Cisco Clean Access Overview (NAC Appliance)

Zeno Dequal

Systems Engineer – Cisco Systems Italy

zdequal@cisco.com

Contents

- The Business Case for Network Admission Control
- Clean Access Product Overview
- Deployment Considerations
- Conclusion
- Demo

The Vulnerability of Networks

- **Every bit of data customers are concerned about touches the network**
- **Every device customers are concerned about is attached to the network**
- **In this environment, EVERYTHING is a potential target AND a potential threat**

Threat vectors have changed: your "trusted users" can be the weakest link in your network's security

The Need For Admission Control

- **Viruses, worms, spyware, etc. still #1 cause of financial loss***

  Downtime, recovery, lost productivity, credibility, legal implications

- **Users routinely authenticated, but...**
- **Endpoint devices (laptops, PCs, PDAs) are not checked for security policy compliance**
- **Unprotected endpoints spread infection**

  Required security software not installed, disabled, or out of date

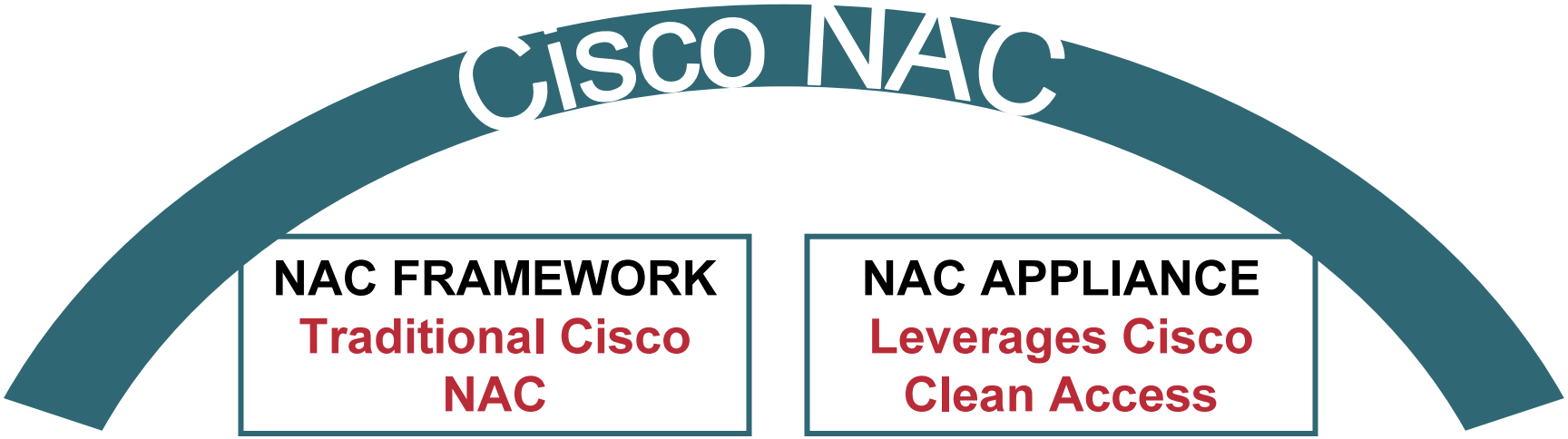
  Checking for compliance is difficult and expensive

***2005 FBI/CSI Report**

"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

Cisco NAC Umbrella: Two Models



Embedded in the infrastructure

Integrated solution leveraging Cisco network and vendor products

Virtual or integrated appliance

Self-contained product integrates but does not rely on partners

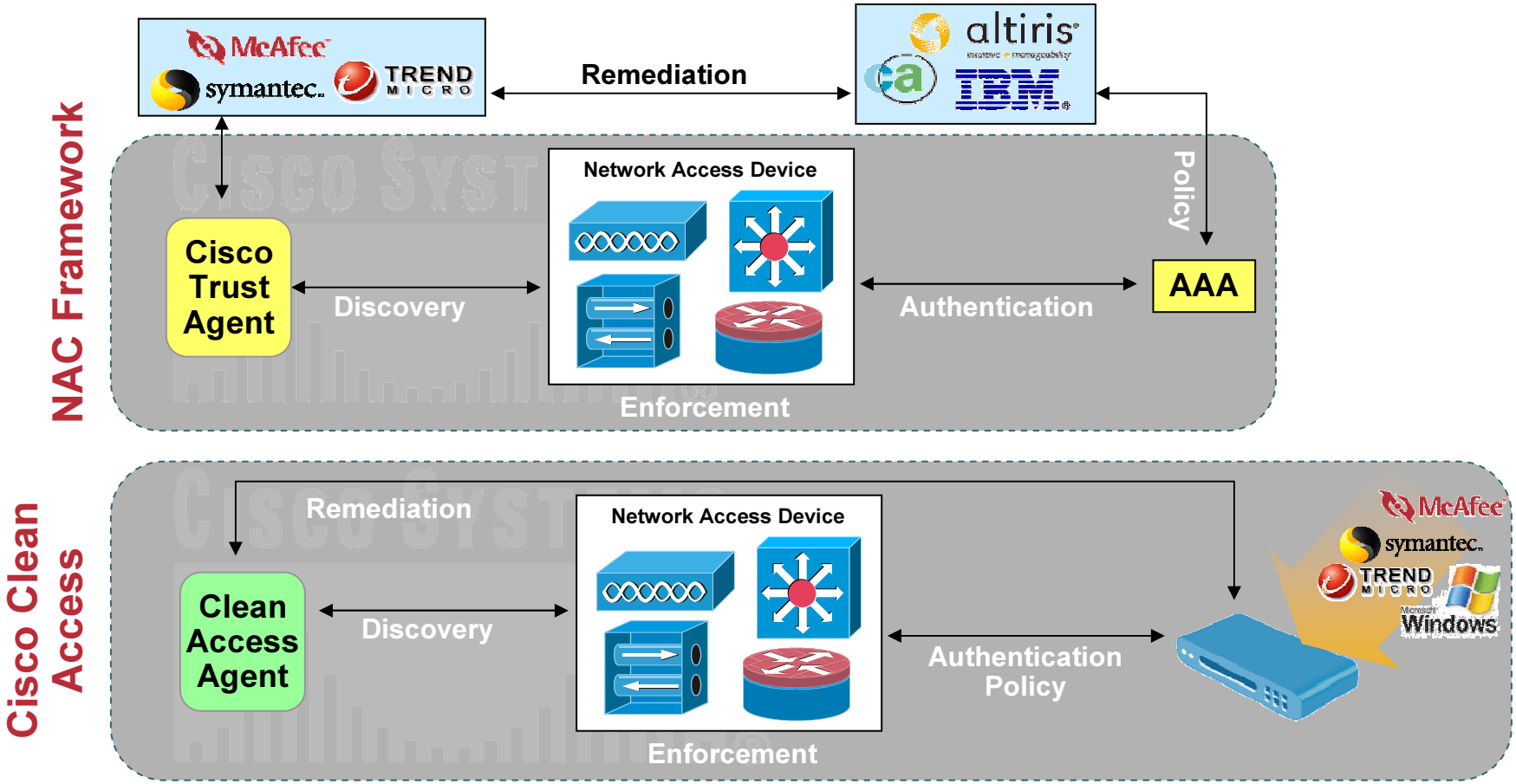
- **Offers customers a deployment timeframe choice**
- **Adapts to customers' investment protection requirements**

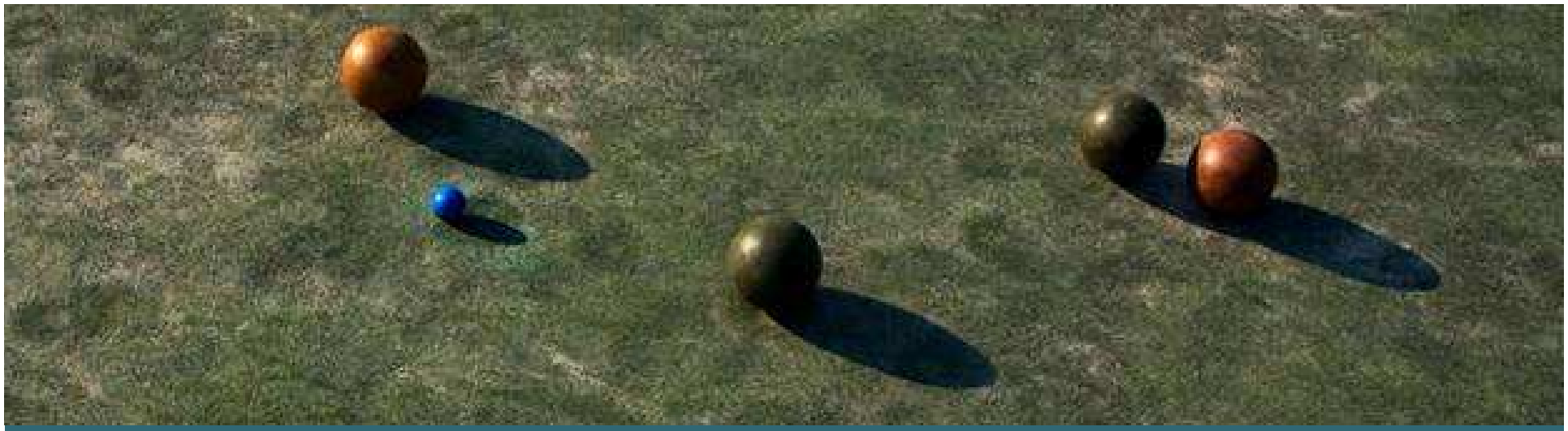
Network Admission Control Options

Two Paths: Both Leverage Cisco Network

NAC Framework: Vendor products provide assess and remediate across an intelligent network

Cisco Clean Access: Turnkey NAC appliance for authentication, assessment, and remediation



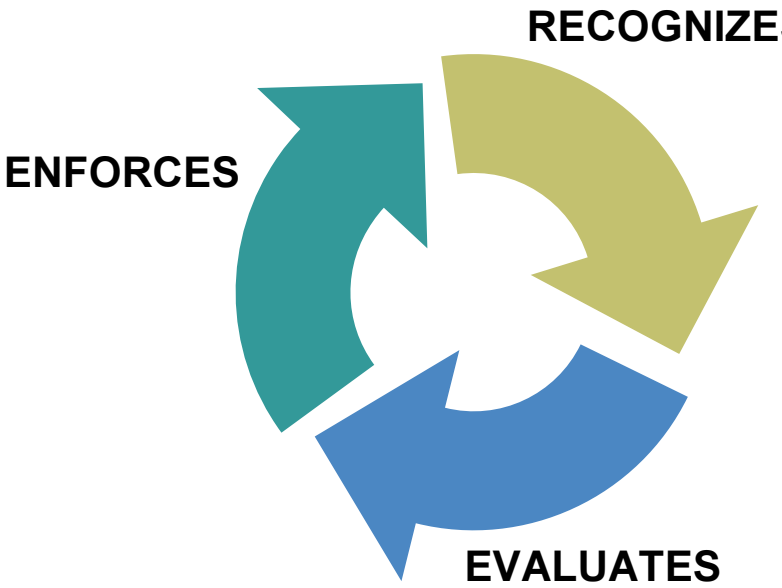


Clean Access Product Overview

2

Cisco Clean Access: NAC Appliance

Before allowing users onto the network, whether it's a local, remote, wired or wireless, Clean Access:



Recognizes:

Users, device, and role (guest, employee, contractor)

Evaluates:

Identify vulnerabilities on devices

Enforces:

Eliminate vulnerabilities before network access

Cisco Clean Access Highlights

- **Fits into widest array of infrastructure requirements**
  - In-band deployment is agnostic to switching and routing infrastructure
  - In-Band or Out-of-Band
  - Virtual Gateway, Real-IP Gateway/NAT or Failover Mode
- **Fast to deploy, inexpensive to manage**
  - Automated updates for Microsoft hotfixes, anti-spyware and AV packages
  - Manage multiple subnets with single box
    - Support for 802.1Q based VLAN trunking
    - Support for /30 subnet per VLAN
- **Scales to your size and accommodates growth**
  - SKUs for 100-user groups to enterprise boxes
  - Grow by adding boxes

Cisco Clean Access Components

- **Cisco Clean Access Manager (CAM)**

  Centralizes management for administrators, support personnel, and operators

- **Cisco Clean Access Server (CAS)**

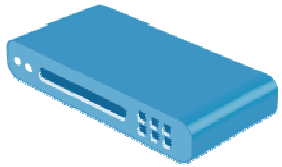
  Serves as an in-band or out-of-band device for network access control

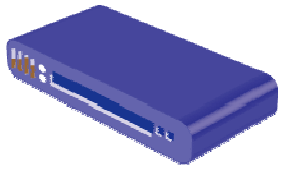
- **Cisco Clean Access Agent**

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

- **Rule Set Updates**

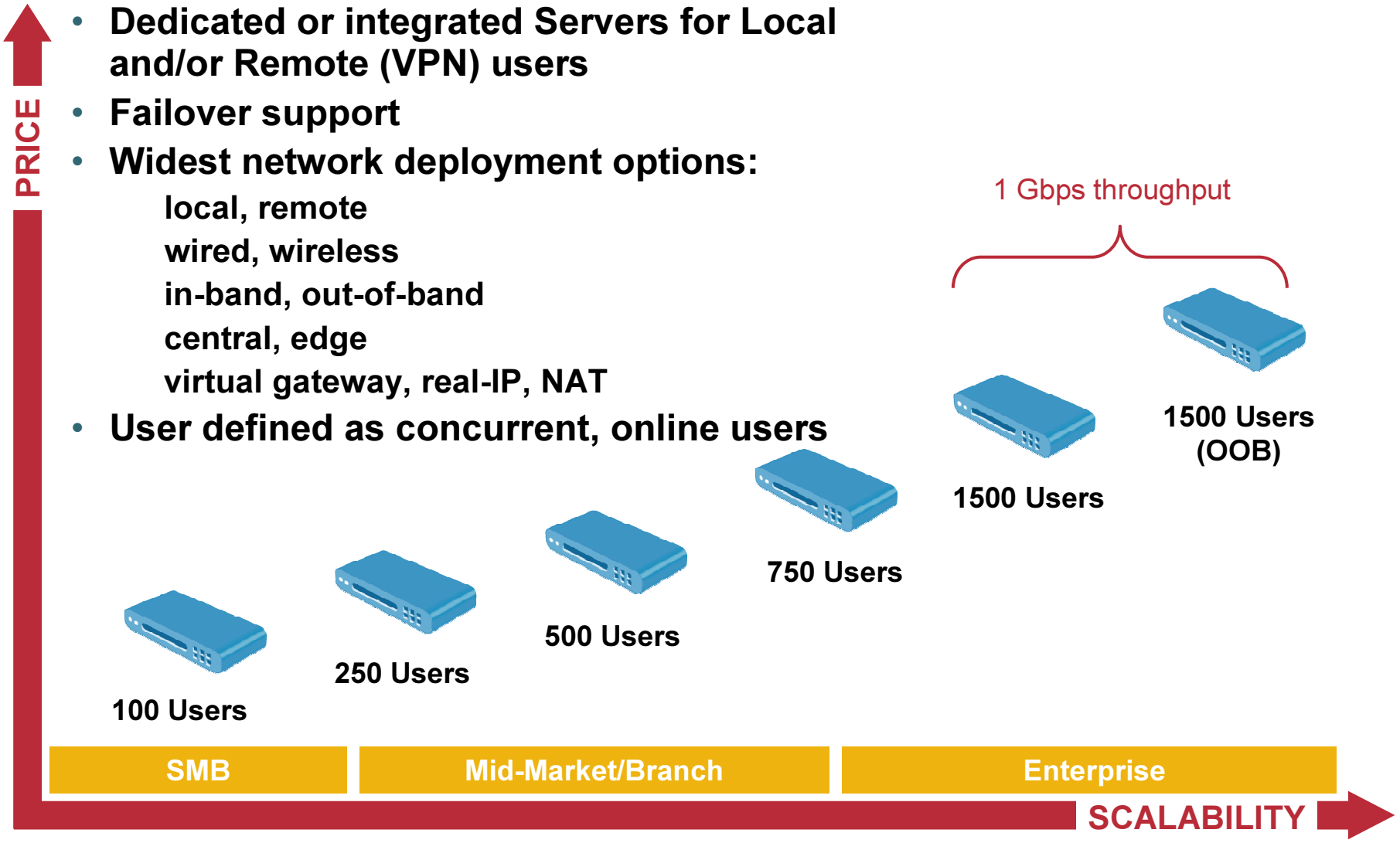
  Scheduled automatic updates for anti-virus, critical hotfixes and other applications



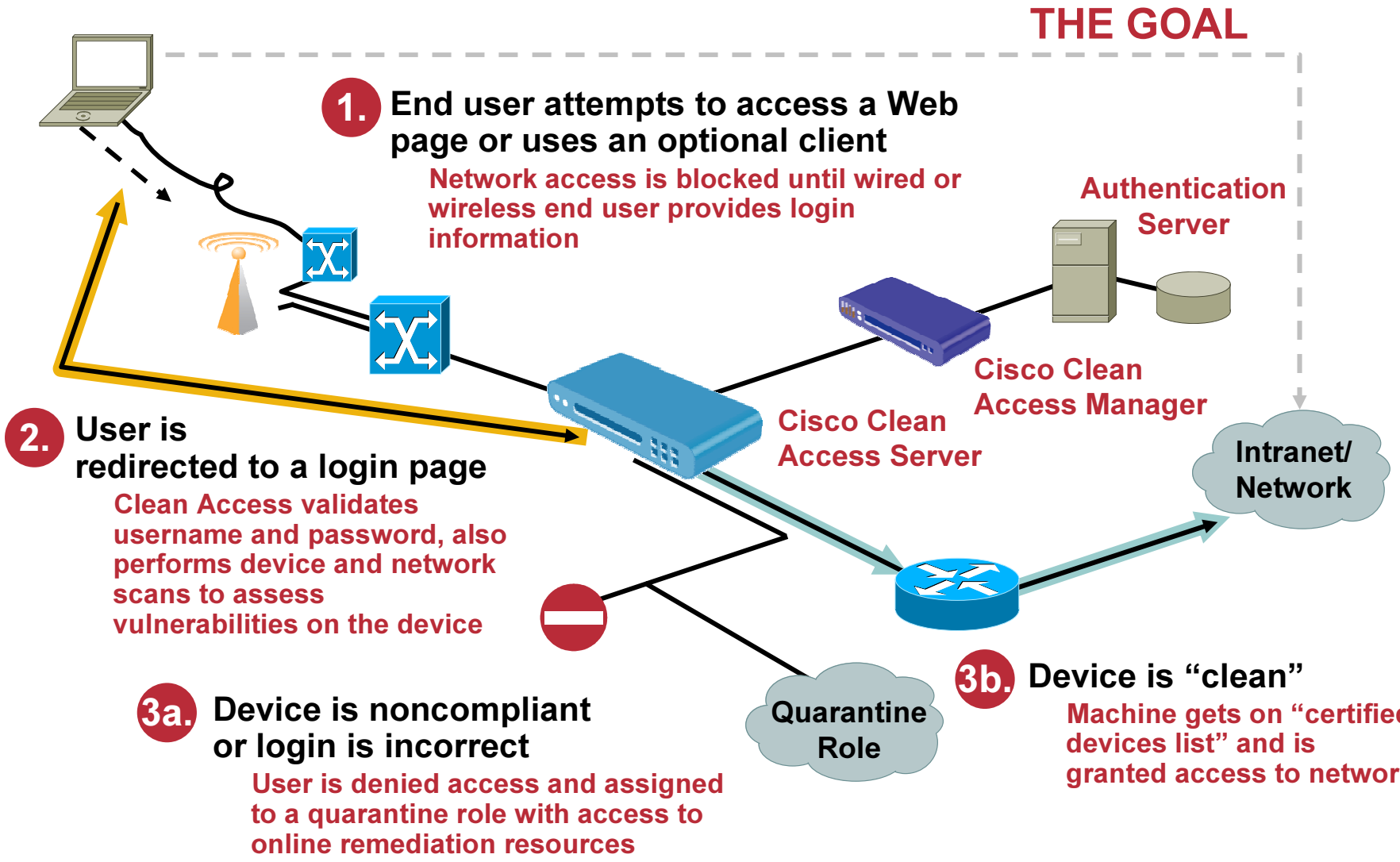


Cisco Clean Access Servers Options

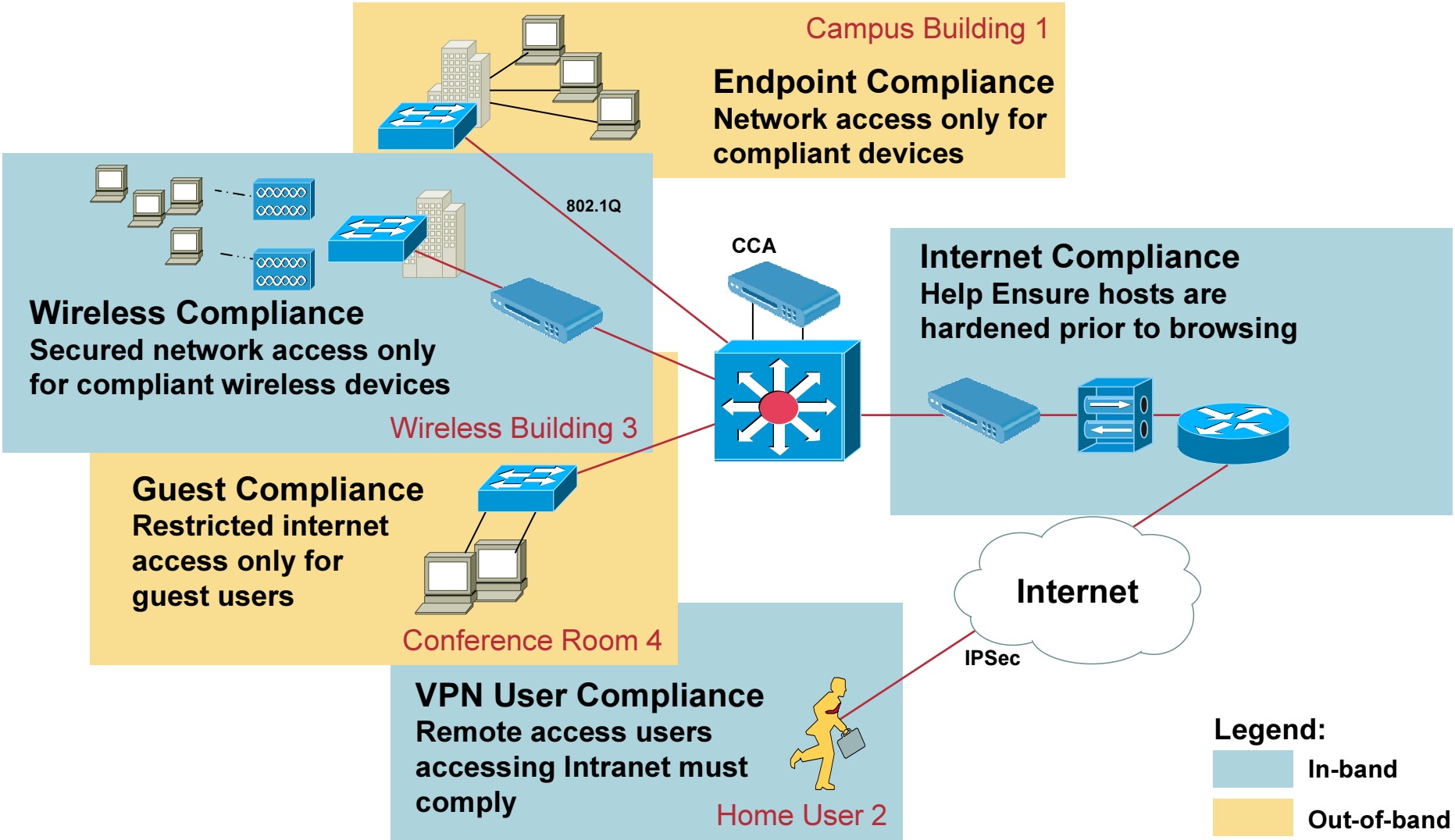
- **Dedicated or integrated Servers for Local and/or Remote (VPN) users**
- **Failover support**
- **Widest network deployment options:**
  - **local, remote**
  - **wired, wireless**
  - **in-band, out-of-band**
  - **central, edge**
  - **virtual gateway, real-IP, NAT**
- **User defined as concurrent, online users**



Cisco Clean Access Overview



Clean Access Use Case Scenarios



Some Pre-Configured Clean Access Checks

- **Critical Windows Updates**

  Windows XP, Windows 2000, Windows 98, Windows ME

- **Anti-Virus Updates**

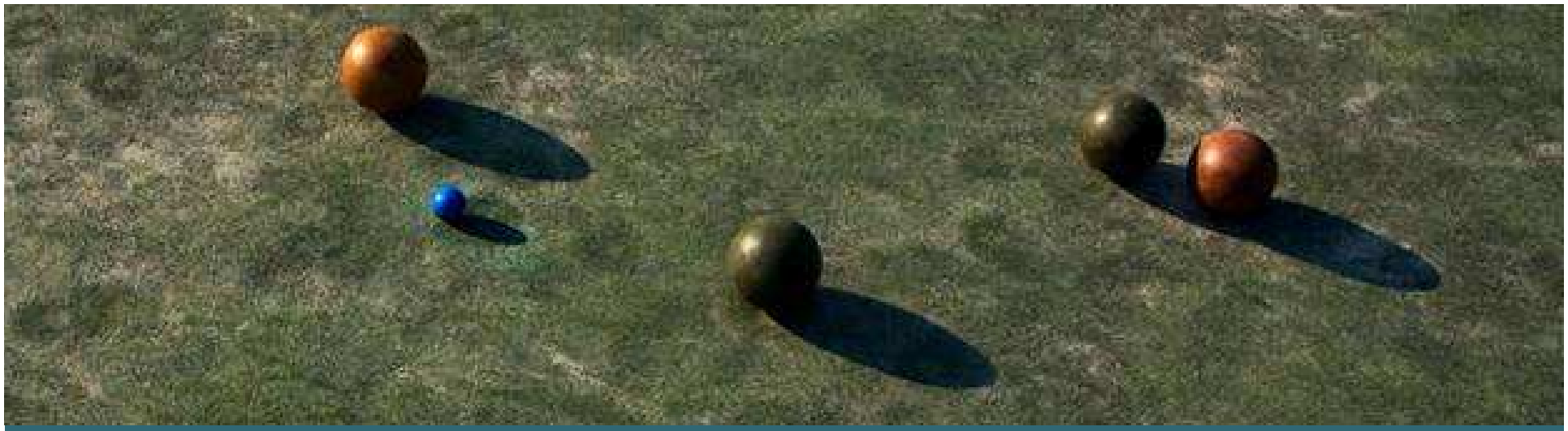
- **Anti-Spyware Updates**
- **Other 3rd Party Checks**

Cisco Security Agent

Customers can easily add customized checks

New Features in Clean Access v3.6

- **Hardware + software appliances for both Clean Access Server and Clean Access Manager**
- **Pre-configured with anti-spyware checks from most major anti-spyware vendors**
- **Single-sign-on capabilities with ASA and VPN3000**



Deployment Considerations

3

In-Band Details

- **The CAS is always inline with user traffic:**
  - **Before, during and after authentication, posture assessment and remediation**
  - **Enforcement is achieved through inline mode**
- **The CAS can be used to securely control authenticated and unauthenticated user traffic by:**
  - **Managing traffic policies based on port, protocol, subnet**
  - **Providing bandwidth policy management based on shared or per-user**
  - **Using time-based session and heartbeat controls**
- **Supports any edge access devices:**
  - **When the MAC address and IP address of the client machine is visible to the CAS**
  - **Deployable in shared situations (e.g. hubs, switches, access points)**
- **Does not provide switch port level control**

In-Band Virtual Gateway

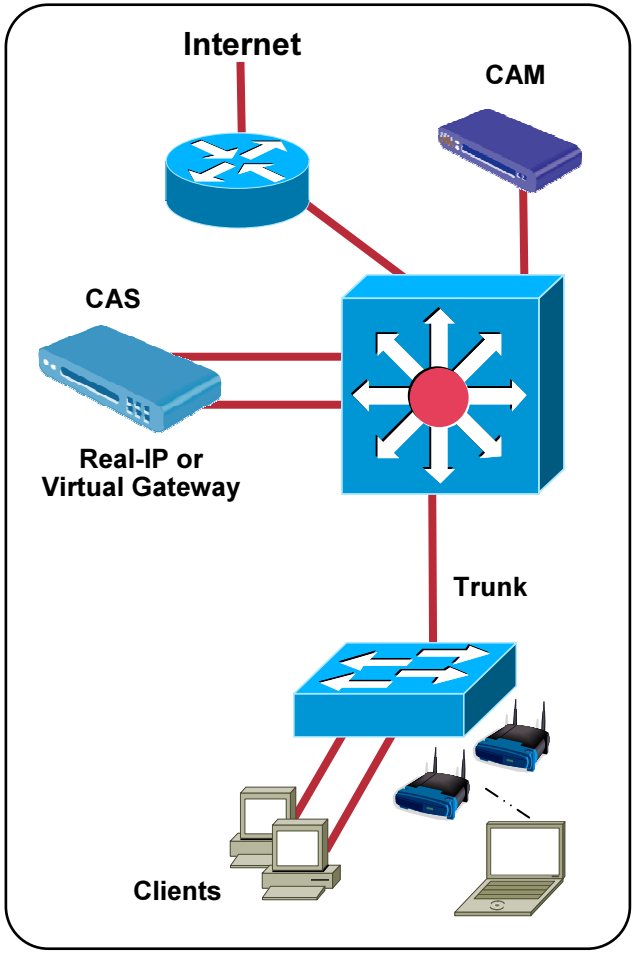
- **CAS acts as a L2 bridge for the managed network:**
  - **VLAN passthrough default enabled for 802.1Q VLANs**
  - **DHCP passthrough default enabled**
- **The CAS becomes an IP filter when authentication, posture assessment and remediation is performed.**
- **CAS deployment modes:**
  - **Edge deployment via VLAN passthrough**
  - **Central deployment via VLAN mapping**
- **Easy-to-configure**
  - **No network routing changes**
  - **No DHCP scope changes**
  - **Core switch interface VLAN configuration for VLAN mapping**

In-Band Real-IP

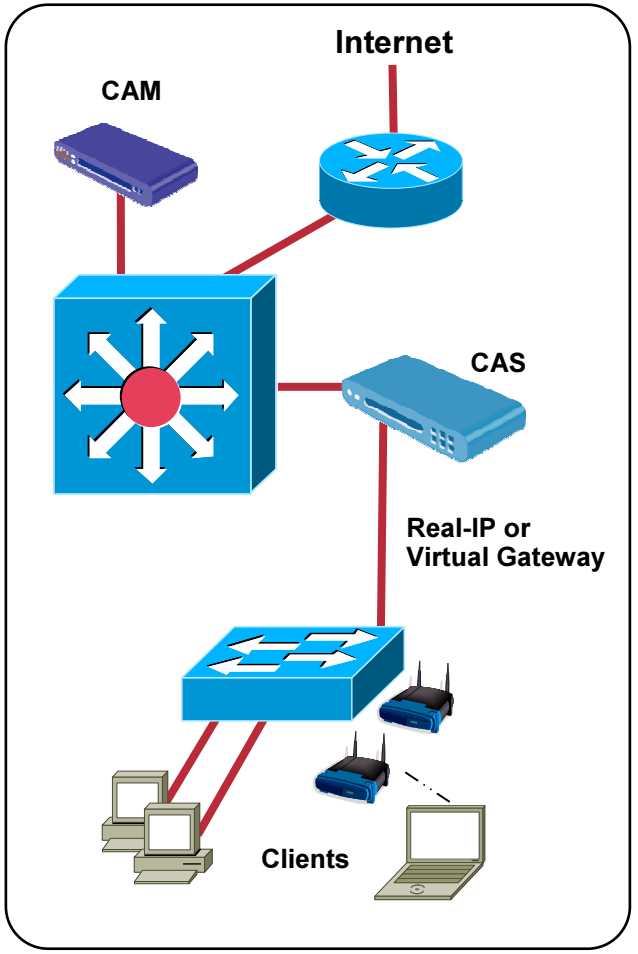
- **The CAS acts as a L3 router for the managed network:**
  - **802.1Q VLAN trunk support via Managed Subnets**
  - **Secondary gateway support for trunked VLAN subnets**
  - **Routing between managed subnets**
- **The CAS can provides advanced DHCP services:**
  - **DHCP /30 network scopes to prevent subnet-based infection**
  - **DHCP quick setup via auto-generate**
  - **DHCP failover support**
- **Configuration on L3 switch or router**
  - **Configure CAS as default gateway for managed subnets**
  - **Turn off routing for managed subnets on L3 switch or router**
  - **Static route for managed subnets via trusted interface**

In-Band Deployment Configuration

Central Deployment



Edge Deployment



Out-of-Band Details

- **The CAS is inline with user traffic:**
  - **Only during the process of authentication, posture assessment and remediation**
  - **Can control or limit user traffic during the process**
- **The CAS is out-of-band once user successfully logged on:**
  - **User traffic bypasses the CAS and traverse the switch port directly**
  - **CAS cannot control or limit user traffic**
  - **Enforcement is achieved through the use of SNMP to control switches and vlan assignments**
- **The CAM provides port or role-level control:**
  - **By assigning ports to specific VLANs**
  - **By assigning users to specific roles that map to specific VLANs**
  - **By providing time-based session timeout per role**
- **Does not support certain access devices:**
  - **Shared or unmanaged (e.g. hubs, access points)**

Out-of-Band Virtual Gateway

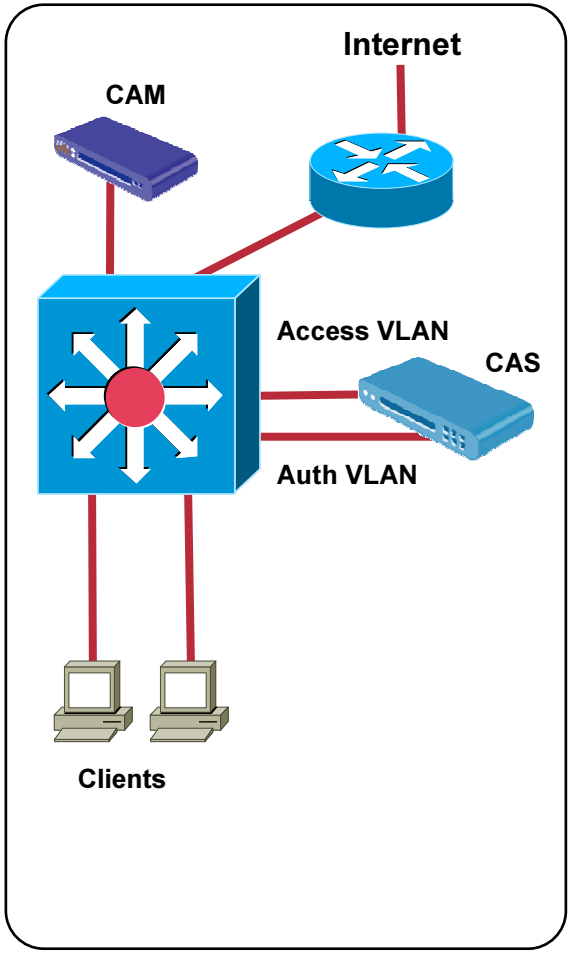
- **CAS acts as a L2 bridge when authentication, posture assessment and remediation is performed.**
  - **Central deployment via VLAN mapping for 802.1Q VLANs**
  - **User obtains real DHCP address from access VLAN**
  - **Provide access to remediation sites only during quarantine**
- **The CAS is out-of-band once user successfully logged on:**
  - **No need to bounce interface for new DHCP address**
  - **User traffic traverses the switch ports directly**
  - **User is logged out via role-based session timer or port link-down**
- **Easy-to-configure**
  - **No network routing changes**
  - **No DHCP scope changes**
  - **Core switch interface VLAN configuration for VLAN mapping**

Out-of-Band Real-IP

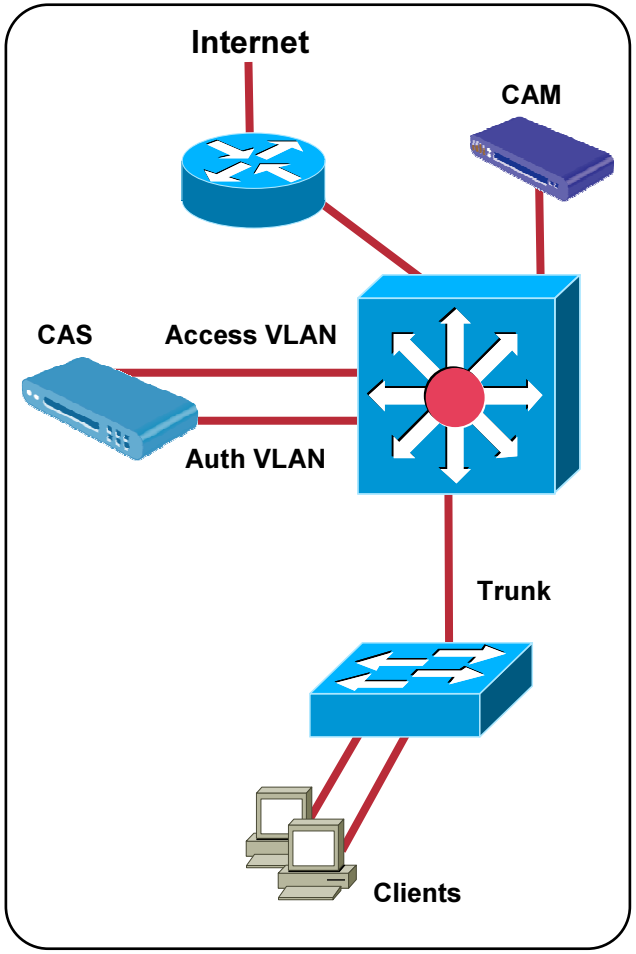
- **The CAS acts as a L3 router during the authentication, posture assessment and remediation process:**
  - **802.1Q VLAN trunk support via Managed Subnets**
  - **User obtains DHCP /30 address from authentication VLAN**
  - **Provide access to remediation sites only during quarantine**
- **The CAS is out-of-band once user successfully logged on:**
  - **Need to bounce interface for new DHCP address in access VLAN**
  - **User traffic traverses the switch ports directly**
  - **User is logged out via role-based session timer or port link-down**
- **Configuration on L3 switch or router**
  - **Configure CAS as default gateway for managed subnets**
  - **Turn off routing for managed subnets on L3 switch or router**
  - **Static route for managed subnets via trusted interface**

Out-of-Band Deployment Configuration

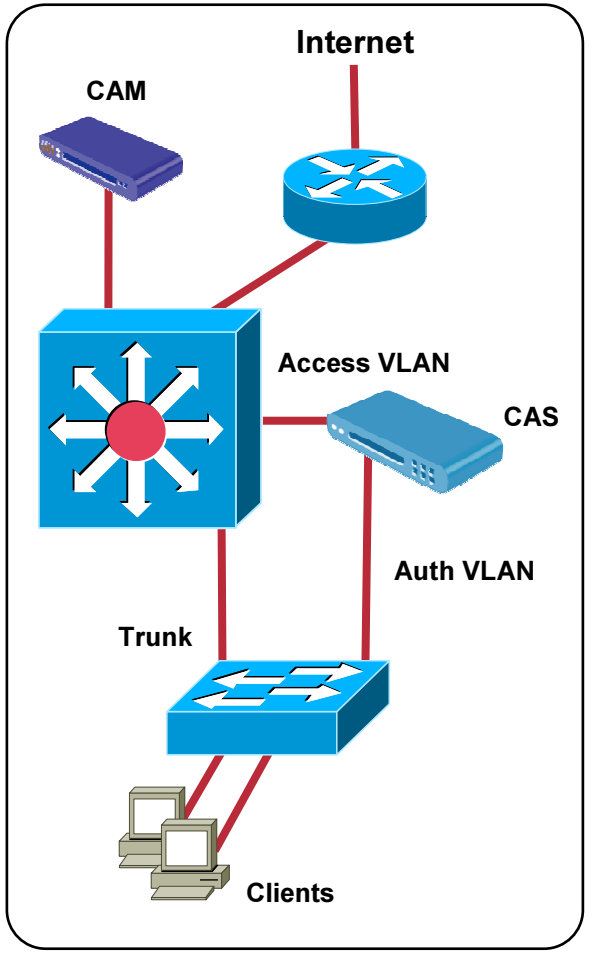
Core 65xx, 45xx Deployment



Core 65xx, 45xx Deployment



Edge 37xx, 35xx Deployment



In-Band and Out-of-Band Comparison

	In-Band	Out-of-Band
Environments	Wireless, shared media, VoIP phones, etc.	Fast core switching infrastructures; high throughput requirements
NAC Enforcement Point	Cisco Clean Access Server in-band	Cisco Clean Access Server with authentication/quarantine VLAN
Quarantine	Based on access control list (ACL)	Based on VLAN
Switches Supported	Switches from any vendor	Cisco Catalyst® 2900, 2940, 2950, 3500, 3550, 3560, 3750, 4500, and 6500 switches

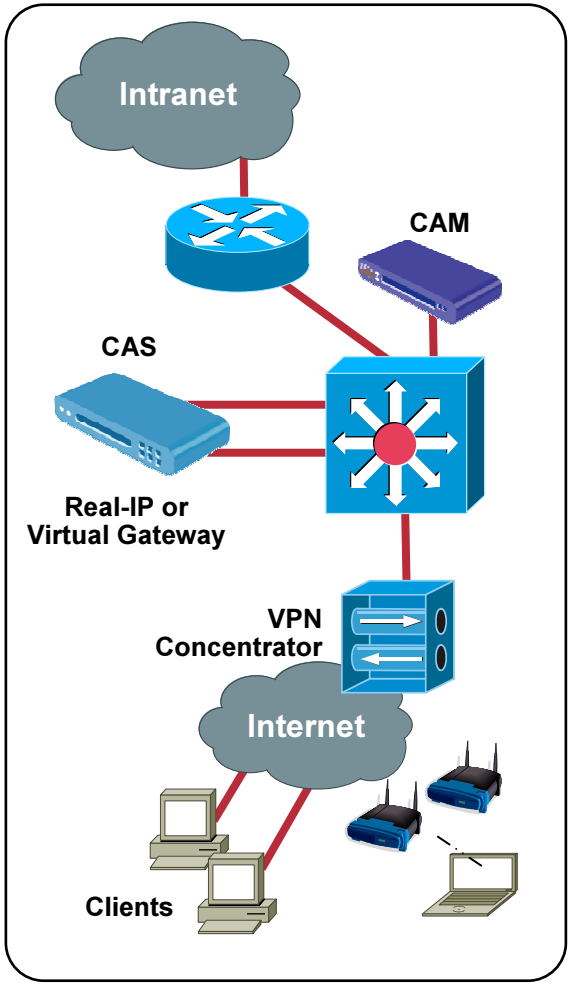
A single deployment can contain both in-band (e.g. for wireless) and out-of-band (e.g. for wired) Clean Access Servers

Remote Users

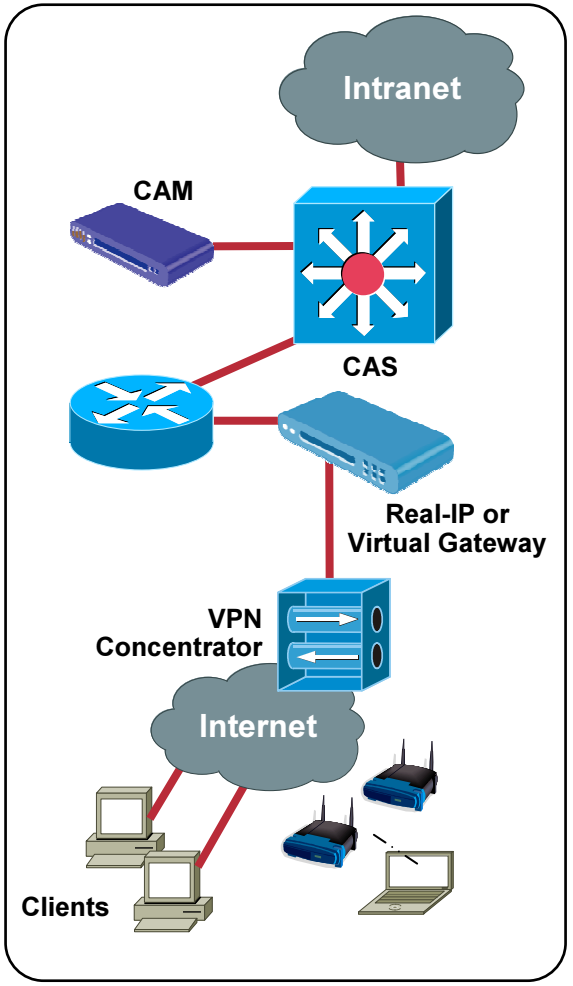
- **The Clean Access Server (CAS) can be deployed:**
  - **One or multi-hop from a Cisco 3000 Series VPN Concentrator or ASA**
  - **In-band Virtual Gateway or Real-IP mode**
- **The CAS acts a Radius Proxy Server:**
  - **Radius accounting on VPN Concentrator directing to CAS**
  - **CAS forwards accounting request to other Radius server**
- **The CAS is inline with VPN user traffic:**
  - **Before, during and after authentication, posture assessment and remediation**
- **The CAS can be used to securely control authenticated user traffic by:**
  - **Managing traffic policies based on protocol/port or subnet**
  - **Providing bandwidth policy management based on shared or per-user**
  - **Using time-based session and Radius session logout controls**

VPN Deployment Configuration

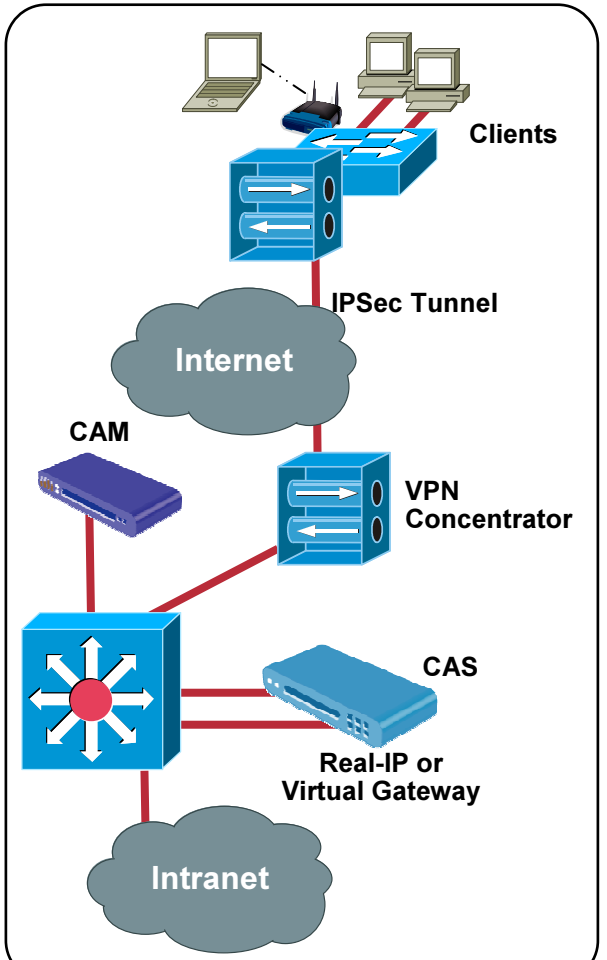
Central Deployment



Edge Deployment



Site Deployment



Conclusion

4

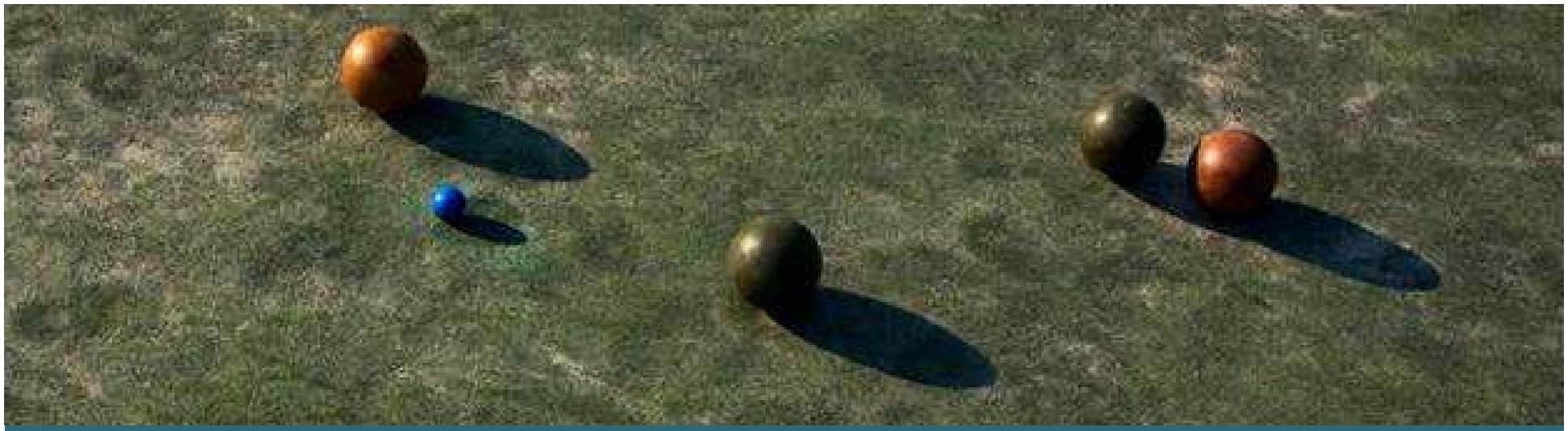
Customer Benefits

- **Dramatically improved security**
  - Proactive protection against worms & viruses
  - Leverage the network to audit & enforce host security policies
  - Network segmentation services for isolation and remediation
- **Extend existing investment**
  - Leverage investment in network infrastructure and host security
  - Focus operations on prevention, not reaction
- **Increase enterprise resilience**
  - Comprehensive admission control across all access methods
  - Ensure endpoints conform to security policy

Cost Savings for Higher Education Customers

Number of computers requiring intervention due to viruses and worms:

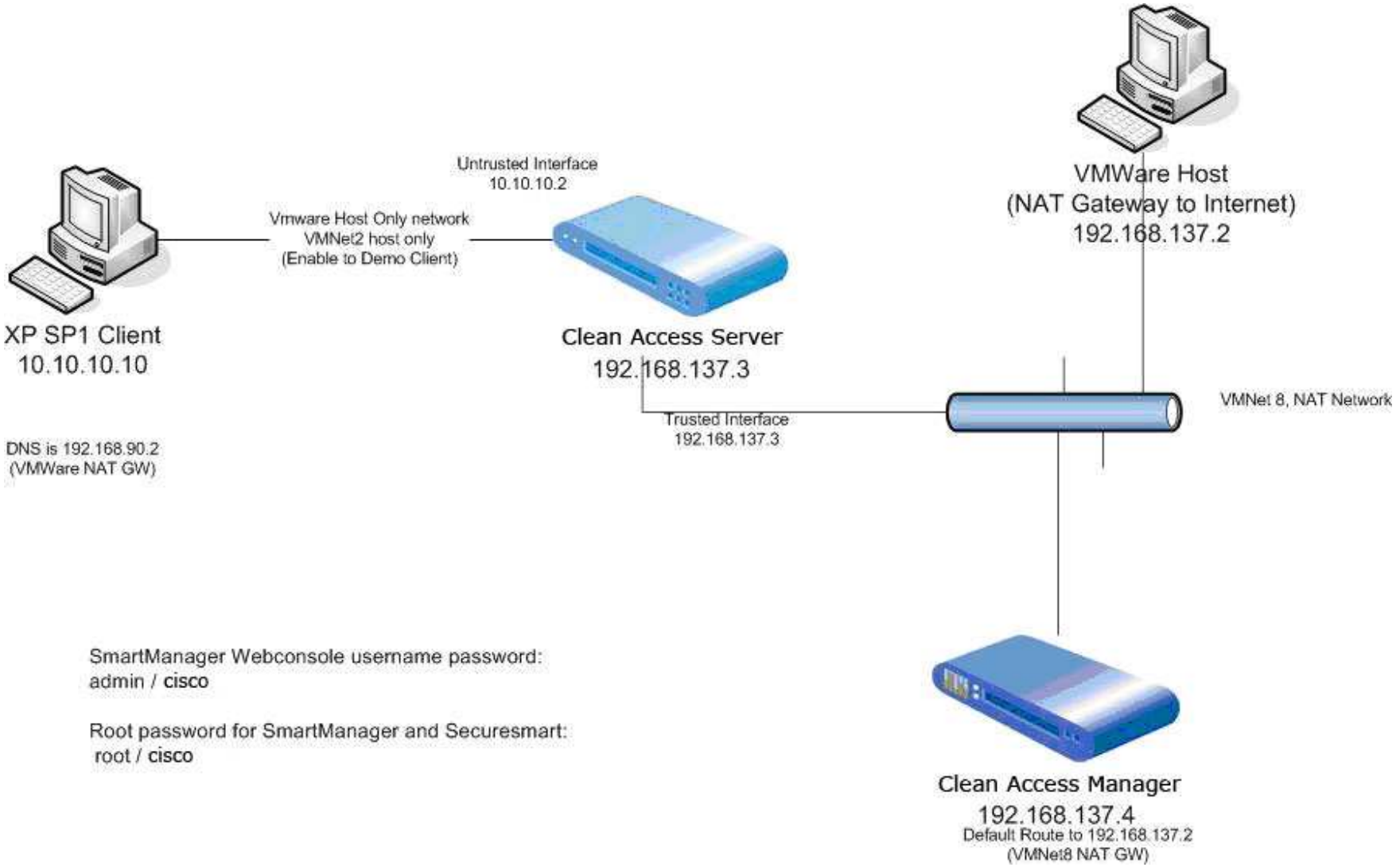
	BEFORE CISCO CLEAN ACCESS	AFTER CISCO CLEAN ACCESS	COST REDUCTION (assumes $100 per computer)
Anderson University	1,500	345	$115,500
Arizona State University	6,000	50	$595,000
Davidson College	1,700	153	$154,700
Fordham University	"enough to bring the network down for 6 weeks"	100	incalculable
Lewis and Clark University	1,725	345	$138,000
University of Mary Washington	2,700	300	$240,000



Demo

5

Schema


Untrusted Interface
10.10.10.2
Vmware Host Only network
VMNet2 host only
(Enable to Demo Client)
VMWare Host
(NAT Gateway to Internet)
192.168.137.2
XP SP1 Client
10.10.10.10
Clean Access Server
192.168.137.3
Trusted Interface
192.168.137.3
VMNet 8, NAT Network
DNS is 192.168.90.2
(VMWare NAT GW)
SmartManager Webconsole username password:
admin / cisco
Root password for SmartManager and Securesmart:
root / cisco
Clean Access Manager
192.168.137.4
Default Route to 192.168.137.2
(VMNet8 NAT GW)


CISCO SYSTEMS