

# Intrusion Detection and Prevention Series

## IDP OS 5.0r3 Release Notes

November 29, 2011  
Revision 03

### Contents

Overview . . . . .	2
Supported Hardware . . . . .	2
New and Changed Features . . . . .	2
Unsupported Features . . . . .	2
Known Limitations . . . . .	3
Supported Upgrade Paths . . . . .	3
Downgrading or Reverting . . . . .	4
Licensing . . . . .	4
Compatibility with Network and Security Manager . . . . .	5
Compatibility with Juniper Networks Infranet Controller . . . . .	5
Browser Requirements . . . . .	5
Upgrading IDP Software . . . . .	5
Upgrading with NSM . . . . .	6
Upgrading with the CLI . . . . .	8
Resolved Issues . . . . .	10
Known Issues . . . . .	13
Documentation . . . . .	17
Getting Help . . . . .	18

## Overview

Juniper Networks Intrusion Detection and Prevention Series devices enable you to enforce a security policy that protects your network from attacks and gather information about applications, clients, and servers in your network.

These release notes contain information about what is included in this product release: supported features, unsupported features, changed features, known problems, and resolved problems. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

## Supported Hardware

IDP 5.0r3 is supported on the following platforms:

- IDP8200, IDP800, IDP250, IDP75
- IDP1100, IDP600, IDP200

IDP OS 5.x does not support IDP50. The IDP50 has a 32-bit CPU. IDP OS 5.x is designed for 64-bit CPU devices.

## New and Changed Features

IDP OS Release 5.0r3 is intended for customers not ready to upgrade to an NSM version required for IDP OS 5.1. We have ported many system improvements from IDP OS 5.1 development work, but we have not ported IDP OS 5.1 features. If upgrading NSM is not an issue for you, we recommend you evaluate the latest IDP OS release. At this time, the latest is IDP OS 5.1r2.

The following table describes new and changed features in IDP OS 5.0r3.

**Table 1: New and Changed Features**

Feature	Description
Auto-recovery	Added a new option for the auto-recovery feature. Enable the new option if the default implementation causes link flapping during the recovery process. For information on the new option, see <a href="#">Tuning the Auto-Recovery Bypass Setting</a> .
Debugging enhancements	A kernel crash now generates a vmcore crash dump file. The vmcore dump file is saved to the coredump directory, for example <code>/var/crash/2011-06-03-23:19/vmcore</code> . You can use gdb or crash tools to examine the vmcore dump file.

## Unsupported Features

The following features are not supported in IDP 5.0r1, 5.0r2, or 5.0r3:

- High availability (standalone or third-party).
- SSL decryption using IDEA-based algorithms or ciphers.

- On IDP8200, 10 Gigabit Ethernet interfaces do not support peer port modulation (PPM).
- On IDP800, the following I/O modules do not support PPM:
  - 4-port 1-GigE fiber SFP (without internal bypass) (IDP-1GE-4SFP)
  - 4-port 1-GigE fiber SX (with internal bypass) (IDP-1GE-4SX-BYP)
- Authentication to the ACM via RADIUS with RSA SecurID (authentication via RADIUS server is supported).

## Known Limitations

---

For single core platforms (IDP75, IDP200, IDP600), we recommend you disable application volume tracking (AVT). The AVT feature is fully functional, but the AVT process is CPU intensive. During stress testing, high CPU usage by the AVT feature resulted in link flapping.

Note that if you disable AVT, IDP Reporter application volume reports are empty.

To disable AVT:

1. From NSM Device Manager, double-click a device and then click **Profiler Settings**.
2. Click the **General** tab.
3. Deselect **Enable AVT**.
4. Click **Apply**.
5. From NSM Device Manager, right-click the device and select **Update Device** to push your configuration change to the device.

## Supported Upgrade Paths

---

You can upgrade directly from any of the following versions:

- 5.0r2
- 5.0r1
- 4.1r4



**NOTE:** The upgrade paths assume your current IDP device has been in use and the device had been added to NSM. You might encounter unexpected behavior during the upgrade if you are upgrading to IDP 5.0r3 from a newly reimaged, undeployed IDP 4.2 or 4.1 device (such as a 2009 factory image of the IDP OS). In these cases, we recommend you add the IDP device to NSM and import the device configuration into NSM prior to performing the 5.0r3 upgrade. Doing so will avoid the file permissions issue described in [KB 15071](#).

Table 2 on page 4 describes the changes to files and directories you will notice when you upgrade.

**Table 2: Changes to Files and Directories**

Upgrade Path	Files and Directories
From 5.0r2	No changes.
From 5.0r1	<p>Before you upgrade, take note of the following changes and recommended actions:</p> <ul style="list-style-type: none"> <li>In IDP 5.0r3, packet logs are stored in numbered subdirectories of <code>/usr/idp/device/var/pktlogs/</code>. To implement this change, your existing <code>/usr/idp/device/var/pktlogs/</code> directory will be overwritten. If you have been using the option to maintain packet data locally and send to NSM on demand, copy any packet logs you want saved from <code>/usr/idp/device/var/pktlogs/</code> to a remote location before you upgrade. Previously collected packet capture logs will not be available to NSM. This action is not required if you have been using the option to always include packet data when NSM sends the event log.</li> <li>Your custom settings in the <code>/usr/idp/device/bin/user_funcs</code> file are preserved when you upgrade from IDP 5.0r1. No action is required. However, if you want to change the default JNET failure count, you must add a variable declaration to the <code>user_funcs</code> file after you upgrade. For details, see <a href="#">Tuning the JNET Driver Failure Count</a>.</li> </ul>
From 4.1r4	<p>When you upgrade from IDP 4.1 to IDP 5.0, you are reimaging the disk with a new operating system. All partitions except <code>/var/idp</code> are rewritten.</p> <p>In addition, in IDP 5.0r3, packet logs are stored in numbered subdirectories of <code>/usr/idp/device/var/pktlogs/</code>. This is the same directory structure introduced in IDP 4.1r4. Note, however, that the upgrade process preserves only packet log files in <code>/usr/idp/device/var/pktlogs/0/</code>. Packet log files in other directories will be lost upon upgrade. If you have been using the option to maintain packet data locally and send to NSM on demand, copy logs from <code>/usr/idp/device/var/pktlogs/1/</code> and higher numbered log directories to a remote location before you upgrade. This action is not required if you have been using the option to always include packet data when NSM sends the event log.</p> <p>The upgrade process restores your license and most of your previous settings. The following settings are not preserved:</p> <ul style="list-style-type: none"> <li>The upgrade does not retain settings no longer supported in IDP 5.0.</li> <li>The upgrade process saves a backup of your previous <code>/usr/idp/device/bin/user_funcs</code> file, but installs a new <code>user_funcs</code> file in order to provide appropriate content for IDP 5.0.</li> </ul>

## Downgrading or Reverting

You cannot downgrade or revert to a previous version. You can reimage the operating system, if necessary. For details on reimaging, see the installation guide.

## Licensing

The upgrade procedure preserves your earlier license configuration. Reimaging does not. If you reimage the appliance, see the installation guide for information on licensing.

---

## Compatibility with Network and Security Manager

---

At the time of the IDP 5.0r3 release, we verified compatibility with the following release of Network and Security Manager (NSM):

- NSM 2010.3r2 (build LGB15z1bc)
- NSM 2011.1 (build LGB14z3a12)

You can download the NSM client and server software from the Juniper Customer Support Software Download website:

<http://www.juniper.net/customers/support/softserv.jsp>



**NOTE:** NSMExpress users should consult [KB 13946](#) for information on how to upgrade NSMExpress to a patch version of NSM.

---

## Compatibility with Juniper Networks Infranet Controller

---

The user-role-based policy feature depends on deployment with Unified Access Control (UAC) 3.0r1 or later.

---

## Browser Requirements

---

The ACM, QuickStart utility, and IDP Reporter have been tested on the following browsers:

- Internet Explorer 7.x, 6.x
- Firefox 3.x, 2.x

---

## Upgrading IDP Software

---

During upgrade, the IDP appliance is gracefully shut down. If you have configured bypass for traffic interfaces, you do not need to be concerned about traffic disruption. If you have not configured bypass, you should plan to complete your upgrade at an appropriate time.

You can use NSM or the CLI to upgrade IDP software. You must use NSM to complete the IDP detector engine and attack object updates.



**TIP:** If possible, use a laptop to connect to the console port of the IDP device when you upgrade. This will enable you to view any console messages that can assist in identifying any issues during upgrade. We understand this is not possible or desirable in all deployments, so connecting via console is not required to upgrade.

This section provides the following upgrade workflows:

- [Upgrading with NSM on page 6](#)
- [Upgrading with the CLI on page 8](#)

## Upgrading with NSM

This section describes a workflow for upgrading IDP software using only NSM.

To update IDP software:

1. Add the IDP software to the NSM GUI server.
2. Push the IDP software from the NSM GUI server to one or more IDP devices.

To add an IDP software image to the NSM GUI server:

1. Download the software image:
  - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
  - b. Enter the IDP device serial number to display a view of applicable software releases available for download.
  - c. Click the applicable link to display the software download page.
  - d. Download the software to a location you can access from your NSM client.
2. From the NSM main menu, select **Tools > Software Manager** to display the Software Manager dialog box.
3. Click the + button to display the Open dialog box.
4. Select the IDP software image you just downloaded and click **Open** to add the software image to the NSM GUI server.
5. Click **OK**.

To push the software image from the NSM GUI server to IDP devices:

1. From the NSM main menu, select **Devices > Software > Install Device Software** to display the Install Device Software dialog box.
2. From the Select OS Name list, select **ScreenOS/IDP**.
3. From the Select Software Image list, select the image file you just added to the NSM GUI server.
4. In the Select Devices list, select the IDP devices on which to install the software update.
5. Click **Next** and complete the wizard steps.
6. Select **Automate ADM Transformation** to automatically update the Abstract Data Model (ADM) for the device after NSM installs the update.



**NOTE:** If you clear this setting, the update is installed onto the device, but you cannot manage the device from NSM until the device ADM is updated.

7. Click **Finish** to display upgrade status in the Job Information dialog box.
8. When the upgrade finishes, click **Close** to exit the Job Information dialog box.
9. If your upgrade path is 5.0r1 to 5.0r3, reimport the device into NSM to avoid the issue reported in PR 499484:

In the NSM Device Manager, right-click the IDP device and select **Import Device**.

The software upgrade is complete.



**NOTE:** You might encounter unexpected behavior if you have changed the factory BIOS settings for the IDP device. We advise that you do not change the factory BIOS settings.

The console will hang at GRUB after reboot if you have changed the BIOS setting **Console redirection > Continue Console redirection after POST** to **ON**.

To resolve this issue, press the Delete key to enter BIOS and set this option to **OFF**.

- Next Steps:**
1. If you are upgrading from IDP 5.0r1 or 5.0r2, skip this step. You completed it when you upgraded to IDP 5.0r1 or 5.0r2. If you are upgrading from 4.2 or 4.1:
    - a. Run through the ACM wizard to [reconfigure your virtual routers](#). In IDP 5.0, you use ACM to configure deployment mode per virtual router.
    - b. If necessary, copy any custom settings from the backup copy of user\_funcs to the new user\_funcs file.
  2. If desired, modify the new default maximum number of packet captures stored locally on the IDP device. For details, see [Enabling Collection of Packet Data in NSM Logs \(NSM Procedure\)](#).
  3. Check to see if J-Security Center has released an update for the detector engine or attack database:
 

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.
  4. Push the updated IDP detector engine to IDP devices:
 

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.



**NOTE:** Updating the IDP detector engine on a device does not require a reboot of the device.

5. Push a security policy update job to update attack objects in use in your security policy:
  - a. In NSM, select **Devices > Configuration > Update Device Config**.
  - b. Select devices to which to push the updates and set update job options.
  - c. Click **OK**.

## Upgrading with the CLI

This section describes a workflow where you use the CLI to upgrade the software image on the IDP device. You still use NSM to update the detector engine and attack objects.

To upgrade IDP software from the CLI:

1. Download the software image to a host that runs an FTP server. Follow these steps:
  - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
  - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote)**. In the row for IDP, click **5.0**.
  - c. Save the **sensor\_version.sh** file (where *version* is the number that identifies the software release version).
2. Connect to the IDP command-line interface in one of the following ways:
  - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and enter **su -** to switch to root.
  - If you prefer, make a connection through the serial port and log in as root.



**NOTE:** To make an SSH connection, you must have enabled SSH for the management port (eth0). For details, see the ACM online Help.

3. Use SCP or FTP to copy the software image file to the IDP appliance. The IDP appliance does not run an FTP server, so you have to initiate the FTP session from the IDP appliance.
4. Run the upgrade script by entering **sh sensor\_version.sh**, where *version* is the number that identifies the software release version. When the script has finished, enter **reboot**.



**NOTE:** You might encounter unexpected behavior if you have changed the factory BIOS settings for the IDP device. We advise that you do not change the factory BIOS settings.

The console will hang at GRUB after reboot if you have changed the BIOS setting **Console redirection > Continue Console redirection after POST** to **ON**.

To resolve this issue, press the Delete key to enter BIOS and set this option to **OFF**.

5. In the NSM Device Manager, right-click the device, select **Adjust OS Version**, and complete the wizard steps.
6. If your upgrade path is 5.0r1 to 5.0r3, reimport the device into NSM to avoid the issue reported in PR 499484:

In the NSM Device Manager, right-click the IDP device and select **Import Device**.

The software upgrade is complete.

**Next Steps:**

1. If you are upgrading from IDP 5.0r1 or 5.0r2, skip this step. You completed it when you upgraded to IDP 5.0r1 or 5.0r2. If you are upgrading from 4.2 or 4.1:
  - a. Run through the ACM wizard to [reconfigure your virtual routers](#). In IDP 5.0, you use ACM to configure deployment mode per virtual router.
  - b. If necessary, copy any custom settings from the backup copy of user\_funcs to the new user\_funcs file.
2. If desired, modify the new default maximum number of packet captures stored locally on the IDP device. For details, see [Enabling Collection of Packet Data in NSM Logs \(NSM Procedure\)](#).
3. Check to see if J-Security Center has released an update for the detector engine or attack database:
 

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.
4. Push the updated IDP detector engine to IDP devices:
 

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.



**NOTE:** Updating the IDP detector engine on a device does not require a reboot of the device.

5. Push a security policy update job to update attack objects in use in your security policy:
  - a. In NSM, select **Devices > Configuration > Update Device Config**.
  - b. Select devices to which to push the updates and set update job options.
  - c. Click **OK**.

## Resolved Issues

The following table describes issues that are resolved when you upgrade to IDP 5.0r3.

**Table 3: Resolved Issues**

PR	Description
<b>NSM</b>	
610324	Resolved an issue with the IDP agent implementation that had resulted in connectivity problems between the IDP Series device and NSM.
<b>Configuration Issues</b>	
517629	Incorporated a fix from IDP OS 5.1r1 to resolve an issue where ACM had rejected Radius username formats containing a period (for example, john.doe).
<b>Logging / Packet Capture</b>	
430766	In IDP OS 5.0r2 release notes, we reported an issue with NSM. In NSM Profiler, updates to Network Profile tab logs had lagged behind Protocol Profile tab logs. This issue was resolved in NSM 2009.1r1-12.1eh.
483683	Resolved a memory-related issue with rule-based packet logging that had resulted in fewer packet captures than expected. We have made the packet logging implementation more robust. We have verified that IDP 5.0r3 packet logging is reliable, and the change does not affect performance.
531644	Incorporated a fix from IDP OS 5.1r1 to resolve an issue that had resulted in erroneous disk usage alarm logs.
542532	Resolved an issue that had resulted in incorrect idpLogReader debug logs. Logs reported via NSM were correct.
547870, 560867, 594694	Resolved an issue that had resulted in an inordinate number of reassembly module debug logs.
553551	Resolved an issue that had resulted in SNMP polling reports listing 1 gigabit (Gb) interfaces as 10 megabit (Mb) interfaces (IDP8200). The issue is resolved by upgrading to Net-SNMP-5.3.3.

Table 3: Resolved Issues (*continued*)

PR	Description
604970	Resolved an issue with autorecovery logs. Previously, the default log implementation included debug-level logs.
<b>CPU Utilization</b>	
502048	Incorporated a fix from IDP OS 5.1r1 to resolve an issue where, if the IDP OS services were restarted while the device was processing traffic, the <code>scio idp-cpu-utilization</code> query returned 0 (an incorrect value).
513844	Incorporated a fix from IDP OS 5.1r1 to resolve an issue where single core IDP Series platforms erroneously reported "CPU usage high" messages to NSM.
<b>Stability</b>	
484858	Resolved an issue with the autorecovery process that had resulted in the MPLS decapsulation setting not being reinitialized.
522406	Incorporated a fix from IDP OS 5.1r1 to resolve an issue that had caused a kernel panic after reboot.
551187	Incorporated a fix from IDP OS 5.1r1 to resolve an issue that had killed the autorecovery process before recovery was completed.
541239	Implemented changes to IDP engine and JNET driver processing to address issues with the bypass feature that had resulted in packet forwarding failures.
548261	Incorporated a fix from IDP OS 5.1r1 to resolve a memory issue that had caused a detector engine update to fail when the security policy was large (IDP75).
552181	Incorporated a fix from IDP OS 5.1r1 to resolve an issue on IDP8200 where IDP engine CPU load had been incorrectly reported as 0%.
553639	Resolved an issue with the APE rulebase that had resulted in a crash under stress test conditions.
558250	Incorporated a fix from IDP OS 5.1r1 to avoid an issue that had resulted in a crash in a stress test environment. Added a logical check in the flow module.
559406	Incorporated a fix from IDP OS 5.1r1 to resolve a memory-related issue that had resulted in an IDP engine crash after a policy push.
545505	Changed implementation of fragmentation detection to avoid an issue that could result in a crash.
556284, 555921	Resolved an issue that had resulted in a hung state (triggering bypass) during a policy push in a stress test environment.
560281, 569184, 584034	Incorporated a fix from IDP OS 5.1r1 to avoid a memory leak issue.
562530, 587960, 602601	Resolved memory-related issues that had resulted in a crash.

Table 3: Resolved Issues (*continued*)

PR	Description
566120	Resolved an issue that had resulted in a hang condition and triggered bypass during a detector engine update. We changed the default behavior for the inactivity watchdog that monitors apparent network outages and triggers bypass. This setting can be modified in the <code>user_funcs</code> file. The variable is <code>nw_outage_trials</code> . The value is a number of 5-second intervals when the IDP device is not processing packets before it triggers. In earlier releases, the default was 5 (30 seconds). 30 seconds is sometimes insufficient for loading the detector engine update or a policy push update. In IDP 5.0r3, the default is 24 (130 seconds).
592095	Incorporated a fix from IDP OS 5.1r1 to resolve an issue with DiffServ marking that had caused a crash in a stress test environment.
594004	Changed implementation of SSL inspection to avoid an issue that had resulted in a crash in a high availability stress test environment.
594028	Incorporated a fix from IDP OS 5.1r2 to avoid a memory-related issue observed during stress testing for IDP1100F.
598575	Incorporated a fix from IDP OS 5.1r2 flow module to avoid a memory leak observed during stress testing.
663697	Incorporated IDP OS 5.1r1 DFA compression functionality to optimize memory and improve performance. With DFA compression, the DFA table is smaller, and you will notice a smaller policy file size.
665004	Added a new option for the auto-recovery feature. Enable the new option if the default implementation causes link flapping during the recovery process. For information on the new option, see <a href="#">Tuning the Auto-Recovery Bypass Setting</a> .
<b>Unexpected Behavior</b>	
510099	Incorporated a fix from IDP OS 5.1r1 to resolve an issue with the Radius PAM module that had resulted in Radius authentication for SSH to fail.
540685	Incorporated a fix from IDP OS 5.1r1 to resolve an issue where the command to disable protocol decoding <code>scio const -d set PROTOCOLNAME 0</code> had resulted in the device dropping traffic rather than passing it through as intended.
554619	Incorporated a fix from IDP OS 5.1r1 to reduce latency. Higher latency had been reported during SMB file transfers.
567916	Incorporated a fix from IDP OS 5.1r1 to resolve an issue where time updates from an NTP server stopped working after installing a patch release.
<b>Troubleshooting / Debugging</b>	
603614, 661503	A kernel crash now generates a vmcore crash dump file. The vmcore dump file is saved to the <code>coredump</code> directory, for example <code>/var/crash/2011-06-03-23:19/vmcore</code> . You can use <code>gdb</code> or <code>crash</code> tools to examine the vmcore dump file.
660935	Improved screen output messages for the <code>scio policy load s0 &lt;policy-file&gt; &lt;detector-path&gt;</code> command. Enhanced <code>idpengine</code> debug logs to include more information related to policy push processes.

Table 3: Resolved Issues (*continued*)

PR	Description
661504	<p>Improved log messages when interface links change state. Note the following changes:</p> <ul style="list-style-type: none"> <li>When a link goes down due to an external event, the log is generated by the interrupt routine of the driver. For these logs, the message string indicates <b>Link UP -&gt; DOWN: eth2</b>, for example.</li> <li>When a link is purposefully brought down by system processes or administrator action, the log is generated by the close routine of the driver. For these logs, the message string indicates <b>Interface brought down: eth2</b>, for example.</li> </ul>
661508	With debug logging enabled, the PPM daemon generates link status change messages when it takes down a peer interface.

## Known Issues

The following table describes issues that are present in IDP 5.0r3.

Table 4: Known Issues

PR	Description
<b>Upgrade</b>	
497226	<p>A manually set IDP device system clock setting is not preserved after upgrading to 5.0r3.</p> <p>Workaround: Use NTP to set the IDP device system clock. If you do not want to use NTP, you can use ACM to reset the system clock after you have completed the upgrade.</p>
499484	After upgrading from IDP 5.0r1 to IDP 5.0r3, the IDP detector version displayed in NSM might be incorrect. The detector engine version installed on the IDP OS 5.0r3 device is 5.0.110110809. In some cases, NSM displays the IDP 5.0r3 software image version number instead. To correct the version mismatch, reimport the device into NSM or perform a detector engine update to version 5.0.110110809.
<b>ACM</b>	
286327	Cosmetic issue: when no installed I/O module supports bypass, the ACM Configure Virtual Routers page should not display the user interface group for NIC State. When no installed I/O module supports bypass, NIC state is non-configurable.
298918	<p>ACM does not reject poorly formed alias names. In particular, ACM does not reject constructions with incomplete double-quote strings. For example, "hello (missing end-quote). As a result, the alias name does not appear in NSM.</p> <p>To avoid this issue, be careful to use complete double-quote constructions for alias names. For example, "hello".</p>

Table 4: Known Issues (*continued*)

PR	Description															
<b>Detection Accuracy</b>																
279408	<p>UDP port scanning works if there is no response from the Victim PC. However, if the response comes in the form of "UDP Port not reachable," the detection ignores the flow because the response packet is more than 20 bytes (default value).</p> <p>To work around this issue:</p> <ol style="list-style-type: none"> <li>1. In the NSM Device Manager, double-click the name of the device to display the configuration editor.</li> <li>2. Click <b>Sensor Settings</b>.</li> <li>3. Click the <b>Run-time parameters</b> tab.</li> <li>4. Under Traffic Signatures, increase the value for <b>Byte threshold for suspicious flows</b>.</li> </ol>															
417818	<p>The SYN Protector rulebase fails to reset the destination server connections when configured in Passive mode. To avoid this issue, use Relay mode instead.</p>															
<b>Configuration</b>																
303672	<p>In custom attack objects, in attack signatures, negation inside case-insensitive block is not supported. To work around this issue, rewrite the signature to avoid negation inside a case-insensitive block.</p>															
415301	<p>Policy validation through NSM does not return a warning if the APE rulebase rate limit you specify exceeds the ingress and egress capacity of device. You must be careful to consider the capacity of your links when you specify APE rulebase rate limiting actions.</p>															
426720	<p>In the following scenario, NSM policy validation should report a rule shadowing condition because the second rule could never be applied.</p> <table border="1"> <thead> <tr> <th>Rule</th> <th>Source</th> <th>Destination</th> <th>Service</th> <th>Attacks</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>any</td> <td>any</td> <td>HTTP</td> <td>All SMTP attacks</td> </tr> <tr> <td>2</td> <td>any</td> <td>any</td> <td>HTTP</td> <td>All HTTP attacks</td> </tr> </tbody> </table> <p>Traffic to port 80 would be inspected for only SMTP attacks and not HTTP attacks.</p>	Rule	Source	Destination	Service	Attacks	1	any	any	HTTP	All SMTP attacks	2	any	any	HTTP	All HTTP attacks
Rule	Source	Destination	Service	Attacks												
1	any	any	HTTP	All SMTP attacks												
2	any	any	HTTP	All HTTP attacks												
666486, 683833	<p>IDP OS release 5.1 includes custom attack signature enhancements: within bytes, within packets, and context checking constraints. The enhancements depend on IDP OS release 5.1. When a user creates a custom attack object for an earlier OS version, such as IDP OS 5.0r3, the features that depend on IDP OS release 5.1 should not appear in the user interface.</p>															
683823	<p>After updating to detector engine 5.0.110110809, the user expected the NSM custom attack object wizard Target and Platform Type page to include an entry for IDP 5.0.110110809. Instead, the nearest release listed in the NSM user interface was IDP 5.0.110110719. To work around this issue, you can select the nearest earlier detector engine. In this case, select IDP 5.0.110110719.</p>															

Table 4: Known Issues (*continued*)

PR	Description
<b>Monitoring / Console</b>	
288824	<p>Under high traffic conditions, the following exception messages are displayed in the console:</p> <pre>ata1.00: exception Emask 0x2 SAct 0xfe SErr 0x400000 action 0x2 frozen ata1.00: (spurious completions during NCQ issue=0x0 SAct=0xfe FIS=005040a1:00000001) ata1.00: cmd 61/30:08:8d:6e:16/00:00:00:00/40 tag 1 cdb 0x0 data 24576 out res 50/00:38:a5:70:16/00:00:00:00/40 Emask 0x2 (HSM violation)</pre> <p>You can safely ignore these messages.</p>
438582	<p>The NSM software version inventory fails to identify a patch version number when you add the IDP device or import a IDP device configuration. To work around this issue, you can use the NSM Device Manager to run an <b>Adjust OS</b> operation or use the IDP CLI to run <b>idp.sh restart</b>. However, the problem will recur following add device or import configuration procedures.</p>
673180	<p>Under some conditions, debug-level JNET driver log messages appear on the console when ACM Quick Start is applied. Debug-level messages should not be displayed in the console. You can safely ignore these messages.</p>
683819	<p>The <b>idp.sh</b> displays status messages to the screen. The messages displayed when running <b>idp.sh restart</b>, include the following:</p> <pre>cat: /sys/module/jnet_e1000/sections/.text: No such file or directory cat: /sys/module/jnet_e1000/sections/.data: No such file or directory</pre> <p>You can safely ignore these messages.</p>
<b>Logging / Packet Capture</b>	
287179	<p>After system unavailability, the system does not send a log that it has returned to normal operations.</p>
388321	<p>When traffic through the IDP appliance exceeds session capacity, the IDP device generates an event log and drops the traffic (if the constant for logging implicit drops is enabled). To avoid generating many logs around a similar event, the IDP appliance does not log additional instances until 1024 additional instances have occurred. We have received a request to make this delay value (1024) configurable. This issue is addressed in IDP OS 5.1r1.</p>
392392	<p>Unable to capture traffic in both directions with <b>tcpdump</b> when packet capture has been enabled with the <b>scio const set sc_pcap_outbound_pkts 1</b> command. This issue is addressed in IDP OS 5.1r1.</p>
407900	<p>In NSM log viewer, the strings for log severities for IDP devices are inconsistent with other network devices. For IDP devices, strings for severity include <b>Device_critical_log</b> and <b>Device_warning_log</b> instead of the strings <b>Critical</b> and <b>Warning</b> that appear for other network devices.</p>
415164	<p>In NSM, packet data cannot be displayed correct for certain malformed IP packets.</p>
419544	<p>In NSM Profiler logs, alert logs when Profiler detects a new, non-IP protocol always show the protocol as HOPOPT instead of the specific protocol.</p>
423852	<p>In NSM log viewer, the value in the Subcategory column for flow bypass and auto-recovery logs is Other. We expect the value to identify the flow bypass or auto-recovery event more specifically.</p>
427100	<p>Syslog issue: auto-recovery events reported in syslog messages do not indicate which IDP engine restarted.</p>

Table 4: Known Issues (*continued*)

PR	Description
429095	Syslog issue: NIC state events reported in syslog messages do not indicate that the virtual router has returned to "Normal mode". NSM logs do indicate this in the Subcategory column. This issue is addressed in IDP OS 5.1r1.
429097	Syslog issue: changes in link status (link down or link up) are not reported in syslog messages. These events are reported to NSM and appear in the Details column. This issue is addressed in IDP OS 5.1r1.
462680	We are tracking work to improve syslog messages so they are more useful when parsed by syslog reporters, such as Juniper Networks STRM.
493119	The SNMP trap <code>jnxIdpSensorFreeDiskSpace</code> is generated when the disk space exceeds the threshold but a down trap is not generated when it falls below the threshold. This issue is addressed in IDP OS 5.1r1.
540264	Errors reported when running <code>scio pcap</code> to replay packet captures. To work around this issue, send a ping through the lab network so that it traverses the same interface that is replaying the packet capture. We have tested this workaround with a lab setup that replays a set of 1 kilobyte packets every 10 seconds.
604426	Unexpected <code>snmpd</code> crashes. We are investigating the root cause.
672104	In IDP8200 autorecovery lab tests, we observed that when more than one IDP engine is killed and <code>idpengine0</code> is not the first to recover, the <code>idpinit</code> log file includes "Failed to recover IDP instance" messages.
<b>CPU Utilization</b>	
434539	In the <b>NSM Device Monitor &gt; View Device Details &gt; Process Status</b> tab, the CPU usage for the IDP engine is reported as 0%. You cannot use NSM to monitor device CPU utilization. We recommend you use SNMP to monitor CPU utilization and CLI utilities when investigating high or low CPU utilization.
474709	We report incorrect CPU utilization for single core platforms (IDP600, IDP200, IDP75). This issue is addressed in IDP OS 5.1r1, which supports use of the Linux <code>top</code> command to report CPU utilization for single core platforms..
<b>Stability</b>	
499447	For single core platforms (IDP75, IDP200, IDP600), we recommend you disable application volume tracking (AVT). AVT processes are CPU intensive, resulting in link flapping under stress.  Note that if you disable AVT, IDP Reporter application volume reports are empty.
<b>Shutdown Operation</b>	
432893	The <code>shutdown -h now</code> command might not behave as expected if you deploy IDP8200 with any of the following fiber I/O modules: IDP-10GE-4SX-BYP, IDP-10GE-2XFP, or IDP-10GE-2SR-BYP. Instead of shutting down, the OS unexpectedly restarts. This issue has been reported only in the initial shipments of this hardware. For details and a solution, contact JTAC.
<b>Documentation</b>	
424045	In NSM Device Manager, a new configuration section for Report Settings does not include online help. For information about the report settings you can configure with NSM, see the <a href="#">"IDP Logs and Reports in NSM Task Summary"</a> section in the <i>IDP Administration Guide</i> .

## Documentation

You can download user documentation from the Juniper Networks Web site:

<http://www.juniper.net/techpubs/>.

Table 5 on page 17 lists related IDP documentation.

**Table 5: Related IDP Documentation**

Document	Description
Juniper Networks Security Information Center	<p>The signature database contains predefined attack objects and predefined application objects used in the IDP security policy. The signature database is updated frequently (two or more times each week). The Security Information Center Web site provides a reference for all predefined attack objects and predefined application objects. You can find this information, as well as steps for subscribing to the RSS feed for the signature database update bulletin in the following location:</p> <p><a href="http://www.juniper.net/us/en/security/">http://www.juniper.net/us/en/security/</a></p>
IDP Detector Engine release notes	<p>The detector engine is a component of the IDP system that is updated quarterly. The detector engine release notes provide information about new features, changed features, fixed problems, and known issues with the IDP Detector Engine release.</p> <p>You can download these release notes from the following location:</p> <p><a href="http://www.juniper.net/techpubs/software/management/idp/de/index.html">http://www.juniper.net/techpubs/software/management/idp/de/index.html</a></p>
<i>IDP Series Deployment Scenarios</i>	Describes in-path (transparent mode), out-of-path (sniffer mode), and redundant path (high availability) deployments.
<i>IDP Series Installation Guide</i>	Describes IDP hardware and provides instructions for installing, configuring, updating, and servicing the device.
IDP Series Pathway Pages	A collection of topics from the <i>IDP Administration Guide</i> and <i>IDP Concepts and Examples Guide</i> , in HTML.
<i>IDP Series Administration Guide</i>	Provides procedures for completing IDP administration tasks with the Network and Security Manager (NSM) central management program; with the IDP device Appliance Configuration Manager (ACM); and with the IDP device command-line interface (CLI).
<i>IDP Series Concepts and Examples Guide</i>	Explains IDP features and provides examples of how to use the system.
<i>IDP Series Custom Attack Objects Reference and Examples Guide</i>	Provides examples and reference information for creating custom attack objects.
<i>IDP Reporter User's Guide</i>	Describes how to use IDP Reporter. The IDP Reporter features and user interface are similar to the Juniper Networks Application Usage Manager features and user interface. Where IDP Reporter includes application usage and attack data for a single IDP device, the application usage manager can aggregate this data for multiple devices and correlate it with subscriber data obtained from SRC devices.

Table 5 on page 17 lists related NSM documentation.

**Table 6: Related NSM Documentation**

Document	Description
Network and Security Manager release notes	Provides information about new features, changed features, fixed problems, and known issues with the NSM release.
<i>Network and Security Manager Installation Guide</i>	Describes how to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NSM.
<i>Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide</i>	Describes how to configure and manage IDP devices using NSM. This guide also helps in understanding of how to configure basic and advanced NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, viewing log information, and monitoring the status of IDP devices.
<i>Network and Security Manager Administration Guide</i>	<p>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI.</p> <p>This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</p>
Network and Security Manager Online Help	Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.

## Getting Help

If you need additional information or assistance, contact Juniper Networks Technical Assistance Center (JTAC) by E-mail ([support@juniper.net](mailto:support@juniper.net)) or telephone (1-888-314-JTAC within the United States or 1-408-745-9500 from outside the United States).

Copyright © 2011, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.