Part No. 320740-A
Septmber 2005

Phone 1-800-4Nortel
http://www.nortel.com

Release Notes for Nortel Threat Protection System 4.1

* 3 2 0 7 4 0 - A *

NORTEL

Nortel reserves the right to change any products described herein at any time, and without notice. Nortel assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Nortel. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Nortel.

Originated in the U.S.A.

Contents

Introduction

This document contains the latest information about the Nortel Threat Protection System (TPS) release 4.1. The Nortel Threat Protection System is a fully integrated intrusion detection system that consists of the following:

- TPS 2070 Defense Center, which manages intrusion sensors in the network environment
- TPS 2050 Intrusion Sensor and TPS 2070 Intrusion Sensor, which detect and track network intrusions, either independently or under the management of the TPS 2070 Defense Center
- TPS 2150 Intrusion Sensor and TPS 2170 Intrusion Sensor, which have fail-open functionality in inline mode

NOTE – The latest information about Real-time Threat Intelligence is contained in *Real-time Threat Intelligence Sensors 3.1 Release Notes*, part number 320741-A, and *Real-time Threat Intelligence Software for TPS Intrusion Sensors 3.1 Release Notes*, part number 320742-A.

Features and functionality – TPS 2070 Defense Center

The TPS 2070 Defense Center contains the following features and functionality in release 4.1:

- New Policy and Response Remediation — Administrators can configure the Policy and Response feature to pass specific event information to a third-party product by way of an Application Programming Interface (API). This data can be processed by a customer-configured script and can carry changes to, for example, network infrastructure.
- Pre-built Remediation Modules — The Remediation API contains pre-built Nortel Application Switch (NAS), OPSEC and Cisco PIX and router modules accessible through the graphical user interface (GUI).

NOTE – The TPS Remediation Module for Nortel Application Switch plug-in software files are available online at www.nortel.com/support. To locate the files do the following: from the pull-down list next to selection 1, Select from, select **Product Categories.** Scroll to Security & VPN in the Product Categories list box. Select **Threat Protection** from the list**.** From selection 2, ... choose a product ..., select the applicable product. From selection 3, ... and get the content., select Software**.** Click **Go**. The product software page opens. The module for Nortel Application Switch running 21.x or 22.x code allows the blocking of source IP addresses but no timeout period. The module for Nortel Application Switches running 23.x or higher allows a timeout period to be set.

- Inline configuration with packet blocking (IPS Mode) — Intrusion Sensors can be deployed in inline mode. Inline mode provides the sensors with the ability to drop traffic or replace malicious content with a benign substitute when a particular rule is fired. Inline mode does not preclude sensors from monitoring events in the traditional passive mode.
- Real-time Threat Intelligence (RTI) License Pooling — When a Defense Center is used to manage RTI Sensors, the host licensing is enforced at the Defense Center, rather than on the individual sensors. Any number of RTI Sensors, including RTI on Intrusion Sensors, share a common pool of host licenses.

NOTE – For maximum performance, Nortel* strongly recommends that RTI Feature Host Licenses are applied on the TPS 2070 Defense Center and that RTI Sensors are managed from the TPS 2070 DC. Once the base RTI sensors are activated, an RTI Feature Host key-code must be applied to the TPS 2070 DC designated to monitor the network. When you purchase an RTI Feature Host license, a certificate containing an authorization serial number, instructions, and an e-mail address used to obtain an RTI Feature Host license key-code is issued. For more information, see the *Nortel TPS Real-time Threat Intelligence Sensor Installation Guide*, part number 320738-A. The e-mail address used to obtain RTI Feature Host keys differs from the e-mail address referenced in the software. Requests for RTI Host keys sent to keyrequest@nortel.com are not processed. Refer to the RTI Feature Host License certificate for the correct e-mail address used to obtain RTI host license keycodes.

- TPS/RTI Event Linked Views — Users can toggle between RTI and intrusion event view, with the same constraints carried through, by clicking a single button. For example, users can analyze a specific intrusion event in the context of the RTI flow data recorded concurrently.
- Defense Center Auditing — Audit data is accessible through a table view of events. Events, including the addition or deletion of user accounts, are also recorded in the audit log. Administrators can see which users visited specific pages and when.
- High Availability for RTI — Similar to Intrusion Sensors, RTI Sensors can forward events to both a primary and a secondary Defense Center.

- Portscan Enhancement — Intrusion Sensors can now detect a variety of portscan techniques including portscans, portsweeps, decoy portscans, and distributed portscans. Administrators can control sensitivity with Low, Medium, and High settings. Protocols that can be analyzed include TCP, UDP, ICMP, and IP.
- Host Criticality Setting — Administrators can attribute one or more hosts with a criticality setting of Low, Medium, or High. This setting can be leveraged in compliance policies and custom workflows. For example, particular servers in a specific location may be considered critical. Consequently, administrators may want to be able to trigger special responses, or construct reports, so that designated servers have the highest priority.
- Vulnerability Review — Administrators can review the vulnerabilities associated with one or more hosts and can validate or invalidate the vulnerabilities. For example, if a server is patched to a certain level, and the administrator determines that a number of vulnerabilities associated with that platform are not present, the administrator can remove the vulnerabilities from the list that is processed when determining the Impact Flag rating for a given event. The result is a more accurate correlation of events between the Intrusion Sensor and RTI.
- RTI Supported on Intrusion Sensors — RTI software can be installed on the TPS 2x50 IS and the TPS 2x70 IS Intrusion Sensors operating in passive mode. RTI cannot be installed on Intrusion Sensors operating in inline mode. Users wishing to run RTI on TPS Intrusion Sensors must install the RTI software for TPS sensors, available for download at www.nortel.com/support. For installation information and performance considerations, refer to the *Nortel RTI Software for TPS Sensors Configuration Guide*, Part number 320758-A.
- Ability to Delete Hosts — To allow efficient use of RTI licensing and provide users an uncluttered view of specific hosts, administrators can remove hosts from the RTI network map.
- Ability to Temporarily Delete Services — To reduce non-relevant vulnerabilities from the host, users can delete services from host profiles for invalid or disabled services.
- Addition of the “From Beginning” option to the byte_jump content keyword — This allows creation of an intrusion rule that skips a calculated number of bytes from the beginning of the packet payload instead of skipping bytes from the end of the calculated byte segment.
- Addition of the “Multiplier” option to the byte_jump content keyword — This allows creation of an intrusion rule that, after calculating the number of bytes to skip, multiplies the initial calculated number of bytes by the integer specified as the argument to the Multiplier option, and then skips forward the final calculated number of bytes in the packet.

- A modified default setting — This modification allows for a greater number of rules that use the flowbits option.
- Addition of a new IP defragmentation preprocessor — A new IP defragmentation preprocessor, frag3, has been added to Snort. Frag3 replaces Frag2.
- Inclusion of a replacement database — A replacement database that improves the stability and performance of the Defense Center is included in version 4.1.
- Replacement of rule updates by Snort Engine Updates (SEUs) — SEUs replace rule updates as the mechanism for updating Snort-based rules. SEUs also provide new and updated methods, including preprocessors and protocol decoders, to aid in detecting intrusion attempts. Ensure that your SEU installation process complies with your network and security policies because SEUs can contain new binaries. If Scheduled Tasks were previously used to upload and install rule packs, create new tasks for uploading and installing SEUs in version 4.1.
- Addition of Shared Object Rules (SORs) — SORs allow the Nortel Threat Protection System Team more flexibility in creating new rules. SORs are delivered in SEUs, in binary format. Text rules, now called Standard Text Rules (STRs) were provided in previous rule packs. SOR rule documentation can be viewed and copied the same way as STRs. However, you cannot view or modify the rule keywords section, including rule content keywords. Only attributes, such as the message, the source and destination ports, and addresses in the rule header can be viewed and modified. STRs can be created and modified as in previous versions and any of the legacy STRs can be viewed, copied, and modified.
- Stream Reassembly performance improvements — The server_inspect_limit option has been added to the stream reassembly preprocessor. This improves Intrusion Sensor performance by limiting inspection of server-side traffic. When the detection engine inspects a specified amount of server-side traffic it suppresses inspection of additional traffic until a client-side packet is detected. When a client-side packet is detected, the detection engine resumes inspection of server-side traffic until it again reaches the specified limit. To use the server-inspect-limit option, edit your user.conf file to include the following line:

  ```
  preprocessor stream4_external: server_inspect_limit number_of_bytes
  ```

  where number_of_bytes is the server-side traffic limit.

NOTE – The flow depth parameter of the HTTP inspection decoder overrides the server_inspect_limit option when inspecting HTTP traffic.

Compatibility

Product compatibility matrix

Table 1 indicates which version of Intrusion Sensors and RTI Sensors are compatible with each version of the Defense Center.

Table 1 Compatibility Matrix

DC Version	IS Versions	RTI Versions
4.1	4.1	3.1
3.2	3.2	n/a

Hardware installation

Refer to the appropriate installation guides for complete instructions on the installation of the TPS 2070 Defense Center, TPS 2050 Intrusion Sensor, TPS 2070 Intrusion Sensor, TPS 2150 Intrusion Sensor, or the TPS 2170 Intrusion Sensor. This documentation is provided on the product Documentation and Restore CD and can also be accessed on the Nortel Technical Support web site at www.nortel.com/support.

General software information

The TPS 2070 Defense Center, TPS 2050 Intrusion Sensor, TPS 2070 Intrusion Sensor, TPS 2150 Intrusion Sensor, and TPS 2170 Intrusion Sensor products are pre-loaded with version 4.1 of the software. The software is available on a CD-ROM that is shipped with the hardware and is also available on the Nortel web site, for contracted customers.

The software file names for release 4.1 are as follows:

- Nortel_TPS_Defense_Center_2070_v4.1.0-78-Restore.iso (TPS 2070 Defense Center)
- Nortel_TPS_Intrusion_Sensor-2050-v4.1.0-78-Restore.iso (TPS 2050 Intrusion Sensor)
- Nortel_TPS_Intrusion_Sensor-2150-v4.1.0-78-Restore.iso (TPS 2150 Intrusion Sensor)
- Nortel_TPS_Intrusion_Sensor-2070-v4.1.0-78-Restore.iso (TPS 2070 Intrusion Sensor)

- Nortel_TPS_Intrusion_Sensor-2170-v4.1.0-78-Restore.iso (TPS 2170 Intrusion Sensor)

The software file names for upgrade from version 3.2.0.3 to version 4.1 are as follows:

- Nortel_TPS_Defense_Center_Upgrade_3.2_to_4.1.0_Upgrade.sh
- Nortel_TPS_Intrusion_Sensor_Upgrade_3.2_to_4.1.0_Upgrade.sh

NOTE – Upgrade software files are available, for contracted customers, on the Nortel web site. Customers operating a system with version 3.2 installed must upgrade to the 3.2.0.3 patch prior to upgrading to version 4.1.

The TPS Remediation Module for Application Switch software file names are as follows:

- nas_21_22_rem_1.0.tgz for the Nortel Application Switch 21.0 and 22.0 version 1.0
- nas_23_rem_1.0.tgz for the Nortel Application Switch 23.0 version 1.0

Updating software

Updates for the Defense Center and Intrusion Sensor software are distributed electronically and can be downloaded from the hardware web interface for contracted customers only. Refer to the Defense Center and Intrusion Sensor User Guides for complete instructions on performing this task.. The titles and part numbers of the user guides are as follows:

- TPS 2070 Defense Center *User's Guide* (Part Number 216886-C)
- TPS 2050 IS/TPS 2150 IS *and* TPS 2070 IS/TPS 2170 IS Intrusion Sensor *User's Guide* (Part Number 216884-C)

Updating intrusion rule packs and SEUs

New intrusion rule packs and SEUs are occasionally made available to update those already in place. When new rule packs and SEUs are available, they can be downloaded from the Nortel web site under the Threat Protection System product family. This service is provided only to customers with valid service contracts.

Upgrading existing Defense Centers

To install a new Defense Center version 4.1 appliance, follow the instructions provided in the *Nortel TPS Intrusion Sensor and Defense Center Installation Guide*, Part Number 320737-A. The installation guide is available on the Defense Center Documentation and Restore CD and on the Nortel Technical Support site at www.nortel.com/support.

Prerequisites for upgrading an existing Defense Center

Defense Center version 3.2.0.3 is required to complete a successful upgrade to version 4.1. Version 3.2.0.3 is available for download from the Nortel web site.

At least 40 Mb of free space is required on the root partition (/), and 78 Mb of free space is required on the /var partition.

Notes on the upgrade process

This section contains important information about upgrading Nortel products. Read the entire section before starting any upgrades.

NOTE – The upgrade process migrates all event and configuration data to a replacement database.

Before you begin the upgrade

- Plan the upgrade for a time when it has the least impact on your deployment because the Defense Center reboots after upgrade.
- Nortel recommends that you back up event and configuration data to a local computer.
- Delete any user-created files from /root before starting the upgrade.
- From the Nortel support site at www.nortel.com/support, obtain the upgrade software file called Nortel_TPS_Defense_Center_Upgrade_3.2_to_4.1.0_Upgrade.sh.

Upgrade

- Upgrade all Defense Centers before upgrading the sensors managed by the Defense Centers.
- Do not perform any administrative or analysis tasks during the upgrade process.
- For Defense Centers managing Intrusion Sensors, check the sensor management page and confirm that each sensor uses a policy that the Defense Center can identify. Any policy listed as unknown must be replaced with a policy pushed from the Defense Center to the sensor before either appliance is upgraded.
- After completion of the Defense Center upgrade, use the scheduling feature to schedule the upgrade push and installation on managed sensors. For information about the scheduling feature, see the *Nortel TPS Defense Center User Guide*, Part Number 216886-C.

- If a managed sensor upgrade process fails, it automatically restarts when using a Defense Center to push and install the upgrade. To cancel the upgrade process, click the **Cancel** button on the Task Queue page.
- To determine whether the upgrade installation is successful, view the Sensor Management page. If the version number of the sensor changes, the remote installation succeeded. Upgrade automatically reboots the sensors at the end of the upgrade process, and the Task Queue page may display a Remote Install Failed message, even in the case of a successful installation.
- If the upgrade halts for any reason, it can be restarted at the point where it stopped because the upgrade tracks its own progress. For example, in the event of a power failure during upgrade, the installation process can be restarted using the GUI. If the upgrade proceeded past the point where the GUI is accessible, edit the /etc/sf/ims.conf file and modify the SWVERSION to match the version being upgraded. For Defense Centers, this is version 3.2.0.3. However, if an upgrade halts for any reason, Nortel recommends that you contact Nortel Technical Support.
- The upgrade has a Revert feature that permits restoration of an upgraded appliance to the previously installed software version. Before using the Revert feature, the Revert process checks to ensure that there is enough free space on the hard drive to complete the task. At least 50% of the size of the event and upgrade data is required. To revert to the previous software version, log into the Defense Center using secure shell (ssh) with the root account and type **`revert`** at the command prompt. Press **Enter**. Intrusion events in the database are not retained and RTI events generated between the upgrade and reversion are not retained. Nortel recommends that you back up all event and configuration data on a local computer before performing Revert on a Defense Center and restore events from the backup file after the reversion is complete.
- Intrusion events on the clipboard, or marked as reviewed, are lost when the appliance is rebooted at the end of the upgrade procedure.
- The upgrade can take several hours, depending on the number of events on the appliance, particularly on Defense Centers and the TPS 2070 IS sensor. Refresh the browser to check the status of the upgrade. When the upgrade is complete, a prompt appears instructing the user to log into the appliance.
- When the upgrade is installed and the Defense Center is running, the new database starts to populate with old events. The population time can vary from 20 minutes, for 1 million intrusion events, to four hours for 10 million events, to 14 hours for 110 million events. Packet data is migrated after event data. You are unable to view packets associated with events until the migration is complete.

- E-mail alerting must be reconfigured after the upgrade is complete because settings for e-mail alerting on intrusion rules are not preserved as part of the upgrade. This applies to Defense Centers that manage Intrusion Sensors and Defense Centers.
- Policy violation events generated on a version 3.2 secondary Defense Center, configured with custom compliance policies and rules, are identified by a number in the policy and rule columns, rather than a name, when both Defense Centers in a high availability pair are upgraded. All events generated after the upgrade will have the correct policy name and rule name.
- The version number on the login page is not updated after the Upgrade. To confirm that the new version is installed, select **Help**. Then select **About** and review the value in the Software Version field.

Upgrade warnings

- During an installation, if the update page is refreshed, HTML code may appear. The HTML code disappears when the update is fully installed. Do not interact with the GUI until the Defense Center completes the upgrade process. (17563 and 18373)
- The pages load slowly. (17567)
- Allow the Defense Center to reboot on its own. If the Defense Center is rebooted before upgrade completion, the upgrade can fail. (19249)

Upgrading a Defense Center from version 3.2.0.3 to version 4.1

Use the following procedure to upgrade a Defense Center from version 3.2.0.3 to version 4.1.

1.Download the Defense Center 4.1 upgrade script.

2. Open the **Defense Center Administration** menu and select the following:

   □ Update

   □ View

3. Click **Browse**. Navigate to the location where the upgrade script is saved.

4. Select the upgrade script.

5. Click **Open**. The update appears in the Upload and Update Package field.

6. Click **Upload**. The 4.1 upgrade appears in the Install update section of the page.

7. Select the button next to the upgrade.

8. Click **Install**. A message appears stating that the appliance will reboot automatically after the upgrade is installed.

9. Click **OK** to continue.

NOTE – If the upgrade halts, Nortel recommends that you do not restart it. Contact Nortel Technical Support.

Confirming new software version

To confirm the new software version after the upgrade is installed and the appliance is rebooted, do the following:

1.Refresh the browser.

2. Select **Help**.

3. Select **About** to view and confirm the software version.

NOTE – Depending on the number of old intrusion events to be migrated into the update, it may take between 20 minutes and 14 hours for old intrusion events to appear on event views and in event statistics.

Restoring a Defense Center

Nortel provides a CD-ROM for restoring a TPS appliance to it original factory settings.

NOTE – Restoring a TPS appliance using the CD-ROM results in the loss of all configuration and event data on the appliance. Nortel recommends that you back up the application before using the Restore CD-ROM. The process retains the license file and network settings but you may need to re-enter the original license file after the Restore process completes.

A keyboard and VGA monitor must be used, rather than the serial port, when restoring the TPS software for the TPS 2070 DC platform to its original state.

Turn off the power to the TPS appliance before connecting the keyboard and monitor. Connect the keyboard and monitor. Turn on the power to the appliance and start it from the Software CD using the Restore procedure, see Step 1 of the following procedure. Follow the instructions on the monitor. When the software has been restored, see Step 4, turn off power to the appliance and disconnect the keyboard and monitor. Continue with Step 5 of the procedure.

To restore a TPS appliance to its original factory settings, use the following procedure:

1. Place the Restore CD-ROM in the CD tray and perform a safe reboot of the appliance. After the appliance reboots, you are prompted to restore the system.
2. At the prompt, type **Yes**.
3. Press **Enter**.
4. At the prompt, confirm that you want to restore the appliance. After the system is restored, the appliance ejects the CD-ROM and reboots.
5. Connect the appliance and restore power.
6. If the Add Feature License page appears, paste the original license file into the License field.
7. Click **Submit License**.

Defense Center resolved issues in version 4.1

- User-defined variables that begin with the same string no longer conflict with default intrusion policies. Any user-defined variable can be safely deleted without causing errors. (7976)
- The documentation correctly states that the clipboard can hold up to 25,000 events. (11021)
- Compliance policies no longer require reactivation after response groups are modified. (12885 and 16165)
- Inadvertent use of public searches as restriction criteria for restricted data user accounts is prevented. Inadvertently making a private search public, if it is used as a restriction criterion, is also prevented. (13561)
- Communication between Defense Centers and managed sensors is more robust. (13703)
- The Defense Center can push and install updates on sensor groups as well as individual sensors. (13864)
- On the packet view, the Delete button deletes only the single event currently being viewed. (13986)

- The packet payload for events generated by rule number 1497 is rendered correctly. (14034)
- On the packet view for intrusion events, the time stamps for the Event Information and the Packet Information now match, regardless of the time zone selected. (14056)
- The Intrusion Event Summary page on the Defense Center correctly lists the number of managed Intrusion Sensors that generated events during the specified time frame. (14089)
- When a new compliance policy is created, the priority assigned to it is correctly saved with the policy. (14121)
- Compliance events generated by policy and response rules containing special characters in the message field can be searched by message. (20052)
- You can toggle between the local and remote datastore options for deployments with managed sensors. (20824)

Defense Center known issues

- Saving a rule containing a syntax error in the TPS rule editor produces an error message. The contents of the rule editor are then cleared, and the rule building process must be restarted. (11488)
- Do not delete any custom rule classifications that meet the following criteria:
    - The classification was used in an intrusion policy applied to an Intrusion Sensor.
    - Any compliance policies were created using rule classifications. (11748, 14546, 15498)
- Do not delete any custom incident types assigned to an incident. (11748, 14546)
- Intrusion event reports that contain more than one million events can take several hours to generate. (13727)
- In High Availability installations, a secondary Defense Center (DC) cannot be removed and replaced using a different Defense Center as the secondary DC. A backup of the original secondary DC must be created, and this backup must be restored on a new secondary DC. A connection is automatically made to the primary DC when the restore is complete. (13788)

- Some Intrusion Sensors added to a Defense Center may be listed as having out-of-date intrusion detection policies on the Sensor Management page. Ignore these messages. However, ensure that the sensors are updated if the policies are subsequently modified. (13965)
- If TPS e-mail alerting is set up, a recurring task named JobSFMail is added to the scheduler. The start time for the task is set for December 31, 1969 and an entry appears on the calendar for each of the recurring instances from 1969. (13978)
- On the View Schedules page, ensure that the correct check boxes are selected after specifying whether the task is recurring or one time only. If the New Task option and Backup for the Job Type are selected, and the Event or Configuration check boxes are selected before changing the task type between once and recurring, then the check boxes clear. (13992)
- The Scheduler page does not display an error message if an e-mail address is specified in the E-mail Status To field before setting up the mail relay host on the Configure E-mail Notification page. (14002)
- If a user account is deleted and a new account is created with the same name but differing access permissions, the new account will revert to the permissions from the deleted account. The new user account must be edited to ensure that account permissions are correct. (14037, 16291)
- The navigation menu disappears on some browsers if the Start Net Backup button on the Backup and Restore page is clicked before the name for the backup file is specified. Refresh the browser window to restore the navigation menu. (14099)
- The Event Summary page, on the Defense Center, may show event percentages that total more than 100 percent. (14151)
- Account privileges for users logged in as Admin may be reduced to Maintenance access. To regain Admin access, log out and log back in. (14725)
- Event searches that include all digit sensor names produce unexpected results. Avoid using all numeric characters for sensor names. (14726)
- When using a Defense Center to manage an Intrusion Sensor with Store Events Only on DC selected, ensure that Store Events Only On DC is deselected before communication between the sensor and the DC is disabled if you decide not to manage the sensor with the DC. (15430, CR Q01142542)
- The Defense Center and managed sensors must be on the same side of a network address translation (NAT) device. If the network environment is not configured in this way, contact Nortel Technical Support for configuration assistance. (15453)

- Connections may be lost before the network traffic reaches the detection engine when using an Intrusion Sensor in inline mode in high traffic cases. The percentage of packets dropped as reported by the sensor refers to the percentage that was not processed by the detection engine. However, other packets may have been dropped before they reached the detection engine. (15898)
- When a compliance policy is created based on the detected criterion “a new transport protocol is detected” using Transport Protocol as the condition, only the protocol abbreviation, for example UDP, and not the protocol number, for example 17, can be used. (15955)
- Destination-based remediations do not work on standalone RTI Sensors because RTI events have only source hosts transmitted in the event. Some of the included remediation modules, for example Cisco PIX Shun, Cisco IOS Null Route, and CheckPoint OPSEC SAM, provide destination-based remediations. (16149)
- A scheduled task cannot be created using the name of the managed sensor as the job name. (16363)
- There may be a temporary pause in traffic if the Intrusion Sensor is deployed in inline mode and the Snort process is restarted. The Snort process may be restarted when modes are switched between passive and inline or when the sensor is rebooted. (16514, 16516)
- Version 4.1 includes a new MIB, called DCEALERT.MIB, for SNMP alerting. The new MIB is available in the /etc/sf directory and supports the new compliance policy features. (16593)
- The delete button on the Defense Center does not function if two or more OPSEC peers are added. (16651)
- When a version 3.2.x Intrusion Sensor is added to a Defense Center, the default 4.1 intrusion policy for that sensor model is automatically pushed to the sensor. To use a different policy, the policy must be pushed to the sensor. (16667)
- Using a fail-open card with an Intrusion Sensor deployed in inline mode, after a new intrusion policy is applied, causes traffic to pass through the sensor for a brief period without being inspected. This occurs when an intrusion policy is applied on a standalone Intrusion Sensor or when an intrusion policy is pushed to a managed Intrusion Sensor. (16702)
- It can take up to five minutes to add another managed sensor to a Defense Center having a large number of events. A large number of events can be considered five million. (16708)

- To use the rule editor to add the replace keyword to a rule, you must use quotation marks around the replacement string, for example, “replacement_string”. You must also ensure that the content keyword being replaced immediately precedes the replace keyword, which must be the last keyword in the rule. (16748, 16750).
- In High Availability environments, a Defense Center must be used to collect custom fingerprints. If a managed sensor is used to collect custom fingerprints, the information collected is not deleted from the sensor. (16809)
- If a new intrusion policy is created based on an existing policy, any settings for SNMP alerting are not copied to the new policy. As a workaround, edit the new policy and use the Alerting option to configure SNMP alerts. (16876)
- Reboot the appliance if it does not restart properly after the DNS server on the Network page is changed. (16909)
- If custom compliance policies or rules are created on a Defense Center that is later added to a High Availability pair as the secondary Defense Center, then all the existing policy violation events on the secondary Defense Center are listed with numbers, rather than names, for the compliance policy and rule. As a workaround, deactivate and reactivate a single policy so that subsequent events have the correct policy and rule names. (16940)
- A mismatch in Snort versions between a version 4.1 Defense Center managing a version 3.2 Intrusion Sensor with a version 3.2.x patch applied may occur. The mismatch causes the Intrusion Sensor to fail to generate new events. When this happens, delete the sensor from the Defense Center and reintroduce it. When the sensor is reintroduced to the Defense Center, a new version of Snort is automatically pushed onto the sensor and the mismatch is eliminated. (16966)
- If you manually upload an update, ensure that it is pushed manually to the appliance and installed manually. A manually uploaded update installed using the Task Scheduler fails but a success e-mail is sent. (17094)
- When creating a Block To/From Destination IP/Network remediation for a Check-Point OPSEC SAM instance, the Log and Alert options are reversed. That is, selecting Log stores the remediation with the log_alert response and selecting Alert stores the remediation with the log_noalert response. (17426)
- It is possible to create and save an incomplete, invalid compliance rule by incorrectly specifying a Host Profile Qualification. The rule is saved even though the GUI displays an error on save. Fix the rule or none of the compliance policies work. (18476)
- The Japanese language is not supported in this release.

- Rebooting a Defense Center while pushing a policy to a sensor causes tasks in the Task Queue to enter a state where they cannot be deleted from the Task Queue page. (19366)
- If a firewall hosts fails when OPSEC SAM responses are set to use more than one firewall host using the All option, the failure message does not indicate which host failed. Review the firewall logs of the management firewall server to determine which responses failed or succeeded. (19684)
- Use Secure Copy (remote file copy program) to copy large backup files to and from the Defense Center. Most web browsers do not support file transfers larger and 2 Gb. Ensure that you use the Access Configuration page to allow a connection between the Defense Center and the local machine where the backup files are stored. On the RTI Sensor backup files are stored in /var/sf/backup. (20061, 20064)
- File and product names used in the installation and restore processes are not rebranded. (20158, 20160)
- Applying any Policy from the DC causes the IS to restart the snort/interface. (CR Q01157243)
- Snort does not restart after a policy is applied with a community and pass rule. (CR Q01154185)
- The DC identifies a custom-rule-based event by rule number only. (CR Q01142513)
- Pushing an update to an IS that is already updated provides an unclear result. (CR Q01166435)
- When a scheduled report named report/workflow emailed is created, the impact block does not appear. (CR Q01172392)
- Sensor current policy appears as unknown on the DC. (CR Q01142482)
- A DC/RTI custom fingerprint on the management interfaces renders the DC/RTI inaccessible. (CR Q01162947)
- Snort causes incorrect error for the replace option (does not have quotes). (CR Q01175453)
- New rule containing content, without quotes, causes fatal error and snort restarts. (CR Q01171982)
- The RTI on IS upgrade file cannot be removed from the Intrusion Sensor on the Intrusion Sensor GUI. (CR Q01175172, see also CR Q01166446)

- Console I/O is not redirected to the serial port when using Restore or Install CD-ROMs for TPS 2070 IS, TPS 2170 IS, TPS 2070 TI, and TPS 2070 DC. (21355, CR Q01173831)
- A rule created or saved as new cannot be deleted unless the appliance is re-installed. (20009, CR Q01153219)
- False errors occur after login to TPS 2070 IS in passive or in-line mode. (21369, CR Q01149339)
- Bookmarks cannot be saved when using Help from within the GUI. (21384, CR Q01150679)
- Pending events cannot be removed from the queue once processing has started. Remediation events requiring completion on the Defense Center are queued and processed one at a time, resulting in a negative impact on Defense Center performance. (CR Q01202128)
- Sensor upgrade installation fails. If the unsupported action of uploading RTI software directly to an Intrusion Sensor, without installing the software, occurs, then an installation attempt using the Defense Center fails. (CR Q01166446)

Features and functionality – TPS 2050 IS, TPS 2150 IS, TPS 2070 IS, and TPS 2170 IS Intrusion Sensors

The TPS 2x50 IS and TPS 2x70 IS Intrusion Sensors contain the following features and functionality in release 4.1:

- Inline configuration with packet blocking (IPS Mode) — Intrusion Sensors can be deployed in inline mode. Inline mode provides the sensors with the ability to drop traffic or replace malicious content with a benign substitute when a particular rule is fired. Inline mode does not preclude sensors from monitoring events in the traditional passive mode.
- Portscan Enhancement — Intrusion Sensors can now detect a variety of postscan techniques including portscans, portsweeps, decoy portscans, and distributed portscans. Administrators can control sensitivity with low, medium, and high settings. Protocols that can be analyzed include TCP, UDP, ICMP, and IP.
- Intrusion Sensor Auditing — Audit data is accessible through a table of view events. Events, including the addition or deletion of user accounts, are also recorded in the audit log. Administrators can see which users visited specific pages and when.
- Default setting modification — A default setting was modified to allow for a greater number of rules that use the flowbits option.
- Addition of the “From Beginning” option to the byte_jump content keyword — This allows creation of an intrusion rule that skips a calculated number of bytes from the beginning of the packet payload instead of skipping bytes from the end of the calculated byte segment.
- Addition of the “Multiplier” option to the byte_jump content keyword — This allows creation of an intrusion rule that, after calculating the number of bytes to skip, multiplies the initial calculated number of bytes by the integer specified as the argument to the Multiplier option, and then skips forward the final calculated number of bytes in the packet.
- Addition of a new fast packet driver to the TPS 2070 IS, increasing inline performance to ~1 Gbps and passive performance to ~1.2 Gbps.
- Addition of a new IP defragmentation preprocessor — A new IP defragmentation preprocessor, frag3, has been added to Snort. Frag3 replaces Frag2.
- Inclusion of a replacement database — A replacement database that improves the stability and performance of the Defense Center is included in version 4.1.

- Replacement of rule updates by Snort Engine Updates (SEUs) — SEUs replace rule updates as the mechanism for updating Snort-based rules. SEUs also provide new and updated methods, including preprocessors and protocol decoders, to aid in detecting intrusion attempts. Ensure that your SEU installation process complies with your network and security policies because SEUs can contain new binaries. If Scheduled Tasks were previously used to upload and install rule packs, create new tasks for uploading and installing SEUs in version 4.1.
- Addition of Shared Object Rules (SORs) — SORs allow the Nortel Vulnerability Research Team more flexibility in creating new rules. SORs are delivered in SEUs, in binary format. Text rules, now called Standard Text Rules (STRs) were provided in previous rule packs. SOR rule documentation can be viewed and copied the same way as STRs. However, you cannot view or modify the rule keywords section, including rule content keywords. Only attributes, such as the message, the source and destination ports, and addresses in the rule header can be viewed and modified. STRs can be created and modified as in previous versions and any of the legacy STRs can be viewed, copied, and modified.
- Stream Reassembly performance improvements — The server_inspect_limit option has been added to the stream reassembly preprocessor. This improves Intrusion Sensor performance by limiting inspection of server-side traffic. When the detection engine inspects a specified amount of server-side traffic it suppresses inspection of additional traffic until a client-side packet is detected. When a client-side packet is detected, the detection engine resumes inspection of server-side traffic until it again reaches the specified limit. To use the server-inspect-limit option, edit your user.conf file to include the following line:

  ```
  preprocessor stream4_external: server_inspect_limit number_of_bytes
  ```

  where number_of_bytes is the server-side traffic limit.

NOTE – The flow depth parameter of the HTTP inspection decoder overrides the server_inspect_limit option when inspecting HTTP traffic.

- Real-time Threat Intelligence (RTI) software version 3.1 can be installed on Intrusion Sensors TPS 20xx IS configured for passive mode.

Upgrading existing Intrusion Sensors

To install a new Intrusion Sensor version 4.1 appliance, follow the instructions provided in the *Nortel TPS Sensor/DC Installation Guide, Release 4.1*, Part Number 320737-A, which is provided on the Intrusion Sensor Documentation and Restore CD. The guide is also available on the Nortel Technical Support site at www.nortel.com/support.

Upgrade prerequisites for Intrusion Sensors

The following prerequisites must be met before existing Intrusion Sensors are upgraded to version 4.1:

- Intrusion Sensor version 3.2.0.3 is required to complete a successful upgrade to version 4.1. Version 3.2.0.3 is available on the Nortel web site.
- At least 40 Mb of free space is required on the root partition (/), and 78 Mb of free space is required on the /var partition.
- For Defense Centers managing Intrusion Sensors, check the sensor management page and confirm that each sensor uses a policy that the Defense Center can identify. Any policy listed as unknown must be replaced with a policy pushed from the Defense Center to the sensor before either appliance is upgraded.
- Upgrade all Defense Centers before upgrading the sensors managed by the Defense Centers.

Notes on the upgrade process

This section contains important information about upgrading Nortel products. Read the entire section before beginning any upgrade.

NOTE – The upgrade process migrates all event and configuration data to a replacement database.

- Plan the upgrade for a time when it has the least impact on your deployment because the Defense Center reboots after upgrade.
- Nortel recommends that you back up event and configuration data to a local computer.
- Delete any user-created files from /root before starting the upgrade.
- Do not perform any administrative or analysis tasks during the upgrade process.
- When the upgrade is complete, the Intrusion Sensor reboots. Intrusion events marked as reviewed are no longer marked as reviewed and events residing on the clipboard are lost.
- E-mail alerting settings on intrusion rules are not preserved as part of the upgrade. Reconfigure e-mail alerting after the upgrade completes.
- After completion of the Defense Center upgrade, obtain the upgrade software file called Nortel_TPS_Intrusion_Sensor_Upgrade_3.2_to_4.1.0_Upgrade.sh from the Nortel support site at www.nortel.com/support.

- Use the scheduling feature to schedule the upgrade push and installation on managed sensors. For information about the scheduling feature, see the *Nortel TPS Defense Center User Guide*, Part Number 216886-C.
- If the upgrade halts for any reason, it can be restarted at the point where it stopped because the upgrade tracks its own progress. For example, in the event of a power failure during upgrade, the installation process can be restarted using the graphical user interface (GUI). If the upgrade proceeded past the point where the GUI is accessible, edit the /etc/sf/ims.conf file and modify the SWVERSION to match the version being upgraded. For Defense Centers this is version 3.2.0.3. However, if an upgrade halts for any reason, Nortel recommends that you contact Nortel Technical Support.
- The upgrade has a Revert feature that permits restoration of an upgraded appliance to the previously installed software version. Before using the Revert feature, the Revert process checks to ensure that there is enough free space is available on the hard drive to complete the task. At least 50 percent of the size of the event and upgrade data is required. To revert to the previous software version, use secure shell (ssh) with the root account to log into the Intrusion Sensor, type **`revert`** at the command prompt and press **Enter**. Nortel recommends that all event and configuration data is backed up on a local computer before performing the Revert operation because intrusion events in the database are not retained. After the Revert operation is complete, restore the events from backup file to the Intrusion Sensor.
- Intrusion events on the clipboard, or marked as reviewed, are lost when the appliance is rebooted at the end of the upgrade procedure.
- The upgrade can take several hours, depending on the number of events on the appliance, particularly on Defense Centers and the TPS 2070 IS sensor. Refresh the browser to check the status of the upgrade. When the upgrade is complete, a prompt appears instructing the user to log into the appliance.
- E-mail alerting must be reconfigured after the upgrade is complete because settings for e-mail alerting on intrusion rules are not preserved as part of the upgrade. This applies to Defense Centers that manage Intrusion Sensors and Intrusion Sensors.
- The version number on the login page is not updated after the Upgrade. To confirm that the new version is installed, select **Help**. Then select **About** and review the value in the Software Version field.

Upgrading an Intrusion Sensor from version 3.2.0.3 to version 4.1

Use the following procedure to upgrade an Intrusion Sensor from version 3.2.0.3 to version 4.1.

1.Download the Intrusion Sensor 4.1 upgrade script.

2. Open the **Intrusion Sensor Administration** menu and select the following:

   □ Update

   □ View

3. Click **Browse**. Navigate to the location where the upgrade script is saved.

4. Select the upgrade script.

5. Click **Open**. The update appears in the Upload and Update Package field.

6. Click **Upload**. The 4.1 upgrade appears in the Install Update section of the page.

7. Select the button next to the upgrade.

8. Click **Install**. A message appears stating that the appliance will reboot automatically after the upgrade is installed.

9. Click **OK** to continue.

NOTE – If the upgrade halts, Nortel recommends that you do not restart it. Contact Nortel Technical Support.

10. Reapply the current intrusion policy.

Reapplying current intrusion policy

To reapply the current intrusion policy, do the following:

1.Select **Detection**.

2. Select **Policy**.

3. Select **Apply**.

4. Select the name of the current policy.

5. Click **Apply**. **TIP**: There may be a brief pause while the new version of Snort restarts on an Intrusion Sensor deployed in inline mode.

To confirm the new software version after the upgrade is installed and the appliance is rebooted, refresh the browser. Then select **Help**. Select **About** to view and confirm the software version.

NOTE – After the upgrade process is complete, depending on the number of intrusion events stored in the old database, it can take from 20 minutes to 14 hours for the new database to populate with old events and for old intrusion events to appear on the event views and in the event statistics. For example, 1 million events can take up to 20 minutes to migrate, 10 million events can take up to four hours to migrate, and 110 million events can take up to 14 hours to migrate to the new database. Since packet data is migrated after event data, until the migration is complete you may be able to view some old events but not the packets associated with them.

Restoring an Intrusion Sensor

Nortel provides a CD-ROM for restoring a TPS appliance to it original factory settings.

NOTE – Restoring a TPS appliance using the CD-ROM results in the loss of all configuration and event data on the appliance. Nortel recommends that you back up the application before using the Restore CD-ROM. The process retains the license file and network settings but you may need to re-enter the original license file after the Restore process completes.

A keyboard and VGA monitor must be used rather than the serial port when restoring the TPS software for the TPS 2070 IS and TPS 2170 IS platforms to its original state. Turn off the power to the TPS appliance before connecting the keyboard and monitor. Connect the keyboard and monitor. Turn on the power to the appliance and start it from the Software CD using the Restore procedure, see Step 1 of the following procedure. Follow the instructions on the monitor. When the software has been restored, Step 4, turn off power to the appliance and disconnect the keyboard and monitor. Continue with Step 5 of the procedure.

To restore a TPS appliance to its original factory settings, use the following procedure:

1. Place the Restore CD-ROM in the CD tray and perform a safe reboot of the appliance. After the appliance reboots, you are prompted to restore the system.
2. At the prompt, type **Yes**.
3. Press **Enter**.
4. At the prompt, confirm that you want to restore the appliance. After the system is restored, the appliance ejects the CD-ROM and reboots.

5. Connect the appliance and restore power..

6. If the Add Feature License page appears, paste the original license file into the License field.

7. Click **Submit License**.

Intrusion Sensor resolved issues in version 4.1

- User-defined variables that begin with the same string no longer conflict with default intrusion policies. Any user-defined variable can be safely deleted without causing errors. (7976)
- The documentation correctly states that the clipboard can hold up to 25,000 events. (11021)
- Inadvertent use of public searches as restriction criteria for restricted data user accounts is prevented. Inadvertently making a private search public, if it is used as a restriction criterion, is also prevented. (13561)
- Communication between Defense Centers and managed sensors is more robust. (13703)
- The Defense Center can push and install updates on sensor groups as well as individual sensors. (13864)
- On the packet view, the Delete button deletes only the single event currently being viewed. (13986)
- The packet payload for events generated by rule number 1497 is rendered correctly. (14034)
- On the packet view for intrusion events, the time stamps for the Event Information and the Packet Information now match, regardless of the time zone selected. (14056)
- You can now use Internet Explorer to perform a net backup for more than 40 files.(16912)
- The reporting subsystem now uses a different method to extract the current model name and version to facilitate future upgrades. (16995)
- A series of issues with the rule editor has been fixed. (18915, 18921, 18931, 18940, 18995, 18996, 19007)

- E-mail alerts on the TPS 2070 DC and the TPS 2070 IS now correctly show the source destination IP and port. (17141)
- Intrusion Sensor — If you stop serving NTP time from the Defense Center excessive syslog error messages no longer received. (17313)
- When editing rule states within an intrusion policy, rules with an SID of greater than 3,000 now appear. (17314)
- The portscan network configuration field has been expanded to 255 characters. (17530)
- Packets generated by the portscan preprocessor no longer appear to be 14 bytes longer than the original packet. (17615)
- You can toggle between the local and remote datastore options for deployments with managed sensors. (20824)

Intrusion Sensors known issues

- Snort does not restart after a policy is applied with a community and pass rule. (CR Q01154185)
- When a scheduled report named report/workflow emailed is created, the impact block does not appear . (CR Q01172392)
- Snort restarts at midnight. This affects TPS 2070 IS in inline mode, build 235, and TPS 2050 IS, build 289. In Inline mode, Snort restarting causes the link to go down and up and will cause failover in a redundant scenario. When Snort is restarted it loses session and state information.(CR Q01158292)
- A TPS 2070 IS in inline mode allows load balance configuration. (CR Q01159577
- Saving a rule containing a syntax error in the IDS rule editor produces an error message. The contents of the rule editor are cleared and the rule-building process must be restarted. (11488)
- Do not delete any custom rule classifications under the following conditions:
  - the classification in an intrusion policy is used and applied to the Intrusion Sensor
  - any compliance policies are created using rule classifications (11748, 14546, 15498)
- Do not delete any custom incident types assigned to an incident. (11748, 14546)

- Intrusion event reports containing more than 1 million events may take more than one hour to generate. (13727)
- Some Intrusion Sensors added to a Defense Center may be listed on the Sensor Management page as having out-of-date intrusion detection policies. Ensure that the sensors are updated if the policies are modified. (13965)
- The start time for IDS e-mail alerting is set for December 1969 and an entry appears on the calendar for each of the recurring instances back to 1969. The task in the scheduler is named JobSFMail. (13978)
- On the View Schedules page, ensure that the correct check boxes are selected after specifying whether the task is recurring or one time only. If the New Task option and Backup for the Job Type are selected, and the Event or Configuration check boxes are selected before changing the task type between once and recurring, then the check boxes clear. (13992)
- The Scheduler page does not display an error message if an e-mail address is specified in the E-mail Status To field before setting up the mail relay host on the Configure E-mail Notification page. (14002)
- If a user account is deleted and a new account is created with the same name but differing access permissions, the new account will revert to the permissions from the deleted account. The new user account must be edited to ensure that account permissions are correct. (14037, 16291)
- The navigation menu disappears on some browsers if the Start Net Backup button on the Backup and Restore page is clicked before the name for the backup file is specified. Refresh the browser window to restore the navigation menu. (14099)
- The Event Summary page, on the Defense Center, may show event percentages that total more than 100 percent. (14151)
- Intrusion Sensors in inline mode process traffic flow unlike Intrusion Sensors in passive mode. In passive mode Intrusion Sensors cannot report the percentage of packets dropped on the Performance Status page. (14719)
- Account privileges for users logged in as Admin may be reduced to Maintenance access. To regain Admin access, log out and log back in. (14725)
- Event searches that include all digit sensor names produce unexpected results. Avoid using all numeric characters for sensor names. (14726)
- When using a Defense Center to manage an Intrusion Sensor with Store Events Only on DC selected, ensure that Store Events Only On DC is deselected before communication between the sensor and the DC is disabled if you decide not to manage the sensor with the DC. (15430, CR Q01142542)

- The Defense Center and managed sensors must be on the same side of a network address translation (NAT) device. If the network environment is not configured in this way, contact Nortel Technical Support for configuration assistance. (15453)
- Connections may be lost before the network traffic reaches the detection engine when using an Intrusion Sensor in inline mode in high traffic cases. The percentage of packets dropped as reported by the sensor refers to the percentage that was not processed by the detection engine. However, other packets may have been dropped before they reached the detection engine. (15898)
- Destination-based remediations do not work on standalone RTI Sensors because RTI events have only source hosts transmitted in the event. Some of the included remediation modules, for example Cisco PIX Shun, Cisco IOS Null Route, and CheckPoint OPSEC SAM, provide destination-based remediations. (16149)
- A scheduled task cannot be created using the name of the managed sensor as the job name. (16363)
- There may be a temporary pause in traffic if the Intrusion Sensor is deployed in inline mode and the Snort process is restarted. The Snort process may be restarted when modes are switched between passive and inline or when the sensor is rebooted. (16514, 16516)
- Version 4.1 includes a new MIB, called DCEALERT.MIB, for SNMP alerting. The new MIB is available in the /etc/sf directory and supports the new compliance policy features. (16593)
- When a version 3.2.x Intrusion Sensor is added to a Defense Center, the default 4.1 intrusion policy for that sensor model is automatically pushed to the sensor. To use a different policy, the policy must be pushed to the sensor. (16667)
- Using a fail-open card with an Intrusion Sensor deployed in inline mode, after a new intrusion policy is applied, causes traffic to pass through the sensor for a brief period without being inspected. This occurs when an intrusion policy is applied on a standalone Intrusion Sensor or when an intrusion policy is pushed to a managed Intrusion Sensor. (16702)
- It can take up to five minutes to add another managed sensor to a Defense Center having a large number of events. A large number of events can be considered five million. (16708)
- To use the rule editor to add the replace keyword to a rule, you must use quotation marks around the replacement string, for example, “replacement_string”. You must also ensure that the content keyword being replaced immediately precedes the replace keyword, which must be the last keyword in the rule. (16748, 16750).

- If a new intrusion policy is created based on an existing policy, any settings for SNMP alerting are not copied to the new policy. As a workaround, edit the new policy and use the Alerting option to configure SNMP alerts. (16876)
- Reboot the appliance if it does not restart properly after the DNS server on the Network page is changed. (16909)
- A mismatch in Snort versions between a version 4.1 Defense Center managing a version 3.2 Intrusion Sensor with a version 3.2.x patch applied may occur. The mismatch causes the Intrusion Sensor to fail to generate new events. When this happens, delete the sensor from the Defense Center and reintroduce it. When the sensor is reintroduced to the Defense Center, a new version of Snort is automatically pushed onto the sensor and the mismatch is eliminated. (16966)
- If you manually upload an update, ensure that it is pushed manually to the appliance and installed manually. A manually uploaded update installed using the Task Scheduler fails but a success e-mail is sent. (17094)
- The Japanese language is not supported in this release.
- Rebooting a Defense Center while pushing a policy to a sensor causes tasks in the Task Queue to enter a state where they cannot be deleted from the Task Queue page. (19366)
- If a firewall hosts fails when OPSEC SAM responses are set to use more than one firewall host using the All option, the failure message does not indicate which host failed. Review the firewall logs of the management firewall server to determine which responses failed or succeeded. (19684)
- Use Secure Copy (remote file copy program) to copy large backup files to and from the Defense Center. Most web browsers do not support file transfers larger and 2 Gb. Ensure that you use the Access Configuration page to allow a connection between the Defense Center and the local machine where the backup files are stored. On the RTI Sensor backup files are stored in /var/sf/backup. (20061, 20064)
- File and product names used in the installation and restore processes are not rebranded. (20158, 20160)
- Console I/O is not redirected to the serial port when using Restore or Install CD-ROMs for TPS 2070 IS, TPS 2170 IS, TPS 2070 TI, and TPS 2070 DC. (21355, CR Q01173831)
- A rule created or saved as new cannot be deleted unless the appliance is re-installed. (20009, CR Q01153219)
- False errors occur after login to TPS 2070 IS in passive or in-line mode. (21369, CR Q01149339)

- Bookmarks cannot be saved when using Help from within the GUI. (21384, CR Q01150679)
- The user interface inserts a dot character at the end of a hostname entered on the Network Configuration page. This produces the following error: alert not sent, socket refused. The Intrusion Sensor does not send a response. Nortel recommends configuring the Intrusion Sensor with a Hostname and Domain name. This permits OPSEC to operate correctly. (CR Q01209729)

Related publications

These release notes supplement the following documents:

- *TPS 2050 and TPS 2070 Intrusion Sensor User's Guide* Release 4.1 (Part Number 216884-C)
- *TPS 2070 Defense Center User's Guide* Release 4.1 (Part Number 216886-C)
- *Real-time Threat Intelligence User Guide Release 3.1* (Part Number 320722-A)
- *TPS Intrusion Sensor and Defense Center Installation Guide* Release 4.1 (Part Number 320737-A)
- *TPS Real-time Threat Intelligence Sensor Installation Guide Release 3.1* (Part Number 320738-A)
- *TPS Remediation Module for Application Switch Installation & Configuration Guide* Release 3.1 (Part Number 320739-A)
- *Real-time Threat Intelligence Sensors 3.1 Release Notes* (Part Number 320741-A)
- *Real-time Threat Intelligence Software for TPS Intrusion Sensors 3.1 Release Notes* (320742-A)
- *Real-time Threat Intelligence Software for TPS Sensor Configuration Guide* Release 3.1 (Part Number 320758-A)

Refer to the documents in the previous list for additional technical information regarding the product architecture and features. These documents are available on the Nortel Technical Support web site. To access these documents, use the following procedure.

1. Open your web browser and enter www.nortel.com/support. The Technical Support page opens.

2. From the pull-down list next to selection 1, Select from, select **Product Categories.**

3. Scroll to Security & VPN in the Product Categories list box.

4. Select **Threat Protection** from the list**.**

5. From selection 2, ... choose a product ..., select the applicable product.

6. From selection 3, ... and get the content., select the type of information you require. For example, select **Documentation**.

7. Click **Go**. The product documentation page opens.

The User's Guide and Installation Instructions are PDF files that can be read and printed using the free Acrobat Reader® software available from Adobe Systems Incorporated at the Adobe web site. To obtain a manual in hardcopy format, contact your Nortel sales representative and order the appropriate part number.

Technical support

You can access technical support for your Nortel product through the Technical Solutions Center.

Technical Solutions Center telephone

Europe, Middle East, and Africa - 00800 8008 9009 or +44 (0) 870 907 9009

North America - (800) 4NORTEL or (800) 466-7835

Asia Pacific - (61) (2) 8870-8800

China - (800) 810-5000

Additional information about the Nortel Technical Solutions Centers is available at www.nortel.com/support.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, refer to www.nortel.com/erc.