CHAPTER 20

Incident Investigation and Mitigation

An incident is a chain of events that are correlated by a rule to signal an attack upon your network. MARS simplifies and expedites the detection, mitigation, reporting, and analysis of the incident. The Network Summary dashboard and the Incident pages help to detect recent incidents and show the rules and the events that compose them. Mitigation refers to the ability of the MARS to isolate the attacking and compromised network devices by identifying and configuring enforcing devices that act as choke points in the network. Queries and reports reveal the scope of a problem and gather data for analysis and regulatory compliance. All this information can be captured in a case report with Case Management and escalated to the relevant personnel.

Incidents Overview

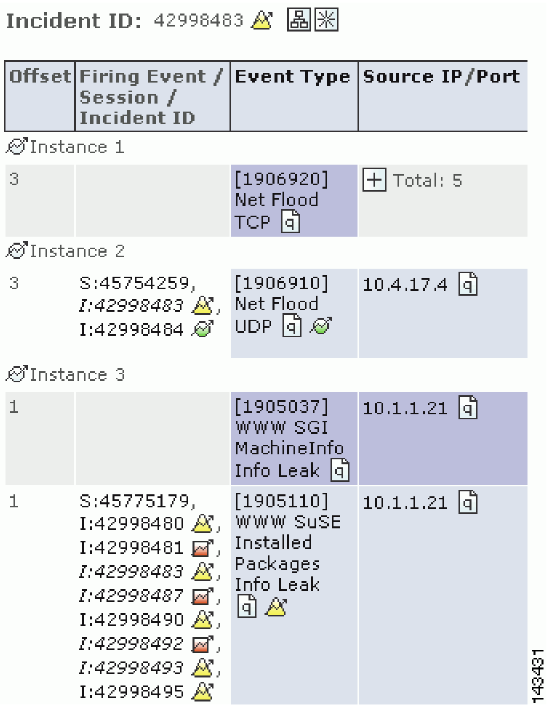
An attack can consist of a reconnaissance activity (for instance, a port scan), followed by a penetration attempt (such as, a buffer overflow), and followed by malicious activity on the target host (for example, a local privilege escalation attack or the installation of backdoors).

An incident, which is generated by a Local Controller, collects the interesting events that constitute an attack scenario and uses rules to describe them. MARS provides you with pre-defined, system rules—which you can fine tune—and gives you the ability to create your own rules.

Incidents are sub-divided into instances to make it easier for you to investigate the attack scenario. Each instance alone is a full attack scenario.

For example, if your network is probed for a DoS attack and then attacked, a rule fires when it sees the follow up attack. The incident displays the instances of this attack.

Figure 20-1 A DoS probe followed by a DoS attack



Incident ID: 42998483

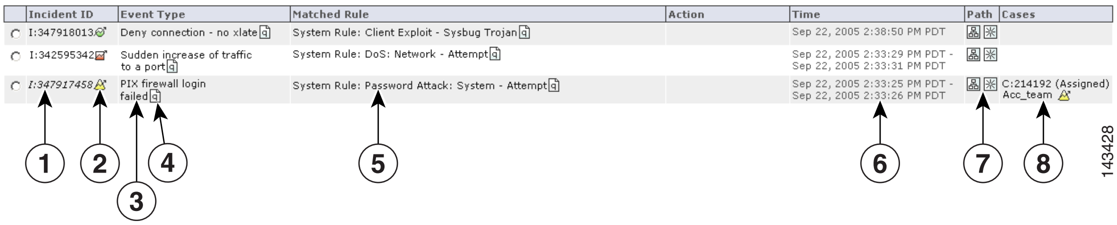
Offset	Firing Event / Session / Incident ID	Event Type	Source IP/Port
Instance 1			
3		[1906920] Net Flood TCP	+ Total: 5
Instance 2			
3	S:45754259, *I:42998483*, I:42998484	[1906910] Net Flood UDP	10.4.17.4
Instance 3			
1		[1905037] WWW SGI MachineInfo Info Leak	10.1.1.21
1	S:45775179, I:42998480, I:42998481, *I:42998483*, *I:42998487*, I:42998490, *I:42998492*, *I:42998493*, I:42998495	[1905110] WWW SuSE Installed Packages Info Leak	10.1.1.21

The Incidents Page

Click the **Incidents** tab to navigate to the Incidents page. The Incidents page displays recent incidents.

Incidents are collections of events and sessions that meet the criteria for a rule, each having helped to cause the rule to fire. An incident's duration only includes the events that contributed to the incident firing.

Figure 20-2 Incidents Navigation



	Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
○	I:347918013	Deny connection - no xlate	System Rule: Client Exploit - Sysbug Trojan		Sep 22, 2005 2:38:50 PM PDT		
○	I:342595342	Sudden increase of traffic to a port	System Rule: DoS: Network - Attempt		Sep 22, 2005 2:33:29 PM PDT - Sep 22, 2005 2:33:31 PM PDT		
○	*I:347917458*	PIX firewall login failed	System Rule: Password Attack: System - Attempt		Sep 22, 2005 2:33:25 PM PDT - Sep 22, 2005 2:33:26 PM PDT		C:214192 (Assigned) Acc_team

1	The Incident ID— Link to the Incident Detail page.	**2**	Incident Severity Icon
3	The events that compose the Incident—Launches the Event Type Details popup window.	**4**	Query icon—Link to the Query page and populates the corresponding query field with the item.
5	The rule that fired to create the incident. Links to the rule page to display the details of the rule.	**6**	Time range of the incident.
7	Launches the Incident Path and Incident Vector diagrams Click to query on the matched rule	**8**	Link to the View Case page

The Incident page's table:

- *Incident ID*

An incident's unique ID.

- *Severity*

Low (green), medium (yellow), and high (red) icons.

- *Event Type*

The normalized signature sent from the reporting devices.

- *Matched Rule*

The rule whose criteria were met.

- *Action*

The description of the notification taken when this rule fires (epage, email, etc.)

- *Time*

A single time or a time range (see Time ranges for Incidents, page 20-4 for more information)

- *Incident Path*

The icon that takes you to the incident's path diagram.

- *Incident Vector*

The icon that takes you to the source, event type, and destination diagram.

Time ranges for Incidents

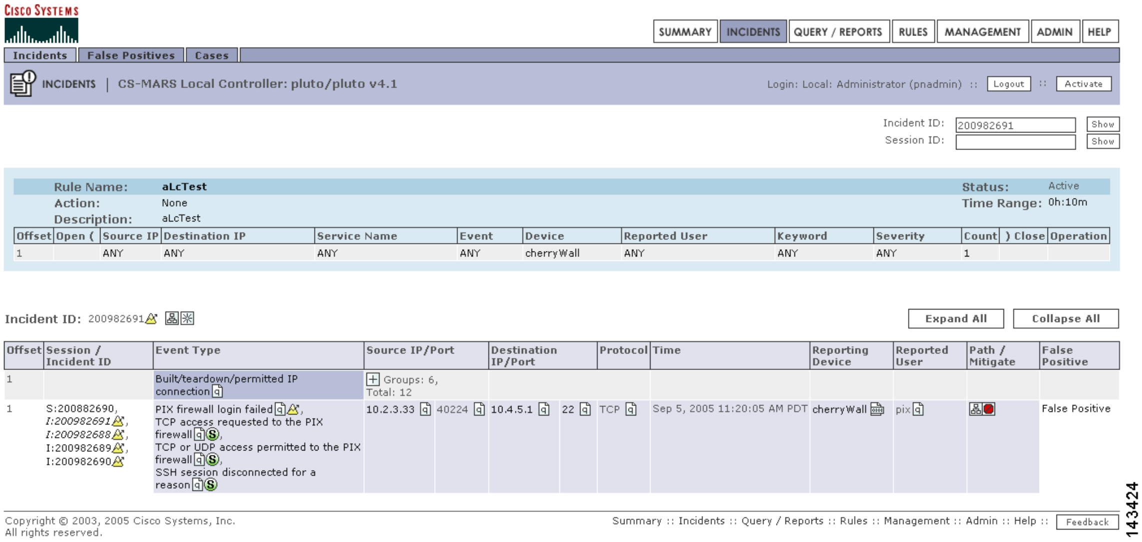
The time column displays both single entries for time (Sep 6, 2003 12:09:54 PM PDT), and time ranges (Sep 6, 2003 12:06:43 PM PDT - Sep 6, 2003 12:06:47 PM PDT).

A single time tells you that all of the firing events were received in the same second. The duration of the incident includes only events that have fired that incident.

Incident Details Page

Clicking the Incident ID takes you to its Incident Details page. The Incident Details page is rich in information and information gathering tools. This page answers questions, such as who did it, what event types happened, when it happened, and to whom it happened.

Figure 20-3 The Incident Details Page



CS-MARS Local Controller: pluto/pluto v4.1

Login: Local: Administrator (pnadmin)

Incident ID: 200982691

Session ID:

Rule Name: aLcTest

Status: Active

Action: None

Time Range: 0h:10m

Description: aLcTest

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		ANY	ANY	ANY	ANY	cherryWall	ANY	ANY	ANY	1		

Incident ID: 200982691

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		Built/teardown/permitted IP connection	⊞ Groups: 6, Total: 12							
1	S:200882690, *I:200982691*, *I:200982688*, I:200982689, I:200982690	PIX firewall login failed, TCP access requested to the PIX firewall, TCP or UDP access permitted to the PIX firewall, SSH session disconnected for a reason	10.2.3.33 40224	10.4.5.1 22	TCP	Sep 5, 2005 11:20:05 AM PDT	cherryWall	pix		False Positive

Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help ::

On the top of this page are the tools that let you search for Incident and Session ID and view the Matched Rule.

To Search for a Session ID or Incident ID

Step 1 Enter the ID into the appropriate field.

Step 2 Click the **Show** button.

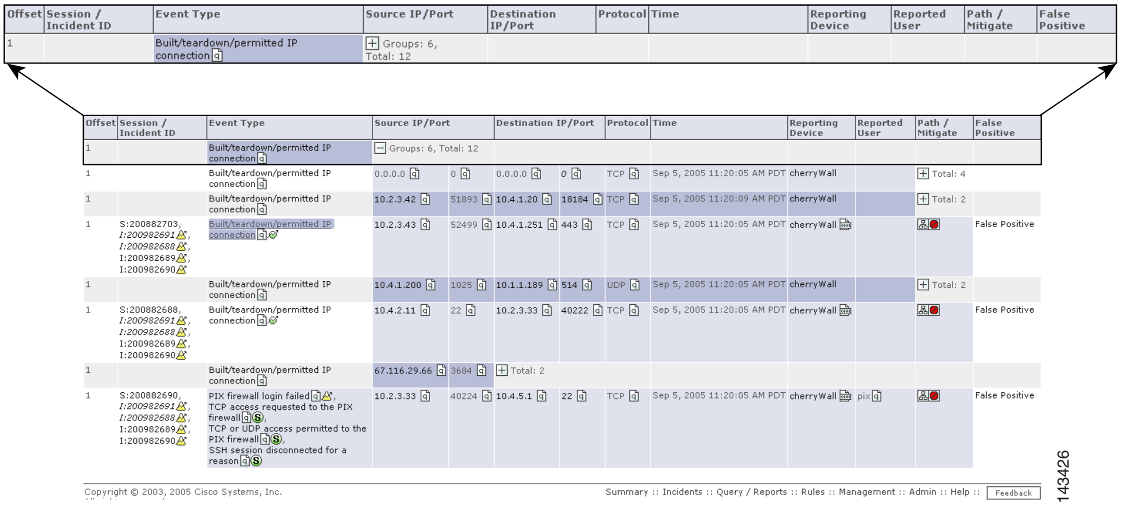
To view a partially hidden rule

Click the Show button next to the Rule Description.

Incident Details Table

Each row of the Incident Details table represents either a session or the information common to a group of sessions. You can see all of the collapsed session information by clicking the plus signs to expand the group. You can expand or collapse all of the incident's information by clicking the **Expand All** or **Collapse All** buttons.

Figure 20-4 Expanding a Row in a Table'



Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		Built/teardown/permitted IP connection	⊞ Groups: 6, Total: 12							

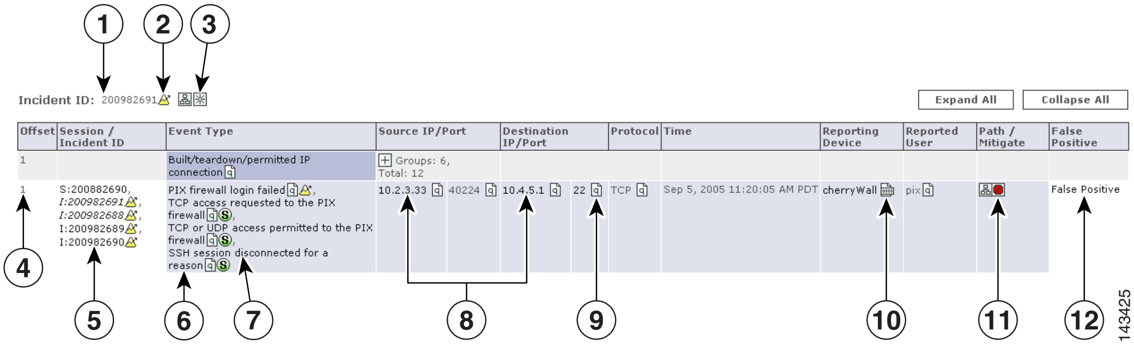
Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		Built/teardown/permitted IP connection	⊟ Groups: 6, Total: 12							
1		Built/teardown/permitted IP connection	0.0.0.0 0	0.0.0.0 0	TCP	Sep 5, 2005 11:20:05 AM PDT	cherryWall		⊞ Total: 4	
1		Built/teardown/permitted IP connection	10.2.3.42 51893	10.4.1.20 18184	TCP	Sep 5, 2005 11:20:09 AM PDT	cherryWall		⊞ Total: 2	
1	S:200882703, I:200982691, I:200982688, I:200982689, I:200982690	Built/teardown/permitted IP connection	10.2.3.43 52499	10.4.1.251 443	TCP	Sep 5, 2005 11:20:05 AM PDT	cherryWall			False Positive
1		Built/teardown/permitted IP connection	10.4.1.200 1025	10.1.1.189 514	UDP	Sep 5, 2005 11:20:05 AM PDT	cherryWall		⊞ Total: 2	
1	S:200882688, I:200982691, I:200982688, I:200982689, I:200982690	Built/teardown/permitted IP connection	10.4.2.11 22	10.2.3.33 40222	TCP	Sep 5, 2005 11:20:05 AM PDT	cherryWall			False Positive
1		Built/teardown/permitted IP connection	67.116.29.66 3684	⊞ Total: 2						
1	S:200882690, I:200982691, I:200982688, I:200982689, I:200982690	PIX firewall login failed, TCP access requested to the PIX firewall, TCP or UDP access permitted to the PIX firewall, SSH session disconnected for a reason	10.2.3.33 40224	10.4.5.1 22	TCP	Sep 5, 2005 11:20:05 AM PDT	cherryWall	pix		False Positive

Copyright © 2003, 2005 Cisco Systems, Inc.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help ::
Feedback
143426

This high-density information table lets you drill deep into incidents. Click the Query icon anywhere on this page to query on a particular criteria. Click the Raw Events icon for raw events for a particular session. You can click the **Tune** link to tune incidents for False Positives, see The False Positive Page, page 20-8 or click the **Mitigate** link to mitigate an attack.

Figure 20-5 Incident Table



Incident ID: 200982691

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		Built/teardown/permitted IP connection	⊞ Groups: 6, Total: 12							
1	S:200882690, I:200982691, I:200982688, I:200982689, I:200982690	PIX firewall login failed, TCP access requested to the PIX firewall, TCP or UDP access permitted to the PIX firewall, SSH session disconnected for a reason	10.2.3.33 40224	10.4.5.1 22	TCP	Sep 5, 2005 11:20:05 AM PDT	cherryWall	pix		False Positive

1	Incident ID	**2**	Severity icon
3	Path and Incident Vector icons. Launch popup windows to display Path and Incident Vector diagrams (L2 or L3 attack path information)	**4**	Offset number
5	Links to Session and Incident Detail pages of all incidents within the session	**6**	Links to the Event Type Details pages

7	Launchs False Positive popup window	**8**	Link to the Device Information page
9	Query icon links to Query page	**10**	Click Device icon to launch popup window to display raw message information
11	Link to the Mitigation Information page	**12**	Link to the False Positive Tuning page

The following information describes some of the fine points of this table.

- *Instances*

Sometimes rows are split into instances. The *only* relationship among the different instances is that they fired the same rule in the same time frame.

- *Session/Incident ID*

This column shows the sessions that contributed to the incident, and the other incidents those sessions belong to.

- *Events column*

The Events column shows types of the firing events. Multiple firing events of the same types are shown once per session.

- *Time column*

An incident's duration only includes the events that contributed to the incident firing.

False Positive Confirmation

When investigating incidents, you will invariably come across false positive events. In some cases, firing events are classified automatically by MARS as system-confirmed false positives and unconfirmed false positives. Vulnerability scanning often identifies the false positive events, but at times you must investigate events to determine their validity.

To understand the false positive nomenclature and what tasks you are expected to perform within the user interface, we must study the possibilities among three variables surrounding possible attacks: legitimate attack, valid target, and attack detected. We examine these differences in Table 20-1.

Table 20-1 Attack Type Truth Table

	Legitimate Attack	Valid Target	Attack Detected
invalid scenario	0	0	0
False Positive	0	0	1
invalid scenario	0	1	0
False Positive	0	1	1
False Negative	1	0	0
Attack/Alarm (noise)	1	0	1
True False Negative	1	1	0
Intrusion/True Alarm	1	1	1

Based on the valid cases in Table 20-1, we can clearly distinguish the false positive terminology:

- A *legitimate attack* is an actual attempt by an attacker to gain access to or information about a specific host using a known exploit.
- A *valid target* is a host that is susceptible to the launched attack. A host can become an *invalid target* if it is properly patched or has some other preventative measure in place, such as a local firewall, virus scanner, or intrusion prevention software that guards against the attack.
- *Attack detected* refers to whether the monitoring device detected the attack and generated an alarm.
- A *false positive* is when the monitoring system generates an alarm for a condition that is benign. In this case, there is no legitimate attack, despite the alarm generation.
- An *unconfirmed false positive* is one where the monitoring system, based on data not available to the reporting device, has determined that an alarm is a false positive. Unconfirmed refers to the fact that the administrator must review and accept or reject the assessment of the false positive.
- A *false negative* is when the monitoring system fails to detect a legitimate attack.
- *Noise* refers to those alarms that are triggered due to attacks against invalid targets. While they can represent real attacks, the target cannot be compromised due to preventative measures. Attacks that fall within the noise category are of secondary importance in terms of investigation and mitigation.
- *Intrusion* identifies a successful attack against the host, where the host is compromised by the attacker.
- A *true false negative* identifies an intrusion that remains undetected by the monitoring system.
- A *true alarm* identifies an intrusion that is detected by the monitoring system.

When a Local Controller receives an event, it is evaluated against the conditions of the defined rules. If the event satisfies the conditions of a rule, then the incident triggers. When an event triggers an incident, we refer to that event as a *firing event*. False positive analysis is performed for such firing events to reduce the number of false alarms.

Using built-in event vulnerability data, learned topology paths, sessionized event data, ACL analysis of layer 2 and 3 reporting devices, supporting data from 3rd-party vulnerability analysis (VA) software (such as Foundstone and eEye), and information that you provide about hosts, MARS analyzes the firing events reported to it determine whether the they hold up to a higher-level review.

In the case of MARS, a *system-confirmed false positive* is where, after further analysis, a firing event is determined to be invalid. Example system-confirmed false positives include:

- When an IDS device monitoring the network outside of a firewall reports an attack; however, the firewall drops that session as part of its standard access restrictions. Therefore, the attack never reaches the target.
- Cisco Security Agent detects an attack and blocks it.

An *unconfirmed false positive* is where, after further analysis, the firing event is believed to be invalid primarily due to the attack being against an invalid target. Example unconfirmed false positives include

- A reporting device reports a valid attack against a host; however, the host is not susceptible to that attack because it targets a different operating system. You can reduce these types of false positives by employing OS fingerprinting technologies on the reporting devices.
- A reporting device reports a valid attack against a host's application; however, the host is not susceptible to that attack because it targets a different application.
- A reporting device reports a valid web attack against TCP port 80, however, dynamic probing determines that no services on the target host listen to TCP port 80.

For unconfirmed false positives, you must manually investigate the alarm and specify in Local Controller whether it is an actual false positive. For actual false positives, you should define a drop rule for the event. Defining a drop rule does not mean that the event is not stored in the database, you have the option of dropping the event from incident evaluation and either shoring it in the database or not. Whether you store the event in the database or not, events matching the event type and target host can no longer act as firing events. By refining the event processing in this fashion, MARS frees up your time to focus on actual incidents by more accurately correlating events into incidents and reducing noise.

As part of your operational strategy, you should strive to refine event generation and processing to tune out the possibility for false positives. You can perform such tuning at the device level, by refining what traffic or action can generate an event, and at the Local Controller level by providing more information about your network, such as identifying the operating system of hosts attached to the network segments monitored by that Local Controller.

The False Positive Page

To navigate to the False Positives page, click **Incidents**, and click the **False Positives** sub-tab.

The False Positives page is where you can see groupings of False Positives.

You can filter categories by clicking on the **Select False Positive** drop-down list. Your choices are:

- *Unconfirmed false positive type*

For this type, the MARS needs user confirmation to determine if the target host is vulnerable to the event type in question.

- *User confirmed false positive type*

For this type, a user has provided confirmation that a firing event is a false positive.

- *User confirmed positive type*

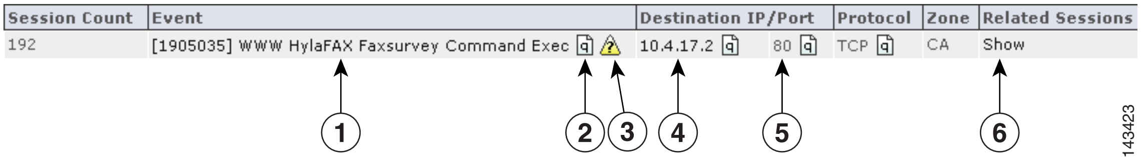
For this type, a user has provided confirmation that a firing event is a true attack.

- *System determined false positive type*

For this type, the system has determined that a firing event is a false positive.

In the False Positives table, you can see how many sessions the false positive has appeared in, the event type, the false positive status confirmation icons, the event type information icon, the destination IP and its port, the destination IP information icon, its protocol, zone, and you can see the sessions that are related to the false positive.

Figure 20-6 False Positive Table



Session Count	Event	Destination IP/Port		Protocol	Zone	Related Sessions
192	[1905035] WWW HylaFAX Faxsurvey Command Exec	10.4.17.2	80	TCP	CA	Show

1	Link to the Event Type Details page	**2**	Query icon links to the Query page and automatically populates the corresponding Query field
3	False Positive type and severity icon	**4**	Launches the Security Device Information popup window
5	Launches Port Information popup window	**6**	Launches False Positive Sessions Details popup window

The following table shows false positive status confirmation and severity icons:Tuning False Positives

Icon	Description
? ? ?	Low, medium, and high severity false positives that require confirmation.
F F F	Low, medium, and high severity user determined false positives.
S S S	Low, medium, and high severity system determined false positives.

From the Incidents page or the False Positives page, you can tune false positives – to verify if they are true or false.

To Tune a False Positive

Step 1 Click one of the **Confirm False Positive** icons. ? ? ?

Step 2 On the False Positive Confirmation page, review the information.

Step 3 If you decide that the event type is a false positive, click the **Yes** radio button, and follow the steps in: To Tune an Unconfirmed False Positive to False Positive, page 20-9.

Step 4 If you decide that the event type is a true positive, click the **No** radio button, and follow the steps in: To Tune an Unconfirmed False Positive to True Positive, page 20-9.

To Tune an Unconfirmed False Positive to False Positive

Step 1 After you determine that a false positive is false, and you have clicked the **Yes** button, click **Next**.

Step 2 On the next page, decide whether or not you want MARS to keep this event type in the database by selecting the appropriate radio button:

- **Dropping these events completely** (that stops logging those events)
- **Log to DB only** (that logs the events to the DB)

Step 3 Once you have decided, click the **Next** button.

Step 4 On the next page, carefully review the information for the false positive and the new rule.

Step 5 When you are ready to commit this new information to the appliance, click the **Confirm** button.

To Tune an Unconfirmed False Positive to True Positive

Step 1 After you determine that a false positive is true, and you have clicked the **No** button, click **Next**.

Step 2 Make a final confirmation that this is a true positive, and click the **Confirm** button.

To Activate False Positive Drop Rules

After you have completed tuning false positives, click **Activate** to immediately implement the changes.

Mitigation

Mitigation refers to the action of limiting an attacking network element's access to the network by modifying the configuration of an enforcement device, usually a switch, router, or firewall. CS-MARS can perform the following actions related to mitigation:

- Identify attacking and compromised hosts
- Plot Layer 2 and Layer 3 topology of the affected network segment to identify mitigation points and enforcement devices
- Recommend configuration commands for Layer 2 and Layer 3 enforcement devices
- Push (that is, download) recommended configuration commands to supported Layer 2 devices

With Telnet, SSH, or SNMP access to switches and routers, CS-MARS can recommend and push mitigation configurations to enforcement devices, as well as generate interactive topology and incident path diagrams. Without Telnet, SSH, or SNMP access, some mitigation information can still be obtained from Cisco switches running specific IEEE 802.1X Port Based Network Access Control protocol configurations, but recommended mitigation commands must be configured manually on the enforcement devices. See Layer 2 Path and Mitigation Configuration Example, page 20-17 for further information and procedures for configuring Layer 2 devices to receive CS-MARS mitigation commands.

Static and Dynamic Network Information

Topology information obtained from access to relatively permanent Layer 2 and Layer 3 devices is called Static Information in the HTML interface. Dynamic Information refers to frequently changing information such as host names, or DHCP-leased IP addresses obtained through devices or agents that report dynamic events, such as 802.1X access control configurations, the Cisco Security Agent, or other security suite software. The CS-MARS can determine a mitigation point and an enforcement device if a Cisco 802.1X-enabled switch is running DHCP-snooping with RADIUS authentication through a Cisco Access Control Server (ACS). When a DHCP-snooping transaction is completed, the switch sends a log message to the ACS. The ACS logs are sent to the CS-MARS to report the Source IP address, user name, connection start and stop times, physical interface, and MAC address of each 802.1X client. Because 802.1X clients are often mobile, remember that 802.1X mitigation actions can occur only when the attacking host is currently connected to the network.

Note For some 802.1X switch configurations, it is not possible for CS-MARS to determine the correct physical interface to which to push a mitigation command. This occurs for switches, such as the Cisco Catalyst 3550 Multilayer switch, where a FastEthernet and a Gigabit Ethernet port can have the same *module/port* designation (for example, 0/1). Because CS-MARS receives only the *module/port* information from the Cisco ACS logs, it cannot identify the specific port to mitigate. The following message appears in these circumstances:
No mitigation possible. Enforcement device exists but interface names conflict. Determine appropriate interface and mitigate manually.

802.1X Mitigation Example

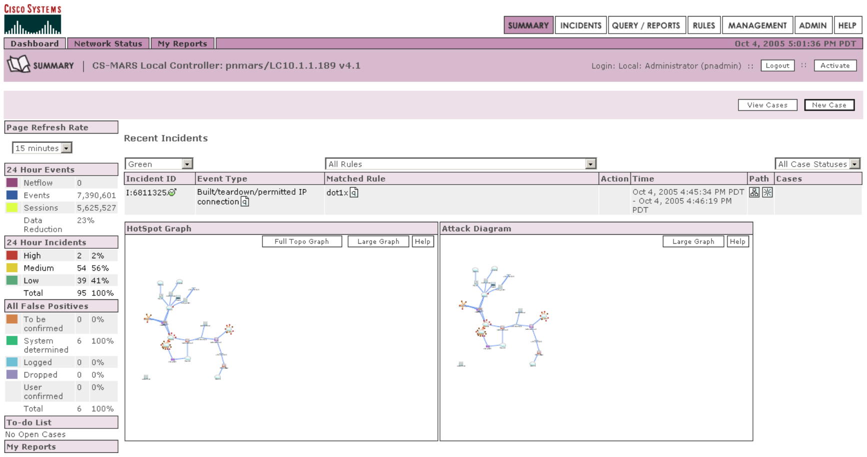
In this procedure, an incident is observed on the Network Summary page, as shown in Figure 20-7, and mitigated through 802.1X network mapping.

Prerequisites for Mitigation with 802.1X Network Mapping

To perform mitigation with 802.1X network mapping with CS-MARS, the following prerequisites are required:

- Cisco switch running Cisco CatOS or IOS and configured with IEEE 802.1X Port Based Network Access Control protocol
- The switch Reporting IP address must be configured on the CS-MARS Security and Monitoring Information page (**Admin** > **Security and Monitor Devices**).
- Cisco DHCP-Snooping enabled on the switch
- The switch performs Remote Access Dial-In User Service (RADIUS) authentication, authorization, and accounting through a Cisco Access Control Server (ACS).
- The Cisco ACS is running pnLogAgent to send logs to CS-MARS
- The Cisco ACS is configured to log Update (Watchdog) packets

Figure 20-7 Summary Page Displaying Incident to Mitigate



CS-MARS Local Controller: pnmars/LC10.1.1.189 v4.1

Login: Local: Administrator (pnadmin)

Page Refresh Rate

24 Hour Events		
🟪	Netflow	0
🟦	Events	7,390,601
🟨	Sessions	5,625,527
	Data Reduction	23%

24 Hour Incidents			
🟥	High	2	2%
🟨	Medium	54	56%
🟩	Low	39	41%
	Total	95	100%

All False Positives			
🟧	To be confirmed	0	0%
🟩	System determined	6	100%
🟦	Logged	0	0%
🟪	Dropped	0	0%
	User confirmed	0	0%
	Total	6	100%

To-do List

No Open Cases

My Reports

Recent Incidents

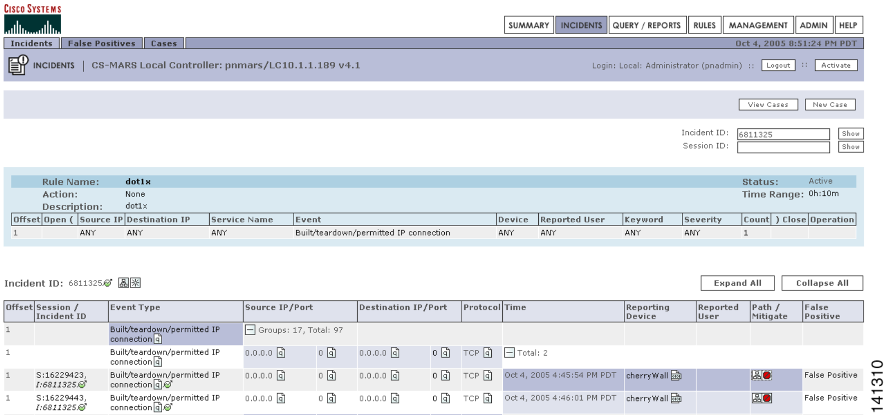
Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:6811325	Built/teardown/permitted IP connection	dot1x		Oct 4, 2005 4:45:34 PM PDT - Oct 4, 2005 4:46:19 PM PDT		

Procedure for Mitigation with 802.1X Network Mapping

Step 1 Click the Incident ID of the recent incident to Mitigate.

Step 2 Click on the Incident ID to display the session summaries, shown in Figure 20-8.

Figure 20-8 Incident Detail Page Displaying Red Mitigation Icon



Oct 4, 2005 8:51:24 PM PDT

INCIDENTS | CS-MARS Local Controller: pnmars/LC10.1.1.189 v4.1

Login: Local: Administrator (pnadmin) ::

Incident ID: 6811325

Session ID:

Rule Name: dot1x

Action: None

Description: dot1x

Status: Active

Time Range: 0h:10m

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		ANY	ANY	ANY	Built/teardown/permitted IP connection	ANY	ANY	ANY	ANY	1		

Incident ID: 6811325

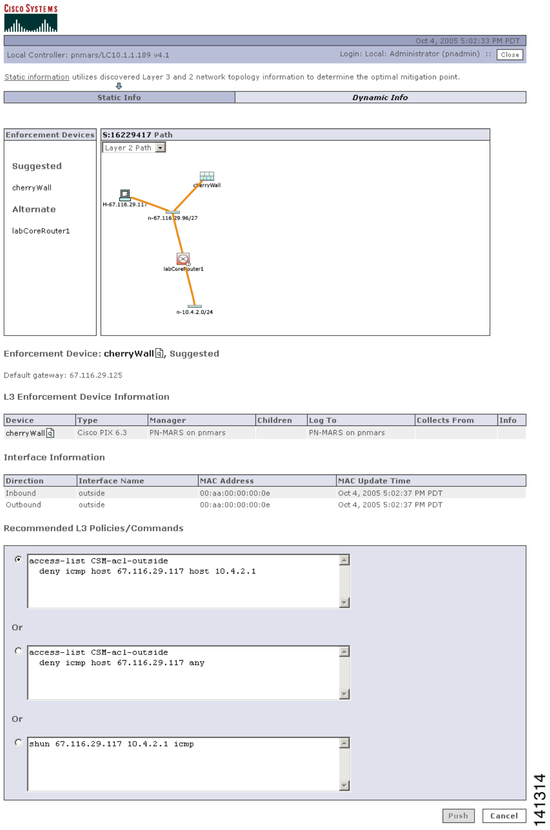
Offset	Session / Incident ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		Built/teardown/permitted IP connection	⊟ Groups: 17, Total: 97									
1		Built/teardown/permitted IP connection	0.0.0.0	0	0.0.0.0	0	TCP	⊟ Total: 2				
1	S:16229423, I:6811325	Built/teardown/permitted IP connection	0.0.0.0	0	0.0.0.0	0	TCP	Oct 4, 2005 4:45:54 PM PDT	cherryWall		●	False Positive
1	S:16229443, I:6811325	Built/teardown/permitted IP connection	0.0.0.0	0	0.0.0.0	0	TCP	Oct 4, 2005 4:46:01 PM PDT	cherryWall		●	False Positive

Step 3 Click the red path information icon in the **Path/Mitigation** column.

The Mitigation pop-up window appears, with any possible Static topology and mitigation information, as shown in Figure 20-9.

CS-MARS recommends enforcement devices and mitigation commands. For static information, if the network is entirely discovered and CS-MARS has command level access to a Layer 2 enforcing device, the Push button appears red, otherwise it is gray. In Figure 20-9, CS-MARS does not have sufficient static information to identify a Layer 2 enforcement device, but can suggest mitigation commands for discovered Layer 3 devices (Cisco PIX firewall, and a Cisco router). Layer 3 mitigation commands must be configured manually on the Layer 3 devices.

Figure 20-9 Path Information Pop-up Window



Local Controller: pnmars/LC10.1.1.189 v4.1 Login: Local: Administrator (pnadmin) ::

Static information utilizes discovered Layer 3 and 2 network topology information to determine the optimal mitigation point.

S:16229417 Path

Suggested

cherryWall

Alternate

labCoreRouter1

Enforcement Device: cherryWall, Suggested

Default gateway: 67.116.29.125

L3 Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
cherryWall	Cisco PIX 6.3	PN-MARS on pnmars		PN-MARS on pnmars		

Interface Information

Direction	Interface Name	MAC Address	MAC Update Time
Inbound	outside	00:aa:00:00:00:0e	Oct 4, 2005 5:02:37 PM PDT
Outbound	outside	00:aa:00:00:00:0e	Oct 4, 2005 5:02:37 PM PDT

Recommended L3 Policies/Commands

●
```
access-list CSM-acl-outside
  deny icmp host 67.116.29.117 host 10.4.2.1
```

Or

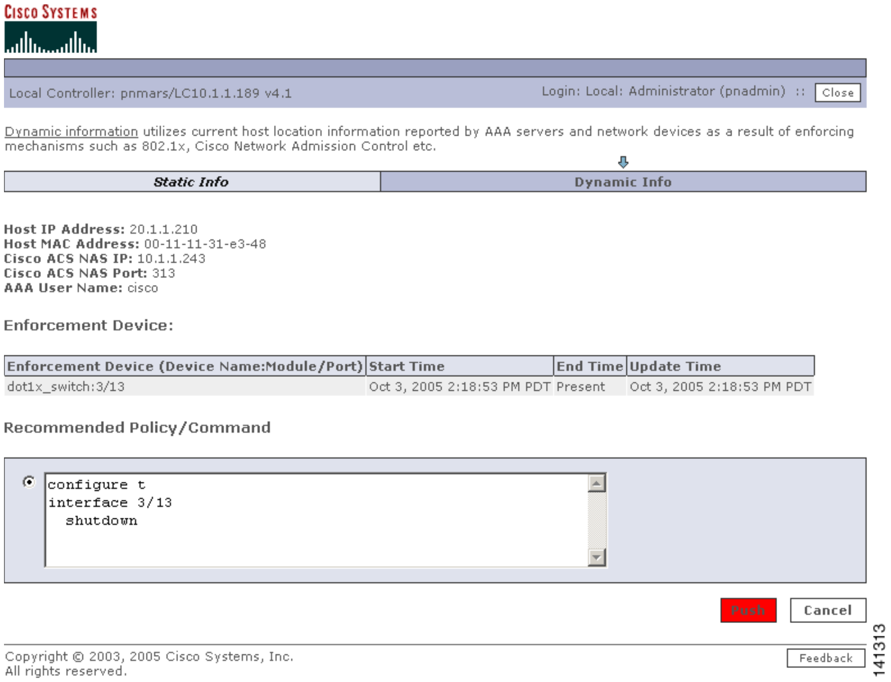
○
```
access-list CSM-acl-outside
  deny icmp host 67.116.29.117 any
```

Or

○
```
shun 67.116.29.117 10.4.2.1 icmp
```

Step 4 Click **Dynamic Info** to view Layer 2 mitigation recommendations derived from 802.1X configurations. The Dynamic Mitigation window appears with host name, IP address, MAC address, and connection status as shown in Figure 20-10.

Figure 20-10 Dynamic Mitigation Information



Local Controller: pnmars/LC10.1.1.189 v4.1 Login: Local: Administrator (pnadmin) ::

Dynamic information utilizes current host location information reported by AAA servers and network devices as a result of enforcing mechanisms such as 802.1x, Cisco Network Admission Control etc.

Host IP Address: 20.1.1.210
Host MAC Address: 00-11-11-31-e3-48
Cisco ACS NAS IP: 10.1.1.243
Cisco ACS NAS Port: 313
AAA User Name: cisco

Enforcement Device:

Enforcement Device (Device Name:Module/Port)	Start Time	End Time	Update Time
dot1x_switch:3/13	Oct 3, 2005 2:18:53 PM PDT	Present	Oct 3, 2005 2:18:53 PM PDT

Recommended Policy/Command

●
```
configure t
interface 3/13
  shutdown
```

Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.

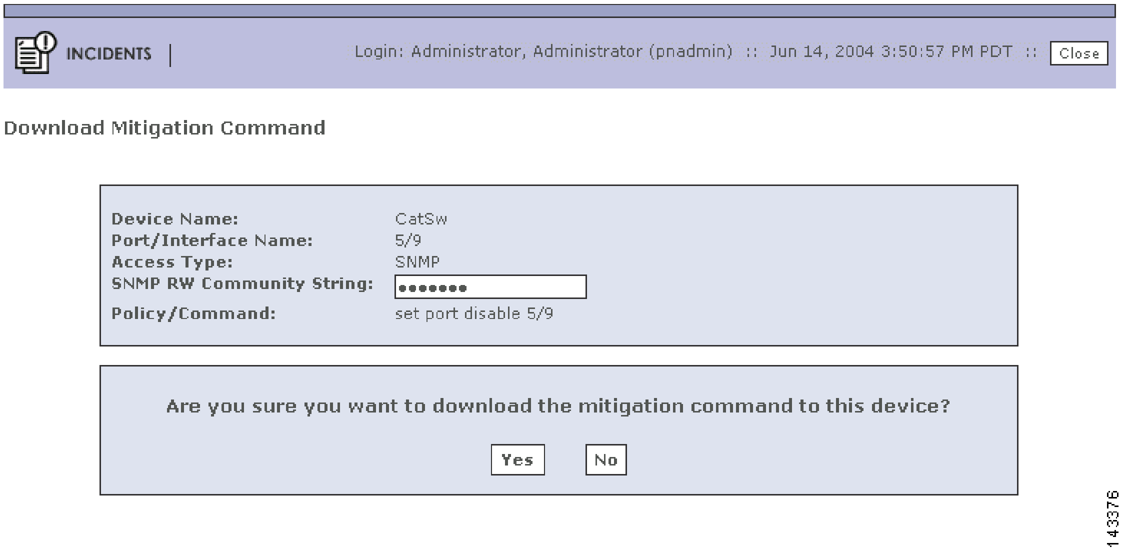
Step 5 Review the enforcement device.

Step 6 Review the Recommended Policies/Commands.

Step 7 Click **Push** to download the recommended mitigation command to the enforcement device. The mitigation confirmation dialog appears, as shown in Figure 20-11.
If the Push button is gray, the mitigation command must be manually configured on the enforcement device.

Note The **Push** button is red and functional when the 802.1X target host is present on the network, and CS-MARS has command access to the enforcement device otherwise, it appears gray and is not functional.

Figure 20-11 Mitigation Confirmation Dialog



INCIDENTS
Login: Administrator, Administrator (pnadmin) :: Jun 14, 2004 3:50:57 PM PDT ::
Close
Yes
No
143376

Download Mitigation Command

Device Name:	CatSw
Port/Interface Name:	5/9
Access Type:	SNMP
SNMP RW Community String:	•••••••
Policy/Command:	set port disable 5/9

Are you sure you want to download the mitigation command to this device?

Step 8 Click **Yes** to confirm.

Display Dynamic Device Information

To display current, session, and all historical information for an IP address on an 802.1X connection, follow these steps:

Step 1 Click on the Incident ID to display the session summaries as shown in Figure 20-8.

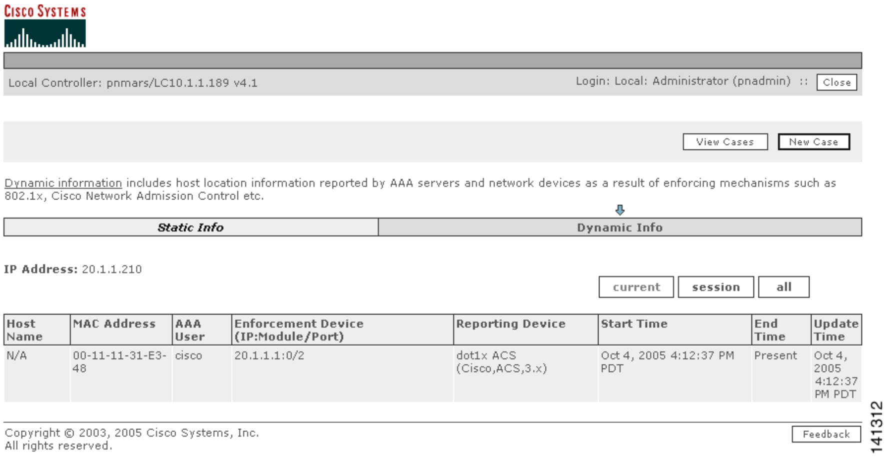
Step 2 Click on the **Source IP/Port** or **Destination IP** link of a session.
When examining an attacking host, the Source IP address is more relevant.

Step 3 The current connection information pop-up window appears to display any static connection information.

Step 4 Click **Dynamic Info** to display current connection information, as shown in Figure 20-11.
Dynamic information can be derived from 802.1X configurations, Cisco Security Agents, or from other security software suites. The current connection information is the most recent network information available for the selected IP address.

Step 5 Click **Session** to display the connections related to the specific session, a shown in Figure 20-13.

Figure 20-12 Dynamic Information—Current Connection Status



Local Controller: pnmars/LC10.1.1.189 v4.1

Login: Local: Administrator (pnadmin) ::

Dynamic information includes host location information reported by AAA servers and network devices as a result of enforcing mechanisms such as 802.1x, Cisco Network Admission Control etc.

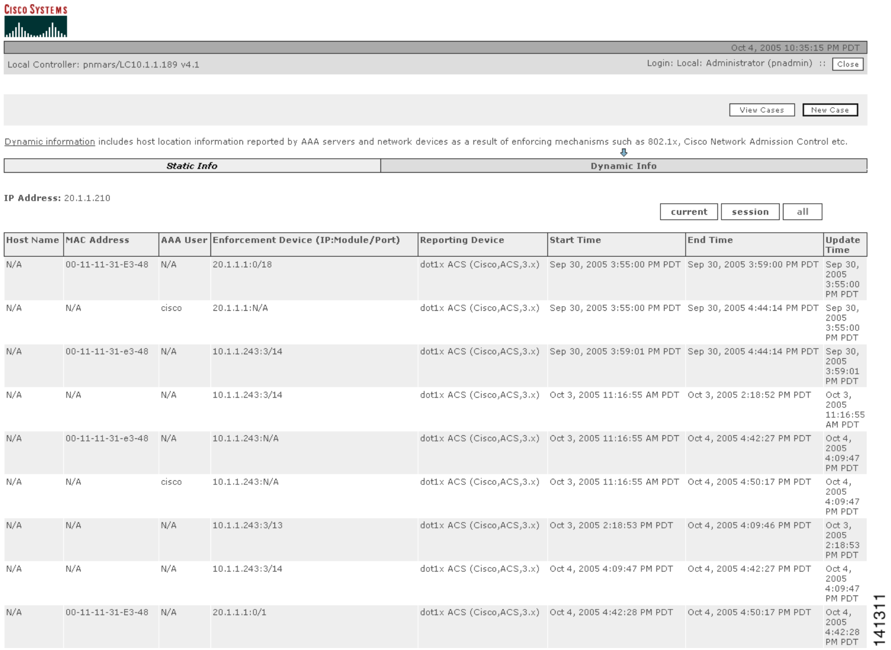
IP Address: 20.1.1.210

Host Name	MAC Address	AAA User	Enforcement Device (IP:Module/Port)	Reporting Device	Start Time	End Time	Update Time
N/A	00-11-11-31-E3-48	cisco	20.1.1.1:0/2	dot1x ACS (Cisco,ACS,3.x)	Oct 4, 2005 4:12:37 PM PDT	Present	Oct 4, 2005 4:12:37 PM PDT

Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.

Step 6 Click **All** to display the entire dynamic information for the specified IP address, as shown in Figure 20-13.

Figure 20-13 Dynamic Information History of a Specified IP Address



Oct 4, 2005 10:35:15 PM PDT

Local Controller: pnmars/LC10.1.1.189 v4.1

Login: Local: Administrator (pnadmin) ::

Dynamic information includes host location information reported by AAA servers and network devices as a result of enforcing mechanisms such as 802.1x, Cisco Network Admission Control etc.

IP Address: 20.1.1.210

Host Name	MAC Address	AAA User	Enforcement Device (IP:Module/Port)	Reporting Device	Start Time	End Time	Update Time
N/A	00-11-11-31-E3-48	N/A	20.1.1.1:0/18	dot1x ACS (Cisco,ACS,3.x)	Sep 30, 2005 3:55:00 PM PDT	Sep 30, 2005 3:59:00 PM PDT	Sep 30, 2005 3:55:00 PM PDT
N/A	N/A	cisco	20.1.1.1:N/A	dot1x ACS (Cisco,ACS,3.x)	Sep 30, 2005 3:55:00 PM PDT	Sep 30, 2005 4:44:14 PM PDT	Sep 30, 2005 3:55:00 PM PDT
N/A	00-11-11-31-e3-48	N/A	10.1.1.243:3/14	dot1x ACS (Cisco,ACS,3.x)	Sep 30, 2005 3:59:01 PM PDT	Sep 30, 2005 4:44:14 PM PDT	Sep 30, 2005 3:59:01 PM PDT
N/A	N/A	N/A	10.1.1.243:3/14	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 11:16:55 AM PDT	Oct 3, 2005 2:18:52 PM PDT	Oct 3, 2005 11:16:55 AM PDT
N/A	00-11-11-31-e3-48	N/A	10.1.1.243:N/A	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 11:16:55 AM PDT	Oct 4, 2005 4:42:27 PM PDT	Oct 4, 2005 4:09:47 PM PDT
N/A	N/A	cisco	10.1.1.243:N/A	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 11:16:55 AM PDT	Oct 4, 2005 4:50:17 PM PDT	Oct 4, 2005 4:09:47 PM PDT
N/A	N/A	N/A	10.1.1.243:3/13	dot1x ACS (Cisco,ACS,3.x)	Oct 3, 2005 2:18:53 PM PDT	Oct 4, 2005 4:09:46 PM PDT	Oct 3, 2005 2:18:53 PM PDT
N/A	N/A	N/A	10.1.1.243:3/14	dot1x ACS (Cisco,ACS,3.x)	Oct 4, 2005 4:09:47 PM PDT	Oct 4, 2005 4:42:27 PM PDT	Oct 4, 2005 4:09:47 PM PDT
N/A	00-11-11-31-E3-48	N/A	20.1.1.1:0/1	dot1x ACS (Cisco,ACS,3.x)	Oct 4, 2005 4:42:28 PM PDT	Oct 4, 2005 4:50:17 PM PDT	Oct 4, 2005 4:42:28 PM PDT

Step 7 Click the **Push** button if available or mitigate from the device. If you select the push button, a confirmation screen appears.

Note To mitigate a device of Access Type SNMP you must have the SNMP Read/Write Community String.

Click the **Yes** button to confirm the mitigation command and have it take effect.

Virtual Private Network Considerations

Currently, MARS cannot display accurate Path/Mitigation information or compute the complete route of an attack originated by a host with a source IP address on a virtual private network (VPN). MARS can identify the attacking host if the VPN IP address of the host was supplied by a Cisco 3000 Series VPN Concentrator configured as a MARS reporting device.

Note You must be able to recognize from your knowledge of your network that the IP address of the attacking host is an IP address allocated to a VPN.

To identify a host attacking from a VPN, perform a query of "Cisco VPN User connected/disconnected" events for the Cisco VPN Concentrator device. The attacking host name or next network element is disclosed in the raw messages of the events.

Layer 2 Path and Mitigation Configuration Example

This section provides a starting point for configuring MARS to perform Layer 2 (L2) path analysis and mitigation using a Cisco switch. It contains the following sections:

Prerequisites for Layer 2 Path and Mitigation

- You need to have the SNMP community strings and IP addresses for the Layer 2 switches and routers.
- You must have STP (Spanning Tree Protocol) configured correctly on the switches.

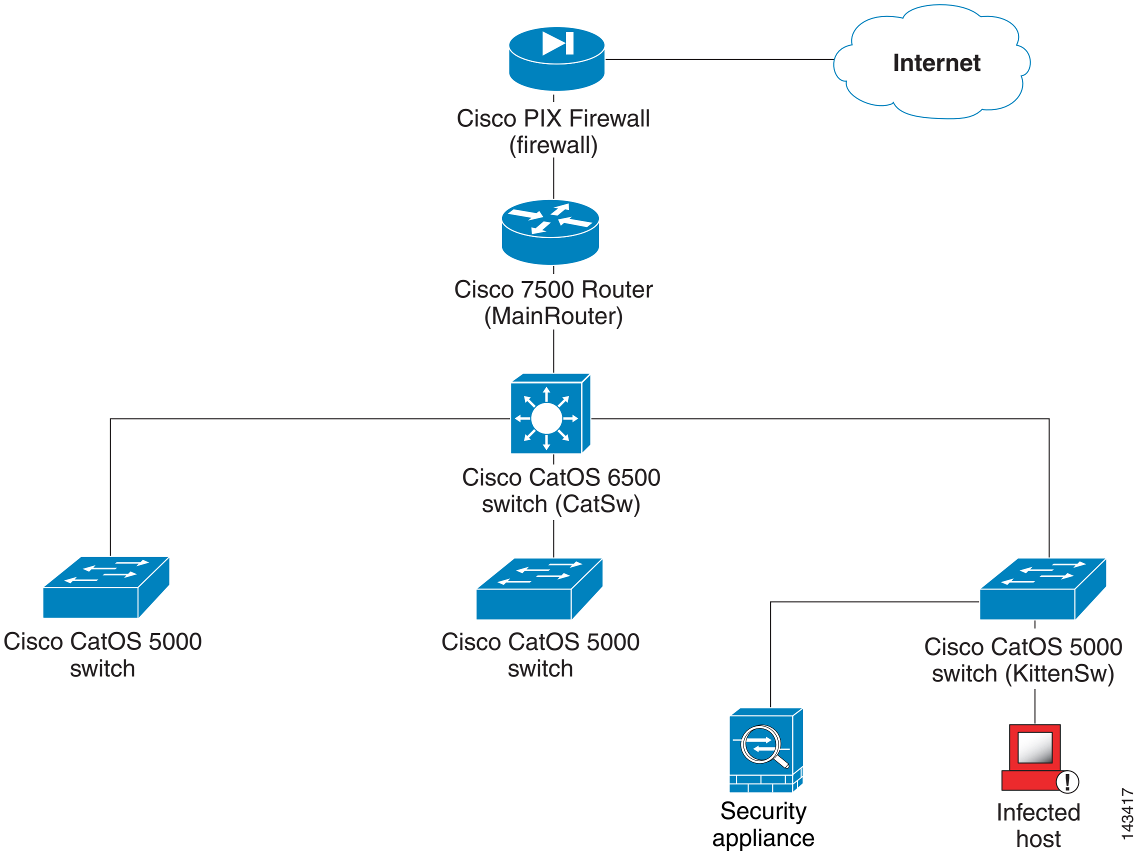
Components Used

- a Cisco Catalyst 5000 with SNMP access enabled
- a Cisco Catalyst 6500 for Layer 2 with SNMP access enabled
- a Cisco 7500 Router with SNMP or TELNET access enabled
- a MARS running software Version 2.5.1

Network Diagram

This section uses the network setup shown in the Figure 20-14.

Figure 20-14 Network Setup



Mitigation uses the Layer 2 path data obtained via SNMP or Telnet protocol to download a mitigation command from the MARS to the device. The Layer 2 path is based on MAC addresses, the Layer 2 forwarding table, and the Layer 3 path. MAC addresses and the Layer 2 forwarding table are obtained using SNMP.

To make the Layer 2 path and mitigation work correctly:

- The associated routers must be discovered via SNMP or a combination of SNMP and Telnet, including the MSFC module in the Catalyst switch.
- The SNMP community string is necessary for L2 switches to be discovered

Note *L2 devices must be added manually; there is no automatic discovery for these devices.* Make sure all the L2 devices (switches) have the SNMP RO community strings specified in the web interface, even if the access type is not SNMP. The SNMP RO community string is always required on Layer 2 devices for L2 mitigation.

- If the switches are interconnected, make sure STP (Spanning Tree Protocol) is enabled and configured on them.

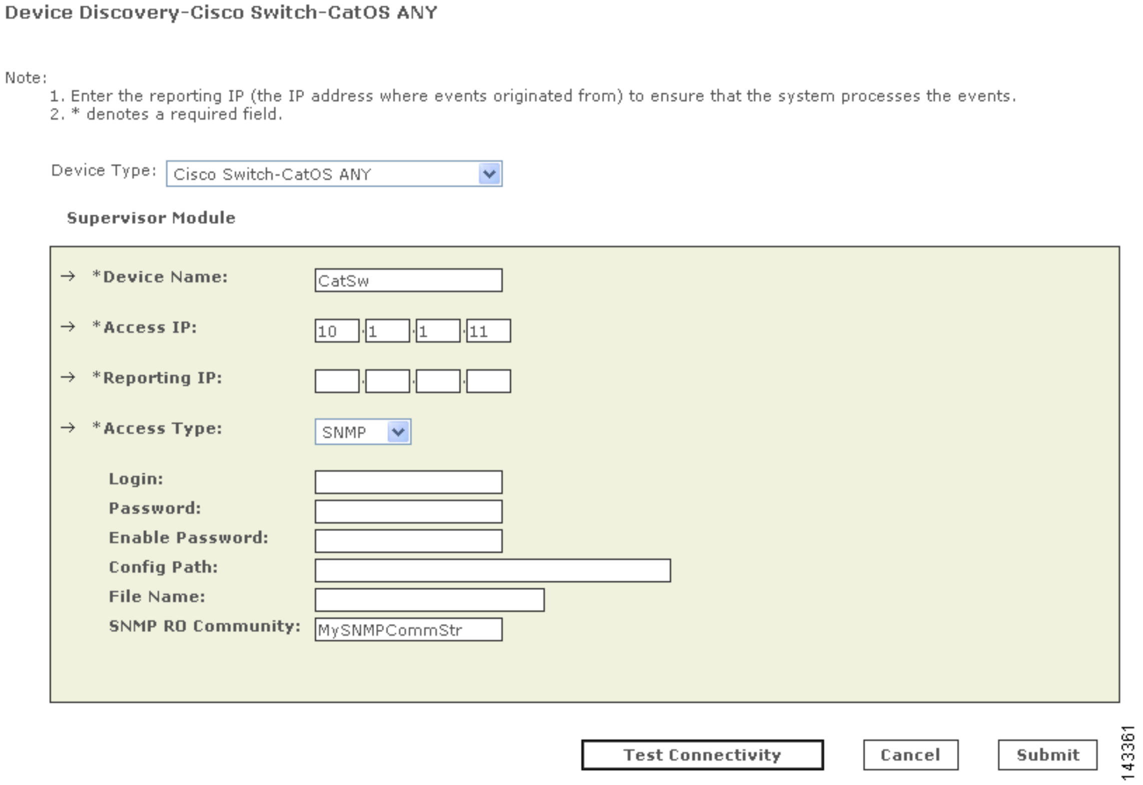
For example, given a topology such as the one in the preceding figure, follow these instructions to discover these devices.

Procedures for Layer 2 Path and Mitigation

Add the Cisco Catalyst 5000 with SNMP as the Access Type.

Step 1 Click **Admin** > **Security and Monitor Devices** > **Add**.

Figure 20-15 Configure Cisco Switch CatOS



Device Discovery-Cisco Switch-CatOS ANY

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco Switch-CatOS ANY

Supervisor Module

→ *Device Name: CatSw
→ *Access IP: 10 . 1 . 1 . 11
→ *Reporting IP:
→ *Access Type: SNMP
Login:
Password:
Enable Password:
Config Path:
File Name:
SNMP RO Community: MySNMPCommStr

Step 2 From the **Device Type** drop-down list, select **Cisco Switch-CatOS ANY**.

Step 3 Enter the **Device Name** of the switch.

Step 4 Enter the **Access IP** address and **Reporting IP** address (the IP address of the device as it appears to the MARS) of the switch. The **Reporting IP** address is usually the same as the **Access IP** address, but if you are using FTP as Access Type, it must be a different IP address. The **Reporting IP** address is required if the device is sending syslog data to the MARS

Step 5 From the **Access Type** drop-down list, select **SNMP** or **TELNET**. Note that which fields need to be completed, along with which you can complete, depend on which Access Type you select.

SNMP:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.

- Enter its **SNMP RO Community**.

TELNET:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community**.

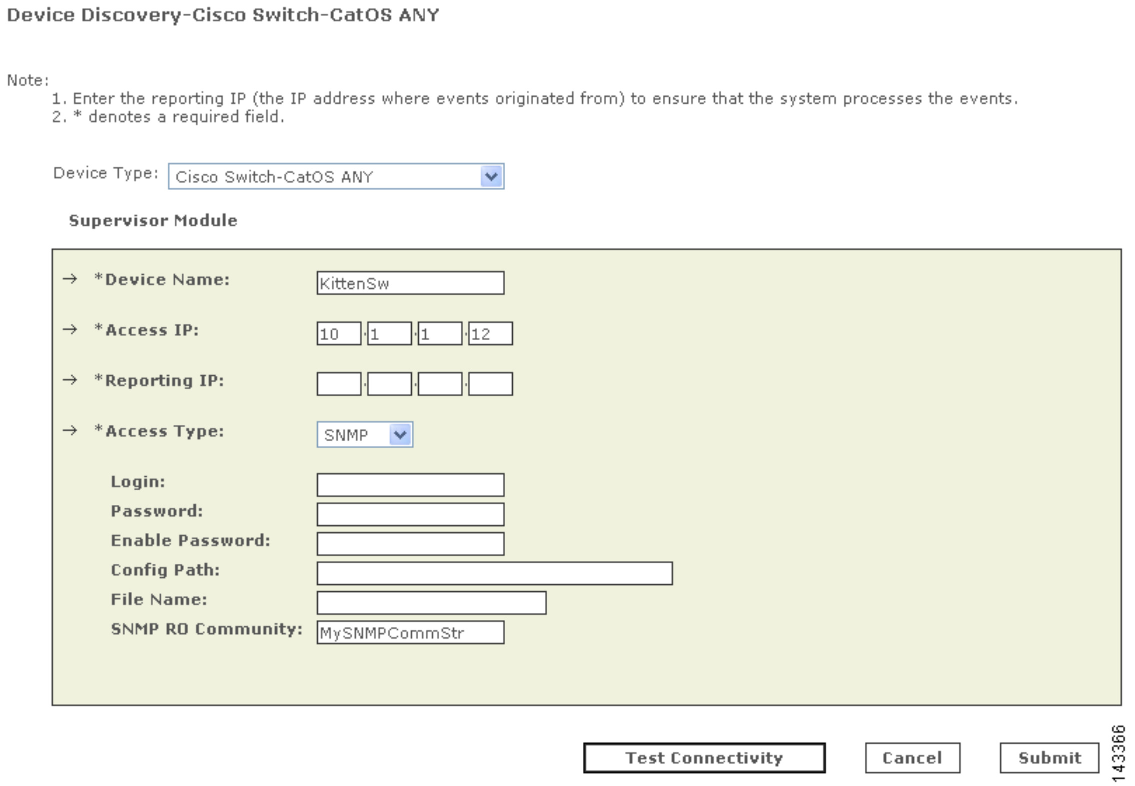
Step 6 Click the **Test Connectivity** button to have the MARS discover the device.

Step 7 Click the **Submit** button.

Add the Cisco Catalyst 6500 with SNMP as Access Type (Layer 2 only).

Step 1 Click **Admin** > **Security and Monitor Devices** > **Add**.

Figure 20-16 Configure Cisco Switch CatOS



Device Discovery-Cisco Switch-CatOS ANY

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco Switch-CatOS ANY

Supervisor Module

→ *Device Name: KittenSw
→ *Access IP: 10 . 1 . 1 . 12
→ *Reporting IP: . . .
→ *Access Type: SNMP
Login:
Password:
Enable Password:
Config Path:
File Name:
SNMP RO Community: MySNMPCommStr

Step 2 From the **Device Type** drop-down list, select **Cisco Switch-CatOS ANY**.

Step 3 Enter the **Device Name** of the switch.

Step 4 Enter the **Access IP** address and **Reporting IP** address of the switch. The **Reporting IP** address is usually the same as the **Access IP** address.

SNMP:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.

- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community**.

TELNET:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community**.

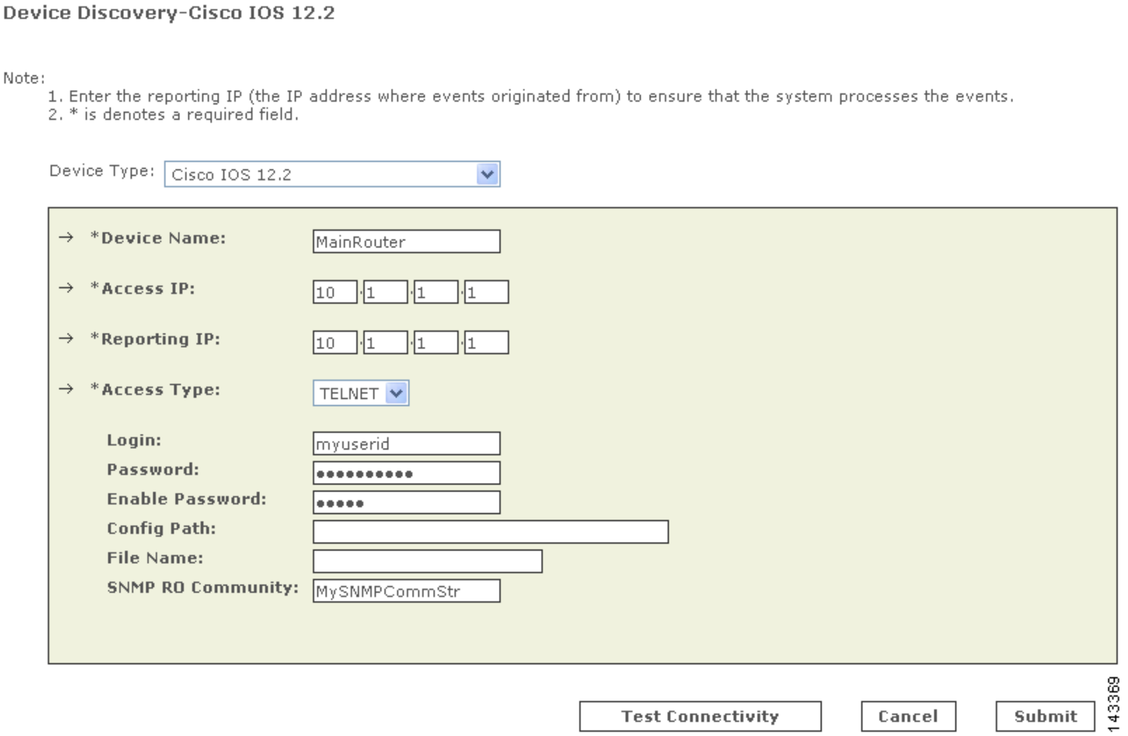
Step 5 Click the **Test Connectivity** button to have the MARS discover the device.

Step 6 Click the **Submit** button.

Add the Cisco 7500 Router with TELNET as the Access Type

Step 1 Click **Admin** > **Security and Monitor Devices** > **Add**.

Figure 20-17 Configure Cisco IOS 12.2



Device Discovery-Cisco IOS 12.2

Note:
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * is denotes a required field.

Device Type: Cisco IOS 12.2

→ *Device Name:	MainRouter
→ *Access IP:	10 . 1 . 1 . 1
→ *Reporting IP:	10 . 1 . 1 . 1
→ *Access Type:	TELNET
Login:	myuserid
Password:	••••••••••
Enable Password:	•••••
Config Path:	
File Name:	
SNMP RO Community:	MySNMPCommStr

Step 2 From the **Device Type** drop-down list, select **Cisco Switch-IOS 12.2**.

Step 3 Enter the **Device Name** of the switch.

Step 4 Enter the **Access IP** address (optional) and **Reporting IP** address of the switch. The **Reporting IP** address is usually the same as the **Access IP** address, but if you are creating an FTP device it must be a different IP address.

If you have entered an Access IP address, from the **Access Type** pull-down menu, select **FTP**:

FTP:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.
- For **Config Path**, enter the path of the configuration file on the FTP server.
- For **File Name**, enter the switch configuration file name on the FTP server.
- Enter its **SNMP RO Community**.

SNMP:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community**.

SSH:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community**.

TELNET:

- For the **Login** ID, enter the user name and **Password** needed to access the switch.
- For **Enable Password**, enter the password to get into Cisco enable mode.
- Enter its **SNMP RO Community** (mandatory).

Step 5 Click the **Test Connectivity** button to have the MARS discover the device.

Step 6 Click the **Submit** button.

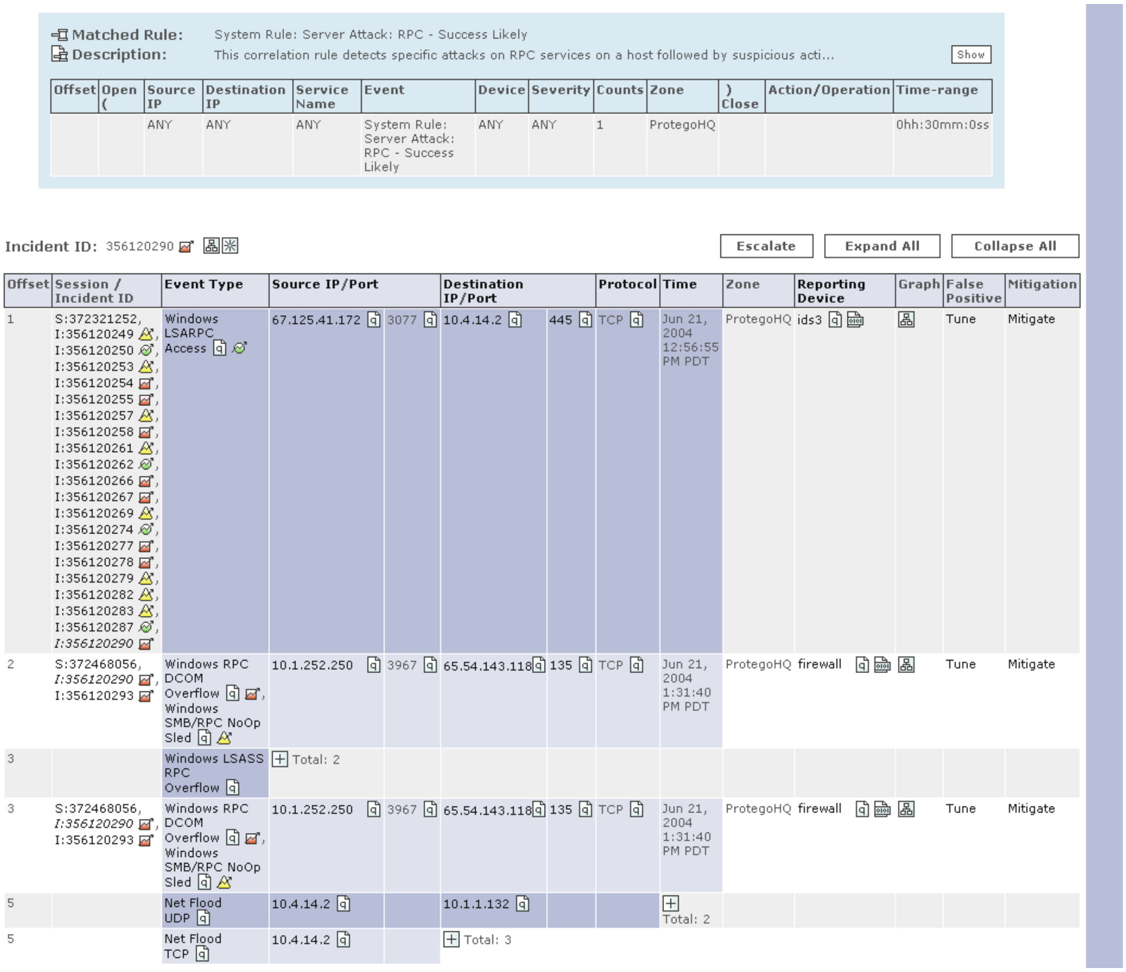
Verify the Connectivity Paths for Layer 3 and Layer 2

Once you have a session, you can view the Layer 3 and Layer 2 topology paths. There are several ways to obtain a session.

- **To view sessions that are part of an Incident:**

Step 1 Click the **Incidents** tab to navigate to the Incidents page. Click an **Incident ID** of an incident you want to view (in this example we use Incident number 356120290). The Incident Details screen appears.

Figure 20-18 Incident Details screen



Matched Rule: System Rule: Server Attack: RPC - Success Likely
Description: This correlation rule detects specific attacks on RPC services on a host followed by suspicious acti...

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
		ANY	ANY	ANY	System Rule: Server Attack: RPC - Success Likely	ANY	ANY	1	ProtegoHQ			0hh:30mm:0ss

Incident ID: 356120290

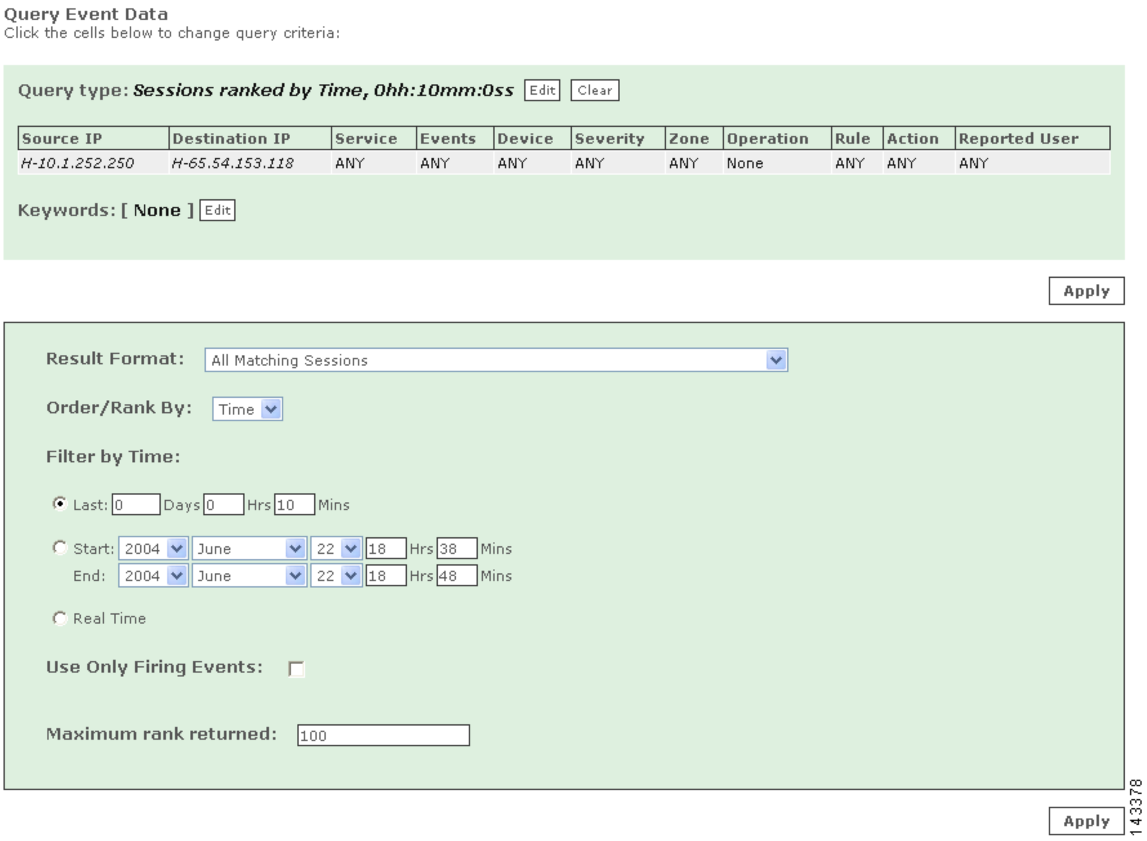
Offset	Session / Incident ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Device	Graph	False Positive	Mitigation
1	S:372321252, I:356120249, I:356120250, I:356120253, I:356120254, I:356120255, I:356120257, I:356120258, I:356120261, I:356120262, I:356120266, I:356120267, I:356120269, I:356120274, I:356120277, I:356120278, I:356120279, I:356120282, I:356120283, I:356120287, *I:356120290*	Windows LSARPC Access	67.125.41.172	3077	10.4.14.2	445	TCP	Jun 21, 2004 12:56:55 PM PDT	ProtegoHQ	ids3		Tune	Mitigate
2	S:372468056, *I:356120290*, I:356120293	Windows RPC DCOM Overflow, Windows SMB/RPC NoOp Sled	10.1.252.250	3967	65.54.143.118	135	TCP	Jun 21, 2004 1:31:40 PM PDT	ProtegoHQ	firewall		Tune	Mitigate
3		Windows LSASS RPC Overflow	Total: 2										
3	S:372468056, *I:356120290*, I:356120293	Windows RPC DCOM Overflow, Windows SMB/RPC NoOp Sled	10.1.252.250	3967	65.54.143.118	135	TCP	Jun 21, 2004 1:31:40 PM PDT	ProtegoHQ	firewall		Tune	Mitigate
5		Net Flood UDP	10.4.14.2		10.1.1.132			Total: 2					
5		Net Flood TCP	10.4.14.2		Total: 3								

Step 2 In the Incident Details screen, in the same row as the Event Type you want to examine (in this example we use Windows RPC DCOM Overflow), click the graph icon under the Graph column to view the topology paths.

- **To view sessions by performing a Query:**

Step 1 Click **QUERY / REPORTS** and submit a query using the appropriate query criteria. Note that in our example, we limit the scope of the query so it runs faster. In the following Query Event Data screen we use the result format **All Matching Sessions** and query events from **Source IP 10.1.252.250** and **Destination IP 65.54.153.118** over the last **10** minutes.

Figure 20-19 Query Event Data screen



Query Event Data
Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 0hh:10mm:0ss* Edit Clear

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
H-10.1.252.250	*H-65.54.153.118*	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	ANY

Keywords: [None] Edit

Result Format: All Matching Sessions

Order/Rank By: Time

Filter by Time:

● Last: 0 Days 0 Hrs 10 Mins

○ Start: 2004 June 22 18 Hrs 38 Mins
End: 2004 June 22 18 Hrs 48 Mins

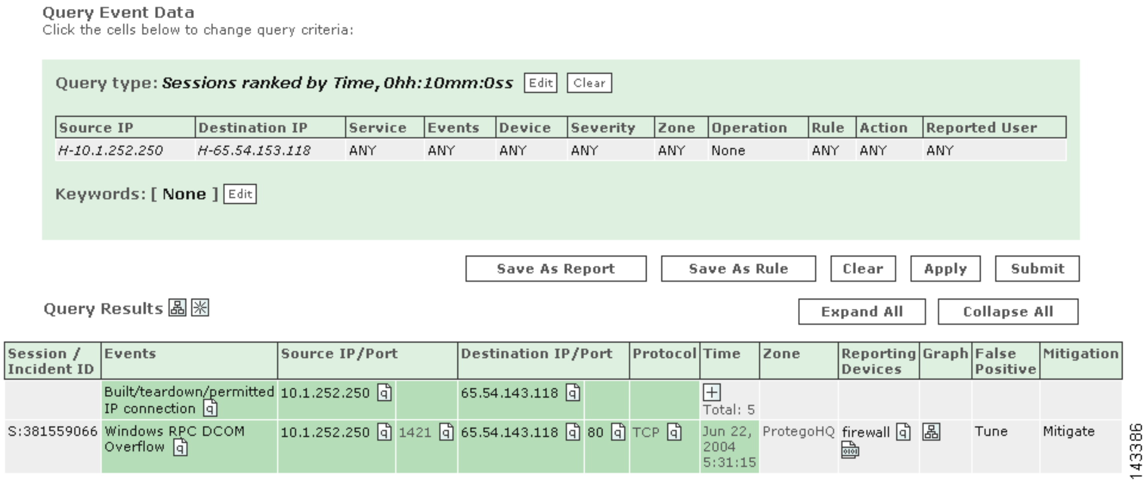
○ Real Time

Use Only Firing Events: □

Maximum rank returned: 100

Step 2 After you **Apply** changes to and **Submit** your query, the Query Results screen appears.

Figure 20-20 Query Results screen



Query Event Data
Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 0hh:10mm:0ss* Edit Clear

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
H-10.1.252.250	*H-65.54.153.118*	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	ANY

Keywords: [None] Edit

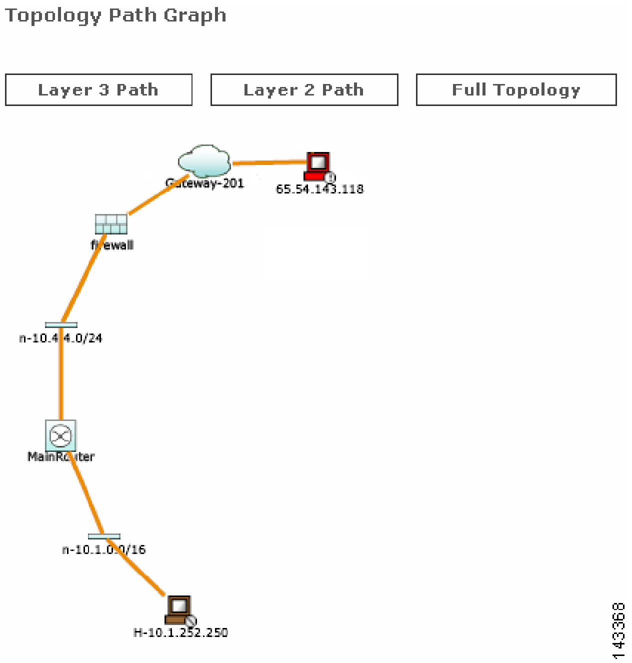
Query Results

Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
	Built/teardown/permitted IP connection	10.1.252.250	65.54.143.118		⊞ Total: 5					
S:381559066	Windows RPC DCOM Overflow	10.1.252.250 1421	65.54.143.118 80	TCP	Jun 22, 2004 5:31:15	ProtegoHQ	firewall		Tune	Mitigate

Step 3 In the Query Results screen, in the same row as the Event Type you want to examine (in this example we use Windows RPC DCOM Overflow), click the icon under the Graph column to view the topology paths.

The first topology path to appear is the Layer 3 topology graph:

Figure 20-21 Layer 3 topology graph

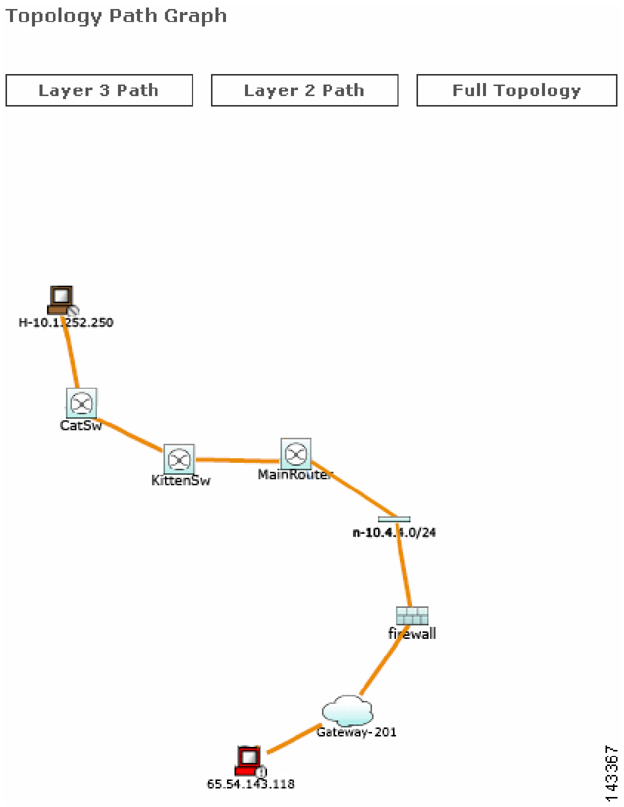


Topology Path Graph

Layer 3 Path | Layer 2 Path | Full Topology

Under **Topology Path Graph**, click the **Layer 2 Path** button to view the Layer 2 topology graph:

Figure 20-22 Layer 2 topology graph



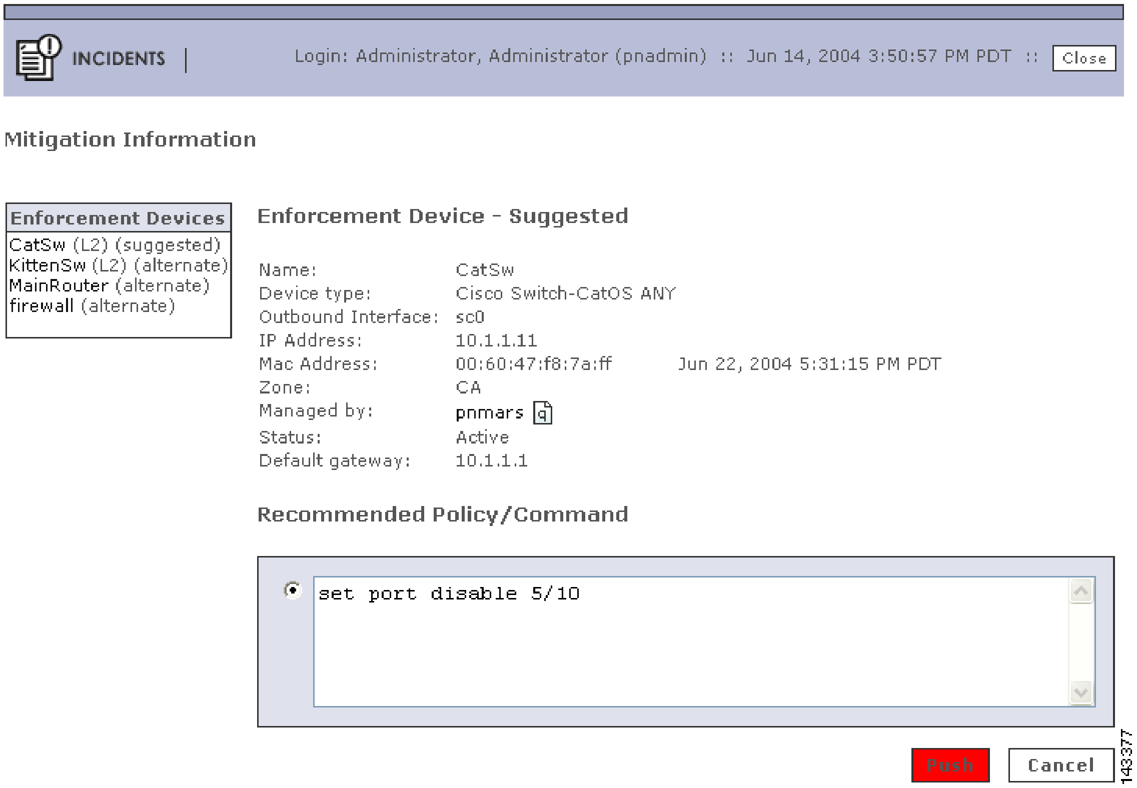
Perform Mitigation

Once you identify the compromised host (in this example, **10.1.252.250** connected to **CatSw**), it is critical to prevent it from attacking other hosts in the same subnet or other parts of the network. The MARS provides one-click mitigation that lets you isolate the compromised host from the rest of the network.

To perform mitigation, perform these steps:

Step 1 On the Incident Details screen, click the **Mitigate** link that corresponds with the **Session** or **Event Type** you want to mitigate (in this case, **Windows RPC DCOM Overflow**). The Mitigation Information screen appears.

Figure 20-23 Mitigation Information screen



Login: Administrator, Administrator (pnadmin) :: Jun 14, 2004 3:50:57 PM PDT ::

Mitigation Information

Enforcement Devices
CatSw (L2) (suggested)
KittenSw (L2) (alternate)
MainRouter (alternate)
firewall (alternate)

Enforcement Device - Suggested

Name:	CatSw	
Device type:	Cisco Switch-CatOS ANY	
Outbound Interface:	sc0	
IP Address:	10.1.1.11	
Mac Address:	00:60:47:f8:7a:ff	Jun 22, 2004 5:31:15 PM PDT
Zone:	CA	
Managed by:	pnmars	
Status:	Active	
Default gateway:	10.1.1.1	

Recommended Policy/Command

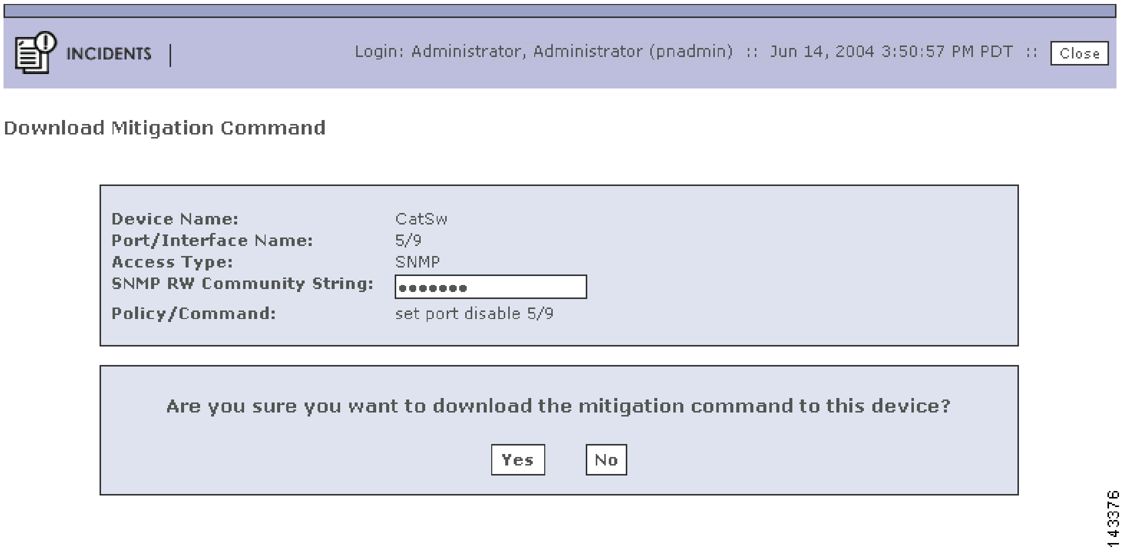
●
```
set port disable 5/10
```

This screen contains information about the device, along with recommended policies or commands for mitigating the compromised host (in the example, 10.1.252.250).

Step 2 If the device where the mitigation command to be downloaded is a Layer 2 device (such as in the example Mitigation Confirmation Dialog), a red **Push** button appears that you can click to mitigate the compromised host. If you select the push button, the Mitigation Confirmation Dialog appears.

Note If the device where the mitigation command to be downloaded is a Layer 3 device, the **Push** button shown in red on the Mitigation Information screen is greyed out and you must use the suggested commands directly on the device to mitigate the compromised host.

Figure 20-24 Mitigation Confirmation screen



Login: Administrator, Administrator (pnadmin) :: Jun 14, 2004 3:50:57 PM PDT ::

Download Mitigation Command

Device Name:	CatSw
Port/Interface Name:	5/9
Access Type:	SNMP
SNMP RW Community String:	●●●●●●●
Policy/Command:	set port disable 5/9

Are you sure you want to download the mitigation command to this device?

Note The SNMP RW community string must be enabled for the MARS to download a mitigation command to a device using the Access Type SNMP.

Step 3 Click **Yes** to confirm the mitigation of the device.