NORTEL

Nortel Threat Protection System

Troubleshooting Guide

Release: 4.7
Document Revision: 01.02

www.nortel.com

NN47240-700 324442-A

Nortel Threat Protection System
Release: 4.7
Publication: NN47240-700
Document status: Standard
Document release date: 12 February 2008

Sourced in Canada and India

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

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.

Contents

New in this release

The following sections detail what's new in the *Nortel Threat Protection System—Troubleshooting Guide* (NN47240-700) for Nortel Threat Protection System Release 4.7. Refer to the *Nortel TPS 4.7 software Release Notes* (NN47240-400) for the known issues.

Features

This document is the first standard release.

Other Changes

The Nortel Threat Protection System—Troubleshooting Guide (NN47240-700) is a new document for Threat Protection System Release 4.7.

Introduction

This chapter describes the prerequisites and various tools used to troubleshoot the Nortel Threat Protection System (TPS). Use these troubleshooting tools to improve 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.

The Nortel TPS 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 failopen functionality in inline mode.

Prerequisites

The TPS Troubleshooting Guide is intended for use by personnel that install and maintain the TPS products. 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
- Capture and analyze HTTP and HTTPS with Tamper Data, a plug-in available for Mozilla Firefox
- Display the time to load Web pages with Faster Fox, a plug-in available for Mozilla Firefox
- Capture and analyze packets with either Sniffer or Wireshark from Network General and

Navigation

Acronyms

This troubleshooting guide uses the following acronyms.

Table 1
Acronyms

ASOS	Application Switch Operating System
ASEM	Application Switch Element Manager
CLI	Command Line Interface
CPU	Central Processing Unit
DAM	Direct Access Mode
DC	Defense Center
DAM	Direct Access Mode
DNS	Domain Name Server
FDB	Forwarding Database
FTP	File Transfer Protocol
GUI	Graphical User Interface
IDS	Intrusion Detection System
IS	Intrusion Sensor (now 3D Sensor)
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Media Access Control
MIP IP	Mapped IP address
MSTP	Multiple Spanning Tree Protocol

Table 1
Acronyms (cont'd.)

NAS	Nortel Application Switch
NSF	Nortel Switched Firewall
NSNA	Nortel Secure Network Access
NTP	Nortel Technical Publication
SSH	Secure Shell
STG	Spanning Tree Group
TFTP	Trivial File Transfer Protocol
TPS	Threat Protection System
TSDMP	Technical Support Dump
STP	Spanning-Tree Potocol
OPSEC	Operations Security
SEU	Snort Engine Upgrade
SMP	Symmetric Multiprocessing
SFTP	SSH File Transfer Protocol
UTC	Coordinated Universal Time

Troubleshooting Fundamentals

This chapter provides cptual information about the methods and tools that you can use to troubleshoot and isolate problems in the Nortel Threat Protection System (TPS).

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 log file **ssl.log**.

For example, enter the following command to view debug information.**`/maint/debug/proxydebug [on|off|once]`**
where:

Variable	Value
on	enable simpleproxy to print out debug message
off	disable simpleproxy to print out debug message
once	enable simpleproxy to print out only the debug message

> **ATTENTION**
> Enabling proxydebug uses more central processing unit (CPU) resources. Make sure to disable it after you finish debugging.

Transmit the event log from the Nortel VPN Gateway to a file on a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (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.

The following table 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 about the CLI engine and is used by engineering to debug issues while in development.
erlerror	This log provides information about the internal Erlang language engine and SSL acceleration. It is used by Engineers to debug issues in development.
erlstart	This log provides information about the internal Erstart language engine and SSL acceleration. It is used by Engineers to debug issues in development.
conslog	This log contains messages displayed on the console port of the device. These messages are generated during the 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 activate the ssldump.
ikelog	IPsec module related messages.
message	This log contains standard syslog type of messages and contains general information such as system-level status and nonapplication 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 restore the customer and update the document:

- If the DC cannot push a policy to the sensors re-image the box with assistance from Sourcefire.
- If the OPSEC is not working properly and the **SFReactd** does not trigger the **fw same dynamic rule** check if the DC and the sensors are configured correctly and trust is established between them. If not, re-image the box with Sorucefire’s assistance.

- If an upgrade fails, you can revert to a previous version of the code. However, note the following:
  - Examine the problem on a case-by-case basis to determine the root cause because the solution depends on where within the upgrade process, the upgrade failed.
  - If the system is in a dubious state when an upgrade failed, reverting to the previous code exacerbates the problem. In this case report the problem to Sourcefire Support.
  - The process for reverting to the previous version is documented in the User Guides. However that process is recommended only in cases where the upgrade was successful but for one reason or another it was deliberately chosen to revert to the previous version.
- If you cannot add a sensor to a DC.

View the output of sf_troubleshoot.pl

This section describes the various commands used to view the output after running the PERL script **/usr/local/sf/bin/sf_troubleshoot.pl**.

Navigation

View the output of sf_troubleshoot.pl at the command-outputs directory

- Use the following commands to obtain information about the state of the file system, because a full file system can cause unexpected problems.
  `ps, top, df` or **`du`**
- Use the following commands for information about hardware issues.
  `lpsci, dmesg`
- Use the following commands for information about database issues.
  `mysql`
- Use the following commands to compare the timestamp on the sensor and the DC. Time differences between these two devices can cause

many problems.
`date`

- Use the following command to find the snort version on the sensor.
  `ls-Ralsh var-sf-detection_engines-.output`
- Use the following commands to check network connections and IP configuration.
  `netstat, ifconfig`

View the output of sf_troubleshoot.pl in the dir-archives directory

View the following output files in the **/etc/sf** directory.

- The file `ims.conf` to confirm the version and the management interface.
- The **licence** file and the **licence.d** directory.
- The **troubleshoot.conf** file. If required, comment out the **myisamchk** line in the file.
- The **sftunnel.conf** file. This file is useful to review the peers. Obtain the troubleshoot file with tunnel issues from both the DC and Sensor for effective troubleshooting.

The following important log files can be viewed at the **var-log** directory.

- **Message** logs
- **Cron** logs
- **Upgrade** logs
  These files are in the **sf** directory.
- **Apache error** logs
  These files are in the **httpd** directory and contain policy related problems.

View the file content

This section describes the file content at various locations. The following are the locations to view them.

- Directory **var/sf/detection_engines**:
  - sensor DE data minus the log files
  - active.rules
  - snort.conf
  - de.info

— de.conf

— instance – 1(2) directories that are useful for statistics

Enter the command
cat now
The 3rd column from left on the output is the speed in Mbps. On the sensor, use the **perfstats** utility, by entering the following command

```
cat now|perfstats
```

A **syns** vs **syn-acks** imbalance indicates asynchronous routing.

- Directory **var/lib/mysql**.
  Find information here on slow queries from mysql.
- Directory **tmp**
  Find the **update.status** file where the latest upgrade/patch redirects logs are located. You can also find the **update.lock** file here.

Open ports in a firewall

If there are one or more firewalls in between the DC and IS open one or more ports on the firewall, depending on the software version of the TPS devices.
For **software release 4.5.x and later**, the DC and the IS only communicate on TCP port 8305, by default. However, the administrator can change this port number.
For **software release 4.1.x and earlier**,
the DC and the IS 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

Hardware Troubleshooting

This chapter provides information to troubleshoot problems related to the Threat Protection System (TPS) hardware.

Navigation

Troubleshoot TPS Hardware through LED indications

This section provides information to troubleshoot hardware problems related to the TPS 2050, TPS 2070, TPS 2150, and TPS 2170 devices. The following table describes the Front Panel LED indicators on the TPS device.

> **ATTENTION**
> Call Nortel for RMA if the Amber System status LED cannot be cleared.

Table 3
Front Panel LEDs

LED Indicator (from left to right)	Description
Amber system status LED OR System status LED	This LED lights up when the system needs attention due to a problem with power supplies, fans, CPU, or system temperature or hard drives.
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.
Overheat indicator LED	This LED is red when the system overheats.

Software Troubleshooting

This chapter describes the various procedures to troubleshoot the software on the Threat Protection System (TPS) devices.

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 4.7 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 following are the software file names for release 4.7:

- 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)

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 required.

> **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 (NN47240-400) for information about 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_scr
ipt.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.

Navigation

- “Resetting the root password of a TPS device” (page 24)
- “Resetting the administrator password for a TPS device” (page 25)

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.

```
LILO 22.2 boot: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

Use this procedure to 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 "Resetting the root password of a TPS device" (page 24), 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 older version of SEU

Use this procedure to install a lower version of Snort Engine Upgrade (SEU), 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--

Handling events

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

Navigation

- “Troubleshooting TPS Sensor when not receiving events” (page 27)
- “Troubleshooting Defense Center when not receiving events” (page 27)

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 27) 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 when not running ” (page 28) 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>
```

4 Delete the IP address of the DC, if it exists.

5 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
```

6 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
```

7 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 when not running

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.

Navigation

- "Troubleshooting mail alerting problems" (page 29)
- "Troubleshooting SNMP alerting problems" (page 29)
- "Troubleshooting syslog alerting problems" (page 30)

Troubleshooting mail alerting problems

Use this procedure to troubleshoot 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 through the DNS.
5	Enter the following command to add hostname information. `/etc/hosts`

--End--

Troubleshooting SNMP alerting problems

Use this procedure to troubleshoot SNMP alerting problems.

Procedure 9
Procedure steps

Step	Action
1	Check if SNMP is running.
2	Restart the process if SNMP is not currently running.

--End--

Troubleshooting syslog alerting problems

Use this procedure to troubleshoot syslog alerting problems.

Procedure 10
Procedure steps

Step	Action
1	Check if syslog is running.
2	Restart the process if syslog is not currently running.

--End--

Troubleshooting events that show incorrect time

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

Procedure 11
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 failure

Use this procedure to troubleshoot LDAP authentication failure.

Procedure 12
Procedure steps

Step	Action
1	Ensure that the user test passes when creating the LDAP object.
2	If the user authentication 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
3	Set the authentication status as **enabled**.
4	Activate the LDAP object under the system policy. Apply the system policy only after activating the LDAP object.
5	Ensure that the user for authentication is created using external authentication method.

6	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-----`

7	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.
8	Obtain the SSL certificate.

9 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.

--End--

Creating RUA

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

Configuring snort through the user interface

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

Procedure 13
Procedure steps

Step	Action
1	Manually add the following variable to provide raw snort configuration through the user interface. **USER_CONF**
2	Apply the policy to store data in the variable **$USER_CONF** at 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 14
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, it implies that the prohibit packet data on DC is done properly.

--End--

Performing RNA IP/Port Exclusion

Use this procedure for RNA IP/Port Exclusion.

Procedure 15
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 ten minutes for the appliance to exclude the IP/Ports.

--End--

Scanning the NMAP

Use this procedure to troubleshoot an NMAP scan failure.

Procedure 16
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--

Remediating Nortel Equipment

This section describes interaction with other Nortel equipment like Nortel Switched Firewall (NSF), Nortel Service Delivery Module 8600 (SDM), Nortel Application Switch (NAS), and the Nortel Secure Network Access (NSNA). Use the following procedures for the remediation of this equipment.

Navigation

- “Remediating NAS” (page 34)
- “Remediating NSF” (page 35)
- “Remediating SDM” (page 36)
- “Remediating NSNA” (page 36)

Remediating NAS

Use this procedure to remediate NAS.

Procedure 17
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--

Remediating NSF

Use this procedure to remediate NSF.

Procedure 18
Procedure steps

Step	Action
1	On TPS DC, add CheckPoint OPSEC SAM version 1.0. On the menu bar select **Policy and Response**, **Responses**, **Remediation**, and then **Instances**.
2	Add the OPSEC application name that is the one you create on CheckPoint OPSEC. For example: **TPS_SAM**
3	Configure the remediation name. For example: • Nortel123 action: Inhibit and closed • logging level: alert • firewall object: all • match protocol: on
4	Create compliance rule(s) and policy, and add Nortel123 responses to compliance policy.
5	On NSF, configure ports mirror on client and server port and port monitor to the HUB.

Step	Action
6	On TPS remediation result message, change the start date and end date. For example: • start date: 12/12/07 • end date: 12/14/07

--End--

Remediating SDM

Use this procedure to remediate SDM.

Procedure 19
Procedure steps

Step	Action
1	Create compliance rule(s) and policy, and add Nortel123 responses to compliance policy.
2	Configure the port mirroring on PP8600. For example create: • in-port in mode: 9/6 • out-port in mode: 3/15 Port 9/6 is SDM data port. Port 3/15 is the monitoring port to the HUB. Traffic is mirrored by both these ports.

--End--

Remediating NSNA

Use this procedure to remediate NSNA.

Procedure 20
Procedure steps

Step	Action
1	Add NSNA module on the DC.
2	Add MIP IP address.
3	Create compliance rule(s) and policy, and add Nortel123 responses to compliance policy.
4	Configure port mirror on the client port and port monitor with NSNA enable.

5 On TPS remediation result message, change the start date and end date. For example:

- start date: 12/12/07
- end date: 12/14/07

--End--

Troubleshooting Global Faults

This section describes global faults and how to troubleshoot them.

Navigation

Troubleshooting when no white list events are generated

Use this procedure to troubleshoot when no white list events are generated for disallowed operating systems, services or appliances.

Procedure 21
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

Use this procedure to troubleshoot an IS that does not generate events.

Procedure 22
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 cannot be added to a DC

Use this procedure to troubleshoot an SDM IS to be managed by a DC, that cannot be added.

Procedure 23
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

Use this procedure to troubleshoot an IS that does not block traffic as expected.

Procedure 24
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

Use this procedure to validate the failopen function if it does not work properly.

Procedure 25
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

Use this procedure to troubleshoot an IS that does not send email.

Procedure 26
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

Select the IS default detection engine when pushing a policy from the DC to a sensor that it is managing.

Troubleshooting a faulty OPSEC

Use this procedure 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 CheckPoint firewall PC to make it work.

Procedure 27
Procedure steps

Step	Action
1	Remove the CheckPoint **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 CheckPoint PC.
3	Ensure that the CheckPoint PC has policy options as **any-any**, **except** or **allow**.
4	Ensure that the **https** traffic is allowed between the TPS DC and the CheckPoint firewall PC.

--End--

Troubleshooting a failed upgrade

Use this procedure to revert 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 28
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

Use this procedure 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 is 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 29
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 web site to see if the associated web page 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 must 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 cannot add a sensor to be managed by a DC

Use this procedure when you cannot add a sensor to be managed by DC. The system responds with the following output message:

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

Procedure 30
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

To troubleshoot a system crash, examine the **syslog** files 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

Us this procedure to troubleshoot snort.

Procedure 31
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 0i
```

3 Enter the following series of commands for a snort packet capture.

```
cd /var/tmp
mkdir logdir
snort -dvei bond 0 (fp1:fp2) -b -l logdir
```

The preceding command results 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

Use this procedure to troubleshoot memory problems. To track memory issues, the maintenance tool `RPM` must be installed. Once installed, the tool does not harm the system.

Procedure 32
Procedure steps

Step	Action
1	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`
2	Add a modified version of top that logs output to the following location every 60 seconds on running the preceding command. `/var/log/top.log`

--End--

Deploying IPS mode cable—Scenarios

This section describes the various IPS mode cable deployment scenarios.

Navigation

Deploying between two endpoints

- Use two straight through cables to deploy the IPS between two end points. No special cabling is needed.
- The sensor supports auto MDI/MDI-X so the link negotiates 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 is 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 a switch and an endpoint

- When the IPS is deployed between a switch and an endpoint a straight through cable must be used between the switch and the IPS. A crossover cable must 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 combines to create a straight through cable that allows normal operation of the connection.

Deploying between a switch and a router

- When the IPS is deployed between a switch and a router a straight through cable must be used between the switch and the IPS. A crossover cable must be used between the IPS and the router.
- The sensor supports auto MDI/MDI-X so the link between the IPS and the router negotiates 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, combines, to create a straight through cable. This allows normal operation of the connection.

Deploying 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 must be used.
- The sensor supports auto MDI/MDI-X so the link negotiates 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 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 must be used.
- The sensor supports auto MDI/MDI-X so the link negotiates 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 firewalls

- When the IPS is deployed between two firewalls no special cabling is needed. Two straight through cables must be used.
- The sensor supports auto MDI/MDI-X so the link negotiates 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 a switch and a firewall

- When the IPS is deployed between a switch and a firewall a straight through cable must be used between the switch and the IPS. A crossover cable must be used between the IPS and the firewall.
- The sensor supports auto MDI/MDI-X so the link between the IPS and the firewall negotiates 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 combinesto create a straight through cable. This allows normal operation of the connection.

Deploying 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 must be used.
- The sensor supports auto MDI/MDI-X so the link negotiates 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

Use this procedure to check IPv6 configurations on the command line interface (CLI).

Procedure 33
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

Use this procedure to verify the maximum and optimal number of detection resources in CLI.

Procedure 34
Procedure steps

Step	Action
1	Enter the following command in the CLI to verify the maximum number of detection resources. `/etc/sf/ims.conf` and search for **MAX_NUM_DR**.
2	Enter the following command in the CLI to verify the maximum number of detection resources. `/etc/sf/ims.conf` and search for **OPTIMAL_NUM_DR**.

--End--

Viewing the enabled rules on the CLI

Use this procedure to view enabled rules on the CLI.

Procedure 35
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

Use this procedure to view the remediation log for Nortel Secure Network Access (NSNA) and Nortel VPN Gateway (NVG).

Procedure 36
Procedure steps

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

Viewing the LDAP SSL certificate

Use this procedure to view the LDAP SSL certificate after it is uploaded.

Procedure 37
Procedure steps

Step	Action
1	Load the LDAP SSL certificate.
2	Enter the following command to view the LDAP SSL certificate, after it is uploaded. `/var/sf/userauth/temp0.pembl`

--End--

Emergency recovery trees

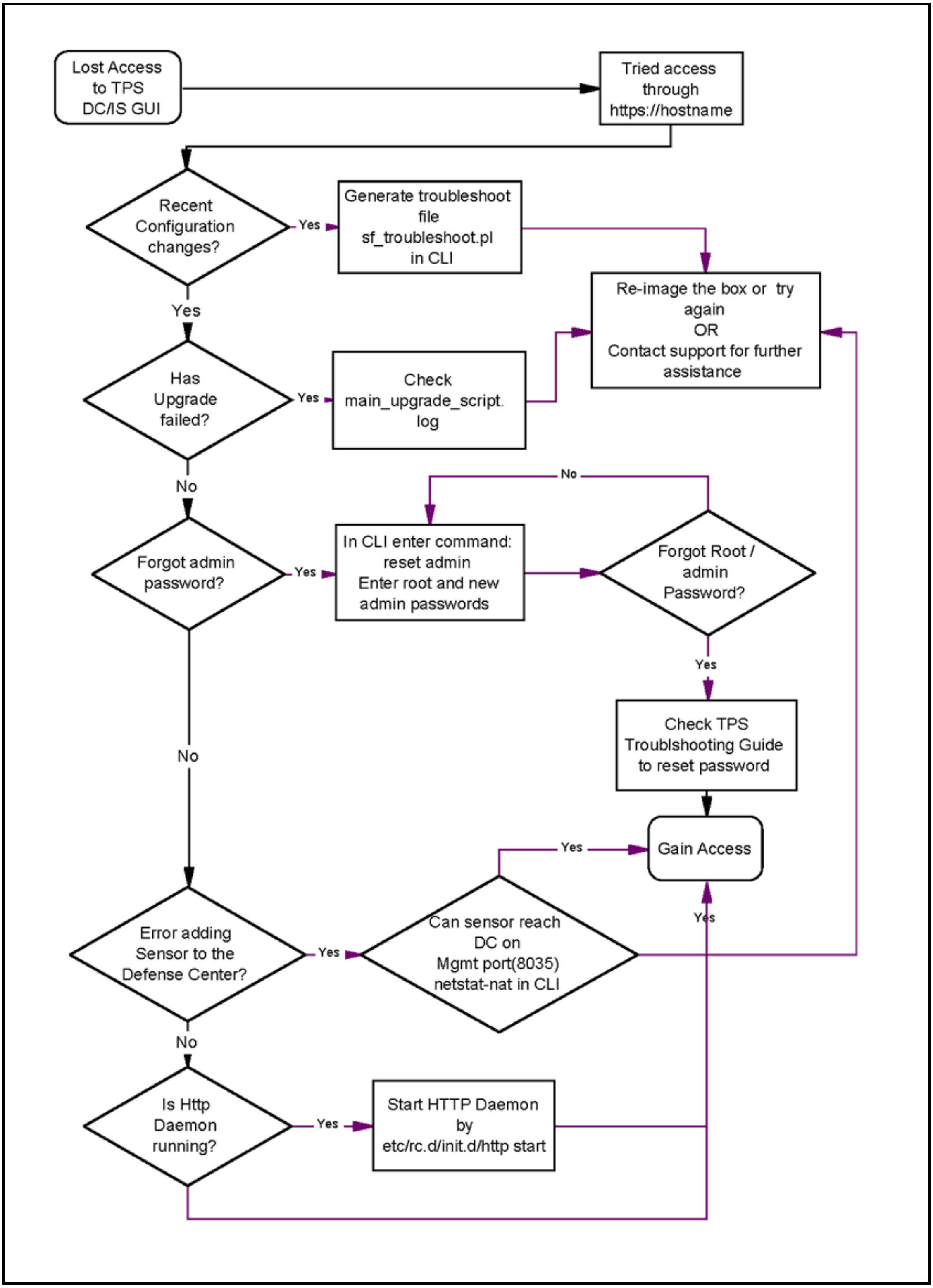
This chapter illustrates the emergency recovery tree flow diagrams that help recover from field outages as quickly as possible.

Navigation

Lost access to the TPS DC/IS device—emergency recovery tree

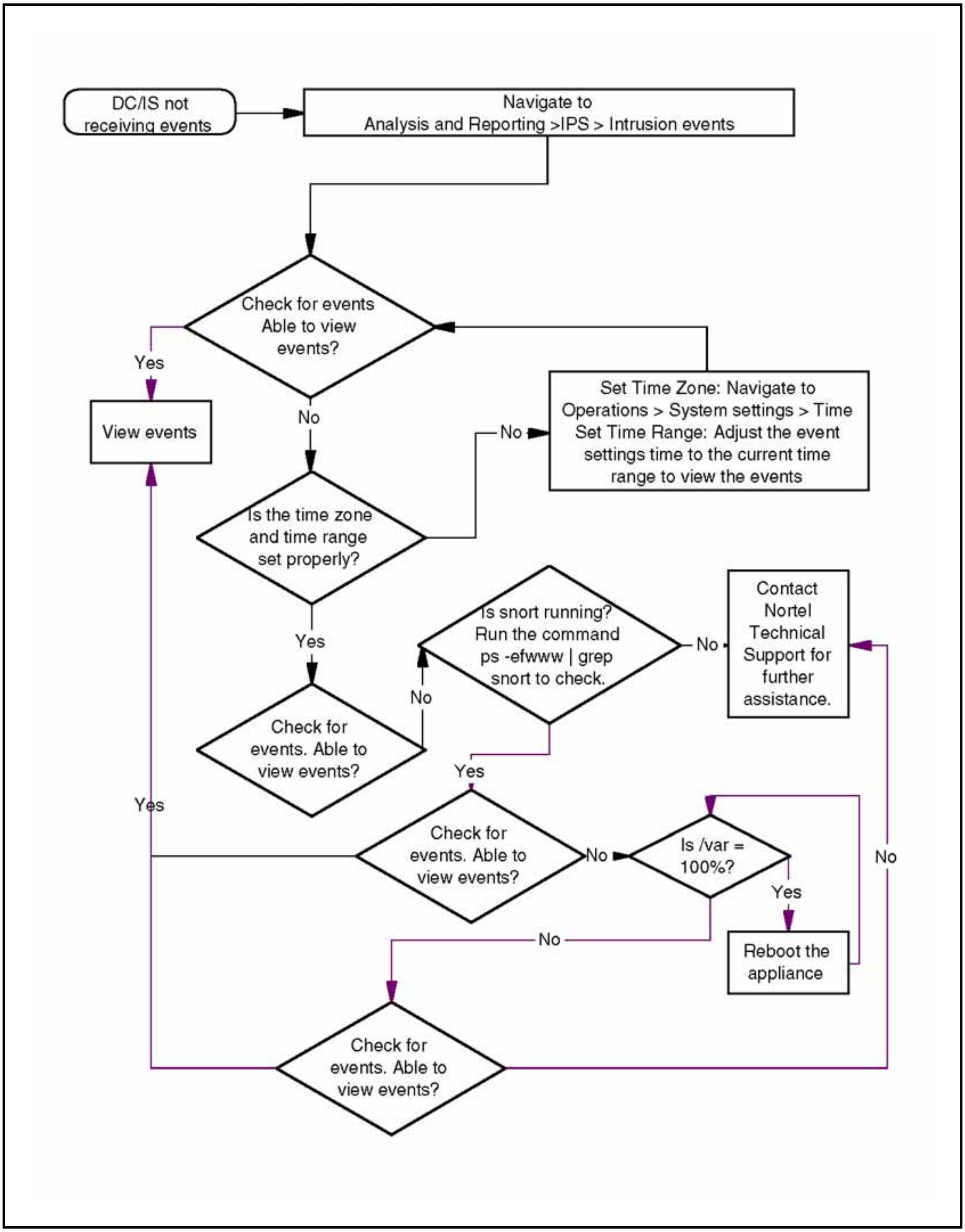
The following flow diagram illustrates the recovery tree when access is lost to the TPS DC/IS Graphical User Interface (GUI).

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


Lost Access to TPS DC/IS GUI
Tried access through https://hostname
Recent Configuration changes?
Yes
Generate troubleshoot file sf_troubleshoot.pl in CLI
Re-image the box or try again OR Contact support for further assistance
Yes
Has Upgrade failed?
Yes
Check main_upgrade_script.log
No
No
Forgot admin password?
Yes
In CLI enter command: reset admin Enter root and new admin passwords
Forgot Root / admin Password?
Yes
Check TPS Troublshooting Guide to reset password
No
Yes
Gain Access
Yes
Error adding Sensor to the Defense Center?
Yes
Can sensor reach DC on Mgmt port(8035) netstat-nat in CLI
No
Is Http Daemon running?
Yes
Start HTTP Daemon by etc/rc.d/init.d/http start

TPS DC/IS cannot receive events—emergency recovery tree

The following flow diagram illustrates the recovery tree when TPS DC/IS cannot receive events.


DC/IS not receiving events
Navigate to Analysis and Reporting >IPS > Intrusion events
Check for events Able to view events?
Yes
View events
No
Set Time Zone: Navigate to Operations > System settings > Time Set Time Range: Adjust the event settings time to the current time range to view the events
No
Is the time zone and time range set properly?
Yes
Is snort running? Run the command ps -efwww | grep snort to check.
No
Contact Nortel Technical Support for further assistance.
No
Check for events. Able to view events?
Yes
Yes
Check for events. Able to view events?
No
Is /var = 100%?
Yes
No
Reboot the appliance
No
Check for events. Able to view 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 http://support.nortel.com/go/main.jsp:

- 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, gather the following critical information that can help the technical support personnel when troubleshooting.

You must attempt to resolve your problem using this troubleshooting guide. Contacting Nortel is a final step taken only when you cannot resolve the issue using the information and steps provided in this troubleshooting guide. Collecting this information helps Nortel analyze and address the reported issue:

- A detailed description of the problem.
- The date and time when the problem started.
- The frequency of the problem.
- Is this a new installation?
- Have you searched 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, is any configuration or code changed?)

If yes, when (date and time) were these changes made? 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.
- The 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 web site allows 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.

Nortel Threat Protection System

Troubleshooting Guide

Release: 4.7
Publication: NN47240-700
Document status: Standard
Document revision: 01.02
Document release date: 12 February 2008

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

www.nortel.com

Sourced in Canada and India

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

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