Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Demystifying TrustSec, Identity, NAC and ISE

BRKSEC-2022

TOMORROW starts here.

Hosuk Won, CCIE# 22231

Technical Marketing Engineer,
Secure Access & Mobility Group

howon@cisco.com

Session Abstract

- This session is a technical breakout that will help demystify the technology behind the Cisco TrustSec System, including the Identity Services Engine.
- We will build use cases to introduce, compare, and contrast different access control features and solutions, and discuss how they are used within the TrustSec System.
- The technologies that will be covered include user & device authorisation, 802.1X, Profiling Technology, Supplicant's, certificates/PKI, Posture, CoA, RADIUS, EAP, Guest Access, Security Group Access (SGA), and 802.1AE (MacSec).
- All of the technologies will be discussed in relation with Cisco's Identity Services Engine

Session Objectives

At the end of the session, you should understand:

- The many parts and pieces that make up Cisco's TrustSec Solution
- How 802.1X works & how to make it work for you ☺
- The benefits of deploying TrustSec
- The different deployment scenarios that are possible

You should also:

- Provide us with feedback!
- Attend related sessions that interest you
- Have a nice glossary of terms at your disposal

Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions and Meet the Engineer
- Visit the Cisco Store to purchase your recommended readings
- Please switch off your mobile phones
- After the event don’t forget to visit Cisco Live Virtual: www.ciscolivevirtual.com

For Your Reference

- There are slides in your PDF's that will not be presented.
- They are there usually valuable, but included only "For your Reference"

For Your Reference

Cisco’s Trusted Security (TrustSec)

What is TrustSec

- Think of it as “Next-Generation NAC”
- TrustSec is a System approach to Identity & Access Control:
  - IEEE 802.1X (Dot1x)
  - Profiling Technologies
  - Guest Services
  - Secure Group Access (SGA)
  - MACSec (802.1AE)
  - Identity Services Engine (ISE)
  - Access Control Server (ACS)

So, TrustSec = Identity, Right?

- Yes, but it refers to an Identity System (or solution)
  - Policy Servers are only as good as the enforcement device
  - (Switches, WLC's, Firewalls, etc…)
- But what is "Identity":
  - Understanding the Who / What / Where / When & How of a user or device's access to a network.

Authentication vs. Authorisation

Driving Home the Point

I'd like 40K from John Chambers Account

Do You Have Identification?

Yes, I Do. Here it is.

Authentication

Sorry, Hosuk Won is not Authorised for John Chambers Account

Authorisation

New Term: Enforcement

The Business Case

Business Case

- Throughout the presentation, we will refer to a business case. One that will continue to evolve:
  - Company: Retailer-X
  - Problem Definition:

    The company stores credit card data from all sales transactions.

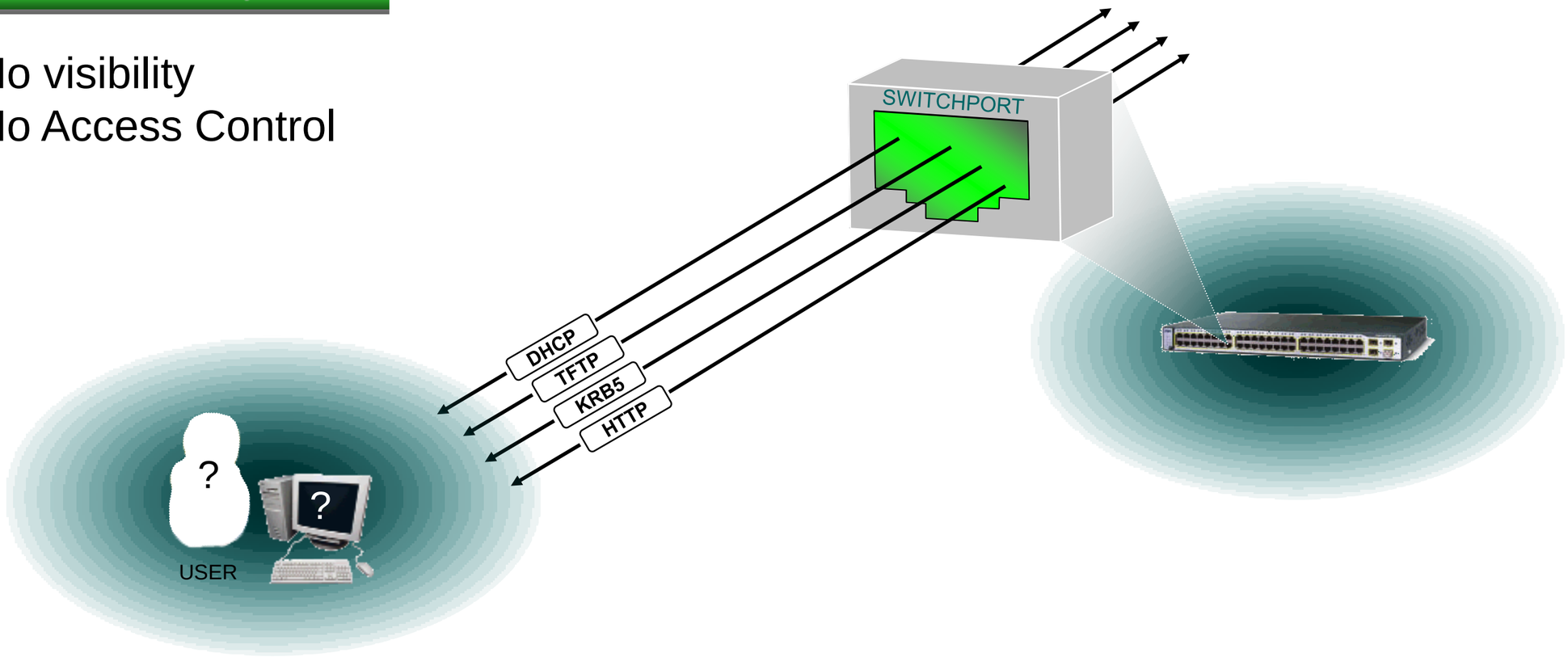
    As with all companies: Vendors & Guests are constantly visiting Retailer-X, to pitch new products to be sold, or even to sell network, security & collaboration equipment to Retailer-X.

    Company must ensure that only Retailer-X employees are gaining access to the network.
  - Solution: Identity with 802.1X

Default Port State without 802.1X

No Authentication Required

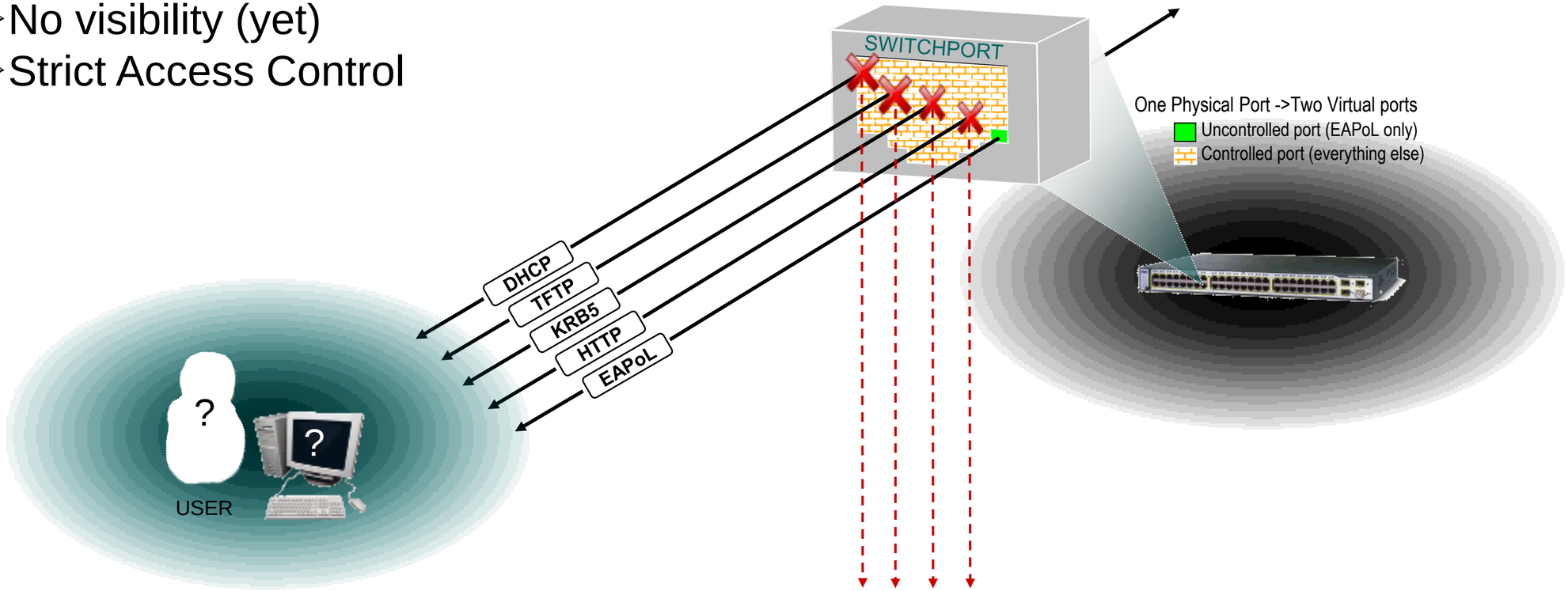
- No visibility
- No Access Control



Default Security with 802.1X

Before Authentication

- No visibility (yet)
- Strict Access Control

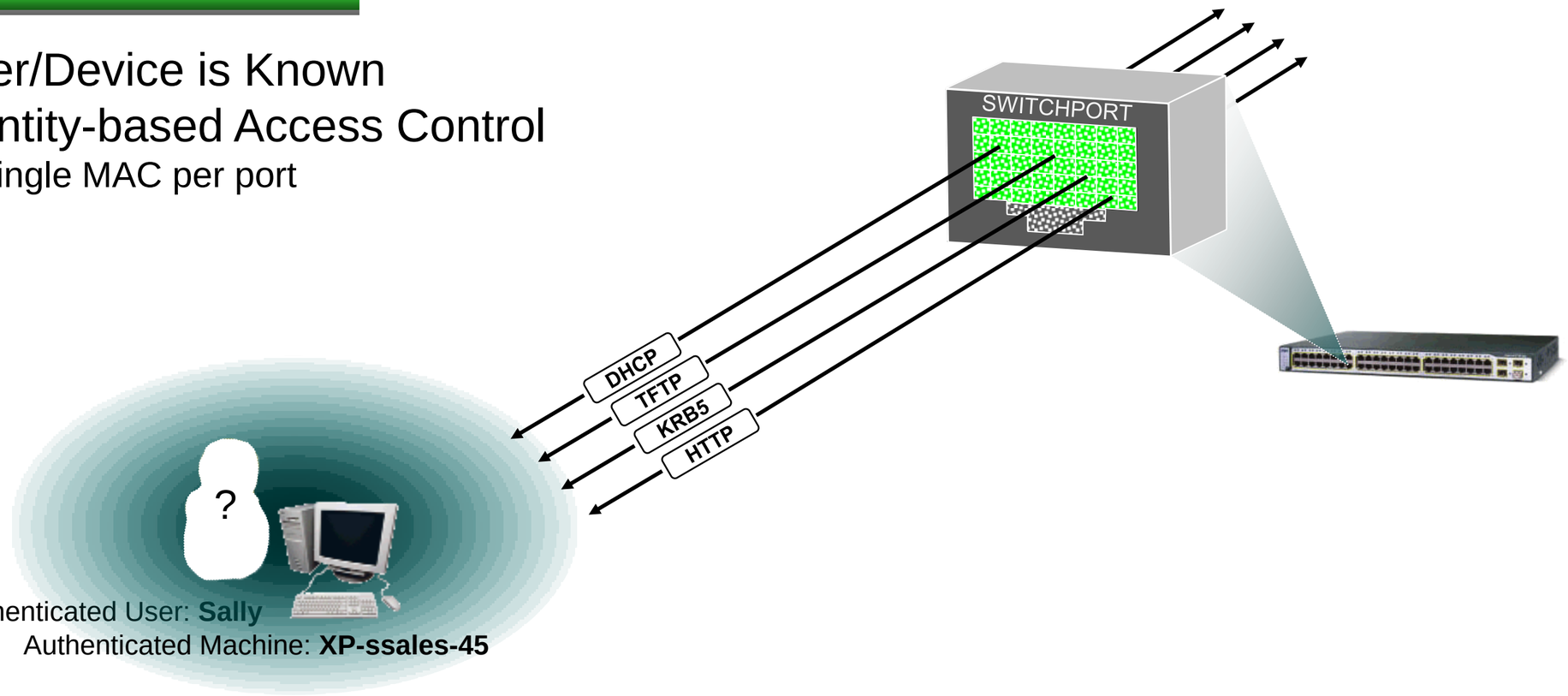


ALL traffic *except* EAPoL is dropped

Default Security with 802.1X

After Authentication

- User/Device is Known
- Identity-based Access Control
  - Single MAC per port



Revisit: Business Case

- Company: Retailer-X
- Problem Definition:
  - The company stores credit card data from all sales transactions.

    As with most companies: Vendors & Guests are constantly visiting Retailer-X, to pitch new products to be sold, or even to sell network, security & collaboration equipment to Retailer-X.
  - Company must ensure that only Retailer-X employees are gaining access to the network.
- Solution: Identity with 802.1X

Revisit: Business Case

- Did we meet the business case? YES!
- But what was missing?
- What lessons have we learned?
  - We called Dot1x an "access prevention" technology

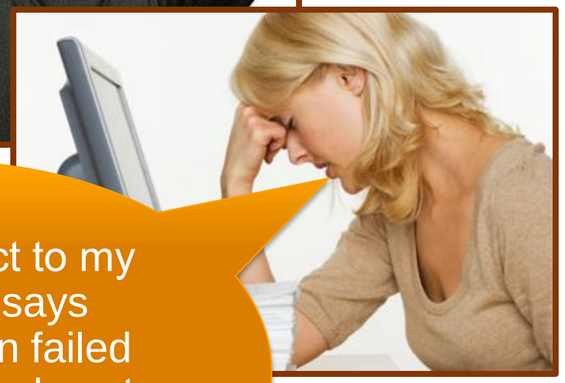
What Happened? What Went Wrong?

@ Retailer-X, **BEFORE** Monitor Mode is available …

IT Mgr.

I've done my homework in Proof of Concept Lab and it looks good. I'm turning on 802.1X tomorrow…

Enabled 802.1X



I can't connect to my network. It says Authentication failed but I don't know how to fix. My presentation is in 2 hours…

Help Desk call increased by 40%

What was Missing?

What Lessons were Learned?

- Access-Prevention Technology
  - A Monitor Mode is necessary
  - Must have ways to implement & see who would succeed & who would fail

    Determine why, and then remediate before taking Dot1x into a stronger enforcement mode.
- Solution = Phased Approach to Deployment:
  - Monitor Mode
  - Low-Impact Mode

    -or-
  - Closed Mode

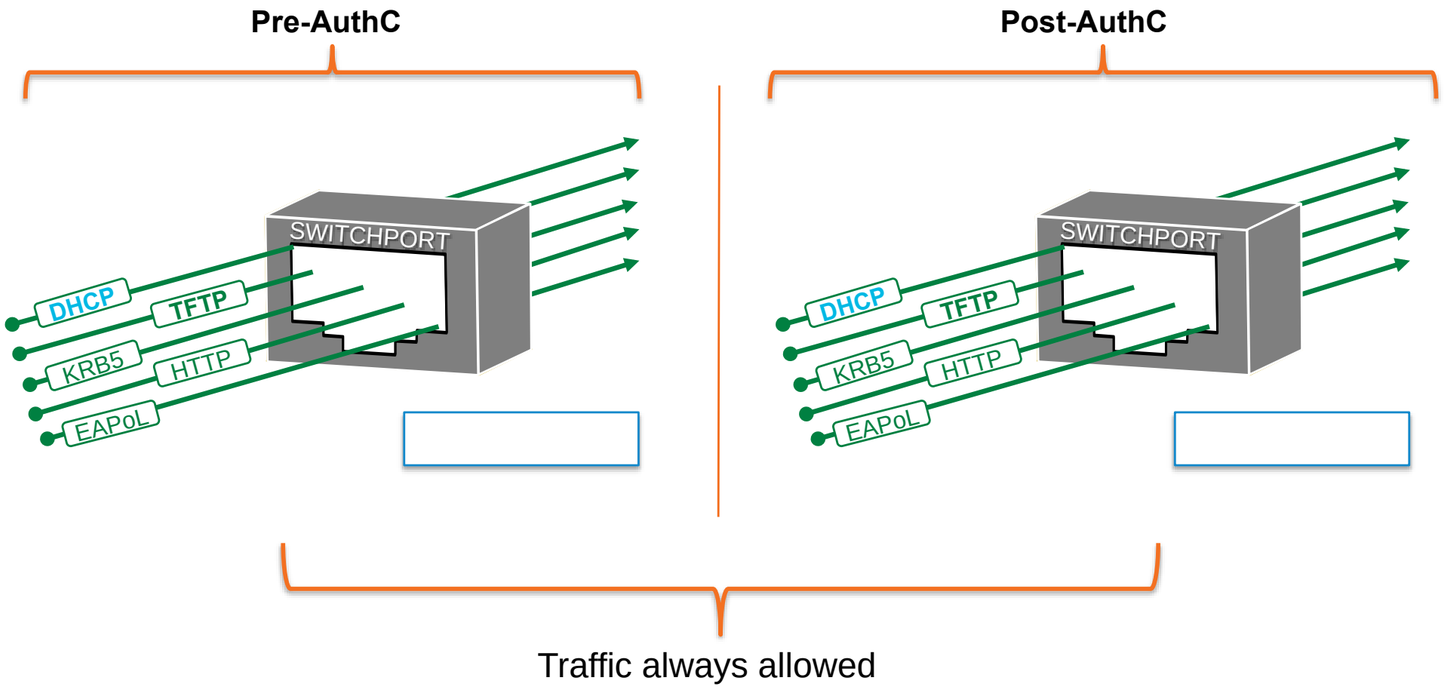
Monitor Mode

A Process, Not Just a Command

Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
```

- Enables 802.1X Authentication on the Switch
- But: Even failed Authentication will gain Access
- Allows Network Admins to see who would have failed, and fix it, before causing a Denial of Service ☺



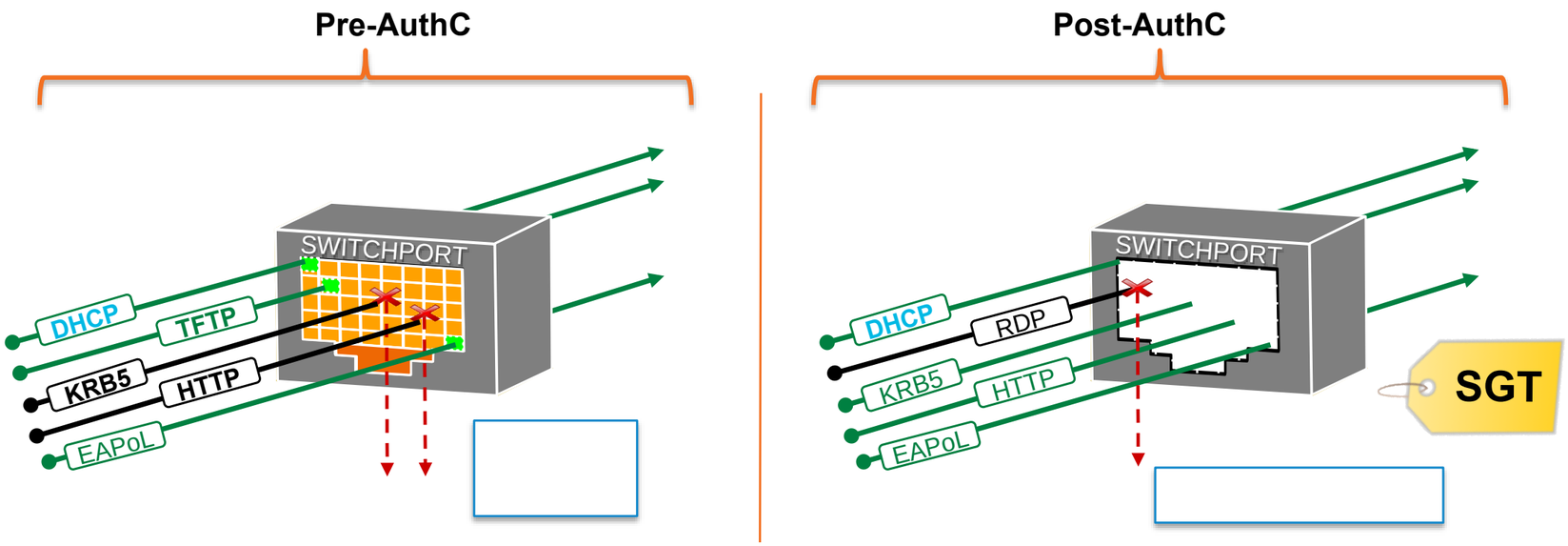
Low-Impact Mode

If Authentication is Valid, Then **Specific** Access!

Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 ip access-group default-ACL in
```

- AuthC Success = Role Specific Access
  - dVLAN Assignment / dACLs
  - Specific dACL, dVLAN
  - Secure Group Access
- Still Allows for pre-AuthC Access for Thin Clients, PXE, etc…
- **WebAuth** for non-Authenticated



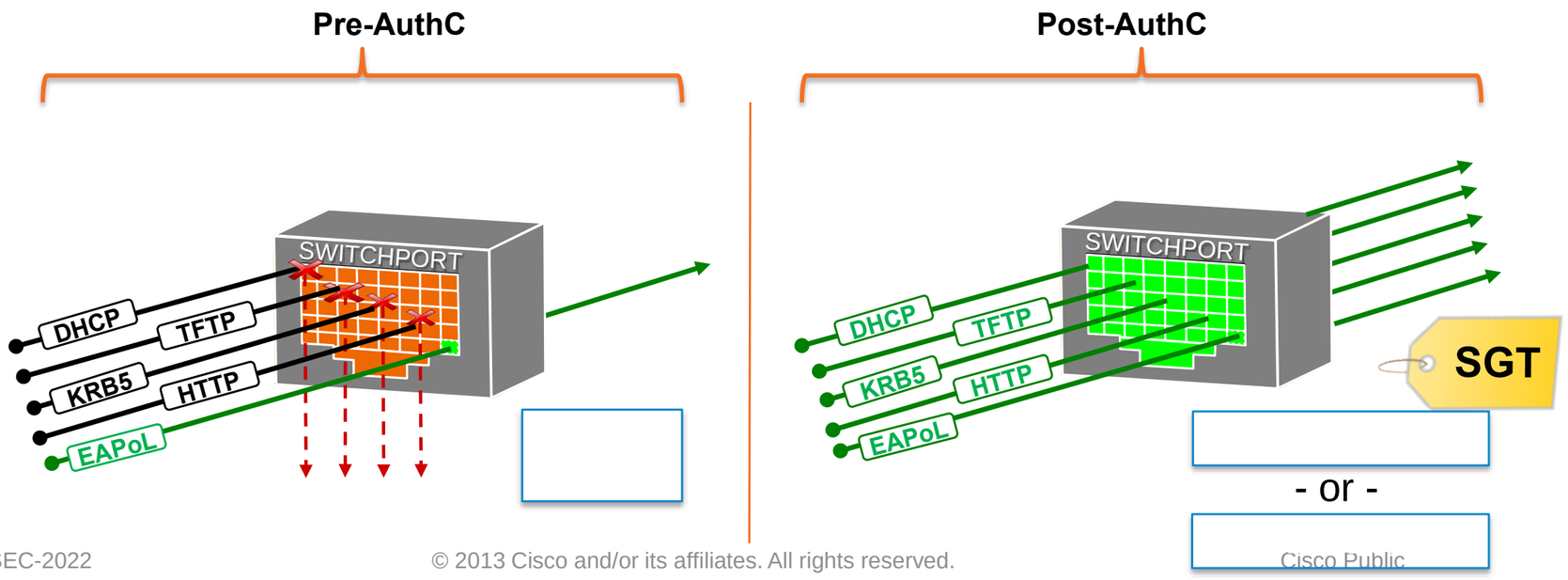
Closed Mode

No Access Prior to Login, Then **Specific** Access!

Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication port-control auto
 mab
 dot1x pae authenticator
```

- Default 802.1X Behaviour
- No access at all prior to AuthC
- Still use all AuthZ Enforcement Types
  - *dACL, dVLAN, SGA*
- Must take considerations for Thin Clients & PXE, etc…



What was Missing?

What Lessons were Learned?

- No visibility from the supplicant
  - Little to no User-Interaction

    User saw an “Authentication Failed” message, and that was all.
  - When everything works – the user is unaware.

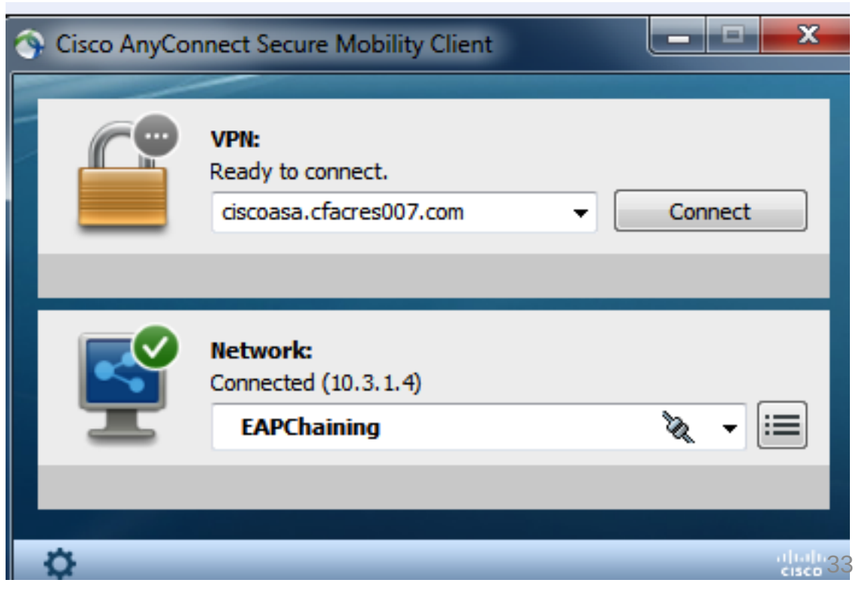
    But, when things stop working…

    No visibility. Just a call to the help-desk
- Solution: 3rd Party Supplicants
  - Cisco’s AnyConnect Supplicant

    Provides a Diagnostic and Reporting Tool (DART)

    Detailed logs from the Client Side

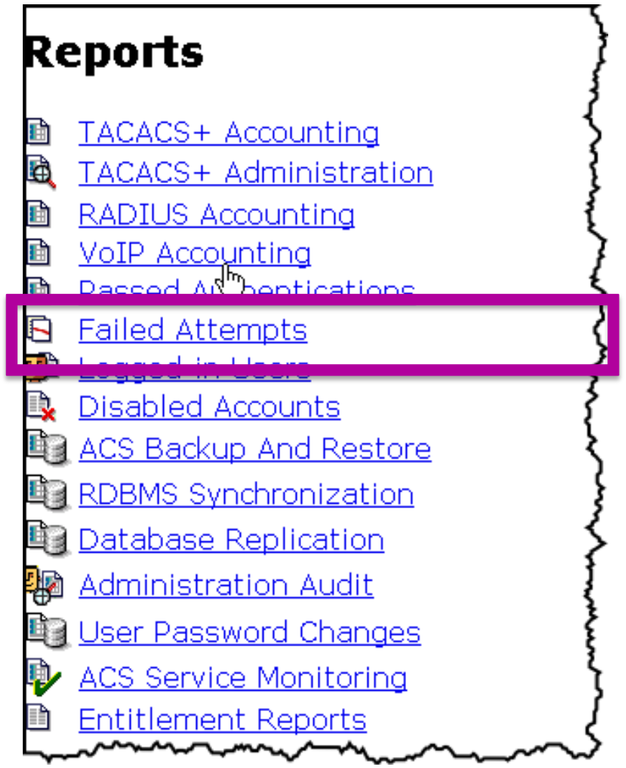
    Unique hooks with RDP and VDI environments

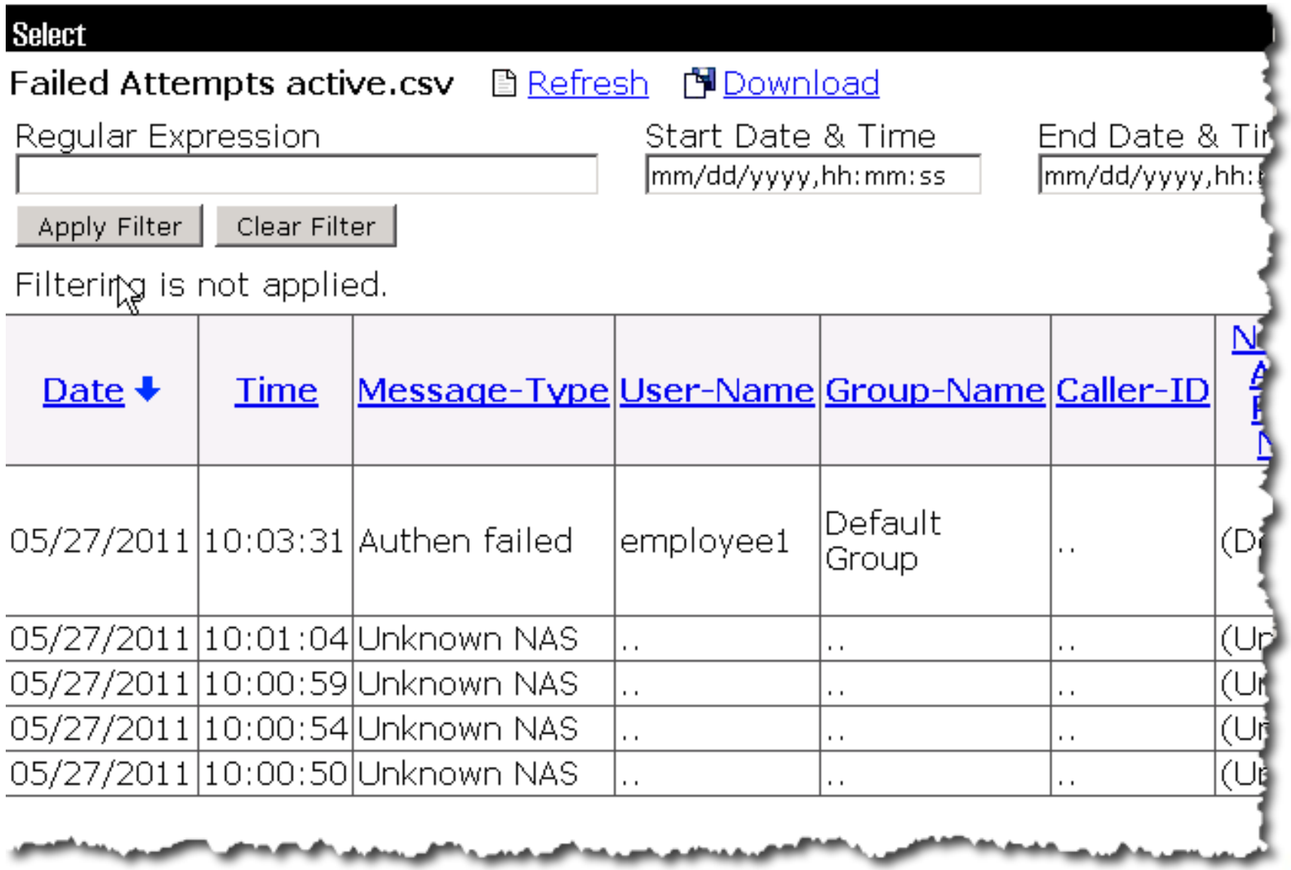


What was Missing?

What Lessons were Learned?

- No Visibility at the RADIUS Server



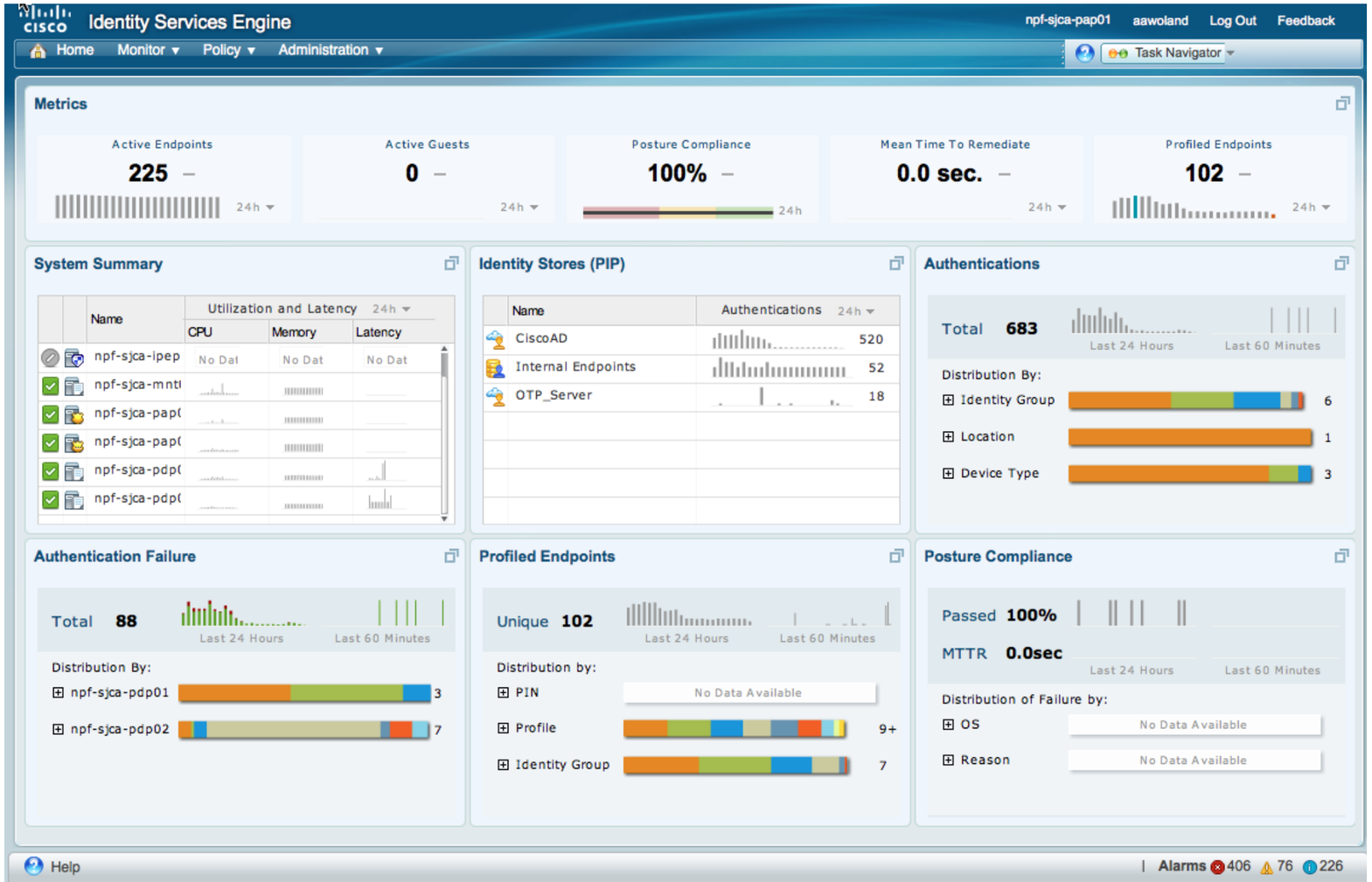


Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	N
05/27/2011	10:03:31	Authen failed	employee1	Default Group	..	(D
05/27/2011	10:01:04	Unknown NAS	..	..	..	(Un
05/27/2011	10:00:59	Unknown NAS	..	..	..	(Un
05/27/2011	10:00:54	Unknown NAS	..	..	..	(Un
05/27/2011	10:00:50	Unknown NAS	..	..	..	(Un

What was Missing?

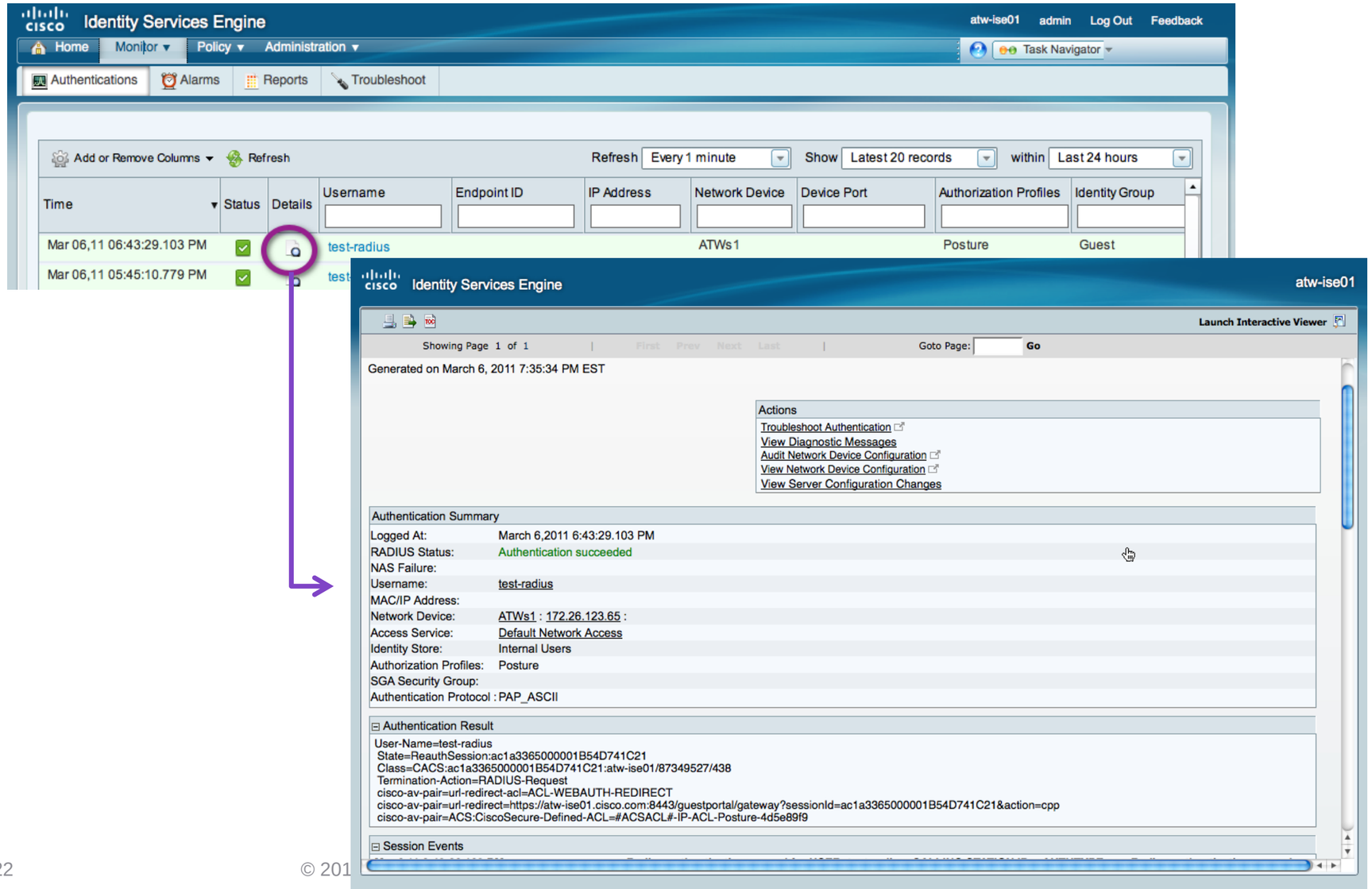
What Lessons were Learned?

- Solution: ACS VIEW → Identity Services Engine (ISE)



What was Missing?

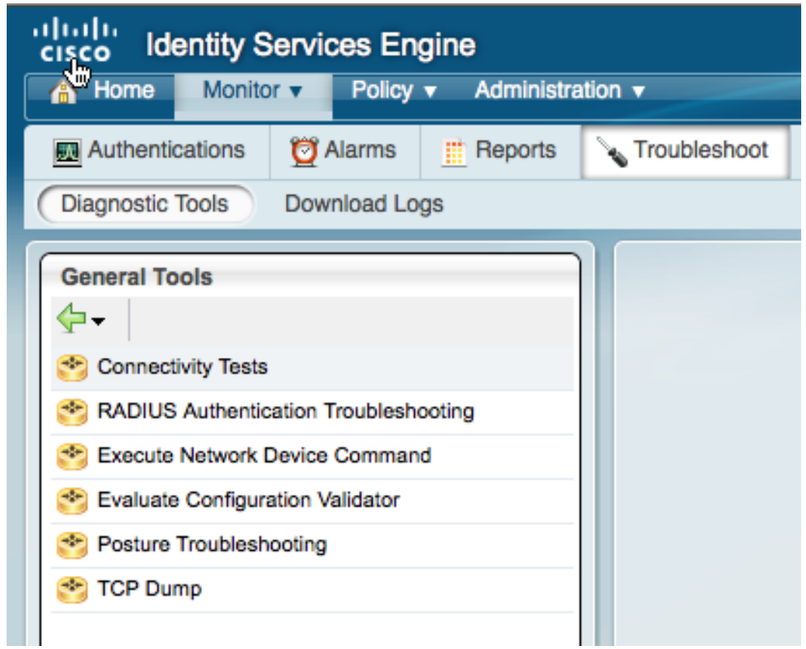
What Lessons were Learned?

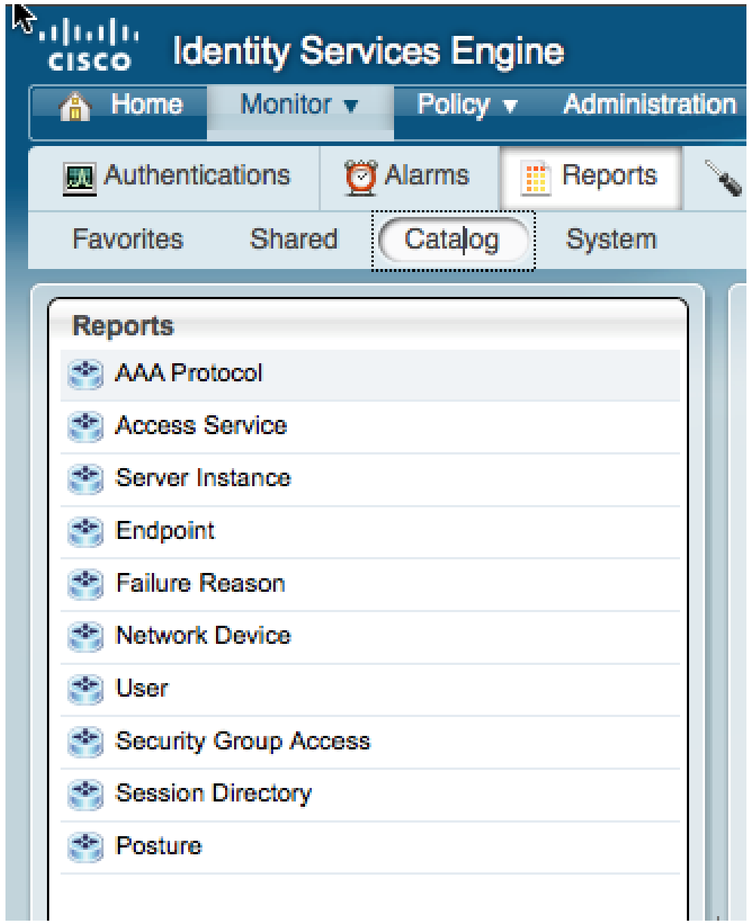


What was Missing?

What Lessons were Learned?

- Solution: ACS VIEW → ISE





What was Missing?

What Lessons were Learned?

- Non-Authenticating Devices
  - These are devices that were forgotten
  - They don't have software to talk EAP on the network
    - Or, they weren't configured for it
    - Printers, IP Phones, Camera's, Badge Readers
  - How to work with these?
    - Don't configure Dot1x on the SwitchPort
    - But, what about when it moves
- ~~Solution? Do not use dot1x on ports~~ with Printers
- Solution: MAC Authentication Bypass (MAB)

MAC Authentication Bypass (MAB)

What is It?

- A list of MAC Addresses that are allowed to “skip” authentication
- Is this a replacement for Dot1X?
  - No Way!
- This is a “Band-aid”
  - In a Utopia: All devices authenticate.
- List may be Local or Centralised
  - Can you think of any benefits to a centralised model?

What was missing?

What Lessons were Learned?

- Guests:
  - Guests will not have configured supplicants.

    Plus: they won't be authorised for access.
  - Original Solution:

    Dot1x Timeouts
  - How this works:

    After a timeout period, the switchport is automatically put into a Guest VLAN which provides Internet access.

What was Missing?

What Lessons were Learned?

- Missing or Misconfigured Supplicants:
  - Group Policies may not have worked
  - Software Distribution may have missed a machine that's been off-network for a period of time.

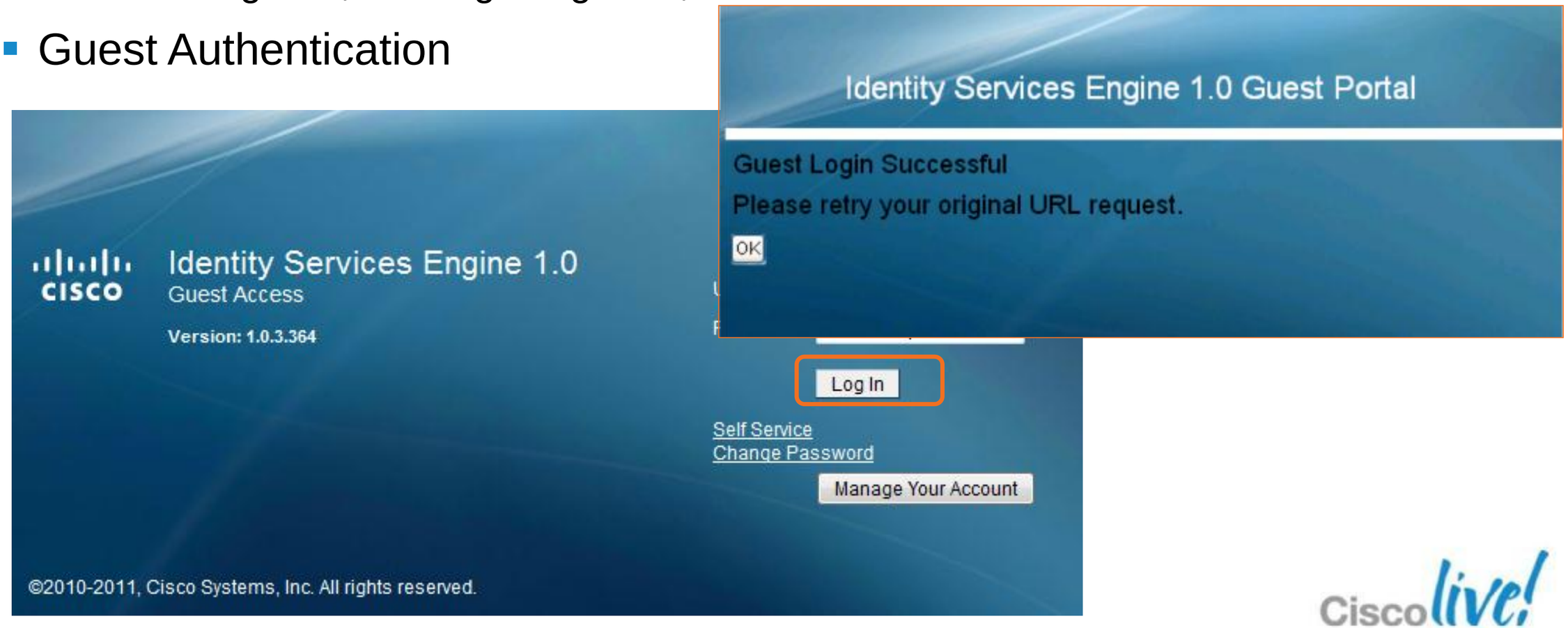
    Etc…
  - Dot1x Timeouts would take effect

    Someone who should have been an authorised user would end-up in the Guest Network

    HelpDesk gets a call from an unhappy user.

Enter: Web Authentication

- Used to identify users without supplicants
  - Mis-configured, missing altogether, etc.
- Guest Authentication

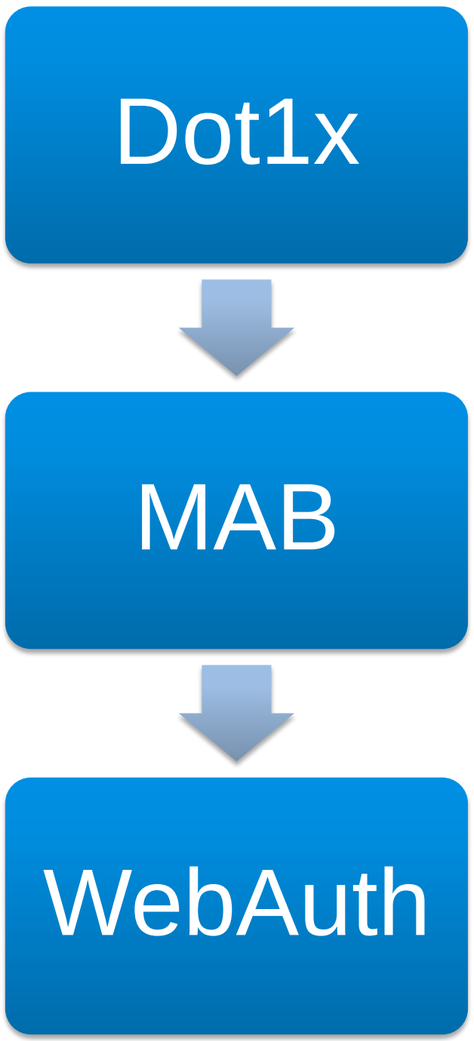


The Flow

New Term: Flex Auth

Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 !
 authentication event fail action next-method
 authentication order mab dot1x
 authentication priority dot1x mab
```



Business Case Continues to Evolve

- Requirements:

  Retailer-X must ensure that only Retailer-X employees are gaining access to the network.

  – **Solution: Identity with 802.1X**

  Authorised Non-Authenticating Devices must continue to have network access.

  – **Solution: Centralised MAB**

  Need to Automate the building of the MAB List

  – **Solution: *<Let's find out>***

Profiling

Profiling Technology

The Ability to Classify Devices

- Why Classify?
  - Originally: identify the devices that cannot authenticate and automagically build the MAB list.

    i.e.: Printer = Bypass Authentication
  - Today: Now we also use the profiling data as part of an authorisation policy.

    i.e.: Authorised User + i-device = Internet Only

Profiling

Visibility

PCs	Non-PCs			
	UPS	Phone	Printer	AP

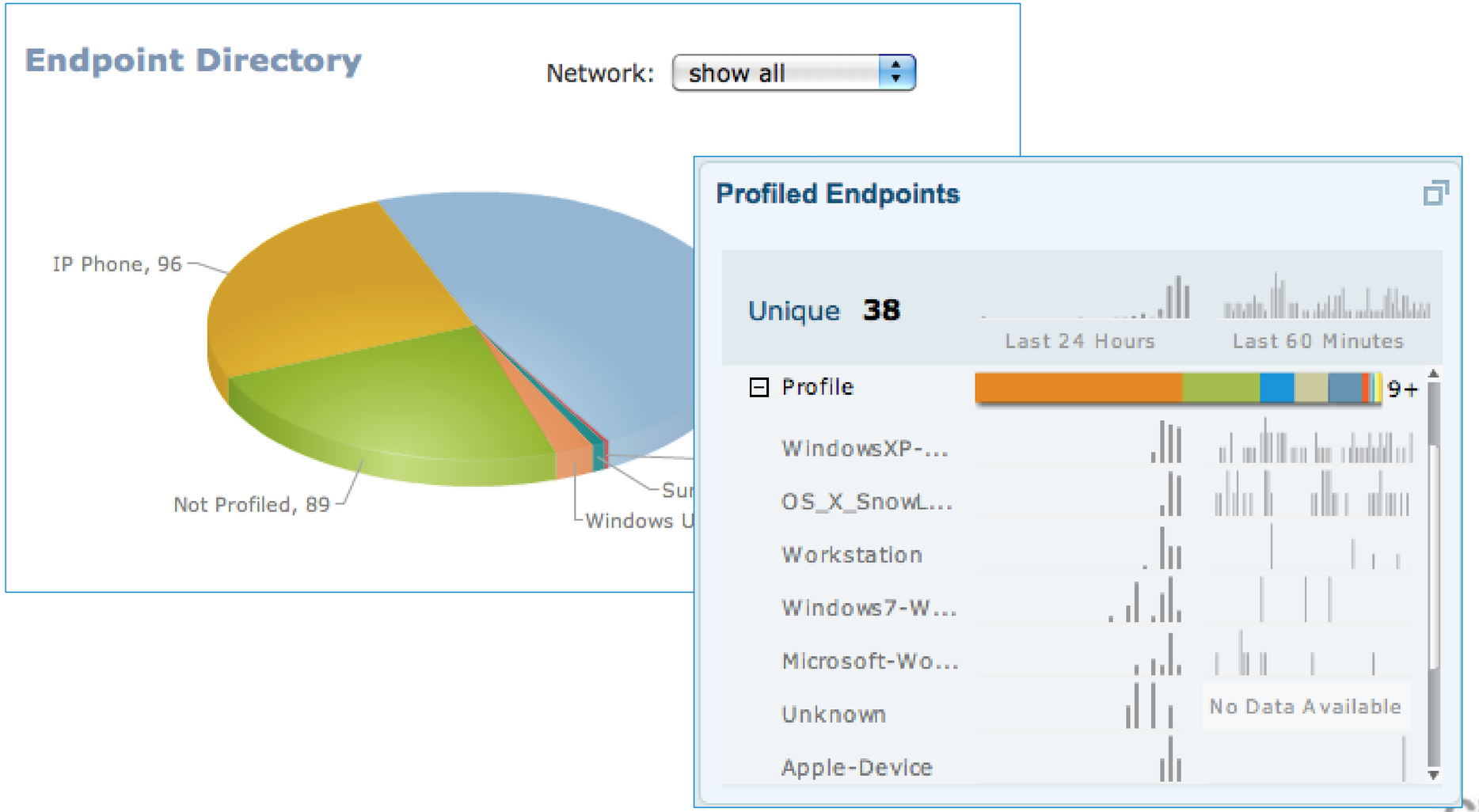
- Additional benefits of Profiling
  - Visibility: A view of what is truly on your network

Tracking of where a device has been, what IP Addresses it has had, and other historical data.

An understanding of WHY the device was profiled as a particular type (what profile signatures were matched)

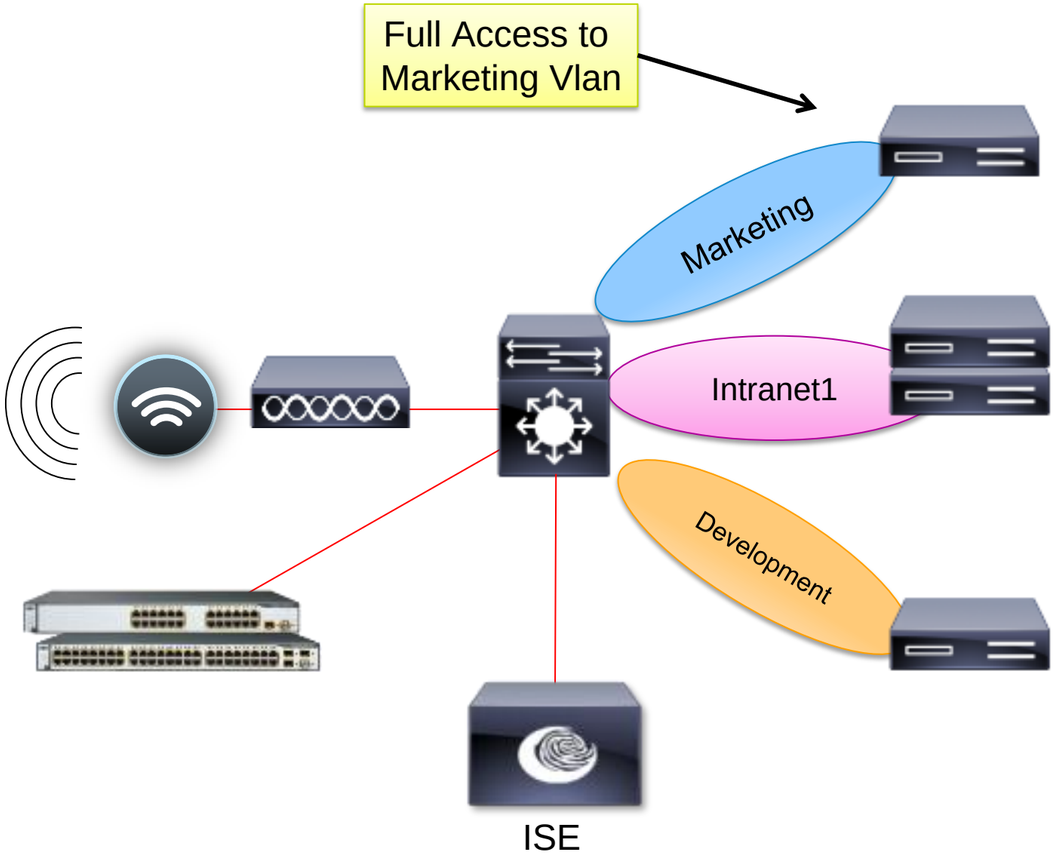
Profiling Technology

Visibility Into What is on the Network



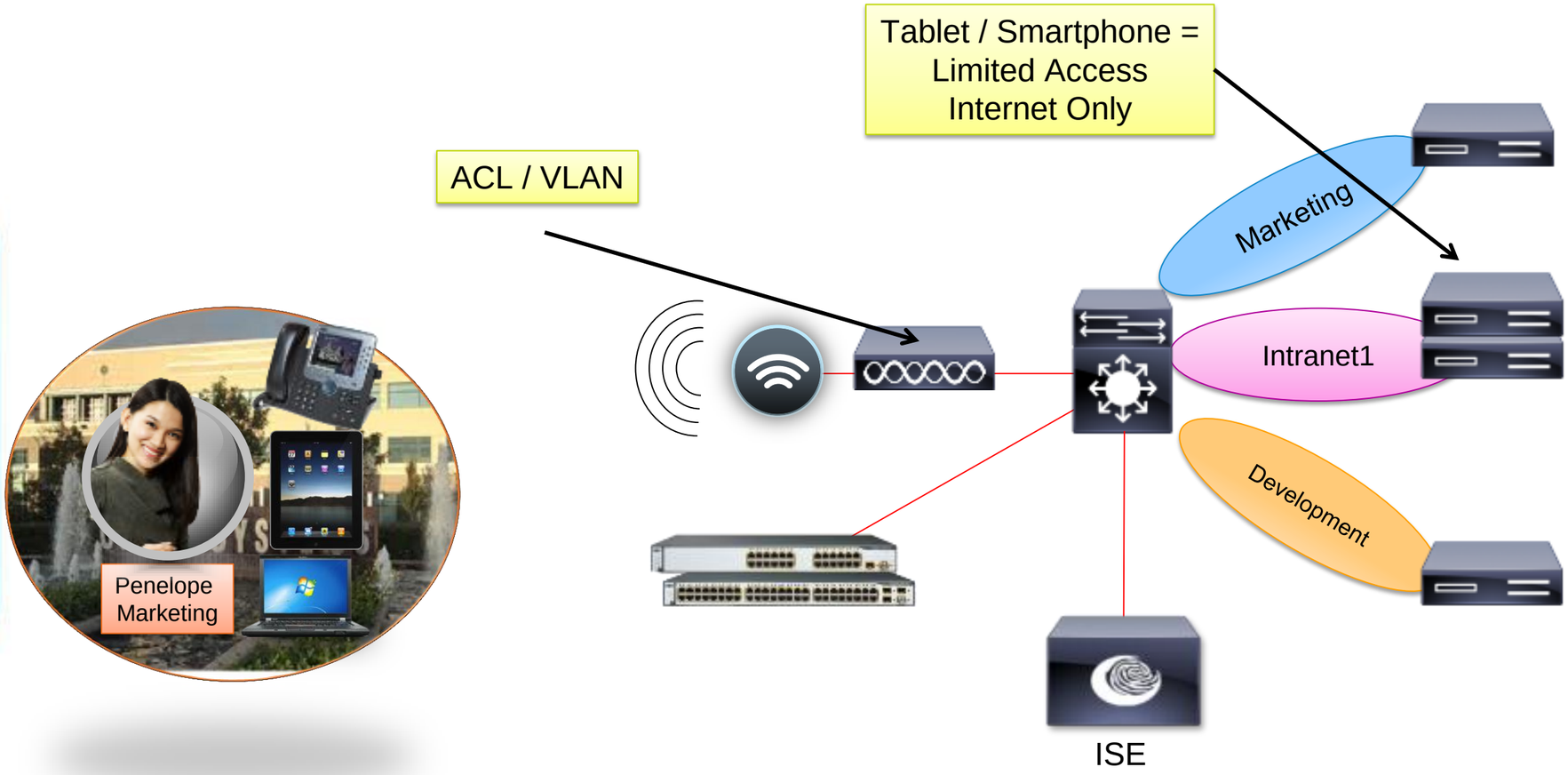
Profiling Benefit:

Access Policy Based on User AND Device Type



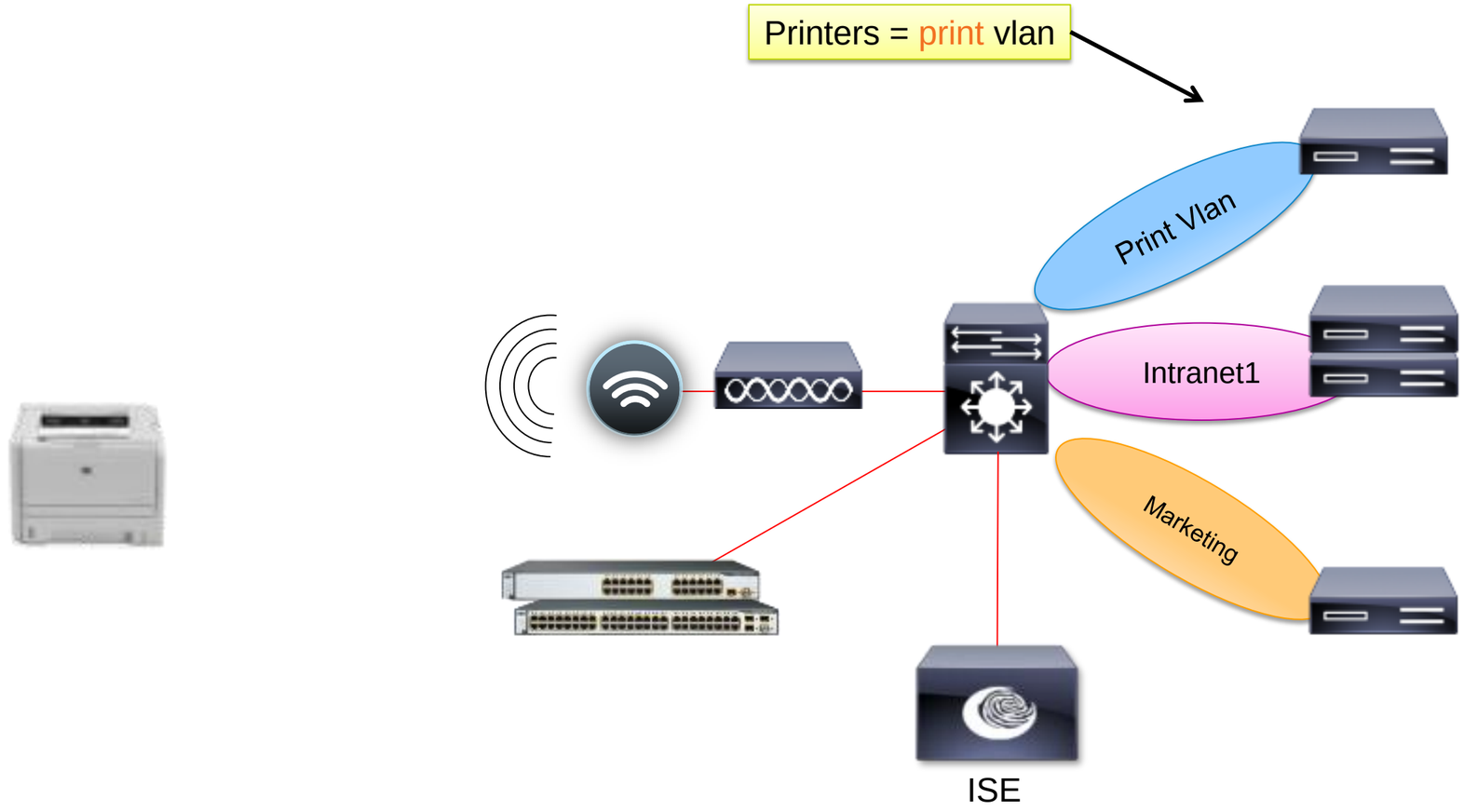
Profiling Benefit

Access Policy Based on User AND Device Type



Profiling Benefit

Access Policy Based on User AND Device Type



Profiling Technology

How Do We Classify a Device?

- Profiling uses Signatures (similar to IPS)

dhcp-client-identifier	d8:a2:5e:6b:41:83
dhcp-lease-time	691200
dhcp-max-message-size	1500
dhcp-message-type	DHCPACK
dhcp-parameter-request-list	1, 3, 6, 15, 119, 252

NetworkDeviceName	atw-wlc
OUI	Apple
PolicyVersion	7

User-Agent	Mozilla/5.0 (iPad; U; CPU OS 4_3_2 like Mac OS X; en-us) AppleWebKit/533.17.9

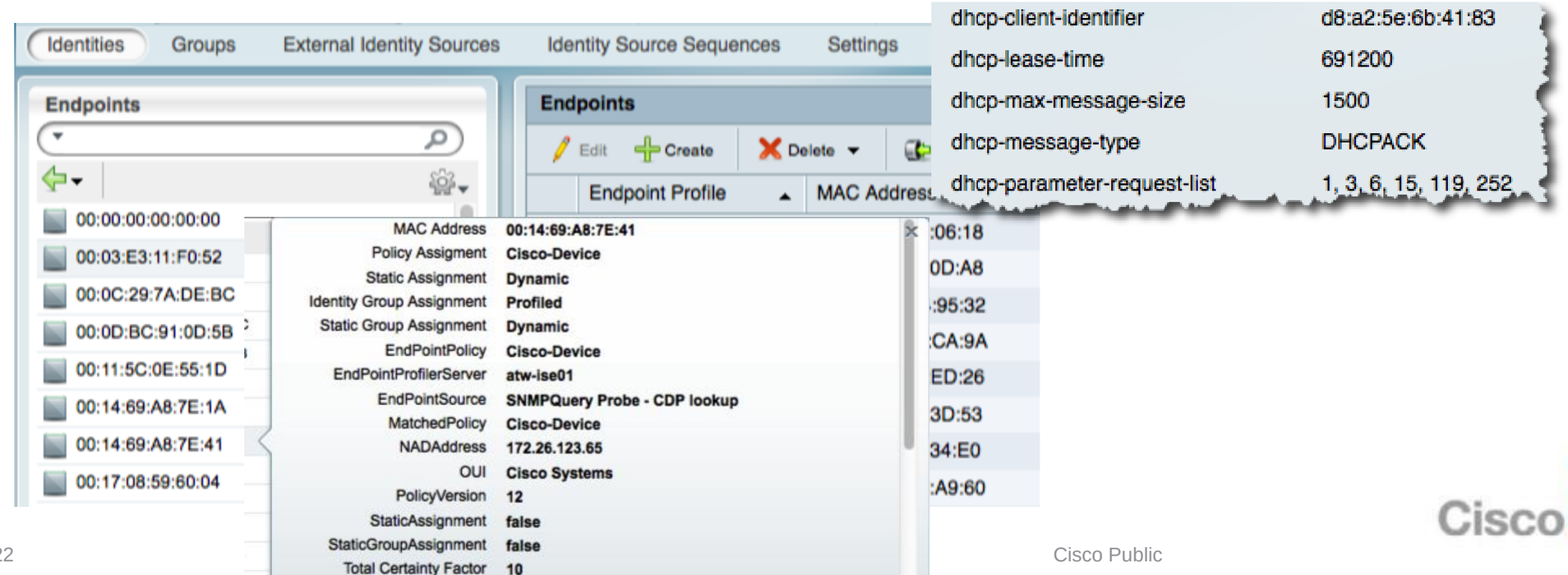
Endpoint List > B8:C7:5D:D4:95:32

* MAC Address	B8:C7:5D:D4:95:32
* Policy Assignment	Apple-iPad
Static Assignment	☐
* Identity Group Assignment	Apple-iPad
Static Group Assignment	☐

Understanding ISE Profiling

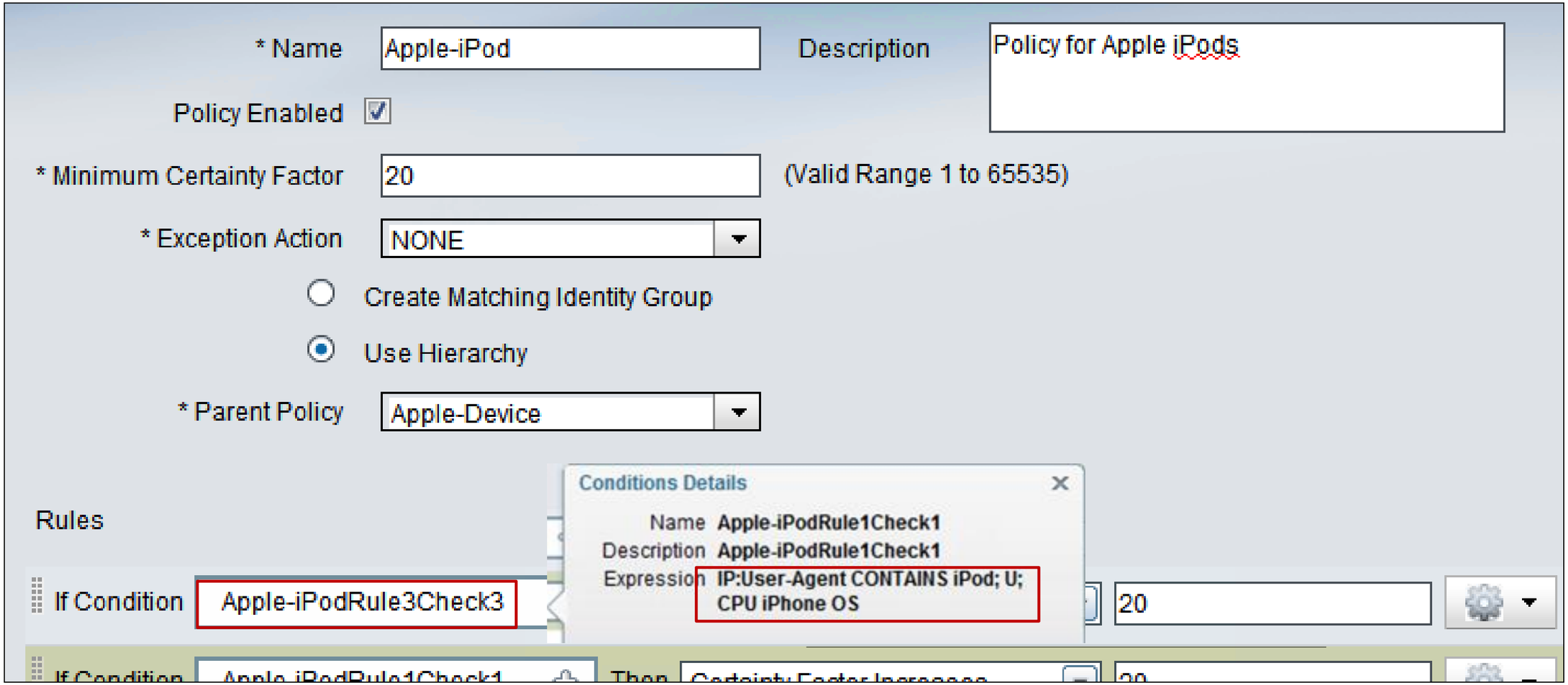
IP to MAC Address is Critical

- All Endpoints are uniquely identified by their MAC Addresses
  - If a Workstation is seen on Wired & Wireless = 2 devices in ISE
- If ISE is not L2 adjacent, then IP to MAC-Address Binding is critical
  - Today: this means DHCP Probe must be in place and working
  - Today: Sensor in the Switch (15.0(2)) Future: Sensor in the WLC (7.2MR)



Profiling

Determining Required Profile Attributes



Profiling

Determining Required Profile Attributes

Profiler Policy List > Apple-iPad

* Name: Apple-iPad

Description: Policy for Apple iPads

Policy Enabled: ☑

* Minimum Certainty Factor: 20 (Valid Range 1 to 65535)

* Exception Action: NONE

Create Matching Identity Group

Use Hierarchy

* Parent Policy: Apple-Device

Rules

If Condition: Apple-iPadRule2Check2 Then Certainty

If Condition: Apple-iPadRule1Check1_AND_Apple-MacBo...

Conditions Details

Name	Expression	Operato
Apple-iPadRule1Check1	IP:User-Agent CONTAINS iPad	AND
Apple-MacBookRuleCheck2	IP:User-Agent CONTAINS Mac OS	AND
Apple-	IP:User-Agent	

Profiling

Profile Conditions Reveal Specific Probes and Attributes

AndroidRule1Check1	User-Agent CONTAINS Android
AndroidRule1Check2	host-name CONTAINS android
Apple-DeviceRule1Check1	OUI CONTAINS Apple
Apple-MacBookRuleCheck1	User-Agent CONTAINS Macintosh
Apple-MacBookRuleCheck2	User-Agent CONTAINS Mac OS
Apple-iPadRule1Check1	User-Agent CONTAINS iPad
Apple-iPadRule1Check3	
Apple-iPadRule2Check2	
Apple-iPhoneRule-TEST	
Apple-iPhoneRule1Check1	

HP-DeviceRule2Check1	OUI CONTAINS Hewlett
HP-JetDirect-Printer-Check	dhcp-class-identifier CONTAINS JetDirect
HTC-DeviceRule1Check1	OUI EQUALS HTC Corporation
ISE-ApplianceCheck	cdpCachePlatform CONTAINS ISE
Kubuntu-WorkstationRule1Check1	User-Agent CONTAINS Kubuntu
Lexmark-DeviceRule1Check1	OUI CONTAINS Lexmark
Lexmark-Printer-E260dnRule1Check1	dhcp-class-identifier CONTAINS Lexmark E

Profiling Technology

Limitations of Profiling

- Best Guess: The profiling is based on Best-Effort
- MAB is a Filter: It was only used to determine what MAC Addresses were allowed to “skip” Authentication
  - Now we also use the profiling data as part of an authorisation policy.
  - i.e.: Authorised User + i-device = Internet Only

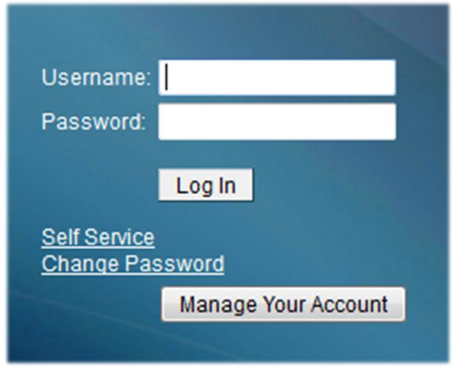
Business Case Continues to Evolve

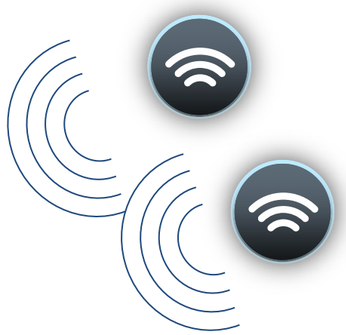
- Requirements:
  1. Retailer-X must ensure that only Retailer-X employees are gaining access to the network.
  – ***Solution: Identity with 802.1X***
  2. Authorised Non-Authenticating Devices must continue to have network access.
  – ***Solution: Centralised MAB***
  3. Need to Automate the building of the MAB List
  – ***Solution: Use Profiling technology to automate the building MAB list.***

Business Case Evolution

Improving Guest Access

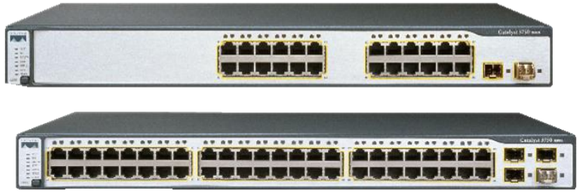
Guest Users' Needs





WLC

Wireless APs



LAN

Internet

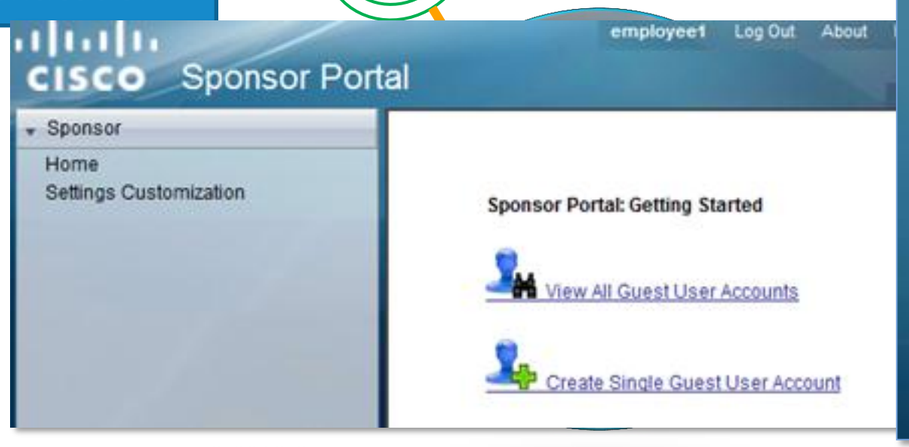
How Does It Work?

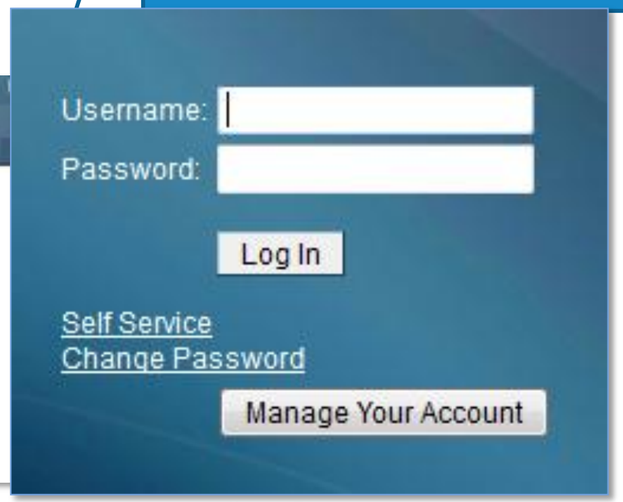
Redirection of the guest web session to ISE guest portal for authentication

Access authorised for guest user

Open SSID « guest » With Web authentication

Guest account needs to be created:
via a sponsor
or self service





Components of a Full Guest Lifecycle Solution

Provisioning: Guest accounts via sponsor portal

Notify: Guests of account details by print, email, or SMS

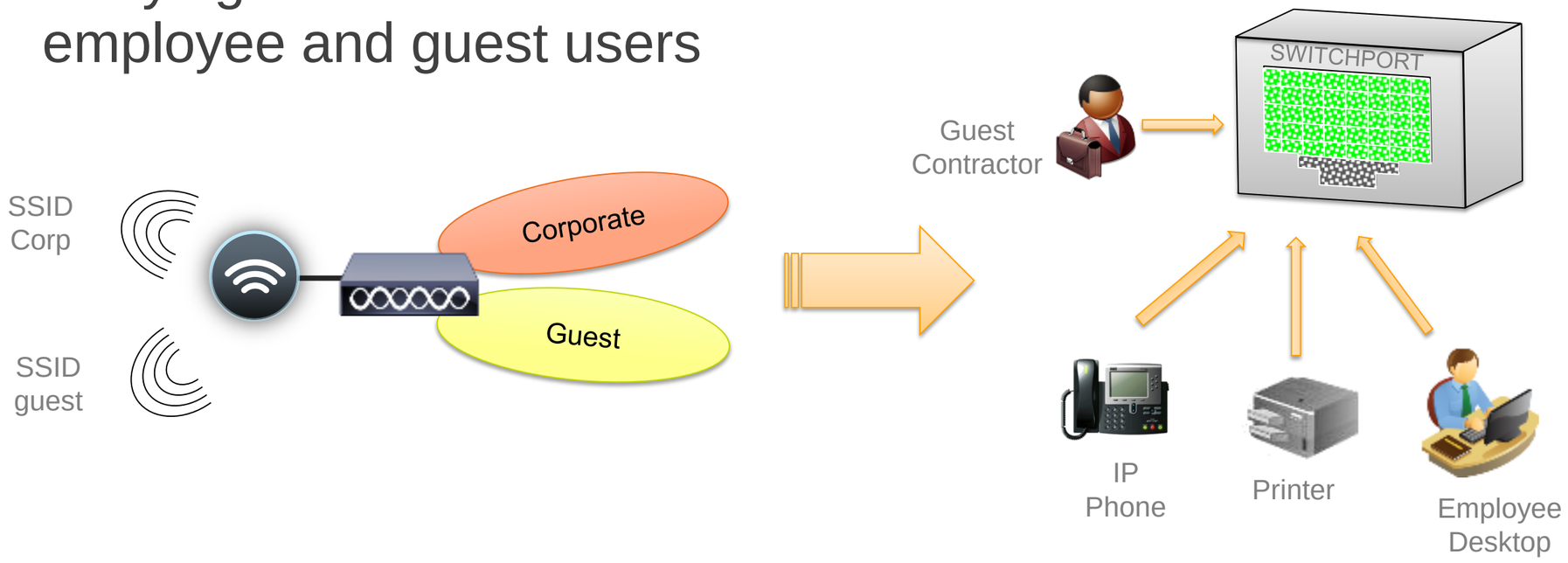
Manage: Sponsor privileges, guest accounts and policies, guest portal

Authenticate/Authorise guest via a guest portal on ISE

Report: On all aspects of guest accounts

Providing Network Access to Guests

- Unifying network access for employee and guest users



On wireless:

- Using multiple SSIDs
- Open SSID for guest

On wired:

- No notion of SSID
- Unified port: need to use different authentication & authorisation methods into one port

Components of a Full Guest Lifecycle Solution

Provisioning: Guest accounts via sponsor portal
Notify: Guests of account details by print, email, or SMS

Manage: Sponsor privileges, guest accounts and policies, guest portal

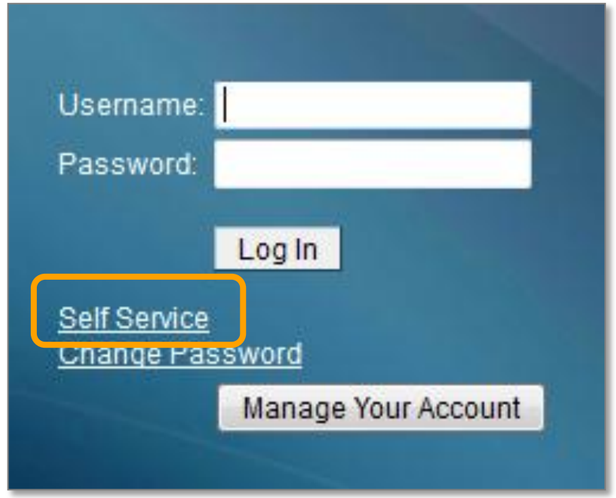
Authenticate/Authorise guest via a guest portal on ISE

Report: On all aspects of guest accounts

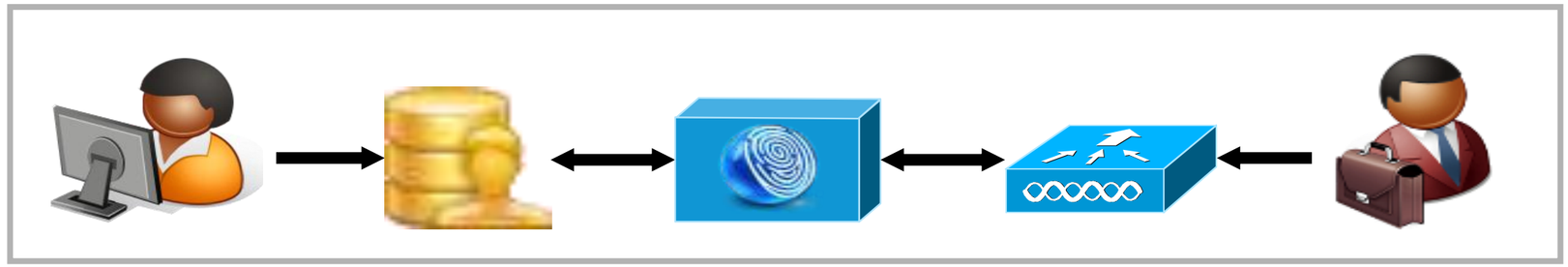
Guest Users DB – Account Creation Methods

Two Ways to Populate ISE Internal Guest Database

- Self-Service
  Option on ISE ‘Guest Portal’



- Sponsoring
  via ISE ‘Sponsor Portal’



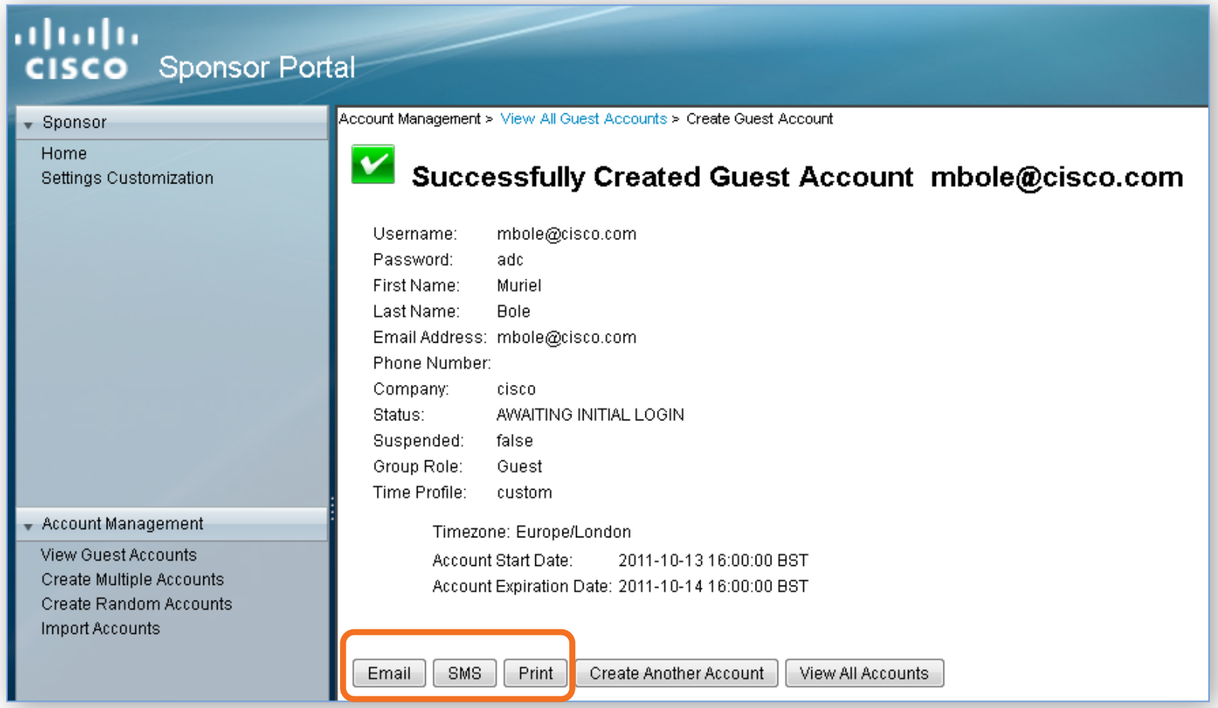
ISE – Sponsor Portal

- Customisable sponsor pages
- Sponsor privileges tied to authentication/ authorisation policy
  - Roles sponsor can create
  - Time profiles can be assigned
  - Management of other guest accounts
  - Single or bulk account creation
- Sponsor and Guest reporting and audit

Sponsor Portal: Informing Guests

Sponsor will have three ways to inform guest

1. Printing the details
2. Sending the details via e-mail
3. Sending the details via SMS



Guest User Roles

- When need for different policies for users

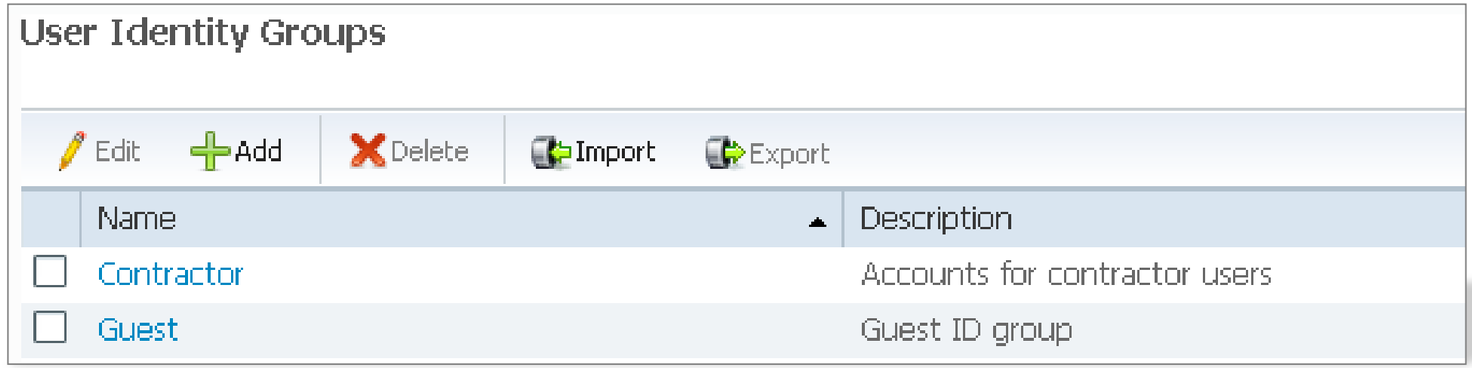
Guest

- Internet access only
- Limited connection time:
½ day, one day

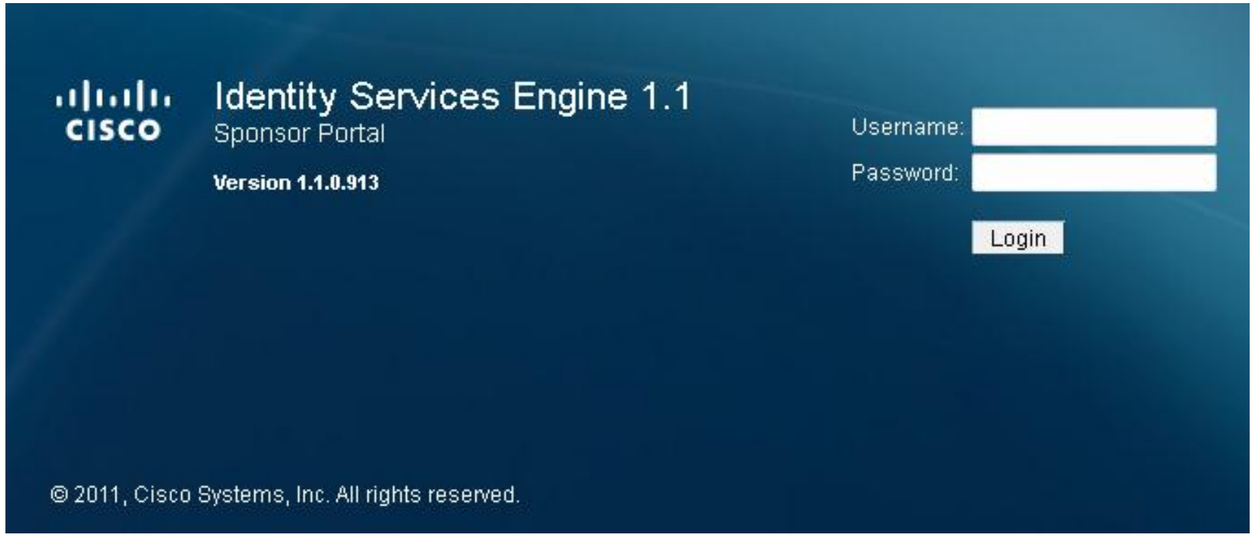
Contractor

- Internet access
- Access to selected resources
- Longer connection time:
one week, one month

- Use of several user identity groups in ISE:



Sponsor Groups and Privileges



Sponsor group1

- Can create user in groups: ‘contractor’ and ‘guest’
- Can use time profiles up to one week
- Can see all accounts in group

Sponsor group2

- Can create user in group ‘guest’ only
- Can use time profiles up to one day
- Cannot do bulk creation

Components of a Full Guest Lifecycle Solution

Provisioning: Guest accounts via sponsor portal

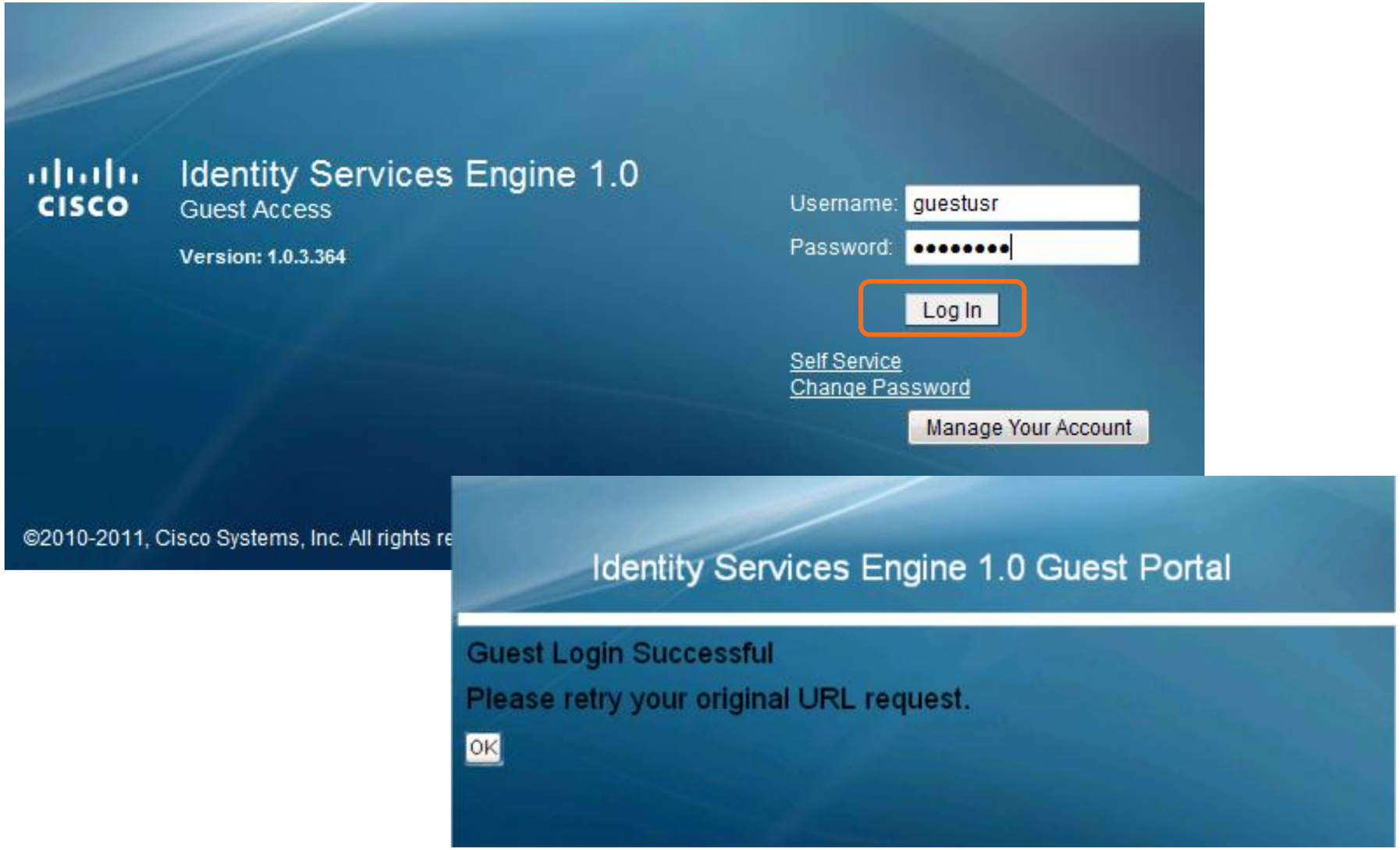
Notify: Guests of account details by print, email, or SMS

Manage: Sponsor privileges, guest accounts and policies, guest portal

Authenticate/Authorise guest via a guest portal on ISE

Report: On all aspects of guest accounts

ISE – Web Authentication



Components of a Full Guest Lifecycle Solution

Provisioning: Guest accounts via sponsor portal

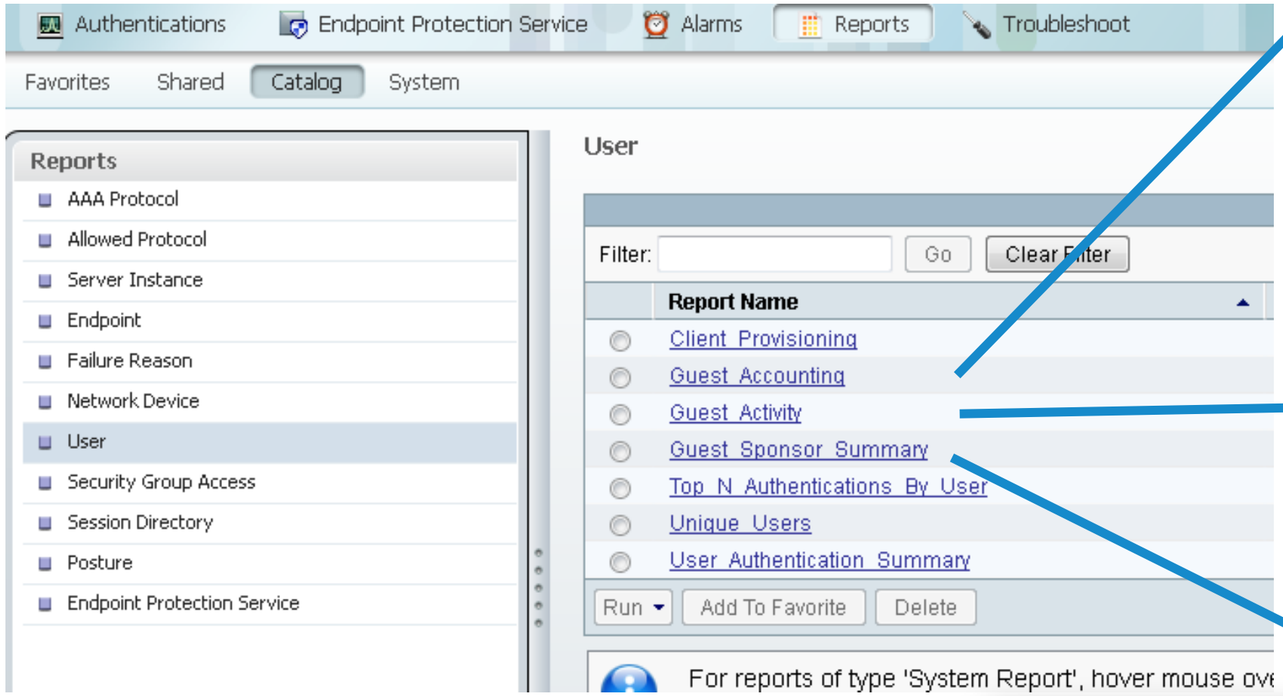
Notify: Guests of account details by print, email, or SMS

Manage: Sponsor privileges, guest accounts and policies, guest portal

Authenticate/Authorise guest via a guest portal on ISE

Report: On all aspects of guest accounts

Full Audit of Guest Lifecycle



Description:
View the logged in/out information for the particular Guest user for a selected time period

Description:
View the Guest information for a selected time period

Description:
View the sponsor information along with the graphical representation for a selected time period

Business Case Evolution

We Have Identity… We Have Guests Lifecycle Management…

Can We Get More Information?

Business Case Continues to Evolve

- Requirements:
  4. Employee's of Retailer-X Must be using a Corporate-owned asset.
  5. All Corporate assets must be running Trend Micro Anti-Virus, and it must be up-to-date.
  6. All guests must run Antivirus (any).
  - ***Solution: Let's find out ☺***

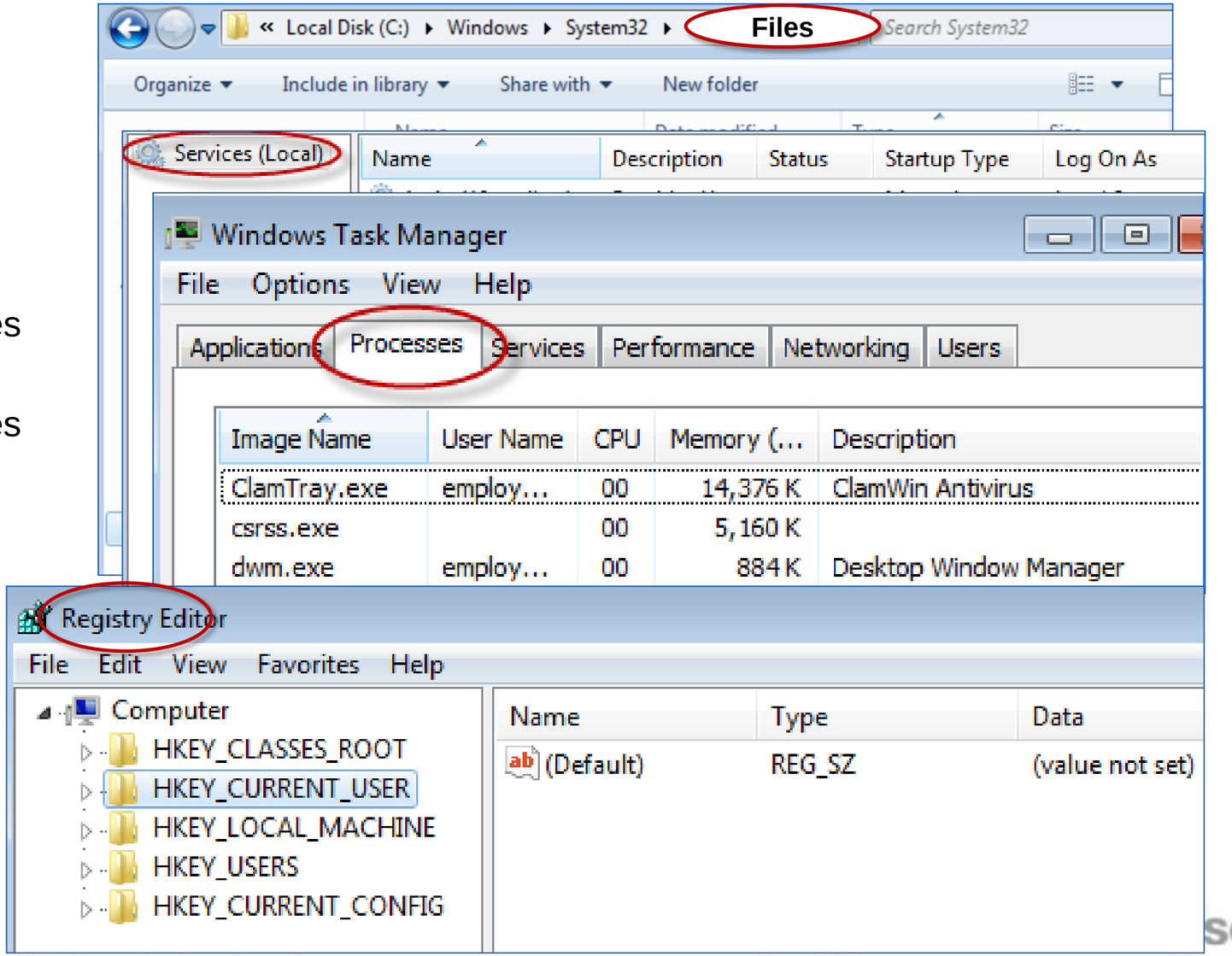
Posture Assessment

Does the Device Meet Security Requirements?

- Posture = the state-of-compliance with the company's security policy.
  - Is the system running the current Windows Patches?
  - Anti-Virus Installed? Is it Up-to-Date?
  - Anti-Spyware Installed? Is it Up-to-Date?
- Now we can extend the user / system Identity to include their Posture Status.

ISE – Posture Assessment Checks

- Microsoft Updates
  - Service Packs
  - Hotfixes
  - OS/Browser versions
- Antivirus
  Installation/Signatures
- Antispyware
  Installation/Signatures
- File data
- Services
- Applications/
  Processes
- Registry keys



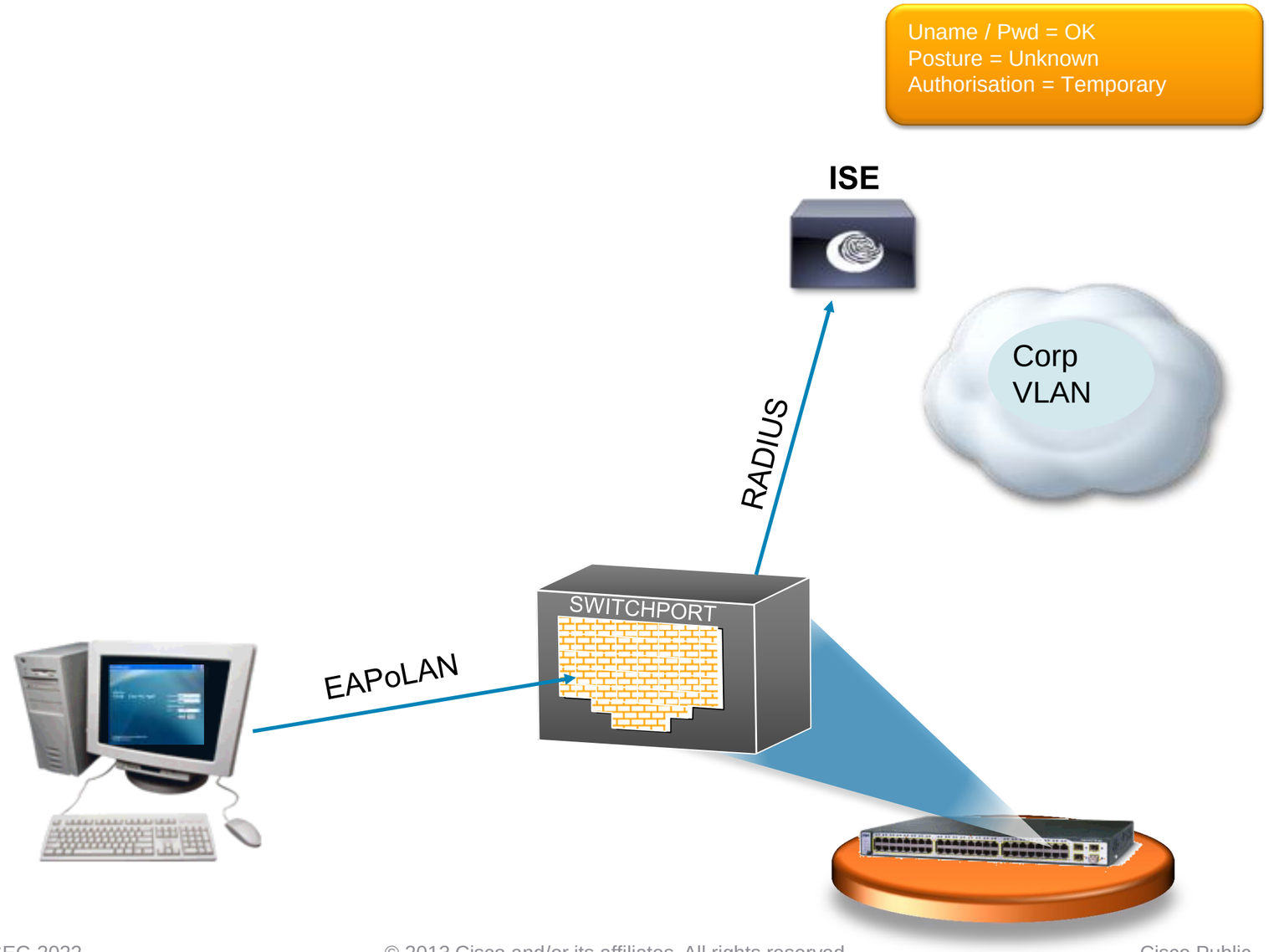
Posture Assessment

What if a User Fail the Check?

- New term: Remediation
  - The act of correcting any missing or out-of-date items from the Posture Assessment.
  - This can trigger the use of:
    - Corporate Patching Systems (ex: BigFix, Altiris, etc.)
    - Windows Software Update Service (WSUS)
    - Windows Update
    - Anti-Virus product Update Services (LiveUpdate.exe, etc.)

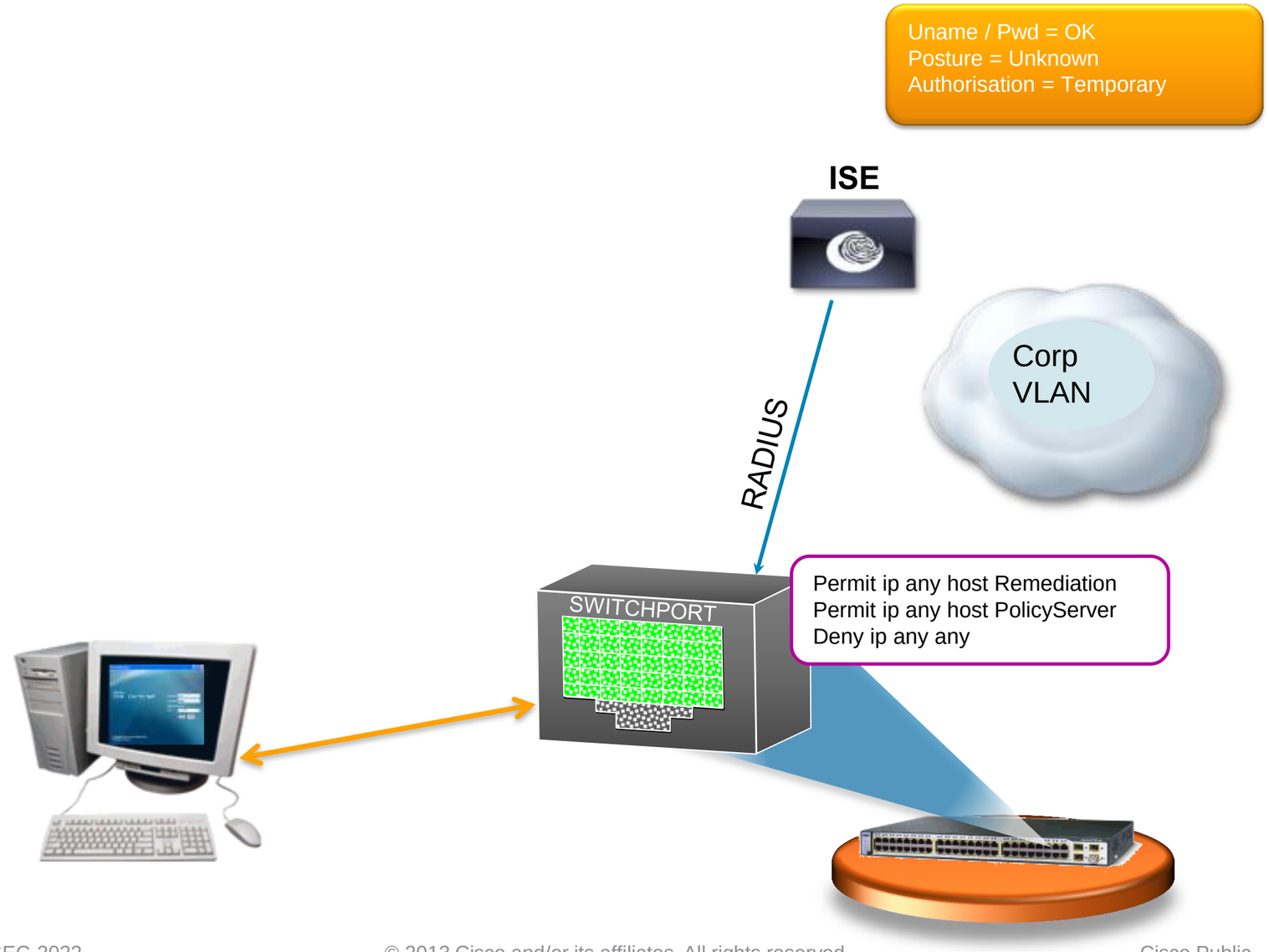
Posture Assessment Flow

Posture



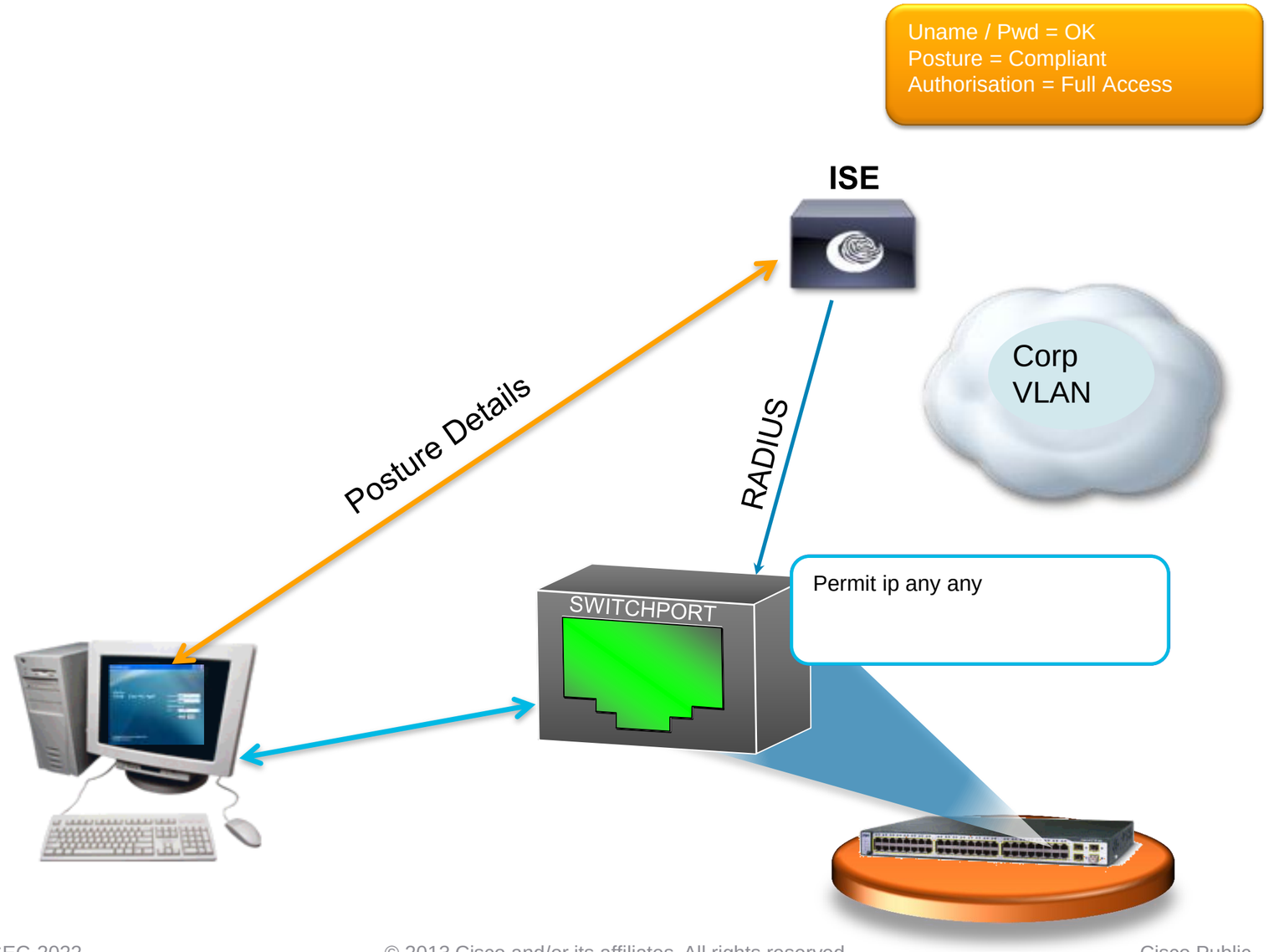
Posture Assessment Flow

Posture



Posture Assessment Flow

Posture



Making this Work Well

Change of Authorisation (CoA)

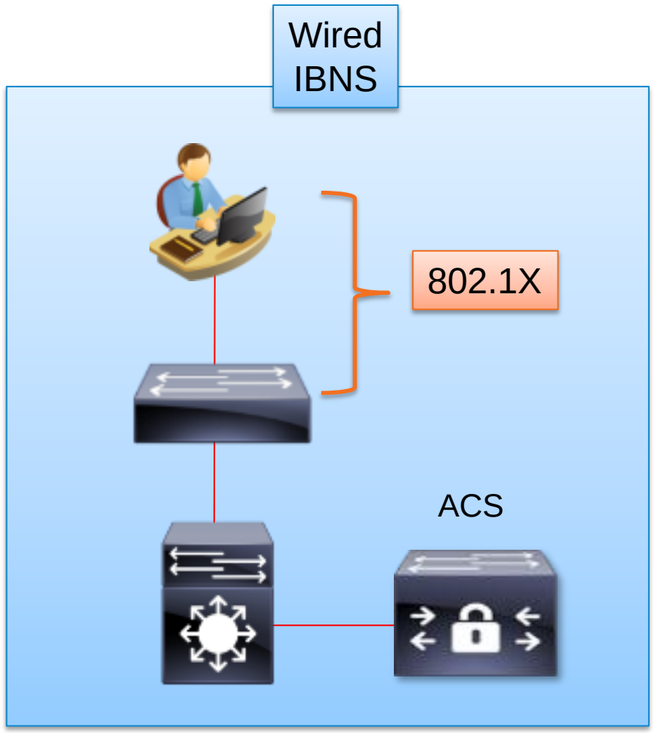
- CoA allows an enforcement device (switchport, wireless controller, VPN device) to change the VLAN/ACL/Redirection for a device/user without having to start the entire process all over again.
- Without it: Remove the user from the network & then have the entire AAA process begin again.
  - i.e.: disassociate wireless device & have to join wireless again.
- RFC 3576 and 5176

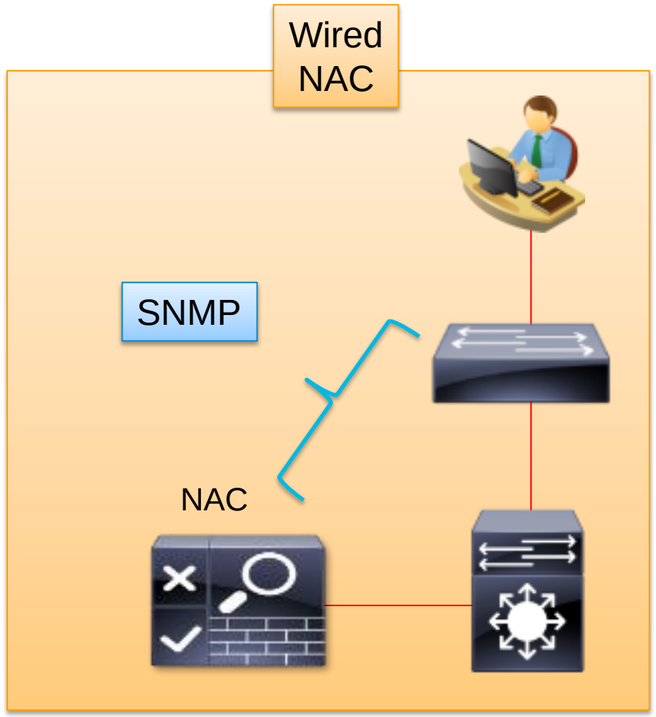
Creating a System out of these Technologies

Network Access Controls

Multiple Options for Wired Networks

- Identity Based Network Services (IBNS):
  - 802.1X for wired access
  - Profiling by NAC Profiler
  - Guest = NGS
- Cisco NAC Appliance:
  - VLAN control via SNMP Control Plane
  - Profiling by NAC Profiler
  - Guest = NGS

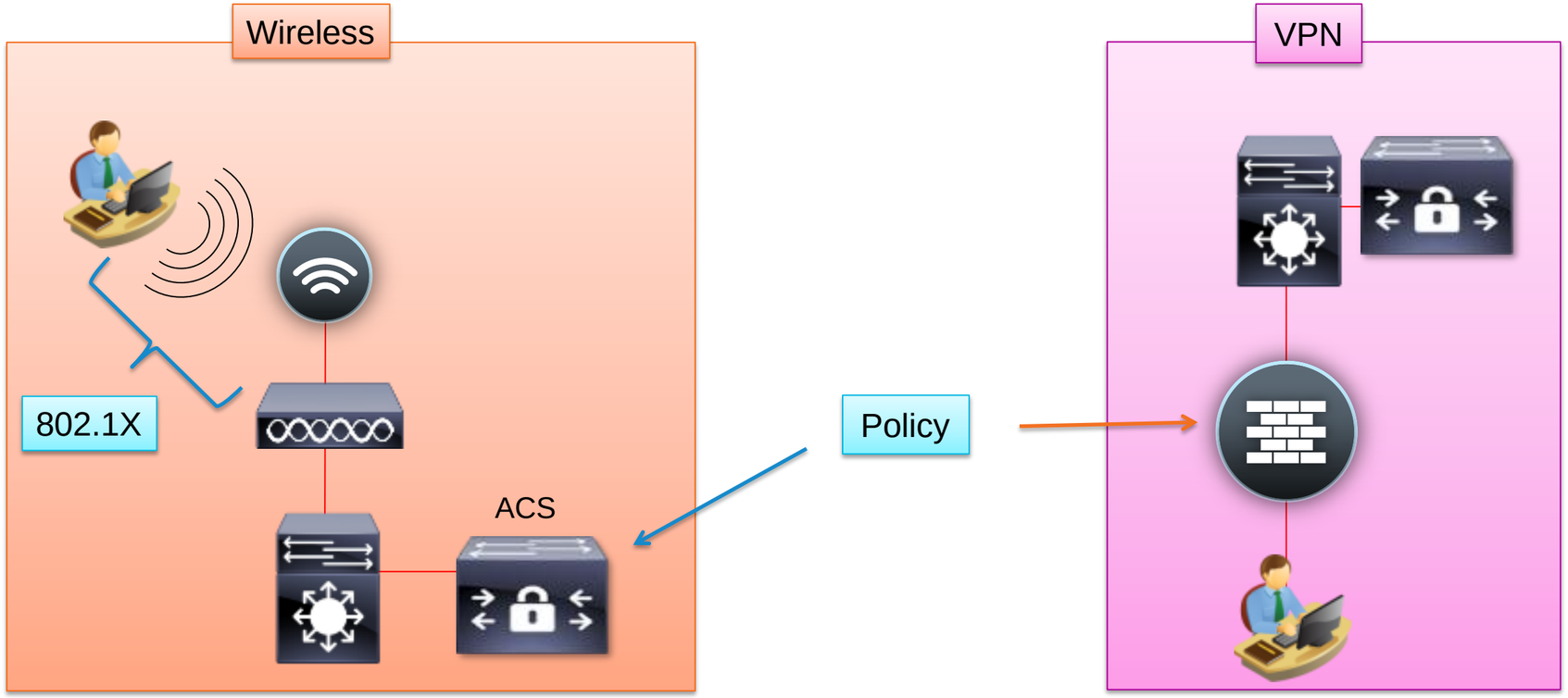




Network Access Controls

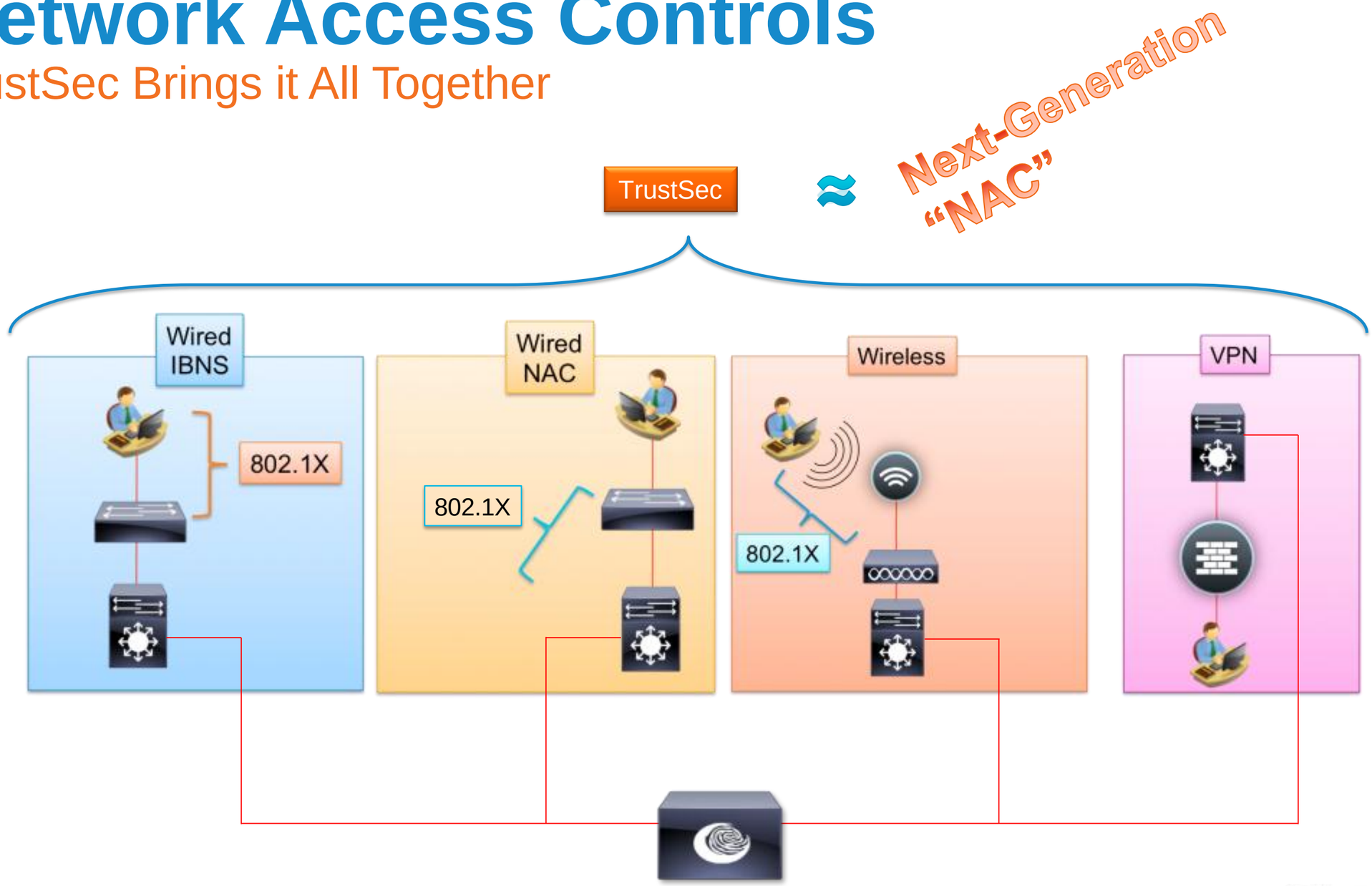
Wireless and VPN Access

- Wireless Access
  - 802.1X controlled by WLC
  - WLC has local enforcement
  - Separate Policies on ACS
- Remote Access VPN
  - Policy controlled by ASA, or:
  - Policy controlled by in-line NAC
  - Separate Policies on ACS



Network Access Controls

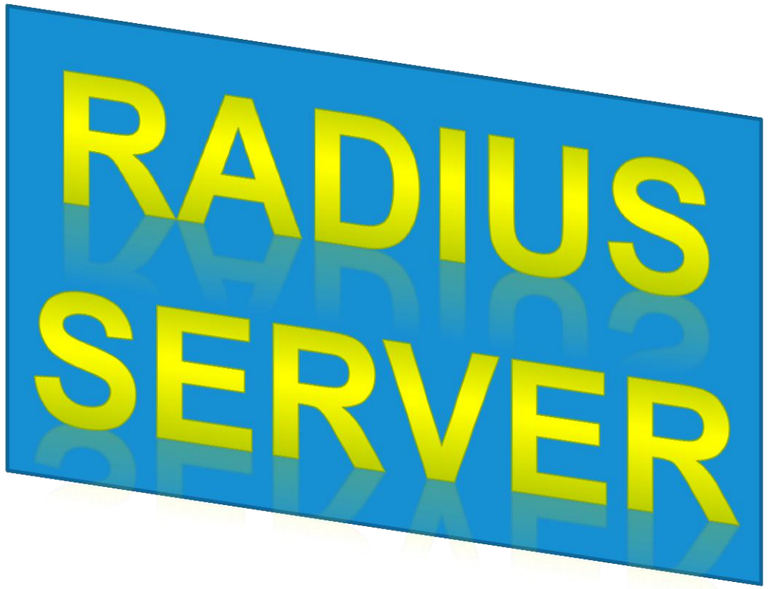
TrustSec Brings it All Together



What is the Identity Services Engine?

ISE is a Next-Generation RADIUS Server

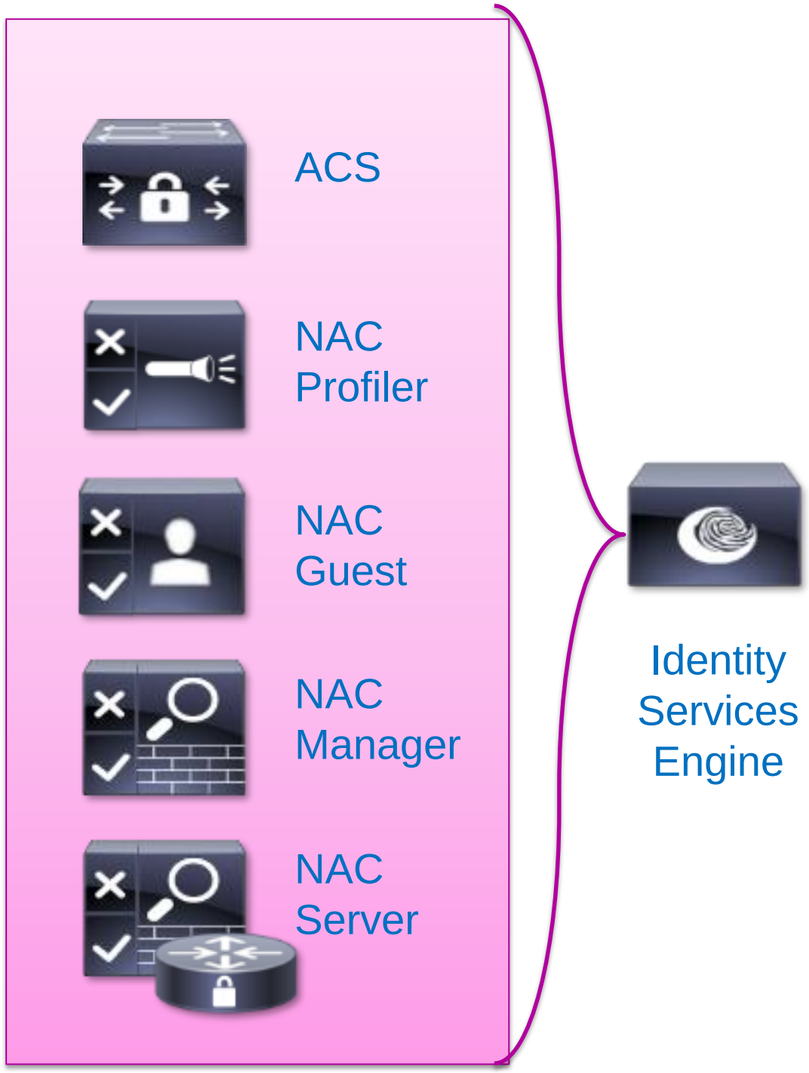
≈



Note: RADIUS for Network Access ONLY

Identity Services Engine

Policy Server Designed for TrustSec



- Centralised Policy
- AAA Services
- Posture Assessment
- Guest Access Services
- Device Profiling
- Monitoring
- Troubleshooting
- Reporting

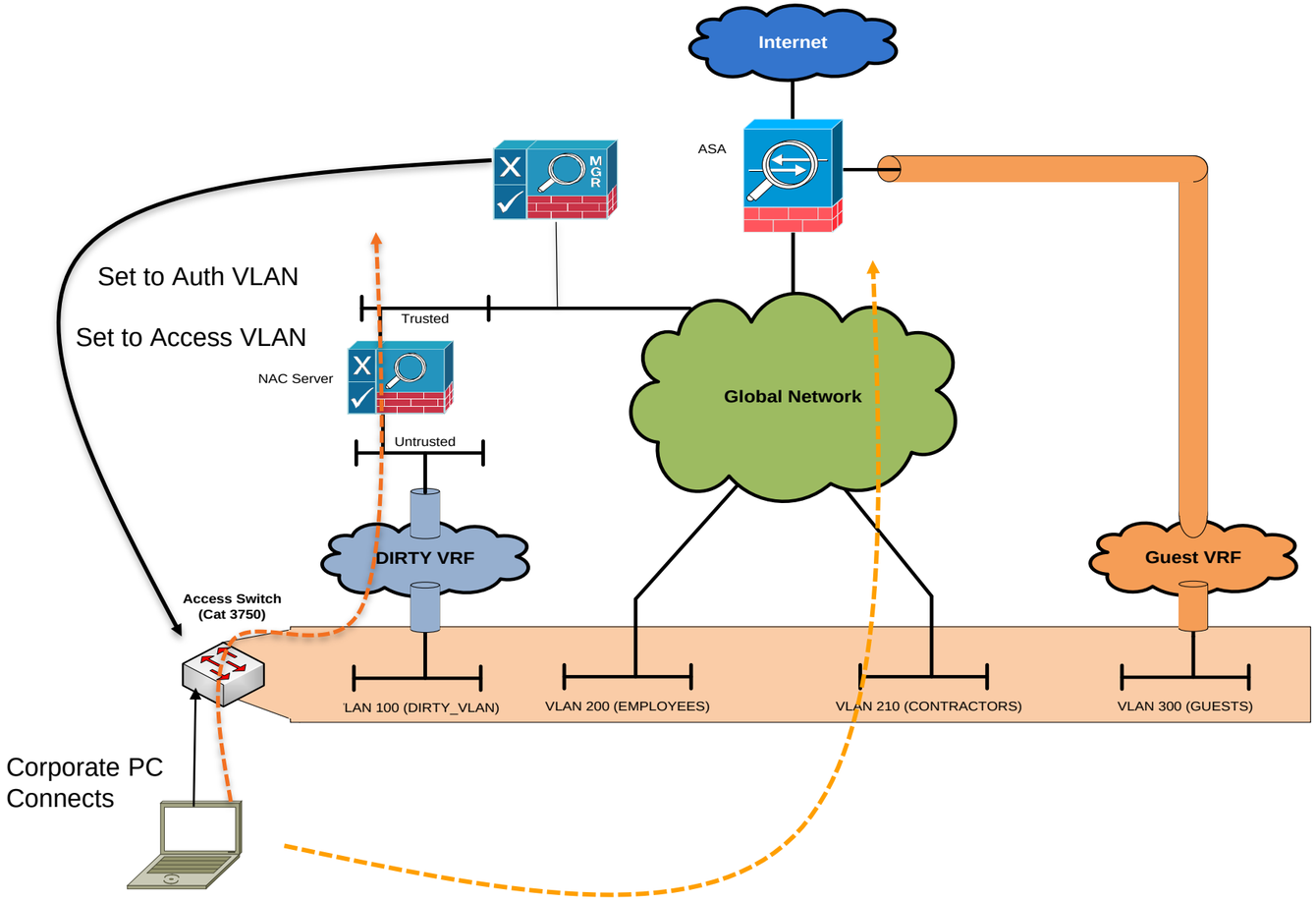
A “Systems” Approach

A Systems Approach

Why is This so Important?

- When Identity is an overlay (like NAC Appliance)
  - There is an appliance or some other device that is doing the enforcement.
    - Called a Policy Enforcement Point (PEP)
  - The trick is to “shape” traffic towards those PEP’s
    - Some use DHCP or DNS Tricks
    - Others use MAC Spoofing (Man-in-the-Middle)
    - Cisco uses the network to get traffic to the Appliance:
      - Virtual Networks (VRF’s)
      - Policy Based Routing (PBR), etc.

Overlay Solution



A Systems Approach

Why is This so Important?

- When Identity is embedded (like 802.1X)
  - The Switch, WLC, or VPN is the enforcement device
    - Called a Policy Enforcement Point (PEP)
  - The Switch does all the work, instead of an appliance
    - URL Redirection
    - Policy Enforcement with ACL's, SGT's, VLAN Assignment, etc…

A Systems Approach

Switch is the Enforcement Point

```
NACs1#sho authentication sess int fa1/0/9
            Interface:  FastEthernet1/0/9
          MAC Address:  0050.56a7.44d7
           IP Address:  172.26.123.67
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4da5104d
                  SGT:  0002-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  AC1A7836000000102A805ACC
      Acct Session ID:  0x0000001A
               Handle:  0xDE000010

Runnable methods list:
       Method   State
       mab      Not run
       dot1x    Authc Success

NACs1#
```

A Systems Approach

Switch is the Enforcement Point

```
NACs1#sho authentication sess int fa1/0/9
            Interface:  FastEthernet1/0/9
          MAC Address:  0050.56a7.44d7
           IP Address:  172.26.123.67
            User-Name:  00-50-56-A7-44-D7
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-INET-ONLY-4dcbe020
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
         URL Redirect:  https://atw-ise01.clt.cisco.com:8443/guestportal/gatewa
?sessionId=AC1A7836000000102A805ACC&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  AC1A7836000000102A805ACC
      Acct Session ID:  0x00000019
               Handle:  0xDE000010

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

Adding Power to Dot1X

Secure Group Access

Topology Independent Access Control

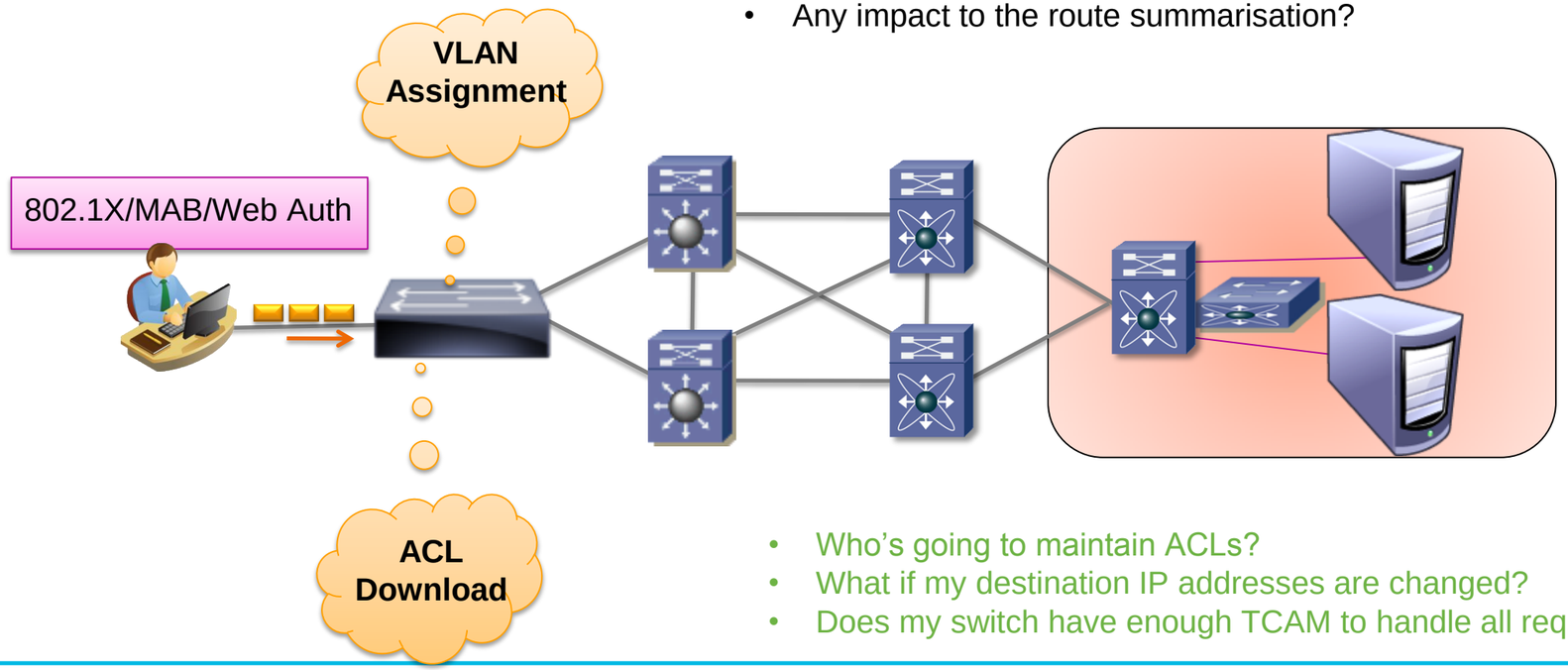
SGT	Public	Private
Staff	Permit	Permit
Guest	Permit	Deny

- Term describing use of:
  - Secure Group TAG (SGT's)
  - Secure Group ACL's (SGACL's)
  - When a user log's in they are assigned a TAG (SGT) that identifies their role
  - The TAG is carried throughout the Network
- Server Switch applies SGACL's based on a "Matrix" (see above).

For more on SGA: BRKSEC-2046 (Security Group Tagging and MACSec)

Customer Challenges - Ingress Access Control

- Can I create / manage the new VLANs or IP Address scope?
- How do I deal with DHCP refresh in new subnet?
- How do I manage ACL on VLAN interface?
- Does protocol such as PXE or WOL work with VLAN assignment?
- Any impact to the route summarisation?



- Who's going to maintain ACLs?
- What if my destination IP addresses are changed?
- Does my switch have enough TCAM to handle all request?

- Traditional access authorisation methods leave some deployment concerns:
  - Detailed design before deployment is required, otherwise…
  - Not so flexible for changes required by today's business
  - Access control project ends up with redesigning whole network

What is Secure Group Access?

SGA is a part of TrustSec

- Next-Generation Access Control Enforcement
  - Removes concern TCAM Space for detailed Ingress ACLs
  - Removes concern of ACE explosion on DC Firewalls
- Assign a TAG at Login → Enforce that tag in the Data Centre.

What is a Secure Group Tag?

A Role-Based TAG:

1. A user (or device) logs into network via 802.1X
2. ISE is configured to send a TAG in the Authorisation Result – based on the “ROLE” of the user/device
3. The Switch Applies this TAG to the users traffic.

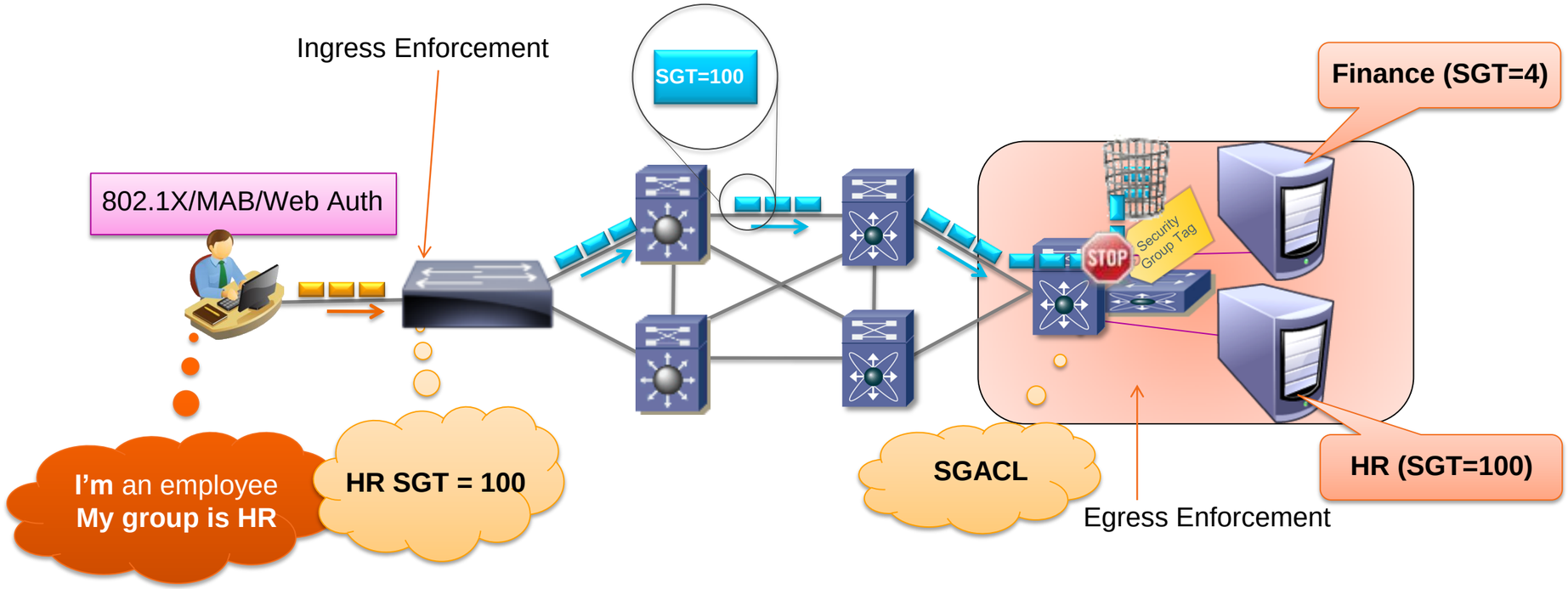
```
C3750X#sho authentication sess int g1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5687.0004
           IP Address:  10.1.10.50
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-Employee-ACL-
                  SGT:  0002-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0130020000002 2DC6C328F
      Acct Session ID:  0x00000033
               Handle:  0xCC000022

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

Security Group Based Access Control

SGA Allows Customers:

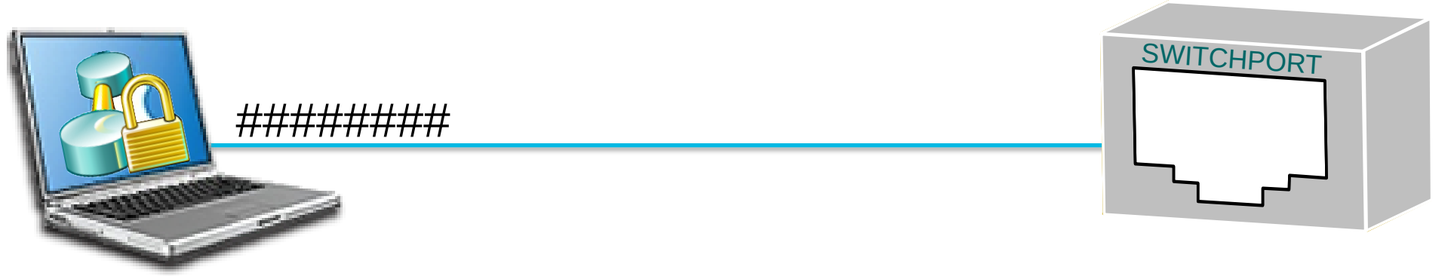
- To keep existing logical design at access layer
- To change / apply policy to meet today's business requirement
- To distribute policy from central management server



Media Access Control Security

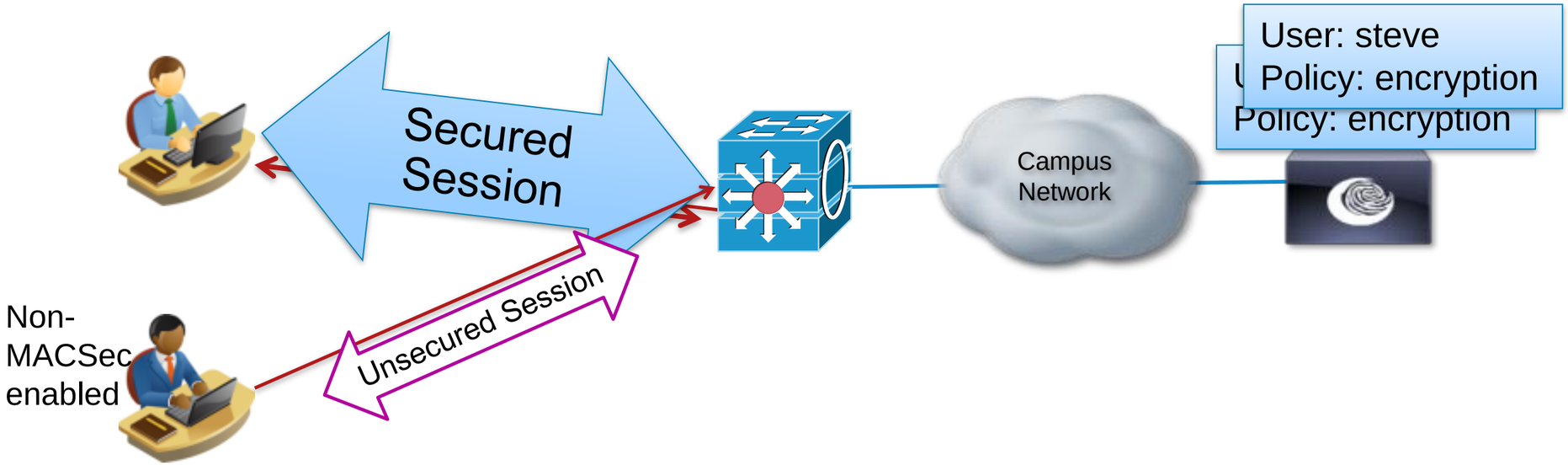
MACSec: Layer-2 Encryption (802.1AE)

- Industry Standard Extension to 802.1X
  - Encrypts the link between the host & the switch.
  - Traffic in the backplane is unencrypted for inspection, etc.
  - Requires a supplicant that supports MACSec and the encryption key-exchange



For more on MACSec: BRKSEC-2046 (Security Group Tagging and MACSec)

MACSec in Action



1. User bob connects.
2. Bob's policy indicates endpoint must encrypt.
3. Key exchange using MKA, 802.1AE encryption complete.
   User is placed in corporate VLAN.
   Session is secured.
4. User steve connects
5. Steve's policy indicates endpoint must encrypt.
6. Endpoint is not MACSec enabled.
   Assigned to guest VLAN.

802.1X-Rev Components

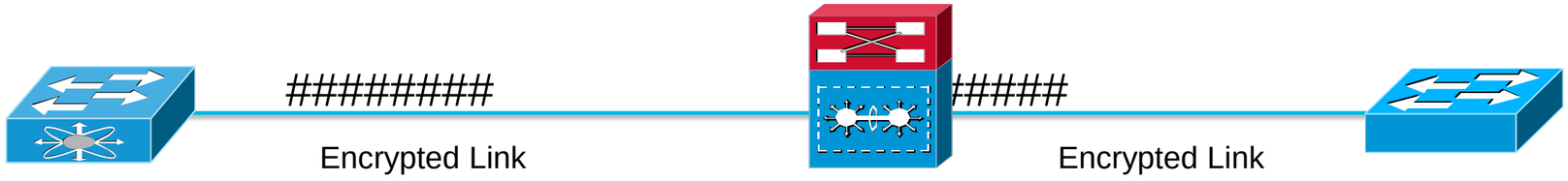
- MACSec enabled switches
- AAA server 802.1X-Rev aware
- Supplicant supporting MKA and 802.1AE encryption

Network Device Admission Control

NDAC: AuthC & AuthZ Network Devices

NDAC

- NDAC adds the ability to Authenticate and Authorise switches entering the network.
  - Encrypts all the links between the Network Devices
    - Uses MACSec
  - Only honors SGT's from Trusted Peers
  - Can "proxy" the Trust & Policies from the ACS/ISE Server to other devices.



For more on NDAC: BRKSEC-2046

Business Case Evolution: B.Y.O.D.

Business Case Continues to Evolve

Executive Bling & the “i-Revolution”

- New Requirement:

  “Our CEO went to a Retail Conference recently and won an iPad. He demands we allow it access to the network, because it is a productivity tool and we prohibiting his productivity without the iPad”

- New Requirement:
  - Allow access to i-devices
- New Term: “Bring Your Own Device” (BYOD)

Market Transitions

5 Billion Mobile Users by 2016

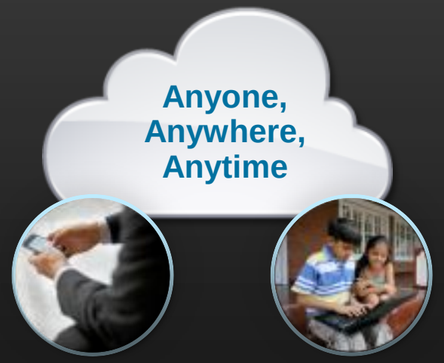
Mobile Users

IT Resources

MOBILITY

Blurring
the Borders

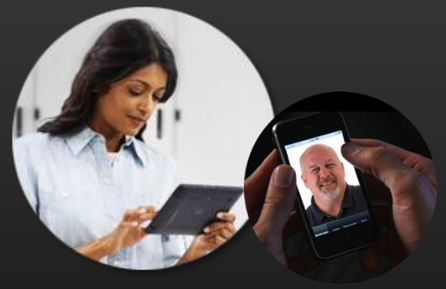
Consumer ↔ Workforce
Employee ↔ Partner
Physical ↔ Virtual



WORKPLACE
EXPERIENCE

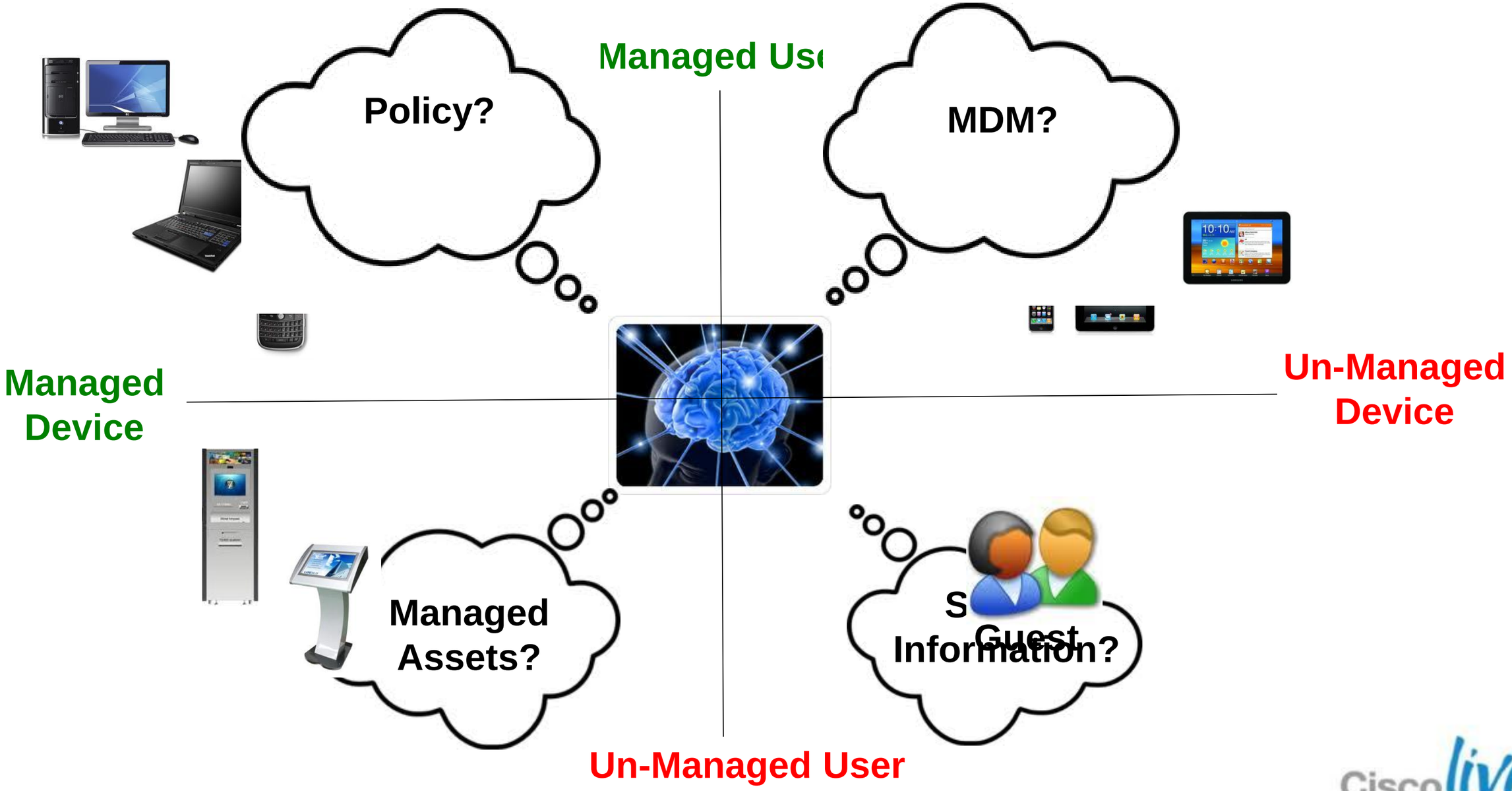
Changing the
Way We Work

71% of the World's
Mobile Data Traffic Will
be Video in 2016



VIDEO

BYOD: What do I need?



Cisco Unique BYOD Value Proposition

One Network, One Policy, One Management

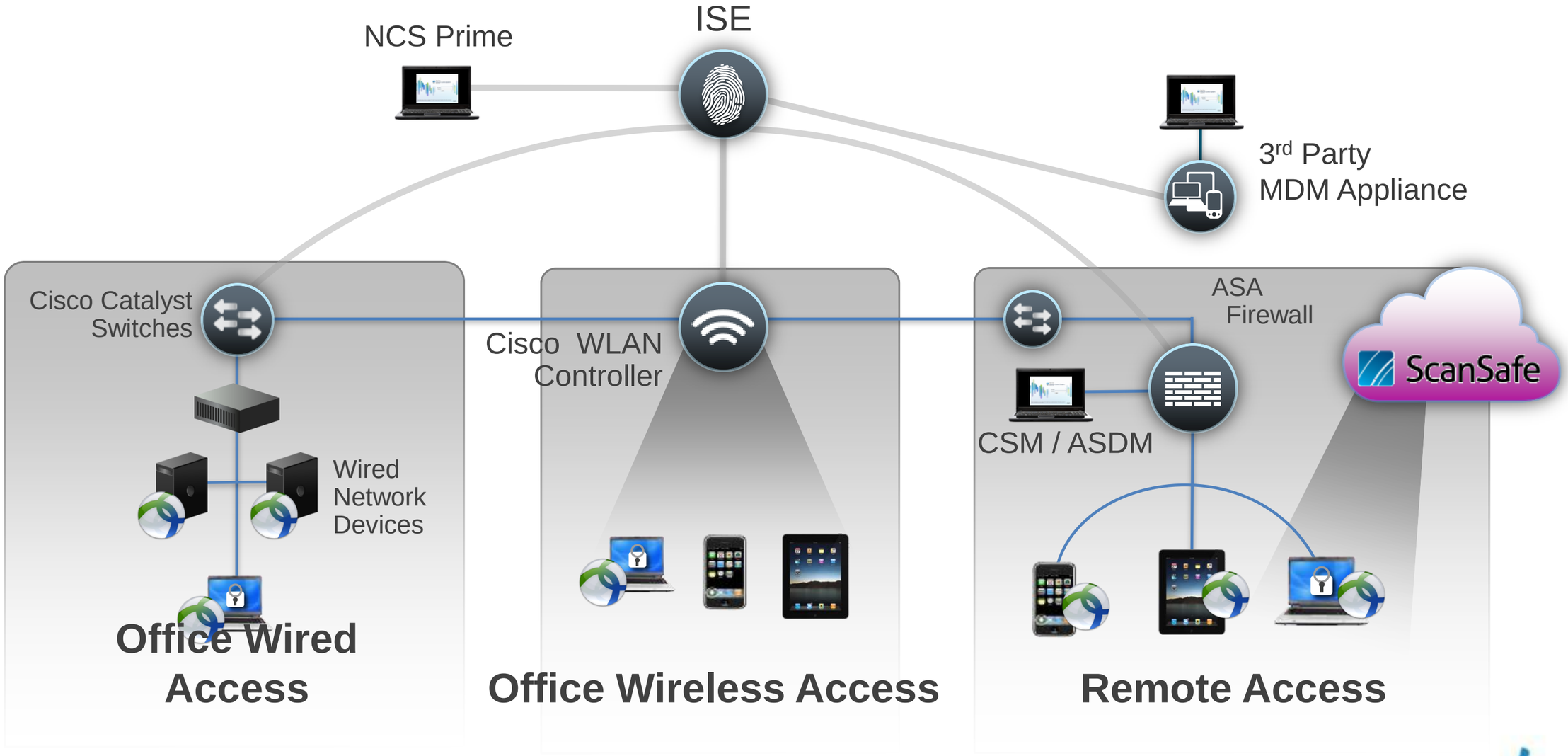
More Than Just Personal Devices	Device ownership is irrelevant: corporate, personal, guest, etc…
More Than Just Wireless Access	BYO devices need wired, wireless, remote and mobile access
More Than Just iPads	BYO devices can be any device: Windows PCs, Mac OS devices, any tablet, any smartphone, gaming consoles, printers… etc

BYOD Spectrum

Where are you on this BYOD spectrum?

Managed User Managed Device	Managed User Un-Managed Device	Managed User Un-Managed Device + Secure	Managed User + Un-Managed Device
Environment requires tight controls	**Basic services and easy access for everyone**	**Register, configure connectivity**	**Company's native applications, new services, and full control**
Company's only device	Block or Allow Internet Access	Securely enabling the device – Device Identification, Certificates, Tracking	Compliance – Encryption enable, PIN Lock, Jail-broken

Enabling Any Device

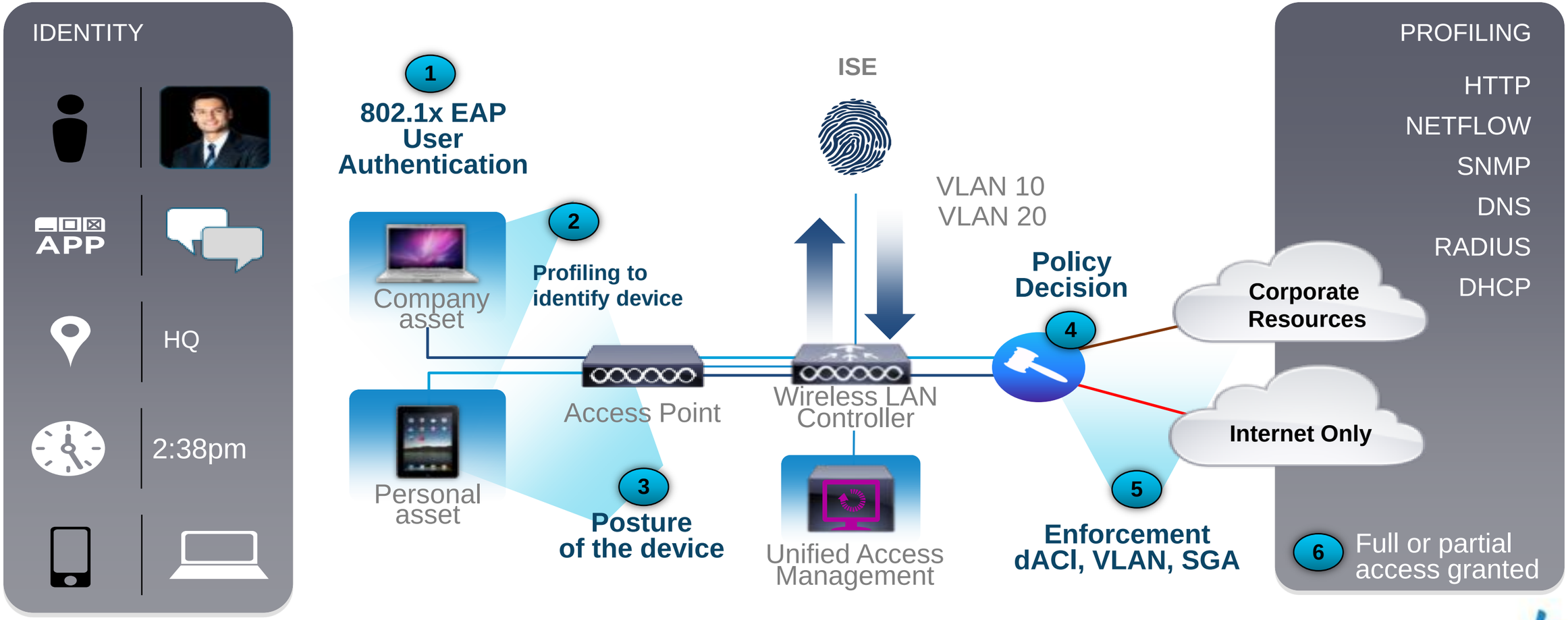


Cisco BYOD Solution Elements

Contextual Policy	On-Board, Registration Differentiated Service: Emp | Guest
Security	Encryption enabled, Certificate Malicious attacks
Central Management	Compliance: Jail-broken, PIN Lock, etc .. Device Tracking and Monitoring
Network	Establish Connectivity Service Compliance Policy
Collaboration Application	Email Jabber, AnyConnect

Contextual Policy for BYOD Deployments

Control and Enforcement



User and Device Roles

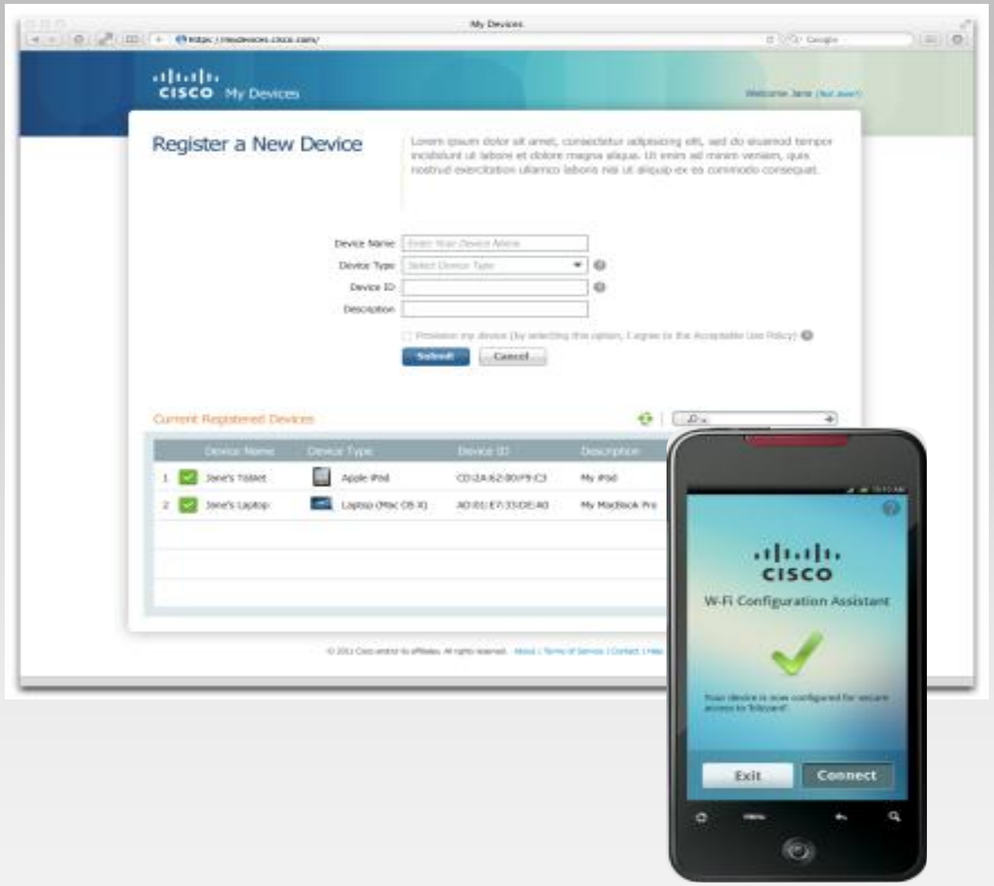
User & Device Role	Any Device	BYOD Devices			Corporate Device
	Internet	Corporate home page	Manager Portal	Employee Application	Financial Information

Un-Registered_Device_BXB	if	(Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND DEVICE:Location EQUALS All Locations#BXB)	then	NSP-Authz-Profile
Registered_Emp_Device_BXB	if	**RegisteredDevices** AND (Wireless_802.1X AND Network Access:EapAuthentication EQUALS EAP-TLS AND DEVICE:Location EQUALS All Locations#BXB)	then	Emp-Permit-Access
Registered_MGT_Device_BXB	if	**RegisteredDevices** AND (Wireless_802.1X AND Network Access:EapAuthentication EQUALS EAP-TLS AND DEVICE:Location EQUALS All Locations#BXB)	then	MGT-Permit-Access
Guest	if	**Guest**	then	Guest_Access

Simplified On-Boarding for BYOD

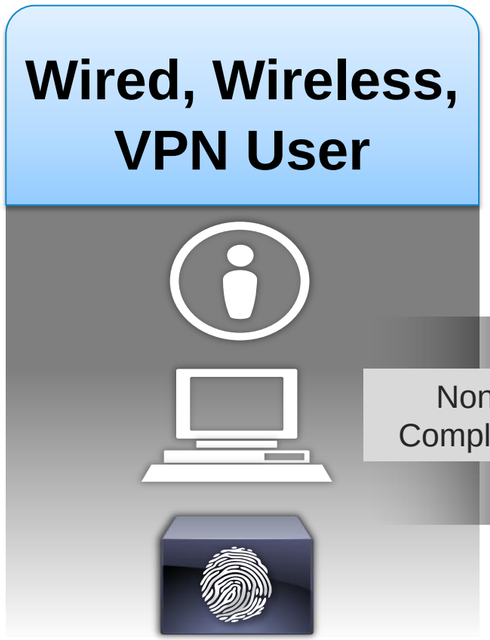
Putting the End User in Control

- **Reduced Burden on IT Staff**
  - Device On-Boarding
  - Self Registration
  - Supplicant Provisioning
  - Certificate Provisioning
- **Self Service Model**
  - myDevice Portal for registration
  - Guest Sponsorship Portal
- **Device Black Listing**
  - User initiated control their devices, black-listing, re-instate device, etc)
- **Support for:**
  - iOS (post 4.x)
  - MAC OSX (10.6, 10.7)
  - Android (2.2 and onward)
  - Windows (XP, Vista, win7K)

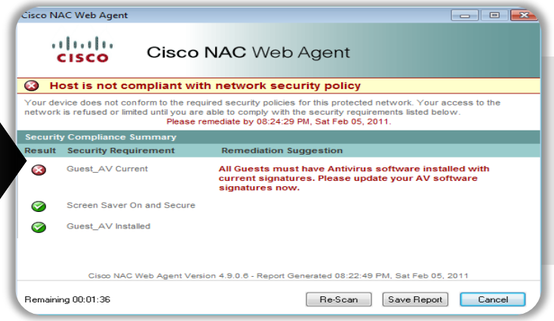


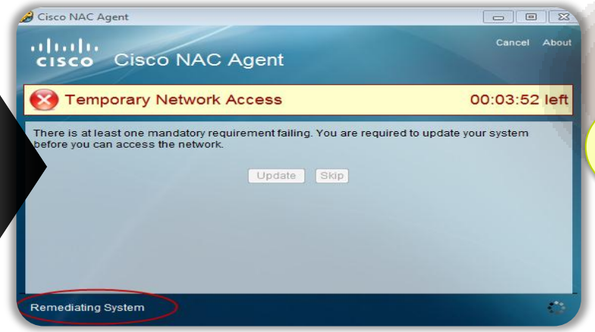
Compliance

Endpoint Health assessment



Non-Compliant





Temporary Limited Network Access Until Remediation Is Complete

Sample Employee Policy:

- Microsoft patches updated
- McAfee AV installed, running, and current
- Corp asset checks
- Enterprise application running

Challenge:

- Understanding health of device
- Varying level of control over devices
- Cost of Remediation

Value:

- Temporal (web-based) or Persistence Agent
- Automatic Remediation
- Differentiated policy enforcement-based on role

Mobile Compliance: ISE + MDM

Initial Vendors

airwatch™ MobileIron® Good ZENPRISE

On Prem MDM Device Registration - non registered clients redirected to MDM registration page

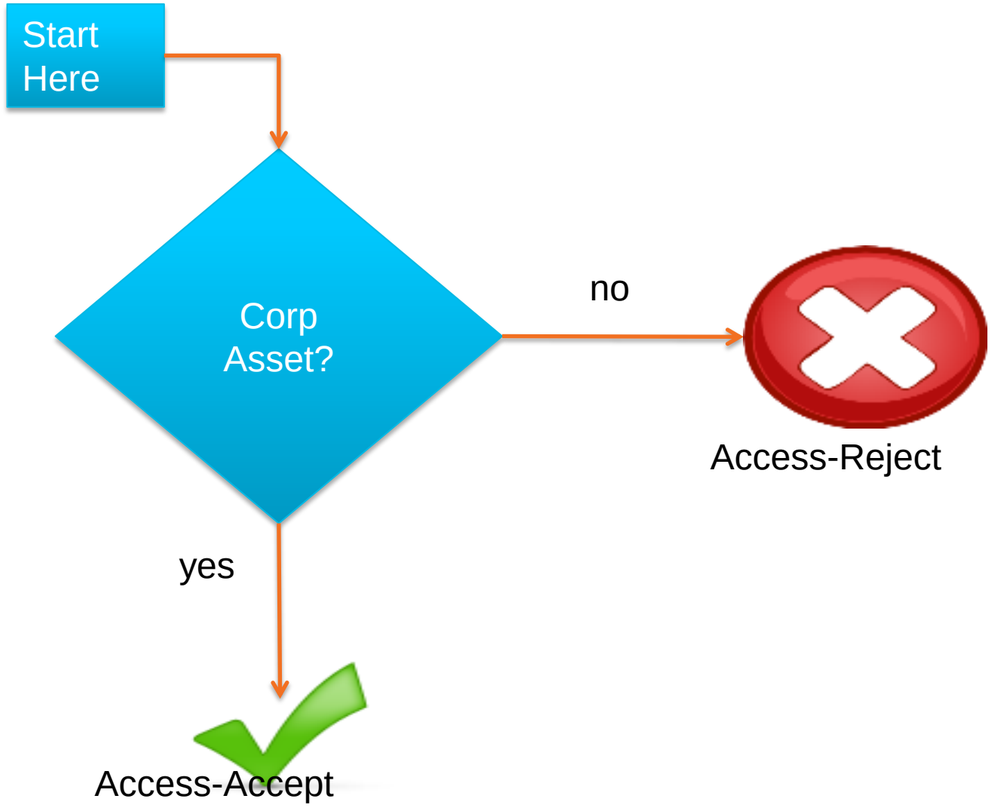
Restricted Access - non compliant clients will be given restricted access based on MDM posture state

Augment Endpoint Data - Update data from endpoint which cannot be gathered by profiling

Ability initiate device action from ISE - eg: device stolen -> need to wipe data on client (Stretch).

What Makes a BYOD Policy?

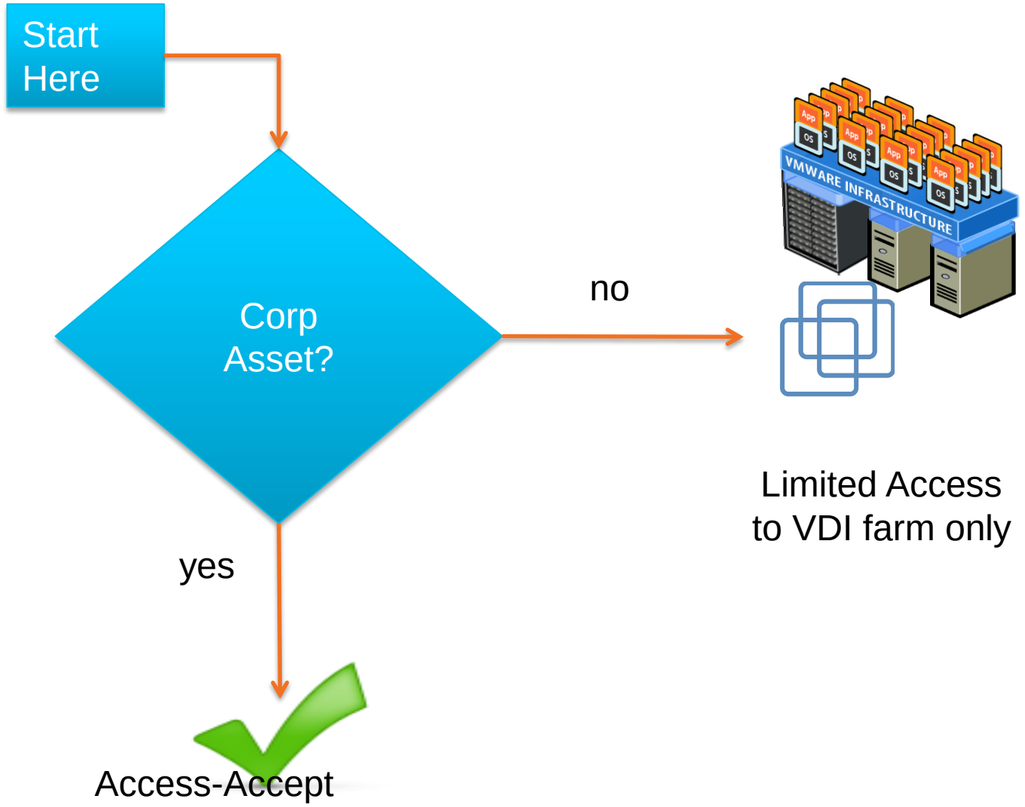
MachineAuth Approach…



- Only corporate devices may access my network, period.
  - Use EAP-TLS with AD-issued non-exportable machine certificates.
  - That is our “BYOD” Policy.
- Not too common anymore.

What Makes a BYOD Policy?

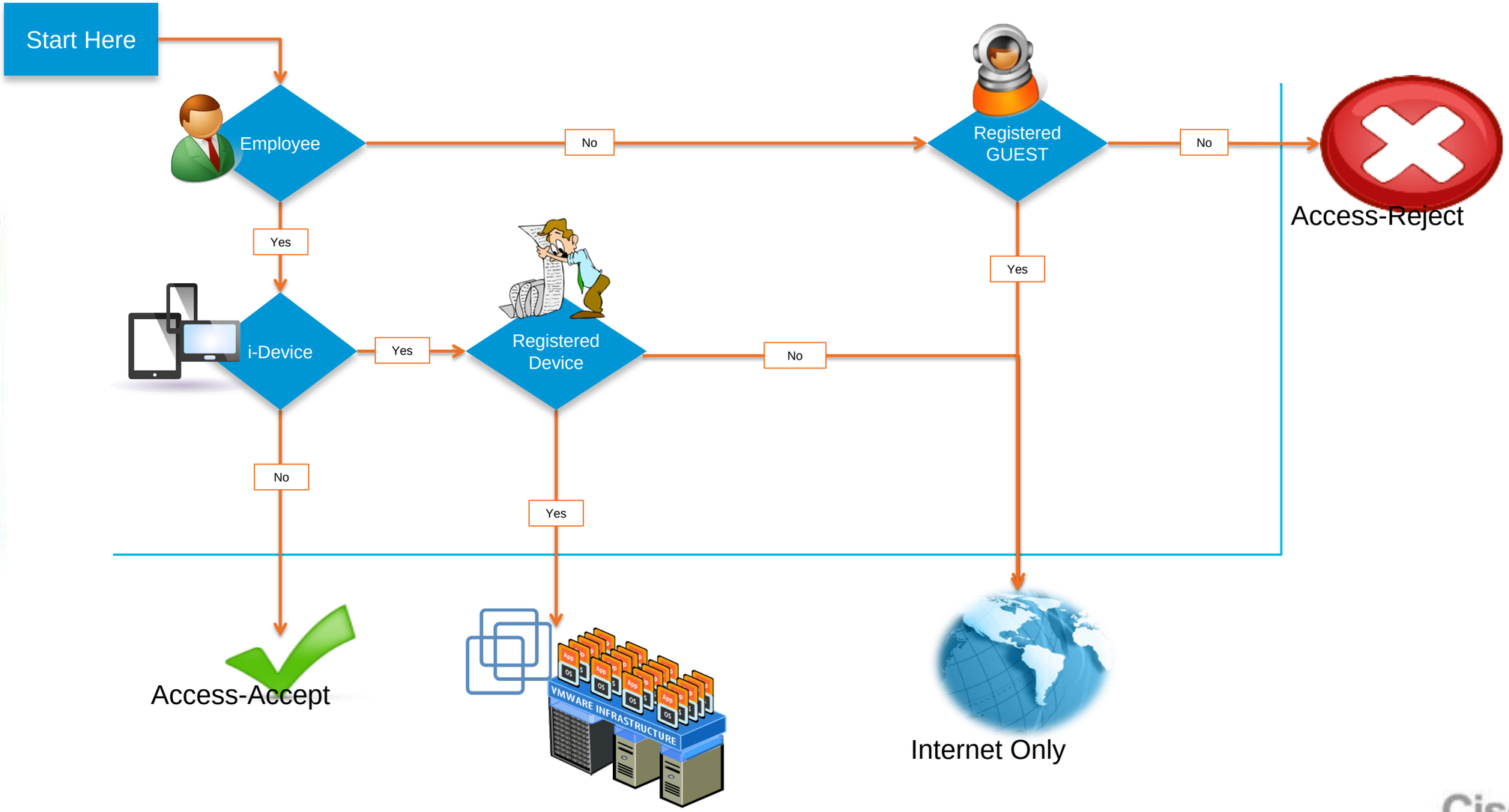
VDx Approach…



- Only corporate devices may access my Corporate Network.
  - Others should get RDP/ICA to a VDI farm.
  - Could use Profiling to determine Corp Asset.
  - Could use Certs or Machine-Auth w/ PEAP-MSChapv2
- Happening a good bit.

What Makes a BYOD Policy?

Even More Complicated



What Makes a BYOD Policy

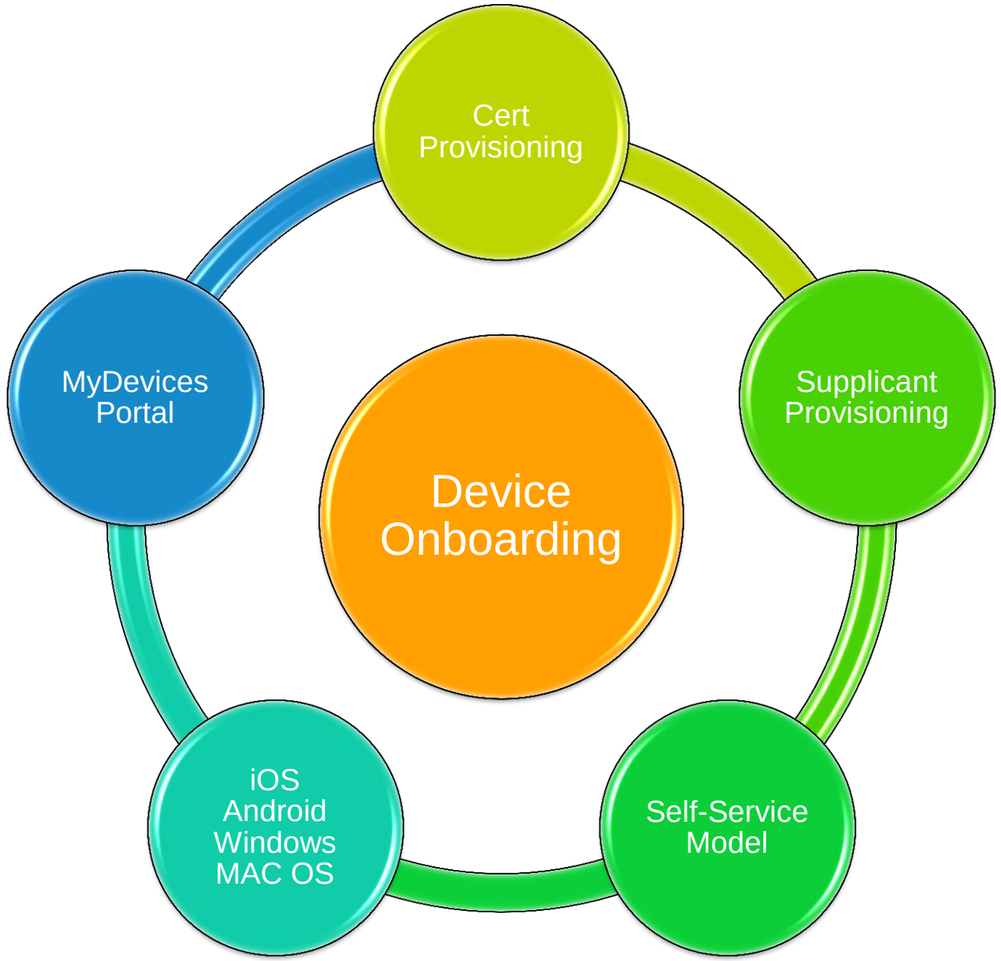
The Policy Server is Critical to Meeting Your Goals

- Identity Services Engine = BYOD engine!

Who? Known users (Employees, Sales, HR) Unknown users (Guests)	**What?** Device identity Device classification (profile) Device health (posture)	**How?** Wired Wireless VPN
Where? Geographic location Department SSID / Switchport	**When?** Date Time Start/Stop Access	**Other?** Custom attributes Device/User states Applications used

ISE BYOD Release

Identity Services Engine 1.1.1 (“Minor Release”)



- Provision a Certificate for the device.
  - Based on Employee-ID & Device-ID.
- Provision the Native Supplicant for the Device:
  - iOS, Android, Win & MAC-OSX
  - Use EAP-TLS or PEAP
- Employees get Self-Service Portal
  - Lost Devices are Blacklisted
- Self-Service Model
  - IT does not need to be in the middle.

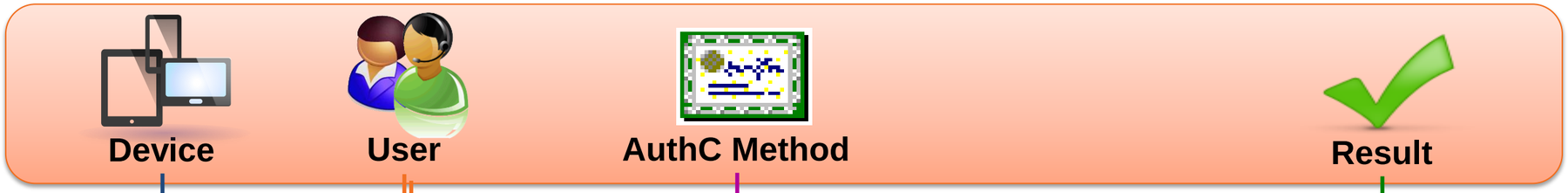
Client Provisioning Policy

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Mac iOS All	and AD1:ExternalGroups EQUALS cts.l...	then WiFi_Profile
Android	If Any	and Android	and AD1:ExternalGroups EQUALS cts.l...	then WiFi_Profile
WinThings	If Any	and Windows...	and AD1:ExternalGroups EQUALS cts.l...	then WinSPWizard 1.0.0.14 And WiFi_Profile
MAC-OSX	If Any	and Mac OSX	and AD1:ExternalGroups EQUALS cts.l...	then MacOsXSPWizard 1.0.0.6 And WiFi_Profile

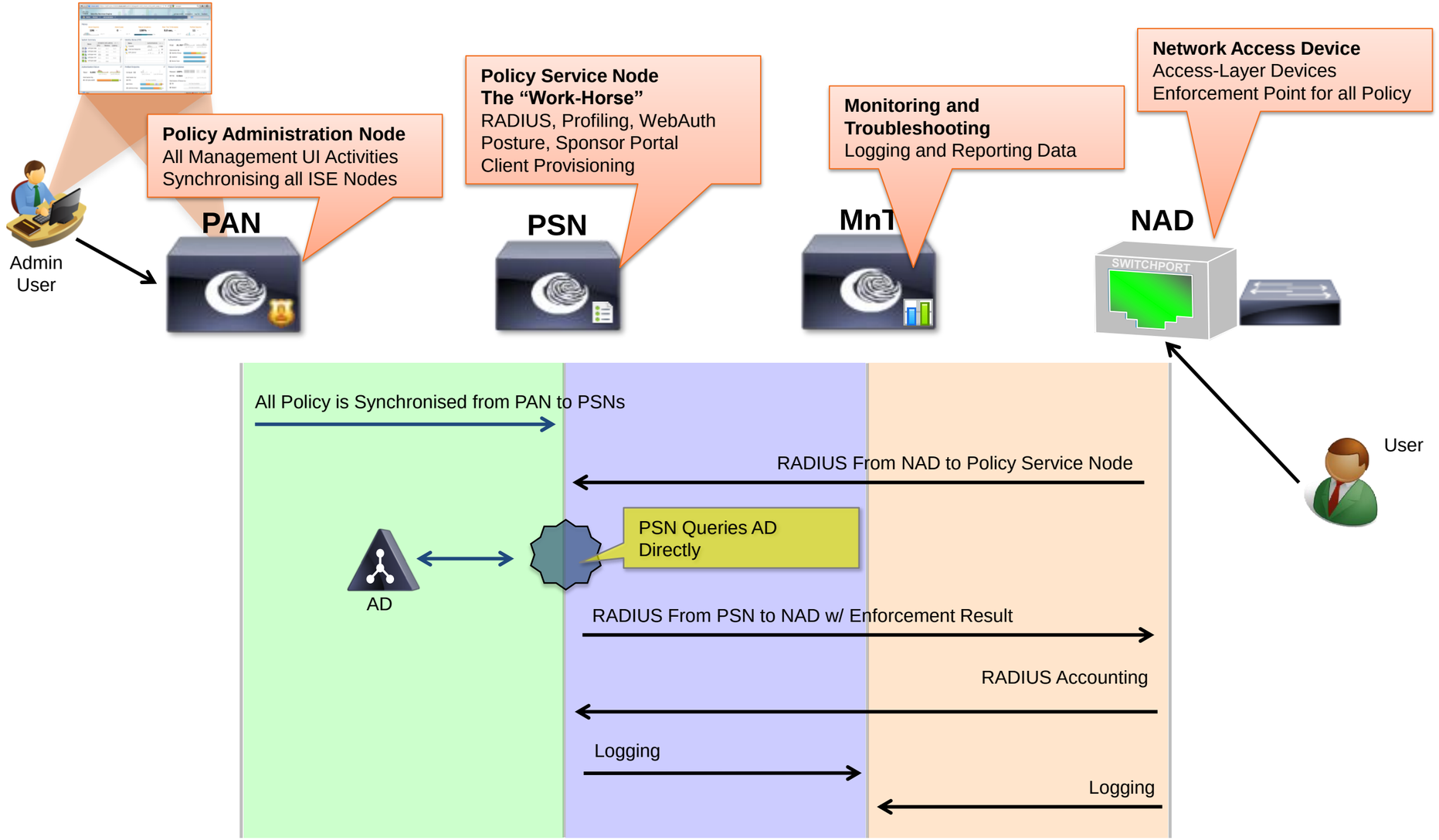
BYOD Policy in ISE



Black List Default	if	**Blacklist**	then	Blacklist_Access
Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
PEAP Rule	if	PEAP	then	SupplicantProvision
Open Rule	if	Wireless_MAB	then	NSP
Employee Rule	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD1:ExternalGroups EQUALS cts.local/Users/Employees)	then	Employee

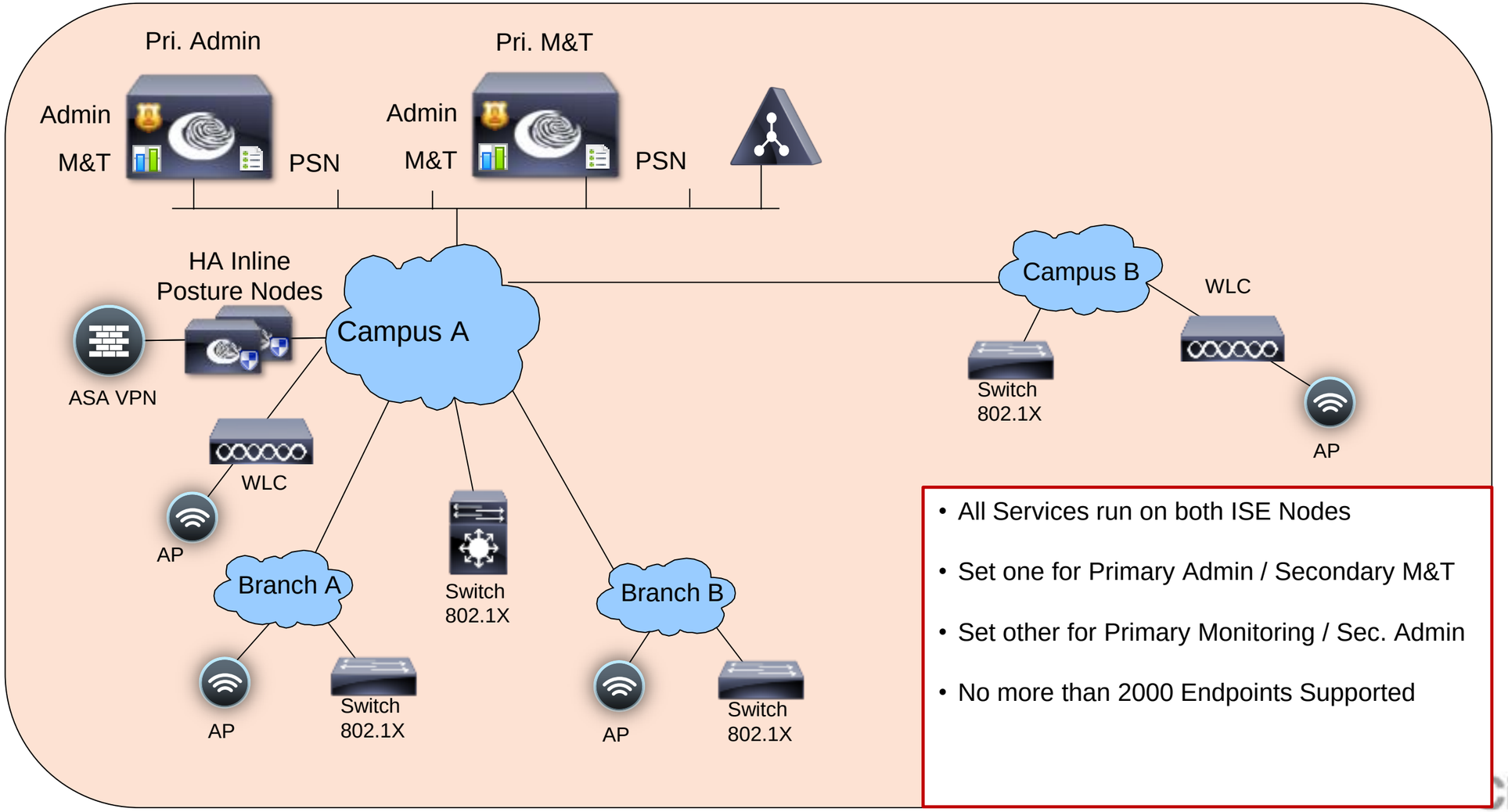
ISE Design & Architecture

Administration Process & Explanation



Basic 2-Node ISE Deployment (Redundant)

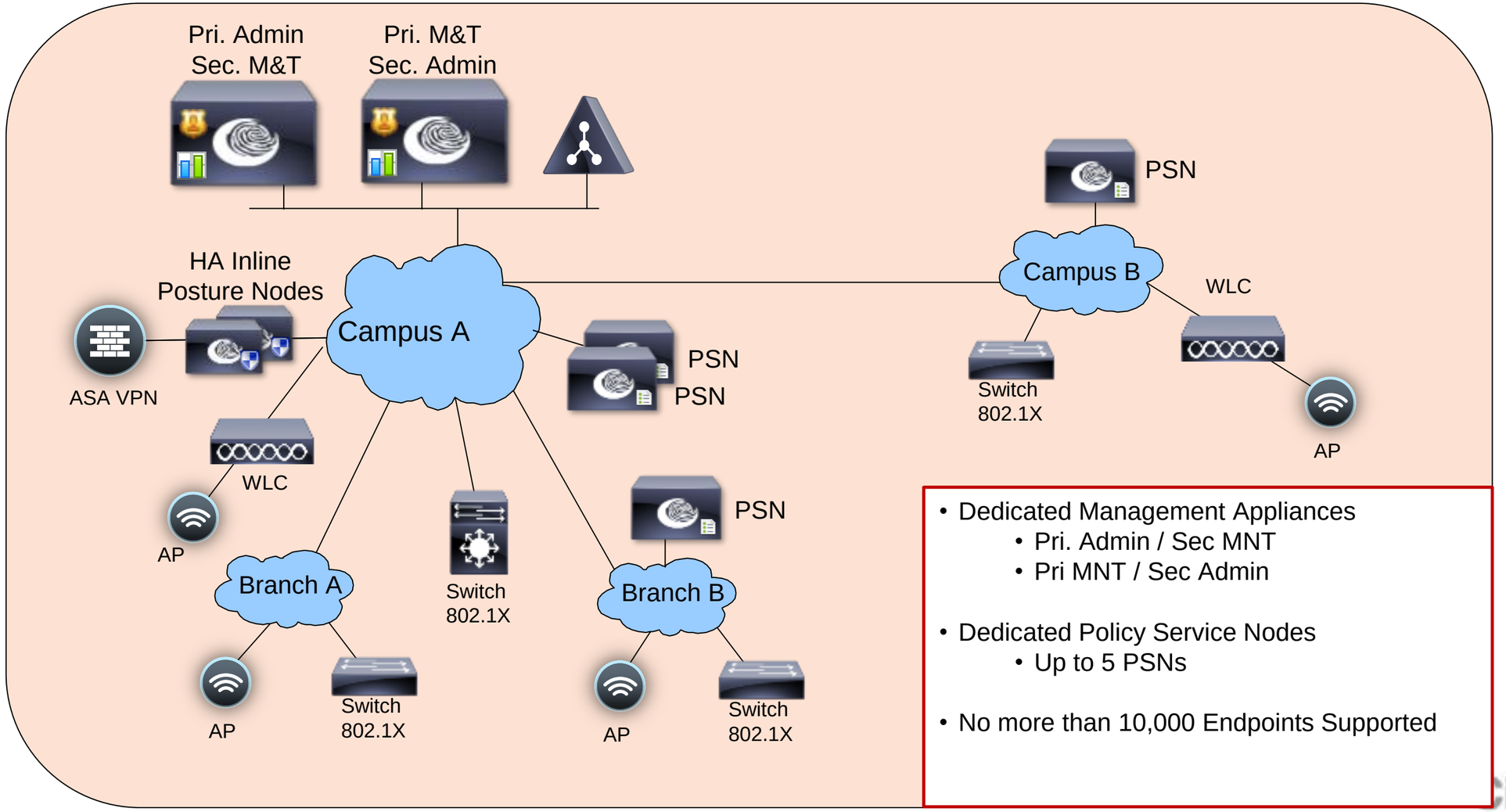
Maximum Endpoints = 2,000



- All Services run on both ISE Nodes
- Set one for Primary Admin / Secondary M&T
- Set other for Primary Monitoring / Sec. Admin
- No more than 2000 Endpoints Supported

Basic Distributed Deployment

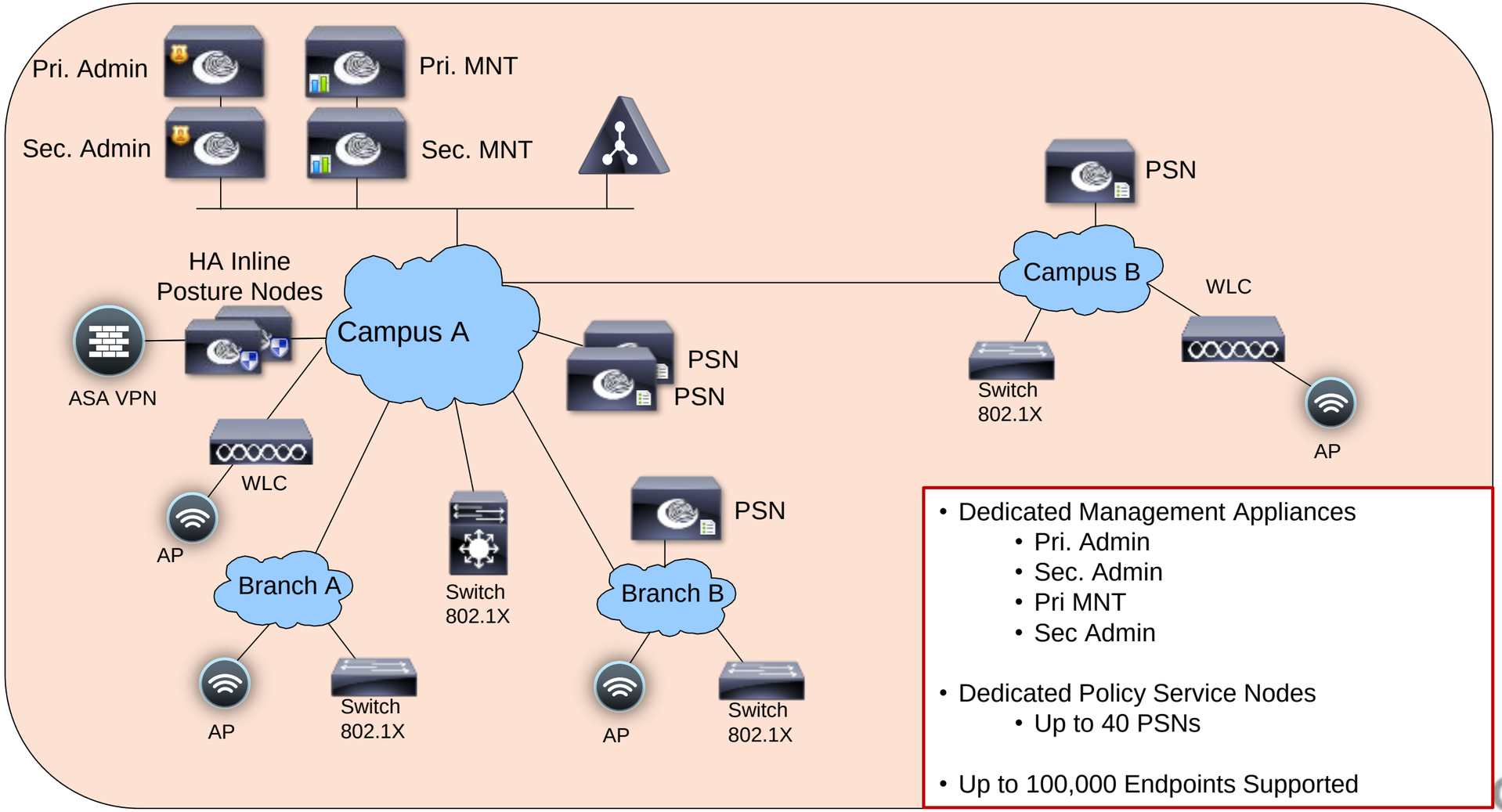
Maximum Endpoints = 10,000 / Maximum 5 PSNs



- Dedicated Management Appliances
  - Pri. Admin / Sec MNT
  - Pri MNT / Sec Admin
- Dedicated Policy Service Nodes
  - Up to 5 PSNs
- No more than 10,000 Endpoints Supported

Fully Distributed Deployment

Maximum Endpoints = 100,000 / Maximum 40 PSNs



- Dedicated Management Appliances
  - Pri. Admin
  - Sec. Admin
  - Pri MNT
  - Sec Admin
- Dedicated Policy Service Nodes
  - Up to 40 PSNs
- Up to 100,000 Endpoints Supported

Summary

Cisco TrustSec Technology Review:

Network Identity & Enforcement

- Authentication - (802.1x, MAB, Web, NAC)
- Authorisation - (VLAN, DACL, SXP or SGT)
- Enforcement – (SGACL and Identity Firewall)

I want to allow guests into the network	Guest Access
I need to allow/deny iPADs in my network	Profiler
I need to ensure my endpoints don't become a threat vector	Posture
I need to ensure data integrity and confidentiality for my users	MACSec encryption
I need a scalable way of authorising users or devices in the network	Security Group Access
How can I set my firewall policies based on identity instead of IP addresses?	Identity-based Firewall

Q & A

Links

- Trustsec & ISE on Cisco.com
  - http://www.cisco.com/go/trustsec
  - http://www.cisco.com/go/ise
  - http://www.cisco.com/go/isepartner
- TrustSec & ISE Deployment Guide:
  - http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html
- YouTube: Fundamentals of TrustSec:
  - http://www.youtube.com/ciscocin#p/c/0/MJJ93N-3Iew

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww