Cisco Identity Services Engine (ISE)

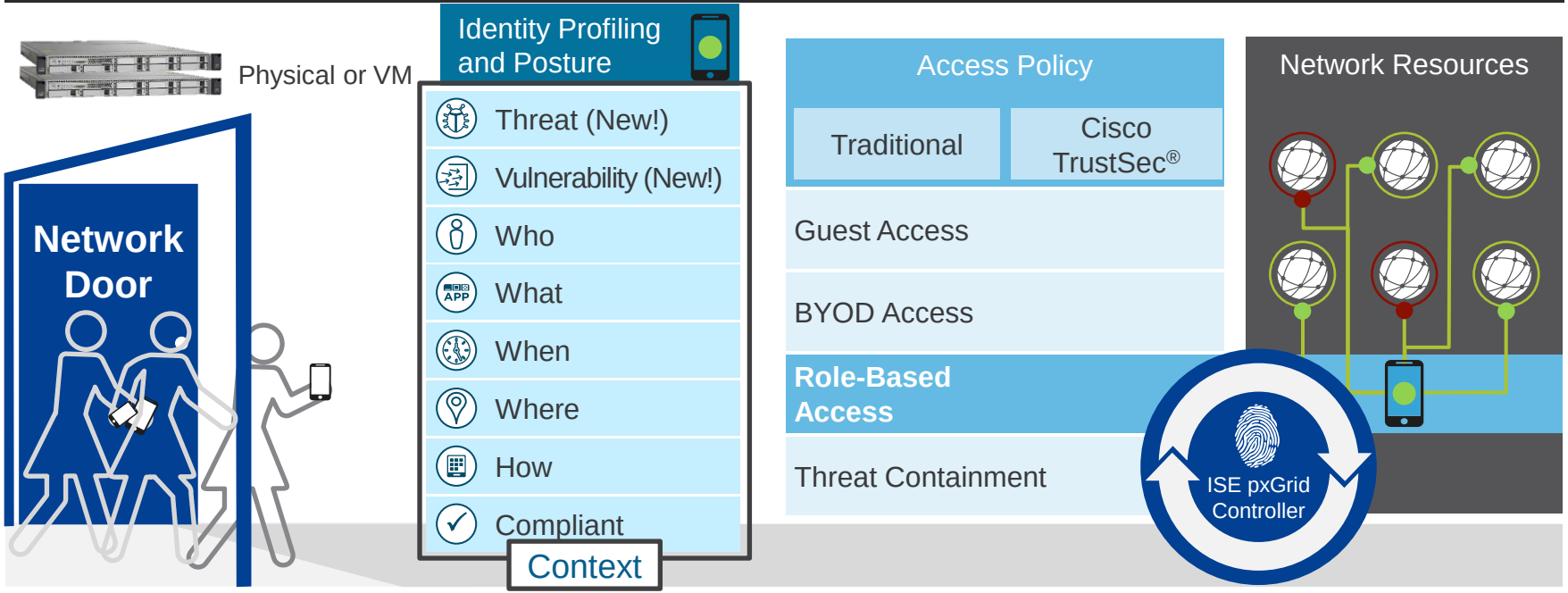
Mobility Roadshow

Jaroslav Čížek, Cisco

November 2016

Introducing Cisco Identity Services Engine

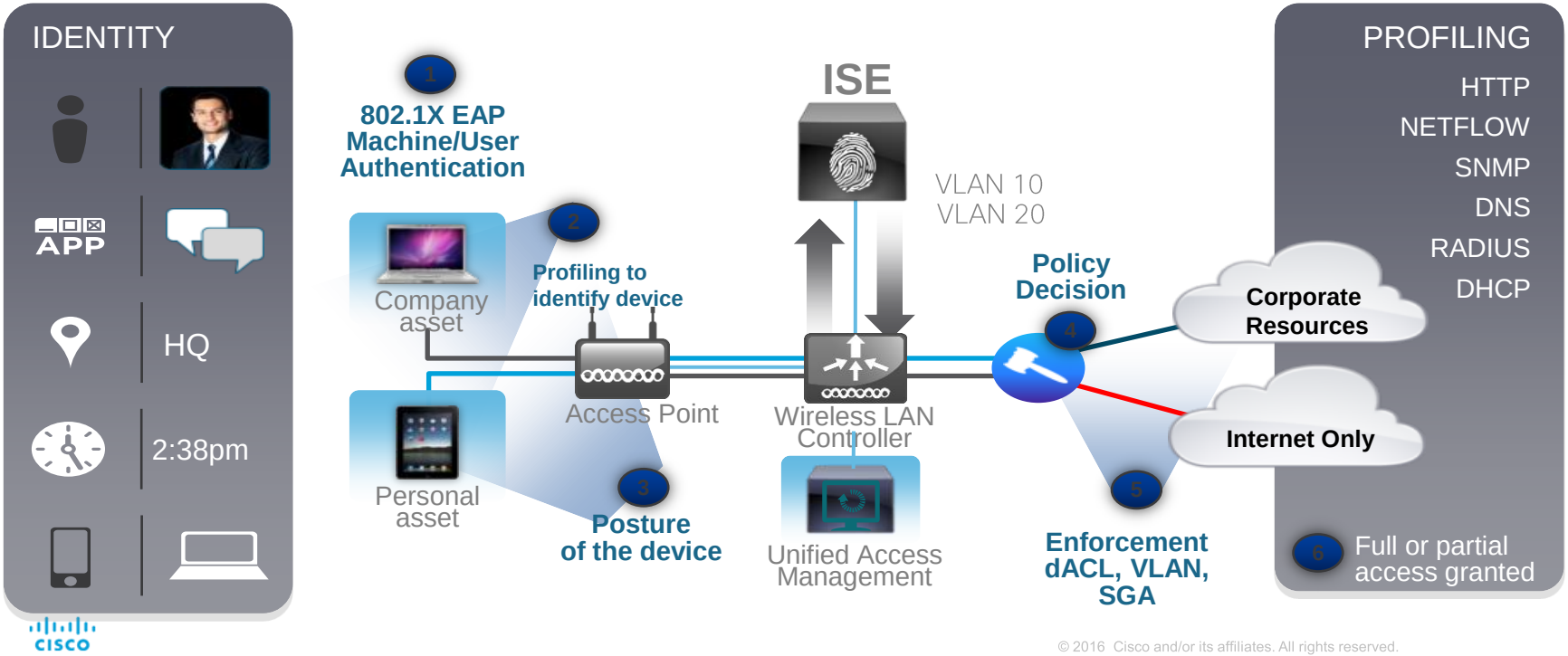
A centralized security solution that automates context-aware access to network resources and shares contextual data



- ***ISE Portal Builder*** – build your own guest portals here - https://isepb.cisco.com
- ***ISE Guest Setup Wizard App*** - Configure ISE and WLC at the same time.
- ***ISE Express Bundle*** - Cisco ISE in an entry-level bundle offered at an aggressive discount

Client Context and Policies

Control and Enforcement



Rich Data Sharing Enhances Protection Across the Attack Continuum

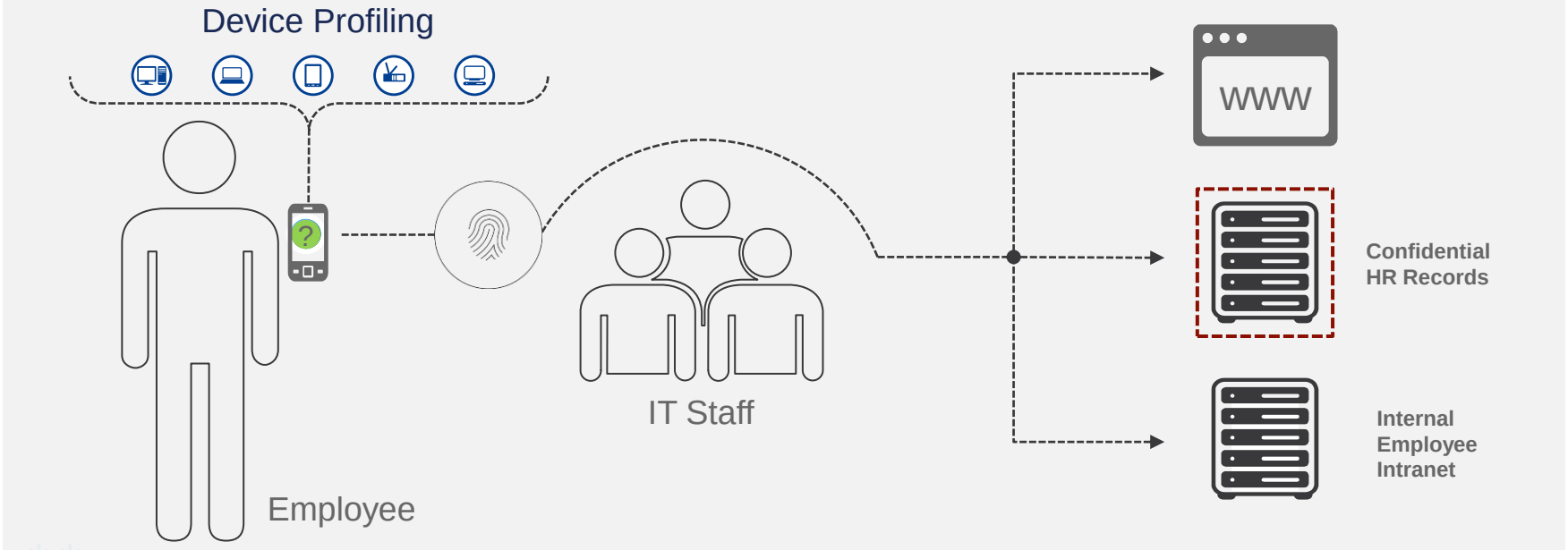
- Gain visibility into who and what is on your network
- Grant access on a "need to know" basis

- Provide threat context to network behavioral analysis
- Contain through network elements and security ecosystem

- Get better forensics and prepare for the next attack by sharing information with ecosystem partners

Enable Faster and Easier Device Onboarding without Any IT Support

Rapid device identification with out-of-the-box profiles	Simplified device management from self-service portal	Automated authentication and access to business assets



Metrics

Total Endpoints	Active Endpoints	Authenticated Guests	BYOD Endpoints	Posture C
4282	3725	0	27	pending: 21%

System Summary

1 nodes

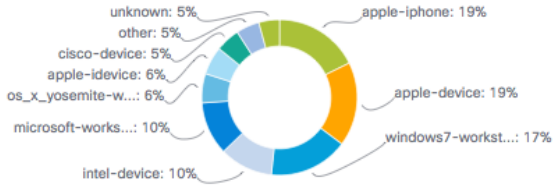
CPU | 24HR

ise-1

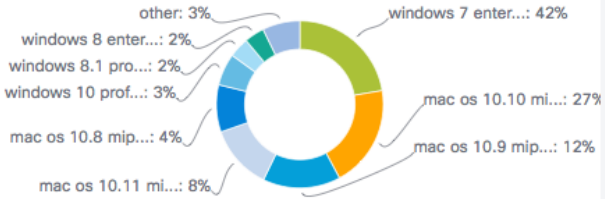
Last refreshed: Tue Feb 02 2016 19:18:01 GMT-0800 (PST)

Profiles

Endpoint Profile



OS Types



Last refreshed: Tue Feb 02 2016 19:18:01 GMT-0800 (PST)

Alarms

Se...	Name	Occur...	Last Oc
⚠	ISE Authentication Inactivity	71	11 days a
ℹ	Configuration Changed	243	11 days a
✖	High Load Average	72	11 days a

Network Devices

Network Device | Device Type | Location

Authentications

Identity Store | Identity Group | Network Device | Failure Reason

ISE use cases

NOTE: To apply the Device Admin, Plus, or ISE Apex licenses, Base licenses must be installed first.

Features included by license type

Benefit	Use case	Base *Perpetual*				Device Admin* *Perpetual*	Plus *Term (1,3,5 year)*					ISE Apex + AnyConnect Apex *Term (1,3,5 year)*		
		RADIUS / 802.1x	AAA	TrustSec security group tagging	Guest services	TACACS+	Rapid threat containment	ANC/EPS	Device profiling and feed service	BYOD with CA	pxGrid context sharing	MDM / EMM	Threat-Centric NAC	Posture (endpoint compliance and remediation)
Control all access from one place	**Guest** Provide unique guest permissions to visitors	●	●		●									
	Secure access Control user access and ensure device authentication	●	●	●										
	Device Admin Differentiate access for device administrators					●								
	BYOD Seamlessly onboard devices with the right access	●	●	●					●	●				
See and share rich user and device details	**Visibility** See when, where, and why users are on your network	●	●	●					●					
	Integration Share information with other products	●	●	●					●		●			
	Compliance Ensure that endpoints meet network standards	●	●	●								●		●
Stop threats from getting in and spreading	**Segmentation** Limit exposure with pre-defined access segmentation	●	●	●										
	Containment Reduce risk with rapid threat containment	●	●	●			●	●	●					
	Prevention Prevent breaches at the endpoint level	●	●	●									●	

What's New in 2.1?

- EasyConnect
- Context Visibility
  - Customizable Dashboard
  - Expanded Profiling Capabilities
- Threat Centric NAC
- **TrustSec Workflow Enhancements**
- TrustSec / ACI Policy Plane Integration

- **(Much!) Expanded 3rd Party Support**
- Major ACS Parity Features
- Compliance & MDM Enhancements
- **BYOD Stand-Up Enhancements**
- **Guest Enhancements**
- New Hardware == New Performance

Wireless TrustSec Support

User to Data Center Access Control

- Context--based access control
- Compliance requirements PCI, HIPAA, export controlled information
- Merger & acquisition integration, divestments

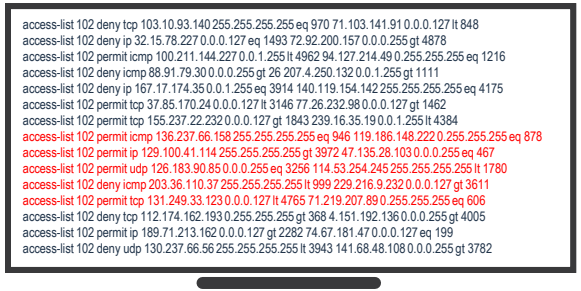
Campus and Branch Segmentation

- Line of business segregation
- PCI, HIPAA and other compliance regulations
- Malware propagation control/quarantine

Feature	Platform
Inline SGT tagging and SG-ACL enforcement	17xx, 27xx,37xx, 18xx, 28xx, 1560 and 38xx 5520 and 8540
SXPv2	5520, 8540, 8510, 7510, vWLC, 5508, WISM2, 2504
SXPv4	17xx, 27xx,37xx, 18xx, 28xx, 1560 and 38xx

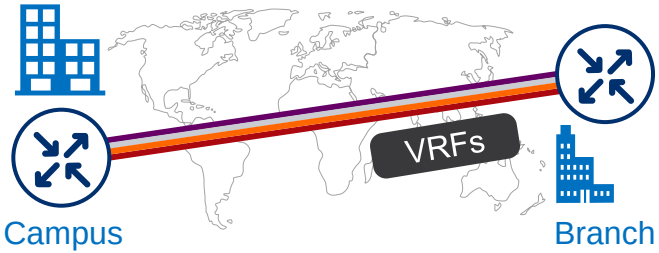
Simple scalable software-defined-access based segmentation and policies

The Segmentation Challenge



Complex IP based policies

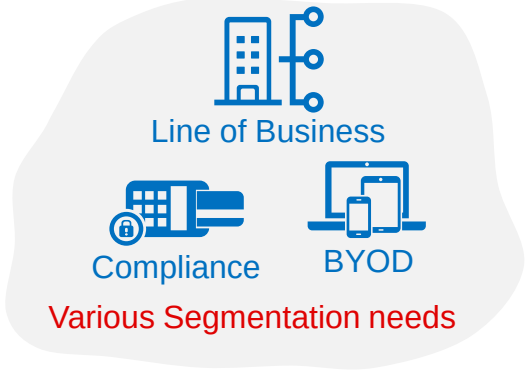
Need updates as topology changes



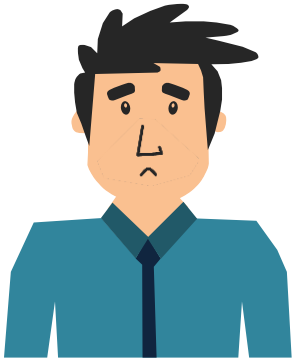
- Employees
- Contractors
- Vendors
- Guests
- PCI Devices

VLANs

Extend segments over - Layer 3 boundaries



Various Segmentation needs

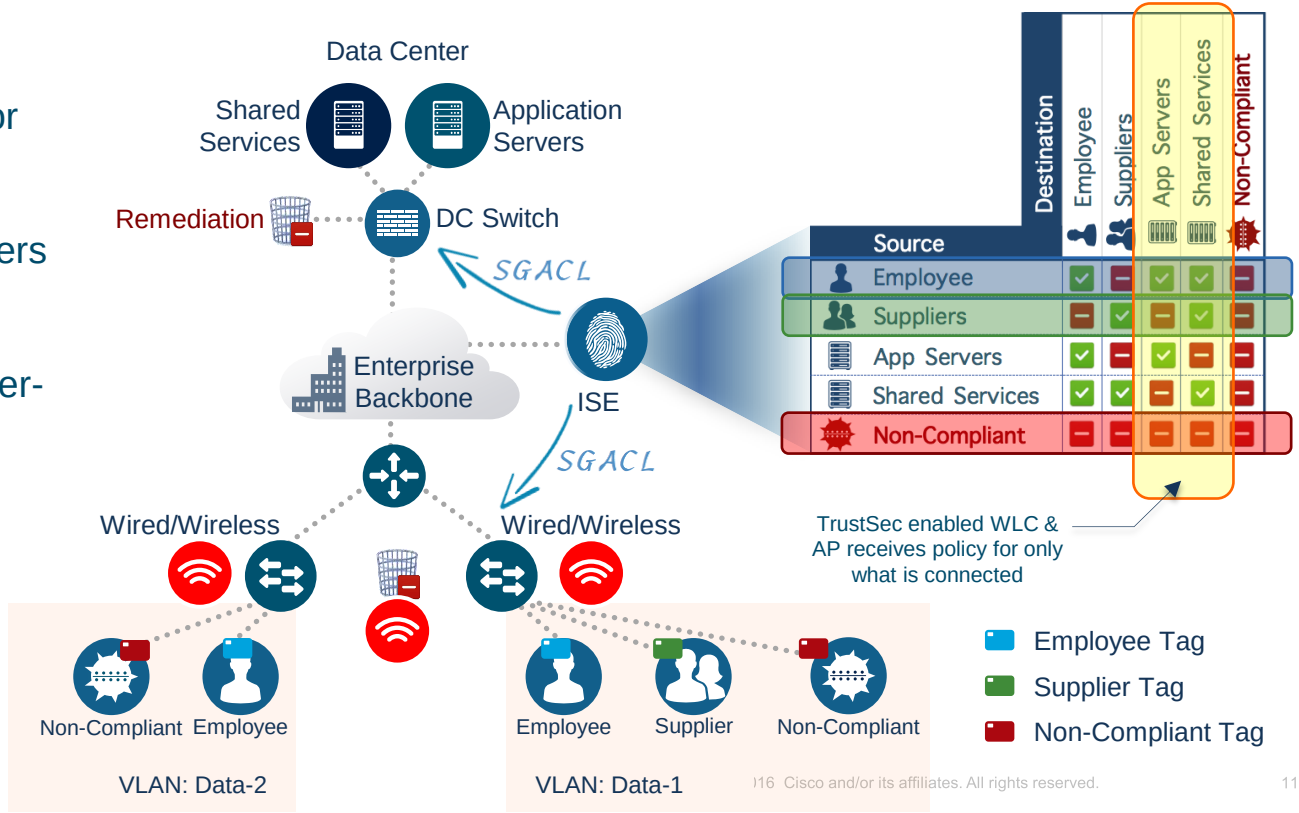


Retain Security & Compliance as network expand and grow

Simplified and Consistent Access governed by TrustSec

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

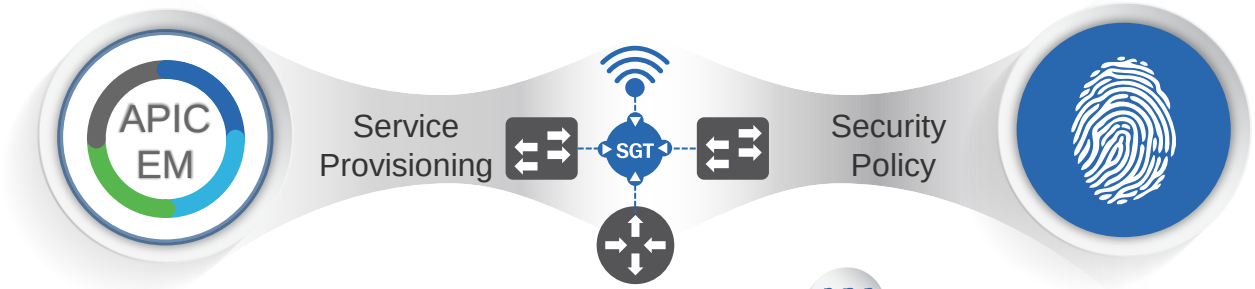
TrustSec simplifies ACL management for intra/inter-VLAN traffic



Cisco DNA and ISE

Network Controller

ISE



- Discover Network Asset & Services
- Check Network Service Readiness
- Provision & Manage Configuration
- Enable additional services instantly
- Provision Network Service Changes

- Identify User and Endpoints
- Profile and Classify devices
- Automate On-Boarding
- Automated Security Policy Provisioning Inside/outside fabric
- Sync groups with security apps and other controllers


CISCO