ScreenOS Message Log Reference Guide

Release 6.1.0, Rev. 2

Part Number: 530-022527-01, Revision 2

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

ScreenOS Message Log Reference Guide
Release 6.1.0

Writing: Juniper Networks ScreenOS Team

Revision History
February 2008—Revision 2

The information in this document is current as of the date listed in the revision history.

Table of Contents

About This Guide

This preface provides the following guidelines for using the ScreenOS Message Log Reference Guide:

- Understanding Messages
- Organization

Understanding Messages

This guide provides administrators, who use network management tools such as Juniper Networks NetScreen-Security Manager, SNMP, syslog, or WebTrends, with a comprehensive list of messages that a security device can generate. This guide is organized by subject, so you can filter messages related to particular areas into meaningful sections in the database.

All messages reporting an administrative action include the location from which that action has been made: either from the console, from an administrator's host IP address via SCS, Telnet, or the Web, or from the LCD display. When devices are used in a redundant cluster for high availability, the message also states whether the action occurred on a primary or backup unit. Source of an action is not included in the messages listed here.

Organization

This book is organized into the following sections:

- Introduction—The Introduction explains the components of a message and the options that affect how a message is displayed.
- Each entry contains the following elements:
  - Message—The text of the message that appears in the log.
  - Meaning—An explanation of what the message means.
  - Action—One or more recommended actions for the administrator to take, when such action is required.

Chapter 1
Introduction

Messages report events useful for system administrators when recording, monitoring, and tracing the operation of a Juniper Networks security device. Messages provide information regarding the following events:

- Firewall attacks
- Configuration changes
- Successful and unsuccessful system operations

Anatomy of a Message

All messages consist of the following elements:

- Date (year-month-day when the event occurred)
- Time (hour:minute:second when the event occurred)
- Module (device type where the event occurred)
- Severity Level
- Message Type (a code number associated with the severity level)
- Message Text (content of the event message)

Messages include the administrator's login name when the administrator performed an action.

Severity Levels and Descriptions

The following is a list of the message severity levels:

- Emergency: Messages on SYN attacks, Tear Drop attacks, and Ping of Death attacks. For more information on these types of attacks, see Volume 4, "Attack Detection and Defense Mechanisms"
- Alert: Messages about conditions that require immediate attention, such as firewall attacks and the expiration of license keys.
- Critical: Messages about conditions that affect the functionality of the device, such as high availability (HA) status changes.

- Error: Messages about error conditions that probably affect the functionality of the device, such as a failure in antivirus scanning or in communicating with SSH servers.
- Warning: Messages about conditions that could affect the functionality of the device, such as a failure to connect to e-mail servers or authentication failures, timeouts, and successes.
- Notification: Notification of normal events, including configuration changes initiated by an admin.
- Information: General information about system operations.
- Debugging: Detailed information useful for debugging purposes.

Chapter 2

Addresses

These messages relate to the creation, modification, and removal of addresses.

Notification (00001)

Message	Address group ⟨*address_group_name*⟩ ⟨*config_action_add_delete_member*⟩ ⟨*member_name*⟩ ⟨*config_changer*⟩ session.
Meaning	An administrator has added or deleted the specified address in the address group.
Action	No recommended action.

Message	Address group ⟨*address_group_name*⟩ ⟨*config_action_add_delete_modify*⟩ ⟨*config_changer*⟩ session.
Meaning	An administrator added, deleted, or modified the specified address group.
Action	No recommended action.

Message	Address ⟨*address_name*⟩ for domain address ⟨*domain_name*⟩ in zone ⟨*zone_name*⟩ ⟨*config_action_add_delete_modify*⟩ ⟨*config_changer*⟩ session.
Meaning	An admin has added, deleted, or modified the address book entry with the specified IP address (or domain name) in the named security zone.
Action	No recommended action.

Message	Address ⟨*address_name*⟩ for ip address ⟨*ip_address*⟩ in zone ⟨*zone_name*⟩ ⟨*config_action_add_delete_modify*⟩ ⟨*config_changer*⟩ session.
Meaning	An administrator added, deleted, or modified the specified address group.
Action	No recommended action.

Message	Address ⟨*address_name*⟩ for IP address ⟨*ip_address*⟩/⟨*net_mask*⟩ in zone ⟨*zone_name*⟩ ⟨*config_action_add_delete_modify*⟩ ⟨*config_changer*⟩ session.
Meaning	An admin has added, deleted, or modified the address book entry with the specified IP address (or domain name) in the named security zone.
Action	No recommended action.

Chapter 3
Admin

These messages relate to the administration of the security device.

Alert (00027)

Message	ScreenOS ⟨*major_version*⟩.⟨*minor_version*⟩.⟨*rev_version*⟩ Serial# ⟨*serial_number*⟩: ⟨*ar_log_initiated_string*⟩
Meaning	An administrator initiated an asset recovery operation for the specified ScreenOS version on a security device with the specified serial number.
Action	No recommended action

Message	ScreenOS ⟨*major_version*⟩.⟨*minor_version*⟩.⟨*rev_version*⟩ Serial# ⟨*serial_number*⟩: ⟨*ar_log_aborted_string*⟩
Meaning	An administrator has aborted an asset recovery operation for the specified ScreenOS version on a security device with the specified serial number.
Action	No recommended action

Message	System configuration has been erased
Meaning	An administrator has erased the system configuration. This may be due to a successful asset recovery executed via a console connection or successful execution of the unset all command.
Action	The system configuration must be reconfigured.

Critical (00027)

Message	Multiple login failures occurred for user ⟨*admin_name*⟩
Meaning	The user made multiple unsuccessful login attempts. (After three failed login attempts, the security device automatically terminates the connection.)
Action	Investigate these login failures and determine whether they were attempts to illegally access the security device.

Message	Multiple login failures occurred for user ⟨*admin_name*⟩ from IP address ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The user made multiple unsuccessful login attempts from the specified IP address and port. After three (default) failed login attempts, the security device Networks security device automatically terminates the connection.
Action	Investigate these login failures and determine whether they were attempts to illegally access the security device.

Warning (00002)

Message	ADMIN AUTH: Local instance of an external admin user privilege has been changed from ⟨*string*⟩ to ⟨*string*⟩.
Meaning	An administrator modified the privileges of an external administrator.
Action	No recommended action

Warning (00515)

Message	Admin user ⟨*admin_name*⟩ has been forced to log out of the serial console session.
Meaning	The specified admin user was forced to log off the serial console session with the security device.
Action	The root administrator made changes to an administrator account, cleared the active session of the specified administrator, or is performing other device management operations that caused the security device to terminate the administrator session. The administrative user should try to log in again or contact the root administrator.

Message	Admin user ⟨*admin_name*⟩ has been forced to log out of the SSH session on host ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The specified administrator was forced to log off the SSH session.
Action	The root administrator made changes to an administrator account, cleared the active session of the specified administrator, or is performing other device management operations that caused the security device to terminate the administrator session. The administrative user should try to log in again or contact the root administrator.

Message	Admin user ⟨*admin_name*⟩ has been forced to log out of the Telnet session on host ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The specified administrator was forced to log off the Telnet session.
Action	The root administrator made changes to the administrator account, cleared the active session of the specified administrator, or is performing other device management operations that caused the security device to terminate the administrator session. The administrative user should try to log in again or contact the root administrator.

Message	Admin user ⟨*admin_name*⟩ has been forced to log out of the Web session on host ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The specified administrator was forced to log off the Web session.
Action	The root administrator made changes to the administrator account, cleared the active session of the specified admin, or is performing other device management operations that caused the security device to terminate the administrator session. The administrative user should try to log in again or contact the root administrator.

Message	Admin user ⟨*admin_name*⟩ has logged on via SSH from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The specified administrator logged on or off the security device from either a Telnet or SSH session.
Action	No recommended action

Message	Admin user ⟨*admin_name*⟩ has logged on via Telnet from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The specified administrator logged on or off the security device from either a Telnet or SSH session.
Action	No recommended action

Message	Admin user ⟨*admin_name*⟩ has logged on via the console
Meaning	The administrator logged on or off the security device from the console.
Action	No recommended action

Message	Admin user ⟨*admin_name*⟩ has logged out via SSH from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The specified administrator logged on or off the security device from either a Telnet or SSH session
Action	No recommended action

Message	Admin user ⟨*admin_name*⟩ has logged out via Telnet from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The specified administrator logged on or off the security device from either a Telnet or SSH session
Action	No recommended action

Message	Admin user ⟨*admin_name*⟩ has logged out via the console
Meaning	The administrator logged on or off the security device from the console.
Action	No recommended action

Message	Login attempt to system by admin ⟨*admin_name*⟩ via SSH from ⟨*ip_addr*⟩:⟨*port*⟩ has failed⟨*reason*⟩
Meaning	An attempt to log in to the security device by the administrator via the console, Telnet, or SSH has failed due to the specified reason.
Action	Determine the reason for the failure and resolve the problem. Verify the administrator user name and password.

Message	Login attempt to system by admin ⟨*admin_name*⟩ via Telnet from ⟨*ip_addr*⟩:⟨*port*⟩ has failed⟨*reason*⟩
Meaning	An attempt to log in to the security device by the administrator via the console, Telnet, or SSH has failed due to the specified reason.
Action	Determine the reason for the failure and resolve the problem. Verify the administrator user name and password.

Message	Login attempt to system by admin ⟨*admin_name*⟩ via the console has failed⟨*reason*⟩
Meaning	An attempt to log in to the security device by the administrator via the console, Telnet, or SSH has failed due to the specified reason.
Action	Determine the reason for the failure and resolve the problem. Verify the administrator user name and password.

Message	Management session via serial console for ⟨*vsys*⟩admin ⟨*admin_name*⟩ has timed out
Meaning	The management session (established via the console, Telnet, or SSH by the named admin) has expired.
Action	No recommended action

Message	Management session via SSH from ⟨*ip_addr*⟩:⟨*port*⟩ for ⟨*vsys*⟩admin ⟨*admin_name*⟩ has timed out
Meaning	The management session (established via the console, Telnet, or SSH by the named admin) has expired.
Action	No recommended action

Message	Management session via Telnet from ⟨*ip_addr*⟩:⟨*port*⟩ for ⟨*vsys*⟩admin ⟨*admin_name*⟩ has timed out
Meaning	The management session (established via the console, Telnet, or SSH by the named admin) has expired.
Action	No recommended action

Message	Remotely authenticated Admin ⟨*admin_name*⟩ demoted from ROOT privilege to RW privilege.
Meaning	The privileges for the specified admin have been downgraded from root to read/write.
Action	No recommended action

Message	Remotely authenticated Admin ⟨*admin_name*⟩ demoted from ⟨*old_priv*⟩ privilege to ⟨*new_priv*⟩ privilege.
Meaning	The privileges for the specified admin have been downgraded.
Action	No recommended action

Message	Vsys admin user ⟨*admin_name*⟩ has logged on via SSH from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The Vsys administrator logged on or logged out of the security device from a Telnet or SSH session.
Action	No recommended action

Message	Vsys admin user ⟨*admin_name*⟩ has logged on via Telnet from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The Vsys administrator logged on or logged out of the security device from a Telnet or SSH session.
Action	No recommended action

Message	Vsys admin user ⟨*admin_name*⟩ has logged on via the console
Meaning	The Vsys administrator logged on or off the security device from the console.
Action	No recommended action

Message	Vsys admin user ⟨*admin_name*⟩ has logged out via SSH from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The Vsys administrator logged on or logged out of the security device from a Telnet or SSH session.
Action	No recommended action

Message	Vsys admin user ⟨*admin_name*⟩ has logged out via Telnet from ⟨*ip_addr*⟩:⟨*port*⟩
Meaning	The Vsys administrator logged on or logged out of the security device from a Telnet or SSH session.
Action	No recommended action

Message	Vsys admin user ⟨*admin_name*⟩ has logged out via the console
Meaning	The Vsys administrator logged on or off the security device from the console.
Action	No recommended action

Warning (00518)

Message	ADM: Local admin authentication failed for login name ⟨*admin_name*⟩: invalid login name
Meaning	An invalid login name was entered at the login prompt. The login name provided did not appear in the local database of defined administrators.
Action	If a valid administrator caused this message, they should attempt to authenticate again and enter a valid login name. This message may indicate that there was an attempt to illegally gain access to the device.

Message	ADM: Local admin authentication failed for login name ⟨*admin_name*⟩: invalid password
Meaning	An invalid password was entered at the password prompt. The password did not match the password associated with the given administrator login name stored in the local administrator database.
Action	If a valid administrator caused this message, they should attempt to authenticate again and enter a valid password. This message may indicate that there was an attempt to illegally gain access to the device.

Message	Admin user ⟨*admin_name*⟩ has been rejected via the ⟨*server_name*⟩ server at ⟨*ip_addr*⟩.
Meaning	The named admin user has been rejected by the specified server.
Action	No recommended action

Warning (00519)

Message	Admin user ⟨*admin_name*⟩ has been accepted via the ⟨*server_name*⟩ server at ⟨*ip_addr*⟩.
Meaning	The named admin user has been accepted by the specified server.
Action	No recommended action

Notification (00002)

Message	Root admin access restriction through console only has been disabled by admin ⟨*username*⟩ ⟨*changed_via*⟩
Meaning	The named root admin has either enabled or disabled the feature that restricts the root admin to logging in to the device through the console only. The name of the admin who made the change appears after the message and how the change was made.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Root admin access restriction through console only has been enabled by admin ⟨*username*⟩ ⟨*changed_via*⟩
Meaning	The named root admin has either enabled or disabled the feature that restricts the root admin to logging in to the device through the console only. The name of the admin who made the change appears after the message and how the change was made.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Root admin password restriction of minimum ⟨*passwd_len*⟩ characters has been disabled by admin ⟨*username*⟩ ⟨*changed_via*⟩
Meaning	The named root admin has either enabled or disabled the feature that specifies the minimum length of the root admin password. The name of the admin who made the change appears after the message and how the change was made.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Root admin password restriction of minimum ⟨*passwd_len*⟩ characters has been enabled by admin ⟨*username*⟩ ⟨*changed_via*⟩
Meaning	The named root admin has either enabled or disabled the feature that specifies the minimum length of the root admin password. The name of the admin who made the change appears after the message and how the change was made.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Single use password restriction for read-write administrators has been disabled by admin ⟨*username*⟩ ⟨*changed_via*⟩
Meaning	An admin enabled or disabled the single use password restriction for read-write administrators. The name of the admin who made the change appears after the message and how the change was made.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Single use password restriction for read-write administrators has been enabled by admin ⟨*username*⟩ ⟨*changed_via*⟩
Meaning	An admin enabled or disabled the single use password restriction for read-write administrators. The name of the admin who made the change appears after the message and how the change was made.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	ADM: Non-primary authentication server ⟨*status*⟩ to authenticate non-ROOT privileged admins. Modifier: ⟨*admin_name*⟩
Meaning	An admin has changed the status of the non-primary server that authenticates non-root admins.
Action	No recommended action

Message	ADM: Non-primary authentication server ⟨*status*⟩ to authenticate ROOT privileged admins. Modifier: ⟨*admin_name*⟩
Meaning	An admin has changed the status of the non-primary server that authenticates root admins.
Action	No recommended action

Message	ADM: Remote authentication server set to ⟨*status*⟩. Modifier: ⟨*admin_name*⟩
Meaning	An admin has changed the status of the remote authentication server.
Action	No recommended action

Message	ADM: Remotely authenticated admins ⟨*status*⟩ READ-ONLY privilege. Modifer: ⟨*admin_name*⟩
Meaning	An admin has changed the status of the remotely authenticated read-only admins.
Action	No recommended action

Message	ADM: Remotely authenticated ROOT privileged admins ⟨*status*⟩. Modifer: ⟨*admin_name*⟩
Meaning	An admin has changed the status of the remotely authenticated root admins.
Action	No recommended action

Message	Maximum failed login attempts before administrative session disconnects has been modified from ⟨*orig_value*⟩ to ⟨*new_value*⟩ by admin ⟨*username*⟩ ⟨*changed_via*⟩
Meaning	An admin changed the maximum number of failed login attempts allowed before the security device terminates the connection. The name of the admin who made the change and how the change was made follows the message.
Action	No recommended action

Notification (00003)

Message	The console debug buffer has been ⟨*status*⟩
Meaning	An admin has enabled (or disabled) the console debug buffer.
Action	No recommended action

Message	The console page size changed from ⟨*old_page_size*⟩ to ⟨*new_page_size*⟩
Meaning	An admin has changed the number of pixels that comprise the console page size.
Action	No recommended action

Message	The console timeout value changed from ⟨*old_timeout_value*⟩ to ⟨*new_timeout_value*⟩ minutes
Meaning	An admin has changed the console idle timeout value. If there is no activity for this specified period of time, the console session terminates.
Action	No recommended action

Message	The serial console has been ⟨*status*⟩ by admin ⟨*string*⟩
Meaning	An admin has enabled (or disabled) serial console connectivity.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Information (00002)

Message	Admin account created for ⟨*admin_name_1*⟩ ⟨*changer*⟩
Meaning	An admin created a new account. The name of the admin who created the account follows the name of the new account.
Action	No recommended action

Message	Admin account deleted for ⟨*admin_name_1*⟩ ⟨*changer*⟩
Meaning	An admin deleted the specified account. The name of the admin who deleted the account appears after the message.
Action	No recommended action

Message	Admin account modified for ⟨*admin_name_1*⟩ ⟨*changer*⟩
Meaning	An admin modified the specified account. The name of the admin who modified the account appears after the message.
Action	No recommended action

Message	Admin name for account ⟨*old_admin_name*⟩ has been modified to ⟨*new_admin_name*⟩ ⟨*changer*⟩
Meaning	An admin changed the account name from name_str1 to name_str2. The name of the administrator who made the account name change follows the message (name_str3)
Action	No recommended action

Message	Admin password for account ⟨*admin_name*⟩ has been modified ⟨*changer*⟩
Meaning	An admin changed the password for the specified account (name_str1). The name of the admin who changed the password follows the message (name_str2).
Action	No recommended action

Message	Dial-in admin authentication timeout value has been changed from ⟨*old_timeout*⟩ to ⟨*new_timeout*⟩ minutes
Meaning	An admin has changed the dial-in authentication timeout value. If there is no successful login in this specified period of time, the dial-in connection is hung up.
Action	No recommended action.

Message	Extraneous exit is issued ⟨*changer*⟩
Meaning	An extraneous exit command was issued either by a script or at a CLI, resulting in an attempt to exit from the root level
Action	Ensure that the device has the intended configuration, especially after a firmware upgrade or configuration merge.

Message	HTTP port has been changed from ⟨*old_port*⟩ to ⟨*new_port*⟩ ⟨*admin_name*⟩
Meaning	An admin has changed the HTTP port.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Management restriction for IP ⟨*ip_addr*⟩ has been removed in vsys ⟨*admin_name*⟩. (by admin ⟨*vsys_name*⟩)
Meaning	An administrator has enabled access to VSYS administrators logging in from the specified IP address or range. VSYS administrators can manage the security device from any IP address within the range. This is the default setting.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Management restriction for IP ⟨*ip_addr*⟩ subnet ⟨*ip_mask*⟩ has been added in vsys '⟨*admin_name*⟩'. (by admin ⟨*vsys_name*⟩)
Meaning	An administrator has restricted access to VSYS administrators logging in from the specified IP address or range.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Management restriction removed for all IPs in vsys ⟨*vsys_name*⟩. (by admin ⟨*admin_name*⟩)
Meaning	An administrator has enabled access to VSYS administrators logging in from any IP address. VSYS administrators can manage the security device from any IP address.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Management restriction removed for all IPs on device. (by admin ⟨*admin_name*⟩)
Meaning	An administrator has enabled access to administrators logging in from any IP address. Administrators can manage the security device from any IP address.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	SSH port has been changed from ⟨*old_port*⟩ to ⟨*new_port*⟩ ⟨*admin_name*⟩
Meaning	An admin has changed the SSH port.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	System IP has been changed from ⟨*old_ip_addr*⟩ to ⟨*new_ip_addr*⟩ ⟨*admin_name*⟩
Meaning	An administrator changed the system IP address.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Telnet port has been changed from ⟨*old_port*⟩ to ⟨*new_port*⟩ ⟨*admin_name*⟩
Meaning	An admin has changed the telnet port.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Web admin authentication idle timeout value has been changed from ⟨*old_timeout*⟩ to ⟨*new_timeout*⟩ minutes
Meaning	An admin has changed the Web administration idle timeout value. If there is no activity for this specified period of time, the WebUI session terminates.
Action	No recommended action

Chapter 4

ADSL

These messages relate to the ADSL line connection on the security device.

Notification (00557)

Message	ADSL Line Activating.
Meaning	The ADSL line is activated.
Action	No recommended action.

Message	ADSL Line Close Rejected.
Meaning	ADSL has rejected the request to close the connection.
Action	No recommended action.

Message	ADSL Line Closed.
Meaning	ADSL has closed the connection.
Action	No recommended action.

Message	ADSL Line Down.
Meaning	There is no physical connection to the ADSL line.
Action	Make sure that the ADSL cable is properly connected and that you have ADSL service on the line.

Message	ADSL Line in an unknown state.
Meaning	An internal error occurred
Action	Contact Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered customer.)

Message	ADSL Line Open Failed (Errored Message Received from ATU-C).
Meaning	The system encountered an unknown error while attempting to open the ADSL connection.
Action	Reopen the ADSL line.

Message	ADSL Line Open Failed (Forced Silence).
Meaning	Failure has occurred while opening the line because the device is required to be quiet for one minute by ATU-C.
Action	Reopen the ADSL line.

Message	ADSL Line Open Failed (Incompatible Line Conditions).
Meaning	The ADSL connection could not be opened. The combination of requested minimum ATM rate, target noise margin, and allowed PSD is not allowed on the line.
Action	Choose appropriate connection parameters and reopen the ADSL line.

Message	ADSL Line Open Failed (Protocol Error).
Meaning	The system encountered a protocol error while attempting to open the ADSL connection.
Action	Reopen ADSL line.

Message	ADSL Line Open Failed (Spurious ATU Detected).
Meaning	The system encountered noise while attempting to open the ADSL connection.
Action	Reopen ADSL line.

Message	ADSL Line Open Failed (Unable to Lock with ATU-C).
Meaning	The ADSL connection could not be opened.
Action	Check the ADSL cable connections and reopen the ADSL line.

Message	ADSL Line Open Failed (Unknown Error Code).
Meaning	ADSL line cannot be activated because of an unknown reason.
Action	Reopen ADSL line.

Message	ADSL Line Open Failed (Unselectable Operation Mode).
Meaning	Failure has occurred while opening the line because the ACTIVATING protocol does not succeed in selecting a common mode of operation.
Action	Reopen the ADSL line.

Message	ADSL Line Open Rejected.
Meaning	There was a received line open request or there was a configure parameter error during activation.
Action	Do not open the line while activating.

Message	ADSL Line Opened (=>Showtime).
Meaning	An ADSL connection has been established with the ATU-C.
Action	No recommended action.

Message	ADSL Line Signal Lost detected.
Meaning	ADSL sent an ATU-C request to prepare to close the ADSL connection.
Action	No recommended action.

Message	ADSL Line Suicide Request Received.
Meaning	ADSL sent an ATU-C request to prepare to close the ADSL connection.
Action	No recommended action.

Message	ADSL Line UP Fast and Interleave Channels.
Meaning	The ADSL line is operational for fast-path and interleaved-path channels.
Action	No recommended action.

Message	ADSL Line UP Fast Channel, change Utopia address to match it.
Meaning	The ADSL line is operational for a fast-path channel, and the address on the ATM connection bus has changed.
Action	No recommended action.

Message	ADSL Line UP Fast Channel.
Meaning	The ADSL line is operational for a fast-path channel.
Action	No recommended action.

Message	ADSL Line UP Interleaved Channel, change Utopia address to match it.
Meaning	The ADSL line is operational for an interleaved channel, and the address on the ATM connection bus has changed.
Action	No recommended action.

Message	ADSL Line UP Interleaved Channel.
Meaning	The ADSL line is operational for an interleaved-path channel.
Action	No recommended action.

Message	ADSL Line Waiting for Activating.
Meaning	The ADSL line is awaiting activation.
Action	No recommended action.

Notification (00616)

Message	ADSL⟨*card number*⟩/0 Line Down.
Meaning	The ADSL line is down.
Action	No recommended action.

Message	ADSL⟨*card number*⟩/0 Line Training.
Meaning	The ADSL line is in training.
Action	No recommended action.

Message	ADSL⟨*card number*⟩/0 Line Up.
Meaning	The ADSL line is up.
Action	No recommended action.

Message	ADSL⟨*card number*⟩/0 SOC Firmware Failed (Load Bootrom Failure).
Meaning	The ADSL interface failed at startup because the bootrom failed to load.
Action	Do the following: Execute the debug adsl all CLI command. Execute the get db s CLI command. Send the debug message to Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	ADSL⟨*card number*⟩/0 SOC Firmware Failed (Load image Failure).
Meaning	The ADSL interface failed at startup because the ADSL image failed to load.
Action	Do the following: Execute the debug adsl all CLI command. Execute the get db s CLI command. Send the debug message to Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	ADSL⟨*card number*⟩/0 SOC Firmware Failed (push configuration failure).
Meaning	The ADSL interface failed at startup because the device failed to load the ADSL configuration. The ADSL SOC was rebooted.
Action	Do the following: Execute the debug adsl all CLI command. Execute the get db s CLI command. Send the debug message to Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	ADSL⟨*card number*⟩/0 SOC Firmware Reboot(Keepalive timeout).
Meaning	The device cannot receive keepalive responses from the ADSL SOC after 30 seconds. The ADSL SOC was rebooted.
Action	Do the following: Execute the exec adsl 1 debug 3 CLI command. Execute the get db s CLI command. Send the debug message to Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	ADSL⟨*card number*⟩/0 SOC Firmware Reset.
Meaning	The ADSL SOC was reset.
Action	Do the following: Execute the exec adsl 1 debug 3 CLI command. Execute the debug adsl basic CLI command. Execute the get db s CLI command. Send the debug message to Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	ADSL⟨*card number*⟩/0 SOC Firmware Startup Failed (Wait Startup timeout).
Meaning	The ADSL SOC startup has timed out. The ADSL image has loaded over 60 seconds.
Action	Do the following: Execute the exec adsl 1 debug 3 CLI command. Execute the debug adsl all CLI command. Execute the get db s CLI command. Send the debug message to Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	ADSL⟨*card number*⟩/0 SOC Firmware Startup Successful.
Meaning	The ADSL SOC system has started.
Action	No recommended action.

Chapter 5
Anti-spam

The following messages relate to the anti-spam feature in ScreenOS.

Warning (00064)

Message	Anti-Spam is attached to policy ID ⟨*integer*⟩.
Meaning	The anti-spam profile is applied to an existing policy ID. Verify the device has the intended configuration.
Action	No action required.

Message	Anti-Spam is detached from policy ID ⟨*integer*⟩.
Meaning	The anti-spam profile is removed from the specified policy ID. Verify the device has the intended configuration.
Action	No action required.

Warning (00563)

Message	Anti-Spam: SPAM FOUND ! ⟨*as_sender_info*⟩.
Meaning	This indicates the software was successful in detecting spam. Verify the spam to make sure it is not a false positive. The < string > may contain the IP address of the sender, host name, and the reason for it being categorized as spam.
Action	No action required.

Notification (00064)

Message	Anti-Spam action changed.
Meaning	This specifies how the device handles messages deemed to be spam. The device can either drop a spam message or identify it as spam by tagging it (default).
Action	No action required.

Message	Anti-Spam blacklist is changed.
Meaning	The anti-spam blacklist is modified by adding or removing an IP address, an email, a hostname, or a domain name from the local anti-spam blacklist. Each entry in a blacklist can identify a possible spammer.
Action	No action required.

Message	Anti-Spam SBL server configured: ⟨*sbl_server_name* ⟩.
Meaning	The device is enabled to use the external spam-blocking SBL service, which uses a blacklist to identify known spam sources. The service replies to queries from the device about whether an IP address belongs to a known spammer.
Action	No action required.

Message	Anti-Spam whitelist is changed.
Meaning	The anti-spam blacklist is modified by adding or removing an IP address, an email, a hostname, or a domain name from the local anti-spam blacklist. Each entry in a whitelist can identify an entity that is not a suspected spammer.
Action	No action required.

Notification (00563)

Message	Anti-Spam key is expired (expiration date: %t2; current date: %t2).
Meaning	The anti-spam license key is expired.
Action	Obtain and install an anti-spam license key on your device.

Message	Anti-Spam: Exceeded maximum concurrent connections (⟨*url_server_vendor_name*⟩).
Meaning	This message is generated when the device stops handling new connections after it has reached its limit of current connections. The maximum concurrent connections value is platform dependant. For example, this may occur if too many email messages are coming in simultaneously.
Action	No action required.

Chapter 6
Antivirus

The following messages relate to the antivirus (AV) protection mechanism in ScreenOS.

Critical (00554)

Message	SCAN-MGR: Cannot write AV pattern file to flash.
Meaning	The device was unable to send the contents of an AV pattern file to the flash memory of the device.
Action	Contact Juniper Networks technical support: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.)

Message	SCAN-MGR: Check AV pattern file failed with error code: ⟨*integer*⟩.
Meaning	The device was unable to use the specified pattern file. The error string provides information you need to get help from Juniper Networks technical support.
Action	If this error persists, contact Juniper Networks technical support: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.)

Message	SCAN-MGR: Check AV pattern file failed with error code: ⟨*string*⟩.
Meaning	The device was unable to use the specified pattern file. The error string provides information you need to get help from Juniper Networks technical support.
Action	If this error persists, contact Juniper Networks technical support: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.)

Message	SCAN-MGR: AV pattern file size is too large (⟨*integer*⟩ bytes).
Meaning	The pattern file size specified in the server initialization file (server.ini) exceeds the maximum prescribed limit, which is 10 megabytes.
Action	Contact Juniper Networks technical support: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.)

Message	WARNING: Current hardware configuration does not support embedded AV scanning. Please upgrade system memory.
Meaning	Embedded AV is supported on select security devices only. This specific device supports embedded AV, only if you increase its system memory.
Action	Upgrade the device memory, if you want to use embedded AV.

Critical (00574)

Message	ICAP: Input file size is too large (⟨*integer*⟩ bytes).
Meaning	The content file size exceeds the maximum prescribed limit, which is dependant on the device.
Action	No action required.

Error (00054)

Message	APPPRY: Suspicious client ⟨*IP address*⟩:⟨*integer*⟩->⟨*IP address*⟩:⟨*integer*⟩ used ⟨*integer*⟩ percent of AV resources, which exceeded the maximum of ⟨*integer*⟩ percent.
Meaning	When the security device attempted to forward traffic for antivirus (AV) scanning, the amount of traffic from the specified source address exceeded the amount permitted from any one source. The maximum amount of traffic from one source that the security device forwards to an AV scanner is a percent of the total amount of traffic.
Action	It is a possible attack, then enter the following command, set av all resources < percent > .

Warning (00066)

Message	AV configures an Extension list ⟨*string*⟩ with extension ⟨*string*⟩.
Meaning	The antivirus scanner configures an extension list (string1) with the specified extensions (string2).
Action	No recommended action.

Message	AV configures MIME list ⟨*string*⟩ with MIME ⟨*string*⟩.
Meaning	The antivirus scanner {configures | removes} a MIME list (string1) with the MIME extensions shown in the second string.
Action	No recommended action.

Message	AV creates profile ⟨*string*⟩.
Meaning	The antivirus scanner creates the specified profile.
Action	No recommended action.

Message	AV object ⟨*string*⟩ ⟨*string*⟩ timeout is reset to default value.
Meaning	An admin has reset the timeout to its default value for the specified AV application. The string variables specify the scan-mgr and the application.
Action	No recommended action.

Message	AV object ⟨*string*⟩ ⟨*string*⟩ timeout is reset to its default value.
Meaning	An admin has reset the timeout to its default value for the specified AV application. The string variables specify the scan-mgr and the application.
Action	No recommended action.

Message	AV pattern type is changed from ⟨*string*⟩ to ⟨*string*⟩ due to increasing pattern file size and limited flash space.
Meaning	When the AV pattern file is too large for the memory and flash disk, the pattern type is downgraded from string1 to string2 to save memory and flash disk usage. The AV pattern file (specified in string1 and string2) is downgraded to the next lower degree of security pattern type. The default AV pattern file, Standard is downgraded to the basic In-the-Wild; Extended is downgraded to the Standard pattern type.
Action	No recommended action.

Message	AV profile ⟨*string*⟩ sets ICAP ⟨*string*⟩ to ⟨*string*⟩.
Meaning	The ICAP settings, req_url/resp_url and server/server-group are set in the AV profile. These options set the request or response URL string on the ICAP server to scan transactions. The value specified for the req_url or resp_url string is specific to the ICAP server.
Action	No recommended action.

Message	AV profile ⟨*string*⟩ ⟨*string*⟩s protocol ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩.
Meaning	The antivirus scanner configures the parameters for the specified AV profile (string1) with (string2) protocol and the following variables: (string3): ext-list name | mime-list name | timeout | email-notify (string4): file ext values; mime ext values (string5): include/exclude | virus/scan-error (string6): sender | recipient
Action	No recommended action.

Message	AV profile ⟨*string*⟩ ⟨*string*⟩s protocol ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩.
Meaning	The antivirus scanner removes the parameters for specified AV profile (string1) with (string2) protocol and the following variables: (string3): ext-list name | mime-list name | timeout | email-notify (string4): file ext values; mime ext values (string5): include/exclude | virus/scan-error (string6): sender | recipient
Action	No recommended action.

Message	AV profile ⟨*string*⟩ unsets ICAP ⟨*string*⟩.
Meaning	The ICAP settings are removed from the AV profile.
Action	No recommended action.

Message	AV removes extension list ⟨*string*⟩.
Meaning	The antivirus scanner removes the extension list (string).
Action	No recommended action.

Message	AV removes MIME list ⟨*string*⟩.
Meaning	The antivirus scanner {configures | removes} a MIME list (string1) with the MIME extensions displayed in the second string.
Action	No recommended action.

Message	AV removes profile ⟨*string*⟩.
Meaning	The antivirus scanner deletes the specified profile.
Action	No recommended action.

Message	AV ⟨*string*⟩ is attached to policy ID ⟨*integer*⟩.
Meaning	AV is applied to the specified policy.
Action	No recommended action.

Message	AV ⟨*string*⟩ is detached from policy ID ⟨*integer*⟩
Meaning	AV is not assigned to the specified policy.
Action	No recommended action.

Warning (00547)

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is dropped because maximum concurrent messages are exceeded.
Meaning	The content cannot be scanned, because you exceeded the maximum number of concurrent messages to scan. See product Release Notes for the maximum number of concurrent messages supported on a device.
Action	No recommended action.

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is dropped because maximum content size is exceeded.
Meaning	Because the amount of traffic that the security device received at one time exceeded the maximum content limit, the AV scanner passed/ dropped the specified traffic.
Action	If this happens frequently, you might want to increase the maximum content limit. You can do this with the following CLI command: set av scan-mgr max-content-size number. The default maximum content size is 10,000 kilobytes of concurrent traffic. The range for the maximum content size is device dependent. See the product Release Notes for the maximum content size supported on each device.

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is dropped due to scan-engine error or constraint with code ⟨*integer*⟩ for ⟨*string*⟩.
Meaning	The internal scan engine on the security device was unable to scan the specified traffic because of an internal error. The reason for error is specified in the string. The AV scanner passes or drops the specified traffic.
Action	To pass traffic, specify the CLI command, set av all fail-mode traffic permit.

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is passed because maximum concurrent messages are exceeded.
Meaning	The content cannot be scanned, because you exceeded the maximum number of concurrent messages to scan. See product Release Notes for the maximum number of concurrent messages supported on a device.
Action	No recommended action.

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is passed because maximum content size is exceeded.
Meaning	Because the amount of traffic that the security device received at one time exceeded the maximum content limit, the AV scanner passed/dropped the specified traffic.
Action	If this happens frequently, you might want to increase the maximum content limit. You can do this with the following CLI command: set av scan-mgr max-content-size number. The default maximum content size is 10,000 kilobytes of concurrent traffic. The range for the maximum content size is device dependent. See the product Release Notes for the maximum content size supported on each device.

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is passed due to scan-engine error or constraint with code ⟨*integer*⟩ for ⟨*string*⟩.
Meaning	The internal scan engine on the security device was unable to scan the specified traffic because of an internal error. The reason for error is specified in the string. The AV scanner passes or drops the specified traffic.
Action	To pass traffic, specify the CLI command, set av all fail-mode traffic permit.

Message	AV: VIRUS FOUND: ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ file % .64s virus ⟨*string*⟩
Meaning	The AV scanner has detected a virus in the traffic from the specified source IP address and port number to the specified destination IP address and port number. The text string at the end of the message contains the name of the contaminated file and the name of the detected virus.
Action	No recommended action

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is dropped due to scan-engine error or constraint with code ⟨*integer*⟩ for ⟨*string*⟩.
Meaning	The external ICAP AV scanner was unable to scan the traffic from the specified source IP address and port number to the specified destination IP address and port number, because of an internal error. The internal error can be an error on the external ICAP server, the security device, or some resource constraint limit. The reason for the internal error is specified in < string3 > . The ICAP scanner passes or drops the specified traffic.
Action	To pass traffic, specify the CLI command, set av all fail-mode traffic permit.

Message	AV: Content from ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*string*⟩ % .64s⟨*string*⟩ is passed due to scan-engine error or constraint with code ⟨*integer*⟩ for ⟨*string*⟩.
Meaning	Because of an internal error, the external ICAP AV scanner was unable to scan the traffic from the specified source IP address and port number to the destination IP address and port number. The internal error can be an error on the external ICAP server, the security device, or some resource constraint limit. The reason for the internal error is specified in < string3 > . The ICAP scanner passes or drops the specified traffic.
Action	To pass traffic, specify the CLI command, set av all fail-mode traffic permit.

Message	AV: VIOLATION FOUND: ⟨*IP address*⟩:⟨*integer*⟩->⟨*IP address*⟩:⟨*string*⟩%.64s⟨*string*⟩ total ⟨*integer*⟩, id ⟨*integer*⟩: violation ⟨*string*⟩ action ⟨*string*⟩.(file ⟨*string*⟩)
Meaning	The external ICAP AV scanner detects a virus in the traffic from the specified source IP address and port number to the specified destination IP address and port number. The text string at the end of the message contains the name of the contaminated file, the name of the detected virus, and the action taken on the contaminated file. The variables in the message is defined as follows: <string1> Specifies an AV file name or an empty string <string2> Specifies file content type (for example, http url: http://) or an empty string <64 byte long string> Specifies an AV file name or an empty string <string3> Specifies an AV file name or an empty string <number1> Specifies the number of current violations <number2> Specifies the index number of the current violation <string4> If the violation is associated with a file, then the <filename> or else "TRAFFIC" is specified. <string5> Specifies name/description of the violation or an empty string <string6> Specifies the action taken for that violation: not fixed, repaired, or deleted
Action	The virus is handled according to the configuration on the external ICAP AV server.

Warning (00566)

Message	APP session ⟨*IP address*⟩:⟨*integer*⟩->⟨*IP address*⟩:⟨*integer*⟩ is aborted due to ⟨*string*⟩ with code ⟨*integer*⟩.
Meaning	Application (FTP, HTTP, POP3, SMTP, IMAP) session from ip_address1 to ip_address2 is aborted because of <string>.
Action	The <string> can be an event such as "run out of packet" or "xxx allocation failure xxx" generated when the system runs out of packet/memory. If you get these messages sequentially, then set max-content-size to a smaller value (set av scan-mgr max-content-size <number>). If your <string> is of the format "xxx parse xxx error," then the application protocol (ftp/http/pop3/smtp/imap) failed to parse the traffic. If your <string> is of the format "sending xxx error," then the session is aborted because it ran out of packets or the session is in an error state. If the application failed to parse the traffic, then collect the ethereal trace at both client and server side and report this issue to Juniper Networks technical support. If the session did not run out of packets, but is in an error state, then you can resend the request. If retry does not help, then collect the ethereal trace at both client and server side and report this issue to Juniper Networks technical support. Open a support case using the Case Manager link at www.juniper.net/support

Message	APP session ⟨*IP address*⟩:⟨*integer*⟩- > ⟨*IP address*⟩:⟨*integer*⟩ notification email failed due to ⟨*string*⟩ with code ⟨*integer*⟩.
Meaning	Application (SMTP, POP3, and IMAP) session failed to send email notification.
Action	Make sure the mail server is Set with the CLI command, set admin mail server-name < string > Accessible from the device Up and running. Use the unset av profile and unset { smtp |pop3|imap } email-notify commands to disable email-notification.

Notification (00066)

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if a corrupt file is detected.
Meaning	The AV scanner is set to drop or pass the content of an incoming message if it contains a corrupted file.
Action	No recommended action.

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if a password protected file is detected.
Meaning	The AV scanner is set to drop or pass the content of an incoming message if the message contains a password protected file.
Action	No recommended action.

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if any error occurs.
Meaning	The AV scanner is set to permit traffic to pass through when an error condition occurs.
Action	No recommended action.

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if content size exceeds maximum.
Meaning	The AV scanner is set to drop or pass the content of an incoming message if it exceeds the configured value for maximum content size.
Action	Increase the value of the maximum content size if you want to scan traffic or unset the drop option if you want the security device to pass unexamined traffic.

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if number of decompress layers exceeds maximum.
Meaning	The AV scanner is set to drop or pass the content of an incoming message if number of decompress layers exceeds the default or configured value for the protocol.
Action	No recommended action.

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if the firewall runs out of resources.
Meaning	The AV scanner is set to drop or pass the content of an incoming message if the device is out of resources.
Action	No recommended action.

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if the operation times out.
Meaning	The AV scanner is set to drop or pass the content of an incoming message if the operation times out.
Action	No recommended action.

Message	AV fail mode is set to ⟨*string*⟩ unexamined traffic if the scan engine is not ready.
Meaning	The AV scanner is set to drop or pass the content of an incoming message if the scan engine is not ready.
Action	No recommended action.

Message	AV HTTP sets webmail pattern ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩.
Meaning	The AV scanner is configured with a different webmail string type to examine for virus patterns. When the URL matches all of the following parameters, the AV scanner performs a virus scan: string2 specifies URL arguments that begin with a question mark (?). string3 specifies the host name included in the URL. string4 specifies the URL path for the Webmail type. Begin the URL path with a backslash (/).
Action	No recommended action.

Message	AV HTTP trickling setting to be trickling ⟨*integer*⟩ byte for every ⟨*integer*⟩ KB if content length is larger than ⟨*integer*⟩ KB, timeout interval is ⟨*integer*⟩ seconds.
Meaning	Trickling automatically forwards specified amounts of unscanned HTTP traffic to the requesting HTTP host. Trickling prevents the host from timing out for one of the following two reasons: if the AV scanner is busy examining downloaded HTTP files or if the file transfer is slow because of the speed of the link. The AV HTTP trickling command is configured to trickle the specified number of bytes of content for every specified KB scanned and to initiate trickling when the HTTP file is equal to the specified amount of KB or larger. If timeout interval is set to a non zero value, some amount of data is trickled for the configured number of seconds.
Action	No recommended action.

Message	AV HTTP trickling setting to be trickling ⟨*integer*⟩ byte for every ⟨*integer*⟩ Mb, if content length is larger than ⟨*integer*⟩ MB.
Meaning	Trickling automatically forwards specified amounts of unscanned HTTP traffic to the requesting HTTP host. Trickling prevents the host from timing out while the AV scanner is busy examining downloaded HTTP files. The length (number1)of each trickle of unscanned HTTP traffic that the security device forwards to the host. The size (number2) of each block of traffic the security device sends to the AV scanner. The minimum HTTP file size (number3) needed to trigger the trickling action.
Action	No recommended action.

Message	AV HTTP turns off HTTP trickling.
Meaning	The AV scanner is not configured for trickling, so the security device does not forward specified amounts of unscanned HTTP traffic to the requesting HTTP host. Trickling prevents the host from timing out while the AV scanner is busy examining downloaded HTTP files.
Action	No recommended action.

Message	AV HTTP turns ⟨*string*⟩ HTTP connection header close modification.
Meaning	The AV scanner uses the HTTP close connection option to prevent the device from modifying a connection header for each request.
Action	No recommended action.

Message	AV HTTP turns ⟨*string*⟩ HTTP webmail scanning.
Meaning	The AV scanner is enabled for Webmail scanning only.
Action	If you want a full HTTP scan, then disable this parameter and make sure a policy enabling HTTP exists.

Message	AV HTTP unsets webmail pattern ⟨*string*⟩.
Meaning	The AV scanner is enabled for HTTP Webmail scanning only. The AV scanner directs the device to exclude webmail traffic that matches string1 and string2.
Action	No recommended action.

Message	AV maximum content size is set to ⟨*integer*⟩ KB.
Meaning	The maximum content size that the AV scanner scans for viruses is set to the specified value.
Action	No recommended action.

Message	AV maximum number of concurrent messages is set to ⟨*integer*⟩.
Meaning	The value specifies the maximum number of concurrent messages that the internal AV scanner scans for virus patterns. If you enable the drop option and the number of messages exceeds the maximum, the internal AV scanner drops the latest message content. The maximum number of concurrent messages supported is device dependent. See the product Release Notes for the maximum concurrent messages supported on each device.
Action	No recommended action.

Message	AV object ⟨*string*⟩ ⟨*string*⟩ is enabled with timeout ⟨*integer*⟩.
Meaning	An admin has enabled AV scanning for the application with the specified timeout. The string variables, for example can be the scan-mgr and the application.
Action	No recommended action.

Message	AV object ⟨*string*⟩ ⟨*string*⟩ is enabled with timeout ⟨*integer*⟩.
Meaning	An admin has enabled AV scanning for the application with the specified timeout. The string variables, for example can be the scan-mgr and the application.
Action	No recommended action.

Message	AV per client allowed resource is set to ⟨*integer*⟩ percent.
Meaning	The number of resources (number of connections, expressed as a percentage of total resources) that the AV scanner is allowed to use per client.
Action	No recommended action.

Message	AV queue size is set to ⟨*integer*⟩.
Meaning	The AV queue size determines the number of messages that each of the 16 queues can support simultaneously. After the security device sends 16 data units to the internal scanner, it stores subsequent data units in queues to await scanning.
Action	No recommended action.

Message	SCAN-MGR: Set scan-mgr pattern-update use-proxy
Meaning	The AV scanner is set to use-proxy.
Action	No recommended action.

Message	SCAN-MGR: Unset scan-mgr pattern-update use-proxy
Meaning	The AV scanner is unset to use-proxy.
Action	No recommended action.

Notification (00081)

Message	ICAP server ⟨*string*⟩ has maximum connections set to ⟨*integer*⟩.
Meaning	The maximum number of connections that the ICAP server processes concurrently. The upper limit and default values for maximum connections are device-dependent.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ is added to server-group ⟨*string*⟩.
Meaning	An ICAP server is added to the specified server group.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ is disabled.
Meaning	When an ICAP server is disabled, it means that ICAP requests are not sent to the ICAP server.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ is enabled.
Meaning	When an ICAP server is enabled, it means that ICAP requests are sent to the ICAP server.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ is removed from server-group ⟨*string*⟩.
Meaning	An ICAP server is removed from the specified server group.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ is removed.
Meaning	An ICAP server is removed.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ is set with host address ⟨*string*⟩ and port ⟨*integer*⟩.
Meaning	An ICAP server is configured with the specified IP address and port number.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ probe interval is set to ⟨*integer*⟩.
Meaning	The device verifies the health of the specified ICAP server at configured intervals in seconds.
Action	No recommended action.

Message	ICAP server ⟨*string*⟩ probe URL is set to ⟨*string*⟩.
Meaning	The ICAP server is probed with the configured URL string.
Action	No recommended action.

Message	ICAP server-group ⟨*string*⟩ is added.
Meaning	An ICAP server group < group-name > is configured.
Action	No recommended action.

Message	ICAP server-group ⟨*string*⟩ is removed.
Meaning	The specified ICAP server group is removed.
Action	No recommended action.

Notification (00547)

Message	ICAP: Server ⟨*string*⟩ status changed from ⟨*string*⟩ to ⟨*string*⟩.
Meaning	An enabled ICAP server <string> is automatically probed to determine its status (in-service or out-of-service). The ICAP server goes into an out-of-service state when three consecutive probes fail. An auto probe returns an out-of-service result for the following conditions: Firewall cannot establish a successful TCP connection to an ICAP server Invalid ICAP server AV license Client-side error response for ICAP options request Server-side error response for ICAP options request
Action	Verify the ICAP server connectivity and availability.

Notification (00554)

Message	SCAN-MGR: Attempted to load AV pattern file created on %t2 after the AV license expired on %t2.
Meaning	The internal AV scanner was unsuccessful in downloading the AV pattern file created on the specified date, because the AV license key had already expired on a previous date.
Action	Renew the AV license key and re-attempt to update the pattern file.

Message	SCAN-MGR: AV scan engine is ready.
Meaning	The embedded or internal AV scan engine is ready to scan traffic.
Action	No recommended action.

Message	SCAN-MGR: Cannot retrieve AV pattern file due to ⟨*string*⟩ (⟨*integer*⟩). HTTP status code: ⟨*integer*⟩.
Meaning	The device was unable to access or retrieve an AV pattern file from a server, identified by IP address and port number, through HTTP. The error code provides information you need to get help from Juniper Networks technical support.
Action	To contact Juniper Networks technical support: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.)

Message	SCAN-MGR: New AV pattern file has been updated. Version: ⟨*string*⟩; size: ⟨*integer*⟩ bytes.
Meaning	The internal AV scanner successfully updated the AV pattern file and may have changed the size of the file in the process.
Action	No recommended action.

Message	SCAN-MGR: ⟨*string*⟩
Meaning	The security device identifies the IP address of the scan-manager server.
Action	No recommended action.

Message	SCAN-MGR: The URL for AV pattern update server is set to ⟨*string*⟩ and the update interval is set to ⟨*integer*⟩ minutes.
Meaning	An admin changed or added the URL string (IP address or domain name) of an AV pattern update server, and set the update interval to the specified value. The embedded AV scanner uses the specified string to download new pattern files.
Action	No recommended action.

Message	SCAN-MGR: The URL for AV pattern update server is unset and the update interval returned to its default.
Meaning	An admin set the URL back to its default, perhaps with the WebUI or with an unset command (CLI). This prevents any further automatic updates to the AV pattern file.
Action	No recommended action.

Chapter 7
ARP

The following messages relate to the Address Resolution Protocol (ARP).

Critical (00031)

Message	⟨*string*⟩ detected an IP conflict (IP ⟨*IP address*⟩, MAC %m) on interface ⟨*string*⟩
Meaning	An ARP request (or reply) reveals that the specified security device interface uses the same IP address as another network device, which creates a conflict.
Action	Change the IP address of one of the devices.

Critical (00079)

Message	⟨*string*⟩ detected a duplicate VSD group master (IP ⟨*IP address*⟩, MAC %m) on interface ⟨*string*⟩
Meaning	An ARP request detected a second virtual security device master IP address on a specified interface.
Action	Check your current NSRP configuration.

Notification (00031)

Message	ARP detected IP conflict: IP address ⟨*ip*⟩ changed from interface ⟨*if_old*⟩ to interface ⟨*if_new*⟩
Meaning	The Address Resolution Protocol (ARP) service noted that the mapping of interface-to-IP address for the specified IP address changed from < interface1 > to < interface2 > . This can cause future ARP errors.
Action	Map ARP to the correct interface.

Notification (00051)

Message	Static ARP entry added to interface ⟨*string*⟩ with IP ⟨*IP address*⟩ and MAC %m
Meaning	A static Address Resolution Protocol entry was added to or removed from an interface with a specified IP address and MAC address.
Action	No recommended action

Notification (00052)

Message	Static ARP entry deleted from interface ⟨*string*⟩ with IP address ⟨*IP address*⟩ and MAC address %m
Meaning	A static Address Resolution Protocol entry was added to or removed from an interface with a specified IP address and MAC address.
Action	No recommended action

Notification (00053)

Message	ARP always on destination enabled
Meaning	An admin enabled the feature that directs the security device to always perform an ARP lookup to learn a destination MAC address.
Action	No recommended action

Notification (00054)

Message	ARP always on destination disabled
Meaning	An admin disabled the feature that directs the security device to always perform an ARP lookup to learn a destination MAC address.
Action	No recommended action

Notification (00082)

Message	IRDP cli: ⟨*string*⟩ ⟨*string*⟩
Meaning	IRDP informational message.
Action	No recommended action.

Chapter 8
Attack Database

The following messages relate to the attack object database that stores the attack objects used to perform Deep Inspection.

Critical (00767)

Message	WARNING: Current hardware configuration cannot support Deep Inspection. Please upgrade system memory.
Meaning	The flash memory space on the security device is not sufficient to support the Deep Inspection (DI) feature. Some security devices come in two types, namely high memory and low memory.
Action	Upgrade to the high memory security device.

Notification (00767)

Message	Attack database version ⟨*version*⟩ is rejected because the authentication check failed.
Meaning	When downloading the specified version of the attack object database, the security device was unable to verify its integrity.
Action	Attempt to download the attack object database again. If this message repeatedly appears, contact Juniper Networks technical support: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.)

Message	Attack database version ⟨*version*⟩ is ⟨*authenticated*⟩saved to flash.
Meaning	An admin saved the specified version of the Deep Inspection (DI) attack object database to flash memory. If the authentication certificate was loaded on the security device, it also authenticated the attack object database. The security device uses the authentication certificate to check the integrity of the ScreenOS image when the device boots up and an attack object database when downloading it to the device.
Action	No recommended action.

Message	Attack group ⟨*member attack group's name*⟩ is added to ⟨*attack group's name*⟩ ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	An admin added a attack group member to the specified attack group using the WebUI or CLI.
Action	No action recommended.

Message	Attack group ⟨*attack group's old name*⟩ is changed to ⟨*attack group's new name*⟩ ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The specified admin modified the attack group name using the WebUI or CLI.
Action	No action recommended.

Message	Attack group ⟨*attack group name*⟩ is created ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The admin created the specified attack group using the WebUI or CLI.
Action	No action recommended.

Message	Attack group ⟨*attack group name*⟩ is deleted ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The admin deleted the specified attack group using the WebUI or CLI.
Action	No action recommended.

Message	Attack group ⟨*member attack group's name*⟩ is removed from ⟨*attack group's name*⟩ ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	An admin removed the attack group member from the specified attack group using the WebUI or CLI.
Action	No action recommended.

Message	Attack ⟨*attack's name*⟩ is added to attack group ⟨*attack group's name*⟩ ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The admin added an attack to the specified attack group using the WebUI or CLI.
Action	No action recommended.

Message	Attack ⟨*attack's old name*⟩ is changed to ⟨*attack's new name*⟩ ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The specified admin modified the attack name using the WebUI or CLI.
Action	No action recommended.

Message	Attack ⟨*attack name*⟩ is created ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The specified admin created the attack group using the WebUI or CLI.
Action	No action recommended.

Message	Attack ⟨*attack name*⟩ is deleted ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The specified admin deleted the attack group using the WebUI or CLI.
Action	No action recommended.

Message	Attack ⟨*attack's name*⟩ is removed from ⟨*attack group's name*⟩ ⟨*config_changer*⟩ ⟨*admin_name*⟩.
Meaning	The admin deleted an attack from the specified attack group using the WebUI or CLI.
Action	No action recommended.

Message	Cannot download attack database from ⟨*server*⟩ (error ⟨*error message*⟩).
Meaning	The security device was unable to download the attack object database from the specified URL as indicated by the error code identifier.
Action	Confirm that the security device has network connectivity to the attack object database server.

Message	Cannot parse attack database header info.
Meaning	After successfully downloading the Deep Inspection (DI) attack object database, the security device was unable to parse the database or the header information at the top of the database, indicating that either the .dat or .bin file was corrupted. The security device first parses the header information. If that is corrupted, the security device stops parsing and generates the message that it was unable to parse the header information. If the security device successfully parses the header information, but discovers that the content is corrupted, it generates the message that it was unable to parse the attack database.
Action	Download another database to the security device. If the problem persists, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Cannot parse attack database.
Meaning	After successfully downloading the Deep Inspection (DI) attack object database, the security device was unable to parse the database or the header information at the top of the database, indicating that either the .dat or .bin file was corrupted. The security device first parses the header information. If that is corrupted, the security device stops parsing and generates the message that it was unable to parse the header information. If the security device successfully parses the header information, but discovers that the content is corrupted, it generates the message that it was unable to parse the attack database.
Action	Download another database to the security device. If the problem persists, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Cannot save attack database version ⟨*version*⟩.
Meaning	The security device was unable to save the specified Deep Inspection (DI) attack object database to flash memory, possibly because of insufficient RAM.
Action	Enter the "get memory command" to see how much RAM has been allocated and how much is still available. If the available RAM is insufficient, switch the database when the amount of traffic becomes less and more RAM is available.

Message	Cannot switch to attack database version ⟨*version*⟩.
Meaning	The security device was unable to change the Deep Inspection (DI) attack object database from the current version to the specified version. When the security device changes from one attack database to another, it must downgrade the protection of all active sessions to which policies with a Deep Inspection component apply from firewall/Deep Inspection to firewall-only. Depending on the number of currently active sessions, the security device might have insufficient RAM to complete the database exchange.
Action	Enter the "get memory command" to see how much RAM has been allocated and how much is still available. If the available RAM is insufficient, switch the database when the amount of traffic becomes less and more RAM is available.

Message	Deep Inspection update key is expired.
Meaning	The license key permitting attack object database updates has expired.
Action	Obtain and load a new license key.

Chapter 9
Attacks

The following messages concern reports of attacks detected through the application of a SCREEN option or Deep Inspection. Messages related to SCREEN and Deep Inspection settings are also included.

Emergency

Message	Ping of Death! From ⟨*src_ip*⟩ to ⟨*dst_ip*⟩, proto 1 (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected an attempted Ping of Death attack at the specified interface, from the specified source IP address, destined for the specified IP address, and using the specified protocol (1). The number of times the attack occurred indicates how many consecutive oversized ICMP echo requests (or PINGs) per second the security device received. When encountering a Ping of Death attack, the security device detects grossly oversized ICMP packets and rejects them.
Action	Investigate the source IP address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois

Emergency

Message	SYN flood! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected an excessive number of SYN packets arriving at the specified interface from the specified source IP address and port, destined for the specified IP address and port, and using Transmission Control Protocol (TCP). The number of times the attack occurred indicates how many consecutive times per second the internal timer detected SYN packets in excess of the SYN attack alarm threshold.
Action	First determine if a valid SYN flood attack triggered the alarm. If the traffic originated from a small number of consistently fixed IP addresses or was destined for a popular server, it might be a false alarm. In that case, you might want to adjust the SYN flood alarm threshold. If the traffic came from a wide range of non contiguous IP addresses or was bound for IP addresses that do not normally receive much traffic, it was probably an attack. In that case, contact your network security officer (NSO) and your upstream service provider to resolve the issue.

Emergency

Message	Teardrop attack! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected a Teardrop attack at the specified interface, from the specified source IP address and port, destined for the specified IP address and port, and using the specified protocol. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number of times the attack occurred indicates how many consecutive fragmented packets per second the security device received and was unable to reassemble because of discrepant fragment sizes and offset values. A Teardrop attack exploits the reassembly of fragmented packets, altering the offset values used when recombining fragments so that the target device cannot successfully complete the reassembly procedure. A flood of such packets can force the target device to expend all its resources on reassembling fragmented packets, causing a denial-of-service (DoS) for legitimate traffic.
Action	Investigate the source IP address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO).

Alert

Message	Address sweep! From ⟨*src_ip*⟩ to ⟨*dst_ip*⟩, proto 1 (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected an excessive number of IP address scans arriving at the specified interface from the specified source IP address and port, and using the ICMP protocol. (Note: The destination IP address that appears in the message is the one in the packet that triggered the address sweep detection feature.) The number indicates how many consecutive times per second the internal timer detected IP addresses being scanned in excess of the address sweep alarm threshold.
Action	Investigate the source IP address. If the address belongs to a server, verify that it is not infected with a port-scanning worm. If the address raises suspicion, notify your network security officer (NSO) and resolve the issue with the owner of the address. Note: If you enable logging on your basic inbound "deny any" policy, all inbound denied packets are logged in the logging table associated with that policy. This allows you to check for patterns of activity and more easily discern suspicious activity from innocent.

Alert

Message	ICMP flood! From ⟨*src_ip*⟩ to ⟨*dst_ip*⟩, proto 1 (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected an excessive number of ICMP echo requests arriving at the specified interface from the specified source IP address, and destined for the specified IP address. The number indicates how many consecutive times the internal timer detected ICMP echo requests in excess of the ICMP attack alarm threshold.
Action	First determine if a valid ICMP flood attack triggered the alarm. If the traffic originated from a small number of consistently fixed IP addresses or was destined for a popular server, it might be a false alarm. In that case, you might want to adjust the ICMP flood alarm threshold. If the traffic came from a wide range of noncontiguous IP addresses or was bound for IP addresses that do not normally receive much traffic, it was probably an attack. In that case, contact your network security officer (NSO) and your upstream service provider to resolve the issue.

Alert

Message	IP spoofing! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto **{** TCP | UDP | ⟨*number1*⟩ **}** (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected and rejected a packet having a source IP address and arriving at an interface that conflicts with the security route table. Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected incidents of spoofed IP packets.
Action	If the IP spoofing continues long enough and you consider it worth the effort, contact your upstream service provider to initiate a backtracking operation, basically tracking packets with the spoofed address from router to router back to their actual source. After locating the source, investigate it to determine if it is the instigator or merely an innocent and unwitting pawn hosting a "zombie agent" controlled by another device.

Alert

Message	Land attack! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected and blocked SYN packets whose source IP addresses have been spoofed to be the same as the destination addresses. The packets used TCP and arrived at the specified interface. The number indicates how many consecutive times per second the internal timer detected incidents of spoofed IP packets with identical source and destination IP addresses. By combining elements of the SYN flood defense and IP Spoofing detection, the security device blocks any attempted attacks of this nature.
Action	If the attack continues long enough and you consider it worth the effort, contact your upstream service provider to initiate a backtracking operation, basically tracking packets with the spoofed address from router to router back to their actual source. After discovering the source, investigate it to determine if it is the instigator or merely an innocent and unwitting pawn hosting a "zombie agent" controlled by another device.

Alert

Message	Port scan! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected an excessive number of port scans arriving at the specified interface from the specified source IP address and port, destined for the specified IP address, and using the specified protocol. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message. Also, the destination port number that appears in the message is the one in the packet that triggered the port scan detection feature.) The number indicates how many times the event was logged.
Action	Investigate the source IP address. If the address belongs to a server, verify that it is not infected with a port-scanning worm. If the address raises suspicion, notify your network security officer (NSO) and resolve the issue with the owner of the address. Note: If you enable logging on your basic inbound "deny any" policy, all inbound denied packets are logged in the logging table associated with that policy. This allows you to check for patterns of activity and more easily discern suspicious activity from innocent.

Alert

Message	Source Route IP option! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected and blocked a packet having the source route option enabled in its header. The packet came from the specified source IP address and port number, bound for the specified destination address and port number, using the specified protocol, and arriving at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets with the source route option enabled in their headers. In IP, the source route option can contain routing information that specifies a different source IP address than that in the packet header. The security device rejects any packets with this option enabled.
Action	Investigate the source IP address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO).

Alert

Message	UDP flood! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto UDP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected an excessive number of UDP packets arriving at the specified interface from the specified source IP address and port, destined for the specified IP address and port, and using User Datagram Protocol (UDP). The number indicates how many consecutive times the internal timer detected UDP packets in excess of the UDP attack alarm threshold.
Action	First, determine if this was indeed a UDP flood attack by checking whether the security device is processing Voice-over-IP (VoIP) or Video over IP (H.323) traffic, which can appear to the device as a flood of UDP traffic. Second, determine if this was an attack by checking if the traffic originated from a small number of consistently fixed IP addresses or was destined for a popular server. If so, it might be a false alarm, and you might want to adjust the ICMP flood alarm threshold. If the traffic came from a wide range of noncontiguous IP addresses or was bound for IP addresses that do not normally receive much traffic, it was probably an attack. In that case, contact your network security officer (NSO) and your upstream service provider to resolve the issue.

Alert

Message	WinNuke attack! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:139, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected and corrected the overlapping offset value of a NetBIOS Session Service (port 139) packet from the specified source IP address and port number, destined for the specified address, using TCP, and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected tampered NetBIOS Session Service (port 139) packets.
Action	Investigate the source IP address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO).

Critical

Message	ActiveX control blocked! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected and blocked a packet containing an ActiveX control from the specified source IP address, to the specified destination IP address, using the specified protocol, and arriving at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets from and to the same addresses containing ActiveX controls.
Action	No recommended action

Critical

Message	Bad IP option! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device detected a packet in which the list of IP options in the IP datagram header is incomplete or malformed. The packet came from the specified source IP address and port number, bound for the specified destination address and port number, using the specified protocol, and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected TCP packets with an incomplete or malformed IP options list.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	Dst IP session limit! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected an excessive number of packets to the same destination IP address, using the specified protocol, and arriving at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets in excess of the session threshold. The source IP address that appears in this message is the address that happened to be in the packet that reached the destination IP session threshold.
Action	Investigate the destination IP address and check the session threshold setting. If the address belongs to a server with a high number of sessions, valid traffic to the address might exceed the threshold. In that case, you might want to adjust the threshold. If the destination address raises suspicion, notify your network security officer (NSO).

Critical

Message	EXE file blocked! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected and blocked a packet containing an .exe file from the specified source IP address, to the specified destination IP address, using the specified protocol, and arriving at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets from and to the same addresses containing .exe files.
Action	No recommended action

Critical

Message	FIN but no ACK bit! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	TCP packets with the FIN flag set normally also have the ACK bit set. The security device has detected a packet in which the FIN flag is set but the ACK bit is not set in the flags field. The packet came from the specified source IP address and port number, bound for the specified destination address and port number, using the specified protocol, and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected TCP packets that do not have both FIN flag and ACK bit set.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	Fragmented traffic! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	An admin has enabled the SCREEN option that allows the security device to block all IP packet fragments that it receives at interfaces bound to a specific security zone.
Action	No recommended action

Critical

Message	ICMP fragment! From ⟨*src_ip*⟩ to ⟨*dst_ip*⟩, proto 1 (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device detected a fragmented ICMP packet. The packet came from the specified source IP address, bound for the specified destination address, using protocol 1, and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected fragmented ICMP packets between the same source and destination addresses.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	Java applet blocked! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected and blocked a packet containing a Java applet from the specified source IP address, to the specified destination IP address, using the specified protocol, and arriving at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets from and to the same addresses containing Java applets.
Action	No recommended action

Critical

Message	Large ICMP packet! From ⟨*src_ip*⟩ to ⟨*dst_ip*⟩, proto 1 (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device detected an ICMP packet larger than 1024 bytes. The packet came from the specified source IP address, bound for the specified destination address, using protocol 1, and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected fragmented ICMP packets between the same source and destination addresses.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	Malicious URL! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected and rejected a HyperText Transport Protocol (HTTP) packet with a URL containing a malicious string used to attack Web servers. The packet came from the specified source IP address and port number, bound for the specified destination address and port number, using the Transmission Control Protocol (TCP), and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected packets with such malicious URL strings.
Action	No recommended action

Critical

Message	No TCP flag! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto **{** TCP | UDP | ⟨*number1*⟩ **}** (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected a TCP packet with no bits set in the flags field. The packet came from the specified source IP address and port number, bound for the specified destination address and port number, using the specified protocol, and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected TCP packets without any flags set.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	Src IP session limit! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto **{** TCP | UDP | ⟨*number1*⟩ **}** (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected an excessive number of packets from the same source IP address, using the specified protocol, and arriving at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets in excess of the session threshold. The destination IP address that appears in this message is the address that happened to be in the packet that reached the source IP session threshold.
Action	Investigate the source IP address and check the session threshold setting. If the address belongs to a server with a high number of sessions, valid traffic from the address might exceed the threshold. In that case, you might want to adjust the threshold. If the source address raises suspicion, check if it is infected with a port-scanning worm (which can quickly generate thousands of sessions) and notify your network security officer (NSO)

Critical

Message	SYN and FIN bits! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	Both the SYN and FIN flags are not normally set in the same packet. The security device has detected a packet with both SYN and FIN flags set. The packet came from the specified source IP address and port number, bound for the specified destination address and port number, and arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected TCP packets with both SYN and FIN flags set.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	SYN fragment! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has detected and blocked fragmented SYN segments arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected incidents of fragmented SYN segments with identical source and destination IP addresses.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	SYN-ACK-ACK Proxy DoS! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto TCP (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number*⟩ times.
Meaning	The security device has created a number of SYN-ACK-ACK sessions in excess of the SYN-ACK-ACK proxy threshold. The sessions initiated from the same source IP address and were destined for the same destination IP address. They used TCP and arrived at the specified interface, which is bound to the security zone mentioned. The number indicates how many consecutive times per second the internal timer detected packets in excess of the SYN-ACK-ACK proxy threshold.
Action	Investigate the source IP address and notify your network security officer (NSO).

Critical

Message	Unknown protocol! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto ⟨*number1*⟩ (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected and blocked traffic using an unknown protocol (with a protocol number of 137 or greater) arriving at the specified interface. The number indicates how many consecutive times per second the internal timer detected packets using an unknown protocol with identical source and destination IP addresses.
Action	If this occurs repeatedly from the same source IP address, investigate the address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address. If the source address raises suspicion, notify your network security officer (NSO)

Critical

Message	ZIP file blocked! From ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dst_ip*⟩:⟨*dst_port*⟩, proto { TCP | UDP | ⟨*number1*⟩ } (zone ⟨*zone_name*⟩, int ⟨*interface_name*⟩). Occurred ⟨*number2*⟩ times.
Meaning	The security device has detected and blocked a packet containing a .zip file from the specified source IP address, to the specified destination IP address, using the specified protocol, and arriving at the specified interface. (Note: If the protocol is not TCP or UDP, the source and destination port numbers are not included in the message.) The number indicates how many consecutive times per second the internal timer detected packets from and to the same addresses containing .zip files.
Action	No recommended action

Critical (00024)

Message	⟨*string*⟩ has overflowed.
Meaning	The number of entries in the specified log has exceeded the maximum allowed in the specified log.
Action	Clear the log entries.

Notification (00002)

Message	Bypass non-IP traffic option is ⟨*action*⟩.
Meaning	An admin has either enabled or disabled one of the following packet handling options: The security device permits IPSec traffic not destined for itself to pass through the firewall when the interfaces are in Transparent mode. The security device does not act as a VPN tunnel gateway but passes the IPSec packets onward to other gateways. The security device permits non-IP traffic, such as IPX, to pass through the firewall when the interfaces are in Transparent mode. (ARP is a special case for non-IP traffic. It is always passed, even if when this feature is disabled.)
Action	No recommended action.

Message	Bypass-others-IPSec option is ⟨*action*⟩.
Meaning	An admin has either enabled or disabled one of the following packet handling options: The security device permits IPSec traffic not destined for itself to pass through the firewall when the interfaces are in Transparent mode. The security device does not act as a VPN tunnel gateway but passes the IPSec packets onward to other gateways. The security device permits non-IP traffic, such as IPX, to pass through the firewall when the interfaces are in Transparent mode. (ARP is a special case for non-IP traffic. It is always passed, even if when this feature is disabled.)
Action	No recommended action.

Message	Logging of dropped traffic to self (excluding multicast) has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of dropped unicast traffic destined for the security device itself.
Action	No recommended action.

Message	Logging of dropped traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of dropped traffic destined for the security device.
Action	No recommended action.

Message	Logging of ICMP traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of ICMP traffic destined for the security device.
Action	No recommended action.

Message	Logging of IKE traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of IKE traffic destined for the security device.
Action	No recommended action.

Message	Logging of SNMP traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of SNMP traffic destined for the security device.
Action	No recommended action.

Message	Malicious URL ⟨*service_name*⟩ is ⟨*service_action*⟩ for ⟨*service_dest_type*⟩ ⟨*service_dest_name*⟩.
Meaning	An admin has added, deleted, or modified the a URL address string for the named zone.
Action	No recommended action.

Message	⟨*service_name*⟩ is ⟨*service_status*⟩ on ⟨*service_dest_type*⟩ ⟨*service_dest_name*⟩ ⟨*admin*⟩.
Meaning	The specified SCREEN option has been enabled or disabled for the named zone.
Action	No recommended action.

Message	⟨*service_name*⟩ is set to ⟨*service_threshold*⟩ for ⟨*service_dest_type*⟩ ⟨*service_dest_name*⟩.
Meaning	An admin has set a value for the specified SCREEN option parameter for the named zone.
Action	No recommended action.

Message	Screening of all attacks is ⟨*action*⟩ on ⟨*service_dest_type*⟩ ⟨*service_dest_name*⟩ ⟨*admin*⟩.
Meaning	An admin has enabled or disabled the screening of all attacks destined for the security device itself.
Action	No recommended action.

Message	Logging of TELNET traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of TELNET traffic destined for the security device.
Action	No recommended action.

Message	Logging of NSM traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of NSM traffic destined for the security device.
Action	No recommended action.

Message	Logging of SSH traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of SSH traffic destined for the security device.
Action	No recommended action.

Message	Logging of WEB traffic to self has been ⟨*action*⟩.
Meaning	An admin has enabled or disabled the logging of WEB traffic destined for the security device.
Action	No recommended action.

Information (00534)

Message	⟨*string*⟩ is cleared.
Meaning	An admin has cleared all attack log information.
Action	No recommended action.

Chapter 10
Auth

The following messages relate to user authentication.

Critical (00015)

Message	Administrator's password complexity is set to scheme '⟨*length*⟩' by admin '⟨*admin_name*⟩'.
Meaning	The identified admin set the complexity of the admin password scheme.
Action	No action recommended.

Message	Administrator's password minimum length is set to '⟨*length*⟩' by admin '⟨*admin_name*⟩'.
Meaning	The identified admin configured the minimum password length.
Action	No action recommended.

Message	Auth user's password complexity is set to scheme '⟨*length*⟩' by admin '⟨*admin_name*⟩'.
Meaning	The identified admin set the complexity of the auth user password scheme.
Action	No action recommended.

Message	Minimum length of Auth user's password is set to '⟨*length*⟩' by admin '⟨*admin_name*⟩'.
Meaning	The identified admin set the minimum length of the Auth user password.
Action	No action recommended.

Critical (00518)

Message	Admin user '⟨*user_name*⟩' authorization failure: Password does not comply with password policy.
Meaning	The identified admin user authorization failed, because the admin password does not meet the password policy requirements.
Action	Investigate and determine whether it was an attempt to illegally access the security device. Admin user passwords must contain at least two upper case letters, two lower case letters, two digits, and two special characters.

Message	Auth user ⟨*user_name*⟩ authorization failure: Password does not comply with password policy.
Meaning	The identified Auth user authorization failed, because the password does not meet the password policy requirements.
Action	Investigate and determine whether it was an attempt to illegally access the security device. Auth user passwords must contain at least two upper case letters, two lower case letters, two digits, and two special characters.

Warning

Message	Active Server Switchover: New requests for ⟨*user_name*⟩ server will try ⟨*active server role*⟩ from now on.
Meaning	The WebAuth user session is terminated using forced timeout because the user exceeded the access time. Only the time and duration of the access time is specified; the auth server name is not displayed.
Action	No recommended action.

Warning

Message	Authentication for client ⟨*client_ip*⟩ was denied (too long a password).
Meaning	The provided password is too long.
Action	Check the password; the length of the password should not exceed 128 characters.

Warning

Message	Authentication for client ⟨*client_ip*⟩ was denied (too long a user name).
Meaning	The provided user name is too long.
Action	Check the user name; the length of the user name should not exceed 64 characters.

Warning (00518)

Message	Authentication for user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was denied (long password).
Meaning	Authentication is denied for the user at the specified IP address, because the length of the password (or password + SecurID) exceeds 128 characters.
Action	The password (password + SecurID) length should be less than 128 characters or investigate to determine whether it was an attempt to illegally access the security device.

Message	Authentication for user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was denied (long password).
Meaning	Authentication is denied for the user at the specified IP address, because the length of the password (or password + SecurID) exceeds 128 characters.
Action	The password (password + SecurID) length should be less than 128 characters or investigate to determine whether it was an attempt to illegally access the security device.

Message	Authentication for user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was denied (long username).
Meaning	Authentication is denied for the user at the specified IP address, because firewall received a username greater than 64 characters.
Action	Username must be less than or equal to 64 characters. Use a shorter username or investigate and determine whether it was an attempt to illegally access the security device.

Message	Authentication for user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was denied (long username).
Meaning	Authentication is denied for the user at the specified IP address, because firewall received a username greater than 64 characters.
Action	Username must be less than or equal to 64 characters. Use a shorter username or investigate and determine whether it was an attempt to illegally access the security device.

Message	Error in authentication for WebAuth user ⟨*user_name*⟩ at ⟨*client_ip*⟩
Meaning	The user attempted authentication via the WebAuth authentication server, but encountered an error condition.
Action	No recommended action.

Message	Local authentication for user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was denied⟨*reason*⟩.
Meaning	The specified user was rejected by the security device because the user name was not in the local database.
Action	No recommended action.

Message	Local authentication for WebAuth user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was denied⟨*reason*⟩
Meaning	The specified WebAuth user was rejected by the security device because the user name was not in the local database. The reason the user was denied access is displayed.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ is challenged by the ⟨*auth_server_type*⟩ server at ⟨*auth_server_ip*⟩. (Rejected because challenge is not supported for FTP).
Meaning	The specified server sent a challenge to the specified user.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ is challenged by the ⟨*auth_server_type*⟩ server at ⟨*auth_server_ip*⟩. (Rejected because challenge is not supported for Web).
Meaning	The specified server sent a challenge to the specified user.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ is rejected by the ⟨*auth_server_type*⟩ server at ⟨*auth_server_ip*⟩.
Meaning	The firewall user has been rejected by the specified server.
Action	Investigate this and determine whether it was an attempt to illegally access the security device.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ is rejected by the ⟨*auth_server_type*⟩ server at ⟨*auth_server_ip*⟩.
Meaning	The named firewall user has been rejected by the specified server.
Action	Investigate this and determine whether it was an attempt to illegally access the security device.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ is rejected through the ⟨*auth_server_type*⟩ server at ⟨*auth_server_ip*⟩.
Meaning	The named firewall user has been rejected by the specified server.
Action	Investigate this and determine whether it was an attempt to illegally access the security device.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ ⟨*auth_server_type*⟩ authentication attempt has timed out.
Meaning	The security device could not make a network connection to the RADIUS, SecurID, LDAP, or Local server to authenticate a user, and the attempt has timed out.
Action	Check the network cable connection, the IP address of the authentication server entered on the security device, and the authentication settings on both the security device and the authentication server.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ ⟨*auth_server_type*⟩ authentication attempt has timed out.
Meaning	The security device could not make a network connection to the RADIUS, SecurID, LDAP, or Local server to authenticate a user, and the attempt has timed out.
Action	Check the network cable connection, the IP address of the authentication server entered on the security device, and the authentication settings on both the security device and the authentication server.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ ⟨*auth_server_type*⟩ authentication attempt has timed out.
Meaning	The security device could not make a network connection to the RADIUS, SecurID, LDAP, or Local server to authenticate a user, and the attempt has timed out.
Action	Check the network cable connection, the IP address of the authentication server entered on the security device, and the authentication settings on both the security device and the authentication server.

Message	WebAuth user ⟨*user_name*⟩ at ⟨*client_ip*⟩ is rejected/timed out by the ⟨*auth_server_type*⟩ server at ⟨*auth_server_ip*⟩.
Meaning	The user at the specified IP address has been rejected by the specified WebAuth authentication server.
Action	No recommended action.

Warning (00519)

Message	Local authentication for user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was successful.
Meaning	The user authenticated successfully.
Action	No recommended action.

Message	Local authentication for WebAuth user ⟨*user_name*⟩ at ⟨*client_ip*⟩ was successful
Meaning	The specified WebAuth user successfully authenticated.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*of_group*⟩ is accepted by the ⟨*client_ip*⟩ server at ⟨*auth_server_type*⟩.
Meaning	The named user has been accepted by the specified server.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*of_group*⟩ is accepted by the ⟨*client_ip*⟩ server at ⟨*auth_server_type*⟩.
Meaning	The named user has been accepted by the specified server.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*of_group*⟩ is accepted via the ⟨*client_ip*⟩ server at ⟨*auth_server_type*⟩.
Meaning	The named user has been accepted by the specified server.
Action	No recommended action.

Message	WebAuth user ⟨*user_name*⟩ at ⟨*client_ip*⟩ is accepted by the ⟨*auth_server_type*⟩ server at ⟨*auth_server_ip*⟩.
Meaning	The user at the specified IP address has been accepted by the specified WebAuth authentication server.
Action	No recommended action.

Warning (00520)

Message	Backup1 ⟨*primary_server_name*⟩, backup2 ⟨*backup1_server_name*⟩, and primary ⟨*backup2_server_name*⟩ servers failed.
Meaning	The connection to the specified servers failed.
Action	Verify network connectivity to the specified servers.

Message	Backup2 ⟨*backup2_server_name*⟩, primary ⟨*primary_server_name*⟩, and backup1 ⟨*backup1_server_name*⟩ servers failed.
Meaning	The connection to the specified servers failed.
Action	Verify network connectivity to the specified servers.

Message	Primary ⟨*primary_server_name*⟩, backup1 ⟨*backup1_server_name*⟩, and backup2 ⟨*backup2_server_name*⟩ servers failed.
Meaning	The connection to the specified servers failed.
Action	Verify network connectivity to the specified servers.

Message	Trying backup1 server ⟨*backup1_server_name*⟩.
Meaning	The security device is trying to connect to the specified primary backup server.
Action	No recommended action.

Message	Trying backup2 server ⟨*backup2_server_name*⟩.
Meaning	The security device is trying to connect to the specified secondary backup server.
Action	No recommended action.

Message	Trying primary server ⟨*primary_server_name*⟩.
Meaning	The security device is trying to connect to the specified server.
Action	No recommended action.

Notification

Message	TACACS auth server '⟨*tacacs_port*⟩' port set to '⟨*integer*⟩'.
Meaning	The TCP port used to communicate to the specified TACACS server has been modified.
Action	Confirm that the declared TCP port matches the TCP port declared on the specified TACACS server.

Notification

Message	TACACS auth server '⟨*tacacs_default_port*⟩' port set to default '⟨*integer*⟩'.
Meaning	The TCP port has been declared to be the default TCP port for the specified TACACS server.
Action	Confirm that the declared TCP port on the specified TACACS server is the default TCP port.

Notification

Message	TACACS auth server '⟨*auth_server_obj_name*⟩' shared secret disabled.
Meaning	The shared secret has been cleared for the specified TACACS server.
Action	Note that the specified TACACS server has been effectively disabled.

Notification

Message	TACACS auth server '⟨*auth_server_obj_name*⟩' shared secret modified.
Meaning	The shared secret has been declared for the specified TACACS server.
Action	Confirm that the declared shared secret matches the shared secret declared on the specified TACACS server.

Notification (00015)

Message	Certificate Authority index for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed.
Meaning	An admin configured the security device to use a different Certificate Authority certificate.
Action	No recommended action.

Message	Certificate subject for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed from ⟨*old_cert_name*⟩ to ⟨*new_cert_name*⟩.
Meaning	An admin configured the security device to use a different certificate name.
Action	No recommended action.

Message	Contact interval for Infranet settings changed from ⟨*old_contact_interval*⟩ to ⟨*new_contact_interval*⟩ seconds.
Meaning	An admin changed the contact interval to a specified number of seconds.
Action	No recommended action.

Message	Infranet Enforcer could not connect to Infranet Controller ⟨*infranet_controller_obj_name*⟩ (ip ⟨*infranet_controller_ip*⟩).
Meaning	The Infranet Enforcer was unable to establish connectivity with the Infranet Controller.
Action	Set an IP address or name for the Infranet Controller.

Message	Infranet Enforcer could not connect to the Infranet Controller because a socket could not be created.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because of a failure to create a new socket on the Controller.
Action	Check system resources, especially the number of sockets in the system.

Message	Infranet Enforcer could not connect to the Infranet Controller because a socket is already connected.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because another device has established a SSL socket with the Controller.
Action	No recommended action.

Message	Infranet Enforcer could not connect to the Infranet Controller because no certificate is set for the Controller.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because there is no certificate set for the Controller.
Action	Set up ca-idx for the Infranet Controller.

Message	Infranet Enforcer could not connect to the Infranet Controller because no IP address is set for the Controller.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because there was no IP address specified for the Infranet Controller.
Action	Set an IP address or name for the Infranet Controller.

Message	Infranet Enforcer could not connect to the Infranet Controller because no password is set for the Controller.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because there is no identifiable password set for the Controller.
Action	Set a password for the Infranet Controller.

Message	Infranet Enforcer could not connect to the Infranet Controller because the Controller could not be reached on the network.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because of some network barrier or failure.
Action	Check the Infranet-Enforcer-to-Infranet-Controller network connectivity.

Message	Infranet Enforcer could not connect to the Infranet Controller because the ⟨*outgoing_interface*⟩ interface could not be bound to the socket.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because of a failure to create a new socket on the Controller.
Action	Src-Interface may be null. Specify an interface. Check system resources.

Message	Infranet Enforcer could not connect to the Infranet Controller because the socket could not be bound to SSL protocol.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because of a failure to establish SSL with the socket on the Infranet Controller.
Action	Check SSL configuration.

Message	Infranet Enforcer could not connect to the Infranet Controller because the socket could not be bound.
Meaning	The Infranet Enforcer attempted to establish connectivity with the Infranet Controller, but was unable to because of a failure to create a new socket on the Controller.
Action	Check system resources, especially sockets. The system may be out of TCP ports.

Message	Infranet Enforcer did not receive a keepalive from the Infranet Controller(⟨*infranet_controller_ip*⟩) in the past ⟨*seconds_for_which_no_keepalive*⟩ seconds. Cleaning up internal state.
Meaning	The Infranet Enforcer has not received a keepalive message from the specified Infranet Controller during the specified time interval (expressed in seconds). Therefore, the Infranet Enforcer is clearing out information concerning the Infranet Controller.
Action	Check to see if the Infranet Enforcer has network connectivity to the Infranet Controller. Confirm that the Infranet Controller and its services are up.

Message	IP address for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed from ⟨*old_ip*⟩ to ⟨*new_ip*⟩.
Meaning	An admin changed the IP address for the Infranet Controller to a specified new address.
Action	No recommended action.

Message	Password for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed.
Meaning	An admin changed the password for the specified Infranet Controller.
Action	No recommended action.

Message	Port number for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed from ⟨*old_port*⟩ to ⟨*new_port*⟩.
Meaning	An admin changed the port number for the Infranet Controller.
Action	No recommended action.

Message	Source interface for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed from ⟨*old_intf_name*⟩ to ⟨*new_intf_name*⟩.
Meaning	An admin changed the source interface of the Infranet Controller.
Action	No recommended action.

Message	Timeout action for Infranet settings changed from ⟨*old_timeout_action*⟩ to ⟨*new_timeout_action*⟩.
Meaning	An admin changed the specified action to take when a timeout occurs.
Action	No recommended action.

Message	Admin user ⟨*admin_user*⟩ attempted to verify the encrypted password ⟨*encr_pass*⟩. Verification failed.
Meaning	The security device was unable to verify the password entered by the admin user.
Action	No recommended action.

Message	Admin user ⟨*admin_user*⟩ attempted to verify the encrypted password ⟨*encr_pass*⟩. Verification was successful.
Meaning	The security device successfully verified the password entered by the admin user.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ account type is set to ⟨*acct_types*⟩.
Meaning	An admin set the account type for the specified auth server to auth, XAuth, L2TP or admin.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ authentication timeout is set to ⟨*auth_timeout*⟩.
Meaning	An admin set the authentication timeout. The timeout countdown begins after the completion of the first authenticated session. If a user initiates a new session before the countdown reaches the timeout threshold, then the user does not have to reauthenticate and the timeout countdown resets.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ backup1 name is unset.
Meaning	An admin unset the server name of the primary backup server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ backup1 server name is set to ⟨*backup1_name*⟩.
Meaning	An admin modified the server name of the primary backup server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ backup2 name is unset.
Meaning	An admin unset the server name of the secondary backup server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ backup2 server name is set to ⟨*backup2_name*⟩.
Meaning	An admin modified the server name of the secondary backup server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ fail-over revert interval is set to ⟨*revert_interval*⟩ seconds.
Meaning	The time interval between revert intervals is set for the specified auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ id is set to ⟨*new_as_id*⟩.
Meaning	An admin set the ID of the Auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ is created.
Meaning	An admin created or modified the specified authentication server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ is deleted.
Meaning	An admin removed the specified server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ is modified.
Meaning	An admin created or modified the specified authentication server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ LDAP cn is set to ⟨*ldap_cn*⟩.
Meaning	An admin set the LDAP common name of the specified auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ LDAP dn is set to ⟨*ldap_dn*⟩.
Meaning	An admin set the LDAP distinguished name of the specified auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ LDAP parameters are set to server name: ⟨*auth_server_name_ip*⟩, port: ⟨*ldap_port*⟩, dn: ⟨*ldap_dn*⟩, cn: ⟨*ldap_cn*⟩.
Meaning	An admin set the LDAP parameters for the specified server.
Action	No recommended action

Message	Auth server ⟨*auth_server_obj_name*⟩ LDAP port number is set to ⟨*ldap_port*⟩.
Meaning	An admin set the port that the security device uses to communicate with the LDAP server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ RADIUS port is set to ⟨*radius_port*⟩.
Meaning	An admin configured the port the security device uses to communicate with the RADIUS server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ RADIUS port is unset to default ⟨*default_radius_port*⟩.
Meaning	An admin unset the configured RADIUS port of the specified auth server to use the default port.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ RADIUS retry timeout is set to default of ⟨*default_radius_retry_timeout*⟩.
Meaning	An admin unset the configured RADIUS server retry timeout.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ RADIUS secret is changed.
Meaning	An admin changed the RADIUS shared secret of the specified auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ RADIUS secret is disabled.
Meaning	An admin unset the RADIUS shared secret of the specified auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID auth port is set to ⟨*auth_port*⟩.
Meaning	An admin set the port number that the security device uses to communicate with the SecurID server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID backup1 server name is set to ⟨*backup1_auth_server_name_ip*⟩.
Meaning	An admin configured the primary backup server of the specified auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID client retries is set to ⟨*securid_client_retries*⟩.
Meaning	An admin set the maximum number of retries that are sent to the SecurID server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID server name is set to ⟨*auth_server_name_ip*⟩.
Meaning	An admin configured the SecurID server name.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID timeout is set to ⟨*securid_client_timeout*⟩.
Meaning	An admin set the timeout value of the specified SecurID server on the security device.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID use duress is disabled.
Meaning	An admin activated or deactivated duress mode.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID use duress is enabled.
Meaning	An admin activated or deactivated duress mode.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID uses DES encryption.
Meaning	An admin activated or deactivated duress mode.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ SecurID uses SDI encryption.
Meaning	An admin activated or deactivated duress mode.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ server name is disabled.
Meaning	An admin unset the specified name of the Auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ server name is set to ⟨*auth_server_name_ip*⟩.
Meaning	An admin configured a new server name for the Auth server.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ timeout is unset to default ⟨*default_auth_timeout*⟩.
Meaning	An admin unset the configured timeout of the specified server. It now uses the default timeout.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ type is set to LDAP.
Meaning	An admin configured the security device to use the specified auth server to authenticate auth users.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ type is set to RADIUS.
Meaning	An admin configured the security device to use the specified RADIUS server to authenticate auth users.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ type is set to SecurID.
Meaning	An admin configured the security device to use the specified auth server to authenticate auth users.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ type is unset to default RADIUS.
Meaning	An admin unset the authentication server that was previously configured. The security device uses the default auth server type, which is RADIUS.
Action	No recommended action.

Message	Auth server ⟨*auth_server_obj_name*⟩ username character separator is set to ⟨ > *separator_char*⟩; number of occurrences of character separator is ⟨*num_occurrence*⟩.
Meaning	The character separator used by an auth server is changed, and the permissible number of occurrences for the character is modified.
Action	No recommended action.

Message	Default firewall authentication server is changed to ⟨*auth_server_obj_name*⟩.
Meaning	An admin configured the default authentication server.
Action	No recommended action.

Message	Forced timeout for Auth server ⟨*auth_server_obj_name*⟩ authentication is set to ⟨*auth_forced_timeout*⟩ minutes.
Meaning	The forced timeout setting is set in minutes for the identified Auth server.
Action	No recommended action.

Message	Forced timeout for Auth server ⟨*auth_server_obj_name*⟩ is unset to its default value, ⟨*default_auth_timeout*⟩ minutes.
Meaning	The forced timeout setting for the identified Auth server is set to its default value.
Action	No recommended action.

Message	Host name for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed from ⟨*old_host_name*⟩ to ⟨*new_host_name*⟩.
Meaning	An admin changed the host name of the Infranet Controller to the specified value.
Action	No recommended action.

Message	Infranet Controller ⟨*infranet_controller_obj_name*⟩ is created.
Meaning	An admin created a new Infranet Controller profile.
Action	No recommended action.

Message	Infranet Controller ⟨*infranet_controller_obj_name*⟩ is deleted.
Meaning	An admin removed the name of an Infranet Controller from the device.
Action	No recommended action.

Message	Infranet Enforcer is connected to Infranet Controller ⟨*infranet_controller_obj_name*⟩ (ip ⟨*infranet_controller_ip*⟩).
Meaning	An admin changed the host name of the Infranet Controller. The Infranet Enforcer is a device that sets up an infranet-auth policy, based upon user configuration/roles/access privileges on the Infranet Controller. When a particular user makes a connection request, the Infranet Controller pushes that user's configuration information to the Infranet Enforcer. The Enforcer then establishes an infranet-auth policy for that user. The Infranet Enforcer can have up to eight configured addresses for connectivity with Infranet Controllers. When the Infranet Enforcer starts up, it attempts to establish connectivity with each specified Controller until one attempt is successful. If all attempts fail, the Enforcer tries again. Note: For clear text mode, the Infranet Enforcer admin must set up the infranet-auth policy. For IPSec mode, the Infranet Controller configures this policy on the Infranet Enforcer.
Action	No recommended action.

Message	Number of RADIUS retries for auth server ⟨*auth_server_obj_name*⟩ is set to ⟨*radius_retry_value*⟩.
Meaning	The maximum number of retries for the auth server is updated.
Action	No recommended action.

Message	Timeout for Infranet Controller ⟨*infranet_controller_obj_name*⟩ changed from ⟨*old_timeout*⟩ to ⟨*new_timeout*⟩ seconds.
Meaning	An admin changed the timeout for the specified Infranet Controller to the specified value. The Infranet Enforcer attempts to establish connectivity with one or more identified Controllers until one attempt is successful. The timeout value is the interval (expressed in seconds) between attempts to connect each Infranet Controller.
Action	No recommended action.

Message	WebAuth is set to ⟨*auth_server_obj_name*⟩.
Meaning	An admin configured the specified WebAuth server.
Action	No recommended action.

Notification (00525)

Message	The new PIN for user ⟨*user_name*⟩ at ⟨*client_ip*⟩ is ⟨*accept_or_reject*⟩ by SecurID ⟨*auth_server_ip*⟩.
Meaning	The SecurID server at the identified IP address has accepted or rejected the specified new PIN number of the user.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ has selected a system-generated PIN for authentication with SecurID ⟨*auth_server_ip*⟩.
Meaning	The specified user has accepted the system-generated PIN for use with the SecurID server.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ must enter New PIN for SecurID ⟨*auth_server_ip*⟩.
Meaning	The user at the specified IP address must enter the new PIN to authenticate with the SecurID server at the specified IP address.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ must enter Next Code for SecurID ⟨*auth_server_ip*⟩.
Meaning	The user at the specified IP address must enter the new code to authenticate with the SecurID server at the specified IP address.
Action	No recommended action.

Message	User ⟨*user_name*⟩ at ⟨*client_ip*⟩ must make a New PIN choice for SecurID ⟨*auth_server_ip*⟩.
Meaning	The user at the identified IP address must do one of the following: create a new user-generated PIN, use a new system-generated PIN, or quit the session. The SecurID server is at the specified IP address.
Action	No recommended action.

Notification (00543)

Message	Access for firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩ through the ⟨*auth_server_obj_name*⟩ auth server) by policy id ⟨*policy_id*⟩ is now over.
Meaning	The time period during which the specified firewall user could access hosts through the security device has expired.
Action	No recommended action.

Message	Access for firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩ via the ⟨*auth_server_obj_name*⟩ auth server) by policy id ⟨*policy_id*⟩ is now over due to forced timeout.
Meaning	User session is terminated using forced timeout, because user exceeded the access time. The auth server name and the time and duration of the user access time is specified.
Action	No recommended action.

Message	Access for firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩) by policy id ⟨*policy_id*⟩ is now over due to forced timeout.
Meaning	User session is terminated using forced timeout, because user exceeded the access time. Only time and duration of the access time is specified; auth server name is not displayed.
Action	No recommended action.

Message	Access for firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩) by policy id ⟨*policy_id*⟩ is now over.
Meaning	The time period during which the specified firewall user could access hosts through the security device has expired.
Action	No recommended action.

Message	Access for WebAuth firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩ through the ⟨*auth_server_obj_name*⟩ auth server) is now over due to forced timeout.
Meaning	WebAuth user session is terminated using forced timeout, because user exceeded the access time. The auth server name and the time and duration of the user access time is specified.
Action	No recommended action.

Message	Access for WebAuth firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩ through the ⟨*auth_server_obj_name*⟩ auth server) is now over.
Meaning	The time period during which the specified WebAuth user could access hosts through the security device has expired.
Action	No recommended action.

Message	Access for WebAuth firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩) is now over due to forced timeout.

Message	Access for WebAuth firewall user ⟨*user_name*⟩ at ⟨*client_ip*⟩ (accepted at ⟨*time_connected_at*⟩2 for duration ⟨*duration_connected_for*⟩) is now over.
Meaning	The time period during which the specified WebAuth user could access hosts through the security device has expired.
Action	No recommended action.

Notification (00546)

Message	User ⟨*user_name*⟩ at ⟨*of_group*⟩ is challenged by the ⟨*client_ip*⟩ server at ⟨*auth_server_type*⟩.
Meaning	The specified server sent a challenge to the specified user.
Action	No recommended action.

Notification (00767)

Message	Cannot get route to SecurID server ⟨*server_ip*⟩.
Meaning	The security device cannot find the route to the SecurID server.
Action	Check that the network settings on the security device are correctly configured, and that the SecurID server has an active physical network connection. Check the route table for the correct route to the SecurID server.

Message	FIPS: Attempt to set RADIUS shared secret with invalid length ⟨*secret_len*⟩.
Meaning	The user attempted to set a RADIUS shared secret that has an invalid length. The shared secret is a password shared between the security device and the RADIUS server. The devices use this secret to encrypt the user password that is sent to the RADIUS server.
Action	Check the documentation for your RADIUS server for the permissible shared secret lengths.

Message	The device cannot contact the SecurID server.
Meaning	The security device cannot make a network connection to the SecurID server.
Action	Check that the network and authentication settings on both the security device and the SecurID server are correctly configured, and that the SecurID server has an active physical network connection.

Message	The device cannot send data to the SecurID server.
Meaning	The device cannot send data to the SecurID server because the server does not recognize the device.
Action	Check the network connections and the configuration of the SecurID server.

Message	The dictionary file version on the RADIUS server ⟨*radius_server_dictionary_version*⟩ does not match the version ⟨*ns_device_dictionary_version*⟩ supported on the firewall.
Meaning	The NetScreen dictionary file version number on the RADIUS server does not match with the RADIUS dictionary file supported on the firewall.
Action	Download the latest RADIUS dictionary file from the Juniper Networks Website and update the NetScreen dictionary file on the RADIUS server.

Message	User ⟨*user_name*⟩ belongs to a different group in the RADIUS server than that allowed in the device.
Meaning	The group name in the RADIUS server for the specified user does not match the group name specified in the firewall.
Action	No recommended action.

Chapter 11
BGP

The following messages relate to the Border Gateway Protocol (BGP) dynamic routing protocol.

Critical (00206)

Message	The total number of redistributed routes into BGP in vrouter (⟨*vrouter-name*⟩) exceeded system limit (⟨*system-limit*⟩)
Meaning	The number of redistributed routes into BGP exceeded the limit.
Action	Check the network topology and try to reduce the number of routes.

Notification (00039)

Message	⟨*configuration_command*⟩
Meaning	An administrator set or unset a specified BGP protocol command from within the root context.
Action	No recommended action

Message	⟨*set_or_unset*⟩ virtual router ⟨*vrouter_name*⟩ with the configuration command ⟨*configuration_command*⟩
Meaning	An administrator set or unset a specified BGP protocol command from within the virtual router context.
Action	No recommended action

Message	⟨*set_or_unset*⟩ virtual router ⟨*vrouter_name*⟩ with the BGP protocol ⟨*configuration_command*⟩
Meaning	An administrator set or unset a specified BGP protocol command from within the BGP context.
Action	No recommended action

Information (00542)

Message	BGP instance created for virtual router ⟨*vrouter_name*⟩
Meaning	A BGP virtual routing instance was created.
Action	No recommended action

Message	BGP instance deleted for virtual router ⟨*vrouter_name*⟩
Meaning	A BGP virtual routing instance was deleted from virtual router < vrouter_name >
Action	No recommended action

Message	BGP of vr: ⟨*vr name*⟩, closing the socket: exceeded maximum number of bgp peers allowed (⟨*total_max_num_bgp_peers_cnt*⟩)
Meaning	The administrator is trying to add a BGP peer, but the new peer entry exceeds the maximum number of peers for the specified vrouter.
Action	Check the network topology or try to aggregate routes for BGP peers to decrease the routing entries.

Message	BGP of vr: ⟨*vr name*⟩, failed to add prefix ⟨*ip_address*⟩/⟨*ip_mask_len*⟩ to FDB
Meaning	The system was unable to add the requested IP address to the FDB for the specified vrouter.
Action	No recommended action

Message	BGP of vr: ⟨*vr name*⟩, prefix adding: ⟨*ip_address*⟩/⟨*ip_mask_len*⟩, ribin overflow ⟨*overflow_count*⟩ times (max rib-in ⟨*ribin count*⟩)
Meaning	In the BGP instance running on the specified vrouter, ribin overflow occurred the specified number of times.
Action	No recommended action

Message	BGP of vr: ⟨*vr name*⟩, Route ⟨*ip_address*⟩/⟨*ip_mask_len*⟩ ignored, Path Attr len: ⟨*path_attr_len*⟩ (greater than max. ⟨*max_path_attr_len*⟩)
Meaning	The path attribute length is longer than allowed for the system, and the update is ignored.
Action	Check for an error in the IP address and mask.

Message	BGP peer ⟨*peer_ip_address*⟩ changed to Established state
Meaning	The address of the specified peer BGP virtual routing instance has taken on the IP address of the current routing instance. A BGP session has been established with peer < peer_ip_addr >
Action	No recommended action.

Message	BGP peer ⟨*peer_ip_address*⟩ changed to Idle state
Meaning	The state of the specified BGP peer changed from a connection state to the idle state. In the idle state, the instance cannot establish a connection with another routing instance.
Action	No recommended action.

Message	BGP peer ⟨*peer_ip_address*⟩ created.
Meaning	An administrator either successfully added or removed the specified BGP peer.
Action	No recommended action

Message	BGP peer ⟨*peer_ip_address*⟩ disabled.
Meaning	An administrator disabled the connection between the local BGP routing instance and the specified peer.
Action	No recommended action

Message	BGP peer ⟨*peer_ip_address*⟩ enabled.
Meaning	An administrator successfully enabled the connection between the local BGP routing instance and the specified peer.
Action	No recommended action

Message	BGP peer ⟨*peer_ip_address*⟩ removed.
Meaning	An administrator either successfully added or removed the specified BGP peer.
Action	No recommended action

Message	BGP received route-refresh request from peer ⟨*peer_ip_address*⟩ for afi/safi: ⟨*address-family*⟩/⟨*sub-address-family*⟩
Meaning	A peer with a given IP address has sent a route-refresh request.
Action	No recommended action.

Message	BGP sent route-refresh request to peer ⟨*peer_ip_address*⟩ for afi/safi: ⟨*address-family*⟩/⟨*sub-address-family*⟩
Meaning	A user initiated a route-refresh request locally and the request has been sent to the specified peer.
Action	No recommended action.

Message	⟨*error_string*⟩ invalid error code from notification message
Meaning	The system detected an unrecognizable error code.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	⟨*notification_type*⟩ ⟨*error_string*⟩
Meaning	A BGP routing message error occurred that was either the result of a bad message header, a bad open message, or an updated message. Each error type can result from a variety of error conditions. The following table details each condition with the message error indicated.Connection not Synchronized (message header) Bad Message Length (message header) Bad Message Type (message header) Unsupported Version Number (open message) Bad Peer Autonomous System (open message) Bad BGP Identifier (open message) Unsupported Optional Parameter (open message) Authentication Failure (open message) Unacceptable Hold Time (open message) Malformed Attribute List (update message) Unrecognized Well-known Attribute (update message) Missing Well-known Attribute (update message) Attribute Flags Error (update message) Attribute Length Error (update message) Invalid Origin Attribute (update message) Autonomous System Routing Loop (update message) Invalid NextHop Attribute (update message) Optional Attribute Error (update message) Invalid Network Field (update message) Malformed AS_PATH (update message)
Action	Verify both local and peer BGP configuration.

Chapter 12

Cisco-HDLC

The following messages relate to Cisco-High-Level Data Link Control (HDLC) configurations.

Alert (00087)

Message	Cisco-HDLC detected loop ⟨*times*⟩ times on interface ⟨*interfacename*⟩.
Meaning	A link loop (when the sender receives the same keepalive packet it sent out) has been detected on the interface.
Action	No recommended action

Notification (00076)

Message	CISCO-HDLC keepalive down count value was changed from ⟨*old_val*⟩ to ⟨*new_val*⟩ on interface ⟨*interfacename*⟩.
Meaning	An admin changed the number of consecutive times that the interface must fail to receive a keepalive before the link is considered to be down.
Action	No recommended action.

Message	CISCO-HDLC keepalive interval was changed from ⟨*old_val*⟩ to ⟨*new_val*⟩ on interface ⟨*interfacename*⟩.
Meaning	An admin changed the interval at which the specified interface sends keepalive packets.
Action	No recommended action.

Message	CISCO-HDLC keepalive is ⟨*enable*⟩ on interface ⟨*interfacename*⟩.
Meaning	The specified interface is able to send keepalive packets. This is the default behavior.
Action	No recommended action.

Message	CISCO-HDLC keepalive up count value was changed from ⟨*old_val*⟩ to ⟨*new_val*⟩ on interface ⟨*interfacename*⟩.
Meaning	An admin changed the number of consecutive times that the interface must receive a keepalive before the link is considered to be up.
Action	No recommended action.

Message	Set interface ⟨*interfacename*⟩ encap as cisco-hdlc.
Meaning	An admin configured Cisco HDLC encapsulation on the specified interface.
Action	No recommended action.

Message	Unset interface ⟨*interfacename*⟩ encap from cisco-hdlc.
Meaning	An admin removed Cisco HDLC encapsulation on the specified interface.
Action	No recommended action.

Notification (00571)

Message	CISCO-HDLC is ⟨*status*⟩ on interface ⟨*interfacename*⟩.
Meaning	The protocol is up or down on the specified interface.
Action	No recommended action.

Chapter 13
Device

The following messages concern security device events. The device generates these messages in response to problems or processes that occur at the hardware or ScreenOS level.

Alert (00767)

Message	⟨*upgrade_message*⟩
Meaning	Device file system is damaged.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. Note: You must be a registered Juniper Networks customer.

Critical

Message	Set fan speed failed duty_reg = %2x speed = ⟨*integer*⟩.
Meaning	Failed to write to the PWM register of the fan control chip.
Action	Check the chip/register address, and read/write again to confirm that it is correct.

Critical (00020)

Message	The system memory is low (⟨*alloc_mem*⟩ bytes allocated out of total ⟨*total_mem*⟩ bytes).
Meaning	The system is using more than its normal threshold of allocated memory out of the total memory.
Action	If the memory alarm threshold was set too low, use the set alarm threshold memory command to increase the threshold. (The default is 95 of the total memory.) Check if a firewall attack is in progress. Seek ways to reduce traffic.

Critical (00022)

Message	All fans are now functioning properly.
Meaning	At least one fan that had malfunctioned has returned to normal operation.
Action	No recommended action.

Message	At least one fan is not functioning properly.
Meaning	At least one fan assembly is incorrectly seated, or malfunctioning in some other way.
Action	First check that the fan assembly is properly in place and that nothing is restricting air flow to the fans. If the problem persists, replace the fan assembly.

Message	The battery is not functioning properly.
Meaning	The battery is incorrectly seated, unplugged, or malfunctioning in some other way.
Action	Check to see if the battery is fully seated, that the power cords are plugged in to both power supplies and plugged in to active power sources, and that the power cords are undamaged. If the problem persists, replace the faulty battery.

Message	The battery is now functioning properly.
Meaning	The battery that had malfunctioned has returned to normal operation.
Action	No recommended action.

Message	The power supply ⟨*power_id*⟩ is functioning properly.
Meaning	The specified power supply, which had malfunctioned, has returned to normal operation.
Action	No recommended action.

Message	The power supply ⟨*power_id*⟩ is not functioning properly.
Meaning	The primary or secondary power supply is incorrectly seated, unplugged, or malfunctioning in some other way.
Action	Check to see if the specified power supply is fully seated, that the power cord is plugged in to both the power supply and an active power source, and that the power cord is undamaged. If the problem persists, replace the power supply.

Message	The system temperature (⟨*sys_tempc*⟩ Centigrade, ⟨*sys_tempf*⟩ Fahrenheit) is OK now.
Meaning	The system temperature which had risen sharply has returned to its normal threshold.
Action	No recommended action.

Message	The system temperature (⟨*sys_tempc*⟩ Centigrade, ⟨*sys_tempf*⟩ Fahrenheit) is too high!
Meaning	The system temperature has exceeded the alarm threshold.
Action	First check that the fan assembly is functioning properly. If it is functioning properly, check that nothing is restricting air flow to the fans. If it is not functioning properly, check that the fan assembly is correctly seated. If the problem persists, replace the fan assembly. Also, remove power from the device and wait until it cools. After it reaches an acceptable temperature range, reconnect the device to a power source and evaluate device components (such as the CPU board) to see if it runs too hot. Report your findings to the network admin.

Message	The system temperature: (⟨*sys_tempc*⟩ Centigrade, ⟨*sys_tempf*⟩ Fahrenheit) is severely high!
Meaning	The system temperature has exceeded the alert threshold.
Action	First check that the fan assembly is functioning properly. If it is functioning properly, check that nothing is restricting air flow to the fans. If it is not functioning properly, check that the fan assembly is correctly seated. If the problem persists, replace the fan assembly. Also, remove power from the device and wait until it cools. After it reaches an acceptable temperature range, reconnect the device to a power source and evaluate device components (such as the CPU board) to see if it runs too hot. Report your findings to the network admin.

Critical (00034)

Message	Ethernet driver ran out of rx bd (port ⟨*port_id*⟩).
Meaning	The receive buffer descriptor of the Ethernet driver was depleted. The device performed a run-time recovery.
Action	No recommended action.

Critical (00092)

Message	WAN card ⟨*slot_num*⟩ is not functioning properly and will be restarted.
Meaning	The WAN card in the specified slot is restarting.
Action	No recommended action.

Critical (00612)

Message	Switch error: get ⟨*register type*⟩ register (dev ⟨*device number*⟩, reg ⟨*register number*⟩) fail.
Meaning	Get switch register failed.
Action	Reboot system.

Message	Switch error: set ⟨*register type*⟩ register (dev ⟨*device number*⟩, reg ⟨*register number*⟩, value 0x⟨*register value*⟩) fail.
Meaning	Set switch register failed.
Action	Reboot system.

Critical (00701)

Message	Security Board ⟨*sm_board_id*⟩ System Hanged
Meaning	The security board < board_id > is hanging.
Action	No recommended action

Critical (00702)

Message	Security Board ⟨*slot_num*⟩ CPU ⟨*cpu_num*⟩ Packet Drop Counter ⟨*fulldrp_cnt*⟩
Meaning	The security module is too busy because memory is low.
Action	Install an extra security module if there is a slot available.

Critical (00751)

Message	Switch error: ⟨*error information*⟩.
Meaning	An error occurred when the driver tried to access the switch MAC address.
Action	Reboot system.

Critical (00767)

Message	⟨*upgrade_message*⟩
Meaning	A low-level ScreenOS problem occurred.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. Note: You must be a registered Juniper Networks customer.

Error (00009)

Message	⟨*integer*⟩/⟨*integer*⟩ vid ⟨*integer*⟩ HW vtable leak, total ⟨*integer*⟩ entries.
Meaning	The device detected that entries are missing from the VLAN table. This error indicates a problem with the device.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Notification

Message	Authentication failed from ⟨*phone_number*⟩ CNID on interface s⟨*port_id*⟩/0.
Meaning	Authentication failed.
Action	No recommended action.

Notification

Message	Authentication passed from ⟨*phone_number*⟩ CNID on interface s⟨*port_id*⟩/0.
Meaning	Authentication passed.
Action	No recommended action.

Notification

Message	Authentication timeout from ⟨*phone_number*⟩ CNID on interface s⟨*port_id*⟩/0; the device hangs up the connection.
Meaning	The configured time limit for authentication has been reached so the connection has been terminated.
Action	No recommended action.

Notification

Message	Maximum authentication attempts were reached from ⟨*phone_number*⟩ CNID on interface s⟨*port_id*⟩/0; the device hangs up the connection.
Meaning	The configured number of attempts for authentication has been reached so the connection has been terminated.
Action	No recommended action.

Notification

Message	Modem interface accepts a call received from ⟨*phone_number*⟩ CNID in white list on interface s⟨*port_id*⟩/0.
Meaning	The modem interface accepts an incoming call in the white list of an interface.
Action	No recommended action.

Notification

Message	Modem interface accepts a call received from unknown CNID('⟨*phone_number*⟩') on interface s⟨*port_id*⟩/0,
Meaning	Accept an unknown incoming call of an interface.
Action	No recommended action.

Notification

Message	Modem interface rejects a call received from ⟨*phone_number*⟩ CNID in black list on interface s⟨*port_id*⟩/0.
Meaning	The modem address rejects an incoming call in the black list of an interface.
Action	No recommended action.

Notification

Message	Modem interface rejects a call received from unknown CNID('⟨*phone_number*⟩') on interface s⟨*port_id*⟩/0.
Meaning	The modem interface rejects an unknown incoming call of an interface.
Action	No recommended action.

Notification

Message	Move ⟨*phone_number*⟩ CNID to ⟨*list_name*⟩ on interface s⟨*port_id*⟩/0 failed; CNID has already been in ⟨*list_name*⟩.
Meaning	The system does not add a new CNID into the white/black list because the CNID has already been in the white/black list.
Action	No recommended action.

Notification

Message	Move ⟨*phone_number*⟩ CNID to ⟨*list_name*⟩ on interface s⟨*port_id*⟩/0 failed; ⟨*list_name*⟩ is full.
Meaning	The system does not move a CNID into the white/black list because the white/black list is full (the size of the white/black list is 20).
Action	No recommended action.

Notification

Message	Move ⟨*phone_number*⟩ CNID to ⟨*list_name*⟩ on interface s⟨*port_id*⟩/0 succeeded.
Meaning	The system added a new CNID into the white/black list of an interface.
Action	No recommended action.

Notification

Message	Remote peer from ⟨*phone_number*⟩ CNID on interface s⟨*port_id*⟩/0 hangs up the connection.
Meaning	The remote peer hangs up the connection.
Action	No recommended action.

Notification

Message	Remove ⟨*phone_number*⟩ CNID from ⟨*list_name*⟩ on interface s⟨*port_id*⟩/0.
Meaning	The system removes a CNID from the white/black list of an interface.
Action	No recommended action.

Notification

Message	⟨*phone_number*⟩ CNID on interface s⟨*port_id*⟩/0 logout.
Meaning	Device logout occurred due to idle timeout or the device admin exited.
Action	No recommended action.

Notification (00002)

Message	LCD control keys have been locked.
Meaning	An admin has locked the LCD control keys on a device.
Action	No recommended action.

Message	LCD display has been turned off and the LCD control keys have been locked.
Meaning	An admin has locked the LCD control keys and turned off the LCD display on a device.
Action	No recommended action.

Message	LCD display has been turned on and the LCD control keys have been unlocked.
Meaning	An admin has turned on the LCD display and unlocked the LCD control keys on a device.
Action	No recommended action.

Message	LCD display has been turned on.
Meaning	An admin has turned on the LCD display on a device.
Action	No recommended action.

Notification (00023)

Message	System configuration has been erased.
Meaning	An admin has turned on the LCD display on a device.
Action	No recommended action.

Notification (00545)

Message	Failed to initialize modem ⟨*modem_name*⟩, ⟨*modem_token_str*⟩
Meaning	A modem unsuccessfully attempted to establish a session through the device.
Action	No recommended action.

Message	Modem ⟨*modem_name*⟩ failed to dial ⟨*phone_number*⟩, ⟨*modem_token_str*⟩
Meaning	A modem unsuccessfully attempted to dial the specified number through the device.
Action	No recommended action.

Message	Modem ⟨*modem_name*⟩ has been disconnected.
Meaning	A RAS user successfully terminated a session via a modem.
Action	No recommended action.

Message	Modem ⟨*modem_name*⟩ is connected. Phone number: ⟨*phone_number*⟩, Account name: ⟨*login_name*⟩, Status ⟨*modem_connect_str*⟩
Meaning	A RAS user successfully established a session via a modem.
Action	No recommended action.

Message	⟨*arg_string*⟩
Meaning	Informational message.
Action	No recommended action.

Notification (00612)

Message	bgroup event: ⟨*event information*⟩.
Meaning	Bgroup configuration was changed.
Action	No recommended action.

Message	bgroup setting: bind port ⟨*port name*⟩ to interface ⟨*interface name*⟩.
Meaning	The < port > port was bound to the < interface > interface.
Action	No recommended action.

Message	bgroup setting: unbind port ⟨*port name*⟩ from interface ⟨*interface name*⟩.
Meaning	The < port > port was unbound from the < interface > interface.
Action	No recommended action.

Message	Switch event: change interface ⟨*interface name*⟩ from mii ⟨*old mii num*⟩ to mii ⟨*new mii num*⟩.
Meaning	The MII configuration was changed
Action	No recommended action.

Message	Switch event: the status of ethernet interface ⟨*interface name*⟩ change to link ⟨*current link status*⟩, duplex ⟨*current duplex*⟩, speed ⟨*current speed*⟩.
Meaning	The Ethernet interface status was changed
Action	No recommended action.

Message	Switch event: the status of ethernet port ⟨*port name*⟩ changed to link ⟨*current link status*⟩, duplex ⟨*current duplex*⟩, speed ⟨*current speed*⟩.
Meaning	The Ethernet port status was changed.
Action	No recommended action.

Message	Switch init: ⟨*init information*⟩.
Meaning	Log information is displayed about the switch module.
Action	No recommended action.

Message	switch install: install port ⟨*port number*⟩ to interface ⟨*interface name*⟩.
Meaning	A port was configured on the specified interface.
Action	No recommended action.

Message	Switch setting: ⟨*switch cli*⟩.
Meaning	The set switch CLI command was used.
Action	No recommended action.

Message	Switch setting: set interface ⟨*ethernet interface name*⟩ ⟨*etnernet interface setting*⟩.
Meaning	Ethernet port configuration was changed.
Action	No recommended action.

Message	Switch setting: set interface ⟨*interface name*⟩ ⟨*interface setting*⟩.
Meaning	Interface configuration was changed.
Action	No recommended action.

Notification (00767)

Message	⟨*upgrade_message*⟩
Meaning	Upgrade operation complete.
Action	No recommended action.

Chapter 14
DHCP

The following messages relate to Dynamic Host Configuration Protocol (DHCP). Some devices can act as a DHCP server or relay agent. Some devices can also act as a DHCP client. The following messages are divided into two sections: The first is for DHCP server and relay agent messages; the second is for DHCP client messages.

Alert (00029)

Message	IP pool of DHCP server on interface ⟨*string*⟩ is full. Unable to ⟨*string*⟩ IP address to client at %m.
Meaning	The DHCP server on the specified interface does not have any more IP addresses to assign to client hosts.
Action	Increase the DHCP server pool for the interface.

Critical (00029)

Message	DHCP server set to OFF on ⟨*string*⟩ (another server found on ⟨*IP address*⟩).
Meaning	An admin disabled the DHCP server on the specified interface. The device found an external DHCP server at the specified IP address.
Action	Enable the interface for DHCP locally, or for using the external DHCP server.

Warning (00527)

Message	IP pool of DHCP server on interface ⟨*string*⟩ is more than 90% allocated.
Meaning	The interface, acting as a DHCP server, has allocated over 90% of its designated address pool to client hosts.
Action	Enlarge the DHCP address pool designated for the interface.

Notification (00009)

Message	DHCP client is ⟨*string*⟩ on interface ⟨*string*⟩ ⟨*string*⟩.
Meaning	An admin enabled or disabled DHCP client on the specified interface.
Action	No recommended action.

Notification (00024)

Message	DHCP client admin preference is set on ⟨*string*⟩ as ⟨*integer*⟩.
Meaning	An admin has changed the admin preference for the specified interface to the specified number.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	DHCP client admin preference is unset on ⟨*string*⟩ from ⟨*integer*⟩.
Meaning	An admin has reset changed or removed one or more of the DHCP settings for the specified interface.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	DHCP relay agent settings on ⟨*string*⟩ are ⟨*string*⟩.
Meaning	The device has been configured to function as a DHCP relay agent. An admin has changed or removed one or more of the DHCP settings for the specified interface.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	DHCP server IP address pool is changed.
Meaning	The device, acting as a DHCP server, has offered, committed, or freed at least one IP address in its DHCP address pool.
Action	No recommended action.

Message	DHCP server is ⟨*string*⟩.
Meaning	An admin has either enabled or disabled the device to act as a DHCP server.
Action	No recommended action.

Message	DHCP server options are ⟨*string*⟩.
Meaning	An admin has changed or removed one or more of the DHCP options that were set. Examples include the IP addresses of the DNS servers, and the gateway IP address or the lease period.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	DHCP server shared IP is ⟨*string*⟩.
Meaning	An admin has enabled a reserved IP address to be assigned dynamically when it is not being used by the registered MAC address.
Action	No recommended action.

Notification (00027)

Message	DHCP client auto-config is ⟨*string*⟩.
Meaning	An admin enabled or disabled DHCP client auto-config.
Action	No recommended action.

Message	DHCP client lease time is set to ⟨*integer*⟩ minutes.
Meaning	An admin changed the DHCP client lease time to the specified number of minutes.
Action	No recommended action.

Message	DHCP client lease time is set to default value.
Meaning	An admin reset the DHCP client least time to the default value.
Action	No recommended action.

Message	DHCP client server IP address is reset.
Meaning	An admin reset the client server IP address to the default value.
Action	No recommended action.

Message	DHCP client server IP address is set to ⟨*IP address*⟩.
Meaning	An admin set the client server IP address to the specified value.
Action	No recommended action.

Message	DHCP client server-update is ⟨*string*⟩.
Meaning	An admin enabled or disabled DHCP server updating.
Action	No recommended action.

Message	DHCP client vendor identifier is reset.
Meaning	An admin reset the vendor ID to the default value.
Action	No recommended action.

Message	DHCP client vendor identifier is set to ⟨*string*⟩.
Meaning	An admin set the vendor ID to the specified value.
Action	No recommended action.

Information (00527)

Message	DHCP server has assigned or released an IP address.
Meaning	The device, acting as a DHCP server, assigned an IP address to a host, or released an existing IP address from a host.
Action	No recommended action.

Message	DHCP server on interface ⟨*string*⟩ received DHCPDISCOVER from %m requesting out-of-scope IP address ⟨*IP address*⟩/⟨*IP address*⟩.
Meaning	The device, acting as a DHCP server, received a DHCPDISCOVER request for an IP address outside of the address range specified for the server.
Action	No recommended action.

Message	DHCP server released an IP address.
Meaning	The device, acting as a DHCP server, has released an IP address.
Action	No recommended action.

Message	IP address ⟨*IP address*⟩ is assigned to %m.
Meaning	An admin assigned an IP address to an entity with the specified MAC address.
Action	No recommended action.

Message	IP address ⟨*IP address*⟩ is released from %m.
Meaning	An admin has manually released an IP address that the device had assigned to a DHCP client. (The client then automatically requests another IP address.)
Action	No recommended action.

Message	MAC address %m has declined address ⟨*IP address*⟩.
Meaning	The DHCP client has detected an IP address conflict and has declined the specified address. (After a DHCP client has been offered an IP address and before it accepts it, the client checks if there is any other host using the same address. If the client does not find a conflict, it accepts the address. If it does find a conflict, it rejects it.)
Action	No recommended action.

Message	One or more IP addresses are expired.
Meaning	The device, acting as a DHCP server, has expired at least one IP address.
Action	No recommended action.

Information (00530)

Message	An IP address conflict is detected and the DHCP client declined address ⟨*IP address*⟩.
Meaning	The DHCP client has detected an IP address conflict and has declined the specified address. (After a DHCP client has been offered an IP address and before it accepts it, the client checks if there is any other host using the same address. If the client does not find a conflict, it accepts the address. If it does find a conflict, it rejects it.)
Action	No recommended action.

Message	DHCP client IP address ⟨*IP address*⟩ for interface ⟨*string*⟩ has been manually released.
Meaning	An admin has manually released the specified IP address assigned to the named interface acting as a DHCP client.
Action	No recommended action.

Message	DHCP client is unable to get IP address for interface ⟨*string*⟩.
Meaning	The device, acting as a DHCP client, was unable to obtain an IP address or release an existing IP address from a host.
Action	No recommended action.

Message	DHCP client lease for ⟨*IP address*⟩ has expired.
Meaning	The specified DHCP client IP address is no longer valid. (The device automatically requests another IP address from the DHCP server.)
Action	No recommended action.

Message	DHCP client on interface ⟨*string*⟩ was offered IP ⟨*IP address*⟩/⟨*IP address*⟩ and did not proceed with DHCPREQUEST. Reason -- ⟨*string*⟩
Meaning	The device, acting as a DHCP client, did not continue with the DHCP request for the reason specified.
Action	No recommended action.

Message	DHCP server ⟨*IP address*⟩ assigned interface ⟨*string*⟩ with IP address ⟨*IP address*⟩ (lease time ⟨*integer*⟩ minutes).
Meaning	The specified DHCP server has assigned an IP address to the named interface for the specified length of time.
Action	No recommended action.

Information (00767)

Message	System auto-config of file ⟨*string*⟩ from TFTP server ⟨*IP address*⟩ has failed.
Meaning	The device failed to load the designated configuration file from the designated TFTP server.
Action	No recommended action.

Message	System auto-config of file ⟨*string*⟩ from TFTP server ⟨*IP address*⟩ is loaded successfully.
Meaning	The device successfully loaded the designated configuration file from the designated TFTP server.
Action	No recommended action.

Chapter 15

DHCP6

The following messages relate to IPv6 DHCP server options and resource allocations.

Notification (00024)

Message	DHCP server IP address pool has changed.
Meaning	The device, acting as a DHCP server, has offered, committed, or freed at least one IP address from its DHCP address pool.
Action	No recommended action.

Message	DHCP6 client is ⟨*string*⟩ on interface ⟨*string*⟩ ⟨*string*⟩.
Meaning	The device, acting as a DHCP server, has offered, committed, or freed at least one IP address in its DHCP address pool.
Action	No recommended action.

Message	DHCP6 server configured on ⟨*string*⟩ is ⟨*string*⟩.
Meaning	This message appears when either of the following conditions occur: —The DHCP6 server configured at the identified interface is enabled or disabled. —The DHCP6 server's DNS preference is updated for the identified interface. The DHCP6 server sends the preference value and the DNS server name to the DHCP6 client, so that the DHCP6 client can decide which DNS server to connect.
Action	No recommended action.

Message	DHCP6 server options at ⟨*string*⟩ are ⟨*string*⟩.
Meaning	An admin has changed or removed one or more of the DHCP options that were set. Examples include the IP addresses of the DNS servers, and the gateway IP address or the lease period.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Information (00527)

Message	DHCP6 client error, received ⟨*integer*⟩ bits prefix with ⟨*integer*⟩ bits in sla id.
Meaning	The DHCP6 client prefix length exceeds 64 bits. Because IPv6 includes 64 bits Interface ID, the sum of the other components in the prefix length (Public Topology) must be less than 64 bits. The prefix length from the DHCP6 server and the Site-Level Aggregation Identifier (SLA ID) is greater than 64 bits.
Action	Check the DHCP6 client's SLA length and the DHCP6 server prefix length. Use the following CLI to verify the sla-len + prefix > 64: -> set interface ethernet3 dhcp6 client pd iapd-id 3 ra-interface ethernet3 sla-id 2222 sla-len 16 -> set interface ethernet3 dhcp6 server options pd duid 00:03:01:00:11:22:33:44:55:66 iapd-id 20 prefix 1111::/64 1800 1800

Message	DHCP6: Client received ⟨*string*⟩ from ⟨*IP address*⟩, xid %x.
Meaning	DHCP6 client received DHCP6 packet from the server.
Action	No recommended action.

Message	DHCP6: Client send ⟨*string*⟩ from ⟨*string*⟩ ⟨*IP address*⟩ to ⟨*IP address*⟩, xid %x len ⟨*integer*⟩.
Meaning	DHCP6 client sent a DHCP6 packet to the DHCP6 server.
Action	No recommended action.

Message	DHCP6: Client start at ⟨*string*⟩.
Meaning	The interface enabled DHCP6 client.
Action	No recommended action.

Message	DHCP6: Server received ⟨*string*⟩ from ⟨*IP address*⟩, xid %x.
Meaning	DHCP6 server received DHCP6 packet from the client.
Action	No recommended action.

Message	DHCP6: Server send ⟨*string*⟩ from ⟨*string*⟩ ⟨*IP address*⟩ to ⟨*IP address*⟩, xid %x len ⟨*integer*⟩.
Meaning	DHCP6 server sent a DHCP6 packet to the DHCP6 client.
Action	No recommended action.

Message	DHCP6: Server send ⟨*string*⟩ from ⟨*string*⟩ ⟨*IP address*⟩ to ⟨*IP address*⟩, xid %x len ⟨*integer*⟩.
Meaning	DHCP6 server sent a DHCP6 packet to the DHCP6 client.
Action	No recommended action.

Chapter 16

DIP, VIP, MIP, and Zones

The following message relate to dynamic IP (DIP) addresses, virtual IP (VIP) addresses, mapped IP (MIP) addresses, and messages related to security and tunnel zones.

Critical (00023)

Message	VIP server ⟨*server_IP*⟩ cannot be contacted.
Meaning	The specified VIP server is not responding to the heartbeat PINGs sent by the security device.
Action	Check that the server is powered up, that it is connected to the network, and that its TCP/IP settings are correct.

Critical (00102)

Message	Utilization of DIP pool ⟨*dip_id*⟩ in vsys ⟨*vsys_name*⟩ hits raise threshold ⟨*threshold*⟩.
Meaning	The device utilized the specified DIP pool in over the specified raise threshold. The device triggers a SNMP trap when DIP utilization exceeds this configured threshold. (By default, DIP utilization alarm is not enabled.)
Action	No recommended action

Critical (00103)

Message	Utilization of DIP pool ⟨*dip_id*⟩ in vsys ⟨*vsys_name*⟩ hits clear threshold ⟨*threshold*⟩.
Meaning	The device utilized the specified DIP pool in over the specified clear threshold. The device triggers a SNMP trap when DIP utilization goes down across this configured threshold.
Action	No recommended action

Notification

Message	DIP IP range ⟨*DIP_min_range*⟩-⟨*DIP_max_range*⟩ was added into DIP pool ⟨*DIP_pool_id*⟩ ⟨*changed_from*⟩
Meaning	An admin added an IP range to the DIP pool.
Action	No recommended action

Notification

Message	DIP IP range ⟨*DIP_min_range*⟩-⟨*DIP_max_range*⟩ was removed from DIP pool ⟨*DIP_pool_id*⟩ ⟨*changed_from*⟩
Meaning	An admin removed an IP range from the DIP pool.
Action	No recommended action

Notification (00010)

Message	Mapped IP ⟨*is_ipv6*⟩-⟨*MIP_mapped_IP*⟩ ⟨*is_ipv6*⟩ ⟨*MIP_host_IP*⟩
Meaning	An admin has added, modified, or deleted the specified mapped IP address.
Action	No recommended action

Notification (00016)

Message	VIP (⟨*VIP_IP_Address*⟩:⟨*VIP_Port*⟩ ⟨*VIP_Service*⟩ ⟨*VIP_Host_Port*⟩) ⟨*action*⟩ ⟨*changed_from*⟩
Meaning	An admin has added, modified, or deleted the specified VIP.
Action	No recommended action

Message	VIP multi-port was disabled ⟨*changed_from*⟩
Meaning	An admin enabled multi-port mapping from a multi-port service to a VIP.
Action	No recommended action

Message	VIP multi-port was enabled ⟨*changed_from*⟩
Meaning	An admin enabled multi-port mapping from a multi-port service to a VIP.
Action	No recommended action

Notification (00021)

Message	DIP group ⟨*DIP_group_id*⟩ was created ⟨*changed_from*⟩
Meaning	An admin deleted a DIP group (< id_num >).
Action	No recommended action

Message	DIP group ⟨*DIP_group_id*⟩ was removed ⟨*changed_from*⟩
Meaning	An admin deleted a DIP group (< id_num >).
Action	No recommended action

Message	DIP IP pool ⟨*DIP_member_id*⟩ was removed from DIP group ⟨*DIP_group_id*⟩ ⟨*changed_from*⟩
Meaning	An admin has added, modified, or deleted the specified VIP.
Action	No recommended action

Message	DIP IP pool ⟨*is_ipv6*⟩-⟨*DIP_min_range*⟩ ⟨*is_ipv6*⟩ ⟨*DIP_max_range*⟩
Meaning	An admin has created, modified, or deleted the DIP pool consisting of the specified range of IP addresses.
Action	No recommended action

Message	DIP pool ⟨*DIP_member_id*⟩ was added into DIP group ⟨*DIP_group_id*⟩ ⟨*changed_from*⟩
Meaning	An admin added a DIP pool (< id_num1 >) to a DIP group (< id_num2 >).
Action	No recommended action

Message	DIP port-translation stickiness was ⟨*new_state*⟩ ⟨*changed_from*⟩
Meaning	An admin has enabled or disabled the DIP-sticky feature. Stickiness ensures that the security device assigns the same IP address from a DIP pool to a host for multiple concurrent sessions, instead of assigning a different source IP address for each session.
Action	No recommended action

Notification (00037)

Message	Asymmetric vpn was ⟨*enabled_disabled*⟩ on zone ⟨*zone_name*⟩.
Meaning	An administrator enabled or disabled the asymmetric VPN feature on the specified zone. When enabled, this option allows any incoming VPN traffic in a zone to match any applicable VPN session, regardless of the origin for the original VPN tunnel.
Action	No recommended action

Message	Intra-zone block for zone ⟨*zone_name*⟩ was set to ⟨*string_on_off*⟩
Meaning	An administrator turned the intra-zone block on or off for the specified zone.
Action	No recommended action

Message	IP/TCP reassembly for ALG was ⟨*enabled_disabled*⟩ on zone ⟨*zone_name*⟩.
Meaning	Layer-3 IP or Layer-4 TCP packet reassembly has been enabled or disabled for a zone.
Action	No recommended action

Message	New zone ⟨*zone_name*⟩ (ID ⟨*zone_id*⟩) was created.
Meaning	An administrator successfully created a new zone with the indicated ID number.
Action	No recommended action

Message	Tunnel zone ⟨*tzone_name*⟩ was bound to out zone ⟨*czone_name*⟩
Meaning	An administrator successfully bound a specified tunnel zone to a specified outbound zone.
Action	No recommended action

Message	Zone ⟨*zone_name*⟩ (ID ⟨*zone_id*⟩) was deleted.
Meaning	An administrator successfully deleted the specified zone.
Action	No recommended action

Message	Zone ⟨*zone_name*⟩ was bound to virtual router ⟨*vr_name*⟩
Meaning	An administrator successfully bound a specified zone to a specified virtual router.
Action	No recommended action

Message	Zone ⟨*zone_name*⟩ was changed to non-shared.
Meaning	An administrator changed a zone's attribute from shared to non-shared, or from non-shared to shared.
Action	No recommended action

Message	Zone ⟨*zone_name*⟩ was changed to shared.
Meaning	An administrator changed a zone's attribute from shared to non-shared, or from non-shared to shared.
Action	No recommended action

Message	Zone ⟨*zone_name*⟩ was unbound from virtual router ⟨*vr_name*⟩
Meaning	An administrator successfully unbound a specified zone, either trust or untrust, from a specified virtual router.
Action	No recommended action

Notification (00533)

Message	VIP server ⟨*server_IP*⟩ is now alive.
Meaning	The Virtual IP server has been brought up and is operational.
Action	No recommended action

Message	VIP server ⟨*server_IP*⟩ is now in manual mode.
Meaning	The admin disabled server auto-detection.
Action	No recommended action

Chapter 17

DNS

The following messages concern Domain Name System (DNS) settings and events.

Critical (00021)

Message	Connection refused by the DNS server.
Meaning	The DNS server is not responding to the DNS request.
Action	Consult the documentation for your DNS server.

Message	DNS server is not configured.
Meaning	The DNS server currently has no specified IP addresses.
Action	Consult the documentation for your DNS server to correct any IP address anomalies.

Message	Unknown DNS error.
Meaning	An unspecified error occurred on the DNS server.
Action	Consult the documentation for your DNS server to correct any current anomalies.

Notification

Message	Service type of DDNS entry with id ⟨*integer*⟩ is set to default value (dyndns).

Notification (00004)

Message	Daily DNS lookup has been disabled.
Meaning	An admin has disabled the automatic daily lookup of entries in the DNS cache table.
Action	To refresh the DNS table, an admin must manually invoke the DNS lookup operation.

Message	Daily DNS lookup time has been changed to start at ⟨*arg1*⟩:⟨*arg2*⟩ with an interval of ⟨*arg3*⟩ hours.
Meaning	An admin has changed the time when the security device performs the daily DNS lookup, resolving domain names with IP addresses in its DNS table.
Action	No recommended action

Message	DNS cache table has been cleared.
Meaning	An admin has cleared the DNS entries stored in the cache table.
Action	No recommended action

Message	DNS Proxy module has been disabled.
Meaning	The DNS Proxy module has either been activated (enabled) or de-activated (disabled).
Action	No recommended action

Message	DNS Proxy module has been enabled.
Meaning	The DNS Proxy module has either been activated (enabled) or de-activated (disabled).
Action	No recommended action

Message	DNS Proxy module has more concurrent client requests than allowed.
Meaning	There were more DNS server requests from clients than the DNS Proxy module can handle concurrently.
Action	No recommended action

Message	DNS Proxy server select table added with domain ⟨*string*⟩, interf ⟨*string*⟩, ip ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩ ⟨*string*⟩.
Meaning	An admin added an entry to the DNS Proxy server select table, where: < dom_name > the domain name of the server in the entry < interface > the interface of the server in the entry < ip_addr1 > the primary DNS server < ip_addr2 > the secondary DNS server < ip_addr3 > the tertiary DNS server
Action	No recommended action

Message	DNS Proxy server select table deleted with domain ⟨*string*⟩.
Meaning	An admin deleted an entry in the DNS Proxy server select table.
Action	No recommended action

Message	DNS Proxy server select table enties exceeded max limit.
Meaning	There are more retries in the DNS Proxy server select table than are allowed.
Action	No recommended action

Message	The { primary | secondary | ternary } DNS server IP address has been changed.
Meaning	An admin has changed the IP address of the primary, secondary, or ternary DNS server.
Action	No recommended action

Message	The { primary | secondary | ternary } DNS server IP address has been changed.
Meaning	An admin has changed the IP address of the primary, secondary, or ternary DNS server.
Action	No recommended action

Message	The { primary | secondary | ternary } DNS server IP address has been changed.
Meaning	An administrator has changed the IP address of the primary, secondary, or ternary DNS server.
Action	No recommended action.

Notification (00029)

Message	DNS has been refreshed.
Meaning	The security device has just performed a DNS lookup and refreshed its DNS table of domain name to IP address mappings. Each domain name has an IP address that identifies the same device that the domain name does. The device stores both the domain name and the IP addresses in the system cache and continually updates the cache by obtaining new domain name and address information coming into the device. This information is made available for checking by performing system refreshes.
Action	No recommended action

Notification (00059)

Message	Agent of DDNS entry with id ⟨*integer*⟩ is reset to its default value.
Meaning	An admin (or some other entity) reset the agent for the entry in the DDNS table.
Action	No recommended action

Message	DDNS entry with id ⟨*integer*⟩ is configured with interface ⟨*string*⟩ host-name ⟨*string*⟩.
Meaning	An admin (or some other entity) added a DDNS entry to the DDNS table, where: < id_num > the identification number for the entry < interface > the interface of the server in the entry < name_str > the host name of the interface
Action	No recommended action

Message	DDNS entry with id ⟨*integer*⟩ is configured with server type ⟨*string*⟩ name ⟨*string*⟩ refresh-interval ⟨*integer*⟩ hours mininum update interval ⟨*integer*⟩ minutes with ⟨*string*⟩ secure connection.
Meaning	An admin (or some other entity) added a DDNS entry to the DDNS table, where: < id_num > the identification number for the entry < string1 > the type of DDNS server (ddo or dyndns) < name_str > the name of the DDNS server < number1 > the refresh interval for the new entry (expressed in hours) < number2 > the minimum update interval for the new entry (expressed in minutes)
Action	No recommended action

Message	DDNS entry with id ⟨*integer*⟩ is configured with user name ⟨*string*⟩ agent ⟨*string*⟩.
Meaning	An admin (or some other entity) added a DDNS entry to the DDNS table.
Action	No recommended action

Message	DDNS entry with id ⟨*integer*⟩ is deleted.
Meaning	An admin (or some other entity) deleted a DDNS entry from the DDNS table.
Action	No recommended action

Message	DDNS module is disabled.
Meaning	The DDNS module has either been activated (enabled) or de-activated (disabled).
Action	No recommended action

Message	DDNS module is enabled.
Meaning	The DDNS module has either been activated (enabled) or de-activated (disabled).
Action	No recommended action

Message	DDNS module is initialized.
Meaning	A DDNS module session has been started (initialized) or terminated (shut down).
Action	No recommended action

Message	DDNS module is shut down.
Meaning	A DDNS module session has been started (initialized) or terminated (shut down).
Action	No recommended action

Message	DDNS server ⟨*string*⟩ returned incorrect ip ⟨*IP address*⟩, local-ip should be ⟨*IP address*⟩.
Meaning	The DDNS server sent the wrong IP address to the client.
Action	No recommended action

Message	Error response received for DDNS entry update for id ⟨*integer*⟩ user ⟨*string*⟩ domain ⟨*string*⟩, server type ⟨*string*⟩ name ⟨*string*⟩.
Meaning	< id_num > the identification number for the entry < name_str1 > the user name for the entry < dom_name > the domain name for the entry < name_str2 > the name of the DDNS server
Action	No recommended action

Message	Hostname of DDNS entry with id ⟨*integer*⟩ is cleared.
Meaning	An admin (or some other entity) cleared the hostname for the entry in the DDNS table.
Action	No recommended action

Message	Minimum update interval of DDNS entry with id ⟨*integer*⟩ is set to default value (60 min).
Meaning	An admin (or some other entity) reset the minimum-update interval for the entry in the DDNS table.
Action	No recommended action

Message	No-Change response received for DDNS entry update for id ⟨*integer*⟩ user ⟨*string*⟩ domain ⟨*string*⟩ server type ⟨*string*⟩, server name ⟨*string*⟩.
Meaning	An admin (or some other entity) successfully updated a DDNS entry to the DDNS table, where: < id_num > the identification number for the entry < name_str1 > the user name for the entry < dom_name > the domain name for the entry
Action	No recommended action

Message	Refresh interval of DDNS entry with id ⟨*integer*⟩ is set to default value (168 hours).
Meaning	An admin (or some other entity) reset the refresh interval for the entry in the DDNS table.
Action	No recommended action

Message	Source interface of DDNS entry with id ⟨*integer*⟩ is cleared.
Meaning	An admin (or some other entity) cleared the source interface specification for the entry in the DDNS table.
Action	No recommended action

Message	Success response received for DDNS entry update for id ⟨*integer*⟩ user ⟨*string*⟩ domain ⟨*string*⟩ server type ⟨*string*⟩ name ⟨*string*⟩.
Meaning	The DDNS server has been successfully updated.
Action	No recommended action.

Message	Updates for DDNS entry with id ⟨*integer*⟩ are set to be sent in secure (https) mode.
Meaning	An admin (or some other entity) specified use of HTTPS (secure HTTP) for the entry in the DDNS table.
Action	No recommended action

Message	Username and password of DDNS entry with id ⟨*integer*⟩ are cleared.
Meaning	An admin (or some other entity) cleared the username or password for the entry in the DDNS table.
Action	No recommended action

Notification (0059)

Message	Server of DDNS entry with id ⟨*integer*⟩ is cleared.
Meaning	An admin (or some other entity) reset the specified server for the entry in the DDNS table.
Action	No recommended action

Information (00004)

Message	DNS entries have been automatically refreshed.
Meaning	An admin has refreshed the entries in the DNS table, or the security device has refreshed the entries through a scheduled operation.
Action	No recommended action

Message	DNS entries have been manually refreshed.
Meaning	An admin has refreshed the entries in the DNS table, or the security device has refreshed the entries through a scheduled operation.
Action	No recommended action

Message	DNS entries have been refreshed as result of DNS server address change.
Meaning	The security device refreshed the entries in the DNS table because an admin changed the address of the DNS server.
Action	No recommended action

Message	DNS entries have been refreshed as result of external event.
Meaning	DNS entries were refreshed in the DNS cache table. This message may occur in response to an automatic update or other action by external sources, which may use configuration protocols like DHCP or PPPoE.
Action	No recommended action

Message	DNS entries have been refreshed by HA.
Meaning	HA has refreshed the entries in the DNS table.
Action	No recommended action

Message	DNS request ⟨*string*⟩ from ⟨*string*⟩/⟨*integer*⟩ is forwarded to server ⟨*string*⟩/⟨*integer*⟩
Meaning	A DNS request is forwarded to the back-end DNS server by DNS proxy.
Action	No recommended action.

Chapter 18
Entitlement and System

The following sections provide descriptions of and recommended action for ScreenOS messages displayed for subscription and entitlement-related events, as well as messages displayed for system-related events.

Emergency (00093)

Message	⟨*attach_detatch*⟩
Meaning	The USB storage device has been attached/detached successfully.
Action	No recommended action

Alert (00027)

Message	License key ⟨*Key name*⟩ expired after 30-day grace period.
Meaning	The thirty-day grace period for the specified license key expired, and the key is no longer valid.
Action	Renew the subscriptions key for your device.

Message	License key ⟨*Key name*⟩ has expired.
Meaning	The specified license key expired, and is no longer valid.
Action	Renew the subscriptions key for your device.

Message	License key ⟨*Key name*⟩ is due to expire in 2 months.
Meaning	The specified license key will expire in two months.
Action	Renew the subscriptions key for your device.

Message	License key ⟨*Key name*⟩ is due to expire in 2 weeks.
Meaning	The specified license key will expire in two weeks.
Action	Renew the subscriptions key for your device.

Message	License key ⟨*Key name*⟩ is due to expire in a month.
Meaning	The specified license key will expire in a month.
Action	Renew the subscriptions key for your device.

Message	Request to register the device failed to reach the server by ⟨*from*⟩. Server url: ⟨*url*⟩.
Meaning	A network administrator unsuccessfully attempted to register the device from the specified server.
Action	Make sure the device can connect to internet and that the url is correct.

Message	Request to retrieve license key failed to reach the server by ⟨*from*⟩. Server url: ⟨*url*⟩
Meaning	A network administrator unsuccessfully attempted to download a license key from the specified server.
Action	Make sure the device can connect to internet, and that the url is correct.

Critical

Message	Session limit alarm has been cleared for policy ⟨*policy_id*⟩ from src-ip ⟨*is_v6*⟩; current session count (⟨*src_ip*⟩) falls into the alarm threshold (⟨*current_sess*⟩).
Meaning	The session count from the specified source IP for the specified policy drops below the alarm threshold.
Action	No recommended action.

Critical

Message	Session limit alarm has been set for policy ⟨*policy_id*⟩ from src-ip ⟨*is_v6*⟩; current session count (⟨*src_ip*⟩) exceeds the alarm threshold (⟨*current_sess*⟩), but the packets will not be dropped.
Meaning	The session count from the specified source IP for the specified policy exceeds the alarm threshold. No traffic will be dropped.
Action	No recommended action.

Critical (00027)

Message	New config includes invalid settings. System rolled back to LKG config.
Meaning	The device encountered invalid settings while attempted to load a new configuration. Upon encountering the invalid settings the device abandoned the new configuration and rolled back to the last known good configuration.
Action	Use the get config command to check the current configuration. Inspect and repair the abandoned configuration before attempting to reload it.

Message	⟨*reset_log_str*⟩
Meaning	This message is a string that indicates the state the device is in during a device reset process. The message can display strings indicating the following states: request to initialize (removing) existing configuration, waiting for confirmation of initialization request, initialization request accepted and executed, initialization process aborted, and not enough power in the existing power supply load (only for NetScreen-5000 systems)
Action	If message indicates the initialization aborted, try resetting the device again. If the message indicates not enough power was available for a NetScreen-5000 system, check to make sure the power supply unit or units are working properly. If you feel you need to add an additional power supply, see your NetScreen 5000 Series User's Guide.

Critical (00051)

Message	Session utilization has dropped below ⟨*number*⟩, which is ⟨*percent*⟩ of the system capacity!
Meaning	The device has dropped below the identified number of concurrent sessions, which is the specified percentage of system capacity.
Action	No recommended action.

Message	Session utilization has reached ⟨*number*⟩, which is ⟨*percent*⟩ of the system capacity!
Meaning	The device has reached the identified number of concurrent sessions, which is the specified percentage of system capacity.
Action	Clear inactive sessions.

Critical (00080)

Message	Cannot create a DI pool with a size of ⟨*integer*⟩ bytes.
Meaning	The device cannot create a Deep Inspection memory pool with the specified number of bytes, because the device is overloaded and out of memory.
Action	Reduce the configuration size or remove some features on the device and then try to create the Deep Inspection memory pool again.

Critical (00081)

Message	Cannot allocate ⟨*integer*⟩ bytes of memory.
Meaning	The message indicates memory allocation failure.
Action	Monitor the device and re-adjust the memory allocation. If error persists, then it is a system capacity issue. Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Critical (00850)

Message	Session limit alarm has been cleared for vsys ⟨*vsys_name*⟩ (current ⟨*current_sess*⟩, dropped packets ⟨*drop_sess*⟩)
Meaning	An admin has cleared the session limit alarm for the specified vsys.
Action	No recommended action.

Message	Session limit alarm has been set for vsys ⟨*vsys_name*⟩ (current ⟨*current_sess*⟩, alarm threshold ⟨*alarm_sess*⟩).
Meaning	An admin has changed the session limit alarm for the specified vsys to the specified value.
Action	No recommended action.

Error (00767)

Message	can only do set alg _all as unset alg _all command has issued.
Meaning	An admin attempted to set an individual application layer gateway after the command unset alg _all was issued.
Action	Issue the set alg _all command before attempting to set an individual application layer gateway.

Notification

Message	CPU-protection throttling mode engaged ⟨*cpu_prot_throttling_times*⟩ times in ⟨*cpu_prot_throttling_interval*⟩ seconds.
Meaning	The CPU-protection throttling throttling mode engaged frenquently.
Action	Please check whether the box is under attack and use blacklists to screen attacking packets.

Notification

Message	Set cpu-protection blacklist: ⟨*cpu_prot_blacklist_str*⟩.
Meaning	Add a new blacklist on the device.
Action	No recommanded action.

Notification

Message	Set cpu-protection threshold ⟨*cpu_prot_threshold*⟩.
Meaning	Set the cpu protection threshold.
Action	No recommanded action.

Notification

Message	Unset cpu-protection blacklist ⟨*cpu_prot_blacklist_id*⟩.
Meaning	Delete a blacklist on the device.
Action	No recommanded action.

Notification (00002)

Message	Session threshold has been changed to percentage ⟨*percent*⟩
Meaning	An admin has changed the session threshold to the specified percentage of system capacity.
Action	No recommended action.

Notification (00006)

Message	Domain set to ⟨*name*⟩.
Meaning	A network administrator set the name of the domain under which the device resides to the specified name.
Action	No recommended action.

Message	Hostname set to ⟨*name*⟩.
Meaning	A network administrator changed the existing hostname for the device.
Action	No recommended action.

Notification (00008)

Message	Configure pattern-update:⟨*string*⟩.
Meaning	Configure pattern update via proxy.
Action	No recommended action.

Message	System clock configurations have been changed ⟨*string*⟩
Meaning	An admin has changed the configuration for the system clock.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	System clock was changed manually from ⟨*previous_value*⟩.
Meaning	An admin changed the clock of the device by synchronizing it with the client or through the CLI.
Action	No recommended action.

Message	System up time shifted by ⟨*integer*⟩ seconds.
Meaning	The device changed the system up time by the specified number of seconds.
Action	No recommended action.

Notification (00036)

Message	An optional ScreenOS feature has been activated via a software key.
Meaning	A network administrator successfully enabled an optional feature.
Action	No recommended action.

Message	No license key is available for retrieval by ⟨*from*⟩.
Meaning	A network administrator unsuccessfully attempted to download a license key from the specified server.
Action	Try to retrieve the key (or keys) again later, or contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Received identical license key by ⟨*from*⟩.
Meaning	A host attempted to download a license key that already exists on the device.
Action	No recommended action

Message	Register device succeeded and warranty key is installed.
Meaning	A network administrator successfully registered the device and installed a warranty key.
Action	No recommended action

Message	Retrieve firmware list failed.
Meaning	The WebUI failed to retrieve the list of available firmware.
Action	Try to retrieve the firmware list later, or contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Retrieve firmware list succeeded: ⟨*number*⟩ firmware.
Meaning	The WebUI successfully retrieved the list of available firmware.
Action	No recommended action

Message	Retrieve firmware list succeeded: ⟨*number*⟩ firmware.
Meaning	The WebUI successfully retrieved the list of available firmware.
Action	No recommended action

Message	⟨*number*⟩ license keys were updated successfully by ⟨*from*⟩.
Meaning	A network administrator successfully retrieved a specified license key for this device.
Action	No recommended action

Notification (00526)

Message	The user limit has been exceeded and ⟨*ipv6*⟩ cannot be added.
Meaning	The device has reached the user limit and cannot add a new session.
Action	Decrease the number of users or upgrade the device by obtaining a software key for an unrestricted number of users.

Notification (00575)

Message	⟨*file_transfer*⟩
Meaning	The specified file has been transferred to or from the USB storage device.
Action	No recommended action

Notification (00767)

Message	Administrator ⟨*string*⟩ issued command ⟨*string*⟩ to redirect output.
Meaning	The network administrator typed a command in a console session that redirects output to another destination other than the device.
Action	No recommended action.

Message	Invalid configuration size (⟨*config_size_limit*⟩).
Meaning	An admin entered an invalid value for the configuration size limit.
Action	Enter a valid size limit value.

Message	Session (id ⟨*sess_id*⟩, ⟨*sess_src_dst_proto*⟩) cleared: ⟨*sess_clr_cmd_issuer*⟩
Meaning	The specified session was cleared.
Action	No recommended action.

Message	System is operational.
Meaning	The system has become initialized and is now operational.
Action	No recommended action.

Message	System was reset at ⟨*string*⟩
Meaning	An administrator reset the device at the specified date and time.
Action	No recommended action.

Message	Trial keys are available to download to enable advanced features. To find out, please visit http://www.juniper.net/products/subscription/trial/.
Meaning	Trial keys are now available.
Action	Visit the URL < url_str > specified in the message.

Message	Unsupported command ⟨*string*⟩
Meaning	The network administrator typed a command in a console session with the device that ScreenOS does not support.
Action	Identify the command that caused the problem and replace it with a command that ScreenOS supports.

Information (00767)

Message	All system configurations saved to ⟨*config_changer*⟩ by ⟨*admin*⟩.
Meaning	Every time a network administrator issues a command to ScreenOS through the Command Line Interface, the system saves it in Flash memory. This message indicates a network administrator set new parameters for multiple configurations on the device.
Action	No recommended action.

Message	Daylight Saving Time ended.
Meaning	Daylight saving time has started or ended. The device automatically reverts to the standard time if the option was previously set.
Action	No recommended action.

Message	Daylight Saving Time has started.
Meaning	Daylight saving time has started or ended. The device automatically reverts to the standard time if the option was previously set.
Action	No recommended action.

Message	Environment variable ⟨*name*⟩ changed to ⟨*data*⟩.
Meaning	This message indicates an administrator issued a command in the ScreenOS CLI that changed the setting of an environment variable.
Action	No recommended action.

Message	Environment variable ⟨*name*⟩ set to ⟨*data*⟩.
Meaning	A network administrator changed an environment variable to a new name.
Action	No recommended action.

Message	Environment variable ⟨*name*⟩ unset.
Meaning	A network administrator unset an environment variable.
Action	No recommended action.

Message	Load file from usb ⟨*usb_filename*⟩ to flash ⟨*flash_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The administrator < string > loaded the file < filename > from the USB storage device to the flash memory.
Action	No recommended action.

Message	Lock configuration aborted because ⟨*integer*⟩ minute(s) timeout was exceeded.
Meaning	The lockout was aborted because the device did not receive a CLI command within the specified timeout value
Action	No recommended action.

Message	Lock configuration aborted explicitly by task ⟨*string*⟩.
Meaning	The lockout was aborted either by an admin via the CLI or by NSM.
Action	No recommended action.

Message	Lock configuration ended by task ⟨*string*⟩.
Meaning	The configuration file is no longer locked.
Action	No recommended action.

Message	Lock configuration started by task ⟨*string*⟩, with a timeout value of ⟨*integer*⟩ minute(s).
Meaning	The configuration file was locked either by an admin via the CLI or by the NetScreen-Security Manager (NSM) application. If the device does not receive a CLI command within the specified timeout value, it restarts using the configuration file that was previously locked.
Action	No recommended action.

Message	New GMT zone ahead or behind by ⟨*integer*⟩ seconds.
Meaning	An admin set the time zone by specifying the number of seconds by which the local time is ahead or behind the Greenwich Mean Time (GMT).
Action	No recommended action.

Message	Save configuration to IP address ⟨*ip*⟩ under filename ⟨*filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The network administrator saved the device configuration to the specified IP address and filename.
Action	No recommended action.

Message	Save new software from ⟨*ip*⟩ under filename ⟨*filename*⟩ to flash memory ⟨*admin*⟩.
Meaning	The named network administrator saved the software to the specified file and IP address.
Action	No recommended action.

Message	Save new software from slot filename ⟨*slot_filename*⟩ to flash memory ⟨*admin*⟩.
Meaning	The specified admin copied a ScreenOS image from a file (< filename >) on a memory card to flash memory.
Action	No recommended action.

Message	Save new software from usb filename ⟨*usb_filename*⟩ to flash memory by administrator ⟨*admin*⟩.
Meaning	The administrator < string > saved the system image < filename > from the USB storage device to flash memory.
Action	No recommended action.

Message	Script Get-command has started.
Meaning	The system has started executing get-command.
Action	No recommended action

Message	Script Get-command has stopped.
Meaning	The system has stopped executing get-command.
Action	No recommended action

Message	Send file ⟨*flash_filename*⟩ from flash to usb ⟨*usb_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The administrator < string > saved the file < filename > from the flash memory to the USB storage device.
Action	No recommended action.

Message	Send new software from flash memory to slot filename ⟨*slot_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The specified admin copied a ScreenOS image from flash memory to a file (< filename >) on a memory card
Action	No recommended action.

Message	Send new software from flash memory to usb filename ⟨*usb_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The administrator < admin > saved the system image < filename > from the flash memory to the USB storage device.
Action	No recommended action.

Message	Send new software from IP address ⟨*ip*⟩ under filename ⟨*filename*⟩ to slot ⟨*slot_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The named administrator saved the software from the specified filename and IP address to the specified file on the memory card.
Action	No recommended action.

Message	Send new software from IP address ⟨*ip*⟩ under filename ⟨*filename*⟩ to usb ⟨*admin*⟩ by administrator ⟨*string*⟩.
Meaning	The administrator < admin > saved the system configuration file < filename > from the TFTP server to the USB storage device.
Action	No recommended action.

Message	Send new software to IP address ⟨*ip*⟩ under filename ⟨*filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The named network administrator saved the software to the specified file and IP address.
Action	No recommended action.

Message	System configuration saved ⟨*config_changer*⟩ by ⟨*admin*⟩.
Meaning	A network administrator saved the system configuration file.
Action	No recommended action.

Message	The system configuration was loaded from flash memory to ⟨*usb_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The administrator < string > saved the system configuration file < filename > from flash memory to the USB storage device.
Action	No recommended action.

Message	The system configuration was loaded from flash memory to slot ⟨*slot_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The named network administrator loaded a configuration file from flash memory to a file (< filename >) on a memory card.
Action	No recommended action.

Message	The system configuration was loaded from ⟨*ip*⟩ under the filename ⟨*filename*⟩ to slot ⟨*slot_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The admin copied the system configuration from the specified file and IP address to the file on the memory card.
Action	No recommended action.

Message	The system configuration was loaded from ⟨*ip*⟩ under the filename ⟨*filename*⟩ to usb ⟨*admin*⟩ by administrator ⟨*string*⟩.
Meaning	The administrator < admin > loaded the system configuration file < filename > from the TFTP server to the USB storage device.
Action	No recommended action.

Message	The system configuration was loaded from IP address ⟨*ip*⟩ under filename ⟨*filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The network administrator loaded the configuration file from the specified IP address and filename.
Action	No recommended action.

Message	The system configuration was loaded from slot ⟨*admin*⟩.
Meaning	A network administrator loaded the system configuration from the specified file in the memory card.
Action	No recommended action.

Message	The system configuration was loaded from usb ⟨*usb_filename*⟩ by administrator ⟨*admin*⟩.
Meaning	The administrator < string > loaded the system configuration file < filename > from the USB storage device.
Action	No recommended action.

Message	The system configuration was not saved ⟨*string*⟩ by administrator ⟨*string*⟩. It was locked by administrator ⟨*string*⟩.
Meaning	The first admin could not save to the configuration file because the second admin locked the configuration file in flash memory.
Action	No recommended action.

Message	Timer ⟨*string*⟩ ⟨*string*⟩
Meaning	An admin reset the timer from a peer unit in a NSRP cluster.
Action	No recommended action.

Chapter 19
FIPs

This message relates to the FIPS mode on the security devices.

Notification (00030)

Message	FIPS error ⟨*string*⟩ error code ⟨*integer*⟩.
Meaning	General FIPS failure message.
Action	Record the error message and number and then contact Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered customer.)

Chapter 20

Flow

The following messages relate to data flow processes.

Alert (00800)

Message	Shared to fair transition forced.
Meaning	A CLI command forced a transition into fair mode.
Action	Verify that this transition is desired.

Alert (00801)

Message	Shared to fair transition: utilization ⟨*utilization*⟩ > = threshold ⟨*threshold*⟩.
Meaning	The firewall automatically transitioned from shared mode to fair mode because the current utilization was greater than or equal to the user-specified threshold.
Action	Identify the cause of the transition to fair mode.

Critical (00802)

Message	Fair to shared transition forced.
Meaning	A CLI command forced a transition into shared mode.
Action	Verify that this transition is desired.

Critical (00803)

Message	Fair to shared transition: time limit exceeded.
Meaning	The firewall automatically transitioned from fair mode to shared mode because the user-specified time to be spent in fair mode was exceeded
Action	Identify the cause of the transition to fair mode, and monitor the firewall in the event that it transitions back to fair mode.

Critical (00804)

Message	Fair to shared transition: utilization ⟨*utilization*⟩ < threshold ⟨*threshold*⟩.
Meaning	The firewall automatically transitioned from fair mode to shared mode because the current utilization was less than the user-specified threshold.
Action	Identify the cause of the transition to fair mode, and monitor the firewall in the event that it transitions back to fair mode.

Notification (00002)

Message	(⟨*admin*⟩/⟨*vsys*⟩) assign vlan group ⟨*vlan group name*⟩ to vsd id ⟨*vsd*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Message	(⟨*string*⟩/⟨*string*⟩) ⟨*string*⟩ vlan group name ⟨*string*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Message	(⟨*string*⟩/⟨*string*⟩) ⟨*string*⟩ vlan group ⟨*string*⟩ ⟨*integer*⟩ ⟨*integer*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Message	(⟨*string*⟩/⟨*string*⟩) ⟨*string*⟩ vlan import ⟨*integer*⟩ ⟨*integer*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Message	(⟨*string*⟩/⟨*string*⟩) set vlan port ⟨*string*⟩ group ⟨*string*⟩ zone ⟨*string*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Message	(⟨*admin*⟩/⟨*vsys*⟩) unassign vlan group ⟨*vlan group name*⟩ from vsd id ⟨*vsd*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Message	(⟨*string*⟩/⟨*string*⟩) unset vlan port ⟨*string*⟩ group ⟨*string*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Message	Transparent virutal wire mode has been ⟨*state*⟩.
Meaning	An admin enabled or disabled transparent virtual wire mode. In this mode, two devices in a NSRP cluster can perform active/active redundancy as Layer-2 switches.
Action	No recommended action.

Notification (00040)

Message	Aggressive age-out value has been changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	The aggressive age-out value has been changed. This value shortens default session timeouts by the amount you specify. The aggressive age-out value can be between 2 and 10 units, where each unit represents a 10-second interval (that is, the aggressive age-out setting can be between 20 and 100 seconds). The default value is 2.
Action	If you need to adjust the aggressive timeout option, use the CLI command set flow aging early-ageout.

Message	High watermark for early aging has been changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	The high watermark was changed to a different value. A watermark is a value that determines when aggressive aging out of processes starts. The high-watermark value sets the point at which the process begins. This value can be from 1 to 100 and indicates a percent of the session table capacity in 1% units. The default is 100, or 100%.
Action	If aggressive aging starts too quickly or too slowly, reset the high-watermark value using the CLI command set flow aging high-watermark.

Message	High watermark for early aging has been changed to the default (⟨*integer*⟩).
Meaning	The low-watermark value has been changed to the default. A watermark is a value that determines when aggressive aging out of processes starts. The high-watermark value determines when the aging out begins. This value can be from 1 to 100 and indicates a percent of the session table capacity in 1 % units. The default is 100, or 100 %. The low-watermark value when the aging out ends. This value can be from 1 to 10, and indicates a percent of the session table capacity in 10 % units. The default is 10, or 100 %.
Action	If aging out starts or ends too quickly or too slowly, reset high- or low-watermark values using the CLI command set flow aging early-ageout.

Message	Low watermark for early aging has been changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	The low watermark was changed to a different value. A watermark is a value that determines when aggressive aging out of processes starts. The low-watermark value sets the point at which the process ends. This value can be from 1 to 10 and indicates a percent of the session table capacity in 10 % units. The default is 10, or 100 %.
Action	If aggressive aging ends too quickly or too slowly, reset the high-watermark value using the CLI command set flow aging high-watermark.

Message	Low watermark for early aging has been changed to the default (⟨*integer*⟩).
Meaning	The low-watermark value has been changed to the default (100). The low-watermark value sets the point at which the aging-out of processes ends. This value can be from 1 to 100 and indicates a percent of the session table capacity. The default is 100.
Action	If aging out ends too quickly or too slowly, reset low-watermark value using the CLI command set flow aging { high-watermark | low-watermark }.

Message	The aggressive age-out value has been changed to the default (⟨*integer*⟩).
Meaning	The aggressive age-out value was changed to the default value (2). The aggressive age-out option shortens default session timeouts by the amount you specify. The aggressive age-out value can be between 2 and 10 units, where each unit represents a 10-second interval (that is, the aggressive age-out setting can be between 20 and 100 seconds).
Action	If you need to adjust the aggressive timeout option, use the CLI command set flow aging early-ageout.

Notification (00079)

Message	CPU limit ⟨*state*⟩.
Meaning	The CPU utilization limit is as stated.
Action	Verify that this configuration is desired.

Message	Desired fair mode changed from ⟨*old*⟩ to ⟨*new*⟩.
Meaning	A new method of exiting fair mode has been chosen.
Action	Verify that this configuration is desired.

Message	Fair to shared hold-down time changed from ⟨*old*⟩ to ⟨*new*⟩.
Meaning	The Fair to shared hold-down time has been changed to a new value. The hold-down time is the minimum amount of time that the flow CPU utilization percentage must exceed the flow CPU utilization percentage threshold.
Action	Verify that this configuration is desired.

Message	Fair to shared threshold changed from ⟨*old*⟩ to ⟨*new*⟩.
Meaning	The fair to share threshold has been changed to a new value.
Action	Verify that this configuration is desired.

Message	Fair to shared time changed from ⟨*old*⟩ to ⟨*new*⟩.
Meaning	The fair to share transition time has been changed to a new value.
Action	Verify that this configuration is desired.

Message	Shared to fair hold-down time changed from ⟨*old*⟩ to ⟨*new*⟩.
Meaning	The shared to fair hold-down time has been changed to a new value. The hold-down time is the time for which the actual utilization must be less than the configured threshold before transitioning back from fair mode to shared mode.
Action	Verify that this configuration is desired.

Message	Shared to fair threshold changed from ⟨*old*⟩ to ⟨*new*⟩.
Meaning	The shared to fair threshold has been changed to a new value.
Action	Verify that this configuration is desired.

Notification (00085)

Message	Flow ⟨*clear-text or tunnel*⟩ reverse-route changed from ⟨*old*⟩ to ⟨*new*⟩.
Meaning	VLAN log information.
Action	No recommended action.

Notification (00573)

Message	Running in Infranet Test mode: Allow packet on Infranet authentication policy. Infranet Controller timeout occurred, time-out action was 'open'. Source IP ⟨*src_ip*⟩, Destination IP ⟨*dst_ip*⟩, Policy ID ⟨*policy_id*⟩.
Meaning	This is a Test mode message indicating an Infranet Controller timeout has occurred. In regular mode, this would indicate an open policy, because the timeout action is confirmed as "open."
Action	No recommended action.

Message	Running in Infranet Test mode: Allow packet. In Regular mode, would drop packet on Infranet authentication policy because Infranet auth table denied it. Source IP ⟨*src_ip*⟩, Destination IP ⟨*dst_ip*⟩, Policy ID ⟨*policy_id*⟩.
Meaning	This is a Test mode message. In regular mode, the packet would have been dropped by the Infranet authentication policy because the auth table match denies it. The packet is let through in test mode.
Action	No recommended action.

Message	Running in Infranet Test mode: Allow packet. In Regular mode, would drop packet on Infranet authentication policy because Infranet Controller timeout occurred and time-out action was 'close'. Source IP ⟨*src_ip*⟩, Destination IP ⟨*dst_ip*⟩, Policy ID ⟨*policy_id*⟩.
Meaning	This is a Test mode message indicating that an Infranet Controller timeout has occurred. In regular mode all matching packets would be denied, because the timeout action is configured as "close." The packet is let through in Test mode.
Action	No recommended action.

Message	Running in Infranet Test mode: Allow packet. In Regular mode, would drop packet on Infranet authentication policy because there is no Infranet auth table entry. Source IP ⟨*src_ip*⟩, Destination IP ⟨*dst_ip*⟩, Policy ID ⟨*policy_id*⟩.
Meaning	This is a Test mode message. In regular mode, the packet would have been dropped by the Infranet auth policy because the auth table has no match. The packet is let through in Test mode.
Action	No recommended action.

Message	Running in Infranet Test mode: Infranet authentication succeeded, let the packet through. Source IP ⟨*src_ip*⟩, Destination IP ⟨*dst_ip*⟩, Policy ID ⟨*policy_id*⟩.
Meaning	This is a Test mode message. In regular mode, Infranet authentication is successful and the packet is let through.
Action	No recommended action.

Notification (00601)

Message	IP action detected attack attempt ⟨*state*⟩.
Meaning	IP attacks have been detected for which you have configured IP blocking.
Action	No recommended action.

Chapter 21

Frame Relay

These messages relate to the Frame Relay and Multi-link Frame Relay encapsulation protocols.

Alert (00085)

Message	[mlfr/lip]: ⟨*interfacename*⟩ detected loop ⟨*times*⟩ times.
Meaning	A link loopback was detected for the indicated number of times.
Action	No recommended action.

Message	[mlfr/lip]: the bid ⟨*lrxbid*⟩ in the ADD_LINK packet from link ⟨*linkname*⟩ is inconsistent with the received bid ⟨*brxbid*⟩ on the bundle ⟨*bundlename*⟩.
Meaning	An invalid bundle ID was detected in the received ADD_LINK packet.
Action	Check the bundle ID configuration at the local and remote endpoints.

Notification (00074)

Message	[fr/cfg]: ⟨*interface*⟩ LMI: set ⟨*param_name*⟩ to ⟨*value*⟩.
Meaning	An admin configured the indicated LMI parameter.
Action	No recommended action.

Message	[fr/cfg]: ⟨*interface*⟩ LMI: set to ⟨*proc*⟩.
Meaning	An admin enabled or disabled LMI on the interface.
Action	No recommended action.

Message	[fr/cfg]: ⟨*interface*⟩: ⟨*config*⟩
Meaning	The specified interface is configured for DTE or DCE operation.
Action	No recommended action.

Message	[fr/cfg]: ⟨*interface*⟩: ⟨*config*⟩
Meaning	An admin configured the DLCI for the interface.
Action	No recommended action.

Notification (00075)

Message	[mlfr/cfg]: add link ⟨*linkname*⟩ to bundle ⟨*bundlename*⟩.
Meaning	An admin added the specified interface to the multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: delete link ⟨*linkname*⟩ from bundle ⟨*bundlename*⟩.
Meaning	An admin removed the specified interface from the multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: set interface ⟨*interfacename*⟩ encap as mlfr-uni-nni.
Meaning	An admin configured the specified interface for Multilink Frame Relay encapsulation.
Action	No recommended action.

Message	[mlfr/cfg]: set lip acknowledge-retries as ⟨*ackretries*⟩ for bundle link ⟨*interfacename*⟩.
Meaning	An admin configured the number of retransmission attempts after the acknowledge timer expires for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: set lip acknowledge-timer as ⟨*acktimer*⟩(s) for bundle link ⟨*interfacename*⟩.
Meaning	An admin configured the maximum period to wait for an acknowledgement for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: set lip fragment-threshold as ⟨*frag*⟩ for bundle link ⟨*interfacename*⟩.
Meaning	An admin configured the maximum size for packet payloads for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: set lip hello-timer as ⟨*hello-timer*⟩(s) for bundle link ⟨*interfacename*⟩.
Meaning	An admin configured the rate at which hello messages are sent for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: set MLFR bundle-id as ⟨*bundle-id*⟩ for multilink interface ⟨*interfacename*⟩.
Meaning	An admin configured a bundle link identifier for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: set MLFR drop-timeout as ⟨*droptime*⟩ for multilink interface ⟨*interfacename*⟩.
Meaning	An admin configured the drop timeout for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: set MLFR minimum-links as ⟨*links*⟩ for multilink interface ⟨*interfacename*⟩.
Meaning	An admin configured the minimum number of links for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: unset bundle link ⟨*interfacename*⟩ lip fragment-threshold to ⟨*mtu*⟩.
Meaning	An admin reset the maximum size for packet payloads for the specified multilink interface to the default (MTU size of the physical link).
Action	No recommended action.

Message	[mlfr/cfg]: unset interface ⟨*interfacename*⟩ encap from mlfr-uni-nni.
Meaning	An admin removed Multilink Frame Relay encapsulation from the specified interface.
Action	No recommended action

Message	[mlfr/cfg]: unset lip acknowledge-retries to default ⟨*ackretries*⟩ for bundle link ⟨*interfacename*⟩.
Meaning	An admin reset the number of retransmission attempts after the acknowledge timer expires for the specified multilink interface to the default (2 times).
Action	No recommended action.

Message	[mlfr/cfg]: unset lip acknowledge-timer to default ⟨*acktimer*⟩(s) for bundle link ⟨*interfacename*⟩.
Meaning	An admin reset the maximum period to wait for an acknowledgement for the specified multilink interface to the default (4 milliseconds).
Action	No recommended action.

Message	[mlfr/cfg]: unset lip hello-timer to default ⟨*hello-timer*⟩(s) for bundle link ⟨*interfacename*⟩.
Meaning	An admin reset the rate at which hello messages are sent on the specified multilink interface to the default (10 milliseconds).
Action	No recommended action.

Message	[mlfr/cfg]: unset MLFR bundle-id as the name of multilink interface ⟨*interfacename*⟩.
Meaning	An admin removed the bundle link identifier from the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: unset MLFR drop-timeout to 0 (disable) for multilink interface ⟨*interfacename*⟩.
Meaning	An admin disabled drop timeout for the specified multilink interface.
Action	No recommended action.

Message	[mlfr/cfg]: unset MLFR minimum-links to default (1) for multilink interface ⟨*interfacename*⟩.
Meaning	An admin reset the minimum number of links for the specified multilink interface to the default (1).
Action	No recommended action.

Notification (00086)

Message	[fr/lmi]: ⟨*interface*⟩: LMI link is down due to errors over threshhold (n392).
Meaning	Local Management Interface is down on the specified interface because the number of errors encountered reached the configured DTE error threshold (default is 3).
Action	No recommended action.

Notification (00569)

Message	[fr/lmi]: ⟨*interface*⟩ dlci(⟨*dlci*⟩) status changed to ⟨*state*⟩.
Meaning	The specified DLCI status has changed, as indicated.
Action	No recommended action.

Message	[fr/lmi]: ⟨*interface*⟩ LMI status changed to ⟨*state*⟩.
Meaning	The LMI status has changed to down or up.
Action	No recommended action.

Notification (00570)

Message	[mlfr/lip]: change bundle ⟨*bundlename*⟩ physical status to down.
Meaning	The specified bundle is down.
Action	No recommended action.

Message	[mlfr/lip]: changed bundle ⟨*bundlename*⟩ physical status to up.
Meaning	The specified bundle is up.
Action	No recommended action.

Message	[mlfr/lip]: link interface ⟨*linkname*⟩ LIP is down at bundle ⟨*bundlename*⟩.
Meaning	Link Interface Protocol is down on the specified link interface in the bundle.
Action	No recommended action

Message	[mlfr/lip]: link interface ⟨*linkname*⟩ LIP is up at bundle ⟨*bundlename*⟩.
Meaning	Link Interface Protocol is up on the specified link interface in the bundle.
Action	No recommended action.

Message	[mlfr/lip]: ⟨*linkname*⟩ LIP FSM: (⟨*oldstate*⟩ -> ⟨*newstate*⟩) by event (⟨*event*⟩).
Meaning	The indicated event has changed the Link Integrity Protocol state (the previous and new states are shown).
Action	No recommended action.

Chapter 22
GTP

The following section provides descriptions of and recommended action for ScreenOS messages displayed for GTP-related events.

Notification (00065)

Message	GTP ⟨*string*⟩ ⟨*string*⟩; ⟨*string*⟩
Meaning	An admin configured the security device to pass or drop version 0 or version 1 of the specified GTP message.
Action	No recommended action.

Message	GTP ⟨*string*⟩; ⟨*string*⟩
Meaning	The specified administrator has unset the minimum or maximum message length in the security device configuration.
Action	No recommended action.

Message	GTP sets ⟨*string*⟩ ⟨*integer*⟩; ⟨*string*⟩
Meaning	An admin configured the security device to only pass GTP messages of the specified maximum or minimum length (in bytes).
Action	No recommended action.

Notification (00567)

Message	GTP ⟨*string*⟩
Meaning	This message indicates that a GTP tunnel was deleted and provides information on the GTP tunnel. The duration is the number of seconds that the GTP tunnel was up.
Action	No recommended action.

Message	GTP ⟨*string*⟩; ⟨*string*⟩
Meaning	When upgrading from ScreenOS 4.0 to ScreenOS 5.0, a GTP object was created based on the former global configuration. The GTP object name is trust_untrust.
Action	No recommended action.

Message	⟨*string*⟩
Meaning	This message provides extended information on a GTP packet and whether the security device passed or dropped it.
Action	No recommended action.

Notification (00568)

Message	⟨*string*⟩
Meaning	This message reveals the content of a GTP packet sent to or originating from a subscriber that the security device was tracing.
Action	No recommended action.

Message	Trace ⟨*integer*⟩: ⟨*string*⟩
Meaning	This message provides the heading information of a GTP packet sent to or originating from a subscriber that the security device was tracing.
Action	No recommended action.

Chapter 23
H.323

The following section provides descriptions of and recommended action for ScreenOS messages displayed for GTP-related events.

Alert (00089)

Message	The number of RAS request messages sent to the GK, ⟨*gk_ip*⟩, exceeds the threshold, ⟨*ras_flooding_msg_threshold*⟩.
Meaning	The number of RAS request messages sent to the GK exceeds the configured message-flood threshold.
Action	No recommended action

Notification (00619)

Message	Failed to allocate memory for H.323 call context objects. Call dropped
Meaning	The system is temporarily out of memory.
Action	No action recommended. If the condition persists, restart the device.

Message	Concurrent H.323 calls exceeding maximum limit: ⟨*max_h323_call_num*⟩.
Meaning	The number of concurent calls on the security device exceeds the capacity of the device.
Action	No recommended action

Message	Failed to get NAT cookie. Too many concurrent H.323 calls: ⟨*active_h323_call_num*⟩. Call dropped.
Meaning	The security device failed to obtain the NAT cookie because call traffic exceeds the capacity of the device.
Action	No recommended action

Chapter 24
HDLC

The following messages relate to HDLC (High-Level Data Link Control) configurations.

Notification (00539)

Message	Dialup HDLC PPP failed to establish a session. No IP address assigned.
Meaning	The device did not establish a HDLC/PPP (High-Level Data Link Control)/(Point-to-Point Protocol) session with a host device, and did not assign an IP address to the serial interface.
Action	No recommended action.

Message	Dialup HDLC PPP failed to establish a session: ⟨*reason string*⟩.
Meaning	The device did not establish a HDLC/PPP (High-Level Data Link Control)/(Point-to-Point Protocol) session with a host device, and did not assign an IP address to the serial interface.
Action	No recommended action.

Message	Dialup HDLC PPP session has been successfully established.
Meaning	The device successfully established a HDLC/PPP (High-Level Data Link Control)/(Point-to-Point Protocol) session with a host device, and the device has a dynamically assigned IP address.
Action	No recommended action.

Chapter 25

High Availability

The following messages concern high availability (HA) settings, features, and operations using the Redundancy Protocol (NSRP), and the related functionality of IP tracking.

Critical (00015)

Message	NSRP: ⟨*string*⟩ ⟨*string*⟩.
Meaning	The HA control(data) channel has changed to NULL or some interface name.
Action	No recommended action.

Message	NSRP: ⟨*string*⟩.
Meaning	The physical link used for NSRP communications has either become active or inactive.
Action	Try to determine why the link went down. Typical reasons include the cable is unplugged, the cable is not seated in the port correctly, or the cable is faulty, possibly due to an electrical short. Also, check the port to see if you can establish a link with it.

Message	Peer device ⟨*integer*⟩ disappeared.
Meaning	The local device either could not locate or located the peer device in the NSRP device cluster.
Action	If the local device could not locate the peer device in the NSRP device cluster, check the cable connections between the two devices. Also, make sure both devices are powered up.

Message	Peer device ⟨*integer*⟩ was discovered.
Meaning	The local device either could not locate or located the peer device in the NSRP device cluster.
Action	If the local device could not locate the peer device in the NSRP device cluster, check the cable connections between the two devices. Also, make sure both devices are powered up.

Message	Peer device ⟨*integer*⟩ in the Virtual Security Device group ⟨*integer*⟩ changed state from ⟨*string*⟩ to ⟨*string*⟩.
Meaning	The state of the local or peer device in the specified VSD group has changed.
Action	No recommended action.

Message	RTO mirror group ⟨*integer*⟩ with direction ⟨*string*⟩ on local device ⟨*integer*⟩, detected a duplicate direction on the peer device ⟨*integer*⟩.
Meaning	This message indicates the direction on the peer device is the same as the one on the local device. A mirror group refers to the two devices in an NSRP cluster that exchange RTOs to each other for backup purposes. You can set a direction that determines which device transmits a copy (direction = out) and which device receives the copy (direction = in) of the RTOs. The specified RTO mirror group is unidirectional, therefore both a group ID and a directional attribute are required to uniquely identify this group.
Action	Check the NSRP configuration. If you detect duplicate directions on an RTO mirror group, change one of the directions so that the mirror group has both an incoming and outgoing direction on it.

Message	The NSRP configuration is out of synchronization between the local device and the peer device.
Meaning	The local device to which the administrative session is linked is not synchronized with the peer device (the other device in the NSRP cluster).
Action	Review the NSRP configuration between the two devices and see if they are configured to be peers. Also, check to make sure cables are connected properly and perform a manual synchronization.

Critical (00060)

Message	RTO mirror group ⟨*integer*⟩ with direction ⟨*string*⟩ changed on the local device from ⟨*string*⟩ to ⟨*string*⟩ state, it had peer device ⟨*integer*⟩.
Meaning	This message indicates that the current RTO mirror group is active and is in the up state. A mirror group refers to the two devices in an NSRP cluster that exchange RTOs to each other for backup purposes. You can set a direction that determines which device transmits a copy (direction = out) and which device receives the copy (direction = in) of the RTOs. The specified RTO mirror group is unidirectional, therefore both a group ID and a directional attribute are required to uniquely identify this group.
Action	No recommended action.

Critical (00061)

Message	RTO mirror group ⟨*integer*⟩ with direction ⟨*string*⟩ on peer device ⟨*integer*⟩ changed from ⟨*string*⟩ to ⟨*string*⟩ state, ⟨*string*⟩.
Meaning	This message indicates that the current RTO mirror group is functioning normally and is in the up state or failed and is in the down state. A mirror group refers to the two devices in an NSRP cluster that exchange RTOs to each other for backup purposes. You can set a direction that determines which device transmits a copy (direction = out) and which device receives the copy (direction = in) of the RTOs. The specified RTO mirror group is unidirectional, therefore both a group ID and a directional attribute are required to uniquely identify this group.
Action	No recommended action.

Critical (00062)

Message	Track IP IP address ⟨*IP address*⟩ succeeded.
Meaning	The Track IP session to detect whether the specified IP address is active either succeeded or failed. If it failed, the path may be blocked.
Action	No recommended action.

Message	Device cannot create Track IP list.
Meaning	The device was unable to create the Track IP object list. A Track IP object list contains a list of all objects that the device was able to contact. In addition, the list contains whether the Track IP was an NSRP Track IP attempt or an Interface Track IP attempt.
Action	No recommended action.

Message	Device cannot create Track IP object list.
Meaning	The device was unable to create the Track IP object list. A Track IP object list contains a list of all objects that the device was able to contact. In addition, the list contains whether the Track IP was an NSRP Track IP attempt or an Interface Track IP attempt.
Action	No recommended action.

Message	No interface/route enables the Track IP IP address ⟨*IP address*⟩ to be transmitted.
Meaning	The device was unable to locate a route to search for the specified IP address.
Action	Check the configuration of the link connection.

Message	Track IP failure reached threshold.
Meaning	The device attempted to track a specified IP address out on the network, and the number of failed attempts has reached a specified threshold.
Action	Verify the network connectivity between the device and the external IP address being tracked.

Message	Track IP IP address ⟨*IP address*⟩ failed.
Meaning	The Track IP session to detect whether the specified IP address is active either succeeded or failed. If it failed, the path may be blocked.
Action	No recommended action.

Critical (00070)

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group ⟨*integer*⟩ changed state from ⟨*string*⟩ to ⟨*string*⟩, ⟨*string*⟩.
Meaning	The state of the local device in the specified VSD group has changed to initial. When a device returns from the ineligible or inoperable state, it transitions to the initial state first.
Action	No recommended action.

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group ⟨*integer*⟩ changed state from ⟨*string*⟩ to ⟨*string*⟩.
Meaning	The state of the local or peer device in the specified VSD group has changed.
Action	No recommended action.

Critical (00071)

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group (⟨*integer*⟩) changed state from ⟨*string*⟩ to ⟨*string*⟩, ⟨*string*⟩.
Meaning	The state of the local device in the specified VSD group has changed to Master. The Master propagates all its network and configuration settings and the current session information to the backup.
Action	No recommended action.

Critical (00072)

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group (⟨*integer*⟩) changed state from ⟨*string*⟩ to ⟨*string*⟩, ⟨*string*⟩.
Meaning	The state of the local device in the specified VSD group has changed to primary backup. The primary backup becomes the master should the current master step down.
Action	No recommended action.

Critical (00073)

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group (⟨*integer*⟩) changed state from ⟨*string*⟩ to ⟨*string*⟩, ⟨*string*⟩.
Meaning	The state of the local device in the specified VSD group has changed to backup. A VSD group member in the backup state monitors the status of the primary backup and elects one of the backup devices to primary backup if the current one steps down.
Action	No recommended action.

Critical (00074)

Message	The local device ⟨*unit_id*⟩ in the Virtual Security Device group ⟨*group_id*⟩ changed state from ⟨*state_old*⟩ to ⟨*state_new*⟩, ⟨*string*⟩.
Meaning	An admin has changed the state of the local device to ineligible so that it cannot participate in the election process.
Action	No recommended action

Critical (00075)

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group ⟨*integer*⟩ changed state from ⟨*string*⟩ to ⟨*string*⟩.
Meaning	The state of the local device has changed to inoperable because of an internal system problem or a link failure.
Action	Check the device. Try to reset the device once you correct the problem.

Critical (00076)

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group ⟨*integer*⟩ sent a 2nd path request to the peer device ⟨*integer*⟩.
Meaning	The local device registered a missed heartbeat from the master device and as a result asks the master to retransmit the heartbeat via the secondary HA path (if it is configured). Having a secondary HA path can minimize the number of failovers in the event that the first HA link fails.
Action	No recommended action.

Critical (00077)

Message	The local device ⟨*integer*⟩ in the Virtual Security Device group ⟨*integer*⟩ received a 2nd path request from peer device ⟨*integer*⟩ to device ⟨*integer*⟩.
Meaning	The local device received a request to retransmit a missed heartbeat via the secondary HA path (if it is configured). Having a secondary HA path can minimize the number of failovers in the event that the first HA link fails.
Action	No recommended action.

Notification (00007)

Message	Message ⟨*msg_type_name*⟩ was dropped because it contained an invalid encryption password.
Meaning	The device dropped a message of the specified type (for example, SESS_CR, SESS_CL, SESS_CH) because one device in an NSRP cluster was encrypted with one key while the corresponding device in the NSRP cluster was encrypted with another key, forcing the operation to fail.
Action	Check the encryption password and correct it if it is wrong.

Message	NSRP black hole prevention disabled. Master(s) of Virtual Security Device groups might not exist.
Meaning	This message indicates that NSRP black hole prevention was disabled.
Action	No recommended action.

Message	NSRP black hole prevention enabled. Master(s) of Virtual Security Device groups always exists.
Meaning	This message indicates that NSRP black hole prevention was enabled.
Action	No recommended action.

Message	NSRP cluster authentication password changed.
Meaning	An NSRP authentication password protects an NSRP authentication session. In this case, the HA authentication session exchanged between two NSRP devices was encrypted with a different password than the receiving device expected from it.
Action	Check the authentication password and correct it if it is wrong.

Message	NSRP cluster encryption password changed.
Meaning	An NSRP encryption password protects an NSRP message. In this case, the HA message passing between two NSRP devices was encrypted with a different password than the receiving device expected from it.
Action	Check the message encryption password and correct it if it is wrong.

Message	NSRP Run Time Object synchronization between devices was disabled.
Meaning	An an admin has disabled run time object synchronization among devices in an NSRP cluster.
Action	No recommended action.

Message	NSRP Run Time Object synchronization between devices was enabled.
Meaning	An an admin enabled run time object synchronization among devices in an NSRP cluster.
Action	No recommended action.

Message	NSRP transparent Active-Active mode was disabled.
Meaning	This message indicates that the NSRP Transparent Active-Active mode was disabled.
Action	No recommended action.

Message	NSRP transparent Active-Active mode was enabled.
Meaning	This message indicates that the NSRP Transparent Active-Active mode was enabled.
Action	No recommended action.

Message	NSRP: ⟨*string*⟩.
Meaning	Probes determine whether the High Availability channel connecting devices in an NSRP cluster is still active. This message indicates that a link probe was enabled.
Action	No recommended action.

Message	The HA channel changed to interface ⟨*interface_name*⟩.
Meaning	Each High Availability (HA) channel maps to a specified interface on the HA device. This message indicates the HA channel now maps to a different interface.
Action	No recommended action.

Message	The heartbeat interval of all Virtual Security Device groups changed from ⟨*int_old*⟩ (milliseconds) to ⟨*int_new*⟩ (milliseconds).
Meaning	An admin has changed the interval (in milliseconds) at which members of a virtual security device (VSD) group send VSD heartbeats.
Action	No recommended action.

Message	Virtual Security Device group ⟨*vsd_id*⟩ changed to non-preempt mode.
Meaning	An admin has either enabled or disabled the preempt mode option on a member of the specified virtual security device (VSD) group. When you enable the preempt option on a device, it becomes the master of the VSD group if the current master has a lesser priority number (farther from zero). If you disable this option, a master with a lesser priority than a backup can keep its position (unless some other factor, such as an internal problem or faulty network connectivity, causes a failover).
Action	No recommended action.

Message	Virtual Security Device group ⟨*vsd_id*⟩ changed to preempt mode.
Meaning	An admin has either enabled or disabled the preempt mode option on a member of the specified virtual security device (VSD) group. When you enable the preempt option on a device, it becomes the master of the VSD group if the current master has a lesser priority number (farther from zero). If you disable this option, a master with a lesser priority than a backup can keep its position (unless some other factor, such as an internal problem or faulty network connectivity, causes a failover).
Action	No recommended action.

Message	A request by device ⟨*integer*⟩ for session synchronization(s) was accepted.
Meaning	Both the local and peer device in an NSRP cluster need to have identical configurations on them. This occurs by the local device copying and transferring its settings to the peer device through a process called synchronization. Both the local and peer device in an NSRP device cluster are periodically synchronized. Synchronization occurs in two ways: at preset intervals or by one device in the device pair requesting a synchronization. This message indicates one of the devices requested a synchronization and the other device responded indicating that it is ready for the process.
Action	No recommended action.

Message	Interface ⟨*string*⟩ was removed from the monitoring list for ⟨*string*⟩.
Meaning	The device and a Virtual Security Device can monitor interfaces for status changes. This message indicates the specified interface was removed from the monitoring list.
Action	No recommended action.

Message	Interface ⟨*string*⟩ with weight ⟨*integer*⟩ was added to or updated on the monitoring list for ⟨*string*⟩.
Meaning	The device and a Virtual Security Device can monitor interfaces for status changes. This message indicates the specified interface was either added to the specified monitoring list or updated with new settings.
Action	No recommended action.

Message	NSRP data forwarding was disabled.
Meaning	An admin has disabled traffic forwarding to other devices in the cluster.
Action	No recommended action.

Message	NSRP data forwarding was enabled.
Meaning	An admin has enabled traffic forwarding to other devices in the cluster.
Action	No recommended action.

Message	RTO mirror group ⟨*integer*⟩ was unset.
Meaning	Run time objects (RTOs) are code objects created dynamically in memory during normal operation, for example, session table entries, ARP cache entries, and DHCP leases. In the event of a failover, it is critical that the current RTOs be maintained by the new master to avoid service interruption. A mirror group refers to the two devices in an NSRP cluster that exchange RTOs to each other for backup purposes. You have successfully removed the local device from the RTO mirror group with the specified ID.
Action	No recommended action.

Message	Run Time Object mirror group ⟨*integer*⟩ direction was set to ⟨*string*⟩.
Meaning	A mirror group refers to the two devices in an NSRP cluster that exchange RTOs to each other for backup purposes. You can set a direction that determines which device transmits a copy (direction = out) and which device receives the copy (direction = in) of the RTOs. This message indicates the mirror group direction was set to the specified direction.
Action	No recommended action.

Message	Run Time Object mirror group ⟨*integer*⟩ was set.
Meaning	Run Time Object mirror group < mirror_group_id > was set.
Action	This message indicates that the RTO mirror group was enabled. A mirror group refers to the two devices in an NSRP cluster that exchange RTOs to each other for backup purposes.

Message	Run Time Object mirror group ⟨*integer*⟩ with direction ⟨*string*⟩ was unset.
Meaning	Run time objects (RTOs) are code objects created dynamically in memory during normal operation, for example, session table entries, ARP cache entries, and DHCP leases. In the event of a failover, it is critical that the current RTOs be maintained by the new master to avoid service interruption. A mirror group refers to the two devices in an NSRP cluster that exchange RTOs to each other for backup purposes. You can set a direction that determines which device transmits a copy (direction = out) and which device receives the copy (direction = in) of the RTOs. The specified RTO mirror group is unidirectional, therefore both a group ID and a directional attribute are required to uniquely identify this group. You have successfully removed the local device from the RTO mirror group by unsetting its direction.
Action	No recommended action.

Message	The current session synchronization by device ⟨*integer*⟩ completed.
Meaning	Both the local and peer device in an NSRP cluster need to have identical information on them. This occurs by the local device copying and transferring its settings to the peer device through a process called synchronization. The current synchronization by a device with the specified device ID and another device completed successfully.
Action	No recommended action.

Message	The interface ⟨*string*⟩ with ifnum ⟨*integer*⟩ was removed from the secondary HA path of the devices.
Meaning	A local and a peer device in an NSRP cluster can have two paths connecting each other, a primary path and a secondary or backup path used when the primary path is down. This message indicates that an administrator removed the interface to which the secondary path maps.
Action	No recommended action.

Message	The interval of the probe detecting the status of High Availability link ⟨*string*⟩ was set to ⟨*integer*⟩ seconds.
Meaning	Probes determine whether the High Availability channel connecting devices in an NSRP cluster is still active. Probes poll for channel status at a specified interval. This message indicates that the interval has been set to the specified number of seconds.
Action	No recommended action.

Message	The probe that detects the status of High Availability link ⟨*string*⟩ was disabled.
Meaning	Probes determine whether the High Availability channel connecting devices in an NSRP cluster is still active. This message indicates the channel connecting the devices was disabled.
Action	No recommended action.

Message	The secondary HA path of the devices changed from ⟨*string*⟩ to ⟨*string*⟩.
Meaning	A local and a peer device in an NSRP cluster can have two paths connecting each other, a primary path and a secondary or backup path used when the primary path is down. An admin successfully established a new secondary path connecting the local device with a peer device in the NSRP cluster.
Action	No recommended action.

Message	The secondary HA path of the devices was set to interface ⟨*string*⟩, with ifnum ⟨*integer*⟩.
Meaning	A local and a peer device in an NSRP cluster can have two paths connecting each other, a primary path and a secondary or backup path used when the primary path is down. Each path maps to a specific interface on the device. This message indicates that the interface to which the secondary path maps changed.
Action	No recommended action.

Message	The threshold of the probe detecting the status of High Availability link ⟨*string*⟩ was set to ⟨*integer*⟩.
Meaning	High Availability probes continually poll the interface that contains the High Availability link to detect the state of the interface. Each interface has a limit to how many times it allows the probe to continuously fail. This message indicates an administrator changed the value of the threshold. Typically, if the network behavior is volatile, you may want to set a higher threshold that enables a broader sampling because the interface state can change. If network behavior is stable, you may want a lower threshold where the probe needs to poll the interface less to obtain a representative snapshot of its state.
Action	No recommended action.

Message	Virtual Security Device group ⟨*unit_id*⟩ was created. The total number of members in the group is ⟨*cluster_id*⟩.
Meaning	An administrator created the specified Virtual Security Device group.
Action	No recommended action.

Message	Virtual Security Device group ⟨*unit_id*⟩ was deleted. The total number of members in the group was ⟨*cluster_id*⟩.
Meaning	An administrator removed the specified Virtual Security Device group.
Action	No recommended action.

Message	Zone ⟨*string*⟩ was removed from the monitoring list for ⟨*string*⟩.
Meaning	The device and a Virtual Security Device can monitor interfaces for status changes. This message indicates the specified zone was removed from the monitoring list.
Action	No recommended action.

Message	Zone ⟨*string*⟩ with weight ⟨*integer*⟩ was added to or updated on the monitoring list for ⟨*string*⟩.
Meaning	The device and a Virtual Security Device can monitor interfaces for status changes. This message indicates the specified zone was either added to the monitoring list or updated with new settings.
Action	No recommended action.

Message	The NSRP encryption key was changed.
Meaning	An admin has changed the encryption password, which in turn has changed the key.
Action	No recommended action.

Message	Device ⟨*int_old*⟩ has joined NSRP cluster ⟨*int_new*⟩ ⟨*string*⟩.
Meaning	An admin either added the specified device from the NSRP cluster.
Action	No recommended action.

Message	Device ⟨*unit_id*⟩ quit current NSRP cluster ⟨*cluster_id*⟩ ⟨*string*⟩.
Meaning	An admin either removed the specified device from the NSRP cluster.
Action	No recommended action.

Message	The monitoring threshold was modified to ⟨*integer*⟩ for ⟨*string*⟩.
Meaning	The device and Virtual Security Device (VSD) group monitor the monitoring list for interfaces, zones, and track IP objects that are down. Each of these objects have a weight value associated with them that an administrator can define. After traversing the monitoring list, the total weights of all the down entities are summed which comprises the threshold by which the device of VSD will tolerate failure on the list.
Action	No recommended action.

Message	Virtual Security Device group ⟨*integer*⟩ priority changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	Each VSD in a High Availability VSD group is assigned a value that indicates how likely the device is to be elected the master in the redundancy relationship established between the two VSD group members. This value is known as a priority and ranges from 1 to 254. The default priority is 100. In this instance the priority value of the current VSD has been changed.
Action	No recommended action.

Notification (00050)

Message	Track IP ⟨*string*⟩
Meaning	Track IP event notification.
Action	No recommended action.

Message	Track default gateway disabled.
Meaning	For the interface to monitor the default gateway, you need to enable the Track IP default gateway. This message indicates the Track IP default gateway was enabled.
Action	No recommended action.

Message	Track IP default gateway enabled.
Meaning	For the interface to monitor the default gateway, you need to enable the Track IP default gateway. This message indicates the Track IP default gateway had the monitoring mode removed (disabled).
Action	No recommended action.

Message	Track IP default gateway updated.
Meaning	Each Track IP attempt to locate an IP address traverses a specified gateway IP address. This message indicates the Track IP default gateway changed.
Action	No recommended action.

Message	Track IP ⟨*vsd_id*⟩ interface changed from ⟨*string*⟩ to ⟨*string*⟩.
Meaning	Each Track IP attempt to locate an IP address originates at a specified interface. An admin has changed the originating interface for the specified tracked IP.
Action	No recommended action.

Message	Track IP ⟨*IP address*⟩ interval changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	An admin has changed the Track IP interval value, which is the specified number of seconds between each Track IP attempt to locate an IP address.
Action	No recommended action.

Message	Track IP ⟨*IP address*⟩ method changed from method name ⟨*string*⟩ to ⟨*string*⟩
Meaning	An admin has changed the method for tracking the specified IP address. Track IP has two methods of locating an IP address path. One way is using the Address Resolution Protocol (ARP) method which deploys a direct connection over the OSI Model Data Link layer (layer 2). The other way is using the Ping method which deploys a virtual connection over the OSI Model Network layer (layer 3).
Action	No recommended action.

Message	Track IP ⟨*IP address*⟩ threshold value changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	An admin has changed the Track IP threshold value which is the number of times the device attempts to locate an IP address before determining the IP address is unreachable.
Action	No recommended action.

Message	Track IP ⟨*IP address*⟩ weight changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	An admin has changed the Track IP weight value of an IP address. This weight value indicates the importance of connectivity to the specified address in relation to reaching other tracked addresses.
Action	No recommended action.

Message	Track IP IP address ⟨*IP address*⟩ added with an interval of ⟨*integer*⟩ seconds, a threshold of ⟨*integer*⟩, a weight of ⟨*integer*⟩ on interface ⟨*string*⟩ using method ⟨*string*⟩.
Meaning	A path was added to the Track IP list.
Action	No recommended action.

Message	Track IP IP address ⟨*IP address*⟩ removed.
Meaning	A path was removed from the Track IP list.
Action	No recommended action.

Message	Track IP object ⟨*string*⟩ weight value set to ⟨*integer*⟩.
Meaning	The < name > track IP object weight value was set to < number > .
Action	No recommended action.

Message	Track IP object ⟨*string*⟩ weight value set to default.
Meaning	Track IP object < track_ip_object_name > failed because the Track IP default weight value was exceeded.
Action	No recommended action.

Message	Track IP threshold set to ⟨*integer*⟩.
Meaning	If the value of the summed weights of all failed Track IPs surpasses a specified value, then the threshold has been exceeded and the Track IP attempt fails. This message indicates the Track IP threshold was exceeded. If this is an interface Track IP attempt, the attempt fails and no more activity occurs. If this is an NSRP Track IP attempt, then the attempt fails, but transfers the activity over to a backup interface.
Action	If you believe the IP address is reachable, you may want to provide a higher Track IP threshold value. If you believe the IP address may have a problem associated with it, check its link connection.

Message	Track IP threshold set to default.
Meaning	A configured Track IP threshold changed back to the default Track IP threshold value.
Action	No recommended action.

Message	Track IP ⟨*IP address*⟩ gateway was changed from gateway IP address ⟨*IP address*⟩ to ⟨*IP address*⟩.
Meaning	This message indicates the gateway address changed.
Action	No recommended action.

Message	Track IP ⟨*IP address*⟩ gateway was changed from gateway IP address ⟨*IP address*⟩ to the interface default gateway.
Meaning	This message indicates the gateway address changed.
Action	No recommended action.

Message	Track IP ⟨*IP address*⟩ gateway was changed from the interface default gateway to gateway IP address ⟨*IP address*⟩.
Meaning	This message indicates the gateway address changed.
Action	No recommended action.

Notification (00084)

Message	RTSYNC: NSRP route synchronization is disabled.
Meaning	Configuration for route synchronization has been removed.
Action	No recommended action.

Message	RTSYNC: NSRP route synchronization is enabled.
Meaning	A user has configured route synchronization.
Action	No recommended action

Notification (00620)

Message	RTSYNC: Event posted to purge backup routes in all vrouters.
Meaning	A task has been scheduled to purge all backup routes.
Action	No recommended action. Informational only.

Message	RTSYNC: Event posted to send all the DRP routes to backup device.
Meaning	As part of route synchronization being enabled, a task has been scheduled to send all the DRP routes to a backup device.
Action	No recommended action. Informational only.

Message	RTSYNC: Recieved coldstart request for route synchronization from NSRP peer.
Meaning	An active device has received a cold-start request to sychronize all DRP routes from a backup device that just came up.
Action	No recommended action. Informational only.

Message	RTSYNC: Serviced coldstart request for route synchronization from NSRP peer.
Meaning	An active device has completed sychronizing all DRP routes as requested by a backup device that just came up.
Action	No recommended action. Informational only.

Message	RTSYNC: Started timer to purge all the DRP backup routes - ⟨*purge_time_in_seconds*⟩ seconds.
Meaning	As part of a backup device becoming active, a timer has been started to purge all DRP routes.
Action	No recommended action. Information only.

Message	RTSYNC: Timer to purge the DRP backup routes is stopped.
Meaning	A purge timer that was started when the backup device became active has been stopped. This is possible if the new active device becomes backup before the timer fires.
Action	No recommended action. Informational only.

Information (00767)

Message	HA: Synchronization file(s) ⟨*filename*⟩ sent to backup device in cluster.
Meaning	The device created a backup of the current HA synchronization file.
Action	No recommended action.

Chapter 26
IGMP

The following messages relate to the Internet Group Management Protocol (IGMP) multicast protocol.

Notification (00055)

Message	IGMP all groups static flag was removed on interface ⟨*string*⟩.
Meaning	An admin deleted the static mapping between the multicast groups and the specified interface.
Action	No recommended action

Message	IGMP function was disabled on interface ⟨*string*⟩.
Meaning	An admin either enabled or disabled IGMP on the specified interface.
Action	No recommended action

Message	IGMP function was enabled on interface ⟨*string*⟩.
Meaning	An admin either enabled or disabled IGMP on the specified interface.
Action	No recommended action

Message	IGMP group ⟨*IP address*⟩ static flag was added on interface ⟨*string*⟩.
Meaning	An admin defined a group as static on the specified interface.
Action	No recommended action

Message	IGMP group ⟨*IP address*⟩ static flag was removed on interface ⟨*string*⟩.
Meaning	An admin deleted the static mapping between the multicast group and the specified interface.
Action	No recommended action

Message	IGMP groups accept list ID was changed to ⟨*integer*⟩ on interface ⟨*string*⟩.
Meaning	An admin changed the access list that identifies the multicast groups the hosts on the specified interface can join.
Action	No recommended action

Message	IGMP host instance was created on interface ⟨*string*⟩.
Meaning	An admin either created or removed the IGMP host instance from the specified interface.
Action	No recommended action

Message	IGMP host instance was deleted on interface ⟨*string*⟩.
Meaning	An admin either created or removed the IGMP host instance from the specified interface.
Action	No recommended action

Message	IGMP hosts accept list ID was changed to ⟨*integer*⟩ on interface ⟨*string*⟩.
Meaning	An admin changed the access list that identifies the hosts from which the interface can accept IGMP messages.
Action	No recommended action

Message	IGMP last member query interval was changed to ⟨*integer*⟩ seconds on interface ⟨*string*⟩.
Meaning	An admin changed the last member query interval on the specified interface.
Action	No recommended action

Message	IGMP leave interval was changed to ⟨*integer*⟩ seconds on interface ⟨*string*⟩.
Meaning	An admin changed the leave interval on the specified interface.
Action	No recommended action

Message	IGMP proxy always is disabled on interface ⟨*string*⟩.
Meaning	An admin disabled the feature that allows the interface to forward IGMP messages in querier and non-querier mode.
Action	No recommended action

Message	IGMP proxy always is enabled on interface ⟨*string*⟩.
Meaning	An admin enabled the feature that allows the interface to forward IGMP messages in querier and non-querier mode.
Action	No recommended action

Message	IGMP proxy was disabled on interface ⟨*string*⟩.
Meaning	An admin disabled the IGMP proxy on the specified interface.
Action	No recommended action

Message	IGMP proxy was enabled on interface ⟨*string*⟩.
Meaning	An admin enabled the IGMP proxy on the specified interface.
Action	No recommended action

Message	IGMP query interval was changed to ⟨*integer*⟩ seconds on interface ⟨*string*⟩.
Meaning	An admin changed the IGMP query interval on the specified interface.
Action	No recommended action

Message	IGMP query max response time was changed to ⟨*integer*⟩ seconds on interface ⟨*string*⟩.
Meaning	An admin changed the maximum response time on the specified interface.
Action	No recommended action

Message	IGMP router instance was created on interface ⟨*string*⟩.
Meaning	An admin either created or removed the IGMP router instance from the specified interface.
Action	No recommended action

Message	IGMP router instance was deleted on interface ⟨*string*⟩.
Meaning	An admin either created or removed the IGMP router instance from the specified interface.
Action	No recommended action

Message	IGMP routers accept list ID was changed to ⟨*integer*⟩ on interface ⟨*string*⟩.
Meaning	An admin changed the access list that identifies the routers that are eligible for Querier election. Only the routers in the specified access list can be elected as Querier.
Action	No recommended action

Message	IGMP static group ⟨*IP address*⟩ was added on interface ⟨*string*⟩.
Meaning	An admin manually added the multicast group to the specified interface.
Action	No recommended action

Message	IGMP version was changed to V⟨*integer*⟩ on interface ⟨*string*⟩.
Meaning	An admin changed the IGMP version that was enabled on the interface.
Action	No recommended action

Message	IGMP will do router alert IP option check on interface ⟨*string*⟩.
Meaning	The specified interface checks whether an IGMP packet has the router-alert IP option before it accepts the packet. The interface drops all packets that do not have this option.
Action	No recommended action.

Message	IGMP will do same subnet check on interface ⟨*string*⟩.
Meaning	The specified interface accepts IGMP messages only from its own subnet.
Action	No recommended action.

Message	IGMP will not do router alert IP option check on interface ⟨*string*⟩.
Meaning	The specified interface does not check whether an IGMP packet has the router-alert IP option before it accepts the packet.
Action	No recommended action.

Message	IGMP will not do same subnet check on interface ⟨*string*⟩.
Meaning	The specified interface accepts IGMP messages from all sources, regardless of their subnet.
Action	No recommended action.

Chapter 27
IKE

The following messages relate to the Internet Key Exchange (IKE) protocol, one of the three main components of IPSec-the other two are the Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols. IKE provides a secure means for the distribution and maintenance of cryptographic keys and the negotiation of the parameters constituting a secure communications channel.

Alert (00026)

Message	IKE ⟨*gateway_ip*⟩: Policy Manager's default CA is used by peer to establish an IPSec VPN.
Meaning	The specified IKE peer has used the default certificate authority (CA) certificate supported by the Policy Manager (PM) component of NetScreen-Global PRO when establishing an IPSec VPN tunnel with the local security device.
Action	Use a different CA certificate.

Message	IPSec tunnel on interface ⟨*if_name*⟩ with tunnel ID 0x⟨*sa_tid_hex*⟩ received a packet with a bad SPI. ⟨*src_ip*⟩->⟨*dst_ip*⟩/⟨*pak_len*⟩, ⟨*esp_or_ah*⟩, SPI 0x⟨*spi_hex*⟩, SEQ 0x⟨*seq_number_hex*⟩.
Meaning	The local security device received a packet with an incorrect security parameters index (SPI) number through the IPSec tunnel with the specified ID number (in hexadecimal notation) arriving at the specified interface. The message indicates the source and destination IP addresses of the outer packet header and the packet length (in bytes). The packet was either formatted for the Encapsulating Security Payload (ESP) or Authentication Header (AH) protocol, and had the specified SPI number and the sequence number—both in hexadecimal notation. The security device dropped the packet, and if it found a valid VPN configuration for the source IP address and Initial Contact notification was enabled, it also sent an Initial Contact Notify message to that address. Note: By default, when the security device detects multiple packets with a bad SPI number, this message appears in the log once every 10 seconds per tunnel. If you want the security device to make a log entry for every detected packet with a bad SPI number, enter the "set firewall log-self ike" command; however, Juniper Networks does not recommend this because the logging can become excessive.
Action	If the problem persists, notify the admin of the remote peer gateway.

Alert (00048)

Message	Number of IAS crossed configured upper threshold ⟨*ias_upper*⟩.
Meaning	The device attempted to establish more IASs (IPSec Access Sessions) than the configured upper threshold.
Action	No recommended action

Alert (00049)

Message	Number of IAS crossed configured lower threshold ⟨*ias_lower*⟩.
Meaning	The device attempted to establish more IASs (IPSec Access Sessions) than the configured lower threshold.
Action	No recommended action

Critical (00000)

Message	Attack alarm: IKE first message DoS attack on interface ⟨*if_name*⟩ from source IP ⟨*src_ip*⟩.
Meaning	An IKE DoS attack packet was received. When DoS attack protection was enabled with the "set ike dos-protection" command, if the first IKE packet number received in the interval time exceeded the threshold, the packet is considered an IKE DoS attack packet.
Action	Check how the IKE DoS protection was configured to confirm whether it's a DoS attacked packet.

Critical (00042)

Message	Replay packet detected on IPSec tunnel on ⟨*if_name*⟩ with tunnel ID 0x⟨*sa_tid_hex*⟩! From ⟨*src_ip*⟩ to ⟨*dst_ip*⟩/⟨*pak_len*⟩, ⟨*esp_or_ah*⟩, SPI 0x⟨*spi_hex*⟩, SEQ 0x⟨*seq_number_hex*⟩.
Meaning	The security device detected and rejected a replay packet arriving at the specified interface through the IPSec tunnel with the specified ID number (in hexadecimal notation). The message indicates the source and destination IP addresses of the outer packet header and the packet length (in bytes). The packet was either formatted for the Encapsulating Security Payload (ESP) or Authentication Header (AH) protocol, and had the specified SPI number and the sequence number—both in hexadecimal notation. Note: By default, when the security device detects multiple replay packets on a VPN tunnel, this message appears in the log once every 10 seconds. If you want the security device to make a log entry for every detected replay packet, enter the "set firewall log-self ike" command; however, Juniper Networks does not recommend this because the logging can become excessive.
Action	This message might indicate an attack or a network loop. If it is an attack, the security device has successfully blocked it, and you need take no further action. If you suspect that it is not an attack, investigate the network for a network loop. For example, you might try performing a traceroute to determine the nodes along the data path, and then use a sniffer to detect where the packet duplicates itself. If the data path flows through a public network such as the Internet, this approach is probably not possible, but other options might be available.

Critical (00111)

Message	Attack alarm: IKE ID enumeration attack on interface ⟨*if_name*⟩ from src_ip ⟨*src_ip*⟩.
Meaning	An IKE ID enumeration attack on the specified interface and from the specified IP address has been detected.
Action	Determine the source of the attack. Consider changing the preshared key more often on the affected IKE gateways.

Critical (00114)

Message	ACVPN: Error in received profile from hub in vr ⟨*vr-name*⟩: ⟨*error_buf*⟩.
Meaning	The AC-VPN profile received from the hub cannot be applied to the current configuration. The dynamic AC-VPN tunnels between spokes might not become operational as expected.
Action	Check the current configuration in the device to see if there is any conflict with the received AC-VPN profile. Also, you might update the administrator of the hub about the error.

Error

Message	IAS for peer ⟨*peer_ip*⟩ has IKE error: ⟨*ias_ike_error_log*⟩.
Meaning	The device established fewer IASs (IPSec Access Sessions) than the configured lower threshold.
Action	No recommended action

Error

Message	IAS for peer ⟨*peer_ip*⟩ has IKE error: ⟨*ias_ike_error_log*⟩.
Meaning	The device established fewer IASs (IPSec Access Sessions) than the configured lower threshold.
Action	No recommended action

Error

Message	The number of IAS exceeds the configured maximum ⟨*ias_max*⟩.
Meaning	The device attempted to establish more IASs (IPSec Access Sessions) than the configured maximum. An IAS is the time interval during which a network access session exists. This interval begins when the first end user connects to the access network and ends when the last user disconnects from the network.
Action	No recommended action

Error (00536)

Message	IAS for peer ⟨*peer_ip*⟩ and XAUTH user ⟨*xauth_uname*⟩ activated.
Meaning	The remote connection for the specified peer and user became active.
Action	No recommended action

Message	IAS for peer ⟨*peer_ip*⟩ and XAUTH user ⟨*xauth_uname*⟩ terminated by ⟨*ternimate_cause*⟩.
Meaning	The connection for the specified remote peer and user was terminated.
Action	No recommended action

Notification (00017)

Message	Gateway ⟨*gateway_name*⟩ at ⟨*gateway_ip*⟩ in ⟨*IKE_XCHG_mode*⟩ mode with ID ⟨*peer_id*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin has added or modified the settings for, or deleted the specified remote IKE gateway. The peer IKE ID is the expected identification of the peer for authentication purposes. ScreenOS supports four types of IKE ID: IP address, domain name, fully qualified domain name (FQDN), and distinguished name (DN). DN is a name used to identify an entry in the Open Systems Interconnection (OSI) Directory; in a certificate, it is used as the primary name to uniquely identify the subject. The IKE ID is optionally configurable. If configured, the peer must send the configured ID for authentication to succeed. If not configured, the implied (default) IDs are assumed. For the preshared-key authentication method, the default ID is the peer's IP address; for RSA signature authentication, the default ID is whatever is specified in the "Alternative Name" field in the certificate. The alternative name can be either IP address, domain name, or FQDN.
Action	No recommended action

Message	P1 proposal ⟨*proposal_name*⟩ with ⟨*auth_method*⟩, DH group ⟨*DH_group*⟩, ESP ⟨*ESP_enc_method*⟩, auth ⟨*ESP_auth_method*⟩, and lifetime ⟨*lifetime*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin has added or deleted the specified Phase 1 proposal, or modified at least one of the following Phase 1 proposal attributes: Preshared Key RSA signature DSA signature Diffie-Hellman group 1, 2, or 5 Note: “DH group ” indicates that a DH group is not employed because the proposal does not contain Perfect Forwarding Secrecy (PFS). Encapsulating Security Payload (ESP) protocol Data Encryption Standard (DES) encryption algorithm Triple DES (3DES) encryption algorithm Advanced Encryption Standard (AES) encryption algorithm Authentication Header (auth) protocol Message Digest version 5 (MD5) hash algorithm Secure Hash Algorithm-1 (SHA-1) hash algorithm Lifetime (number in seconds, minutes, hours, or days)
Action	No recommended action

Message	P2 proposal ⟨*proposal_name*⟩ with DH group ⟨*DH_group*⟩, ⟨*protocol*⟩, enc ⟨*ESP_enc_method*⟩, auth ⟨*ESP_auth_method*⟩, and lifetime (⟨*lifetime*⟩ sec/⟨*lifesize*⟩ KB) ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin has added or deleted the specified Phase 1 proposal, or modified at least one of the following attributes: Diffie-Hellman group 1, 2, or 5 Note: "DH group " indicates that a DH group is not employed because the proposal does not contain Perfect Forwarding Secrecy (PFS). Authentication Header (AH) protocol Encapsulating Security Payload (ESP) protocol DSA signature Data Encryption Standard (DES) encryption algorithm Triple DES (3DES) encryption algorithm Advanced Encryption Standard (AES) encryption algorithm Message Digest version 5 (MD5) hash algorithm Secure Hash Algorithm-1 (SHA-1) hash algorithm Lifetime—number in seconds, minutes, hours, or days; and number in kilobytes
Action	No recommended action

Information

Message	IKE Heartbeat configuration ⟨*configure_item_name*⟩
Meaning	The configuration for IKE heartbeat has changed.
Action	No recommended action

Information (00536)

Message	IAS for peer ⟨*peer_ip*⟩ and XAUTH user ⟨*xauth_uname*⟩ activated.
Meaning	An IAS (IPSec Access Session) is the time interval during which a network access session exists. The IAS time interval begins when the first end user connects to the access network and ends when the last user disconnects from the network.
Action	No recommended action

Message	IAS for peer ⟨*peer_ip*⟩ and XAUTH user ⟨*xauth_uname*⟩ terminated by ⟨*ternimate_cause*⟩.
Meaning	An IAS (IPSec Access Session) was terminated due to a condition or action (string).
Action	No recommended action

Message	IKE gateway ⟨*gateway_name*⟩ has been disabled because the peer IP address ⟨*peer_ip*⟩ is already in use by another IKE gateway on interface ⟨*gateway_name*⟩.
Meaning	When an administrator configured the named IKE gateway with a host name or a fully qualified domain name (FQDN = host name + domain name), the security device successfully resolved the name to an IP address but then discovered that another IKE gateway configuration has already used the same IP address. As a result, the security device has temporarily disabled that IKE gateway.
Action	Check that the host name or FQDN is correct. Check the IKE gateway configurations.

Message	IKE gateway ⟨*gateway_name*⟩ has been disabled. The peer address ⟨*peer_addr_name*⟩ cannot be resolved to an IP address.
Meaning	When an administrator configured the named IKE gateway with a host name or a fully qualified domain name (FQDN = host name + domain name), the security device was unable to resolve the name to an IP address. As a result, the security device has temporarily disabled that IKE gateway.
Action	Check that the host name or FQDN is correct. Ensure that the security device is properly configured for DNS service. Also check if the security device can connect to the DNS server and that the DNS server is responsive to DNS queries.

Message	IKE gateway ⟨*gateway_name*⟩ has been enabled. The peer address ⟨*peer_addr_name*⟩ has been resolved to ⟨*peer_ip*⟩.
Meaning	When an administrator configured the named IKE gateway with a host name or a fully qualified domain name (FQDN = host name + domain name), the security device was unable to resolve the name to an IP address. As a result, the security device has temporarily disabled that IKE gateway.
Action	Check that the host name or FQDN is correct. Ensure that the security device is properly configured for DNS service. Also check if the security device can connect to the DNS server and that the DNS server is responsive to DNS queries.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Aborted negotiations because the time limit has elapsed. (⟨*p1_state_mask*⟩x/⟨*p1_state*⟩)
Meaning	The security device has aborted Phase 1 or Phase 2 negotiations with the specified remote peer because the time limit—60 seconds for Phase 1 and 40 seconds for Phase 2—has elapsed. The information that appears in parentheses at the end of the message is for internal use only.
Action	Verify network connectivity to the peer gateway. Consult the local log and request the remote gateway admin to consult their log to determine why the negotiations timed out before completion.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Aggressive mode negotiations have failed.
Meaning	The Phase 1 session initiated by the local security device to the specified peer has failed. The session was in either Main mode or Aggressive mode.
Action	Check the event log on the local device and request the remote admin to consult the event log on the remote device to determine the cause of the failure.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Cannot use a preshared key because the peer gateway ⟨*gateway_name*⟩ has a dynamic IP address and negotiations are in Main mode.
Meaning	When configuring an IPSec tunnel to the specified remote gateway, which has a dynamically assigned IP address, an admin specified a preshared key and selected Main mode for the Phase 1 negotiations. Authentication via preshared key is not allowed when Main mode is used with a peer at a dynamically assigned IP address.
Action	Reconfigure the VPN using a certificate to authenticate the remote party, or select Aggressive mode for use with preshared key authentication.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Cannot verify DSA signature.
Meaning	The local security device cannot verify the RSA or DSA signature sent by the specified IKE peer.
Action	Contact the remote admin to check if he or she sent a certificate with the public key matching the private key used to produce the signature.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Cert received has a different FQDN SubAltName than expected.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject alternative name (SubAltName) than was configured as the IKE ID on the local device. The SubAltName is an alternative name for the subject of a certificate. Juniper Networks supports the following kinds: IP address, such as 209.157.66.170 Fully qualified domain name (FQDN), such as www.juniper.net User's fully qualified domain name (UFQDN), such as jsmith@juniper.net
Action	Recommend the peer use a certificate with the expected SubAltName or change the IKE ID in the local VPN configuration to match that of the certificate.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Cert received has a different IP address SubAltName than expected.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject alternative name (SubAltName) than was configured as the IKE ID on the local device. The SubAltName is an alternative name for the subject of a certificate. Juniper Networks supports the following kinds: IP address, such as 209.157.66.170 Fully qualified domain name (FQDN), such as www.juniper.net User's fully qualified domain name (UFQDN), such as jsmith@juniper.net
Action	Recommend the peer use a certificate with the expected SubAltName or change the IKE ID in the local VPN configuration to match that of the certificate.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Cert received has a different UFQDN SubAltName than expected.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject alternative name (SubAltName) than was configured as the IKE ID on the local device. The SubAltName is an alternative name for the subject of a certificate. Juniper Networks supports the following kinds: IP address, such as 209.157.66.170 Fully qualified domain name (FQDN), such as www.juniper.net User's fully qualified domain name (UFQDN), such as jsmith@juniper.net
Action	Recommend the peer use a certificate with the expected SubAltName or change the IKE ID in the local VPN configuration to match that of the certificate.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Cert received has a subject name that does not match the ID payload.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject than the IKE ID sent by the peer. The subject of a certificate can be a distinguished name (DN) composed of a concatenation of the common name elements listed in the request submitted for that certificate. The DN is the identity of the certificate holder.
Action	Advise the peer to change the IKE ID in its VPN configuration to match that of the certificate, or use a certificate with a subject name that matches the IKE ID configured for the VPN.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Completed Aggressive mode negotiations with a ⟨*lifetime*⟩-second lifetime.
Meaning	The security device and the specified remote gateway have successfully completed Phase 1 negotiations in either Aggressive mode or Main mode with the lifetime of the Phase 1 security association (SA) defined in seconds.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Completed for user ⟨*user_name*⟩.
Meaning	The security device and the specified remote IKE user have successfully completed Phase 1 negotiations.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Completed Main mode negotiations with a ⟨*lifetime*⟩-second lifetime.
Meaning	The security device and the specified remote gateway have successfully completed Phase 1 negotiations in either Aggressive mode or Main mode with the lifetime of the Phase 1 security association (SA) defined in seconds.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Discarded a second initial packet, which arrived within 5 seconds after the first.
Meaning	The local security device received two initial Phase 1 packets from the peer at the specified address within a five-second interval. As a result, the local device dropped the second initial packet.
Action	Verify if the packets came from a legitimate peer gateway. If so, check the local logs and request the remote gateway admin to check his logs to uncover the cause of the difficulty in completing the Phase 1 negotiations.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Discarded peer's P1 request because there are currently ⟨*ongoing_sessions*⟩ sessions--max is ⟨*max_allowed*⟩.
Meaning	The local security device rejected an initial Phase 1 packet from the peer at the specified address because the number of concurrent sessions was too high.
Action	The peer can try again at a later time when the number of sessions might be lower.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Main mode negotiations have failed.
Meaning	The Phase 1 session initiated by the local security device to the specified peer has failed. The session was in either Main mode or Aggressive mode.
Action	Check the event log on the local device and request the remote admin to consult the event log on the remote device to determine the cause of the failure.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: No private key exists to sign packets.
Meaning	The private key needed to create an RSA or DSA signature to authenticate packets destined for the specified IKE peer does not exist. This situation can arise if the following conditions are met: (1) If the local configuration for the remote gateway specifies a local certificate that an admin later removes (2) If there are no local certificates in the certificate store and no local certificate is specified in the remote gateway configuration
Action	Obtain and load a certificate for use in authenticating IKE packets.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Received an incorrect public key authentication method.
Meaning	In the first and second Phase 1 messages, the IKE participants agreed to use a preshared key for packet authentication. Then, in the fifth or sixth message (Main mode) or second or third message (Aggressive mode), the remote peer sent a signature payload, which requires the local device to use a public key (not a preshared key) to authenticate the packet. The security device, however, does not attempt to authenticate the packet; it drops the packet.
Action	Check if the remote peer is a legitimate IKE peer. If so, contact the remote admin to check if that device has malfunctioned. If not, this might be an ineffectual attack in which the attacker is attempting to force the security device to consume bandwidth while trying to verify bogus signature payloads.

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Responder starts ⟨*phase_1_mode*⟩ mode negotiations.
Meaning	The remote peer at the specified IP address has initiated Phase 1 negotiations in either Main or Aggressive mode, and the local security device (the "Responder") has begun its response.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 1: Retransmission limit has been reached.
Meaning	The local security device has reached the retransmission limit (10 failed attempts) during Phase 1 negotiations with the specified remote peer because the local device has not received a response. Note: If the local device continues receiving outbound traffic for the remote peer after the first 10 failed attempts, it makes another 10 attempts, and continues to do so until it either succeeds at contacting the remote gateway or it no longer receives traffic bound for that gateway.
Action	Verify network connectivity to the peer gateway. Request the remote gateway admin to consult the log to determine if the connection requests reached it and, if so, why the device did not respond.

Message	IKE ⟨*gateway_ip*⟩ Phase 2 msg ID ⟨*message_id*⟩x: Completed negotiations with SPI ⟨*spi*⟩x, tunnel ID ⟨*tunnel_id*⟩, and lifetime ⟨*lifetime*⟩ seconds/⟨*lifesize*⟩ KB.
Meaning	The local security device has successfully negotiated a Phase 2 session with the specified peer. The Phase 2 session consists of the specified attributes.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 2 msg ID ⟨*message_id*⟩x: Negotiations have failed for user ⟨*user_name*⟩.
Meaning	The specified Phase 2 negotiations to the identified IKE user have failed.
Action	Examine the local log and VPN configuration, and request the remote IKE user to examine the configuration on their VPN client for possible causes.

Message	IKE ⟨*gateway_ip*⟩ Phase 2 msg ID ⟨*message_id*⟩x: Negotiations have failed.
Meaning	The specified Phase 2 negotiations to an unidentified IKE user have failed.
Action	Examine the local log and VPN configuration, and request the remote IKE user to examine the configuration on their VPN client for possible causes.

Message	IKE ⟨*gateway_ip*⟩ Phase 2 msg ID ⟨*message_id*⟩x: Responded to the peer's first message from user ⟨*user_name*⟩.
Meaning	The local security device has responded to the specified peer, which sent the first message for Phase 2 IKE negotiations.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 2 msg ID ⟨*message_id*⟩x: Responded to the peer's first message.
Meaning	The local security device has responded to the specified peer, which sent the first message for Phase 2 IKE negotiations.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 2 msg-id ⟨*message_id*⟩x: Completed for user ⟨*user_name*⟩.
Meaning	The security device and the specified remote IKE user have successfully completed Phase 2 negotiations.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 2: Aborted negotiations because the time limit has elapsed. (⟨*p1_state_mask*⟩x/⟨*p1_state*⟩, session ID ⟨*session_id*⟩x)
Meaning	The security device has aborted Phase 1 or Phase 2 negotiations with the specified remote peer because the time limit—60 seconds for Phase 1 and 40 seconds for Phase 2—has elapsed. The information that appears in parentheses at the end of the message is for internal use only.
Action	Verify network connectivity to the peer gateway. Consult the local log and request the remote gateway admin to consult their log to determine why the negotiations timed out before completion.

Message	IKE ⟨*gateway_ip*⟩ Phase 2: Initiated negotiations.
Meaning	The local security device has sent the initial message for IKE Phase 2 negotiations to the specified peer.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ Phase 2: Negotiations have failed. Policy-checking has been disabled but multiple VPN policies to the peer exist.
Meaning	An admin has disabled policy-checking although multiple access policies for VPN traffic to the specified peer exist. Consequently, the IKE module cannot find the correct security association (SA) for traffic covered by each policy. Note: Policy-checking must be enabled if multiple policies for VPN traffic to the same gateway exist.
Action	Enable policy-checking or limit one policy per remote gateway.

Message	IKE ⟨*gateway_ip*⟩ Phase 2: No policy exists for the proxy ID received: local ID (⟨*local IP*⟩/⟨*local mask*⟩, ⟨*local protocol*⟩, ⟨*local port*⟩) remote ID (⟨*remote IP*⟩/⟨*remote mask*⟩, ⟨*remote protocol*⟩, ⟨*remote port*⟩).
Meaning	When the local security device received an IKE Phase 2 message from the specified peer, it detected that no policy exists matching the attributes specified in the proxy ID payload.
Action	If you intend to allow IPSec traffic between the specified local and remote end entities, configure the necessary policy.

Message	IKE ⟨*gateway_ip*⟩ Phase 2: Received a message but did not check a policy because id-mode was set to IP or policy-checking was disabled.
Meaning	When the local security device received an IKE Phase 2 message from the specified peer, it could not check for a policy because the id-mode was set to IP or policy-checking was disabled. If the id-mode is set to IP, the remote peer does not send the proxy ID payload when initiating a Phase 2 session. The proxy ID consists of the local end entity's IP address and netmask, protocol, and port number; and those for the remote end entity. Consequently, the local peer cannot use the information in the proxy ID to match the information in a local policy. If policy-checking is disabled for IKE traffic with the specified peer, the IKE module builds an security association (SA) without verifying the policy configuration.
Action	Verify if this is intended behavior. If not, set the id-mode to subnet (set ike id-mode subnet) and enable policy-checking (set ike policy-checking).

Message	IKE ⟨*gateway_ip*⟩ Phase 2: Received DH group ⟨*dh_group_actual*⟩ instead of expected group ⟨*dh_group_expected*⟩ for PFS.
Meaning	While executing a Diffie-Hellman exchange to refresh the cryptographic keys with Perfect Forward Secrecy (PFS) during Phase 2 Messages 1 and 2, the remote peer used a different Diffie-Hellman group than did the local security device. Consequently, the Phase 2 session has failed.
Action	Change the Phase 2 configuration on the local peer or request the admin for the remote peer to change that configuration so that both employ the same Diffie-Hellman group for PFS.

Message	IKE ⟨*gateway_ip*⟩: Added Phase 2 session tasks to the task list.
Meaning	The IKE module in the local security device has added the task to start a Phase 2 session with the specified peer to the task list for the Phase 1 SA being negotiated.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Added the initial contact task to the task list.
Meaning	The IKE module in the local security device has added to the task list the transmission of an initial contact notification message for the Phase 1 SA being negotiated. The device sends the initial contact notification message in either the fifth message (when the device is the initiator) or the sixth message (when it is the responder) of Main mode message exchanges. When using Aggressive mode, it sends the notification after the Phase 1 negotiations are completed.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: An SA (ID ⟨*new_sa_tunnel_id*⟩) with a higher weight replaced the SA (ID ⟨*policy_id*⟩) in policy ID ⟨*old_sa_tunnel_id*⟩.
Meaning	The monitoring device in a redundant VPN group, having established a security association (SA) with a targeted device with a higher weight (priority) than the currently active target, has failed over VPN traffic from tunnel tun_id_num2 to tunnel tun_id_num1. The IP address belongs to the targeted remote gateway to which the VPN traffic has been redirected. The policy ID number belongs to the policy that references this particular redundant VPN group.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Changed heartbeat interval to ⟨*heartbeat_interval*⟩.
Meaning	After detecting that the specified peer is using a shorter heartbeat interval than was originally configured locally, the local device has adjusted its rate of heartbeat transmission to that peer.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Dropped a packet from the peer because no policy permits it.
Meaning	The local security device has dropped a packet from the specified IKE peer because there was no policy referencing that peer.
Action	If you intend to establish a security association (SA) with the specified peer, verify that a policy permitting traffic via that peer exists and is positioned correctly in the policy list.

Message	IKE ⟨*gateway_ip*⟩: Heartbeats have been disabled because the peer is not sending them.
Meaning	The local security device has detected that the specified peer has not enabled IKE heartbeat transmission, so the local device has also disabled heartbeat transmission to that peer. Both ends of the IPSec tunnel must enable IKE heartbeat transmission for this feature to remain active. If the local peer detects that the remote peer has not enabled this feature, the local peer automatically ceases heartbeat transmission
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Heartbeats have been lost ⟨*count*⟩ times.
Meaning	The IKE heartbeats that the local security device sends to the specified peer through the IPSec tunnel have been lost the specified number of times.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Missing heartbeats have exceeded the threshold. All Phase 1 and 2 SAs have been removed.
Meaning	The number of IKE heartbeats that the local security device sends to the specified peer through the IPSec tunnel has exceeded the failure threshold. The security associations (SAs) for both Phase 1 and Phase 2 have been removed.
Action	Verify network connectivity to the peer gateway. Check if the peer has changed or deleted the tunnel configuration or rebooted the remote gateway device.

Message	IKE ⟨*gateway_ip*⟩: New SA (ID ⟨*new_sa_tunnel_id*⟩) is up. Switch policy ID ⟨*policy_id*⟩ from SA ⟨*old_sa_tunnel_id*⟩.
Meaning	The monitoring device in a redundant VPN group, having established a security association (SA) with a targeted device with a higher priority than the currently active target, has attempted to transfer VPN traffic from tunnel tun_id_num1 to tunnel tun_id_num2. The IP address belongs to the targeted remote gateway to which the VPN traffic has been redirected. The policy ID number belongs to the policy that references this particular redundant VPN group.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Phase 1 SA (my cookie:⟨*cookie_byte_1*⟩x) was removed due to a simultaneous rekey.
Meaning	The security device deleted the Phase 1 security association (SA) for the specified IKE gateway because both the local device and the remote peer attempted to rekey at the same time. Each Phase 1 SA is identified by one of a pair of cookies—one that the initiator provides, and one that the responder provides.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Phase 2 msg ID ⟨*message_id*⟩x: Received responder lifetime notification. (⟨*lifetime*⟩ sec/⟨*lifesize*⟩ KB)
Meaning	The local security device has received a responder lifetime notification message from the specified peer. The Phase 2 negotiation is identified by the specified message ID. The notification includes the Phase 2 security association (SA) lifetime in both seconds and kilobytes. The peers use the shortest lifetime defined.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Phase 2 negotiation request is already in the task list.
Meaning	The IKE module in the local security device, when attempting to add a Phase 2 negotiation task to its task list, discovered that the list already contained an identical task for the specified peer. When beginning Phase 1 negotiations, the security device adds the tasks that the Phase 1 security association (SA) must do to its Phase 1 task list. One such task is to perform Phase 2 negotiations. If Phase 1 negotiations progress too slowly, local traffic might initiate another Phase 2 SA request to the IKE module. If so, before the security device adds the Phase 2 task to its task list, it will discover that an identical task is already in the list and refrain from adding the duplicate.
Action	Check if the IKE Phase 1 negotiations with that peer have successfully completed.

Message	IKE ⟨*gateway_ip*⟩: Received a notification message for DOI ⟨*doi_number*⟩ ⟨*message_type*⟩ ⟨*message_text*⟩.
Meaning	The device has received one of the following notification messages in the specified Domain of Interpretation (DOI): Error Types INVALID-PAYLOAD-TYPE 1 DOI-NOT-SUPPORTED 2 SITUATION-NOT-SUPPORTED 3 INVALID-COOKIE 4 INVALID-MAJOR-VERSION 5 INVALID-MINOR-VERSION 6 INVALID-EXCHANGE-TYPE 7 INVALID-FLAGS 8 INVALID-MESSAGE-ID 9 INVALID-PROTOCOL-ID 10 INVALID-SPI 11 INVALID-TRANSFORM-ID 12 ATTRIBUTES-NOT-SUPPORTED 13 NO-PROPOSAL-CHOSEN 14 BAD-PROPOSAL-SYNTAX 15 PAYLOAD-MALFORMED 16 INVALID-KEY-INFORMATION 17 INVALID-ID-INFORMATION 18 INVALID-CERT-ENCODING 19 INVALID-CERTIFICATE 20 CERT-TYPE-UNSUPPORTED 21 INVALID-CERT-AUTHORITY 22 INVALID-HASH-INFORMATION 23 AUTHENTICATION-FAILED 24 INVALID-SIGNATURE 25 ADDRESS-NOTIFICATION 26 NOTIFY-SA-LIFETIME 27 CERTIFICATE-UNAVAILABLE 28 UNSUPPORTED-EXCHANGE-TYPE 29 UNEQUAL-PAYLOAD-LENGTHS 30 Status Types CONNECTED RESPONDER-LIFETIME REPLAY-STATUS INITIAL-CONTACT NOTIFY_NS_NHTB_INFORM You can find descriptions of error types 1 — 30 and status type 16384 in RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP) . For descriptions of status types 24576 — 24578, refer to RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP . Status type 40001 is a proprietary notify message. It indicates that during Phase 2 negotiations, an IKE peer transmitted the information necessary to support the next-hop tunnel binding (NHTB) feature.
Action	For the error notification messages, take action as appropriate for the error described. For the status notification messages, no action is necessary.

Message	IKE ⟨*gateway_ip*⟩: Received a TRNXTN_XCHG payload with type ⟨*payload_type*⟩.
Meaning	After Phase 1 negotiations are completed, the security device received a transaction exchange (TRNXTN_XCHG) packet with a number indicating one of the following TRNXTN_XCHG payload types: request, reply, set, ack.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Received initial contact notification and removed Phase 1 SAs.
Meaning	The local security device has received an initial contact notification message from a peer and removed all IKE Phase 1 or Phase 2 security associations (SAs) for that peer. Note: When the security device receives an initial contact notification message, it removes all Phase 1 and Phase 2 SAs. However, because the removal of Phase 1 and Phase 2 SAs occurs separately, the security device logs both removals separately.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Received initial contact notification and removed Phase 2 SAs.
Meaning	The local security device has received an initial contact notification message from a peer and removed all IKE Phase 1 or Phase 2 security associations (SAs) for that peer. Note: When the security device receives an initial contact notification message, it removes all Phase 1 and Phase 2 SAs. However, because the removal of Phase 1 and Phase 2 SAs occurs separately, the security device logs both removals separately.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Sent an initial contact notification message because of a bad SPI.
Meaning	In response to an invalid security parameters index (SPI) number in IPSec traffic from the specified peer, the local security device sent an initial contact notification message.
Action	Receiving a few messages of this kind during rekey is normal. However, if you receive a large number of these messages, check the security association (SA) status.

Message	IKE ⟨*gateway_ip*⟩: Sent initial contact notification to peer to use a new SA.
Meaning	The local security device has sent an initial contact notification message to the specified remote gateway. After rebooting, the local device sends an initial contact notification message when contacting a peer for the first time. The message informs the peer that the local device has no previous state with it and to delete any existing security associations (SAs).
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: The initial contact task is already in the task list.
Meaning	Before adding the initial contact task to the task list, the IKE module in the local security device noted that the task was already in the task list. This can occur if a pending task exists. The device sends the initial contact notification message after the Phase 1 negotiations are completed.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: User ⟨*user_name*⟩ has exceeded the configured share-limit of ⟨*share_limit*⟩.
Meaning	The configured share-limit is an integer specifying the number of users that can establish tunnels concurrently using partial IKE identities. The identified user attempted to use the configured IKE (identified by number), causing the number of users to exceed this value
Action	Increase the share-limit value for the IKE definition

Message	IKE ⟨*gateway_ip*⟩: XAuth login expired and was terminated for username ⟨*user_name*⟩ at ⟨*user_ip*⟩/⟨*IP address*⟩.
Meaning	The login operation timed out for the specified XAuth user before he or she successfully completed it. The first IP address (ip_addr1) is that of the remote gateway. The second IP address (ip_addr2) is that of the XAuth user. (On a NetScreen-Remote client, the second IP address is a virtual internal IP address.)
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: XAuth login failed for gateway ⟨*gateway_name*⟩, username ⟨*user_name*⟩, retry: ⟨*retry_count*⟩, timeout: ⟨*timeout*⟩.
Meaning	The security device passed or failed the login attempt by the specified XAuth user, or the user aborted the attempt. The number of retries indicates how many login attempts the XAuth user made. The timeout value only appears in the message for failed login attempts.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: XAuth login was aborted for gateway ⟨*gateway_name*⟩, username ⟨*user_name*⟩, retry: ⟨*retry_count*⟩.
Meaning	The security device passed or failed the login attempt by the specified XAuth user, or the user aborted the attempt. The number of retries indicates how many login attempts the XAuth user made. The timeout value only appears in the message for failed login attempts.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: XAuth login was passed for gateway ⟨*gateway_name*⟩, username ⟨*user_name*⟩, retry: ⟨*retry_count*⟩, Client IP Addr ⟨*client_ip*⟩, IPPool name: ⟨*ippool_name*⟩, Session-Timeout: ⟨*session_timeout*⟩s, Idle-Timeout: ⟨*idle_timeout*⟩s.
Meaning	The security device passed or failed the login attempt by the specified XAuth user, or the user aborted the attempt. The number of retries indicates how many login attempts the XAuth user made. The timeout value only appears in the message for failed login attempts.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: XAuth login was refreshed for username ⟨*user_name*⟩ at ⟨*user_ip*⟩/⟨*IP address*⟩.
Meaning	The security device refreshed the login for the specified XAuth user. The first IP address (ip_addr1) is that of the remote gateway. The second IP address (ip_addr2) is that of the XAuth user. (On a NetScreen-Remote client, the second IP address is a virtual internal IP address.)
Action	No recommended action

Message	IKE: Removed Phase 2 SAs after receiving a notification message.
Meaning	The local security device has received a notification message from a peer and removed all IKE Phase 2 security associations (SAs) for that peer. A notification to remove Phase 2 SAs can occur when the lifetime of a Phase 2 SA expires or when the peer manually deletes an SA before it expires. (To delete a specific SA, use the "clear sa id_number" CLI command. To delete all SAs, use the "clear ike all" command.)
Action	No recommended action

Message	IKE: User ⟨*user_name*⟩ with ID ⟨*user_id*⟩ requested a connection.
Meaning	The security device has received a connection request from the IKE user with the specified ID.
Action	No recommended action

Message	IKE: XAuth assign DNS ⟨*DNS ip address pointer*⟩.
Meaning	XAuth successfully assigned a new DNS name to an interface.
Action	No recommended action

Message	IKE: XAuth assign dns1 ⟨*DNS1 ip address*⟩ dns2 ⟨*DNS2 ip address*⟩ wins1 ⟨*wins1 ip address*⟩ wins2 ⟨*wins2 ip address*⟩.
Meaning	XAuth successfully assigned new IP addresses to DNS1, DNS2, WINS1, or WINS2. dns1 is the IP for the primary DNS server. dns2 is the IP for the secondary DNS server. wins1 is the IP for the primary WINS server. wins2 is the IP for the secondary WINS server.
Action	No recommended action

Message	IKE: XAuth assign prefix ⟨*prefix ip address pointer*⟩/⟨*prefix length*⟩ to interface ⟨*interface name*⟩ failed.
Meaning	There was a failed attempt by XAuth to assign a new prefix and prefix length to an interface.
Action	No recommended action

Message	IKE: XAuth assign prefix ⟨*prefix ip address pointer*⟩/⟨*prefix length*⟩ to interface ⟨*interface name*⟩.
Meaning	Action by XAuth assigned a new prefix and prefix length to an interface.
Action	No recommended action

Message	IKE: XAuth IP pool ⟨*pool name*⟩ not configured.
Meaning	The IP pool name returned by the XAuth Radius server is does not exist on the device.
Action	Ensure that the configuration is valid, specifically that the pool name specified in the Radius is the same as the pool name configured on the local equipment.

Message	IKE: XAuth no more IP addresses in IP pool ⟨*pool name*⟩.
Meaning	The XAuth IP address pool has been exhausted.
Action	Reduce the number of remote xauth connections or enlarge the IP pool.

Message	IKE < ⟨*gateway_ip*⟩ > Phase 1: IKE initiator has detected NAT in front of the local device.
Meaning	The device has detected Network Address Translation (NAT) between itself and the VPN tunnel.
Action	No recommended action

Message	IKE < ⟨*gateway_ip*⟩ > Phase 1: IKE initiator has detected NAT in front of the remote device.
Meaning	The device has detected Network Address Translation (NAT) between the VPN tunnel and the remote device.
Action	No recommended action

Message	IKE < ⟨*gateway_ip*⟩ > Phase 1: IKE responder has detected NAT in front of the local device.
Meaning	The device has detected Network Address Translation (NAT) between itself and the VPN tunnel.
Action	No recommended action

Message	IKE < ⟨*gateway_ip*⟩ > Phase 1: IKE responder has detected NAT in front of the remote device.
Meaning	The device has detected Network Address Translation (NAT) between the VPN tunnel and the remote device.
Action	No recommended action

Message	IKE⟨*gateway_ip*⟩ Phase 1: Cannot verify RSA signature.
Meaning	The local security device cannot verify the RSA or DSA signature sent by the specified IKE peer.
Action	Contact the remote admin to check if he or she sent a certificate with the public key matching the private key used to produce the signature.

Message	IKE⟨*gateway_ip*⟩ Phase 1: Negotiations have failed for user ⟨*user_name*⟩.
Meaning	The Phase 1 negotiations have failed for the specified IKE user.
Action	Check the event log and configuration on the local device and request the remote IKE user to check the configuration on the VPN client to determine the cause of the failure.

Message	IKE⟨*source_ip*⟩ ⟨*dest_ip*⟩ Phase 1: Initiated negotiations in ⟨*phase_1_mode*⟩ mode.
Meaning	The local security device has initiated Phase 1 negotiations in either Aggressive mode or Main mode from the outgoing interface to the specified peer.
Action	No recommended action

Message	IKE⟨*gateway_ip*⟩: XAuth login was terminated because the user logged in again. Previous gateway: ⟨*old_gateway_ip*⟩. Username: ⟨*user_name*⟩ at ⟨*user_ip*⟩/⟨*user_mask*⟩.
Meaning	The security device terminated one login instance for the specified XAuth user because the user logged in again from a gateway with a different IP address. The first IP address (ip_addr1) in the message is that of the current remote gateway. The second IP address is that of the previous remote gateway (ip_addr2). The third IP address is that of the XAuth user. (On a NetScreen-Remote client, the second IP address is a virtual internal IP address.)
Action	No recommended action

Message	Received an IKE packet on ⟨*interface_name*⟩ from ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dest_ip*⟩:⟨*dest_port*⟩/⟨*pak_len*⟩. Cookies: ⟨*init_cookie*⟩, ⟨*resp_cookie*⟩.
Meaning	The security device has received an IKE packet on the indicated interface from the specified source IP address and port number bound for the specified destination IP address and port number. The message also includes the cookies for the initiator (string1) and the responder (string2) involved in the IKE negotiation process. The security device logs this information if an admin has enabled such logging through the "set firewall log-self ike" command.
Action	No recommended action

Message

Rejected an IKE packet on ⟨*interface_name*⟩ from ⟨*src_ip*⟩:⟨*src_port*⟩ to ⟨*dest_ip*⟩:⟨*dest_port*⟩ with cookies ⟨*init_cookie*⟩ and ⟨*resp_cookie*⟩ because ⟨*reason*⟩⟨*msg_pad1*⟩⟨*msg_str*⟩.

Meaning

The security device rejected the IKE packet that arrived on the named interface from the specified source IP address and port number bound for the specified destination IP address and port number. The message also includes the cookies for the initiator (string1) and the responder (string2) involved in the IKE negotiation process. This message includes a reason why the security device rejected the packet. An explanation of each reason follows. Because of the large number of reasons that can appear in this message—each one requiring you to take a different action—each reason is immediately followed by its corresponding action: Meaning: The security device received an initial IKE Phase 1 packet from a source that was not one of its IKE peers. Action: If you suspect that the packet came from a source that should be an IKE peer, check the local VPN configuration, and contact the remote admin to check the VPN configuration there. Meaning: The security device did not accept any of the IKE Phase 1 or Phase 2 proposals that the specified IKE peer sent. Action: Check the local VPN configuration. Either change the local configuration to accept at least one of the remote peer's Phase 1 and Phase 2 proposals, or contact the remote peer's admin and arrange for the IKE configurations at both ends of the tunnel to use at least one mutually acceptable Phase 1 and Phase 2 proposal. Meaning: The security device received a packet from a source for which there was a gateway configuration; however, that gateway was not referenced in any VPN tunnel configuration. Action: Review the local VPN configurations to determine if the packet came from a legitimate peer. Also, contact the remote admin to check the VPN configuration at that end as well. Meaning: The security device received a packet that was either In cipher text (encrypted) when it expected it to be in clear text (unencrypted) or vice versa. Action: Ask the remote peer's admin to check his VPN configuration. If the configuration is valid, there might be a compatibility issue between the remote device and the local security device, possibly because the remote peer's VPN implementation does not conform to the RFCs. Meaning: The specified IKE peer used a different IKE ID payload type than what the security device expected. security supports the following four IKE ID types: IP address, such as 209.157.66.170 Fully qualified domain name (FQDN), such as www.juniper.net User's fully qualified domain name (U-FQDN), such as jsmith@juniper.net Abstract Syntax Notation, version 1, distinguished name (ASN1_DN), such as cn = ns100, ou = eng, o = juniper, l = santa clara, s = ca, c = us Action: Review the local VPN configuration. Either change the local configuration to match the IKE ID type sent, or contact the remote peer's admin and arrange for him to use an IKE ID payload type that is mutually acceptable to you both. Meaning: An IKE peer sent a different IKE ID payload than what the security device expected. Action: Review the local VPN configuration. Either change the local configuration to match the IKE ID payload sent, or contact the remote peer's admin and arrange for him to send an IKE ID payload that is mutually acceptable to you both. Meaning: Before Phase 1 negotiations were completed,

the specified IKE peer sent a packet with a message ID, which is only used during Phase 2 negotiations. Action: This can happen if the last Phase 1 packet that the remote peer sends does not reach the local security device. If this event occurred once, you can safely disregard this message. However, if this occurs repeatedly, investigate the problem locally, and contact the peer to investigate the problem at that end. When investigating, check for any reason why the security device might repeatedly drop packets, such as heavy network traffic or high CPU usage. Meaning: IKE Phase 1 negotiations were unsuccessful, possibly because the preshared keys were different. Action: Review the local configuration and ask the remote peer's admin to review his configuration. In particular, confirm that both ends of the tunnel are using the same preshared key. (Mismatched preshared keys are a common cause for the occurrence of this message.) Note that Group IKE IDs use a preshared key seed value that the security device at a central site combines with the remote peer's full IKE ID to generate a preshared key on the fly. For details, refer to volume 5 “VPNs”in the Concepts & Examples ScreenOS Reference Guide. Meaning: The hash payload for the IKE INFO, Quick mode (QM), or Transaction exchange mode was invalid. Negotiating entities use the hash payload to verify the integrity of the data. Action: The occurrence of this event might indicate a deliberate attack or a VPN implementation at the remote site that does not conform to IKE-related RFCs. If it is an attack, the security device has successfully deflected it by rejecting the packet and you need take no further action. If it is an implementation issue, contact the remote admin to discuss the situation. Meaning: Before the XAuth operation had completed, the specified IKE peer sent a Phase 2 packet. (XAuth must be finished before Phase 2 can start.) Action: This can happen if the last XAuth packet that the remote peer sends does not reach the local security device. If this event occurred once, you can safely disregard this message. However, if this occurs repeatedly, investigate the problem locally, and contact the peer to investigate the problem at that end. When investigating, check for any reason why the security device might repeatedly drop packets, such as heavy network traffic or high CPU usage. Alternatively, there be a compatibility issue between the remote device and the local security device, possibly because the remote peer's VPN implementation does not conform to the IKE-related RFCs or interprets the RFCs differently than Juniper Networks does. Meaning: The specified peer did not send a proxy ID during Phase 2 negotiations. Action: Ask the remote admin to check the configuration to ensure that there is a proxy ID for this VPN tunnel. Meaning: The specified peer sent a proxy ID during Phase 2 negotiations, but it did not match the proxy ID in the security association (SA) configuration. Action: Ensure that the proxy IDs at both the local and remote sites match exactly by checking the local VPN configuration and asking the remote admin to check the VPN configuration at that end. Meaning: A session from the same IKE peer was already in progress when the peer sent this packet during Phase 2 negotiations. Action: No recommended action Meaning: Although Perfect Forward Secrecy (PFS) was specified for Phase 2, the IKE peer did not send a Key Exchange (KE) payload to start

negotiations for a new key. Action: The occurrence of this event might indicate that the VPN implementation at the remote site that does not conform to IKE-related RFCs. If it is an implementation issue, contact the remote admin to discuss the situation. Meaning: The specified IKE peer sent one of the following IKE ID payload types, which Juniper Networks does not support. The ID payload content is followed by the ID type value—see RFC 2407: ipv4_addr_subnet, 4 ipv6_addr, 5 ipv6_addr_subnet, 6 ipv4_addr_range, 7 ipv6_addr_range, 8 der_asn1_gn, 10 key_id, 11 Action: Ask the remote admin to use one of the IKE ID types that Juniper Networks supports: IP address (ID type 1) Fully qualified domain name (2) User's fully qualified domain name (3) Abstract Syntax Notation, version 1, distinguished name (9) Meaning: The security device has a valid configuration for the remote IKE gateway and a VPN tunnel referencing that gateway. However, the tunnel is not referenced in a policy—for a policy-based VPN—or bound to a tunnel interface—for a route-based VPN. Consequently, the security device does not have a security association (SA) for this tunnel. Action: Check the configuration, and either reference the VPN tunnel in a policy or bind it to a tunnel interface for a policy-based VPN or a route-based VPN respectively. Meaning: The security device received a Phase 1 packet from a remote IKE user but was unable to find a configuration using the IKE ID that the user sent. The message includes the IKE ID type and value that the remote user sent: IP Address, 1 FQDN, 2 U-FQDN, 3 ASN1_DN, 9 Action: Check the configuration on the security device. If the local configuration is correct, instruct the remote user to change the IKE ID type and content that he sends. If the local configuration is incorrect, change the IKE ID type and content in the local configuration. (Note: If no IKE ID is specified in the configuration, the IP address becomes the default IKE ID. If this is the case, check that the IP address of the remote gateway matches the source IP address of the packet.) The security device logs messages with the following reasons only if an admin has enabled such logging through the "set firewall log-self ike" command: Meaning: The exchange mode—such as Main mode or Aggressive mode—requires a different packet format than what the security device received. Action: Contact the remote peer's admin and ask him to investigate the cause of this behavior. The peer used the correct exchange mode, but the packet was not in the required format. Meaning: The specified responder cookie that the security device received during Phase 1 or 2 did not match the responder cookie that the peer sent previously. Action: If this event occurred after resetting the local security device, the remote peer might still have been using a cookie pair that existed before the local device cleared it from its cache. If that is the case, you can safely disregard this message. If this is not the case, this message might indicate an attack from someone spoofing the source address of a legitimate IKE peer in an attempt to uncover a weakness in the ScreenOS firmware. If it is an attack, the security device has successfully deflected it by rejecting the packet and you need take no further action. If it is an implementation issue, contact the remote admin to discuss the situation. Meaning: The security device received a retransmitted packet from the specified source IP address. Action:

This message might appear because the remote peer was expecting a packet from the local security device that it never received. The peer might not have received a packet if it was lost in transit, dropped by the peer while processing it, or if there were heavy traffic conditions at either or both ends of the tunnel. If the local security device frequently receives retransmitted packets from the same address, consider the above possibilities during your investigation. Meaning: At least one required IKE payload was missing from the rejected packet. For information regarding the required payloads, refer to RFC 2407. Action: Ask the remote peer's admin to check his VPN configuration. If the configuration is valid, there might be a compatibility issue between the remote device and the local security device, possibly because the remote peer's VPN implementation does not conform to the IKE-related RFCs. Meaning: The remote entity sent a packet for one type of exchange mode after beginning the exchange with another type. Action: The occurrence of this event might indicate a deliberate attack or a VPN implementation at the remote site that does not conform to IKE-related RFCs. If it is an attack, the security device has successfully deflected it by rejecting the packet and you need take no further action. If it is an implementation issue, contact the remote admin to discuss the situation. Meaning: The specified IKE peer attempted to use the type of exchange mode (indicated by its type ID value) to perform Phase 1 or Phase 2 negotiations, but the local security device does not support it. Juniper Networks supports the following exchange mode types: Main mode (Phase 1 negotiations with identity protection); type ID value: 2 Aggressive mode (Phase 1 negotiations without identity protection); type ID value: 4 Informational mode (for Notify messages); type ID value: 5 Transaction Exchange (for XAuth); type ID value: 6 Quick mode (Phase 2 negotiations); type ID value: 32 Action: Contact the IKE peer and arrange for him to use one of the exchange modes that Juniper Networks supports. Meaning: The host at the specified IP address sent a packet using UDP port 500, but the IKE header format was invalid. For information regarding the proper ISAKMP header format, refer to RFC 2408. The packet length is provided to help locate the problem packet when troubleshooting. Action: The host at the source IP address might be using UDP port 500 for a service other than IKE. Contact the owner of that IP address and ask him to change his configuration. (You can determine the owner of an IP address by checking a service such as the American Registry of Internet Numbers (ARIN) in the United States and performing a Whois lookup on the address.) Meaning: The host at the specified IP address sent a cookie pair that was not previously in use. Action: If this event occurred after resetting the local security device, the remote peer might still have been using a cookie pair that existed before the local device cleared it from its cache. If that is the case, you can safely disregard this message. If this is not the case, this message might indicate an attack from someone spoofing the source address of a legitimate IKE peer in an attempt to uncover a weakness in the ScreenOS firmware. If it is an attack, the security device has successfully deflected it by rejecting the packet and you need take no further action. If it is an implementation issue, contact the remote

admin to discuss the situation. Meaning: The specified IKE peer sent a packet containing a malformed payload for one of the following types (for information on ISAKMP payload formats, refer to RCF 2408): Security Association (SA) — 1 Proposal (P) — 2 Transform (T) — 3 Key Exchange (KE) — 4 Identification (ID) — 5 Certificate (CERT) — 6 Certificate Request (CR) — 7 Hash (HASH) — 8 Signature (SIG) — 9 Nonce (NONCE) — 10 Notification (N) — 11 Delete (D) — 12 Vendor ID (VID) — 13 Action: The occurrence of this event might indicate a deliberate attack or a VPN implementation at the remote site that does not conform to IKE-related RFCs. If it is an attack, the security device has successfully deflected it by rejecting the packet and you need take no further action. If it is an implementation issue, contact the remote admin to discuss the situation. Meaning: The security device encountered an error when processing one of the following payload types: Security Association (SA) — 1 Proposal (P) — 2 Transform (T) — 3 Key Exchange (KE) — 4 Identification (ID) — 5 Certificate (CERT) — 6 Certificate Request (CR) — 7 Hash (HASH) — 8 Signature (SIG) — 9 Nonce (NONCE) — 10 Notification (N) — 11 Delete (D) — 12 Vendor ID (VID) — 13 Action: First, check memory usage. If it is unusually high, this type of processing error might occur. If memory usage does not appear to be the problem, then it might be that the payload type was incompatible and that the VPN implementation at the remote site that does not conform to IKE-related RFCs. Meaning: The specified IKE peer erroneously sent one of the following notify messages in clear text. Note that the notify message type is followed by its ID value. Error Types INVALID-PAYLOAD-TYPE 1 DOI-NOT-SUPPORTED 2 SITUATION-NOT-SUPPORTED 3 INVALID-COOKIE 4 INVALID-MAJOR-VERSION 5 INVALID-MINOR-VERSION 6 INVALID-EXCHANGE-TYPE 7 INVALID-FLAGS 8 INVALID-MESSAGE-ID 9 INVALID-PROTOCOL-ID 10 INVALID-SPI 11 INVALID-TRANSFORM-ID 12 ATTRIBUTES-NOT-SUPPORTED 13 NO-PROPOSAL-CHOSEN 14 BAD-PROPOSAL-SYNTAX 15 PAYLOAD-MALFORMED 16 INVALID-KEY-INFORMATION 17 INVALID-ID-INFORMATION 18 INVALID-CERT-ENCODING 19 INVALID-CERTIFICATE 20 CERT-TYPE-UNSUPPORTED 21 INVALID-CERT-AUTHORITY 22 INVALID-HASH-INFORMATION 23 AUTHENTICATION-FAILED 24 INVALID-SIGNATURE 25 ADDRESS-NOTIFICATION 26 NOTIFY-SA-LIFETIME 27 CERTIFICATE-UNAVAILABLE 28 UNSUPPORTED-EXCHANGE-TYPE 29 UNEQUAL-PAYLOAD-LENGTHS Status Types CONNECTED RESPONDER-LIFETIME REPLAY-STATUS INITIAL-CONTACT NOTIFY_NS_NHTB_INFORM You can find descriptions of error types 1 — 30 and status type 16384 in RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP) . For descriptions of status types 24576 — 24578, refer to RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP . Status type 40001 is a proprietary notify message. It indicates that during Phase 2 negotiations, an IKE peer transmitted the information necessary to support the next-hop tunnel binding (NHTB) feature. Action: Ask the remote peer's admin to check his VPN configuration. If the configuration is valid, there might be a compatibility issue between the remote device and the local security device, possibly

	because the remote peer's VPN implementation does not conform to the RFCs. Meaning: The security device encountered an error when sending a reply to the socket. Action: Because this message typically results from a network or routing problem, check network connectivity and route tables. Meaning: The host at the specified IP address sent an IKE packet whose stated length did not match its actual length. Action: The packet length stated in the header and its actual length might have been in conflict when the remote host initially created it, or it might have been modified in transit. If this event occurred only once and there are no further packet-length discrepancies in subsequent packets from that IP address, you can safely disregard this message. If the problem persists, ask the peer to resend the packet and use a sniffer at the remote site—and, if possible, at other points along the data path—to determine where the stated packet length diverges from the actual packet length. Meaning: The local security device detected a network address translation (NAT) device in the data path during IKE negotiations; however, the remote peer did not shift (or “float”) the UDP port number from 500 to 4500 as required to perform NAT-Traversal (NAT-T) as specified in draft-ietf-ipsec-nat-t-ike-02.txt . Action: Gather information by doing the following procedure: set console dbuf clear dbuf debug ike detail Attempt to make another VPN tunnel to the remote peer. undebug all get dbuf stream all tftp ip_addr filename1 get tech-support tftp ip_addr filename2 Report your case to Juniper Networks technical support and include the two files: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.) Meaning: The local security device received an IKE packet with a UDP port number that shifted (or “floated”) from 500 to 4500, as required to support draft-ietf-ipsec-nat-t-ike-02.txt . However, the local device did not receive the vendor ID payload from the remote peer stating that it supports NAT-T as specified in draft-ietf-ipsec-nat-t-ike-02.txt , so the use of a floated port number from the peer was unexpected. UDP port 4500 is the shifted (or “floated”) port number that NAT-T uses to avoid inadvertent processing by intermediary IKE/IPSec-aware NAT devices. Action: Gather information by doing the following procedure: set console dbuf clear dbuf debug ike detail Attempt to make another VPN tunnel to the remote peer. undebug all get dbuf stream all tftp ip_addr filename1 get tech-support tftp ip_addr filename2 Report your case to Juniper Networks technical support and include the two files: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). Note: You must be a registered Juniper Networks customer.
Action	See Meaning.

Message	A Phase 2 packet arrived while XAuth was still pending
Meaning	This tunnel requires XAuth after the Phase 1 exchange but before the phase 2 exchange. An IKE Phase 2 message was received but the XAuth had not yet passed and the message was dropped silently. This might be an implementation compatible issue.
Action	Try to restart tunnel negotiation by executing the "clear ike-cookie all" command and sending trigger traffic. You might also try different setting for IAS, DPD, and so on.

Message	A required payload was missing
Meaning	All the required payloads in the packet from the peer are not present. Either the peer is not functioning properly or this might be an attack from a random device.
Action	Verify the configuration on the peer device.

Message	an initial Phase 1 packet arrived from an unrecognized peer gateway
Meaning	When configuring an IPSec tunnel to the specified remote gateway, which has a dynamically assigned IP address, an admin specified a preshared key and selected Main mode for the Phase 1 negotiations. Authentication via preshared key is not allowed when Main mode is used with a peer at a dynamically assigned IP address.
Action	Reconfigure the VPN using a certificate to authenticate the remote party, or select Aggressive mode for use with preshared key authentication.

Message	An unencrypted packet unexpectedly arrived
Meaning	An unexpected unencrypted packet arrived.
Action	Verify the IKE protocol implementation of the remote device.

Message	An unexpected encrypted packet arrived
Meaning	An unexpected encrypted packet arrived.
Action	Verify the IKE protocol implementation of the remote device.

Message	IKE DPD configuration changed, ⟨*configure_item_name*⟩
Meaning	An admin changed a DPD configuration item, identified by the string value.
Action	No recommended action

Message	IKE DPD found peer at ⟨*peer IP*⟩ not responding.
Meaning	The local device detected a peer device that did not send a R-U-THERE-ACK message in response to R-U-THERE messages sent by the local device. The device sends an R-U-THERE request if and only if it has not received any traffic from the peer during a specified DPD interval. If a DPD-enabled device receives traffic on a tunnel, it resets its R-U-THERE counter for that tunnel, thus starting a new interval. If the device receives an R-U-THERE-ACK from the peer during this interval, it considers the peer alive. If the device does not receive an R-U-THERE-ACK response during the interval, it considers the peer dead.
Action	No recommended action

Message	No VPN tunnel references the gateway
Meaning	The packet was dropped because the remote gateway is not used in any VPN tunnel configurations.
Action	Verify the VPN configuration.

Message	Phase 1 negotiations failed. (The preshared keys might not match.)
Meaning	The configured preshared key does not match the preshared key configured in the peer device.
Action	Ensure that preshared keys match.

Message	Phase-1: no user configuration was found for the received IKE ID type:
Meaning	ScreenOS did not find a user configuration based on the Phase 1 ID payload received from the remote device.
Action	Verify that the local-side user configuration and remote-side phase 1 ID payload match.

Message	ScreenOS does not support the ID payload type:
Meaning	The local device does not support the ID payload received from the remote device.
Action	Make sure the remote device is configured to send an ID payload supported by the local device, which includes IP address, domain name, email address, and distinguish name.

Message	The exchange modes (main or aggressive) do not match
Meaning	The exchange mode is not the same as the one used by the peer.
Action	Ensure that the configuration on this device is consistent with the configuration on the peer device.

Message	The format used did not match the exchange mode indicated:
Meaning	The packet is not the first IKE message and the system cannot locate the phase 1 session for the packet.
Action	Check the system log for a possible attack.

Message	The IKE INFO exchange mode hash payload was invalid
Meaning	The information exchange mode hash payload sent by the peer is not what was expected.
Action	Verify the configuration on the peer device.

Message	The IKE packet length was inconsistent
Meaning	An IKE Phase 1 or Phase 2 message was received, but the actual total length of all payloads inside the message is not consistent with the announced total length for the message. This might be an implementation compatible issue.
Action	Try different setting to determine if there is any difference.

Message	The IKE packet unexpectedly had a floated port number
Meaning	Received floated IKE packets but NAT Traversal is not enabled on the IKE gateway.
Action	Verify the IKE configuration.

Message	The IKE packet unexpectedly had a port number that was not floated.
Meaning	This is a not a floated IKE packet but port floating has been completed.
Action	Restart IKE negotiation by clearing the IKE cookie.

Message	The IKE QM exchange mode hash payload was invalid
Meaning	An IKE Phase 2 quick mode message was received but failed to pass the message authentication check. This might be an implementation compatible issue.
Action	Try different phase 2 proposal settings. You might also try different settings for the phase 1 security association (SA) proposal, Diffie-Hellman exchange, transform, Perfect Forward Secrecy (PFS), and so on.

Message	The IKE Transaction exchange mode hash payload was invalid
Meaning	The IKE Transaction exchange mode hash payload sent by the peer is not what was expected.
Action	Verify the configuration on the peer device.

Message	The notify message was in clear text:
Meaning	An unprotected Notify payload has been received and rejected.
Action	Verify the IKE implementation on the remote device.

Message	The peer did not send a proxy ID
Meaning	An IKE Phase 2 quick mode message was received but contained either the wrong proxy ID, or no proxy ID (local and remote subnets protected by the tunnel).
Action	Verify proxy ID (local and remote subnets) setting for this tunnel and try again.

Message	The peer sent a duplicate message
Meaning	The peer sent a duplicate message.
Action	Verify the IKE protocol implementation of the remote device.

Message	The peer sent a malformed payload:
Meaning	An IKE Phase 1 or Phase 2 message was received, but there is a problem with at least one security association (SA) payload for proposals or transforms within it. The actual length of the payload might differ from the announced length, or the payload ID might be incorrect. This might be an implementation compatibility issue.
Action	Try a different ID, SA proposal, or transform setting.

Message	The peer sent a nonexistent cookie pair:
Meaning	An IKE Phase 2 message was received, but there is no corresponding phase 1 security association (SA) for this message. The system cannot determine the phase 1 SA from the initiator and responder cookies of the message. The local-side device probably failed and was restarted. There are currently no SAs for the local side but there are some SAs for the remote side.
Action	Try to negotiate a new phase 1 SA for this tunnel from the remote side. For example, from the remote side, execute the "clear ike-cookie all" command and trigger the negotiation by sending some traffic.

Message	The peer sent a packet with a message ID before Phase 1 authentication was done
Meaning	The peer sent a packet with a message ID before Phase 1 authentication was completed.
Action	Verify the IKE protocol implementation of the remote device.

Message	The peer sent a proxy ID that did not match the one in the SA config
Meaning	An IKE Phase 2 quick mode message was received and a corresponding Phase 1 security association (SA) was found, but the proxy ID (local and remote subnets protected by this tunnel) within the message was not consistent with the proxy ID setting for this tunnel's configuration.
Action	Verify the proxy ID (local and remote subnets) setting for this tunnel and try again.

Message	The peer sent the incorrect IKE ID payload type:
Meaning	The packet was dropped due to an incorrect IKE ID payload type.
Action	Verify the IKE gateway configuration.

Message	The peer sent the incorrect IKE ID payload:
Meaning	The packet was dropped due to an incorrect IKE ID payload value.
Action	Verify the VPN configuration.

Message	The peer used an invalid IKE header format.
Meaning	The IKE header sent by the peer contains either a mismatch in the supported versions, unexpected cookie values, or unexpected mode values.
Action	Verify the configuration on the peer device.

Message	The peer used an unsupported exchange mode:
Meaning	The Exchange mode used by the peer is not one of the expected values, which must be main, aggressive, quick, info, or transaction.
Action	Verify the configuration on the peer device.

Message	The specified responder cookie does not exist
Meaning	The system cannot locate the Phase 1 session for the packet and the responder cookie is not zero.
Action	Restart IKE negotiation by clearing the IKE cookie on the peer.

Message	The VPN does not have an application SA configured
Meaning	The local device cannot find the IKE Phase 2 security association (SA) configuration based on the quick mode ID payloads sent by the remote device.
Action	Verify VPN policy or VPN proxy ID configuration.

Message	There was a preexisting session from the same peer
Meaning	The local device gave up quick negotiation because the remote device had initiated a quick mode negotiation at the same time.
Action	No recommended action.

Message	There was an error when processing the payload
Meaning	IKE payload processing failed.
Action	Verify the configuration.

Message	There was an error when sending a reply to the socket
Meaning	IKE module failed to send an IKE reply message.
Action	Enable flow debug to see why the packet send operation failed.

Message	There was no KE payload for PFS
Meaning	The local device did not receive the Key Exchange (KE) payload required by the configured Perfect Forward Secrecy (PFS).
Action	Verify that the remote device is also configured for PFS.

Message	There were no acceptable Phase 1 proposals
Meaning	None of the Phase 1 proposal(s) sent by the remote device has been chosen.
Action	Check IKE phase 1 configuration of both devices. At least one proposal should match.

Message	There were no acceptable Phase 2 proposals.
Meaning	The specified negotiations to the identified IKE failed.
Action	Examine the local log and VPN configuration, and request the remote IKE user to examine the configuration on their VPN client for possible causes.

Chapter 28
IKE V2

The following messages relate to the Internet Key Exchange (IKE) protocol, one of the three main components of IPSec-the other two are the Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols. IKE provides a secure means for the distribution and maintenance of cryptographic keys and the negotiation of the parameters constituting a secure communications channel.

Critical (00000)

Message	Attack alarm: IKE first message DoS attack on interface ⟨*if_name*⟩ from source IP ⟨*src_ip*⟩.
Meaning	An IKE V2 DoS attack packet was received.
Action	Check how the IKE V2 stateless cookie threshold was configured to confirm whether it's a DoS attacked packet.

Notification (00017)

Message	Gateway ⟨*gateway_name*⟩ at ⟨*gateway_ip*⟩ in IKE V2 with ID ⟨*peer_id*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin has added or modified the settings for, or deleted the specified remote IKE gateway. The peer IKE ID is the expected identification of the peer for authentication purposes. ScreenOS supports four types of IKE ID: IP address, domain name, fully qualified domain name (FQDN), and distinguished name (DN). DN is a name used to identify an entry in the Open Systems Interconnection (OSI) Directory; in a certificate, it is used as the primary name to uniquely identify the subject. The IKE ID is optionally configurable. If configured, the peer must send the configured ID for authentication to succeed. If not configured, the implied (default) IDs are assumed. For the preshared-key authentication method, the default ID is the peer's IP address; for RSA signature authentication, the default ID is whatever is specified in the "Alternative Name" field in the certificate. The alternative name can be either IP address, domain name, or FQDN.
Action	No recommended action

Information (00536)

Message	IKE ⟨*gateway_ip*⟩ IKESA: Completed for user ⟨*user_name*⟩.
Meaning	The security device and the specified remote IKE user have successfully completed IKE security association (SA) negotiations.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ CHILD SA with ⟨*exch_type*⟩: Completed negotiations with SPI ⟨*spi*⟩x, tunnel ID ⟨*tunnel_id*⟩, and lifetime ⟨*lifetime*⟩ seconds/⟨*lifesize*⟩ KB.
Meaning	The local security device has successfully negotiated a CHILD security association (SA) session with the specified peer. The session consists of the specified attributes.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ CHILD SA with ⟨*exch_type*⟩: Initiated negotiations.
Meaning	The local security device has sent the initial message for IKE CHILD security association (SA) negotiations to the specified peer.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ IKESA : Completed IKESA negotiations with ⟨*exch_type*⟩.
Meaning	The security device and the specified remote gateway have successfully completed IKE security association (SA) negotiations using the displayed exchange type.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ IKESA: Responder starts negotiations.
Meaning	The remote peer at the specified IP address has initiated IKE security association (SA) negotiations, and the local security device has begun its response.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩ IKEV2 packet: Retransmission limit has been reached.
Meaning	The local security device has reached the retransmission limit (10 failed attempts) during negotiations with the specified remote peer because the local device has not received a response. Note: If the local device continues receiving outbound traffic for the remote peer after the first 10 failed attempts, it makes another 10 attempts, and continues to do so until it either succeeds at contacting the remote gateway or it no longer receives traffic bound for that gateway.
Action	Verify network connectivity to the peer gateway. Request the remote gateway admin to consult the log to determine if the connection requests reached it and, if so, why the device did not respond.

Message	IKE ⟨*gateway_ip*⟩ ⟨*sa_type*⟩: Received DH group ⟨*dh_group_actual*⟩ instead of expected group ⟨*dh_group_expected*⟩.
Meaning	Diffie-Hellman group mismatch between security association (SA) proposal and Key Exchange (KE).
Action	Change configuration on the local peer or request the admin for the remote peer to change that configuration so that both employ the same Diffie-Hellman group.

Message	IKE ⟨*gateway_ip*⟩: IKE SA (my cookie:⟨*cookie_byte_1*⟩x) was removed due to a simultaneous rekey.
Meaning	The security device deleted the IKE security association (SA) for the specified IKE gateway because both the local device and the remote peer attempted to rekey at the same time. Each IKE SA is identified by one of a pair of cookies; one that the initiator provides, and one that the responder provides.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: EAP login failed for user ⟨*user_name*⟩ in ⟨*role*⟩.
Meaning	The security device failed the login attempt by the specified EAP user.
Action	Check that the user name and password are configured the same in the supplicant and EAP server.

Message	IKE ⟨*gateway_ip*⟩: EAP login was aborted for user ⟨*user_name*⟩ in ⟨*role*⟩.
Meaning	The security device aborted the login attempt by the specified EAP user.
Action	Check the EAP server's configuration.

Message	IKE ⟨*gateway_ip*⟩: EAP login was passed for user ⟨*user_name*⟩ in ⟨*role*⟩.
Meaning	The security device passed the login attempt by the specified EAP user.
Action	No recommended action

Message	IKE ⟨*gateway_ip*⟩: Received initial contact notification and removed other IKESAs and all their CHILD SAs.
Meaning	The local security device has received an initial contact notification message from a peer and removed all IKE and CHILD security associations (SAs) for that peer. Note: When the security device receives an initial contact notification message, it removes all IKE and CHILD SAs. However, because the removal of IKE and CHILD SAs occurs separately, the security device logs both removals separately.
Action	No recommended action

Message	IKE V2 ⟨*gateway_ip*⟩ : Cannot verify RSA signature.
Meaning	The local security device cannot verify the RSA or DSA signature sent by the specified IKE peer.
Action	Contact the remote admin to check if the admin sent a certificate with the public key matching the private key used to produce the signature.

Message	IKE V2 ⟨*gateway_ip*⟩ : Cannot verify DSA signature.
Meaning	The local security device cannot verify the RSA or DSA signature sent by the specified IKE peer.
Action	Contact the remote admin to check if the admin sent a certificate with the public key matching the private key used to produce the signature.

Message	IKE v2 ⟨*gateway_ip*⟩ : No private key exists to sign packets.
Meaning	The private key needed to create an RSA or DSA signature to authenticate packets destined for the specified IKE peer does not exist. This situation can arise if the following conditions are met: (1) If the local configuration for the remote gateway specifies a local certificate that an admin later removes (2) If there are no local certificates in the certificate store and no local certificate is specified in the remote gateway configuration
Action	Obtain and load a certificate for use in authenticating IKE packets.

Message	IKE V2 ⟨*gateway_ip*⟩ : Received an incorrect public key authentication method.
Meaning	In the first and second sa_init messages, the IKE participants agreed to use a preshared key for packet authentication. Then, in the third or forth message, the remote peer sent a auth payload, which requires the local device to use a public key (not a preshared key) to authenticate the packet. The security device, however, does not attempt to authenticate the packet; it drops the packet.
Action	Check if the remote peer is a legitimate IKE peer. If so, contact the remote admin to check if that device has malfunctioned. If not, this might be an ineffectual attack in which the attacker is attempting to force the security device to consume bandwidth while trying to verify bogus signature payloads.

Message	IKE V2 ⟨*gateway_ip*⟩ IKESA: Cert received has a different FQDN SubAltName than expected.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject alternative name (SubAltName) than was configured as the IKE ID on the local device. The SubAltName is an alternative name for the subject of a certificate. Juniper Networks supports the following kinds: IP address, such as 209.157.66.170 Fully qualified domain name (FQDN), such as www.juniper.net User's fully qualified domain name (UFQDN), such as jsmith@juniper.net
Action	Recommend the peer use a certificate with the expected SubAltName or change the IKE ID in the local VPN configuration to match that of the certificate.

Message	IKE V2 ⟨*gateway_ip*⟩ IKESA: Cert received has a different IP address SubAltName than expected.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject alternative name (SubAltName) than was configured as the IKE ID on the local device. The SubAltName is an alternative name for the subject of a certificate. Juniper Networks supports the following kinds: IP address, such as 209.157.66.170 Fully qualified domain name (FQDN), such as www.juniper.net User's fully qualified domain name (UFQDN), such as jsmith@juniper.net
Action	Recommend the peer use a certificate with the expected SubAltName or change the IKE ID in the local VPN configuration to match that of the certificate.

Message	IKE V2 ⟨*gateway_ip*⟩ IKESA: Cert received has a different UFQDN SubAltName than expected.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject alternative name (SubAltName) than was configured as the IKE ID on the local device. The SubAltName is an alternative name for the subject of a certificate. Juniper Networks supports the following kinds: IP address, such as 209.157.66.170 Fully qualified domain name (FQDN), such as www.juniper.net User's fully qualified domain name (UFQDN), such as jsmith@juniper.net
Action	Recommend the peer use a certificate with the expected SubAltName or change the IKE ID in the local VPN configuration to match that of the certificate.

Message	IKE V2 ⟨*gateway_ip*⟩ IKESA: Cert received has a subject name that does not match the ID payload.
Meaning	The local security device received a certificate from the specified IKE peer that contained a different subject than the IKE ID sent by the peer. The subject of a certificate can be a distinguished name (DN) composed of a concatenation of the common name elements listed in the request submitted for that certificate. The DN is the identity of the certificate holder.
Action	Advise the peer to change the IKE ID in its VPN configuration to match that of the certificate, or use a certificate with a subject name that matches the IKE ID configured for the VPN.

Message	IKE V2 ⟨*gateway_ip*⟩: Negotiations have failed for user ⟨*user_name*⟩.
Meaning	The negotiations have failed for the specified IKE user.
Action	Check the event log and configuration on the local device and request the remote IKE user to check the configuration on the VPN client to determine the cause of the failure.

Message	IKE V2 ⟨*gateway_ip*⟩: Received a notification message for ⟨*message_type*⟩ ⟨*message_text*⟩.
Meaning	The device has received one of the following notification messages : NOTIFY_MSG_UNSUPPORTED_CRITICAL_PAYLOAD 1 NOTIFY_MSG_INVALID_IKE_SPI 4 NOTIFY_MSG_INVALID_MAJOR_VERSION 5 NOTIFY_MSG_INVALID_SYNTAX 7 NOTIFY_MSG_INVALID_MESSAGE_ID 9 NOTIFY_MSG_INVALID_SPI 11 NOTIFY_MSG_NO_PROPOSAL_CHOSEN 14 NOTIFY_MSG_INVALID_KE_PAYLOAD 17 NOTIFY_MSG_AUTHENTICATION_FAILED 24 NOTIFY_MSG_SINGLE_PAIR_REQUIRED 34 NOTIFY_MSG_NO_ADDITIONAL_SAS 35 NOTIFY_MSG_INTERNAL_ADDRESS_FAILURE 36 NOTIFY_MSG_FAILED_CP_REQUIRED 37 NOTIFY_MSG_TS_UNACCEPTABLE 38 NOTIFY_MSG_INVALID_SELECTORS 39 NOTIFY_MSG_MAX_ERR_CODE 16383 NOTIFY_MSG_INITIAL_CONTACT 16384 NOTIFY_MSG_SET_WINDOW_SIZE 16385 NOTIFY_MSG_ADDITIONAL_TS_POSSIBLE 16386 NOTIFY_MSG_IPCOMP_SUPPORTED 16387 NOTIFY_MSG_NAT_DETECTION_SOURCE_IP 16388 NOTIFY_MSG_NAT_DETECTION_DESTINATION_IP 16389 NOTIFY_MSG_COOKIE 16390 NOTIFY_MSG_USE_TRANSPORT_MODE 16391 NOTIFY_MSG_HTTP_CERT_LOOKUP_SUPPORTED 16392 NOTIFY_MSG_REKEY_SA 16393 NOTIFY_MSG_ESP_TFC_PADDING_NOT_SUPPORTED 16394 NOTIFY_MSG_NON_FIRST_FRAGMENTS_ALSO 16395 You can find descriptions of error and status type in RFC 4306, Internet Key Exchange (IKEv2) Protocol.
Action	For the error notification messages, take action as appropriate for the error described. For the status notification messages, no action is necessary.

Message	IKE V2 ⟨*gateway_ip*⟩:negotiating ⟨*exch_type*⟩ packet in status ⟨*status*⟩ has failed with ⟨*err_string*⟩.
Meaning	The session initiated by the local security device to the specified peer has failed.
Action	Check the event log on the local device and request the remote admin to consult the event log on the remote device to determine the cause of the failure.

Message	IKE: Removed child SAs after receiving a notification message: ⟨*notify_type*⟩.
Meaning	The local security device has received a notification message from a peer and removed all CHILD security associations (SAs) for that peer. A notification to remove CHILD SAs can occur when the lifetime of a CHILD SA expires or when the peer manually deletes an SA before it expires. (To delete a specific SA, use the "clear sa id_number" CLI command. To delete all SAs, use the "clear ike all" command.)
Action	No recommended action

Message	IKE⟨*source_ip*⟩ ⟨*dest_ip*⟩ IKESA: Initiated negotiations.
Meaning	The local security device has initiated IKE security association (SA) negotiations from the outgoing interface to the specified peer.
Action	No recommended action

Message	IKESA negotiations failed. (The preshared keys might not match.)
Meaning	The configured preshared key does not match the preshared key configured in the peer device.
Action	Ensure that preshared keys match.

Message	An initial packet arrived from an unrecognized peer gateway
Meaning	When the first IKE V2 packet was received, the matched remote gateway from the IPSec configuration was not found.
Action	Check the IKE gateway's configuration.

Message	ID MATCH: no user configuration was found for the received IKE ID type:
Meaning	ScreenOS did not find a user configuration based on the ID payload received from the remote device.
Action	Verify that the local-side user configuration and remote-side IKE ID payload match.

Message	The exchange type does not match
Meaning	The exchange type in the packet received is not one expected during IKE security association (SA) negotiation.
Action	Verify the configuration on the peer device.

Message	The peer sent a nonexistent cookie pair:
Meaning	An IKE message was received, but there is no corresponding security association (SA) for this message. The system cannot determine the SA from the initiator and responder cookies of the message.
Action	No recommended action.

Message	The peer sent a packet with ETV2_CREATE_CHILD_SA before IKESA authentication was done
Meaning	The peer sent a packet with ETV2_CREATE_CHILD_SA before IKE security association (SA) authentication was completed.
Action	Verify the IKE protocol implementation of the remote device.

Message	The peer sent a TS that did not match the one in the SA config
Meaning	The Traffic Sector (TS) payload (local and remote subnets protected by this tunnel) within the message was not consistent with the TS setting for this VPN configuration.
Action	Verify the proxy ID (local and remote subnets) setting for this tunnel and try again.

Message	The peer sent an unsupported or unexpected exchange type after IKESA negotiation finished :
Meaning	The exchange type in the packet received is unsupported .
Action	Verify the configuration on the peer device.

Chapter 29

Interface

The following messages relate to interface configurations.

Critical (00090)

Message	Failover to secondary untrust interface occurred.
Meaning	The primary interface in a redundant interface failed, and the secondary interface took over transmission of traffic. (The redundant interface is bound to the Untrust zone.)
Action	Check the primary physical interface for disconnection.

Message	Recovery to primary untrust interface occurred.
Meaning	The primary interface in a redundant interface returned to operation, and is now performing transmission of traffic. (The redundant interface is bound to the Untrust zone.)
Action	No recommended action.

Critical (00091)

Message	L3 backup failover from interface ⟨*pri_if_name*⟩ to interface ⟨*bak_if_name*⟩.
Meaning	A L3 backup failover occurred from the identified primary_interface to the specified backup interface.
Action	No recommended action.

Message	L3 backup recover from interface ⟨*bak_if_name*⟩ to interface ⟨*pri_if_name*⟩.
Meaning	A L3 backup failover occurred from the specified backup interface to the primary interface.
Action	No recommended action.

Notification

Message	Interface ⟨*interface_name*⟩ switching to annexL del test mode.
Meaning	The ADSL interface has changed to annexL delete test mode.
Action	No recommended action.

Notification

Message	Interface ⟨*interface_name*⟩ switching to annexL mode.
Meaning	The ADSL interface has changed to annexL mode.
Action	No recommended action.

Notification

Message	Interface ⟨*interface_name*⟩ switching to ITU G.992.3 annexM mode.
Meaning	The ADSL interface has changed to ITU G.992.3 annexM mode.
Action	No recommended action.

Notification

Message	Interface ⟨*interface_name*⟩ switching to ITU G.992.5 annexM mode.
Meaning	The ADSL interface has changed to ITU G.992.5 annexM mode.
Action	No recommended action.

Notification (00009)

Message	802.1Q VLAN tag ⟨*interface_tag*⟩ has been created.
Meaning	An admin has created the specified VLAN tag.
Action	No recommended action.

Message	802.1Q VLAN tag ⟨*interface_tag*⟩ has been removed.
Meaning	An admin has deleted the specified VLAN tag.
Action	No recommended action.

Message	Activation delay for interface ⟨*pri_if_name*⟩ has been changed to ⟨*activation_delay*⟩.
Meaning	The primary interface activation delay is changed.
Action	No recommended action.

Message	Admin status for interface ⟨*interface_name*⟩ has been changed to ⟨*value*⟩.
Meaning	The admin status for the identified interface is changed.
Action	No recommended action.

Message	Auto-failover for interface ⟨*pri_if_name*⟩ has been changed to ⟨*auto_state*⟩.
Meaning	The primary interface auto-failover is changed.
Action	No recommended action.

Message	Deactivation delay for interface ⟨*pri_if_name*⟩ has been changed to ⟨*deactivation_delay*⟩.
Meaning	The primary interface deactivation delay is changed.
Action	No recommended action.

Message	DNS proxy was ⟨*new_status*⟩ on interface ⟨*interface_name*⟩.
Meaning	An admin enabled or disabled Domain Name Service (DNS) proxy on the named interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ 802.1Q tag has been changed to ⟨*interface_tag*⟩ ⟨*changed_from*⟩.
Meaning	An admin has changed the 802.1Q VLAN tag for the specified interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ 802.1Q tag has been removed ⟨*changed_from*⟩.
Meaning	An admin deleted the specified interface and 802.1Q VLAN tag.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ 802.1Q VLAN trunking has been turned OFF ⟨*changed_from*⟩.
Meaning	An admin disabled VLAN trunking for the specified interface. A trunk port allows a switch to bundle traffic from several VLANs through a single physical interface, sorting the various packets by the VLAN identifier (VID) in their frame headers.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ 802.1Q VLAN trunking has been turned ON ⟨*changed_from*⟩.
Meaning	An admin enabled VLAN trunking for the specified interface. A trunk port allows a switch to bundle traffic from several VLANs through a single physical interface, sorting the various packets by the VLAN identifier (VID) in their frame headers.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ bandwidth has been changed to ⟨*bandwidth*⟩ Kbps.
Meaning	An admin has changed the configured bandwidth for the specified interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ gateway IP has been changed from ⟨*old_interface_gateway_IP*⟩ to ⟨*new_interface_gateway_IP*⟩ ⟨*changed_from*⟩.
Meaning	An admin has changed the IP address of the gateway for the specified interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been added to aggregate interface ⟨*aggregate_interface_name*⟩.
Meaning	An admin added an interface in an aggregate interface. An aggregate interface consists of two or more physical interfaces, each of which shares the traffic load directed to the IP address of the aggregate interface. An aggregate interface increases the amount of bandwidth available to a single IP address. Also, if one member of an aggregate interface fails, other members can continue processing traffic.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been added to redundant interface ⟨*redundant_interface_name*⟩.
Meaning	An admin added an interface in the specified redundant interface group.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been added to shared interface ⟨*shared_interface_name*⟩.
Meaning	An admin added an interface to a shared interface. A shared interface is an interface shared between systems (vsys or root). For an interface to be sharable, you must configure it at the root level and bind it to a shared zone in a shared virtual router. For example, by default the predefined untrust-vr is a shared virtual router, and the predefined Untrust zone is a shared zone. Consequently, a vsys can share any root-level physical interface, subinterface, redundant interface, or aggregate interface that you bind to the Untrust zone.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been changed from local to VSI.
Meaning	An admin changed an interface to a VSI. A VSI (Virtual Security Interface) is a logical entity at layer 3 that is linked to multiple layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover and it becomes the new master.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been changed from VSI to local.
Meaning	An admin changed a VSI to a local interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been removed from aggregate interface ⟨*aggregate_interface_name*⟩.
Meaning	An admin removed an interface in an aggregate interface. An aggregate interface consists of two or more physical interfaces, each of which shares the traffic load directed to the IP address of the aggregate interface. An aggregate interface increases the amount of bandwidth available to a single IP address. Also, if one member of an aggregate interface fails, other members can continue processing traffic.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been removed from redundant interface ⟨*redundant_interface_name*⟩.
Meaning	An admin added an interface in the specified redundant interface group.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ has been removed from shared interface ⟨*shared_interface_name*⟩.
Meaning	An admin removed an interface from a shared interface. A shared interface is an interface shared between systems (vsys or root). For an interface to be sharable, you must configure it at the root level and bind it to a shared zone in a shared virtual router. For example, by default the predefined untrust-vr is a shared virtual router, and the predefined Untrust zone is a shared zone. Consequently, a vsys can share any root-level physical interface, subinterface, redundant interface, or aggregate interface that you bind to the Untrust zone.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ holddown time interval has been set to ⟨*holddown_time*⟩.
Meaning	An admin changed the holddown time interval for a physical interface. The holddown time interval determines how long the device delays the following failover actions: Switching traffic to the backup interface, when the primary interface fails. Switching traffic from the backup interface to the primary interface, when the primary interface becomes available again. The default holddown interval is 30 seconds.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ in ⟨*vsys_name*⟩ was removed ⟨*changed_from*⟩.
Meaning	An admin has removed the specified interface from the virtual system.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ in ⟨*vsys_name*⟩ with IP ⟨*interface_IP*⟩ mask ⟨*interface_netmask*⟩ tag ⟨*interface_tag*⟩ was created ⟨*changed_from*⟩.
Meaning	An admin has created an interface for the specified virtual system. It has the specified IP address, netmask, and VLAN tag.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ in ⟨*vsys_name*⟩ with IP ⟨*interface_IP*⟩ mask ⟨*interface_netmask*⟩ was created ⟨*changed_from*⟩.
Meaning	An admin has created an interface for the specified virtual system. It has the specified IP address and netmask.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ IP address can be used to manage the device.
Meaning	An admin successfully specified an IP address to access and configure the device (with the WebUI management application).
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ IP address cannot be used to manage the device.
Meaning	An admin unsuccessfully specified an IP address to access and configure the device (with the WebUI management application).
Action	Find out what the manage-ip address is for the interface. (This address must be in the same subnet as the interface IP address.)

Message	Interface ⟨*interface_name*⟩ IP has been changed from ⟨*old_interface_IP*⟩ to ⟨*new_interface_IP*⟩ ⟨*changed_from*⟩.
Meaning	An admin has changed the IP address for the specified interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ management IP has been changed from ⟨*old_management_IP*⟩ to ⟨*new_management_IP*⟩ ⟨*changed_from*⟩.
Meaning	An admin has changed the manage IP address for the specified interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ netmask has been changed from ⟨*old_interface_netmask*⟩ to ⟨*new_interface_netmask*⟩ ⟨*changed_from*⟩.
Meaning	An admin has changed the netmask for the specified interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ operational mode has been changed to ⟨*operational_mode*⟩ ⟨*changed_from*⟩.
Meaning	An admin has changed the operational mode for the specified interface to { Route | NAT }.
Action	Check access policy configurations to ensure that they function properly in the new operational mode.

Message	Interface ⟨*interface_name*⟩ switching to ANSI T1.413 Issue 2 mode.
Meaning	The named interface is changing to ANSI T1.413 Issue 2 mode to complete an ADSL connection.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to auto-negotiating mode.
Meaning	The named interface is set to auto-negotiate the wireless mode.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to G.Lite mode.
Meaning	The named interface is changing to G.992.2 (G.lite) to complete an ADSL connection.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to ITU G.992.1 mode.
Meaning	ITU (International Telecommunications Union) G.992.1 (also known as G.dmt), is an interface mode that supports minimum data rates of 6.144 Mbps downstream and 640 kbps upstream.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to ITU G.992.3 del test mode.
Meaning	The ADSL interface has changed to ITU G.922.3 del test mode.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to ITU G.992.3 mode.
Meaning	The ADSL interface has changed to ITU G.922.3 mode.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to ITU G.992.5 del test mode.
Meaning	The ADSL interface has changed to ITU G.922.5 del test mode.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to ITU G.992.5 mode.
Meaning	The ADSL interface has changed to ITU G.922.5 mode.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ switching to loopback mode.
Meaning	An admin placed an interface to loopback mode. A loopback interface is a logical interface that emulates a physical interface on the security device. However, unlike a physical interface, a loopback interface is always in the up state as long as the device on which it resides is up. Loopback interfaces are named loopback.id_num, where id_num is a number greater than or equal to and denotes a unique loopback interface on the device. Like a physical interface, you must assign an IP address to a loopback interface and bind it to a security zone.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ was bound to zone ⟨*zone_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin bound the named interface to the specified zone.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ was removed from the monitoring list of ⟨*interface_name2*⟩.
Meaning	An admin removed an interface from the monitoring list of another interface.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ was unbound from zone ⟨*zone_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin unbound the named interface from the specified zone.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ with weight ⟨*weight*⟩ was added to the monitoring list of ⟨*interface2_name*⟩.
Meaning	An admin added an interface to the monitoring list of another interface.
Action	No recommended action.

Message	IPv4 Path-MTU has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has enabled or disabled the Path-MTU feature for the specified interface.
Action	No recommended action.

Message	IPv6 Path-MTU has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin enabled or disabled path-MTU (maximum transmission unit) discovery. If the device receives a packet that must be fragmented, it sends an ICMP packet suggesting a smaller packet size.
Action	No recommended action.

Message	Maximum bandwidth ⟨*maximum_bandwidth*⟩ Kbps on interface ⟨*interface_name*⟩ is less than total guaranteed bandwidth ⟨*guaranteed_bandwidth*⟩ Kbps.
Meaning	The specified interface bandwidth settings are insufficient for the total guaranteed bandwidth specified in the traffic shaping option of the access policies that traverse that interface.
Action	Increase the interface bandwidth settings or decrease the traffic shaping bandwidth settings on the access policies.

Message	Monitoring threshold was modified to ⟨*threshold*⟩ of ⟨*interface_name*⟩.
Meaning	An admin changed the threshold of a monitoring parameter for an interface.
Action	No recommended action.

Message	Mtrace has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin enabled or disabled mtrace on the named interface.
Action	No recommended action.

Message MTU for interface ⟨*interface_name*⟩ has been changed to ⟨*mtu*⟩.

Meaning An admin changed the Maximum Transmission Unit (MTU) for the specified interface.

Action No recommended action.

Message Primary interface ⟨*pri_if_name*⟩ set backup interface ⟨*bak_if_name*⟩, type is ⟨*type*⟩.

Meaning The primary interface is configured to switch over to backup interface based on type of tracking or monitoring configured on the primary interface. You can configure the following types of tracking: IP tracking, Tunnel-if tracking, or Route monitoring.

Action No recommended action.

Message Primary interface ⟨*pri_if_name*⟩ unset backup interface ⟨*bak_if_name*⟩.

Meaning A network administrator has unset the backup interface feature on the primary interface.

Action No recommended action.

Message Route between secondary IP addresses on interface ⟨*interface_name*⟩ has been disabled.

Meaning An admin has disabled the routes to all secondary IP addresses on the specified interface.

Action No recommended action.

Message Route between secondary IP addresses on interface ⟨*interface_name*⟩ has been enabled.

Meaning An admin has enabled the routes to all secondary IP addresses on the specified interface.

Action No recommended action.

Message ⟨*phy_name*⟩ for interface ⟨*interface_name*⟩ has been changed to ⟨*value*⟩.

Meaning An admin has changed the value of an interface option (such as clocking, hold time up/down, BERT algorithm/error rate/period, build out, byte encoding, etc.).

Action No recommended action.

Message	Secondary IP address ⟨*IP*⟩ has been deleted from interface ⟨*interface_name*⟩.
Meaning	An admin successfully deleted a specified IP address to a specified interface.
Action	No recommended action.

Message	Secondary IP address ⟨*IP*⟩/⟨*netmask*⟩ has been added to interface ⟨*interface_name*⟩.
Meaning	An admin successfully added a specified IP address to a specified interface.
Action	No recommended action.

Message	Zone ⟨*zone_name*⟩ was removed from the monitoring list of ⟨*interface_name*⟩.
Meaning	An admin removed a zone from the monitoring list that was associated with an interface.
Action	No recommended action.

Message	Zone ⟨*zone_name*⟩ with weight ⟨*weight*⟩ was added to the monitoring list of ⟨*interface_name*⟩.
Meaning	An admin added a zone to the monitoring list of an interface.
Action	No recommended action.

Notification (00078)

Message	A dialer CLI is configured: ⟨*cli_string*⟩.
Meaning	A dialer interface setting is configured.
Action	No recommended action.

Notification (00513)

Message	The physical state of interface ⟨*interface_name*⟩ has changed to ⟨*new_state*⟩.
Meaning	An interface has become active (up) or inactive (down).
Action	If the interface is down, check to see if the interface is necessary for transmission of traffic.

Notification (00613)

Message	Interface ⟨*interface_name*⟩ dialed out at channel ⟨*channel*⟩.
Meaning	The dialer interface dialed out from the specified channel.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ disconnects at channel ⟨*channel*⟩.
Meaning	The dialer interface is disconnected on the specified channel.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ idle timer expired.
Meaning	The dialer interface idle timer is expired.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ is connected at channel ⟨*channel*⟩.
Meaning	The dialer interface is established a connection on the specified channel.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ is disconnecting at channel ⟨*channel*⟩.
Meaning	The dialer interface is disconnecting on the specified channel.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ traffic (⟨*traffic*⟩ bps) decreased (less than load-threshold).
Meaning	The traffic on the dialer interface decreased and is less than the load threshold.
Action	No recommended action.

Message	Interface ⟨*interface_name*⟩ traffic (⟨*traffic*⟩ bps) increased (greater than load-threshold).
Meaning	The traffic on the dialer interface increased and is greater than the load threshold.
Action	No recommended action.

Information

Message	G-ARP has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled the G-ARP knob for the specified interface. An admin can use the G-ARP knob setting to accept/ignore incoming gratuitous ARP packets.
Action	No recommended action

Information (00009)

Message	Global-PRO has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled Global-PRO access for the specified interface.
Action	No recommended action.

Message	Ident-reset has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled Ident-reset access for the specified interface.
Action	No recommended action.

Message	NSGP ⟨*enforcing_IPSec*⟩ has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin enabled or disabled NSGP for the specified interface. NSGP is a protocol for GPRS Overbilling Attack notification feature on a Gi firewall (the server). An Overbilling attack can occur in various ways. It can occur when a legitimate subscriber returns his IP address to the IP pool, at which point an attacker can hijack the IP address, which is vulnerable because the session is still open. When the attacker takes control of the IP address, without being detected and reported, the attacker can download data for free (or more accurately, at the expense of the legitimate subscriber) or send data to other subscribers. An Overbilling attack can also occur when an IP address becomes available and gets reassigned to another MS. Traffic initiated by the previous MS might be forwarded to the new MS, therefore causing the new MS to be billed for unsolicited traffic.
Action	No recommended action.

Message	Ping has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled the ping functionality for the specified interface.
Action	No recommended action.

Message	SCS has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled the SCS functionality for the specified interface.
Action	No recommended action.

Message	SNMP has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled the SNMP functionality for the specified interface.
Action	No recommended action.

Message	SSL has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled SSL access for the specified interface.
Action	No recommended action.

Message	Telnet has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled the telnet connection functionality for the specified interface.
Action	No recommended action.

Message	Web has been ⟨*new_status*⟩ on interface ⟨*interface_name*⟩ ⟨*changed_from*⟩.
Meaning	An admin has either enabled or disabled web access for the specified interface.
Action	No recommended action.

Chapter 30

Interface6

The following messages apply to IPv6 network deployments.

Critical (00101)

Message	DAD detected duplicates for IPv6 address ⟨*IP address*⟩ on interface ⟨*string*⟩
Meaning	Duplicate Address Detection (DAD) determines if more than one on-link device has the same unicast address.
Action	Check online hosts for duplicate addresses. Remove duplicate address from the host, then reset the host. IPv6 address autoconfiguration should then assign a unique address to the host.

Notification (00009)

Message	⟨*new_status*⟩ IPv6 function on the interface ⟨*interface_name*⟩.
Meaning	Enabling or disabling the IPv6 functions on an interface.
Action	

Message	Setting interface ⟨*interface_name*⟩ IPv6 mode to ⟨*mode*⟩.
Meaning	The interface of the device is set to function as an IPv6 host or router. In Host mode, the interface functions as an IPv6 host and autoconfigures itself by requesting and accepting Router Advertisement (RA) messages from other devices. In Router mode, the interface functions as an IPv6 router. An IPv6 router replies to Router Solicitation (RS) messages from IPv6 hosts by sending RAs. In addition, the interface can broadcast RAs periodically or in response to configuration changes to keep the on-link hosts updated.
Action	No recommended action

Message	Unsetting IPv6 mode on interface ⟨*interface_name*⟩.
Meaning	The interface of the device is set to mode none, which means IPv6 is not used on the interface. In the CLI, the unset IPv6 mode command is successful only after the IPv6 is disabled on the interface.
Action	No recommended action.

Notification (00071)

Message	DAD completed for IPv6 address ⟨*IP address*⟩ on interface ⟨*string*⟩
Meaning	DAD (Duplicate Address Detection) successfully confirmed that there are no on-link hosts with duplicate IPv6 addresses.
Action	No recommended action.

Message	Initialized IPv6 address ⟨*IP address*⟩ on interface ⟨*string*⟩
Meaning	An admin assigned an IPv6 address to an interface.
Action	No recommended action.

Notification (00072)

Message	IPv6 Router advertisement reception disabled on interface ⟨*string*⟩
Meaning	An admin enabled or disabled router advertisment (RA) reception on the specified interface.
Action	No recommended action.

Message	IPv6 Router advertisement reception enabled on interface ⟨*string*⟩
Meaning	An admin enabled or disabled router advertisment (RA) reception on the specified interface.
Action	No recommended action.

Message	IPv6 Router advertisement transmission disabled on interface ⟨*string*⟩
Meaning	An admin enabled or disabled router advertisment (RA) transmission on the specified interface. (A Router Advertisement (RA) is a message sent by a router to on-link hosts, either periodically or in response to a Router Solicitation (RS) request from another host.
Action	No recommended action.

Message	IPv6 Router advertisement transmission enabled on interface ⟨*string*⟩
Meaning	An admin enabled or disabled router advertisment (RA) transmission on the specified interface. (A Router Advertisement (RA) is a message sent by a router to on-link hosts, either periodically or in response to a Router Solicitation (RS) request from another host.
Action	No recommended action.

Chapter 31
ISDN

The following messages relate to the Integrated Services Digital Network (ISDN) feature in ScreenOS.

Notification (00083)

Message	[isdn] Interface ⟨*interfacename*⟩ is configured for leased-line ⟨*speed*⟩.
Meaning	The BRI interface (ISDN) is configured for leased line at 128 kbps.
Action	No action required.

Message	[isdn] Interface ⟨*interfacename*⟩ is configured to work with switch type ⟨*switch_type_name*⟩ (after reboot).
Meaning	The BRI interface (ISDN) is configured to work with the specified switch type.
Action	No action required.

Message	[isdn] Interface ⟨*interfacename*⟩ is set for TEI negotiation at ⟨*tei_negotiation_time*⟩.
Meaning	The BRI interface (ISDN) is configured for Terminal Endpoint Identifier (TEI) negotiation, which is useful for switches that may deactivate Layer 1 or 2 when there are no active calls. TEI negotiation occurs when the first call is made (default) or at device power up.
Action	No action required.

Message	[isdn] Interface ⟨*interfacename*⟩ will not send Sending Complete in SETUP message.
Meaning	The BRI interface (ISDN) does not add the Sending Complete information element in the outgoing call-setup message.
Action	No action required.

Message	[isdn] Interface ⟨*interfacename*⟩ will send Sending Complete in SETUP message.
Meaning	The BRI interface (ISDN) adds the Sending Complete information element in the outgoing call-setup message to indicate that the entire number is included.
Action	No action required.

Message	[isdn] Leased-line is removed for interface ⟨*interfacename*⟩.
Meaning	The BRI interface (ISDN) is not configured for leased line.
Action	No action required.

Message	[isdn] SPID1 for interface ⟨*interfacename*⟩ is set to ⟨*spid*⟩.
Meaning	The BRI interface (ISDN) is configured with a Service Profile Identifier (SPID) number. Your Carrier defines the SPID number. Your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the ISP when it accesses the switch to initialize the connection.
Action	No action required.

Message	[isdn] SPID2 for interface ⟨*interfacename*⟩ is set to ⟨*spid*⟩.
Meaning	The BRI interface (ISDN) is configured with a Service Profile Identifier (SPID) number. For some ISDN switch types, two SPIDs are assigned, one for each B-channel. Your Carrier defines the SPID numbers.
Action	No action required.

Message	[isdn] The calling number for interface ⟨*interfacename*⟩ is set to ⟨*calling_number*⟩.
Meaning	The BRI interface (ISDN) is configured with a calling number to make outgoing calls to the ISDN switch.
Action	No action required.

Message	[isdn] The T310 value for interface ⟨*interfacename*⟩ is changed from ⟨*t310_old*⟩ to ⟨*t310_new*⟩.
Meaning	The T310 value for the BRI interface (ISDN) is modified. The value can range between 5 and 100 seconds. The default T310 timeout value is 10 seconds.
Action	No action required.

Notification (00618)

Message	[isdn] Interface ⟨*d_channel*⟩ connected on B channel ⟨*b_channel*⟩.
Meaning	A call is set up successfully on a B channel.
Action	No action required.

Message	[isdn] Interface ⟨*d_channel*⟩ disconnected on B channel ⟨*b_channel*⟩.
Meaning	A call is ended on a B channel.
Action	No action required.

Message	[isdn] Layer2 is ⟨*status*⟩ on D channel ⟨*d_channel*⟩.
Meaning	When the dialer is trying to dial out, it first brings up Layer 2. For some switch types, Layer 2 is initially down and all subsequent calls on this BRI interface hang up. The UP message appears when the TEI-negotiation is updated from first-call to power-up.
Action	No action required.

Chapter 32

L2TP

The following messages concern the configuration and operation of Layer 2 Tunneling Protocol (L2TP).

Alert (00043)

Message	Receive StopCCN_msg, remove l2tp tunnel (⟨*local_ip*⟩-⟨*peer_ip*⟩), Result code ⟨*result_code*⟩ (⟨*result_code_str*⟩).
Meaning	The Juniper device received an L2TP Stop-Control-Connection-Notification (StopCCN) message, which signals the termination of an L2TP tunnel. The message also includes a result code ID number and message. For information about result code ID numbers 0-7 for the StopCCN message, refer to "Section 4.4.2 Result and Error Codes" in RFC 2661, Layer Two Tunneling Protocol "L2TP".
Action	No recommended action

Alert (00044)

Message	Receive StopCCN_msg, remove l2tp tunnel (⟨*local_ip*⟩-⟨*peer_ip*⟩), Result code ⟨*result_code*⟩ (⟨*result_code_str*⟩), Error code ⟨*error_code*⟩ (⟨*error_code_str*⟩).
Meaning	The Juniper device received an L2TP Stop-Control-Connection-Notification (StopCCN) message, which signals the termination of an L2TP tunnel. The message also includes a result code ID number and message, and an error code ID number and message. For information about result code ID numbers 0-7 for the StopCCN message and error code ID numbers 0-8, refer to "Section 4.4.2 Result and Error Codes" in RFC 2661, Layer Two Tunneling Protocol "L2TP".
Action	No recommended action

Alert (00045)

Message	Receive CDN_msg, remove l2tp call, id = ⟨*call_id*⟩, user = ⟨*user_name*⟩, assigned ip = ⟨*assigned_ip*⟩, Result code ⟨*result_code*⟩ (⟨*result_code_str*⟩).
Meaning	The Juniper device received an L2TP Call-Disconnect-Notify (CDN) message, which requests the disconnection of a specific call within an L2TP tunnel. The message also includes the following details: Call ID number L2TP user name IP address assigned to the L2TP user Result code ID number and message For information about result code ID numbers 0-11 for a CDN message, refer to "Section 4.4.2 Result and Error Codes" in RFC 2661, Layer Two Tunneling Protocol "L2TP".
Action	No recommended action

Alert (00046)

Message	Receive CDN_msg, remove l2tp call, id = ⟨*call_id*⟩, user = ⟨*user_name*⟩, assigned ip = ⟨*assigned_ip*⟩, Result code ⟨*result_code*⟩ (⟨*result_code_str*⟩), Error code ⟨*error_code*⟩ (⟨*error_code_str*⟩).
Meaning	The peer device sent an L2TP Call-Disconnect-Notify (CDN) message, which requests the disconnection of a specific call within an L2TP tunnel. The message also includes the following details: Call ID number L2TP user name IP address assigned to the L2TP user Result code ID number and message Error code ID number and message For information about result code ID numbers 0-11 for a CDN message and error code ID numbers 0-8, refer to "Section 4.4.2 Result and Error Codes" in RFC 2661, Layer Two Tunneling Protocol "L2TP".
Action	No recommended action

Notification (00017)

Message	L2TP ⟨*l2tp_name*⟩, all-L2TP-users secret ⟨*secret*⟩ keepalive ⟨*keepalive*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin changed the L2TP keepalive value for all L2TP users. The keepalive value defines how many seconds of inactivity, the Juniper device (LNS) waits before sending a hello message to the dialup client (LAC).
Action	No recommended action

Message	L2TP ⟨*l2tp_name*⟩, ⟨*user_or_group*⟩ ID ⟨*user_id*⟩ secret ⟨*secret*⟩ keepalive ⟨*keepalive*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin changed the L2TP keepalive value for a specified user or user group. The keepalive value defines how many seconds of inactivity, the Juniper device (LNS) waits before sending a hello message to the dialup client (LAC).
Action	No recommended action

Message	L2TP default auth type changed to ⟨*auth_type*⟩.
Meaning	An admin changed the authentication type for L2TP.
Action	No recommended action

Message	L2TP default ippool changed from ⟨*old_ippool_name*⟩ to ⟨*new_ippool_name*⟩.
Meaning	An admin changed the name of the L2TP default IP pool
Action	No recommended action

Message	L2TP default PPP auth type changed to ⟨*ppp_auth_type*⟩.
Meaning	An admin changed the Point-to-Point Protocol (PPP) authentication type.
Action	No recommended action

Message	L2TP default primary DNS server changed from ⟨*old_ip*⟩ to ⟨*new_ip*⟩.
Meaning	An admin changed the IP address of the primary or secondary DNS or WINS server.
Action	No recommended action

Message	L2TP default primary WINS server changed from ⟨*old_ip*⟩ to ⟨*new_ip*⟩.
Meaning	An admin changed the IP address of the primary or secondary DNS or WINS server.
Action	No recommended action

Message	L2TP default RADIUS port changed to ⟨*radius_port*⟩.
Meaning	An admin changed the RADIUS port number to the designated value.
Action	No recommended action

Message	L2TP default RADIUS secret changed to ⟨*radius_secret*⟩.
Meaning	An admin changed the RADIUS secret to the designated value.
Action	No recommended action

Message	L2TP default RADIUS server changed to ⟨*radius_server*⟩.
Meaning	An admin changed the designated RADIUS server.
Action	No recommended action

Message	L2TP default secondary DNS server changed from ⟨*old_ip*⟩ to ⟨*new_ip*⟩.
Meaning	An admin changed the IP address of the primary or secondary DNS or WINS server.
Action	No recommended action

Message	L2TP default secondary WINS server changed from ⟨*old_ip*⟩ to ⟨*new_ip*⟩.
Meaning	An admin changed the IP address of the primary or secondary DNS or WINS server.
Action	No recommended action

Message	L2TP ippool is unset to default.
Meaning	An admin unset the currently designated default L2TP IP pool.
Action	No recommended action

Message	L2TP primary DNS server is unset to default.
Meaning	An admin unset the currently designated primary or secondary DNS or WINS server.
Action	No recommended action

Message	L2TP primary WINS server is unset to default.
Meaning	An admin unset the currently designated primary or secondary DNS or WINS server.
Action	No recommended action

Message	L2TP RADIUS port changed to ⟨*radius_port*⟩.
Meaning	An admin changed the L2TP RADIUS port to the designated port number.
Action	No recommended action

Message	L2TP RADIUS secret is unset to default.
Meaning	An admin unset the currently designated L2TP RADIUS secret.
Action	No recommended action

Message	L2TP RADIUS server is unset to default.
Meaning	An admin unset the currently designated L2TP RADIUS server.
Action	No recommended action

Message	L2TP secondary DNS server is unset to default.
Meaning	An admin unset the currently designated primary or secondary DNS or WINS server.
Action	No recommended action

Message	L2TP secondary WINS server is unset to default.
Meaning	An admin unset the currently designated primary or secondary DNS or WINS server.
Action	No recommended action

Information (00536)

Message	Incorrect L2TP secret in tunnel authentication for L2TP (⟨*peer_ip*⟩).
Meaning	The device detected an incorrect L2TP secret during authentication for an L2TP tunnel.
Action	No recommended action

Message	L2TP at ⟨*peer_ip*⟩ PPP failed, Failure in ⟨*error_code*⟩.
Meaning	A PPP error condition occurred causing L2TP communication failure.
Action	No recommended action

Message	L2TP tunnel ⟨*l2tp_name*⟩ created between ⟨*local_ip*⟩:⟨*local_port*⟩ and ⟨*peer_ip*⟩:⟨*peer_port*⟩.
Meaning	An admin defined an L2TP tunnel between two endpoints, each defined as an IP address and port number.
Action	No recommended action

Message	l2tp(⟨*local_ip*⟩/⟨*local_port*⟩- > ⟨*peer_ip*⟩/⟨*peer_port*⟩), user authentication passed. IP address ⟨*assigned_ip*⟩ assigned to user.
Meaning	User authentication occurred at a specified host (< ip_addr3 >) for an L2TP tunnel.
Action	No recommended action

Message	Retry time-out interval expired. L2TP call (peer at ⟨*peer_ip*⟩, local at ⟨*local_ip*⟩) removed, tunnel ID ⟨*tunnel_id*⟩, call ID ⟨*call_id*⟩.
Meaning	An attempt to establish an L2TP session failed due to expiration of the retry timeout interval.
Action	No recommended action

Message	Retry time-out interval expired. L2TP tunnel removed (peer at ⟨*peer_ip*⟩, local at ⟨*local_ip*⟩), tunnel ID ⟨*tunnel_id*⟩.
Meaning	An attempt to establish an L2TP session failed due to expiration of the retry timeout interval.
Action	No recommended action

Chapter 33
Logging

The following messages relate to the event, self and traffic logs.

Warning (00002)

Message	Cannot connect to e-mail server ⟨*server_name*⟩.
Meaning	The security device cannot connect to the SMTP server used for sending e-mail event alarm notifications.
Action	Check the IP address of the SMTP server.

Message	Mail recipients were not configured.
Meaning	The e-mail addresses of the recipients of the event alarm notifications were not configured.
Action	Configure at least one recipient with the set admin mail mail-addr1 command.

Message	Mail server is not configured.
Meaning	The security device cannot send e-mail event alarm notifications because the SMTP server was not configured.
Action	Use the set admin mail server-name ip_addr command to configure the mail server.

Message	Unexpected error from e-mail server(state = ⟨*state*⟩): ⟨*error*⟩.
Meaning	An e-mail server generated an error condition with the specified ID number. The security device typically generates this message when the mail server does not accept SMTP messages from the security device.
Action	Check if the mail server is allowed to receive messages from the IP address of the security device. Add the IP address of the security device to the mail server application, if necessary.

Notification (00002)

Message	E-mail address 1 has been changed.
Meaning	An admin has changed the primary or secondary e-mail address to which the security device sends event alarm notifications.
Action	No recommended action

Message	E-mail address 2 has been changed.
Meaning	An admin has changed the primary or secondary e-mail address to which the security device sends event alarm notifications.
Action	No recommended action

Message	E-mail notification has been disabled.
Meaning	E-mail notification of event alarms has been either enabled or disabled.
Action	No recommended action

Message	E-mail notification has been enabled.
Meaning	E-mail notification of event alarms has been either enabled or disabled.
Action	No recommended action

Message	Inclusion of traffic logs with e-mail notification of event alarms has been disabled.
Meaning	An admin has enabled or disabled the inclusion of traffic logs with e-mail event alarm notifications.
Action	No recommended actio

Message	Inclusion of traffic logs with e-mail notification of event alarms has been enabled.
Meaning	An admin has enabled or disabled the inclusion of traffic logs with e-mail event alarm notifications.
Action	No recommended action

Message	Mail server domain name has been changed.
Meaning	The IP address or domain name of the SMTP server used for sending e-mail event alarm notifications has been changed.
Action	No recommended action

Message	Mail server IP address has been changed.
Meaning	The IP address or domain name of the SMTP server used for sending e-mail event alarm notifications has been changed.
Action	No recommended action

Chapter 34

MGCP

The following messages relate to the Media Gateway Control Protocol (MGCP), a standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet.

Alert (00063)

Message	MGCP ALG configured to drop unidentified message in NAT mode.
Meaning	The MGCP ALG is configured to drop unidentified MGCP messages in NAT mode.
Action	No recommended action.

Message	MGCP ALG configured to drop unidentified message in route mode.
Meaning	The MGCP ALG is configured to drop unidentified MGCP messages in route mode.
Action	No recommended action.

Message	MGCP ALG configured to pass unidentified message in NAT mode.
Meaning	The MGCP ALG is configured to pass unidentified MGCP messages in NAT mode.
Action	No recommended action.

Message	MGCP ALG configured to pass unidentified message in route mode.
Meaning	The MGCP ALG is configured to pass unidentified MGCP messages in route mode.
Action	No recommended action.

Message	MGCP ALG configured to screen high connection rate.
Meaning	MGCP connection flood screening is enabled
Action	No recommended action.

Message	MGCP ALG connection flood rate threshold set to default.
Meaning	The MGCP ALG connection flood rate threshold is set to the default value.
Action	No recommended action.

Message	MGCP ALG connection flood rate threshold value set to ⟨*num_of_connections_per_second*⟩ connections per second.
Meaning	The MGCP ALG connection flood rate threshold is set to the indicated value.
Action	No recommended action.

Message	MGCP ALG disabled on the device.
Meaning	The MGCP ALG is disabled on the device.
Action	No recommended action.

Message	MGCP ALG enabled on the device.
Meaning	The MGCP ALG is enabled.
Action	No recommended action.

Message	MGCP ALG inactive media timeout value set to default.
Meaning	The MGCP ALG inactive media timeout set to the default value.
Action	No recommended action.

Message	MGCP ALG inactive media timeout value set to ⟨*inactive_media_timeout*⟩ seconds.
Meaning	The MGCP ALG inactive media timeout is set to the indicated value.
Action	No recommended action.

Message	MGCP ALG maximum call duration value set to default.
Meaning	The MGCP ALG maximum call duration is set to the default value.
Action	No recommended action.

Message	MGCP ALG maximum call duration value set to ⟨*max_call_duration*⟩ minutes.
Meaning	The MGCP ALG maximum call duration is set to the indicated value.
Action	No recommended action.

Message	MGCP ALG message flood rate threshold value set to default.
Meaning	The MGCP ALG message flood rate threshold is set to the default value.
Action	No recommended action.

Message	MGCP ALG message flood rate threshold value set to ⟨*num_of_messages_per_second*⟩ messages per second.
Meaning	The MGCP ALG message flood rate threshold is set to the indicated value.
Action	No recommended action.

Message	MGCP ALG removed the check for message flood rate.
Meaning	MGCP message flood screening is disabled
Action	No recommended action.

Message	MGCP ALG transaction timeout value set to default.
Meaning	The MGCP ALG transaction timeout is set to the default value.
Action	No recommended action.

Message	MGCP ALG transaction timeout value set to ⟨*transaction_timeout*⟩ seconds.
Meaning	The MGCP ALG transaction timeout is set to the indicated value.
Action	No recommended action.

Message	The MGCP ALG is configured to screen high message rate.
Meaning	The MGCP message flood screening is enabled
Action	No recommended action.

Message	The MGCP ALG removed the check for connection rate.
Meaning	The MGCP connection flood screening is disabled
Action	No recommended action.

Alert (00084)

Message	The device cannot delete MGCP CA Port.
Meaning	The device failed to delete the MGCP ALG service
Action	No recommended action

Message	The device cannot delete MGCP UA ALG Port.
Meaning	The device failed to delete the MGCP ALG service
Action	No recommended action

Message	The device cannot initialize memory for MGCP.
Meaning	The device failed to initialize the MGCP ALG service
Action	No recommended action

Message	The device cannot register MGCP CA Port.
Meaning	The device failed to initialize the MGCP ALG service
Action	No recommended action

Message	The device cannot register MGCP UA Port.
Meaning	The device cannot initialize the MCCP ALG service.
Action	No recommended action

Message	The device cannot unregister MGCP ALG handler.
Meaning	The device failed to delete the MGCP ALG service
Action	No recommended action

Notification

Message	MGCP decoder error ⟨*msg*⟩.

Notification

Message	The device cannot allocate sufficient memory for the MGCP ALG request.

Notification (00084)

Message	Device failure handling MGCP call because the number of calls exceeded the system limit.
Meaning	The number of calls has exceeded the capacity of the system.
Action	No recommended action.

Message	The device cannot register the MGCP ALG request to RM.
Meaning	The device failed to initialize the MGCP ALG service
Action	No recommended action

Message	The device cannot register the Network Address Translation vector for the MGCP ALG request.
Meaning	The device cannot initialize the MGCP ALG service.
Action	No recommended action

Message	The device does not have MGCP ALG client id with RM.
Meaning	The device failed to initialize the MGCP ALG service
Action	No recommended action

Message	The device failed in unregistering MGCP client with RM.
Meaning	When a network administrator unset the MGCP ALG, the device failed to remove the MGCP ALG.
Action	No recommended action

Chapter 35

Multicast

The following message relates to multicast routes.

Alert (00601)

Message	Error in initializing multicast.
Meaning	An error occurred when the Juniper device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Failure in initializing multicast data handler task.
Meaning	An error occurred when the Juniper device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Failure in initializing multicast route task.
Meaning	An error occurred when the Juniper device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Failure in registering for multicast data packet.
Meaning	An error occurred when the Juniper device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Failure in shutting down multicast route task.
Meaning	An error occurred when the Juniper device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	System-wide multicast cachemiss node limit reached, ⟨*number-of-cachemiss-add_failed-from-last-exceed*⟩ nodes not added since limit exceeded.
Meaning	The Juniper device did not add the new negative multicast route to the cache because the number of entries exceeded the maximum allowed.
Action	Modify the negative cache timer to age out more entries.

Critical (00601)

Message	Failure adding output interface to multicast route list due to exceeding system max. ⟨*number-of-output-interface-add_failed-from-last-exceed*⟩ interfaces not added since limit exceeded.
Meaning	The Juniper device did not add the egress interface to the multicast route entry because the number of egress interfaces exceeded the maximum allowed.
Action	Clear any unused multicast routes.

Message	⟨*vrouter-name*⟩: virtual router multicast route limit exceeded, mroute addition failed.
Meaning	The Juniper device did not add the new multicast route to the multicast route table because the number of multicast route entries exceeded the maximum configured for the virtual router.
Action	You can remove the configured maximum number of entries with the unset vrouter < name_str > mroute max-entries command.

Message	⟨*vrouter-name*⟩: virtual router multicast route maximum, routes not added since limit exceeded - ⟨*number-of-mroute-add_failed-from-last-exceed*⟩.
Meaning	The Juniper device did not add multicast routes to the multicast route table because the number of multicast route entries exceeded the maximum configured for the named virtual router. The message displays how many routes were not added from the last time the limit was exceeded.
Action	You can remove the configured maximum number of entries with the unset vrouter < name_str > mroute max-entries command.

Message	System wide multicast route limit exceeded, mroute add failed.
Meaning	The Juniper device did not add the new multicast route to the multicast route table because the number of multicast route entries exceeded the maximum allowed. The maximum number of entries allowed depends on the Juniper device.
Action	Clear any unused multicast routes.

Message	System wide multicast route limit reached, routes not added since limit exceeded - ⟨*number-of-mroute-add_failed-from-last-exceed*⟩.
Meaning	The Juniper device did not add multicast routes to the multicast route table because the number of multicast route entries exceeded the maximum allowed. The maximum number of entries allowed depends on the Juniper device. The message displays how many routes were not added from the last time the limit was exceeded.
Action	Clear any unused multicast routes.

Notification (00056)

Message	⟨*string*⟩.
Meaning	A multicast configuration policy has been removed.
Action	No recommmended action.

Message	⟨*string*⟩.
Meaning	A multicast configuration policy has been added.
Action	No recommended action.

Notification (00057)

Message	⟨*vrouter-name*⟩: maximum multicast routes limit configured to ⟨*maximum-mroutes*⟩.
Meaning	An admin set the maximum number of allowed multicast routes for the virtual router.
Action	No recommended action

Message	⟨*vrouter-name*⟩: maximum multicast routes limit removed.
Meaning	An admin removed the configured limit on the number of multicast routes allowed for the virtual router.
Action	No recommended action

Message	⟨*vrouter-name*⟩: multicast negative cache routes feature configured.
Meaning	An admin enabled the negative cache feature on the specified virtual router.
Action	No recommended action

Message	⟨*vrouter-name*⟩: multicast negative cache routes feature removed.
Meaning	An admin enabled the negative cache feature on the specified virtual router.
Action	No recommended action

Message	⟨*vrouter-name*⟩: multicast negative cache routes timer configured to default.
Meaning	An admin set the negative cache timer to the default number of seconds.
Action	No recommended action

Message	⟨*vrouter-name*⟩: multicast negative cache routes timer configured to ⟨*negative-cache-timer-in-seconds*⟩ seconds.
Meaning	An admin set the negative cache timer to the specified number of seconds.
Action	No recommended action

Message	⟨*vrouter-name*⟩: static multicast route src = ⟨*source-ip-address*⟩, grp = ⟨*group-ip-address*⟩ ifp = ⟨*incoming-interface-name*⟩ deleted.
Meaning	An admin removed the specified static multicast route from the multicast route table of the virtual router.
Action	No recommended action

Message	⟨*vrouter-name*⟩: static multicast route src = ⟨*source-ip-address*⟩, grp = ⟨*group-ip-address*⟩ input ifp = ⟨*incoming-interface-name*⟩ output ifp = ⟨*outgoing-interface-name*⟩ added.
Meaning	An admin added the specified static multicast route to the multicast route table of the virtual router.
Action	No recommended action

Chapter 36
NSM

The following messages relate to the NetScreen-Security Manager (NSM) central management software.

Notification (00033)

Message	CA certificate field of NACN policy manager ⟨*integer*⟩ has been set to ⟨*string*⟩.
Meaning	An admin has set the CA certificate field of the policy manager to the specified string.
Action	No recommended action

Message	CA certificate field of NACN policy manager ⟨*integer*⟩ has been unset.
Meaning	An admin has cleared the CA certificate field of the specified policy manager.
Action	Specify a CA certificate if necessary.

Message	Cert-Subject field of NACN policy manager ⟨*integer*⟩ has been set to ⟨*string*⟩.
Meaning	An admin has set the subject name field in the Policy Manager certificate.
Action	No recommended action

Message	Cert-Subject field of NACN policy manager ⟨*integer*⟩ has been unset.
Meaning	An admin has cleared the Cert-Subject field of the specified policy manager.
Action	Specify the expected subject name of the certificate installed on the Policy Manager.

Message	Host field of NACN policy manager ⟨*integer*⟩ has been set to ⟨*string*⟩.
Meaning	An admin has set the host field to the specified hostname.
Action	No recommended action

Message	Host field of NACN policy manager ⟨*integer*⟩ has been unset.
Meaning	An admin cleared the IP address of the server running Policy Manager.
Action	Set a new IP address for the server running Policy Manager if necessary.

Message	NSM Device ID was set to ⟨*string*⟩.
Meaning	An admin either set the device ID to the specified value or unset the existing device ID. This ID is used when a connection is initiated between the security device and the management server.
Action	No recommended action

Message	NSM Device ID was unset.
Meaning	An admin either set the device ID to the specified value or unset the existing device ID. This ID is used when a connection is initiated between the security device and the management server.
Action	No recommended action

Message	NSM installer name (⟨*string*⟩) and password were set.
Meaning	An admin either set or unset the installer name and password, which are optionally used when the NSRD configlet is uploaded to the security device.
Action	No recommended action

Message	NSM installer name and password were unset.
Meaning	An admin either set or unset the installer name and password, which are optionally used when the NSRD configlet is uploaded to the security device.
Action	No recommended action

Message	NSM keys were deleted.
Meaning	An admin deleted the public and private keys used to connect to the management server.
Action	No recommended action

Message	NSM one-time-password was set.
Meaning	An admin set the One-Time Password (OTP). The security device uses this password to contact NSM.
Action	No recommended action

Message	NSM one-time-password was unset.
Meaning	An admin unset the One-Time Password (OTP). The security device uses this password to contact NSM.
Action	No recommended action

Message	NSM primary server with name ⟨*string*⟩ was set: addr ⟨*IP address*⟩, port ⟨*string*⟩
Meaning	An admin set the host name and/or IP address and port of the NSM primary or secondary server.
Action	No recommended action

Message	NSM primary server with name ⟨*string*⟩ was unset.
Meaning	An admin unset the specified primary or secondary NSM server.
Action	No recommended action

Message	NSM secondary server with name ⟨*string*⟩ was set: addr ⟨*IP address*⟩, port ⟨*string*⟩
Meaning	An admin set the host name and/or IP address and port of the NSM primary or secondary server.
Action	No recommended action

Message	NSM secondary server with name ⟨*string*⟩ was unset.
Meaning	An admin unset the specified primary or secondary NSM server.
Action	No recommended action

Message	Outgoing interface of NACN policy manager ⟨*integer*⟩ has been set to ⟨*string*⟩.
Meaning	An admin has set the outgoing interface for NACN policy manager to the specified interface.
Action	No recommended action

Message	Outgoing interface of NACN policy manager ⟨*integer*⟩ has been unset.
Meaning	An admin has cleared the outgoing interface of the specified policy manager.
Action	Set the interface to any interface name to enable the interface.

Message	Password field of NACN policy manager ⟨*integer*⟩ has been ⟨*string*⟩.
Meaning	An admin has changed the password for the specified NACN policy manager.
Action	No recommended action

Message	Policy-domain field of NACN policy manager ⟨*integer*⟩ has been set to ⟨*string*⟩.
Meaning	An admin has set the policy-domain field of the NACN policy manager to the specified domain name. The Policy Manager was set and will search for a specified policy domain.
Action	No recommended action

Message	Policy-domain field of NACN policy manager ⟨*integer*⟩ has been unset.
Meaning	An admin has cleared the policy-domain field for the NACN policy manager. Policy Manager will search all policy domains instead of only a specified domain.
Action	Specify a policy domain in Policy Manager.

Message	Port field of NACN policy manager ⟨*integer*⟩ has been reset to the default value.
Meaning	An admin has reverted the port field of the specified policy manager to the default.
Action	No recommended action

Message	Port field of NACN policy manager ⟨*integer*⟩ has been set to ⟨*integer*⟩.
Meaning	An admin has set the port field of the policy manager to the specified value.
Action	No recommended action

Message	Reporting of attack alarms to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of attack alarms, such as syn-flag or syn-flood.
Action	No recommended action

Message	Reporting of attack alarms to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of attack alarms, such as syn-flag or syn-flood.
Action	No recommended action

Message	Reporting of attack statistics table to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of messages containing attack statistics.
Action	No recommended action

Message	Reporting of attack statistics table to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of messages containing attack statistics.
Action	No recommended action

Message	Reporting of configuration logs to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of log messages for events triggered by changes in device configuration.
Action	No recommended action

Message	Reporting of configuration logs to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of log messages for events triggered by changes in device configuration.
Action	No recommended action

Message	Reporting of deep inspection alarms to ⟨*string*⟩ has been disabled
Meaning	An admin either enabled or disabled the transmission of attack alarms generated during Deep Inspection.
Action	No recommended action

Message	Reporting of deep inspection alarms to ⟨*string*⟩ has been enabled
Meaning	An admin either enabled or disabled the transmission of attack alarms generated during Deep Inspection.
Action	No recommended action

Message	Reporting of ethernet statistics table to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of messages containing ethernet statistics.
Action	No recommended action

Message	Reporting of ethernet statistics table to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of messages containing ethernet statistics.
Action	No recommended action

Message	Reporting of flow statistics table to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of messages containing traffic flow statistics
Action	No recommended action

Message	Reporting of flow statistics table to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of messages containing traffic flow statistics
Action	No recommended action

Message	Reporting of information logs to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of low-level notification log messages about non-severe changes that occur on the device, as when an authentication procedure fails.
Action	No recommended action

Message	Reporting of information logs to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of low-level notification log messages about non-severe changes that occur on the device, as when an authentication procedure fails.
Action	No recommended action

Message	Reporting of miscellaneous alarms to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of alarms generated by the security device.
Action	No recommended action

Message	Reporting of miscellaneous alarms to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of alarms generated by the security device.
Action	No recommended action

Message	Reporting of policy table to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of messages containing policy statistics.
Action	No recommended action

Message	Reporting of policy table to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of messages containing policy statistics.
Action	No recommended action

Message	Reporting of protocol distribution table to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of generated protocol distribution parameters.
Action	No recommended action

Message	Reporting of protocol distribution table to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of generated protocol distribution parameters.
Action	No recommended action

Message	Reporting of self management logs to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of log messages concerning dropped packets (such as those denied by a policy) and traffic that terminates at the security device (such as administrative traffic).
Action	No recommended action

Message	Reporting of self management logs to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of log messages concerning dropped packets (such as those denied by a policy) and traffic that terminates at the security device (such as administrative traffic).
Action	No recommended action

Message	Reporting of traffic alarms to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of alarms generated while the device monitors and records the traffic permitted by policies.
Action	No recommended action

Message	Reporting of traffic alarms to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of alarms generated while the device monitors and records the traffic permitted by policies.
Action	No recommended action

Message	Reporting of traffic logs to ⟨*string*⟩ has been disabled.
Meaning	An admin either enabled or disabled the transmission of log messages generated while the device monitors and records the traffic permitted by policies.
Action	No recommended action

Message	Reporting of traffic logs to ⟨*string*⟩ has been enabled.
Meaning	An admin either enabled or disabled the transmission of log messages generated while the device monitors and records the traffic permitted by policies.
Action	No recommended action

Message	⟨*string*⟩ has been disabled.
Meaning	An admin has configured the device to disable management by Netscreen-Security Manager.
Action	No recommended action

Message	⟨*string*⟩ has been enabled.
Meaning	An admin has configured the device to enable management by Netscreen-Security Manager.
Action	No recommended action

Message	⟨*string*⟩ ⟨*string*⟩ host has been disabled.
Meaning	An admin has disabled the Netscreen-Security Manager primary or secondary host.
Action	No recommended action

Message	⟨*string*⟩ ⟨*string*⟩ host has been set to ⟨*IP address*⟩.
Meaning	An admin has set the Netscreen-Security Manager primary or secondary host to the specified IP address.
Action	No recommended action

Message	⟨*string*⟩ ⟨*string*⟩ host has been set to ⟨*string*⟩.
Meaning	An admin has set the Netscreen-Security Manager primary or secondary host to the specified hostname.
Action	No recommended action

Message	⟨*string*⟩ VPN management tunnel has been disabled.
Meaning	A VPN tunnel for administrative traffic has been disabled.
Action	No recommended action

Message	⟨*string*⟩ VPN management tunnel has been enabled.
Meaning	A VPN tunnel for administrative traffic has been configured.
Action	No recommended action

Message	The NACN protocol has been ⟨*string*⟩
Meaning	An admin has enabled or disaled the NACN protocol. When enabled, the security device attempts to contact the server running Policy Manager whenever an interface IP address change occurs.
Action	No recommeded action

Message	Timeout value of ⟨*string*⟩ has been set to ⟨*integer*⟩ seconds (default)
Meaning	An admin has reset the Netscreen-Security Manager timeout to the default value.
Action	No recommended action

Message	Timeout value of ⟨*string*⟩ has been set to ⟨*integer*⟩ seconds.
Meaning	An admin has set the Netscreen-Security Manager timeout to the specified value.
Action	No recommended action

Message	User-defined service ⟨*string*⟩ has been added to ⟨*string*⟩ protocol distribution.
Meaning	An admin has either added or removed the specified service on the protocol distribution events report.
Action	No recommended action

Message	User-defined service ⟨*string*⟩ has been removed from ⟨*string*⟩ protocol distribution.
Meaning	An admin has either added or removed the specified service on the protocol distribution events report.
Action	No recommended action

Information (00538)

Message	Connection to ⟨*string*⟩ data collector at ⟨*IP address*⟩ has timed out.
Meaning	The connection with the data collector timed out.
Action	Confirm that the data collector is up and reachable, and is properly configured.

Message	Device is not known to ⟨*string*⟩ data collector at ⟨*IP address*⟩.
Meaning	The data collector rejected the connection with the device.
Action	Confirm that the data collector and security device are properly configured.

Message	Lost socket connection to ⟨*string*⟩ data collector at ⟨*IP address*⟩.
Meaning	The socket connection at the data collector was closed unexpectedly.
Action	Confirm that the data collector is up and reachable, and is properly configured.

Message	NACN failed to register to policy manager ⟨*string*⟩ because of ⟨*string*⟩.
Meaning	The device failed to register with the NACN policy manager for the specified reason.
Action	Confirm that the policy manager is up and reachable.

Message	NACN successfully registered to policy manager ⟨*string*⟩: ⟨*string*⟩.
Meaning	The device successfully registered with the specified NACN policy manager.
Action	No recommended action

Message	NSM request may fail due to low memory (malloc failed)
Meaning	The device failed to allocate adequate memory for an NetScreen-Security Manager request.
Action	Reduce the number of objects (interfaces, VPNs, tunnels) on the device. Consider upgrading the device memory or upgrading to a device with more memory.

Message	NSM: Cannot connect to NSM server at ⟨*IP address*⟩. Reason: ⟨*integer*⟩, ⟨*string*⟩ (⟨*integer*⟩ connect attempt(s))
Meaning	The security device tried and failed to connect to the NSM server after the specified number of connection attempts.
Action	Investigate the reason for the connection failure. Check the cables on the device and the network connections. Verify whether the NSM server is up and operational.

Message	NSM: Connected to NSM server at ⟨*IP address*⟩ (⟨*integer*⟩ connect attempt(s))
Meaning	The security device successfully connected to the NSM server after the specified number of connection attempts.
Action	No recommended action

Message	NSM: Connection to NSM server at ⟨*IP address*⟩ is down. Reason: ⟨*integer*⟩, ⟨*string*⟩
Meaning	The connection between the NSM server and the security device is down. Reason: < string >
Action	Investigate the reason for the connection failure. Check the cables on the device and the network connections. Verify whether the NSM server is up and operational.

Message	NSM: Sent ⟨*string*⟩ message
Meaning	The security device sent the specified message to NSM.
Action	No recommended action

Message	The NACN protocol has started for policy manager ⟨*integer*⟩ on hostname ⟨*string*⟩ IP address ⟨*IP address*⟩ port ⟨*integer*⟩
Meaning	The security device started the NACN protocol.
Action	No recommended action.

Chapter 37

NSRD

The following messages relate to events generated by the RD (Rapid Deployment) process.

Error (00551)

Message	Error ⟨*integer*⟩ occurred during configlet file processing.
Meaning	During attempted execution of the Configlet file, the specified error condition occurred.
Action	Consult your Security-Manager admin.

Warning (00551)

Message	Configlet file authentication failed.
Meaning	Authentication failed during execution of the Configlet.
Action	Consult your Security-Manager admin.

Message	Configlet file decryption failed.
Meaning	Decryption of the Configlet file was unsuccessful.
Action	Consult your Security-Manager admin.

Message	Error ⟨*integer*⟩ occurred, causing failure to establish secure management with Management System.
Meaning	Netscreen-Security Manager uses two components to allow remote communication with security devices. The Management System, a set of services that reside on an external server. These services process, track, and store device management information exchanged between the device and the Netscreen-Security Manager UI. The Agent, a service that resides on each managed security device. The Agent receives configuration parameters from the external Management System and pushes it to ScreenOS. The Agent also monitors the device and transmits reports back to the Management System. This error message usually means that the Agent was unable establish a management relationship between the Agent and the Management System.
Action	Consult your Security-Manager admin.

Information (00551)

Message	Rapid Deployment cannot start because gateway has undergone configuration changes.
Meaning	Because RD (Rapid Deployment) requires factory-default settings, a security device (gateway) with non-default configurations cannot use RD.
Action	Reset the device to factory default settings by executing the CLI command unset all, then save, then reset.

Message	Secure management established successfully with remote server.
Meaning	Management communication between the Agent (on the device) and the Management System (on an external host) is now established.
Action	No recommended action.

Chapter 38
NTP

The following messages relate to the Network Time Protocol (NTP).

Notification (00531)

Message	Administrator ⟨*admin_name*⟩ changed the Network Time Protocol authentication mode to ⟨*auth_mode*⟩ (⟨*config_changer*⟩)
Meaning	The named admin set the authentication mode for NTP traffic to either required or preferred.
Action	No recommended action

Message	Administrator ⟨*admin_name*⟩ changed the Network Time Protocol maximum adjustment value from ⟨*old_adj*⟩ to ⟨*new_adj*⟩ seconds (⟨*config_changer*⟩)
Meaning	The named admin changed the maximum time adjustment value to the specified number of seconds. This value represents the acceptable time difference between the security device system clock and the time received from an NTP server.
Action	No recommended action

Message	An acceptable time could not be obtained from ⟨*ntp_server_type*⟩ NTP server ⟨*ntp_server_name*⟩
Meaning	The security device could not obtain a time from the NTP server that fell within the range of the maximum adjustment value.
Action	Configure a higher maximum adjustment value.

Message	An administrator aborted the NTP time update.
Meaning	An administrator aborted the NTP update request.
Action	No recommended action

Message	An error occurred in setting the system clock.
Meaning	An unspecific error occurred when a security device attempted to set the system clock.
Action	Try to initiate the NTP update again.

Message	Authentication failed for Network Time Protocol server ⟨*ntp_server_type*⟩ ⟨*ntp_server_name*⟩ because ⟨*fail_reason*⟩
Meaning	Authentication failed between the security device and the named NTP server due to the specified reason.
Action	Check the configurations on the security device and on the NTP server.

Message	Network Time Protocol adjustment of ⟨*msec_adjustment*⟩ ms from NTP server ⟨*ntp_server_name*⟩ exceeds the allowed adjustment of ⟨*msec_adjustment_allowed*⟩ ms.
Meaning	The difference between the time received from the named NTP server and the time on the security device system clock exceeds the allowed number of milliseconds. The security device does not synchronize its clock and proceeds to try the first backup NTP server configured on the security device. If the security device does not receive a valid reply after trying all the configured NTP servers, it generates an error message in the event log.
Action	Set a larger maximum adjustment value.

Message	Network Time Protocol settings changed.
Meaning	An admin changed the NTP settings.
Action	No recommended action

Message	No acceptable time could be obtained from any NTP server.
Meaning	The security device could not obtain a time from any of the configured NTP servers.
Action	Configure a higher maximum adjustment value on the appropriate server.

Message	No NTP server could be contacted.
Meaning	The security device could not contact any of the configured NTP servers.
Action	Common reasons for an inability to connect are a cable may be disconnected, the DNS name provided may not be resolvable, or the NTP servers may be down. Test for all possible causes and when you determine the cause, take the necessary action.

Message	NTP request cannot be sent. No key found for server ⟨*ntp_server_type*⟩ ⟨*ntp_server_name*⟩
Meaning	The security device could not send a request to the NTP server because authentication was enabled, but a preshared key was not assigned to the specified server.
Action	Assign a unique key id and preshared key to each NTP server you configure on the security device.

Message	NTP request cannot be sent. No key id found for Network Time Protocol server ⟨*ntp_server_type*⟩ ⟨*ntp_server_name*⟩
Meaning	The security device could not send a request to the NTP server because authentication was enabled, but a key ID was not assigned to the specified server.
Action	Assign a unique key id and preshared key to each NTP server you configure on the security device.

Message	⟨*ntp_server_type*⟩ NTP server ⟨*ntp_server_name*⟩ could not be contacted.
Meaning	The security device could not contact the specified NTP server.
Action	Check the cables and the network connections.

Message	The system clock was updated from ⟨*ntp_server_type*⟩ NTP server type ⟨*ntp_server_name*⟩ with an adjustment of ⟨*msec_adjustment*⟩ ms. Authentication was ⟨*auth_mode*⟩. Update mode was ⟨*update_mode*⟩
Meaning	The security device synchronized its clock with the named NTP server with the specified settings.
Action	No recommended action

Notification (00548)

Message	The NetScreen device is attempting to contact the primary backup NTP server ⟨*ntp_server_name*⟩
Meaning	The security device is attempting to make a connection with the specified primary backup NTP server.
Action	No recommended action

Message	The NetScreen device is attempting to contact the primary NTP server ⟨*ntp_server_name*⟩
Meaning	The security device is attempting to make a connection with the specified primary NTP server.
Action	No recommended action.

Message	The NetScreen device is attempting to contact the secondary backup NTP server ⟨*ntp_server_name*⟩
Meaning	The security device is attempting to make a connection with the specified secondary backup NTP server.
Action	The security device is attempting to make a connection with the specified secondary backup NTP server.

Chapter 39
OSPF

The following messages relate to the Open Shortest Path First (OSPF) dynamic routing protocol.

Critical (00206)

Message	LSA flood in OSPF with router ID ⟨*self-router-id*⟩ on interface ⟨*interface-name*⟩ forced the interface to drop a packet.
Meaning	The number of Link State Advertisements that attempted to enter the interface is greater than the LSA threshold value set for the interface. When more LSAs attempt to enter the interface than the port can administer, the interface drops packets.
Action	Configure a higher LSA flood threshold value that enables the interface to manage the number of LSAs attempting to enter the interface.

Message	LSA ID ⟨*lsa-id*⟩, router ID ⟨*lsa-advertisig-router-id*⟩, type ⟨*lsa-type*⟩ cannot be deleted from the real-time database in area ⟨*lsa-area-id*⟩
Meaning	A specific LSA has protections that block an administrator from deleting it in a specific OSPF area.
Action	Remove the delete protection from the LSA in the specific OSPF area.

Message	OSPF instance with router ID ⟨*self-router-id*⟩ received a Hello packet flood from neighbor (IP address ⟨*neighbor-ip-address*⟩, router ID ⟨*neighbor-router-id*⟩) on interface ⟨*interface-name*⟩ forcing the interface to drop the packet.
Meaning	The number of Hello packets that attempted to enter the interface is greater than the Hello packet threshold value set for the interface. When more Hello packets attempt to enter the interface drops packets.
Action	Configure a higher Hello packet threshold that enables the interface to manage the number of Hello packets attempting to enter the interface.

Message	Reject second OSPF neighbor (⟨*neighbor-ip*⟩) on interface (⟨*interface name*⟩) since it's configured as point-to-point interface
Meaning	A point-to-point interface requires only one OSPF neighbor. Any others will be rejected.
Action	No recommended action

Message	The total number of redistributed routes into OSPF in vrouter (⟨*vrouter-name*⟩) exceeded system limit (⟨*system-limit*⟩)
Meaning	The total number of routes that were redistributed into OSPF exceeds the system limit.
Action	No recommended action

Notification (00038)

Message	⟨*configuration_command*⟩
Meaning	The specified configuration command is active.
Action	No recommended action

Message	⟨*set_or_unset*⟩ virtual router ⟨*vrouter_name*⟩ with the configuration command ⟨*configuration_command*⟩
Meaning	An administrator either set or unset a virtual routing instance.
Action	No recommended action

Message	⟨*set_or_unset*⟩ virtual router ⟨*vrouter_name*⟩ with the OSPF protocol ⟨*configuration_command*⟩
Meaning	An administrator either set or unset an OSPF virtual routing instance.
Action	No recommended action

Message	OSPF virtual routing instance in virtual router ⟨*vrouter_name*⟩ created.
Meaning	An administrator created or removed an OSPF routing instance in the specified virtual router.
Action	No recommended action

Message	OSPF virtual routing instance in virtual router ⟨*vrouter_name*⟩ deleted.
Meaning	An administrator created or removed an OSPF routing instance in the specified virtual router.
Action	No recommended action

Information (00541)

Message	Killing of OSPF neighbor ⟨*neighbor ip address*⟩ delayed by ⟨*delay in seconds to trigger nbr dead event*⟩ seconds, last hello packet received time ⟨*sys_up_sec when flow level last received hello packet*⟩ ms and last processed hello packet occuring at ⟨*sys_up_sec when task level last received hello packet*⟩ ms.
Meaning	Each routing instance has a flow received time and task received time transmission interval that is allowed so many seconds both can be delayed. Both the flow time and task received time took longer than the delay time allowed.
Action	Configure a higher delay time for both the flow received time and task received time transmission interval.

Message	LSA in following area aged out: LSA area ID ⟨*lsa-area-id*⟩, LSA ID ⟨*lsa-id*⟩, router ID ⟨*advertising router id*⟩, type ⟨*lsa type*⟩ in OSPF.
Meaning	When a Link State Advertisement remains in an OSPF area longer than the amount of time allowed for it to be there, the routing instance removes it or ages it out.
Action	If you want LSAs to remain in an OSPF for a longer period of time than the current age-out interval, increase the age-out interval.

Message	Neighbor router ID - ⟨*neighbor-router-id*⟩ IP address - ⟨*neighbor-ip-address*⟩ changed its state to ⟨*neighbor-state*⟩.
Meaning	An OSPF router goes through several states to form an adjacency. They are Init, Two-Way, Exchange, and Adjacency. This message indicates the specified OSPF router changed its state.
Action	No recommended action

Message	The system killed OSPF neighbor because of elapsed Hello time ⟨*time elapsed in seconds since we last received hello from this neighbor*⟩ sec (neighbor router ID ⟨*neighbor router id*⟩, IP address ⟨*neighbor ip address*⟩).
Meaning	Each router has a Hello interval assigned to it which is the number of seconds allowed to elapse between transmissions of a Hello packet. If the router waits more than the time allowed in the Hello interval to send the next Hello packet, it violates the rule and a consequence occurs. In this case, the system kills neighbor routing instance.
Action	Configure a higher Hello interval value for the neighbor virtual routing instance.

Message	OSPF interface ⟨*ospf interface name*⟩ has become inactive, kill neighbor (IP address ⟨*neighbor ip address*⟩, router ID ⟨*neighbor router-id*⟩) on this interface.
Meaning	The specified interface is disabled and the neighbor adjacency was terminated.
Action	No recommended action

Message	OSPF neighbor ⟨*neighbor ip address*⟩ timeout, with last hello packet received at time ⟨*sys_up_sec when flow level last received hello packet*⟩ ms, and last processed hello packet occurring at time ⟨*sys_up_sec when task level last received hello packet*⟩ ms, current elapsed time in seconds ⟨*current elapsed time in seconds* ⟩.
Meaning	A router sends a special packet to all its neighbors in the current routing domain at a specified interval indicating it is active. This packet is called a Hello packet. This message indicates a neighbor did not receive the Hello packet from the current virtual routing instance within the specified time interval, indicating the router may be inactive.
Action	Check to determine whether the current virtual routing instance is active. If it is inactive, perform necessary steps to determine why it crashed. if it is active, configure a higher value for the interval at which the current virtual routing instance sends a Hello packet to its neighbors.

Message	OSPF packet retransmit counter exceeds limit, killing neighbor (IP address ⟨*neighbor ip address*⟩, router ID ⟨*neighbor router-id*⟩).
Meaning	The specified interface is disabled and the neighbor adjacency was terminated.
Action	No recommended action

Message	The system killed OSPF neighbor because the current router could not see itself in the hello packet. Neighbor changed state from ⟨*neighbor-old-state*⟩ to Init state, (neighbor router-id ⟨*neighbor-router-id*⟩, ip-address ⟨*neighbor-ip-address*⟩).
Meaning	An OSPF router goes through several states to form an adjacency. They are Init, Two-Way, Exchange, and Adjacency. The current virtual routing instance did not recognize a Hello packet sent to it from a neighbor router.
Action	No recommended action

Chapter 40
PIM

These messages relate to the Protocol Independent Multicast-Sparse Mode (PIM-SM) protocol.

Alert (00602)

Message	PIMSM Error in initializing access-list change handler.
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing drp vsi elect change handler
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing interface delete handler
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing interface state change
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing IP change handler
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing MCAST policy change handler.
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing nsrp state change handler.
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing packet copy handler
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing vrouter delete handler
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PIMSM Error in initializing zone delete handler
Meaning	An error occurred when the security device started up.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Notification (00058)

Message	PIMSM interface ⟨*interface-name*⟩ accept neighbors access list ⟨*acl-id*⟩ configured
Meaning	An admin set the feature that restricts the interface to forming adjacencies with the routers in the specified access list.
Action	No recommended action

Message	PIMSM interface ⟨*interface-name*⟩ BSR border removed.
Meaning	An admin unset the specified interface as a bootstrap border.
Action	No recommended action

Message	PIMSM interface ⟨*interface-name*⟩ configured as boot-strap border
Meaning	An admin configured the specified interface as a bootstrap border. A bootstrap border processes bootstrap messages but does not forward them to any other interface.
Action	No recommended action

Message	PIMSM interface ⟨*interface-name*⟩ DR priority set to ⟨*dr-priority*⟩
Meaning	An admin set the designated router (DR) priority of the interface to the specified number.
Action	No recommended action

Message	PIMSM interface ⟨*interface-name*⟩ hello holdtime set to ⟨*hello-hold-time*⟩ seconds
Meaning	An admin set the hello holdtime on the specified interface.
Action	No recommended action

Message	PIMSM interface ⟨*interface-name*⟩ Join-Prune Interval set to ⟨*join-prune-interval*⟩ seconds
Meaning	An admin set the interval at which the specified interface sends join-prune messages to its upstream routers.
Action	No recommended action

Message	PIMSM interface ⟨*interface-name*⟩ neighbor access list removed.
Meaning	An admin removed the access list that specifies the allowed neighbor adjacencies on the specified interface.
Action	No recommended action

Message	PIMSM interface ⟨*interface-name*⟩'s Hello Interval set to ⟨*join-prune-interval*⟩ seconds
Meaning	An admin set the interval at which the specified interface sends hello messages to its neighboring routers.
Action	No recommended action

Message	PIMSM protocol configured in vrouter ⟨*vrouter-name*⟩
Meaning	An admin configured a PIM-SM routing instance on the specified virtual router.
Action	No recommended action

Message	PIMSM protocol configured on interface ⟨*interface-name*⟩
Meaning	An admin configured the PIM-SM protocol on the specified interface.
Action	No recommended action

Message	PIMSM protocol disabled in vrouter ⟨*vrouter-name*⟩
Meaning	An admin disabled PIM-SM on the specified virtual router.
Action	No recommended action

Message	PIMSM protocol disabled on interface ⟨*interface-name*⟩
Meaning	An admin disabled PIM-SM on the specified interface.
Action	No recommended action

Message	PIMSM protocol enabled in vrouter ⟨*vrouter-name*⟩
Meaning	An admin enabled PIM-SM on the specified virtual router.
Action	No recommended action

Message	PIMSM protocol enabled on interface ⟨*interface-name*⟩
Meaning	An admin enabled PIM-SM on the specified interface.
Action	No recommended action

Message	PIMSM protocol removed from vrouter ⟨*vrouter-name*⟩
Meaning	An admin deleted the PIM-SM instance from the specified virtual router.
Action	No recommended action

Message	PIMSM protocol unconfigured on interface ⟨*interface-name*⟩
Meaning	An admin unset the PIM-SM protocol on the specified interface.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM multicast group access list removed
Meaning	An admin removed the restriction that limits the virtual router to processing multicast messages only from the multicast groups in the access list.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM multicast group access-list ⟨*multicast-group-ip-address-access-list*⟩ has been configured
Meaning	The named virtual router can process PIM messages from the multicast groups in the specified access list.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM multicast group ⟨*multicast-group-ip-address*⟩ has been configured with RP access list ⟨*access-list*⟩
Meaning	The security device allows the named multicast group to accept multicast traffic only from the RPs in the specified access list.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM multicast group ⟨*multicast-group-ip-address*⟩ has been configured with source access list ⟨*access-list*⟩
Meaning	The specified multicast group can accept multicast traffic only from the sources in the access list.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM Rendezvous point access list for multicast group ⟨*multicast-group-ip-address*⟩ removed
Meaning	An admin removed the restriction on routers that can function as the RPs for the specified multicast group. Any router can now function as the RP for the multicast group.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM RP address ⟨*RP-ip-address*⟩ configured for multicast group access list ⟨*multicast-group-address-access-list*⟩ in zone ⟨*zone-name*⟩
Meaning	An admin mapped the specified RP address to the multicast groups in the access list.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM RP candidate on interface ⟨*RP-candidate-interface*⟩ configured for multicast group access list ⟨*multicast-group-address-access-list*⟩ in zone ⟨*zone-name*⟩ with priority ⟨*RP-candidate-priority*⟩ and holdtime ⟨*RP-candidate-hold-time*⟩
Meaning	An admin configured an RP candidate on the named interface for the multicast groups in the specified access list and zone.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM RP Candidate removed from zone ⟨*zone-name*⟩
Meaning	An admin removed the RP candidate from the specified zone in the virtual router.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM RP ⟨*rp-ip-address*⟩ removed from zone ⟨*zone-name*⟩
Meaning	An admin removed the specified RP from the named zone in the virtual router.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM RP Proxy removed from zone ⟨*zone-name*⟩
Meaning	An admin deleted the proxy RP instance from the specified zone in the named virtual router.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM source access list for multicast group ⟨*multicast-group-ip-address*⟩ removed
Meaning	An admin removed the restriction that limits the multicast group to accepting traffic only from the sources specified in an access list.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM SPT threshold set to infinity
Meaning	An admin set the SPT threshold to infinity; therefore the virtual router never joins the SPT.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM SPT threshold set to ⟨*packets-per-second*⟩ packets per second
Meaning	An admin set the shortest-path tree (SPT) threshold of the specified interface.
Action	No recommended action

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM zone ⟨*zone-name*⟩ configured as RP Proxy.
Meaning	An admin configured proxy RP on the specified zone in the named virtual router.
Action	No recommended action

Notification (00555)

Message	Vrouter ⟨*vrouter-name*⟩ PIMSM cannot process non-multicast address ⟨*ip-address*⟩
Meaning	The specified IP address is not a valid multicast address.
Action	Replace the invalid IP address with a valid multicast group address.

Chapter 41
PKI

The following messages relate to Public Key Infrastructure (PKI).

Notification (00535)

Message	PKI: A configurable item (⟨*item name*⟩) has changed from (⟨*old value*⟩) to (⟨*new value*⟩).
Meaning	PKI: A configurable item { Name | phone | e-mail | country | state | county/locality | organization | unit/department | IP address | e-mail to } field has changed from { string1 > to none | none to string2 | string1 to string2}.
Action	An admin has changed the specified common name (CN) field within the distinguished name (DN) of a X509 certificate request.

Message	PKI: A configurable item (⟨*item name*⟩) has changed from (⟨*old setting*⟩) to (⟨*new setting*⟩).
Meaning	PKI: A configurable item { Name | phone | e-mail | country | state | county/locality | organization | unit/department | IP address | e-mail to } field has changed from { string1 to none | none to string2 > | string1 to string2}.
Action	An admin has changed the specified common name (CN) field within the distinguished name (DN) of a X509 certificate request.

Message	PKI: Adjusted key pair length from 0 to 1024 bits.
Meaning	An admin has attempted to generate a public/private key pair with a key length of 0, which is invalid. To correct this problem, the security device automatically adjusted the length to the default: 1024 bits.
Action	No recommended action

Message	PKI: An incoming certificate is broken.
Meaning	The security device was unable to decode the certificate data that it received. One reason might be that the peer's certificate was incorrectly formatted.
Action	To determine the source of the certificate, consult the event log messages surrounding this PKI (most likely IKE or SSL messages). Then ask the peer to check the certificate, and if it is valid, to send it again.

Message	PKI: Auto-generated self-signed cert was deleted.
Meaning	An administrator deleted the self-signed certificate that the security device had generated automatically.
Action	No recommended action

Message	PKI: Cannot access OCSP server to get revocation status for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device attempted to check the revocation status of the certificate with the specified subject name online using Online Certificate Status Protocol (OCSP), but it was unable to access the OCSP server.
Action	Check that the security device has network connectivity to the OCSP server.

Message	PKI: Cannot auto generate a self-signed cert.
Meaning	The security device was unable to generate a self-signed certificate automatically.
Action	Attempt to create a self-signed certificate manually. (For details, refer to the Concepts and Examples ScreenOS Reference Guide.) If you cannot generate a self-signed certificate manually, contact Juniper Networks technical support: Open a support case using the Case Manager link at www.juniper.net/support Call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot build certificate chain for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was unable to build a certificate chain for the certificate with the specified subject name. Starting with an end entity certificate and ending with a root certificate authority (CA) certificate (or that of a trusted subordinate CA), a certificate chain is a hierarchy of certificates, each of which issued the one preceding it in the chain. The security verifies the validity of each certificate in the chain except the topmost certificate, which must be preloaded on the security device and is considered as a trust anchor.
Action	Request the peer to use a different certificate.

Message	PKI: Cannot compose HTTP packet to send to URL ⟨*url string*⟩.
Meaning	The security device was unable to create an HTTP packet to send to the specified URL. The PKI module uses HTTP for online certificate retrieval, OCSP certificate revocation checking, SCEP certificate requests.
Action	Check if the amount of available RAM is low. (To see how much RAM has been allocated and how much is still available, use the get memory command.) If it is unaccountably low, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot connect to LDAP server ⟨*peer host name*⟩:⟨*peer port*⟩ through ⟨*local outgoing interface name*⟩.
Meaning	The security device was unable to establish a connection to an LDAP server at the specified address and port number through the specified outgoing interface.
Action	Check that the LDAP server settings are correct and that the security device can establish a network connection with the LDAP server.

Message	PKI: Cannot contact HTTP server at URL ⟨*url string*⟩.
Meaning	The security device was unable to contact the Hypertext Transfer Protocol (HTTP) server at the specified URL address while attempting to do one of the following operations: Request a certificate using Simple Certificate Enrollment Protocol (SCEP) Check the status of a peer's certificate using Online Certificate Status Protocol (OCSP) Retrieve a certificate revocation list (CRL) from an online CRL server
Action	Check that the security device has network connectivity to the server at the specified URL.

Message	PKI: Cannot create a socket to URL ⟨*url string*⟩.
Meaning	The security device was unable to contact the Hypertext Transfer Protocol (HTTP) server at the specified URL address while attempting to do one of the following operations: Request a certificate using Simple Certificate Enrollment Protocol (SCEP) Check the status of a peer's certificate using Online Certificate Status Protocol (OCSP) Retrieve a certificate revocation list (CRL) from an online CRL server
Action	Check that the security device has network connectivity to the server at the specified URL and that a route table entry exists to allow connectivity to the server.

Message	PKI: Cannot decode CRL data.
Meaning	The security device cannot decode the certificate revocation list (CRL) because it has become corrupted when loading it from flash memory.
Action	Save a new CRL on the security device.

Message	PKI: Cannot decrypt public key of cert with subject name ⟨*certificate subject name*⟩.
Meaning	After processing the peer certificate with the specified subject name, the security device was unable to decrypt its public key, possibly because the certificate became corrupted after its processing.
Action	Contact Juniper Networks technical support.

Message	PKI: Cannot delete the key-pair object for cert with subject name ⟨*subject name*⟩.
Meaning	The security device was unable to locate or delete a public/private key pair.
Action	If the security device fails to locate a key pair, generate a new public/private key pair. If this action does not correct the problem, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot extract SCEP SUCCESS response. Error: ⟨*error reason*⟩, for cert request with subject name ⟨*cert subject name*⟩.
Meaning	The security device was unable to extract data from a response to a certificate request with the specified subject name through SCEP. The error identifies the type of error that caused the failure.
Action	Check the available amount of memory by entering the get memory command. If a sufficient amount of memory appears to be available, make another certificate request to the SCEP server. If there appears to be a severe memory problem or if the second attempt was unsuccessful, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot generate cert request. Reason: ⟨*reason of failure*⟩ (subject name ⟨*subject name*⟩).
Meaning	The security device was unable to generate a PKCS #10 file to use when requesting a certificate.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot generate PKCS #10 file for certificate request.
Meaning	The security device was unable to generate a certificate request file in PKCS #10 (Certificate Request Syntax Standard) format.
Action	Enter the get memory command to see how much RAM has been allocated and how much is still available. If there appears to be sufficient RAM available, reboot the security device and attempt to generate certificate request again. If there appears to be a severe memory problem or if your second attempt was also unsuccessful, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot generate ⟨*key type string*⟩ key pair with subject name ⟨*subject name*⟩.
Meaning	The security device was unable to generate an RSA or DSA public/private key pair to use when requesting a certificate with the specified subject name.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot generate SCEP data. Cmd: ⟨*command*⟩, error: ⟨*error reason*⟩, for cert request with subject name ⟨*cert subject name*⟩.
Meaning	The security device was unable to generate the data to make a certificate request with the specified subject name through SCEP. The command identifier refers to an internal processing command, and the error identifies the type of error that caused the failure.
Action	Check the available amount of memory by entering the get memory command. If a sufficient amount of memory appears to be available, attempt to resubmit the certificate request. If there appears to be a severe memory problem or if your second attempt was unsuccessful, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot initiate SCEP request with subject name ⟨*cert subject name*⟩.
Meaning	The security device was unable to initiate a certificate request with the specified subject name through SCEP.
Action	Check the available amount of memory by entering the get memory command. If a sufficient amount of memory appears to be available, make another certificate request to the SCEP server. If there appears to be a severe memory problem or if your second attempt was unsuccessful, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot load CRL for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was unable to load a certificate revocation list (CRL) for the certificate with the specified subject name from an outside source to RAM because of limited available RAM.
Action	Enter the get memory command to see how much RAM has been allocated and how much is still available. If there appears to be sufficient RAM available, reboot the security device and attempt to load the CRL again. If there appears to be a severe memory problem or if your second attempt was also unsuccessful, contact

Message	PKI: Cannot load item from flash. Reason: ⟨*reason string*⟩, type: ⟨*type object*⟩, DN: ⟨*distinguished name*⟩.
Meaning	When the security device attempted to load PKI objects from flash memory to RAM during the bootup process, it was unable to load the object with the specified distinguished name (DN). The message indicates the type of PKI object and the reason it was unable to load it.
Action	Check which object the security device was unable to load. If possible, save the object to flash again from an external source. Then reboot the security device. If the problem persists, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot load ⟨*file type*⟩ file.
Meaning	The security device cannot load the specified PKI object from an outside source to RAM. The filename can be the name of a certificate or certificate revocation list (CRL).
Action	Enter the get memory command to see how much RAM has been allocated and how much is still available. If there appears to be a severe memory problem, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot locate config for CA with ID ⟨*id number of CA certificate*⟩.
Meaning	An admin upgraded the device to ScreenOS 5.0.0 from a version of ScreenOS earlier than ScreenOS 4.0.0. Because these earlier ScreenOS versions used a global internal storage space for all certificate authority (CA) configurations instead of storage on a per-CA basis, the security device was unable to find a CA-specific configuration. During the upgrade procedure, the security device automatically created individual storage spaces for each CA.
Action	No recommended action

Message	PKI: Cannot locate key pair with ID ⟨*key id number*⟩ for SCEP.
Meaning	When attempting to submit a certificate request via Simple Certificate Enrollment Protocol (SCEP), the security device was unable to locate the specified public/private key pair.
Action	Use the following CLI command to check that a key pair exists for this ID number: get pki x509 list key-pair.

Message	PKI: Cannot locate the key-pair object for cert with subject name ⟨*subject name*⟩.
Meaning	The security device was unable to locate or delete a public/private key pair.
Action	If the security device fails to locate a key pair, generate a new public/private key pair. If this action does not correct the problem, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot retrieve the ⟨*type of object*⟩ with subject name ⟨*subject name*⟩.
Meaning	The security device was unable to load the PKI object with the specified subject name into RAM from the PKI storage space in flash memory.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot return to the original certificate chain. Cookies: (⟨*certificate chain identifier*⟩x)(⟨*certificate chain identifier*⟩x)(⟨*certificate chain identifier*⟩x)(⟨*certificate chain identifier*⟩x).
Meaning	While the security device used the Online Certificate Status Protocol (OCSP) to perform a certificate revocation check, the certificate chain sent by the peer expired.
Action	Evaluate the verification checking procedure for the certificates in the chain that the security device forwards to the OCSP server. Verifying multiple certificates in a chain through OCSP might exceed the certificate verification timeout interval. Also, check that the revocation check settings are accurate. If they are accurate, check how long the revocation check took. If it took a long time, check if the server is online and responding.

Message	PKI: Cannot save CA config (CA cert subject name ⟨*CA certificate subject name*⟩).
Meaning	An admin's attempt to save the certificate authority (CA) configuration settings for a CA was unsuccessful because the number of objects in the internal PKI storage space had already reached the maximum limit.
Action	Remove obsolete or unneeded PKI objects from the internal PKI storage space to lower the number of objects below the maximum limit. Consult the data sheet for your security device to see the maximum number of PKI objects allowed in the internal PKI storage space. Each device has a different maximum.

Message	PKI: Cannot save CA configuration (CA cert subject name ⟨*CA certificate subject name*⟩).
Meaning	An admin attempted to save the certificate authority (CA) certificate with the specified subject name, but the attempt failed.
Action	No recommended action

Message	PKI: Cannot save new item to flash. Max: (⟨*max size allowed for flash*⟩), item: (⟨*got size to be saved to flash*⟩).
Meaning	The security device was unable to save a PKI object to flash memory. The message includes the maximum amount of PKI storage space and the size of the object that it was unable to save.
Action	Remove unused PKI objects to free up more space, and then attempt to save the PKI object again.

Message	PKI: Cannot save the key-pair object for cert with subject name ⟨*subject name*⟩.
Meaning	An admin unsuccessfully attempted to save the key pair for the certificate with specified subject name to flash memory but the key pair was corrupted.
Action	Try to generate a new key pair.

Message	PKI: Cannot save the ⟨*object type name*⟩ with subject name ⟨*subject name*⟩.
Meaning	An admin unsuccessfully attempted to save the PKI object with the specified subject name to flash memory.
Action	Remove obsolete or unneeded PKI objects from the internal PKI storage space to lower the number of objects below the maximum limit. Consult the data sheet for your security device to see the maximum number of PKI objects allowed in the internal PKI storage space. Each device has a different maximum.

Message	PKI: Cannot send HTTP packet through socket to URL ⟨*url string*⟩.
Meaning	The security device was unable to contact the Hypertext Transfer Protocol (HTTP) server at the specified URL address while attempting to do one of the following operations: Request a certificate using Simple Certificate Enrollment Protocol (SCEP) Check the status of a peer's certificate using Online Certificate Status Protocol (OCSP) Retrieve a certificate revocation list (CRL) from an online CRL server
Action	Check that the security device has network connectivity to the server at the specified URL and that a route table entry exists to allow connectivity to the server.

Message	PKI: Cannot send PKCS #10 cert request to e-mail address ⟨*email address*⟩.
Meaning	The security device was unable to send the PKCS #10 certificate request to the specified e-mail address.
Action	Ensure that the Simple Mail Transfer Protocol (SMTP) configuration settings on the security device and the e-mail address of the recipient are correct, and then try again.

Message	PKI: Cannot store config for CA with cert subject name ⟨*CA certificate subject name*⟩.
Meaning	An admin unsuccessfully attempted to save configuration settings for the certificate authority (CA) whose CA certificate contains the specified subject name. However, the number of objects in the internal PKI storage space had already reached the maximum limit.
Action	Remove obsolete or unneeded PKI objects from the internal PKI storage space to lower the number of objects below the maximum limit. Consult the data sheet for your security device to see the maximum number of PKI objects allowed in the internal PKI storage space. Each device has a different maximum.

Message	PKI: Cannot sync data to NSRP peer. (command ⟨*command*⟩).
Meaning	The local security device in an NSRP cluster was unable to synchronize PKI data with another member in the NSRP cluster. When one member of an NSRP cluster attempted a cold sync of its PKI objects with another member of the cluster, one of the following synchronization commands failed: 0x00010000: synchronize certificate files 0x00020000: synchronize RSA key files 0x00030000: synchronize DSA key files 0x00040000: synchronize deleted X.509 objects 0x00050000: synchronize the refreshed trust store 0x00060000: synchronize deleted CRLs 0x00070000: synchronize SCEP local certificates 0x00080000: synchronize SCEP CA certificates 0x00090000: synchronize added CA configurations 0x000A0000: synchronize deleted CA configurations 0x000B0000: synchronize added CRLs 0x000C0000: synchronize deleted RSA keys 0x000D0000: synchronize deleted DSA keys The cold sync operation automatically synchronizes all PKI objects such as certificate revocation lists (CRLs), public/private key pairs, local certificates, certificate authority (CA) certificates, and certificate authority configurations between two NSRP cluster members. The operation synchronizes the objects in blocks of 30 items each. If a cold sync attempt is unsuccessful, the cluster members can make up to a total of 30 attempts to synchronize them.
Action	Check that the devices are correctly configured for NSRP. If the configuration is correct and the problem persists, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot sync ⟨*name of the object*⟩ to NSRP peer. (command ⟨*command*⟩).
Meaning	The local security device in an NSRP cluster was unable to synchronize the specified PKI object with another member in the NSRP cluster. The command number at the end of the message represents an internal identifying number for the type of data being sent.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cannot verify cert for ScreenOS image authentication.
Meaning	The security device was unable to verify the signature of the image authentication certificate when loading a new ScreenOS image.
Action	Check the signature of the image signer certificate.

Message	PKI: Cannot verify OCSP responder cert with subject name ⟨*certificate subject name*⟩.
Meaning	When checking the revocation status of the certificate with the specified subject name online using Online Certificate Status Protocol (OCSP), the security device was unable to verify the signature on the response from the OCSP server.
Action	Contact the OCSP server admin to check that the signature on the OCSP response is signed with the correct private key.

Message	PKI: Cannot verify signature on OCSP response for cert with subject name ⟨*certificate subject name*⟩.
Meaning	When checking the revocation status of the certificate with the specified subject name online using Online Certificate Status Protocol (OCSP), the security device was unable to verify the digital signature on the response from the OCSP server.
Action	Contact the OCSP server admin to check that the signature on the OCSP response is signed with the correct private key.

Message	PKI: Cannot wrap SCEP request. Error: ⟨*error reason*⟩, for cert request with subject name ⟨*cert subject name*⟩.
Meaning	When the security device attempted to submit a certificate request through the Simple Certificate Enrollment Protocol (SCEP), it was unable to wrap a certificate request file using the Public Key Cryptography Standards (PKCS) #7 Cryptographic Message Syntax Standard. When submitting a certificate request via SCEP, the security device generates both an inner and outer envelope in PKCS #7 format.
Action	Check the available amount of memory by entering the get memory command. If a sufficient amount of memory appears to be available, attempt to resubmit the certificate request. If there appears to be a severe memory problem or if your second attempt was unsuccessful, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Cert has expired (subject name ⟨*certificate subject name*⟩).
Meaning	When the security device received the certificate with the specified subject name, it checked its validity period and discovered that it had expired. Consequently, the security device rejected the certificate.
Action	Ask the peer to use a certificate that is currently valid.

Message	PKI: Cert is not yet valid (subject name ⟨*certificate subject name*⟩).
Meaning	When the security device received the certificate with the specified subject name, it checked its validity period and discovered that the starting date had not yet occurred. Consequently, the security device rejected the certificate.
Action	Check whether the system clock on the security device is set properly. If it is, ask the peer to use a certificate that is currently valid.

Message	PKI: Cert requested already exists for subject name ⟨*cert subject name*⟩.
Meaning	When making a certificate request through the Simple Certificate Enrollment Protocol (SCEP), the security device detected that it already has a certificate identical to the requested one on the device. Consequently, the security device aborted the certificate request.
Action	Do not repeat the certificate request for that particular certificate, or remove the existing request.

Message	PKI: Certificate chain is too long for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device received a certificate chain with more than eight certificates. The first certificate in the chain is identified by its subject name. Because the chain was too long, the security device rejected the certificate.
Action	Notify the peer to use a shorter certificate chain, or load a certificate authority (CA) certificate lower in the trust hierarchy to shorten the chain between the peer's certificate and the trust anchor. (A trust anchor is a CA certificate loaded on the security device that verifies the validity of other certificates issued under it in a hierarchy of trust.)

Message	PKI: Certificate has been revoked (subject name ⟨*certificate subject name*⟩).
Meaning	After checking a certificate revocation list (CRL), the security device discovered that the certificate authority (CA) had revoked the certificate with the specified subject name.
Action	Request the peer to use a different, valid certificate.

Message	PKI: Completed NSRP cold start sync after ⟨*number of attempts*⟩ attempts.
Meaning	NSRP cluster members were able to successfully complete a cold sync operation at the specified attempt. The operation synchronizes PKI objects in blocks of 30 items each. If a cold sync attempt is unsuccessful, the cluster members can make up to a total of 30 attempts to synchronize them.
Action	No recommended action

Message	PKI: Completed SCEP cert request.
Meaning	The security device successfully generated and submitted a certificate request through the Simple Certificate Enrollment Protocol (SCEP).
Action	No recommended action

Message	PKI: CRL cannot be saved to flash, issuer (⟨*issuer subject name*⟩).
Meaning	The security device was unable to save the certificate revocation list (CRL) from the specified certificate authority (CA).
Action	Remove unused or expired CRLs to free up more space. To see the maximum limit for storage space in flash memory per CRL, consult the data sheet for your security device. Each device has a different maximum.

Message	PKI: CRL has a bad timestamp. (CA ⟨*issuer subject name*⟩).
Meaning	In attempting to verify that a certificate issued by the specified certificate authority (CA) had not been revoked, the security device checked the certificate revocation list (CRL). However, when it did so, it discovered that the timestamp was invalid. Consequently, the security device was unable to use the CRL.
Action	Reload the CRL, or obtain a new CRL from the CA.

Message	PKI: CRL has bad signature for cert with subject name ⟨*certificate subject name*⟩.
Meaning	When attempting to authenticate a certificate revocation list (CRL), the security device discovered that its digital signature was invalid. The CRL was for the certificate authority (CA) that issued the end-entity certificate with the specified subject name. A digital signature of the CRL is a digest that the CA encrypted with its private key. To check that signature is valid, the security device uses the CA's public key to decrypt it. The security device then uses the same hashing algorithm that the CA used to create the first hash. Finally, the security device compares the two hashes. If they match, then the signature is valid by virtue of the fact that private key that encrypted the digest belongs to the same key pair as the public key that decrypted it. Furthermore, because the public key comes from the CA's certificate, the private key must also belong to the CA.
Action	Check that the correct CRL options and CRL URL settings were configured on the security device for this particular CA. If the configuration is correct, contact the CA to check if the CRL is valid.

Message	PKI: CRL has expired for cert with subject name ⟨*certificate subject name*⟩.
Meaning	When the security device checked the certificate revocation list (CRL) for the certificate authority (CA) that issued the certificate with the specified subject name, it discovered that the CRL might already be expired.
Action	Obtain a currently valid CRL.

Message	PKI: CRL has expired. (CA ⟨*issuer subject name*⟩).
Meaning	The certificate revocation list (CRL) for the specified certificate authority (CA) has expired.
Action	Load a currently valid CRL.

Message	PKI: CRL is not issued by the CA that signed the cert with subject name ⟨*certificate subject name*⟩.
Meaning	A different certificate authority (CA) signed the certificate revocation list (CRL) from the CA that signed the certificate with the specified subject name.
Action	Check that the correct CRL options and CRL URL settings were configured on the security device for this particular CA.

Message	PKI: CRL is not yet valid for cert with subject name ⟨*certificate subject name*⟩.
Meaning	When the security device checked the certificate revocation list (CRL) for the certificate authority (CA) that issued the certificate with the specified subject name, it discovered that the starting date of the CRL validity period had not yet occurred.
Action	The typical cause for such a message is that the system clock on the security device is not set properly. Therefore, check the system clock.

Message	PKI: CRL is too big (⟨*size of CRL*⟩) to load. Max: ⟨*max size allowed for flash*⟩, CA: ⟨*issuer subject name*⟩.
Meaning	The security device cannot load the certificate revocation list (CRL) from the specified certificate authority (CA) to RAM because it is too big.
Action	Consider checking the revocation status of certificates from Online Certificate Status Protocol (OCSP) for this CA. To see the maximum limit for storage space in flash memory per CRL, consult the data sheet for your security device. Each device has a different maximum.

Message	PKI: CRL is too big (⟨*size of CRL*⟩) to save to flash. Max: ⟨*max size allowed for flash*⟩, CA: ⟨*issuer subject name*⟩.
Meaning	The security device cannot save the certificate revocation list (CRL) from the specified certificate authority (CA) because it would exceed the maximum limit for storage space in flash memory.
Action	Remove unused or expired CRLs to free up more space. If that is not possible, you need to ensure that the CRL is available online, or manually load it after each device reboot.

Message	PKI: CRL server closed LDAP socket when verifying cert with subject name ⟨*certificate subject name*⟩.
Meaning	While verifying a certificate, the socket to the certificate revocation list (CRL) server was closed by server.
Action	Check that the security device has network connectivity to the server at the specified URL and that a route table entry exists to allow connectivity to the server.

Message	PKI: CRL will be refreshed as configured on the interupdate refresh setting. (CA ⟨*issuer subject name*⟩).
Meaning	As configured on the interupdate refresh setting, the security device will soon attempt to refresh the certificate revocation list (CRL) for the specified certificate authority (CA) because the CRL is about to expire.
Action	No recommended action

Message	PKI: Failed to obtain CRL for CA issuing cert with subject name ⟨*certificate subject name*⟩.
Meaning	When attempting to verify the certificate with the specified subject name, the security device was unable to obtain the certificate authority (CA)'s certificate revocation list (CRL). The security device checks for CRLs in its internal PKI object storage space and online. For online CRL checking, the security device uses the URL specified in the distribution point extension contained in the end-entity certificate. If the certificate does not include a CRL distribution point, the security device uses the URL configured for that CA on the security device.
Action	Check that the correct CRL options and CRL URL settings were configured on the security device. Also verify that you can get the CRL online. If not, obtain a valid CRL and load it on the security device manually.

Message	PKI: Failed to obtain object ID (⟨*object id number*⟩x)(⟨*object id number*⟩).
Meaning	Because the PKI objects stored in two NSRP cluster members were not synchronized when an admin attempted to add a new object, the ID number of one member's PKI object conflicted with the number that the other tried to assign the new object. The ID number is presented in both hexadecimal and decimal formats.
Action	For a situation involving NSRP: Synchronize the PKI objects on both NSRP members first, and then add the new item. If this occurs while the security device is operating by itself, you can try to resolve the problem by removing some unused or obsolete objects and then attempting to save the object again. However, such an issue might indicate an internal problem. Therefore, if the problem persists, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Format error in CRL lastUpdate field for cert with subject name ⟨*certificate subject name*⟩.
Meaning	When the security device retrieved the certificate revocation list (CRL) for the certificate authority (CA) that issued the certificate with the specified subject name, it discovered that either the "lastUpdate" or "nextUpdate" field was improperly formatted. Consequently, the security device was unable to verify if the CRL was valid.
Action	Obtain another CRL with correct formatting.

Message	PKI: Format error in CRL nextUpdate field for cert with subject name ⟨*certificate subject name*⟩.
Meaning	When the security device retrieved the certificate revocation list (CRL) for the certificate authority (CA) that issued the certificate with the specified subject name, it discovered that either the "lastUpdate" or "nextUpdate" field was improperly formatted. Consequently, the security device was unable to verify if the CRL was valid.
Action	Obtain another CRL with correct formatting.

Message	PKI: Format error in the notAfter field of cert with subject name ⟨*certificate subject name*⟩.
Meaning	When the security device received the certificate with the specified subject name from a peer, it checked the period of time during which the certificate is valid. However, because either the "notBefore" or "notAfter" field was improperly formatted, the security device was unable to verify if the certificate was valid.
Action	Notify the IKE peer to use a different certificate because it is unclear if the one sent is valid.

Message	PKI: Format error in the notBefore field of cert with subject name ⟨*certificate subject name*⟩.
Meaning	When the security device received the certificate with the specified subject name from a peer, it checked the period of time during which the certificate is valid. However, because either the "notBefore" or "notAfter" field was improperly formatted, the security device was unable to verify if the certificate was valid.
Action	Notify the IKE peer to use a different certificate because it is unclear if the one sent is valid.

Message	PKI: Incorrect fingerprint for CA cert with subject name ⟨*CA cert subject name*⟩.
Meaning	The security device rejected the fingerprint, or hash digest, of the certificate authority (CA) certificate containing the specified subject name. The digest is used to verify the integrity of the certificate. If the digest that the security device produces does not match the digest that the peer sent, the content might have been altered between the creation of the two digests and thus cannot be trusted.
Action	Contact the CA and request another CA certificate.

Message	PKI: Internal configuration error. Cannot verify cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device cannot find the internal configuration information for the certificate authority (CA) that issued the certificate with the specified subject name.
Action	Verify that the CA certificate is loaded and that its attribute settings are correctly configured.

Message	PKI: Invalid certificate (subject name ⟨*certificate subject name*⟩).
Meaning	The security device has determined that the certificate with the specified subject name is invalid.
Action	Request the peer to use a different, valid certificate.

Message	PKI: item in flash file incorrect, type(%8x) len(⟨*integer*⟩).
Meaning	A PKI object of the specified type and length (in kilobytes) is no longer valid. (This message might appear after downgrading to an earlier ScreenOS release.)
Action	Check all the PKI objects and determine what is missing. After you discover the missing item, you might be able to reload it. If that is not possible, you might have to regenerate the lost item; for example, by requesting a new certificate to replace the one that is no longer valid.

Message	PKI: LDAP bind operation timed out for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device attempted to validate the status of the certificate with the specified subject name by checking an online certificate revocation list (CRL). However, the CRL server did not respond to the inquiry.
Action	No recommended action.

Message	PKI: LDAP cannot search for DN (⟨*Distinguished name*⟩) using filter (⟨*filter*⟩).
Meaning	While attempting to retrieve a certificate revocation list (CRL) from an online LDAP server to check the revocation status of a certificate, the search filter employed by the LDAP server was unable to locate the specified distinguished name (DN).
Action	Check that the LDAP server settings are correct.

Message	PKI: LDAP modify add is not supported.
Meaning	The certificate has been verified.
Action	Check that the LDAP server settings are correct.

Message	PKI: LDAP modify delete is not supported.
Meaning	The certificate has been verified.
Action	Check that the LDAP server settings are correct.

Message	PKI: LDAP operation timed out for cert with subject name ⟨*certificate subject name*⟩.
Meaning	When the security device attempted to retrieve a certificate revocation list (CRL) for the peer's certificate with the specified subject name, the search operation timed out before it was completed.
Action	Check that the LDAP server settings are correct for the certificate authority (CA) that issued the peer's certificate.

Message	PKI: Loaded a flash file with PKI data in an earlier format (version 0).
Meaning	The security device loaded a version of the certificate database that is earlier than the current version. This action can occur if the security device is an older model.
Action	No recommended action

Message	PKI: No response for status inquiry for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device attempted to validate the status of the certificate with the specified subject name by checking an online certificate revocation list (CRL). However, the CRL server did not respond to the inquiry.
Action	Check that the security device has the correct CRL options and CRL URL settings for the certificate authority (CA) that issued the certificate whose status you want to validate.

Message	PKI: No revocation check, per config, for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device accepted the certificate with the specified subject name without checking its status on a certificate revocation list (CRL). (Note: For security reasons, security does not recommend disabling CRL checking.)
Action	No recommended action

Message	PKI: NSRP cold start sync attempt ⟨*current attempt*⟩ failed.
Meaning	During a cold sync operation between members of an NSRP cluster, the security devices were unable to synchronize all PKI objects at the specified cold sync attempt. The cold sync operation automatically synchronizes all PKI objects such as certificate revocation lists (CRLs), public/private key pairs, local certificates, certificate authority (CA) certificates, and certificate authority configurations between two NSRP cluster members. The operation synchronizes the objects in blocks of 30 items each. If a cold sync attempt is unsuccessful, the cluster members can make up to a total of 30 attempts to synchronize them.
Action	If, after 30 attempts, the NSRP cluster members were unable to synchronize the PKI objects, manually synchronize the objects by entering one of the following commands: If RTO synchronization is enabled, enter exec nsrp sync global-config run (which does not require rebooting the device), and then exec nsrp sync rto pki from peer. If RTO synchronization is disabled, enter exec nsrp sync global-config save, then reboot the device.

Message	PKI: NSRP cold start sync failed.
Meaning	During a cold sync operation between members of an NSRP cluster, the security devices were unable to synchronize all PKI objects after the maximum number of synchronization attempts (30). The cold sync operation automatically synchronizes all PKI objects such as certificate revocation lists (CRLs), public/private key pairs, local certificates, certificate authority (CA) certificates, and certificate authority configurations between two NSRP cluster members. The operation synchronizes the objects in blocks of 30 items each. If a cold sync attempt is unsuccessful, the cluster members can make up to a total of 30 attempts to synchronize them.
Action	If, after 30 attempts, the NSRP cluster members were unable to synchronize the PKI objects, manually synchronize the objects by entering one of the following commands: If RTO synchronization is enabled, enter exec nsrp sync global-config run (which does not require resetting the device), and then exec nsrp sync rto pki from peer. If RTO synchronization is disabled, enter exec nsrp sync global-config save, then reset the device.

Message	PKI: NSRP cold start sync for ⟨*number of items in this cold start sync session*⟩ items.
Meaning	When the local security device came online in an NSRP cluster, an existing cluster member started a cold sync of the specified number of PKI objects from itself to the newly arrived member. The cold sync operation automatically synchronizes all PKI objects such as certificate revocation lists (CRLs), public/private key pairs, local certificates, certificate authority (CA) certificates, and certificate authority configurations between two NSRP cluster members. The operation synchronizes the objects in blocks of 30 items each. If a cold sync attempt is unsuccessful, the cluster members can make up to a total of 30 attempts to synchronize them.
Action	No recommended action

Message	PKI: NSRP cold start sync session cannot locate item ⟨*index number of an item*⟩.
Meaning	When attempting to cold sync PKI objects between members of an NSRP cluster, the security device was unable to locate the specified object. The cold sync operation automatically synchronizes all PKI objects such as certificate revocation lists (CRLs), public/private key pairs, local certificates, certificate authority (CA) certificates, and certificate authority configurations between two NSRP cluster members. The operation synchronizes the objects in blocks of 30 items each. If a cold sync attempt is unsuccessful, the cluster members can make up to a total of 30 attempts to synchronize them.
Action	If, after 30 attempts, the NSRP cluster members were unable to synchronize the PKI objects, manually synchronize the objects by entering one of the following commands: If RTO synchronization is enabled, enter exec nsrp sync global-config run (which does not require resetting the device), and then exec nsrp sync rto pki from peer. If RTO synchronization is disabled, enter exec nsrp sync global-config save, and then reset the device.

Message	PKI: NSRP cold start sync session interrupted by normal sync item.
Meaning	During a cold sync operation between members of an NSRP cluster, the local security device received an PKI object that was not in the list of items being synchronized and stopped the current cold sync attempt. If one cold sync attempt is unsuccessful, the cluster members can make up to 29 more attempts to synchronize them. The cold sync operation automatically synchronizes all PKI objects such as certificate revocation lists (CRLs), public/private key pairs, local certificates, certificate authority (CA) certificates, and certificate authority configurations between two NSRP cluster members. The operation synchronizes the objects in blocks of 30 items each.
Action	If, after 30 attempts, the NSRP cluster members were unable to synchronize the PKI objects, manually synchronize the objects by entering one of the following commands: If RTO synchronization is enabled, enter exec nsrp sync global-config run (which does not require resetting the device), and then exec nsrp sync rto pki from peer. If RTO synchronization is disabled, enter exec nsrp sync global-config save, then reset the device.

Message	PKI: NSRP cold start sync. Received item ⟨*number of currently received item*⟩ before first item.
Meaning	At the start of a cold sync operation between members of an NSRP cluster, the local security device initially received an PKI object other than the first one in the PKI object table. When NSRP cluster members perform a cold sync of PKI objects, the sender sends the objects in the order in which they appear in the PKI table in flash memory. If the transmission begins with any object other than the first one, the devices stop the current cold sync attempt, and begin another one. Cluster members can make up to a total of 30 attempts to synchronize PKI objects.
Action	If, after 30 attempts, the NSRP cluster members were unable to synchronize the PKI objects, manually synchronize the objects by entering one of the following commands: If RTO synchronization is enabled, enter exec nsrp sync global-config run (which does not require resetting the device), and then exec nsrp sync rto pki from peer. If RTO synchronization is disabled, enter exec nsrp sync global-config save, then reset the device.

Message	PKI: NSRP cold start sync. Received item ⟨*number of currently received item*⟩ out of order, expecting ⟨*number of expected item*⟩ of ⟨*number of total items in this session*⟩.
Meaning	During a cold start sync operation between members of an NSRP cluster, the local security device received an PKI item out of numerical order. The security device expected to receive item number2 but received item number1 instead. When NSRP cluster members perform a cold sync of PKI objects, the sender notifies the receiver of the total number of objects to expect. It then sends them in the order in which they appear in the PKI object table in flash memory. If an object arrives out of order, the devices stop the current cold sync attempt, and begin another one. Cluster members can make up to a total of 30 attempts to synchronize PKI objects.
Action	If, after 30 attempts, the NSRP cluster members were unable to synchronize the PKI objects, manually synchronize the objects by entering one of the following commands: If RTO synchronization is enabled, enter exec nsrp sync global-config run (which does not require resetting the device), and then exec nsrp sync rto pki from peer. If RTO synchronization is disabled, enter exec nsrp sync global-config save, and then reset the device.

Message	PKI: Number of PKI objects exceeds storage maximum (⟨*maximum number of items in storage*⟩).
Meaning	The number of PKI objects that the security device has attempted to store in its database is greater than the maximum limit specified. Typical PKI objects are certificate revocation lists (CRLs), public/private key pairs, local certificates, certificate authority (CA) certificates, pending certificates, and certificate authority configurations.
Action	Free up space in the flash memory by removing obsolete or unused objects from the database.

Message	PKI: OCSP response was inconclusive for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The result of the revocation status check of the certificate with the specified subject name online using Online Certificate Status Protocol (OCSP) was inconclusive.
Action	Check that the correct OCSP server is configured for the certificate authority (CA) that issued the specified certificate.

Message	PKI: Out of memory. Cannot process cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device does not have enough memory to process the certificate.
Action	Restart the device, then make another attempt.

Message	PKI: Per config, accepted cert even though CRL has a bad signature. (subject name ⟨*certificate subject name*⟩).
Meaning	The security device was unable to verify the digital signature on the certificate revocation list (CRL) and, therefore, was unable to trust the CRL. Still, because the configuration instructs the security device to accept certificates even if it cannot verify the signature on the CRL, the security device accepted the certificate with the specified subject name.
Action	Verify that the configured behavior is intentional.

Message	PKI: Per config, accepted cert even though revocation check was inconclusive (subject name ⟨*certificate subject name*⟩).
Meaning	The security device accepted the certificate with the specified subject name even though it was not possible to determine its current revocation status.
Action	No recommended action

Message	PKI: PKI objects exceeded maximum capacity (⟨*maximum number of item list*⟩).
Meaning	The number of PKI objects in flash memory has exceeded the maximum capacity.
Action	Remove unused PKI objects to make more space available.

Message	PKI: PKI storage file is empty.
Meaning	This message appears after completing the bootup process if there are no PKI objects such as certificates, certificate revocation lists (CRLs), or key pairs on the security device.
Action	No recommended action

Message	PKI: Received a SCEP FAILURE message for cert request with subject name ⟨*cert subject name*⟩.
Meaning	A Simple Certificate Enrollment Protocol (SCEP) server rejected a certificate request with the specified subject name.
Action	Check the SCEP configuration on the security device. Regenerate the certificate request, and attempt to submit it to the certificate authority (CA) through SCEP again. If you receive another failure message, contact the CA admin about the problem.

Message	PKI: Received a self-signed cert in a certificate chain for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device received a certificate chain for the end-entity certificate with the specified subject name. One of the certificates in the chain was signed by the owner of the certificate, not by an issuing certificate authority (CA). The security device rejected the end-entity certificate. Starting with an end entity certificate and ending with a root CA certificate (or that of a trusted subordinate CA), a certificate chain is a hierarchy of certificates, each of which issued the one preceding it in the chain. The security device must have the top of a certificate chain preloaded for it to accept the end entity certificate. This topmost certificate in the hierarchy is known as a trust anchor.
Action	Request the peer to use another certificate that does not include a self-signed certificate in its certificate chain.

Message	PKI: Received a self-signed cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device received a certificate signed by the owner of the certificate, not by an issuing certificate authority (CA).
Action	Request the peer to use another certificate that does not include a self-signed certificate in its certificate chain.

Message	PKI: Received bad LDAP response for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device received a response from an LDAP server that it cannot decode.
Action	Check that the LDAP server settings are correct for the certificate authority (CA) that issued the peer's certificate.

Message	PKI: Received CA cert with bad fingerprint (CA cert subject name ⟨*CA cert subject name*⟩).
Meaning	The security device rejected the fingerprint, or hash digest, of the certificate authority (CA) certificate with the specified subject name that the security device received through Simple Certificate Enrollment Protocol (SCEP). The digest is used to verify the integrity of the certificate. If the digest that the security device produces does not match the digest that the peer sent, the content might have been altered between the creation of the two digests and thus cannot be trusted.
Action	Contact the CA and report the problem.

Message	PKI: Renewing cert through SCEP (subject name ⟨*string*⟩).
Meaning	The security device automatically submitted a renewal request for the certificate with the specified subject name through the Simple Certificate Enrollment Protocol (SCEP) as prescribed in the SCEP interval configuration.
Action	No recommended action

Message	PKI: request NSRP cold start sync at ⟨*number of attempts*⟩ seconds.
Meaning	NSRP cluster members were able to successfully complete a cold sync operation at the specified attempt. Cold start sync was requested at seconds after system up.
Action	No recommended action

Message	PKI: ⟨*object type string*⟩ has been deleted. (subject name ⟨*subject name*⟩).
Meaning	An admin or PKI process has removed either an IKE object related to the certificate with the specified subject name or the certificate itself.
Action	No recommended action

Message	PKI: ⟨*object type string*⟩ has been deleted. (subject name ⟨*subject name*⟩).
Meaning	A certificate has been deleted, and cannot be deleted again.
Action	No recommended action

Message	PKI: Saved CA config (CA cert subject name ⟨*CA certificate subject name*⟩).
Meaning	An admin saved the certificate authority (CA) certificate with the specified subject name or configuration settings for that CA in the internal PKI storage space.
Action	No recommended action

Message	PKI: Saved CA configuration (CA cert subject name ⟨*CA certificate subject name*⟩).
Meaning	An admin saved the certificate authority (CA) certificate with the specified subject name or configuration settings for that CA in the internal PKI storage space.
Action	No recommended action

Message	PKI: Saved PKI objects to flash.
Meaning	The security device successfully saved PKI objects from RAM to flash memory.
Action	No recommended action

Message	PKI: Saved ⟨*object type name*⟩ with subject name ⟨*Distinguished Name*⟩.
Meaning	An admin saved the PKI object with the specified subject name to flash memory.
Action	No recommended action

Message	PKI: SCEP error: ⟨*string*⟩, for cert with subject name ⟨*string*⟩.
Meaning	The security device encountered the specified error when it submitted a request via Simple Certificate Enrollment Protocol (SCEP) for a certificate with the specified subject name.
Action	When possible, use the indicated error type to correct the SCEP and configuration. For example: Change one or more of the elements composing the distinguished name in the certificate request. Regenerate the key pair. Remove an existing certificate identical to the requested certificate Then, regenerate the certificate request and resubmit it. When the problem is unclear, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	PKI: Successfully loaded image signer's public key.
Meaning	An admin has successfully updated the DSA key that authenticates the ScreenOS image.
Action	No recommended action

Message	PKI: System auto generated a self-signed cert.
Meaning	During the bootup process, the security device automatically generated a self-signed certificate.
Action	No recommended action

Message	PKI: Top cert of chain for peer's cert was wrong. Config required ⟨*required CA certificate subject name*⟩, but derived ⟨*CA certificate subject name at top of the chain*⟩.
Meaning	The local security device designated a specific certificate authority (CA) for the remote peer to use. However, the peer sent a certificate that had a different CA at the top of the derived chain. Starting with an end entity certificate and ending with a root CA certificate (or that of a trusted subordinate CA), a certificate chain is a hierarchy of certificates, each of which issued the one preceding it in the chain. The security device must have the top of a certificate chain preloaded for it to accept the end entity certificate. This topmost certificate in the hierarchy is known as a trust anchor.
Action	Do either of the following: On the local security device, designate the CA that the peer used. Contact the remote IKE peer to use the CA that you prefer.

Message	PKI: Unable to authenticate cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was unable to authenticate the certificate with the specified subject name. To authenticate a certificate the security device performs the following three steps: The security device uses the certificate authority (CA)'s public key to decrypt the digital signature on the issued certificate. (The CA encrypted a digest of the issued certificate with its private key. The result of this operation is known as a digital signature.) The security device uses the same hashing algorithm that the CA used to create the first hash. The security device compares the two hashes. If they match, then the signature is valid by virtue of the fact that private key that encrypted the digest belongs to the same key pair as the public key that decrypted it. Furthermore, because the public key comes from the CA's certificate, the private key must also belong to the CA.
Action	Contact the peer and ask if the certificate is valid.

Message	PKI: Unable to decode issuer's public key for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was unable to decode the public key in the certificate belonging to the certificate authority (CA) that issued the certificate with the specified subject name.
Action	Reload the CA certificate on the security device. If the problem persists, verify the fingerprint on the CA certificate. To do that, compare the fingerprint that appears in the output of the get pki x509 cert id_num with the fingerprint published at the CA's Web site. If the problem still persists, arrange with the peer to use certificates from a different CA.

Message	PKI: Unable to decrypt signature of cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was unable to decrypt the digital signature of the certificate with the specified subject name. Consequently, it rejected the certificate. To decrypt a digital signature, the security device uses the certificate authority's public key and the encryption algorithm that the certificate authority (CA) used to encrypt a digest of the end-entity certificate.
Action	Ensure that the peer is using a valid end-entity certificate.

Message	PKI: Unable to decrypt signature of CRL for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was unable to decrypt the digital signature of the certificate revocation list (CRL) for the certificate authority (CA) that issued the certificate with the specified subject name. This event occurred when the security device attempted to retrieve the CRL online but was unable to verify its signature. To decrypt a digital signature, the security device uses the CA's public key and the encryption algorithm that the CA used to encrypt a digest of the CRL.
Action	Check that the correct CRL options and CRL URL settings were configured on the security device for this particular CA. If the configuration is correct, contact the CA to check if the CRL is valid.

Message	PKI: Unable to get issuer cert for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device checked its local storage space and the peer's certificate chain, if the peer sent one for the certificate of the certificate authority (CA) that issued the certificate with the specified subject name, but it was unable to locate it. Consequently, it rejected the certificate. Starting with an end entity certificate and ending with a root CA certificate (or that of a trusted subordinate CA), a certificate chain is a hierarchy of certificates, each of which issued the one preceding it in the chain. The security device must have the top of a certificate chain preloaded for it to accept the end entity certificate. This topmost certificate in the hierarchy is known as a "trust anchor."
Action	Ask the peer that sent the certificate which CA issued it. If you trust that CA, obtain its certificate and load it on the security device. If you do not trust it, request the peer to use a certificate from a different CA.

Message	PKI: Unable to get local issuer cert for cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device did not have the certificate authority (CA) certificate for the CA that issued the certificate with the specified subject name. The security device rejected the certificate.
Action	Load the CA certificate for the CA that issued the IKE peer's certificate, or request the IKE peer to send a certificate chain containing the issuing CA's certificate.

Message	PKI: Unable to verify first cert in a certificate chain (subject name ⟨*certificate subject name*⟩).
Meaning	The security device received a certificate chain, but was unable to verify the first certificate in the chain. (The first certificate is identified in the message by its subject name) The security device rejected the certificate.
Action	Notify the peer that the security device was unable to verify the signature on his certificate and advise him to investigate.

Message	PKI: Unable to verify the validity of cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was unable to verify that the certificate with the specified subject name was valid. For example, the security device might not have been able to construct a certificate chain from the peer certificate to a trust anchor.
Action	Make sure that the certificate chain links the peer's certificate with a trust anchor loaded on the security device. (A trust anchor is a certificate authority (CA) certificate loaded on the security device that verifies the validity of other certificates issued under it in a hierarchy of trust.)

Message	PKI: Updated config for CA with ID ⟨*id number of CA certificate*⟩ from a global CA config.
Meaning	An admin upgraded the device to ScreenOS 5.0.0 from a version of ScreenOS earlier than ScreenOS 4.0.0. If a certificate authority (CA) configuration used global settings instead of CA-specific settings, the security device duplicated an individual storage space for this CA from the global configuration.
Action	No recommended action

Message	PKI: Verified cert with subject name ⟨*certificate subject name*⟩.
Meaning	The security device was able to verify the validity of the certificate with the specified subject name.
Action	No recommended action

Chapter 42
Policy

The following messages relate to the configuration of access policies.

Notification (00018)

Message	Default policy of the device has been changed to ⟨*policy_action_permit_or_deny*⟩ ⟨*config_changer*⟩.
Meaning	An admin (name_str) has modified the default policy of the device.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	In policy ⟨*policy_id*⟩, the application was modified to ⟨*application_name*⟩ ⟨*config_changer*⟩.
Meaning	The application to which the policy applied was changed to the one specified.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	In policy ⟨*policy_id*⟩, the attack severity was modified ⟨*config_changer*⟩.
Meaning	An admin modified the severity level of attacks in the specified policy.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	In policy ⟨*policy_id*⟩, the DI attack component was modified ⟨*config_changer*⟩.
Meaning	An admin modified the attack objects in the specified policy.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Policy (⟨*policy_id*⟩, global, ⟨*policy_src_name*⟩- > ⟨*policy_dst_name*⟩,⟨*policy_service_name*⟩, ⟨*policy_action*⟩) was added ⟨*config_changer*⟩.
Meaning	An admin (name_str) has added an global policy with the following attributes on the current device: id_num: The ID number of the access policy. src_addr: The name of the source address from which the traffic is sent. (Note: If the source address appears as NULL Name, an error has occurred and the security device cannot find the source address name.) dst_addr: The name of the destination address to which the traffic is sent. (Note: If the destination address appears as NULL Name, an error has occurred and the security device cannot find the destination address name.) svc_name: The kind of traffic (such as HTTP, FTP, or ANY which means all kinds of traffic) The action that the security device takes when this policy matches traffic received: Reject packets Permitting traffic to pass Denying traffic Tunneling traffic through a VPN tunnel
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Policy (⟨*policy_id*⟩, ⟨*policy_from_zone*⟩- > ⟨*policy_to_zone*⟩, ⟨*policy_src_name*⟩- > ⟨*policy_dst_name*⟩,⟨*policy_service_name*⟩, ⟨*policy_nat*⟩ ⟨*policy_action*⟩) was added ⟨*config_changer*⟩.
Meaning	An admin has added an access policy with the following attributes on the current device: id_num - The ID number of the access policy. zone1 - The zone from which traffic originates. zone2 - The zone to which traffic travels. src_addr - The name of the source address from which the traffic is sent. (Note: If the source address appears as NULL Name, an error has occurred and the security device cannot find the source address name.) dst_addr - The name of the destination address to which the traffic is sent. (Note: If the destination address appears as NULL Name, an error has occurred and the security device cannot find the destination address name.) svc_name - The kind of traffic (such as HTTP, FTP, or ANY-which means all kinds of traffic) The action that the security device takes when this policy matches traffic received: Reject packets Permitting traffic to pass Denying traffic Tunneling traffic through a VPN tunnel
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Policy (⟨*policy_id*⟩, ⟨*policy_from_zone*⟩- > ⟨*policy_to_zone*⟩, ⟨*policy_src_name*⟩- > ⟨*policy_dst_name*⟩,⟨*policy_service_name*⟩, ⟨*policy_action*⟩) was deleted ⟨*config_changer*⟩.
Meaning	An admin (name_str) has deleted an access policy with the following attributes on the current device: id_num: The ID number of the access policy. zone1: The zone from which traffic originates. zone2: The zone to which traffic travels. src_addr: The name of the source address from which the traffic is sent. (Note: If the source address appears as NULL Name, an error has occurred and the security device cannot find the source address name.) dst_addr: The name of the destination address to which the traffic is sent. (Note: If the destination address appears as NULL Name, an error has occurred and the security device cannot find the destination address name.) svc_name: The kind of traffic (such as HTTP, FTP, or ANY which means all kinds of traffic) The action that the security device takes when this policy matches traffic received: Reject packets Permitting traffic to pass Denying traffic Tunneling traffic through a VPN tunnel
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Policy (⟨*policy_id*⟩, ⟨*policy_from_zone*⟩- > ⟨*policy_to_zone*⟩, ⟨*policy_src_name*⟩- > ⟨*policy_dst_name*⟩,⟨*policy_service_name*⟩, ⟨*policy_action*⟩) was modified ⟨*config_changer*⟩.
Meaning	An admin (name_str) has modified an access policy with the following attributes on the current device: id_num: The ID number of the access policy. zone1: The zone from which traffic originates. zone2: The zone to which traffic travels. src_addr: The name of the source address from which the traffic is sent. (Note: If the source address appears as NULL Name, an error has occurred and the security device cannot find the source address name.) dst_addr: The name of the destination address to which the traffic is sent. (Note: If the destination address appears as NULL Name, an error has occurred and the security device cannot find the destination address name.) svc_name: The kind of traffic (such as HTTP, FTP, or ANY which means all kinds of traffic) The action that the security device takes when this policy matches traffic received: Reject Packets Permitting traffic to pass Denying traffic Tunneling traffic through a VPN tunnel
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Policy (⟨*policy_id*⟩, ⟨*policy_from_zone*⟩- > ⟨*policy_to_zone*⟩, ⟨*policy_src_name*⟩- > ⟨*policy_dst_name*⟩,⟨*policy_service_name*⟩, ⟨*policy_action*⟩) was ⟨*policy_state_enabled_or_disabled*⟩ ⟨*config_changer*⟩.
Meaning	An admin (name_str) has enabled or disabled an access policy with the following attributes on the current device: id_num - The ID number of the access policy. zone1—The zone from which traffic originates. zone2—The zone to which traffic travels. src_addr—The name of the source address from which the traffic is sent. (Note: If the source address appears as NULL Name, an error has occurred and the security device cannot find the source address name.) dst_addr—The name of the destination address to which the traffic is sent. (Note: If the destination address appears as NULL Name, an error has occurred and the security device cannot find the destination address name.) svc_name—The kind of traffic (such as HTTP, FTP, or ANY which means all kinds of traffic) The action that the security device takes when this policy matches traffic received: Reject Packets Permitting traffic to pass Denying traffic Tunneling traffic through a VPN tunnel
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Policy ⟨*src_policy_id*⟩ has been moved after ⟨*dst_policy_id*⟩ ⟨*admin_name*⟩.
Meaning	An admin (name_str) has exchanged the positions of the two specified policies (id_num1 and id_num2).
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Policy ⟨*src_policy_id*⟩ has been moved before ⟨*dst_policy_id*⟩ ⟨*admin_name*⟩.
Meaning	An admin (name_str) has exchanged the positions of the two specified policies (id_num1 and id_num2).
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	⟨*cell_name*⟩ ⟨*cell_obj_name*⟩ was ⟨*action_add_delete*⟩ policy ID ⟨*policy_id*⟩ ⟨*config_changer*⟩.
Meaning	An admin added or deleted an attack object from the specified policy.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Chapter 43

PPP

The following messages relate to the configuration of PPP (Point-to-Point Protocol) connections.

Alert (00095)

Message	No IP pool has been assigned. You cannot allocate an IP address.
Meaning	There is currently no assigned PPPoE IP address pool, so the device cannot generate IP addresses.
Action	Define an address pool, either with the WebUI or the set ippool CLI command .

Alert (00096)

Message	Cannot allocate IP address from pool ⟨*ip_pool_name*⟩ for user ⟨*user_name*⟩.
Meaning	The IP address pool is of insufficient size, or an IP address is already in use by PPP.
Action	Possible solutions are as follows: Increase size of ip pool. Free an IP address by disconnecting one or more users from this L2TP connection.

Notification

Message	PPP profile ⟨*string*⟩ sets ncp ⟨*string*⟩.
Meaning	User sets the NCP type for a PPP profile.
Action	No recommended action.

Notification

Message	PPP protocol on interface ⟨*string*⟩ is ⟨*string*⟩, local IPV6: ⟨*IP address*⟩, peer IPV6: ⟨*IP address*⟩ .
Meaning	The interface becomes up/down if PPP is up/down. If both IPV6CP and IPCP are selected, the interface becomes up only when both of them are up.
Action	No recommended action

Notification

Message	PPP updates interface ⟨*string*⟩'s IPV6 to ⟨*IP address*⟩.
Meaning	The interface's IPV6 address is changed because PPP is now up/down.
Action	No recommended action

Notification (00017)

Message	IP address pool ⟨*ip_pool_name*⟩ was removed ⟨*config_changer*⟩.
Meaning	An admin (< name_str >) removed a PPPoE IP address pool.
Action	No recommended action.

Message	IP address pool ⟨*ip_pool_name*⟩ with range ⟨*start_ip*⟩ - ⟨*end_ip*⟩ was created ⟨*config_changer*⟩.
Meaning	The IP address pool is of insufficient size, or an IP address is already in use by PPP.
Action	Possible solutions are as follows: Increase size of ip pool. Free an IP address by disconnecting one or more users from this L2TP connection.

Message	IP address pool ⟨*ip_pool_name*⟩ with range ⟨*start_ip*⟩ - ⟨*end_ip*⟩ was removed ⟨*config_changer*⟩.
Meaning	An admin (< name_str2 >) removed an IP range from an IP address pool (< name_str2 >). Since the IP pool only contained one range the IP pool will also be removed.
Action	No recommended action.

Message	Range ⟨*start_ip*⟩ - ⟨*end_ip*⟩ was added to IP pool ⟨*ip_pool_name*⟩ ⟨*config_changer*⟩.
Meaning	An admin (< name_str2 >) added a IP range to an IP address pool (< name_str2 >).
Action	No recommended action.

Message	Range ⟨*start_ip*⟩ - ⟨*end_ip*⟩ was removed from IP pool ⟨*ip_pool_name*⟩ ⟨*config_changer*⟩.
Meaning	An admin (< name_str2 >) added an IP range to an IP address pool (< name_str2 >).
Action	No recommended action.

Notification (00077)

Message	PPP on ⟨*string*⟩ detects loopback.
Meaning	PPP found a loopback on the specified interface.
Action	Check to see why the loopback is occurring.

Message	PPP profile ⟨*string*⟩ changes authentication type to ⟨*string*⟩.
Meaning	An admin changed the authentication method in the specified profile.
Action	No recommended action.

Message	PPP profile ⟨*string*⟩ changes local-name to ⟨*string*⟩.
Meaning	An admin changed the local name in the specified profile.
Action	No recommended action.

Message	PPP profile ⟨*string*⟩ changes secret to ⟨*string*⟩.
Meaning	An admin changed the password in the specified profile.
Action	No recommended action.

Message	PPP profile ⟨*string*⟩ is ⟨*string*⟩.
Meaning	Ad admin has created or deleted a PPP profile with the specified name.
Action	No recommended action.

Message	PPP profile ⟨*string*⟩ ⟨*string*⟩ passive mode CHAP.
Meaning	An admin enabled or disabled passive mode in the specified profile.
Action	No recommended action.

Message	PPP profile ⟨*string*⟩ sets netmask ⟨*IP address*⟩.
Meaning	An admin set a netmask in the specified profile.
Action	No recommended action.

Message	PPP profile ⟨*string*⟩ sets ⟨*string*⟩ use static IP.
Meaning	An admin set the use of a static IP address in the specified profile.
Action	No recommended action.

Message	PPP ⟨*string*⟩ encapsulation ⟨*string*⟩ for interface ⟨*string*⟩.
Meaning	An admin set or unset PPP or MLPPP encapsulation for the specified interface.
Action	No recommended action.

Message	PPP ⟨*string*⟩ interface ⟨*string*⟩ ⟨*string*⟩ bundle ⟨*string*⟩.
Meaning	An admin added or deleted an interface to or from the specified bundle.
Action	No recommended action.

Message	PPP ⟨*string*⟩ profile ⟨*string*⟩ for interface ⟨*string*⟩.
Meaning	An admin bound or unbound a profile to the specified interface.
Action	No recommended action.

Message	PPP ⟨*string*⟩ short sequence number for interface ⟨*string*⟩.
Meaning	An admin set or unset the use of a 12-bit sequence header format in MLPPP packets for the specified multilink interface.
Action	No recommended action.

Message	PPP set MRRU ⟨*integer*⟩ for interface ⟨*string*⟩.
Meaning	An admin set a new maximum received reconstructed unit size for the specified multilink interface.
Action	No recommended action.

Notification (00088)

Message	PPP control packet queue on ⟨*string*⟩ takes on ⟨*string*⟩ packets.
Meaning	The "too many" message is generated when the queued packet number is too large. The "normal number" message is generated when the number returns back to a normal level.
Action	If the "too many" message appears, check the peer or other task for abnormal operation.

Notification (00572)

Message	PPP authentication state on interface ⟨*string*⟩: ⟨*string*⟩.
Meaning	PPP authentication state on the specified interface is one of the following: Peer failed to authenticate itself Peer authenticated itself successfully Local failed to authenticate itself Local authenticated itself successfully
Action	If either the peer or local failed to authenticate itself, check the user name and password configured on both sides.

Message	PPP bundle ⟨*string*⟩ is ⟨*string*⟩ and then brings ⟨*string*⟩ bundle NCP.
Meaning	The specified bundle is up or down, and brings up or down NCP.
Action	No recommended action.

Message	PPP LCP on interface ⟨*string*⟩ is ⟨*string*⟩.
Meaning	LCP state on the specified interface changed to up or down.
Action	No recommended action.

Message	PPP member ⟨*string*⟩ fails to join bundle ⟨*string*⟩ for ⟨*string*⟩.
Meaning	The interface was not able to join the specified bundle for one of the following reasons: No empty member entry is available Either side does not negotiate the MRRU The joining member carries a different EPD The peer joining member carries a different MRRU The peer joining member carries a different SSN flag The local joining member carries a different MRRU The local MRU is grater than the local MRRU
Action	Check the specified reason. Make sure both sides of the link are using acceptable parameters.

Message	PPP member ⟨*string*⟩ joins bundle ⟨*string*⟩ successfully.
Meaning	The interface successfully joined the specified bundle after LCP.
Action	No recommended action.

Message	PPP on interface ⟨*string*⟩ finds possible loopback.
Meaning	PPP found a loopback on the specified interface, according to the LCP request packet.
Action	Check to see why the loopback is occurring and that the LCP request packet is correct.

Message	PPP on interface ⟨*string*⟩ is terminated by missing too many echo replies.
Meaning	The local side sent many Echo-Requests without receiving a reply, so it terminated and then reset the PPP session.
Action	Check to see why the peer failed to reply to the Echo-Requests.

Message	PPP on interface ⟨*string*⟩ is terminated by receiving Terminate-Request.
Meaning	The peer sent a request to terminate the PPP session.
Action	No recommended action.

Message	PPP on ⟨*string*⟩ resets LCP for ⟨*string*⟩.
Meaning	PPP has reset the Link Control Protocol because of one of the following reasons: IPCP finished LCP finished The profile was updated The Hostname was updated LCP failed to come up after negotiation NCP failed to come up after negotiation A profile was not obtained after NCP The IP address could not be modified after NCP The host route could not be set An admin changed the interface's IP address An admin changed the interface of the MTU
Action	Check the specified reason.

Message	PPP protocol on interface ⟨*string*⟩ is ⟨*string*⟩, local IP: ⟨*IP address*⟩, peer IP: ⟨*IP address*⟩ .
Meaning	PPP is up or down; the local and peer IP addresses are shown.
Action	No recommended action.

Message	PPP updates interface ⟨*string*⟩'s IP to ⟨*IP address*⟩ .
Meaning	PPP updated the interface's IP address to the assigned address.
Action	No recommended action.

Message	PPP updates interface ⟨*string*⟩'s L3 MTU to ⟨*integer*⟩.
Meaning	Based upon the results of PPP negotiation, the interface's MTU is updated to the specified number.
Action	No recommended action.

Chapter 44

PPPoA

These messages relate to the configuration of Point-to-Point Protocol over Asynchronous Transfer Mode (ATM) virtual circuits.

Notification (00060)

Message	PPPoA is disabled on ⟨*interface_name*⟩ interface.
Meaning	The PPPoA client on the security device was enabled or disabled on the specified interface.
Action	No recommended action.

Message	PPPoA is enabled on ⟨*interface_name*⟩ interface.
Meaning	The PPPoA client on the security device was enabled or disabled on the specified interface.
Action	No recommended action.

Notification (00558)

Message	PPPoA ⟨*PPPoA name*⟩ connected successfully.
Meaning	The PPPoA client on the security device successfully established a session with the PPPoA server.
Action	No recommended action.

Message	PPPoA ⟨*PPPoA name*⟩ connection attempt failed (⟨*reason*⟩).
Meaning	The security device was unsuccessful in its attempt to establish a session with a PPPoA server for the reason displayed.
Action	Check the PPPoA configuration.

Message	PPPoA ⟨*PPPoA name*⟩ failed to modify the gateway for the interface.
Meaning	During the PPPoA session, a new IP address was assigned to the default gateway for the interface but failed to update on the device.
Action	Reboot the device.

Message	PPPoA ⟨*PPPoA name*⟩ failed to modify the IP for the interface.
Meaning	During the PPPoA session, a new IP address was assigned to the interface but failed to update on the device.
Action	Reboot the device.

Message	PPPoA ⟨*PPPoA name*⟩ failed to negotiate the IP for the interface.
Meaning	No IP address was assigned to the interface during the PPPoA session.
Action	Check the PPPoA configuration on the device. Recheck the PPPoA configuration parameters on the service provider's server.

Message	PPPoA ⟨*PPPoA name*⟩ idle timeout.
Meaning	The security device terminated the PPPoA connection due to inactivity. The default idle timeout is 30 minutes.
Action	Specify a higher idle timeout value (valid range is up to 10000 minutes), or set the idle timeout to 0, which turns off the timeout.

Message	PPPoA ⟨*PPPoA name*⟩ shutdown.
Meaning	The security device shut down the PPPoA session.
Action	No recommended action

Message	PPPoA ⟨*PPPoA name*⟩ started negotiation.
Meaning	The PPPoA client on the security device has initiated a session with the PPPoA server.
Action	No recommended action.

Chapter 45

PPPoE

The following messages relate to the configuration of Point-to-Point Protocol over Ethernet (PPPoE) connections.

Notification (00034)

Message	Point-to-Point Protocol over Ethernet (PPPoE) settings changed.
Meaning	PPPoE parameters on the device changed.
Action	No recommended action

Message	PPPoE is disabled on ⟨*interface_name*⟩ interface.
Meaning	Point-to-Point Protocol over Ethernet (PPPoE) is enabled or disabled on the specified interface.
Action	No recommended action.

Message	PPPoE is enabled on ⟨*interface_name*⟩ interface.
Meaning	Point-to-Point Protocol over Ethernet (PPPoE) is enabled or disabled on the specified interface.
Action	No recommended action.

Notification (00537)

Message	AC ⟨*url_string*⟩ is advertising URL ⟨*string*⟩
Meaning	The access concentrator to which the device connects, advertised a URL.
Action	No recommended action.

Message	Failed to set PPPoE interface gateway.
Meaning	After attempting to establish a PPPoE session on the device, the session failed and no gateway was assigned.
Action	No recommended action.

Message	Failed to set PPPoE interface IP address.
Meaning	The device failed to assign an IP address to a host.
Action	No recommended action.

Message	Failed to set PPPoE IPv6 interface gateway.
Meaning	The device failed to set an IPv6 gateway for local hosts.
Action	No recommended action.

Message	Message from AC ⟨*access_concentrator*⟩: ⟨*message_from_ac*⟩
Meaning	The access concentrator to which the device connects, sent the displayed message.
Action	No recommended action.

Message	Point-to-Point Protocol over Ethernet (PPPoE) connection failed to establish a session. No IP address assigned.
Meaning	After attempting to establish a PPPoE session on the device, the session failed and no IP address was assigned.
Action	No recommended action.

Message	Point-to-Point Protocol over Ethernet (PPPoE) connection failed to establish a session. No IPv6 address assigned.
Meaning	The device failed to assign an IPv6 address to a host.
Action	No recommended action.

Message	Point-to-Point Protocol over Ethernet (PPPoE) connection failed to establish a session. ⟨*pppoe_packet_received_type*⟩ received.
Meaning	The PPPoE connection was unable to create a session. A message string was received.
Action	No recommended action

Message	Point-to-Point Protocol over Ethernet (PPPoE) connection failed to establish a session. Timeout ⟨*timeout_reason*⟩
Meaning	The device was unsuccessful in its attempt to establish a session with a PPPoE server of the reason displayed.
Action	Increase the session timeout value.

Message	PPPoE session closed by AC.
Meaning	The access concentrator to which the device connects terminated a PPPoE session.
Action	No recommended action.

Message	PPPoE session shut down by user.
Meaning	A user terminated the Point-to-Point Protocol over Ethernet (PPPoE) session on the device.
Action	No recommended action.

Message	PPPoE session shut down, PPPoE disabled.
Meaning	PPPoE is disabled so the session has shut down.
Action	No recommended action.

Message	PPPoE session shut down. Idle timeout.
Meaning	The PPPoE session was idle for the specified idle timeout so the session has shut down.
Action	No recommended action.

Message	PPPoE session shuts down for ⟨*pppoe_instance_name*⟩ instance due to system reset.
Meaning	The device was reset so the session has shut down.
Action	No recommended action.

Message	PPPoE session started negotiations.
Meaning	The PPPoE client on the device has initiated a session with the PPPoE server.
Action	No recommended action.

Message	PPPoE session termination or failure during: ⟨*ppp_fail_reason*⟩
Meaning	PPPoE encountered a failure %s during an attempt to establish a session. Possible values for %s; include: LCP, CHAP/PAP, IPCP link setup LCP Keep alive CHAP/PAP Authentication
Action	No recommended action.

Message	PPPoE session was successfully established.
Meaning	PPPoE successfully assigned an IP address for a session.
Action	No recommended action.

Chapter 46
RIP

The following messages relate to the Routing Information Protocol (RIP) dynamic routing protocol.

Critical (00207)

Message	RIP database size limit exceeded for ⟨*vrouter_name*⟩, RIP route dropped.
Meaning	vrouter is dropping RIP routes because the RIP database is full.
Action	No recommended action.

Message	System wide RIP route limit exceeded, RIP route dropped.
Meaning	The system is not able to accept more RIP routes and is dropping RIP routes to preserve system resources.
Action	Decrease the number of RIP routes for the system.

Message	⟨*route_drop_count*⟩ RIP routes dropped, RIP database size exceeded in vr ⟨*vrouter_name*⟩.
Meaning	The specified vrouter experienced excess RIP route entries in the RIP database, and it dropped the specified number of RIP routes.
Action	Reduce the number of RIP routes.

Message	⟨*route-drop-count*⟩ RIP routes dropped, system wide RIP route limit exceeded.
Meaning	The vrouter dropped < number > of RIP routes when the system reached capacity.
Action	Decrease the number of RIP routes for the system.

Message	The total number of redistributed routes into RIP in vrouter (⟨*vrouter-name*⟩) exceeded system limit (⟨*system-limit*⟩).
Meaning	The number of redistributed routes into RIP exceeded the limit.
Action	Check the network topology and try to reduce the number of routes.

Critical (00227)

Message	RIPng database size limit exceeded for ⟨*vrouter_name*⟩, RIPng route dropped.
Meaning	< vrouter > is dropping RIPng routes because the RIPng database is full.
Action	Decrease the number RIPng routes.

Message	System wide RIPng route limit exceeded, RIPng route dropped.
Meaning	The system is not able to accept more RIPng routes and is dropping RIP routes to preserve system resources.
Action	Decrease the number of RIPng routes for the system.

Message	⟨*route_drop_count*⟩ RIPng routes dropped, RIP database size exceeded in vr ⟨*vrouter_name*⟩.
Meaning	The specified virtual router experienced excess RIPng route entries in the RIPng database, and it dropped the specified number of RIPng routes.
Action	Decrease the number RIPng routes.

Message	⟨*route-drop-count*⟩ RIPng routes dropped, system wide RIPng route limit exceeded.
Meaning	The virtual router dropped < number > of RIPng routes when the system reached capacity.
Action	Decrease the number RIPng routes.

Message	Virtual router ⟨*vrouter_name*⟩ that received an update packet flood from neighbor ⟨*neighbor-ip-address*⟩ on interface ⟨*interface-name*⟩ dropped a packet.
Meaning	Routing instances send update packets to neighbor virtual routing instances continually to inform them of changes that occurred in their routing tables. Sometimes a neighbor sends more packets during a set update interval than a routing instance can process. When this event occurs, the interface to which the routing instance is mapped may respond by dropping packets entering the interface.
Action	Provide a higher value for the RIP update packet interval on the virtual routing instance which drops the packets.

Message	Virtual router ⟨*vrouter_name*⟩ that received an update packet flood from neighbor ⟨*neighbor-ip-address*⟩ on interface ⟨*interface-name*⟩ dropped a packet.
Meaning	Routing instances send update packets to neighbor virtual routing instances continually to inform them of changes that occurred in their routing tables. Sometimes a neighbor sends more packets during a set update interval than a routing instance can process. When this event occurs, the interface to which the routing instance is mapped may respond by dropping packets entering the interface.
Action	Provide a higher value for the RIP update packet interval on the virtual routing instance which drops the packets.

Message	The total number of redistributed routes into RIPng in vrouter (⟨*vrouter-name*⟩) exceeded system limit (⟨*system-limit*⟩).
Meaning	The specified virtual router experienced an excess number of RIPng redistributed routes.
Action	Decrease the number of redistributed routes.

Notification (00045)

Message	RIP instance in virtual router ⟨*vrouter_name*⟩ was created.
Meaning	An administrator successfully created or removed a RIP instance on the specified virtual router.
Action	No recommended action

Message	RIP instance in virtual router ⟨*vrouter_name*⟩ was removed.
Meaning	An administrator successfully created or removed a RIP instance on the specified virtual router.
Action	No recommended action

Message	⟨*configuration_command*⟩
Meaning	An administrator set or unset a RIP configuration command at the root level.
Action	No recommended action

Message	⟨*set_or_unset*⟩ virtual router ⟨*vrouter_name*⟩ with the configuration command ⟨*configuration_command*⟩.
Meaning	An administrator set a value on the RIP virtual routing instance using a RIP command.
Action	No recommended action

Message	⟨*set_or_unset*⟩ vrouter ⟨*vrouter_name*⟩ protocol RIP received configuration command ⟨*configuration_command*⟩.
Meaning	The RIP router received a configuration command issued to it.
Action	No recommended action

Notification (00073)

Message	RIPng instance in virtual router ⟨*vrouter_name*⟩ created.
Meaning	An administrator successfully created or removed a RIP instance on the specified virtual router.
Action	No recommended action.

Message	RIPng instance in virtual router ⟨*vrouter_name*⟩ removed.
Meaning	An administrator successfully created or removed a RIP instance on the specified virtual router.
Action	No recommended action.

Message	⟨*configuration_command*⟩
Meaning	An administrator set or unset a RIP configuration command at the root level.
Action	No recommended action

Message	⟨*set_or_unset*⟩ virtual router ⟨*vrouter_name*⟩ with the configuration command ⟨*configuration_command*⟩.
Meaning	An administrator set a value on the RIP virtual routing instance using a RIP command.
Action	No recommended action

Message	⟨*set_or_unset*⟩ vrouter ⟨*vrouter_name*⟩ protocol RIP received configuration command ⟨*configuration_command*⟩.
Meaning	The RIP router received a configuration command issued to it.
Action	No recommended action

Information (00544)

Message	RIP neighbor ⟨*neighbor-ip-address*⟩ in virtual router ⟨*vrouter_name*⟩ added.
Meaning	The current RIP routing instance received the new address of a neighbor and added it to the routing table.
Action	No recommended action

Message	RIP neighbor ⟨*neighbor-ip-address*⟩ in virtual router ⟨*vrouter_name*⟩ removed.
Meaning	The current RIP routing instance removed an existing neighbor address from the routing table.
Action	No recommended action

Information (00562)

Message	RIPng neighbor ⟨*neighbor-ip-address*⟩ in virtual router ⟨*vrouter_name*⟩ added.
Meaning	The current RIP routing instance received the new address of a neighbor and added it to the routing table.
Action	No recommended action

Message	RIPng neighbor ⟨*neighbor-ip-address*⟩ in virtual router ⟨*vrouter_name*⟩ removed.
Meaning	The current RIP routing instance removed an existing neighbor address from the routing table.
Action	No recommended action

Chapter 47
Route

The following sections provide descriptions of and recommended actions for ScreenOS messages displayed for route-related events.

Critical (00205)

Message	A new route cannot be added to the device because the maximum number of system route entries (⟨*max_routes*⟩) has been exceeded.
Meaning	A new route could not be added because the number of route entries exceeds the system-wide maximum number of routes.
Action	Check the network topology and try to reduce the number of routes.

Message	A route ⟨*ipv6_addr*⟩/⟨*ip_mask*⟩ cannot be added to the virtual router ⟨*vrouter_name*⟩ because the number of route entries in the virtual router exceeds the maximum number of routes (⟨*max_routes*⟩) allowed.
Meaning	Each virtual routing instance's routing table has a maximum number of routes it accepts. Once the number of routes in the route table surpasses the maximum number value, the routing instance cannot add any more routes to the table. The virtual routing instance was unable to add a route to its route table because the number of routes in its route table has reached the maximum value.
Action	Change the virtual router's maximum routes value.

Message	A route ⟨*ip_addr*⟩/⟨*ip_mask*⟩ cannot be added to the virtual router ⟨*vrouter_name*⟩ because the number of route entries in the virtual router exceeds the maximum number of routes (⟨*max_routes*⟩) allowed
Meaning	Each virtual routing instance's routing table has a maximum number of routes it accepts. Once the number of routes in the route table surpasses the maximum number value, the routing instance cannot add any more routes to the table. The virtual routing instance was unable to add a route to its route table because the number of routes in its route table has reached the maximum value.
Action	Change the virtual router's maximum routes value.

Message	An error occurred on virtual router ⟨*vrouter_name*⟩ while removing route ⟨*ip_addr*⟩/⟨*ip_mask*⟩ from virtual router route table.
Meaning	While attempting to remove a route in the specified virtual routing instance's route table, an error occurred that prevents the administrator from successfully removing the route. The error could be an issue with permission level for the administrator attempting to remove the route.
Action	Configure the network administrator with the proper permissions that enable him or her to remove a route from the virtual routing instance.

Message	Error occurred while adding route ⟨*ip_addr*⟩/⟨*ip_mask*⟩ to virtual router ⟨*vrouter_name*⟩ route table because the db_insert function failed.
Meaning	While attempting to add a route to the specified virtual routing instance's route table, an error occurred with the db_insert function that prevents the administrator from successfully adding the route. db_insert is a function that adds a route to a virtual routing instance's route table.
Action	Look at other system parameters like memory usage, etc. The system may be running out of memory.

Message	Error occurred while adding route ⟨*ip_addr*⟩/⟨*ip_mask*⟩ to virtual router ⟨*vrouter_name*⟩ route table because the prefix add function failed.
Meaning	While attempting to add a route to the specified virtual routing instance's route table, an error occurred with the prefix_add function that prevents the administrator from successfully adding the route. prefix_add is a function that adds a route to a virtual routing instance's route table.
Action	Look at other system parameters like memory usage etc. The system may be running out of memory.

Message	Error while adding IPv6 route ⟨*ipv6_addr*⟩/⟨*ip_mask*⟩ to vrouter ⟨*vrouter_name*⟩, db_insert failed.
Meaning	Insertion of an IPv6 route to route database failed. It could be because of the max. number of routes allowed in the system has been reached.
Action	Ensure that the total number of routes doesn't exceed the maximum limit for the system.

Message	Error while adding route ⟨*ipv6_addr*⟩/⟨*ip_mask*⟩ to vrouter ⟨*vrouter_name*⟩, prefix add failed.
Meaning	Adding the IPv6 route into RIB failed. System may be low on memory.
Action	Free up system memory.

Message	IPv6 neighbor gateway ⟨*ipv6_addr*⟩ is reachable.
Meaning	IPv6 neighbor on given interface is now reachable.
Action	No action is required. All the routes with this next-hop will be added to FIB.

Message	IPv6 neighbor gateway ⟨*ipv6_addr*⟩ is unreachable.
Meaning	IPv6 neighbor on given interface is now unreachable.
Action	No action is required. All the routes with this next-hop will be deleted from FIB.

Message	⟨*vrouter_name*⟩ Error while deleting route ⟨*ipv6_addr*⟩/⟨*ip_mask*⟩ from route table.
Meaning	Deleting the IPv6 route from route database failed. This is possible if the route is not found in route database.
Action	Ensure that the route has already been added.

Critical (00229)

Message	Error in rebuilding the PBR policy lookup tree for ⟨*pbr_policy_name*⟩ in virtual router ⟨*vrouter_name*⟩.
Meaning	There was an error while rebuilding the PBR policy lookup tree for a policy.
Action	Check to ensure there are entries configured in match-groups and the extended access-lists used in match-groups. If there are no entries in extended access-lists, the event may be treated as informatory.

Message	Unable to add PBR policy ⟨*pbr_policy_name*⟩ in virtual router ⟨*vrouter_name*⟩. Exceeded maximum number of policies (⟨*max_pbr_pol_num*⟩).
Meaning	Because the maximum number of policies allowable on a device has been exceeded, a PBR policy was unable to be added.
Action	Ensure the number of PBR policies are below the maximum.

Notification (00011)

Message	An SIBR route in virtual router ⟨*vrouter_name*⟩ with an IP address ⟨*ip_addr*⟩/⟨*ip_mask*⟩ and next-hop as virtual router ⟨*next_hop_vrouter_name*⟩ created.
Meaning	A source interface-based route (SIBR) is created with a virtual router as the next hop.
Action	No recommended action.

Message	IPv6 route in virtual router ⟨*vrouter_name*⟩ that has IP address ⟨*ipv6_addr*⟩/⟨*ip_mask*⟩ through interface ⟨*interface_name*⟩ and gateway ⟨*ipv6_addr*⟩ with metric ⟨*route_metric*⟩ created.
Meaning	An IPv6 route with the specified IP address have been created.
Action	No recommended action.

Message	IPv6 route in virtual router ⟨*vrouter_name*⟩ with an IP address ⟨*ipv6_addr*⟩/⟨*ip_mask*⟩ and next-hop as virtual router ⟨*next_hop_vrouter_name*⟩ created.
Meaning	An IPv6 route with the specified IP address have been created.
Action	No recommended action.

Message	IPv6 Route(s) in virtual router ⟨*vrouter_name*⟩ with an IP address ⟨*ipv6_addr*⟩/⟨*ip_mask*⟩ and gateway ⟨*ipv6_addr*⟩ deleted.
Meaning	IPv6 route(s) with the specified IP address have been deleted from the specified gateway.
Action	No recommended action.

Message	Route in virtual router ⟨*vrouter_name*⟩ that has IP address ⟨*ip_addr*⟩/⟨*ip_mask*⟩ through interface ⟨*interface_name*⟩ and gateway ⟨*gateway*⟩ with metric ⟨*route_metric*⟩ created.
Meaning	A route with the specified parameters was created in the route table of the current virtual routing instance.
Action	No recommended action

Message	Route in virtual router ⟨*vrouter_name*⟩ with IP address ⟨*ip_addr*⟩/⟨*ip_mask*⟩ and next-hop as virtual router ⟨*next_hop_vrouter_name*⟩ created.
Meaning	A route with the specified virtual router as the next hop was created in the current virtual routing instance.
Action	No recommended action

Message	Route(s) in virtual router ⟨*vrouter_name*⟩ with an IP address ⟨*ip_addr*⟩/⟨*ip_mask*⟩ and gateway ⟨*gateway*⟩ deleted.
Meaning	One or more routes were removed from the route table of the current virtual routing instance.
Action	No recommended action

Message	Source route in virtual router ⟨*vrouter_name*⟩ with an IP address ⟨*ip_addr*⟩/⟨*ip_mask*⟩ and next-hop as virtual router ⟨*next_hop_vrouter_name*⟩ created.
Meaning	A source-based route is created with a virtual router as the next hop.
Action	No recommended action.

Message	Source route(s) in virtual router ⟨*vrouter_name*⟩ with route addresses of ⟨*ip_addr*⟩/⟨*ip_mask*⟩ and a default gateway address of ⟨*next_hop_ip_addr*⟩ removed.
Meaning	Source routes are used when doing a route lookup based on source IP rather than destination IP. This message indicates a source route was removed.
Action	No recommended action

Message	Source route(s) in virtual router ⟨*vrouter_name*⟩ with route addresses of ⟨*ip_addr*⟩/⟨*ip_mask*⟩ through interface ⟨*interface_name*⟩ and a default gateway address ⟨*next_hop_ip_addr*⟩ with metric ⟨*route_metric*⟩ created.
Meaning	Source routes are used when doing a route lookup based on source IP rather than destination IP. This message indicates a source route was created.
Action	No recommended action

Message	IPv4 default-router ⟨*ip_addr*⟩ learned from RA added.
Meaning	A IPv4 default router has been learned and added.
Action	No recommended action.

Message	IPv4 default-router ⟨*ip_addr*⟩ learned from RA deleted.
Meaning	A IPv4 default router has been learned and added.
Action	No recommended action.

Message	IPv6 default-router ⟨*ipv6_addr*⟩ learned from RA added.
Meaning	IPv6 auto-discovered route has been learned and added.
Action	No action is required.

Message	IPv6 default-router ⟨*ipv6_addr*⟩ learned from RA deleted.
Meaning	IPv6 auto-discovered route has been learned and deleted.
Action	No action is required.

Message	SIBR route in virtual router ⟨*vrouter_name*⟩ for interface ⟨*interface_name*⟩ that has IP address ⟨*ip_addr*⟩/⟨*ip_mask*⟩ through interface ⟨*interface_name*⟩ and gateway ⟨*next_hop_ip_addr*⟩ with metric ⟨*route_metric*⟩ created.
Meaning	An administrator created a SIBR route for the specified vrouter on the specified interface. The route IP address and mask, gateway information and metric appear in the notification.
Action	No recommended action

Message	SIBR Route(s) in virtual router ⟨*vrouter_name*⟩ for interface ⟨*interface_name*⟩ with an IP address ⟨*ip_addr*⟩/⟨*ip_mask*⟩ and gateway ⟨*next_hop_ip_addr*⟩ removed.
Meaning	An administrator deleted the specified SIBR route.
Action	No recommended action

Notification (00048)

Message	access list ⟨*access-list-id*⟩ sequence number ⟨*access-list-sequence-num*⟩ default-route with action ⟨*permit_or_deny*⟩ is created in vrouter ⟨*vrouter-name*⟩
Meaning	
Action	

Message	Access list entry ⟨*access-list-id*⟩ was removed from virtual router ⟨*vrouter-name*⟩
Meaning	The specified access list entry was added to or removed from the virtual routing instance. If the entry was removed, all conditions and resulting actions that this entry enforced are no longer present on the routing instance.
Action	No recommended action

Message	Access list entry ⟨*access-list-id*⟩ was removed from virtual router ⟨*vrouter-name*⟩
Meaning	The specified access list entry was added to or removed from the virtual routing instance. If the entry was removed, all conditions and resulting actions that this entry enforced are no longer present on the routing instance.
Action	No recommended action

Message	Access list entry ⟨*access-list-id*⟩ with a sequence number ⟨*access-list-sequence-num*⟩ that ⟨*permit_or_deny*⟩ IP address ⟨*ip_address*⟩/⟨*ip_mask*⟩ is being deleted from virtual router ⟨*vrouter-name*⟩
Meaning	The specified access list entry on the current virtual routing instance that either permitted or denied entry into the device was removed. Access lists provide filtering mechanisms or preset criteria by which packets attempting to enter a device must fulfill to be forwarded to the device.
Action	No recommended action

Message	Access list entry ⟨*access-list-id*⟩ with sequence number ⟨*access-list-sequence-num*⟩ with an action of ⟨*permit_or_deny*⟩ with an IP address and subnetwork mask of ⟨*ip_address*⟩/⟨*ip_mask*⟩ was created on virtual router ⟨*vrouter-name*⟩
Meaning	The specified access list entry on the current virtual routing instance that either permitted or denied entry into the device was added.
Action	No recommended action

Message	An ⟨*import_or_export_rule*⟩ rule applied to a connection between virtual router ⟨*source-vrouter-name*⟩ and virtual router ⟨*destination-vrouter-name*⟩ with IP prefix ⟨*ip_address*⟩/⟨*ip_mask*⟩ was ⟨*created_or_deleted*⟩
Meaning	A route import or export rule was created or removed from the current virtual routing instance. Route import rules determine whether the virtual routing instance should import routes from other specified routers. Route export rules determine whether a virtual routing instance should export routes from its routing table to other specified routers.
Action	No recommended action

Message	An ⟨*import_or_export_rule*⟩ rule in virtual router ⟨*source-vrouter-name*⟩ to virtual router ⟨*destination-vrouter-name*⟩ with route map ⟨*route-map-name*⟩ and protocol ⟨*protocol-name*⟩ was ⟨*created_or_deleted*⟩
Meaning	A route import/export rule was created or removed from the current virtual routing instance. Route import rules determine whether the specified virtual routing instance should import routes from other specified routers. Route export rules determine whether a virtual routing instance should export routes from its routing table to other specified routers.
Action	No recommended action

Message	Ipv6 access list ⟨*access-list-id*⟩ created in vrouter ⟨*vrouter-name*⟩
Meaning	
Action	

Message	Ipv6 access list ⟨*access-list-id*⟩ sequence number ⟨*access-list-sequence-num*⟩ ⟨*permit_or_deny*⟩ ip ⟨*ip_address*⟩/⟨*ip_mask*⟩ created in vrouter ⟨*vrouter-name*⟩
Meaning	
Action	

Message	IPv6 access list ⟨*access-list-id*⟩ sequence number ⟨*access-list-sequence-num*⟩ ⟨*permit_or_deny*⟩ ip ⟨*ip_address*⟩/⟨*ip_mask*⟩ is being deleted in vrouter ⟨*vrouter-name*⟩
Meaning	
Action	

Message	Route entry with sequence number ⟨*route-map-sequence-number*⟩ in route map ⟨*route-map-name*⟩, virtual router ⟨*vrouter-name*⟩ was removed.
Meaning	A route map performs an action on a packet that attempts to enter the virtual routing instance. This message indicates a specified sequence in a route map was removed.
Action	No recommended action

Message	Route map entry with sequence number ⟨*route-map-sequence-number*⟩ in route map ⟨*route-map-name*⟩ in virtual router ⟨*vrouter-name*⟩ was created.
Meaning	An administrator added a new route entry in the identified route map.
Action	No recommended action

Message	Route map ⟨*route-map-name*⟩ in virtual router ⟨*vrouter-name*⟩ was removed.
Meaning	A route map performs an action on a packet that attempts to enter the virtual routing instance. This message indicates a specified route map was removed from the virtual routing instance.
Action	No recommended action

Message	⟨*configuration_command*⟩
Meaning	
Action	

Notification (00080)

Message	PBR policy ⟨*pbr_policy_name*⟩ added to virtual router ⟨*vrouter_name*⟩. Total policies in vr: ⟨*num_pbr_pol_in_vrouter*⟩.
Meaning	A PBR policy was added to a virtual router.
Action	No recommended action.

Message	PBR policy ⟨*pbr_policy_name*⟩ deleted from virtual router ⟨*vrouter_name*⟩. Total policies in vr: ⟨*num_pbr_pol_in_vrouter*⟩.
Meaning	A PBR policy was deleted from a virtual router.
Action	No recommended action.

Notification (00615)

Message	PBR policy ⟨*pbr_policy_name*⟩ lookup tree rebuilt successfully in virtual router ⟨*vrouter_name*⟩.
Meaning	The policy lookup tree for a policy has been rebuilt successfully.
Action	No recommended action.

Message	PBR policy ⟨*pbr_policy_name*⟩ rebuilding lookup tree for virtual router ⟨*vrouter_name*⟩.
Meaning	PBR policy lookup tree is being rebuilt for the specified policy because of the change in match-group or extended ACL configuration used by this PBR policy.
Action	No recommended action.

Chapter 48

SCCP

The following messages relate to the Skinny Client Control Protocol (SCCP), a standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet.

Alert

Message Can't allocate memory for SCCP call context.

Alert

Message Can't allocate NAT cookie (Cause is probably too many calls).

Alert

Message SCCP ALG strict parsing disabled on the device.

Alert

Message SCCP ALG strict parsing enabled on the device.

Alert (00062)

Message SCCP ALG call flood rate threshold set to default of ⟨*calls-per-minute*⟩ per minute.

Meaning A network administrator set the call flood protection to the default on the device.

Action No recommended action

Message SCCP ALG call flood rate threshold set to ⟨*calls-per-minute*⟩ calls per minute.

Meaning A network administrator set the call flood rate on the device.

Action No recommended action

Message	SCCP ALG disabled on the device.
Meaning	A network administrator disabled the SCCP ALG
Action	No recommended action

Message	SCCP ALG enabled on the device.
Meaning	A network administrator enabled the SCCP ALG
Action	No recommended action

Message	SCCP ALG inactive media timeout configured to default ⟨*inactive-media-timeout*⟩ seconds.
Meaning	A network administrator set the inactive-media-timeout parameter to the default value.
Action	No recommended action

Message	SCCP ALG inactive media timeout configured to ⟨*inactive-media-timeout*⟩ seconds.
Meaning	A network administrator set the inactive-media-timeout parameter to the specified value.
Action	No recommended action

Message	SCCP ALG protection against call flood is disabled.
Meaning	A network administrator disabled call flood protection on the device.
Action	No recommended action

Message	SCCP ALG protection against call flood is enabled.
Meaning	A network administrator enabled call flood protection on the device.
Action	No recommended action

Message	SCCP ALG registered line break to ⟨*type-of-line-break-proxy-or-rsm*⟩.
Meaning	The device cannot initialize the SCCP ALG service.
Action	No recommended action

Message	SCCP ALG will drop the unknown messages in NAT mode.
Meaning	A network administrator set the SCCP ALG to deny unknown messages in NAT mode. This means the security device will not accept SCCP messages of unknown type. This is the default.
Action	No recommended action

Message	SCCP ALG will drop the unknown messages in route mode.
Meaning	A network administrator set the SCCP ALG to deny unknown messages in Route mode. This means the security device will not accept SCCP messages of unknown type. This is the default.
Action	No recommended action

Message	SCCP ALG will not drop the unknown messages in NAT mode.
Meaning	A network administrator set the SCCP ALG to permit unknown messages in NAT mode. This means the security device will accept SCCP messages of unknown type.
Action	No recommended action

Message	SCCP ALG will not drop the unknown messages in route mode.
Meaning	A network administrator set the SCCP ALG to permit unknown messages in Route mode. This means the security device will accept SCCP messages of unknown type.
Action	No recommended action

Alert (00083)

Message	SCCP ALG maximum call environment value (⟨*sccp_max_call_env_value*⟩) invalid, maximum call number set to ⟨*sccp_max_call_value_set*⟩.
Meaning	The SCCP maximum call value is not within the acceptable range
Action	No recommended action

Message	SCCP call from ⟨*client-ip-address*⟩ dropped due to out-bound call rate exceed from that client.
Meaning	The call from specified address was dropped because the outbound call rate for that client was exceeded.
Action	No recommended action

Message	The device cannot delete SCCP ALG Port.
Meaning	The device failed to delete the SCCP ALG service
Action	No recommended action

Message	The device cannot initialize memory for SCCP.
Meaning	The device failed to initialize the SCCP ALG service
Action	No recommended action

Message	The device cannot register SCCP Port.
Meaning	The device cannot initialize the SCCP ALG service.
Action	No recommended action

Message	The device cannot register the Network Address Translation vector for the SCCP ALG request.
Meaning	The device cannot initialize the SCCP ALG service.
Action	No recommended action

Message	The device cannot register the SCCP ALG request to RM.
Meaning	The device cannot initialize the SCCP ALG service.
Action	No recommended action

Message	The device cannot unregister SCCP ALG handler.
Meaning	The device failed to delete the SCCP ALG service
Action	No recommended action

Message	The device does not have SCCP ALG client id with RM.
Meaning	The device cannot initialize the SCCP ALG service.
Action	No recommended action

Message	The device failed in handling SCCP call since number of calls exceeded the system limit.
Meaning	The SCCP call failed because the number of calls exceeded the system limit.
Action	No recommended action

Message	The device failed in registering SCCP client with VSIP.
Meaning	The device failed to initialize the SCCP ALG service.
Action	No recommended action

Message	The device failed in unregistering SCCP client with RM.
Meaning	When a network administrator unset the SCCP ALG, the device failed to remove the SCCP ALG.
Action	No recommended action

Notification

Message	SCCP decoder error ⟨*msg*⟩.

Notification (00561)

Message	The device cannot allocate sufficient memory for the SCCP ALG request.
Meaning	The device cannot initialize the SCCP ALG service.
Action	No recommended action

Chapter 49

Schedule

The following message relates to schedules created for use in access policies.

Notification (00020)

Message	Schedule ⟨*sched_name*⟩ ⟨*action_added_modified_deleted*⟩ ⟨*config_changer*⟩.
Meaning	An admin has added, modified, or deleted the specified schedule.
Action	No recommended action.

Chapter 50
Service

The following messages relate to user-defined and predefined services, and service groups.

Notification (00012)

Message	Service group ⟨*service_group_name*⟩ ⟨*config_action_add_delete_member*⟩ ⟨*member_name*⟩ ⟨*config_changer*⟩.
Meaning	An admin has added the specified service to or deleted a service from the named service group
Action	No recommended action.

Message	Service group ⟨*service_group_name*⟩ ⟨*config_action_add_delete_modify*⟩ ⟨*config_changer*⟩.
Meaning	An admin has added, modified, or deleted the specified service group.
Action	No recommended action.

Message	Service ⟨*service_name*⟩ ⟨*config_action_add_delete_modify*⟩ ⟨*config_changer*⟩.
Meaning	An admin has added, modified, or deleted the specified user-defined service.
Action	No recommended action.

Chapter 51
SFP

The following messsages relate to small form-factor pluggable (SFP) connections.

Critical (00620)

Message	Sfp error: get ⟨*register type*⟩ register (dev ⟨*device number*⟩, reg ⟨*register number*⟩) fail.
Meaning	The SFP module encountered an error.
Action	Record the error message and number then contact Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered customer.)

Message	Sfp error: set ⟨*register type*⟩ register (dev ⟨*device number*⟩, reg ⟨*register number*⟩, value 0x⟨*register value*⟩) fail.
Meaning	The SFP module encountered an error.
Action	Record the error message and number then contact Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered customer.)

Critical (00752)

Message	Sfp error: ⟨*error information*⟩.
Meaning	The SFP module encountered an error.
Action	Record the error message and number then contact Juniper Networks technical support by visiting http://www.juniper.net/support. (Note: You must be a registered customer.)

Notification (00620)

Message	Sfp event: ⟨*event information*⟩.
Meaning	Informational message
Action	No recommended action

Message	Sfp event: the status of sfp interface ⟨*interface name*⟩ change to link ⟨*current link status*⟩, duplex ⟨*current duplex*⟩, speed ⟨*current speed*⟩.
Meaning	The interface changed to the specified state.
Action	No recommended action

Message	Sfp init: ⟨*init information*⟩.
Meaning	Informational message
Action	No recommended action

Message	Sfp setting: set interface ⟨*interface name*⟩ ⟨*interface setting*⟩.
Meaning	The interface changed to the specified state.
Action	No recommended action

Chapter 52
SHDSL

The following messages relate to symmetric high-speed digital subscriber line (SHDSL) connections.

Notification

Message	configure G.SHDSL interface ⟨*interface*⟩: ⟨*config*⟩.

Notification

Message	interface ⟨*interface*⟩ error: ⟨*event*⟩.
Meaning	The specified G.SHDSL interface encountered an error.
Action	Use the get interface < interface > CLI command to check connection status. Confirm that all cables are connected. Confirm that the configuration of the G.SHDSL interface matches the configuration at the remote interface.

Notification (00617)

Message	interface ⟨*interface*⟩ link status change to up.
Meaning	The G.SHDSL interface is connected.
Action	No recommended action.

Message	G.SHDSL card on slot ⟨*slot number*⟩ is found.
Meaning	The system found a G.SHDSL card in the specified slot.
Action	No recommended action.

Message	G.SHDSL card on slot ⟨*slot number*⟩ set up completely.
Meaning	The G.SHDSL card in the specified slot is properly configured.
Action	No recommended action.

Message	interface ⟨*interface*⟩ link status change to down.
Meaning	The G.SHDSL interface is no longer connected.
Action	Use the get interface < interface > CLI command to check connection status.

Chapter 53

SIP

The following messages relate to the Session Initiation Protocol (SIP), a standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet.

Alert (00046)

Message	An administrator disables SIP ALG.
Meaning	An administrator disabled the SIP Application Layer Gateway (ALG).
Action	No recommended action.

Notification (00046)

Message	An administrator enables SIP ALG.
Meaning	An administrator enabled the SIP Application Layer Gateway (ALG).
Action	No recommended action.

Message	An administrator enables SIP IP denial protection for all servers.
Meaning	An administrator set the SIP IP denial protection for all SIP proxy servers. This means the security device will deny repeat SIP INVITE requests to all proxy servers that denied an initial request, for the specified timeout period, before it begins accepting them again.
Action	No recommended action.

Message	An administrator permits SIP unknown messages in NAT mode.
Meaning	An administrator set the security device to allow SIP messages of unknown Method type in Network Address Translation (NAT) mode.
Action	No recommended action.

Message	An administrator permits SIP unknown messages in route mode.
Meaning	An administrator set the security device to allow SIP messages of unknown Method type in route mode.
Action	No recommended action.

Message	An administrator set SIP IP denial timeout to default.
Meaning	An administrator set the SIP IP denial to the default, which is five seconds, This means the security device will deny repeat SIP INVITE requests to a proxy server that denied the initial request for a period of 5 seconds before it begins accepting them again.
Action	No recommended action.

Message	An administrator set SIP unknown messages permission to default.
Meaning	An administrator set the SIP unknown messages feature to default mode, which is to not permit SIP messages of unknown Method type, in route mode.
Action	No recommended action.

Message	An administrator set the media inactivity timeout value to its default value of ⟨*timeout*⟩ seconds.
Meaning	An administrator has set the media inactivity timeout value to its default value. The media inactivity timeout parameter indicates the maximum length of time a call can remain active without any SIP signaling traffic.
Action	No recommended action.

Message	An administrator set the SIP invite timeout value to its default value of ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP INVITE request, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, the device removes the call. This message indicates an administrator set the SIP INVITE request timeout value to its default value.
Action	No recommended action.

Message An administrator set the SIP invite timeout value to ⟨*timeout*⟩ seconds.

Meaning When the device receives a SIP INVITE request, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, then the device removes the call. This message indicates an administrator modified the SIP INVITE default timeout value.

Action No recommended action.

Message An administrator set the SIP media inactivity timeout value to ⟨*timeout*⟩ seconds.

Meaning An administrator has modified the media inactivity timeout value. The media inactivity timeout parameter indicates the maximum length of time a call can remain active without any SIP signaling traffic.

Action No recommended action.

Message An administrator set the SIP ringing timeout value to its default value of ⟨*timeout*⟩ seconds.

Meaning When the device receives a SIP Ringing response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, the device removes the call. This message indicates an administrator set the SIP Ringing response timeout value to its default value.

Action No recommended action.

Message An administrator set the SIP ringing timeout value to ⟨*timeout*⟩ seconds.

Meaning When the device receives a SIP Ringing response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, then the device removes the call. This message indicates an administrator modified the SIP Ringing timeout value.

Action No recommended action.

Message An administrator set the SIP signaling inactivity timeout value to its default value of ⟨*timeout*⟩ seconds.

Meaning An administrator set the SIP signaling inactivity timeout value to its default value. If no signaling occurs for the call within the amount of time specified by the signaling inactivity timeout value, then the device removes the call.

Action No recommended action.

Message	An administrator set the SIP signaling inactivity timeout value to ⟨*timeout*⟩ seconds.
Meaning	An administrator modified the SIP signaling inactivity value. If no signaling occurs for the call within the amount of time specified by the signaling inactivity timeout value, the device removes the call.
Action	No recommended action.

Message	An administrator set the SIP trying timeout value to its default value of ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP Trying response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, the device removes the call. This message indicates an administrator set the SIP Trying response timeout value to its default value.
Action	No recommended action.

Message	An administrator set the SIP trying timeout value to ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP Trying response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, then the device removes the call. This message indicates an administrator modified the SIP Trying timeout value.
Action	No recommended action.

Message	An administrator sets SIP C timeout to default value.
Meaning	An administrator set the SIP C timeout, the INVITE transaction timeout at the proxy, to the default value, which is 30 minutes.
Action	No recommended action.

Message	An administrator sets SIP C timeout to ⟨*timeout*⟩ minutes.
Meaning	An administrator set the SIP C timeout, which is the INVITE transaction timeout at the proxy.
Action	No recommended action.

Message An administrator sets SIP IP denial protection for IP ⟨*ip*⟩.

Meaning An administrator set the SIP IP denial protection for the SIP proxy server with the specified IP address. This means the security device will deny repeat SIP INVITE requests to the proxy server with the specified IP address, for the specified timeout period, before it begins accepting them again.

Action No recommended action.

Message An administrator sets SIP IP denial protection for IPv6 ⟨*ip*⟩.

Meaning An administrator set the SIP IP denial protection for the SIP proxy server with the specified IP address. This means the security device will deny repeat SIP INVITE requests to the proxy server with the specified IP address, for the specified timeout period, before it begins accepting them again.

Action No recommended action.

Message An administrator sets SIP IP denial timeout to ⟨*time*⟩.

Meaning An administrator set the SIP IP denial timeout value. This value determines how long the security device will deny repeat SIP INVITE requests to a proxy server that denied the initial request before it begins accepting them again.

Action No recommended action.

Message An administrator sets SIP T1 interval to default value.

Meaning An administrator set the SIP T1 interval, the roundtrip time estimate of a transaction between endpoints, to the default value, which is 500 milliseconds.

Action No recommended action.

Message An administrator sets SIP T1 interval to ⟨*timeout*⟩ msec.

Meaning An administrator set the SIP T1 interval, which is the roundtrip time estimate of a transaction between endpoints.

Action No recommended action.

Message An administrator sets SIP T4 interval to default value.

Meaning An administrator set the SIP T4 interval, the maximum time a message remains in the network, to the default value, which is 5 seconds.

Action No recommended action.

Message	An administrator sets SIP T4 interval to ⟨*timeout*⟩ seconds.
Meaning	An administrator set the SIP T4 interval, which is the maximum time a message remains in the network.
Action	No recommended action.

Message	An administrator sets SIP unknown messages permission to default.
Meaning	An administrator set the security device to allow SIP messages of unknown Method type in Network Address Translation (NAT) mode.
Action	No recommended action.

Message	An administrator unsets SIP IP denial protection for IP ⟨*ip*⟩.
Meaning	An administrator unset the SIP IP denial timeout value, This means the security device will not protect the proxy server with that IP address from repeat INVITE requests.
Action	No recommended action.

Message	An administrator unsets SIP IP denial protection for IPv6 ⟨*ip*⟩.
Meaning	An administrator unset the SIP IP denial timeout value, This means the security device will not protect the proxy server with that IP address from repeat INVITE requests.
Action	No recommended action.

Message	An administrator unsets SIP IP denial protection.
Meaning	An administrator unset the SIP IP denial protection, This means the security device will not protect the proxy server from repeat INVITE requests.
Action	No recommended action.

Notification (00767)

Message	Cannot allocate SIP call because device is fielding too many calls.
Meaning	The device does not have enough resources to process the current call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Security devices do not support multicast IP addresses ⟨*ip_addr*⟩ in SIP ⟨*header_field* > ⟩.
Meaning	The security device received a SIP message in which the destination IP address is a multicast IP address, but Juniper Networks does not currently support multicast with SIP.
Action	No recommended action.

Message	Security devices do not support multiple IP addresses ⟨*ip_addr*⟩ or ports ⟨*port* > ⟩ in SIP headers ⟨*header_field* > ⟩.
Meaning	Juniper Networks security devices do not support multiple IP addresses or ports in SIP headers.
Action	No recommended action.

Message	SIP ALG is unregistered by RM.
Meaning	A non-specific internal error occurred in the SIP Application Layer Gateway (ALG).
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SIP call information data is too long.
Meaning	The size of some of the SIP header fields exceeds the maximum size limit and the device might not be able to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SIP parser error ⟨*msg*⟩.
Meaning	The SIP Application Layer Gateway (ALG) parser, which processes SIP messages, encountered an unknown error.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SIP structure is corrupted.
Meaning	A non-specific internal error occurred in the SIP Application Layer Gateway (ALG).
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot allocate sufficient memory for the SIP ALG request.
Meaning	During the process of an incoming call, the device does not have enough memory to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot initialize memory pool.
Meaning	The device failed to initialize the SIP Application Layer Gateway (ALG) service.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot initialize SIP Endpoint listener.
Meaning	The device failed to initialize the SIP Application Layer Gateway (ALG) service.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot initialize SIP Endpoint.
Meaning	The device failed to initialize the SIP Application Layer Gateway (ALG) service.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot register SIP ALG port.
Meaning	The device failed to initialize the SIP Application Layer Gateway (ALG) service.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot register the NAT vector for the SIP ALG request.
Meaning	The device cannot write the Network Address Translation (NAT) vector being requested by the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot register the SIP ALG request to RM.
Meaning	During the initialization of the SIP Application Layer Gateway (ALG), where resources are being allocated, the gateway module could not contact the Resource Manager.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot remove SIP ALG port.
Meaning	The device failed to initialize the SIP Application Layer Gateway (ALG) service.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device failed to remove NAT vector.
Meaning	When an administrator unset the SIP Application Layer Gateway (ALG), the device failed to remove the SIP ALG service.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Too many call segments for response.
Meaning	The device does not have enough resources to process the current call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Too many call segments.
Meaning	The device does not have enough resources to process the current call.
Action	No recommended action.

Message	Transaction data is too long.
Meaning	The size of some of the SIP header fields exceeds the maximum size limit and the device might not be able to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Transaction data too long for response.
Meaning	The size of some of the SIP header fields exceeds the maximum size limit and the device might not be able to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Chapter 54
SNMP

The following messages pertain to the Simple Network Management Protocol (SNMP).

Notification (00002)

Message	SNMP listen port has been changed from ⟨*integer*⟩ to ⟨*integer*⟩.
Meaning	An admin has changed the user-configured SNMP listen port number to another user-configured port number.
Action	Advise the SNMP admin to change the port number on the SNMP manager at which it makes SNMP requests.

Notification (00031)

Message	SNMP system contact has been changed to ⟨*string*⟩.
Meaning	An admin has modified the SNMP contact name.
Action	No recommended action

Message	SNMP system location has been changed to ⟨*string*⟩.
Meaning	An admin has modified the information about the physical location of the security device.
Action	No recommended action

Message	SNMP system name has been changed to ⟨*string*⟩.
Meaning	An admin has modified the SNMP system name.
Action	No recommended action

Information ()

Message	SNMP request has been received from host ⟨*IP address*⟩:⟨*integer*⟩ with read-only privileges.
Meaning	An SNMP request from a host at the specified IP address and port number with read-only privileges has been received.
Action	If you want the host to have read/write privileges, change the configuration on the security device for that SNMP community to permit it.

Information (00524)

Message	SNMP request from an unknown SNMP community ⟨*string*⟩ at ⟨*IP address*⟩:⟨*integer*⟩ has been received.
Meaning	A request from the specified SNMP manager has been received. However, the security device does not recognize the specified SNMP community name.
Action	If the SNMP manager IP address and port number are legitimate, advise the SNMP admin to check the configuration.

Message	SNMP request from ⟨*IP address*⟩:⟨*integer*⟩ has been received, but the SNMP version type is incorrect.
Meaning	A request from the specified SNMP manager has been received. However, the SNMP manager making the request uses a different version of the protocol and the agent cannot respond to the request.
Action	If the request is from a legitimate SNMP manager, advise the admin to use SNMP version 1 or 2c.

Message	SNMP request has been received from an unknown host in SNMP community ⟨*string*⟩ at ⟨*IP address*⟩:⟨*integer*⟩.
Meaning	An SNMP request from an unknown host in the specified SNMP community has been received.
Action	If the SNMP request is from a legitimate SNMP community member, add the IP address for that host to the SNMP community configuration on the security device.

Message	SNMP request has been received from host ⟨*IP address*⟩:⟨*integer*⟩ without read privileges .
Meaning	An SNMP request from a host at the specified IP address and port number without read privileges has been received.
Action	If you want the host to have read privileges, change the configuration on the security device for that SNMP community to permit it.

Message	SNMP response to the SNMP request from ⟨*IP address*⟩:⟨*integer*⟩ has failed due to a coding error.
Meaning	When the security device responded to an SNMP request, a BER coding/decoding error occurred. BER (Basic Encoding Rules) converts data into bits and bytes and is the transfer syntax for SNMP.
Action	Advise the SNMP admin to retry.

Message	SNMP: The security device has responded successfully to the SNMP request from ⟨*IP address*⟩:⟨*integer*⟩.
Meaning	The SNMP agent located in the security device has successfully responded to an SNMP request from the specified SNMP manager.
Action	No recommended action

Chapter 55
SSHv1

The following messages relate to events generated during configuration or operation of SSHv1 (Secure Shell, version 1).

Critical (00034)

Message	SSH: FIPS self test failed.
Meaning	The device unsuccessfully performed a FIPS self test during the SSH connection procedure.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SSH: Security device failed to generate a PKA RSA challenge for SSH admin ⟨*admin_name*⟩ at ⟨*ip_addr*⟩ (Key ID ⟨*key_id*⟩).
Meaning	The device unsuccessfully performed a FIPS self test during the SCS connection procedure.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SSH: Unable to perform FIPS self test.
Meaning	The device unsuccessfully attempted to perform a FIPS self test during the SSH connection procedure.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Error (00034)

Message	SSH: Maximum number of SSH sessions (⟨*max_count*⟩) exceeded. Connection request from SSH user ⟨*admin_name*⟩ at ⟨*ip_addr*⟩ denied.
Meaning	The maximum number of concurrent SSH sessions was reached. Depending on the specific platform, this number can be 3 to 24. If this value is exceeded, the device denies the connection request from the SSH admin.
Action	The admin should wait for one of the currently active sessions to close before attempting another SCS connection.

Message	SSH: Unable to validate cookie from the SSH client at ⟨*ip_addr*⟩.
Meaning	The specified SSH client sent an invalid cookie during the SSH connection procedure.
Action	An attempted security attack might be in progress. First, validate the source of the connection attempt. If you repeatedly receive this message, you might want to disable SSH until you determine the cause.

Error (00528)

Message	SSH: Failed to send identification string to client host at ⟨*ip_addr*⟩.
Meaning	The device, acting as the SSH server, failed to identify itself or send the identification string to the specified SSH client during the SSH connection procedure. This most likely is the result of a low-level internal processing error.
Action	The SSH admin should initiate another connection with the device. If the problem persists, reset the device and have the SSH admin try again.

Message	SSH: Incompatible SSH version string has been received from SSH client at ⟨*ip_addr*⟩.
Meaning	The device, acting as the SCS server, has received an incompatible version of the SSH protocol from the specified SSH client during the SCS connection procedure.
Action	The SSH admin should run SSH version 1 for compatibility with a device.

Message	SSH: Security device failed to identify itself to the SSH client at ⟨*ip_addr*⟩.
Meaning	The device, acting as the SCS server, failed to identify itself to the specified SSH client during the SCS connection procedure. This most likely is the result of a low-level internal processing error.
Action	The SSH admin should initiate another connection with the device. If the problem persists, reset the device and have the SSH admin try again.

Warning (00528)

Message	SSH: Disabled for ⟨*vsys_name*⟩. Attempted connection failed from ⟨*addr*⟩:⟨*port*⟩.
Meaning	The specified SSH client has attempted to make an SSH connection to the specified virtual system. However, because SSH is not enabled for that virtual system, the attempt was unsuccessful.
Action	If you want the SSH client to be able to access the specified virtual system via SCS, enter that virtual system and enable SSH manageability.

Message	SSH: Host client has requested NO cipher from ⟨⟩.
Meaning	The host client has requested that no encryption algorithm be used for the SSH message exchange.
Action	The SSH client should reconfigure its request, using a cipher algorithm supported by the device, to make the connection more secure.

Message	SSH: SSH client at ⟨*remote_addr*⟩ tried unsuccessfully to establish an SSH connection to interface ⟨*interface_name*⟩ with IP ⟨*local_addr*⟩ SSH disabled on that interface.
Meaning	The specified SSH client has attempted to make an SCS connection to the device at the specified interface. However, because SCS was not enabled on that interface, the attempt was unsuccessful.
Action	If you want the SSH client to be able to access the device on the specified interface via SCS, enable SCS manageability for that interface.

Message	SSH: SSH client at ⟨*remote_addr*⟩ tried unsuccessfully to make an SSH connection to interface ⟨*interface_name*⟩ with IP ⟨*local_addr*⟩ SSH not enabled on that interface.
Meaning	The specified SSH client has attempted to make an SCS connection to the device at the specified interface. However, because SCS was not enabled on that interface, the attempt was unsuccessful.
Action	If you want the SSH client to be able to access the device on the specified interface via SCS, enable SCS manageability for that interface.

Message	SSH: SSH client ⟨*ip_addr*⟩ unsuccessfully attempted to make an SSH connection to ⟨*vsys_name*⟩ SSH was not completely initialized for that system.
Meaning	The SCS utility was unable to generate the host and server keys for the specified virtual system on the device before the connection request timed out.
Action	The SSH client should wait one minute and then attempt another SCS connection.

Message	SSH: SSH user ⟨*admin_name*⟩ at ⟨*ip_addr*⟩ tried unsuccessfully to log in to ⟨*vsys_name*⟩ using the shared untrusted interface. SSH disabled on that interface.
Meaning	The specified SSH admin failed to make an SSH connection to the specified virtual system, which shares the untrusted interface with the root system.
Action	Because the device uses the host and server keys of the root system and not those of the virtual system when sharing the untrusted interface, make sure that the SSH client has the public host key of the root system loaded on its system. To allow SSH management of a virtual system sharing the untrusted interface with the root system, make sure that SSH is enabled at the root level. As an option, create a separate untrusted subinterface for that virtual system and enable SSH manageability on its untrusted subinterface.

Message	SSH: Unsupported cipher type '⟨*cipher_name*⟩' requested from ⟨*ip_addr*⟩.
Meaning	The specified SSH client attempted to make an SSH connection to the device but failed because it requested a cipher not supported by the device.
Action	The SSH client should reconfigure its request, using a cipher supported by the device (DES and 3DES are supported) and then attempt another SCS connection.

Information (00026)

Message	SSH: SSH disabled for ⟨*vsys_name*⟩.
Meaning	An administrator disabled SSH for the device.
Action	No recommended action.

Message	SSH: SSH enabled for ⟨*vsys_name*⟩.
Meaning	An administrator enabled SSH for the device.
Action	No recommended action.

Information (00528)

Message	SSH: Connection has been terminated for admin user ⟨*admin_name*⟩ at ⟨*ip_addr*⟩.
Meaning	The connection to a host running an SSH session with the device terminated.
Action	No recommended action.

Message	SSH: Key regeneration interval has been changed from ⟨*old_interval*⟩ to ⟨*new_interval*⟩.
Meaning	An admin changed the interval between automatic updates of SSH keys.
Action	No recommended action.

Message	SSH: SSH has been disabled for ⟨*vsys_name*⟩ with ⟨*key_count*⟩ existing PKA key(s) bound to ⟨*user_count*⟩ SSH user(s).
Meaning	The specified vsys has been disabled for SSH. The vsys now has the number of PKA keys indicated, which are bound to the specified number of users for that vsys.
Action	No recommended action.

Message	SSH: SSH has been enabled for ⟨*vsys_name*⟩ with ⟨*key_count*⟩ existing PKA key(s) bound to ⟨*user_count*⟩ SSH user(s).
Meaning	The specified vsys has been enabled for SSH. The vsys now has the number of PKA keys indicated, which are bound to the specified number of users for that vsys.
Action	No recommended action.

Message	SSH: SSH user ⟨*admin_name*⟩ at ⟨*ip_addr*⟩ failed the PKA RSA challenge. (Key ID ⟨*key_id*⟩).
Meaning	An admin tried to establish an SSH session with the Security device, but PKA RSA authentication failed.
Action	No recommended action.

Message	SSH: SSH user ⟨*admin_name*⟩ at ⟨*ip_addr*⟩ has requested password authentication, which is not enabled for that user.
Meaning	An admin attempted to authenticate using a password that does not belong to that admin.
Action	No recommended action.

Message	SSH: SSH user ⟨*admin_name*⟩ at ⟨*ip_addr*⟩ has requested PKA RSA authentication which is not supported for that user.
Meaning	An admin attempted to use PKA RSA authentication without the necessary admin account permission.
Action	No recommended action.

Message	SSH: SSH user ⟨*admin_name*⟩ has been authenticated using password from ⟨*ip_addr*⟩.
Meaning	The named admin has been authenticated.
Action	No recommended action.

Message	SSH: SSH user ⟨*admin_name*⟩ has been authenticated using PKA RSA from ⟨*ip_addr*⟩ (Key ID ⟨*key_id*⟩).
Meaning	An admin successfully authenticated with the device via SSH.
Action	No recommended action.

Chapter 56
SSHv2

The following messages relate to events generated during configuration or operation of SSHv1 (Secure Shell, version 2).

Critical (00034)

Message	SCP: Admin user '⟨*admin_name*⟩' attempted to transfer file '⟨*direction*⟩' ⟨*file_name*⟩ the device with insufficient privilege.
Meaning	An admin attempted to transmit a file using SSH without the necessary privilege.
Action	Check the permissions granted by the device.

Message	SSH: Error processing packet from host ⟨*addr*⟩ (Code ⟨*code_id*⟩).
Meaning	The device received an invalid SSH packet, and dropped the packet.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SSH: Failed to retrieve PKA key bound to SSH user ⟨*admin_name*⟩ (Key ID ⟨*key_id*⟩).
Meaning	The device unsuccessfully attempted to retrieve the specified Public Key Authentication (PKA) key bound to the specified admin attempting to log in using SSH.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Error (00026)

Message	SSH: Attempt to bind duplicate PKA key to admin user '⟨*admin_name*⟩' (Key ID ⟨*key_id*⟩).
Meaning	An admin attempted to bind a Public Key Authentication (PKA) key to an admin when the key already existed for that admin.
Action	Verify that the specified key is actually bound to the specified admin.

Message	SSH: Failed to bind PKA key to SSH admin user '⟨*admin_name*⟩'. (Key ID ⟨*key_id*⟩).
Meaning	An admin unsuccessfully attempted to bind or unbind the specified Public Key Authentication (PKA) key to the specified admin.
Action	If binding is the problem, it might be that the specified PKA key is already bound to the specified admin or that four PKA keys (the maximum) are already bound to the admin. In the latter case, you must first unbind one of the other keys from the admin before binding the new one. If unbinding is the problem, verify that the specified key is actually bound to the specified admin.

Message	SSH: Failed to unbind PKA key from admin user '⟨*admin_name*⟩' (Key ID ⟨*key_id*⟩).
Meaning	An admin unsuccessfully attempted to bind or unbind the specified Public Key Authentication (PKA) key to the specified admin.
Action	If binding is the problem, it might be that the specified PKA key is already bound to the specified admin or that four PKA keys (the maximum) are already bound to the admin. In the latter case, you must first unbind one of the other keys from the admin before binding the new one. If unbinding is the problem, verify that the specified key is actually bound to the specified admin.

Message	SSH: Maximum number of PKA keys (⟨*max_key_count*⟩) has been bound to user '⟨*admin_name*⟩' Key not bound. (Key ID ⟨*key_id*⟩).
Meaning	An admin unsuccessfully attempted to bind a Public Key Authentication (PKA) key to the specified admin beyond the maximum number of keys allowed for that admin.
Action	First unbind one of the other keys from the admin before binding the new one.

Error (00034)

Message	SSH: Device failed to send initialization string to client at ⟨*ip_addr*⟩.
Meaning	The device, acting as the SCS server, failed to identify itself or send the identification string to the specified SSH client during the SCS connection procedure. This most likely is the result of a low-level internal processing error.
Action	The SSH admin should initiate another connection with the device. If the problem persists, reset the device and have the SSH admin try again.

Error (00528)

Message	SSH: Client at ⟨*ip_addr*⟩ attempted to connect with invalid version string.
Meaning	The first step of the SSH connection process is for the client and the server to exchange SSH version strings. During this process, the device, acting as the SCS server, has received an incompatible version of the SSH protocol from the specified SSH client during the SCS connection procedure. Although the device supports SSHv1 and SSHv2, it only supports one of these versions at a time. For example, if the device is configured for SSHv2 and a client attempts to connect to the device with an SSHv1 application, the device generates this message. In addition, this message could mean that a remote host inappropriately connected to the SSH port on the device. This could mean that an attacker is trying to gain access to the device.
Action	The SSH admin should run whatever SSH version the device uses, for compatibility.

Message	SSH: Failed to negotiate encryption algorithm with host ⟨*ip_addr*⟩.
Meaning	The device could not resolve the encryption algorithm with a host and the negotiation failed.
Action	Verify that the SSH client is configured to negotiate an encryption algorithm that the device supports. Note: For this release, SSHv2 implementation on the device supports only the 3DES encryption algorithm.

Message	SSH: Failed to negotiate host key algorithm with host ⟨*ip_addr*⟩.
Meaning	The device and the SSH client could not agree on a host key algorithm. The device uses the host key algorithm to authenticate the device to a SSH client during the initial SSH connection setup phase.
Action	Verify that the SSH client is configured to support a host key algorithm supported by the device. Note: At this time, the device supports only the DSA algorithm for host key authentication.

Message	SSH: Failed to negotiate key exchange algorithm with host ⟨*ip_addr*⟩.
Meaning	The device failed to establish a session key because an error occurred during key exchange.
Action	Verify that the SSH client is configured to use a KEX algorithm supported by the device. Note: Devices currently support the Diffie-Hellman KEX algorithm only.

Message	SSH: Failed to negotiate MAC algorithm with host ⟨*ip_addr*⟩.
Meaning	The device and the SSH client failed to negotiate a MAC algorithm. The SSH connection that the SSH client attempted to create with the device was not created.
Action	Verify that the SSH client is configured to use a MAC algorithm supported by the devices. Note: For this release, devices currently support the SHA MAC algorithm only.

Warning (00528)

Message	SCP: Admin user '⟨*admin_name*⟩' requested unknown file '⟨*file_name*⟩'.
Meaning	An admin requested an unknown or unavailable file from the SSH client.
Action	No recommended action.

Message	SCP: Admin '⟨*admin_name*⟩' at host ⟨*ip_addr*⟩ executed invalid scp command: '⟨*command*⟩'.
Meaning	The specified admin executed a Simple Control Protocol (SCP) command that failed. SCP is a protocol with which files can be transferred to or from the device in a secure manner. The SSH protocol provides the security of SCP, which includes authentication, encryption, and integrity for the SCP connection.
Action	The admin should retry the command.

Message	SCP: Disabled for '⟨*vsys_name*⟩'. Attempted file transfer failed from host ⟨*ip_addr*⟩.
Meaning	The specified SSH client has attempted to make a Simple Control Protocol (SCP) connection to the specified virtual system. However, because SCP is not enabled for that virtual system, the attempt was unsuccessful.
Action	If you want the SSH client to be able to access the specified virtual system via SCP, enter that virtual system and enable SCP manageability.

Message	SSH: Admin '⟨*admin_name*⟩' at host ⟨*ip_addr*⟩ attempted to be authenticated with no authentication methods enabled.
Meaning	While attempting to make an SSH connection to the device, the specified SSH admin requested an authentication mode, when no such modes are enabled
Action	Enable the requested authentication method on the device.

Message	SSH: Admin user '⟨*admin_name*⟩' at host ⟨*ip_addr*⟩ requested unsupported PKA algorithm ⟨*pka_alg_name*⟩.
Meaning	While attempting to make an SSH connection to the device, the specified SSH admin requested an authentication mode, such as password or Public Key Authentication (PKA) RSA, that had not been configured for that admin.
Action	Enable the requested authentication method on the device or reconfigure the SSH client application to use the method already enabled on the device.

Message	SSH: Admin user ⟨*admin_name*⟩ at host ⟨*ip_addr*⟩ requested unsupported authentication method ⟨*auth_method_name*⟩.
Meaning	While attempting to make an SSH connection to the device, the specified SSH admin requested an authentication mode that had not been configured for that admin.
Action	Enable the requested authentication method on the device or reconfigure the SSH client application to use the method already enabled on the device.

Message	SSH: Disabled for '⟨*vsys_name*⟩'. Attempted connection failed from ⟨*addr*⟩:⟨*port*⟩.
Meaning	The specified SSH client has attempted to make an SSH connection to the specified virtual system. However, because SSH is not enabled for that virtual system, the attempt was unsuccessful.
Action	If you want the SSH client to be able to access the specified virtual system via SCS, enter that virtual system and enable SSH manageability.

Message	SSH: Password authentication failed for admin user '⟨*admin_name*⟩' at host. ⟨*ip_addr*⟩
Meaning	The device, acting as the SCS server, was able or unable to authenticate the specified SSH client during the SCS connection procedure. Failure occurs due to incorrect password.
Action	If failure occurs, the SSH admin should verify the password. Otherwise, No recommended action

Message	SSH: Password authentication successful for admin user '⟨*admin_name*⟩' at host ⟨*ip_addr*⟩.
Meaning	The device, acting as the SCS server, was able or unable to authenticate the specified SSH client during the SCS connection procedure. Failure occurs due to incorrect password.
Action	If failure occurs, the SSH admin should verify the password. Otherwise, no recommended action

Message	SSH: PKA authentication failed for admin user '⟨*admin_name*⟩' at host ⟨*ip_addr*⟩.
Meaning	The device, acting as the SCS server, was unable to authenticate the specified SSH client during the SCS connection procedure.
Action	The SSH admin should verify that the SSH client software is configured correctly and is using a cipher that the device supports (DES and 3DES are supported).

Message	SSH: PKA authentication successful for admin user '⟨*admin_name*⟩' at host ⟨*ip_addr*⟩.
Meaning	The device, acting as the SCS server, was unable to authenticate the specified SSH client during the SCS connection procedure.
Action	The SSH admin should verify that the SSH client software is configured correctly and is using a cipher that the device supports (DES and 3DES are supported).

Notification (00026)

Message	SCP: Admin user '⟨*admin_name*⟩' transferred file '⟨*file_name*⟩' from device to host ⟨*ip_addr*⟩.
Meaning	An admin used a Simple Control Protocol (SCP) to transfer a file from the device to the host residing at the specified IP address.
Action	No recommended action.

Message	SCP: Admin user '⟨*admin_name*⟩' transferred file '⟨*file_name*⟩' to device from host ⟨*ip_addr*⟩.
Meaning	An admin used a Simple Control Protocol (SCP) to transfer a file to memory on the device from the host residing at the specified IP address.
Action	No recommended action.

Information (00026)

Message	SSH: Host key deleted for ⟨*vsys_name*⟩.
Meaning	An administrator removed a host key for the specified vsys.
Action	An administrator removed a host key for the specified vsys.

Message	SSH: PKA key has been bound to admin user '⟨*admin_name*⟩' (Key ID ⟨*key_id*⟩).
Meaning	The root admin has either bound the public key with the specified key ID number to the named admin, or unbound the key from the admin. This key is used to authenticate the admin via Public Key Authentication (PKA) when making an SCS connection to the device.
Action	No recommended action.

Message	SSH: PKA key has been unbound from admin user '⟨*admin_name*⟩' (Key ID ⟨*key_id*⟩).
Meaning	The root admin has either bound the public key with the specified key ID number to the named admin, or unbound the key from the admin. This key is used to authenticate the admin via Public Key Authentication (PKA) when making an SCS connection to the device.
Action	No recommended action.

Message	SSH: SCP disabled for ⟨*vsys_name*⟩.
Meaning	An administrator enabled or disabled a Simple Control Protocol (SCP) for the specified vsys.
Action	No recommended action

Message	SSH: SCP enabled for ⟨*vsys_name*⟩.
Meaning	An administrator enabled or disabled a Simple Control Protocol (SCP) for the specified vsys.
Action	No recommended action.

Message	SSH: SSH disabled for ⟨*vsys_name*⟩.
Meaning	An admin enabled SSH for the specified virtual system (< vsys >).
Action	No recommended action.

Message	SSH: SSH enabled for ⟨*vsys_name*⟩.
Meaning	An admin enabled SSH for the specified virtual system (< vsys >).
Action	No recommended action.

Message	SSH: Upgrade performed (to version ⟨*version*⟩).
Meaning	An administrator performed an upgrade of SSH to new version.
Action	No recommended action.

Chapter 57
SSL

The following messages relate to the Secure Socket Layer (SSL) protocol.

Warning (00515)

Message	Admin user ⟨*admin_user_name*⟩ logged out for Web(⟨*protocol*⟩) management (port ⟨*dst_port*⟩) from ⟨*ip_addr*⟩:⟨*src_port*⟩
Meaning	An admin logged out from the specified username, protocol, address, and port.
Action	No recommended action.

Warning (00518)

Message	Admin user ⟨*admin_user_name*⟩ login attempt for Web(⟨*protocol*⟩) management (port ⟨*dst_port*⟩) from ⟨*ip_addr*⟩:⟨*src_port*⟩ failed due to an incorrect client ID.
Meaning	An admin attempted unsuccessfully to log in using the specified username, protocol, address, and port. The login attempt failed because the client ID was incorrect or not recognized.
Action	Ensure that the login attempt was legitimate.

Message	Admin user ⟨*admin_user_name*⟩ login attempt for Web(⟨*protocol*⟩) management (port ⟨*dst_port*⟩) from ⟨*ip_addr*⟩:⟨*src_port*⟩ failed.
Meaning	An admin attempted unsuccessfully to log in using the specified username, protocol, address, and port.
Action	Ensure that the login attempt was legitimate.

Warning (00519)

Message	Admin user ⟨*admin_user_name*⟩ logged in for Web(⟨*protocol*⟩) management (port ⟨*dst_port*⟩) from ⟨*ip_addr*⟩:⟨*src_port*⟩
Meaning	An admin logged in using the specified username, protocol, address, and port.
Action	No recommended action.

Notification (00035)

Message	⟨*name*⟩ SSL CA is changed to none ⟨*config_changer*⟩.
Meaning	A network administrator unset the specified Secure Socket Layer (SSL) certificate authority (CA).
Action	No recommended action.

Message	⟨*name*⟩ SSL certificate authority is changed to none ⟨*config_changer*⟩.
Meaning	A network administrator has made one of two changes to the certificate that is used when making an administrative connection to a device via Secure Socket Layer (SSL): The admin has changed the SSL configuration to use the default SSL certificate, which is the automatically generated self-signed certificate. If the automatically generated self-signed certificate was previously deleted, the admin has assigned no certificate for use with SSL.
Action	No recommended action.

Message	⟨*string*⟩ SSL certificate authority name is changed to ⟨*string*⟩.
Meaning	A network administrator changed the Secure Socket Layer (SSL) certificate authority (CA).
Action	No recommended action.

Message	⟨*string*⟩ SSL certificate is changed to ⟨*string*⟩.
Meaning	A network administrator changed the SSL certificate.
Action	No recommended action.

Message	⟨*string*⟩ SSL cipher name is changed from ⟨*string*⟩ to ⟨*string*⟩ ⟨*string*⟩.
Meaning	A network administrator changed the cipher used by the device to secure communications.
Action	No recommended action.

Information (00002)

Message	PKI: The device failed to generate the certificate request file in PKCS #10 format.
Meaning	The security device was unable to generate a certificate request file in PKCS #10 (Certificate Request Syntax Standard) format.
Action	Enter the get memory command to see how much RAM has been allocated and how much is still available. If there appears to be sufficient RAM available, reboot the security device and attempt to generate certificate request again. If there appears to be a severe memory problem or if your second attempt was also unsuccessful, contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	User ⟨*admin user*⟩ clicked Get Tech on WebUI
Meaning	An admin clicked the "Get Tech" button on the WebUI Help page.
Action	No recommended action.

Message	User ⟨*admin user*⟩ clicked Get Tech on WebUI, but response may not complete due to resource problem
Meaning	An admin clicked the "Get Tech" button on the WebUI Help page, but there may not have been adequate system resources to complete the operation. This message is usually caused by shortage of memory. The "get tech" file is large, and the Web task must collect all information in a RAM file before the web server can deliver the file to the user.
Action	Free some resources and try again.

Message	Web SSL port changed from ⟨*orig_port*⟩ to ⟨*new_port*⟩ ⟨*config_changer*⟩
Meaning	An admin has changed the port used for managing the device via SSL.
Action	No recommended action.

Message	Web SSL ⟨*status*⟩ ⟨*config_changer*⟩
Meaning	An admin has either enabled or disabled an SSL connection.
Action	No recommended action.

Information (00540)

Message	Firewall-only system does not allow ⟨*string*⟩ SSL cipher type ⟨*string*⟩.
Meaning	The specified cipher type is not allowed on a firewall-only system.
Action	Currently, 3DES is the only cipher type that is not allowed on a firewall-only system. Use a different cipher to secure communications.

Message	No context exists for the SSL connection. The device is not ready for an SSL connection.
Meaning	The device cannot make a Secure Socket Layer (SSL) connection because no SSL context exists.
Action	Configure SSL on the device.

Message	The subject field of the SSL certificate reports a mismatch with the subject name (⟨*string*⟩ received while expecting subject name ⟨*string*⟩).
Meaning	The Secure Socket Layer (SSL) context on the device received a certificate with the wrong subject from a PKI service on the device.
Action	Make sure the certificate authority (CA) certificates match on both the Web server and the device.

Chapter 58

Syslog and Webtrends

The following messages pertain to configuring and enabling syslog and WebTrends facilities.

Critical (00020)

Message	⟨*string*⟩System memory is low (⟨*integer*⟩ allocated out of ⟨*integer*⟩) ⟨*integer*⟩ times in 1 minute
Meaning	The number of bytes allocated for system memory has surpassed the alarm threshold.
Action	If the memory alarm threshold was set too low, use the set alarm threshold memory command to increase the threshold. (The default is 95% of the total memory.) Check if a firewall attack is in progress. Seek ways to reduce traffic.

Critical (00030)

Message	⟨*string*⟩System CPU utilization is high (⟨*integer*⟩ > alarm threshold:⟨*integer*⟩) ⟨*integer*⟩ times in 1 minute
Meaning	CPU utilization has surpassed the alarm threshold.
Action	If the CPU alarm threshold was set too low, use the set alarm threshold cpu command to increase the threshold. Check if a firewall attack is in progress. Seek ways to reduce traffic.

Warning (00019)

Message	Syslog cannot connect to the TCP server ⟨*string*⟩; the connection is closed.
Meaning	The device cannot connect to the syslog server using the TCP transport protocol.
Action	Check the network connections.

Notification ()

Message	WebTrends host port number has been changed to ⟨*integer*⟩
Meaning	An admin has changed the IP address or domain name of the WebTrends host or the port number to which the device sends packets bound for the WebTrends host.
Action	No recommended action

Notification (00019)

Message	Attempt to enable WebTrends has failed because WebTrends settings have not yet been configured.
Meaning	An admin has attempted to enable the WebTrends facility before configuring the WebTrends settings. Consequently, the attempt has failed.
Action	Before attempting to enable WebTrends, configure the WebTrends settings.

Message	All syslog message levels have been cleared.
Meaning	An admin removed the severity levels for the messages sent to the syslog host(s).
Action	Select a severity level. If you do not specify a severity level, the device does not send any message to the syslog host.

Message	All syslog servers were removed.
Meaning	An admin removed all syslog servers.
Action	No recommended action

Message	CLI log file size has been set to ⟨*size*⟩ bytes by admin '⟨*admin_name*⟩'.
Meaning	An admin has changed the maximum CLI log file size.
Action	No recommended action

Message	CLI logging has been disabled by admin '⟨*admin_name*⟩'.
Meaning	An admin has disabled CLI logging.
Action	No recommended action

Message	Event logging for syslog server ⟨*string*⟩ has been disabled.
Meaning	An admin has either enabled or disabled the syslog facility.
Action	No recommended action

Message	Event logging for syslog server ⟨*string*⟩ has been enabled.
Meaning	An admin has either enabled or disabled the syslog facility.
Action	No recommended action

Message	IDP logging for syslog server ⟨*string*⟩ has been disabled.
Meaning	An admin has either enabled or disabled IDP logging via syslog.
Action	No recommended action

Message	IDP logging for syslog server ⟨*string*⟩ has been enabled.
Meaning	An admin has either enabled or disabled IDP logging via syslog.
Action	No recommended action

Message	⟨*string*⟩ VPN management tunnel has been enabled.
Meaning	A VPN tunnel for administrative traffic has been configured.
Action	No recommended action

Message	Socket cannot be assigned for syslog.
Meaning	The device cannot allocate an IP socket for the syslog facility.
Action	To free up a socket, close other management facilities that use sockets as connection tools, such as Telnet or the Web, and which are not currently in use.

Message	Socket cannot be assigned for WebTrends
Meaning	The device cannot allocate an IP socket for the WebTrends facility.
Action	To free up a socket, close some other facilities, such as Telnet, which are not currently in use.

Message	Syslog facility for ⟨*string*⟩ has been changed to ⟨*string*⟩
Meaning	An admin has changed the name of the syslog facility or security facility for the messages sent to the syslog host.
Action	No recommended action

Message	Syslog has been disabled.
Meaning	An admin has either enabled or disabled the syslog facility or traffic logging via syslog.
Action	No recommended action

Message	Syslog has been enabled.
Meaning	An admin has either enabled or disabled the syslog facility or traffic logging via syslog.
Action	No recommended action

Message	Syslog security facility for ⟨*string*⟩ has been changed to ⟨*string*⟩
Meaning	An admin has changed the name of the syslog facility or security facility for the messages sent to the syslog host.
Action	No recommended action

Message	Syslog server ⟨*string*⟩ host port number has been changed to ⟨*integer*⟩
Meaning	An admin has changed the port number to which the device sends packets bound for the syslog host.
Action	No recommended action

Message	Syslog server ⟨*string*⟩ hostname has been changed to ⟨*string*⟩
Meaning	An admin has changed the name of the syslog host.
Action	No recommended action

Message	Syslog server ⟨*string*⟩ was added.
Meaning	An admin has either added or removed the specified syslog server.
Action	No recommended action

Message	Syslog server ⟨*string*⟩ was removed.
Meaning	An admin has either added or removed the specified syslog server.
Action	No recommended action

Message	Syslog source interface has been changed to ⟨*string*⟩
Meaning	An admin modified the specified source interface.
Action	No recommended action

Message	Syslog source interface was removed.
Meaning	An admin removed the source interface.
Action	No recommended action

Message	Syslog VPN encryption has been disabled.
Meaning	An admin has either enabled or disabled VPN encryption of all syslog messages sent from the device to the syslog host.
Action	No recommended action

Message	Syslog VPN encryption has been enabled.
Meaning	An admin has either enabled or disabled VPN encryption of all syslog messages sent from the device to the syslog host.
Action	No recommended action

Message	Traffic logging for syslog server ⟨*string*⟩ has been disabled.
Meaning	An admin has either enabled or disabled traffic logging via syslog.
Action	No recommended action

Message	Traffic logging for syslog server ⟨*string*⟩ has been enabled.
Meaning	An admin has either enabled or disabled traffic logging via syslog.
Action	No recommended action

Message	Transport protocol for syslog server ⟨*string*⟩ was changed to ⟨*string*⟩
Meaning	An admin changed the transport protocol for syslog messages to either UDP or TCP
Action	No recommended action

Message	WebTrends has been disabled
Meaning	An admin has either enabled or disabled the WebTrends facility.
Action	No recommended action

Message	WebTrends has been enabled
Meaning	An admin has either enabled or disabled the WebTrends facility.
Action	No recommended action

Message	WebTrends host domain name has been changed to ⟨*string*⟩
Meaning	An admin has changed the IP address or domain name of the WebTrends host or the port number to which the device sends packets bound for the WebTrends host.
Action	No recommended action

Message	WebTrends VPN encryption has been disabled
Meaning	An admin has either enabled or disabled VPN encryption of all WebTrends messages sent from the device to the WebTrends host.
Action	No recommended action

Message	WebTrends VPN encryption has been enabled
Meaning	An admin has either enabled or disabled VPN encryption of all WebTrends messages sent from the device to the WebTrends host.
Action	No recommended action

Notification (00019:)

Message	CLI logging has been enabled by admin '⟨*admin_name*⟩'.
Meaning	An admin has enabled CLI logging.
Action	No recommended action

Notification (00022)

Message	⟨*string*⟩ VPN management tunnel has been disabled.
Meaning	A VPN tunnel for administrative traffic has been disabled.
Action	No recommended action

Notification (00767)

Message	Alarm log was reviewed ⟨*string*⟩.
Meaning	The entries in the specified log have been viewed.
Action	No recommended action

Message	All logged events or alarms were cleared ⟨*string*⟩
Meaning	All entries from the event or alarm log were deleted.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	All self logs were cleared ⟨*string*⟩
Meaning	All entries from the specified log were deleted.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	All traffic logs were cleared ⟨*string*⟩
Meaning	All entries from the specified log were deleted.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Asset-recovery log was reviewed ⟨*string*⟩.
Meaning	The entries in the specified log have been viewed.
Action	No recommended action

Message	Event log was reviewed ⟨*string*⟩.
Meaning	The entries in the specified log have been viewed.
Action	No recommended action

Message	Log setting was modified to disable ⟨*string*⟩ level ⟨*string*⟩
Meaning	Logging of messages has either been enabled or disabled at the specified severity level: emergency, alert, critical, error, warning, notification, information, or debugging.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Log setting was modified to enable ⟨*string*⟩ level ⟨*string*⟩
Meaning	Logging of messages has either been enabled or disabled at the specified severity level: emergency, alert, critical, error, warning, notification, information, or debugging.
Action	Confirm that the action was appropriate, and performed by an authorized admin.

Message	Self log was reviewed ⟨*string*⟩.
Meaning	The entries in the specified log have been viewed.
Action	No recommended action

Message	System log was reviewed ⟨*string*⟩.
Meaning	The entries in the specified log have been viewed.
Action	No recommended action

Message	Traffic log was reviewed ⟨*string*⟩.
Meaning	The entries in the specified log have been viewed.
Action	No recommended action

Information (00767)

Message	Log buffer was full and remaining messages were sent to external destination. ⟨*integer*⟩ packets were dropped.
Meaning	When the log buffer in the security device reached its capacity, the device sent all log entries to an external host for storage. During the transmission process, the security device stopped receiving traffic and "as reported on some security devices" dropped the specified number of packets. Note: After the device transmits all log entries, it resumes receiving and processing traffic.
Action	No recommended action

Chapter 59

System Authentication

The following messages relate to system authentication.

Notification (00105)

Message	[1X] 802.1X session run out of memory.
Meaning	Sessions have exceeded 255 and no more sessions can be allocated.
Action	Use the get dot1x session CLI command to view how many sessions are currently configured. Configure more than 255 clients on device if necessary.

Message	[1X] 802.1X interface ⟨*interface*⟩ link status changed to down.
Meaning	The 802.1x interface is not connected.
Action	Use the get interface, interface, CLI command to check connection status. Use the set interface, interface, phy link CLI command to reestablish connectivity.

Message	[1X] 802.1X interface ⟨*interface*⟩ link status changed to up.
Meaning	The 802.1x interface is connected.
Action	No recommended action.

Notification (00614)

Message	[1X] host ⟨*host_mac*⟩ started authentication on interface ⟨*interface*⟩ with 802.1X session id ⟨*id*⟩.
Meaning	802.1X authentication has started.
Action	No recommended action.

Message	[1X] host ⟨*host_mac*⟩ failed authentication on interface ⟨*interface*⟩ with 802.1X session id ⟨*id*⟩.
Meaning	802.1X authentication failed.
Action	Confirm that all auth parameters are correct.

Message	[1X] host ⟨*host_mac*⟩ logged off interface ⟨*interface*⟩ with 802.1X session id ⟨*id*⟩.
Meaning	The client has logged off from authentication.
Action	No recommended action.

Message	[1X] host ⟨*host_mac*⟩ passed authentication on interface ⟨*interface*⟩ with 802.1X session id ⟨*id*⟩.
Meaning	802.1X authentication has completed.
Action	No recommended action.

Message	[1X] host ⟨*host_mac*⟩ started re-authentication on interface ⟨*interface*⟩ with 802.1X session id ⟨*id*⟩.
Meaning	802.1X authentication has restarted.
Action	No recommended action.

Chapter 60
Traffic Shaping

The following messages relate to the configuration of traffic shaping. Traffic shaping is the allocation of the appropriate amount of network bandwidth to every user and application on an interface.

Notification (00002)

Message	Traffic shaping clearing DSCP selector is turned ⟨*mode*⟩.
Meaning	An admin has enabled or disabled DiffServ Codepoint Marking. Differentiated Services (DiffServ) is a system for tagging (or "marking") traffic at a position within a hierarchy of priority. You can map the eight NetScreen priority levels to the DiffServ system. By default, the highest priority (priority 0) in the NetScreen system maps to the first three bits (0111) in the DiffServ field (see RFC 2474), or the IP precedence field in the ToS byte (see RFC 1349), in the IP packet header. The lowest priority (priority 7) in the NetScreen system maps to (0000) in the ToS DiffServ system.
Action	No recommended action

Message	Traffic shaping is turned ⟨*mode*⟩.
Meaning	An admin enabled or disabled traffic shaping. Traffic shaping is the allocation of the appropriate amount of network bandwidth to every user and application on an interface. The appropriate amount of bandwidth is defined as cost-effective carrying capacity at a guaranteed Quality of Service (QoS). You can use a security device to shape traffic by creating policies and by applying appropriate rate controls to each class of traffic going through the security device.
Action	No recommended action

Chapter 61

User

The following messages pertain to events that affect user settings and status.

Notification (00014)

Message	The user group ⟨*user_group_name*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	The named user group was added, deleted, or modified by the specified admin. The user group event was logged.
Action	No recommended action.

Message	The user ⟨*user_name*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	The named user was either enabled or disabled in the internal database by the specified admin. The user event was logged.
Action	No recommended action.

Chapter 62
Virtual Router

The following sections provide descriptions of and recommended actions for ScreenOS messages displayed for events related to virtual routers, including Virtual Router Redundancy Protocol (VRRP) and Next Hop Routing Protocol (NHRP).

Critical (00082)

Message	VRRP group ⟨*integer*⟩ on interface ⟨*string*⟩ gives up mastership.
Meaning	The specified VRRP group is no longer the master group.
Action	No recommended action.

Message	VRRP group ⟨*integer*⟩ on interface ⟨*string*⟩ is now the master.
Meaning	The specified VRRP group is now the master group.
Action	No recommended action.

Critical (00230)

Message	NHRP : VR(⟨*NHRP-vr*⟩) Drop pending registration-request to NHS ⟨*NHS-ip*⟩: outgoing ifp(⟨*outgoing-ifp*⟩) NHRP disabled.
Meaning	An NHRP Registration Request has failed because NHRP is not enabled on the outgoing tunnel.
Action	Enable NHRP on the outgoing tunnel.

Message	NHRP : VR(⟨*NHRP-vr*⟩) Drop purge-reply from ⟨*src-ip*⟩: failed to match NHRP entry from client information element ⟨*cie-nc-prot*⟩/⟨*prot-address*⟩ - > ⟨*NMBA-address*⟩.
Meaning	An NHRP Registration Request message has been sent to the Hub.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) Drop resolution-ack from ⟨*src-ip*⟩: failed to find NHRP entry inclient information exchange ⟨*cie-nc-prot*⟩/⟨*prot-address*⟩ - > ⟨*NMBA-address*⟩.
Meaning	The hub has received a Resolution Set acknowledgment from a spoke but there is not a valid NRHP entry on the hub for the spoke.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) drop ⟨*NHRP-[mesg|error]-type*⟩ who has ⟨*address*⟩ : fail make fix/mandatory hdr.
Meaning	An NHRP Registration Request or Resolution Set message has failed or been dropped because of a failure in mandatory header creation.
Action	Verify NHRP configuration.

Notification (00049)

Message	A ⟨*optional_sharable*⟩ virtual router using name ⟨*vrouter_name*⟩ and id ⟨*vrouter_id*⟩ has been created
Meaning	An admin created the identified virtual on the routing domain on the security device.
Action	No recommended action

Message	A virtual router with name ⟨*vrouter_name*⟩ and ID ⟨*vrouter_id*⟩ has been removed
Meaning	An admin removed the specified virtual router.
Action	No recommended action

Message	Fast route lookup was disabled in virtual router ⟨*vrouter_name*⟩
Meaning	A network administrator set SNMP traps for the dynamic routing MIBs to be private or public. This option is available only for the default root-level virtual router.
Action	No recommended action

Message	Fast route lookup was enabled in virtual router ⟨*vrouter_name*⟩
Meaning	A network administrator set SNMP traps for the dynamic routing MIBs to be private or public. This option is available only for the default root-level virtual router.
Action	No recommended action

Message	Route-lookup preference changed to ⟨*route_lookup_method_name*⟩(⟨*preference_value*⟩) = > ⟨*route_lookup_method_name*⟩(⟨*preference_value*⟩) = > ⟨*route_lookup_method_name*⟩(⟨*preference_value*⟩) in virtual router (⟨*vrouter_name*⟩).
Meaning	An administrator changed the route-lookup method and preference values.
Action	No recommended action

Message	Routes defined on inactive interfaces will be exported into other virtual routers, protocols in virtual router (⟨*vrouter_name*⟩)
Meaning	Routes on inactive interfaces can be advertised to other routers. This feature has either been enabled or disabled.
Action	No recommended action

Message	Routes defined on inactive interfaces will not be exported into other vrouters, protocols in vrouter (⟨*vrouter_name*⟩)
Meaning	Routes on inactive interfaces can be advertised to other routers. This feature has either been enabled or disabled.
Action	No recommended action

Message	SIBR routing disabled in virtual router ⟨*vrouter_name*⟩
Meaning	SIBR allows routing based on source interface. An administrator { enabled | disabled } the SIBR routing feature.
Action	No recommended action

Message	SIBR routing enabled in virtual router ⟨*vrouter_name*⟩
Meaning	SIBR allows routing based on source interface. An administrator { enabled | disabled } the SIBR routing feature.
Action	No recommended action

Message	SNMP trap made private in virtual router ⟨*vrouter_name*⟩
Meaning	A network administrator set SNMP traps for the dynamic routing MIBs to be private. This option is available only for the default root-level virtual router.
Action	No recommended action

Message	SNMP trap made public in vrouter (⟨*vrouter_name*⟩)
Meaning	A network administrator set SNMP traps for the dynamic routing MIBs to be public. This option is available only for the default root-level virtual router.
Action	No recommended action

Message	Source-based routing disabled in vrouter (⟨*vrouter_name*⟩)
Meaning	An admin has disabled source-based routing in the specified virtual router. Source-based routing is the process of a virtual router using a source address to determine how to send a packet rather than a destination address.
Action	No recommended action.

Message	Source-based routing enabled in virtual router ⟨*vrouter_name*⟩
Meaning	An admin has enabled source-based routing in the specified virtual router. Source-based routing is the process of a virtual router using a source address to determine how to send a packet rather than a destination address.
Action	No recommended action.

Message	Subnetwork conflict checking for interfaces in virtual router (⟨*vrouter_name*⟩) has been enabled.
Meaning	The subnetwork conflict checking feature allows interfaces in the virtual router to have overlapping subnetwork addresses. This message indicates this feature was enabled.
Action	No recommended action.

Message	The auto-route-export feature in virtual router ⟨*vrouter_name*⟩ has been disabled.
Meaning	An admin has either enabled or disabled auto-exporting for the current virtual router. Auto-exporting is the process of automatically exporting routes defined on routable interfaces from system-created virtual routers like the trust-vr and vsys virtual routers.
Action	No recommended action

Message	The auto-route-export feature in virtual router ⟨*vrouter_name*⟩ has been enabled
Meaning	An admin has either enabled or disabled auto-exporting for the current virtual router. Auto-exporting is the process of automatically exporting routes defined on routable interfaces from system-created virtual routers like the trust-vr and vsys virtual routers.
Action	No recommended action

Message	The maximum number of routes that can be created in virtual router ⟨*vrouter_name*⟩ is ⟨*max_routes*⟩
Meaning	An admin has set the maximum number of routes that can be set for the current virtual router. Once the number of routes in the route table equals this maximum number, the router cannot learn any new routes.
Action	No recommended action

Message	The maximum routes limit in virtual router ⟨*vrouter_name*⟩ has been removed.
Meaning	An admin has unset the maximum number of routes that can be set for the current virtual router, returning it to the default value. Once the number of routes in the route table equals this maximum number, the router cannot learn any new routes.
Action	No recommended action

Message	The router-id of virtual router ⟨*vrouter_name*⟩ used by OSPF, BGP routing instances id has been uninitialized.
Meaning	An admin uninitialized the router ID. The router ID is a value that identifies the router as a distinct entity on the network.
Action	No recommended action

Message	The router-id that can be used by OSPF, BGP routing instances in virtual router ⟨*vrouter_name*⟩ has been set to ⟨*vrouter_id*⟩
Meaning	An admin set the router ID for the specified virtual router.
Action	No recommended action

Message	The routing preference for protocol ⟨*protocol_name*⟩ in virtual router ⟨*vrouter_name*⟩ has been reset.
Meaning	The local preference parameter specifies the desirability of a path to an autonomous system. The lower the value, the more desirable the path. An admin has unset a previously set local preference value for the specified virtual routing instance, returning the value to its default setting.
Action	No recommended action

Message	The routing preference for protocol ⟨*protocol_name*⟩ in virtual router ⟨*vrouter_name*⟩ has been set to ⟨*preference_value*⟩
Meaning	An admin has set a local preference parameter for the specified protocol for the virtual router. The local preference parameter specifies the desirability of a path. The lower the value, the more desirable the path.
Action	No recommended action

Message	The subnetwork conflict checking feature for interfaces in virtual router ⟨*vrouter_name*⟩ was removed.
Meaning	The subnetwork conflict checking feature allows interfaces in the virtual router to have overlapping subnetwork addresses. This message indicates this feature was disabled.
Action	No recommended action.

Message	The system default-route in virtual router (⟨*vrouter_name*⟩) has been removed.
Meaning	An admin has deleted the default route in the specified virtual router.
Action	No recommended action

Message	The system default-route through virtual router ⟨*vrouter_name*⟩ has been added in virtual router ⟨*next_hop_vrouter_name*⟩
Meaning	The default route used in a specified virtual router has been added to another specified virtual router. This route can be used by another virtual routing instance.
Action	No recommended action

Message	The virtual router ⟨*vrouter_name*⟩ has been made default virtual router for virtual system (⟨*vsys_name*⟩)
Meaning	An administrator has bound the specified virtual routing instance to the specified Vsys and configured it to be the default virtual router on the Vsys.
Action	No recommended action

Message	The virtual router ⟨*vrouter_name*⟩ has been made sharable
Meaning	An admin designated the current virtual router sharable to other virtual systems. Only sharable virtual systems are visible to other vsys's.
Action	No recommended action

Message	The virtual router ⟨*vrouter_name*⟩ has been made unsharable.
Meaning	An admin designated the current virtual router sharable to other virtual systems. Only sharable virtual systems are visible to other vsys's.
Action	No recommended action

Notification (00061)

Message	Configuration of VRRP on interface ⟨*string*⟩ is removed.
Meaning	VRRP configuration on the specified interface has been removed.
Action	No recommended action.

Message	VRRP group ⟨*integer*⟩ created on interface ⟨*string*⟩.
Meaning	A VRRP group has been created on the specified interface.
Action	No recommended action.

Message	VRRP group ⟨*integer*⟩ on interface ⟨*string*⟩ changed advertisement interval to ⟨*integer*⟩ seconds.
Meaning	The specified VRRP group has changed its advertisement interval.
Action	No recommended action.

Message	VRRP group ⟨*vsd_id*⟩ on interface ⟨*string*⟩ changed preempt hold on time to ⟨*integer*⟩ seconds.
Meaning	The specified VRRP group has changed its preempt hold time.
Action	No recommended action.

Message	VRRP group ⟨*integer*⟩ on interface ⟨*string*⟩ changed preempt to ⟨*string*⟩.
Meaning	The preemption for the specified VRRP group has changed.
Action	No recommended action.

Message	VRRP group ⟨*integer*⟩ on interface ⟨*string*⟩ changed priority to ⟨*integer*⟩.
Meaning	The priority level of the specified VRRP group has changed.
Action	No recommended action.

Message	VRRP group ⟨*integer*⟩ removed from interface ⟨*string*⟩.
Meaning	A VRRP group has been removed on the specified interface.
Action	No recommended action.

Message	VRRP on interface ⟨*string*⟩ is configured.
Meaning	VRRP on the specified interface has been configured.
Action	No recommended action.

Message	VRRP on interface ⟨*string*⟩ is disabled.
Meaning	VRRP on the specified interface has been disabled.
Action	No recommended action.

Message	VRRP on interface ⟨*string*⟩ is enabled.
Meaning	VRRP on the specified interface has been enabled.
Action	No recommended action.

Information (00622)

Message	NHRP : VR(⟨*NHRP-vr*⟩) Dynamic tunnel establishment between ⟨*spoke1*⟩ and ⟨*spoke2*⟩ for packets between ⟨*srcip*⟩ and ⟨*dstip*⟩, not initiated as both gateways are behind NAT.
Meaning	Both spokes involed in initating dynamic tunnels are in NAT mode.
Action	No recommended action.

Message	NHRP : NHRP instance in virtual router (⟨*NHRP-vr*⟩) is created.
Meaning	NHRP has been enabled on the virtual router.
Action	No recommended action.

Message	NHRP : NHRP instance in virtual router (⟨*NHRP-vr*⟩) is deleted.
Meaning	NHRP has been disabled on the virtual router.
Action	No recommended action.

Message	NHRP : recieved a valid ⟨*NHRP-mesg-type*⟩ from ⟨*NHC-ip-address*⟩ via ⟨*interface-name*⟩.
Meaning	An NHRP Registration Request message containing virtual router information has been received.
Action	No recommended action.

Message	NHRP : sending a valid ⟨*NHRP-mesg-type*⟩ to ⟨*NHC-ip-address*⟩ via ⟨*interface-name*⟩.
Meaning	A valid NHRP Registration Reply message has been sent to the spoke.
Action	No action recommended.

Message	NHRP : VR(⟨*NHRP-vr*⟩) construct ⟨*NHRP-mesg-type*⟩ to NHS ⟨*NHS-ip-address*⟩.
Meaning	An NHRP Registration Request message has been sent to the Hub.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) purge-reply ID(⟨*NHRP-mesg-id*⟩) from ⟨*src-ip*⟩.
Meaning	An NHRP Purge Request message has been acknowledged.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) resolution-ack ID(⟨*NHRP-mesg-id*⟩) from ⟨*src-ip*⟩.
Meaning	The hub recieved an NHRP Resolution Set acknowledgment from the initiating spoke.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) resolution-Query (⟨*NHRP-mesg-type*⟩) ID (⟨*NHRP-mesg-id*⟩) to NHS from ⟨*NHS-ip-address*⟩ via ⟨*interface-name*⟩.
Meaning	An attempt has been made to refresh the NHRP entry by sending out an NHRP Resolution Request message.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) resolution-reply ID(⟨*NHRP-mesg-id*⟩) from ⟨*src-ip*⟩, state: ⟨*NHRP-RSI-state*⟩.
Meaning	The NHRP Resolution set message status is in the initial state. The spokes have exchanged the profile information they each need to set up dynamic tunnels.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) resolution-reply ID(⟨*NHRP_mesg_id*⟩) from ⟨*src_ip*⟩, state: ⟨*NHRP-RSI-state*⟩.
Meaning	The NHRP Resolution Set message status is in the final state. The spokes have exchanged then profile information they each need to set up dynamic tunnels.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) Rx purge-request ID(⟨*NHRP-mesg-id*⟩) from ⟨*src-ip*⟩: ⟨*nhrp-cie-code-string*⟩ ; CIE ⟨*nhrp-prot-ip*⟩/⟨*nhrp-prot-mask*⟩- > ⟨*nhrp-nbma-ip*⟩.
Meaning	An NHRP Purge Request message has been received.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) Rx resolution-⟨*NHRP-reply-or-set-mesg*⟩ ID(⟨*NHRP-mesg-id*⟩) from ⟨*src-ip*⟩: ⟨*nhrp-cie-code-string*⟩ ; CIE ⟨*nhrp-prot-ip*⟩/⟨*nhrp-prot-mask*⟩- > ⟨*nhrp-nbma-ip*⟩; trigger ⟨*trigger-vpn*⟩.
Meaning	The spoke has recieved an NHRP Resolution Set message from the hub.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) Tx mesg : ⟨*NHRP-reply-mesg*⟩ ID(⟨*NHRP-mesg-id*⟩) to ⟨*dst-ip*⟩.
Meaning	The hub has acknowledged an NHRP Purge Request message.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) Tx res mesg : ⟨*NHRP-reply-mesg*⟩ ID(⟨*NHRP-mesg-id*⟩) to ⟨*dst-ip*⟩.
Meaning	The spoke has acknowledged to the hub that it recieved an NHRP Resolution Set message.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) validate registration-reply from ⟨*NHC-ip-address*⟩ via ⟨*interface-name*⟩
Meaning	A NHRP valid NHRP Registration Reply message from the hub has been received.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) add ne ⟨*NHRP-ne-address*⟩/⟨*NHRP-ne-mask*⟩ -> ⟨*NHRP-NBMA-address*⟩/⟨*NHRP-nexthop-address*⟩) ⟨*tunnel-interface-name*⟩ TTL(⟨*NHRP-ne-ttl*⟩) to FIB ⟨*NHRP-ne-in-fib*⟩.
Meaning	An NHRP dynamic routing entry has been added into the forwarding base.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) del ne ⟨*NHRP-ne-address*⟩/⟨*NHRP-ne-mask*⟩ -> ⟨*NHRP-NBMA-address*⟩/⟨*NHRP-nexthop-address*⟩) ⟨*tunnel-interface-name*⟩.
Meaning	An NHRP dynamic routing entry has been deleted from the forwarding base.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) construct ⟨*NHRP-mesg-type*⟩ ID(⟨*NHRP-mesg-id*⟩) this ⟨*NMBA-address*⟩ has ⟨*address*⟩/⟨*mask*⟩.
Meaning	The hub has triggered the Resolution Set message, first to the responding spoke, then to the initiating spoke.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) construct ⟨*NHRP-mesg-type*⟩ ID(⟨*NHRP-mesg-id*⟩) this ⟨*NMBA-address*⟩ no longer has ⟨*address*⟩/⟨*mask*⟩.
Meaning	A spoke has sent an NHRP Purge Request message to the hub to purge information about itself the hub has cached. The hub will attempt to update all other spokes to which it has sent resolution information about this spoke: hence this message also appears on the hub. Upon receiving this update message, each spoke will send a new Registration Request message to get the latest updates from the hub.
Action	No recommended action.

Message	NHRP : VR(⟨*NHRP-vr*⟩) construct ⟨*NHRP-mesg-type*⟩ to ⟨*NMBA-address*⟩ over ⟨*interface-name*⟩ with ID(⟨*NHRP-mesg-id*⟩).
Meaning	An NHRP Purge Request message with multiple NHRP cache entries has been sent.
Action	No recommended action.

Chapter 63

VPNs

The following messages relate to IPSec virtual private network (VPN) tunnels and VPN-related technologies.

Critical (00040)

Message	VPN '⟨*vpn_name*⟩' ⟨*user_id*⟩from ⟨*spacer*⟩ is up.
Meaning	10.100.37.180The status of the specified VPN tunnel has changed from down to up.
Action	No recommended action

Critical (00041)

Message	VPN '⟨*vpn_name*⟩' ⟨*user_id*⟩from ⟨*spacer*⟩ is down.
Meaning	The status of the specified VPN tunnel has changed from up to down.
Action	No recommended action

Critical (00112)

Message	VPN TUNNEL LIMIT (⟨*max_vpn_num*⟩) REACHED. No more VPN tunnels can be created.
Meaning	The total number of VPN Tunnels reached the soft limit imposed by licensing restrictions. Creation of any new tunnels (either statically using configuration or dynamically by means of dialup-clients or AC-VPNs) is not possible.
Action	Either upgrade your licensing keys, or use the unset or clear commands to clean up the unused VPN tunnels.

Notification (00017)

Message	IPSec NAT-T for VPN ⟨*vpn_name*⟩ has been disabled.
Meaning	An admin has either enabled or disabled the NAT traversal (NAT-T) option for the specified VPN. NAT traversal adds an extra layer of encapsulation, encapsulating the original IPSec packet (using ESP or AH protocols) within a UDP packet. Most NAT servers cannot recognize the ESP or AH protocols and drop IPSec packets. When the NAT-T option is enabled, the sender encapsulates the ESP or AH packet within a UDP packet. The NAT server recognizes the UDP protocol and sends it on. The recipient then strips off the UDP packet and processes the inner ESP or AH packet accordingly.
Action	No recommended action

Message	IPSec NAT-T for VPN ⟨*vpn_name*⟩ has been enabled.
Meaning	An admin has either enabled or disabled the NAT traversal (NAT-T) option for the specified VPN. NAT traversal adds an extra layer of encapsulation, encapsulating the original IPSec packet (using ESP or AH protocols) within a UDP packet. Most NAT servers cannot recognize the ESP or AH protocols and drop IPSec packets. When the NAT-T option is enabled, the sender encapsulates the ESP or AH packet within a UDP packet. The NAT server recognizes the UDP protocol and sends it on. The recipient then strips off the UDP packet and processes the inner ESP or AH packet accordingly.
Action	No recommended action

Message	The DF-BIT for VPN ⟨*vpn_name*⟩ has been set to ⟨*action*⟩.
Meaning	For the specified VPN tunnel, an admin has cleared or set the Don't Fragment BIT in the outside header of an encapsulated packet, or copied the DF-BIT setting from the inside header to the outside header.
Action	No recommended action

Message	VPN monitoring for VPN ⟨*vpn_name*⟩ has been disabled.
Meaning	An admin has disabled the VPN monitoring option for the specified VPN tunnel.
Action	No recommended action

Message	VPN monitoring for VPN ⟨*vpn_name*⟩ has been enabled (src int ⟨*src_interface*⟩, dst IP ⟨*dest_ip*⟩, rekeying ⟨*rekeying_or_not*⟩, scalability optimization ⟨*optimized_or_not*⟩).
Meaning	An admin has enabled the VPN monitoring option for the specified VPN tunnel between the specified source interface and destination IP address. The admin has also enabled or disabled the IKE rekey option and scalability optimization. VPN monitoring sends ICMP echo requests through a VPN tunnel to check if the tunnel is up or down. If the state changes from up to down and the IKE rekey option is enabled, the security device attempts IKE Phase 2 negotiations (and possibly Phase 1 negotiations-if the Phase 1 lifetime has timed out). When scalability optimization is enabled, the security device reduces VPN traffic by suppressing the transmission of ICMP echo requests when the tunnel is active with other types of traffic.
Action	No recommended action

Message	VPN monitoring interval has been set to ⟨*vpnmon_interval*⟩ seconds.
Meaning	An admin has changed the VPN monitoring frequency to the specified number of seconds. The VPN monitoring feature sends an ICMP echo request (PING) through a VPN tunnel from end to end at the specified frequency to check if the tunnel is up or down.
Action	No recommended action

Message	VPN monitoring interval has been unset.
Meaning	An admin has returned the VPN monitoring frequency to its default setting. The VPN monitoring feature sends an ICMP echo request (PING) through a VPN tunnel from end to end to check if the tunnel is up or down. The default setting is one PING per minute.
Action	No recommended action

Message	VPN monitoring threshold has been set to ⟨*vpnmon_threshold*⟩.
Meaning	An admin has changed the VPN monitoring threshold to the specified number of packets. The VPN monitoring feature sends an ICMP echo request (PING) through a VPN tunnel from end to end at the specified frequency to check if the tunnel is up or down. The threshold value indicates the number of these requests that can be sent before determining if the tunnel is up or down.
Action	No recommended action

Message	VPN monitoring threshold has been unset.
Meaning	An admin has returned the VPN monitor threshold to its default setting.
Action	No recommended action

Message	VPN ⟨*vpn_name*⟩ with gateway ⟨*gateway_ip*⟩ and SPI ⟨*local_spi*⟩/⟨*remote_spi*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin has added or deleted the specified VPN, or modified at least one of its attributes.
Action	No recommended action

Message	VPN ⟨*vpn_name*⟩ with gateway ⟨*gateway_name*⟩ and P2 proposal ⟨*p2_proposal*⟩ ⟨*action*⟩ ⟨*by_whom*⟩.
Meaning	An admin has added or deleted the specified VPN, or modified at least one of its attributes.
Action	No recommended action

Message	VPN tunnel limit (⟨*max_vpn_num*⟩) reached. No more VPN tunnels can be created.
Meaning	The total number of VPN Tunnels reached the soft limit imposed by licensing restrictions. Creation of any new tunnels (either statically using configuration or dynamically by means of dialup-clients or AC-VPNs) is not possible.
Action	Either upgrade your licensing keys, or use the unset or clear commands to clean up the unused VPN tunnels.

Message	VPN ⟨*vpn_name*⟩ has been bound to tunnel interface ⟨*tunnel_if_name*⟩.
Meaning	An admin has bound the specified VPN tunnel to either an interface, a tunnel zone, or a security zone.
Action	No recommended action

Message	VPN ⟨*vpn_name*⟩ has been bound to tunnel zone ⟨*tunnel_zone_name*⟩.
Meaning	An admin has bound the specified VPN tunnel to either an interface, a tunnel zone, or a security zone.
Action	No recommended action

Message	VPN ⟨*vpn_name*⟩ has been unbound from tunnel zone ⟨*tunnel_zone_name*⟩.
Meaning	An admin unbound the specified VPN tunnel from the specified tunnel zone.
Action	No recommended action

Information (00536)

Message	FIPS error: AES encryption using key sizes greater than 128 may not be configured via SSH.
Meaning	When the security device was in FIPS mode, an admin logged in via an SSH connection and attempted to define a Manual Key VPN tunnel using AES encryption. However, FIPS does not allow an admin using an SSH connection, which does not support AES encryption, to configure a VPN tunnel with a more secure encryption algorithm such as AES.
Action	Configure the VPN tunnel with 3-DES or DES encryption.

Message	IKE < ⟨*gateway_ip*⟩ > : IP address of local interface has been changed from 0.0.0.0 to ⟨*new_local_ip*⟩.
Meaning	An admin has changed the IP address that the local device can use for VPN termination from 0.0.0.0 to the specified IP address.
Action	No recommended action

Message	IKE < ⟨*gateway_ip*⟩ > : IP address of local interface has been changed to 0.0.0.0, and VPNs cannot terminate at it.
Meaning	An admin has changed the IP address used for VPN termination on the local device to 0.0.0.0. Consequently, no VPN traffic can reach or leave the device. If the device is in NAT or Route mode, the admin has changed the IP address of the untrusted interface to 0.0.0.0/0. If the device is in Transparent mode, the admin has changed the system IP address to 0.0.0.0.
Action	If you made the change by mistake, return the changed address to its previous setting. If you made the change intentionally (for example, you changed the operational mode from NAT or Route mode to Transparent mode) and you want to maintain VPN activity with existing peers, set a valid IP address and notify all remote gateway admins of the address change so they can reconfigure their VPN configurations.

Message	IKE < ⟨*gateway_ip*⟩ > : Policy ID ⟨*integer*⟩ failed over from SA ⟨*integer*⟩ to SA ⟨*integer*⟩.
Meaning	The monitoring device in a redundant VPN group failed over VPN traffic from the tunnel with the security association (SA) < id_num1 > to the tunnel with the SA < id_num2 > . The IP address belongs to the targeted remote gateway to which the VPN traffic has been redirected. The policy ID number belongs to the policy that references this particular redundant VPN group.
Action	No recommended action

Message	IKE < ⟨*gateway_ip*⟩ > : VPN ID number cannot be assigned.
Meaning	During VPN tunnel configuration, security device was unable to assign the VPN tunnel an ID number, possibly because the maximum number of tunnels had been reached. Consequently, the configuration of the VPN tunnel was unsuccessful.
Action	Check if the number of the defined VPN tunnels has reached the maximum limit.

Message	Phase 2 SA for tunnel ID ⟨*sa_tunnel_id*⟩ has been idle too long. Deactivated P2 SA and sent a Delete msg to peer.
Meaning	Because the specified Phase 2 security association (SA) has been idle for too long, the security device deactivated the SA and sent a "delete" message to its peer.
Action	No recommended action

Message	VPN monitoring for VPN ⟨*vpn_name*⟩ has deactivated the SA with ID 0x⟨*sa_tunnel_id*⟩x.
Meaning	The security device determined that the VPN monitoring status for the specified VPN tunnel changed from up to down. Consequently, the security device deactivated the specified Phase 2 security association (SA).
Action	No recommended action

Chapter 64
Vsys

The following sections provide descriptions of and recommended action for ScreenOS messages displayed for events relating to virtual systems.

Alert (00046)

Message	An administrator disables SIP ALG.
Meaning	A network administrator disabled the SIP ALG.
Action	No recommended action

Notification (00032)

Message	ID for vsys ⟨*vsys_name*⟩ has been changed from ⟨*old_id*⟩ to ⟨*new_id*⟩ ⟨*config_changer*⟩.
Meaning	A root level administrator changed the name of the specified vsys.
Action	No recommended action

Message	NSRP VSD group ID for vsys ⟨*vsys_name*⟩ has been changed from ⟨*old_id*⟩ to ⟨*new_id*⟩ ⟨*config_changer*⟩.
Meaning	A root level administrator changed the NSRP Virtual Security Device group ID of the specified vsys.
Action	No recommended action.

Message	Vsys ⟨*old_vsys_name*⟩ has been changed to ⟨*new_vsys_name*⟩ ⟨*config_changer*⟩.
Meaning	A root level administrator changed the ID of the specified vsys.
Action	No recommended action

Message	Vsys ⟨*vsys_name*⟩ has been removed ⟨*config_changer*⟩
Meaning	A root level administrator created the specified virtual system (vsys).
Action	No recommended action

Message	Vsys ⟨*vsys_name*⟩ profile has been changed from ⟨*old_vsys_profile_name*⟩ to ⟨*new_vsys_profile_name*⟩.
Meaning	The vsys profile name has been changed to a new name.
Action	No recommended action

Message	Vsys ⟨*vsys_name*⟩ with profile ⟨*vsys_profile_name*⟩ has been created ⟨*config_changer*⟩.
Meaning	A root level administrator created the specified virtual system (vsys).
Action	No recommended action

Message	Vsys profile ⟨*vsys_profile_name*⟩ created with default vsys limits.
Meaning	A vsys profile with default limits has been created.
Action	No recommended action

Message	Vsys profile ⟨*vsys_profile_name*⟩ deleted.
Meaning	A vsys profile has been deleted.
Action	No recommended action

Message	Vsys profile ⟨*vsys_profile_name*⟩ limit ⟨*vsys_profile_limit_name*⟩ has been set to ⟨*vsys_profile_limit_max*⟩ ⟨*vsys_profile_limit_max_value*⟩ ⟨*vsys_profile_limit_reserved*⟩ ⟨*vsys_profile_limit_reserved_value*⟩.
Meaning	The limits (reserved and max) have been changed for a vsys profile.
Action	No recommended action

Notification (00043)

Message	IP classification for not classified traffic has been changed to ⟨*policy_name*⟩.
Meaning	An admin changed the IP classification policy for unclassified traffic.
Action	No recommended action

Message	IP classification has been ⟨*state_enabled_disabled*⟩ on zone ⟨*zone_name*⟩.
Meaning	Virtual system IP classification is now enabled or disabled. Such classification associates IP addresses with particular virtual systems, as opposed to VLAN tagging.
Action	No recommended action

Message	IP classification mode has been changed to ⟨*mode_name*⟩.
Meaning	An admin changed the IP classification mode.
Action	No recommended action

Message	IP classification object ⟨*string_subnet_or_range*⟩ has been added on zone ⟨*zone_name*⟩.
Meaning	An admin added or deleted an IP address and subnet mask, or an address range, on the designated zone.
Action	No recommended action

Message	IP classification object ⟨*string_subnet_or_range*⟩ has been deleted on zone ⟨*zone_name*⟩.
Meaning	An admin added or deleted an IP address and subnet mask, or an address range, on the designated zone.
Action	No recommended action

Notification (00046)

Message	An administrator enables SIP ALG.
Meaning	A network administrator enabled the SIP ALG
Action	No recommended action

Message	An administrator set the media inactivity time-out value to its default value of ⟨*timeout*⟩ seconds.
Meaning	A network administrator has set the media inactivity timeout value to its default value. The media inactivity timeout parameter indicates the maximum length of time a call can remain active without any SIP signaling traffic.
Action	No recommended action

Message	An administrator set the SIP invite time-out value to its default value of ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP INVITE request, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, the device removes the call. This message indicates a network administrator set the SIP INVITE request timeout value to its default value.
Action	No recommended action

Message	An administrator set the SIP invite time-out value to ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP INVITE request, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, then the device removes the call. This message indicates a network administrator modified the SIP INVITE default timeout value.
Action	No recommended action

Message	An administrator set the SIP media inactivity time-out value to ⟨*timeout*⟩ seconds.
Meaning	A network administrator has modified the media inactivity timeout value. The media inactivity timeout parameter indicates the maximum length of time a call can remain active without any SIP signaling traffic.
Action	No recommended action

Message	An administrator set the SIP ringing time-out value to its default value of ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP Ringing response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, the device removes the call. This message indicates a network administrator set the SIP Ringing response timeout value to its default value.
Action	No recommended action

Message	An administrator set the SIP ringing time-out value to ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP Ringing response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, then the device removes the call. This message indicates a network administrator modified the SIP Ringing timeout value.
Action	No recommended action

Message	An administrator set the SIP signaling inactivity time-out value to its default value of ⟨*timeout*⟩ seconds.
Meaning	A network administrator set the SIP signaling inactivity timeout value to its default value. If no signaling occurs for the call within the amount of time specified by the signaling inactivity timeout value, then the device removes the call.
Action	No recommended action

Message	An administrator set the SIP signaling inactivity time-out value to ⟨*timeout*⟩ seconds.
Meaning	A network administrator modified the SIP signaling inactivity value. If no signaling occurs for the call within the amount of time specified by the signaling inactivity timeout value, then the device removes the call.
Action	No recommended action

Message	An administrator set the SIP trying time-out value to its default value of ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP Trying response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, the device removes the call. This message indicates a network administrator set the SIP Trying response timeout value to its default value.
Action	No recommended action

Message	An administrator set the SIP trying time-out value to ⟨*timeout*⟩ seconds.
Meaning	When the device receives a SIP Trying response, it sets a timeout value for activity on the call. If the call has no activity within the amount of time specified by the timeout, then the device removes the call. This message indicates a network administrator modified the SIP Trying timeout value.
Action	No recommended action

Notification (00515)

Message	Vsys admin user ⟨*vsys_user_name*⟩ logged on via Telnet from remote IP address ⟨*remote_ip*⟩ using port ⟨*remote_port*⟩.
Meaning	The named vsys admin logged on to the specified vsys via Telnet from the specified IP address, using the specified port number.
Action	No recommended action

Message	Vsys admin user ⟨*vsys_user_name*⟩ logged on via the console.
Meaning	An admin logged on to the specified vsys through a console connection.
Action	No recommended action

Notification (00767)

Message	Cannot allocate SIP call because device is fielding too many calls.
Meaning	The device does not have enough resources to process the current call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Security devices do not support multicast IP addresses ⟨*ip_addr*⟩ in SIP ⟨*header_field* > ⟩.
Meaning	The security device received a SIP message in which the destination IP address is a multicast IP address, but Juniper Networks does not currently support multicast with SIP.
Action	No recommended action

Message	Security devices do not support multiple IP addresses ⟨*ip_addr*⟩ or ports ⟨*port* > ⟩ in SIP headers ⟨*header_field* > ⟩.
Meaning	Juniper Networks security devices do not support multiple IP addresses or ports in SIP headers.
Action	No recommended action

Message	SIP ALG is unregistered by RM.
Meaning	A non-specific internal error occurred in the SIP Application Layer Gateway.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SIP call information data is too long.
Meaning	The size of some of the SIP header fields exceeds the maximum size limit and the device might not be able to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SIP parser error ⟨*msg*⟩.
Meaning	The SIP Application Layer Gateway parser which processes SIP messages, encountered an unknown error.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	SIP structure is corrupted.
Meaning	A non-specific internal error occurred in the SIP Application Layer Gateway.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot allocate sufficient memory for the SIP ALG request.
Meaning	During the process of an incoming call, the device does not have enough memory to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot register the Network Address Translation vector for the SIP ALG request.
Meaning	The device cannot write the NAT vector being requested by the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	The device cannot register the SIP ALG request to RM.
Meaning	During the initialization of the SIP Application Layer Gateway (ALG) where resources are being allocated, the gateway module could not contact the Resource Manager.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Too many call segments for response.
Meaning	The device does not have enough resources to process the current call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Too many call segments.
Meaning	The device does not have enough resources to process the current call.
Action	No recommended action

Message	Transaction data is too long.
Meaning	The size of some of the SIP header fields exceeds the maximum size limit and the device might not be able to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	Transaction data too long for response.
Meaning	The size of some of the SIP header fields exceeds the maximum size limit and the device might not be able to process the call.
Action	Contact Juniper Networks technical support by visiting www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Chapter 65
Web Filtering

The following messages relate to events generated during configuration or execution of web filtering.

Alert (00014)

Message	Communication error with ⟨*url_server_vendor_name*⟩ server[⟨*url_server_ip_address*⟩]: SrvErr(⟨*url_server_error_code*⟩), SockErr(⟨*url_server_socket_error*⟩), Valid(⟨*url_server_sockets_valid*⟩), Connected(⟨*url_server_sockets_connected*⟩)
Meaning	An error occurred during communication with the Websense or SurfControl server.
Action	Check the documentation for the Websense or SurfControl server, and confirm that it is configured properly.

Error (00556)

Message	UF-MGR: Failed to abort a transaction. Reason: ⟨*string*⟩.
Meaning	The security device failed to abort a transaction due to the specified reason.
Action	Contact Juniper Networks technical support at www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	UF-MGR: Failed to disable cache.
Meaning	The security device failed to disable the web filtering cache.
Action	Contact Juniper Networks technical support at www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	UF-MGR: Failed to enable cache.
Meaning	The security device failed to enable the web filtering cache.
Action	Contact Juniper Networks technical support at www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	UF-MGR: Failed to process a request. Reason: ⟨*string*⟩.
Meaning	The security device failed to process a request to access a URL due to the specified reason.
Action	Contact Juniper Networks technical support at www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	UF-MGR: Internal error: ⟨*string*⟩.
Meaning	The security device failed to allocate the uf_record, which is a memory resource required to process URL filtering.
Action	Contact Juniper Networks technical support at www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Message	UF-MGR: Web filtering license is expired (expiration date: %t2; current date: %t2).
Meaning	Your Web filtering license is expired on the specified date. Integrated Web filtering requires a valid license.
Action	Obtain and install the Web filtering license key on your security device.

Warning (00556)

Message	UF-MGR: URL FILTER ERR: ⟨*IP address*⟩(⟨*integer*⟩)->⟨*IP address*⟩(⟨*integer*⟩), host:⟨*string*⟩ page:⟨*string*⟩ code:⟨*string*⟩ reason: ⟨*string*⟩.
Meaning	The security device failed to process the request.
Action	Contact Juniper Networks technical support at www.juniper.net/support. (Note: You must be a registered Juniper Networks customer.)

Warning (00769)

Message	UF-MGR: URL BLOCKED: ⟨*IP address*⟩(⟨*integer*⟩)- > ⟨*IP address*⟩(⟨*integer*⟩) ⟨*string*⟩ CATEGORY: ⟨*string*⟩ REASON: ⟨*string*⟩ PROFILE: ⟨*string*⟩
Meaning	The Web filtering module blocks the user from accessing the specified URL defined in the URL category. The message indicates the source IP/port, destination IP/port, the reason to block access to the URL, and the assigned Web filtering profile.
Action	Take action based on your company policy.

Notification (00013)

Message	⟨*string*⟩
Meaning	Web filtering is enabled or disabled for the specified vsys.
Action	No recommended action.

Message	Web filtering socket count is changed to ⟨*url_server_timeout*⟩.
Meaning	Specifies the maximum number of sockets that are open to communication for each Web filtering server.
Action	No recommended action.

Message	Web filtering source interface is changed to ⟨*interface_name*⟩.
Meaning	The Web filtering interface is modified.
Action	No recommended action.

Message	Web-filtering fail mode is changed to ⟨*fail_mode_string*⟩.
Meaning	An admin changed the fail mode to permit or block.
Action	No recommended action.

Message	Web-filtering message is changed.
Meaning	An admin updated the message that is generated when Web filtering blocking occurs (if the message type is set to "Juniper Networks").
Action	No recommended action.

Message	Web-filtering message type is changed to ⟨*mesage_type_string*⟩.
Meaning	An admin changed the message type, which specifies the source (the security device, the Websense server, or the SurfControl server) of the message that the security device delivers to clients when the device blocks URLs.
Action	No recommended action.

Message	Web-filtering server account name is changed to ⟨*url_server_account_name*⟩.
Meaning	An admin changed the account name of the Web filtering server.
Action	No recommended action.

Message	Web-filtering server name is changed to ⟨*url_server_name*⟩.
Meaning	An admin changed the host name of the web filtering server.
Action	No recommended action.

Message	Web-filtering server port is changed to ⟨*url_server_port_number*⟩.
Meaning	An admin changed the web filtering server port number.
Action	No recommended action.

Message	Web-filtering timeout is changed to ⟨*url_server_timeout*⟩.
Meaning	An admin changed the timeout for communication with the URL server.
Action	No recommended action.

Notification (00523)

Message	Web filtering received an error from ⟨*url_server_vendor_name*⟩ (error 0x⟨*url_server_socket_error*⟩).
Meaning	An error status is returned from an URL server.
Action	Check the documentation for the Websense or SurfControl server, and confirm that it is configured properly. For more information, turn off "debug url receive" to see a buffer dump.

Message	Web filtering received an error from ⟨*url_server_vendor_name*⟩ (error 0x⟨*url_server_socket_error*⟩, flag 0x⟨*url_server_error_flag*⟩, cmd 0x⟨*url_server_failing_cmd*⟩).
Meaning	An error status is returned from an URL server.
Action	Check the documentation for the Websense or SurfControl server, and confirm that it is configured properly. For more information, turn off "debug url receive" to see a buffer dump.

Message	Web filtering successfully connected ⟨*url_server_vendor_name*⟩ server (connections ⟨*url_server_connection_count*⟩).
Meaning	The security device established connectivity with the Web filtering server.
Action	No recommended action.

Notification (00556)

Message	UF-MGR: The action for other in profile ⟨*string*⟩ is set to ⟨*string*⟩.
Meaning	An admin defined the default action for the specified profile.
Action	No recommended action.

Message	UF-MGR: The action for ⟨*string*⟩ in profile ⟨*string*⟩ is changed to ⟨*string*⟩.
Meaning	An admin changed the action of the specified category in the named profile.
Action	No recommended action.

Message	UF-MGR: The category list from the CPA server is updated on the device.
Meaning	The category list from the SurfControl CPA server was updated on the security device.
Action	No recommended action.

Message	UF-MGR: The category ⟨*string*⟩ is added into profile ⟨*string*⟩ with action ⟨*string*⟩.
Meaning	An admin added the specified category and its corresponding action to the named profile.
Action	No recommended action.

Message	UF-MGR: The category ⟨*string*⟩ is created.
Meaning	An admin created or deleted the specified category.
Action	No recommended action.

Message	UF-MGR: The category ⟨*string*⟩ is removed from profile ⟨*string*⟩ with action ⟨*string*⟩.
Meaning	An admin removed the specified category and its corresponding action from the named profile.
Action	No recommended action.

Message	UF-MGR: The category ⟨*string*⟩ is removed.
Meaning	An admin created or deleted the specified category.
Action	No recommended action.

Message	UF-MGR: The category ⟨*string*⟩ is set in profile ⟨*string*⟩ as the black list.
Meaning	An admin added the specified category to either the black list or the white list of the named profile.
Action	No recommended action.

Message	UF-MGR: The category ⟨*string*⟩ is set in profile ⟨*string*⟩ as the white list.
Meaning	An admin added the specified category to either the black list or the white list of the named profile.
Action	No recommended action.

Message	UF-MGR: The profile ⟨*string*⟩ black list is removed.
Meaning	An admin deleted the white list or black list from the specified profile.
Action	No recommended action.

Message	UF-MGR: The profile ⟨*string*⟩ is created.
Meaning	An admin created or deleted the specified profile.
Action	No recommended action.

Message	UF-MGR: The profile ⟨*string*⟩ is removed.
Meaning	An admin created or deleted the specified profile.
Action	No recommended action.

Message	UF-MGR: The profile ⟨*string*⟩ white list is removed.
Meaning	An admin deleted the white list or black list from the specified profile.
Action	No recommended action.

Message	UF-MGR: The URL filtering deny message is set as ⟨*string*⟩.
Meaning	An admin set the SC-CPA deny message.
Action	No recommended action.

Message	UF-MGR: The URL filtering deny message is unset and changed to the default deny message.
Meaning	An admin unset the SC-CPA deny message.
Action	No recommended action.

Message	UF-MGR: The url ⟨*string*⟩ is removed from category ⟨*string*⟩.
Meaning	An admin deleted a URL from the specified category.
Action	No recommended action.

Message	UF-MGR: The URL ⟨*string*⟩ was added to category ⟨*string*⟩.
Meaning	An admin added a URL from the specified category.
Action	No recommended action.

Message	UF-MGR: Cache disabled.
Meaning	An admin disabled the web filtering cache.
Action	No recommended action.

Message	UF-MGR: Cache enabled.
Meaning	An admin enabled the web filtering cache.
Action	No recommended action.

Message	UF-MGR: Cache size is changed to ⟨*integer*⟩(K).
Meaning	An admin changed the size of the web filtering cache.
Action	No recommended action.

Message	UF-MGR: Cache timeout is changed to ⟨*integer*⟩ (hours).
Meaning	An admin changed the timeout value of the web filtering cache.
Action	No recommended action.

Message	UF-MGR: Category update interval is changed to ⟨*integer*⟩ (weeks).
Meaning	An admin changed the interval at which the security device queries the CPA server for category updates.
Action	No recommended action.

Message	UF-MGR: Primay CPA server changed to ⟨*string*⟩.
Meaning	An admin changed the primary SurfControl server.
Action	No recommended action.

Message	UF-MGR: ⟨*string*⟩ CPA server host changed to ⟨*string*⟩.
Meaning	An admin changed the SurfControl server host name.
Action	No recommended action.

Message	UF-MGR: ⟨*string*⟩ CPA server port changed to ⟨*integer*⟩.
Meaning	An admin changed the port number of the SurfControl server.
Action	No recommended action.

Message	UF-MGR: SurfControl Web filtering disabled.
Meaning	An admin enabled or disabled the integrated web filtering feature.
Action	No recommended action.

Message	UF-MGR: SurfControl Web filtering enabled.
Meaning	An admin enabled or disabled the integrated web filtering feature.
Action	No recommended action.

Information (00769)

Message	UF-MGR: URL PERMITTED: ⟨*IP address*⟩(⟨*integer*⟩)- > ⟨*IP address*⟩(⟨*integer*⟩) ⟨*string*⟩ CATEGORY: ⟨*string*⟩ REASON: ⟨*string*⟩ PROFILE: ⟨*string*⟩
Meaning	The Web filtering module permits the user from accessing the specified URL defined in the URL category. The message indicates the source IP/port, destination IP/port, the reason to permit access to the URL, and the assigned Web filtering profile.
Action	No action recommended.

Chapter 66
WLAN

The following are related to a wireless device, referred to in the messages as wireless AP.

Alert (00564)

Message	Wireless AP re-initiated: ⟨*Re-initiated Cause*⟩
Meaning	A fatal error occurred on the wireless interface.
Action	Perform the following according to the reason displayed: AP detected radar interference: Make sure radio channel is set to auto. AP detected radio interference: Make sure the channel is not busy. Too many beacons stuck: Make sure the channel is not busy. Other reason: Run the exec wlan reactivate CLI command to reset the wireless interface.

Error (00564)

Message	Wireless AP re-activated with error: \n⟨*Atheros CLIs*⟩\nError index: ⟨*Error index*⟩\nError code: ⟨*Error code*⟩
Meaning	An incorrect command was configured before reactivating the wireless interface.
Action	Check the incorrect command from the error index.

Notification (00564)

Message	Wireless AP in ⟨*Wireless AP Mode*⟩ mode.
Meaning	Displays the status switch of the wireless interface.
Action	No recommended action.

Message	Wireless CLI updated: ⟨*wireless cli*⟩
Meaning	Recorded the CLI commands entered for the wireless configuration.
Action	No recommended action.

Message	Wireless RADIUS event: ⟨*RADIUS event*⟩.
Meaning	Displays the information about the station that is using 802.1x authentication.
Action	No recommended action.

Message	Wireless station event: ⟨*Station event*⟩.
Meaning	Displays the station association information.
Action	No recommended action.