

Example: Fine-Tuning a Security Policy

This topic provides a suggested workflow for getting started and fine-tuning a security policy. It includes the following subtopics:

- Fine-Tuning Security Policies Process Overview on page 1
- Getting Started with the Recommended Security Policy on page 1
- Refining Rule Matching Properties on page 2
- Reducing False Positives on page 3
- Adding Rulebases on page 6

Fine-Tuning Security Policies Process Overview

You want to tune a security policy so that it is:

- Comprehensive—Detects all possible attacks on specific hosts in your network.
- Optimized—Each attack object specified in an IDP rulebase rule has a performance cost. In general, you want more rules with a few attack objects in each rather than fewer rules with many attack objects. In addition, we recommend that a single rule includes only the attack objects that are applicable to the rule destination server and only those of a severity that concerns you.
- Precise—Generates few false positives.
- Maintainable—As you refine your rules, you want to leverage as much of the built-in logic as possible. In your IDP rulebase rules, for example, you want to use the application identification feature, dynamic attack object groups, recommended attack objects, and recommended actions as much as possible, knowing the Juniper Networks Security Center team updates these as needed (even daily).

Fine-tuning is an iterative process. The process involves the following steps:

1. “Getting Started with the Recommended Security Policy” on page 1
2. “Refining Rule Matching Properties” on page 2
3. “Reducing False Positives” on page 3
4. “Adding Rulebases” on page 6

Getting Started with the Recommended Security Policy

When you add the IDP appliance to the NSM Device Manager, NSM automatically pushes the recommended policy to the IDP appliance. The recommended policy protects your network from the most frequent and severe attacks.

Table 1 summarizes the properties of the Recommended security policy.

Table 1: Recommended Security Policy Definition

Property	Value
Rulebase	IDP rulebase
Rules	Nine rules, distinguished by attack object
Source	Any
Destination	Any
Service	Default, meaning the matching property is based on the service bindings of the attack object specified by the rule
Attack objects	Recommended IP, Recommended TCP, Recommended ICMP, Recommended HTTP, Recommended SMTP, Recommended DNS, Recommended FTP, Recommended POP3, Recommended IMAP, Recommended Trojan, Recommended Virus, Recommended Worm
Action	Recommended, meaning the action is specified by the attack object
Notification	Logging



NOTE: In the Recommended security policy, the source and destination matching parameters for rules are set to **Any**. These broad settings provide comprehensive protection, but they entail a performance cost and might result in more logs than are necessary. We recommend you customize these settings for destination servers.

Refining Rule Matching Properties

The source and destination matching parameters for template rules are set to **Any**. These broad settings provide comprehensive protection, but they entail a performance cost and might result in more logs than are necessary. We recommend you customize these settings.

Run the Profiler for several days to gather information about the hosts and applications running in your network. After several days, you should have the data you need to complete the following tasks:

- Create NSM address objects that identify groups of internal servers. When you configure rules to examine client to server traffic, you specify the internal servers as the rule's destination servers.
- Create an address object that defines your internal network. When you configure rules to examine traffic from your network to hosts on the world wide web, you can specify the internal network address object as the rule's source.
- Create NSM service objects to identify services running on internal servers. In most cases, you can specify **Default** for service so the rule uses the service relevant to the attack object. However, there might be cases where you want to specify a service object or service group.

- Identify predefined attack groups related to services (or create your own attack group, if necessary).
- Refine the IDP rulebase rule set so that each rule is focused on a single destination server (client to server traffic) or service (server to client traffic).

Reducing False Positives

A *false positive* is a log record that reflects an event on your network that you are not concerned about and no longer want to see in your logs. The IDP security policy found traffic that matched your rule, but over time you realize you do not need to track such events.

To determine whether a log is a false positive, you need to understand why the IDP device triggered the log and whether or not the traffic poses a real risk to the target server.

Suppose your security policy rule includes the following attack object: Predefined :: HTTP: Windows Media Services NSISlog.DLL Buffer Overflow. It generates a log when it identifies the attack pattern in traffic through the IDP device. Use the reference information in the details pane below the log table to learn more about the attack. You can click the hypertext linked name of the attack object in the summary tab to display reference information for the attack, as shown in Figure 1.

Figure 1: Using NSM Log Viewer Attack Reference Information

The screenshot displays the NSM Log Viewer interface. The main window shows a table of logs with columns for Log ID, Time Received, Alert, User Flag, Comment, Src Addr, Dst Addr, Action, Protocol, Dst., Nat Sr., Nat Ds., Details, Category, Subcategory, and Severity. A log entry for Log ID 20090806/416967 is highlighted, with a comment 'Windows 2000 SP4 only?'. A detailed view pane is open for the attack object 'HTTP: Windows Media Services NSISlog.DLL Buffer Overflow'. This pane includes a 'References' section with links to security advisories, an 'Extended Description' section, and a 'Technical Information' section detailing the vulnerability in Windows Media Services.

Log ID	Time Received	Alert	User Flag	Comment	Src Addr	Dst Addr	Action	Protocol	Dst.	Nat Sr.	Nat Ds.	Details	Category	Subcategory	Severity	
20090806/416941	8/5/09 11:13:33 PM	Alert			1.1.0.115	1.2.0.58	Conn Dropped	TCP	80	4	0.0.0.0	0.0.0.0	interface=eth2	Predefined	HTTP: IIS cmd.exe Command Exec...	Major
20090806/416943	8/5/09 11:13:33 PM	Alert			1.1.0.192	1.2.0.102	Conn Dropped	TCP	80	3	0.0.0.0	0.0.0.0	interface=eth2	Predefined	HTTP: IIS WebDAV SEARCH Co...	Device
20090806/416945	8/5/09 11:13:33 PM	Alert			1.1.0.212	1.2.0.241	Conn Dropped	TCP								
20090806/416948	8/5/09 11:13:33 PM	Alert			1.1.0.248	1.2.0.132	Conn Dropped	TC								
20090806/416949	8/5/09 11:13:36 PM	Alert			1.1.0.63	1.2.0.159	Conn Dropped	TC								
20090806/416950	8/5/09 11:13:36 PM	Alert			1.1.0.88	1.2.0.56	Conn Dropped	TC								
20090806/416951	8/5/09 11:13:36 PM	Alert			1.1.0.161	1.2.0.81	Conn Dropped	TC								
20090806/416956	8/5/09 11:13:36 PM	Alert			1.1.0.231	1.2.0.243	Conn Dropped	TC								
20090806/416957	8/5/09 11:13:36 PM	Alert			1.1.0.231	1.2.0.243	Conn Dropped	TC								
20090806/416961	8/5/09 11:13:36 PM	Alert			1.1.0.241	1.2.0.121	Conn Dropped	TC								
20090806/416966	8/5/09 11:13:42 PM	Alert			1.1.0.170	1.2.0.91	Conn Dropped	TC								
20090806/416967	8/5/09 11:13:42 PM	Alert		Windows 2000 SP4 only?	1.1.0.88	1.2.0.56	Conn Dropped	TC								
20090806/416971	8/5/09 11:13:45 PM	Alert			1.1.0.241	1.2.0.121	Conn Dropped	TC								
20090806/416972	8/5/09 11:13:45 PM	Alert			1.1.0.231	1.2.0.139	Conn Dropped	TC								
20090806/417097	8/5/09 11:14:59 PM	Alert			1.1.0.188	1.2.0.231	Conn Dropped	TC								
20090806/417098	8/5/09 11:17:37 PM	Alert			1.1.0.20	1.2.0.143	Conn Dropped	TC								
20090806/417099	8/5/09 11:17:40 PM	Alert			1.1.0.199	1.2.0.227	Conn Dropped	TC								
20090806/417100	8/5/09 11:17:40 PM	Alert			1.1.0.114	1.2.0.190	Conn Dropped	TC								
20090806/417101	8/5/09 11:17:40 PM	Alert			1.1.0.234	1.2.0.123	Conn Dropped	TC								
20090806/417102	8/5/09 11:17:40 PM	Alert			1.1.0.189	1.2.0.95	Conn Dropped	TC								
20090806/417103	8/5/09 11:17:40 PM	Alert			1.1.0.48	1.2.0.155	Conn Dropped	TC								
20090806/417104	8/5/09 11:17:40 PM	Alert			1.1.0.48	1.2.0.155	Conn Dropped	TC								
20090806/417105	8/5/09 11:17:40 PM	Alert			1.1.0.48	1.2.0.155	Conn Dropped	TC								
20090806/417106	8/5/09 11:17:40 PM	Alert			1.1.0.48	1.2.0.155	Conn Dropped	TC								
20090806/417107	8/5/09 11:17:43 PM	Alert			1.1.0.205	1.2.0.103	Conn Dropped	TC								
20090806/417108	8/5/09 11:17:43 PM	Alert			1.1.0.109	1.2.0.55	Conn Dropped	TC								

In this example, we learn that the threat detected applies only to Microsoft Windows 2000 Server SP4. It is a false positive because all of the Windows servers in our network are Windows Server 2008. You can use the NSM Log Viewer flag and comment features to mark logs as false positives. In Figure 2, we have marked the log ID 20090806/416967 as a false positive because the attack targets server versions not present in our network.

Figure 2: Using NSM Log Viewer Flag and Comment Features

The screenshot displays the NSM Log Viewer interface. At the top, it shows the current network configuration: "per Networks - NSM - global : current". Below this is a search bar and a "Log Viewer [3-IDP00I]" window. The main area contains a table of log entries with columns for Log ID, Time Received, Alert, User Flag, Comment, Src Addr, Dst Addr, Action, Protocol, Dst..., Nat Sr..., and Nat Ds... The entry for Log ID 20090806/416967 is highlighted, and a context menu is open over it. The menu includes options like Filter, Find, Flag, Exempt..., Show, Hide Log, Unhide Log, and Goto Policy. The 'Flag' sub-menu is open, showing options like High, Medium, Low, Closed, False Positive, Assigned, Investigate, Follow-Up, Pending, and Clear. The 'False Positive' option is selected. Below the table is a timeline view showing dates from Jul 30 to Aug 7. At the bottom, there is a summary section with tabs for "Summary", "All Fields", "Whois Lookup", and "Quick Report". The summary section shows a predefined signature for "HTTP: Windows Media Services NSISlog.DLL Buffer Overflow" and a matching data snippet in HEX format. The interface is filtered on "Category".

Log ID	Time Received	Alert	User Flag	Comment	Src Addr	Dst Addr	Action	Protocol	Dst...	Nat Sr...	Nat Ds...
20090806/416941	8/5/09 11:13:33 PM	[Alert Icon]			1.1.0.115	1.2.0.58	Conn Dropped	TCP	80	4	0.0.0.0 0.0.0.0
20090806/416943	8/5/09 11:13:33 PM	[Alert Icon]			1.1.0.192	1.2.0.102	Conn Dropped	TCP	80	3	0.0.0.0 0.0.0.0
20090806/416945	8/5/09 11:13:33 PM	[Alert Icon]			1.1.0.212	1.2.0.241	Conn Dropped	TCP	80	4	0.0.0.0 0.0.0.0
20090806/416948	8/5/09 11:13:33 PM	[Alert Icon]			1.1.0.248	1.2.0.132	Conn Dropped	TCP	80	4	0.0.0.0 0.0.0.0
20090806/416949	8/5/09 11:13:36 PM	[Alert Icon]			1.1.0.63	1.2.0.159	Conn Dropped	TCP	80	3	0.0.0.0 0.0.0.0
20090806/416950	8/5/09 11:13:36 PM	[Alert Icon]			1.1.0.88	1.2.0.56	Conn Dropped	TCP	80	3	0.0.0.0 0.0.0.0
20090806/416951	8/5/09 11:13:36 PM	[Alert Icon]			1.1.0.161	1.2.0.81	Conn Dropped	TCP	80	3	0.0.0.0 0.0.0.0
20090806/416956	8/5/09 11:13:36 PM	[Alert Icon]			1.1.0.231	1.2.0.243	Conn Dropped	TCP	80	4	0.0.0.0 0.0.0.0
20090806/416957	8/5/09 11:13:36 PM	[Alert Icon]			1.1.0.231	1.2.0.243	Conn Dropped	TCP	80	4	0.0.0.0 0.0.0.0
20090806/416961	8/5/09 11:13:36 PM	[Alert Icon]			1.1.0.241	1.2.0.121	Conn Dropped	TCP	80	4	0.0.0.0 0.0.0.0
20090806/416966	8/5/09 11:13:42 PM	[Alert Icon]			1.1.0.170	1.2.0.91	Conn Dropped	TCP	80	4	0.0.0.0 0.0.0.0
20090806/416967	8/5/09 11:13:42 PM	[Alert Icon]	[Flag Icon]	Windows 2000 SP4 only?	1.1.0.88	1.2.0.56	Cor		3	0.0.0.0	0.0.0.0
20090806/416971	8/5/09 11:13:45 PM	[Alert Icon]			1.1.0.241	1.2.0.121	Cor		3	0.0.0.0	0.0.0.0
20090806/416972	8/5/09 11:13:45 PM	[Alert Icon]			1.1.0.23	1.2.0.139	Cor		4	0.0.0.0	0.0.0.0
20090806/417097	8/5/09 11:14:59 PM	[Alert Icon]			1.1.0.188	1.2.0.231	Cor				
20090806/417098	8/5/09 11:17:37 PM	[Alert Icon]			1.1.0.20	1.2.0.143	Cor				
20090806/417099	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.199	1.2.0.227	Cor				
20090806/417100	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.114	1.2.0.190	Cor				
20090806/417101	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.234	1.2.0.123	Cor				
20090806/417102	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.189	1.2.0.95	Cor				
20090806/417103	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.48	1.2.0.155	Cor				
20090806/417104	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.48	1.2.0.155	Cor				
20090806/417105	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.48	1.2.0.155	Conn Dropped	TCP	1		
20090806/417106	8/5/09 11:17:40 PM	[Alert Icon]			1.1.0.48	1.2.0.155	Conn Dropped	TCP	1		
20090806/417107	8/5/09 11:17:43 PM	[Alert Icon]			1.1.0.205	1.2.0.103	Conn Dropped	TCP	1		
20090806/417108	8/5/09 11:17:43 PM	[Alert Icon]			1.1.0.109	1.2.0.55	Conn Dropped	TCP	1		

There are a number of ways you can tune your security policy to reduce false positives. Table 2 summarizes some basic tunings.

Table 2: Actions to Take To Reduce False Positives

Type of False Positive	Tuning Required
You trust the source.	Add an Exempt rulebase rule to “whitelist” the trusted source.
The attack applies to a hardware or software version that does not match your destination server.	You have many options: <ul style="list-style-type: none">■ Delete the attack from the rule.■ Modify an attack group to exclude the object.■ Add an Exempt rulebase rule to whitelist the non-offending attack object.■ Modify rule action so traffic is stopped or permitted differently from before.■ Modify the rule severity so that you can filter these events differently from before.
Your team has already patched the vulnerability detected by the attack.	Same as previous.
Upon examination, benign traffic crosses thresholds that trigger protocol anomaly events.	Use the NSM Device Manager to modify protocol anomaly thresholds.

Adding Rulebases

The IDP rulebase is the primary rulebase in an IDP security policy. When you have sufficiently tuned your IDP rulebase rules so that the security policy generates the level of logs you want, you can add additional rulebases to enable additional detection methods.

Take the same approach to tuning these additional rulebases. Instead of refining the group of attack objects that are relevant, you tune the IDP runtime parameters that set thresholds for detection mechanisms.

Related Topics The following related topics are included in the *IDP Concepts and Examples Guide*:

- Profiler Overview
- Understanding the Rule-Matching Algorithm
- Understanding IDP Rulebase Rule Match Settings
- Understanding the Components of an IDP Security Policy
- Understanding the Exempt Rulebase
- Using Attack Objects
- IDP Logs Overview

The following related topic is included in the *IDP Administration Guide*:

- Modifying the IDP Device Configuration

Published: 2010-01-12