Part No. 320741-A
Septmber 2005

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

Release Notes for Nortel Real-time Threat Intelligence Sensors 3.1

320741-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 Real-time Threat Intelligence (RTI) Sensors release 3.1. The Nortel Real-time Threat solution consists of the following:

- TPS 2050 TI RTI Sensor with version 3.1
- TPS 2070 TI RTI Sensor with version 3.1
- RTI Host User license applied to the Nortel TPS 2070 Defense Center (based on the number of network hosts being monitored)

Features and functionality

TPS 2050 TI and TPS 2070 TI RTI Sensors

The TPS 2050 TI and TPS 2070 TI RTI Sensors contain the following features and functionality in release 3.1:

- 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 out any number of 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 GUI.
- The TPS Remediation Module for Nortel Application Switch plug-in software files are available online at www.nortel.com/support. When the Technical Support page opens select **Product Categories** from the pull-down list next to selection 1, Select from**.** 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 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.

- 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 share a common pool of host licenses.
- IDS/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.
- RTI Sensor 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.
- 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 can determine 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 2050 IS and the TPS 2070 IS passive mode intrusion sensors. RTI cannot be installed on the TPS 2150 IS or the TPS 2170 IS inline mode intrusion sensors.
- 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.

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.

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
v 4.1	v. 4.1	v 3.1
v 3.2	v 3.2	N/A

Hardware installation

Refer to the appropriate installation guides for complete instructions on the installation of the TPS 2070 Defense Center, the TPS 2050 TI RTI Sensor, or the TPS 2070 TI RTI 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 2050 TI RTI Sensor, and the TPS 2070 TI RTI Sensor products are pre-loaded with version 3.1. of the software. The software is also available on a CD that is shipped with the hardware and is available on the Nortel Technical Support web site at www.nortel.com/support for contracted customers.

The software file names for release 3.1 are:

- **Nortel_TPS_RTI_Sensor-2050-v3.1.0-78-Restore.iso** (TPS 2050 TI RTI Sensor)
- **Nortel_TPS_RTI_Sensor-2070-v3.1.0-78-Restore.iso** (TPS 2070 TI RTI Sensor)

Updating software

Updates for RTI Sensor software are distributed electronically and can be downloaded from the hardware web interface. Refer to the *Nortel TPS Real-time Threat Intelligence User Guide*, Part Number 320722-A for complete instructions on performing this task.

Restoring a Threat Intelligence Sensor

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

IMPORTANT! – 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 TI 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, conform 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**.

Known issues

- 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)
- 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)
- 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 Support for configuration assistance. (15453)

- When a compliance policy is created based on the “a new transport protocol is detected” criterion using Transport Protocol as the condition, only the protocol abbreviation, for example UDP, can be used (and not the protocol number, for example 17). (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)
- Configure the DHCP server to transmit the same NTP server. Otherwise, when the time is set on the sensor using the Via NTP Server option, and the DHCP server transmits a different NTP server record, the DHCP-provided NTP server is used when the sensor is rebooted. (16452)
- In High Availability environments, a Defense Center must be used to collect custom fingerprints. (16809)
- The information collected is not deleted from the sensor if a managed sensor is used to collect custom fingerprints. (16809)
- Reboot the appliance if it does not restart properly after the DNS server on the Network page is changed. (16909)
- If you manually upload an update, ensure that you manually push the update to the appliance and install the update manually. If you manually upload an update and use the Task Scheduler to schedule the installation it fails. A success e-mail is sent even though the installation has failed. (17094)
- When creating a Block To/From Destination IP/Network remediation for a CheckPoint 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)
- The Japanese language is not supported in this release.
- 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)
- SSL access restriction locks out approved device. (CR Q01163853)

- The RTI/Maintenance/Task is missing. (CR Q01154875)
- 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)
- Bookmarks cannot be saved when using Help from within the GUI. (21384, CR Q01150679)
- 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)

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* (Part Number 320737-A)
- *TPS Real-time Threat Intelligence Sensor Installation Guide* (Part Number 320738-A)
- *TPS Remediation Module for Application Switch Installation & Configuration Guide* (Part Number 320739-A)
- *Threat Protection System 4.1 Release Notes* (Part Number 320740-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* (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:

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.