

Experience Today the
Network of Tomorrow.

Cisco Expo
2009

Operational Firewall and IPS
Management
Using Cisco Security Manager
and Cisco Security MARS



Nadhem J. AlFardan
Consulting Systems Engineer

Welcome to the Human Network.



- Security Management Challenges
- Security Provisioning with Cisco Security Manager – Some Best Practices
- Security Monitoring with Cisco Security MARS – Some Best Practices
- Incident investigation – Two Examples

Security Management Challenges

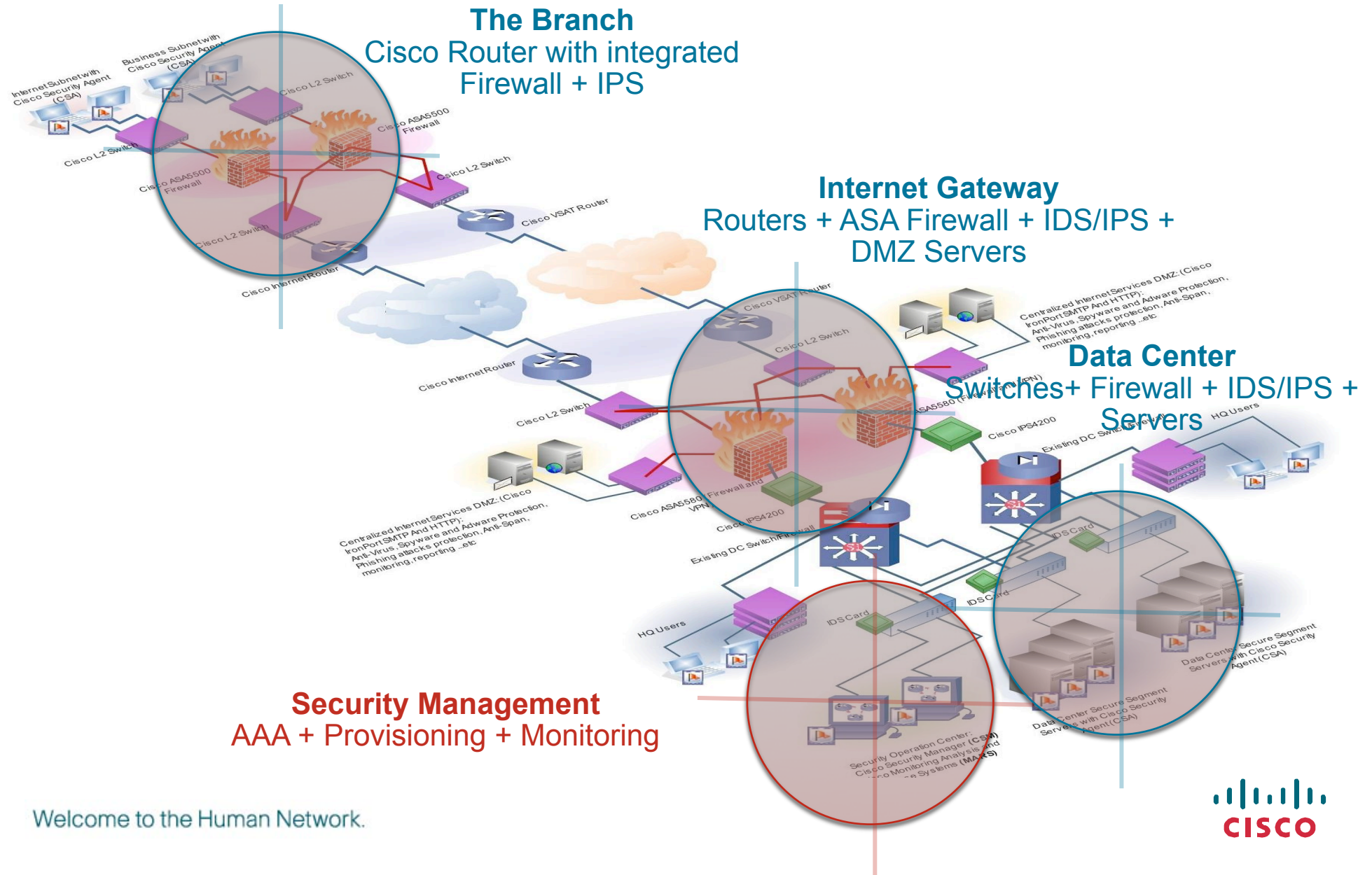


Cisco Expo
2009

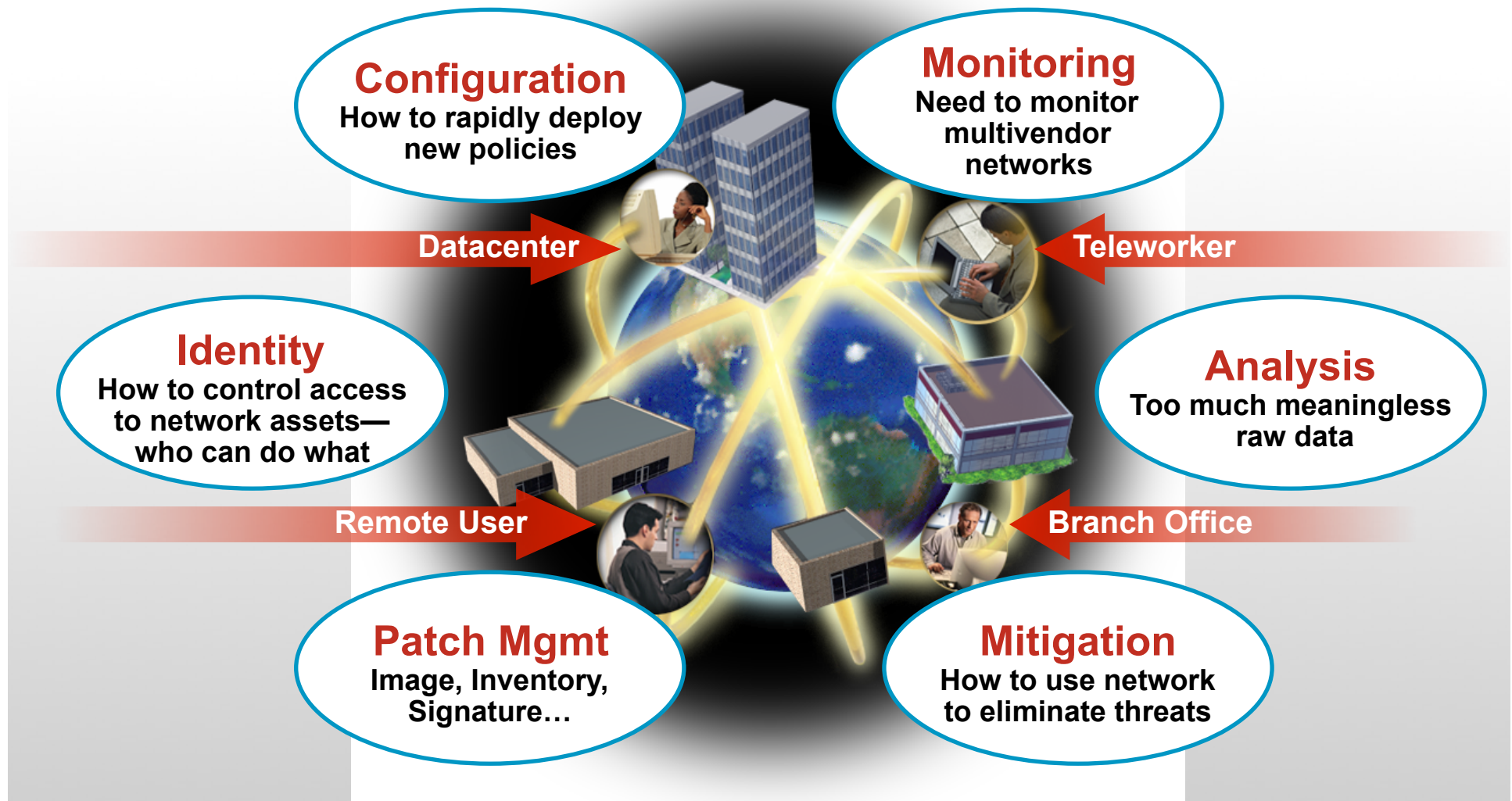
Welcome to the Human Network.



Cisco Expo 2009 The Challenge of Managing Security



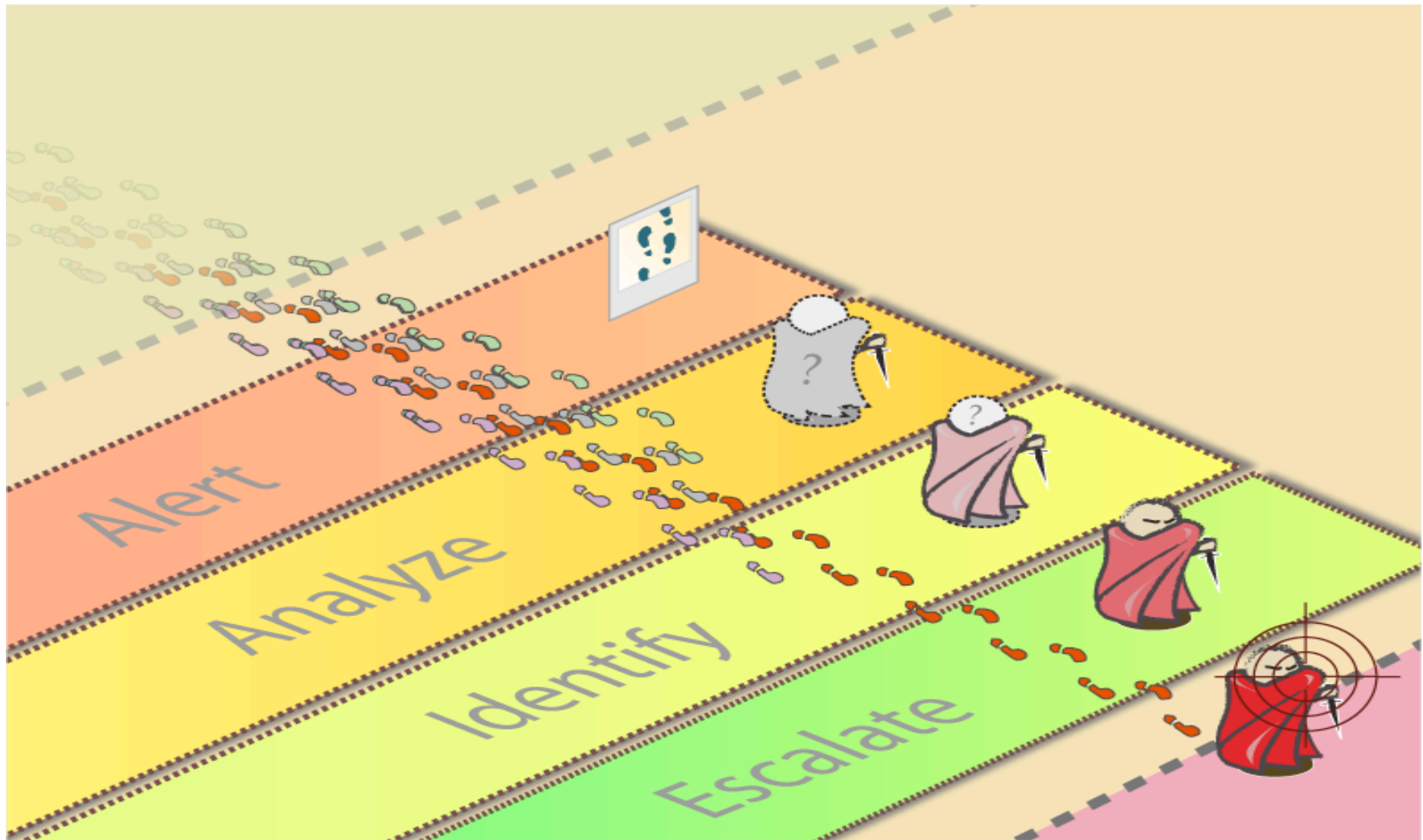
The Challenge of Managing Security



I Drive Fast .. How fast !!

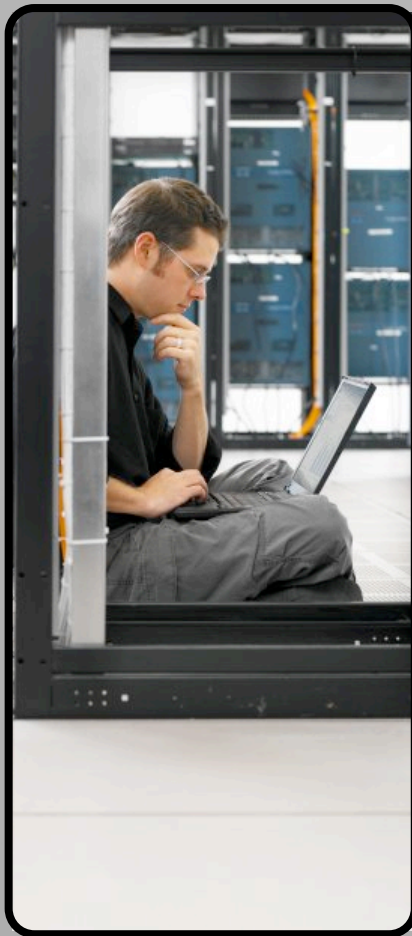


Processes from only footprints to ?



Welcome to the Human Network.

What's in the mind of an admin !



Today's network environments are comprised of:

- Various products with their own specific configuration interfaces
- High log volume from network devices
- Security events and alarms from disparate network elements
- Separate security policy management and information management systems
- Lack of integrated reporting

Addressing the Challenges



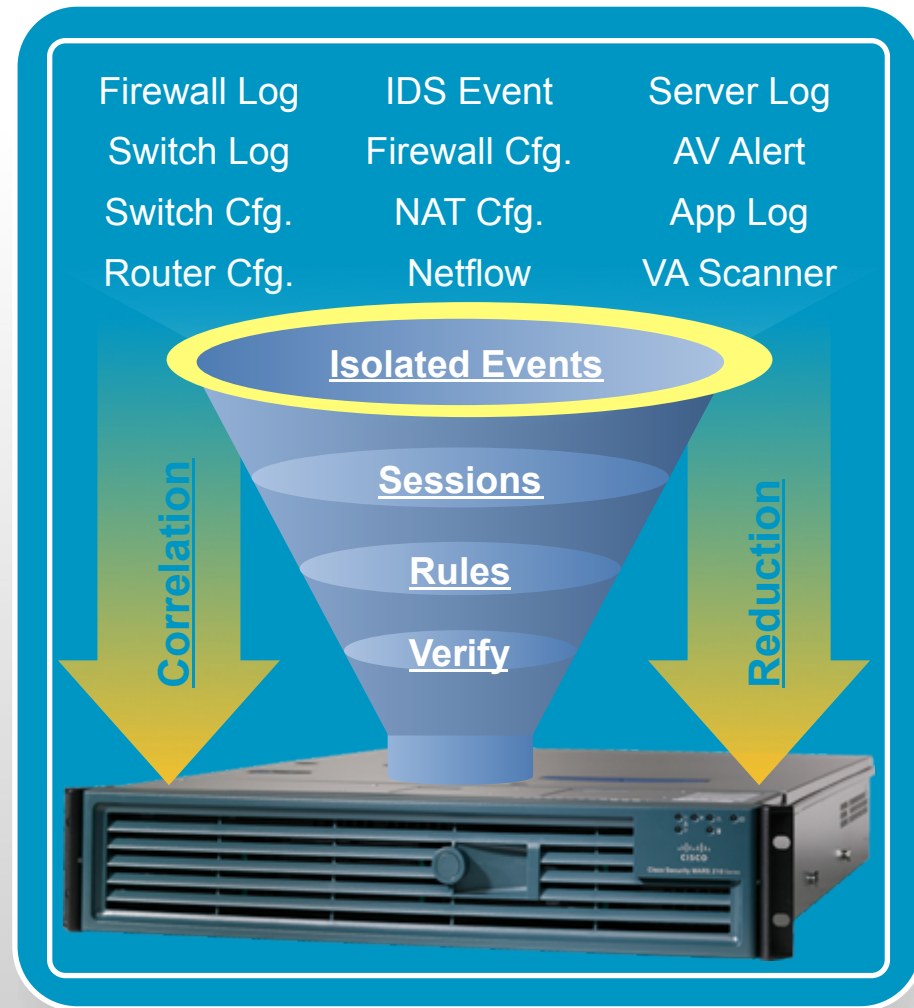
**Effective risk analysis and operational
control**

Cisco Security Manager (CSM)

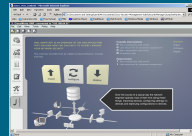


- Unified services management for security including firewall, IPsec VPN, SSL VPN, and IPS
- Different views for different administrative preferences
 - Device View
 - Topology View
 - Policy View
- Efficient management architecture for large-scale security deployments

- MARS is an acronym = Monitoring, Analysis, and Response System
- Security threat mitigation appliance
- Rapid threat detection, isolation and mitigation, topologically aware
- Command and control for your existing network security
- Correlates data from across disparate multi-vendor security devices and applications



Cisco Security Manager



Simplified **Policy Administration**

End-to-End
Configuration

Network-Wide or
Device-Specific

Cisco Security Mars



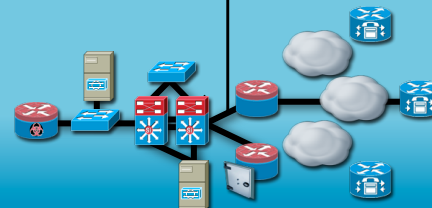
Rapid **Threat Identification**
and Mitigation

Topology
Awareness

Data Correlation

Configuration
Provisioning

Monitoring
Analysis
Mitigation



Self-Defending Network

- Integration to Cisco Secure Access Control Server
 - Role-based access control
 - Privilege-based access to management functionality
- With the context of auditing services

Security Provisioning Some Best Practices



Cisco Expo
2009

Welcome to the Human Network.



Provisioning Requirements

- Scaling from tens to many thousands of devices
 - Efficiency in distributing changes to connected and non connected devices
 - Make device settings common across devices
- Standardize on common policy, constructs and controls
 - Setting corporate rules and enforcing best-practice guidelines
 - Enabling SecOps and NetOps to work together
 - Controlling who can do what on which device
- Abstract polices from device implementation
 - Reducing the complexity of different device types

Best Practice Requirement

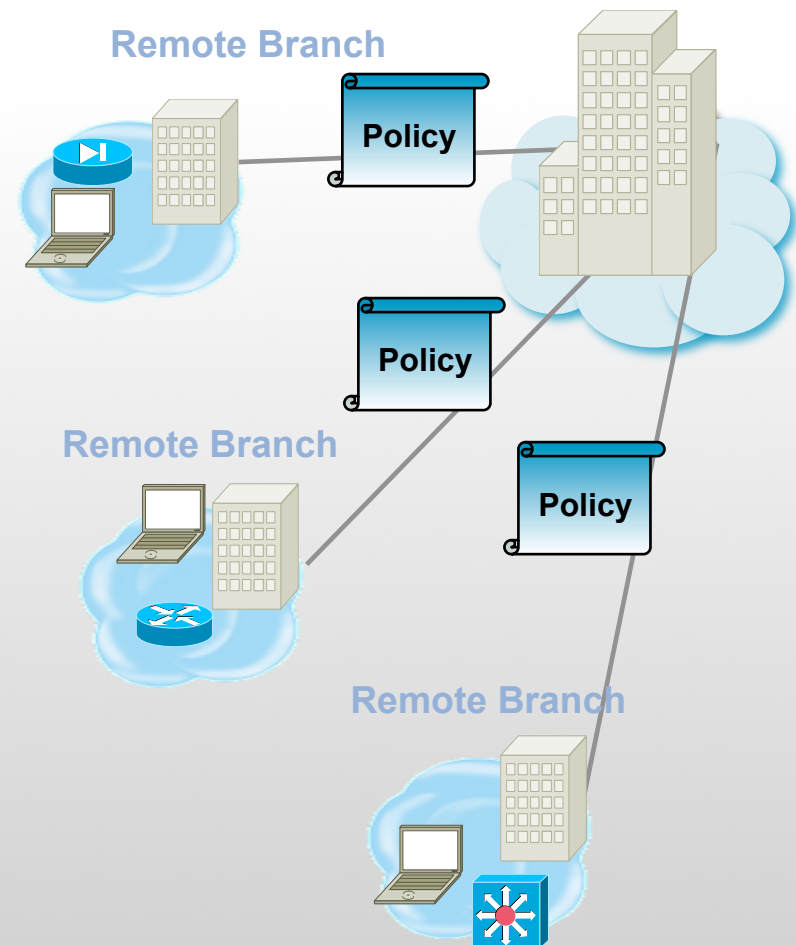
- Share policies across security platforms
- Branch level customization

Example

- For retail or multi-branch +90% policies are the same
- Minor differences at local branch level
- Strive broad commonality
- Allow admin to override policy to meet local branch needs

Benefit

- Maintain consistency with a single policy view leading to simplification
- Roll out new services to all branches with a single policy operation
- Reduce time and effort for adds moves and changes



Policy Hierarchy and Inheritance

Best Practice Requirement

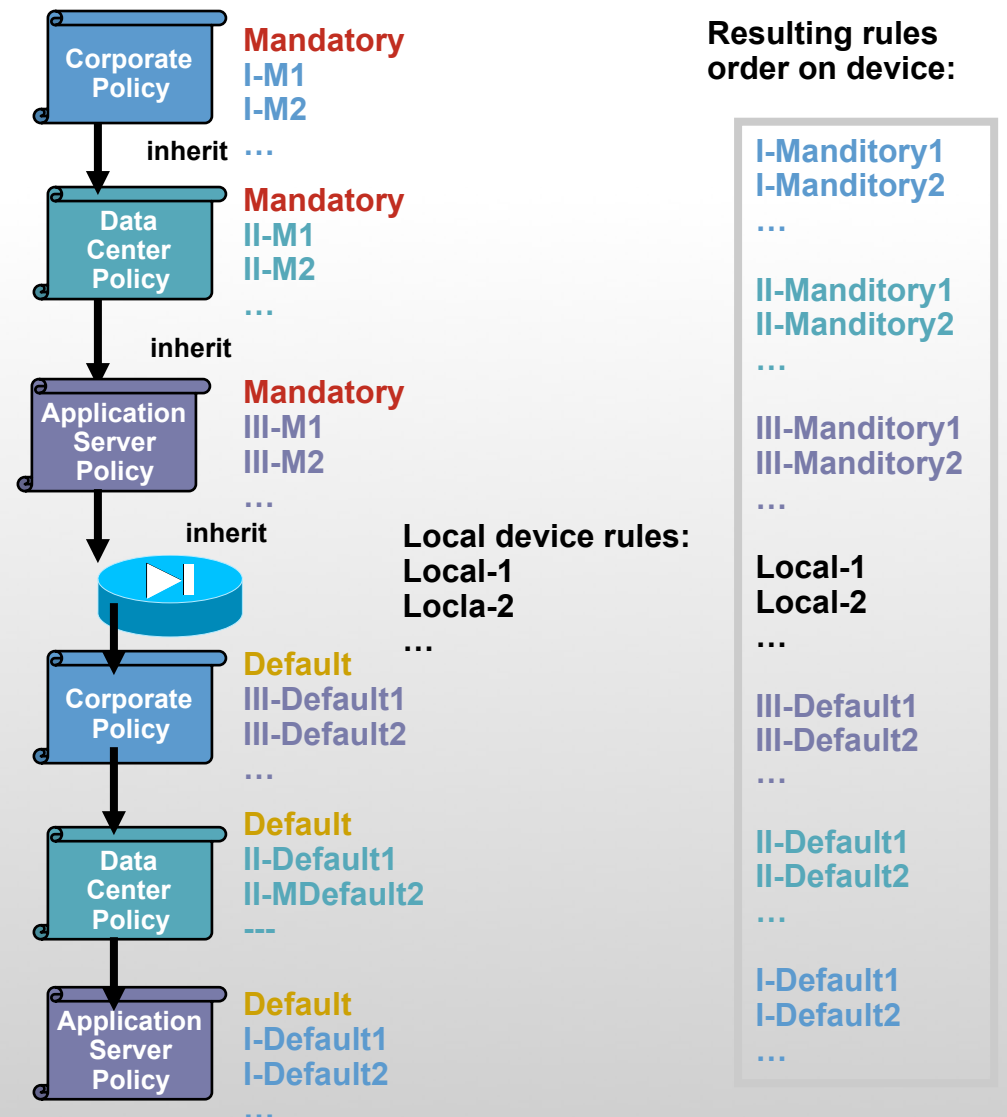
- Enable IT to create mandatory policies that are enforceable with minimum effort
- Options to make it user customizable

Example

- No IM file transfer, period
- Allow SSH, SSL

Benefit

- Organizational fit
- Cooperative behavior
- Organization level control
- Reduce time to introduce new devices



Workflow

Best Practice Requirement

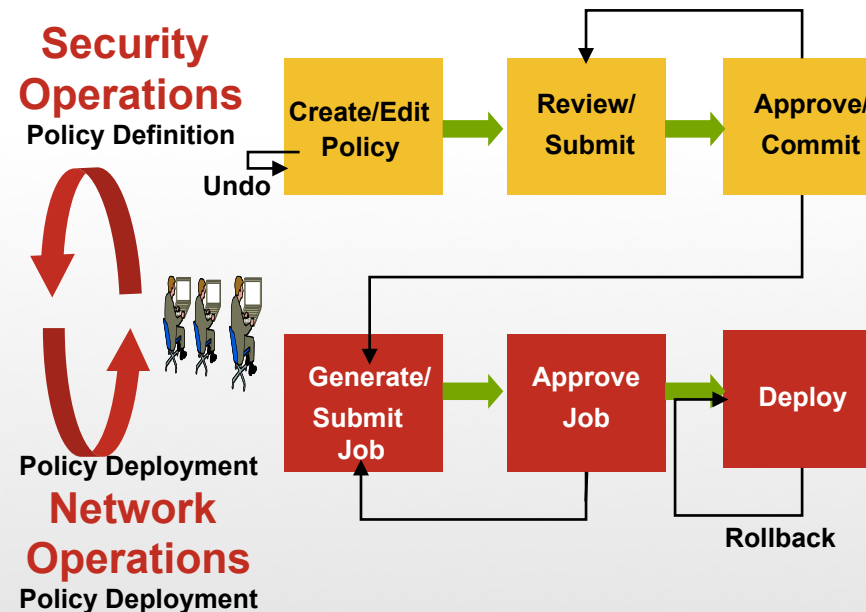
- Allow NetOps and SecOps to work as a team
- Workflow for deployment with approvals at each stage

Example

- All policy changes need to be approved
- Deployment to the network must be during the change window

Benefit

- Enables teamwork and collaboration between NetOps and SecOps
- Increased network uptime



- Who can modify device configs?
- Who can view changes?
- Who can approve changes?
- Who can deploy changes to devices?

Role Based Access Control **Best Practice Requirement**

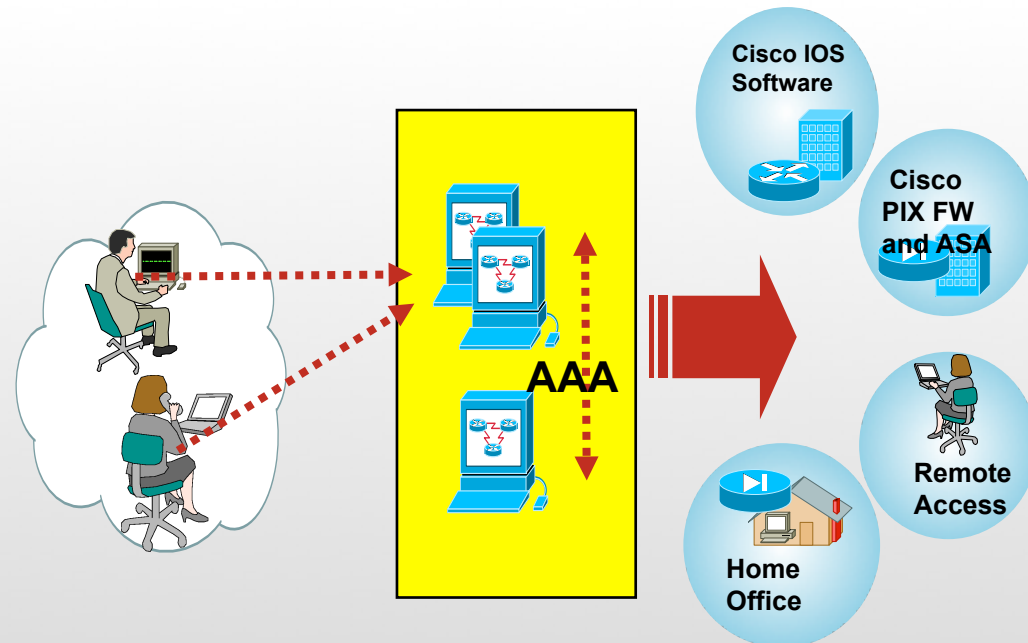
- Authenticate admin access to management system
- Determine who has access to specific devices and policy functions

Example

- Verify admin and associate them to specific roles as to who can do what

Benefit

- Enable delegation of admin tasks to multiple operators
- Provides appropriate separation of ownership and controls



Security Monitoring Some Best Practices



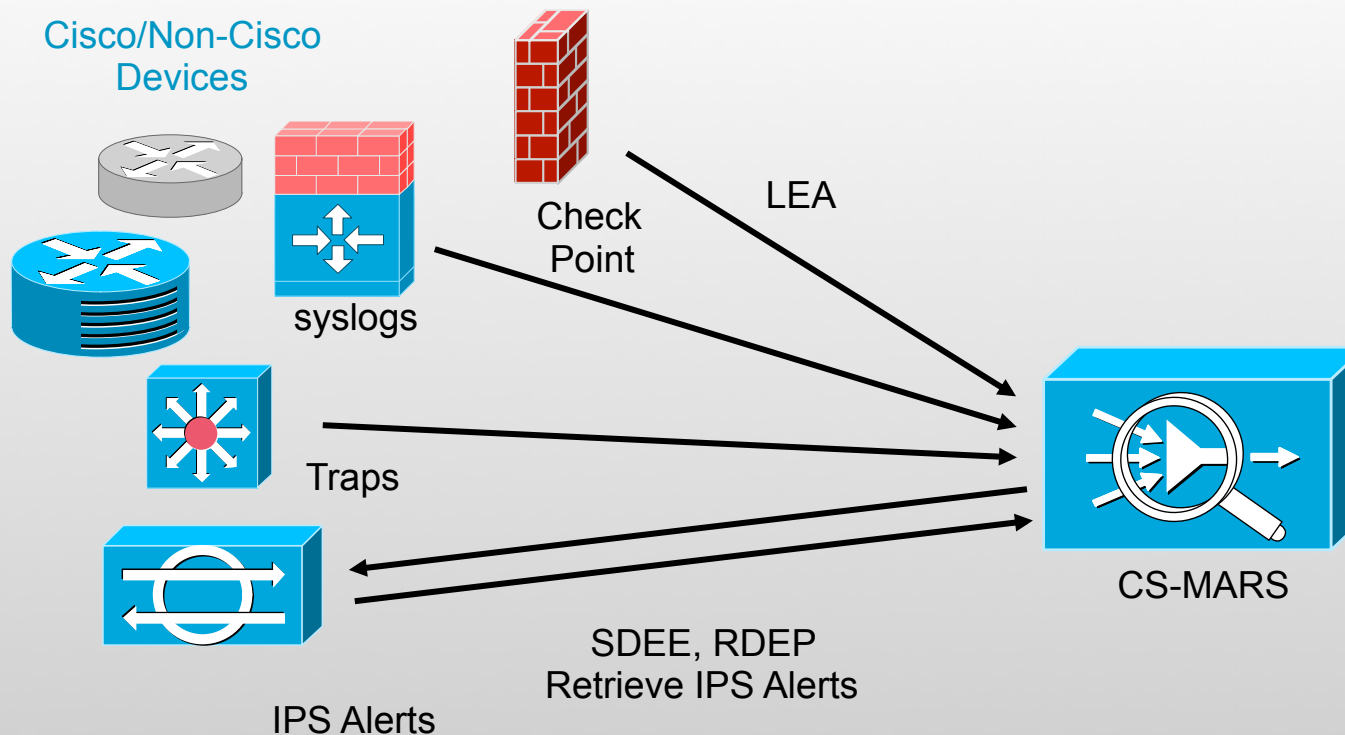
Cisco Expo
2009

Welcome to the Human Network.

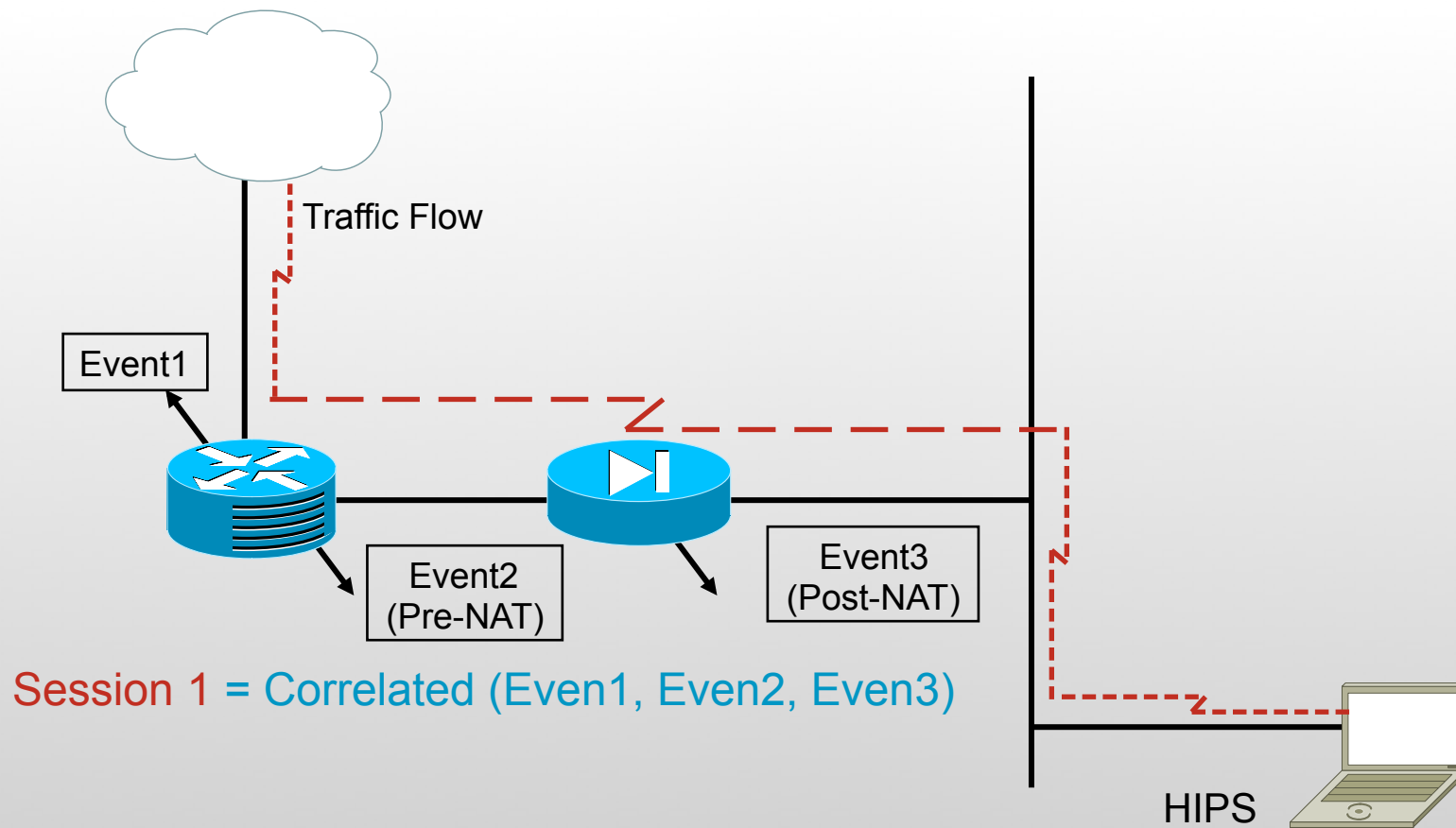


Key Concepts—Events

- Events—Reporting devices send raw messages (syslogs, traps...) to CS-MARS or CS-MARS retrieves raw messages (IPS alerts, Windows log....) from the reporting devices and maps the raw messages into events

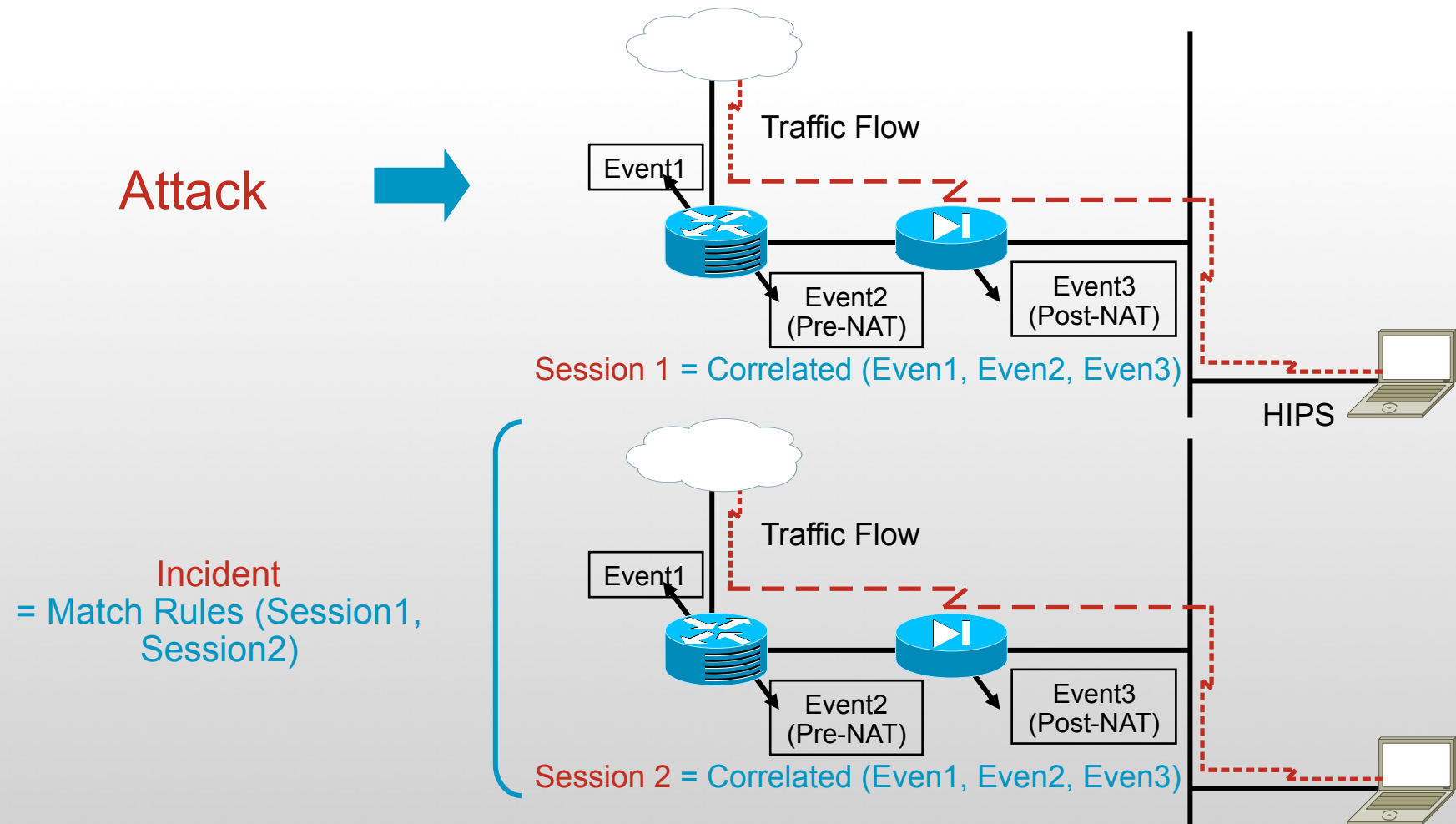


- Sessions—CS-MARS correlates events in sessions (for example, across NAT boundaries)



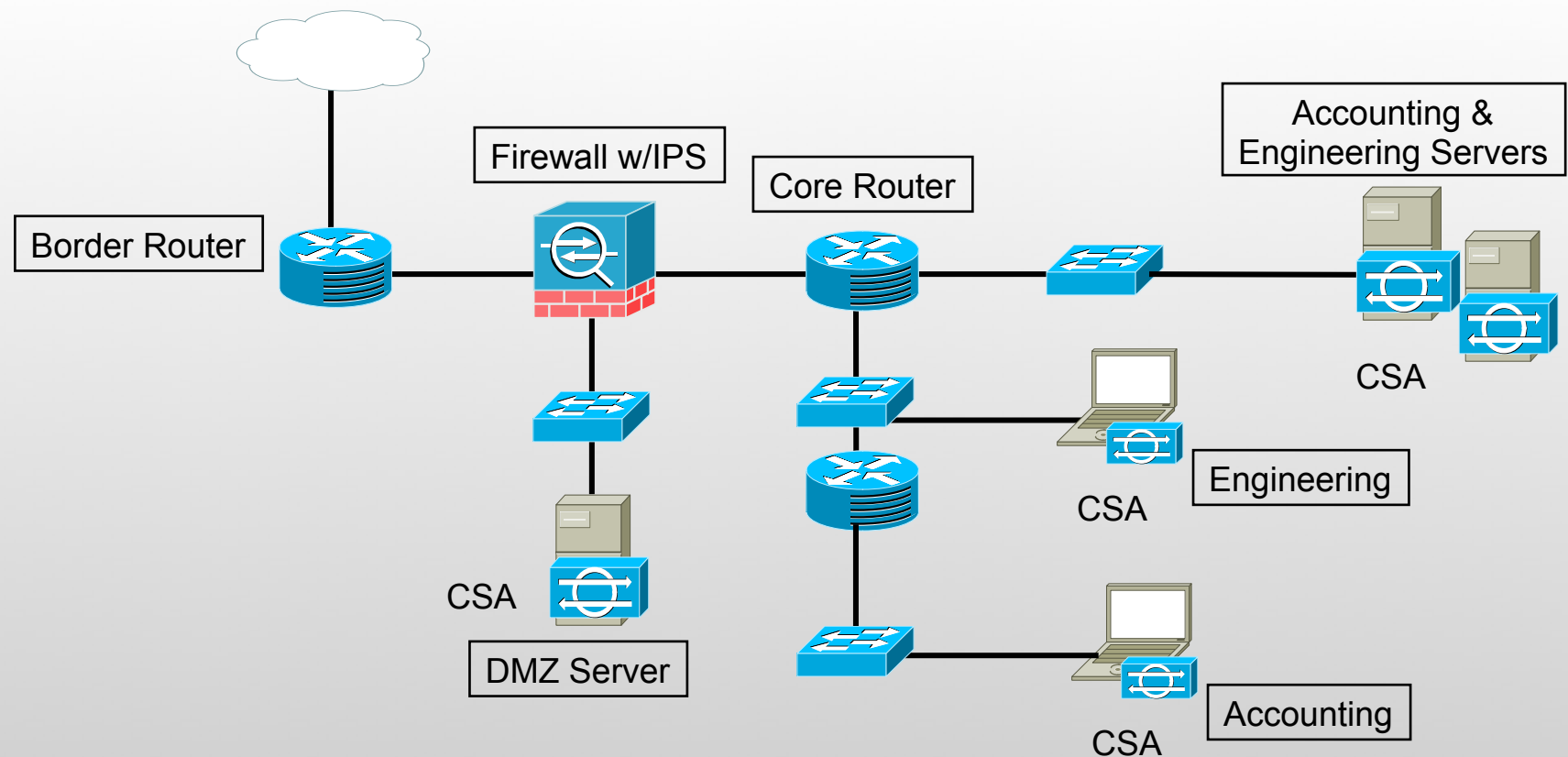
Key Concepts—Incidents

- Incidents—Rules fire to create incidents



What to Monitor

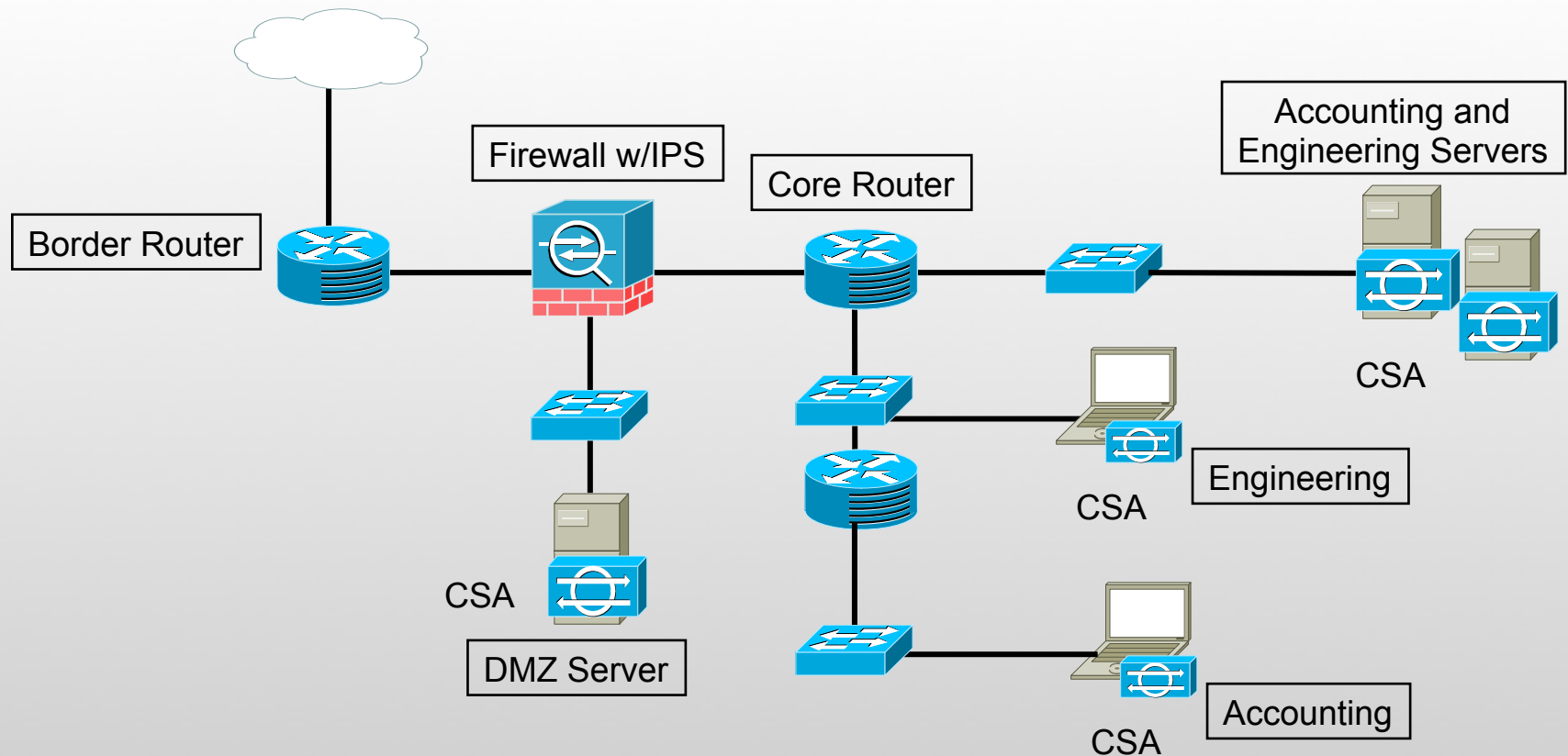
- The engineer must decide what devices to report to CS-MARS



-
- The diagram illustrates a network architecture with the following components and connections:
- Cloud:** Connected to the **Border Router**.
 - Border Router:** Connected to the **Firewall w/IPS**.
 - Firewall w/IPS:** Connected to the **Core Router**.
 - Core Router:** Connected to a switch, which is connected to the **Accounting and Engineering Servers**.
 - Core Router:** Connected to a switch, which is connected to the **DMZ Server**.
 - Core Router:** Connected to a switch, which is connected to a **laptop (Engineering)** and a **laptop (Accounting)**.
- Each server and laptop is associated with a **CSA** (Content Security Agent) icon.

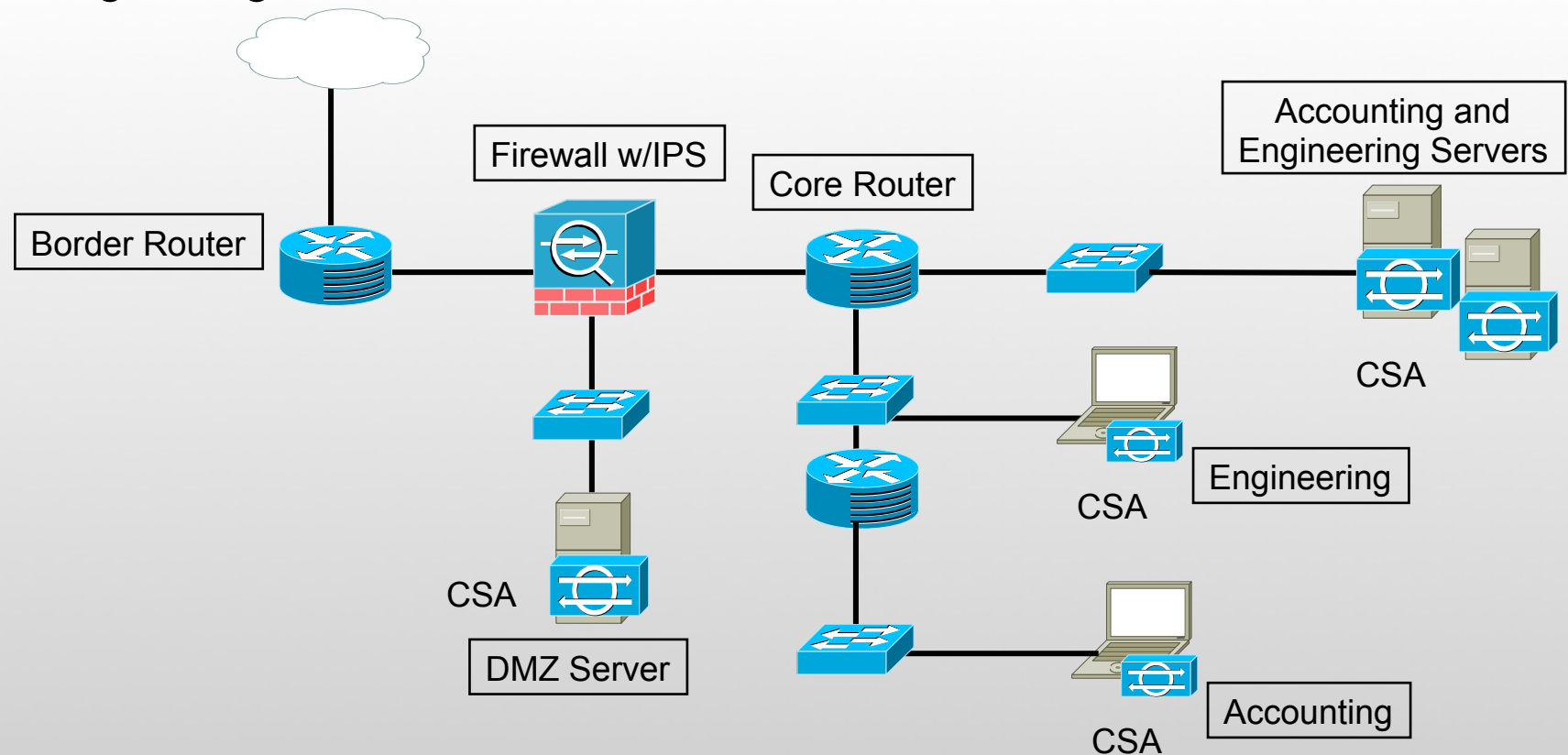
What to Monitor: Firewall

- Will monitor firewall to follow NATed traffic
- Wants to know whenever firewall configuration changes



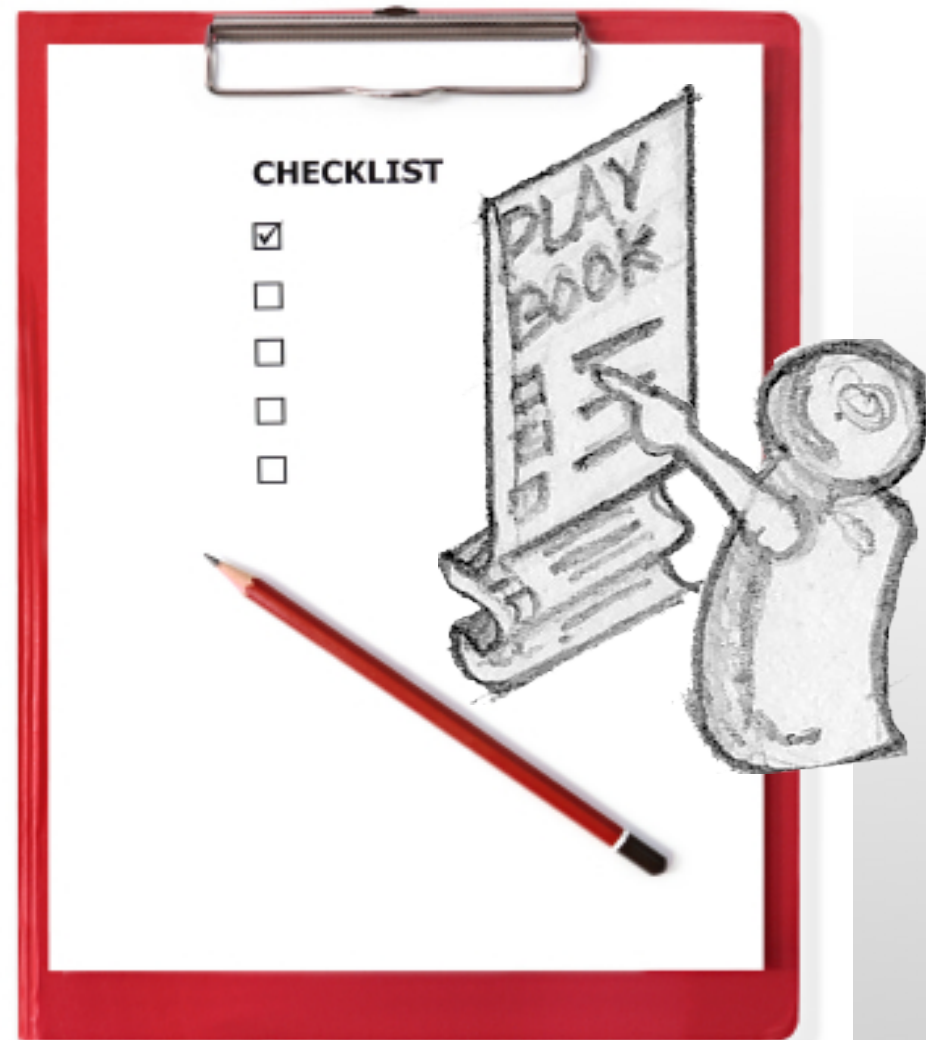
What to Monitor: DMZ

- Will monitor DMZ servers to watch for attacks
- Will monitor DMZ switch to enable layer 2 mitigation and monitor config changes



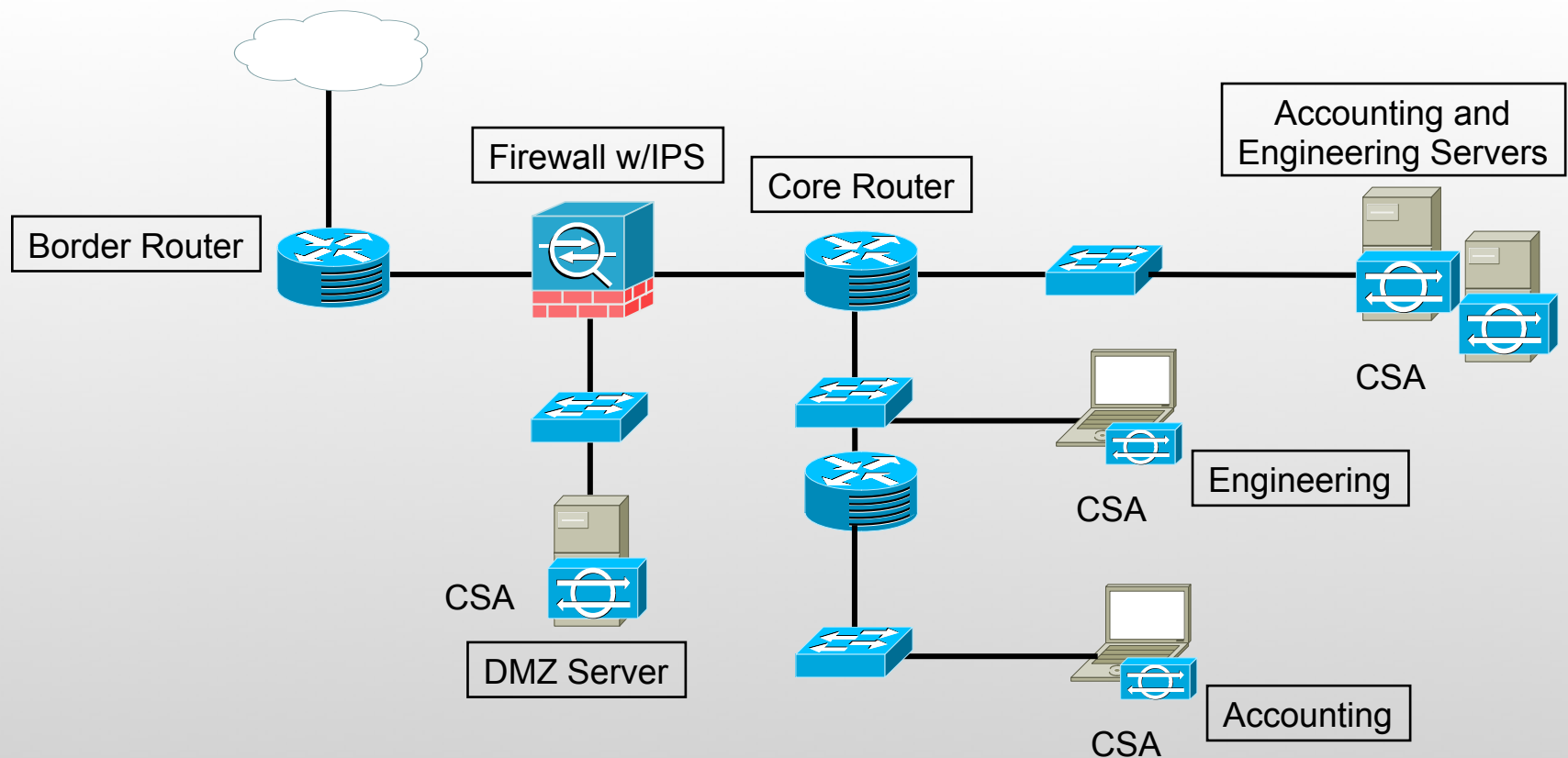
-
- The diagram illustrates a network architecture with the following components and connections:
- Cloud:** Represented by a cloud icon at the top left.
 - Border Router:** A blue router icon connected to the cloud.
 - Firewall w/IPS:** A blue firewall icon with a red brick base, connected to the Border Router.
 - Core Router:** A blue router icon connected to the Firewall w/IPS.
 - Accounting and Engineering Servers:** A group of server icons connected to the Core Router.
 - DMZ Server:** A server icon connected to a switch, which is connected to the Core Router.
 - Engineering:** A laptop icon connected to a switch, which is connected to the Core Router.
 - Accounting:** A laptop icon connected to a switch, which is connected to the Core Router.

Cisco Expo 2009 Build a Playbook .. Don't Just sit down !



What to Monitor: IDS Sensor

- Will monitor IDS sensor as best source of security events
- CS-MARS stays in sync with signatures through auto-update



Going through the live of an Incident investigation



Cisco Expo
2009

Welcome to the Human Network.

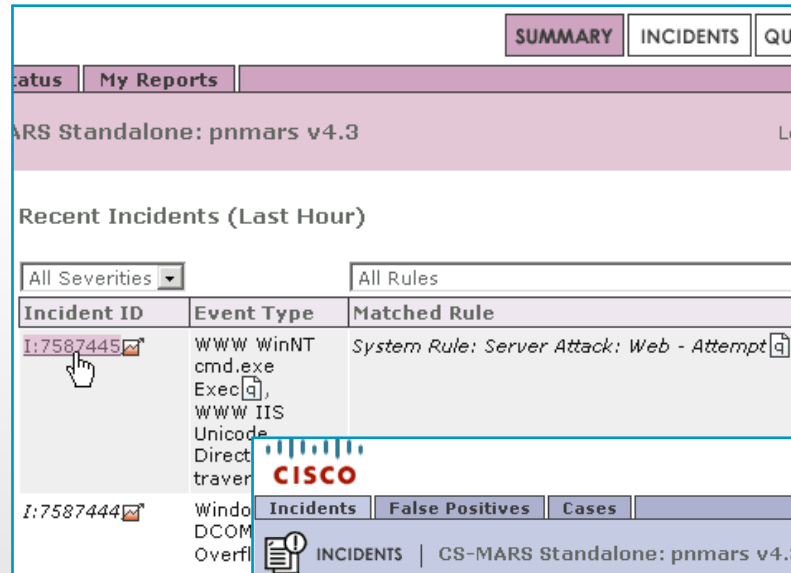


- Start from MARS
- Find an interesting incident
- Investigate the attack
- Review the mitigation
- Follow the linkage to CSM
- Update the policy

MARS → CSM

Example 1: IPS Event to Policy

1. Access CS-MARS from browser either – **Summary** or **Incidents**
2. Drill-down into the IPS incident.



Summary Incidents QUE

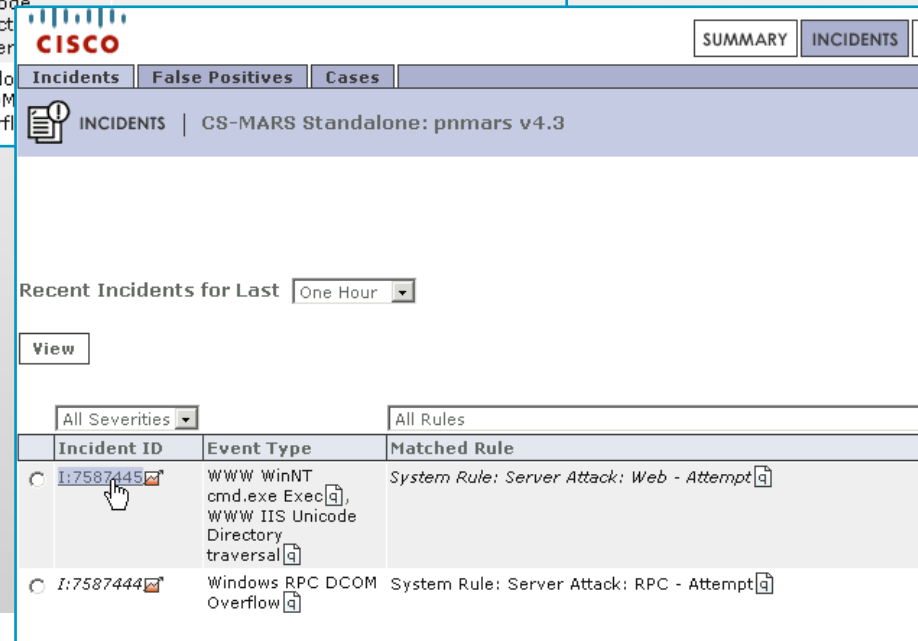
Status My Reports

CS-MARS Standalone: pnmars v4.3

Recent Incidents (Last Hour)

All Severities All Rules

Incident ID	Event Type	Matched Rule
I:7587445	WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal	System Rule: Server Attack: Web - Attempt
I:7587444	Windows DCOM Overflow	



Summary Incidents

Incidents False Positives Cases

INCIDENTS | CS-MARS Standalone: pnmars v4.3

Recent Incidents for Last One Hour

View

All Severities All Rules

Incident ID	Event Type	Matched Rule
<input checked="" type="radio"/> I:7587445	WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal	System Rule: Server Attack: Web - Attempt
<input type="radio"/> I:7587444	Windows RPC DCOM Overflow	System Rule: Server Attack: RPC - Attempt

Example 1: IPS Event to Policy

- Expand incidents and look for the reporting device, in this scenario is the **ssm-ips**
- Click into the CSM policy query icon.
- Another page may display multiple entries, select one of interest and click on the CSM icon.

Incident ID: 7587445

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device
3		WWW WinNT cmd.exe Exec	Groups: 2, Total: 6				
3		WWW WinNT cmd.exe Exec	10.10.80.40	172.16.1.200	TCP	Total: 4	
3	S:7498208, I:7587445	WWW WinNT cmd.exe Exec	10.10.80.40	172.16.1.200	TCP	Mar 5, 2008 1:08:31 AM PST	ssm-ips
3	S:7498212, I:7587445	WWW WinNT cmd.exe Exec	10.10.80.40	172.16.1.200	TCP	Mar 5, 2008 1:08:33 AM PST	ssm-ips

ssm-ips



Event / Session / Incident ID	Reporting Device	Time	Policy	Raw Message
E:7498209, S:7498208	ssm-ips	Mar 5, 2008 1:08:31 AM PST		0000 47 45 54 2 0010 63 30 25 6 0020 73 74 65 6 0030 2b 64 6 0040 31
E:7498208, S:7498208, I:7587445	ssm-ips	Mar 5, 2008 1:08:31 AM PST		10.10.80.40/1562 -- 5081/0,Time:12047

Example 1: IPS Event to Policy

6. MARS may request for CSM authentication, if so enter your CSM credentials. Check **Save Credentials***** to reuse the credentials for the session if needed.

*** **Credentials are only cached for the browser session**

Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device
10.10.80.40 [q]	1183 [q]	172.16.1.200 [q]	80 [q]	TCP [q]
			Mar 5, 2008 12:44:47 AM PST	ssm-ips [0101]

*User Name:

*Password:

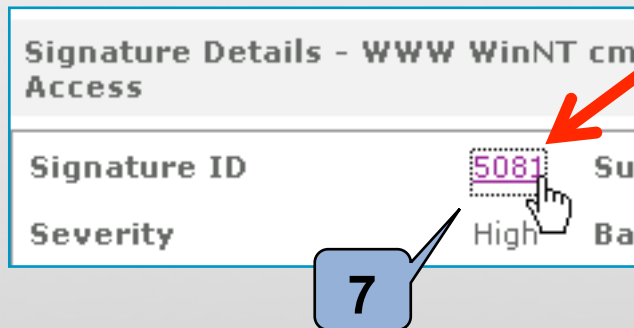
☒ Save Credentials

6

Example 1: IPS Event to Policy

MARS provides the full policy-query page, with greater details into the selected incident → signature.

7. Click into the **Signature ID**



Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol
E:7498208, S:7498208, I:7587445	WWW WinNT cmd.exe Exec	10.10.80.40 1562	172.16.1.200 80	TCP

Signature Details - WWW WinNT cmd.exe Access

[Edit Signature](#) [Add Filter](#)

Signature ID	5081	Sub Signature ID	0
Severity	High	Base Risk Rating	60
Fidelity	60	Engine	Service HTTP
Source Policy	Local		
Inheritance Mandatory	<input type="checkbox"/>	Enabled	<input checked="" type="checkbox"/>
Actions	Produce Alert		
Retired	<input type="checkbox"/>	Obsoleted	<input type="checkbox"/>

Signature Parameters


Parameters

Alert Severity	High
Sig Fidelity Rating	60
Promiscuous Delta	10
Sig Description	
Engine	
Event Counter	
Alert Frequency	
Status	
Vulnerable OS List	Windows NT/2K/XP
Mars Category	Yes

[CS Manager Details](#)

Example 1: IPS Event to Policy

MARS cross-launch to Cisco
Security Center's **IntelliShield**
to provide latest signature detail.


Worldwide [change]

Solutions	Products & Services	Ordering	Support	Training & Events	Partner Central
-----------	---------------------	----------	---------	-------------------	-----------------

[HOME](#)
[Security Center](#)

[ABOUT CISCO](#)

Benign Triggers

Host sweep signatures 3030 and 3032 detect behaviors that should not be observed from sources outside the local network but are normal behaviors for sources from within the local network.

IntelliShield Event Responses	Release: S109 (download)	Fidelity: 100
Cisco IPS Signatures	Original Release Date: August 16, 2004	
Cisco IPS Active Update Bulletins	Latest Release Date: August 16, 2004	
Self-Defending Network Case Studies	Default Enabled: True	
Technical White Papers	Default Retired: False	
Cisco Emergency Response	Description Triggers when the use of the Windows NT cmd.exe is detected in a URL.	
Technical Resources	Recommended Filter	
Security Intelligence RSS		

Example 1: IPS Event to Policy

8. Return to the MARS policy-query page.
9. Click on the **Edit Signature** button.

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol
E:7498208, S:7498208, I:7587445	WWW WinNT cmd.exe Exec	10.10.80.40 1562	172.16.1.200 80	TCP

Signature Details - WWW WinNT cmd.exe Access

Edit Signature

Add Filter

Signature ID

5081

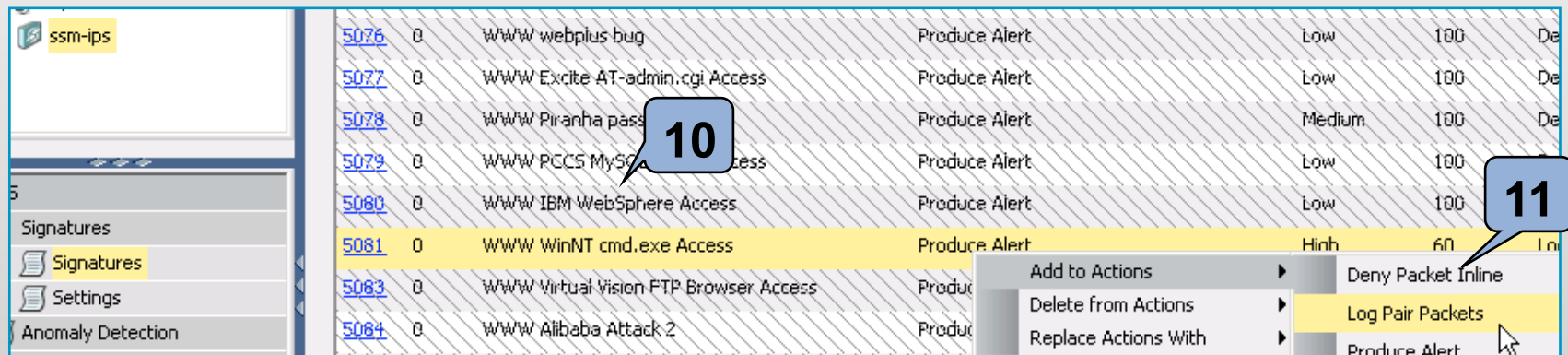
Sub Signature ID

0

Edit Signature in CS Manager

Example 1: IPS Event to Policy

10. MARS provides a link to cross-launch to CSM → navigates to the device, in this scenario is the **ssm-ips** → automatically highlights the signature (5081).
11. From here, the user can configure the policy as needed → e.g. add to action.



The screenshot shows the Cisco MARS interface. On the left, there is a sidebar with a tree view containing 'ssm-ips', 'Signatures', 'Settings', and 'Anomaly Detection'. The 'ssm-ips' item is selected. The main area displays a table of signatures. The signature with ID 5081, titled 'WWW WinNT cmd.exe Access', is highlighted in yellow. A context menu is open over this signature, showing options: 'Add to Actions', 'Delete from Actions', and 'Replace Actions With'. The 'Add to Actions' option is selected, and a sub-menu is visible with options: 'Deny Packet Inline', 'Log Pair Packets', and 'Produce Alert'. The 'Log Pair Packets' option is highlighted. A blue callout bubble with the number '10' points to the signature 5081, and another blue callout bubble with the number '11' points to the 'Log Pair Packets' option in the context menu.

Signature ID	Signature Name	Action	Severity	Score	Category
5076	WWW webplus bug	Produce Alert	Low	100	De
5077	WWW Excite AT-admin.cgi Access	Produce Alert	Low	100	De
5078	WWW Piranha pass	Produce Alert	Medium	100	De
5079	WWW PCCS MyS	Produce Alert	Low	100	
5080	WWW IBM WebSphere Access	Produce Alert	Low	100	
5081	WWW WinNT cmd.exe Access	Produce Alert	High	60	Ln
5083	WWW Virtual Vision FTP Browser Access	Produce			
5084	WWW Alibaba Attack 2	Produce			

Example 1: IPS Event to Policy

12. Return to MARS policy-query page → click **Add Filter**
13. MARS will cross-launch CSM → provide the **Add Filter Item** dialog. The fields are conveniently pre-populated with variables provided from MARS and IPS events.
14. Make any changes and finalize by giving a **Name** to the filter → click **OK** when finished.

Changes will be made during next deployment to the IPS device.

The screenshot shows the 'Add Filter Item' dialog box in the MARS interface. Callout 12 points to the 'Add Filter' button on the main page. Callout 13 points to the 'Add Filter Item' dialog box. Callout 14 points to the 'OK' button at the bottom right of the dialog box.

Add Filter Item

☒ Active
☒ Enabled

Name: * myEAF1

Signature ID: 5081

SubSignature ID: 0

Attacker Address: 10.10.80.40

Attacker Port: 0-65535

Victim Address: 172.16.1.200

Victim Port: 80

Risk Rating Min: 0 Max: 100

OS Relevance: Not Relevant
Relevant
Unknown

Comments:

Actions to Subtract:

- Deny Attacker Inline
- Deny Attacker Service Pair Inline
- Deny Attacker Victim Pair Inline
- Deny Connection Inline
- Deny Packet Inline
- Log Attacker Packets
- Log Attacker/Victim Pair Packets**
- Log Victim Packets
- Produce Alert
- Produce Verbose Alert**
- Request Block Connection
- Request Block Host
- Request Rate Limit
- Request Snmp Trap
- Reset Tcp Connection

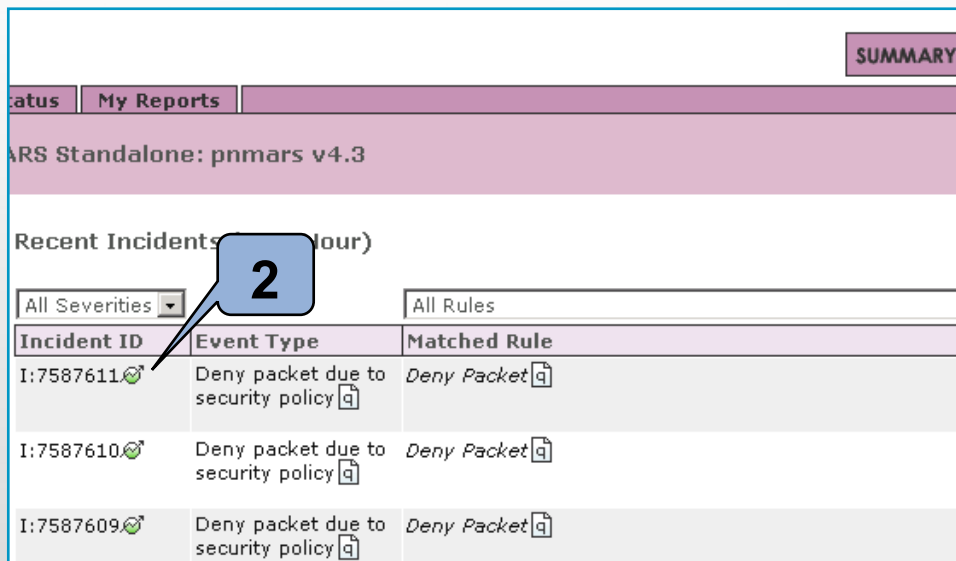
% to Deny: 100

☐ Show

Example 2: FW Event to Policy

1. Open the CS-MARS GUI

2. From either the Summary or Incidents tab, Drill-down into the FW incident.



SUMMARY

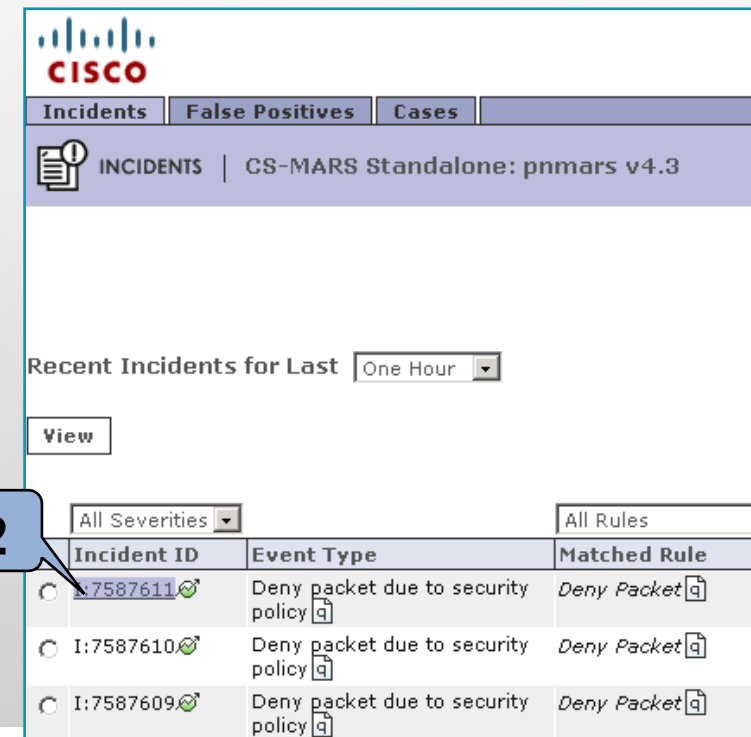
status My Reports

ARS Standalone: pnmars v4.3

Recent Incidents (four)

All Severities All Rules

Incident ID	Event Type	Matched Rule
I:7587611	Deny packet due to security policy	Deny Packet
I:7587610	Deny packet due to security policy	Deny Packet
I:7587609	Deny packet due to security policy	Deny Packet



CISCO

Incidents False Positives Cases

INCIDENTS | CS-MARS Standalone: pnmars v4.3

Recent Incidents for Last One Hour

View

All Severities All Rules

Incident ID	Event Type	Matched Rule
I:7587611	Deny packet due to security policy	Deny Packet
I:7587610	Deny packet due to security policy	Deny Packet
I:7587609	Deny packet due to security policy	Deny Packet

Example 2: FW Event to Policy

3. Another window opens with more details on the incident.
4. Click on path icon it will display the incident network path
5. Next click on the CSM icon to get more details on the reporting device and Raw message.

Incident ID: 7587612

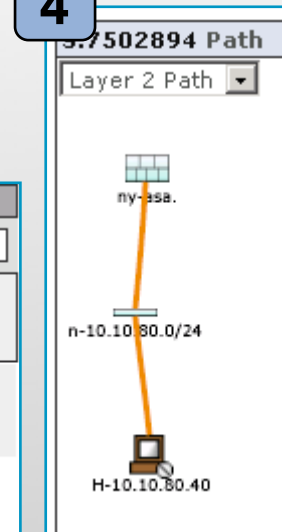
Expand All

Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
1	S:7502894, I:7587612	Deny packet due to security policy	10.10.80.40 1028	10.100.1.15 6161	UDP	Mar 6, 2008 7:46:28 AM PST - Mar 6, 2008 7:47:43 AM PST	ny-asa.cisco.com			False Positive Tuning

6. In the "Raw message" screen below click on the CSM icon. This will display the CSM rule table with the ACE that generated the Syslog highlighted in yellow.

Mar 6, 2008 7:55:39 AM PST			
Standalone: pnmars v4.3		Login: Administrator (pnadmin) :: Close	
Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:7502894, S:7502894, I:7587612	ny-asa.cisco.com	Mar 6, 2008 7:46:28 AM PST	<164>%ASA-4-106023: Deny udp src inside:10.10.80.40/1028 dst outside:10.100.1.15/6161 by access-group "CSM_FW_ACL_OUT_outside" [0x0, 0x0]
E:7502898, S:7502894, I:7587612	ny-asa.cisco.com	Mar 6, 2008 7:47:43 AM PST	<164>%ASA-4-106023: Deny udp src inside:10.10.80.40/1028 dst outside:10.100.1.15/6161 by access-group "CSM_FW_ACL_OUT_outside" [0x0, 0x0]



Example 2: FW Event to Policy

7. Clicking on the highlighted rule or on any rule number on the table will cross launch CSM.

Found 1 matches in 8 rules. Go to matched rule Local 5

Edit	Permit	Source	Destination	Service	Interface	Dir.	Option	Category	Description
Local (8 Rules)									
<u>1</u>	✗	any	172.16.1.200	ICMP	outside	out	Informational/5	None	
<u>2</u>	✓	any	any	ICMP	outside	out	Informational/300	None	
<u>3</u>	✓	any	172.16.1.200	FTP	outside	out	Informational/300	None	
<u>4</u>	✗	any	172.16.1.0/24	FTP	outside	out	Informational/5	None	
<u>5</u>	✗	any	any	udp/6161	outside	out		None	
<u>6</u>	✓	any	any	ICMP	outside	in	Informational/300	None	
<u>7</u>	✓	any	any	IP	outside	in		None	
<u>8</u>	✓	any	any	IP	inside	in		None	

Go to page 1 Rows per page 50

- Note the Cisco Applied Mitigation Bulletin column

Worldwide [change] [Log In](#) | [Register](#) | [About Cisco](#)

Search

[Solutions](#) [Products & Services](#) [Ordering](#) [Support](#) [Training & Events](#) [Partner Central](#)

Security Center

Inform, Protect, Respond
Early-warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions to help protect networks

Powered by **IntelliShield** [Advanced Search](#) View Alerts: [Most Recent](#)

Security Alert	CVSS Score	Cisco IPS Signature	Cisco PSIRT Advisory	Cisco Applied Mitigation Bulletin	Affected Cisco Products
Cisco Unified Communications Manager SQL Injection Vulnerability	4.0/3.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MySQL Enterprise and Community Server SSL Library Buffer Overflow Vulnerability	7.5/5.9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Linux Kernel get_iovec_page_array() Privilege Escalation Vulnerability	6.8/5.6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mozilla Firefox, SeaMonkey, and Thunderbird Browser Engine Memory Corruption Vulnerability	9.3/6.9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Emergency Response

- » Emergency response for network incidents:
Cisco Technical Support
800 553-2447 (U.S.)
[Worldwide Contacts](#)
- » Urgent assistance for incidents with Cisco products:
[PSIRT](#)
877 228-7302 (U. S.)
+1 408 525 6532 (outside U. S.)
- » Report an incident involving the Cisco corporate network:
infosec@cisco.com

[Cisco Vulnerability Policy](#)

- The Security Center Website offers advice for security alerts including:

Reports and screenshots for CS-MARS

IPS Signature information – including false positive triggers – Very helpful for tuning sensors

Cisco Security Monitoring, Analysis, and Response System

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can create incidents on events for the following Microsoft Security Bulletins. After the S316 dynamic signature update has been downloaded, using the following keywords for each of the respective IPS signatures and a query type of **All Matching Events** on the Cisco Security MARS appliance will provide a report that lists the incidents created by these IPS signatures.

Microsoft ID	Signature ID(s)	MARS Query Keyword(s)
MS08-004	6257-0	NR-6257
MS08-007	6771-0	NR-6771
MS08-008	6777-0	NR-6777
	6777-1	
	6777-2	

Q & A



Cisco Expo
2009

Welcome to the Human Network.



