Cisco Expo 2008

Odkrivanje, analiziranje in odpravljanje varnostnih groženj z uporabo Cisco Security MARS

Dejan Miletić, univ.dipl.inž.el.

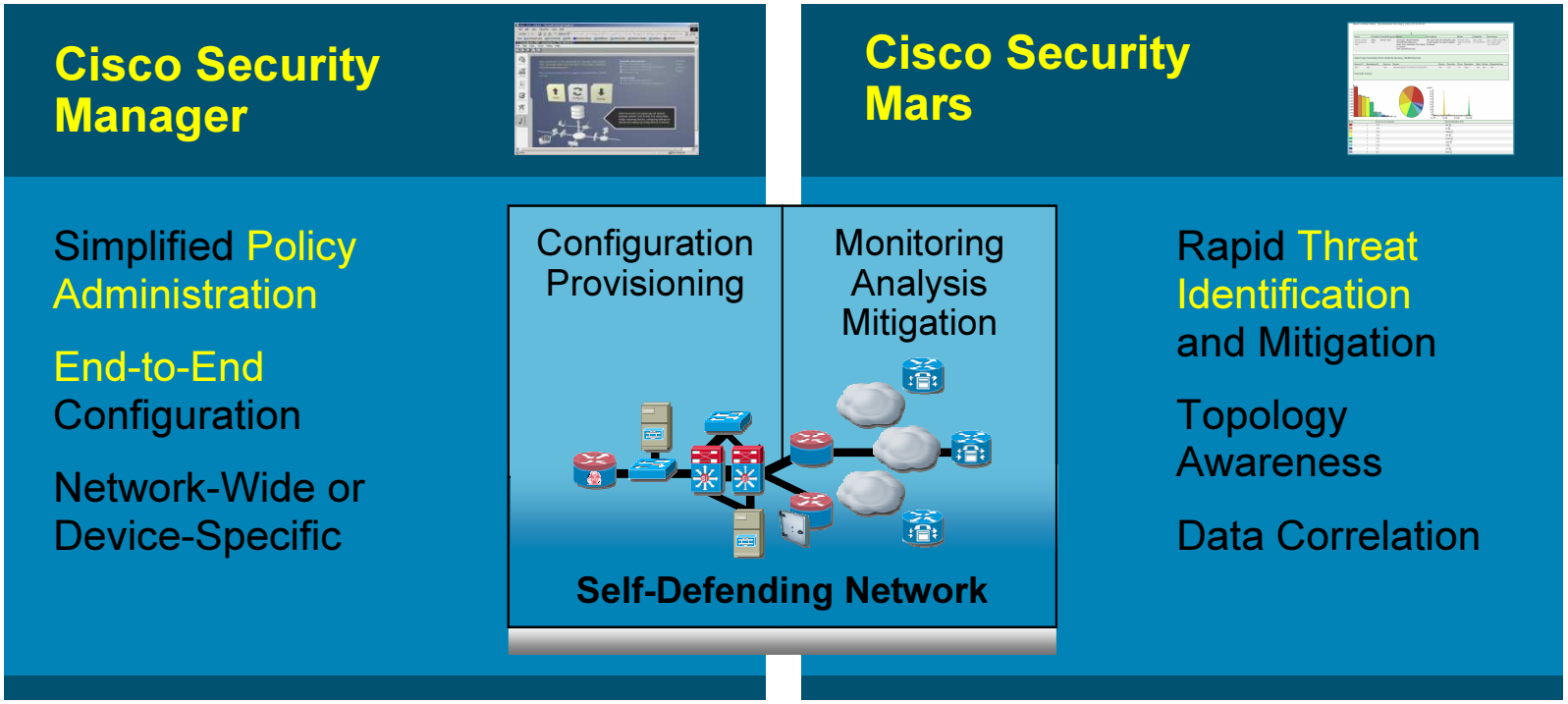
CCNP, CCDP, CCIP, CCSP

Enable Your Network
Empower Your Business

Agenda

- Security Threat Management Overview
- Monitoring, Analysis and Response with MARS
- MARS Features and Functions
- Reporting in MARS
- MARS Appliances
- Use-case example
- MARS demo
- Q & A

Cisco Security Management Suite



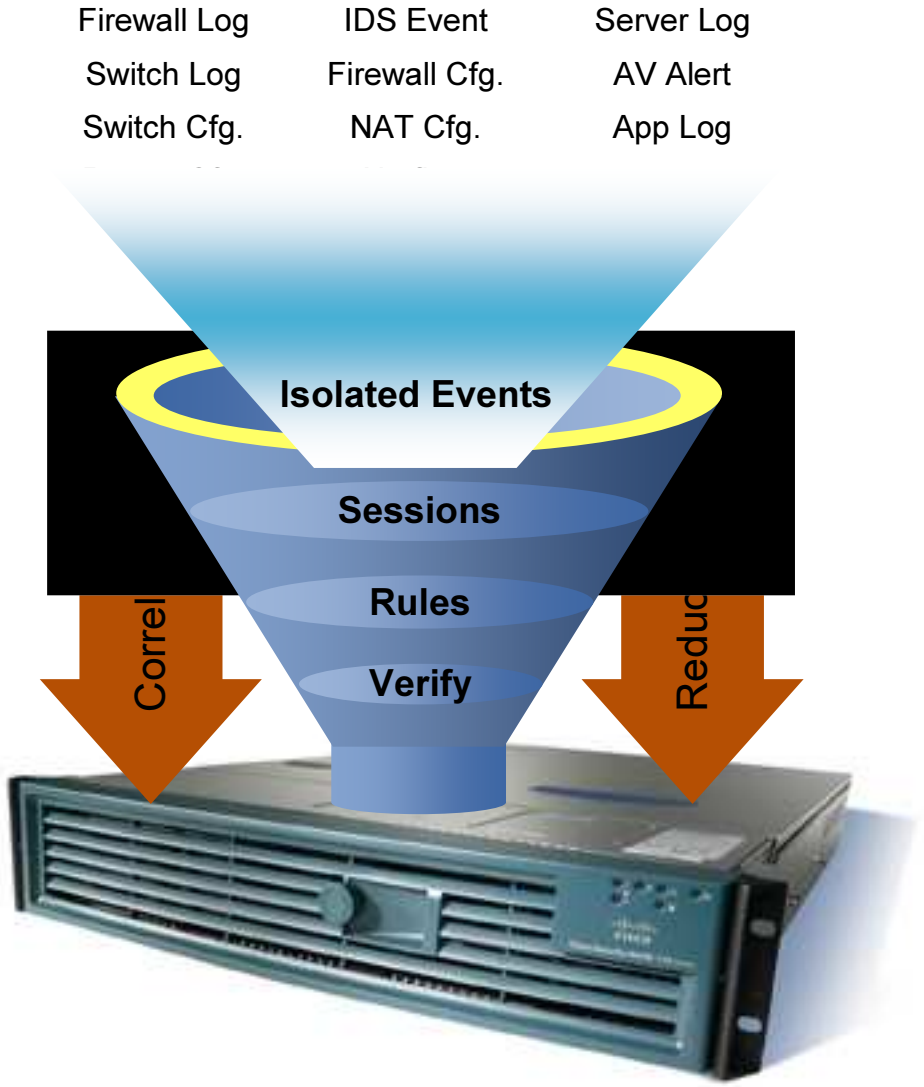
- Integrated Security Management and Monitoring

Monitoring, Analysis and Response with MARS

Cisco Security MARS

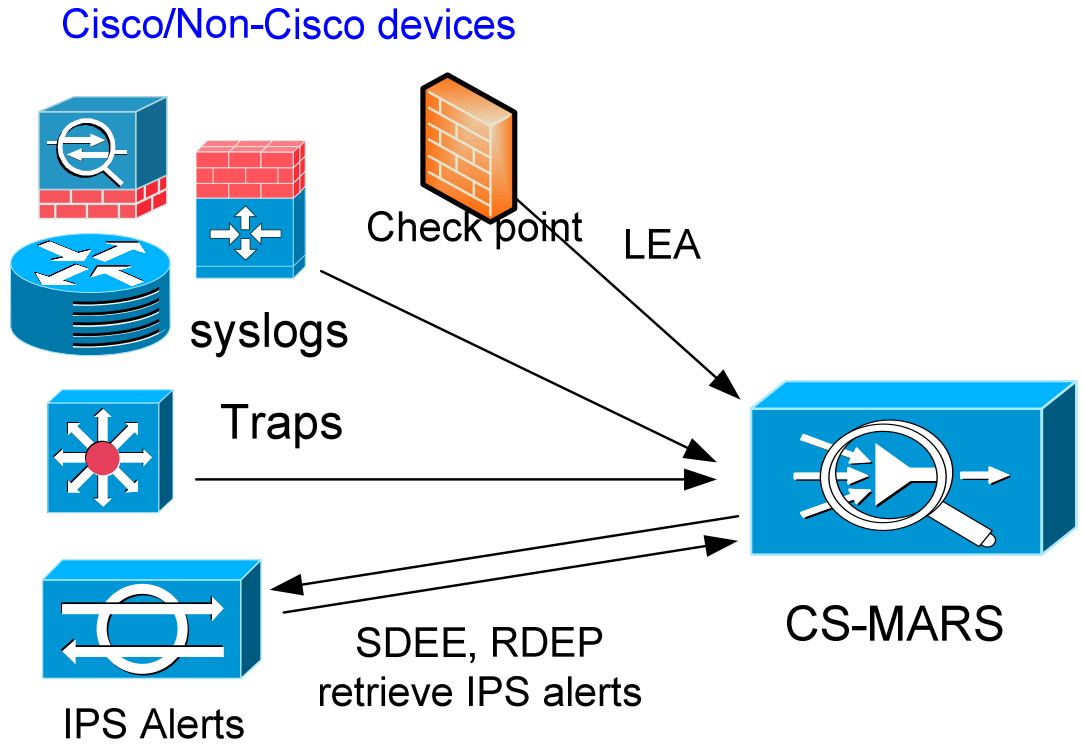
Comprehensive Threat Management

- MARS is an acronym = Monitoring, Analysis and Response System
- 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



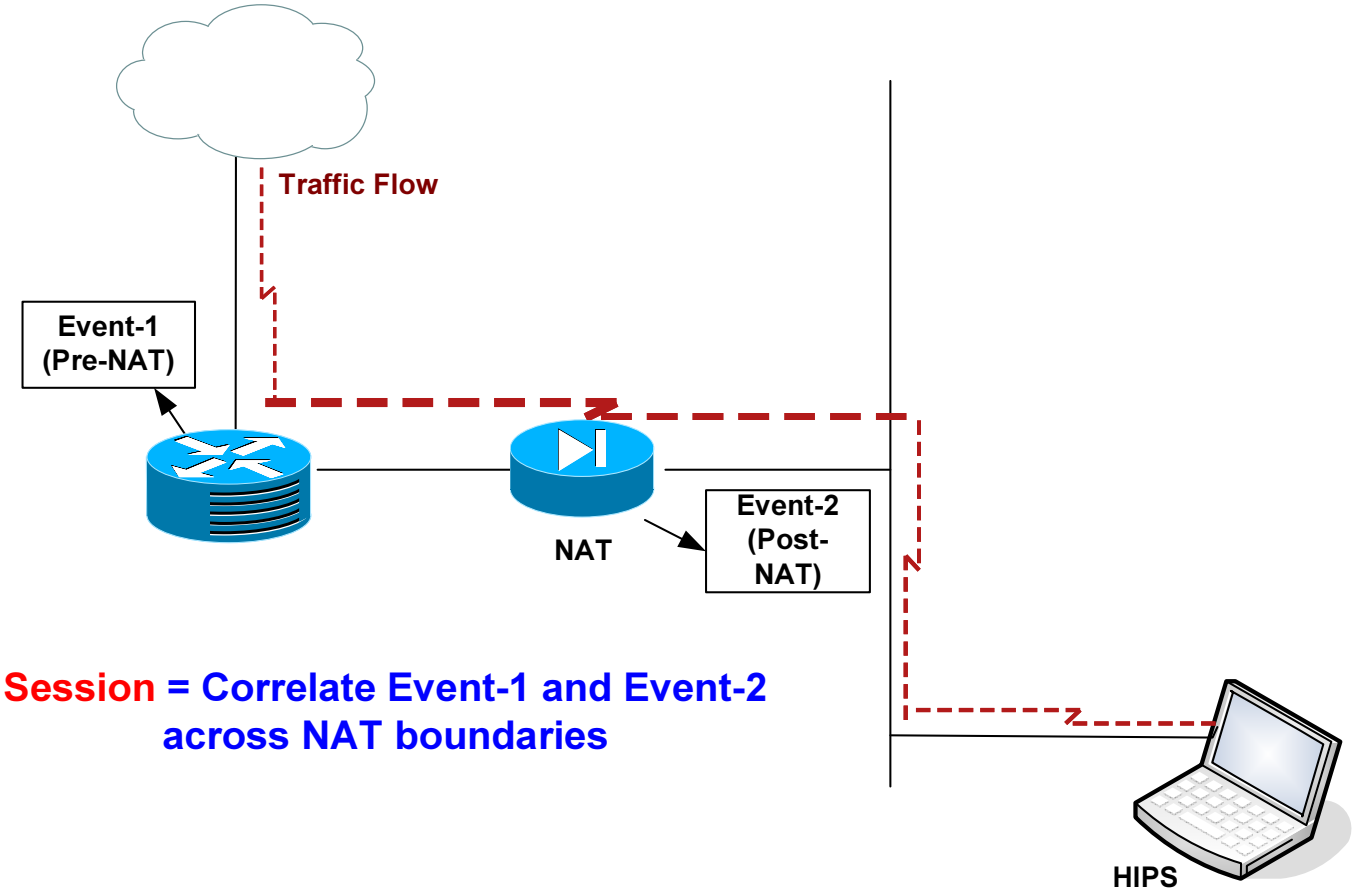
Key Concepts - Events

- **Events** — “Push” of messages to MARS by the monitoring reporting devices (syslogs, traps…) <OR> MARS “Pulls” events from the monitoring reporting devices (IPS alerts, Windows log….).



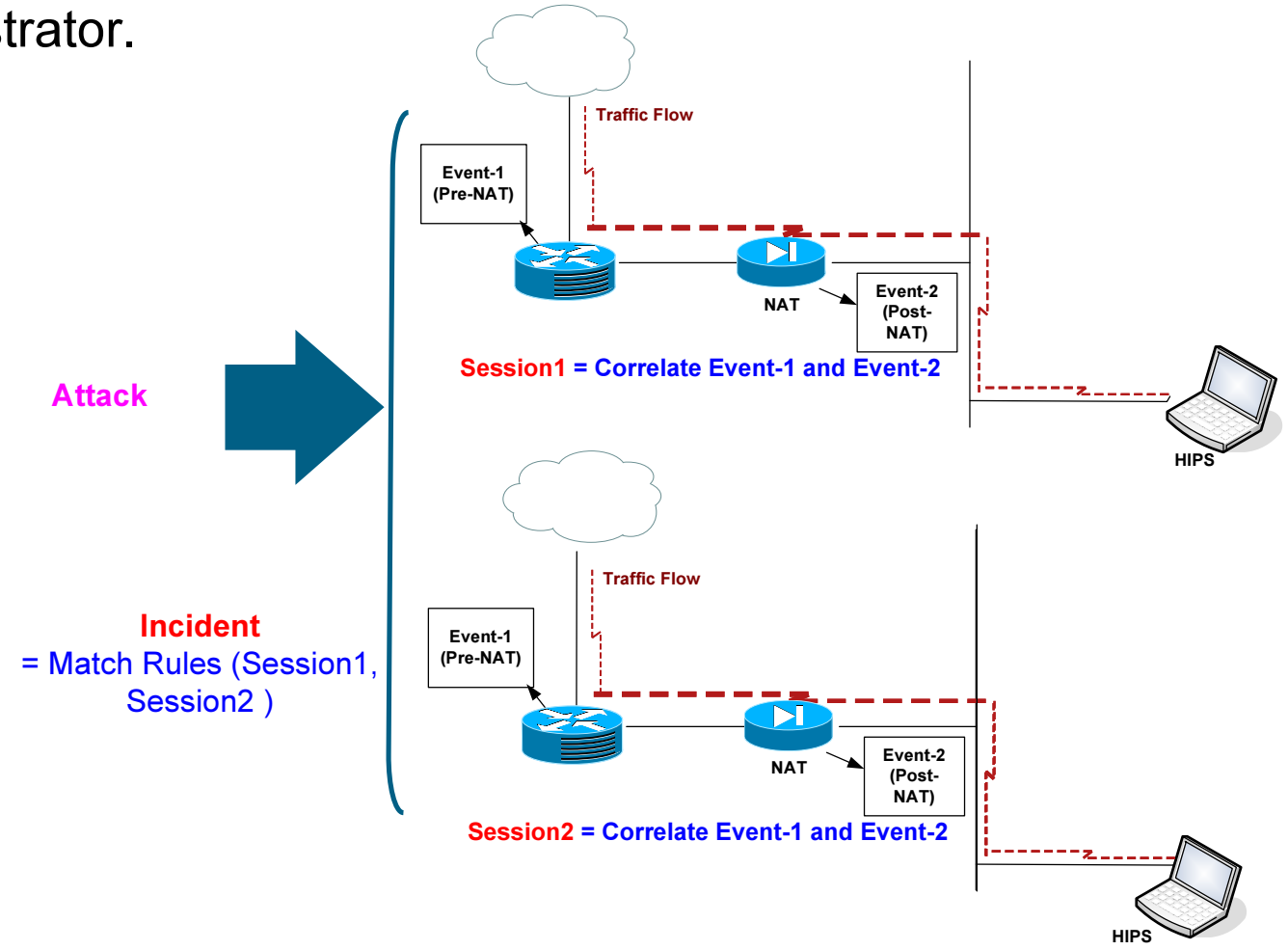
Key Concepts - Sessions

- **Sessions** — set of messages (events) that are correlated by the MARS across NAT boundaries.



Key Concepts - Incidents

- **Incidents** — set of sessions that match defined inspection rules. Rules are either included in the MARS system or defined by the administrator.



How MARS Works

1st phase, Normalization

2nd phase, Rules applied

3rd phase, Analysis and Mitigation

1. **Events come into MARS from Network Devices**
2. **Events are Parsed**
3. **Normalized**
4. **Sessionized/NAT correlation**
5. **Analyzed against Rule Engine**
6. **Vulnerability Assessment against suspected hosts**
7. **False Positive Analysis**
8. **Traffic profiling and statistical anomaly detection**

MARS Features and Functions

Cisco Security - MARS Feature Overview

Goal:

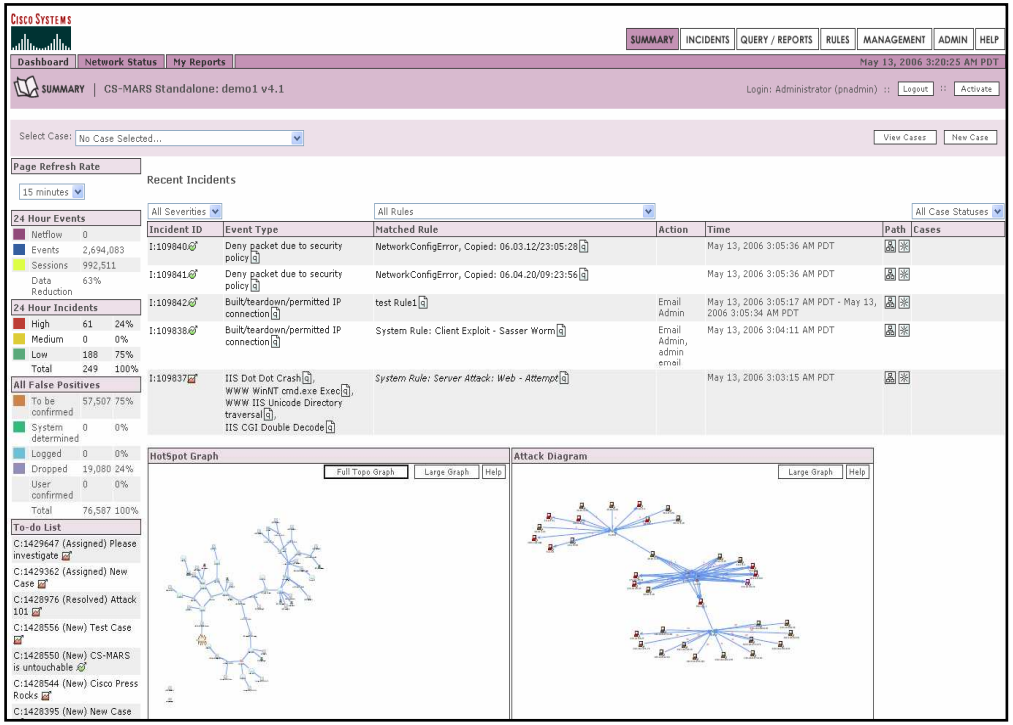
- MARS Transforms raw network and security data into actionable intelligence

Key features

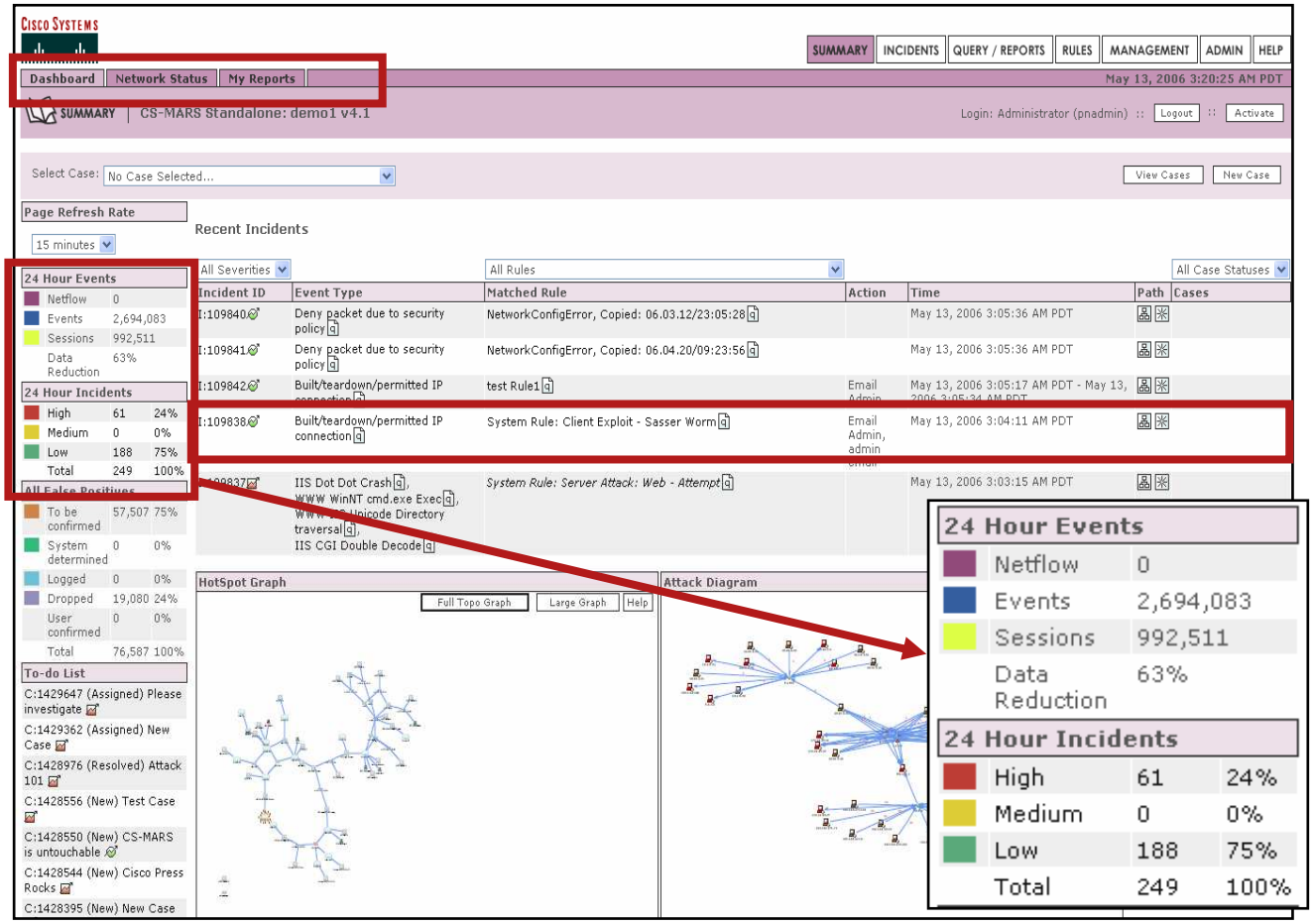
- Appliance-based Threat Mitigation
- Centralized dashboard to unify Security Operations
- Collect, aggregate & correlate from heterogeneous devices in a single appliance
  - SDEE, Syslog, Host logs, Firewall logs …. From Cisco, Non-Cisco and Custom devices
  - No software agents required
- Network Behavioral Analysis (NBA)
  - Netflow and Traffic Flow analysis provides enhanced threat detection precision
- Topological Awareness
  - Device Configuration (+NAT, +Routing) knowledge critical to global decision making
- Mitigation Capabilities
  - Layer 2 / Layer 3 Mitigation Suggestions (port disable, shun commands, ACLs etc.)

Big Picture Command and Control

- Centralizing Netflow, Syslog and device topology as inputs to MARS builds the command and control center



Critical Data Reduction



Incident Dashboard
- Aggregate
- Correlate
- Summarize

2,694,083 Events

↓

992,511 Sessions

↓

249 Incidents

↓

61 High Severity Incidents

Impactful Data Reduction, allows Administrators to focus on priorities

Attack Path and Topology Awareness

Victim/contaminated host

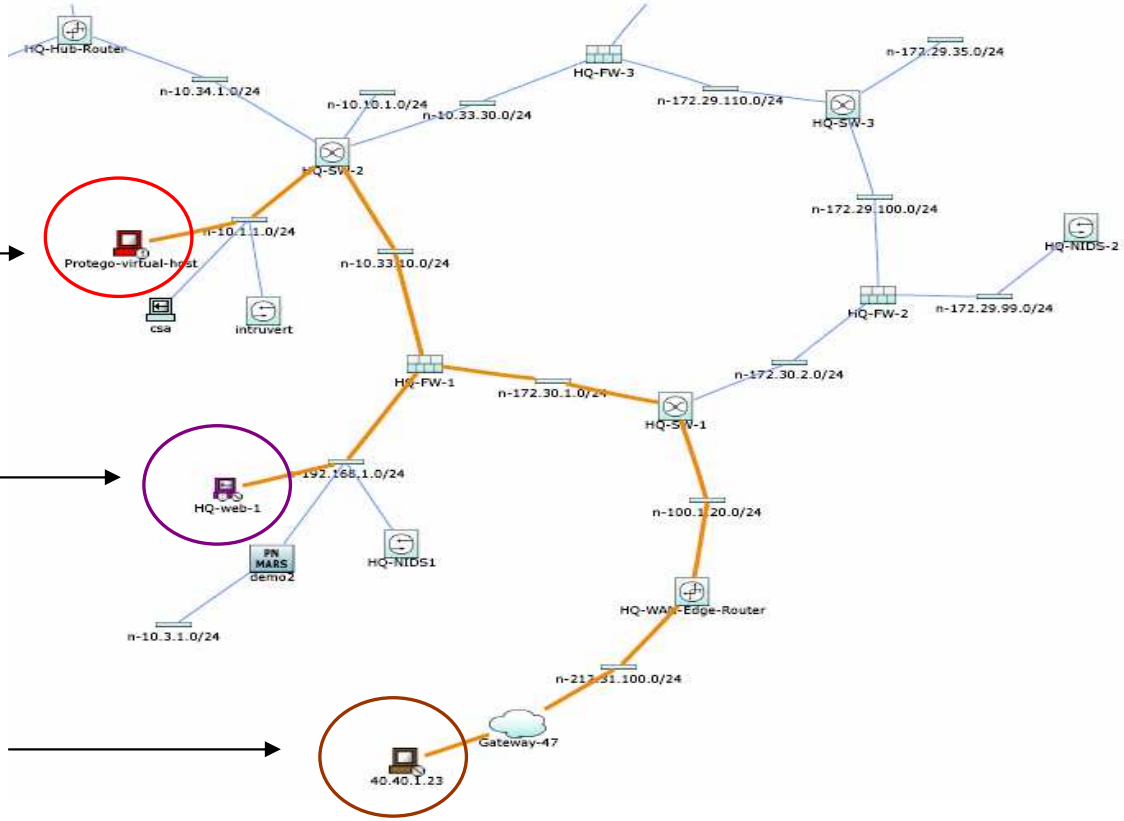
(red)

Compromised host propagating attack

(purple)

Attack Start

(brown)



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		

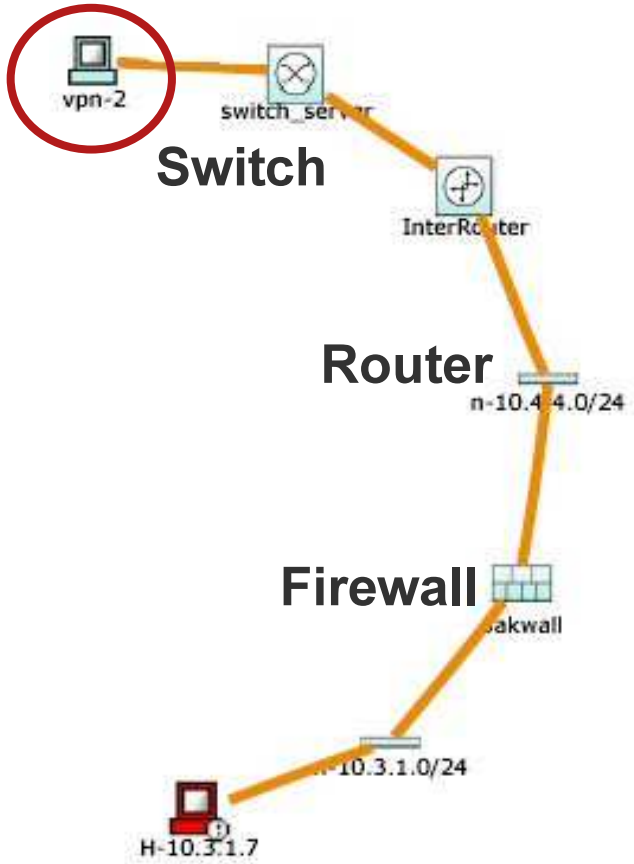
Interface Information

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

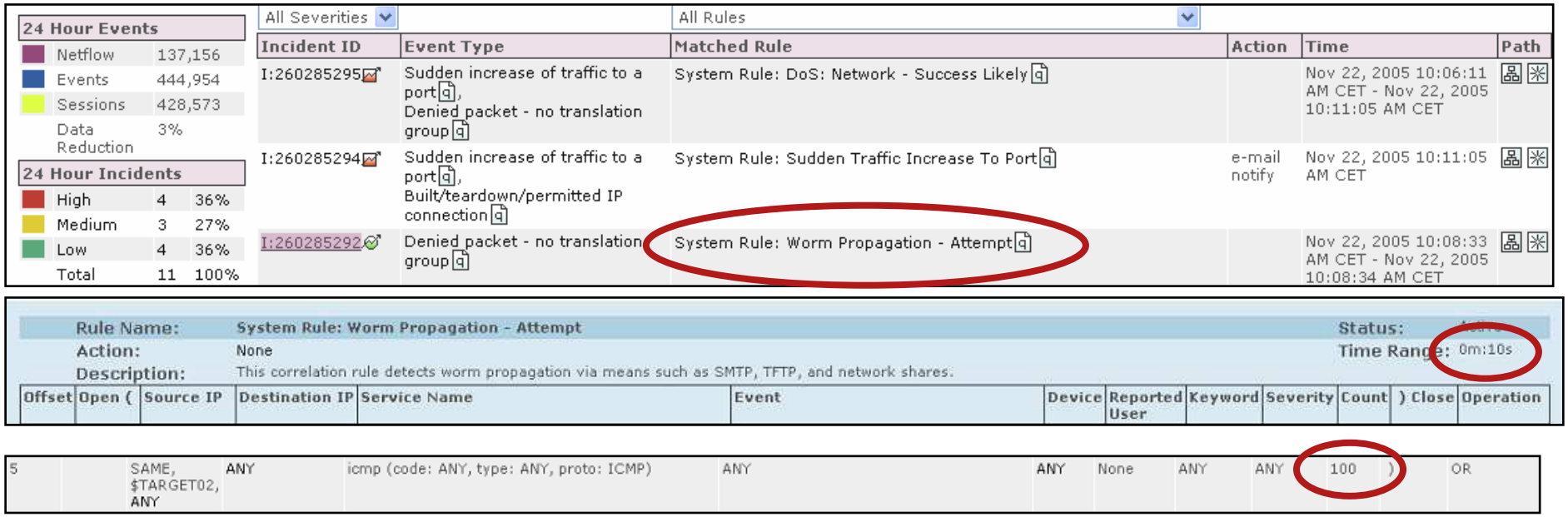
Recommended Policy/Command

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

Push Cancel



Command and Control Dashboard



24 Hour Events		
Netflow	137,156	
Events	444,954	
Sessions	428,573	
Data Reduction	3%	

24 Hour Incidents		
High	4	36%
Medium	3	27%
Low	4	36%
Total	11	100%

All Severities | All Rules

Incident ID	Event Type	Matched Rule	Action	Time	Path
I:260285295	Sudden increase of traffic to a port, Denied packet - no translation group	System Rule: DoS: Network - Success Likely		Nov 22, 2005 10:06:11 AM CET - Nov 22, 2005 10:11:05 AM CET	
I:260285294	Sudden increase of traffic to a port, Built/teardown/permitted IP connection	System Rule: Sudden Traffic Increase To Port	e-mail notify	Nov 22, 2005 10:11:05 AM CET	
I:260285292	Denied packet - no translation group	System Rule: Worm Propagation - Attempt		Nov 22, 2005 10:08:33 AM CET - Nov 22, 2005 10:08:34 AM CET	

Rule Name: System Rule: Worm Propagation - Attempt
Status:
Action: None
Time Range: 0m:10s
Description: This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
5		SAME, $TARGET02, ANY	ANY	icmp (code: ANY, type: ANY, proto: ICMP)	ANY	ANY	None	ANY	ANY	100	)	OR

Denied packet - no translation group	10.1.1.246	0	10.1.61.1
Denied packet - no translation group	10.1.1.246	0	10.1.61.2
Denied packet - no translation group	10.1.1.246	0	10.1.61.3
Denied packet - no translation group	10.1.1.246	0	10.1.61.4

- 100 ICMP messages from the same source within ten seconds must mean something is wrong

Customizable System Defined Rules

Rule Definition

- Define offsets

Rule Name:	Sasser Rule										Status:	Active
Action:	None										Time Range:	0h:05m
Description:	This rule matches the traffic pattern of the Sasser worm.											
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		$TARGET01	$TARGET02	User Defined (src port: ANY, dst port: 445, proto: TCP)	ANY	ANY	None	ANY	ANY	1		AND
2		$TARGET01	$TARGET02	User Defined (src port: ANY, dst port: 9996, proto: TCP)	ANY	ANY	None	ANY	ANY	1		AND
3		$TARGET02	$TARGET01	User Defined (src port: ANY, dst port: 5554, proto: TCP)	ANY	ANY	None	ANY	ANY	1		FOLLOWED-BY
4		$TARGET02	DISTINCT	User Defined (src port: ANY, dst port: 445, proto: TCP)	ANY	ANY	None	ANY	ANY	20		

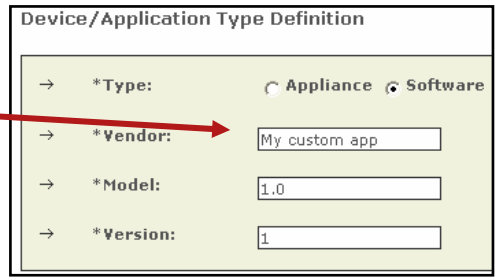
- Specify number of occurrence
- Specify time range

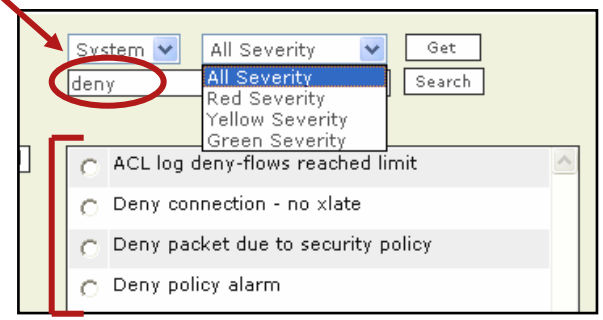
Rule can also be used to generate reports

Custom Parser

It Is Possible to Create a Custom Parser for Any Device Sending Syslog or SNMP Traps

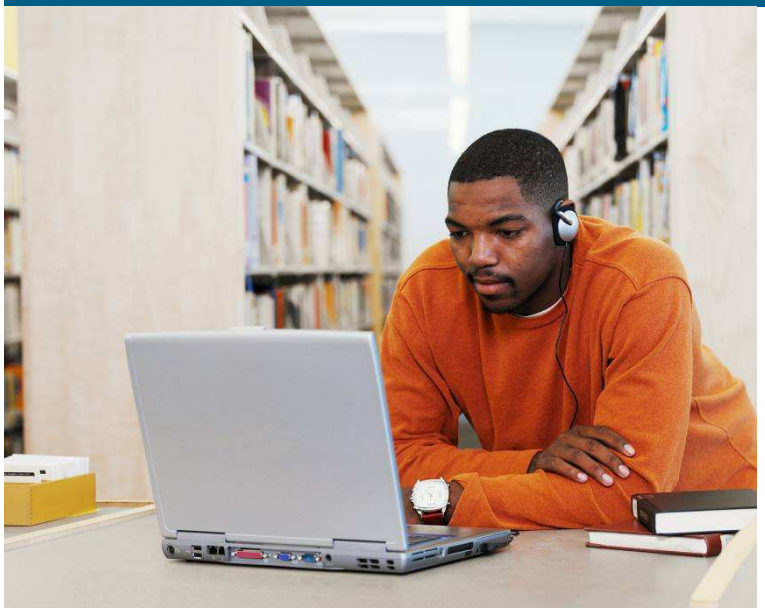
1. Create a new device/ application type
2. Create an event type for the new device/application
3. Define the patterns associated to the event type
4. Add this new device/application into MARS

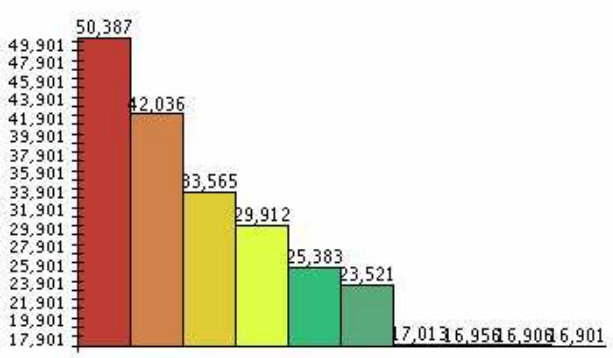


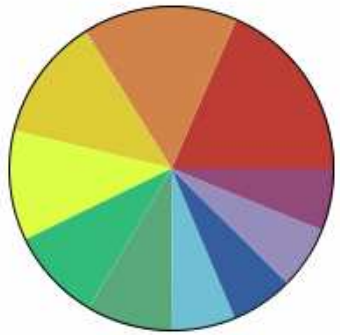


Note: If You Re-Use Events Already in the Database, the Predefined Reports and Rules Will Work Also for the Newly Defined Device

Reporting in MARS







Apr 3, 2007 3:50:00 PM PDT - Apr 3, 2007 4:00:00 PM PDT

Peak	Rank	Number of Sessions at Peak
Peak	1	50,387
Peak	2	42,036
Peak	3	33,565
Peak	4	29,912
Peak	5	25,383
Peak	6	23,521
Peak	7	17,013
Peak	8	16,956
Peak	9	16,906
Peak	10	16,901

System Defined/Customizable Reports

Example: Report showing top destination ports that were denied by Firewall

Report scheduled hourly

Report over 24 hours

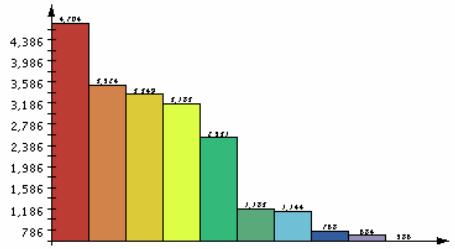
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

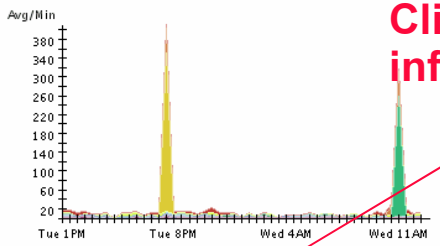
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination 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]

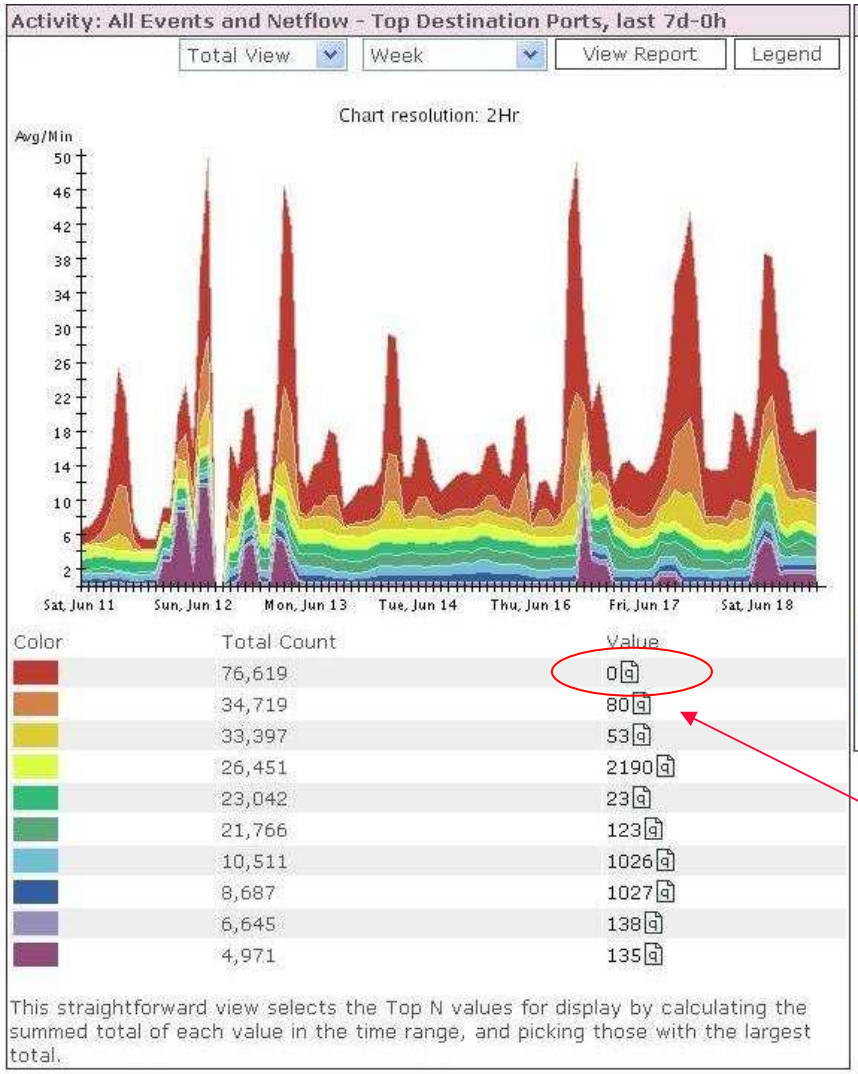


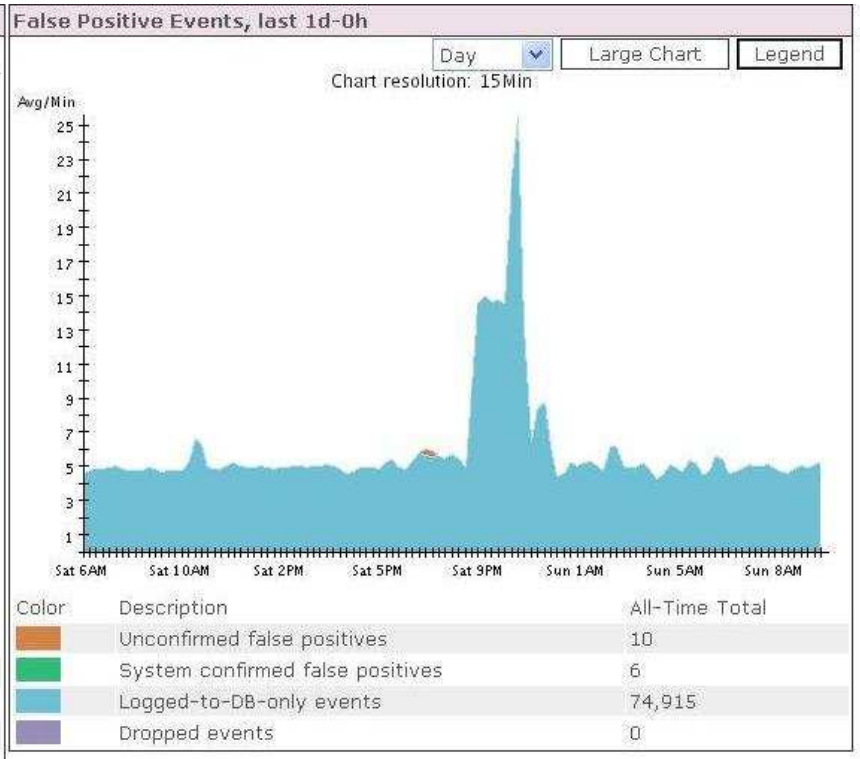


Click "q" icon to get detail information about port 445

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

Network Traffic Investigation





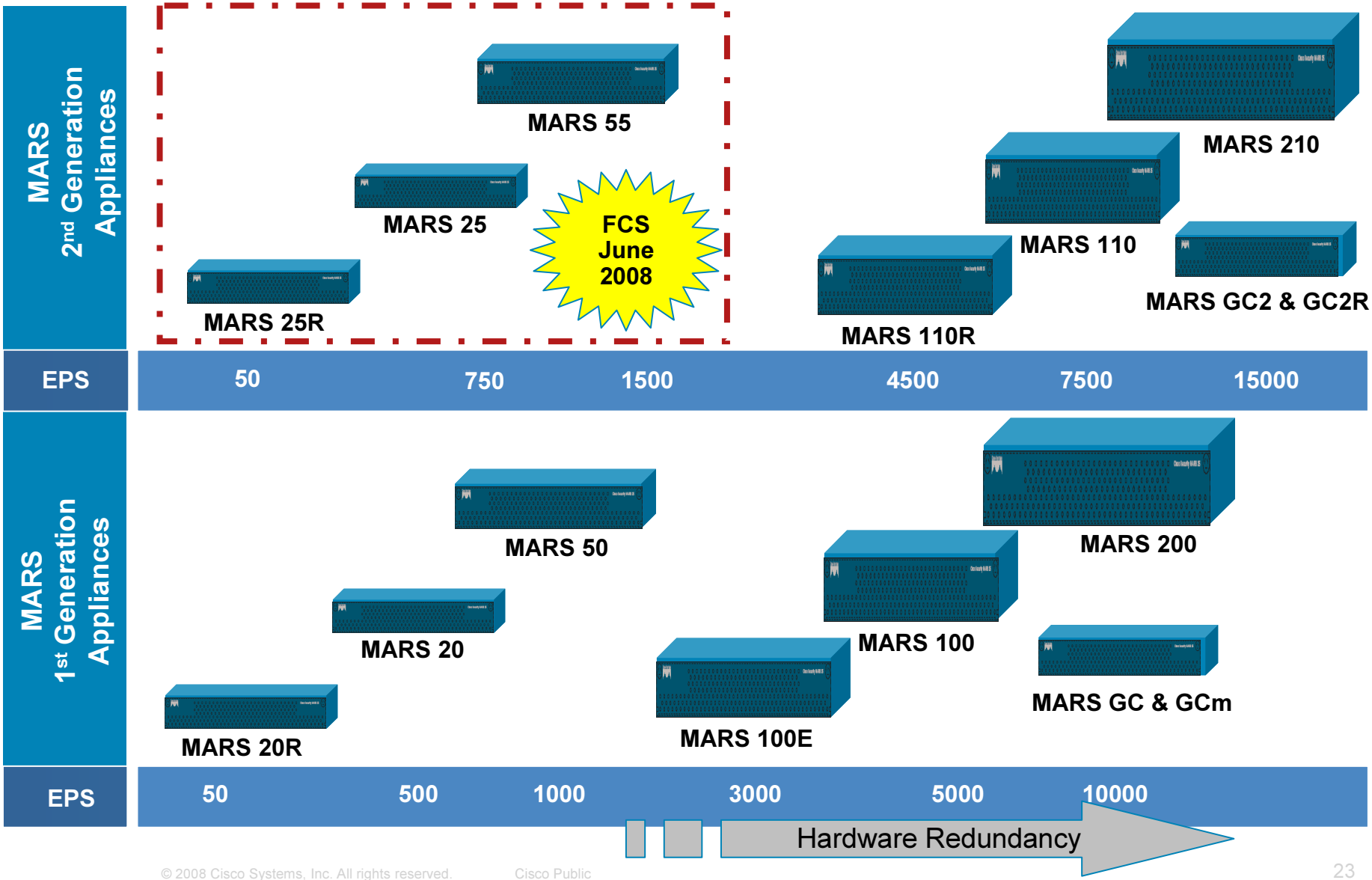
Why Port 0 traffic?

Is it real Port0 attack or events that have no port information?

Need further investigation

MARS Appliances

Cisco Security MARS
Appliance Overview



CS-MARS Overall Product Line

Local Controller Models	Events/ Sec[1]	NetFlows/ Sec	Storage	Rack Unit	Power
Cisco Security MARS 20R (CS-MARS-20R-K9)	50	1500	120 GB (non-RAID)	1 RU x 16 in.	300W, 120/240V autoswitch
Cisco Security MARS 20 (CS-MARS-20-K9)	500	15,000	120 GB (non-RAID)	1 RU x 16 in.	300W, 120/240V autoswitch
Cisco Security MARS 50 (CS-MARS-50-K9)	1,000	30,000	240 GB RAID 0	1 RU x 25.6 in.	300W, 120/240V autoswitch
Cisco Security MARS 100e (CS-MARS-100e-K9)	3000	75,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 in.	500W dual-redundant, 120/240V autoswitch
Cisco Security MARS 100 (CS-MARS-100-K9)	5000	150,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 in.	500W dual-redundant, 120/240V autoswitch
Cisco Security MARS 200 (CS-MARS-200-K9)	10,000	300,000	1,000 GB RAID 10 hot-swappable	4 RU x 25.6 in.	500W dual-redundant, 120/240V autoswitch
Cisco Security MARS 110R (CS-MARS-110R-K9)	4,500	75,000	1,500 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W dual-redundant, 120/240V autoswitch
Cisco Security MARS 110 (CS-MARS-110-K9)	7,500	150,000	1,500 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W dual-redundant, 120/240V autoswitch
Cisco Security MARS 210 (CS-MARS-210-K9)	15,000	300,000	2,000 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W dual-redundant, 120/240V autoswitch

[1] Events per second: Maximum events per second with dynamic correlation and all features enabled.

2nd Generation Hardware Update

- Next-Gen appliances launched May 2007

  Refresh for current shipping models (MARS 100e, MARS 100, MARS 200, MARS GC) with new hardware components

  1.5x EPS performance, 2x Storage, Slim form factor

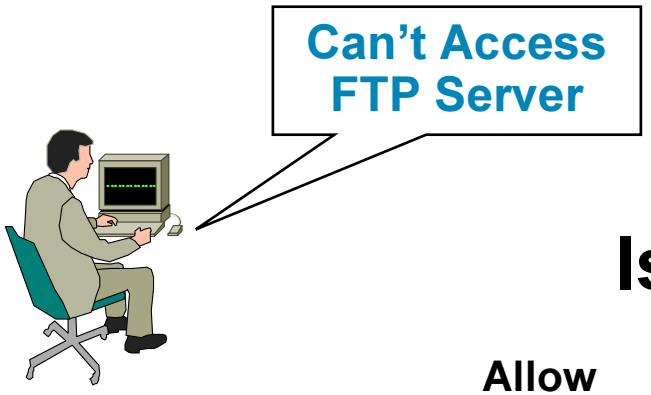
- Software feature parity between appliances

  Similar functionality to end-customers

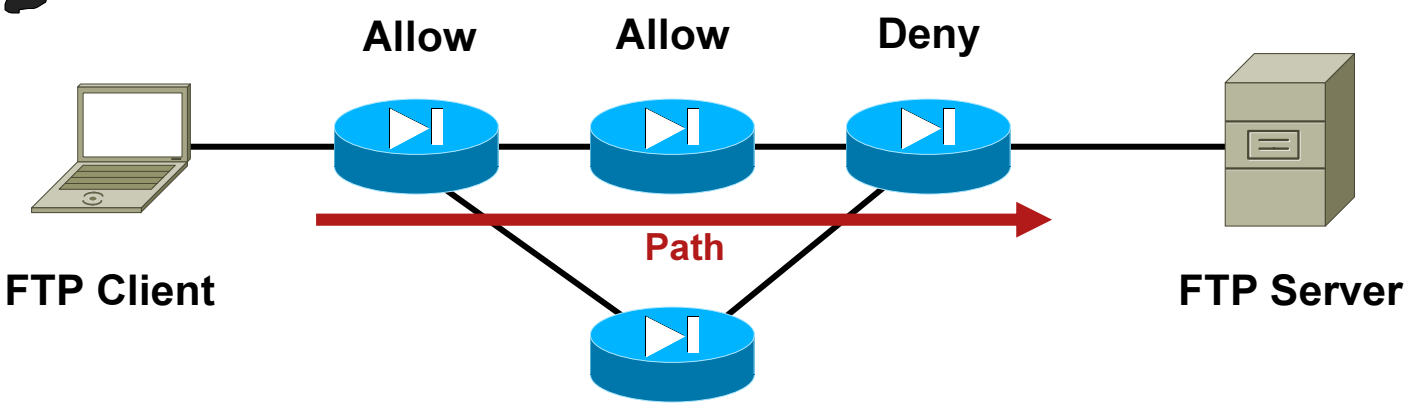
- Existing and Next-Gen hardware interoperable

Use-case Example

CSM and MARS Cross Launch:
Troubleshooting no FTP Access

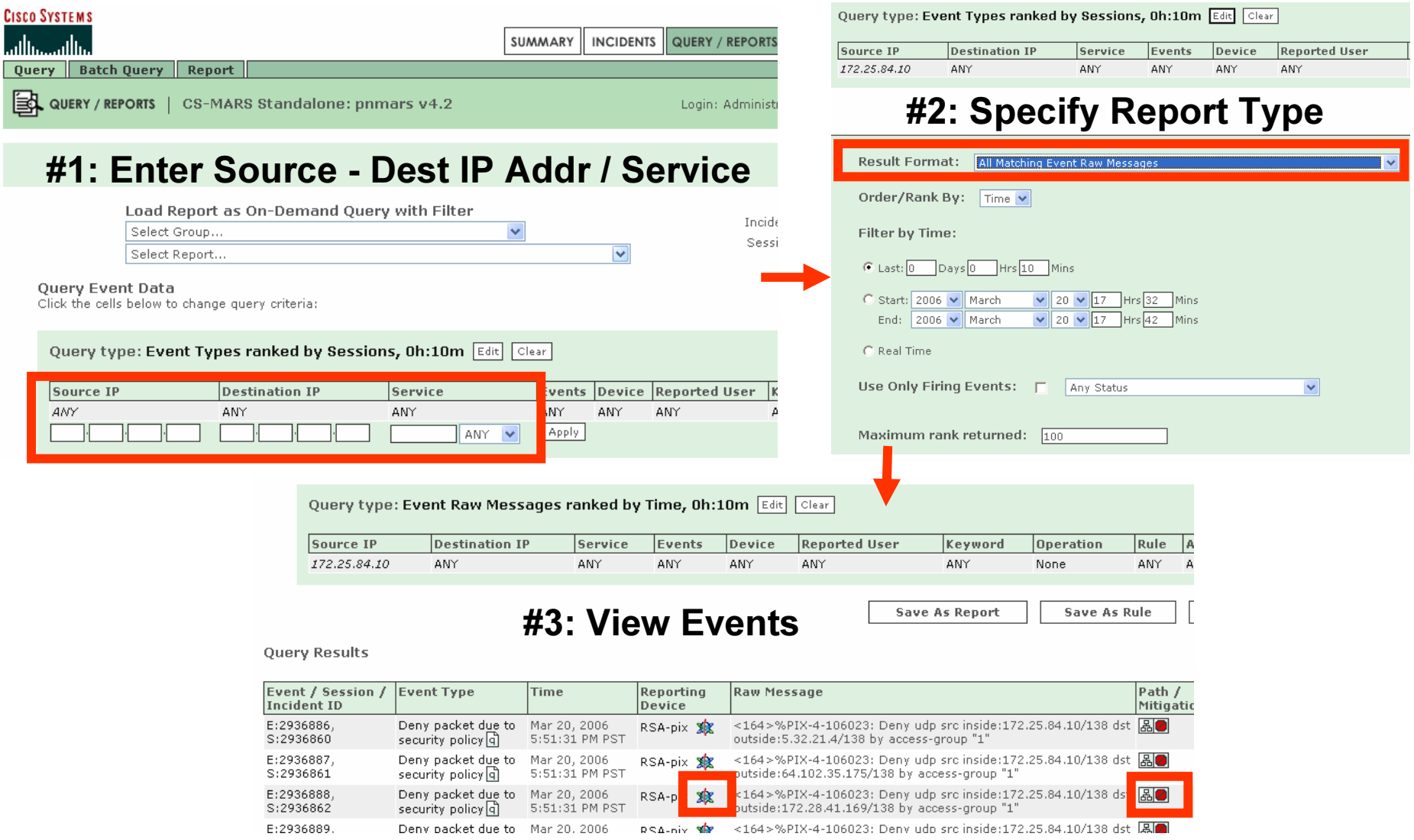


Is a firewall denying access?



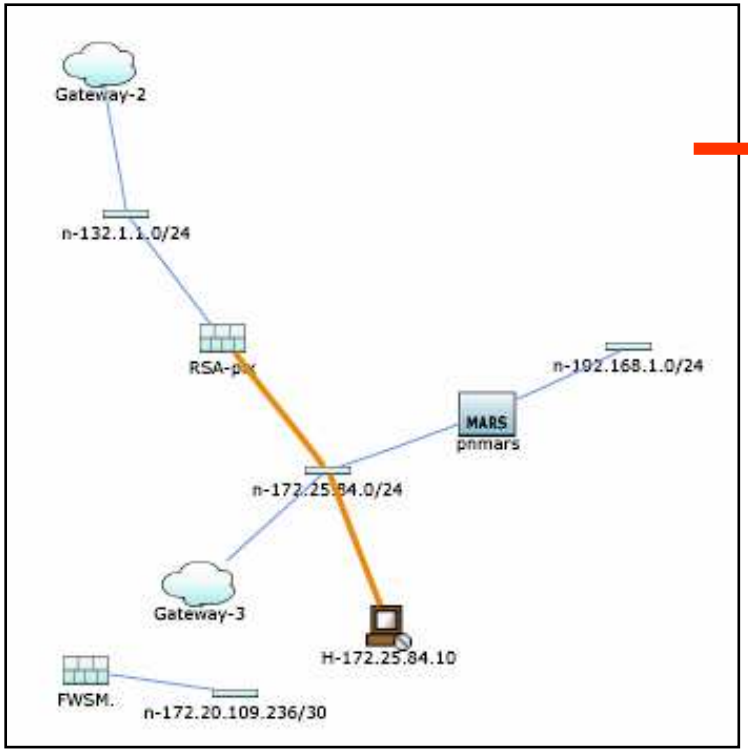
How many firewalls are in the path?
Are there multiple paths?

Flow Troubleshooting: MARS



Flow Troubleshooting: MARS

#4: View Topology



#5: View Firewall Rule Table

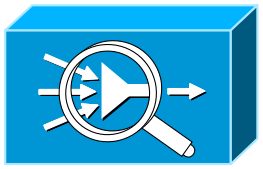
Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:2936886, S:2936860	Deny packet due to security policy	172.25.84.10 138	5.32.21.4 138	UDP	Mar 20, 2006 5:51:31 PM PST	RSA-pix		False Positive

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		

MARS demo

Demo Server



Q & A

dmiletic@cisco.com