

Understanding Traffic Anomalies Rulebase Notification Options

By default, logging is enabled for Traffic Anomalies rulebase rules. Table 1 describes notification options. You also have the option of disabling logging.

Table 1: Traffic Anomalies Rulebase Notification Options

Option	Description
Event logs and alerts	You can enable the following delivery and handling options for logs: <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	Packet capture is not available for Traffic Anomalies rulebase rules.



NOTE: Traffic Anomalies rulebase notification options are the same as IDP rulebase options, except that packet capture is not applicable.

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

- Understanding the Traffic Anomalies Rulebase
- IDP Logs Overview

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

- Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)

Published: 2010-01-12