IDP Series Release Notes
IDP OS 5.1r3

January 25, 2012
Revision 01

Contents

Overview

Juniper Networks Intrusion Detection and Prevention Series devices enable you to enforce a security policy that leverages continuous security research by the Juniper Networks Security Intelligence Center to protect your network from attacks. The IDP Series also includes features that enable you to gather information about applications 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 5.1r3 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

There are no new features introduced IDP OS Release 5.1r3. If you are not familiar with IDP OS 5.1 features, see the IDP OS Release 5.1r1 release notes.

Unsupported Features

The following features are not supported in IDP OS Release 5.1r3:

- SSL decryption using IDEA-based algorithms or ciphers. Also not supported in IDP OS Release 5.0.x.
- On IDP8200, 10 Gigabit fiber interfaces do not support interface signaling or peer port modulation. Also not supported in IDP OS Release 5.0.x.
- Authentication to the ACM via RADIUS with RSA SecurID (authentication via RADIUS server is supported). Same as IDP OS Release 5.0.x.

Note that IDP75 does not have an HA interface. We do not support an HA deployment with IDP75 devices. Also, IDP75 has only one pair of traffic interfaces. We do not support a mixed mode deployment with IDP75 devices.

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:

- 5.1r2
- 5.0r2
- 4.1r2

NOTE: The upgrade paths assume your current IDP Series 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 from a newly reimaged, undeployed device (such as a 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 upgrade. Doing so will avoid the file permissions issue described in KB 15071.

Table 1 on page 3 describes the changes to files and directories you will notice when you upgrade.

Table 1: Changes to Files, Directories, and Key Settings

Upgrade Path	Files and Directories
From 5.1r2	No special changes to attend to before or after upgrade.
From 5.0r2	No special changes to attend to before or after upgrade.

Table 1: Changes to Files, Directories, and Key Settings *(continued)*

Upgrade Path	Files and Directories
From 4.1r2	*Before* upgrading to IDP OS 5.1r3, you must ensure the IDP Series device is deployed in transparent or sniffer mode. Beginning with IDP OS 5.0, IDP Series does not support bridge, proxy-arp, or router mode. To ensure a smooth upgrade, you must redeploy the device running IDP OS 4.1r2 in transparent or sniffer mode *before* you perform the upgrade to IDP OS 5.1r3.
	After you have performed the software upgrade, you must use ACM to configure the deployment mode for your virtual routers. Beginning with IDP OS 5.0, you configure deployment mode per virtual router, not one setting for all virtual routers.
	Before you upgrade, you might have to copy packet logs to a remote storage location. When you upgrade from IDP OS 4.1 to IDP OS 5.0 (or later), you are reimaging the disk with a new operating system. All partitions except **/var/idp** are rewritten. In addition, in IDP OS 5.1r3, packet logs are stored in numbered subdirectories of **/usr/idp/device/var/pktlogs/**. This is the same directory structure introduced in IDP OS 4.1r4. Note, however, that the upgrade process preserves only packet log files in **/usr/idp/device/var/pktlogs/0/**. 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 **/usr/idp/device/var/pktlogs/1/** 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.
	After you upgrade, you might have to redo custom settings in your **user_funcs** file. The upgrade process restores your license and most of your previous settings. The following settings are not preserved: • The upgrade does not retain settings no longer supported in IDP OS 5.0 (or later). • The upgrade process saves a backup of your previous **/usr/idp/device/bin/user_funcs** file, but installs a new **user_funcs** file in order to provide appropriate content for IDP OS 5.1r3.

Table 1: Changes to Files, Directories, and Key Settings *(continued)*

Upgrade Path	Files and Directories
	Before and *after* you upgrade, use ACM to review your NIC state settings. In IDP OS 4.1r2, NIC state options are **Normal**, **NIC bypass**, or **External bypass**. In subsequent releases, the NIC state options are **NICs off**, **NIC bypass**, or **External bypass**. In IDP OS 5.1r3, you use **NICs off** instead of **Normal**. If your IDP OS 4.1r2 configuration has NIC state set to **NIC bypass** or **External bypass**, there are no upgrade caveats to consider. If your IDP OS 4.1r2 configuration has NIC state set to **Normal**, there is an upgrade issue for you to consider. Consider these recommendations: • For standalone deployments, we recommend you set NIC state to **NIC bypass** before the upgrade, and, if you do not want to use NIC bypass going forward, set NIC state to **NICs off** after the upgrade. • For high availability deployments, setting NIC state to **NIC bypass** is not an option because the settings for HA and bypass are mutually exclusive (you cannot enable both HA and bypass). Be aware that during upgrades of an IDP OS 4.1r2 device with NIC state set to **Normal**, the NICs remain on and function as usual, but you will observe logs indicating that the nicBypass.sh process and network outage monitoring have been stopped. Do not be alarmed by these logs. However, do take action: use ACM to verify NIC state has been set to **NICs off** and apply the configuration to ensure network outage monitoring gets restarted.

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 for your IDP Series device.

Licensing

The upgrade procedure preserves your earlier license configuration. The reimaging procedure 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 OS Release 5.1r3, we verified compatibility with the following release of Network and Security Manager (NSM):

- NSM 2010.4Q59

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

Look for the NSM 2011.4 release in early 2012. Check the forthcoming NSM 2011.4 release notes for information about its support for the IDP OS. Information about NSM releases is available on the NSM documentation website.

NOTE: NSMXpress users should consult KB 13946 for information on how to upgrade NSMXpress to a patch version of NSM.

Compatibility with Juniper Networks Infranet Controller

The user-role-based policy feature depends on deployment with IC Series Unified Access Control (UAC) 4.1r1 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 Software on an HA Cluster

Upgrading an HA deployment involves special considerations. For information on upgrading an HA deployment, see "Workflow: Upgrading an IDP OS 4.1r4 Cluster to IDP OS 5.1" in *IDP Series Deployment Scenarios*.

Upgrading Software on a Standalone Device

During upgrade, the IDP Series device 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 the IDP OS software. You must use NSM to complete the IDP detector engine and attack object updates.

This section provides the following alternative workflows:

- Upgrading with NSM on page 6
- Upgrading with the CLI on page 9

TIP: If possible, use a laptop to connect to the console port of the IDP Series 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.

Upgrading with NSM

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

To update the IDP OS software:

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

To add an IDP OS 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 Series 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 OS 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 Series 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 Series 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.

The software upgrade is complete.

NOTE: You might encounter unexpected behavior if you have changed the factory BIOS settings for the IDP Series 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 later), skip this step. You completed it when you upgraded to IDP 5.0r1 (or later). If you are upgrading from 4.1r2:

   a. Run through the ACM wizard to reconfigure your virtual routers. In IDP 5.1, you use ACM to configure deployment mode per virtual router.

      In addition, for IDP200, IDP600, and IDP1100, the NIC state **NICs off** replaces **Normal**. Verify and apply your intended settings.

   b. If necessary, copy any custom settings from the backup copy of user_funcs to the new user_funcs file.

   c. If desired, modify the new default maximum number of packet captures stored locally on the IDP Series device. For details, see Enabling Collection of Packet Data in NSM Logs (NSM Procedure).

2. Check to see if the Juniper Networks Security Intelligence 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.

3. Push the updated IDP detector engine to IDP Series 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.**

4. 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 Series device. You still use NSM to update the detector engine and attack objects.

To upgrade IDP OS 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. Enter the IDP Series 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. Save the **sensor_*version*.sh** file (where version is the number that identifies the software release version).
2. Connect to the IDP OS 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 the user admin and enter **su -** to switch to the user 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 must initiate the FTP session from the IDP Series device.
4. Run the upgrade script by entering **sh sensor_*version*.sh**, where *version* is the number that identifies the OS 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 Series 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.

The software upgrade is complete.

Next Steps:

1. If you are upgrading from IDP 5.0r1 (or later), skip this step. You completed it when you upgraded to IDP 5.0r1 (or later). If you are upgrading from 4.1r2:

   a. Run through the ACM wizard to reconfigure your virtual routers. In IDP 5.1, you use ACM to configure deployment mode per virtual router.

      In addition, for IDP200, IDP600, and IDP1100, the NIC state **NICs off** replaces **Normal**. Verify and apply your intended settings.

   b. If necessary, copy any custom settings from the backup copy of user_funcs to the new user_funcs file.

   c. If desired, modify the new default maximum number of packet captures stored locally on the IDP Series device. For details, see Enabling Collection of Packet Data in NSM Logs (NSM Procedure).

2. Check to see if the Juniper Networks Security Intelligence 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.

3. Push the updated IDP detector engine to IDP Series 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.

4. 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 from IDP OS Release 5.1r2 to IDP OS Release 5.1r3. If you are upgrading from an earlier version, read the release notes for the subsequent releases to learn about the issues that were resolved in them.

Table 2: Resolved Issues

PR	Description
Upgrade	
613294	Resolved an issue in upgrades from IDP OS 4.2 in which ownership of the **/var/idp/device/cache** had been set incorrectly.
ACM	
679403, 702536	Enhanced security for the ACM web server.
NSM	
610324	Resolved an issue with the IDP agent implementation that had resulted in connectivity problems between the IDP Series device and NSM. Incorporated a fix from IDP OS 5.0r3.
System Files / Settings	
587306	Removed duplicate entries for **export nw_outage_trails** and **export max_intf_recv_failed_cnt_nicbypass** settings in **/usr/idp/device/bin/user_funcs**.
702811	Enhanced security related to system startup files.
Detection	
660632	Resolved an issue that had resulted in an **extended application object mismatch** error when processing a policy matching both an extended application and a simple application.

Table 2: Resolved Issues *(continued)*

PR	Description
Bypass	
685550	Changed bypass behavior when a traffic interface is down. In earlier releases, when one interface link in a virtual router (also called NIC pair) changed to a down state, a NIC pair configured for bypass would enter bypass mode. Beginning with IDP OS 5.1r3, a down interface link does not trigger bypass. We changed the implementation to make the IDP Series easier to maintain. Now, when a down interface is brought back up, traffic processing resumes automatically—without need for the administrator to restart the IDP service. In the case of a down link, we concluded the bypass functionality had provided little value: bypass would not prevent traffic outages because traffic would be stopped at the down link. The purpose of the bypass functionality remains to keep traffic flowing (uninspected) through the device when the IDP engine is unavailable.
Logging / Packet Capture	
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. Incorporated a fix from IDP OS 5.0r3.
553551	Resolved an issue that had resulted in SNMP polling reports listing 1 gigabit (Gb) interfaces as 10 megabit (Mb) interfaces (IDP8200). Incorporated a fix from IDP OS 5.0r3. The issue is resolved by upgrading to Net-SNMP-5.3.3.
595781	Resolved an issue with agent logs. Previously, the default log implementation included debug-level logs.
604970	Resolved an issue with autorecovery logs. Previously, the default log implementation included debug-level logs.
609165	Added a log pruning process that periodically purges debug log files that are saved in the **/var/idp/device/sysinfo/logs/** directory. The script does not prune event logs or packet logs, just system logs used for debugging. The script is located in **/usr/idp/device/bin/idplogpurger.sh**. The script belongs to a chron job that runs at 23:59 PM every day. The script performs the following actions: • Creates an archive of the debug log files found in **/var/idp/device/sysinfo/logs/**. The archive is compressed. The archive filename is related to the date the archive was created. For example, the archive **ziplog.20111011235952.tar.bz2** was created in Year 2011, Month 11, Day 12, Hour 23, Minute 59, Second 52. • Deletes the accumulated system process log files, except the latest one of each. • Deletes the 21st oldest archive file. In other words, the program maintains a collection of the 20 most recent archive files created as a result of the idplogpurger.sh process, pruning the oldest when it creates the newest.
672147	Resolved an issue with the idpLogReader process that could occur when the logging rate is high. The idpLogReader process now tracks the log temp file count and deletes files when the count exceeds 50,000.
683933	Resolved an issue that had resulted in a large number of httpd messages being written to **/var/log/httpd/error_log**. The Apache log level is now set to Warn instead of Debug.
Stability	
539476	Resolved an implementation issue that had resulted in policy push failure when multiple policies containing the APE rulebase are pushed in succession.

Table 2: Resolved Issues *(continued)*

PR	Description
587960	Resolved memory-related issues that had resulted in a crash. Incorporated a fix from IDP OS 5.0r3.
594004, 662920	Resolved an issue with flow implementation for SSL traffic that had resulted in a crash under stress test conditions.
613362, 691093	Resolved a memory-related issue with the Profiler Application Volume Tracking (AVT) feature that had resulted in core dumps.
668580	Resolved an issue with the Syn Protector rulebase Passive mode implementation that had resulted in a crash.
670039	Resolved an issue with session initiation protocol (SIP) processing that had resulted in a crash in a stress test environment.
677182	Resolved a memory-related issue with application signature processing for UDP packets. The issue had caused a crash in a stress test environment.
681301, 704715	We now disable the DVD-ROM driver after the system has completed its boot process to avoid an issue that had caused the system to hang after an upgrade to IDP OS 5.1r2. The root cause was related to the Linux kernel behavior with particular hardware. This issue had affected IDP1100, IDP600, or IDP200 only.
685456	Resolved an issue with the NTP client implementation that had resulted in an ntpd OpenSSL version mismatch error.
702897	Resolved a memory-related issue with the way flows are destructed. Incorporated a fix from ScreenOS 6.3.0r10.
Troubleshooting / Debugging	
660935	Improved screen output messages for the **scio policy load s0 <*policy-file*> <*detector-path*>** command. Enhanced idpengine debug logs to include more information related to policy push processes. Incorporated a fix from IDP OS 5.0r3.
661503	A kernel crash now generates a vmcore crash dump file. The vmcore dump file is saved to the coredump directory, for example **/var/crash/2011-06-03-23:19/vmcore**. JTAC can use the core dump file to debug the system. Incorporated a fix from IDP OS 5.0r3.
661504	Improved log messages when interface links change state. Incorporated a fix from IDP OS 5.0r3. Note the following changes: • 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 **Link UP -> DOWN: eth2**, for example. • 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 **Interface brought down: eth2**, for example.
661508	With debug logging enabled, the PPM daemon generates link status change messages when it takes down a peer interface. Incorporated a fix from IDP OS 5.0r3.

Known Issues

The following table describes issues that are present in IDP 5.1r3.

Table 3: Known Issues

PR	Description
Upgrade	
428341	During upgrade with NSM, the NSM Job Information window displays status information that is not consistent with the operations occurring on the IDP Series device.
497226	A manually set IDP Series device system clock setting is not preserved after upgrading to IDP OS 5.1 (release 5.1r1, 5.1r2, or 5.1r3). Workaround: Use NTP to set the IDP Series 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.

591151	During upgrade, userspace device management failure messages like those shown below are printed to the serial port console screen. You can ignore these messages.
	
	`GRUB Loading stage2...`
	`Press any key to continue.`
	`Press any key to continue.`
	`Press any key to continue.`
	`Press any key to continue.`
	`Press any key to continue.Red Hat nash version 5.1.19.6 starting`
	`Welcome to Juniper Networks IDP OS`
	`Press 'I' to enter interactive startup.`
	`Setting clock (utc): Wed Mar 9 02:51:43 PST 2011 [ OK ]`
	`Starting udev: udevd-event[2198]: wait_for_sysfs: waiting for`
	`'/sys/devices/pci0000:00/0000:00:1f.2/host1/ioerr_cnt' failed`
	`udevd-event[2199]: wait_for_sysfs: waiting for`
	`'/sys/devices/pci0000:00/0000:00:1f.2/host2/ioerr_cnt' failed`
	`udevd-event[2201]: wait_for_sysfs: waiting for`
	`'/sys/devices/pci0000:00/0000:00:1f.1/host4/ioerr_cnt' failed`
	`udevd-event[2202]: wait_for_sysfs: waiting for`
	`'/sys/devices/pci0000:00/0000:00:1f.1/host5/ioerr_cnt' failed`
	`udevd-event[2197]: wait_for_sysfs: waiting for`
	`'/sys/devices/pci0000:00/0000:00:1f.2/host0/ioerr_cnt' failed`
	`udevd-event[2200]: wait_for_sysfs: waiting for`
	`'/sys/devices/pci0000:00/0000:00:1f.2/host3/ioerr_cnt' failed`
	`udevd-event[2807]: wait_for_sysfs: waiting for`
	`'/sys/devices/pci0000:00/0000:00:1f.2/host0/target0:0:0/ioerr_cnt' failed`
	`[ OK ]`
	`Loading default keymap (us): [ OK ]`

Table 3: Known Issues *(continued)*

PR	Description
705930	In IDP OS 4.1r2, NIC state options are **Normal**, **NIC bypass**, or **External bypass**. In subsequent releases, the NIC state options are **NICs off**, **NIC bypass**, or **External bypass**. In IDP OS 5.1r3, you use **NICs off** instead of **Normal**. If your IDP OS 4.1r2 configuration has NIC state set to **NIC bypass** or **External bypass**, there are no upgrade caveats to consider. If your IDP OS 4.1r2 configuration has NIC state set to **Normal**, there is an upgrade issue for you to consider. Consider these recommendations: • For standalone deployments, we recommend you set NIC state to **NIC bypass** before the upgrade, and, if you do not want to use NIC bypass going forward, set NIC state to **NICs off** after the upgrade. • For high availability deployments, setting NIC state to **NIC bypass** is not an option because the settings for HA and bypass are mutually exclusive (you cannot enable both HA and bypass). Be aware that during upgrades of an IDP OS 4.1r2 device with NIC state set to **Normal**, the NICs remain on and function as usual, but you will observe logs indicating that the nicBypass.sh process and network outage monitoring have been stopped. Do not be alarmed by these logs. However, do take action: use ACM to verify NIC state has been set to **NICs off** and apply the configuration to ensure network outage monitoring gets restarted.
ACM	
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	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. To avoid this issue, be careful to use complete double-quote constructions for alias names. For example, “hello”.
591152	After you use ACM to apply a configuration change, ACM displays a page with status on the update. Within these logs, there is an erroneous message that you can ignore: "/bin/echo: write error: Invalid argument".
591857	After you use ACM to apply a configuration change that requires a reboot, ACM displays a page that confirms the configuration changes. The page is labeled “Configuration Saved & Applied”. In previous releases, this page was labeled “Confirm Configuration”.
Configuration	
303672	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.
415301	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.

Table 3: Known Issues *(continued)*

PR	Description

426720	In the following scenario, NSM policy validation should report a rule shadowing condition because the second rule could never be applied.
	
	`Rule Source Destination Service Attacks`
	
	`1 any any HTTP All SMTP attacks`
	
	`2 any any HTTP All HTTP attacks`
	
	Traffic to port 80 would be inspected for only SMTP attacks and not HTTP attacks.

431702	You must be careful configuring speed and duplex for IDP75 and IDP800 onboard interfaces and IDP8200 I/O module copper interfaces. The speed and duplex setting for the IDP Series interfaces and the peer switch or firewall interfaces must match. The best practice is to set both to AUTO. If you do not use auto-negotiation on both sides, you must ensure the explicitly specified speed and duplex settings match. We have observed traffic dropping if the IDP Series interfaces are configured as 100/10/1000 half/full duplex (AUTO-OFF) and the peer switch or firewall is configured as AUTO-ON.
536881	The NSM object editor does not enforce correct use of the within bytes constraint for custom signature attack objects. When you set a byte range constraint, you set a start point that is Context, Packet, or Stream. Your selection must be consistent with the pattern context setting for the attack object. For example, if you configured one of the service contexts, select **Context**. If you configured one of the packet contexts, select **Packet**. If you configured one of the stream contexts, select **Stream**. In NSM, it is possible to select a start point that is inconsistent with the pattern context setting. For example, the NSM object editor allows you to configure a pattern context http-variable and then set a within bytes start point that is start-of-packet. However, the within bytes match logic will be resolved to the start point you should have selected: context.
536967	When you configure a custom signature attack object, you can optionally set multiple within bytes constraints. Multiple entries are evaluated as a Boolean OR. This PR is to track a request for support for cases where you would want multiple entries processed as a Boolean AND.
537217	If you change the third-party HA setting (enable to disable, and vice versa), ACM reboots the device.
537481	IDP OS 5.1 (release 5.1r1, 5.1r2, or 5.1r3) does not support the within bytes constraint for custom compound attack objects.
538247	When you configure a custom compound attack object, you can optionally set within packets constraints. If you set a packet constraint for one member, the program logic counts packets beginning implicitly with the start-of-stream. Request is to include a UI option to specify the starting point.
539399	In ACM, you have the option to use a RADIUS server as an authentication source for access to ACM. However, the username format allowed by the ACM configuration page does not support all formats deemed valid by RFC 2486. In IDP OS Release 5.1 (release 5.1r1 or 5.1r2), you can specify a usernames that include periods (such as john.doe), but not special characters such as @ or + that are conventions in the username formats used by some enterprises (such as john.doe@company.com).

Table 3: Known Issues *(continued)*

PR	Description
552167	HA deployment has an IDP system requirement that a virtual router named vr0 contain eth1 (the HA state sync interface). If you upgrade an IDP OS 4.1r4 device that has HA enabled, eth1 is added to vr0 automatically. Otherwise, you must check the ACM Configure Virtual Routers page to ensure this HA system requirement is met. This requirement only applies if the device belongs to an HA deployment.
Monitoring / Console	
288824	Under high traffic conditions, the following exception messages are displayed in the console: `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:16/00:00:00:00:00/40 tag 1 cdb 0x0 data 24576 out res 50/00:38:a5:70:16/00:00:00:00:00/40 Emask 0x2 (HSM violation)` You can safely ignore these messages.
438582	The NSM software version inventory fails to identify a patch version number when you add the IDP Series device or import a IDP Series device configuration. To work around this issue, you can use the NSM Device Manager to run an Adjust OS operation or use the IDP OS CLI to run **idp.sh restart**. However, the problem will recur following add device or import configuration procedures.
Logging / Packet Capture	
227241, 416708	Profiler is unable to capture the OS fingerprint for some destination servers. Reports show “Unknown OS”.
287179	After system unavailability, the IDP Series device does not send a log that the device has returned to normal operations.
407900	In NSM log viewer, the strings for log severities for IDP Series devices are inconsistent with other network devices. For IDP Series devices, strings for severity include **Device_critical_log** and **Device_warning_log** instead of the strings **Critical** and **Warning** that appear for other network devices.
415164	In NSM, packet data cannot be displayed correct for certain malformed IP packets.
418220	Logs to IC Series: When log suppression is enabled, logs sent to the IC Series should indicate the repeat count when applicable.
419544	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.
423852	In NSM log viewer, the value in the Subcategory column for flow bypass and autorecovery logs is Other. We expect the value to identify the flow bypass or autorecovery event more specifically.
427100	Syslog issue: autorecovery events reported in syslog messages do not indicate which IDP engine restarted.
429086	Database limit exceeded alert log are not displayed in Profiler logs.
437768	We have observed a minor loss of application volume tracking (AVT) data If the AVT .stat file is larger than 1 GB.

Table 3: Known Issues *(continued)*

PR	Description
446451	Logs generated when a RADIUS user accesses ACM are sent to NSM but not to syslog. The logs should be sent to both (if syslog has been set up).
462005	IDP Reporter Application reports show incorrect statistics for bytes transferred. The report shows only client-to-server bytes, not total bytes.
462680	Request to change content of some syslog messages so they are more useful when viewed through syslog readers, such as STRM.

575772	SNMP: For IDP8200 only, the values reported for the following MIB objects are incorrect:
	• jnxIdpSensorFreePktBuffersFiveSec.0
	• jnxIdpSensorFreePktBuffersOneMin.0
	• jnxIdpSensorPktsRxdPerIntfcTable
	• jnxIdpSensorPktsTxRatePerIntfcTable
	• jnxIdpSensorPktsDropOnAllIntfc.0
	• jnxIdpSensorSignatureStatsTable
	• jnxIdpSensorTopTenSignatureStatsTable
	As a workaround, you can use NSM and IDP Reporter top attack reports to see the data for signature matches. You can log into the CLI and use the **jnetStats** command to retrieve packet buffer and packet transmission statistics. For example:
	`[root@defaulthost ~]# jnetStats`
	`../../jnetLib.c built on Dec 20 2010 at 23:05:51 with PRODUCTION build of SALEEN -43e.`
	`-- Worker Id 0 Stats:`
	`freePackets: 444032`
	`dropCount: 0`
	
	`-- Thread Id 0 Stats:`
	`rxPackets: 20846535763`
	`rxBytes: 14757418499789`
	`rxOverflow: 0`
	`rxQueued: 0`
	`txComplete: 18487802326`
	`txCompleteBytes: 14691015670286`
	`allocQueueSize: 1023`
	`txPackets: 18487802326`
	`txBytes: 14692307273740`
	
	`-- Device Id 0 (eth2) Stats:`
	`Link Status: Down`
	`rxPackets: 0`
	`rxBytes: 0`
	`rxOverflow: 0`
	`txPackets: 0`
	`txBytes: 0`
	`[...]`

Table 3: Known Issues *(continued)*

PR	Description

590812	The following log messages appear periodically in lkmStart log entries:
	
	`[WARN]:STARTING /usr/idp/device/bin/lkmStart.sh recover`
	`[WARN]:STARTING /usr/idp/device/bin/lkmStart.sh recover`
	
	The following unexpected log messages appear in idpHMD log entries:
	
	`[Error] DVRdriveStatus failed`
	`[Error] DVRdriveStatus failed`
	
	Please ignore these log messages. They are not related to the true state of the system or system events.

719478	We have observed a problem with flow bypass logs and counters. The problem occurs only when debug logging is enabled, logs are being generated at a high rate, and the test traffic load fluctuates above and below the flow bypass threshold. In these conditions, the log rate is so rapid that the IDP OS drops logs for some events. It can be confusing if the IDP OS log record is missing a flow bypass triggered or flow bypass reset message. We acknowledge the problem.
CPU Utilization	
434539	In the NSM Device Monitor > View Device Details > Process Status tab, the CPU utilization 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. For single core platforms, the CPU utilization reported to SNMP is based on the results of the **top** command. For mulitcore platforms, the CPU utilization reported to SNMP is based on the results of the **scio idp-cpu-utilization** command.
603547	Counterintuitive behavior—In an HA deployment, the IDP Series device in the inactive path shows occasional spikes in CPU utilization eventhough it is not processing packets. This is expected. The CPU usage is related to state synch operations between the active device and the passive device.
Stability	
430363	IDP8200 stops processing traffic at high load with SYN protection enabled.
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.
573031	Low memory triggered JNET bypass on IDP800.
593999	PKID crash related to SSL inspection (forward proxy) in a stress-test environment.
594004	In a stress-test environment, we observed a condition where SSL forward-proxy processing results in a crash with coredump.
601870	In an IDP8200 stress test, we observed an IDP engine hang related to TSIG processing and subsequent spike in CPU utilization.
604848	In an IDP8200 stress test, we observed a crash with core at sc_icache_instance.

Table 3: Known Issues *(continued)*

PR	Description
Detection Accuracy	
279408	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). To work around this issue: 1. In the NSM Device Manager, double-click the name of the device to display the configuration editor. 2. Click **Sensor Settings**. 3. Click the **Run-time parameters** tab. 4. Under Traffic Signatures, increase the value for **Byte threshold for suspicious flows**.
508363	False positive where SSL:Audit:Non-SSL is wrongly detected in HTTPS traffic. The issue only occurs when SSL:Audit:Non-SSL is included in a compound signature with another member having stream256 context.
Shutdown Operation	
432893	The **shutdown -h now** command might not behave as expected if you deploy IDP8200 with any of the following fiber I/O modules: IDP-1GE-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.
Unsupported Functionality	
572045	When you encounter a hung system, you might want to force a core dump. To do this, you type a SysRq key combination. You can use the SysRq key combination on IDP8200, IDP800, IDP250, and IDP75. This PR has been filed to support the SysRq key combination core dump method for IDP1100, IDP600, and IDP200.
Expected Behavior	
547354	Packet drops are possible in simulation mode if the JNET free packet buffer is 0.
High Availability	
550567	Synchronization from primary device to backup device includes updates to the application identification matches for predefined signatures (the appsig cache). Updates do not include cached entries for custom applications or extended applications (the extappsig cache).
558837	Due to a hardware limitation, interface signaling is not supported for IDP8200 10 Gb fiber interfaces.
559087	We do not support attack detection (flow-based or packet-based) in synced sessions processed by the standby device after retransmission on the redundant path. Packets for these sessions are passed through, uninspected. New sessions traversing the redundant path are inspected.

Table 3: Known Issues *(continued)*

PR	Description

720406	In a test lab environment, we have observed conditions in which the JNET driver free packet buffer count does not recover from zero availability. Depletion of the free pack buffer results in failover to the secondary device. After failover, the secondary device free packet buffer is depleted, resulting in bypass. The behavior is not consistently reproducible.
	
	If you observe this behavior, you can take either one of the following actions to restore the IDP Series devices to health:
	
	• On the primary and the secondary device, reset the HA interface using the following commands:
	`[root@defaulthost ~]# ifconfig down`
	`[root@defaulthost ~]# ifconfig up`
	• On the primary and the secondary device, turn off the interface pause parameters for the HA interface using the following commands:
	`[root@defaulthost ~]# ethtool -A eth1 autoneg off`
	`[root@defaulthost ~]# ethtool -A eth1rx off`
	`[root@defaulthost ~]# ethtool -A eth1tx off`
	`[root@defaulthost ~]# ethtool -a eth1`
	`Pause parameters for eth1:`
	`Autonegotiate: off`
	`RX: off`
	`TX: off`

Documentation	
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 "IDP Logs and Reports in NSM Task Summary" section in the *IDP Series Administration Guide*.

Documentation

You can download user documentation from the Juniper Networks Web site: http://www.juniper.net/techpubs/. The user documentation on the IDP OS 5.1 site applies to IDP OS 5.1r3. Table 4 on page 21 lists the user documentation related to the IDP Series appliance.

Table 4: Related IDP Series Documentation

Document	Description
Juniper Networks Security Intelligence Center Attack Signatures	Lists predefined attack signatures developed by the Juniper Networks Security Intelligence Center.
Juniper Networks Security Intelligence Center Application Signatures	Lists predefined application signatures developed by the Juniper Networks Security Intelligence Center.
IDP Detector Engine release notes	Provides information about IDP Detector Engine releases, including new features, changed features, fixed problems, and known issues.
IDP Series installation guides	Describes IDP Series hardware and provides instructions for installing, configuring, updating, and servicing the device.

Table 4: Related IDP Series Documentation *(continued)*

Document	Description
IDP Series Feature Documentation	A collection of topics from the *IDP Series Administration Guide* and *IDP Series Concepts and Examples Guide*, in HTML.
IDP Series Administration Guide	Provides procedures for completing IDP Series administration tasks with the Network and Security Manager (NSM) central management program; with the IDP Series device Appliance Configuration Manager (ACM); and with the IDP Series device command-line interface (CLI).
IDP Series Concepts and Examples Guide	Explains IDP Series features and provides examples of how to use the system.
IDP Series Custom Attack Objects Reference and Examples Guide	Provides examples and reference information for creating custom attack objects.
IDP Reporter User's Guide	Describes how to use IDP Reporter, an on-box reporting platform that includes predefined reports on attack detection and application usage. You can also use IDP Reporter to schedule regular publication of reports that are of interest to you or your stakeholders.

Table 4 on page 21 lists related NSM documentation.

Table 5: 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.
Network and Security Manager Installation Guide	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.
Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide	Describes how to configure and manage IDP Series 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 Series devices.
Network and Security Manager Administration Guide	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. 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.

Table 5: Related NSM Documentation *(continued)*

Document	Description
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) or telephone (1-888-314-JTAC within the United States or 1-408-745-9500 from outside the United States).