Nortel Threat Protection System

Threat Protection System Troubleshooting Guide

Release: 4.7
Document Revision: 01.01

www.nortel.com

NN47240-700 324442-A

Nortel Threat Protection System
Release: 4.7
Publication: NN47240-700
Document status: Standard
Document release date: 11 2007

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the Apache Software Foundation http://www.apache.org/.

This product includes a TAP-Win32 driver derived from the CIPE-Win32 kernel driver, Copyright © Damion K. Wilson, and is licensed under the GPL.

See Appendix D, "License Information", in the *User's Guide* for more information

Contents

New in this release

The *Nortel Threat Protection System Release. 4.7 Troubleshooting Guide with Emergency Recovery Tree* (NN47240-700) is a new document for Nortel Threat Protection System Release 4.7.

Navigation

Introduction

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

This chapter describes the prerequisites and various tools used to troubleshoot the Nortel TPS 4.7. Use these troubleshooting tools to enhance the overall performance, resolve error messages, and increase response time for a specific feature. Each tool is described by purpose, usage procedures, and how to interpret the output.

Prerequisites

Nortel recommends you to use one or more of the following commercially available troubleshooting tools as well as the tools described in this document.

- Capture and analyze HTTP and HTTPS with the HTTP Analyzer from IE Inspector http://www.ieinspector.com/
- Capture and analyze HTTP and HTTPS with Tamper Data, a plug-in available for Mozilla Firefox https://addons.mozilla.org/en-US/firefox/addon/966
- Display the time to load Web pages with Faster Fox, a plug-in available for Mozilla Firefox https://addons.mozilla.org/en-US/firefox/addon/1269
- Capture and analyze packets with either Sniffer or Wireshark from Network General http://www.wireshark.org/ and http://www.networkgeneral.com/

Navigation

Acronyms

Table 1 "Acronyms" (page 10) lists the acronyms used in this guide.

Table 1
Acronyms

TPS	Threat Protection System
CLI	Command Line Interface
LED	Light Emitting Diode

Troubleshooting Fundamentals

This section provides conceptual information about the methods and tools that you can use to troubleshoot and isolate problems in TPS 4.7

Navigation

Log files

View the log files to see the history of system events.

This troubleshooting guide documents only the most common messages from the ssl.log.

/maint/debug/proxydebug [on|off|once]

on: enable simpleproxy to print out debug message.

off: disable simpleproxy to print out debug message.

once: enable simpleproxy to print out debug message only once.

ATTENTION
Enabling proxydebug will use more CPU resource. Make sure to disable it after you finish debugging.

Transmit the event log from the Nortel VPN Gateway to a file on a TFTP, FTP, or SFTP server. Specify the IP address or host name of the server as well as the file name. The default value is TFTP.

Table 2 "Log file types in a log dump" (page 11) lists the log file types in a log dump.

Table 2
Log file types in a log dump

Log file type	Description
clierror	This log provides information on the CLI engine and is used by engineering to debug issues while in development.

Table 2
Log file types in a log dump (cont'd.)

erlerror	This log provides information on the internal Erlang language engine and SSL acceleration. It is used by Engineers to debug issues while in development.
erlstart	This log provides information on the internal Erstart language engine and SSL acceleration. It is used by Engineers to debug issues while in development.
conslog	This log contains messages displayed on the console port of the device. These messages are the one that are generated during boot sequence. These messages are generated during boot sequence.
dmesg	This log contains messages generated by the kernel.
ssl.log	This log contains messages generated by the simpleproxy features. The user needs to completely logoff and then close the browser ; login and then active the ssldump.
ikelog	IPsec module related messages.
message	This log contains standard syslog types of messages and contains general information such as system-level status and non-application acceleration errors across the device.
Procomm	Kernel panic message with debug information can be captured from console directly. Use Procomm to capture those messages.

Issues that require Sourcefire assistance

Contact Sourcefire for assistance on the following issues and request the process that was taken to update customer details and restore the document.

1. **The DC cannot push a policy to the sensors**
   The customer may have to re-image the box.
2. **OPSEC is not working properly**
   The trust between the DC and the sensors are configured correctly and the trust is established but the **SFReactd**does not seem to trigger the**fw same dynamic rule**. The customer may have to re-image the box.
3. **Software upgrade fails**
   This largely depends on where within the upgrade process, the upgrade fails. In most cases, the problem will need to be examined on a case-by-case basis to determine what happened.
   If an upgrade has failed, the system may be in a dubious state for which reverting may exacerbate the problem. Any such problem should be reported to Sourcefire Support.
   There is a process for reverting to the previous version, which is documented in the User Guides, however that process is only

recommended in cases where the upgrade was successful but for one reason or another the customer has chosen to revert to the previous version.

4. **Customer is not able to add a sensor to be managed by a DC**

Hardware Troubleshooting

This section describes the feature-specific troubleshooting tools available at the operating system level.

Navigation

TPS Hardware

This section provides information to troubleshoot hardware problems related to the TPS 2050, TPS 2070 and TPS 2150 devices.
The table Front Panel LEDs describes the Front Panel LED indicators on the TPS device.

Table 3
Front Panel LEDs

LED Indicator (from left to right)	Description
Amber system status LED	The amber system status LED lights up when the system needs attention due to a problem with power supplies, fans, CPU, or system temperature.
Hard-disk drive activity LED	This LED blinks when activity is detected on the hard-disk drive.
System power LED	This LED is green when the power supply is turned on.
System status LED	The system status LED lights up when the system needs attention due to a problem with power supplies, fans, system temperature, or hard drives.
Overheat indicator LED	This LED is red when the system overheats.

ATTENTION
Call Nortel for RMA if Amber System status LED can not be cleared.

Ports to open in a firewall

If there are one or more firewalls in between the Defense Center and Intrusion Sensors, then you will need to open one or more ports on the firewall, depending on the software version of the TPS devices.

Software release 4.5.x and above

The Defense Center and the Intrusions Sensors communicate on TCP port 8305 only, by default. The administrator can change this port number.

Software release 4.1.x and below

The Defense Center and the Intrusions Sensors communicate on the following TCP ports.

TCP Port		Direction To/From DC	Description
22	SSH	Outbound from DC to Sensor	DC uses this port to push configurations, updates, & HA
8300	SSL	Inbound from Sensor to DC	Management functions
8301	SSL	Inbound from Third Parties to DC	eStreamer API (event data streams)
8302	SSL	Inbound from Sensor to DC	eStreamer from Intrusion Sensors
8303	SSL	Inbound from Sensor to DC	Heartbeat Protocol

Software Troubleshooting

The TPS 2070 Defense Center (DC), TPS 2050 Intrusion Sensor (IS), 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 website, 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)

This chapter describes the various procedures to troubleshoot the software on the TPS devices.

Navigation

Creating a troubleshoot file from a TPS device

Use this procedure to create a compressed troubleshoot file from a TPS device to obtain critical information to troubleshoot it.

CAUTION
Only authorized administrators must create a troubleshoot file from a TPS device.

Procedure 1
Procedure steps

Step	Action
1	Open a case with Nortel Enterprise Technical Support (NETS).
2	Enter the following command to go to the default location. `/usr/local/sf/bin`
3	Run the script **sf_troublshoot.pl**
4	Enter the following command to obtain the default configuration file**troubleshoot.conf**. `/etc/sf/troubleshoot.conf`
5	Customize the **troublshoot.conf** file into a **custom.conf** file if necessary. **ATTENTION** Although there is a predefined set of data to collect, defined in **troublshoot.conf**file, you can specify a**custom.conf** file to customize what data is collected.
6	Enter the following command to obtain the **default results** file. FTP the SFTP client to obtain the file. `/var/tmp/results` The format of the**results** file is:

results-mm-dd-yyyy--xxxxxxx.tag.gz
You can use the **-t**option to allow the case number to be placed within the name of the **results** file.

ATTENTION
WINSCP is a freeware SFTP client for windows and can be downloaded from the location http://www.winscp.com/

--End--

Obtaining the troubleshoot file following a failed software upgrade

Use this procedure to obtain a troubleshoot file from a TPS device in case of a failed Nortel TPS Defense Center Upgrade. An upgrade on a TPS device is done by customers or support personnel.

CAUTION
Refer TPS 4.7 Release Notes (part number) for information on prerequisites, detailed steps and tips on performing a complete and correct Nortel TPS DC 4.5.1 Upgrade on a TPS device.

Procedure 2
Procedure steps

Step	Action
1	Enter the following command to obtain the output file that contains the list of updates pushed to the TPS device. `/var/sf/updates/ls-alshL var-sf-updates.output`
2	Verify that the correct upgrade script was used to upgrade the TPS device.
3	Enter the following command to obtain the troubleshoot log file. `\results-dd-mm-yyyy--191127\dir-archives\var-log\sf\Nortel_TPS_DC_Upgrade-4.5.1\main_uograde_script.log` This log file is a complete account of the upgrade process. **ATTENTION** The name of the folder in which the troubleshoot log file is extracted, includes the version of the software you upgrade to.

--End--

Resetting passwords

This section describes resetting passwords on TPS devices.

Resetting the root password of a TPS device

Use this procedure to reset the root password of a TPS device (2050 model), if it is lost or forgotten.

Procedure 3
Procedure steps

Step	Action
1	Connect the TPS device (2050 model) to a PC or laptop, using a console cable. **ATTENTION** Connect the TPS device to a monitor and keyboard, if the device is a 2070 model.
2	Power cycle the TPS device.
3	Press any arrow key during the boot sequence at the LILO boot prompt. **ATTENTION** Press any arrow key during the boot sequence when the LILO boot menu appears, if the device is a 2070 model.

4	Enter the following command at the LILO boot prompt to load the linux operating system.
	`linux -s`
	
	System response:
	`Loading linux.....`
	`Linux version 2.4.26st.p4smp-13 (build@renowm.sfeng.so urcefire.com)(gcc version 2.95.320010315 (release)) #1 SMP Fri Aug 12 16:37:04 UTC 2005`

5	Enter the following command: LILO 22.2 boot:**`passwd root`** At the prompt, enter the new root password. Reenter to confirm the root password.
6	Enter the following command to reboot the 2050 TPS device. LILO 22.2 boot:**`reboot`**
7	Enter the following command to login to the 2050 TPS device: Nortel TPS 2X50 DC Series v4.1.0 (build 78) DC2050.ca.nortel.com login: **root**

Enter the password at the prompt:
Password:**<password here>**
System response:

```
Copyright 2007 Nortel Networks, Inc.  and
Sourcefire, Inc..  All rights reserved.
Sourcefire is a registered trademark of Sourcefire,
Inc.  All other trademarks are property of their
respective owners.
Nortel Linux OS v4.0.1 (build 21)
Notel TPS 2X70 DC Series v4.1.0 (build 78)

Last login:  Mon Oct 24 15:25:54 +0000 2005 on
ttyS0.
No mail.
```

--End--

Resetting the Administrator Password for a TPS device

Reset the administrator password for a TPS device if it is lost or forgotten.

CAUTION
Reset the administrator password, if and only if you know the **root** password for the TPS device. Refer section "Modifying root password for a TPS device", if you forget or lose the password, to reset the same.

Procedure 4
Procedure steps

Step	Action
1	Go to root prompt on the TPS device (2070 model).
2	Enter the following command: root@DC2070: ~#**resetadmin**
3	Enter the root login password at the password prompt. Please enter the root login password:**<password here>**.
4	Enter the administrator login password at the password prompt. Please enter the admin login password:**<password here>**
5	Reenter the administrator login password at the reenter login password prompt. Please enter the admin login password again:**<password here>**. System response:

```
Password reset successfully
```
Control returns to the root prompt.

--End--

Installing an Old Version of SEU

Use this procedure to install a lower version of Snort Engine Upgrade (SEU) than that currently installed, for test purposes.

Procedure 5
Procedure steps

Step	Action
1	Enter the following command to query the versions of SEUs currently installed. **run rpm -qa**
2	Enter the following sequence of commands to install an earlier version of an SEU. **rpm -e snort-#.#.#-##** **rpm -e Sourcefire_Module_Pack-#-dev** **rpm -e Sourcefire_Rule_Pack-##-vrt** **rpm -e Sourcefire_Snort_Engine_Upgrade-##-###** where the character # represents placeholders for the current version.  **CAUTION** Do not enter any other **rpm -e** commands at the command prompt except the ones listed in step 2.

--End--

Event handling

This section describes the corrective steps to be taken when TPS devices do not handle events correctly.

Troubleshooting TPS Sensor when not receiving events

Use this procedure to take corrective action when the TPS sensor does not receive events.

1. Check if the time is set correctly.
2. Check if snort is running.
3. Enter the following command to check if the TPS Sensor has attained 100% capacity.
   `/var`

Troubleshooting Defense Center when not receiving events

Use this procedure to take corrective action when the Defense Center (DC) does not receive events.

1. Enter the following command to check if the TPS DC has attained 100% capacity.
   `/var`
2. Check if the TPS sensor(s) is (are) receiving events. Refer section "Troubleshooting TPS Sensor when not receiving events" (page 23)for more information.
3. Check if the time is synchronized between the DC and sensor(s).
4. Check if the sensor(s) can reach the DC on ports 8300-8303.
5. Troubleshoot the SFDataCorrelator. Refer section "Troubleshooting the SFDataCorrelator", for more information.

Troubleshooting errors when adding sensor to DC

Use this procedure to troubleshoot errors that arise when adding a sensor to DC.

Procedure 6
Procedure steps

Step	Action
1	Check **httpsd_error_log** for errors on the DC.
2	Click **Reset Comm** in the Sensor GUI.
3	SSH to the Sensor. Enter the following command to check for the IP address of the DC **`/var/sf/managed/<DC_IP>`** Delete the IP address of the DC, if it exists.
4	Enter the following command to find the size of the authorized_keys and check if it is the same size as

authorized_keys.default
/var/sf/snorty/.ssh/authorized_keys

5 If the sizes do not match, enter the following sequence of commands.
cd /var/sf/snorty/.ssh
rm authorized_keys
authorized_keys.default authorized_keys

6 SSH to the Sensor. Enter the following command to check for the IP address of the Sensor
/var/sf/managed/<Sensor_IP>
Delete the IP address of the Sensor, if it exists.

--End--

Table 4
Variable Definitions

Variable	Value
<DC_IP>	IP address of the DC
<Sensor_IP>	IP address of the Sensor

Troubleshooting the SFDataCorrelator

Use this procedure to troubleshoot a SFDataCorrelator that is not running.

Procedure 7
Procedure steps

Step	Action
1	Enter the following command to check for error messages. **/var/log/messages**
2	Enter the following command to run the initialization script. **/etc/rc.d/init.d/SFDataCorrelator start**
3	If the SFDataCorrelator fails to start, repeat step 1 to check for error messages.
4	If the SFDataCorrelator still fails to start, enter the following command to delete the **event table**. **mysql -uroot -padmin sfsnort -e "drop table event"**
5	Enter the following command to rerun the initialization script. Wait for a minute after running the script. **/etc/rc.d/init.d/SFDataCorrelator restart**

6	Enter the following command **`ps auxww	grep SFD`** Send the output to the respective development team.

--End--

Troubleshooting alerting problems

Use this procedure to troubleshoot alerting problems in mail, SNMP and Syslog.

Troubleshooting mail alerting problems

Use this procedure to roubleshoot email alerting problems.

Procedure 8
Procedure steps

Step	Action
1	Check if the mailing application is configured and enabled for email alerting.
2	Run the following shell script at the command prompt. **`sfmail.sh`**
3	Enter the following command to check for errors. **`/var/log/messages`**
4	Ensure that the IP address of the Sensor or DC is reverse resolvable via DNS.
5	Enter the following command to add hostname information. **`/etc/hosts`**

--End--

Troubleshooting SNMP alerting problems

Check if SNMP is running.

Troubleshooting Syslog alerting problems

Check if syslog is running.

Troubleshooting events that show incorrect time

Use this procedure to troubleshoot events that do not show correct time.

Procedure 9
Procedure steps

Step	Action
1	Check if the system clock is set to **UTC**.

2	Enter the following command to check the current system time.
	`date`
	OR
	`date -u`

3	If the current system time is wrong, enter the following commands to change the local time.
	`rm /etc/localtime`
	`ln -s /usr/share/zoneinfo/<tzfile>/etc/localtime`

4	Set the parameter**timezone**in **User Preferences** dialog box.
5	Set up the NTP.

--End--

Troubleshooting LDAP authentication

Use this procedure to troubleshoot LDAP authentication failure

Procedure 10
Procedure steps

Action
If LDAP authenication fails do the following sequence of actions • Ensure that the user test passes when creating the LDAP object • If the user test fails, do the following. — Ensure that the LDAP server is working properly. — Check if the DC can communicate with the LDAP server. — Check if the LDAP server uses the correct port. — Enter the following commands to check the corresponding user name template: – `%s@xxx.com` for MS Active Directory – `cn=%s,dc=xxx,dc=com` for OpenLDAP – `uid=%s,dc=tps,dc=com` for Sun Directory • Set the authentication status as **enabled**. • Activate the LDAP object under the system policy.

- Apply the system policy only after activating the LDAP object.
- Ensure that the user for authentication is created using external authentication method.
- If the MSAD Certification authentication fails do the following. Ensure that the MSAD certificate is in the following format.
  [Base-64 encoded data from pem file you exported on your Active-Directory CA machine]
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  [Base-64 encoded data from pem file that contains the certificate from the AD mail server]
  -----END CERTIFICATE-----
- Do the following steps if there is a certificate for SSL/TLS
  - Ensure that the hostname of LDAP server — at Server IP address field, is used instead of its IP address
  - Enter the hostname as the common name in the certificate.
- Obtain the SSL certificate.
- Do the following to interact with the user interface when LDAP fails.
  - Edit the following file on the appliance:
    `/etc/sf/ims.conf`
  - Add the following to the end of the file:
    `LDAP_INFO = 1`
    Retry the connection from the Authentication Object page. Expand the check box that appears at the bottom of the page to view the errors in greater detail.

RUA

- Obtain the RUA licence. It is mandatory.
- Create the RUA Detection Engine, since RUA requires it.

Configuring Snort through the User Interface

Use this procedure to make Snort configuration via the user interface (user.conf) editable by the user. To support the dynamic features of Snort outside of the core product releases, you can provide the raw snort configuration via the user.conf.

Procedure 11
Procedure steps

Step	Action
1	Manually add the following variable to provide raw snort configuration via the user interface. **USER_CONF**
2	Apply the policy to store data in the variable **$USER_CONF**athe the following location: `/var/sf/detection_engines/[uuid]/user.conf`

--End--

Verifying prohibit packet data on the DC

Use this procedure to verify prohibit packet data on the DC.

Procedure 12
Procedure steps

Step	Action
1	Register a 4.7 IS sensor to the DC.
2	Select the Prohibit Packet Data from Sensor option at the registration screen.

3	On the managed sensor or IS, ensure that the following line
	`ignore_packet_data 1`
	is present in:
	`/var/sf/peers/[DC UUID]/ids_forward.conf`
	If the parameter ignore_packet_data is set to 1, then the prohibit packet data on DC is done properly.

--End--

Performing RNA IP/Port Exclusion

Use this procedure for RNA IP/Port Exclusion

Procedure 13
Procedure steps

Step	Action
1	Configure the RNA detection policy and apply the policy.
2	Run the traffic to see the RNA events and flow events for the particular ports and IPs.

3	Configure Exclusion of IP/Port pairs for the RNA Detection Policy
4	Apply the detection policy. The traffic is still seen from the particular ports which is the previous traffic before exclusion of IP/Port.
5	Purge the RNA events and flow events. Wait for 10 minutes for the appliance to exclude the IP/Ports.

--End--

Scanning the NMAP

Use this procedure to troubleshoot an NMAP scan failure.

Procedure 14
Procedure steps

Step	Action
1	Ensure that the scanning host is reachable from DC and IS.
2	Ensure that the scanning host is **A&R, RNA** and then **Network map**.
3	If the scanning host still fails the NMAP scan, enter the following command to debug. Set **sfmgr**and **sftunnel** to debug.
4	Find the sfmgr and sftunnel processes at the following location:**`/etc/sf/PM.conf`**
5	Scan the same host that failed again, by entering the following series of commands. **`option -d`** **`option -f`** **`option /etc/sf/sftunnel.conf`** **`option -D`**.
6	View the error details logged in the following files: **`/var/log/messages`** **`/var/log/httpd/httpsd_error_log`**

--End--

Remediation Procedures

Use these remediation procedues for NSF, SDM, NAS and NSNA.

Remediating NAS

Use this procedure to remediate NAS.

Procedure 15
Procedure steps

Step	Action
1	Add NAS module on the DC.
2	Create compliance rule(s) and policy, and add Nortel123 responses to compliance policy.
3	Add NAS IPaddress.
4	Enable IP ACL, on WEBOS configuration for TPS to enforce blocking the remediation.
5	Enable SSHv2 access to allow Defense Center or RTI Sensor to access the NAS
6	Enable the login display ensuring that the login banner is displayed during every SSH access.

--End--

Troubleshooting Global Faults

This section describes global faults and how to troubleshoot them.

Navigation

- “Viewing remediation log” (page 42)
- “Viewing the LDAP SSL certificate” (page 42)

Troubleshooting when no white list events are generated

This section describes troubleshooting when no white list events are generated for disallowed operating systems, services or appliances.

Procedure 16
Procedure steps

Step	Action
1	Ensure that the RNA is monitoring the hosts in the network.
2	Ensure that the white list is created for the proper network.
3	Ensure that a policy is created and activated for the white list.
4	Ensure that the time range for showing white list events is correct.

--End--

Troubleshooting an IS that does not generate events

This section describes the steps to troubleshoot an IS that does not generate events.

Procedure 17
Procedure steps

Step	Action
1	Ensure that the correct policy is applied.
2	Ensure that the rules are configured properly.
3	Ensure that the rules are selected as **Enable /Drop** in the **Rule State** page.
4	Ensure that the **Time Range** is suitable.

--End--

Troubleshooting an SDM IS that could not be added to a DC

This section describes troubleshooting an SDM IS to be managed by a DC, that could not be added.

Procedure 18
Procedure steps

Step	Action
1	Fill in all the information in the fields marked **required** .
2	Fill in the **optional** field, when there is a known issue that is not fixed yet.

--End--

Troubleshooting an IS that does not block traffic

This section describes troubleshooting an IS that does not block traffic as expected.

Procedure 19
Procedure steps

Step	Action
1	Create the **Interface Set** with the **Inline** or **Inline Failopen**options selected.
2	Configure the IPS policy.
3	Configure the rules and select these rules as the **Drop** status.
4	Ensure that both the hosts are connected to both the **inline** or **Inline Failopen**interfaces.

--End--

Validating the failopen function

This section describes the validation process when the failopen function does not work properly.

Procedure 20
Procedure steps

Step	Action
1	Ensure that the **Interface Set** is **failopen**.
2	Ensure that the policy is **IPS**.
3	Ensure that both **endHosts** are connected to both sides of the **failopen** card.
4	Ensure that the cables are correct.

5	Ensure that the STP is disabled at the switch ports.

--End--

Troubleshooting an IS that does not send email

This section describes troubleshooting an IS that does not send email.

Procedure 21
Procedure steps

Step	Action
1	Check if the **Host Address**is correct.
2	Ensure that the system policy is applied.

--End--

Troubleshooting a DC that cannot push a policy to a sensor that it is managing

Select the IS default detection engine when pushing a policy from the DC.

Troubleshooting a faulty OPSEC

This section describes how to troubleshoot a faulty OPSEC. If the DC and sensors are configured correctly, a trust is established between them. However, if for some reason, the **SFReactd** does not trigger the **fw sam dynamic rule**, stop reimaging the check point firewall PC to make it work.

Procedure 22
Procedure steps

Step	Action
1	Remove the check point **firewall/vpn** if installed on the local PC, so as to enable**SFReactd** to trigger the **fw dynamic rule**.
2	Enter the following command at the DOS command prompt, to check if the firewall policy is installed. `fw stat` Ensure that no **firewall/vpn** is installed on the local check point PC.
3	Ensure that the check point PC has policy options as **any-any**, **except** or **allow**.

4	Ensure that the **https**traffic is allowed between the TPS DC and the check point firewall PC.

--End--

Troubleshooting a failed upgrade

This section outlines the documented mechanism for reverting back to the previous version of code if an upgrade fails. Downgrade is supported from version 4.6.0 (1145 builds) to version 4.5.1.3.

CAUTION
Only **upgrade-revert-upgrade** is supported, not **upgrade-revert-upgrade-revert**.

Procedure 23
Procedure steps

Step	Action
1	When an upgrade fails, enter the following command to revert back to the previous code. `revert`
2	Wait for the system to reboot completely.
3	Login to the Graphical User Interface (GUI). On the menu bar choose **Operation**, **Help** and then **About** to check the reverted software version.

--End--

Troubleshooting a failed automatic SEU Update

This section describes how to troubleshoot an SEU update when the auto update feature is not working. The system responds with the following output message:

```
An error message occurred while running task
```

ATTENTION
This issue has been fixed by Sourcefire and Nortel IT team. Perform the steps in the following procedure if a problem with downloading and importing the SEU still persists.

Procedure 24
Procedure steps

Step	Action
1	Configure the primary DNS server at the following location: **Mgmt Interface/Netmask/Default Network Gateway/Domain/Primary DNS Server**
2	At the TPS IS/DC command line, ping the Nortel update website to see if the associated webpage appears. **www.nortel.autoupdates.com**
3	Ensure that the time settings on both the TPS IS/DC and the local PC are the same. On the menu bar choose **Operation**, **System settings**, **Time** and then **Set Time** to check the time (for example: America/Los Angeles, Tuesday, December 12, 2006) on the TPS. This should match the time on the local PC.
4	Ensure that the SEU downloading and importing are not scheduled to occur at the same time.

--End--

Troubleshooting when a customer is unable to add a sensor to be managed by a DC

This section describes the troubleshooting steps when a customer was not able to add a sensor to be managed by DC. The system responds with the following output message:

```
Could not establish a connection with sensor
```

Procedure 25
Procedure steps

Step	Action
1	Check if the registration keys on the IS and the DC match. On the IS menu bar choose **Operations**, **System Setting**, **Remote Manager** and then **Add Manager** to check the registration key (for example: Nortel). On the DC menu bar choose **Operations**, **Sensor**, and then **Add new sensor** to check the registration key (for example: Nortel)

2	Ensure that the software version on Is 2x70 and DC 2x70 are the same. On the IS and DC menu bar choose **Operations**, **Help**and then **About** to ensure that the software versions are compatible.
3	Ensure that the IS and DC are on the same network and the network is not blocking connection.
4	Check if the status changes from **pending registration**to **registered**, indicating that the sensor **x.x.x.x**is successfully added to the DC

--End--

Troubleshooting a system crash

This section describes the details and files to look into in the event of a system crash. This depends largely on how the system crash is defined for a given incident.

Procedure 26
Procedure steps

Action
Examine the **syslog** at the following location. `/var/log/messages`

Verify the ports to be opened in the firewall for 4.6

The default port is 8305, which is user configurable. For more information, refer section **Remote Management** in the User Guide.

Troubleshooting Snort

This section describes the steps to troubleshoot snort.

Procedure 27
Procedure steps

Step	Action
1	Enter the following command to obtain the snort configuration file **snort.conf**.
2	Enter the following command to view the traffic. `snort -dvei fp1:fp2` OR `snort -dvei bond 0`i
3	Enter the following series of commands for a snort packet capture.

```
cd /var/tmp
mkdir logdir
snort -dvei bond0 (fp1:fp2) -b -l logdir
```

The preceding command will result in a log file as follows:
snort.log.1135279299

4 Enter the following series of commands for a packet capture with tcpdump. Set the parameter **snaplen**to 0, to catch whole packets.

```
cd /var/tmp
tcpdump -I bond0 (fp1:fp2) -s0 -w pcapfile
```

--End--

Troubleshooting memory problems

This section describes the process of troubleshooting memory problems. To track memory issues, the maintenance tool **RPM**must be installed. Once installed the tool does not harm the system.

Procedure 28
Procedure steps

Action

Run the following command to install the RPM that collects data for troubleshooting performance issues.

```
rpm -I Sourcefire_Maintenance_Tools-0.1.0-1.i386.rpm
```

Running the preceding command adds a modified version of top that logs output to the following location every 60 seconds.

```
/var/log/top.log
```

IPS mode cable Deployment Scenarios

This section describes the various IPS mode cable deployment scenarios.

Deploying between two endpoints

- Use two straight through cables to deploy the IPS between 2 end points. No special cabling is needed.
- The sensor supports auto MDI/MDI-X so the link will be negotiated properly when the sensor is in the normal operational state.
- When the sensor is placed into bypass mode it internally implements a crossover and allows normal operation of the connection.

Deploying between two network switches

- Use two straight through cables to deploy the IPS between two network switches. No special cabling is needed.
- The sensor supports auto MDI/MDI-X so the link will be negotiated properly when the sensor is in the normal operational state.
- When the sensor is placed into bypass mode it internally implements a crossover and allows normal operation of the connection.

Between a switch and an endpoint

- When the IPS is deployed between a switch and an endpoint a straight through cable should be used between the switch and the IPS. A crossover cable should be used between the IPS and the endpoint.
- When the sensor is placed into bypass mode the internal crossover and the crossover cable between the endpoint and the IPS will combine to create a straight through cable and allows normal operation of the connection.

Between a switch and a router

- When the IPS is deployed between a switch and a router a straight through cable should be used between the switch and the IPS. A crossover cable should be used between the IPS and the router.
- The sensor supports auto MDI/MDI-X so the link between the IPS and the router will be negotiated properly when the sensor is in the normal operational state.
- When the sensor is placed into bypass mode the internal crossover and the crossover cable between the endpoint and the IPS will combine to create a straight through cable. This will allow normal operation of the connection.

Between a router and an endpoint

- When the IPS is deployed between a router and an endpoint no special cabling is needed. Two straight through cables should be used.
- The sensor supports auto MDI/MDI-X so the link will be negotiated properly when the sensor is in the normal operational state.
- When the sensor is placed into bypass mode it internally implements a crossover and allows normal operation of the connection.

Between a firewall and an endpoint

- When the IPS is deployed between a firewall and an endpoint no special cabling is needed. Two straight through cables should be used.
- The sensor supports auto MDI/MDI-X so the link will be negotiated properly when the sensor is in the normal operational state.
- When the sensor is placed into bypass mode it internally implements a crossover and allows normal operation of the connection.

Between two firewalls

- When the IPS is deployed between two firewalls no special cabling is needed. Two straight through cables should be used.
- The sensor supports auto MDI/MDI-X so the link will be negotiated properly when the sensor is in the normal operational state.
- When the sensor is placed into bypass mode it internally implements a crossover and allows normal operation of the connection.

Between a switch and a firewall

- When the IPS is deployed between a switch and a firewall a straight through cable should be used between the switch and the IPS. A crossover cable should be used between the IPS and the firewall.
- The sensor supports auto MDI/MDI-X so the link between the IPS and the firewall will be negotiated properly when the sensor is in the normal operational state
- When the sensor is placed into bypass mode the internal crossover and the crossover cable between the firewall and the IPS will combine to create a straight through cable. This will allow normal operation of the connection.

Between router and a firewall

- When the IPS is deployed between a router and a firewall no special cabling is needed. Two straight through cables should be used.
- The sensor supports auto MDI/MDI-X so the link will be negotiated properly when the sensor is in the normal operational state.
- When the sensor is placed into bypass mode it internally implements a crossover and allows normal operation of the connection.

Checking IPv6 configurations on the CLI

This section describes checking IPv6 configurations on the command line interface (CLI).

Procedure 29
Procedure steps

Step	Action
1	Enter the following command on the CLI `/var/sf/detection_engines/[uuid]/`
2	Disable **SMTP** globally in **Detection and Prevention** options for a particular policy, when working on the IPv6 partial support feature.

--End--

Verification of Detection Resources on the CLI

This section describes the verification of the maximum and optimal number of detection resources in CLI.

Procedure 30
Procedure steps

Action
Enter the following command in the CLI. `/etc/sf/ims.conf – Search for MAX_NUM_DR/OPTIMAL _NUM_DR`

Viewing the enabled rules on the CLI

This section describes viewing enabled rules on the CLI.

Procedure 31
Procedure steps

Step	Action
1	Enter the following command in the CLI. `/var/sf/detection_engines/[de uuid]/active.rules`.

2 Enter the following command to view the list of rules that are imported in the SEU.
/var/sf/rules/sid-msg.map

--End--

Viewing remediation log

This section describes viewing the remediation log for Nortel Secure Network Access (NSNA) and Nortel VPN Gateway (NVG).

Procedure 32
Procedure steps

Action
View the remediation log at the following location. **/tmp/<RemediationName>/<RemediationName.log>**

Viewing the LDAP SSL certificate

This section describes how to view the LDAP SSL certificate once it is uploaded.

Procedure 33
Procedure steps

Action
Enter the following command to view the LDAP SSL certificate, once it is uploaded. **/var/sf/userauth/temp0.pembl**

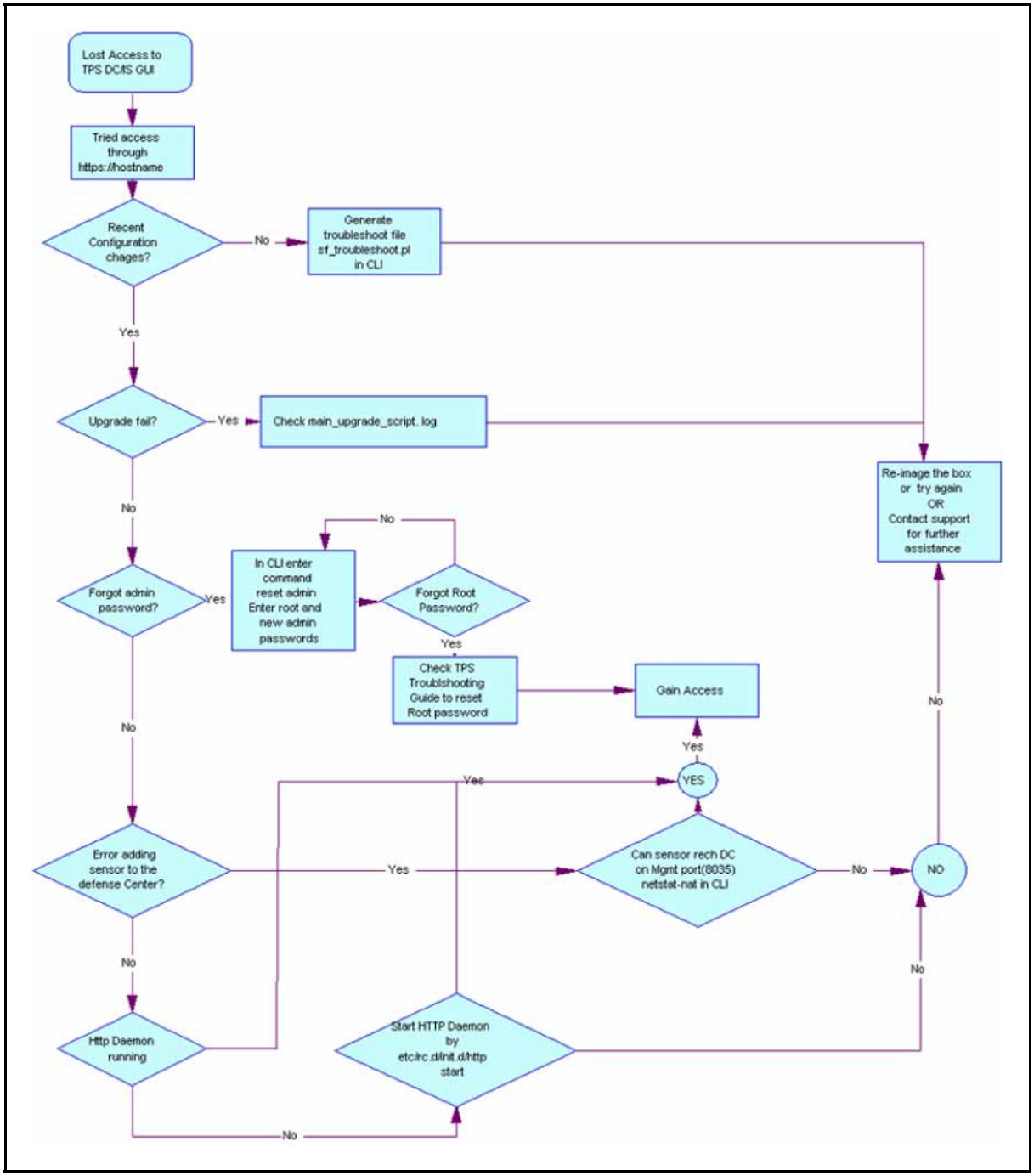
Emergency recovery trees

This chapter provides the procedures to recover from field outages as quickly as possible.

Lost access to the TPS DC/IS device -- recovery tree

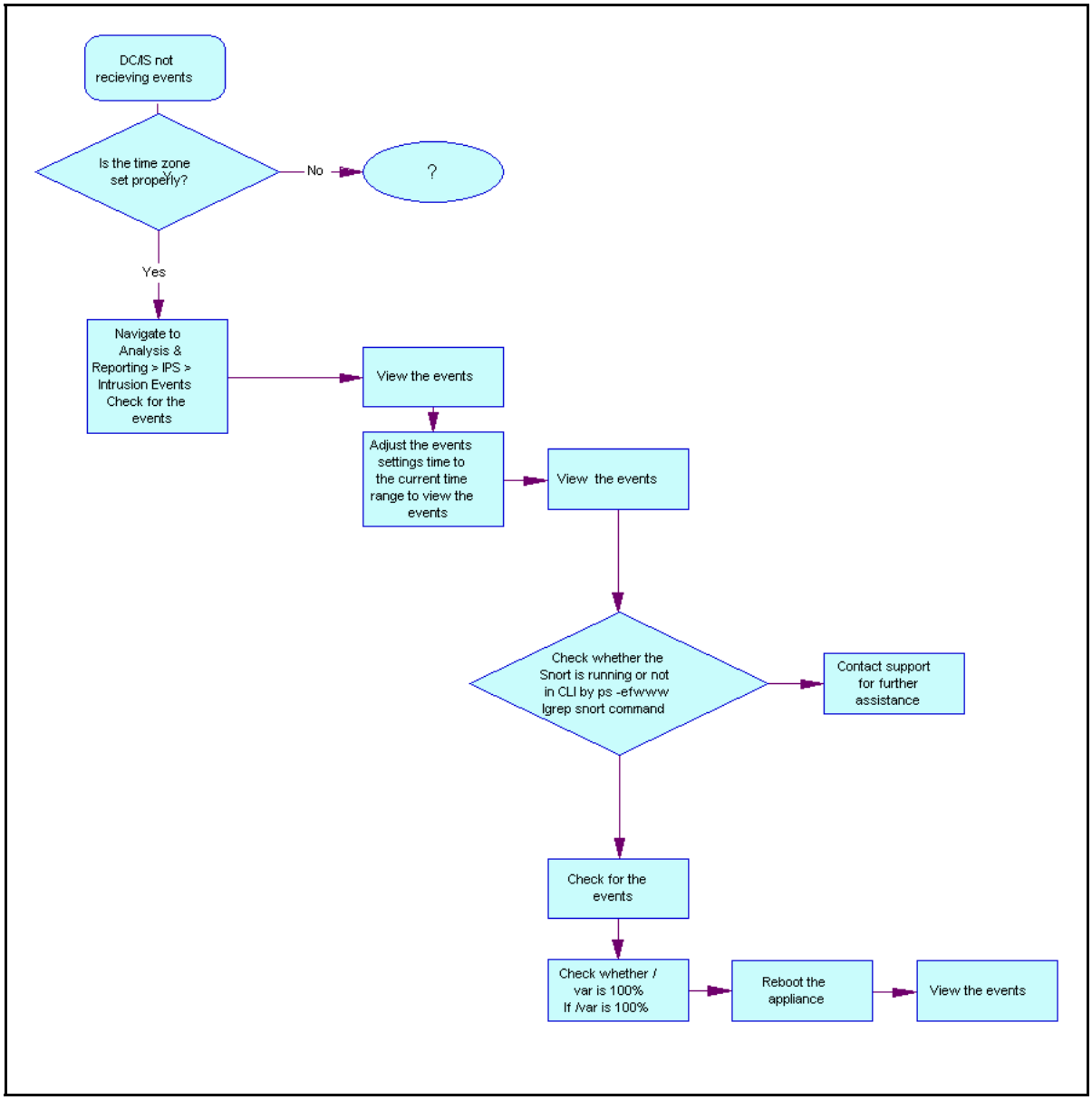
This section details the flow diagram for the recovery tree -- Lost access the TPS DC/IS GUI

Figure 1
Recover lost access to a TPS DC/IS device



The TPS DC/ IS cannot receive events -- recovery tree

This section details the flow diagram for the recovery tree -- The TPS DC/IS does not receive events.



Reference to third party Application Guides

This section contains reference to third party Application Guides for VPN product. You can refer to the following Application Guides available at :

- SSL VPN - Authentication using Steel Belted RADIUS server
- SSL VPN - NTML Authentication
- SSL VPN - CRL retrieval
- SSL VPN - Configuring NetDirect
- SSL VPN - Authentication using certificates
- SSL VPN – Authentication using Netegrity SiteMinder
- SSL VPN - Syslog and Traffic log
- SSL VPN - External Authentication using Remote Authentication Dial-In User Service (RADIUS)
- SSL VPN - External LDAP Authentication using Active Directory
- SSL VPN - Configuring access rules
- SSL VPN - Adding links to a portal page
- SSL VPN - Configuring User Types SSL VPN - Configuring User Types
- Adding a Server Certificate and/or Private Key
- HTTP to HTTPS Redirect Service
- Using Netegrity SiteMinder with Nortel Networks SSL VPN
- Technical Configuration Guide Using Citrix with the Alteon SSL VPN
- SSL VPN and SafeWord for Nortel Technical Config Guide

Contact Nortel technical support

This section provides the information about Nortel technical support.

Navigation

Gathering critical information

Before contacting Nortel Technical Support, you must gather information that can help the technical support personnel when troubleshooting. This section identifies all the critical information that should be gathered before contacting Nortel Technical Support.

You must attempt to resolve your problem using this troubleshooting guide. Contacting Nortel is a final step taken only when you have been unable to resolve the issue using the information and steps provided in this troubleshooting guide.

Gather the following information before contacting Nortel Tech Support. Collecting this information helps Nortel analyze and address the reported issue:

- Detailed description of the problem
- Date and time when the problem started
- Frequency of the problem
- Is this a new installation?

- Have you search the solutions database? Were any related solutions found? Is there currently a workaround for this issue?
- Have you recently changed or upgraded your system, your network, or a custom application? (For example, has any configuration or code been changed?)
  When were these changes made? Provide the date and time. Who made these changes? Were the changes made by a partner or customer? Provide the names of the individuals who made the changes.

Also provide Nortel Technical Support with the following information:

- A copy of your configuration files
- A detailed network topology diagram
- Log files

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/help/contact/global/index.html

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/help/contact/erc/

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Glossary

PERL	
TPS	Threat Protection System
UTC	
NTP	Nortel Technical Publication
LADP	
OS	
RNA	
IS	Intrusion Sensor
STP	
OPSEC	
DNS	
SDM IS	
SEU	Snort Engine Upgrade
LDAP	
MSAD	
RUA	

Nortel Threat Protection System

Threat Protection System Troubleshooting Guide

Release: 4.7
Publication: NN47240-700
Document status: Standard
Document revision: 01.01
Document release date: 11 2007

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the Apache Software Foundation http://www.apache.org/.

This product includes a TAP-Win32 driver derived from the CIPE-Win32 kernel driver, Copyright © Damion K. Wilson, and is licensed under the GPL.

See Appendix D, "License Information", in the *User's Guide* for more information

NORTEL