Cisco Networkers Solutions Forum 2008

Cisco Security : Responding to Emerging Threats

Timothy Snow

Consulting System Engineer

Asia Pacific

snow@cisco.com

Agenda

- What we’re up against
- Using the tools we have now to protect our assets

"You can’t predict when and where things will happen, so you’ll have to understand the how.“

John Chambers, CEO, Cisco Systems

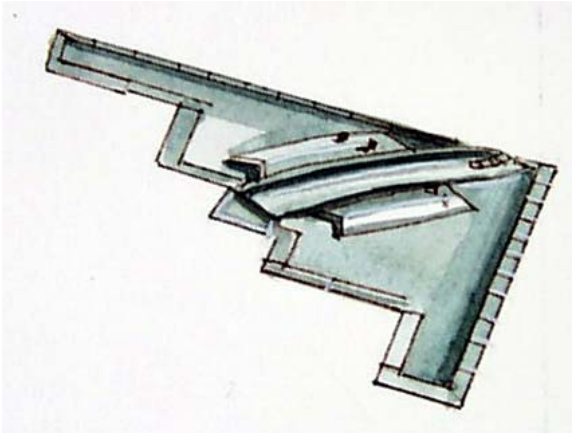
What happens when it stops working?

Changing Face of the Threat Landscape

Attackers Continue to Evolve

- **Change in *Purpose***
  - **Shift from fame to profit**
  - **Shift from attracting notice to developing an asset with economic value**

- **Change in *Expected Behavior***
  - **Less Noisy**
  - **More Sophisticated**
  - **More Variants, smaller scope of each**



Principles

1. Don’t Get Caught
   The first principle is the most important. It is no fun getting caught, prosecuted, and throw in jail.
2. Don’t work too hard
   Use the easiest attack/penetration vector available in the toolkit to achieve the job’s objective. (DOS, DLP)
3. Follow the money
   If there is no money in the crime then it is not worth the effort/risk.
4. If you cannot take out the target, move the attack to a coupled dependency of the target.
   Eg. Instead of attack a database server, take out the web front end, router, switch.

The most important tools we have.

Architecture, Cross-functional Teamwork & Open Communications Across the Enterprise.

Security is *not* a product.

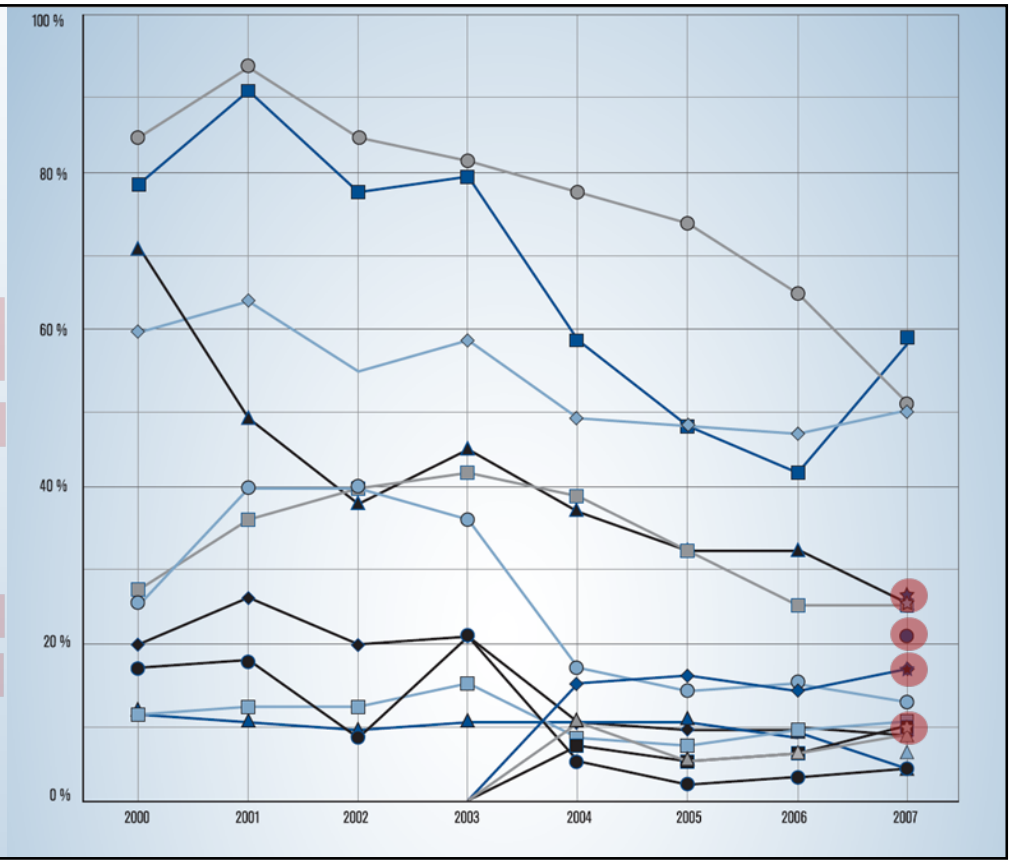
Security is *not* a box which can be bolted onto the network.

Security must be *designed into* the architecture at all 7 layers.

There are *no* 'silver bullets'; defense-in-depth is required.

The Evolving Security Challenge: Emergence of New Attack Types

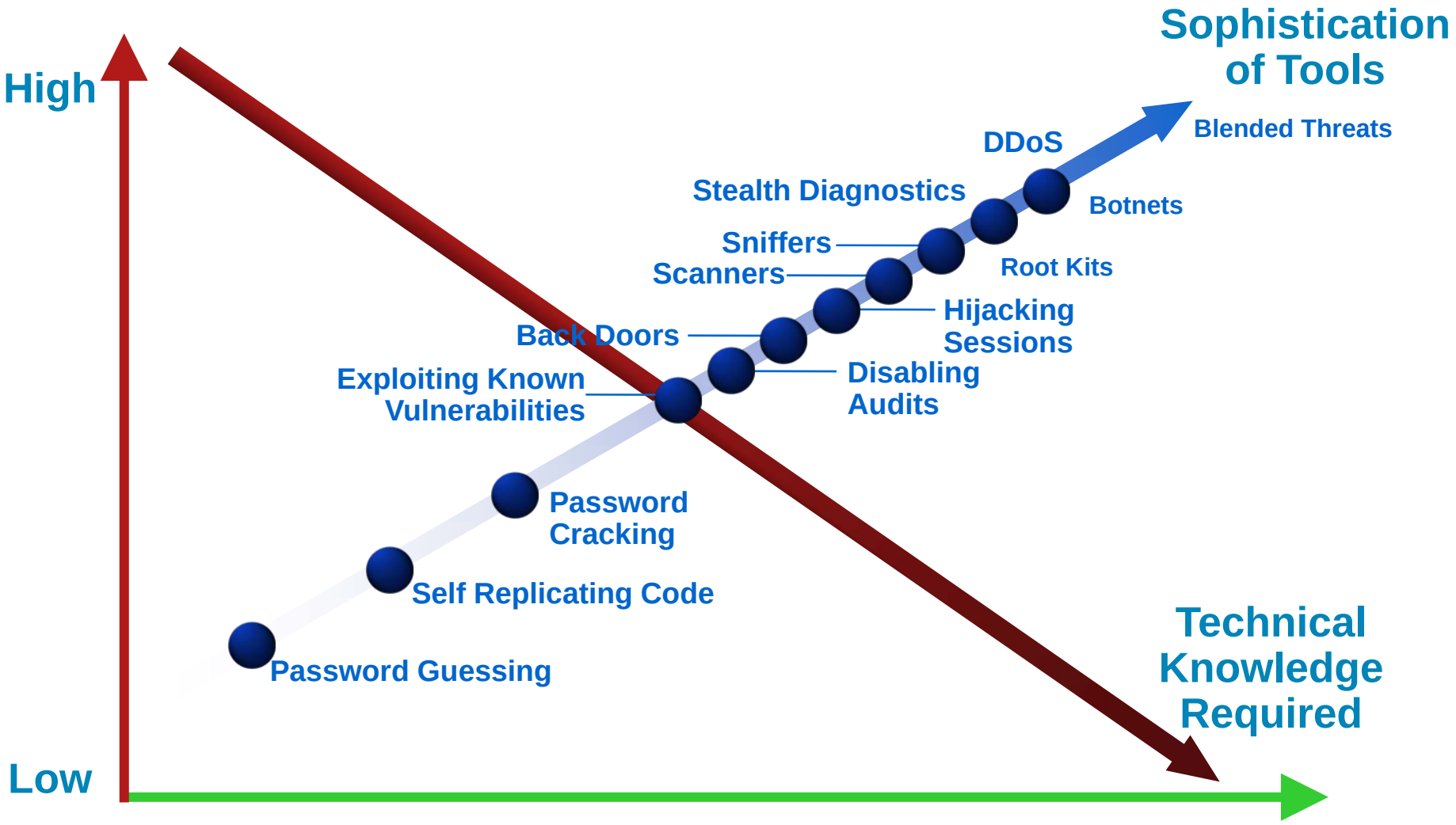
TYPE OF ATTACK	2007
Insider abuse of Net access	59%
Virus	52%
Laptop / mobile device theft	50%
Phishing where your organization was fraudulently represented as sender**	26%
Instant messaging misuse**	25%
Denial of service	25%
Unauthorized access to information	25%
Bots within the organization**	21%
Theft of customer / employee data**	17%
Abuse of wireless network*	17%
System penetration	13%



Source: 2007 CSI Survey

4 new attack types not in last years report

Evolution of Threats and Exploits



Sophisticated Hacking Tools Are Easily Accessible

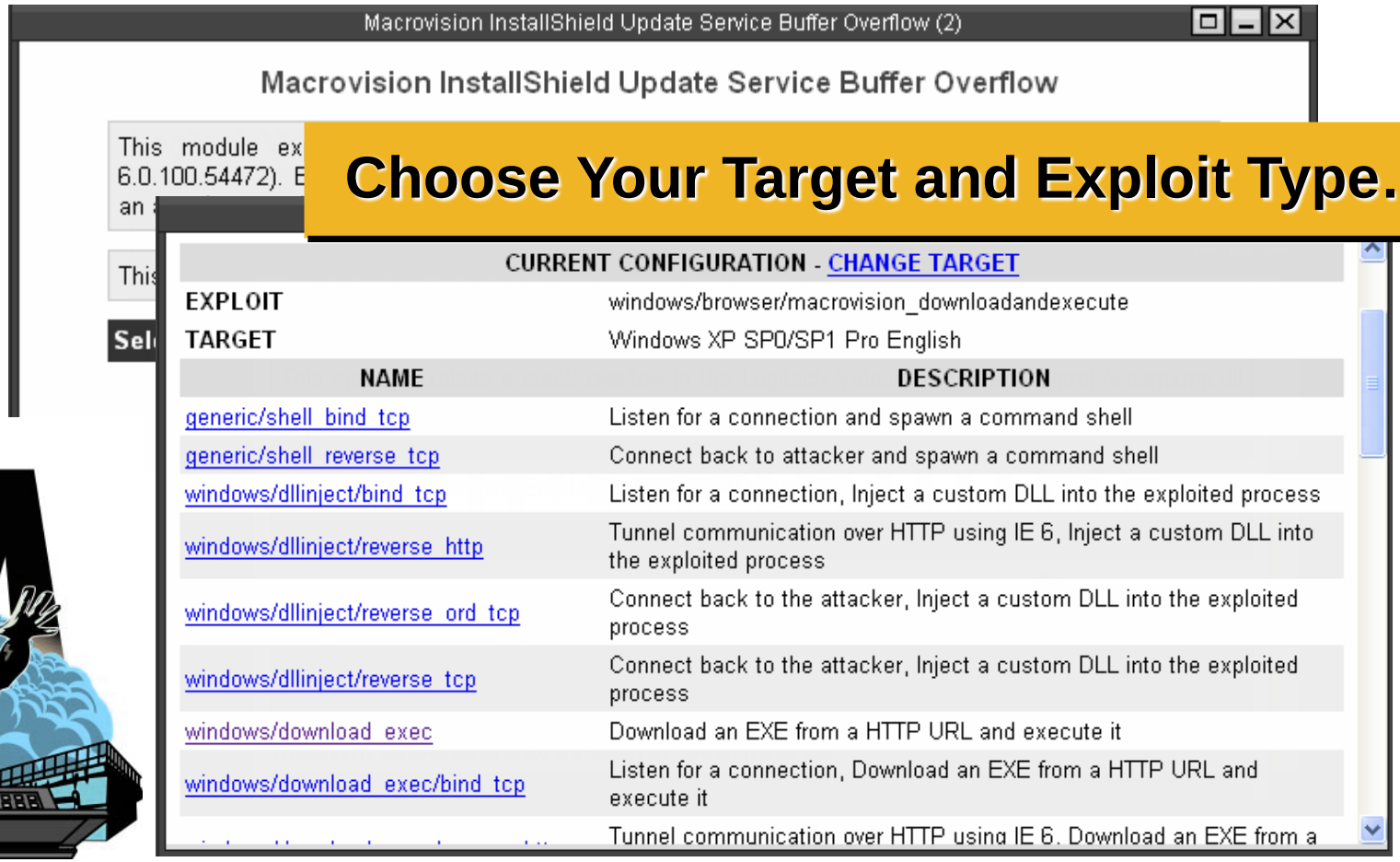
Austin, Texas, January 28th, 2008 -- The Metasploit Project announced today the **free**, world-wide availability of version 3.1 of their exploit development and attack framework. The latest version features a graphical user interface, full support for the Windows platform, and over 450 modules, including 265 remote exploits.

"…provides a wizard-based exploitation system"

"…includes a bristling arsenal of exploit modules that are sure to put a smile on the face of every information warrior"

metasploit framework

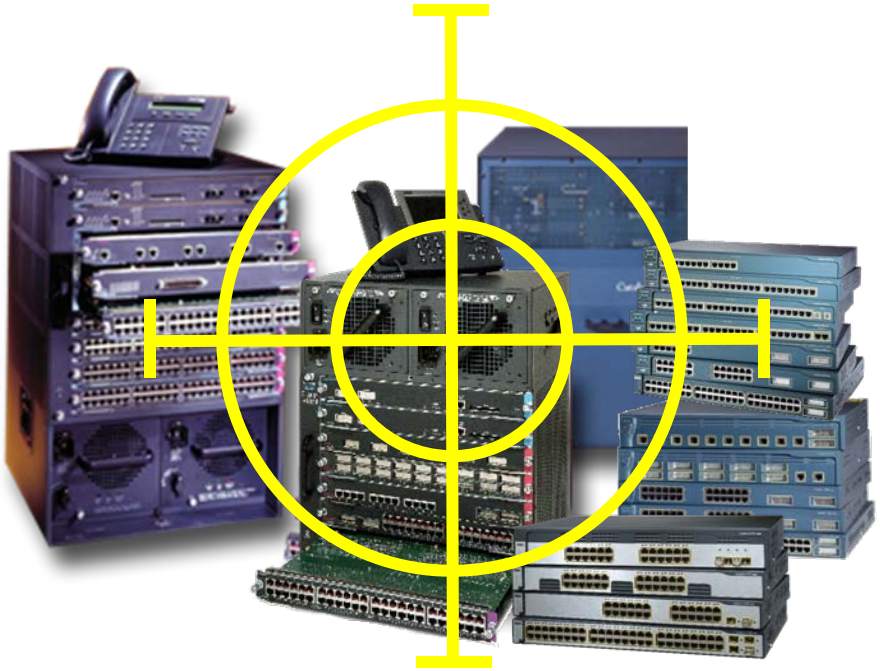
Sophisticated Hacking Tools Are Easy to Use too…



metasploit Framework

The Infrastructure has been targetted

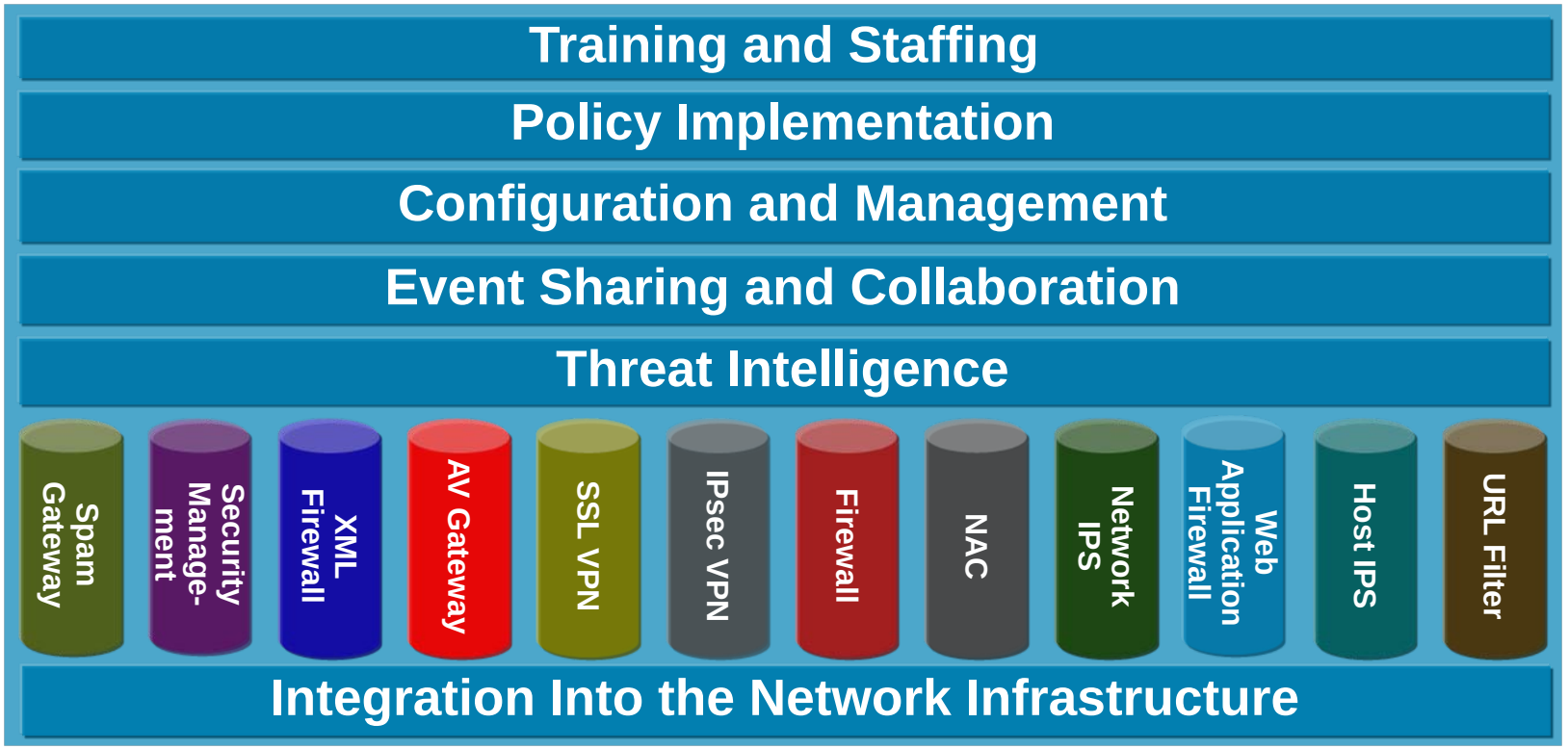
- Security Threats often target the infrastructure itself in order to slow down or halt operation of the device under attack
- Worms, viruses, denial-of-service attacks and flooding attacks are most common
- Your “arsenal” of tools:
  - Access Control Lists
  - Cisco Express Forwarding
  - Control-plane Policing
  - Scavenger-Class Queue (QOS)
  - Port Security
  - Broadcast Suppression
  - BPDU-Guard/Root-Guard
  - Network Admission Control



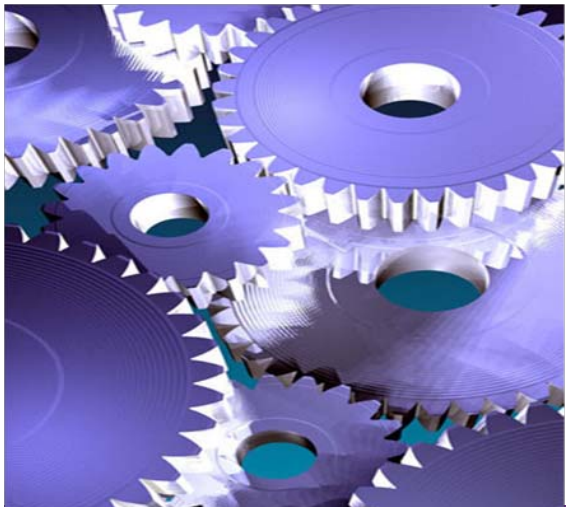
Cisco SDN 3.0: Cisco Self-Defending Network

The Challenges of Approaching Security Without an End-to-End, Systems Approach

The Advantages of a Systems Approach: Lower Cost, Higher Efficiency, Greater Effect

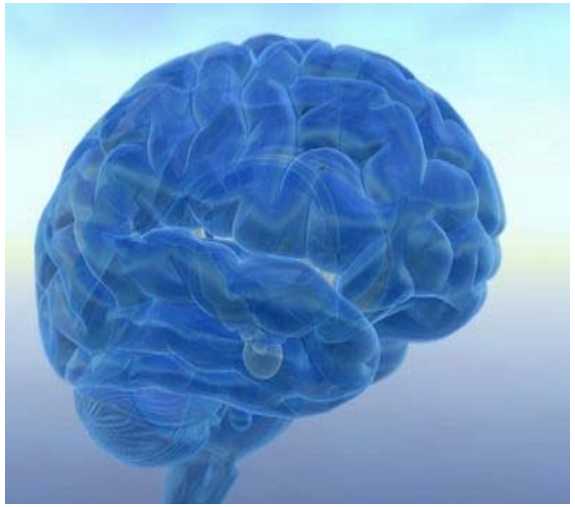


Cisco Self-Defending Network:
A Systems Approach to IT Security



Integrated

Enabling Every Element to Be a Point of Defense and Policy Enforcement



Adaptive

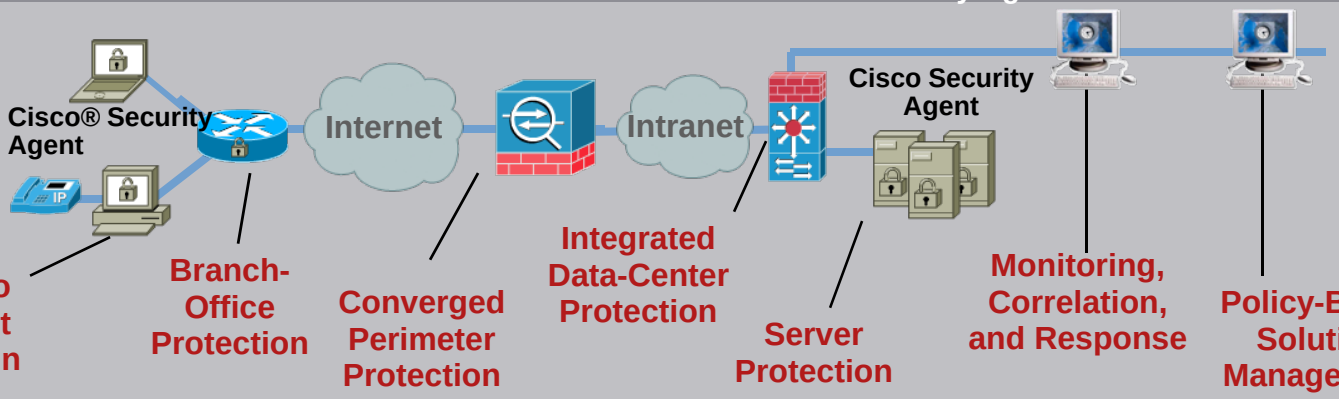
Proactive Security Technologies that Automatically Prevent Threats

Collaborative

Collaboration Among the Services and Devices Throughout the Network to Thwart Attacks

Mitigating Targeted Attacks and Malware
Self-Defending Network Applied

Cisco® Security Agent	Cisco Integrated Services Routers with IPS Cisco ASA 5500 with Content Security	Cisco ASA 5500 Adaptive Security Appliance with IPS and Cisco IronPort	Cisco Catalyst® Services Modules Cisco IPS 4200 Series Cisco ASA 5500 Series Cisco Security Agent	Cisco Security Management Suite



Branch

- Converged branch protection
- Local content scanning to mitigate malware introduction
- Network Admission Control to prevent malware and enforce policy
- Router-based IPS to protect local clients and preserve bandwidth

Campus

- Endpoint protection from spyware, botnets, spam, and Trojan horses
- High-capacity Internet-edge security
- Inbound, outbound, and intra-LAN protection and control
- Content security and Network Admission Control to mitigate malware propagation

Data Center

- High-capacity protection of servers and applications
- Application and protocol inspection to protect servers and systems
- Local server protection from targeted exploit attempts

New Cisco IPS 4270 Sensor

Relentless Performance for the Human Network

New!

- **Protecting media-rich environments**

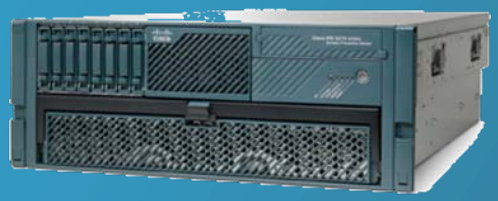
  4 Gbps of protection for Web content, video, data replication, and other media-rich environments

- **Protecting transactional environments**

  2 Gbps and 20,000 transactions per second of protection for e-Commerce, voice, IM, and other transactional environments

- **Protecting the data center**

  High-density interface support (16 GB interafaces and 10GB interfaces) that brings high-performance IPS to the data center



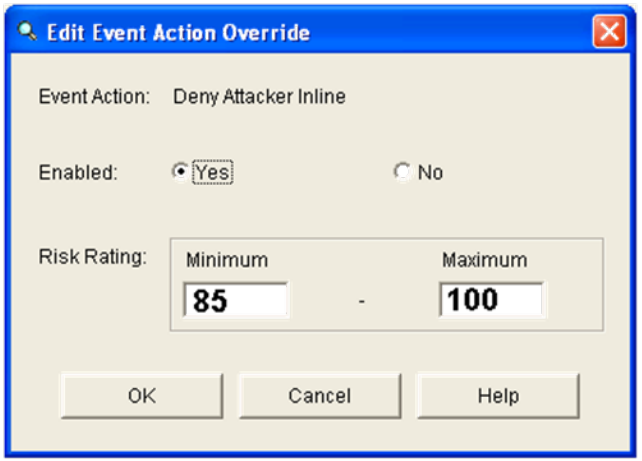
New High-Performance IPS from the IPS Market Leader

Source: Infonetics Q2CY07 Network IDS/IPS Market Share

Cisco IPS has been Number 1 market share holder for 4 consecutive quarters

Cisco IPS Risk Rating:
Risk-Management-based Security Policy

Event Severity		How urgent is the threat?
Signature Fidelity	+	How Prone to false positive?
Attack Relevancy	+	Is attack relevant to host being attacked?
Asset Value of Target	+	How critical is this destination host?



= Risk Rating

Drives Mitigation Policy

Customizable Risk Rating Thresholds :

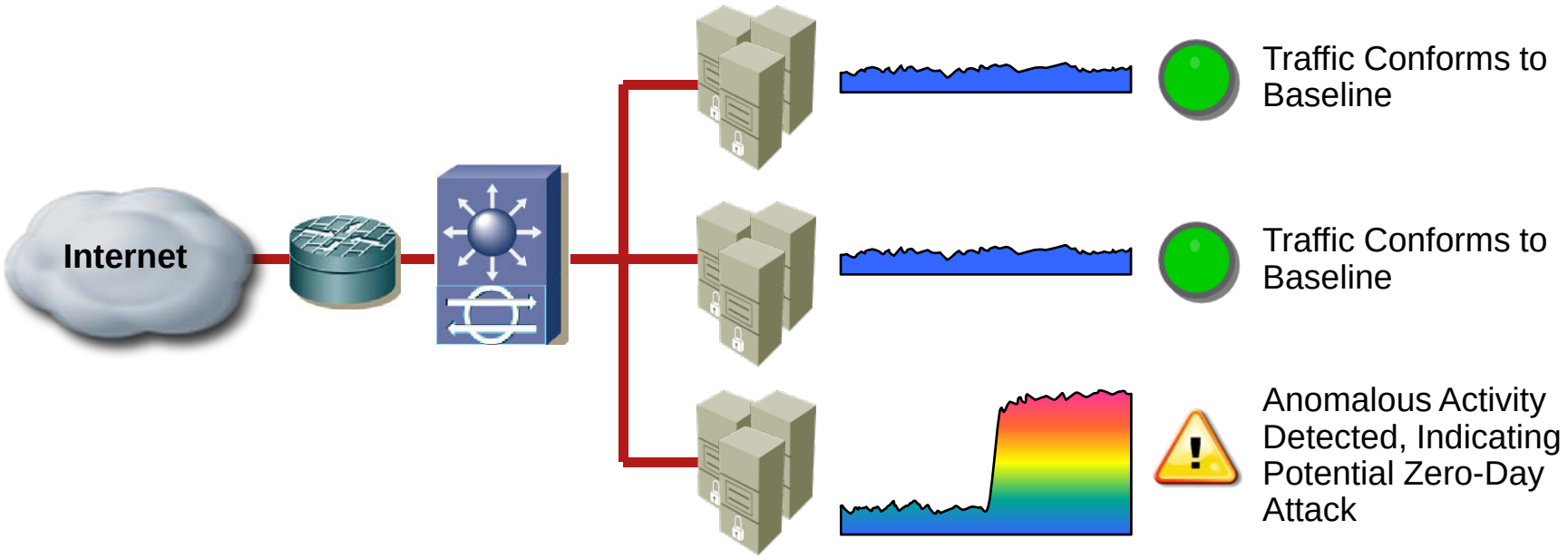
0 < RR < 35	Alarm
35 < RR < 85	Alarm & Log Packets
85 < RR < 100	Drop Packet

Result: Calibrated Risk Rating enables scalable management of sophisticated threat prevention technologies

Real-Time Anomaly Detection for Zero-Day Threats

New!

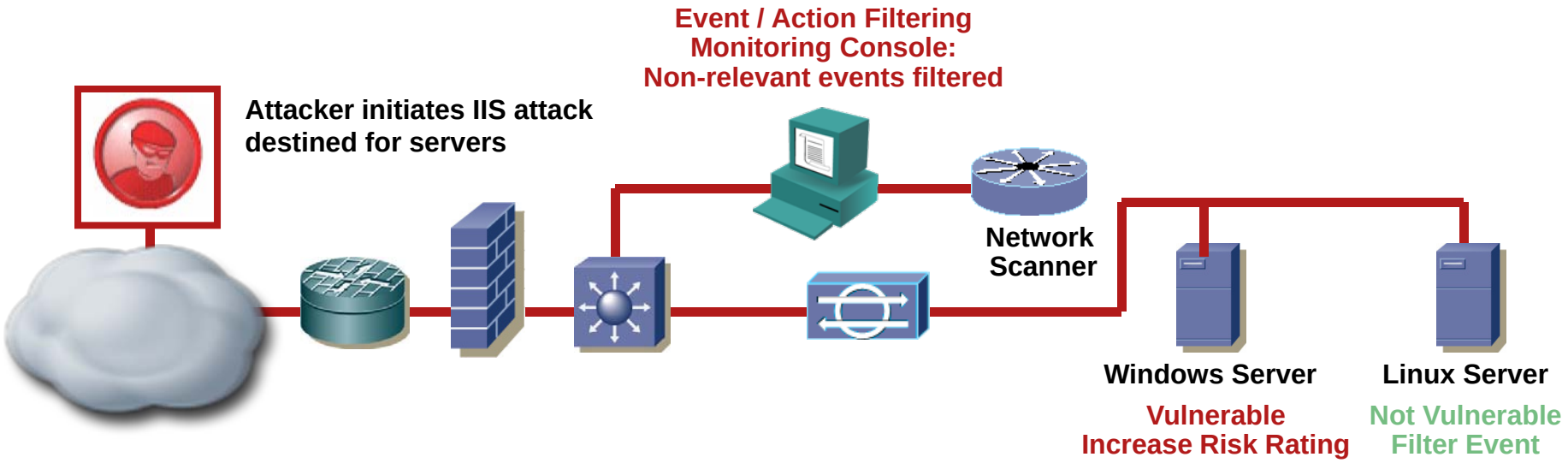
- Anomaly-detection algorithms to detect and stop zero-day threats
- Real-time learning of normal network behavior
- Automatic detection and policy-based protection from anomalous threats to the network
- **Result:** Protection against attacks for which there is no signature



New in IPS 6.0:
Endpoint Attack Relevance Visibility

New!

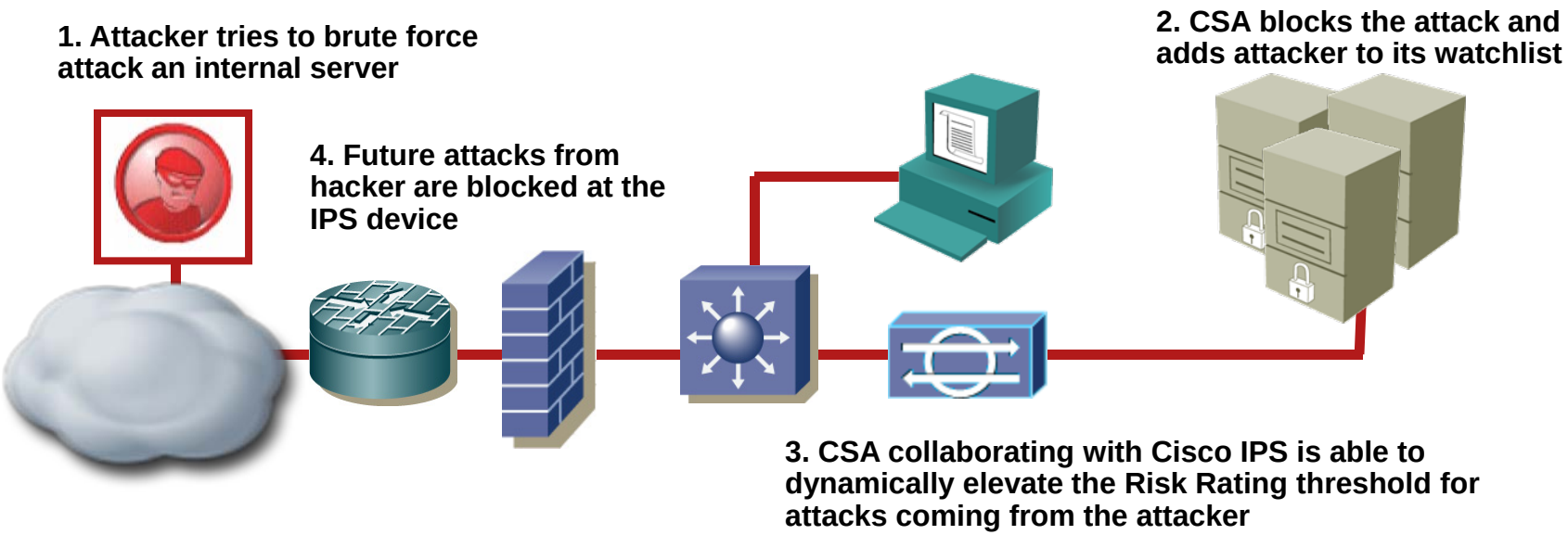
- Contextual information on attack target used to refine security response
- Contextual information gathered through:
  - Passive OS fingerprinting
  - Static OS mapping for exception handling
- Dynamic Risk Rating adjustment based on attack relevance
- **Result:** More appropriate and effective security response actions



New in IPS 6.0:
Visibility to Endpoint Trustworthiness – CSA Collaboration

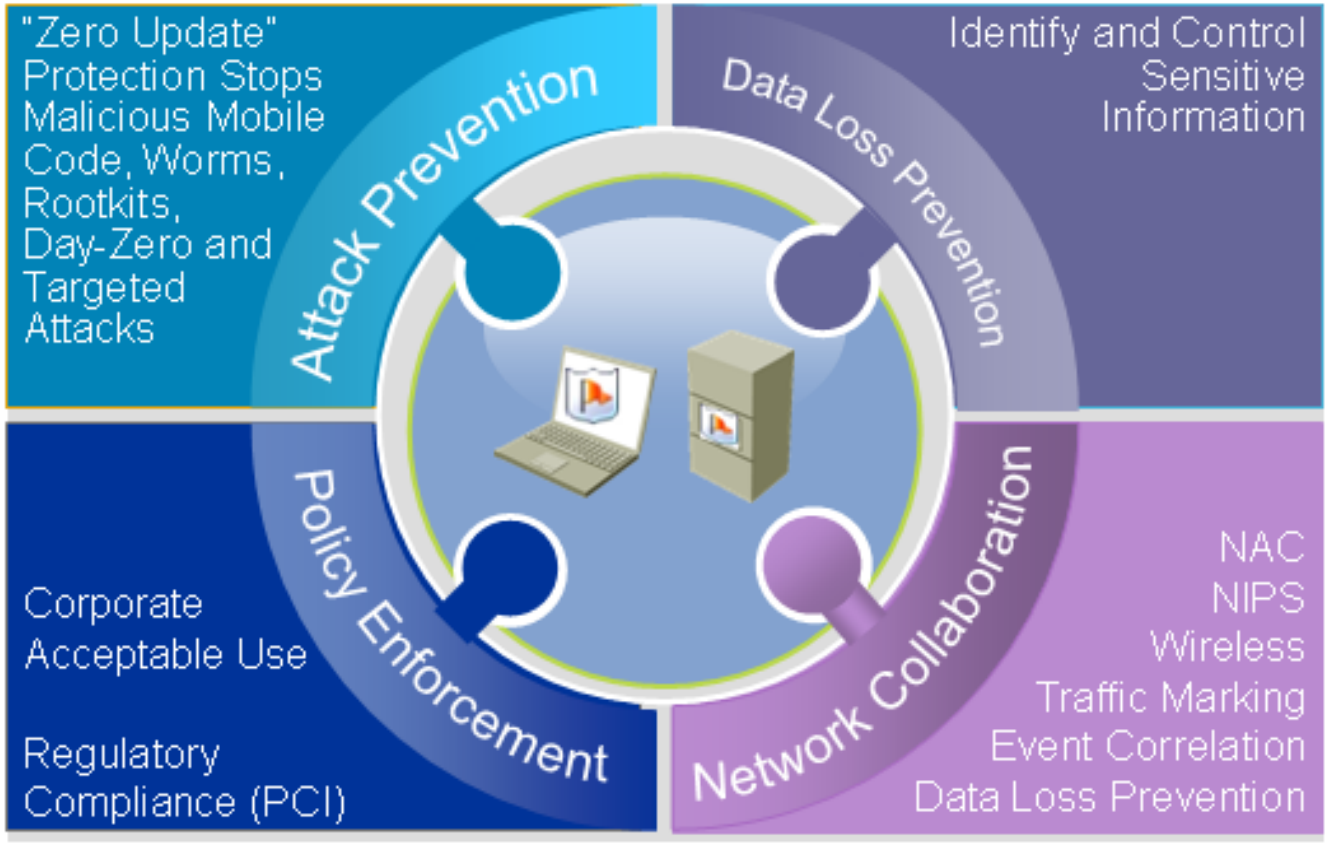
New!

- Cisco Security Agent (CSA) provides notion of suspicious hosts through CSA Watch List
- IPS Sensor risk sensitivity increased dynamically for suspicious hosts (risk rating increase)
- **Result:** Better manage risk from suspicious sources



Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



Laptop – Desktop Protection

Server Protection

POS/ IP ATM Protection

SINGLE INTEGRATED AGENT AND MANAGEMENT

Intrusion Prevention
"Zero Update" Track Record

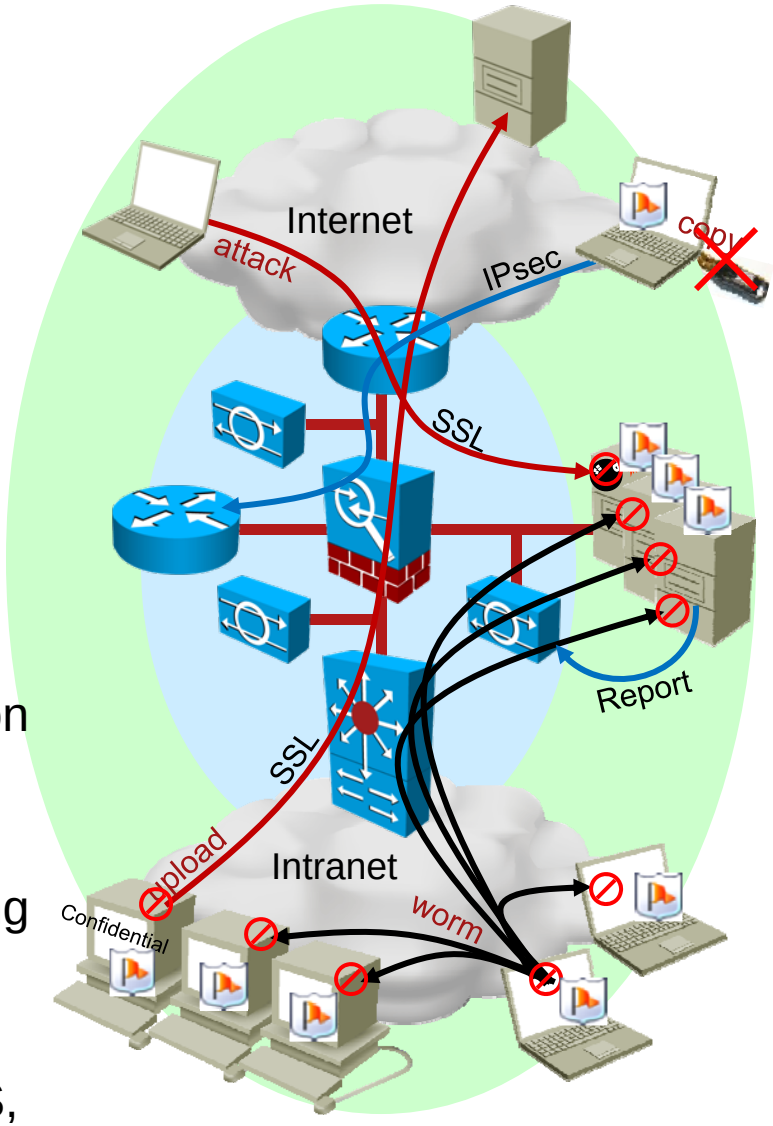
- Cisco Security Agent has a proven track record of stopping brand new exploits, botnets, targeted attacks, worms, and viruses over past 7 years:
  - 2001 – Code Red, Nimda (all 5 exploits), Pentagone (Gonner)
  - 2002 – Sircam, Debploit, SQL Snake, Bugbear,
  - 2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer
  - 2004 – MyDoom, Bagle, Sasser, JPEG browser exploit (MS04-028), RPC-DCOM exploit (MS03-039), Buffer Overflow in Workstation service (MS03-049)
  - 2005 – Internet Explorer Command Execution Vulnerability, Zotob
  - 2006 – USB Hacksaw, IE VML exploit, WMF, IE Textrange, RDS Dataspace
  - 2007 – Rinbot, Storm Trojan, Big Yellow, Word(MS07-014), MS ANI 0Day, MS DNS 0Day

No signatures or configuration updates required

Advanced Endpoint Security

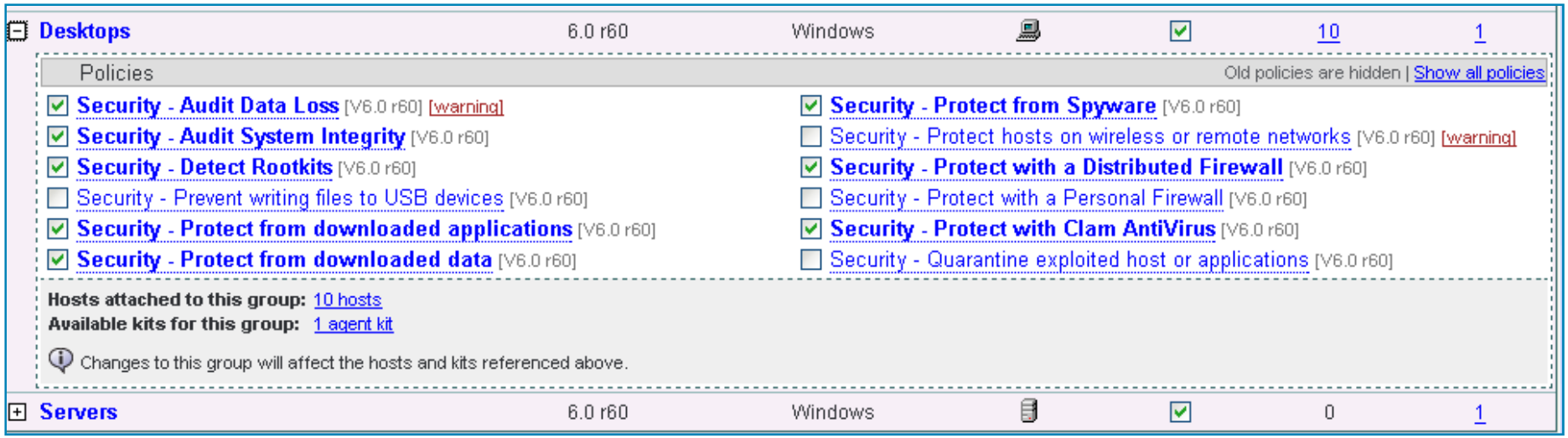
with Cisco Security Agent

- CSA extends network security solutions to end hosts
- Cisco Security Agent enhances security with:
  - **Zero Update protection** based on OS and application behavior
  - **Control of content** after decryption or before encryption (e.g. SSL, IPsec)
  - **Access control for I/O devices** based on process, network location and even file content (USB, IPhone, CDRW)
  - **Centralized management** and monitoring of events
  - **SDN Interaction** with other network solutions such as NAC, IPS, QoS, MARS, VOIP, etc



Host Security Page
Where you configure security protection

Host Security Page offers built-in security protection options: DLP, Firewall, Wireless



"Zero Update" Security policies includes policies to protect from spyware, bots, downloaded data, viruses, network attacks

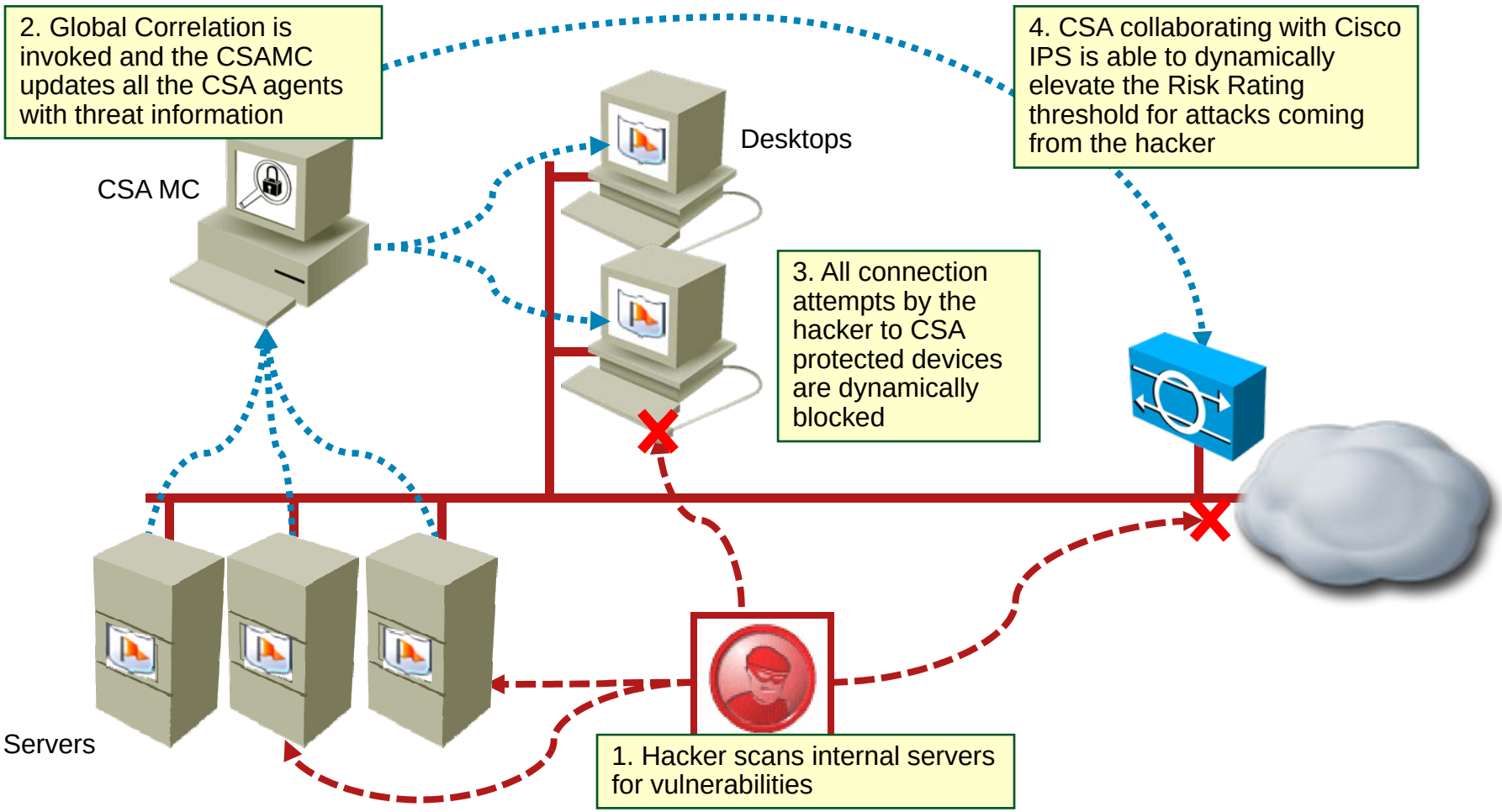
QOS Policy, Network/Firewall Integration

Intrusion Detection policies (Host IPS) detects rootkits, unauthorized configuration changes, keyloggers, sniffers

Acceptable Use policies control wireless security, personal firewall, USB device control, and data loss

Inform NIPS of Hostile Hosts

Configured via CSAMC Advanced GUI option

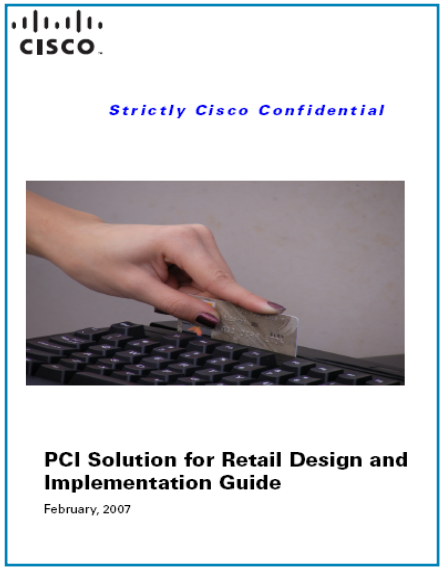


Regulatory Compliance
Benefits for PCI Compliance

- Provides compliance solution for 9 out of 12 PCI requirements
- Predefined PCI Policies offer ease of management & audit

  26 Rule Modules, 150 rules
- Validated by Cybertrust (official PCI auditor)
- Runs on Servers, Point-Of-Sale/IP ATM terminals, desktops and laptops
- CSA can be customized for other compliance mandates

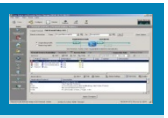
cybertrust



http://www.cisco.com/go/compiance

Management and Instrumentation Overview

Cisco® Security Device Manager



- Quickest way to setup a device
- Wizards to configure firewall, IPS, VPN, QoS, and wireless
- Ships with device

Cisco Security Manager

- New solution for configuring routers, appliances, switches
- New user-centered design
- New levels of scalability

Cisco Security MARS

- Solution for monitoring and mitigation
- Uses control capabilities within infrastructure to eliminate attacks
- Visualizes attack paths

Cisco IOS® Instrumentation

- Industry leadership in instrumentation
- Feeds into Cisco Security MARS
- Partitioned access for network and security operations teams

Operational Control and Monitoring: Total Security System Management

Reduced complexity for more effective risk analysis and operational control

Cisco Security Manager Benefits Control and Visibility

Efficient Day-to-Day Operation and Fast Response

- Role Based enables NetOps and SecOps to work together
- Strong sharing and inheritance built in (global policies)
- Enforces corporate rules and provides best-practice guidelines (Compliance – SOX, Hippa, GLBA)

Integrated Service-Based Approach

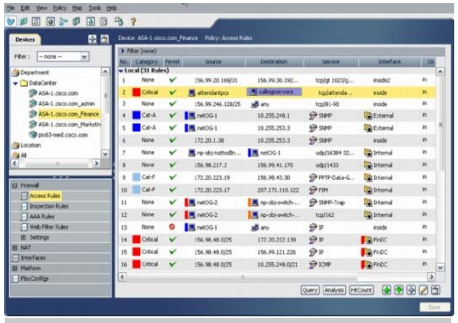
- Firewall, VPN, and IPS management all natively on a single interface

Collaboration between Configuration and Monitoring

- Transparent device manager cross-launch to access rich monitoring and troubleshooting tools; integration between Cisco® Security Manager and Cisco Security MARS

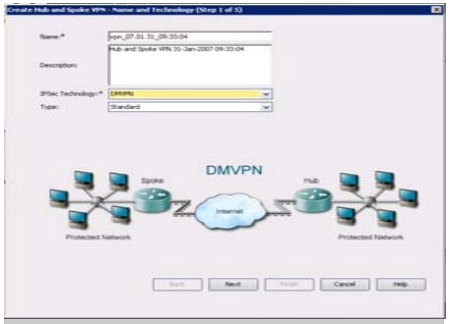
Cisco Security Manager

Integrated Security Configuration Management



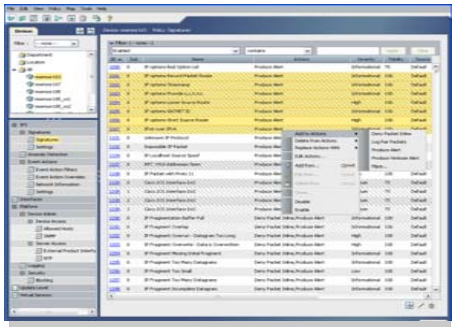
Firewall Management

- Support for Cisco® PIX® Firewall, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), and Cisco IOS® Software Routers
- Rich firewall rule definition: shared objects, rule grouping, and inheritance
- Powerful analysis tools: conflict detection, rule combiner, hit counts, …



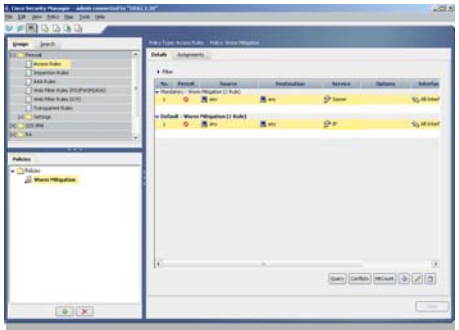
VPN Management

- Support for Cisco PIX Firewall, Cisco ASA, VPN services module (VPNSM), VPN shared port adapter (SPA), and Cisco IOS Software routers
- Support for wide array of VPN technolgies, such as DMVPN, Easy VPN, and SSL VPN
- VPN wizard for 3-step point-and-click VPN creation



IPS Management

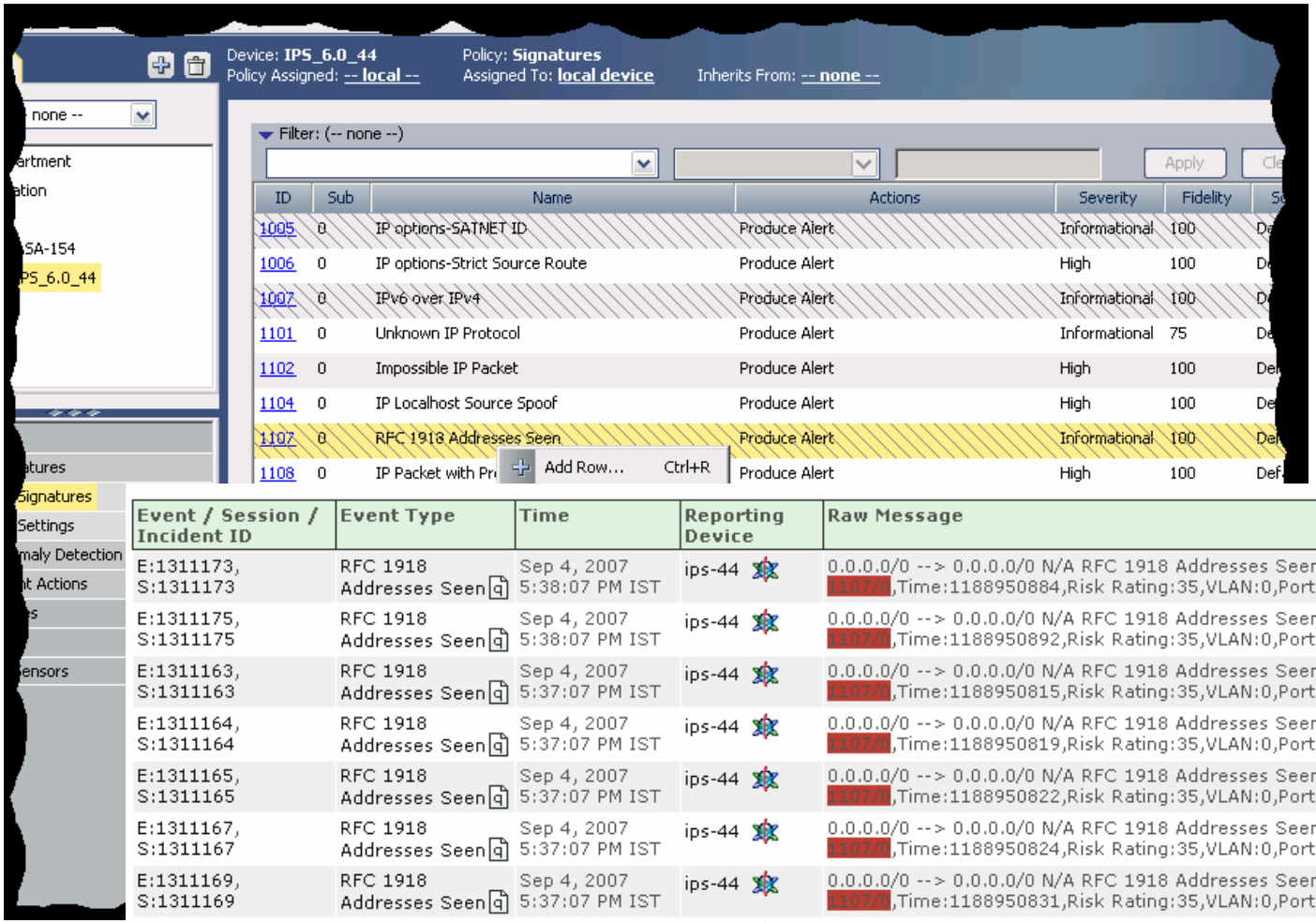
- Support for IPS sensors and Cisco IOS IPS
- Automatic policy-based IPS sensor software and signature updates
- Signature update wizard allowing easy review and editing prior to deployment



Productivity

- Unified security management for Cisco devices supporting firewall, VPN, and IPS
- Efficient management of up to 10000 devices per server
- Multiple views for task optimization
  - Device view
  - Policy view
  - Topology view
- Role-Based
- Workflow Audits
- Configuration/Activity Reports

CS-Manager to CS-MARS for IPS



Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:1311173, S:1311173	RFC 1918 Addresses Seen	Sep 4, 2007 5:38:07 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950884,Risk Rating:35,VLAN:0,Port List:,139	N/A	False Positive Tuning
E:1311175, S:1311175	RFC 1918 Addresses Seen	Sep 4, 2007 5:38:07 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950892,Risk Rating:35,VLAN:0,Port List:,138	N/A	False Positive Tuning
E:1311163, S:1311163	RFC 1918 Addresses Seen	Sep 4, 2007 5:37:07 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950815,Risk Rating:35,VLAN:0,Port List:,445	N/A	False Positive Tuning
E:1311164, S:1311164	RFC 1918 Addresses Seen	Sep 4, 2007 5:37:07 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950819,Risk Rating:35,VLAN:0,Port List:,137	N/A	False Positive Tuning
E:1311165, S:1311165	RFC 1918 Addresses Seen	Sep 4, 2007 5:37:07 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950822,Risk Rating:35,VLAN:0,Port List:,123	N/A	False Positive Tuning
E:1311167, S:1311167	RFC 1918 Addresses Seen	Sep 4, 2007 5:37:07 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950824,Risk Rating:35,VLAN:0,Port List:,42342	N/A	False Positive Tuning
E:1311169, S:1311169	RFC 1918 Addresses Seen	Sep 4, 2007 5:37:07 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950831,Risk Rating:35,VLAN:0,Port List:,42342	N/A	False Positive Tuning
E:1310982, S:1310982	RFC 1918 Addresses Seen	Sep 4, 2007 5:29:02 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:1188950330,Risk Rating:35,VLAN:0,Port List:,42342	N/A	False Positive Tuning
E:1310984, S:1310984	RFC 1918 Addresses Seen	Sep 4, 2007 5:29:02 PM IST	ips-44	0.0.0.0/0 --> 0.0.0.0/0 N/A RFC 1918 Addresses Seen,NR-1107[illegible],Time:118[illegible],Port List:,137	N/A	False Positive

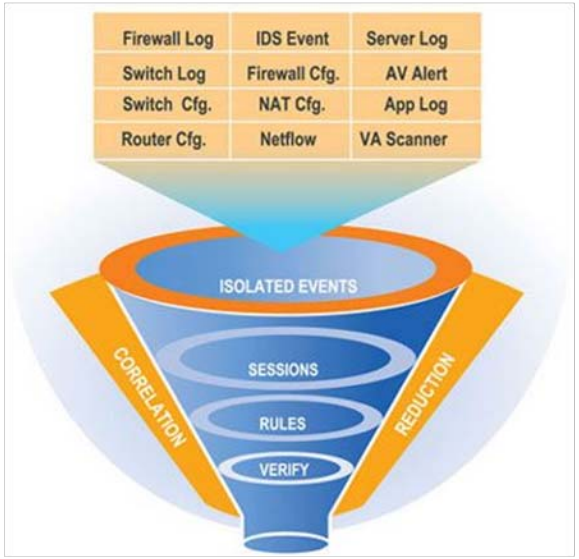
- CS-Manager - Ability to launch CS-MARS for Realtime or Historical Events based from device and signature (IE: When did this signature ever fire?)

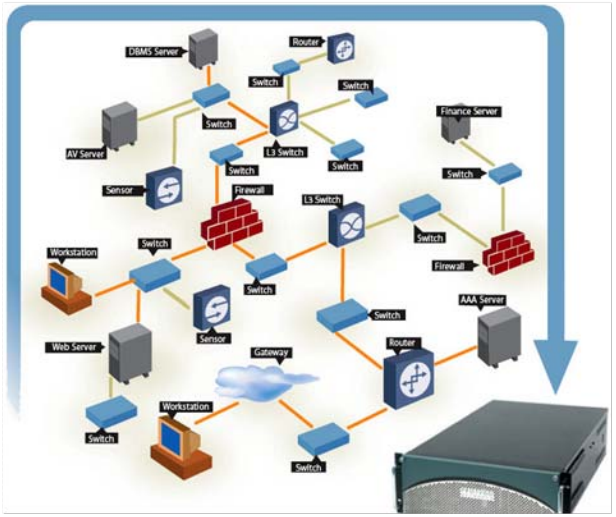
Cisco Security – MARS
Monitoring, Analysis and Response System

- **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*"

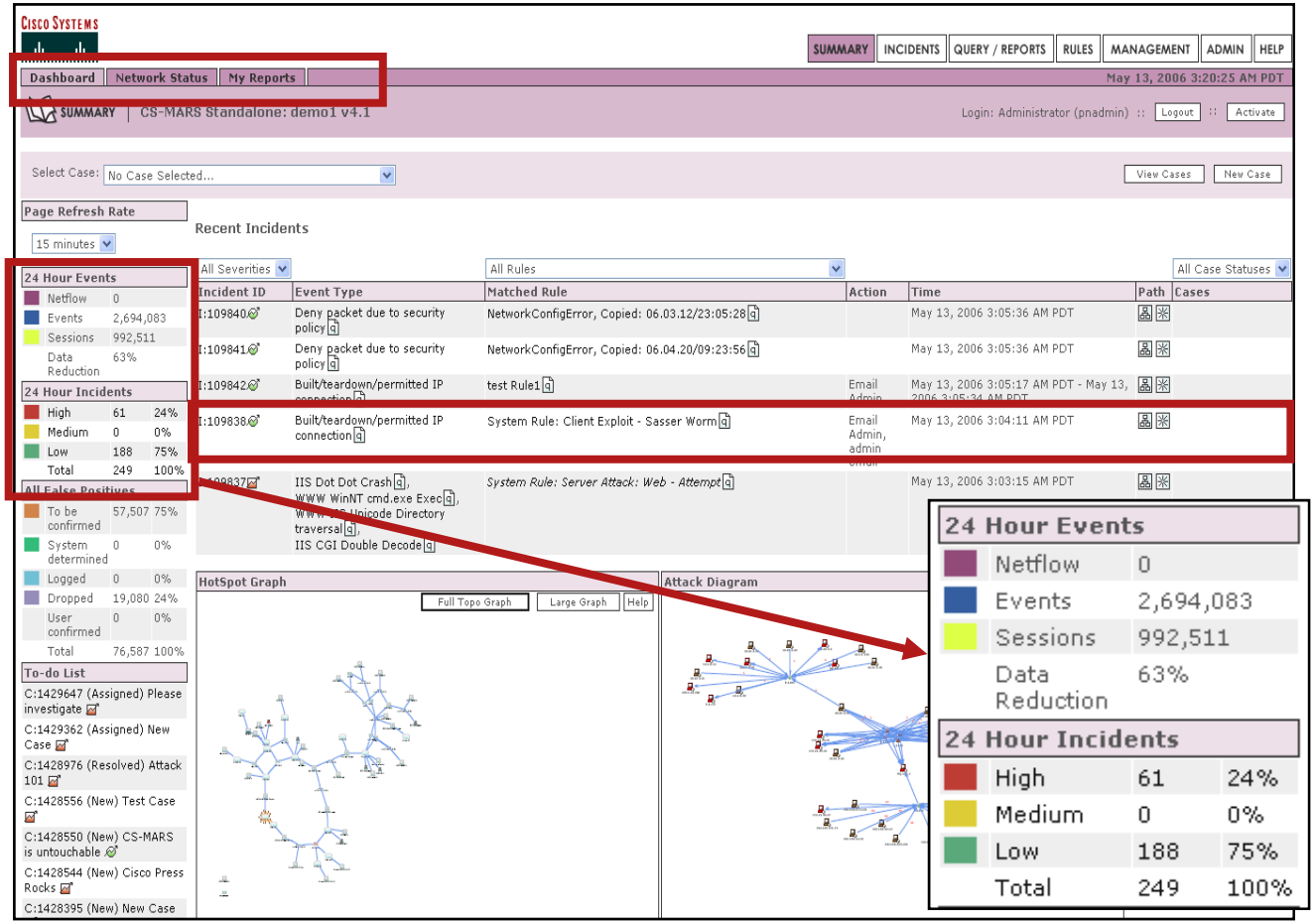
  ***Incidents* are topologically aware for visualization and replay**

  Mitigation on L2 ports and L3 chokepoints

Cisco Security MARS
Device Support – Not Just Cisco!

- Networking
  - Cisco IOS Router, Catalyst OS
  - Cisco NetFlow
  - Cisco Secure ACS
  - Extreme Extremeware Firewall/VPN
  - Cisco PIX, ASA, FWSM
  - Cisco IOS Firewall Feature Set
  - Cisco VPN Concentrator
  - Check Point Firewall-1 NG, NGX, FPx, VPN-1
  - Juniper (NetScreen) Firewall
  - Nokia (Check Point) Firewall
- IDS/IPS
  - Cisco NIDS, IDSM, IPS ASA module
  - Cisco IOS IPS module
  - Intruvert IntruShield
  - Enterasys Dragon
  - ISS RealSecure Sensor
  - Snort
  - McAfee Intrushield NIDS
  - Juniper (NetScreen)
  - Symantec ManHunt
- Vulnerability Assessment
  - eEye REM
  - Foundstone FoundScan
  - Qualys QualysGuard
- Host Security
  - Cisco Security Agent (CSA)
  - McAfee Entercept, ePolicy
  - ISS RealSecure Host Sensor
  - Symantec AnitVirus
  - Network Associates VirusScan
- Host Operating System Logs
  - Windows NT, 2000, 2003 (agent/agent-less)
  - Solaris
  - Redhat Linux
- SYSLOG/SNMP
  - Universal device support
- Applications
  - Web Servers (IIS, iPlanet, Apache)
  - Oracle 9i, 10g database audit logs
  - Network Appliance NetCache
- Security Policy Managers
  - Cisco Security Manager

Cisco Security MARS
Web Interface Dash Board/ Critical Data Reduction



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

Cisco Security MARS
Attack Path and Topology Awareness

Victim/contaminated host

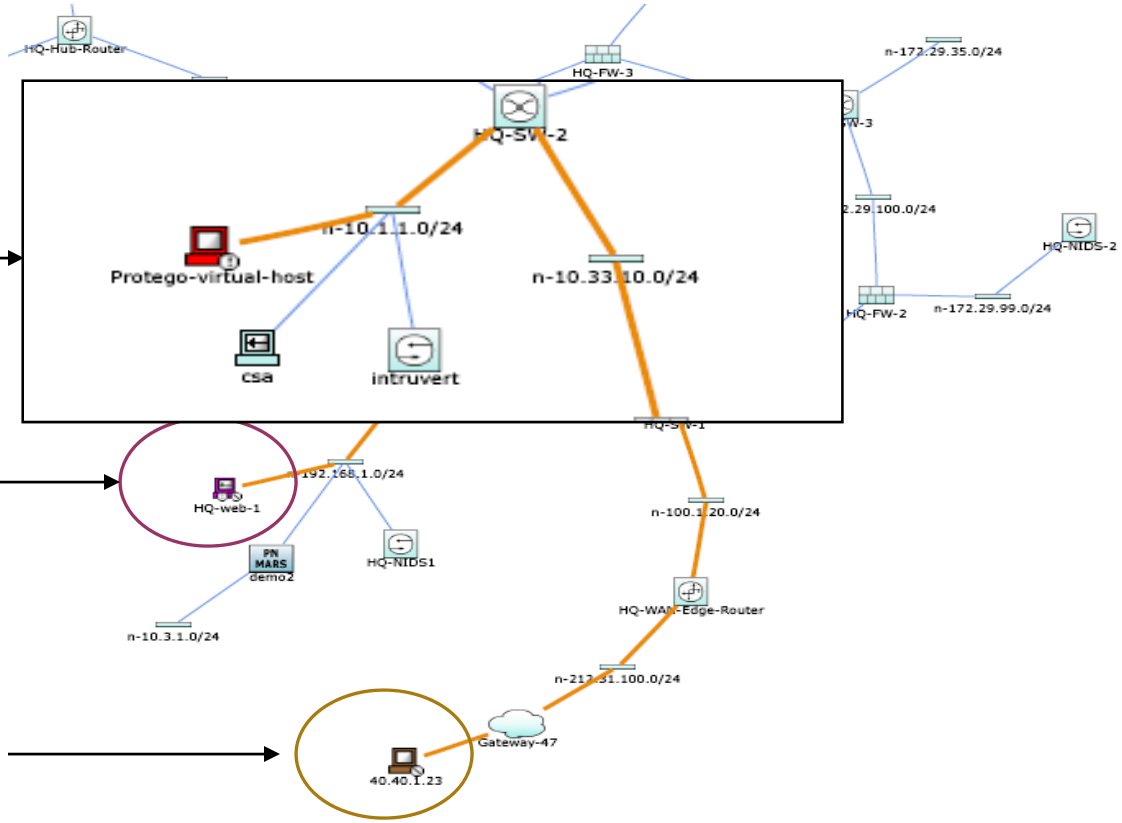
(red)

Compromised host propagating attack

(purple)

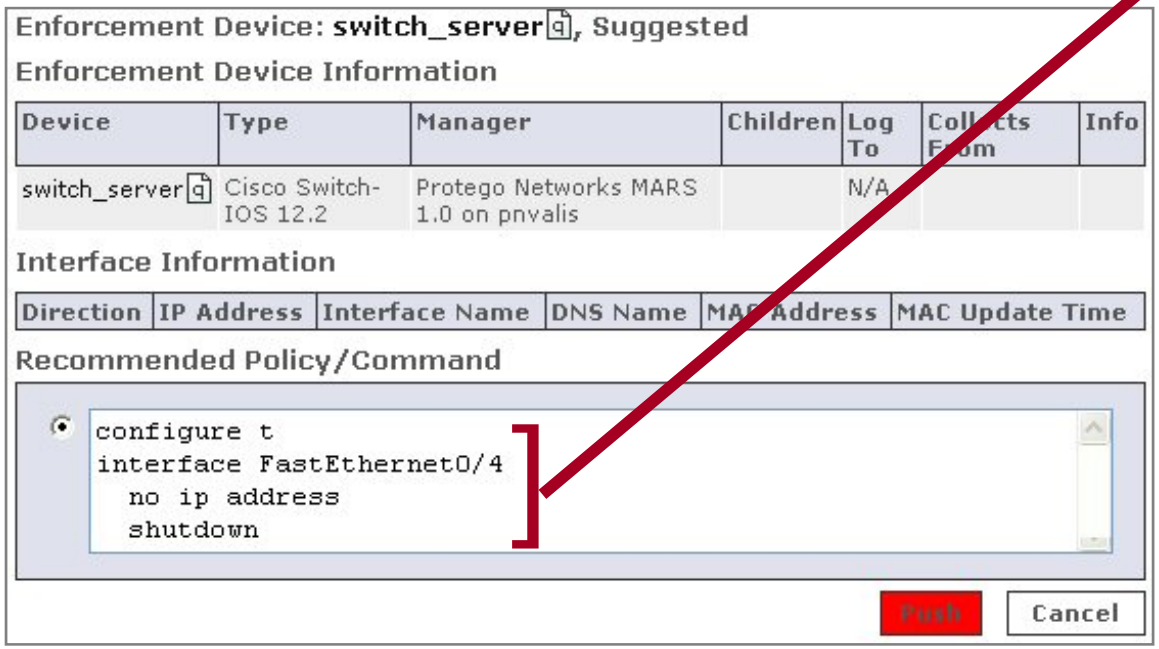
Attack Start

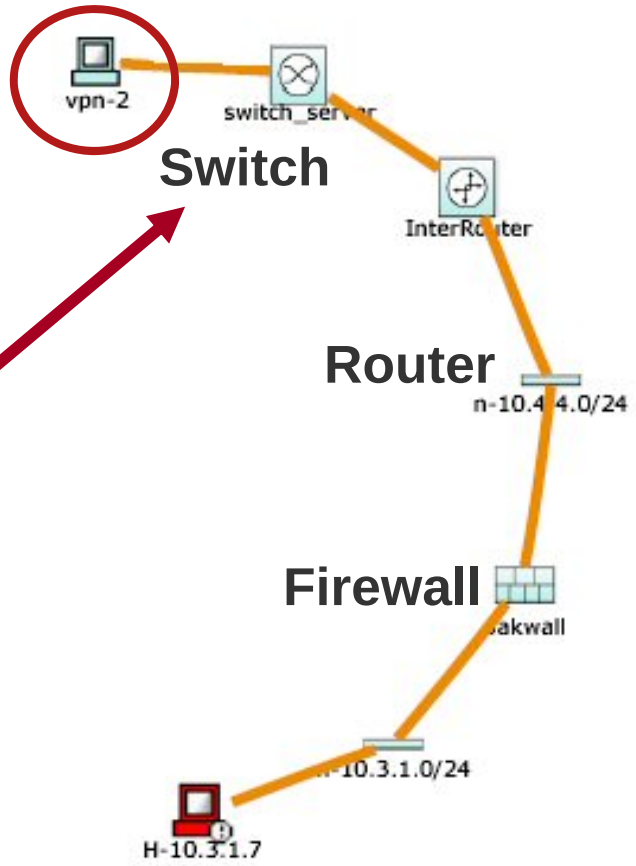
(brown)



Cisco Security MARS
Monitoring, Analysis and Response System

- **MARS visually represents an attack path and provides the ability to respond to the attack with an exact device command**





Compliance Reports

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

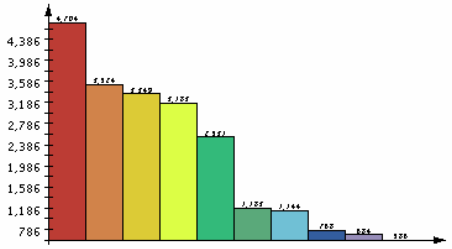
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

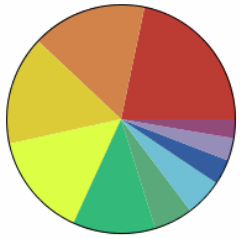
Name	Schedule	Format	Recipients	Query	Description
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.

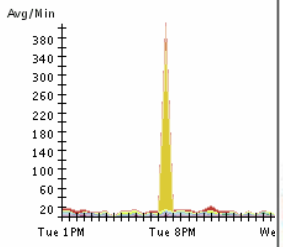
Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY

Keywords: [None]





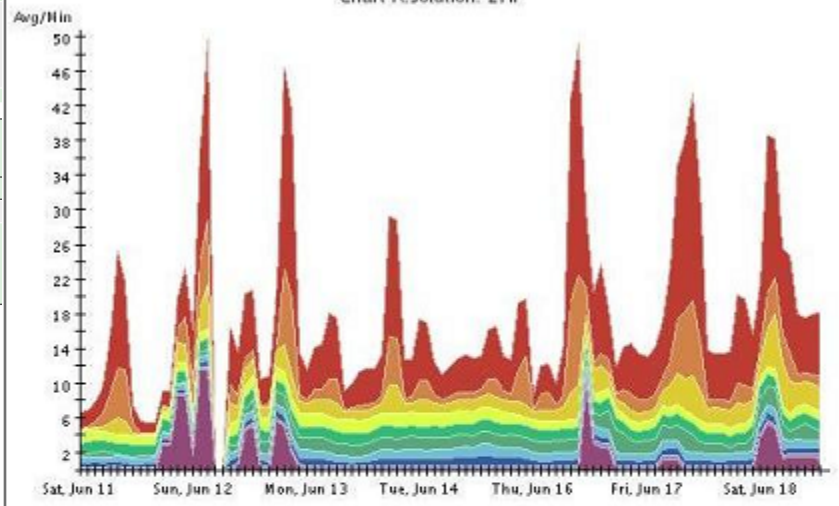


Rank		Count (# of sessions)	Raw Destina
	1	4704	445
	2	3524	80
	3	3349	26686
	4	3183	135
	5	2531	47683
	6	1183	1026
	7	1144	0
	8	768	139
	9	684	9898

Activity: All Events and Netflow - Top Destination Ports, last 7d-0h

Total View | Week | View Report | Legend

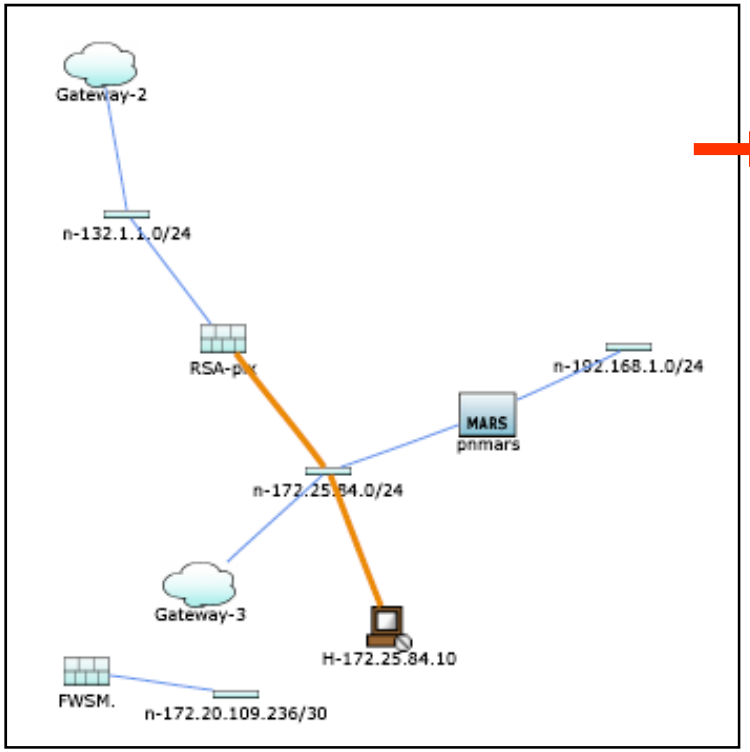
Chart resolution: 2Hr



Color	Total Count	Value
	76,619	0
	34,719	80
	33,397	53
	26,451	2190
	23,042	23
	21,766	123
	10,511	1026
	8,687	1027
	6,645	138
	4,971	135

Enhanced Flow Troubleshooting: MARS

View Topology



View Firewall Rule Table

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:2936886, S:2936860	Deny packet due to security policy	172.25.84.10 138	5.32.21.4 138	UDP	Mar 20, 2006 5:51:31 PM PST	RSA-pix		False Positive

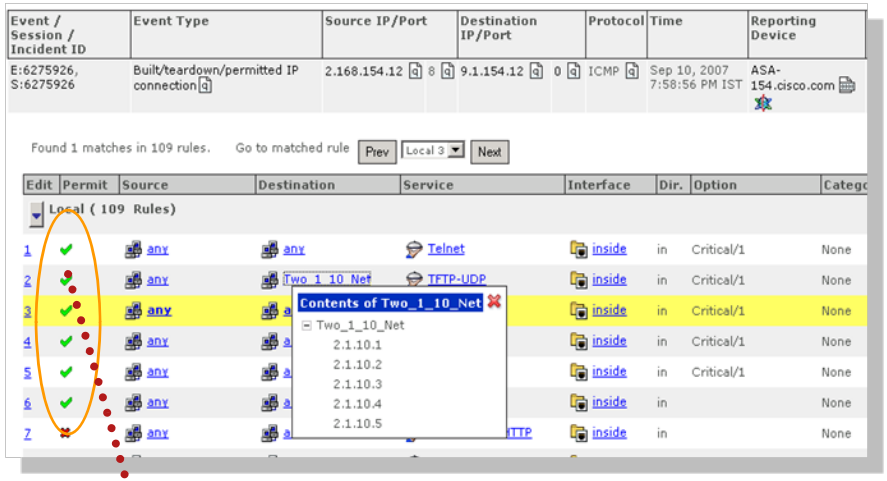
Total policies returned: **12**, Number of matched policies: **1**, Jump to matched policy: First Last

No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Category	Description	Prev/Nex
Local (12 Rules)										
1	✓	NMAP	RSA-Demo-Servers	IP	inside	in	LOG	None		
2	✓	RSA-Demo-Servers	Gateway	IP	inside	in	LOG	None		
3	⊘	any	162.2.2.2	udp/444	inside	in	LOG	None		
4	⊘	any	162.0.0.0/255.0.0.0	IP	inside	in	LOG	None		
5	✓	any	179.0.0.0/255.0.0.0	IP	inside	in	LOG	None		
6	⊘	any	BadDests	IP	inside	in	LOG	None		
7	⊘	any	BadDests	IP	outside	in	LOG	None		
8	⊘	NMAP	any	IP	inside	in	LOG	None		« »
9	✓	172.25.84.0/24	any	IP	inside	in	LOG	None		
10	✓	any	any	IP	inside	in	LOG	None		
11	✓	any	any	TCP	inside	in	LOG	None		
12	⊘	any	any	IP	All-Interfaces	in	LOG	None		

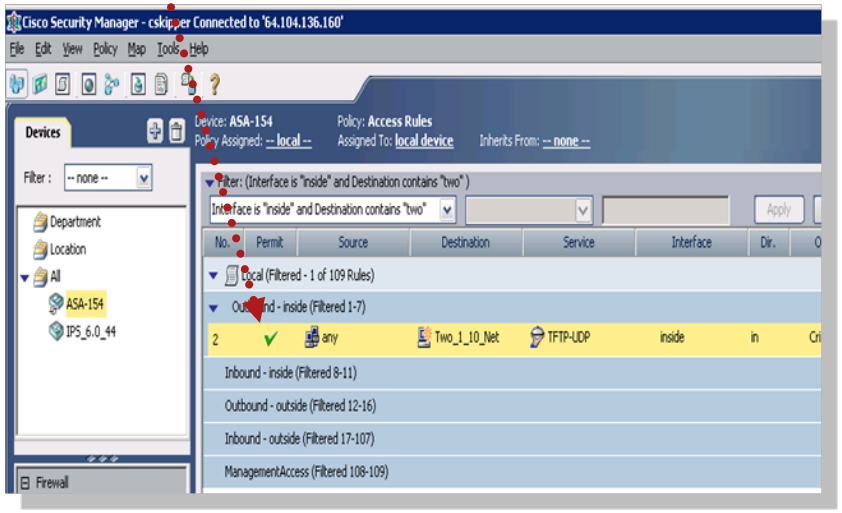
CS-M/CS-MARS Firewall Linkages Event to Rule

- Trace events back to the triggering rules and make changes on the fly
- Better understand the meaning of raw log data
- CS-MARS queries CS-Manager with parameters from the rule (Policy Query), first match from the top will be the matching rule
- Within CS-MARS an operator can view the content of Building Blocks
- Selecting the rule number will cross launch CS-Manager automatically and navigate to the rule

CS-MARS



CS-M



A Systems Approach to Streamline IT Risk Management for Security and Compliance