CHAPTER 22

Rules

This chapter discusses MARS Inspection and Drop rules in the following sections:

- Rules Overview, page 22-1
- Constructing a Rule, page 22-5
- Working with System and User Inspection Rules, page 22-17
- Working with Drop Rules, page 22-21
- Setting Alerts, page 22-23
- Rule and Report Groups, page 22-24

Rules Overview

An inspection rule is a real-time filter that detects interesting patterns of network activity. These patterns can signify attacks or false positives, and they inform you of network configuration errors and other anomalous network behavior. An attack might be straightforward, or it could be a probe, an attack, and then a follow-up to the attack. Whatever the method of attack, attacks share common traits, and you can use rules to define these traits to identify and mitigate attacks.

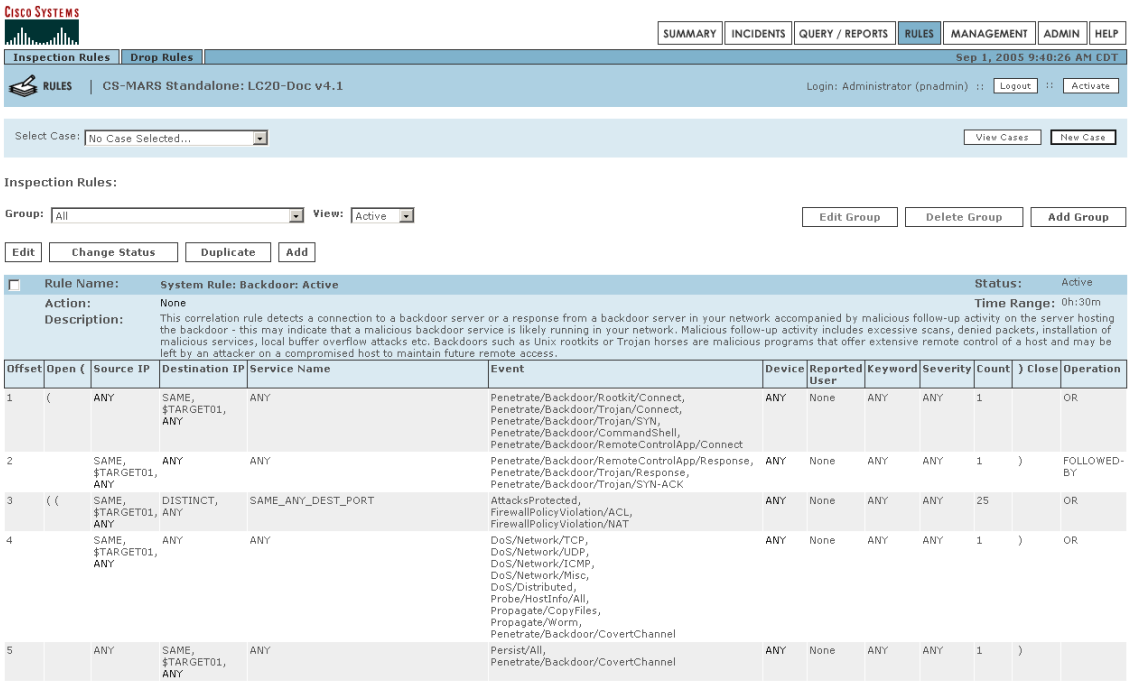
Rules create incidents. Rules connect the information you receive from your networks' reporting devices, linking them together to form a chain of events that describes an unfolding intrusion. They classify incoming events as firing events by matching them against the rule criteria. They also determine when a false positive is either dropped completely or kept as information in the database.

A rule is either active or inactive. Active means the rule is operating and is being applied to incoming events. Inactive indicates that the rule is inoperative and not consuming CS-MARS resources. To view a list of all System Inspection rules, see Appendix D, "System Rules and Reports."

Note A rule cannot be deleted, it can be made active or inactive.

Figure 22-1 shows a portion of the Inspection Rules page of the Rules tab.

Figure 22-1 Top Portion of Inspections Rules Page



Prioritizing and Identifying

Your first order of business is to prioritize your network's assets; in other words, figure out what is going to cost you the most money if it goes down. Next, identify your networks' most exploitable weaknesses. Choose which ones you are willing and able to close, and rank the remaining weaknesses by risk and exploitability.

Use this ranked list to guide your time and energy expenditures when customizing the CS-MARS rule set.

Think Like a Black Hat

Ignore for a moment the benign users who do legitimate business on your networks.

Get inside the mind of the black hat that wants to take your network down. The person who should concern you is the one with a plan.

Good plans have a sequence of steps, contingencies, and metrics to determine success or failure. The more fully you can anticipate these plans, the fewer attacks will be able to execute unhindered and unobserved. The black hat is looking for wide-open doors and easy access. Failing that, the black hat is going to look for specific and obvious exploitable weaknesses.

Planning an Attack

Start to detail your plan. You want to penetrate a network. You'd like to avoid detection and identification if possible. You want root access on a host.

How do you get root access? You do not have a preexisting account, and physical access isn't feasible. The first few options that come to mind are password guessing, password brute force, or exploiting a known weakness on the host.

You decide to exploit services running on the host, so you need to find out what it is running. To do this, you have a number of techniques: port scans, OS fingerprinting, banner probing, etc.

Once you've identified a vulnerable service or software, you can attack it with a catalogue of exploit software. Depending on what you find and your available exploits, there are a number of different effects, usually allowing you to execute arbitrary code.

You now own the host. What happens next is up to you. You have many options: you can install a root kit, you can crash the machine, etc. You have full access—you can do just about anything on to/from that host.

Back to Being the Admin

You must now express the plan in terms of information that is reported to you. This attack plan contains an attack with a follow up of some kind. You might write your plan like:

- probe
- attacker to target, buffer overflow
- attacker to target, root login (compromised host)

At this point, the black hat has compromised the host. What happens next is up to the attacker. This makes the next few steps especially hard to predict. They want to be able to manipulate the world, they want to make change. Your newly compromised host is the instrument for change. You can specify additional potential steps in the plan that make it even more urgent to take care of the situation immediately. Such as:

- target to FTP server, code download
- target to secondary target, buffer overflow

The attacker is now using your compromised host as a launching point for further attacks.

One you've mapped out the anticipated attack to watch for, you can define a monitoring plan. The following task flow outlines the tasks involved in implementing a monitoring plan:

Step 1 Ensure your reporting devices are providing all the data you need. This step involves ensuring that each device is generating logs about the events that you expect to occur as the result of the probes and attacks. Depending on the device type, this can involve several substeps, such as specify a logging level, enable logging for the specific event, and ensuring that the reporting device publishes events to the Local Controller appliance. It can also involve enabling administrative access to the reporting device from the Local Controller appliance.

Step 2 Configure CS-MARS to pull events from the reporting devices on your network. This step involves adding each reporting device to Local Controller. If the reporting device type is not directly supported, you must define a custom device type for the reporting device. To add a supported reporting device, see Adding Reporting and Mitigation Devices, page 2-17. To define a custom device type, see Adding User Defined Log Parser Templates, page 16-1 and Define a Custom Device/Application Type, page 16-2.

Step 3 Ensure that the event types that you need to study are accepted and processed by Local Controller. If they are not, you must define a custom log parser template for each event and a custom device template to which the custom log parser templates are associated. For device types supported by CS-MARS, this should not be necessary. To define a new parser template, see Adding User Defined Log Parser Templates, page 16-1 and Add Parser Log Templates for the Custom Device/Application, page 16-3.

Note You cannot define a custom log parser template for a reporting device that is supported out of the box. In this case, to define log parser for an unsupported event type, you must still define a custom device type before you can define the log parser.

Step 4 Check to see if a system rule will capture the information that you want, otherwise write your own user inspection rule. Define user inspection rules that monitor for the event types and correlate those events into a structure that will help you identify the incident. You can also specify who should be notified and how if the rule fires.

Types of Rules

Note A rule cannot be deleted, it can be made active or inactive.

Inspection Rules

An inspection rule states the logic by which the CS-MARS tests whether or not a single network event or series of events is a noteworthy incident. An event or series of events with attributes that match the attributes specified in an inspection rule causes the rule to trigger (or "fire") to create an incident. Incidents may be attacks, network configuration errors, false positives, or just anomalous network activity. The over 100 inspection rules that ship with MARS are called System Inspection Rules. The number and structure of system rules are updated in signature upgrades and with more recent software releases. Both types of upgrades are performed from the Admin > System Maintenance > Upgrade page.

You can create custom inspection rules by editing or duplicating system inspection rules, by adding your own from the Inspection Rules page, or by using the Query interface. Customized inspection rules are called User Inspection Rules and are displayed on the Inspection Rules page.

Inspection rules can be created on both the Global Controller and the Local Controllers.

Global User Inspection Rules

Global Inspection Rules are inspection rules you create on a Global Controller then push to the Local Controller. From the Local Controller, you can edit only the Source IP Address, Destination IP Address, and Action fields of a Global Inspection Rule. To change the arguments of the other fields, you must edit the rule on the Global Controller. When you edit a global inspection rule on the Local Controller then edit it again on the Global Controller, the Global Controller version overwrites the Local Controller version. Global Inspection rule names are displayed with the prefix "Global Rule."

Drop Rules

Drop rules allow false positive tuning on a MARS, and are defined only on the Local Controller Drop Rules page. They allow you to refine the inspected event stream by specifying events and streams to be ignored and whether those data should be stored in the database or discarded entirely. Drop rules are applied to events as they come in from a reporting device, after they have been parsed and before they have been sessionized. Events that match active drop rules are not used to construct incidents. Because the Global Controller does not receive events from reporting devices, rather it receives them from Local Controllers, you cannot define drop rules for the Global Controller.

Note For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

Constructing a Rule

Each step of your plan corresponds to a line of a rule. Each line identifies a set of conditions. A rule can have a single line, two lines, or multiple lines. You link these lines together using the logical operators, "AND, OR, FOLLOWED-BY (in time)."

For more information on the conditions and operators found in a rule, see Table 22-1 on page 22-6.

The first step of the example plan, identified in Back to Being the Admin, page 22-3, involved probing the target host. You can express a probe by selecting the appropriate event type groups as the line's event type criteria. Also, you want to use dollar variables ($TARGET)[1] to constrain your host to ensure that

For more information on the conditions and operators found in a rule, see Table 22-1.

The first step of the example plan, identified in the section Back to Being the Admin, page 22-3, involved probing the target host. You can express a probe by selecting the appropriate event type groups as the line's event type criteria. Also, you want to use dollar variables ($TARGET)[2] to constrain your host to ensure that the probe and attacks that are reported have happened to the same host. Then you need to figure out the logical step for the next line. In this case, the probe could be optional depending on the time frame that the probe was sent and its subtlety.

Rule logic is simple. You have a row. Every row has cells. 'The logical expressions connecting different cells are "and," while the expressions connecting items inside a cell are either "or" or "and not", depending which clause is chosen—the equal to or not equal to.

By studying the system inspection rules, you can identify three commonly used rules: attempts, success likely, and failures, The most common rule structure is the basic three-line rule that identifies an attempted attack. It is expressed as:

```
(Probe AND
Attack) OR
Attack)
```

Note To clarify this pseudocode, keep in mind that uppercase AND, OR and FOLLOWED-BY identify a logical operator between two rule lines. Lowercase "and" identifies a logical operator between two cells. Lowercase "or" and "and not" identify a logical operator between two items within a cell.

Success likely rules extend the attempt rules by identifying suspicious activities originating from the attacked host. The general structure of these rules is:

```
((Probe AND
Attack) OR
Attack)) FOLLOWED BY
```

1. A variable, such as ($TARGET), serves two purposes in the rule: 1.) It captures the number of times the same cell value is matched upon—the count for that cell, e.g., ten login failures from the same source address. 2.) It correlates the same value of a cell across rule lines, e.g., a probe from a source address AND an attack from that same source address.

2. A variable, such as ($TARGET), serves two purposes in the rule: 1.) It captures the number of times the same cell value is matched upon—the count for that cell, e.g., ten login failures from the same source address. 2.) It correlates the same value of a cell across rule lines, e.g., a probe from a source address AND an attack from that same source address.

```
(Suspicious Activity[1]..Suspicious Activity[n])
```

Failures identify an event from a reporting device that the device classifies as a failure. Often, these rules simply match to known syslog or SNMP messages indicating some failure on the device. You can define alerts to keep you abreast of device failures. These rules follow one of two general structures: a one line failure—

```
Failure
```

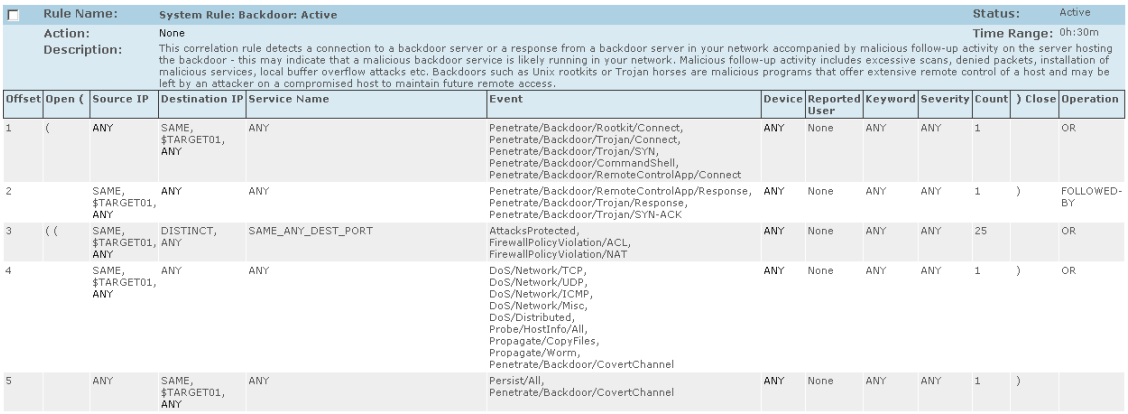
—or multi-line failures separated by the *OR* operator—

```
1..N Failure OR
```

Failure

In the HTML interface, system rules are displayed in rows and columns. The row number is called the Offset. A rule can have more than one row (or offset), as shown in Figure 22-2.

Figure 22-2 Rule with Multiple Offsets



Rule Name: System Rule: Backdoor: Active — Status: Active
Action: None — Time Range: 0h:30m
Description: This correlation rule detects a connection to a backdoor server or a response from a backdoor server in your network accompanied by malicious follow-up activity on the server hosting the backdoor - this may indicate that a malicious backdoor service is likely running in your network. Malicious follow-up activity includes excessive scans, denied packets, installation of malicious services, local buffer overflow attacks etc. Backdoors such as Unix rootkits or Trojan horses are malicious programs that offer extensive remote control of a host and may be left by an attacker on a compromised host to maintain future remote access.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1	(	ANY	SAME, $TARGET01, ANY	ANY	Penetrate/Backdoor/Rootkit/Connect, Penetrate/Backdoor/Trojan/Connect, Penetrate/Backdoor/Trojan/SYN, Penetrate/Backdoor/CommandShell, Penetrate/Backdoor/RemoteControlApp/Connect	ANY	None	ANY	ANY	1		OR
2		SAME, $TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/RemoteControlApp/Response, Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK	ANY	None	ANY	ANY	1	)	FOLLOWED-BY
3	((	SAME, $TARGET01, ANY	DISTINCT, ANY	SAME_ANY_DEST_PORT	AttacksProtected, FirewallPolicyViolation/ACL, FirewallPolicyViolation/NAT	ANY	None	ANY	ANY	25		OR
4		SAME, $TARGET01, ANY	ANY	ANY	DoS/Network/TCP, DoS/Network/UDP, DoS/Network/ICMP, DoS/Network/Misc, DoS/Distributed, Probe/HostInfo/All, Propagate/CopyFiles, Propagate/Worm, Penetrate/Backdoor/CovertChannel	ANY	None	ANY	ANY	1	)	OR
5		ANY	SAME, $TARGET01, ANY	ANY	Persist/All, Penetrate/Backdoor/CovertChannel	ANY	None	ANY	ANY	1	)	

143411

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Offset	The row number.	
Open (	Identifies the open of a clause. Clauses are used to compare one or more compound conditions in a rule.	Displays the open braces you create a clauses.

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Source IP	IP address of the packet originator.	
	Variables	*ANY*—(Default). Signifies that the IP address for each count is any IP address. *SAME*—Signifies that the IP address for each count is the same IP address. This variable is local to its offset. *DISTINCT*— Signifies that the IP address for each count is a unique IP address. This variable is local to its offset. *$Target01 to $Target20*—The same variable in another field or offset signifies that the IP address for each count is the same IP address.
	Network Groups	*Defined network groups*—Topologically valid network groups as defined under Management > IP Management.
	Networks	Topologically valid network groups as defined under Management > IP Management.
	Devices	The hosts and reporting devices present in the system.
	IP addresses	IP addresses present on devices in the system or user entered dotted quads.
	IP ranges	The range of addresses between two dotted quads.

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Destination IP	IP address of the packet destination. Often referred to as the target.	
	Variables	*ANY*—(Default). Signifies that the IP address for each count is any IP address. *SAME*—Signifies that the IP address for each count is the same IP address. This variable is local to its offset. *DISTINCT*—Signifies that the IP address for each count is a unique IP address. This variable is local to its offset. *$Target01 to $Target20*—The same variable in another field or offset signifies that the IP address for each count is the same IP address.
	Network Groups—	*Defined network groups*—Topologically valid network groups as defined under Management > IP Management.
	Networks—	Topologically valid network groups as defined under Management > IP Management.
	Devices—The hosts and reporting devices present in the system.	The hosts and reporting devices present in the system.
	IP addresses—	IP addresses present on devices in the system or user entered dotted quads.
	IP ranges—The range of addresses between two dotted quads.	The range of addresses between two dotted quads.
Service Name	A TCP/IP-based network service, identified by protocol and port, defined within the packet.	

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
	Variables	**ANY**—(Default) No constraint is placed on the source or destination ports or protocol or port. SAME type variables signify that the specified destination port, source port and protocol are the same for each count. These variables are local to the offset. • SAME_ANY_DEST_PORT SAME_TCP_DEST_PORT SAME_UDP_DEST_PORT • SAME_ANY_SRC_PORT SAME_TCP_SRC_PORT SAME_UDP_SRC_PORT DISTINCT type variables signify that the specified destination port, source port and protocol are unique for each count. These variables are local to the offset. • DISTINCT_ANY_DEST_PORT DISTINCT_TCP_DEST_PORT DISTINCT_UDP_DEST_PORT Identical variables in different fields or offsets signify that the specified port and protocol for each count are identical to each other. • $ANY_BOTH_PORT5 • $ANY_DEST_PORT1 to ANY_DEST_PORT5 • $ANY_SRC_PORT1 • $TCP_BOTH_PORT1, $TCP_BOTH_PORT2 • $TCP_DEST_PORT1 to $TCP_DEST_PORT5 • $TCP_SRC_PORT1, $TCP_SRC_PORT2 • $UDP_BOTH_PORT1, $UDP_BOTH_PORT2 • $UDP_DEST_PORT1 to $UDP_DEST_PORT5 • $UDP_SRC_PORT1, $UDP_SRC_PORT2

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
	Defined services—One or more services defined under Management > Service Management.	
	Service groups—One or more service groups defined under Management > Service Management.	• Backdoor • Instant Messaging • Mail Retrieval • Online Game • P2P • Recent Backdoor • TCP-highport • UDP-highport • vulnerable-protocols
Event	Identifies one or more event types. An event type indicates some type of network activity or condition. Sometimes, events reported from different devices and different device types identify the same activity or condition, and therefore, they map to the same event type within MARS. Event types are sorted into event groups, such as "Probe/PortSweep/Stealth", to catch any of the network conditions identified by the group.	
	Variables—Signify any single event type defined under Management > Event Management, only useful for lines in tandem with the same variable.	• **ANY**—Any of the active event types can match this rule. • SAME • DISTINCT • $EVENT_TYPE01, $EVENT_TYPE10
	Event types—Events that have been merged into types.	• ANY • SAME • DISTINCT • All events
	Event type groups—Groups of event types.	• ANY • SAME • DISTINCT
	Red Severity Event Types—Displays all severe event types	
	Yellow Severity Event Types—Displays all yellow event types	

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
	Green Severity Event Types—Displays all green event types	
Device	The value of this condition can be one of the following:	
	Variables—Signify any single device defined under Admin > System Management > Security and Monitor Devices, only useful for lines in tandem with the same variable.	• **ANY**—(Default) Specifies that this rule is applied to events generated by any of the reporting devices defined in MARS. • SAME • DISTINCT • **Unknown Reporting Device**—Specifies that this rule is applied to events generated by any reporting device that is not defined in MARS. • $DEVICE01 to $DEVICE10
	• **Reporting Devices**—Identifies one or more hosts or reporting devices for which events are inspected. Valid values are one or more devices as defined under Admin > System Setup > Security and Monitor Devices.	
	Defined Device Types—	
Reported User	Identifies the active user on the host when this event was recorded. Not all events include this data. The value of this condition can be one of the following:	• **ANY**—No constraint is placed on the reported user. • **NONE**—(Default) Specifies that this condition should not be used to match this rule. • **Variables**—Signify any single user, only useful for lines in tandem with the same variable. • **Invalid User Name**—Specifies that this condition is met when the user name reported is invalid.

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Severity	The value of this condition can be one of the following:	• **ANY**—(Default) Specifies that this rule is applied to events of all severity levels. • **Green**—Restricts this rule to firing against low-severity events. • **Yellow**—Restricts this rule to firing against medium-severity events. • **Red**—Restricts this rule to firing against high-severity events.
Count	Identifies the number of items the event must occur before the condition is met. The value for this condition is a whole number ranging between 1 and 100. The default value is 1. **Note** Events of the same event type occurring in the same session in a three-second period increment the active count by one. This inherent threshold ensures that a event floods of the same type does not increase the active count arbitrarily and incorrectly fire the rule.	*Example usage*: When a backdoor rootkit install is detected, the count should be 1 as it is only going to be reported once and it is not something you expect to ever see on your network. However, if you are using deny messages to detect infected hosts, you may want the count value to be higher. For example, you may want to allow for several common mistakes, such as password failures, before firing a rule for the event. People accidentally mistype passwords, they don't accidentally install a rootkit.
Close	Identifies the close of a clause.	

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Operation	The value of this field can be one of the following:	• **None**—(Default) Defines a single-line rule or a simple condition. • **AND**—A boolean "and" used to construct a compound condition (two or more lines). This line and the next line must both be satisfied before the compound condition is met. • **OR**—A boolean "or" used to construct a compound condition (two or more lines). Either this line or the next line can be satisfied to meet the compound condition. • **FOLLOWED-BY**—Identifies a compound condition (two or more lines). specifically a sequential order of occurrence. Also referred to as a time conditional rule (e.g., Y must happen after X).The condition of this line must be met, and then the condition of the next line must be met before the compound condition is met.

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Time Range	Identifies the period of time over which the count value is augmented. For rules that have a Count value greater than one, the Time Range value determines how long the period should be before the count value is reset. For example, you can assume that if no more than three login attempts have occurred over a 10-minute period that counter can be reset.	Usage Guideline: The Time Range value combined with the Count value can affect the operation of your MARS. Each time an event is captured that satisfied a unique instance of an inspection rule, a monitoring session is constructed to track possible future occurrences until either the Count value is reached or the time period expires.

Table 22-1 Rule Fields and Arguments

Rule Field	Field Description and Arguments	Argument Descriptions
Action	Identifies the action that MARS will take when the rule is fired. Actions are user-defined alerts that include an action name and description, which also doubles at the message text provided in the alert. Each action can combine alert techniques, such as email and syslog. Each alert technique can have multiple values. For example, an action can generate two emails, a page, and a SNMP trap. Each rule can have multiple such actions. Alerts can be constructed using one or more of the following techniques: **Note** You will see the column Action/Operation. In this case, you can select either one of the following actions or one of the operators.	• **NONE**—(Default) This action states that no further action will be taken. When NONE value is selected, the firing of the rule causes an event record to be created and stored in MARS. Regardless of the selected action, this record is always created. • **Email**—Identifies the list of administrators to whom an alert should be sent. An e-mail address must be defined for the selected administrators. • **Syslog**—Identifies the list of hosts to whom an alert should be sent. You can select any number of devices to which you want a syslog message sent. • **Page**—Identifies the list of administrators to whom an alert should be sent. The message format is text. A pager number must be defined for the selected administrators. • **SNMP**—Lists the hosts to which a Simple Network Management Protocol (SNMP) alert can be sent. • **SMS**—List of users to receive notification by Short Message Service (SMS). The message can be up to 160 characters. An SMS number must be ten numbers and a domain name, for example, 1234567890@provider.com. • **Distributed Threat Mitigation (DTM)**—Not supported at this time. Lists the Cisco IOS Intrusion Prevention System (IPS) devices to which an IPS alert action can be sent (alarm, alarm and drop, or alarm and reset if it is a TCP session.)

Working Examples

The examples in this section demonstrate the use of variables, in particular, how to use variables to detect Deny patterns.

Note We recommend that you study the system inspection rules for more complex examples. To view a list of system rule names and descriptions, see Appendix D, "System Rules and Reports."

Note For a single offset rule, the variables SAME and SAME_ANY_DEST_PORT can be substituted in any of the examples for $TARGET01 and $ANY_DEST_PORT1, respectively. The "ANY" in $ANY_DEST_PORT1 means either UDP or TCP protocol.

Example A: Excessive Denies to a Particular Port on the Same Host

Figure 22-3 Rule for Excessive Denies to a Particular Port on the Same Host

Rule Name:	Example A							Status:	Active
Action:								Time Range:	0hh:0mm:10ss
Description:	Excessive denies to a particular port on the same host.								
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Operation
1		ANY	$TARGET01	$ANY_DEST_PORT1	FirewallPolicyViolation/ACL	ANY	ANY	100	Training		

143408

In this example, the rule fires when 100 of the specified events occur from any source IP address to the same destination IP address, and the destination port numbers are identical.

Example B: Same Source Causing Excessive Denies on a Particular Port

Figure 22-4 Rule for Same Source Doing Excessive Denies on a Particular Port

Rule Name:	Example B							Status:	Active
Action:								Time Range:	0hh:0mm:10ss
Description:	Same source doing excessive denies on a particular port.								
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Operation
1		$TARGET01	ANY	$ANY_DEST_PORT1	FirewallPolicyViolation/ACL	ANY	ANY	100	Training		

143409

In this example, the rule fires when 100 of the specified events occur that have the source IP address, any Destination IP address, and identical destination port numbers.

Example C: Same Host, Same Destination, Same Port Denied

Figure 22-5 Rule for Same Host, Destination, Same Port Denied

Rule Name:	Example C							Status:	Active
Action:								Time Range:	0hh:0mm:10ss
Description:	Same host, destination, same port getting denied.								
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Operation
1		$TARGET01	$TARGET02	$ANY_DEST_PORT1	FirewallPolicyViolation/ACL	ANY	ANY	20	Training		

143410

In this example, the rule fires when 20 of the specified events occur that have the same source and destination addresses, and identical destination port numbers.

Working with System and User Inspection Rules

Navigate to the **Inspection Rules** page by clicking the **Rules** tab.

You can perform the following actions with Inspection Rules:

- Change the Source IP, Destination IP and Device fields of a System Inspection rule
- Duplicate any Inspection Rule then edit the fields to make a new User Inspection Rule
- Build a new User Inspection Rule with the Rule wizard
- Edit any field of a User Inspection Rule
- Make any rule active or inactive
- Edit, delete, or add, a Rule Group

Note When you add or edit a rule, you must click **Activate** to enable the changes.

Note Upgrade the MARS software regularly to obtain new and updated System Inspection rules. For more information, see the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*. To view a list of System Inspection rules, see Appendix D, "System Rules and Reports."

Change Rule Status—Active and Inactive

The CS-MARS correlation engine continuously tests only active rule criteria against incoming events to identify incidents. Inactive rules do not consume resources used for realtime operations.

Note A rule cannot be deleted, it can be made active or inactive.

To change the status of a rule, follow these steps:

Step 1 Navigate to the **Rules** > **Inspection Rules** page.

Step 2 Select the checkbox of the rule (or rules) to change.

Step 3 Click **Change Status**.
The selected rules are made inactive if active, and active if inactive and displayed on a different page.

Step 4 To display inactive rules, select **Inactive** from the View dropdown list. To display active rules, select **Active**.

Duplicate a Rule

Duplicating a rule creates a new rule that is a copy of an existing system or user inspection rule. You can edit all of the fields of a duplicate rule, but only the Source IP, Destination IP, and Device fields of a system inspection rule. The original rule is left unchanged after duplication.

Note You cannot delete a rule after it is created by **Duplicate** or **Add**.

To duplicate a rule, follow these steps:

Step 1 Select the checkbox of the rule to duplicate.

Step 2 Click **Duplicate**.
The name of duplicated rule is the name of the original rule extended with a timestamp of when the original was duplicated (for example, System Rule: Client Exploit - Sasser Worm Copied: 05.10.05/16:54:21). The name can be changed by editing the duplicate rule.

Edit a Rule

You can edit rules with inline editing, or with the rule wizard. To edit inline, you click the argument to edit. The rule wizard is invoked by selecting a rule to edit then clicking **Edit**. The rule wizard begins with the Rule Name field and progress through each subsequent field.

Note You only edit the Source IP, Destination IP, and Device fields of a system inspection rule. See Duplicate a Rule, page 22-17 for further information on modifying system inspection rules.

Note A rule cannot be deleted, it can be made active or inactive.

Edit a Rule with Inline Editing

You can perform inline editing to rules from the Incidents Detail page, or from the Inspections Rules page. To edit a rule with the Inline Editing, follow these steps:

Step 1 Click the Rule argument that you want to edit.
The edit page for the selected field appears.

Step 2 Change the argument, then click **Apply**.

Step 3 Repeat Step 1 as required.

Step 4 Add Open and Close parentheses as required then click **Submit**.
If no parentheses are required, just click **Submit**.

Step 5 Click **Activate** to include the rule in event correlation processing.

Edit a Rule with the Rule Wizard

The Rule Wizard can only be invoked from the Inspections Rule page.

To edit a rule with the Rule Wizard, follow these steps:

Step 1 Select the check box of the rule to edit.

Step 2 Click **Edit**.
The rule wizard page appears for the Rule Name field.

Step 3 Do one of the following actions:

- Change the argument of the field, then click **Apply**. Proceed to Step 6.
- Change the argument, then click **Next** to proceed to the next field.
- Click **Next** to proceed to the next field without changing the argument.
- Click **Previous** to go back to the previous field.
  Previous does not appear for the Rule Name page.

Step 4 Repeat • as required.

Step 5 Click **Apply** after making all edits.

Tip To skip to the end, click the Count argument, after which, only the **Action**, and **Time Range** fields must be reviewed.

Step 6 Add Open and Close parentheses as required then click **Submit**.
If no parentheses are required, just click **Submit**.

Step 7 Click **Activate** to include the rule in event correlation processing.

Add an Inspection Rule

Note Rules that you add are called User Inspection Rules.

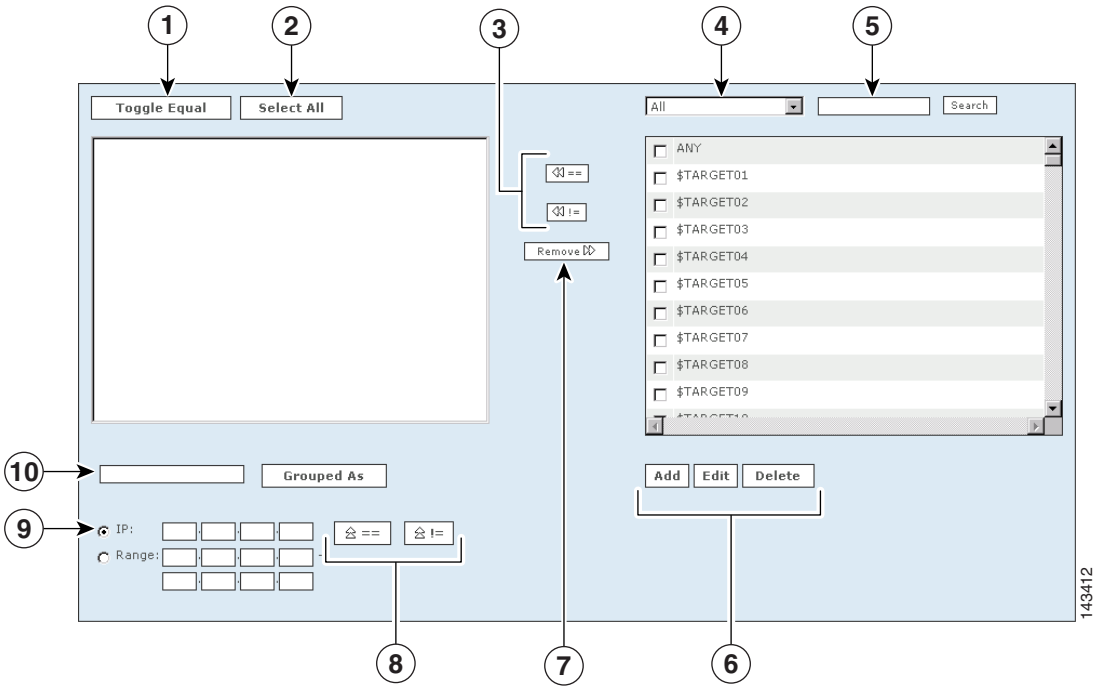
Step 1 Navigate to the Inspection Rules page.

Step 2 Click **Add**.

Step 3 Enter a name and description for the rule, then click **Next**.

Step 4 Select Source IP address.

Figure 22-6 User Inspection Rule Wizard Form



The following numbers correspond to the numbers shown in Figure 22-6.

1. Check the boxes next to the items in the **Sources Selected** field to select them, and click the **Toggle Equal** button to change them between equal and not equal.
2. Click the **Select All** button to select all items in the **Sources Selected** field. Items selected in the Sources Selected field are deselected when you click **Select All**.
3. Use the **Equal** and **Not Equal** buttons to bring highlighted items from the **Sources Available** field into the **Sources Selected** field.
4. Filter sources from this drop-down list.
5. Enter search text, and click **Enter** to move items that match the search criteria from the **Sources Available** field to the **Sources Selected** field.
6. To add a new item to the sources, click the **Add** button. To edit or delete an existing source, click the **Edit** or **Delete** button.
7. Click an item or items in the Sources Selected field, and use the **Remove** button.
8. To move IP values up into the Sources Selected field, click the **Equal** up icon, or the **Not Equal** up icon.
9. Check the radio button next to **IP** or **Range**, and enter an IP address or a range of IP addresses into their respective fields.
10. Select items in the Sources Selected field by clicking them. Enter a group name, and click the **Grouped As** button to group them.

Step 5 Follow the wizard, and select the values for the rule, clicking the **Next** button to progress to the next step.

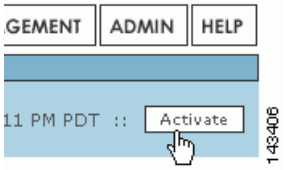
Step 6 When you are asked, "Are you done defining the rule conditions," you can:

- Click the **Yes** button for a single line rule. Continue to add repetition requirements (counts), alert information, and valid time ranges for each line.

- Click the **No** button, to create a multi-line rule that uses an operator (OR, AND, or FOLLOWED BY). Return to Step 4 and continue to make your selections. Continue to add rule information, and click **Submit** when finished.
- Click the **Submit** button when finished.

Step 7 When the rule is complete, you need to activate it by clicking the **Activate** button.

Figure 22-7 Clicking the Activate button



Note If you are creating or editing several rules, it is better for the system to click the **Activate** button for several changes rather than for each individual change.

Working with Drop Rules

Navigate to the Drop Rules page by clicking the **Rules > Drop Rules** tabs.

Drop rules instruct the MARS to either drop a false positive completely from the appliance, or to keep it in the database. On the Drop Rules page, you add, edit, duplicate, activate an inactive rule, or inactivate an active rule. Inactive rules do not fire.

Note For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

While working with drop rules is similar to working with inspection rules, it is not identical.

Change Drop Rule Status— Active and Inactive

Step 1 Check the box next to the rule.

Step 2 Click **Change Status**.

When you change the status to inactive, the rule displays only on the inactive rules page.

Step 3 To display inactive Drop Rules, select **Inactive** from the **View** dropdown list.

Duplicate a Drop Rule

Step 1 Check the box next to the rule.

Step 2 Click the **Duplicate**.

After duplicating a rule, you can edit the duplicate without altering the original.

Edit a Drop Rule

Step 1 Check the box next to the rule.

Step 2 Click **Edit** on the field that you want to change.

Step 3 Follow the rule's wizard and complete any other changes to the rule.

Step 4 Click **Submit**.

Note When the rule or rules are complete, click **Activate**.

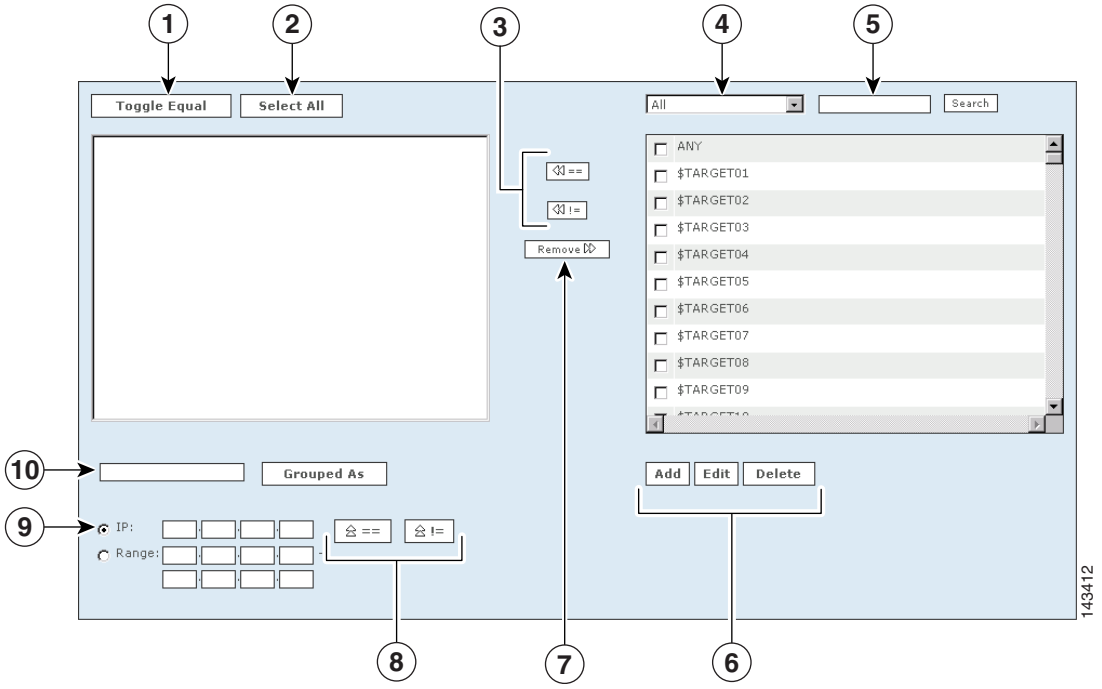
Add a Drop Rule

Step 1 Click **Add**.

Step 2 Enter a name and description for the rule, and click **Next**.

Step 3 Select your sources.

Figure 22-8 Drop Rule Creation Form



The following numbers correspond to the numbers in the Drop Rule Creation Form as shown in Figure 22-8:

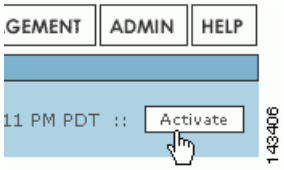
1. Check the boxes next to the items in the **Sources Selected** field to select them, and click the **Toggle Equal** button to change them between equal and not equal.
2. Click the **Select All** button to select all items in the **Sources Selected** field. (Note: if you have items highlighted in the Sources Selected field, clicking **Select All** will de-select them.)
3. Use the **Equal** and **Not Equal** buttons to bring highlighted items from the **Sources Available** field into the **Sources Selected** field.
4. Filter sources from this drop-down list.
5. Enter search text, and click **Enter** to move items that match the search criteria from the **Sources Available** field to the **Sources Selected** field.
6. To add a new item to the sources, click the **Add** button. To edit or delete an existing source, click the **Edit** or **Delete** button. See IP Management, page 24-3 for more information.
7. Click an item or items in the Sources Selected field, and use the **Remove** button.
8. To move IP values up into the Sources Selected field, click the **Equal** (Up) icon, or the **Not Equal** (Up) icon.
9. Check the radio button next to **IP** or **Range**, and enter an IP address or a range of IP addresses into their respective fields.
10. Select items in the Sources Selected field by clicking them. Enter a group name, and click the **Grouped As** button to group them.

Step 4 Follow the wizard, and select the values for the rule, clicking the **Next** button to progress to the next step.

Step 5 When you are asked, "Are you done defining the rule conditions," click the **Submit** button.

Step 6 When the rule is complete, you need to activate it by clicking the **Activate** button.

Figure 22-9 Clicking the Activate button



Note If you are creating or editing several rules, it is better for the system to click the **Activate** button for several changes rather than for each individual change.

Setting Alerts

You have two options for learning about rules that have fired: you can log in and view the appropriate pages in the HTML interface or you can have MARS send alerts to external devices and users. Actions provide instructions to MARS on the second method.

Using Rules, you can alert a person if a rule has fired. The roles and groups you can choose are determined by the information you have entered in User Management. for more information on adding users into the Local Controller.

Configure an Alert for an Existing Rule

Step 1 Click on a rule argument.

Step 2 Click **Next** until the Action/Operation column is selected.

Step 3 Click the **Add** button to add users for an alert.

Step 4 Enter a **Name** and **Description** for the notification.

Step 5 Check the box next to the type of notification that you want to send. Your choices are:

- **Email** – select the roles or groups that you want to receive an email.
- **Syslog** – select the systems that you want to receive the syslogs.
- **Page** – select the roles or groups that you want to receive an electronic page on their pagers or cellular telephones.
- **SNMP** – select the systems that you want to receive the SNMP trap information.

Note For SNMP and Syslog, you need to configure the receiving systems for this feature to work.

Step 6 Click the **Change Recipient** button to add or edit recipients for alerts for that notification type (email, syslog, page, or SNMP).

Step 7 Check the box next to the role, group, or system that you want to receive alerts.

- Click the **Add** button to select recipients (to move them into the left field.)
- To remove recipients, click their names to highlight them (in the left field) and click the **Remove** button.

Step 8 Repeat steps 5 - 7 for all the alert selections that you want to include.

Step 9 Click the **Submit** button.

Step 10 Click the **Apply** button.

Note If a user adds an alert to a rule created on the Global Controller, and the rule is pushed down and fired on the Local Controller, the designated user receives the alert from the Local Controller and not the Global Controller

Rule and Report Groups

This section contains the following subsections:

- Rule and Report Group Overview, page 22-25
- Global Controller and Local Controller Restrictions for Rule and Report Groups, page 22-26

- Add, Modify, and Delete a Rule Group, page 22-27
- Add, Modify, and Delete a Report Group, page 22-29
- Display Incidents Related to a Rule Group, page 22-31
- Create Query Criteria with Report Groups, page 22-31
- Using Rule Groups in Query Criteria, page 22-32

Rule and Report Group Overview

Note To view a list of all System Inspection rules and reports, see Appendix D, "System Rules and Reports."

Rule and report groups help you manage rules and reports by speeding access to those rules and reports relevant to your task at hand. You can create groups, or use the groups provided with CS-MARS (System groups). Groups act as filters to limit the display of rules, reports, and incidents in the CS-MARS HTML interface. All groups can be modified or deleted.

CS-MARS provides over 100 system rules and 150 system reports. More can be added by creating custom rules and reports, and by performing periodic software updates. A rule or report group contains a subset of these rules or reports as members. Usually rules or reports within the same group have related functions (such as, reconnaissance activities, server attack, etc.). When you select a group from a dropdown filter, only those rules and reports that are members are displayed on the page. When you select a rule group on the Incidents page, only those incidents related to the rules of the selected group display. Report and rule groups can also be used when constructing queries.

For instance, there are at least 16 system rules that detect suspicious network access events and incidents, and 15 system reports to report this information. CS-MARS provides a system rule group and a system report group named "Access" that can filter the Inspection Rules, Incidents, and Report pages to display only those rules and reports related to monitoring access event (such as password attacks), thereby eliminating the need to search for the pertinent rules and reports within the complete rule and report pages or dropdown lists. CS-MARS provides system rule and report groups as listed in Table 22-2.

Table 22-2 Predefined Rule and Report Groups

System Report Groups	Corresponding System Rule Groups
System: Access	System: Access
System: All Events - Aggregate View	—
System: All Exploits - Aggregate View	—
System: COBIT DS3.3 - Monitoring and Reporting	—
System: COBIT DS5.10: Security Violations	—
System: COBIT DS5.19: Malicious software	—
System: COBIT DS5.20: Firewall control	—
System: COBIT DS5.2: Authentication and Access	—
System: COBIT DS5.4: User Account Changes	—
System: COBIT DS5.7: Security Surveillance	—

Table 22-2 Predefined Rule and Report Groups (continued)

System Report Groups	Corresponding System Rule Groups
System: COBIT DS9.4: Configuration Control	—
System: COBIT DS9.5: Unauthorized Software	—
System: CS-MARS Distributed Threat Mitigation (Cisco DTM)	System: CS-MARS Distributed Threat Mitigation (Cisco DTM)
System: CS-MARS Incident Response	System: CS-MARS Incident Response
System: CS-MARS Issue	
System: Client Exploits, Virus, Worm and Malware	System: Client Exploits, Virus, Worm and Malware
System: Configuration Changes	—
System: Configuration Issue	System: Configuration Issue
System: Database Server Activity	System: Database Server Activity
System: Host Activity	System: Host Activity
System: Network Attacks and DoS	System: Network Attacks and DoS
System: New Malware Outbreak (Cisco ICS)	System: New Malware Outbreak (Cisco ICS)
System: Operational Issue	System: Operational Issue
System: Reconnaissance	System: Reconnaissance
System: Resource Issue	System: Resource Issue
System: Resource Usage	—
System: Restricted Network Traffic	System: Restricted Network Traffic
System: SOX 302(a)(4)(A)	—
System: SOX 302(a)(4)(D)	—
System: Security Posture Compliance (Cisco NAC)	System: Security Posture Compliance (Cisco NAC)
System: Server Exploits	System: Server Exploits

Global Controller and Local Controller Restrictions for Rule and Report Groups

Global Controller and Local Controller rule and report groups have the following restrictions:

- Rule and report groups created on the Global Controller are pushed to all the Local Controllers.
- Rule groups created on a Local Controller are local to the Local Controller. They are not copied to the Global Controller or to other Local Controllers.
- Local Controller account holders can edit only the Source IP, Destination IP, and Device fields of a rule group created on a Global Controller.
- Local Controller account holders cannot edit Global Controller report groups.
- Local Controller account holders cannot delete Global Controller rule and report groups.

Note The procedures described in this section are valid for both the Local and Global Controllers, except that the Case Bar does not appear on the Global Controller HTML interface.

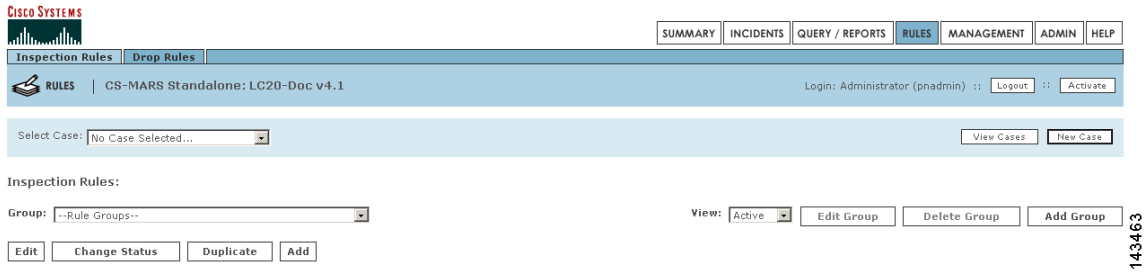
Add, Modify, and Delete a Rule Group

Adding a New Rule Group

To add a rule group follow these steps:

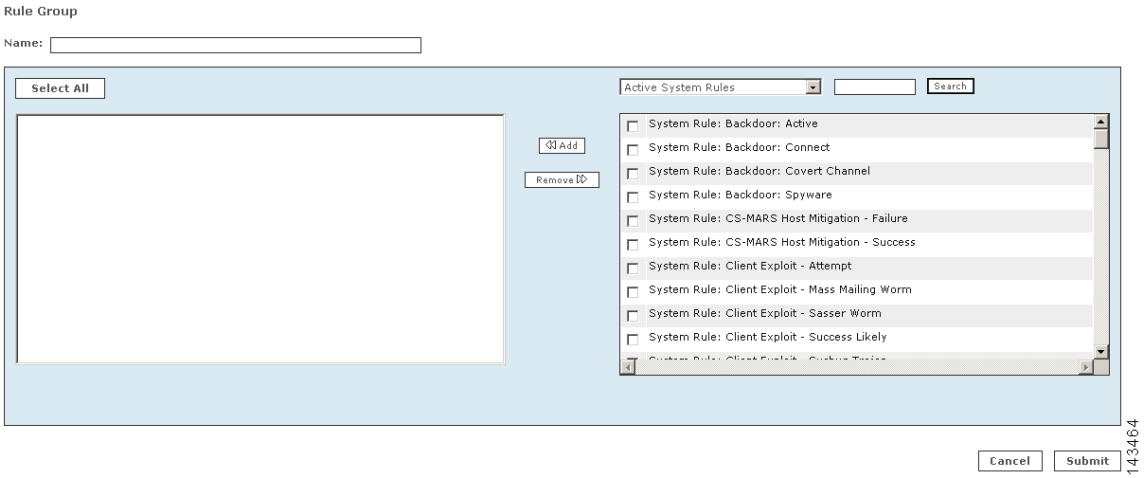
Step 1 Navigate to the Inspection Rules page, as shown in Figure 22-10.

Figure 22-10 Inspection Rules Page



Step 2 Click **Add Group**.
The Add Group dialog box appears, as shown in Figure 22-11.

Figure 22-11 Add Group Dialog Box



Step 3 Enter the new group name in the **Name** field.

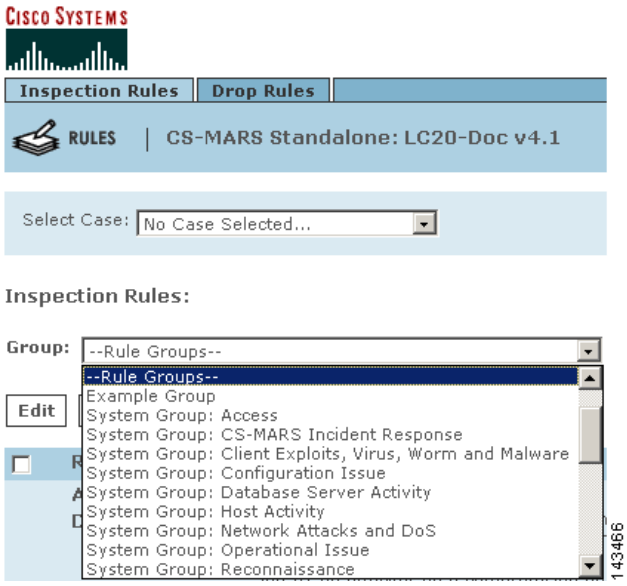
Step 4 Click the checkboxes of the rules to be added to the new rule group.

Tip The dropdown list above the list of rules can limit the display of rules to active system rules, active user rules, or inactive rules. The search function displays only those rules that match a search string (for example, “New Malware Traffic Match.”). The asterisk wildcard character (*) is supported.

Step 5 Click **Add.**
The selected rules appear in the lefthand pane of the dialog box. To remove a rule from the group, highlight the item in the lefthand pane and click **Remove**.

Step 6 Click **Submit.**
The new rule group name appears in the **Group** dropdown filter on the Inspection Rules page, as shown in Figure 22-12. In this example, the new rule group name is "Example Group." Because it is a user-created rule group, the rule group name appears without the prefix "System." You can also click **Cancel** to return to the Inspection Rules page without creating a new rule group.

Figure 22-12 New Rule Group Appears on the Dropdown List of the Inspections Rules Page



Modifying a Rule Group

To edit a rule group, follow these steps:

Step 1 Navigate to the Inspection Rules page, as shown in Figure 22-10.

Step 2 Select the rule group to edit in the **Group** pulldown filter.

Step 3 Click **Edit Group**.
The Add Group dialog box appears, as shown in Figure 22-11. The rule group name appears in the **Name** field, and the included rules appear as selected rules in the lefthand pane of the dialog box.

Step 4 To add additional rules, click the checkbox of all the rules to be added to the group, then click **Add**. To remove rules, highlight the items in the lefthand pane to remove, then click **Remove**.

Step 5 Click **Submit.**

Deleting a Rule Group

Step 1 Navigate to the Inspection Rules page, as shown in Figure 22-10.

Step 2 Select the rule group to delete in the **Group** pulldown filter.

Step 3 Click **Delete Group**.
The Delete Group dialog box appears listing the rules in the group to be deleted. You are prompted to confirm deletion.

Step 4 Click **Yes.**
The rule group no longer appears in the **Group** dropdown filters on the Incident and Inspection Rules pages.

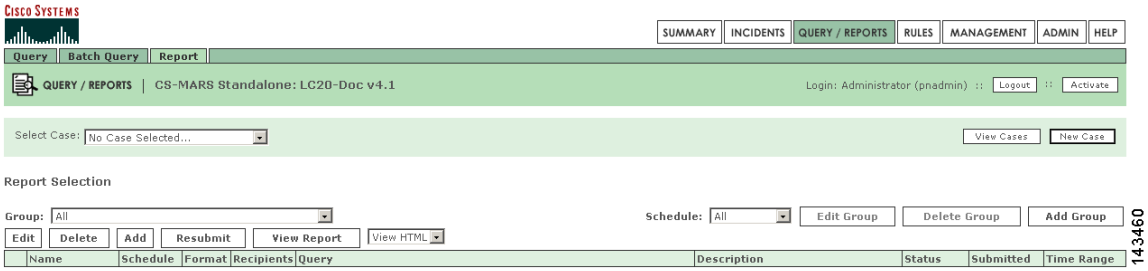
Add, Modify, and Delete a Report Group

Adding a New Report Group

To add a report group follow these steps:

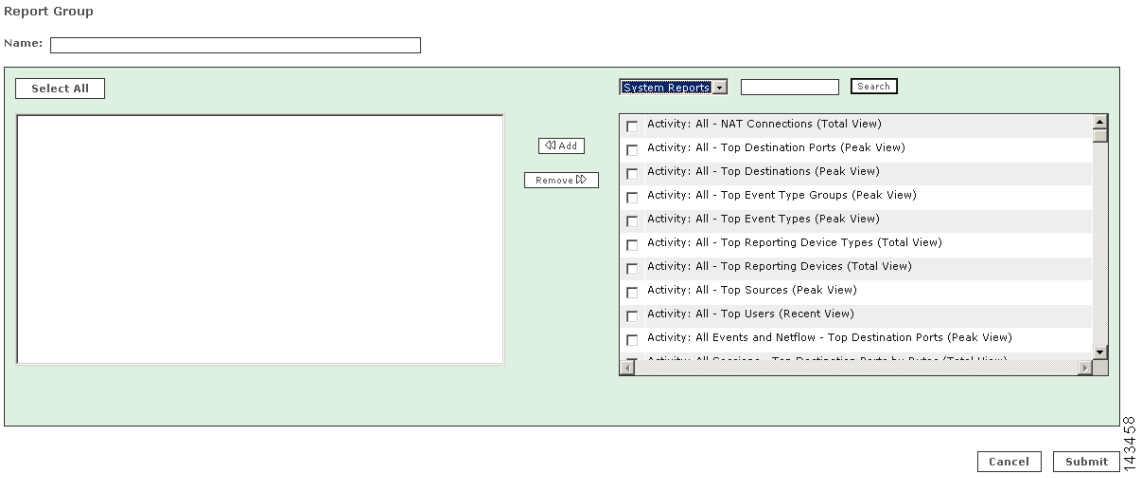
Step 1 Navigate to the Report page, as shown in Figure 22-13.

Figure 22-13 Reports Page



Step 2 Click **Add Group**.
The Add Group dialog box appears, as shown in Figure 22-14.

Figure 22-14 Add Report Group Dialog Box



Step 3 Enter the new report group name in the **Name** field.

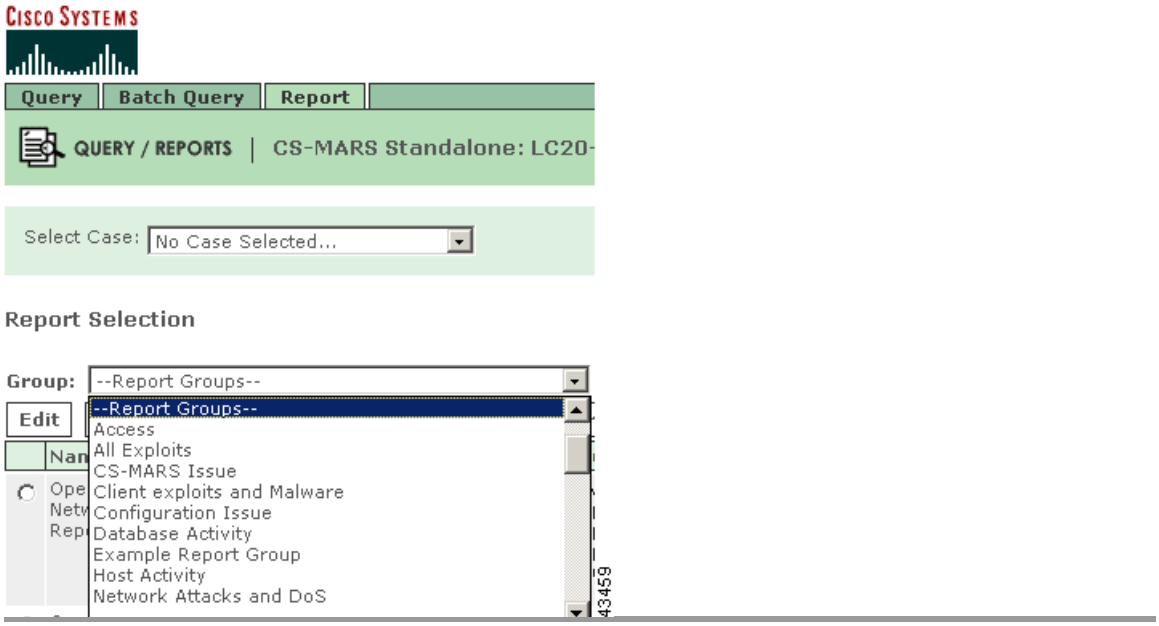
Step 4 Click the checkboxes of the reports to be added to the new report group.

Tip The dropdown filter above the list of reports can filter the display of reports to display system reports, user reports, or all reports. The search function displays only those reports that match a search string (for example, “Spy” for Spyware). The asterisk wildcard character (*) is supported.

Step 5 Click **Add.**
The selected reports appear in the lefthand pane of the dialog box. To remove a report from the group, highlight the item in the lefthand pane and click **Remove**.

Step 6 Click **Submit.**
The new report group name appears in the **Group** dropdown list display filter on the Report page, as shown in Figure 22-15, and on the Query Page. Because it is a user-created report group, the report group name appears without the prefix "system." You can also click **Cancel** to return to the Report page without creating a new report group.

Figure 22-15 The New Report Group Appears on the Dropdown Filter of the Report Page



Modifying a Report Group

To edit a report group, follow these steps:

Step 1 Navigate to the Reports page, as shown in Figure 22-13.

Step 2 Select the report group to edit from the **Group** pull-down list.

Step 3 Click **Edit Group**.
The Add Report Group dialog box appears, as shown in Figure 22-14. The report group name appears in the **Name** field, and the reports that comprise the report group appear in the lefthand pane of the dialog box.

Step 4 To add additional reports, click the checkboxes of the reports to be added to the group, then click **Add**. To remove reports, highlight the items to remove in the lefthand pane, then click **Remove**.

Step 5 Click **Submit.**

Deleting a Report Group

Step 1 Navigate to the Reports page, as shown in Figure 22-13.

Step 2 Select the report group to delete in the **Group** pulldown filter.

Step 3 Click **Delete Group**.
The Delete Report Group dialog box appears listing the reports in the group to delete. You are prompted to verify deletion.

Step 4 Click **Yes.**
The report group no longer appears in the report group dropdown lists on the Report and Query pages.

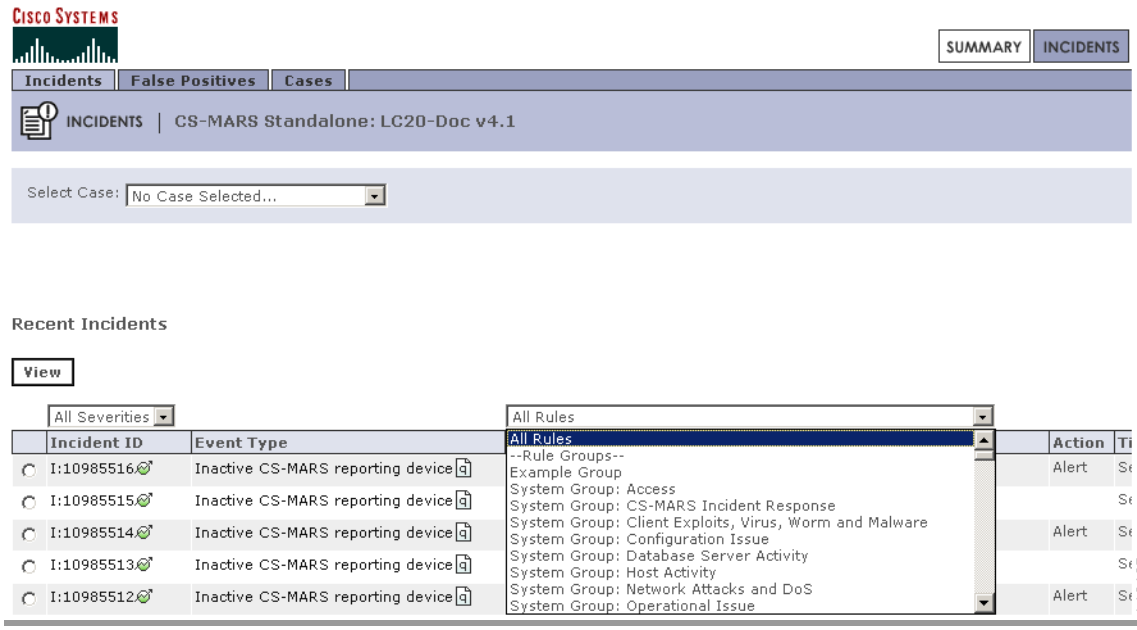
Display Incidents Related to a Rule Group

To display incidents that occur from the firing of rules in a specific rule group, follow these steps:

Step 1 Navigate to the Incidents page.

Step 2 Select the rule group in the dropdown filter above the Matched Rules column, as shown in Figure 22-16. The Incidents page will display only those incidents that occurred from rules firing in the selected rule group.

Figure 22-16 Rule Group on Incidents Page



Create Query Criteria with Report Groups

To create queries from report groups, follow these steps:

Step 1 Navigate to the Query page.

Step 2 Select a report group in the **Load Report as On-Demand Query with Filter** dropdown filter, as shown in Figure 22-17.
Only the reports that comprise the report group can now display in the Select Report dropdown list, as shown in Figure 22-18.

Figure 22-17 Selecting A Report Group to Make a Query

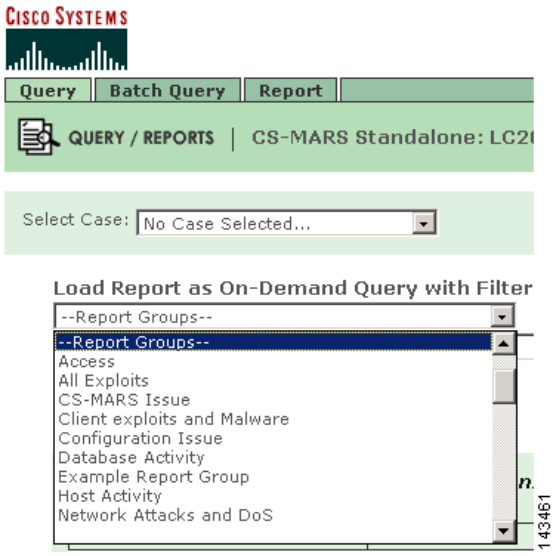
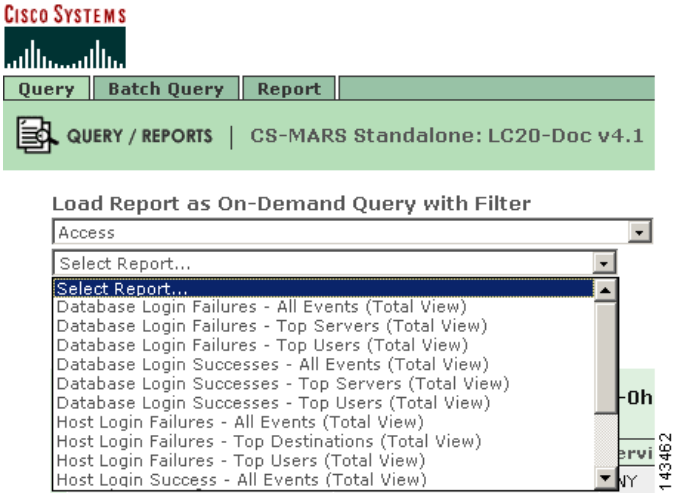


Figure 22-18 Selecting a Report Within the Report Group to Make a Query



Step 3 Select the report in the secondary dropdown list.
The **Query** criteria are automatically populated per the selected report.

Using Rule Groups in Query Criteria

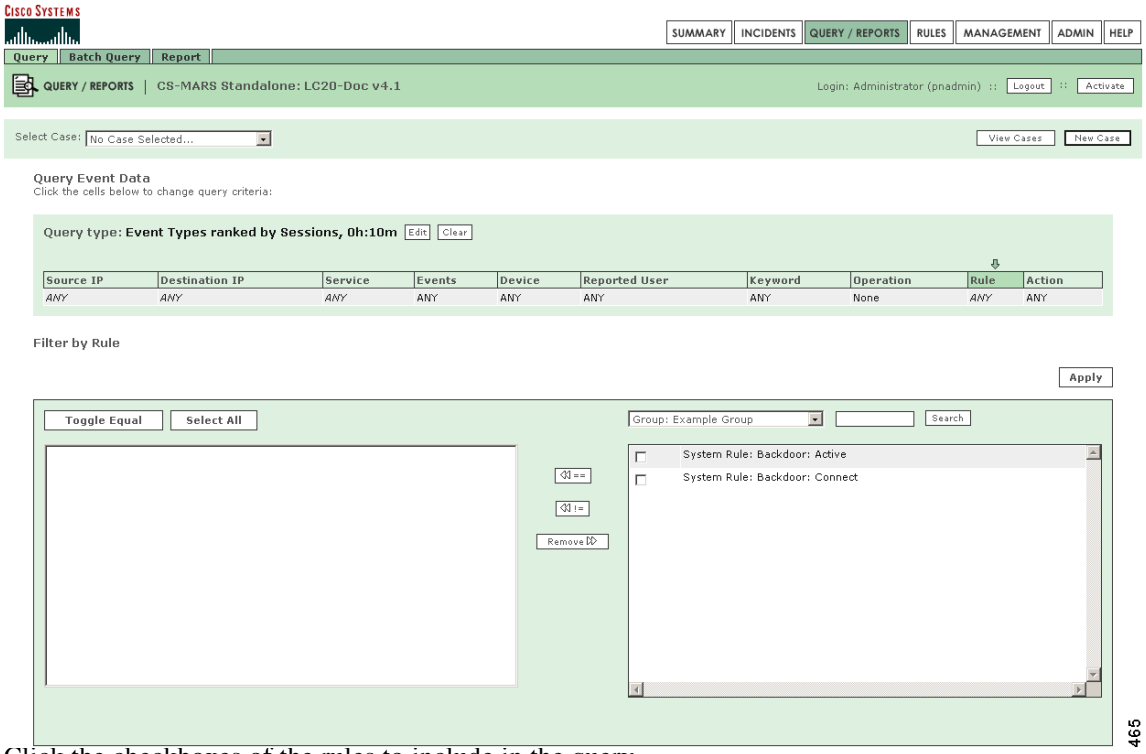
To populate the Rule field of the **Query Event Data** bar using rule groups, follow these steps:

Step 1 Navigate to the Query page.

Step 2 Click **Any** in the **Rules** field of the **Query Event Data** bar.
The Filter by Rule dialog box appears as shown in Figure 22-19.

Step 3 Select the rule group in the dropdown list above the list of rules, as shown in Figure 22-14.
The list of rules will display only those rules in the selected rule group.

Figure 22-19 Rule Group Used to Populate Rule Criterion in Query



Step 4 Click the checkboxes of the rules to include in the query.

Step 5 Click **Add**. The selected items appear in the lefthand pane of the Query dialog box.
To remove rules, highlight the items to remove in the lefthand pane, then click **Remove**.

Step 6 Click **Apply**.
The selected rules appear in the **Rules** field of the **Query Event Data** bar.