



NAC Appliance



Jeff DiMaio
CISSP
Systems Engineer
Cisco Systems

CBC Grand Opening- October 20

- Agenda
- 12:30–1:00 p.m. Registration
- 1:00–1:30 p.m. Leading Life's Experiences,
- Are You Ready?—Carl Wiese, Vice President, Advanced Technology
- 1:30–2:15 p.m. Network as the Platform- Tracey Newell, Area Vice President
- 2:15–2:30 p.m. Break
- 2:30–3:30 p.m. Customer Panel hosted by Jeff Sharritts, Operations Director, and Lisa Loftus, Regional Sales Manager
- 2:30 -3:30 p.m. CBC Tours
- 3:30–4:30 p.m. Reception

Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features**
4. **Clean Access Server Foundation Concepts**
5. **NAC Appliance Technical Benefits**



Productivity Causes Complexity



WHAT SYSTEM IS IT?

Windows, Mac or Linux
Laptop or desktop or PDA
Printer or other corporate asset

WHO OWNS IT?

Company
Employee
Contractor
Guest
Unknown

WHERE IS IT COMING FROM?

VPN
LAN
WLAN
WAN

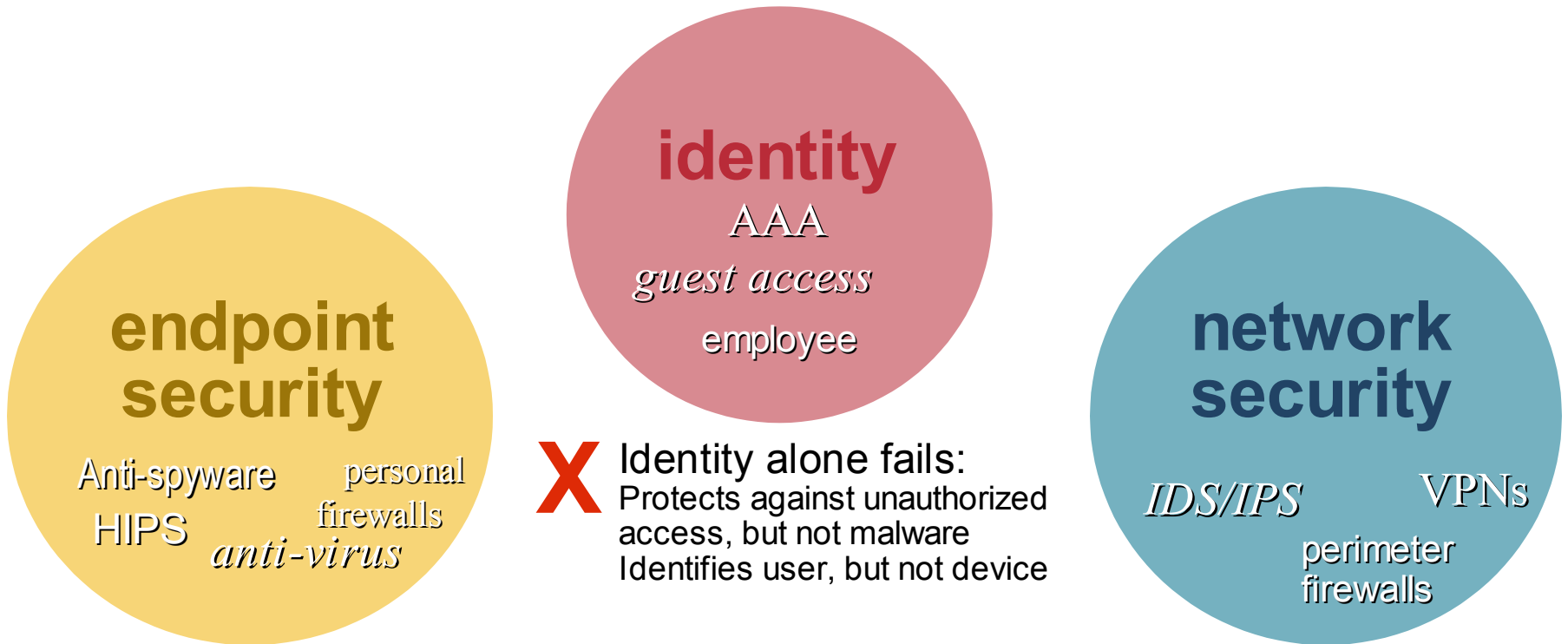
WHAT'S ON IT?
IS IT RUNNING?

Anti-virus, anti-spyware
Personal firewall
Patching tools

WHAT'S THE PREFERRED WAY TO CHECK/FIX IT?

Pre-configured checks
Customized checks
Self-remediation or auto-remediation
Third-party software

Complexity Demands Defense-in-Depth



X Identity alone fails:
Protects against unauthorized access, but not malware
Identifies user, but not device

X Endpoint security alone fails:
99% have AV, but infections persist!
Host based apps are easily manipulated—even unintentionally
Time gap between virus and virus def/repair

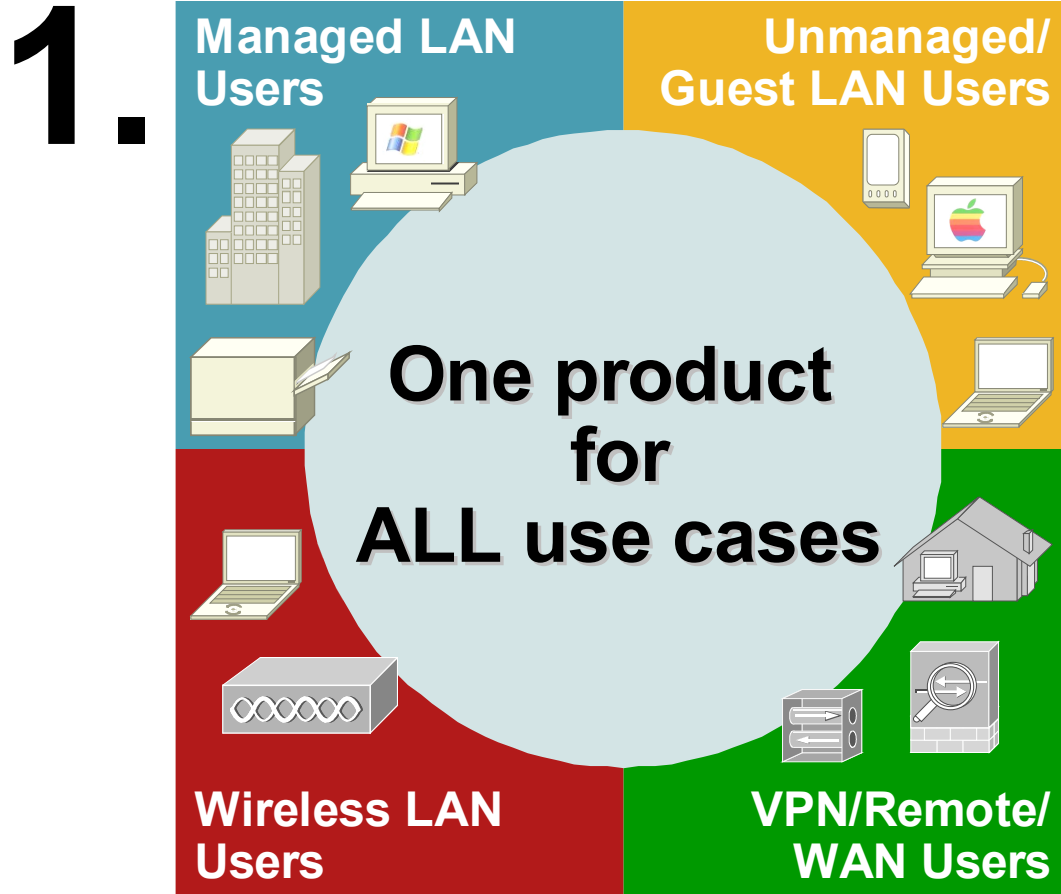
X Network security alone fails:
Firewalls cannot block legitimate ports
VPNs cannot block legitimate users
Malware signatures must be known
Detection often occurs after-the-fact

Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features**
4. **Clean Access Server Foundation Concepts**
5. **NAC Appliance Technical Benefits**



NAC Appliance



- 2.** 600+ customers across all use cases: No. 1 NAC solution
- 3.** Most deployments ready under 5 days
- 4.** Scales from 100 users to 100,000+ user, across 150+ locations
- 5.** Does not require infrastructure upgrade

NAC Appliance Overview

All-in-One Policy Compliance and Remediation Solution



AUTHENTICATE & AUTHORIZE

- Enforces authorization policies and privileges
- Supports multiple user roles

SCAN & EVALUATE

- Agent scan for required versions of hotfixes, AV, and other software
- Network scan for virus and worm infections and port vulnerabilities

QUARANTINE

- Isolate non-compliant devices from rest of network
- MAC and IP-based quarantine effective at a per-user level

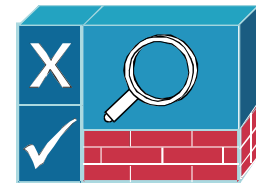
UPDATE & REMEDIATE

- Network-based tools for vulnerability and threat remediation
- Help-desk integration

NAC Appliance Overview: Components

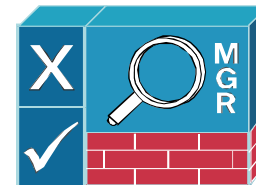
- Cisco Clean Access Server

Serves as an in-band or out-of-band device for network access control



- Cisco Clean Access Manager

Centralizes management for administrators, support personnel, and operators



- Cisco Clean Access Agent

Optional lightweight client for device-based registry scans in unmanaged environments



- Rule-set Updates

Scheduled automatic updates for anti-virus, critical hot-fixes and other applications



NAC Appliance Overview: Components

Critical Windows Updates

**Windows XP, Windows 2000,
Windows 98, Windows ME**



Anti-Virus Updates



Anti-Spyware Updates

Other 3rd Party Checks



Customers can easily add customized checks

User Experience with Agent

Login Screen



Cisco Clean Access Agent

Clean Access Agent

Please enter your user name and password:

User Name :

Password :

Remember Me

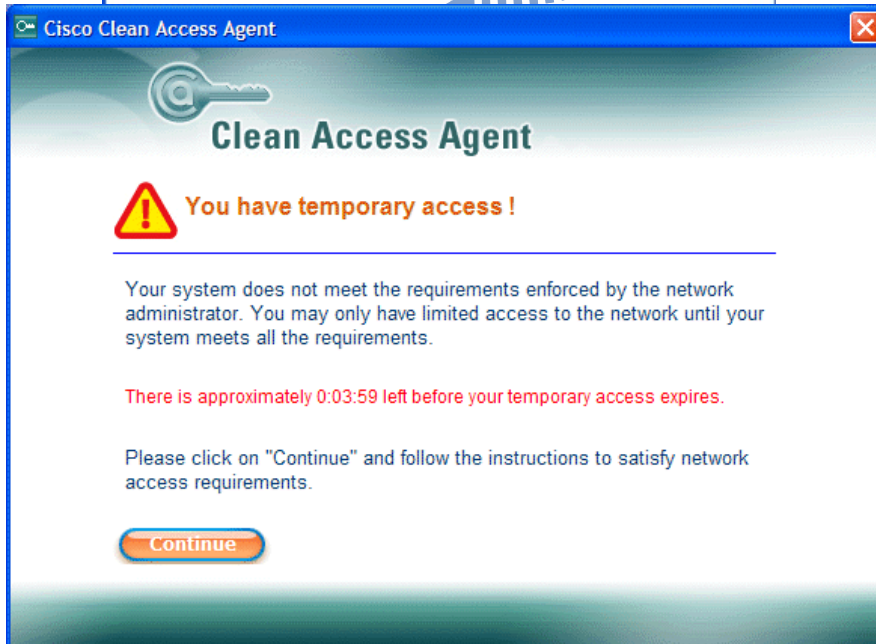
Please select your authentication provider:

Local DB

Scan is performed
(types of checks depend on user role)

Scan fails

Remediate



Cisco Clean Access Agent

Clean Access Agent

! You have temporary access !

Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.

There is approximately 0:03:59 left before your temporary access expires.

Please click on "Continue" and follow the instructions to satisfy network access requirements.

Continue



Cisco Clean Access Agent

Clean Access Agent

! Please download and install the required software before accessing the network.

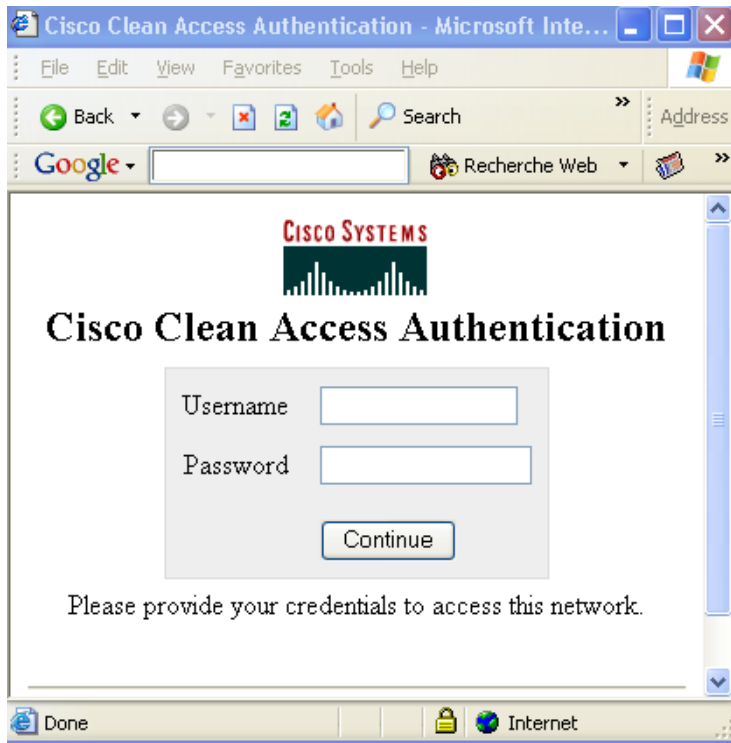
Required Software (0:03:10 left)

Name : Anti-Spyware (Optional) Software
Version :
Location : <http://www.lavasoft.com/support/download/>

Description : Our security policy recommends that you download an anti-spyware program. Click Go To Link to download a free Anti-Spyware program or click Next to skip.

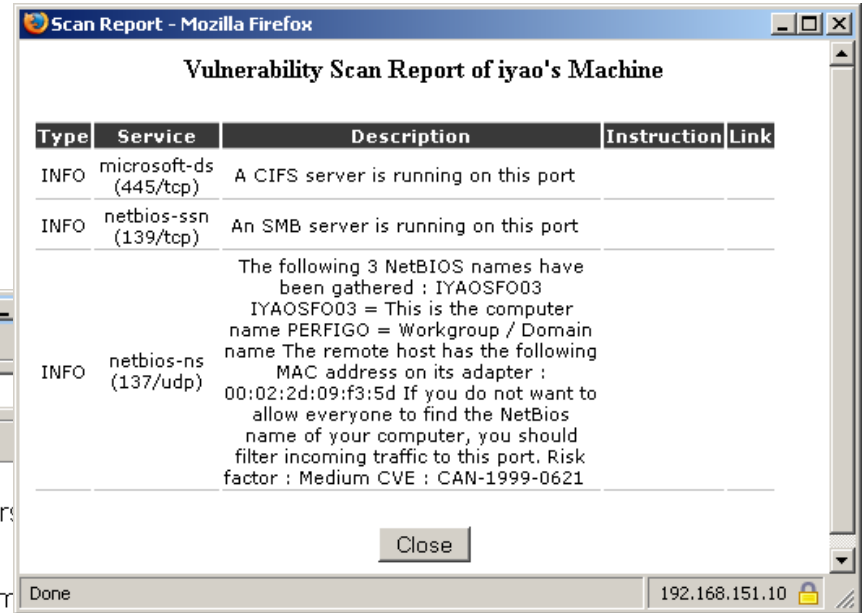
Go To Link **Next** **Cancel**

User Experience via Web Browser



Login Screen

Scan is performed (types of checks depend on user role/OS)



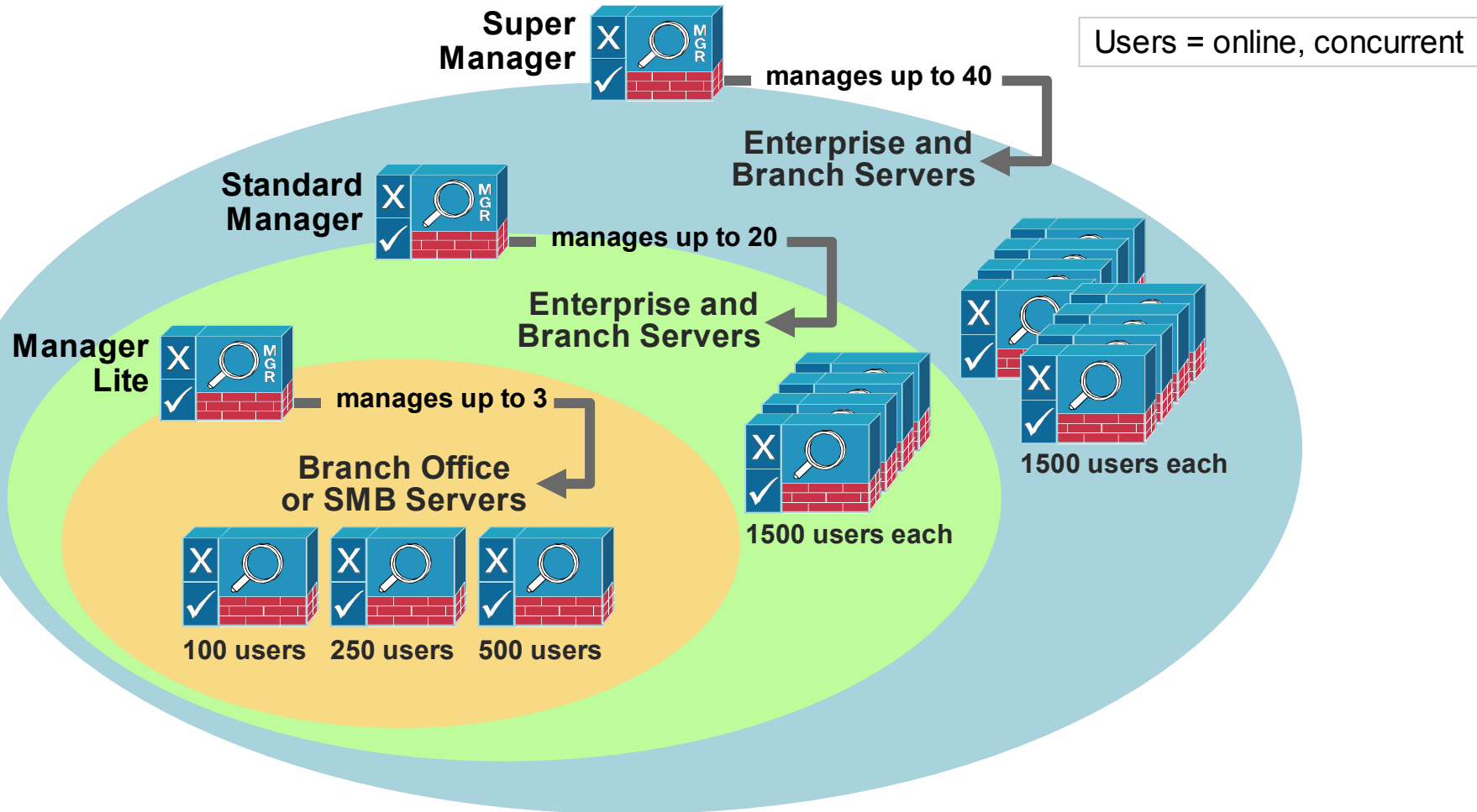
Guided self-remediation

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact

Accept Decline

NAC Appliance Sizing



Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features**
Checks, Rules, Requirements
4. **Clean Access Server Foundation Concepts**
5. **NAC Appliance Technical Benefits**



Posture Validation Overview

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

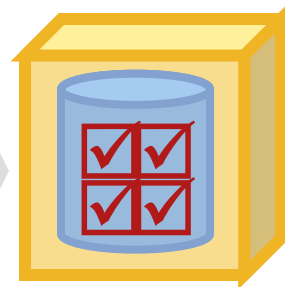
Checks
assess the state of a file, application, service, or registry key



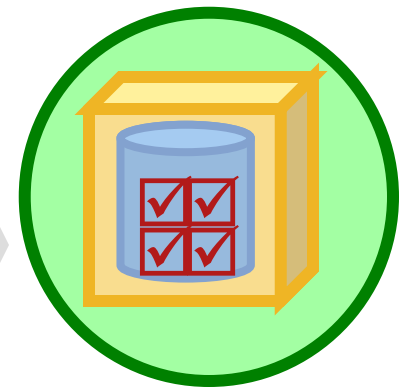
Rules
contain single or multiple **Checks**



Requirements
contain single or multiple **Rules**



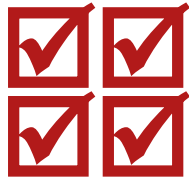
Roles
have one or more **Requirements**



Checks and Rules: An Example

Checks

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

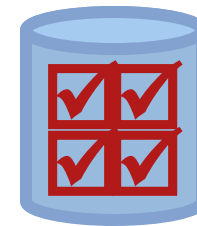


Is anti-spyware installed?
(application present, file present)
Is anti-spyware up-to-date?
(file version > or =)
Is anti-spyware running?
(service / exe running)



Rules

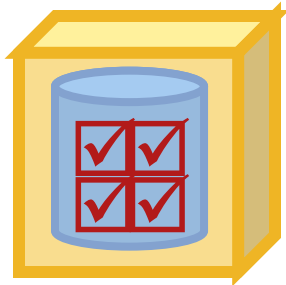
assemble individual checks together to make a posture assessment



Anti_Spyware_Installed_Check
AND
Anti_Spyware_UptoDate_Check
AND
Anti_Spyware_Running_Check

Requirements and Roles

Requirements
tie remediation actions
directly to a rule



Roles
determine which
requirements and which
security filters apply



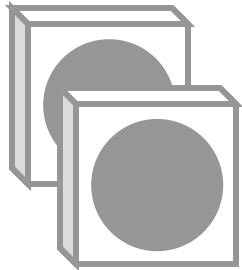
Remediation methods include:

- File Distribution (“[Download antispyware.exe](#)”)
- Link Distribution (“[windowsupdate.com](#)”)
- Local Check ([text instructions or messages](#))
- Definition Update ([direct launch of supported AV or AS](#))

**Option to dynamically assign
VLANs**

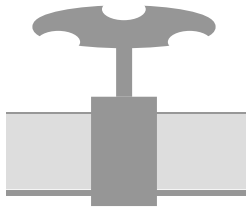
**Apply individual URL redirection
per role, as well as Acceptable
Usage Policies, User Pages,
and more**

Filters and Bandwidth



SECURITY FILTERS behave the same as Access Control Lists with additional `http://weblink` and Layer 2 protocol capabilities.

Each role has its own filter, with access levels controlled by the system administrator.



BANDWIDTH CONTROLS allow for either per-user or per-role restrictions.

Common for remediation and guest access applications.

Clean Access Manager Benefits Summary

- Centralized and scalable management and policy configuration
- Pre-configured checks drastically reduce “Day 2” support and maintenance
- Full access to the rules engine can create a posture assessment for any application
- Flexible remediation options give users as much power as desired to self-repair, reducing help desk dependence

Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features In-Depth**
4. **Clean Access Server Foundation Concepts:**
 - Virtual Gateway / Real IP Gateway
 - Central Deployment / Edge Deployment
 - Layer 2 / Layer 3
 - In Band / Out of Band
5. **NAC Appliance Technical Benefits**

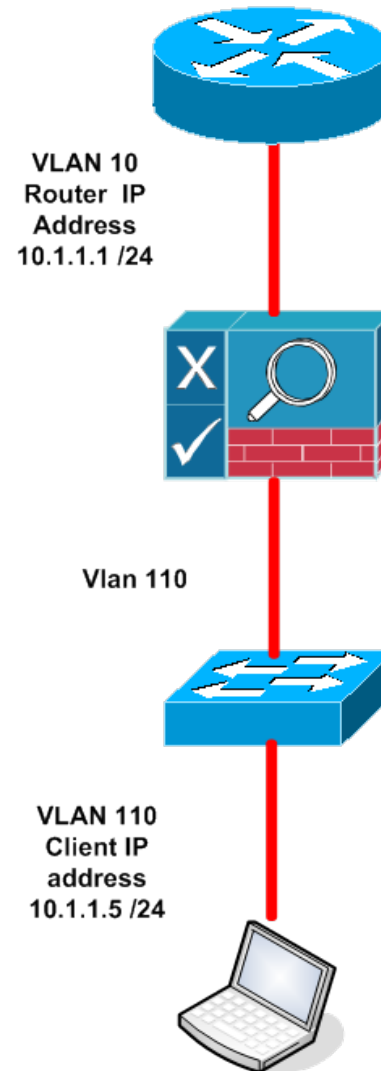


CAS Foundation: Virtual Gateway & Real IP Gateway

- Clean Access Servers at the most basic level can pass traffic in one of two ways:
 - Bridged Mode = Virtual Gateway
 - Routed Mode = Real IP Gateway / NAT Gateway
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Gateway mode selection affects the logical traffic path
- Does not affect whether a CAS is in Layer 2 mode, Layer 3 mode, In Band or Out of Band

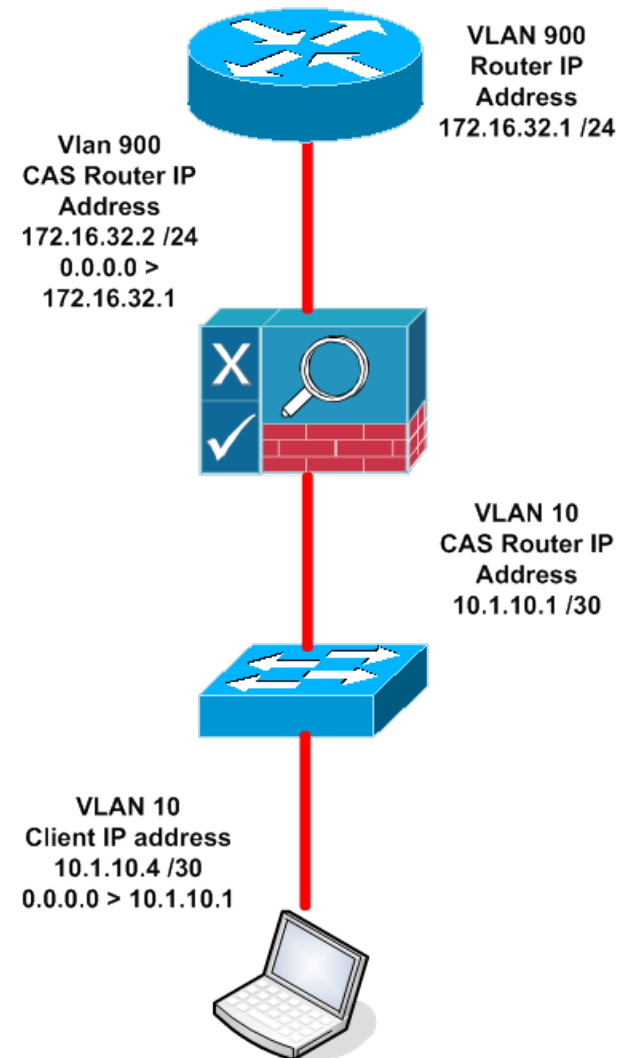
CAS Foundation: Virtual Gateway

- Direct Bridging: Frame Comes In, Frame Goes Out
- VLAN IDs are either passed through untouched or mapped from A to B
- DHCP and Client Routes point directly to network devices on the Trusted side
- CAS is an IP passive bump in the wire, like a transparent firewall



CAS Foundation: Real IP / NAT Gateway

- CAS is Routing, Packet Comes In, Packet Goes Out
- VLAN IDs terminate at the CAS, no pass-through or mapping
- DHCP and Client Routes usually point to the CAS for /30
- CAS is an active IP router, can also NAT outbound packets **

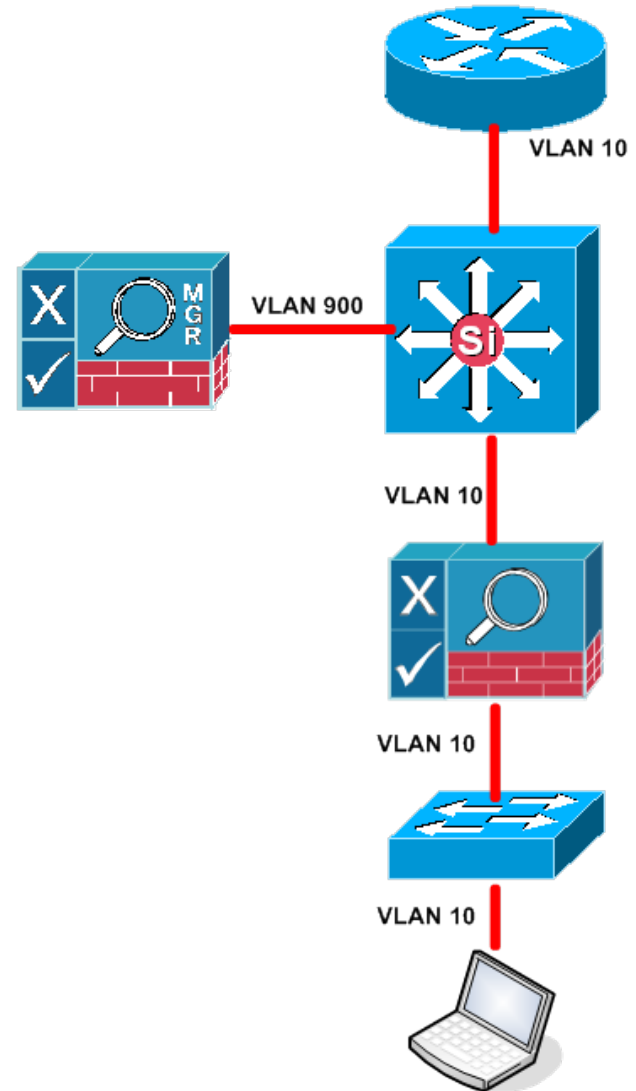


CAS Foundation: Central & Edge Deployment

- Clean Access Servers have two physical deployment models
 - Edge Deployment
 - Central Deployment
- Any CAS can be configured for either method
- Deployment mode selection affects the physical traffic path
- Does not affect whether a CAS is in Layer 2 mode, Layer 3 mode, In Band or Out of Band

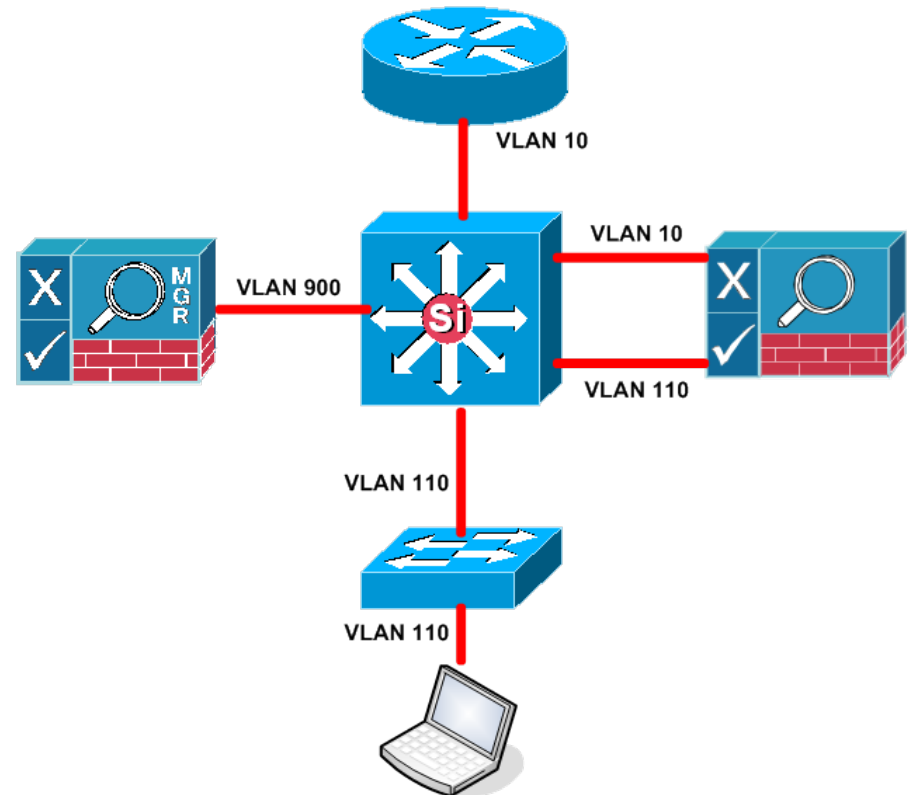
CAS Foundation: Edge Deployment

- Easiest deployment option to understand
- CAS is logically inline, and Physically inline
- Supports all Catalyst Switches
- VLAN IDs are passed straight through when in VGW
10 → 10
- Installations with multiple Access Layer closets can become complex

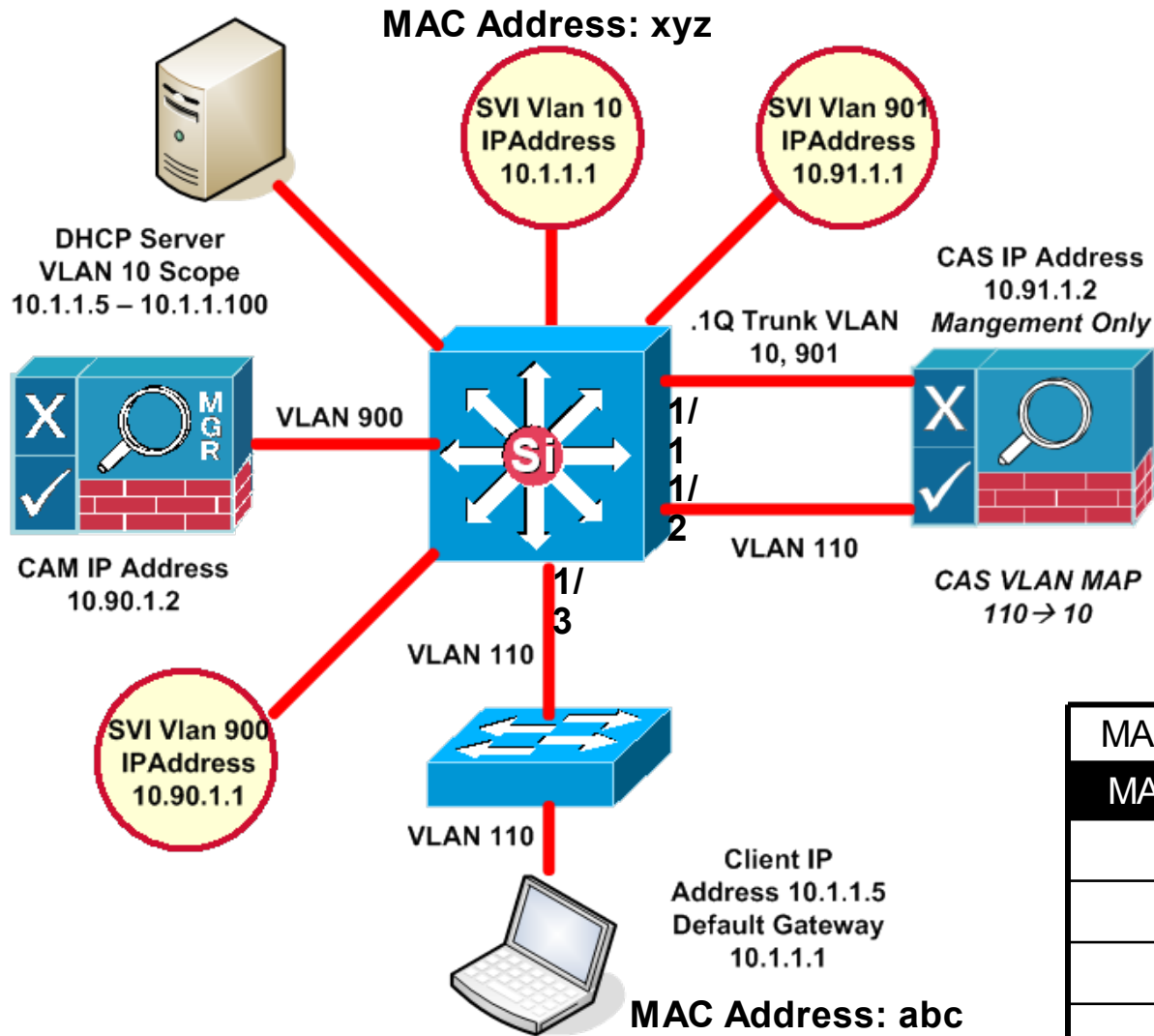


CAS Foundation: Central Deployment

- Most common deployment option
- CAS is logically inline, NOT physically inline
- Supports 6500 / 4500 / 3750 / 3560 **
- VLAN IDs are mapped when in VGW
- 110 à 10
- Easiest installation
- Most scalable in large environments



CAS Foundation: Central Deployment



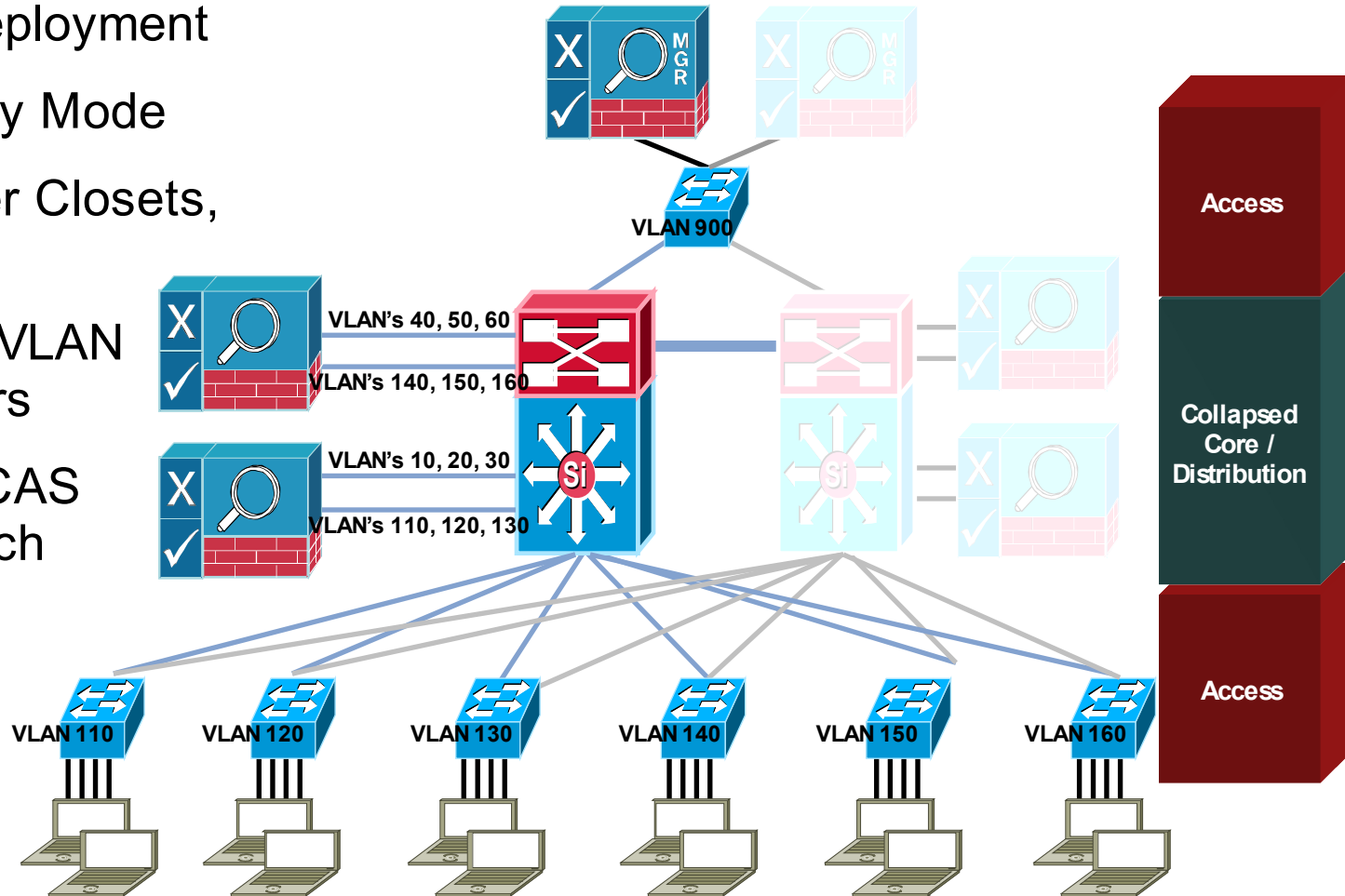
MAC Address Table on Core switch		
MAC Address	Vlan	Port
abc	110	1/3
abc	10	1/1
xyz	110	1/2
xyz	10	Router

CAS Foundation: Centralized Deployment

Example: Collapsed Core
Centralized Deployment

Virtual Gateway Mode

- 6 Access Layer Closets, 6 Data VLANs
- 500 users per VLAN total 3000 users
- 3 VLANs per CAS 1500 users each

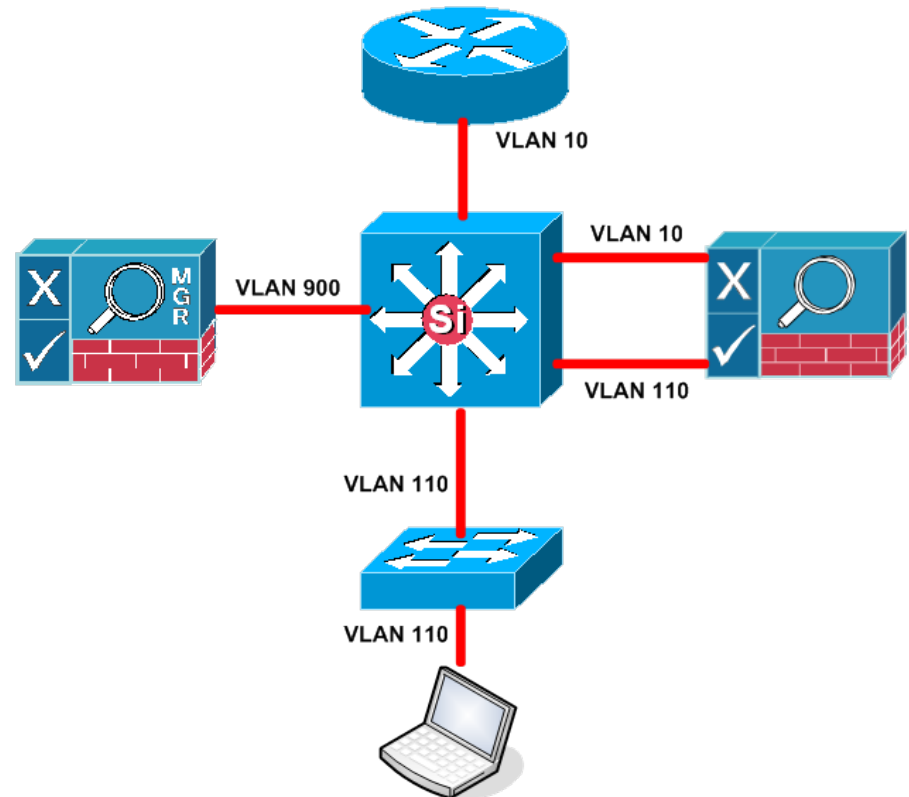


CAS Foundation: Layer 2 Mode & Layer 3 Mode

- Clean Access Servers have two client access deployment models
 - Layer 2 Mode
 - Layer 3 Mode
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Deployment mode selection is based on whether the client is Layer 2 adjacent to the CAS

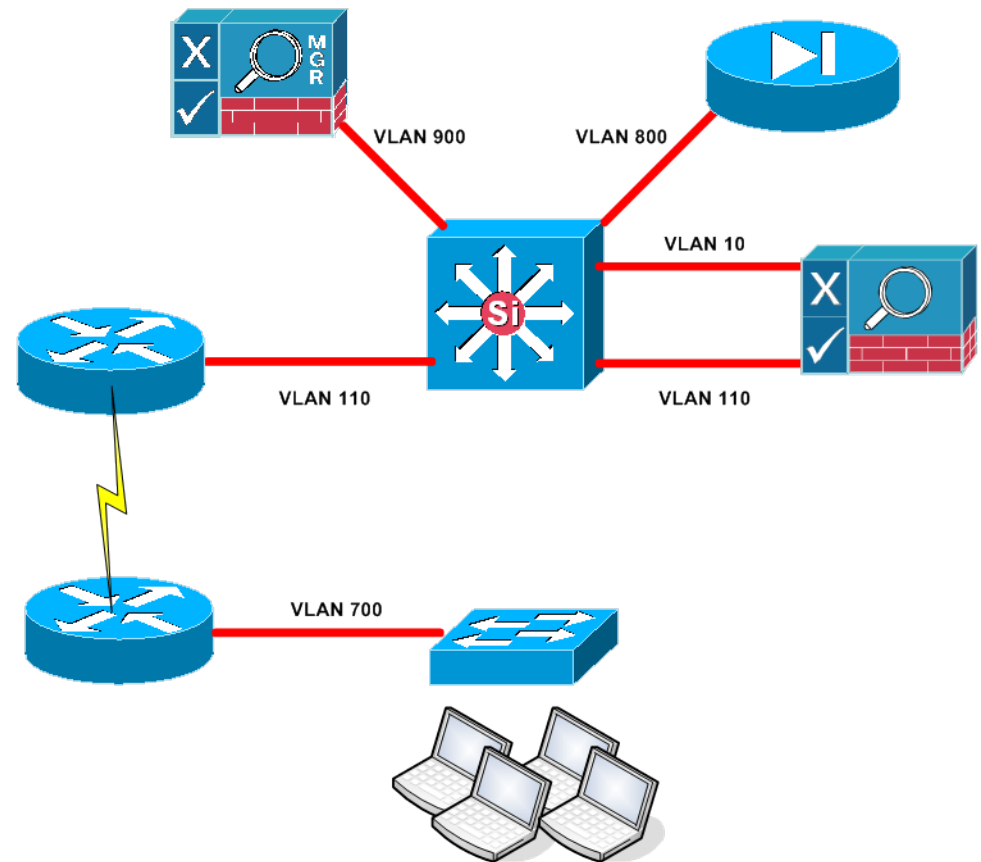
CAS Foundation: Layer 2 Mode

- Client is Layer 2 Adjacent to the CAS
- MAC address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports both In Band and Out of Band
- Most common deployment model for LANs



CAS Foundation: Layer 3 Mode

- Client is NOT Layer 2 Adjacent to the CAS
- IP Address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports In Band Mode**
- Needed for WAN and VPN deployments

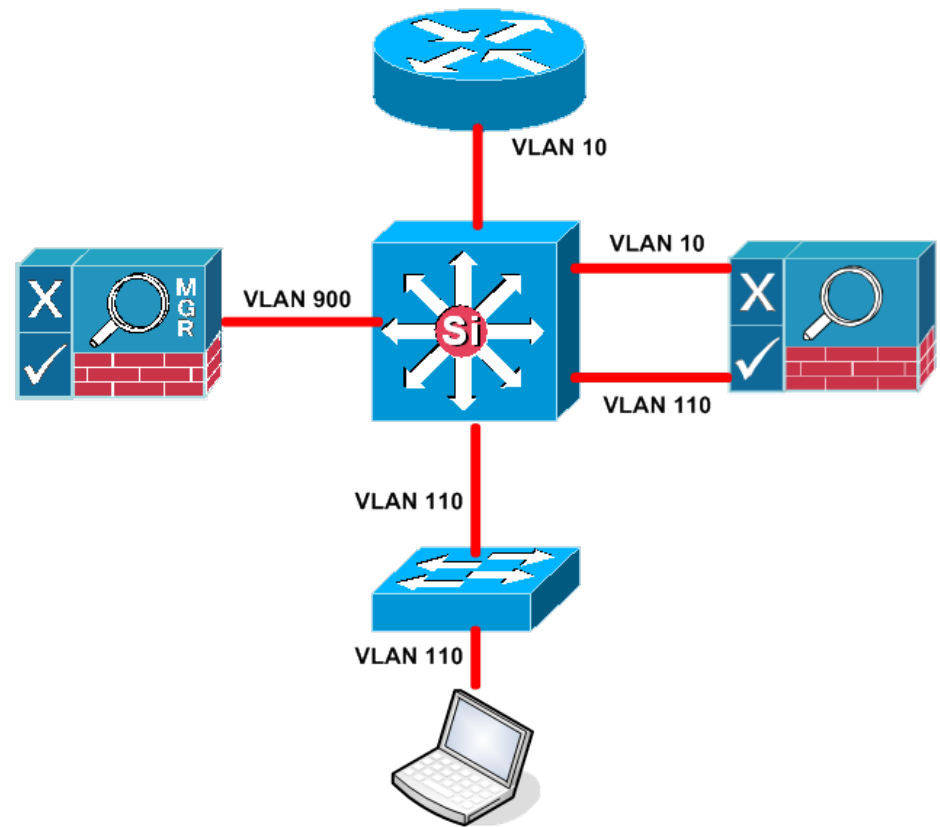


CAS Foundation: In Band & Out of Band

- Clean Access Servers have two traffic flow deployment models
 - In Band
 - Out of Band
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Selection is based on whether the customer wants to remove the CAS from the data path
- CAS is **ALWAYS** inline during Posture Assessment

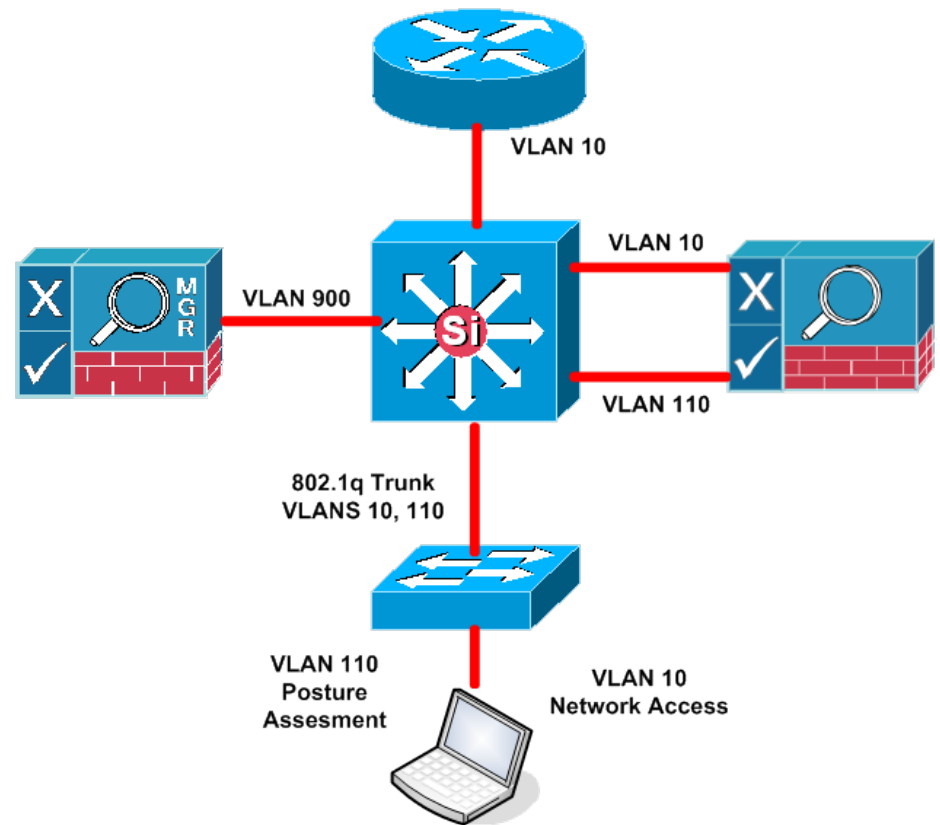
CAS Foundation: In Band

- Easiest deployment option
- CAS is Inline (in the data path) before and after posture assessment
- Supports any switch, any hub, any AP
- Role Based Access Control Guest, Contractor, Employee
- ACL Filtering and Bandwidth Throttling

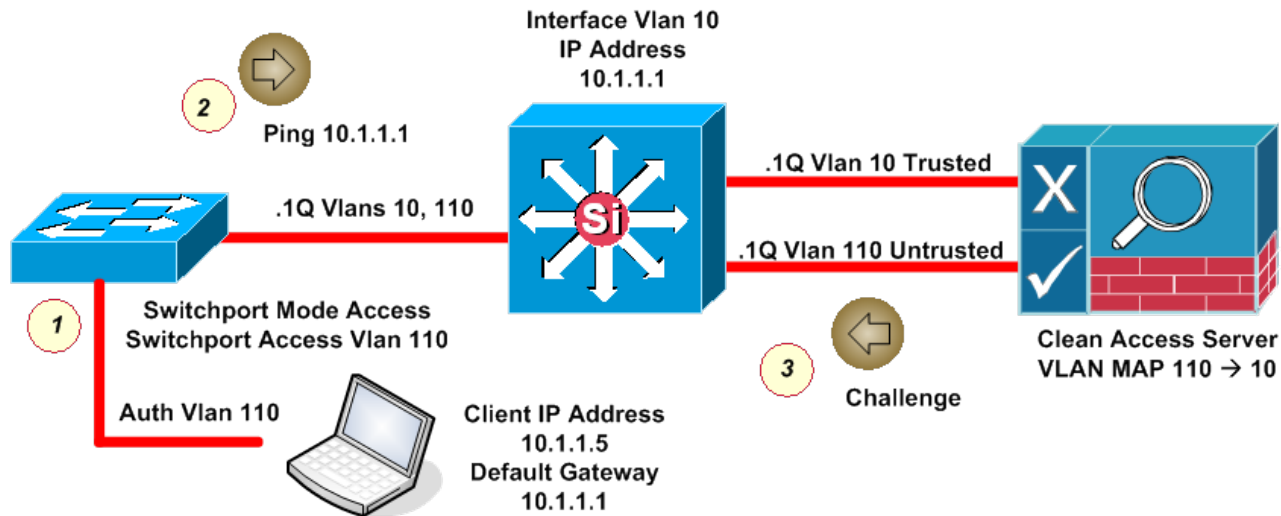


CAS Foundation: Out of Band

- Multi-Gig Throughput deployment option
- CAS is Inline for Posture Assessment Only
- Supports most common Cisco Switches **
- Port VLAN Based and Role Based Access Control
- ACL Filtering and Bandwidth Throttling for Posture Assessment Only

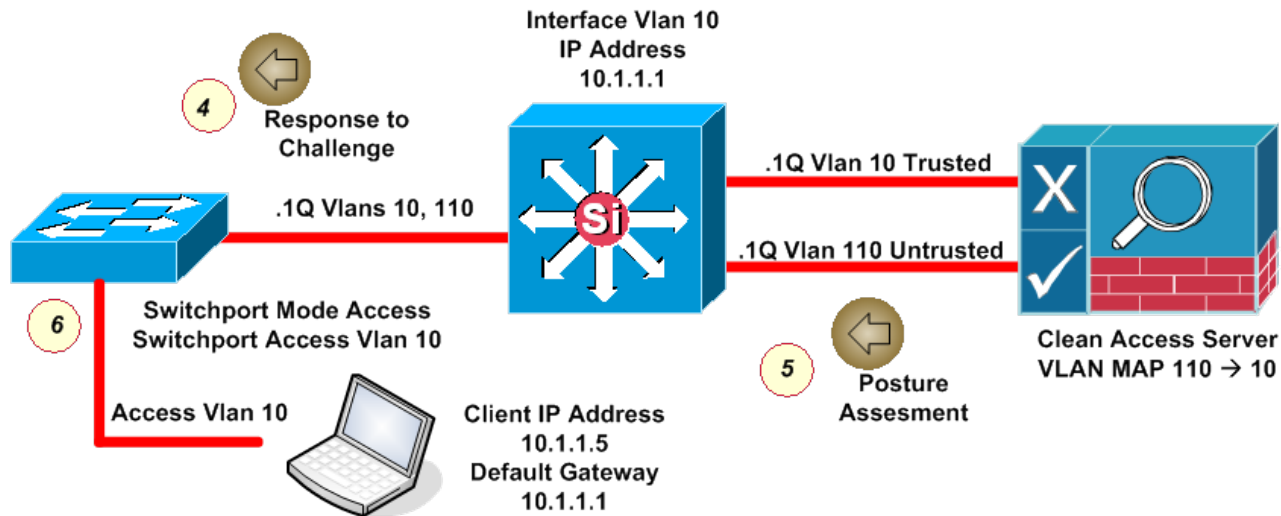


Out Of Band Process Flow



3. New MAC Notification sent to CAM
4. Unauthenticated client discovery (Agent popup or new traffic)
5. CAS challenges for credentials

Out Of Band Process Flow



4. Client sends credentials to CAS
5. CAS performs Posture Assessment
6. CAM changes VLAN from Auth to Access

Network Design

- CAS selection can become complex, think it through and weigh the pros and cons
- General guideline is to start out with L2 IB VGW Central
 - Go Real IP Gateway if you want /30
 - Go out of band if you think you'll oversubscribe the ports
 - Go L3 if you cannot ensure MAC address
- The simpler the deployment the easier it is to manage going forward

CAS Foundation Summary

1

Virtual Gateway mode is usually the easiest integration into existing networks

2

Central deployments will make up 99% of designs

3

Layer 2 adjacent clients give more options for security with Layer 2 strict mode

4

Pay close attention to In-Band math: it's 1Gig for 1500 users, not 1Gig for the whole network.

Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features In-Depth**
4. **Clean Access Server Foundation Concepts**
5. **NAC Appliance Technical Benefits**



NAC Appliance Technical Benefits

Product Experience

With 500+ deployments, Cisco understands the technical impact on your network

Defense-in-Depth

NAC Appliance is a self-contained, proactive way to enforce policy compliance on all incoming devices

Rapid Setup Easy Mgmt

Pre-configured rulesets and checks make it easy to setup, maintain, modify, and expand

Flexible Deployment

Broad deployment options means that NAC Appliance fits into your network the way you need it to

Future Proof

NAC Appliance is core to Cisco's strategic NAC vision and can be leveraged across all future deployment options



Product Demonstration





NAC Appliance



Jeff DiMaio
CISSP
Systems Engineer
Cisco Systems

CBC Grand Opening- October 20

- Agenda
- 12:30–1:00 p.m. Registration
- 1:00–1:30 p.m. Leading Life's Experiences,
- Are You Ready?—Carl Wiese, Vice President, Advanced Technology
- 1:30–2:15 p.m. Network as the Platform- Tracey Newell, Area Vice President
- 2:15–2:30 p.m. Break
- 2:30–3:30 p.m. Customer Panel hosted by Jeff Sharritts, Operations Director, and Lisa Loftus, Regional Sales Manager
- 2:30 -3:30 p.m. CBC Tours
- 3:30–4:30 p.m. Reception

Agenda

1. Securing Complexity
2. NAC Appliance Product Overview
3. NAC Appliance Features
4. Clean Access Server Foundation Concepts
5. NAC Appliance Technical Benefits

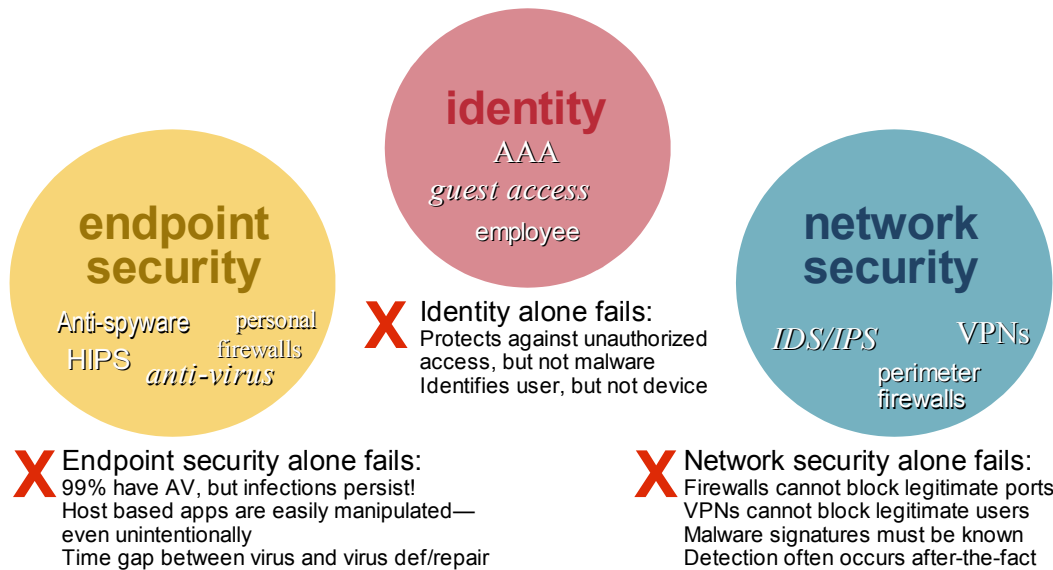


Productivity Causes Complexity



WHAT SYSTEM IS IT?	Windows, Mac or Linux Laptop or desktop or PDA Printer or other corporate asset
WHO OWNS IT?	Company Employee Contractor Guest Unknown
WHERE IS IT COMING FROM?	VPN LAN WLAN WAN
WHAT'S ON IT? IS IT RUNNING?	Anti-virus, anti-spyware Personal firewall Patching tools
WHAT'S THE PREFERRED WAY TO CHECK/FIX IT?	Pre-configured checks Customized checks Self-remediation or auto-remediation Third-party software

Complexity Demands Defense-in-Depth

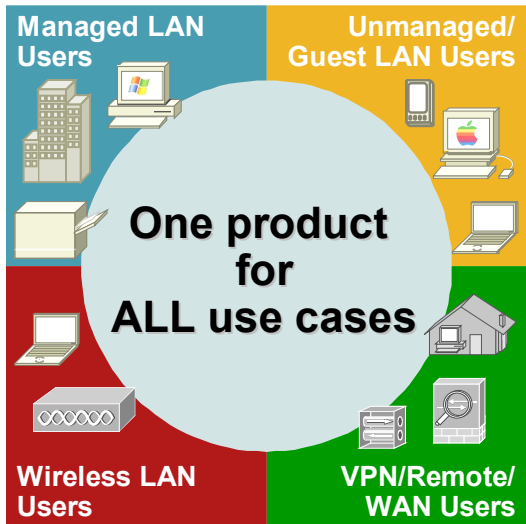


Agenda

1. Securing Complexity
2. NAC Appliance Product Overview
3. NAC Appliance Features
4. Clean Access Server Foundation Concepts
5. NAC Appliance Technical Benefits



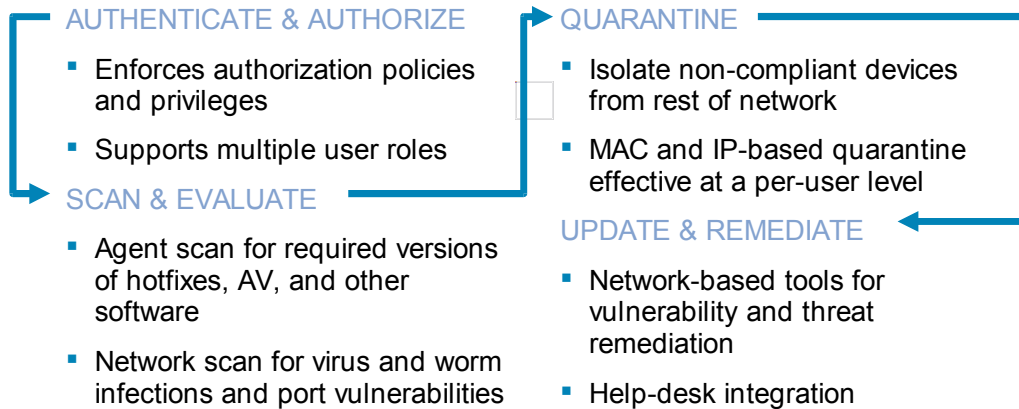
NAC Appliance

- 

1. One product for ALL use cases
- 2.** 600+ customers across all use cases: No. 1 NAC solution
- 3.** Most deployments ready under 5 days
- 4.** Scales from 100 users to 100,000+ user, across 150+ locations
- 5.** Does not require infrastructure upgrade

NAC Appliance Overview

All-in-One Policy Compliance and Remediation Solution



Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

8

4 Components to good NAC solution

- Who is the user- consultant, faculty staff, employee, guest?, which privileges should I give? Which kind of posture assessment to carry out? Employee- antivirus? Guest- any antivirus
- Scan- NAC decision- 2 Ways-
 - Agent-based- registry key- value?, File exists- date, version? Application or Service running
 - Network Scan using NESSUS- compliant or not compliant
- Quarantine- only has access to patch server
- Update and Remediate- want to have the user self remediate, decrease load on network admin staff

NAC Appliance Overview: Components

- Cisco Clean Access Server

Serves as an in-band or out-of-band device for network access control



- Cisco Clean Access Manager

Centralizes management for administrators, support personnel, and operators



- Cisco Clean Access Agent

Optional lightweight client for device-based registry scans in unmanaged environments



- Rule-set Updates

Scheduled automatic updates for anti-virus, critical hot-fixes and other applications



Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

9

- CCA solution consists of four components:
 - Clean Access Server (Required)
 - All user traffic hits server, challenges for authentication, does posture assessment, allows remediation to happen, determines which privileges on network
 - 2) Clean Access Manager (Required)
 - Central management station where you define policies and push to CAS
 - 3) Clean Access Agent (Optional)
 - 99% of users utilize this component. Optional client for device-based registry scans on unmanaged environments. Read only client. Downloadable and provisional over the web. Read only client with only one configuration.
 - Rule Set Updates
 - Consider- 2 rules- McAfee is running and completed and updated, old 4.2.3.2, new 4.2.3.3
 - You'd have to change the version on the rules
 - Cisco has servers that poll antivirus- 24 spyware- 17 vendors, check every 30 minutes
 - CAM polls cisco.com servers. once rules configured. rules are updated

NAC Appliance Overview: Components

Critical Windows Updates

**Windows XP, Windows 2000,
Windows 98, Windows ME**



Anti-Virus Updates



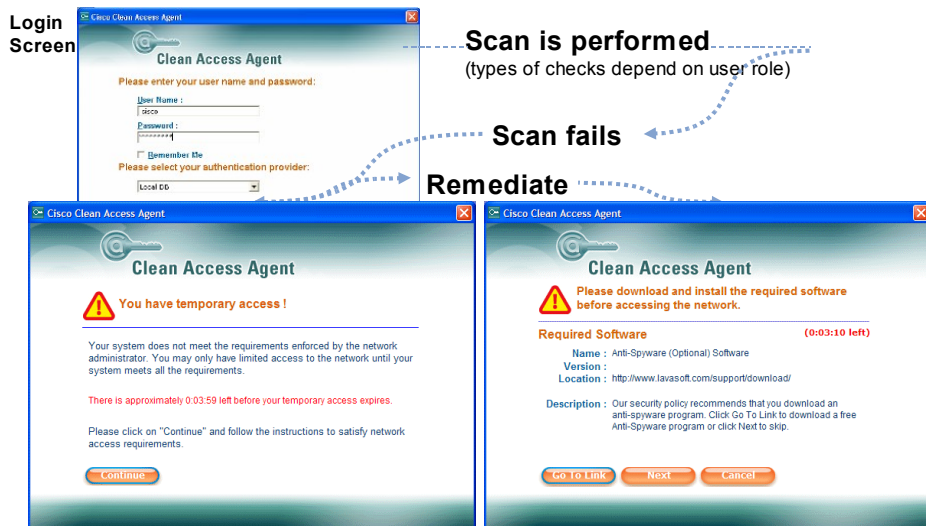
Anti-Spyware Updates
Other 3rd Party Checks



Customers can easily add customized checks

- Subset of

User Experience with Agent



Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

11

- End User Experience: with Agent

- Access Agent is popped up (top left screen shot) because it is requiring authentication.



- If scan fails, user put into a temporary role. In temporary role the user given temporary access. In temporary access role the user only have access to the files, checks, patches, and links they need to remediate the problem – user not on the network yet.



- User receives file or link with instructions (customizable to the end user) to install and run on their machines before they can get on network access. A seamless process. Note - after user applies patches to their machines, Clean Access rescans their machine to make sure they are running before it allows them on to the network.

- If scan does not fail, the user is authenticated right to the network.

User Experience via Web Browser

The image shows two browser windows. The left window is titled "Cisco Clean Access Authentication" and contains a login form with fields for "Username" and "Password", a "Continue" button, and a message: "Please provide your credentials to access this network." Below the form is a "Visa Bulletin" section with text about anti-virus software and a link to a "How-To" document. The right window is titled "Scan Report - Mozilla Firefox" and displays a "Vulnerability Scan Report of iyao's Machine". The report includes a table with columns for "Type", "Service", "Description", and "Instruction/Link".

Login Screen → **Scan is performed (types of checks depend on user role/OS)**

Type	Service	Description	Instruction/Link
INFO	microsoft-ds (445/tcp)	A CIFS server is running on this port	
INFO	netbios-ssn (139/tcp)	An SMB server is running on this port	
INFO	netbios-ns (137/udp)	The following 3 NetBIOS names have been gathered : IYAO\$F003 IYAO\$F003 = This is the computer name PERFIGO = Workgroup / Domain name The remote host has the following MAC address on its adapter : 00:02:2d:09:f3:5d If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621	

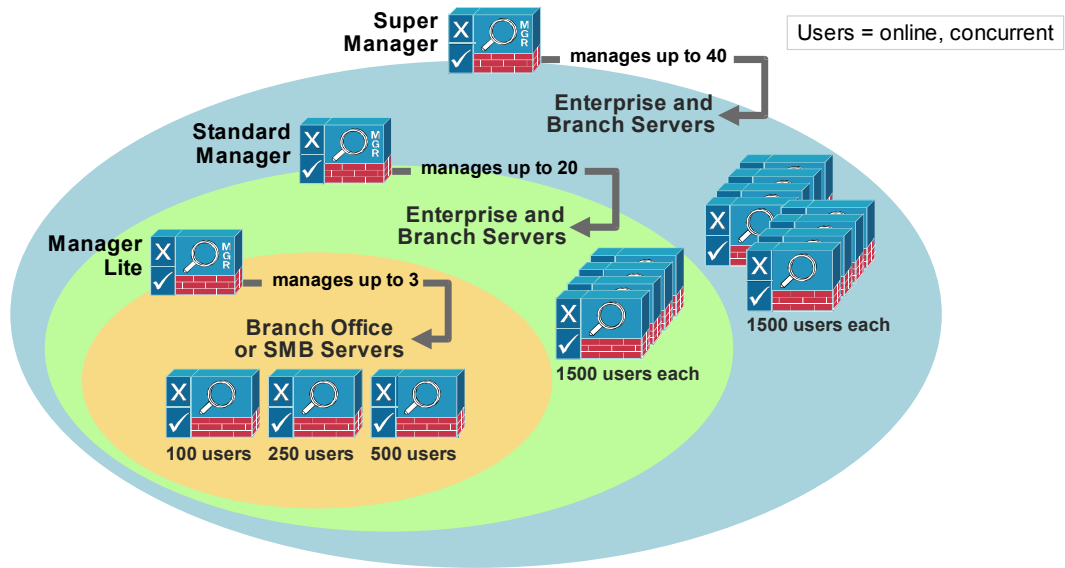
Guided self-remediation

Accept Decline

Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential 12

- End User Experience: Web-based
- Typically used for guest user access or conferences. This is also the first experience for any user coming onto to the network to also get the agent on their machines. On first page user name and access is required. As the user gives their credentials it will report back with an optional vulnerability scan report, which will provide them the information (i.e. type of worm or virus found, the service that was running, a description of that service, as well as instructions to customize and a link). All based on OS and user role.
- Above and beyond , after vulnerability report, the user will receive a web page they can customize for universities for computing policies they can accept or decline. After that they will be authenticated to the network and on the network as normal.

NAC Appliance Sizing



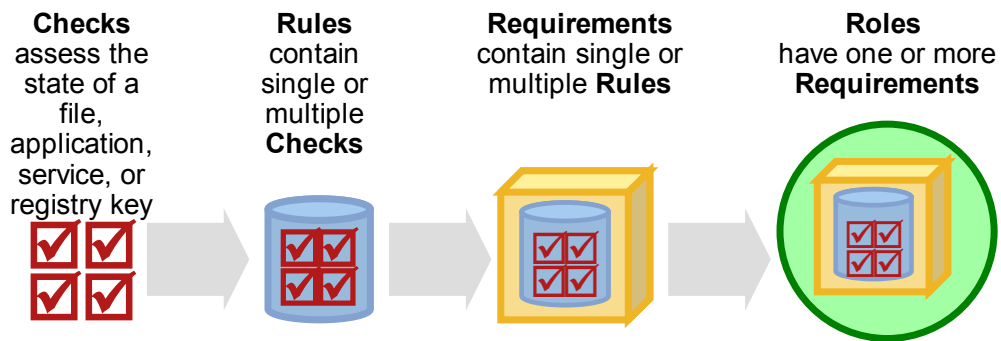
Agenda

1. Securing Complexity
2. NAC Appliance Product Overview
3. NAC Appliance Features
Checks, Rules, Requirements
4. Clean Access Server
Foundation Concepts
5. NAC Appliance Technical Benefits



Posture Validation Overview

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



Checks and Rules: An Example

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



Rules
assemble individual
checks together to make
a posture assessment



Is anti-spyware installed?
(application present, file present)
Is anti-spyware up-to-date?
(file version > or =)
Is anti-spyware running?
(service / exe running)

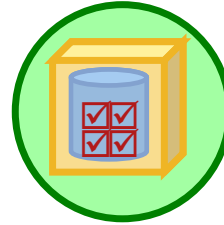
Anti_Spyware_Installed_Check
AND
Anti_Spyware_UptoDate_Check
AND
Anti_Spyware_Running_Check

Requirements and Roles

Requirements
tie remediation actions
directly to a rule



Roles
determine which
requirements and which
security filters apply



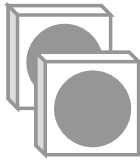
Remediation methods include:

- File Distribution (“Download antispyware.exe”)
- Link Distribution (“windowsupdate.com”)
- Local Check (text instructions or messages)
- Definition Update (direct launch of supported AV or AS)

**Option to dynamically assign
VLANs**

**Apply individual URL redirection
per role, as well as Acceptable
Usage Policies, User Pages,
and more**

Filters and Bandwidth



SECURITY FILTERS behave the same as Access Control Lists with additional <http://weblink> and Layer 2 protocol capabilities.

Each role has its own filter, with access levels controlled by the system administrator.



BANDWIDTH CONTROLS allow for either per-user or per-role restrictions.

Common for remediation and guest access applications.

Clean Access Manager Benefits Summary

- Centralized and scalable management and policy configuration
- Pre-configured checks drastically reduce “Day 2” support and maintenance
- Full access to the rules engine can create a posture assessment for any application
- Flexible remediation options give users as much power as desired to self-repair, reducing help desk dependence

Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features In-Depth**
4. **Clean Access Server Foundation Concepts:**
 - Virtual Gateway / Real IP Gateway
 - Central Deployment / Edge Deployment
 - Layer 2 / Layer 3
 - In Band / Out of Band
5. **NAC Appliance Technical Benefits**

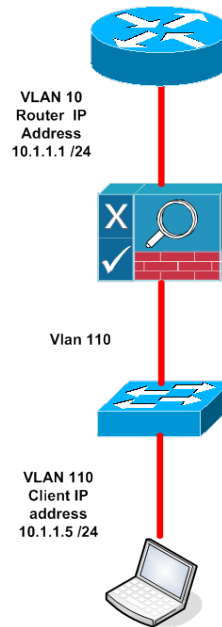


CAS Foundation: Virtual Gateway & Real IP Gateway

- Clean Access Servers at the most basic level can pass traffic in one of two ways:
 - Bridged Mode = Virtual Gateway
 - Routed Mode = Real IP Gateway / NAT Gateway
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Gateway mode selection affects the logical traffic path
- Does not affect whether a CAS is in Layer 2 mode, Layer 3 mode, In Band or Out of Band

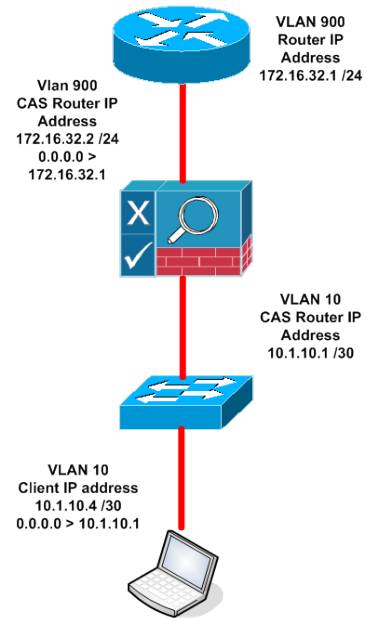
CAS Foundation: Virtual Gateway

- Direct Bridging: Frame Comes In, Frame Goes Out
- VLAN IDs are either passed through untouched or mapped from A to B
- DHCP and Client Routes point directly to network devices on the Trusted side
- CAS is an IP passive bump in the wire, like a transparent firewall



CAS Foundation: Real IP / NAT Gateway

- CAS is Routing, Packet Comes In, Packet Goes Out
- VLAN IDs terminate at the CAS, no pass-through or mapping
- DHCP and Client Routes usually point to the CAS for /30
- CAS is an active IP router, can also NAT outbound packets **

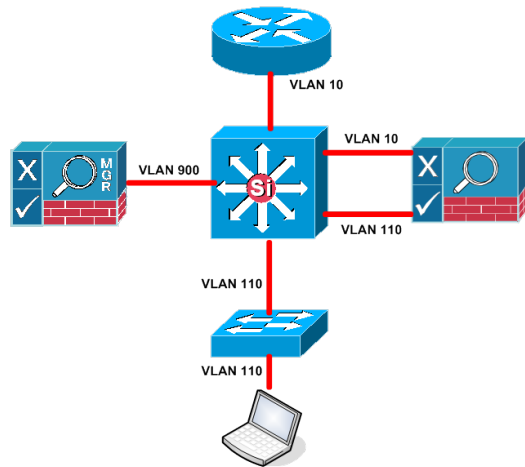


CAS Foundation: Central & Edge Deployment

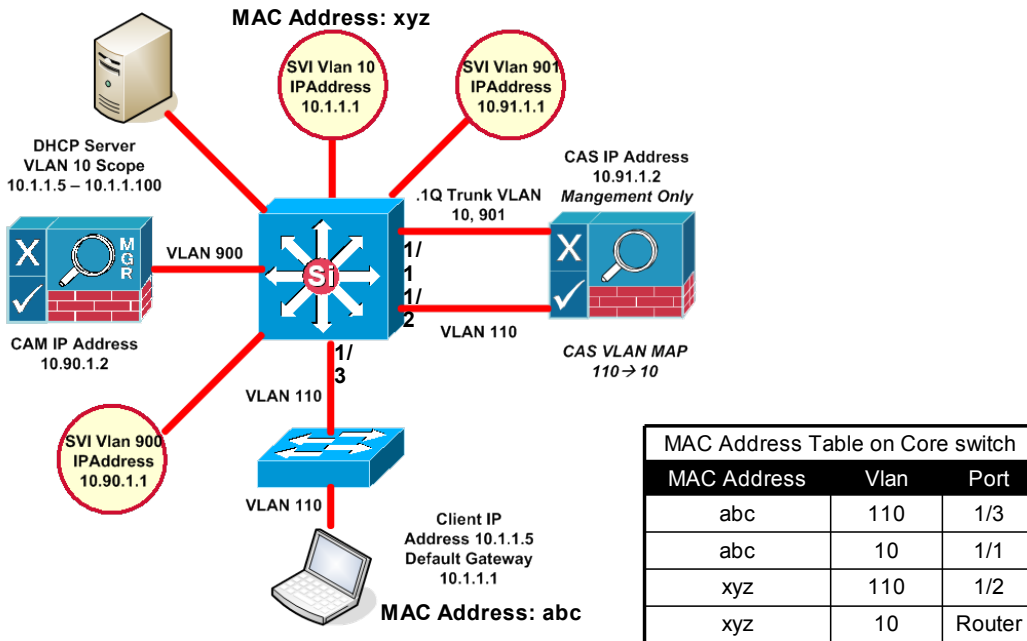
- Clean Access Servers have two physical deployment models
 - Edge Deployment
 - Central Deployment
- Any CAS can be configured for either method
- Deployment mode selection affects the physical traffic path
- Does not affect whether a CAS is in Layer 2 mode, Layer 3 mode, In Band or Out of Band

CAS Foundation: Central Deployment

- Most common deployment option
- CAS is logically inline, NOT physically inline
- Supports 6500 / 4500 / 3750 / 3560 **
- VLAN IDs are mapped when in VGW
 - 110 à 10
- Easiest installation
- Most scalable in large environments



CAS Foundation: Central Deployment

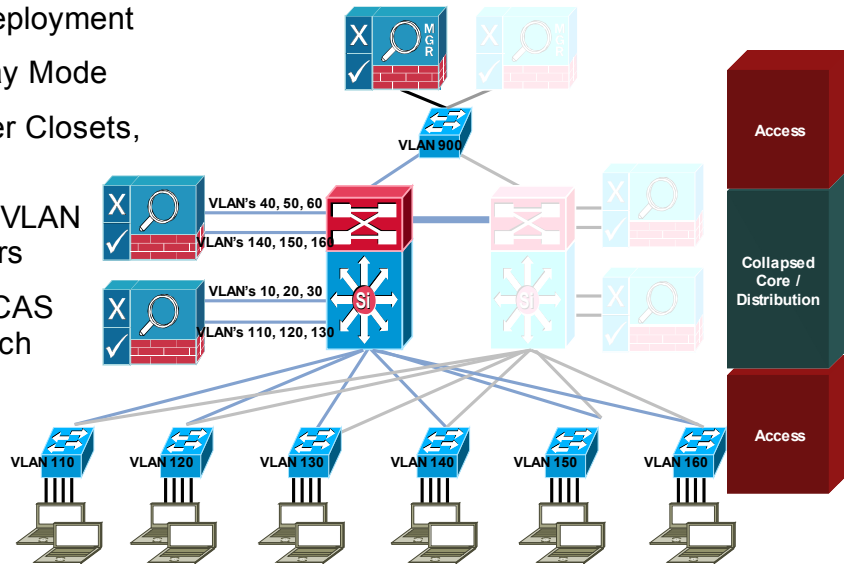


CAS Foundation: Centralized Deployment

Example: Collapsed Core
Centralized Deployment

Virtual Gateway Mode

- 6 Access Layer Closets, 6 Data VLANs
- 500 users per VLAN total 3000 users
- 3 VLANs per CAS 1500 users each

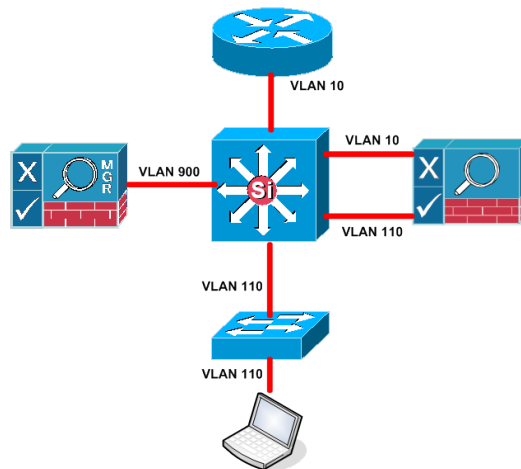


CAS Foundation: Layer 2 Mode & Layer 3 Mode

- Clean Access Servers have two client access deployment models
 - Layer 2 Mode
 - Layer 3 Mode
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Deployment mode selection is based on whether the client is Layer 2 adjacent to the CAS

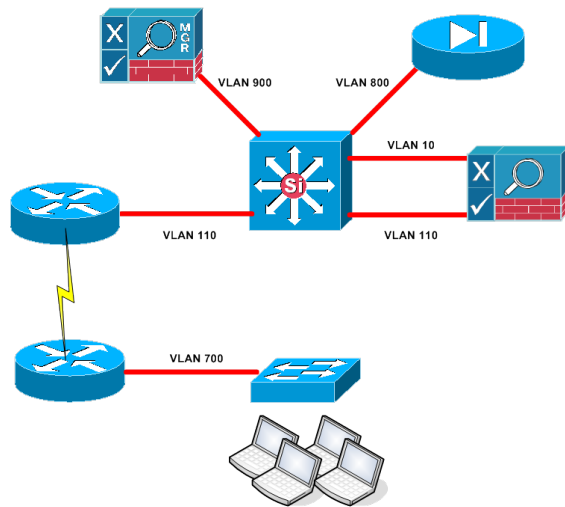
CAS Foundation: Layer 2 Mode

- Client is Layer 2 Adjacent to the CAS
- MAC address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports both In Band and Out of Band
- Most common deployment model for LANs



CAS Foundation: Layer 3 Mode

- Client is NOT Layer 2 Adjacent to the CAS
- IP Address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports In Band Mode**
- Needed for WAN and VPN deployments

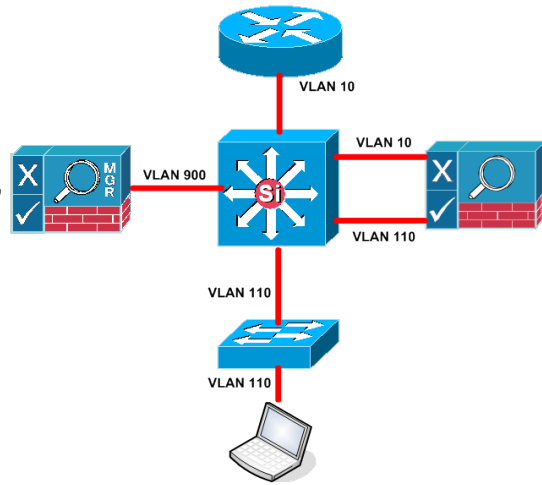


CAS Foundation: In Band & Out of Band

- Clean Access Servers have two traffic flow deployment models
 - In Band
 - Out of Band
- Any CAS can be configured for either method, but a CAS can only be one at a time
- Selection is based on whether the customer wants to remove the CAS from the data path
- CAS is ALWAYS inline during Posture Assessment

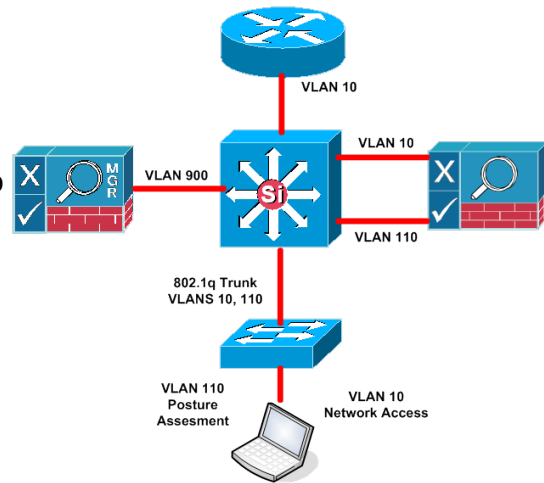
CAS Foundation: In Band

- Easiest deployment option
- CAS is Inline (in the data path) before and after posture assessment
- Supports any switch, any hub, any AP
- Role Based Access Control
Guest, Contractor, Employee
- ACL Filtering and Bandwidth Throttling

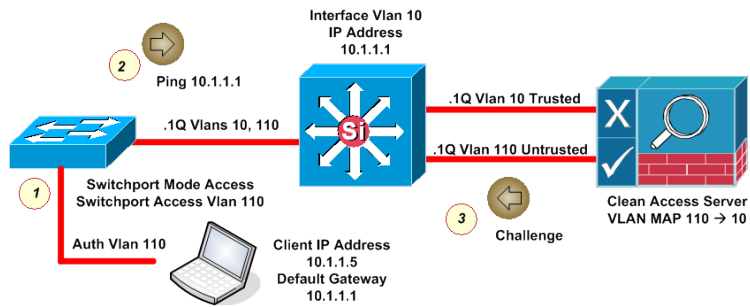


CAS Foundation: Out of Band

- Multi-Gig Throughput deployment option
- CAS is Inline for Posture Assessment Only
- Supports most common Cisco Switches **
- Port VLAN Based and Role Based Access Control
- ACL Filtering and Bandwidth Throttling for Posture Assessment Only

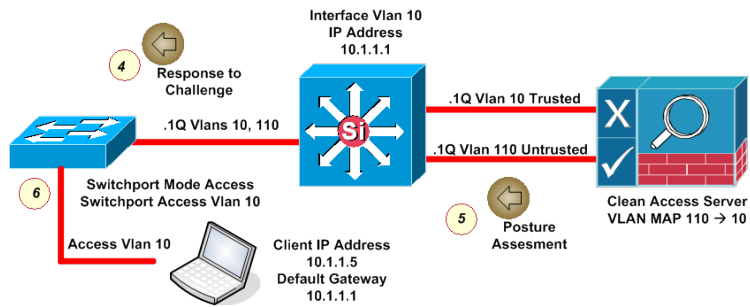


Out Of Band Process Flow



3. New MAC Notification sent to CAM
4. Unauthenticated client discovery (Agent popup or new traffic)
5. CAS challenges for credentials

Out Of Band Process Flow



4. Client sends credentials to CAS
5. CAS performs Posture Assessment
6. CAM changes VLAN from Auth to Access

Network Design

- CAS selection can become complex, think it through and weigh the pros and cons
- General guideline is to start out with L2 IB VGW Central
 - Go Real IP Gateway if you want /30
 - Go out of band if you think you'll oversubscribe the ports
 - Go L3 if you cannot ensure MAC address
- The simpler the deployment the easier it is to manage going forward

CAS Foundation Summary

1	Virtual Gateway mode is usually the easiest integration into existing networks
2	Central deployments will make up 99% of designs
3	Layer 2 adjacent clients give more options for security with Layer 2 strict mode
4	Pay close attention to In-Band math: it's 1Gig for 1500 users, not 1Gig for the whole network.

Agenda

1. Securing Complexity
2. NAC Appliance Product Overview
3. NAC Appliance Features In-Depth
4. Clean Access Server Foundation Concepts
5. **NAC Appliance Technical Benefits**

NAC Appliance Technical Benefits

Product Experience	With 500+ deployments, Cisco understands the technical impact on your network
Defense-in-Depth	NAC Appliance is a self-contained, proactive way to enforce policy compliance on all incoming devices
Rapid Setup Easy Mgmt	Pre-configured rulesets and checks make it easy to setup, maintain, modify, and expand
Flexible Deployment	Broad deployment options means that NAC Appliance fits into your network the way you need it to
Future Proof	NAC Appliance is core to Cisco's strategic NAC vision and can be leveraged across all future deployment options



Product Demonstration

