



# Tablets and Smartphones Welcomed!

How to Get Any Device on Any Network Reliably and Securely

Emerging East - One Cisco

# Agenda

- Introduction
- Identity Services Engine
- ISE Architecture
- ISE as a Cisco differentiator
- Emerging East ISE demo labs
- Call to action
- Q and A



# Introduction

# Own device vs. business usage

## “Bring Your Own Device”, BYOD



# BYOD: Bring Your Own Device Access Challenges

## IT Is Struggling With:

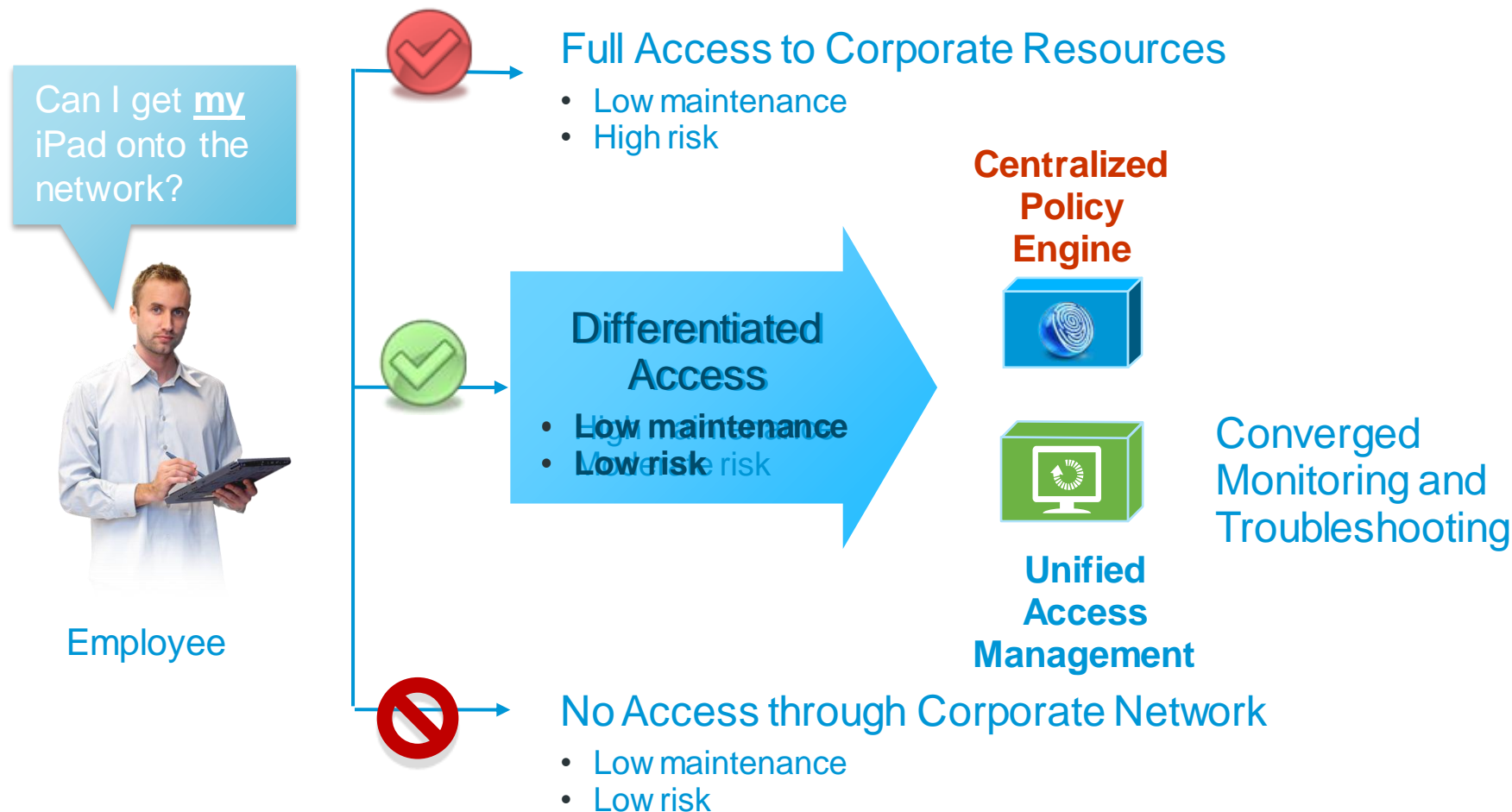
- Classifying managed vs unmanaged endpoints
- ID devices that cannot authenticate
- Users to devices

## But There **are** Barriers:

- Multiple access mediums
- Endpoint certainty
- No automated way to discover new endpoints



# Typical Policy Options



# Comprehensive Policy Solution for Any Device Is Required

## Purpose-Built, Complete, and Reliable Profiling

- Wide variety of protocols used: SNMP, NetFlow, DNS, RADIUS, HTTP, and DHCP to increase accuracy, reduce spoofability
- Unified solution for wired and wireless
- Completely integrated with RADIUS/AAA
- Additional services (posture, guest/portal, etc.)

## Scalable Policy Enforcement

- Switch, WLAN controller, and VPN as an enforcement point
- Flexible control (VLAN, dACL/ACL, QoS, SGA, etc.) based on any contextual attributes (user, device, group, location, time, etc.)

## Unified Management

- Detailed reporting and troubleshooting tools (user, device, session, etc.) and integration with network management platform providing a single pane of glass into user, device, and network across wired and wireless infrastructure



# Please, Ask Yourself the Following Questions

- Do you ...
  - want an integrated access management for wired, wireless and VPN infrastructures?
  - see a problem with a fact that well defended network perimeter disappeared?
  - have to follow regulatory compliance requirements?
  - have problem with new devices in the network, like “BYOD”?



If the answer is yes to at least one question, please stay with us and you will learn the answer...



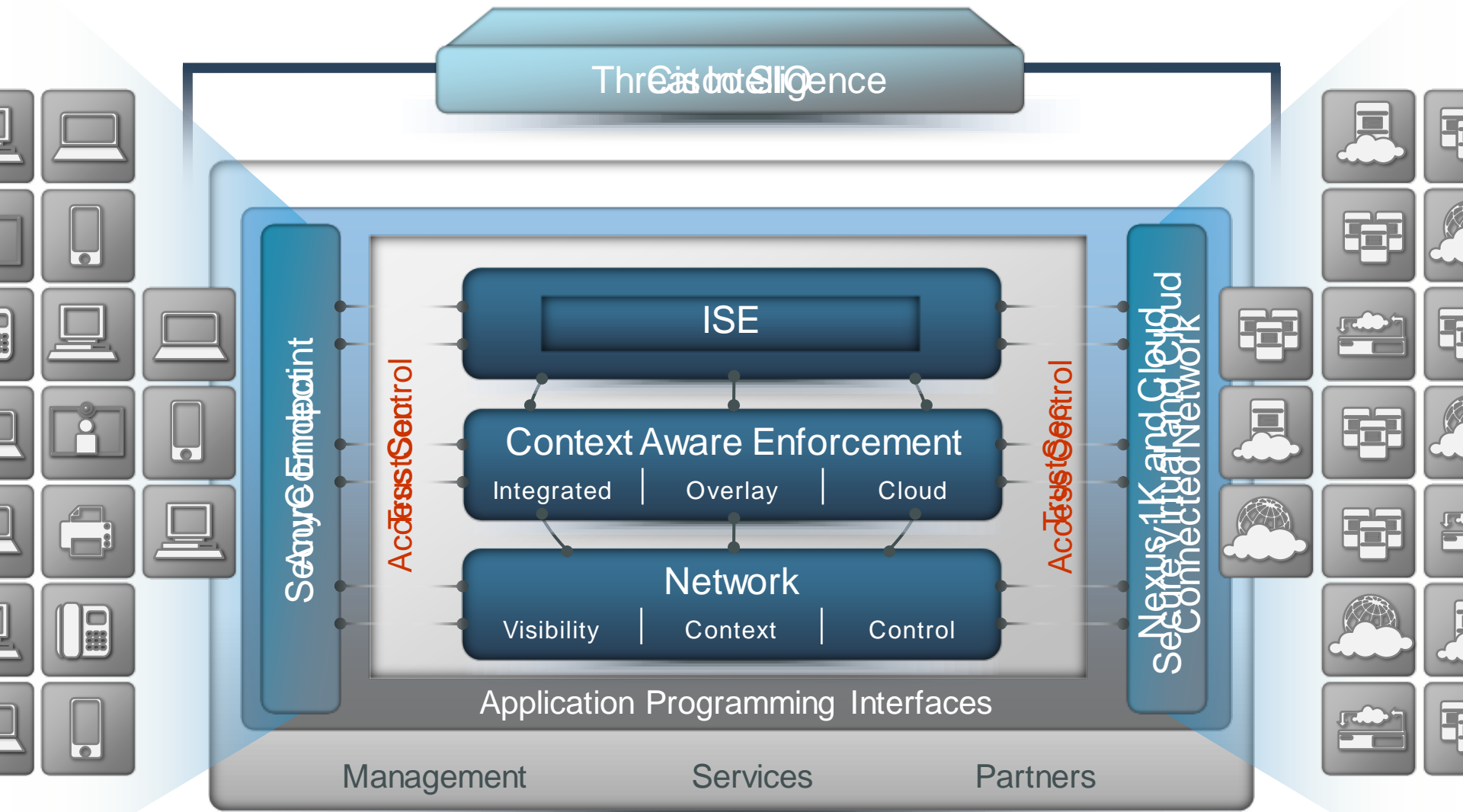


# Identity Services Engine

# Cisco Borderless Network Architecture



# Cisco SecureX Architecture



# Cisco Trustsec: Identity Services Engine

ISE: Policies for people and devices



## Authorized Access

- How can I restrict access to my network?
- Can I manage the risk of using personal PCs, tablets, smart-devices?
- Access rights on-prem, at home, on the road?
- Devices are healthy?



## Guest Access

- Can I allow guests Internet-only access?
- How do I manage guest access?
- Can this work in wireless and wired?
- How do I monitor guest activities?



## Non-User Devices

- How do I discover non-user devices?
- Can I determine what they are?
- Can I control their access?
- Are they being spoofed?

# Two-Year Roadmap Outlook

## Converged Policy Platform

NAC ACS  
Guest  
Profiler

ISE

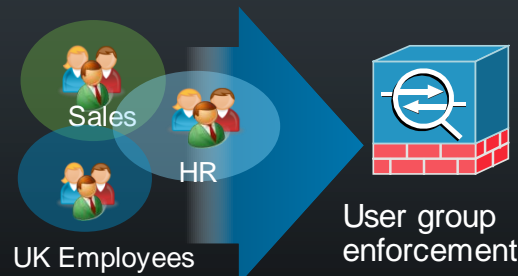
- AAA, 802.1x, guest, profiler, posture
- System monitor & diagnosis
- "ISE": Next-generation ACS + NAC

## Unified Agent



- Offers Cisco AnyConnect™ technology: On- and off-premises security
- Extends 802.1x & VPN client + NAC
- Extends management to ISE

## Identity Based Firewall



- User, group, device based policy
- ASA & ISE platforms

## Simplified Device Profiling



- Cisco delivered device template feed
- Switches collect & forward device fingerprint, no traffic re-engineering

## Network Infection Containment



- Streamline the locate, contain, & remediation process
- Leverage reputation & NIPS feeds

## System-wide Monitoring & Troubleshooting

Network  
Device  
Provisioning

Identity Policy

Client  
Management

Monitoring &  
Troubleshooting

- Single admin pane-of-glass
- Wired & wireless infrastructure

# ISE Packaging and Licensing

## Base Feature Set

Perpetual Licensing

- **Authentication / Authorization**
- **Guest Provisioning**
- **Link Encryption Policies**

## Advanced Feature Set

Term Licensing

- **Device Profiling**
- **Host Posture**
- **Security Group Access**

## Appliance Platforms

Small 3315/1121 | Medium 3355 | Large 3395 | Virtual Appliance

# Upgrades and Migrations



- Current hardware is software upgradeable (1121/3315/3355/3395)
- Migration program for older hardware at large discount levels
- License migration program for all software licenses
- Data and Configurations migration tools available\*



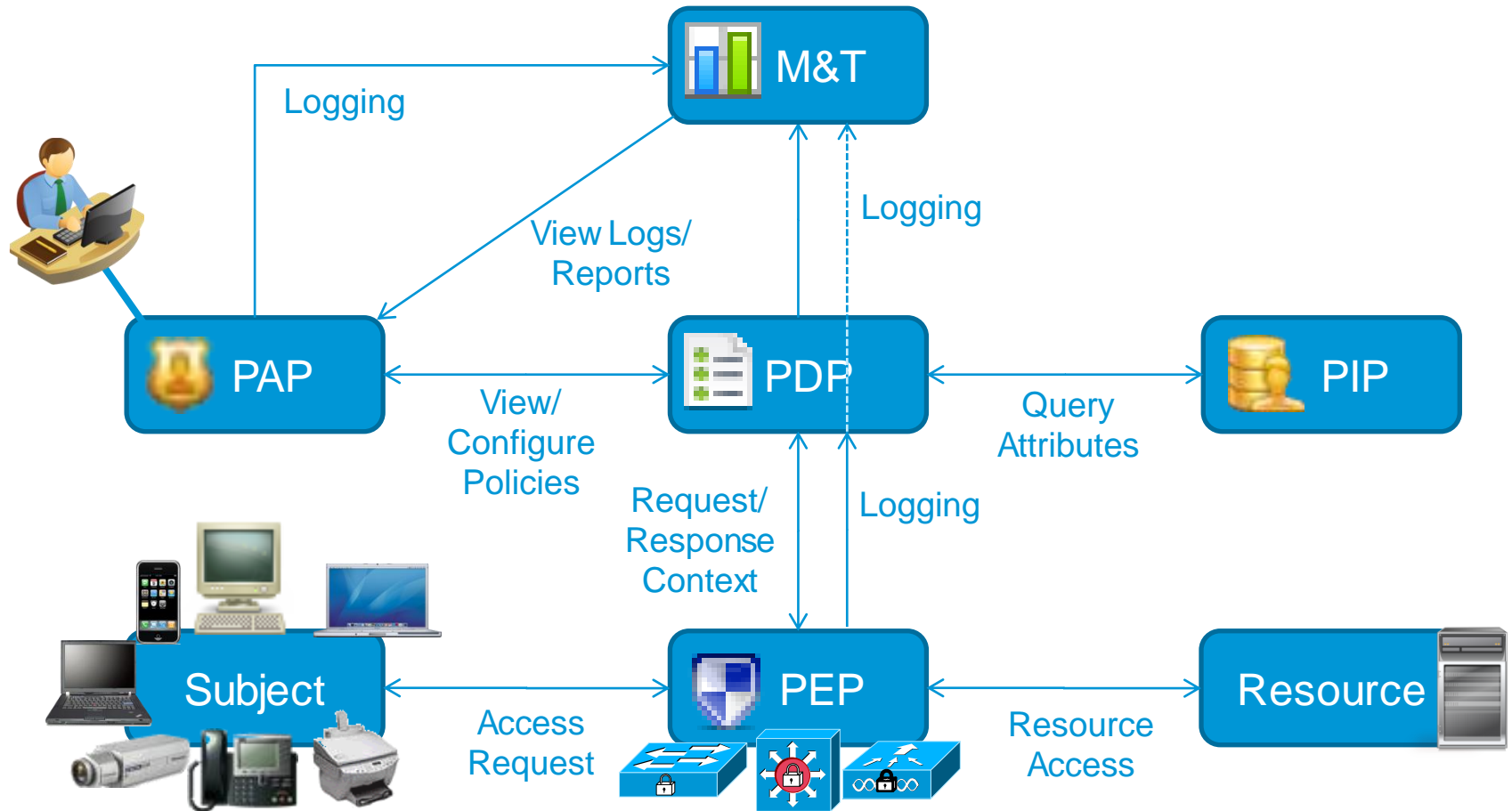
\*Available over future releases

## Existing Investments Protected

# ISE Architecture

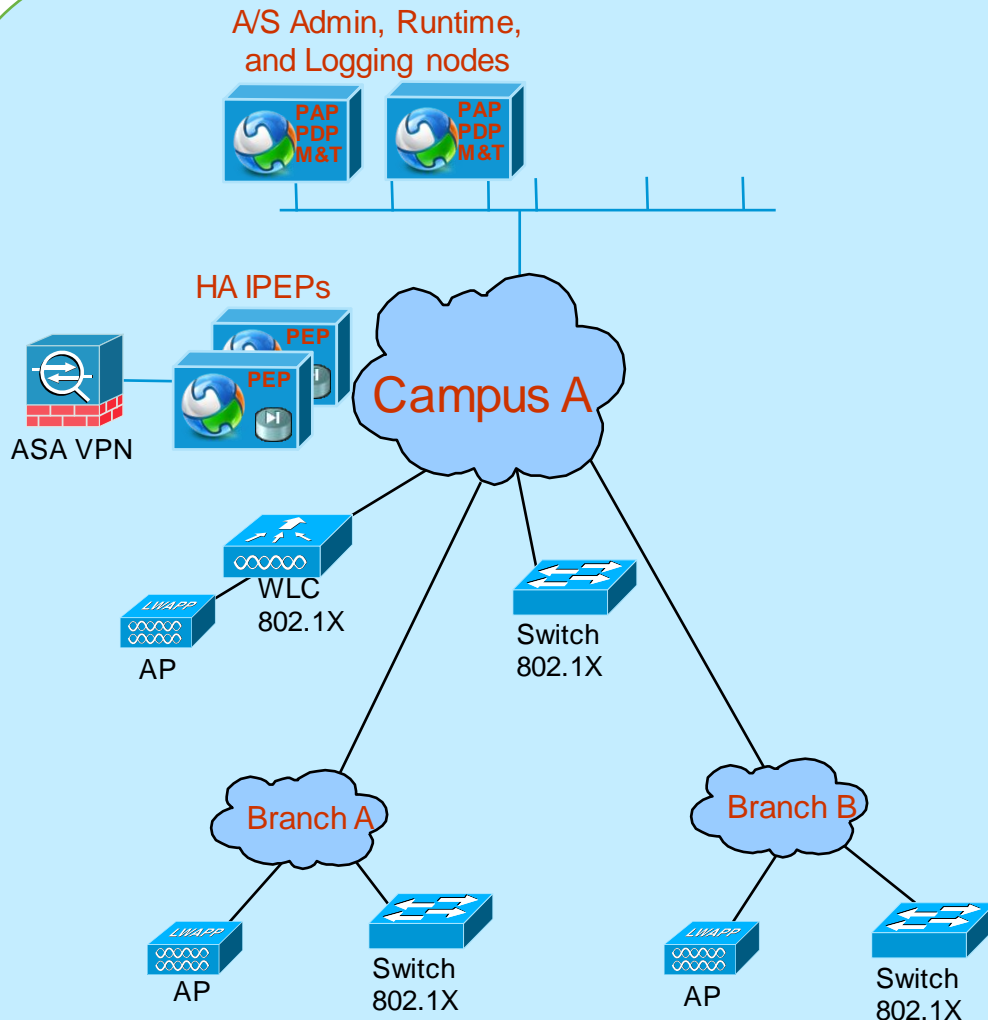


# ISE Architecture



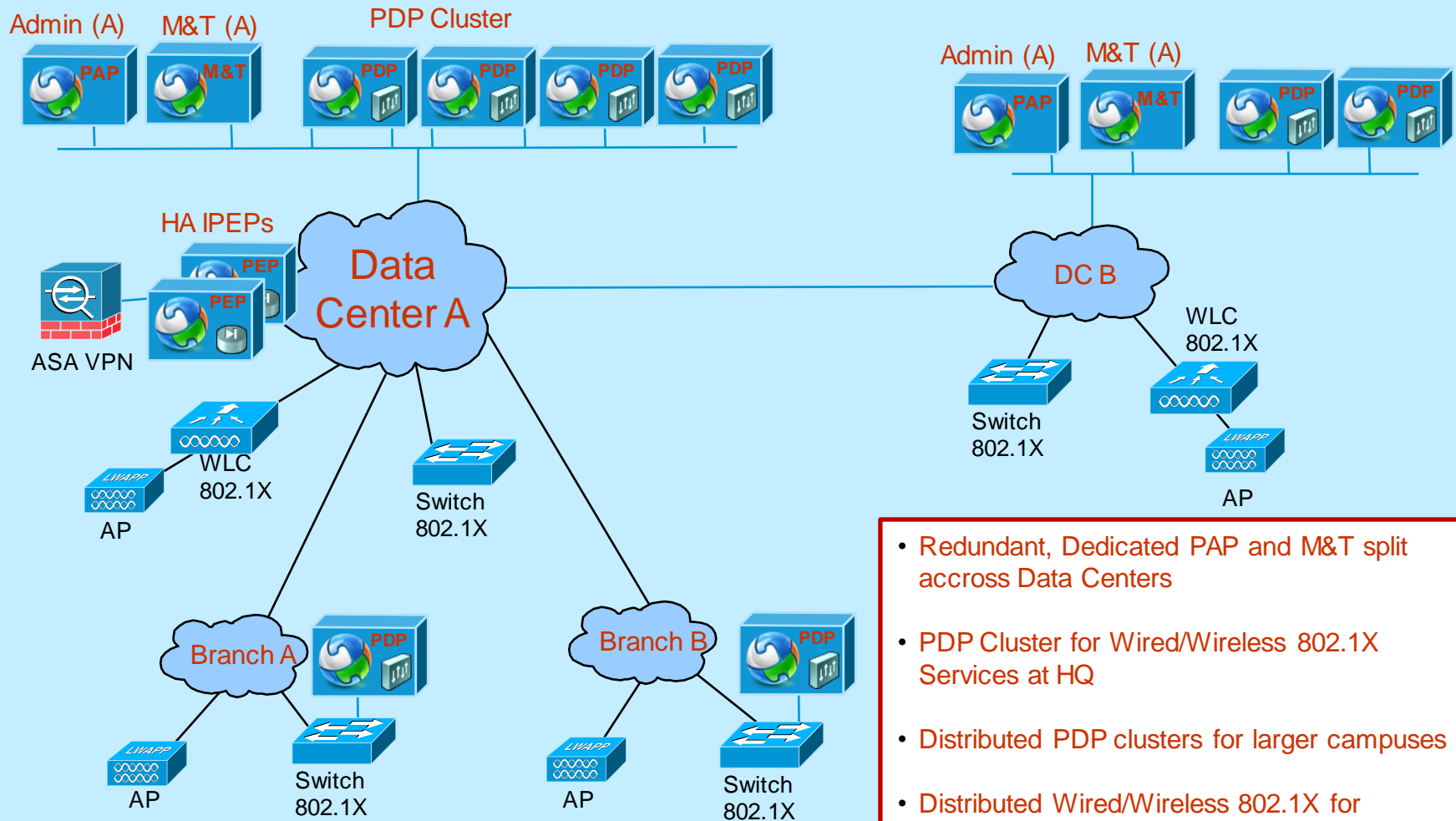
# Typical ISE Deployment: SMB

## Example Topology



- Centralized Wired 802.1X Services
- Local VPN support at HQ via HA iPEPs
- Centralized Wireless 802.1X Services for HQ and branch offices (centralized WLCs w/CoA)
- Centralized 802.1X Services for branch offices

# Typical ISE Deployment: Enterprise Example Topology



- Redundant, Dedicated PAP and M&T split across Data Centers
- PDP Cluster for Wired/Wireless 802.1X Services at HQ
- Distributed PDP clusters for larger campuses
- Distributed Wired/Wireless 802.1X for Branches
- VPN/Wireless (non-CoA) at HQ via HA iPEPs

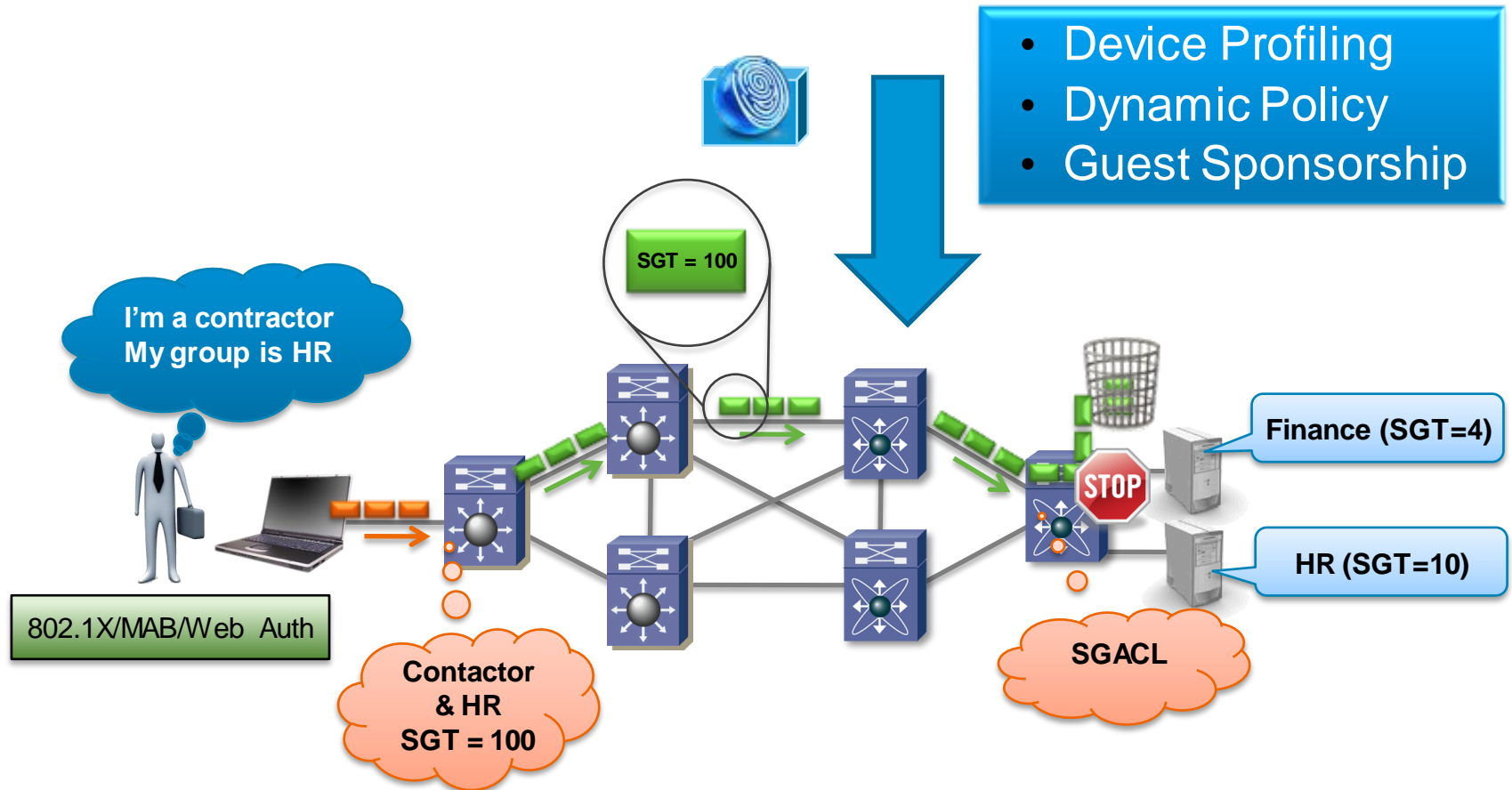
# ISE as a Cisco differentiator

# ISE as a differentiator

- As a company, Cisco is positioned to be a leader in mobility with strong offerings in LAN, Wireless LAN and Remote Access (VPN). In fact, Only Cisco is ranked in the Leader Quadrant of all three Magic Quadrants from Gartner.
- ISE Provides unique management for both Wired, Wireless and VPN**



# ISE in Wired Environment



- TrustSec provides:
  - Authentication, Confidentiality
  - Role based tagging and control

# ISE in Wireless Environment

## User and Device Specific Attributes



### Employees

- Gold QoS
- Employee VLAN

### Employee iPads

- Employee VLAN
- Gold QoS
- Restrictive ACL

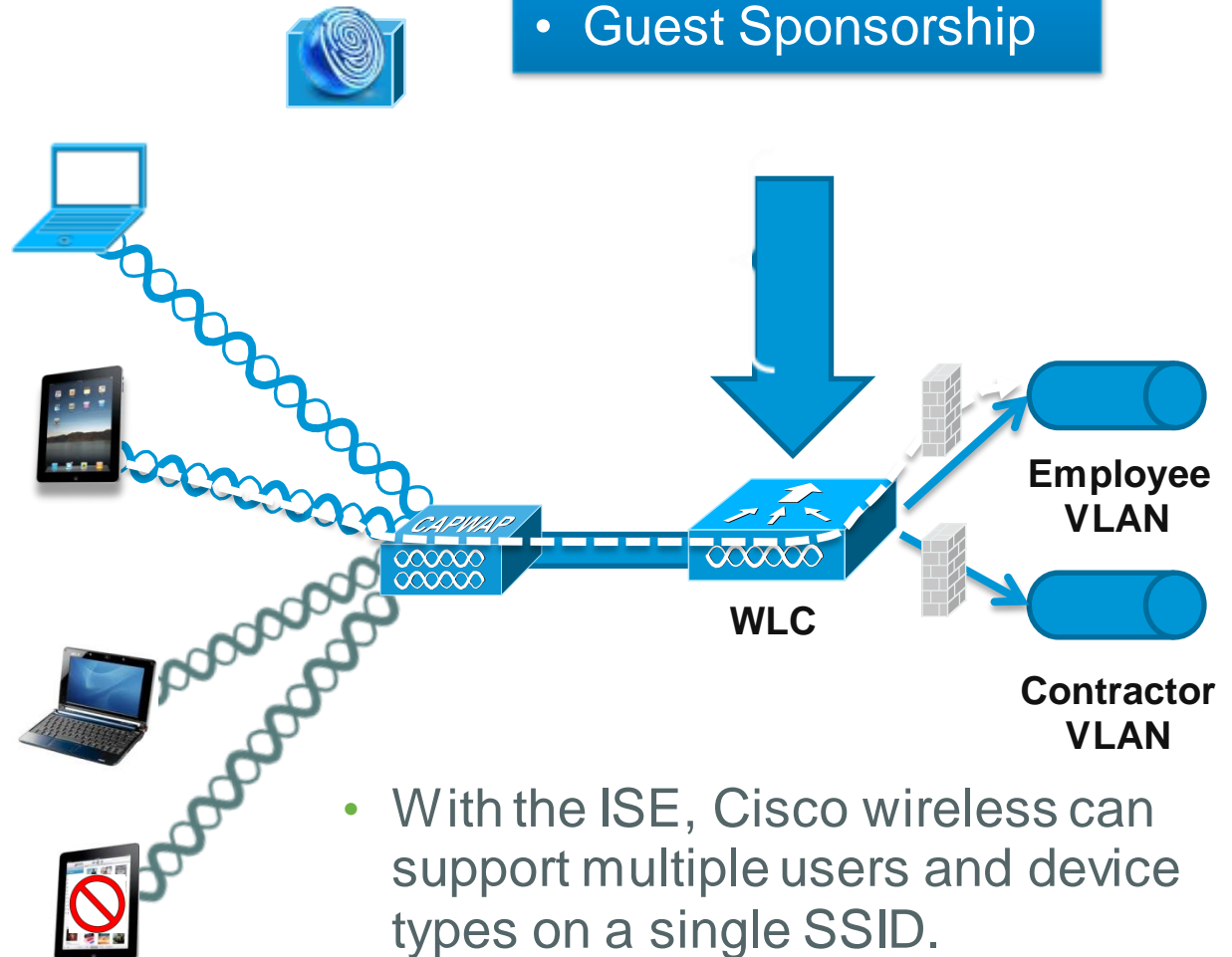
### Contractors

- Contractor VLAN
- No QoS
- Restrictive ACL

### Contractor iPads

- No Access

- Device Profiling
- Dynamic Policy
- Guest Sponsorship



- With the ISE, Cisco wireless can support multiple users and device types on a single SSID.

# Differentiation to HP





## ISE as a differentiator – Against HP LAN switching

- HP has basic 802.1X and L2 security services, built-in security and other modules (firewall from Fortinet, Riverbed for WAAS)
- Advanced Security Features from TrustSec are needed, like
  - Posture Assessment (not recognized as a NAC by market),
  - **Profiler**, 802.1X monitor mode
  - Scalable Access Control,
  - MACSec
  - Guest



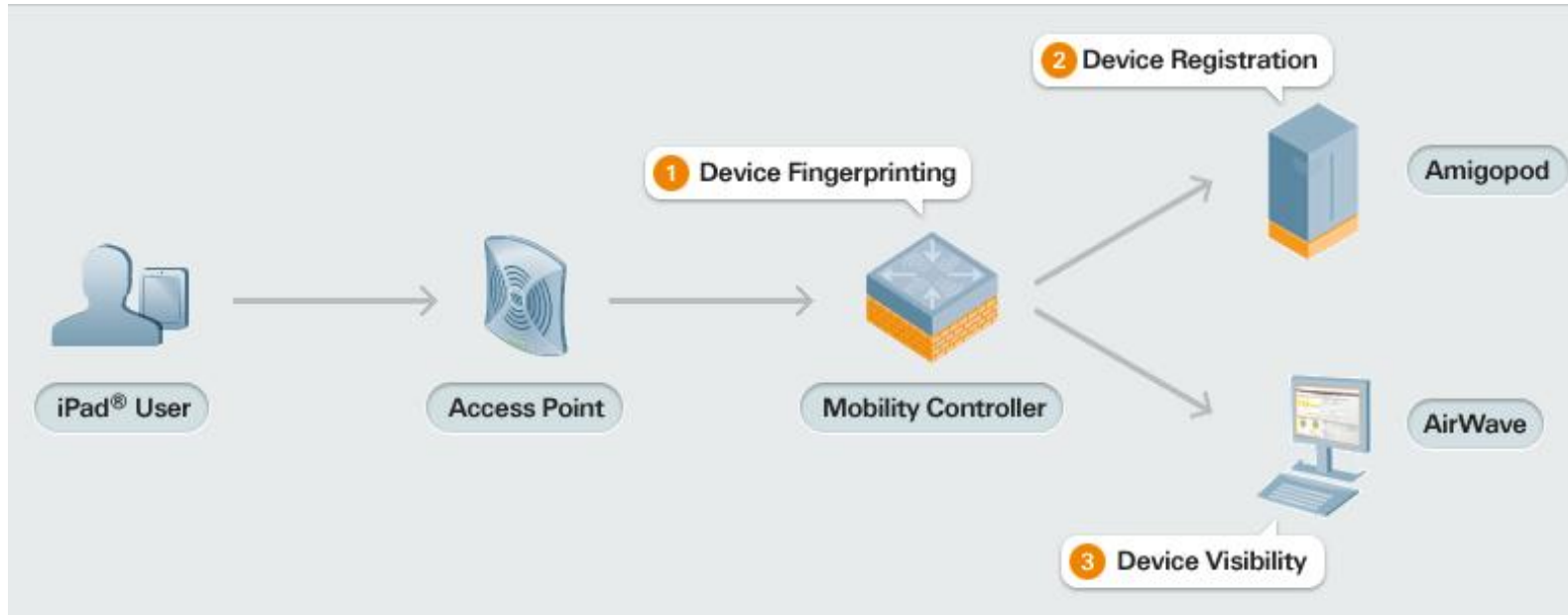
# Comparing with HP



		
802.1X solution	Supplicant, switch, policy server	Supplicant, switch, policy server Limited features on switches
Deployment Models	802.1X, In-Band, and SNMP OOB	802.1X
Guest Lifecycle Management	Complete Guest Management, Control, and Auditing Solution	Limited functionality
Access Control for Non-User Devices	MAB, local database	MAC Authentication, local database
Profiler	NAC appliance, ISE	None
Posture	NAC appliance, 802.1X with ISE	802.1x with IMC/EAD
Segmentation Methods	VLAN, dACL, SGA	VLAN, dACL
Enforcement	Switches, NAC appliance	Switches
Client Integration	Any Connect (VPN, 802.1X, Posture, Web Security, MACSec)	iNode (VPN, 802.1X, Portal)

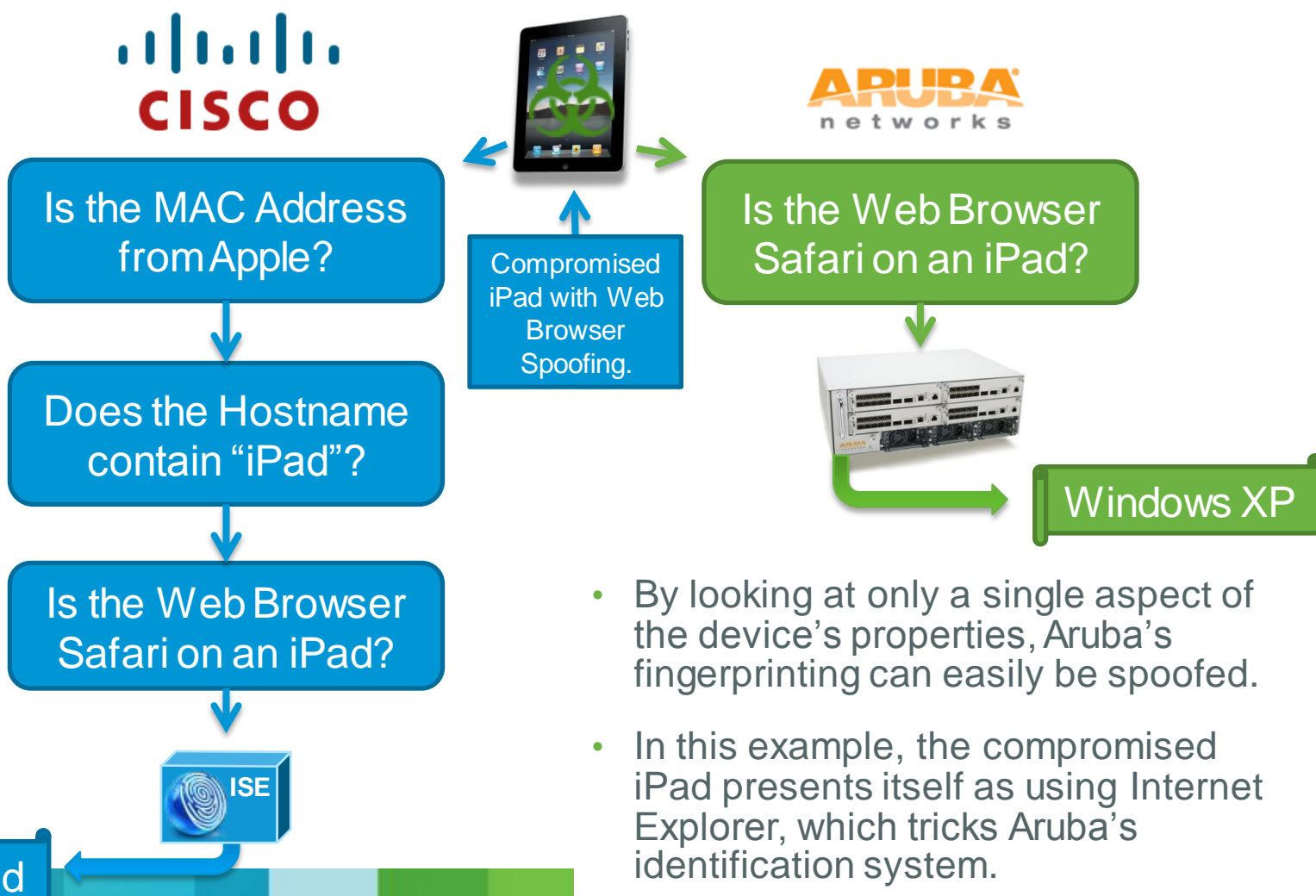
# Differentiation to Aruba

# What is the Problem and What is Aruba's Solution? –looks the same, but it is not





- Aruba is trying to address the wave of new mobile devices by:
  - Identifying mobile devices as they access the network.
  - Require users to register their devices for network access.
  - Apple iOS devices are provided a certificate for authentication after registration.
- AirWave provides insight into what devices are connected.

# Cisco's Multi-faceted Device Profiling is More Comprehensive than Aruba's



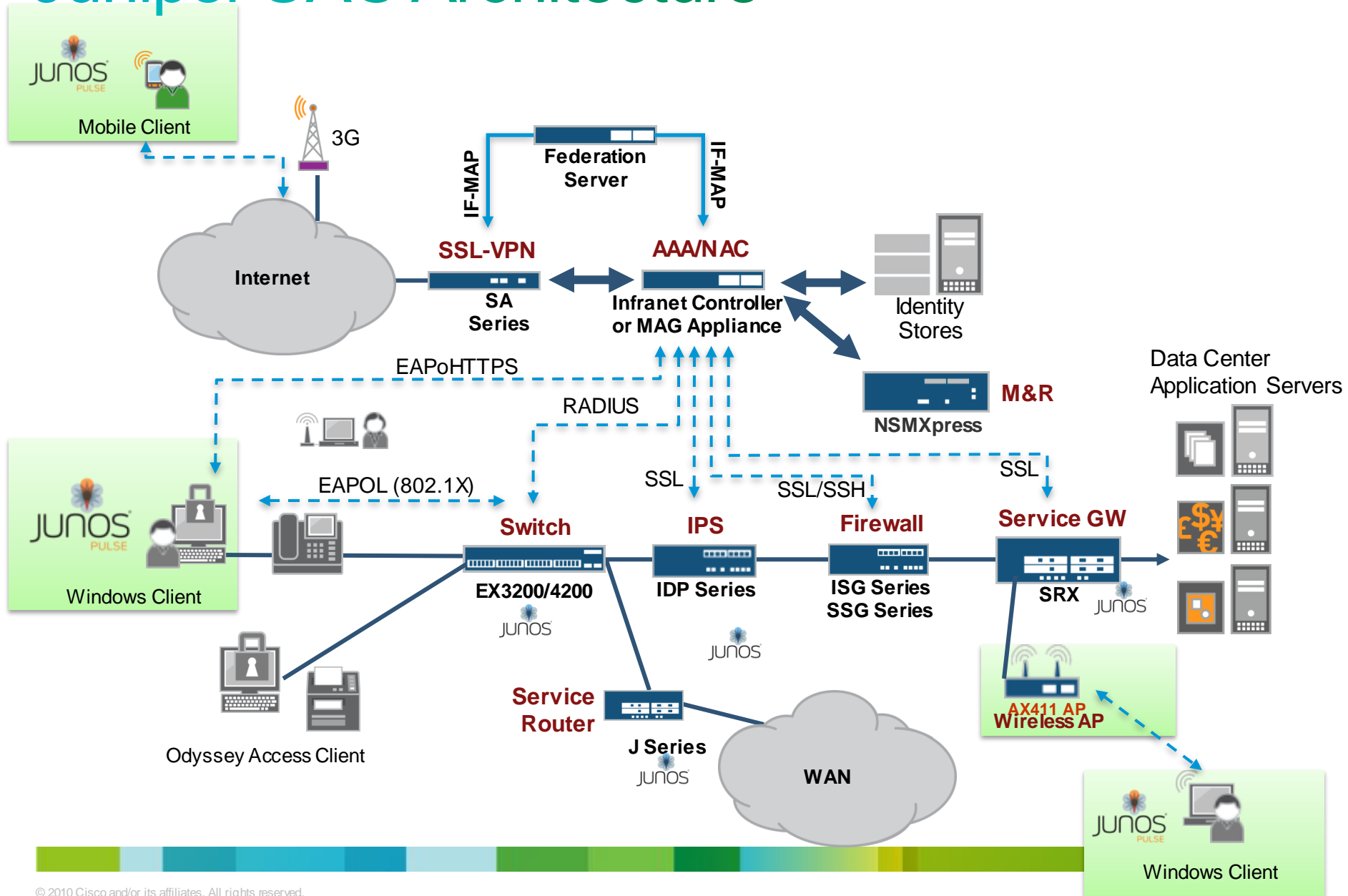
# Mobile Device Access Solution Comparison

		
<b>Device Fingerprinting</b>	At ISE	At each controller
<b>User Authentication</b>	At ISE	At an external RADIUS Server*
<b>Guest Registration / Sponsorship</b>	At ISE	At Amigopod Appliance
<b>Single SSID Solution</b>	Yes	No
<b>Comprehensive Client Profiling</b>	Yes	No
<b>Centralized Wired/Wireless Policy and Visibility</b>	Yes	No

\*The Aruba controller or Amigopod Appliance can be a RADIUS server, but lacks certain EAP types.



# Differentiation to Juniper

# Juniper UAC Architecture





# Comparing with Juniper

		
802.1X solution	Supplicant, switch, policy server	Supplicant, switch, policy server. Limited features on switches
Deployment Models	802.1X, In-Band, and SNMP OOB	802.1X and In-Band, FW layer 3 enforcement
Guest Lifecycle Management	Complete Guest Management, Control, and Auditing Solution	Simple Captive Portal Solution (limited guest account management)
Access Control for Non-User Devices	MAB, local database	Yes, MAB, local database
Profiler	NAC appliance, ISE	Reference Great Bay sell
Posture	NAC appliance, 802.1X with ISE	802.1X, Host Checker
Segmentation Methods	VLAN, dACL, SGA	VLAN, dACL
Enforcement	Switches, NAC appliance	Switches, routers, firewalls, IDS/IPS
Client Integration	Any Connect (VPN, 802.1X, Posture, Web Security, MACSec)	Junos Pulse (802.1X, VPN, Posture, WAN Acceleration)

# How to compete against Juniper

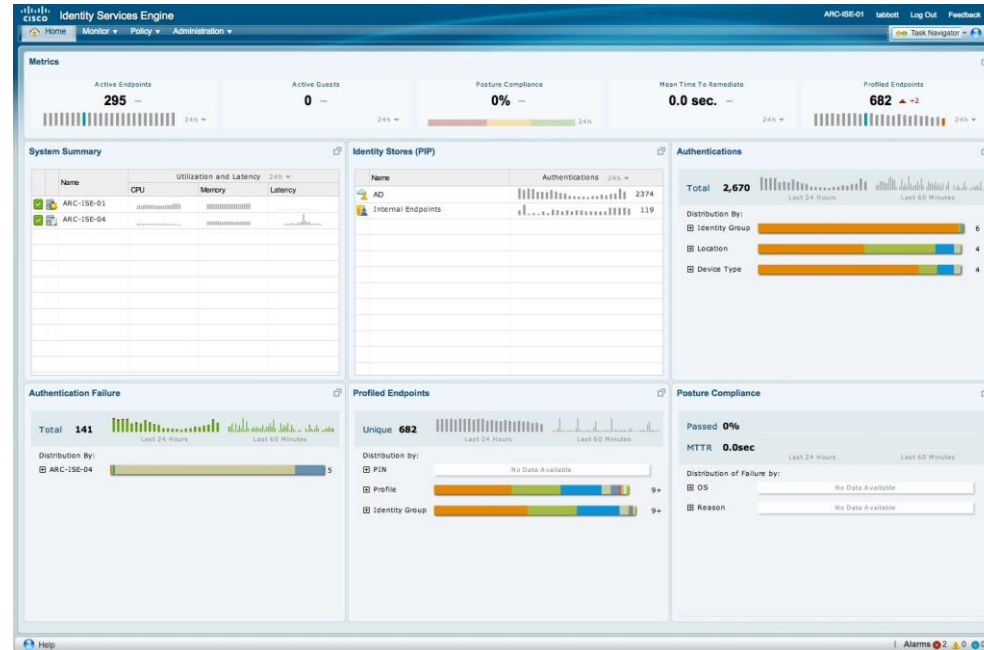
- Without 802.1X, all traffic must be inline for enforcement via Juniper's firewalls
- Lacks support for full complement of authentication methods
- No Juniper-branded solution for securing non-user devices
- Lack of comprehensive guest services
- No 802.1AE port-level encryption
- Lacks full visibility into users and devices on the network
- Largely manual user requirements for posture & remediation



# ISE Demo



# ISE Demo





# Call to Action

# Please, Ask Yourself the Following Questions

- Do you...
  - want an integrated access management for wired, wireless and VPN infrastructures?
  - see a problem with a fact that well defended network perimeter disappeared?
  - have to follow regulatory compliance requirements?
  - have problem with new devices in the network, like “BYOD”?



And the answer is...

# Start Considering Cisco ISE

- You can address your need for advanced access security
- You may achieve advanced profiling of any device in your network (incl. BYOD's)
- And finally you may deploy posture assessment (NAC evolution) solution as part of one platform



# Summary



# Summary

- ISE is the central TrustSec solution to overcome wireless BYOD challenges and provide advanced security features on wired
- Please request one to one session with Cisco Systems Engineers and see the details

Thank you.

