



---

# ScreenOS Message Log Reference Guide

Release

6.3.0, Rev. 01



---

Published: 2013-04-25

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JunosE is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Copyright © 2009, Juniper Networks, Inc.

All rights reserved.

#### Revision History

April 2013—Revision 03

Content subject to change. The information in this document is current as of the date listed in the revision history.

#### SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Website at [www.juniper.net/techpubs](http://www.juniper.net/techpubs).

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	<b>About This Guide</b> .....	<b>xi</b>
	Understanding Messages .....	xi
	Organization .....	xi
<b>Chapter 1</b>	<b>Introduction</b> .....	<b>1</b>
	Anatomy of a Message .....	1
	Severity Levels and Descriptions .....	1
<b>Chapter 2</b>	<b>Addresses</b> .....	<b>3</b>
	Notification (00001) .....	3
<b>Chapter 3</b>	<b>Admin</b> .....	<b>5</b>
	Alert (00027) .....	5
	Critical (00027) .....	6
	Warning (00002) .....	7
	Warning (00515) .....	7
	Warning (00518) .....	12
	Warning (00519) .....	13
	Notification (00002) .....	13
	Notification (00003) .....	16
	Information (00002) .....	17
	Information (00519) .....	21
<b>Chapter 4</b>	<b>Anti-spam</b> .....	<b>23</b>
	Warning (00064) .....	23
	Warning (00563) .....	23
	Notification (00064) .....	24
	Notification (00563) .....	24
<b>Chapter 5</b>	<b>Antivirus</b> .....	<b>27</b>
	Critical (00554) .....	27
	Error (00054) .....	28
	Warning (00066) .....	29
	Warning (00547) .....	32
	Warning (00566) .....	34
	Notification (00066) .....	34
	Notification (00554) .....	40
<b>Chapter 6</b>	<b>ARP</b> .....	<b>43</b>
	Critical (00031) .....	43
	Critical (00079) .....	43
	Notification (00031) .....	43
	Notification (00051) .....	44

	Notification (00052) .....	44
	Notification (00053) .....	44
	Notification (00054) .....	44
	Notification (00082) .....	44
	Notification (00088) .....	45
	Notification (90) .....	45
	Notification (92) .....	45
	Information (90) .....	46
<b>Chapter 7</b>	<b>Attack Database .....</b>	<b>47</b>
	Critical (00767) .....	47
	Warning (00767) .....	47
	Notification (00767) .....	47
<b>Chapter 8</b>	<b>Attacks .....</b>	<b>53</b>
	Emergency (00005) .....	53
	Emergency (00006) .....	54
	Emergency (00007) .....	54
	Alert (00004) .....	55
	Alert (00008) .....	55
	Alert (00009) .....	56
	Alert (00010) .....	56
	Alert (00011) .....	57
	Alert (00012) .....	57
	Alert (00016) .....	58
	Alert (00017) .....	58
	Critical (00032) .....	59
	Critical (00033) .....	59
	Critical (00412) .....	60
	Critical (00413) .....	60
	Critical (00414) .....	61
	Critical (00415) .....	61
	Critical (00430) .....	62
	Critical (00431) .....	62
	Critical (00432) .....	63
	Critical (00433) .....	63
	Critical (00434) .....	64
	Critical (00435) .....	64
	Critical (00436) .....	65
	Critical (00437) .....	65
	Critical (00438) .....	66
	Critical (00439) .....	66
	Critical (00440) .....	66
	Notification (00002) .....	67
<b>Chapter 9</b>	<b>Auth .....</b>	<b>71</b>
	Critical (00015) .....	71
	Critical (00518) .....	72
	Warning (00015) .....	72
	Warning (00518) .....	73

	Warning (00519) .....	76
	Warning (00520) .....	77
	Notification (00015) .....	79
	Notification (00525) .....	92
	Notification (00543) .....	93
	Notification (00546) .....	95
	Notification (00767) .....	95
<b>Chapter 10</b>	<b>Cisco-HDLC .....</b>	<b>99</b>
	Alert (00087) .....	99
	Notification (00076) .....	99
	Notification (00571) .....	100
<b>Chapter 11</b>	<b>Device .....</b>	<b>101</b>
	Notification (00560) .....	101
<b>Chapter 12</b>	<b>DHCP .....</b>	<b>103</b>
	Alert (00029) .....	103
	Critical (00029) .....	103
	Warning (00527) .....	103
	Notification (00009) .....	104
	Notification (00024) .....	104
	Notification (00027) .....	105
	Information (00527) .....	107
	Information (00530) .....	108
	Information (00767) .....	109
<b>Chapter 13</b>	<b>DHCP6 .....</b>	<b>111</b>
	Notification (00009) .....	111
	Notification (00024) .....	111
	Information (00527) .....	112
<b>Chapter 14</b>	<b>DIP, VIP, MIP, and Zones .....</b>	<b>115</b>
	Critical (00023) .....	115
	Critical (00102) .....	115
	Critical (00103) .....	115
	Notification (00010) .....	116
	Notification (00016) .....	116
	Notification (00021) .....	116
	Notification (00037) .....	118
	Notification (00533) .....	120
<b>Chapter 15</b>	<b>DNS .....</b>	<b>121</b>
	Critical (00021) .....	121
	Notification (00004) .....	121
	Notification (00029) .....	124
	Notification (00059) .....	124
	Notification (0059) .....	128
	Information (00004) .....	128
	Information (00529) .....	129

<b>Chapter 16</b>	<b>Entitlement and System</b> . . . . .	<b>131</b>
	Alert (00027) . . . . .	131
	Critical (00027) . . . . .	132
	Critical (00051) . . . . .	133
	Critical (00850) . . . . .	133
	Critical (00851) . . . . .	133
	Notification (00002) . . . . .	134
	Notification (00006) . . . . .	134
	Notification (00018) . . . . .	134
	Notification (00036) . . . . .	134
	Notification (00526) . . . . .	136
	Notification (00553) . . . . .	136
	Notification (00625) . . . . .	136
	Notification (00767) . . . . .	136
	Information (00767) . . . . .	138
<b>Chapter 17</b>	<b>Flow</b> . . . . .	<b>145</b>
	Alert (00800) . . . . .	145
	Alert (00801) . . . . .	145
	Critical (00026) . . . . .	145
	Critical (00802) . . . . .	146
	Critical (00803) . . . . .	146
	Critical (00804) . . . . .	146
	Critical (00805) . . . . .	147
	Critical (00806) . . . . .	147
	Error (00805) . . . . .	147
	Notification (00002) . . . . .	148
	Notification (00040) . . . . .	150
	Notification (00079) . . . . .	152
	Notification (00085) . . . . .	153
	Notification (00573) . . . . .	153
	Notification (00601) . . . . .	155
	Notification (00624) . . . . .	155
	Notification (00767) . . . . .	155
<b>Chapter 18</b>	<b>Frame Relay</b> . . . . .	<b>157</b>
	Alert (00085) . . . . .	157
	Notification (00074) . . . . .	157
	Notification (00075) . . . . .	158
	Notification (00086) . . . . .	161
	Notification (00569) . . . . .	162
	Notification (00570) . . . . .	162
<b>Chapter 19</b>	<b>H.323</b> . . . . .	<b>165</b>
	Alert (00089) . . . . .	165
	Notification (00619) . . . . .	165
<b>Chapter 20</b>	<b>Interface</b> . . . . .	<b>167</b>
	Critical (00091) . . . . .	167
	Critical (00094) . . . . .	167

	Notification (00009) .....	168
	Notification (00078) .....	180
	Notification (00513) .....	180
	Notification (00613) .....	180
	Notification (00626) .....	182
	Information (00009) .....	182
<b>Chapter 21</b>	<b>Interface6 .....</b>	<b>185</b>
	Critical (00101) .....	185
	Notification (00009) .....	185
	Notification (00071) .....	186
	Notification (00072) .....	186
<b>Chapter 22</b>	<b>ISDN .....</b>	<b>189</b>
	Notification (00083) .....	189
	Notification (00618) .....	191
<b>Chapter 23</b>	<b>Logging .....</b>	<b>193</b>
	Warning (00002) .....	193
	Notification (00002) .....	194
<b>Chapter 24</b>	<b>NAT IPsec .....</b>	<b>197</b>
	Notification (00004) .....	197
	Information (00536) .....	197
<b>Chapter 25</b>	<b>NSM .....</b>	<b>199</b>
	Notification (00033) .....	199
	Information (00538) .....	211
<b>Chapter 26</b>	<b>NSRD .....</b>	<b>215</b>
	Error (00551) .....	215
	Warning (00551) .....	215
	Information (00551) .....	216
<b>Chapter 27</b>	<b>NSRP .....</b>	<b>217</b>
	Critical (00015) .....	217
	Critical (00060) .....	219
	Critical (00061) .....	219
	Critical (00070) .....	219
	Critical (00071) .....	220
	Critical (00072) .....	220
	Critical (00073) .....	220
	Critical (00074) .....	220
	Critical (00075) .....	221
	Critical (00076) .....	221
	Critical (00077) .....	221
	Notification (00007) .....	221
<b>Chapter 28</b>	<b>NTP .....</b>	<b>231</b>
	Notification (00531) .....	231
	Notification (00548) .....	234

<b>Chapter 29</b>	<b>Policy</b> .....	<b>237</b>
	Notification (00018) .....	237
<b>Chapter 30</b>	<b>PPP</b> .....	<b>243</b>
	Alert (00095) .....	243
	Alert (00096) .....	243
	Notification (00017) .....	243
	Notification (00077) .....	245
	Notification (00088) .....	247
	Notification (00572) .....	248
<b>Chapter 31</b>	<b>PPPoA</b> .....	<b>251</b>
	Notification (00060) .....	251
	Notification (00558) .....	251
<b>Chapter 32</b>	<b>PPPoE</b> .....	<b>253</b>
	Notification (00034) .....	253
	Notification (00537) .....	253
<b>Chapter 33</b>	<b>Route</b> .....	<b>257</b>
	Critical (00205) .....	257
	Notification (00011) .....	260
<b>Chapter 34</b>	<b>SCCP</b> .....	<b>265</b>
	Alert (00062) .....	265
	Alert (00083) .....	267
	Notification (00062) .....	269
	Notification (00561) .....	270
<b>Chapter 35</b>	<b>Schedule</b> .....	<b>271</b>
	Notification (00020) .....	271
<b>Chapter 36</b>	<b>Service</b> .....	<b>273</b>
	Notification (00012) .....	273
<b>Chapter 37</b>	<b>SSL</b> .....	<b>275</b>
	Warning (00515) .....	275
	Warning (00518) .....	275
	Warning (00519) .....	276
	Information (00002) .....	276
	Information (00545) .....	277
<b>Chapter 38</b>	<b>Syslog and Webtrends</b> .....	<b>279</b>
	Critical (00019) .....	279
	Critical (00020) .....	279
	Critical (00030) .....	280
	Critical (00035) .....	280
	Critical (00036) .....	281
	Critical (00037) .....	281
	Warning (00019) .....	281
	Notification (00019) .....	281
	Notification (00022) .....	292

	Notification (00628) .....	292
	Notification (00631) .....	297
	Notification (00632) .....	297
	Notification (00767) .....	297
	Information (00767) .....	300
<b>Chapter 39</b>	<b>System Authentication .....</b>	<b>301</b>
	Notification (00105) .....	301
	Notification (00614) .....	301
<b>Chapter 40</b>	<b>Traffic Shaping .....</b>	<b>303</b>
	Notification (00002) .....	303
<b>Chapter 41</b>	<b>Virtual Router .....</b>	<b>305</b>
	Critical (00082) .....	305
	Notification (00061) .....	305
<b>Chapter 42</b>	<b>Vsys .....</b>	<b>309</b>
	Notification (00032) .....	309
	Notification (00043) .....	311
	Notification (00515) .....	312
<b>Chapter 43</b>	<b>Web Filtering .....</b>	<b>313</b>
	Alert (00014) .....	313
	Notification (00013) .....	313
	Notification (00523) .....	315



# About This Guide

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

- [Understanding Messages on page xi](#)
- [Organization on page xi](#)

## Understanding Messages

---

This guide provides administrators who use network management tools, such as Juniper Networks Network and Security Manager (NSM), 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: 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 a backup unit. The source of an action is not included in the messages listed in this guide.

## Organization

---

This guide 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 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 on page 1](#)

## 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 list describes the message severity levels:

- Emergency: Messages on SYN attacks, Tear Drop attacks, and Ping of Death attacks. For more information about these types of attacks, see the *Concepts & Examples ScreenOS Reference Guide, 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 <i>&lt;address-group-name&gt;</i> <i>&lt;config-action&gt;</i> <i>&lt;member-name&gt;</i> <i>&lt;user-name&gt;</i> session.
Meaning	An administrator has added or deleted the specified address in the address group.
Action	No recommended action.
Message	Address group <i>&lt;address-group-name&gt;</i> <i>&lt;config-action&gt;</i> <i>&lt;user-name&gt;</i> session.
Meaning	An administrator added, deleted, or modified the specified address group.
Action	No recommended action.
Message	Address <i>&lt;address-name&gt;</i> for domain address <i>&lt;domain-name&gt;</i> in zone <i>&lt;zone-name&gt;</i> <i>&lt;config-action&gt;</i> <i>&lt;user-name&gt;</i> 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 <i>&lt;address-name&gt;</i> for ip address <i>&lt;ip-address&gt;</i> in zone <i>&lt;zone-name&gt;</i> <i>&lt;config-action&gt;</i> <i>&lt;user-name&gt;</i> session.
Meaning	An administrator added, deleted, or modified the specified address group.
Action	No recommended action.
Message	Address <i>&lt;address-name&gt;</i> for IP address <i>&lt;ip-address&gt;/&lt;net-mask&gt;</i> in zone <i>&lt;zone-name&gt;</i> <i>&lt;config-action&gt;</i> <i>&lt;user-name&gt;</i> 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	Admin <i>&lt;user-name&gt;</i> is locked and will be unlocked after <i>&lt;time&gt;</i> minutes
Meaning	The admin user is locked after the number of failed login attempts reaches the specified value.
Action	Monitor the login sessions to check if there is any hacking to the device.
Message	Admin <i>&lt;user-name&gt;</i> is locked, please contact Security Administrator to unlock it
Meaning	The admin user is disabled after the number of failed login attempts reaches the specified value.
Action	Monitor the login sessions to check if there is any hacking to the device.
Message	Login attempt by admin <i>&lt;user-name&gt;</i> from <i>&lt;src-ip&gt;</i> is refused as this account is locked
Meaning	Login attempt by a locked admin.
Action	Monitor the login sessions to check if there is any hacking to the device.
Message	ScreenOS <i>&lt;major_version&gt;</i> . <i>&lt;minor_version&gt;</i> . <i>&lt;rev_version&gt;</i> Serial# <i>&lt;serial_number&gt;</i> : <i>&lt;ar_log_initiated_string&gt;</i>
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 <i>&lt;major_version&gt;.&lt;minor_version&gt;.&lt;rev_version&gt;</i> Serial# <i>&lt;serial_number&gt;</i> : <i>&lt;ar_log_aborted_string&gt;</i>
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	Admin <i>&lt;user-name&gt;</i> has been re-enabled <i>&lt;changer&gt;</i> after being locked due to excessive failed login attempts
Meaning	Lock for an admin is cleared by the security admin.
Action	No recommended action.

Message	Multiple login failures occurred for user <i>&lt;user-name&gt;</i>
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 <i>&lt;user-name&gt;</i> from IP address <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i>
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.

Message	Remote authentication is refused for admin <i>&lt;user-name&gt;</i> since the maximum number of locked admin has been reached
Meaning	Remote authentication is denied for an admin because the locking table has reached maximum number of locked admins.
Action	Monitor the login sessions to check if there is any hacking to the device.

### Warning (00002)

Message	ADMIN AUTH: Local instance of an external admin user privilege has been changed from <i>&lt;privilege&gt;</i> to <i>&lt;privilege&gt;</i> .
Meaning	An administrator modified the privileges of an external administrator.
Action	No recommended action.

### Warning (00515)

Message	Admin user <i>&lt;user-name&gt;</i> 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 <i>&lt;user-name&gt;</i> has been forced to log out of the SSH session on host <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> has been forced to log out of the Telnet session on host <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> has been forced to log out of the Web session on host <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> has logged on via SSH from <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> has logged on via Telnet from <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> 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 <i>&lt;user-name&gt;</i> has logged out via SSH from <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> has logged out via Telnet from <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> 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 <i>&lt;user-name&gt;</i> via SSH from <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> has failed <i>&lt;reason&gt;</i>
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 <i>&lt;user-name&gt;</i> via Telnet from <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> has failed <i>&lt;reason&gt;</i>
Meaning	An attempt to login 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's user name and password.

Message	Login attempt to system by admin <i>&lt;user-name&gt;</i> via the console has failed <i>&lt;reason&gt;</i>
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 <i>&lt;vsys&gt;</i> admin <i>&lt;user-name&gt;</i> 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 <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i> for <i>&lt;vsys&gt;</i> admin <i>&lt;user-name&gt;</i> 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 <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i> for <i>&lt;vsys&gt;</i> admin <i>&lt;user-name&gt;</i> 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 <i>&lt;user-name&gt;</i> 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 *<user-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 *<user-name>* has logged on via SSH from *<src-ip>*:*<src-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 *<user-name>* has logged on via Telnet from *<src-ip>*:*<src-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 *<user-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 *<user-name>* has logged out via SSH from *<src-ip>*:*<src-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 <i>&lt;user-name&gt;</i> has logged out via Telnet from <i>&lt;src-ip&gt;:&lt;src-port&gt;</i>
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 <i>&lt;user-name&gt;</i> 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 <i>&lt;user-name&gt;</i> : 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 <i>&lt;user-name&gt;</i> : 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 <i>&lt;user-name&gt;</i> has been rejected via the <i>&lt;server_name&gt;</i> server at <i>&lt;ip_addr&gt;</i> .
Meaning	The named admin user has been rejected by the specified server.
Action	No recommended action.

### Warning (00519)

Message	Admin user <i>&lt;user-name&gt;</i> has been accepted via the <i>&lt;server_name&gt;</i> server at <i>&lt;ip_addr&gt;</i> .
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 <i>&lt;user-name&gt;</i> <i>&lt;changed_via&gt;</i>
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 <i>&lt;user-name&gt;</i> <i>&lt;changed_via&gt;</i>
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 <i>&lt;passwd_len&gt;</i> characters has been disabled by admin <i>&lt;user-name&gt;</i> <i>&lt;changed_via&gt;</i>
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 <i>&lt;passwd_len&gt;</i> characters has been enabled by admin <i>&lt;user-name&gt;</i> <i>&lt;changed_via&gt;</i>
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 <i>&lt;user-name&gt;</i> <i>&lt;changed_via&gt;</i>
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 <i>&lt;user-name&gt;</i> <i>&lt;changed_via&gt;</i>
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	Access scheduler <i>&lt;scheduler_name&gt;</i> is affiliated with admin <i>&lt;attached_admin&gt;</i> in vsys <i>&lt;vsys_name&gt;</i> . (by admin <i>&lt;cmd_admin&gt;</i> ).
Meaning	Admin is only allowed to access firewall in the time window which is defined by the scheduler.
Action	No recommended action.
Message	Access scheduler <i>&lt;scheduler_name&gt;</i> is unaffiliated with admin <i>&lt;attached_admin&gt;</i> in vsys <i>&lt;vsys_name&gt;</i> . (by admin <i>&lt;cmd_admin&gt;</i> ).
Meaning	Admin is restored to access firewall at any time.
Action	No recommended action.

Message      Access scheduler affiliated with admin *<attached\_admin>* is changed from *<old\_scheduler\_name>* to *<new\_scheduler\_name>* in vsys *<vsys\_name>*. (by admin *<user-name>*).

Meaning      Admin is restored to access firewall at any time.

Action        No recommended action.

Message      ADM: Non-primary authentication server *<status>* to authenticate non-ROOT privileged admins. Modifier: *<user-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: *<user-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: *<user-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. Modifier: *<user-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 <i>&lt;status&gt;</i> . Modifier: <i>&lt;user-name&gt;</i>
Meaning	An admin has changed the status of the remotely authenticated root admins.
Action	No recommended action.

Message	Admin user <i>&lt;user-name&gt;</i> with role <i>&lt;role&gt;</i> violated the role privilege attempting to run command of <i>&lt;cmd_line&gt;</i>
Meaning	The admin user noted with the listed role attempted to run a command that is not permitted by the role.
Action	No recommended action.

Message	Maximum failed login attempts before administrative session disconnects has been modified from <i>&lt;orig_value&gt;</i> to <i>&lt;new_value&gt;</i> <i>&lt;changed_via&gt;</i>
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 <i>&lt;status&gt;</i>
Meaning	An admin has enabled (or disabled) the console debug buffer.
Action	No recommended action.

Message	The console page size changed from <i>&lt;old_page_size&gt;</i> to <i>&lt;new_page_size&gt;</i>
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 <i>&lt;old_timeout_value&gt;</i> to <i>&lt;new_timeout_value&gt;</i> 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 <i>&lt;status&gt;</i> by admin <i>&lt;user-name&gt;</i>
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 <i>&lt;user-name&gt;</i> <i>&lt;changer&gt;</i>
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 <i>&lt;user-name&gt;</i> <i>&lt;changer&gt;</i>
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 <i>&lt;user-name&gt;</i> <i>&lt;changer&gt;</i>
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 <i>&lt;old_admin_name&gt;</i> has been modified to <i>&lt;new_admin_name&gt;</i> <i>&lt;changer&gt;</i>
Meaning	An admin changed the account name from <i>name_str1</i> to <i>name_str2</i> . The name of the administrator who made the account name change follows the message ( <i>name_str3</i> )
Action	No recommended action.
Message	Admin password for account <i>&lt;user-name&gt;</i> has been modified <i>&lt;changer&gt;</i>
Meaning	An admin changed the password for the specified account ( <i>name_str1</i> ). The name of the admin who changed the password follows the message ( <i>name_str2</i> ).
Action	No recommended action.
Message	Dial-in admin authentication timeout value has been changed from <i>&lt;old_timeout&gt;</i> to <i>&lt;new_timeout&gt;</i> 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 <i>&lt;changer&gt;</i>
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 <i>&lt;old_port&gt;</i> to <i>&lt;new_port&gt;</i> <i>&lt;user-name&gt;</i>
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 <i>&lt;ip_addr&gt;</i> has been removed in vsys <i>&lt;vsys_name&gt;</i> . (by admin <i>&lt;admin_name&gt;</i> )
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 <i>&lt;ip_addr&gt;</i> subnet <i>&lt;ip_mask&gt;</i> has been added in vsys ' <i>&lt;vsys_name&gt;</i> '. (by admin <i>&lt;admin_name&gt;</i> )
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 <i>&lt;vsys_name&gt;</i> . (by admin <i>&lt;admin_name&gt;</i> )
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 <i>&lt;admin_name&gt;</i> )
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	Role for admin <i>&lt;admin_name&gt;</i> has been modified from <i>&lt;old_role&gt;</i> to <i>&lt;new_role&gt;</i> <i>&lt;user-name&gt;</i>
Meaning	An admin has modified the role of a specified account. The name of the admin who modified the role appears after the message.
Action	No recommended action.
Message	SSH port has been changed from <i>&lt;old_port&gt;</i> to <i>&lt;new_port&gt;</i> <i>&lt;user-name&gt;</i>
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 <i>&lt;old_ip_addr&gt;</i> to <i>&lt;new_ip_addr&gt;</i> <i>&lt;user-name&gt;</i>
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 <i>&lt;old_port&gt;</i> to <i>&lt;new_port&gt;</i> <i>&lt;user-name&gt;</i>
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 <i>&lt;old_timeout&gt;</i> to <i>&lt;new_timeout&gt;</i> 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.

**Information (00519)**

Message	ADM: Local admin authentication successful for login name ( <i>user-name</i> )
Meaning	The specified admin has been successfully authenticated in the local database.
Action	No recommended action.



## CHAPTER 4

# Anti-spam

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

### Warning (00064)

Message	Anti-Spam is attached to policy ID <i>&lt;policy-id&gt;</i> .
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 <i>&lt;policy-id&gt;</i> .
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 ! <i>&lt;as-sender-info&gt;</i> .
Meaning	This indicates the software was successful in detecting spam. Verify the spam to make sure it is not a false positive. The <i>&lt;string&gt;</i> 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: <i>&lt;sbl-server-name&gt;</i> .
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: <i>&lt;expiration-date&gt;</i> 2; current date: <i>&lt;current-date&gt;</i> 2).
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 ( <i>&lt;url-server-vendor-name&gt;</i> ).
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 5

# 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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> 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: <i>&lt;outcome&gt;</i> .
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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> 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: <i>&lt;outcome&gt;</i> .
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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> 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 ( <i>&lt;size&gt;</i> 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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> 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.

## Error (00054)

Message	APPPRY: Suspicious client <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i> -> <i>&lt;dst-ip&gt;</i> : <i>&lt;dst-port&gt;</i> used <i>&lt;used&gt;</i> percent of AV resources, which exceeded the maximum of <i>&lt;max&gt;</i> 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 <i>&lt;percent&gt;</i> .

## Warning (00066)

Message	AV configures an Extension list <i>&lt;extension-list&gt;</i> with extension <i>&lt;extension&gt;</i> .
Meaning	The antivirus scanner configures an extension list (string1) with the specified extensions (string2).
Action	No recommended action.
Message	AV configures MIME list <i>&lt;MIME-list&gt;</i> with MIME <i>&lt;MIME&gt;</i> .
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 <i>&lt;profile&gt;</i> .
Meaning	The antivirus scanner creates the specified profile.
Action	No recommended action.
Message	AV object <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> 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 <i>&lt;pre-dbtype&gt;</i> to <i>&lt;new-dbtype&gt;</i> 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 <i>&lt;common-name&gt;</i> sets ICAP <i>&lt;param-type&gt;</i> to <i>&lt;suffix&gt;</i> .
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 <i>&lt;common-name&gt;</i> <i>&lt;cmd-name&gt;</i> s protocol <i>&lt;app-type&gt;</i> <i>&lt;param-type&gt;</i> <i>&lt;dim0&gt;</i> <i>&lt;value&gt;</i> <i>&lt;dim1&gt;</i> <i>&lt;dim2&gt;</i> .
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 <i>&lt;common-name&gt;</i> <i>&lt;cmd-name&gt;</i> s protocol <i>&lt;app-type&gt;</i> <i>&lt;param-type&gt;</i> <i>&lt;dim0&gt;</i> <i>&lt;value&gt;</i> <i>&lt;dim1&gt;</i> <i>&lt;dim2&gt;</i> .
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 <i>&lt;common-name&gt;</i> unsets ICAP <i>&lt;param-type&gt;</i> .
Meaning	The ICAP settings are removed from the AV profile.
Action	No recommended action.
Message	AV removes extension list <i>&lt;extension-list&gt;</i> .
Meaning	The antivirus scanner removes the extension list (string).
Action	No recommended action.
Message	AV removes MIME list <i>&lt;MIME-list&gt;</i> .
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 <i>&lt;profile&gt;</i> .
Meaning	The antivirus scanner deletes the specified profile.
Action	No recommended action.
Message	AV <i>&lt;av&gt;</i> is attached to policy ID <i>&lt;policy-id&gt;</i> .
Meaning	AV is applied to the specified policy.
Action	No recommended action.
Message	AV <i>&lt;av&gt;</i> is detached from policy ID <i>&lt;policy-id&gt;</i>
Meaning	AV is not assigned to the specified policy.
Action	No recommended action.

## Warning (00547)

Message	AV: Content from <i>&lt;ip&gt;:&lt;port&gt;-&gt;&lt;ip&gt;:&lt;port&gt;&lt;none&gt;64s&lt;caption&gt;</i> 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 <i>&lt;ip&gt;:&lt;port&gt;-&gt;&lt;ip&gt;:&lt;port&gt;&lt;none&gt;64s&lt;caption&gt;</i> 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: <code>set av scan-mgr max-content-size number</code> . 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 <i>&lt;ip&gt;:&lt;port&gt;-&gt;&lt;ip&gt;:&lt;port&gt;&lt;none&gt;64s&lt;caption&gt;</i> is dropped due to scan-engine error or constraint with code <i>&lt;file&gt;</i> for <i>&lt;none&gt;</i> .
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, <code>set av all fail-mode traffic permit</code> .

Message	AV: Content from <i>&lt;ip&gt;:&lt;port&gt;-&gt;&lt;ip&gt;:&lt;port&gt;&lt;none&gt;64s&lt;caption&gt;</i> 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 <i>&lt;ip&gt;:&lt;port&gt;-&gt;&lt;ip&gt;:&lt;port&gt;&lt;none&gt;64s&lt;caption&gt;</i> 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: <code>set av scan-mgr max-content-size number</code> . 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 <i>&lt;ip&gt;:&lt;port&gt;-&gt;&lt;ip&gt;:&lt;port&gt;&lt;none&gt;64s&lt;caption&gt;</i> is passed due to scan-engine error or constraint with code <i>&lt;file&gt;</i> for <i>&lt;none&gt;</i> .
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, <code>set av all fail-mode traffic permit</code> .
Message	AV: VIRUS FOUND: <i>&lt;ip&gt;:&lt;port&gt;-&gt;&lt;ip&gt;:&lt;port&gt;&lt;none&gt;64s&lt;caption&gt;</i> file <i>&lt;file&gt;64s</i> virus <i>&lt;none&gt;</i> virus description: <i>&lt;file&gt;</i>
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.

## Warning (00566)

Message	APP session $\langle src-ip \rangle : \langle src-port \rangle - \rightarrow \langle dst-ip \rangle : \langle dst-port \rangle$ is aborted due to $\langle msg \rangle$ with code $\langle code \rangle$ .
Meaning	Application (FTP, HTTP, POP3, SMTP, IMAP) session from $ip\_address1$ to $ip\_address2$ is aborted because of $\langle string \rangle$ .
Action	The $\langle string \rangle$ 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 $\langle number \rangle$ ). If your $\langle string \rangle$ is of the format "xxx parse xxx error," then the application protocol (ftp/http/pop3/smtp/imap) failed to parse the traffic. If your $\langle string \rangle$ 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 <a href="http://www.juniper.net/support">www.juniper.net/support</a>
Message	APP session $\langle src-ip \rangle : \langle src-port \rangle - \rightarrow \langle dst-ip \rangle : \langle dst-port \rangle$ notification email failed due to $\langle none \rangle$ with code $\langle outcome \rangle$ .
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 $\langle string \rangle$ 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 configuration: charset of virus notification E-mail is removed.
Meaning	The user-defined charset of the virus notification e-mail is removed.
Action	No recommended action.

Message	AV configuration: charset of virus notification E-mail is set to <i>&lt;charset&gt;</i> .
Meaning	The user-defined charset of the virus notification e-mail is specified.
Action	No recommended action.
Message	AV configuration: source address of notification E-mail is removed.
Meaning	The user-defined source address of the notification e-mail is removed.
Action	No recommended action.
Message	AV configuration: source address of notification E-mail is set to <i>&lt;src-ip&gt;</i> .
Meaning	The user-defined source address of the notification e-mail is specified.
Action	No recommended action.
Message	AV configuration: subject of virus notification E-mail is set to <i>&lt;subject&gt;</i> .
Meaning	The user-defined subject of the virus notification e-mail is specified.
Action	No recommended action.
Message	AV configuration: virus warning message is removed.
Meaning	The user-defined warning message for the virus notification is removed.
Action	No recommended action.
Message	AV configuration: virus warning message is set to <i>&lt;warning-msg&gt;</i> .
Meaning	The user-defined warning message for virus notification is specified.
Action	No recommended action.
Message	AV fail mode is set to <i>&lt;fail-mode&gt;</i> 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 <i>⟨fail-mode⟩</i> 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 <i>⟨fail-mode⟩</i> 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 <i>⟨fail-mode⟩</i> 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 <i>⟨fail-mode⟩</i> 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 <i>⟨fail-mode⟩</i> 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 <i>&lt;fail-mode&gt;</i> 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 <i>&lt;fail-mode&gt;</i> 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 <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> byte for every <i>&lt;none&gt;</i> KB if content length is larger than <i>&lt;none&gt;</i> KB, timeout interval is <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> byte for every <i>&lt;none&gt;</i> Mb, if content length is larger than <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> .
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 <i>&lt;size&gt;</i> 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 <i>&lt;max-concurrent-messages&gt;</i> .
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 <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> is enabled with timeout <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> is enabled with timeout <i>&lt;none&gt;</i> .
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 <i>&lt;resource-allowed&gt;</i> 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 <i>&lt;queue-size&gt;</i> .
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: <i>&lt;none&gt;</i> sending Admin E-mail after AV pattern file updated.
Meaning	The AV scanner is set either to send or not to send an Admin e-mail after AV pattern file is updated.
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 (00554)

Message	SCAN-MGR: Attempted to load AV pattern file created on <i>&lt;none&gt;</i> 2 after the AV license expired on <i>&lt;none&gt;</i> 2.
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 <i>&lt;msg&gt;</i> ( <i>&lt;outcome&gt;</i> ). HTTP status code: <i>&lt;status&gt;</i> .
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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> 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: <i>&lt;version&gt;</i> ; size: <i>&lt;size&gt;</i> 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: <i>&lt;none&gt;</i>
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 <i>&lt;url&gt;</i> and the update interval is set to <i>&lt;interval&gt;</i> 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 6

# ARP

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

### Critical (00031)

Message	<i>&lt;detected-name&gt;</i> detected an IP conflict (IP <i>&lt;ip&gt;</i> , MAC <i>&lt;mac&gt;</i> ) on interface <i>&lt;interface-name&gt;</i>
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	<i>&lt;detected-name&gt;</i> detected a duplicate VSD group master (IP <i>&lt;ip&gt;</i> , MAC <i>&lt;mac&gt;</i> ) on interface <i>&lt;interface-name&gt;</i>
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 <i>&lt;ip&gt;</i> changed from interface <i>&lt;interface-name&gt;</i> to interface <i>&lt;interface-name&gt;</i>
Meaning	The Address Resolution Protocol (ARP) service noted that the mapping of interface-to-IP address for the specified IP address changed from <i>&lt;interface1&gt;</i> to <i>&lt;interface2&gt;</i> . This can cause future ARP errors.
Action	Map ARP to the correct interface.

**Notification (00051)**

Message	Static ARP entry added to interface <i>&lt;interface-name&gt;</i> with IP <i>&lt;ip&gt;</i> and MAC <i>&lt;mac&gt;</i>
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 <i>&lt;interface-name&gt;</i> with IP address <i>&lt;ip&gt;</i> and MAC address <i>&lt;mac&gt;</i>
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 has 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 has 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: <i>&lt;none&gt;</i> <i>&lt;none&gt;</i>
Meaning	IRDP informational message.
Action	No recommended action.

### Notification (00088)

Message	The DSCP value <i>&lt;dscp-value&gt;</i> is set for <i>&lt;service&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	Set the DSCP value for a specified service.
Action	No recommended action.

Message	The DSCP value is unset for <i>&lt;service&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	Unset the DSCP value for a specified service.
Action	No recommended action.

### Notification (90)

Message	Proxy-arp-entry was added to interface <i>&lt;interface-name&gt;</i> with IP range from <i>&lt;proxy_arp_entry_min&gt;</i> to <i>&lt;proxy_arp_entry_max&gt;</i> in VSYS <i>&lt;vsys_name&gt;</i>
Meaning	A proxy-arp-entry is added to the interface.
Action	No recommended action.

Message	Proxy-arp-entry was removed from interface <i>&lt;interface-name&gt;</i> with IP range from <i>&lt;proxy_arp_entry_min&gt;</i> to <i>&lt;proxy_arp_entry_max&gt;</i> in VSYS <i>&lt;vsys_name&gt;</i>
Meaning	A proxy-arp-entry is removed from the interface.
Action	No recommended action.

### Notification (92)

Message	TCP keep-alive idle time has been changed from <i>&lt;old-idle-time&gt;</i> to <i>&lt;idle-time&gt;</i> by <i>&lt;user-name&gt;</i>
Meaning	The TCP keep-alive idle time has changed.
Action	No recommended action.

Message	TCP keep-alive probe interval has been changed from <i>&lt;old-probe-interval&gt;</i> to <i>&lt;probe-interval&gt;</i> by <i>&lt;user-name&gt;</i>
Meaning	The TCP keep-alive probe interval has changed.
Action	No recommended action.

Message	TCP keep-alive probes threshold has been changed from <i>⟨old-probe-threshold⟩</i> to <i>⟨probe-threshold⟩</i> by <i>⟨user-name⟩</i>
Meaning	The TCP keep-alive probes threshold has changed.
Action	none

### Information (90)

Message	Dst NAT ARP is enabled, but it is deprecated
Meaning	The command entered is deprecated. Use the new command.
Action	Use the new proxy-arp-entry command.

## CHAPTER 7

# 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 flavors, namely high memory and low memory.
Action	Upgrade to the high memory security device.

### Warning (00767)

Message	Attack database update cannot be rolled back.
Meaning	After failing to update the attack database, the security device tried to rollback to the original attack database, but failed.
Action	Download another database to the security device. If the problem persists, contact Juniper Networks technical support by visiting <a href="http://www.juniper.net/support">www.juniper.net/support</a> . (Note: You must be a registered Juniper Networks customer.)

### Notification (00767)

Message	Attack database update has been rolled back.
Meaning	After failing to update the attack database, the security device successfully uses the original attack database.
Action	Download another database to the security device. If the problem persists, contact Juniper Networks technical support by visiting <a href="http://www.juniper.net/support">www.juniper.net/support</a> . (Note: You must be a registered Juniper Networks customer.)

Message	Attack database version <i>&lt;none&gt;</i> 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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> 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 <i>&lt;none&gt;</i> is <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> is added to <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin added a attack group member to the specified attack group using the WebUI or CLI.
Action	No recommended action.
Message	Attack group <i>&lt;none&gt;</i> is changed to <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The specified admin modified the attack group name using the WebUI or CLI.
Action	No recommended action.
Message	Attack group <i>&lt;none&gt;</i> is created <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The admin created the specified attack group using the WebUI or CLI.
Action	No recommended action.

Message	Attack group <i>&lt;none&gt;</i> is deleted <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The admin deleted the specified attack group using the WebUI or CLI.
Action	No recommended action.
Message	Attack group <i>&lt;none&gt;</i> is removed from <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin removed the attack group member from the specified attack group using the WebUI or CLI.
Action	No recommended action.
Message	Attack <i>&lt;none&gt;</i> is added to attack group <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The admin added an attack to the specified attack group using the WebUI or CLI.
Action	No recommended action.
Message	Attack <i>&lt;none&gt;</i> is changed to <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The specified admin modified the attack name using the WebUI or CLI.
Action	No recommended action.
Message	Attack <i>&lt;none&gt;</i> is created <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The specified admin created the attack group using the WebUI or CLI.
Action	No recommended action.
Message	Attack <i>&lt;none&gt;</i> is deleted <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The specified admin deleted the attack group using the WebUI or CLI.
Action	No recommended action.

Message	Attack <i>&lt;none&gt;</i> is removed from <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The admin deleted an attack from the specified attack group using the WebUI or CLI.
Action	No recommended action.
Message	Cannot download attack database from <i>&lt;none&gt;</i> (error <i>&lt;none&gt;</i> ).
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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> . (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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> . (Note: You must be a registered Juniper Networks customer.)
Message	Cannot save attack database version <i>(none)</i> .
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 <i>(none)</i> .
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 8

# 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 (00005)

Message	SYN flood! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 (00006)

Message	Teardrop attack! From <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;</i> : <i>&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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).

## Emergency (00007)

Message	Ping of Death! From <i>&lt;src-ip&gt;</i> to <i>&lt;dst-ip&gt;</i> , proto 1 (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Internet Control Messages Protocol (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

### Alert (00004)

Message	WinNuke attack! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:139</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (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).

### Alert (00008)

Message	IP spoofing! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00009)

Message	Source Route IP option! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00010)

Message	Land attack! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (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 (00011)

Message	ICMP flood! From <i>&lt;src-ip&gt;</i> to <i>&lt;dst-ip&gt;</i> , proto 1 (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> times.
Meaning	The security device has detected an excessive number of Internet Control Messages Protocol (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 (00012)

Message	UDP flood! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto UDP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> times.
Meaning	The security device has detected an excessive number of User Datagram Protocol (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 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 (00016)

Message	Port scan! From $\langle src-ip \rangle$ : $\langle src-port \rangle$ to $\langle dst-ip \rangle$ : $\langle dst-port \rangle$ , proto { TCP   UDP   $\langle protocol \rangle$ } (zone $\langle zone-name \rangle$ , int $\langle interface-name \rangle$ ). Occurred $\langle none \rangle$ 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00017)

Message	Address sweep! From $\langle src-ip \rangle$ to $\langle dst-ip \rangle$ , proto 1 (zone $\langle zone-name \rangle$ , int $\langle interface-name \rangle$ ). Occurred $\langle none \rangle$ 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 Internet Control Messages Protocol (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.

**Critical (00032)**

Message	Malicious URL! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 (00033)**

Message	Src IP session limit! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00412)

Message	SYN fragment! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 (00413)

Message	No TCP flag! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> times.
Meaning	The security device has detected a Transmission Control Protocol (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 Transmission Control Protocol (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 (00414)**

Message	Unknown protocol! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto <i>&lt;protocol&gt;</i> (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 (00415)**

Message	Bad IP option! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 (00430)

Message	Dst IP session limit! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00431)

Message	ZIP file blocked! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00432)

Message	Java applet blocked! From $\langle src-ip \rangle : \langle src-port \rangle$ to $\langle dst-ip \rangle : \langle dst-port \rangle$ , proto { TCP   UDP   $\langle protocol \rangle$ } (zone $\langle zone-name \rangle$ , int $\langle interface-name \rangle$ ). Occurred $\langle none \rangle$ 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00433)

Message	EXE file blocked! From $\langle src-ip \rangle : \langle src-port \rangle$ to $\langle dst-ip \rangle : \langle dst-port \rangle$ , proto { TCP   UDP   $\langle protocol \rangle$ } (zone $\langle zone-name \rangle$ , int $\langle interface-name \rangle$ ). Occurred $\langle none \rangle$ 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00434)

Message	ActiveX control blocked! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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 (00435)

Message	ICMP fragment! From <i>&lt;src-ip&gt;</i> to <i>&lt;dst-ip&gt;</i> , proto 1 (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> times.
Meaning	The security device detected a fragmented Internet Control Messages Protocol (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 (00436)**

Message	Large ICMP packet! From <i>&lt;src-ip&gt;</i> to <i>&lt;dst-ip&gt;</i> , proto 1 (zone <i>&lt;zone-name&gt;</i> ), int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> times.
Meaning	The security device detected an Internet Control Messages Protocol (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 (00437)**

Message	SYN and FIN bits! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (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 (00438)

Message	FIN but no ACK bit! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> times.
Meaning	Transmission Control Protocol (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 (00439)

Message	SYN-ACK-ACK Proxy DoS! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto TCP (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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 Transmission Control Protocol (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 (00440)

Message	Fragmented traffic! From <i>&lt;src-ip&gt;:&lt;src-port&gt;</i> to <i>&lt;dst-ip&gt;:&lt;dst-port&gt;</i> , proto { TCP   UDP   <i>&lt;protocol&gt;</i> } (zone <i>&lt;zone-name&gt;</i> , int <i>&lt;interface-name&gt;</i> ). Occurred <i>&lt;none&gt;</i> 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.

## Notification (00002)

Message	Bypass non-IP traffic option is <i>&lt;action&gt;</i> .
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. (Address Resolution Protocol (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-icmpv6-mld option is <i>&lt;action&gt;</i> .
Meaning	The security device permits Multicast Listener Discovery packet to pass through the firewall when the interfaces are in Transparent mode.
Action	No recommended action.
Message	Bypass-icmpv6-mrd option is <i>&lt;action&gt;</i> .
Meaning	The security device permits Multicast Router Discovery packet to pass through the firewall when the interfaces are in Transparent mode.
Action	No recommended action.
Message	Bypass-icmpv6-msp option is <i>&lt;action&gt;</i> .
Meaning	The security device permits Mobility Support Protocol packet to pass through the firewall when the interfaces are in Transparent mode.
Action	No recommended action.
Message	Bypass-icmpv6-ndp option is <i>&lt;action&gt;</i> .
Meaning	The security device permits Neighbor Discovery Protocol packet to pass through the firewall when the interfaces are in Transparent mode.
Action	No recommended action.

Message	Bypass-icmpv6-snd option is <i>&lt;action&gt;</i> .
Meaning	The security device permits Secure Neighbor Discovery Protocol packet to pass through the firewall when the interfaces are in Transparent mode.
Action	No recommended action.
Message	Bypass-ipv6-others-IPSec option is <i>&lt;action&gt;</i> .
Meaning	The security device permits IPv6 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.
Action	No recommended action.
Message	Bypass-others-IPSec option is <i>&lt;action&gt;</i> .
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. (Address Resolution Protocol (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 <i>&lt;action&gt;</i> .
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 <i>&lt;action&gt;</i> .
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 <i>&lt;action&gt;</i> .
Meaning	An admin has enabled or disabled the logging of Internet Control Messages Protocol (ICMP) traffic destined for the security device.
Action	No recommended action.
Message	Logging of IKE traffic to self has been <i>&lt;action&gt;</i> .
Meaning	An admin has enabled or disabled the logging of Internet Key Exchange (IKE) traffic destined for the security device.
Action	No recommended action.
Message	Logging of SNMP traffic to self has been <i>&lt;action&gt;</i> .
Meaning	An admin has enabled or disabled the logging of Simple Network Management Protocol (SNMP) traffic destined for the security device.
Action	No recommended action.
Message	Malicious URL <i>&lt;service-name&gt;</i> is <i>&lt;action&gt;</i> for <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> .
Meaning	An admin has added, deleted, or modified the a URL address string for the named zone.
Action	No recommended action.
Message	<i>&lt;service-name&gt;</i> is <i>&lt;none&gt;</i> on <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> .
Meaning	The specified SCREEN option has been enabled or disabled for the named zone.
Action	No recommended action.
Message	<i>&lt;service-name&gt;</i> is set to <i>&lt;none&gt;</i> for <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> .
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 <i>&lt;action&gt;</i> on <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> .
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 <i>&lt;action&gt;</i> .
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 <i>&lt;action&gt;</i> .
Meaning	An admin has enabled or disabled the logging of Netscreen and Security Manager (NSM) traffic destined for the security device.
Action	No recommended action.
Message	Logging of SSH traffic to self has been <i>&lt;action&gt;</i> .
Meaning	An admin has enabled or disabled the logging of Secure Shell (SSH) traffic destined for the security device.
Action	No recommended action.
Message	Logging of WEB traffic to self has been <i>&lt;action&gt;</i> .
Meaning	An admin has enabled or disabled the logging of WEB traffic destined for the security device.
Action	No recommended action.

## CHAPTER 9

# Auth

The following messages relate to user authentication.

### Critical (00015)

Message	Administrator's password complexity is set to scheme ' <i>&lt;length&gt;</i> ' by admin ' <i>&lt;user-name&gt;</i> '.
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 ' <i>&lt;length&gt;</i> ' by admin ' <i>&lt;user-name&gt;</i> '.
Meaning	The identified admin configured the minimum password length.
Action	No action recommended.
Message	Auth user's password complexity is set to scheme ' <i>&lt;length&gt;</i> ' by admin ' <i>&lt;user-name&gt;</i> '.
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 ' <i>&lt;length&gt;</i> ' by admin ' <i>&lt;user-name&gt;</i> '.
Meaning	The identified admin set the minimum length of the auth user password.
Action	No action recommended.

## Critical (00518)

Message	Admin user ' <i>&lt;user-name&gt;</i> ' 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 ' <i>&lt;user-name&gt;</i> ' 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 (00015)

Message	IDP attack notifications to Infranet Controller are being dropped because too many attacks are being detected in too short a period of time.
Meaning	The Infranet Enforcer is dropping some attack notifications instead of sending them to the Infranet Controller because too many attacks are being detected all at once. The reason to drop the notifications is to avoid denial-of-service attacks against the communication channel between the Infranet Enforcer and Infranet Controller.
Action	Check Infranet Controller and NSM logs for information about the attacks that are being detected.

## Warning (00518)

Message	Authentication for user <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i>
Meaning	The user attempted authentication via the WebAuth authentication server, but encountered an error condition.
Action	No recommended action.
Message	Local authentication for user <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> was denied <i>&lt;reason&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> was denied <i>&lt;reason&gt;</i>
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	Authentication for client <i>&lt;src-ip&gt;</i> 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.
Message	Authentication for client <i>&lt;src-ip&gt;</i> was denied (too long a username).
Meaning	The provided user name is too long.
Action	Check the user name; the length of the user name should not exceed 64 characters.
Message	User <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> is challenged by the <i>&lt;auth_server_type&gt;</i> server at <i>&lt;auth_server_ip&gt;</i> . (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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> is challenged by the <i>&lt;auth_server_type&gt;</i> server at <i>&lt;auth_server_ip&gt;</i> . (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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> is rejected by the <i>&lt;auth_server_type&gt;</i> server at <i>&lt;auth_server_ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> is rejected by the <i>&lt;auth_server_type&gt;</i> server at <i>&lt;auth_server_ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> is rejected through the <i>&lt;auth_server_type&gt;</i> server at <i>&lt;auth_server_ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> <i>&lt;auth_server_type&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> <i>&lt;auth_server_type&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> <i>&lt;auth_server_type&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> is rejected/timed out by the <i>&lt;server-type&gt;</i> server at <i>&lt;dst-ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> was successful.
Meaning	The user authenticated successfully.
Action	No recommended action.
Message	Local authentication for WebAuth user <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> was successful
Meaning	The specified WebAuth user successfully authenticated.
Action	No recommended action.

Message User *<user-name>* at *<of\_group>* is accepted by the *<src-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 *<src-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 *<src-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 *<src-ip>* is accepted by the *<server-type>* server at *<dst-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 Server *<server-ip>* is unavailable.

Meaning The communicating server notifies the security device that another server is not responding.

Action No recommended action.

Message Active Server Switchover: New requests for *<server-ip>* server will try *<next-server-ip>* from now on.

Meaning The server under communication is not responding. The device is trying to connect to another configured server.

Action No recommended action.

Message	Backup1 <i>&lt;primary_server_name&gt;</i> , backup2 <i>&lt;backup1_server_name&gt;</i> , and primary <i>&lt;backup2_server_name&gt;</i> servers failed.
Meaning	The connection to the specified servers failed.
Action	Verify network connectivity to the specified servers.
Message	Backup2 <i>&lt;backup2_server_name&gt;</i> , primary <i>&lt;primary_server_name&gt;</i> , and backup1 <i>&lt;backup1_server_name&gt;</i> servers failed.
Meaning	The connection to the specified servers failed.
Action	Verify network connectivity to the specified servers.
Message	Primary <i>&lt;primary_server_name&gt;</i> , backup1 <i>&lt;backup1_server_name&gt;</i> , and backup2 <i>&lt;backup2_server_name&gt;</i> servers failed.
Meaning	The connection to the specified servers failed.
Action	Verify network connectivity to the specified servers.
Message	Trying backup1 server <i>&lt;backup1_server_name&gt;</i> .
Meaning	The security device is trying to connect to the specified primary backup server.
Action	No recommended action.
Message	Trying backup2 server <i>&lt;backup2_server_name&gt;</i> .
Meaning	The security device is trying to connect to the specified secondary backup server.
Action	No recommended action.
Message	Trying primary server <i>&lt;primary_server_name&gt;</i> .
Meaning	The security device is trying to connect to the specified server.
Action	No recommended action.

## Notification (00015)

Message	Certificate Authority index for Infranet Controller <i>&lt;infranet_controller_obj_name&gt;</i> 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 <i>&lt;infranet_controller_obj_name&gt;</i> changed from <i>&lt;old_cert_name&gt;</i> to <i>&lt;new_cert_name&gt;</i> .
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 <i>&lt;old_contact_interval&gt;</i> to <i>&lt;new_contact_interval&gt;</i> 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 <i>&lt;infranet_controller_obj_name&gt;</i> (ip <i>&lt;infranet_controller_ip&gt;</i> ).
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 <i>&lt;outgoing_interface&gt;</i> 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( <i>&lt;infranet_controller_ip&gt;</i> ) in the past <i>&lt;seconds_for_which_no_keepalive&gt;</i> 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	Infranet Enforcer has stopped dropping IDP attack notifications. IDP attack notifications are being sent to the Infranet Controller.
Meaning	The frequency of detected attacks has dropped so that the Infranet Enforcer is able to send them all to the Infranet Controller.
Action	Check NSM logs for information about the attacks that were detected.
Message	IP address for Infranet Controller <i>&lt;infranet_controller_obj_name&gt;</i> changed from <i>&lt;old_ip&gt;</i> to <i>&lt;new_ip&gt;</i> .
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 <i>&lt;infranet_controller_obj_name&gt;</i> changed.
Meaning	An admin changed the password for the specified Infranet Controller.
Action	No recommended action.
Message	Port number for Infranet Controller <i>&lt;infranet_controller_obj_name&gt;</i> changed from <i>&lt;old_port&gt;</i> to <i>&lt;new_port&gt;</i> .
Meaning	An admin changed the port number for the Infranet Controller.
Action	No recommended action.
Message	Source interface for Infranet Controller <i>&lt;infranet_controller_obj_name&gt;</i> changed from <i>&lt;old_intf_name&gt;</i> to <i>&lt;new_intf_name&gt;</i> .
Meaning	An admin changed the source interface of the Infranet Controller.
Action	No recommended action.
Message	Switch global reject un-authentication action to <i>&lt;old_reject_action&gt;</i> .
Meaning	When reject un-auth action switch on, box will send back RST or ICMP dst unreachable packet to client.
Action	No recommended action.

Message	Timeout action for Infranet settings changed from <i>&lt;old_timeout_action&gt;</i> to <i>&lt;new_timeout_action&gt;</i> .
Meaning	An admin changed the specified action to take when a timeout occurs.
Action	No recommended action.
Message	Accounting port of server <i>&lt;auth_server_obj_name&gt;</i> is reset to default <i>&lt;acct_port&gt;</i> .
Meaning	The accounting port of the specified accounting server has been set to its default value.
Action	Confirm that the accounting port of the specified sever has been set.
Message	Accounting port of server <i>&lt;auth_server_obj_name&gt;</i> is set to <i>&lt;acct_port&gt;</i> .
Meaning	The accounting port of the specified accounting server has been modified.
Action	Confirm that the accounting port of the specified sever has been set.
Message	Admin user <i>&lt;user-name&gt;</i> attempted to verify the encrypted password <i>&lt;encr_pass&gt;</i> . Verification failed.
Meaning	The security device was unable to verify the password entered by the admin user.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> attempted to verify the encrypted password <i>&lt;encr_pass&gt;</i> . Verification was successful.
Meaning	The security device successfully verified the password entered by the admin user.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> account type is set to <i>&lt;acct_types&gt;</i> .
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 <i>&lt;auth_server_obj_name&gt;</i> authentication timeout is set to <i>&lt;auth_timeout&gt;</i> .
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 <i>&lt;auth_server_obj_name&gt;</i> backup1 name is unset.
Meaning	An admin unset the server name of the primary backup server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> backup1 server name is set to <i>&lt;backup1_name&gt;</i> .
Meaning	An admin modified the server name of the primary backup server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> backup2 name is unset.
Meaning	An admin unset the server name of the secondary backup server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> backup2 server name is set to <i>&lt;backup2_name&gt;</i> .
Meaning	An admin modified the server name of the secondary backup server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> fail-over revert interval is set to <i>&lt;revert_interval&gt;</i> seconds.
Meaning	The time interval between revert intervals is set for the specified auth server.
Action	No recommended action.

Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> id is set to <i>&lt;new_as_id&gt;</i> .
Meaning	An admin set the ID of the Auth server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> is created.
Meaning	An admin created or modified the specified authentication server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> is deleted.
Meaning	An admin removed the specified server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> is modified.
Meaning	An admin created or modified the specified authentication server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> LDAP cn is set to <i>&lt;ldap_cn&gt;</i> .
Meaning	An admin set the LDAP common name of the specified auth server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> LDAP dn is set to <i>&lt;ldap_dn&gt;</i> .
Meaning	An admin set the LDAP distinguished name of the specified auth server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> LDAP parameters are set to server name: <i>&lt;auth_server_name_ip&gt;</i> , port: <i>&lt;ldap_port&gt;</i> , dn: <i>&lt;ldap_dn&gt;</i> , cn: <i>&lt;ldap_cn&gt;</i> .
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 <i>&lt;auth_server_obj_name&gt;</i> SecurID auth port is set to <i>&lt;auth_port&gt;</i> .
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 <i>&lt;auth_server_obj_name&gt;</i> SecurID backup1 server name is set to <i>&lt;backup1_auth_server_name_ip&gt;</i> .
Meaning	An admin configured the primary backup server of the specified auth server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> SecurID client retries is set to <i>&lt;securid_client_retries&gt;</i> .
Meaning	An admin set the maximum number of retries that are sent to the SecurID server.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> SecurID server name is set to <i>&lt;auth_server_name_ip&gt;</i> .
Meaning	An admin configured the SecurID server name.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> SecurID timeout is set to <i>&lt;securid_client_timeout&gt;</i> .
Meaning	An admin set the timeout value of the specified SecurID server on the security device.
Action	No recommended action.
Message	Auth server <i>&lt;auth_server_obj_name&gt;</i> 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 <i>&lt;auth_server_obj_name&gt;</i> 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 <i>&lt;auth_server_obj_name&gt;</i> 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 <i>&lt;auth_server_obj_name&gt;</i> 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 <i>&lt;auth_server_obj_name&gt;</i> 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 <i>&lt;auth_server_obj_name&gt;</i> username character separator is set to <i>&lt;separator_char&gt;</i> ; number of occurrences of character separator is <i>&lt;num_occurrence&gt;</i> .
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 <i>&lt;auth_server_obj_name&gt;</i> .
Meaning	An admin configured the default authentication server.
Action	No recommended action.

Message	Forced timeout for Auth server <i>&lt;auth_server_obj_name&gt;</i> authentication is set to <i>&lt;auth_forced_timeout&gt;</i> 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 <i>&lt;auth_server_obj_name&gt;</i> is unset to its default value, <i>&lt;default_auth_timeout&gt;</i> 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 <i>&lt;infranet_controller_obj_name&gt;</i> changed from <i>&lt;old_host_name&gt;</i> to <i>&lt;new_host_name&gt;</i> .
Meaning	An admin changed the host name of the Infranet Controller to the specified value.
Action	No recommended action.
Message	Infranet Controller <i>&lt;infranet_controller_obj_name&gt;</i> is created.
Meaning	An admin created a new Infranet Controller profile.
Action	No recommended action.
Message	Infranet Controller <i>&lt;infranet_controller_obj_name&gt;</i> 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	TACACS auth server '<server>' port set to '<tacacs_port>'.
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.
Message	TACACS auth server '<server>' port set to default '<tacacs_default_port>'.
Meaning	The TCP port has been declared to be the default TCP port for the specified TACACS server.
Action	Confirm the declared TCP port on the specified TACACS server is the default TCP port.

Message	TACACS auth server ' <i>&lt;auth_server_obj_name&gt;</i> ' 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.
Message	TACACS auth server ' <i>&lt;auth_server_obj_name&gt;</i> ' shared secret modified.
Meaning	Shared secret has been declared for the specified TACACS server.
Action	Confirm the declared shared secret matches the shared secret declared on the specified TACACS server.
Message	Timeout for Infranet Controller <i>&lt;infranet_controller_obj_name&gt;</i> changed from <i>&lt;old_timeout&gt;</i> to <i>&lt;new_timeout&gt;</i> 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 <i>&lt;auth_server_obj_name&gt;</i> .
Meaning	An admin configured the specified WebAuth server.
Action	No recommended action.

### Notification (00525)

Message	The new PIN for user <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> is <i>&lt;accept_or_reject&gt;</i> by SecurID <i>&lt;auth_server_ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> has selected a system-generated PIN for authentication with SecurID <i>&lt;auth_server_ip&gt;</i> .
Meaning	The specified user has accepted the system-generated PIN for use with the SecurID server.
Action	No recommended action.
Message	User <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> must enter New PIN for SecurID <i>&lt;auth_server_ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> must enter Next Code for SecurID <i>&lt;auth_server_ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> must make a New PIN choice for SecurID <i>&lt;auth_server_ip&gt;</i> .
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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> through the <i>&lt;auth_server_obj_name&gt;</i> auth server) by policy id <i>&lt;policy-id&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> ) via the <i>&lt;auth_server_obj_name&gt;</i> auth server) by policy id <i>&lt;policy-id&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> ) by policy id <i>&lt;policy-id&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> ) by policy id <i>&lt;policy-id&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> ) through the <i>&lt;auth_server_obj_name&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> through the <i>&lt;auth_server_obj_name&gt;</i> 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 <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> ) is now over due to forced timeout.
---------	--

Message	Access for WebAuth firewall user <i>&lt;user-name&gt;</i> at <i>&lt;src-ip&gt;</i> (accepted at <i>&lt;time_connected_at&gt;</i> 2 for duration <i>&lt;duration_connected_for&gt;</i> ) 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 <i>&lt;user-name&gt;</i> at <i>&lt;of_group&gt;</i> is challenged by the <i>&lt;src-ip&gt;</i> server at <i>&lt;auth_server_type&gt;</i> .
Meaning	The specified server sent a challenge to the specified user.
Action	No recommended action.

### Notification (00767)

Message	Cannot get route to SecuriD server <i>&lt;server_ip&gt;</i> .
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 <i>&lt;secret_len&gt;</i> .
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 <i>&lt;radius_server_dictionary_version&gt;</i> does not match the version <i>&lt;ns_device_dictionary_version&gt;</i> 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 Web site and update the NetScreen dictionary file on the RADIUS server.

Message	User <i>&lt;user-name&gt;</i> 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 10

# Cisco-HDLC

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

### Alert (00087)

Message	Cisco-HDLC detected loop <i>&lt;times&gt;</i> times on interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;old_val&gt;</i> to <i>&lt;new_val&gt;</i> on interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;old_val&gt;</i> to <i>&lt;new_val&gt;</i> on interface <i>&lt;interface-name&gt;</i> .
Meaning	An admin changed the interval at which the specified interface sends keepalive packets.
Action	No recommended action.

Message	CISCO-HDLC keepalive is <i>&lt;enable&gt;</i> on interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;old_val&gt;</i> to <i>&lt;new_val&gt;</i> on interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> encap as cisco-hdlc.
Meaning	An admin configured Cisco HDLC encapsulation on the specified interface.
Action	No recommended action.

Message	Unset interface <i>&lt;interface-name&gt;</i> 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 <i>&lt;status&gt;</i> on interface <i>&lt;interface-name&gt;</i> .
Meaning	The protocol is up or down on the specified interface.
Action	No recommended action.

## CHAPTER 11

# 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.

### Notification (00560)

Message	NAS: <i>&lt;nas_obj_name&gt;</i> object <i>&lt;action_name&gt;</i> <i>&lt;update_initiator&gt;</i>
Meaning	Update NetScreen Application Security (NAS) configuration.
Action	No recommended action.



## CHAPTER 12

# 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 <i>&lt;interface-name&gt;</i> is full. Unable to <i>&lt;none&gt;</i> IP address to client at <i>&lt;mac&gt;</i> .
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 <i>&lt;interface-name&gt;</i> (another server found on <i>&lt;ip_address&gt;</i> ).
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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;none&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;none&gt;</i> .
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 <i>&lt;interface-name&gt;</i> as <i>&lt;admin-preference&gt;</i> .
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 <i>&lt;interface-name&gt;</i> from <i>&lt;admin-preference&gt;</i> .
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 <i>&lt;interface-name&gt;</i> are <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> .
Meaning	An admin enabled or disabled DHCP client auto-config.
Action	No recommended action.

Message	DHCP client client identifier is set to <i>&lt;client_id&gt;</i> .
Meaning	An admin set the DHCP client ID to the specified value.
Action	No recommended action.

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

Message	DHCP client lease time is set to <i>&lt;lease&gt;</i> 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 <i>&lt;ip_address&gt;</i> .
Meaning	An admin set the client server IP address to the specified value.
Action	No recommended action.
Message	DHCP client server-update is <i>&lt;none&gt;</i> .
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 <i>&lt;vendor_id&gt;</i> .
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 <i>&lt;interface-name&gt;</i> received DHCPDISCOVER from <i>&lt;mac&gt;</i> requesting out-of-scope IP address <i>&lt;ip_address&gt;/&lt;netmask&gt;</i> .
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 <i>&lt;ip_address&gt;</i> is assigned to <i>&lt;mac&gt;</i> .
Meaning	An admin assigned an IP address to an entity with the specified MAC address.
Action	No recommended action.
Message	IP address <i>&lt;ip_address&gt;</i> is released from <i>&lt;mac&gt;</i> .
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 <i>&lt;mac&gt;</i> has declined address <i>&lt;ip_address&gt;</i> .
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 <i>&lt;ip_address&gt;</i> .
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 <i>&lt;ip_address&gt;</i> for interface <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> .
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 <i>&lt;ip_address&gt;</i> 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 <i>&lt;interface-name&gt;</i> was offered IP <i>&lt;ip_address&gt;/&lt;netmask&gt;</i> and did not proceed with DHCPREQUEST. Reason -- <i>&lt;reason&gt;</i>
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 <i>&lt;ip_address&gt;</i> assigned interface <i>&lt;interface-name&gt;</i> with IP address <i>&lt;ip_address&gt;</i> (lease time <i>&lt;lease&gt;</i> 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 <i>&lt;filename&gt;</i> from TFTP server <i>&lt;ip_address&gt;</i> 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 <i>&lt;filename&gt;</i> from TFTP server <i>&lt;ip_address&gt;</i> is loaded successfully.
Meaning	The device successfully loaded the designated configuration file from the designated TFTP server.
Action	No recommended action.



## CHAPTER 13

# DHCP6

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

### Notification (00009)

Message	DHCP6 client is <i>&lt;none&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;none&gt;</i> .
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.

### 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 relay is <i>&lt;none&gt;</i> on <i>&lt;interface-name&gt;</i> <i>&lt;none&gt;</i> .
Meaning	This message appears when DHCP6 relay enables or disables the server-ip or option interface-id.
Action	No recommended action.

Message	DHCP6 server configured on <i>&lt;interface-name&gt;</i> is <i>&lt;none&gt;</i> .
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 <i>&lt;interface-name&gt;</i> are <i>&lt;none&gt;</i> .
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 <i>&lt;prefix-len&gt;</i> bits prefix with <i>&lt;sla-len&gt;</i> 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 <i>&lt;msgtype&gt;</i> from <i>&lt;src-ip&gt;</i> , xid <i>&lt;xid&gt;</i> .
Meaning	DHCP6 client received DHCP6 packet from the server.
Action	No recommended action.

Message	DHCP6: Client send <i>&lt;msgtype&gt;</i> from <i>&lt;interface-name&gt;</i> <i>&lt;src-ip&gt;</i> to <i>&lt;dst-ip&gt;</i> , xid <i>&lt;xid&gt;</i> len <i>&lt;length&gt;</i> .
Meaning	DHCP6 client sent a DHCP6 packet to the DHCP6 server.
Action	No recommended action.
Message	DHCP6: Client start at <i>&lt;interface-name&gt;</i> .
Meaning	The interface enabled DHCP6 client.
Action	No recommended action.
Message	DHCP6: Server received <i>&lt;msgtype&gt;</i> from <i>&lt;src-ip&gt;</i> , xid <i>&lt;xid&gt;</i> .
Meaning	DHCP6 server received DHCP6 packet from the client.
Action	No recommended action.
Message	DHCP6: Server received <i>&lt;msgtype&gt;</i> from <i>&lt;src-ip&gt;</i> .
Meaning	DHCP6 server received DHCP6 packet from the relay.
Action	No recommended action.
Message	DHCP6: Server send <i>&lt;msgtype&gt;</i> from <i>&lt;interface-name&gt;</i> <i>&lt;src-ip&gt;</i> to <i>&lt;dst-ip&gt;</i> , xid <i>&lt;xid&gt;</i> len <i>&lt;length&gt;</i> .
Meaning	DHCP6 server sent a DHCP6 packet to the DHCP6 client.
Action	No recommended action.
Message	DHCP6: Server send <i>&lt;msgtype&gt;</i> from <i>&lt;interface-name&gt;</i> <i>&lt;src-ip&gt;</i> to <i>&lt;dst-ip&gt;</i> , xid <i>&lt;xid&gt;</i> len <i>&lt;length&gt;</i> .
Meaning	DHCP6 server sent a DHCP6 packet to the DHCP6 client.
Action	No recommended action.



## CHAPTER 14

# DIP, VIP, MIP, and Zones

The following messages 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 <i>&lt;server_IP&gt;</i> cannot be contacted.
Meaning	The specified Virtual IP (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 <i>&lt;dip_id&gt;</i> in vsys <i>&lt;vsys_name&gt;</i> hits raise threshold <i>&lt;threshold&gt;</i> .
Meaning	The device utilized the specified DIP pool in over the specified raise threshold. The device triggers an 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 <i>&lt;dip_id&gt;</i> in vsys <i>&lt;vsys_name&gt;</i> hits clear threshold <i>&lt;threshold&gt;</i> .
Meaning	The device utilized the specified DIP pool in over the specified clear threshold. The device triggers an SNMP trap when DIP utilization goes down across this configured threshold.
Action	No recommended action.

### Notification (00010)

Message	Mapped IP <i>&lt;is_ipv6&gt;-&lt;MIP_mapped_IP&gt; &lt;is_ipv6&gt; &lt;MIP_host_IP&gt;</i>
Meaning	An admin has added, modified, or deleted the specified mapped IP address.
Action	No recommended action.

### Notification (00016)

Message	VIP <i>&lt;(&lt;VIP_IP_Address&gt;:&lt;VIP_Port&gt; &lt;VIP_Service&gt; &lt;VIP_Host_Port&gt;) &lt;action&gt; &lt;changed_from&gt;</i>
Meaning	An admin has added, modified, or deleted the specified Virtual IP (VIP).
Action	No recommended action.

Message	VIP <i>&lt;(&lt;VIP_IP_Address&gt;:&lt;Vport_low&gt;-&lt;Vport_high&gt; &lt;Host_ip&gt;:&lt;Hport_low&gt;-&lt;Hport_high&gt;) &lt;protocol&gt; &lt;action&gt; &lt;changed_from&gt;</i>
Meaning	An admin has added, modified, or deleted a specified Virtual IP (VIP).
Action	No recommended action.

Message	VIP multi-port was disabled <i>&lt;changed_from&gt;</i>
Meaning	An admin enabled multi-port mapping from a multi-port service to a Virtual IP (VIP).
Action	No recommended action.

Message	VIP multi-port was enabled <i>&lt;changed_from&gt;</i>
Meaning	An admin enabled multi-port mapping from a multi-port service to a Virtual IP (VIP).
Action	No recommended action.

### Notification (00021)

Message	DIP group <i>&lt;DIP_group_id&gt;</i> was created <i>&lt;changed_from&gt;</i>
Meaning	An admin deleted a DIP group ( <i>&lt;id_num&gt;</i> ).
Action	No recommended action.

Message	DIP group <i>&lt;DIP_group_id&gt;</i> was removed <i>&lt;changed_from&gt;</i>
Meaning	An admin deleted a DIP group ( <i>&lt;id_num&gt;</i> ).
Action	No recommended action.
Message	DIP IP pool <i>&lt;DIP_member_id&gt;</i> was removed from DIP group <i>&lt;DIP_group_id&gt;</i> <i>&lt;changed_from&gt;</i>
Meaning	An admin has added, modified, or deleted the specified VIP.
Action	No recommended action.
Message	DIP IP pool <i>&lt;is_ipv6&gt;</i> - <i>&lt;DIP_min_range&gt;</i> (scale-size= <i>&lt;is_ipv6&gt;</i> ) <i>&lt;DIP_max_range&gt;</i> <i>&lt;dip_scale_size&gt;</i>
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 IP range <i>&lt;DIP_min_range&gt;</i> - <i>&lt;DIP_max_range&gt;</i> was added into DIP pool <i>&lt;DIP_pool_id&gt;</i> <i>&lt;changed_from&gt;</i>
Meaning	An admin added an IP range to the DIP pool.
Action	No recommended action.
Message	DIP IP range <i>&lt;DIP_min_range&gt;</i> - <i>&lt;DIP_max_range&gt;</i> was removed from DIP pool <i>&lt;DIP_pool_id&gt;</i> <i>&lt;changed_from&gt;</i>
Meaning	An admin removed an IP range from the DIP pool.
Action	No recommended action.
Message	DIP pool <i>&lt;DIP_member_id&gt;</i> was added into DIP group <i>&lt;DIP_group_id&gt;</i> <i>&lt;changed_from&gt;</i>
Meaning	An admin added a DIP pool ( <i>&lt;id_num1&gt;</i> ) to a DIP group ( <i>&lt;id_num2&gt;</i> ).
Action	No recommended action.

Message	DIP port-translation stickiness was <i>&lt;new_state&gt;</i> <i>&lt;changed_from&gt;</i>
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 <i>&lt;enabled_disabled&gt;</i> on zone <i>&lt;zone_name&gt;</i> .
Meaning	An administrator enabled or disabled the asymmetric VPN option for the specified zone. When this option is enabled, the device matches the incoming packets to their proper sessions regardless of the tunnels through which the packets pass.
Action	No recommended action.

Message	Intra-zone block for zone <i>&lt;zone_name&gt;</i> was set to <i>&lt;string_on_off&gt;</i>
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 <i>&lt;enabled_disabled&gt;</i> on zone <i>&lt;zone_name&gt;</i> .
Meaning	Layer-3 IP or Layer-4 TCP packet reassembly has been enabled or disabled for the specified zone.
Action	No recommended action.

Message	New zone <i>&lt;zone_name&gt;</i> (ID <i>&lt;zone_id&gt;</i> , vsys <i>&lt;vsys_name&gt;</i> ) was created.
Meaning	An administrator successfully created a new zone with the indicated ID number.
Action	No recommended action.

Message	Shared-DMZ zone <i>&lt;zone_name&gt;</i> was created.
Meaning	An administrator successfully created a new shared-DMZ zone.
Action	No recommended action.
Message	Shared-DMZ zone <i>&lt;zone_name&gt;</i> was deleted.
Meaning	An administrator successfully deleted the shared-DMZ zone.
Action	No recommended action.
Message	Tunnel zone <i>&lt;tzone_name&gt;</i> was bound to out zone <i>&lt;czzone_name&gt;</i>
Meaning	An administrator successfully bound a specified tunnel zone to a specified outbound zone.
Action	No recommended action.
Message	Zone <i>&lt;zone_name&gt;</i> (ID <i>&lt;zone_id&gt;</i> , vsys <i>&lt;vsys_name&gt;</i> ) was deleted.
Meaning	An administrator successfully deleted the specified zone.
Action	No recommended action.
Message	Zone <i>&lt;zone_name&gt;</i> was bound to virtual router <i>&lt;vr_name&gt;</i>
Meaning	An administrator successfully bound a specified zone to a specified virtual router.
Action	No recommended action.
Message	Zone <i>&lt;zone_name&gt;</i> 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 <i>&lt;zone_name&gt;</i> 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 <i>&lt;zone_name&gt;</i> was unbound from virtual router <i>&lt;vr_name&gt;</i>
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 <i>&lt;server_IP&gt;</i> is now alive.
Meaning	The Virtual IP server has been brought up and is operational.
Action	No recommended action.

Message	VIP server <i>&lt;server_IP&gt;</i> is now in manual mode.
Meaning	An admin disabled server auto-detection.
Action	No recommended action.

## CHAPTER 15

# 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 (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 <i>&lt;arg1&gt;</i> : <i>&lt;arg2&gt;</i> with an interval of <i>&lt;arg3&gt;</i> 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 <i>&lt;none&gt;</i> , interf <i>&lt;none&gt;</i> , ip <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> .
Meaning	An admin deleted an entry in the DNS Proxy server select table.
Action	No recommended action.
Message	DNS Proxy server select table entries exceeded max limit.
Meaning	There are more retries in the DNS Proxy server select table than are allowed.
Action	No recommended action.
Message	<i>&lt;none&gt;</i> logging DNS access request.
Meaning	Enable or disable DNS access request log.
Action	No recommended action.
Message	The { primary   secondary   tertiary } DNS server IP address has been changed.
Meaning	An admin has changed the IP address of the primary, secondary, or tertiary DNS server.
Action	No recommended action.

Message	The { primary   secondary   tertiary } DNS server IP address has been changed.
---------	--

Meaning	An admin has changed the IP address of the primary, secondary, or tertiary DNS server.
---------	--

Action	No recommended action.
--------	------------------------

Message	The { primary   secondary   tertiary } DNS server IP address has been changed.
---------	--

Meaning	An administrator has changed the IP address of the primary, secondary, or tertiary 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 <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> is configured with interface <i>&lt;none&gt;</i> host-name <i>&lt;none&gt;</i> .
Meaning	An admin (or some other entity) added a DDNS entry to the DDNS table, where: <i>&lt;id_num&gt;</i> the identification number for the entry <i>&lt;interface&gt;</i> the interface of the server in the entry <i>&lt;name_str&gt;</i> the host name of the interface
Action	No recommended action
Message	DDNS entry with id <i>&lt;none&gt;</i> is configured with server type <i>&lt;none&gt;</i> name <i>&lt;none&gt;</i> refresh-interval <i>&lt;none&gt;</i> hours minimum update interval <i>&lt;none&gt;</i> minutes with <i>&lt;none&gt;</i> secure connection.
Meaning	An admin (or some other entity) added a DDNS entry to the DDNS table, where: <i>&lt;id_num&gt;</i> the identification number for the entry <i>&lt;string1&gt;</i> the type of DDNS server (ddo or dyndns) <i>&lt;name_str&gt;</i> the name of the DDNS server <i>&lt;number1&gt;</i> the refresh interval for the new entry (expressed in hours) <i>&lt;number2&gt;</i> the minimum update interval for the new entry (expressed in minutes)
Action	No recommended action
Message	DDNS entry with id <i>&lt;none&gt;</i> is configured with user name <i>&lt;none&gt;</i> agent <i>&lt;none&gt;</i> .
Meaning	An admin (or some other entity) added a DDNS entry to the DDNS table.
Action	No recommended action
Message	DDNS entry with id <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> returned incorrect ip <i>&lt;none&gt;</i> , local-ip should be <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> user <i>&lt;none&gt;</i> domain <i>&lt;none&gt;</i> , server type <i>&lt;none&gt;</i> name <i>&lt;none&gt;</i> .
Meaning	<i>&lt;id_num&gt;</i> the identification number for the entry <i>&lt;name_str1&gt;</i> the user name for the entry <i>&lt;dom_name&gt;</i> the domain name for the entry <i>&lt;name_str2&gt;</i> the name of the DDNS server
Action	No recommended action
Message	Hostname of DDNS entry with id <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> user <i>&lt;none&gt;</i> domain <i>&lt;none&gt;</i> server type <i>&lt;none&gt;</i> , server name <i>&lt;none&gt;</i> .
Meaning	An admin (or some other entity) successfully updated a DDNS entry to the DDNS table, where: <i>&lt;id_num&gt;</i> the identification number for the entry <i>&lt;name_str1&gt;</i> the user name for the entry <i>&lt;dom_name&gt;</i> the domain name for the entry
Action	No recommended action
Message	Refresh interval of DDNS entry with id <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> user <i>&lt;none&gt;</i> domain <i>&lt;none&gt;</i> server type <i>&lt;none&gt;</i> name <i>&lt;none&gt;</i> .
Meaning	The DDNS server has been successfully updated.
Action	No recommended action.

Message	Updates for DDNS entry with id <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> 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 <i>&lt;none&gt;</i> is cleared.
Meaning	An admin (or some other entity) reset the specified server for the entry in the DDNS table.
Action	No recommended action

Message	Service type of DDNS entry with id <i>&lt;none&gt;</i> is set to default value (dyndns).
---------	--

### 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.

### Information (00529)

Message	DNS request <i>&lt;none&gt;</i> from <i>&lt;none&gt;/&lt;none&gt;</i> is forwarded to server <i>&lt;none&gt;/&lt;none&gt;</i>
Meaning	A DNS request is forwarded to the back-end DNS server by DNS proxy.
Action	No recommended action.



## CHAPTER 16

# 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.

### Alert (00027)

Message	License key <i>&lt;key-name&gt;</i> 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 <i>&lt;key-name&gt;</i> has expired.
Meaning	The specified license key expired, and is no longer valid.
Action	Renew the subscriptions key for your device.
Message	License key <i>&lt;key-name&gt;</i> 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 <i>&lt;key-name&gt;</i> 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 *<retrieval-from>*. Server url: *<url>*.

Meaning A network administrator unsuccessfully attempted to register the device from the specified server.

Action Make sure that the device can connect to internet and that the url is correct.

Message Request to retrieve license key failed to reach the server by *<retrieval-from>*. Server url: *<url>*

Meaning A network administrator unsuccessfully attempted to download a license key from the specified server.

Action Make sure that the device can connect to internet and that the url is correct.

## Critical (00027)

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 <i>&lt;number&gt;</i> , which is <i>&lt;percent&gt;</i> 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 <i>&lt;number&gt;</i> , which is <i>&lt;percent&gt;</i> 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 (00850)**

Message	Session limit alarm has been cleared for vsys <i>&lt;vsys-name&gt;</i> (current <i>&lt;current-sess&gt;</i> , dropped packets <i>&lt;drop-sess&gt;</i> )
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 <i>&lt;vsys-name&gt;</i> (current <i>&lt;current-sess&gt;</i> , alarm threshold <i>&lt;alarm-sess&gt;</i> ).
Meaning	An admin has changed the session limit alarm for the specified vsys to the specified value.
Action	No recommended action.

**Critical (00851)**

Message	Session limit alarm has been cleared for policy <i>&lt;policy-id&gt;</i> from src-ip <i>&lt;none&gt;</i> , current session count ( <i>&lt;src-ip&gt;</i> ) falls into the alarm threshold ( <i>&lt;session-count&gt;</i> ).
Meaning	The session count from the specified source IP for the specified policy drops below the alarm threshold.
Action	No recommended action.

Message	Session limit alarm has been set for policy <i>&lt;policy-id&gt;</i> from src-ip <i>&lt;none&gt;</i> , current session count ( <i>&lt;src-ip&gt;</i> ) exceeds the alarm threshold ( <i>&lt;session-count&gt;</i> ), <i>&lt;threshold&gt;</i> .
Meaning	The session count from the specified source IP for the specified policy exceeds the alarm threshold.
Action	Clear inactive sessions of the specified policy.

### Notification (00002)

Message	Session threshold has been changed to percentage <i>&lt;percent&gt;</i> <i>&lt;user-name&gt;</i>
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 <i>&lt;name&gt;</i> .
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 <i>&lt;name&gt;</i> .
Meaning	A network administrator changed the existing hostname for the device.
Action	No recommended action.

### Notification (00018)

Message	In policy <i>&lt;policy-id&gt;</i> , the session limit per source IP is set to <i>&lt;threshold&gt;</i> <i>&lt;user-name&gt;</i> .
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.

### 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 <i>&lt;retrieval-from&gt;</i> .
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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> . (Note: You must be a registered Juniper Networks customer.)
Message	Received identical license key by <i>&lt;retrieval-from&gt;</i> .
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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> . (Note: You must be a registered Juniper Networks customer.)
Message	Retrieve firmware list succeeded: <i>&lt;firmware-count&gt;</i> firmware.
Meaning	The WebUI successfully retrieved the list of available firmware.
Action	No recommended action.
Message	Retrieve firmware list succeeded: <i>&lt;firmware-count&gt;</i> firmware.
Meaning	The WebUI successfully retrieved the list of available firmware.
Action	No recommended action.

Message	<i>&lt;key-count&gt;</i> license keys were updated successfully by <i>&lt;retrieval-from&gt;</i> .
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 <i>&lt;ipv6&gt;</i> 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 (00553)

Message	Invalid configuration size ( <i>&lt;config-size-limit&gt;</i> ).
Meaning	An admin entered an invalid value for the configuration size limit.
Action	Enter a valid size limit value.

#### Notification (00625)

Message	Session (id <i>&lt;session-id&gt;</i> src-ip <i>&lt;state&gt;</i> dst-ip <i>&lt;src-ip&gt;</i> dst port <i>&lt;state&gt;</i> ) route is invalid.
Meaning	The session route is invalid.
Action	No recommended action.
Message	Session (id <i>&lt;session-id&gt;</i> src-ip <i>&lt;state&gt;</i> dst-ip <i>&lt;src-ip&gt;</i> dst port <i>&lt;state&gt;</i> ) route is valid.
Meaning	The session route is valid.
Action	No recommended action.

#### Notification (00767)

Message	notification packets for <i>&lt;missed-notify-cnt&gt;</i> sessions are not sent.
Meaning	Missed notification packets to sessions.
Action	No recommended action.

Message CPU-protection throttling mode engaged *<cpu-prot-throttling-times>* times in *<cpu-prot-throttling-interval>* seconds.

Meaning The CPU-protection throttling mode engaged frequently.

Action Please check whether the box is under attack and use blacklists to screen attacking packets.

Message Fcb pool size is *<fcb-pool-size>*.

Meaning Current IP packet Fragment Control Block (FCB) pool size is shown.

Action No recommended action.

Message Fcb pool size is erroneous, change to default size *<fcb-pool-size>*.

Meaning Environment variable is erroneous; change IP packet Fragment Control Block (FCB) pool size to default size.

Action No recommended action.

Message Session (id *<session-id>*, *<sess\_src\_dst\_proto>*) cleared: *<sess\_clr\_cmd\_issuer>*

Meaning The specified session was cleared.

Action No recommended action.

Message Set cpu-protection blacklist: *<cpu-prot-blacklist-str>*.

Meaning Add a new blacklist on the device.

Action No recommended action.

Message Set cpu-protection threshold *<cpu-prot-threshold>*.

Meaning Set the cpu protection threshold.

Action No recommended action.

Message	Trial keys are available to download to enable advanced features. To find out, please visit <a href="http://www.juniper.net/products/subscription/trial/">http://www.juniper.net/products/subscription/trial/</a> .
---------	---

Meaning	Trial keys are now available.
---------	-------------------------------

Action	Visit the URL <url_str> specified in the message.
--------	---

Message	<session-count> sessions in <vsys-name> were cleared due to <cmd> issued by <user-name>
---------	---

Meaning	The matched sessions were cleared.
---------	------------------------------------

Action	No recommended action.
--------	------------------------

Message	Unset all blacklist.
---------	----------------------

Meaning	All blacklist entries have been unset.
---------	--

Action	No recommended action.
--------	------------------------

Message	Unset cpu-protection blacklist <cpu-prot-blacklist-id>.
---------	---

Meaning	Delete a blacklist on the device.
---------	-----------------------------------

Action	No recommended action.
--------	------------------------

## Information (00767)

Message	All system configurations saved to <config-changer> by <user-name>.
---------	---

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	Environment variable <variable-name> changed to <variable-value>.
---------	---

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 <i>&lt;variable-name&gt;</i> set to <i>&lt;variable-value&gt;</i> .
Meaning	A network administrator changed an environment variable to a new name.
Action	No recommended action.
Message	Environment variable <i>&lt;variable-name&gt;</i> unset.
Meaning	A network administrator unset an environment variable.
Action	No recommended action.
Message	Load file from usb <i>&lt;usb-filename&gt;</i> to flash <i>&lt;flash-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;string&gt;</i> loaded the file <i>&lt;filename&gt;</i> from the USB storage device to the flash memory.
Action	No recommended action.
Message	Lock configuration aborted because <i>&lt;timeout&gt;</i> 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 <i>&lt;task-name&gt;</i> .
Meaning	The lockout was aborted either by an admin via the CLI or by Network and Security Manager (NSM).
Action	No recommended action.
Message	Lock configuration ended by task <i>&lt;task-name&gt;</i> .
Meaning	The configuration file is no longer locked.
Action	No recommended action.

Message	Lock configuration started by task <i>&lt;task-name&gt;</i> , with a timeout value of <i>&lt;timeout&gt;</i> minute(s).
Meaning	The configuration file was locked either by an admin via the CLI or by the Network and 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	Save configuration to IP address <i>&lt;dst-ip&gt;</i> under filename <i>&lt;file-name&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The network administrator saved the device configuration to the specified IP address and filename.
Action	No recommended action.
Message	Save new patch from <i>&lt;src-ip&gt;</i> under filename <i>&lt;file-name&gt;</i> to flash memory <i>&lt;user-name&gt;</i> .
Meaning	The network administrator saved the hot patch to the specified file and IP address.
Action	No recommended action.
Message	Save new software from <i>&lt;src-ip&gt;</i> under filename <i>&lt;file-name&gt;</i> to flash memory <i>&lt;user-name&gt;</i> .
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 <i>&lt;slot-filename&gt;</i> to flash memory <i>&lt;user-name&gt;</i> .
Meaning	The specified admin copied a ScreenOS image from a file ( <i>&lt;filename&gt;</i> ) on a memory card to flash memory.
Action	No recommended action.

Message	Save new software from usb filename <i>&lt;usb-filename&gt;</i> to flash memory by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;string&gt;</i> saved the system image <i>&lt;filename&gt;</i> from the USB storage device to flash memory.
Action	No recommended action.
Message	Send file <i>&lt;flash-filename&gt;</i> from flash to usb <i>&lt;usb-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;string&gt;</i> saved the file <i>&lt;filename&gt;</i> from the flash memory to the USB storage device.
Action	No recommended action.
Message	Send new software from flash memory to slot filename <i>&lt;slot-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The specified admin copied a ScreenOS image from flash memory to a file ( <i>&lt;filename&gt;</i> ) on a memory card
Action	No recommended action.
Message	Send new software from flash memory to usb filename <i>&lt;usb-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;admin&gt;</i> saved the system image <i>&lt;filename&gt;</i> from the flash memory to the USB storage device.
Action	No recommended action.
Message	Send new software from IP address <i>&lt;src-ip&gt;</i> under filename <i>&lt;file-name&gt;</i> to slot <i>&lt;slot-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
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 <i>&lt;src-ip&gt;</i> under filename <i>&lt;file-name&gt;</i> to usb <i>&lt;usb-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;admin&gt;</i> saved the system configuration file <i>&lt;filename&gt;</i> from the TFTP server to the USB storage device.
Action	No recommended action.
Message	Send new software to IP address <i>&lt;dst-ip&gt;</i> under filename <i>&lt;file-name&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The named network administrator saved the software to the specified file and IP address.
Action	No recommended action.
Message	System configuration saved <i>&lt;config-changer&gt;</i> by <i>&lt;user-name&gt;</i> .
Meaning	A network administrator saved the system configuration file.
Action	No recommended action.
Message	The system configuration was loaded from flash memory to <i>&lt;usb-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;string&gt;</i> saved the system configuration file <i>&lt;filename&gt;</i> from flash memory to the USB storage device.
Action	No recommended action.
Message	The system configuration was loaded from flash memory to slot <i>&lt;slot-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The named network administrator loaded a configuration file from flash memory to a file ( <i>&lt;filename&gt;</i> ) on a memory card.
Action	No recommended action.

Message	The system configuration was loaded from <i>&lt;src-ip&gt;</i> under the filename <i>&lt;file-name&gt;</i> to slot <i>&lt;slot-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
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 <i>&lt;src-ip&gt;</i> under the filename <i>&lt;file-name&gt;</i> to usb <i>&lt;usb-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;admin&gt;</i> loaded the system configuration file <i>&lt;filename&gt;</i> from the TFTP server to the USB storage device.
Action	No recommended action.
Message	The system configuration was loaded from IP address <i>&lt;src-ip&gt;</i> under filename <i>&lt;file-name&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
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 <i>&lt;user-name&gt;</i> .
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 <i>&lt;usb-filename&gt;</i> by administrator <i>&lt;user-name&gt;</i> .
Meaning	The administrator <i>&lt;string&gt;</i> loaded the system configuration file <i>&lt;filename&gt;</i> from the USB storage device.
Action	No recommended action.

Message	The system configuration was not saved <i>&lt;config-changer&gt;</i> by administrator <i>&lt;user-name&gt;</i> . It was locked by administrator <i>&lt;task-name&gt;</i> .
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.

## CHAPTER 17

# 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 <i>&lt;utilization&gt;</i> $\geq$ threshold <i>&lt;threshold&gt;</i> .
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 (00026)

Message	Encryption failure exceed the threshold <i>&lt;threshold&gt;</i>
Meaning	The encryption failed due to a certain time period being exceeded.
Action	No recommended action.
Message	Decryption failure exceed the threshold <i>&lt;threshold&gt;</i>
Meaning	The decryption failed due to a certain time period being exceeded.
Action	No recommended action.

Message	Failed to perform decryption with tunnel ID <i>&lt;tunnel-id&gt;</i> 's symmetric key
Meaning	The packet is dropped because it cannot be decrypted.

Action	No recommended action.
--------	------------------------

Message	Failed to perform encryption tunnel ID <i>&lt;tunnel-id&gt;</i> 's symmetric key
Meaning	The packet is dropped because it cannot be encrypted.

Action	No recommended action.
--------	------------------------

Message	IPSEC tunnel with ID <i>&lt;tunnel-id&gt;</i> fails to authenticate the packet.
Meaning	The incoming packet from ipsec tunnel is dropped because it cannot pass the authentication.

Action	No recommended action.
--------	------------------------

#### 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 <i>&lt;utilization&gt;</i> < threshold <i>&lt;threshold&gt;</i> .
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.
--------	---

**Critical (00805)**

Message	Potential violation destination table fills up <i>&lt;counter&gt;</i> times in <i>&lt;period&gt;</i> seconds.
Meaning	An attempt to access a restricted resource is prohibited by the policy. The recording table is full.
Action	No recommended action.

Message	Potential violation service table fills up <i>&lt;counter&gt;</i> times in <i>&lt;period&gt;</i> seconds.
Meaning	An attempt to access a restricted resource is prohibited by the policy. The recording table is full.
Action	No recommended action.

Message	Potential violation source table fills up <i>&lt;counter&gt;</i> times in <i>&lt;period&gt;</i> seconds.
Meaning	An attempt to access a restricted resource is prohibited by the policy, but the recording table is full.
Action	No recommended action.

**Critical (00806)**

Message	Session cache miss rate for vsys <i>&lt;vsys-name&gt;</i> is over 90 <i>&lt;number&gt;</i> or an hour.
Meaning	Session cache miss rate is too high. It may degrade the performance of the system.
Action	No recommended action.

**Error (00805)**

Message	Potential violation from <i>&lt;src-ip&gt;</i> occurred <i>&lt;counter&gt;</i> times (exceeded threshold <i>&lt;threshold&gt;</i> ) in <i>&lt;period&gt;</i> seconds.
Meaning	An attempt to access a restricted resource is prohibited by the policy.
Action	No recommended action.

Message	Potential violation to <i>&lt;dst-ip&gt;</i> occurred <i>&lt;counter&gt;</i> times (exceeded threshold <i>&lt;threshold&gt;</i> ) in <i>&lt;period&gt;</i> seconds.
Meaning	An attempt to access a restricted resource is prohibited by the policy.
Action	No recommended action.
Message	Potential violation with policy group <i>&lt;name&gt;</i> occurred <i>&lt;counter&gt;</i> times (exceeded threshold <i>&lt;threshold&gt;</i> ) in <i>&lt;period&gt;</i> seconds.
Meaning	An attempt to access a restricted resource is prohibited by the policy.
Action	No recommended action.
Message	Potential violation with protocol <i>&lt;protocol&gt;</i> to destination port <i>&lt;dst-port&gt;</i> occurred <i>&lt;counter&gt;</i> times (exceeded threshold <i>&lt;threshold&gt;</i> ) in <i>&lt;period&gt;</i> seconds.
Meaning	An attempt to access a restricted resource is prohibited by the policy.
Action	No recommended action.

#### Notification (00002)

Message	<i>&lt;(user-name)/(vsys-name)&gt;</i> assign vlan group <i>&lt;vlan-grp&gt;</i> to vsd id <i>&lt;vsd-id&gt;</i> .
Meaning	VLAN log information.
Action	No recommended action.
Message	<i>&lt;(user-name)/(vsys-name)&gt;</i> <i>&lt;(none)&gt;</i> vlan group name <i>&lt;vlan-grp&gt;</i> .
Meaning	VLAN log information.
Action	No recommended action.
Message	<i>&lt;(user-name)/(vsys-name)&gt;</i> <i>&lt;(none)&gt;</i> vlan group <i>&lt;vlan-grp&gt;</i> <i>&lt;(none)&gt;</i> <i>&lt;(none)&gt;</i> .
Meaning	VLAN log information.
Action	No recommended action.

Message `((user-name)/(vsys-name)) (none) vlan import (none) (none).`

Meaning VLAN log information.

Action No recommended action.

Message `((user-name)/(vsys-name)) (none) vlan retag name (vlan-retag).`

Meaning VLAN log information.

Action No recommended action.

Message `((user-name)/(vsys-name)) set vlan port (interface-name) group (vlan-grp) zone (zone-name).`

Meaning VLAN log information.

Action No recommended action.

Message `((user-name)/(vsys-name)) unassign vlan group (vlan-grp) from vsd id (vsd-id).`

Meaning VLAN log information.

Action No recommended action.

Message `((user-name)/(vsys-name)) unset vlan port (interface-name) group (vlan-grp).`

Meaning VLAN log information.

Action No recommended action.

Message Naked TCP RST is `(none)` to pass through firewall.

Meaning The configuration to allow naked TCP reset pass through is changed.

Action No recommended action.

Message	Strict TCP SYN check is <i>&lt;none&gt;</i> .
Meaning	The configuration of strict TCP SYN check is changed.
Action	No recommended action.

Message	Transparent virtual wire mode has been <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <code>set flow aging early-ageout</code> .
Message	High watermark for early aging has been changed from <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <code>set flow aging high-watermark</code> .

Message	High watermark for early aging has been changed to the default ( <i>none</i> ).
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 <code>set flow aging early-ageout</code> .
Message	Low watermark for early aging has been changed from <i>none</i> to <i>none</i> .
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 <code>set flow aging high-watermark</code> .
Message	Low watermark for early aging has been changed to the default ( <i>none</i> ).
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 <code>set flow aging { high-watermark   low-watermark }</code> .

Message	The aggressive age-out value has been changed to the default ( <i>&lt;none&gt;</i> ).
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 <code>set flow aging early-ageout</code> .

### Notification (00079)

Message	CPU limit <i>&lt;none&gt;</i> .
Meaning	The CPU utilization limit is as stated.
Action	Verify that this configuration is desired.
Message	Desired fair mode changed from <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <i>&lt;threshold&gt;</i> to <i>&lt;threshold&gt;</i> .
Meaning	The shared to fair threshold has been changed to a new value.
Action	Verify that this configuration is desired.

### Notification (00085)

Message	Flow <i>&lt;none&gt;</i> reverse-route changed from <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <i>&lt;src-ip&gt;</i> , Destination IP <i>&lt;dst-ip&gt;</i> , Policy ID <i>&lt;policy-id&gt;</i> .
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 <i>&lt;src-ip&gt;</i> , Destination IP <i>&lt;dst-ip&gt;</i> , Policy ID <i>&lt;policy-id&gt;</i> .
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 <i>&lt;src-ip&gt;</i> , Destination IP <i>&lt;dst-ip&gt;</i> , Policy ID <i>&lt;policy-id&gt;</i> .
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 <i>&lt;src-ip&gt;</i> , Destination IP <i>&lt;dst-ip&gt;</i> , Policy ID <i>&lt;policy-id&gt;</i> .
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: Allow packet. In Regular mode, would respond RST packet on Infranet authentication policy because Infranet auth table reject it. Source IP <i>&lt;src-ip&gt;</i> , Destination IP <i>&lt;dst-ip&gt;</i> , Policy ID <i>&lt;policy-id&gt;</i> .
Meaning	This is a Test mode message. In regular mode, the packet would have been responded by RST packet the Infranet authentication policy because the auth table match reject it. 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 <i>&lt;src-ip&gt;</i> , Destination IP <i>&lt;dst-ip&gt;</i> , Policy ID <i>&lt;policy-id&gt;</i> .
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 <i>&lt;none&gt;</i> .
Meaning	IP attacks have been detected for which you have configured IP blocking.
Action	No recommended action.

### Notification (00624)

Message	Fail to reassemble packet fragments for <i>&lt;src-ip&gt;-&gt;&lt;dst-ip&gt;</i> id:0x <i>&lt;none&gt;</i> due to <i>&lt;none&gt;</i> .
Meaning	Indicates fragment abnormality occurred during IP reassembly.
Action	No recommended action.

Message	Fail to reassemble packet fragments for <i>&lt;src-ip&gt;-&gt;&lt;dst-ip&gt;</i> id:0x <i>&lt;none&gt;</i> due to <i>&lt;none&gt;</i> .
Meaning	Indicates fragment abnormality occurred during IPv6 reassembly.
Action	No recommended action.

### Notification (00767)

Message	snoop has been turned off <i>&lt;none&gt;</i> .
Meaning	An admin has disabled the snoop.
Action	No recommended action.

Message	snoop has been turned on <i>&lt;none&gt;</i> .
Meaning	An admin has enabled the snoop.
Action	No recommended action.



## CHAPTER 18

# Frame Relay

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

### Alert (00085)

Message	[mlfr/lip]: <i>&lt;interface-name&gt;</i> detected loop <i>&lt;times&gt;</i> times.
Meaning	A link loopback was detected for the indicated number of times.
Action	No recommended action.
Message	[mlfr/lip]: the bid <i>&lt;lrxbid&gt;</i> in the ADD_LINK packet from link <i>&lt;interface-name&gt;</i> is inconsistent with the received bid <i>&lt;brxbid&gt;</i> on the bundle <i>&lt;interface-name&gt;</i> .
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]: <i>&lt;interface-name&gt;</i> LMI: set <i>&lt;param_name&gt;</i> to <i>&lt;value&gt;</i> .
Meaning	An admin configured the indicated LMI parameter.
Action	No recommended action.
Message	[fr/cfg]: <i>&lt;interface-name&gt;</i> LMI: set to <i>&lt;proc&gt;</i> .
Meaning	An admin enabled or disabled LMI on the interface.
Action	No recommended action.

Message	[fr/cfg]: <i>&lt;interface-name&gt;</i> : <i>&lt;config&gt;</i>
Meaning	The specified interface is configured for DTE or DCE operation.

Action	No recommended action.
--------	------------------------

Message	[fr/cfg]: <i>&lt;interface-name&gt;</i> : <i>&lt;config&gt;</i>
Meaning	An admin configured the DLCI for the interface.

Action	No recommended action.
--------	------------------------

### Notification (00075)

Message	[mlfr/cfg]: add link <i>&lt;interface-name&gt;</i> to bundle <i>&lt;interface-name&gt;</i> .
Meaning	An admin added the specified interface to the multilink interface.

Action	No recommended action.
--------	------------------------

Message	[mlfr/cfg]: delete link <i>&lt;interface-name&gt;</i> from bundle <i>&lt;interface-name&gt;</i> .
Meaning	An admin removed the specified interface from the multilink interface.

Action	No recommended action.
--------	------------------------

Message	[mlfr/cfg]: set interface <i>&lt;interface-name&gt;</i> 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 <i>&lt;ackretries&gt;</i> for bundle link <i>&lt;interface-name&gt;</i> .
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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

Meaning An admin configured the minimum number of links for the specified multilink interface.

Action No recommended action.

Message [mlfr/cfg]: unset bundle link *<interface-name>* lip fragment-threshold to *<frag>*.

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 *<interface-name>* encaps 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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

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 *<interface-name>*.

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-name>*: LMI link is down due to errors over threshold (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]: <i>&lt;interface-name&gt;</i> dlc( <i>&lt;dlci&gt;</i> ) status changed to <i>&lt;state&gt;</i> .
Meaning	The specified DLCI status has changed, as indicated.
Action	No recommended action.

Message	[fr/lmi]: <i>&lt;interface-name&gt;</i> LMI status changed to <i>&lt;state&gt;</i> .
Meaning	The LMI status has changed to down or up.
Action	No recommended action.

## Notification (00570)

Message	[mlfr/lip]: change bundle <i>&lt;interface-name&gt;</i> physical status to down.
Meaning	The specified bundle is down.
Action	No recommended action.

Message	[mlfr/lip]: changed bundle <i>&lt;interface-name&gt;</i> physical status to up.
Meaning	The specified bundle is up.
Action	No recommended action.

Message	[mlfr/lip]: link interface <i>&lt;interface-name&gt;</i> LIP is down at bundle <i>&lt;interface-name&gt;</i> .
Meaning	Link Interface Protocol is down on the specified link interface in the bundle.
Action	No recommended action

Message	[mlfr/lip]: link interface <i>&lt;interface-name&gt;</i> LIP is up at bundle <i>&lt;interface-name&gt;</i> .
Meaning	Link Interface Protocol is up on the specified link interface in the bundle.
Action	No recommended action.

Message	[mlfr/lip]: <i>&lt;interface-name&gt;</i> LIP FSM: ( <i>&lt;oldstate&gt;</i> ) -> ( <i>&lt;newstate&gt;</i> ) by event ( <i>&lt;event&gt;</i> ).
Meaning	The indicated event has changed the Link Integrity Protocol state (the previous and new states are shown).
Action	No recommended action.



## CHAPTER 19

# 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, <i>&lt;gk-ip&gt;</i> , exceeds the threshold, <i>&lt;ras-flooding-msg-threshold&gt;</i> .
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: <i>&lt;max-h323-call-num&gt;</i> .
Meaning	The number of concurrent 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: <i>&lt;active-h323-call-num&gt;</i> . 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 20

# Interface

The following messages relate to interface configurations.

### Critical (00091)

Message	L3 backup failover from interface <i>&lt;interface-name&gt;</i> to interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> to interface <i>&lt;interface-name&gt;</i> .
Meaning	A L3 backup failover occurred from the specified backup interface to the primary interface.
Action	No recommended action.

### Critical (00094)

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.

## Notification (00009)

Message	802.1Q VLAN tag <i>&lt;tag&gt;</i> has been created.
Meaning	An admin has created the specified VLAN tag.
Action	No recommended action.

Message	802.1Q VLAN tag <i>&lt;tag&gt;</i> has been removed.
Meaning	An admin has deleted the specified VLAN tag.
Action	No recommended action.

Message	Activation delay for interface <i>&lt;interface-name&gt;</i> has been changed to <i>&lt;activation_delay&gt;</i> .
Meaning	The primary interface activation delay is changed.
Action	No recommended action.

Message	Admin status for interface <i>&lt;interface-name&gt;</i> has been changed to <i>&lt;value&gt;</i> .
Meaning	The admin status for the identified interface is changed.
Action	No recommended action.

Message	Auto-failover for interface <i>&lt;interface-name&gt;</i> has been changed to <i>&lt;auto_state&gt;</i> .
Meaning	The primary interface auto-failover is changed.
Action	No recommended action.

Message	Deactivation delay for interface <i>&lt;interface-name&gt;</i> has been changed to <i>&lt;deactivation_delay&gt;</i> .
Meaning	The primary interface deactivation delay is changed.
Action	No recommended action.
Message	DNS proxy was <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> .
Meaning	An admin enabled or disabled Domain Name Service (DNS) proxy on the named interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> 802.1Q tag has been changed to <i>&lt;tag&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has changed the 802.1Q VLAN tag for the specified interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> 802.1Q tag has been removed <i>&lt;user-name&gt;</i> .
Meaning	An admin deleted the specified interface and 802.1Q VLAN tag.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> 802.1Q VLAN trunking has been turned OFF <i>&lt;user-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> 802.1Q VLAN trunking has been turned ON <i>&lt;user-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> bandwidth has been changed to <i>&lt;bandwidth&gt;</i> Kbps.
Meaning	An admin has changed the configured bandwidth for the specified interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> gateway IP has been changed from <i>&lt;ip&gt;</i> to <i>&lt;ip&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has changed the IP address of the gateway for the specified interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> has been added to aggregate interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> has been added to redundant interface <i>&lt;interface-name&gt;</i> .
Meaning	An admin added an interface in the specified redundant interface group.
Action	No recommended action.

Message	Interface <i>&lt;interface-name&gt;</i> has been added to shared interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> has been changed from VSI to local.
Meaning	An admin changed a VSI to a local interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> has been removed from aggregate interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> has been removed from redundant interface <i>&lt;interface-name&gt;</i> .
Meaning	An admin added an interface in the specified redundant interface group.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> has been removed from shared interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> holddown time interval has been set to <i>&lt;holddown_time&gt;</i> .
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 <i>&lt;interface-name&gt;</i> in <i>&lt;vsys_name&gt;</i> was removed <i>&lt;user-name&gt;</i> .
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 *<ip>* mask *<netmask>* tag *<tag>* was created *<user-name>*.

**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 *<ip>* mask *<netmask>* was created *<user-name>*.

**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 *<ip>* to *<ip>* *<user-name>*.

**Meaning** An admin has changed the IP address for the specified interface.

**Action** No recommended action.

Message	Interface <i>&lt;interface-name&gt;</i> management IP has been changed from <i>&lt;ip&gt;</i> to <i>&lt;ip&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has changed the manage IP address for the specified interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> netmask has been changed from <i>&lt;netmask&gt;</i> to <i>&lt;netmask&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has changed the netmask for the specified interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> operational mode has been changed to <i>&lt;operational_mode&gt;</i> <i>&lt;user-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> physical setting has been changed: <i>&lt;command&gt;</i>
Meaning	Interface physical setting has been changed.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> switching to annexL del test mode.
Meaning	The ADSL interface has changed to annexL delete test mode.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> switching to annexL mode.
Meaning	The ADSL interface has changed to annexL mode.
Action	No recommended action.

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 annexM mode.

Meaning The ADSL interface has changed to ITU G.992.3 annexM mode.

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 annexM mode.

Meaning The ADSL interface has changed to ITU G.992.5 annexM 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>* *<user-name>*.

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-name>*.

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>* *<user-name>*.

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 *<interface-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>* *<user-name>*.

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>* *<user-name>*.

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 <i>&lt;maximum_bandwidth&gt;</i> Kbps on interface <i>&lt;interface-name&gt;</i> is less than total guaranteed bandwidth <i>&lt;guaranteed_bandwidth&gt;</i> 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 <i>&lt;threshold&gt;</i> of <i>&lt;interface-name&gt;</i> .
Meaning	An admin changed the threshold of a monitoring parameter for an interface.
Action	No recommended action.
Message	Mtrace has been <i>&lt;state&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin enabled or disabled mtrace on the named interface.
Action	No recommended action.
Message	MTU for interface <i>&lt;interface-name&gt;</i> has been changed to <i>&lt;mtu&gt;</i> .
Meaning	An admin changed the Maximum Transmission Unit (MTU) for the specified interface.
Action	No recommended action.
Message	Primary interface <i>&lt;interface-name&gt;</i> set backup interface <i>&lt;interface-name&gt;</i> , type is <i>&lt;type&gt;</i> .
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 <i>&lt;interface-name&gt;</i> unset backup interface <i>&lt;interface-name&gt;</i> .
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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> has been enabled.
Meaning	An admin has enabled the routes to all secondary IP addresses on the specified interface.
Action	No recommended action.
Message	<i>&lt;phy_name&gt;</i> for interface <i>&lt;interface-name&gt;</i> has been changed to <i>&lt;value&gt;</i> .
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 <i>&lt;p&gt;</i> has been deleted from interface <i>&lt;interface-name&gt;</i> .
Meaning	An admin successfully deleted a specified IP address to a specified interface.
Action	No recommended action.

Message	Secondary IP address <i>&lt;ip&gt;/&lt;netmask&gt;</i> has been added to interface <i>&lt;interface-name&gt;</i> .
---------	--

Meaning	An admin successfully added a specified IP address to a specified interface.
---------	--

Action	No recommended action.
--------	------------------------

Message	Zone <i>&lt;zone_name&gt;</i> was removed from the monitoring list of <i>&lt;interface-name&gt;</i> .
---------	---

Meaning	An admin removed a zone from the monitoring list that was associated with an interface.
---------	---

Action	No recommended action.
--------	------------------------

Message	Zone <i>&lt;zone_name&gt;</i> with weight <i>&lt;weight&gt;</i> was added to the monitoring list of <i>&lt;interface-name&gt;</i> .
---------	---

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: <i>&lt;cli_string&gt;</i> .
---------	---

Meaning	A dialer interface setting is configured.
---------	---

Action	No recommended action.
--------	------------------------

### Notification (00513)

Message	The physical state of interface <i>&lt;interface-name&gt;</i> has changed to <i>&lt;new_state&gt;</i> .
---------	---

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 <i>&lt;interface-name&gt;</i> dialed out at channel <i>&lt;channel&gt;</i> .
---------	--

Meaning	The dialer interface dialed out from the specified channel.
---------	---

Action	No recommended action.
--------	------------------------

Message	Interface <i>&lt;interface-name&gt;</i> disconnects at channel <i>&lt;channel&gt;</i> .
Meaning	The dialer interface is disconnected on the specified channel.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> idle timer expired.
Meaning	The dialer interface idle timer is expired.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> is connected at channel <i>&lt;channel&gt;</i> .
Meaning	The dialer interface is established a connection on the specified channel.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> is disconnecting at channel <i>&lt;channel&gt;</i> .
Meaning	The dialer interface is disconnecting on the specified channel.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> traffic ( <i>&lt;traffic&gt;</i> 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 <i>&lt;interface-name&gt;</i> traffic ( <i>&lt;traffic&gt;</i> 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.

## Notification (00626)

Message	Egress traffic notifies interface <i>&lt;interface-name&gt;</i> to start dial-up.
Meaning	The traffic out of dial interface leads to dial-up of the interface.
Action	No recommended action.
Message	The interface <i>&lt;interface-name&gt;</i> starts auto dial-up after <i>&lt;seconds&gt;</i> s.
Meaning	The dial-up starts automatically after the auto-connect time elapses.
Action	No recommended action.
Message	The interface <i>&lt;interface-name&gt;</i> starts to hang-up after idle time <i>&lt;seconds&gt;</i> s.
Meaning	The hang-up starts automatically after the idle time elapses.
Action	No recommended action.

## Information (00009)

Message	packet distribution mode has changed to <i>&lt;hashing_mode&gt;</i> in slot <i>&lt;slot_id&gt;</i> .
Meaning	Policy mode has changed.
Action	No recommended action.
Message	GARP has been <i>&lt;state&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	The G-ARP knob state has changed to on or off.
Action	No recommended action.
Message	Global-PRO has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled Global-PRO access for the specified interface.
Action	No recommended action.

Message	Ident-reset has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled Ident-reset access for the specified interface.
Action	No recommended action.
Message	Interface <i>&lt;interface-name&gt;</i> has switched to <i>&lt;mode-name&gt;</i> mode.
Meaning	Interface physical mode has changed (between auto-negotiation and manual).
Action	No recommended action.
Message	NSGP <i>&lt;enforcing_IPSec&gt;</i> has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
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 <i>&lt;state&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled the ping functionality for the specified interface.
Action	No recommended action.

Message	SCS has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled the SCS functionality for the specified interface.
Action	No recommended action.
Message	set <i>&lt;hashing_mode&gt;</i> on slot <i>&lt;slot_id&gt;</i> chip <i>&lt;chip_id&gt;</i> of 8G2.
Meaning	Policy mode has changed.
Action	No recommended action.
Message	SNMP has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled the SNMP functionality for the specified interface.
Action	No recommended action.
Message	SSL has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled SSL access for the specified interface.
Action	No recommended action.
Message	Telnet has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled the telnet connection functionality for the specified interface.
Action	No recommended action.
Message	Web has been <i>&lt;new_status&gt;</i> on interface <i>&lt;interface-name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin has either enabled or disabled web access for the specified interface.
Action	No recommended action.

## CHAPTER 21

# Interface6

The following messages apply to IPv6 network deployments.

### Critical (00101)

Message	DAD detected duplicates for IPv6 address <i>&lt;ip&gt;</i> on interface <i>&lt;interface-name&gt;</i>
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	<i>&lt;new_status&gt;</i> IPv6 function on the interface <i>&lt;interface-name&gt;</i> .
Meaning	Enabling or disabling the IPv6 functions on an interface.
Action	
Message	Setting interface <i>&lt;interface-name&gt;</i> IPv6 mode to <i>&lt;mode&gt;</i> .
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 <i>&lt;interface-name&gt;</i> .
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 <i>&lt;ip&gt;</i> on interface <i>&lt;interface-name&gt;</i>
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 <i>&lt;ip&gt;</i> on interface <i>&lt;interface-name&gt;</i>
Meaning	An admin assigned an IPv6 address to an interface.
Action	No recommended action.

### Notification (00072)

Message	IPv6 Router advertisement reception disabled on interface <i>&lt;interface-name&gt;</i>
Meaning	An admin enabled or disabled router advertisement (RA) reception on the specified interface.
Action	No recommended action.
Message	IPv6 Router advertisement reception enabled on interface <i>&lt;interface-name&gt;</i>
Meaning	An admin enabled or disabled router advertisement (RA) reception on the specified interface.
Action	No recommended action.

Message	IPv6 Router advertisement transmission disabled on interface <i>&lt;interface-name&gt;</i>
Meaning	An admin enabled or disabled router advertisement (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 <i>&lt;interface-name&gt;</i>
Meaning	An admin enabled or disabled router advertisement (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 22

# ISDN

The following messages relate to the Integrated Services Digital Network (ISDN) feature in ScreenOS.

### Notification (00083)

Message	[isdn] Interface <i>&lt;interface-name&gt;</i> is configured for leased-line <i>&lt;none&gt;</i> .
Meaning	The BRI interface (ISDN) is configured for leased line at 128 kbps.
Action	No action required.
Message	[isdn] Interface <i>&lt;interface-name&gt;</i> is configured to work with switch type <i>&lt;none&gt;</i> (after reboot).
Meaning	The BRI interface (ISDN) is configured to work with the specified switch type.
Action	No action required.
Message	[isdn] Interface <i>&lt;interface-name&gt;</i> is set for TEI negotiation at <i>&lt;none&gt;</i> .
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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> .
Meaning	The BRI interface (ISDN) is not configured for leased line.
Action	No action required.
Message	[isdn] SPID1 for interface <i>&lt;interface-name&gt;</i> is set to <i>&lt;none&gt;</i> .
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 <i>&lt;interface-name&gt;</i> is set to <i>&lt;none&gt;</i> .
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 <i>&lt;interface-name&gt;</i> is set to <i>&lt;none&gt;</i> .
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 <i>&lt;interface-name&gt;</i> is changed from <i>&lt;none&gt;</i> to <i>&lt;none&gt;</i> .
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 <i>&lt;interface-id&gt;</i> connected on B channel <i>&lt;none&gt;</i> .
Meaning	A call is set up successfully on a B channel.
Action	No action required.
Message	[isdn] Interface <i>&lt;interface-id&gt;</i> disconnected on B channel <i>&lt;none&gt;</i> .
Meaning	A call is ended on a B channel.
Action	No action required.
Message	[isdn] Layer2 is <i>&lt;none&gt;</i> on D channel <i>&lt;none&gt;</i> .
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 23

# Logging

The following messages relate to the event, self and traffic logs.

### Warning (00002)

Message	Cannot connect to e-mail server <i>&lt;server_name&gt;</i> .
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 action

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 24

# NAT IPsec

The following messages relate to the Network Address Translation (NAT) IP security (IPsec) feature in ScreenOS.

### Notification (00004)

Message	It <i>&lt;inhibit-or-not&gt;</i> to transfer DNS 'AAAA' request to 'A' request <i>&lt;user-name&gt;</i> .
Meaning	It specifies the inhibition of "AAAA" request from v6 to v4 side in NAT-PT DNS ALG.
Action	No recommended action.

### Information (00536)

Message	The IKE packet from <i>&lt;none&gt;</i> to <i>&lt;src-ip&gt;</i> is dropped since pinhole with id <i>&lt;none&gt;</i> have existed.
Meaning	The IKE packet is dropped since there is another IKE negotiation that has DIP IP and dst IP as that of the current IKE packet.
Action	No recommended action.



## CHAPTER 25

# NSM

The following messages relate to the NetScreen-Security Manager (NSM) central management software.

### Notification (00033)

Message	Admin user <i>&lt;user-name&gt;</i> has disabled debug no-off-on-exit feature.
Meaning	An admin has disabled debug no-off-on-exit feature. The debug option will be turned off when user logged out.

Action	No recommended action.
--------	------------------------

Message	Admin user <i>&lt;user-name&gt;</i> has enabled debug no-off-on-exit feature.
Meaning	An admin has enabled debug no-off-on-exit feature. The debug option will not be turned off when user logged out.

Action	No recommended action.
--------	------------------------

Message	CA certificate field of NACN policy manager <i>&lt;manager_id&gt;</i> has been set to <i>&lt;ca&gt;</i> .
---------	---

Meaning	An admin set the Certificate Authority (CA) certificate field of the policy manager to the specified string.
---------	--

Action	No recommended action.
--------	------------------------

Message	CA certificate field of NACN policy manager <i>&lt;manager_id&gt;</i> has been unset.
---------	---

Meaning	An admin cleared the Certificate Authority (CA) certificate field of the specified policy manager.
---------	--

Action	Specify a CA certificate if necessary.
--------	--

Message	Cert-Subject field of NACN policy manager <i>&lt;manager_id&gt;</i> has been set to <i>&lt;cert_sub&gt;</i> .
Meaning	An admin set the subject name field in the Policy Manager certificate.
Action	No recommended action.
Message	Cert-Subject field of NACN policy manager <i>&lt;manager_id&gt;</i> has been unset.
Meaning	An admin 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 <i>&lt;manager_id&gt;</i> has been set to <i>&lt;host&gt;</i> .
Meaning	An admin set the host field to the specified hostname.
Action	No recommended action.
Message	Host field of NACN policy manager <i>&lt;manager_id&gt;</i> 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 <i>&lt;id&gt;</i> .
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 ( <i>&lt;name&gt;</i> ) 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 Network and Security Manager (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 Network and Security Manager (NSM).
Action	No recommended action.
Message	NSM primary server with name <i>&lt;name&gt;</i> was set: addr <i>&lt;ip_addr&gt;</i> , port <i>&lt;port&gt;</i>
Meaning	An admin set the host name and/or IP address and port of the Network and Security Manager (NSM) primary or secondary server.
Action	No recommended action.

Message	NSM primary server with name <i>&lt;name&gt;</i> was set: addr <i>&lt;ip_addr&gt;</i> , port <i>&lt;port&gt;</i>
Meaning	An admin set the host name and/or IP address and port of NSM primary or secondary server.
Action	No recommended action.
Message	NSM primary server with name <i>&lt;name&gt;</i> was unset.
Meaning	An admin unset the specified primary or secondary Network and Security Manager (NSM) server.
Action	No recommended action.
Message	NSM secondary server with name <i>&lt;name&gt;</i> was set: addr <i>&lt;ip_addr&gt;</i> , port <i>&lt;port&gt;</i>
Meaning	An admin set the host name and/or IP address and port of the Network and Security Manager (NSM) primary or secondary server.
Action	No recommended action.
Message	NSM secondary server with name <i>&lt;name&gt;</i> was set: addr <i>&lt;ip_addr&gt;</i> , port <i>&lt;port&gt;</i>
Meaning	An admin set the host name and/or IP address and port of NSM primary or secondary server.
Action	No recommended action.
Message	NSM secondary server with name <i>&lt;name&gt;</i> was unset.
Meaning	An admin unset the specified primary or secondary Network and Security Manager (NSM) server.
Action	No recommended action.

Message	Outgoing interface of NACN policy manager <i>&lt;manager_id&gt;</i> has been set to <i>&lt;interface&gt;</i> .
Meaning	An admin set the outgoing interface for NACN policy manager to the specified interface.
Action	No recommended action.
Message	Outgoing interface of NACN policy manager <i>&lt;manager_id&gt;</i> has been unset.
Meaning	An admin 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 <i>&lt;manager_id&gt;</i> has been <i>&lt;string&gt;</i> .
Meaning	An admin changed the password for the specified NACN policy manager.
Action	No recommended action.
Message	Policy-domain field of NACN policy manager <i>&lt;manager_id&gt;</i> has been set to <i>&lt;domain&gt;</i> .
Meaning	An admin 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 <i>&lt;manager_id&gt;</i> has been unset.
Meaning	An admin 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 <i>&lt;manager_id&gt;</i> has been reset to the default value.
Meaning	An admin reverted the port field of the specified policy manager to the default.
Action	No recommended action.
Message	Port field of NACN policy manager <i>&lt;manager_id&gt;</i> has been set to <i>&lt;port_field&gt;</i> .
Meaning	An admin set the port field of the policy manager to the specified value.
Action	No recommended action.
Message	Reporting of attack alarms to <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 <i>&lt;sme_name&gt;</i> 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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 *<sme\_name>* 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	<i>&lt;sme_name&gt;</i> has been disabled.
Meaning	An admin configured the device to disable management by Network and Security Manager (NSM).
Action	No recommended action.
Message	<i>&lt;sme_name&gt;</i> has been enabled.
Meaning	An admin configured the device to enable management by Network and Security Manager (NSM).
Action	No recommended action.
Message	<i>&lt;sme_name&gt;</i> <i>&lt;which&gt;</i> host has been disabled.
Meaning	An admin disabled the Network and Security Manager (NSM) primary or secondary host.
Action	No recommended action.
Message	<i>&lt;sme_name&gt;</i> <i>&lt;which&gt;</i> host has been set to <i>&lt;host_ip&gt;</i> .
Meaning	An admin set the Network and Security Manager (NSM) primary or secondary host to the specified IP address.
Action	No recommended action.
Message	<i>&lt;sme_name&gt;</i> <i>&lt;which&gt;</i> host has been set to <i>&lt;host&gt;</i> .
Meaning	An admin set the Network and Security Manager (NSM) primary or secondary host to the specified hostname.
Action	No recommended action.
Message	<i>&lt;sme_name&gt;</i> VPN management tunnel has been disabled.
Meaning	A VPN tunnel for administrative traffic has been disabled.
Action	No recommended action.

Message	<i>&lt;sme_name&gt;</i> 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 <i>&lt;status&gt;</i>
Meaning	An admin enabled or disabled 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 recommended action.
Message	Timeout value of <i>&lt;name&gt;</i> has been set to <i>&lt;second&gt;</i> seconds (default)
Meaning	An admin reset the Network and Security Manager (NSM) timeout to the default value.
Action	No recommended action.
Message	Timeout value of <i>&lt;name&gt;</i> has been set to <i>&lt;second&gt;</i> seconds.
Meaning	An admin set the Network and Security Manager (NSM) timeout to the specified value.
Action	No recommended action.
Message	User-defined service <i>&lt;service_name&gt;</i> has been added to <i>&lt;sme_name&gt;</i> protocol distribution.
Meaning	An admin either added or removed the specified service on the protocol distribution events report.
Action	No recommended action.
Message	User-defined service <i>&lt;service_name&gt;</i> has been removed from <i>&lt;sme_name&gt;</i> protocol distribution.
Meaning	An admin either added or removed the specified service on the protocol distribution events report.
Action	No recommended action.

## Information (00538)

Message	Connection to <i>&lt;host_name&gt;</i> data collector at <i>&lt;ip_addr&gt;</i> 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 <i>&lt;host_name&gt;</i> data collector at <i>&lt;ip_addr&gt;</i> .
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 <i>&lt;host_name&gt;</i> data collector at <i>&lt;ip_addr&gt;</i> .
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 <i>&lt;host_name&gt;</i> because of <i>&lt;reason&gt;</i> .
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 <i>&lt;host_name&gt;</i> : <i>&lt;string&gt;</i> .
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 a Network and Security Manager (NSM) request.
Action	Reduce the number of objects (interfaces, VPNs, and 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 <i>&lt;ip_addr&gt;</i> . Reason: <i>&lt;err_id&gt;</i> , <i>&lt;reason&gt;</i> ( <i>&lt;count&gt;</i> ) connect attempt(s))
Meaning	The device tried and failed to connect to the Network and Security Manager (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: Cannot connect to NSM server at <i>&lt;ip_addr&gt;</i> . Reason: <i>&lt;err_id&gt;</i> , <i>&lt;reason&gt;</i> ( <i>&lt;count&gt;</i> ) connect attempt(s))
Meaning	The security device tried but failed to connect to the NSM server after the specified number of 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 <i>&lt;ip_addr&gt;</i> ( <i>&lt;count&gt;</i> ) connect attempt(s))
Meaning	The device successfully connected to the Network and Security Manager (NSM) server after the specified number of connection attempts.
Action	No recommended action.
Message	NSM: Connected to NSM server at <i>&lt;ip_addr&gt;</i> ( <i>&lt;count&gt;</i> ) 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 <i>&lt;nsm_server&gt;</i> is down. Reason: <i>&lt;err_id&gt;</i> , <i>&lt;reason&gt;</i>
Meaning	The connection between the Network and Security Manager (NSM) server and the security device is down. Reason: <i>&lt;string&gt;</i>
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: Connection to NSM server at <i>&lt;nsm_server&gt;</i> is down. Reason: <i>&lt;err_id&gt;</i> , <i>&lt;reason&gt;</i>
Meaning	The connection between the NSM server and the security device is down. Reason: <i>&lt;string&gt;</i>
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 <i>&lt;message&gt;</i> message
Meaning	The device sent the specified message to Netscreen and Security Manager.
Action	No recommended action.
Message	The NACN protocol has started for policy manager <i>&lt;manager_id&gt;</i> on hostname <i>&lt;host_name&gt;</i> IP address <i>&lt;ip_addr&gt;</i> port <i>&lt;port&gt;</i>
Meaning	The device started the NACN protocol.
Action	No recommended action.



## CHAPTER 26

# NSRD

The following messages relate to events generated by the RD (Rapid Deployment) process.

### Error (00551)

Message	Error <i>&lt;error_no&gt;</i> 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 <i>&lt;error_no&gt;</i> occurred, causing failure to establish secure management with Management System.
Meaning	Network and 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 Network and 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 to 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 Rapid Deployment (RD) 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 <code>unset all</code> , 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 27

# NSRP

The following messages relate to the NetScreen Redundancy Protocol (NSRP).

### Critical (00015)

Message	NSRP: <i>&lt;nsrp&gt; &lt;nsrp&gt;</i> .
Meaning	The HA control(data) channel has changed to NULL or some interface name.
Action	No recommended action.
Message	NSRP: <i>&lt;nsrp&gt;</i> .
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 <i>&lt;device-id&gt;</i> 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 <i>&lt;device-id&gt;</i> 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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group <i>&lt;group-id&gt;</i> changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> .
Meaning	The state of the local or peer device in the specified VSD group has changed.
Action	No recommended action.
Message	RTO mirror group <i>&lt;group-id&gt;</i> with direction <i>&lt;direction&gt;</i> on local device <i>&lt;device-id&gt;</i> , detected a duplicate direction on the peer device <i>&lt;device-id&gt;</i> .
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 <i>&lt;group-id&gt;</i> with direction <i>&lt;direction&gt;</i> changed on the local device from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> state, it had peer device <i>&lt;device-id&gt;</i> .
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 <i>&lt;group-id&gt;</i> with direction <i>&lt;direction&gt;</i> on peer device <i>&lt;device-id&gt;</i> changed from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> state, <i>&lt;state-string&gt;</i> .
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 (00070)

Message	The local device <i>&lt;device-id&gt;</i> in the Virtual Security Device group <i>&lt;group-id&gt;</i> changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> , <i>&lt;state-string&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group <i>&lt;group-id&gt;</i> changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group ( <i>&lt;group-id&gt;</i> ) changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> , <i>&lt;state-string&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group ( <i>&lt;group-id&gt;</i> ) changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> , <i>&lt;state-string&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group ( <i>&lt;group-id&gt;</i> ) changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> , <i>&lt;state-string&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group <i>&lt;group-id&gt;</i> changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> , <i>&lt;state-string&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group <i>&lt;group-id&gt;</i> changed state from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group <i>&lt;group-id&gt;</i> sent a 2nd path request to the peer device <i>&lt;device-id&gt;</i> .
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 <i>&lt;device-id&gt;</i> in the Virtual Security Device group <i>&lt;group-id&gt;</i> received a 2nd path request from peer device <i>&lt;device-id&gt;</i> to device <i>&lt;device-id&gt;</i> .
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 <i>&lt;message&gt;</i> 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: <i>&lt;nsrp&gt;</i> .
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 <i>&lt;interface-name&gt;</i> .
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 <i>&lt;time&gt;</i> (milliseconds) to <i>&lt;time&gt;</i> (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 <i>&lt;vsd-id&gt;</i> 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 <i>&lt;vsd-id&gt;</i> 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 <i>&lt;device-id&gt;</i> 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 <i>&lt;interface-name&gt;</i> was removed from the monitoring list for <i>&lt;group-id&gt;</i> .
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 <i>&lt;interface-name&gt;</i> with weight <i>&lt;weight&gt;</i> was added to or updated on the monitoring list for <i>&lt;group-id&gt;</i> .
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 <i>&lt;group-id&gt;</i> 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 <i>&lt;group-id&gt;</i> direction was set to <i>&lt;none&gt;</i> .
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 <i>&lt;group-id&gt;</i> was set.
Meaning	Run Time Object mirror group <i>&lt;mirror_group_id&gt;</i> 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 <i>&lt;group-id&gt;</i> with direction <i>&lt;direction&gt;</i> 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 <i>&lt;device-id&gt;</i> 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 <i>&lt;interface-name&gt;</i> with ifnum <i>&lt;interface-id&gt;</i> 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 <i>&lt;link&gt;</i> was set to <i>&lt;time&gt;</i> 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 <i>&lt;link&gt;</i> 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 <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> .
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 <i>&lt;interface-name&gt;</i> , with ifnum <i>&lt;interface-id&gt;</i> .
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 <i>&lt;link&gt;</i> was set to <i>&lt;time&gt;</i> .
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 <i>&lt;group-id&gt;</i> was created. The total number of members in the group is <i>&lt;group-count&gt;</i> .
Meaning	An administrator created the specified Virtual Security Device group.
Action	No recommended action.
Message	Virtual Security Device group <i>&lt;group-id&gt;</i> was deleted. The total number of members in the group was <i>&lt;group-count&gt;</i> .
Meaning	An administrator removed the specified Virtual Security Device group.
Action	No recommended action.

Message	Zone <i>&lt;zone-name&gt;</i> was removed from the monitoring list for <i>&lt;none&gt;</i> .
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 <i>&lt;zone-name&gt;</i> with weight <i>&lt;weight&gt;</i> was added to or updated on the monitoring list for <i>&lt;none&gt;</i> .
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 <i>&lt;device-id&gt;</i> has joined NSRP cluster <i>&lt;cluster-id&gt;</i> <i>&lt;name&gt;</i> .
Meaning	An admin either added the specified device from the NSRP cluster.
Action	No recommended action.
Message	Device <i>&lt;device-id&gt;</i> quit current NSRP cluster <i>&lt;cluster-id&gt;</i> <i>&lt;name&gt;</i> .
Meaning	An admin either removed the specified device from the NSRP cluster.
Action	No recommended action.

Message	The monitoring threshold was modified to <i>&lt;none&gt;</i> for <i>&lt;none&gt;</i> .
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 <i>&lt;group-id&gt;</i> priority changed from <i>&lt;state-old&gt;</i> to <i>&lt;state-new&gt;</i> .
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.

## CHAPTER 28

# NTP

The following messages relate to the Network Time Protocol (NTP).

### Notification (00531)

Message	Administrator <i>&lt;user-name&gt;</i> changed the Network Time Protocol authentication mode to <i>&lt;auth_mode&gt;</i> ( <i>&lt;none&gt;</i> )
Meaning	The named admin set the authentication mode for NTP traffic to either required or preferred.
Action	No recommended action.
Message	Administrator <i>&lt;user-name&gt;</i> changed the Network Time Protocol maximum adjustment value from <i>&lt;old_adj&gt;</i> to <i>&lt;new_adj&gt;</i> seconds ( <i>&lt;none&gt;</i> )
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 <i>&lt;ntp_server_type&gt;</i> NTP server <i>&lt;ntp_server_name&gt;</i>
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 <i>&lt;ntp_server_type&gt;</i> <i>&lt;ntp_server_name&gt;</i> because <i>&lt;fail_reason&gt;</i>
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 <i>&lt;msec_adjustment&gt;</i> ms from NTP server <i>&lt;ntp_server_name&gt;</i> exceeds the allowed adjustment of <i>&lt;msec_adjustment_allowed&gt;</i> 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 by <i>&lt;user-name&gt;</i> .
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 <i>&lt;ntp_server_type&gt;</i> <i>&lt;ntp_server_name&gt;</i>
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 <i>&lt;ntp_server_type&gt;</i> <i>&lt;ntp_server_name&gt;</i>
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 is disabled on interface <i>&lt;interface-name&gt;</i>
Meaning	An admin has disabled the NTP server on an interface.
Action	No recommended action.

Message NTP server is enabled on interface *<interface-name>*, mode: *<ntp\_mode>*  
Meaning An admin has enabled the NTP server on an interface.

Action No recommended action.

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.

Message The system clock will be changed from *<old\_system\_time>* to *<new\_system\_time>* received from *<ntp\_server\_type>* NTP server *<ntp\_server\_name>*  
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 <i>&lt;ntp_server_name&gt;</i>
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 <i>&lt;ntp_server_name&gt;</i>
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 29

# Policy

The following messages relate to the configuration of access policies.

### Notification (00018)

Message	Default policy of the device has been changed to <i>&lt;state&gt; &lt;user-name&gt;</i> .
Meaning	An admin ( <i>name_str</i> ) has modified the default policy of the device.
Action	Confirm that the action was appropriate, and performed by an authorized admin.
Message	In policy <i>&lt;policy-id&gt;</i> , the application was modified to <i>&lt;service-name&gt; &lt;user-name&gt;</i> .
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 <i>&lt;policy-id&gt;</i> , the attack severity was modified <i>&lt;user-name&gt;</i> .
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 <i>&lt;policy-id&gt;</i> , the DI attack component was modified <i>&lt;user-name&gt;</i> .
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	In policy <i>&lt;policy-id&gt;</i> , the option <i>&lt;opt-name&gt;</i> was <i>&lt;opt-status&gt;</i> .
Meaning	Enable or disable the policy option.
Action	Confirm that the option was appropriate, and performed by an authorized admin.
Message	Policy ( <i>&lt;policy-id&gt;</i> , global, <i>&lt;addr-name&gt;</i> -> <i>&lt;addr-name&gt;</i> ), <i>&lt;service-name&gt;</i> , <i>&lt;action&gt;</i> ) was added <i>&lt;user-name&gt;</i> .
Meaning	An admin ( <i>name_str</i> ) has added an global policy with the following attributes on the current device: <i>id_num</i> : The ID number of the access policy. <i>src_addr</i> : 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.) <i>dst_addr</i> : 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.) <i>svc_name</i> : 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>, <zone-name>-><zone-name>, <addr-name>-><addr-name>,<service-name>, <nat> <action>) was added <user-name>.
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>, <zone-name>-><zone-name>, <addr-name>-><addr-name>,<service-name>, <action>) was deleted <user-name>.
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>, <zone-name>-><zone-name>, <addr-name>-><addr-name>,<service-name>, <action>) was modified <user-name>.
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>, <zone-name>-><zone-name>, <addr-name>-><addr-name>,<service-name>, <action>) was <state> <user-name>.
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 <i>&lt;policy-id&gt;</i> has been moved after <i>&lt;dst_policy_id&gt;</i> <i>&lt;user-name&gt;</i> .
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 <i>&lt;policy-id&gt;</i> has been moved before <i>&lt;dst_policy_id&gt;</i> <i>&lt;user-name&gt;</i> .
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	<i>&lt;cell-name&gt;</i> <i>&lt;cell-name&gt;</i> was <i>&lt;action&gt;</i> policy ID <i>&lt;policy-id&gt;</i> <i>&lt;user-name&gt;</i> .
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.
Message	The policy install hold-interval is set to <i>&lt;hold-interval&gt;</i> seconds <i>&lt;user-name&gt;</i> .
Meaning	An administrator modified the hold-interval of policy installation.
Action	Confirm that the action was appropriate, and performed by an authorized administrator.



## CHAPTER 30

# 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 <i>&lt;ip_pool_name&gt;</i> for user <i>&lt;user-name&gt;</i> .
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 (00017)

Message	IP address pool <i>&lt;ip_pool_name&gt;</i> was removed <i>&lt;user-name&gt;</i> .
Meaning	An admin ( <i>&lt;name_str&gt;</i> ) removed a PPPoE IP address pool.
Action	No recommended action.

Message	IP address pool <i>&lt;ip_pool_name&gt;</i> with range <i>&lt;ip_address&gt;</i> - <i>&lt;ip_address&gt;</i> was created <i>&lt;user-name&gt;</i> .
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 <i>&lt;ip_pool_name&gt;</i> with range <i>&lt;ipv6_address&gt;</i> - <i>&lt;ipv6_address&gt;</i> was created <i>&lt;user-name&gt;</i> .
Meaning	An admin ( <i>&lt;name_str2&gt;</i> ) added an IP range to an IP address pool ( <i>&lt;name_str2&gt;</i> ).
Action	No recommended action.
Message	IP address pool <i>&lt;ip_pool_name&gt;</i> with range <i>&lt;ip_address&gt;</i> - <i>&lt;ip_address&gt;</i> was removed <i>&lt;user-name&gt;</i> .
Meaning	An admin ( <i>&lt;name_str2&gt;</i> ) removed an IP range from an IP address pool ( <i>&lt;name_str2&gt;</i> ). Since the IP pool only contained one range the IP pool will also be removed.
Action	No recommended action.
Message	IP address pool <i>&lt;ip_pool_name&gt;</i> with range <i>&lt;ipv6_address&gt;</i> - <i>&lt;ipv6_address&gt;</i> was removed <i>&lt;user-name&gt;</i> .
Meaning	An admin ( <i>&lt;name_str2&gt;</i> ) removed an IP range from an IP address pool ( <i>&lt;name_str2&gt;</i> ). Since the IP pool only contained one range the IP pool will also be removed.
Action	No recommended action.
Message	Range <i>&lt;ip_address&gt;</i> - <i>&lt;ip_address&gt;</i> was added to IP pool <i>&lt;ip_pool_name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin ( <i>&lt;name_str2&gt;</i> ) added a IP range to an IP address pool ( <i>&lt;name_str2&gt;</i> ).
Action	No recommended action.

Message	Range <i>&lt;ipv6_address&gt;</i> - <i>&lt;ipv6_address&gt;</i> was added to IP pool <i>&lt;ip_pool_name&gt;</i> <i>&lt;user-name&gt;</i> .
Meaning	An admin ( <i>&lt;name_str2&gt;</i> ) added a IP range to an IP address pool ( <i>&lt;name_str2&gt;</i> ).

Action	No recommended action.
--------	------------------------

Message	Range <i>&lt;ip_address&gt;</i> - <i>&lt;ip_address&gt;</i> was removed from IP pool <i>&lt;ip_pool_name&gt;</i> <i>&lt;user-name&gt;</i> .
---------	---

Meaning	An admin ( <i>&lt;name_str2&gt;</i> ) removed an IP range to an IP address pool ( <i>&lt;name_str2&gt;</i> ).
---------	---

Action	No recommended action.
--------	------------------------

Message	Range <i>&lt;ipv6_address&gt;</i> - <i>&lt;ipv6_address&gt;</i> was removed from IP pool <i>&lt;ip_pool_name&gt;</i> <i>&lt;user-name&gt;</i> .
---------	---

Meaning	An admin ( <i>&lt;name_str2&gt;</i> ) removed an IP range to an IP address pool ( <i>&lt;name_str2&gt;</i> ).
---------	---

Action	No recommended action.
--------	------------------------

### Notification (00077)

Message	PPP profile <i>&lt;profile-name&gt;</i> changes authentication type to <i>&lt;auth-type&gt;</i> .
---------	---

Meaning	An admin changed the authentication method in the specified profile.
---------	--

Action	No recommended action.
--------	------------------------

Message	PPP profile <i>&lt;profile-name&gt;</i> changes local-name to <i>&lt;local-name&gt;</i> .
---------	---

Meaning	An admin changed the local name in the specified profile.
---------	---

Action	No recommended action.
--------	------------------------

Message	PPP profile <i>&lt;profile-name&gt;</i> changes secret to <i>&lt;secret&gt;</i> .
---------	---

Meaning	An admin changed the password in the specified profile.
---------	---

Action	No recommended action.
--------	------------------------

Message	PPP profile <i>&lt;profile-name&gt;</i> is <i>&lt;none&gt;</i> .
Meaning	Ad admin has created or deleted a PPP profile with the specified name.
Action	No recommended action.
Message	PPP profile <i>&lt;profile-name&gt;</i> <i>&lt;none&gt;</i> passive mode CHAP.
Meaning	An admin enabled or disabled passive mode in the specified profile.
Action	No recommended action.
Message	PPP profile <i>&lt;profile-name&gt;</i> sets ncp <i>&lt;ncp-type&gt;</i> .
Meaning	User sets the NCP type for a PPP profile.
Action	No recommended action.
Message	PPP profile <i>&lt;profile-name&gt;</i> sets netmask <i>&lt;netmask&gt;</i> .
Meaning	An admin set a netmask in the specified profile.
Action	No recommended action.
Message	PPP profile <i>&lt;profile-name&gt;</i> sets <i>&lt;none&gt;</i> use static IP.
Meaning	An admin set the use of a static IP address in the specified profile.
Action	No recommended action.
Message	PPP <i>&lt;none&gt;</i> encapsulation <i>&lt;encap-type&gt;</i> for interface <i>&lt;interface-name&gt;</i> .
Meaning	An admin set or unset PPP or multilink PPP (MLPPP) encapsulation for the specified interface.
Action	No recommended action.
Message	PPP <i>&lt;none&gt;</i> interface <i>&lt;interface-name&gt;</i> <i>&lt;none&gt;</i> bundle <i>&lt;interface-name&gt;</i> .
Meaning	An admin added or deleted an interface to or from the specified bundle.
Action	No recommended action.

Message PPP *<none>* profile *<profile-name>* for interface *<interface-name>*.  
 Meaning An admin bound or unbound a profile to the specified interface.

Action No recommended action.

Message PPP *<none>* short sequence number for interface *<interface-name>*.  
 Meaning An admin set or unset the use of a 12-bit sequence header format in multilink PPP (MLPPP) packets for the specified multilink interface.

Action No recommended action.

Message PPP set MRRU *<MRRU>* for interface *<interface-name>*.  
 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 *<interface-name>* takes on *<none>* 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.

Message PPP on *<interface-name>* detects loopback.  
 Meaning PPP found a loopback on the specified interface.  
 Action Check to see why the loopback is occurring.

## Notification (00572)

Message	PPP authentication state on interface <i>&lt;interface-name&gt;</i> : <i>&lt;none&gt;</i> .
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 <i>&lt;interface-name&gt;</i> is <i>&lt;none&gt;</i> and then brings <i>&lt;none&gt;</i> 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 <i>&lt;interface-name&gt;</i> is <i>&lt;none&gt;</i> .
Meaning	Link Control Protocol (LCP) state on the specified interface changed to up or down.
Action	No recommended action.
Message	PPP member <i>&lt;interface-name&gt;</i> fails to join bundle <i>&lt;interface-name&gt;</i> for <i>&lt;reason&gt;</i> .
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 greater than the local MRRU
Action	Check the specified reason. Make sure both sides of the link are using acceptable parameters.

Message	PPP member <i>&lt;interface-name&gt;</i> joins bundle <i>&lt;interface-name&gt;</i> successfully.
Meaning	The interface successfully joined the specified bundle after Link Control Protocol (LCP).
Action	No recommended action.
Message	PPP on interface <i>&lt;interface-name&gt;</i> finds possible loopback.
Meaning	PPP found a loopback on the specified interface, according to the Link Control Protocol (LCP) request packet.
Action	Check to see why the loopback is occurring and that the LCP request packet is correct.
Message	PPP on interface <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> is terminated by receiving Terminate-Request.
Meaning	The peer sent a request to terminate the PPP session.
Action	No recommended action.
Message	PPP on <i>&lt;interface-name&gt;</i> resets LCP for <i>&lt;reason&gt;</i> .
Meaning	PPP has reset the Link Control Protocol (LCP) 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 maximum transmission unit (MTU)
Action	Check the specified reason.

Message	PPP protocol on interface <i>&lt;interface-name&gt;</i> is <i>&lt;status&gt;</i> , local IP: <i>&lt;local-ip&gt;</i> , peer IP: <i>&lt;peer-ip&gt;</i> .
Meaning	PPP is up or down; the local and peer IP addresses are shown.
Action	No recommended action.
Message	PPP protocol on interface <i>&lt;interface-name&gt;</i> is <i>&lt;none&gt;</i> , local IPv6: <i>&lt;ipv6_address&gt;</i> , peer IPv6: <i>&lt;ipv6_address&gt;</i> .
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
Message	PPP updates interface <i>&lt;interface-name&gt;</i> 's IP to <i>&lt;ip_address&gt;</i> .
Meaning	PPP updated the interface's IP address to the assigned address.
Action	No recommended action.
Message	PPP updates interface <i>&lt;interface-name&gt;</i> 's IPv6 to <i>&lt;ipv6_address&gt;</i> .
Meaning	The interface's IPv6 address is changed because PPP is now up/down.
Action	No recommended action
Message	PPP updates interface <i>&lt;interface-name&gt;</i> 's L3 MTU to <i>&lt;MTU&gt;</i> .
Meaning	Based upon the results of PPP negotiation, the interface's maximum transmission unit (MTU) is updated to the specified number.
Action	No recommended action.

## CHAPTER 31

# 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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;pppoa_name&gt;</i> connected successfully.
Meaning	The PPPoA client on the security device successfully established a session with the PPPoA server.
Action	No recommended action.

Message	PPPoA <i>&lt;pppoa_name&gt;</i> connection attempt failed ( <i>&lt;reason&gt;</i> ).
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 32

# 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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;interface-name&gt;</i> 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 <i>&lt;access_concentrator&gt;</i> is advertising URL <i>&lt;url_string&gt;</i>
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 <i>&lt;access_concentrator&gt;</i> : <i>&lt;message_from_ac&gt;</i>
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. <i>&lt;pppoe_packet_received_type&gt;</i> 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 <i>&lt;timeout_reason&gt;</i>
---------	---

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 <i>&lt;pppoe_instance_name&gt;</i> 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: <i>&lt;ppp_fail_reason&gt;</i>
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 33

# 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 ( <i>&lt;max-routes&gt;</i> ) 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 <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> cannot be added to the virtual router <i>&lt;vrouter-name&gt;</i> because the number of route entries in the virtual router exceeds the maximum number of routes ( <i>&lt;max-routes&gt;</i> ) 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 <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> cannot be added to the virtual router <i>&lt;vrouter-name&gt;</i> because the number of route entries in the virtual router exceeds the maximum number of routes ( <i>&lt;max-routes&gt;</i> ) 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 <i>&lt;vrouter-name&gt;</i> while removing route <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> 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 <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> to virtual router <i>&lt;vrouter-name&gt;</i> 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 <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> to virtual router <i>&lt;vrouter-name&gt;</i> 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 <code>prefix_add</code> function that prevents the administrator from successfully adding the route. <code>prefix_add</code> 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 <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> to vrouter <i>&lt;vrouter-name&gt;</i> , <code>db_insert</code> 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 <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> to vrouter <i>&lt;vrouter-name&gt;</i> , 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 <i>&lt;gateway&gt;</i> 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 <i>&lt;gateway&gt;</i> 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	<i>&lt;vrouter-name&gt;</i> Error while deleting route <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> 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.

## Notification (00011)

Message	An IPV6 SIBR route in virtual router <i>&lt;vrouter-name&gt;</i> with an IP address <i>&lt;src-ip&gt;/&lt;src-mask&gt;</i> and next-hop as virtual router <i>&lt;next-hop-vrouter-name&gt;</i> created.
Meaning	An IPV6 source interface-based route (SIBR) is created with a virtual router as the next hop.
Action	No recommended action.

Message	An SIBR route in virtual router <i>&lt;vrouter-name&gt;</i> with an IP address <i>&lt;src-ip&gt;/&lt;src-mask&gt;</i> and next-hop as virtual router <i>&lt;next-hop-vrouter-name&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> that has IP address <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> through interface <i>&lt;interface-name&gt;</i> and gateway <i>&lt;gateway&gt;</i> with metric <i>&lt;route-metric&gt;</i> created.
Meaning	An IPv6 route with the specified IP address have been created.
Action	No recommended action.

Message	IPv6 route in virtual router <i>&lt;vrouter-name&gt;</i> with an IP address <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> and next-hop as virtual router <i>&lt;next-hop-vrouter-name&gt;</i> created.
Meaning	An IPv6 route with the specified IP address have been created.
Action	No recommended action.

Message	IPv6 Route(s) in virtual router <i>&lt;vrouter-name&gt;</i> with an IP address <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> and gateway <i>&lt;gateway&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> that has IP address <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> through interface <i>&lt;interface-name&gt;</i> and gateway <i>&lt;gateway&gt;</i> with metric <i>&lt;route-metric&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> with IP address <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> and next-hop as virtual router <i>&lt;next-hop-vrouter-name&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> with an IP address <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> and gateway <i>&lt;gateway&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> with an IP address <i>&lt;src-ip&gt;/&lt;src-mask&gt;</i> and next-hop as virtual router <i>&lt;next-hop-vrouter-name&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> with route addresses of <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> and a default gateway address of <i>&lt;next-hop-ip-addr&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> with route addresses of <i>&lt;dst-ip&gt;/&lt;dst-mask&gt;</i> through interface <i>&lt;interface-name&gt;</i> and a default gateway address <i>&lt;next-hop-ip-addr&gt;</i> with metric <i>&lt;route-metric&gt;</i> 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 <i>&lt;dst-ip&gt;</i> learned from RA added.
Meaning	A IPv4 default router has been learned and added.
Action	No recommended action.
Message	IPv4 default-router <i>&lt;dst-ip&gt;</i> learned from RA deleted.
Meaning	A IPv4 default router has been learned and added.
Action	No recommended action.
Message	IPv6 default-router <i>&lt;dst-ip&gt;</i> learned from RA added.
Meaning	IPv6 auto-discovered route has been learned and added.
Action	No action is required.
Message	IPv6 default-router <i>&lt;dst-ip&gt;</i> learned from RA deleted.
Meaning	IPv6 auto-discovered route has been learned and deleted.
Action	No action is required.

Message	IPv6 SIBR route in virtual router <i>&lt;vrouter-name&gt;</i> for interface <i>&lt;interface-name&gt;</i> that has IP address <i>&lt;src-ip&gt;/&lt;src-mask&gt;</i> through interface <i>&lt;interface-name2&gt;</i> and gateway <i>&lt;next-hop-ip-addr&gt;</i> with metric <i>&lt;route-metric&gt;</i> created.
Meaning	An administrator created an IPv6 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	IPv6 SIBR Route(s) in virtual router <i>&lt;vrouter-name&gt;</i> for interface <i>&lt;interface-name&gt;</i> with an IP address <i>&lt;src-ip&gt;/&lt;src-mask&gt;</i> and gateway <i>&lt;next-hop-ip-addr&gt;</i> removed.
Meaning	An administrator deleted the specified IPv6 SIBR route.
Action	No recommended action
Message	SIBR route in virtual router <i>&lt;vrouter-name&gt;</i> for interface <i>&lt;interface-name&gt;</i> that has IP address <i>&lt;src-ip&gt;/&lt;src-mask&gt;</i> through interface <i>&lt;interface-name2&gt;</i> and gateway <i>&lt;next-hop-ip-addr&gt;</i> with metric <i>&lt;route-metric&gt;</i> 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 <i>&lt;vrouter-name&gt;</i> for interface <i>&lt;interface-name&gt;</i> with an IP address <i>&lt;src-ip&gt;/&lt;src-mask&gt;</i> and gateway <i>&lt;next-hop-ip-addr&gt;</i> removed.
Meaning	An administrator deleted the specified SIBR route.
Action	No recommended action



## CHAPTER 34

# 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 (00062)

Message	SCCP ALG call flood rate threshold set to default of <i>&lt;calls-per-minute&gt;</i> 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 <i>&lt;calls-per-minute&gt;</i> calls per minute.
---------	---

Meaning	A network administrator set the call flood rate on the device.
---------	--

Action	No recommended action
--------	-----------------------

Message	SCCP ALG inactive media timeout configured to default <i>&lt;inactive-media-timeout&gt;</i> 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 <i>&lt;inactive-media-timeout&gt;</i> 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 <i>&lt;type-of-line-break-proxy-or-rsm&gt;</i> .
Meaning	The device cannot initialize the SCCP ALG service.
Action	No recommended action
Message	SCCP ALG strict parsing disabled on the device.
Message	SCCP ALG strict parsing enabled on the device.
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	Can't allocate memory for SCCP call context.
Message	Can't allocate NAT cookie (Cause is probably too many calls).
Message	SCCP ALG maximum call environment value ( <i>&lt;sccp-max-call-env-value&gt;</i> ) invalid, maximum call number set to <i>&lt;sccp-max-call-value-set&gt;</i> .
Meaning	The SCCP maximum call value is not within the acceptable range
Action	No recommended action

Message	SCCP call from <i>&lt;src-ip&gt;</i> 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 (00062)

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

#### Notification (00561)

Message	SCCP decoder error <i>&lt;msg&gt;</i> .
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 35

# Schedule

The following message relates to schedules created for use in access policies.

### Notification (00020)

Message	Schedule <i>&lt;sched_name&gt;</i> <i>&lt;action_added_modified_deleted&gt;</i> <i>&lt;config_changer&gt;</i> .
Meaning	An admin has added, modified, or deleted the specified schedule.
Action	No recommended action.



## CHAPTER 36

# Service

The following messages relate to user-defined and predefined services, and service groups.

### Notification (00012)

Message	Service group <i>&lt;service_group_name&gt;</i> <i>&lt;config_action_add_delete_modify&gt;</i> <i>&lt;member_name&gt;</i> <i>&lt;config_changer&gt;</i> .
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 <i>&lt;service_group_name&gt;</i> <i>&lt;config_action_add_delete_modify&gt;</i> <i>&lt;config_changer&gt;</i> .
Meaning	An admin has added, modified, or deleted the specified service group.
Action	No recommended action.
Message	Service <i>&lt;service_name&gt;</i> <i>&lt;config_action_add_delete_modify&gt;</i> <i>&lt;config_changer&gt;</i> .
Meaning	An admin has added, modified, or deleted the specified user-defined service.
Action	No recommended action.



## CHAPTER 37

# SSL

The following messages relate to the Secure Socket Layer (SSL) protocol

### Warning (00515)

Message	Admin user <i>&lt;user-name&gt;</i> logged out for Web( <i>&lt;protocol&gt;</i> ) management (port <i>&lt;dst-port&gt;</i> ) from <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i>
Meaning	An admin logged out from the specified username, protocol, address, and port.
Action	No recommended action.

### Warning (00518)

Message	Admin user <i>&lt;user-name&gt;</i> login attempt for Web( <i>&lt;protocol&gt;</i> ) management (port <i>&lt;dst-port&gt;</i> ) from <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i> 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 <i>&lt;user-name&gt;</i> login attempt for Web( <i>&lt;protocol&gt;</i> ) management (port <i>&lt;dst-port&gt;</i> ) from <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i> 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 <i>&lt;user-name&gt;</i> logged in for Web( <i>&lt;protocol&gt;</i> ) management (port <i>&lt;dst-port&gt;</i> ) from <i>&lt;src-ip&gt;</i> : <i>&lt;src-port&gt;</i>
Meaning	An admin logged in using the specified username, protocol, address, and port.
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 <a href="http://www.juniper.net/support">www.juniper.net/support</a> . (Note: You must be a registered Juniper Networks customer.)
Message	User <i>&lt;admin_user&gt;</i> clicked Get Tech on WebUI
Meaning	An admin clicked the "Get Tech" button on the WebUI Help page.
Action	No recommended action.
Message	User <i>&lt;admin_user&gt;</i> 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 <i>&lt;src-port&gt;</i> to <i>&lt;dst-port&gt;</i> <i>&lt;config_changer&gt;</i>
Meaning	An admin has changed the port used for managing the device via Secure Socket Layer (SSL).
Action	No recommended action.
Message	Web SSL <i>&lt;status&gt;</i> <i>&lt;config_changer&gt;</i>
Meaning	An admin has either enabled or disabled an Secure Socket Layer (SSL) connection.
Action	No recommended action.

### Information (00545)

Message	The MD5 hash value generated from the configuration file does not match the MD5 hash value provided!
Meaning	If a user provides MD5 hash of the uploaded configuration file, MD5 hash check will be done on the received configuration file. If the computed MD5 does not match the one provided by the user, the update operation will be terminated.
Action	Ensure that the configuration file received was correct.



## CHAPTER 38

# Syslog and Webtrends

The following messages pertain to configuring and enabling syslog and WebTrends facilities.

### Critical (00019)

Message	SECURITY ALARM is disabled by <i>&lt;user-name&gt;</i> .
Meaning	The security alarm function is disabled.
Action	No recommended action.

Message	SECURITY ALARM is enabled by <i>&lt;user-name&gt;</i> .
Meaning	The security alarm function is enabled.
Action	No recommended action.

### Critical (00020)

Message	<i>&lt;none&gt;</i> System memory is low ( <i>&lt;none&gt;</i> bytes allocated out of <i>&lt;none&gt;</i> bytes) <i>&lt;none&gt;</i> 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	<i>&lt;none&gt;</i> CPU utilization is high ( <i>&lt;none&gt;</i> > alarm threshold: <i>&lt;none&gt;</i> ) <i>&lt;none&gt;</i> 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.

### Critical (00035)

Message	Log queue high watermark reached. Audit loss mitigation starting. New firewall sessions not permitted.(dlog chunk in use: <i>&lt;chunk_in_use&gt;</i> high threshold: <i>&lt;threshold&gt;</i> ).
Meaning	Log queue has reached the high threshold.
Action	Once the high threshold of the log queue reached, please check whether the firewall is properly connected with log destination.
Message	Log queue low watermark reached. Audit loss mitigation ending. New firewall sessions permitted again.(dlog chunk in use: <i>&lt;chunk_in_use&gt;</i> low threshold: <i>&lt;threshold&gt;</i> ).
Meaning	Log queue has reached the low threshold.
Action	none.
Message	<i>&lt;audit-storage-name&gt;</i> audit trail has reached the storage capacity <i>&lt;capacity&gt;</i> .
Meaning	Audit trail has reached the storage capacity.
Action	If the audit trail has reached the storage capacity, check if the audit storage should be cleared.
Message	<i>&lt;audit-storage-name&gt;</i> audit trail has reached the threshold of storage capacity <i>&lt;threshold&gt;</i> (records: <i>&lt;record-number&gt;</i> capacity: <i>&lt;capacity&gt;</i> ).
Meaning	Audit trail has reached the threshold of storage capacity.
Action	If the audit trail has reached the threshold of storage capacity, check if the audit storage should be cleared.

**Critical (00036)**

Message	<i>&lt;none&gt;</i> System memory went to normal ( <i>&lt;none&gt;</i> bytes allocated out of <i>&lt;none&gt;</i> bytes) in 1 minute
Meaning	The number of bytes allocated for system memory has not been larger than the alarm threshold.
Action	none.

**Critical (00037)**

Message	<i>&lt;none&gt;</i> CPU utilization went from high to normal ( <i>&lt;none&gt;</i> is not larger than alarm threshold: <i>&lt;none&gt;</i> ) in 1 minute
Meaning	CPU utilization has not been larger than the alarm threshold.
Action	none.

**Warning (00019)**

Message	Syslog cannot connect to the TCP server <i>&lt;server-ip&gt;</i> ; the connection is closed.
Meaning	The device cannot connect to the syslog server using the TCP transport protocol.
Action	Check the network connections.

Message	WebTrends cannot connect to the TCP server <i>&lt;server-ip&gt;</i> ; the connection is closed.
Meaning	The device cannot connect to the webtrends server using the TCP transport protocol.
Action	Check the network connections.

**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	Admin user <i>&lt;user-name&gt;</i> disable the feature that display alarm on local console regardless of whether an administrator is logged in.
Meaning	Turn off the feature that display alarm on local console regardless of whether an administrator is logged in. The alarm is displayed on local console only when administrator is logged in.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> enable the feature that display alarm on local console regardless of whether an administrator is logged in.
Meaning	Turn on the feature that display alarm on local console regardless of whether an administrator is logged in.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> set the refresh interval to <i>&lt;interval&gt;</i> seconds for security alarm.
Meaning	Set the refresh interval for security alarm.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> turn off the audible feature for security alarm.
Meaning	The audible feature is turned off.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> turn on the audible feature for security alarm.
Meaning	The audible feature is turned on.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> unset the refresh interval.
Meaning	Unset the refresh interval for security alarm. Use the default interval value.
Action	No recommended action.

Message	Admin user <i>&lt;user-name&gt;</i> set exclude rule id <i>&lt;exclude-id&gt;</i>
Meaning	Admin user set exclude configuration.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> set the percentage threshold <i>&lt;threshold&gt;</i> for audit storage
Meaning	Admin user has set audit storage alarm percentage threshold.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> unset exclude rule id <i>&lt;exclude-id&gt;</i>
Meaning	Admin user unset exclude configuration.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> unset the percentage threshold for audit storage
Meaning	Admin user has unset audit storage alarm percentage threshold.
Action	No recommended action.
Message	All logging for webtrends server <i>&lt;server-ip&gt;</i> has been disabled.
Meaning	An admin has either enabled or disabled all logging via webtrends.
Action	No recommended action.
Message	All logging for webtrends server <i>&lt;server-ip&gt;</i> has been enabled.
Meaning	An admin has either enabled or disabled all logging via webtrends.
Action	No recommended action.

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	All webtrends servers were removed.
Meaning	An admin removed all webtrends servers.
Action	No recommended action.
Message	CLI log file size has been set to <i>&lt;size&gt;</i> bytes by admin ' <i>&lt;user-name&gt;</i> '.
Meaning	An admin has changed the maximum CLI log file size.
Action	No recommended action.
Message	CLI logging has been disabled by admin ' <i>&lt;user-name&gt;</i> '.
Meaning	An admin has disabled CLI logging.
Action	No recommended action.
Message	CLI logging has been enabled by admin ' <i>&lt;user-name&gt;</i> '.
Meaning	An admin has enabled CLI logging.
Action	No recommended action.
Message	Event logging for syslog server <i>&lt;server-ip&gt;</i> has been disabled.
Meaning	An admin has either enabled or disabled the syslog facility.
Action	No recommended action.

Message	Event logging for syslog server <i>&lt;server-ip&gt;</i> has been enabled.
Meaning	An admin has either enabled or disabled the syslog facility.
Action	No recommended action.
Message	Event logging for webtrends server <i>&lt;server-ip&gt;</i> has been disabled.
Meaning	An admin has either enabled or disabled event logging via webtrends.
Action	No recommended action.
Message	Event logging for webtrends server <i>&lt;server-ip&gt;</i> has been enabled.
Meaning	An admin has either enabled or disabled event logging via webtrends.
Action	No recommended action.
Message	IDP logging for syslog server <i>&lt;server-ip&gt;</i> 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 <i>&lt;server-ip&gt;</i> has been enabled.
Meaning	An admin has either enabled or disabled IDP logging via syslog.
Action	No recommended action.
Message	IDP logging for webtrends server <i>&lt;server-ip&gt;</i> has been disabled.
Meaning	An admin has either enabled or disabled IDP logging via webtrends.
Action	No recommended action.
Message	IDP logging for webtrends server <i>&lt;server-ip&gt;</i> has been enabled.
Meaning	An admin has either enabled or disabled IDP logging via webtrends.
Action	No recommended action.

Message	<i>&lt;VPN-name&gt;</i> 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 <i>&lt;facility&gt;</i> has been changed to <i>&lt;facility&gt;</i>
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 <i>&lt;facility&gt;</i> has been changed to <i>&lt;facility&gt;</i>
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 <i>&lt;server-ip&gt;</i> host port number has been changed to <i>&lt;dst-port&gt;</i>
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 <i>&lt;server-ip&gt;</i> hostname has been changed to <i>&lt;host-name&gt;</i>
Meaning	An admin has changed the name of the syslog host.
Action	No recommended action.
Message	Syslog server <i>&lt;server-ip&gt;</i> was added.
Meaning	An admin has either added or removed the specified syslog server.
Action	No recommended action.
Message	Syslog server <i>&lt;server-ip&gt;</i> 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 <i>&lt;interface-name&gt;</i>
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	The feature that device serial number is included in log messages has been disabled <i>(user-name)</i>
Meaning	Admin user unset log serial number configuration.
Action	No recommended action.
Message	The feature that device serial number is included in log messages has been enabled <i>(user-name)</i>
Meaning	Admin user set log serial number configuration.
Action	No recommended action.
Message	The traffic/IDP syslog is disabled on backup device <i>(user-name)</i> .
Meaning	An admin has either enabled or disabled traffic/IDP syslog on the backup device.
Action	No recommended action.

Message      The traffic/IDP syslog is enabled on backup device *<user-name>*.  
Meaning      An admin has either enabled or disabled traffic/IDP syslog on the backup device.

Action      No recommended action.

Message      The traffic/IDP webtrends log is disabled on backup device *<user-name>*.  
Meaning      An admin has either enabled or disabled traffic/IDP webtrends log on the backup device.

Action      No recommended action.

Message      The traffic/IDP webtrends log is enabled on backup device *<user-name>*.  
Meaning      An admin has either enabled or disabled traffic/IDP webtrends log on the backup device.

Action      No recommended action.

Message      Traffic logging for syslog server *<server-ip>* 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 *<server-ip>* has been enabled.  
Meaning      An admin has either enabled or disabled traffic logging via syslog.

Action      No recommended action

Message      Traffic logging for webtrends server *<server-ip>* has been disabled.  
Meaning      An admin has either enabled or disabled traffic logging via webtrends.

Action      No recommended action

Message	Traffic logging for webtrends server <i>&lt;server-ip&gt;</i> has been enabled.
Meaning	An admin has either enabled or disabled traffic logging via webtrends.
Action	No recommended action.
Message	Transport protocol for syslog server <i>&lt;server-ip&gt;</i> was changed to <i>&lt;server-ip&gt;</i>
Meaning	An admin changed the transport protocol for syslog messages to either UDP or TCP.
Action	No recommended action.
Message	Transport protocol for webtrends server <i>&lt;server-ip&gt;</i> was changed to <i>&lt;protocol&gt;</i>
Meaning	An admin has changed the transport protocol to either UDP or TCP for webtrends messages.
Action	No recommended action.
Message	WebTrends has been disabled <i>&lt;user-name&gt;</i>
Meaning	An admin has either enabled or disabled the WebTrends facility.
Action	No recommended action.
Message	WebTrends has been enabled <i>&lt;user-name&gt;</i>
Meaning	An admin has either enabled or disabled the WebTrends facility.
Action	No recommended action.
Message	WebTrends host domain name <i>&lt;server-ip&gt;</i> has been changed to <i>&lt;server-ip&gt;</i>
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 server <i>&lt;server-ip&gt;</i> port number has been changed to <i>&lt;dst-port&gt;</i>
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 server <i>&lt;server-ip&gt;</i> was added.
Meaning	An admin has either added or removed the specified webtrends server.
Action	No recommended action.
Message	WebTrends server <i>&lt;server-ip&gt;</i> was removed.
Meaning	An admin has either added or removed the specified webtrends server.
Action	No recommended action.
Message	WebTrends source interface has been changed to <i>&lt;interface-name&gt;</i>
Meaning	An admin has modified the specified source interface.
Action	No recommended action.
Message	WebTrends source interface was removed.
Meaning	An admin has removed the source interface.
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 (00022)

Message	<i>&lt;VPN-name&gt;</i> VPN management tunnel has been disabled.
Meaning	A VPN tunnel for administrative traffic has been disabled.
Action	No recommended action.

### Notification (00628)

Message	Admin user <i>&lt;user-name&gt;</i> add policy group <i>&lt;group-name&gt;</i> .
Meaning	Admin user has set the policy group.
Action	No recommended action.

Message	Admin user <i>&lt;user-name&gt;</i> add policy id <i>&lt;policy-id&gt;</i> into policy group <i>&lt;group-name&gt;</i> .
Meaning	Admin user has set the policy group.
Action	No recommended action.

Message	Admin user <i>&lt;user-name&gt;</i> clear the statistics of policy violation <i>&lt;table-name&gt;</i> table.
Meaning	Admin user has cleared the statistics of some policy violation table.
Action	No recommended action.

Message	Admin user <i>&lt;user-name&gt;</i> delete policy group <i>&lt;group-name&gt;</i> .
Meaning	Admin user has unset policy group.
Action	No recommended action.

Message      Admin user *<user-name>* delete policy id *<policy-id>* from policy group *<group-name>*.

Meaning      Admin user has unset some policy from policy group.

Action        No recommended action.

Message      Admin user *<user-name>* disable overwrite configuration for security alarm

Meaning      Admin user has disabled the security alarm audit trail overwrite configuration.

Action        No recommended action.

Message      Admin user *<user-name>* disable the policy violation analysis mechanisms.

Meaning      Admin user has disabled the policy violation analysis mechanism.

Action        No recommended action.

Message      Admin user *<user-name>* disable the potential security violation analysis mechanisms for *<violation-name>*

Meaning      Admin user has disabled the potential security violation analysis mechanism.

Action        No recommended action.

Message      Admin user *<user-name>* enable overwrite configuration for security alarm

Meaning      Admin user has enabled the security alarm audit trail overwrite configuration.

Action        No recommended action.

Message      Admin user *<user-name>* enable the policy violation analysis mechanisms

Meaning      Admin user has enabled the policy violation analysis mechanism.

Action        No recommended action.

Message	Admin user <i>&lt;user-name&gt;</i> enable the potential security violation analysis mechanisms for <i>&lt;violation-name&gt;</i>
Meaning	Admin user has enabled the potential security violation analysis mechanism.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> has disabled the audit loss mitigation feature.
Meaning	Admin user has disabled the audit loss mitigation feature.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> has enabled the audit loss mitigation feature.
Meaning	Admin user has enabled the audit loss mitigation feature.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> <i>&lt;action&gt;</i> audit trail config
Meaning	Admin user has added, deleted, or edited audit trail configuration.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> set configure by CLI [ <i>&lt;cli-string&gt;</i> ]
Meaning	Admin user has set audit alarm configuration.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> set policy violation duration <i>&lt;duration&gt;</i> .
Meaning	Admin user has set the policy violation duration.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> set policy violation threshold <i>&lt;threshold&gt;</i> .
Meaning	Admin user has set the policy violation threshold.
Action	No recommended action.

Message      Admin user *<user-name>* set *<action>* when audit storage is full  
Meaning      Admin user has set overwrite / drop action when overwrite occurs.

Action      No recommended action.

Message      Admin user *<user-name>* set the size of policy violation *<table-name>*  
table to *<table-size>*

Meaning      Admin user has set the size of policy violation table.

Action      No recommended action.

Message      Admin user *<user-name>* unset policy violation duration.

Meaning      Admin user has unset the policy violation duration.

Action      No recommended action.

Message      Admin user *<user-name>* unset policy violation threshold.

Meaning      Admin user has unset the policy violation threshold.

Action      No recommended action.

Message      Admin user *<user-name>* unset the size of policy violation *<table-name>*  
table.

Meaning      Admin user has unset the size of policy violation table.

Action      No recommended action.

Message      Admin user *<user-name>* view the audit trail

Meaning      Admin user has viewed the audit trail.

Action      No recommended action.

Message	All security alarms are acknowledged by <i>&lt;user-name&gt;</i> .
Meaning	All of security alarms in the security alarm queue are acknowledged by administrator.
Action	No recommended action.
Message	audit log queue <i>&lt;ostor-name&gt;</i> is overwritten
Meaning	This generates an event log entry with the ostor name indicating that the event log is overflowing and begins to overwrite.
Action	Administrator can clean the event log to release more space to save the event log.
Message	Audit trail event storage failure
Meaning	The audit trail log storage failed.
Action	No recommended action.
Message	event log entry for set log exclude-id testing user-id <i>&lt;user-name&gt;</i> , src-ip <i>&lt;none&gt;</i> , dst-ip <i>&lt;src-ip&gt;</i> , dst-port <i>&lt;none&gt;</i> , rule-id <i>&lt;dst-ip&gt;</i> , outcome <i>&lt;dst-port&gt;</i>
Meaning	This generates an event log entry with all fields which test the command "set log exclude-id..." needs.
Action	No recommended action.
Message	EVENT Log <i>&lt;user-name&gt;</i> is excluded by exclude rule <i>&lt;rule-id&gt;</i> .
Meaning	The specified security alarm in the security alarm queue is acknowledged by administrator.
Action	No recommended action.
Message	SECURITY ALARM ACK ID <i>&lt;ack-id&gt;</i> is auto acked
Meaning	When the security alarm queue is full and overwrite is disable, the alarm is auto acked (dropped), an event log is generated.
Action	No recommended action.

Message	SECURITY ALARM ACK ID <i>&lt;ack-id&gt;</i> is overwritten
Meaning	When the security alarm queue is full and overwrite is enable, the alarm will overwrite the oldest one, an event log is generated.
Action	No recommended action.
Message	Security alarm <i>&lt;ack-id&gt;</i> is acknowledged by <i>&lt;user-name&gt;</i> .
Meaning	The specified security alarm in the security alarm queue is acknowledged by administrator.
Action	No recommended action.

#### Notification (00631)

Message	The webtrends server <i>&lt;server-name&gt;</i> is not resolved.
Meaning	A webtrends server configured to a hostname is not resolved.
Action	Check the configuration of the webtrends server.

#### Notification (00632)

Message	The syslog server <i>&lt;server-name&gt;</i> is not resolved.
Meaning	A syslog server is configured to a hostname that cannot be resolved.
Action	Check the configuration of the syslog server.

#### Notification (00767)

Message	Admin user <i>&lt;user-name&gt;</i> set the detail level of traffic log to <i>&lt;detail-level&gt;</i>
Meaning	Admin user has changed the detail level of traffic log.
Action	No recommended action.
Message	Admin user <i>&lt;user-name&gt;</i> viewed the detail level of traffic log
Meaning	Admin user has viewed the detail level of traffic log.
Action	No recommended action.

Message	Alarm log was reviewed <i>&lt;user-name&gt;</i> .
Meaning	The entries in the specified log have been viewed.
Action	No recommended action.
Message	All logged events or alarms were cleared <i>&lt;user-name&gt;</i>
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 <i>&lt;user-name&gt;</i>
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 <i>&lt;user-name&gt;</i>
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 <i>&lt;user-name&gt;</i> .
Meaning	The entries in the specified log have been viewed.
Action	No recommended action.
Message	Event log was reviewed <i>&lt;user-name&gt;</i> .
Meaning	The entries in the specified log have been viewed.
Action	No recommended action.

Message	Log setting was modified to disable <i>&lt;level&gt;</i> level <i>&lt;user-name&gt;</i>
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 <i>&lt;none&gt;</i> level <i>&lt;user-name&gt;</i>
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 <i>&lt;user-name&gt;</i> .
Meaning	The entries in the specified log have been viewed.
Action	No recommended action.
Message	System log was reviewed <i>&lt;user-name&gt;</i> .
Meaning	The entries in the specified log have been viewed.
Action	No recommended action.
Message	The following change was made <i>&lt;user-name&gt;</i> in VSYS <i>&lt;vsys&gt;</i> : <i>&lt;cli-string&gt;</i>
Meaning	An admin made configuration changes.
Action	No recommended action.
Message	Traffic log was reviewed <i>&lt;user-name&gt;</i> .
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. <i>&lt;packet-count&gt;</i> 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 39

# 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 <i>&lt;interface&gt;</i> 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 <i>&lt;interface&gt;</i> link status changed to up.
Meaning	The 802.1x interface is connected.
Action	No recommended action.

### Notification (00614)

Message	[1X] host <i>&lt;host_mac&gt;</i> started authentication on interface <i>&lt;interface&gt;</i> with 802.1X session id <i>&lt;id&gt;</i> .
Meaning	802.1X authentication has started.
Action	No recommended action.

Message	[1X] host <i>&lt;host_mac&gt;</i> failed authentication on interface <i>&lt;interface&gt;</i> with 802.1X session id <i>&lt;id&gt;</i> .
Meaning	802.1X authentication failed.
Action	Confirm that all auth parameters are correct.
Message	[1X] host <i>&lt;host_mac&gt;</i> logged off interface <i>&lt;interface&gt;</i> with 802.1X session id <i>&lt;id&gt;</i> .
Meaning	The client has logged off from authentication.
Action	No recommended action.
Message	[1X] host <i>&lt;host_mac&gt;</i> passed authentication on interface <i>&lt;interface&gt;</i> with 802.1X session id <i>&lt;id&gt;</i> .
Meaning	802.1X authentication has completed.
Action	No recommended action.
Message	[1X] host <i>&lt;host_mac&gt;</i> started re-authentication on interface <i>&lt;interface&gt;</i> with 802.1X session id <i>&lt;id&gt;</i> .
Meaning	802.1X authentication has restarted.
Action	No recommended action.

## CHAPTER 40

# 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 ( <i>shaping-mode</i> ).
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 ( <i>shaping-mode</i> ).
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 41

# 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 <i>&lt;vrrp-group&gt;</i> on interface <i>&lt;interface-name&gt;</i> gives up mastership.
---------	--

Meaning	The specified VRRP group is no longer the master group.
---------	---

Action	No recommended action.
--------	------------------------

Message	VRRP group <i>&lt;vrrp-group&gt;</i> on interface <i>&lt;interface-name&gt;</i> is now the master.
---------	--

Meaning	The specified VRRP group is now the master group.
---------	---

Action	No recommended action.
--------	------------------------

### Notification (00061)

Message	Configuration of VRRP on interface <i>&lt;interface-name&gt;</i> is removed.
---------	--

Meaning	VRRP configuration on the specified interface has been removed.
---------	---

Action	No recommended action.
--------	------------------------

Message	VRRP group <i>&lt;vrrp-group&gt;</i> created on interface <i>&lt;interface-name&gt;</i> .
---------	---

Meaning	A VRRP group has been created on the specified interface.
---------	---

Action	No recommended action.
--------	------------------------

Message	VRRP group <i>&lt;vrrp-group&gt;</i> on interface <i>&lt;interface-name&gt;</i> changed advertisement interval to <i>&lt;interval&gt;</i> seconds.
Meaning	The specified VRRP group has changed its advertisement interval.
Action	No recommended action.
Message	VRRP group <i>&lt;vrrp-group&gt;</i> on interface <i>&lt;interface-name&gt;</i> changed preempt hold on time to <i>&lt;time&gt;</i> seconds.
Meaning	The specified VRRP group has changed its preempt hold time.
Action	No recommended action.
Message	VRRP group <i>&lt;vrrp-group&gt;</i> on interface <i>&lt;interface-name&gt;</i> changed preempt to <i>&lt;none&gt;</i> .
Meaning	The preemption for the specified VRRP group has changed.
Action	No recommended action.
Message	VRRP group <i>&lt;vrrp-group&gt;</i> on interface <i>&lt;interface-name&gt;</i> changed priority to <i>&lt;priority&gt;</i> .
Meaning	The priority level of the specified VRRP group has changed.
Action	No recommended action.
Message	VRRP group <i>&lt;vrrp-group&gt;</i> removed from interface <i>&lt;interface-name&gt;</i> .
Meaning	A VRRP group has been removed on the specified interface.
Action	No recommended action.
Message	VRRP on interface <i>&lt;interface-name&gt;</i> is configured.
Meaning	VRRP on the specified interface has been configured.
Action	No recommended action.

Message	VRRP on interface <i>&lt;interface-name&gt;</i> is disabled.
Meaning	VRRP on the specified interface has been disabled.
Action	No recommended action.
Message	VRRP on interface <i>&lt;interface-name&gt;</i> is enabled.
Meaning	VRRP on the specified interface has been enabled.
Action	No recommended action.



## CHAPTER 42

# Vsys

The following sections provide descriptions of and recommended action for ScreenOS messages displayed for events relating to virtual systems.

### Notification (00032)

Message	Assign shared-DMZ zone <i>&lt;zone-name&gt;</i> to vsys <i>&lt;vsys-name&gt;</i> .
Meaning	A root-level administrator assigned a shared-DMZ zone to the specified vsys.
Action	No recommended action.
Message	Assign shared-DMZ zone <i>&lt;zone-name&gt;</i> to vsys-profile <i>&lt;vsys-profile-name&gt;</i> .
Meaning	A root-level administrator assigned a shared-DMZ zone to the specified vsys-profile.
Action	No recommended action.
Message	ID for vsys <i>&lt;vsys-name&gt;</i> has been changed from <i>&lt;old-id&gt;</i> to <i>&lt;new-id&gt;</i> <i>&lt;config-changer&gt;</i> .
Meaning	A root level administrator changed the name of the specified vsys.
Action	No recommended action.
Message	NSRP VSD group ID for vsys <i>&lt;vsys-name&gt;</i> has been changed from <i>&lt;old-id&gt;</i> to <i>&lt;new-id&gt;</i> <i>&lt;config-changer&gt;</i> .
Meaning	A root level administrator changed the NSRP Virtual Security Device group ID of the specified vsys.
Action	No recommended action.

Message	Reassign shared-DMZ zone <i>&lt;zone-name&gt;</i> from vsys <i>&lt;vsys-name&gt;</i> .
Meaning	A root-level administrator reassigned a shared-DMZ zone from the specified vsys.
Action	No recommended action.
Message	Reassign shared-DMZ zone <i>&lt;zone-name&gt;</i> from vsys-profile <i>&lt;vsys-profile-name&gt;</i> .
Meaning	A root-level administrator reassigned a shared-DMZ zone from the specified vsys-profile.
Action	No recommended action.
Message	Vsys <i>&lt;old-vsys-name&gt;</i> has been changed to <i>&lt;new-vsys-name&gt;</i> <i>&lt;config-changer&gt;</i> .
Meaning	A root level administrator changed the ID of the specified vsys.
Action	No recommended action.
Message	Vsys <i>&lt;vsys-name&gt;</i> has been removed <i>&lt;config-changer&gt;</i>
Meaning	A root level administrator created the specified virtual system (vsys).
Action	No recommended action.
Message	Vsys <i>&lt;vsys-name&gt;</i> profile has been changed from <i>&lt;old_vsys_profile_name&gt;</i> to <i>&lt;new_vsys_profile_name&gt;</i> .
Meaning	The vsys profile name has been changed to a new name.
Action	No recommended action.
Message	Vsys <i>&lt;vsys-name&gt;</i> with profile <i>&lt;vsys-profile-name&gt;</i> has been created <i>&lt;config-changer&gt;</i> .
Meaning	A root level administrator created the specified virtual system (vsys).
Action	No recommended action.

Message	Vsys profile <i>&lt;vsys_profile_name&gt;</i> created with default vsys limits.
Meaning	A vsys profile with default limits has been created.
Action	No recommended action.
Message	Vsys profile <i>&lt;vsys_profile_name&gt;</i> deleted( <i>&lt;config-changer&gt;</i> ).
Meaning	A vsys profile has been deleted.
Action	No recommended action.
Message	Vsys profile <i>&lt;vsys_profile_name&gt;</i> limit <i>&lt;vsys_profile_limit_name&gt;</i> has been set to <i>&lt;vsys_profile_limit_max&gt;</i> <i>&lt;vsys_profile_limit_max_value&gt;</i> <i>&lt;vsys_profile_limit_reserved&gt;</i> <i>&lt;vsys_profile_limit_reserved_value&gt;</i> ( <i>&lt;config-changer&gt;</i> ).
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 <i>&lt;policy-name&gt;</i> .
Meaning	An admin changed the IP classification policy for unclassified traffic.
Action	No recommended action
Message	IP classification has been <i>&lt;state&gt;</i> on zone <i>&lt;zone-name&gt;</i> .
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 <i>&lt;ip-class-mode-name&gt;</i> .
Meaning	An admin changed the IP classification mode.
Action	No recommended action

Message	IP classification object <i>&lt;string_subnet_or_range&gt;</i> has been added on zone <i>&lt;zone-name&gt;</i> .
---------	--

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 <i>&lt;string_subnet_or_range&gt;</i> has been deleted on zone <i>&lt;zone-name&gt;</i> .
---------	--

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 (00515)

Message	Vsys admin user <i>&lt;user-name&gt;</i> logged on via Telnet from remote IP address <i>&lt;remote-ip&gt;</i> using port <i>&lt;remote-port&gt;</i> .
---------	---

Meaning	The named vsys admin logged into the specified vsys via Telnet from the specified IP address, using the specified port number.
---------	--

Action	No recommended action.
--------	------------------------

Message	Vsys admin user <i>&lt;user-name&gt;</i> logged on via the console.
---------	---

Meaning	An admin logged into the specified vsys through a console connection.
---------	---

Action	No recommended action.
--------	------------------------

## CHAPTER 43

# Web Filtering

The following messages relate to events generated during configuration or execution of web filtering.

### Alert (00014)

Message	Communication error with <i>&lt;url-server-vendor-name&gt;</i> server[ <i>&lt;url-server-ip-address&gt;</i> ]: <i>SE(&lt;url-server-code&gt;)</i> <i>SOE(&lt;url-server-code&gt;)</i> <i>ED(&lt;url-server-code&gt;)</i> <i>Comed(&lt;url-server-code&gt;)</i>
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.

### Notification (00013)

Message	<i>&lt;url-filter-state&gt;</i>
Meaning	Web filtering is enabled or disabled for the specified vsys.
Action	No recommended action.
Message	Web filtering socket count is changed to <i>&lt;url-server-timeout&gt;</i> .
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 <i>&lt;interface-name&gt;</i> .
Meaning	The Web filtering interface is modified.
Action	No recommended action.

Message	Web-filtering fail mode is changed to <i>⟨fail-mode-string⟩</i> .
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 <i>⟨message-type-string⟩</i> .
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 <i>⟨url-server-account-name⟩</i> .
Meaning	An admin changed the account name of the Web filtering server.
Action	No recommended action.
Message	Web-filtering server name is changed to <i>⟨url-server-name⟩</i> .
Meaning	An admin changed the host name of the web filtering server.
Action	No recommended action.
Message	Web-filtering server port is changed to <i>⟨url-server-port-number⟩</i> .
Meaning	An admin changed the web filtering server port number.
Action	No recommended action.

Message	Web-filtering timeout is changed to <i>&lt;url-server-timeout&gt;</i> .
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 <i>&lt;url-server-vendor-name&gt;</i> (error <i>Ox&lt;url-server-socket-error&gt;</i> ).
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 <i>&lt;url-server-vendor-name&gt;</i> (error <i>Ox&lt;url-server-socket-error&gt;</i> , flag <i>Ox&lt;url-server-error-flag&gt;</i> , cmd <i>Ox&lt;url-server-failing-cmd&gt;</i> ).
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 <i>&lt;url-server-vendor-name&gt;</i> server (connections <i>&lt;url-server-connection-count&gt;</i> ).
Meaning	The security device established connectivity with the Web filtering server.
Action	No recommended action.

