TrustSec Identity Services Engine Overview

Adam Obszyński

Systems Engineer, CCIE #8557

aobszyns@cisco.com

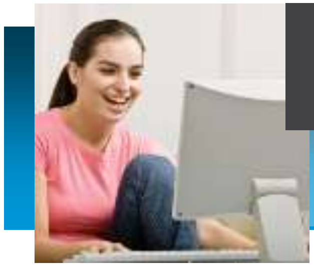
Important!

Many of the products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis.

Roadmaps are subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery or failure to deliver any of the products or features set forth in this document.

Context-Aware Identity - Critical When Networks Are Borderless

Security Challenges



Who?

Identify users and provide differentiated access in a dynamic, borderless environment

What?

Enforcing compliance for proliferating consumer and network capable purpose-built devices

Where?

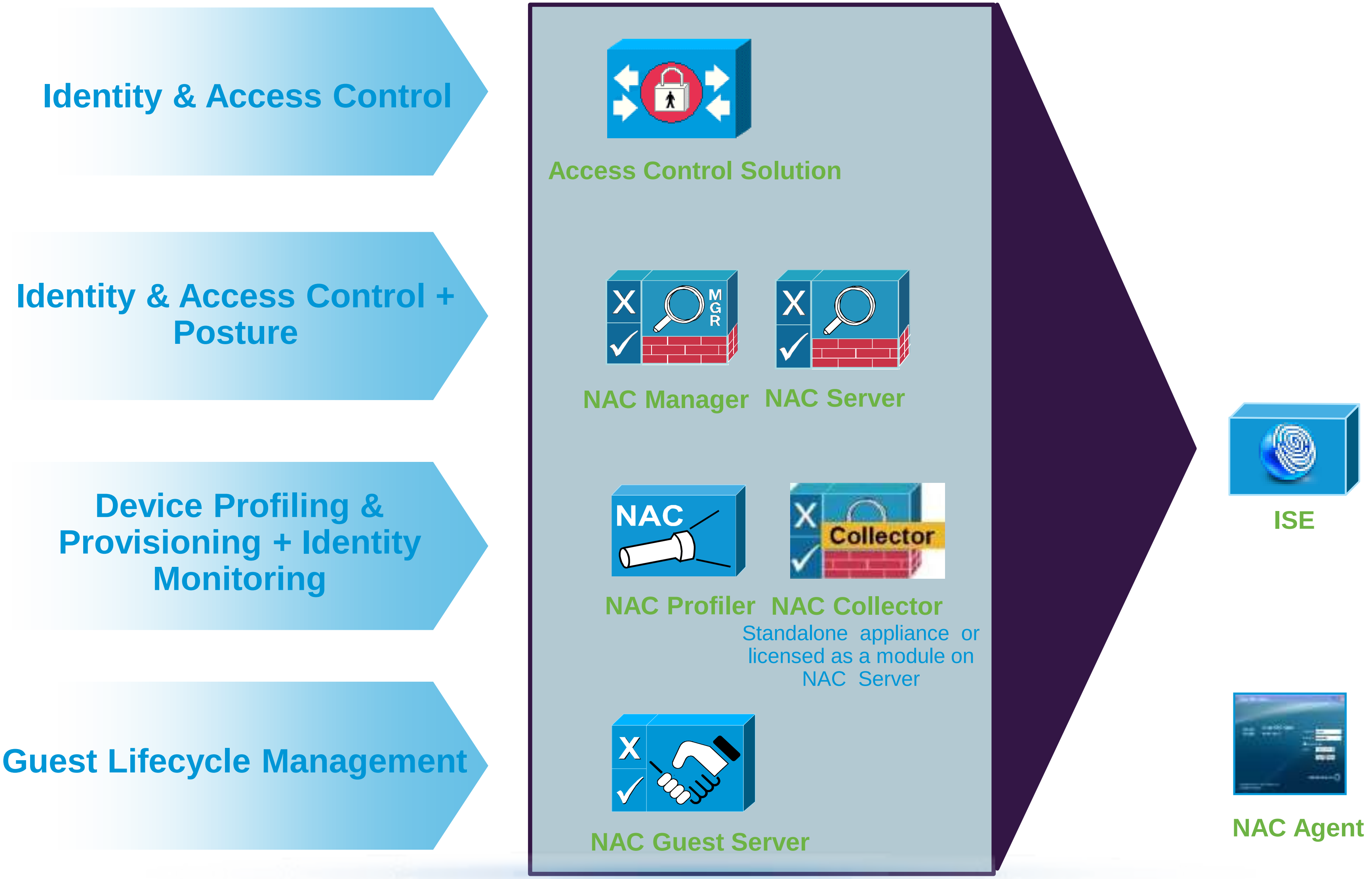
Traditional borders are blurred. Access is possible from anywhere

How?

Establish, monitor, and enforce consistent global access policies

Introducing Identity Services Engine

Next Generation PMBU Solution Portfolio



Identity & Access Control

Identity & Access Control + Posture

Device Profiling & Provisioning + Identity Monitoring

Guest Lifecycle Management

Access Control Solution

NAC Manager

NAC Server

NAC Profiler

NAC Collector

Standalone appliance or licensed as a module on NAC Server

NAC Guest Server

ISE

NAC Agent

Agenda

- FILM #3

2 ISE TechWise TV -- 5m total.wmv - BESTplayer 2.106 (beta)
Otwórz Widok Dźwięk Obraz Napisy Odtwarzanie Narzędzia Pomoc
Otwórz Napisy Opcje Regulacje OnTop Pełny ekran PanScan Aktualizuj Sugestie Przybornik
0:00:09/0:05:18
Playlista Powtarzanie
Odtwarzanie 2 ISE TechWise TV -- 5m total.wmv 0:00:09 / 0:05:18

ISE 1.0: Feature Package Mapping

Current Deployed Products	ISE Package Mapping
ACS	Base Package
NAC Guest Server	
ACS + NAC Guest Server	
ACS + NAC Profiler	Advanced Package
ACS + NAC Guest Server + NAC Profiler	
NAC Appliance	
NAC Appliance + NAC Guest Server	
NAC Appliance + NAC Profiler	
NAC Appliance + NAC Guest Server + NAC Profiler	
NAC Profiler	

Base Package	🟩
Advanced Package	🟦

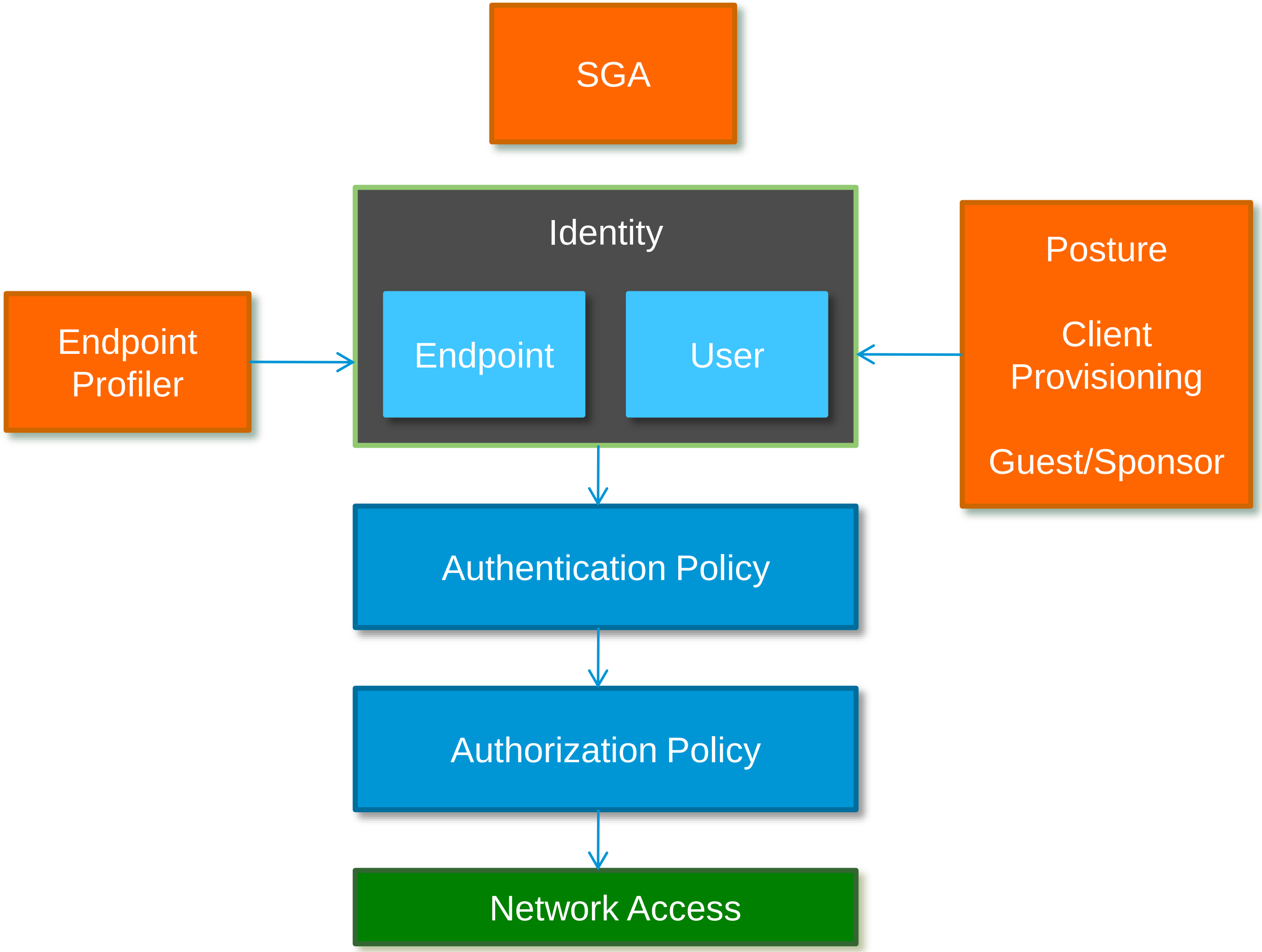
Agenda

- FILM #4

Wireless LAN Controller & Identity Services Engine iPad Demo

Paul Nguyen
Technical Marketing Engineer, WNBU

Attribute-based Policy Model


SGA

Identity

Endpoint

User

Endpoint Profiler

Posture

Client Provisioning

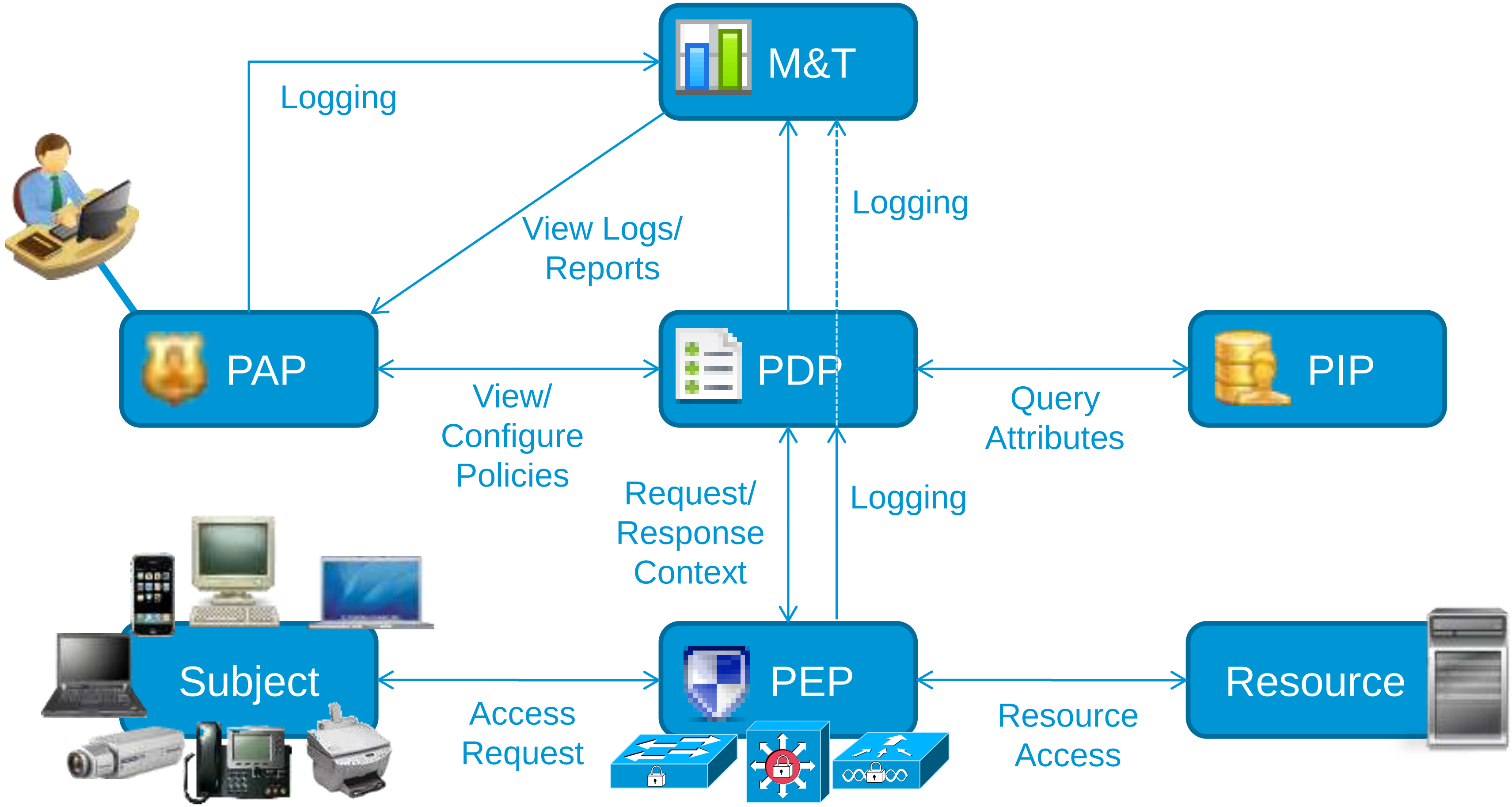
Guest/Sponsor

Authentication Policy

Authorization Policy

Network Access

ISE Architecture



ISE Architecture

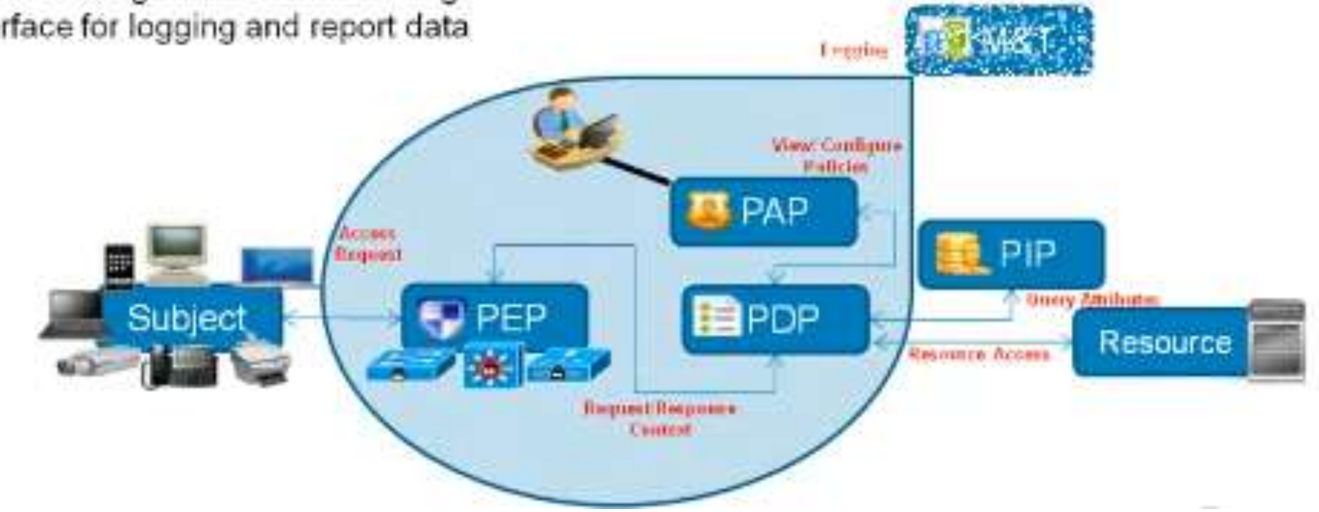
PIP – Policy Information Point
Interface to retrieve policy or policy information

PAP – Policy Administration Point
Interface to configure policies

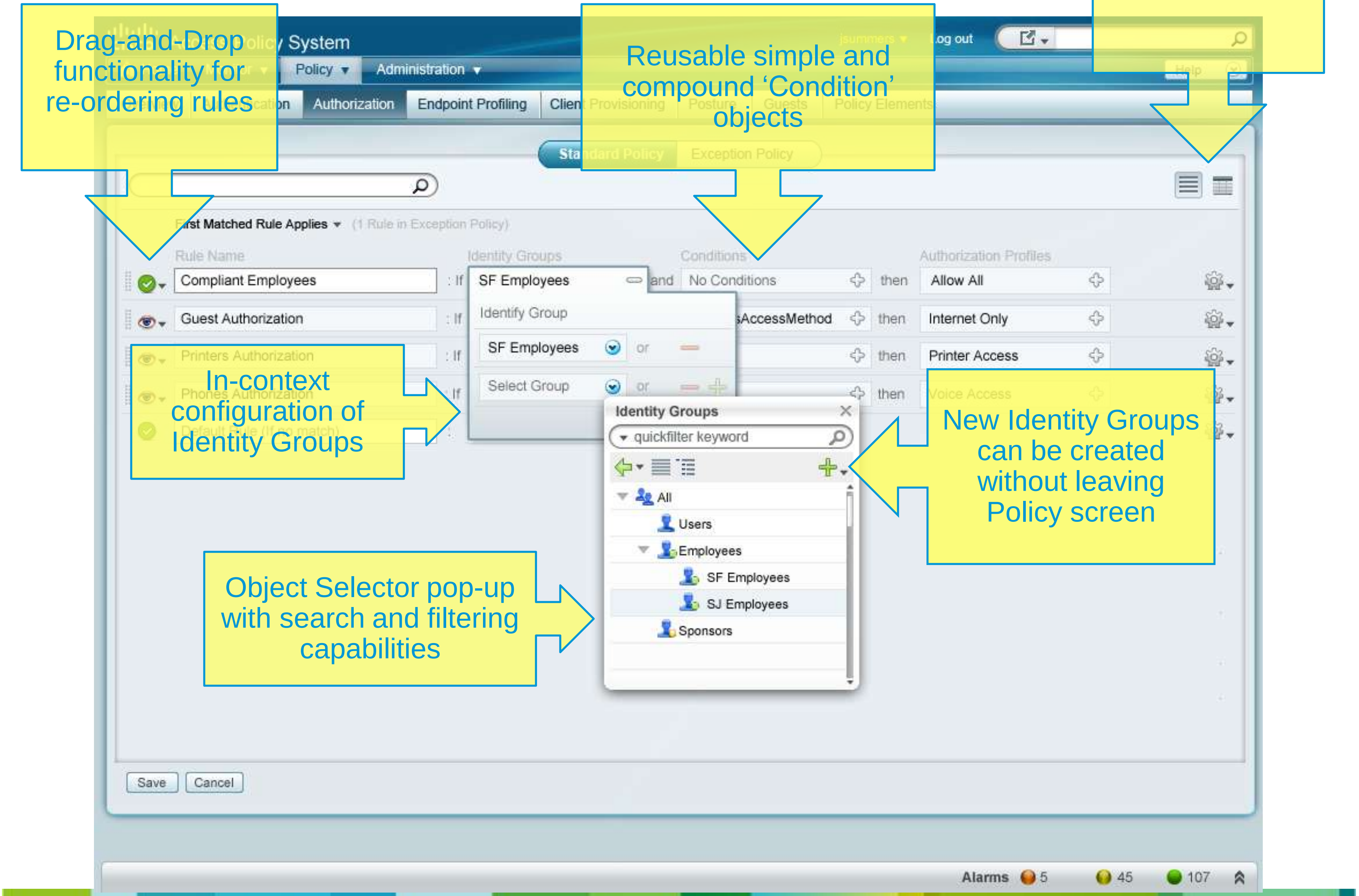
PDP – Policy Decision Point
Engine that makes policy decisions

PEP – Policy Enforcement Point
Interface that queries PDP and enforces policy

M&T – Monitoring and Troubleshooting
Interface for logging and report data



Robust UI



Drag-and-Drop functionality for re-ordering rules

Reusable simple and compound ‘Condition’ objects

Tabular View is also available

In-context configuration of Identity Groups

New Identity Groups can be created without leaving Policy screen

Object Selector pop-up with search and filtering capabilities

Rule Name		Identity Groups		Conditions		Authorization Profiles
Compliant Employees	: If	SF Employees	and	No Conditions	then	Allow All
Guest Authorization	: If			...AccessMethod	then	Internet Only
Printers Authorization	: If				then	Printer Access
Phones Authorization	: If				then	Voice Access
Default Rule (If no match)	:					

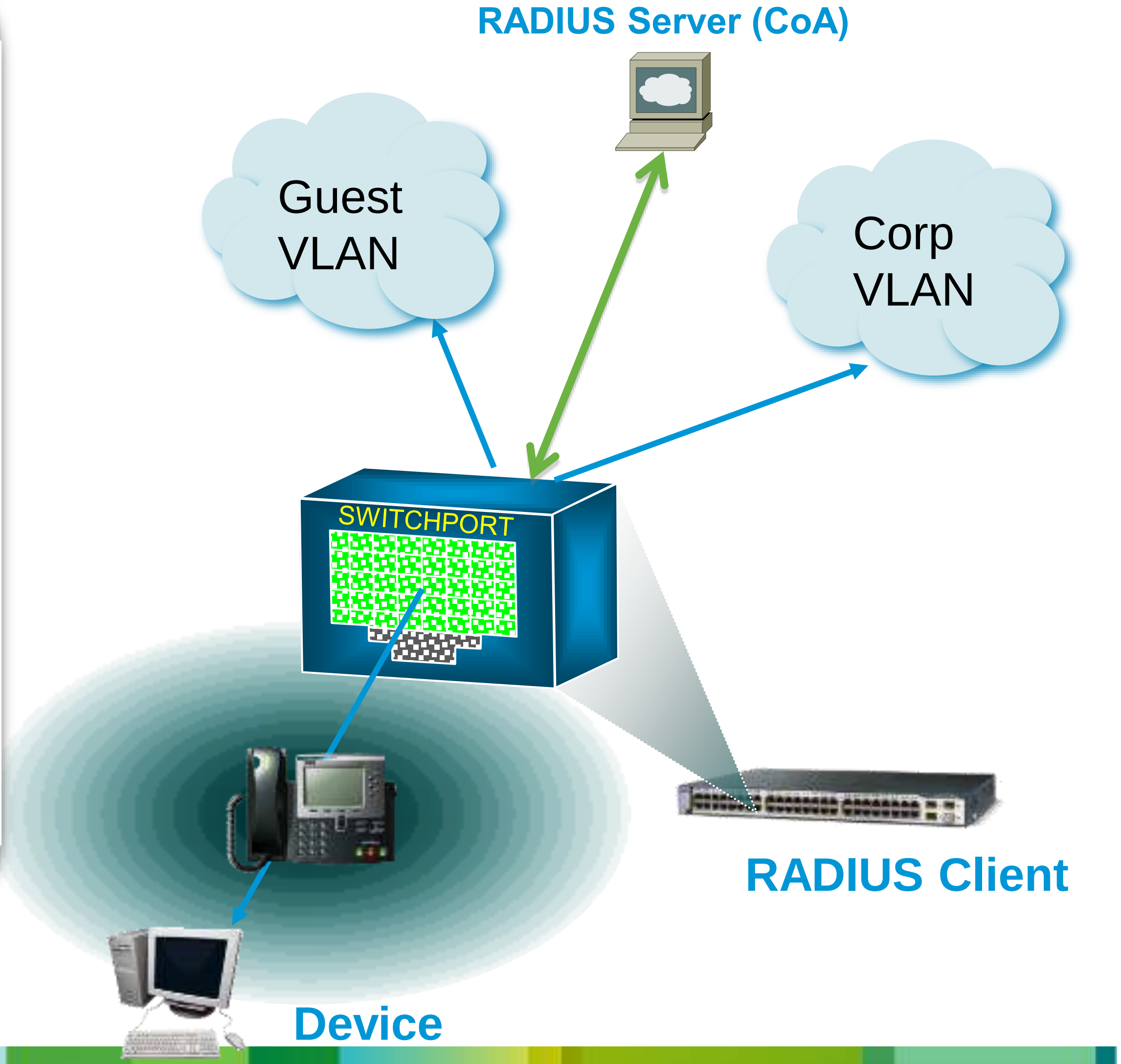
Identify Group
SF Employees or
Select Group or

Identity Groups
quickfilter keyword
- All
  - Users
  - Employees
    - SF Employees
    - SJ Employees
  - Sponsors

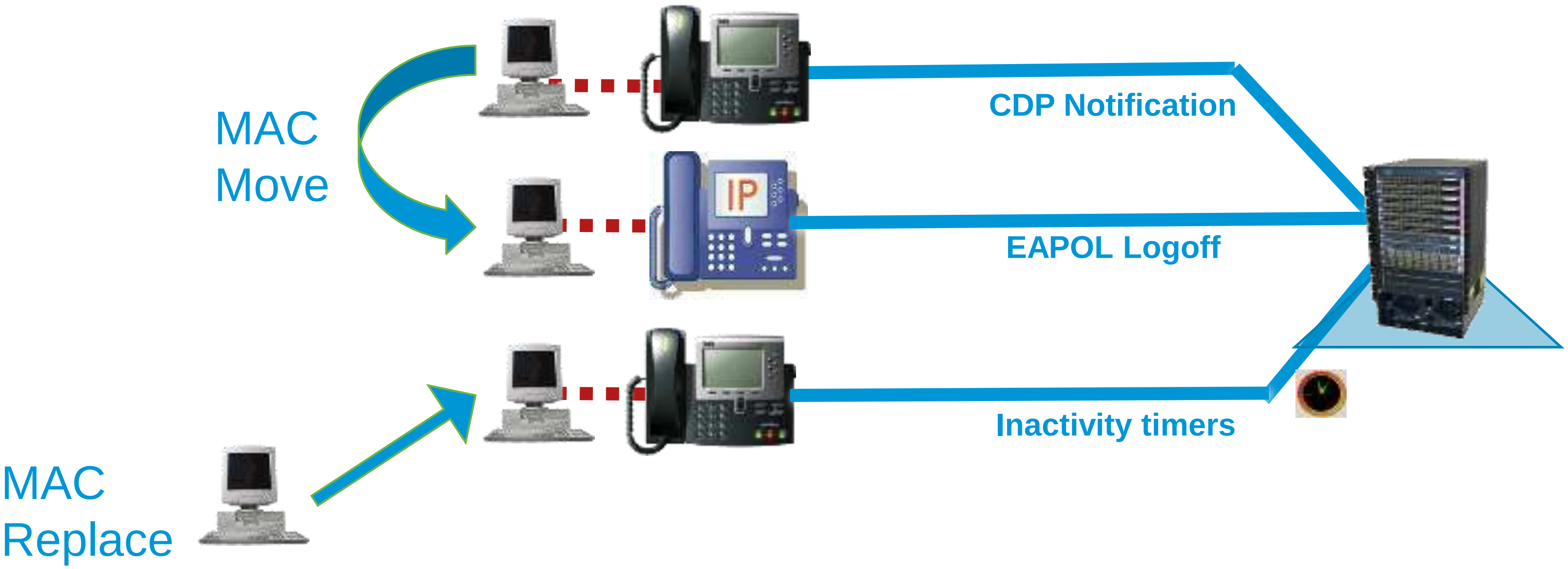
RADIUS Change of Authorization (CoA)

Dynamic session control from a Policy server

- Re-authenticate session
- Terminate session
- Terminate session with port bounce
- Disable host port
- Session Query
  - For Active Services
  - For Complete Identity
  - Service Specific
- Service Activate
- Service De-activate
- Service Query



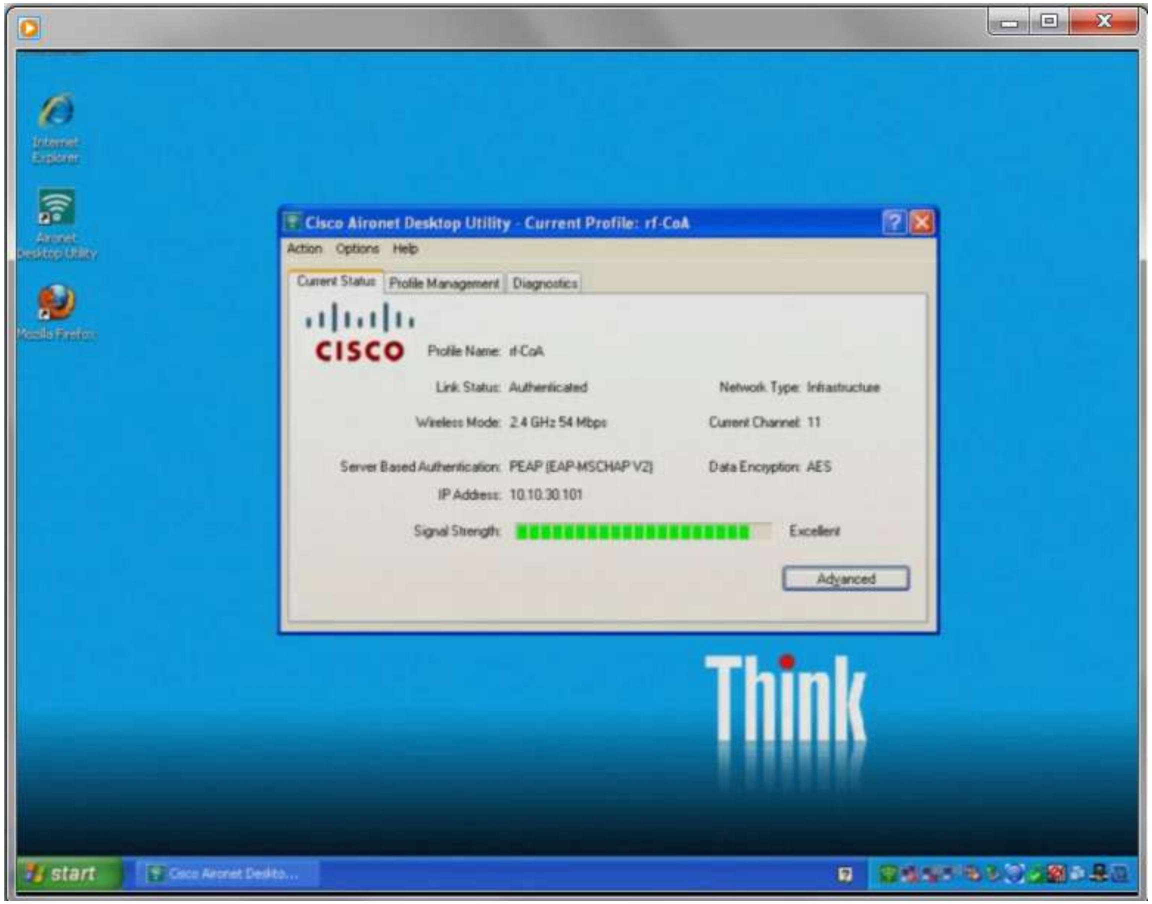
CoA & Options for Security Violations



End Devices Mobility Enhancements	
Existing Mechanisms	**ID 4.1 Enhancements**
CDP Notification	MAC Move
EAPoL Logoff	MAC Replace
Inactivity Timers	ARP Probe Inactivity

Agenda

- FILM #5



Cisco Aironet Desktop Utility - Current Profile: rf-CoA

Profile Name: rf-CoA

Link Status: Authenticated

Network Type: Infrastructure

Wireless Mode: 2.4 GHz 54 Mbps

Current Channel: 11

Server Based Authentication: PEAP (EAP-MSCHAP V2)

Data Encryption: AES

IP Address: 10.10.30.101

Signal Strength: Excellent

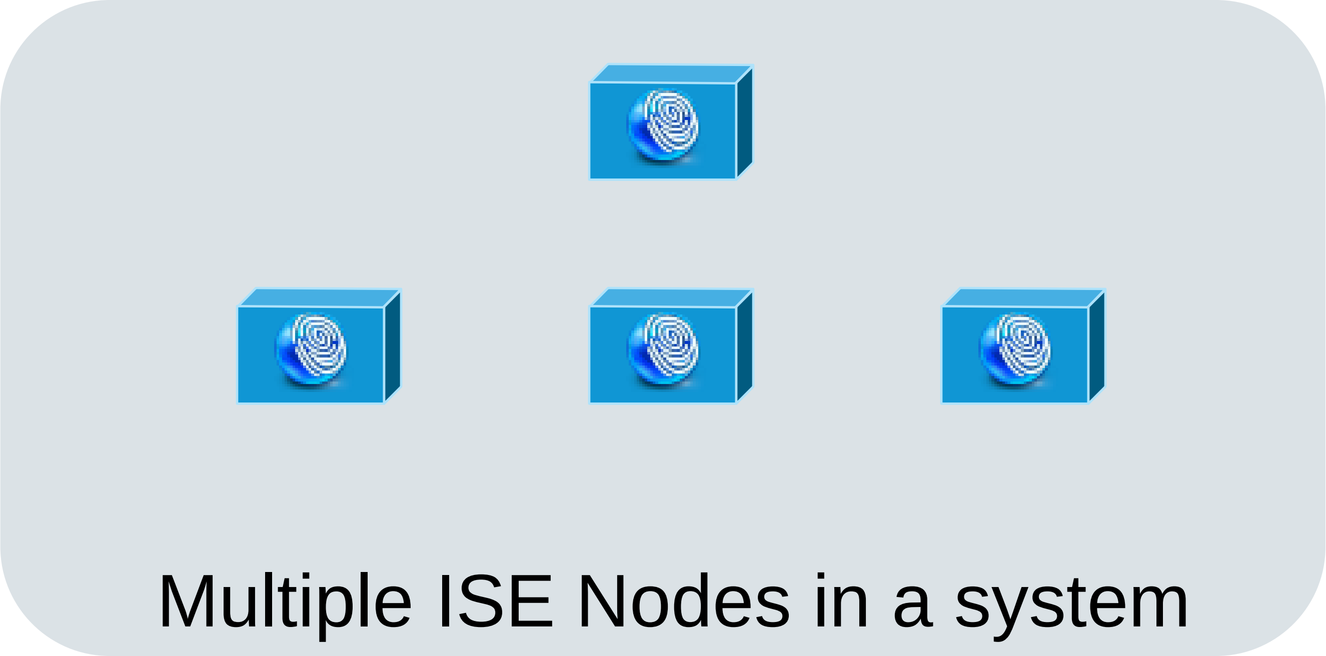
A single appliance deployment

Single ISE Node
providing all services

For smaller environments

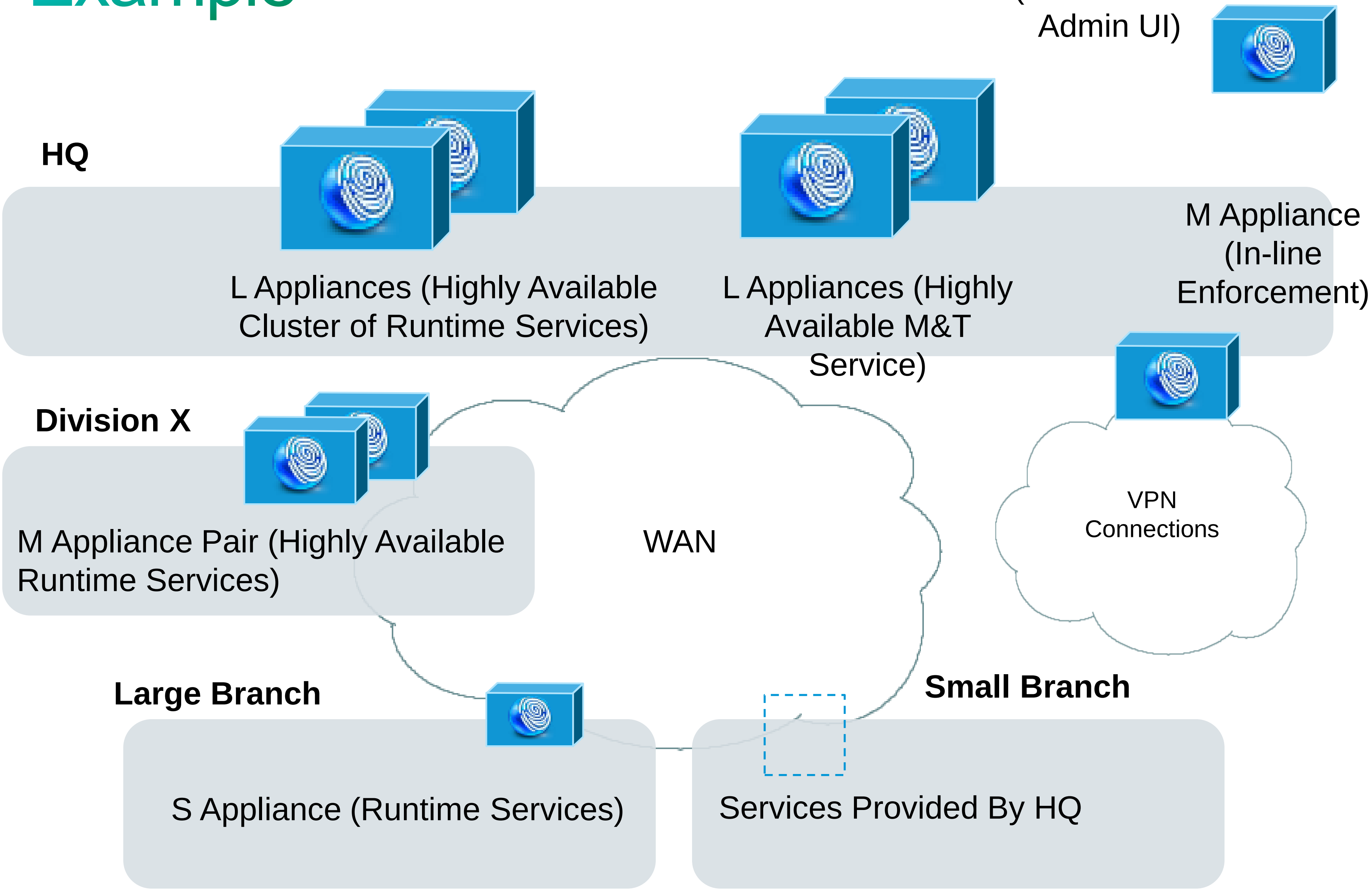
2 boxes
for resiliency

A multi-box deployment


Multiple ISE Nodes in a system

More than 1 box for medium to large environments, or distributed organization. Services can be turned on or off on each individual node as necessary

Example



Virtual Appliance (Dedicated to Admin UI)

HQ

L Appliances (Highly Available Cluster of Runtime Services)

L Appliances (Highly Available M&T Service)

M Appliance (In-line Enforcement)

Division X

M Appliance Pair (Highly Available Runtime Services)

WAN

VPN Connections

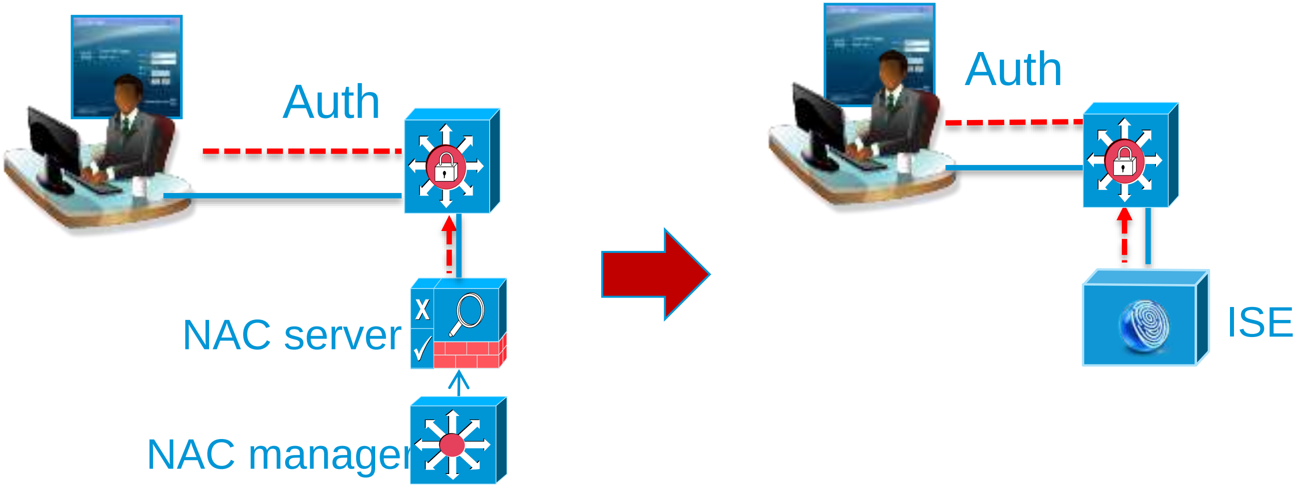
Large Branch

S Appliance (Runtime Services)

Small Branch

Services Provided By HQ

Posture and ISE 1.0



Posture with NAC

Posture with ISE

Features	NAC	ISE 1.0
Client	NAC agent	NAC Agent
Authentication	Kerberos	802.1X
Posture Validation	Opswat	Opswat
Control Plane	SNMP	Radius
Control Technologies	VLAN, IB	VLAN, dACL, SXP/SGT

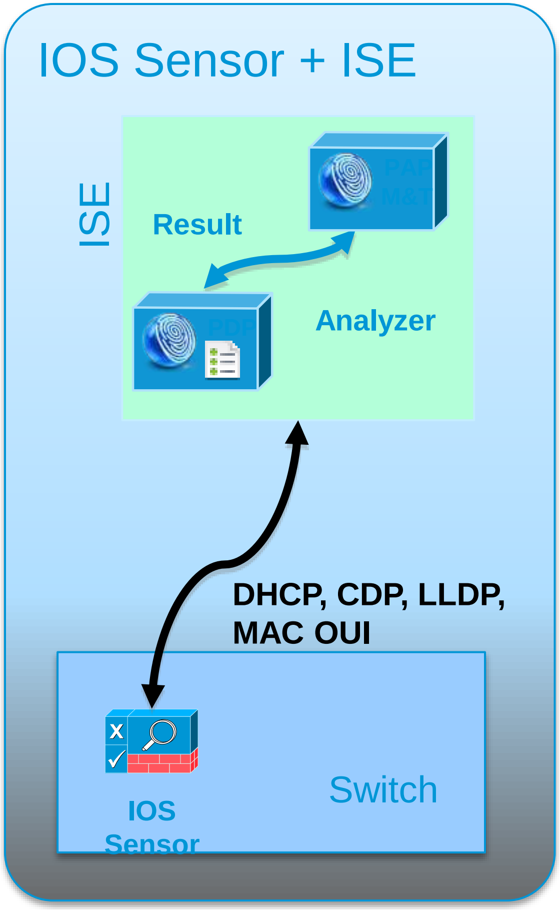
Profiler Sensors on Switch

Solution

- Perform inspection on switch (or WLC)
- Pass info via RADIUS to ISE

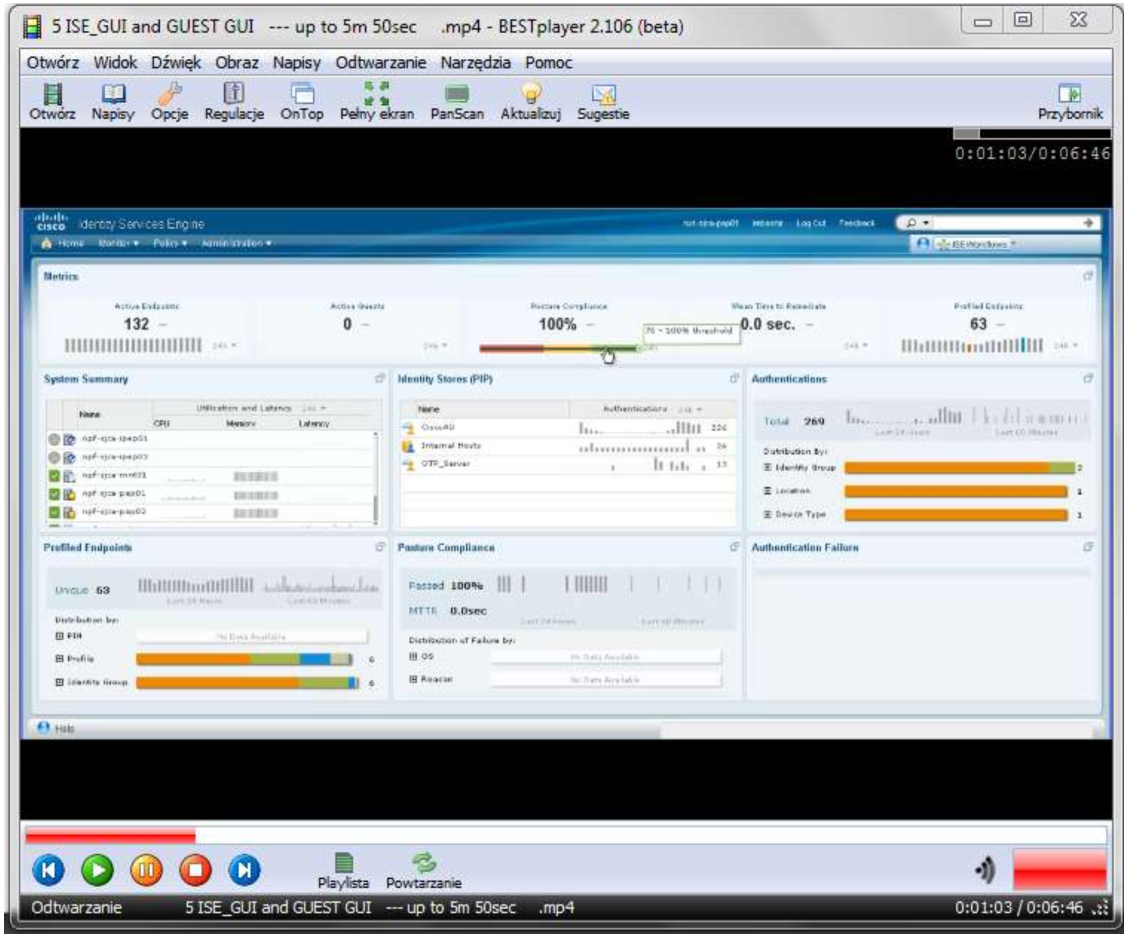
Customer Benefit

- Low touch deployment
- Centralize visibility without big ISE sensor investment

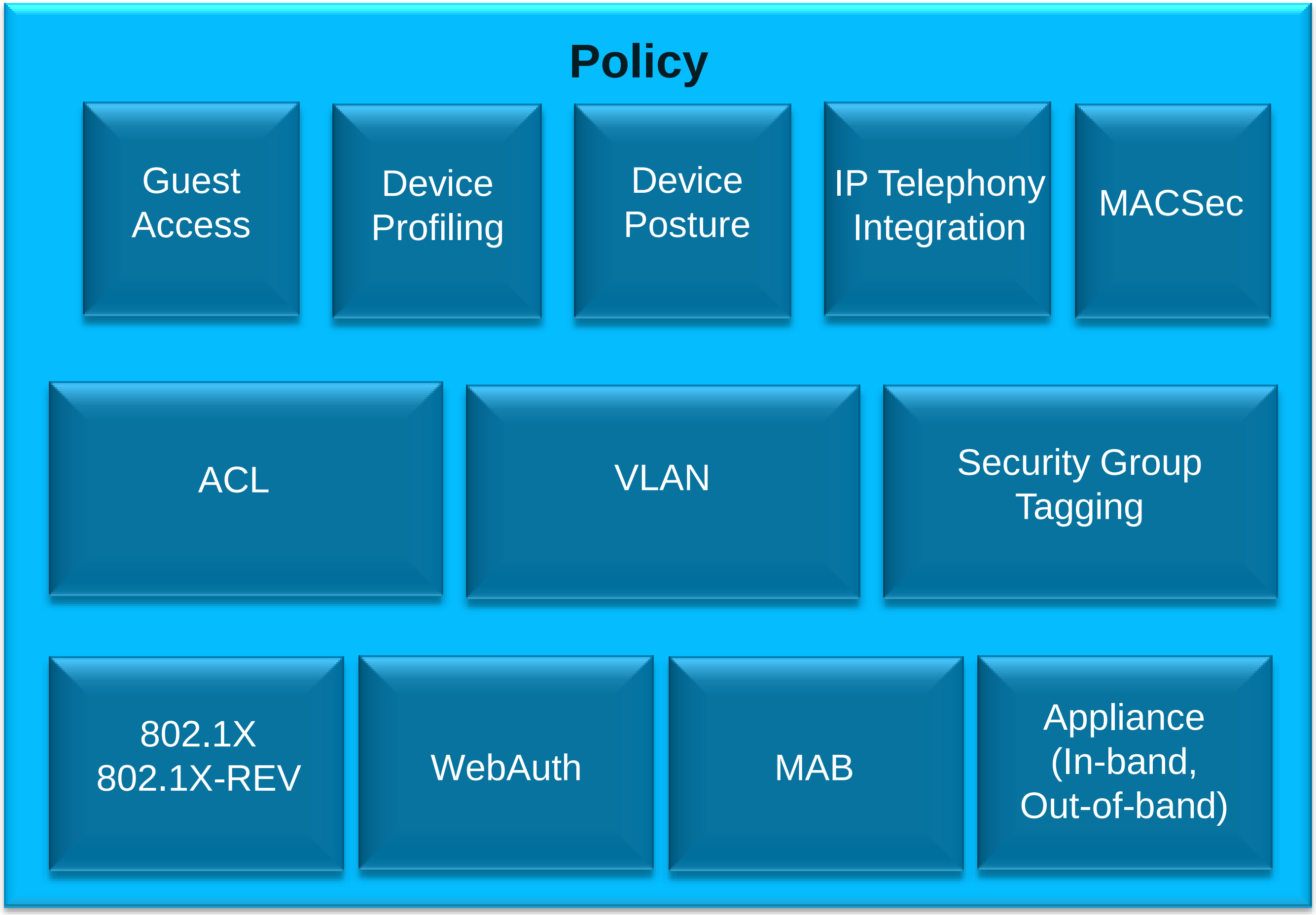


Agenda

- FILM #6



Cisco TrustSec Architecture



TrustSec Key Features

Security Group Based Access Control

- Topology independent access control based on roles
- Scalable **ingress tagging via Source Group Tag (SGT) / egress filtering via Source Group ACL (SGACL)**
- Centralized Policy Management / Distributed Policy Enforcement

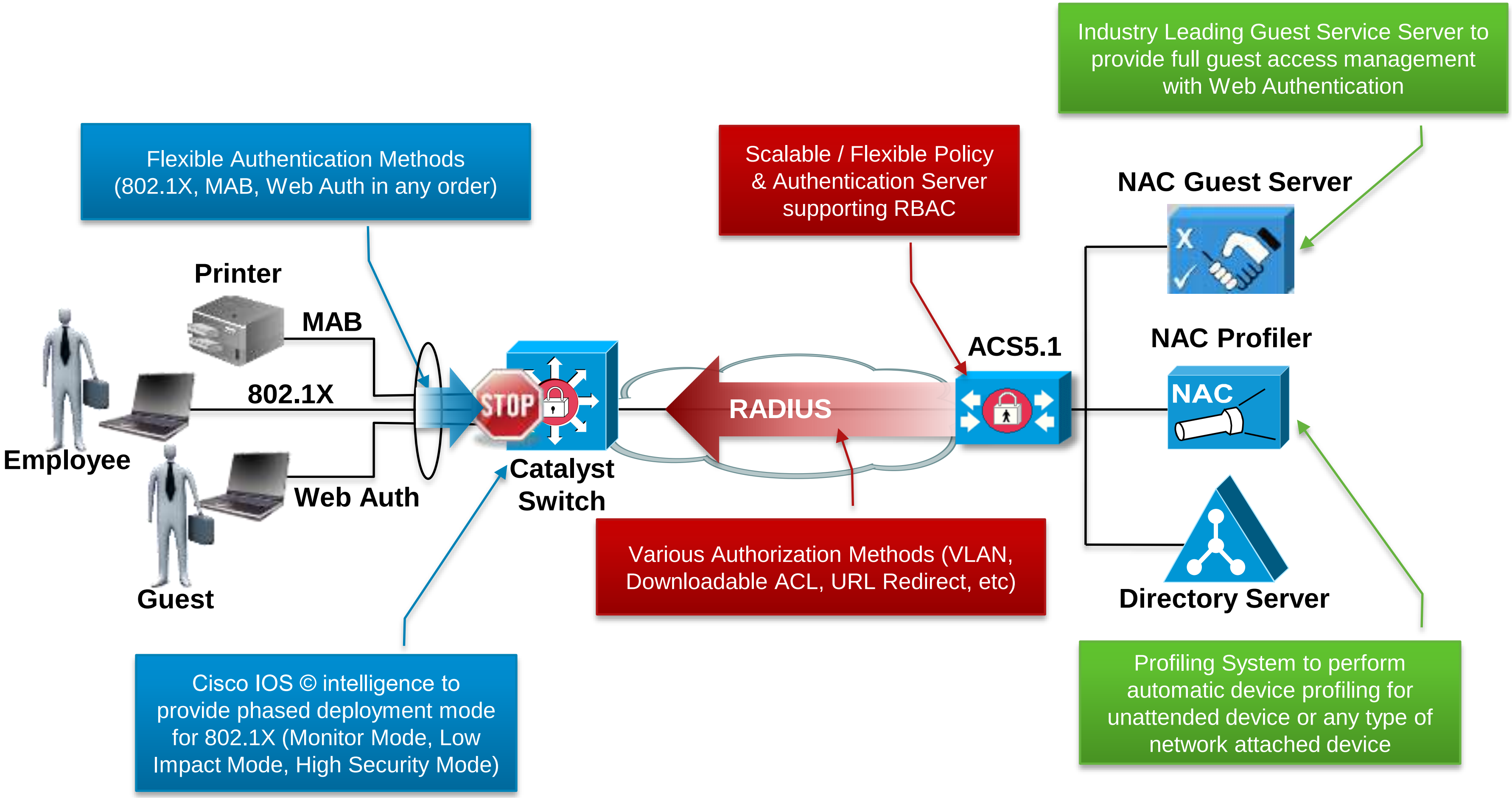
Authenticated Networking Environment

- Endpoint admission enforced via 802.1X authentication, MAB, Web Auth (Full IBNS compatibility)
- Network device admission control based on 802.1X creates trusted networking environment
- Only trusted network imposes Security Group TAG

Confidentiality and Integrity

- Encryption based on **IEEE802.1AE** (AES-GCM 128-Bit)
- **Wire rate** hop to hop layer 2 encryption
- Key management based on 802.11n (SAP), awaiting for standardization in 802.1X-REV

Cisco Identity Solution Overview



Industry Leading Guest Service Server to provide full guest access management with Web Authentication

Flexible Authentication Methods (802.1X, MAB, Web Auth in any order)

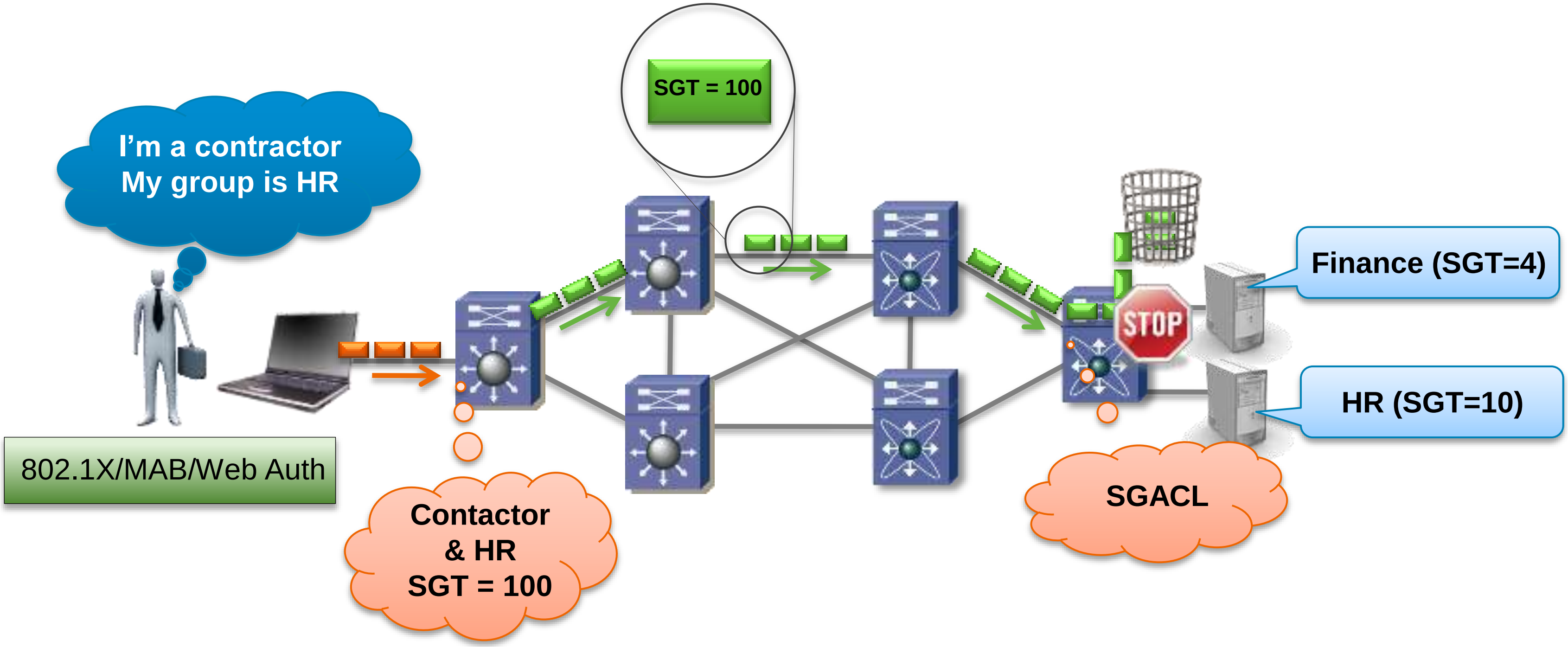
Scalable / Flexible Policy & Authentication Server supporting RBAC

Various Authorization Methods (VLAN, Downloadable ACL, URL Redirect, etc)

Cisco IOS © intelligence to provide phased deployment mode for 802.1X (Monitor Mode, Low Impact Mode, High Security Mode)

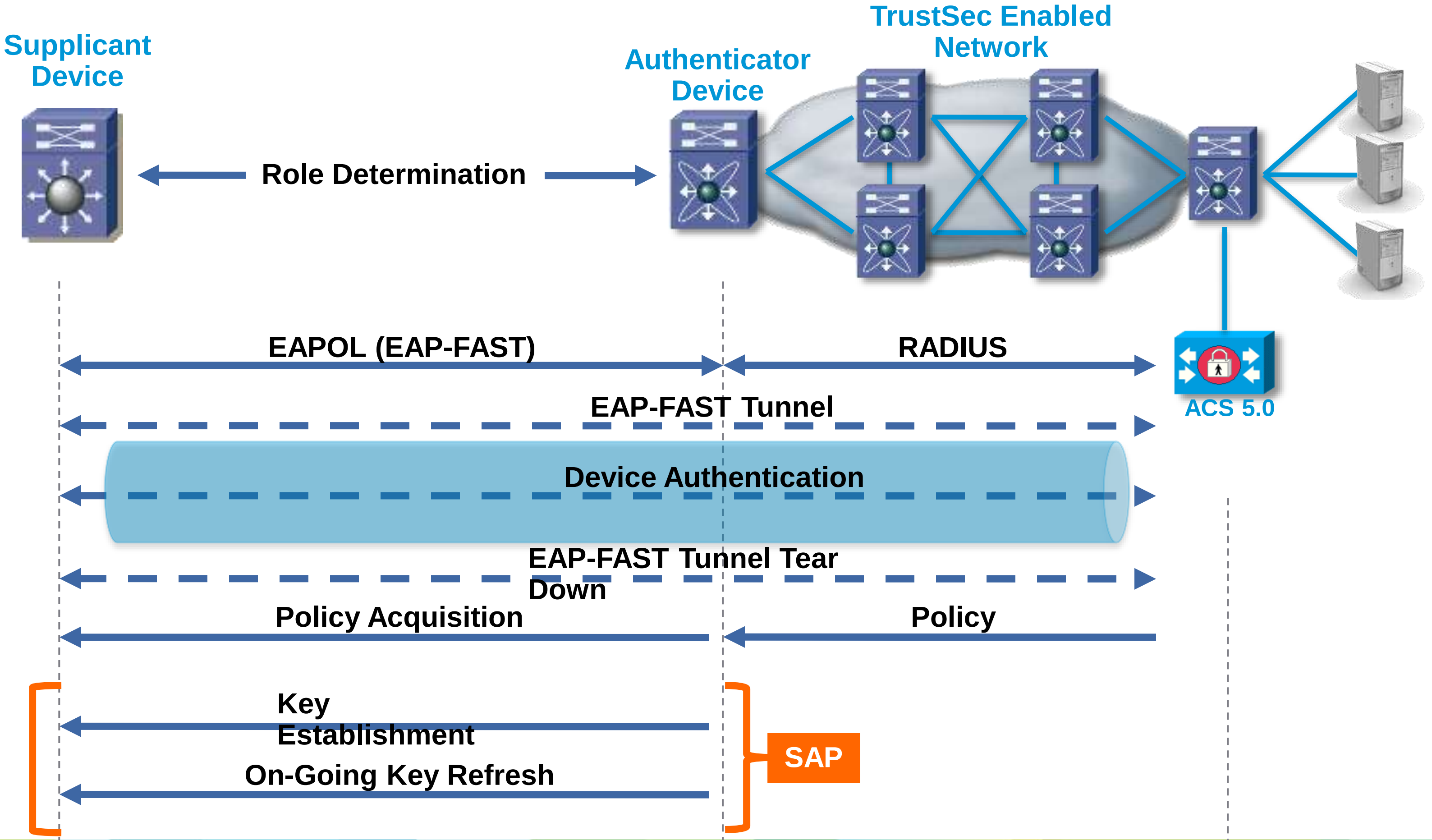
Profiling System to perform automatic device profiling for unattended device or any type of network attached device

Security Group Based Access Control



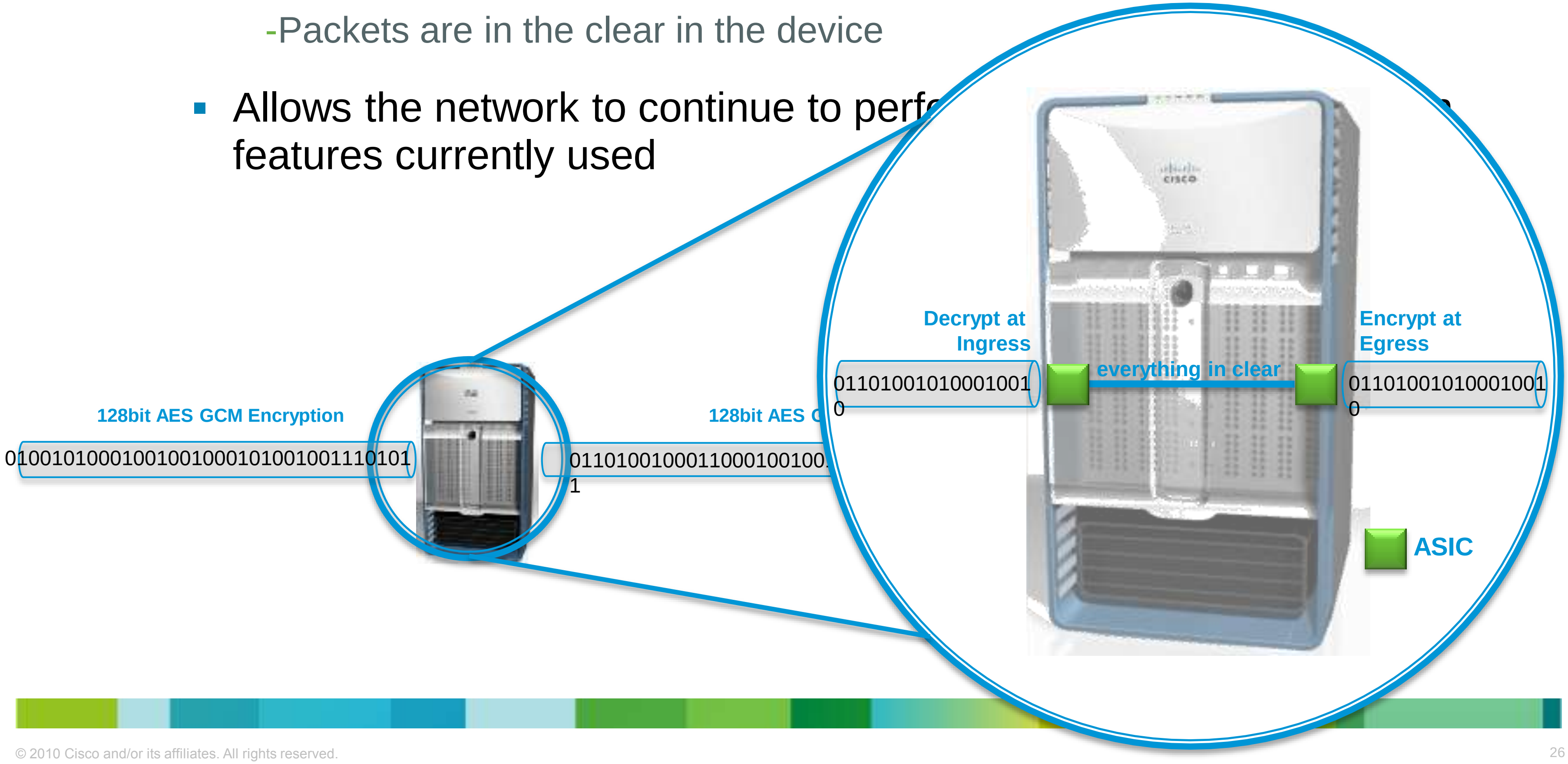
- Security Group Based Access Control allows customers
    - To keep existing logical design at access layer
    - To change / apply policy to meet today's business requirement
    - To distribute policy from central management server

NDAC Authentication / SAP

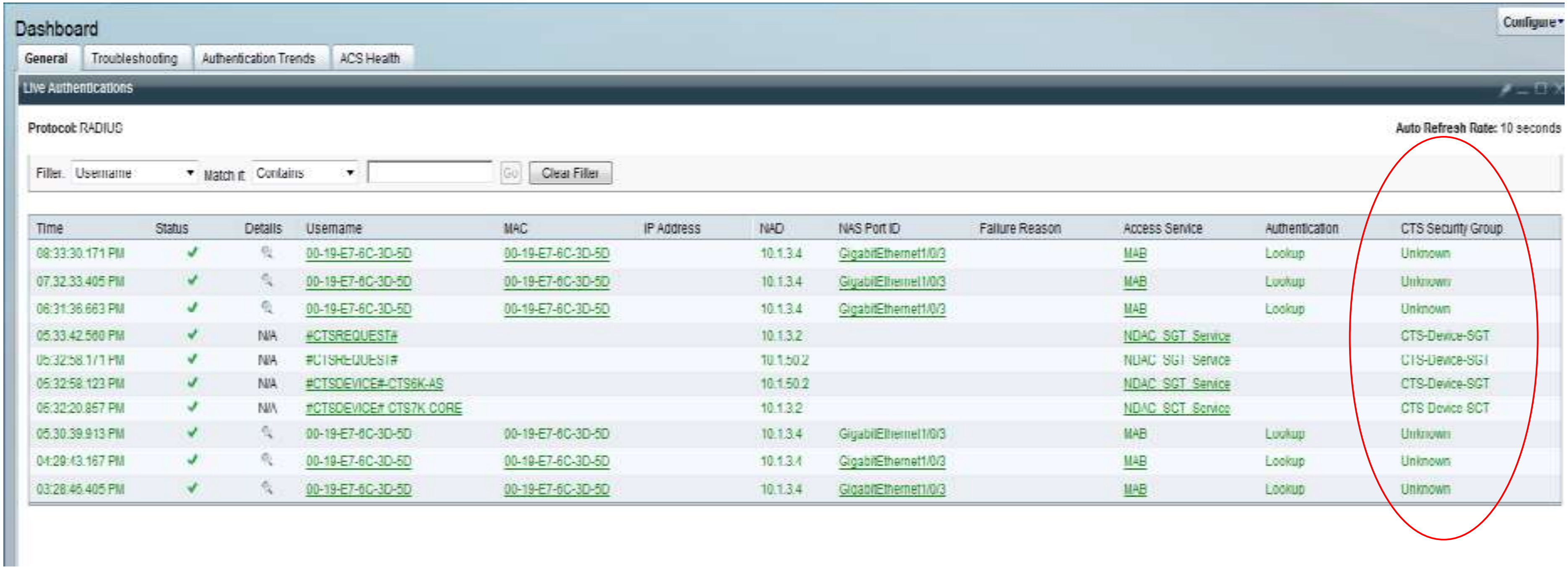


Hop-by-Hop Encryption via IEEE802.1AE

- “Bump-in-the-wire” model
  - -Packets are encrypted on egress
  - -Packets are decrypted on ingress
  - -Packets are in the clear in the device
- Allows the network to continue to perf
  features currently used



TrustSec Information in Basic Reports



Dashboard

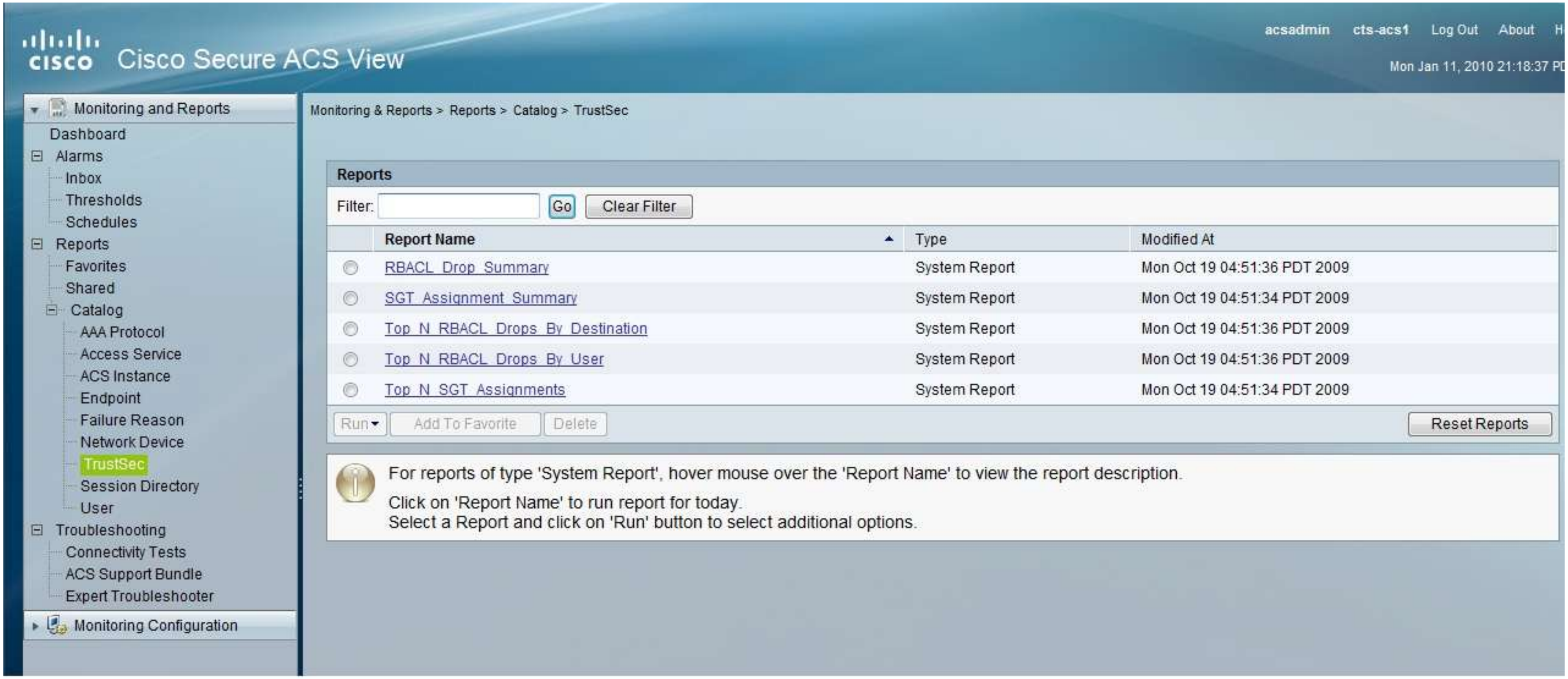
Protocol: RADIUS

Auto Refresh Rate: 10 seconds

Filter: Username ▾ Match if: Contains ▾ Go Clear Filter

Time	Status	Details	Username	MAC	IP Address	NAD	NAS Port ID	Failure Reason	Access Service	Authentication	CTS Security Group
08:33:30.171 PM	✓	🔍	00-19-E7-6C-3D-5D	00-19-E7-6C-3D-5D		10.1.3.4	GigabitEthernet1/0/3		MAB	Lookup	Unknown
07.32.33.405 PM	✓	🔍	00-19-E7-6C-3D-5D	00-19-E7-6C-3D-5D		10.1.3.4	GigabitEthernet1/0/3		MAB	Lookup	Unknown
06:31:36.663 PM	✓	🔍	00-19-E7-6C-3D-5D	00-19-E7-6C-3D-5D		10.1.3.4	GigabitEthernet1/0/3		MAB	Lookup	Unknown
05.33.42.560 PM	✓	N/A	#CTSREQUEST#			10.1.3.2			NDAC_SGT_Service		CTS-Device-SGT
05:32:58.171 PM	✓	N/A	#CTSREQUEST#			10.1.50.2			NDAC_SGT_Service		CTS-Device-SGT
05:32:58.123 PM	✓	N/A	#CTSDEVICE#-CTS6K-AS			10.1.50.2			NDAC_SGT_Service		CTS-Device-SGT
05:32:20.857 PM	✓	N/A	#CTSDEVICE#-CTS7K-CORE			10.1.3.2			NDAC_SGT_Service		CTS-Device-SGT
05.30.39.913 PM	✓	🔍	00-19-E7-6C-3D-5D	00-19-E7-6C-3D-5D		10.1.3.4	GigabitEthernet1/0/3		MAB	Lookup	Unknown
04:29:43.167 PM	✓	🔍	00-19-E7-6C-3D-5D	00-19-E7-6C-3D-5D		10.1.3.4	GigabitEthernet1/0/3		MAB	Lookup	Unknown
03:28:46.405 PM	✓	🔍	00-19-E7-6C-3D-5D	00-19-E7-6C-3D-5D		10.1.3.4	GigabitEthernet1/0/3		MAB	Lookup	Unknown

TrustSec Reports



Monitoring & Reports > Reports > Catalog > TrustSec

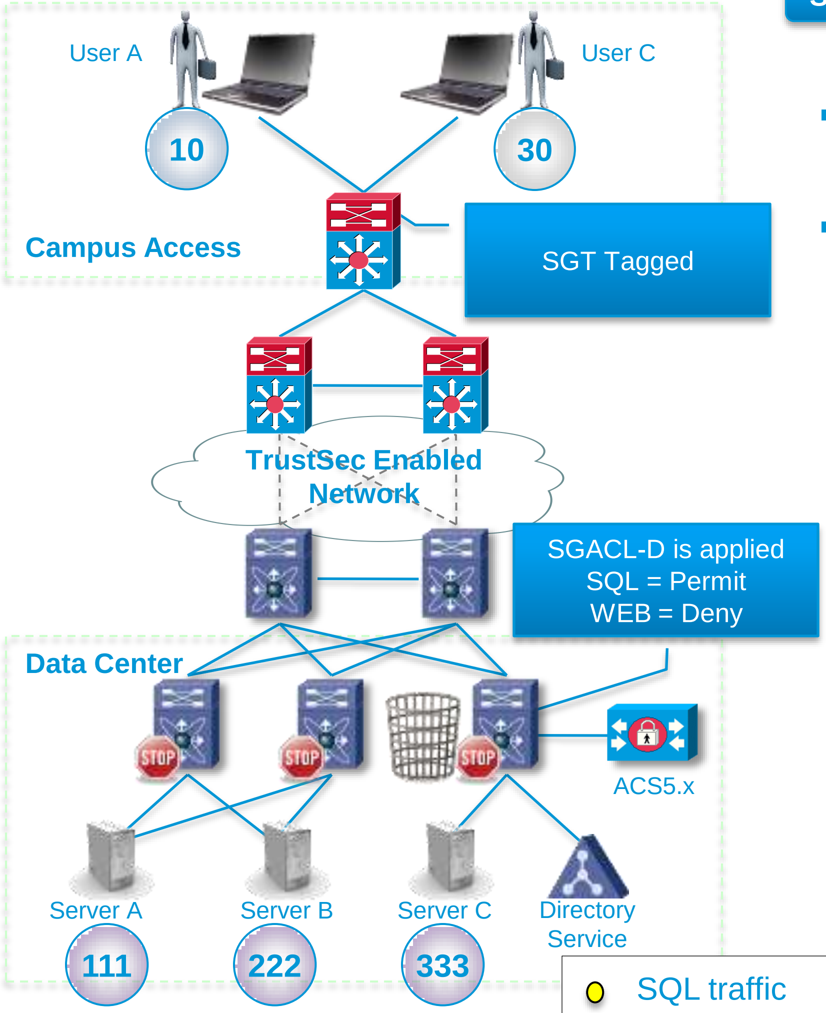
Reports

	Report Name	Type	Modified At
○	RBACL_Drop_Summary	System Report	Mon Oct 19 04:51:36 PDT 2009
○	SGT_Assignment_Summary	System Report	Mon Oct 19 04:51:34 PDT 2009
○	Top_N_RBACL_Drops_By_Destination	System Report	Mon Oct 19 04:51:36 PDT 2009
○	Top_N_RBACL_Drops_By_User	System Report	Mon Oct 19 04:51:36 PDT 2009
○	Top_N_SGT_Assignments	System Report	Mon Oct 19 04:51:34 PDT 2009

For reports of type 'System Report', hover mouse over the 'Report Name' to view the report description.

Click on 'Report Name' to run report for today.
Select a Report and click on 'Run' button to select additional options.

SGACL Enforcement



SGT Tagged

SGACL-D is applied
SQL = Permit
WEB = Deny

● SQL traffic
● Web traffic
STOP SGACL

Step 5 **SGACL allows topology independent access control**

- Even another user accesses on same VLAN as previous example, his traffic is tagged differently
- If traffic is destined to restricted resources, packet will be dropped at egress port of TrustSec domain

SRC\ DST	Server A (111)	Server B (222)	Server C (333)
User A (10)	Permit all	Deny all	Deny all
User B (20)	SGACL-B	SGACL-C	Deny all
User C (30)	Deny all	Permit all	**SGACL-D**

SGACL-D

```
permit tcp  src  dst  eq 1433
#remark destination SQL permit
permit tcp src  eq 1433  dst
#remark source SQL permit
deny tcp  src  dst eq 80
# web deny
deny tcp  src  dst eq 443
# secure web deny
deny all
```

Reference Slide

TrustSec Component Support Matrix

Platforms	Available Feature	OS Version	Notes
Nexus 7000 series Switch	SGACL, 802.1AE + SAP, NDAC, SXP, IPM, EAC	Cisco NX-OS® 4.2.2. Advanced Service Package license is required	Mandatory as enforcement point
Catalyst 6500E Switch (Supervisor 32, 720, 720-VSS)	NDAC (No SAP), SXP, EAC	Cisco IOS® 12.2 (33) SXI3 or later release. IP Base w/ K9 image required	Campus access / distribution switch, DC access switch
Catalyst 49xx switches	SXP, EAC	Cisco IOS® 12.2 (53) SG or later release. IP Base w/ K9 image required.	Optional as an DC access switch
Catalyst 4500 Switch (Supervisor 6L-E or 6-E)	SXP, EAC	Cisco IOS® 12.2 (53) SG or later release. IP Base w/ K9 image required.	Optional as Campus access switch
Catalyst 3760(E) / 3750(E) Switches	SXP, EAC	Cisco IOS® 12.2 (53) SE or later release. IP Base w/ K9 image required.	Optional as Campus access switch
Catalyst Blade Module 3x00 Switches	SXP, EAC	Cisco IOS® 12.2 (53) SE or later release. IP Base w/ K9 image required.	Optional as DC access switch
Cisco EtherSwitch service module for ISR Routers	SXP, EAC	Cisco IOS® 12.2 (53) SE or later release. IP Base w/ K9 image required.	Optional as Branch access
Cisco Secure ACS	Centralized Policy Management for TrustSec / NDAC + EAC Authentication Server	ACS Version 5.1 with TrustSec license required. CSACS1120 appliance or ESX Server 3.5 or 4.0 is supported	Mandatory as main policy server

TrusctSec

- **Next Generation Fixed Switches: Catalyst 3750-X, 3560-X, 2960-S**

  802.1AE (MACSec) encryption on the 3750-X and 3560-X : only the user/down-link ports (links between the switch and endpoint devices such as a PC or IP phone) can be secured using MACsec

- **Supervisor Engine 7-E on Catalyst 4500-E, 48G/slot**

  Gigabit and 10 Gigabit line cards

  TrustSec with 802.1ae (MACSec) encryption and Security Group Tags

  hardware : ready, software: end of 2011

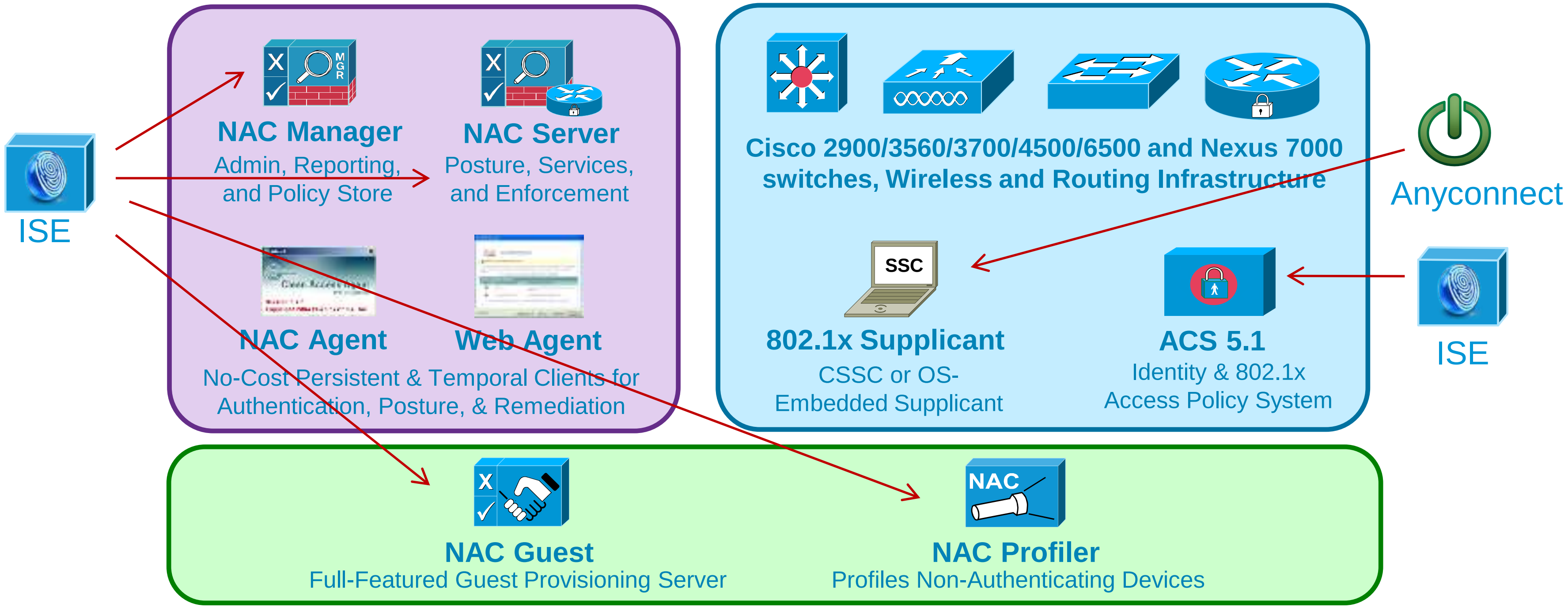
TrustSec 2.0 Deployment Modes

NAC Appliances

802.1X/Infrastructure

NAC overlay solution for quick deployment and/or heterogeneous environments

Robust integrated enforcement solution for 802.1X-enabled infrastructures



ISE

NAC Manager
Admin, Reporting, and Policy Store

NAC Server
Posture, Services, and Enforcement

NAC Agent

Web Agent

No-Cost Persistent & Temporal Clients for Authentication, Posture, & Remediation

Cisco 2900/3560/3700/4500/6500 and Nexus 7000 switches, Wireless and Routing Infrastructure

Anyconnect

802.1x Supplicant
CSSC or OS-Embedded Supplicant

ACS 5.1
Identity & 802.1x Access Policy System

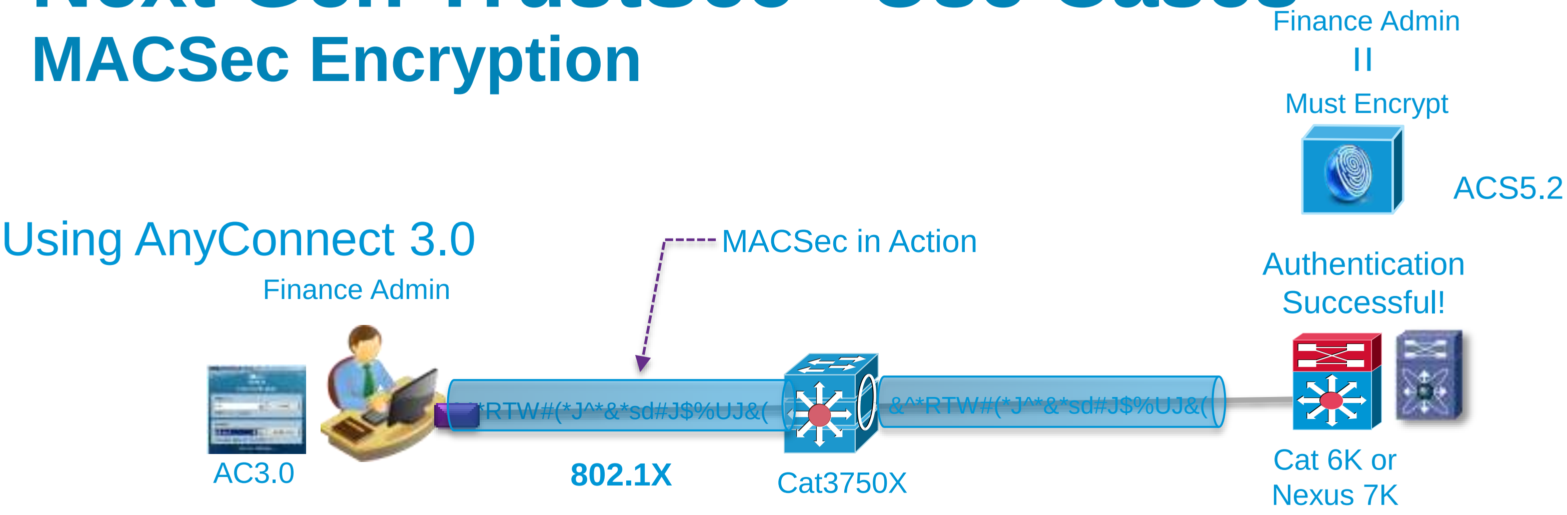
ISE

NAC Guest
Full-Featured Guest Provisioning Server

NAC Profiler
Profiles Non-Authenticating Devices

Next Gen TrustSec - Use Cases

MACSec Encryption



Note:

Already supported:

- MACSec encryption supported in DC between Nexus 7K
- Downlink encryption from AC to Cat 3KX (MKA)

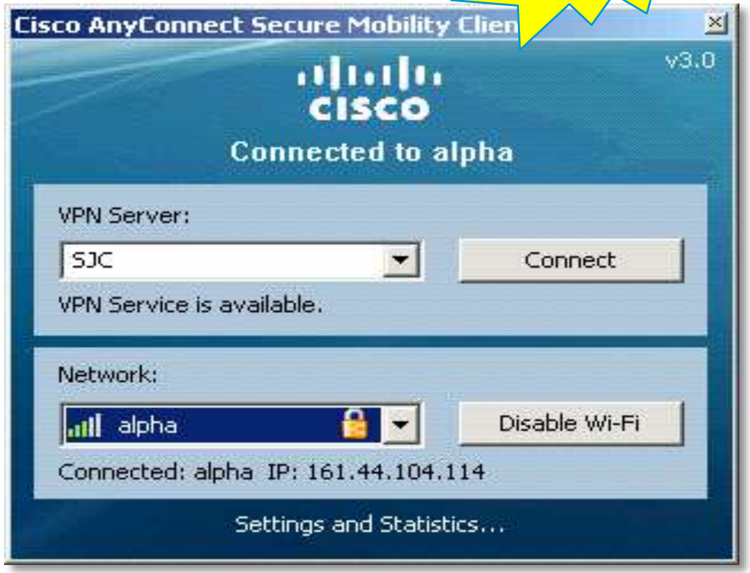
Next Gen TrustSec adds:

- Switch to switch encryption (Cat 3Kx – Cat6K or Nexus 7K)
- Note that encryption uses SAP, not MKA

Anyconnect 3.0

Download All Modes on CCO

- AnyConnect 3.0 provides
  - Unified access interface for SSL-VPN, IPSec and 802.1X for LAN / WLAN
  - Support MACSec / MKA (802.1X-REV) for data encryption in software (Performance is based on CPU of the endpoint)
  - MACSec capable hardware (network interface card) enhance performance with AnyConnect 3.0


Cisco AnyConnect Secure Mobility Clien

v3.0

Connected to alpha

VPN Server: SJC

VPN Service is available.

Network: alpha

Connected: alpha IP: 161.44.104.114

For TrustSec:

- 802.1x – headend is switch, ASA is not needed. Option to license under investigation
- MACSec:
  - • Hardware encryption – Requires Anyconnect and MACSec-ready hardware: (Intel 82576 Gigabit Ethernet Controller, Intel 82599 10 Gigabit Ethernet Controller, Intel ICH10 - Q45 Express Chipset (1Gbe LOM) (Dell, Lenovo, Fujitsu, and HP have desktops shipping with this LOM.)
  - • Software encryption – Requires Anyconnect and uses CPU of PC

Thank you.

cisco