

IDP Logs Overview

The IDP system generates logs for device events and security events.

Device event logs are related to the operation of the IDP appliance. By default, the system logs events when it reaches the rising and reset threshold for memory usage, CPU usage, disk space usage, or maximum number of active sessions. The default threshold is 90%. You can optionally configure logging for other operational events, such as flow or fragment errors.

Security event logs are related to traffic that matches security policy rules, Layer 2 detection settings, or IP spoof attack settings.

Table 1 summarizes options for viewing and managing logs.

Table 1: IDP Logging Options

Option	Description
Network and Security Manager (NSM)	<p>IDP devices automatically send device event logs to NSM. IDP devices send security event logs when traffic matches security policy rules for which logging has been enabled. You can use the NSM log viewer to sort through and analyze logs. If you enable packet logging for a security policy rule, you can use the NSM packet viewer to display packet data.</p> <p>For details on using NSM log utilities, see the <i>Network and Security Manager Administration Guide</i>.</p>
Syslog	<p>You can configure IDP devices to forward logs to a syslog server, a commonly used method for storing logs for troubleshooting or record-keeping.</p> <p>For details on configuring syslog collection, see the <i>IDP Administration Guide</i>.</p>
SNMP	<p>You can enable SNMP reporting. With SNMP enabled and configured, an SNMP manager can use the snmp get command to query the IDP appliance statistics for CPU usage, memory usage, disk usage, and session count. In addition, the IDP sends an SNMP trap when usage exceeds 90%.</p> <p>For details on configuring SNMP reporting, see the <i>IDP Administration Guide</i>.</p>
Log suppression	<p>You can configure log suppression to reduce the volume of logs. The log suppression feature eliminates multiple log entries for events with the same properties. Instead, in NSM Log Viewer, a single entry appears along with a count of all such matching events.</p> <p>For details on configuring log suppression, see the <i>IDP Administration Guide</i>.</p>



NOTE: To avoid issues with reports, we highly recommend that you synchronize the network clocks for all devices to the same NTP server. For example, the network clocks for all IDP appliances and NSM clients should be synchronized to the NTP server specified in the NSM configuration.

Table 2 describes the fields that appear in log entries.

Table 2: NSM Log Viewer: Log Columns

Column	Description
Log ID	Unique ID for the log entry, derived by combining the date and log number.
Time Received	Date and time that the management system received the log entry.
Alert	NSM-defined alert for this type of log entry. Configure alerts in policy rules.
User Flag	To set a flag, right-click the log row, select Flag, and then select one of the following flags: <ul style="list-style-type: none"> ■ High ■ Medium ■ Low ■ Closed ■ False Positive ■ Assigned ■ Investigate ■ Follow-up ■ Pending
Src Addr	Source IP address of the packet that generated the log entry.
Dst Addr	Destination IP address of the packet that generated the log entry.
Action	Action the security device performed on the packet/connection that generated this log entry: <ul style="list-style-type: none"> ■ Accepted—Did not block the packet. ■ Closed Client—Closed the connection and sent an RST packet to the client, but did neither to the server. ■ Closed Server—Closed the connection and sent an RST packet to the server, but did neither to the client. ■ Closed—Closed the connection and sent an RST packet to both the client and the server. ■ Dropped—Dropped the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination. ■ Dropped Packet—Dropped a matching packet before it could reach its destination but did not close the connection. ■ Ignored—Matched the attack, did not take action, and ignored the remainder of the connection. <p>NOTE: IDP logs show the action that was set in the rule, not necessarily the actual action taken. For TCP events, these are the same. For UDP and ICMP events, the IDP logs show close client, close server, and close client and server actions, even when the actual action taken was a drop (close actions are not possible for UDP or ICMP packets).</p>
Protocol	Protocol that the packet that generated the log entry used.
Dst Port	Destination port of the packet that generated the log entry.
Rule #	Security policy rule that generated the log entry.
Nat Src Addr	NAT source address of the packet that generated the log entry.
Nat Dst Addr	NAT destination address of the packet that generated the log entry.

Table 2: NSM Log Viewer: Log Columns (continued)

Column	Description
Details	Miscellaneous string associated with log entry.
Category	Type of log entry: <ul style="list-style-type: none"> ■ Admin ■ Alarm—The device generates event alarms for any security event that has a predefined severity level of emergency, critical, or alert. Additionally, the device generates traffic alarm log entries when it detects network traffic that exceeds the specified alarm threshold in a rule (the traffic alarm log entry describes the security event that triggered the alarm). ■ Config—A configuration change occurred on the device. ■ Custom—A match with a custom attack object was detected. ■ Implicit—An implicit rule was matched. ■ Info—General system information. ■ Predefined. A match with a predefined attack object was detected. ■ Profiler—Traffic matches a Profiler alert setting. ■ Screen—Not applicable for IDP appliances. Generated by ScreenOS firewall devices. ■ Self—The device generated this log for a non-traffic related reason. ■ Sensor. ■ Traffic—Traffic matches a rule you have configured for harmless traffic. ■ URL Filtering—Not applicable for IDP appliances. Generated by ScreenOS firewall devices. ■ User.
Subcategory	Category-specific type of log entry (examples are "Reboot" or message ID).
Severity	Severity rating associated (if any) with this type of log entry: <ul style="list-style-type: none"> ■ Not Set (the device could not determine a severity for this log entry) ■ Info ■ Device_warning_log ■ Minor ■ Major ■ Device_critical_log ■ Emergency ■ Error ■ Notice ■ Informational ■ Debug
Device	Device that generated this log entry.
Comment	User-defined comment about the log entry.
Application Name	Application associated with the current log.
Bytes In	For sessions, specifies the number of inbound bytes.
Bytes Out	For sessions, specifies the number of outbound bytes.

Table 2: NSM Log Viewer: Log Columns (continued)

Column	Description
Bytes Total	For sessions, specifies the combined number of inbound and outbound bytes.
Dev Domain Ver	Domain version that generated this log entry.
Device Domain	Domain for the device that generated this log entry.
Device family	Family of the device that generated this log entry.
Dst Intf	Name of the outbound interface of the packet that generated this log entry.
Dst Zone	Destination zone associated with a traffic log entry.
Elapsed Secs	For sessions, specifies how long the session lasted.
Has Packet Data	Indicates whether the log entry has associated packet data.
NAT Dst Port	The NAT destination port of the packet that generated the log entry.
NAT Src Port	The NAT source port of the packet that generated the log entry.
Packets In	For sessions, specifies the number of inbound packets.
Packets Out	For sessions, specifies the number of outbound packets.
Packets Total	For sessions, specifies the combined number of inbound and outbound packets.
Policy	Security policy that generated the log entry.
Roles	Role group associated with this log entry.
Rule Domain	The domain of the rule that generated the log entry.
Rule Domain Ver	The domain version of the rule that generated the log entry.
Rulebase	Security policy rulebase that generated the log entry.
Src Intf	Name of the inbound interface of the packet that generated this log entry.
Src Port	Source port of the packet that generated the log entry.
Src Zone	Source zone associated with a traffic log entry.
Time Generated	Date and time the device generated the log entry.
User	User associated with this log entry.

The following example shows a syslog message record:

```
[syslog@juniper.net dayId="20061012" recordId="0" timeRecv="2006/10/12 21:52:21" timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0" device_ip="10.209.83.4" cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN"
```

```
srcZn="NULL" srcIntf="NULL" srcAddr="192.168.170.20" srcPort="63396"
natSrcAddr="NULL" natSrcPort="0" dstZn="NULL" dstIntf="NULL"
dstAddr="192.168.170.10" dstPort="27374" natDstAddr="NULL" natDstPort="0"
protocol="TCP" ruleDomain="" ruleVer="5" policy="Policy2" rulebase="IDS"
ruleNo="4" action="NONE" severity="LOW" alert="no" elapsedTime="0" inbytes="0"
outbytes="0" totBytes="0" inPak="0" outPak="0" totPak="0" repCount="0"
packetData="no" varEnum="31" misc="<017>'interface=eth2" user="NULL"
app="NULL" uri="NULL"]
```

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

- Developing a Logging Strategy
- Developing a Log Storage Strategy
- Example: Using NSM Log Viewer Features
- Example: Packet Logging Workflow
- Understanding IDP Rulebase Notification Options
- Understanding Backdoor Rulebase Notification Options
- Understanding SYN Protector Rulebase Notification Options
- Understanding Traffic Anomalies Rulebase Notification Options
- Understanding Network Honeypot Rulebase Notification Options
- Layer 2 Attack Prevention Overview
- IP Spoof Attack Prevention Overview

The following related topics are included in the *IDP Administration Guide*:

- IDP Logs and Reports in NSM Task Summary
- Using tcpdump to Capture Packets