Cisco Security Agent (CSA)

Network Admission Control (NAC)

Pascal Delprat
Security Consultant
Cisco France

Vincent Bieri
Marketing Manager, Security
EMEA Technology Marketing Organisation

Agenda

- CSA and NAC Presentation (30') –vincent bieri
- CSA Demo (20') – pascal delprat
- Q&A / Discussions (10') – all

Cisco Security Agent (CSA)

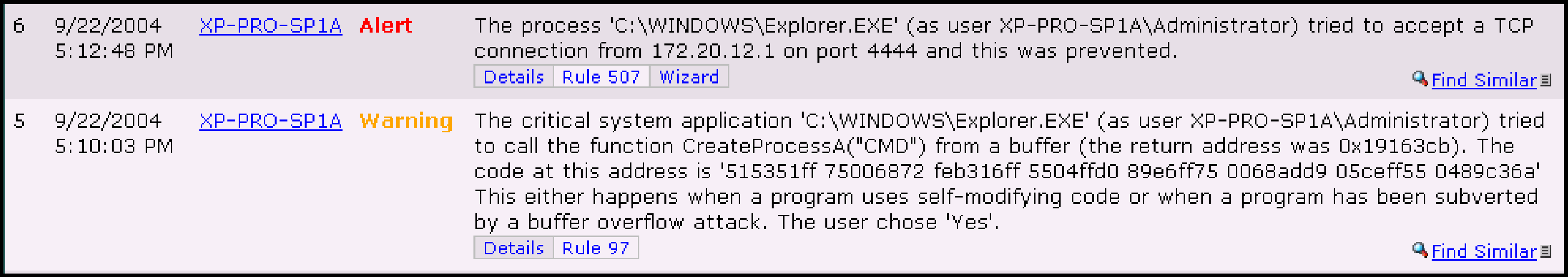
Agenda – CSA

- Overview of Cisco Security Agent
- Management Model
- CSA Implementation and Architecture
- Security Functions
- Performance Impact
- Integration with Other Security Technologies
- Roadmap CSA 4.5

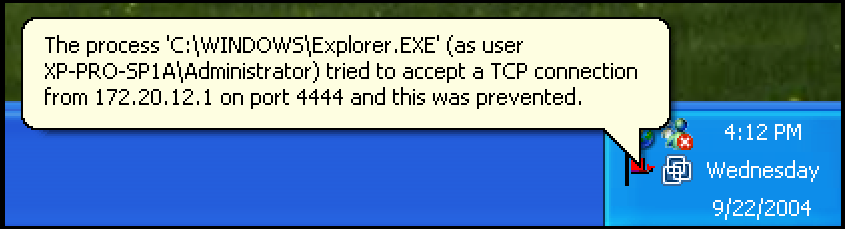
What is Cisco Security Agent?

- A security software for desktop, laptop, & server computers that minimizes patch and security problems with **behavior-based OS kernel wrappers**
- Centrally administered, with distributed, autonomous policy enforcement
  - Scales well & also **works with intermittently connected hosts**
  - Can also adapt defenses based upon **correlation of events from different hosts**
- Effective against existing & previously unseen attacks
  - **Stopped nimda, code red, slammer, blaster with out-of-the-box policies**

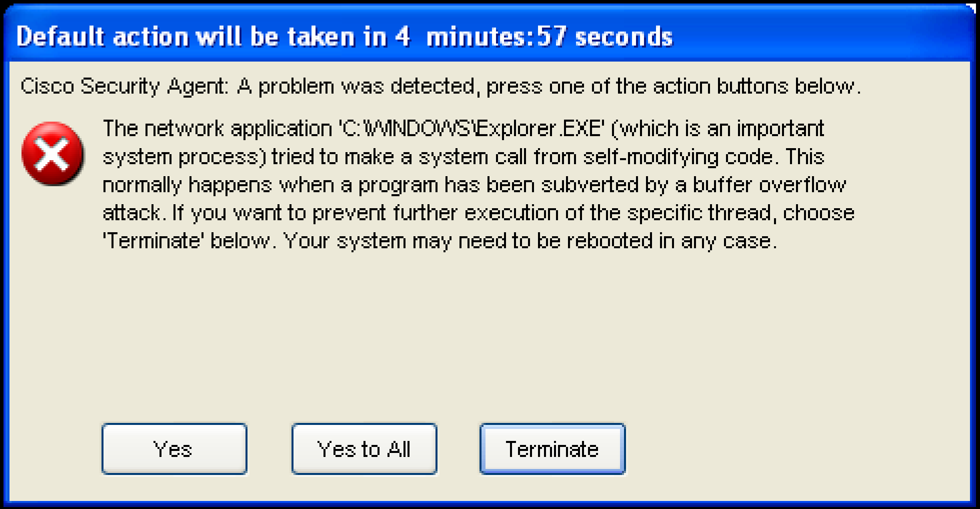
JPEG (GDI+) OVERFLOW



6	9/22/2004 5:12:48 PM	XP-PRO-SP1A	Alert	The process 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to accept a TCP connection from 172.20.12.1 on port 4444 and this was prevented.
5	9/22/2004 5:10:03 PM	XP-PRO-SP1A	Warning	The critical system application 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to call the function CreateProcessA("CMD") from a buffer (the return address was 0x19163cb). The code at this address is '515351ff 75006872 feb316ff 5504ffd0 89e6ff75 0068add9 05ceff55 0489c36a' This either happens when a program uses self-modifying code or when a program has been subverted by a buffer overflow attack. The user chose 'Yes'.



The process 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to accept a TCP connection from 172.20.12.1 on port 4444 and this was prevented.

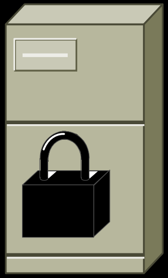


Default action will be taken in 4 minutes:57 seconds

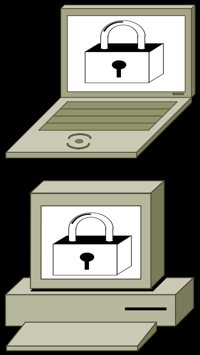
Cisco Security Agent: A problem was detected, press one of the action buttons below.

The network application 'C:\WINDOWS\Explorer.EXE' (which is an important system process) tried to make a system call from self-modifying code. This normally happens when a program has been subverted by a buffer overflow attack. If you want to prevent further execution of the specific thread, choose 'Terminate' below. Your system may need to be rebooted in any case.

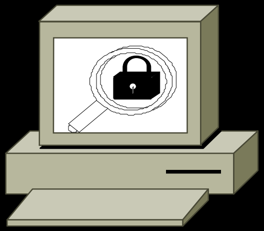
Cisco Security Agent (CSA) Components



Management Server—deploys Security Policies, Receives and Stores Events in SQL Database, Alerts Administrators, Deploys Software, Part of Cisco VPN and Security Management System

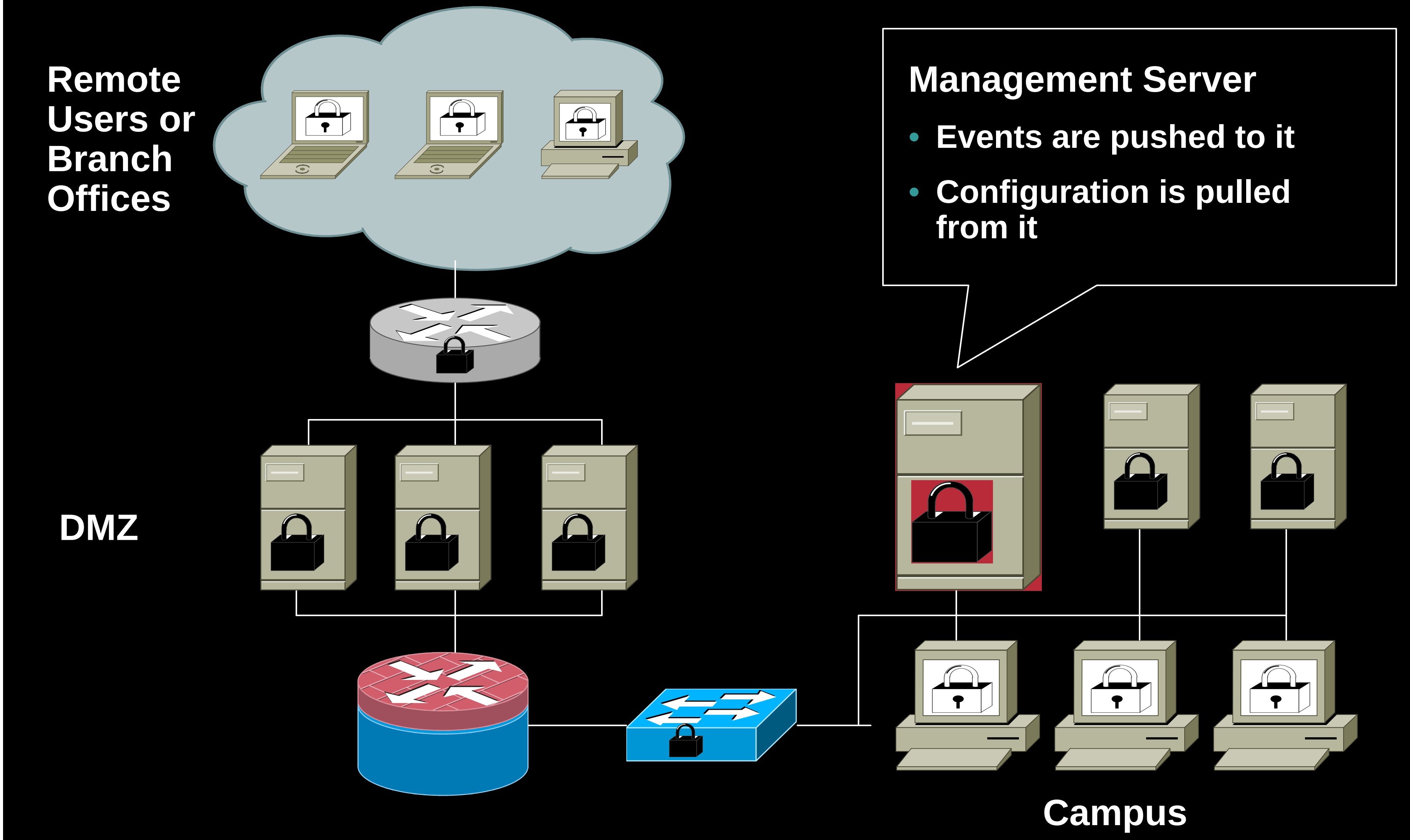


Cisco Security Agents—Enforce Security Policy Received from Management Server, Sends Events Immediately, Interacts with User (If Necessary), Protects Itself, Poll for Policy Updates, Run on Windows and Solaris



CSA Management Console—Web Browser Interface, Policy Configuration Tool, Event Views

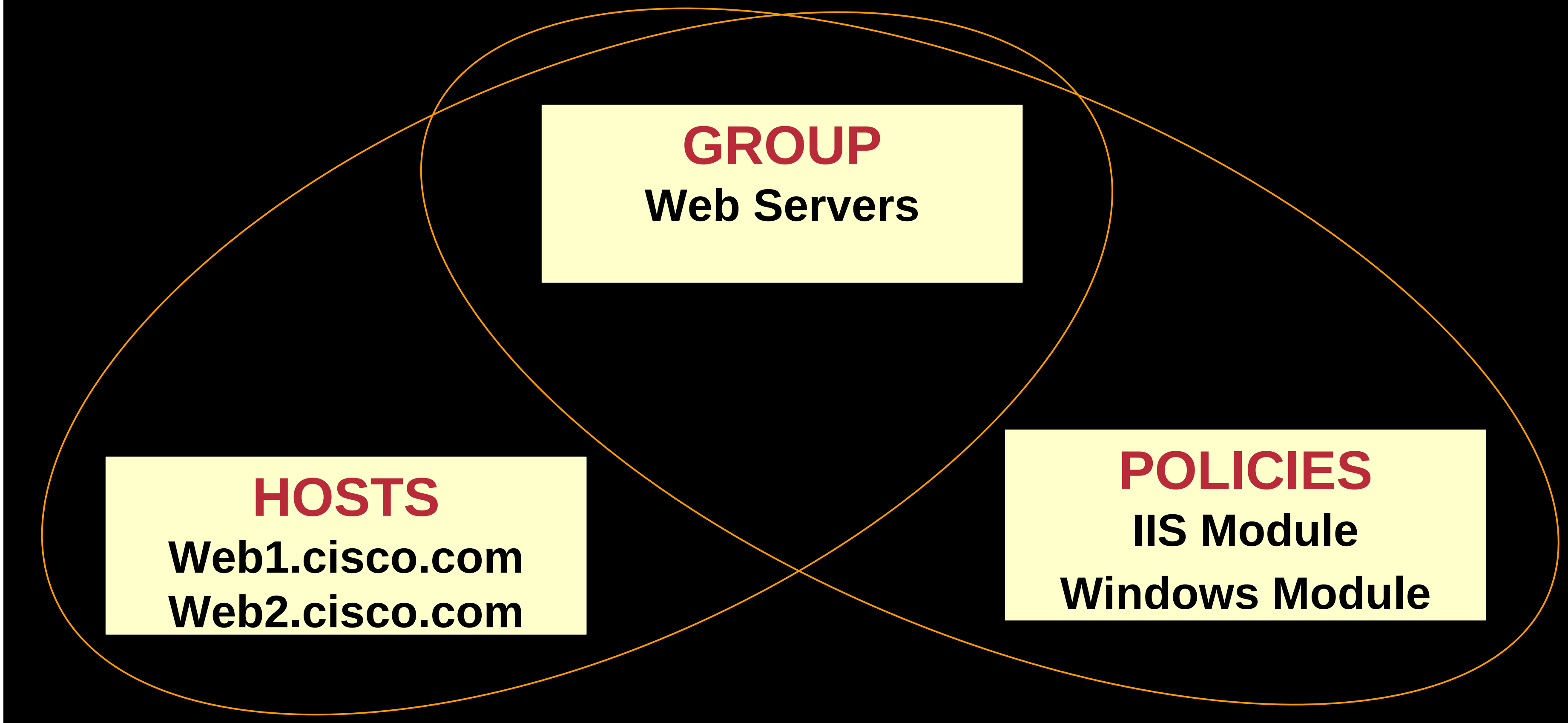
Management Architecture



Management Server

- Events are pushed to it
- Configuration is pulled from it

Hosts are Attached to a Group that includes a set of Policies defined by Rules



GROUP

Web Servers

HOSTS

Web1.cisco.com

Web2.cisco.com

POLICIES

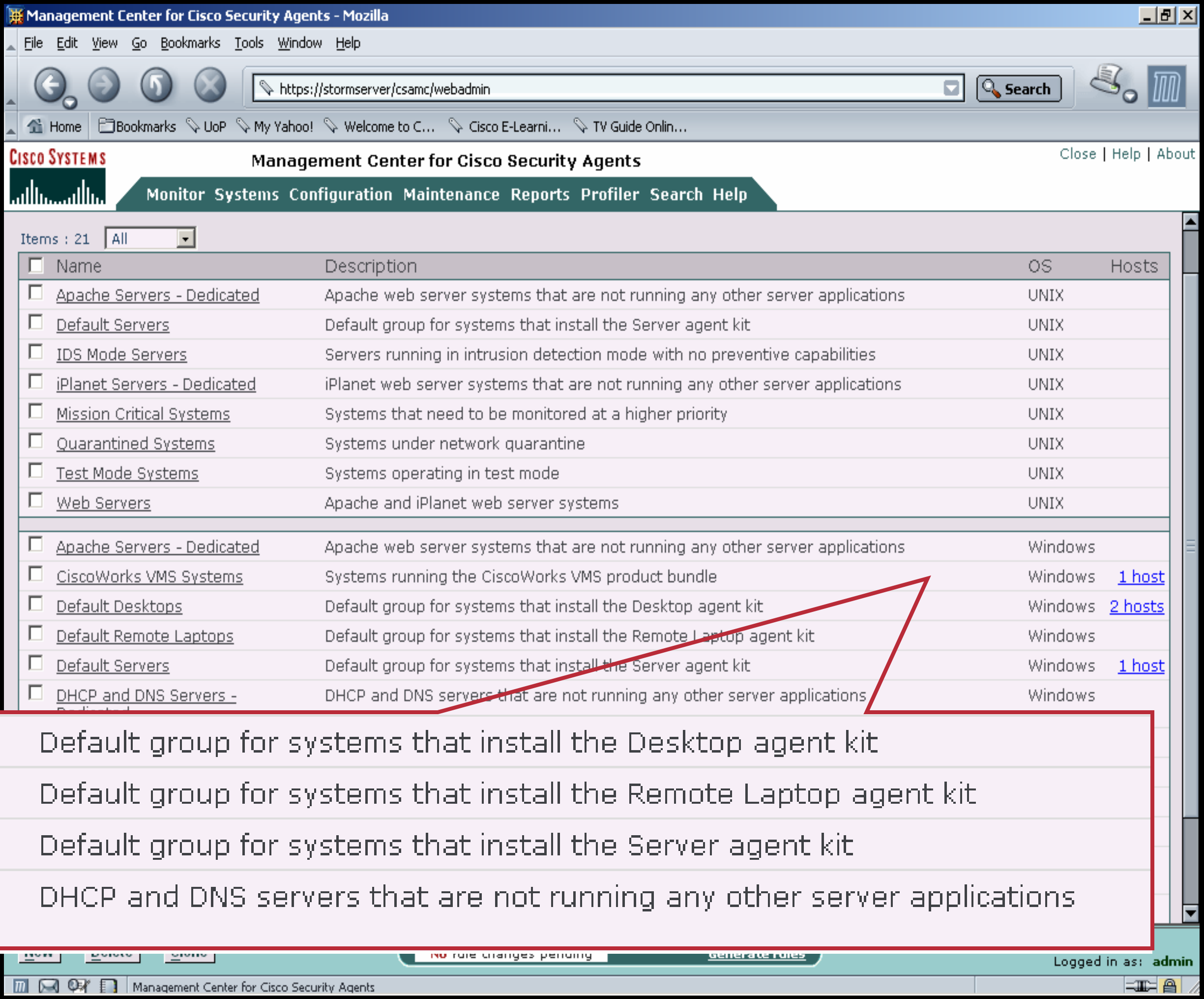
IIS Module

Windows Module

Groups

- **Used to Organize Logical Collections of Hosts**

  e.g. “IIS Servers”, “Executive Desktops”, or “SQL Servers”

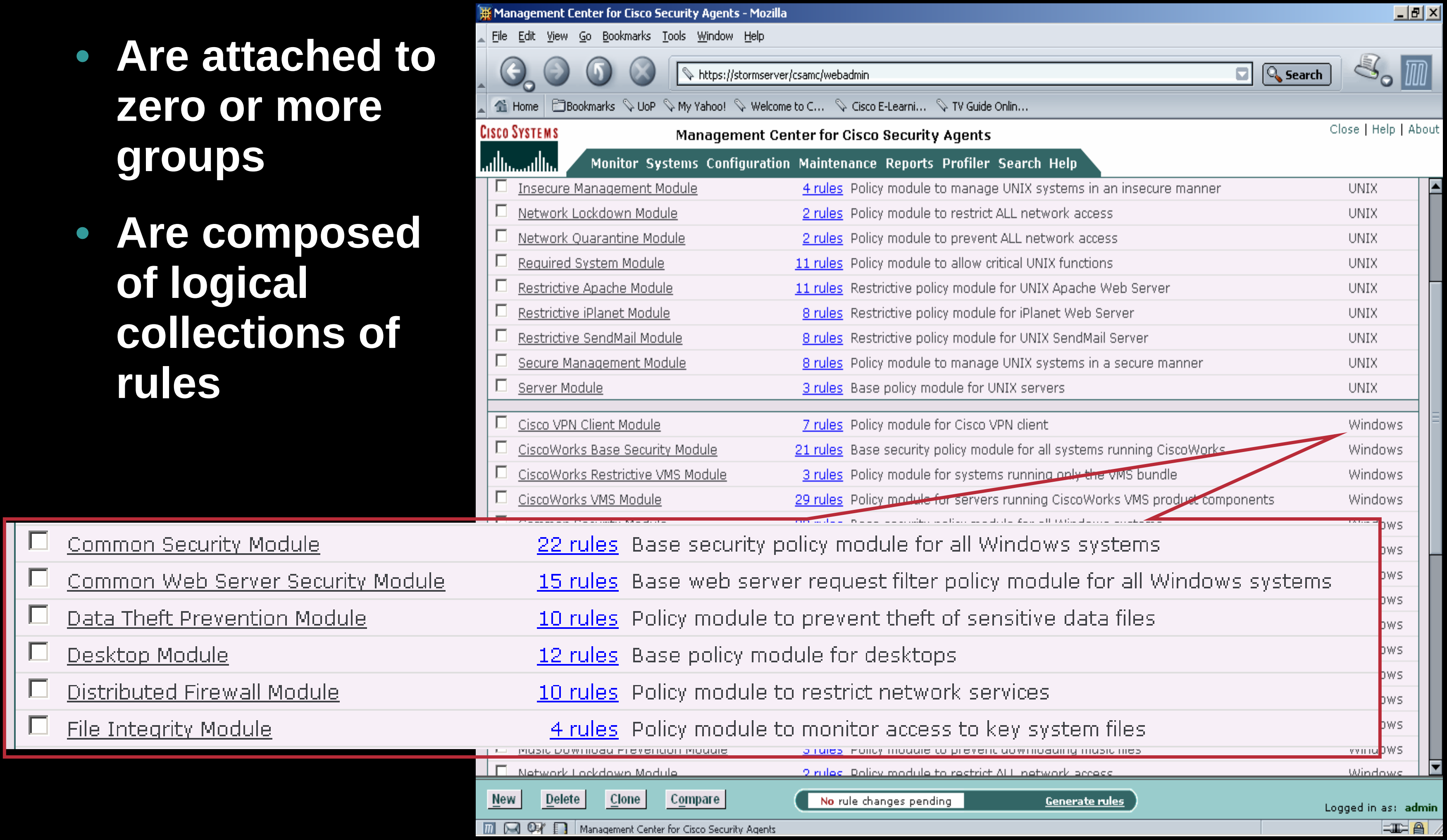

Management Center for Cisco Security Agents - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://stormserver/csamc/webadmin
Search
Home
Bookmarks
UoP
My Yahoo!
Welcome to C...
Cisco E-Learni...
TV Guide Onlin...
CISCO SYSTEMS
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Items : 21
All
New
Delete
Clone
No rule changes pending
Generate rules
Logged in as: admin
Management Center for Cisco Security Agents

	Name	Description	OS	Hosts
□	Apache Servers - Dedicated	Apache web server systems that are not running any other server applications	UNIX	
□	Default Servers	Default group for systems that install the Server agent kit	UNIX	
□	IDS Mode Servers	Servers running in intrusion detection mode with no preventive capabilities	UNIX	
□	iPlanet Servers - Dedicated	iPlanet web server systems that are not running any other server applications	UNIX	
□	Mission Critical Systems	Systems that need to be monitored at a higher priority	UNIX	
□	Quarantined Systems	Systems under network quarantine	UNIX	
□	Test Mode Systems	Systems operating in test mode	UNIX	
□	Web Servers	Apache and iPlanet web server systems	UNIX	
□	Apache Servers - Dedicated	Apache web server systems that are not running any other server applications	Windows	
□	CiscoWorks VMS Systems	Systems running the CiscoWorks VMS product bundle	Windows	1 host
□	Default Desktops	Default group for systems that install the Desktop agent kit	Windows	2 hosts
□	Default Remote Laptops	Default group for systems that install the Remote Laptop agent kit	Windows	
□	Default Servers	Default group for systems that install the Server agent kit	Windows	1 host
□	DHCP and DNS Servers -	DHCP and DNS servers that are not running any other server applications	Windows	

□	Default Desktops	Default group for systems that install the Desktop agent kit
□	Default Remote Laptops	Default group for systems that install the Remote Laptop agent kit
□	Default Servers	Default group for systems that install the Server agent kit
□	DHCP and DNS Servers - Dedicated	DHCP and DNS servers that are not running any other server applications

Policies

- Are attached to zero or more groups
- Are composed of logical collections of rules



Management Center for Cisco Security Agents - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://stormserver/csamc/webadmin
Search
Home Bookmarks UoP My Yahoo! Welcome to C... Cisco E-Learni... TV Guide Onlin...
Cisco Systems
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help

Management Center for Cisco Security Agents

☐	Insecure Management Module	4 rules	Policy module to manage UNIX systems in an insecure manner	UNIX
☐	Network Lockdown Module	2 rules	Policy module to restrict ALL network access	UNIX
☐	Network Quarantine Module	2 rules	Policy module to prevent ALL network access	UNIX
☐	Required System Module	11 rules	Policy module to allow critical UNIX functions	UNIX
☐	Restrictive Apache Module	11 rules	Restrictive policy module for UNIX Apache Web Server	UNIX
☐	Restrictive iPlanet Module	8 rules	Restrictive policy module for iPlanet Web Server	UNIX
☐	Restrictive SendMail Module	8 rules	Restrictive policy module for UNIX SendMail Server	UNIX
☐	Secure Management Module	8 rules	Policy module to manage UNIX systems in a secure manner	UNIX
☐	Server Module	3 rules	Base policy module for UNIX servers	UNIX
☐	Cisco VPN Client Module	7 rules	Policy module for Cisco VPN client	Windows
☐	CiscoWorks Base Security Module	21 rules	Base security policy module for all systems running CiscoWorks	Windows
☐	CiscoWorks Restrictive VMS Module	3 rules	Policy module for systems running only the VMS bundle	Windows
☐	CiscoWorks VMS Module	29 rules	Policy module for servers running CiscoWorks VMS product components	Windows
☐	Common Security Module	22 rules	Base security policy module for all Windows systems	Windows
☐	Common Web Server Security Module	15 rules	Base web server request filter policy module for all Windows systems	Windows
☐	Data Theft Prevention Module	10 rules	Policy module to prevent theft of sensitive data files	Windows
☐	Desktop Module	12 rules	Base policy module for desktops	Windows
☐	Distributed Firewall Module	10 rules	Policy module to restrict network services	Windows
☐	File Integrity Module	4 rules	Policy module to monitor access to key system files	Windows
☐	Music Download Prevention Module	3 rules	Policy module to prevent downloading music files	Windows
☐	Network Lockdown Module	2 rules	Policy module to restrict ALL network access	Windows

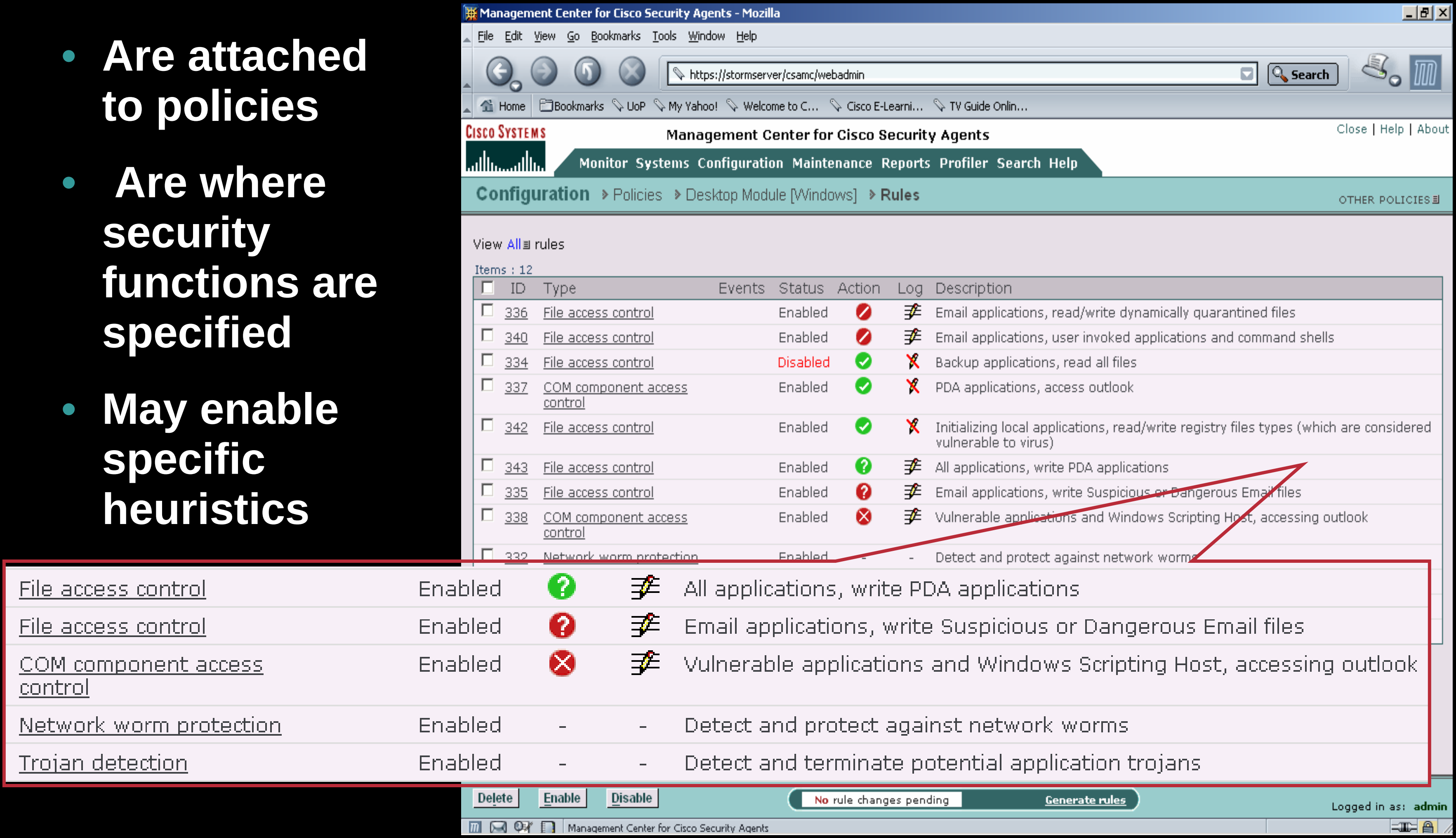
No rule changes pending

Logged in as: admin

Management Center for Cisco Security Agents

Rules

- Are attached to policies
- Are where security functions are specified
- May enable specific heuristics


Management Center for Cisco Security Agents - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://stormserver/csamc/webadmin
Search
Home Bookmarks UoP My Yahoo! Welcome to C... Cisco E-Learni... TV Guide Onlin...
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Configuration › Policies › Desktop Module [Windows] › Rules
OTHER POLICIES

View All rules

Items : 12

□	ID	Type	Events	Status	Action	Log	Description
□	336	File access control		Enabled	⊘	✎	Email applications, read/write dynamically quarantined files
□	340	File access control		Enabled	⊘	✎	Email applications, user invoked applications and command shells
□	334	File access control		Disabled	✓	✗	Backup applications, read all files
□	337	COM component access control		Enabled	✓	✗	PDA applications, access outlook
□	342	File access control		Enabled	✓	✗	Initializing local applications, read/write registry files types (which are considered vulnerable to virus)
□	343	File access control		Enabled	?	✎	All applications, write PDA applications
□	335	File access control		Enabled	?	✎	Email applications, write Suspicious or Dangerous Email files
□	338	COM component access control		Enabled	✗	✎	Vulnerable applications and Windows Scripting Host, accessing outlook
□	332	Network worm protection		Enabled	-	-	Detect and protect against network worms

File access control	Enabled	?	✎	All applications, write PDA applications
File access control	Enabled	?	✎	Email applications, write Suspicious or Dangerous Email files
COM component access control	Enabled	✗	✎	Vulnerable applications and Windows Scripting Host, accessing outlook
Network worm protection	Enabled	-	-	Detect and protect against network worms
Trojan detection	Enabled	-	-	Detect and terminate potential application trojans

No rule changes pending

Logged in as: admin

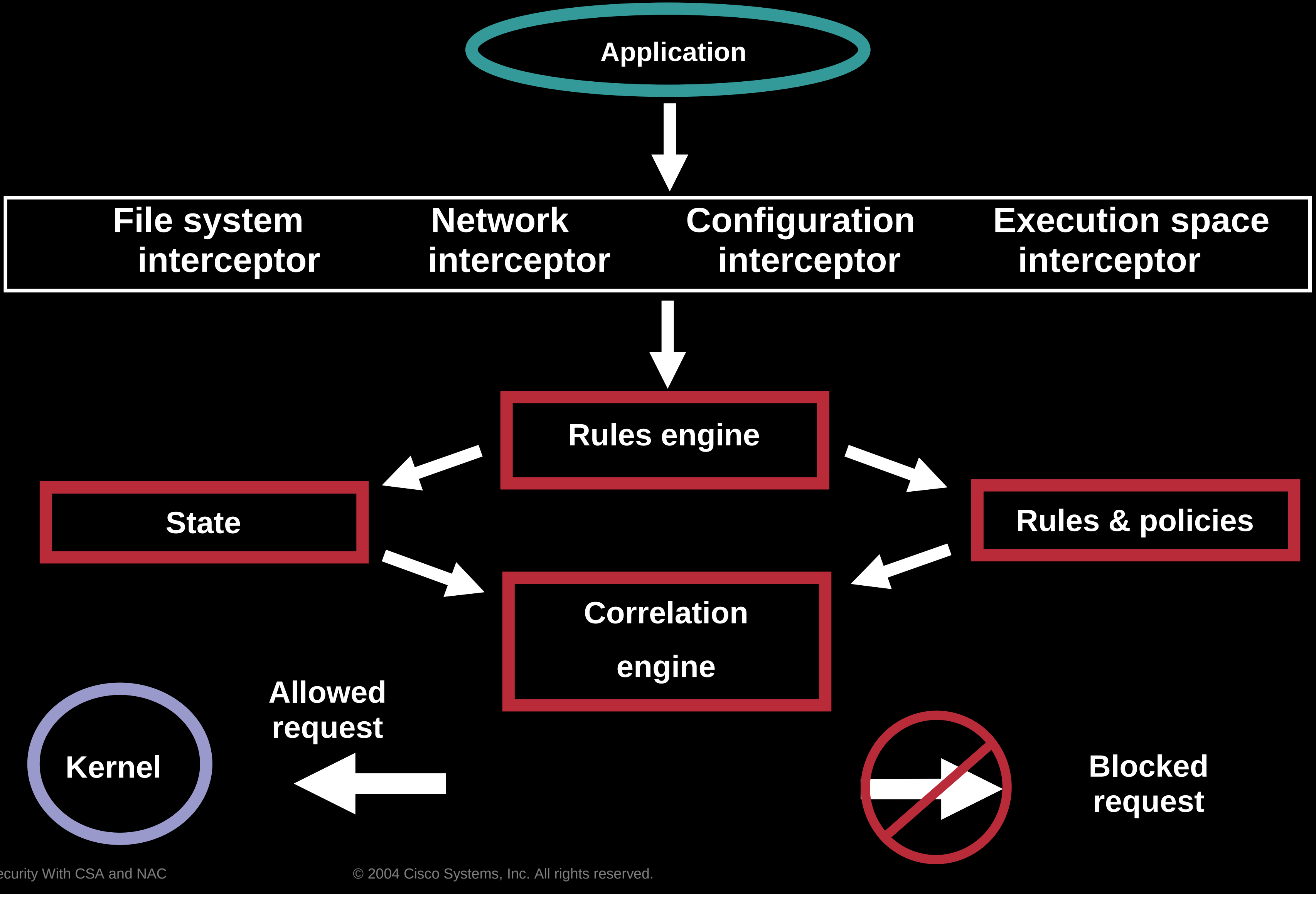
CSA Security Functions

- **System hardening**
  - Syn-flood protection
  - Malformed packet protection
  - Restart of failed services
- **Resource protection**
  - File access control
  - Network access control
  - Registry access control
  - COM component access control
- **Control of executable content**
  - Protection against email worms
  - Protection against automatic execution of downloaded files or ActiveX controls
- **Application-related**
  - Application run control
  - Executable file version control
  - Protection against code injection
  - Protection of process memory
  - Protection against buffer overflows
  - Protection against keystroke logging
- **Detection**
  - Packet sniffers and unauthorized protocols
  - Network scans
  - Monitoring of OS event logs
- **Network firewalling**

CSA Implementation Approaches

- Call Interception
  - Intercept system calls between applications and the operating system
- Security policy
  - Pre-defined rules
  - Heuristics
  - Combination of methods
- System “state” monitoring
  - Application behavior—What are the running applications doing?

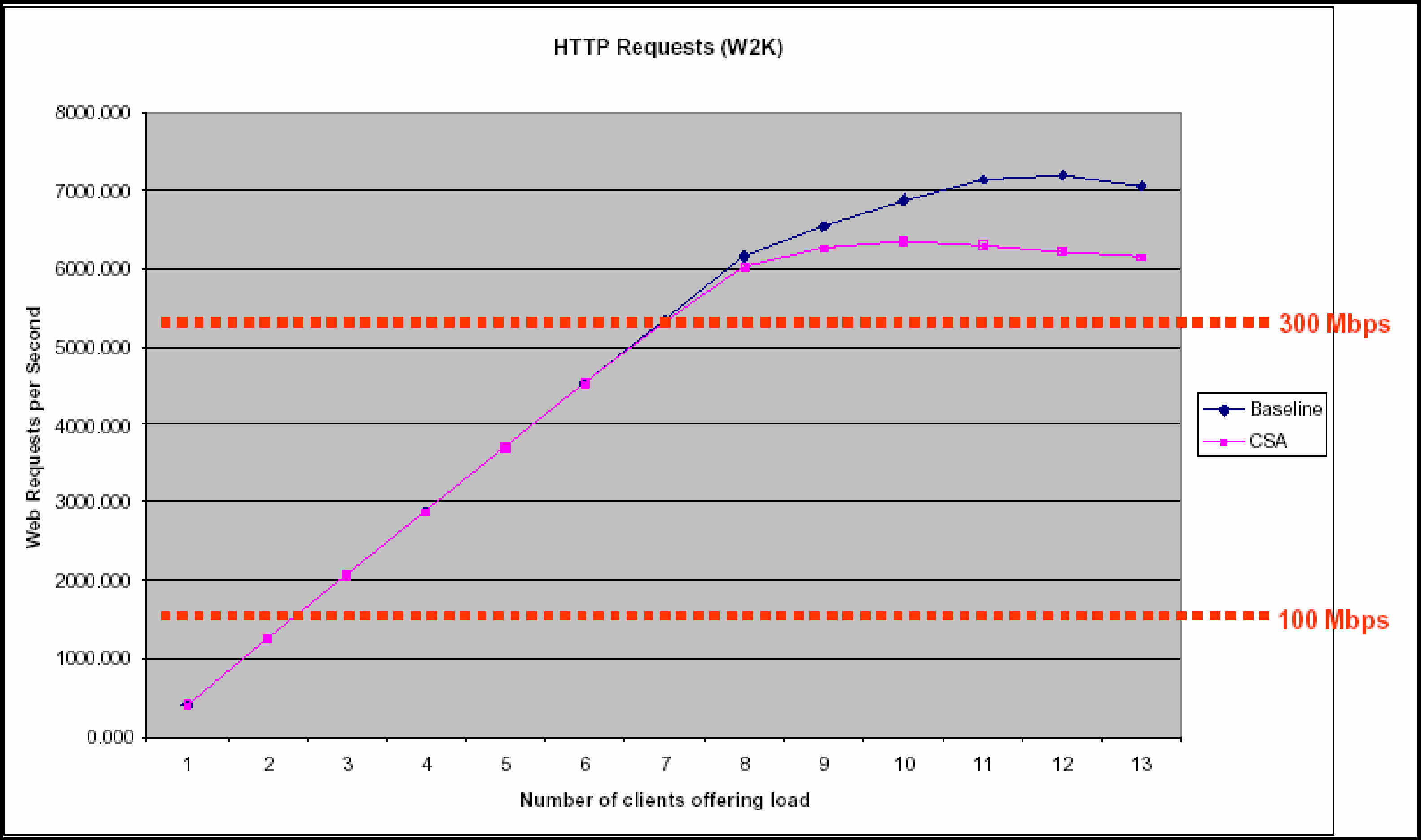
CSA Architecture Overview



Performance Impact

- Windows CPU usage: 1-5%
- Solaris CPU usage: 3-10%
- Memory usage: 7–10MB, up to 20
- Network impact:
  - Policy download: 35-70k
  - Event: ~3k
  - Poll: ~2.5k
  - Polling interval change: ~3k
  - Software update: Varies
- Transactions per second is a very good way to measure latency

Performance: Transactions per Second



Note: Performed on W2K SP3 Running IIS 5.0; Single 2Ghz P4 CPU, 1Gbps NIC, Non-hyperthreaded, 533Mhz System Bus

CSA Integration other Security Technologies

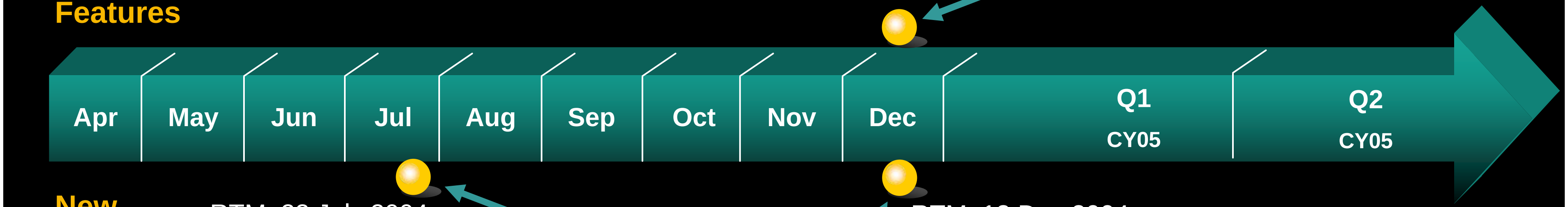
- VPN “Are You There”
  - Requires version 4.0 of Cisco VPN client and concentrator
  - Also supported in Checkpoint VPN-1
- Network Admission Control (NAC)
- Complement NIDS and AV
  - Combining signature detection and behavioral protection
  - Need AV to eradicate a virus, worm, or trojan
- Log Collectors and Correlators
- Windows Event Viewer and AV logs into CSA events

Cisco Security Agent Roadmap

New Features – version 4.5

- MC Scalable to 100,000 agents
- Antivirus DAT version checking
- Application/patch tracking
- Location-based policies
- User-based profiles
- Agent Internationalization & Localization
- Policies based on NAC status
- Security Enhancements

New Features



New Agent Platforms

RTM: 22 July 2004
CCO Download: 22 July 2004
FCS: 22 July 2004

New Agent Platforms – ver 4.0.3

- Windows 2003 Server
- Windows XP SP2

RTM: 13 Dec 2004
CCO Download: 13 Dec 2004

New Agent Platforms – ver 4.5

- Windows Clusters
- RedHat Enterprise Linux 3.0
  - Enterprise Server, Workstation
  - Advanced Server (Stretch Goal)
- Windows XP Home Edition

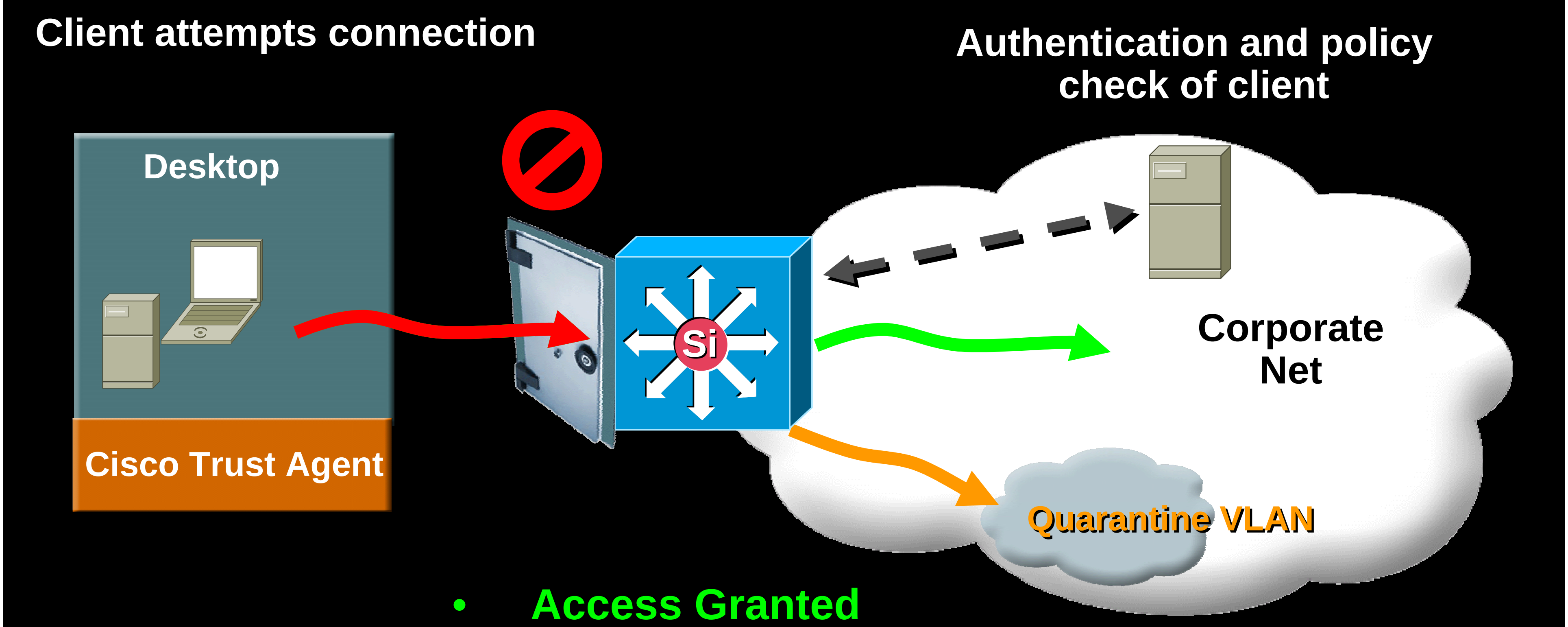
Network Admission Control (NAC)

Agenda – NAC

- Overview of Network Admission Control
- NAC Phase 1 (Current) Model and Components
- NAC Credentials
- NAC Phase 2 (Future) Model and Components

Network Admission Control (NAC)

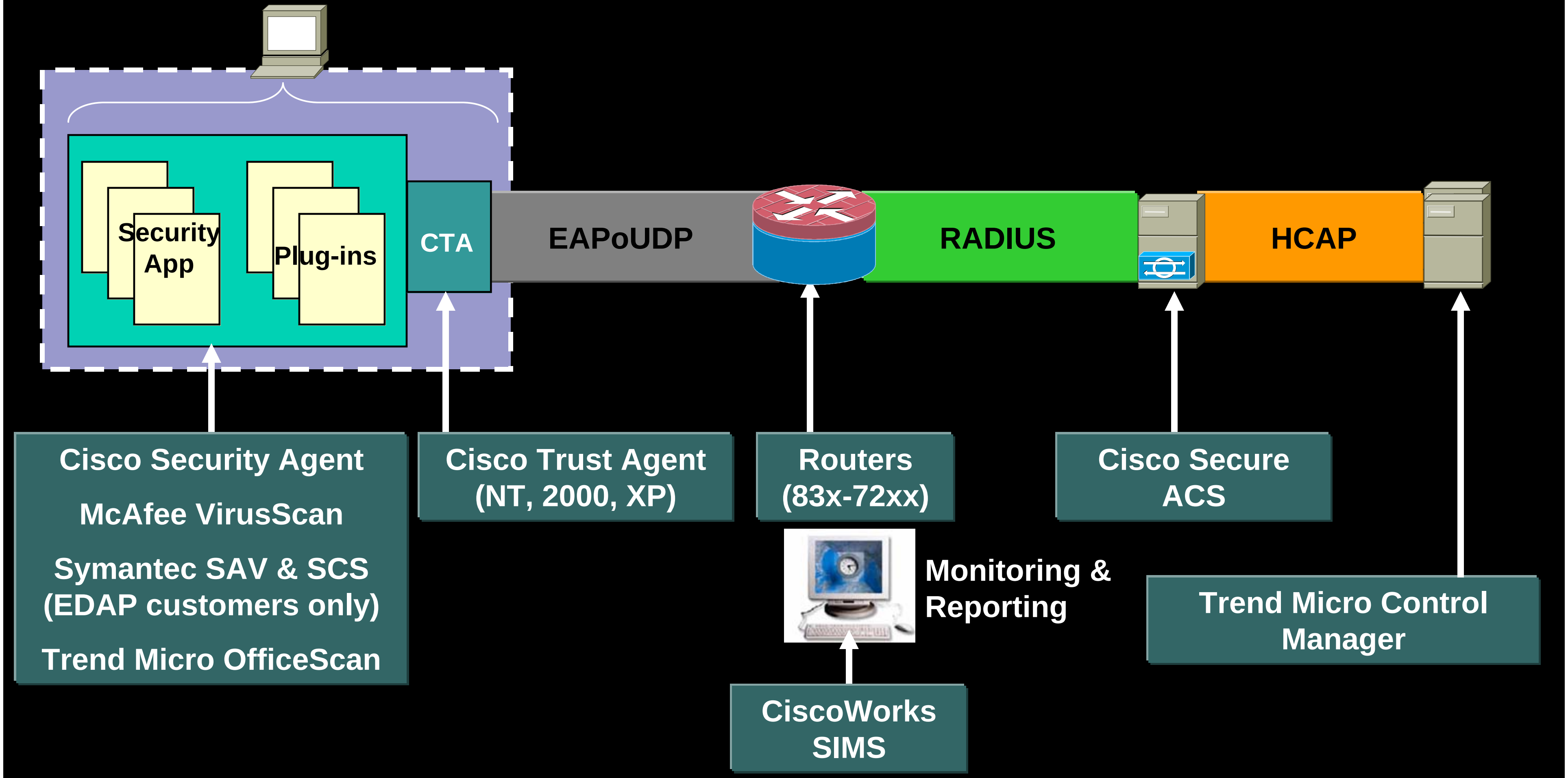
preventing non-compliant host


Client attempts connection
Authentication and policy check of client
Desktop
Cisco Trust Agent
Si
Corporate Net
Quarantine VLAN

- Access Granted
- Access Denied
- Quarantine Remediation

NAC Phase 1 Logical Components

June 2004



Cisco Security Agent

McAfee VirusScan

Symantec SAV & SCS (EDAP customers only)

Trend Micro OfficeScan

Cisco Trust Agent (NT, 2000, XP)

Routers (83x-72xx)

Cisco Secure ACS

Monitoring & Reporting

Trend Micro Control Manager

CiscoWorks SIMS

Credentials Available

- NAC credentials characterize the state of an asset, and compliment ID credentials for the asset and user
- Credentials form the basis for policy expressions for network admission control
- Below are most of the initial credentials available at NAC phase 1 ship
- Vendors will add new credentials often and at any time

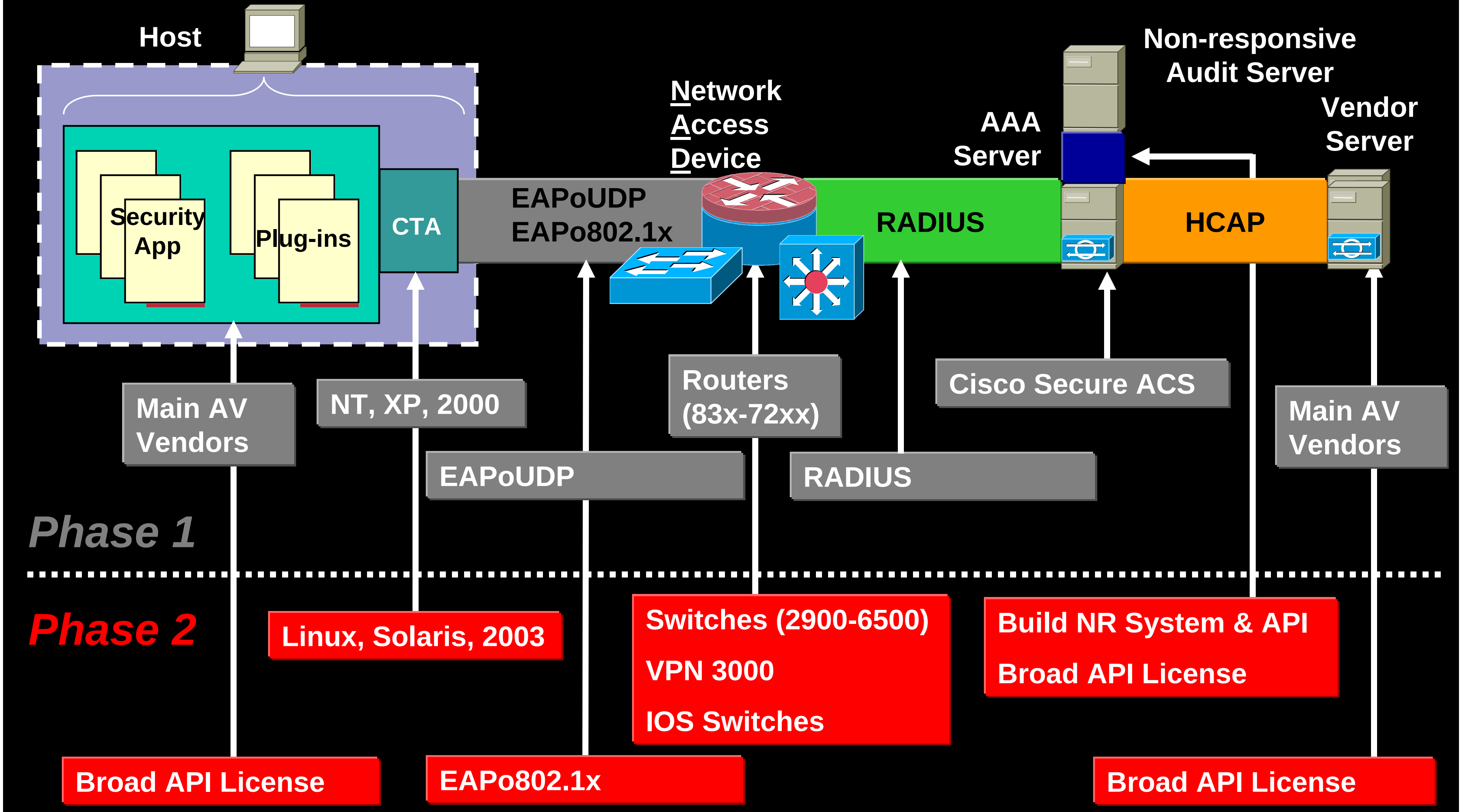
FROM CISCO AGENTS

- CTA 1.0
  - CTA version
  - Operating system name
  - Operating system version
- CSA 4.0.2
  - Installed Service Packs
  - Installed hotfixes
  - CSA version
  - CSA enabled or disabled
  - FQDN of CSA-MC (VMS)
  - CSA status
  - Last poll of CSA-MC (VMS)

FROM VENDORS

- Anti-Virus
  - AV software name or identifier
  - Software version
  - Scan engine version
  - DAT/pattern file version
  - AV enabled or not
  - On-access scan enabled
  - DAT/pattern file release date
- Other Software
  - Varies by vendor
  - E.g. SYMC SCS 2.0 includes FW and HIDS

NAC Phase 2 Logical Components



Host

Security App

Plug-ins

CTA

EAPoUDP
EAPo802.1x

Network Access Device

AAA Server

RADIUS

Non-responsive Audit Server

HCAP

Vendor Server

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

Cisco Systems®