Security for a Converged Network

Peter Holliday, Defence Network Architect – APAC

Peter Labbe, Defence Network Architect – Naval Systems

© 2003 Cisco Systems, Inc. All rights reserved.

Agenda

- **Self Defending Networks**
  - **Network Admission Control**
  - **Vendor Integration**
- **Security Architectures for IP Communications**
- **Defence Case Studies**

© 2003 Cisco Systems, Inc. All rights reserved.

Overview

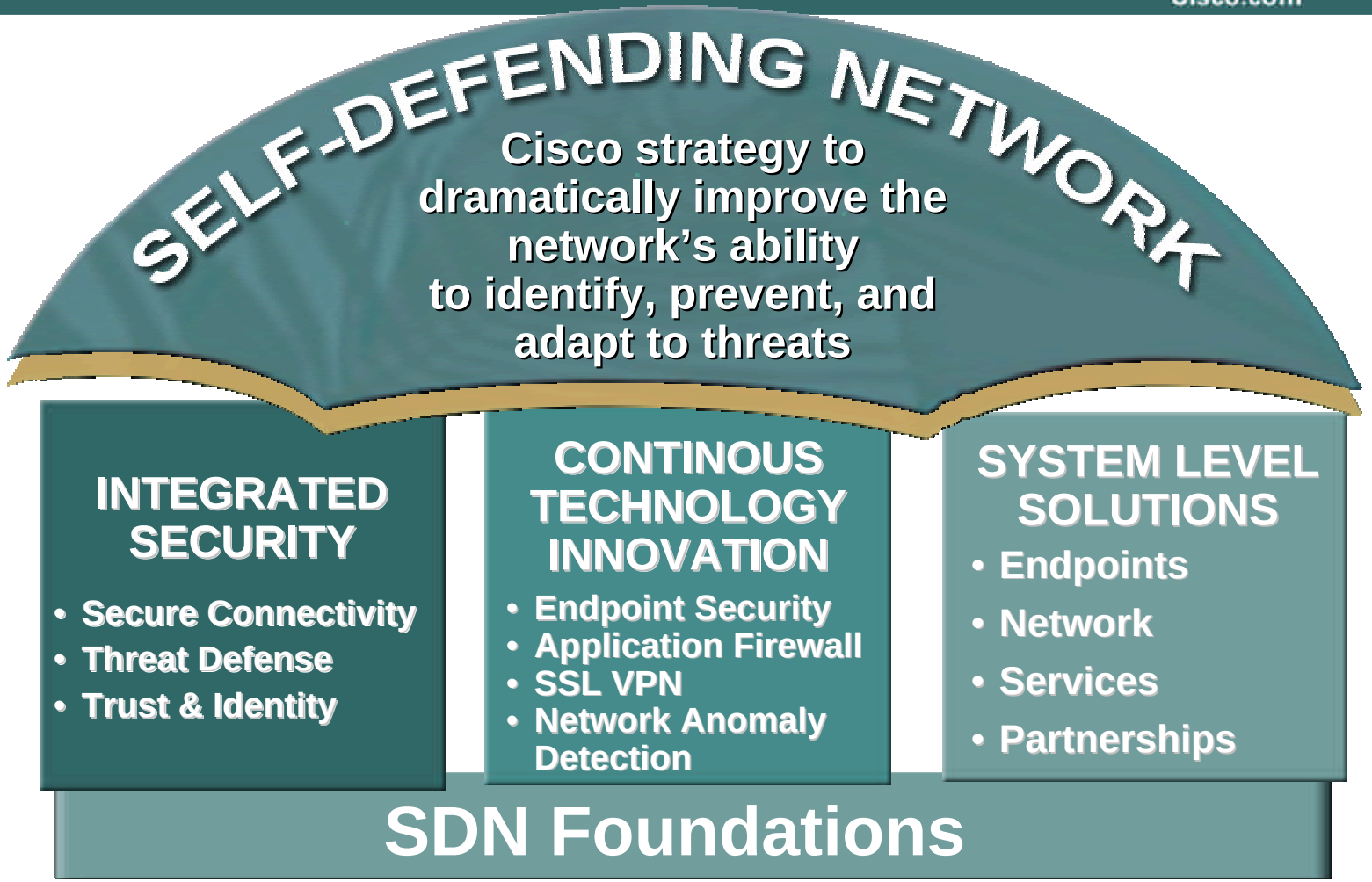
© 2003 Cisco Systems, Inc. All rights reserved.

“ANYONE CAN BUILD A STOP SIGN – OR EVEN A TRAFFIC LIGHT – BUT IT TAKES A DIFFERENT MIND-SET ENTIRELY TO CONCEIVE OF A CITY-WIDE TRAFFIC CONTROL SYSTEM.”

Bruce Schneier, “Beyond Fear”

© 2003 Cisco Systems, Inc. All rights reserved.

Self Defending Network Strategy



© 2003 Cisco Systems, Inc. All rights reserved.

Customer Problems with Host Security

- Viruses and worms continue to disrupt business
- Day-zero attacks make reactive solutions less effective
- Point technologies preserve host rather than network availability and enterprise resiliency
- Non-compliant servers and desktops common, difficult to detect and contain
- Locating and isolating infected systems time and resource intensive

Cisco's Layered Host Security Strategy

- **Endpoint Protection – CSA**

  Alleviates patching and signature update pressure with behavior-based protection technology

- **Network Admission Control**

  Preserves enterprise resilience by auditing and enforcing adherence to corporate endpoint security policies when accessing the network

- **Network Infection Containment**

  Limit the severity of infections by reducing the response time spent identifying and isolating infected systems, and cleansing traffic

© 2003 Cisco Systems, Inc. All rights reserved.

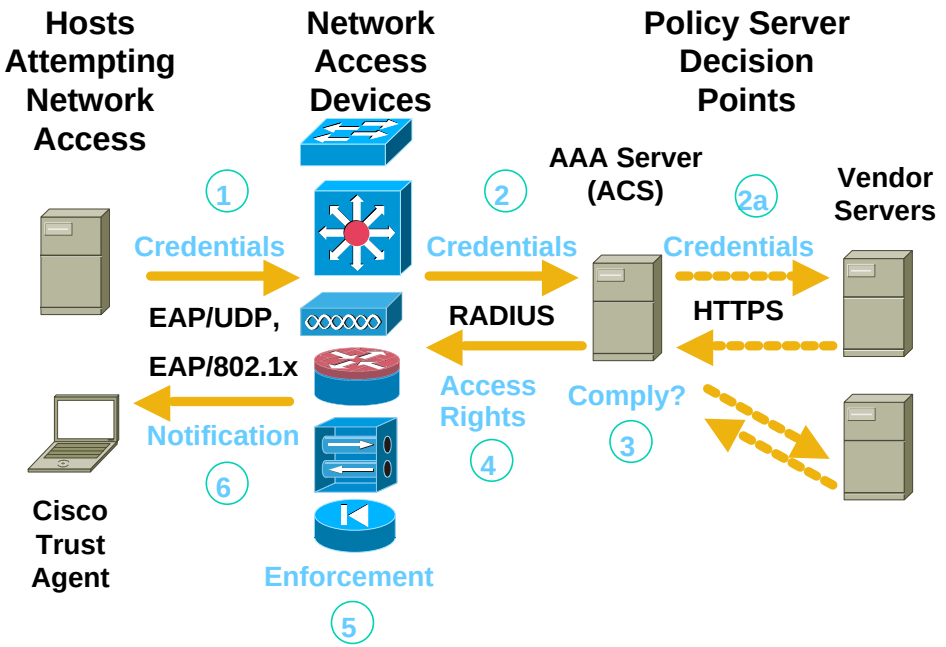
Cisco Network Admission Control (NAC)

- **Cisco-led, Multi-partner Program**
  - Limits damage from viruses & worms
  - Coalition of market leading vendors
- **Restricts and Controls Network Access**
  - Endpoint device interrogated for policy compliance
  - Network determines appropriate admission enforcement: permit, deny, quarantine, restrict
- **A Cisco Self-Defending Network Initiative**
  - Dramatically improves network's ability to identify, prevent, and adapt to threats

© 2003 Cisco Systems, Inc. All rights reserved.

Cisco NAC Solution Overview

NAC Solution: Leverage the network to intelligently enforce access privileges based on endpoint security posture



NAC Characteristics:

- Ubiquitous solution for *all* connection methods
- Validates *all* hosts
- Leverages customer investments in Cisco network and AV solutions
- Supports Multiple AV vendors & Cisco Security Agent
- Network provides visibility, forces authentication, isolation services
- Applications gather & assess credentials, remediation services

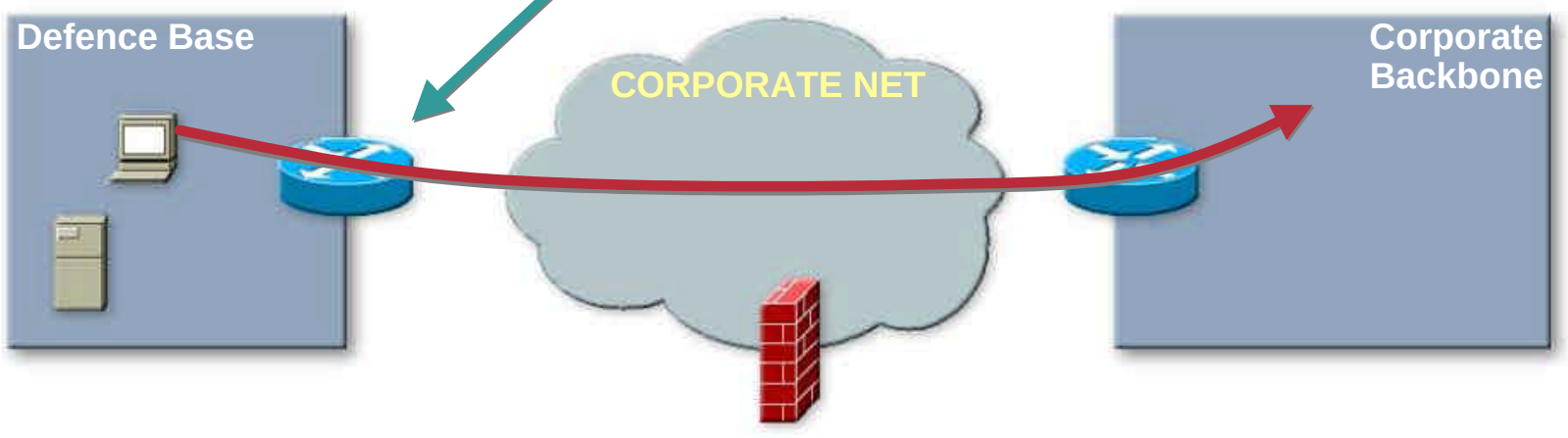
© 2003 Cisco Systems, Inc. All rights reserved.

Network Admission Control

© 2003 Cisco Systems, Inc. All rights reserved.

Why Network Admission Control?

1. Non-compliant endpoint attempts connection
2. Connection allowed
3. Infection spreads; endpoints exposed

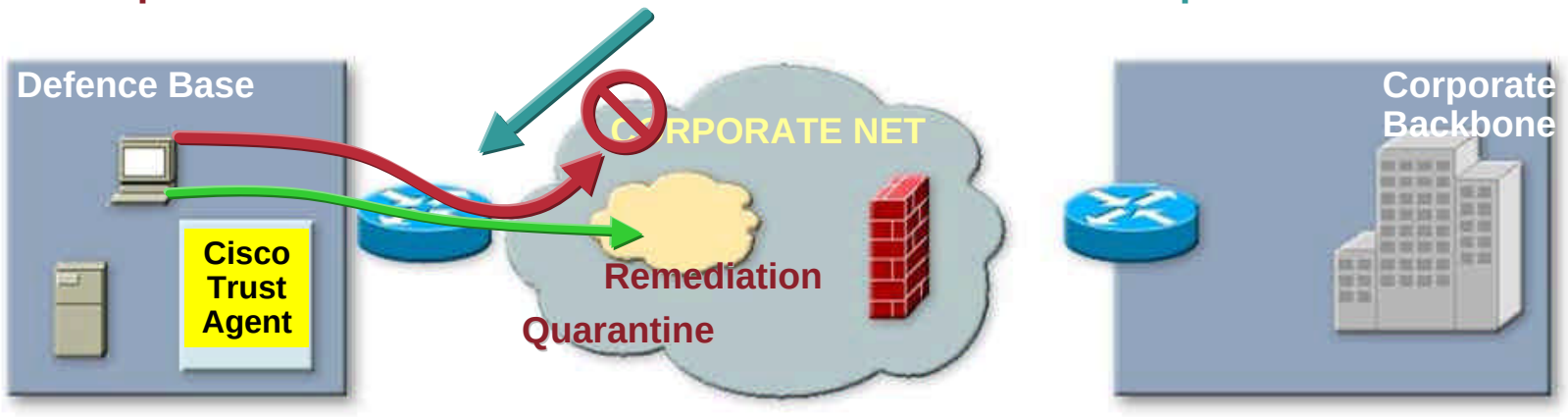


© 2003 Cisco Systems, Inc. All rights reserved.

Cisco Network Admission Control:

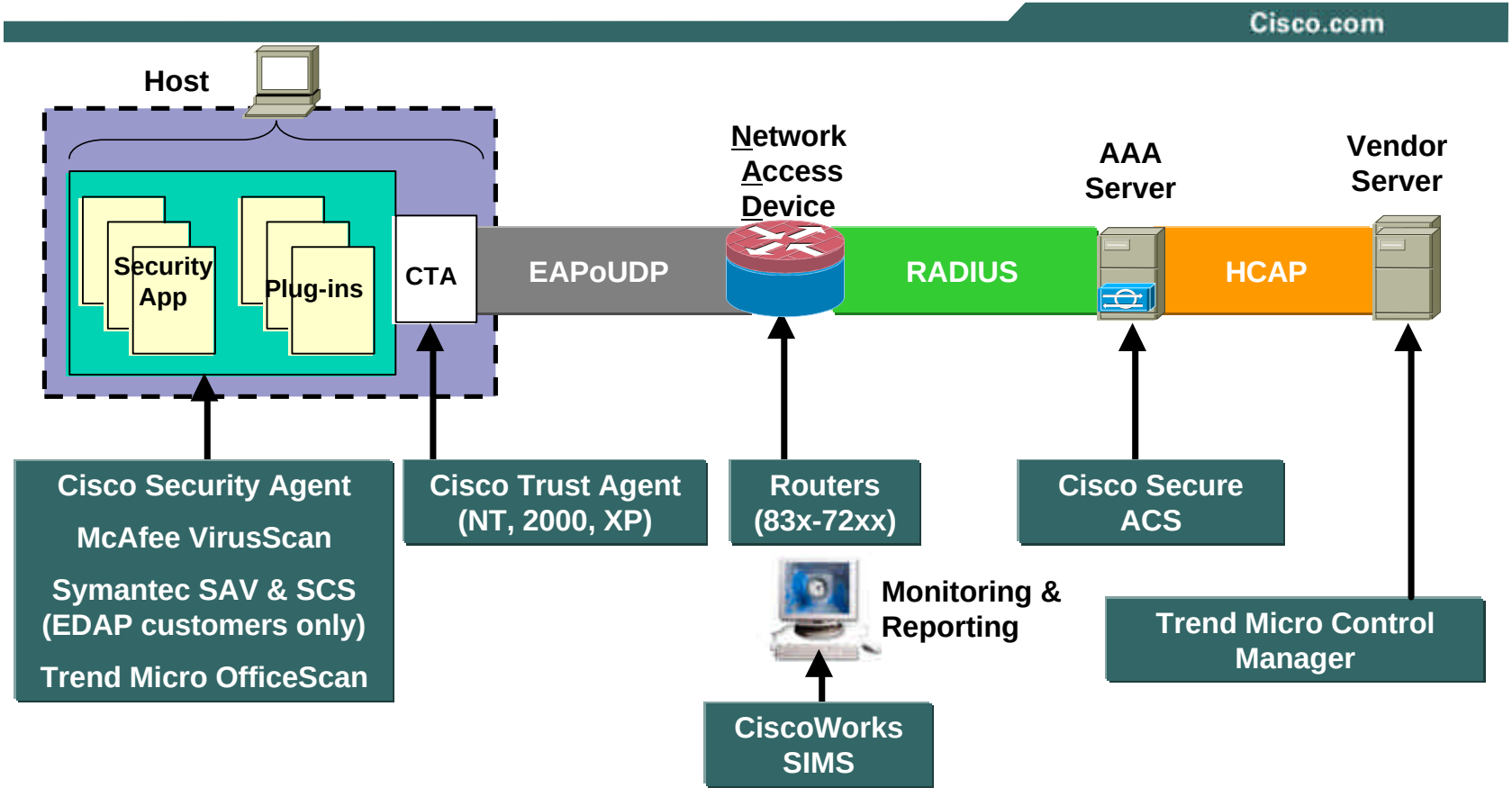
What It Does

1. Non-compliant endpoint attempts connection
2. Quarantine/ remediation
3. Infection containment; endpoints secured



© 2003 Cisco Systems, Inc. All rights reserved.

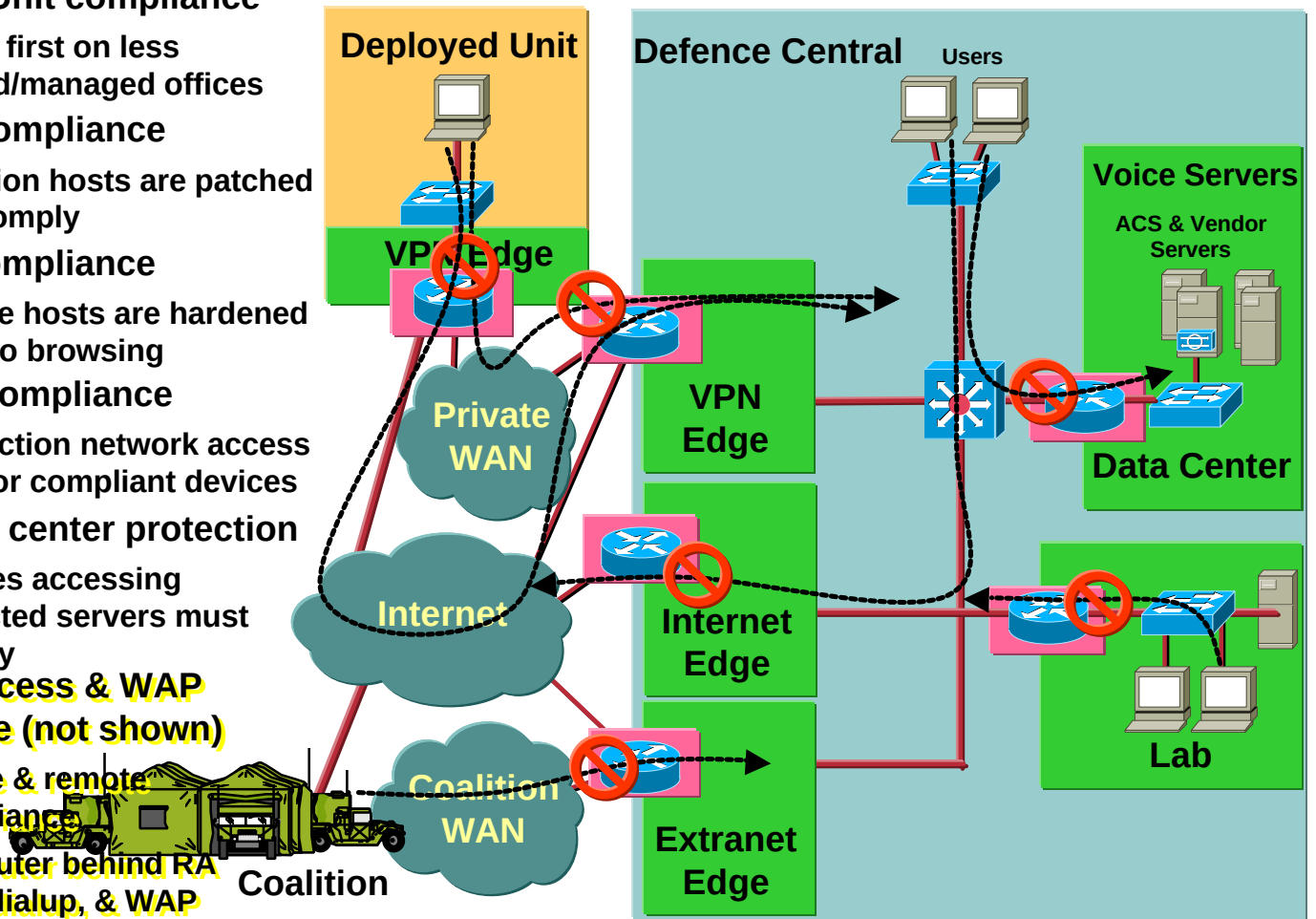
Logical Components



© 2003 Cisco Systems, Inc. All rights reserved.

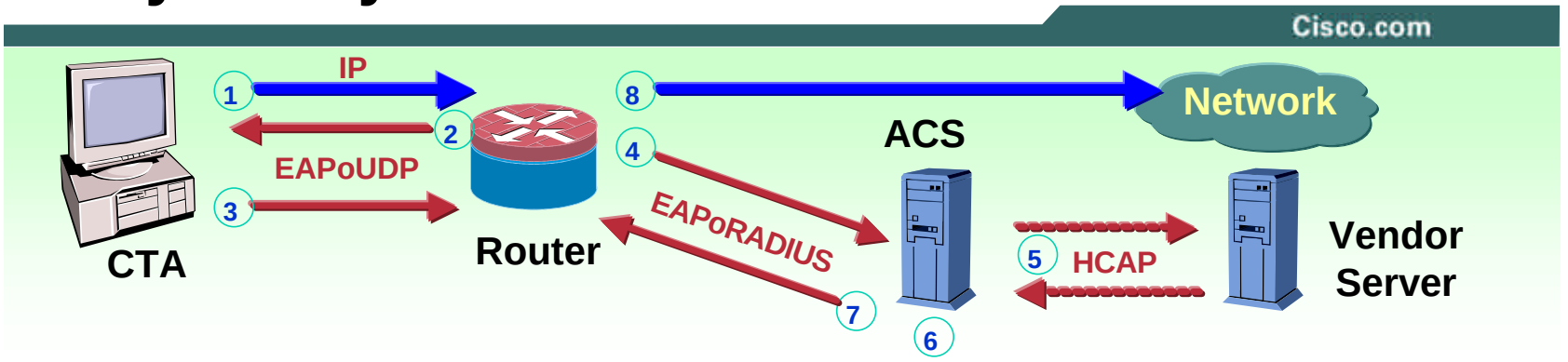
Router-Based Deployment Scenarios

- Deployed Unit compliance
  - Focus first on less trusted/managed offices
- Extranet compliance
  - Coalition hosts are patched and comply
- Internet compliance
  - Ensure hosts are hardened prior to browsing
- Lab/R&D compliance
  - Production network access only for compliant devices
- Voice/Data center protection
  - Devices accessing protected servers must comply
- Remote access & WAP compliance (not shown)
  - Mobile & remote compliance
  - Put router behind RA VPN, dialup, & WAP



© 2003 Cisco Systems, Inc. All rights reserved.

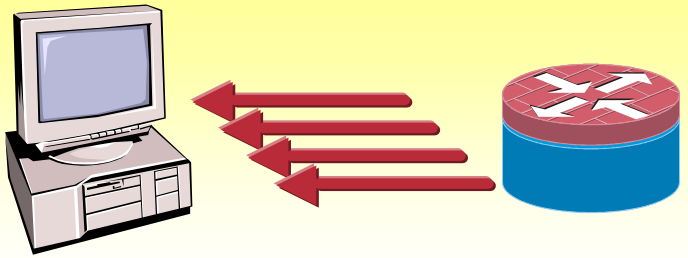
Layer 3 System Flow



1. IP packet triggers *Intercept ACL* on router
   - Default ACL determines initial & interim network access
2. Router triggers posture validation with CTA *(EAPoUDP)*
3. CTA sends posture credentials to router *(EAPoUDP)*
4. Router sends posture credentials to ACS *(EAPoRADIUS)*
5. ACS can proxy portions of posture authentication to vendor server(s) *(HCAP)*
6. ACS validates posture, determines authorization rights *(Healthy, Checkup, Quarantine)*
7. ACS sends authorization policy to router *(ACLs, URL redirection)*
   - Notification may be sent to applications on host also
8. Host IP access granted *(or denied, restricted, URL redirected)*

© 2003 Cisco Systems, Inc. All rights reserved.

Periodic Reassessment



1. **Inactive Endpoint – Confirm inactive endpoint has not changed**

   Called “L3 EAP Status Query”: New EAP method between CTA and router (not ACS)

   Router periodically polls to make sure:

   1) CTA is still there

   2) It’s the same validated device

   3) Posture hasn’t changed

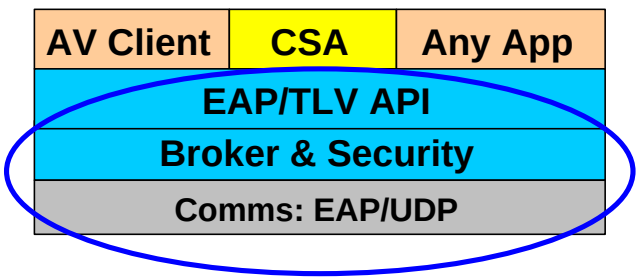
   Authentication based on keyed MAC (Uses keys derived in EAP-Posture (PEAP))

2. **Reassess Active Endpoint – Confirm continued compliance**

   CTA indicates posture change by not responding to Status Query, triggers revalidation

© 2003 Cisco Systems, Inc. All rights reserved.

Cisco Trust Agent (CTA)

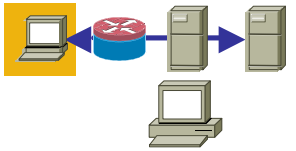


Cisco Trust Agent

- **Endpoint agent for communications**
  - Windows NT, XP, 2000
- **Performs three primary functions**
  - Network comms (EAPoUDP)
  - Application comms (EAP/TLV broker)
  - Authenticate ACS & encrypt comms
- **Application integration**
  - Initial focus: OS & AV patches
  - Co-sponsors: McAfee, Symantec, Trend Micro
  - Plug-in multi-vendor applications via common EAP API to obtain posture information
- **Availability**
  - No charge component, available from CCO
  - Licensees *may* redistribute for free

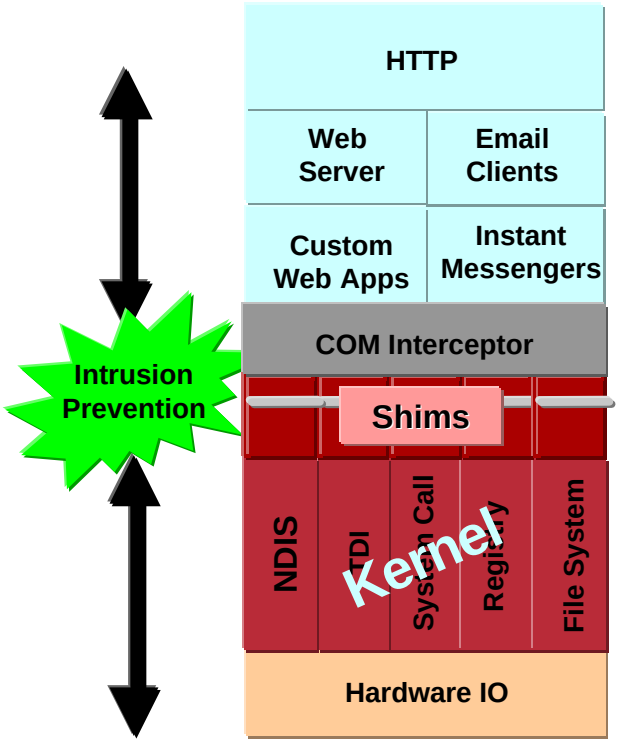
© 2003 Cisco Systems, Inc. All rights reserved.

CSA Integration



Cisco.com

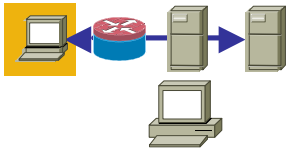
Kernel Shim Wrappers



- **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

© 2003 Cisco Systems, Inc. All rights reserved.

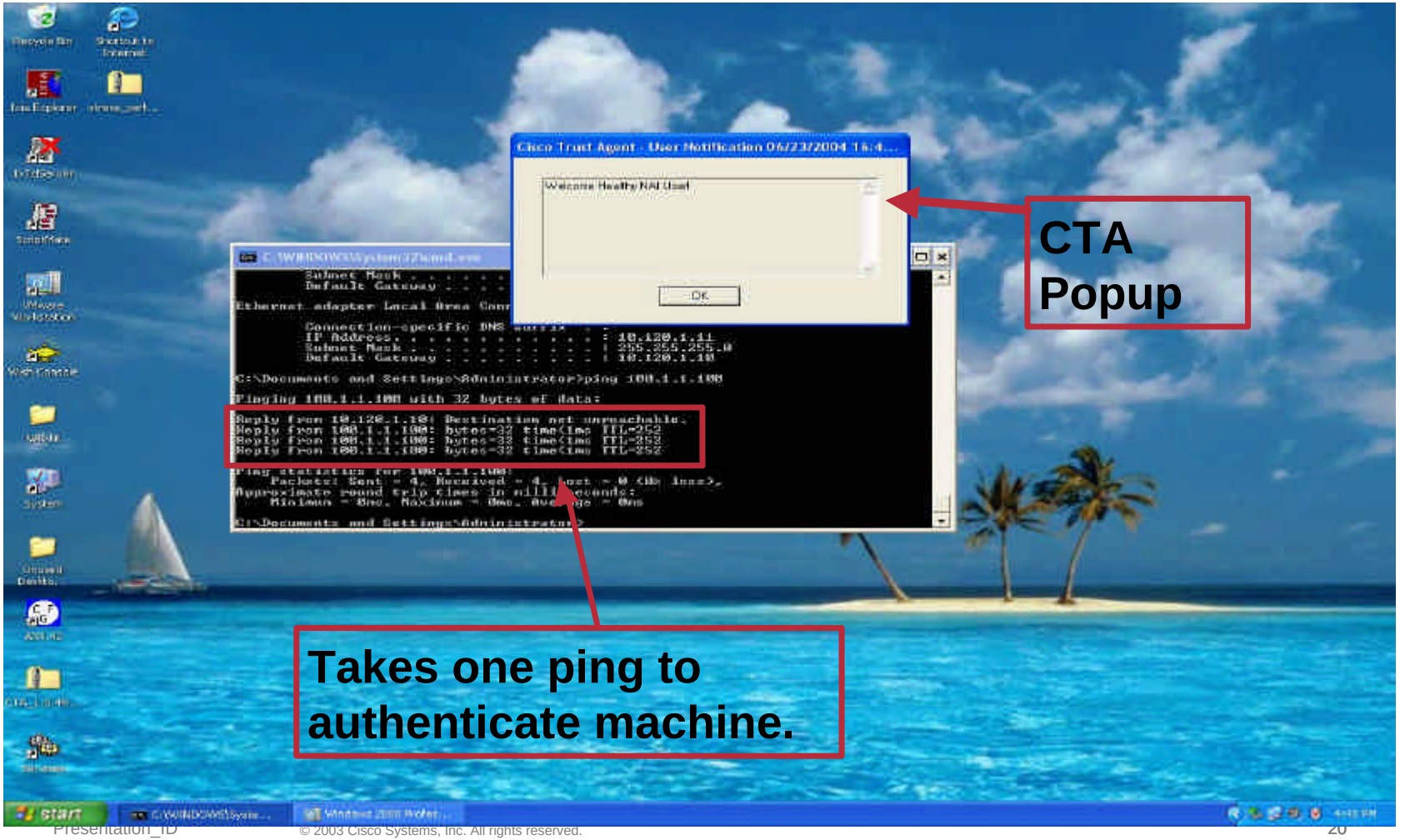
Vendor Integration



- **McAfee (NAI)**
  - VirusScan 7.x, 8.0i integration
  - ePO integration & CTA bundling timeline TBD
- **Symantec**
  - Enterprise Development Alliance Program (EDAP) support in 2004, commercial in 2005
  - SAV 9.0 [AV] & SCS 2.0 [AV, FW, HIDS] integration
  - Policy manager integration (target Nov), CTA TBD
- **Trend Micro**
  - OfficeScan Corporate Edition & Trend Micro Control Manager integration (June) -- OfficeScan CE 6.5
  - CTA bundled in OfficeScan
- **IBM**
  - Tivoli integration in progress, first release 4QC04
  - Targets compliance validation & remediation services
- **Computer Associates**
  - Signed agreement, not announced publicly
  - Integrating a range of products into NAC

ns, Inc. All rights reserved.

NAC Client – End User Experience



© 2003 Cisco Systems, Inc. All rights reserved.

Securing IP Communications

© 2003 Cisco Systems, Inc. All rights reserved.

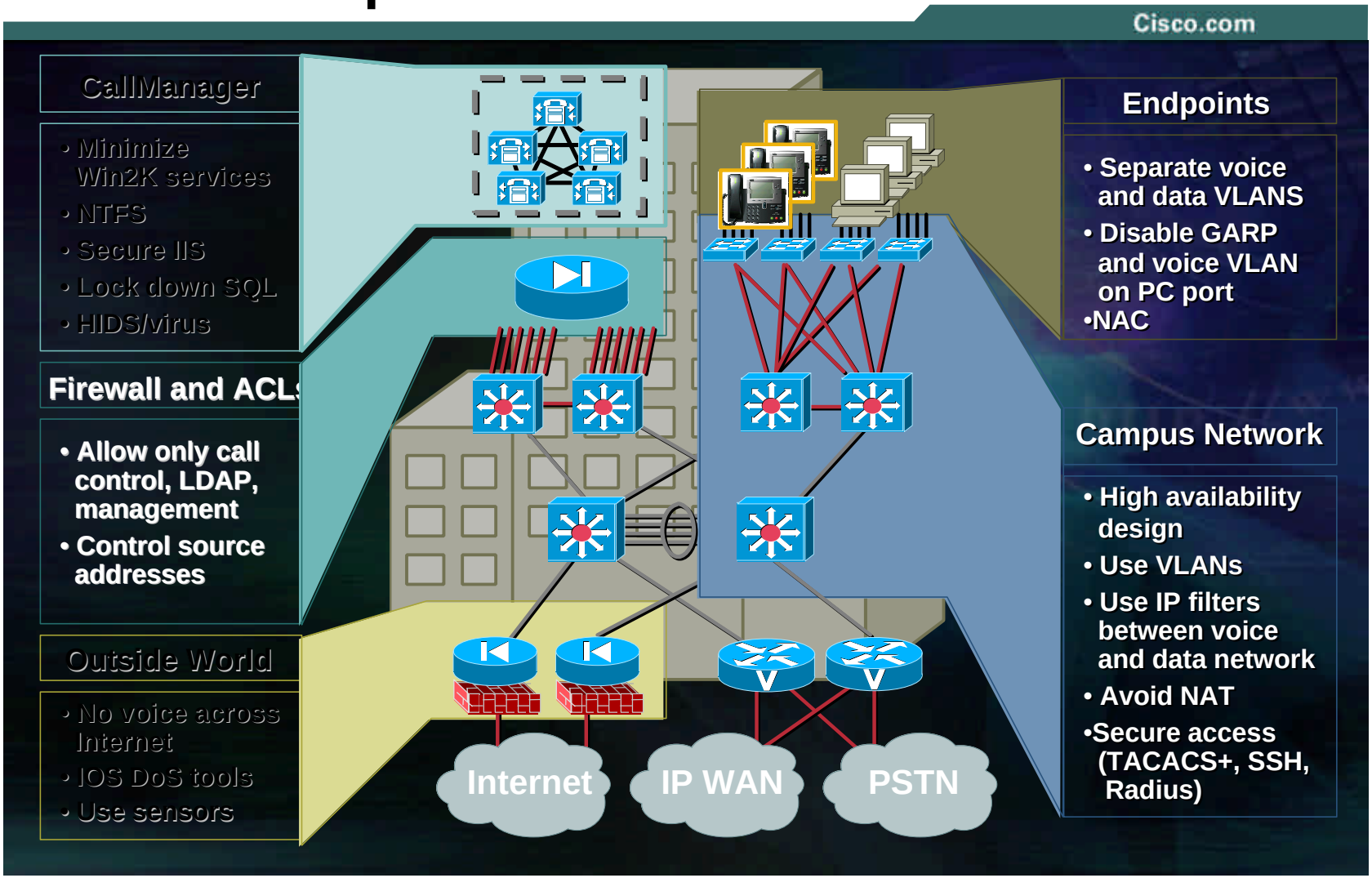
Securing IP Communications

Cisco.com

- SAFE Architecture for protecting Call Manager Servers
- Authentication, Integrity and Encryption
  - TFTP File manipulation
  - Call signal protection
  - Man in the Middle Attacks
  - Phone and Server Identity Theft
- New Call Manager Features
  - Image Authentication
  - Device Authentication
  - File Auhentication
  - Signalling Authentication
  - Phone Hardening

© 2003 Cisco Systems, Inc. All rights reserved.

SAFE Blueprint for IP Communications



Summary

© 2003 Cisco Systems, Inc. All rights reserved.

Summary

- **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

© 2003 Cisco Systems, Inc. All rights reserved.

© 2003 Cisco Systems, Inc. All rights reserved.