



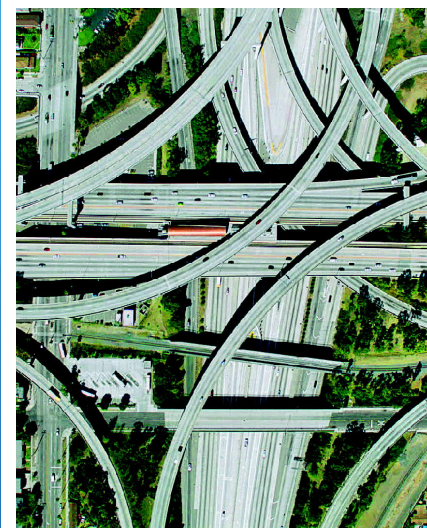
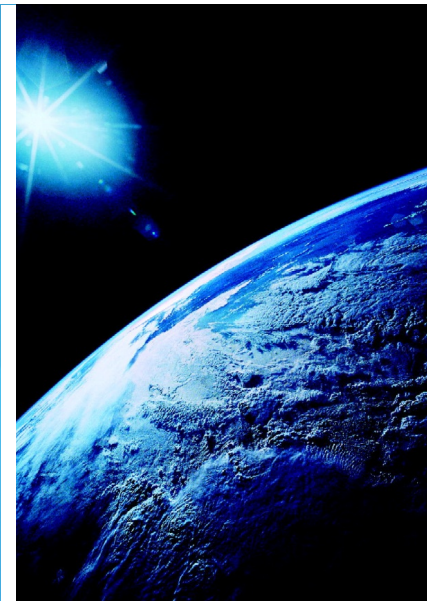
Praha, hotel Clarion
10. – 11. dubna 2013

Kontextové řízení přístupu do sítě

Sec3/L2

Jiří Tesař – Cisco

© 2013 Cisco and/or its affiliates. All rights reserved.





Network Security of Yesterday

Corporate Assets

Corporate Connectivity

Limited Remote Connectivity

Employees Only Access

♣ Routers

♣ Firewalls

♣ Switches



Network Security Policy Yesterday

Secure Access Control

Authentication

Authorisation

Accounting



Network Security of Today

Corporate and Commercialised Assets

Mobile Smart Devices – The iRevolution

Corporate, Partner, Public, Cloud Connectivity

Wireless Infrastructures

Unified Communications

Virtualised Data Centres

Employees, Contractors and Guests Access

♣ Routers, Switches, Firewalls, IPS

♣ Email and Web Security

♣ Network Admission Control, Posture Control



Obsah

Jak získat identitu uživatele ?

Co více potřebujeme vědět ?

Jak zabezpečit přístupovou vrstvu ?

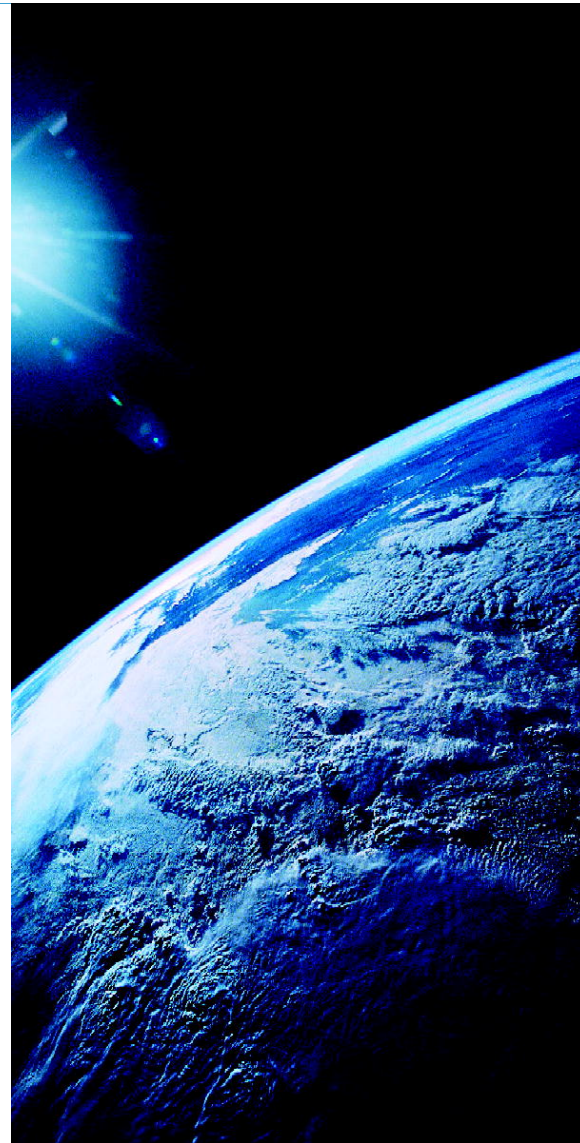
Zaměstnanci, hosté, dodavatelé

Další bezpečnostní prvky v síti ...

Propojení ...

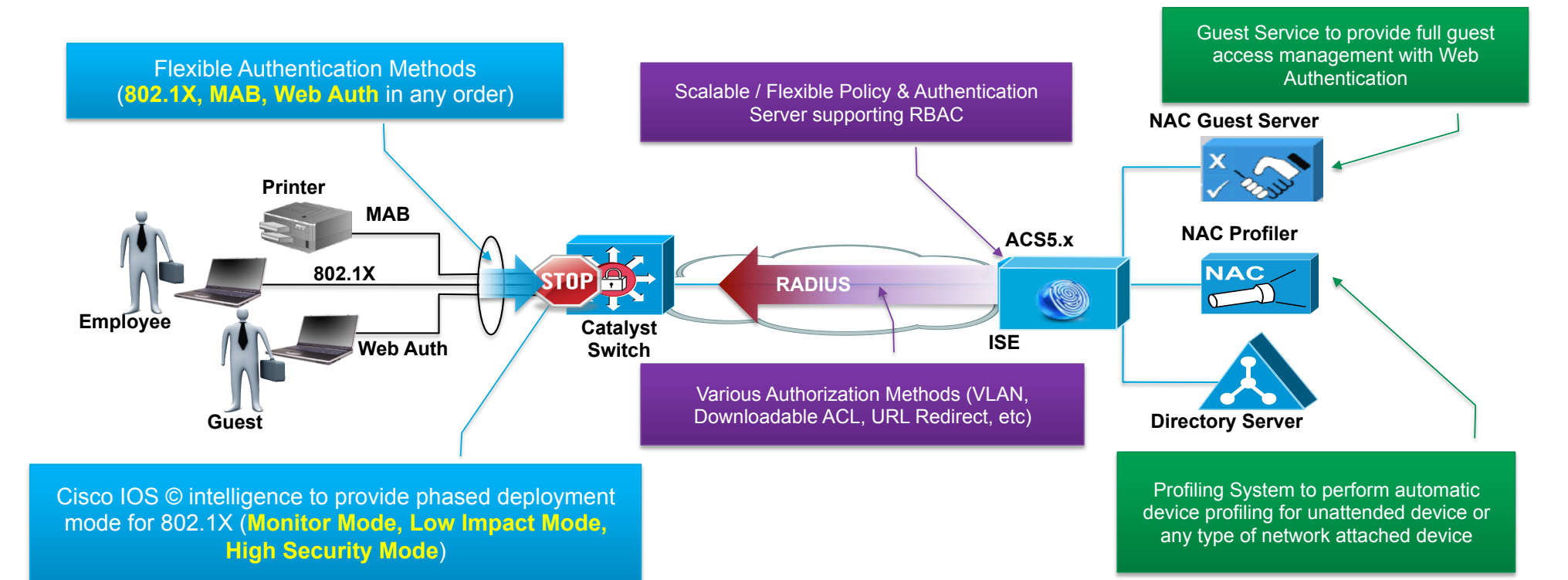
How to Recognize the Identity

© 2013 Cisco and/or its affiliates. All rights reserved.



Cisco Connect

7



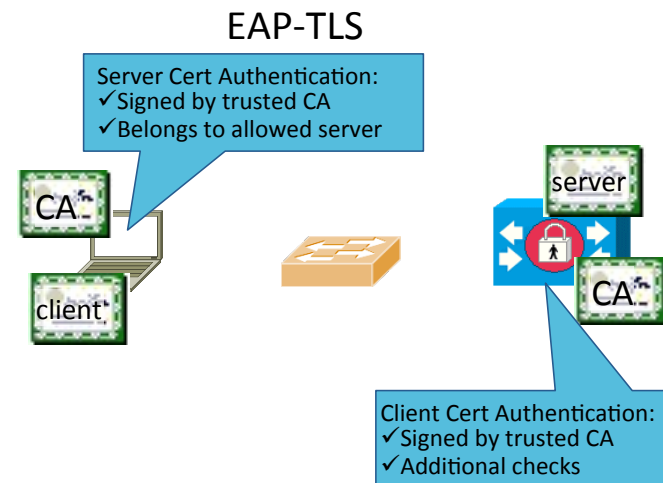
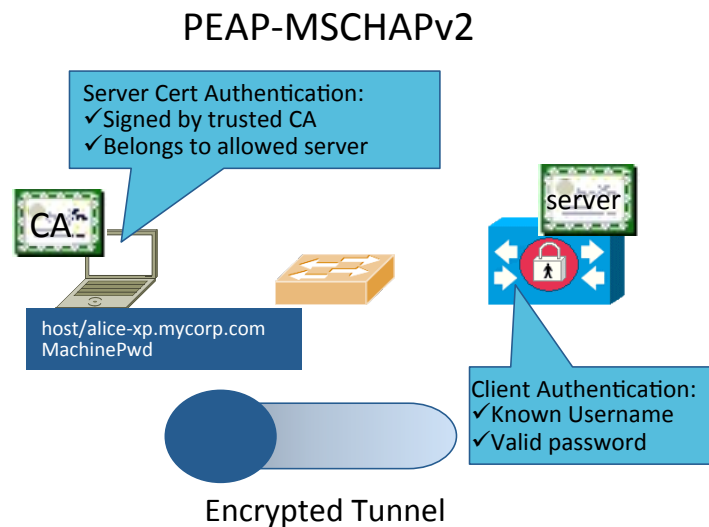
How To Submit Credentials

Mutual Authentication

- Server must validate client's identity **and vice versa**

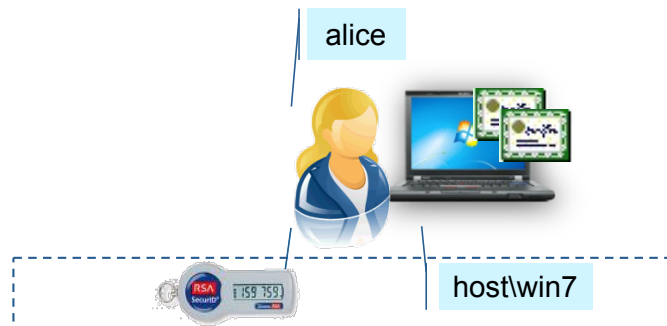
Security

- Client credentials cannot be snooped or cracked.



Users and Machines Can Have Credentials

Machine Authentication

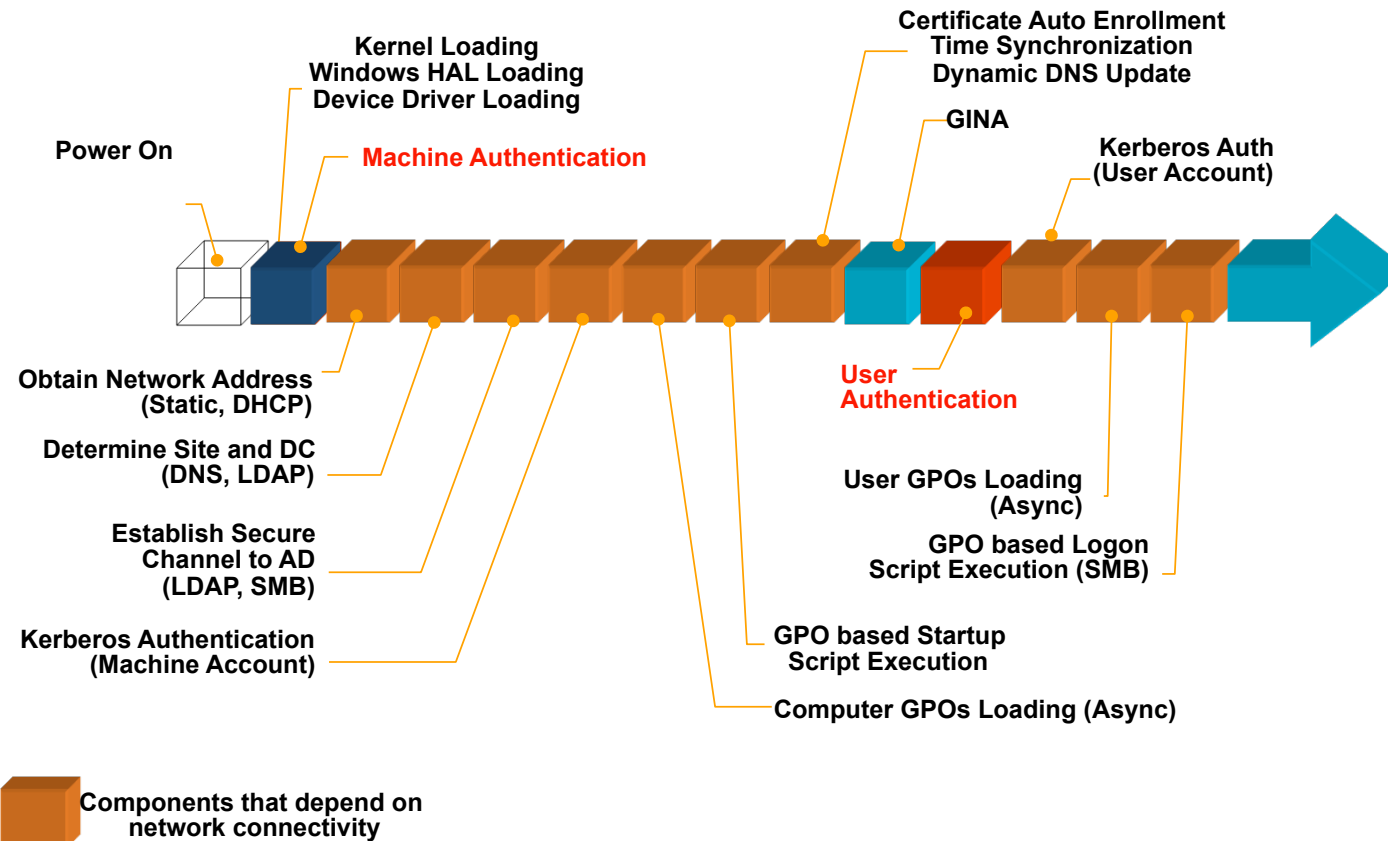


- Enables Devices To Access Network Prior To (or In the Absence of) User Login
- Enables Critical Device Traffic (DHCP, NFS, Machine GPO)
- Is **Required** In Managed Wired Environments

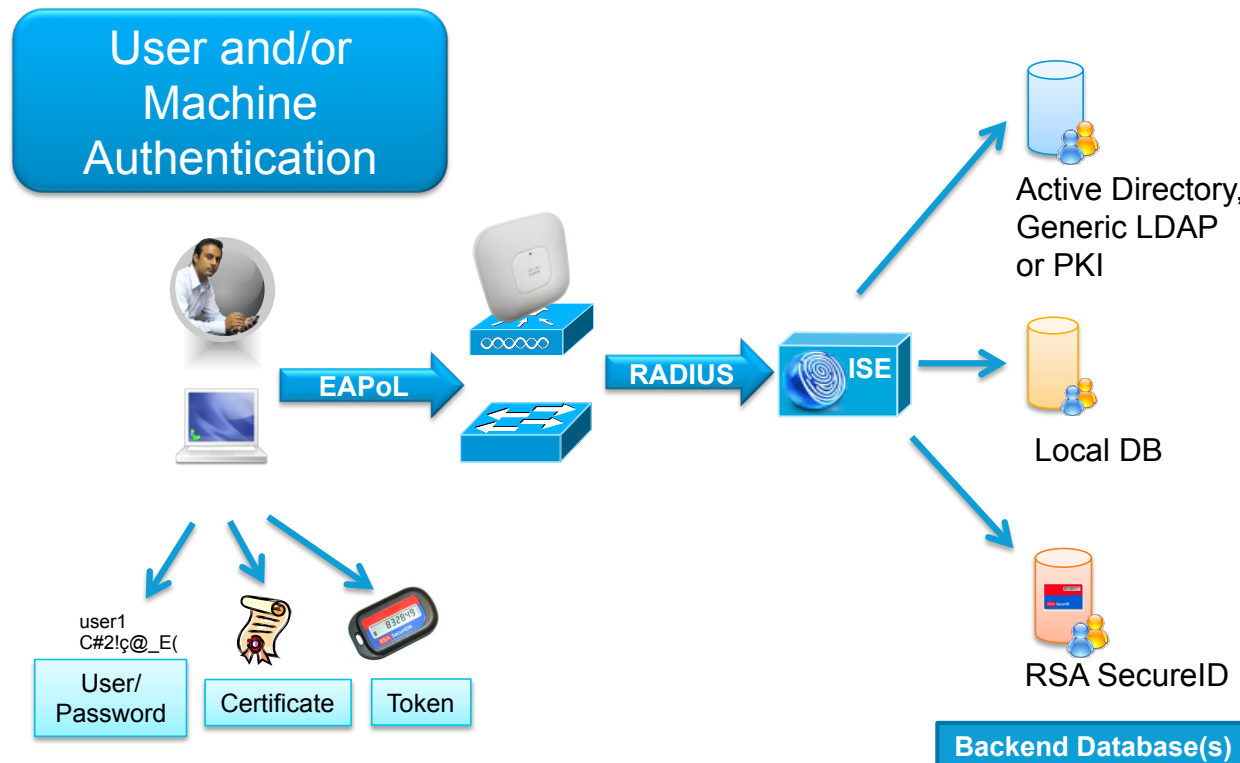
User Authentication



- Enables User-Based Access Control and Visibility
- If Enabled, Should Be **In Addition To** Device Authentication



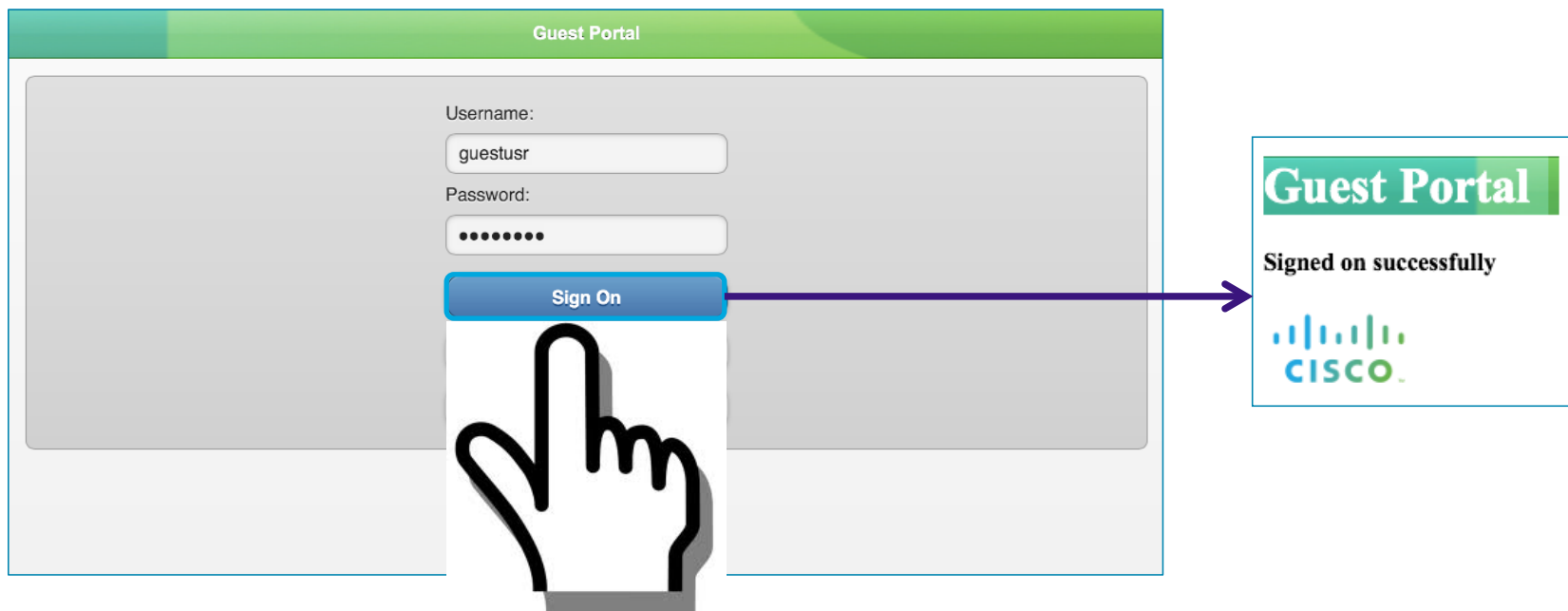
Authentication Sources



- Cisco ISE can reference backend identity stores including Active Directory, PKI, LDAP and RSA SecureID.
- The local database can also be used on the ISE itself for small deployments.

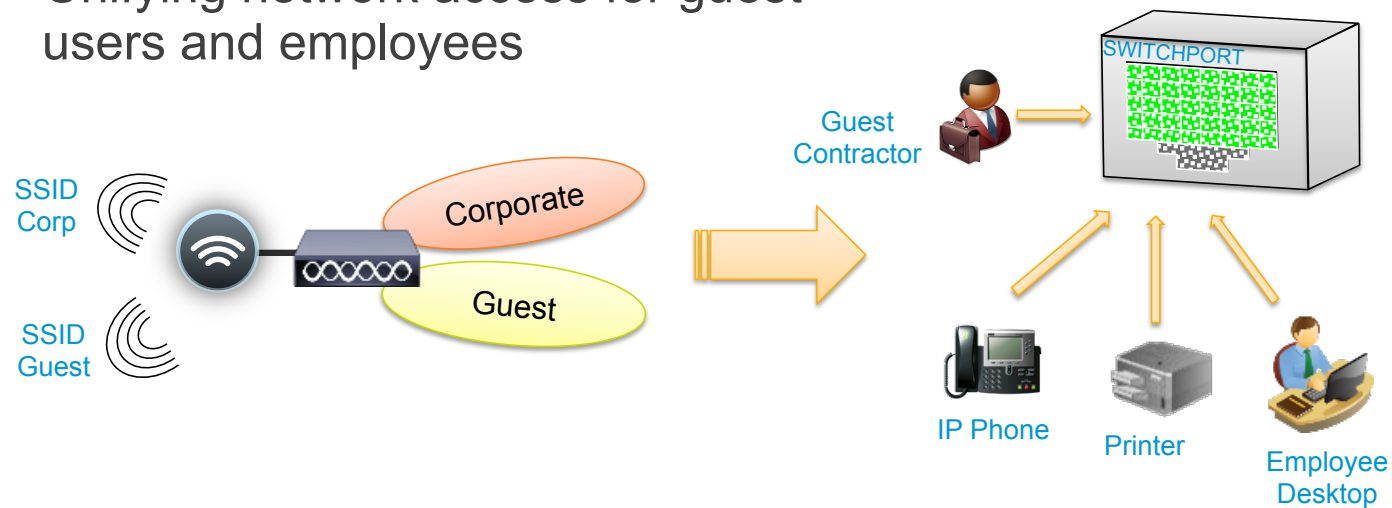
Web Authentication

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



Providing Network Access to Guests and Employees

- Unifying network access for guest users and employees



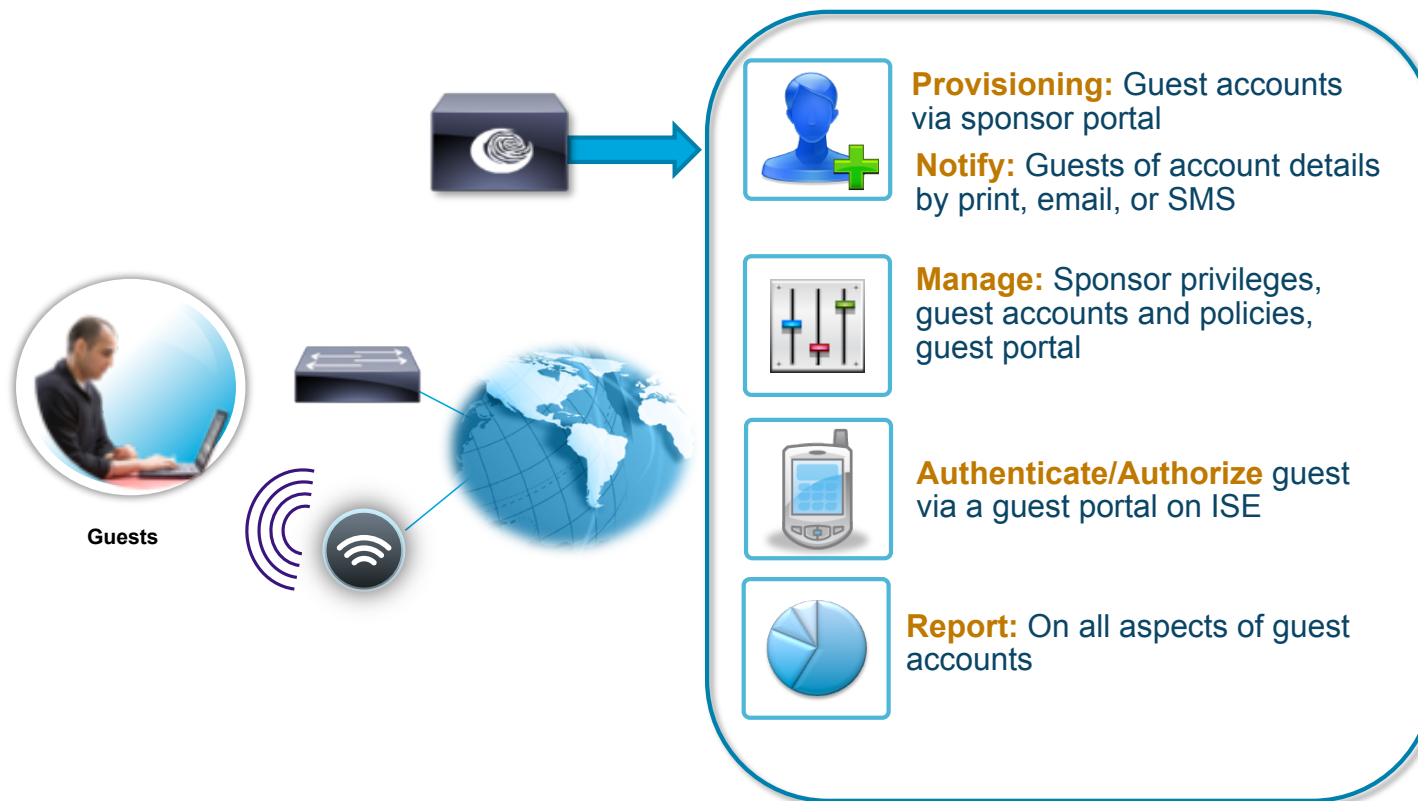
On wireless:

- Using multiple SSIDs
- Open SSID for Guest

On wired:

- No notion of SSID
- Unified port: Need to use different auth methods on single port ► [Enter Flex Auth](#)

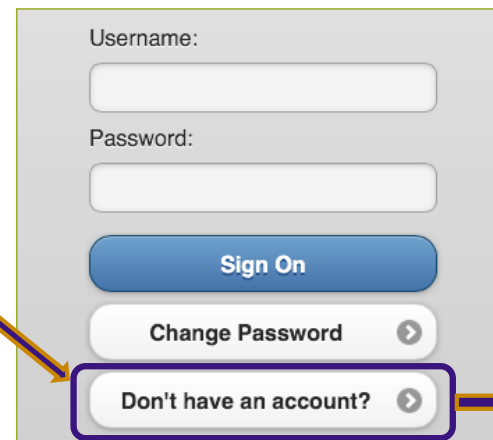
Components of a Full Guest Lifecycle Solution



Guest Users DB – Account Creation Methods

Two Ways to Populate ISE Internal Guest Database

- Self-Service Option on ISE 'Guest Portal'



Username:

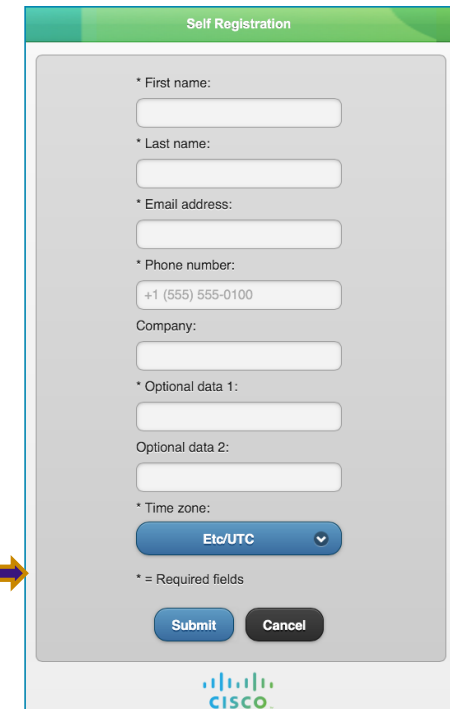
Password:

Sign On

Change Password >

Don't have an account? >

- Sponsoring via ISE 'Sponsor Portal'



Self Registration

* First name:

* Last name:

* Email address:

* Phone number:

Company:

* Optional data 1:

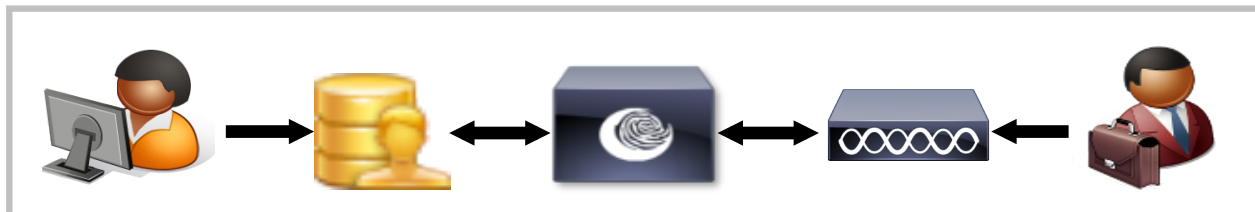
Optional data 2:

* Time zone:
Etc/UTC v

* = Required fields

Submit **Cancel**





ISE: Web Authentication

The screenshot displays the Cisco Guest Portal interface. At the top, the Cisco logo and 'Guest Portal' text are visible. A dark blue header bar contains the Cisco logo, 'Guest Portal', and a welcome message for 'guestuser' with a 'Sign Out' link. A large white box in the center of the page displays the message 'Signed on successfully' and 'Try accessing the web site again.' Below this, the login form shows the 'Username' field with 'guestuser' and the 'Password' field with masked characters. A 'Sign On' button is highlighted with a red box, and a red arrow points from it to the success message box. Below the login fields are links for 'Don't have an account?' and 'Change Password'. At the bottom, a row of icons depicts various guest services: a person with a suitcase, a person with a suitcase and a bag, a handshake, a person with a suitcase, and a person with a suitcase and a bag.

Header: Cisco Guest Portal | Welcome guestuser ([Sign Out](#))

Success Message: Signed on successfully
Try accessing the web site again.

Login Fields:
Username:
Password:

Buttons: [Sign On](#)

Links: [Don't have an account?](#) | [Change Password](#)

Footer Icons: Icons representing guest services: a person with a suitcase, a person with a suitcase and a bag, a handshake, a person with a suitcase, and a person with a suitcase and a bag.

ISE – Multiple Guest Portals

- Several portals may be needed to support different groups/users based on:
 - Location / country
 - Type of device: WLC, switches
 - Local language support
- ISE can hold several portals
- Multiple portals can be used simultaneously for authentication

Multi-Portal Configurations		
 Edit  Add  Delete		
☐	Multi-Portal Name	Portal Type
☐	CustomDeviceWebAuthPortal	CustomDeviceWebAuth
☐	CustomPortal	CustomDefault
☐	DefaultDeviceWebAuthPortal	DeviceWebAuth
☐	DefaultGuestPortal	Default
☐	GuestPortalwNSP	Default
☐	MobilePortal	CustomDefault
☐	PostureGuestPortal	Default



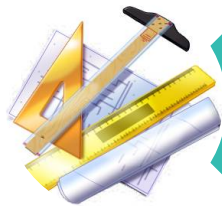
MAC Authentication

MAC Databases: Device Discovery



Find It

- Leverage Existing Asset Database
- e.g. Purchasing Department, CUCM



Build It

- Bootstrap methods to gather data
- e.g. SNMP, Syslog, Accounting



Buy It

- Automated Device Discovery
- e.g. ISE

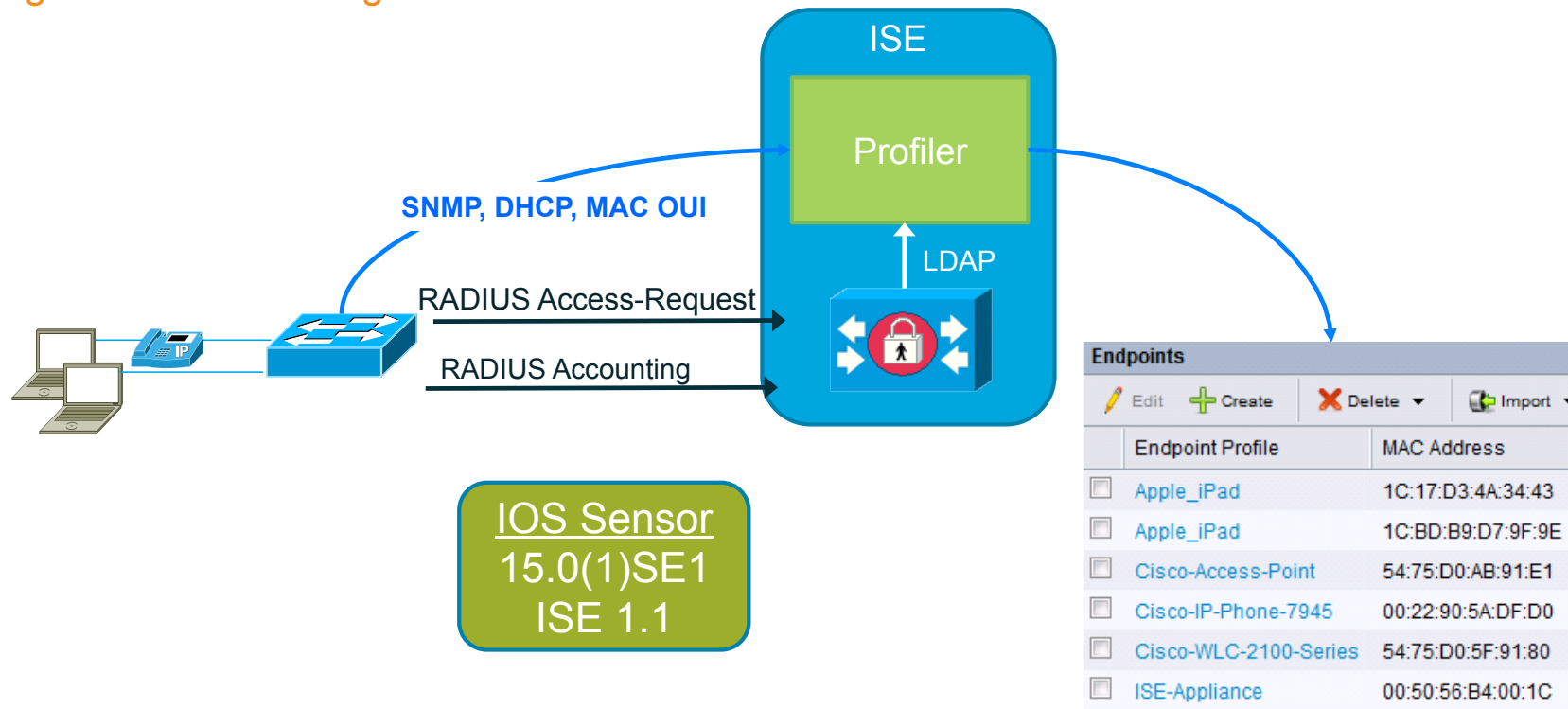


Key Questions

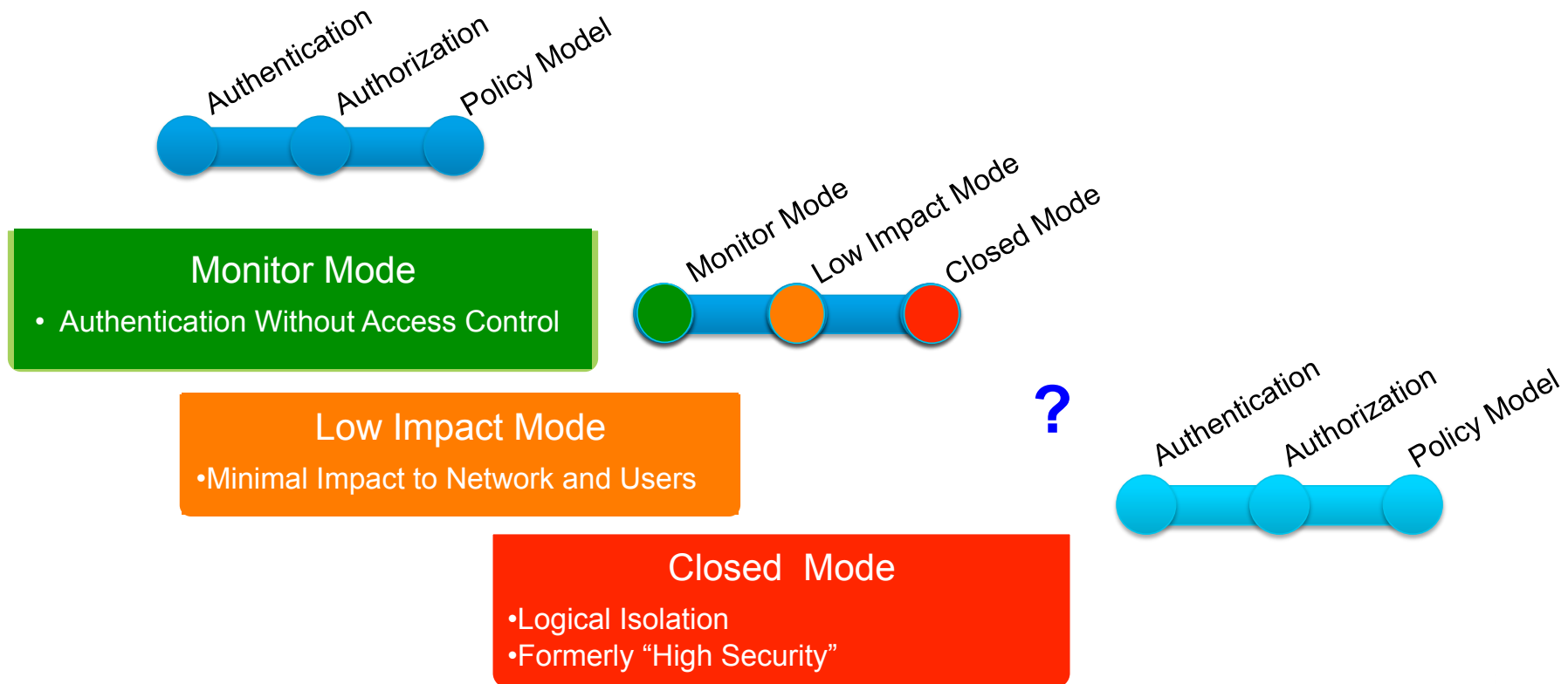
- How Will You Know What's "Yours"?
- How Much Do You Care?
- Better Knowledge Requires More Effort

Building Your MAB Database

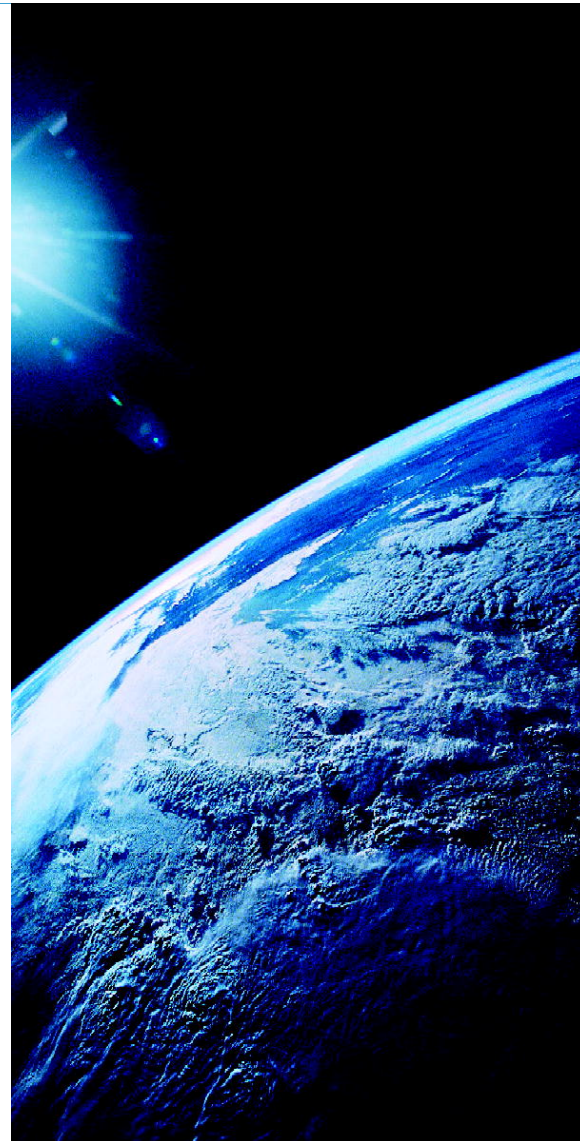
Profiling Tools Are Evolving



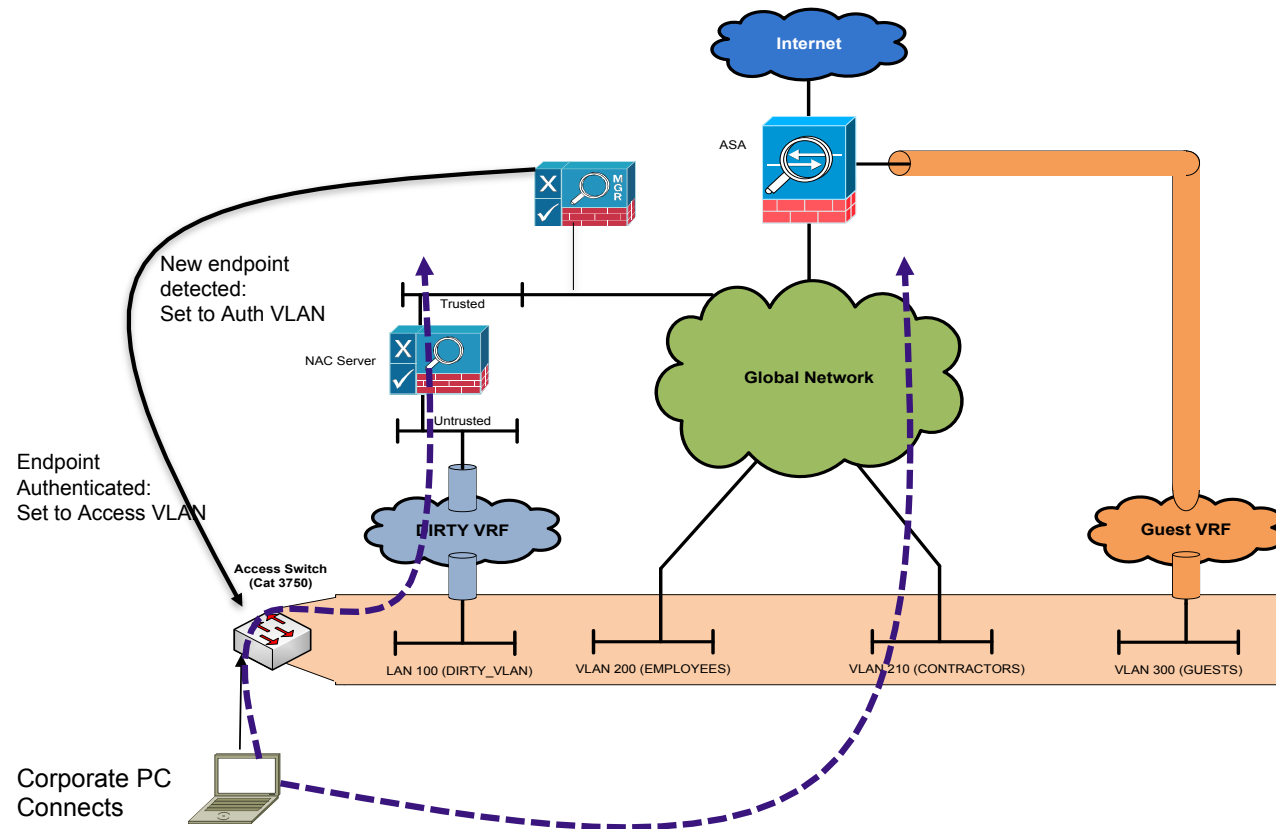
Phased deployment mode for 802.1X



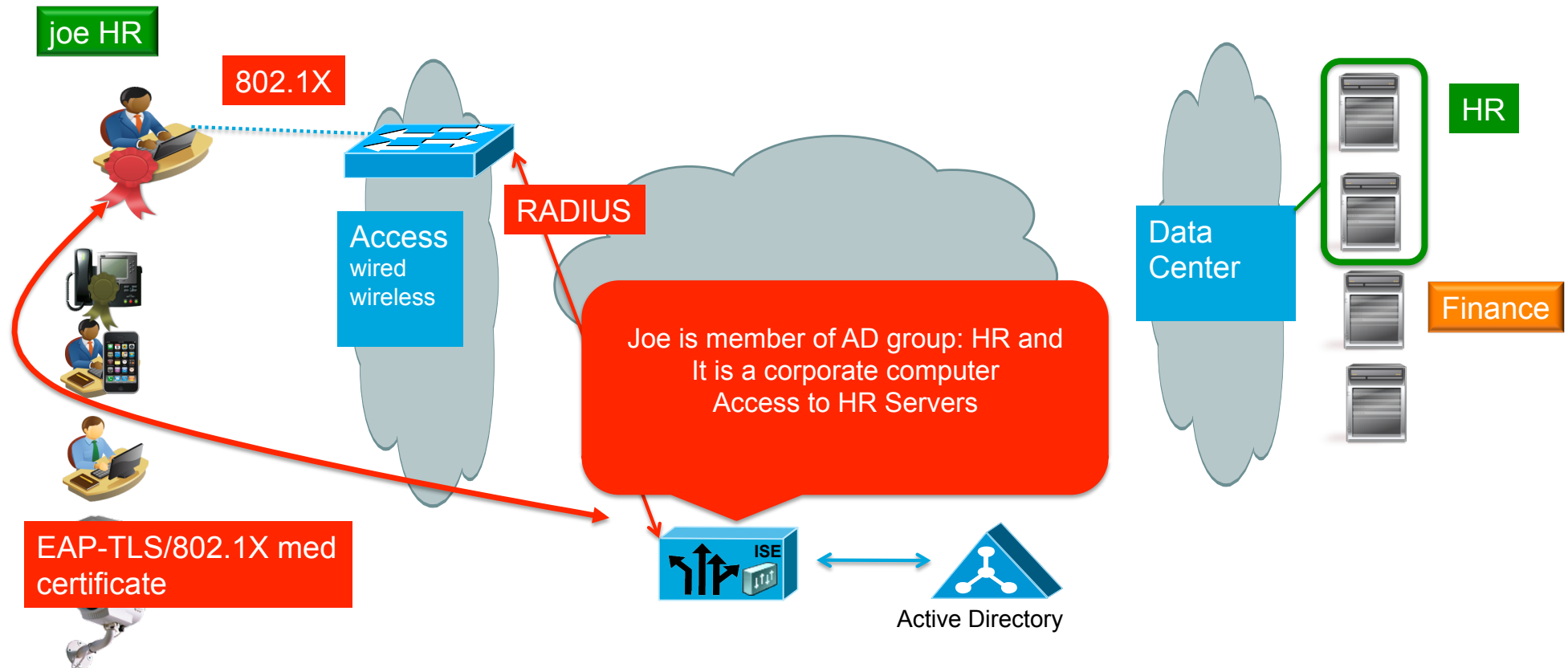
Using the Identity



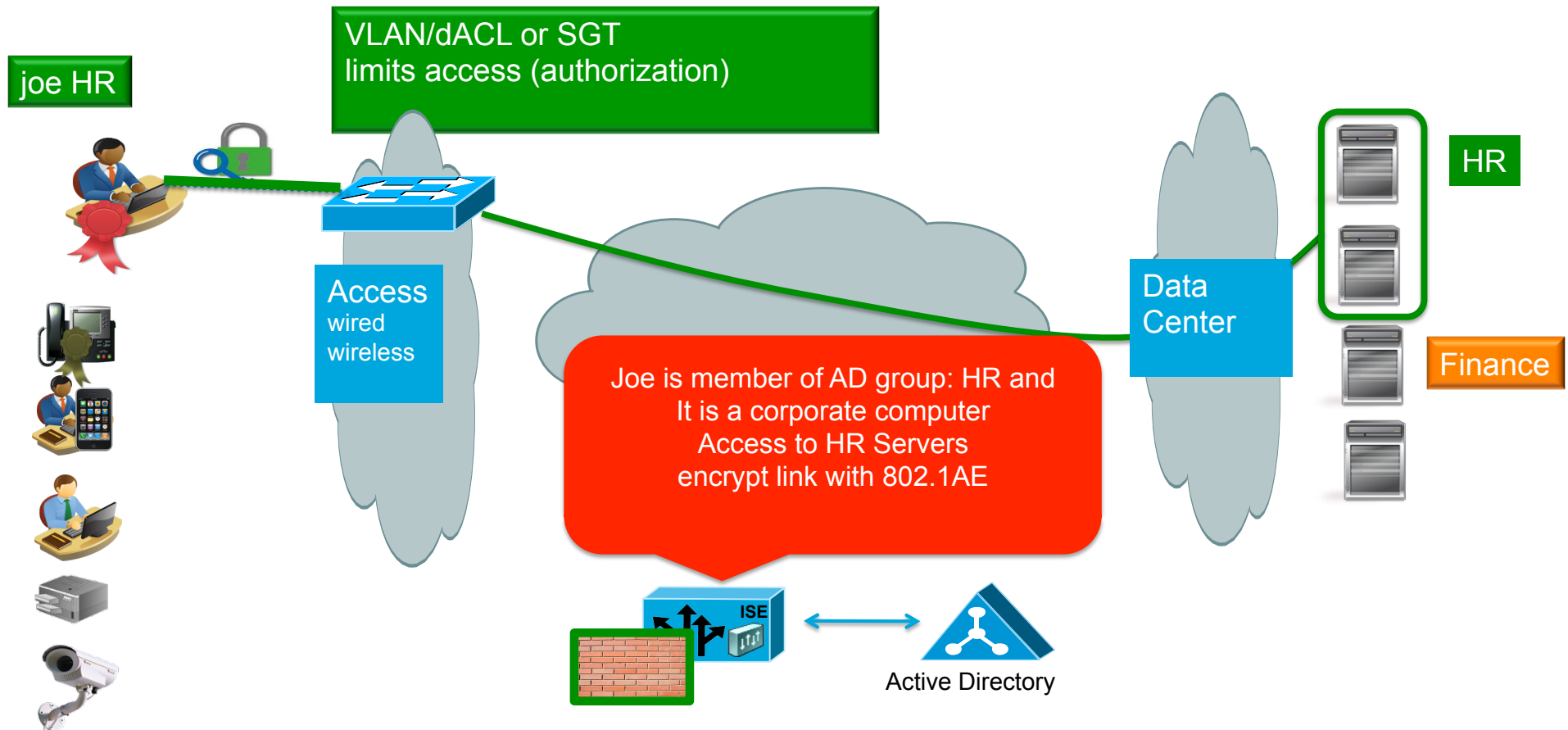
Overlay Solution



When Identity is embedded (like 802.1X)



Mapping user's group to security role



A Systems Approach

Switch/Controller 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#
```

Clients > Detail

General

AVC Statistics

Client Properties

MAC Address	7c:6d:62:e3:d5:05
IPv4 Address	10.1.41.100
IPv6 Address	fe80::7e6d:62ff:fee3:d505, ...
Client Type	Regular
User Name	
Port Number	1
Interface	guest
VLAN ID	41
CCX Version	Not Supported
RF Version	Not Supported
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	2
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	PERMIT_ALL_TRAFFIC
IPv4 ACL Applied Status	Yes
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable

A Systems Approach

Switch/Controller 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-TP-TNET-ONLY-4dche020
  URL Redirect ACL: ACL-WEBAUTH-REDIRECT
  URL Redirect: https://atw-ise01.clt.cisco.com:8443/guestportal/
?sessionId=AC1A783600000102A805ACC&action=cwa
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: AC1A783600000102A805ACC
  Acct Session ID: 0x00000019
  Handle: 0xDE000010

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

Clients > Detail

General

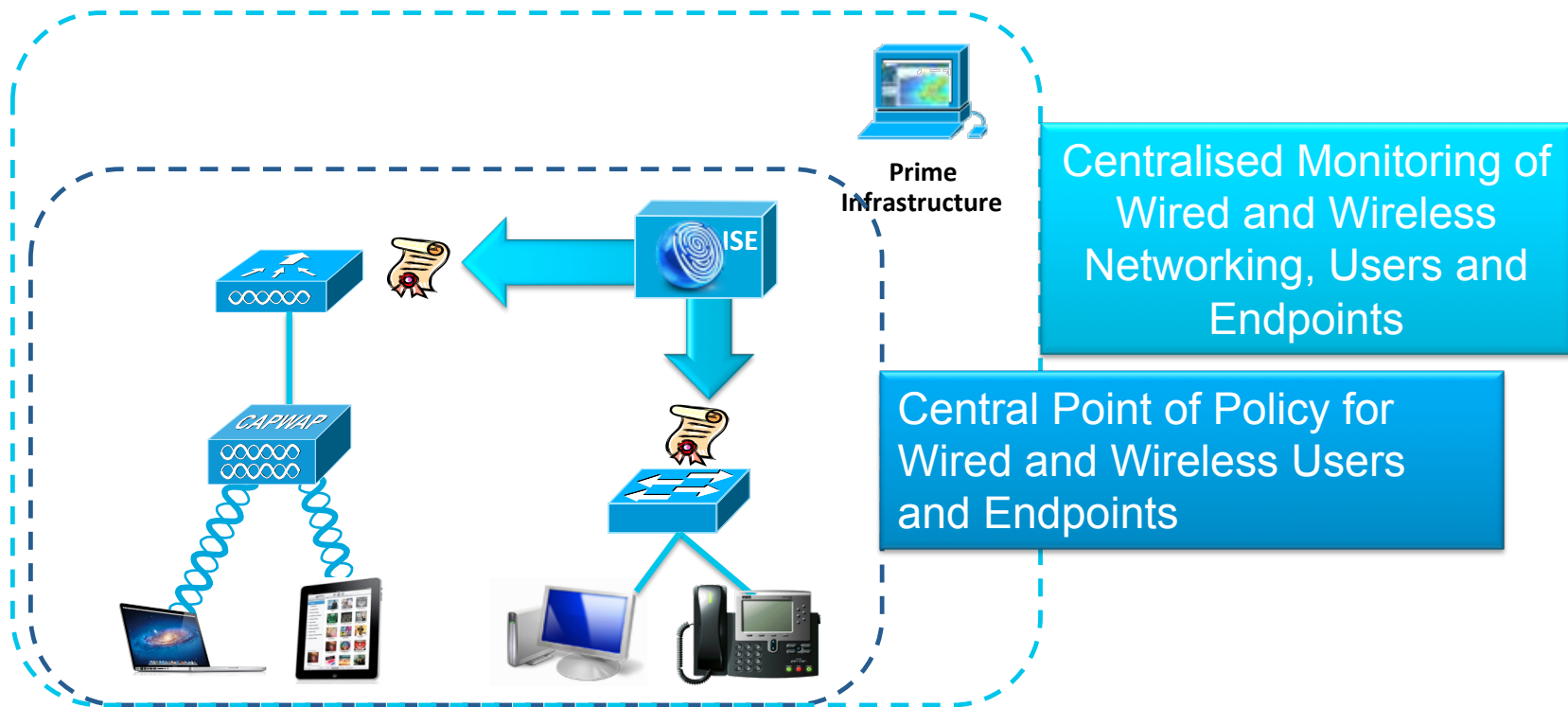
AVC Statistics

Client Properties

MAC Address	7c:6d:62:e3:d5:05
IPv4 Address	10.1.41.100
IPv6 Address	fe80::7e6d:62ff:fee3:d505,
Client Type	Regular
User Name	
Port Number	1
Interface	guest
VLAN ID	41
Policy Manager State	CENTRAL_WEB_AUTH
Management Frame Protection	No
Security Policy Completed	No
SNMP NAC State	Access
Radius NAC State	CENTRAL_WEB_AUTH
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	ACL-WEBAUTH-REDIRECT
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	https://ise-mdm.cts.local:8443/guestportal/gateway?s
IPv4 ACL Name	none
IPv4 ACL Applied Status	Unavailable
IPv6 ACL Name	none

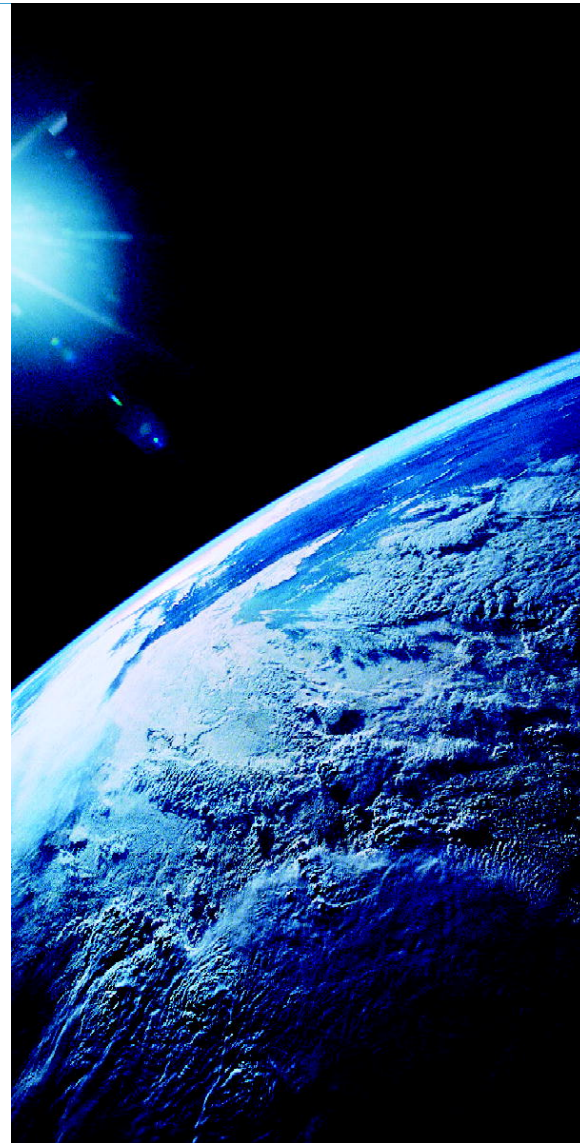
Cisco ISE Provides Policy for Wired and Wireless LANs

Unified wired and wireless policy (ISE) and management (PI)



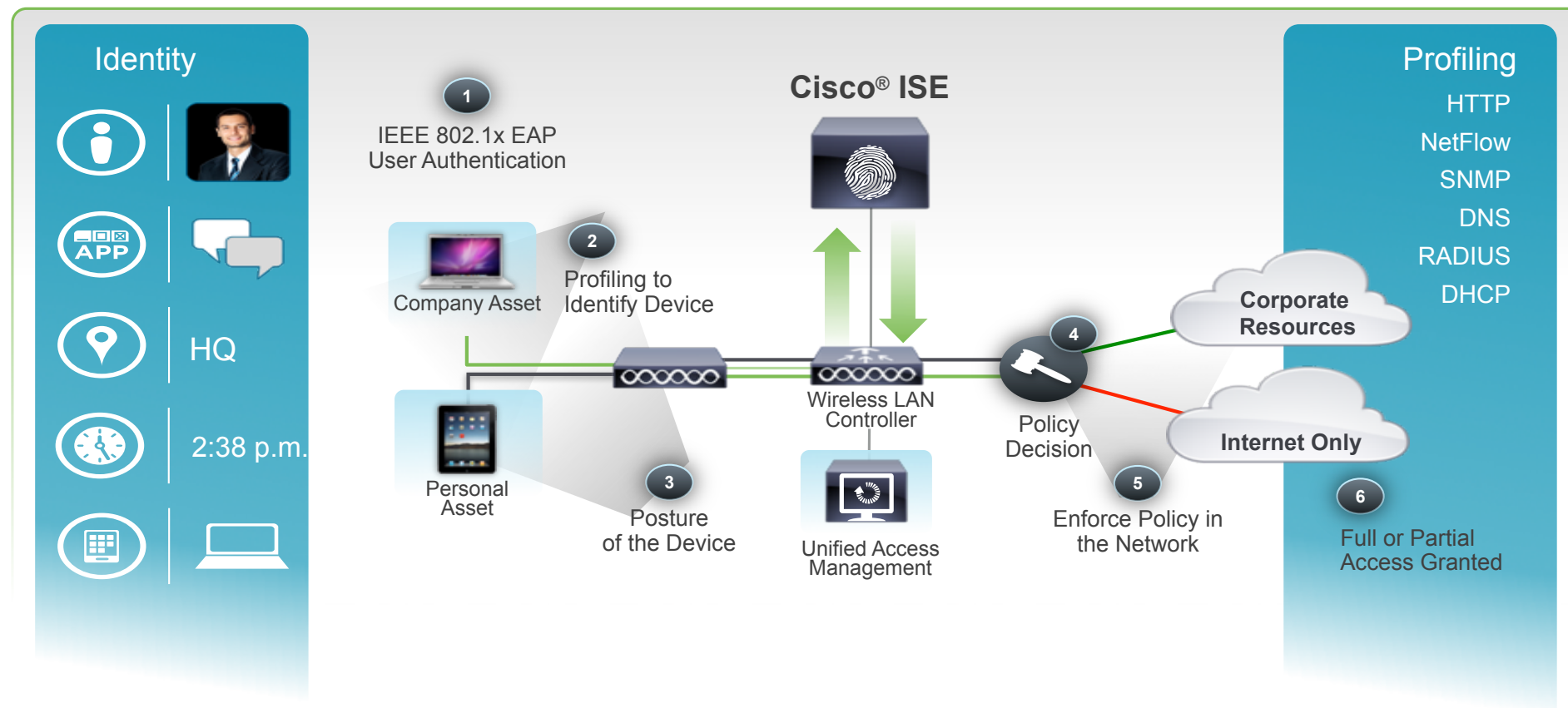
But we need more
information !

Context Awareness



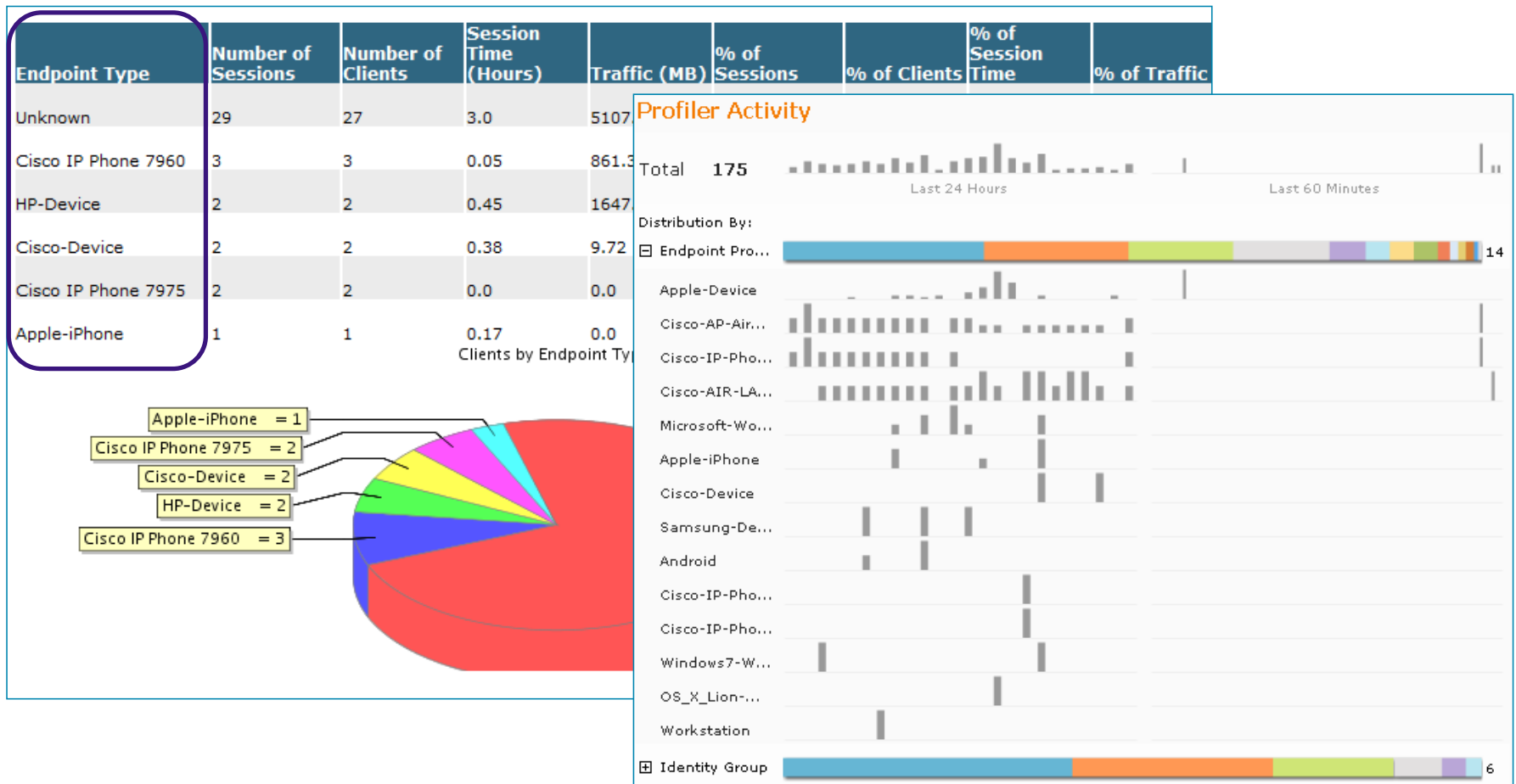
Policy: Who, What, Where, When, and How?

Network Access Workflow



Profiling Technology

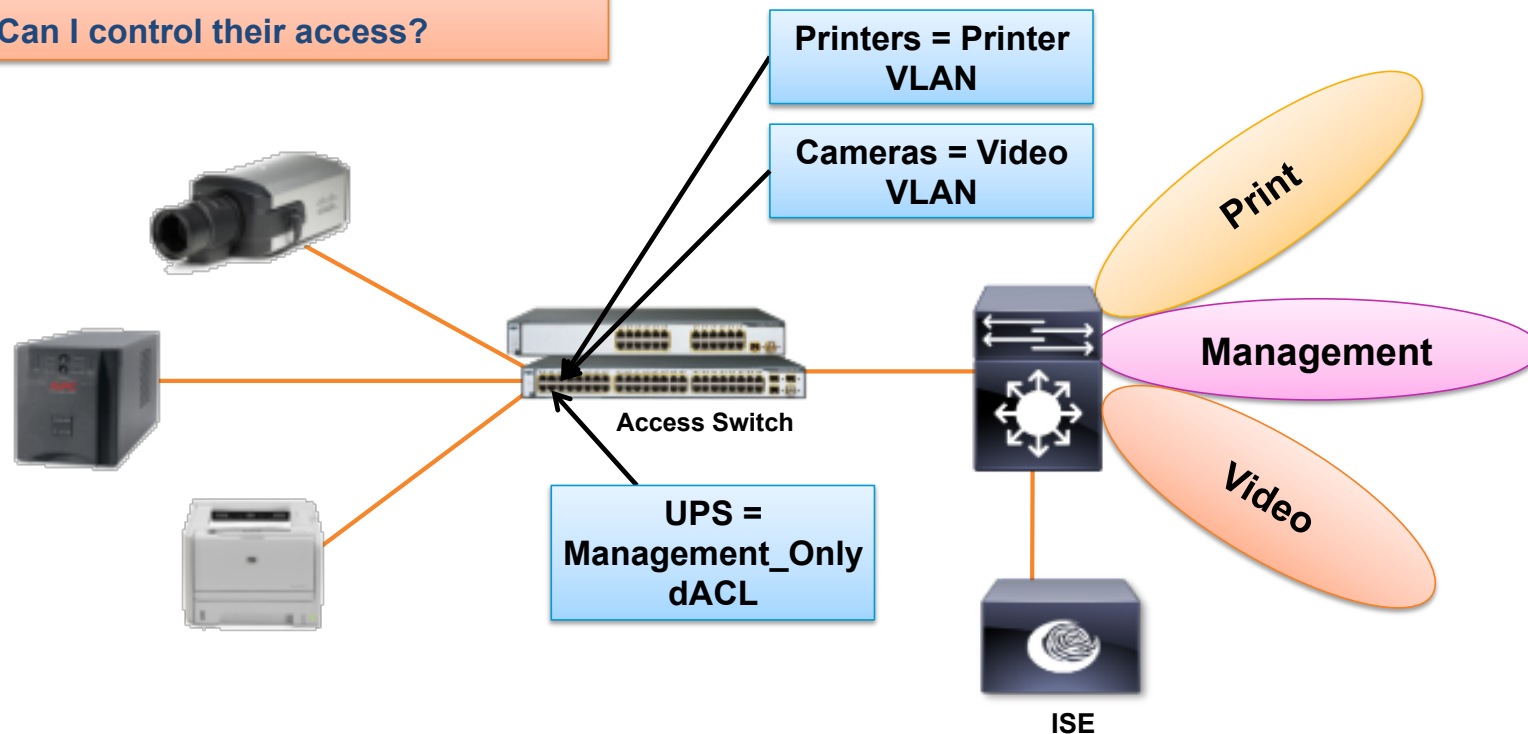
Visibility Into What Is On the Network



Profiling Non-User Devices

Dynamic Population of MAB Database Based on Device Type

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



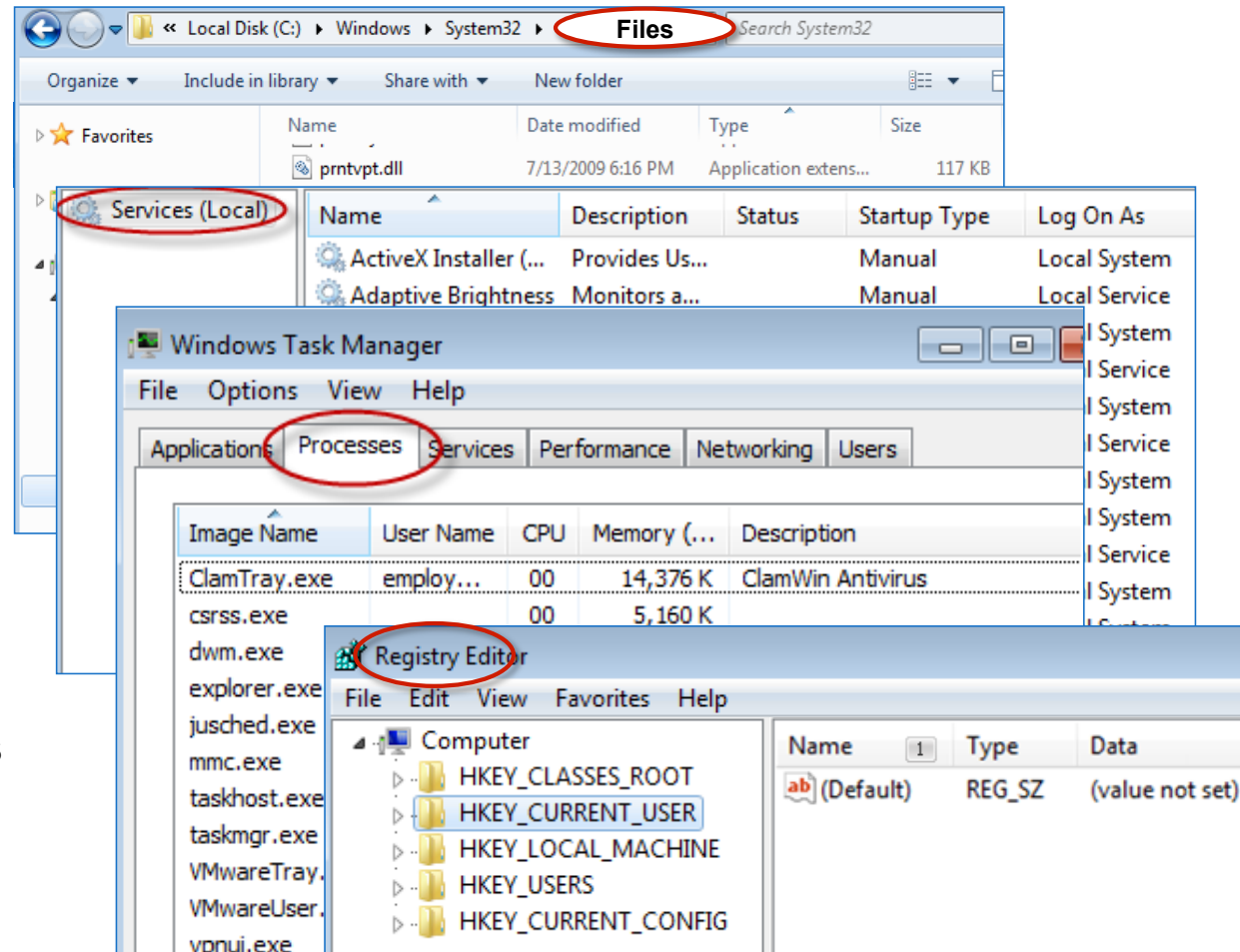
Differentiated Access Based on Device Type

-



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



ISE – Posture Policies

Employee Policy:

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

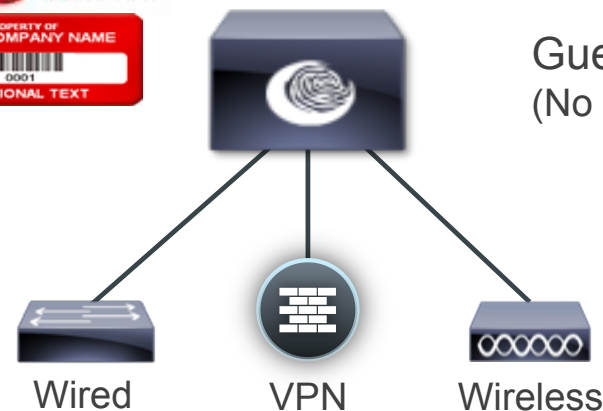
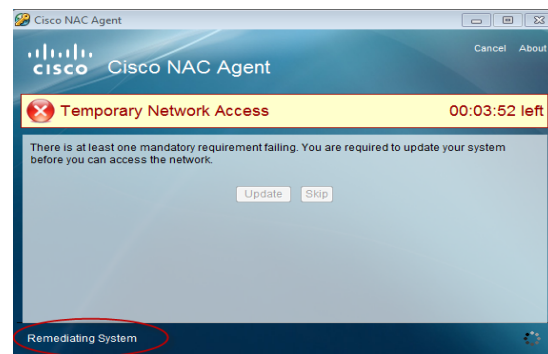


Contractor Policy:

- Any AV installed, running, and current



Guest Policy: Accept AUP (No posture - Internet Only)



Employees

Contractors/Guests

Tying it All Together

ISE Authorization Policy Definition



User



Device Type



Location



Posture



Time



Access Method



Custom

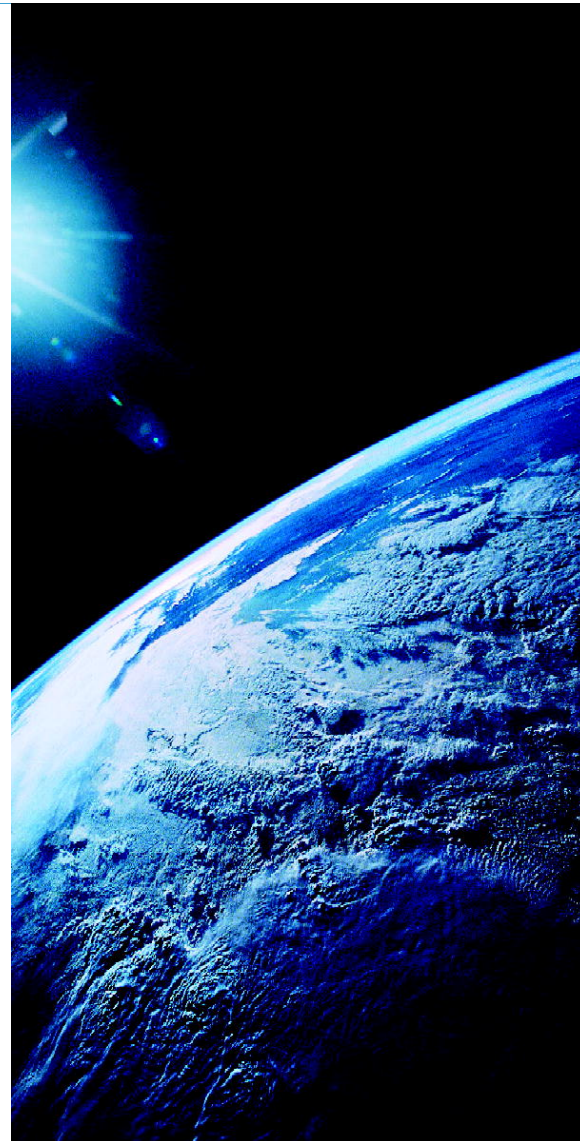
Authorization Policy At A Glance

First Matched Rule Applies

Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
✓ Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
✓ Enabled	Game_Console	Game_Console-Registered		Game_Console
✓ Enabled	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers AND San_Jose AND CERTIFICATE:Subject Alternative Name MATCHES.*(demo.local)\$ AND Radius:User-Name MATCHES ^(host/).*	AD_Login
✓ Enabled	Employee-Wired	Any	Employee_Wired AND Posture_Compliant	Employee
✓ Enabled	Employee-Wireless	Workstation	Employee_Wireless AND Posture_Compliant AND LDAP1:badPwdCount MATCHES [0-5]	Employee_Wireless
✓ Enabled	Employee-iPAD	Apple-iPad	Employee_Wireless AND Posture_Compliant AND North_America	Employee_iPAD
✓ Enabled	Contractor-iPAD	Android OR Apple-iPad OR Apple-iPhone OR Apple-iPod OR BlackBerry	Contractor_Wireless AND Posture_Compliant AND North_America	Contractor_iPAD
✓ Enabled	Guest-Wired	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wired AND Posture_Compliant	Guest
✓ Enabled	Guest-Wireless	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wireless AND Posture_Compliant	Guest_Wireless
⊖ Disabled	Default-Posture	Any		CWA_Posture_Remediation
✓ Enabled	Default	Any		Central_Web_Auth

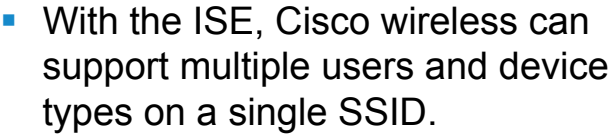
BYOD

© 2013 Cisco and/or its affiliates. All rights reserved.



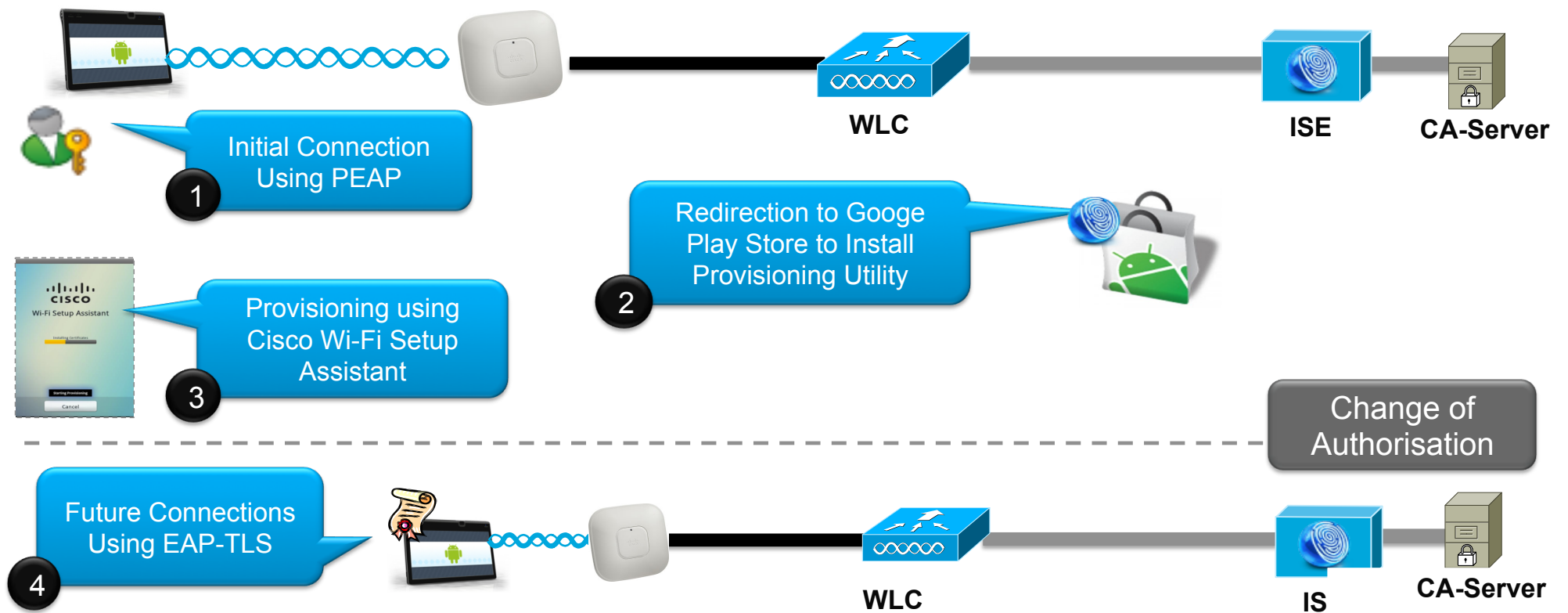
Cisco Connect

44



Android Device Provisioning

Wide variety of OS flavours = no consistent native API



"My Devices" Portal

Self-Registration and Self-Blacklisting of BYOD Devices

The screenshot displays the Cisco My Devices Portal interface. At the top, the Cisco logo and 'My Devices Portal' are visible, along with a 'Welcome tom (Sign Out)' message. The main section is titled 'Register a New Device' and includes instructions: 'To register a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.' Below this are input fields for '* Device ID' and 'Description', with 'Submit' and 'Cancel' buttons. A table titled 'Current Registered Devices' lists four devices: Motorola Xoom, Apple iPhone, Macbook Pro, and Apple iPod, each with 'Edit' and 'Blacklist' links. A blue callout bubble with a '1' points to the 'Description' field, stating 'New Devices Can be Added with a Description'. Another blue callout bubble with a '2' points to the 'Blacklist' link in the table, stating 'Devices can be Blacklisted By the User.' To the right, a separate section shows a registration attempt for a device with ID '78-A3-E4-BA-89-80'. It includes a 'Register' button and a message: 'This device has not been registered. To register this device, please enter the Device ID (MAC Address format nn:nn:nn:nn:nn:nn where n is either 0-9 or a-f); then click the \'Register\' button to complete the registration.' A blue callout bubble with a '3' points to this section, stating 'Devices Can be Self-Registered, Up to an Administrator Defined Limit'. Below this, a warning message states: 'You cannot register this device, since you have reached the maximum number of devices allowed per user. Please delete one or more of your registered devices, to get you under the device registration limit. This will allow you to register this device. Maximum number of devices you are allowed to register: 5'.

1 New Devices Can be Added with a Description

2 Devices can be Blacklisted By the User.

3 Devices Can be Self-Registered, Up to an Administrator Defined Limit

You cannot register this device, since you have reached the maximum number of devices allowed per user.

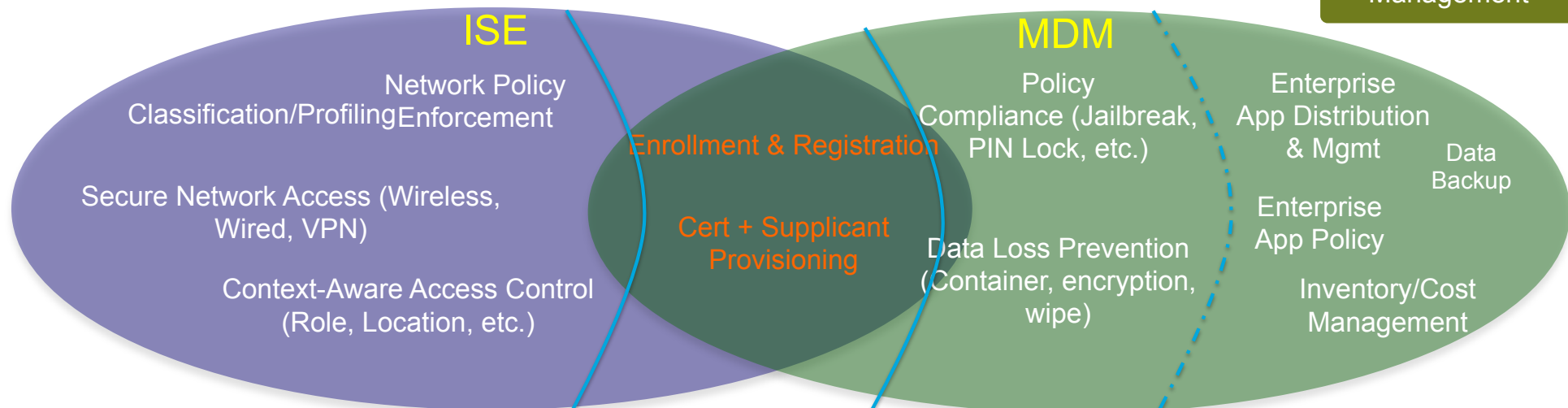
Please delete one or more of your registered devices, to get you under the device registration limit. This will allow you to register this device.

Maximum number of devices you are allowed to register: 5

Identity
and Policy

Management

Evolving Roles of ISE and MDMs



ISE 1.0 & 1.1

Native ISE functionality

- Profiling
- Authentication
- Policy Enforcement
- etc.

ISE 1.1.x

Native ISE functionality

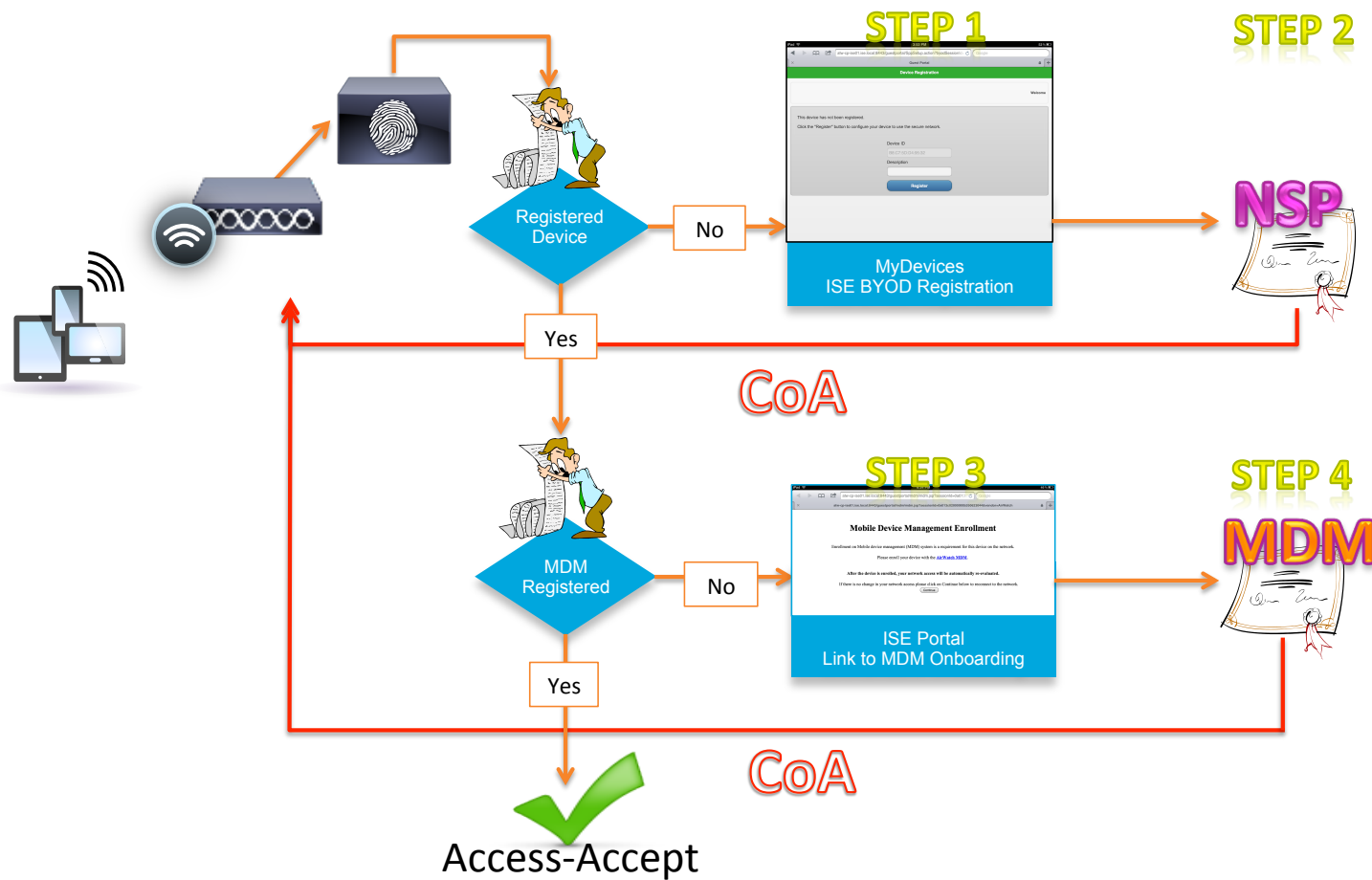
- Enrollment/Registration
- Self-Enroll Portal
- Certificate Enrollment
- Blacklisting

ISE 1.2 (Jul '13)

ISE – MDM API

- Additional device data
- Policy compliance
- Data wipe

MDM Onboarding Flow



airwatch™

Mobile Iron®

Good

ZENPRISE

SYBASE®

MDM Integration

Remediation

- Administrator / user can issue remote actions on the device through MDM server (Example: remote wiping the device)
 - MyDevices Portal
 - ISE Endpoints Directory

Endpoints

Edit Add Delete Import Export MDM Actions

Endpoint Profile	MAC
☐ Android	F4:6
☐ Android	00:23:76:95:86:93
☐ Android	00:23:76:95:86:93
☐ Android	00:18:A4:06:71:4F

MDM Actions dropdown menu:

- Full Wipe
- Corporate Wipe
- PIN Lock

CISCO My Devices Portal

Welcome employee1@ise.local ([Sign Out](#))

Add a New Device

To add a device, enter the Device ID and description and click Submit.

Your devices

Select	Device ID	Description	State
☐	00:22:44:11:33:55	My XBOX360 Game Console	...
☐	Apple-1pad	My iPad Gen1	✓

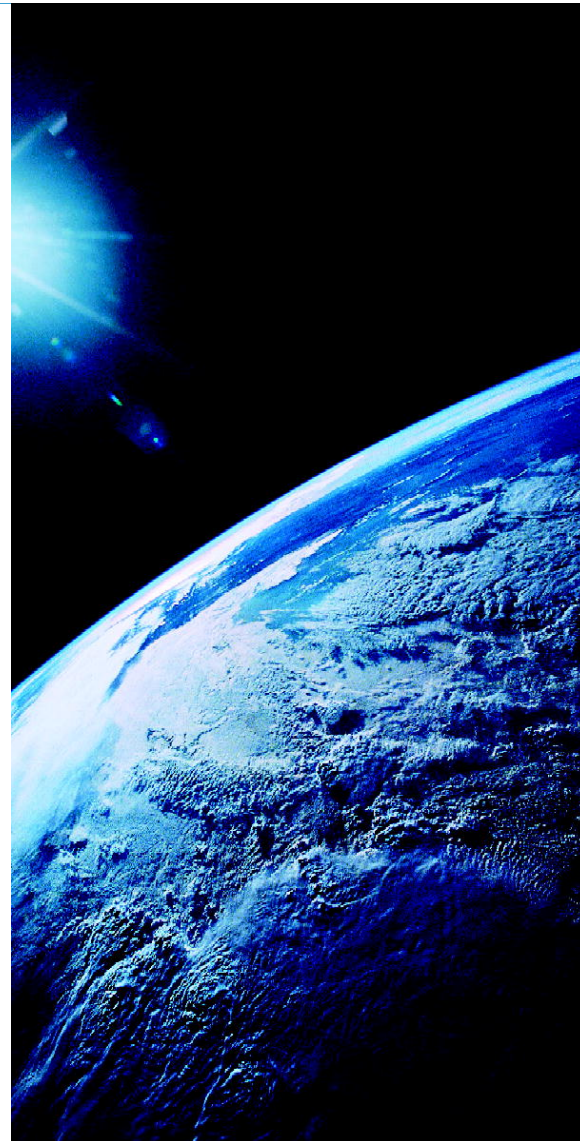
Actions: Edit Reinstall Lost? Delete Full Wipe Corporate Wipe PIN Lock

Options

- Edit
- Reinstall
- Lost?
- Delete
- Full Wipe
- Corporate Wipe
- PIN Lock

Using Context in Network

© 2013 Cisco and/or its affiliates. All rights reserved.



Cisco Connect

56

Security Group Tag (SGT) Overview

Translating Business Policy to the Network

SGT lets you define policy in meaningful business terms

Business Policy



Destination Source	HR Database	Corp. Data	Storage
Empl. BYOD	✗	✗	✗
Empl. PC	✗	✓	✗
HR Admin	✓	✓	✗
IT Admin	✓	✓	✓



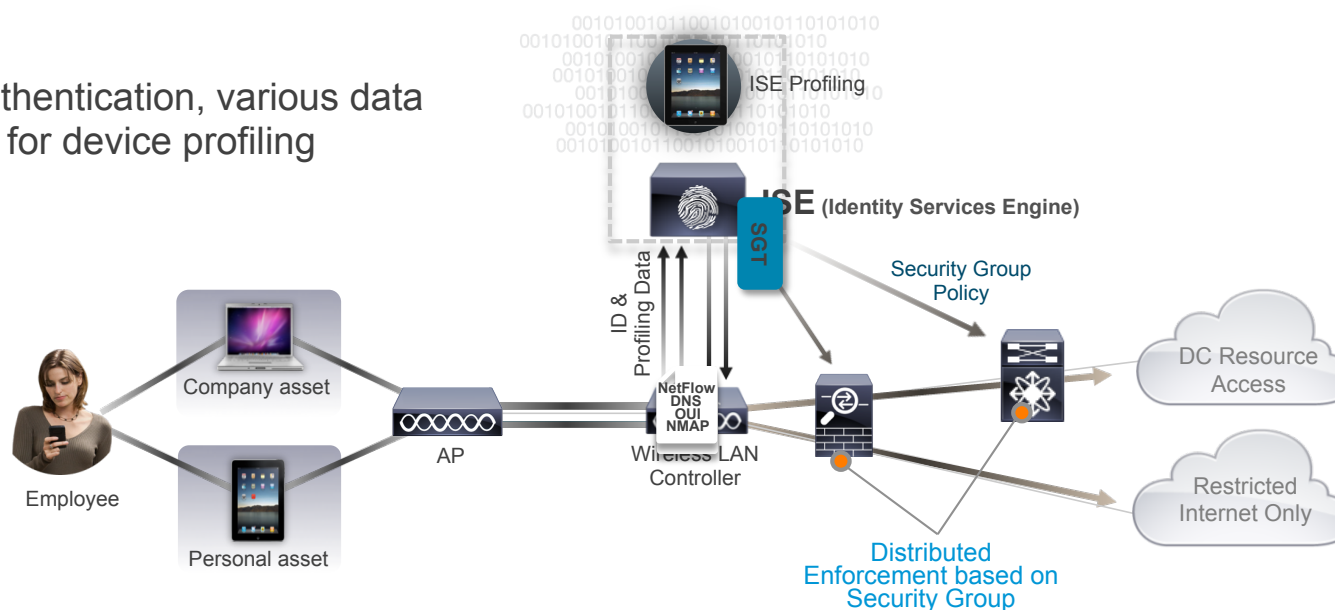
Rich Context Classification with ISE BYOD Use Case

Classification Result:

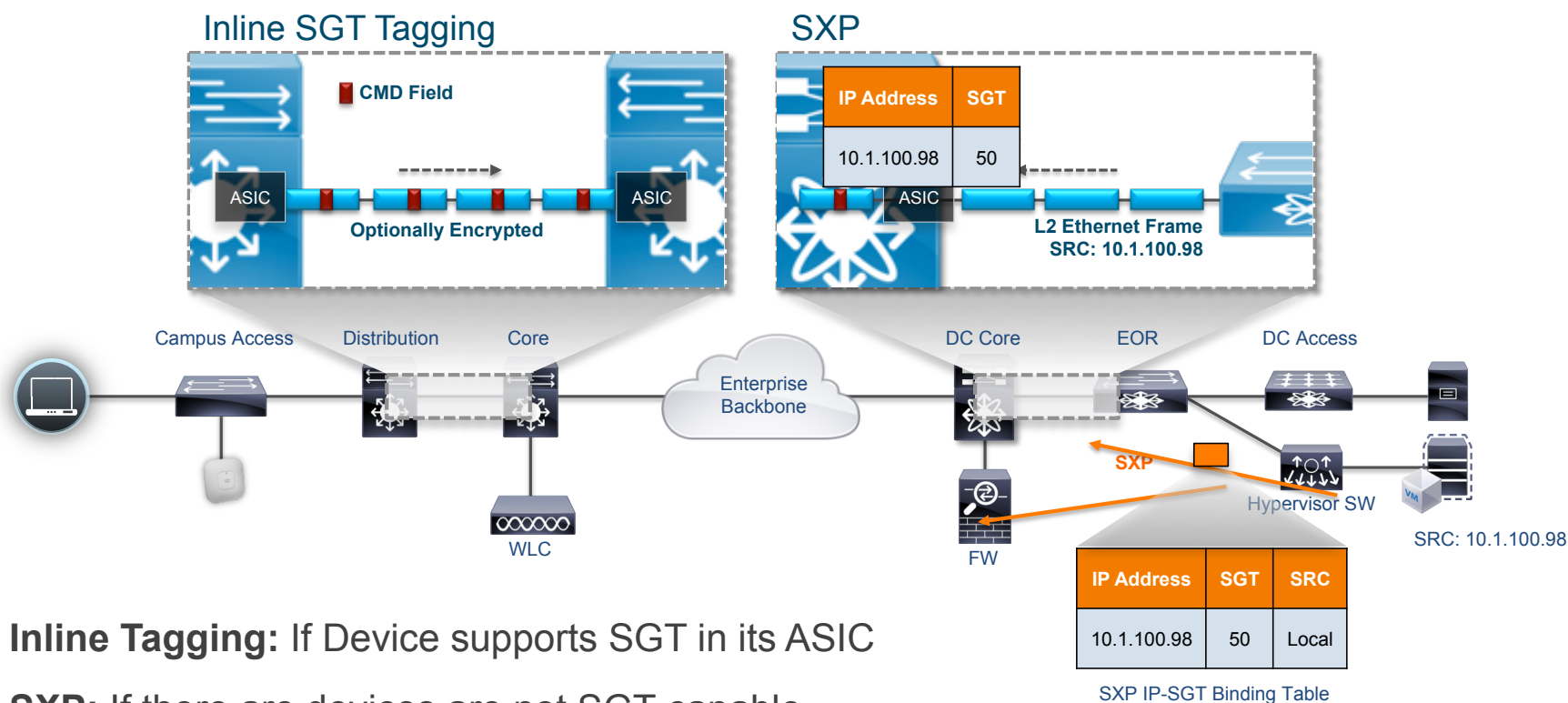
Device Type: Apple iPad
User: Mary
Group: Employee
Corporate Asset: No

Personal Asset SGT

Along with authentication, various data is sent to ISE for device profiling



How SGT is Transported?



- **Inline Tagging:** If Device supports SGT in its ASIC
- **SXP:** If there are devices are not SGT-capable

SGT/IPSEC WAN Deployment - ISRG2



- IPSEC inline Tagging – ESP Header
- SGT Capability exchange during IKEv2 negotiations
- Learn SGT from SXP or Auth-methods
- Site-to-Site IPSEC such as DMVPN, DVTI, SVTI methods supported

SGT- GETVPN WAN Deployment

ISRG2 15.(x)T and ASR 3.9*



- GETVPN inline Tagging – GET Header
- SGT Capability exchange during GET key negotiations
- Learn SGT from SXP, inline tag or Auth-methods
- Site-to-Site IPSEC such as DMVPN, DVTI, SVTI methods supported

SGT Platform Support



Classification

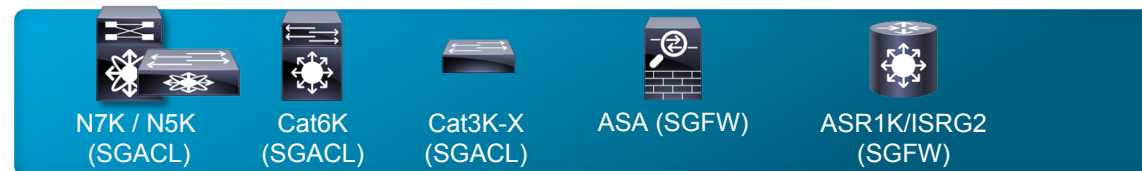


Transport



MACsec Capable with Tagging: Cat3K-X, Cat6K-Sup2T, N7K

Enforcement



Enforcing Traffic on Firewall (ASA) - SGFW

The screenshot displays the Cisco ASDM 6.7 for ASA - 10.1.201.2 interface. The left pane shows the 'Device List' with '10.1.201.2' selected. The main pane shows the 'Configuration > Firewall > Access Rules' configuration page. The table below lists the configured rules.

#	Enabled	Source Criteria:	Destination Criteria:	Service	Action	Hits	Logging	Time	Descript						
		Source	User	Security Group	Destination	Security Group									
Inside (1 incoming rule)															
1	☒	any			any				ip	Permit	0				
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 Management_SGT	any	Employee_Portal		http https	Permit	0					
4	☒	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal		http https	Deny	0					
5	☒	any		Management_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	Deny	0					Time Card Application
9	☒	any		CC_Scanner_SGT	any	CreditCard_Ser...		https	Permit	0					Credit Card Scan Communication
Global (1 implicit rule)															
1		any			any			ip	Deny						Implicit rule

Source Tags

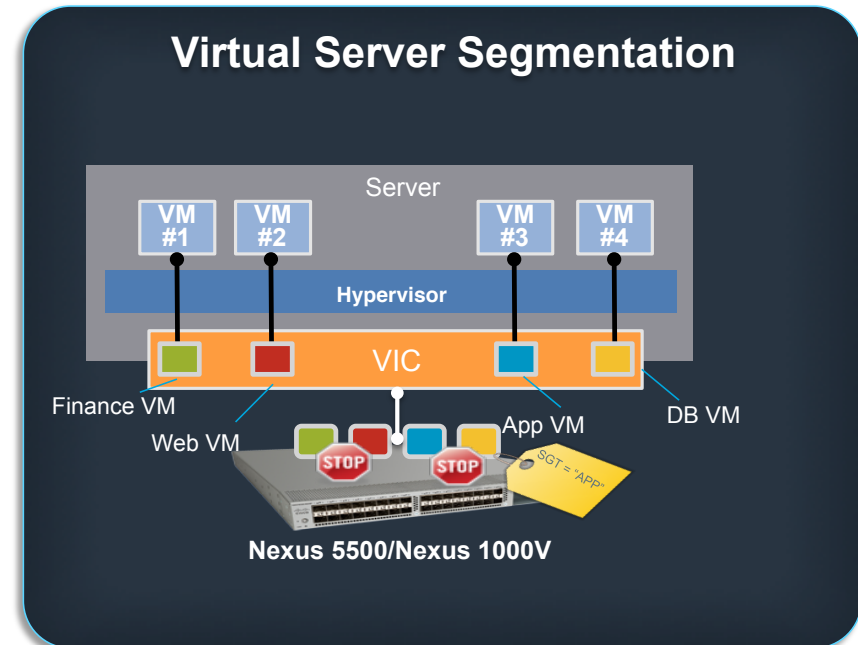
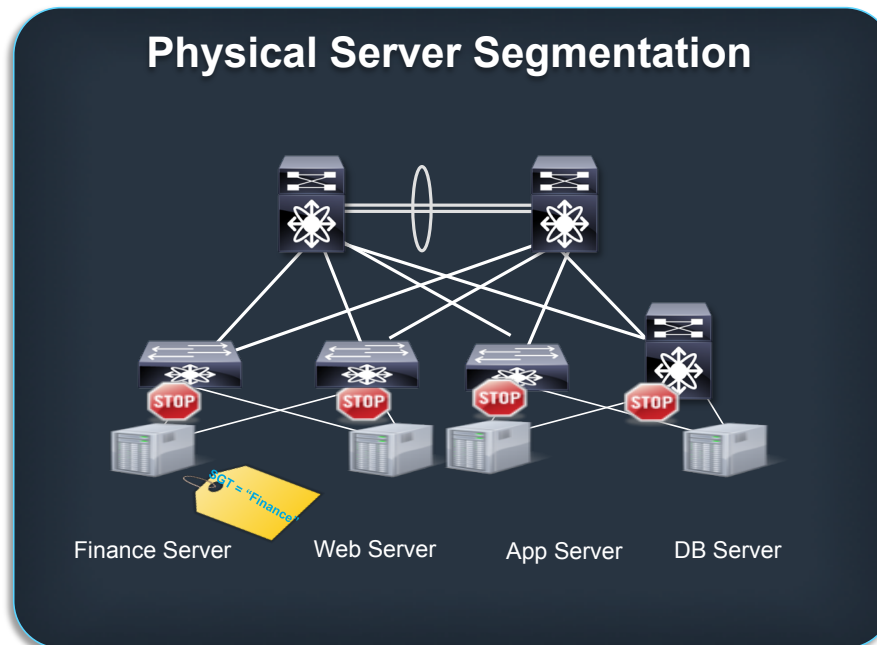
Destination Tags

Configuration changes saved successfully.

<admin> 15 5/31/12 11:53:50 PM PDT

Use Case: Segmentation

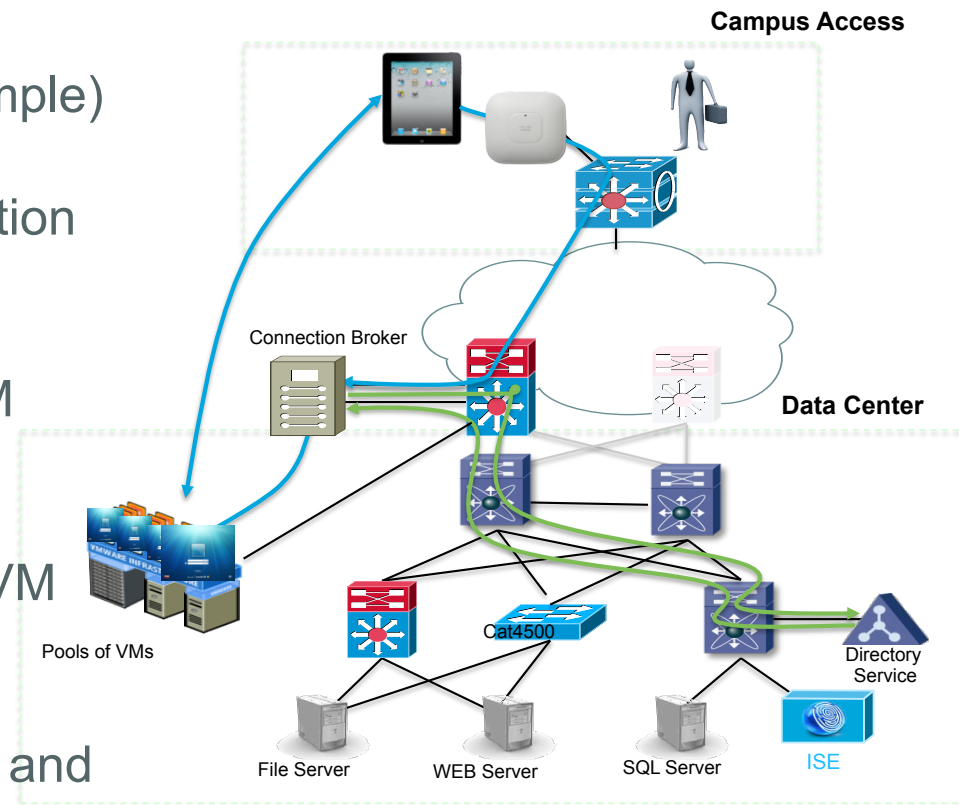
Physical or VM server segmentation for compliance



- Manually tag servers or using dynamic lookup (IPM, Port Profile, 802.1X, MAB)
- Use SGACL to enforce traffic between servers (VM, physical, VM-physical)
- Applicable for inter-security zone and intra-security zone (inside a VLAN)

Background: Connection Brokers

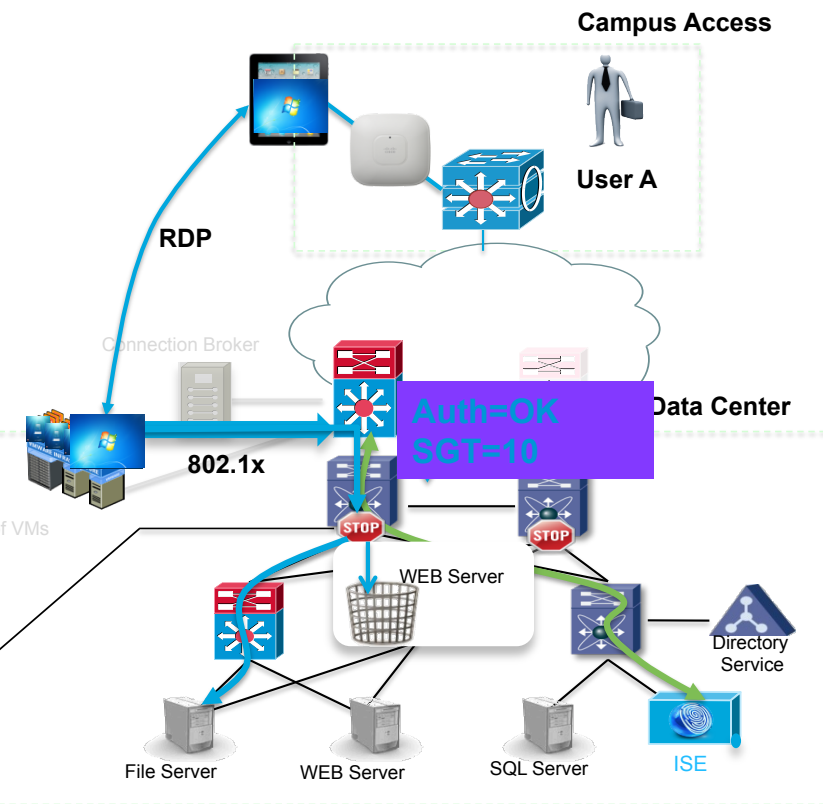
- User logs into the thin client (no user authentication performed for this example)
- User initiates a connection to Connection Broker via RDP, PCoIP protocols
- Broker queries Active Directory for VM pool assignment
- Broker redirects user to an available VM in the VM pool
- User is now able to remotely view and control the VM



Applying 802.1x and SGA to VDI

- User logs into VM which triggers 802.1x authentication
- Authentication succeeds. Authorization assigns the SGT for the user.
- Traffic hits the egress enforcement point
- Only permitted traffic path (source SGT to destination SGT) is allowed

SRC \ DST	File Server(111)	Web Server (222)
User A (10)	Permit all	Deny All
User B (20)	Deny all	SGACL-C



MACSec and NDAC

Media Access Control Security and Network Device Admission Control



MACSec: Layer-2 Encryption (802.1AE)

Industry Standard Extension to 802.1X

Encrypts the links between host and switch and links between switches.

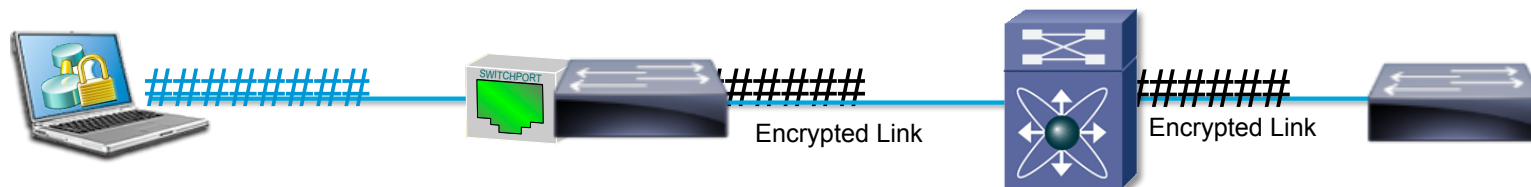
Traffic in the backplane is unencrypted for inspection, etc.

Client requires a supplicant that supports MACSec and the encryption key-exchange

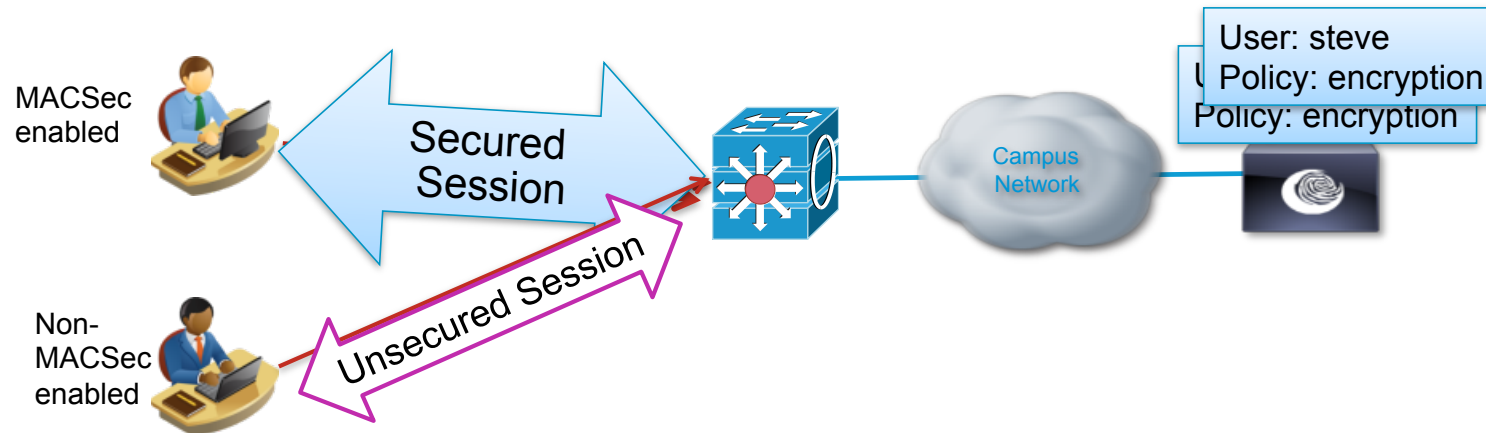
NDAC: Authenticate and Authorize switches entering the network

Only honors SGTs from Trusted Peers

Can retrieve policies from the ACS/ISE Server and “proxy” the trust to other devices.



Client 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

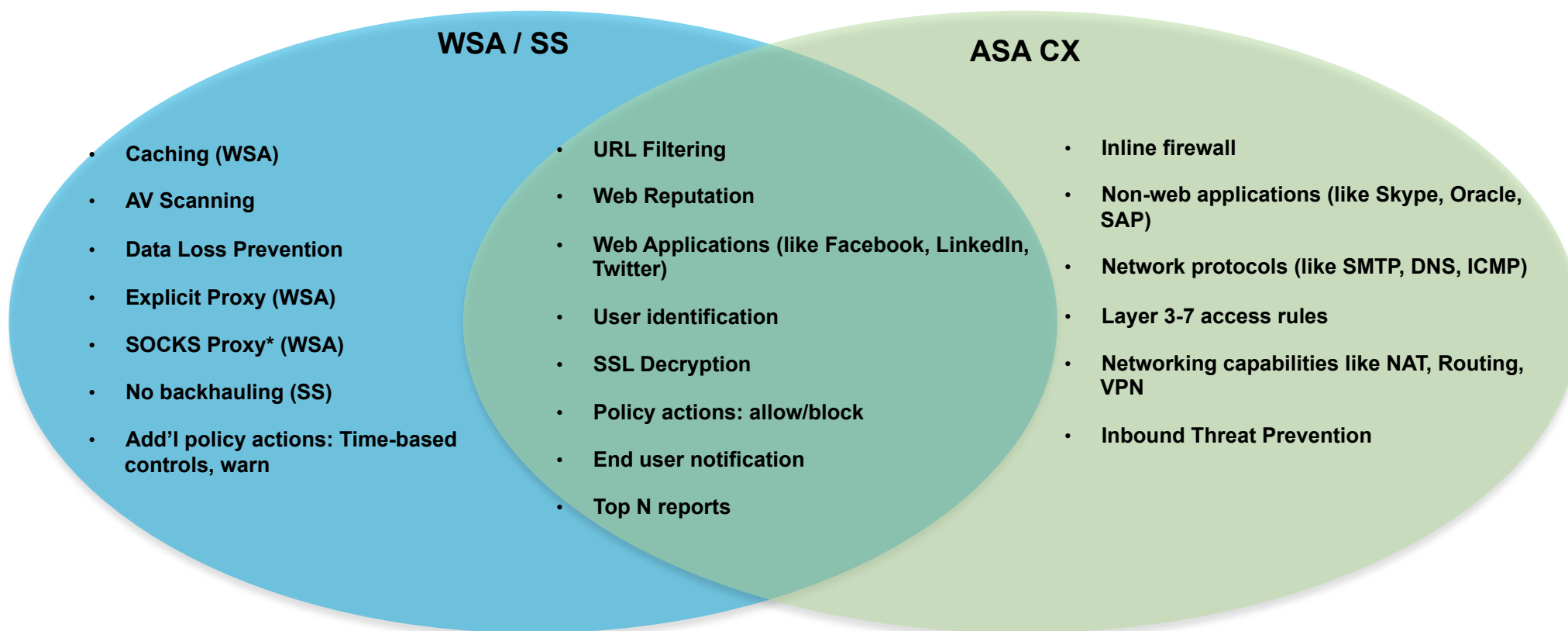


SGT - Summary

- SGTs builds upon Identity and Unified Access services
- SGTs provides a scalable Identity and Unified Access role based access control model
- SGTs has migration strategies allow customer to deploy with existing hardware
- Unified Access and SGTs are deployable **today**

“Context” Firewall ASA-CX = Application FW

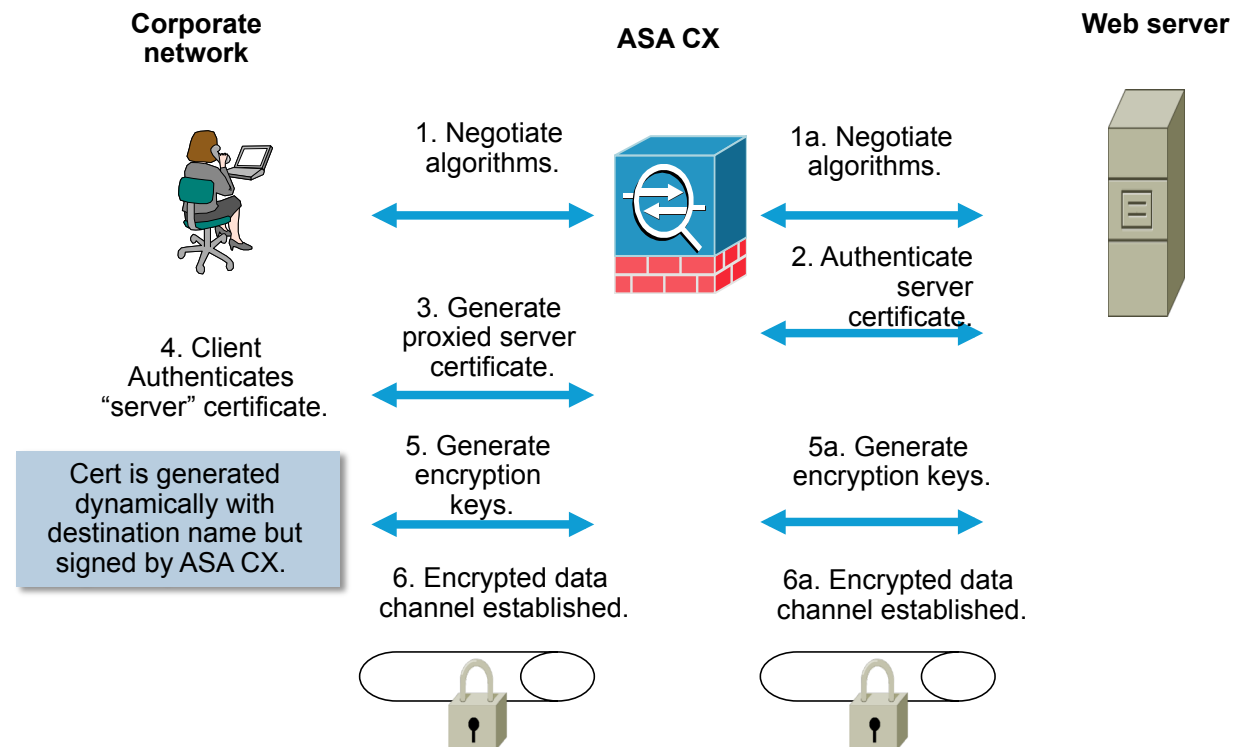
ASA CX & WSA/SS: Feature Overlap & Differences



ASA CX – Decryption Policies

TLS Decryption – Man In The Middle Flow

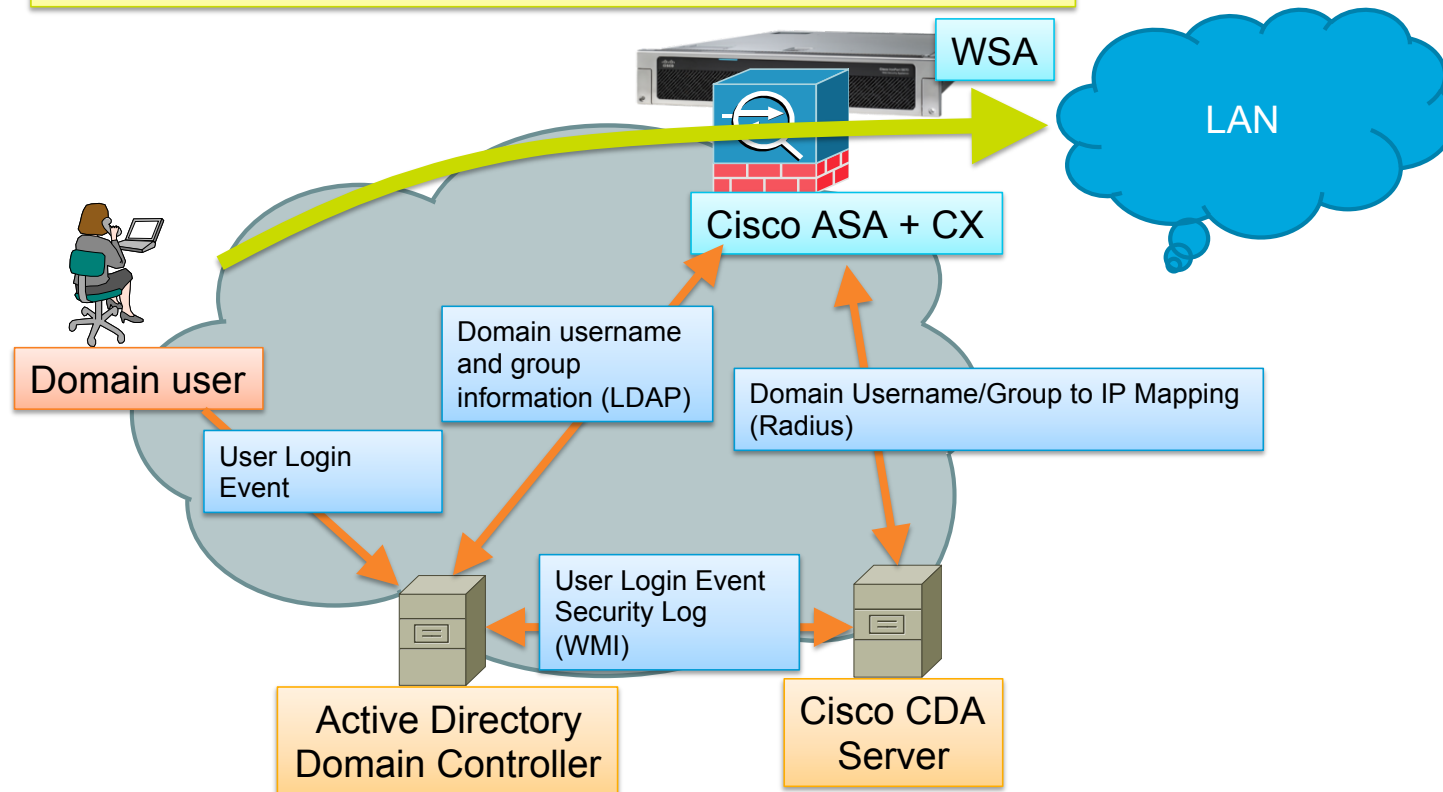
ASA CX acts as a CA and issues a certificate ‘on behalf of’ the real web-site.



ASA CX – Identity Policies

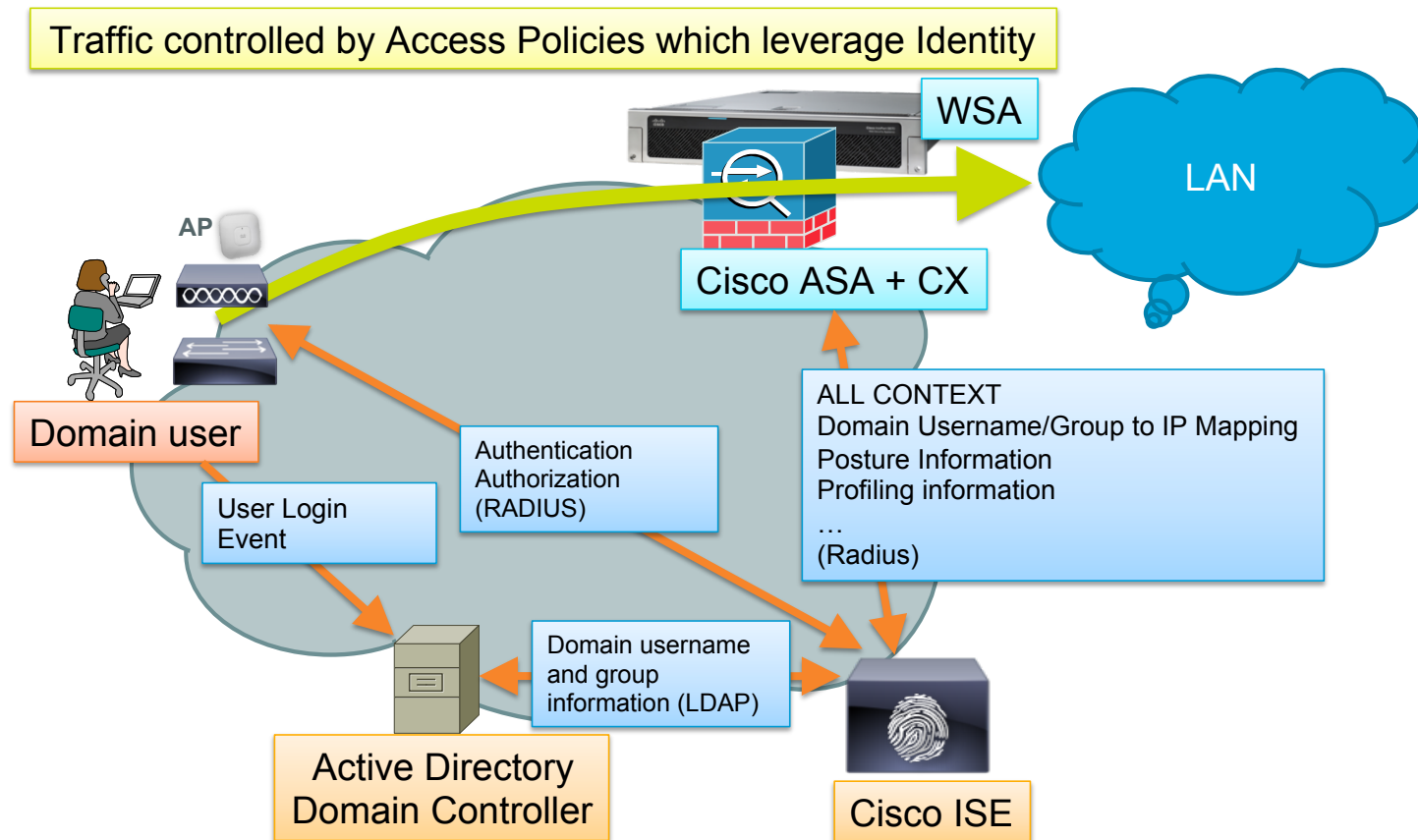
Passive Authentication Architecture

Traffic controlled by Access Policies which leverage Identity



ASA CX – Identity Policies

The Future is in "Unified" Identity Source



Applications: Visibility With Control



Broad... ... classification of all traffic 1,000+ apps	      
MicroApp Engine Deep classification of targeted traffic 75,000+ MicroApps	       
App Behavior Control user interaction with the application	           

WHAT

Business Class URL Filtering

Web Usage Control



60
languages

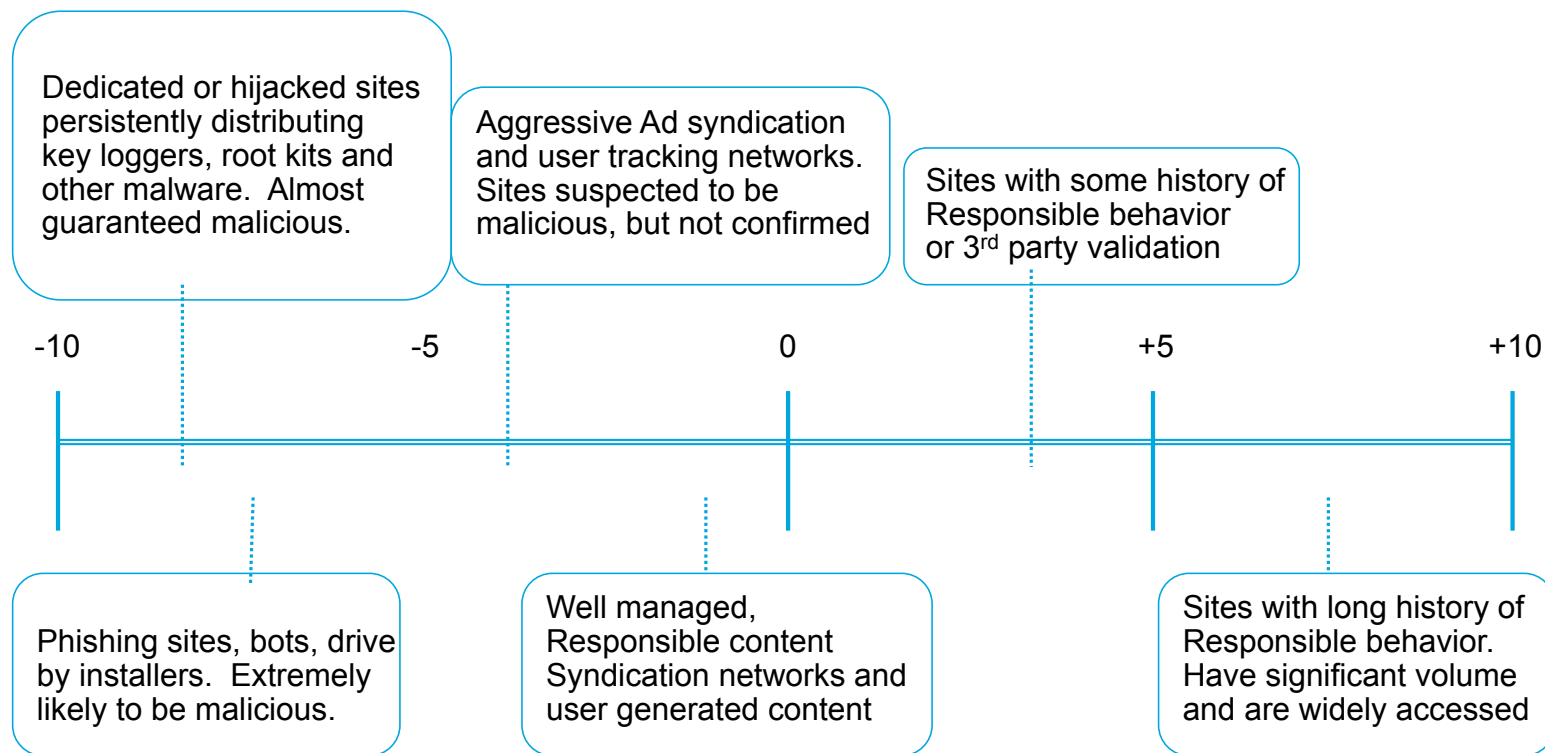
200
countries

20
mn URLs

98%
coverage

ASA CX – Advanced Inspection Policies

Understanding Web Reputation Scores



Reputation Database from Security Intelligence Operations

Cloud-Based Global Threat Intelligence

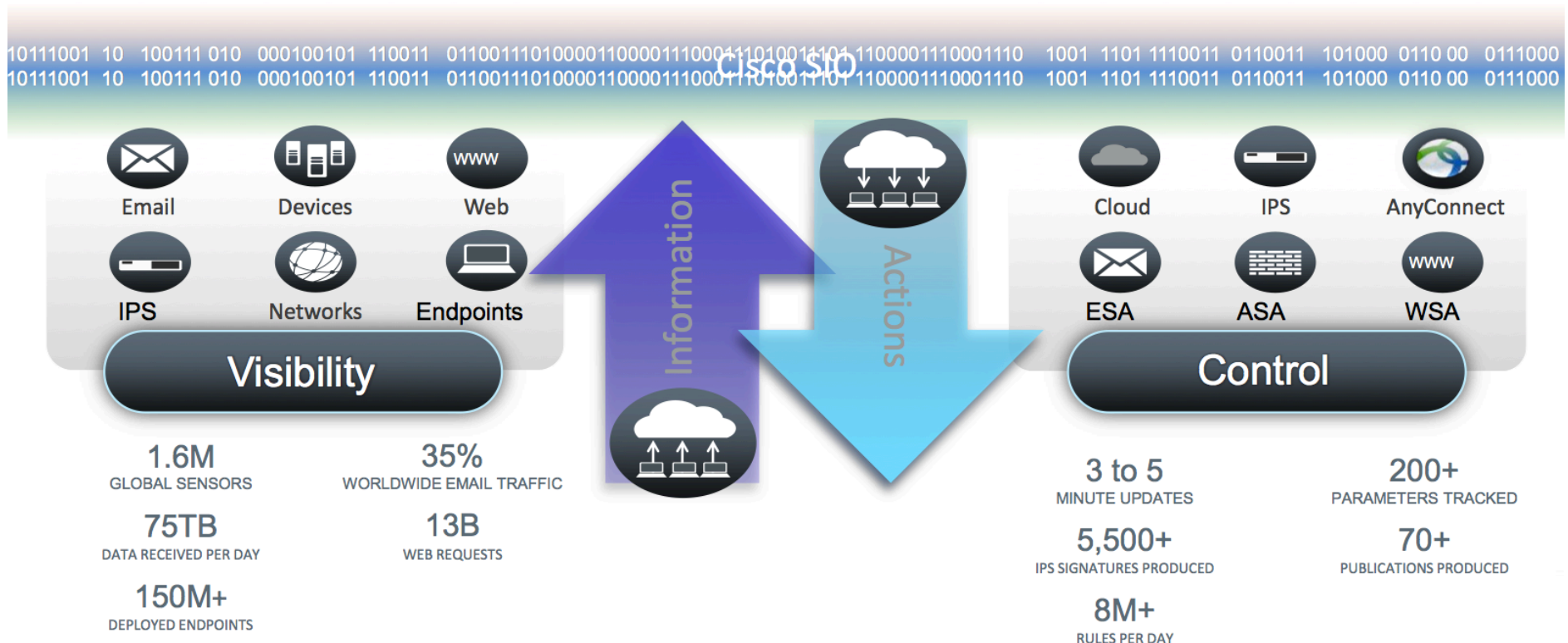
24x7x365
OPERATIONS

40+
LANGUAGES

\$100M+
SPENT IN DYNAMIC RESEARCH AND
DEVELOPMENT

600+
ENGINEERS, TECHNICIANS AND
RESEARCHERS

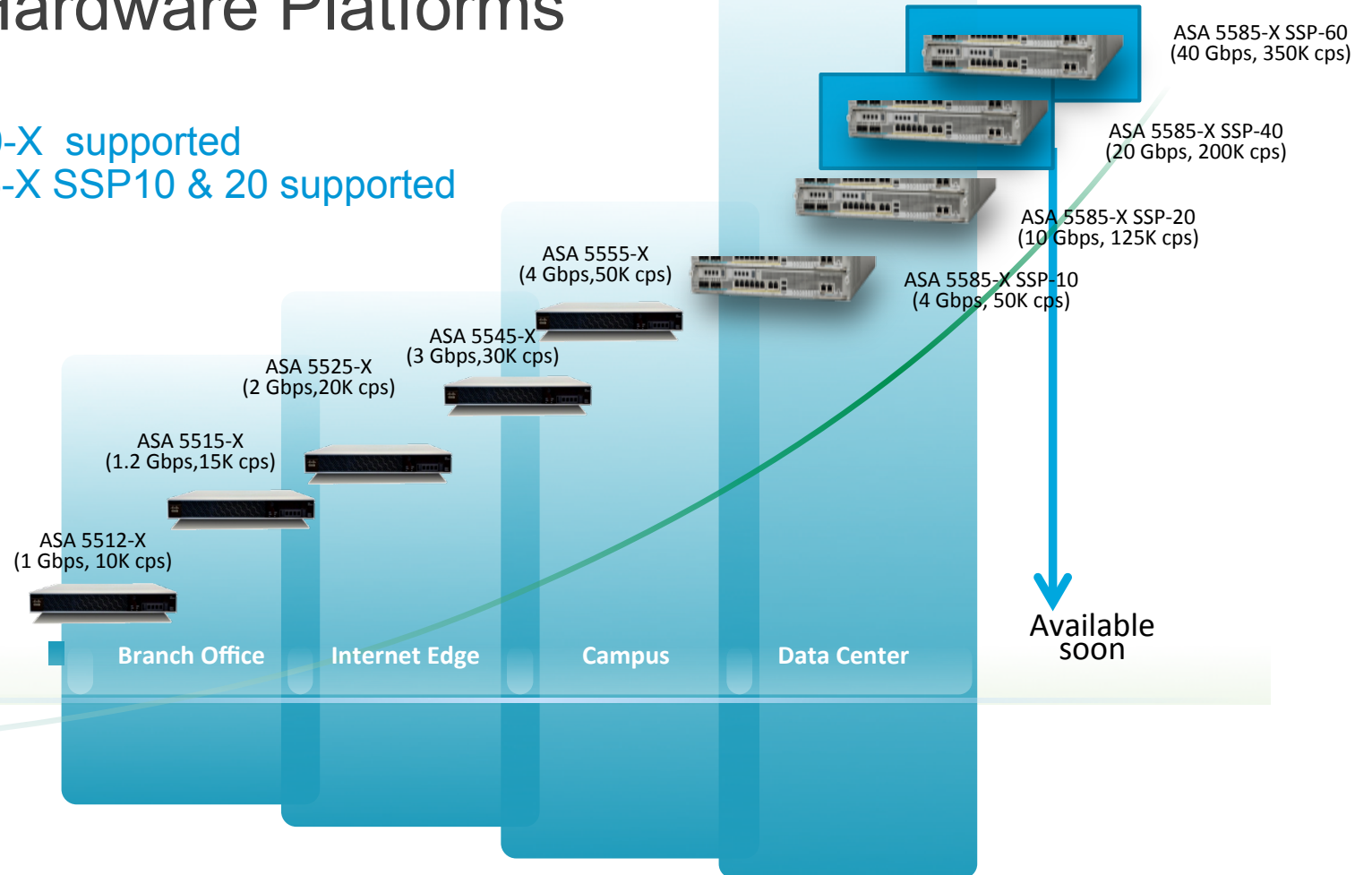
80+
PH.D.S, CCIE, CISSP, MSCE



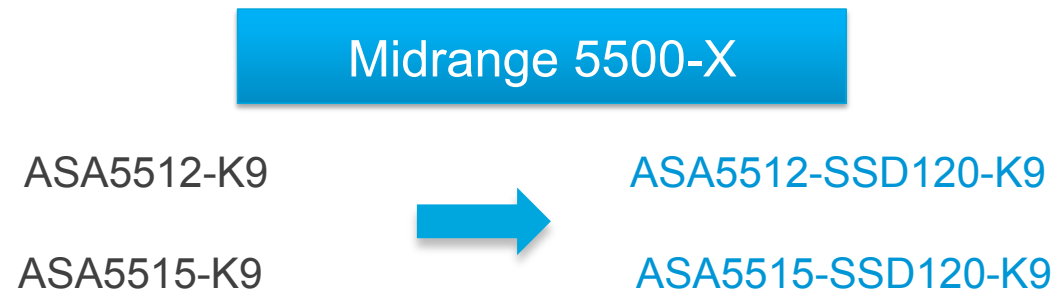
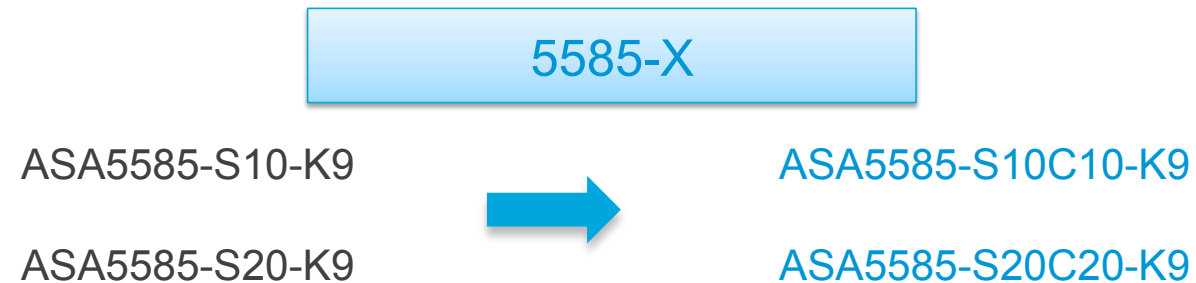
Supported Hardware Platforms

ASA 5500-X supported
ASA 5585-X SSP10 & 20 supported

Performance and Scalability



ASA CX Ready SKUs

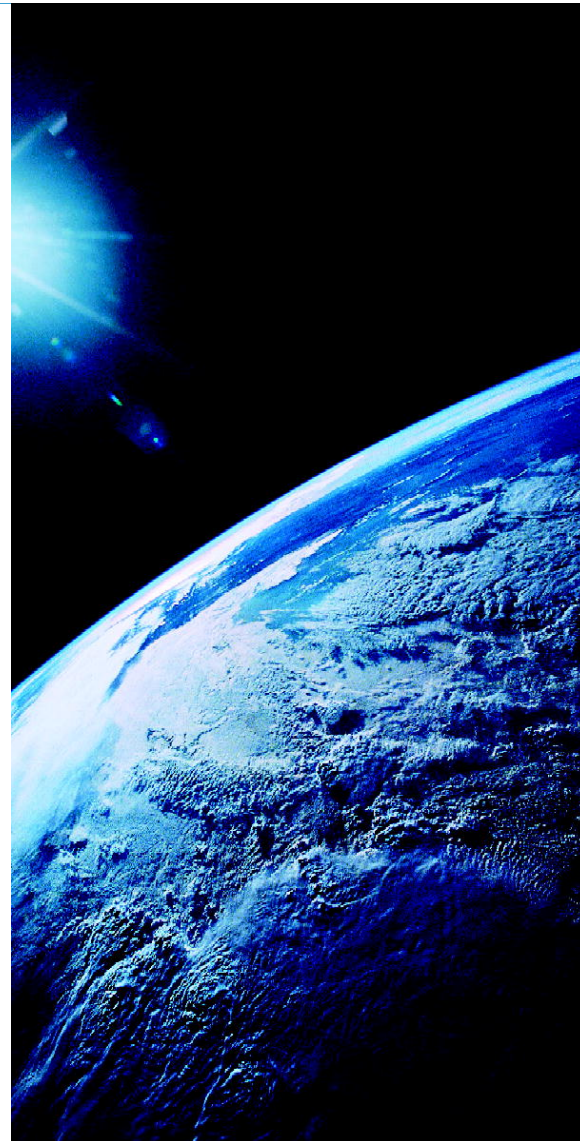


...

Plus, add subscription licenses and PRSM

Complex Policy for Remote Access

© 2013 Cisco and/or its affiliates. All rights reserved.



Cisco Connect

92

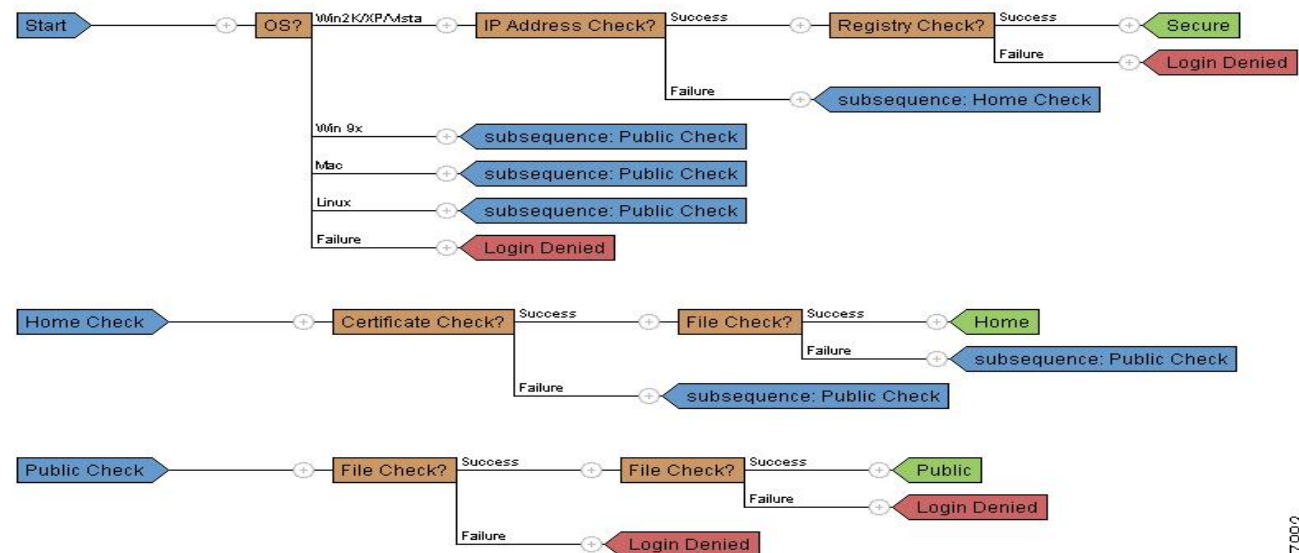
Hostscan

Posture checking for remote PC

Identify the OS, antivirus, antispyware, and firewall software installed on the host - > coming from CSD, but it is not the replacement

ASA: prelogin policy that evaluates :

- OS,
- IP address,
- registry entries,
- Local certificates
- filenames.

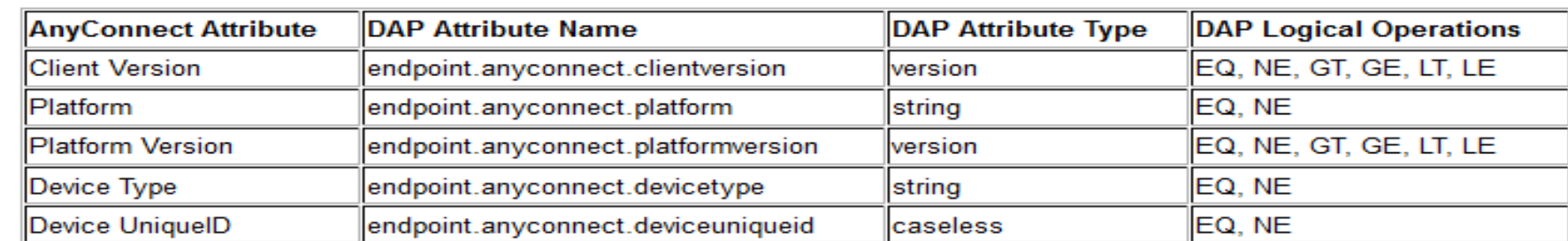


Configurable from ASDM

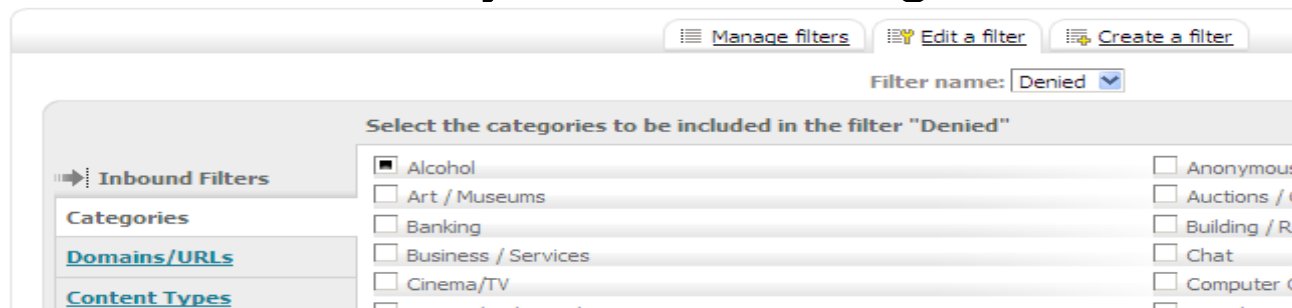
Additional access authorization capabilities based on endpoint

ASA 8.4.2+, 8.2.5+

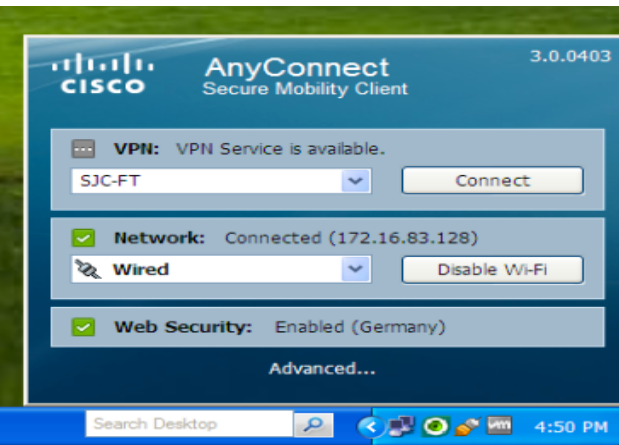
Android 2.4.x, Apple iOS 2.5.x



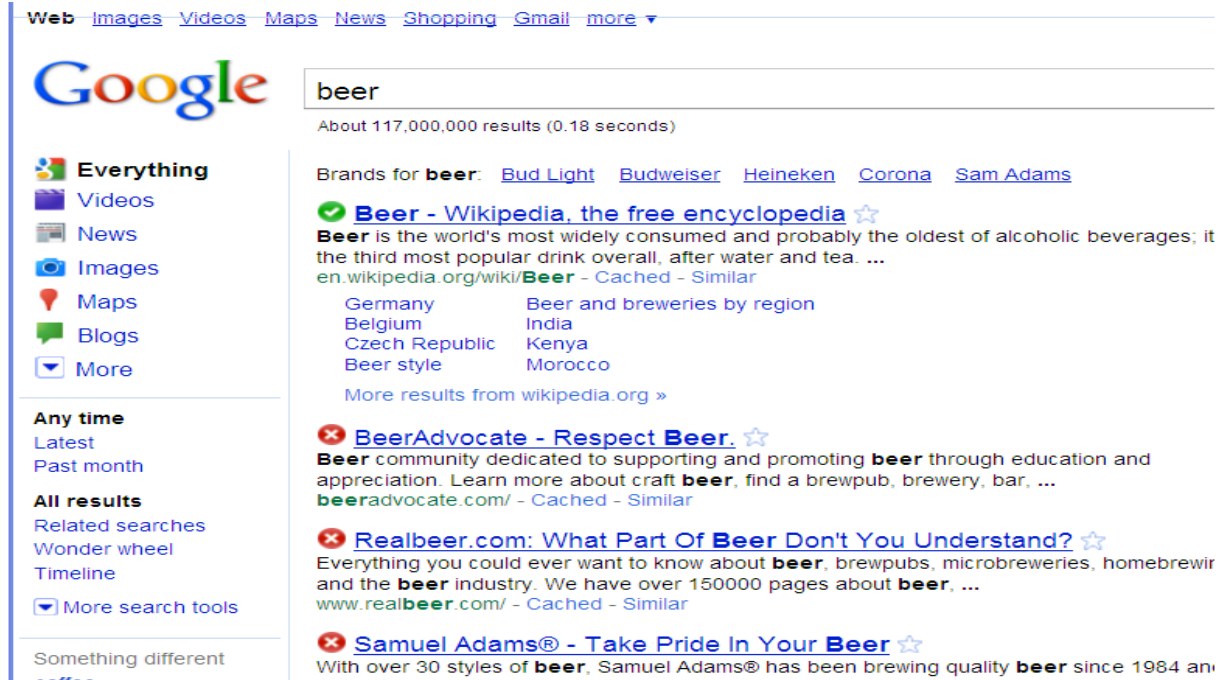
ScanSafe & AnyConnect Integration



The screenshot shows the ScanSafe filter configuration interface. At the top, there are buttons for 'Manage filters', 'Edit a filter', and 'Create a filter'. Below these, a dropdown menu shows 'Filter name: Denied'. The main section is titled 'Select the categories to be included in the filter "Denied"'. On the left, there is a sidebar with 'Inbound Filters' and 'Categories'. The 'Categories' section is expanded, showing a list of categories with checkboxes: Alcohol, Art / Museums, Banking, Business / Services, Cinema/TV, Anonymous, Auctions / C, Building / Re, Chat, Computer G, and Social Media. The 'Alcohol' checkbox is checked.



The screenshot shows the AnyConnect Secure Mobility Client interface. It features the Cisco logo and the version number 3.0.0403. The interface is divided into three main sections: VPN, Network, and Web Security. The VPN section shows 'VPN: VPN Service is available.' with a dropdown menu set to 'SJC-FT' and a 'Connect' button. The Network section shows 'Network: Connected (172.16.83.128)' with a 'Wired' dropdown menu and a 'Disable Wi-Fi' button. The Web Security section shows 'Web Security: Enabled (Germany)' and an 'Advanced...' link. At the bottom, there is a 'Search Desktop' bar and a system clock showing '4:50 PM'.

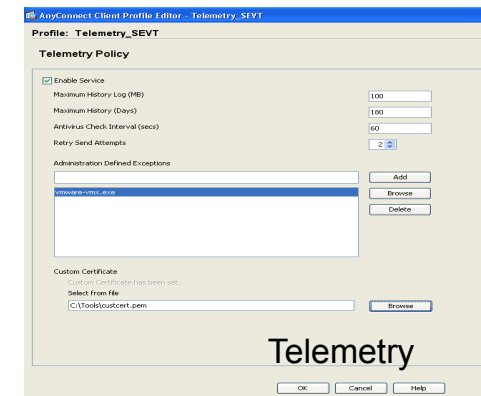
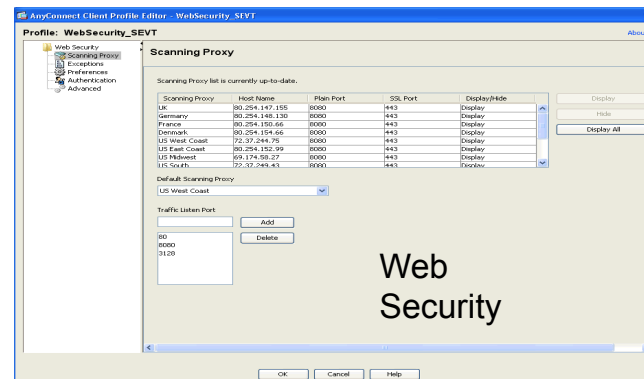
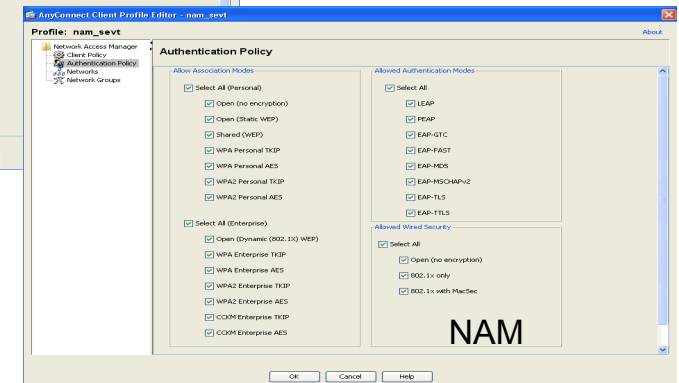
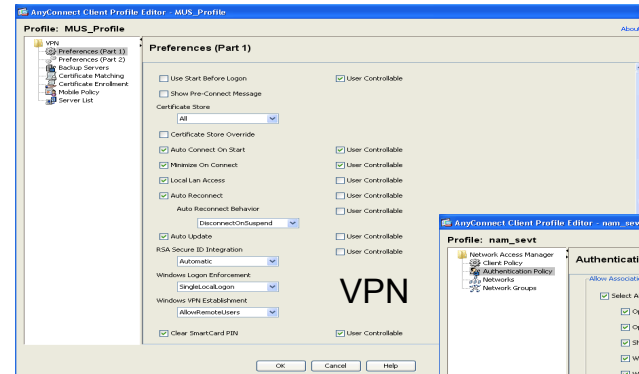


The screenshot shows a Google search results page for the query 'beer'. The search bar at the top contains the word 'beer'. Below the search bar, it says 'About 117,000,000 results (0.18 seconds)'. The results are categorized into 'Brands for beer' (Bud Light, Budweiser, Heineken, Corona, Sam Adams), 'Beer - Wikipedia, the free encyclopedia' (with a star icon), 'BeerAdvocate - Respect Beer.' (with a star icon), 'Realbeer.com: What Part Of Beer Don't You Understand?' (with a star icon), and 'Samuel Adams® - Take Pride In Your Beer' (with a star icon). The Wikipedia entry is expanded, showing the text: 'Beer is the world's most widely consumed and probably the oldest of alcoholic beverages; it the third most popular drink overall, after water and tea. ... en.wikipedia.org/wiki/Beer - Cached - Similar'. The BeerAdvocate entry is also expanded, showing the text: 'Beer community dedicated to supporting and promoting beer through education and appreciation. Learn more about craft beer, find a brewpub, brewery, bar, ... beeradvocate.com/ - Cached - Similar'. The Realbeer.com entry is expanded, showing the text: 'Everything you could ever want to know about beer, brewpubs, microbreweries, homebrewir and the beer industry. We have over 150000 pages about beer, ... www.realbeer.com/ - Cached - Similar'. The Samuel Adams entry is expanded, showing the text: 'With over 30 styles of beer, Samuel Adams® has been brewing quality beer since 1984 an...

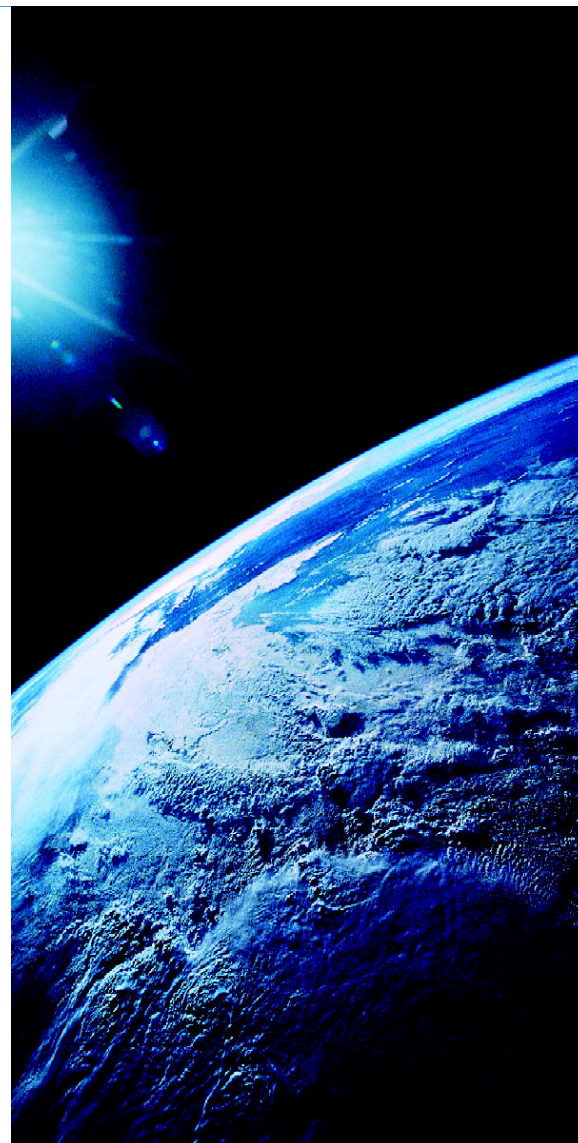
AnyConnect

Deployment – Profile Editors

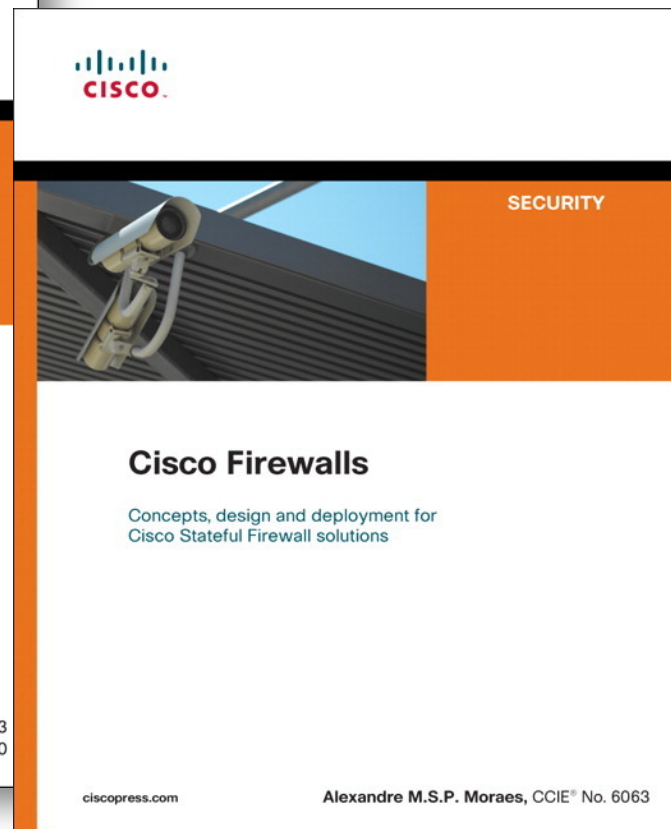
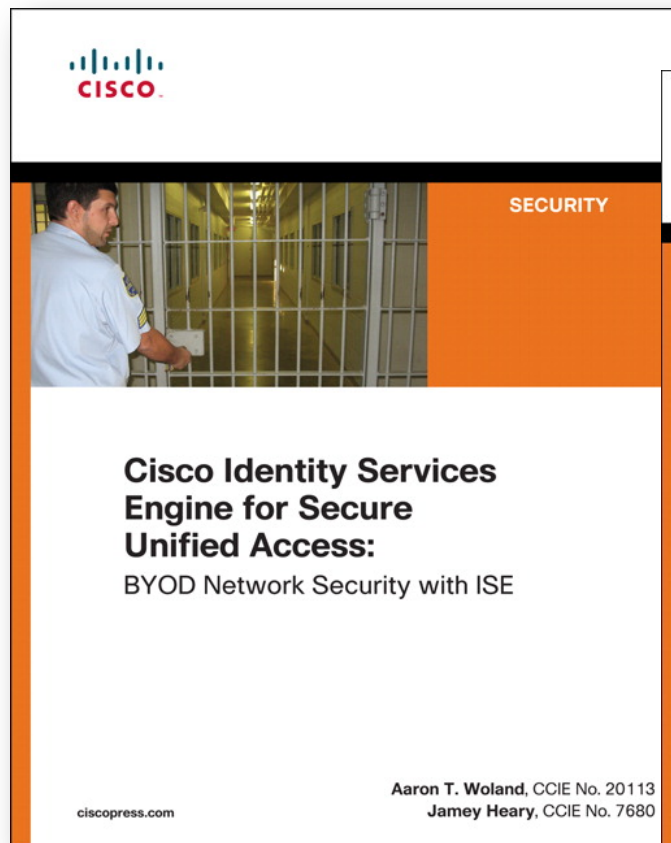
- Profile Editors integrated in ASDM
- Profiles with policy rules distributed centrally
- Group Policy with AD/LDAP or RADIUS



Odkazy



Recommended Reading



Recommended Reading



- Network Complexity - Michael H. Behringer: Classifying Network Complexity; slides; ACM ReArch'09 workshop; 2009 <http://networkcomplexity.org/wiki/index.php?title=References>
- Cisco TrustSec 2.1 Design and Implementation Guide
<http://www.cisco.com/go/trustsec/>
- Cisco Wireless LAN Security -
<http://www.ciscopress.com/bookstore/product.asp?isbn=1587051540>
- Managing Cisco Network Security -
<http://www.ciscopress.com/bookstore/product.asp?isbn=1578701031>
- Cisco Firewalls –<http://www.ciscopress.com/bookstore/product.asp?isbn=1587141094>
- Cisco LAN Switch Security: What Hackers Know About Your Switches -
<http://www.ciscopress.com/bookstore/product.asp?isbn=1587052563>

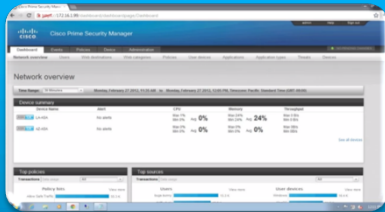
Where To Find Out More

Whitepapers

www.cisco.com/go/ibns

Deployment Scenario Design Guide	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_C11-530469.html
Deployment Scenario Config Guide	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/Whitepaper_c11-532065.html
IEEE 802.1X Deep Dive	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/guide_c07-627531.html
MAB Deep Dive	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/config_guide_c17-663759.html
Web Auth Deep Dive	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/app_note_c27-577494.html http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/app_note_c27-577490.html
Flex Auth App Note	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html
IP Telephony Deep Dive	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/config_guide_c17-605524.html
MACSec Deep Dive	http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/deploy_guide_c17-663760.html

ASA-CX Demo



Cisco ASA CX Context-Aware Security

<http://www.youtube.com/watch?v=4yYIJnJhTVg>



TechWiseTV 115: Firewall Reinvention with the New ASA CX

http://www.youtube.com/watch?v=JG12_pidHr8



Cisco ASA CX Context-Aware - Video Data Sheet

<http://www.youtube.com/watch?v=rTAKew41RB8>

Otázky a odpovědi

Zodpovíme též v “Ptali jste se” v sále LEO v 17:45 – 18:30

e-mail: connect-cz@cisco.com

Prosíme, ohodnotte
tuto přednášku.