Self Defending Network, Cisco Network Admission Control

Michal Remper
System Engineer
mremper@cisco.com

The Need for Admission Control

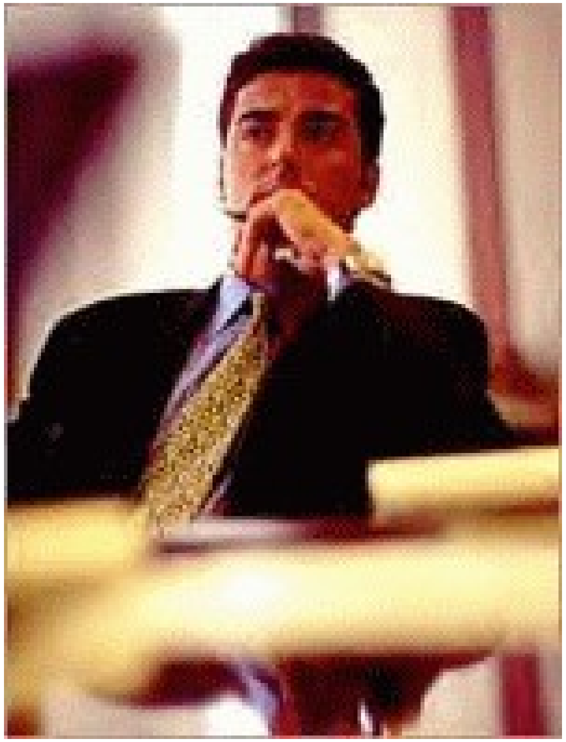
- Viruses, worms, spyware, etc. continue to plague organizations

    Viruses still #1 cause of financial loss* (downtime, recovery, productivity, etc.)

- While most *users* are authenticated, their endpoint devices (laptops, PCs, PDAs, etc.) are ***not*** checked for security policy compliance

- These unprotected endpoint devices are often responsible for spreading infection

    Ensures devices accessing the network comply with policy (required security software installed, enabled, and current) is difficult and expensive



"**Endpoint systems are vulnerable** and represent the most likely point of infection from which a virus or worm can spread rapidly and cause serious disruption and economic damage."
– Burton Group

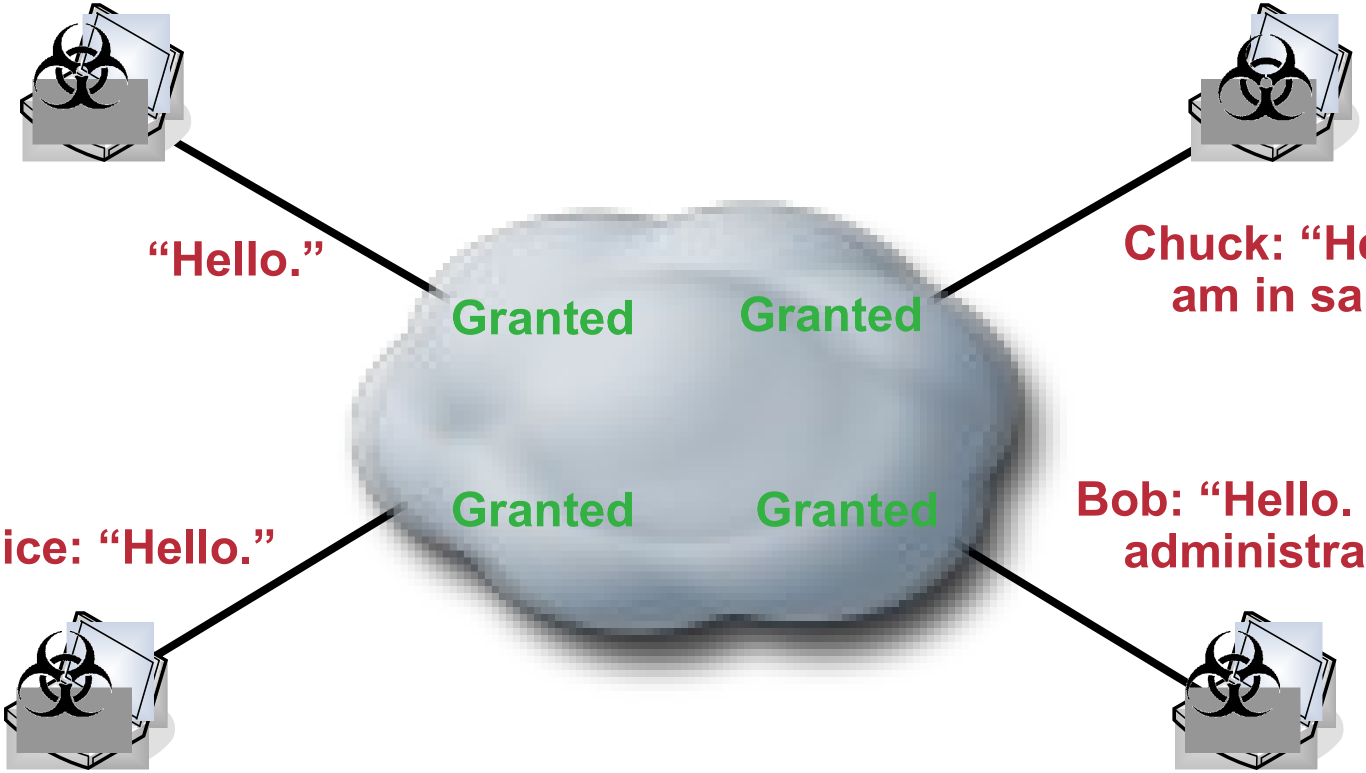
*2005 FBI/CSI Report

Why Use The Network?

- Every bit of data you are concerned about touches the network
- Every device you are concerned about is attached to the network.
- Gives you the ability to deploy the broadest possible security solution covering the largest number of networked devices
- Also leverages existing infrastructure, security, and management deployments, so it has the smallest IT footprint possible

Prior Methods for Network Admission

Chuck: “I am running an unpatched Windows 2000 system. I am Gigabit Ethernet connected with worm de jour and this one is really nasty. Have a nice day!”



“Hello.”

Chuck: “Hello. I am in sales.”

Granted

Granted

Granted

Granted

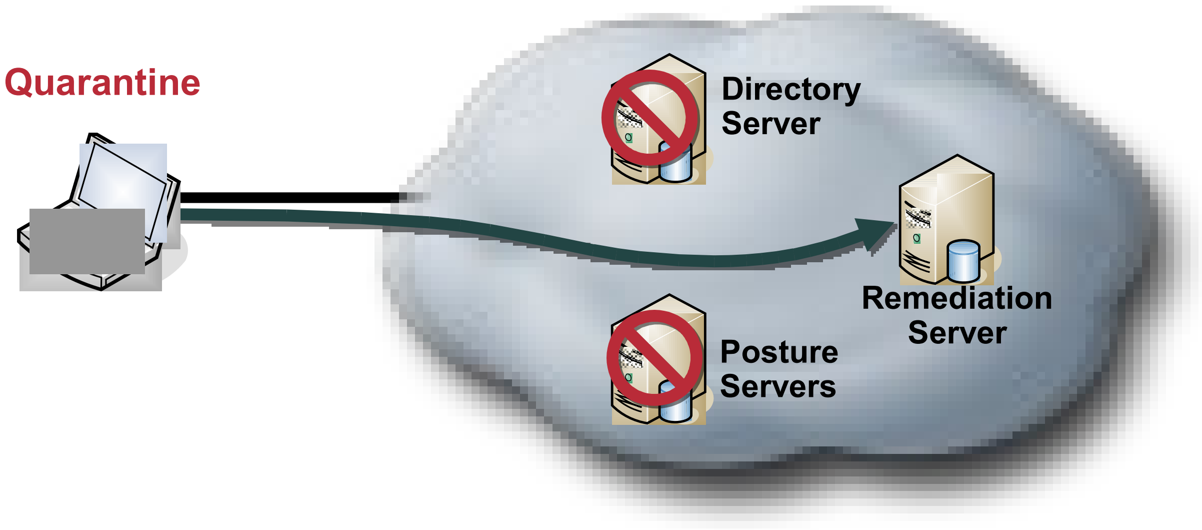
Alice: “Hello.”

Bob: “Hello. I am an administrator”

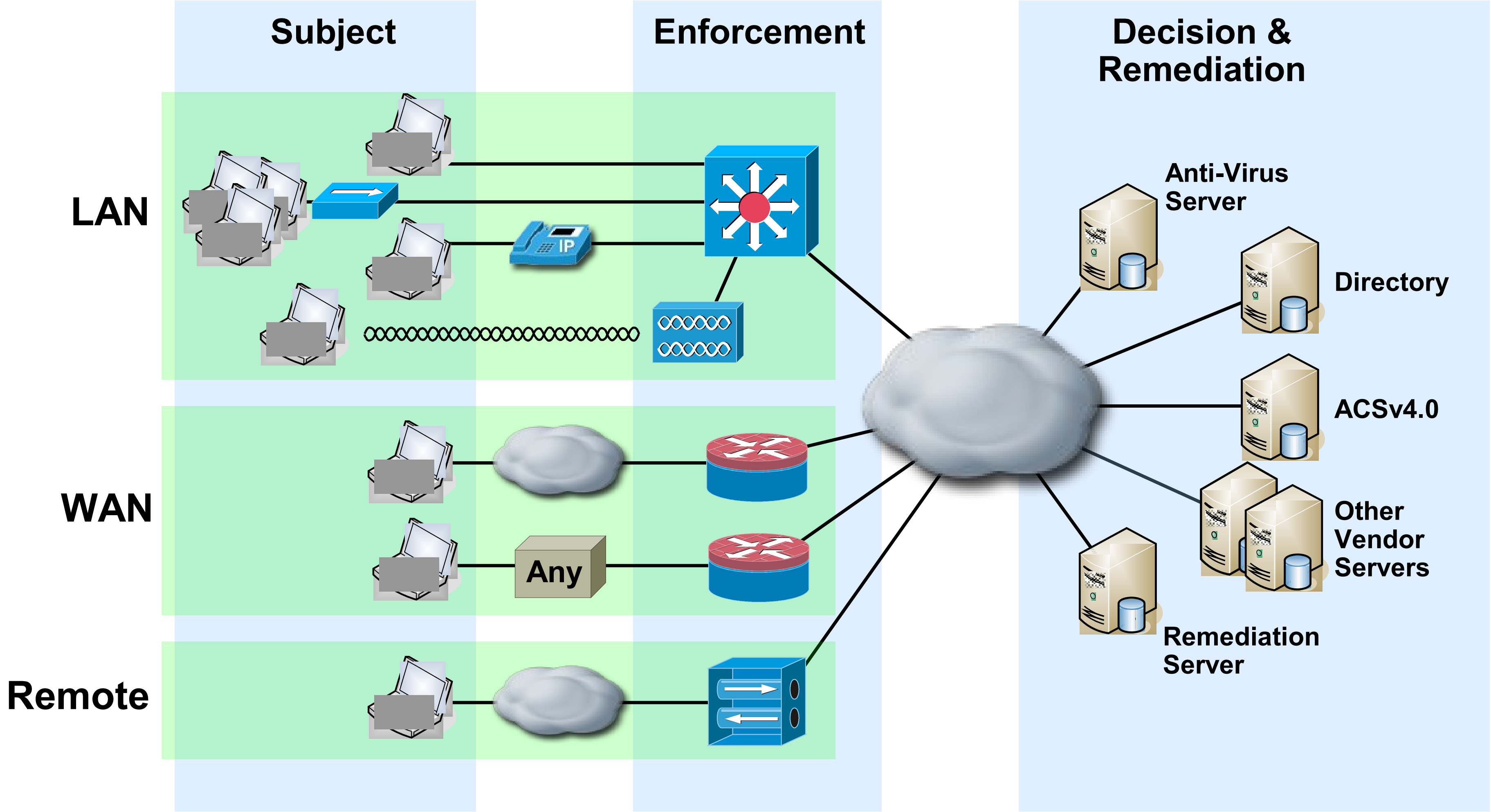
The Right Way: Network Admission Control

Admission Policy:
- Identity
- Windows XP
- Service Pack 2
- CTA 2.0
- Anti-Virus
- Patch Management

Chuck: Sales
Windows 2000
No Service Pack
No Anti-Virus
No Patch Management



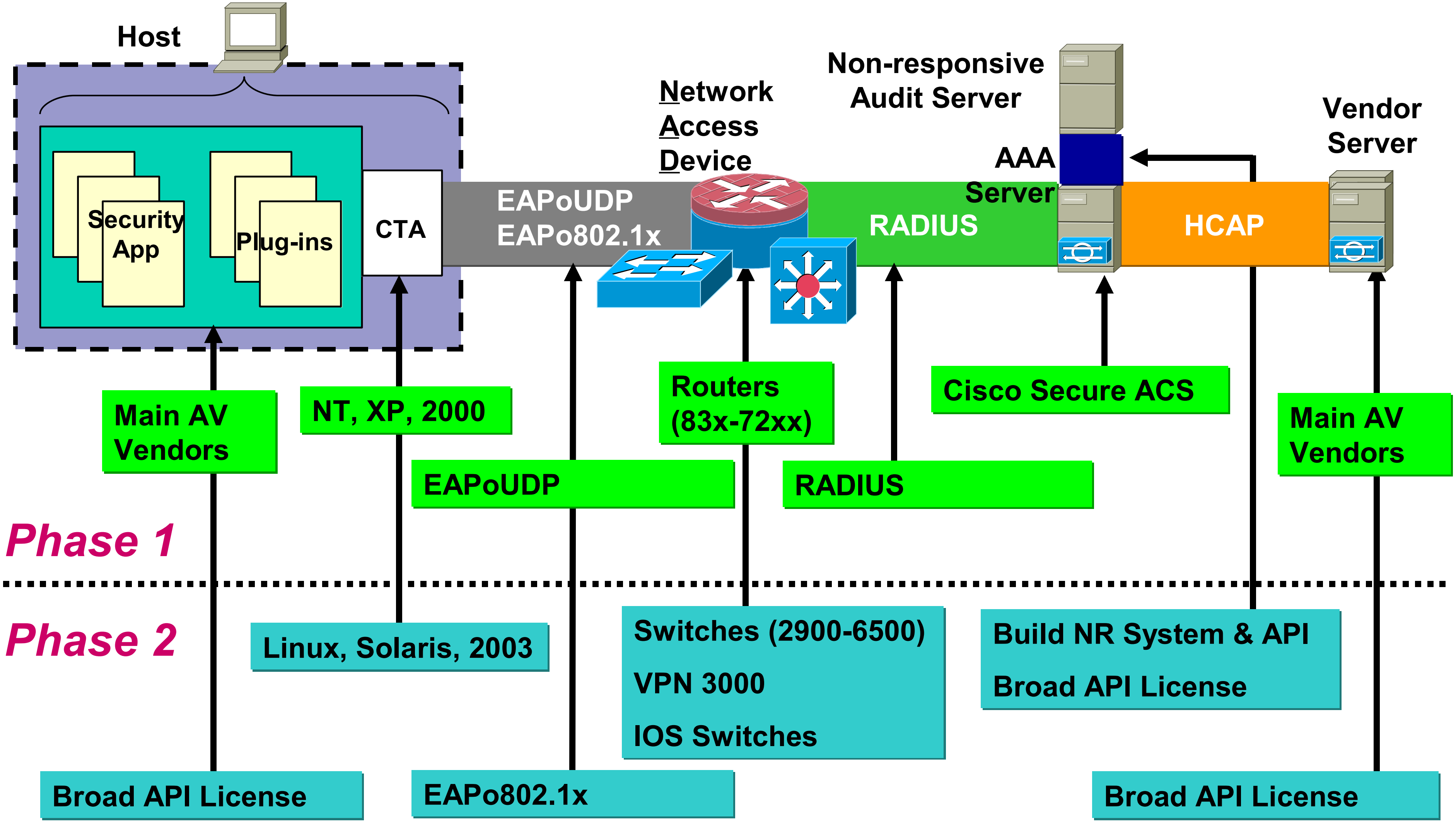
NAC Framework Deployment Scenarios



NAC Benefits

- Ubiquitous solution for all connection methods
- Validates all hosts - any OS, agent or not
- Leverages existing infrastructure – network hardware and security software
- Supports multiple security and patch software vendors through APIs
- Applications gather & assess credentials, remediation services
- Network provides visibility, enforces compliance, provides isolation, allows update services

NAC Phase 2 Logical Components



Host

Security App

Plug-ins

CTA

EAPoUDP
EAPo802.1x

Network
Access
Device

Non-responsive
Audit Server

AAA
Server

RADIUS

Vendor
Server

HCAP

Main AV
Vendors

NT, XP, 2000

Routers
(83x-72xx)

Cisco Secure ACS

Main AV
Vendors

EAPoUDP

RADIUS

Phase 1

Phase 2

Linux, Solaris, 2003

Switches (2900-6500)

VPN 3000

IOS Switches

Build NR System & API

Broad API License

Broad API License

EAPo802.1x

Broad API License

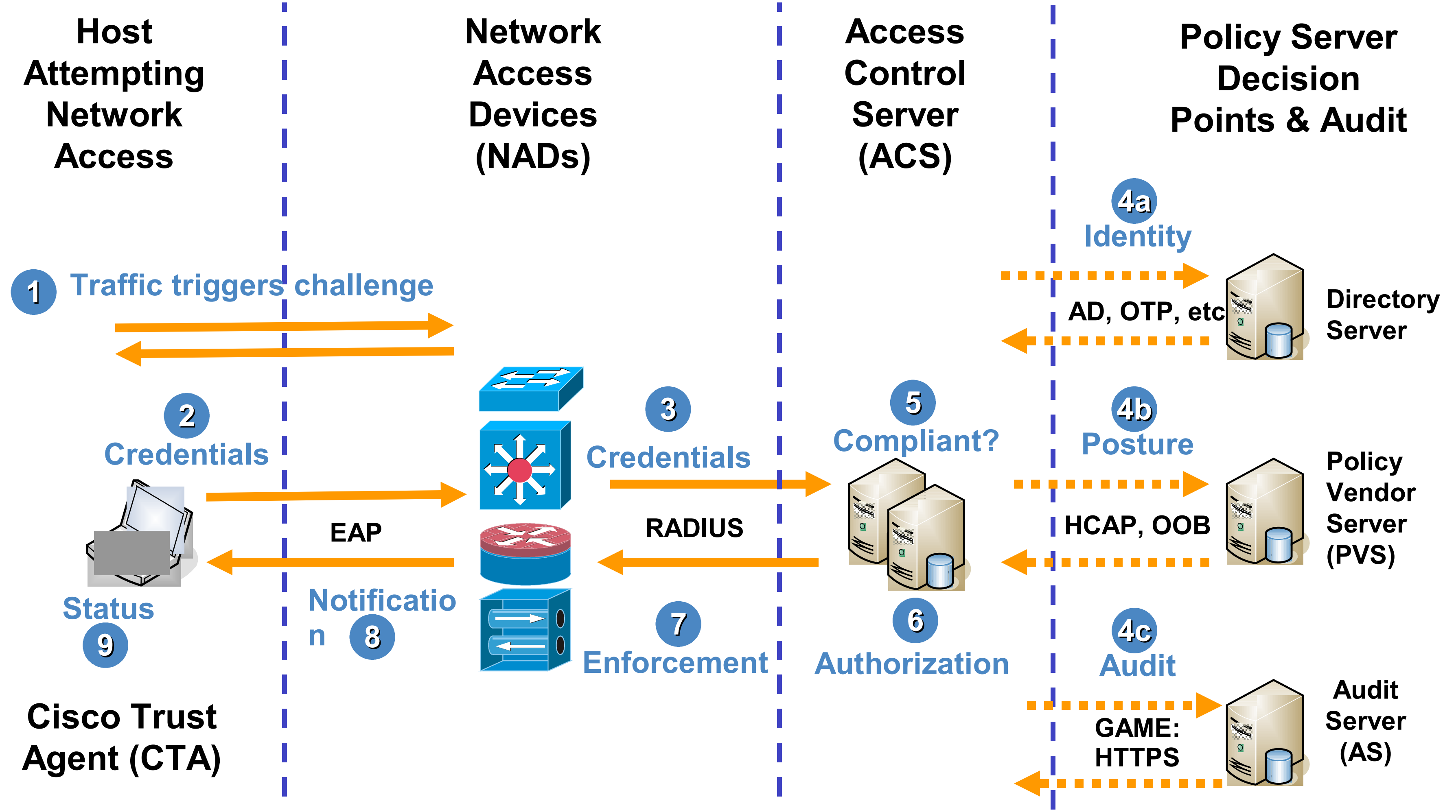
NAC Posture States

- **Healthy -** Host is compliant; no restrictions on network access.
- **Checkup –** Host is within policy but an update is available. Used to proactively remediate a host to the Healthy state.
- **Transition –** Host posturing is in process; give interim access pending full posture validation. Applicable during host boot when all services may not be running or audit results are not yet available**.**
- **Quarantine –** Host is out of compliance; restrict network access to a quarantine network for remediation. The host is not an active threat but is vulnerable to a known attack or infection
- **Infected –** Host is an active threat to other endpoint devices; network access should be severely restricted or totally denied all network access.
- **Unknown -** Host posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined. May also

NAC Admission Flow

Key: Optional

Mandatory



Host Attempting Network Access

Network Access Devices (NADs)

Access Control Server (ACS)

Policy Server Decision Points & Audit

1 Traffic triggers challenge

2 Credentials

EAP

3 Credentials

RADIUS

4a Identity

AD, OTP, etc

Directory Server

4b Posture

HCAP, OOB

Policy Vendor Server (PVS)

4c Audit

GAME: HTTPS

Audit Server (AS)

5 Compliant?

6 Authorization

7 Enforcement

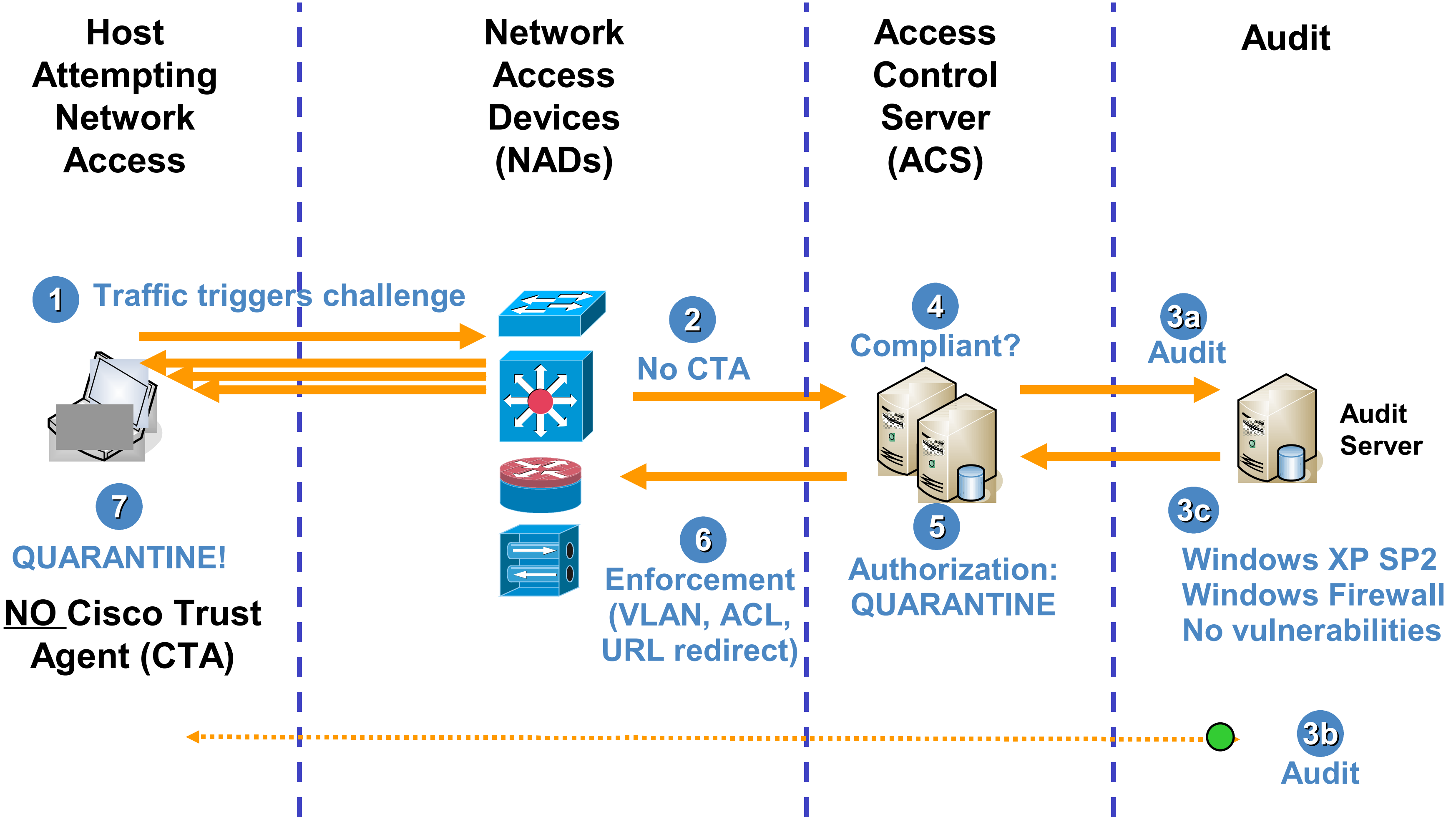
Notification 8

Status 9

Cisco Trust Agent (CTA)

Status: Result of host’s interrogation determines access to network: Full access, limited access, no access, quarantined access

NAC Agentless Host (NAH)


Host Attempting Network Access
Network Access Devices (NADs)
Access Control Server (ACS)
Audit
1 Traffic triggers challenge
2 No CTA
4 Compliant?
3a Audit
Audit Server
3c
Windows XP SP2
Windows Firewall
No vulnerabilities
5 Authorization: QUARANTINE
6 Enforcement (VLAN, ACL, URL redirect)
7 QUARANTINE!
NO Cisco Trust Agent (CTA)
3b Audit

Status: Quarantine because OS patch level is compliant except CTA is missing. After CTA is installed, on the next posture check the client would most likely become HEALTHY.

Strong NAC Partner Program

http://www.cisco.com/en/US/partners/pr46/nac/partners.html

ANTI VIRUS

McAfee®

symantec.

TREND MICRO

AhnLab

ca

金山在线 www.kingsoft.com

F-SECURE®

NORMAN®

SOPHOS

Panda Software

RISING® 瑞星

REMEDIATION

IBM®

altiris® intuitive > manageability

BIGFIX®

iPass®

LANDesk® SOFTWARE

PATCHLINK™ The Patch Management Experts™

CLIENT SECURITY

authentium

CITADEL SECURITY SOFTWARE

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

Netcordia

secure elements

SkyRecon®

BELARC

CREDANT® TECHNOLOGIES Be mobile. Be secure.

infoexpress network integrity enforcement

NEW BOUNDARY TECHNOLOGIES

Safend

StillSecure®

BINDVIEW Insight at Work

elemental security

eEye Digital Security®

INTERNET SECURITY SYSTEMS®

OPSWAT

SENFORCE

SYGATE

BLUECAT NETWORKS® secure networks, simplified.

ENDFORCE

PREVENTSYS

TRUST DIGITAL®

CAYMAS SYSTEMS

GUARDEDNET®

lockdown NETWORKS

phoenix® technologies

PREDATORWATCH

TriGeo Network Security

WHOLESECURITY

Microsoft / Cisco Joint Announcement

October 18, 2004

Microsoft®

Cisco and Microsoft Team to Improve Network Security

Companies will work toward compatibility, interoperability of respective security architectures

Cisco and Microsoft announced that they will work together to ensure compatibility and develop interoperability between their respective security architectures. For Cisco this collaboration further demonstrates the company's commitment to reinventing network security.

Interoperability **Integration** **Standardization**

NAC Advantages

- Appliance ***and*** Framework solutions
- Comprehensive span of control
  - Routers, Switches, VPNs, wireless, plus complex deployments, including IP Telephony
- 100% host and device compliance
  - No need to install multiple servers
- Controls managed, unmanaged, and guest endpoint devices
  - Only solution to integrate device posture and user identity
- Device health decisions made at the network, not on the endpoint device
  - Limits ability to misrepresent device as "healthy" to the network
- Enjoys widest use of any technology
  - Including the most robust partner program
- NAC Appliance interoperable with NAC Framework
  - Future integration will provide smooth transition to architecture-based approach

NAC Benefits

Dramatically Improves Security

- Ensures endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy
- Proactively protects against worms, viruses, spyware, and malware
- Focuses operations on prevention, not reaction

Extends Existing Investments

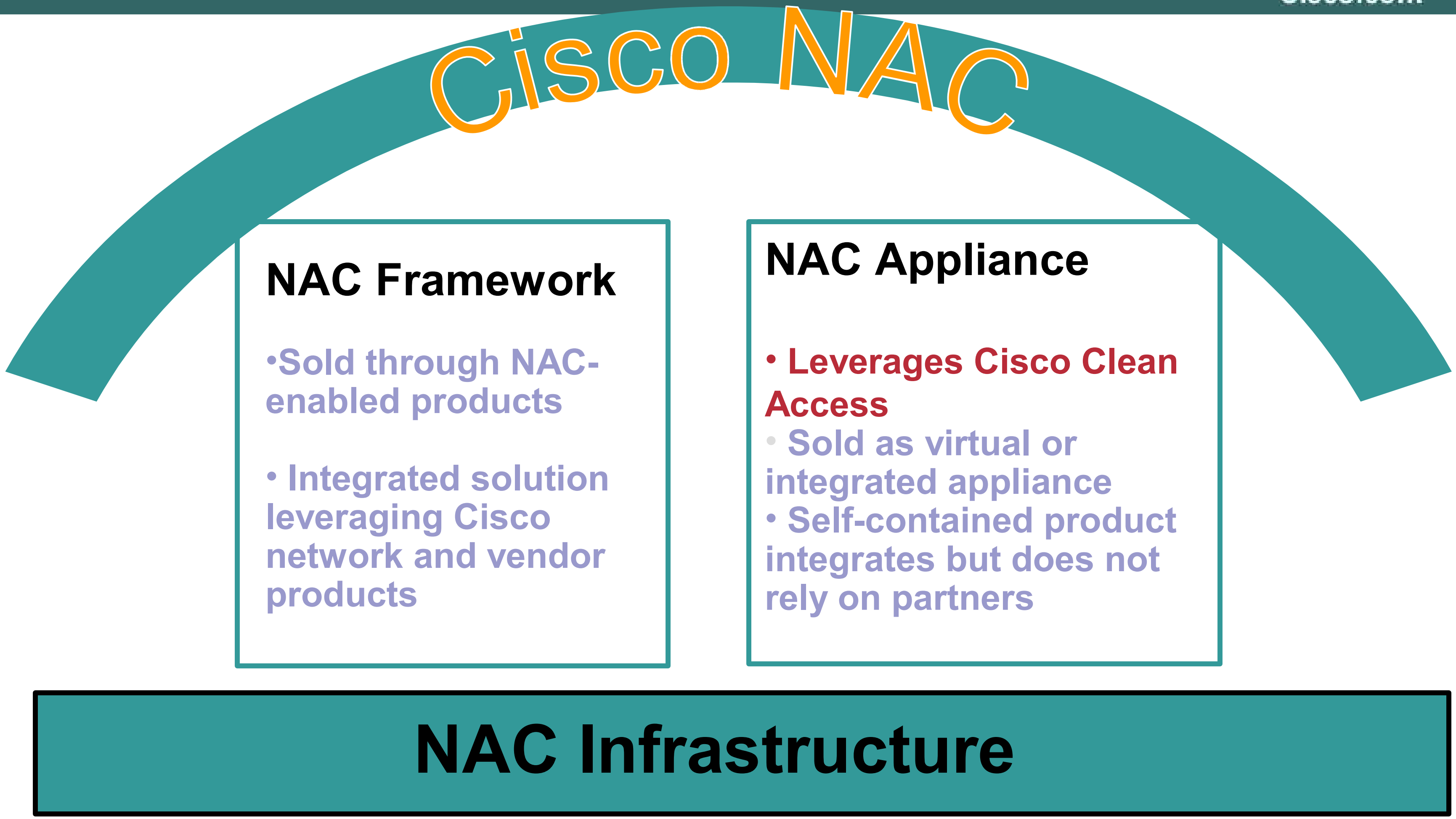
- Broad integration with multi-vendor antivirus, security, and management software
- Enhances investment in network infrastructure and vendor software

Increases Enterprise Resilience

- Comprehensive admission control across all access methods (LAN, WAN, Wireless, VPN, etc.)
- Prevents non-compliant and rogue endpoints from impacting network availability
- Reduces OpEx related to identifying and repairing non-compliant, rogue, and infected systems

NAC Positioning Change

End-April with CCO OOB Release



Cisco NAC

NAC Framework

- Sold through NAC-enabled products
- Integrated solution leveraging Cisco network and vendor products

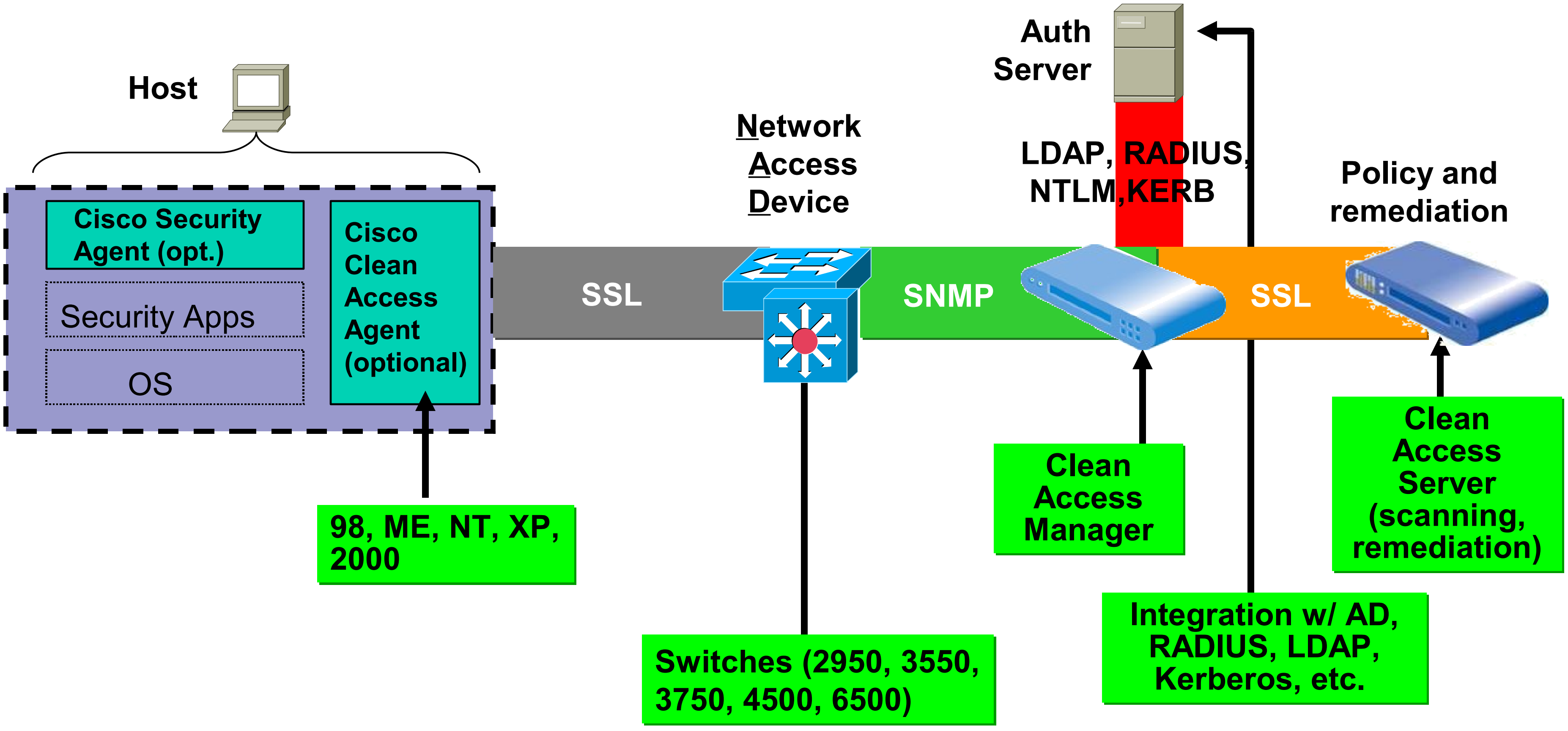
NAC Appliance

- Leverages Cisco Clean Access
- Sold as virtual or integrated appliance
- Self-contained product integrates but does not rely on partners

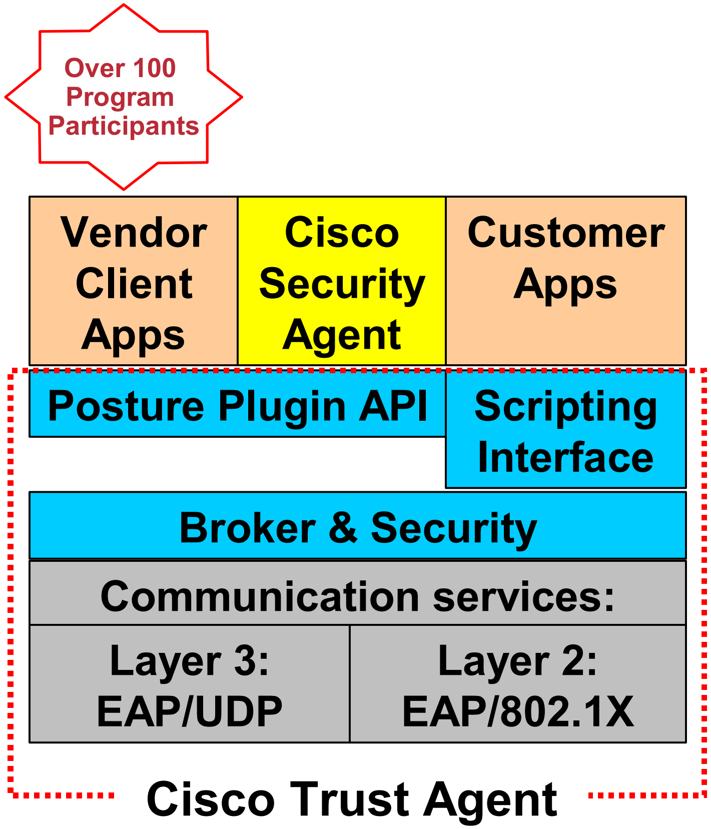
NAC Infrastructure

- Offers customers a deployment timeframe choice
- Adapts to customers' investment protection requirements

NAC Appliance Logical Components


Host
Cisco Security Agent (opt.)
Security Apps
OS
Cisco Clean Access Agent (optional)
98, ME, NT, XP, 2000
SSL
Network Access Device
Switches (2950, 3550, 3750, 4500, 6500)
SNMP
Auth Server
LDAP, RADIUS, NTLM,KERB
Clean Access Manager
Integration w/ AD, RADIUS, LDAP, Kerberos, etc.
SSL
Policy and remediation
Clean Access Server (scanning, remediation)

Cisco Trust Agent 2.0



- Supported on Windows 2000, XP, 2003 and Red Hat Linux
- Supports 2 transport layers

  EAPoUDP - layer 3

  EAPo802.1x - layer 2 (Windows only)
- Includes OEM 802.1x supplicant from Meetinghouse Communications

  Wired functionality only

  Can be replaced by a retail version from either Funk or MDC for full feature support
- Gathers OS information including patch and hotfixes
- Includes Customer Scripting Interface for custom posture information
- Backward compatible with CTA 1.0 posture plugins from NAC Program Participants
- Expanded debug/diagnostic output

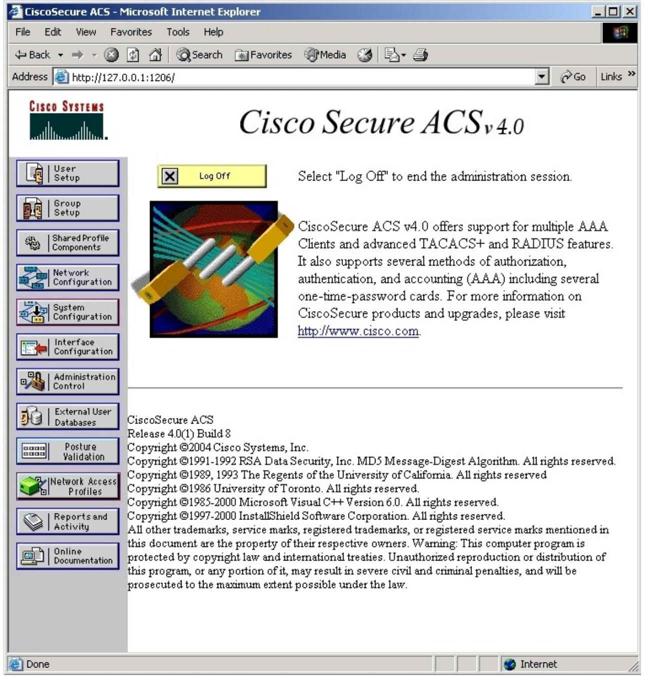
Access Control Server (ACS) v4.0

New Features

- Network Access Profiles
  - Services: Groups, Protocols, Attributes
  - Authentication: Protocols, Directories
  - Compliance: Posture & Audit Policies
  - Authorization: Groups, RACs, ACLs
- Audit Services

Software only release

Appliance update in v4.1



Select "Log Off" to end the administration session.

CiscoSecure ACS v4.0 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

CiscoSecure ACS
Release 4.0(1) Build 8
Copyright ©2004 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Router Platform Support

- **NAC L3 IP shipped June 2004**

  T-train images with Security

  The same image that includes firewall, NIPS, and crypto

- **NAC Agentless host assessment expected in NAC2.1**

- **Mirage support expected in NAC2.1**

  16, 24, 48 port NM

  2800, 3700, 3800 switch platforms

  NAC L2 802.1x & NAC L2 IP

Cisco 18xx, 28xx, 38xx	Yes

Cisco 72xx, 75xx	Yes
Cisco 37xx	Yes
Cisco 3640, 3660-ENT Series	Yes
Cisco 2600XM, 2691	Yes
Cisco 1701,1711, 1712, 1721, 1751, 1751-V, 1760	Yes
Cisco 83x	Yes
Cisco 74xx, 73xx, 71xx (S-train)	TBD
Cisco 5xxx	TBD
Cisco 4500	No
Cisco 3660-CO Series	No
Cisco 3620	No
Cisco 2600 non-XM Models	No
Cisco 1750, 1720, 1710	No

VPN Concentrators

- Models 3005-3080
- Release v4.7 supports NAC L3 IP
- VPN Client does not include CTA
- Works with IPSec and L2TP/IPSec remote access sessions.

  NAC processing starts after an IPsec session is established

  Communication with CTA is within IPsec SAs

  NAC does not apply to PPTP, L2TP or LAN-to-LAN sessions
- Local exception lists also include OS type
- NAC Agentless Host assessment is not supported yet; timeline is TBD

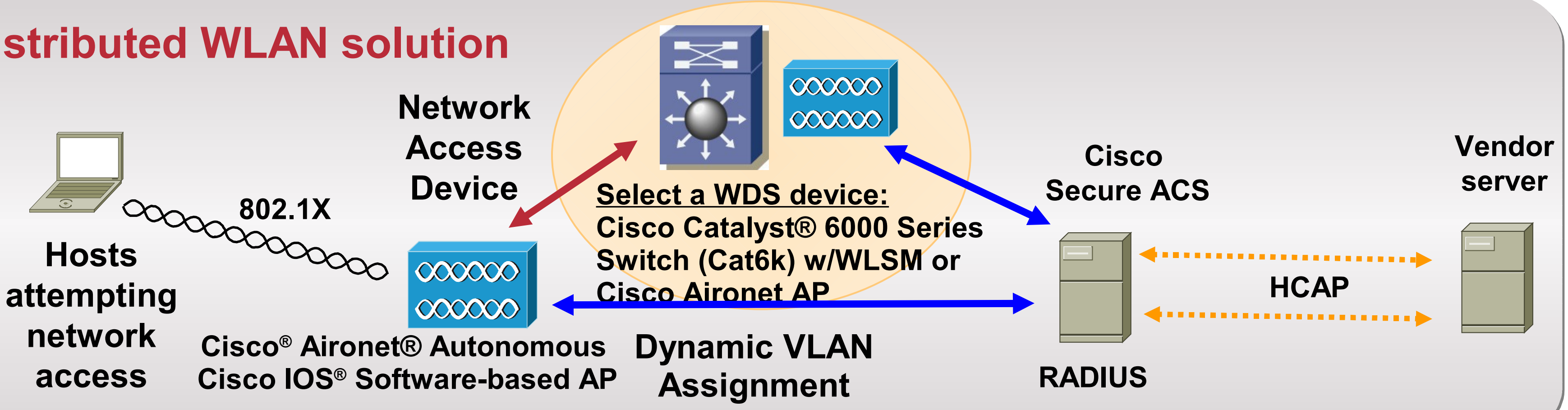
Switch Platforms

Progressive Functional Tiers

Platform, Supervisor	OS	NAC L2 802.1x	NAC L2 IP	NAC L3 IP	NAC Agentless Host
6500 – Sup32, 720	Native IOS	Future	Future	Future	Future
6500 – Sup2	Native IOS	Future	No	No	Future
6500 – Sup32, 720	Hybrid	2.0	2.0	Future	2.0 (NAC L2 IP)
6500 – Sup2	Hybrid	2.0	2.0	No	2.0 (NAC L2 IP)
6500 – Sup2, 32, 720	CATOS	2.0	2.0	No	2.0 (NAC L2 IP)
4000 Series – Sup2+, 3-5	IOS	2.0	2.0	Future	2.0 (NAC L2 IP)
3550, 3560, 3750	EMI, SMI	2.0	2.0	No	2.0 (NAC L2 IP)
2950	EI, SI	2.0	No	No	No
2940, 2955, 2970	All	2.0	No	No	No
6500 – Sup1A	All	No	No	No	No
5000	All	No	No	No	No
4000/4500	CATOS	No	No	No	No
3500XL	All	No	No	No	No
2900XM	All	No	No	No	No

NAC Framework
WLAN Deployment

Distributed WLAN solution



Hosts attempting network access

802.1X

Network Access Device

Cisco® Aironet® Autonomous Cisco IOS® Software-based AP

__Select a WDS device:__
Cisco Catalyst® 6000 Series Switch (Cat6k) w/WLSM or Cisco Aironet AP

Dynamic VLAN Assignment

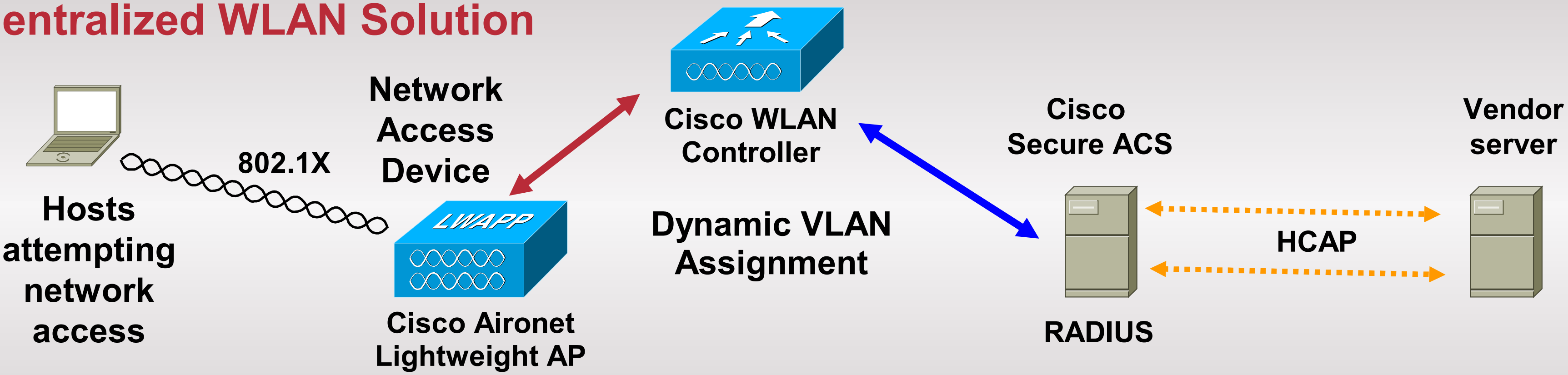
Cisco Secure ACS

RADIUS

HCAP

Vendor server

Centralized WLAN Solution



Hosts attempting network access

802.1X

Network Access Device

Cisco Aironet Lightweight AP

Cisco WLAN Controller

Dynamic VLAN Assignment

Cisco Secure ACS

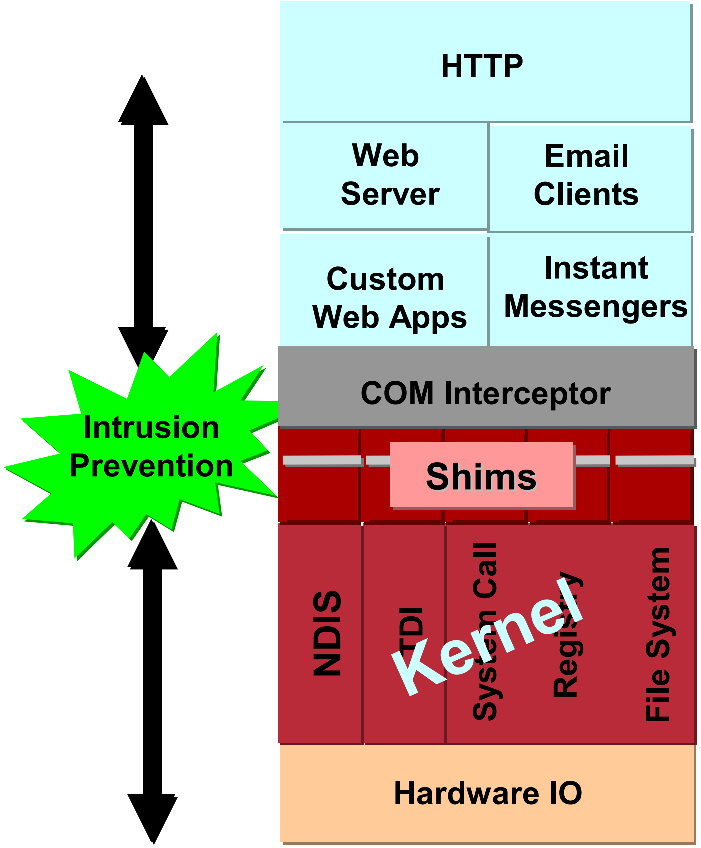
RADIUS

HCAP

Vendor server

CSA Integration

Kernel Shim Wrappers



- **CSA a valuable optional component**
  - CSA receives no special privileges vs vendor apps
- **Offers OS credentials & endpoint integrity**
  - Provides OS info including patch & hotfix
  - Hardens endpoint, more immune to attack
  - Protects CTA from application spoofing
  - Custom policy that 'understands' CTA behavior
- **NAC Support**
  - CSA 4.0.2 integrated with CTA/NAC
  - CSA 4.5 bundles CTA for distribution

Cisco Security Agent (CSA)

- CSA is an optional NAC component
- CSA v4.5 and later includes CTA v1.0

    CTA 2.0 bundling expected

- HIPS technology is recommended to protect the integrity files of all host security applications, including CTA!
- CSA policies can lockdown the host based on the posture received from a NAC authorization

    e.g. CSA can disable all host applications except patch management and anti-virus upon NAC Quarantine response

CISCO SYSTEMS