

## Understanding IDP Rulebase Notification Options

You use notification features to help you manage your network, analyze your network security, validate your security policy, and capture forensic evidence of attacks. You can set notification options per rule.

The first time you design a security policy, you might be tempted to log all data for all attacks and let the policy run indefinitely. We recommend you take a more refined approach. Some attack objects are informational only, and others can generate false positives and redundant logs. If you become overloaded with data, you can miss something important. Remember that security policies that generate too many log records are hazardous to the security of your network, as you might discover an attack too late or miss a security breach entirely as a result of having to sift through hundreds of log records. Excessive logging can also affect IDP throughput, performance, and available disk space. A good security policy generates enough logs to fully document only the important security events on your network.

By default, logging is enabled for IDP rulebase rules. Table 1 describes the notification options you can configure. You also have the option to disable logging.

**Table 1: IDP Rulebase Notification Options**

Option	Description
Event logs and alerts	<p>You can enable the following delivery and handling options for logs:</p> <ul style="list-style-type: none"><li>■ Send to NSM log viewer.</li><li>■ Send to NSM log viewer and flag as an alert.</li><li>■ Send to an e-mail address list.</li><li>■ Send to syslog.</li><li>■ Send to SNMP trap.</li><li>■ Save in XML format.</li><li>■ Save in CVS format.</li><li>■ Process with a script.</li></ul>
Packet captures	<p>Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.</p> <p>If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure rule 1 to capture 10 packets before and after the attack, and you configure rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.</p> <p>You can capture up to 256 packets before the event and 256 packets after the event.</p> <p><b>NOTE:</b> If necessary, you can improve performance by logging only the packets received after the attack.</p>

For complete procedures on setting IDP rulebase notification options, see the *IDP Administration Guide*.

**Related Topics** The following related topic is included in the *IDP Concepts and Examples Guide*:

- Understanding the IDP Rulebase
- IDP Logs Overview

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

- IDP Logs and Reports in NSM Task Summary

---

Published: 2010-01-12