

IDP Detector Engine Release Notes

Part Number: 530-029025-01
Revision January 15, 2009

Contents

Recent Release History	2
IDP Detector Engine Overview	3
Understanding IDP Detector Engine Version Numbers	3
Displaying the IDP Detector Engine Version Number (NSM Procedure)	4
Displaying the IDP Detector Engine Version Number (CLI Procedure)	4
Updating the IDP Detector Engine	5
Troubleshooting an IDP Detector Engine Update	5
Reverting the IDP Detector Engine Version	6
New Features and Resolved Issues	6
Known Issues	9
Contacting Juniper Networks Technical Assistance Center (JTAC)	9

Recent Release History

The following table summarizes the features and resolved issues in recent releases. You can use this table to help you decide to update the IDP detector engine version in your deployment.

Table 1: IDP Detector Engine Features and Resolved Issues by Release

Release Date	Detector Engine Version	Features and Resolved Issues
January 15, 2009	<ul style="list-style-type: none"> ■ 4.1.110090107 ■ 4.0.110090107 ■ 3.4.121591 ■ 3.1.121592 	<p>Major update, including:</p> <ul style="list-style-type: none"> ■ A new decoder for the MODBUS serial communications protocol. ■ Resolution of issues with DNS, H.225 SGN, LDAP, MS-SQL, SIP, SMB, and TNS decoders. ■ Increased security coverage with new anomalies. ■ Improved accuracy with new contexts and other changes to reduce false positives. <p>For details, see “New Features and Resolved Issues” on page 6.</p>
January 5, 2009	<ul style="list-style-type: none"> ■ 3.4.118904 ■ 3.1.118905 	<p>Provides the following new features and fixes:</p> <ul style="list-style-type: none"> ■ 397759, 397759-2. Resolved an issue in the DNS decoder that could result in a security module crash. ■ 400464, 400467. Improved the SMB decoder with new features and anomalies. ■ 400468, 400469. Resolved an issue in the SMB decoder. It now generates UUID context.
December 31, 2008	<ul style="list-style-type: none"> ■ 4.1.110081106 ■ 4.0.110081106 	Improves coverage and accuracy for the SIP, SMB, DNS, MS-SQL, and HTTP protocols.
October 23, 2008	<ul style="list-style-type: none"> ■ 4.1.110081008 ■ 4.0.110081008 ■ 3.4.117413 ■ 3.1.117412 	Improves coverage and accuracy for LDAP, SSL, and HTTP protocols.
September 18, 2008	<ul style="list-style-type: none"> ■ 4.1.110080916 	Improves coverage and accuracy for SSI and SIP protocols.
August 21, 2008	<ul style="list-style-type: none"> ■ 3.4.114929 ■ 3.1.115140 	Improves coverage and accuracy for the VOIP/SIP protocol.
July 22, 2008	<ul style="list-style-type: none"> ■ 4.1.110080701 ■ 4.0.110080701 	Improves coverage and accuracy for SMTP, SIP, and H.225 protocols.
July 17, 2008	<ul style="list-style-type: none"> ■ 4.1.110080700 ■ 4.0.110080700 	Improves coverage and accuracy for HTTP, LDAP, and SMB protocols.
June 19, 2008	<ul style="list-style-type: none"> ■ 4.1.110080600 ■ 4.0.110080600 	Improves coverage and accuracy for SIP, HTTP, and MSSQL protocols.

Table 1: IDP Detector Engine Features and Resolved Issues by Release *(continued)*

Release Date	Detector Engine Version	Features and Resolved Issues
June 10, 2008	■ 3.4.112183	Improves coverage and accuracy for SIP and HTTP protocols.

IDP Detector Engine Overview

The IDP detector engine is a dynamic protocol decoder that includes support for decoding more than 60 protocols and more than 500 service contexts. The IDP detector engine is used by the IDP process engine in packet analysis.

The detector engine code base is packaged and released separately from the IDP or ScreenOS operating system and software code base. Juniper Networks Security Center (J-Security Center) releases IDP detector engine updates more frequently in order to ensure IDP products protect your network against recently discovered vulnerabilities.



NOTE: We recommend you subscribe to the IDP Signature Updates technical bulletin to be notified when J-Security Center releases IDP detector engine updates. Go to <https://www.juniper.net/alerts/>.

Understanding IDP Detector Engine Version Numbers

The IDP detector engine versions that are compatible with your system vary by product line and operating system version. The following table summarizes IDP detector engine version compatibility.

Table 2: IDP Detector Engine Version Compatibility

Hardware	Operating System	IDP Detector Engine Version
IDP 8200	IDP 4.2.x	4.2.xxxxx
IDP 75/250/800, IDP 50/200/600/1100, IDP 10/100/500/1000	IDP 4.1.x	4.1.xxxxx
IDP 50/200/600/1100, IDP 10/100/500/1000	IDP 4.0.x	4.0.xxxxx
ISG 1000/2000	ScreenOS 6.2.x	3.5.xxxxx
ISG 1000/2000	ScreenOS 6.0.x	3.4.xxxxx
ISG 1000/2000	ScreenOS 5.4.x, 5.0.x	3.1.xxxxx

Displaying the IDP Detector Engine Version Number (NSM Procedure)

To view the version of the latest IDP detector engine that has been downloaded to the NSM GUI server:

- In NSM, select **Tools > View/Update NSM Attack Database** and click **Next**.

The wizard displays the IDP detector engine version that has been downloaded to the NSM GUI server.

To view version information for the IDP detector engine installed on an IDP device:

- In the NSM device manager, double-click the IDP or ISG device to display the device configuration editor.

For standalone IDP devices, the Info node displays version information, including the IDP detector engine version.

For ISG devices, navigate to **Security > SM Settings** to display the IDP detector engine version.

Displaying the IDP Detector Engine Version Number (CLI Procedure)

To display the IDP detector engine version number on an IDP device:

1. Connect to the CLI as the user **admin** and switch to the user **root**.
2. Run the **scio getsystem** command as shown in the following example:

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Dec 17 10:23:16 2008 from 172.23.8.84
[admin@default host admin]$ su root
Password:
[root@default host admin]# scio getsystem
Product Name: NS-IDP-600C
Serial Number: 0147032005000002
Software Version: 4.1.115771
IDP Mode: transparent
HA Mode: Disabled
Detector Version: 4.1.104259
Software License: Evaluation
Software Expiration Date: 4/25/2009
[root@default host admin]# [root@default host admin]#
```

To display the IDP detector engine version number on an ISG device:

1. Connect to the CLI as the user **admin** and switch to the user **root**.
2. Run the **get system** command as shown in the following example:

```
[root@default host admin]# get system
```

```
[..]
IDP files version:

detector.so 3.1.101390

[root@default host admin]# [root@default host admin]#
```

The line for detector.so shows the version of the detector—in this example, version 3.1.101390.

Updating the IDP Detector Engine

Updating the IDP detector engine is a three part process.

To update IDP detector engine:

1. Download IDP detector engine and NSM attack database updates to the NSM GUI server:

In NSM, select **Tools > View/Update NSM attack database** and complete the wizard steps.

2. Push the updated IDP detector engine to IDP devices:

In NSM, select **Devices > IDP Detector Engine > Load IDP Detector Engine** and complete the wizard steps.



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

3. Run a security policy update job to initialize the IDP detector engine update:
 - 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**.

Troubleshooting an IDP Detector Engine Update

The default URL from which to obtain updates is <https://services.netscreen.com/restricted/sigupdates/nsm-updates/NSM-SecurityUpdateInfo.dat>. If you encounter connection errors, ensure this setting has not been inadvertently changed.

To restore the default URL:

1. Select **Tools > Preferences**.
2. Click **Attack Object**.
3. Click **Restore Defaults**.

NSM restores the URL in the **Download URL for ScreenOS Devices** text box.

4. Click **OK**.

Reverting the IDP Detector Engine Version

In most cases, your use of IDP will not benefit from reverting the IDP detector engine version. In some cases, however, you might be required to revert. If you encounter an issue and need to revert, contact Juniper Networks Technical Assistance Center (JTAC).

New Features and Resolved Issues

The following table lists new features and resolved issues included in this release.

Table 3: New Features and Resolved issues

Category	Features and Resolved Issue
New features	269559, 403143. Added a new protocol decoder for the MODBUS serial communications protocol.
	274654. Added a new anomaly LDAP_CONTROLS_MISMATCH to support detection of Microsoft vulnerability MS08-003 CVE-2008-0088.
	290741. Added new MS-SQL contexts: mssql-login-server, mssql-login-language, mssql-login-database, mssql-rpc-name, mssql-query, mssql-login, mssql-rpc, mssql-cancel, mssql-0x12.
	295716. Added a feature to count established RTP/SIP sessions. scio counter get flow has a new counter sc_flow_gate_add to show this value.
	300565. Added an anomaly to replace signature SMTP_MICROSOFT_EXCHANGE_MALFORMED_MIME_ATTACHMENT for performance reasons.
	305008. Added a new anomaly DNS_TRANSPOOFF. Detects attempts to exploit a known vulnerability against most DNS servers. Attackers can spoof DNS replies by sending multiple crafted packets to DNS servers. A successful attack can result in redirected traffic to unintended locations. There is a related threshold to this attack - sc_dns_mismatch_rate.
	309099. Added anomalies: URL-THRESHOLD-256, URL-THRESHOLD-512, URL-THRESHOLD-1024, URL-THRESHOLD-2048, URL-THRESHOLD-4096, URL-THRESHOLD-8192.
	398505. Added new SMB decoder anomalies: DUPLICATE_SESSION and REFLECTION.
Changes to defaults	414182. Added new anomalies to detect unrecognized encrypted traffic with respective level of confidence: ENCRYPTED_TRAFFIC_1, ENCRYPTED_TRAFFIC_2, ENCRYPTED_TRAFFIC_3.
	301844. Removed the default association of port TCP/88 to HTTP. The service is now detected by AI.

Table 3: New Features and Resolved issues *(continued)*

Category	Features and Resolved Issue
Stability improvements	258702. Fixed a crash in the TNS decoder flow initiation function.
	275506. Fixed a crash in the SMB decoder.
	276555. Fixed a crash in the DNS decoder due to malformed DNS traffic.
	281617, 281618. Fixed a crash in URL parsing.
	289399, 291850, 308357. Fixed a problem with the SIP decoder that had caused a crash under stress.
	302871. Fixed a crash that could occur in H.225 SGN flow initiation.
	389022. Fixed a memory leak issue with the LDAP decoder.
	402026. Fixed a crash in the MS-SQL decoder that could occur on session teardown.
	403225. Fixed a crash in the DNS decoder due to buffer overrun in RR - Resource Record.

Table 3: New Features and Resolved issues (continued)

Category	Features and Resolved Issue
Improved Accuracy	222543. Fixed a false positive with anomaly HTTP_REQERR_REG-INVALID-FORMAT that was not recognizing "-" as a valid character.
	259621. Fixed a false positive anomaly with SMTP_AUDIT_TEXT-LINE. The anomaly used to get triggered after line reconstruction with an exceeded allowed size. Now it is triggered only prior to normalization of header line continuation.
	263943. Fixed a false positive with anomaly WHOIS_INVALID_EO due to a changed common practice.
	270992. Fixed a false positive with anomaly SIP_SECURITY_PARAMETER_ERROR that was triggered wrongly by treating the space characters in headers as separators.
	272372. Fixed a false positive with anomaly SIP_URI_ERROR that was triggered wrongly by treating the space characters in URI's display-name as separators.
	276481. Fixed a false positive with anomaly HTTP_REQERR_REQ_LONG_UTF8CODE that was triggered when parsing the parameter portion of the URL
	280021. Fixed a false positive with anomaly SMB_SECUR_TOKEN_OVERFLOW.
	286628, 297066. Fixed a false positive with anomaly LDAP_FORMAT_ENC_INCORRECT_TAG. We had treated an optional tag as mandatory.
	286831. Fixed a false positive with anomaly SMTP_AUDIT_INVALID-FILENAME. Binary data (BDAT) had been parsed the same way as SMTP headers.
	287692. Fixed a false positive with anomaly SMTP_TEXT_LINE. The anomaly used to get triggered after line reconstruction with an exceeded allowed size. Now it is triggered only prior to normalization of header line continuation.
	294633. Fixed a false positive with anomaly HTTP_INVALID_MISSING_REQ that was triggered on legitimate HTTP CONNECT messages.
	297842. Fixed a false positive anomaly in LDAP_DISTINGUISHED_FORMAT_ERROR.
	299858. Fixed a false negative with anomaly SMB_GRIND. The detector now accounts for more-processing-required status code in SMB command response sc_smb_session_setup_andx.
	302449, 404359. Fixed a false positive with anomaly SIP: Unknown Request Method.
313686. Fixed a false negative with anomaly HTTP_VERSION. Had not properly checked for minor version.	
387759. Fixed a false positive with HTTP when error code 400 responses are interleaved with error code 200.	
388005. Fixed a false positive with anomaly HTTP_CONTENT_OVERFLOW.	

Known Issues

The following table identifies known issues in this release.

Table 4: Known Issues

Detector Engine Version	Issue
■ 4.1.xxxxx	310511, 313472. In SSL decrypted traffic, some attacks are not detected. The root cause of this problem appears to be an insufficient SSL buffer size.
■ 4.0.xxxxx	

Contacting Juniper Networks Technical Assistance Center (JTAC)

If you need additional information or assistance, contact 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).

Copyright © 2009, 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. JUNOS 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.