Cisco Network Admission Control
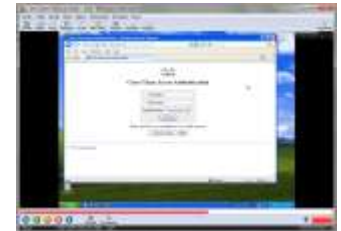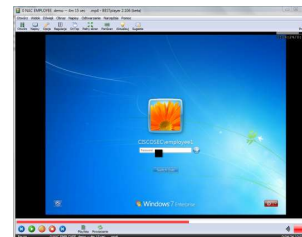
A technical overview

Adam Obszyński

Systems Engineer, Public Sector, CCIE #8557

aobszyns@cisco.com

Czy wiesz kto i jakie urządzenia korzystają z Twojej sieci?

Agenda

#1	Introduction
#2	Cisco NAC Overview
#3	Cisco NAC Solutions
#4	Cisco NAC Components
#5	Summary

Introduction

The Transformation:
The World Is Our New Workspace

Right Resource

Right Device

Right Person

Right Place
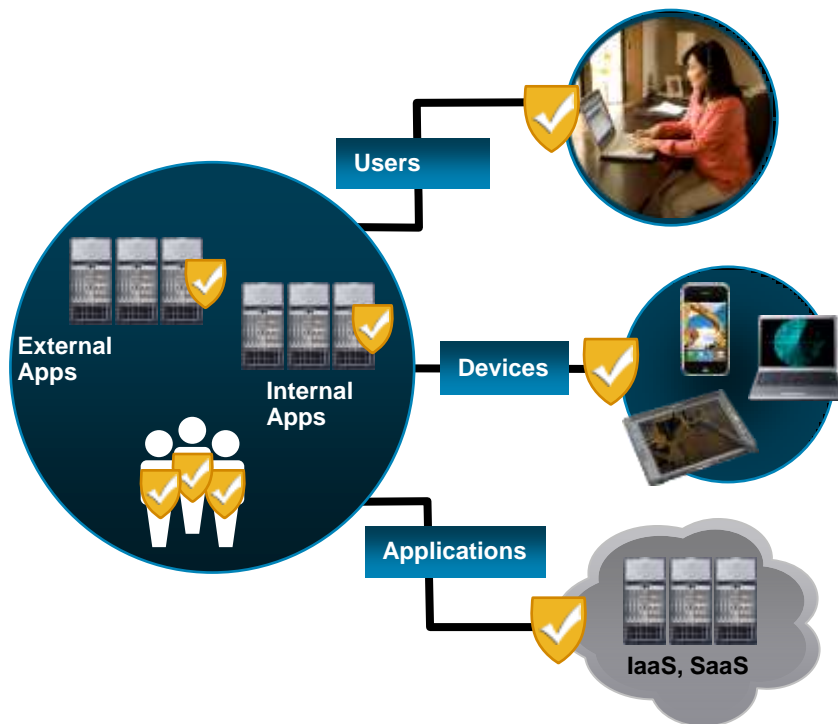
BORDERLESS NETWORKS
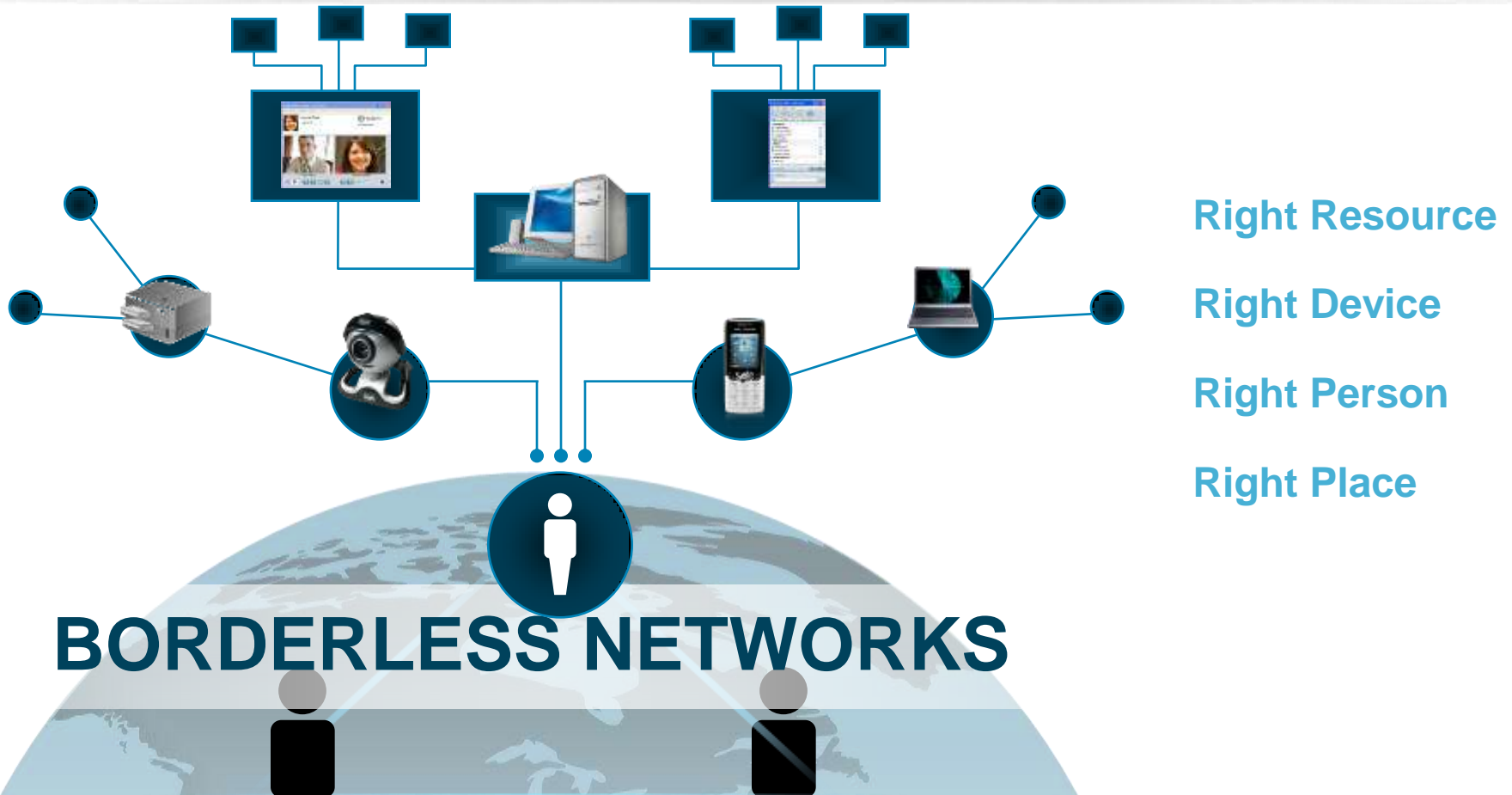
A Next Generation Architecture to Deliver the New Workspace Experience

Borderless Network Market Drivers

- **Complex workforce – employees, guests, contractors, partners**

- **Employees demand mobility and device choice**

Users

External Apps

Internal Apps

Devices

- **Consumerization of access devices**

- **Purpose-built devices becoming network enabled**

Applications

IaaS, SaaS

- **Increased use of virtualization**

- **Move to cloud-based access and services**

Cisco TrustSec –
Identity Solution for a Borderless World

Supports Compliance

Enables corporate governance through consistent access policy for all users and devices
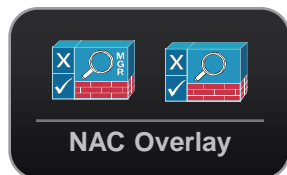
Strengthens Security

Enforce consistent security policy, ensure endpoint health, deliver a secure network fabric

Increases Efficiency

Reduces IT overhead through centralized identity management and integrated policy enforcement

Two TrustSec Options for Any Customer

NAC Overlay

802.1X/Infrastructure

NAC overlay solution for quick deployment and/or heterogeneous environments

Robust integrated enforcement solution for 802.1X-enabled infrastructures

NAC Manager
Admin, Reporting, and Policy Store

NAC Server
Posture, Services, and Enforcement

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

Web Agent

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

SSC

802.1X Supplicant
CSSC or OS-Embedded Supplicant

ACS 5.x
Identity & 802.1X Access Policy System
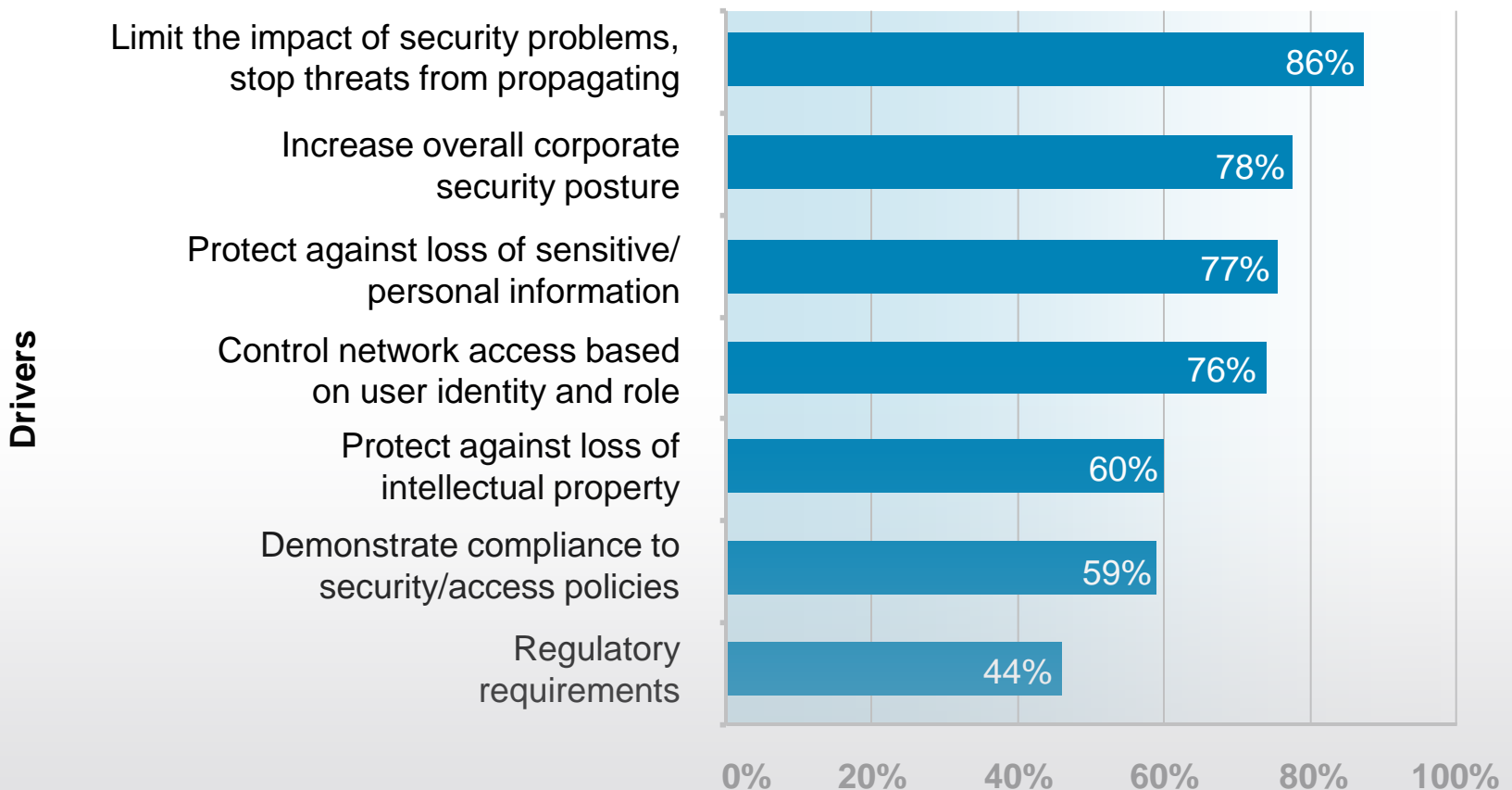
NAC Guest
Full-Featured Guest Provisioning Server

NAC

NAC Profiler
Profiles Non-Authenticating Devices

What's Right For Me?	
Immediate need for posture assessment?	NAC
Largely non-Cisco access infrastructure?	NAC
802.1X or industry standard mandate over next 1-2 years?	Infra-structure
Have or plan to deploy a service-enabled infrastructure?	Infra-structure
Note –Guest Server and Profiler can be deployed with both NAC and ACS	

NAC Overview

The Business Case for NAC

Drivers

Driver	Percentage
Limit the impact of security problems, stop threats from propagating	86%
Increase overall corporate security posture	78%
Protect against loss of sensitive/ personal information	77%
Control network access based on user identity and role	76%
Protect against loss of intellectual property	60%
Demonstrate compliance to security/access policies	59%
Regulatory requirements	44%

0%   20%   40%   60%   80%   100%

Source: Infonetics Research, June 2009

Cisco 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

How do you secure access to your network ?

NAC Role based access for "employees"

- Users must authenticate with NAC

- Devices must then be checked for your security compliance

- Switchports are in the Unauthenticated VLAN by default

- All users are enforced in the Unauthenticated Role before accessing the network.

```
100  client-net-100          active   Fa0/1, Fa0/3, Fa0/4, Fa0/5
                              Fa0/6, Fa0/7, Fa0/10, Fa0/11
                              Fa0/13, Fa0/14, Fa0/15, Fa0/16
                              Fa0/17, Fa0/18, Fa0/19, Fa0/20
                              Fa0/21, Fa0/22
101 client-untrusted -net   active
                              Fa0/2, Fa0/8, Fa0/9, Fa0/12
102  client-net-102           active
103  client-untrusted-cas2    active
104  3560-GUEST-VLAN          active
```

How do you ensure end users have the latest hotfixes, patches and updates?

- NAC will check Microsoft patches

- Users will be checked for AV/AS version compliance

- Services will be checked to make sure they are running

- If requirements fail the device will be quarantined

X
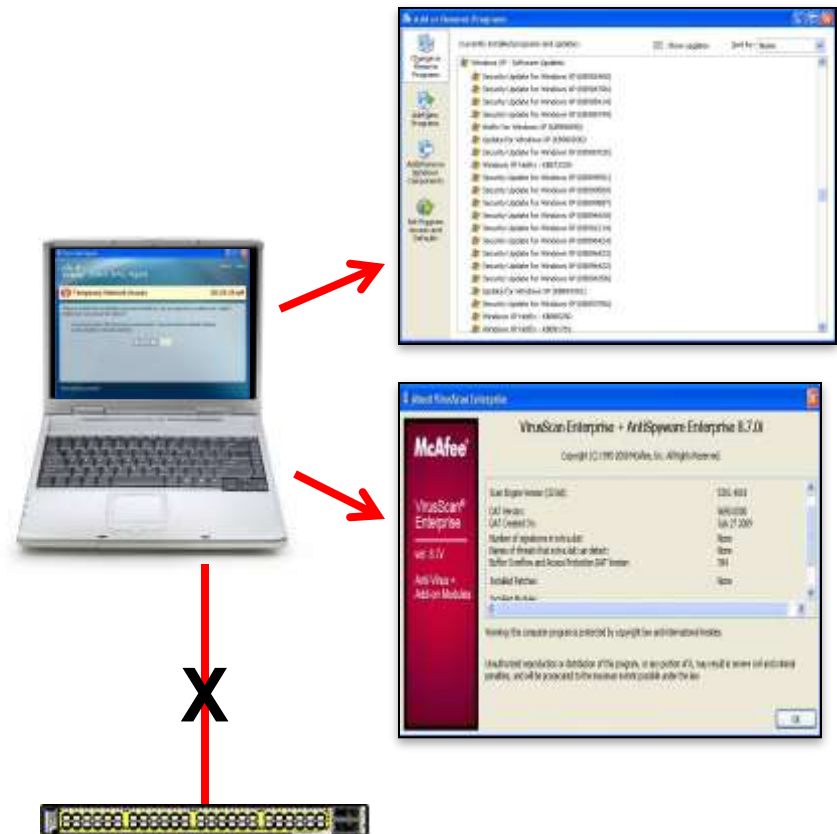
How do you centrally provision and manage guests who access your network?

PROVISION
a guest account securely

NOTIFY
your guests by print, email or SMS

MANAGE
guest network & lifecycle
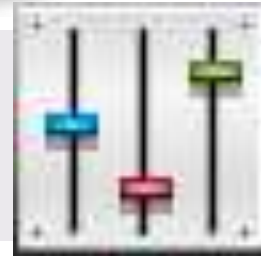
REPORT
on all aspects of guest accounts

How do you record and track non-authenticating devices in your environment?

PCs	Non-PCs			
	UPS	Phone	Printer	AP

Cisco NAC

DISCOVER	and profile all devices

MONITOR	device conformance to identity

Automated Identity & Analysis

NAC Solutions

Film #1

NAC for Campus

NAC Manager

Profiler

Guest

Device information

Device information

**NAC Server
with Collector**

**NAC Server
with Collector**

L2

L3
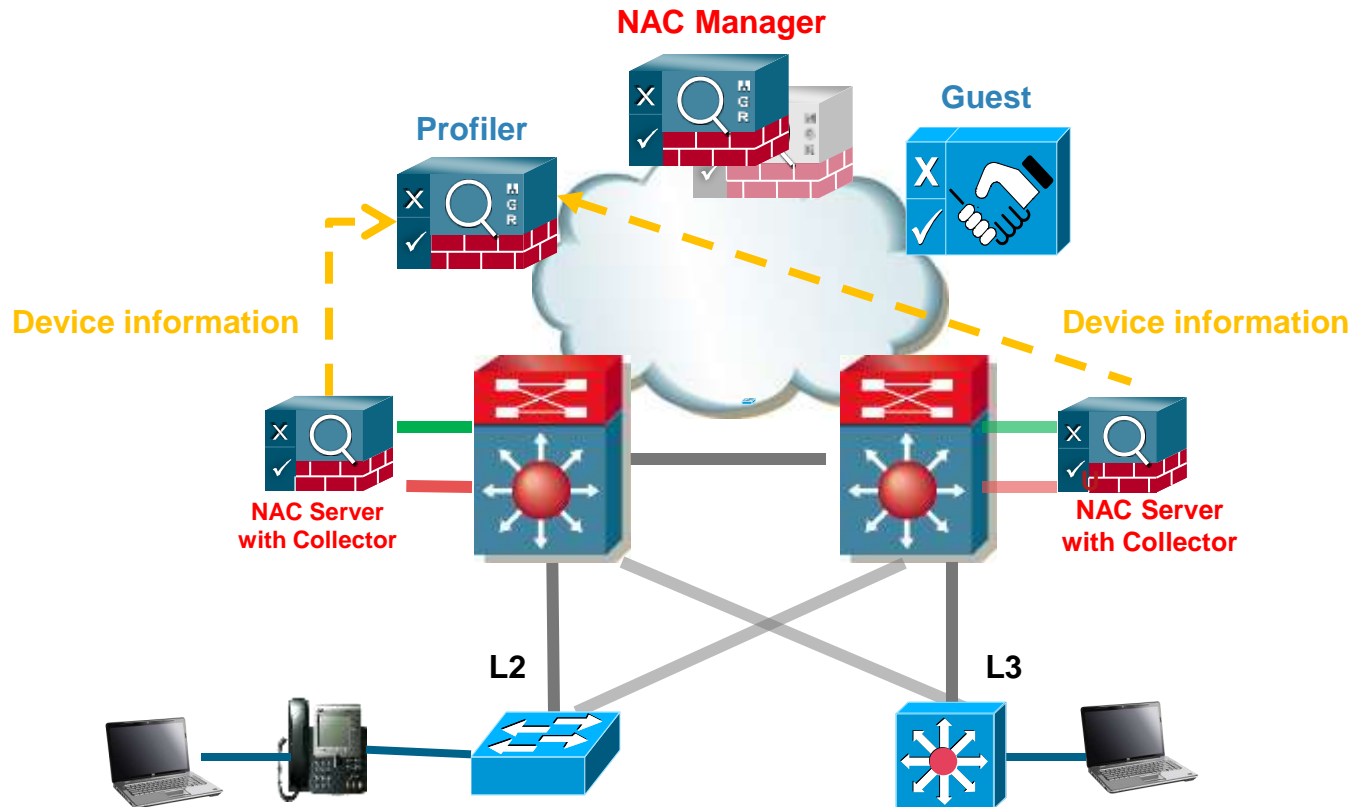
FEATURES	BENEFITS
▪ **Servers deployed in Distribution Layer** ▪ **Supports multiple access switches** ▪ **Layer 2 and Layer 3 Access support to Nac Servers**	• **Scalable solution to support up to 3,500 users per NAC server** • **Supports multiple access switches**

NAC for Branch

Branch Office

Employee

Wireless

Guest

NACS (Optional)

NAC ISR (Optional)

WAN

Central Office

Guest

NAC Manager

Device info

NAC Server with Collector (Central Deployment)

Profiler
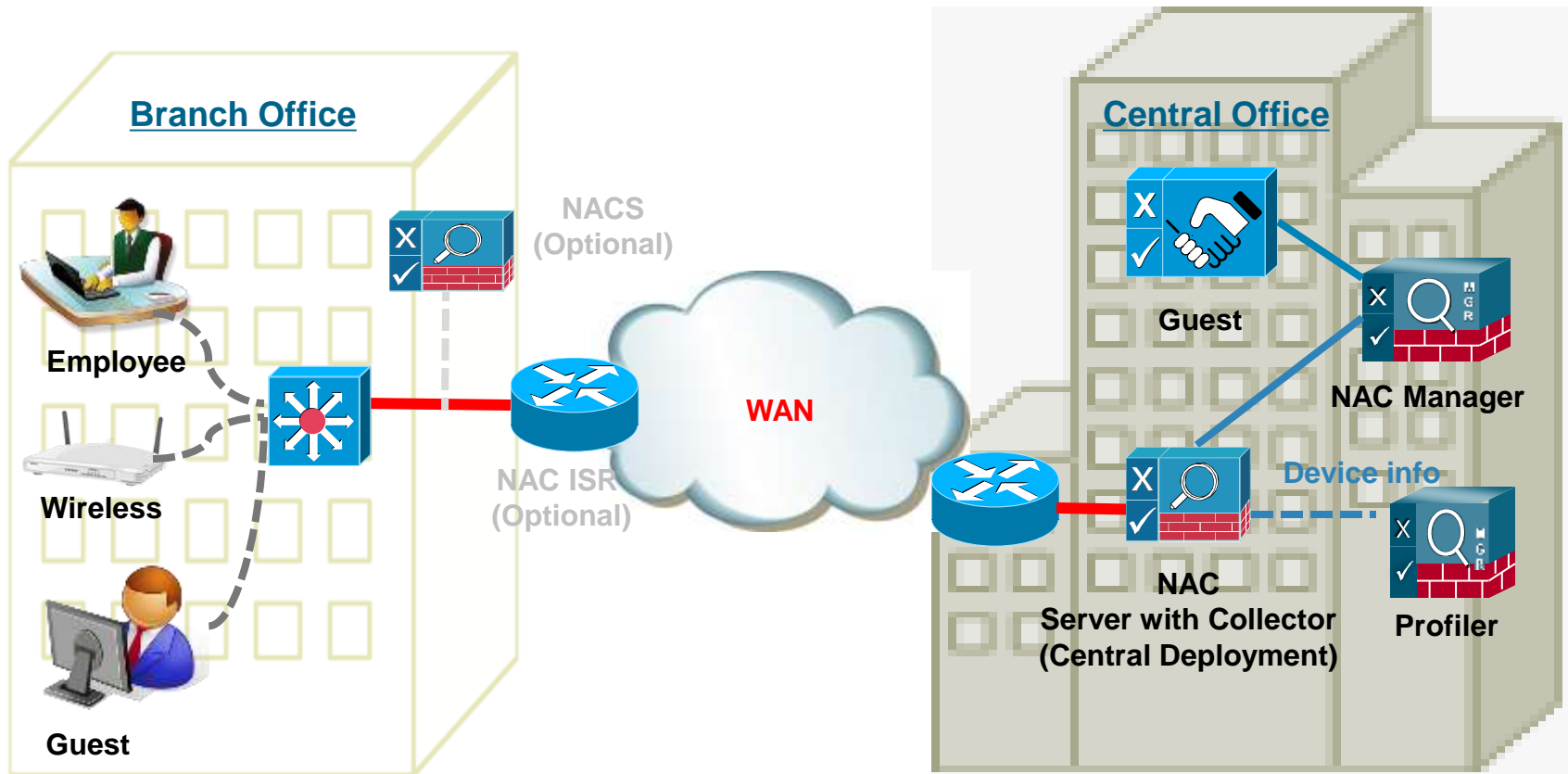
FEATURES	BENEFITS
▪ **Supports Multiple Server Deployment Options** ▪ **Ability to Control remote Branch Users** ▪ **Supports In-Band or Out of Band at branch**	▪ **Extends policy enforcement and compliance to remote Branches** ▪ **Leverages all NAC benefits to remote office**

NAC Appliance for VPN

Central Site

NAC Manager

NAC Server

Account Manager
Mobile User

AnyConnect VPN

IPSec VPN

Home Office
Unmanaged Desktop
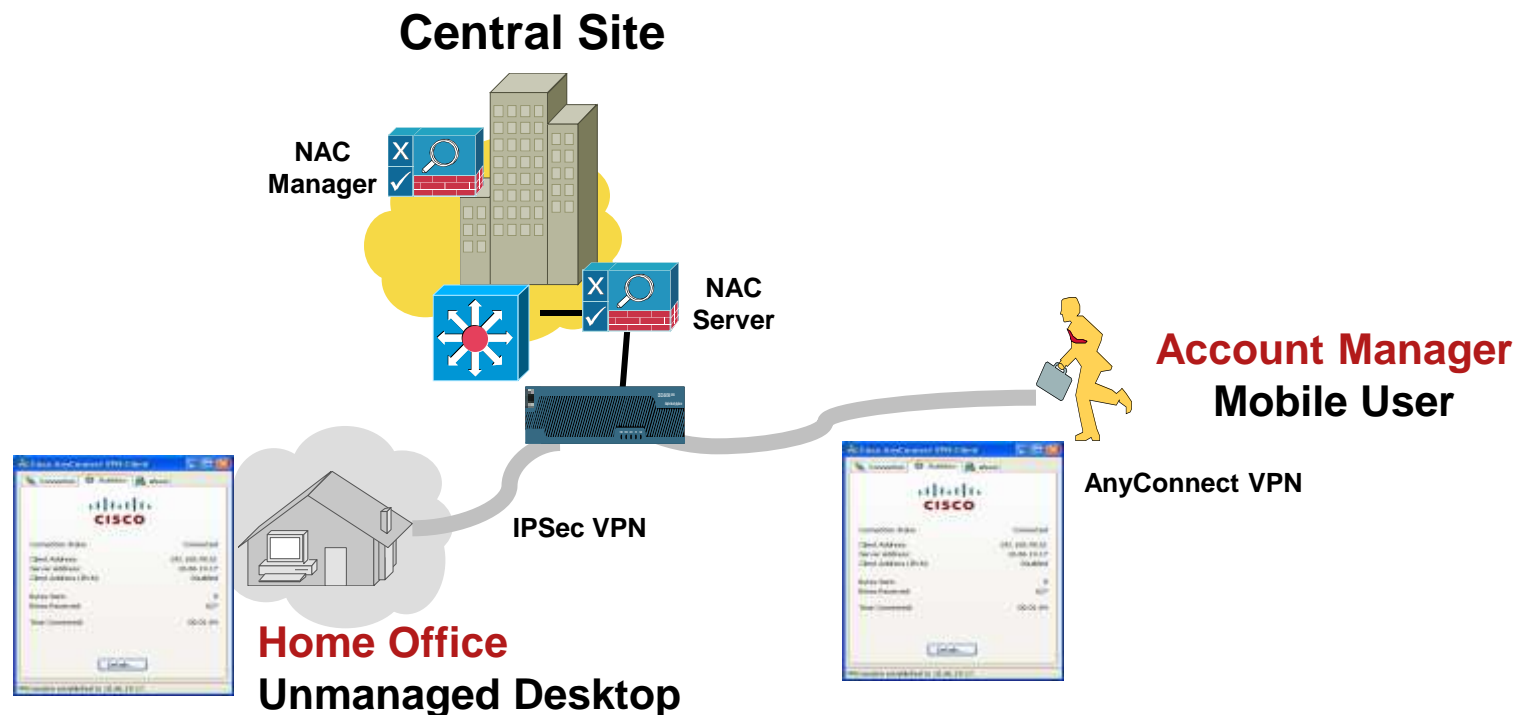
FEATURES	BENEFITS
Supports IPSec and AnyConnect VPNs **Supports site-to-site VPNs** **Supports Single sign-on** **Posture assessment after authentication**	**Extends policy enforcement and compliance to remote access and VPN users** **Extends enforcement to site-to-site VPN partners** **Leverages VPN sign-on for single-sign-on**

NAC Appliance for Wireless Users

Central Site

NACM

Guest

NACS

Wireless Network
WLSM Guest Users

802.1q

Wireless Network
LWAPP/CAPWAPP Users

802.1q

GRE

Campus Building
Wireless Users
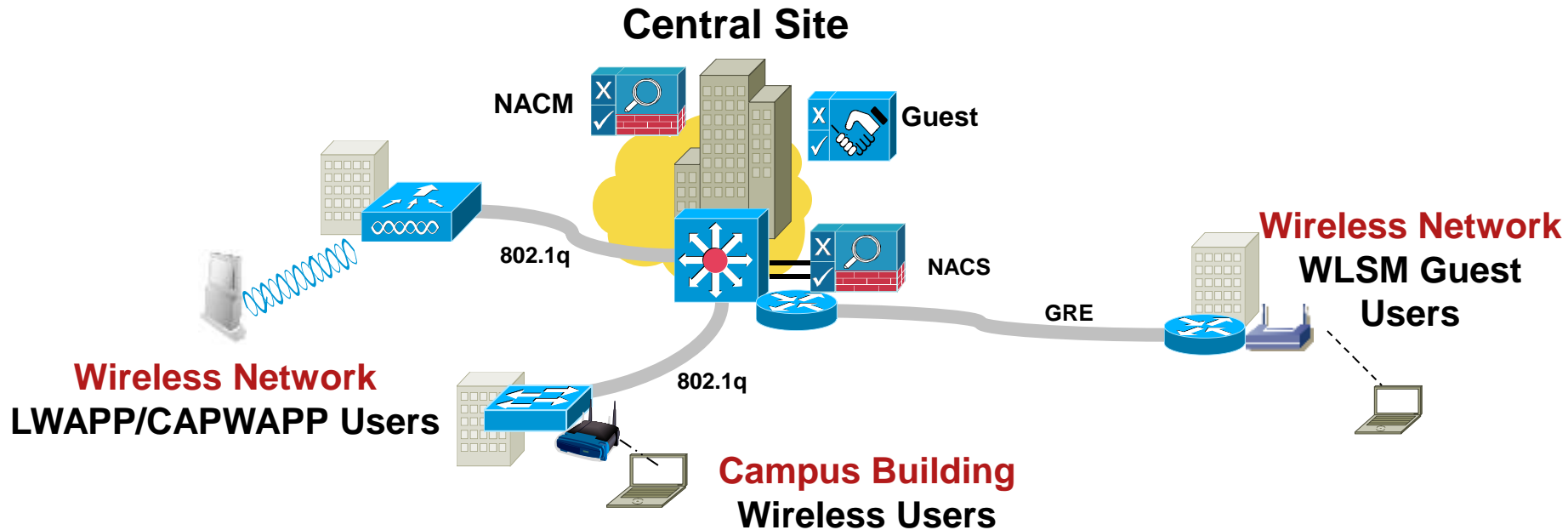
FEATURES	BENEFITS
Supports thin or thick wireless 802.11 APs **Supports Wireless user single-sign-on** **Posture after the Wireless connection** **Supports Wireless Guests** **In-Band or Out-of Band Deployments**	**Enables central deployment mode** **End user devices can be several hops away** **Extends enforcement to any wireless networks** **Leverages 802.1x sign-on for single-sign-on** **Handles Guests with Guest Server Lifecycle**

NAC Core Components
Manager and Server

NAC Manager Overview

- Controls all NAC servers centrally

- Configuration policies pushed to all servers

- Communicates with servers for status and updates

- Scalable to support multiple servers

NAC Manager

NAC Server

NAC Server

NAC Server
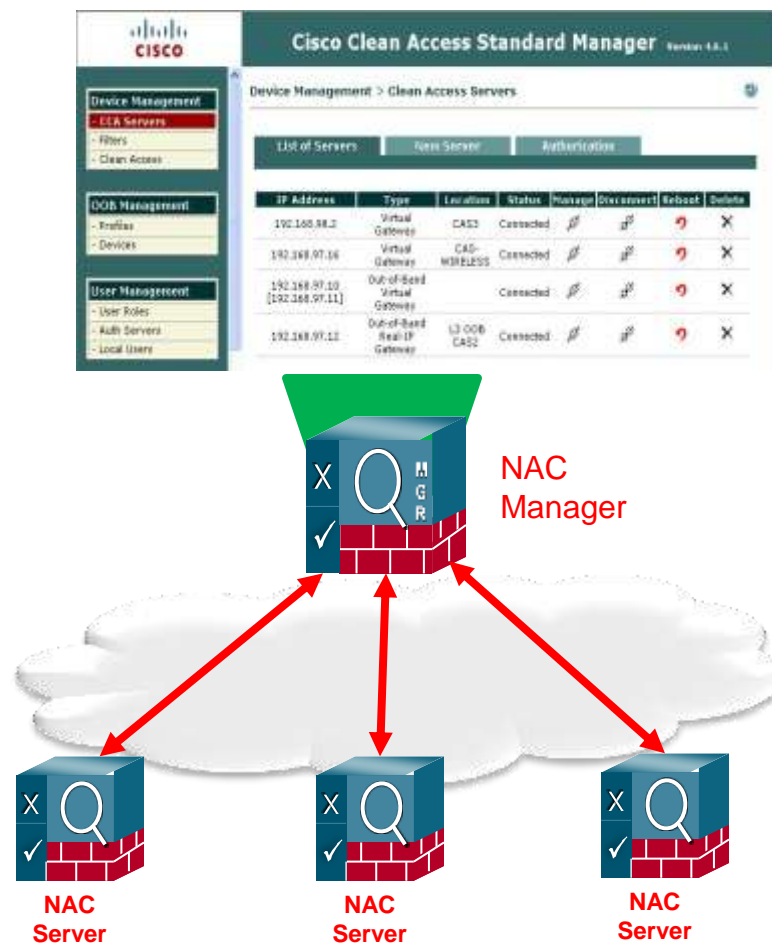
NAC Manager
Role Based Access

- **Manager uses backend authentication servers for granular control of users and role based access**
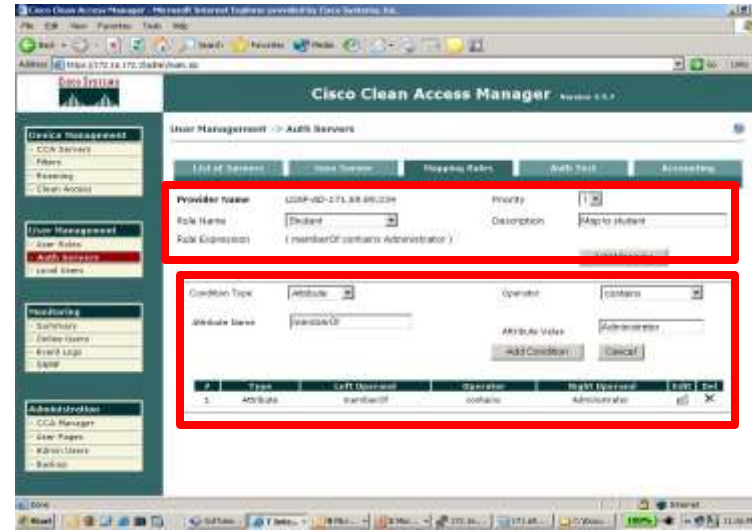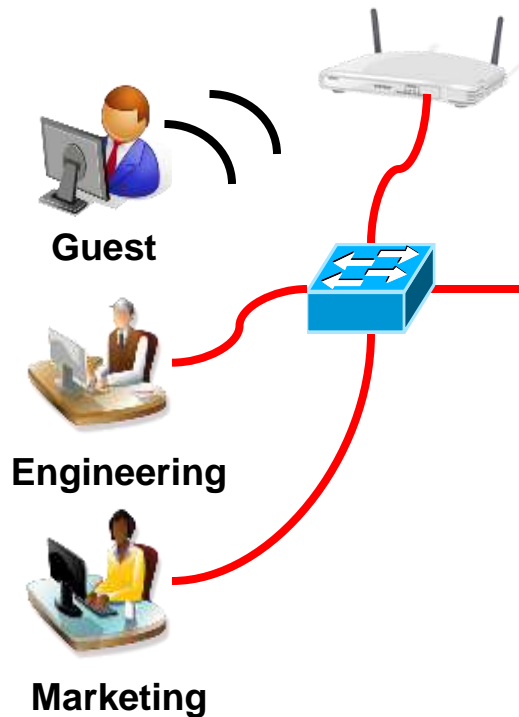
- **Active Directory Attributes**

Guest

Engineering

Marketing

NAC Server

NAC Manager

LDAP

Active Directory

Domain

Group

List of Roles		New Role		Traffic Control	Bandwidth	
Role Name	**IPSec**	**Roam**	**VLAN**	**Description**		
Unauthenticated Role	deny	deny		Role for unauthenticated users		
Temporary Role	deny	deny		Role for users to download requirements		
Quarantine Role	deny	deny		Role for quarantined users		
Allow All	deny	deny		Full Access		
Guest Access	deny	deny	:666	guest privileges		
consultant access	deny	deny	:55	consultant privileges		

NAC Manager Users and Policy

- **Maintains the List of Active Users**

- **Stores the User Roles and their corresponding Policy Controls**

- **Policies can be Traffic Control lists or Vlans by name or number**

Active users: 1 (Max users since last reset: 1)							Reset Max Users	
					Online Users 1 - 1 of 1	First	Previous	Next	Last		
User Name	**User IP**	**User MAC**	**Provider**	**Role**	**VLAN**	**OS**	**Login Time**	X
se space@SE.CCA.CISCO.COM	10.201.30.14	00:0C:29:03:21:D7	CCASE	Allow All	30	Windows 2000	01/11/07 18:35:10	☐

List of Roles	New Role		Traffic Control	Bandwidth	
Role Name	**IPSec**	**Roam**	**VLAN**	**Description**	
Unauthenticated Role	deny	deny		Role for unauthenticated users	
Temporary Role	deny	deny		Role for users to download requirements	
Quarantine Role	deny	deny		Role for quarantined users	
Allow All	deny	deny		Full Access	
Guest Access	deny	deny	:666	guest privileges	
consultant access	deny	deny	:55	consultant privileges	

NAC Manager Administration

- **Ability to add users to Manage**

- **Different levels of administration**

- **Allow Help Desk and others to help Manage NAC**

- **Full Administration or Read Only Access**

- **API Access for things like Profiler and Guest**

- **Admin Groups**

NAC Server can be deployed In-Line or Out-of-Band

NAC In-Line

- **Traffic enforcement at all times**
- **Role Based Access**

NAC Manager

NAC Server

Employee Role

Unauthenticated Role

Remediation Role

Cisco Clean Access Standard Manager
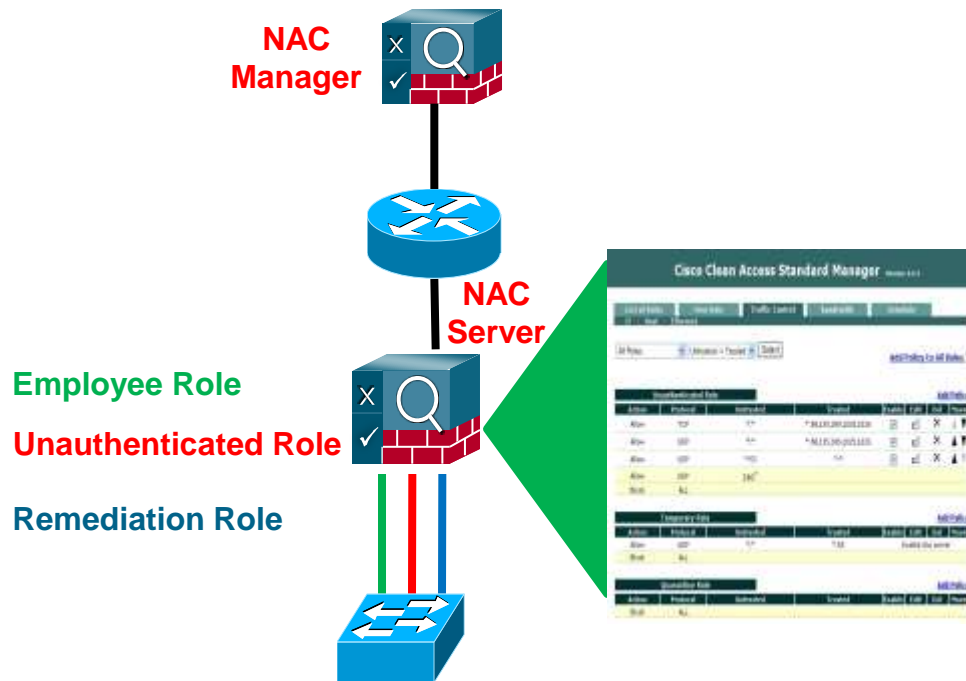
NAC Out Of Band

* Enforcement ONLY during Authentication, Posture, or Remediation

NAC Manager

NAC Server

VLAN 10

VLAN 100

* Vlan Provisioning
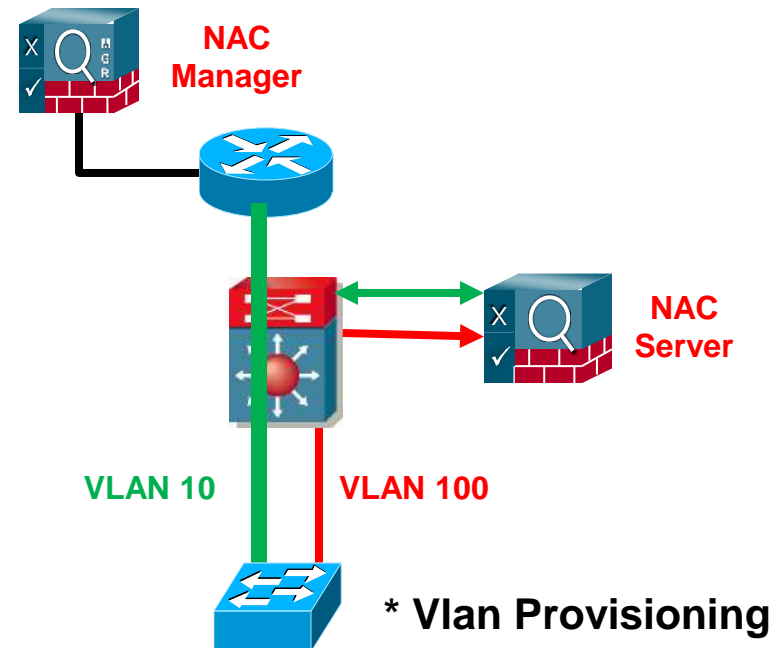
NAC Server

- **NAC Server has two key interfaces (eth0/eth1):**

    Untrusted Interface (eth1): Facing end users to be NACed

    Trusted Interface (eth0): Facing the network to be secured

- **Traffic is BRIDGED (Virtual Gateway) or ROUTED (Real IP Gateway) between the two interfaces**

VIRTUAL GATEWAY

SVI : Vlan 10

Vlan 10

eth0

Vlan 10

eth1

Frame in > Frame out

SVI : Vlan 40

Vlan 40

eth0

Map
10>>40

eth1

Vlan 10

**Frame in
VLAN-Map on Server
Frame Out**

REAL IP GATEWAY

10.10.20.0/24

eth1

10.10.10.0/24

eth0

**Packet in
Routed by Server
packet Out**
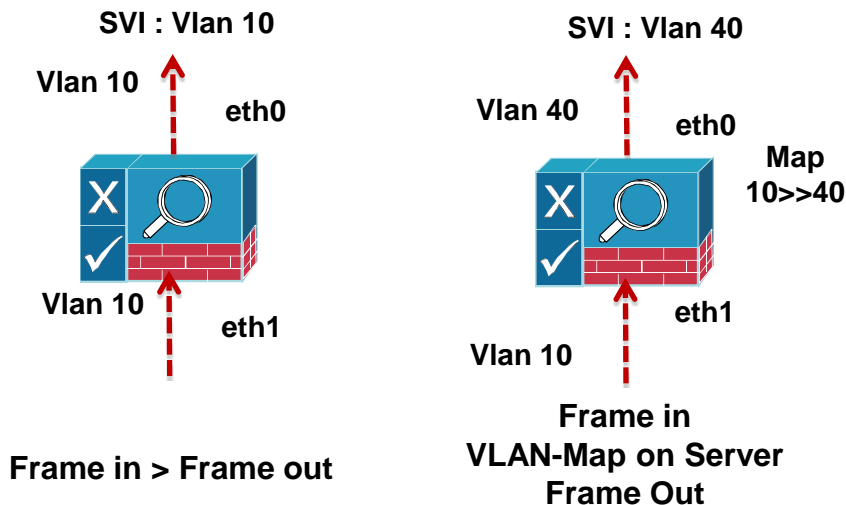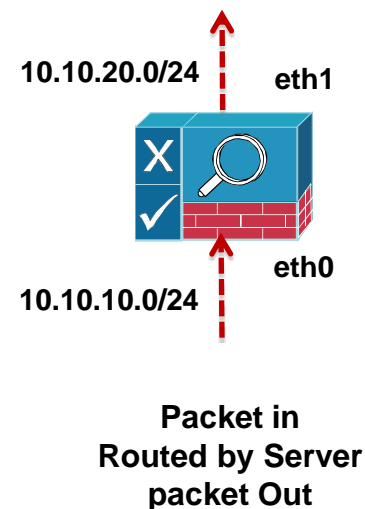
NAC Guest Component
Wired NAC Guest Access

NAC Guest Server and Users

- Who should create user accounts?

    Receptionist/Lobby Ambassador

    IT Security

    Managers

    Help Desk

    Anyone

- NAC Guest Server lets you choose based upon your security policy

- Allowing anyone to create accounts provides increased usage and will be just as secure

- Reduced Cost
- Full Audit Trail
- Speed of access
- Ease of use

Film #2
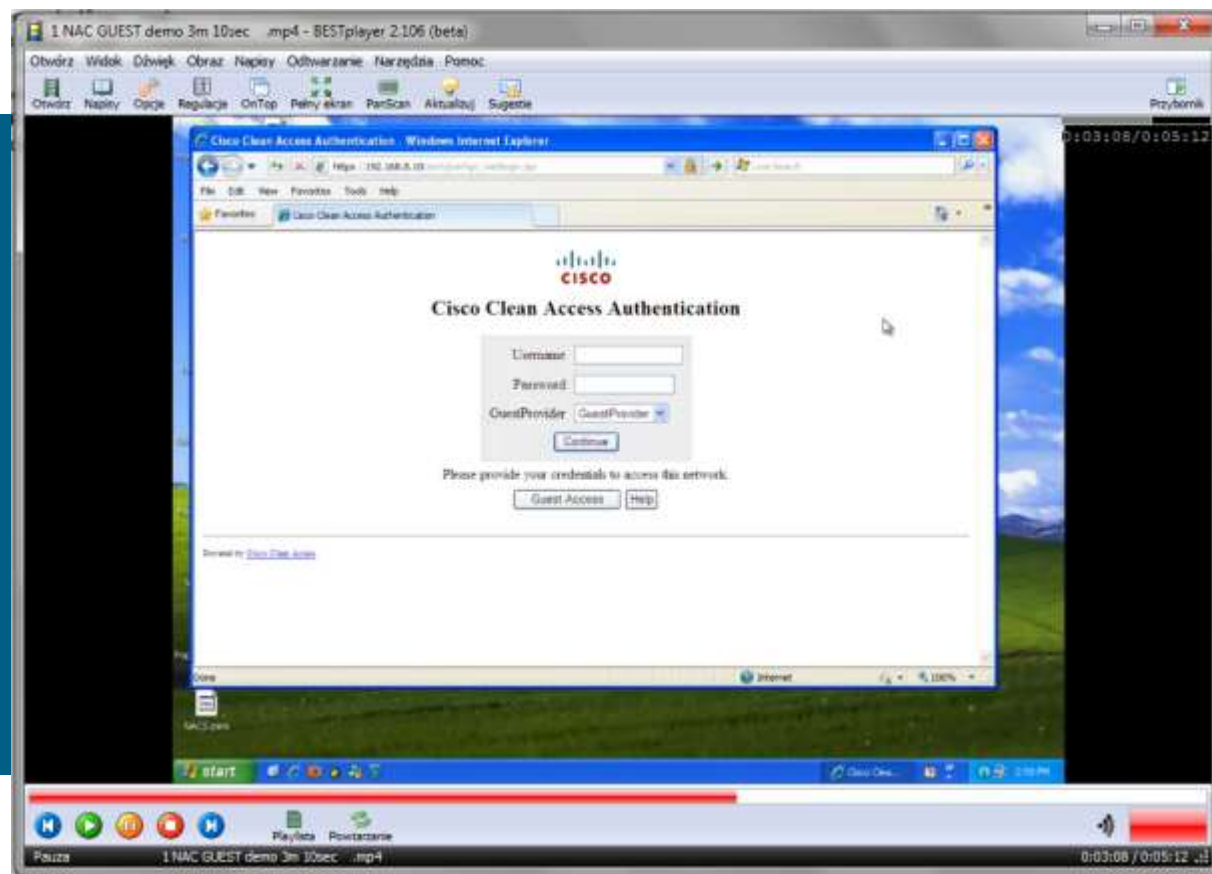
Creating Guest Accounts

1. Enter user details

2. Specify start and end times

3. Add user

Guest User Account Detail Delivery

Send account information via print-out, email, or SMS

NAC wired Guest Walkthrough

NAC Guest Server

1. Sponsor creates account on the NAC Guest Server

API
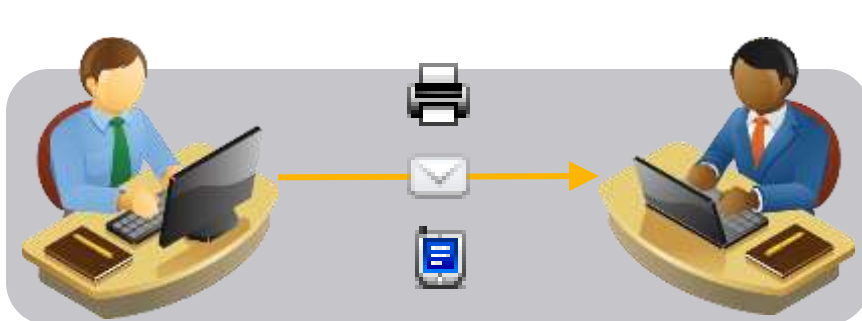
2. Sponsor gives the credentials to the guest via print-out, email or sms

3. When the account is valid the NAC Guest Server creates the account on the NAC Manager

NAC wired Guest Walkthrough

NAC Server
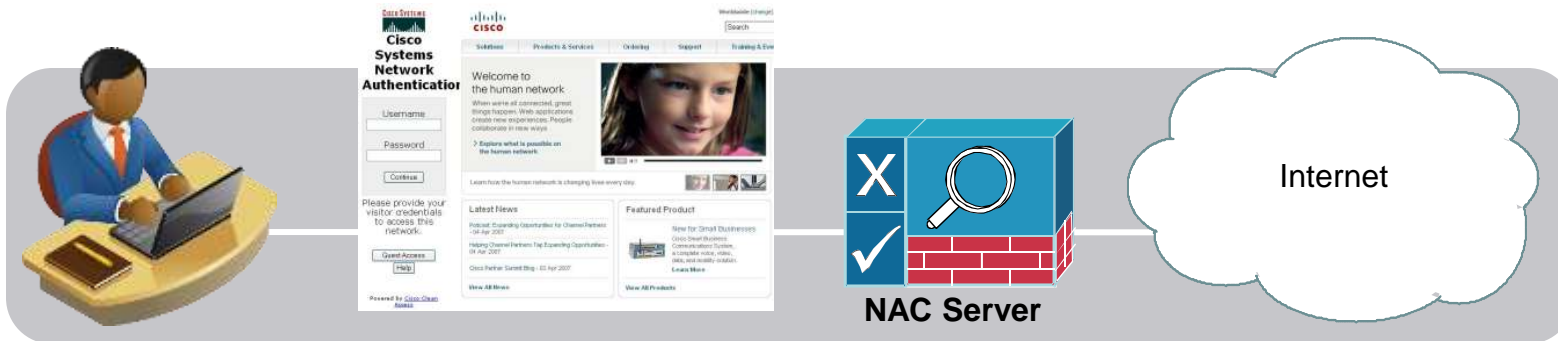
Internet

4. Guest authenticates with the web portal on the NAC Server and is given Internet access
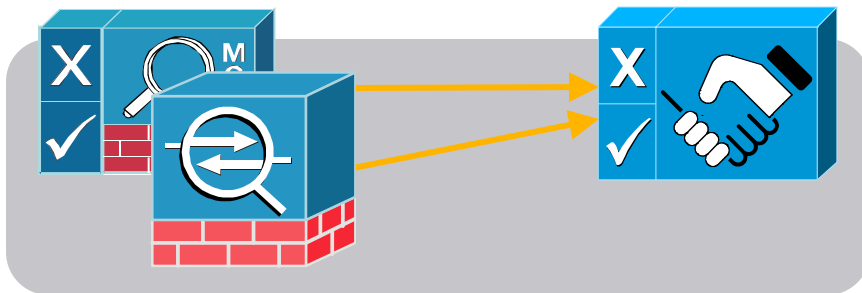
5. NAC and Firewalls provide audit information to the NAC Guest Server

API
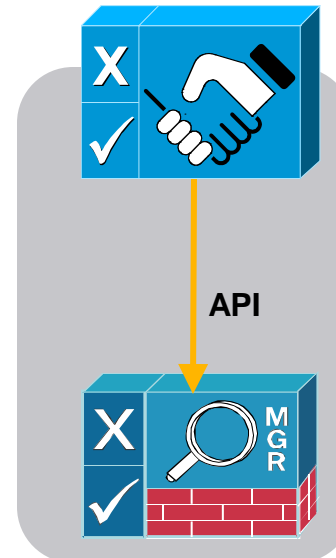
6. When the account expires the NAC Guest Server removes the account and logs off the guest

NAC Guest Component
Wireless Guests, plus Guest Reporting

NAC Wireless Guest Walkthrough

NAC Guest Server

1. Sponsor creates account on the NAC Guest Server

2. Sponsor gives the credentials to the guest via print-out, email or sms
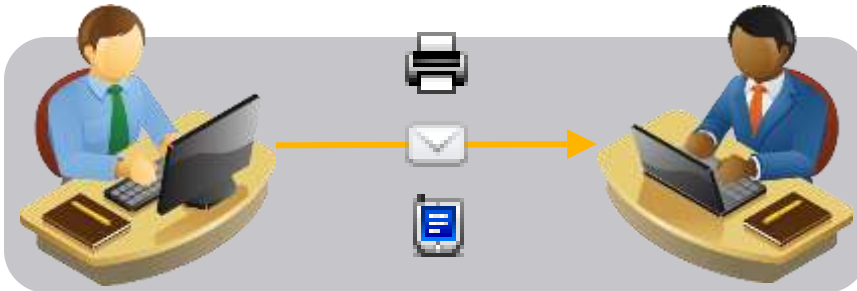
Wireless LAN Controller   **NAC Guest Server**
RADIUS
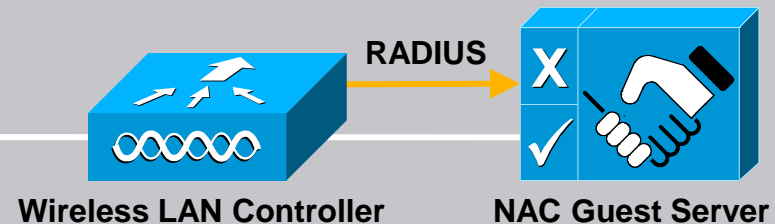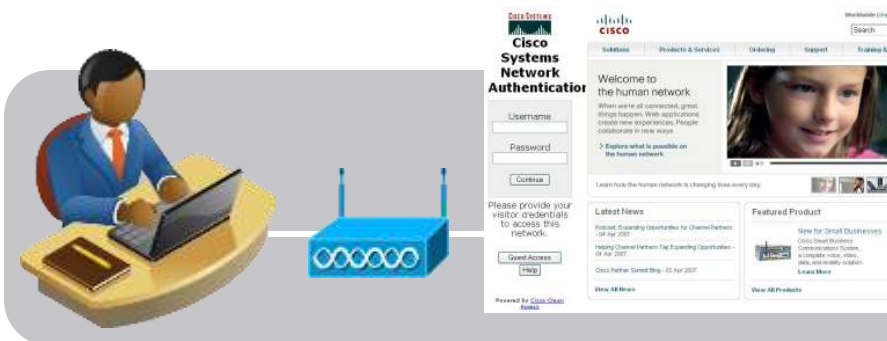
3. Guest authenticates with the web portal on the WLC which authenticates the guest by RADIUS to the NGS

NAC Wireless Guest Walkthrough

Internet

Wireless LAN Controller
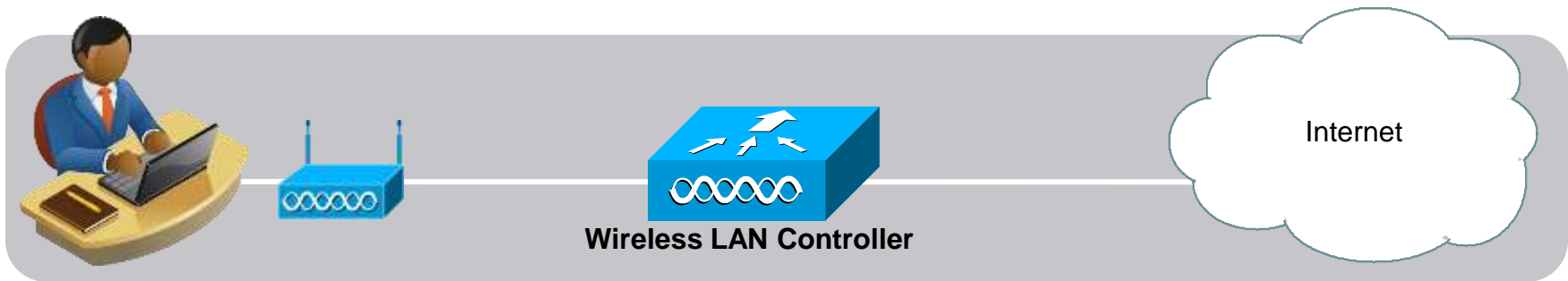
4. If auth is successful the guest is given Internet access
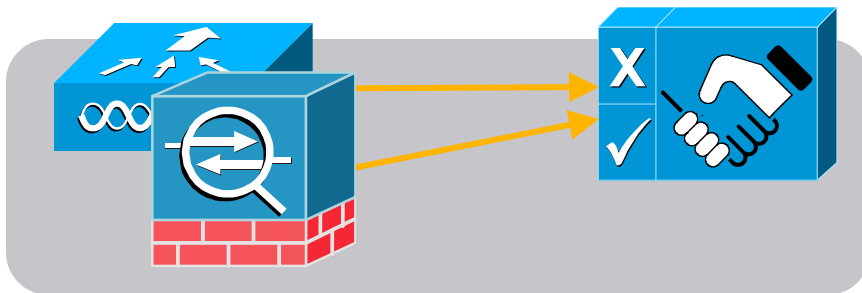
5. Wireless LAN Controller and Firewalls provide audit information to the NAC Guest Server
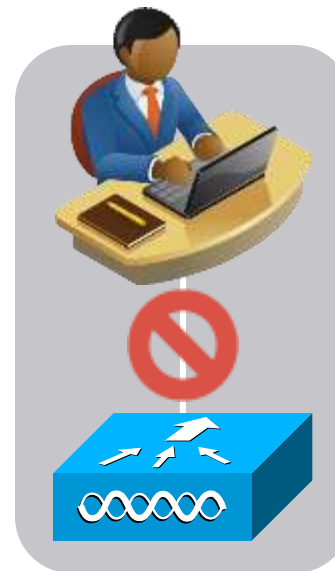
6. When the account expires the Wireless LAN Controller logs off the guest

Audit and Reports

Visibility and Management of Guest Users

Status: Inactive,Active,Expired,Suspended; Start Time between 13-Dec-2008 and 11-Feb-2009   (Advanced Search >>)

(Download CSV)

Cisco NAC Guest Server Reporting   Showing 1-4 of 4   [10 $\updownarrow$]   Per Page

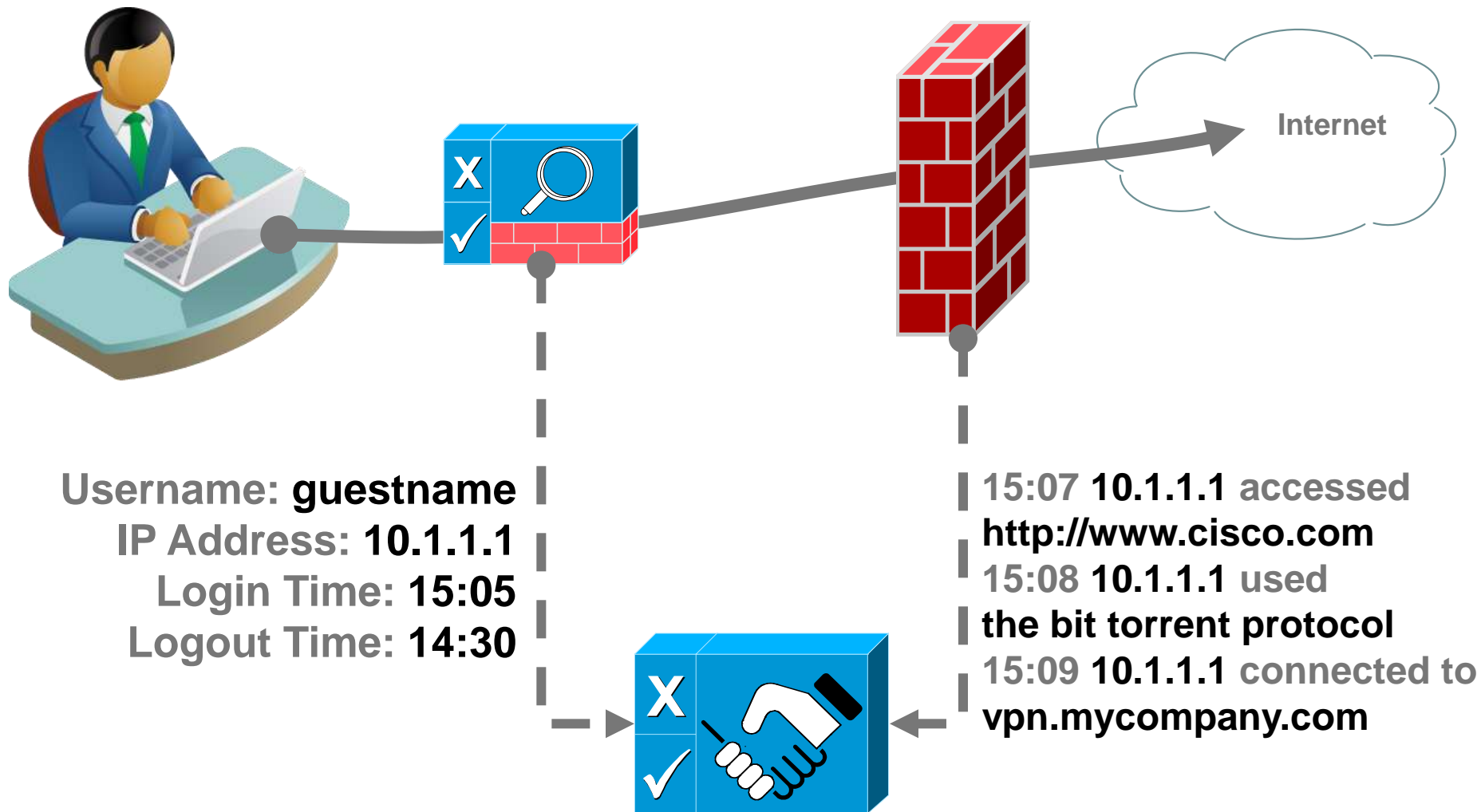| Created By ▲▼	Username ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Email ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
duarte	jcarter@policyapp.com	-sY5Nmzb	John	Carter	jcarter@policyapp.com	Suspended	12-Jan-2009 7:42 AM America/Los_Angeles	12-Jan-2009 11:59 PM America/Los_Angeles	✏🗒🖨✉📋
mark	rooney@manutd.com	*ckI0IMT	Wayne	Rooney	rooney@manutd.com	Active	12-Jan-2009 7:41 AM America/Los_Angeles	12-Jan-2009 11:59 PM America/Los_Angeles	⊘✏🗒🖨✉📋
niall	jsmith@mycustomer.com	ZYy:X9PW	John	Smith	jsmith@mycustomer.com	Inactive	12-Jan-2009 9:00 AM America/Los_Angeles	12-Jan-2009 5:30 PM America/Los_Angeles	⊘✏🗒🖨✉📋
niall	jsmith@mycustomer.com	GpOCK8*j	john	smith	jsmith@mycustomer.com	Expired	10-Jan-2009 5:52 PM America/Los_Angeles	10-Jan-2009 11:59 PM America/Los_Angeles	✏🗒🖨✉📋

Page [1] of 1
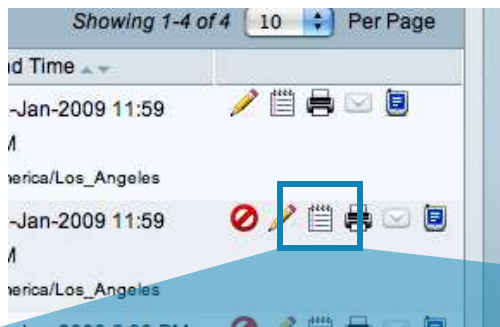
Sponsor Information

Guest Information

Account Management

Guest Activity Reporting

Internet

Username: guestname
IP Address: 10.1.1.1
Login Time: 15:05
Logout Time: 14:30

15:07 10.1.1.1 accessed
http://www.cisco.com
15:08 10.1.1.1 used
the bit torrent protocol
15:09 10.1.1.1 connected to
vpn.mycompany.com

Consolidated Audit Report of Guest Activity

Detailed guest audit information

- **When** they logged in
- **Where** they logged in
- The guests **address**

- **What** they did
- What was **allowed**
- What was **disallowed**

Detailed Login Report for: jsmith@mycustomer.com   Showing 1-1 of 1 | 10 | Per Page

NAS IP Address ▲ ▼	Users IP Address ▲ ▼	Logged In ▲ ▼	Logged Out ▲ ▼	Duration
192.168.137.20	1.0.0.7	12:-Jan-2009 9:31 AM	12-Jan-2009 9:45 AM	14 Minute(s)

Page 1 of 1

Activity Log: jsmith@mycustomer.com   Showing 1-3 of 3 | 10 | Per Page

Date/Time ▲ ▼	Device ▲ ▼	Message ▲ ▼
12-Jan-2009 9:31 AM	192.168.137.20	1.0.0.7 TCP connection permitted to 198.133.219.25:80
12-Jan-2009 9:31 AM	192.168.137.20	1.0.0.7 accessed URL http://www.cisco.com
12-Jan-2009 9:32 AM	192.168.137.20	1.0.0.7 TCP connection denied to 204.65.34.23:4662

Page 1 of 1

NAC Endpoints
Agent Types, Posture, and Profiling

Installed Agent, Web Agents, or Agent-less

NAC Full Agent

NAC Web Agent

Web Authentication

Deploy different agents for different Users/Roles

Cisco NAC Agent

- **Users and endpoints communicate with NAC through the NAC Agents**

NACServer

SSL

SSL

NAC Manager
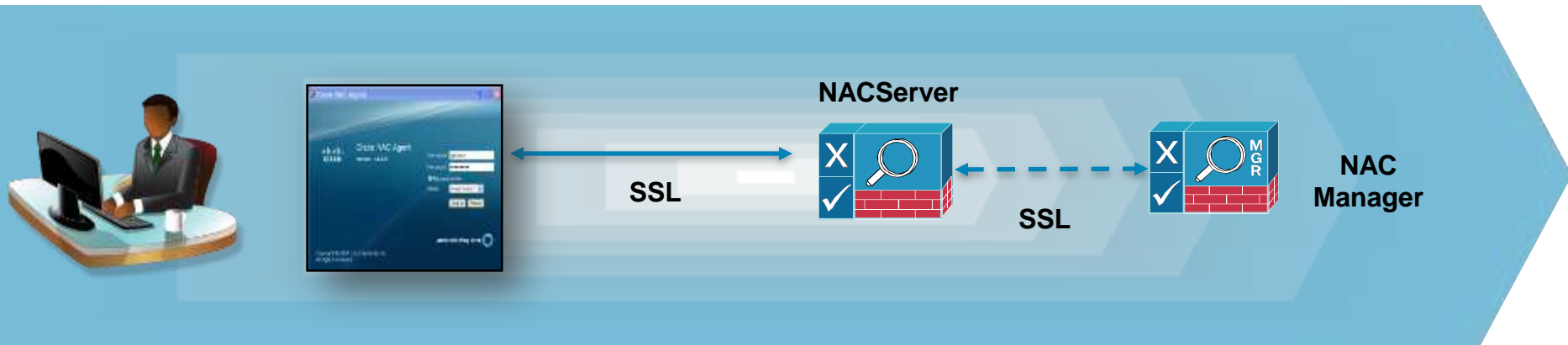
- **NAC Agent is vital to check and remediate all devices trying to connect to your network.**

- **NAC Agent has full system control and Auto-Remediation capabilities**

- **64-Bit OS Support XP and Vista**
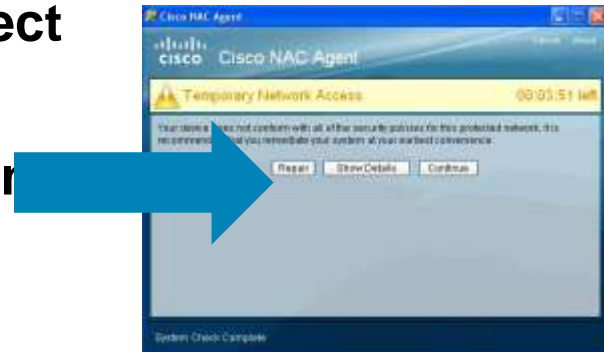
NAC Agent Single Sign-on

- **Active Directory Support**

- **VPN and Wireless support via**

  Radius Attributes

- **No need for additional credentials**

- **Creates seamless user flow and experience**
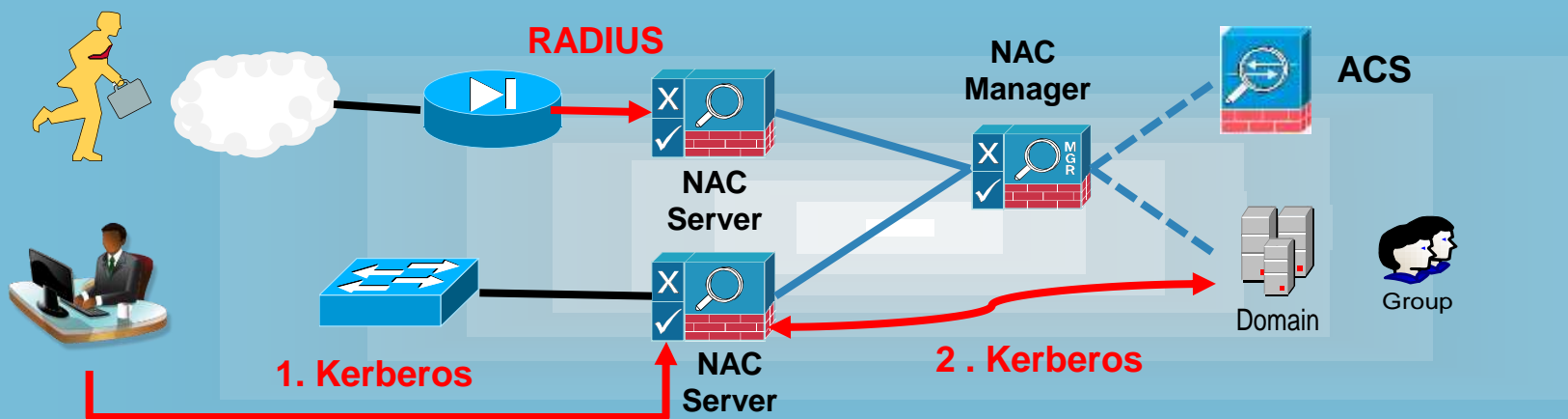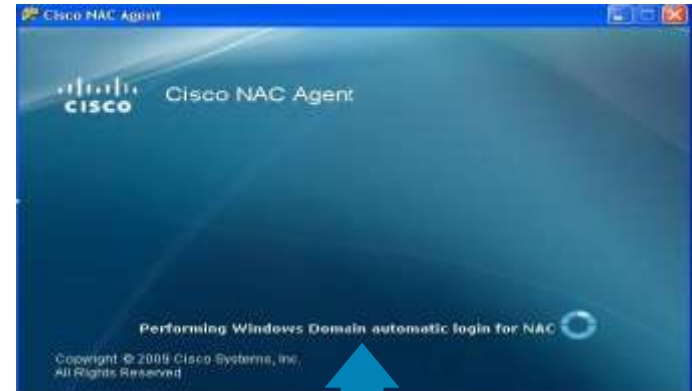
Cisco NAC Web Agent
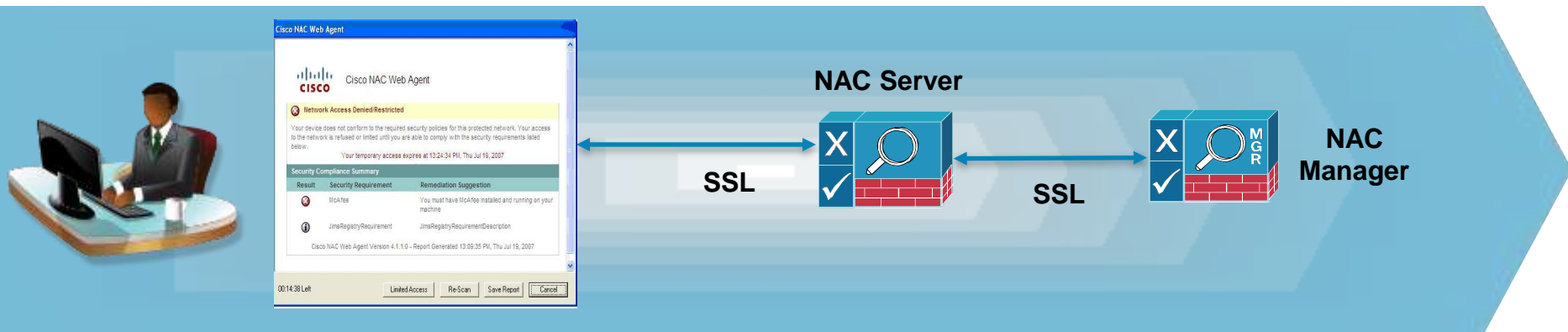
- **Agent launches during authentication and Posture assessment**

- **Removed after the login session**

- **Supports all browsers by the way of Active-X or Java Applet**

- **NAC Web Agent does posture assessment and tells user what requirements have passed or failed**

NAC Agent - MAC OS Support

MAC OS X	NAC Agent	Posture	Authentication	Remediation
10.2	4.1.3 or >	No	Yes	No
10.3	4.1.3 or >	No	Yes	No
10.4	4.1.3 or >	Yes	Yes	Yes
10.5	4.1.3 or >	Yes	Yes	Yes

NAC Posture

NAC Posture: Checks, Rules, and Roles

NAC posture validation is a hierarchical process with either pre-loaded or custom profiles

CHECKS
assess the state of a file, application, service, or registry key

RULES
contain single or multiple Checks

REQUIREMENTS
contain single or multiple Rules
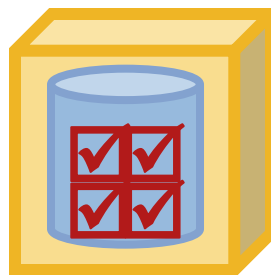
ROLES
have one or more Requirements
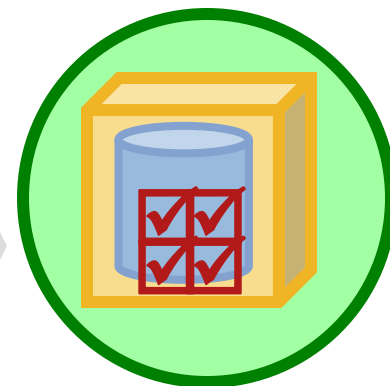
NAC Agent: Posture Assessment

Validate the compliance of
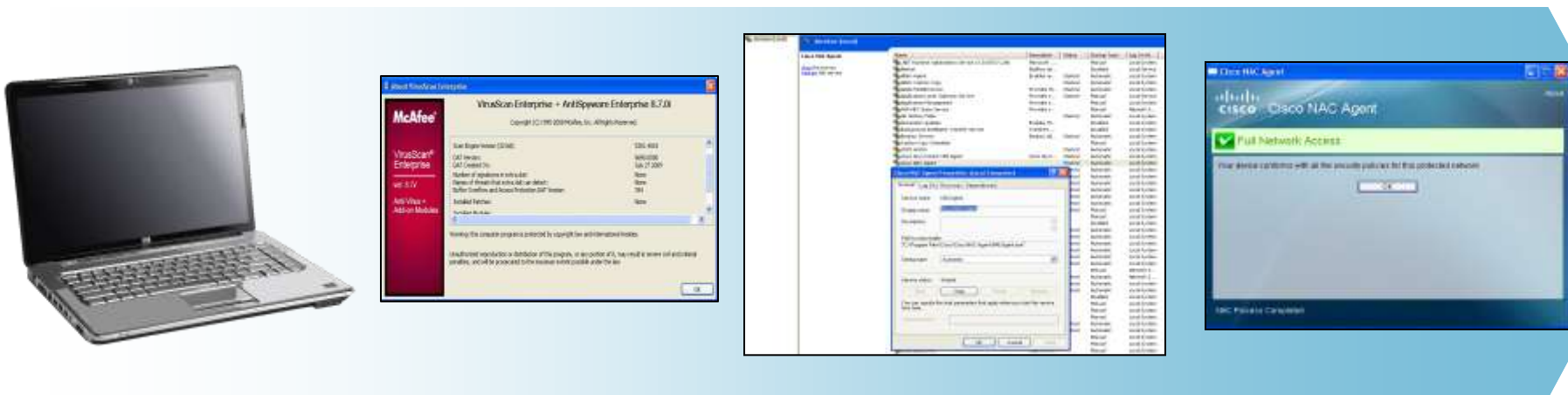
Anti-Virus
Anti-Spyware
Windows Files

Registry Entries
Services
Applications

NAC Agent Remediation

- **When Requirements Fail, Remediation kicks in**

- **Remediation can be automatic to update AV and AS**

- **AV update service is launched by the NAC Agent**

- **Allows Devices to self remediate before accessing the network**

- **IT Staff has more time to tend to other problems**
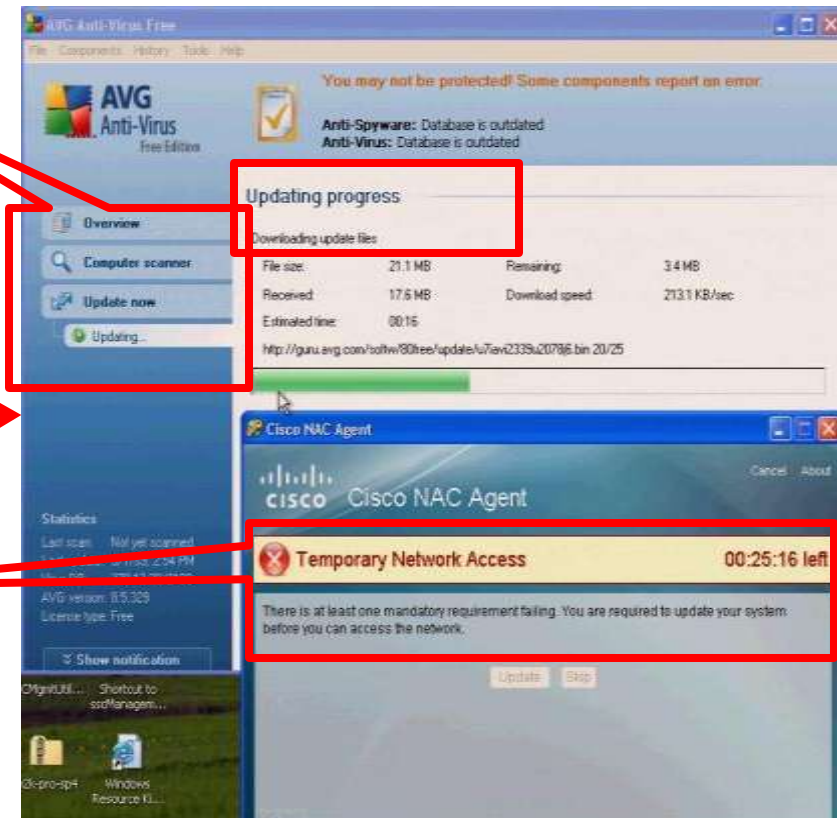
Cisco NAC Services
Automated Policy Updates

Automated Cisco Rulesets

Simplify support for over 350+
security and management applications

AutoUpdates Hotfixes,
Service Packs
(direct to WSUS Server)

Cisco NAC Manager

NAC Non-Authenticating Devices

NAC Gap: Non-PC Endpoint Devices

Do you have a full record of devices on the network?

Enterprises without VoIP
Wired Endpoints Distribution

50% Windows

50% Other
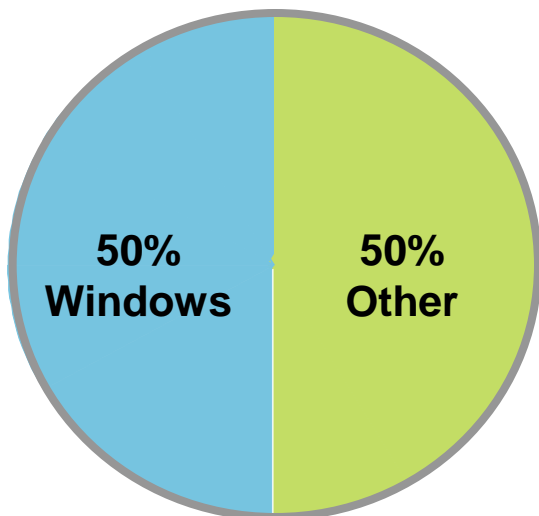
Enterprises with VoIP
Wired Endpoints Distribution

33% Windows

33% IP phones

33% Other
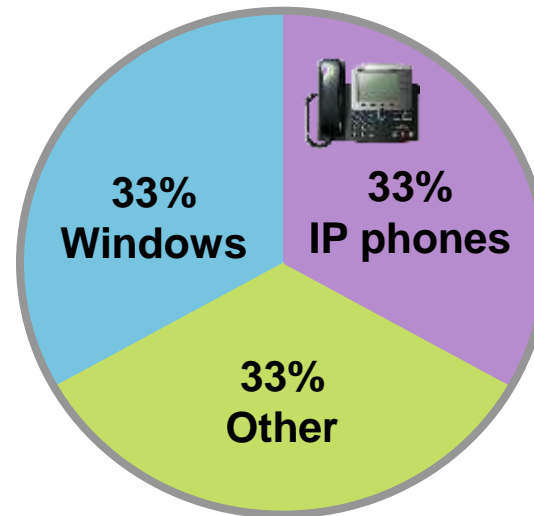
How do you create and manage non-authenticating devices in your environment ?

- NAC Profiler can manage all other non-authenticating devices

- Automatic Discovery and Inventory via SNMP

- Profiles Devices into NAC Roles

SPAN

NACS/Collector

SNMP

PROFILER

API

NACM

- **Devices added to Filter List from Profiler**
- •Devices get proper access under NAC

Build Device Inventory in NAC Profiler

NAC Profiler Server aggregates the information and maintains a database of all network-attached endpoints

Dynamic Provisioning into NAC Manager

NAC Profiler profiles device and automatically places it in the NAC Manager filter list

Detailed Device Information

Summary

Cisco NAC Addresses Customer Needs

Solves Customer Pain Points Today

- Identity-based access control; guest handling
- Endpoint policy enforcement
- Compliance requirements

Most Comprehensive NAC Solution

- Flexible deployment options
- Covers all use cases

Improves Security and IT Operations

- Secures wired, secure wireless, and compliance solutions
- Reduces complexity and operational costs

Additional Resources

Further Information at:

http://www.cisco.com/go/nacappliance

Po przerwie (15 min.) – nowa generacja Cisco NAC: Cisco ISE