Security Management

Omar Contreras G. omcontre@cisco.com

Connected World with Complex Security Challenges

Collaboration and Communication

- TelePresence/ Video / IM / Email
- Mobility
- Web 2.0 / Web Services / SOA

The New Threat Environment

- The Eroding Perimeter
- SPAM / Malware / Profit Driven Hacking
- Data Loss and Theft

The Business Impact of Security

- IT Risk Management
- Regulatory Compliance
- Security as Business Enabler

Why do I need security management?

Security management is about having the right tools on the right place

Sometimes security can be a barrier

Network Security Policy

- Generic document to "keep the bad guys out"
- How policies are enforced
- Rules are for individuals or groups in a company
- Understand what information and services are available
- What the potential is for a damage
- Is any protection already in place

- No direct privileged logins
  Monitor IDS, SSH logs for successful root logins
- Use strong passwords
  Vulnerability scan for routers with default passwords
- No internet access from production servers
  Deny servers connecting directly to Internet
- No protocol tunneling
  Monitor IDS alerts for protocols tunneled over DNS to/from non-DNS servers

For connections into *Unclassified* classified segments		
From	**Control Type**	**Comment**
Unclassified	No controls	
Shared	No controls	
Company Only	No controls	*With the exception of the Internet*
Confidential	No controls	

For connections into *Shared* classified segments		
From	**Control Type**	**Comment**
Unclassified	No controls	
Shared	No controls	
Company Only	No controls	
Confidential	No controls	

For connections into *Company Only* classified segments		
From	**Control Type**	**Comment**
Unclassified	Via a proxy: Network level control to and from the proxy. Direct: Strong user-level control	*This allows both for things like incoming SMTP and user dial-in.*
Shared	Network level control	
Company Only	No controls	
Confidential	No controls	

For connections into *Confidential* classified segments		
From	**Control Type**	**Comment**
Unclassified	Not permitted	
Shared	Not permitted	
Company Only	Strong user-level control	
Confidential	No Control	

Why do I need security management?

- Security is not a product its all about a process
- Security management is a process to handle and save companies assets, IT and knowhow
- No best practice how to secure your network
- Security is individual for each enterprise to determine what security is required, where and when the process starts with an understanding of the potential threats
- Threats must be evaluated in terms of corporate risk
- Risk determines whether the implementation of security to mitigate the threat is justified
- Risks can vary greatly between customers

Correlating information
What You Have to Deal With :

#	Date	Host	Severity	Event
112	3/14/2006 3:47:48 PM	LON-CSAMC.rtbc.cisco.com	Alert	The process 'C:\Program Files\RealVNC' AUTHORITY\SYSTEM) attempted to ac from 10.21.121.208. The operation was Details Rule 223 Wizard 2 sim
111	3/14/2006 7:07:33 AM	LON-CSAMC.rtbc.cisco.com	Alert	The process 'System' (as user NT AUTH connection as a server on TCP port 44 Details Rule 223 Wizard 22 sim
110	3/14/2006 12:08:49 AM	-	Information	Application Deployment Analysis data h 31 sim
109	3/13/2006 4:29:20 PM	-	Notice	The following hosts are not actively po Current inactive hosts 11 sim
108	3/10/2006 7:19:25 PM	VIM-LAPTOP1.rtbc.cisco.com	Alert	TESTMODE: The process 'C:\WINDOWS RTBC\fgandola15) attempted to initiate 172.16.100.8. The operation would hav Details Rule 571 Wizard 177 sim
107	3/10/2006 7:19:25 PM	VIM-LAPTOP1.rtbc.cisco.com	Alert	TESTMODE: The process 'C:\WINDOWS AUTHORITY\LOCAL SERVICE) attempte 445 to 172.16.100.8. The operation wo Details Rule 571 Wizard 2361 sim

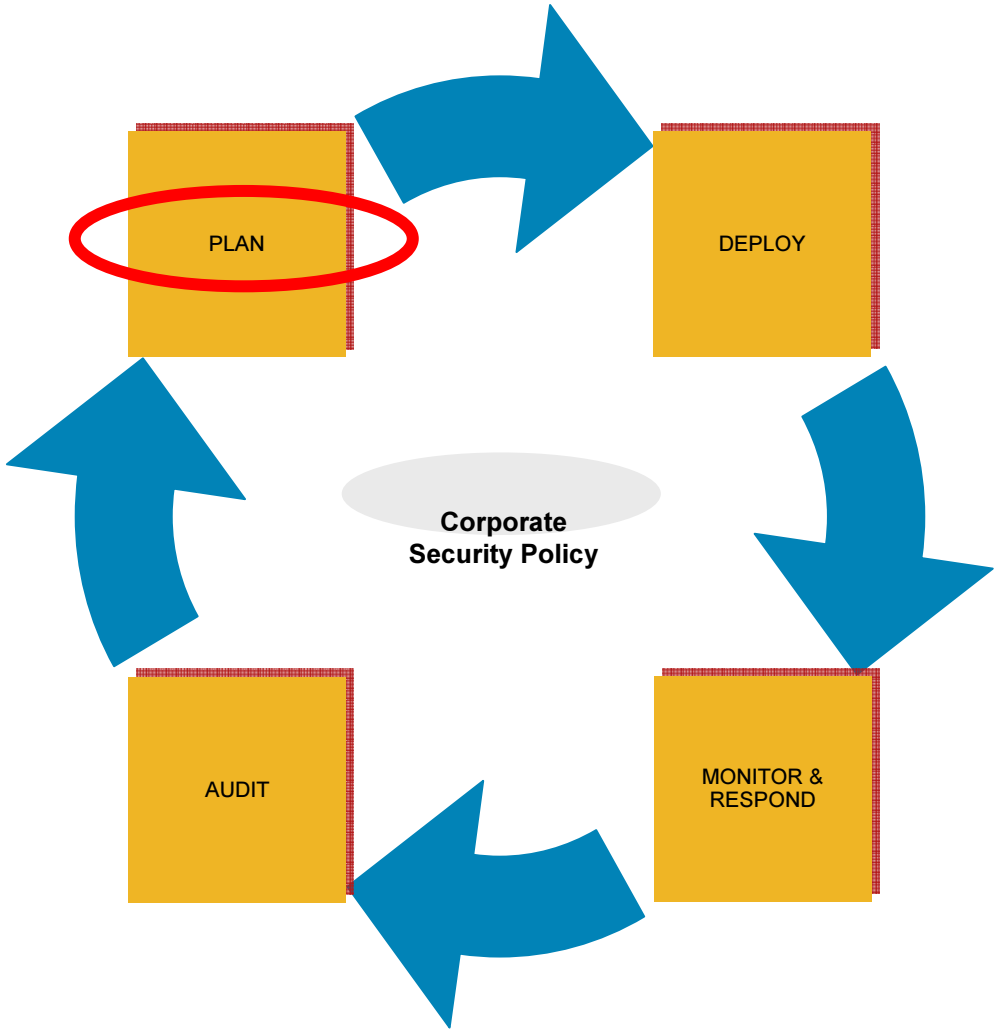
```
Mar 14 15:37:30.621: eou-ev:Starting Retransmit timer 3(172.17.20.11)
Mar 14 15:37:30.621: eou-ev:eou_send_hello_request: Send Hello Request host=
Mar 14 15:37:33.626: %EOU-6-CTA: IP=172.17.20.11| CiscoTrustAgent=NOT DETECT
Mar 14 15:37:33.626: eou-ev:172.17.20.11: msg = 17(eventEouAAAReq)
Mar 14 15:37:33.650: eou-ev:Starting Hold timer 180(172.17.20.11)all
0000D0  00 00 00 50 FF 53 4D 42 75 00 00 00 00 18 07 C8  ...P.SMBu.......
0000E0  00 00 DC 19 0A 85 ED 00 96 A5 00 00 00 00 FF FE  ................
0000F0  02 30 C0 15 04 FF 00 50 00 08 00 01 00 25 00 00  .0.....P.....%..
  riskRatingValue: 65
```

Security Management Life Cycle

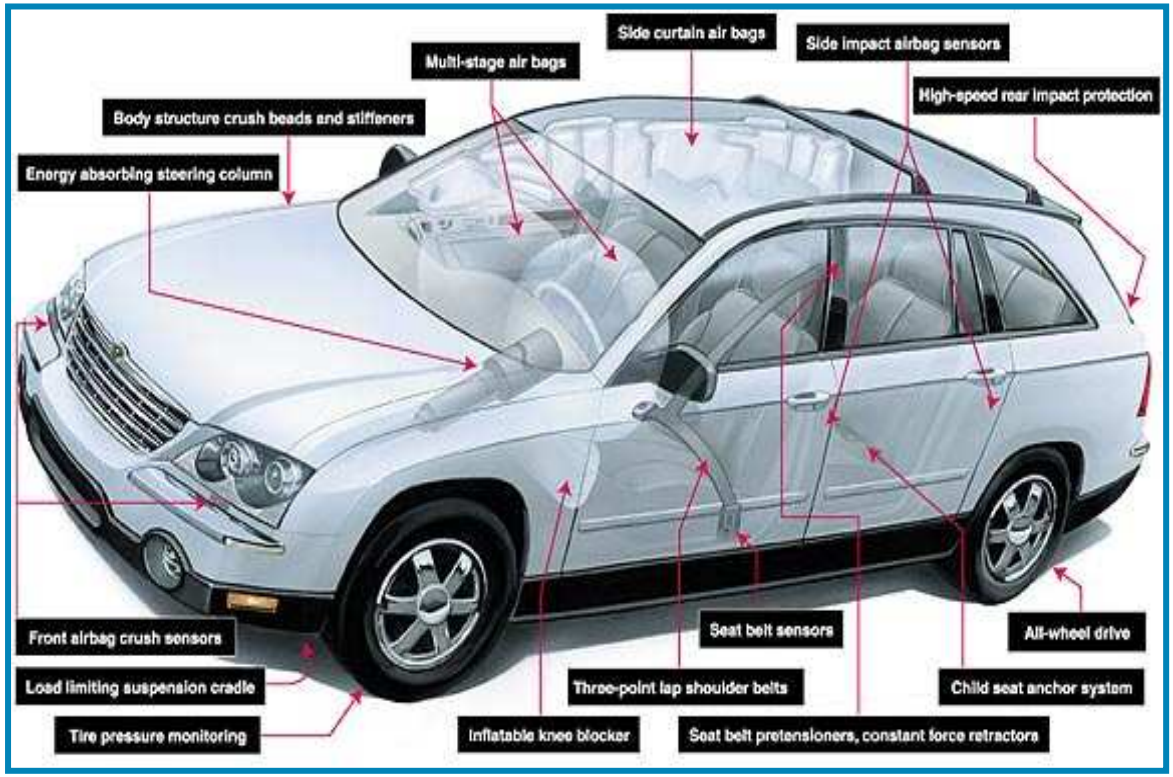
Security is a proccess which we called
Security Management Life Cycle

- **Plan** your security
- Implement and **deploy** your security
- **Monitor** the incidents and **respond** to them
- **Audit** and Improve your security policy

Agenda



Security is integrated in the system



Security isn’t added to the network, it is the network

Planning your Security
Technology

- Secure access to your devices
  - SSH, SSL, SCP, Secure access VTY
  - SNMPv3
  - **AAA & role based access**
  - **Out of band management**
- Protect your network
  - Firewall
  - ACL
  - IPS/IDS
  - VPN – IPsec & SSLVPN
- Protect the core
  - Control Plane Protection
  - **Management Plane Protection**
- Secure your monitoring
  - **ACL syslog correlation**
  - Netflow for security
  - **SDEE**
  - **Embedded Event Manager**
  - Embeddded Syslog Manager

Being told to secure my network !!!

Industry Security Best practices. In addition to CCO resources:

http://www.first.org/resources/guides/
http://www.sans.org/resources/policies/
http://www.ietf.org/html.charters/opsec-charter.html

Subset of Cisco Security Features/Technology (continued ...)

NetFlow	Disable any unused protocols	secure VTY	FPM
IP source tracker	VTY ACLs	SSH Configuration	NBAR
ACLs	Community ACL	SNMP	SSLVPN
uRPF	Prevent dead TCP sessions	Passwords	PEAP
RTBH	service tcp-keepalives-in	Granular Access	EAP
QoS tools	Use ‘type 5’ password	AutoSecure	EAP-FAST
Control Plane Policing	service password encryption	TACACS	NAC
iACL’s BGP best practices	AAA	RADIUS 802.1x	TKIP
CPU & memory thresholding	SSH	Port Security	AES
Syslog	IPSec	DHCP Snooping	Netflow9
SSHv2	3DES	Source Guard	PVLAN
SNMPv3	NIPS/IDS	Trunking	Host IDS/IPS
AutoSecurer	FW	Spanning Tree	AV
CLI views	SSLVPN	PVLAN	Certificate
Netflowv9	3DES	VACL	ARP Inspection

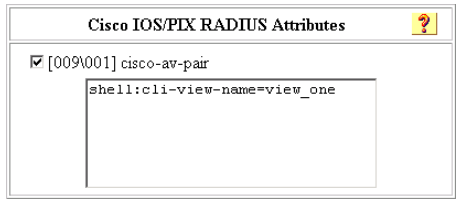
Role-Based Access Control

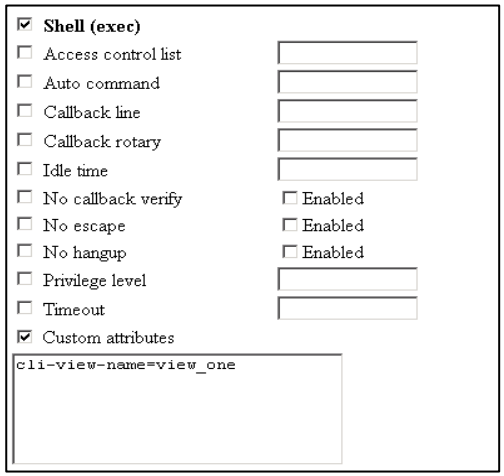
Role-Based CLI Access

- Defines CLI access based on administrative roles
- Defining the set of CLI commands that are accessible to a particular user
- Avoids unintentional execution of CLI commands by unauthorized personnel
- Prohibits users from viewing CLI commands that are inaccessible to them

```
Router(config)# parser view outsource-1
  Router(config-view)# password 5 V14o5g1
  Router(config-view)# commands exec include show version
  Router# enable view outsource-1
```

Role Based CLI Views with Cisco Secure ACS





http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_role_base_cli_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Out-Band Network Management (OOB)

Out-of-band management addresses the limitation by creating a management channel that is physically isolated from the data channel

4 Types of out-of-band-management

in-band-management:

Traffic passes on same network path as end-user and server traffic

pseudo out-of-band-management:

NOC traffic runs over different VLANs/subnets than user and server traffic

real out-of-band-management:

User, server and NOC traffic on console ports. No shared paths, no IP, management by 'show' commands

data communications network (DCN):

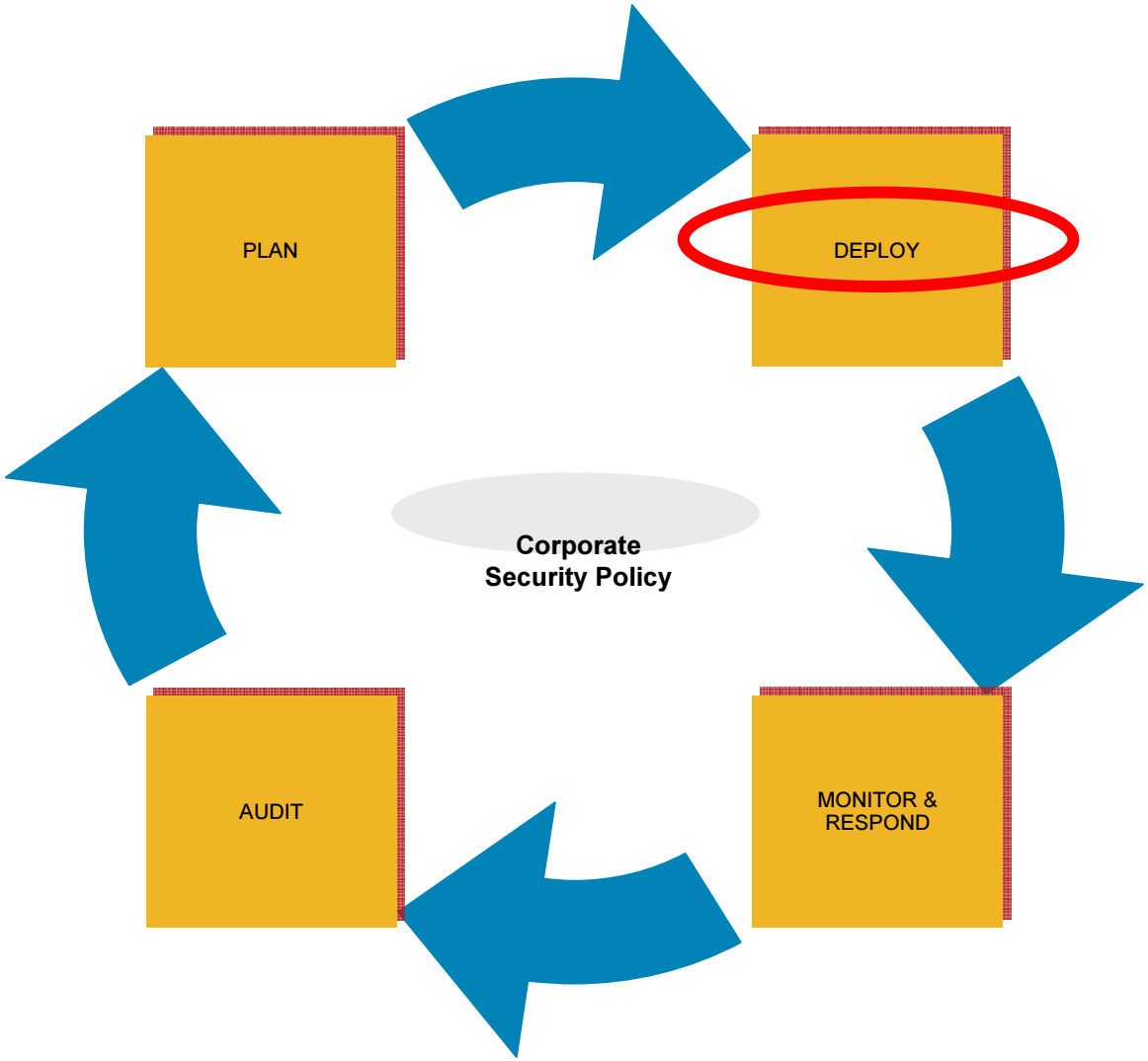
DCN is network management network. Service providers use DCN for connectivity between their OSS applications and network elements. Normal Data Plane traffic NEVER touches the DCN

Summary: Planning your security

Security management is about having the right tools on the right place

- Is your network ready for future incidents?
- Is your security policy up-to-date?
- Ask in your company for your security policy !!!
- What is the best tool/instrumentation to secure your network?
- Do you know your security-life-cycle in your company?

Agenda



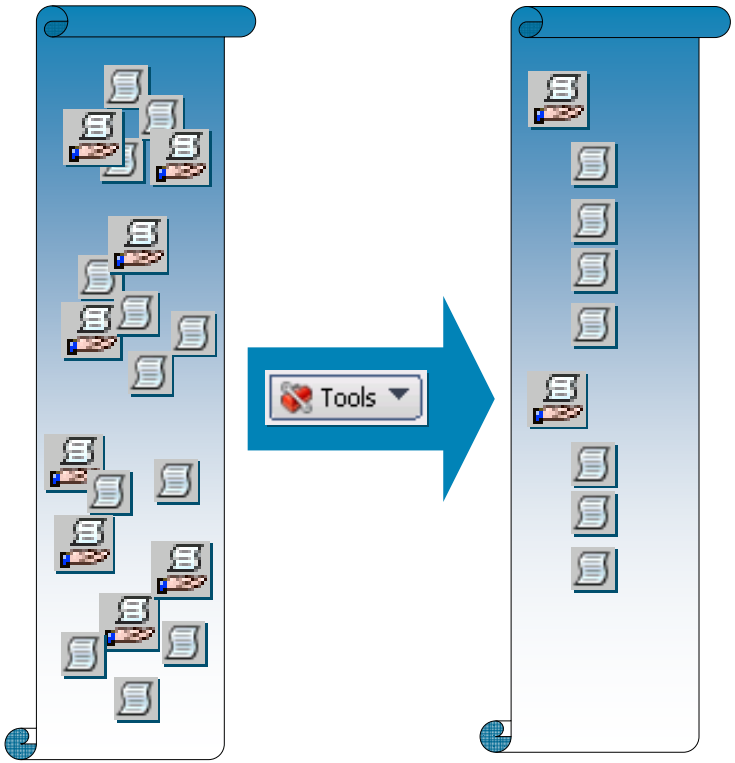
Reduce Policy Administration Complexity

Problem
Inconsistent large rule base, rules are redundant based on usage

Solution
Advanced analysis tools for the rule base

Example
Rule optimization, real-time hit count, redundant and bypassed rules analysis

Benefit
Consistent and optimized rule base



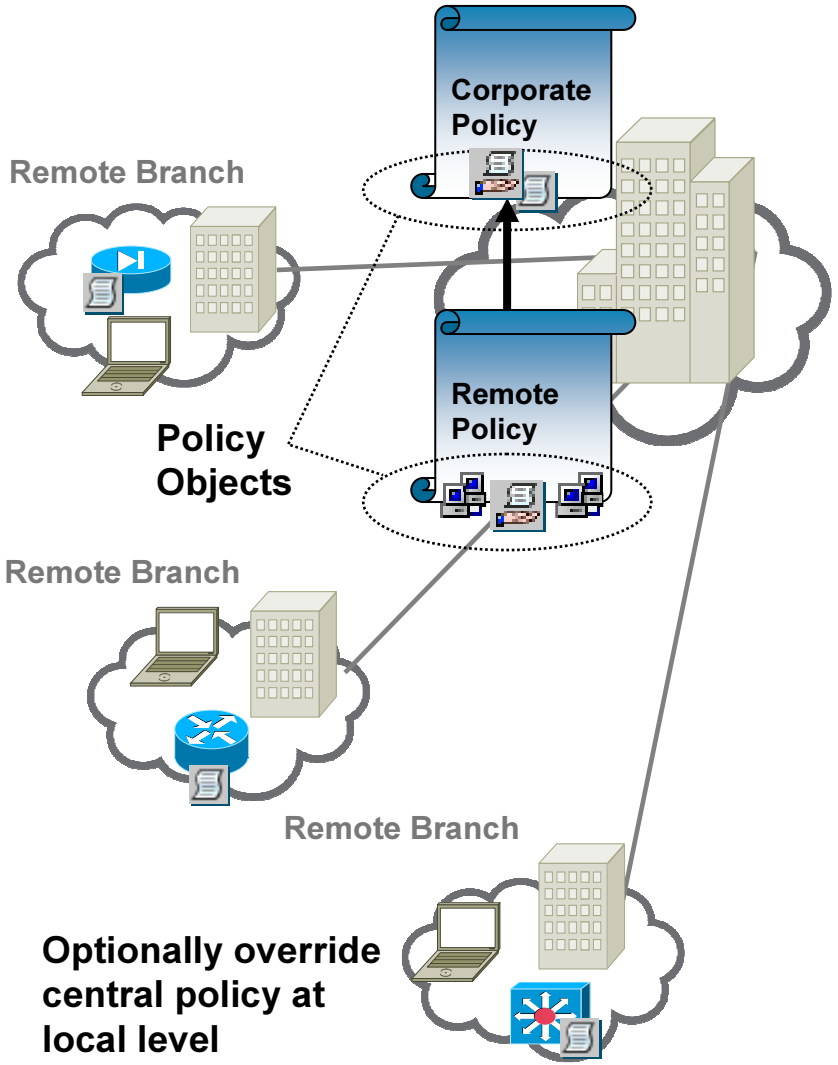
Reduce Policy Administration Complexity

Problem
Enforcing consistent policies across large numbers of devices

Solution
Policy sharing and inheritance

Example
Share common polices:
e.g., no Napster traffic, allow SSH, SSL

Benefit
Consistency of policies at scale



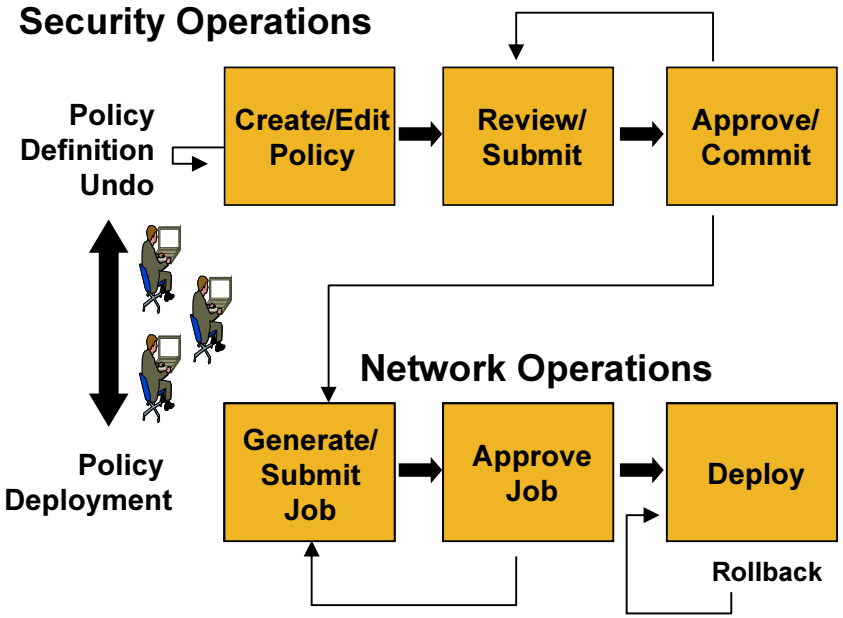
Implement Collaborative Change Control

Problem
Enforcing internal governance of policy change management

Solution
Workflow for change approval and deployment

Example
Mandate approval before change deployments

Benefit
Enable collaboration between NetOps and SecOps



Collaborate with Confidence

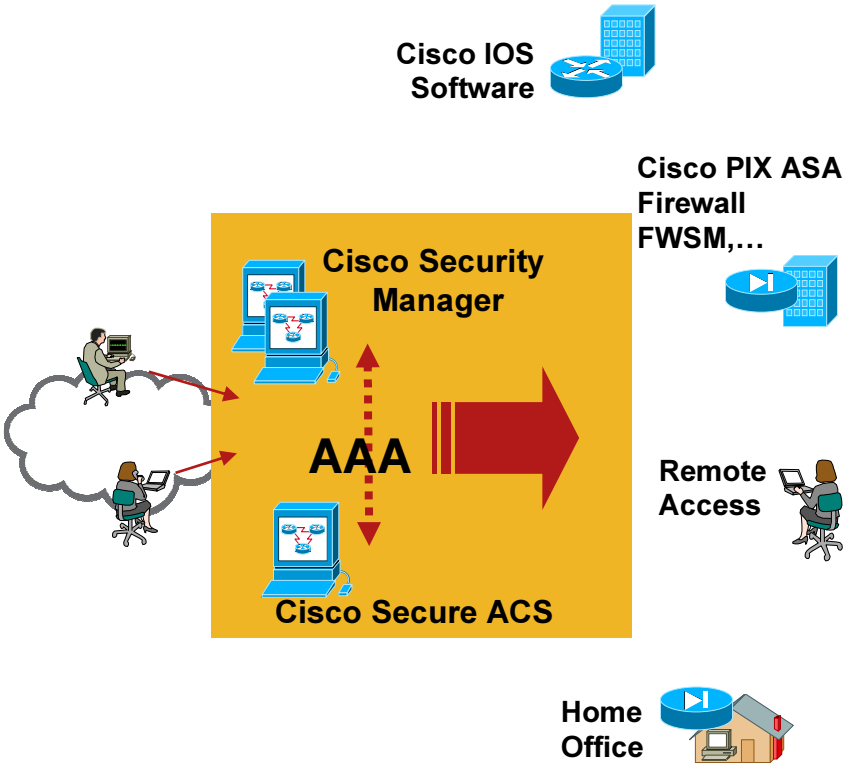
Administrator Roles-Based Access Control

Problem
Enabling multiple users to make controlled changes to network policy

Solution
Role-based access to specific devices and policy functions, supporting multiple simultaneous users

Example
Chris can change East coast firewalls while Pat tunes West coast IPSs

Benefit
Enable separation of duties and report on adds, moves and changes



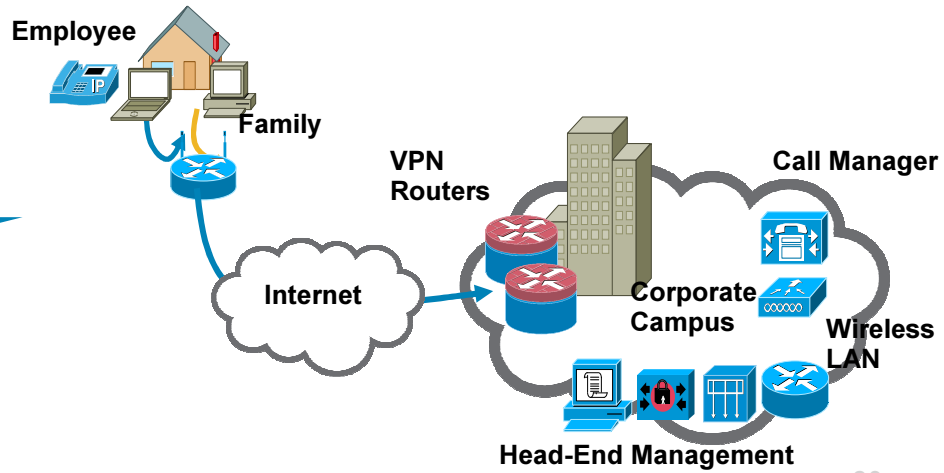
Optimize IT Resources at Branch Locations

Problem
Managing large and distributed branch and tele-worker deployments

Solution
Zero-touch simplified, distributed deployment

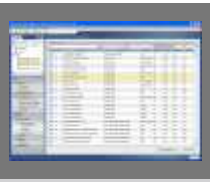
Example
Self provision the installation of a new branch office or tele-worker

Benefit
Reduced technical staff at remote sites, decreased OpEx



The Tooling

Cisco Security Manager (CS-M)



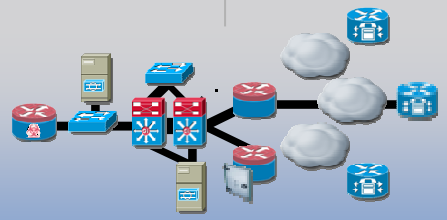
Simplified Policy Administration

End-to-End Configuration

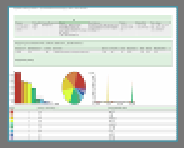
Networkwide or Device-Specific

Configuration Provisioning

Monitoring Analysis Mitigation



Cisco Security Monitoring, Analysis and Response System (CS-MARS)



Rapid Threat Identification and Mitigation

Topology Awareness

Data Correlation

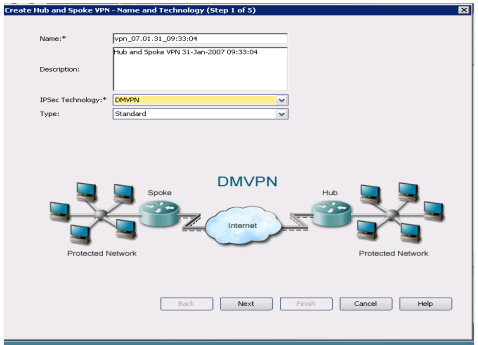
CS-Manager and CS-MARS work together to provide an integrated configuration and monitoring solution

Cisco Security Manager

Integrated Security Configuration Management

Firewall Mgmt

- Support for PIX, ASA, FWSM, and IOS Routers
- Rich FW rule definition: shared objects, rule grouping, and inheritance
- Powerful analysis tools: conflict detection, rule combiner, hit counts, …

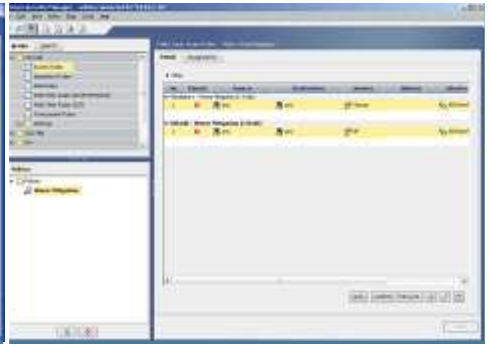


VPN Mgmt

- Support for PIX, ASA, VPNSM, VPN SPA, and IOS Routers
- Support for wide array of VPN technologies such as, DMVPN, Easy VPN, and SSL VPN
- VPN Wizard for 3-Step Point-and-Click VPN Creation

IPS Mgmt

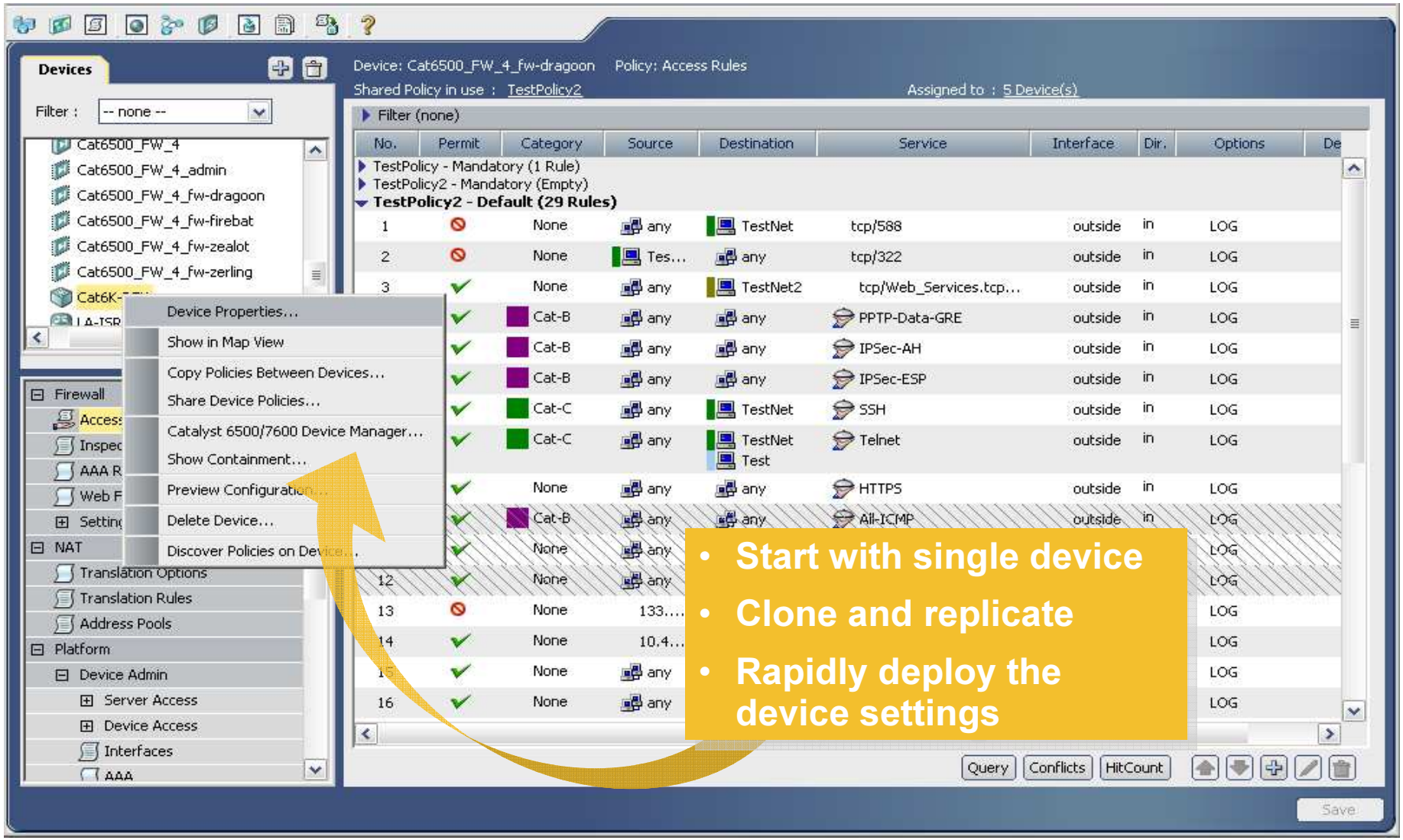
- Support for IPS Sensors and IOS IPS
- Automatic policy based IPS Sensor software and signature updates
- Signature Update Wizard allowing easy review/editing prior to deployment



Reduce OPEX

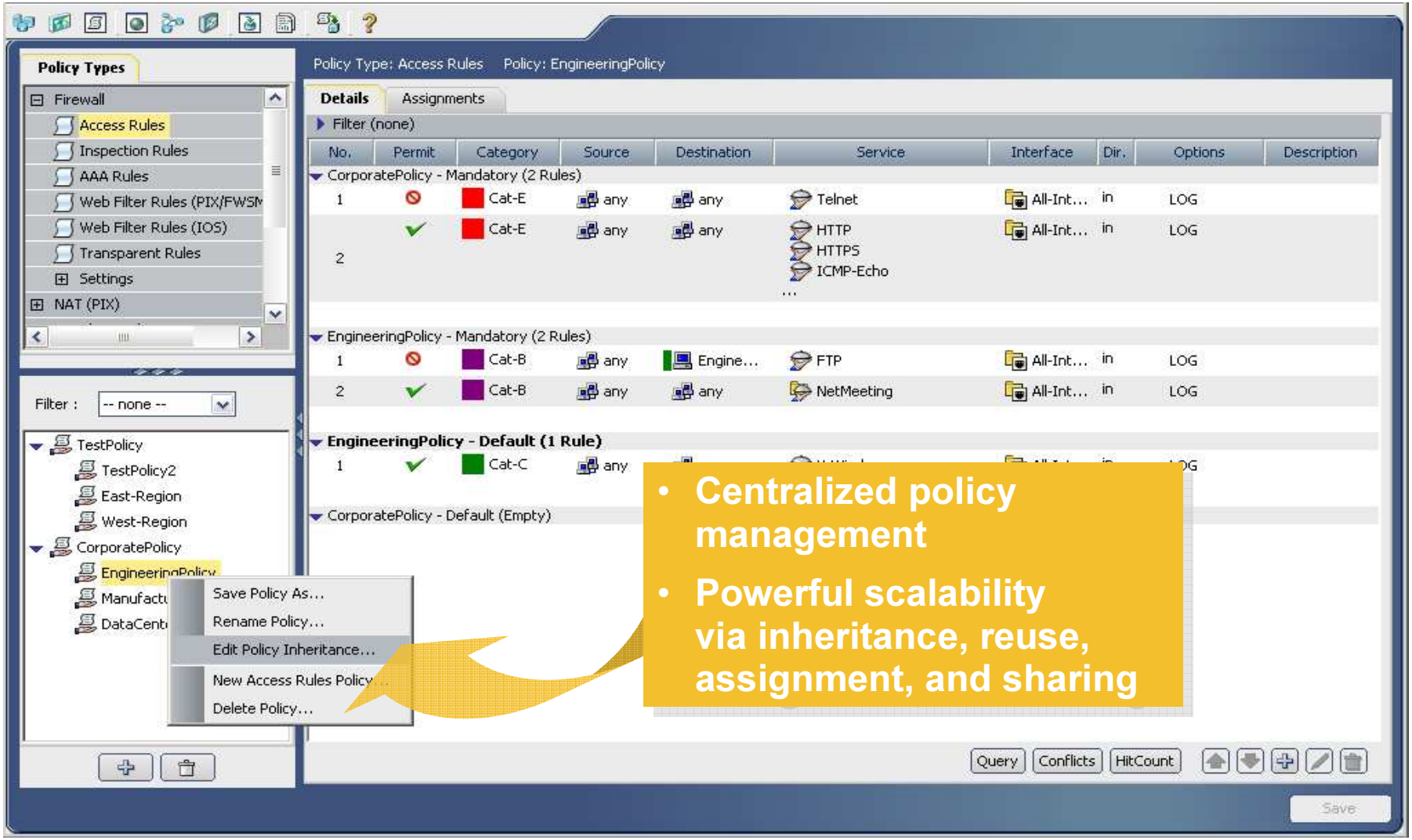
- Unified security management for Cisco devices supporting FW, VPN, and IPS
- Efficiently manage up to 5000 devices per server
- Multiple views for task optimization
  - Device View
  - Policy View
  - Topology View

Device-Centric View



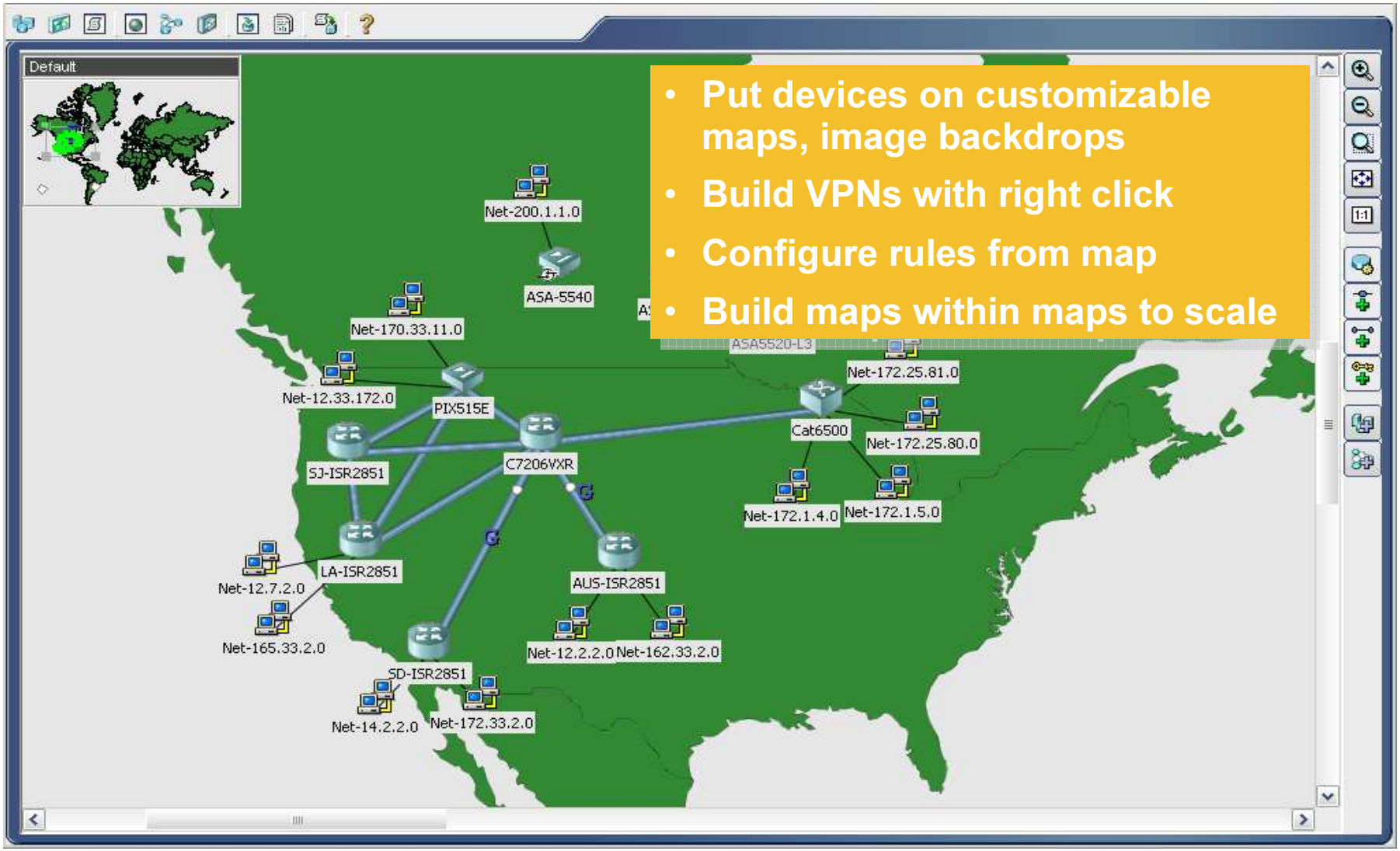
- Start with single device
- Clone and replicate
- Rapidly deploy the device settings

Policy-Centric View



- Centralized policy management
- Powerful scalability via inheritance, reuse, assignment, and sharing

Topology-Centric View



- Put devices on customizable maps, image backdrops
- Build VPNs with right click
- Configure rules from map
- Build maps within maps to scale

Policy Sharing – Write once, deploy accross devices with the same capability

What Is It?

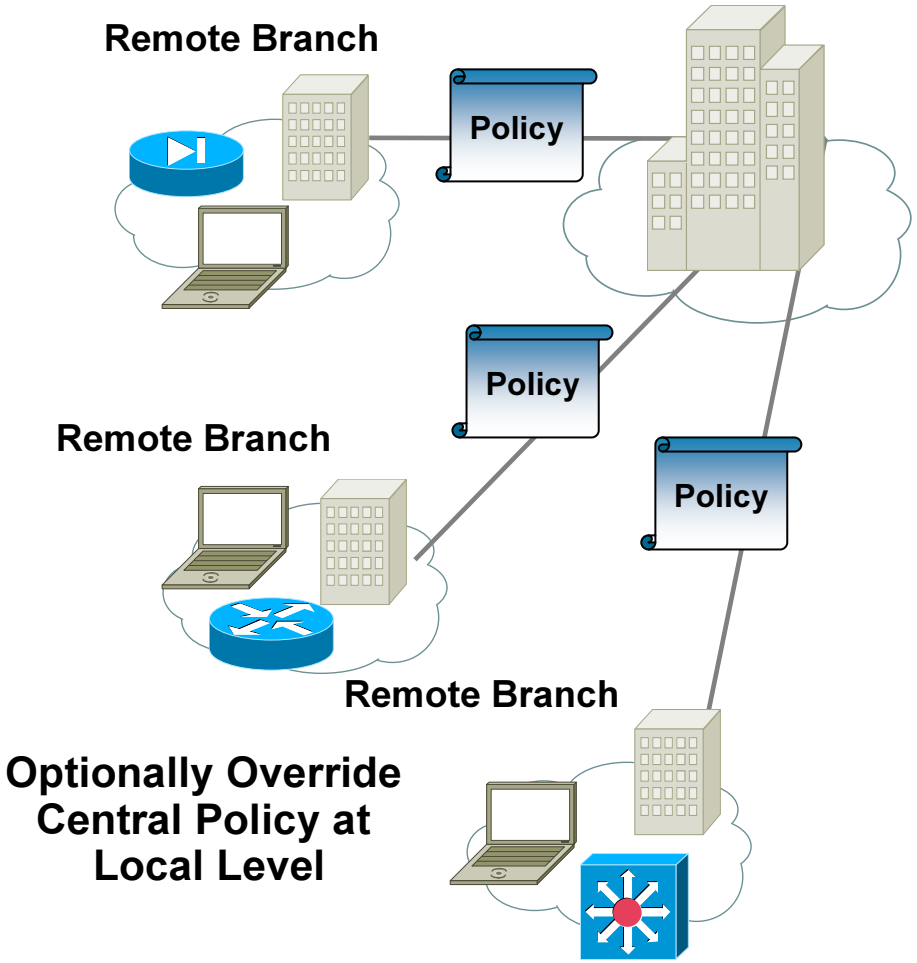
- Decoupled devices from polices

Example

- Share common policies across device groups for
  - –Branch firewall
  - –Site-to-site VPN
  - –Device administration
- Corporate mandatory policies
  - –No Napster traffic, period
  - –Allow SSH and SSL

Benefit

- Reduced complexity for administrators
- Do more with fewer resources



Role Based Access Control

What Is It?

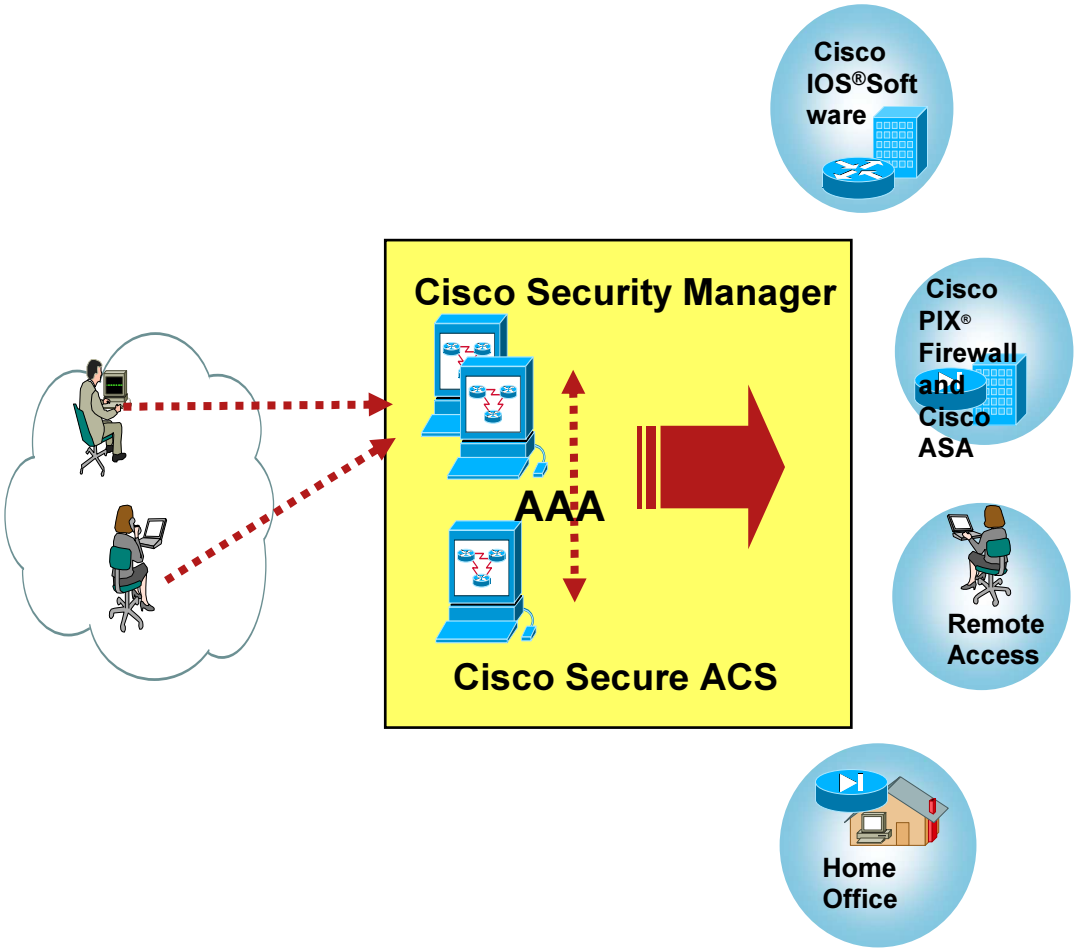
- Authenticates administrator's access to management system
- Determines who has access to specific devices and policy functions

Example

- Verifies administrator and associate administrators to specific roles as to who can do what

Benefit

- Enables delegation of administrator tasks to multiple operators
- Provides appropriate separation of ownership and controls



Workflow

"Enable different management teams to work together"

What Is It?

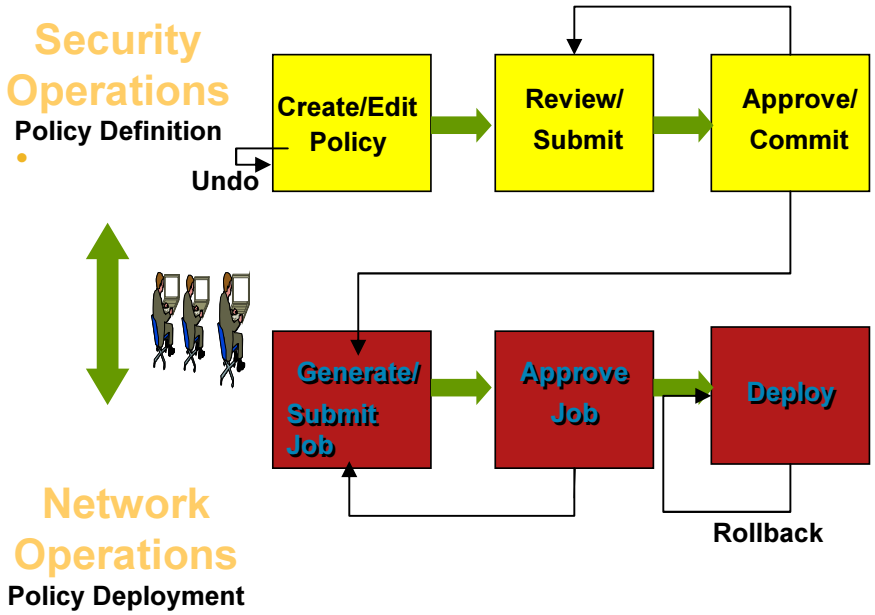
- Structured process for change management that complements your operational environment

Example

- Who can set policies
- Who can approve them
- Who can approve deployment and when
- Who can deploy them

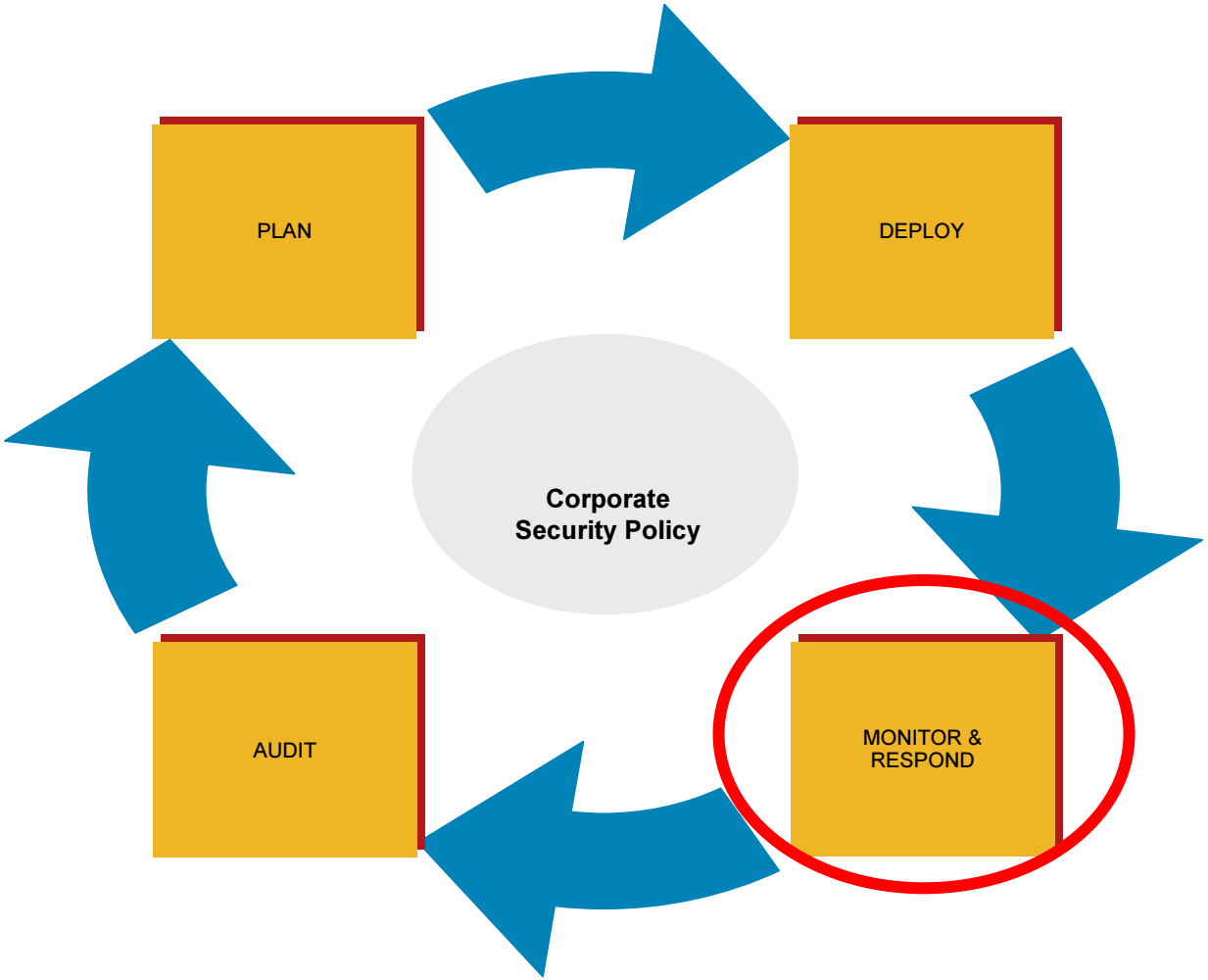
Benefit

- Enables teamwork and collaboration between NetOps and SecOps
- Provides scope of control



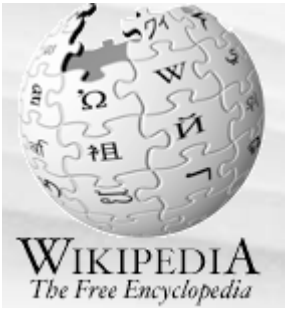
Firewall, VPN, and IPS Services

Agenda



What is a Threat?

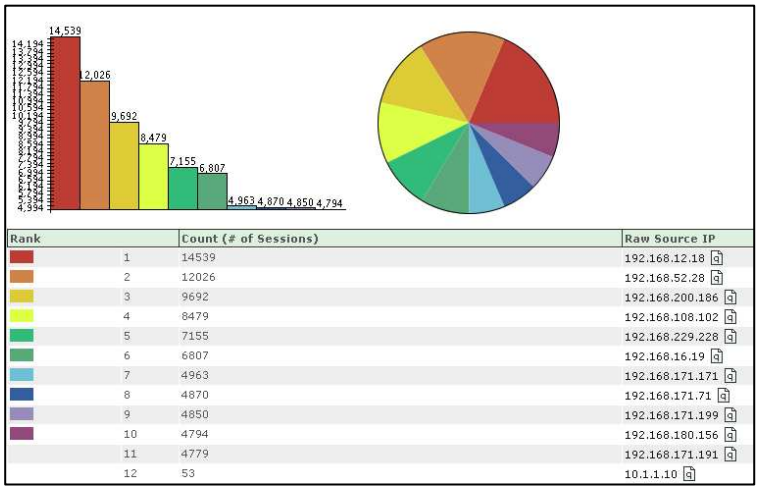
- **Definition:**
  - A probable impending danger or warning of impending danger, e.g. "a terrorist threat"
  - An act of coercion wherein a negative consequence is proposed to elicit response



- You need to determine what is considered a threat in your environment. What others consider a threat can be a business opportunity for you!
- Knowing what to look for, you can implement some kind of Threat Detection.
- Only once you know what happened and where, you can take proper actions.

Security Information Management

- **Definition:** SIM refers to the collection of data into a central repository for trend analysis, reduce the number of security events to a manageable and actionable list, automating analysis such that real attacks and intruders can be discerned.
- A SIM consists of 5 major elements:
  - ✓Log consolidation
  - ✓ Threat correlation
  - ✓ Incident management
  - ✓ Reporting
  - ✓Topology awareness



HIPAA.ORG

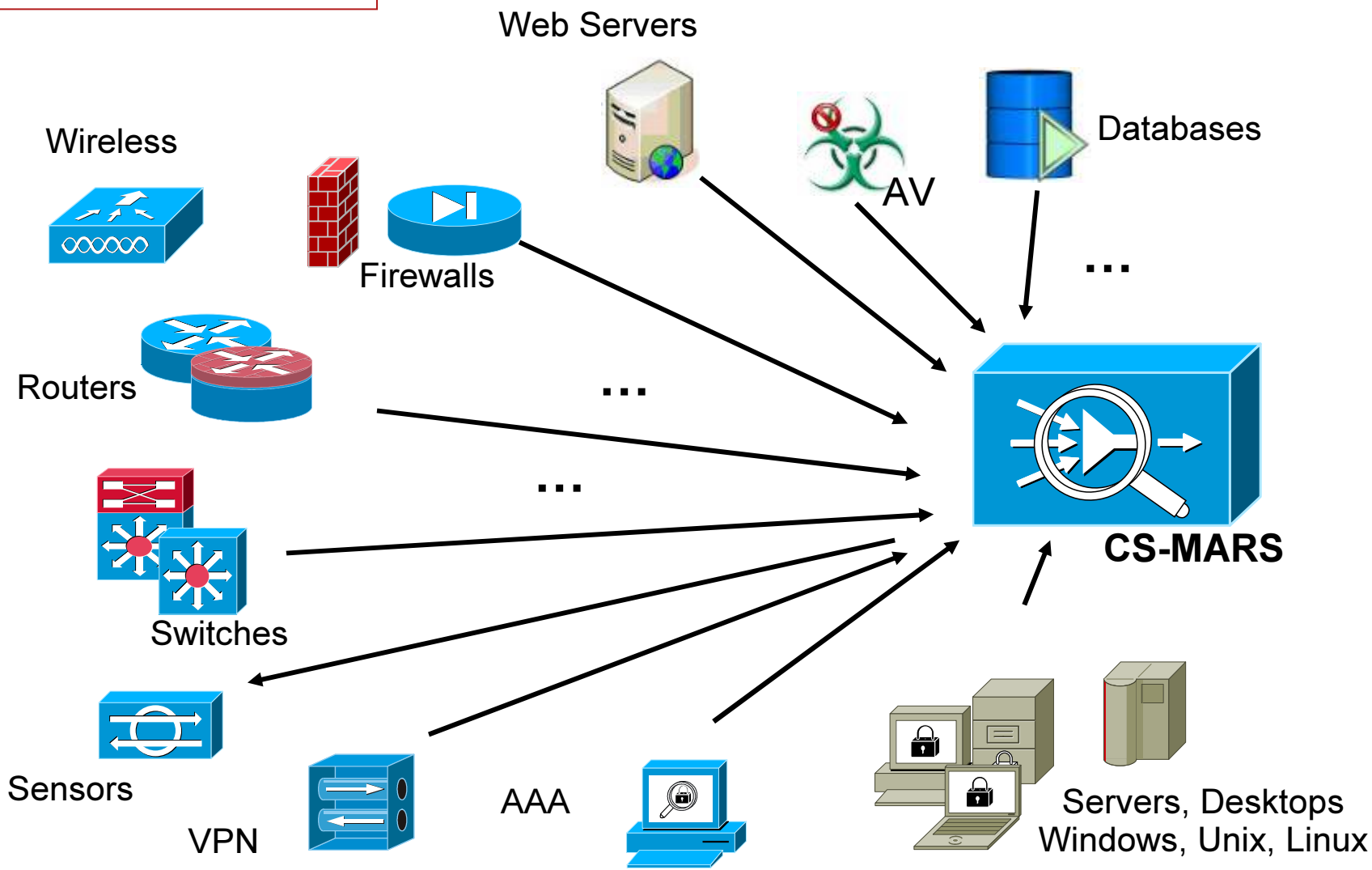
The Gramm-Leach Bliley Act

PRIVACY INITIATIVES

Compliance is an orthogonal process to correlation

Define your reporting devices

Multivendor



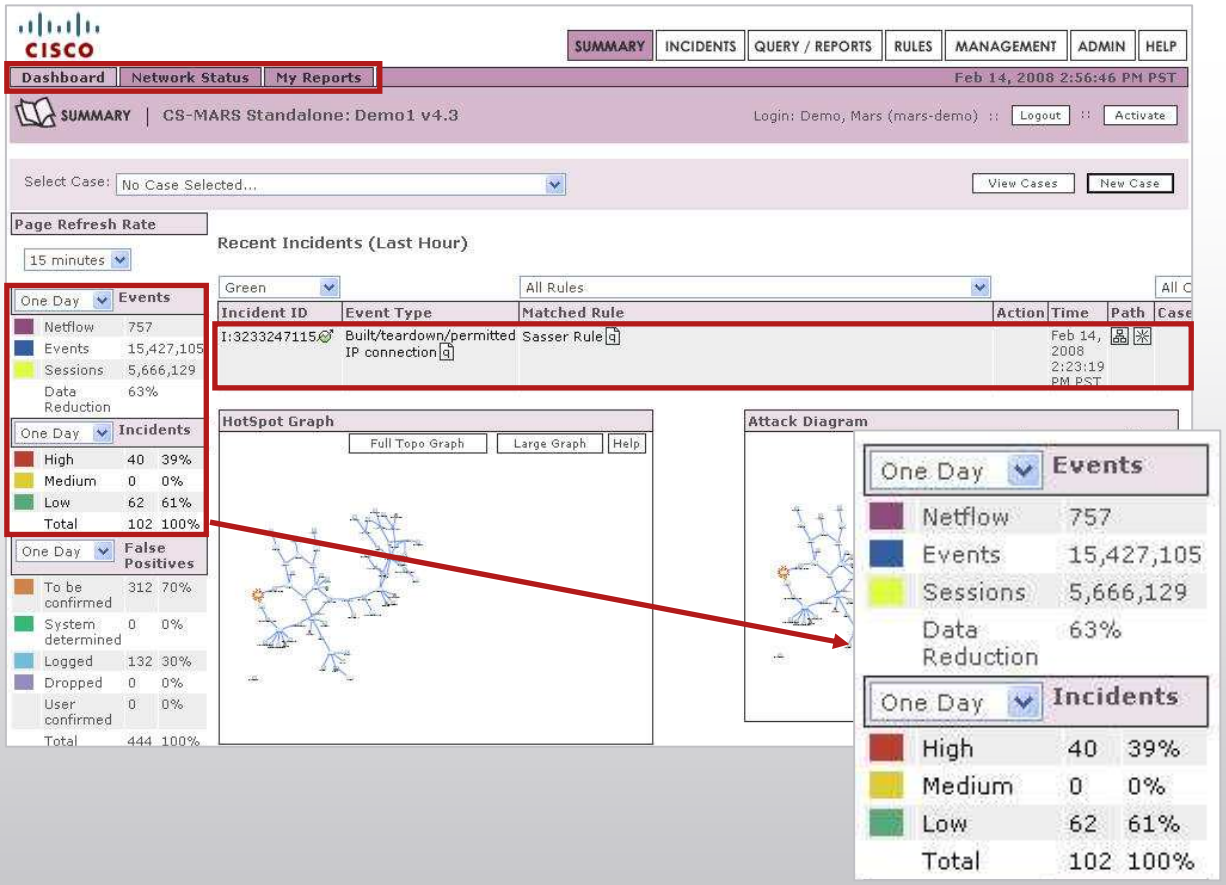
Cisco Security MARS

Appliance Based, Purpose-Built Solution

- **Scalable from SMB through Enterprise markets**
  - **Standalone Appliances**
  - **Distributed Standalone Appliances**
  - **Tiered Appliances utilizing a Global Controller**
- **Collector, Database, and Reporting engine all in one box, saving power and rack space**
- **Simple licensing – no administrator licenses and no agent costs**
- **Hardened OS is pre-installed, shortening the installation time**
- **Database is pre-installed, self-contained, and self-maintaining**
  - **No DBA Staff required**
  - **Helps in controlling ongoing expenses**
- **Models available with redundant drives and power supplies to increase solution uptimes**

Cisco Security MARS

Intuitive Operational Dashboard



Incident Dashboard

- Aggregate
- Correlate
- Summarize

15,427,105 Events

5,666,129 Sessions

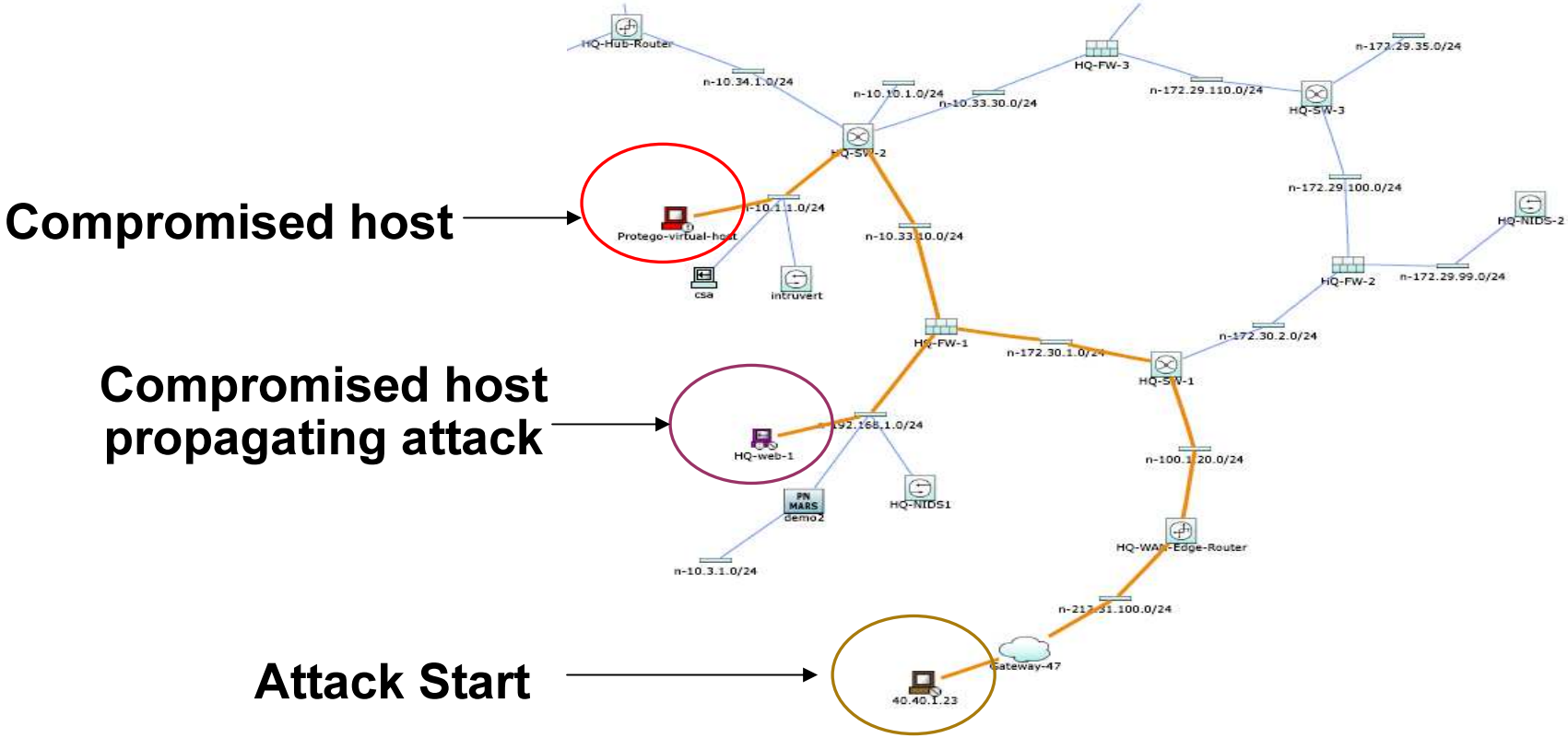
102 Incidents

40 High Severity Incidents

- Device configuration, logging, and network topology information enables MARS to build a threat resolution dashboard
- Rapidly identify and resolve threats via Real-time Data Reduction, Allows Administrators to Focus On Priorities

Attack Path and Topology Awareness

Rapid Threat Identification Improves Response Time



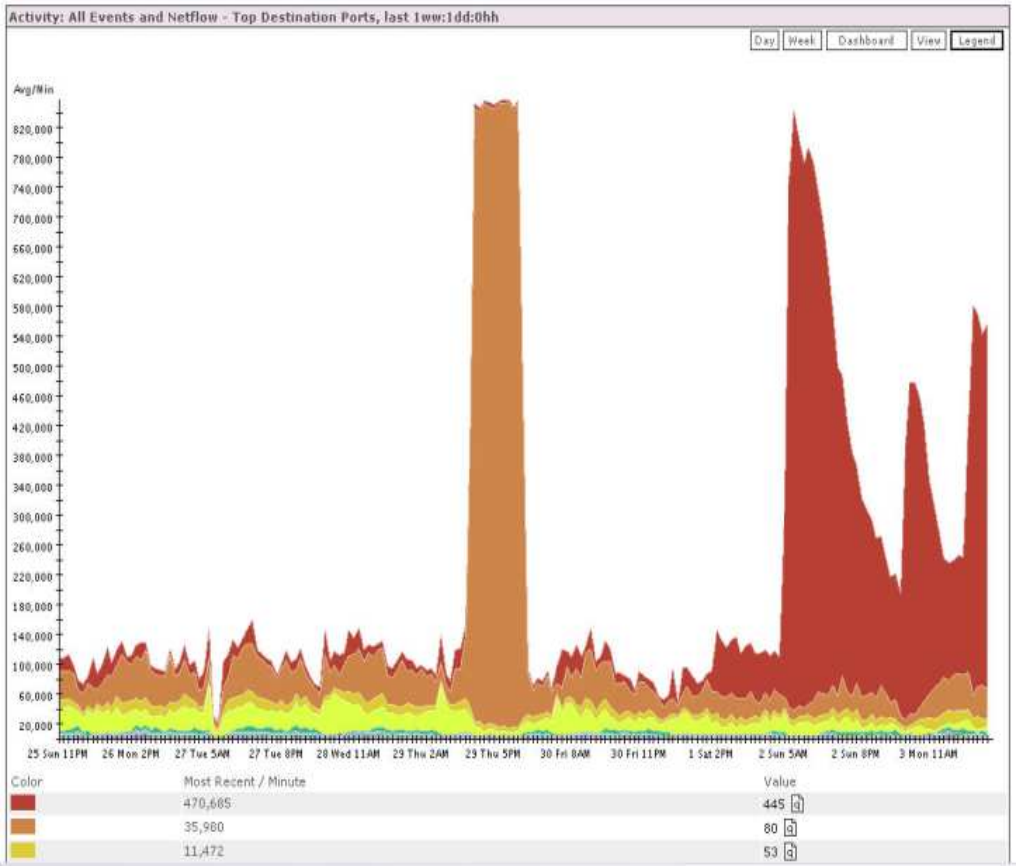
- **CS-MARS builds an understanding of the network topology and uses this in displaying the path an attack takes through the network.**

- **Color coding of elements allows for rapid identification of troubled devices while the topological layout helps to improve troubleshooting and response times.**

Anomaly Detection

Day Zero Threat Detection Improves Response Time

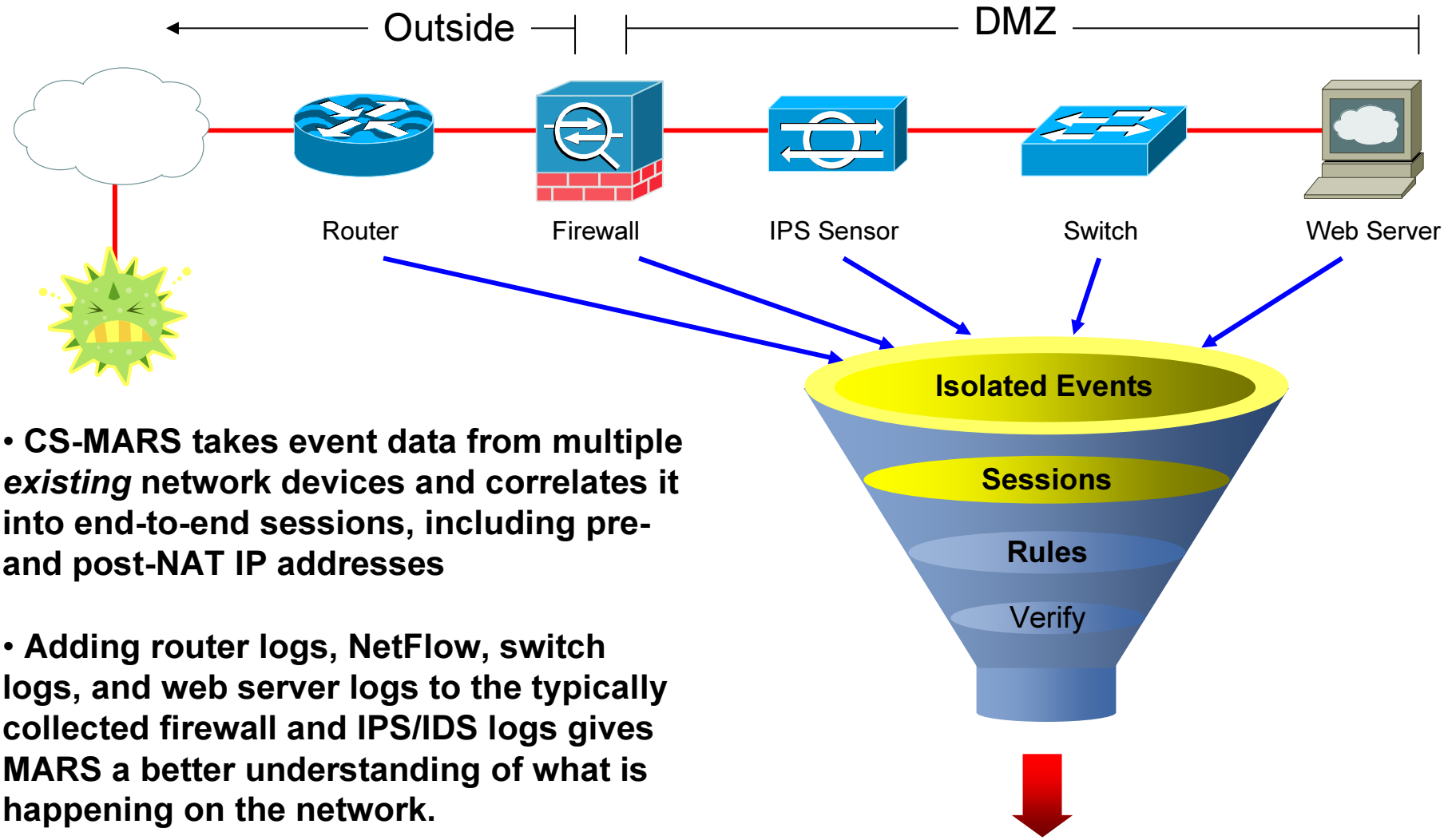
- **Leverages NetFlow or firewall Syslog messages to profile the network usage**
- **Detect statistically significant anomalous behavior from computed baseline, including viruses, worms, and policy violations such as peer-to-peer file sharing**
- **Correlate anomalous behavior to attacks and other events reported by Network IDS systems.**
- **Enables detection of attacks where IDS/IPS signatures do not exist and firewalls allow traffic through**



Example of a Sasser-D breakout from a customer's site

Data Correlation

Increase the ROI for your Existing Equipment



- **CS-MARS takes event data from multiple *existing* network devices and correlates it into end-to-end sessions, including pre- and post-NAT IP addresses**

- **Adding router logs, NetFlow, switch logs, and web server logs to the typically collected firewall and IPS/IDS logs gives MARS a better understanding of what is happening on the network.**

Actionable Intelligence

Internal Threat Resolution

Improve Threat Response Times

- **Use control capabilities within your infrastructure**
  - **Layer 2/3 attack path is clearly visible**
  - **Enforcement devices are identified**
  - **Resolution commands are provided**
  - **Alternate enforcement devices also suggested**

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		

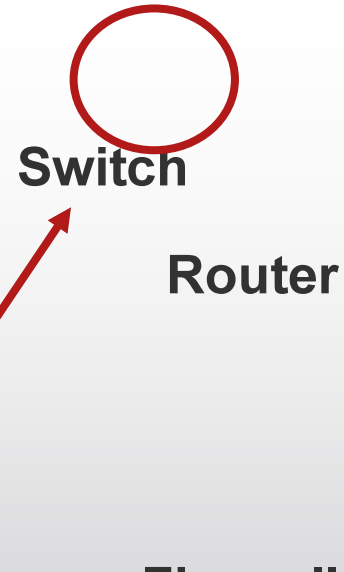
Interface Information

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

Recommended Policy/Command

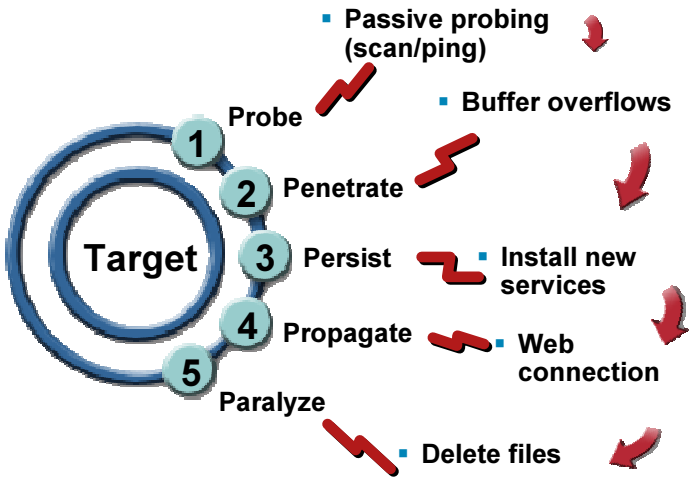
```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```

Push Cancel



Reduce the time it takes to identify where and how to block an attack

Rules based correlation



- Depending on the incident type, you could have only some of the steps.
- The format and the events type will determine the incident severity

Rule Name: Successful Reconn and Buffer Overflow
Status: Active
Action: None
Time Range: 0h:05m
Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/Non-stealth	ANY	None	ANY	ANY	1		OR
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/Stealth, ApplPolicyViolation/Misc	ANY	None	ANY	ANY	1		FOLLOWED-BY
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/Login, Penetrate/BufferOverflow/Web	ANY	None	ANY	ANY	1		FOLLOWED-BY
4		$TARGET01	ANY	ANY	Info/AllSession	ANY	None	ANY	ANY	1		

Variables and Operators allow Context Sensitive Correlation

MARS Tuning: Adapt rules to your network

In the System Rules, You Can Modify the Following:

- Source IP
- Destination IP
- Reporting device

→ Add an Action (i.e. email alert)

Rule Name: System Rule: Server Attack: Web - Attempt

Status: Active

Action: None

Time Range: 0h:30m

Description: This correlation rule detects attacks on a web server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, denial of service attempts etc.

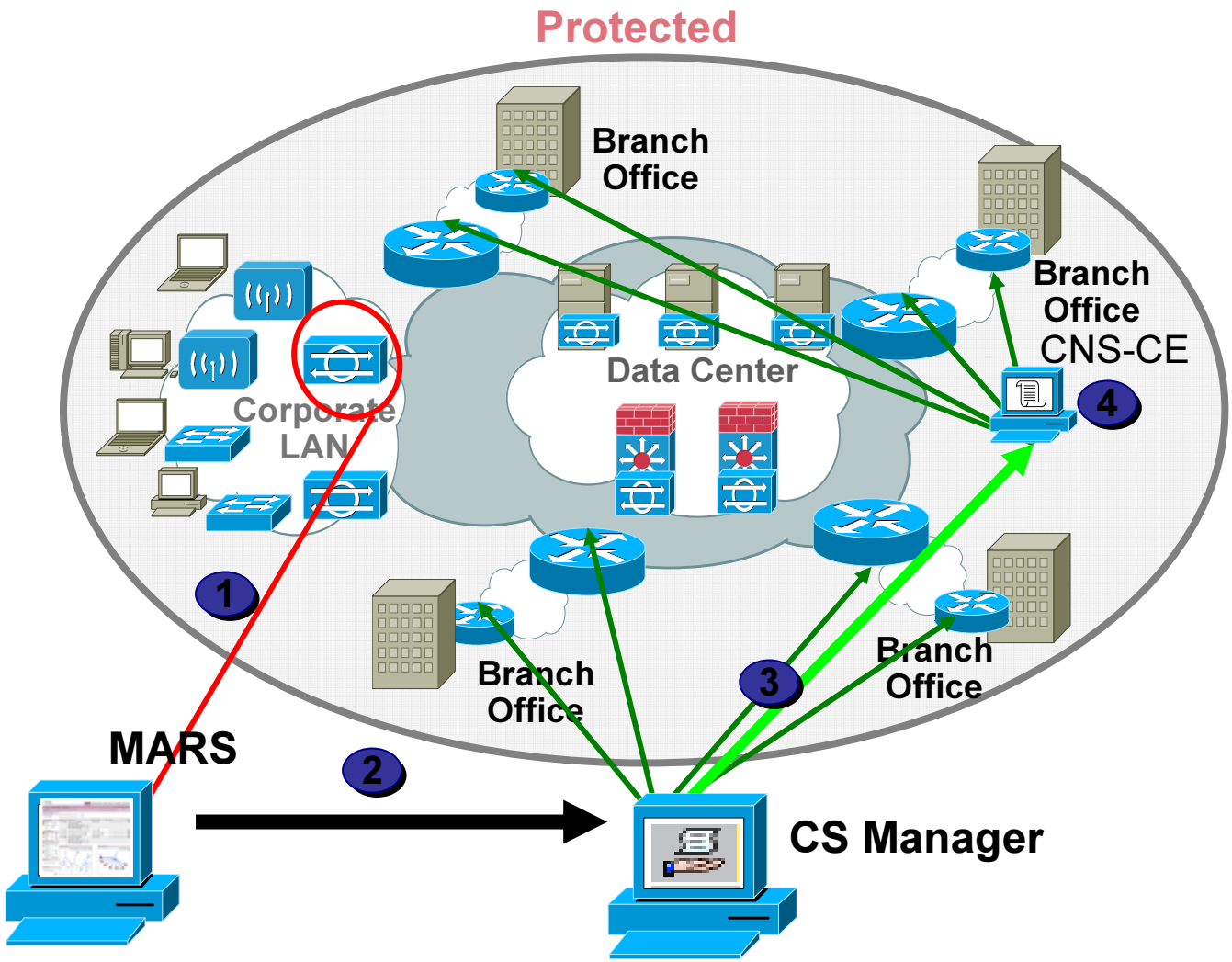
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1	(	ANY	SAME, $TARGET01, ANY	ANY	Probe/HostInfo/All, Probe/ServerInfo/Web, Penetrate/ViewFiles/DirTraversal/Web, Penetrate/GuessPassword/WebServer, Penetrate/ViewFiles/Sensitive, Penetrate/SpoofIdentity/TCPIP	ANY	None	ANY	ANY	1		FOLLOWED-BY

Examples of Good Places to Start With:

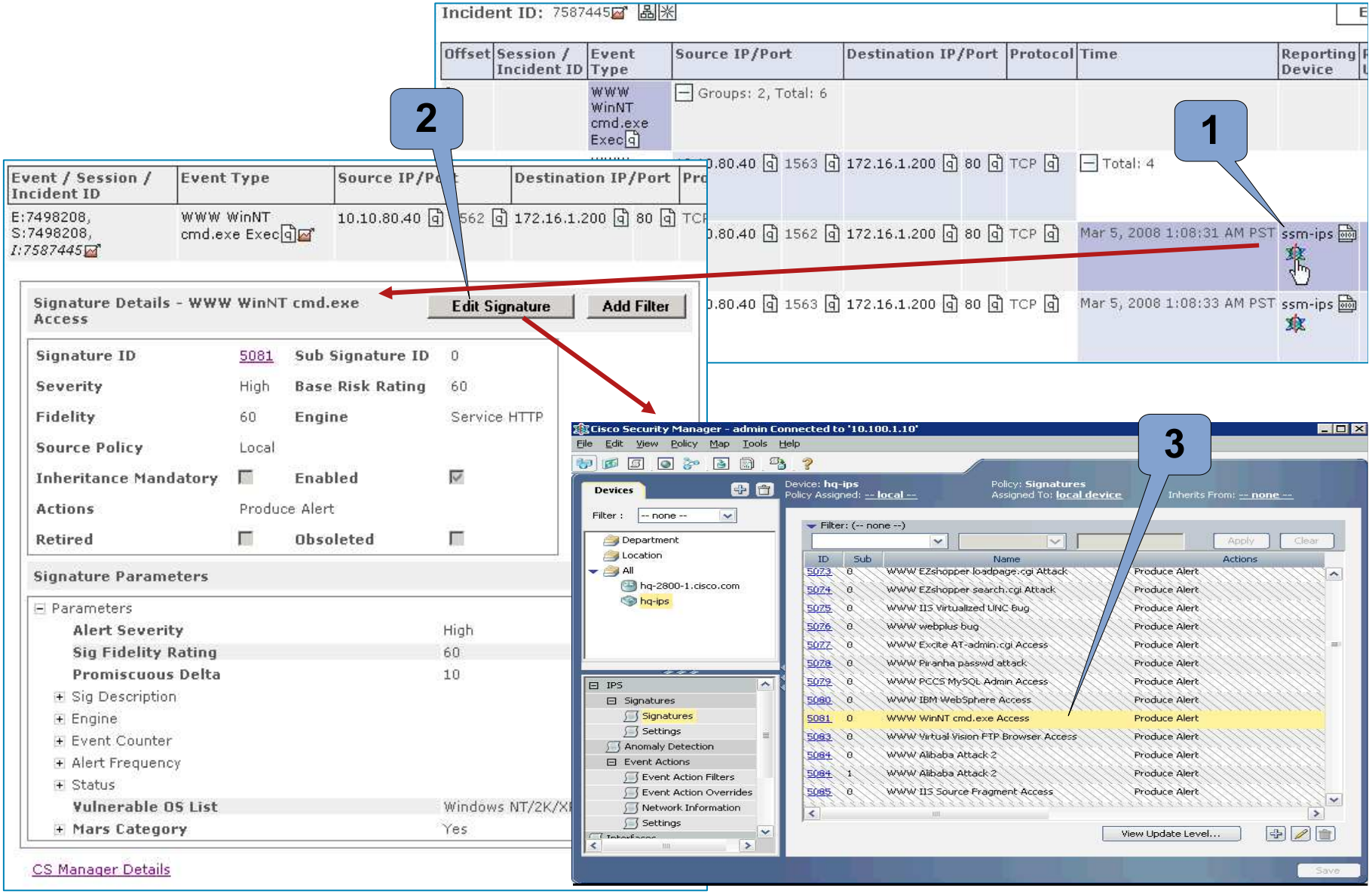
- Excessive denies from the same src
- Worm propagation
- Excessive e-mail from the same src (tune it to != e-mail servers)
- Sudden increase of traffic (set Netflow valid networks to your inside network)

Distributed Protection
CS MARS and CS Manager in Action

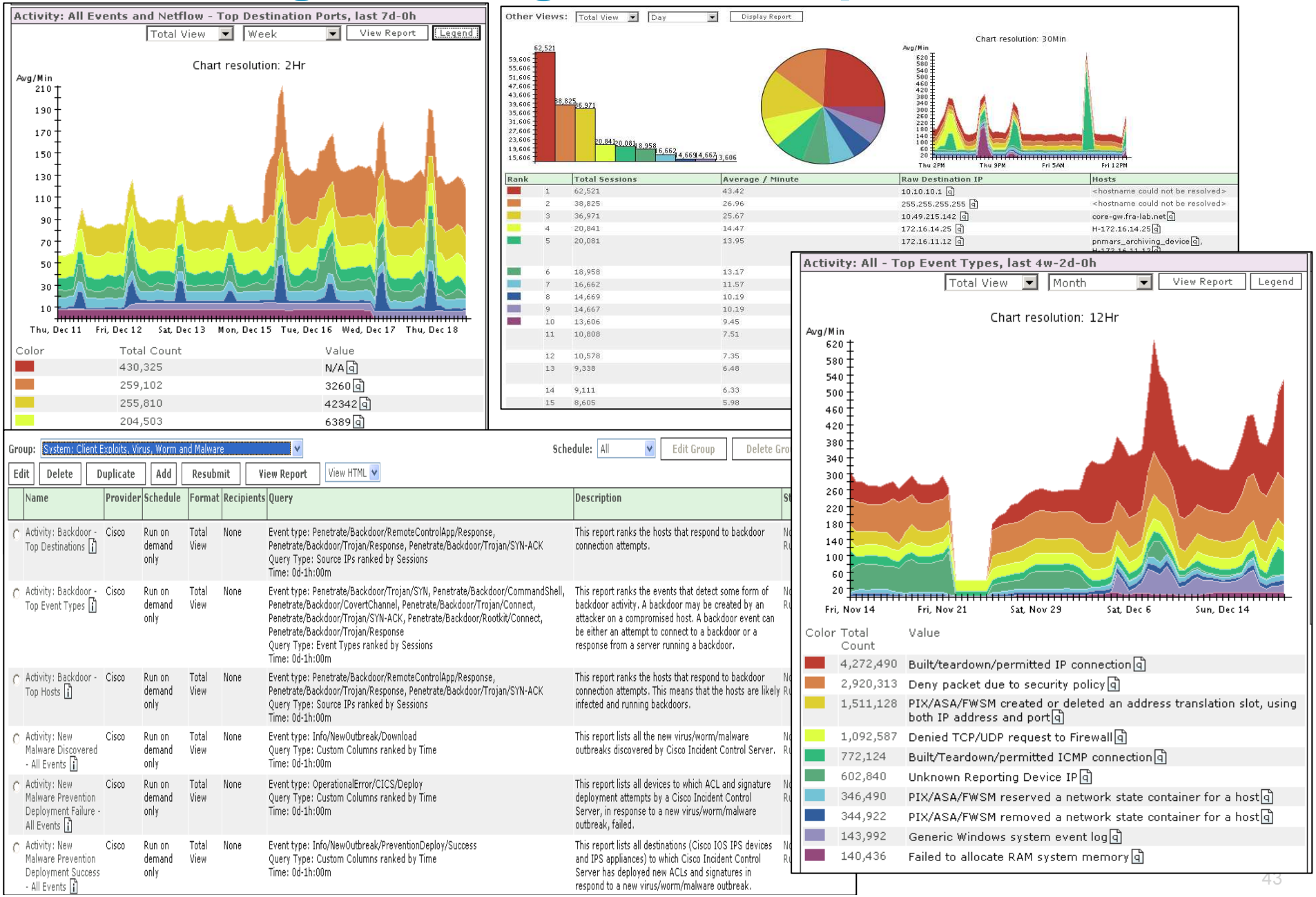
- MARS detects an attack or network issue with mitigation point
- In CS-Manager an Administrator updates a shared policy in one place
- Policy deployed to all appropriate devices



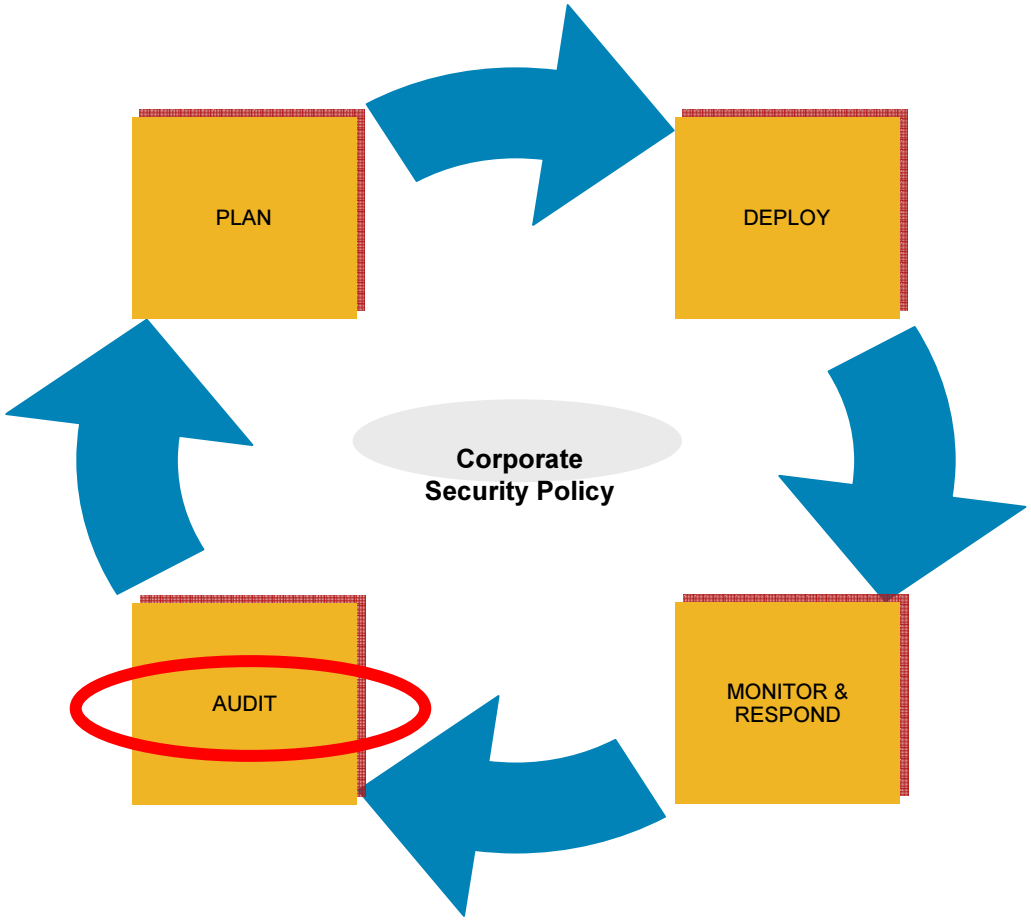
Device Tuning: Events to Policy Editing



Trending and high level Reports



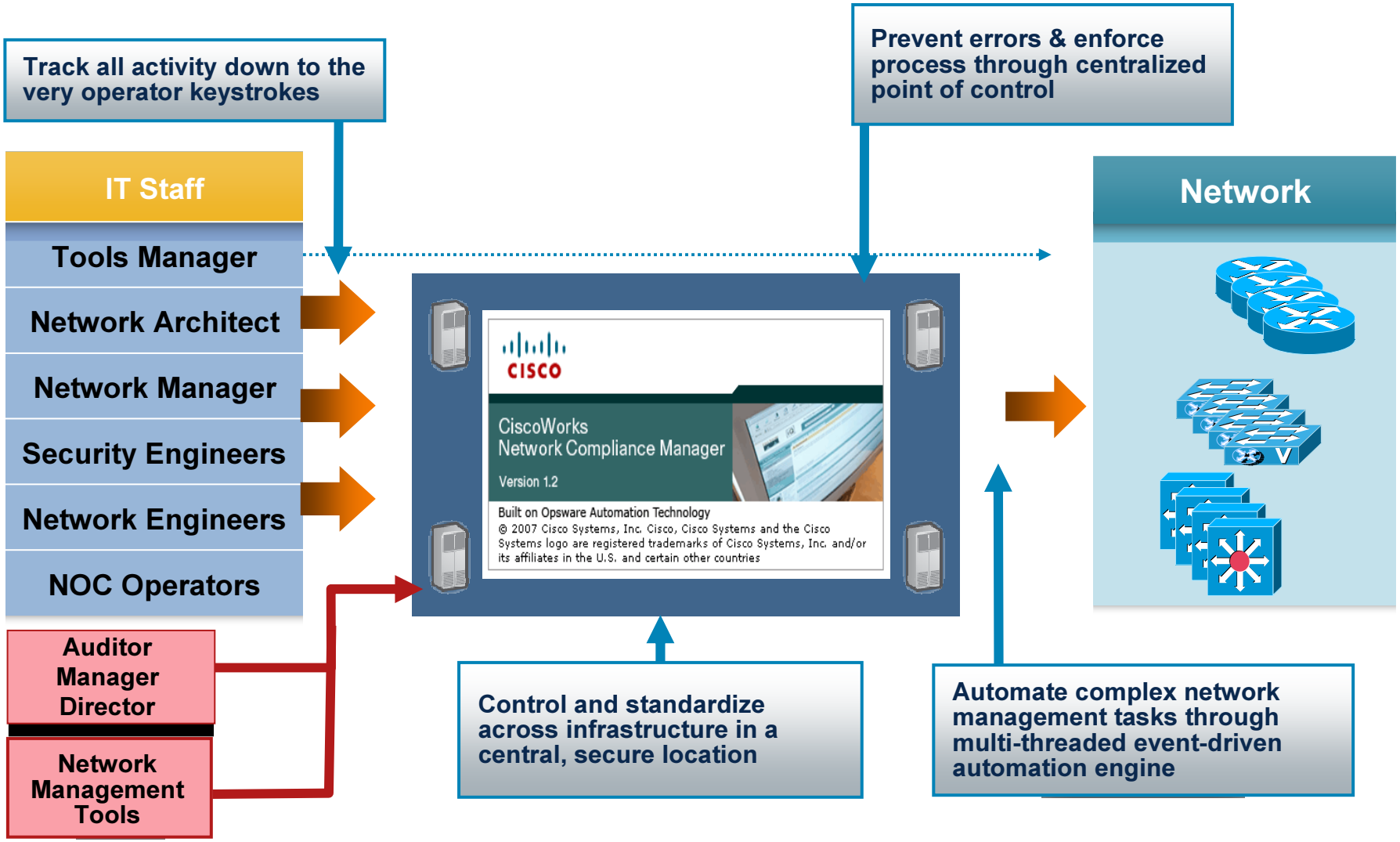
Agenda



Regulatory Compliance Requirements

- ***Assessment -*** Companies must assess the IT information security levels within their organization.
- ***Remediation -*** After the assessment, organizations must bring the various IT systems in line with the established security standards. This includes action plans for providing adequate information security.
- ***Enforcement -*** Companies must establish and enforce processes to ensure security standards are met. This includes things like plans for continuity of operations for information system resources in case of disaster and procedures for detecting and responding to security incidents.

Fully automated network configuration and change management (NCCM)



CiscoWorks Network Compliance Manager (NCM) Overview

A highly scalable, multi-vendor offering for centralized network compliance management

Best-in-breed Network Configuration and Change Management (NCCM)

- Real-time change detection
- Pre-deployment validation
- Policy enforcement

Sophisticated Audit and Compliance Analysis

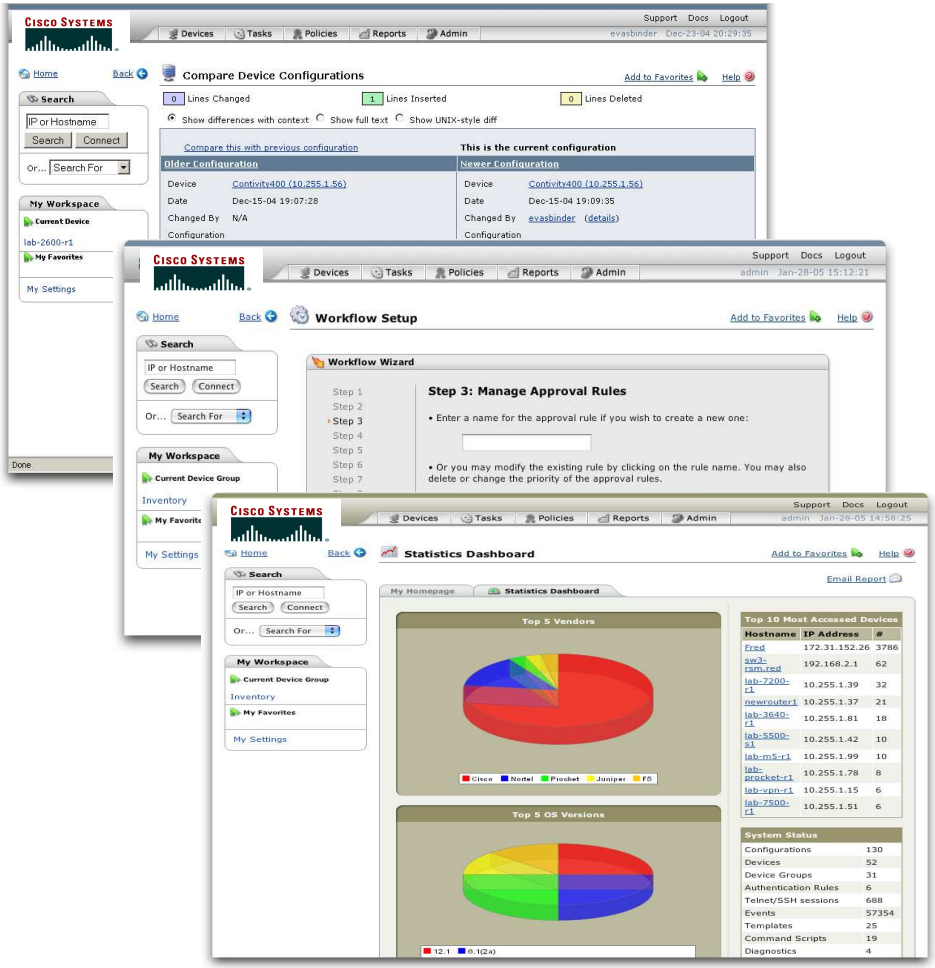
- Set policy to track compliance
- Automated generation of compliance reports (SOX, VISA CISP, HIPAA, GLBA, ITIL, CobiT, COSO)

Advanced Workflows

- Model complex projects
- Define custom approval policies

Extensive Reporting

- Network status
- Compliance



CiscoWorks NCM Features - 1

Key Features	Benefits
Network discovery & inventory import	Elimination of manual administration of devices
Network diagram	Easy visualization of topology Facilitation of troubleshooting
Configuration & change management	Maximized uptime Easy audit of configuration changes
Audit & compliance management	Easy modeling of regulatory, corporate, IT, technology policies Visibility into network's compliance with policies Identification of critical risks and violations Prioritized triage of compliance violations

CiscoWorks NCM Features - 2

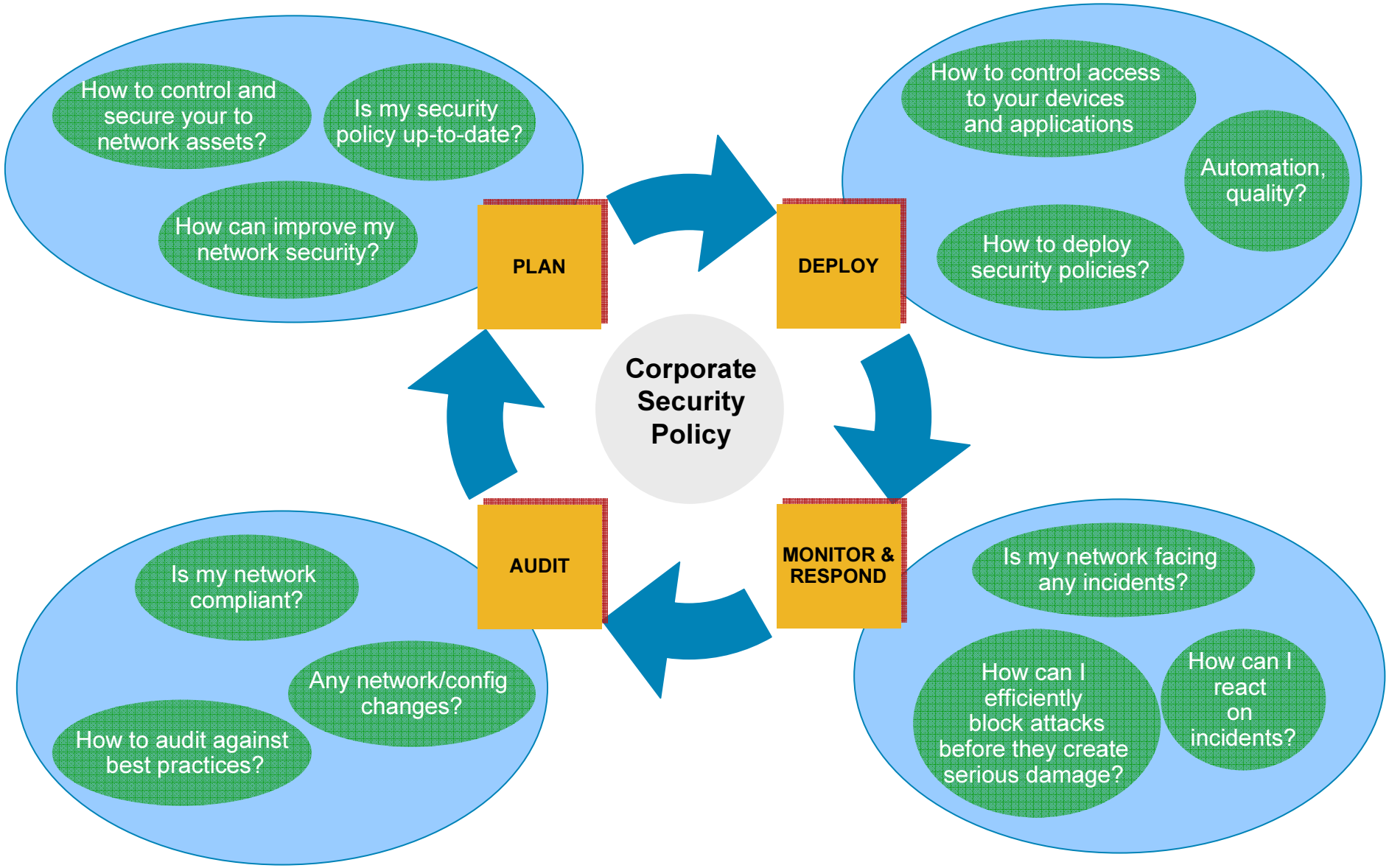
Key Features	Benefits
Integration with CiscoWorks applications	Easy cross launch of CiscoWorks NCM and CiscoWorks LMS Consistent network database via Device Credential Repository (DCR) Combination of network configuration, change, compliance, Cisco IOS/CatOS image management
Security management	Role-based access control and lock down Centralized ACL management
Advanced workflow and approvals	Close the change loop with real-time process enforcement
Multivendor support	Thousands of device models/versions supported out of the box across Cisco and 35 other vendors Object-oriented driver architecture enables rapid driver development Frequent driver releases

NCM Benefits

Manual Configuration	Automated Configuration
▪MTTR from configuration error: **150 minutes**	▪MTTR from configuration error: 15 minutes
▪Outages & security incidents due to manual mis-configurations: **80%**	▪Outages & security incidents due to manual mis-configurations: 20%
▪Average time to discover security vulnerability: **2 weeks**	▪Average time to discover security vulnerability: Less than 2 minutes
▪Provision new device: **6 hours**	▪Provision new device: 20 minutes
▪Changes per hour: **20**	▪Changes per hour: 5,000
▪Average amount of network in compliance: **3%**	▪Average amount of network in compliance: 100%

Source: 2005 EMA Survey and customer feedback

Security Management Life Cycle



26. April 1986, Tschernobyl

Security Policy is a must !!!

power plant control center

Security Management is a must !!!