Nortel Threat Protection System 3.2

Release Notes

part number: 318730-A, January 2005

4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
http://www.nortelnetworks.com

Release Notes

This document contains the latest information about the Nortel Networks Threat Protection System release 3.2. The Nortel Threat Protection System is a fully integrated intrusion detection system (IDS) that consists of:

- 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.

Features and Functionality

TPS 2070 Defense Center

The TPS 2070 Defense Center contains the following features and functionality in release 3.2:

- A web-based interface allows management of the Defense Center through a web browser using a Secure Socket Layer (SSL) connection. The web browser must support JavaScript, cookies, and the SSL protocol.
- Configurable user accounts allow the system administrator to customize user access based on the tasks the users perform. The five types of user accounts are:
  - Admin Access
  - Data Access
  - Restricted Data Access
  - Maintenance Access
  - Rules Access
- The establishment of sensor groups allows the application of policies and rules to clusters of intrusion sensors. This eases the management of intrusion sensors by allowing a group to be treated as a single entity.

- Intrusion detection policies define how the intrusion sensors inspect network traffic. Default policies are included with the Defense Center but the creation of custom rules is fully supported.
- The Defense Center supports dynamic load balancing across intrusion sensors that are on the same network segment and that were previously configured for management by the Defense Center. This feature allows the creation of load balancing groups and the application of common policies across the managed sensors. This feature combined with the high availability features of the Defense Center provides operational continuity.
- Two Defense Centers can be configured to act in a primary/secondary console configuration. This configuration provides high availability and failover support when managing Intrusion Sensors.
- When an intrusion is detected, events are generated to define the type of intrusion. The **Event Summary** page gives an overview of these events as well as a quick overview of the current Defense Center status.
- Event graphs allow the user to graphically represent the following information over the range of the last hour, last day, last week, and last month:
  - Top 10 destination ports
  - Top 10 source IP addresses
  - Top 10 event messages
- Event workflows allow the user to investigate intrusion occurrences. Default workflows are provided with the Defense Center. In addition to these default workflows, custom workflows enable the administrator to tailor the event pages that investigate intrusion events.
- Event pages analyze individual intrusion events. The three types of event pages are:
  - Drill-down view
  - Table view
  - Packet view

  Once an event is viewed through an event page, it is marked as reviewed and is no longer presented on an event page. These events are, however, still stored in the event database.

- Bookmarking capabilities allow any user with unrestricted data access to return quickly to a specific point in the event analysis process. Bookmarks retain information about:
  - the workflow being used
  - the portion of the workflow being viewed
  - workflow page number
  - selected time range
- The Defense Center web interface integrates Whois functionality to allow quick look up of an IP address from within the management interface.
- An integrated clipboard allows for the storage of up to 25 000 events for later inspection.
- The Defense Center can search for events based on a number of criteria. Commonly used searches can be saved publicly or privately and the results used to form the basis of a custom report profile. Default searches are also included to aid in quickly looking for anomalous network activity.
- Incident handling facilities in the Defense Center allow for the creation and tracking of an intrusion event. Incident handling supports the concept of an incident lifecycle. That is, as the investigation of an incident progresses, the status of the incident changes as data about the event is stored with the incident.
- Incident reports based on stored incidents can be produced. These incident reports can include a summary of an incident, status information, comments, and the event information that originally led to the creation of the incident.
- The Defense Center supports the ability to fully configure the notification process for an intrusion event. This includes the ability to:
  - limit how many times a particular intrusion event is brought to the attention of the system administrator
  - provide notification of an event through Simple Network Management Protocol (SNMP) devices, e-mail, or an external system log.
  - integrate with a Check Point firewall to respond to an intrusion event
- Report generation gives the system administrator many options for representing event data. Reports can be created from one or more events currently being viewed, or they can be defined using report profiles. Report profiles give the system administrator the flexibility to create dynamic reports based on selected criteria. Report profiles are stored on the system and are available until removed.

- A scheduler is available to handle recurring tasks. The scheduler can automate the following tasks:
  - system backups
  - report generation
  - application of intrusion detection policies
- The Defense Center can function as a Dynamic Host Configuration Protocol (DHCP) client.
- The Defense Center can function either as a Nortel Networks internal time server or a Network Time Protocol (NTP) server. The Defense Center can also act as clients to either service.

TPS 2050 and TPS 2070 Intrusion Sensor

The TPS 2050 and TPS 2070 Intrusion Sensor contains the following features and functionality in release 3.2:

- A web-based interface allows management of the Intrusion Sensor through a web browser using a Secure Socket Layer (SSL) connection. The web browser must support JavaScript, cookies, and the SSL protocol.
- Configurable user accounts allow the system administrator to customize user access based on the tasks the users perform. The five types of user accounts are:
  - Admin Access
  - Data Access
  - Restricted Data Access
  - Maintenance Access
  - Rules Access
- When an intrusion is detected, events are generated to define the type of intrusion. The **Event Summary** page gives an overview of these events as well as a quick overview of the current Intrusion Sensor status.

- Event graphs allow the user to graphically represent the following information over the range of the last hour, last day, last week, and last month:
  - Top 10 destination ports
  - Top 10 source IP addresses
  - Top 10 event messages
- Event workflows allow the user to investigate intrusion occurrences. Default workflows are provided with the Intrusion Sensor. In addition to these default workflows, custom workflows enable the administrator to tailor the event pages that investigate intrusion events.
- Event pages analyze individual intrusion events. The three types of event pages provided are:
  - Drill-down view
  - Table view
  - Packet view

  Once an event is viewed through an event page, it is marked as reviewed and is no longer presented on an event page. These events are, however, still stored in the event database.
- Bookmarking capabilities allow any user with unrestricted data access to return quickly to a specific point in the event analysis process. Bookmarks retain information about:
  - the workflow being used
  - the portion of the workflow being viewed
  - workflow page number
  - selected time range
- The Intrusion Sensor web interface integrates Whois functionality to allow quick look up of an IP address from within the management interface.
- An integrated clipboard allows for the storage of up to 25 000 events for later inspection.
- The Intrusion Sensor can search for events based on a number of criteria. Commonly used searches can be saved publicly or privately and the results used to form the basis of a custom report profile. Default searches are also included to aid in quickly looking for anomalous network activity.
- Incident handling facilities in the Intrusion Sensor allow for the creation and tracking of an intrusion event. Incident handling supports the concept of an incident lifecycle. That is, as the investigation of an incident progresses, the status of the incident changes as data about the event is stored with the incident.

- Incident reports based on stored incidents can be produced. These incident reports can include a summary of an incident, status information, comments, and the event information that originally led to the creation of the incident.
- The Intrusion Sensor supports the ability to fully configure the notification process for an intrusion event. This includes the ability to:
  - limit how many times a particular intrusion event is brought to the attention of the system administrator
  - provide notification of an event through Simple Network Management Protocol (SNMP) devices, e-mail, or the use of an external system log.
  - integrate with a Check Point firewall to respond to an intrusion event
- Report generation gives the system administrator many options for representing event data. Reports can be created from one or more events currently being viewed or they can be defined using report profiles. Report profiles give the system administrator the flexibility to create dynamic reports based on selected criteria. Report profiles are stored on the system and are available until removed.
- A scheduler is available to handle recurring tasks. The scheduler can automate the following tasks:
  - system backups
  - report generation
  - application of intrusion detection policies
- The Intrusion Sensor can function as a Dynamic Host Configuration Protocol (DHCP) client.
- The Intrusion Sensor can function either as a Nortel Networks internal time server or a Network Time Protocol (NTP) server. Intrusion Sensors can also act as clients to either service.
- The Intrusion Sensor generates audit records for every action performed in the user interface. This includes viewing, deleting, reviewing, and unreviewing events; changing system settings; and logging out of the system.
- The Intrusion Sensor can be configured to send e-mail notifications when the intrusion event database and audit log are pruned using the **Delete Notification Address** field.
- The “From Beginning” option of the **byte_jump** content keyword allows for the creation of intrusion rules that skip a calculated number of bytes from the beginning of the packet payload instead of skipping bytes from the end of the calculated byte segment.
- The “Multiplier” option of the **byte_jump** content keyword allows for the creation of intrusion rules that, after calculating the number bytes to skip, multiples the initially calculated number of bytes by the integer specified for the option. The intrusion rule then uses this number to skip forward the calculated number of bytes in the packet.

Compatibility

Hardware Compatibility Matrix

Table 1 indicates which versions of the TPS 2070 Defense Center are compatible with each version of the TPS 2050 Intrusion Sensor and TPS 2070 Intrusion Sensor.

Table 1 Nortel Threat Protection System Hardware Compatibility

Defense Center Versions	Intrusion Sensor Versions
TPS 2070 Defense Center release 3.2	TPS 2050 Intrusion Sensor release 3.2 TPS 2070 Intrusion Sensor release 3.2

For reference, the part numbers for each unit in the Nortel Threat Protection System are:

- TPS 2070 Defense Center - EB1639142
- TPS 2050 Intrusion Sensor - EB1639140
- TPS 2070 Intrusion Sensor - EB1639141

Hardware Installation

Refer to the appropriate installation guides for complete instructions on the installation of the TPS 2070 Defense Center, TPS 2050 Intrusion Sensor, or TPS 2070 Intrusion Sensor. This documentation is provided on the product's *Documentation and Restore CD* and can also be accessed on the Nortel Networks Support web site.

Software Installation

General Software Information

The TPS 2070 Defense Center, TPS 2050 Intrusion Sensor, and TPS 2070 Intrusion Sensor products are pre-loaded with release 3.2 of the software. The software is also available on a CD that is shipped with the hardware and is available on the Nortel Networks web site for contracted customers.

The software file names for release 3.2 are:

- **TPS_2070_DC_NORTEL_3.2.0-Restore.iso** (TPS 2070 Defense Center)
- **TPS_2050_IS_NORTEL_3.2.0-Restore.iso** (TPS 2050 Intrusion Sensor)
- **TPS_2070_IS_NORTEL_3.2.0-Restore.iso** (TPS 2070 Intrusion Sensor)

Updating Software

Updates for the Defense Center and Intrusion Sensor software are distributed electronically and can be downloaded from the hardware web interface. Refer to the section entitled "Remote Update Distribution" in the Defense Center and Intrusion Sensor User Guides for complete instructions on performing this task. These user guides are:

- *TPS 2070 Defense Center User's Guide* (Part Number 216886-A)
- *TPS 2050 and TPS 2070 Intrusion Sensor User's Guide* (Part Number 216884-A)

Updating Intrusion Rule Packs

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

Software Feature Limitations

TPS 2070 Defense Center

The feature set in release 3.2 of the TPS 2070 Defense Center software has the following known limitations:

- Flow-portscan events appear with a source and destination port of N/A, but N/A is not an option on the **Event Search** page when searching for this type of event.
  - To find all flow-portscan events, enter the flow-portscan generator ID (121) in the **Generator** field as the search criterion.
- If two user-defined variables that begin with the same string exist, and one of the variables is in use in an intrusion detection policy, the other unused variable cannot be deleted.
- After configuring Check Point firewall responses in the creation of a custom intrusion detection policy, the success message that the system presents does not clearly indicate how the policy was modified.

- The product documentation does not state that the clipboard has a capacity of 25 000 intrusion events.
- If a syntax error is present when saving a rule in the **Rule Editor**, the contents of the **Rule Editor** are cleared and a error message appears. The rule must then be re-created from the beginning.
- If a custom rule classification has been applied to an Intrusion Sensor through an IDS policy, do not delete it.
- If a custom incident type has been used with an incident, do not delete it.
- Adding a column for Reviewed status on a custom workflow results in the corresponding event page only showing unreviewed events.
  - As a solution, add the Reviewed status column and use the "Reviewed/Unreviewed" search option in the **Event Search** page. The resulting event pages include a Reviewed column and indicate whether or not the events have been reviewed.
- If account privileges are reduced to Maintenance access while logged in with Admin access, log out and log in to have the Admin access restored.
- Ensure that private searches are used as restriction criteria for Restricted Data User accounts. If private searches are not used as criteria, restricted users can edit the search and change their own restrictions.
- If possible, avoid using all numeric characters for sensor names. Event searches conducted on sensors with completely numeric names can produce unexpected results.
- Anomalies in the sfmbproxy and watchdog processes may cause multiple instances of defunct sfmbproxy processes to appear in the process list. These should clear over time without user intervention.
- In High Availability situations, the Defense Center that is acting in a secondary role cannot automatically be replaced with another Defense Center.
  - To switch which Defense Center is acting in the secondary role, make a backup of the original, secondary Defense Center and restore the backup to the new secondary Defense Center. Once the restoration process has been successfully completed, a connection is automatically made to the primary Defense Center.
- Reconfiguration of a heavily loaded Defense Center that is monitoring 40 or more sensors may result in the Defense Center refusing to process events transmitted by the registered sensors.
  - If this behavior is noticed, reboot the Defense Center to restart event processing.
- The Defense Center interface allows the creation of duplicate and blank sensor group names. This behavior is incorrect.

- When viewing the list of generated reports on the **Report** page, the default file name in the Download option is always *view.cgi*. Rename the file and ensure that the file extension is appropriate for the type of file that you wish to create. For example, ".pdf" for a PDF file, ".csv" for a CSV file, and so on.
- The successful addition of an Intrusion Sensor to a Defense Center may result in the sensor being listed as having out-of-date intrusion detection policies. These messages can be safely ignored, but sensors should be updated if the policy is changed later.
- After creating an IDS e-mail alert, a recurring task called JobSFMail is added to the scheduler. The start date of this task is set to December 31, 1969 and an entry appears in the calendar for each instance back to 1969.
- If necessary, set the time back manually by setting the drop-down options that appear on the page.
- When creating a new Backup job type in the **New Task** option on the **View Schedules** page, be aware of a certain page behavior. If you select the **Event** or **Configuration** check boxes and then change the **Task Type** between **Once** and **Recurring**, the check boxes become de-selected. Ensure that you manually re-select the appropriate check box after making such a change.
- To ensure that the Defense Center can send e-mail notifications, correctly configure the **Host Name** and **Domain** on the **Network Settings** page. Refer to the User Guide for configuration instructions. If the Defense Center is set up to be a DHCP client, ensure that the DHCP server provides the Defense Center with a host name.
- No error message is supplied if an e-mail address is specified in the **Email Status To** field on the **Scheduler** page without first setting up the **Mail Relay Host** on the **Configure Email Notification** page.
- The **Configure Email Notification** page incorrectly states a default value of *mail* in the **Mail Relay Host** field. There is in fact no default mail relay host. Ensure that this field is supplied with a proper value before the generation of any e-mail notifications.
- The creation of a scheduled task for a policy application on the Defense Center lists the network loopback address (127.0.0.1) as one of the targets of the policy. You can safely ignore this address.
- If an account is created with specific access permissions deleted, and a new account is created with the same user name, the account incorrectly assumes the permissions of the original account.
- The **Maintenance Access** option is not automatically selected when creating a new account with Admin access. Ensure the selection of this option before you save the new user account.
- Timestamps listed for the **Event Information** and **Packet Information** on the packet view for intrusion events differ by the number of hours between Greenwich Mean Time (GMT) and the time zone you selected.

- De-selecting all of the filtering check boxes on the **Scheduler** page results in all tasks being listed at the bottom of the page.
- The **IDS Event Summary** page incorrectly lists the number of Intrusion Sensors managed by the Defense Center.
- Clicking the **Start Net Backup** button on the **Backup and Restore** page without first entering a name for the backup file may cause the navigation menu to disappear in some browsers. Refreshing the browser window may be necessary.
- During the creation of a new compliance policy, the priority initially assigned to the policy is not saved with the policy. Edit the policy and assign it a priority to ensure that the proper priority is designated.
- If you use a custom workflow that includes only a table view of events and then use that workflow for a time range that includes no events, the GUI displays an error page instead of showing an empty table.
- Activation of rule 1497 may cause the packet payload to appear incorrectly in the packet view.
- Under certain conditions, the percentages shown in the **Event Summary** page may add up to more than 100%.
- Nested negated variables are not supported. Table 2 shows the declaration of a nested negated variable. Table 3 shows an example of a variable declaration that would have the same effect,

Table 2 Nested Negated Variable Example

```
NONCORE_NET:
var HOME_NET [10.1.0.0/16,10.2.0.0/16,10.3.0.0/16]
var EXTERNAL_NET !$HOME_NET
var DMZ_NET 10.4.0.0/16
var NOTDMZ_NET !$DMZ_NET
var NONCORE_NET [$EXTERNAL_NET, $NOTDMZ_NET]
```

Table 3 Nested Negated Variable Alternative

```
var HOME_NET [10.1.0.0/16,10.2.0.0/16,10.3.0.0/16]
var DMZ_NET 10.4.0.0/16
var NONCORE_NET ! [$HOME_NET,$DMZ_NET]
```

- Two variables cannot co-exist in an intrusion detection rule if one variable is an IP range and the other variable is the negation of an IP address inside the IP range of the first variable.

- Currently rules that match patterns in the next header cannot be written because content matches begin with the last decoded protocol.
  - Patterns can be matched in TCP headers by using rule options.
- The IP fragmentation preprocessor correctly generates an event for the first packets in an overlapping fragmentation attack such as Teardrop. Subsequent overlapping packets may not generate events, however.
- Up to 255 characters may be used when naming rule classifications, but pages can be difficult to read if more than 40 characters are used.
- The Defense Center can be used to push and install updates to individual sensors but cannot be used to push and install updates to sensor groups. If this is attempted, a success message appears after the install step. However, because the update was never pushed to the sensor, there is nothing to install
- While viewing multiple events in packet view, clicking the **Delete** button deletes all events rather than the one currently being viewed.
- The scheduler cannot be used to automatically download the Defense Center patch from the Nortel Networks Support web site. The patch must be manually downloaded as described in the Installation Instructions.
- The scheduler cannot be used to push the Defense Center patch to sensor groups. If the **Email** option is enabled on the scheduler, an erroneous message that the job successfully completed is generated. The patch can be pushed to individual sensors however.
- If an Instrusion Sensor is being managed by a Defense Center with the **Store Events Only on DC** option enabled, ensure that this option is not selected if the sensor is no longer to be managed by the Defense Center.
- If a custom intrusion rule is created on an Intrusion Sensor and the same rule is not created on the Defense Center managing it, intrusion events generated by the rule are identified only by a rule number on the Defense Center. As a solution to this ensure that custom rules are created on the Defense Center, included as part of an intrusion policy, and the policy is pushed to the managed Intrusion Sensor.
- If the high availability option is in use, and an Intrusion Sensor with a non-default intrusion policy is added to the Defense Center for management, it is possible that the policy name will be incorrectly identified. Ensure that the correct policies are applied to all sensors immediately after adding them to the high availability pair.
- The product documentation states that providing an e-mail address in the **Deletion Notification Address** field will send notification when any event is pruned from the Defense Center database. Notifications are actually sent only when intrusion and audit events are pruned.
- Enabling external SNMP trap alerting will generate errors.

TPS 2050 and TPS 2070 Intrusion Sensor

The feature set in release 3.2 of the TPS 2050 and TPS 2070 Intrusion Sensor software has the following known limitations:

- Flow-portscan events appear with a source and destination port of N/A, but N/A is not an option on the **Event Search** page when searching for this type of event.
  - To find all flow-portscan events, enter the flow-portscan generator ID (121) in the **Generator** field as the search criterion.
- If two user-defined variables that begin with the same string exist, and one of the variables is in use in an intrusion detection policy, the other unused variable cannot be deleted.
- After configuring Check Point firewall responses in the creation of a custom intrusion detection policy, the success message that the system presents does not clearly indicate how the policy was modified.
- The product documentation does not state that the clipboard has a capacity of 25 000 intrusion events.
- If a syntax error is present when saving a rule in the **Rule Editor**, the contents of the **Rule Editor** are cleared and a error message appears. The rule must then be re-created from the beginning.
- If a custom rule classification has been applied to an Intrusion Sensor through an IDS policy, do not delete it.
- If a custom incident type has been used with an incident, do not delete it.
- Adding a column for Reviewed status on a custom workflow results in the corresponding event page only showing unreviewed events.
  - As a solution, add the Reviewed status column and use the Reviewed/Unreviewed search option in the Event Search page. The resulting event pages include a Reviewed column and indicate whether or not the events have been reviewed.
- If account privileges are reduced to Maintenance access while logged in with Admin access, log out and log in to have the Admin access restored.
- Ensure that private searches are used as restriction criteria for Restricted Data User accounts. If private searches are not used as criteria, restricted users can edit the search and change their own restrictions.
- Anomalies in the sfmbproxy and watchdog processes may cause multiple instances of defunct sfmbproxy processes to appear in the process list. These should clear over time without user intervention.
- When viewing the list of generated reports on the **Report** page, the default file name in the **Download** option is always *view.cgi*. Rename the file and ensure that the file extension is appropriate for the type of file that you wish to create. For example, ".pdf" for a PDF file, ".csv" for a CSV file, and so on.

- After creating an IDS e-mail alert, a recurring task called JobSFMail is added to the scheduler. The start date of this task is set to December 31, 1969, and an entry appears in the calendar for each instance back to 1969.
- If necessary, set the time back manually by setting the drop-down options that appear on the page.
- When creating a new Backup job type in the **New Task** option on the **View Schedules** page, be aware of a certain page behavior. If you select the **Event** or **Configuration** check boxes and then change the **Task Type** between **Once** and **Recurring**, the check boxes become de-selected. Ensure that you manually re-select the appropriate check box after making such a change.
- To ensure that the Intrusion Sensor can send e-mail notifications, correctly configure the **Host Name** and **Domain** on the **Network Settings** page. Refer to the User Guide for configuration instructions. If the Intrusion Sensor is set up to be a DHCP client, ensure that the DHCP server provides the Intrusion Sensor with a host name.
- A message such as *opensnort kernel: bond_enslave(): failed to get speed/duplex from eth1, speed forced to 100Mbps, duplex forced to Full* may appear in the Intrusion Sensor syslog. This message can be safely ignored as the speed on the sensing device has not been affected.
- No error message is supplied if an e-mail address is specified in the **Email Status To** field on the **Scheduler** page without first setting up the **Mail Relay Host** on the **Configure Email Notification** page.
- The **Configure Email Notification** page incorrectly states a default value of *mail* in the **Mail Relay Host** field. There is in fact no default mail relay host. Ensure that this field is supplied with a proper value before the generation of any e-mail notifications.
- If an account is created with specific access permissions, deleted, and a new account is created with the same user name, the account incorrectly assumes the permissions of the original account.
- The Maintenance Access option is not automatically selected when creating a new account with Admin access. Ensure the selection of this option before you save the new user account.
- Timestamps listed for the **Event Information** and **Packet Information** on the packet view for intrusion events differ by the number of hours between Greenwich Mean Time (GMT) and the time zone you selected.
- The syslog may list messages that the file pruner is attempting to delete **.done* files. Any such messages can be safely ignored as this file type is not present on the Intrusion Sensor.
- De-selecting all of the filtering check boxes on the **Scheduler** page results in all tasks being listed at the bottom of the page.

- Clicking the **Start Net Backup** button on the **Backup and Restore** page without first entering a name for the backup file may cause the navigation menu to disappear in some browsers. Refreshing the browser window may be necessary.
- If you use a custom workflow that includes only a table view of events and then use that workflow for a time range that includes no events, the GUI displays an error page instead of showing an empty table.
- The process for uploading individual Snort rule files to the Defense Center and Intrusion Sensor policies was not originally documented. The process is as follows:
  - From the **Detection** menu choose **Rules** and then select **Import**. This menu is located under the **Network Sensor** menu on the Defense Center.
  - Select **Rule Pack To Upload** and **Apply** and browse to the rules file.
  - Click **Update**.

  The rules will be added to the *Local Rules* directory but the resulting list of rules that changed in the rule file may not be correct.
- Activation of rule 1497 may cause the packet payload to appear incorrectly in the packet view.
- Flow-portscan events are correctly shown with a source and destination port of N/A in the table view of events because they have no port information associated with them. If the Message column is removed from the table view however, the source and destination ports are incorrectly listed as 0/.
- Nested negated variables are not supported. Table 4 shows the declaration of a nested negated variable. Table 5 shows an example of a variable declaration that would have the same effect,

Table 4 Nested Negated Variable Example

```
NONCORE_NET:
var HOME_NET [10.1.0.0/16,10.2.0.0/16,10.3.0.0/16]
var EXTERNAL_NET !$HOME_NET
var DMZ_NET 10.4.0.0/16
var NOTDMZ_NET !$DMZ_NET
var NONCORE_NET [$EXTERNAL_NET, $NOTDMZ_NET]
```

Table 5 Nested Negated Variable Alternative

```
var HOME_NET [10.1.0.0/16,10.2.0.0/16,10.3.0.0/16]
var DMZ_NET 10.4.0.0/16
var NONCORE_NET ! [$HOME_NET,$DMZ_NET]
```

- Two variables cannot co-exist in an intrusion detection rule if one variable is an IP range and the other variable is the negation of an IP address inside the IP range of the first variable.
- Currently rules that match patterns in the next header cannot be written because content matches begin with the last decoded protocol.
  - Patterns can be matched in TCP headers by using rule options.
- The IP fragmentation preprocessor correctly generates an event for the first packets in an overlapping fragmentation attack such as Teardrop. Subsequent overlapping packets may not generate events, however.
- Up to 255 characters may be used when naming rule classifications, but pages can be difficult to read if more than 40 characters are used.
- While viewing multiple events in packet view, clicking the **Delete** button deletes all events rather than the one currently being viewed.
- E-mails generated by the Intrusion Sensor do not contain the IP address of the sensor.
- If the DNS server of a TPS 2070 Intrusion Sensor is changed on the **Network** page, the sensor will need to be rebooted if it does not restart properly.

Related Publications

These release notes supplement the following documents:

- *TPS 2070 Defense Center User's Guide* (Part Number 216886-A)
- *TPS 2070 Defense Center Installation Guide* (Part Number 216883-A)
- *TPS 2050 and TPS 2070 Intrusion Sensor User's Guide* (Part Number 216884-A)
- *TPS 2050 Intrusion Sensor Installation Guide* (Part Number 216881-A)
- *TPS 2070 Intrusion Sensor Installation Guide* (Part Number 216882-A)

Refer to these documents for additional technical information regarding the product architecture and features. These documents are available on the Nortel Networks Technical Support web site. To access these documents:

- Open your web browser and enter http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp. The Technical Support page opens.
- Select the **Browse Product Support** tab if it is not already selected.

- Select the following:
  - Product Family (Threat Protection System)
  - Product (The applicable product)
  - Content (Documentation)
- Click **Go**. The product documentation page opens, listing the appropriate documentation sorted by date.

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

Technical Support

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

Technical Solutions Center Telephone

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

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

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

China - (800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available at the following URL: http://www.nortelnetworks.com/help/contact/global.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, refer to the following URL: http://www.nortelnetworks.com/help/contact/erc/index.html.

Additional Information

The following additional information supplements information found in the Threat Protection System documentation suite.

Setting the IP Address for the Management Interface

The section entitled "Setting the IP Address for the Management Interface", found in Chapter 2 of the *TPS 2070 Defense Center Installation Guide* (Part Number 216883-A) and *TPS 2070 Intrusion Sensor Installation Guide* (Part Number 216882-A), states that the user may connect a monitor and keyboard to the TPS 2070 Intrusion Sensor or TPS 2070 Defense Center and set the management interface to an IP address on the same subnet as the administration system.

Use the console serial port instead of a monitor and keyboard.

To use the serial port, follow this procedure:

1. **Connect the serial cable shipped with the TPS product to the male DB-9 connector of an ASCII terminal or a computer running terminal emulation software.**
2. **Connect the other end of the serial cable to the serial port on the back of the TPS product.**
3. **Set the terminal or the terminal emulation software to use the parameters listed in Table 6.**

Table 6 Terminal Connection Parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Chassis Dimensions

The section entitled “Chassis Dimensions”, found in Chapter 3 of the *TPS 2070 Defense Center Installation Guide* (Part Number 216883-A) and *TPS 2070 Intrusion Sensor Installation Guide* (Part Number 216882-A), states that the chassis depth is 22.6 inches. The actual chassis depth is 25.6 inches.