Nortel TPS 4.5.1 to 4.5.1.1 Patch Release Notes

August 15, 2006

New Features and Functionality

This patch release includes no new features or functionality.

Issues Resolved in Version 4.5.1.1

The following issues are resolved in Version 4.5.1.1:

- Fixed multiple issues for compliance rules that are triggered from flow data events.
- Improved the stability of communications channels for large deployments.
- Improved performance of health monitoring for large deployments.
- Fixed stability issues in SFDataCorrelator for large deployments.
- Fixed an issue that occasionally causes SEU installations to fail while importing new rules.
- Changed the Create Interface Set page so that the Transparent Inline Mode check box reflects the current state of the selected interface set.
- Fixed an issue that caused variable names in mixed case to be handled incorrectly.
- Fixed an issue with DNS resolution that occasionally caused the sensor registration process to time out.
- Intrusion event searches by GID:SID now consistently returns the correct events.
- The Defense Center can now serve time to sensors using NTP regardless of how its local time is set.
- Fixed an issue that caused the Defense Center to generate a link that returned a "URI too long" error message.
- Fixed an issue that prevented unified2 archive files from being pruned on the Defense Center.
- The speed and duplex settings for a network interface are now retained after a reboot.
- Fixed an issue that prevented a compliance rule from generating events when the rule included a service name condition or was triggered by an event based on new information about a TCP or UDP service.
- Fixed an issue that sometimes causes incorrect packet displays on a Defense Center managing both Intrusion Sensors and Agents.
- Improved performance when you view the packet details for a single intrusion event and the database contains many intrusion events.

Upgrading Existing Defense Centers

Make sure you read the following sections before you begin the upgrade:

- Prerequisites
- Important Upgrade Notes
- Upgrade Procedures

Prerequisites

- You must be running TPS Defense Center Version 4.5.1 to complete this upgrade successfully. If your Defense Center is running an earlier version, you can obtain upgrades from the Nortel Support Site .
- You must have at least 7 MB of free space on the `/` partition and 17 MB of free space on the `/var` partition to complete this upgrade successfully.
- Make sure you upgrade the Defense Center **before** you upgrade any sensors it manages.

Important Upgrade Notes

Before you begin the upgrade, Nortel **strongly** recommends that you back up all your event and configuration data and save it on a local computer.

Make sure you plan your upgrade for a time when it will have the least impact on your deployment; be sure to schedule the upgrade during non-peak hours.

WARNING! If you have issues with the upgrade, for example, it halts for any reason, do **not** restart it. Instead, please contact Nortel Support for more information.

Also, there are some important points you should keep in mind:

- When you upgrade a Defense Center that is half of a high availability pair, the Defense Centers in the pair stop sharing configuration information until the second Defense Center is upgraded. Make sure you upgrade the primary Defense Center first. After the primary Defense Center is upgraded, make sure it is communicating with all of its managed sensors. Do not change any settings on it until after you upgrade the secondary Defense Center. Then, upgrade the secondary Defense Center. Note that until you upgrade the secondary Defense Center, the health monitor on the primary Defense Center displays the status of the secondary Defense Center as Critical. Only after both Defense Centers are communicating with their managed sensors should you upgrade the sensors.
- Do **not** use the web interface until the upgrade has completed and the appliance reboots.
- Before starting the upgrade, either stop all tasks in the task queue or make sure they are completed.

- If an intrusion sensor fails to start up correctly after you upgrade it (CPUs appear to be dead or interfaces appear to be missing) log in to the sensor as root and type `reboot` at the command prompt. Contact Nortel Support if the issue persists.

- After installing the patch, the currently applied intrusion policies will be shown as modified since they were last applied. Nortel recommends that you reapply your intrusion policies after installing the patch.

- An uninstall might take a minute or more to complete, and the task status might stay at 69% for a short period of time. This is normal behavior.

Upgrade Procedures

After you upgrade the Defense Center, you can use it to upgrade any sensors it manages.

Upgrading the Defense Center

To upgrade a Defense Center:

1. Download the Nortel TPS 4.5.1.1_patch.zip file from the Nortel Support Site. Extract script file `Nortel_TPS_Defense_Center_Patch_4.5.1_to_4.5.1.1_Patch-15.sh`.

   WARNING! Download update files directly from the Nortel Support Site and do not transfer them by email. If you transfer an update file by email, it may become corrupted.

2. On the Defense Center, select **Operations > Update.**

   The Patch Update Management page appears.

3. Click **Upload Update** to browse to the location where you saved the upgrade script, then click **Upload.**

   The upgrade appears in the Updates list.

4. Next to the upgrade you just uploaded, click **Install.**

   The Install Update page appears.

5. Under Selected Update, select the Defense Center and click **Install.**

   WARNING! If you have issues with the upgrade, for example, it halts for any reason, do **not** restart it. Instead, contact Nortel Support for more information.

6. Select **Operations > Help > About** and confirm that the software version is listed as 4.5.1.1.

7. Verify that all managed sensors are successfully communicating with the Defense Center.

8. Upgrade any managed sensors in your deployment.

   Upgrading Managed Sensors

Before you upgrade a managed sensor using the Defense Center, you **must** first upgrade the Defense Center and verify that the sensor is successfully communicating with the Defense Center.

To upgrade managed sensors:

1. Download the Nortel TPS 4.5.1.1_patch.zip file from the Nortel Support Site. Extract script file `Nortel_TPS_Intrusion_Sensor_Patch_4.5.1_to_4.5.1.1_Patch-15.sh`.

.

WARNING! Download update files directly from the Nortel Support Site and do not transfer them by email. If you transfer an update file by email, it may become corrupted.

2. On the Defense Center, select **Operations > Update.**

The Patch Update Management page appears.

3. Click **Upload Update** to browse to the upgrade script you downloaded, then click **Upload.**

The upgrade script is uploaded to the Defense Center.

4. Next to the upgrade script, click **Push.**

The Push Update page appears.

5. Select the sensors or sensor groups that you want to upgrade.

6. From the **Batch size for this push** list, select the number of sensors to which the Defense Center should copy the upgrade script at a time.

For example, if you have 20 managed sensors to upgrade, you can specify 5 as the batch size to push the updates to 5 sensors at a time, and then push to the next 5 sensors.

7. Click **Push.**

You can monitor the progress of the push in the task queue (**Operations > Monitoring > Task Status**). When the push is complete, continue with the next step.

8. Next to the upgrade script, click **Install.**

The Install Update page appears.

9. Select the sensors or sensor groups to which you pushed the upgrade script and click **Install.**

The upgrade is installed and the sensors are automatically rebooted. The Defense Center then automatically applies an updated intrusion policy to any Intrusion Sensors you upgraded.

TIP! You can monitor the progress of the upgrade in the task queue (**Operations > Monitoring > Task Status**). If the task queue stops updating with current status, manually refresh your browser.

WARNING! If you have issues with the upgrade, for example, it halts for any reason, do **not** restart it. Instead, contact Nortel Support for more information.

10. On the Defense Center, select **Operations > Sensors** and confirm that the sensors you upgraded have the correct versions listed: 4.5.1.1

|| Uninstalling the Patch

IMPORTANT! You **cannot** use the Defense Center to uninstall the upgrade from managed sensors. For information on how to uninstall the upgrade from a sensor, refer to the sensor release notes.

To uninstall the upgrade from the Defense Center:

1. Select **Operations > Update.**

   The Patch Update Management page appears.

2. Select the uninstaller that matches the upgrade you want to remove and click **Install.**

   The Install Update page appears.

3. Under Selected Update, select the Defense Center and click **Install.**

   The update is removed, and the Defense Center reverts to its previous version.

   TIP! The uninstall can take a minute or more to complete and the task status might stay at 69% for a while; you can monitor the progress of the uninstall in the task queue (**Operations > Monitoring > Task Status**).

   WARNING! If you have issues with the uninstall, for example, it halts for any reason, do **not** restart it. Instead, contact Nortel Support for more information.

4. Select **Operations > Help > About** and confirm that the software version is listed as 4.5.1.

|| Known Issues

There are no known issues with Version 4.5.1.1. See the release notes for Version for 4.5.1 for known issues at the times of those releases.

How to get help: If you have purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com, and then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4 NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

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, go to http://www.nortel.com/support . Click on the link for Express Routing Codes located at the bottom-right corner of the Web page.