs, SDKs, and closed-loop integrations, untangle the complexities of interconnecting third party systems

Cisco Catalyst 9000 Family

Cisco Catalyst 9300 Series

Cisco Catalyst 9400 Series

Cisco Catalyst 9200 Series

Cisco Catalyst 9500 Series

Cisco Catalyst 9600 Series

Cisco Catalyst 9800 Series

Cisco Catalyst 9100 Series

Access switching

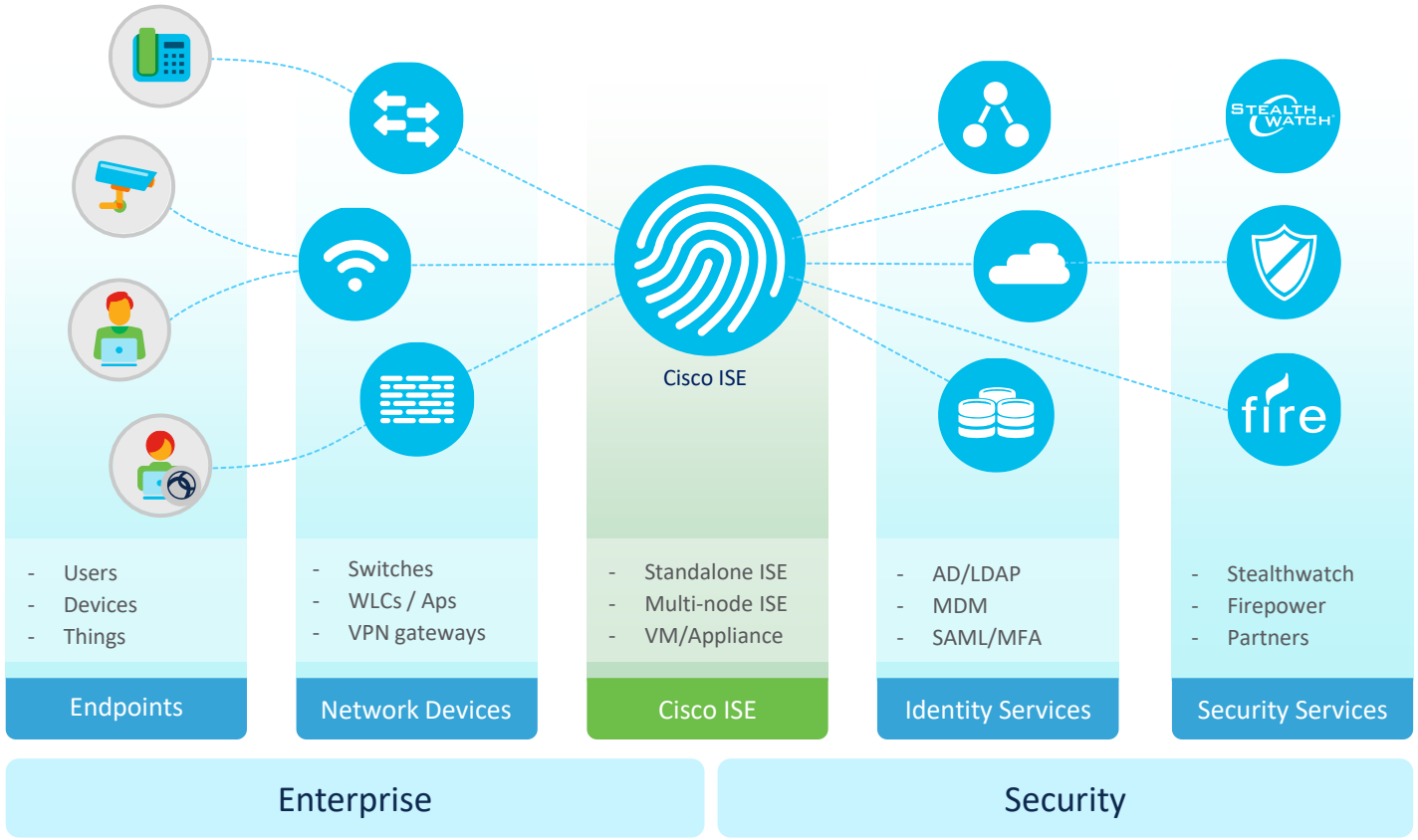
Core/Dist switching

Wireless

IOS-XE
Common Software Architecture

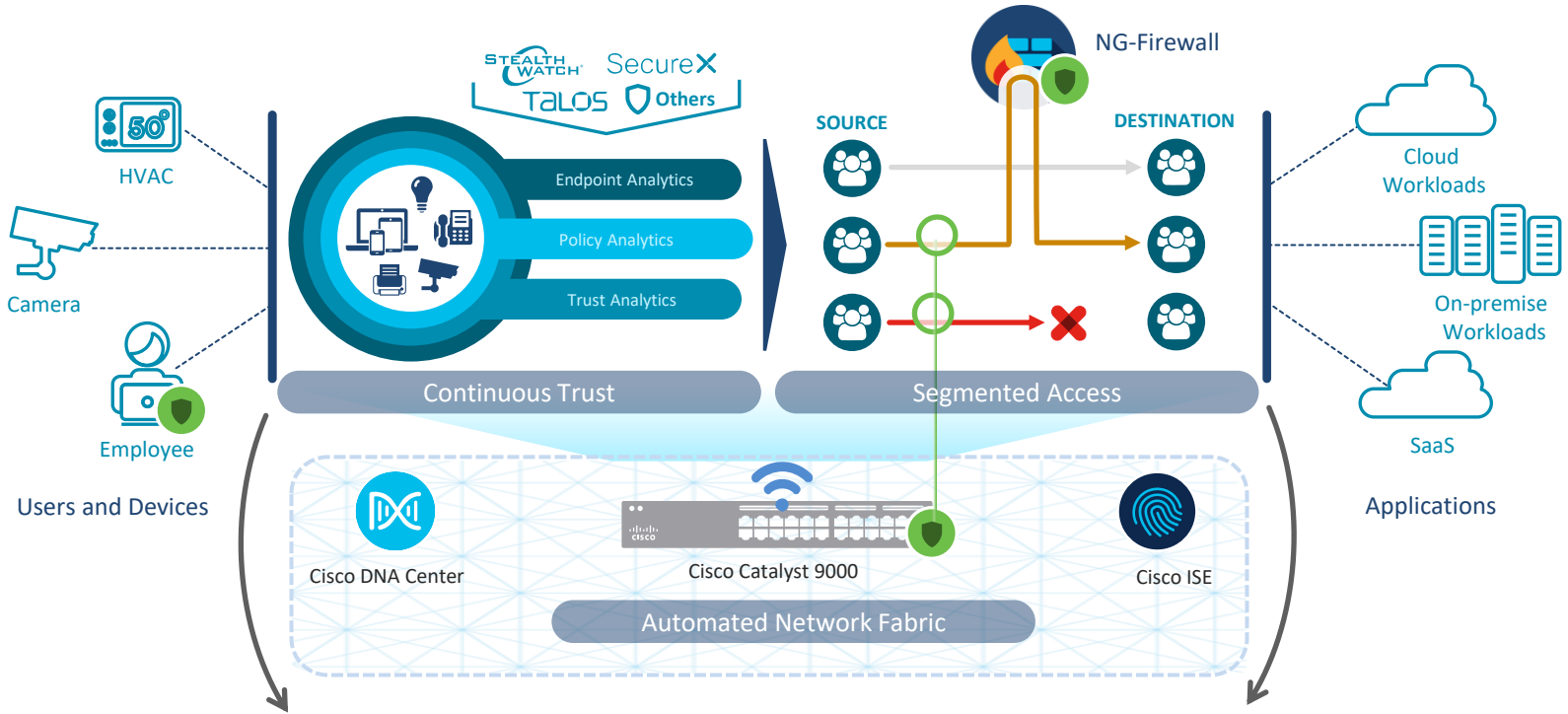
Programmable ASIC
Common Hardware Architecture

Identity with ISE is Secures the Enterprise



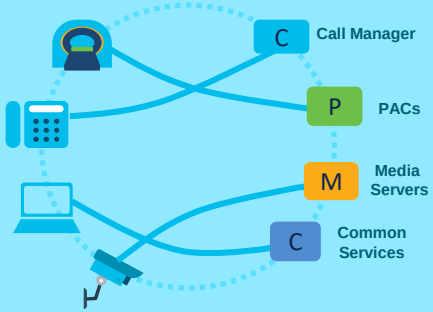
SD-Access Delivers Trusted Workplace

Leverage Network and ML to Scale Workplace Zero-Trust

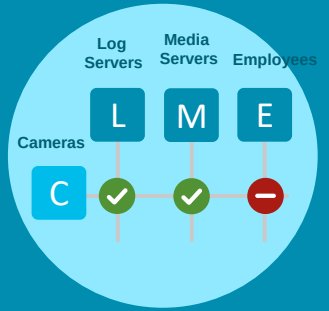


Continuous Trust

KNOW
Your
Endpoints



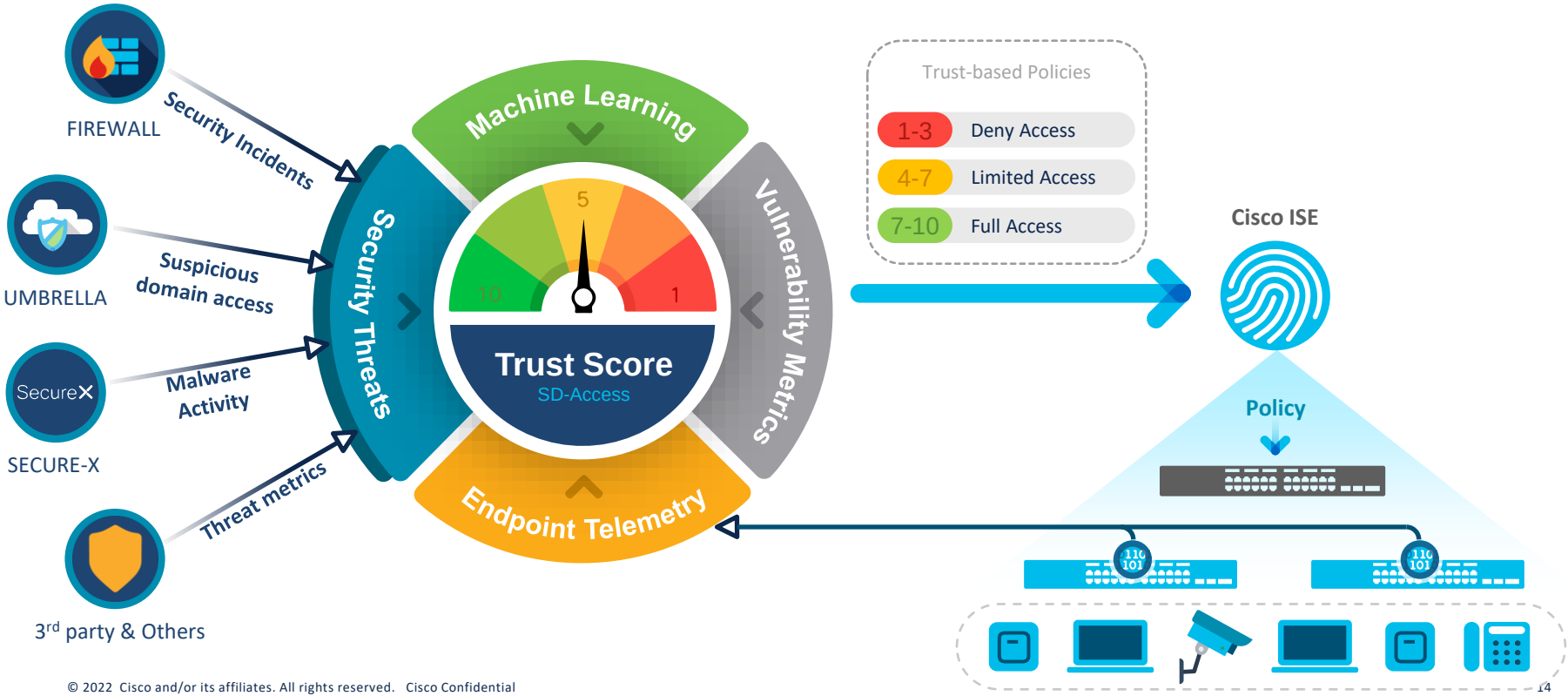
SEE
what they
talk to



DO/CREATE
the right
segmentation
policy

Workplace Zero-Trust manifested as Trust Score

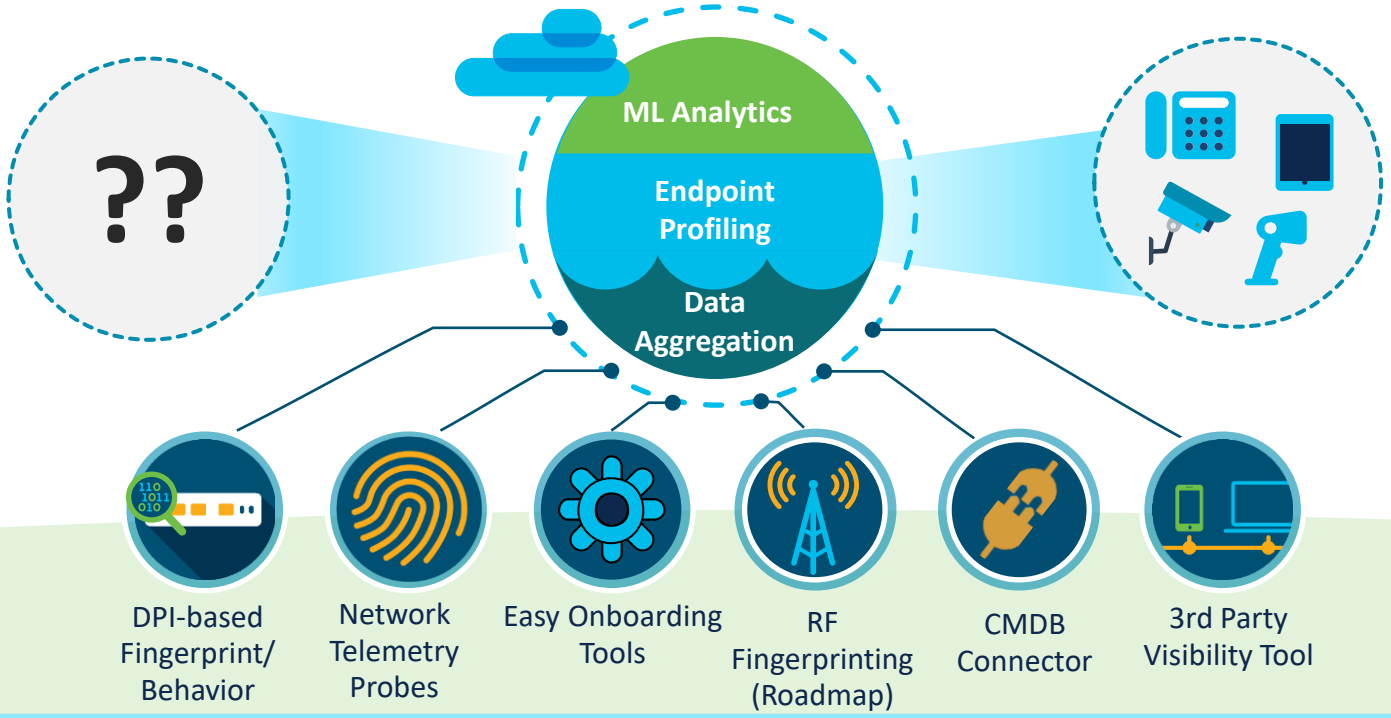
Automate Threat Response with Trust-based Policies



Endpoint Analytics

Endpoint Analytics on Cisco DNA Center

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



AI Endpoint Analytics: Multifactor classification

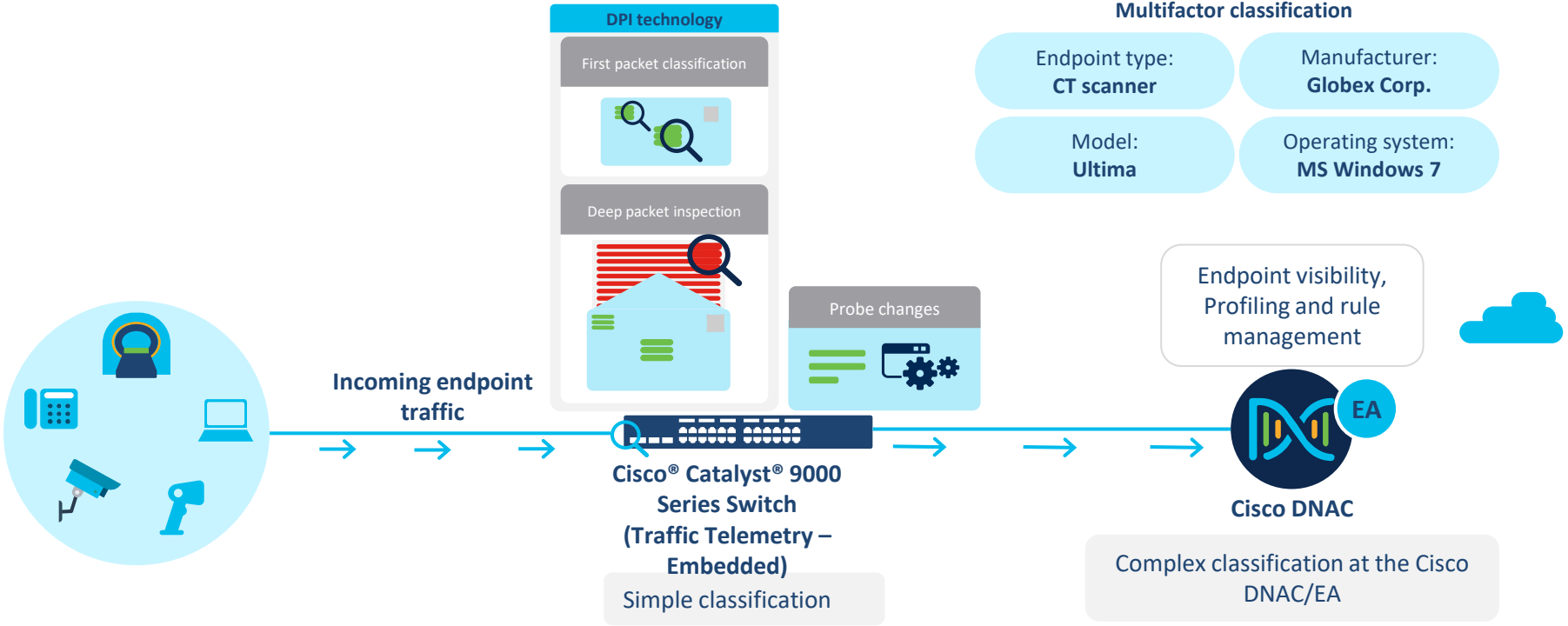
Classifying endpoints using four independent label categories for more flexible profiling

Device type	Hardware model	Hardware manufacturer	Operating system
Laptop	MacBook Pro	Apple	MacOS 10.14.6
CT scanner	Optima CT540	GE	CTT OS 6.3.x Linux
Smartphone	Galaxy S8	Samsung	Android 9.0

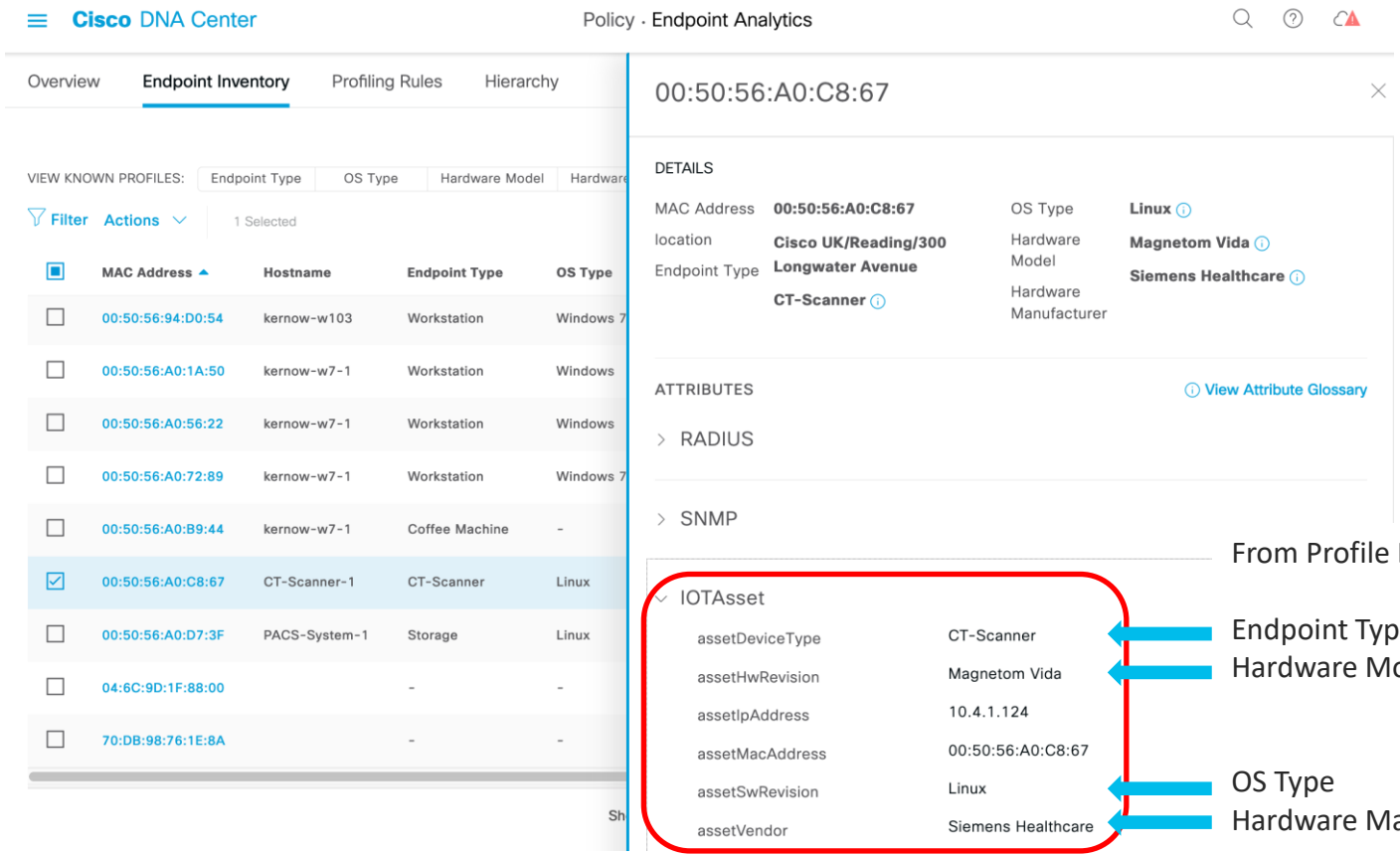
Cisco ISE probes and data sources

Unique Cisco ISE probes used in EA			
ISE and Third party	RADIUS	AD	MDM
AnyConnect	ACIDex		

EA Profiling using Embedded Traffic Telemetry



IOTAsset Attributes in Endpoint Analytics

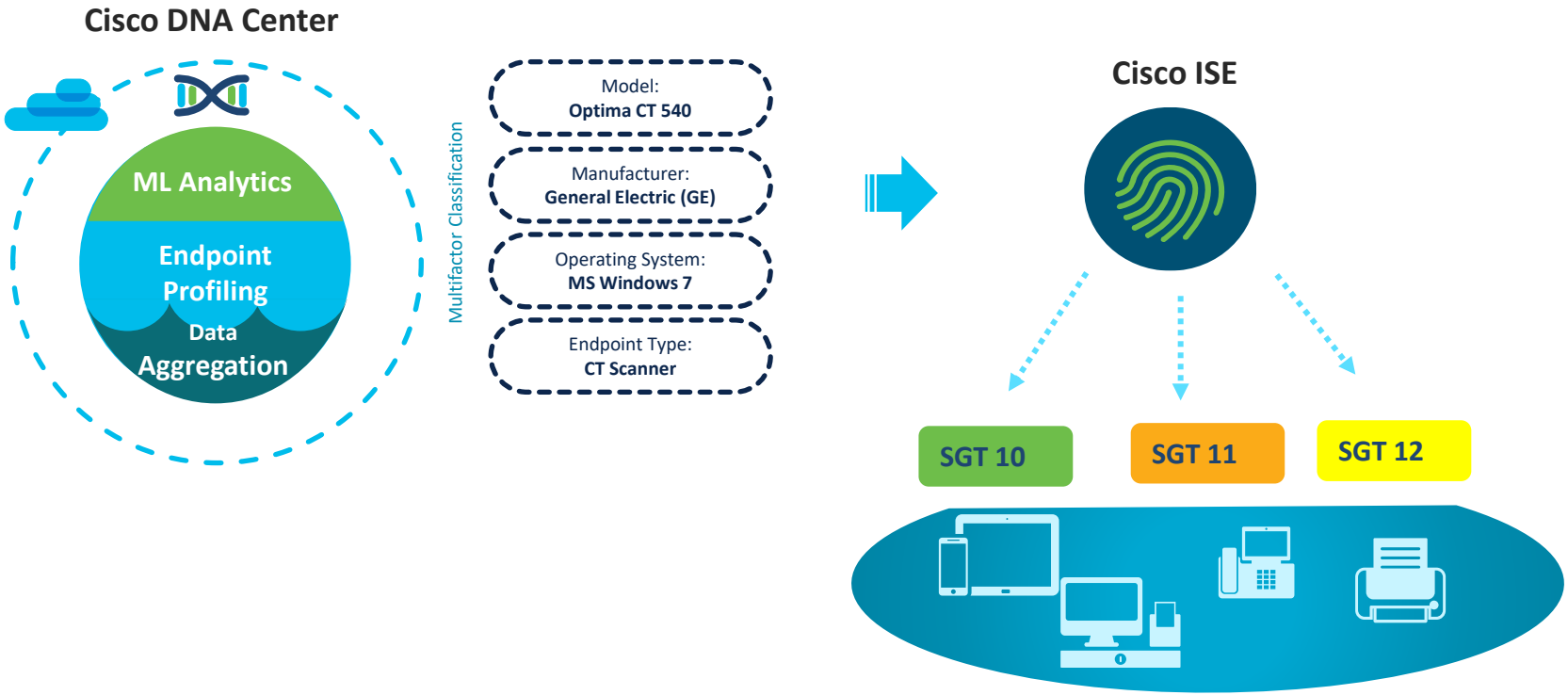


From Profile Label:

Endpoint Type
Hardware Model

OS Type
Hardware Manufacturer

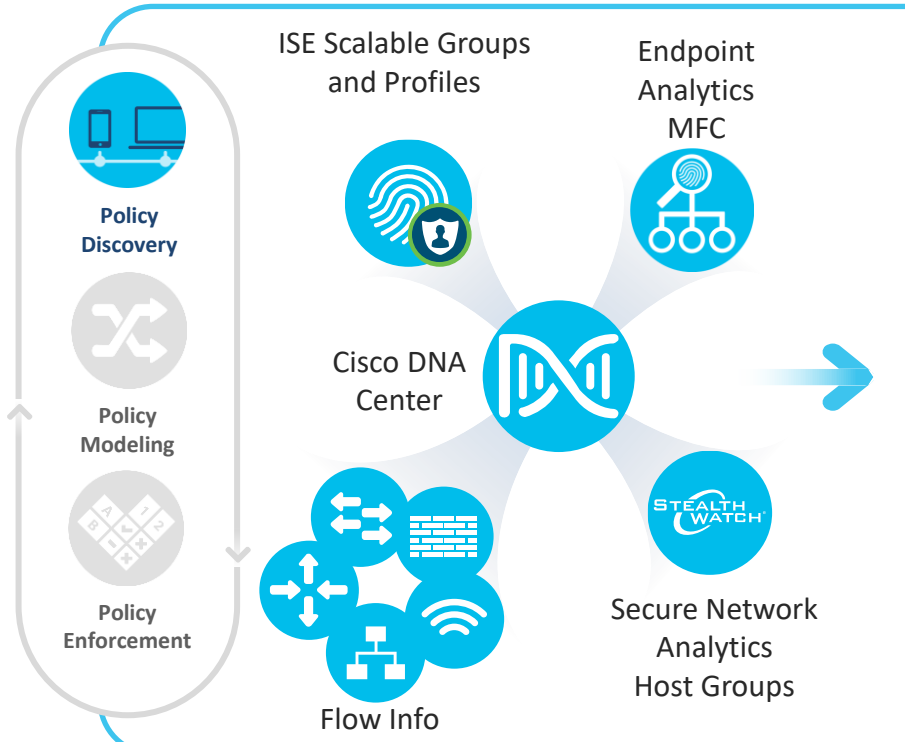
Better Classification reduces unauthorized access



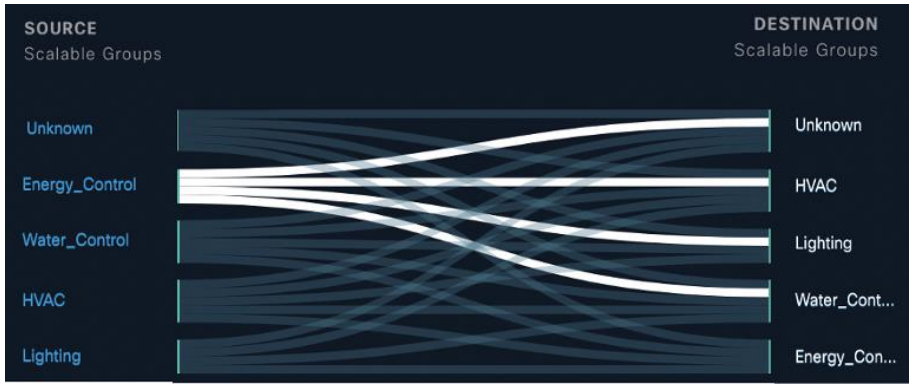
Policy Analytics

Group-Based Policy Analytics

Application on Cisco DNA Center: Turn policy on incrementally!

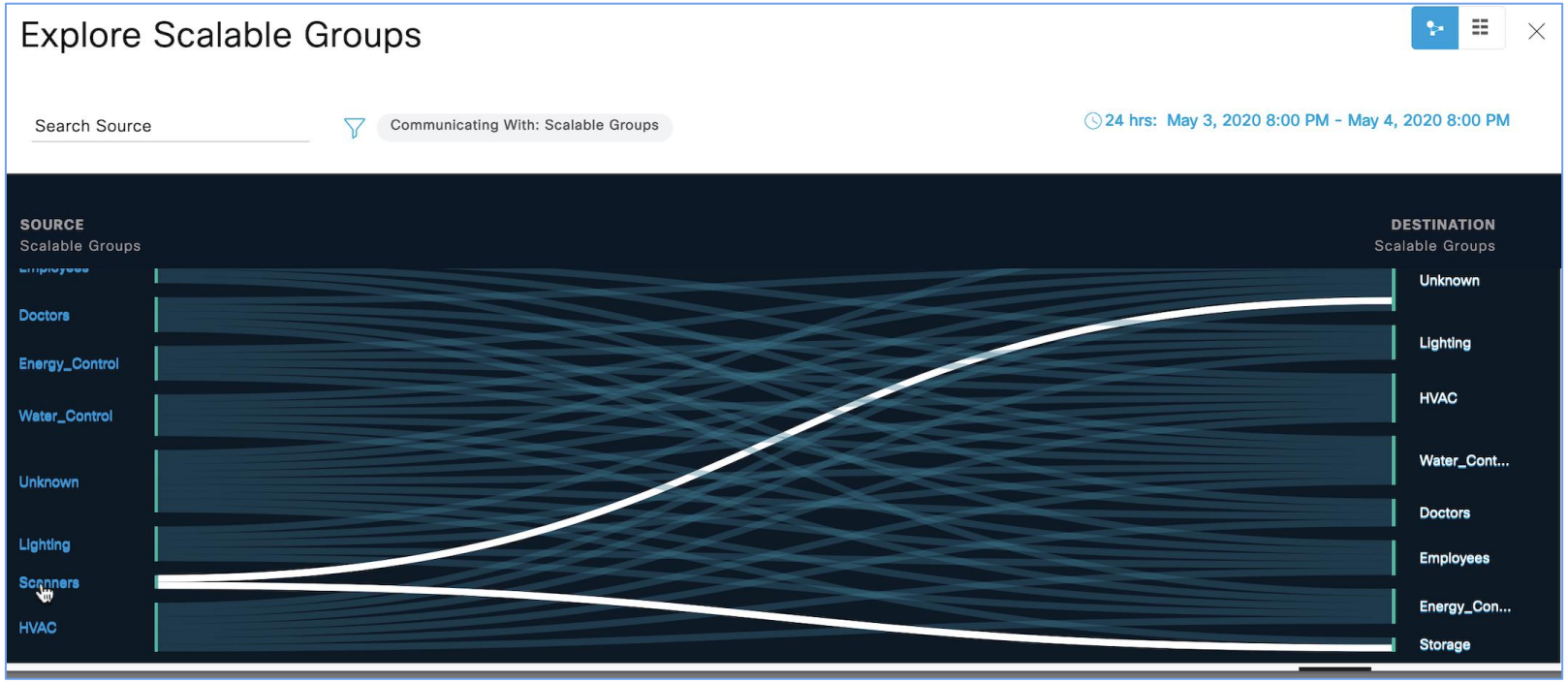


Group-Group Activity

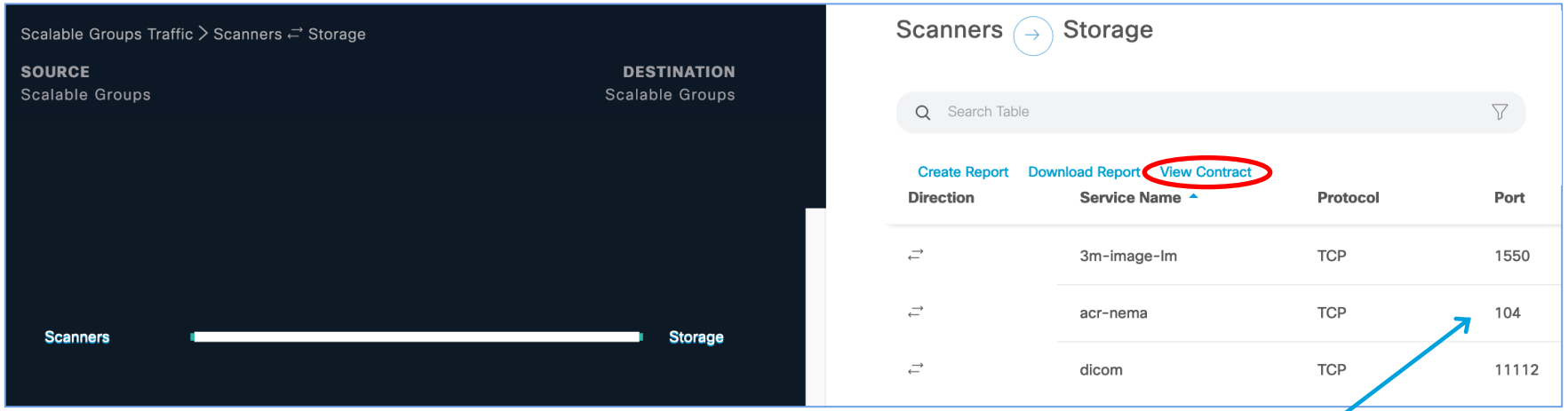


Direction	Service Name	Protocol	Port
⇄	3m-image-lm	TCP	1550
⇄	acr-nema	TCP	104
⇄	dicom	TCP	11112

Group to Group Activity



Detecting Ports/Protocols Between Groups

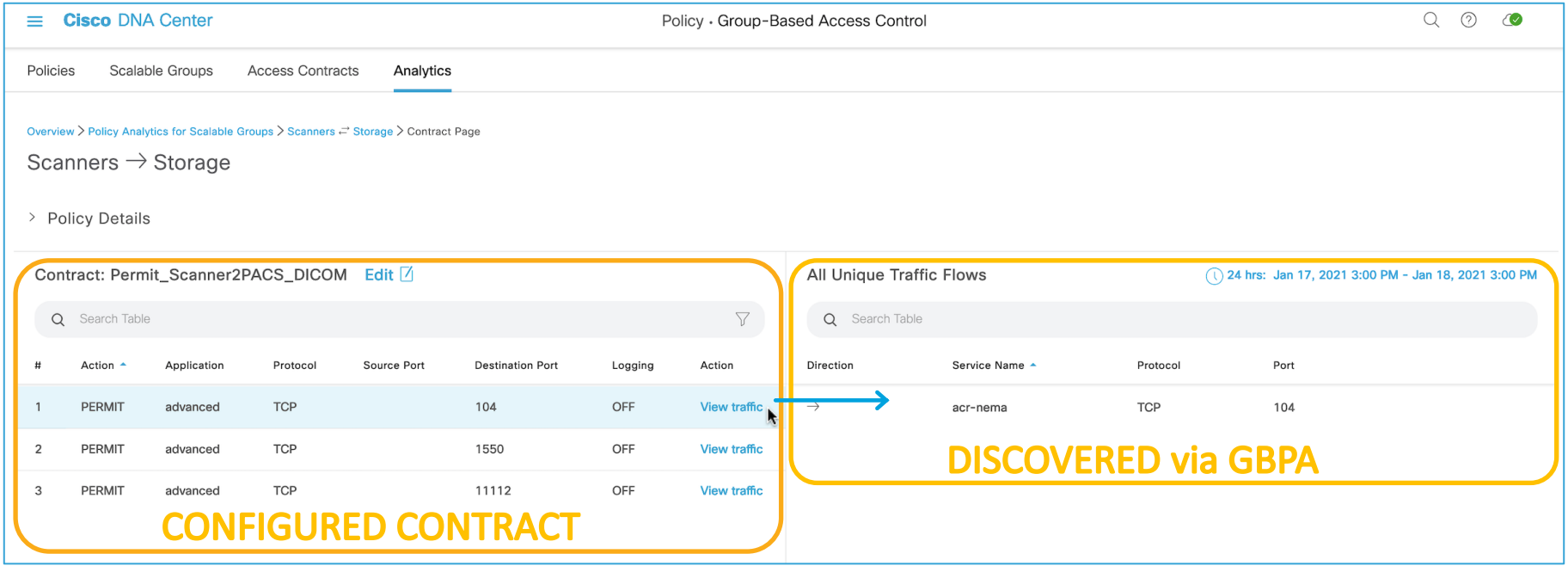


N.B. DICOM: Digital Imaging and Communications in Medicine

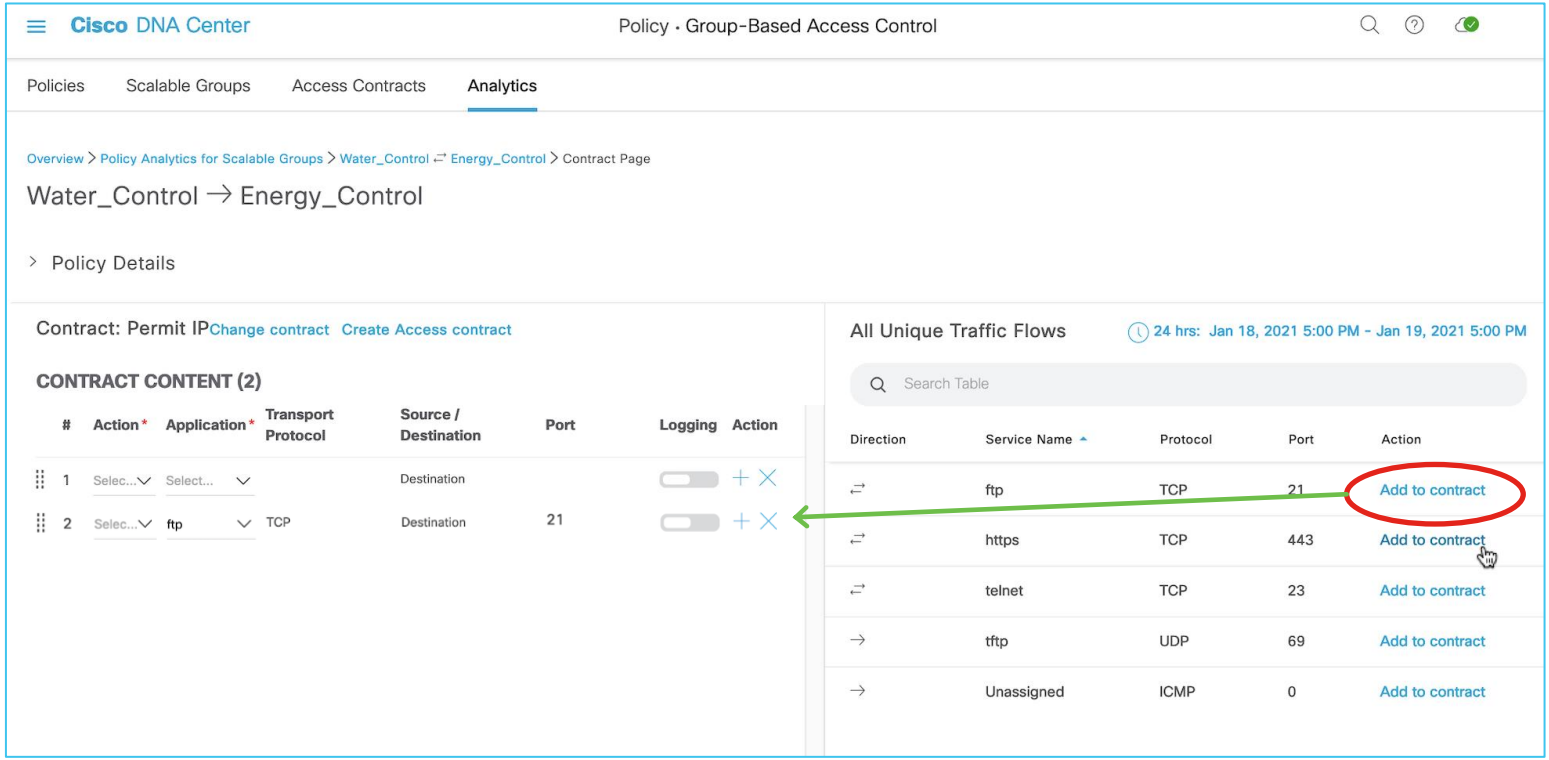
Ports 104, 1550 and 11112 detected between Scanners and Storage groups, all used for DICOM interaction

Identify the specific ports/protocols needed in access control policies

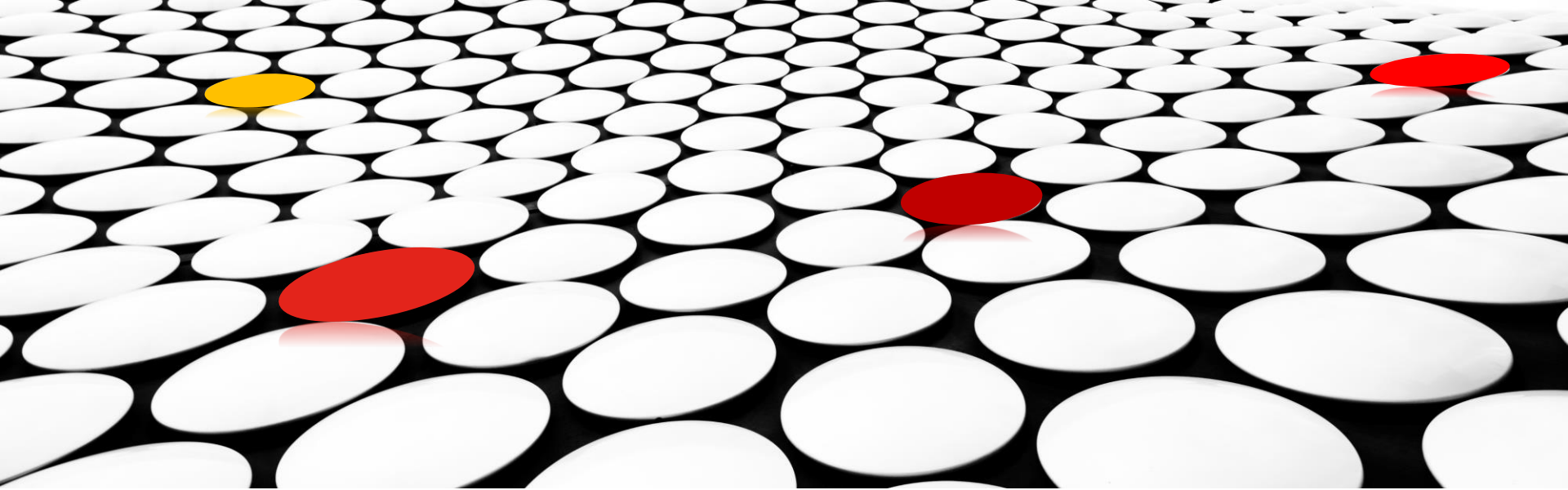
Contract and Discovered Information Side-by-Side
(GBPA App on Cisco DNA Center)



Create/Edit Contract Easily Based on Discovered Flows
(GBPA App on Cisco DNA Center)



Trust Analytics



Trust Analytics:

Continuous evaluation of endpoint behavior /anomalies to provide right level of access.

Trust context and impact on Trust score

Positive Influence

- Secure Authentication
- Posture Compliance

Negative Influence

- Suspicious behavior (Impersonation using MAC spoofing)
- Connections to Low reputation IP’s.
- Insecure interface (Unauthorized ports/weak credentials)

…

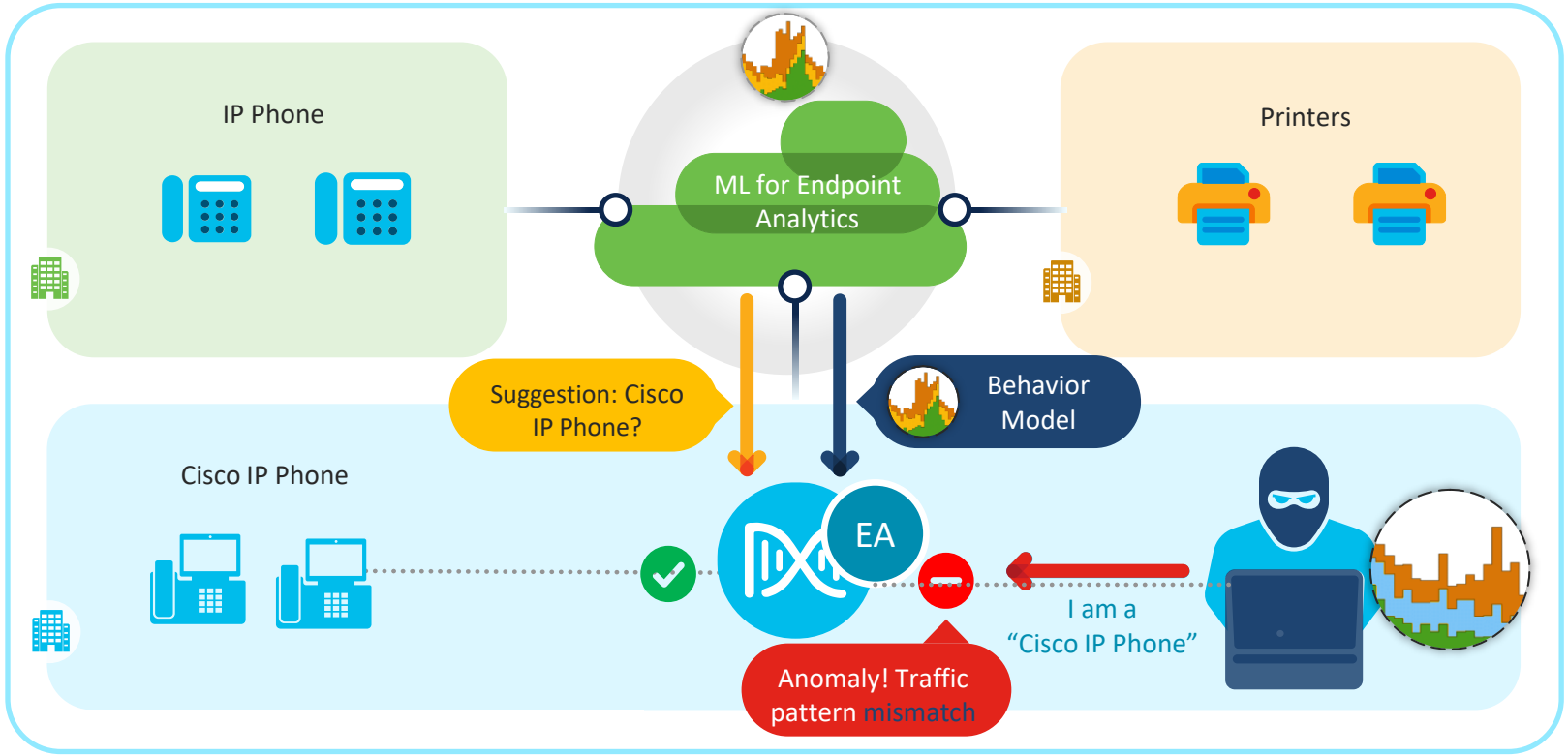
…

Access Control and Threat Containment based on continuous trust evaluation

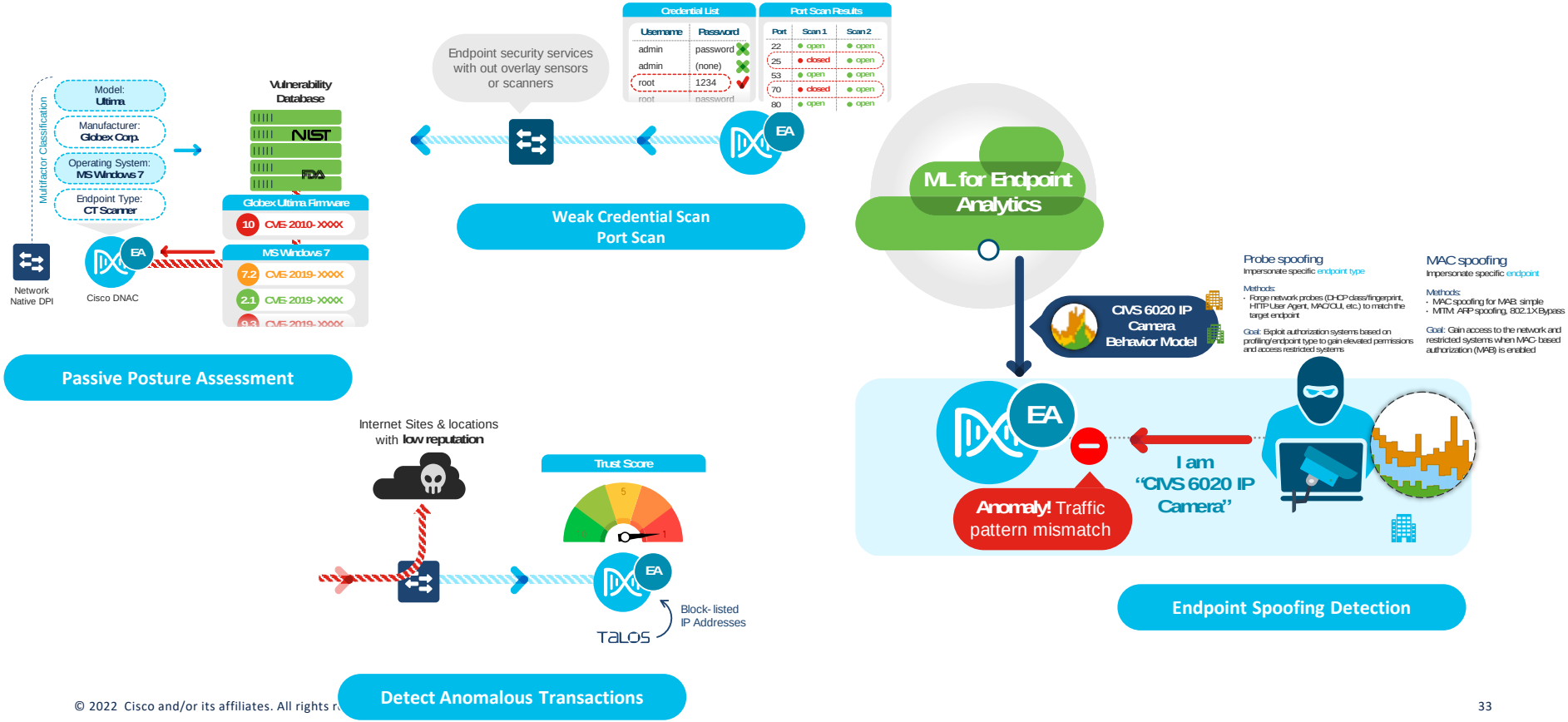
Trust-based Policies

1-3	Deny Access
4-7	Limited Access
7-10	Full Access

AI Spoofing Detection



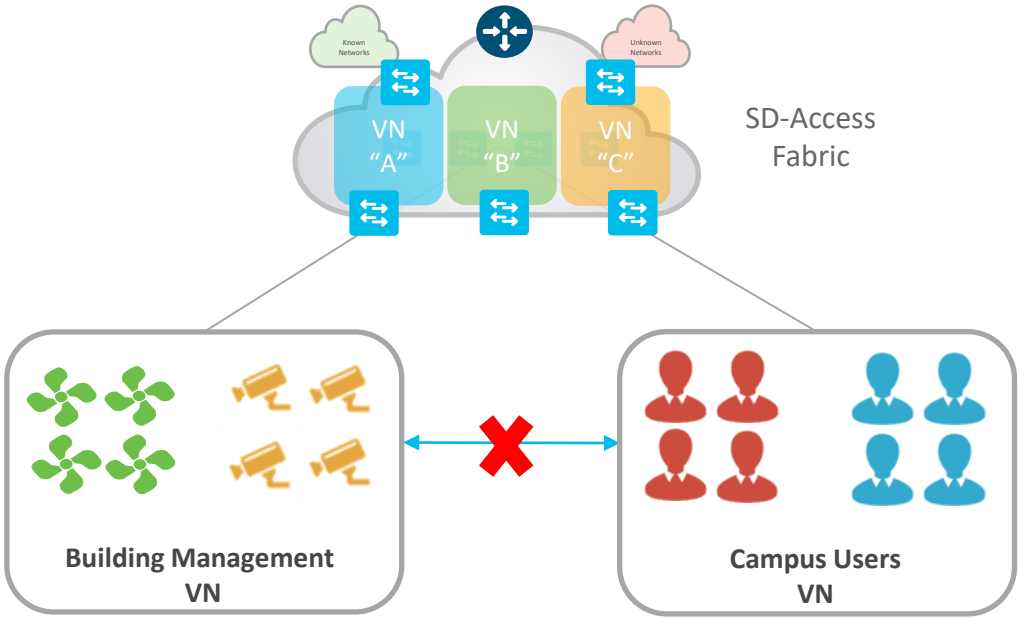
Verify Trust continuously for connected endpoints[1]



Segmented Access

SD-Access Segmentation

Two Level Hierarchy - Macro Segmentation

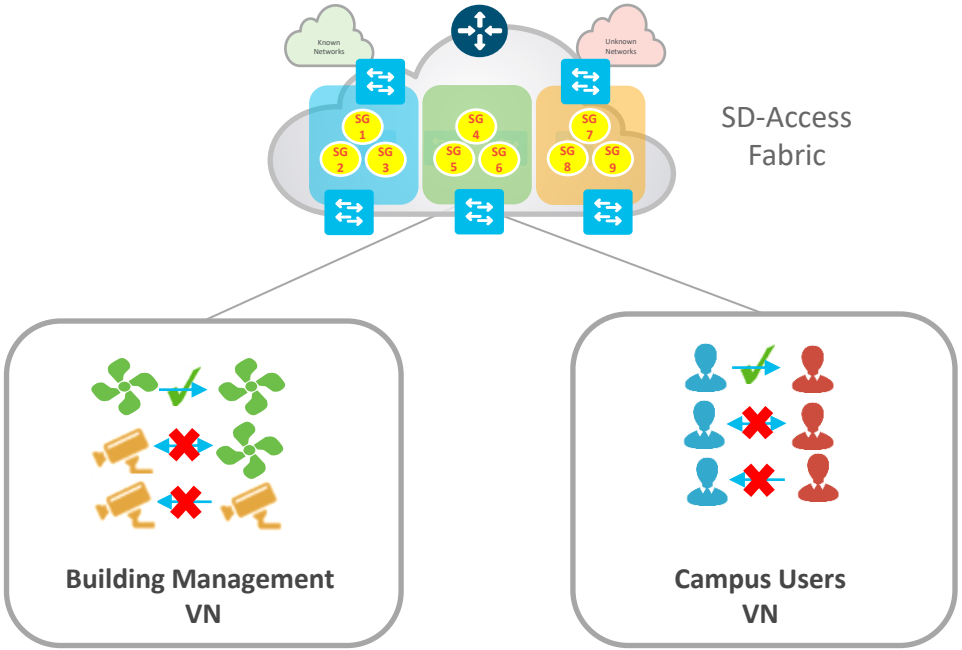


Virtual Network (VN)

First level Segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one management plane.

SD-Access Segmentation

Two Level Hierarchy - Micro Segmentation



Security Group (SG)

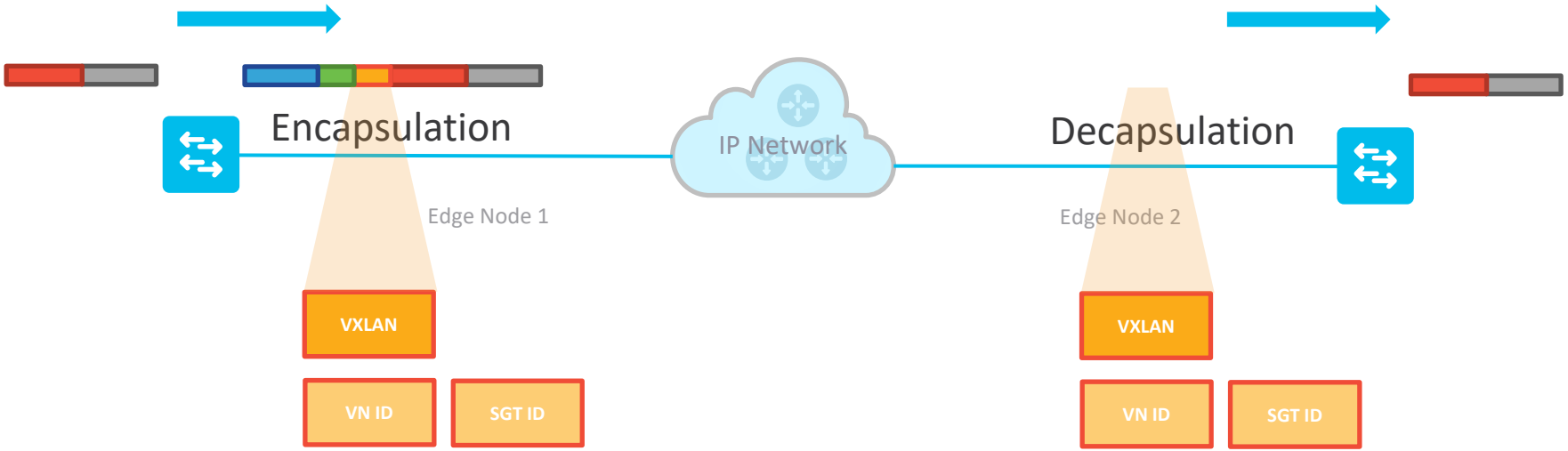
Second level Segmentation ensures **role based access control** between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

Identity-Based Segmentation

- 802.1x/RADIUS
- Passive Authorization Policy based on Endpoint Analytics attributes
- Static Port Assignment via DNA Center UI

Packet Flow in SD-Access Fabric

VN & SGT in VXLAN-GPO Encapsulation

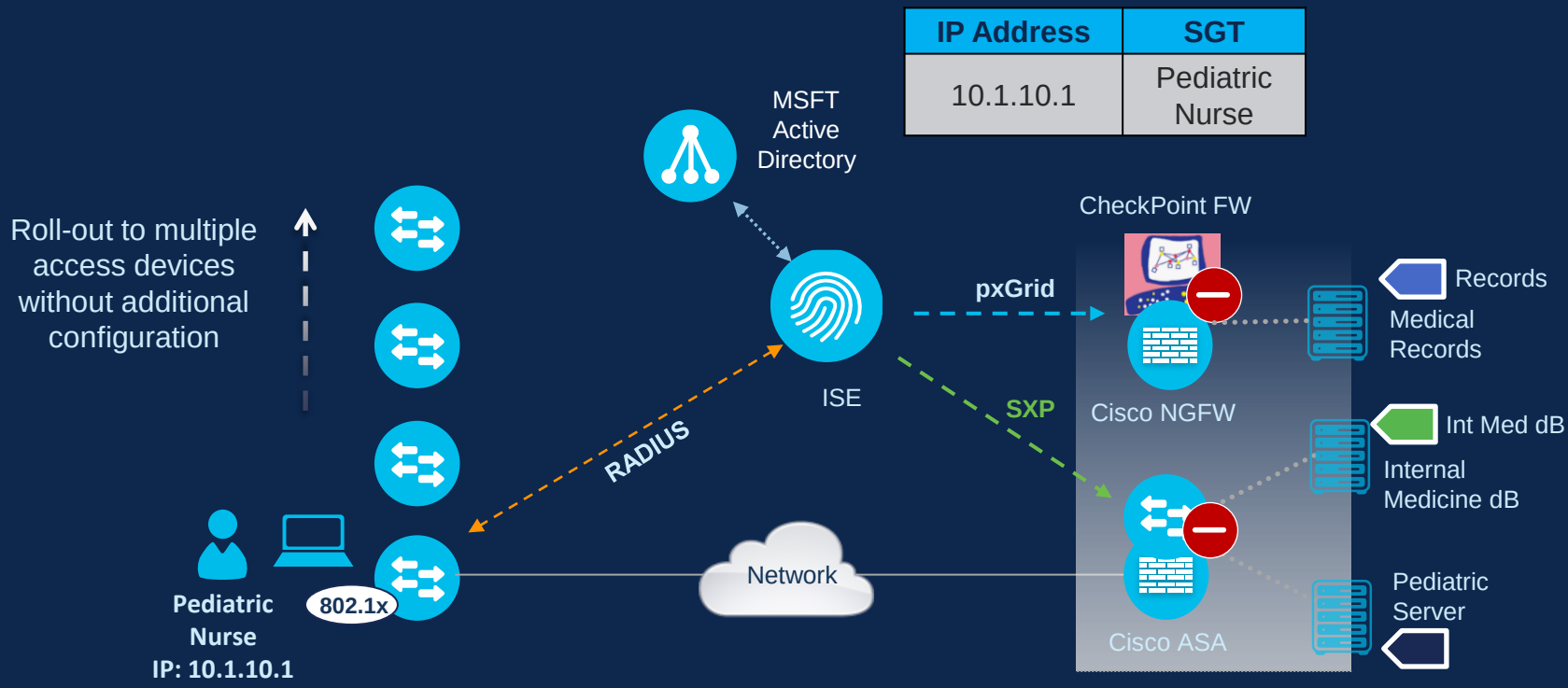


Classification
Static or Dynamic VN and SGT assignments

Propagation
Carry VN and Group context across the network

Enforcement
Group Based Policies
ACLs, Firewall Rules

SGT Propagation using ISE (SXP and pxGrid)



Rapid Threat Control

Trusted access using seamless ISE integration

Use case

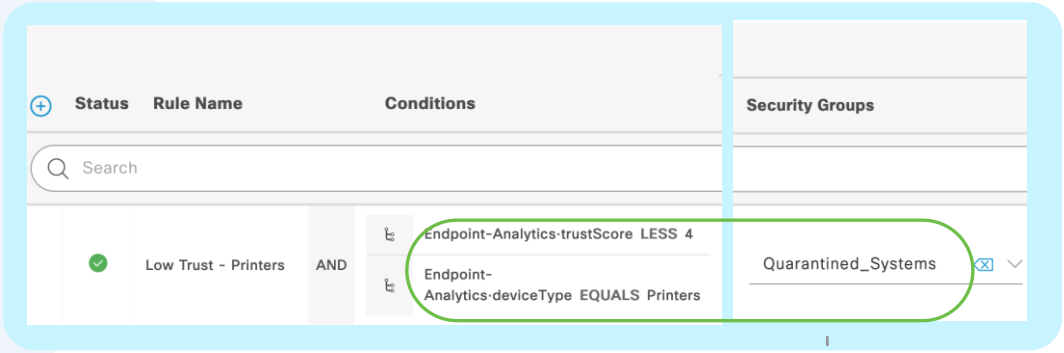
ISE admins has to manually create custom profiles per endpoint type creating additional configuration overhead and reclassification

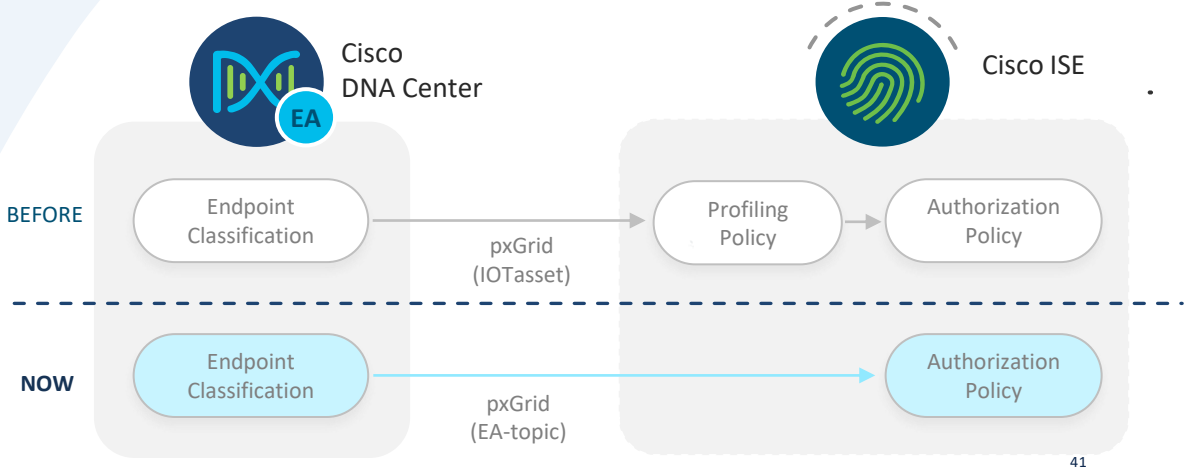
Capability

Sharing endpoint profile labels, scores, CMDB attributes in authorization policy eradicates the need for custom profile and ISE profiler reclassification.

Considerations

DNAC Version: 2.2.3 (Shockwave)
ISE Version: 3.1





EA: Endpoint Analytics

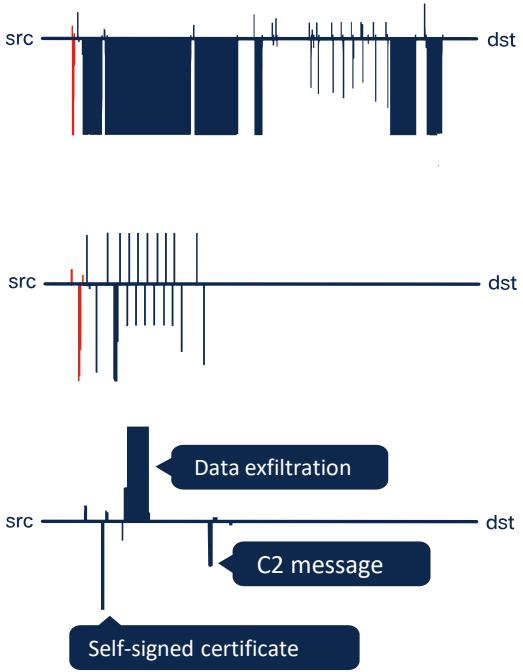
Machine learning identifies malware

Malware in encrypted traffic

Security AND privacy

Detection: 99.99% accuracy

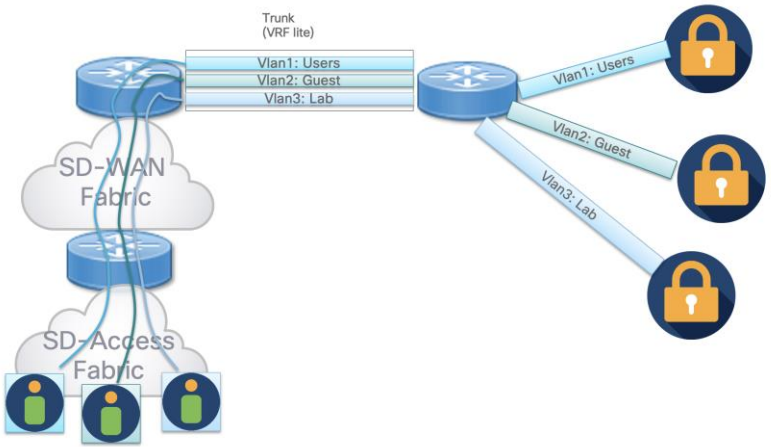
Infrastructure view of the data

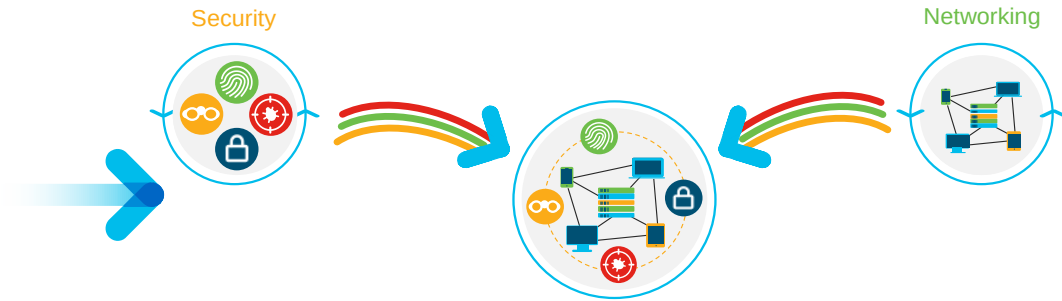


Bonus

Secure Service Insertion

Security Service Insertion - Extending Intent to Security Services





Intent-Based Network but Topology-Based Service Insertion

- Intent-Based Security Services delivered as part of the network
- Flexible security services with reusable objects shared between network and security services

Use Cases

- Policy Driven Traffic Steering
- Better Utilization of Firewall Resources
- Secure IoT network
- Secure Guest Network

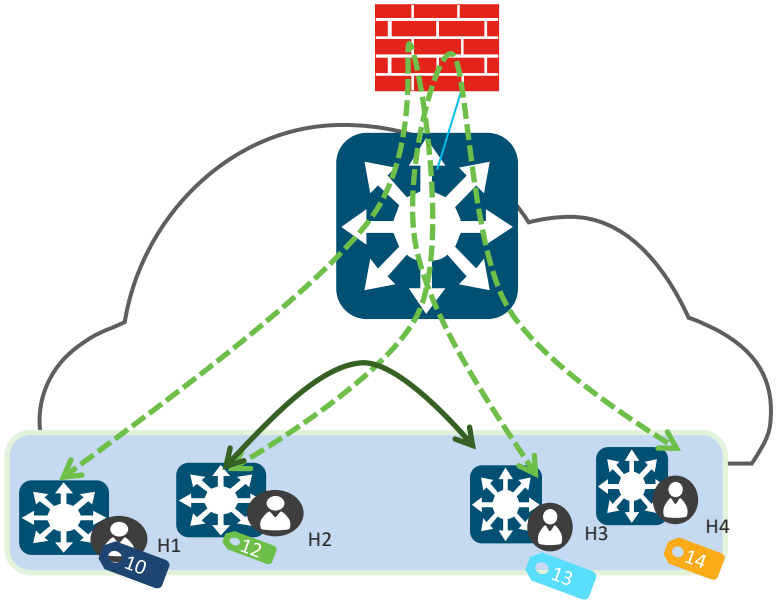
Policy Driven Traffic Steering

Use Case

- Subject traffic from one microsegment to another to specific security functions on the firewall
- Zero day protection with unpatched/end of support Windows devices.

Benefit

- Insertion of security services selectivity for specific traffic subsets in the enterprise, in an automated and policy driven manner (OpEx advantage)
- Avoids network-redesign to insert security + maintains network availability and performance
- Visibility and policy for traffic that is typically not subjected to firewall functions (SecOps value)



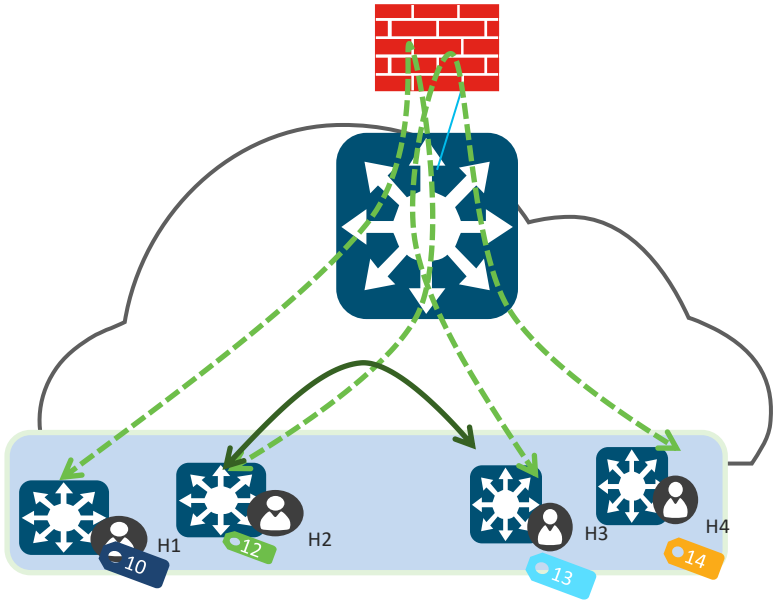
Better Utilization of Firewall Resources

Use Case

- Bypass the FW if redirection not required
- Improve the overall firewall throughput
- Improve the firewall CPU performance for higher bandwidth tasks

Benefit

- Enable higher firewall throughput by redirecting specific part of the network to firewall
- Better firewall performance



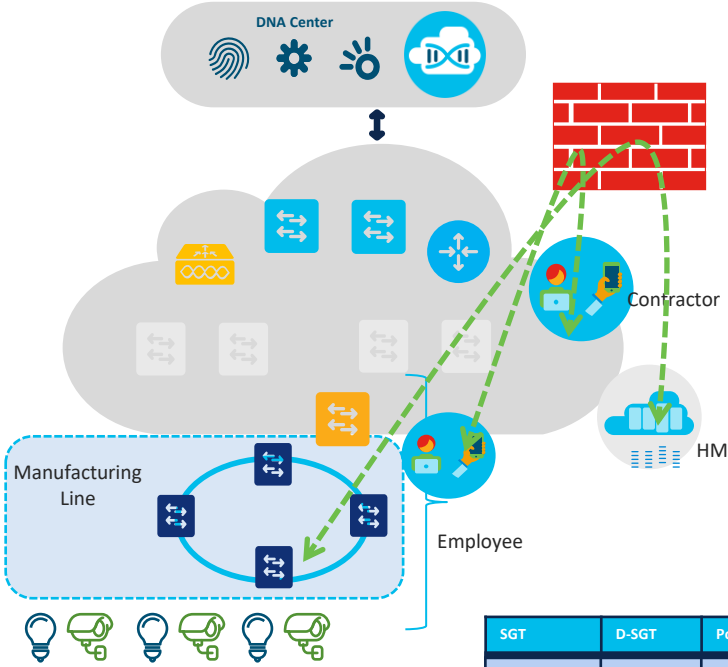
Secure IOT Network

Use Case

- Firewall will be required to inspect traffic between different groups of users and devices in IOT network
- Allow consistent policy and redirection with user mobility without increasing capex and opex

Benefit

- Secure IoT network
- Allow for movement without adding firewalls to multiple places in the factory or manufacturing flow



SGT	D-SGT	Policy
PLC	HMI	FW
HMI	Historian	FW
Engineer	Historian	FW
Contractor	PLC	FW

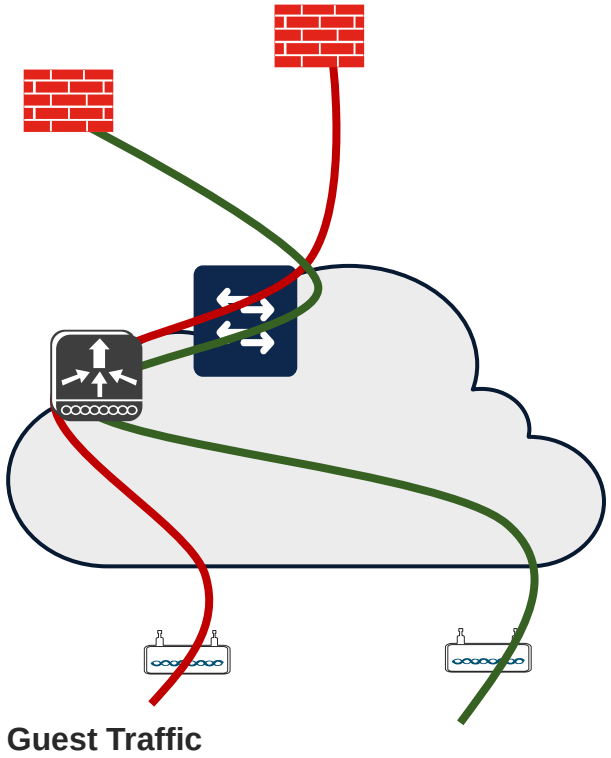
Secure Guest Network

Use Case

- Guest traffic must be segmented from internal network
- Guest traffic need to be redirected to FW

Benefit

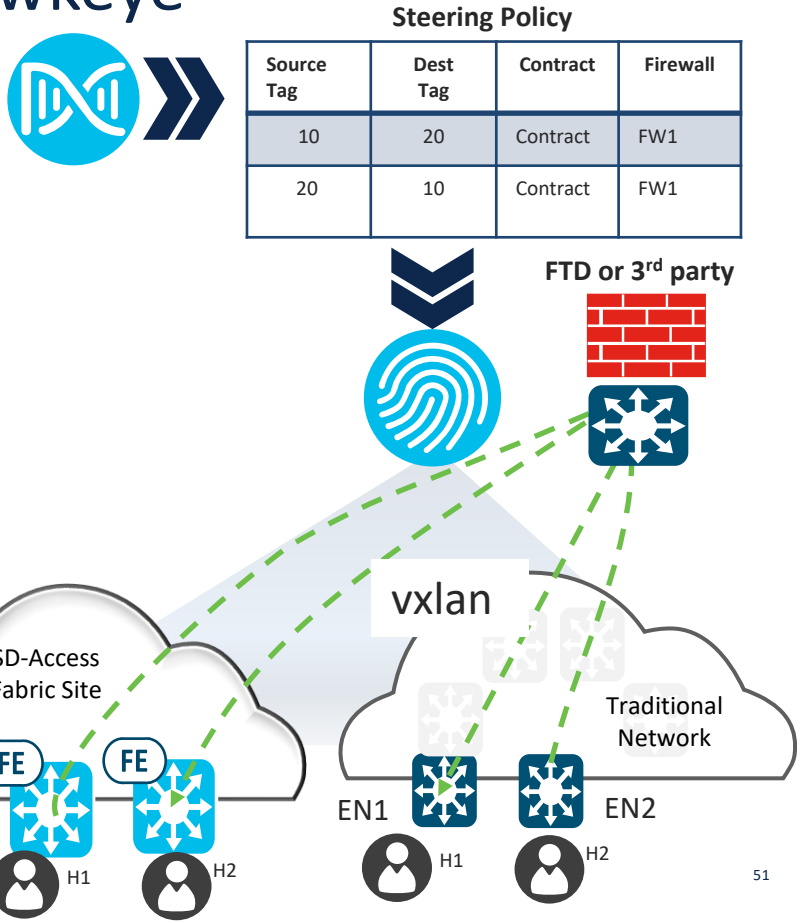
- We can use traffic steering mechanism to redirect all the guest traffic to a FW service directly from the WLC
- Remove the requirement for anchor controller



Security Services Insertion-”Hawkeye”

- Policy Based Traffic Steering

1) Create traffic steering policy on DNA Center
2) DNA Center sends steering policy to ISE (GA)
3) Steering policy programmed in the network upon request
4) Host’s traffic redirected to FW based on the steering policy



Key Takeaways

- Clear picture on Cisco DNA Architecture
- Understand how Cisco DNA with SD-Access can help you to implement Zerto Trust Architecture at your Workplace
- Inspired to do some Proof of Concept or Proof of Value activities


CISCO