Bezpečný přístup na základě identity

Jiří Tesař

CSE Security, CCIE #14558

jitesar@cisco.com

Program

- Problematika přístupu do sítě
- Bezpečnost postavená na identitě uživatele
- Jak na BYODy ?
- Nastavení mobilních platforem a řízení přístupu do sítě
- Vzdálené VPN přístupy
- Kontextová bezpečnost

Problematika bezpečných přístupů do sítě

Network Admission Control

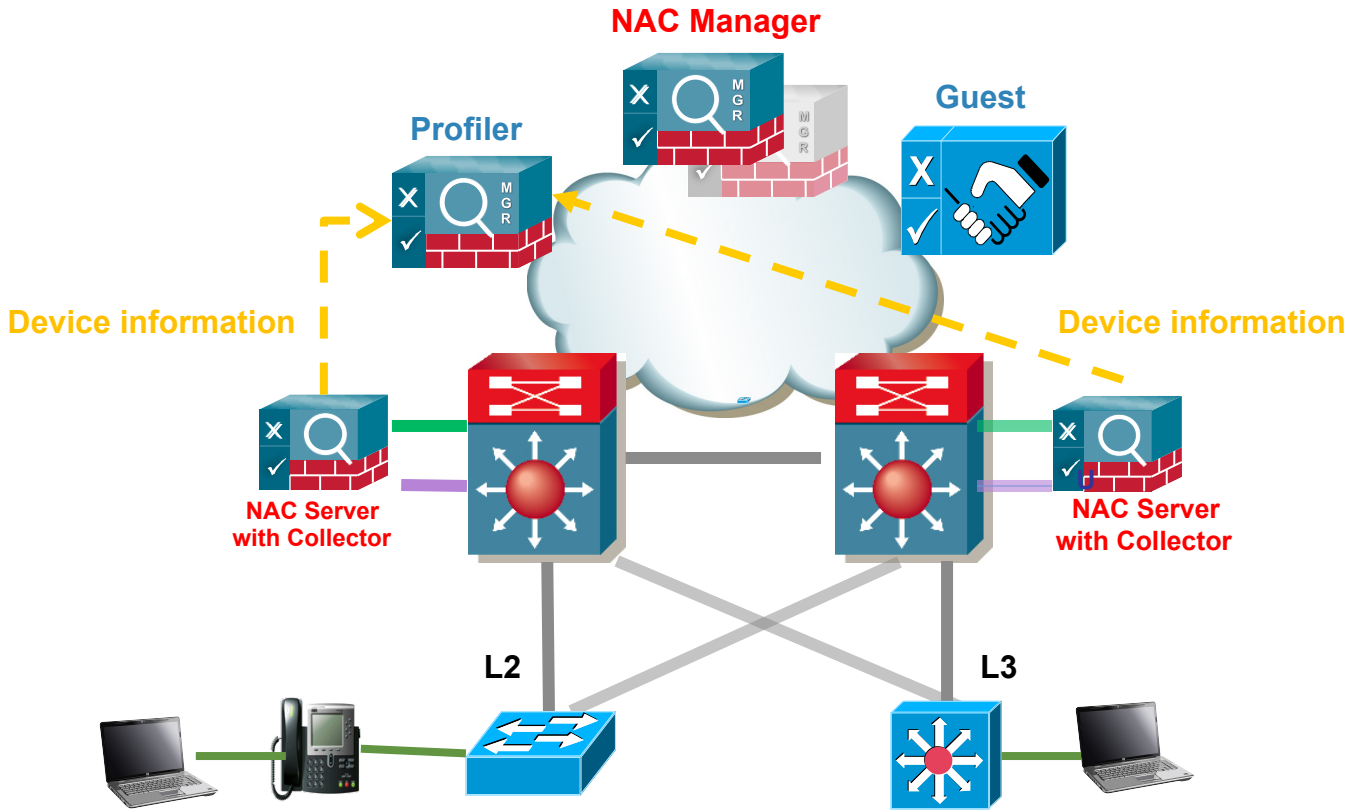
AUTHENTICATE
users and devices to the network

Posture and Remediate
the device for policy compliance

Differentiated Access
role based access control

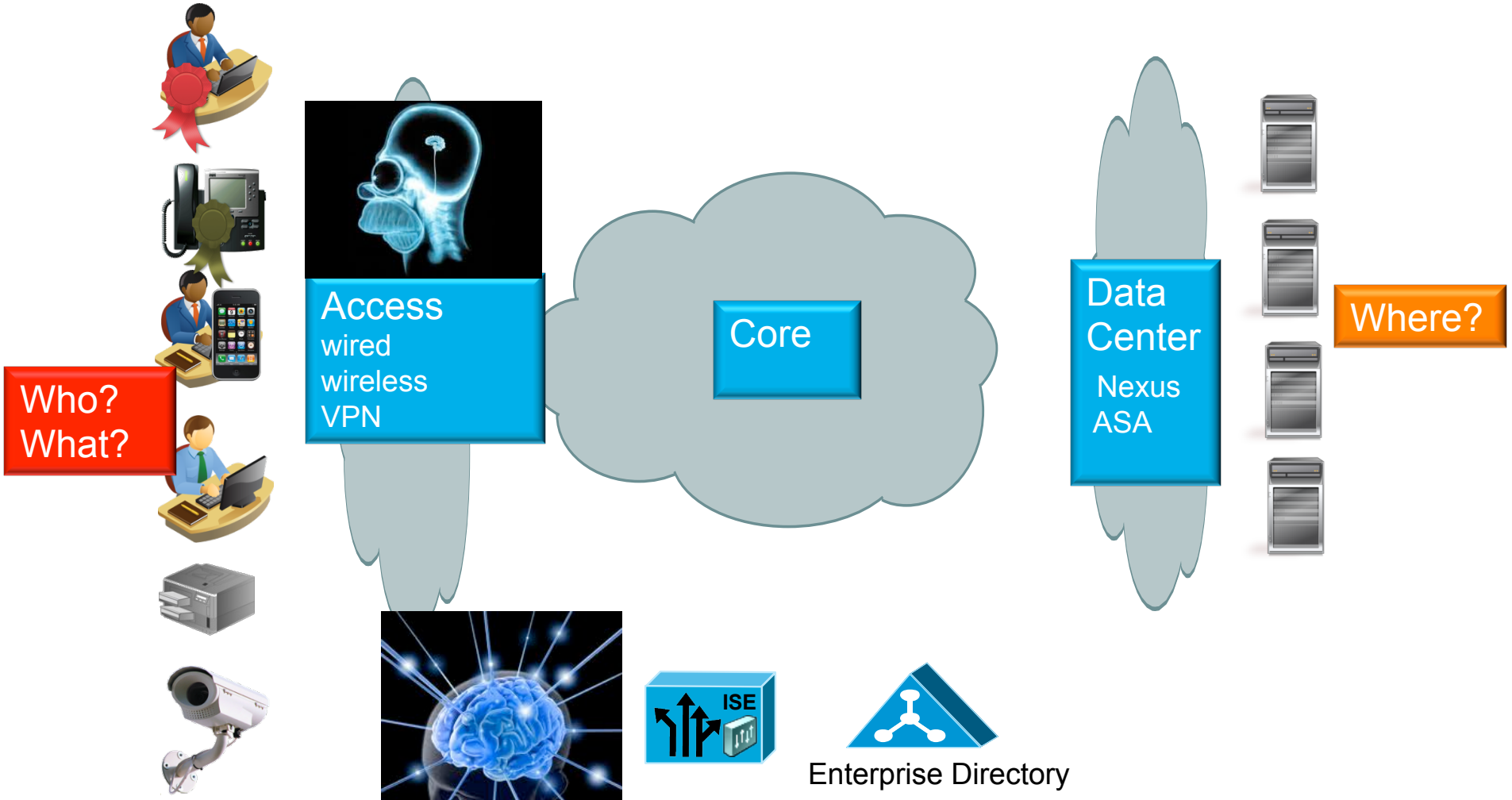
Audit and Report
who is on my network

a) NAC – Centralized Deployment

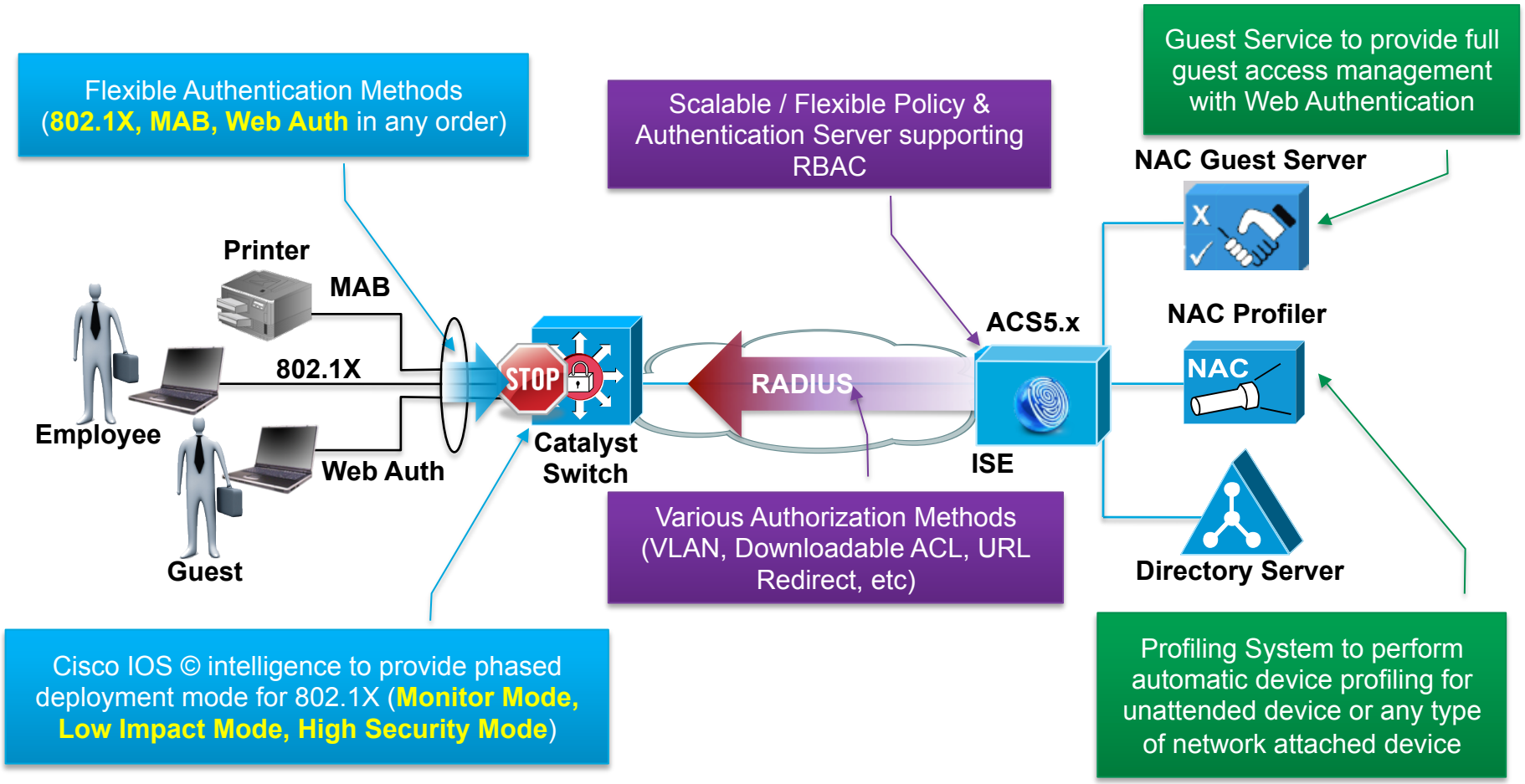


FEATURES	BENEFITS
▪ Servers deployed in Distribution Layer ▪ Supports multiple access switches ▪ Layer 2 and Layer 3 Access support to Nac Servers	• Scalable solution to support up to 3,500 users per NAC server • Supports multiple access switches

b) Adding Intelligence to the Network

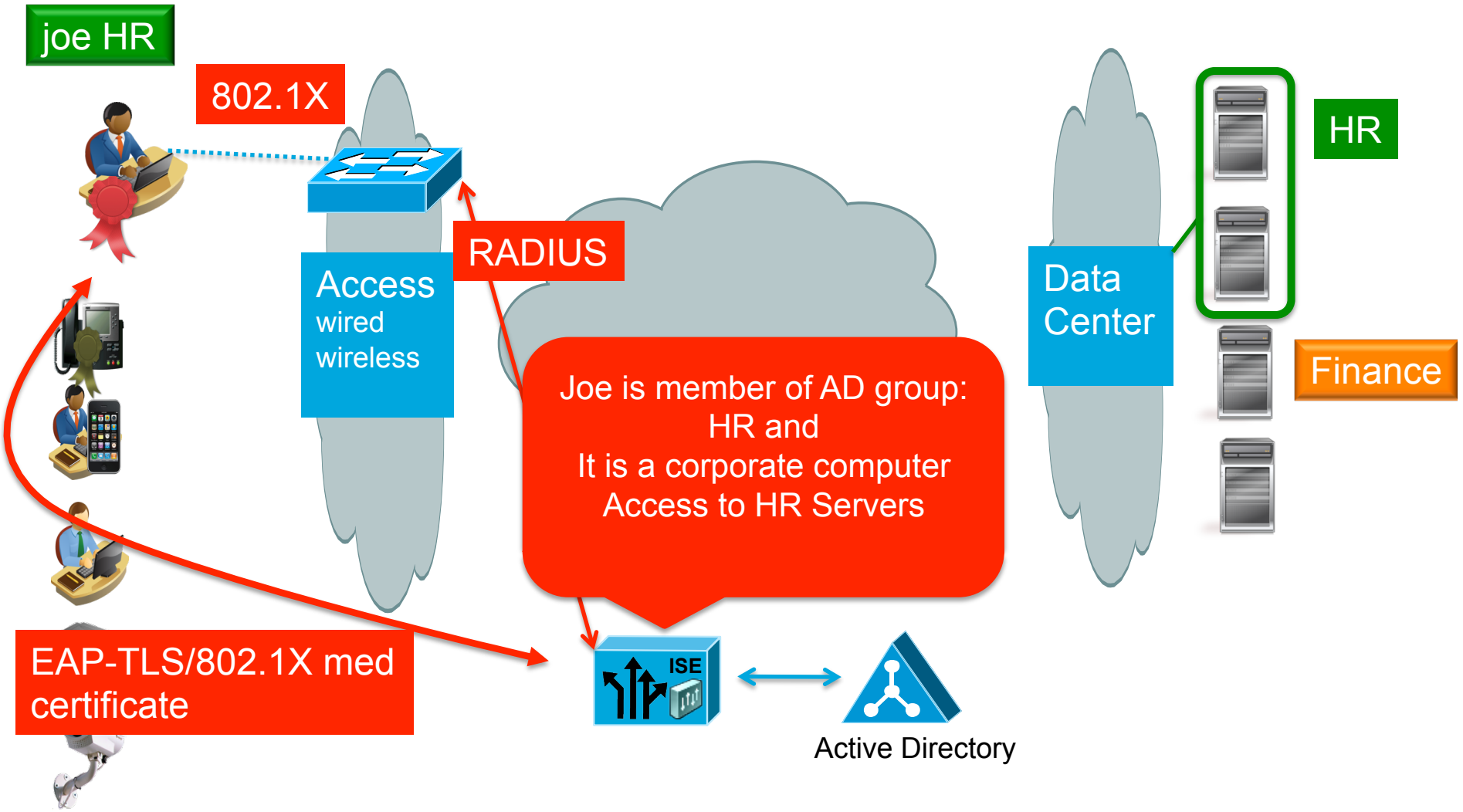


Identity Solution Specifics

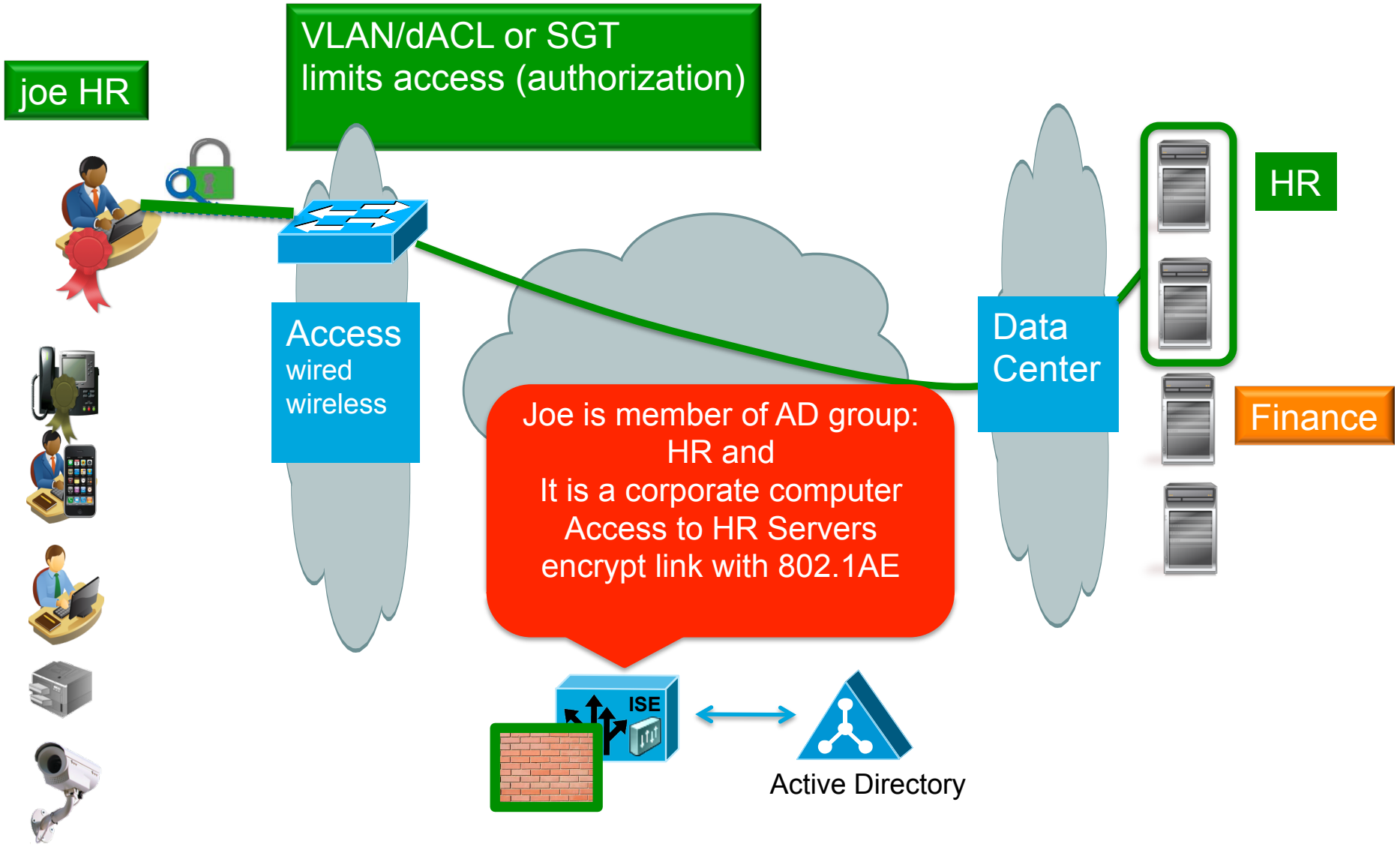


Základní řízení přístupu podle identity

Mapping user's group to security role



Mapping user's group to security role



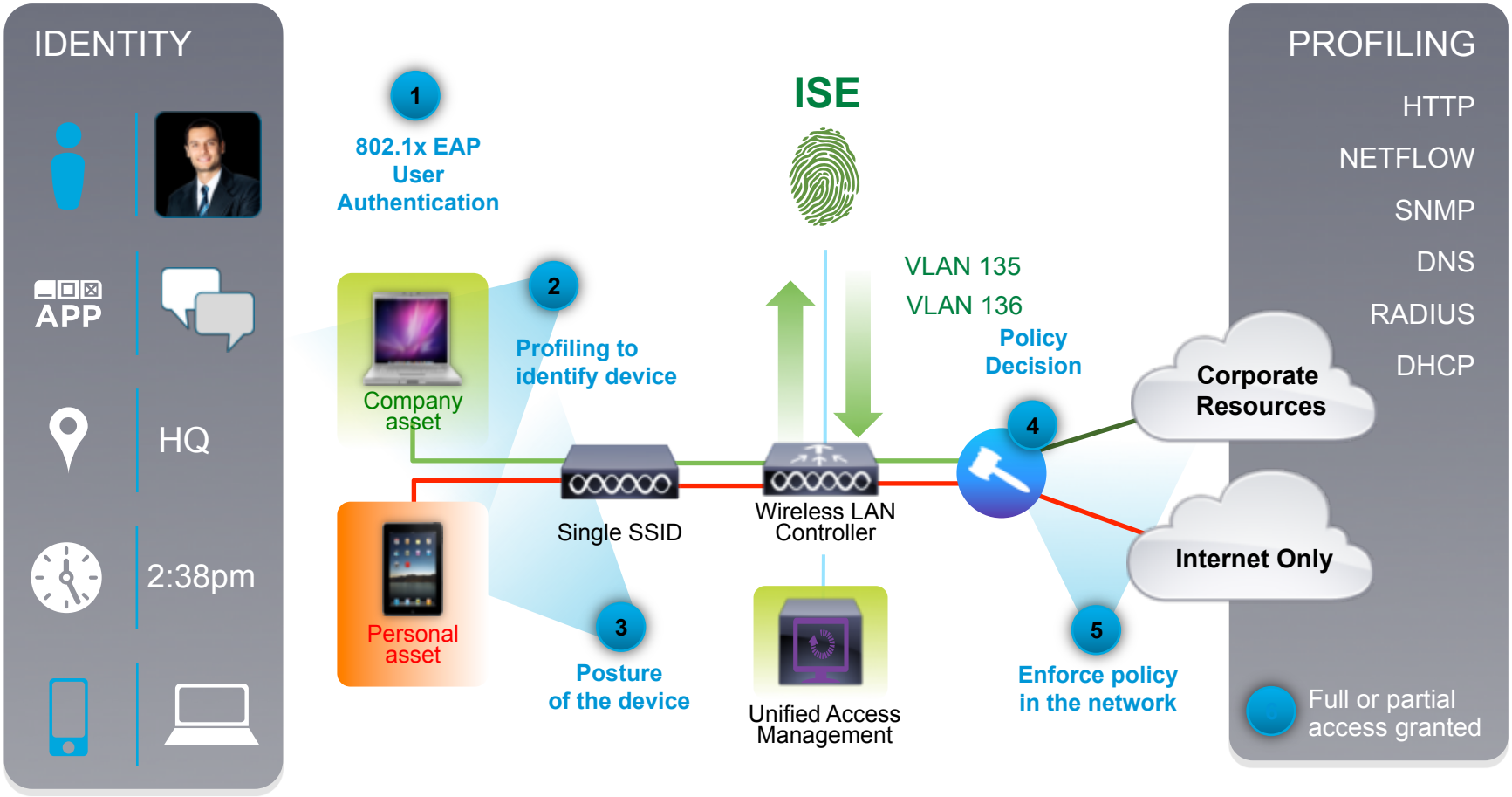

BYOD

Example of BYOD

Enforcing Different Policies for Corporate and Personal Devices

Identity and Policy

Unified Infrastructure

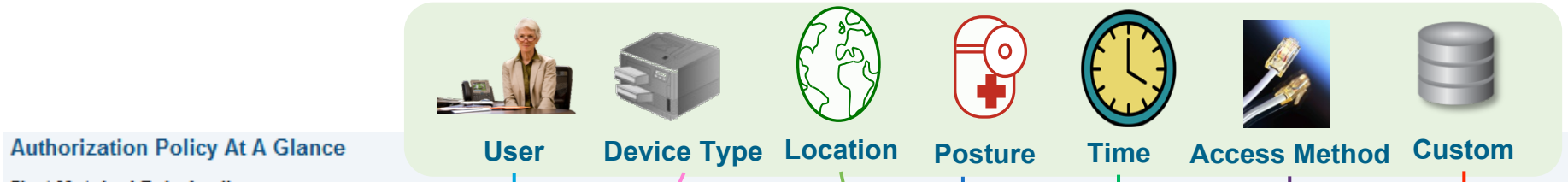


ISE: Powerful, Flexible Solution

No other solution brings all the context together

Identity and Policy

Unified Infrastructure



Authorization Policy At A Glance

First Matched Rule Applies

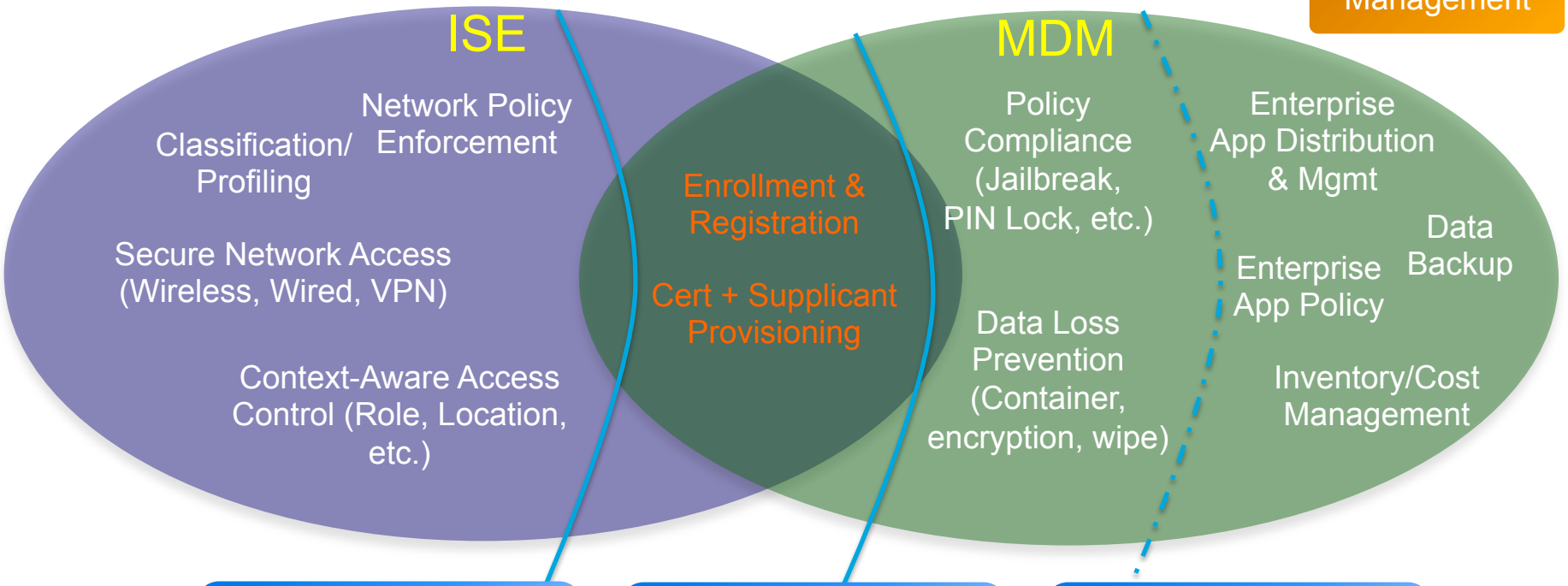
Standard

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 Nam 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:badPwdCour 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	Contrator_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

Evolving Roles of ISE and MDMs

Identity and Policy

Management



ISE 1.0 & 1.1

Native ISE functionality
- Profiling
- Authentication
- Policy Enforcement
- etc.

ISE 1.1.1 (Jun '12)

Native ISE functionality
- Enrollment/ Registration
- Self-Enroll Portal
- Certificate Enrollment
- Blacklisting

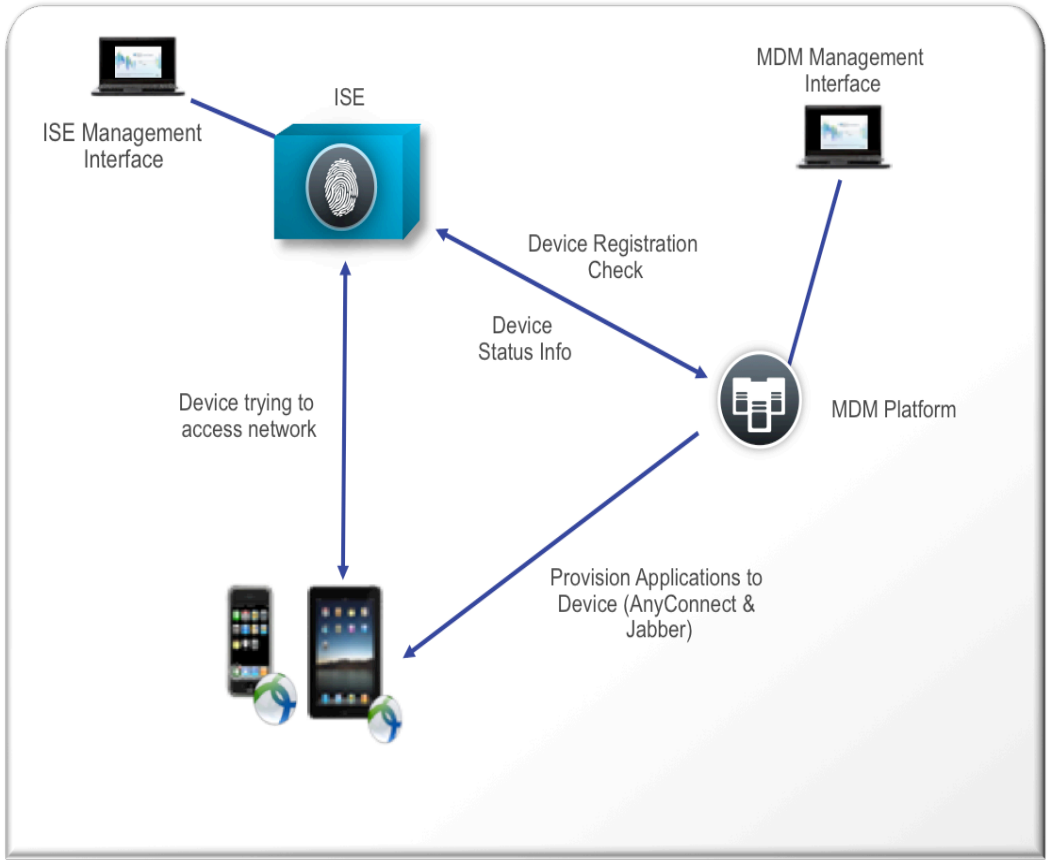
ISE 1.2 (May '13)

ISE – MDM API
- Additional device data
- Policy compliance
- Data wipe

ISE 1.2 & MDM Integration - Scope

High Level Goals of Integration

- 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 to Initiate Device Action from ISE
  - Device stolen -> need to wipe data on client



airwatch™ MobileIron® Good ZENPRISE

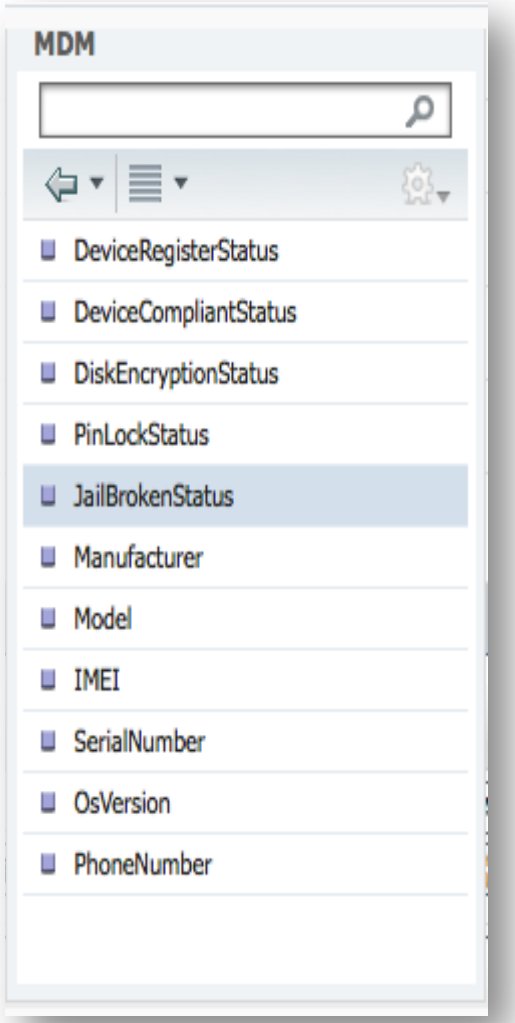
Attributes from MDM

- With the API, we can query on:

  General Compliant or ! Compliant (Macro level) -or-

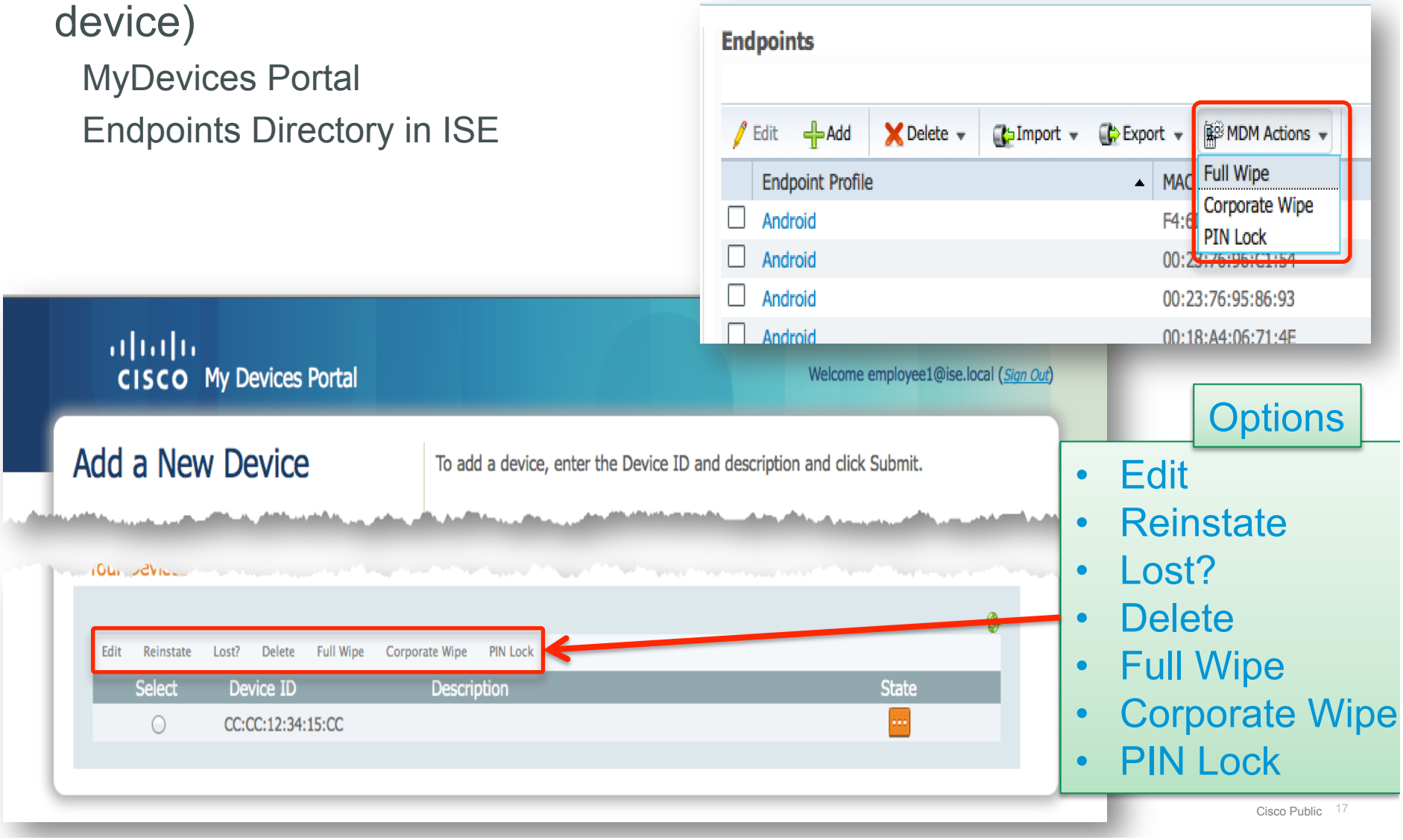
  - Disk encryption is one
  - Pin lock
  - Jail broken

- Bulk re-check against the MDM every 4 hours.
  - But we are not using the cached data in the AuthZ
  - If result of Bulk Re-check shows that a device is no longer compliant – we will send a CoA to terminate session.
  - Works same with all 4 vendors.



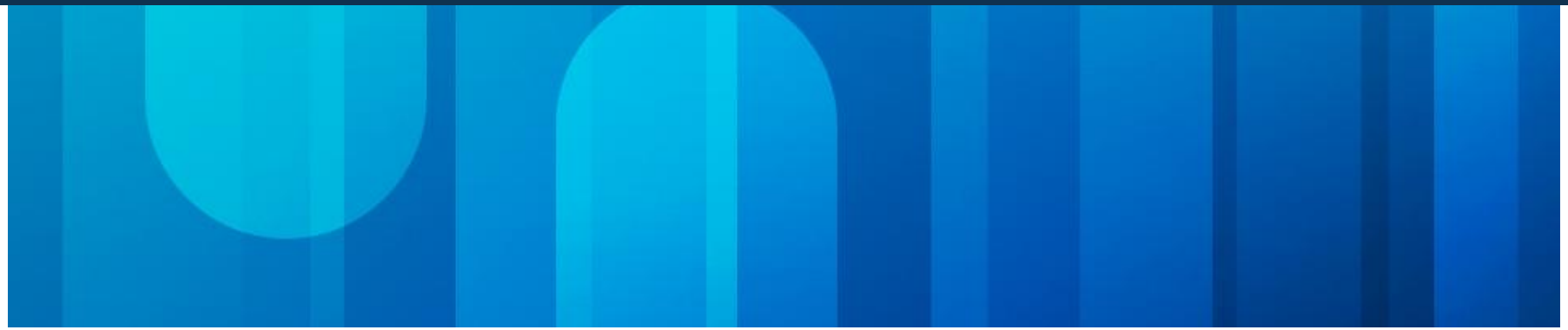
MDM Integration

- Ability for administrator and user in ISE to issue remote actions on the device through the MDM server (eg: remote wiping the device)
  - MyDevices Portal
  - Endpoints Directory in ISE




Provisioning

Onboarding & Provisioning Demo



© 2011 Cisco and/or its affiliates. All rights reserved.

VPN Access

AnyConnect

Mobile Host Scan ("MDM Lite")

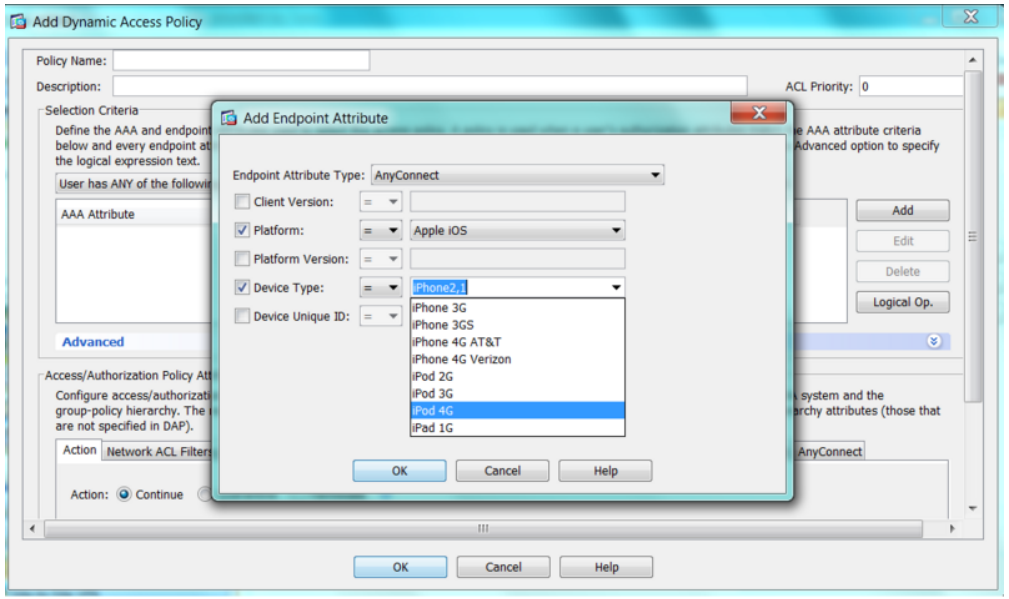
Additional access authorization capabilities based on endpoint

Premium license requirement

ASA 8.4.2+, 8.2.5+

Android 2.4.x, Apple iOS 2.5.x

Desktop post 3.1

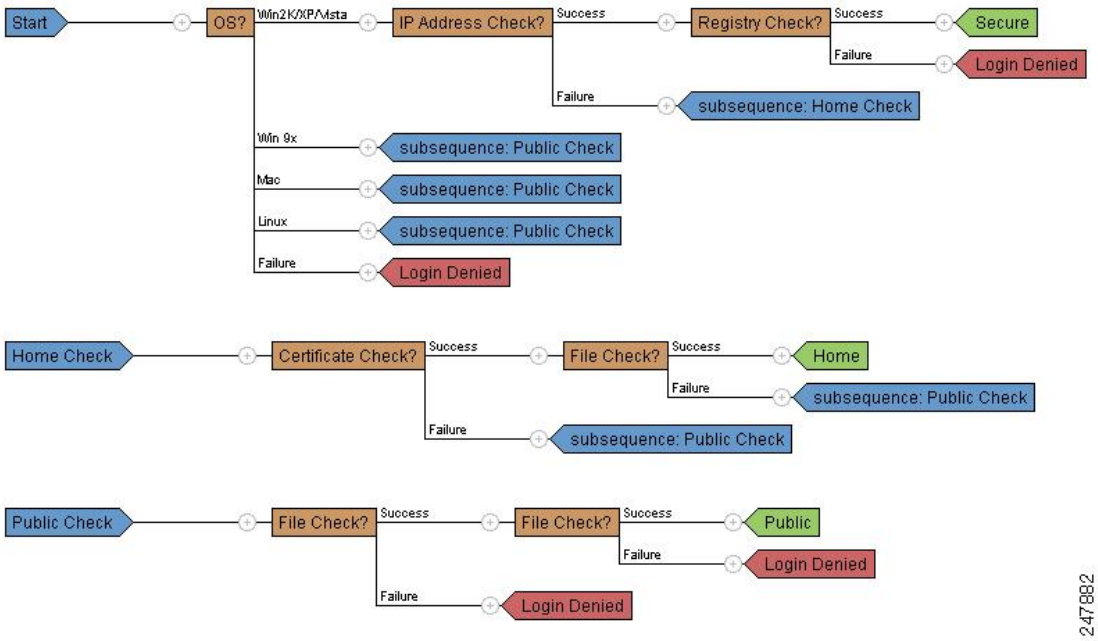


AnyConnect Attribute	DAP Attribute Name	DAP Attribute Type	DAP Logical Operations
Client Version	endpoint.anyconnect.clientversion	version	EQ, NE, GT, GE, LT, LE
Platform	endpoint.anyconnect.platform	string	EQ, NE
Platform Version	endpoint.anyconnect.platformversion	version	EQ, NE, GT, GE, LT, LE
Device Type	endpoint.anyconnect.devicetype	string	EQ, NE
Device UniqueID	endpoint.anyconnect.deviceuniqueid	caseless	EQ, NE

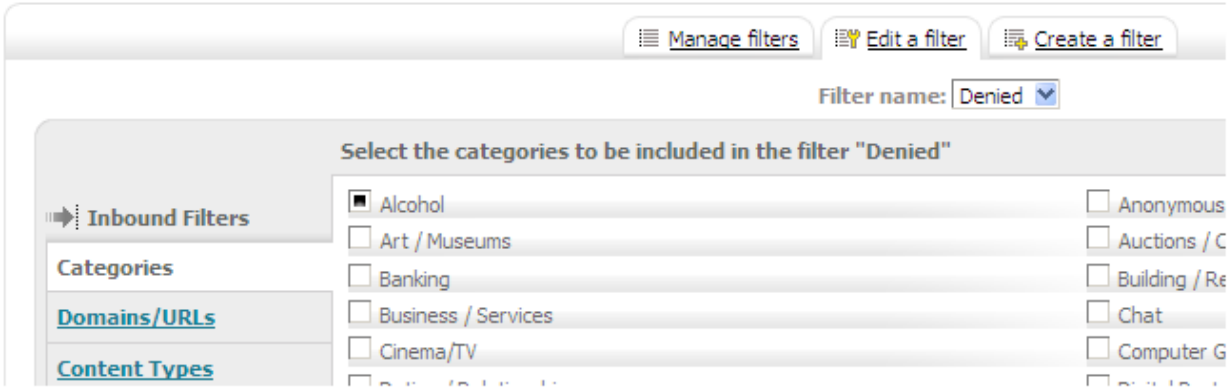
Hostscan

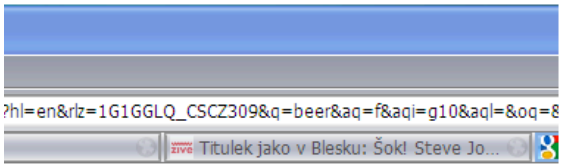
Yes, we can check health of client's PC

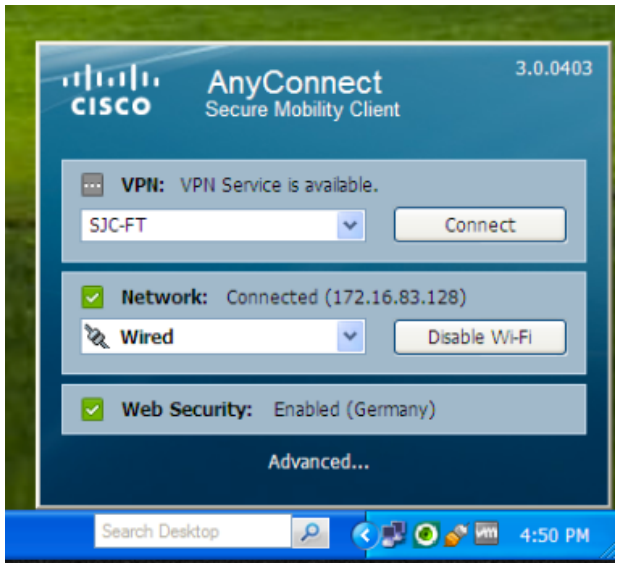
- Identify the OS, antivirus, antispyware, and firewall software installed on the host - > coming from CSD, but it is not the replacement
- ASA: prelogin policy that evaluates :
  - OS,
  - IP address,
  - registry entries,
  - Local certificates
  - filenames.
- Configurable from ASDM

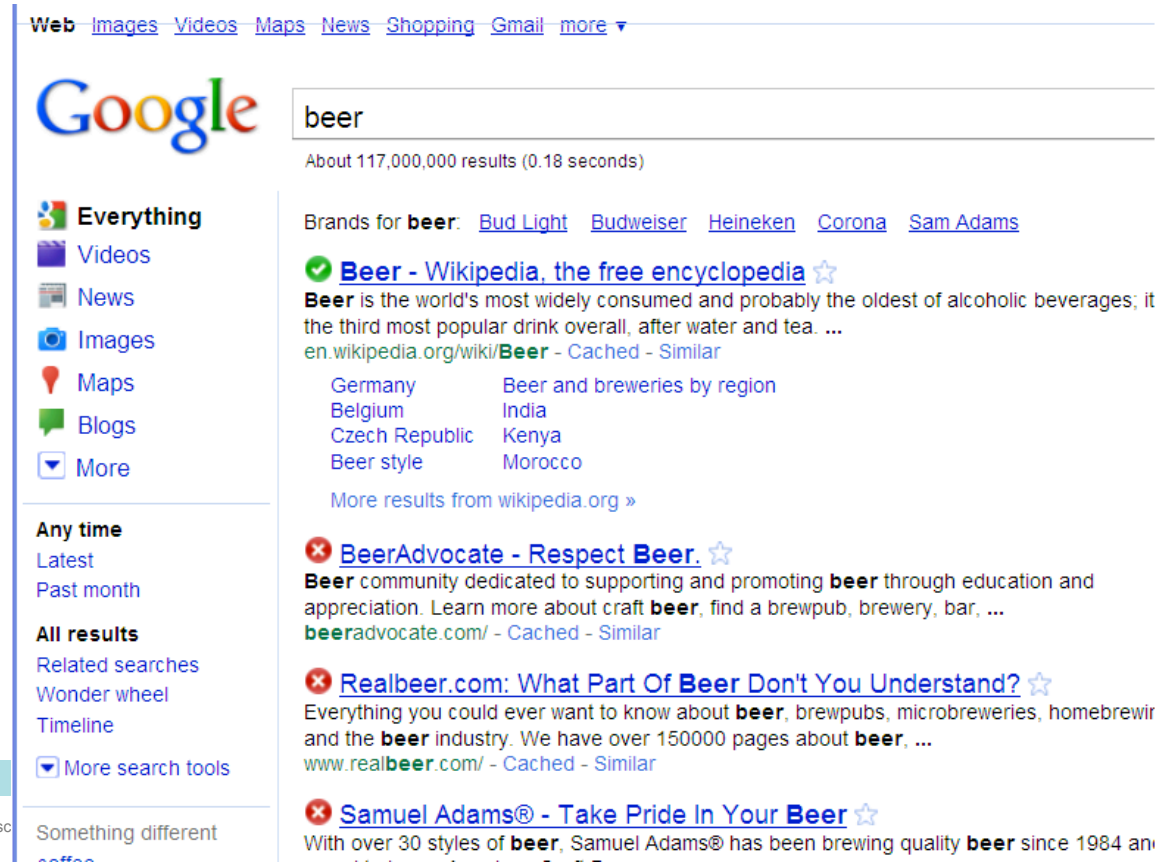


ScanSafe & AnyConnect Integration



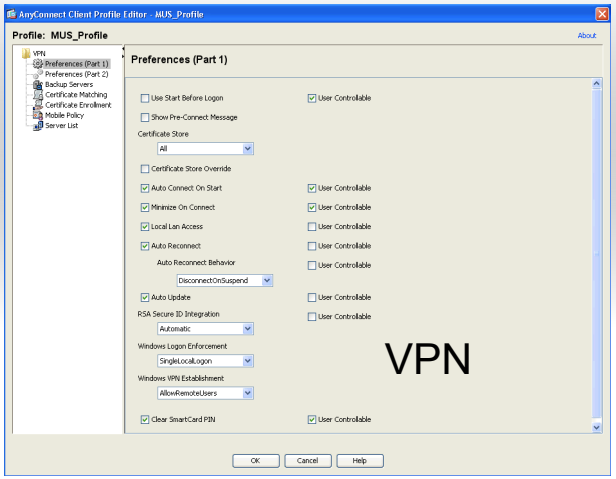


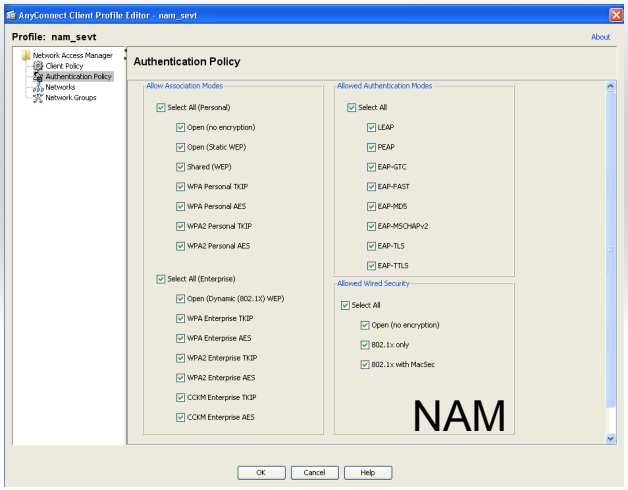


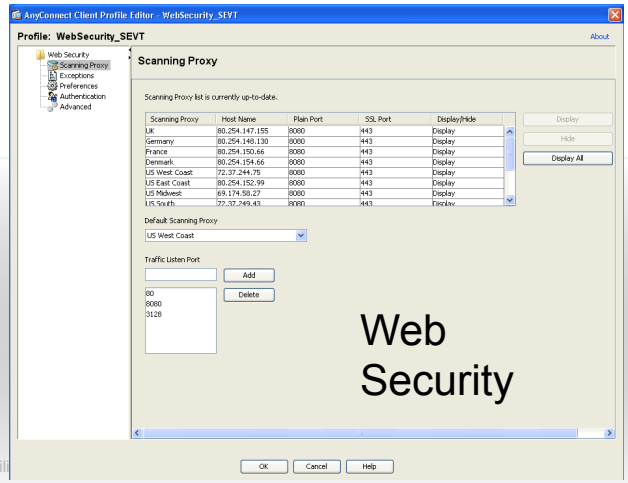


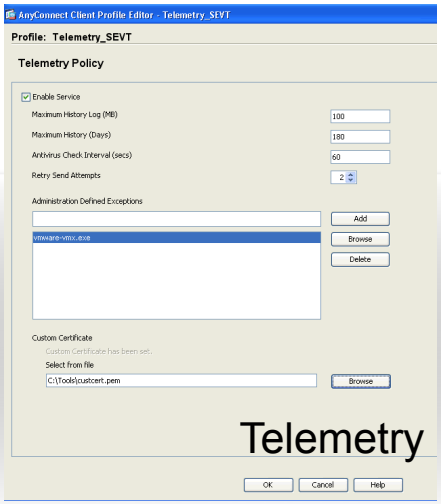
AnyConnect 3.0
Deployment – Profile Editors

- Profile Editors integrated in ASDM 6.4







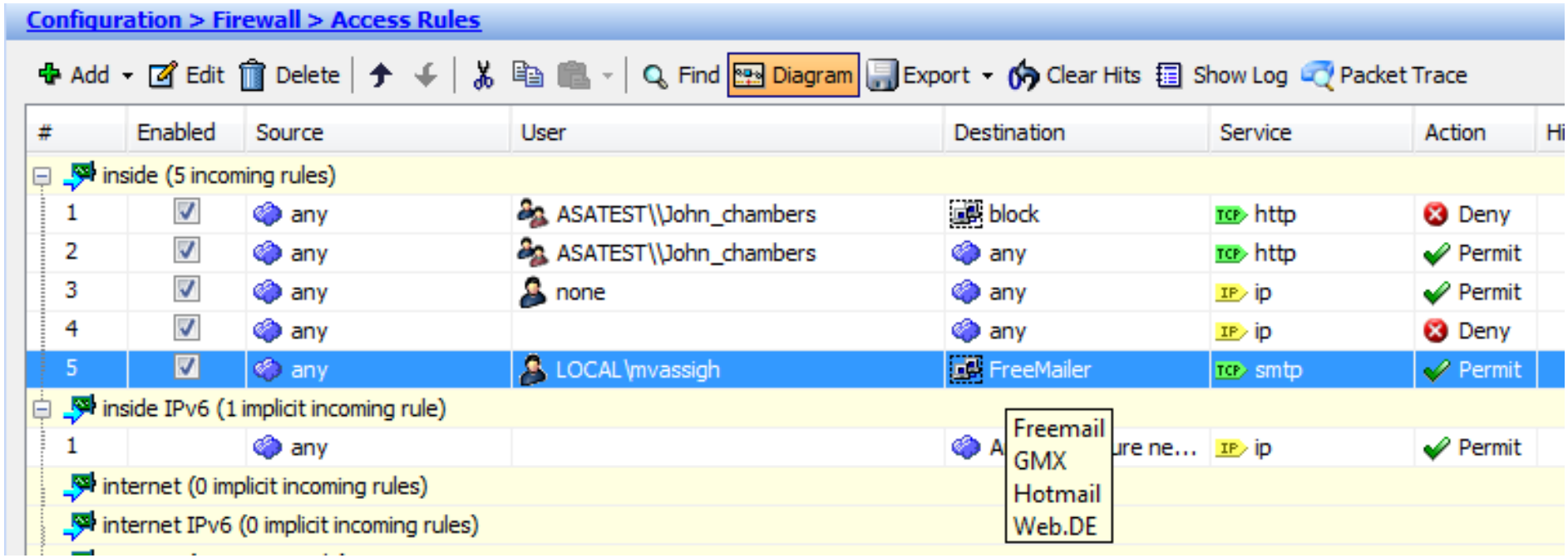


NG Encryption with ASA 9.0

- AES-GCM/GMAC support (128-, 192-, and 256-bit keys)
  - IKEv2 payload encryption and authentication
  - ESP packet encryption and authentication
- SHA-2 (Phase 3a) support (256-, 384-, and 512-bit hashes)
  - ESP packet authentication
- ECDH support (groups 19, 20, and 21)
  - IKEv2 key exchange
  - IKEv2 PFS
- ECDSA support (256-, 384-, and 521-bit elliptic curves)
  - IKEv2 user authentication
  - PKI certificate enrollment
  - PKI certificate generation and verification

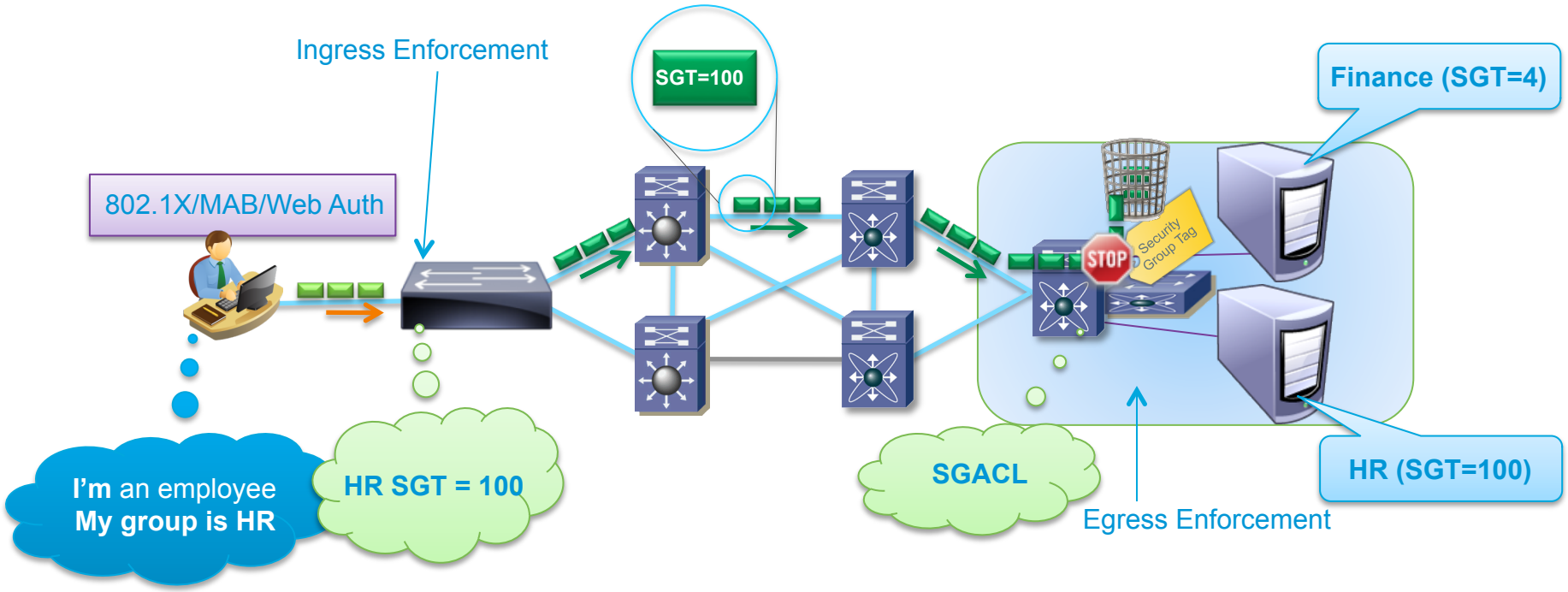
Identity Based Security @Infrastructure

Identity Based Security on FW



Security Group Based Access Control

- SGA allows customers:
  - Provides topology independent policy
  - Flexible and scalable policy based on user role
  - Centralized Policy Management for Dynamic policy provisioning
  - Egress filtering results to reduce TCAM impact



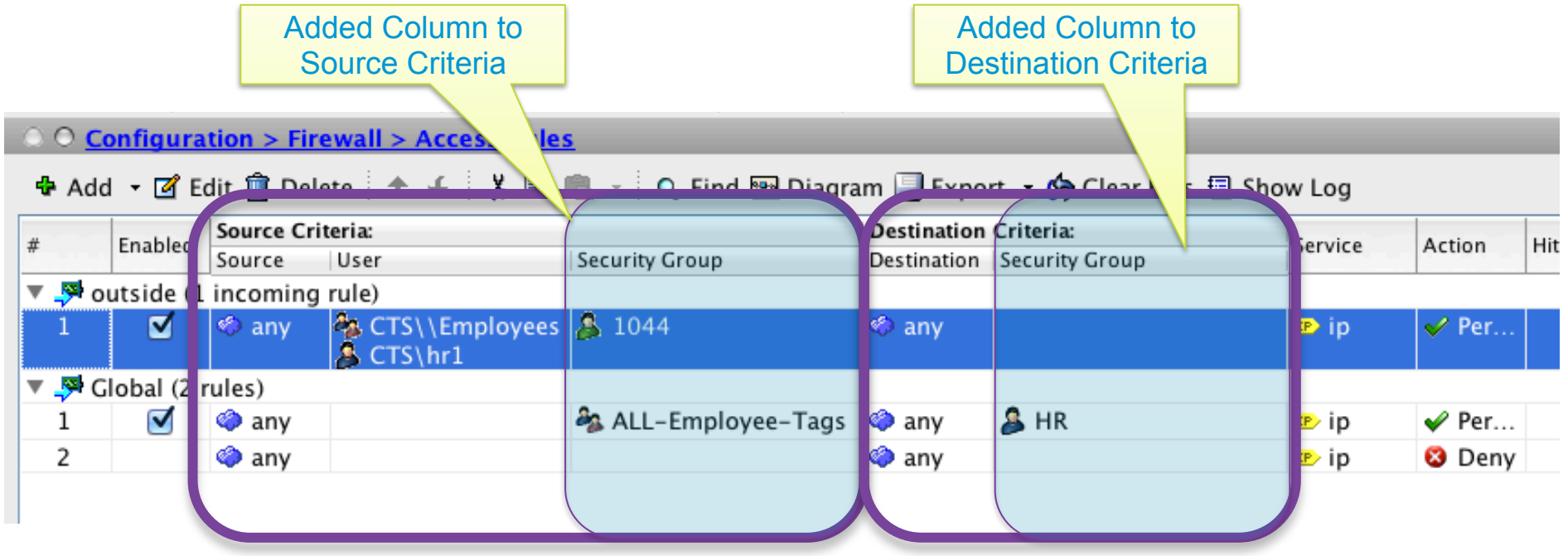
Secure Group Access

Topology Independent Access Control

- 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 below).

SGT	Public	Private
Staff	Permit	Permit
Guest	Permit	Deny

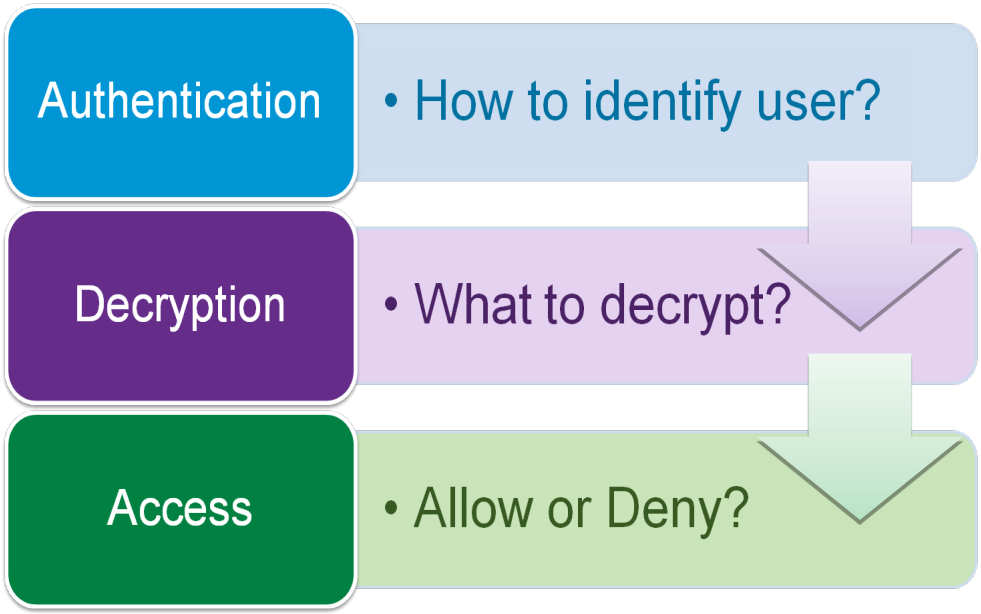
Using the SGT's in the FW Policy



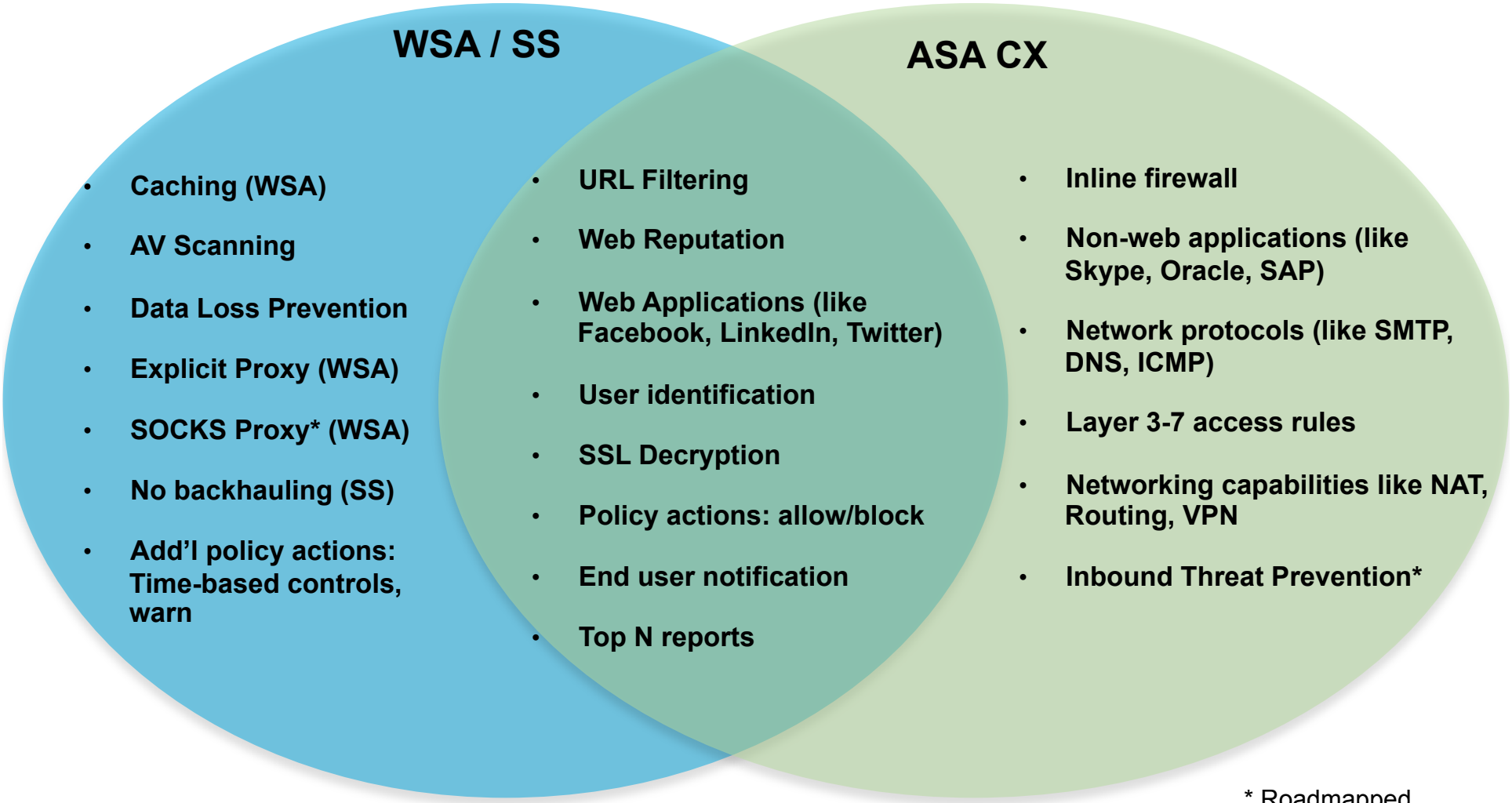
Next Generation Firewall

ASA-CX

- Context-Aware Firewall
- Active/Passive Authentication
- Application Visibility and Control
- Reputation Filtering
- URL Filtering
- SSL Decryption
- Secure Mobility
- Reports

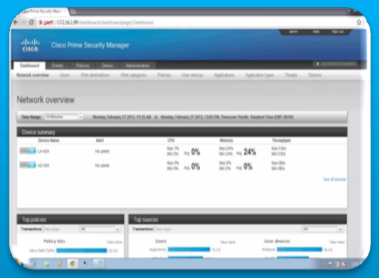


ASA CX & WSA/SS: Feature Overlap & Differences



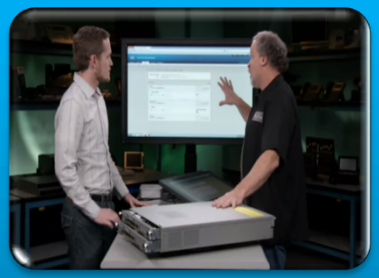
* Roadmapped

ASA-CX Demo



Cisco ASA CX Context-Aware Security

http://www.youtube.com/watch?v=4yYlJnJhTVg



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


cisco