Technical Dive into Network Admission Control and Next Generation Event Management (MARS)

Haider Pasha, CISSP

Consulting Systems Engineer, MEA

hpasha@cisco.com

© 2007 Cisco Systems, Inc. All rights reserved.

Network Admission Control

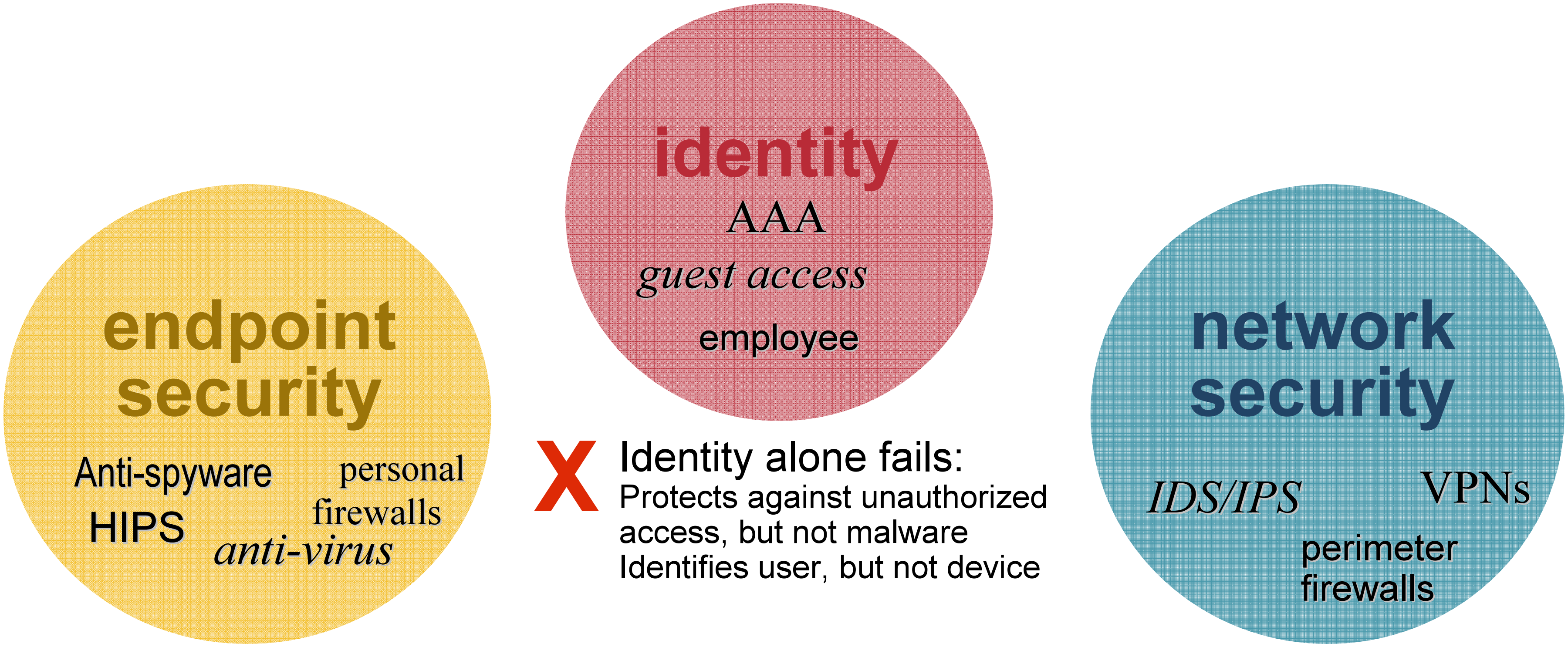
© 2007 Cisco Systems, Inc. All rights reserved.

Agenda

- The Business Case for Network Admission Control
- Overview on Network Admission Control
- NAC Deployment models

© 2007 Cisco Systems, Inc. All rights reserved.

Complexity Demands Defense-in-Depth



identity
AAA
guest access
employee

endpoint security
Anti-spyware
personal firewalls
HIPS
anti-virus

network security
IDS/IPS
VPNs
perimeter firewalls

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

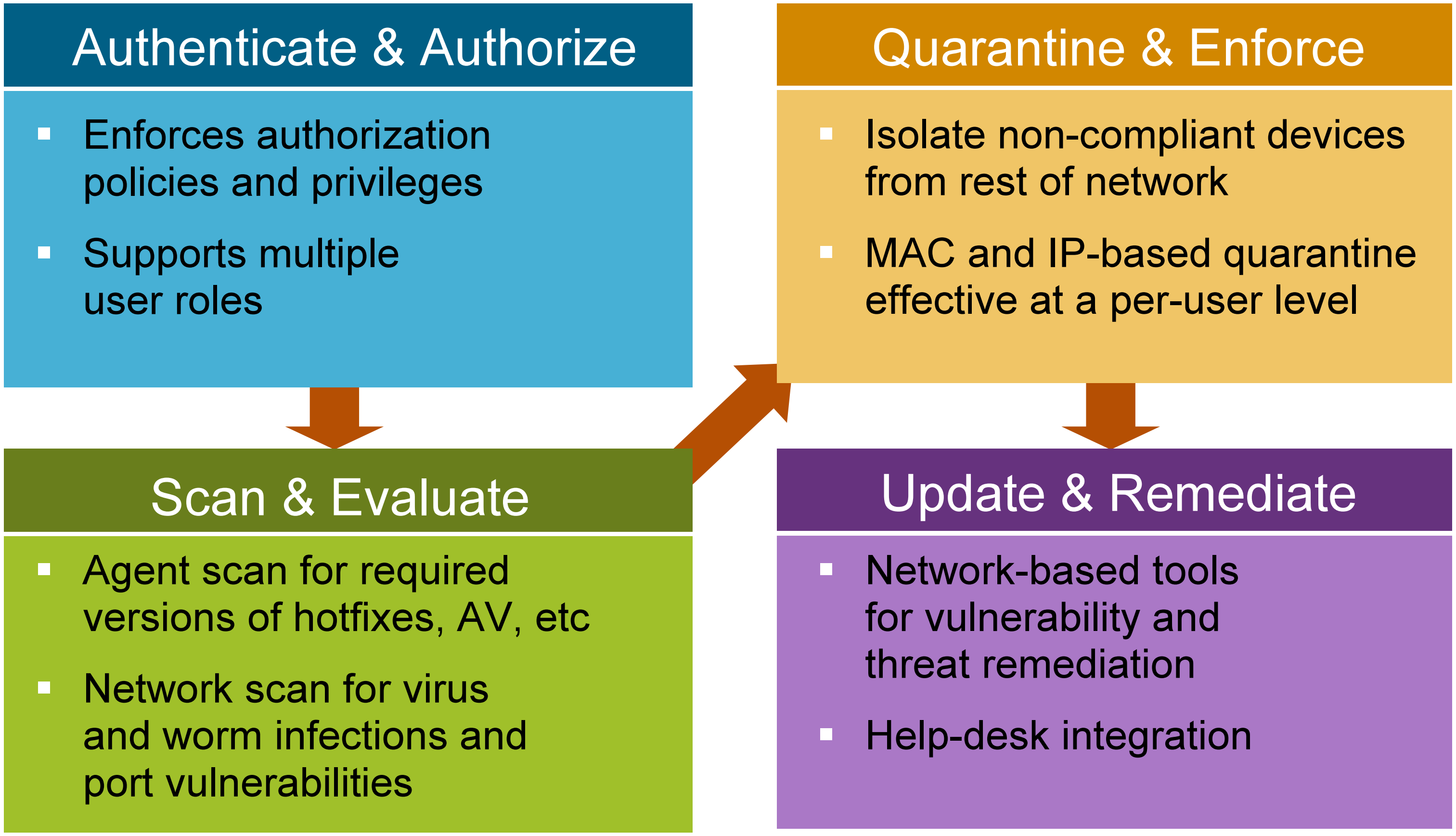
X **Endpoint security alone fails:**
99% have AV, but infections persist!
Host based apps are easily manipulated—even unintentionally
Time gap between virus and virus def/repair

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

© 2007 Cisco Systems, Inc. All rights reserved.

Make Access Contingent on Compliance

First, establish ACCESS POLICIES. Then:



Authenticate & Authorize

- Enforces authorization policies and privileges
- Supports multiple user roles

Scan & Evaluate

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

Quarantine & Enforce

- 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

NO COMPLIANCE = NO NETWORK ACCESS

© 2007 Cisco Systems, Inc. All rights reserved.

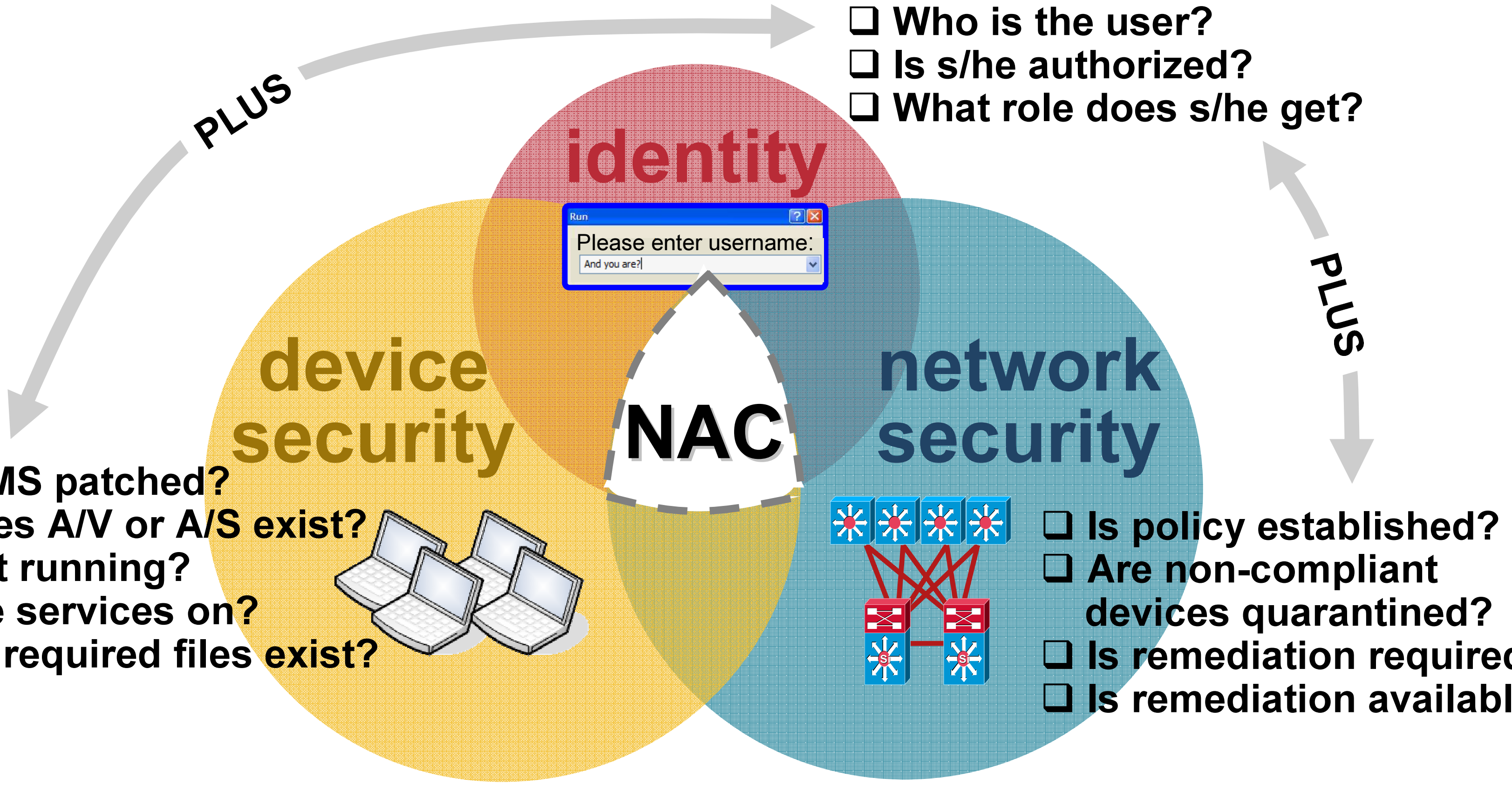
Agenda

- The Business Case for Network Admission Control
- Overview on Network Admission Control
- NAC Deployment models

© 2007 Cisco Systems, Inc. All rights reserved.

What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.



- ❑ Who is the user?
- ❑ Is s/he authorized?
- ❑ What role does s/he get?

- ❑ Is MS patched?
- ❑ Does A/V or A/S exist?
- ❑ Is it running?
- ❑ Are services on?
- ❑ Do required files exist?

- ❑ Is policy established?
- ❑ Are non-compliant devices quarantined?
- ❑ Is remediation required?
- ❑ Is remediation available?

© 2007 Cisco Systems, Inc. All rights reserved.

Four Key Capabilities of Cisco NAC

	SECURELY IDENTIFY DEVICE & USER	ENFORCE CONSISTENT POLICY	QUARANTINE AND REMEDIATE	CONFIGURE AND MANAGE
WHAT IT MEANS	Uniquely identifies users and devices, and creates associations between the two	Assess and enforce a ubiquitous policy across the entire network	Acts on posture assessment results, isolates device, and brings it into compliance	Easily creates comprehensive, granular policies that map quickly to user groups and roles
WITHOUT IT . . .	Critical to associate users and devices with roles to know which policies apply; prevents device spoofing.	A decentralized policy mechanism (e.g. on endpoint) can leave gaping security holes.	Just knowing a device is non-compliant is not enough—someone still needs to fix it.	Policies that are too complex or difficult to create and use will lead to abandonment of project.

Any robust NAC solution must have all four capabilities.

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco NAC Is Widely Deployed Today

- Cisco NAC Appliance has 2500+ customers
- Mid-market and large enterprises
  - Financial services
  - Healthcare
  - Public sector
  - Manufacturing
- **One product for all use cases**
  - Remote access VPN
  - Guest users
  - Wireless
  - LAN
  - VoIP

UNITED STATES POSTAL SERVICE
NOAA
SDV
PG&E
McDonald's
Johnson & Johnson
ABN·AMRO
Nestlé
ALLIANCE DATA SYSTEMS
TESCO
Whirlpool
Cummins
KEYSPAN
London Stock Exchange
BLACKROCK
BlueCross BlueShield of Minnesota
VIKING
Great-West

© 2007 Cisco Systems, Inc. All rights reserved.

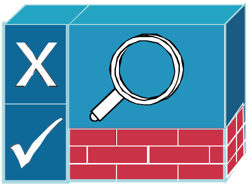
NAC Appliance Components

- **Cisco NAC Appliance Manager**

  Centralizes management for administrators, support personnel, and operators

- **Cisco NAC Appliance Server**

  Serves as posture, remediation and enforcement access control



- **Cisco NAC Appliance Agent**

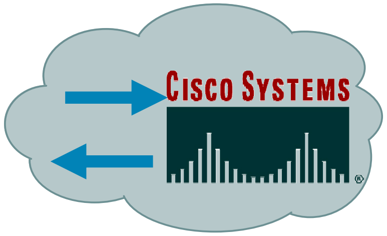
  Optional lightweight client for device-based registry scans in unmanaged environments

Clean Access Agent
by Cisco Systems

Version 3.4.0
Copyright 2004 Cisco Systems, Inc.

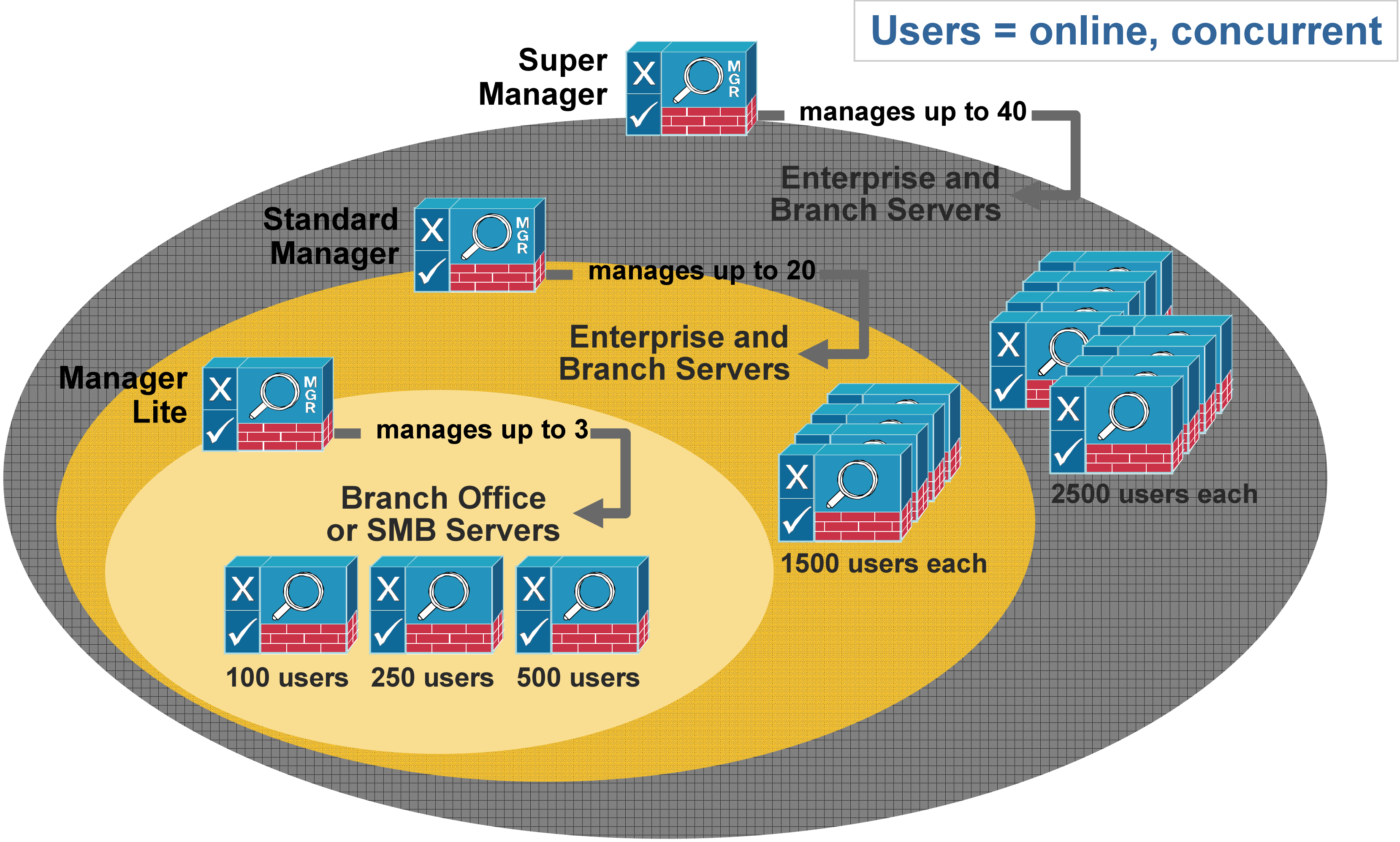
- **Rule-set Updates**

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



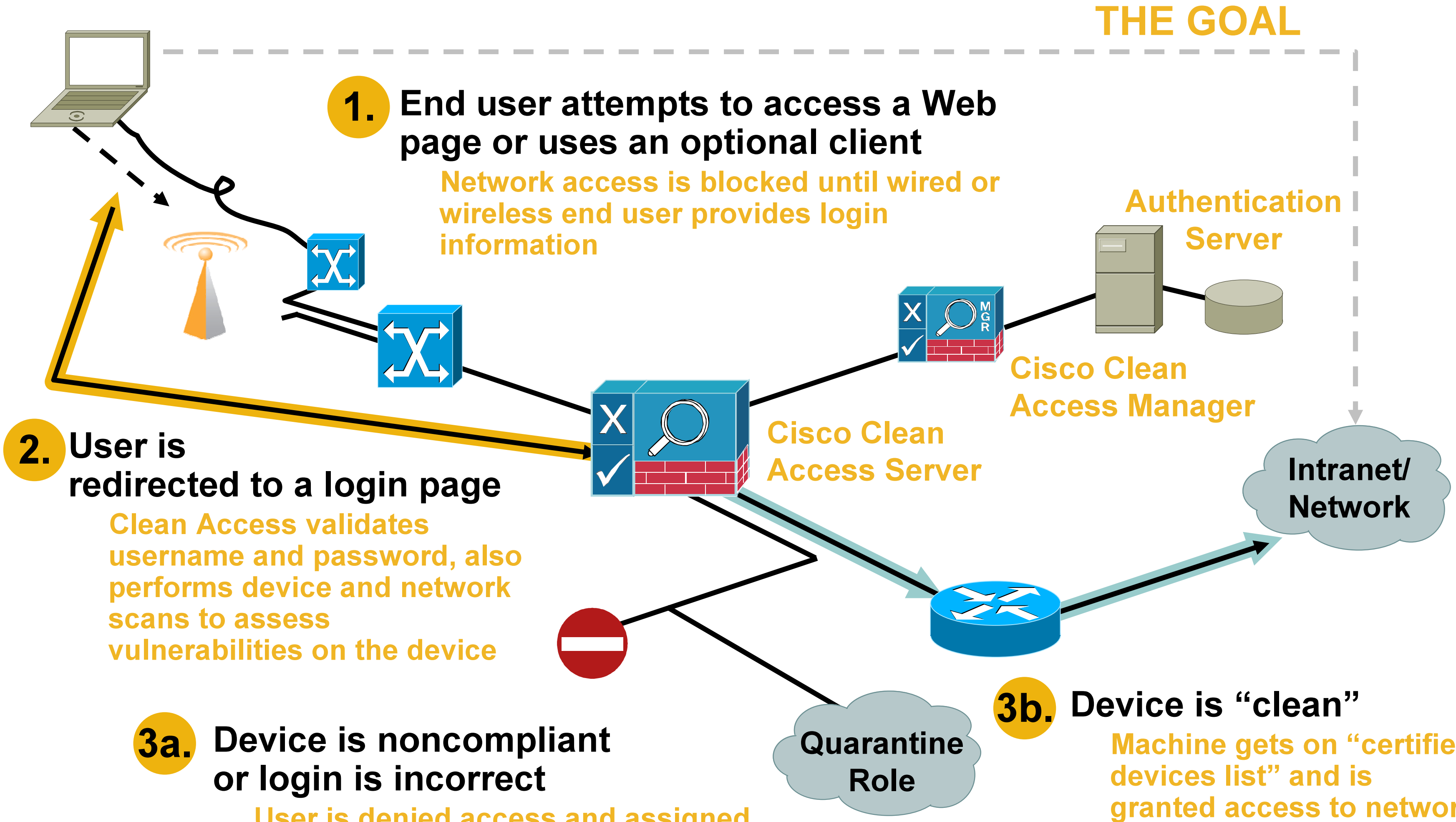
© 2007 Cisco Systems, Inc. All rights reserved.

NAC Appliance Sizing (100,000+ User support)



© 2007 Cisco Systems, Inc. All rights reserved.

Cisco NAC Appliance Overview



1. End user attempts to access a Web page or uses an optional client

Network access is blocked until wired or wireless end user provides login information

2. User is redirected to a login page

Clean Access validates username and password, also performs device and network scans to assess vulnerabilities on the device

3a. Device is noncompliant or login is incorrect

User is denied access and assigned to a quarantine role with access to online remediation resources

3b. Device is "clean"

Machine gets on "certified devices list" and is granted access to network

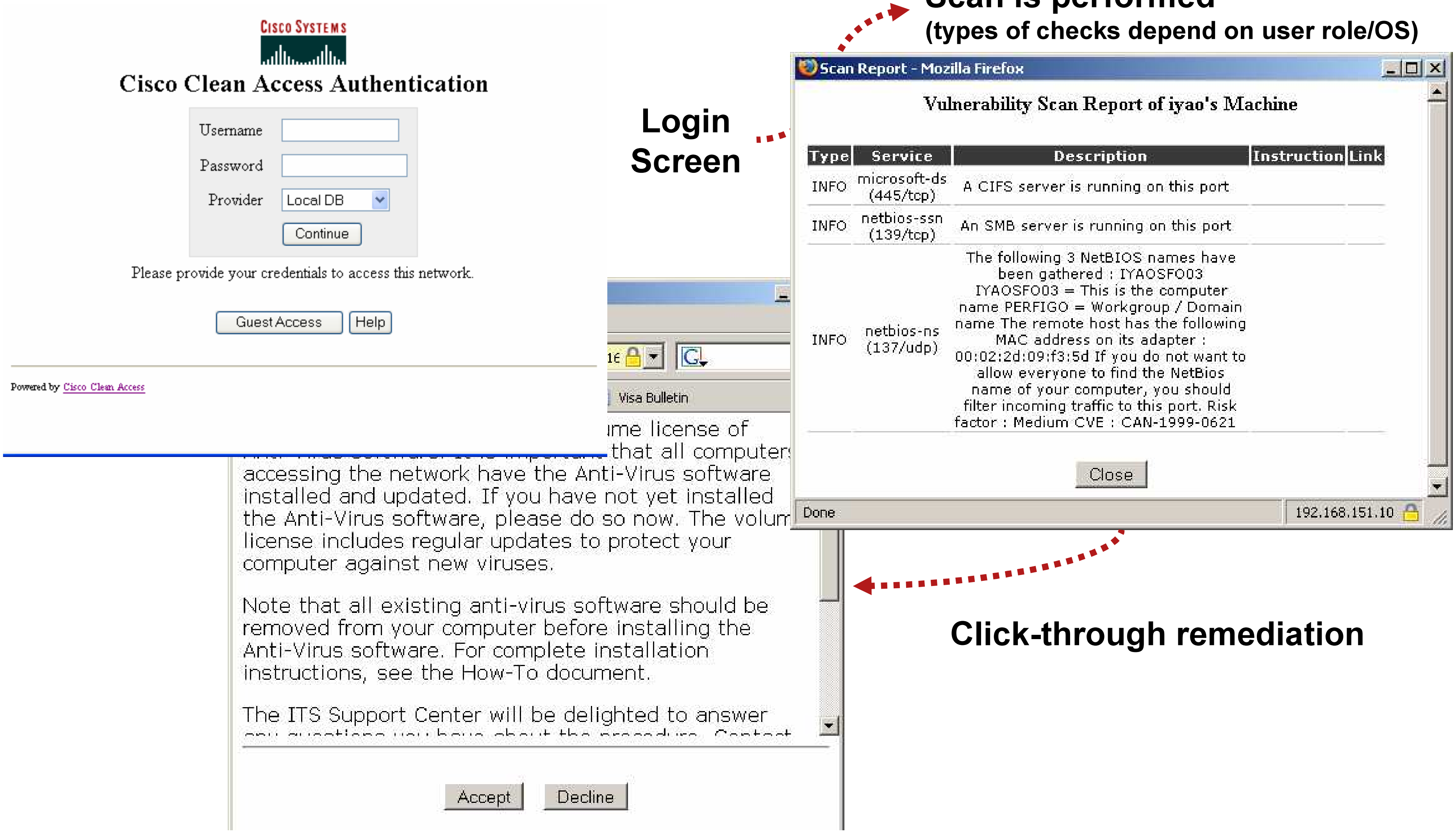
© 2007 Cisco Systems, Inc. All rights reserved.

Endpoint Security Posture

End User Experience Demo

© 2007 Cisco Systems, Inc. All rights reserved.

End User Experience: Web-based



Scan is performed

(types of checks depend on user role/OS)

Login Screen

Click-through remediation

Cisco Clean Access Authentication

Username

Password

Provider: Local DB

Please provide your credentials to access this network.

Powered by Cisco Clean Access

ıme license of
that all computer
accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volum
license includes regular updates to protect your computer against new viruses.

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

Vulnerability Scan Report of iyao's Machine

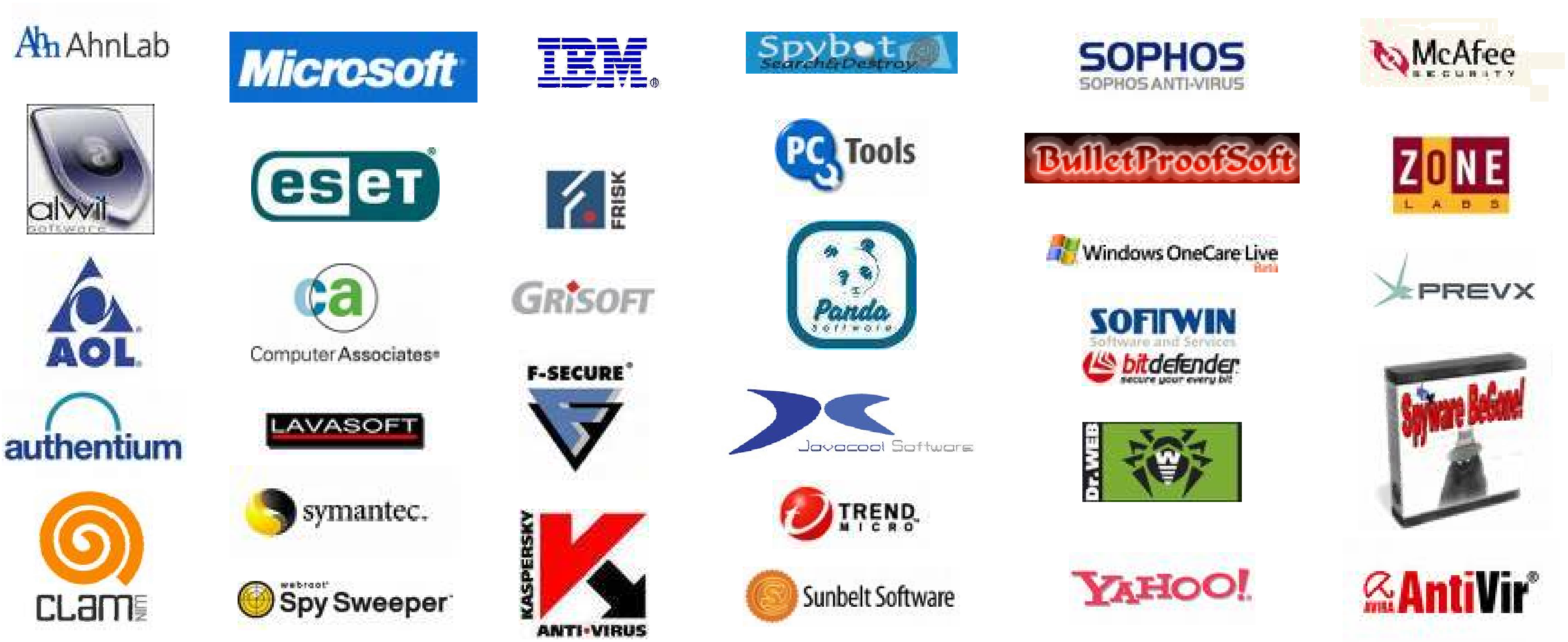
Type	Service	Description	Instruction	Link
INFO	microsoft-ds (445/tcp)	A CIFS server is running on this port		
INFO	netbios-ssn (139/tcp)	An SMB server is running on this port		
INFO	netbios-ns (137/udp)	The following 3 NetBIOS names have been gathered : IYAOSFO03 IYAOSFO03 = This is the computer name 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		

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco NAC Appliance Partnerships

Cisco NAC is committed to protecting customer’s investments in partner applications

NAC Appliance Supports Policies for 250+ Applications, Including These Vendors:



© 2007 Cisco Systems, Inc. All rights reserved.

NAC - Microsoft Support

Current Support

Window OS Agent Support
Vista (Business Edition)
XP (Home/Pro/MCE/Tablet)
2000/ME/98 (Agent)

Windows Agentless Support
WinCE, WinMobile
IE5.x, 6.x and 7.x

Windows Language Pack Support
15+ languages supported

Windows Hotfixes/AV Checks
Auto-updates to pre-configured Hotfix and oneCare AV checks

Windows Update via windowsupdate.com
Redirect to windowsupdate.com for remediation

Windows Update via WSUS
Ability to configure Windows Updater parameters
Launch WSUS agent for auto-remediation

GPO/Login

AD Single-Sign-On
Windows 2003/2000 Server

GPO Launch post Authentication
Ability to launch GPO to tie AD desktop policy to access VLAN

Login Script “hold” Configuration
Provide a configuration to hold login script mapping till access VLAN

Upcoming

WSUS Agent immediate launch
Ability to force WSUS agent to remediate now

Microsoft SMS Agent remediation
Launch SMS Agent during remediation or x-days old

Vista Consumer Support

© 2007 Cisco Systems, Inc. All rights reserved.

Agenda

- The Business Case for Network Admission Control
- Overview on Network Admission Control
- Deployment of Network Admission Control

© 2007 Cisco Systems, Inc. All rights reserved.

Examples of Posture Assessment

Corporate Asset Tag

- Unique registries inserted into corporate devices
- Corporate PKI certificates installed in corporate devices

Microsoft Hotfixes:

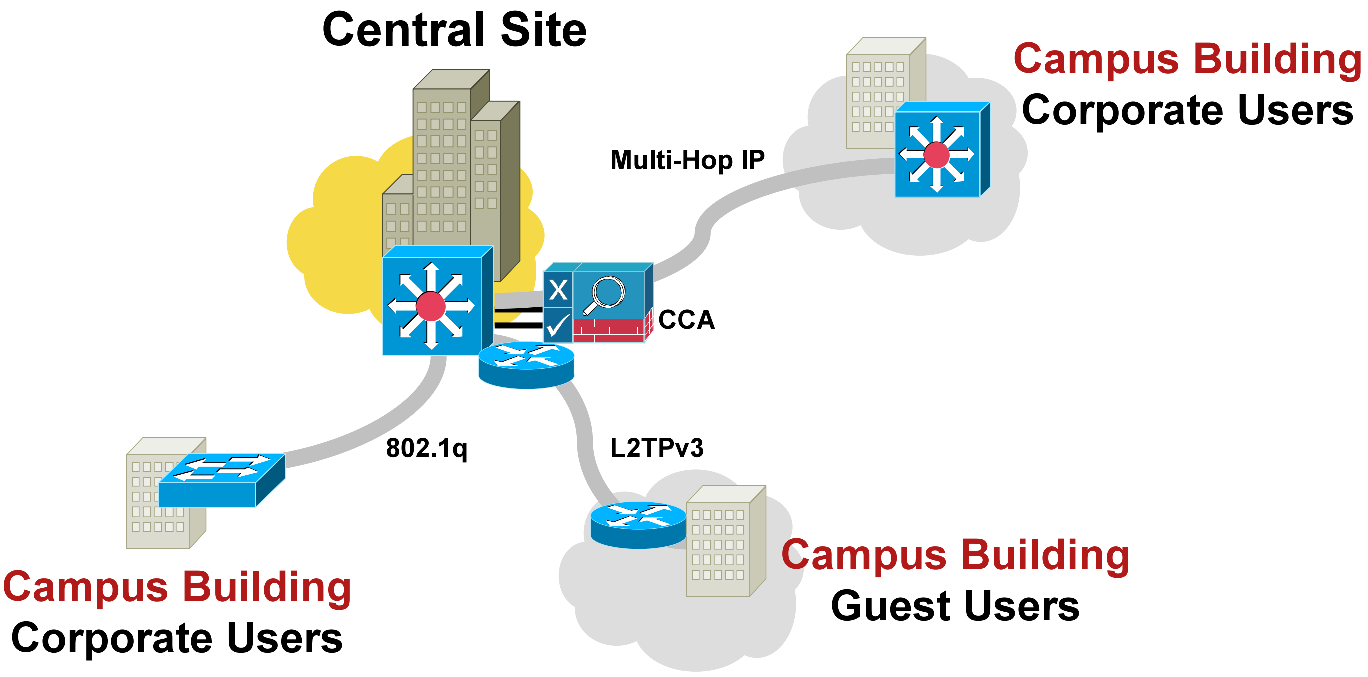
- Critical hot-fixes checks (provided via Cisco automated updates)
- SUS/WUS running or AU Options (can force setting)
- Patch Management SW running (can launch qualified .exe)

Security Applications:

- HIDS (CSA) or Personal Firewall installed and running
- AV installed, running and latest DAT (can launch AV)
- Anti-Spyware installed and running
- Encryption software installed and running

© 2007 Cisco Systems, Inc. All rights reserved.

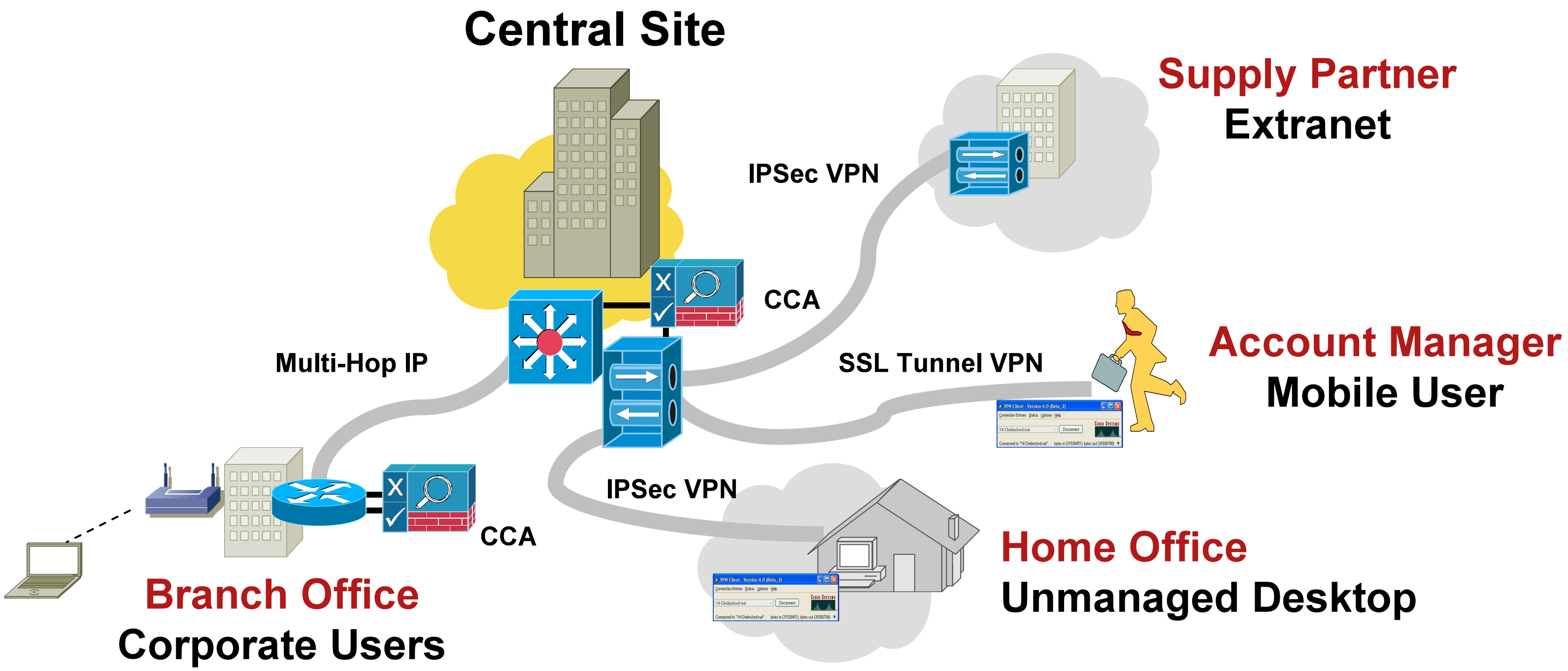
NAC Appliance for Corporate LAN



FEATURES	BENEFITS
▪ Supports 802.1q trunking ▪ Supports both L3 multi-hop and L2 ▪ Supports L2TPv3 tunneling ▪ Supports both inband and out-of-band	▪ Enables central deployment mode ▪ End user devices can be several hops away ▪ Extends enforcement to campus buildings

© 2007 Cisco Systems, Inc. All rights reserved.

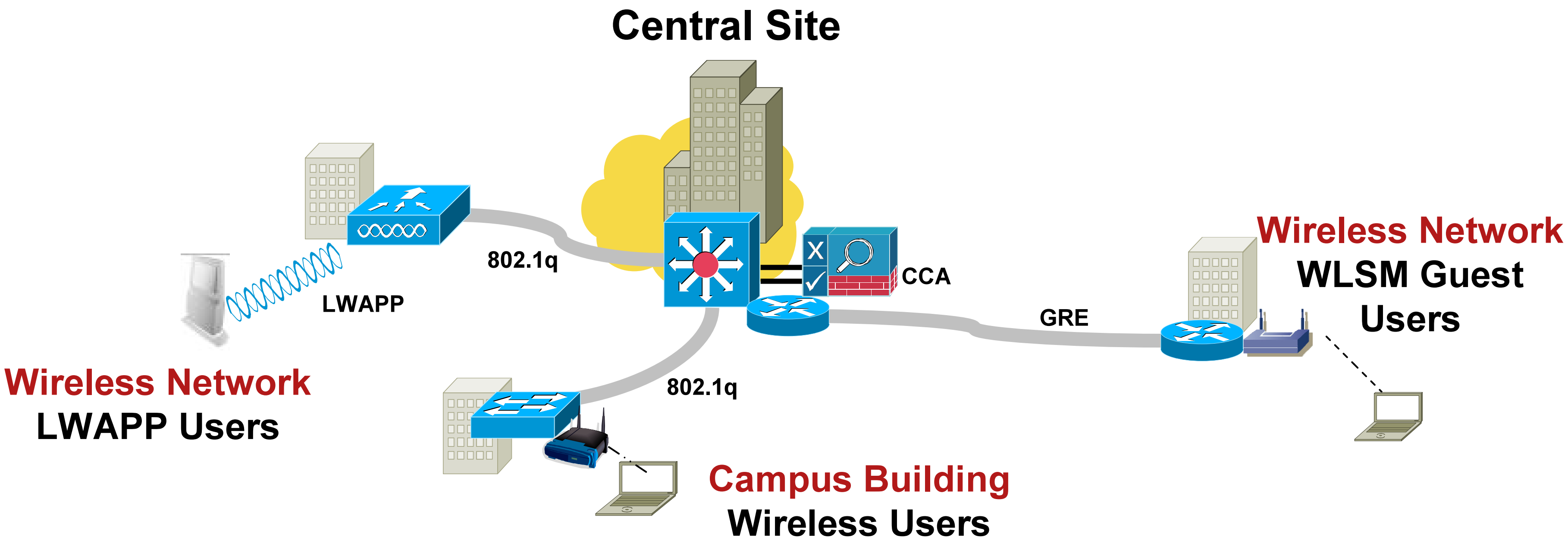
NAC Appliance for Remote Users



FEATURES	BENEFITS
▪ Supports IPSec and SSL Tunnel VPNs	▪ Extends policy enforcement and compliance to remote access and VPN users
▪ Supports site-to-site VPNs	▪ Extends enforcement to site-to-site VPN partners
▪ Supports VPN user sign-on	▪ Leverages VPN sign-on for single-sign-on

© 2007 Cisco Systems, Inc. All rights reserved.

NAC Appliance for Wireless Users



FEATURES	BENEFITS
▪ Supports 802.1q trunking ▪ Support L2TPv3 or GRE tunneling ▪ Supports thin or thick wireless 802.11 APs ▪ Supports Wireless user sign-on	▪ Enables central deployment mode ▪ End user devices can be several hops away ▪ Extends enforcement to any wireless networks ▪ Leverages EAP sign-on for single-sign-on

© 2007 Cisco Systems, Inc. All rights reserved.

Deployment Tips and Best Practices

In-Band

- Required for wireless.
- Required for VPN.
- Deployed in 'Real-IP' mode when users are multiple hops away from the CAS.
- Direct traffic to the untrusted interface (eth1) using 802.1q or policy-based routes for users or
- VLANs that need to become certified.

Out-of-Band

- Deployed in networks where high network throughput is required.
- MAC notification is preferable to Link-State notification as a means of trap reporting because it is quicker.
- To ensure proper SNMP configuration enterprise wide, the use of an SNMP manager such as Cisco Works is highly recommended.
- If deploying into a network with VOIP, MAC Notification is required on the access switch if PC's will be plugged into the back of the phone.

© 2007 Cisco Systems, Inc. All rights reserved.

Monitoring, Analysis and Response System

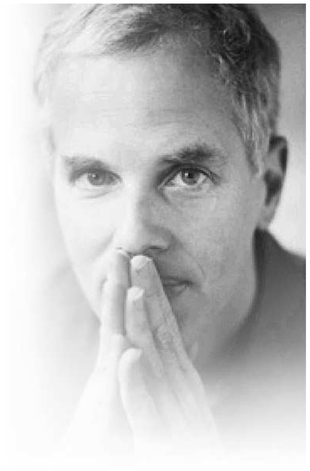
© 2007 Cisco Systems, Inc. All rights reserved.

Agenda

- Security Management Challenges
- Overview on Cisco MARS
- MARS in Action

© 2007 Cisco Systems, Inc. All rights reserved.

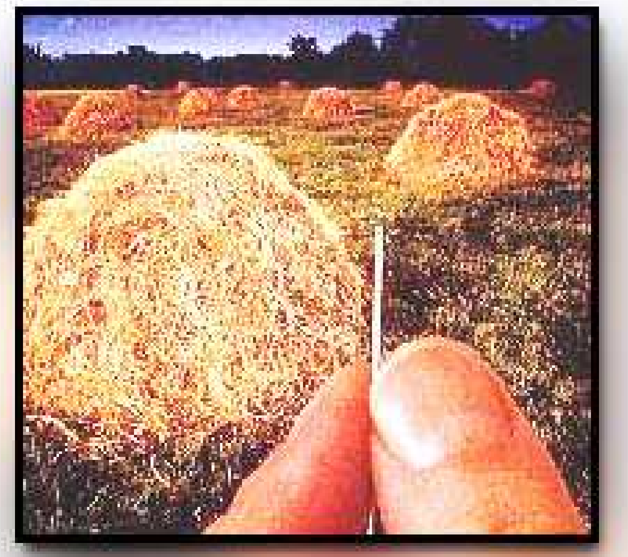
Security Logging



	Events /Sec	MB/Hr
Small VPN Gateway	50	27.4
Entry Firewall	100	54.8
High Router	200	109.6
Mid IPS	400	219.2

Reasons for logging:

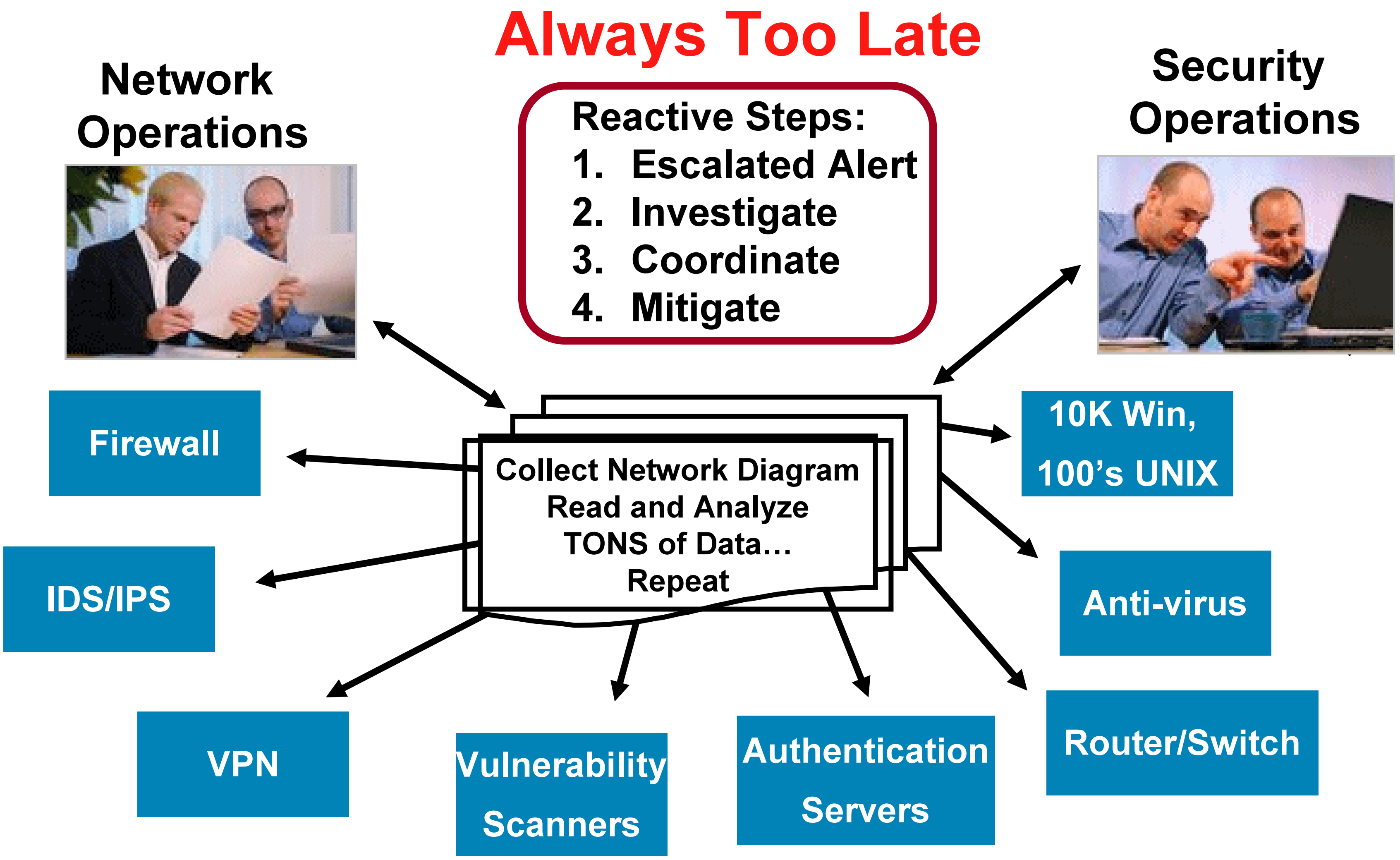
- **I don't need it, so I don't log it**
- **I log for troubleshooting reasons**
- **I log for security analysis**
- **I am logging for legal reasons**



**Too Many Devices, Too Much Data—
All to Find a Needle in a Haystack**

© 2007 Cisco Systems, Inc. All rights reserved.

Security Operations Response



Always Too Late

Network Operations

Security Operations

Reactive Steps:

1. Escalated Alert
2. Investigate
3. Coordinate
4. Mitigate

Collect Network Diagram
Read and Analyze
TONS of Data…
Repeat

Firewall

IDS/IPS

VPN

Vulnerability Scanners

Authentication Servers

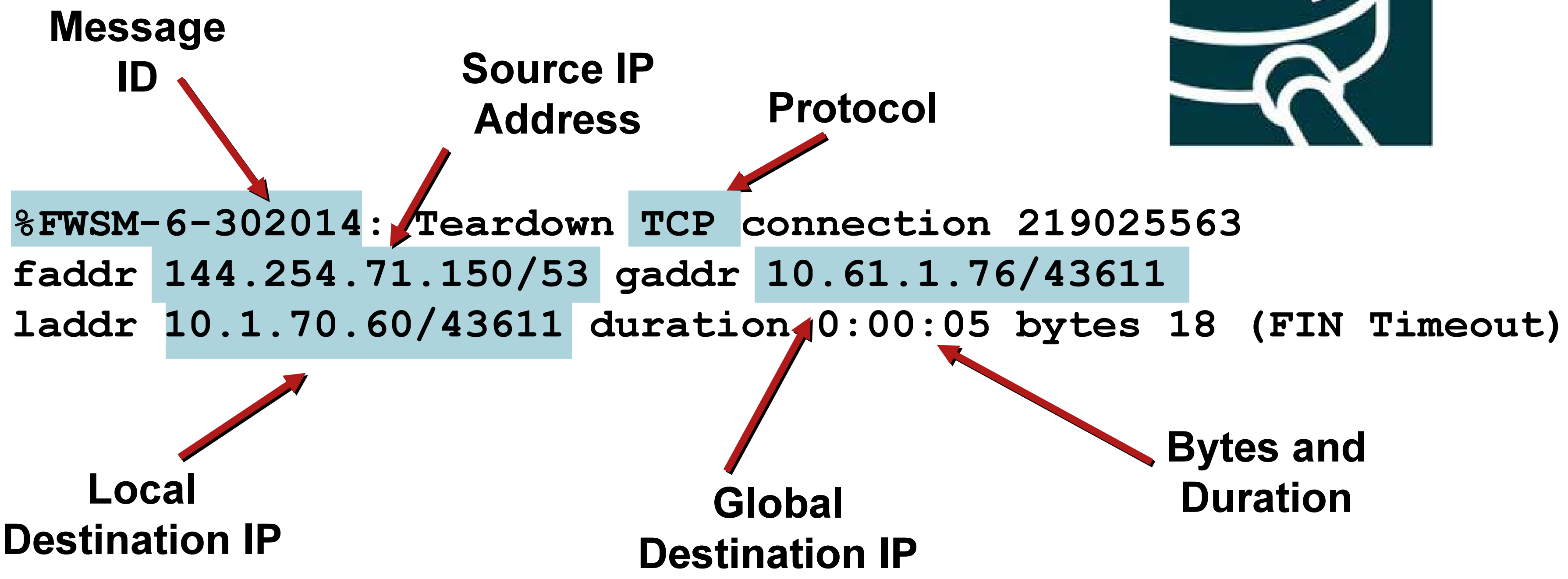
Router/Switch

Anti-virus

10K Win, 100’s UNIX

© 2007 Cisco Systems, Inc. All rights reserved.

Interpreting a Syslog Message



```
%FWSM-6-302014: Teardown TCP connection 219025563
faddr 144.254.71.150/53 gaddr 10.61.1.76/43611
laddr 10.1.70.60/43611 duration 0:00:05 bytes 18 (FIN Timeout)
```

Message ID

Source IP Address

Protocol

Local Destination IP

Global Destination IP

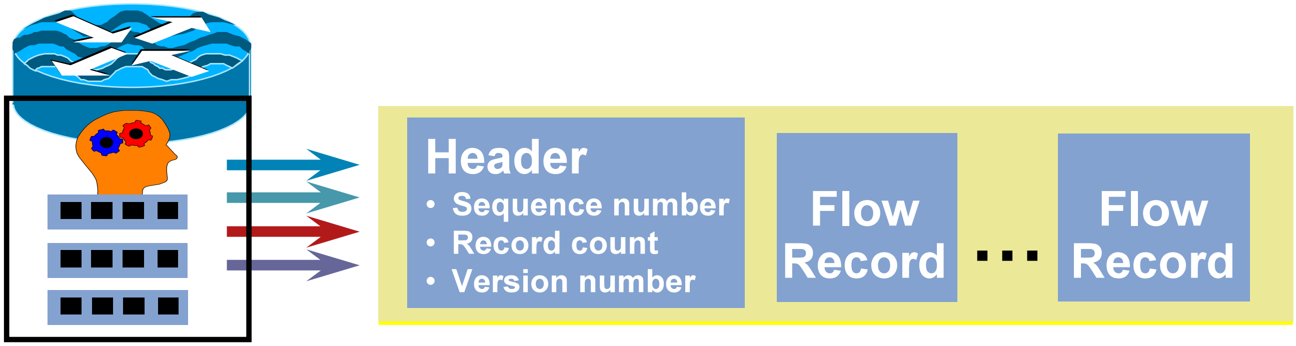
Bytes and Duration

© 2007 Cisco Systems, Inc. All rights reserved.

NetFlow

```
router (config-if)#ip flow ingress
router (config)#ip flow-export destination 172.17.246.225 9996
```

- NetFlow is available on routers and switches
- Have syslog like information without having to buy a firewall
- One NetFlow packet has information about multiple flows



Header
- Sequence number
- Record count
- Version number

Flow Record … Flow Record

NetFlow Cache

© 2007 Cisco Systems, Inc. All rights reserved.

Agenda

- Security Management Challenges
- Overview on Cisco MARS
- MARS in Action

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Security - MARS Feature Overview

Summary:

- Next Generation SIM/STM Appliances
- Transforms raw network and security data into actionable intelligence

Key features

- Collect, aggregate & correlate from heterogeneous devices in a single appliance
  - SDEE, Syslog, Host logs, Firewall logs …. From Cisco, Non-Cisco and Custom devices
  - No software agents required
- Network behavioural Analysis and Reporting (NBAR)
  - Netflow and Traffic Flow analysis provides enhanced threat detection precision
- Topological Awareness
  - Device Configuration (+NAT, +Routing) knowledge critical to global decision making
  - Attack-path views for detailed investigation and troubleshooting
- Centralized dashboard for Unified Security Operations
- Mitigation Capabilities
  - Layer 2 / Layer 3 Mitigation Suggestions (port disable, shun commands, ACLs etc.)
- Policy-Management Linkages

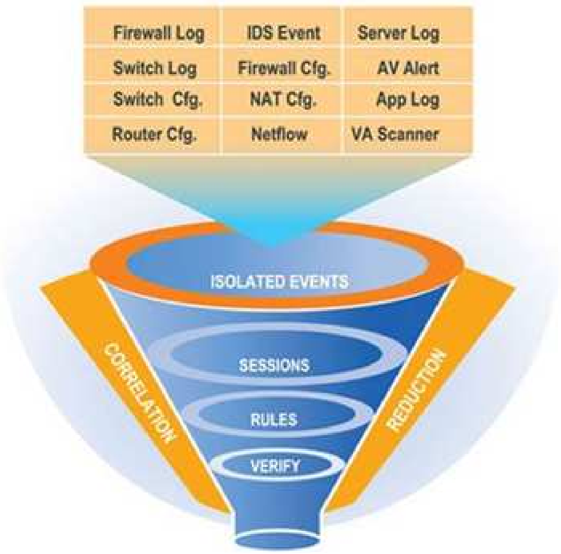
© 2007 Cisco Systems, Inc. All rights reserved.

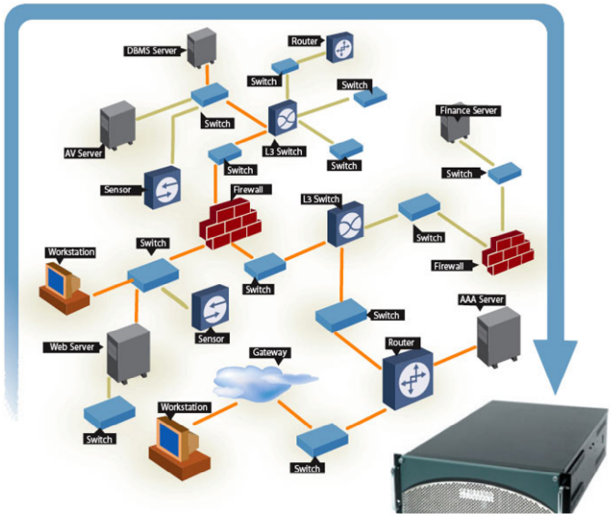
Cisco Security – MARS
Monitoring, Analysis and Response System

- Command and control of your existing investment to build “pervasive security”
- Correlate data from across the Enterprise

  NIDS, Firewalls, Routers, Switches, CSA

  Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs, Multi-Vendor
- Rapidly locate and mitigate attacks





- Key Features

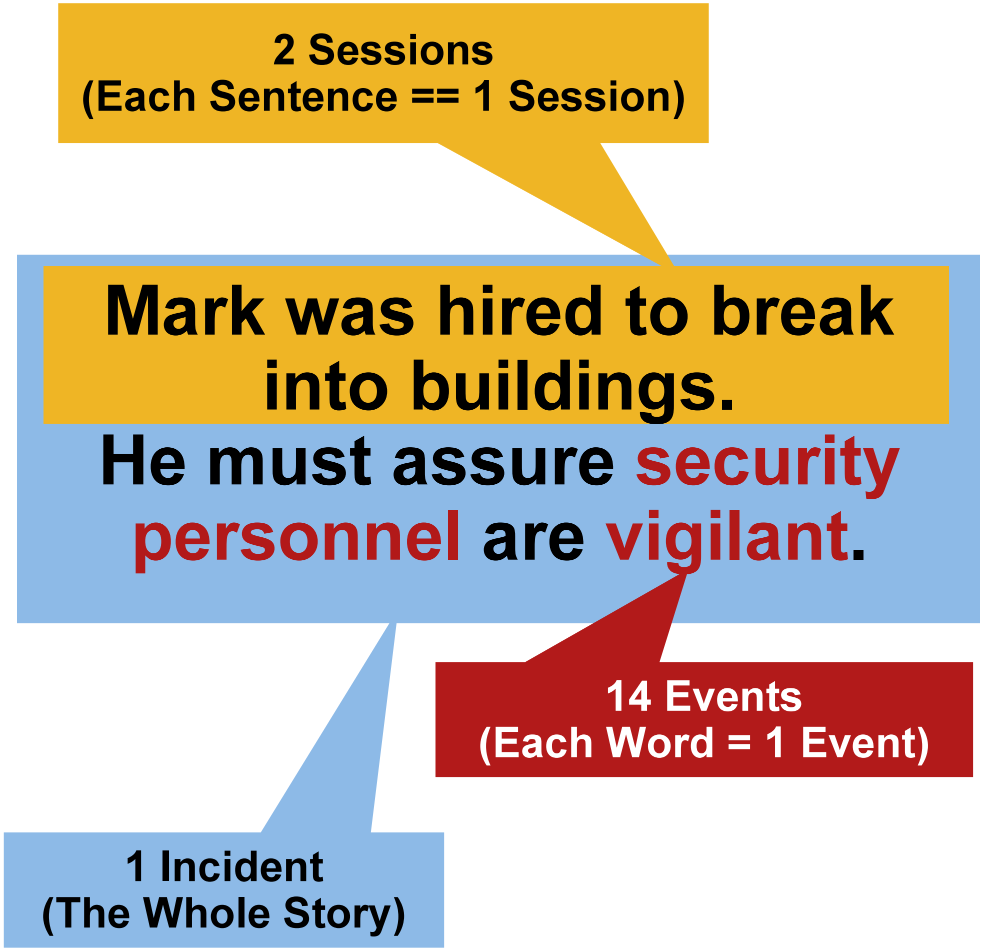
  Determines security *incidents* based on device *messages*, *events*, and “*sessions”*

  Incidents are topologically aware for visualization and replay

  Mitigation on L2 ports and L3 chokepoints

© 2007 Cisco Systems, Inc. All rights reserved.

Key Concept and Terminologies



2 Sessions
(Each Sentence == 1 Session)

Mark was hired to break into buildings.
He must assure security personnel are vigilant.

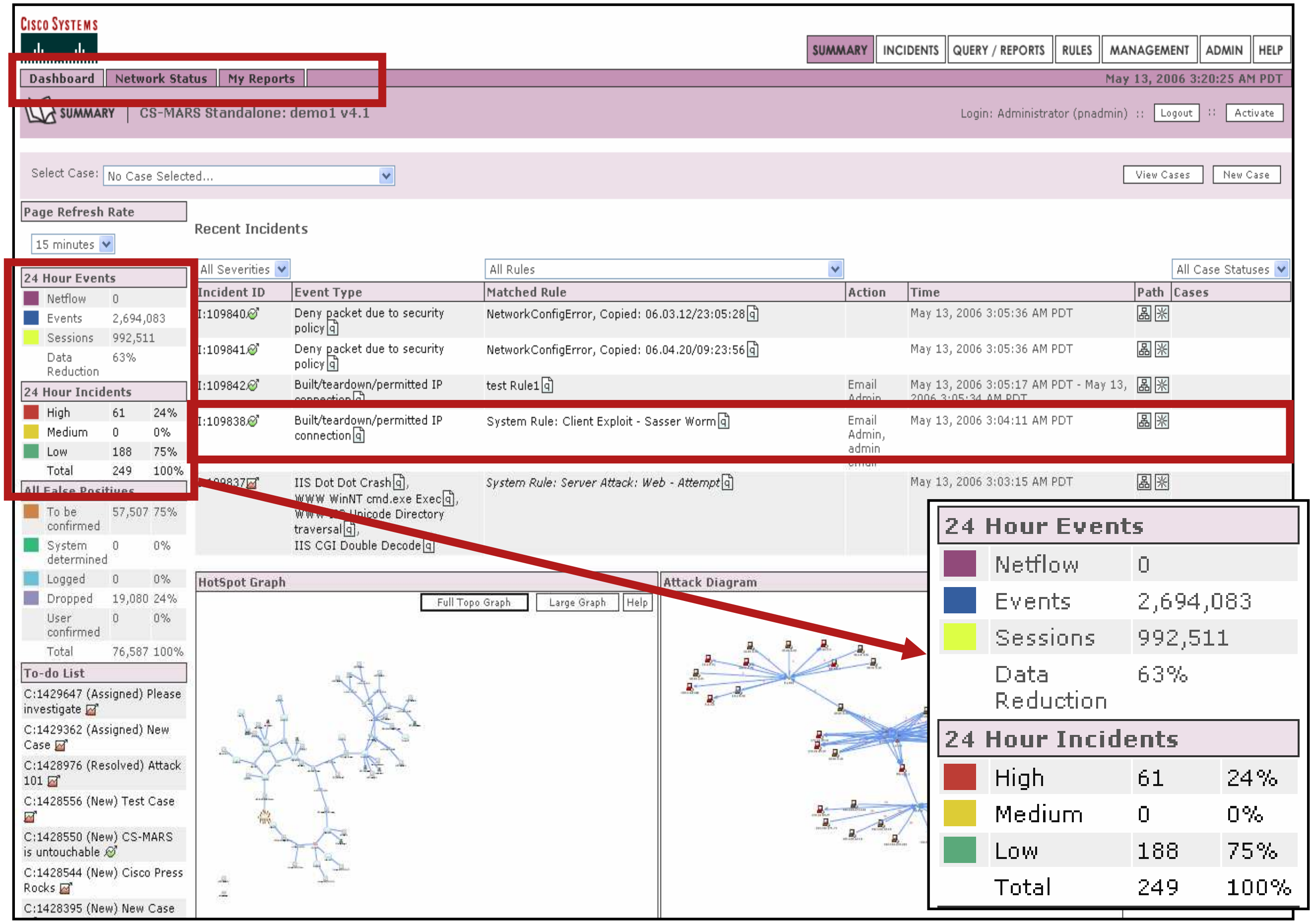
14 Events
(Each Word = 1 Event)

1 Incident
(The Whole Story)

- Events—raw messages sent to CS-MARS by the monitoring/ reporting devices
- Sessions—events that are correlated by the CS-MARS across NAT boundaries
- Incidents—identification of sessions to correlation rules

© 2007 Cisco Systems, Inc. All rights reserved.

Command and Control:
Critical Data Reduction



May 13, 2006 3:20:25 AM PDT

SUMMARY | CS-MARS Standalone: demo1 v4.1

Login: Administrator (pnadmin) :: Logout :: Activate

Select Case: No Case Selected...

Page Refresh Rate

15 minutes

24 Hour Events

🟪	Netflow	0
🟦	Events	2,694,083
🟨	Sessions	992,511
	Data Reduction	63%

24 Hour Incidents

🟥	High	61	24%
🟨	Medium	0	0%
🟩	Low	188	75%
	Total	249	100%

All False Positives

🟧	To be confirmed	57,507	75%
🟩	System determined	0	0%
🟦	Logged	0	0%
🟪	Dropped	19,080	24%
	User confirmed	0	0%
	Total	76,587	100%

To-do List

C:1429647 (Assigned) Please investigate

C:1429362 (Assigned) New Case

C:1428976 (Resolved) Attack 101

C:1428556 (New) Test Case

C:1428550 (New) CS-MARS is untouchable

C:1428544 (New) Cisco Press Rocks

C:1428395 (New) New Case

Recent Incidents

All Severities | All Rules | All Case Statuses

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:109840	Deny packet due to security policy	NetworkConfigError, Copied: 06.03.12/23:05:28		May 13, 2006 3:05:36 AM PDT		
I:109841	Deny packet due to security policy	NetworkConfigError, Copied: 06.04.20/09:23:56		May 13, 2006 3:05:36 AM PDT		
I:109842	Built/teardown/permitted IP connection	test Rule1	Email Admin	May 13, 2006 3:05:17 AM PDT - May 13, 2006 3:05:34 AM PDT		
I:109838	Built/teardown/permitted IP connection	System Rule: Client Exploit - Sasser Worm	Email Admin, admin email	May 13, 2006 3:04:11 AM PDT		
I:109837	IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	*System Rule: Server Attack: Web - Attempt*		May 13, 2006 3:03:15 AM PDT		

HotSpot Graph

Attack Diagram

24 Hour Events

🟪	Netflow	0
🟦	Events	2,694,083
🟨	Sessions	992,511
	Data Reduction	63%

24 Hour Incidents

🟥	High	61	24%
🟨	Medium	0	0%
🟩	Low	188	75%
	Total	249	100%

Incident Dashboard
- Aggregate
- Correlate
- Summarize

2,694,083 Events

992,511 Sessions

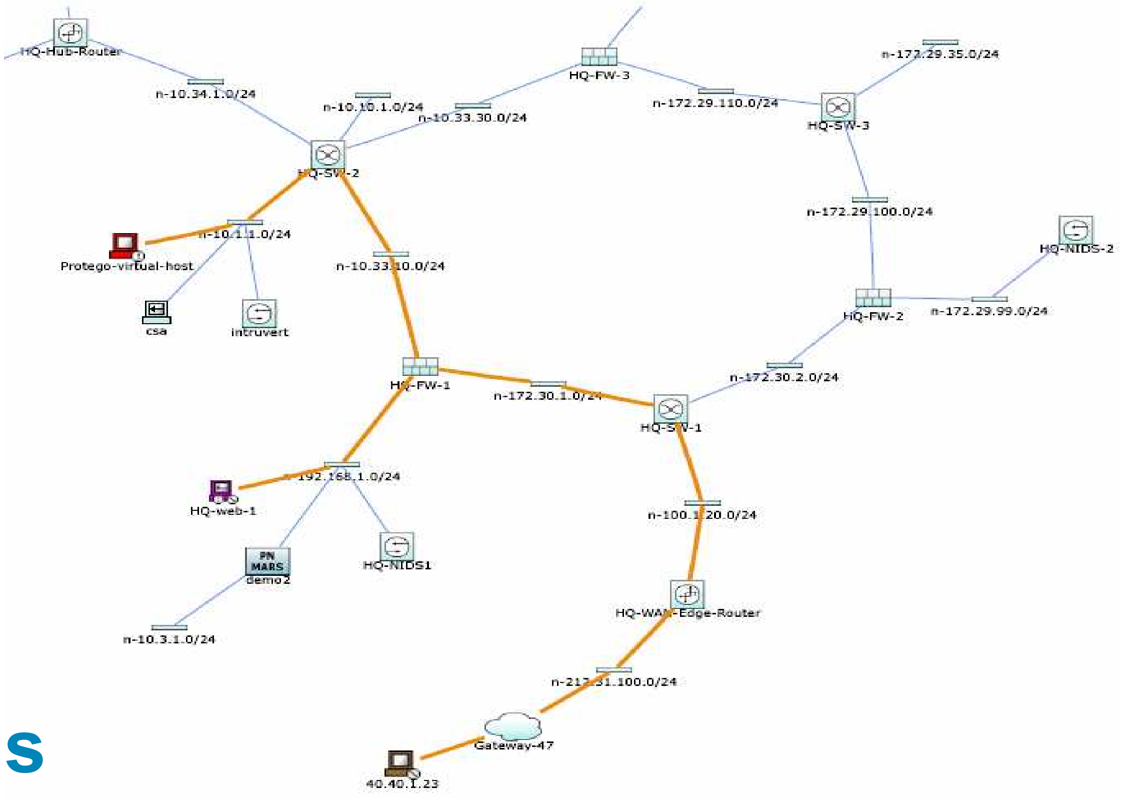
249 Incidents

61 High Severity Incidents

I Need to Clean My Network and Investigate Further

© 2007 Cisco Systems, Inc. All rights reserved.

Attack Topology Awareness



SureVector Analysis

Visible and accurate attack path

Drill-down, full incident and raw event details

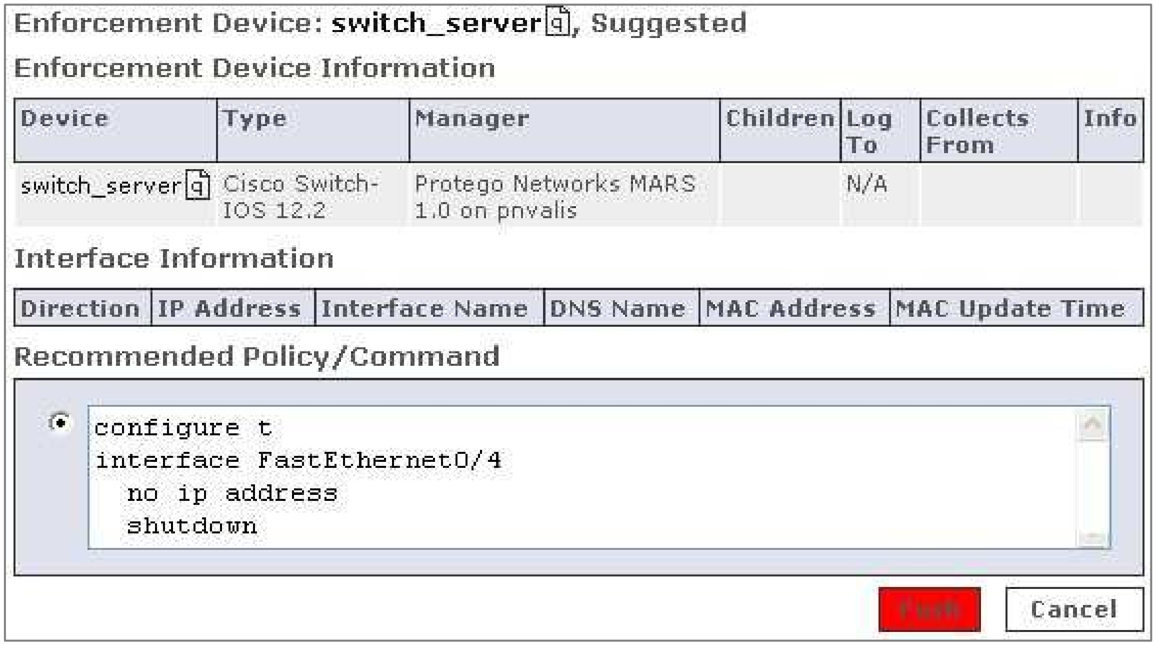
Pinpoint the true sources of anomalous and attack behavior

More complete and accurate story

© 2007 Cisco Systems, Inc. All rights reserved.

Command and Control: Attack Mitigation

- **Use control capabilities within your infrastructure**
  - **Layer 2/3 attack path is clearly visible**
  - **Mitigation enforcement devices are identified**
  - **Exact mitigation command is provided**



Enforcement Device: **switch_server**, Suggested

Enforcement Device Information

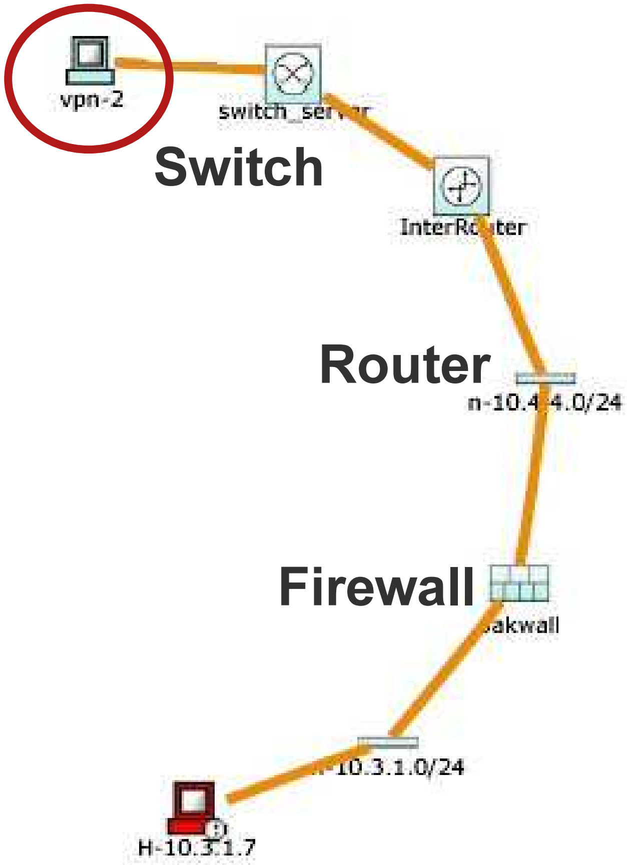
Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch-IOS 12.2	Protego Networks MARS 1.0 on pnvalis		N/A		

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time

Recommended Policy/Command

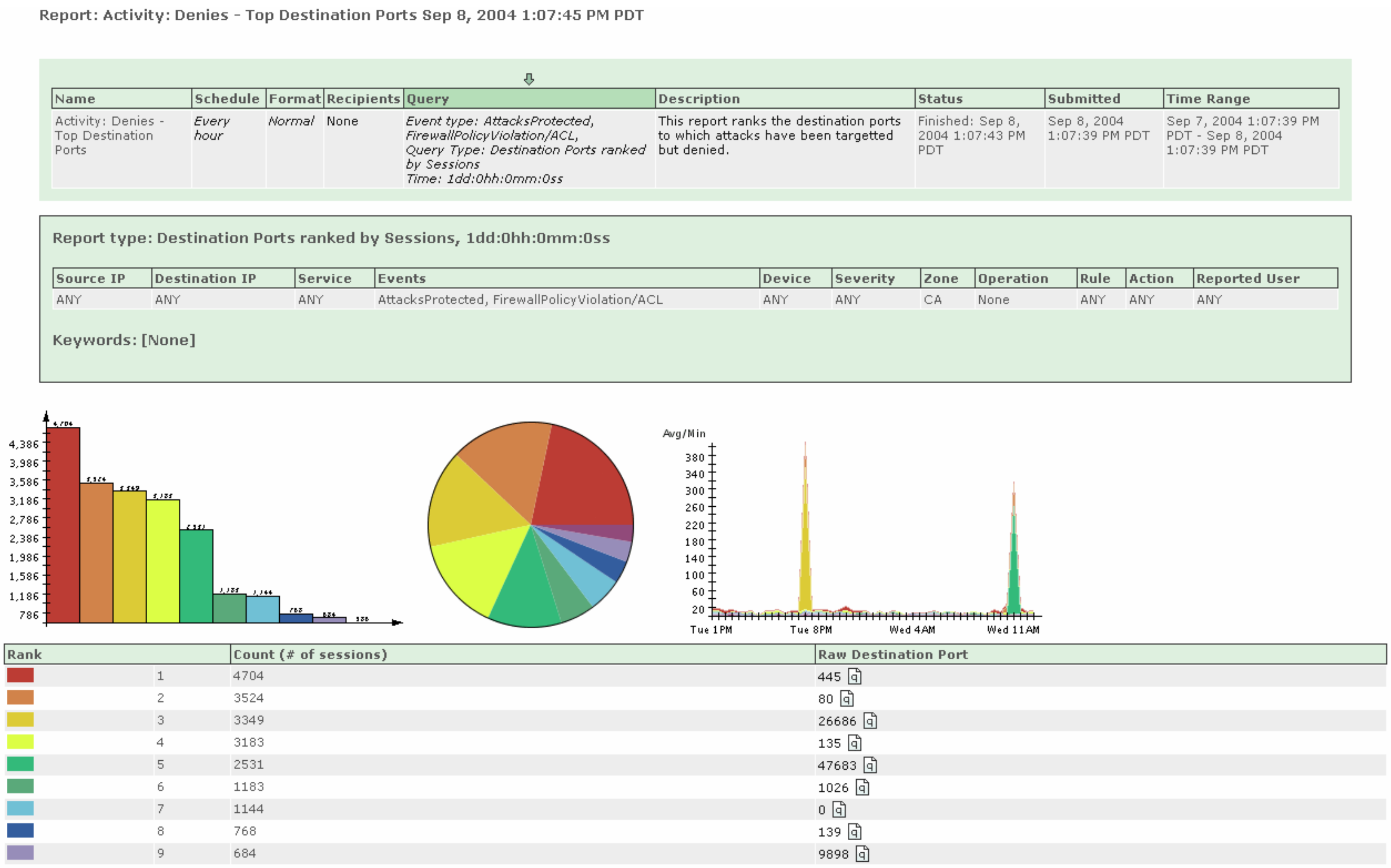
●
```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```



© 2007 Cisco Systems, Inc. All rights reserved.

Compliance Reports

Popular Reports With Customization and Distribution Options
Queries Saved as Rules or Reports—Intuitive Framework



Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

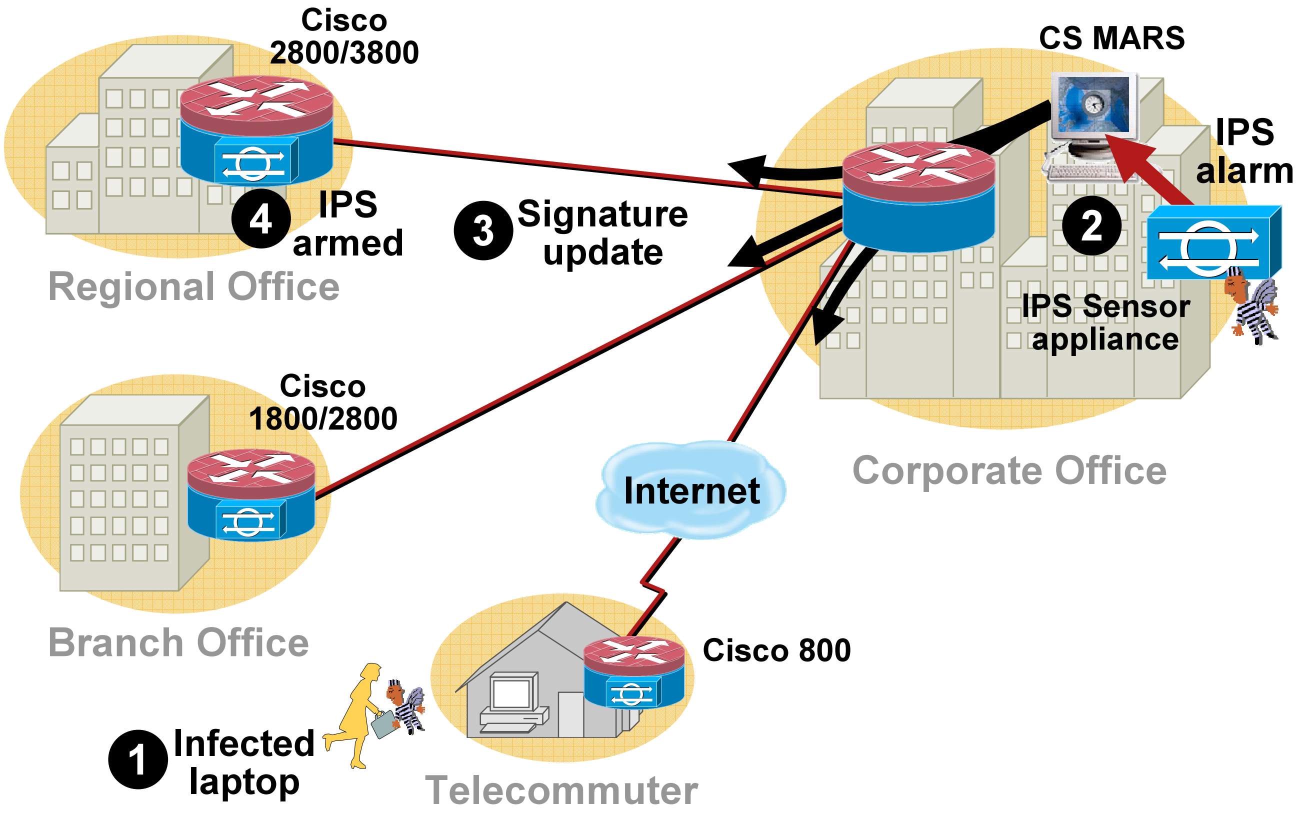
Keywords: [None]

Rank		Count (# of sessions)	Raw Destination Port
🟥	1	4704	445
🟧	2	3524	80
🟨	3	3349	26686
🟨	4	3183	135
🟩	5	2531	47683
🟩	6	1183	1026
🟦	7	1144	0
🟦	8	768	139
🟪	9	684	9898

© 2007 Cisco Systems, Inc. All rights reserved.

MARS in Action:

Distributed Threat Mitigation with IPS



1. Infected telecommuter connects to the corporate network
2. Virus sets off IPS alarm on the sensor appliance at corporate office
3. CS MARS distributes signatures to all security routers
4. Armed routers protect all remote sites

Benefits:

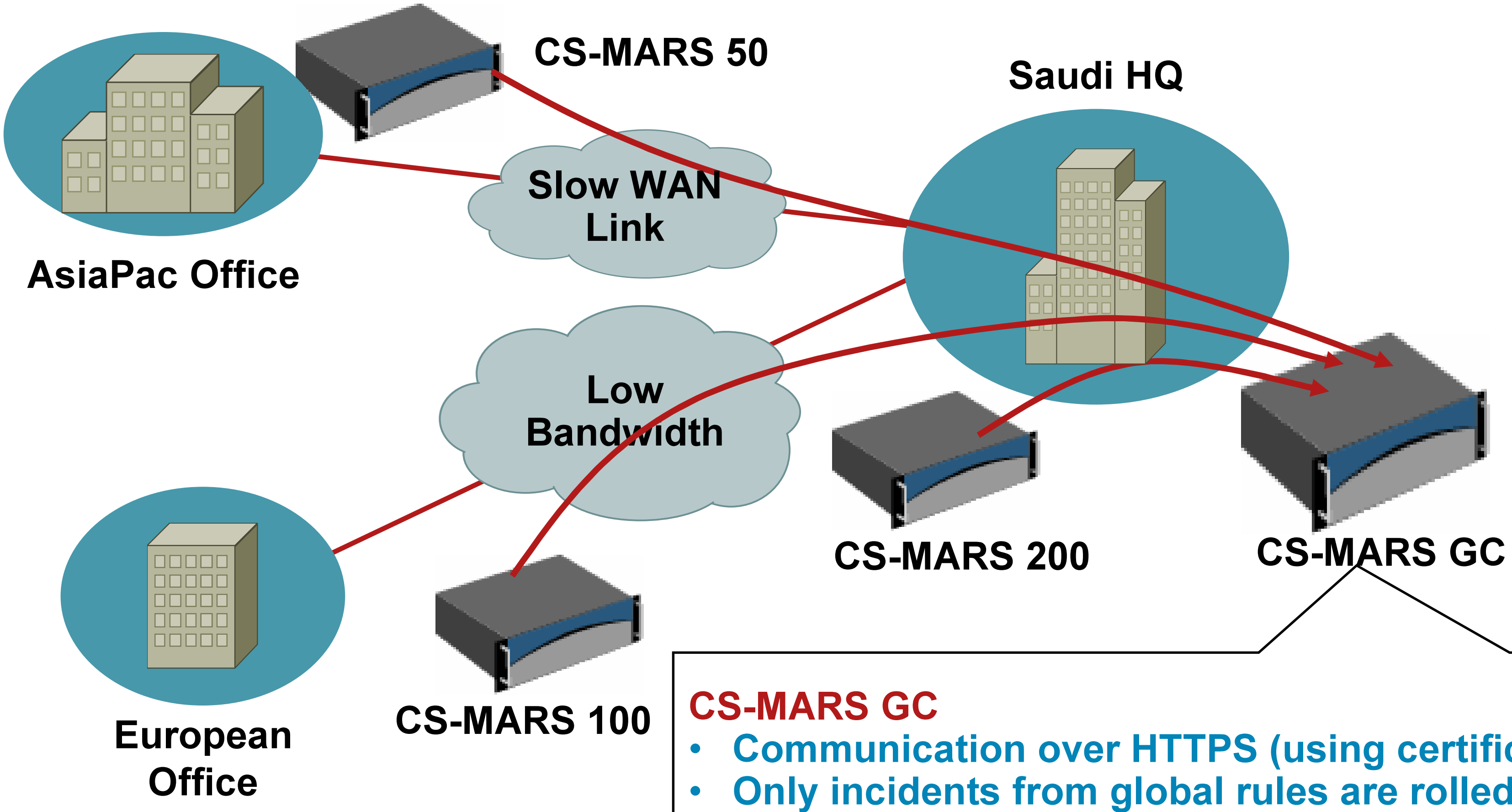
- Automating mitigation reduces administrative costs
- Dropping malicious traffic near source preserves WAN bandwidth & performance
- Adapting to attacks at branch routers uses security resources efficiently

Agenda

- Security Management Challenges
- Overview on Cisco MARS
- MARS in Action

© 2007 Cisco Systems, Inc. All rights reserved.

CS-MARS Deployment

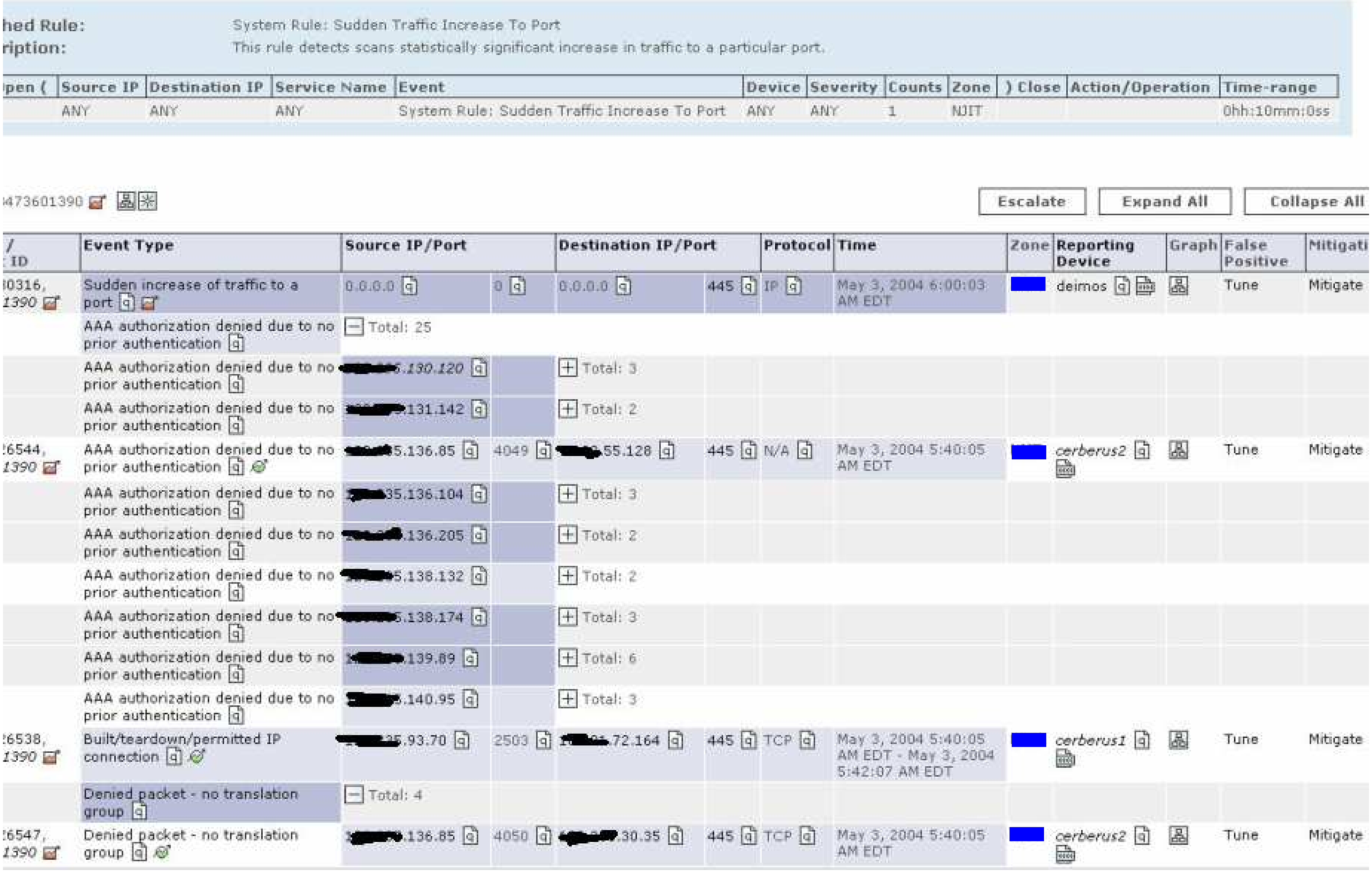


CS-MARS GC

- Communication over HTTPS (using certificates)
- Only incidents from global rules are rolled up
- GC can distribute updates, rules, report templates, access rules, and queries across LC

© 2007 Cisco Systems, Inc. All rights reserved.

Incident that Pops Up in the Dashboard



hed Rule: System Rule: Sudden Traffic Increase To Port

ription: This rule detects scans statistically significant increase in traffic to a particular port.

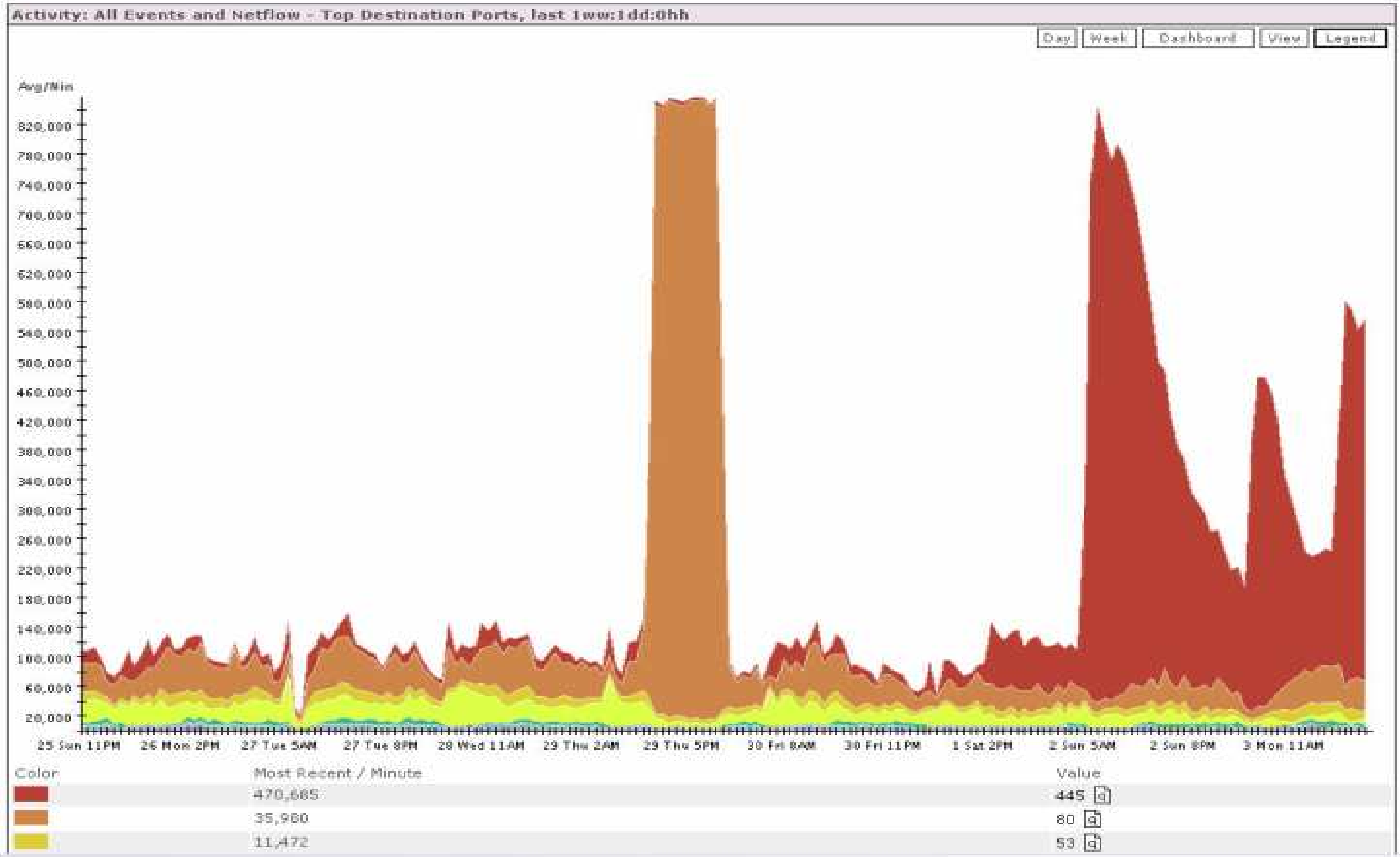
pen (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
	ANY	ANY	ANY	System Rule: Sudden Traffic Increase To Port	ANY	ANY	1	NJIT			0hh:10mm:0ss

473601390

Escalate | Expand All | Collapse All

/ ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Device	Graph	False Positive	Mitigati
0316, 1390	Sudden increase of traffic to a port	0.0.0.0	0	0.0.0.0	445	IP	May 3, 2004 6:00:03 AM EDT	🟦	deimos		Tune	Mitigate
	AAA authorization denied due to no prior authentication	⊟ Total: 25										
	AAA authorization denied due to no prior authentication	[redacted]5.130.120		⊞ Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].131.142		⊞ Total: 2								
6544, 1390	AAA authorization denied due to no prior authentication	[redacted]5.136.85	4049	[redacted].55.128	445	N/A	May 3, 2004 5:40:05 AM EDT	🟦	cerberus2		Tune	Mitigate
	AAA authorization denied due to no prior authentication	[redacted]35.136.104		⊞ Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].136.205		⊞ Total: 2								
	AAA authorization denied due to no prior authentication	[redacted]5.138.132		⊞ Total: 2								
	AAA authorization denied due to no prior authentication	[redacted]5.138.174		⊞ Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].139.89		⊞ Total: 6								
	AAA authorization denied due to no prior authentication	[redacted].140.95		⊞ Total: 3								
6538, 1390	Built/teardown/permitted IP connection	[redacted]5.93.70	2503	[redacted].72.164	445	TCP	May 3, 2004 5:40:05 AM EDT - May 3, 2004 5:42:07 AM EDT	🟦	cerberus1		Tune	Mitigate
	Denied packet - no translation group	⊟ Total: 4										
6547, 1390	Denied packet - no translation group	[redacted].136.85	4050	[redacted].30.35	445	TCP	May 3, 2004 5:40:05 AM EDT	🟦	cerberus2		Tune	Mitigate

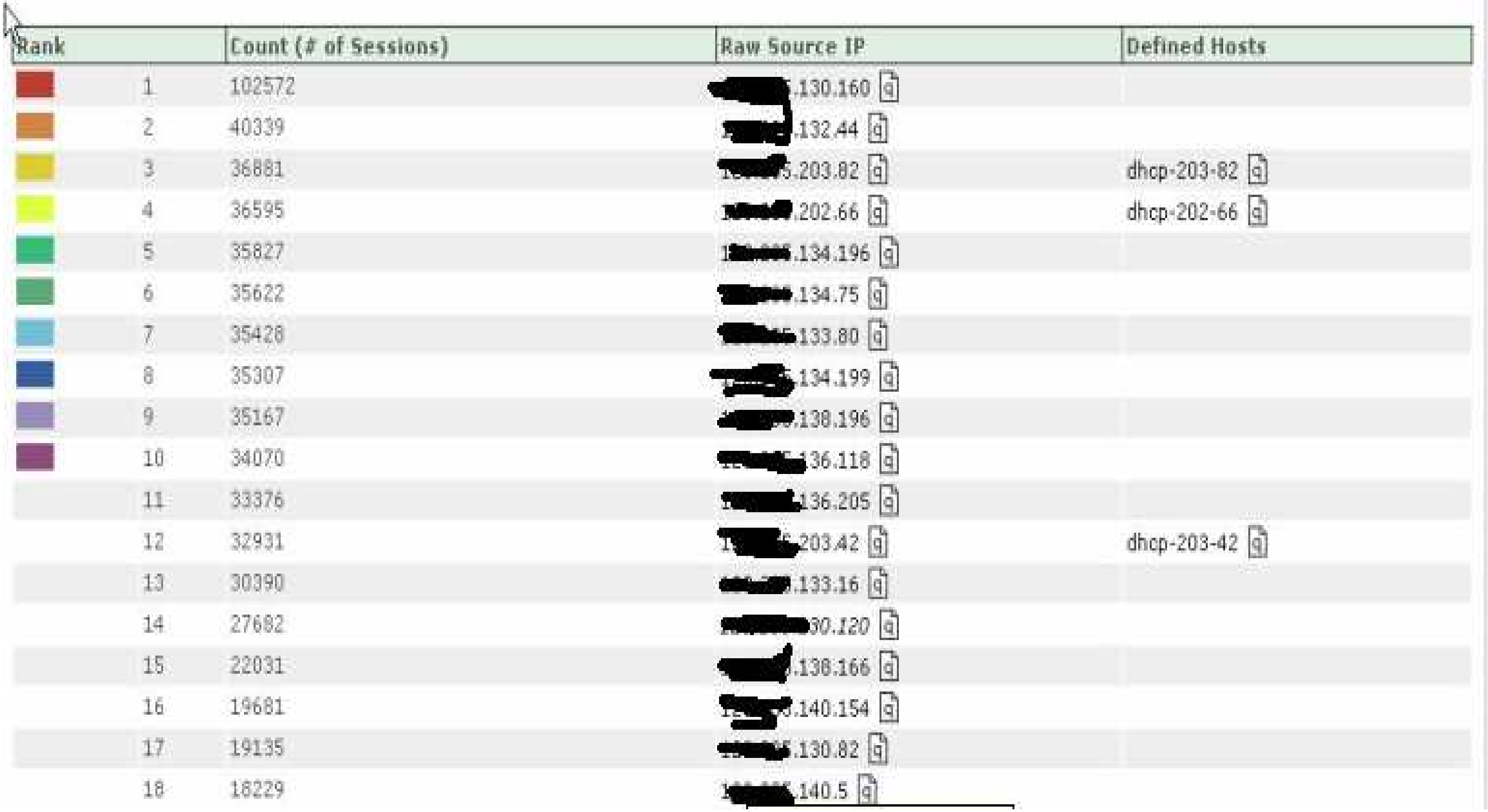
Graph Says It All



Activity: All Events and Netflow - Top Destination Ports, last 1ww:1dd:0hh

Color	Most Recent / Minute	Value
🟥	470,665	445
🟧	35,960	80
🟨	11,472	53

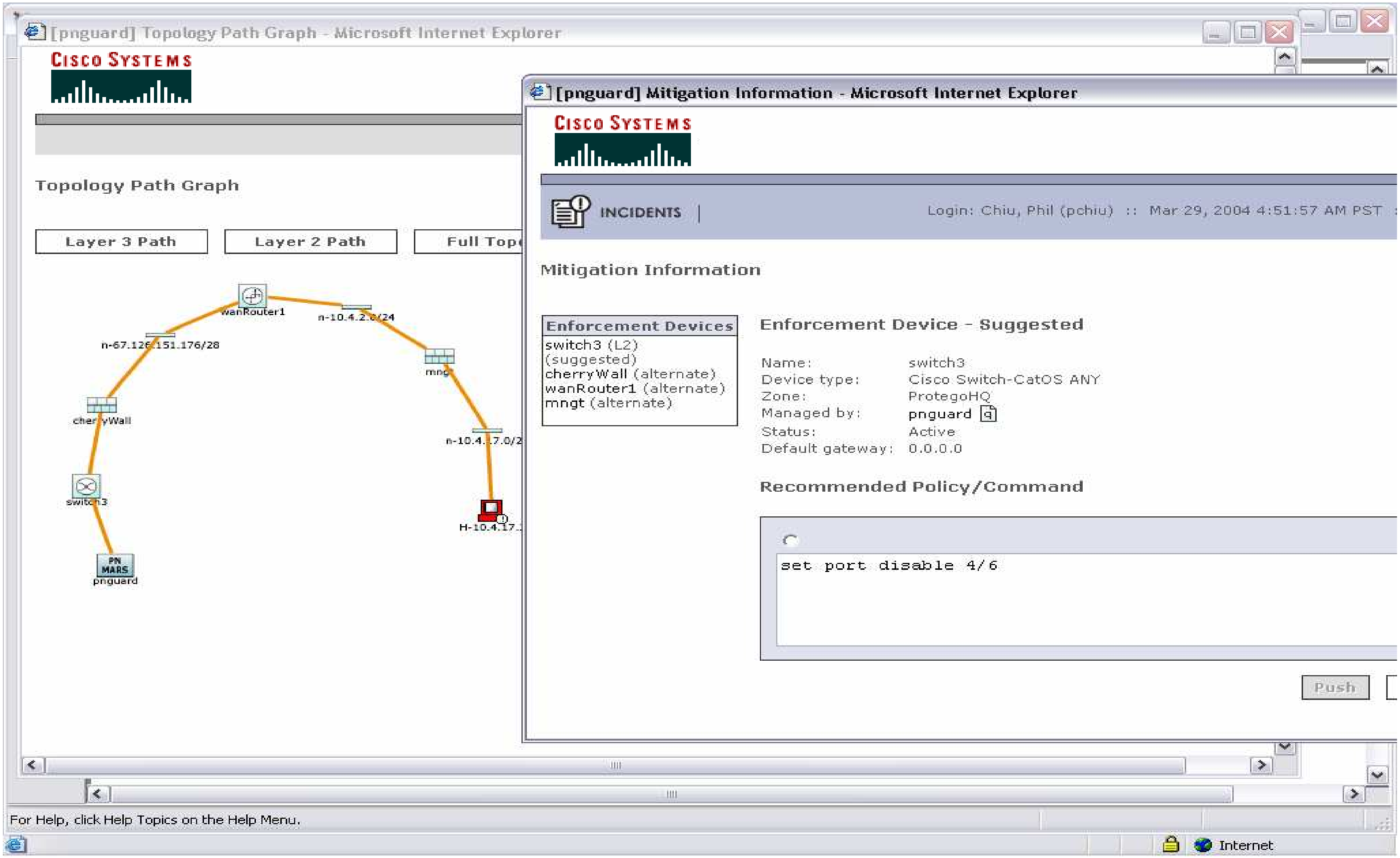
Example of Compromised Hosts



Rank	Count (# of Sessions)	Raw Source IP	Defined Hosts
🟥 1	102572	[redacted].130.160	
🟧 2	40339	[redacted].132.44	
🟨 3	36881	[redacted].203.82	dhcp-203-82
🟨 4	36595	[redacted].202.66	dhcp-202-66
🟩 5	35827	[redacted].134.196	
🟩 6	35622	[redacted].134.75	
🟦 7	35428	[redacted].133.80	
🟦 8	35307	[redacted].134.199	
🟪 9	35167	[redacted].138.196	
🟪 10	34070	[redacted]136.118	
11	33376	[redacted]136.205	
12	32931	[redacted]203.42	dhcp-203-42
13	30390	[redacted].133.16	
14	27682	[redacted]30.120	
15	22031	[redacted].138.166	
16	19681	[redacted].140.154	
17	19135	[redacted].130.82	
18	18229	[redacted].140.5	

© 2007 Cisco Systems, Inc. All rights reserved.

Attack Path with Layer 2 Mitigation



Login: Chiu, Phil (pchiu) :: Mar 29, 2004 4:51:57 AM PST

Mitigation Information

Enforcement Devices

switch3 (L2) (suggested)
cherryWall (alternate)
wanRouter1 (alternate)
mngt (alternate)

Enforcement Device - Suggested

Name:	switch3
Device type:	Cisco Switch-CatOS ANY
Zone:	ProtegoHQ
Managed by:	pnguard
Status:	Active
Default gateway:	0.0.0.0

Recommended Policy/Command

○

```
set port disable 4/6
```

© 2007 Cisco Systems, Inc. All rights reserved.