

Understanding Backdoor Rulebase Notification Options

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

Table 1: Backdoor 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">■ Send to NSM log viewer.■ Send to NSM log viewer and flag as an alert.■ Send to an e-mail address list.■ Send to syslog.■ Send to SNMP trap.■ Save in XML format.■ Save in CVS format.■ Process with a script.
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, the IDP device 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, the IDP device 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>NOTE: If necessary, you can improve performance by logging only the packets received after the attack.</p>



NOTE: Backdoor rulebase notification options are the same as IDP rulebase options.

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

- Understanding the Backdoor Rulebase
- IDP Logs Overview

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

- Configuring Backdoor Rulebase Rules (NSM Procedure)

Published: 2010-01-12