Architecting Network Security Policy

Using the Network as a Sensor and Enforcer

Paul Forbes Bigbee, Sr Product Manager

January 2016

Security Challenges

Growing Attack Surface

Dynamic Threat Landscape

Complexity and Fragmentation

Internet of Things Complicates Matters

50 Billion Connected Devices by 2020

Attack Surface Increases

Cyber threats targeting IOT systems

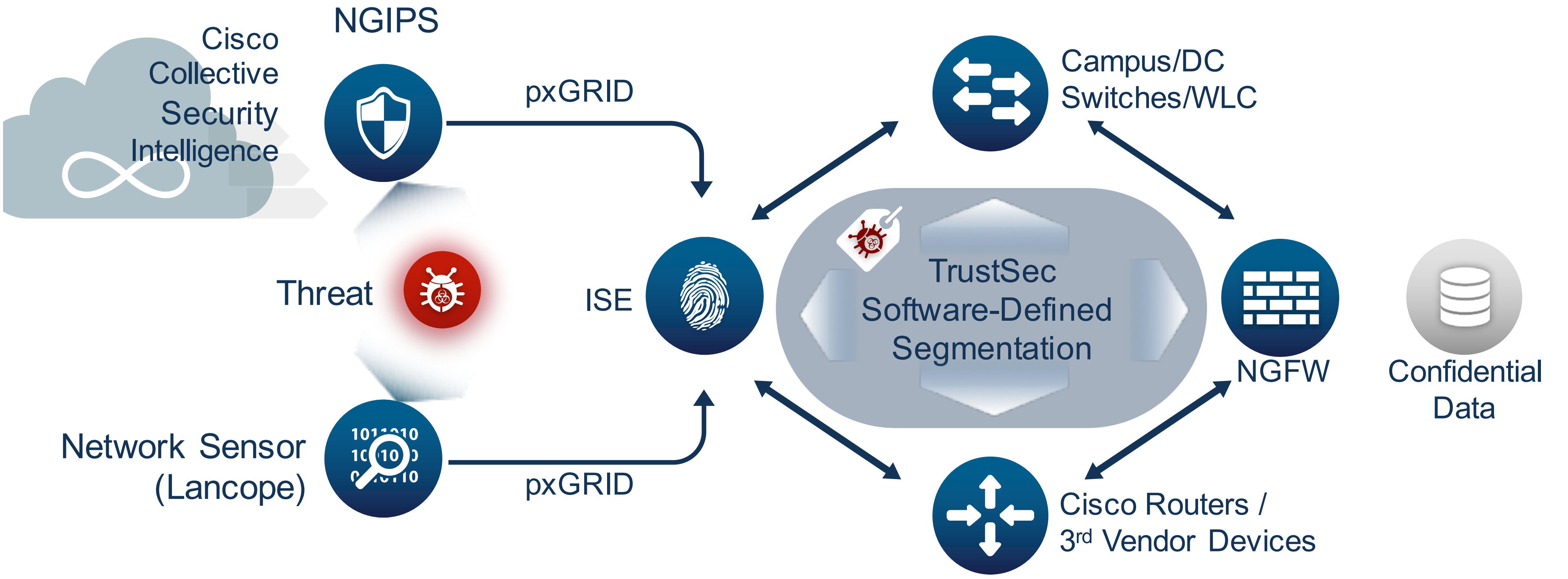
Poor Patch management and security design

Limited downtime windows, sophisticated malware

Security directly impacting business continuity

Integrated Threat Defense

Combining Network as a Sensor / Network as an Enforcer

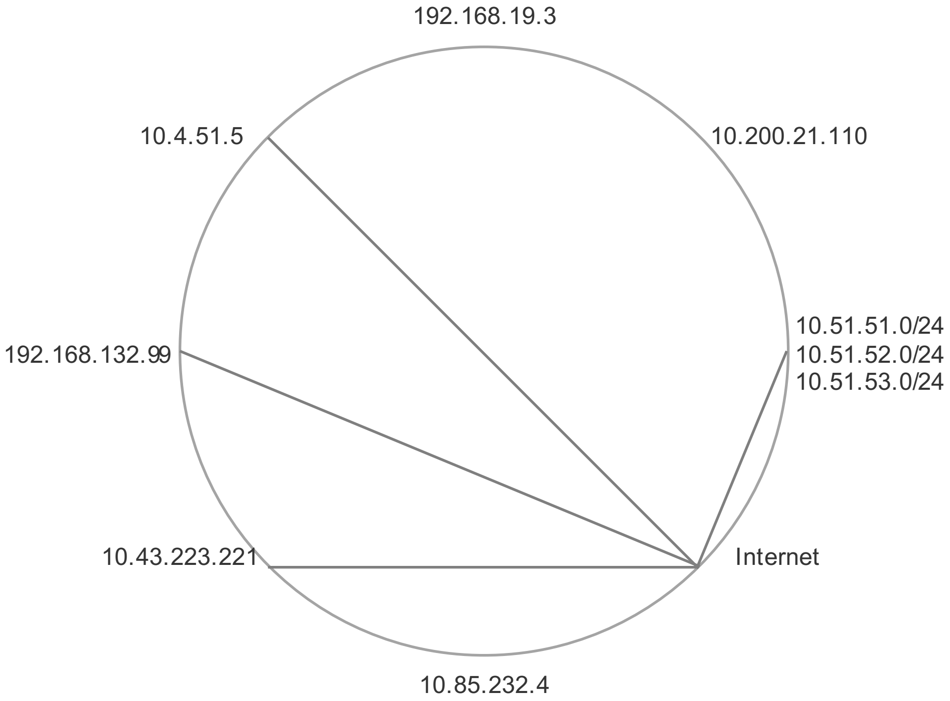


Network Sensors	Policy & Context Sharing	Network Enforcers

Network with Only Perimeter Visibility

Many devices in your network without visibility

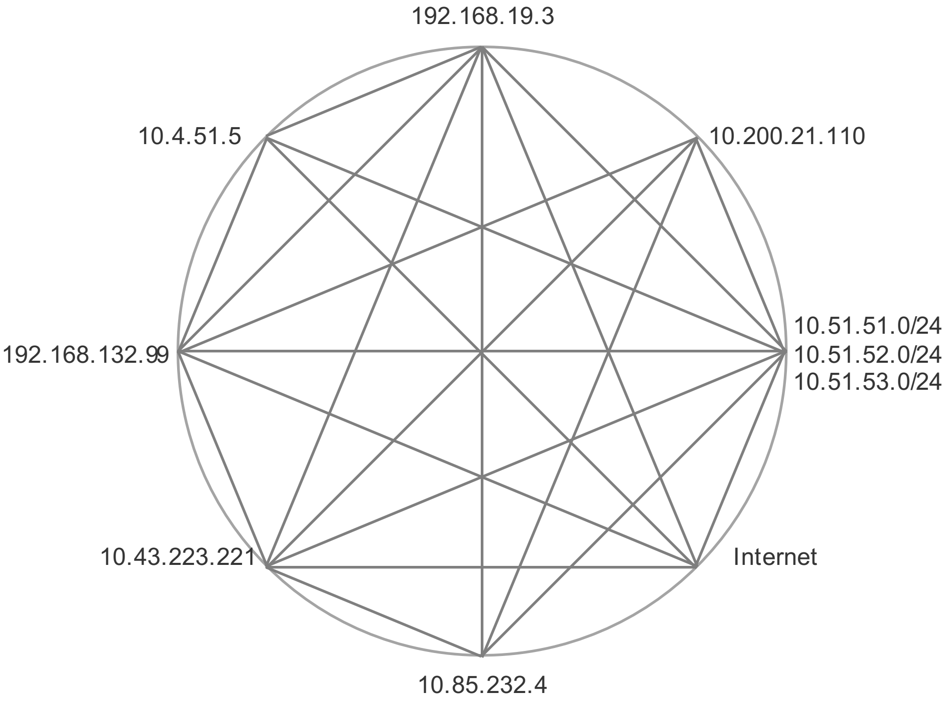
Visibility available for traffic transiting through perimeter



Enabling Visibility Inside Your Network

Cryptic network addresses that may change constantly

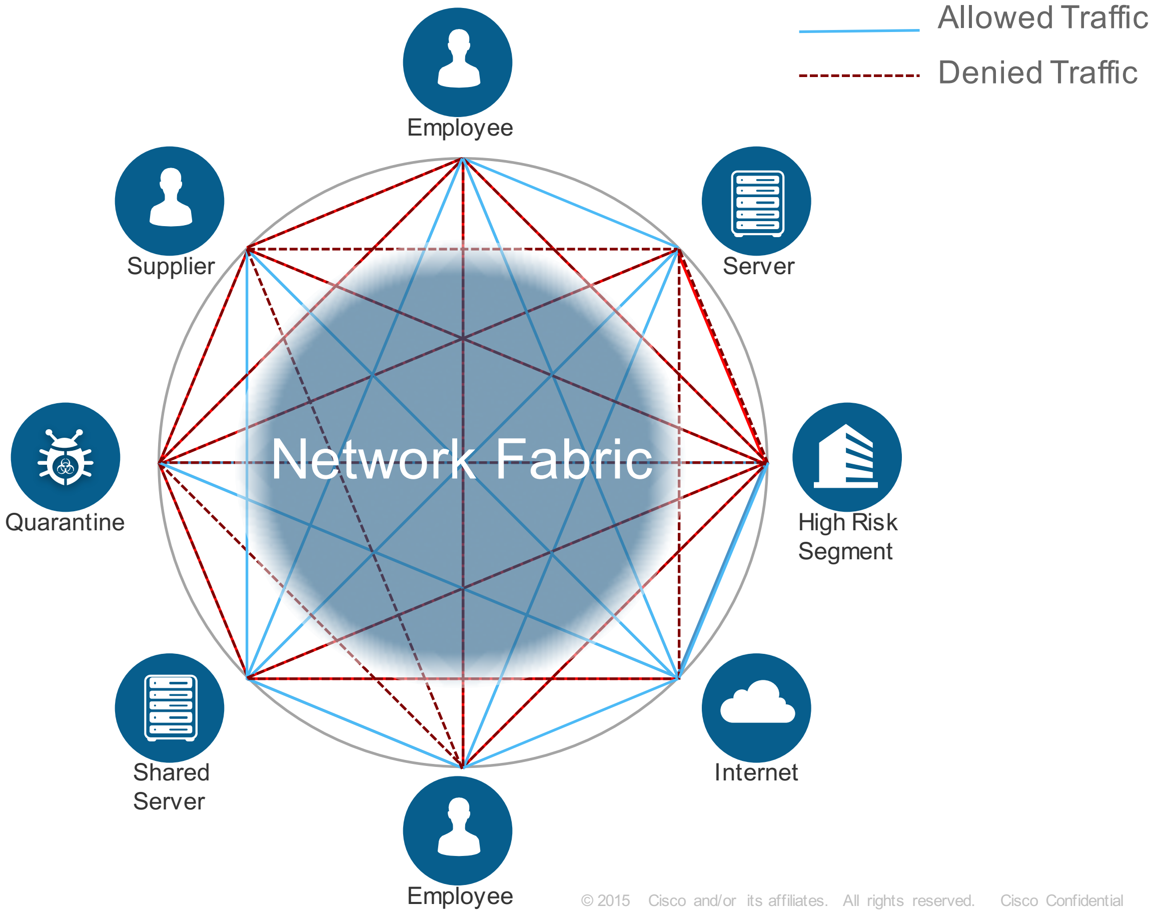
Difficult to manage policy without any context



Visibility with Context and Control

Clear understanding of traffic flow with context

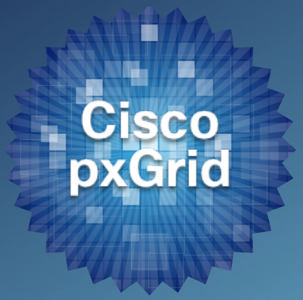
Easier to create & apply policy based on such context



Increased Visibility through Partnerships

Cisco ISE Shares Context with an Even Broader Ecosystem

ISE Ecosystem



Delivering a deeper level of contextual data to external and internal ecosystem partner solutions to better identify, mitigate, and remediate network threats.

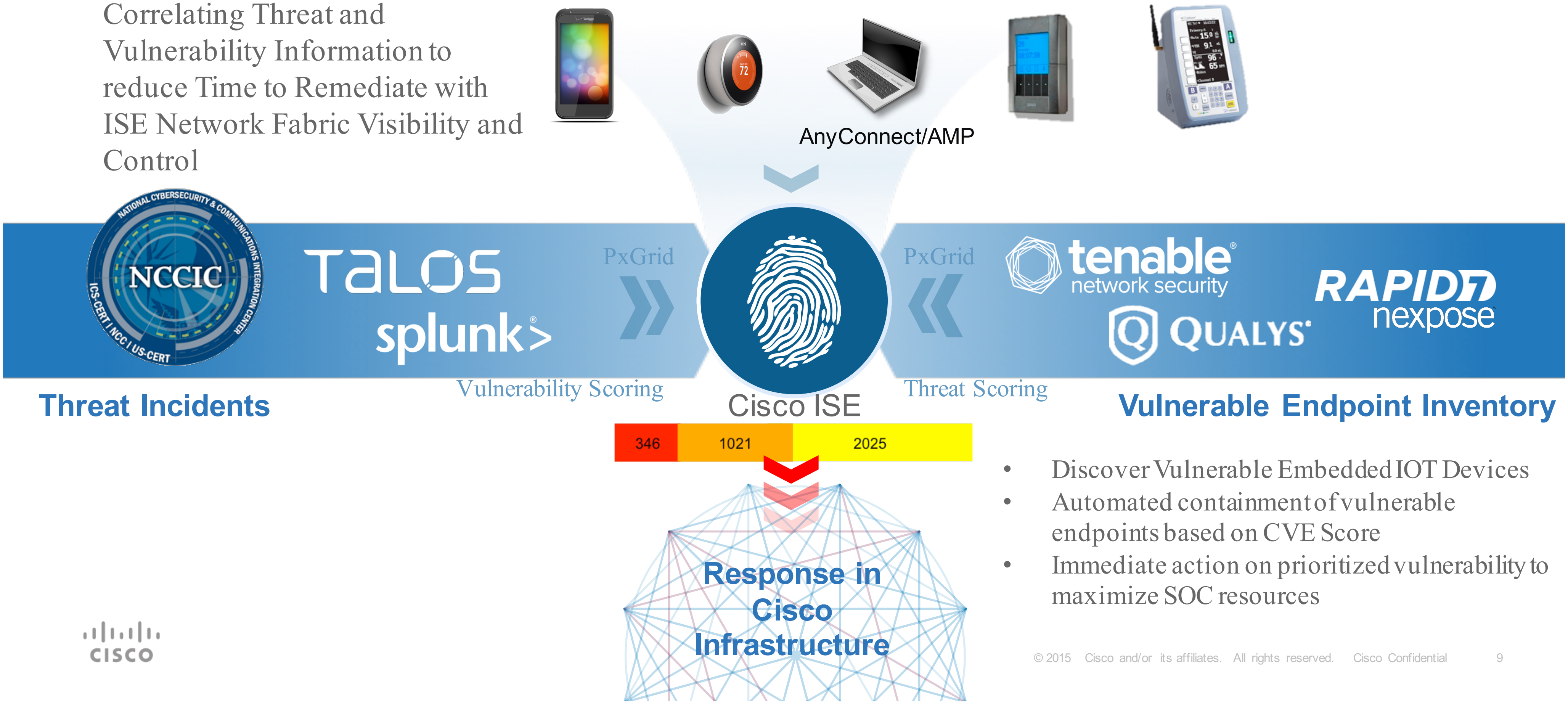
- Faster Remediation of Threats with SIEM /TD
- Extension of Access Policy & Compliance with MDM
- Context-driven OT Policy and Segmentation for IOT
- Endpoint Vulnerability Remediation
- Simplified Network Troubleshooting and Forensics
- SSO Secure Access to Sensitive Data on Mobile Devices
- Cloud Access Security for Monitoring SaaS Services
- Network / Application Performance Monitoring

Lancope Network Performance + Security Monitoring™
EMULEX
Ping Identity
elastica
skyhigh
tenable network security
LogRhythm
RAPID7
FORTSCALE
cisco meraki

splunk>
BAYSHORE INDUSTRIAL-STRENGTH CYBERSECURITY
LiveAction
savvius
NetIQ
SECUREAUTH

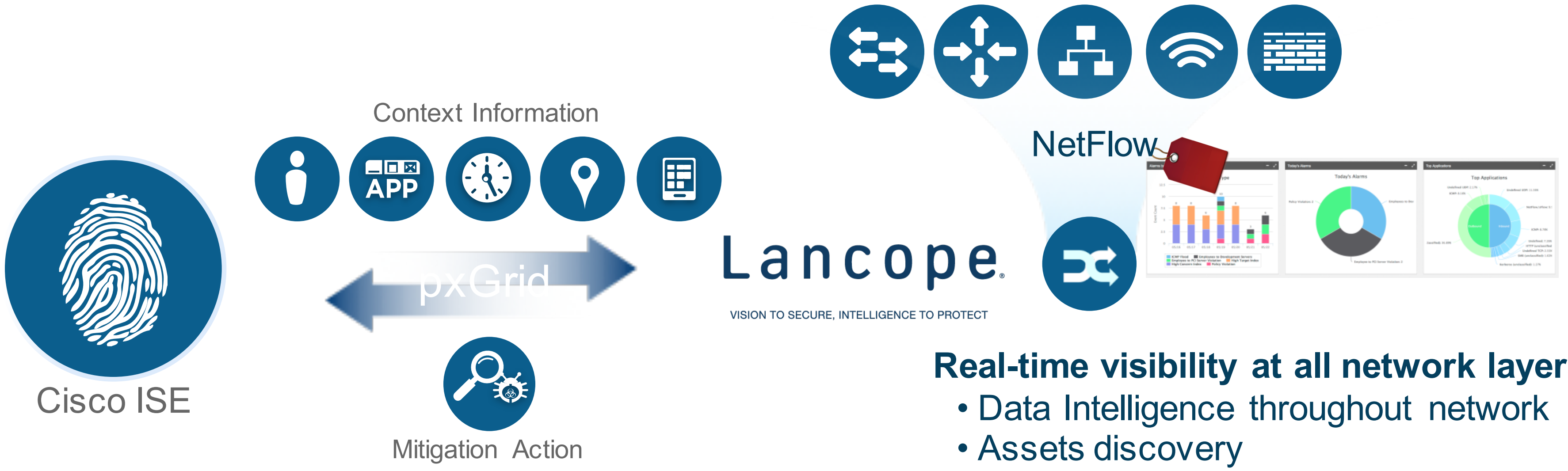
Threat Centric NAC

Correlating Threat and Vulnerability Information to reduce Time to Remediate with ISE Network Fabric Visibility and Control



- Discover Vulnerable Embedded IOT Devices
- Automated containment of vulnerable endpoints based on CVE Score
- Immediate action on prioritized vulnerability to maximize SOC resources

Network as a Sensor: Lancope StealthWatch

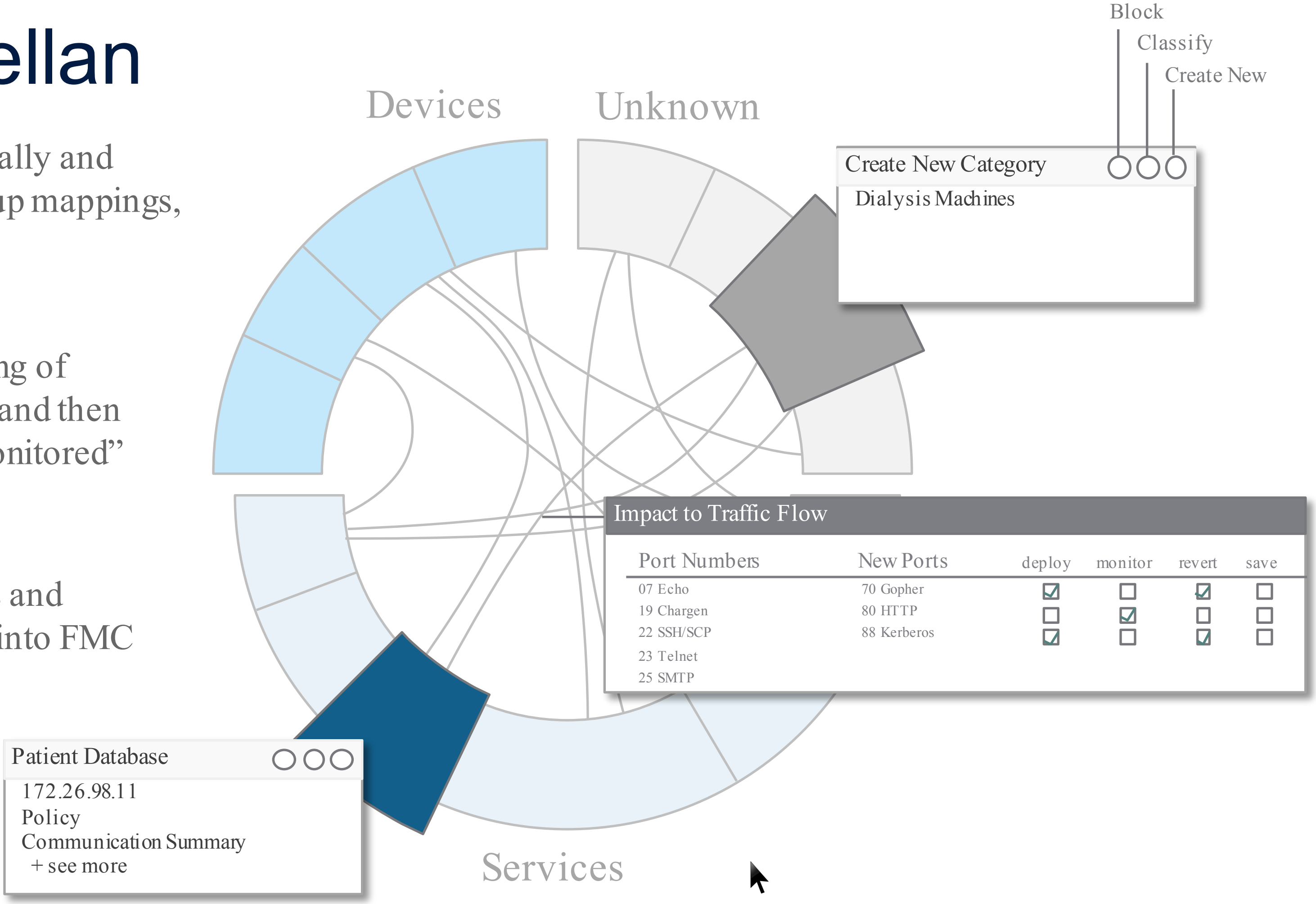


Real-time visibility at all network layers

- Data Intelligence throughout network
- Assets discovery
- Network profile
- Security policy monitoring
- Anomaly detection
- Accelerated incident response

Project Magellan

- **Discover** Allow for manually and automatically generated group mappings, aggregate network telemetry
- **Model** Re-grouping/pivoting of relationships; approval flow and then monitor deviations from "monitored" service
- **Author** Policy suggestions and potential ramifications back into FMC and ISE policy managers



Create New Category ○○○

Dialysis Machines

Impact to Traffic Flow

Port Numbers	New Ports	deploy	monitor	revert	save
07 Echo	70 Gopher	☑	□	☑	□
19 Chargen	80 HTTP	□	☑	□	□
22 SSH/SCP	88 Kerberos	☑	□	☑	□
23 Telnet					
25 SMTP					

Patient Database ○○○

172.26.98.11
Policy
Communication Summary
+ see more

Customer Case:
Global Retailer using Network As A Sensor

Customer Pain Points:

- Limited visibility & intelligence across their highly-distributed retail footprint
- Ability to correlate numerous data sets

Environment:

- Cisco Switches & Routers
- ASA & ISE

Cisco Proposal:

- Deploy StealthWatch
- Integrate with ISE

POV Findings
Segmentation Violation
Infected Servers
Network Application Usage
Unauthorized Applications
Misconfigured Devices
Suspicious DNS Activity
Retail Point-of-Presence Visibility

Result:

- Network as a Sensor provides visibility to security challenges enabling them to take action

Network Segmentation is a Best Practice

Australian Government
Department of Defence
Intelligence and Security

Network segmentation… is one of the most effective controls an agency can implement to mitigate the second stage of a network intrusion, propagation or lateral movement

InformationWeek NETWORKComputing

"Recent security breaches underscore the importance of maintaining proper network segmentation."

verizon 2014 DATA BREACH INVESTIVATIONS REPORT

"Good network and role segmentation will do wonders for containing an incident."

TechTarget®

Not only are performance benefits to be gained, but such segmentation can also limit the scope of a compromise, whether it is an internal or external attack, a malicious breach or even a non-malicious misconfiguration.

NETWORKWORLD

"It's a much easier to equip your organization with a secure defense through proper network segmentation than to explain to shareholders and the media how hackers were able to access millions of records on your system"

What TrustSec Provides

Software defined Network Segmentation

Context-based Data Access

Agile Security Policy Changes and Simpler Management

Context based Service Chaining

Network as a Sensor / Enforcer Use Cases

Healthcare

Protect EMR; Protect medical equipment from malware

Financial

Control access to regulated apps; Simplify audit & compliance; Accelerate security policy provisioning for new server

Manufacturing

Security controls for IoE, Simplified segmentation for manufacturing zones, Supply-chain partner security

Retail

Scope reduction for PCI compliance; Protect sensitive information from other connected devices

Education

Control student access to classroom media, Scalable access control policy for students and faculty

Consistent Policy

Policy across campus, branch & DC for ACI & non-ACI

Secure BYOD

Maximizing BYOD investment while protecting sensitive information

Simplified Firewall Rule Management

Faster data center service / application provisioning

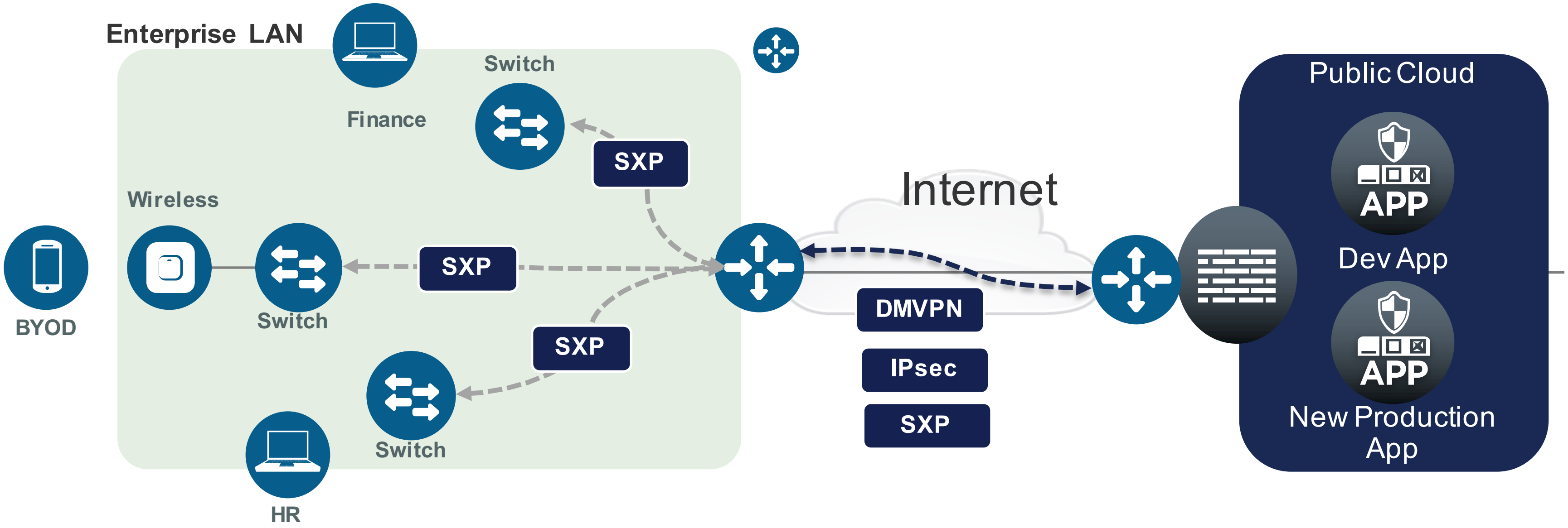
Threat Mitigation

Mitigate malware scanning and propagation with actionable intelligence to find needle in haystack

Secure Remote Access

Differentiated access for contractors & partners

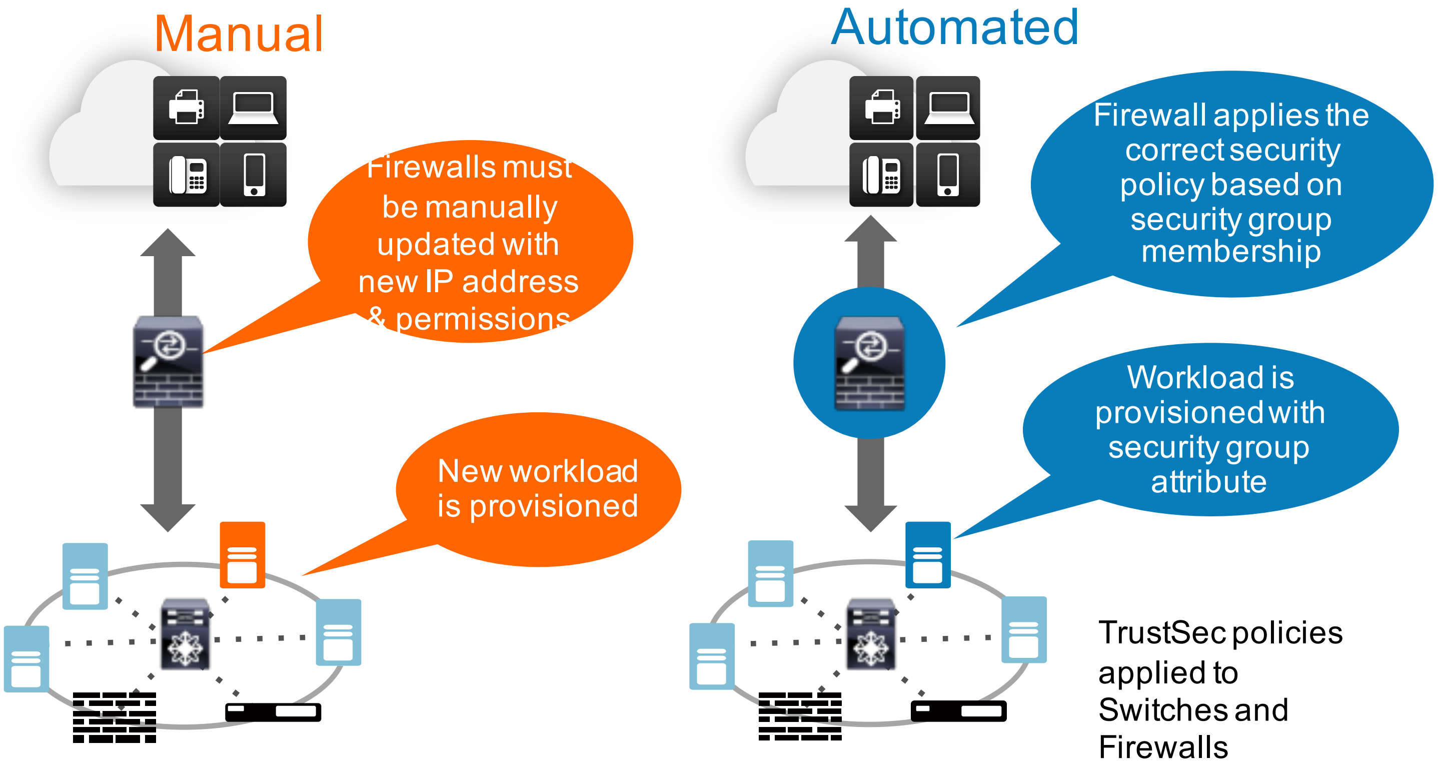
Extending Enterprise TrustSec Policy to Cloud



- Extending Enterprise Policy Enforcement to public clouds
- CSR-1000V, ASAv, Nexus 1000v all provide enforcement based on SGT classification from the Enterprise

Example: Ease of Data Centre Provisioning

Ease of **Provisioning**



Manual

Firewalls must be manually updated with new IP address & permissions

New workload is provisioned

Automated

Firewall applies the correct security policy based on security group membership

Workload is provisioned with security group attribute

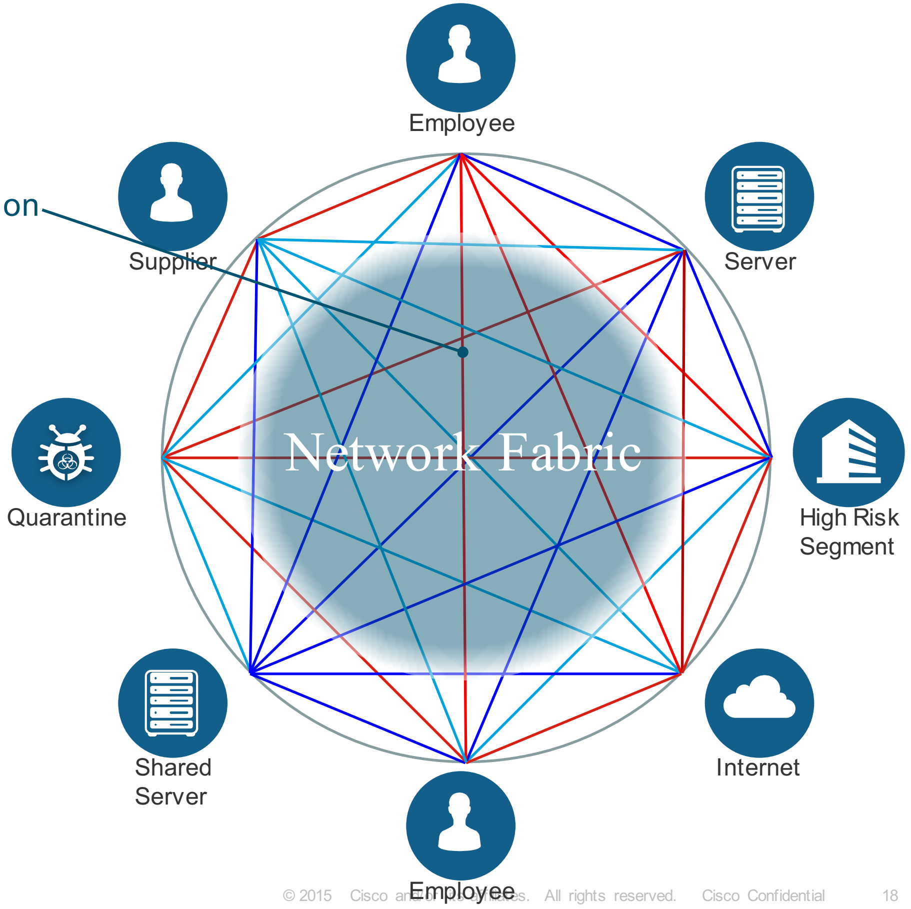
TrustSec policies applied to Switches and Firewalls

Building Complex Security Policy Very Simply

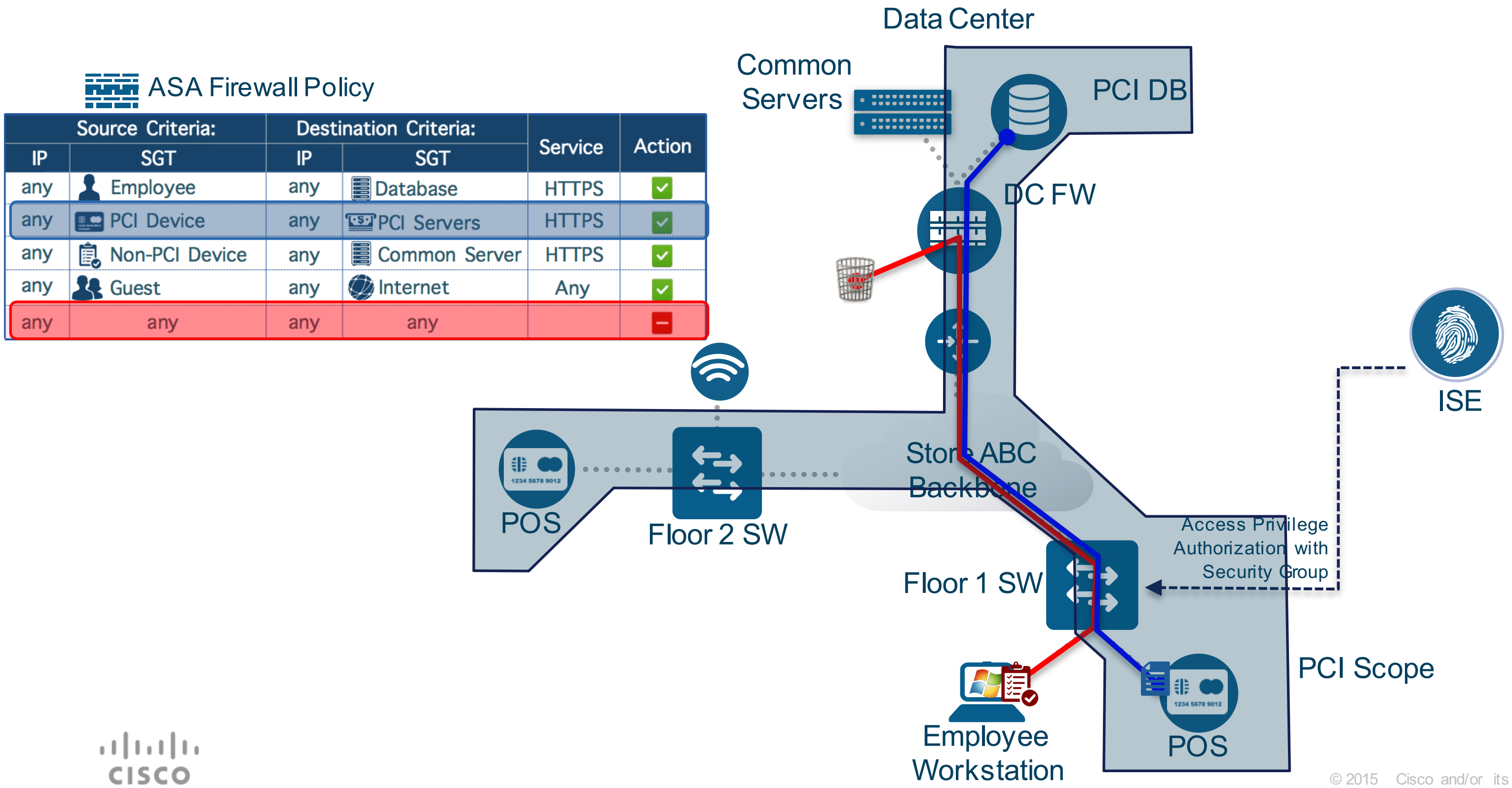
```
deny icmp
deny udp employee employee eq domain
deny tcp employee employee eq 3389
deny tcp employee employee eq 1433
deny tcp employee employee eq 1521
deny tcp employee employee eq 445
deny tcp employee employee eq 137
deny tcp employee employee eq 138
deny tcp employee employee eq 139
deny udp employee employee eq snmp
deny tcp employee employee eq telnet
deny tcp employee employee eq www
deny tcp employee employee eq 443
deny tcp employee employee eq 22
deny tcp employee employee eq pop3
deny tcp employee employee eq 123
```

Block Lateral Movement & Privilege Escalation

Source \ Destination	Employee	Suppliers	App Servers	Shared Services	Quarantine
Employee	−	−	✓	✓	−
Suppliers	−	✓	−	✓	−
App Servers	✓	−	✓	−	−
Shared Services	✓	✓	−	✓	−
Quarantine	−	−	−	−	−



PCI Segmentation using TrustSec



ASA Firewall Policy

Source Criteria:		Destination Criteria:		Service	Action
IP	SGT	IP	SGT		
any	Employee	any	Database	HTTPS	✓
any	PCI Device	any	PCI Servers	HTTPS	✓
any	Non-PCI Device	any	Common Server	HTTPS	✓
any	Guest	any	Internet	Any	✓
any	any	any	any		⛔

OS Type: Windows 8
User: John
AD Group: Floor Staff
Device Group: Nurse Workstation
Security Group = Employee

OS Type: Windows 7 Embedded
User: George
AD Group: Point-of-Sales Admin
Device Group: POS
Security Group = PCI Device

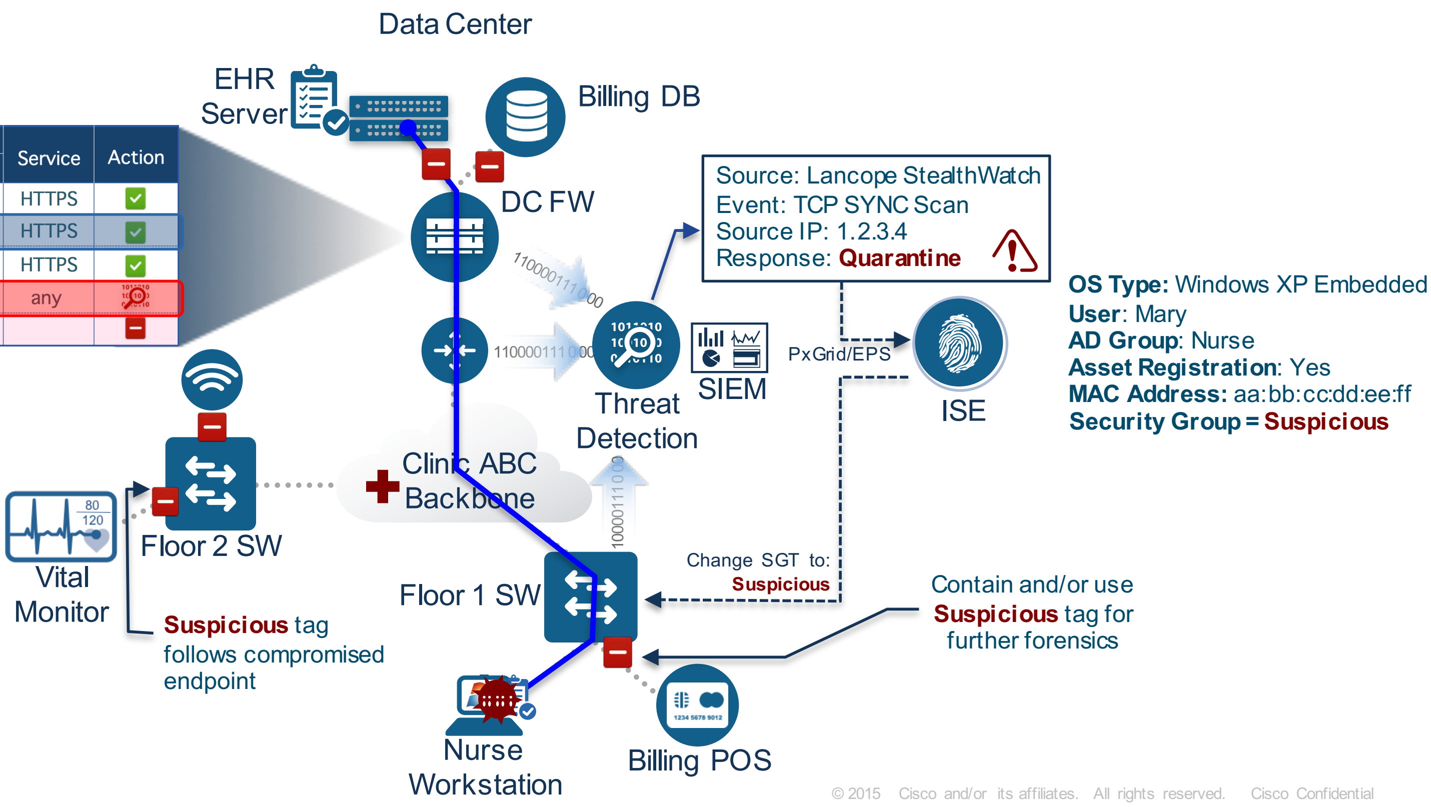
Threat Detection & Remediation using TrustSec

ASA Firewall Policy

Source Criteria:		Destination Criteria:		Service	Action
IP	SGT	IP	SGT		
any	Doctors	any	EHR Server	HTTPS	✓
any	Clinical Dev.	any	EHR Server	HTTPS	✓
any	PCI Device	any	Billing DB	HTTPS	✓
any	Suspicious	any	any	any	🔍
any	any	any	any		−

SGACL Policy

Source \ Destination	Doctors	Clinical Dev.	PCI Device	Suspicious	Patients
Doctors	✓	✓	−	−	−
Clinical Dev.	✓	✓	−	−	−
PCI Device	−	−	✓	−	−
Suspicious	−	−	−	−	−
Patients	−	−	−	−	✓



Source: Lancope StealthWatch
Event: TCP SYNC Scan
Source IP: 1.2.3.4
Response: **Quarantine**

OS Type: Windows XP Embedded
User: Mary
AD Group: Nurse
Asset Registration: Yes
MAC Address: aa:bb:cc:dd:ee:ff
Security Group = Suspicious

Change SGT to: **Suspicious**

Contain and/or use **Suspicious** tag for further forensics

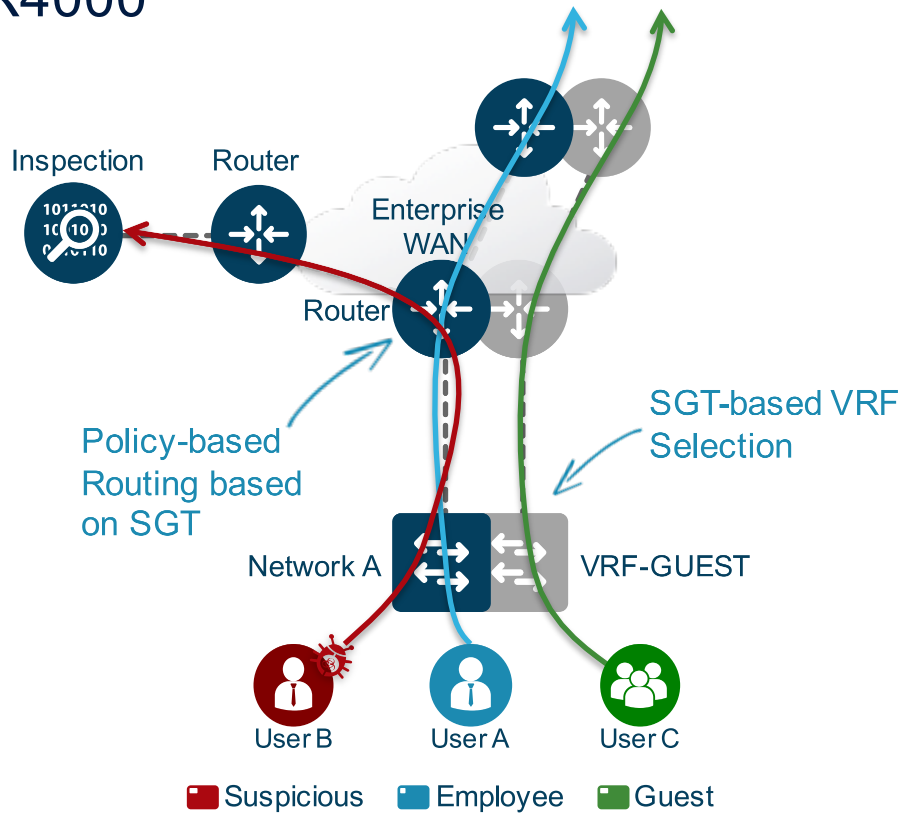
Suspicious tag follows compromised endpoint

Path selection based on SGT

Now Available in ASA, ASR1000, ISR4000

Security Example

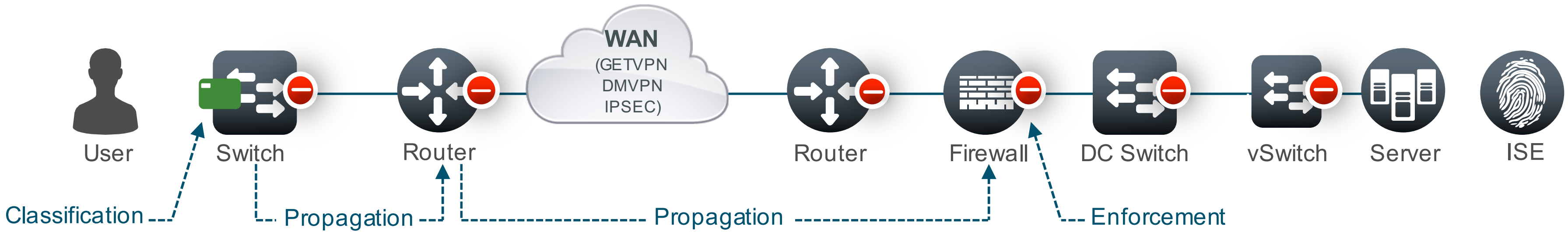
✓ Redirect traffic from malware-infected hosts
- Contain threats
- Pass traffic through centralised analysis and inspection functions



Other Examples

✓ To map different user groups to different WAN service
- Segment in a site with TrustSec
- SGT routes traffic to correct WAN/VRF

TrustSec Supported Platforms



Classification

Catalyst 2960-S/-C/-Plus/-X/-XR
Catalyst 3560-E/-C/-X/-CX
Catalyst 3750-E/-X
Catalyst 3850/3650
Catalyst 4500E (Sup6E/7E)
Catalyst 4500E (Sup8)
Catalyst 6500E (Sup720/2T)
Catalyst 6800
WLC 2500/5500/WiSM2
WLC 5760
Nexus 7000
Nexus 6000
Nexus 5500/2200
Nexus 1000v
ISRG2, CGR2000, ISR4000
IE2000/3000/CGR2000
ASA5500 (RAS VPN)

Propagation

Catalyst 2960-S/-C/-Plus/-X/-XR
Catalyst 3560-E/-C/, 3750-E
Catalyst 3560-X/3750-X
Catalyst 3850/3650
Catalyst 4500E (Sup6E)
Catalyst 4500E (Sup, 7E, 7LE, 8E)
Catalyst 4500X
Catalyst 6500E (Sup720)
Catalyst 6500/Sup2T, 6800
WLC 2500/5500/WiSM2
WLC 5760
Nexus 7000
Nexus 6000
Nexus 5500/2200
Nexus 1000v
ISRG2,ISR4000
IE2000/3000/CGR2000
ASR1000
ASA5500

Enforcement

Catalyst 3560-X
Catalyst 3750-X
Catalyst 3850/3650
WLC 5760
Catalyst 4500E (7E)
Catalyst 4500E (8E)
Catalyst 6500E (2T)
Catalyst 6800
Nexus 7000
Nexus 6000
Nexus 5500
Nexus 1000v
ISR G2 Router, CGR2000
ASR 1000 Router
CSR-1000v Router
ASA 5500 Firewall
ASAv Firewall
Web Security Appliance

Vision

Web Security Integration (Released)

Service (PBR, PfR, QoS) Chaining

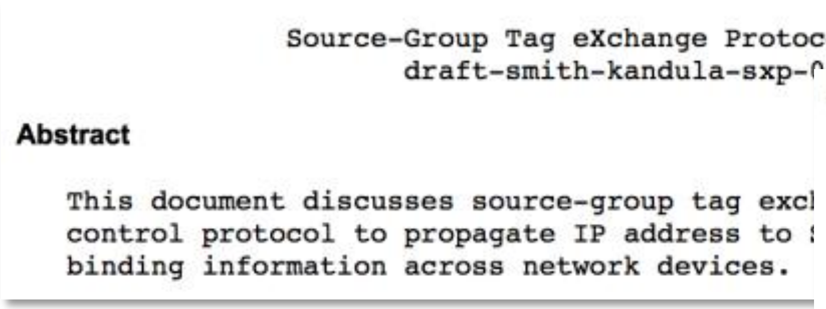
IPv6 Policy Enforcement

SDN Integration

cisco TOMORROW starts here.

Open TrustSec

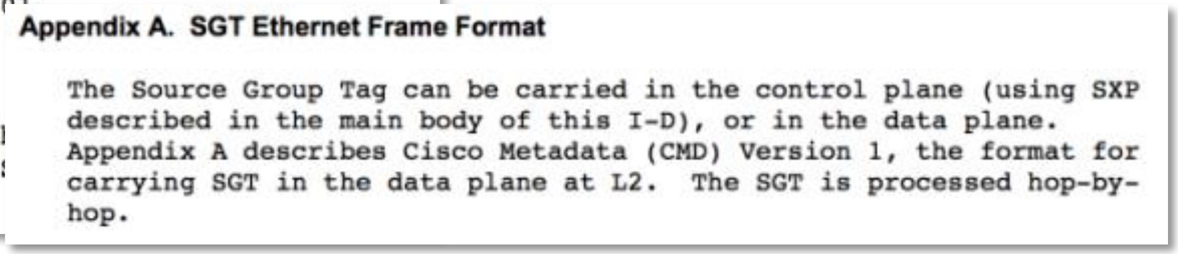
- SXP and Inline Tagging submitted to the IETF :-
  - ‘Source-Group Tag eXchange Protocol’ IETF Informational Draft
    https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/



Source-Group Tag eXchange Protocol (SXP)
draft-smith-kandula-sxp-0

Abstract

This document discusses source-group tag exch
control protocol to propagate IP address to
binding information across network devices.

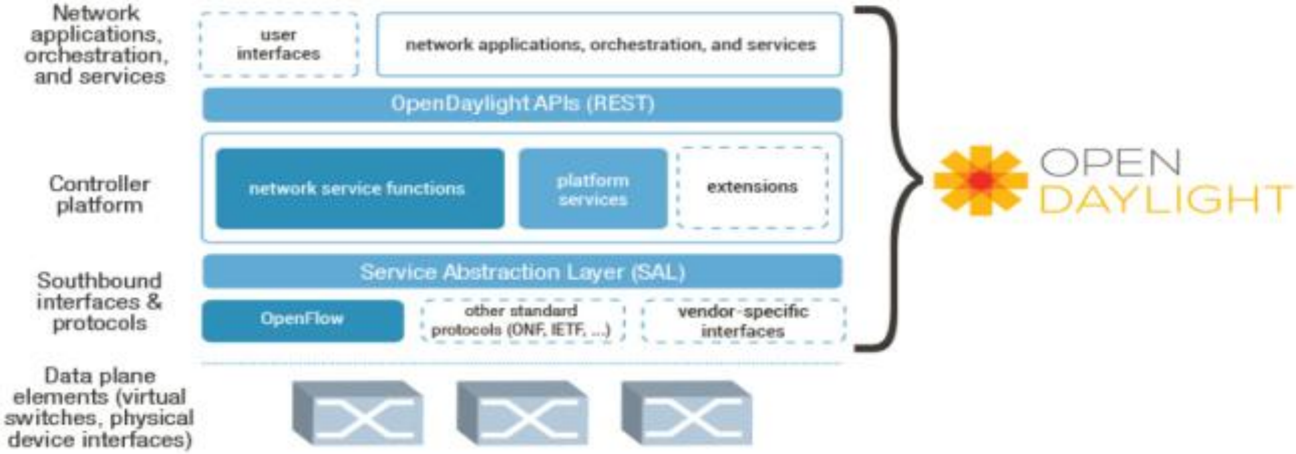


Appendix A. SGT Ethernet Frame Format

The Source Group Tag can be carried in the control plane (using SXP described in the main body of this I-D), or in the data plane. Appendix A describes Cisco Metadata (CMD) Version 1, the format for carrying SGT in the data plane at L2. The SGT is processed hop-by-hop.

- SGT can be carried in standards-track Network Services Header (NSH)
  - Allows for SGTs to be mapped to Source Class and Destination Class
  - https://tools.ietf.org/html/draft-guichard-sfc-nsh-dc-allocation-01

Open Source TrustSec


Network applications, orchestration, and services
user interfaces
network applications, orchestration, and services
OpenDaylight APIs (REST)
Controller platform
network service functions
platform services
extensions
Southbound interfaces & protocols
Service Abstraction Layer (SAL)
OpenFlow
other standard protocols (ONF, IETF, ...)
vendor-specific interfaces
Data plane elements (virtual switches, physical device interfaces)
OPEN DAYLIGHT

SXP is now included in the Open Daylight SDN Controller

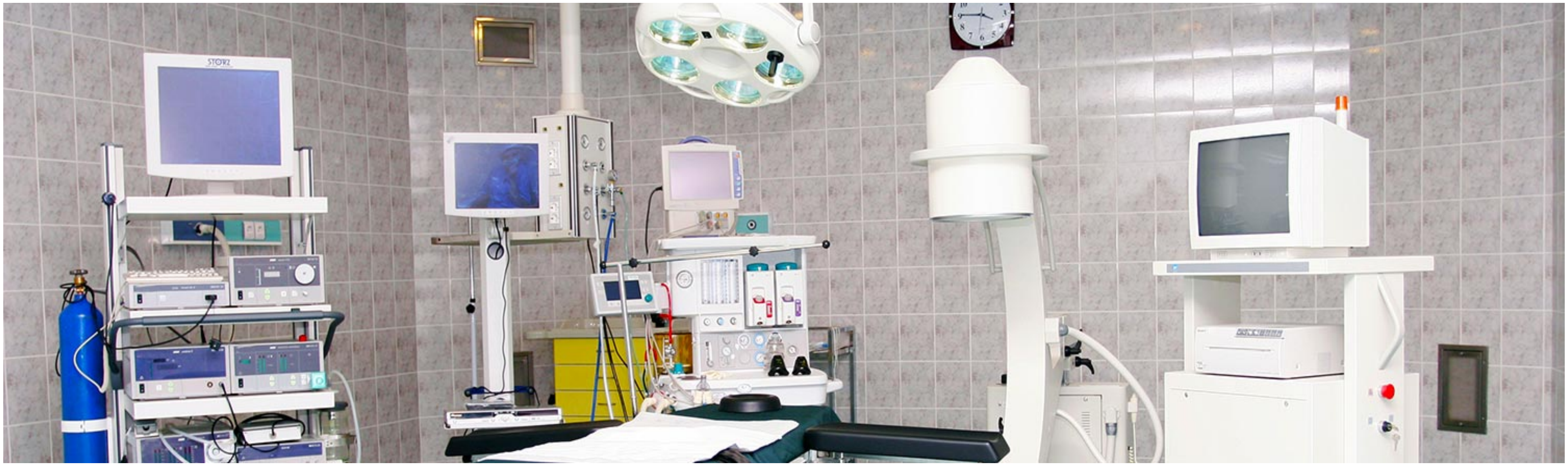
https://www.opendaylight.org/whats-new-lithium

Allows other vendors to integrate at Controller level instead of network

Open Source SXP implementation now available via Github

https://github.com/opendaylight/sxp

Allows other vendors to use to implement in their own products (e.g. we use this in ISE 2.0)



Healthcare Organization

Situation: A risk audit determined the organization’s flat network exposed medical devices and patient data to compromise and recommended an access control and segmentation strategy. Firewall-only strategy was deselected due to inflexibility and operations costs.

Solution: Network refresh with TrustSec-ready network devices segments based on security groups (doctor, patient, endpoint type, application) and controls usage within groups. ISE provides policy control, contextual identity and access control. Lancope netflow analysis monitors policy and enables risk and compliance oversight. Threat mitigation via pxGrid is planned.

Result: Security and risk compliance assurance, lower operating costs, business agility, long-term investment value

Oil and Gas Producer

Situation: IT had initiatives to institute BYOD and guest access control, unify fragmented access and security operations, and quickly take action on security breaches.

Solution: ISE is deployed for BYOD, guest services and to unify access control into one operation. Splunk's integration with pxGrid provides ISE contextual data to a security dashboard for rich endpoint monitoring, analysis and reporting. In addition, IT staff uses pxGrid integration to take immediate action to mitigate misbehaving endpoints.

Result: ISE helps unify and centralize security operations and Splunk's integration with pxGrid improves security visibility and response.

International Bank

Situation: A board-level directive required IT to move quickly to protect critical business applications and improve visibility across an open and fragmented network comprising headquarters, data centers and 2,000+ access sites.

Solution: IT implemented TrustSec segmentation in the data center with ISE as controller and Lancope to monitor SGTs. ISE controls access on wireless and wired networks and AnyConnect secures remote access. ASA with FirePower and TrustSec in the data center simplifies firewall rule management and selectively applies IPS on the SGT value of the user or server.

Result: IT quickly exceeded the directive to protect applications, gain visibility, and enforce policy at a granular level across a diverse collection of sites and data centers. In addition, they instituted rogue device detection and control and accelerated the time-to-deploy applications and servers in the data center.

Automobile Manufacturer

Situation: An OT (operational technology) initiative identified network security gaps that meant robot endpoints are subject to security breaches, operational mishaps, and failures that could disrupt production and threaten worker safety.

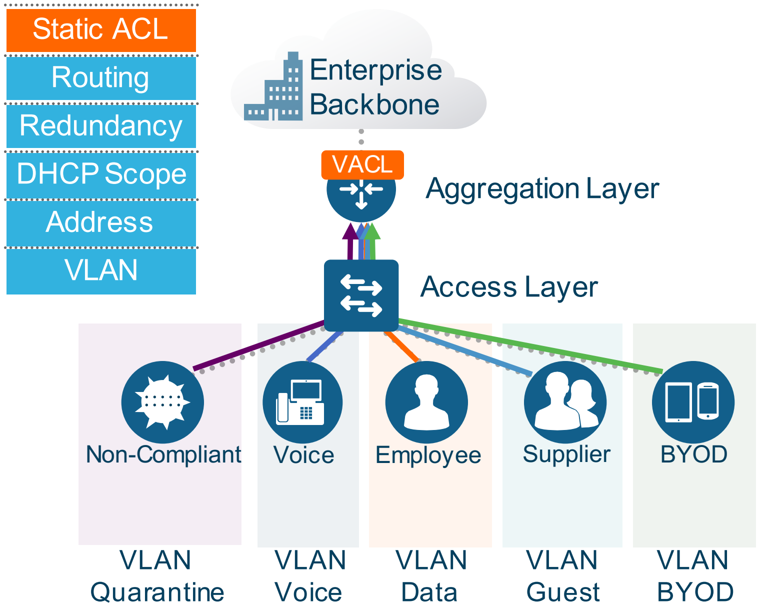
Solution: Granular access and behavior control. ISE provides contextual network access control that is used by TrustSec to classify and tag network traffic. Bayshore's content inspection engine uses pxGrid to identify TrustSec tags and TrustSec SXP integration to read the tags, determine if the behaviors are appropriate for the 'security group', and dynamically retag (mitigate) improper traffic. This solution also enables real-time performance monitoring for that enables proactive robot maintenance.

Result: Integration of manufacturing security intelligent that improves OT security, worker safety and increases system uptime.

Software Defined Segmentation with TrustSec

Segmentation is Expensive

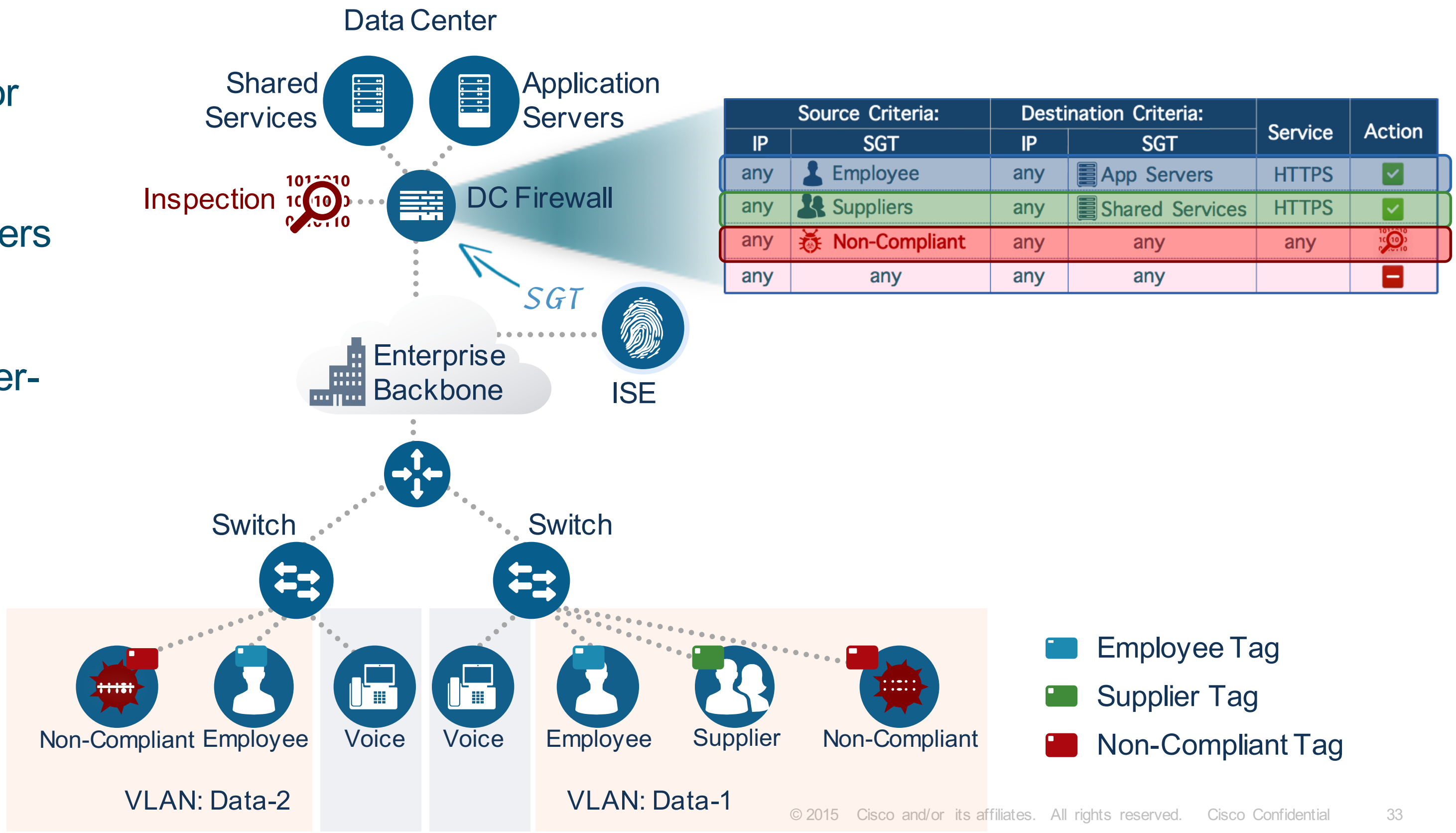
Design needs to be replicated for floors, buildings, offices, and other facilities. Cost could be extremely high



Context Based Application Access

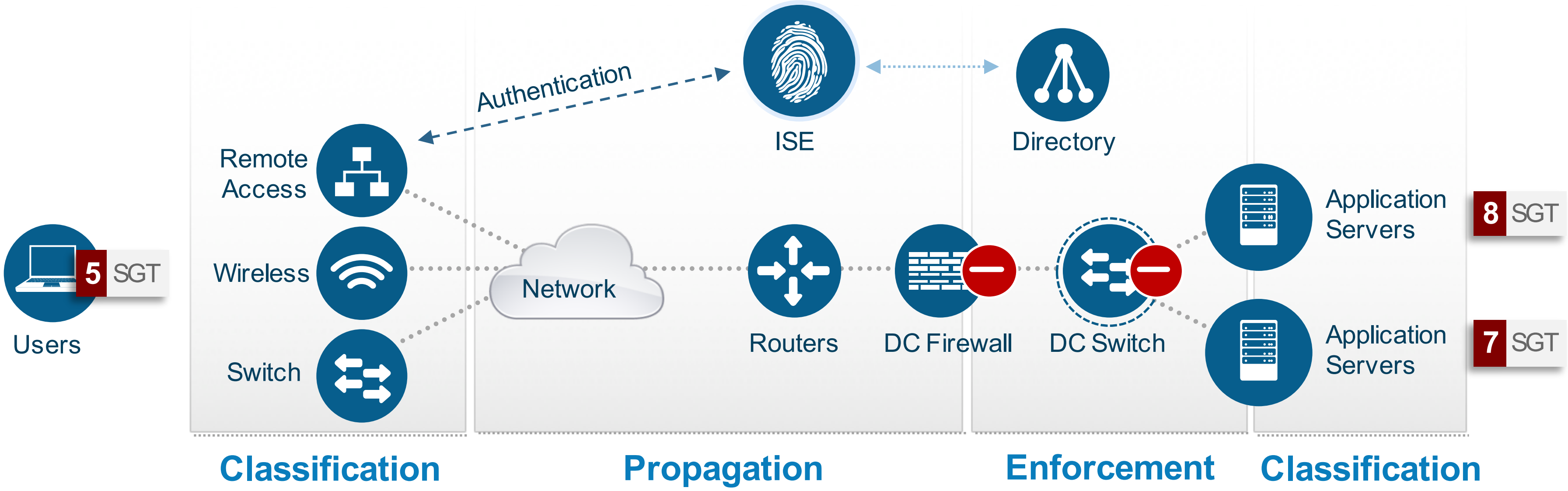
Regardless of topology or location, policy (Security Group Tag) stays with users, devices, and servers

TrustSec simplifies ACL management for intra/inter-VLAN traffic



Source Criteria:		Destination Criteria:		Service	Action
IP	SGT	IP	SGT		
any	Employee	any	App Servers	HTTPS	✓
any	Suppliers	any	Shared Services	HTTPS	✓
any	Non-Compliant	any	any	any	🔍
any	any	any	any		⛔

TrustSec in Action



TrustSec Functions

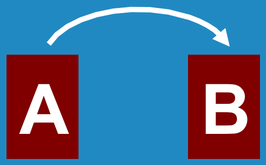
Classification

5	Employee
6	Supplier
8	Suspicious

Static

Dynamic

Propagation

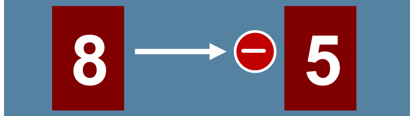


Inline

SXP

WAN

Enforcement



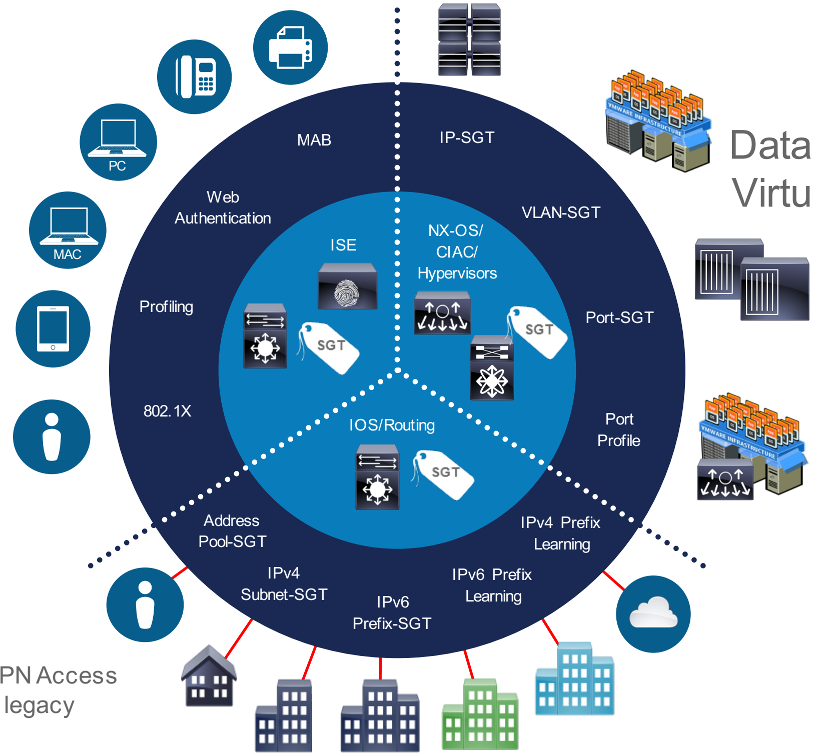
SGACL

SGFW

SGZBFW

How to Tag Users / Devices?

- TrustSec decouples network topology and security policy to simplify access control and segmentation
- Classification process groups network resources into Security Groups



User/Device/ Location Cisco Access Layer

Data Center/ Virtualization

Campus & VPN Access non-Cisco & legacy environment

Business Partners and Supplier Access Controls

MAB

Web Authentication

Profiling

802.1X

ISE

IP-SGT

VLAN-SGT

NX-OS/ CIAC/ Hypervisors

Port-SGT

Port Profile

IOS/Routing

Address Pool-SGT

IPv4 Subnet-SGT

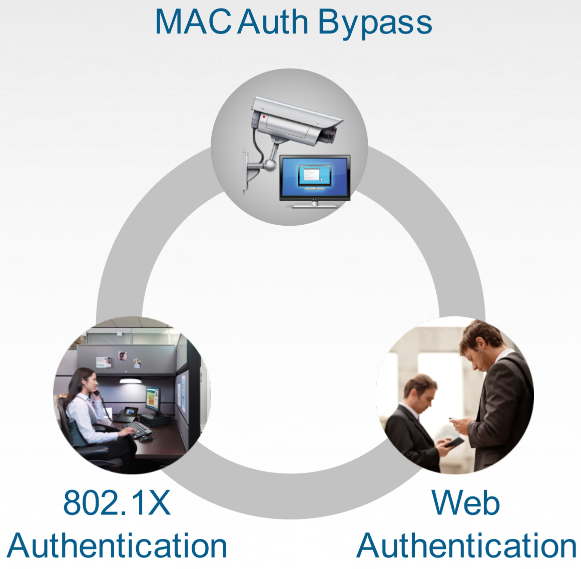
IPv6 Prefix-SGT

IPv6 Prefix Learning

IPv4 Prefix Learning

Classification Types

DYNAMIC CLASSIFICATION



Common Classification for Mobile Devices

STATIC CLASSIFICATION

IP Address

VLANs

Subnets

L2 Interface

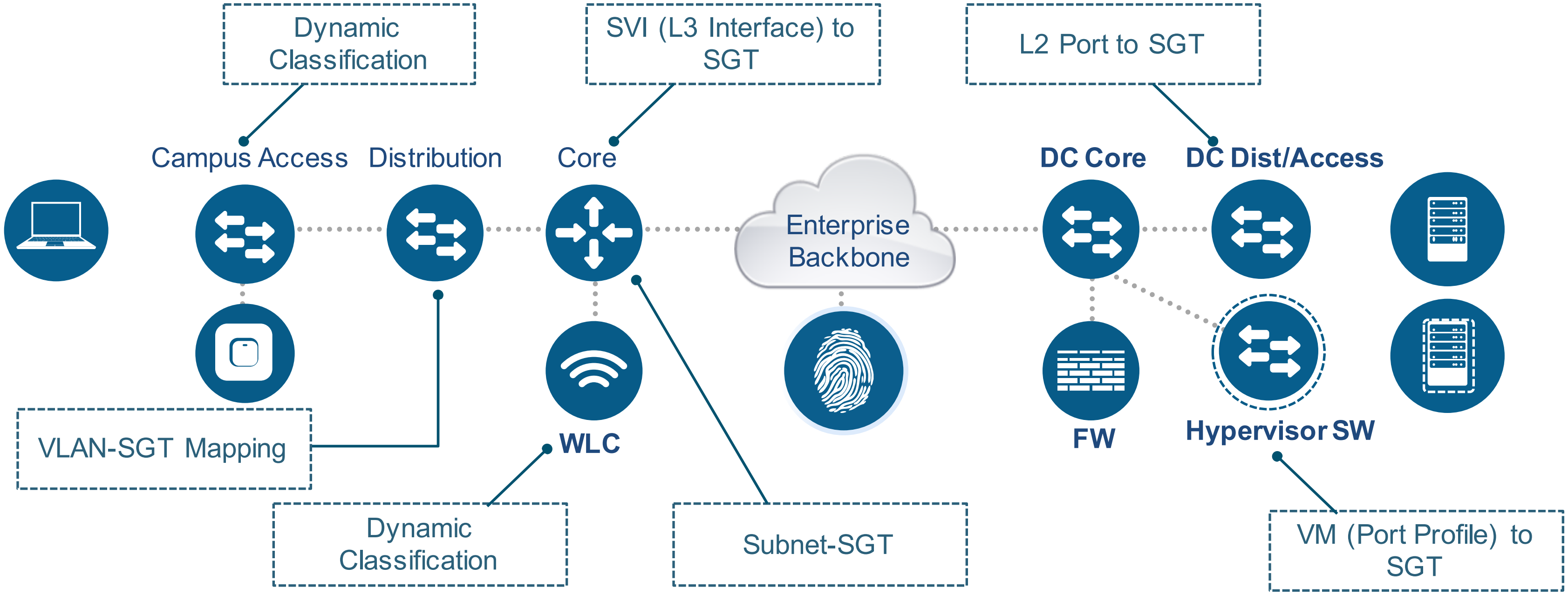
L3 Interface

Virtual Port Profile

Layer 2 Port Lookup

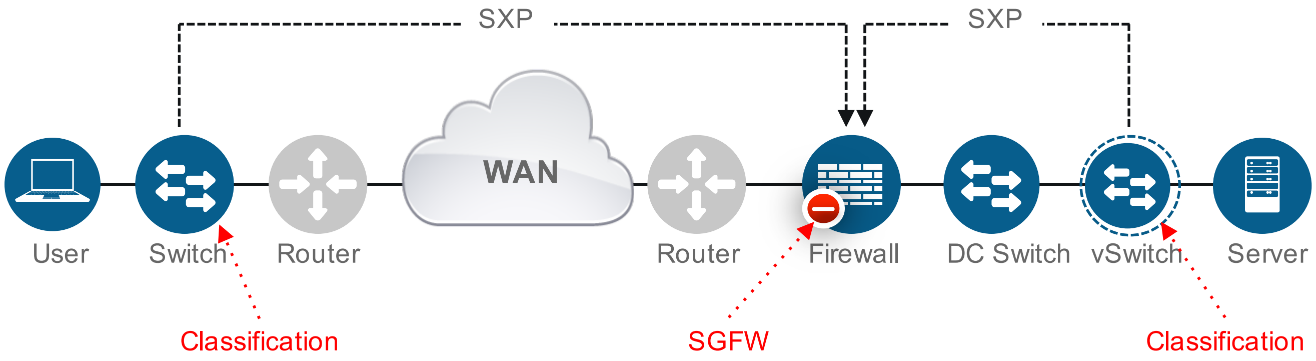
Common Classification for Servers, Topology-based Policy, etc.

Assigning Security Group Tags

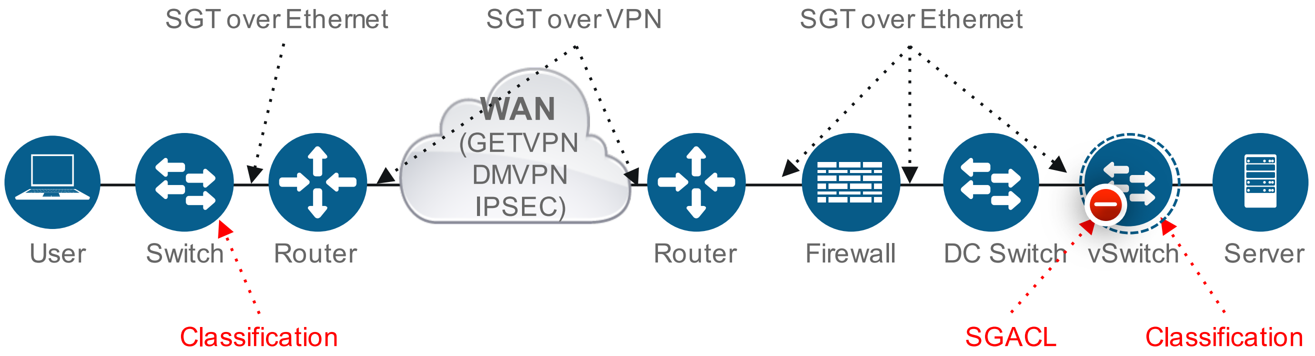


Propagation Options

Heterogeneous Network Support



TrustSec Fully Supported Network



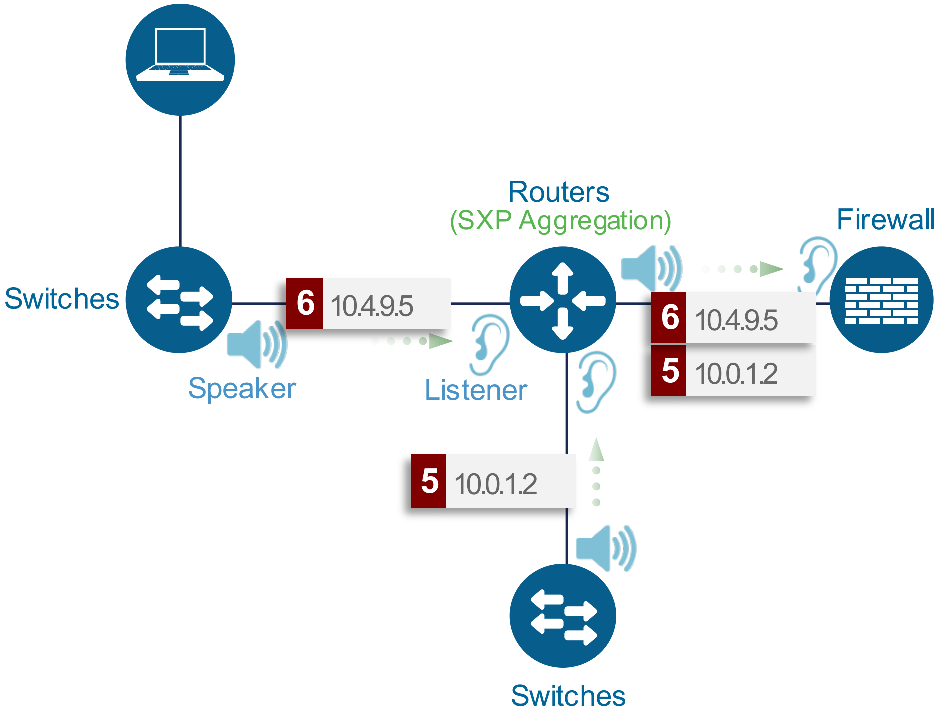
SXP/SGToEthernet are on Internet Draft

https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/

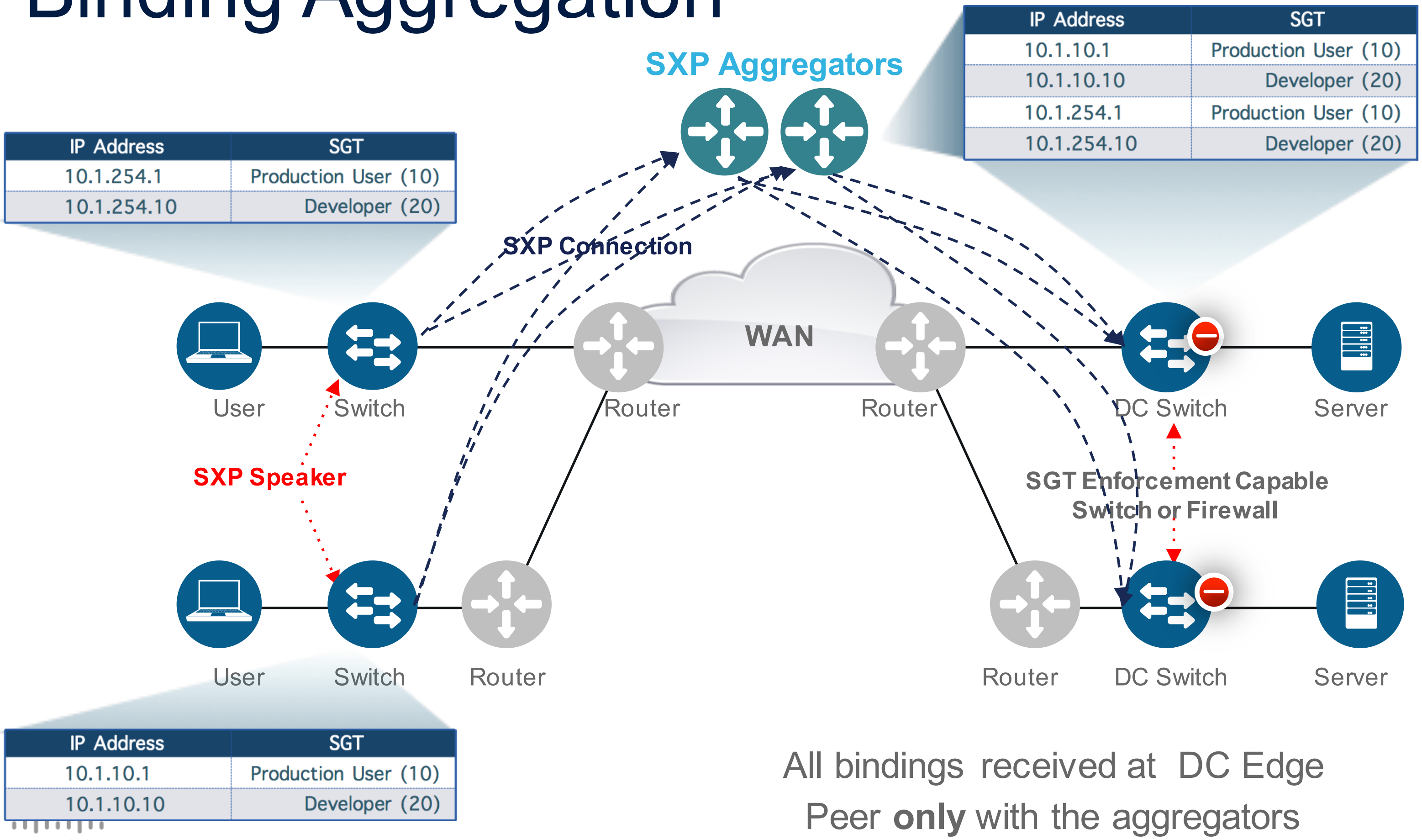
https://wiki.opendaylight.org/images/6/6c/SXP_Specification_and_Architecture_v00.pdf

SGT Exchange Protocol (SXP)

- Propagation method of IP-SGT binding
  - Propagate IP-SGT from classification to enforcement point
- Open protocol (IETF-Draft) & ODL Supported
  - TCP - Port:64999
- Role: Speaker (initiator) and Listener (receiver)
- Use MD5 for authentication and integrity check
- Support Single Hop SXP & Multi-Hop SXP (aggregation)



Binding Aggregation



IP Address	SGT
10.1.10.1	Production User (10)
10.1.10.10	Developer (20)
10.1.254.1	Production User (10)
10.1.254.10	Developer (20)

IP Address	SGT
10.1.254.1	Production User (10)
10.1.254.10	Developer (20)

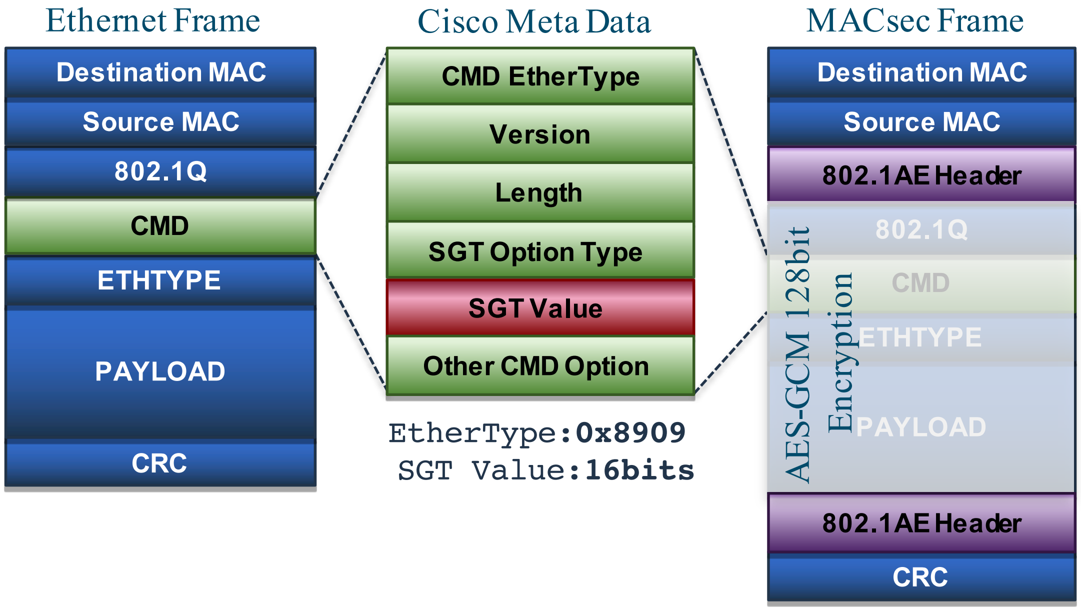
IP Address	SGT
10.1.10.1	Production User (10)
10.1.10.10	Developer (20)

All bindings received at DC Edge

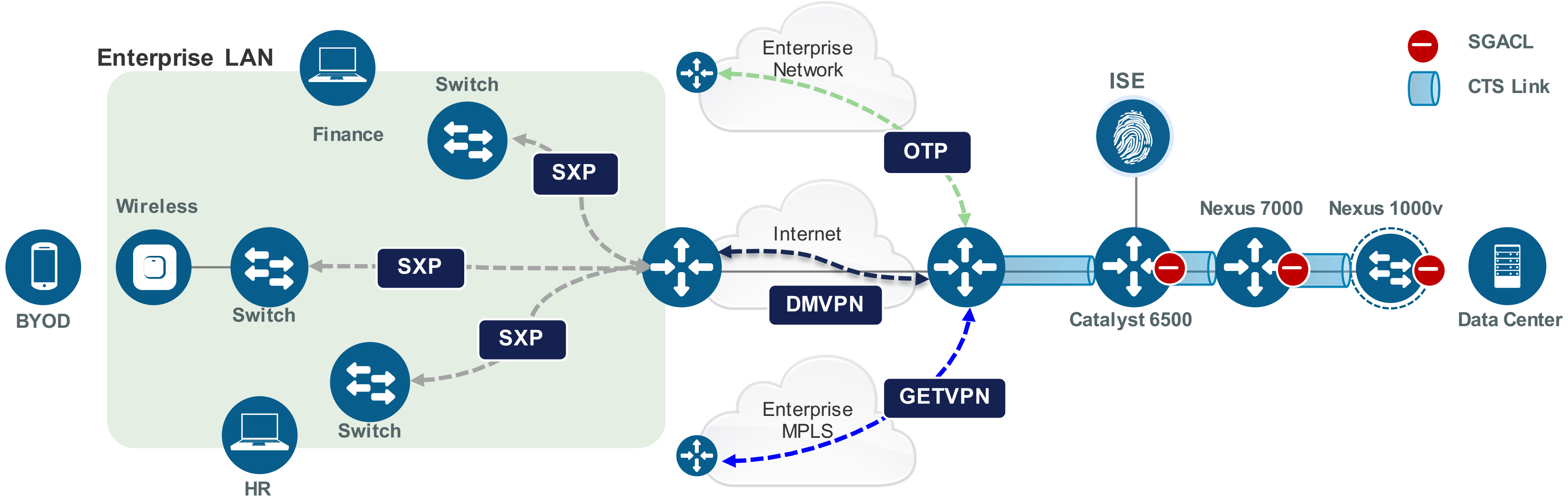
Peer **only** with the aggregators

High Speed Tag Propagation
(L2 Frame Embedded Tag)

- Faster, and most scalable way to propagate SGT within LAN or Data Center
- SGT embedded within Cisco Meta Data (CMD) in Layer 2 frame
- Capable switches understands and process SGT in line-rate
- Protected by enabling MACsec (IEEE802.1AE) – optional for capable hardware
- No impact to QoS, IP MTP/Fragmentation
- L2 Frame Impact: ~20 bytes
- 16 bits field gives ~ 64,000 tag space
- Non-capable device drops frame with unknown Ethertype

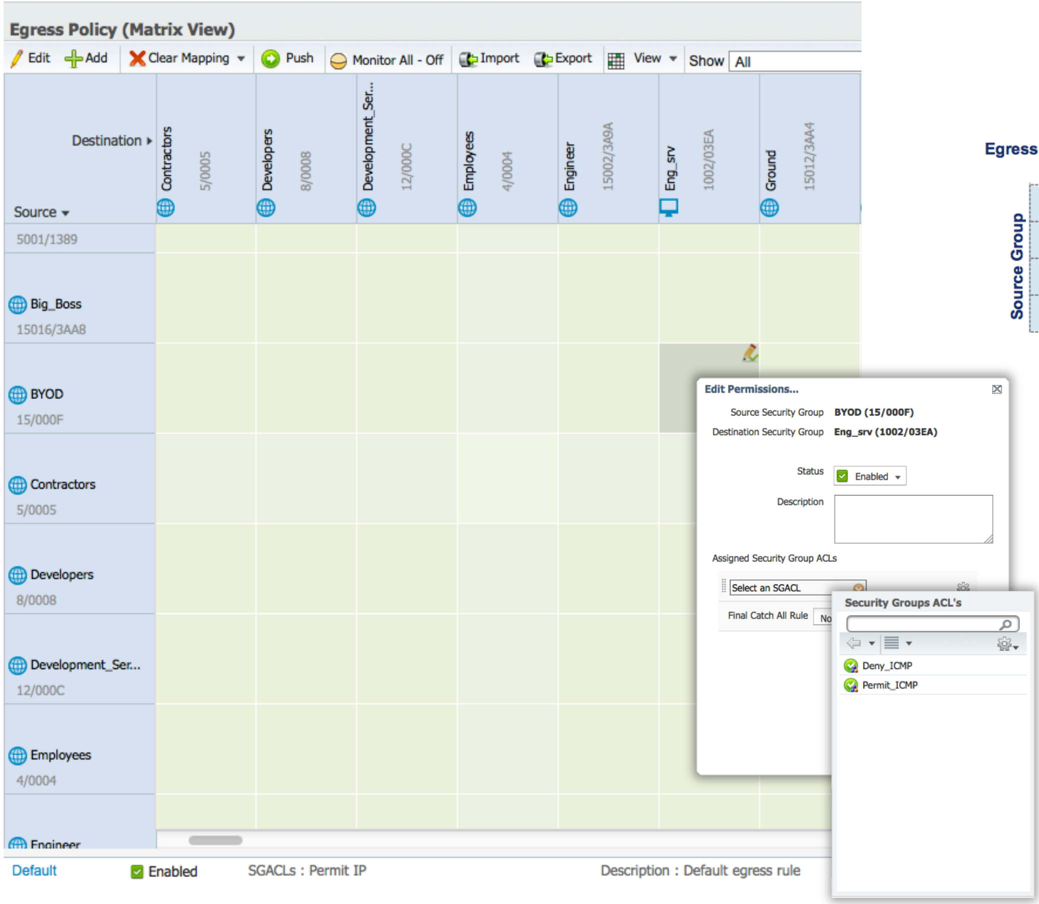


SGT Transport over L3 networks



- Multiple options for SGT transport over non CTS Layer 3 networks
- DMVPN for Internet based VPNS
- GETVPN for security private MPLS clouds
- Over The Top (OTP) for private enterprise networks (1HCY15)

SGACL Egress Matrix on ISE 2.0



Source ▾ \ Destination ▸	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Employees 4/0004	Engineer 15002/3A9A	Eng_srv 1002/03EA	Ground 15012/3A44
5001/1389							
Big_Boss 15016/3AA8							
BYOD 15/000F							
Contractors 5/0005							
Developers 8/0008							
Development_Ser... 12/000C							
Employees 4/0004							
Engineer							

Default ☑ Enabled SGACLs : Permit IP Description : Default egress rule

Edit Permissions...

Source Security Group BYOD (15/000F)

Destination Security Group Eng_srv (1002/03EA)

Status ☑ Enabled

Description

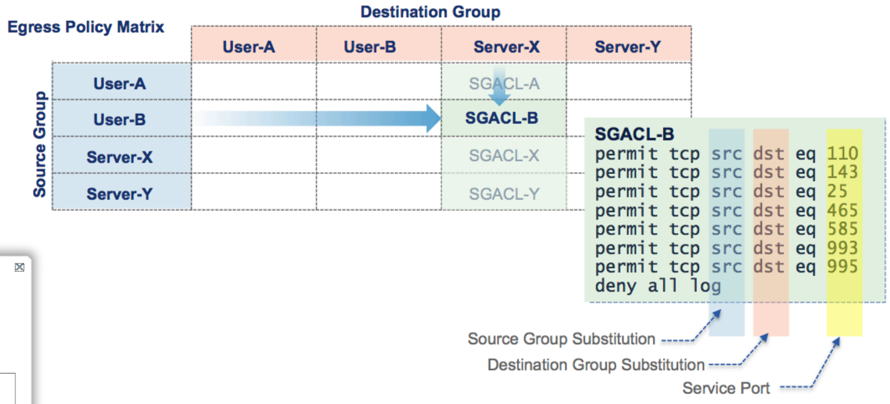
Assigned Security Group ACLs

Select an SGACL

Final Catch All Rule No

Security Groups ACL's

- Deny_ICMP
- Permit_ICMP



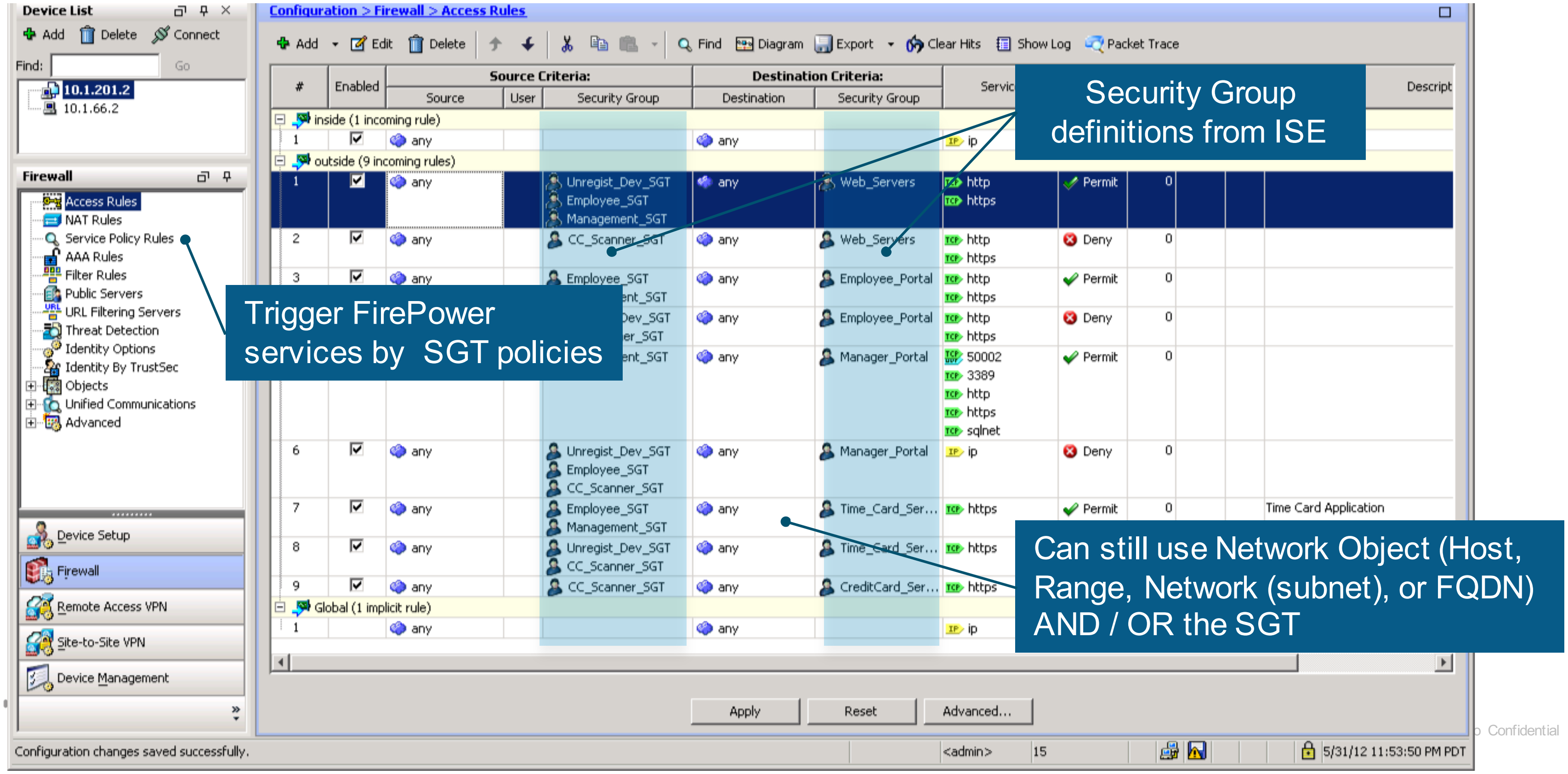
Egress Policy Matrix

Source Group \ Destination Group	User-A	User-B	Server-X	Server-Y
User-A			SGACL-A	
User-B			SGACL-B	
Server-X			SGACL-X	
Server-Y			SGACL-Y	

SGACL-B

```
permit tcp src dst eq 110
permit tcp src dst eq 143
permit tcp src dst eq 25
permit tcp src dst eq 465
permit tcp src dst eq 585
permit tcp src dst eq 993
permit tcp src dst eq 995
deny all log
```

Firewall Policy based on SGT



Device List

Add Delete Connect

Find: Go

- 10.1.201.2
- 10.1.66.2

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity By TrustSec
- Objects
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Firewall > Access Rules

Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

#	Enabled	Source Criteria:			Destination Criteria:		Servic					Descript
		Source	User	Security Group	Destination	Security Group						
inside (1 incoming rule)												
1	☑	any			any		ip					
outside (9 incoming rules)												
1	☑	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit	0			
2	☑	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny	0			
3	☑	any		Employee_SGT ent_SGT	any	Employee_Portal	http https	Permit	0			
				Dev_SGT er_SGT	any	Employee_Portal	http https	Deny	0			
				ent_SGT	any	Manager_Portal	50002 3389 http https sqlnet	Permit	0			
6	☑	any		Unregist_Dev_SGT Employee_SGT CC_Scanner_SGT	any	Manager_Portal	ip	Deny	0			
7	☑	any		Employee_SGT Management_SGT	any	Time_Card_Ser...	https	Permit	0			Time Card Application
8	☑	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Time_Card_Ser...	https					
9	☑	any		CC_Scanner_SGT	any	CreditCard_Ser...	https					
Global (1 implicit rule)												
1		any			any		ip					

Apply Reset Advanced...

Configuration changes saved successfully. <admin> 15 5/31/12 11:53:50 PM PDT

Security Group definitions from ISE

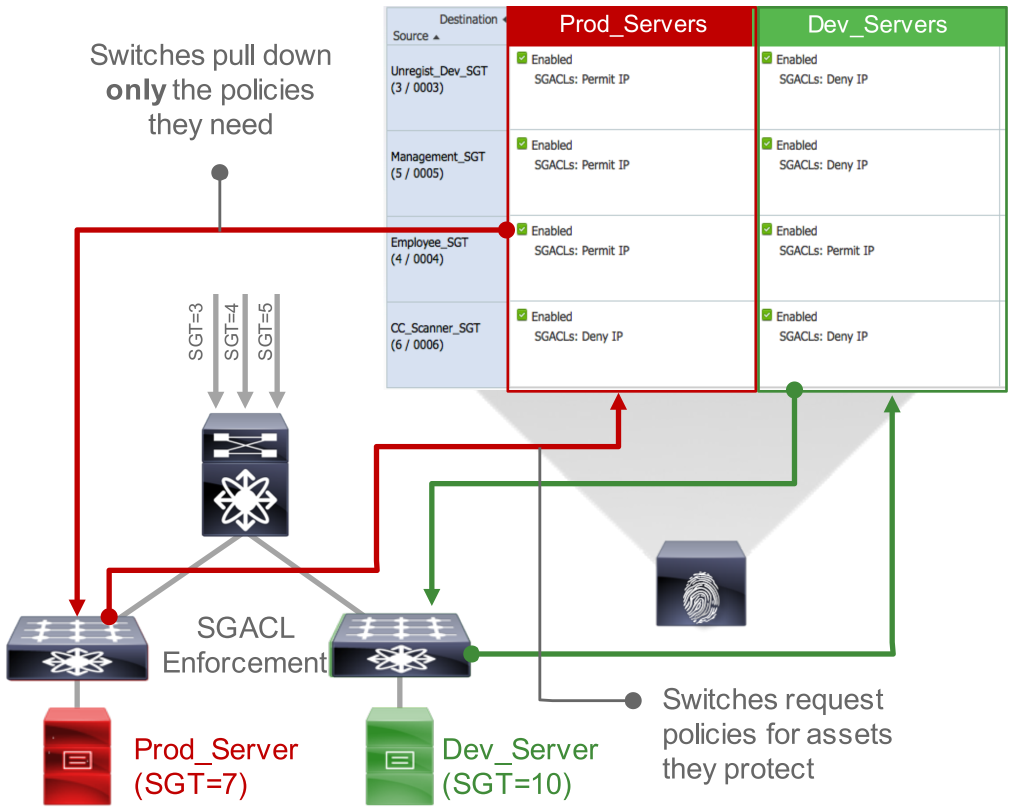
Trigger FirePower services by SGT policies

Can still use Network Object (Host, Range, Network (subnet), or FQDN) AND / OR the SGT

SGACL Scaling Segmentation

- New User/Device/Servers provisioned, e.g Prod Server and Dev Server Roles
- TrustSec switch requests policies for assets they protect
- Policies downloaded & applied dynamically
- Result: Software-Defined Segmentation
  - All controls centrally managed
  - Security policies de-coupled from network topology
  - **No switch-specific security** configs needed
  - One place to audit network-wide policies
  - Scales via two mechanisms
    - Put destination SGT in FIB, derive source SGT from frame/FIB
    - Only protocol/port information put into TCAM

SEGMENTATION DEFINED IN ISE

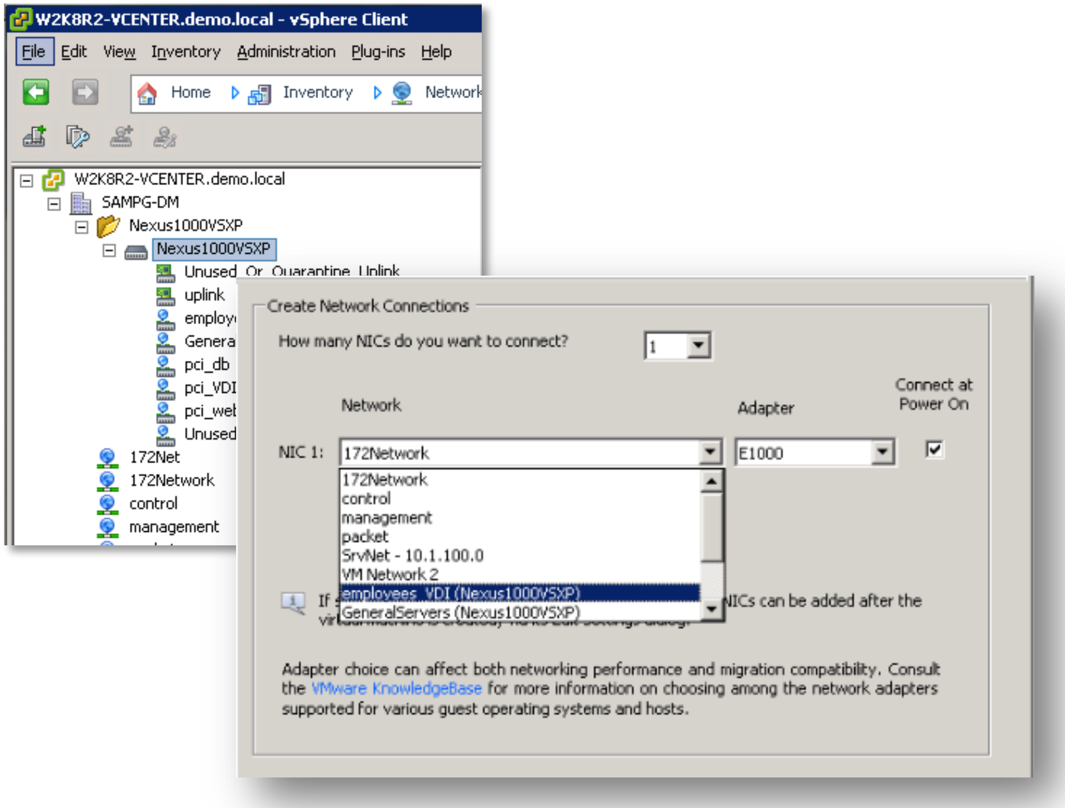


Destination ▸ Source ▴	Prod_Servers	Dev_Servers
Unregist_Dev_SGT (3 / 0003)	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Deny IP
Management_SGT (5 / 0005)	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Deny IP
Employee_SGT (4 / 0004)	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Permit IP
CC_Scanner_SGT (6 / 0006)	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: Deny IP

Switches pull down **only** the policies they need
SGT=3
SGT=4
SGT=5
SGACL Enforcement
Prod_Server (SGT=7)
Dev_Server (SGT=10)
Switches request policies for assets they protect

Classifying Virtual Machines in DC : Nexus 1000v

- Port Profile
  - Container of network properties
  - Applied to different interfaces
- Server Admin may assign Port Profiles to new VMs
- VMs inherit network properties of the port-profile including SGT
- SGT stays with the VM even if moved



Create Network Connections

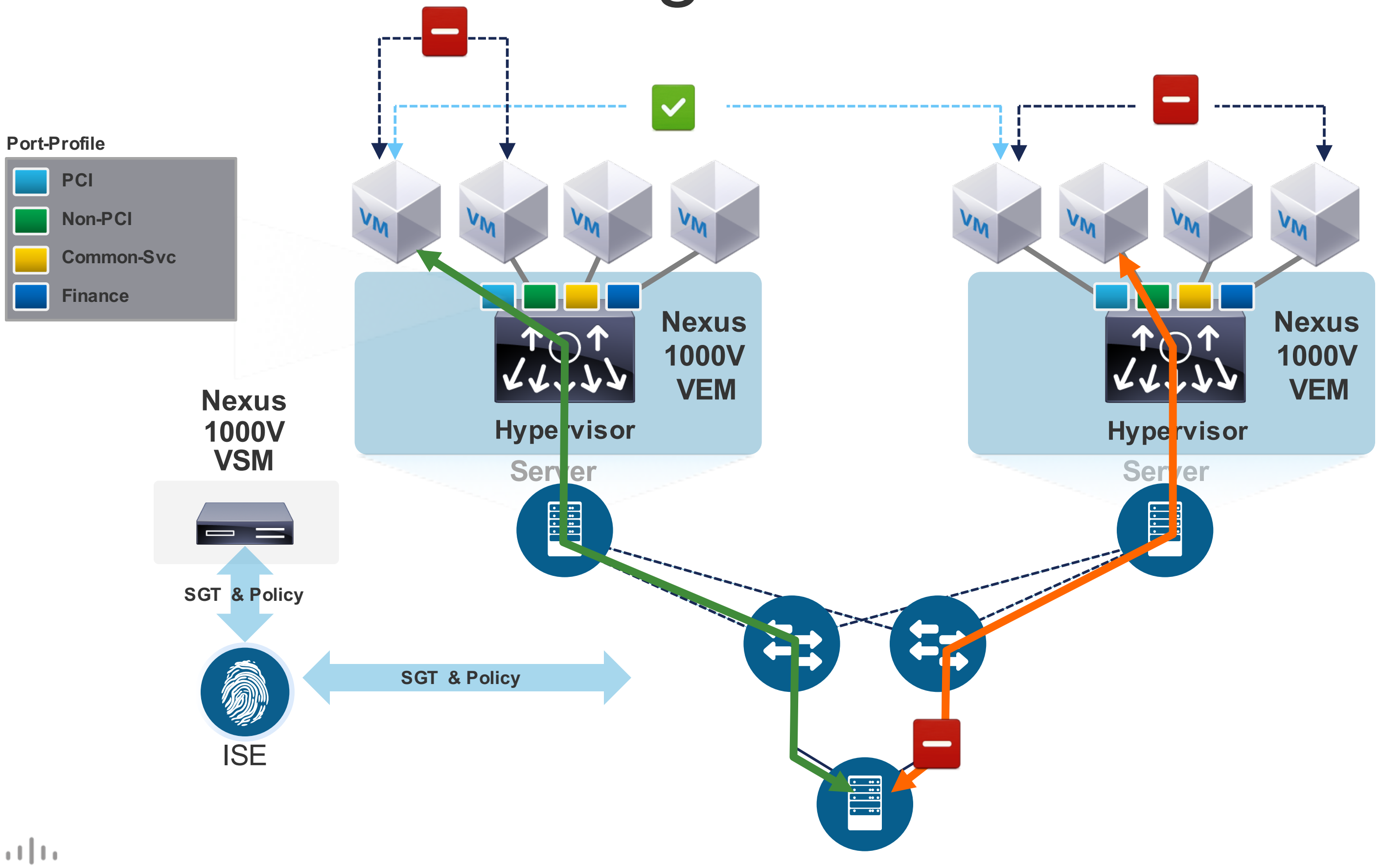
How many NICs do you want to connect? 1

NIC 1: 172Network E1000 ☑

If NICs can be added after the vir

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

TrustSec Micro Segmentation with Nexus 1000v



TrustSec in the Data Center

Common policy objects (tags) used throughout FW and ACL logic

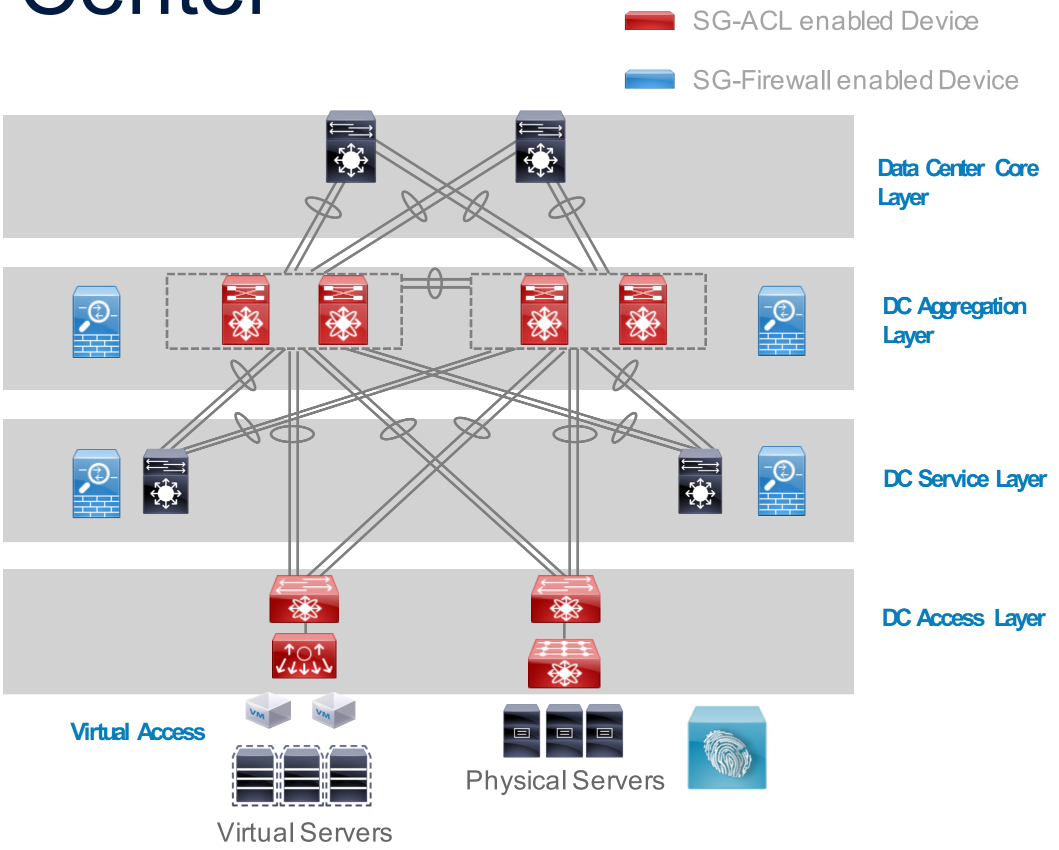
- Consistent semantics
- Centralized ACL definition & automation
- Scalable policy enforcement

Security Group Firewalling 🟦

Firewall rule automation using ASA SG-Firewall functions

Security Group ACLs 🟥

- Segmentation defined in a simple policy matrix
- Applied across Nexus switches – scalable and simple


🟥 SG-ACL enabled Device
🟦 SG-Firewall enabled Device
Data Center Core Layer
DC Aggregation Layer
DC Service Layer
DC Access Layer
Virtual Access
VM
VM
Virtual Servers
Physical Servers