



## **Cisco Security Appliance Logging Configuration and System Log Messages**

For the Cisco PIX 500 Series and Cisco ASA Series Security Appliance

Software Version 7.2

### **Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Text Part Number: OL-10099-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Cisco Security Appliance Logging Configuration and System Log Messages*  
© 2006 Cisco Systems, Inc. All rights reserved.



## **Preface xxxix**

Document Objectives	xxxix
Audience	xxxix
Document Organization	xi
Document Conventions	xi
Related Documentation	xi
Obtaining Documentation	xi
Cisco.com	xli
Documentation DVD	xli
Ordering Documentation	xli
Documentation Feedback	xlii
Cisco Product Security Overview	xlii
Reporting Security Problems in Cisco Products	xlii
Obtaining Technical Assistance	xliii
Cisco Technical Support Website	xliii
Submitting a Service Request	xliii
Definitions of Service Request Severity	xliv
Obtaining Additional Publications and Information	xliv

---

## **CHAPTER 1**

### **Configuring Logging and SNMP 1-1**

Configuring SNMP	1-1
SNMP Overview	1-1
Enabling SNMP	1-3
Configuring and Managing Logs	1-5
Logging Overview	1-5
Logging in Multiple Context Mode	1-5
Enabling and Disabling Logging	1-6
Enabling Logging to All Configured Output Destinations	1-6
Disabling Logging to All Configured Output Destinations	1-6
Viewing the Log Configuration	1-6
Configuring Log Output Destinations	1-7
Sending System Log Messages to a Syslog Server	1-7
Sending System Log Messages to the Console	1-8
Sending System Log Messages to an E-mail Address	1-8

- Sending System Log Messages to ASDM 1-10
- Sending System Log Messages to a Telnet or SSH Session 1-11
- Sending System Log Messages to the Log Buffer 1-12
- Filtering System Log Messages 1-14
  - Message Filtering Overview 1-14
  - Filtering System Log Messages by Class 1-15
  - Filtering System Log Messages with Custom Message Lists 1-16
- Customizing the Log Configuration 1-18
- Customizing the Log Configuration 1-18
  - Configuring the Logging Queue 1-18
  - Including the Date and Time in System Log Messages 1-18
  - Including the Device ID in System Log Messages 1-19
  - Generating System Log Messages in EMBLEM Format 1-19
  - Disabling a System Log Message 1-20
  - Changing the Severity Level of a System Log Message 1-20
  - Changing the Amount of Internal Flash Memory Available for Logs 1-21
- Understanding System Log Messages 1-22
  - System Log Message Format 1-22
  - Severity Levels 1-23
  - Variables Used in System Log Messages 1-23

**CHAPTER 2**

**System Log Messages 2-1**

- Messages 101001 to 199009 2-1
  - 101001 2-1
  - 101002 2-2
  - 101003, 101004 2-2
  - 101005 2-2
  - 102001 2-2
  - 103001 2-3
  - 103002 2-3
  - 103003 2-4
  - 103004 2-4
  - 103005 2-4
  - 104001, 104002 2-4
  - 104003 2-5
  - 104004 2-5
  - 105001 2-5
  - 105002 2-6
  - 105003 2-6
  - 105004 2-6

105005	2-6
105006, 105007	2-7
105008	2-7
105009	2-7
105010	2-8
105011	2-8
105020	2-8
105021	2-8
105031	2-9
105032	2-9
105034	2-9
105035	2-9
105036	2-9
105037	2-10
105038	2-10
105039	2-10
105040	2-11
105042	2-11
105043	2-11
105044	2-11
105045	2-12
105046	2-12
105047	2-12
105048	2-12
106001	2-13
106002	2-13
106006	2-13
106007	2-14
106010	2-14
106011	2-14
106012	2-14
106013	2-15
106014	2-15
106015	2-15
106016	2-16
106017	2-16
106018	2-16
106020	2-17
106021	2-17
106022	2-17

106023	2-18
106024	2-18
106025, 106026	2-18
106027	2-19
106100	2-19
106101	2-20
107001	2-20
107002	2-20
107003	2-21
108002	2-21
108003	2-21
108004	2-22
108005	2-22
108006	2-23
109001	2-23
109002	2-23
109003	2-24
109005	2-24
109006	2-24
109007	2-24
109008	2-25
109010	2-25
109011	2-25
109012	2-25
109013	2-26
109014	2-26
109016	2-26
109017	2-26
109018	2-27
109019	2-27
109020	2-27
109021	2-27
109022	2-28
109023	2-28
109024	2-28
109025	2-28
109026	2-29
109027	2-29
109028	2-29
109029	2-30

109030	2-30
109031	2-30
109032	2-31
109033	2-31
109034	2-31
110001	2-32
111001	2-32
111002	2-32
111003	2-33
111004	2-33
111005	2-33
111007	2-33
111008	2-34
111009	2-34
111111	2-34
112001	2-34
113001	2-35
113003	2-35
113004	2-35
113005	2-36
113006	2-36
113007	2-36
113008	2-36
113009	2-37
113010	2-37
113011	2-37
113012	2-37
113013	2-38
113014	2-38
113015	2-38
113016	2-38
113017	2-39
113018	2-39
113019	2-39
113020	2-40
114001	2-40
114002	2-41
114003	2-41
114004	2-42
114005	2-42

114006	2-43
114007	2-43
114008	2-44
114009	2-45
114010	2-45
114011	2-46
114012	2-47
114013	2-47
114014	2-48
114015	2-49
114016	2-49
114017	2-50
114018	2-51
114019	2-51
114020	2-52
199001	2-52
199002	2-53
199003	2-53
199005	2-53
199006	2-53
199007	2-54
199008	2-54
199009	2-55
Messages 201002 to 219002	2-55
201002	2-55
201003	2-55
201004	2-56
201005	2-56
201006	2-56
201008	2-57
201009	2-57
201010	2-57
201011	2-58
201012	2-58
201013	2-59
202001	2-59
202005	2-60
202011	2-60
208005	2-60
209003	2-61



209004	2-61
209005	2-61
210001	2-62
210002	2-62
210003	2-62
210005	2-62
210006	2-63
210007	2-63
210008	2-63
210010	2-63
210020	2-64
210021	2-64
210022	2-64
211001	2-64
211003	2-65
212001	2-65
212002	2-65
212003	2-66
212004	2-66
212005	2-66
212006	2-67
213001	2-67
213002	2-67
213003	2-67
213004	2-68
214001	2-68
215001	2-68
217001	2-68
216001	2-69
216002	2-69
216003	2-70
218001	2-70
218002	2-71
218003	2-71
218004	2-71
219002	2-72
Messages 302003 to 335014	2-73
302003	2-73
302004	2-73
302009	2-74

302010	2-74
302012	2-74
302013	2-74
302014	2-75
302015	2-76
302016	2-77
302017	2-77
302018	2-78
302019	2-78
302020	2-79
302021	2-79
302302	2-79
303002	2-79
303004	2-80
303005	2-80
304001	2-81
304002	2-81
304003	2-81
304004	2-81
304005	2-82
304006	2-82
304007	2-82
304008	2-82
304009	2-83
305005	2-83
305006	2-83
305007	2-84
305008	2-84
305009	2-85
305010	2-85
305011	2-85
305012	2-85
308001	2-86
308002	2-86
311001	2-86
311002	2-86
311003	2-87
311004	2-87
312001	2-87
313001	2-87

313004	2-88
313005	2-88
313008	2-88
314001	2-89
315004	2-89
315011	2-90
316001	2-91
317001	2-91
317002	2-92
317003	2-92
317004	2-92
317005	2-92
318001	2-92
318002	2-93
318003	2-93
318004	2-93
318005	2-93
318006	2-93
318007	2-94
318008	2-94
318009	2-94
319001	2-94
319002	2-95
319003	2-95
319004	2-95
320001	2-95
321001	2-96
321002	2-96
321003	2-96
321004	2-96
322001	2-97
322002	2-97
322003	2-97
322004	2-98
323001	2-98
323002	2-98
323003	2-99
323004	2-99
323005	2-100
323006	2-100

324000	2-100
324001	2-101
324002	2-101
324003	2-102
324004	2-102
324005	2-102
324006	2-102
324007	2-103
324300	2-103
324301	2-103
325001	2-104
325002	2-104
325003	2-104
326001	2-104
326002	2-105
326004	2-105
326005	2-105
326006	2-105
326007	2-106
326008	2-106
326009	2-106
326010	2-106
326011	2-107
326012	2-107
326013	2-107
326014	2-107
326015	2-108
326016	2-108
326017	2-108
326019	2-108
326020	2-109
326021	2-109
326022	2-109
326023	2-109
326024	2-110
326025	2-110
326026	2-110
326027	2-110
326028	2-111
327001	2-111

327002	2-111
327003	2-111
328001	2-112
329001	2-112
331001	2-112
331002	2-113
332003	2-113
332004	2-113
333001	2-114
333002	2-114
333003	2-114
333004	2-114
333005	2-115
333006	2-115
333007	2-115
333008	2-115
333009	2-116
333010	2-116
334001	2-116
334002	2-116
334003	2-117
334004	2-117
334005	2-117
334006	2-117
334007	2-118
334008	2-118
335001	2-118
335002	2-118
335003	2-119
335004	2-119
335004	2-119
335005	2-119
335006	2-120
335007	2-120
335008	2-120
335009	2-120
335010	2-121
335011	2-121
335012	2-121
335013	2-121

335014	2-122
Messages 400000 to 450001	2-122
4000nn	2-122
401001	2-125
401002	2-125
401003	2-125
401004	2-125
401005	2-126
402101	2-126
402102	2-126
402103	2-127
402106	2-127
402114	2-127
402115	2-128
402116	2-128
402117	2-129
402118	2-130
402119	2-130
402120	2-131
402123	2-131
403101	2-131
403102	2-132
403103	2-132
403104	2-132
403106	2-132
403107	2-133
403108	2-133
403109	2-133
403110	2-133
403500	2-134
403501	2-134
403502	2-134
403503	2-135
403504	2-135
403505	2-135
403506	2-136
403507	2-136
404101	2-136
404102	2-137
405001	2-137

405101	2-137
405002	2-138
405101	2-138
405102	2-138
405103	2-139
405104	2-139
405105	2-139
405106	2-139
405107	2-140
405201	2-140
405300	2-140
405301	2-141
406001	2-141
406002	2-141
407001	2-142
407002	2-142
407003	2-143
408001	2-143
408002	2-143
408003	2-143
409001	2-144
409002	2-144
409003	2-144
409004	2-144
409005	2-145
409006	2-145
409007	2-145
409008	2-145
409009	2-146
409010	2-146
409011	2-146
409012	2-146
409013	2-147
409023	2-147
410001	2-147
410002	2-147
410003	2-148
410004	2-149
410008	2-149
411001	2-150

411002	2-150
411003	2-150
411004	2-151
412001	2-151
412002	2-151
413001	2-152
413002	2-152
413003	2-152
413004	2-153
414001	2-153
414002	2-154
415001	2-154
415002	2-155
415003	2-155
415004	2-156
415005	2-156
415006	2-157
415007	2-157
415008	2-158
415009	2-158
415010	2-159
415011	2-159
415012	2-160
415013	2-160
415014	2-161
415015	2-161
415016	2-162
415017	2-162
415018	2-163
415019	2-163
415020	2-164
416001	2-164
417001	2-165
417004	2-165
417006	2-165
417008	2-165
417009	2-166
418001	2-166
419001	2-166
419002	2-167



420001	2-167
420002	2-168
420003	2-169
421001	2-169
421002	2-169
421003	2-170
421004	2-170
421005	2-170
421006	2-171
421007	2-171
422004	2-171
422005	2-172
422006	2-172
423001	2-172
423002	2-172
423003	2-173
423004	2-173
423005	2-173
424001	2-173
424002	2-174
431001	2-174
431002	2-175
450001	2-175
Messages 500001 to 509001	2-176
500001	2-176
500002	2-176
500003	2-176
500004	2-177
501101	2-177
502101	2-177
502102	2-177
502103	2-178
502111	2-178
502112	2-178
503001	2-178
504001	2-179
504002	2-179
505001	2-179
505002	2-179
505003	2-179

505004	2-180
505005	2-180
505006	2-180
505007	2-180
505008	2-181
505009	2-181
505010	2-181
505011	2-182
505012	2-182
505013	2-182
506001	2-183
507001	2-183
507002	2-184
508001	2-184
508002	2-184
509001	2-185
Messages 602101 to 622102	2-185
602101	2-185
602103	2-185
602104	2-186
602201	2-186
602202	2-187
602203	2-187
602303	2-187
602304	2-187
603101	2-188
603102	2-188
603103	2-188
603104	2-188
603105	2-189
603106	2-189
603107	2-189
603108	2-189
603109	2-190
604101	2-190
604102	2-190
604103	2-190
604104	2-191
605004	2-191
605005	2-191

606001	2-192
606002	2-192
606003	2-192
606004	2-193
607001	2-193
607002	2-193
607003	2-194
608001	2-195
608002	2-195
608003	2-196
608004	2-196
608005	2-197
609001	2-197
609002	2-197
610001	2-198
610002	2-198
610101	2-198
6108005	2-199
611101	2-199
611102	2-199
611103	2-200
611104	2-200
611301	2-200
611302	2-200
611303	2-200
611304	2-201
611305	2-201
611306	2-201
611307	2-201
611308	2-201
611309	2-202
611310	2-202
611311	2-202
611312	2-202
611313	2-203
611314	2-203
611315	2-203
611316	2-203
611317	2-204
611318	2-204

611319	2-204
611320	2-205
611321	2-205
611322	2-205
611323	2-205
612001	2-206
612002	2-206
612003	2-206
613001	2-206
613002	2-207
613003	2-207
614001	2-207
614002	2-207
615001	2-208
615002	2-208
616001	2-208
617001	2-208
617002	2-209
617003	2-209
617004	2-209
617100	2-209
620001	2-210
620002	2-210
621001	2-210
621002	2-211
621003	2-211
621006	2-211
621007	2-211
621008	2-212
621009	2-212
621010	2-212
622001	2-212
622101	2-213
622102	2-213
Messages 701001 to 726001	2-213
701001	2-214
701002	2-214
702201	2-214
702202	2-214
702203	2-215

702204	2-215
702205	2-215
702206	2-215
702207	2-216
702208	2-216
702209	2-216
702210	2-216
702211	2-217
702212	2-217
702305	2-217
702307	2-217
703001	2-218
703002	2-218
709001, 709002	2-218
709003	2-219
709004	2-219
709005	2-219
709006	2-219
709007	2-220
710001	2-220
710002	2-220
710003	2-220
710004	2-221
710005	2-221
710006	2-222
711001	2-222
711002	2-222
713004	2-222
713006	2-223
713008	2-223
713009	2-223
713010	2-224
713012	2-224
713014	2-224
713016	2-224
713017	2-225
713018	2-225
713020	2-225
713022	2-225
713024	2-226

713025	2-226
713026	2-226
713027	2-226
713028	2-227
713029	2-227
713030	2-227
713031	2-227
713032	2-228
713033	2-228
713034	2-228
713035	2-228
713036	2-229
713037	2-229
713039	2-229
713040	2-229
713041	2-230
713042	2-230
713043	2-230
713047	2-230
713048	2-231
713049	2-231
713050	2-231
713051	2-231
713052	2-231
713056	2-232
713059	2-232
713060	2-232
713061	2-233
713062	2-233
713063	2-233
713065	2-233
713066	2-234
713068	2-234
713072	2-234
713073	2-234
713074	2-235
713075	2-235
713076	2-235
713078	2-235
713081	2-236

713082	2-236
713083	2-236
713084	2-236
713085	2-237
713086	2-237
713088	2-237
713092	2-237
713094	2-238
713098	2-238
713099	2-238
713102	2-238
713103	2-239
713104	2-239
713105	2-239
713107	2-239
713109	2-240
713112	2-240
713113	2-240
713114	2-240
713115	2-241
713116	2-241
713117	2-241
713118	2-241
713119	2-242
713120	2-242
713121	2-242
713122	2-242
713123	2-243
713124	2-243
713127	2-243
713128	2-243
713129	2-244
713130	2-244
713131	2-244
713132	2-244
713133	2-245
713134	2-245
713135	2-245
713136	2-245
713137	2-246

713138	2-246
713139	2-246
713140	2-246
713141	2-247
713142	2-247
713143	2-247
713144	2-248
713145	2-248
713146	2-248
713147	2-248
713148	2-249
713149	2-249
713152	2-249
713154	2-249
713155	2-250
713156	2-250
713157	2-250
713158	2-250
713159	2-251
713160	2-251
713161	2-251
713162	2-252
713163	2-252
713164	2-252
713165	2-252
713166	2-253
713167	2-253
713168	2-253
713169	2-253
713170	2-254
713171	2-254
713172	2-254
713174	2-254
713176	2-255
713177	2-255
713178	2-255
713179	2-255
713182	2-256
713184	2-256
713185	2-256



713186	2-256
713187	2-257
713189	2-257
713190	2-257
713193	2-257
713194	2-258
713195	2-258
713196	2-258
713197	2-258
713198	2-259
713199	2-259
713203	2-259
713204	2-259
713205	2-260
713206	2-260
713208	2-260
713209	2-261
713210	2-261
713211	2-261
713212	2-262
713213	2-262
713214	2-262
713215	2-263
713216	2-263
713217	2-263
713218	2-263
713219	2-264
713220	2-264
713221	2-264
713222	2-264
713223	2-265
713224	2-265
713225	2-265
713226	2-265
713228	2-266
713229	2-266
713230	2-266
713231	2-267
713232	2-267
713233	2-267

713234	2-268
713235	2-268
713236	2-268
713237	2-269
713238	2-269
713239	2-269
713240	2-270
713241	2-270
713242	2-270
713243	2-271
713244	2-271
713245	2-271
713246	2-272
713247	2-272
713248	2-272
713249	2-273
713250	2-273
713251	2-273
713252	2-273
713253	2-274
713900	2-274
713901	2-274
713902	2-275
713903	2-275
713904	2-275
714001	2-275
714002	2-276
714003	2-276
714004	2-276
714005	2-276
714006	2-276
714007	2-277
714011	2-277
715001	2-277
715004	2-277
715005	2-278
715006	2-278
715007	2-278
715008	2-278
715009	2-279

715013	2-279
715019	2-279
715020	2-279
715021	2-280
715022	2-280
715027	2-280
715028	2-280
715033	2-281
715034	2-281
715035	2-281
715036	2-281
715037	2-282
715038	2-282
715039	2-282
715040	2-282
715041	2-283
715042	2-283
715044	2-283
715045	2-283
715046	2-284
715047	2-284
715048	2-284
715049	2-284
715050	2-284
715051	2-285
715052	2-285
715053	2-285
715054	2-285
715055	2-286
715056	2-286
715057	2-286
715058	2-286
715059	2-287
715060	2-287
715061	2-287
715062	2-287
715063	2-288
715064	2-288
715065	2-288
715066	2-288

715067	2-289
715068	2-289
715069	2-289
715070	2-290
715071	2-290
715072	2-290
715074	2-290
715075	2-291
715076	2-291
715077	2-292
715078	2-292
715079	2-293
715080	2-293
716001	2-293
716002	2-293
716003	2-294
716004	2-294
716005	2-295
716006	2-295
716007	2-295
716008	2-295
716009	2-296
716010	2-296
716011	2-296
716012	2-296
716013	2-296
716014	2-297
716015	2-297
716016	2-297
716017	2-297
716018	2-297
716019	2-298
716020	2-298
716021	2-298
716022	2-298
716023	2-298
716024	2-299
716025	2-299
716026	2-299
716027	2-299

716028	2-300
716029	2-300
716030	2-300
716031	2-301
716032	2-301
716033	2-301
716034	2-301
716035	2-302
716036	2-302
716037	2-302
716038	2-302
716039	2-303
716040	2-303
716041	2-303
716042	2-303
716043	2-304
716044	2-304
716045	2-304
716046	2-305
716047	2-305
716048	2-305
716049	2-306
716050	2-306
716051	2-306
716052	2-306
716053	2-307
716054	2-307
716055	2-307
716056	2-308
716090	2-308
716091	2-309
717001	2-309
717002	2-309
717003	2-310
717004	2-310
717005	2-310
717006	2-310
717007	2-311
717008	2-311
717009	2-311

717010	2-311
717011	2-312
717012	2-312
717013	2-312
717014	2-313
717015	2-313
717016	2-313
717017	2-314
717018	2-314
717019	2-314
717021	2-315
717022	2-315
717023	2-315
717024	2-316
717025	2-316
717026	2-316
717027	2-317
717028	2-317
717029	2-317
717030	2-318
717031	2-318
717032	2-318
717033	2-319
717034	2-319
717035	2-319
717036	2-319
717037	2-320
717038	2-320
718001	2-320
718002	2-321
718003	2-321
718004	2-321
718005	2-321
718006	2-322
718007	2-322
718008	2-322
718009	2-322
718010	2-323
718011	2-323
718012	2-323

718013	2-323
718014	2-323
718015	2-324
718016	2-324
718017	2-324
718018	2-324
718019	2-325
718020	2-325
718021	2-325
718022	2-325
718023	2-325
718024	2-326
718025	2-326
718026	2-326
718027	2-326
718028	2-327
718029	2-327
718030	2-327
718031	2-327
718032	2-327
718033	2-328
718034	2-328
718035	2-328
718036	2-328
718037	2-329
718038	2-329
718039	2-329
718040	2-329
718041	2-330
718042	2-330
718043	2-330
718044	2-330
718045	2-330
718046	2-331
718047	2-331
718048	2-331
718049	2-331
718050	2-331
718051	2-332
718052	2-332

718053	2-332
718054	2-332
718055	2-332
718056	2-333
718057	2-333
718058	2-333
718059	2-333
718060	2-334
718061	2-334
718062	2-334
718063	2-334
718064	2-335
718065	2-335
718066	2-335
718067	2-335
718068	2-336
718069	2-336
718070	2-336
718071	2-336
718072	2-336
718073	2-337
718074	2-337
718075	2-337
718076	2-337
718077	2-338
718078	2-338
718079	2-338
718080	2-338
718081	2-339
718084	2-339
718085	2-339
718086	2-339
718087	2-340
718088	2-340
719001	2-340
719002	2-340
719003	2-341
719004	2-341
719005	2-341
719006	2-341



719007	2-342
719008	2-342
719009	2-342
719010	2-342
719011	2-343
719012	2-343
719013	2-343
719014	2-344
719015	2-344
719016	2-344
719017	2-345
719018	2-345
719019	2-345
719020	2-345
719021	2-346
719022	2-346
719023	2-346
719024	2-346
719025	2-347
719026	2-347
720001	2-347
720002	2-347
720003	2-348
720004	2-348
720005	2-348
720006	2-348
720007	2-349
720008	2-349
720009	2-349
720010	2-349
720011	2-350
720012	2-350
720013	2-350
720014	2-350
720015	2-351
720016	2-351
720017	2-351
720018	2-351
720019	2-352
720020	2-352

720021	2-352
720022	2-352
720023	2-353
720024	2-353
720025	2-353
720026	2-354
720027	2-354
720028	2-354
720029	2-354
720030	2-355
720031	2-355
720032	2-355
720033	2-356
720034	2-356
720035	2-356
720036	2-357
720037	2-357
720038	2-357
720039	2-358
720040	2-358
720041	2-358
720042	2-359
720043	2-359
720044	2-359
720045	2-360
720046	2-360
720047	2-360
720048	2-361
720049	2-361
720050	2-361
720051	2-362
720052	2-362
720053	2-362
720054	2-363
720055	2-363
720056	2-363
720057	2-364
720058	2-364
720059	2-364
720060	2-364

720061	2-365
720062	2-365
720063	2-365
720064	2-366
720065	2-366
720066	2-366
720067	2-367
720068	2-367
720069	2-367
720070	2-368
720071	2-368
720072	2-368
720073	2-369
722001	2-369
722002	2-369
722003	2-369
722004	2-370
722005	2-370
722006	2-370
722007	2-370
722008	2-371
722009	2-371
722010	2-371
722011	2-372
722012	2-372
722013	2-372
722014	2-373
722015	2-373
722016	2-374
722017	2-374
722018	2-374
722019	2-374
722020	2-375
722021	2-375
722022	2-375
722023	2-375
722024	2-376
722025	2-376
722026	2-376
722027	2-376

722028	2-377
722029	2-377
722030	2-377
722031	2-378
722032	2-378
722033	2-378
722034	2-378
722035	2-379
722036	2-379
722037	2-379
722038	2-380
722039	2-380
723002	2-380
723003	2-381
723004	2-381
723005	2-382
723006	2-382
723007	2-382
723008	2-383
723009	2-383
723010	2-384
723011	2-384
723012	2-385
723013	2-385
723014	2-386
724001	2-386
724002	2-386
725001	2-387
725002	2-387
725003	2-387
725004	2-388
725005	2-388
725006	2-388
725007	2-389
725008	2-389
725009	2-389
725010	2-390
725011	2-390
725012	2-390
725013	2-390

725014 2-391

726001 2-391

---

**APPENDIX A****Messages Listed by Severity Level A-1**

Alert Messages, Severity 1 A-1

Critical Messages, Severity 2 A-3

Error Messages, Severity 3 A-4

Warning Messages, Severity 4 A-14

Notification Messages, Severity 5 A-22

Informational Messages, Severity 6 A-29

Debugging Messages, Severity 7 A-40

---

**INDEX**





## Preface

---

This preface describes:

- [Document Objectives, page xxxix](#)
- [Audience, page xxxix](#)
- [Document Organization, page xl](#)
- [Document Conventions, page xl](#)
- [Related Documentation, page xl](#)
- [Obtaining Documentation, page xl](#)
- [Obtaining Technical Assistance, page xliii](#)

## Document Objectives

This guide describes the system log (syslog) messages generated by the security appliance software. Messages that display on the console from non-syslog errors are not listed.

This guide describes the system log (syslog) messages generated by the Cisco Security Appliance software Version 7.0. Messages that display on the console from non-syslog errors are not listed.

## Audience

This guide is intended for network managers who perform any of the following tasks:

- Managing network security
- Configuring, administering, and troubleshooting firewalls

This guide assumes that you are familiar with the commands and configuration options described in the *Cisco Security Appliance Command Reference*. In addition, you should be familiar with the network within which the security appliance operates.

# Document Organization

This guide is organized as follows:

- [Chapter 1, “Configuring Logging and SNMP”](#) describes the system log message function, and explains the format of log messages.
- [Chapter 2, “System Log Messages”](#) lists the system log messages, indicates the probable cause of each message, and provides instructions for resolving the condition that caused the log message.
- [Appendix A, “Messages Listed by Severity Level”](#) lists message numbers and text by each severity level.

# Document Conventions

This guide uses the following conventions:

- Filenames, directory names, and arguments for which you supply values are in *italics*.
- The symbol ^ represents the key labeled **Ctrl** (control). To enter a control key; for example, ^z, hold down the **Ctrl** key while you press the **z** key.
- Command names, keys, buttons, and keywords in text are shown in **boldface**. The security appliance commands are described in detail in the *Cisco Security Appliance Command Reference*.
- Variables in command syntax descriptions are shown in *italics*. Command options in square brackets [ ] can be optionally entered, and parameters separated by a vertical bar (|) require you to enter one parameter, but not the other(s).
- Examples depict screen displays and the command line in *screen* font.
- Information you need to enter in examples is shown in **boldface screen** font.
- Variables that require you to supply a value are shown in *italic screen* font.
- Selecting a menu item (or screen) is indicated by the following convention:  
Click **screen1>screen2>screen3**.

**Note**

---

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

---

# Related Documentation

Use this document with the security appliance documentation set, which is available online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix\\_sw/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix_sw/index.htm)

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.



## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



### Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

### Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



#### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

### Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>





# Configuring Logging and SNMP

---

This chapter describes how to configure logging and SNMP. It also describes the contents of system log messages and the system log message format. This chapter does not provide comprehensive information about all monitoring and logging commands and options. For detailed descriptions and additional commands, see the *Cisco Security Appliance Command Reference*.

This chapter includes the following sections:

- [Configuring SNMP, page 1-1](#)
- [Configuring and Managing Logs, page 1-5](#)

## Configuring SNMP

This section describes how to use SNMP and includes the following topics:

- [SNMP Overview, page 1-1](#)
- [Enabling SNMP, page 1-3](#)

## SNMP Overview

The security appliance provides support for network monitoring using SNMP V1 and V2c. The security appliance supports traps and SNMP read access, but does not support SNMP write access.

You can configure the security appliance to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the security appliance. MIBs are a collection of definitions, and the security appliance maintains a database of values for each definition. Browsing a MIB entails issuing an SNMP get request from the NMS. Use CiscoWorks for Windows or any other SNMP V1, MIB-II compliant browser to receive SNMP traps and browse a MIB.

**Table 1-1** lists supported MIBs and traps for the security appliance and, in multiple mode, for each context. You can download Cisco MIBs from the following website.

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

After you download the MIBs, compile them for your NMS.

Table 1-1 SNMP MIB and Trap Support

MIB or Trap Support	Description
SNMP core traps	<p>The security appliance sends the following core SNMP traps:</p> <ul style="list-style-type: none"> <li>• authentication—An SNMP request fails because the NMS did not authenticate with the correct community string.</li> <li>• linkup—An interface has transitioned to the “up” state.</li> <li>• linkdown—An interface is down, for example, if you removed the <b>nameif</b> command.</li> <li>• coldstart—The security appliance is running after a reload.</li> </ul>
MIB-II	<p>The security appliance supports browsing of the following groups and tables:</p> <ul style="list-style-type: none"> <li>• system</li> </ul>
IF-MIB	<p>The Cisco ASA supports browsing of the following tables:</p> <ul style="list-style-type: none"> <li>• ifTable</li> <li>• ifXTable</li> </ul>
RFC1213-MIB	<p>The Cisco ASA supports browsing of the following table:</p> <ul style="list-style-type: none"> <li>• ip.ipAddrTable</li> </ul>
SNMPv2-MIB	<p>The Cisco ASA supports browsing the following:</p> <ul style="list-style-type: none"> <li>• snmp</li> </ul>
ENTITY-MIB	<p>The security appliance supports browsing of the following groups and tables:</p> <ul style="list-style-type: none"> <li>• entPhysicalTable</li> <li>• entLogicalTable</li> </ul> <p>The security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• config-change</li> <li>• fru-insert</li> <li>• fru-remove</li> </ul>
CISCO-IPSEC-FLOW-MONITOR-MIB	<p>The security appliance supports browsing of the MIB.</p> <p>The security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• start</li> <li>• stop</li> </ul>
CISCO-REMOTE-ACCESS-MONITOR-MIB	<p>The security appliance supports browsing of the MIB.</p> <p>The security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• session-threshold-exceeded</li> </ul>
CISCO-CRYPTO-ACCELERATOR-MIB	<p>The security appliance supports browsing of the MIB.</p>
ALTIGA-GLOBAL-REG	<p>The security appliance supports browsing of the MIB.</p>



Table 1-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
Cisco Firewall MIB	The security appliance supports browsing of the following groups: <ul style="list-style-type: none"> <li>cfwSystem The information is cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context.</li> </ul>
Cisco Memory Pool MIB	The security appliance supports browsing of the following table: <ul style="list-style-type: none"> <li>ciscoMemoryPoolTable—The memory usage described in this table applies only to the security appliance general-purpose processor, and not to the network processors.</li> </ul>
Cisco Process MIB	The security appliance supports browsing of the following table: <ul style="list-style-type: none"> <li>cpmCPUTotalTable</li> </ul>
Cisco Syslog MIB	The security appliance supports the following trap: <ul style="list-style-type: none"> <li>clogMessageGenerated</li> </ul> You cannot browse this MIB.

## Enabling SNMP

The SNMP agent that runs on the security appliance performs two functions:

- Replies to SNMP requests from NMSs.
- Sends traps (event notifications) to NMSs.

To enable the SNMP agent and identify an NMS that can connect to the security appliance, follow these steps:

**Step 1** Ensure that the SNMP server on the security appliance is enabled by entering the following command:

```
hostname(config)# snmp-server enable
```

The SNMP server is enabled by default.

**Step 2** To identify the IP address of the NMS that can connect to the security appliance, enter the following command:

```
hostname(config)# snmp-server host interface_name ip_address [trap | poll]
[community text] [version {1 | 2c}] [udp-port port]
```

Specify **trap** or **poll** if you want to limit the NMS to receiving traps only or browsing (polling) only. By default, the NMS can use both functions.

SNMP traps are sent on UDP port 162 by default. You can change the port number using the **udp-port** keyword.

**Step 3** To specify the community string, enter the following command:

```
hostname(config)# snmp-server community key
```

The SNMP community string is a shared secret between the security appliance and the NMS. The key is a case-sensitive value up to 32 characters in length. Spaces are not permitted.

**Step 4** (Optional) To set the SNMP server location or contact information, enter the following command:

```
hostname(config)# snmp-server {contact | location} text
```

**Step 5** To enable the security appliance to send traps to the NMS, enter the following command:

```
hostname(config)# snmp-server enable traps [all | syslog | snmp [trap] [...] |  
entity [trap] [...] | ipsec [trap] [...] | remote-access [trap]]
```

Enter this command for each feature type to enable individual traps or sets of traps, or enter the **all** keyword to enable all traps.

The default configuration has all **snmp** traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart**). You can disable these traps using the **no** form of this command with the **snmp** keyword. However, the **clear configure snmp-server** command restores the default enabling of SNMP traps.

If you enter this command and do not specify a trap type, then the default is **syslog**. (The default **snmp** traps continue to be enabled along with the **syslog** trap.)

Traps for **snmp** include:

- **authentication**
- **linkup**
- **linkdown**
- **coldstart**

Traps for **entity** include:

- **config-change**
- **fru-insert**
- **fru-remove**

Traps for **ipsec** include:

- **start**
- **stop**

Traps for remote-access include:

- **session-threshold-exceeded**

Traps for NAC include:

- **eap**
- **eapoudp**
- **nac**

**Step 6** To enable system messages to be sent as traps to the NMS, enter the following command:

```
hostname(config)# logging history level
```

You must also enable **syslog** traps using the preceding **snmp-server enable traps** command.

**Step 7** To enable logging, so system messages are generated and can then be sent to an NMS, enter the following command:

```
hostname(config)# logging enable
```

---

The following example sets the security appliance to receive requests from host 192.168.3.2 on the inside interface.

```
hostname(config)# snmp-server host 192.168.3.2
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact Pat lee
hostname(config)# snmp-server community ohwhatakeyisthee
```

## Configuring and Managing Logs

This section describes the logging functionality and configuration. It also describes the system log message format, options and variables.

- [Logging Overview, page 1-5](#)
- [Logging in Multiple Context Mode, page 1-5](#)
- [Enabling and Disabling Logging, page 1-6](#)
- [Configuring Log Output Destinations, page 1-7](#)
- [Filtering System Log Messages, page 1-14](#)
- [Customizing the Log Configuration, page 1-18](#)
- [Understanding System Log Messages, page 1-22](#)

## Logging Overview

The security appliance system logs provide you with information for monitoring and troubleshooting the security appliance. Using the logging feature, you can do the following:

- Specify which system log messages should be logged.
- Disable or change the severity level of a system log message.
- Specify one or more locations where system log messages should be sent, including an internal buffer, one or more syslog servers, ASDM, an SNMP management station, specified e-mail addresses, or to Telnet and SSH sessions.
- Configure and manage system log messages in groups, such as by severity level or class of message.
- Specify what happens to the contents of the internal buffer when the buffer becomes full: overwrite the buffer, send the buffer contents to an FTP server, or save the contents to internal Flash memory.

You can choose to send all system log messages, or subsets of system log messages, to any or all output locations. You can filter which system log messages are sent to which locations by the severity of the system log message, the class of the system log message, or by creating a custom log message list.

## Logging in Multiple Context Mode

Each security context includes its own logging configuration and generates its own messages. If you log in to the system or admin context, and then change to another context, messages you view in your session are only those that are related to the current context.

System messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure logging or view any logging information in the system execution space.

You can configure the security appliance to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID. For more information about enabling logging device IDs, see the [“Including the Device ID in System Log Messages”](#) section on page 1-19.

## Enabling and Disabling Logging

This section describes how to enable and disable logging on the security appliance. It includes the following sections:

- [Enabling Logging to All Configured Output Destinations](#), page 1-6
- [Disabling Logging to All Configured Output Destinations](#), page 1-6
- [Viewing the Log Configuration](#), page 1-6

### Enabling Logging to All Configured Output Destinations

The following command enables logging; however, you must also specify at least one output destination so that you can view or save the logged messages. If you do not specify an output destination, the security appliance does not save system log messages generated when events occur.

For more information about configuring log output destinations, see the [“Configuring Log Output Destinations”](#) section on page 1-7.

To enable logging, enter the following command:

```
hostname(config)# logging enable
```

### Disabling Logging to All Configured Output Destinations

To disable all logging to all configured log output destinations, enter the following command:

```
hostname(config)# no logging enable
```

### Viewing the Log Configuration

To view the running log configuration, enter the following command:

```
hostname(config)# show logging
```

The output of the **show logging** command is similar to the following:

```
Syslog logging: enabled
  Facility: 16
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: level errors, facility 16, 3607 messages logged
    Logging to infrastructure 10.1.2.3
  History logging: disabled
```

```
Device ID: 'inside' interface IP address "10.1.1.1"  
Mail logging: disabled  
ASDM logging: disabled
```

## Configuring Log Output Destinations

This section describes how to specify where the security appliance should save or send the log messages it generates. To view logs generated by the security appliance, you must specify a log output destination. If you enable logging without specifying a log output destination, the security appliance generates messages but does not save them to a location from which you can view them.

This section includes the following topics:

- [Sending System Log Messages to a Syslog Server, page 1-7](#)
- [Sending System Log Messages to the Console, page 1-8](#)
- [Sending System Log Messages to an E-mail Address, page 1-8](#)
- [Sending System Log Messages to ASDM, page 1-10](#)
- [Sending System Log Messages to the Log Buffer, page 1-12](#)

## Sending System Log Messages to a Syslog Server

This section describes how to configure the security appliance to send logs to a syslog server.

Configuring the security appliance to send logs to a syslog server enables you to archive logs, limited only by the available disk space on the server, and it enables you to manipulate log data after it is saved. For example, you could specify actions to be executed when certain types of system log messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

The syslog server must run a program (known as a server) called syslogd. UNIX provides a syslog server as part of its operating system. For Windows 95 and Windows 98, obtain a syslogd server from another vendor.



### Note

To start logging to a syslog server you define in this procedure, be sure to enable logging for all output locations. See the [“Enabling Logging to All Configured Output Destinations”](#) section on page 1-6. To disable logging, see the [“Disabling Logging to All Configured Output Destinations”](#) section on page 1-6.

To configure the security appliance to send system log messages to a syslog server, perform the following steps:

**Step 1** To designate a syslog server to receive the logs, enter the following command:

```
hostname(config)# logging host interface_name ip_address [tcp[/port] | udp[/port]]  
[format emblem]
```

Where the **format emblem** keyword enables EMBLEM format logging for the syslog server. (UDP only).

The *interface\_name* argument specifies the interface through which you access the syslog server.

The *ip\_address* argument specifies the IP address of the syslog server.

The `tcp[/port]` or `udp[/port]` argument specifies that the security appliance should use TCP or UDP to send system log messages to the syslog server. The default protocol is UDP. You can configure the security appliance to send data to a syslog server using either UDP or TCP, but not both. If you specify TCP, the security appliance discovers when the syslog server fails and discontinues sending logs. If you specify UDP, the security appliance continues to send logs regardless of whether the syslog server is operational. The `port` argument specifies the port that the syslog server listens to for system log messages. Valid port values are 1025 through 65535, for either protocol. The default UDP port is 514. The default TCP port is 1470.

For example:

```
hostname(config)# logging host dmz1 192.168.1.5
```

If you want to designate more than one syslog server as an output destination, enter a new command for each syslog server.

- Step 2** To specify which system log messages should be sent to the syslog server, enter the following command:

```
hostname(config)# logging trap {severity_level | message_list}
```

Where the `severity_level` argument specifies the severity levels of messages to be sent to the syslog server. You can specify the severity level number (0 through 7) or name. For severity level names, see the “[Severity Levels](#)” section on page 1-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The `message_list` argument specifies a customized message list that identifies the system log messages to send to the syslog server. For information about creating custom message lists, see the “[Filtering System Log Messages with Custom Message Lists](#)” section on page 1-16.

The following example specifies that the security appliance should send to the syslog server all system log messages with a severity level of level 3 (errors) and higher. The security appliance will send messages with the severity of 3, 2, and 1.

```
hostname(config)# logging trap errors
```

- Step 3** (Optional) If needed, set the logging facility to a value other than its default of 20 by entering the following command:

```
hostname(config)# logging facility number
```

Most UNIX systems expect the system log messages to arrive at facility 20.

## Sending System Log Messages to the Console

## Sending System Log Messages to an E-mail Address

You can configure the security appliance to send some or all system log messages to an e-mail address. When sent by e-mail, a system log message appears in the subject line of the e-mail message. For this reason, we recommend configuring this option to notify administrators of system log messages with high severity levels, such as critical, alert, and emergency.

**Note**

To start logging to an e-mail address you define in this procedure, be sure to enable logging for all output locations. See the “[Enabling Logging to All Configured Output Destinations](#)” section on page 1-6. To disable logging, see the “[Disabling Logging to All Configured Output Destinations](#)” section on page 1-6.

To designate an e-mail address as an output destination, perform the following steps:

- Step 1** To specify the system log messages to be sent to one or more e-mail addresses, enter the following command:

```
hostname(config)# logging mail {severity_level | message_list}
```

Where the *severity\_level* argument specifies the severity levels of messages to be sent to the e-mail address. You can specify the severity level number (0 through 7) or name. For severity level names, see the “[Severity Levels](#)” section on page 1-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message\_list* argument specifies a customized message list that identifies the system log messages to send to the e-mail address. For information about creating custom message lists, see the “[Filtering System Log Messages with Custom Message Lists](#)” section on page 1-16.

The following example uses a *message\_list* with the name “high-priority,” previously set up with the **logging list** command:

```
hostname(config)# logging mail high-priority
```

- Step 2** To specify the source e-mail address to be used when sending system log messages to an e-mail address, enter the following command:

```
hostname(config)# logging from-address email_address
```

For example:

```
hostname(config)# logging from-address xxx-001@example.com
```

- Step 3** Specify the recipient e-mail address to be used when sending system log messages to an e-mail destination. You can configure up to five recipient addresses. You must enter each recipient separately.

To specify a recipient address, enter the following command:

```
hostname(config)# logging recipient-address e-mail_address [severity_level]
```

If a severity level is not specified, the default severity level is used (error condition, severity level 3).

For example:

```
hostname(config)# logging recipient-address admin@example.com
```

- Step 4** To specify the SMTP server to be used when sending system log messages to an e-mail destination, enter the following command:

```
hostname(config)# smtp-server ip_address
```

For example:

```
hostname(config)# smtp-server 10.1.1.1
```

## Sending System Log Messages to ASDM

You can configure the security appliance to send system log messages to ASDM. The security appliance sets aside a buffer area for system log messages waiting to be sent to ASDM and saves messages in the buffer as they occur. The ASDM log buffer is a different buffer than the internal log buffer. For information about the internal log buffer, see the [“Sending System Log Messages to the Log Buffer” section on page 1-12](#).

When the ASDM log buffer is full, the security appliance deletes the oldest system log message to make room in the buffer for new system log messages. To control the number of system log messages retained in the ASDM log buffer, you can change the size of the buffer.

This section includes the following topics:

- [Configuring Logging for ASDM, page 1-10](#)
- [Clearing the ASDM Log Buffer, page 1-11](#)

### Configuring Logging for ASDM



#### Note

To start logging to ASDM as defined in this procedure, be sure to enable logging for all output locations. See the [“Enabling Logging to All Configured Output Destinations” section on page 1-6](#). To disable logging, see the [“Disabling Logging to All Configured Output Destinations” section on page 1-6](#).

To specify ASDM as an output destination, perform the following steps:

**Step 1** To specify which system log messages should go to ASDM, enter the following command:

```
hostname(config)# logging asdm {severity_level | message_list}
```

Where the *severity\_level* argument specifies the severity levels of messages to be sent to ASDM. You can specify the severity level number (0 through 7) or name. For severity level names, see the [“Severity Levels” section on page 1-23](#). For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message\_list* argument specifies a customized message list that identifies the system log messages to send to ASDM. For information about creating custom message lists, see the [“Filtering System Log Messages with Custom Message Lists” section on page 1-16](#).

The following example shows how enable logging and send to the ASDM log buffer system log messages of severity levels 0, 1, and 2.

```
hostname(config)# logging asdm 2
```

**Step 2** To specify the number of system log messages retained in the ASDM log buffer, enter the following command:

```
hostname(config)# logging asdm-buffer-size num_of_msgs
```

Where *num\_of\_msgs* specifies the number of system log messages that the security appliance retains in the ASDM log buffer.

The following example shows how to set the ASDM log buffer size to 200 system log messages.

```
hostname(config)# logging asdm-buffer-size 200
```



## Clearing the ASDM Log Buffer

To erase the current contents of the ASDM log buffer, enter the following command:

```
hostname(config)# clear logging asdm
```

## Sending System Log Messages to a Telnet or SSH Session

Viewing system log messages in a Telnet or SSH session requires two steps:

1. Specify which messages should be sent to Telnet or SSH sessions.
2. View logs in the current session.

This section includes the following topics:

- [Configuring Logging for Telnet and SSH Sessions, page 1-11](#)
- [Viewing System Log Messages in the Current Session, page 1-11](#)

## Configuring Logging for Telnet and SSH Sessions



### Note

To start logging to a Telnet or SSH session as defined in this procedure, be sure to enable logging for all output locations. See the [“Enabling Logging to All Configured Output Destinations”](#) section on page 1-6. To disable logging, see the [“Disabling Logging to All Configured Output Destinations”](#) section on page 1-6.

To specify which messages should be sent to Telnet or SSH sessions, enter the following command:

```
hostname(config)# logging monitor {severity_level | message_list}
```

Where the *severity\_level* argument specifies the severity levels of messages to be sent to the session. You can specify the severity level number (0 through 7) or name. For severity level names, see the [“Severity Levels”](#) section on page 1-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message\_list* argument specifies a customized message list that identifies the system log messages to send to the session. For information about creating custom message lists, see the [“Filtering System Log Messages with Custom Message Lists”](#) section on page 1-16.

## Viewing System Log Messages in the Current Session

- Step 1** After you log in to the security appliance, enable logging to the current session by entering the following command:

```
hostname# terminal monitor
```

This command enables logging only for the current session. If you log out, and then log in again, you need to reenter this command.

- Step 2** To disable logging to the current session, enter the following command:

```
hostname(config)# terminal no monitor
```

## Sending System Log Messages to the Log Buffer

If configured as an output destination, the log buffer serves as a temporary storage location for system log messages. New messages are appended to the end of the listing. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated, unless you configure the security appliance to save the full buffer to another location.

This section includes the following topics:

- [Enabling the Log Buffer as an Output Destination, page 1-12](#)
- [Viewing the Log Buffer, page 1-12](#)
- [Automatically Saving the Full Log Buffer to Flash Memory, page 1-13](#)
- [Automatically Saving the Full Log Buffer to an FTP Server, page 1-13](#)
- [Saving the Current Contents of the Log Buffer to Internal Flash Memory, page 1-14](#)
- [Clearing the Contents of the Log Buffer, page 1-14](#)

### Enabling the Log Buffer as an Output Destination



#### Note

To start logging to the buffer as defined in this procedure, be sure to enable logging for all output locations. See the [“Enabling Logging to All Configured Output Destinations”](#) section on page 1-6. To disable logging, see the [“Disabling Logging to All Configured Output Destinations”](#) section on page 1-6.

To enable the log buffer as a log output destination, enter the following command:

```
hostname(config)# logging buffered {severity_level | message_list}
```

Where the *severity\_level* argument specifies the severity levels of messages to be sent to the buffer. You can specify the severity level number (0 through 7) or name. For severity level names, see the [“Severity Levels”](#) section on page 1-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message\_list* argument specifies a customized message list that identifies the system log messages to send to the buffer. For information about creating custom message lists, see the [“Filtering System Log Messages with Custom Message Lists”](#) section on page 1-16.

For example, to specify that messages with severity levels 1 and 2 should be saved in the log buffer, enter one of the following commands:

```
hostname(config)# logging buffered critical
```

or

```
hostname(config)# logging buffered level 2
```

For the *message\_list* option, specify the name of a message list containing criteria for selecting messages to be saved in the log buffer.

```
hostname(config)# logging buffered notif-list
```

### Viewing the Log Buffer

To view the log buffer, enter the following command:

```
hostname(config)# show logging
```

## Changing the Log Buffer Size

By default, the log buffer size is 4 KB. To change the size of the log buffer, enter the following command:

```
hostname(config)# logging buffer-size bytes
```

Where the *bytes* argument sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the security appliance uses 8 KB of memory for the log buffer.

The following example specifies that the security appliance uses 16 KB of memory for the log buffer:

```
hostname(config)# logging buffer-size 16384
```

## Automatically Saving the Full Log Buffer to Flash Memory

Unless configured otherwise, the security appliance address messages to the log buffer on a continuing basis, overwriting old messages when the buffer is full. If you want to keep a history of logs, you can configure the security appliance to send the buffer contents to another output location each time the buffer fills. Buffer contents can be saved either to internal Flash memory or to an FTP server.

When saving the buffer content to another location, the security appliance creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

While the security appliance writes the log buffer contents to internal Flash memory or an FTP server, it continues saving new messages to the log buffer.

To specify that messages in the log buffer should be saved to internal Flash memory each time the buffer wraps, enter the following command:

```
hostname(config)# logging flash-bufferwrap
```

## Automatically Saving the Full Log Buffer to an FTP Server

See the [“Saving the Current Contents of the Log Buffer to Internal Flash Memory”](#) section for more information about saving the buffer.

To specify that messages in the log buffer should be saved to an FTP server each time the buffer wraps, perform the following steps.

- 
- Step 1** To enable the security appliance to send the log buffer contents to an FTP server every time the buffer wraps, enter the following command:

```
hostname(config)# logging ftp-bufferwrap
```

- Step 2** To identify the FTP server, entering the following command:

```
hostname(config)# logging ftp-server server path username password
```

Where the *server* argument specifies the IP address of the external FTP server

The *path* argument specifies the directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory.

The *username* argument specifies a username that is valid for logging into the FTP server.

The *password* argument specifies the password for the username specified.

For example:

```
hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
```

---

### Saving the Current Contents of the Log Buffer to Internal Flash Memory

At any time, you can save the contents of the buffer to internal Flash memory. To save the current contents of the log buffer to internal Flash memory, enter the following command:

```
hostname(config)# logging savelog [savefile]
```

For example, the following example saves the contents of the log buffer to internal Flash memory using the file name latest-logfile.txt:

```
hostname(config)# logging savelog latest-logfile.txt
```

### Clearing the Contents of the Log Buffer

To erase the contents of the log buffer, enter the following command:

```
hostname(config)# clear logging buffer
```

## Filtering System Log Messages

This section describes how to specify which system log messages should go to output destinations, and includes the following topics:

- [Message Filtering Overview, page 1-14](#)
- [Filtering System Log Messages by Class, page 1-15](#)
- [Filtering System Log Messages with Custom Message Lists, page 1-16](#)

### Message Filtering Overview

You can filter generated system log messages so that only certain system log messages are sent to a particular output destination. For example, you could configure the security appliance to send all system log messages to one output destination and also to send a subset of those system log messages to a different output destination.

Specifically, you can configure the security appliance so that system log messages are directed to an output destination according to the following criteria:

- System log message ID number
- System log message severity level
- System log message class (equivalent to a functional area of the security appliance)

You customize the above criteria by creating a message list that you can specify when you set the output destination in the “[Configuring Log Output Destinations](#)” section on page 1-7.

You can alternatively configure the security appliance to send a particular message class to each type of output destination independently of the message list.

For example, you could configure the security appliance to send to the internal log buffer all system log messages with severity levels of 1, 2 and 3, send all system log messages in the “ha” class to a particular syslog server, or create a list of messages that you name “high-priority” that are sent to an e-mail address to notify system administrators of a possible problem.

## Filtering System Log Messages by Class

The system log message class provides a method of categorizing system log messages by type, equivalent to a feature or function of the security appliance. For example, the “vpnc” class denotes the VPN client.

This section includes the following topics:

- [Message Class Overview, page 1-15](#)
- [Sending All Messages in a Class to a Specified Output Destination, page 1-15](#)

### Message Class Overview

With logging classes, you can specify an output location for an entire category of system log messages with a single command.

You can use system log message classes in two ways:

- Issue the **logging class** command to specify an output location for an entire category of system log messages.
- Create a message list using the **logging list** command that specifies the message class. See the [“Filtering System Log Messages with Custom Message Lists” section on page 1-16](#) for this method.

All system log messages in a particular class share the same initial 3 digits in their system log message ID numbers. For example, all system log message IDs that begin with the digits 611 are associated with the vpnc (VPN client) class. System log messages associated with the VPN client feature range from 611101 to 611323.

### Sending All Messages in a Class to a Specified Output Destination

When you configure all messages in a class to go to a type of output destination, this configuration overrides the configuration in the specific output destination command. For example, if you specify that messages at level 7 should go to the log buffer, and you also specify that ha class messages at level 3 should go to the buffer, then the latter configuration takes precedence.

To configure the security appliance to send an entire system log message class to a configured output destination, enter the following command:

```
hostname(config)# logging class message_class {buffered | history | mail | monitor | trap}
[severity_level]
```

Where the *message\_class* argument specifies a class of system log messages to be sent to the specified output destination. See [Table 1-2](#) for a list of system log message classes.

The **buffered**, **history**, **mail**, **monitor**, and **trap** keywords specify the output destination to which system log messages in this class should be sent. The **history** keyword enables SNMP logging. The **monitor** keyword enables Telnet and SSH logging. The **trap** keyword enables syslog server logging. Select one destination per command line entry. If you want to specify that a class should go to more than one destination, enter a new command for each output destination.

The *severity\_level* argument further restricts the system log messages to be sent to the output destination by specifying a severity level. For more information about message severity levels, see the “[Severity Levels](#)” section on page 1-23.

The following example specifies that all system log messages related to the class *ha* (high availability, also known as failover) with a severity level of 1 (alerts) should be sent to the internal logging buffer.

```
hostname(config)# logging class ha buffered alerts
```

[Table 1-2](#) lists the system log message classes and the ranges of system log message IDs associated with each class.

**Table 1-2 System Log Message Classes and Associated Message ID Numbers**

Class	Definition	System Log Message ID Numbers
<b>ha</b>	Failover (High Availability)	101, 102, 103, 104, 210, 311, 709
<b>rip</b>	RIP Routing	107, 312
<b>auth</b>	User Authentication	109, 113
<b>bridge</b>	Transparent Firewall	110, 220
<b>config</b>	Command interface	111, 112, 208, 308
<b>sys</b>	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711
<b>session</b>	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
<b>ip</b>	IP Stack	209, 215, 313, 317, 408
<b>snmp</b>	SNMP	212
<b>vpdn</b>	PPTP and L2TP Sessions	213, 403, 603
<b>vpn</b>	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
<b>ospf</b>	OSPF Routing	318, 409, 503, 613
<b>np</b>	Network Processor	319
<b>rm</b>	Resource Manager	321
<b>ids</b>	Intrusion Detection System	400, 401, 415
<b>vpnc</b>	VPN Client	611
<b>webvpn</b>	Web-based VPN	716
<b>ca</b>	PKI Certification Authority	717
<b>e-mail</b>	E-mail Proxy	719
<b>vpnlb</b>	VPN Load Balancing	718
<b>vpnfo</b>	VPN Failover	720
<b>npssl</b>	NP SSL	725

## Filtering System Log Messages with Custom Message Lists

Creating a custom message list is a flexible way to exercise fine control over which system log messages are sent to which output destination. In a custom system log message list, you specify groups of system log messages using any or all of the following criteria: severity level, message IDs, ranges of system log message IDs, or by message class.

For example, message lists can be used to:

- Select system log messages with severity levels of 1 and 2 and send them to one or more e-mail addresses.
- Select all system log messages associated with a message class (such as “ha”) and save them to the internal buffer.

A message list can include multiple criteria for selecting messages. However, you must add each message selection criteria with a new command entry. It is possible to create a message list containing overlapping message selection criteria. If two criteria in a message list select the same message, the message is logged only once.

To create a customized list that the security appliance can use to select messages to be saved in the log buffer, perform the following steps:

**Step 1** Create a message list containing criteria for selecting messages by entering the following command:

```
hostname(config)# logging list name {level level [class message_class] |
message start_id[-end_id]}
```

Where the *name* argument specifies the name of the list. Do not use the names of severity levels as the name of a system log message list. Prohibited names include “emergencies,” “alert,” “critical,” “error,” “warning,” “notification,” “informational,” and “debugging.” Similarly, do not use the first three characters of these words at the beginning of a file name. For example, do not use a filename that starts with the characters “err.”

The **level level** argument specifies the severity level. You can specify the severity level number (0 through 7) or name. For severity level names, see the “Severity Levels” section on page 1-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The **class message\_class** argument specifies a particular message class. See Table 1-2 on page 1-16 for a list of class names.

The **message start\_id[-end\_id]** argument specifies an individual system log message ID number or a range of numbers.

The following example creates a message list named `notif-list` that specifies messages with a severity level of 3 or higher should be saved in the log buffer:

```
hostname(config)# logging list notif-list level 3
```

**Step 2** (Optional) If you want to add more criteria for message selection to the list, enter the same command as in the previous step specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion you want to add to the list.

The following example adds criteria to the message list: a range of message ID numbers, and the message class `ha` (high availability or failover).

```
hostname(config)# logging list notif-list 104024-105999
hostname(config)# logging list notif-list level critical
hostname(config)# logging list notif-list level warning class ha
```

The preceding example states that system log messages that match the criteria specified will be sent to the output destination. The specified criteria for system log messages to be included in the list are:

- System log message IDs that fall in the range of 104024 to 105999
- All system log messages with critical level or higher (emergency, alert, or critical)
- All `ha` class system log messages with warning level or higher (emergency, alert, critical, error, or warning)

A system log message is logged if it satisfies any of these conditions. If a system log satisfies more than one of the conditions, the message is logged only once.

---

## Customizing the Log Configuration

### Customizing the Log Configuration

This section describes other options for fine tuning the logging configuration. It includes the following topics:

- [Configuring the Logging Queue, page 1-18](#)
- [Including the Date and Time in System Log Messages, page 1-18](#)
- [Including the Device ID in System Log Messages, page 1-19](#)
- [Generating System Log Messages in EMBLEM Format, page 1-19](#)
- [Disabling a System Log Message, page 1-20](#)
- [Changing the Severity Level of a System Log Message, page 1-20](#)
- [Changing the Amount of Internal Flash Memory Available for Logs, page 1-21](#)

### Configuring the Logging Queue

The Cisco ASA has a fixed number of blocks in memory that can be allocated for buffering system log messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the system log message queue and the number of syslog servers specified.

To specify the number of system log messages the security appliance can hold in its queue before sending them to the configured output destination, enter the following command:

```
hostname(config)# logging queue message_count
```

Where the *message\_count* variable specifies the number of system log messages that can remain in the system log message queue while awaiting processing. The default is 512 system log messages. A setting of 0 (zero) indicates unlimited system log messages, that is, the queue size is limited only by block memory availability.

To view the queue and queue statistics, enter the following command:

```
hostname(config)# show logging queue
```

### Including the Date and Time in System Log Messages

To specify that system log messages should include the date and time that the system log messages was generated, enter the following command:

```
hostname(config)# logging timestamp
```



## Including the Device ID in System Log Messages

To configure the security appliance to include a device ID in non-EMBLEM-format system log messages, enter the following command:

```
hostname(config)# logging device-id {context-name | hostname | ipaddress interface_name | string text}
```

You can specify only one type of device ID for the system log messages.

The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.

The **hostname** keyword specifies that the hostname of the security appliance should be used as the device ID.

The **ipaddress interface\_name** argument specifies that the IP address of the interface specified as *interface\_name* should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified security appliance interface IP address, regardless of the interface from which the system log message is sent. This keyword provides a single, consistent device ID for all system log messages that are sent from the device.

The **string text** argument specifies that the text string should be used as the device ID. The string can contain as many as 16 characters. You cannot use blank spaces or any of the following characters:

- & (ampersand)
- ' (single quote)
- " (double quote)
- < (less than)
- > (greater than)
- ? (question mark)



### Note

If enabled, the device ID does not appear in EMBLEM-formatted system log messages or SNMP traps.

The following example enables the logging device ID for the FWSM:

```
hostname(config)# logging device-id hostname
```

The following example enables the logging device ID for a security context on the FWSM:

```
hostname(config)# logging device-id context-name
```

## Generating System Log Messages in EMBLEM Format

- To use the EMBLEM format for system log messages sent to destinations other than a syslog server, enter the following command:

```
hostname(config)# logging emblem
```

- To use the EMBLEM format for system log messages sent to a syslog server over UDP, specify the **format emblem** option when you configure the syslog server as a n output destination. See the [“Sending System Log Messages to a Syslog Server” section on page 1-7](#) for more information about syslog servers. Enter the following command:

```
hostname(config)# logging host interface_name ip_address {tcp[/port] | udp[/port]}
[format emblem]
```

Where the *interface\_name* and *IP\_address* specifies the syslog server to receive the system log messages, **tcp[/port]** and **udp[/port]** indicate the protocol and port that should be used, and **format emblem** enables EMBLEM formatting for messages sent to the syslog server.

The Cisco ASA can send system log messages using either the UDP or TCP protocol; however, you can enable the EMBLEM format only for messages sent over UDP. The default protocol and port are UDP/514.

For example:

```
hostname(config)# logging host interface_1 122.243.006.123 udp format emblem
```

## Disabling a System Log Message

- To prevent the security appliance from generating a particular system log message, enter the following command:

```
hostname(config)# no logging message message_number
```

For example:

```
hostname(config)# no logging message 113019
```

- To reenabling a disabled system log message, enter the following command:

```
hostname(config)# logging message message_number
```

For example:

```
hostname(config)# logging message 113019
```

- To see a list of disabled system log messages, enter the following command:

```
hostname(config)# show logging message
```

- To reenabling logging of all disabled system log messages, enter the following command:

```
hostname(config)# clear config logging disabled
```

## Changing the Severity Level of a System Log Message

- To specify the logging level of a system log message, enter the following command:

```
hostname(config)# logging message message_ID level severity_level
```

The following example modifies the severity level of system log message ID 113019 from 4 (warnings) to 5 (notifications):

```
hostname(config)# logging message 113019 level 5
```

- To reset the logging level of a system log message to its default level, enter the following command.

```
hostname(config)# no logging message message_ID level current_severity_level
```

The following example modifies the severity level of system log message ID 113019 to its default value of 4 (warnings).

```
hostname(config)# no logging message 113019 level 5
```

- To see the severity level of a specific message, enter the following command:

```
hostname(config)# show logging message message_ID
```

- To see a list of system log messages with modified severity levels, enter the following command:

```
hostname(config)# show logging message
```

- To reset the severity level of all modified system log messages back to their defaults, enter the following command:

```
hostname(config)# clear configure logging level
```

The series of commands in the following example illustrates the use of the **logging message** command to control both whether a system log message is enabled and the severity level of the system log message.

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

## Changing the Amount of Internal Flash Memory Available for Logs

You can cause the security appliance to save the contents of the log buffer to Internal Flash memory in two ways:

- Configure logging so that the contents of the log buffer are saved to internal Flash memory each time the buffer wraps
- Enter a command instructing the security appliance to save the current contents of the log buffer to internal Flash memory immediately

By default, the security appliance can use up to 1 MB of internal Flash memory for log data. The default minimum amount of internal Flash memory that must be free for the security appliance to save log data is 3 MB.

If a log file being saved to internal Flash memory would cause the amount of free internal Flash memory to fall below the configured minimum limit, the security appliance deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the security appliance fails to save the new log file.

To modify the settings for the amount of internal Flash memory available for logs, perform the following steps:

- Step 1** To specify the maximum amount of internal Flash memory available for saving log files, enter the following command:

```
hostname(config)# logging flash-maximum-allocation kbytes
```

Where *kbytes* specifies the maximum amount of internal Flash memory, in kilobytes, that can be used for saving log files.

The following example sets the maximum amount of internal Flash memory that can be used for log files to approximately 1.2 MB:

```
hostname(config)# logging flash-maximum-allocation 1200
```

- Step 2** To specify the minimum amount of internal Flash memory that must be free for the security appliance to save a log file, enter the following command:

```
hostname(config)# logging flash-minimum-free kbytes
```

Where *kbytes* specifies the minimum amount of internal Flash memory, in kilobytes, that must be available before the security appliance saves a new log file.

The following example specifies that the minimum amount of free internal Flash memory must be 4000 KB before the security appliance can save a new log file:

```
hostname(config)# logging flash-minimum-free 4000
```

## Understanding System Log Messages

This section describes the contents of system log messages generated by the security appliance. It includes the following topics:

- [System Log Message Format, page 1-22](#)
- [Severity Levels, page 1-23](#)
- [Variables Used in System Log Messages, page 1-23](#)

### System Log Message Format

System Log messages begin with a percent sign (%) and are structured as follows:

```
%PIX|ASA Level Message_number: Message_text
```

Field descriptions are as follows:

<i>PIX ASA</i>	Identifies the system log message facility code for messages generated by the Cisco ASA . This value is always PIX ASA .
<i>Level</i>	1-7. The level reflects the severity of the condition described by the system log message. The lower the number, the more severe the condition. See <a href="#">Table 1-3</a> for more information.
<i>Message_number</i>	A unique 6-digit number that identifies the system log message.
<i>Message_text</i>	A text string describing the condition. This portion of the system log message sometimes includes IP addresses, port numbers, or usernames. <a href="#">Table 1-4</a> lists the variable fields and the type of information in them.

## Severity Levels

Table 1-3 lists the system log message severity levels.

**Table 1-3 System Log Message Severity Levels**

Level Number	Level Keyword	Description
0	<b>emergencies</b>	System unusable.
1	<b>alert</b>	Immediate action needed.
2	<b>critical</b>	Critical condition.
3	<b>error</b>	Error condition.
4	<b>warning</b>	Warning condition.
5	<b>notification</b>	Normal but significant condition.
6	<b>informational</b>	Informational message only.
7	<b>debugging</b>	Appears during debugging only.



### Note

The security appliance does not generate system log messages with a severity level of 0 (emergencies). This level is provided in the **logging** command for compatibility with the UNIX system log feature, but is not used by the Cisco ASA.

## Variables Used in System Log Messages

System log messages often contain variables. Table 1-4 lists most variables that are used in this guide to describe system log messages. Some variables that appear in only one system log message are not listed.

**Table 1-4 Variable Fields in System Log Messages**

Variable	Type of Information
<i>acl_ID</i>	An ACL name.
<i>bytes</i>	The number of bytes.
<i>code</i>	A decimal number returned by the system log message to indicate the cause or source of the error, depending on the system log message.
<i>command</i>	A command name.
<i>command_modifier</i>	The <i>command_modifier</i> is one of the following strings: <ul style="list-style-type: none"> <li>• cmd (this string means the command has no modifier)</li> <li>• clear</li> <li>• no</li> <li>• show</li> </ul>
<i>connections</i>	The number of connections.

**Table 1-4 Variable Fields in System Log Messages (continued)**

Variable	Type of Information
<i>connection_type</i>	The connection type: <ul style="list-style-type: none"> <li>• SIGNALLING UDP</li> <li>• SIGNALLING TCP</li> <li>• SUBSCRIBE UDP</li> <li>• SUBSCRIBE TCP</li> <li>• Via UDP</li> <li>• Route</li> <li>• RTP</li> <li>• RTCP</li> </ul>
<i>dec</i>	Decimal number.
<i>dest_address</i>	The destination address of a packet.
<i>dest_port</i>	The destination port number.
<i>device</i>	The memory storage device. For example, the floppy disk, internal Flash memory, TFTP, the failover standby unit, or the console terminal.
<i>econns</i>	Number of embryonic connections.
<i>elimit</i>	Number of embryonic connections specified in the <b>static</b> or <b>nat</b> command.
<i>filename</i>	A filename of the type Cisco ASA image, ASDM file, or configuration.
<i>ftp-server</i>	External FTP server name or IP address.
<i>gateway_address</i>	The network gateway IP address.
<i>global_address</i>	Global IP address, an address on a lower security level interface.
<i>global_port</i>	The global port number.
<i>hex</i>	Hexadecimal number.
<i>inside_address</i>	Inside (or local) IP address, an address on a higher security level interface.
<i>inside_port</i>	The inside port number.
<i>interface_name</i>	The name of the interface.
<i>IP_address</i>	IP address in the form <i>n.n.n.n</i> , where <i>n</i> is an integer from 1 to 255.
<i>MAC_address</i>	The MAC address.
<i>mapped_address</i>	The translated IP address.
<i>mapped_port</i>	The translated port number.
<i>message_class</i>	Category of system log messages associated with a functional area of the security appliance.
<i>message_list</i>	Name of a file you create containing a list of system log message ID numbers, classes, or severity levels.
<i>message_number</i>	The system log message ID.
<i>nconns</i>	Number of connections permitted for the static or xlate table.
<i>netmask</i>	The subnet mask.
<i>number</i>	A number. The exact form depends on the system log message.

**Table 1-4** Variable Fields in System Log Messages (continued)

<b>Variable</b>	<b>Type of Information</b>
<i>octal</i>	Octal number.
<i>outside_address</i>	Outside (or foreign) IP address, an address of a syslog server typically on a lower security level interface in a network beyond the outside router.
<i>outside_port</i>	The outside port number.
<i>port</i>	The TCP or UDP port number.
<i>privilege_level</i>	The user privilege level.
<i>protocol</i>	The protocol of the packet, for example, ICMP, TCP, or UDP.
<i>real_address</i>	The real IP address, before Network Address Translation (NAT).
<i>real_port</i>	The real port number, before NAT.
<i>reason</i>	A text string describing the reason for the system log message.
<i>service</i>	The service specified by the packet, for example, SNMP or Telnet.
<i>severity_level</i>	The severity level of a system log message.
<i>source_address</i>	The source address of a packet.
<i>source_port</i>	The source port number.
<i>string</i>	Text string (for example, a username).
<i>tcp_flags</i>	Flags in the TCP header such as: <ul style="list-style-type: none"> <li>• ACK</li> <li>• FIN</li> <li>• PSH</li> <li>• RST</li> <li>• SYN</li> <li>• URG</li> </ul>
<i>time</i>	Duration, in the format <i>hh:mm:ss</i> .
<i>url</i>	A URL.
<i>user</i>	A username.







## System Log Messages

---

This chapter lists the system log messages in numerical order.



**Note**

---

When a number is skipped from a sequence, the message is no longer in the security appliance code.

---

This chapter includes the following sections:

- [Messages 101001 to 199009, page 2-1](#)
- [Messages 201002 to 219002, page 2-55](#)
- [Messages 302003 to 335014, page 2-73](#)
- [Messages 400000 to 450001, page 2-122](#)
- [Messages 500001 to 509001, page 2-176](#)
- [Messages 602101 to 622102, page 2-185](#)
- [Messages 701001 to 726001, page 2-213](#)

### Messages 101001 to 199009

This section contains messages from 101001 to 199009.

#### 101001

**Error Message** %PIX|ASA-1-101001: (Primary) Failover cable OK.

**Explanation** This is a failover message. This message reports that the failover cable is present and functioning correctly. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 101002

**Error Message** %PIX|ASA-1-101002: (Primary) Bad failover cable.

**Explanation** This is a failover message. This message reports that the failover cable is present but not functioning correctly. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Replace the failover cable.

## 101003, 101004

**Error Message** %PIX|ASA-1-101003: (Primary) Failover cable not connected (this unit).

**Error Message** %PIX|ASA-1-101004: (Primary) Failover cable not connected (other unit).

**Explanation** Both instances are failover messages. These messages are logged when failover mode is enabled, but the failover cable is not connected to one unit of the failover pair. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Connect the failover cable to both units of the failover pair.

## 101005

**Error Message** %PIX|ASA-1-101005: (Primary) Error reading failover cable status.

**Explanation** This is a failover message. This message is displayed if the failover cable is connected, but the primary unit is unable to determine its status.

**Recommended Action** Replace the cable.

## 102001

**Error Message** %PIX|ASA-1-102001: (Primary) Power failure/System reload other side.

**Explanation** This is a failover message. This message is logged if the primary unit detects a system reload or a power failure on the other unit. “Primary” can also be listed as “Secondary” for the secondary unit.

**Recommended Action** On the unit that experienced the reload, issue the **show crashinfo** command to determine if there is a traceback associated with the reload. Also verify that the unit is powered on and that power cables are properly connected.

## 103001

**Error Message** %PIX|ASA-1-103001: (Primary) No response from other firewall (reason code = *code*).

**Explanation** This is a failover message. This message is displayed if the primary unit is unable to communicate with the secondary unit over the failover cable. (Primary) can also be listed as (Secondary) for the secondary unit. [Table 2-1](#) lists the reason codes and the descriptions to determine why the failover occurred.

**Table 2-1 Reason Codes**

Reason Code	Description
1	No failover hello seen on serial cable for 30+ seconds. This ensures that failover is running properly on the other unit.
2	An interface did not pass one of the 4 failover tests. The four tests are as follows: 1) Link Up, 2) Monitor for Network Traffic, 3) ARP test, 4) Broadcast Ping test.
3	No proper ACK for 15+ seconds after a command was sent on the serial cable.
4	The local unit is not receiving the hello packet on the failover LAN and other data interfaces and it is declaring that the peer is down.
5	The standby peer went down during the configuration synchronization process.

**Recommended Action** Verify that the failover cable is connected properly and both units have the same hardware, software, and configuration; otherwise, contact the Cisco TAC.

## 103002

**Error Message** %PIX|ASA-1-103002: (Primary) Other firewall network interface *interface\_number* OK.

**Explanation** This is a failover message. This message is displayed when the primary unit detects that the network interface on the secondary unit is okay. (Primary) can also be listed as (Secondary) for the secondary unit. Refer to [Table 1-4](#) in [Chapter 1, “Configuring Logging and SNMP,”](#) for possible values for the *interface\_number* variable.

**Recommended Action** None.

## 103003

**Error Message** %PIX|ASA-1-103003: (Primary) Other firewall network interface *interface\_number* failed.

**Explanation** This is a failover message. This message is displayed if the primary unit detects a bad network interface on the secondary unit. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Check the network connections on the secondary unit and check the network hub connection. If necessary, replace the failed network interface.

## 103004

**Error Message** %PIX|ASA-1-103004: (Primary) Other firewall reports this firewall failed.

**Explanation** This is a failover message. This message is displayed if the primary unit receives a message from the secondary unit indicating that the primary has failed. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Verify the status of the primary unit.

## 103005

**Error Message** %PIX|ASA-1-103005: (Primary) Other firewall reporting failure.

**Explanation** This is a failover message. This message is displayed if the secondary unit reports a failure to the primary unit. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Verify the status of the secondary unit.

## 104001, 104002

**Error Message** %PIX|ASA-1-104001: (Primary) Switching to ACTIVE (cause: *string*).

**Error Message** %PIX|ASA-1-104002: (Primary) Switching to STNDBY (cause: *string*).

**Explanation** Both instances are failover messages. These messages usually are logged when you force the pair to switch roles, either by entering the **failover active** command on the standby unit, or the **no failover active** command on the active unit. (Primary) can also be listed as (Secondary) for the secondary unit. Possible values for the *string* variable are as follows:

- state check
- bad/incomplete config

- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state

**Recommended Action** If the message occurs because of manual intervention, no action is required. Otherwise, use the cause reported by the secondary unit to verify the status of both units of the pair.

## 104003

**Error Message** %PIX|ASA-1-104003: (Primary) Switching to FAILED.

**Explanation** This is a failover message. This message is displayed when the primary unit fails.

**Recommended Action** Check the system log messages for the primary unit for an indication of the nature of the problem (see message 104001). (Primary) can also be listed as (Secondary) for the secondary unit.

## 104004

**Error Message** %PIX|ASA-1-104004: (Primary) Switching to OK.

**Explanation** This is a failover message. This message is displayed when a previously failed unit now reports that it is operating again. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 105001

**Error Message** %PIX|ASA-1-105001: (Primary) Disabling failover.

**Explanation** This is a failover message. This message is displayed when you enter the **no failover** command on the console. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 105002

**Error Message** %PIX|ASA-1-105002: (Primary) Enabling failover.

**Explanation** This is a failover message. This message is displayed when you enter the **failover** command with no arguments on the console, after having previously disabled failover. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 105003

**Error Message** %PIX|ASA-1-105003: (Primary) Monitoring on interface *interface\_name* waiting

**Explanation** This is a failover message. The security appliance is testing the specified network interface with the other unit of the failover pair. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None. The security appliance monitors its network interfaces frequently during normal operations.

## 105004

**Error Message** %PIX|ASA-1-105004: (Primary) Monitoring on interface *interface\_name* normal

**Explanation** This is a failover message. The test of the specified network interface was successful. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 105005

**Error Message** %PIX|ASA-1-105005: (Primary) Lost Failover communications with mate on interface *interface\_name*.

**Explanation** This is a failover message. This message is displayed if this unit of the failover pair can no longer communicate with the other unit of the pair. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Verify that the network connected to the specified interface is functioning correctly.

## 105006, 105007

**Error Message** %PIX|ASA-1-105006: (Primary) Link status 'Up' on interface *interface\_name*.

**Error Message** %PIX|ASA-1-105007: (Primary) Link status 'Down' on interface *interface\_name*.

**Explanation** Both instances are failover messages. These messages report the results of monitoring the link status of the specified interface. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** If the link status is down, verify that the network connected to the specified interface is operating correctly.

## 105008

**Error Message** %PIX|ASA-1-105008: (Primary) Testing interface *interface\_name*.

**Explanation** This is a failover message. This message is displayed when the tests a specified network interface. This testing is performed only if the security appliance fails to receive a message from the standby unit on that interface after the expected interval. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 105009

**Error Message** %PIX|ASA-1-105009: (Primary) Testing on interface *interface\_name* {Passed|Failed}.

**Explanation** This is a failover message. This message reports the result (either Passed or Failed) of a previous interface test. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None required if the result is Passed. If the result is Failed, you should check the network cable connection to both failover units, that the network itself is functioning correctly, and verify the status of the standby unit.

## 105010

**Error Message** %PIX|ASA-3-105010: (Primary) Failover message block alloc failed

**Explanation** Block memory was depleted. This is a transient message and the security appliance should recover. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Use the **show blocks** command to monitor the current block memory.

## 105011

**Error Message** %PIX|ASA-1-105011: (Primary) Failover cable communication failure

**Explanation** The failover cable is not permitting communication between the primary and secondary units. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Ensure that the cable is properly connected.

## 105020

**Error Message** %PIX|ASA-1-105020: (Primary) Incomplete/slow config replication

**Explanation** When a failover occurs, the active security appliance detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Once the failover is detected by the security appliance, the security appliance automatically reloads itself and loads configuration from Flash memory and/or resynchronizes with another security appliance. If failovers happen continuously, check the failover configuration and make sure both security appliance units can communicate with each other.

## 105021

**Error Message** %PIX|ASA-1-105021: (*failover\_unit*) Standby unit failed to sync due to a locked *context\_name* config. Lock held by *lock\_owner\_name*

**Explanation** During configuration synchronizing, a standby unit will reload itself if some other process locks the configuration for more than 5 minutes, which prevents the failover process from applying the new configuration. This can occur when an administrator pages through a running configuration on the standby unit while configuration synchronization is in process. See also the **show running-config EXEC** command and the **pager lines num CONFIG** command.

**Recommended Action** Avoid viewing or modifying configuration on standby unit when it first comes up and is in the process of establishing a failover connection with the active unit.



## 105031

**Error Message** %PIX|ASA-1-105031: Failover LAN interface is up

**Explanation** LAN failover interface link is up.

**Recommended Action** None.

## 105032

**Error Message** %PIX|ASA-1-105032: LAN Failover interface is down

**Explanation** LAN failover interface link is down.

**Recommended Action** Check the connectivity of the LAN failover interface. Make sure that the speed/duplex setting is correct.

## 105034

**Error Message** %PIX|ASA-1-105034: Receive a LAN\_FAILOVER\_UP message from peer.

**Explanation** The peer has just booted and sent the initial contact message.

**Recommended Action** None.

## 105035

**Error Message** %PIX|ASA-1-105035: Receive a LAN failover interface down msg from peer.

**Explanation** The peer LAN failover interface link is down. The unit switches to active mode if it is in standby mode.

**Recommended Action** Check the connectivity of the peer LAN failover interface.

## 105036

**Error Message** %PIX|ASA-1-105036: dropped a LAN Failover command message.

**Explanation** The security appliance dropped an unacknowledged LAN failover command message, indicating a connectivity problem on the LAN failover interface.

**Recommended Action** Check that the LAN interface cable is connected.

## 105037

**Error Message** %PIX|ASA-1-105037: The primary and standby units are switching back and forth as the active unit.

**Explanation** The primary and standby units are switching back and forth as the active unit, indicating a LAN failover connectivity problem or software bug.

**Recommended Action** Check that the LAN interface cable is connected.

## 105038

**Error Message** %PIX|ASA-1-105038: (Primary) Interface count mismatch

**Explanation** When a failover occurs, the active security appliance detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** Once the failover is detected by the security appliance, the security appliance automatically reloads itself and loads the configuration from Flash memory and/or resyncs with another security appliance. If failovers happen continuously, check the failover configuration and make sure that both security appliance units can communicate with each other.

## 105039

**Error Message** %PIX|ASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.

**Explanation** Failover initially verifies that the number of interfaces configured on the primary and secondary security appliances are the same. This message indicates that the primary security appliance is not able to verify the number of interfaces configured on the secondary security appliance. This message indicates that the primary security appliance is not able to communicate with the secondary security appliance over the failover interface. (Primary) can also be listed as (Secondary) for the secondary security appliance.

**Recommended Action** Verify the failover LAN, interface configuration, and status on the primary and secondary security appliances. Make sure that the secondary security appliance is running the security appliance application and that failover is enabled.

## 105040

**Error Message** %PIX|ASA-1-105040: (Primary) Mate failover version is not compatible.

**Explanation** The primary and secondary security appliance should run the same failover software version to act as a failover pair. This message indicates that the secondary security appliance failover software version is not compatible with the primary security appliance. Failover is disabled on the primary security appliance. (Primary) can also be listed as (Secondary) for the secondary security appliance.

**Recommended Action** Maintain consistent software versions between the primary and secondary security appliances to enable failover.

## 105042

**Error Message** %PIX|ASA-1-105042: (Primary) Failover interface OK

**Explanation** LAN failover interface link is up.

**Explanation** The interface used to send failover messages to the secondary security appliance is functioning. (Primary) can also be listed as (Secondary) for the secondary security appliance.

**Recommended Action** None.

## 105043

**Error Message** %PIX|ASA-1-105043: (Primary) Failover interface failed

**Explanation** LAN failover interface link is down.

**Recommended Action** Check the connectivity of the LAN failover interface. Make sure that the speed/duplex setting is correct.

## 105044

**Error Message** %PIX|ASA-1-105044: (Primary) Mate operational mode *mode* is not compatible with my mode *mode*.

**Explanation** When the operational mode (single or multi) does not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same operational mode, and then reenables failover.

## 105045

**Error Message** %PIX|ASA-1-105045: (Primary) Mate license (*number contexts*) is not compatible with my license (*number contexts*).

**Explanation** When the feature licenses do not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same feature license, and then reenable failover.

## 105046

**Error Message** %PIX|ASA-1-105046 (Primary|Secondary) Mate has a different chassis

**Explanation** This message is issued when two failover units have a different type of chassis. For example, one is a PIX, the other is an ASA-5520, or one has a 3-slot chassis, the other has a 6-slot chassis.

**Recommended Action** Make sure that the two failover units are the same.

## 105047

**Error Message** %PIX|ASA-1-105047: Mate has a *io\_card\_name1* card in slot *slot\_number* which is different from my *io\_card\_name2*

**Explanation** The two failover units have different types of cards in their respective slots.

**Recommended Action** Make sure that the card configurations for the failover units are the same.

## 105048

**Error Message** %ASA-1-105048: (*unit*) Mate's service module (*application*) is different from mine (*application*)

**Explanation** The failover process detected that different applications are running on the service modules in the active and standby units. The two failover units are incompatible if different service modules are used.

*unit*—Primary or secondary.

*application*—The name of the application, such as InterScan Security Card.

**Recommended Action** Make sure that both units have identical service modules before trying to re-enable failover.

## 106001

**Error Message** %PIX|ASA-2-106001: Inbound TCP connection denied from *IP\_address/port* to *IP\_address/port* flags *tcp\_flags* on interface *interface\_name*

**Explanation** This is a connection-related message. This message occurs when an attempt to connect to an inside address is denied by your security policy. Possible *tcp\_flags* values correspond to the flags in the TCP header that were present when the connection was denied. For example, a TCP packet arrived for which no connection state exists in the security appliance, and it was dropped. The *tcp\_flags* in this packet are FIN and ACK.

The *tcp\_flags* are as follows:

- ACK—The acknowledgment number was received.
- FIN—Data was sent.
- PSH—The receiver passed data to the application.
- RST—The connection was reset.
- SYN—Sequence numbers were synchronized to start a connection.
- URG—The urgent pointer was declared valid.

**Recommended Action** None.

## 106002

**Error Message** %PIX|ASA-2-106002: *protocol* Connection denied by outbound list *acl\_ID* src *inside\_address* dest *outside\_address*

**Explanation** This is a connection-related message. This message is displayed if the specified connection fails because of an **outbound deny** command. The *protocol* variable can be ICMP, TCP, or UDP.

**Recommended Action** Use the **show outbound** command to check outbound lists.

## 106006

**Error Message** %PIX|ASA-2-106006: Deny inbound UDP from *outside\_address/outside\_port* to *inside\_address/inside\_port* on interface *interface\_name*.

**Explanation** This is a connection-related message. This message is displayed if an inbound UDP packet is denied by your security policy.

**Recommended Action** None.

## 106007

**Error Message** %PIX|ASA-2-106007: Deny inbound UDP from *outside\_address/outside\_port* to *inside\_address/inside\_port* due to DNS {Response|Query}.

**Explanation** This is a connection-related message. This message is displayed if a UDP packet containing a DNS query or response is denied.

**Recommended Action** If the inside port number is 53, the inside host probably is set up as a caching name server. Add an **access-list** command statement to permit traffic on UDP port 53. If the outside port number is 53, a DNS server was probably too slow to respond, and the query was answered by another server.

## 106010

**Error Message** %PIX|ASA-3-106010: Deny inbound *protocol src interface\_name:dest\_address/dest\_port dst interface\_name:source\_address/source\_port*

**Explanation** This is a connection-related message. This message is displayed if an inbound connection is denied by your security policy.

**Recommended Action** Modify the security policy if traffic should be permitted. If the message occurs at regular intervals, contact the remote peer administrator.

## 106011

**Error Message** %PIX|ASA-3-106011: Deny inbound (No xlate) *string*

**Explanation** The message will appear under normal traffic conditions if there are internal users that are accessing the Internet through a web browser. Any time a connection is reset, when the host at the end of the connection sends a packet after the security appliance receives the reset, this message will appear. It can typically be ignored.

**Recommended Action** Prevent this system log message from getting logged to the syslog& server by entering the **no logging message 106011** command.

## 106012

**Error Message** %PIX|ASA-6-106012: Deny IP from *IP\_address* to *IP\_address*, IP options *hex*.

**Explanation** This is a packet integrity check message. An IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded.

**Recommended Action** Contact the remote host system administrator to determine the problem. Check the local site for loose source routing or strict source routing.

## 106013

**Error Message** %PIX|ASA-2-106013: Dropping echo request from *IP\_address* to PAT address *IP\_address*

**Explanation** The security appliance discarded an inbound ICMP Echo Request packet with a destination address that corresponds to a PAT global address. The inbound packet is discarded because it cannot specify which PAT host should receive the packet.

**Recommended Action** None.

## 106014

**Error Message** %PIX|ASA-3-106014: Deny inbound icmp src *interface\_name*: *IP\_address* dst *interface\_name*: *IP\_address* (type *dec*, code *dec*)

**Explanation** The security appliance denied any inbound ICMP packet access. By default, all ICMP packets are denied access unless specifically permitted.

**Recommended Action** None.

## 106015

**Error Message** %PIX|ASA-6-106015: Deny TCP (no connection) from *IP\_address/port* to *IP\_address/port* flags *tcp\_flags* on interface *interface\_name*.

**Explanation** The security appliance discarded a TCP packet that has no associated connection in the security appliance connection table. The security appliance looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is not an existing connection, the security appliance discards the packet.

**Recommended Action** None required unless the security appliance receives a large volume of these invalid TCP packets. If this is the case, trace the packets to the source and determine the reason these packets were sent.

## 106016

**Error Message** %PIX|ASA-2-106016: Deny IP spoof from (*IP\_address*) to *IP\_address* on interface *interface\_name*.

**Explanation** The security appliance discarded a packet with an invalid source address, which may include one of the following or some other invalid address:

- Loopback network (127.0.0.0)
- Broadcast (limited, net-directed, subnet-directed, and all-subnets-directed)
- The destination host (land.c)

To further enhance spoof packet detection, use the **access-list** command to configure the security appliance to discard packets with source addresses belonging to the internal network. Now that the **icmp** command has been implemented, the **access-list** command has been deprecated and is no longer guaranteed to work properly.

**Recommended Action** Determine if an external user is trying to compromise the protected network. Check for misconfigured clients.

## 106017

**Error Message** %PIX|ASA-2-106017: Deny IP due to Land Attack from *IP\_address* to *IP\_address*

**Explanation** The security appliance received a packet with the IP source address equal to the IP destination, and the destination port equal to the source port. This message indicates a spoofed packet that is designed to attack systems. This attack is referred to as a Land Attack.

**Recommended Action** If this message persists, an attack may be in progress. The packet does not provide enough information to determine where the attack originates.

## 106018

**Error Message** %PIX|ASA-2-106018: ICMP packet type *ICMP\_type* denied by outbound list *acl\_ID* src *inside\_address* dest *outside\_address*

**Explanation** The outgoing ICMP packet with the specified ICMP from local host (*inside\_address*) to the foreign host (*outside\_address*) was denied by the outbound ACL list.

**Recommended Action** None.



## 106020

**Error Message** %PIX|ASA-2-106020: Deny IP teardrop fragment (size = *number*, offset = *number*) from *IP\_address* to *IP\_address*

**Explanation** The security appliance discarded an IP packet with a teardrop signature containing either a small offset or fragment overlapping. This is a hostile event that circumvents the security appliance or an Intrusion Detection System.

**Recommended Action** Contact the remote peer administrator or escalate this issue according to your security policy.

## 106021

**Error Message** %PIX|ASA-1-106021: Deny *protocol* reverse path check from *source\_address* to *dest\_address* on interface *interface\_name*

**Explanation** An attack is in progress. Someone is attempting to spoof an IP address on an inbound connection. Unicast RPF, also known as reverse route lookup, detected a packet that does not have a source address represented by a route and assumes that it is part of an attack on your security appliance.

This message appears when you have enabled Unicast RPF with the **ip verify reverse-path** command. This feature works on packets input to an interface; if it is configured on the outside, then the security appliance checks packets arriving from the outside.

The security appliance looks up a route based on the *source\_address*. If an entry is not found and a route is not defined, then this system log message appears and the connection is dropped.

If there is a route, the security appliance checks which interface it corresponds to. If the packet arrived on another interface, it is either a spoof or there is an asymmetric routing environment that has more than one path to a destination. The security appliance does not support asymmetric routing.

If the security appliance is configured on an internal interface, it checks static **route** command statements or RIP, and if the *source\_address* is not found, then an internal user is spoofing their address.

**Recommended Action** Even though an attack is in progress, if this feature is enabled, no user action is required. The security appliance repels the attack.

## 106022

**Error Message** %PIX|ASA-1-106022: Deny *protocol* connection spoof from *source\_address* to *dest\_address* on interface *interface\_name*

**Explanation** A packet matching a connection arrives on a different interface from the interface that the connection began on.

For example, if a user starts a connection on the inside interface, but the security appliance detects the same connection arriving on a perimeter interface, the security appliance has more than one path to a destination. This is known as asymmetric routing and is not supported on the security appliance.

An attacker also might be attempting to append packets from one connection to another as a way to break into the security appliance. In either case, the security appliance displays this message and drops the connection.

**Recommended Action** This message appears when the **ip verify reverse-path** command is not configured. Check that the routing is not asymmetric.

## 106023

**Error Message** %PIX|ASA-4-106023: Deny protocol src  
[interface\_name:source\_address/source\_port] dst  
interface\_name:dest\_address/dest\_port [type {string}, code {code}] by  
access\_group acl\_ID

**Explanation** An IP packet was denied by the ACL. This message displays even if you do not have the **log** option enabled for an ACL.

**Recommended Action** If messages persist from the same source address, messages might indicate a foot-printing or port-scanning attempt. Contact the remote host administrators.

## 106024

**Error Message** %PIX|ASA-2-106024: Access rules memory exhausted

**Explanation** The access list compilation process has run out of memory. All configuration information that has been added since the last successful access list was removed from the system, and the most recently compiled set of access lists will continue to be used.

**Recommended Action** Access lists, AAA, ICMP, SSH, Telnet, and other rule types are stored and compiled as access list rule types. Remove some of these rule types so that others can be added.

## 106025, 106026

**Error Message** %PIX|ASA-6-106025: Failed to determine the security context for the  
packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol

**Error Message** %PIX|ASA-6-106026: Failed to determine the security context for the  
packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol

**Explanation** The security context of the packet in multiple context mode cannot be determined. Both messages can be generated for IP packets being dropped in either router and transparent mode.

**Recommended Action** None.

## 106027

**Error Message** %PIX|ASA-4-106027:Failed to determine the security context for the packet:vlan source Vlan#:ethertype src sourceMAC dst destMAC

**Explanation** The security context of the packet in multiple context mode cannot be determined. This message is generated for non-IP packets being dropped in transparent mode only.

**Recommended Action** None.

## 106100

**Error Message** %PIX|ASA-4-106100: access-list *acl\_ID* {permitted | denied | est-allowed} *protocol interface\_name/source\_address(source\_port) -> interface\_name/dest\_address(dest\_port) hit-cnt number* ({first hit | number-second interval})

**Explanation** If you configured the **log** option for the **access-list** command, the packets matched an ACL statement. The message level depends on the level set in the **access-list** command (by default, the level is 6). The message indicates either the initial occurrence or the total number of occurrences during an interval. This message provides more information than message 106023, which only logs denied packets, and does not include the hit count or a configurable level. The following list describes the message values:

- *permitted | denied | est-allowed*—These values specify if the packet was permitted or denied by the ACL. If the value is *est-allowed*, the packet was denied by the ACL but was allowed for an already established session (for example, an internal user is allowed to access the Internet, and responding packets that would normally be denied by the ACL are accepted).
- *protocol*—TCP, UDP, ICMP, or an IP protocol number.
- *interface\_name*—The interface name for the source or destination of the logged flow. The VLAN interfaces are supported.
- *source\_address*—The source IP address of the logged flow.
- *dest\_address*—The destination IP address of the logged flow.
- *source\_port*—The source port of the logged flow (TCP or UDP). For ICMP, this field is 0.
- *dest\_port*—The destination port of the logged flow (TCP or UDP). For ICMP, this field is *icmp-type*.
- *hit-cnt number*—The number of times this flow was permitted or denied by this ACL entry in the configured time interval. The value is 1 when the security appliance generates the first system log message for this flow.
- *first hit*—The first message generated for this flow.
- *number-second interval*—The interval in which the hit count is accumulated. Set this interval using the **access-list** command with **interval** option.

**Recommended Action** None.

## 106101

**Error Message** %PIX|ASA-1-106101 The number of ACL log deny-flows has reached limit (*number*).

**Explanation** If you configured the **log** option for an ACL **deny** statement (**access-list id deny** command), and a traffic flow matches the ACL statement, the security appliance caches the flow information. This message indicates that the number of matching flows that are cached on the security appliance exceeds the user-configured limit (using the **access-list deny-flow-max** command).

The *number value* is the limit configured using the **access-list deny-flow-max** command.

**Recommended Action** None. This message might be generated as a result of a DoS attack.

## 107001

**Error Message** %PIX|ASA-1-107001: RIP auth failed from *IP\_address*: version=*number*, type=*string*, mode=*string*, sequence=*number* on interface *interface\_name*

**Explanation** This is an alert log message. The security appliance received a RIP reply message with bad authentication. This message might be caused by a misconfiguration on the router or the security appliance or by an unsuccessful attempt to attack the routing table of the security appliance.

**Recommended Action** This message indicates a possible attack and should be monitored. If you are not familiar with the source IP address listed in this message, change your RIP authentication keys between trusted entities. An attacker might be trying to determine the existing keys.

## 107002

**Error Message** %PIX|ASA-1-107002: RIP pkt failed from *IP\_address*: version=*number* on interface *interface\_name*

**Explanation** This is an alert log message. This message could be caused by a router bug, a packet with non-RFC values inside, or a malformed entry. This should not happen, and may be an attempt to exploit routing table of the security appliance.

**Recommended Action** This message indicates a possible attack and should be monitored. The packet has passed authentication, if enabled, and bad data is in the packet. Monitor the situation and change the keys if there are any doubts about the originator of the packet.

## 107003

**Error Message** %PIX-3-107003: RIP: Attempted reference of stale data encountered in *function*, line: *line\_num*

**Explanation** This syslog message is generated when RIP is running and tries to reference some related data structures that have been removed elsewhere. Clearing the interface and router configurations might correct the problem. However, when this syslog message appears, it is an indication that some sequence of steps caused premature deletion of data structures and that should be investigated.

*function* : The function that received the unexpected event.

*line\_num* : The line number in the code.

**Recommended Action** Copy the error message exactly as it appears, and report it to Cisco TAC.

## 108002

**Error Message** %PIX|ASA-2-108002: SMTP replaced *string*: out *source\_address* in *inside\_address* data: *string*

**Explanation** This is a Mail Guard (SMTP) message generated by the **fixup protocol smtp** command. This message is displayed if the security appliance replaces an invalid character in an e-mail address with a space.

**Recommended Action** None.

## 108003

**Error Message** %PIX|ASA-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dset\_port*. Data:*string*

**Explanation** This message is generated by Mail Guard (SMTP). This message is displayed if the security appliance detects malicious pattern in an e-mail address and drops the connection. This indicates an attack in progress.

**Recommended Action** None Required.

## 108004

**Error Message** %PIX|ASA-4-108004: *action\_class: action* ESMTP *req\_resp* from *src\_ifc:sip|sport* to *dest\_ifc:dip|dport;further\_info*

**Explanation** This event is generated when a ESMTP classification is performed on a ESMTP message and the specified criteria are satisfied. The configured action is taken.

- *action\_class*—The class of action: "ESMTP Classification" for ESMTP match commands; "ESMTP Parameter" for parameter commands.
- *action*—action taken: "Dropped", "Dropped connection for", "Reset connection for" or "Masked header flags for"
- *req\_resp*—"Request" or "Response"
- *src\_ifc*—Source interface name
- *sip|sport*—Source IP address or source port
- *dest\_ifc*—Destination interface name
- *dip|dport*—Destination IP address or destination port
- *further info*—One of the following:
  - For single match command: matched Class *id: match\_command* (for example, matched Class 1234: match body length 100).
  - For parameter commands: *parameter-command: descriptive-message* (for example, mail-relay: No Mail Relay allowed).

**Recommended Action** None required.

## 108005

**Error Message** %PIX|ASA-6-108005: *action\_class: Received* ESMTP *req\_resp* from *src\_ifc:sip|sport* to *dest\_ifc:dip|dport;further\_info*

**Explanation** This event is generated when a ESMTP classification is performed on a ESMTP message and the specified criteria are satisfied. The standalone log action is taken.

- *action\_class*—The class of action: "ESMTP Classification" for ESMTP match commands; "ESMTP Parameter" for parameter commands.
- *req\_resp*—"Request" or "Response"
- *src\_ifc*—Source interface name
- *sip|sport*—Source IP address or source port
- *dest\_ifc*—Destination interface name
- *dip|dport*—Destination IP address or destination port
- *further info*—One of the following:
  - For single match command: matched Class *id: match\_command* (for example, matched Class 1234: match body length 100).

- For parameter commands (commands under parameter section): *parameter-command: descriptive-message* (for example, mail-relay: No Mail Relay allowed).

**Recommended Action** None required.

## 108006

**Error Message** %PIX|ASA-7-108006: Detected ESMTP size violation from *src\_ifc:sip|sport* to *dest\_ifc:dip|dport*; declared size is: *decl\_size*, actual size is *act\_size*.

**Explanation** This event is generated when an ESMTP message size exceeds the size declared in the RCPT command.

- *src\_ifc*—Source interface name
- *sip|sport*—Source IP address or source port
- *dest\_ifc*—Destination interface name
- *dip|dport*—Destination IP address or destination port
- *decl\_size*—Declared size
- *act\_size*—Actual size

**Recommended Action** None required.

## 109001

**Error Message** %PIX|ASA-6-109001: Auth start for user *user* from *inside\_address/inside\_port* to *outside\_address/outside\_port*

**Explanation** This is an authentication, authorization and accounting (AAA) message. This message is displayed if the security appliance is configured for AAA and detects an authentication request by the specified user.

**Recommended Action** None.

## 109002

**Error Message** %PIX|ASA-6-109002: Auth from *inside\_address/inside\_port* to *outside\_address/outside\_port* failed (server *IP\_address* failed) on interface *interface\_name*.

**Explanation** This is an AAA message. This message is displayed if an authentication request fails because the specified authentication server cannot be contacted by the module.

**Recommended Action** Check that the authentication daemon is running on the specified authentication server.

## 109003

**Error Message** %PIX|ASA-6-109003: Auth from *inside\_address* to *outside\_address/outside\_port* failed (all servers failed) on interface *interface\_name*.

**Explanation** This is an AAA message. This message is displayed if no authentication server can be found.

**Recommended Action** Ping the authentication servers from the security appliance. Make sure that the daemons are running.

## 109005

**Error Message** %PIX|ASA-6-109005: Authentication succeeded for user *user* from *inside\_address/inside\_port* to *outside\_address/outside\_port* on interface *interface\_name*.

**Explanation** This is an AAA message. This message is displayed when the specified authentication request succeeds.

**Recommended Action** None.

## 109006

**Error Message** %PIX|ASA-6-109006: Authentication failed for user *user* from *inside\_address/inside\_port* to *outside\_address/outside\_port* on interface *interface\_name*.

**Explanation** This is an AAA message. This message is displayed if the specified authentication request fails, possibly because of an incorrect password.

**Recommended Action** None.

## 109007

**Error Message** %PIX|ASA-6-109007: Authorization permitted for user *user* from *inside\_address/inside\_port* to *outside\_address/outside\_port* on interface *interface\_name*.

**Explanation** This is an AAA message. This message is displayed when the specified authorization request succeeds.

**Recommended Action** None.



## 109008

**Error Message** %PIX|ASA-6-109008: Authorization denied for user *user* from *outside\_address/outside\_port* to *inside\_address/ inside\_port* on interface *interface\_name*.

**Explanation** This is an AAA message. This message is displayed if a user is not authorized to access the specified address, possibly because of an incorrect password.

**Recommended Action** None.

## 109010

**Error Message** %PIX|ASA-3-109010: Auth from *inside\_address/inside\_port* to *outside\_address/outside\_port* failed (too many pending auths) on interface *interface\_name*.

**Explanation** This is an AAA message. This message is displayed if an authentication request cannot be processed because the server has too many requests pending.

**Recommended Action** Check to see if the authentication server is too slow to respond to authentication requests. Enable the Flood Defender feature with the **floodguard enable** command.

## 109011

**Error Message** %PIX|ASA-2-109011: Authen Session Start: user '*user*', sid *number*

**Explanation** An authentication session started between the host and the security appliance and has not yet completed.

**Recommended Action** None.

## 109012

**Error Message** %PIX|ASA-5-109012: Authen Session End: user '*user*', sid *number*, elapsed *number* seconds

**Explanation** The authentication cache has timed out. Users must reauthenticate on their next connection. You can change the duration of this timer with the **timeout uauth** command.

**Recommended Action** None.

## 109013

**Error Message** %PIX|ASA-3-109013: User must authenticate before using this service

**Explanation** The user must be authenticated before using the service.

**Recommended Action** Authenticate using FTP, Telnet, or HTTP before using the service.

## 109014

**Error Message** %PIX|ASA-7-109014: uauth\_lookup\_net fail for uauth\_in()

**Explanation** A request to authenticate did not have a corresponding request for authorization.

**Recommended Action** Ensure that both the **aaa authentication** and **aaa authorization** command statements are included in the configuration.

## 109016

**Error Message** %PIX|ASA-3-109016: Can't find authorization ACL *acl\_ID* for user 'user'

**Explanation** The access control list specified on the AAA server for this user does not exist on the security appliance. This error can occur if you configure the AAA server before you configure the security appliance. The Vender-Specific Attribute (VSA) on your AAA server might be one of the following values:

- `acl=acl_ID`
- `shell:acl=acl_ID`
- `ACS:CiscoSecured-Defined-ACL=acl_ID`

**Recommended Action** Add the ACL to the security appliance, making sure to use the same name specified on the AAA server.

## 109017

**Error Message** %PIX|ASA-4-109017: User at *IP\_address* exceeded auth proxy connection limit (max)

**Explanation** A user has exceeded the user authentication proxy limit, and has opened too many connections to the proxy.

**Recommended Action** Increase the proxy limit by entering the **proxy-limit** *proxy\_limit* command, or ask the user to close unused connections. If the error persists, it may indicate a possible DoS attack.

## 109018

**Error Message** %PIX|ASA-3-109018: Downloaded ACL *acl\_ID* is empty

**Explanation** The downloaded authorization access control list has no ACEs. This situation might be caused by misspelling the attribute string “ip:inacl#” or omitting the **access-list** command.

```
junk:junk# 1=permit tcp any any eq junk ip:inacl#1=
```

**Recommended Action** Correct the ACL components that have the indicated error on the AAA server.

## 109019

**Error Message** %PIX|ASA-3-109019: Downloaded ACL *acl\_ID* has parsing error; ACE string

**Explanation** An error is encountered during parsing the sequence number NNN in the attribute string ip:inacl#NNN= of a downloaded authorization access control list. The reasons include: - missing = - contains non-numeric, non-space characters between '#' and '=' - NNN is greater than 999999999.

```
ip:inacl# 1 permit tcp any any
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 1000000000=permit tcp any any
```

**Recommended Action** Correct the ACL element that has the indicated error on the AAA server.

## 109020

**Error Message** %PIX|ASA-3-109020: Downloaded ACL has config error; ACE

**Explanation** One of the components of the downloaded authorization access control list has a configuration error. The entire text of the element is included in the system log message. This message is usually caused by an invalid **access-list** command statement.

**Recommended Action** Correct the ACL component that has the indicated error on the AAA server.

## 109021

**Error Message** %PIX|ASA-7-109021: Uauth null proxy error

**Explanation** An internal User Authentication error has occurred.

**Recommended Action** None. However, if this error appears repeatedly, contact the Cisco TAC.

## 109022

**Error Message** %PIX|ASA-4-109022: exceeded HTTPS proxy process limit

**Explanation** For each HTTPS authentication, the security appliance dedicates a process to service the authentication request. When the number of concurrently running processes exceeds the system-imposed limit, the security appliance does not perform the authentication, and this message is displayed.

**Recommended Action** None.

## 109023

**Error Message** %PIX|ASA-3-109023: User from *source\_address/source\_port* to *dest\_address/dest\_port* on interface *outside\_interface* must authenticate before using this service.

**Explanation** This is an AAA message. Based on the configured policies, you need to be authenticated before you can use this service port.

**Recommended Action** Authenticate using Telnet, FTP, or HTTP before attempting to use the above service port.

## 109024

**Error Message** %PIX|ASA-6-109024: Authorization denied from *source\_address/source\_port* to *dest\_address/dest\_port* (not authenticated) on interface *interface\_name* using *protocol*

**Explanation** This is an AAA message. This message is displayed if the security appliance is configured for AAA and a user attempted to make a TCP connection across the security appliance without prior authentication.

**Recommended Action** None.

## 109025

**Error Message** %PIX|ASA-6-109025: Authorization denied (acl=*acl\_ID*) for user '*user*' from *source\_address/source\_port* to *dest\_address/dest\_port* on interface *interface\_name* using *protocol*

**Explanation** The access control list check failed. The check either matched a deny or did not match anything, such as an implicit deny. The connection was denied by the user access control list *acl\_ID*, which was defined per the AAA authorization policy on Cisco Secure Access Control Server (ACS).

**Recommended Action** None.

## 109026

**Error Message** %PIX|ASA-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.

**Explanation** The response from the AAA server could not be validated. It is likely that the configured server key is incorrect. This event may be generated during transactions with RADIUS or TACACS+ servers.

**Recommended Action** Verify that the server key, configured using the **aaa-server** command, is correct.

## 109027

**Error Message** %PIX|ASA-4-109027: [aaa protocol] Unable to decipher response message  
Server = *server\_IP\_address*, User = *user*

**Explanation** The response from the AAA server could not be validated. The configured server key is probably incorrect. This message may be displayed during transactions with RADIUS or TACACS+ servers. The *server\_IP\_address* is the IP address of the relevant AAA server. The *user* is the user name associated with the connection.

**Recommended Action** Verify that the server key, configured using the **aaa-server** command, is correct.

## 109028

**Error Message** %PIX|ASA-4-109028: aaa bypassed for same-security traffic from  
*ingress\_interface:source\_address/source\_port* to  
*egress\_interface:dest\_address/dest\_port*

**Explanation** AAA is being bypassed for same security traffic that matches a configured AAA rule. This can only occur when traffic passes between two interfaces that have the same configured security level, when the same security traffic is permitted, and if the AAA configuration uses the include or exclude syntax.

**Recommended Action** None.

## 109029

**Error Message** %PIX|ASA-5-109029: Parsing downloaded ACL: *string*

**Explanation** A syntax error was encountered while parsing an access list that was downloaded from a RADIUS server during user authentication.

*string*—An error message detailing the syntax error that prevented the access list from parsing correctly.

**Recommended Action** Use the information presented in this message to identify and correct the syntax error in the access list definition within the RADIUS server configuration.

## 109030

**Error Message** %PIX|ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL *access\_list source | dest netmask netmask*.

**Explanation** This message is displayed when a dynamic ACL that is configured on a RADIUS server is not converted by the mechanism for automatically detecting wildcard netmasks. The problem occurs because this mechanism could not determine if the netmask is a wildcard or a normal netmask.

*access\_list*—The access list that could not be converted

*source*—The source IP address.

*dest*—The destination IP address.

*netmask*—The subnet mask for the destination or source address in dotted-decimal notation.

**Recommended Action** Check the access list netmask on the RADIUS server for wildcard configuration. If it is meant to be a wildcard, and if all access list netmasks on that server are wildcard then use the **wildcard** setting for **acl-netmask-convert** for the AAA server. Otherwise, change the netmask to a normal netmask or to a wildcard netmask that does not contain holes. In other words, where the netmask presents consecutive binary 1's. For example, 00000000.00000000.00011111.11111111 or hex 0.0.31.255. If the mask is meant to be normal and all access list netmasks on that server are normal then use the **normal** setting **acl-netmask-convert** for the AAA server.

## 109031

**Error Message** %PIX|ASA-4-109031: NT Domain Authentication Failed: rejecting guest login for *username*.

**Explanation** This message is displayed when a user tries to authenticate to an NT Auth domain that was configured for guest account access and the username is not a valid username on the NT server. The connection is denied.

**Recommended Action** If the user is a valid user add an account to the NT server. If the user is not allowed access, no action is required.

## 109032

**Error Message** %PIX|ASA-3-109032: Unable to install ACL *access\_list*, downloaded for user *username*; Error in ACE: *ace*.

**Explanation** This message is displayed when an access control list is received from a RADIUS server during the authentication of a network user. The log event indicates a syntax error in one of the elements of the access list. When this occurs, the element is discarded but the rest of access list is still applied. The entire text of the malformed element is included in the message. Note that this condition does not result in an authentication failure.

*access\_list*—The name assigned to the dynamic access list as it would appear in the output of the **show access-list** command.

*username*—The name of the user whose connection will be subject to this access list.

*ace*—The access list entry that was being processed when the error was detected.

**Recommended Action** Correct the access list definition in the RADIUS server configuration.

## 109033

**Error Message** %PIX|ASA-4-109033: Authentication failed for admin user *user* from *src\_IP*. Interactive challenge processing is not supported for *protocol* connections

**Explanation** AAA challenge processing was triggered during authentication of an administrative connection, but the security appliance cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

*user*—The name of the user being authenticated.

*src\_IP*—The IP address of the client host.

*protocol*—The client connection protocol. Possible values: "SSH v1" or "administrative HTTP".

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

## 109034

**Error Message** %PIX|ASA-4-109034: Authentication failed for network user *user* from *src\_IP/port* to *dst\_IP/port*. Interactive challenge processing is not supported for *protocol* connections

**Explanation** AAA challenge processing was triggered during authentication of a network connection, but the security appliance cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

*user*—The name of the user being authenticated.

*src\_IP/port*—The IP address and port of the client host.

*dst\_IP/port*—The IP address and port of the server to which the client is attempting to connect.

*protocol*—The client connection protocol. Possible value: "FTP".

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

## 110001

**Error Message** %PIX|ASA-6-110001: No route to *dest\_address* from *source\_address*

**Explanation** This message indicates a route lookup failure. A packet is looking for a destination IP address that is not in the routing table.

**Recommended Action** Check the routing table and make sure that there is a route to the destination.

## 111001

**Error Message** %PIX|ASA-5-111001: Begin configuration: *IP\_address* writing to *device*

**Explanation** This message is displayed when you enter the **write** command to store your configuration on a *device* (either floppy, Flash memory, TFTP, the failover standby unit, or the console terminal). The *IP\_address* indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None.

## 111002

**Error Message** %PIX|ASA-5-111002: Begin configuration: *IP\_address* reading from *device*

**Explanation** This message is displayed when you enter the <> command to read your configuration from a *device* (either floppy, Flash memory, TFTP, the failover standby unit, or the console terminal). The *IP\_address* indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None.



## 111003

**Error Message** %PIX|ASA-5-111003: *IP\_address* Erase configuration

**Explanation** This is a management message. This message is displayed when you erase the contents of Flash memory by entering the **write erase** command at the console. The *IP\_address* value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** After erasing the configuration, reconfigure the security appliance and save the new configuration. Alternatively, you can restore information from a configuration that was previously saved, either on floppy or on a TFTP server elsewhere on the network.

## 111004

**Error Message** %PIX|ASA-5-111004: *IP\_address* end configuration: {FAILED|OK}

**Explanation** This message is displayed when you enter the **config floppy/memory/ network** command or the **write floppy/memory/network/standby** command. The *IP\_address* value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required if the message ends with OK. If the message indicates a failure, try to fix the problem. For example, if writing to a floppy disk, ensure that the floppy disk is not write protected; if writing to a TFTP server, ensure that the server is up.

## 111005

**Error Message** %PIX|ASA-5-111005: *IP\_address* end configuration: OK

**Explanation** This message is displayed when you exit the configuration mode. The *IP\_address* value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None.

## 111007

**Error Message** %PIX|ASA-5-111007: Begin configuration: *IP\_address* reading from *device*.

**Explanation** This message is displayed when you enter the **reload** or **configure** command to read in a configuration. The *device* text can be floppy, memory, net, standby, or terminal. The *IP\_address* value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None.

## 111008

**Error Message** %PIX|ASA-5-111008: User *user* executed the command *string*

**Explanation** The user entered a command that modified the configuration. This message does not appear for **show** commands.

**Recommended Action** None.

## 111009

**Error Message** %PIX|ASA-7-111009:User *user* executed cmd:*string*

**Explanation** The user entered a command that does not modify the configuration. This message appears only for **show** commands.

**Recommended Action** None.

## 111111

**Error Message** %PIX|ASA-1-111111 *error\_message*

**Explanation** System or infrastructure error has occurred.

**Recommended Action** Copy the error message and submit it to TAC along with the configuration and any details about the events leading up to this error.

## 112001

**Error Message** %PIX|ASA-2-112001: (*string:dec*) Clear complete.

**Explanation** This message is displayed when a request to clear the module configuration is completed. The source file and line number are identified.

**Recommended Action** None.

## 113001

**Error Message** %PIX|ASA-3-113001: Unable to open AAA session. Session limit [*limit*] reached.

**Explanation** An AAA operation on an IPSec tunnel or WebVPN connection could not be performed because of the unavailability of system resources. The *limit* value indicates the maximum number of concurrent AAA transactions.

**Recommended Action** Reduce the demand for AAA resources if possible.

## 113003

**Error Message** %PIX|ASA-6-113003: AAA group policy for user *user* is being set to *policy\_name*.

**Explanation** The group policy that is associated with the tunnel-group is being overridden with a user specific policy, *policy\_name*. The *policy\_name* is specified using the **username** command when LOCAL authentication is configured or is returned in the RADIUS CLASS attribute when RADIUS authentication is configured.

**Recommended Action** None.

## 113004

**Error Message** %PIX|ASA-6-113004: AAA user *aaa\_type* Successful: server = *server\_IP\_address*, User = *user*

**Explanation** This is an indication that an AAA operation on an IPSec or WebVPN connection has been completed successfully. The AAA types are “authentication,” “authorization,” or “accounting.” The *server\_IP\_address* is the IP address of the relevant AAA server. The *user* is the user name associated with the connection.

**Recommended Action** None.

## 113005

**Error Message** %PIX|ASA-6-113005: AAA user authentication Rejected: reason = *string*:  
server = *server\_IP\_address*, User = *user*

**Explanation** This is an indication that either an authentication or authorization request for a user associated with an IPSec or WebVPN connection has been rejected. Details of why the request was rejected are provided in the *reason* field. *server\_IP\_address* is the IP address of the relevant AAA server. *user* is the user name associated with the connection. *aaa\_operation* is either authentication or authorization.

**Recommended Action** None.

## 113006

**Error Message** %PIX|ASA-6-113006: User *user* locked out on exceeding *number* successive failed authentication attempts

**Explanation** A locally configured user is being locked out. This happens when a configured number of consecutive authentication failures have occurred for this user and indicates that all future authentication attempts by this user will be rejected until an administrator unlocks the user using the **clear aaa local user lockout** command. *user* is the user that is now locked and *number* is the consecutive failure threshold configured with the **aaa local authentication attempts max-fail** command.

**Recommended Action** Try unlocking the user using the **clear aaa local user lockout** command or adjusting the maximum number of consecutive authentication failures that are tolerated.

## 113007

**Error Message** %PIX|ASA-6-113007: User *user* unlocked by *administrator*

**Explanation** A locally configured user that was locked out after exceeding the maximum number of consecutive authentication failures set by the **aaa local authentication attempts max-fail** command has been unlocked by the indicated administrator.

**Recommended Action** None.

## 113008

**Error Message** %PIX|ASA-6-113008: AAA transaction status ACCEPT: user = *user*

**Explanation** An AAA transaction for a user associated with an IPSec or WebVPN connection was completed successfully. The *user* is the username associated with the connection.

**Recommended Action** None.

## 113009

**Error Message** %PIX|ASA-6-113009: AAA retrieved default group policy *policy* for user *user*

**Explanation** This message may be generated during the authentication or authorization of an IPsec or WebVPN connection. The attributes of the group policy that were specified with the **tunnel-group** or **webvpn** commands have been retrieved.

**Recommended Action** None.

## 113010

**Error Message** %PIX|ASA-6-113010: AAA challenge received for user *user* from server *server\_IP\_address*

**Explanation** This message may be generated during the authentication of an IPsec connection when the authentication is done with a SecurID server. The user will be prompted to provide further information prior to being authenticated. *server\_IP\_address* is the IP address of the relevant AAA server. *user* is the username associated with the connection.

**Recommended Action** None.

## 113011

**Error Message** %PIX|ASA-6-113011: AAA retrieved user specific group policy *policy* for user *user*

**Explanation** This event may be generated during the authentication or authorization of an IPsec or WebVPN connection. The attributes of the group policy that was specified with the **tunnel-group** or **webvpn** commands have been retrieved.

**Recommended Action** None.

## 113012

**Error Message** %PIX|ASA-6-113012: AAA user authentication Successful: local database : user = *user*

**Explanation** The user associated with a IPsec or WebVPN connection has been successfully authenticated to the local user database. *user* is the username associated with the connection.

**Recommended Action** None.

## 113013

**Error Message** %PIX|ASA-6-113013: AAA unable to complete the request Error: reason =  
*reason*: user = *user*

**Explanation** An AAA transaction for a user associated with an IPSec or WebVPN connection has failed due to an error or has been rejected due to a policy violation. Details are provided in the *reason* field. *user* is the username associated with the connection.

**Recommended Action** None.

## 113014

**Error Message** %PIX|ASA-6-113014: AAA authentication server not accessible: server =  
*server\_IP\_address*: user = *user*

**Explanation** The device was unable to communicate with the configured AAA server during an AAA transaction associated with an IPSec or WebVPN connection. This may or may not result in a failure of the user connection attempt depending on the backup servers configured in the *aaa-server* group and the availability of those servers.

**Recommended Action** Verify connectivity with the configured AAA servers.

## 113015

**Error Message** %PIX|ASA-6-113015: AAA user authentication Rejected: reason = *reason* :  
local database: user = *user*

**Explanation** A request for authentication to the local user database for a user associated with an IPSec or WebVPN connection has been rejected. Details of why the request was rejected are provided in the *reason* field. *user* is the username associated with the connection.

**Recommended Action** None.

## 113016

**Error Message** %PIX|ASA-6-113016: AAA credentials rejected: reason = *reason*: server =  
*server\_IP\_address*: user = *user*

**Explanation** An AAA transaction for a user associated with an IPSec or WebVPN connection has failed due to an error or rejected due to a policy violation. Details are provided in the *reason* field. *server\_IP\_address* is the IP address of the relevant AAA server. *user* is the username associated with the connection.

**Recommended Action** None.

## 113017

**Error Message** %PIX|ASA-6-113017: AAA credentials rejected: reason = *reason*: local database: user = *user*\

**Explanation** This is an indication that an AAA transaction for a user associated with an IPSec or WebVPN connection has failed due to an error or rejected due to a policy violation. Details are provided in the *reason* field. This event only appears when the AAA transaction is with the local user database rather than with an external AAA server. *user* is the username associated with the connection.

**Recommended Action** None.

## 113018

**Error Message** %PIX|ASA-3-113018: User: *user*, Unsupported downloaded ACL Entry: *ACL\_entry*, Action: *action*

**Explanation** An ACL entry in unsupported format was downloaded from the authentication server. The following list describes the message values:

- *user*—User trying to login.
- *ACL\_entry*—Unsupported ACL entry downloaded from the authentication server.
- *action*—Action taken on encountering the unsupported ACL Entry.

**Recommended Action** The ACL entry on the authentication server has to be changed appropriately by the administrator to conform with the supported ACL entry formats.

## 113019

**Error Message** %PIX|ASA-4-113019: Group = *group*, Username = *user*, IP = *peer\_address*, Session disconnected. Session Type: *type*, Duration: *duration*, Bytes xmt: *count*, Bytes rcv: *count*, Reason: *reason*

**Explanation** This is an information message.

*group*—group name

*user*—username

*peer\_address*—peer address

*type*—session type (for example, IPSec/UDP)

*duration*—connect duration

*count*—number of bytes

*reason*—disconnect reason

**Recommended Action** None.

## 113020

**Error Message** %PIX|ASA-3-113020: Kerberos error : Clock skew with server *ip\_address* greater than 300 seconds

**Explanation** This message is displayed when authentication for an IPSec or WebVPN user through a Kerberos server fails because the clocks on the security appliance the server are more than five minutes (300 seconds) apart. When this occurs, the connection attempt is rejected.

*ip\_address*—The IP address of the Kerberos server.

**Recommended Action** Synchronize the clocks on the security appliance and the Kerberos server.

## 114001

**Error Message** %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to initialize an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.



## 114002

**Error Message** %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error *error\_string*).

This message is displayed when the system fails to initialize an SFP connector in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSupport
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114003

**Error Message** %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to run cached commands in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR

- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSupport
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114004

**Error Message** %ASA-6-114004: 4GE SSM I/O Initialization start.

**Explanation** This message is displayed to notify the user that an 4GE SSM I/O Initialization is starting.

*syslog\_id*—Message identifier

**Recommended Action** No action is required.

## 114005

**Error Message** %ASA-6-114005: 4GE SSM I/O Initialization end.

**Explanation** This message is displayed to notify user that an 4GE SSM I/O Initialization is finished.

*syslog\_id*—Message identifier

**Recommended Action** No action is required.

## 114006

**Error Message** %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to get port statistics in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSupport
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114007

**Error Message** %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to get the current module status register information in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR

- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114008

**Error Message** %ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.

**Explanation** This message is displayed when the system fails to enable a port after the link transition to Up state is detected in an 4GE SSM I/O card due to either an I2C serial bus access error or a switch access error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114009

**Error Message** %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to set the multicast address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114010

**Error Message** %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to set the multicast hardware address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR

- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114011

**Error Message** %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error *error\_string*).

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Explanation** This message is displayed when the system fails to delete the multicast address in an 4GE SSM I/O card due to either an I2C error or a switch initialization error.

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114012

**Error Message** %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error *error\_string*).

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Explanation** This message is displayed when the system fails to delete the multicast hardware address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114013

**Error Message** %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to set the MAC address table in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR

- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114014

**Error Message** %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error *error\_string*).

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Explanation** This message is displayed when the system fails to set the MAC address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.



## 114015

**Error Message** %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error *error\_string*).

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Explanation** This message is displayed when the system fails to set individual/promiscuous mode in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114016

**Error Message** %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error *error\_string*).

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR

- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Explanation** This message is displayed when the system fails to set the multicast mode in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114017

**Error Message** %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to get link status in an 4GE SSM I/O card due to either an I2C serial bus access error or a switch access error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Notify the system administrator
2. Log and review the messages and the errors associated with the event.
3. Reboot the software running on the system.
4. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
5. If the problem persists, contact the Cisco TAC.

## 114018

**Error Message** %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to set the port speed in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114019

**Error Message** %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error *error\_string*).

**Explanation** This message is displayed when the system fails to set the media type in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

*syslog\_id*—Message identifier

*error\_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR

- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSupport
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114020

**Error Message** %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.

**Explanation** This message is displayed when the system cannot detect the port link speed in an 4GE SSM I/O card.

**Recommended Action** Perform the following steps:

1. Log and review the messages associated with the event.
2. Reset the 4GE SSM I/O card and observe if the software automatically recovers from the event.
3. If the software does not recover automatically, power cycle the box. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

## 199001

**Error Message** %PIX|ASA-5-199001: Reload command executed from telnet (remote IP\_address).

**Explanation** This message logs the address of the host that is initiating a security appliance reboot with the **reload** command.

**Recommended Action** None.

## 199002

**Error Message** %PIX|ASA-6-199002: startup completed. Beginning operation.

**Explanation** The security appliance finished its initial boot and the Flash memory reading sequence, and is ready to begin operating normally.



**Note** This message cannot be blocked by using the **no logging message** command.

**Recommended Action** None.

## 199003

**Error Message** %PIX|ASA-6-199003: Reducing link MTU *dec*.

**Explanation** The security appliance received a packet from the outside network that uses a larger MTU than the inside network. The security appliance then sent an ICMP message to the outside host to negotiate an appropriate MTU. The log message includes the sequence number of the ICMP message.

**Recommended Action** None.

## 199005

**Error Message** %PIX|ASA-6-199005: Startup begin

**Explanation** The security appliance started.

**Recommended Action** None.

## 199006

**Error Message** %PIX|ASA-5-199006: Orderly reload started at *when* by *whom*. Reload reason: *reason*

**Explanation** This message is generated when a reload operation is started.

- *when*—The time at which orderly reload operation begins. The time is in the format of hh:mm:ss timezone weekday month day year, for example “13:23:45 UTC Sun Dec 28 2003.”
- *whom*—The user or system that scheduled the reload. The user or system is in the format username from where, for example “enable\_15 from ssh (remote 30.0.0.122).”

- *reason*—The reload reason. String will be *unspecified* if a more complete reason is not displayed.

**Recommended Action** No action is required from the user.

## 199007

**Error Message** %PIX|ASA-5-199007: Reload scheduled for *when* by *whom* at *when-command-issued*. Reload reason: *reason*

**Explanation** This message is generated when a reload operation is scheduled by using the *in* or *at* option of the reload command.

- *when*—The time at which the reload operation should begin. The time is in the format of hh:mm:ss timezone weekday month day year, for example “13:23:45 UTC Sun Dec 28 2003.”
- *whom*—The user or system that scheduled the reload. The user or system is in the format username from where, for example “enable\_15 from ssh (remote 30.0.0.122.”
- *when-command-issued*—The time that the reload command is issued. The time is in the format of hh:mm:ss timezone weekday month day year.
- *reason*—The reload reason. String will be *unspecified* if a more complete reason is not displayed.

**Recommended Action** No action is required from the user.

## 199008

**Error Message** %PIX|ASA-5-199008: Scheduled reload for *when-reload-is-supposed-to-happen* cancelled by *whom* at *when*.

**Explanation** This message is generated when a scheduled reload operation is cancelled.

- *when-reload-is-supposed-to-happen*—The when the reload was supposed to happen. The time is in the format of hh:mm:ss timezone weekday month day year, for example “13:23:45 UTC Sun Dec 28 2003.”
- *whom*—The user or system that cancelled the reload. The user or system is in the format username from where, for example “enable\_15 from ssh (remote 30.0.0.122.”
- *when*—The time at which the reload operation is cancelled. The time is in the format of hh:mm:ss timezone weekday month day year.

**Recommended Action** No action is required from the user.

## 199009

**Error Message** %PIX|ASA-7-199009: Reloaded at *when* by *whom*. Reload reason: *reason*

**Explanation** This message is generated when a reload operation is started.

- *when*—The time at which orderly reload operation begins. The time is in the format of hh:mm:ss timezone weekday month day year, for example “13:23:45 UTC Sun Dec 28 2003.”
- *whom*—The user or system that scheduled the reload. The user or system is in the format username from where, for example “enable\_15 from ssh (remote 30.0.0.122).”
- *reason*—The reload reason. String will be *unspecified* if a more complete reason is not displayed.

**Recommended Action** No action is required from the user.

## Messages 201002 to 219002

This section contains messages from 201002 to 219002.

### 201002

**Error Message** %PIX|ASA-3-201002: Too many TCP connections on {static|xlate} *global\_address*! *econns nconns*

**Explanation** This is a connection-related message. This message is displayed when the maximum number of TCP connections to the specified global address was exceeded. The *econns* variable is the maximum number of embryonic connections and the *nconns* variable is the maximum number of connections permitted for the static or xlate.

**Recommended Action** Use the **show static** or **show nat** command to check the limit imposed on connections to a static address. The limit is configurable.

### 201003

**Error Message** %PIX|ASA-2-201003: Embryonic limit exceeded *nconns/elimit* for *outside\_address/outside\_port* (*global\_address*) *inside\_address/inside\_port* on interface *interface\_name*

**Explanation** This is a connection-related message regarding traffic to the security appliance. This message is displayed when the number of embryonic connections from the specified foreign address with the specified static global address to the specified local address exceeds the embryonic limit. When the limit on embryonic connections to the security appliance is reached, the security appliance attempts to accept them anyway, but puts a time limit on the connections. This situation allows some

connections to succeed even if the security appliance is very busy. The *nconns* variable lists the number of embryonic connections received and the *elimit* variable lists the maximum number of embryonic connections specified in the **static** or **nat** command.

**Recommended Action** This message indicates a more serious overload than message 201002. It could be caused by a SYN attack, or by a very heavy load of legitimate traffic. Use the **show static** command to check the limit imposed on embryonic connections to a static address.

## 201004

**Error Message** %PIX|ASA-3-201004: Too many UDP connections on {static|xlate} *global\_address!* *udp connections limit*

**Explanation** This is a connection-related message. This message is displayed when the maximum number of UDP connections to the specified global address was exceeded. The *udp conn limit* variable is the maximum number of UDP connections permitted for the static or translation.

**Recommended Action** Use the **show static** or **show nat** command to check the limit imposed on connections to a static address. You can configure the limit.

## 201005

**Error Message** %PIX|ASA-3-201005: FTP data connection failed for IP\_address *IP\_address*

**Explanation** The security appliance could not allocate a structure to track the data connection for FTP because of insufficient memory.

**Recommended Action** Reduce the amount of memory usage or purchase additional memory.

## 201006

**Error Message** %PIX|ASA-3-201006: RCMD backconnection failed for *IP\_address/port*

**Explanation** This is a connection-related message. This message is displayed if the security appliance is unable to preallocate connections for inbound standard output for **rsh** commands due to insufficient memory.

**Recommended Action** Check the **rsh** client version; the security appliance only supports the Berkeley **rsh**. You can also reduce the amount of memory usage, or purchase additional memory.



## 201008

**Error Message** %PIX|ASA-3-201008: The security appliance is disallowing new connections.

**Explanation** This message appears when you have enabled TCP system log messaging and the syslog server cannot be reached, or when using the security appliance Syslog Server (PFSS) and the disk on the Windows NT system is full, or when the auto-update timeout is configured and the auto-update server is not reachable.

**Recommended Action** Disable TCP system log messaging. If using PFSS, free up space on the Windows NT system where PFSS resides. Also, make sure that the syslog server is up and you can ping the host from the security appliance console. Then restart TCP system message logging to allow traffic. If the Auto Update Server has not been contacted for a certain period of time, the following command will cause it to cease sending packets: [no] auto-update timeout period.

## 201009

**Error Message** %PIX|ASA-3-201009: TCP connection limit of *number* for host *IP\_address* on *interface\_name* exceeded

**Explanation** This is a connection-related message. This message is displayed when the maximum number of connections to the specified static address was exceeded. The *number* variable is the maximum of connections permitted for the host specified by the *IP\_address* variable.

**Recommended Action** Use the **show static** and **show nat** commands to check the limit imposed on connections to an address. The limit is configurable.

## 201010

**Error Message** %PIX|ASA-3-201010: Embryonic connection limit exceeded *econns/limit* for *dir* packet from *source\_address/source\_port* to *dest\_address/dest\_port* on interface *interface\_name*

**Explanation** An attempt to establish a TCP connection failed due to an exceeded embryonic connection limit, which was configured with the **set connection embryonic-conn-max** MPC command for a traffic class.

- *econns*— The current count of embryonic connections associated to the configured traffic class.
- *limit*—The configured embryonic connection limit for the traffic class.
- *dir*—  
input: The first packet that initiates the connection is an input packet on the interface *interface\_name*.  
output: The first packet that initiates the connection is an output packet on the interface *interface\_name*.
- *source\_address/source\_port*—The source IP address and the source port of the packet initiating the connection.

- *dest\_address/dest\_port*—The destination IP address and the destination port of the packet initiating the connection.
- *interface\_name*—The name of the interface on which the policy limit is enforced.

**Recommended Action** None.

## 201011

**Error Message** %PIX|ASA-3-201011: Connection limit exceeded *cnt/limit* for *dir* packet from *sip/sport* to *dip/dport* on interface *if\_name*

**Explanation** A new connection through the firewall device resulted in exceeding at least one of the configured maximum connection limits. This message applies to either connection limits configured using a “static” command, or to those configured using the Cisco Modular Policy Framework. The new connection will not be allowed through the firewall device until one of the existing connections is torn down, thereby bringing the current connection count below the configured maximum.

- *cnt*—The current connection count.
- *limit*—The configured connection limit.
- *dir*—The direction of traffic, inbound or outbound.
- *sip*—The source IP address.
- *sport*—The source port.
- *dip*—The destination IP address.
- *dport*—The destination port.
- *if\_name*—The name of the interface on which the traffic was received.

**Recommended Action** None required.

## 201012

**Error Message** %ASA-6-201012: Per-client embryonic connection limit exceeded *curr num/limit* for [input|output] packet from *IP\_address/ port* to *ip/port* on interface *interface\_name*

**Explanation** An attempt to establish a TCP connection failed because the per-client embryonic connection limit was exceeded. By default, this message is rate limited to 1 message every 10 seconds.

*curr num*—The current number.

*limit*—The configured limit.

[input|output]—Input or output packet on interface *interface\_name*.

*IP\_address*—IP address.

*port*—TCP or UDP port.

*interface\_name*—The name of the interface on which the policy is applied.

**Recommended Action** When the limit is reached, any new connection request will be proxied by the security appliance to prevent a SYN flood attack. The security appliance will only connect to the server if the client is able to finish the three-way handshake. This usually does not affect the end user or the application. However, if this creates a problem for any application that has a legitimate need for a higher number of embryonic connections, you can adjust the setting by entering the **set connection per-client-embryonic-max** command.

## 201013

**Error Message** %ASA-3-201013: Per-client connection limit exceeded *curr num/limit* for [input|output] packet from ip/*port* to ip/*port* on interface *interface\_name*

**Explanation** A connection was rejected because the per-client connection limit was exceeded.

*curr num*—The current number.

*limit*—The configured limit.

[input|output]—The input or output packet on interface *interface\_name*.

*IP\_address*—The IP address.

*port*—The TCP or UDP port.

*interface\_name*—The name of the interface on which the policy is applied.

**Recommended Action** When the limit is reached any new connection request will be silently dropped. Normally an application will retry. This will cause delay or even a timeout if all retries also fail. If an application has a legitimate need for a higher number of concurrent connections, you can adjust the setting by entering the **set connection per-client-max** command.

## 202001

**Error Message** %PIX|ASA-3-202001: Out of address translation slots!

**Explanation** This is a connection-related message. This message is displayed if the security appliance has no more address translation slots available.

**Recommended Action** Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translates and connections. This error message could also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory usage if possible.

## 202005

**Error Message** %PIX|ASA-3-202005: Non-embryonic in embryonic list  
*outside\_address/outside\_port inside\_address/inside\_port*

**Explanation** This is a connection-related message. This message is displayed when a connection object (xlate) is in the wrong list.

**Recommended Action** contact the Cisco TAC.

## 202011

**Error Message** %PIX|ASA-3-202011: Connection limit exceeded *econns/limit* for *dir* packet from *source\_address/source\_port* to *dest\_address/dest\_port* on interface *interface\_name*

**Explanation** This message is displayed when an attempt to create a TCP or UDP connection fails due to an exceeded connection limit which is configured with the **set connection conn-max MPC** command for a traffic class.

- *econns*— The current count of embryonic connections associated to the configured traffic class.
- *limit*—The configured embryonic connection limit for the traffic class.
- *dir*—
  - input— The first packet that initiates the connection is an input packet on the interface *interface\_name*.
  - output— The first packet that initiates the connection is an output packet on the interface *interface\_name*.
- *source\_address/source\_port*—The source IP address and the source port of the packet initiating the connection.
- *dest\_address/dest\_port*—The destination IP address and the destination port of the packet initiating the connection.
- *interface\_name*—The name of the interface on which the policy limit is enforced.

**Recommended Action** None.

## 208005

**Error Message** %PIX|ASA-3-208005: (*function:line\_num*) clear command return code

**Explanation** The security appliance received a nonzero value (an internal error) when attempting to clear the configuration in Flash memory. The message includes the reporting subroutine filename and line number.

**Recommended Action** For performance reasons, the end host should be configured to not inject IP fragments. This configuration change is probably due to NFS. Set the read and write size equal to the interface MTU for NFS.

## 209003

**Error Message** %PIX|ASA-4-209003: Fragment database limit of *number* exceeded: src = *source\_address*, dest = *dest\_address*, proto = *protocol*, id = *number*

**Explanation** Too many IP fragments are currently awaiting reassembly. By default, the maximum number of fragments is 200 (refer to the **fragment size** command in the *Cisco Security Appliance Command Reference* to raise the maximum). The security appliance limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the security appliance under abnormal network conditions. In general, fragmented traffic should be a small percentage of the total traffic mix. An exception is in a network environment with NFS over UDP where a large percentage is fragmented traffic; if this type of traffic is relayed through the security appliance, consider using NFS over TCP instead. To prevent fragmentation, see the **sysopt connection tcpmss bytes** command in the *Cisco Security Appliance Command Reference*.

**Recommended Action** If this message persists, a denial of service (DoS) attack might be in progress. Contact the remote peer administrator or upstream provider.

## 209004

**Error Message** %PIX|ASA-4-209004: Invalid IP fragment, size = *bytes* exceeds maximum size = *bytes*: src = *source\_address*, dest = *dest\_address*, proto = *protocol*, id = *number*

**Explanation** An IP fragment is malformed. The total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes.

**Recommended Action** A possible intrusion event may be in progress. If this message persists, contact the remote peer's administrator or upstream provider.

## 209005

**Error Message** %PIX|ASA-4-209005: Discard IP fragment set with more than *number* elements: src = Too many elements are in a fragment set.

**Explanation** The security appliance disallows any IP packet that is fragmented into more than 24 fragments. Refer to the **fragment** command in the *Cisco Security Appliance Command Reference* for more information.

**Recommended Action** A possible intrusion event may be in progress. If the message persists, contact the remote peer administrator or upstream provider. You can change the number of fragments per packet by using the **fragment chain xxx interface\_name** command.

## 210001

**Error Message** %PIX|ASA-3-210001: LU *sw\_module\_name* error = *number*

**Explanation** A Stateful Failover error occurred.

**Recommended Action** If this error persists after traffic lessens through the security appliance, report this error to Cisco TAC.

## 210002

**Error Message** %PIX|ASA-3-210002: LU allocate block (*bytes*) failed.

**Explanation** Stateful Failover could not allocate a block of memory to transmit stateful information to the standby security appliance.

**Recommended Action** Check the failover interface using the **show interface** command to make sure its transmit is normal. Also check the current block memory using the **show block** command. If current available count is 0 within any of the blocks of memory, then reload the security appliance software to recover the lost blocks of memory.

## 210003

**Error Message** %PIX|ASA-3-210003: Unknown LU Object *number*

**Explanation** Stateful Failover received an unsupported Logical Update object and therefore was unable to process it. This could be caused by corrupted memory, LAN transmissions, and other events.

**Recommended Action** If you see this error infrequently, then no action is required. If this error occurs frequently, check the Stateful Failover link LAN connection. If the error was not caused by a faulty failover link LAN connection, determine if an external user is trying to compromise the protected network. Check for misconfigured clients.

## 210005

**Error Message** %PIX|ASA-3-210005: LU allocate connection failed

**Explanation** Stateful Failover cannot allocate a new connection on the standby unit. This may be caused by little or no RAM memory available within the security appliance.

**Recommended Action** Check the available memory using the **show memory** command to make sure that the security appliance has free memory in the system. If there is no available memory, add more physical memory to the security appliance.

## 210006

**Error Message** %PIX|ASA-3-210006: LU look NAT for *IP\_address* failed

**Explanation** Stateful Failover was unable to locate a NAT group for the IP address on the standby unit. The active and standby security appliance units may be out of synchronization.

**Recommended Action** Use the **write standby** command on the active unit to synchronize system memory with the standby unit.

## 210007

**Error Message** %PIX|ASA-3-210007: LU allocate xlate failed

**Explanation** Stateful Failover failed to allocate a translation (xlate) slot record.

**Recommended Action** Check the available memory by using the **show memory** command to make sure that the security appliance has free memory in the system. If no memory is available, add more memory.

## 210008

**Error Message** %PIX|ASA-3-210008: LU no xlate for *inside\_address/inside\_port*  
*outside\_address/outside\_port*

**Explanation** Unable to find a translation slot (xlate) record for a Stateful Failover connection; unable to process the connection information.

**Recommended Action** Enter the **write standby** command on the active unit to synchronize system memory between the active and standby units.

## 210010

**Error Message** %PIX|ASA-3-210010: LU make UDP connection for *outside\_address:outside\_port*  
*inside\_address:inside\_port* failed

**Explanation** Stateful Failover was unable to allocate a new record for a UDP connection.

**Recommended Action** Check the available memory by using the **show memory** command to make sure that the security appliance has free memory in the system. If no memory is available, add more memory.

## 210020

**Error Message** %PIX|ASA-3-210020: LU PAT port *port* reserve failed

**Explanation** Stateful Failover is unable to allocate a specific PAT address which is in use.

**Recommended Action** Enter the **write standby** command on the active unit to synchronize system memory between the active and standby units.

## 210021

**Error Message** %PIX|ASA-3-210021: LU create static xlate *global\_address* ifc *interface\_name* failed

**Explanation** Stateful Failover is unable to create a translation slot (xlate).

**Recommended Action** Enter the **write standby** command on the active unit to synchronize system memory between the active and standby units.

## 210022

**Error Message** %PIX|ASA-6-210022: LU missed *number* updates

**Explanation** Stateful Failover assigns a sequence number for each record sent to the standby unit. When a received record sequence number is out of sequence with the last updated record, the information in between is assumed lost and this error message is sent.

**Recommended Action** Unless there are LAN interruptions, check the available memory on both security appliance units to ensure that there is enough memory to process the stateful information. Use the **show failover** command to monitor the quality of stateful information updates.

## 211001

**Error Message** %PIX|ASA-3-211001: Memory allocation Error

**Explanation** Failed to allocate RAM system memory.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.



## 211003

**Error Message** %PIX|ASA-3-211003: CPU utilization for *number* seconds = *percent*

**Explanation** This message is displayed if the percentage of CPU usage is greater than 100 percent for the *number* of seconds.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

## 212001

**Error Message** %PIX|ASA-3-212001: Unable to open SNMP channel (UDP port *port*) on interface *interface\_number*, error code = *code*

**Explanation** This is an SNMP message. This message reports that the security appliance is unable to receive SNMP requests destined for the security appliance from SNMP management stations located on this interface. This does not affect the SNMP traffic passing through the security appliance through any interface.

An error code of -1 indicates that the security appliance could not open the SNMP transport for the interface. This can occur when the user attempts to change the port on which SNMP accepts queries to one that is already in use by another feature. In this case, the port used by SNMP will be reset to the default port for incoming SNMP queries (UDP/161).

An error code of -2 indicates that the security appliance could not bind the SNMP transport for the interface.

**Recommended Action** After the security appliance reclaims some of its resources when traffic is lighter, reenter the **snmp-server host** command for that interface.

## 212002

**Error Message** %PIX|ASA-3-212002: Unable to open SNMP trap channel (UDP port *port*) on interface *interface\_number*, error code = *code*

**Explanation** This is an SNMP message. This message reports that the security appliance is unable to send its SNMP traps from the security appliance to SNMP management stations located on this interface. This does not affect the SNMP traffic passing through the security appliance through any interface.

An error code of -1 indicates that the security appliance could not open the SNMP trap transport for the interface.

An error code of -2 indicates that the security appliance could not bind the SNMP trap transport for the interface.

**Recommended Action** After the security appliance reclaims some of its resources when traffic is lighter, reenter the **snmp-server host** command for that interface.

## 212003

**Error Message** %PIX|ASA-3-212003: Unable to receive an SNMP request on interface *interface\_number*, error code = *code*, will try again.

**Explanation** This is an SNMP message. This message is displayed because of an internal error in receiving an SNMP request destined for the security appliance on the specified interface.

**Recommended Action** None. The security appliance SNMP agent goes back to wait for the next SNMP request.

## 212004

**Error Message** %PIX|ASA-3-212004: Unable to send an SNMP response to IP Address *IP\_address* Port *port* interface *interface\_number*, error code = *code*

**Explanation** This is an SNMP message. This message is displayed because of an internal error in sending an SNMP response from the security appliance to the specified host on the specified interface.

**Recommended Action** None.

## 212005

**Error Message** %PIX|ASA-3-212005: incoming SNMP request (*number* bytes) on interface *interface\_name* exceeds data buffer size, discarding this SNMP request.

**Explanation** This is an SNMP message. This message reports that the length of the incoming SNMP, request which is destined for the security appliance exceeds the size of the internal data buffer (512 bytes) used for storing the request during internal processing. The security appliance is unable to process this request. This situation does not affect the SNMP traffic passing through the security appliance using any interface.

**Recommended Action** Have the SNMP management station resend the request with a shorter length. For example, instead of querying multiple MIB variables in one request, try querying only one MIB variable in a request. You may need to modify the configuration of the SNMP manager software.

## 212006

**Error Message** %PIX|ASA-3-212006: Dropping SNMP request from *source\_address/source\_port* to *interface\_name:dest\_address/dest\_port* because: *reason*.

**Explanation** This is a SNMP message. This message is displayed if the device is unable to process a SNMP request to the device for the following reasons.

- snmp-server is disabled
- SNMPv3 is not supported

**Recommended Action** Make sure that the SNMP daemon is entering by issuing the **snmp-server enable** command. Only SNMPv1 and v2c packets are handled by the device.

## 213001

**Error Message** %PIX|ASA-3-213001: PPTP control daemon socket io *string*, errno = *number*.

**Explanation** An internal TCP socket I/O error occurred.

**Recommended Action** Contact the Cisco TAC.

## 213002

**Error Message** %PIX|ASA-3-213002: PPTP tunnel hashtable insert failed, peer = *IP\_address*.

**Explanation** An internal software error occurred while creating a new PPTP tunnel.

**Recommended Action** Contact the Cisco TAC.

## 213003

**Error Message** %PIX|ASA-3-213003: PPP virtual interface *interface\_number* isn't opened.

**Explanation** An internal software error occurred while closing a PPP virtual interface.

**Recommended Action** Contact the Cisco TAC.

## 213004

**Error Message** %PIX|ASA-3-213004: PPP virtual interface *interface\_number* client ip allocation failed.

**Explanation** An internal software error occurred while allocating an IP address to the PPTP client.

**Recommended Action** This error occurs when the IP local address pool was depleted. Consider allocating a larger pool with the **ip local pool** command.

## 214001

**Error Message** %PIX|ASA-2-214001: Terminating manager session from *IP\_address* on interface *interface\_name*. Reason: incoming encrypted data (*number* bytes) longer than *number* bytes

**Explanation** An incoming encrypted data packet destined for the security appliance management port indicates a packet length exceeding the specified upper limit. This may be a hostile event. The security appliance immediately terminates this management connection.

**Recommended Action** Ensure that the management connection was initiated by Cisco Secure Policy Manager.

## 215001

**Error Message** %PIX|ASA-2-215001:Bad route\_compress() call, sdb= *number*

**Explanation** An internal software error occurred.

**Recommended Action** Contact the Cisco TAC.

## 217001

**Error Message** %PIX|ASA-2-217001: No memory for *string* in *string*

**Explanation** An operation failed due to low memory.

**Recommended Action** If sufficient memory exists, then copy the error message, the configuration, and any details about the events leading up the error to the Cisco TAC.

## 216001

**Error Message** %ASA-*n*-216001: internal error in: *function*: *message*

**Explanation** This message reports a variety of internal errors that should not appear during normal operation. The severity level varies depending on the cause of the message.

*n*—The message severity.

*function*—The affected component.

*message*—A message describing the cause of the problem.

**Recommended Action** Search the [Bug Toolkit](#) for the specific text message and also try to use the [Output Interpreter](#) to resolve the problem. If you still require assistance, copy the entire error message from the console or the system log. Enter the **show tech-support** command and provide the output along with the error message to Cisco TAC. Use the [Internet](#) to open the case or contact your Cisco TAC representative.

## 216002

**Error Message** PIX|ASA-3-216002: Unexpected event (major: *major\_id*, minor: *minor\_id*) received by *task\_string* in *function* at line: *line\_num*

**Explanation** This message is displayed when a task registers for event notification and the task cannot handle the specific event. Events that can be watched include those associated with queues, booleans, timer services, and so forth. If any of the registered events occur, the scheduler wakes up the task to process the event. This message is generated if an unexpected event woke up the task and it does not know how to handle the event.

If an event is left unprocessed, it can wake up the task very often to make sure it is processed, but this should not occur under normal conditions. If this message is displayed, it does not necessarily mean the box is unusable, but something unusual has occurred and needs to be investigated.

*major\_id*—Event identifier

*minor\_id*—Event identifier

*task\_string*—Custom string passed by the task to identify itself

*function*—The function that received the unexpected event

*line\_num* —Line number in the code

**Recommended Action** Copy the error message and submit it to Cisco TAC along with the configuration and any details about the events leading up to this error.

## 216003

**Error Message** %PIX|ASA-3-216003: Unrecognized timer *timer\_ptr*, *timer\_id* received by *task\_string* in *function* at line: *line\_num*

**Explanation** This message is displayed when an unexpected timer event woke up the task and the task does not know how to handle the event. A task can register a set of timer services with the scheduler. If any of the timers expire, the scheduler wakes up the task to take action. This message is generated if the task is woken up by an unrecognized timer event.

An expired timer, if left unprocessed, wakes up the task continuously to make sure it is processed, and this is undesirable. This should not occur under normal conditions. If This message is displayed, it does not necessarily mean the box is unusable, but something unusual has occurred and needs to be investigated.

*timer\_ptr*—Pointer to the timer

*timer\_id*—Timer identifier

*task\_string*—Custom string passed by the task to identify itself

*function*—The function that received the unexpected event

*line\_num*—Line number in the code

**Recommended Action** Copy the error message and submit it to the Cisco TAC along with the configuration and any details about the events leading up to this error.

## 218001

**Error Message** %PIX|ASA-2-218001: Failed Identification Test in *slot#* [*fail#*/*res*].

**Explanation** The module in *slot#* of the security appliance could not be identified as a genuine Cisco product. Cisco warranties and support programs apply only to genuine Cisco products. If Cisco determines that the cause of a support issue is related to non-Cisco memory, SSM modules, SSC cards, or other modules, Cisco may deny support under your warranty or under a Cisco support program such as SmartNet.

**Recommended Action** If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If you still require assistance, contact the Cisco TAC and provide the representative with the information you gathered. You can access the Output Interpreter, Bug Toolkit, or open a case with the Cisco TAC online at <http://www.cisco.com/kobayashi/support/tac/tools.shtml>.

## 218002

**Error Message** %PIX|ASA-2-218002: Module (*slot#*) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.

**Explanation** Hardware in the specified location is a prototype module that came from a Cisco lab.

**Recommended Action** If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search of the Bug Toolkit. If you still require assistance, contact the Cisco TAC and provide the representative with the information you gathered. You can access the Output Interpreter, Bug Toolkit, or open a case with the Cisco TAC online at <http://www.cisco.com/kobayashi/support/tac/tools.shtml>.

## 218003

**Error Message** %PIX|ASA-2-218003: Module Version in <slot#> is obsolete. The module in slot = <slot#> is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.

**Explanation** This syslog message is generated when obsolete hardware is detected or when the **show module** command is entered for the module. This syslog is generated every minute once it starts.

**Recommended Action** If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search of the Bug Toolkit. If you still require assistance, contact the Cisco TAC and provide the representative with the information you gathered. You can access the Output Interpreter, Bug Toolkit, or open a case with the Cisco TAC online at <http://www.cisco.com/kobayashi/support/tac/tools.shtml>.

## 218004

**Error Message** %PIX|ASA-2-218004: Failed Identification Test in *slot#* [*fail#*/*res*]

**Explanation** There was a problem while identifying hardware in the specified location.

**Recommended Action** If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search of the Bug Toolkit. If you still require assistance, contact the Cisco TAC and provide the representative with the information you gathered. You can access the Output Interpreter, Bug Toolkit, or open a case with the Cisco TAC online at <http://www.cisco.com/kobayashi/support/tac/tools.shtml>.

## 219002

**Error Message** %ASA-3-219002: *I2C\_API\_name* error, slot = *slot\_number*, device = *device\_number*, address = *address*, byte count = *count*. Reason: *reason\_string*

**Explanation** The I2C serial bus API has failed. This might be because of a hardware or software problem.

- *I2C\_API\_name*—The I2C API that failed:
  - I2C\_read\_byte\_w\_wait()
  - I2C\_read\_word\_w\_wait()
  - I2C\_read\_block\_w\_wait()
  - I2C\_write\_byte\_w\_wait()
  - I2C\_write\_word\_w\_wait()
  - I2C\_write\_block\_w\_wait()
  - I2C\_read\_byte\_w\_suspend()
  - I2C\_read\_word\_w\_suspend()
  - I2C\_read\_block\_w\_suspend()
  - I2C\_write\_byte\_w\_suspend()
  - I2C\_write\_word\_w\_suspend()
  - I2C\_write\_block\_w\_suspend()
- *slot\_number*—The hexadecimal number of the slot where the I/O operation that generated the syslog occurred. The slot number cannot be unique to a slot in the chassis. Depending on the chassis, two different slots might have the same I2C slot number. Also the value is not necessarily less than or equal to the number of slots. The value depends on the way the I2C hardware is wired.
- *device\_number*—The hexadecimal number of the device on the slot the I/O operation was performed.
- *address*—This is the hexadecimal address of the device on which the I/O operation occurred.
- *byte\_count*—This is the byte count in decimal of the I/O operation.
- *error\_string*—The reason for the error:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UNSupport
  - I2C\_BYTE\_COUNT\_ERROR



- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event. If the syslog message does not occur continuously and goes away after a few minutes, it might be because the I2C serial bus is busy.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## Messages 302003 to 335014

This section contains messages from 302003 to 335014.

### 302003

**Error Message** %PIX|ASA-6-302003: Built H245 connection for foreign\_address outside\_address/outside\_port local\_address inside\_address/inside\_port

**Explanation** This is a connection-related message. This message is displayed when an H.245 connection is started from the *outside\_address* to the *inside\_address*. This message only occurs if the security appliance detects the use of an Intel Internet phone. The foreign port (outside port) only displays on connections from outside the security appliance. The local port value (inside port) only appears on connections started on an internal interface.

**Recommended Action** None.

### 302004

**Error Message** %PIX|ASA-6-302004: Pre-allocate H323 UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port

**Explanation** This is a connection-related message. This message is displayed when an H.323 UDP back-connection is preallocated to the foreign address (*outside\_address*) from the local address (*inside\_address*). This message only occurs if the security appliance detects the use of an Intel Internet phone. The foreign port (*outside\_port*) only displays on connections from outside the security appliance. The local port value (*inside\_port*) only appears on connections started on an internal interface.

**Recommended Action** None.

## 302009

**Error Message** %PIX|ASA-6-302009: Rebuilt TCP connection number for foreign\_address outside\_address/outside\_port global\_address global\_address/global\_port local\_address inside\_address/inside\_port

**Explanation** This is a connection-related message. This message appears after a TCP connection is rebuilt after a failover. A sync packet is not sent to the other security appliance. The *outside\_address* IP address is the foreign host, the *global\_address* IP address is a global address on the lower security level interface, and the *inside\_address* IP address is the local IP address “behind” the security appliance on the higher security level interface.

**Recommended Action** None.

## 302010

**Error Message** %PIX|ASA-6-302010: connections in use, connections most used

**Explanation** This is a connection-related message. This message appears after a TCP connection restarts. *connections* is the number of connections.

**Recommended Action** None.

## 302012

**Error Message** %PIX|ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP\_address/port to laddr IP\_address

**Explanation** An H.225 secondary channel has been preallocated.

**Recommended Action** None.

## 302013

**Error Message** %PIX|ASA-6-302013: Built {inbound|outbound} TCP connection\_id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]

**Explanation** A TCP connection slot between two hosts was created.

- *connection\_id* is a unique identifier.
- *interface, real-address, real-port* identify the actual sockets.
- *mapped-address, mapped-port* identify the mapped sockets.
- *user* is the AAA name of the user.

If inbound is specified, the original control connection was initiated from the outside. For example, for FTP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, the original control connection was initiated from the inside.

**Recommended Action** None.

## 302014

**Error Message** %PIX|ASA-6-302014: Teardown TCP connection *id* for *interface:real-address/real-port* to *interface:real-address/real-port* duration *hh:mm:ss* bytes *bytes* [*reason*] [*user*]

**Explanation** A TCP connection between two hosts was deleted. The following list describes the message values:

- connection *id* is a unique identifier.
- *interface*, *real-address*, *real-port* identify the actual sockets.
- *duration* is the lifetime of the connection.
- bytes *bytes* is the data transfer of the connection.
- *user* is the AAA name of the user.

The *reason* variable presents the action that causes the connection to terminate. Set the *reason* variable to one of the TCP termination reasons listed in [Table 2-2](#).

**Table 2-2 TCP Termination Reasons**

Reason	Description
Conn-timeout	Connection ended because it was idle longer than the configured idle timeout.
Deny Terminate	Flow was terminated by application inspection.
Failover primary closed	The standby unit in a failover pair deleted a connection because of a message received from the active unit.
FIN Timeout	Force termination after 10 minutes awaiting the last ACK or after half-closed timeout.
Flow closed by inspection	Flow was terminated by inspection feature.
Flow terminated by IPS	Flow was terminated by IPS.
Flow reset by IPS	Flow was reset by IPS.
Flow terminated by TCP Intercept	Flow was terminated by TCP Intercept.
Invalid SYN	SYN packet not valid.
Idle Timeout	Connection timed out because it was idle longer than timeout value.
IPS fail-close	Flow was terminated due to IPS card down.
SYN Control	Back channel initiation from wrong side.
SYN Timeout	Force termination after 30 seconds awaiting three-way handshake completion.

**Table 2-2 TCP Termination Reasons (continued)**

Reason	Description
TCP bad retransmission	Connection terminated because of bad TCP retransmission.
TCP FINs	Normal close down sequence.
TCP Invalid SYN	Invalid TCP SYN packet.
TCP Reset-I	Reset was from the inside.
TCP Reset-O	Reset was from the outside.
TCP segment partial overlap	Detected a partially overlapping segment.
TCP unexpected window size variation	Connection terminated due to variation in the TCP window size.
Tunnel has been torn down	Flow terminated because tunnel is down.
Unauth Deny	Denied by URL filter.
Unknown	Catch-all error.
Xlate Clear	Command-line removal

**Recommended Action** None.

## 302015

**Error Message** %PIX|ASA-6-302015: Built {inbound|outbound} UDP connection *number* for *interface\_name:real\_address/real\_port (mapped\_address/mapped\_port)* to *interface\_name:real\_address/real\_port (mapped\_address/mapped\_port)* [(*user*)]

**Explanation** A UDP connection slot between two hosts is created. The following list describes the message values:

- *connection number*—A unique identifier.
- *interface, real\_address, real\_port*—The actual sockets.
- *mapped\_address and mapped\_port*—The mapped sockets.
- *user*—The AAA name of the user.

If inbound is specified, then the original control connection is initiated from the outside. For example, for UDP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, then the original control connection is initiated from the inside.

**Recommended Action** None.

## 302016

**Error Message** %PIX|ASA-6-302016: Teardown UDP connection *number* for *interface:real-address/real-port* to *interface:real-address/real-port* duration *hh:mm:ss* bytes *bytes* [ (*user*) ]

**Explanation** A UDP connection slot between two hosts was deleted. The following list describes the message values:

- *connection number* is an unique identifier.
- *interface, real\_address, real\_port* are the actual sockets.
- *time* is the lifetime of the connection.
- *bytes* is the data transfer of the connection.
- *connection id* is an unique identifier.
- *interface, real-address, real-port* are the actual sockets.
- *duration* is the lifetime of the connection.
- *bytes* is the data transfer of the connection.
- *user* is the AAA name of the user.

**Recommended Action** None.

## 302017

**Error Message** %PIX|ASA-6-302017: Built {*inbound|outbound*} GRE connection *id* from *interface:real\_address (translated\_address)* to *interface:real\_address/real\_cid (translated\_address/translated\_cid)* [ (*user*) ]

**Explanation** A GRE connection slot between two hosts is created. The *id* is an unique identifier. The *interface, real\_address, real\_cid* tuple identifies the one of the two simplex PPTP GRE streams. The parenthetical *translated\_address, translated\_cid* tuple identifies the translated value with NAT.

If *inbound* is indicated, then the connection can only be used inbound. If *outbound* is indicated, then the connection can only be used for outbound. The following list describes the message values:

- *id*—Unique number identifying the connection.
- *inbound*—Control connection is for inbound PPTP GRE flow.
- *outbound*—Control connection is for outbound PPTP GRE flow.
- *interface\_name*—The interface name.
- *real\_address*—IP address of the actual host.
- *real\_cid*—Untranslated call-ID for the connection.
- *translated\_address*—IP address after translation.
- *translated\_cid*—Translated call.

- *user*—AAA user name.

**Recommended Action** This is an informational message.

## 302018

**Error Message** %PIX|ASA-6-302018: Teardown GRE connection *id* from *interface:real\_address (translated\_address)* to *interface:real\_address/real\_cid (translated\_address/translated\_cid)* duration *hh:mm:ss* bytes *bytes [(user)]*

**Explanation** A GRE connection slot between two hosts is deleted. The *interface*, *real\_address*, *real\_port* tuples identify the actual sockets. *Duration* accounts the lifetime of the connection. The following list describes the message values:

- *id*—Unique number identifying the connection.
- *interface*—The interface name.
- *real\_address*—IP address of the actual host.
- *real\_port*—Port number of the actual host.
- *hh:mm:ss*—Time in hour:minute:second format.
- *bytes*—Number of PPP bytes transferred in the GRE session.
- *reason*—Reason why the connection was terminated.
- *user*—AAA user name.

**Recommended Action** This is an informational message.

## 302019

**Error Message** %PIX|ASA-3-302019: H.323 *library\_name* ASN Library failed to initialize, error code *number*

**Explanation** The specified ASN library that the security appliance uses for decoding the H.323 messages failed to initialize; the security appliance cannot decode or inspect the arriving H.323 packet. The security appliance allows the H.323 packet to pass through without any modification. When the next H.323 message arrives, the security appliance attempts to initialize the library again.

**Recommended Action** If this message is generated consistently for a particular library, contact the Cisco TAC and provide them with all log messages (preferably with timestamps).

## 302020

**Error Message** %PIX|ASA-6-302020: Built {in | out}bound ICMP connection for faddr {faddr | icmp\_seq\_num} gaddr {gaddr | cmp\_type} laddr laddr

**Explanation** An ICMP session was established in fast-path when stateful ICMP is enabled using the **fixup protocol icmp** command.

**Recommended Action** None.

## 302021

**Error Message** %PIX|ASA-6-302021: Teardown ICMP connection for faddr {faddr | icmp\_seq\_num} gaddr {gaddr | cmp\_type} laddr laddr

**Explanation** An ICMP session was removed in fast-path when stateful ICMP is enabled using the **fixup protocol icmp** command.

**Recommended Action** None.

## 302302

**Error Message** %PIX|ASA-3-302302: ACL = deny; no sa created

**Explanation** IPSec proxy mismatches. Proxy hosts for the negotiated SA correspond to a deny **access-list** command policy.

**Recommended Action** Check the **access-list** command statement in the configuration. Contact the administrator for the peer.

## 303002

**Error Message** PIX-6-303002: FTP connection from *src\_ifc:src\_ip/src\_port* to *dst\_ifc:dst\_ip/dst\_port*, user *username* action *file filename*

**Explanation** This event is generated whenever a client uploads or downloads a file from the FTP server.

*src\_ifc*—The interface where the client resides.

*src\_ip*—The IP address of the client.

*src\_port*—The client port.

*dst\_ifc*—The interface where the server resides.

*dst\_ip*—The IP address of the FTP server.

*dst\_port*—The server port.

*username*—The FTP username.

*action*—The stored/retrieved actions.

*filename*—The file stored or retrieved.

**Recommended Action** None.

## 303004

**Error Message** %PIX|ASA-5-303004: FTP *cmd\_string* command unsupported - failed strict inspection, terminating connection from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_interface*

**Explanation** This message is generated when using strict FTP inspection on FTP traffic. It is displayed if an FTP request message contains a command that is not recognized by the device.

**Recommended Action** None.

## 303005

**Error Message** %PIX|ASA-5-303005: Strict FTP inspection matched *match\_string* in policy-map *policy-name*, *action\_string* from *src\_ifc:sip/sport* to *dest\_ifc:dip/dport*

**Explanation** This message is generated when FTP inspection matches any of the following configured values: filename, file type, request command, server, or user name. Then the action specified by the *action\_string* in this syslog message occurs.

*match\_string*—The match clause in the policy-map.

*policy-name*—The policy-map that matched.

*action\_string*—The action to take; for example, “Reset Connection.”

*src\_ifc*—The source interface name.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

**Recommended Action** None.



## 304001

**Error Message** %PIX|ASA-5-304001: *user source\_address* Accessed {JAVA URL|URL}  
*dest\_address: url*.

**Explanation** This is an FTP/URL message. This message is displayed when the specified host attempts to access the specified URL.

**Recommended Action** None.

## 304002

**Error Message** %PIX|ASA-5-304002: Access denied URL *chars* SRC *IP\_address* DEST *IP\_address*:  
*chars*

**Explanation** This is an FTP/URL message. This message is displayed if access from the source address to the specified URL or FTP site is denied.

**Recommended Action** None.

## 304003

**Error Message** %PIX|ASA-3-304003: URL Server *IP\_address* timed out URL *url*

**Explanation** A URL server timed out.

**Recommended Action** None.

## 304004

**Error Message** %PIX|ASA-6-304004: URL Server *IP\_address* request failed URL *url*

**Explanation** This is an FTP/URL message. This message is displayed if a Websense server request fails.

**Recommended Action** None.

## 304005

**Error Message** %PIX|ASA-7-304005: URL Server *IP\_address* request pending URL *url*

**Explanation** This is an FTP/URL message. This message is displayed when a Websense server request is pending.

**Recommended Action** None.

## 304006

**Error Message** %PIX|ASA-3-304006: URL Server *IP\_address* not responding

**Explanation** This is an FTP/URL message. The Websense server is unavailable for access, and the security appliance attempts to either try to access the same server if it is the only server installed, or another server if there is more than one.

**Recommended Action** None.

## 304007

**Error Message** %PIX|ASA-2-304007: URL Server *IP\_address* not responding, ENTERING ALLOW mode.

**Explanation** This is an FTP/URL message. This message is displayed when you use the **allow** option of the **filter** command, and the Websense servers are not responding. The security appliance allows all web requests to continue without filtering while the servers are not available.

**Recommended Action** None.

## 304008

**Error Message** %PIX|ASA-2-304008: LEAVING ALLOW mode, URL Server is up.

**Explanation** This is an FTP/URL message. This message is displayed when you use the **allow** option of the **filter** command, and the security appliance receives a response message from a Websense server that previously was not responding. With this response message, the security appliance exits the allow mode, which enables the URL filtering feature again.

**Recommended Action** None.

## 304009

**Error Message** %PIX|ASA-7-304009: Ran out of buffer blocks specified by `url-block` command

**Explanation** The URL pending buffer block is running out of space.

**Recommended Action** Change the buffer block size by entering the `url-block block block_size` command.

## 305005

**Error Message** %PIX|ASA-3-305005: No translation group found for `protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port`

**Explanation** A packet does not match any of the outbound `nat` command rules.

**Recommended Action** This message indicates a configuration error. If dynamic NAT is desired for the source host, ensure that the `nat` command matches the source IP address. If static NAT is desired for the source host, ensure that the local IP address of the `static` command matches. If no NAT is desired for the source host, check the ACL bound to the NAT 0 ACL.

## 305006

**Error Message** %PIX|ASA-3-305006: {outbound static|identity|portmap|regular) translation creation failed for `protocol src interface_name:source_address/source_port dst interface_name:dest_address/dest_port`

**Explanation** A protocol (UDP, TCP, or ICMP) failed to create a translation through the security appliance. This message appears as a fix to caveat CSCdr00663 that requested that security appliance not allow packets that are destined for network or broadcast addresses. The security appliance provides this checking for addresses that are explicitly identified with `static` command statements. With the change, for inbound traffic, the security appliance denies translations for a destined IP address identified as a network or broadcast address.

The security appliance does not apply PAT to all ICMP message types; it only applies PAT ICMP echo and echo-reply packets (types 8 and 0). Specifically, only ICMP echo or echo-reply packets create a PAT xlate. So, when the other ICMP messages types are dropped, system log message 305006 (on the security appliance) is generated.

The security appliance utilizes the global IP and mask from configured `static` command statements to differ regular IP addresses from network or broadcast IP addresses. If the global IP address is a valid network address with a matching network mask, then the security appliance does not create a translation for network or broadcast IP addresses with inbound packets.

For example:

```
static (inside,outside) 10.2.2.128 10.1.1.128 netmask 255.255.255.128
```

Global address 10.2.2.128 is responded to as a network address and 10.2.2.255 is responded to as the broadcast address. Without an existing translation, security appliance denies inbound packets destined for 10.2.2.128 or 10.2.2.255, and logs this system log message.

When the suspected IP is a host IP, configure a separated **static** command statement with a host mask in front of the subnet static (first match rule for **static** command statements). The following static causes the security appliance to respond to 10.2.2.128 as a host address:

```
static (inside,outside) 10.2.2.128 10.2.2.128 netmask 255.255.255.255
static (inside,outside) 10.2.2.128 10.2.2.128 netmask 255.255.255.128
```

The translation may be created by traffic started with the inside host with the questioned IP address. Because the security appliance views a network or broadcast IP address as a host IP address with overlapped subnet static configuration, the network address translation for both **static** command statements must be the same.

**Recommended Action** None.

## 305007

**Error Message** %PIX|ASA-6-305007: addrpool\_free(): Orphan IP *IP\_address* on interface *interface\_number*

**Explanation** The security appliance has attempted to translate an address that it cannot find in any of its global pools. The security appliance assumes that the address was deleted and drops the request.

**Recommended Action** None.

## 305008

**Error Message** %PIX|ASA-3-305008: Free unallocated global IP address.

**Explanation** The security appliance kernel detected an inconsistency condition when trying to free an unallocated global IP address back to the address pool. This abnormal condition may occur if the security appliance is running a Stateful Failover setup and some of the internal states are momentarily out of synchronization between the active unit and the standby unit. This condition is not catastrophic, and the sync recovers automatically.

**Recommended Action** Report this condition to Cisco TAC if you continue to see this message.

## 305009

**Error Message** %PIX|ASA-6-305009: Built {dynamic|static} translation from *interface\_name [(acl-name)]:real\_address* to *interface\_name:mapped\_address*

**Explanation** An address translation slot was created. The slot translates the source address from the local side to the global side. In reverse, the slot translates the destination address from the global side to the local side.

**Recommended Action** None.

## 305010

**Error Message** %PIX|ASA-6-305010: Teardown {dynamic|static} translation from *interface\_name:real\_address* to *interface\_name:mapped\_address* duration *time*

**Explanation** The address translation slot was deleted.

**Recommended Action** None.

## 305011

**Error Message** %PIX|ASA-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from *interface\_name:real\_address/real\_port* to *interface\_name:mapped\_address/mapped\_port*

**Explanation** A TCP, UDP, or ICMP address translation slot was created. The slot translates the source socket from the local side to the global side. In reverse, the slot translates the destination socket from the global side to the local side.

**Recommended Action** None.

## 305012

**Error Message** %PIX|ASA-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from *interface\_name [(acl-name)]:real\_address/{real\_port|real\_ICMP\_ID}* to *interface\_name:mapped\_address/{mapped\_port|mapped\_ICMP\_ID}* duration *time*

**Explanation** The address translation slot was deleted.

**Recommended Action** None.

## 308001

**Error Message** %PIX|ASA-6-308001: console enable password incorrect for *number* tries (from *IP\_address*)

**Explanation** This is a security appliance management message. This message is displayed after the specified number of times a user incorrectly types the password to enter privileged mode. The maximum is three attempts.

**Recommended Action** Verify the password and try again.

## 308002

**Error Message** %PIX|ASA-4-308002: static *global\_address inside\_address* netmask *netmask* overlapped with *global\_address inside\_address*

**Explanation** The IP addresses in one or more **static** command statements overlap. *global\_address* is the global address, which is the address on the lower security interface, and *inside\_address* is the local address, which is the address on the higher security-level interface.

**Recommended Action** Use the **show static** command to view the **static** command statements in your configuration and fix the commands that overlap. The most common overlap occurs if you specify a network address such as 10.1.1.0, and in another **static** command you specify a host within that range such as 10.1.1.5.

## 311001

**Error Message** %PIX|ASA-6-311001: LU loading standby start

**Explanation** Stateful Failover update information was sent to the standby security appliance when the standby security appliance is first to be online.

**Recommended Action** None.

## 311002

**Error Message** %PIX|ASA-6-311002: LU loading standby end

**Explanation** Stateful Failover update information stopped sending to the standby security appliance.

**Recommended Action** None.

## 311003

**Error Message** %PIX|ASA-6-311003: LU recv thread up

**Explanation** An update acknowledgment was received from the standby security appliance.

**Recommended Action** None.

## 311004

**Error Message** %PIX|ASA-6-311004: LU xmit thread up

**Explanation** This message appears when a Stateful Failover update is transmitted to the standby security appliance.

**Recommended Action** None.

## 312001

**Error Message** %PIX|ASA-6-312001: RIP hdr failed from *IP\_address*: cmd=*string*, version=*number* domain=*string* on interface *interface\_name*

**Explanation** The security appliance received a RIP message with an operation code other than reply, the message has a version number different from what is expected on this interface, and the routing domain entry was nonzero.

**Recommended Action** This message is informational, but it may also indicate that another RIP device is not configured correctly to communicate with the security appliance.

## 313001

**Error Message** %PIX|ASA-3-313001: Denied ICMP type=*number*, code=*code* from *IP\_address* on interface *interface\_name*

**Explanation** When using the **icmp** command with an access list, if the first matched entry is a permit entry, the ICMP packet continues processing. If the first matched entry is a deny entry or an entry is not matched, the security appliance discards the ICMP packet and generates this system log message. The **icmp** command enables or disables pinging to an interface. With pinging disabled, the security appliance cannot be detected on the network. This feature is also referred to as configurable proxy pinging.

**Recommended Action** Contact the administrator of the peer device.

## 313004

**Error Message** %PIX|ASA-4-313004:Denied ICMP type=*icmp\_type*, from *source\_address* on interface *interface\_name* to *dest\_address*:no matching session

**Explanation** ICMP packets were dropped by the security appliance because of security checks added by the stateful ICMP feature that are usually either ICMP echo replies without a valid echo request already passed across the security appliance or ICMP error messages not related to any TCP, UDP, or ICMP session already established in the security appliance.

**Recommended Action** None.

## 313005

**Error Message** %PIX|ASA-4-313005: No matching connection for ICMP error message: *icmp\_msg\_info* on *interface\_name* interface. Original IP payload:  
*embedded\_frame\_info icmp\_msg\_info = icmp src src\_interface\_name:src\_address dst dest\_interface\_name:dest\_address (type icmp\_type, code icmp\_code)*  
*embedded\_frame\_info = prot src source\_address/source\_port dst dest\_address/dest\_port*

**Explanation** ICMP error packets were dropped by the security appliance because the ICMP error messages are not related to any session already established in the security appliance.

**Recommended Action** If the cause is an attack, you can deny the host by using ACLs.

## 313008

**Error Message** %PIX|ASA-3-313008: Denied ICMPv6 type=*number*, code=*code* from *IP\_address* on interface *interface\_name*

**Explanation** When using the **icmp** command with an access list, if the first matched entry is a permit entry, the ICMPv6 packet continues processing. If the first matched entry is a deny entry, or an entry is not matched, the security appliance discards the ICMPv6 packet and generates this system log message.

The **icmp** command enables or disables ping to an interface. When ping is disabled, the security appliance is undetectable on the network. This feature is also referred to as “configurable proxy ping.”

**Recommended Action** Contact the administrator of the peer device.



## 314001

**Error Message** %PIX|ASA-6-314001: Pre-allocate RTSP UDP backconnection for foreign\_address *outside\_address/outside\_port* to local\_address *inside\_address/inside\_port*

**Explanation** The security appliance opened an RTSP connection for the specified IP addresses and ports.

**Recommended Action** None.

## 315004

**Error Message** %PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.

**Explanation** The security appliance could not find the security appliance RSA host key, which is required for establishing an SSH session. The security appliance host key may be absent because it was not generated or because the license for this security appliance does not allow DES or 3DES.

**Recommended Action** From the security appliance console, enter the **show crypto key mypubkey rsa** command to verify that the RSA host key is present. If the host key is not present, enter the **show version** command to verify that DES or 3DES is allowed. If an RSA host key is present, restart the SSH session. To generate the RSA host key, enter the **crypto key mypubkey rsa** command.

## 315011

**Error Message** %PIX|ASA-6-315011: SSH session from *IP\_address* on interface *interface\_name* for user *user* disconnected by SSH server, reason: *reason*

**Explanation** This message appears after an SSH session completes. If a user enters **quit** or **exit**, the **terminated normally** message displays. If the session disconnected for another reason, the text describes the reason. [Table 2-3](#) lists the possible reasons why a session disconnected.

**Table 2-3 SSH Disconnect Reasons**

Text String	Explanation	Action
Bad checkbytes	A mismatch was detected in the check bytes during an SSH key exchange.	Restart the SSH session.
CRC check failed	The CRC value computed for a particular packet does not match the CRC value embedded in the packet; the packet is bad.	None. If this message persists, call Cisco TAC.
Decryption failure	Decryption of an SSH session key failed during an SSH key exchange.	Check the RSA host key and try again.
Format error	A non-protocol version message was received during an SSH version exchange.	Check the SSH client, to ensure it is a supported version.
Internal error	This message indicates either an error internal to SSH on the security appliance or an RSA key may not have been entered on the security appliance or cannot be retrieved.	From the security appliance console, enter the <b>show crypto key mypubkey rsa</b> command to verify that the RSA host key is present. If the host key is not present, enter the <b>show version</b> command to verify that DES or 3DES is allowed. If an RSA host key is present, restart the SSH session. To generate the RSA host key, enter the <b>crypto key mypubkey rsa</b> command.
Invalid cipher type	The SSH client requested an unsupported cipher.	Enter the <b>show version</b> command to determine what features your license supports, then reconfigure the SSH client to use the supported cipher.
Invalid message length	The length of SSH message arriving at the security appliance exceeds 262,144 bytes or is shorter than 4096 bytes. The data may be corrupted.	None.
Invalid message type	The security appliance received a non-SSH message, or an unsupported or unwanted SSH message.	Check whether the peer is an SSH client. If it is a client supporting SSHv1, and this message persists, from the security appliance serial console enter the <b>debug ssh</b> command and capture the debug messages. contact the Cisco TAC.

**Table 2-3 SSH Disconnect Reasons (continued)**

Text String	Explanation	Action
Out of memory	This message appears when the security appliance cannot allocate memory for use by the SSH server, probably when the security appliance is busy with high traffic.	Restart the SSH session later.
Rejected by server	User authentication failed.	Ask the user to verify their username and password.
Reset by client	An SSH client sent the SSH_MSG_DISCONNECT message to the security appliance.	None.
status code: <i>hex</i> ( <i>hex</i> )	Users closed the SSH client window (running on Windows) instead of entering <b>quit</b> or <b>exit</b> at the SSH console.	None. Encourage users to exit the client gracefully instead of just exiting.
Terminated by operator	The SSH session was terminated by entering the <b>ssh disconnect</b> command at the security appliance console.	None.
Time-out activated	The SSH session timed out because the duration specified by the <b>ssh timeout</b> command was exceeded.	Restart the SSH connection. You can use the <b>ssh timeout</b> command to increase the default value of 5 minutes up to 60 minutes if required.

**Recommended Action** None.

## 316001

**Error Message** %PIX|ASA-3-316001: Denied new tunnel to *IP\_address*. VPN peer limit (*platform\_vpn\_peer\_limit*) exceeded

**Explanation** If more VPN tunnels (ISAKMP/IPSec) are concurrently attempting to be established than supported by the platform VPN peer limit, then the excess tunnels are aborted.

**Recommended Action** None.

## 317001

**Error Message** %PIX|ASA-3-317001: No memory available for limit\_slow

**Explanation** The requested operation failed because of a low-memory condition.

**Recommended Action** Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

## 317002

**Error Message** %PIX|ASA-3-317002: Bad path index of *number* for *IP\_address*, *number* max

**Explanation** A software error occurred.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC for assistance.

## 317003

**Error Message** %PIX|ASA-3-317003: IP routing table creation failure - *reason*

**Explanation** An internal software error occurred, which prevented the creation of new IP routing table.

**Recommended Action** Copy the message exactly as it appears, and report it to Cisco TAC.

## 317004

**Error Message** %PIX|ASA-3-317004: IP routing table limit warning

**Explanation** The number of routes in the named IP routing table has reached the configured warning limit.

**Recommended Action** Reduce the number of routes in the table, or reconfigure the limit.

## 317005

**Error Message** %PIX|ASA-3-317005: IP routing table limit exceeded - *reason*, *IP\_address* *netmask*

**Explanation** Additional routes will be added to the table.

**Recommended Action** Reduce the number of routes in the table, or reconfigure the limit.

## 318001

**Error Message** %PIX|ASA-3-318001: Internal error: *reason*

**Explanation** An internal software error occurred. This message occurs at 5-second intervals.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC for assistance.

## 318002

**Error Message** %PIX|ASA-3-318002: Flagged as being an ABR without a backbone area

**Explanation** The router was flagged as an area border router (ABR) without a backbone area configured in the router. This message occurs at 5-second intervals.

**Recommended Action** Restart the OSPF process.

## 318003

**Error Message** %PIX|ASA-3-318003: Reached unknown state in neighbor state machine

**Explanation** An internal software error occurred. This message occurs at 5 second intervals.

**Recommended Action** None.

## 318004

**Error Message** %PIX|ASA-3-318004: area *string* lsid *IP\_address* mask *netmask* adv *IP\_address* type *number*

**Explanation** OSPF had a problem locating the link state advertisement (LSA), which might lead to a memory leak.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC for assistance.

## 318005

**Error Message** %PIX|ASA-3-318005: lsid *ip\_address* adv *IP\_address* type *number* gateway *gateway\_address* metric *number* network *IP\_address* mask *netmask* protocol *hex* attr *hex* net-metric *number*

**Explanation** OSPF found an inconsistency between its database and the IP routing table.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC for assistance.

## 318006

**Error Message** %PIX|ASA-3-318006: if *interface\_name* if\_state *number*

**Explanation** An internal error occurred.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC for assistance.

## 318007

**Error Message** %PIX|ASA-3-318007: OSPF is enabled on *interface\_name* during idb initialization

**Explanation** An internal error occurred.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC for assistance.

## 318008

**Error Message** %PIX|ASA-3-318008: OSPF process *number* is changing router-id. Reconfigure virtual link neighbors with our new router-id

**Explanation** The OSPF process is being reset, and it is going to select a new router ID. This action will bring down all virtual links.

**Recommended Action** Change virtual link configuration on all of the virtual link neighbors to reflect the new router ID.

## 318009

**Error Message** %PIX|ASA-3-318009: OSPF: Attempted reference of stale data encountered in *function*, line: *line\_num*

**Explanation** This message is displayed when OSPF is running and tries to reference some related data structures that have been removed elsewhere. Clearing interface and router configurations may resolve the problem. However, if this message appears, some sequence of steps caused premature deletion of data structures and this needs to be investigated.

*function*—The function that received the unexpected event

*line\_num*—Line number in the code

**Recommended Action** Copy the error message and submit it to the Cisco TAC along with the configuration and any details about the events leading up to this error.

## 319001

**Error Message** %PIX|ASA-3-319001: Acknowledge for arp update for IP address *dest\_address* not received (*number*).

**Explanation** The ARP process in the security appliance lost internal synchronization because the system was overloaded.

**Recommended Action** No immediate action is required. The failure is only temporary. Check the average load of the system and make sure it is not used beyond its capabilities.

## 319002

**Error Message** %PIX|ASA-3-319002: Acknowledge for route update for IP address *dest\_address* not received (*number*).

**Explanation** The routing module in the security appliance lost internal synchronization because the system was overloaded.

**Recommended Action** No immediate action required. The failure is only temporary. Check the average load of the system and make sure it is not used beyond its capabilities.

## 319003

**Error Message** %PIX|ASA-3-319003: Arp update for IP address *address* to NPn failed.

**Explanation** When an ARP entry has to be updated, a message is sent to the network processor (NP) in order to update the internal ARP table. If the module is experiencing high utilization of memory or if the internal table is full, the message to the NP may be rejected and this message generated.

**Recommended Action** Verify if the ARP table is full. If it is not full, check the load of the module with respect to the CPU utilization and connections per second. If CPU utilization is high and/or there is a large number of connections per second, normal operations will resume when the load returns to normal.

## 319004

**Error Message** %PIX|ASA-3-319004: Route update for IP address *dest\_address* failed (*number*).

**Explanation** The routing module in the FWSM lost internal synchronization because the system was overloaded.

**Recommended Action** No immediate action required. The failure is only temporary. Check the average load of the system and make sure it is not used beyond its capabilities.

## 320001

**Error Message** %PIX|ASA-3-320001: The subject name of the peer cert is not allowed for connection

**Explanation** When the security appliance is an easy VPN remote device or server, the peer certificate contains a subject name that does not match the **ca verifycertdn** command.

**Recommended Action** This message might indicate a “man in the middle” attack, where a device spoofs the peer IP address and attempts to intercept a VPN connection from the security appliance.

## 321001

**Error Message** %PIX|ASA-5-321001: Resource *var1* limit of *var2* reached.

**Explanation** A configured resource usage or rate limit for the indicated resource was reached.

**Recommended Action** None.

## 321002

**Error Message** %PIX|ASA-5-321002: Resource *var1* rate limit of *var2* reached.

**Explanation** A configured resource usage or rate limit for the indicated resource was reached.

**Recommended Action** None.

## 321003

**Error Message** %PIX|ASA-6-321003: Resource *var1* log level of *var2* reached.

**Explanation** A configured resource usage or rate log level for the indicated resource was reached.

**Recommended Action** None.

## 321004

**Error Message** %PIX|ASA-6-321004: Resource *var1* rate log level of *var2* reached

**Explanation** A configured resource usage or rate log level for the indicated resource was reached.

**Recommended Action** None.



## 322001

**Error Message** %PIX|ASA-3-322001: Deny MAC address *MAC\_address*, possible spoof attempt on interface *interface*

**Explanation** The security appliance received a packet from the offending MAC address on the specified interface but the source MAC address in the packet is statically bound to another interface in your configuration. This could be caused by either be a MAC-spoofing attack or a misconfiguration.

**Recommended Action** Check the configuration and take appropriate action by either finding the offending host or correcting the configuration.

## 322002

**Error Message** %PIX|ASA-3-322002: ARP inspection check failed for arp {request|response} received from host *MAC\_address* on interface *interface*. This host is advertising MAC Address *MAC\_address\_1* for IP Address *IP\_address*, which is {statically|dynamically} bound to MAC Address *MAC\_address\_2*.

**Explanation** If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured or dynamically learned IP-MAC address binding before forwarding ARP packets across the security appliance. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

## 322003

**Error Message** %PIX|ASA-3-322003:ARP inspection check failed for arp {request|response} received from host *MAC\_address* on interface *interface*. This host is advertising MAC Address *MAC\_address\_1* for IP Address *IP\_address*, which is not bound to any MAC Address.

**Explanation** If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured IP-MAC address binding before forwarding ARP packets across the security appliance. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

## 322004

**Error Message** %PIX|ASA-6-322004: No management IP address configured for transparent firewall. Dropping protocol *protocol* packet from *interface\_in:source\_address/source\_port* to *interface\_out:dest\_address/dest\_port*

**Explanation** The security appliance dropped a packet due to no management IP address configured in the transparent mode.

*protocol*—Protocol string or value

*interface\_in*—Input interface name

*source\_address*—Source IP address of the packet

*source\_port*—Source port of the packet

*interface\_out*—Output interface name

*dest\_address*—Destination IP address of the packet

*dest\_port*—Destination port of the packet

**Recommended Action** Configure the device with management IP address and mask values.

## 323001

**Error Message** %ASA-3-323001: Module in slot *slotnum* experienced a control channel communications failure.

**Explanation** System is unable to communicate via control channel with module installed in slot *slot*.

- *slotnum*—The slot in which the failure occurred. Slot = 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot. For this error, slot should always be 1.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 323002

**Error Message** %ASA-3-323002: Module in slot *slotnum* is not able to shut down, shut down request not answered.

**Explanation** Module installed in slot *slot* didn't respond to a shut down request.

- *slotnum*—The slot in which the failure occurred. Slot = 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot. For this error, slot should always be 1.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 323003

**Error Message** %ASA-3-323003: Module in slot *slotnum* is not able to reload, reload request not answered.

**Explanation** Module installed in slot *slot* didn't respond to a reload request.

- *slotnum*—The slot in which the failure occurred. Slot = 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot. For this error, slot should always be 1.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 323004

**Error Message** %ASA-3-323004: Module in slot *slotnum* failed to write software *vnewver* (currently *vver*), *reason*. Hw-module reset is required before further use.

**Explanation** The module in the specified slot number failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. The module is not usable until the software is updated.

*slotnum*—The slot number containing the module.

*newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0)

*ver*—The current version number of the software on the module (for example, 1.0(1)0).

*reason*—The reason the new version could not be written to the module. The possible values for *reason* include the following:

- write failure.
- failed to create a thread to write the image.

**Recommended Action** The module must be reset by using the **hw-module module *slotnum* reset** before further upgrade attempts will be made. If the module software can not be updated it will not be usable. Ensure the module is completely seated in the chassis. contact the Cisco TAC if further attempts to update the module software are not successful.

## 323005

**Error Message** %ASA-3-323005: Module in slot *slotnum* can not be powered on completely

**Explanation** This message indicates that the module can not be powered up completely. The module will remain in the UNRESPONSIVE state until this condition is corrected. A likely cause of this is a module that is not fully seated in the slot.

*slotnum*—The slot number containing the module

**Recommended Action** Verify that the module is fully seated in the slot and check if any status LEDs on the module are on. It may take a minute after fully reseating the module for the system to recognize that it is powered up. If this message appears after verifying that the module is seated and after resetting the module using the **hw-module module *slotnum* reset** command, contact the Cisco TAC.

## 323006

**Error Message** %ASA-3-323006: Module in slot *slot* experienced a data channel communication failure, data channel is DOWN.

**Explanation** This message indicates that a data channel communication failure occurred and the system was unable to forward traffic to the 4GE SSM. This failure triggers a failover when it occurs on the active appliance in a failover pair. It also results in the configured fail open or fail closed policy being enforced on traffic that would normally be sent to the 4GE SSM. This message is generated whenever there is a communication problem over the security appliance dataplane between the system module and the 4GE SSM. This can be caused when the 4GE SSM stops, resets, or is removed.

*slot*—The slot in which the failure occurred

**Recommended Action** If this is not the result of the 4GE SSM reloading or resetting and a corresponding message 5-505010 is not seen after the 4GE SSM returns to an UP state, the module may need to be reset using the **hw-module module 1 reset** command.

## 324000

**Error Message** %PIX|ASA-3-324000: Drop GTPv *version* message *msg\_type* from *source\_interface*:*source\_address*/*source\_port* to *dest\_interface*:*dest\_address*/*dest\_port* Reason: *reason*

**Explanation** The packet being processed did not meet the filtering requirements as described in the *reason* variable and is being dropped.

**Recommended Action** None.

## 324001

**Error Message** %PIX|ASA-3-324001: GTPv0 packet parsing error from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_port*, TID: *tid\_value*, Reason: *reason*

**Explanation** There was an error processing the packet. The following are possible reasons:

- Mandatory IE is missing
- Mandatory IE incorrect
- IE out of sequence
- Invalid message format.
- Optional IE incorrect
- Invalid TEID
- Unknown IE
- Bad length field
- Unknown GTP message.
- Message too short
- Unexpected message seen
- Null TID
- Version not supported

**Recommended Action** If this message is seen periodically, it can be ignored. If it is seen frequently, then the endpoint maybe sending out bad packets as part of an attack.

## 324002

**Error Message** %PIX|ASA-3-324002: No PDP[MCB] exists to process GTPv0 *msg\_type* from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_port*, TID: *tid\_value*

**Explanation** If this message was preceded by message 321100: Memory allocation Error, the message indicates that there were not enough resources to create the PDP Context. If not, it was not preceded by message 321100, for version 0 it indicates that the corresponding PDP context could not be found. For version 1, if this message was preceded by message 324001, then a packet-processing error occurred, and the operation stopped.

**Recommended Action** If this message repeats frequently because of the memory allocation error, contact the Cisco TAC.

## 324003

**Error Message** %PIX|ASA-3-324003: No matching request to process GTPv *version msg\_type* from *source\_interface:source\_address/source\_port* to *source\_interface:dest\_address/dest\_port*

**Explanation** The response received does not have a matching request in the request queue and should not be processed further.

**Recommended Action** If this message is seen periodically, it can be ignored. But if it is seen frequently, then the endpoint maybe sending out bad packets as part of an attack.

## 324004

**Error Message** %PIX|ASA-3-324004: GTP packet with version%d from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_port* is not supported

**Explanation** The packet being processed has a version other than the currently supported version, which is 0 or 1. If the version number printed out is an incorrect number and is seen frequently, then the endpoint may be sending out bad packets as part of an attack.

**Recommended Action** None.

## 324005

**Error Message** %PIX|ASA-3-324005: Unable to create tunnel from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_port*

**Explanation** An error occurred while trying to create the tunnel for the TPDU.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, collect the necessary debugs and contact the Cisco TAC.

## 324006

**Error Message** %PIX|ASA-3-324006:GSN *IP\_address* tunnel limit *tunnel\_limit* exceeded, PDP Context TID *tid* failed

**Explanation** The GSN sending the request has exceeded the maximum allowed tunnels created, so no tunnel will be created.

**Recommended Action** Check to see whether the tunnel limit should be increased or if there is a possible attack on the network.

## 324007

**Error Message** %PIX|ASA-3-324007: Unable to create GTP connection for response from *source\_interface:source\_address/0* to *dest\_interface:dest\_address/dest\_port*

**Explanation** An error occurred while trying to create the tunnel for the TPDU's for a different SGSN or GGSN.

**Recommended Action** Check debugs and messages to see why the connection was not created properly. If you are unable to debug the problem, collect the necessary debugs and contact the Cisco TAC.

## 324300

**Error Message** %PIX-3-324300: Radius Accounting Request from *from\_addr* has an incorrect request authenticator

**Explanation** When a shared secret is configured for a host, the request-authenticator is verified with that secret. If it fails, it is logged and packet processing stops.

*from\_addr*—The IP address of the host sending the RADIUS accounting request.

**Recommended Action** Check to see that the correct shared secret was configured. If it is, double-check the source of the packet to make sure it is not spoofed.

## 324301

**Error Message** %PIX|ASA-3-324301: Radius Accounting Request has a bad header length *hdr\_len*, packet length *pkt\_len*

**Explanation** The accounting request message has a header length that is not the same as the actual packet length, so packet processing stops.

*hdr\_len*— The length indicated in the request header.

*pkt\_len*—The actual packet length.

**Recommended Action** Make sure the packet is not spoofed. If the packet is legitimate, then capture the packet and make sure the header length is incorrect as indicated by the syslog. If the header length is correct, then collect all the debugs, traces, and syslogs and open a case with the Cisco TAC.

## 325001

**Error Message** %PIX|ASA-3-325001: Router *ipv6\_address* on *interface* has conflicting ND (Neighbor Discovery) settings

**Explanation** Another router on the link sent router advertisements with conflicting parameters. *ipv6\_address* is the IPv6 address of the other router. *interface* is the interface name of the link with the other router.

**Recommended Action** Verify that all IPv6 routers on the link have the same parameters in the router advertisement for *hop\_limit*, *managed\_config\_flag*, *other\_config\_flag*, *reachable\_time* and *ns\_interval*, and that preferred and valid lifetimes for the same prefix, advertised by several routers are the same. To list the parameters per interface enter the command `show ipv6 interface`.

## 325002

**Error Message** %PIX|ASA-4-325002: Duplicate address *ipv6\_address/MAC\_address* on *interface*

**Explanation** Another system is using your IPv6 address. *ipv6\_address* is the IPv6 address of the other router. *MAC\_address* is the MAC address of the other system if known, otherwise “unknown.” *interface* is the interface name of the link with the other system.

**Recommended Action** Change the IPv6 address of one of the two systems.

## 325003

**Error Message** %PIX-3-325003: EUI-64 source address check failed. Dropped packet from *interface\_in:source\_address/source\_port* to *dest\_address/dest\_port* with source MAC address *MAC\_address*.

**Explanation** The `ipv6 enforce-eui64` command is configured for the input interface of this packet, but the source address of the packet is not a correct EUI-64 address derived from the source MAC address.

**Recommended Action** None.

## 326001

**Error Message** %PIX|ASA-3-326001: Unexpected error in the timer library: *error\_message*

**Explanation** A managed timer event was received without a context or a proper type or no handler exists. This message will also be displayed if the number of events queued exceed a system limit and will be attempted to be processed at a later time.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.



## 326002

**Error Message** %PIX|ASA-3-326002: Error in *error\_message* : *error\_message*

**Explanation** The IGMP process failed to shut down upon request. Events that are performed in preparation for this shut down may be out of synchronization.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326004

**Error Message** %PIX|ASA-3-326004: An internal error occurred while processing a packet queue

**Explanation** The IGMP packet queue received a signal without a packet.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326005

**Error Message** %PIX|ASA-3-326005: Mrib notification failed for (*IP\_address*, *IP\_address*)

**Explanation** A packet triggering a data-driven event was received, and the attempt to notify the MRIB failed.

**Recommended Action** If this message persists after the system is up copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326006

**Error Message** %PIX|ASA-3-326006: Entry-creation failed for (*IP\_address*, *IP\_address*)

**Explanation** The MFIB received an entry update from the MRIB, but failed to create the entry related to the addresses displayed, which can cause insufficient memory.

**Recommended Action** If sufficient memory exists, then copy the error message and submit it, the config and any details about the events leading up to this error to the Cisco TAC.

## 326007

**Error Message** %PIX|ASA-3-326007: Entry-update failed for (*IP\_address, IP\_address*)

**Explanation** The MFIB received an interface update from the MRIB, but failed to create the interface related to the addresses displayed. The likely result is insufficient memory.

**Recommended Action** If sufficient memory exists, then copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326008

**Error Message** %PIX|ASA-3-326008: MRIB registration failed

**Explanation** The MFIB failed to register with the MRIB.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326009

**Error Message** %PIX|ASA-3-326009: MRIB connection-open failed

**Explanation** The MFIB failed to open a connection to the MRIB.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326010

**Error Message** %PIX|ASA-3-326010: MRIB unbind failed

**Explanation** The MFIB failed to unbind from the MRIB.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326011

**Error Message** %PIX|ASA-3-326011: MRIB table deletion failed

**Explanation** The MFIB failed to retrieve the table that was supposed to be deleted.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to the Cisco TAC.

## 326012

**Error Message** %PIX|ASA-3-326012: Initialization of *string* functionality failed

**Explanation** The initialization of a functionality failed. This component might still operate without the functionality.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to the Cisco TAC.

## 326013

**Error Message** %PIX|ASA-3-326013: Internal error: *string* in *string* line %d(%s)

**Explanation** A fundamental error occurred in the MRIB.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to the Cisco TAC.

## 326014

**Error Message** %PIX|ASA-3-326014: Initialization failed: error\_message *error\_message*

**Explanation** The MRIB failed to initialize.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to Cisco TAC.

## 326015

**Error Message** %PIX|ASA-3-326015: Communication error: error\_message error\_message

**Explanation** The MRIB received a malformed update.

**Recommended Action** Copy the error message and submit it, the configuration and any details about the events leading up to this error to Cisco TAC.

## 326016

**Error Message** %PIX|ASA-3-326016: Failed to set un-numbered interface for interface\_name (string)

**Explanation** The PIM tunnel is not usable without a source address. This situation occurs because a numbered interface could not be found, or because of some internal error.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326017

**Error Message** %PIX|ASA-3-326017: Interface Manager error - string in string : string

**Explanation** An error occurred while creating a PIM tunnel interface.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326019

**Error Message** %PIX|ASA-3-326019: string in string : string

**Explanation** An error occurred while creating a PIM RP tunnel interface.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326020

**Error Message** %PIX|ASA-3-326020: List error in *string* : *string*

**Explanation** An error occurred while processing a PIM interface list.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326021

**Error Message** %PIX|ASA-3-326021: Error in *string* : *string*

**Explanation** An error occurred while setting the SRC of a PIM tunnel interface.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326022

**Error Message** %PIX|ASA-3-326022: Error in *string* : *string*

**Explanation** The PIM process failed to shut down upon request. Events that are performed in preparation for this shut down may be out of sync.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326023

**Error Message** %PIX|ASA-3-326023: *string* - *IP\_address* : *string*

**Explanation** An error occurred while processing a PIM group range.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326024

**Error Message** %PIX|ASA-3-326024: An internal error occurred while processing a packet queue.

**Explanation** The PIM packet queue received a signal without a packet.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326025

**Error Message** %PIX|ASA-3-326025: *string*

**Explanation** An internal error occurred while trying to send a message. Events scheduled to happen on receipt of the message such as deletion of the PIM tunnel IDB may not take place.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326026

**Error Message** %PIX|ASA-3-326026: Server unexpected error: *error\_message*

**Explanation** The MRIB failed to register a client.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326027

**Error Message** %PIX|ASA-3-326027: Corrupted update: *error\_message*

**Explanation** The MRIB received a corrupt update.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 326028

**Error Message** %PIX|ASA-3-326028: Asynchronous error: *error\_message*

**Explanation** An unhandled asynchronous error occurred in the MRIB API.

**Recommended Action** Copy the error message and submit it, the configuration, and any details about the events leading up to this error and submit it to Cisco TAC.

## 327001

**Error Message** %PIX|ASA-3-327001: IP SLA Monitor: Cannot create a new process

**Explanation** IP SLA Monitor was unable to start a new process.

**Recommended Action** Check the system memory. If memory is low, then this is the likely cause. Try to reenter the commands when memory is available. If there is sufficient memory, then contact the Cisco TAC and provide output from the **show memory**, **show processes**, and **show tech-support** commands.

## 327002

**Error Message** %PIX|ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work

**Explanation** IP SLA monitor failed to initialize. This condition is caused by either the timer wheel timer functionality failed to initialize or a process could not be created. A likely cause of this condition is that sufficient memory is not available to complete the task.

**Recommended Action** Check the system memory. If memory is low, then this is the likely cause. Try to reenter the commands when memory is available. If there is sufficient memory, then contact the Cisco TAC and provide output from the **show memory**, **show processes**, and **show tech-support** commands.

## 327003

**Error Message** %PIX|ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize

**Explanation** IP SLA monitor could not initialize the timer wheel.

**Recommended Action** Check the system memory. If memory is low, then the timer wheel functionality did not initialize. Try to reenter the commands when memory is available. If there is sufficient memory, then contact the Cisco TAC and provide output from the **show memory**, **show processes**, and **show tech-support** commands.

## 328001

**Error Message** %PIX|ASA-3-328001: Attempt made to overwrite a set stub function in *string*.

**Explanation** A single function can be set as a callback for when a stub w/ check registry is invoked. This message indicates that an attempt to set a new callback failed because a callback function has already been set.

*string*—The name of the function.

**Recommended Action** Copy the error message exactly as it appears and report it to the Cisco TAC.

## 329001

**Error Message** %PIX|ASA-3-329001: The *string0* subblock named *string1* was not removed

**Explanation** A software error has occurred. This message displays when IDB subblocks cannot be removed.

*string0*—SWIDB or HWIDB.

*string1*—The name of the subblock.

**Recommended Action** Copy the error message exactly as it appears and report it to the Cisco TAC.

## 331001

**Error Message** ASA|PIX-3-331001: Dynamic DNS Update for '*fqdn\_name*' <=> *ip\_address* failed

**Explanation** This message is generated when the dynamic DNS subsystem fails to update the resource records on the DNS server. This failure might occur if the security appliance is unable to contact the DNS server or DNS service is not running on the destination system.

*fqdn\_name*—The fully qualified domain name for which the DNS update was attempted.

*ip\_address*—The IP address of the DNS update.

**Recommended Action** Make sure a DNS server is configured and reachable by the security appliance. Enable **debug ddns** and submit the output to Cisco TAC, with the configuration and any details about the events leading up to this error.



## 331002

**Error Message** ASA|PIX-5-331002: Dynamic DNS *type* RR for '*fqdn\_name*' -> *ip\_address* successfully updated in DNS server *dns\_server\_ip*

**Error Message** ASA|PIX-5-331002: Dynamic DNS *type* RR for *ip\_address* -> '*fqdn\_name*' successfully updated in DNS server *dns\_server\_ip*

**Explanation**

*type*—The type of resource record, could be “A” or “PTR”.

*fqdn\_name*—The fully qualified domain name for which the DNS update was attempted.

*ip\_address*—The IP address of the DNS update.

*dns\_server\_ip*—The IP address of the DNS server.

**Error Message** This message is generated when Dynamic DNS updates succeed in the DNS server.

## 332003

**Error Message** %ASA|PIX-5-332003: Web Cache *IP\_address/service\_ID* acquired

**Explanation** A service from the web cache of the security appliance was acquired.

*IP\_address*—The IP address of the web cache.

*service\_ID*—The WCCP service identifier.

**Recommended Action** None.

## 332004

**Error Message** %ASA|PIX-1-332004: Web Cache *IP\_address/service\_ID* lost

**Explanation** A service from the web cache of the security appliance was lost.

*IP\_address*—The IP address of the web cache.

*service\_ID*—The WCCP service identifier.

**Recommended Action** None.

## 333001

**Error Message** %PIX|ASA-6-333001: EAP association initiated - context:*EAP-context*

**Explanation** An EAP association has been initiated with a remote host.

*EAP-context*—A unique identifier for the EAP session, displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** None.

## 333002

**Error Message** %PIX|ASA-5-333002: Timeout waiting for EAP response - context:*EAP-context*

**Explanation** A timeout occurred while waiting for an EAP response.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** None.

## 333003

**Error Message** %PIX|ASA-6-333003: EAP association terminated - context:*EAP-context*

**Explanation** The EAP association has been terminated with the remote host.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** None.

## 333004

**Error Message** %PIX|ASA-7-333004: EAP-SQ response invalid - context:*EAP-context*

**Explanation** The EAP-Status Query response failed basic packet validation.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** Contact the Cisco TAC for assistance.

## 333005

**Error Message** %PIX|ASA-7-333005: EAP-SQ response contains invalid TLV(s) - context: *EAP-context*

**Explanation** The EAP-Status Query response has one or more invalid TLVs.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** Contact the Cisco TAC for assistance.

## 333006

**Error Message** %PIX|ASA-7-333006: EAP-SQ response with missing TLV(s) - context: *EAP-context*

**Explanation** The EAP-Status Query response is missing one or more mandatory TLVs.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** Contact the Cisco TAC for assistance.

## 333007

**Error Message** %PIX|ASA-7-333007: EAP-SQ response TLV has invalid length - context: *EAP-context*

**Explanation** The EAP-Status Query response contains a TLV with an invalid length.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** Contact the Cisco TAC for assistance.

## 333008

**Error Message** %PIX|ASA-7-333008: EAP-SQ response has invalid nonce TLV - context: *EAP-context*

**Explanation** The EAP-Status Query response contains an invalid nonce TLV.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** Contact the Cisco TAC for assistance.

## 333009

**Error Message** %PIX|ASA-6-333009: EAP-SQ response MAC TLV is invalid - context:*EAP-context*

**Explanation** The EAP-Status Query response contains a MAC which does not match the calculated MAC.

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** Contact the Cisco TAC for assistance.

## 333010

**Error Message** %PIX|ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:*EAP-context*

**Explanation** The EAP-Status Query response contains a Validation Flags TLV which indicates that the peer requested a full posture validation.

**Recommended Action** None.

## 334001

**Error Message** %PIX|ASA-6-334001: EAPoUDP association initiated - <host-address>

**Explanation** An EAPoUDP association has been initiated with a remote host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 334002

**Error Message** %PIX|ASA-5-334002: EAPoUDP association successfully established - *host-address*

**Explanation** An EAPoUDP association has been successfully established with the host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 334003

**Error Message** %PIX|ASA-5-334003: EAPoUDP association failed to establish - *host-address*

**Explanation** An EAPoUDP association has failed to establish with the host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** Verify configuration of Cisco Secure Access Control Server.

## 334004

**Error Message** %PIX|ASA-6-334004: Authentication request for NAC Clientless host - *host-address*

**Explanation** An authentication request was made for a NAC Clientless host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 334005

**Error Message** %PIX|ASA-5-334005: Host put into NAC Hold state - *host-address*

**Explanation** The NAC session for the host was put into the Hold state.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 334006

**Error Message** %PIX|ASA-5-334006: EAPoUDP failed to get a response from host - *host-address*

**Explanation** An EAPoUDP response was not received from the host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 334007

**Error Message** %PIX|ASA-6-334007: EAPoUDP association terminated - *host-address*

**Explanation** An EAPoUDP association has terminated with the host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 334008

**Error Message** %PIX|ASA-6-334008: NAC EAP association initiated - *host-address*, EAP context:*EAP-context*

**Explanation** EAPoUDP has initiated EAP with the host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

*EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

**Recommended Action** None.

## 335001

**Error Message** %PIX|ASA-6-335001: NAC session initialized - *host-address*

**Explanation** A NAC session has started for a remote host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335002

**Error Message** %PIX|ASA-5-335002: Host is on the NAC Exception List - *host-address*, OS:*oper-sys*

**Explanation** The client is on the NAC Exception List is therefore not subject to Posture Validation.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

*oper-sys*—The operating system (e.g., Windows XP) of the host.

**Recommended Action** None.

## 335003

**Error Message** %PIX|ASA-5-335003: NAC Default ACL applied, ACL:ACL-name - host-address

**Explanation** The NAC Default ACL has been applied for the client.

*ACL-name*—The name of the ACL being applied.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335004

**Error Message** %PIX|ASA-6-335004: NAC is disabled for host - host-address

**Explanation** NAC is disabled for the remote host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335004

**Error Message** %PIX|ASA-6-335004: NAC is disabled for host - host-address

**Explanation** NAC is disabled for the remote host.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335005

**Error Message** %PIX|ASA-4-335005: NAC Downloaded ACL parse failure - host-address

**Explanation** Parsing of downloaded ACL failed.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** Verify configuration of Cisco Secure Access Control Server.

## 335006

**Error Message** %PIX|ASA-6-335006: NAC Applying ACL:*ACL-name* - *host-address*

**Explanation** Name of the ACL being applied as a result of NAC Posture Validation.

*ACL-name*—The name of the ACL being applied.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335007

**Error Message** %PIX|ASA-7-335007: NAC Default ACL not configured - *host-address*

**Explanation** NAC Default ACL has not been configured.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335008

**Error Message** %PIX|ASA-5-335008: NAC IPSec terminate from dynamic ACL:*ACL-name* - *host-address*

**Explanation** A dynamic ACL obtained as a result of PV warrants IPSec termination.

*ACL-name*—The name of the ACL being applied.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335009

**Error Message** %PIX|ASA-6-335009: NAC 'Revalidate' request by administrative action - *host-address*

**Explanation** NAC “Revalidate” was requested by the administrator.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.



## 335010

**Error Message** %PIX|ASA-6-335010: NAC 'Revalidate All' request by administrative action - *num* sessions

**Explanation** NAC “Revalidate All” was requested by the administrator.

*num*—A decimal integer that indicates the number of sessions to be revalidated.

**Recommended Action** None.

## 335011

**Error Message** %PIX|ASA-6-335011: NAC 'Revalidate Group' request by administrative action for *group-name* group - *num* sessions

**Explanation** NAC “Revalidate Group” was requested by the administrator.

*group-name*—The VPN group name.

*num*—A decimal integer that indicates the number of sessions to be revalidated.

**Recommended Action** None.

## 335012

**Error Message** %PIX|ASA-6-335012: NAC 'Initialize' request by administrative action - *host-address*

**Explanation** NAC “Initialize” was requested by the administrator.

*host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

**Recommended Action** None.

## 335013

**Error Message** %PIX|ASA-6-335013: NAC 'Initialize All' request by administrative action - *num* sessions

**Explanation** NAC “Initialize All” was requested by the administrator.

*num*—A decimal integer that indicates the number of sessions to be revalidated.

**Recommended Action** None.

## 335014

**Error Message** %PIX|ASA-6-335014: NAC 'Initialize Group' request by administrative action for *group-name* group - *num* sessions

**Explanation** NAC 'Initialize Group' was requested by the administrator.

*group-name*—The VPN group name.

*num*—A decimal integer that indicates the number of sessions to be revalidated.

**Recommended Action** None.

## Messages 400000 to 450001

This section contains messages from 400000 to 450001.

### 4000nn

**Error Message** %PIX|ASA-4-4000nn: IPS:*number string* from *IP\_address* to *IP\_address* on interface *interface\_name*

**Explanation** Messages 400000 through 400051 are Cisco Intrusion Detection System signature messages.

**Recommended Action** Refer to the *Cisco Intrusion Detection System User Guide* at the following website:

<http://www.cishttp://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/>

All signature messages are not supported by the security appliance in this release. IPS system log messages all start with 4-4000nn and have the following format:

Options:

<i>number</i>	The signature number. Refer to the <i>Cisco Intrusion Detection System User Guide</i> at the following website:  <a href="http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm">http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm</a>
<i>string</i>	The signature message—approximately the same as the NetRanger signature message.
<i>IP_address</i>	The local to remote address to which the signature applies.
<i>interface_name</i>	The name of the interface on which the signature originated.

- *number*

The signature number. Refer to the *Cisco Intrusion Detection System User Guide* at the following website:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm>

- string

The signature message, which is approximately the same as the NetRanger signature message.

- IP\_address

The local to remote address to which the signature applies.

- interface\_name

The name of the interface on which the signature originated.

For example:

```
%PIX|ASA-4-400013 IPS:2003 ICMP redirect from 10.4.1.2 to 10.2.1.1 on interface dmz
%PIX|ASA-4-400032 IPS:4051 UDP Snork attack from 10.1.1.1 to 192.168.1.1 on interface
outside
```

Table 2-4 lists the supported signature messages.

**Table 2-4** IPS Syslog Messages

Message Number	Signature ID	Signature Title	Signature Type
400000	1000	IP options-Bad Option List	Informational
400001	1001	IP options-Record Packet Route	Informational
400002	1002	IP options-Timestamp	Informational
400003	1003	IP options-Security	Informational
400004	1004	IP options-Loose Source Route	Informational
400005	1005	IP options-SATNET ID	Informational
400006	1006	IP options-Strict Source Route	Informational
400007	1100	IP Fragment Attack	Attack
400008	1102	IP Impossible Packet	Attack
400009	1103	IP Fragments Overlap	Attack
400010	2000	ICMP Echo Reply	Informational
400011	2001	ICMP Host Unreachable	Informational
400012	2002	ICMP Source Quench	Informational
400013	2003	ICMP Redirect	Informational
400014	2004	ICMP Echo Request	Informational
400015	2005	ICMP Time Exceeded for a Datagram	Informational
400016	2006	ICMP Parameter Problem on Datagram	Informational
400017	2007	ICMP Timestamp Request	Informational
400018	2008	ICMP Timestamp Reply	Informational
400019	2009	ICMP Information Request	Informational
400020	2010	ICMP Information Reply	Informational

**Table 2-4** *IPS Syslog Messages (continued)*

<b>Message Number</b>	<b>Signature ID</b>	<b>Signature Title</b>	<b>Signature Type</b>
400021	2011	ICMP Address Mask Request	Informational
400022	2012	ICMP Address Mask Reply	Informational
400023	2150	Fragmented ICMP Traffic	Attack
400024	2151	Large ICMP Traffic	Attack
400025	2154	Ping of Death Attack	Attack
400026	3040	TCP NULL flags	Attack
400027	3041	TCP SYN+FIN flags	Attack
400028	3042	TCP FIN only flags	Attack
400029	3153	FTP Improper Address Specified	Informational
400030	3154	FTP Improper Port Specified	Informational
400031	4050	UDP Bomb attack	Attack
400032	4051	UDP Snork attack	Attack
400033	4052	UDP Chargen DoS attack	Attack
400034	6050	DNS HINFO Request	Attack
400035	6051	DNS Zone Transfer	Attack
400036	6052	DNS Zone Transfer from High Port	Attack
400037	6053	DNS Request for All Records	Attack
400038	6100	RPC Port Registration	Informational
400039	6101	RPC Port Unregistration	Informational
400040	6102	RPC Dump	Informational
400041	6103	Proxied RPC Request	Attack
400042	6150	ypserv (YP server daemon) Portmap Request	Informational
400043	6151	ypbind (YP bind daemon) Portmap Request	Informational
400044	6152	yppasswdd (YP password daemon) Portmap Request	Informational
400045	6153	ypupdated (YP update daemon) Portmap Request	Informational
400046	6154	ypxfrd (YP transfer daemon) Portmap Request	Informational
400047	6155	mountd (mount daemon) Portmap Request	Informational
400048	6175	rex (remote execution daemon) Portmap Request	Informational
400049	6180	rex (remote execution daemon) Attempt	Informational
400050	6190	statd Buffer Overflow	Attack

## 401001

**Error Message** %PIX|ASA-4-401001: Shuns cleared

**Explanation** The **clear shun** command was entered to remove existing shuns from memory.

**Recommended Action** None. This message is displayed to allow an institution to keep a record of shunning activity.

## 401002

**Error Message** %PIX|ASA-4-401002: Shun added: *IP\_address IP\_address port port*

**Explanation** A **shun** command was entered, where the first IP address is the shunned host. The other addresses and ports are optional and are used to terminate the connection if available.

**Recommended Action** None. This message is displayed to allow an institution to keep a record of shunning activity.

## 401003

**Error Message** %PIX|ASA-4-401003: Shun deleted: *IP\_address*

**Explanation** A single shunned host was removed from the shun database.

**Recommended Action** None. This message is displayed to allow an institution to keep a record of shunning activity.

## 401004

**Error Message** %PIX|ASA-4-401004: Shunned packet: *IP\_address ==> IP\_address* on interface *interface\_name*

**Explanation** A packet was dropped because the host defined by IP SRC is a host in the shun database. A shunned host cannot pass traffic on the interface on which it is shunned. For example, an external host on the Internet can be shunned on the outside interface.

**Recommended Action** None. This message provides a record of the activity of shunned hosts. This message and %PIX|ASA-4-401005 can be used to evaluate further risk assessment concerning this host.

## 401005

**Error Message** %PIX|ASA-4-401005: Shun add failed: unable to allocate resources for *IP\_address IP\_address port port*

**Explanation** The security appliance is out of memory; a shun could not be applied.

**Recommended Action** The Cisco Intrusion Detection System should continue to attempt to apply this rule. Attempt to reclaim memory and reapply a shun manually, or wait for the Cisco Intrusion Detection System to do this.

## 402101

**Error Message** %PIX|ASA-4-402101: decaps: rec'd IPSEC packet has invalid spi for *destaddr=dest\_address, prot=protocol, spi=number*

**Explanation** Received IPsec packet specifies a security parameters index (SPI) that does not exist in the security association database (SADB). This may be a temporary condition due to slight differences in aging of SAs between the IPsec peers or it may be due to the clearing of the local SAs. This condition may also be caused by incorrect packets sent by the IPsec peer. This may also be an attack.

**Recommended Action** The peer may not acknowledge that the local SAs have been cleared. If a new connection is established from the local router, the two peers may then reestablish successfully. If the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer's administrator.

## 402102

**Error Message** %PIX|ASA-4-402102: decapsulate: packet missing {AH|ESP}, *destaddr=dest\_address, actual prot=protocol*

**Explanation** Received IPsec packet is missing an expected AH or ESP header. The peer is sending packets that do not match the negotiated security policy. This may be an attack.

**Recommended Action** Contact the peer's administrator.

## 402103

**Error Message** %PIX|ASA-4-402103: identity doesn't match negotiated identity (ip) dest\_address= *dest\_address*, src\_addr= *source\_address*, prot= *protocol*, (ident) local=*inside\_address*, remote=*remote\_address*, local\_proxy=*IP\_address/IP\_address/port/port*, remote\_proxy=*IP\_address/IP\_address/port/port*

**Explanation** An unencapsulated IPSec packet does not match the negotiated identity. The peer is sending other traffic through this security association because of a security association selection error by the peer. This may be a hostile event.

**Recommended Action** Contact the peer's administrator to compare policy settings.

## 402106

**Error Message** %PIX|ASA-4-402106: Rec'd packet not an IPSEC packet (ip) dest\_address= *dest\_address*, src\_addr= *source\_address*, prot= *protocol*

**Explanation** The received packet matched the crypto map ACL, but it is not IPSec-encapsulated; the IPSec peer is sending unencapsulated packets. This error can occur because of a policy setup error on the peer. For example, the security appliance only accepts encrypted Telnet traffic to the outside interface port 23. If you attempt to Telnet without IPSec encryption to the outside interface on port 23, this message appears. This error can also signify a hostile event. This system log message is not generated except under the conditions cited (for example, it is not generated for traffic to the security appliance interfaces themselves). See messages 710001, 710002, and 710003 for messages that track TCP and UDP requests.

**Recommended Action** Contact the peer's administrator to compare policy settings.

## 402114

**Error Message** %PIX|ASA-4-402114: IPSEC: Received an *protocol* packet (SPI=*spi*, sequence number= *seq\_num*) from *remote\_IP* to *local\_IP* with an invalid SPI.

*protocol*—IPSec protocol

*spi*—IPSec Security Parameters Index

*seq\_num*—IPSec sequence number

*remote\_IP*—IP address of the remote endpoint of the tunnel

*username*—Username associated with the IPSec tunnel

*local\_IP*—IP address of the local endpoint of the tunnel

**Explanation** This message is displayed when an IPSec packet is received that specifies an SPI that does not exist in the SA database. This may be a temporary condition due to slight differences in aging of SAs between the IPSec peers, or it may be because the local SAs have been cleared. It may also indicate incorrect packets sent by the IPSec peer, which may be part of an attack. This message is rate limited to no more than one message every five seconds.

**Recommended Action** The peer may not acknowledge that the local SAs have been cleared. If a new connection is established from the local router, the two peers may then reestablish successfully. Otherwise, if the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer administrator.

## 402115

**Error Message** %PIX|ASA-4-402115: IPSEC: Received a packet from *remote\_IP* to *local\_IP* containing *act\_prot* data instead of *exp\_prot* data.

**Explanation** This message is displayed when an IPSec packet is received that is missing the expected ESP header. The peer is sending packets that do not match the negotiated security policy. This may indicate an attack. This message is rate limited to no more than one message every five seconds.

*remote\_IP*—IP address of the remote endpoint of the tunnel

*local\_IP*—IP address of the local endpoint of the tunnel

*act\_prot*—Received IPSec protocol

*exp\_prot*—Expected IPSec protocol

**Recommended Action** Contact the peer administrator.

## 402116

**Error Message** %PIX|ASA-4-402116: IPSEC: Received an *protocol* packet (SPI=*spi*, sequence number=*seq\_num*) from *remote\_IP* (*username*) to *local\_IP*. The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as *pkt\_daddr*, its source as *pkt\_saddr*, and its protocol as *pkt\_prot*. The SA specifies its local proxy as *id\_daddr* /*id\_dmask* /*id\_dprot* /*id\_dport* and its remote proxy as *id\_saddr* /*id\_smask* /*id\_sprot* /*id\_sport*.

**Explanation** This message is displayed when a decapsulated IPSec packet does not match the negotiated identity. The peer is sending other traffic through this security association. It may be due to a security association selection error by the peer, or it may be part of an attack. This message is rate limited to no more than one message every five seconds.

*protocol*—IPSec protocol

*spi*—IPSec Security Parameters Index

*seq\_num*—IPSec sequence number

*remote\_IP*—IP address of the remote endpoint of the tunnel

*username*—Username associated with the IPSec tunnel

*local\_IP*—IP address of the local endpoint of the tunnel



*pkt\_daddr*—Destination address from the decapsulated packet

*pkt\_saddr*—Source address from the decapsulated packet

*pkt\_prot*—Transport protocol from the decapsulated packet

*id\_daddr*—Local proxy IP address

*id\_dmask*—Local proxy IP subnet mask

*id\_dprot*—Local proxy transport protocol

*id\_dport*—Local proxy port

*id\_saddr*—Remote proxy IP address

*id\_smask*—Remote proxy IP subnet mask

*id\_sprot*—Remote proxy transport protocol

*id\_sport*—Remote proxy port

**Recommended Action** Contact the peer administrator and compare policy settings.

## 402117

**Error Message** %PIX|ASA-4-402117: IPSEC: Received a non-IPSec (*protocol*) packet from *remote\_IP* to *local\_IP*.

**Explanation** This message is displayed when the received packet matched the crypto map ACL, but it is not IPSec-encapsulated. The IPSec Peer is sending unencapsulated packets. This error can occur because of a policy setup error on the peer. For example, the firewall may be configured to only accept encrypted Telnet traffic to the outside interface port 23. If you attempt to Telnet without IPSec encryption to the outside interface on port 23, this message appears, but not on telnet or traffic to the outside interface on ports other than 23. This error can also indicate an attack. This system log message is not generated except under these conditions (for example, it is not generated for traffic to the firewall interfaces themselves). See messages 710001, 710002, and 710003 for messages that track TCP and UDP requests. This message is rate limited to no more than one message every five seconds

*protocol*—IPSec protocol

*remote\_IP*—IP address of the remote endpoint of the tunnel

*local\_IP*—IP address of the local endpoint of the tunnel

**Recommended Action** Contact the peer administrator to compare policy settings.

## 402118

**Error Message** %PIX|ASA-4-402118: IPSEC: Received an *protocol* packet (SPI=*spi*, sequence number *seq\_num*) from *remote\_IP* (*username*) to *local\_IP* containing an illegal IP fragment of length *frag\_len* with offset *frag\_offset*.

**Explanation** This message is displayed when a decapsulatd IPsec packet contains an IP fragment with an offset less than or equal to 128 bytes. The latest version of the Security Architecture for IP RFC recommends 128 bytes as the minimum IP fragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.

*protocol*—IPsec protocol

*spi*—IPsec Security Parameters Index

*seq\_num*—IPsec sequence number

*remote\_IP*—IP address of the remote endpoint of the tunnel

*username*—Username associated with the IPsec tunnel

*local\_IP*—IP address of the local endpoint of the tunnel

*frag\_len*—IP fragment length

*frag\_offset*—IP fragment offset in bytes

**Recommended Action** Contact the administrator of the remote peer to compare policy settings.

## 402119

**Error Message** %PIX|ASA-4-402119: IPSEC: Received an *protocol* packet (SPI=*spi*, sequence number=*seq\_num*) from *remote\_IP* (*username*) to *local\_IP* that failed anti-replay checking.

**Explanation** This message is displayed when an IPsec packet is received with an invalid sequence number. The peer is sending packets containing sequence numbers that may have been previously used. This system log message indicates that an IPsec packet has been received with a sequence number outside of the acceptable window. This packet will be dropped by IPsec as part of a possible attack. This message is rate limited to no more than one message every five seconds.

*protocol*—IPsec protocol

*spi*—IPsec Security Parameters Index

*seq\_num*—IPsec sequence number

*remote\_IP*—IP address of the remote endpoint of the tunnel

*username*—Username associated with the IPsec tunnel

*local\_IP*—IP address of the local endpoint of the tunnel

**Recommended Action** Contact the peer administrator.

## 402120

**Error Message** %PIX|ASA-4-402120: IPSEC: Received an *protocol* packet (SPI=*spi*, sequence number=*seq\_num*) from *remote\_IP* (*username*) to *local\_IP* that failed authentication.

**Explanation** This message is displayed when an IPsec packet is received and fails authentication. The packet is dropped. The packet may have been corrupted in transit or the peer may be sending invalid IPsec packets. This may indicate an attack if many of these packets are received from the same peer. This message is rate limited to no more than one message every five seconds.

*protocol*—IPsec protocol

*spi*—IPsec Security Parameters Index

*seq\_num*—IPsec sequence number

*remote\_IP*—IP address of the remote endpoint of the tunnel

*username*—Username associated with the IPsec tunnel

*local\_IP*—IP address of the local endpoint of the tunnel

**Recommended Action** Contact the administrator of the remote peer if many failed packets are received.

## 402123

**Error Message** %PIX|ASA-4-402123: CRYPTO: The *accel\_type* hardware accelerator encountered an error (code=*error\_string*) while executing crypto command *command* .

*accel\_type*—Hardware accelerator type

*error\_string*—Code indicating the type of error

*command*—Crypto command that generated the error

**Explanation** This message is displayed when an error is detected while running a crypto command with a hardware accelerator. This could indicate a problem with the accelerator. This type of error may occur for a variety of reasons, and this message supplements the crypto accelerator counters to help determine the cause.

**Recommended Action** contact the Cisco TAC for assistance.

## 403101

**Error Message** %PIX|ASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel\_id=*number*, session\_id=*number*

**Explanation** The security appliance received a PPTP XGRE packet without a corresponding control connection session.

**Recommended Action** If this message occurs frequently, report the problem to Cisco TAC.

## 403102

**Error Message** %PIX|ASA-4-403102: PPP virtual interface *interface\_name* rcvd pkt with invalid protocol: *protocol*, reason: *reason*.

**Explanation** The module received an XGRE encapsulated PPP packet with an invalid protocol field.

**Recommended Action** If this message occurs frequently, report the problem to Cisco TAC.

## 403103

**Error Message** %PIX|ASA-4-403103: PPP virtual interface max connections reached.

**Explanation** The module cannot accept additional PPTP connections.

**Recommended Action** None. Connections are allocated as soon as they are available.

## 403104

**Error Message** %PIX|ASA-4-403104: PPP virtual interface *interface\_name* requires mschap for MPPE.

**Explanation** The Microsoft Point-to-Point Encryption (MPPE) is configured but MS-CHAP authentication is not.

**Recommended Action** Add MS-CHAP authentication with the **vpdn group** *group\_name* **ppp authentication** command.

## 403106

**Error Message** %PIX|ASA-4-403106: PPP virtual interface *interface\_name* requires RADIUS for MPPE.

**Explanation** The MPPE is configured but RADIUS authentication is not.

**Recommended Action** Add RADIUS authentication with the **vpdn group** *group\_name* **ppp authentication** command.

## 403107

**Error Message** %PIX|ASA-4-403107: PPP virtual interface *interface\_name* missing aaa server group info

**Explanation** The AAA server configuration information cannot be found.

**Recommended Action** Add the AAA server information with the **vpdn group** *group\_name* **client authentication aaa** *aaa\_server\_group* command.

## 403108

**Error Message** %PIX|ASA-4-403108: PPP virtual interface *interface\_name* missing client ip address option

**Explanation** The client IP address pool information is missing.

**Recommended Action** Add IP address pool information with the **vpdn group** *group\_name* **client configuration address local** *address\_pool\_name* command.

## 403109

**Error Message** %PIX|ASA-4-403109: Rec'd packet *not an PPTP packet.* (ip) dest\_address=*dest\_address*, src\_addr=*source\_address*, data: *string*.

**Explanation** The module received a spoofed PPTP packet. This may be a hostile event.

**Recommended Action** Contact the peer's administrator to check the PPTP configuration settings.

## 403110

**Error Message** %PIX|ASA-4-403110: PPP virtual interface *interface\_name*, user: *user* missing MPPE key from aaa server.

**Explanation** The AAA server is not returning the MPPE key attributes required to set up the MPPE encryption policy.

**Recommended Action** Check the AAA server configuration and if the AAA server cannot return MPPE key attributes, use local authentication instead with the **vpdn group** *group\_name* **client authentication local** command.

## 403500

**Error Message** %PIX|ASA-6-403500: PPPoE - Service name 'any' not received in PADO.  
Intf:*interface\_name* AC:*ac\_name*.

**Explanation** The security appliance requested the PPPoE service “any” from the access controller at the Internet service provider. The response from the service provider includes other services but does not include the service “any.” This is a discrepancy in the implementation of the protocol. The PADO packet is processed normally and connection negotiations continue.

**Recommended Action** None.

## 403501

**Error Message** %PIX|ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped.  
Intf:*interface\_name* AC:*ac\_name*

**Explanation** The security appliance sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The security appliance is unable to identify the corresponding connection request for this response. The packet is dropped and connection negotiations are discontinued.

**Recommended Action** Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value or the PADO packet is being forged.

## 403502

**Error Message** %PIX|ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet.  
Intf:*interface\_name* AC:*ac\_name*

**Explanation** The security appliance sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The security appliance is unable to identify the corresponding connection request for this response. The packet was dropped and connection negotiations were discontinued.

**Recommended Action** Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value or the PADO packet is being forged.

## 403503

**Error Message** %PIX|ASA-3-403503: PPPoE:PPP link down:*reason*

**Explanation** The PPP link has gone down. There are many reasons why this could happen. The first format will display a reason if PPP provides one.

**Recommended Action** Check the network link to ensure that the link is connected. The access concentrator could be down. Ensure that your authentication protocol matches the access concentrator. Ensure that your name and password are correct. Check with your ISP or network support person.

## 403504

**Error Message** %PIX|ASA-3-403504: PPPoE:No 'vpdn group *group\_name*' for PPPoE is created

**Explanation** PPPoE requires a dial-out configuration before starting a PPPoE session. In general, the configuration should specify a dialing policy, the PPP authentication, the username, and a password. The following example configures the security appliance for PPPoE dialout. The **my-username** and **my-password** commands are used to authenticate the access concentrator, using PAP if necessary.

For example:

```
vpdn group my-pppoe request dialout pppoe
vpdn group my-pppoe ppp authentication pap
vpdn group my-pppoe localname my-username
vpdn username my-username password my-password
ip address outside pppoe setroute
```

**Recommended Action** Configure a VPDN group for PPPoE.

## 403505

**Error Message** %PIX|ASA-4-403505: PPPoE:PPP - Unable to set default route to *IP\_address* at *interface\_name*

**Explanation** This message is usually followed by the message - **default route already exists**.

**Recommended Action** Remove the current default route or remove the “setroute” parameter so that there is no conflict between PPPoE and the manually configured route.

## 403506

**Error Message** %PIX|ASA-4-403506: PPPoE:failed to assign PPP *IP\_address* netmask *netmask* at *interface\_name*

**Explanation** This message is followed by - **subnet is the same as interface, or on failover channel.**

**Recommended Action** In the first case, change the address causing the conflict. In the second case, configure the PPPoE on an interface other than the failover interface.

## 403507

**Error Message** %PIX|ASA-3-403507:PPPoE:PPPoE client on interface *interface* failed to locate PPPoE vpdn group *group\_name*

**Explanation** You can configure the PPPoE client on an interface to use a particular VPDN group by entering the **pppoe client vpdn group** *group\_name* command. If a PPPoE VPDN group of the configured name is not located during system startup, this syslog message is generated.

*interface*—The interface on which the PPPoE client failed.

*group\_name* —The VPDN group name of the PPPoE client on the interface.

**Recommended Action** Perform the following steps:

1. Add the required VPDN group by entering the **vpdn group** *group\_name* command. Request dialout PPPoE in global configuration mode and add all the group properties.
2. Remove the **pppoe client vpdn group** *group\_name* command from the interface indicated. In this case, the PPPoE client will attempt to use the first PPPoE VPDN group defined.



**Note** All changes take effect only after the PPPoE client on the interface is restarted by entering the **ip address pppoe** command.

## 404101

**Error Message** %PIX|ASA-4-404101: ISAKMP: Failed to allocate address for client from pool *string*

**Explanation** ISAKMP failed to allocate an IP address for the VPN client from the pool that you specified with the **ip local pool** command.

**Recommended Action** Use the **ip local pool** command to specify additional IP addresses for the pool.



## 404102

**Error Message** %PIX|ASA-3-404102: ISAKMP: Exceeded embryonic limit

**Explanation** More than 500 embryonic security associations (SAs) exist, which could mean a DoS attack.

**Recommended Action** Enter the **show crypto isakmp ca** command to determine the origin of the attack. After the source is identified, deny access to the offending IP address or network.

## 405001

**Error Message** %PIX|ASA-4-405001: Received ARP {request | response} collision from *IP\_address/MAC\_address* on interface *interface\_name*

**Explanation** The security appliance received an ARP packet, and the MAC address in the packet differs from the ARP cache entry.

**Recommended Action** This traffic might be legitimate, or it might indicate that an ARP poisoning attack is in progress. Check the source MAC address to determine where the packets are coming from and check to see if it belongs to a valid host.

## 405101

**Error Message** %PIX|ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign\_address *outside\_address[/outside\_port]* to local\_address *inside\_address[/inside\_port]*

**Explanation** The module failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC. You can check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translates and connections. This error message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory.

## 405002

**Error Message** %PIX|ASA-4-405002: Received mac mismatch collision from *IP\_address/MAC\_address* for authenticated host

**Explanation** This packet appears for one of the following conditions:

- The security appliance received a packet with the same IP address but a different MAC address from one of its uauth entries.
- You configured the **vpnclient mac-exempt** command on the security appliance, and the security appliance receives a packet with an exempt MAC address but a different IP address from the corresponding uauth entry.

**Recommended Action** This traffic might be legitimate, or it might indicate that a spoofing attack is in progress. Check the source MAC address and IP address to determine where the packets are coming from and check to see if they belong to a valid host.

## 405101

**Error Message** %PIX|ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign\_address *outside\_address[/outside\_port]* to local\_address *inside\_address[/inside\_port]*

**Explanation** The security appliance failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

**Recommended Action** Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of xlates and connections. This could also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory. If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

## 405102

**Error Message** %PIX|ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign\_address *outside\_address[/outside\_port]* to local\_address *inside\_address[/inside\_port]*

**Explanation** The security appliance failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

**Recommended Action** Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of xlates and connections. This could also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory. If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

## 405103

**Error Message** %PIX|ASA-4-405103: H225 message from *source\_address/source\_port* to *dest\_address/dest\_port* contains bad protocol discriminator *hex*

**Explanation** PIX is expecting the protocol discriminator, 0x08, but it received something other than 0x08. This might happen because the endpoint is sending a bad packet, or received a message segment other than the first segment.

**Recommended Action** None. The packet is allowed through.

## 405104

**Error Message** %PIX|ASA-4-405104: H225 message received from *outside\_address/outside\_port* to *inside\_address/inside\_port* before SETUP

**Explanation** This message appears after an H.225 message is received out of order. The H.225 message was received before the initial SETUP message, which is not allowed. The security appliance must receive an initial SETUP message for that H.225 call signalling channel before accepting any other H.225 messages.

**Recommended Action** None.

## 405105

**Error Message** %PIX|ASA-4-405105: H323 RAS message AdmissionConfirm received from *source\_address/source\_port* to *dest\_address/dest\_port* without an *AdmissionRequest*

**Explanation** A gatekeeper has sent an admission confirm (ACF), but the security appliance did not send an admission request (ARQ) to the gatekeeper.

**Recommended Action** Check the gatekeeper with the specified *source\_address* to determine why it sent an ACF without receiving an ARQ from the security appliance.

## 405106

**Error Message** %PIX|ASA-4-405106: H323 *num* channel is not created from %I/%d to %I/%d %s\n

**Explanation** This syslog message is generated when the security appliance attempts to create a match condition on the H.323 media-type channel. See the **match media-type** command for more information.

**Recommended Action** None.

## 405107

**Explanation** %PIX|ASA-4-405107: H245 Tunnel is detected and connection dropped from *%I/%d* to *%I/%d %s\n*

**Explanation** This syslog message is generated when an H.323 connection has been dropped because of attempted H.245 tunnel control during call setup. See the **h245-tunnel-block** command for more information.

**Recommended Action** None.

## 405201

**Error Message** %PIX|ASA-4-405201: ILS *ILS\_message\_type* from *inside\_interface:source\_IP\_address* to *outside\_interface:/destination\_IP\_address* has wrong embedded address *embedded\_IP\_address*

**Explanation** The embedded address in the ILS packet payload is not the same as the source IP address of the IP packet header.

**Recommended Action** Check the host with the specified with the *source\_IP\_address* to determine why it sent an ILS packet with an incorrect embedded IP address.

## 405300

**Error Message** %PIX|ASA-4-405300: Radius Accounting Request received from *from\_addr* is not allowed

**Explanation** The accounting request came from a host that was not configured in the policy-map. The message is logged and processing stops.

*from\_addr*—The IP address of the host sending the request.

**Recommended Action** If the host was configured to send RADIUS accounting messages to the security appliance, make sure it was configured in the correct policy-map that was applied to the service-policy. If the host was not configured to send RADIUS accounting messages to the security appliance, then check to see why the messages are being sent. If the messages are illegitimate, then create the proper ACLs to drop the packets.

## 405301

**Error Message** %PIX|ASA-4-405301: Attribute *attribute\_number* does not match for user *user\_ip*

**Explanation** When the **validate-attribute** command is entered, the attribute values stored in the Accounting Request Start received do not match those stored in entry, if it exists.

*attribute\_number*—The RADIUS attribute to be validated with RADIUS accounting. Values range from 1 to 191. Vendor-specific attributes are not supported.

*user\_ip*—The IP address (framed IP attribute) of the user.

**Recommended Action** None.

## 406001

**Error Message** %PIX|ASA-4-406001: FTP port command low port: *IP\_address/port* to *IP\_address* on interface *interface\_name*

**Explanation** A client entered an FTP port command and supplied a port less than 1024 (in the well-known port range typically devoted to server ports). This is indicative of an attempt to avert the site security policy. The security appliance drops the packet, terminates the connection, and logs the event.

**Recommended Action** None.

## 406002

**Error Message** %PIX|ASA-4-406002: FTP port command different address: *IP\_address(IP\_address)* to *IP\_address* on interface *interface\_name*

**Explanation** A client issued an FTP port command and supplied an address other than the address used in the connection. This error message is indicative of an attempt to avert the site's security policy. For example, an attacker might attempt to hijack an FTP session by changing the packet on the way, and putting different source information instead of the correct source information. The security appliance drops the packet, terminates the connection, and logs the event. The address in parenthesis is the address from the port command.

**Recommended Action** None.

## 407001

**Error Message** %PIX|ASA-4-407001: Deny traffic for local-host *interface\_name:inside\_address*, license limit of *number* exceeded

**Explanation** The host limit was exceeded. An inside host is counted toward the limit when one of the following conditions is true:

- The inside host has forwarded traffic through the security appliance within the last five minutes.
- The inside host currently reserved an xlate connection or user authentication at the security appliance.

**Recommended Action** The host limit is enforced on the low-end platforms. Use the **show version** command to view the host limit. Use the **show local-host** command to view the current active hosts and the inside users that have sessions at the security appliance. To forcefully disconnect one or more users, use the **clear local-host** command. To expire the inside users more quickly from the limit, set the xlate, connection, and uauth timeouts to the recommended values or lower. (See [Table 2-5](#).)

**Table 2-5 Timeouts and Recommended Values**

Timeout	Recommended Value
xlate	00:05:00 (five minutes)
conn	00:01:00 (one hour)
uauth	00:05:00 (five minutes)

## 407002

**Error Message** %PIX|ASA-4-407002: Embryonic limit *nconns/limit* for through connections exceeded.*outside\_address/outside\_port* to *global\_address (inside\_address)/inside\_port* on interface *interface\_name*

**Explanation** This message is about connections through the security appliance. This message is displayed when the number of connections from a specified foreign address over a specified global address to the specified local address exceeds the maximum embryonic limit for that static. The security appliance attempts to accept the connection if it can allocate memory for that connection. It proxies on behalf of local host and sends a SYN\_ACK packet to the foreign host. The security appliance retains pertinent state information, drops the packet, and waits for the client's acknowledgment.

**Recommended Action** The message might indicate legitimate traffic, or indicate that a denial of service (DoS) attack is in progress. Check the source address to determine where the packets are coming from and whether it is a valid host.

## 407003

**Error Message** %PIX|ASA-4-407003: Established limit for RPC services exceeded *number*

**Explanation** The security appliance tried to open a new hole for a pair of RPC servers or services that have already been configured after the maximum number of holes has been met.

**Recommended Action** Wait for other holes to be closed (through associated timeout expiration) or limit the number of active pairs of servers or services.

## 408001

**Error Message** %PIX|ASA-4-408001: IP route counter negative - *reason*, *IP\_address*  
Attempt: *number*

**Explanation** An attempt to decrement the IP route counter into a negative value failed.

**Recommended Action** Enter the **clear ip route \*** command to reset the route counter. If the message continues to appear consistently, copy the messages exactly as they appear, and report it to Cisco TAC.

## 408002

**Error Message** %PIX|ASA-4-408002: ospf process *id* route type update *address1 netmask1*  
[*distance1/metric1*] via source *IP:interface1 address2 netmask2* [*distance2/metric2*] *interface2*

**Explanation** A network update was received from a different interface with the same distance and a better metric than the existing route. The new route overrides the existing route that was installed through another interface. The new route is for redundancy purposes only and means that a path has shifted in the network. This change must be controlled through topology and redistribution. Any existing connections affected by this change are probably disabled and will timeout. This path shift only occurs if the network topology has been specifically designed to support path redundancy, in which case it is expected.

**Recommended Action** None.

## 408003

**Error Message** %PIX|ASA-4-408003: can't track this type of object *hex*

**Explanation** A component of the tracking system has encountered an object type that is not supported by the component. A STATE object was expected.

*hex*—A hexadecimal value(s) depicting variable value(s) or addresses in memory.

**Recommended Action** Reconfigure the track object to make it a STATE object.

## 409001

**Error Message** %PIX|ASA-4-409001: Database scanner: external LSA *IP\_address netmask* is lost, reinstalls

**Explanation** The software detected an unexpected condition. The router will take corrective action and continue.

**Recommended Action** None.

## 409002

**Error Message** %PIX|ASA-4-409002: db\_free: external LSA *IP\_address netmask*

**Explanation** An internal software error occurred.

**Recommended Action** None.

## 409003

**Error Message** %PIX|ASA-4-409003: Received invalid packet: *reason* from *IP\_address*, *interface\_name*

**Explanation** An invalid OSPF packet was received. Details are included in the error message. The cause might be an incorrect OSPF configuration or an internal error in the sender.

**Recommended Action** Check the OSPF configuration of the receiver and the sender configuration for inconsistency.

## 409004

**Error Message** %PIX|ASA-4-409004: Received *reason* from unknown neighbor *IP\_address*

**Explanation** The OSPF hello, database description, or database request packet was received, but the router could not identify the sender.

**Recommended Action** This situation should correct itself.



## 409005

**Error Message** %PIX|ASA-4-409005: Invalid length number in OSPF packet from *IP\_address* (ID *IP\_address*), *interface\_name*

**Explanation** The system received an OSPF packet with a field length of less than normal header size or inconsistent with the size of the IP packet in which it arrived. This indicates a configuration error in the sender of the packet.

**Recommended Action** From a neighboring address, locate the problem router and reboot it.

## 409006

**Error Message** %PIX|ASA-4-409006: Invalid lsa: *reason* Type *number*, LSID *IP\_address* from *IP\_address*, *IP\_address*, *interface\_name*

**Explanation** The router received an LSA with an invalid LSA type. The cause is either memory corruption or unexpected behavior on a router.

**Recommended Action** From a neighboring address, locate the problem router and reboot it. To determine what is causing this problem, contact the Cisco TAC for assistance.

## 409007

**Error Message** %PIX|ASA-4-409007: Found LSA with the same host bit set but using different mask LSA ID *IP\_address netmask* New: Destination *IP\_address netmask*

**Explanation** An internal software error occurred.

**Recommended Action** To determine what is causing this problem, contact the Cisco TAC for assistance.

## 409008

**Error Message** %PIX|ASA-4-409008: Found generating default LSA with non-zero mask LSA type : *number* Mask: *netmask* metric : *number* area : *string*

**Explanation** The router tried to generate a default LSA with the wrong mask and possibly wrong metric due to an internal software error.

**Recommended Action** To determine what is causing this problem, contact the Cisco TAC for assistance.

## 409009

**Error Message** %PIX|ASA-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID

**Explanation** OSPF failed while attempting to allocate a router ID from the IP address of one of its interfaces.

**Recommended Action** Make sure that there is at least one interface that is up and has a valid IP address. If there are multiple OSPF processes running on the router, each requires a unique router ID. You must have enough interfaces up so that each of them can obtain a router ID.

## 409010

**Error Message** %PIX|ASA-4-409010: Virtual link information found in non-backbone area: *string*

**Explanation** An internal error occurred.

**Recommended Action** To determine what is causing this problem, contact the Cisco TAC for assistance.

## 409011

**Error Message** %PIX|ASA-4-409011: OSPF detected duplicate router-id *IP\_address* from *IP\_address* on interface *interface\_name*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

## 409012

**Error Message** %PIX|ASA-4-409012: Detected router with duplicate router ID *IP\_address* in area *string*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

## 409013

**Error Message** %PIX|ASA-4-409013: Detected router with duplicate router ID *IP\_address* in Type-4 LSA advertised by *IP\_address*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

## 409023

**Error Message** %PIX|ASA-4-409023: Attempting AAA Fallback method *method\_name* for *request\_type* request for user *user* :Auth-server group *server\_tag* unreachable

**Explanation** An authentication or authorization attempt to an external server has failed and will now be performed using the local user database. *aaa\_operation* is either “authentication” or “authorization.” *username* is the user associated with the connection. *server\_group* is the name of the AAA server whose servers were unreachable.

**Recommended Action** Investigate any connectivity problems with the AAA servers configured in the first method. Ping the authentication servers from the security appliance. Make sure that the daemons are running on your AAA server.

## 410001

**Error Message** %PIX|ASA-4-410001: UDP DNS request from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_port*; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.

**Explanation** This syslog message is generated when the domain-name length exceeds 255 bytes in a UDP DNS packet. (See RFC 1035 section 3.1.)

**Recommended Action** None.

## 410002

**Error Message** %PIX|ASA-2-410002: Dropped *num* DNS responses with mis-matched id in the past *sec* second(s): from *src\_ifc:sip/sport* to *dest\_ifc:dip/dport*

**Explanation** This syslog message is generated when the security device detects an excess number of DNS responses with a mismatched DNS identifier. The threshold is set by the **id-mismatch** DNS policy-map parameter submode command.

*num*—The number of ID mismatch instances as configured by the **id-mismatch** command.

*sec*—The duration in seconds as configured by the **id-mismatch** command.

*src\_ifc*—The source interface name at which the DNS message is received with a mismatched DNS identifier.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

**Recommended Action** A high rate of mismatched DNS identifiers might indicate an attack on the cache. Check the IP address/port in the syslog message to trace the source of the attack. You can configure ACLs to block traffic permanently from the source.

## 410003

**Error Message** %PIX|ASA-4-410003: *action\_class: action* DNS *query\_response* from *src\_ifc:sip/sport* to *dest\_ifc:dip/dport*; *further\_info*

**Explanation** This syslog message is generated when a DNS classification is performed on a DNS message and the specified criteria is satisfied. Then the configured action occurs.

*action\_class*—The “DNS Classification” action class.

*action*—The action taken: “Dropped,” “Dropped (no TSIG),” or “Masked header flags for.”

*query\_response*—Either “query” or “response.”

*src\_ifc*—The source interface name.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

*further\_info*—One of the following: “matched Class id: *class\_name*,” “matched Class id: *match\_command*” (for a standalone **match** command), or “TSIG resource record not present” (for syslogs generated by the **tsig enforced** command).

**Recommended Action** None.

## 410004

**Error Message** %ASA-6-410004: *action\_class: action DNS query\_response from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info*

**Explanation** This event is generated when a DNS classification is performed on a DNS message and the specified criteria is satisfied.

*action\_class*—The “DNS Classification” action class.

*action*—The action taken: “Received” or “Received (no TSIG).”

*query\_response*—Either “query” or “response.”

*src\_ifc*—The source interface name.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

*further\_info*—One of the following: “matched Class id: *class\_name*,” “matched Class id: *match\_command*” (for a standalone **match** command), or “TSIG resource record not present” (for syslogs generated by the **tsig enforced** command).

**Recommended Action** None.

## 410008

**Error Message** %ASA-4-4108004: *action\_class: action ESMTTP req\_resp from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info*

*action\_class*—The class of action: “ESMTTP Classification” for ESMTTP match commands; “ESMTTP Parameter” for parameter commands.

*action*—action taken: “Dropped”, “Dropped connection for”, “Reset connection for”, or “Masked header flags for”.

*req\_resp*—“Request” or “Response”.

*src\_ifc*—The source interface name.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

*further\_info*—One of the following:

- For single match command: matched Class *id: match\_command*; for example, matched Class 1234: match body length 100.
- For parameter commands: *parameter-command: descriptive-message*; for example, mail-relay: No Mail Relay allowed.

**Explanation** This event is generated when a ESMTP classification is performed on an ESMTP message and the specified criteria is satisfied. The configured action occurs.

**Recommended Action** None.

## 411001

**Error Message** %PIX|ASA-4-411001: Line protocol on interface *interface\_name* changed state to up

**Explanation** The status of the line protocol has changed from down to up. If *interface\_name* is a logical interface name such as “inside” and “outside,” this message indicates that the logical interface line protocol has changed from down to up. If *interface\_name* is a physical interface name such as “Ethernet0” and “GigabitEthernet0/1,” this message indicates that the physical interface line protocol has changed from down to up.

**Recommended Action** None.

## 411002

**Error Message** %PIX|ASA-4-411002: Line protocol on interface *interface\_name* changed state to down

**Explanation** The status of the line protocol has changed from up to down. If *interface\_name* is a logical interface name such as “inside” and “outside,” this message indicates that the logical interface line protocol has changed from up to down. In this case, the physical interface line protocol status is not affected. If *interface\_name* is a physical interface name such as “Ethernet0” and “GigabitEthernet0/1,” this message indicates that the physical interface line protocol has changed from up to down.

**Recommended Action** If this is an unexpected event on the interface, check the physical line.

## 411003

**Error Message** %PIX|ASA-4-411003: Configuration status on interface *interface\_name* changed state to downup

**Recommended Action** If this is an unexpected event, check the physical line.

## 411004

**Error Message** %PIX|ASA-4-411004: Configuration status on interface *interface\_name* changed state to up

**Explanation** The configuration status of the interface has changed from down to up.

**Recommended Action** None.

## 412001

**Error Message** %PIX|ASA-4-412001:MAC *MAC\_address* moved from *interface\_1* to *interface\_2*

**Explanation** This message is generated when a host move is detected from one module interface to another. In a transparent security appliance, mapping between the host (MAC) and security appliance port is maintained in a Layer 2 forwarding table. The table dynamically binds packet source MAC addresses to a security appliance port. In this process, whenever movement of a host from one interface to another interface is detected, this message is generated.

**Recommended Action** The host move might be valid or the host move might be an attempt to spoof host MACs on other interfaces. If it is a MAC spoof attempt, you can either locate vulnerable hosts on your network and remove them or configure static MAC entries, which will not allow MAC address and port binding to change. If it is a genuine host move, no action is required.

## 412002

**Error Message** %PIX|ASA-4-412002:Detected bridge table full while inserting MAC *MAC\_address* on interface *interface*. Number of entries = *num*

**Explanation** This message is generated when the bridge table is full and an attempt is made to add one more entry. The security appliance maintains a separate Layer 2 forwarding table per context and the message is generated whenever a context exceeds its size limit. The MAC address will be added, but it will replace the oldest existing dynamic entry (if available) in the table

**Recommended Action** This might be an attempted attack. Make sure that the new bridge table entries are valid. In case of attack, use EtherType ACLs to access control vulnerable hosts.

## 413001

**Error Message** %ASA-4-413001: Module in slot *slotnum* is not able to shut down.  
Module Error: *errnum message*

**Explanation** The module in *slotnum* was not able to comply with a request from the ASA system module to shut down. It may be performing a task that could not be interrupted, like a software upgrade. The *errnum* and *message* text describes the reason why the module could not shut down, and recommends action.

**Recommended Action** Wait for the task on the module to complete before shutting down the module, or use the session command to access the module's CLI and stop the task that's preventing the module from shutting down.

## 413002

**Error Message** %ASA-4-413002: Module in slot *slotnum* is not able to reload. Module Error: *errnum message*

**Explanation** The module in *slotnum* was not able to comply with a request from the ASA system module to reload. It may be performing a task that could not be interrupted, like a software upgrade. The *errnum* and *message* text describes the reason why the module could not reload, and the recommended action.

**Recommended Action** Wait for the task on the module to complete before reloading the module, or use the session command to access the module's CLI and stop the task that's preventing the module from reloading.

## 413003

**Error Message** %ASA-4-413003: Module in slot *slotnum* is not a recognized type

**Explanation** Generated whenever a card is detected that is not recognized as a valid card type.

**Recommended Action** Upgrade to a version of ASA system software that supports the module type installed.



## 413004

**Error Message** %ASA-4-413004: Module in slot *slotnum* failed to write software *vnewver* (currently *vver*), *reason*. Trying again.

**Explanation** The module in the specified slot number failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. Another attempt will be made to update the module software.

*slotnum*—The slot number containing the module.

*newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0).

*ver*—The current version number of the software on the module (for example, 1.0(1)0).

*reason*—The reason the new version could not be written to the module. The possible values for *reason* include the following:

- write failure.
- failed to create a thread to write the image.

**Recommended Action** None. Subsequent attempts will either generate a message indicating a successful update or failure. You may verify the module transitions to UP after a subsequent update attempt by using the **show module** *slotnum* command.

## 414001

**Error Message** %PIX|ASA-3-414001: Failed to save logging buffer using file name *filename* to FTP server *ftp\_server\_address* on interface *interface\_name*: [*fail\_reason*]

**Explanation** This system log message is generated when logging module failed to save the logging buffer to external FTP server.

**Recommended Action** Take appropriate action based on the failed reason:

- Protocol error—Make sure no connectivity issue between the FTP server and security appliance, and FTP sever can accept FTP PORT command and put request.
- Invalid username or password—Make sure that the configured FTP client username and password are correct.
- All other errors—Contact the Cisco TAC for further assistance.

## 414002

**Error Message** %PIX|ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: *filename*: [*fail\_reason*]

**Explanation** This system log message is generated when logging module failed to save the logging buffer to system flash.

**Recommended Action** If the failed reason is due to insufficient space, check the system flash's free space, make sure that the configured limits of the logging flash-size command are set properly. If the error is flash file system IO error, then contact the Cisco technical support for assistance.

## 415001

**Error Message** %PIX|ASA-6-415001: HTTP - matched *matched\_string* in policy-map *map\_name*, header field count exceeded *connection\_action* from *int\_type*:*IP\_address/port\_num* to *int\_type*:*IP\_address/port\_num*

**Explanation** This syslog message is generated when one of the following occurs:

- The total number of fields in the HTTP header exceeds the user-configured number of header fields. The relevant command is : **match { request | response } header count num..**
- The appearance of a specified field in the HTTP header exceeds the user-configured number for this header field. The relevant command is: **match { request | response } header header-name count num.**

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } header** command to reconfigure the HTTP header field value.

## 415002

**Error Message** %PIX|ASA-6-415002: HTTP - matched *matched\_string* in policy-map *map\_name*, header field length exceeded *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog is generated when the specified HTTP header field length exceeds the user-configured length.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } header *header\_name* length gt *num*** command to change the HTTP header field length.

## 415003

**Error Message** %PIX|ASA-6-415003: HTTP - matched *matched\_string* in policy-map *map\_name*, body length exceeded *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the length of the message body exceeds user-configured length.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } body length gt *num*** command to change the length of the message body.

## 415004

**Error Message** %PIX|ASA-5-415004: HTTP - matched *matched\_string* in policy-map *map\_name*, content-type verification failed *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the “magic number” in the body of the HTTP message is not the correct magic number for the mime-type specified in the “content-type” field in the HTTP message header.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } header content-type violation** command to correct the error.

## 415005

**Error Message** %PIX|ASA-5-415005: HTTP - matched *matched\_string* in policy-map *map\_name*, URI length exceeded *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the length of the URI exceeds the user-configured length.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match request uri length gt num** command to change the length of the URI.

## 415006

**Error Message** %PIX|ASA-5-415006: HTTP - matched *matched\_string* in policy-map *map\_name*, URI matched *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the URI matches the regular expression that the user configured. See the **match request uri regex { regex-name | class class-name }** command for more information.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** None.

## 415007

**Error Message** %PIX|ASA-5-415007: HTTP - matched *matched\_string* in policy-map *map\_name*, Body matched *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the message body matches the regular expression that the user configured. See the **match { request | response } body regex { regex-name | class class-name }** command for more information.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** None.

## 415008

**Error Message** %PIX|ASA-5-415008: HTTP - matched *matched\_string* in policy-map *map\_name*, header matched *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when a value in a user-specified field in the message header matches the regular expression that the user configured. See the **match { request | response } header *header-field-name* { *regex-name* | **class** *class-name* }** command for more information.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** None.

## 415009

**Error Message** %PIX|ASA-5-415009: HTTP - matched *matched\_string* in policy-map *map\_name*, method matched *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the HTTP method matches the user-configured regular expression. See the **match request method { *regex-name* | **class** *class-name* }** command for more information.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** None.

## 415010

**Error Message** %PIX|ASA-5-415010: matched *matched\_string* in policy-map *map\_name*, transfer encoding matched *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog is issued when the value in the “transfer encoding” field matches the user-configured regular expression or keyword. See the **match { request | response } header transfer-encoding { { regex-name | class class-name } | keyword }** command for more information.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** None.

## 415011

**Error Message** %PIX|ASA-5-415011: HTTP - policy-map *map\_name*:Protocol violation *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the HTTP parser cannot detect a valid HTTP message in the first few bytes of an HTTP message.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **protocol-violation action { drop | reset } log** command to correct the problem.

## 415012

**Error Message** %PIX|ASA-5-415012: HTTP - matched *matched\_string* in policy-map *map\_name*, Unknown mime-type *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the “content-type” field does not contain a mime type that matches a built-in mime type.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } header content-type unknown** command to correct the problem.

## 415013

**Error Message** %PIX|ASA-5-415013: HTTP - policy-map *map-name*:Malformed chunked encoding *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when a chunked encoding is malformed and the HTTP message cannot be parse, and whenever logging for the **protocol-violation** command is configured.

*map-name*— The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.



*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **protocol-violation action { drop | reset } log** command to correct the problem.

## 415014

**Error Message** %PIX|ASA-5-415014: HTTP - matched *matched\_string* in policy-map *map\_name*, Mime-type in response wasn't found in the accept-types of the request *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the mime type in an HTTP response is not in the “accept” field of the request.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match req-resp content-type mismatch** command to correct the problem.

## 415015

**Error Message** %PIX|ASA-5-415015: HTTP - matched *matched\_string* in policy-map *map\_name*, transfer-encoding unknown *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the an empty transfer encoding occurs.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } header transfer-encoding empty** command to correct the problem.

## 415016

**Error Message** %PIX|ASA-4-415016: policy-map *map\_name*:Maximum number of unanswered HTTP requests exceeded *connection\_action* from *int\_type*:*IP\_address/port\_num* to *int\_type*:*IP\_address/port\_num*

**Explanation** This syslog message is generated when the the number of unanswered HTTP requests exceeds the internal number of requests allowed.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **protocol-violation action { drop | reset } log** command to correct the problem.

## 415017

**Error Message** %PIX|ASA-6-415017: HTTP - *matched\_string* in policy-map *map\_name*, arguments matched *connection\_action* from *int\_type*:*IP\_address/port\_num* to *int\_type*:*IP\_address/port\_num*

**Explanation** This syslog message is generated when a pattern in the arguments matches the user-configured regular expression or keyword. See the **match request args regex { regex-name | class class-name }** command for more information.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** None.

## 415018

**Error Message** %PIX|ASA-5-415018: HTTP - matched *matched\_string* in policy-map *map\_name*, Header length exceeded *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the total header length exceeds the user-configured length for the header.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } header length gt num** command to reduce the length of the header.

## 415019

**Error Message** %PIX|ASA-5-415019: HTTP - matched *matched\_string* in policy-map *map\_name*, status line matched *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when the status line in a response matches user-configured regex. See the **match response status-line regex { regex-name | class class-name }** for more information.

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** None.

## 415020

**Error Message** %PIX|ASA-5-415020: HTTP - matched *matched\_string* in policy-map *map\_name*, a non-ASCII character was matched *connection\_action* from *int\_type:IP\_address/port\_num* to *int\_type:IP\_address/port\_num*

**Explanation** This syslog message is generated when a non-ASCII character is found.

### Explanation

*matched\_string*—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string displays when the class map is user configured.
- The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

*map\_name*—The name of the policy map.

*connection\_action*—“- Dropping connection” or “- Resetting connection.”

*interface\_type*—The type of interface, for example, DMZ, outside, etc.

*IP\_address*—The IP address of the interface.

*port\_num*—The port number.

**Recommended Action** Enter the **match { request | response } header non-ascii** command to correct the problem.

## 416001

**Error Message** %PIX|ASA-4-416001: Dropped UDP SNMP packet from *source\_interface* :*source\_IP/source\_port* to *dest\_interface:dest\_address/dest\_port*; version (*prot\_version*) is not allowed through the firewall

**Explanation** An SNMP packet was denied passage through the security appliance because of a bad packet format or a because the *prot\_version* is not allowed through the security appliance. The field *prot\_version* can be one of the following values: 1, 2, 2c, 3.

**Recommended Action** Change the settings for SNMP inspection using the **snmp-map** command, which allows the user to permit or deny specific protocol versions.

## 417001

**Error Message** %PIX|ASA-4-417001: Unexpected event received: *number*

**Explanation** A process received a signal but no handler was found for the event.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

## 417004

**Error Message** %PIX|ASA-4-417004: Filter violation error: conn *number* (*string:string*) in *string*

**Explanation** A client tried to modify a route attribute that the client does not own.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

## 417006

**Error Message** %PIX|ASA-4-417006: No memory for *string*) in *string*. Handling: *string*

**Explanation** An operation failed due to low memory but will be handled with another mechanism.

**Explanation** If sufficient memory exists, copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

## 417008

**Error Message** %PIX-4-417008 AutoRP: removed *string* embedded group *address1/mask1* on interface *interface-name* from *address2* due to overlap *address3/mask2*

**Explanation** The multicast boundary has a longer mask than the AutoRp encoded group.

*string*—Either “Announcement” or “Discovery.”

*interface-name*—The interface name on which the packet was received.

*address1*—The embedded multicast group address.

*address2*—The source IP address of the AutoRP packet.

*address3*—The multicast boundary group address.

*mask1*—The embedded multicast group mask.

*mask2*—The multicast boundary group mask.

**Recommended Action** Adjust the boundary access rules or RP mappings.

## 417009

**Error Message** %PIX-4-417009 AutoRp: discarded *string* on interface *interface-name* from *address* due to malformed packet

**Explanation** An AutoRp packet was received without a group count in the RP mapping.

*string*—"Announcement" or "Discovery."

*interface-name*—The name of the interface on which the packet was received.

*address*—The source IP address of the AutoRP packet.

**Recommended Action** The originating device might not be RFC compliant. Upgrade the originating device or notify the owner of the device.

## 418001

**Error Message** %PIX|ASA-4-418001: Through-the-device packet to/from management-only network is denied: *protocol\_string* from *interface\_name* *IP\_address* (*port*) to *interface\_name* *IP\_address* (*port*)

**Explanation** A packet from the specified source to the destination is dropped because it is traversing the security appliance to/from the management only network.

*protocol\_string*—TCP, UDP, ICMP or protocol ID as a number in decimal.

*interface\_name*— Interface name.

*IP\_address*—IP address.

*port*—Port number.

**Recommended Action** Investigate who is generating such packet and why.

## 419001

**Error Message** %PIX|ASA-4-419001: Dropping TCP packet from *src\_ifc:src\_IP/src\_port* to *dest\_ifc:dest\_IP/dest\_port*, reason: MSS exceeded, MSS *size*, data *size*

**Explanation** This message is generated when the length of the TCP packet exceeds the MSS advertised in the 3-way handshake.

*src\_ifc*—Input interface name

*src\_IP*—The source IP address of the packet

*src\_port*—The source port of the packet

*dest\_ifc*—The output interface name

*dest\_IP*—The destination IP address of the packet

*dest\_port*—The destination port of the packet

**Recommended Action** If there is a need to allow packets that exceed the MSS, create a TCP map using the **exceed-mss** command, as in the following example:

```
access-list http-list permit tcp any host server_ip eq 80

class-map http
  match access-list http-list

tcp-map tmap
  exceed-mss allow

policy-map global_policy
  class http
    set connection advanced-options tmap
```

## 419002

**Error Message** %ASA-4-419002: Received duplicate TCP SYN from *in\_interface:src\_address/src\_port* to *out\_interface:dest\_address/dest\_port* with different initial sequence number.

**Explanation** A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number than the SYN that opened the embryonic connection. This could indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

*in\_interface*—The input interface.

*src\_address*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*out\_interface*—The output interface.

*dest\_address*—The destination IP address of the packet.

*dest\_port*—The destination port of the packet.

**Recommended Action** None.

## 420001

**Error Message** %ASA-3-420001 : IPS card not up and fail-close mode used, dropping ICMP packet *ifc\_in:SIP* to *ifc\_out:DIP* (type*ICMP\_TYPE*, code *ICMP\_CODE*) "

```
%ASA-3-420001 : IPS card not up and fail-close mode used, dropping TCP packet from
ifc_in:SIP/SPORT to ifc_out:DIP/DPORT\n"
```

```
%ASA-3-420001 : IPS card not up and fail-close mode used, dropping UDP packet from
ifc_in:SIP/SPORT to ifc_out:DIP/DPORT\n"
```

```
%ASA-3-420001 : IPS card not up and fail-close mode used, dropping protocol protocol
packet from ifc_in:SIP to ifc_out:DIP\n"
```

**Explanation** This message is displayed when packets are dropped when IPS fail-close mode is used and the IPS card is not up. This message is rate limited.

*ifc\_in*—Input interface name

*ifc\_out*—Output interface name

*SIP*—Source IP of the packet

*SPORT* —Source port of the packet

*DIP*—Destination IP of the packet

*DPORT* —Destination port of the packet

*ICMP\_TYPE*—Type of the ICMP packet

*ICMP\_CODE*—Code of the ICMP packet

**Recommended Action** Check and bring up the IPS card.

## 420002

**Error Message** %ASA-4-420002 : IPS requested to drop ICMP packets *ifc\_in:SIP* to *ifc\_out:DIP* (type*ICMP\_TYPE*, code *ICMP\_CODE*) "

```
%ASA-4-420002 : IPS requested to drop TCP packet from ifc_in:SIP/SPORT to
ifc_out:DIP/DPORT\n"
```

```
%ASA-4-420002 : IPS requested to drop UDP packet from ifc_in:SIP/SPORT to
ifc_out:DIP/DPORT\n"
```

```
%ASA-4-420002 : IPS requested to drop protocol packet from ifc_in:SIP to
ifc_out:DIP\n"
```

**Explanation** This message is displayed when when IPS requests the packet to be dropped.

*ifc\_in*—Input interface name

*ifc\_out*—Output interface name

*SIP*—Source IP of the packet

*SPORT* —Source port of the packet

*DIP*—Destination IP of the packet

*DPORT* —Destination port of the packet

*ICMP\_TYPE*—Type of the ICMP packet

*ICMP\_CODE*—Code of the ICMP packet

**Recommended Action** No action required



## 420003

**Error Message** %ASA-4-420003 : IPS requested to reset TCP connection from *ifc\_in:SIP/SPORT* to *ifc\_out:DIP/DPORT*"

**Explanation** This message is displayed when IPS requests to reset a TCP connection.

*ifc\_in*—Input interface name

*ifc\_out*—Output interface name

*SIP*—Source IP of the packet

*SPORT* —Source port of the packet

*DIP*—Destination IP of the packet

*DPORT* —Destination port of the packet

**Recommended Action** None.

## 421001

**Error Message** %ASA-3-421001: TCP|UDP flow from *interface\_name:ip/port* to *interface\_name:ip/port* is dropped because *application* has failed.

**Explanation** A packet was dropped because the CSC SSM application failed. By default, this message is rate limited to 1 message every 10 seconds.

*interface\_name*—The interface name.

*IP\_address*—The IP address.

*port*—The port number.

*application*—The CSC SSM is the only application supported in the current release.

**Recommended Action** Immediately investigate the problem with the service module.

## 421002

**Error Message** %ASA-6-421002: TCP|UDP flow from *interface\_name:IP\_address/port* to *interface\_name:IP\_address/port* bypassed *application* checking because the protocol is not supported.

**Explanation** Connection bypassed service module security checking because the protocol it is using cannot be scanned by the service module. For example, the CSC SSM is not capable of scanning TELNET traffic. If user configures TELNET traffic to be scanned, the traffic will bypass the scanning service. By default, this message is rate limited to 1 message every 10 seconds.

*IP\_address*—The IP address.

*port*—The port number.

*interface\_name*—The name of the interface on which the policy is applied.

*application*—The CSC SSM is the only application supported in the current release.

**Recommended Action** The configuration should be modified to only include protocols that are supported by the service module.

## 421003

**Error Message** %ASA-3-421003: Invalid data plane encapsulation.

**Explanation** A packet injected by the service module did not have the correct data plane header. Packets exchanged on data backplane adhere to a Cisco proprietary protocol called ASDP. Any packet that does not have the proper ASDP header is dropped.

**Recommended Action** Use the **capture name type asp-drop [ssm-asdp-invalid-encap]** command to capture the offending packets and contact the Cisco TAC.

## 421004

**Error Message** %ASA-7-421004: Failed to inject {TCP|UDP} packet from *IP\_address/port* to *IP\_address/port*

**Explanation** The security appliance has failed to inject a packet as instructed by the service module. This could happen if the security appliance tries to inject a packet into a flow that has already been released.

*IP\_address*—The IP address.

*port*—The port number.

**Recommended Action** This could happen because the security appliance maintains its connection table independently from the service module. Normally it will not cause any problem. If this affects security appliance performance, contact the Cisco TAC.

## 421005

**Error Message** %ASA-6-421005: *interface\_name:IP\_address* is counted as a user of *application*

**Explanation** A host has been counted toward the license limit. The specified host was counted as a user of *application*. The total number of users in 24 hours is calculated at midnight for license validation.

*interface\_name*—The interface name.

*IP\_address*—The IP address.

*application*—The CSC SSM is the only application supported in the current release.

**Recommended Action** None. However, if the overall count exceeds the user license you have purchased, contact the Cisco to upgrade your license.

## 421006

**Error Message** %ASA-6-421006: There are *number* users of *application* accounted during the past 24 hours.

**Explanation** Identifies the total number of users who have used *application* for the past 24 hours. This message is generated every 24 hours to give the total number of hosts that have used services provided by the service module.

**Recommended Action** None. However, if the overall count exceeds the user license you have purchased, contact the Cisco to upgrade your license.

## 421007

**Error Message** %ASA-3-421007: TCP|UDP flow from *interface\_name:IP\_address/port* to *interface\_name:IP\_address/port* is skipped because *application* has failed.

**Explanation** This message is generated when a flow is skipped because the service module application has failed. By default, this message is rate limited to 1 message every 10 seconds.

*IP\_address*—The IP address.

*port*—The port number.

*interface\_name*—The name of the interface on which the policy is applied.

*application*—the CSC SSM is the only application supported in the current release.

**Recommended Action** Immediately investigate the problem with the service module.

## 422004

**Error Message** %PIX|ASA-4-422004: IP SLA Monitor *number0*: Duplicate event received.  
Event number *number1*

**Explanation** The IP SLA monitor process has received a duplicate event. Currently, this message applies to destroy events. Only one destroy request will be applied.

*number0*—The SLA operation number.

*number1*—The SLA operation event ID.

**Recommended Action** This is only a warning message. If this reoccurs, enter the **show sla monitor configuration** *SLA\_operation\_id* command and copy the output of the command. Copy the message as it appears on the console or in the system log. Then contact your Cisco technical support representative and provide the representative with the information you gathered, along with information about the application that is configuring and polling the SLA probes.

## 422005

**Error Message** %PIX|ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.

**Explanation** One or more IP SLA monitor probes could not be scheduled because the system clock is not set.

**Recommended Action** Ensure that the system clock is functional by using NTP or another mechanism.

## 422006

**Error Message** %PIX|ASA-4-422006: IP SLA Monitor Probe *number: string*

**Explanation** The IP SLA monitor probe could not be scheduled. Either the configured starting time has already occurred or the starting time is invalid.

*number*—The SLA operation ID.

*string*—A string describing the error.

**Recommended Action** Reschedule the failed probe with a valid start time.

## 423001

**Error Message** %ASA-4-423001: {Allowed | Dropped} invalid NBNS *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name:ip\_address/port* to *ifc\_name:ip\_address/port*.

**Explanation** The NBNS packet format is incorrect.

**Recommended Action** None.

## 423002

**Error Message** %ASA-4-423002: {Allowed | Dropped} mismatched NBNS *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name:ip\_address/port* to *ifc\_name:ip\_address/port*.

**Explanation** There is an NBNS ID mismatch.

**Recommended Action** None.

## 423003

**Error Message** %ASA-4-423003: {Allowed | Dropped} invalid NBDGM *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name:ip\_address/port* to *ifc\_name:ip\_address/port*.

**Explanation** The NBDGM packet format is incorrect.

**Recommended Action** None.

## 423004

**Error Message** %ASA-4-423004: {Allowed | Dropped} mismatched NBDGM *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name:ip\_address/port* to *ifc\_name:ip\_address/port*.

**Explanation** There is an NBDGM ID mismatch.

**Recommended Action** None.

## 423005

**Error Message** %ASA-4-423005: {Allowed | Dropped} NBDGM *pkt\_type\_name* fragment with *error\_reason\_str* from *ifc\_name:ip\_address/port* to *ifc\_name:ip\_address/port*.

**Explanation** The NBDGM fragment format is incorrect.

**Recommended Action** None.

## 424001

**Error Message** %ASA-4-424001: Packet denied *protocol\_string* *intf\_in:src\_ip/src\_port* *intf\_out:dst\_ip/dst\_port*. [Ingress|Egress] interface is in a backup state.

**Explanation** A packet was dropped because it was traversing the security appliance to/from a redundant interface. Interface functionality is limited on low-end platforms. The interface specified by the **backup interface** command can only be a backup for the primary interface configured. If the default route to the primary interface is up, any traffic through the device from the backup interface will be denied. Conversely, if the default route to the primary interface is down, traffic through the device from the primary interface will be denied.

*protocol\_string*—The protocol string; for example, TCP or protocol ID (a decimal number).

*intf\_in*—The input interface name.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*intf\_out*—The output interface name.

*dst\_ip*—The destination IP address of the packet.

*dst\_port*—The destination port of the packet.

**Recommended Action** Investigate the source of the denied packet.

## 424002

**Error Message** %ASA-4-424002: Connection to the backup interface is denied:  
*protocol\_string intf:src\_ip/src\_port intf:dst\_ip/dst\_port*

**Explanation** A connection was dropped because it is in a backup state. Interface functionality is limited on low-end platforms. The backup interface can only be a backup for the primary interface specified by the **backup interface** command. If the default route to the primary interface is up, any connection to the security appliance through the backup interface will be denied. Conversely, if the default route to the primary interface is down, connections to the security appliance through the primary interface will be denied.

*protocol\_string*—The protocol string; for example, TCP or protocol ID (a decimal number).

*intf\_in*—The input interface name.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*intf\_out*—The output interface name.

*dst\_ip*—The destination IP address of the packet.

*dst\_port*—The destination port of the packet.

**Recommended Action** Investigate the source of the denied packet.

## 431001

**Error Message** %PIX|ASA-4-431001: RTP conformance: Dropping RTP packet from  
*in\_ifc:src\_ip/src\_port* to *out\_ifc:dst\_ip/dest\_port*, Drop reason: *drop\_reason*  
*value*

**Explanation** The RTP packet was dropped.

*in\_ifc*—The input interface.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*out\_ifc*—The output interface.

*dst\_ip*—The destination IP address of the packet.

*dst\_port*—The destination port of the packet.

*drop\_reason*—One of the following drop reasons:

- Incorrect version *value*—The version number from the packet is incorrect.
- Invalid payload-type *value*—The payload type from the packet is invalid.

- Incorrect SSRC *value*—The SSRC from the packet is incorrect.
- Out of range sequence number *value* sequence number from the packet.
- Out of sequence in packet in probation *value* sequence number from the packet.

**Recommended Action** Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the security appliance.

## 431002

**Error Message** %PIX|ASA-4-431002: RTCP conformance: Dropping RTCP packet from *in\_ifc:src\_ip/src\_port* to *out\_ifc:dest\_ip/dest\_port*, Drop reason: *drop\_reason value*

*in\_ifc*—The input interface.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*out\_ifc*—The output interface.

*dest\_ip*—The destination IP address of the packet.

*dest\_port*—The destination port of the packet.

*drop\_reason*—One of the following drop reasons:

- Incorrect version *value*—The version number from the packet is incorrect.
- Invalid payload-type *value*—The payload type from the packet is incorrect.

**Recommended Action** Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the security appliance.

## 450001

**Error Message** ASA-4-450001: Deny traffic for protocol *protocol\_id* src *interface\_name:IP\_address/port* dst *interface\_name:IP\_address/port*, licensed host limit of *num* exceeded.

**Explanation** The licensed host limit was exceeded. This message applies to the ASA 5505 adaptive security appliance only.

*protocol\_id*—The protocol ID number.

*interface\_name*—The interface associated with the sender/receiver of the packet.

*IP\_address*—The IP address of the sender/receiver of the packet.

*port*—The port number of the packet transmitted.

*num*—The maximum host limit value.

**Recommended Action** None.

## Messages 500001 to 509001

This section contains messages from 500001 to 509001.

### 500001

**Error Message** %PIX|ASA-5-500001: ActiveX content modified src *IP\_address* dest *IP\_address* on interface *interface\_name*.

**Explanation** This message is displayed after you turn on the **activex** option using the **filter** command, and the security appliance detects an ActiveX object. The **activex** option allows the security appliance to filter out ActiveX contents by modifying it so that it no longer is tagged as an HTML object.

**Recommended Action** None.

### 500002

**Error Message** %PIX|ASA-5-500002: Java content modified src *IP\_address* dest *IP\_address* on interface *interface\_name*.

**Explanation** This message is displayed after you turn on the **java** option using the **filter** command, and the security appliance detects an Java applet. The **java** option allows the security appliance to filter out Java contents by modifying it so that it no longer is tagged as an HTML object.

**Recommended Action** None.

### 500003

**Error Message** %PIX|ASA-5-500003: Bad TCP hdr length (hdrlen=*bytes*, pktlen=*bytes*) from *source\_address/source\_port* to *dest\_address/dest\_port*, flags: *tcp\_flags*, on interface *interface\_name*

**Explanation** This message indicates that a header length in TCP is incorrect. Some operating systems do not handle TCP resets (RSTs) correctly when responding to a connection request to a disabled socket. If a client tries to connect to an FTP server outside the security appliance and FTP is not listening, then the server sends an RST. Some operating systems send incorrect TCP header lengths, which causes this problem. UDP uses ICMP port unreachable messages.

The TCP header length may indicate that it is larger than the packet length, which results in a negative number of bytes being transferred. A negative number is displayed by system log message as an unsigned number, which makes it appear much larger than it would be normally; for example, it may show 4 GB transferred in 1 second.

**Recommended Action** None. This message should occur infrequently.



## 500004

**Error Message** %PIX|ASA-4-500004: Invalid transport field for protocol=*protocol*, from *source\_address/source\_port* to *dest\_address/dest\_port*

**Explanation** This message appears when there is an invalid transport number, in which the source or destination port number for a protocol is zero. The *protocol* value is 6 for TCP and 17 for UDP.

**Recommended Action** If these messages persist, contact the peer's administrator.

## 501101

**Error Message** %PIX|ASA-5-501101: User transitioning priv level

**Explanation** The privilege level of a command was changed.

**Recommended Action** None.

## 502101

**Error Message** %PIX|ASA-5-502101: New user added to local dbase: Uname: *user* Priv: *privilege\_level* Encpass: *string*

**Explanation** A new username record was created. The message lists the username, privilege level, and encrypted password.

**Recommended Action** None.

## 502102

**Error Message** %PIX|ASA-5-502102: User deleted from local dbase: Uname: *user* Priv: *privilege\_level* Encpass: *string*

**Explanation** A username record was deleted. The message lists the username, privilege level, and encrypted password.

**Recommended Action** None.

## 502103

**Error Message** %PIX|ASA-5-502103: User priv level changed: Uname: *user* From: *privilege\_level* To: *privilege\_level*

**Explanation** The privilege level of a user changed.

**Recommended Action** None.

## 502111

**Error Message** %PIX|ASA-5-502111: New group policy added: name: *policy\_name* Type: *policy\_type*

**Explanation** This is an indication that a group policy has been configured using the **group-policy** CLI command. *policy\_name* is the name of the group policy. *policy\_type* is either “internal” or “external.”

**Recommended Action** None.

## 502112

**Error Message** %PIX|ASA-5-502112: Group policy deleted: name: *policy\_name* Type: *policy\_type*

**Explanation** A group policy has been removed using the **group-policy** CLI command. *policy\_name* is the name of the group policy. *policy\_type* is either “internal” or “external.”

**Recommended Action** None.

## 503001

**Error Message** %PIX|ASA-5-503001: Process number, Nbr *IP\_address* on *interface\_name* from *string* to *string*, *reason*

**Explanation** An OSPF neighbor has changed its state. The message describes the change and the reason for it. This message appears only if the **log-adjacency-changes** command is configured for the OSPF process.

**Recommended Action** To determine what is causing this problem, contact the Cisco TAC for assistance.

## 504001

**Error Message** %PIX|ASA-5-504001: Security context *context\_name* was added to the system

**Explanation** A security context was successfully added to the system.

**Recommended Action** None.

## 504002

**Error Message** %PIX|ASA-5-504002: Security context *context\_name* was removed from the system

**Explanation** A security context was successfully removed from the system.

**Recommended Action** None.

## 505001

**Error Message** %ASA-5-505001: Module in slot *slotnum* is shutting down. Please wait...

**Explanation** Generated when a card is being shut down.

**Recommended Action** None.

## 505002

**Error Message** %ASA-5-505002: Module in slot *slotnum* is reloading. Please wait...

**Explanation** Generated when a card is being reloaded

**Recommended Action** None.

## 505003

**Error Message** %ASA-5-505003: Module in slot *slotnum* is resetting. Please wait...

**Explanation** Generated when a module is being reset .

**Recommended Action** None.

## 505004

**Error Message** %ASA-5-505004: Module in slot *slotnum* shutdown is complete.

**Explanation** Generated when a module has been shut down.

**Recommended Action** None.

## 505005

**Error Message** %ASA-5-505005: Module in slot *slotnum* is initializing control communication. Please wait...

**Explanation** Generated when a module has been detected and the ASA system module is initializing control channel communication with it.

**Recommended Action** None.

## 505006

**Error Message** %ASA-5-505006: Module in slot *slotnum* is Up.

**Explanation** Generated when a module has completed control channel initialization and is in the UP state.

**Recommended Action** None.

## 505007

**Error Message** %ASA-5-505007: Module in slot *slotnum* is recovering. Please wait...

**Explanation** Generated when a module is being recovered with the **hw-module module *slotnum* recover boot** command.

**Recommended Action** None.

## 505008

**Error Message** %ASA-5-505008: Module in slot *slotnum* software is being updated to *vnewver* (currently *vver*)

**Explanation** This message appears when the 4GE SSM module software is being upgraded by the system module.

*slotnum*—The slot number containing the module

*newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0)

*ver*—The current version number of the software on the module (for example, 1.0(1)0)

**Recommended Action** None. The update is proceeding normally.

## 505009

**Error Message** %ASA-5-505009: Module in slot *slotnum* software was updated to *vnewver* (previously *vver*)

**Explanation** :This message appears when the 4GE SSM module software is successfully upgraded by the system module.

*slotnum*—The slot number containing the module

*newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0)

*ver*—The current version number of the software on the module (for example, 1.0(1)0)

**Recommended Action** None. The update has completed successfully.

## 505010

**Error Message** %ASA-5-505010: Module in slot *slot* data channel communication is UP.

**Explanation** This message is generated whenever the data channel communication recovers from a DOWN state. This message indicates that data channel communication is operating normally. It occurs after the data channel communication fails and then recovers.

*slot*—The slot that has established data channel communication.

**Recommended Action** No action required unless this message was generated as a result of a previous data channel communication failure (message 3-323006). In that case, check the 4GE SSM messages to determine the cause of the communication failure.

## 505011

**Error Message** %ASA-5-505011: Module in slot *slot*, application detected *application*, version *version*.

**Explanation** A new application was detected on a 4GE SSM. This may occur when the system boots, when the 4GE SSM boots, or when the 4GE SSM starts a new application.

*slot*—The slot in which the application was detected.

*application*—The name of the application detected.

*version*—The application version detected.

**Recommended Action** No action required if the activity described is normal and expected.

## 505012

**Error Message** %ASA-5-505012: Module in slot *slot*, application stopped *application*, version *version*

**Explanation** This message is generated whenever an application is stopped or removed from a 4GE SSM. This may occur when the 4GE SSM upgrades an application or when an application on the 4GE SSM is stopped or uninstalled.

*slot*—The slot in which the application was stopped.

*application*—The name of the application stopped.

*version*—The application version stopped.

**Recommended Action** If an upgrade was not occurring on the 4GE SSM or the application was not intentionally stopped or uninstalled, review the logs from the 4GE SSM to determine why the application stopped.

## 505013

**Error Message** %ASA-5-505013: Module in slot *slot* application changed from: *application* version *version* to: *newapplication* version *newversion*.

**Explanation** This message is generated whenever an application version changes, such as after an upgrade. This occurs when a software update for the application on the module is complete.

*slot*—The slot in which the application was upgraded.

*application*—The name of the application that was upgraded.

*version*—The application version that was upgraded.

*slot*—The slot in which the application was upgraded.

*application*—The name of the application that was upgraded.

*version*—The application version that was upgraded.

*newapplication*—The new application name.

*newversion*—The new application version.

**Recommended Action** Verify that the upgrade was expected and that the new version is correct.

## 506001

**Error Message** %ASA-5-506001: *event\_source\_string event\_string*

**Explanation** Status of a file system has changed. The message describes the event and the source of the event that caused a file system to become available or unavailable. Examples of sources and events that could cause a file system status change are as follows:

- External Compact Flash removed
- External Compact Flash inserted
- External Compact Flash -unknown event

**Recommended Action** None required

## 507001

**Error Message** %PIX|ASA-5-507001: Terminating TCP-Proxy connection from *interface\_inside:source\_address/source\_port* to *interface\_outside:dest\_address/dest\_port* - reassembly limit of *limit* bytes exceeded

**Explanation** This message is displayed when reassembly buffer limit is exceeded during assembling TCP segments.

- *source\_address/source\_port*—The source IP address and the source port of the packet initiating the connection.
- *dest\_address/dest\_port*—The destination IP address and the destination port of the packet initiating the connection.
- *interface\_inside*—The name of the interface on which the packet which initiated the connection arrives.
- *interface\_outside*—The name of the interface on which the packet which initiated the connection exits.
- *limit*—The configured embryonic connection limit for the traffic class.

**Recommended Action** None.

## 507002

**Error Message** %PIX|ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit

**Explanation** This syslog message is generated when there is an operational error when processing a fragmented TCP message.

**Recommended Action** None.

## 508001

**Error Message** %PIX|ASA-5-508001: DCERPC *message\_type* non-standard *version\_type* *version\_number* from *src\_if:src\_ip/src\_port* to *dest\_if:dest\_ip/dest\_port*, terminating connection.

**Explanation** This message is generated when using DCERPC inspection. It is logged when a message header contains a nonstandard major or minor version.

*message\_type*—The DCERPC message type.

*version\_type*—The version type, major or minor.

*version\_number*—The nonstandard version in the message header.

**Recommended Action** If this is a valid version, contact the Cisco TAC.

## 508002

**Error Message** %PIX|ASA-5-508002: DCERPC response has low endpoint port *port\_number* from *src\_if:src\_ip/src\_port* to *dest\_if:dest\_ip/dest\_port*, terminating connection.

**Explanation** This message is generated when using DCERPC inspection. The message is logged when a response message contains an endpoint port number less than 1024 (in the range of well-known server ports).

**Recommended Action** None.



## 509001

**Error Message** %ASA-5-509001: Connection attempt from *src\_intf:src\_ip/src\_port* to *dst\_intf:dst\_ip/dst\_port* was prevented by “no forward” command.

**Explanation** The **no forward interface** command was entered to block traffic from the source interface to the destination interface given in the syslog message. This command is required on low-end platforms to allow the creation of interfaces beyond the licensed limit.

*src\_intf*—The name of the source interface to which the **no forward interface** command restriction applies.

*dst\_intf*—The name of the destination interface to which the **no forward interface** command restriction applies.

**Recommended Action** Upgrade the license to remove the requirement of this command on low-end platforms and remove the command from the configuration.

## Messages 602101 to 622102

This section contains messages from 602101 to 622102.

### 602101

**Error Message** %PIX|ASA-6-602101: PMTU-D packet *number* bytes greater than effective mtu *number* dest\_addr=*dest\_address*, src\_addr=*source\_address*, prot=*protocol*

**Explanation** This message occurs when the security appliance sends an ICMP destination unreachable message and when fragmentation is needed, but the “don’t-fragment” bit is set.

**Recommended Action** Ensure that the data is sent correctly.

### 602103

**Error Message** %PIX|ASA-6-602103: IPSEC: Received an ICMP Destination Unreachable from *src\_addr* with suggested PMTU of *rcvd\_mtu*; PMTU updated for SA with peer *peer\_addr*, SPI *spi*, tunnel name *username*, old PMTU *old\_mtu*, new PMTU *new\_mtu*.

**Explanation** This message is displayed when the MTU of an SA is changed. When a packet is received for an IPsec tunnel, the corresponding SA is located and the MTU is updated based on the MTU suggested in the ICMP packet. If the suggested MTU is greater than 0 but less than 256, then the new MTU is set to 256. If the suggested MTU is 0, the old MTU is reduced by 256 or it is set to 256, whichever value is greater. If the suggested MTU is greater than 256, then the new MTU is set to the suggested value.

*src\_addr* —IP address of the PMTU sender

*rcvd\_mtu*—Suggested MTU received in the PMTU message

*peer\_addr*—IP address of the IPsec peer  
*spi*—IPsec Security Parameters Index  
*username*—Username associated with the IPsec tunnel  
*old\_mtu*—Previous MTU associated with the IPsec tunnel  
*new\_mtu*—New MTU associated with the IPsec tunnel

**Recommended Action** None.

## 602104

**Error Message** %PIX|ASA-6-602104: IPSEC: Received an ICMP Destination Unreachable from *src\_addr*, PMTU is unchanged because suggested PMTU of *rcvd\_mtu* is equal to or greater than the current PMTU of *curr\_mtu*, for SA with peer *peer\_addr*, SPI *spi*, tunnel name *username*.

*src\_addr*—IP address of the PMTU sender  
*rcvd\_mtu*—Suggested MTU received in the PMTU message  
*curr\_mtu*—Current MTU associated with the IPsec tunnel  
*peer\_addr*—IP address of the IPsec peer  
*spi*—IPsec Security Parameters Index  
*username*—Username associated with the IPsec tunnel

**Explanation** This message occurs when an ICMP message is received indicating that a packet sent over an IPsec tunnel exceeded the path MTU and the suggested MTU is greater than or equal to the current MTU. Because the MTU value is already correct, no MTU adjustment is made. This may happen when multiple PMTU messages are received from different intermediate stations and the MTU is adjusted before the current PMTU message is processed.

**Recommended Action** None.

## 602201

**Error Message** %PIX|ASA-6-602201: ISAKMP Phase 1 SA created (local *IP\_address/port* (initiator|responder), remote *IP\_address/port*, authentication=*auth\_type*, encryption=*encr\_alg*, hash=*hash\_alg*, group=*DH\_grp*, lifetime=*seconds*)

**Explanation** This message is displayed when an ISAKMP SA is created.

**Recommended Action** None.

## 602202

**Error Message** %PIX|ASA-6-602202: ISAKMP session connected (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** An ISAKMP peer has connected.

**Recommended Action** None.

## 602203

**Error Message** %PIXPIX|ASA-6-602203: ISAKMP session disconnected (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** An ISAKMP peer has disconnected.

**Recommended Action** None.

## 602303

**Error Message** %PIX|ASA-6-602303: IPSEC: An *direction tunnel\_type* SA (SPI=*spi*) between *local\_IP* and *remote\_IP* (*username*) has been created.

*direction*—SA direction (inbound or outbound)

*tunnel\_type*—SA type (remote access or L2L)

*spi*—IPSec Security Parameters Index

*local\_IP*—IP address of the tunnel local endpoint

*remote\_IP*—IP address of the tunnel remote endpoint

*username*—Username associated with the IPSec tunnel

**Explanation** A new security association (SA) was created.

**Recommended Action** No action is required.

## 602304

**Error Message** %PIX|ASA-6-602304: IPSEC: An *direction tunnel\_type* SA (SPI=*spi*) between *local\_IP* and *remote\_IP* (*username*) has been deleted.

**Explanation** This message is displayed when an SA is deleted.

*direction*—SA direction (inbound or outbound)

*tunnel\_type*—SA type (remote access or L2L)

*spi*—IPSec Security Parameters Index

*local\_IP*—IP address of the tunnel local endpoint  
*remote\_IP*—IP address of the tunnel remote endpoint  
*username*—Username associated with the IPsec tunnel

**Recommended Action** No action is required.

## 603101

**Error Message** %PIX|ASA-6-603101: PPTP received out of seq or duplicate pkt, tnl\_id=*number*, sess\_id=*number*, seq=*number*.

**Explanation** The security appliance received a PPTP packet that was out of sequence or duplicated.

**Recommended Action** If the packet count is high, contact the peer administrator to check client PPTP configuration.

## 603102

**Error Message** %PIX|ASA-6-603102: PPP virtual interface *interface\_name* - user: *user* aaa authentication started.

**Explanation** The security appliance sent an authentication request to the AAA server.

**Recommended Action** None.

## 603103

**Error Message** %PIX|ASA-6-603103: PPP virtual interface *interface\_name* - user: *user* aaa authentication *status*

**Explanation** The security appliance received an authentication response from the AAA server .

**Recommended Action** None.

## 603104

**Error Message** %PIX|ASA-6-603104: PPTP Tunnel created, tunnel\_id is *number*, remote\_peer\_ip is *remote\_address*, ppp\_virtual\_interface\_id is *number*, client\_dynamic\_ip is *IP\_address*, username is *user*, MPPE\_key\_strength is *string*

**Explanation** A PPTP tunnel was created.

**Recommended Action** None.

## 603105

**Error Message** %PIX|ASA-6-603105: PPTP Tunnel deleted, tunnel\_id = *number*, remote\_peer\_ip= *remote\_address*

**Explanation** A PPTP tunnel was deleted.

**Recommended Action** None.

## 603106

**Error Message** %PIX|ASA-6-603106: L2TP Tunnel created, tunnel\_id is *number*, remote\_peer\_ip is *remote\_address*, ppp\_virtual\_interface\_id is *number*, client\_dynamic\_ip is *IP\_address*, username is *user*

**Explanation** An L2TP tunnel was created.

**Recommended Action** None.

## 603107

**Error Message** %PIX|ASA-6-603107: L2TP Tunnel deleted, tunnel\_id = *number*, remote\_peer\_ip = *remote\_address*

**Explanation** An L2TP tunnel was deleted.

**Recommended Action** None.

## 603108

**Error Message** %PIX|ASA-6-603108: Built PPTP Tunnel at *interface\_name*, tunnel-id = *number*, remote-peer = *IP\_address*, virtual-interface = *number*, client-dynamic-ip = *IP\_address*, username = *user*, MPPE-key-strength = *number*

**Explanation** This message is displayed each time a new PPPoE tunnel is created.

**Recommended Action** None.

## 603109

**Error Message** %PIX|ASA-6-603109: Teardown PPPOE Tunnel at *interface\_name*, tunnel-id = *number*, remote-peer = *IP\_address*

**Explanation** This message is displayed each time a new PPPoE tunnel is deleted.

**Recommended Action** None.

## 604101

**Error Message** %PIX|ASA-6-604101: DHCP client interface *interface\_name*: Allocated ip = *IP\_address*, mask = *netmask*, gw = *gateway\_address*

**Explanation** The security appliance DHCP client successfully obtained an IP address from a DHCP server. The **dhcpc** command statement allows the security appliance to obtain an IP address and network mask for a network interface from a DHCP server as well as a default route. The default route statement uses the gateway address as the address of the default router.

**Recommended Action** None.

## 604102

**Error Message** %PIX|ASA-6-604102: DHCP client interface *interface\_name*: address released

**Explanation** The security appliance DHCP client released an allocated IP address back to the DHCP server.

**Recommended Action** None.

## 604103

**Error Message** %PIX|ASA-6-604103: DHCP daemon interface *interface\_name*: address granted *MAC\_address* (*IP\_address*)

**Explanation** The security appliance DHCP server granted an IP address to an external client.

**Recommended Action** None.

## 604104

**Error Message** %PIX|ASA-6-604104: DHCP daemon interface *interface\_name*: address released

**Explanation** An external client released an IP address back to the security appliance DHCP server.

**Recommended Action** None.

## 605004

**Error Message** %PIX|ASA-6-605004: Login denied from *source-address/source-port* to *interface:destination/service* for user "*username*"

The following form of the message is displayed when the user tries to login to the console:

```
Login denied from serial to console for user "username"
```

**Explanation** This message appears after an incorrect login attempt or a failed login to the security appliance. For all logins, three attempts are allowed per session, and the session is terminated after three incorrect attempts. For SSH and TELNET logins, this message is generated after the third failed attempt or if the TCP session is terminated after one or more failed attempts. For other types of management sessions, this message is generated after every failed attempt.

*source-address*—Source address of the login attempt

*source-port*—Source port of the login attempt

*interface*—Destination management interface

*destination*—Destination IP address

*service*—Destination service

*username* —Destination management interface

**Recommended Action** If this message appears infrequently, no action is required. If this message appears frequently, it may indicate an attack. Communicate with the user to verify the username and password.

## 605005

**Error Message** %PIX|ASA-6-605005: Login permitted from *source-address/source-port* to *interface:destination/service* for user "*username*"

The following form of the message is displayed when the user logs in to the console:

```
Login permitted from serial to console for user "username"
```

**Explanation** This message appears when a user is authenticated successfully and a management session starts.

*source-address*—Source address of the login attempt

*source-port*—Source port of the login attempt

*interface*—Destination management interface

*destination*—Destination IP address

*service*—Destination service

*username*—Destination management interface

**Recommended Action** None.

## 606001

**Error Message** %PIX|ASA-6-606001: ASDM session number *number* from *IP\_address* started

**Explanation** This message indicates that an administrator has been authenticated successfully and a ASDM session was started.

**Recommended Action** None.

## 606002

**Error Message** %PIX|ASA-6-606002: ASDM session number *number* from *IP\_address* ended

**Explanation** This message indicates that a ASDM session ended.

**Recommended Action** None.

## 606003

**Error Message** %PIX|ASA-6-606003: ASDM logging session number *id* from *IP\_address* started *id* session ID assigned

**Explanation** An ASDM logging connection is started by a remote management client.

*IP\_address*—IP address of remote management client

**Recommended Action** No action is required from the user.



## 606004

**Error Message** %PIX|ASA-6-606004: ASDM logging session number *id* from *IP\_address* ended

**Explanation** An ASDM logging connection is terminated.

*id*—session ID assigned

*IP\_address*—IP address of remote management client

**Recommended Action** No action is required from the user.

## 607001

**Error Message** %PIX|ASA-6-607001: Pre-allocate SIP *connection\_type* secondary channel for *interface\_name:IP\_address/port* to *interface\_name:IP\_address* from *string* message

**Explanation** This message indicates that the **fixup sip** command preallocated a SIP connection after inspecting a SIP message. The *connection\_type* is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

**Recommended Action** None.

## 607002

**Error Message** %PIX|ASA-4-607002: *action\_class: action* SIP *req\_resp req\_resp\_info* from *src\_ifc:sip/sport* to *dest\_ifc:dip/dport; further\_info*

**Explanation** This message is generated when a SIP classification is performed on a SIP message and the specified criteria is satisfied. Then the configured action occurs.

*action\_class*—The class of the action: "SIP Classification" for SIP match commands or "SIP Parameter" for parameter commands.

*action*—The action taken: "Dropped," "Dropped connection for," "Reset connection for," or "Masked header flags for."

*req\_resp*—"Request" or "Response."

*req\_resp\_info*—The SIP method name if the type is "Request": INVITE, CANCEL, etc. The SIP response code if type is "Response": 100, 183, 200, etc.

*src\_ifc*—The source interface name.  
*sip*—The source IP address.  
*sport*—The source port.  
*dest\_ifc*—The destination interface name.  
*dip*—The destination IP address.  
*dport*—The destination port.  
*further\_info*—Displays more information for SIP match and SIP parameter commands, as follows:

- For SIP match commands:

matched Class *id: class-name*—For example:

```
matched Class 1234: my_class
```

- For SIP parameter commands:

*parameter-command: descriptive-message*—For example:

```
strict-header-validation: Mandatory header field 'Via' is missing
state-checking: Message CANCEL is not permitted to create a Dialog.
```

**Recommended Action** None.

## 607003

**Error Message** %PIX|ASA-6-607003: *action\_class*: Received SIP *req\_resp req\_resp\_info* from *src\_ifc:sip/sport* to *dest\_ifc:dip/dport*; *further\_info*

**Explanation** This event is generated when a SIP classification is performed on a SIP message and the specified criteria is satisfied. Then the standalone log action occurs.

*action\_class*—"SIP Classification" for SIP match commands or "SIP Parameter" for parameter commands.

*req\_resp*—"Request" or "Response."

*req\_resp\_info*—The SIP method name if the type is "Request": INVITE, CANCEL, etc. The SIP response code if type is "Response": 100, 183, 200, etc.

*src\_ifc*—The source interface name.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

*further\_info*—Displays more information for SIP match and SIP parameter commands, as follows:

- For SIP match commands:

matched Class *id: class-name*—For example:

```
matched Class 1234: my_class
```

- For SIP parameter commands:

*parameter-command: descriptive-message*—For example:

strict-header-validation: Mandatory header field 'Via' is missing  
state-checking: Message CANCEL is not permitted to create a Dialog.

**Recommended Action** None.

## 608001

**Error Message** %PIX|ASA-6-608001: Pre-allocate Skinny *connection\_type* secondary channel for *interface\_name:IP\_address* to *interface\_name:IP\_address/port* from *string* message

**Explanation** This message indicates that the **inspect skinny** command preallocated a Skinny connection after inspecting a Skinny message. The *connection\_type* is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

**Recommended Action** None.

## 608002

**Error Message** %PIX|ASA-4-608002: Dropping Skinny message for *in\_ifc:src\_ip/src\_port* to *out\_ifc:dest\_ip/dest\_port*, SCCPPrefix length value too small

**Explanation** A Skinny (SSCP) message was received with an SCCP prefix length less than the minimum length configured.

*in\_ifc*—The input interface.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*out\_ifc*—The output interface.

*dest\_ip*—The destination IP address of the packet.

*dest\_port*—The destination port of the packet.

*value*—The SCCP prefix length of the packet.

**Recommended Action** If the SCCP message is valid, then customize the Skinny policy map to increase the minimum length value of the SSCP prefix.

## 608003

**Error Message** %PIX|ASA-4-608003: Dropping Skinny message for *in\_ifc:src\_ip/src\_port* to *out\_ifc:dest\_ip/dest\_port*, SCCPPrefix length *value* too large

**Explanation** A Skinny (SSCP) message was received with an SCCP prefix length greater than the maximum length configured.

*in\_ifc*—The input interface.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*out\_ifc*—The output interface.

*dest\_ip*—The destination IP address of the packet.

*dest\_port*—The destination port of the packet.

*value*—The SCCP prefix length of the packet.

**Recommended Action** If the SCCP message is valid, then customize the Skinny policy map to increase the maximum length value of the SCCP prefix.

## 608004

**Error Message** %PIX|ASA-4-608004: Dropping Skinny message for *in\_ifc:src\_ip/src\_port* to *out\_ifc:dest\_ip/dest\_port*, message id *value* not allowed

*in\_ifc*—The input interface.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*out\_ifc*—The output interface.

*dest\_ip*—The destination IP address of the packet.

*dest\_port*—The destination port of the packet.

*value*—The SCCP prefix length of the packet.

**Explanation** This SCCP message ID is not allowed.

**Recommended Action** If the SCCP messages should be allowed, then customize the Skinny policy map to allow them.

## 608005

**Error Message** %PIX|ASA-4-608005: Dropping Skinny message for *in\_ifc:src\_ip/src\_port* to *out\_ifc:dest\_ip/dest\_port*, message id value registration not complete

**Explanation** This SCCP message ID is not allowed because the endpoint did not complete registration.

*in\_ifc*—The input interface.

*src\_ip*—The source IP address of the packet.

*src\_port*—The source port of the packet.

*out\_ifc*—The output interface.

*dest\_ip*—The destination IP address of the packet.

*dest\_port*—The destination port of the packet.

*value*—The SCCP prefix length of the packet.

**Recommended Action** If the SCCP messages that are being dropped are valid, then customize the Skinny policy map to disable registration enforcement.

## 609001

**Error Message** %PIX|ASA-7-609001: Built local-host *interface\_name:IP\_address*

**Explanation** A network state container is reserved for host *IP\_address* connected to interface *interface\_name*. This is an informational message.

**Recommended Action** None.

## 609002

**Error Message** %PIX|ASA-7-609002: Teardown local-host *interface\_name:IP\_address* duration *time*

**Explanation** A network state container for host *IP\_address* connected to interface *interface\_name* is removed. This is an informational message.

**Recommended Action** None.

## 610001

**Error Message** %PIX|ASA-3-610001: NTP daemon interface *interface\_name*: Packet denied from *IP\_address*

**Explanation** An NTP packet was received from a host that does not match one of the configured NTP servers. The security appliance is only an NTP client; it is not a time server and does not respond to NTP requests.

**Recommended Action** None.

## 610002

**Error Message** %PIX|ASA-3-610002: NTP daemon interface *interface\_name*: Authentication failed for packet from *IP\_address*

**Explanation** The received NTP packet failed the authentication check.

**Recommended Action** Ensure that both the security appliance and the NTP server are set to use authentication, and the same key number and value.

## 610101

**Error Message** %PIX|ASA-6-610101: Authorization failed: Cmd: *command* Cmdtype: *command\_modifier*

**Explanation** Command authorization failed for the specified command. The *command\_modifier* is one of the following strings:

- **cmd** (this string means the command has no modifier)
- **clear**
- **no**
- **show**

**Explanation** If the security appliance encounters any other value other than the four command types listed, the message “unknown command type” is displayed.

**Recommended Action** None.

## 6108005

**Error Message** %ASA-6-6108005: *action\_class*: Received ESMTP *req\_resp* from *src\_ifc*:*sip*/*sport* to *dest\_ifc*:*dip*/*dport*; *further\_info*

**Explanation** This event is generated when a ESMTP classification is performed on a ESMTP message and the specified criteria is satisfied. The standalone log action occurs.

*action\_class* - The class of action: "ESMTP Classification" for ESMTP match commands; "ESMTP Parameter" for parameter commands.

*req\_resp*—"Request" or "Response".

*src\_ifc*—The source interface name.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

*further\_info*—One of the following:

- For a single match command: matched Class *id*: *match\_command*; for example, matched Class 1234: match body length 100.
- For parameter commands (commands under parameter section): *parameter-command*: *descriptive-message*; for example, mail-relay: Mail Relay not allowed.

**Recommended Action** None.

## 611101

**Error Message** %PIX|ASA-6-611101: User authentication succeeded: Uname: *user*

**Explanation** User authentication succeeded when accessing the security appliance succeeded.

**Recommended Action** None.

## 611102

**Error Message** %PIX|ASA-6-611102: User authentication failed: Uname: *user*

**Explanation** User authentication failed when attempting to access the security appliance.

**Recommended Action** None.

## 611103

**Error Message** %PIX|ASA-5-611103: User logged out: Uname: *user*

**Explanation** The specified user logged out.

**Recommended Action** None.

## 611104

**Error Message** %PIX|ASA-5-611104: Serial console idle timeout exceeded

**Explanation** The configured idle timeout for the security appliance serial console was exceeded because of no user activity.

**Recommended Action** None.

## 611301

**Error Message** %PIX|ASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: *mapped\_address*

**Explanation** The VPN client policy for client mode with no split tunneling was installed.

**Recommended Action** None.

## 611302

**Error Message** %PIX|ASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling

**Explanation** VPN client policy for network extension mode with no split tunneling was installed.

**Recommended Action** None.

## 611303

**Error Message** %PIX|ASA-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: *mapped\_address* Split Tunnel Networks: *IP\_address/netmask IP\_address/netmask ...*

**Explanation** VPN client policy for client mode with split tunneling was installed.

**Recommended Action** None.



## 611304

**Error Message** %PIX|ASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: *IP\_address/netmask IP\_address/netmask ...*

**Explanation** VPN client policy for network extension mode with split tunneling was installed.

**Recommended Action** None.

## 611305

**Error Message** %PIX|ASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: *IP\_address* Secondary DNS: *IP\_address* Primary WINS: *IP\_address* Secondary WINS: *IP\_address*

**Explanation** VPN client policy for DHCP was installed.

**Recommended Action** None.

## 611306

**Error Message** %PIX|ASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed

**Explanation** Perfect forward secrecy was configured as part of the VPN client download policy.

**Recommended Action** None.

## 611307

**Error Message** %PIX|ASA-6-611307: VPNClient: Head end : *IP\_address*

**Explanation** The VPN client is connected to the specified headend.

**Recommended Action** None.

## 611308

**Error Message** %PIX|ASA-6-611308: VPNClient: Split DNS Policy installed: List of domains: *string string ...*

**Explanation** A split DNS policy was installed as part of the VPN client downloaded policy.

**Recommended Action** None.

## 611309

**Error Message** %PIX|ASA-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: *IP\_address*

**Explanation** A VPN client is disconnecting and uninstalling a previously installed policy.

**Recommended Action** None.

## 611310

**Error Message** %PIX|ASA-6-611310: VNPClient: XAUTH Succeeded: Peer: *IP\_address*

**Explanation** The VPN client Xauth succeeded with the specified headend.

**Recommended Action** None.

## 611311

**Error Message** %PIX|ASA-6-611311: VNPClient: XAUTH Failed: Peer: *IP\_address*

**Explanation** The VPN client Xauth failed with the specified headend.

**Recommended Action** None.

## 611312

**Error Message** %PIX|ASA-6-611312: VPNClient: Backup Server List: *reason*

**Explanation** When the security appliance is an Easy VPN remote device, this message indicates that the Easy VPN server downloaded a list of backup servers to the security appliance. This list overrides any backup servers you configured locally. If the downloaded list is empty, then the security appliance uses no backup servers. The *reason* is one of the following messages:

- A list of backup server IP addresses
- Received NULL list. Deleting current backup servers.

**Recommended Action** None.

## 611313

**Error Message** %PIX|ASA-3-611313: VPNClient: Backup Server List Error: *reason*

**Explanation** When the security appliance is an Easy VPN remote device, and the Easy VPN server downloads a backup server list to the security appliance, this message indicates that the list contains an invalid IP address or a hostname. The security appliance does not support DNS, and therefore does not support hostnames for servers unless you manually map a name to an IP address using the **name** command.

**Recommended Action** On the Easy VPN server, make sure that the server IP addresses are correct, and configure the servers as IP addresses instead of hostnames. If you must use hostnames on the server, use the **name** command on the Easy VPN remote device to map the IP addresses to names.

## 611314

**Error Message** %PIX|ASA-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: *IP\_address* has redirected the to server *IP\_address*

**Explanation** When the security appliance is an Easy VPN remote device, the master server of the load balancing cluster redirected the security appliance to connect to a particular server.

**Recommended Action** None.

## 611315

**Error Message** %PIX|ASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member *IP\_address*

**Explanation** When the security appliance is an Easy VPN remote device, this message indicates that it disconnected from a load balancing cluster server.

**Recommended Action** None.

## 611316

**Error Message** %PIX|ASA-6-611316: VPNClient: Secure Unit Authentication Enabled

**Explanation** When the security appliance is an Easy VPN remote device, the downloaded VPN policy enabled Secure Unit Authentication (SUA).

**Recommended Action** None.

## 611317

**Error Message** %PIX|ASA-6-611317: VPNClient: Secure Unit Authentication Disabled

**Explanation** When the security appliance is an Easy VPN remote device, the downloaded VPN policy disabled Secure Unit Authentication (SUA).

**Recommended Action** None.

## 611318

**Error Message** %PIX|ASA-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: *IP\_address* Auth Server Port: *port* Idle Timeout: *time*

**Explanation** When the security appliance is an Easy VPN remote device, the downloaded VPN policy enabled Individual User Authentication (IUA) for users on the security appliance inside network.

*IP\_address*—The server IP address to which the security appliance sends authentication requests.

*port*—The server port to which the security appliance sends authentication requests.

*time*—The idle timeout value for authentication credentials.

**Recommended Action** None.

## 611319

**Error Message** %PIX|ASA-6-611319: VPNClient: User Authentication Disabled

**Explanation** When the security appliance is an Easy VPN remote device, the downloaded VPN policy disabled Individual User Authentication (IUA) for users on the security appliance inside network.

**Recommended Action** None.

## 611320

**Error Message** %PIX|ASA-6-611320: VPNClient: Device Pass Thru Enabled

**Explanation** When the security appliance is an Easy VPN remote device, the downloaded VPN policy enabled device pass through. The device pass through feature allows devices that cannot perform authentication (such as an IP phone) to be exempt from authentication when Individual User Authentication (IUA) is enabled.

**Recommended Action** None. If the Easy VPN server enables this feature, you can specify the devices that should be exempt from authentication (IUA) using the **vpnclient mac-exempt** command on the security appliance.

## 611321

**Error Message** %PIX|ASA-6-611321: VPNClient: Device Pass Thru Disabled

**Explanation** When the security appliance is an Easy VPN remote device, the downloaded VPN policy disabled device pass through.

**Recommended Action** None.

## 611322

**Error Message** %PIX|ASA-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled

**Explanation** When the security appliance is an Easy VPN remote device and the downloaded VPN policy disabled secure unit authentication (SUA), the Easy VPN server uses two-factor/SecurID/cryptocard-based authentication mechanisms to authenticate the security appliance using XAUTH.

**Recommended Action** If you want the Easy VPN remote device to be authenticated using two-factor/SecureID/cryptocard-based authentication mechanisms, enable SUA on the server.

## 611323

**Error Message** %PIX|ASA-6-611323: VPNClient: Duplicate split nw entry

**Explanation** When the security appliance is an Easy VPN remote device, this message indicates that the downloaded VPN policy contains duplicate split network entries. An entry is considered a duplicate if it matches both the network address and the network mask.

**Recommended Action** Remove duplicate split network entries from the VPN policy on the Easy VPN server.

## 612001

**Error Message** %PIX|ASA-5-612001: Auto Update succeeded:*filename*, version:*number*

**Explanation** An update from an Auto Update server was successful. The *filename* variable is **image**, **ASDM file**, or **configuration**. The **version number** variable is the version number of the update.

**Recommended Action** None.

## 612002

**Error Message** %PIX|ASA-4-612002: Auto Update failed:*filename*, version:*number*, reason:*reason*

**Explanation** This message indicates that an update from an Auto Update server failed. The *filename* variable is **image**, **ASDM file**, or **configuration**. The **version number** variable is the version number of the update. The *reason* variable describes why the update failed. Possible reasons for the failure include invalid image file, connection lost to server, configuration errors, etc.

**Recommended Action** Check the configuration of the Auto Update server.

## 612003

**Error Message** %PIX|ASA-4-612003:Auto Update failed to contact:*url*, reason:*reason*

**Explanation** This indicates that the Auto Update daemon was unable to contact the specified URL *url*. This could be the URL of the Auto Update server or one of the file server URLs returned by the Auto Update server. The *reason* field describes why the contact failed. Possible reasons for the failure include no response from server, authentication failed, file not found, etc.

**Recommended Action** Check the configuration of the Auto Update server.

## 613001

**Error Message** %PIX|ASA-6-613001: Checksum Failure in database in area *string* Link State Id *IP\_address* Old Checksum *number* New Checksum *number*

**Explanation** OSPF has detected a checksum error in the database due to memory corruption.

**Recommended Action** Restart the OSPF process.

## 613002

**Error Message** %PIX|ASA-6-613002: interface *interface\_name* has zero bandwidth

**Explanation** The interface reports its bandwidth as zero.

**Recommended Action** To determine what is causing this problem, contact the Cisco TAC for assistance.

## 613003

**Error Message** %PIX|ASA-6-613003: *IP\_address netmask* changed from area *string* to area *string*

**Explanation** An OSPF configuration change has caused a network range to change areas.

**Recommended Action** Reconfigure OSPF with the correct network range.

## 614001

**Error Message** %PIX|ASA-6-614001: Split DNS: request patched from server: *IP\_address* to server: *IP\_address*

**Explanation** Split DNS is redirecting DNS queries from the original destination server to the primary enterprise DNS server.

**Recommended Action** None.

## 614002

**Error Message** %PIX|ASA-6-614002: Split DNS: reply from server:*IP\_address* reverse patched back to original server:*IP\_address*

**Explanation** Split DNS is redirecting DNS queries from the enterprise DNS server to the original destination server.

**Recommended Action** None.

## 615001

**Error Message** %PIX|ASA-6-615001: vlan number not available for firewall interface

**Explanation** The switch removed the VLAN from the FWSM.

**Recommended Action** This is an informational message.

## 615002

**Error Message** %PIX|ASA-6-615002: vlan number available for firewall interface

**Explanation** The switch added the VLAN to the FWSM.

**Recommended Action** This is an informational message.

## 616001

**Error Message** %PIX|ASA-6-616001:Pre-allocate MGCP *data\_channel* connection for *inside\_interface:inside\_address* to *outside\_interface:outside\_address/port* from *message\_type message*

**Explanation** An MGCP data channel connection, RTP, or RTCP is preallocated. The message text also specifies which message has triggered the connection preallocation.

**Recommended Action** None.

## 617001

**Error Message** %PIX|ASA-6-617001: GTPv *version msg\_type* from *source\_interface:source\_address/source\_port* not accepted by *source\_interface:dest\_address/dest\_port*

**Explanation** This message appears when a request was not accepted by the peer. This is usually seen with a Create PDP Context request.

**Recommended Action** None.



## 617002

**Error Message** %PIX|ASA-6-617002: Removing v1 PDP Context with TID *tid* from GGSN *IP\_address* and SGSN *IP\_address*, Reason: *reason* or Removing v1 *primary|secondary* PDP Context with TID *tid* from GGSN *IP\_address* and SGSN *IP\_address*, Reason: *reason*

**Explanation** This message appears when a PDP context is removed from the database either because it expired, a Delete PDP Context Request/Response was exchanged, or a user removed it using the CLI.

**Recommended Action** None.

## 617003

**Error Message** %PIX|ASA-6-617003: GTP Tunnel created from *source\_interface:source\_address/source\_port* to *source\_interface:dest\_address/dest\_port*

**Explanation** This message appears when a GTP tunnel was created after receiving a Create PDP Context Response that accepted the request.

**Recommended Action** None.

## 617004

**Error Message** %PIX|ASA-6-617004: GTP connection created for response from *source\_interface:source\_address/0* to *source\_interface:dest\_address/dest\_port*

**Explanation** This message appears when the SGSN or GGSN signaling address in the Create PDP Context Request or Response, respectively, is different than the SGSN/GGSN sending it.

**Recommended Action** None.

## 617100

**Error Message** PIX|ASA-6-617100: Teardown *num\_conns* connection(s) for user *user\_ip*

**Explanation** The connections for this user were torn down because either a RADIUS accounting stop or RADIUS accounting start was received, which contains attributes configured in the policy-map for a match. The attributes did not match those stored for the user entry, if the user entry exists.

*num\_conns*—The number of connections torn down.

*user\_ip*—The IP address (framed IP attribute) of the user.

**Recommended Action** None.

## 620001

**Error Message** %PIX|ASA-6-620001: Pre-allocate CTIQBE {RTP | RTCP} secondary channel for *interface\_name:outside\_address[/outside\_port]* to *interface\_name:inside\_address[/inside\_port]* from *CTIQBE\_message\_name message*

**Explanation** The security appliance pre-allocates a connection object for the specified CTIQBE media traffic. This message is rate limited to one message every 10 seconds.

**Recommended Action** None.

## 620002

**Error Message** %PIX|ASA-4-620002: Unsupported CTIQBE version: *hex*: from *interface\_name:IP\_address/port* to *interface\_name:IP\_address/port*

**Explanation** The security appliance received a CTIQBE message with an unsupported version number. The security appliance drops the packet. This message is rate limited to one message every 10 seconds.

**Recommended Action** If the version number captured in the log message is unreasonably large (greater than 10), the packet could be malformed, a non-CTIQBE packet, or corrupted before it arrives at the security appliance. We recommend that you determine the source of the packets. If the version number is reasonably small (less than or equal to 10), then contact the Cisco TAC to see if a new security appliance image that supports this CTIQBE version is available.

## 621001

**Error Message** %PIX|ASA-6-621001: Interface *interface\_name* does not support multicast, not enabled

**Explanation** This message appears when an attempt was made to enable PIM on an interface that does not support multicast

**Recommended Action** Copy this error message and submit it, the configuration, and any details about the events leading up to this error to Cisco TAC.

## 621002

**Error Message** %PIX|ASA-6-621002: Interface *interface\_name* does not support multicast, not enabled

**Explanation** This message appears when an attempt was made to enable igmp on an interface that doesn't support multicast.

**Recommended Action** Copy this error message and submit it, the configuration, and any details about the events leading up to this error to Cisco TAC.

## 621003

**Error Message** %PIX|ASA-6-621003: The event queue size has exceeded *number*

**Explanation** This message appears when the number of event managers created has exceeded the expected amount.

**Recommended Action** Copy this error message and submit it, the configuration, and any details about the events leading up to this error to the Cisco TAC.

## 621006

**Error Message** %PIX|ASA-6-621006: Mrib disconnected, (*IP\_address,IP\_address*) event cancelled

**Explanation** This message appears when a packet triggering a data-driven event was received but the connection to the MRIB was down. The notification was cancelled.

**Recommended Action** If this message persists after the system is up, copy the error message and submit it, the configuration and any details about the events leading up to this error to the TAC.

## 621007

**Error Message** %PIX|ASA-6-621007: Bad register from *interface\_name:IP\_address* to *IP\_address* for (*IP\_address, IP\_address*)

**Explanation** This message appears when a PIM router configured as a rendezvous point or with network address translation (NAT) has received a PIM register packet from another PIM router. The data encapsulated in this packet is invalid.

**Recommended Action** It is likely that the sending router is erroneously sending non-RFC registers . Upgrade the sending router.

## 621008

**Error Message** %PIX-6-621008 AutoRP: discard *string* on interface *interface-name* from *address* due to incorrect version.

**Explanation** Received an AutoRP packet with incorrect version.

**Recommended Action** None.

## 621009

**Error Message** %PIX-6-621009 AutoRP: discard *string* on interface *interface-name* from *address* due to incorrect *type number*

**Explanation** An AutoRP packet was received with an incorrect AutoRP type.

**Recommended Action** None.

## 621010

**Error Message** %PIX-6-621010 AutoRP: discard *string* on interface *interface-name* from *address* due to zero RP count

**Explanation** An AutoRP packet was received with no RP mappings. Or because of the multicast boundary, all RP mappings were removed.

**Recommended Action** Adjust the boundary access rules or RP mappings.

## 622001

**Error Message** %PIX|ASA-6-622001: *string* tracked route *network mask address*, distance *number*, table *string*, on interface *interface-name*

**Explanation** A tracked route has been added to or removed from a routing table, which means that the state of the tracked object has changed from up or down.

*string*—"Adding" or "Removing."

*network*—The network address.

*mask*—The network mask.

*address*—The gateway address.

*number*—The route administrative distance.

*string*—The routing table name.

*interface-name*—The interface name as specified by the **nameif** command.

**Recommended Action** None. This is an informational message that indicates a change in routing and a likely change in forwarding paths, as configured by the tracking and SLA commands.

## 622101

**Error Message** %PIX|ASA-6-622101: Starting regex table compilation for *match\_command*; table entries = *regex\_num* entries

**Explanation** Provides information on the background activities of regex compilation.

*match\_command*—The match command to which the regex table is associated.

*regex\_num*—The number of regex entries to be compiled.

**Recommended Action** None.

## 622102

**Error Message** %PIX|ASA-6-622102: Completed regex table compilation for *match\_command*; table size = *num* bytes

**Explanation** Provides information on the background activities of the regex compilation.

*match\_command*—The match command to which the regex table is associated.

*num*—The size, in bytes, of the compiled table.

**Recommended Action** None.

## Messages 701001 to 726001

This section contains messages from 701001 to 726001.

Most of the ISAKMP syslogs have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a system log message when available. If the object is not known at the time the system log message is generated, the specific "*heading = value*" combination will not be displayed.

The objects will be prepended as follows:

"Group = *groupname*, Username = *user*, IP = *IP\_address*, ..."

Where the Group identifies the tunnel-group, the username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or L2L peer.

## 701001

**Error Message** %PIX|ASA-7-701001: alloc\_user() out of Tcp\_user objects

**Explanation** This is an AAA message. This message is displayed if the user authentication rate is too high for the module to handle new AAA requests.

**Recommended Action** Enable Flood Defender with the **floodguard enable** command.

## 701002

**Error Message** %PIX|ASA-7-701002: alloc\_user() out of Tcp\_proxy objects

**Explanation** This is a AAA message. This message is displayed if the user authentication rate is too high for the module to handle new AAA requests.

**Error Message** Enable Flood Defender with the **floodguard enable** command.

## 702201

**Error Message** %PIX|ASA-7-702201: ISAKMP Phase 1 delete received (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** An ISAKMP delete message has been received.

**Recommended Action** None.

## 702202

**Error Message** %PIX|ASA-7-702202: ISAKMP Phase 1 delete sent (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** An ISAKMP delete message has been sent.

**Recommended Action** None.

## 702203

**Error Message** %PIX|ASA-7-702203: ISAKMP DPD timed out (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** Remote peer is not responding, DPD has timed out the peer.

**Recommended Action** Check network connectivity to remote host.

## 702204

**Error Message** %PIX|ASA-7-702204: ISAKMP Phase 1 retransmission (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** Remote peer is not responding, ISAKMP is retransmitting the previous packet.

**Recommended Action** Check network connectivity to remote host, check VPN configuration of local and remote devices.

## 702205

**Error Message** %PIX|ASA-7-702205: ISAKMP Phase 2 retransmission (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** Remote peer is not responding, ISAKMP is retransmitting the previous packet.

**Recommended Action** Check network connectivity to remote host, check VPN configuration of local and remote devices.

## 702206

**Error Message** %PIX|ASA-7-702206: ISAKMP malformed payload received (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** ISAKMP received an illegal or malformed message. May indicate an out of sync problem with the remote peer, a problem decrypting a message, or a message received out of order.

**Recommended Action** If using preshared key, verify local preshared key is configured correctly on local and remote device. Check local and remote configuration, additional troubleshooting may be required if SA fails to come up.

## 702207

**Error Message** %PIX|ASA-7-702207: ISAKMP duplicate packet detected (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** ISAKMP received a duplicate of the previously received packet. May occur during normal operation, or as a side effect of previous errors in an ISAKMP exchange.

**Recommended Action** Check connectivity, check local and remote configuration.

## 702208

**Error Message** %PIX|ASA-7-702208: ISAKMP Phase 1 exchange started (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** ISAKMP has started a new Phase 1 message exchange with the remote peer.

**Recommended Action** None.

## 702209

**Error Message** %PIX|ASA-7-702209: ISAKMP Phase 2 exchange started (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** ISAKMP has started a new Phase 2 message exchange with the remote peer.

**Recommended Action** None.

## 702210

**Error Message** %PIX|ASA-7-702210: ISAKMP Phase 1 exchange completed(local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** ISAKMP has finished a Phase 1 exchange.

**Recommended Action** None.



## 702211

**Error Message** %PIX|ASA-7-702211: ISAKMP Phase 2 exchange completed(local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** ISAKMP has finished a Phase 2 exchange.

**Recommended Action** None.

## 702212

**Error Message** %PIX|ASA-7-702212: ISAKMP Phase 1 initiating rekey (local *IP\_address* (initiator|responder), remote *IP\_address*)

**Explanation** ISAKMP is initiating Phase 1 rekeying.

**Recommended Action** None.

## 702305

**Error Message** %PIX|ASA-3-702305: IPSEC: An *direction tunnel\_type* SA (SPI=*spi*) between *local\_IP* and *remote\_IP* (*username*) is rekeying due to sequence number rollover.

**Explanation** This message is displayed when more than 4 billion packets have been received in the IPsec tunnel and a new tunnel is being negotiated.

*direction*—SA direction (inbound or outbound)

*tunnel\_type*—SA type (remote access or L2L)

*spi*—IPsec Security Parameters Index

*local\_IP*—IP address of the tunnel local endpoint

*remote\_IP*—IP address of the tunnel remote endpoint

*username*—Username associated with the IPsec tunnel

**Recommended Action** Contact the peer administrator to compare the SA lifetime setting.

## 702307

**Error Message** %PIX|ASA-3-702307: IPSEC: An *direction tunnel\_type* SA (SPI=*spi*) between *local\_IP* and *remote\_IP* (*username*) is rekeying due to data rollover.

*direction*—SA direction (inbound or outbound)

*tunnel\_type*—SA type (remote access or L2L)

*spi*—IPsec Security Parameters Index

*local\_IP*—IP address of the tunnel local endpoint  
*remote\_IP*—IP address of the tunnel remote endpoint  
*username*—Username associated with the IPSec tunnel

**Explanation** This message is displayed when an SA data life span expires. This message indicates that an IPSec SA is rekeying as a result of the amount of data transmitted with that SA. This information is useful for debugging rekey issues.

**Recommended Action** None.

## 703001

**Error Message** %PIX|ASA-7-703001: H.225 message received from *interface\_name:IP\_address/port* to *interface\_name:IP\_address/port* is using an unsupported *version number*

**Explanation** The security appliance received an H.323 packet with an unsupported version number. The security appliance might re-encode the protocol version field of the packet to the highest supported version.

**Recommended Action** Use the version of H.323 that the security appliance supports in the VoIP network.

## 703002

**Error Message** %PIX|ASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for *interface\_name:IP\_address* to *interface\_name:IP\_address/port*

**Explanation** This is debugging message indicates that the security appliance received the specified H.225 message, and that the security appliance opened a new signaling connection object for the two specified H.323 endpoints.

**Recommended Action** None.

## 709001, 709002

**Error Message** %PIX|ASA-7-709001: FO replication failed: cmd=*command* returned=*code*

**Error Message** %PIX|ASA-7-709002: FO unreplicable: cmd=*command*

**Explanation** These failover messages only appear during the development debug testing phase.

**Recommended Action** None.

## 709003

**Error Message** %PIX|ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.

**Explanation** This is a failover message. This message is displayed when the active unit starts replicating its configuration to the standby unit. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 709004

**Error Message** %PIX|ASA-1-709004: (Primary) End Configuration Replication (ACT)

**Explanation** This is a failover message. This message is displayed when the active unit completes replicating its configuration on the standby unit. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 709005

**Error Message** %PIX|ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.

**Explanation** This message indicates that the standby the security appliance received the first part of the configuration replication from the active the security appliance. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 709006

**Error Message** %PIX|ASA-1-709006: (Primary) End Configuration Replication (STB)

**Explanation** This is a failover message. This message is displayed when the standby unit completes replicating a configuration sent by the active unit. (Primary) can also be listed as (Secondary) for the secondary unit.

**Recommended Action** None.

## 709007

**Error Message** %PIX|ASA-2-709007: Configuration replication failed for command *command*

**Explanation** This is a failover message. This message is displayed when the standby unit is unable to complete replicating a configuration sent by the active unit. The command that caused the failure displays at the end of the message.

**Recommended Action** Write down the command name and inform Cisco TAC.

## 710001

**Error Message** %PIX|ASA-7-710001: TCP access requested from *source\_address/source\_port* to *interface\_name:dest\_address/service*

**Explanation** This message appears when the first TCP packet destined to the security appliance requests to establish a TCP session. This packet is the first SYN packet of the three-way handshake. This message appears when the respective access control list (telnet, http or ssh) has permitted the packet. However, the SYN cookie verification is not yet completed and no state is reserved.

**Recommended Action** None.

## 710002

**Error Message** %PIX|ASA-7-710002: {TCP|UDP} access permitted from *source\_address/source\_port* to *interface\_name:dest\_address/service*

**Explanation** For a TCP connection, this message appears when the second TCP packet destined to the security appliance requests to establish a TCP session. This packet is the final ACK of the three-way handshake. This message appears when the respective access control list (Telnet, HTTP, or SSH) has permitted the packet. Also, the SYN cookie verification is successful and the state is reserved for the TCP session.

For a UDP connection, the connection was permitted. For example, this message appears (with the service snmp) when the module receives an SNMP request from an authorized SNMP management station, and the request has been processed. This message is rate limited to one message every 10 seconds..

**Recommended Action** None.

## 710003

**Error Message** %PIX-3-710003: {TCP|UDP} access denied by ACL from *source\_IP/source\_port* to *interface\_name:dest\_IP/service*

The following is an example:

```
%PIX-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to outside:95.1.1.13/1005
```

**Explanation** This message is displayed when the security appliance denies an attempt to connect to the interface service. For example, this message may occur when the firewall receives an SNMP request from an unauthorized SNMP management station.

**Recommended Action** Use the **show run http**, **show run ssh**, or **show run telnet** commands to verify that the security appliance is configured to permit the service access from the host or network. If this message appears frequently, it can indicate an attack.

## 710004

**Error Message** %PIX|ASA-7-710004: TCP connection limit exceeded from *source\_address/source\_port* to *interface\_name:dest\_address/service*

**Explanation** The maximum number of security appliance management connections for the service was exceeded. The security appliance permits at most five concurrent management connections per management service.

**Recommended Action** From the console, use the **kill** command to release the unwanted session.

## 710005

**Error Message** %PIX|ASA-7-710005: {TCP|UDP} request discarded from *source\_address/source\_port* to *interface\_name:dest\_address/service*

**Explanation** This message appears when the security appliance does not have a UDP server that services the UDP request. The message can also indicate a TCP packet that does not belong to any session on the security appliance. In addition, this message appears (with the service **snmp**) when the security appliance receives an SNMP request with an empty payload, even if it is from an authorized host. When the service is **snmp**, this message occurs a maximum of 1 time every 10 seconds so that the log receiver is not overwhelmed.

**Recommended Action** In networks that heavily utilize broadcasting services such as DHCP, RIP or NetBios, the frequency of this message can be high. If this message appears in excessive number, it may indicate an attack.

## 710006

**Error Message** %PIX|ASA-7-710006: *protocol* request discarded from *source\_address* to *interface\_name:dest\_address*

**Explanation** This message appears when the security appliance does not have an IP server that services the IP protocol request; for example, the security appliance receives IP packets that are not TCP or UDP, and the security appliance cannot service the request.

**Recommended Action** In networks that heavily utilize broadcasting services such as DHCP, RIP or NetBios, the frequency of this message can be high. If this message appears in excessive numbers, it may indicate an attack.

## 711001

**Error Message** %PIX|ASA-7-711001: *debug\_trace\_msg*

**Explanation** This system log message appears after you enter the logging debug-trace command for the logging feature. When logging debug-trace is enabled, all debug messages will be redirected to the system log message for processing. For security reasons, the system log message output must be encrypted or sent over a secure out-of-band network.

**Recommended Action** None.

## 711002

**Error Message** PIX/ASA-7-711002: Task ran for *elapsed\_time* msec, process = *process\_name*, PC = *PC* Tracebeback = *traceback*

**Explanation** This message appears when a process uses the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

*PC*—Instruction pointer of the CPU hogging process.

*traceback*—Stack trace of the CPU hogging process, which can include up to 12 addresses.

**Recommended Action** None.

## 713004

**Error Message** %PIX|ASA-3-713004: *device* scheduled for reboot or shutdown, IKE key acquire message on interface *interface num*, for Peer *IP\_address* ignored

**Explanation** This message appears when the security appliance has received an IKE packet from a remote entity trying to initiate a tunnel. Since the security appliance is scheduled for a reboot or shutdown, it does not allow any more tunnels to be established. The IKE packet is ignored and dropped.

**Explanation** None.

## 713006

**Error Message** %PIX|ASA-5-713006: Failed to obtain state for message Id *message\_number*, Peer Address: *IP\_address*

**Explanation** This message indicates that the security appliance does not know about the received message ID. The message ID is used to identify a specific IKE Phase 2 negotiation. This is most likely an error condition on the security appliance but may indicate that the two IKE peers are out of synchronization.

**Recommended Action** None.

## 713008

**Error Message** %PIX|ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel

**Explanation** This message indicates that a key ID value was received in the ID payload which was longer than the maximum allowed size of a groupname for this IKE session using preshared keys authentication. This is an invalid value and the session is rejected. Note that the key ID specified would never work because a groupname of that size cannot be created in the security appliance. Notify the user to change the incorrect groupname on the client.

**Recommended Action** Make sure that the client peer (most likely an Altiga RA Client) specifies a valid groupname. The current maximum length for a groupname is 32.

## 713009

**Error Message** %PIX|ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel

**Explanation** This message indicates that an OU value in the DN was received in the ID payload which was longer than the maximum allowed size of a groupname for this IKE session using Certs authentication. This OU is skipped and another OU or other criteria may find a matching group.

**Recommended Action** For the client to be able to use an OU to find a group in the security appliance, the groupname must be a valid length. The current maximum length of a groupname is 32.

## 713010

**Error Message** %PIX|ASA-5-713010: *IKE area: failed to find centry for message Id message\_number*

**Explanation** This message appears when an attempt is made to locate a conn\_entry (IKE phase 2 struct that corresponds to an IPSec SA) by the unique Message ID failed. The internal structure was not found. This can occur if a session is terminated in a non-standard way, but it is more likely that it indicates an internal error.

**Recommended Action** If this problem persists, investigate the peer.

## 713012

**Error Message** %PIX|ASA-3-713012: Unknown protocol (*protocol*). Not adding SA w/spi=*SPI value*

**Explanation** This message appears when an illegal or unsupported IPSec protocol has been received from the peer.

**Recommended Action** Check the ISAKMP Phase 2 configuration on peer(s) to make sure it is compatible with the security appliance.

## 713014

**Error Message** %PIX|ASA-3-713014: Unknown Domain of Interpretation (DOI): *DOI value*

**Explanation** This message appears when the ISAKMP Domain of Interpretation received from the peer is unsupported.

**Recommended Action** Check the ISAKMP DOI configuration on peer(s).

## 713016

**Error Message** %PIX|ASA-3-713016: Unknown identification type, Phase 1 or 2, Type *ID\_Type*

**Explanation** This message indicates that the ID received from the peer is unknown. The ID could be an unfamiliar valid ID or an invalid or corrupted ID.

**Recommended Action** Check the configuration on headend and peer(s).



## 713017

**Error Message** %PIX|ASA-3-713017: Identification type not supported, Phase 1 or 2,  
Type *ID\_Type*

**Explanation** This message indicates that the Phase 1 or Phase 2 ID received from the peer is legal but not supported.

**Recommended Action** Check the configuration on the headend and peer(s).

## 713018

**Error Message** %PIX|ASA-3-713018: Unknown ID type during find of group name for certs,  
Type *ID\_Type*

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 713020

**Error Message** %PIX|ASA-3-713020: No Group found by matching OU(s) from ID payload:  
*OU\_value*

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 713022

**Error Message** %PIX|ASA-3-713022: No Group found matching *peer\_ID* or *IP\_address* for  
Pre-shared key peer *IP\_address*

**Explanation** This message indicates that there was no group in the group database with the same name as the value (key ID or IP address) specified by the peer.

**Recommended Action** Verify the configuration on the peer.

## 713024

**Error Message** %PIX|ASA-7-713024: Received local Proxy Host data in ID Payload:  
Address *IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has received the remote peer's Phase 2 local proxy ID payload.

**Recommended Action** None.

## 713025

**Error Message** %PIX|ASA-7-713025: Received remote Proxy Host data in ID Payload:  
Address *IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has received the remote peer's Phase 2 remote proxy ID payload.

**Recommended Action** None.

## 713026

**Error Message** %PIX|ASA-7-713026: Transmitted local Proxy Host data in ID Payload:  
Address *IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has transmitted the Phase 2 local proxy ID payload.

**Recommended Action** None.

## 713027

**Error Message** %PIX|ASA-7-713027: Transmitted remote Proxy Host data in ID Payload:  
Address *IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has transmitted the Phase 2 remote proxy ID payload.

**Recommended Action** None.

## 713028

**Error Message** %PIX|ASA-7-713028: Received local Proxy Range data in ID Payload:  
Addresses *IP\_address - IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has received the remote peer's Phase 2 local proxy ID payload and it contained an IP address range.

**Recommended Action** None.

## 713029

**Error Message** %PIX|ASA-7-713029: Received remote Proxy Range data in ID Payload:  
Addresses *IP\_address - IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has received the remote peer's Phase 2 remote proxy ID payload and it contained an IP address range.

**Recommended Action** None.

## 713030

**Error Message** %PIX|ASA-7-713030: Transmitted local Proxy Range data in ID Payload:  
Addresses *IP\_address - IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has transmitted the Phase 2 local proxy ID payload.

**Recommended Action** None.

## 713031

**Error Message** %PIX|ASA-7-713031: Transmitted remote Proxy Range data in ID Payload:  
Addresses *IP\_address - IP\_address*, Protocol *protocol*, Port *port*

**Explanation** This message indicates that the security appliance has transmitted the Phase 2 remote proxy ID payload.

**Recommended Action** None.

## 713032

**Error Message** %PIX|ASA-3-713032: Received invalid local Proxy Range *IP\_address* - *IP\_address*

**Explanation** This message appears when the local ID payload contained the range ID type and the specified low address was not less than the high address. This may indicate a configuration problem.

**Recommended Action** Check the configuration of ISAKMP Phase 2 parameters.

## 713033

**Error Message** %PIX|ASA-3-713033: Received invalid remote Proxy Range *IP\_address* - *IP\_address*

**Explanation** This message appears when the remote ID payload contained the range ID type and the specified low address was not less than the high address. This may indicate a configuration problem.

**Recommended Action** Check the configuration of ISAKMP Phase 2 parameters.

## 713034

**Error Message** %PIX|ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address *IP\_address*, Mask *netmask*, Protocol *protocol*, Port *port*

**Explanation** This message appears when the local IP Proxy Subnet data has been received in the Phase 2 ID Payload.

**Recommended Action** None.

## 713035

**Error Message** %PIX|ASA-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address *IP\_address*, Mask *netmask*, Protocol *protocol*, Port *port*

**Explanation** This message appears when the remote IP Proxy Subnet data has been received in the Phase 2 ID Payload.

**Recommended Action** None.

## 713036

**Error Message** %PIX|ASA-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address *IP\_address*, Mask *netmask*, Protocol *protocol*, Port *port*

**Explanation** This message appears when the local IP Proxy Subnet data in has been transferred in the Phase 2 ID Payload.

**Recommended Action** None.

## 713037

**Error Message** %PIX|ASA-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address *IP\_address*, Mask *netmask*, Protocol *protocol*, Port *port*

**Explanation** This message appears when the remote IP Proxy Subnet data has been transferred in the Phase 2 ID Payload.

**Recommended Action** None.

## 713039

**Error Message** %PIX|ASA-7-713039: Send failure: Bytes (*number*), Peer: *IP\_address*

**Explanation** This message appears when an internal software error has occurred and the ISAKMP packet could not be transmitted.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713040

**Error Message** %PIX|ASA-7-713040: Could not find connection entry and can not encrypt: msgid *message\_number*

**Explanation** This message indicates that an internal software error has occurred and a Phase 2 data structure could not be found.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713041

**Error Message** %PIX|ASA-5-713041: IKE Initiator: *new or rekey* Phase 1 or 2, Intf *interface\_number*, IKE Peer *IP\_address* local Proxy Address *IP\_address*, remote Proxy Address *IP\_address*, Crypto map (*crypto map tag*)

**Explanation** This message indicates that the security appliance is negotiating a tunnel as the initiator.

**Recommended Action** None.

## 713042

**Error Message** %PIX|ASA-3-713042: IKE Initiator unable to find policy: Intf *interface\_number*, Src: *source\_address*, Dst: *dest\_address*

**Explanation** This message indicates that the IPsec fast path processed a packet that triggered IKE, but IKE's policy lookup failed. This error could be timing related. The ACLs that triggered IKE might have been deleted before IKE processed the initiation request. This problem will most likely correct itself.

**Explanation** If the condition persists, check the L2L configuration, paying special attention to the ACLs associated with crypto maps.

## 713043

**Error Message** %PIX|ASA-3-713043: Cookie/peer address *IP\_address* session already in progress

**Explanation** This message indicates that IKE has been triggered again while the original tunnel is in progress.

**Recommended Action** None.

## 713047

**Error Message** %PIX|ASA-3-713047: Unsupported Oakley group: Group *Diffie-Hellman group*

**Explanation** This message indicates that the security appliance does not support the Diffie-Hellman group proposed by the remote peer. The Diffie-Hellman group is used during Phase 1 to generate the Diffie-Hellman keys, and during Phase 2 to generate the Diffie-Hellman keys for Perfect Forward Secrecy (PFS).

**Explanation** Check the configuration of the Diffie-Hellman keys on the peer. Also check for correct proposals on the security appliance.

## 713048

**Error Message** %PIX|ASA-3-713048: Error processing payload: Payload ID: *id*

**Explanation** This message indicates that a packet has been received with a payload we could not process.

**Recommended Action** If this problem persists, there might be a misconfiguration on the peer.

## 713049

**Error Message** %PIX|ASA-5-713049: Security negotiation complete for *tunnel\_type* type (*group\_name*) *Initiator/Responder*, Inbound SPI = *SPI*, Outbound SPI = *SPI*

**Explanation** This message indicates the start of an IPsec tunnel.

**Recommended Action** None.

## 713050

**Error Message** %PIX|ASA-5-713050: Connection terminated for peer *IP\_address*. Reason: *termination reason* Remote Proxy *IP\_address*, Local Proxy *IP\_address*

**Explanation** This message indicates the termination of an IPsec tunnel.

**Recommended Action** None.

## 713051

**Error Message** %PIX|ASA-3-713051: Terminating connection attempt: IPSEC not permitted for group (*group\_name*)

**Explanation** This message indicates that the user, group, or interface policy is rejecting IPsec tunnels.

**Recommended Action** To use IPsec select the appropriate tunneling protocol in the policy.

## 713052

**Error Message** %PIX|ASA-7-713052: User (*user*) authenticated.

**Explanation** This message indicates that the remote access user was authenticated.

**Recommended Action** None.

## 713056

**Error Message** %PIX|ASA-3-713056: Tunnel rejected: SA (*SA\_name*) not found for group (*group\_name*) !

**Explanation** This message indicates that the IPsec SA was not found.

**Recommended Action** If this is a remote access tunnel, check the group and user configuration and verify that a tunnel group and group policy has been configured for the user's group. For externally authenticated users and groups, check the returned authentication attributes.

## 713059

**Error Message** %PIX|ASA-3-713059: Tunnel Rejected: User (*user*) matched with group name, group-lock check failed.

**Explanation** This message indicates that the user tried to authenticate by using the same string for both the tunnel group and username.

**Recommended Action** The group and username must be different for the user to be authenticated.

## 713060

**Error Message** %PIX|ASA-3-713060: Tunnel Rejected: User (*user*) not member of group (*group\_name*), group-lock check failed.

**Explanation** This message indicates that the user is configured for a different group than what was sent in the IPsec negotiation.

**Recommended Action** If you are using the Cisco VPN client and preshared keys, make sure that the group configured on the client is the same as the group associated with the user on the security appliance. If using digital certificates, the group is dictated either by the OU field of the certificate or the user will default to the remote access default group.



## 713061

**Error Message** %PIX|ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:*source\_address*, Dst: *dest\_address*!

**Explanation** This message indicates that the security appliance was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the security appliance. This is most likely a misconfiguration.

**Recommended Action** Check the protected network configuration in the crypto ACLs on both sides and make sure that the local net on the initiator is the remote net on the responder and vice-versa. Pay special attention to wildcard masks, host addresses versus network addresses, etc. Non-Cisco implementations may have the private addresses labeled as proxy addresses or red networks.

## 713062

**Error Message** %PIX|ASA-3-713062: IKE Peer address same as our interface address *IP\_address*

**Explanation** The IP address configured as the IKE peer is the same as the IP address configured on one of the security appliance IP interfaces.

**Recommended Action** Check the L2L configuration and configuration of IP interface(s).

## 713063

**Error Message** %PIX|ASA-3-713063: IKE Peer address not configured for destination *IP\_address*

**Explanation** This message appears when the IKE peer address is not configured for a L2L tunnel.

**Recommended Action** Check the L2L configuration.

## 713065

**Error Message** %PIX|ASA-3-713065: IKE Remote Peer did not negotiate the following: *proposal attribute*

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713066

**Error Message** %PIX|ASA-7-713066: IKE Remote Peer configured for SA: *SA\_name*

**Explanation** This message indicates the peer's crypto policy settings.

**Recommended Action** None.

## 713068

**Error Message** %PIX|ASA-5-713068: Received non-routine Notify message: *notify\_type* (*notify\_value*)

**Explanation** This message indicates that notification messages that cause this event are not explicitly handled in the notify processing code.

**Recommended Action** Examine the specific reason information to determine the action to take. Many notification messages indicate a configuration mismatch between the IKE peers.

## 713072

**Error Message** %PIX|ASA-3-713072: Password for user (*user*) too long, truncating to *number* characters

**Explanation** This message indicates that the user's password is too long.

**Recommended Action** Correct password lengths on the authentication server.

## 713073

**Error Message** %PIX|ASA-5-713073: Responder forcing change of *Phase 1/Phase 2* rekeying duration from *larger\_value* to *smaller\_value* seconds

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the initiator's value is the lower one.

**Recommended Action** None.

## 713074

**Error Message** %PIX|ASA-5-713074: Responder forcing change of IPSec rekeying duration from *larger\_value* to *smaller\_value* Kbs

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the initiator's value is the lower one.

**Recommended Action** None.

## 713075

**Error Message** %PIX|ASA-5-713075: Overriding Initiator's IPSec rekeying duration from *larger\_value* to *smaller\_value* seconds

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the responder's value is the lower one.

**Recommended Action** None.

## 713076

**Error Message** %PIX|ASA-5-713076: Overriding Initiator's IPSec rekeying duration from *larger\_value* to *smaller\_value* Kbs

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the responder's value is the lower one.

**Recommended Action** None.

## 713078

**Error Message** %PIX|ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize *available\_size*, used *value*

**Explanation** This message indicates that an internal software error has occurred while processing modecfg attributes.

**Recommended Action** Disable any unnecessary tunnel group attributes or shorten any text messages that are excessively long. If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information along with your configuration file.

## 713081

**Error Message** %PIX|ASA-3-713081: Unsupported certificate encoding type *encoding\_type*

**Explanation** This message indicates that one of the loaded certificates is unreadable, and could be an unsupported encoding scheme.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

## 713082

**Error Message** %PIX|ASA-3-713082: Failed to retrieve identity certificate

**Explanation** Could not find the Identity Certificate for this tunnel.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

## 713083

**Error Message** %PIX|ASA-3-713083: Invalid certificate handle

**Explanation** This message indicates that the identity certificate for this tunnel could not be found.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

## 713084

**Error Message** %PIX|ASA-3-713084: Received invalid phase 1 port value (*port*) in ID payload

**Explanation** This message indicates that the port value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 500 (ISAKMP aka IKE).

**Recommended Action** This may indicate a peer that does not conform to the IKE standards or a network problem that results in corrupted packets.

## 713085

**Error Message** %PIX|ASA-3-713085: Received invalid phase 1 protocol (*protocol*) in ID payload

**Explanation** This message indicates that the protocol value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 17 (UDP).

**Recommended Action** This may indicate a peer that does not conform to the IKE standards or a network problem that results in corrupted packets.

## 713086

**Error Message** %PIX|ASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (*Auth method (auth numerical value)*)

**Explanation** This message appears when a cert payload was received but our internal cert handle indicates that we do not have an identity cert. This could mean that the cert handle was not obtained through a normal enrollment method. One likely reason this can happen is that the authentication method is not RSA or DSS signatures, although the IKE SA negotiation should fail if each side is misconfigured.

**Recommended Action** Check the trustpoint and ISAKMP configuration settings on the appliance and peer.

## 713088

**Error Message** %PIX|ASA-3-713088: Set Cert filehandle failure: no IPsec SA in group *group\_name*

**Explanation** This message indicates that the tunnel group could not be found based on the digital certificate information.

**Recommended Action** Verify that the tunnel group is set up appropriately to handle the peer's certificate information.

## 713092

**Error Message** %PIX|ASA-5-713092: Failure during phase 1 rekeying attempt due to collision

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** This is often a benign event but if it has serious repercussions, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713094

**Error Message** %PIX|ASA-7-713094: Cert validation failure: handle invalid for *Main/Aggressive Mode Initiator/Responder!*

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** You may have to reenroll the trustpoint. If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713098

**Error Message** %PIX|ASA-3-713098: Aborting: No identity cert specified in IPsec SA (*SA\_name*) !

**Explanation** This message appears when an attempt is made to establish a Certs-based IKE session, but no identity certificate have been specified in the crypto policy.

**Recommended Action** Specify the identity certificate/trustpoint that you want to transmit to peers.

## 713099

**Error Message** %PIX|ASA-7-713099: Tunnel Rejected: Received NONCE length *number* is out of range!

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713102

**Error Message** %PIX|ASA-3-713102: Phase 1 ID Data length *number* too long - reject tunnel!

**Explanation** This message indicates that IKE has received an ID payload containing an Identification Data field of size 2K or greater.

**Recommended Action** None.

## 713103

**Error Message** %PIX|ASA-7-713103: Invalid (NULL) secret key detected while computing hash

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713104

**Error Message** %PIX|ASA-7-713104: Attempt to get Phase 1 ID data failed while *hash computation*

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713105

**Error Message** %PIX|ASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing

**Explanation** This message indicates that a peer sent an ID payload without including any ID data, which is invalid.

**Recommended Action** Check the configuration of the peer.

## 713107

**Error Message** %PIX|ASA-3-713107: IP\_Address request attempt failed!

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713109

**Error Message** %PIX|ASA-3-713109: Unable to process the received peer certificate

**Explanation** This message indicates that the security appliance was unable to process the certificate received from the remote peer. This can occur if the certificate data was malformed or if the data in the certificate could not be stored by the appliance. One such possibility is if the public key size is larger than 4096 bits.

**Recommended Action** Try to reestablish the connection using a different certificate on the remote peer.

## 713112

**Error Message** %PIX|ASA-3-713112: Failed to process CONNECTED notify (SPI *SPI\_value*)!

**Explanation** This message indicates that the security appliance was unable to successfully process the notify payload that contained notify type CONNECTED. This could occur if the IKE phase 2 structure could not be found using the SPI to locate it, or the commit bit had not been set in the received ISAKMP header. This later case could indicate a non-conforming IKE peer.

**Recommended Action** If the problem persists, check the peer's configuration and/or disable commit bit processing.

## 713113

**Error Message** %PIX|ASA-7-713113: Deleting IKE SA with associated IPsec connection entries. IKE peer: *IP\_address*, SA address: *internal\_SA\_address*, tunnel count: *count*

**Explanation** This message indicates that an IKE SA is being deleted with a non-0 tunnel count. This means that either the IKE SA tunnel count has lost synchronization with the associated connection entries or the associated connection entries' cookie fields have lost synchronization with the cookie fields of the IKE SA that the connection entry points to. If this occurs, the IKE SA and its associated data structures will not be freed, so that the entries which may point to it will not have a stale pointer.

**Recommended Action** None. Error recovery is built-in.

## 713114

**Error Message** %PIX|ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (*SA\_internal\_address*) for peer *IP\_address*, but cookies don't match

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.



## 713115

**Error Message** %PIX|ASA-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec

**Explanation** This message indicates the client rejected an attempt by the security appliance to use IPsec over UDP. IPsec over UDP is used to allow multiple clients to establish simultaneous tunnels to the security appliance through a NAT device. The client may have rejected the request either because it does not support this feature or because it is configured to not use it.

**Recommended Action** Verify the configuration on the headend and peer.

## 713116

**Error Message** %PIX|ASA-3-713116: Terminating connection attempt: L2TP-over-IPSEC attempted by group (*group\_name*) but L2TP disabled

**Explanation** This message indicates that the user or group entity has attempted an L2TP-over-IPsec connection, but the L2TP protocol is not enabled for this security appliance.

**Recommended Action** Verify the L2TP configuration.

## 713117

**Error Message** %PIX|ASA-7-713117: Received Invalid SPI notify (SPI *SPI\_Value*)!

**Explanation** This message indicates the IPsec SA identified by the SPI value is no longer active on the remote peer. This might indicate that the remote peer has rebooted or been reset.

**Recommended Action** This problem should correct itself once DPDs recognize that the peer no longer has the appropriate SAs established. If DPD is not enabled, this may require a manual reestablishment of the affected tunnel.

## 713118

**Error Message** %PIX|ASA-3-713118: Detected invalid Diffie-Hellman *group\_descriptor* *group\_number*, in IKE area

**Explanation** This message indicates that the *group\_descriptor* field contains an unsupported value. Currently we support only groups 1, 2, 5, and 7. In the case of a centry the *group\_descriptor* field may also be set to 0, to indicate that Perfect Forward Secrecy (PFS) is disabled.

**Recommended Action** Check the peer Diffie-Hellman configuration.

## 713119

**Error Message** %PIX|ASA-3-713119: PHASE 1 COMPLETED

**Explanation** This message appears when IKE Phase 1 has completed successfully.

**Recommended Action** None.

## 713120

**Error Message** %PIX|ASA-5-713120: PHASE 2 COMPLETED (msgid=*msg\_id*)

**Explanation** This message appears when IKE Phase 2 has completed successfully.

**Recommended Action** None.

## 713121

**Error Message** %PIX|ASA-7-713121: Keep-alive type for this connection: *keepalive\_type*

**Explanation** This message indicates the type of keep-alive mechanism being used for this tunnel.

**Recommended Action** None.

## 713122

**Error Message** %PIX|ASA-3-713122: Keep-alives configured *keepalive\_type* but peer *IP\_address* support keep-alives (type = *keepalive\_type*)

**Explanation** This message indicates that keep-alives are configured on/off for this device, but the IKE peer does/doesn't support keep-alives.

**Recommended Action** This requires no action if this is intentional. If it is not intentional, change the keepalive configuration on both devices.

## 713123

**Error Message** %PIX|ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: *keepalive\_type*)

**Explanation** This message indicates that the remote IKE peer did not respond to keep-alives within the expected window of time, so the connection to the IKE peer was terminated. The message includes the keep-alive mechanism used.

**Recommended Action** None.

## 713124

**Error Message** %PIX|ASA-3-713124: Received DPD sequence number *rcv\_sequence\_#* in *DPD Action, description expected seq #*

**Explanation** This message indicates that the remote IKE peer sent a DPD with a sequence number that did not match the expected sequence number. The packet is discarded.

**Recommended Action** This might indicate a packet loss problem with the network.

## 713127

**Error Message** %PIX|ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list

**Explanation** This message appears when the peer wants to perform a XAUTH but the security appliance did not choose the XAUTH IKE proposal.

**Recommended Action** Check the priorities of the IKE xauth proposals in IKE proposal list.

## 713128

**Error Message** %PIX|ASA-3-713128: Connection attempt to VCPIP redirected to VCA peer *IP\_address* via load balancing

**Explanation** This message appears when a connection attempt has been made to the VCPIP and has been redirected to a less loaded peer using load balancing.

**Recommended Action** None.

## 713129

**Error Message** %PIX|ASA-3-713129: Received unexpected Transaction Exchange payload type: *payload\_id*

**Explanation** This message indicates that an unexpected payload has been received during XAUTH or Mode-cfg. This may indicate that the two peers are out of synchronization, that the XAUTH or Mode-cfg versions do not match, or that the remote peer is not complying to the appropriate RFCs.

**Recommended Action** Verify the configuration between peers.

## 713130

**Error Message** %PIX|ASA-5-713130: Received unsupported transaction mode attribute: *attribute id*

**Explanation** This message indicates that the device received a request for a valid transaction mode attribute (XAUTH or Mode Cfg) that is currently not supported. This is generally a benign condition.

**Recommended Action** None.

## 713131

**Error Message** %PIX|ASA-5-713131: Received unknown transaction mode attribute: *attribute\_id*

**Explanation** This message indicates that the security appliance has received a request for a transaction mode attribute (XAUTH or Mode Cfg) that is outside the range of known attributes. The attribute may be valid but only supported in later versions of config mode, or the peer may be sending an illegal or proprietary value. This should not cause connectivity problems but may affect the functionality of the peer.

**Recommended Action** None.

## 713132

**Error Message** %PIX|ASA-3-713132: Cannot obtain an *IP\_address* for remote peer

**Explanation** This message indicates that a request for an IP address for a remote access client from the internal utility that provides these addresses could not be satisfied.

**Recommended Action** Check configuration of IP address assignment methods.

## 713133

**Error Message** %PIX|ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group *DH group\_id*) with phase 1 group(DH group *DH group\_number*)

**Explanation** The configured Phase 2 PFS Group differs from the DH group that was negotiated for phase 1.

**Recommended Action** None.

## 713134

**Error Message** %PIX|ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection

**Explanation** This message appears when the configured LAN-to-LAN proposal is different from the one accepted for the LAN-to-LAN connection. Depending on which side is the initiator, different proposals will be used.

**Recommended Action** None.

## 713135

**Error Message** %PIX|ASA-5-713135: message received, redirecting tunnel to *IP\_address*.

**Explanation** This message indicates that the tunnel is being redirected due to load balancing on the remote security appliance. This message will be seen when a REDIRECT\_CONNECTION notify packet is received.

**Recommended Action** None.

## 713136

**Error Message** %PIX|ASA-5-713136: IKE session establishment timed out [*IKE\_state\_name*], aborting!

**Explanation** This occurs when the reaper has detected an SA stuck in a non-active state. The reaper will try to remove the hung SA.

**Recommended Action** None.

## 713137

**Error Message** %PIX|ASA-5-713137: Reaper overriding refCnt [*ref\_count*] and tunnelCnt [*tunnel\_count*] -- deleting SA!

**Explanation** This message indicates that an internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713138

**Error Message** %PIX|ASA-3-713138: Group *group\_name* not found and BASE GROUP default preshared key not configured

**Explanation** This message appears when there is no group in the group database with the same name as the IP address of the peer. In Main Mode, the security appliance will fall back and try to use the default preshared key configured in one of the default groups. The default preshared key is not configured.

**Recommended Action** Verify the configuration of the preshared keys.

## 713139

**Error Message** %PIX|ASA-5-713139: *group\_name* not found, using BASE GROUP default preshared key

**Explanation** There was no tunnel group in the group database with the same name as the IP address of the peer. In Main Mode, the security appliance will fall back and use the default preshared key configured in the default group.

**Recommended Action** None.

## 713140

**Error Message** %PIX|ASA-3-713140: Split Tunneling Policy requires network list but none configured

**Explanation** This message appears when split tunneling policy is set to either split tunneling or allow local LAN access, a split tunneling ACL must be defined to represent the information required by the VPN Client.

**Recommended Action** Check the configuration of the ACLs.

## 713141

**Error Message** %PIX|ASA-3-713141: Client-reported firewall does not match configured firewall: *action* tunnel. Received -- Vendor: *vendor(id)*, Product *product(id)*, Caps: *capability\_value*. Expected -- Vendor: *vendor(id)*, Product: *product(id)*, Caps: *capability\_value*

**Explanation** This message indicates that the security appliance installed on the client does not match the configured required security appliance. This message lists the actual and expected values, and whether the tunnel is terminated or allowed.

**Recommended Action** You may need to install a different personal security appliance on the client or a change of configuration on the security appliance.

## 713142

**Error Message** %PIX|ASA-3-713142: Client did not report firewall in use, but there is a configured firewall: *action* tunnel. Expected -- Vendor: *vendor(id)*, Product *product(id)*, Caps: *capability\_value*

**Explanation** This message appears when the client did not report a security appliance in use using ModeCfg but one is required. The event lists the expected values, and whether the tunnel is terminated or allowed. Note that the number following the product string is a bitmask of all of the allowed products.

**Recommended Action** You may need to install a different personal security appliance on the client or a change of configuration on the security appliance.

## 713143

**Error Message** %PIX|ASA-7-713143: Processing firewall record. Vendor: *vendor(id)*, Product: *product(id)*, Caps: *capability\_value*, Version Number: *version\_number*, Version String: *version\_text*

**Explanation** This message provides debug information about the security appliance installed on the client.

**Recommended Action** None.

## 713144

**Error Message** %PIX|ASA-5-713144: Ignoring received malformed firewall record; reason - *error\_reason* TLV type *attribute\_value* *correction*

**Explanation** This message indicates that bad security appliance information was received from the client.

**Recommended Action** Check the personal security appliance configuration on the client and the security appliance.

## 713145

**Error Message** %PIX|ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: *IP\_address*, mask: *netmask*

**Explanation** This message indicates that a tunnel with a hardware client in network extension mode has been negotiated and a static route is being added for the private network behind the hardware client. This enables the security appliance to make the remote network known to all the routers on the private side of the head-end.

**Recommended Action** None.

## 713146

**Error Message** %PIX|ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: *IP\_address*, mask: *netmask*

**Explanation** This message indicates that an internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated and an attempt to add the static route for the private network behind the hardware client failed. This could indicate that the routing table is full or a possible addressing error.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713147

**Error Message** %PIX|ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: *IP\_address*, mask: *netmask*

**Explanation** This message indicates that a tunnel to a hardware client in network extension mode is being removed and the static route for the private network is being deleted behind the hardware client.

**Recommended Action** None.



## 713148

**Error Message** %PIX|ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: *IP\_address*, mask: *netmask*

**Explanation** This message indicates that while a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client could not be deleted.

**Recommended Action** This might indicate an addressing or software problem. Check the routing table to ensure that the route is not there. If it is, it may have to be removed manually but only if the tunnel to the hardware client has been completely removed.

## 713149

**Error Message** %PIX|ASA-3-713149: Hardware client security attribute *attribute\_name* was enabled but not requested.

**Explanation** This message indicates that the head-end security appliance has the specified hardware client security attribute enabled, but the attribute was not requested by the VPN3002 hardware client.

**Recommended Action** Check the configuration on the hardware client.

## 713152

**Error Message** %PIX|ASA-3-713152: Unable to obtain any rules from filter *ACL\_tag* to send to client for CPP, terminating connection.

**Explanation** This message indicates that the client is required to use CPP to provision its security appliance, but the head-end device was unable to obtain any ACLs to send to the client. This is probably due to a misconfiguration.

**Recommended Action** Check the ACLs specified for CPP in the client's group policy.

## 713154

**Error Message** %PIX|ASA-4-713154: DNS lookup for *peer\_description* Server [*server\_name*] failed!

**Explanation** This message appears when DNS lookup for the specified server has not been resolved.

**Recommended Action** Check DNS server configuration on the security appliance. Also check the DNS server to ensure that it is operational and has the hostname to IP address mapping.

## 713155

**Error Message** %PIX|ASA-5-713155: DNS lookup for Primary VPN Server [*server\_name*] successfully resolved after a previous failure. Resetting any Backup Server init.

**Explanation** A previous DNS lookup failure for the primary server might have caused the system to initialize a backup peer. This message indicates that a later DNS lookup on the primary server finally succeeded and is resetting any backup server initializations. A tunnel initiated after this point will be aimed at the primary server.

**Recommended Action** None.

## 713156

**Error Message** %PIX|ASA-5-713156: Initializing Backup Server [*server\_name* or *IP\_address*]

**Explanation** This message indicates that the client is failing over to a backup server or a failed DNS lookup for the primary server caused the system to initialize a backup server. A tunnel initiated after this point will be aimed at the specified backup server.

**Recommended Action** None.

## 713157

**Error Message** %PIX|ASA-4-713157: Timed out on initial contact to server [*server\_name* or *IP\_address*] Tunnel could not be established.

**Explanation** This message indicates that the client tried to initiate a tunnel by sending out IKE MSG1, but didn't receive a response from the security appliance on the other end. If backup servers are available, the client will attempt to connect to one of them.

**Recommended Action** Verify connectivity to the head-end security appliance.

## 713158

**Error Message** %PIX|ASA-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP

**Explanation** This message indicates that the client is configured to use IPsec over TCP. The client rejected the attempt by the security appliance to use IPsec over UDP.

**Recommended Action** If TCP is desired, no action is required. Otherwise, check the client configuration.

## 713159

**Error Message** %PIX|ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access

**Explanation** This message indicates that the TCP connection to the security appliance server was lost for some reason. Likely reasons are that the server has rebooted, has a network problem, has an SSL mismatch, etc.

**Recommended Action** If the server connection was lost after the initial connection was made, then the server and network connections must be checked. If the initial connection is lost immediately, this could indicate an SSL authentication problem.

## 713160

**Error Message** %PIX|ASA-7-713160: Remote user (session Id - *id*) has been granted access by the Firewall Server

**Explanation** This message indicates normal authentication of the remote user to the security appliance server.

**Recommended Action** None.

## 713161

**Error Message** %PIX|ASA-3-713161: Remote user (session Id - *id*) network access has been restricted by the Firewall Server

**Explanation** The security appliance server has sent the security appliance a message indicating that this user must be restricted. There are several reasons for this including security appliance software upgrades, changes in permissions, etc. The security appliance server will transition the user back into full access mode as soon as the operation has been completed.

**Recommended Action** No action is required unless the user is never transitioned back into full access state. If this does not happen, refer to the security appliance server for more information on the operation that is being performed and the state of the security appliance software running on the remote machine.

## 713162

**Error Message** %PIX|ASA-3-713162: Remote user (session Id - *id*) has been rejected by the Firewall Server

**Explanation** This message indicates that the security appliance server has rejected this user.

**Recommended Action** Check the policy information on the security appliance server to make sure that the user is configured correctly.

## 713163

**Error Message** %PIX|ASA-3-713163: Remote user (session Id - *id*) has been terminated by the Firewall Server

**Explanation** This message indicates that the security appliance server has terminated this user session. This can happen if the integrity agent stops running on the client machine or if the security policy is modified by the remote user in any way.

**Recommended Action** Verify that the security appliance software on the client machine is still running and that the policy is correct.

## 713164

**Error Message** %PIX|ASA-7-713164: The Firewall Server has requested a list of active user sessions

**Explanation** This message indicates that the security appliance server will request the session information if it detects that it has stale data or if it loses the session data (as in a reboot).

**Recommended Action** None.

## 713165

**Error Message** %PIX|ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode

**Explanation** This message indicates that the client negotiated with preshared keys while its tunnel group points to a policy that is configured to use digital certificates.

**Recommended Action** Check the client configuration.

## 713166

**Error Message** %PIX|ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password

**Explanation** This message indicates that the hardware client has failed extended authentication. This is most likely a username/password problem or authentication server issue.

**Recommended Action** Verify that the configured username and password values on each side match. Also verify that the authentication server at the head-end is operational.

## 713167

**Error Message** %PIX|ASA-3-713167: Remote peer has failed user authentication - check configured username and password

**Explanation** This message indicates that the remote user has failed to extend authentication. This is most likely a username or password problem or authentication server issue.

**Recommended Action** Verify that the configured username and password values on each side match. Also verify that the authentication server being used to authenticate the remote is operational.

## 713168

**Error Message** %PIX|ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!

**Explanation** This message indicates that reauthentication on rekey has been enabled but the tunnel authentication requires manual intervention.

**Recommended Action** If manual intervention is desired, no action is required. Otherwise, check the interactive authentication configuration.

## 713169

**Error Message** %PIX|ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: *IP\_address*, SA address: *internal\_SA\_address*, tunnelCnt: *tunnel\_count*

**Explanation** This message indicates that IKE has received a delete message from the remote peer to delete its old IKE SA after a rekey has completed.

**Recommended Action** None.

## 713170

**Error Message** %PIX|ASA-7-713170: IKE Received delete for rekeyed centry IKE peer: *IP\_address*, centry address: *internal\_address*, msgid: *id*

**Explanation** IKE receives a delete message from the remote peer to delete its old centry after phase 2 rekeying is completed.

**Recommended Action** None.

## 713171

**Error Message** %PIX|ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload

**Explanation** UDP-Encapsulated-Transport was either proposed or selected during phase 2. Need to send this payload for NAT-Traversal in this case.

**Recommended Action** None.

## 713172

**Error Message** %PIX|ASA-6-713172: Automatic NAT Detection Status: Remote end *is/is not* behind a NAT device This end *is/is not* behind a NAT device

**Explanation** Results from NAT auto-detection by NAT-Traversal.

**Recommended Action** None.

## 713174

**Error Message** %PIX|ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!

**Explanation** A Hardware Client is attempting to tunnel in using network extension mode but network extension mode is not allowed.

**Recommended Action** Verify configuration of Network Extension Mode versus. PAT mode.

## 713176

**Error Message** %PIX|ASA-2-713176: *Device\_type* memory resources are critical, IKE key acquire message on interface *interface\_number*, for Peer *IP\_address* ignored

**Explanation** This event indicates that the appliance is processing data intended to trigger an IPSec tunnel to the indicated peer. Since memory resources are at a critical state, it is not initiating any more tunnels. The data packet has been ignored and dropped.

**Recommended Action** If condition persists, verify that appliance is efficiently configured. This event could indicate that an appliance with increased memory is required for this application.

## 713177

**Error Message** %PIX|ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: *host\_name* Address *IP\_address*, Protocol *protocol*, Port *port*

**Explanation** A Phase 2 ID payload containing an FQDN has been received from the peer.

**Recommended Action** None.

## 713178

**Error Message** %PIX|ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie

**Explanation** An internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 713179

**Error Message** %PIX|ASA-5-713179: IKE AM Initiator received a packet from its peer without a *payload\_type* payload

**Explanation** An internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 713182

**Error Message** %PIX|ASA-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!

**Explanation** An internal software error has occurred.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 713184

**Error Message** %PIX|ASA-6-713184: Client Type: *Client\_type* Client Application Version: *Application\_version\_string*

**Explanation** This event indicates the client operating system and application version. If the information is not available, then N/A will be indicated.

**Recommended Action** None.

## 713185

**Error Message** %PIX|ASA-3-713185: Error: Username too long - connection aborted

**Explanation** The client returned an invalid length username and the tunnel was torn down.

**Recommended Action** Check the username and make changes if necessary.

## 713186

**Error Message** %PIX|ASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: *list\_text* Character *index (value)* is illegal

**Explanation** An invalid secondary domain name list was received from an external RADIUS authentication server. When split tunnelling is used, this list identifies the domains that the client should resolve through the tunnel.

**Recommended Action** Correct the specification of the Secondary-Domain-Name-List attribute (vendor specific attribute 29) on the RADIUS server. The list must be specified as a comma delimited list of domain names. Domain names may not include any characters other than alpha-numeric, hyphen, underscore and period.



## 713187

**Error Message** %PIX|ASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: *IP\_address*, Remote peer address: *IP\_address*

**Explanation** The IKE peer that is attempting to bring up this tunnel is not the one that is configured in the ISAKMP configuration that is bound to the received remote subnet(s).

**Recommended Action** Verify proper L2L settings on headend and peer.

## 713189

**Error Message** %PIX|ASA-3-713189: Attempted to assign network or broadcast *IP\_address*, removing (*IP\_address*) from pool.

**Explanation** The IP address from the pool is either the network or broadcast address for this subnet. This address will be marked as unavailable.

**Recommended Action** This error is generally benign but the IP address pool configuration should be checked.

## 713190

**Error Message** %PIX|ASA-7-713190: Got bad refCnt (*ref\_count\_value*) assigning *IP\_address* (*IP\_address*)

**Explanation** The reference counter for this SA is invalid.

**Recommended Action** This issue should correct itself.

## 713193

**Error Message** %PIX|ASA-3-713193: Received packet with missing payload, Expected payload: *payload\_id*

**Explanation** The Appliance received an encrypted/unencrypted packet of the specified exchange type that had one or more missing payloads. This usually indicates a problem on the peer.

**Recommended Action** Verify peer is sending valid IKE messages.

## 713194

**Error Message** %PIX|ASA-3-713194: *IKEIPSec* Delete With Reason message: *termination\_reason*

**Explanation** Indicates that a delete message with a termination reason code was received.

**Recommended Action** None.

## 713195

**Error Message** %PIX|ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!

**Explanation** Originate Only peer can accept incoming connections only after it brings up the first P2 tunnel. At that point, data from either direction can initiate additional Phase 2 tunnels.

**Recommended Action** If a different behavior is desired, the originate only configuration needs to be revisited.

## 713196

**Error Message** %PIX|ASA-5-713196: Remote L2L Peer *IP\_address* initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!

**Explanation** The remote L2L peer has initiated a Public-Public tunnel. It expects an answer only peer at the other end and we are not one. Possible misconfiguration.

**Recommended Action** Check the L2L configuration on both sides.

## 713197

**Error Message** %PIX|ASA-5-713197: The configured Confidence Interval of *number* seconds is invalid for this *tunnel\_type* connection. Enforcing the second default.

**Explanation** The configured Confidence Interval in the group is outside of the valid range.

**Recommended Action** Check the Confidence Setting in the group to make sure it is within the valid range.

## 713198

**Error Message** %PIX|ASA-3-713198: User Authorization failed: *user* User authorization failed.

**Explanation** This event will contain a reason string.

**Recommended Action** Check group configuration and client authorization.

## 713199

**Error Message** %PIX|ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (*counter\_value*)!

**Explanation** Reaper corrected an internal software error.

**Recommended Action** If condition persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 713203

**Error Message** %PIX|ASA-3-713203: IKE Receiver: Error reading from socket.

**Explanation** This message indicates that there was an error while reading a received IKE packet. This is generally an internal error and might indicate a software problem.

**Recommended Action** This problem is usually benign and the system will correct itself. If this problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information

## 713204

**Error Message** %PIX|ASA-7-713204: Adding static route for client address: *IP\_address*

**Explanation** This message indicates that a route to the peer-assigned address or to the networks protected by a hardware client was added to the routing table.

**Recommended Action** None.

## 713205

**Error Message** %PIX|ASA-3-713205: Could not add static route for client address:  
*IP\_address*

**Explanation** This message indicates a failed attempt to add a route to the client-assigned address or to the networks protected by a hardware client. This could indicate duplicate routes in the routing table or a corrupted network address. The duplicate routes could be caused by routes not cleaned up properly or by having multiple clients sharing networks or addresses.

**Recommended Action** Check the IP local pool configuration as well as any other IP address-assigning mechanism being used (for example: DHCP or RADIUS). Ensure that routes are being cleared from the routing table. Also check the configuration of networks and/or addresses on the peer system.

## 713206

**Error Message** %PIX|ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by  
tunnel-group and group-policy

**Explanation** This message appears when a tunnel is dropped because the allowed tunnel specified in the group policy is different than the allowed tunnel in the tunnel-group configuration.

**Recommended Action** Check the tunnel-group and group-policy configuration.

## 713208

**Error Message** %PIX|ASA-3-713208: Cannot create dynamic rule for Backup L2L entry *rule*  
*rule\_id*

**Explanation** This message indicates that there was a failure in creating the ACLs that trigger IKE and allow IPSec data to be processed properly. The failure was specific to the Backup L2L configuration. This may indicate a configuration error, a capacity error or an internal software error.

**Recommended Action** If the device is running at maximum security appliance cons and maximum VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configuration, specifically the ACLs associated with the crypto maps.

## 713209

**Error Message** %PIX|ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry *rule\_id*

**Explanation** This message indicates that there was a failure in deleting the ACLs that trigger IKE and allow IPSec data to be processed properly. The failure was specific to the Backup L2L configuration. This may indicate an internal software error.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 713210

**Error Message** %PIX|ASA-3-713210: Cannot create dynamic map for Backup L2L entry *rule\_id*

**Explanation** This message indicates that there was a failure in creating a run-time instance of the dynamic crypto map associated with backup L2L configuration. This may indicate a configuration error, a capacity error or an internal software error.

**Recommended Action** If the device is running at maximum security appliance cons and maximum VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configuration, specifically the ACLs associated with the crypto maps.

## 713211

**Error Message** %PIX|ASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: *IP\_address*, mask: *netmask*

**Explanation** This message indicates that the security appliance is adding a route for the private address or networks of the peer. In this case, the peer is either a Client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

**Recommended Action** None.

## 713212

**Error Message** %PIX|ASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: *IP\_address*, mask: *netmask*

**Explanation** This message appears when the security appliance failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a Client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This could indicate duplicate routes. A full routing table or a failure of the security appliance to remove previously used routes.

**Recommended Action** Check the routing table to make sure there is room for additional routes and that obsolete routes are not present. If the table is full or contains obsolete routes, remove the routes and try again. If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information

## 713213

**Error Message** %PIX|ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: *IP\_address*, mask: *netmask*

**Explanation** This message indicates that the security appliance is deleting a route for the private address or networks of the peer. In this case, the peer is either a Client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

**Recommended Action** None.

## 713214

**Error Message** %PIX|ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: *IP\_address*, mask: *netmask*

**Explanation** This message indicates that the security appliance experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a Client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This event may indicate that the route has already been deleted or that an internal software error has occurred.

**Recommended Action** If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information

## 713215

**Error Message** %PIX|ASA-6-713215: No match against Client Type and Version rules.  
Client: *type version is/is not* allowed by default

**Explanation** This message indicates that the client type and the version of a client did not match any of the rules configured on the security appliance. The default action is displayed.

**Recommended Action** Determine what the default action and deployment requirements are and make the appropriate changes.

## 713216

**Error Message** %PIX|ASA-5-713216: Rule: *action* Client type : *version* Client: *type version is/is not* allowed

**Explanation** This message indicates that the client type and the version of a client has matched one of the rules. The result of the match and the rule are displayed.

**Recommended Action** Determine what the deployment requirements are and make the appropriate changes.

## 713217

**Error Message** %PIX|ASA-3-713217: Skipping unrecognized rule: action: *action* client type: *client\_type* client version: *client\_version*

**Explanation** This message indicates that there is a malformed client type and version rule. The required format is *action client type | client version action* either “permit” or “deny” *client type* and *client version* are displayed under Session Management. Only one wildcard per parameter (\*) is supported.

**Recommended Action** Correct the rule.

## 713218

**Error Message** %PIX|ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.

**Explanation** This message indicates that the client was rejected access per the configured rules.

**Recommended Action** None.

## 713219

**Error Message** %PIX|ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when P1 SA is complete.

**Explanation** This message indicates that Phase 2 messages are being enqueued after Phase 1 completes.

**Recommended Action** None.

## 713220

**Error Message** %PIX|ASA-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.

**Explanation** This message indicates that queued Phase 2 messages are now being processed.

**Recommended Action** None.

## 713221

**Error Message** %PIX|ASA-7-713221: Static Crypto Map check, checking map = *crypto\_map\_tag*, seq = *seq\_number*...

**Explanation** This message indicates that the security appliance is iterating through the crypto maps looking for configuration information.

**Recommended Action** None.

## 713222

**Error Message** %PIX|ASA-7-713222: Static Crypto Map check, map = *crypto\_map\_tag*, seq = *seq\_number*, ACL does not match proxy IDs src:*source\_address* dst:*dest\_address*

**Explanation** This message indicates that while iterating through the configured crypto maps, the security appliance could not match any of the associated ACLs. This generally means that an ACL was misconfigured.

**Recommended Action** Check the ACLs associated with this tunnel peer and make sure they specify the appropriate private networks from both sides of the VPN tunnel.



## 713223

**Error Message** %PIX|ASA-7-713223: Static Crypto Map check, map = *crypto\_map\_tag*, seq = *seq\_number*, no ACL configured

**Explanation** This message indicates that the crypto map associated with this peer is not linked to an ACL.

**Recommended Action** Make sure there is an ACL associated with this crypto map and that the ACL contains the appropriate private addresses or network from both sides of the VPN tunnel.

## 713224

**Error Message** %PIX|ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!

**Explanation** This message indicates that the crypto map associated with this VPN tunnel is missing critical information.

**Recommended Action** Verify that the crypto map is configured correctly with both the VPN peer, a transform set, and an associated ACL.

## 713225

**Error Message** %PIX|ASA-7-713225: [IKEv1], Static Crypto Map check, map *map\_name*, seq = *sequence\_number* is a successful match

**Explanation** This message indicates that the security appliance found a valid matching crypto map for this VPN tunnel.

**Recommended Action** None.

## 713226

**Error Message** %PIX|ASA-3-713226: Connection failed with peer *IP\_address*, no trust-point defined in tunnel-group *tunnel\_group*

**Explanation** When the device is configured to use digital certificates, a trust point must be specified in the configuration. When the trust point is missing from the config, this message is generated to flag an error.

*IP\_address*—IP Address of the peer

*tunnel\_group*—Tunnel group for which trust point was missing in the configuration.

**Recommended Action** The administrator of the device has to specify a trust point in the configuration.

## 713228

**Error Message** %PIX|ASA-6-713228: Assigned private IP address *assigned\_private\_IP assigned\_private\_IP*—Assigned client IP assigned by DHCP or from the local address pool

**Explanation** This message is generated when IKE obtains an address for the client private IP address from DHCP or from the address pool. The message specifies the IP address assigned to the client.

**Recommended Action** None.

## 713229

**Error Message** %PIX|ASA-5-713229: Auto Update - Notification to client *client\_ip* of update string: *message\_string*.

**Explanation** This message is displayed when a VPN remote access client is notified that updated software is available for download. The remote client user is responsible for choosing to update the client access software.

*client\_ip*—The IP address of the remote client

*message\_string*—The message text sent to the remote client

**Recommended Action** None.

## 713230

**Error Message** %PIX|ASA-3-713230 Internal Error, ike\_lock trying to lock bit that is already locked for type *type*

*type*—String that describes the type of semaphore that had a locking issue.

**Explanation** This message is displayed due to an internal error, which is reporting that the IKE subsystem is attempting to lock memory that has already been locked. This indicates errors on semaphores used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has happened and steps are automatically being taken for recovery.

**Recommended Action** Contact TAC and report the error.

## 713231

**Error Message** %PIX|ASA-3-713231 Internal Error, ike\_lock trying to unlock bit that is not locked for type *type*

**Explanation** This message is displayed due to an internal error, which is reporting that the IKE subsystem is attempting to unlock memory that is not currently locked. This indicates errors on semaphores used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has happened and steps are automatically being taken for recovery.

*type*—String that describes the type of semaphore that had a locking issue.

**Recommended Action** Contact TAC and report the error.

## 713232

**Error Message** %PIX|ASA-3-713232 SA lock refCnt = *value*, bitmask = *hexvalue*, p1\_decrypt\_cb = *value*, qm\_decrypt\_cb = *value*, qm\_hash\_cb = *value*, qm\_spi\_ok\_cb = *value*, qm\_dh\_cb = *value*, qm\_secret\_key\_cb = *value*, qm\_encrypt\_cb = *value*

**Explanation** This message displays all the IKE SA locks and is displayed when a possible error has been detected. This message reports errors on semaphores used to protect memory violations for IKE SAs.

*value*—Decimal value

*hexvalue*—Hexadecimal value

**Recommended Action** Contact TAC and report the error.

## 713233

**Error Message** %PIX|ASA-7-713233: (VPN-*unit*) Remote network (*remote network*) validated for network extension mode.

**Explanation** This message is displayed when the remote network received during the Phase 2 negotiation is validated. This message indicates the results of the remote network check during Phase 2 negotiations for Network Extension Mode clients. This is part of an existing feature that prevents users from misconfiguring their HW Client network (for example, configuring overlapping networks or the same network on multiple clients).

*remote network*—Subnet address and subnet mask from Phase 2 proxy

**Recommended Action** None.

## 713234

**Error Message** %PIX|ASA-7-713234: (VPN-unit) Remote network (*remote network*) from network extension mode client mismatches AAA configuration (*aaa network*).

**Explanation** This message is displayed when the remote network received during the Phase 2 negotiation does not match the framed-ip-address and framed-subnet-mask returned from the AAA server for this session.

*remote network*—Subnet address and subnet mask from Phase 2 proxy

*aaa network*—Subnet address and subnet mask configured through AAA

**Recommended Action** Do one of the following:

- Check the address assignment for this user and group, check the network configuration on the HW client, and fix any inconsistencies.
- Disable address assignment for this user and group.

## 713235

**Error Message** %PIX|ASA-7-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!

**Explanation** Normally, IKE packets should never be sent from the standby unit to the remote peer. This message is displayed if such an attempt is made due to an internal logic error. The packet never leaves the standby unit because of protective code. This message is mainly to facilitate debugging.

**Recommended Action** No action is required by the user. Developers should look into the condition causing the IKE packet to be sent from the standby unit.

## 713236

**Error Message** %PIX|ASA-7-713236: IKE\_DECODE tx/rx Message (msgid=msgid) with payloads :payload1 (payload1\_len) + payload2 (payload2\_len)...total length : tlen

**Explanation** This message is displayed when IKE sends or receives various messages.

The following example shows the output when IKE receives a message with an 8-byte hash payload, an 11-byte notify payload and two 13-byte vendor-specific payloads:

```
%PIX-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads : HDR + HASH (8) +
NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

**Recommended Action** None.

## 713237

**Error Message** %PIX|ASA-5-713237: ACL update (*access\_list*) received during re-key re-authentication will not be applied to the tunnel.

*access\_list*—Name associated with the static or dynamic access-list, as displayed in the output of the **show access-list** command

**Explanation** This message is displayed during the Phase 1 rekey of a remote access IPsec tunnel under the following conditions:

- The tunnel is configured to reauthenticate the user when the tunnel is rekeyed.
- The RADIUS server returns an access list or a reference to a locally configured access list that is different from the one that was returned when the tunnel was first established.

Under these conditions, the security appliance ignores the new access list and this message is generated.

**Recommended Action** IPsec users must reconnect for new user-specific access lists to take effect.

## 713238

**Error Message** %PIX|ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client

**Explanation** The private side address of a network extension mode client came across as 0.0.0.0. This usually indicates that no IP address was set on the private interface of the hardware client.

**Recommended Action** Verify the configuration of the remote client.

## 713239

**Error Message** %ASA-4-713239: *IP\_Address*: Tunnel Rejected: The maximum tunnel count allowed has been reached

**Explanation** An attempt to create a tunnel has occurred after the maximum number of tunnels allowed has been reached.

*IP\_Address*—The IP address of the peer.

**Recommended Action** None.

## 713240

**Error Message** %ASA-4-713240: Received DH key with bad length: received length=*rlength* expected length=*elength*

**Explanation** A Diffie-Hellman key with the incorrect length was received from the peer.

*rlength*—The length of the DH key that was received.

*elength*—The expected length (based on DH key size).

**Recommended Action** None.

## 713241

**Error Message** %ASA-4-713241: IE Browser Proxy Method setting\_number is Invalid

**Explanation** An invalid proxy setting was found during ModeCfg processing. P1 negotiation will fail.

**Recommended Action** Check the **msie-proxy method** command settings (a subcommand of the **group-policy** command), which should conform to one of the following: [ **auto-detect** | **no-modify** | **no-proxy** | **use-server** ]. Any other value or no value is incorrect. Try resetting the "msie-proxy method" settings. If that does not correct the problem, copy the error message exactly as it appears on the console or in the system log. Then contact the Cisco TAC for assistance.

## 713242

**Error Message** %ASA-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.

**Explanation** The security appliance has detected a request to start an IKE rekey for a tunnel configured to use Hybrid Xauth, but the rekey was not started. The security appliance will wait for the client to detect and initiate an IKE rekey.

**Recommended Action** None.

## 713243

**Error Message** %ASA-4-713243: *META-DATA* Unable to find the requested certificate

**Explanation** The IKE peer requested a certificate from the cert-req payload. However, no valid identity certificate was issued by the requested DN was found.

**Recommended Action** Perform the following steps:

1. Check the identity certificates.
2. Enroll or import the desired certificate.
3. Enable certificate debugging for more details.

## 713244

**Error Message** %ASA-4-713244: *META-DATA* Received Legacy Authentication Method(LAM) type *type* is different from the last type received *type*.

*type*—The LAM type.

**Explanation** The LAM attribute type received differs from the last type received. The type must be consistent throughout the user authentication process. The user authentication process cannot proceed and the VPN connection will not be established.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

## 713245

**Error Message** %ASA-4-713245: *META-DATA* Unknown Legacy Authentication Method(LAM) type *type* received.

**Explanation** An unsupported LAM type was received during the CRACK challenge/response user authentication process. The user authentication process cannot proceed and the VPN connection will not be established.

*type*—The LAM type.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

## 713246

**Error Message** %ASA-4-713246: *META-DATA* Unknown Legacy Authentication Method(LAM) attribute type *type* received.

**Explanation** The device received an unknown LAM attribute type, which should not cause connectivity problems but might affect the functionality of the peer.

*type*—The LAM attribute type.

**Recommended Action** None.

## 713247

**Error Message** %ASA-4-713247: *META-DATA* Unexpected error: in Next Card Code mode while not doing SDI.

**Explanation** An unexpected error occurred during state processing.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

## 713248

**Error Message** %ASA-5-713248: *META-DATA* Rekey initiation is being disabled during CRACK authentication.

**Explanation** When an IKE SA is negotiated using the CRACK authentication method, Phase 1 SA rekey timer at the headend expired before a successful rekey. Because the remote client is always the initiator of the exchange when using the CRACK authentication method, the headend will not initiate the rekey. Unless the remote peer initiates a successful rekey before the IKE SA expires, the connection will come down upon IKE SA expiration.

**Recommended Action** None.



## 713249

**Error Message** %ASA-4-713249: *META-DATA* Received unsupported authentication results:  
*result*

**Explanation** While negotiating an IKE SA using the CRACK authentication method, the IKE subsystem received a result that is not supported during CRACK authentication from the authentication subsystem. The user authentication fails and the VPN connection is torn down.

*result*—The result returned from the authentication subsystem.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

## 713250

**Error Message** %ASA-5-713250: *META-DATA* Received unknown Internal Address attribute:  
*attribute*

**Explanation** The device received a request for an Internal Address attribute that is not recognizable. The attribute might be valid, but not currently supported or the peer might be sending an illegal value. This should not cause connectivity problems but might affect the functionality of the peer.

**Recommended Action** None.

## 713251

**Error Message** %ASA-4-713251: *META-DATA* Received authentication failure message

**Explanation** The device received a notify message indicating authentication failure while an IKE SA is negotiated using the CRACK authentication method. The connection is torn down.

**Recommended Action** None.

## 713252

**Error Message** %ASA-vpn-5-713252: Group = *group*, Username = *user*, IP = *ip*, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.

**Explanation** When the group policy is configured to require the client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator depending on the fail policy configured. If the fail policy is to reject the client connection, this syslog message is generated when a Zonelab Integrity Server is not connected to the security appliance at the time the client is connecting.

*group*—The tunnel group to which the remote access user is connecting.

*user*—The remote access user.

*ip*—The IP address of the remote access user.

**Recommended Action** Check that the configurations on the concentrator and the Zonelab Integrity Server match. Then verify communication between the concentrator and the Zonelab Integrity Server.

## 713253

**Error Message** %ASA-vpn-5-713253: Group = *group*, Username = *user*, IP = *ip*, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.

**Explanation** When the group policy is configured to require a client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator, depending on the fail policy configured. If the fail policy is to accept the client connection, and provides unrestricted network access, this syslog message is generated when a Zonelab Integrity Server is not connected to the security appliance at the time the client is connecting.

*group*—The tunnel group to which the remote access user is connecting.

*user*—The remote access user.

*ip*—The IP address of the remote access user.

**Recommended Action** Check that the configurations on the security device and the Zonelab Integrity Server match, and verify communication between the security appliance and the Zonelab Integrity Server.

## 713900

**Error Message** %PIX|ASA-7-713900: *Descriptive\_event\_string*.

**Explanation** A message with several possible text strings describing a serious event or failure.

**Recommended Action** Copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

## 713901

**Error Message** %PIX|ASA-7-713901: *Descriptive\_event\_string*.

**Explanation** Message with several possible text strings describing an error which has occurred. This may be the result of configuration error on the headend or remote access client. The event string provides details about the error that occurred.

**Recommended Action** You may need to troubleshoot the to determine what caused the error. Check the **isakmp** and **crypto map** configuration on both peers.

## 713902

**Error Message** %PIX|ASA-3-713902 *descriptive\_event\_string*

**Explanation** This system log message could have several possible text strings describing an error. This may be the result of a configuration error either on the headend or remote access client.

**Recommended Action** It might be necessary to troubleshoot the configuration to determine the cause of the error. Check the ISAKMP and crypto map configuration on both peers.

## 713903

**Error Message** %PIX|ASA-4-713903:*descriptive\_event\_string*.

**Explanation** Syslog with several possible text strings providing a warning. This may be the result of unexpected behavior of a peer (for example, loss of connectivity)

**Recommended Action** Informational only.

## 713904

**Error Message** %PIX|ASA-5-713904:*descriptive\_event\_string*.

**Explanation** Syslog with several possible text strings describing some general status information. These messages are used to keep track of events that have occurred.

**Recommended Action** Informational only.

## 714001

**Error Message** %PIX|ASA-7-714001: *description\_of\_event\_or\_packet*

**Explanation** Description of IKE protocol event or packet.

**Recommended Action** Informational only.

## 714002

**Error Message** %PIX|ASA-7-714002: IKE Initiator starting QM: msg id = *message\_number*

**Explanation** The security appliance has sent the first packet of the Quick mode exchange as the Phase 2 initiator.

**Recommended Action** Informational only.

## 714003

**Error Message** %PIX|ASA-7-714003: IKE Responder starting QM: msg id = *message\_number*

**Explanation** The security appliance has received the first packet of the Quick mode exchange as the Phase 2 responder.

**Recommended Action** Informational only.

## 714004

**Error Message** %PIX|ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = *message\_number*

**Explanation** Protocol decode of the first Quick Mode packet.

**Recommended Action** Informational only.

## 714005

**Error Message** %PIX|ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = *message\_number*

**Explanation** Protocol decode of the second Quick Mode packet.

**Recommended Action** Informational only.

## 714006

**Error Message** %PIX|ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = *message\_number*

**Explanation** Protocol decode of the third Quick Mode packet.

**Recommended Action** Informational only.

## 714007

**Error Message** %PIX|ASA-7-714007: IKE Initiator sending Initial Contact

**Explanation** The security appliance is building and sending the initial contact payload.

**Recommended Action** Informational only.

## 714011

**Error Message** %PIX|ASA-7-714011: *Description of received ID values*

**Explanation** Received the displayed ID information during the negotiation.

**Recommended Action** Informational only.

## 715001

**Error Message** %PIX|ASA-7-715001: *Descriptive statement*

**Explanation** This message provides a description of an event or problem encountered by the security appliance.

**Recommended Action** The action depends on the description.

## 715004

**Error Message** %PIX|ASA-7-715004: subroutine *name()* Q Send failure: RetCode (*return\_code*)

**Explanation** This message indicates that there was an internal error when attempting to put messages in a queue.

**Recommended Action** This is often a benign condition but if the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 715005

**Error Message** %PIX|ASA-7-715005: subroutine *name*() Bad message code: Code (*message\_code*)

**Explanation** This message indicates that an internal subroutine received a bad message code.

**Recommended Action** This is often a benign condition but if the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information

## 715006

**Error Message** %PIX|ASA-7-715006: IKE got SPI from key engine: SPI = *SPI\_value*

**Explanation** This message indicates that the IKE subsystem received an SPI value from IPsec.

**Recommended Action** None.

## 715007

**Error Message** %PIX|ASA-7-715007: IKE got a KEY\_ADD msg for SA: SPI = *SPI\_value*

**Explanation** This message indicates that IKE has completed tunnel negotiation and has successfully loaded the appropriate encryption and hashing keys for IPsec use.

**Recommended Action** None.

## 715008

**Error Message** %PIX|ASA-7-715008: Could not delete SA *SA\_address*, refCnt = *number*, caller = *calling\_subroutine\_address*

**Explanation** This message indicates that the calling subroutine could not delete the IPsec SA. This could indicate a reference count problem.

**Recommended Action** If the number of stale SAs grows as a result of this event, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information

## 715009

**Error Message** %PIX|ASA-7-715009: IKE Deleting SA: Remote Proxy *IP\_address*, Local Proxy *IP\_address*

**Explanation** This message indicates that SA is being deleted with the listed proxy addresses.

**Recommended Action** None.

## 715013

**Error Message** %PIX|ASA-7-715013: Tunnel negotiation in progress for destination *IP\_address*, discarding data

**Explanation** This message indicates that IKE is in the process of establishing a tunnel for this data. All packets to be protected by this tunnel will be dropped until the tunnel is fully established.

**Recommended Action** None.

## 715019

**Error Message** %PIX|ASA-7-715019: IKEGetUserAttributes: Attribute name = *name*

**Explanation** This message displays the *modcfg* attribute name and value pair being processed by the security appliance.

**Recommended Action** None.

## 715020

**Error Message** %PIX|ASA-7-715020: construct\_cfg\_set: Attribute name = *name*

**Explanation** This message displays the *modcfg* attribute name and value pair being transmitted by the security appliance.

**Recommended Action** None.

## 715021

**Error Message** %PIX|ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

**Explanation** This message indicates that quick mode processing is being delayed until all Phase 1 processing has been completed (transaction mode, etc.).

**Recommended Action** None.

## 715022

**Error Message** %PIX|ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

**Explanation** This message indicates that Phase 1 processing has completed and quick mode is being resumed.

**Recommended Action** None.

## 715027

**Error Message** %PIX|ASA-7-715027: IPSec SA Proposal # *chosen\_proposal*, Transform # *chosen\_transform* acceptable Matches global IPSec SA entry # *crypto\_map\_index*

**Explanation** This message appears when the indicated IPSec SA proposal and transform were selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

**Recommended Action** None.

## 715028

**Error Message** %PIX|ASA-7-715028: IKE SA Proposal # 1, Transform # *chosen\_transform* acceptable Matches global IKE entry # *crypto\_map\_index*

**Explanation** This message appears when the indicated IKE SA transform was selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

**Recommended Action** None.



## 715033

**Error Message** %PIX|ASA-7-715033: Processing CONNECTED notify (MsgId *message\_number*)

**Explanation** This message indicates that the security appliance is processing a message containing a notify payload with notify type CONNECTED (16384). The CONNECTED notify is used to complete the commit bit processing and should be included in the fourth overall quick mode packet, which is sent from the responder to the initiator.

**Recommended Action** None.

## 715034

**Error Message** %PIX|ASA-7-715034: *action* IOS keep alive payload: proposal=*time 1*/*time 2* sec.

**Explanation** This message indicates that processing for sending/receiving a keepalive payload message is being performed.

**Recommended Action** None.

## 715035

**Error Message** %PIX|ASA-7-715035: Starting IOS keepalive monitor: *seconds* sec.

**Explanation** This message indicates that the keepalive timer will monitor for a variable number of seconds for keepalive messages.

**Recommended Action** None.

## 715036

**Error Message** %PIX|ASA-7-715036: Sending keep-alive of type *notify\_type* (seq number *number*)

**Explanation** This message indicates that processing for sending a keepalive notify message is being performed.

**Recommended Action** None.

## 715037

**Error Message** %PIX|ASA-7-715037: Unknown IOS Vendor ID version: *major.minor.variance*

**Explanation** This message indicates that we do not know the capabilities of this version of IOS.

**Recommended Action** There may be interoperability issues with features like IKE keepalives. If this results in this type of interoperability problem, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information along with the software version information for both IOS and the security appliance.

## 715038

**Error Message** %PIX|ASA-7-715038: *action Spoofing\_information* Vendor ID payload (version: *major.minor.variance*, capabilities: *value*)

**Explanation** This message indicates that processing for the IOS Vendor ID payload has been performed. The message being performed could be Altiga spoofing IOS.

**Recommended Action** None.

## 715039

**Error Message** %PIX|ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.

**Explanation** This message indicates that there was an entry in the IKE tunnel table that was never removed when the SA was freed. This indicates a bug in the state machine.

**Recommended Action** If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support, and provide the gathered information.

## 715040

**Error Message** %PIX|ASA-7-715040: Deleting active auth handle during SA deletion:  
handle = *internal\_authentication\_handle*

**Explanation** This message indicates that the auth handle was still active during SA deletion. This is part of cleanup recovery during the error condition.

**Recommended Action** None.

## 715041

**Error Message** %PIX|ASA-7-715041: Received keep-alive of type *keepalive\_type*, not the negotiated type

**Explanation** This indicates that a keep-alive of the type indicated in the message was received unexpectedly.

**Recommended Action** Check keepalive configuration on both peers.

## 715042

**Error Message** %PIX|ASA-7-715042: IKE received response of type *failure\_type* to a request from the *IP\_address* utility

**Explanation** This indicates that a request for an IP address for a remote access client from the internal utility that provides these addresses could not be satisfied. Variable text in the message string indicates more specifically what went wrong.

**Recommended Action** Check IP address assignment configuration and adjust accordingly.

## 715044

**Error Message** %PIX|ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability

**Explanation** Received IOS Keepalive payload from vendor without KA capabilities set. Payload is ignored.

**Recommended Action** Informational only.

## 715045

**Error Message** %PIX|ASA-7-715045: ERROR: malformed Keepalive payload

**Explanation** Malformed Keepalive payload received. Payload is ignored.

**Recommended Action** Informational only.

## 715046

**Error Message** %PIX|ASA-7-715046: constructing *payload\_description* payload

**Explanation** Displays details about the IKE payload being constructed.

**Recommended Action** Informational only.

## 715047

**Error Message** %PIX|ASA-7-715047: processing *payload\_description* payload

**Explanation** Displays details about the IKE payload received and being processed.

**Recommended Action** Informational only.

## 715048

**Error Message** %PIX|ASA-7-715048: Send *VID\_type* VID

**Explanation** Displays type of Vendor ID payload being sent.

**Recommended Action** Informational only.

## 715049

**Error Message** %PIX|ASA-7-715049: Received *VID\_type* VID

**Explanation** Displays type of Vendor ID payload received.

**Recommended Action** Informational only.

## 715050

**Error Message** %PIX|ASA-7-715050: Claims to be IOS but failed authentication

**Explanation** Looks like IOS VID but doesn't match *hmac\_sha*.

**Recommended Action** Check Vendor ID configuration on both peers. If this issue affects interoperability, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 715051

**Error Message** %PIX|ASA-7-715051: Received unexpected TLV type *TLV\_type* while processing FWTYPE ModeCfg Reply

**Explanation** An unknown TLV was received in a security appliance record while a FWTYPE ModeCfg Reply was being processed. This will be discarded. This could occur either because of packet corruption or because the connecting client supports a later version of the security appliance protocol.

**Recommended Action** Check the personal FW installed on the Cisco VPN Client and the Personal FW configuration on the security appliance. This may also indicate a version mismatch between the VPN Client and the security appliance.

## 715052

**Error Message** %PIX|ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries

**Explanation** The old P1 SA is being deleted but it has no new SA to transition to since it was marked for deletion as well. This generally indicates that the 2 IKE peers are out of synchronization and may be using different rekey times. The problem should correct itself but there may be some small amount of data loss until a fresh P1 SA is reestablished.

**Recommended Action** Informational only.

## 715053

**Error Message** %PIX|ASA-7-715053: MODE\_CFG: Received request for *attribute\_info!*

**Explanation** Received a mode configuration message requesting the specified attribute.

**Recommended Action** Informational only.

## 715054

**Error Message** %PIX|ASA-7-715054: MODE\_CFG: Received *attribute\_name* reply: *value*

**Explanation** Received a mode configuration reply message from the remote peer.

**Recommended Action** Informational only.

## 715055

**Error Message** %PIX|ASA-7-715055: Send *attribute\_name*

**Explanation** Sent a mode configuration message to the remote peer.

**Recommended Action** Informational only.

## 715056

**Error Message** %PIX|ASA-7-715056: Client is configured for *TCP\_transparency*

**Explanation** Since the remote end (client) is configured for IPsec Over TCP, the headend security appliance must not negotiate IPsec Over UDP or IPsec over NAT-T with the client.

**Recommended Action** May require adjustment to the NAT transparency configuration of one of the peers if the tunnel does not come up. Otherwise this is an informational message.

## 715057

**Error Message** %PIX|ASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPsec-over-UDP configuration.

**Explanation** IPsec-over-UDP Mode Config info will not be exchanged because NAT-Traversal was detected.

**Recommended Action** Informational only.

## 715058

**Error Message** %PIX|ASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.

**Explanation** The remote end didn't provide NAT-D payloads required for NAT-Traversal after exchanging NAT-Traversal VIDs. At least two NAT-D payloads must be received.

**Recommended Action** This may indicate a non-conforming NAT-T implementation. If the offending peer is a Cisco product, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information along with product numbers and software versions. If the offending peer is not a Cisco product, then contact the manufacturer support team.

## 715059

**Error Message** %PIX|ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal

**Explanation** Need to use these modes instead of the usual Transport and Tunnel modes defined in the SA to successfully negotiate NAT-Traversal

**Recommended Action** Informational only.

## 715060

**Error Message** %PIX|ASA-7-715060: Dropped received IKE fragment. Reason: *reason*

**Explanation** The reason for dropping the fragment will be shown.

**Recommended Action** Depends on the drop reason but could indicate a problem with an intervening NAT device or a non-conforming peer.

## 715061

**Error Message** %PIX|ASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.

**Explanation** This could be either a resend of the same packet but fragmented to a different MTU, or another packet altogether.

**Recommended Action** Informational only.

## 715062

**Error Message** %PIX|ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.

**Explanation** There is a gap in fragment numbers.

**Recommended Action** This could indicate a network problem. If the condition results in dropped tunnels or prevents certain peers from negotiating with the security appliance, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information along with product numbers and software versions.

## 715063

**Error Message** %PIX|ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!

**Explanation** Assembly for a fragmented pkt that was rcv'd was successful

**Recommended Action** Informational only.

## 715064

**Error Message** %PIX|ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: *true/false* Aggressive Mode: *true/false*

**Explanation** Peer supports IKE fragmentation based on the info provided in the message.

**Recommended Action** Informational only.

## 715065

**Error Message** %PIX|ASA-7-715065: IKE *state\_machine subtype* FSM error history (struct *data\_structure\_address*) *state, event: state/event* pairs

**Explanation** A phase 1 error occurred and the *state, event* history pairs will be displayed in reverse chronological order.

**Recommended Action** Most of these errors are benign. If these messages are associated with undesirable behavior, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 715066

**Error Message** %PIX|ASA-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.

**Explanation** The logical ID in the IKE SA is NULL. The phase II negotiation will be torn down.

**Recommended Action** An internal error has occurred. If the device does not recover and operate normally, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.



## 715067

**Error Message** %PIX|ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa

**Explanation** The LAN-TO-LAN SA that is being established already exists, in other words, an SA with the same remote networks, but is sourced from a different peer. This new SA will be deleted since this is not a legal configuration.

**Recommended Action** Check the LAN-TO-LAN configuration on all associated peers. Specifically, multiple peers should not be sharing private networks.

## 715068

**Error Message** %PIX|ASA-7-715068: QM IsRekeyed: duplicate sa found by *address*, deleting old sa

**Explanation** The remote access SA that is being established already exists, in other words, an SA with the same remote networks, but is sourced from a different peer. The old SA will be deleted, since the peer may simply have changed its IP address.

**Recommended Action** This may be a benign condition, especially if a Client tunnel was terminated abruptly. If the message is associated with undesirable behavior then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 715069

**Error Message** %PIX|ASA-7-715069: Invalid ESP SPI size of *SPI\_size*

**Explanation** Received an IPSec SA proposal with an invalid ESP SPI size. This proposal will be skipped.

**Recommended Action** Generally, this is a benign condition but could indicate that a peer may be non-conforming. If the problem persists and prevents peers from negotiating a tunnel successfully, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 715070

**Error Message** %PIX|ASA-7-715070: Invalid IPComp SPI size of SPI\_size

**Explanation** Received an IPsec SA proposal with an invalid IPComp SPI size. This proposal will be skipped.

**Recommended Action** Generally, this is a benign condition but could indicate that a peer is non-conforming. If the problem persists and prevents peers from negotiating a tunnel successfully, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 715071

**Error Message** %PIX|ASA-7-715071: AH proposal not supported

**Explanation** IPsec AH proposal is not supported. This proposal will be skipped.

**Recommended Action** Informational only.

## 715072

**Error Message** %PIX|ASA-7-715072: Received proposal with unknown protocol ID  
*protocol\_ID*

**Explanation** Received an IPsec SA proposal with unknown protocol ID. This proposal will be skipped.

**Recommended Action** Generally, this is a benign condition but could indicate that a peer is non-conforming. If the problem persists and prevents peers from negotiating a tunnel successfully, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 715074

**Error Message** %PIX|ASA-7-715074: Could not retrieve authentication attributes for  
peer *IP\_address*

**Explanation** Could not get authorization information for the remote user.

**Recommended Action** Ensure that all authentication and authorization configuration is set correctly. If the problem persists and prevents peers from negotiating a tunnel successfully, then copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 715075

**Error Message** %PIX|ASA-7-715075: Group = *group\_name*, Username = *client*, IP = *IP\_address*  
Received keep-alive of type *message\_type* (seq number *number*)

**Explanation** This new message is in pair with 715036 “DPD R-U-THERE” message which logs the DPD sending messages.

Two possible cases:

- 1) received peer sending “DPD R-U-THERE” message
- 2) received peer reply “DPD R-U-THERE-ACK” message

The user is recommended to observe the following:

Case 1—The “DPD R-U-THERE” is received and its sequence number matches with the outgoing DPD reply message's.

If f1 sends a “DPD R-U-THERE-ACK” without prior receiving “DPD R-U-THERE” from peer, it is likely experiencing security breach.

Case 2—The received “DPD R-U-THERE-ACK” message's sequence number is matched with previous sending DPD message's.

If f1 did not receive a “DPD R-U-THERE-ACK” for a reasonable time lap after sending “DPD R-U-THERE” to peer, the tunnel is most likely down.

*group\_name*—The peer's VPN group name.

*client*—The peer's username.

*IP\_address*—IP address of the VPN peer.

*message\_type*—The message type (“DPD R-U-THERE” or “DPD R-U-THERE-ACK”).

*number*—The DPD sequence number.

**Recommended Action** No action required from user.

## 715076

**Error Message** %PIX|ASA-7-715076: Computing hash for ISAKMP

**Explanation** This message is displayed when IKE computes various hash values.

This object will be prepended as follows:

Group = *groupname*, Username = *username*, IP = *ip\_address*, ...

**Recommended Action** None.

## 715077

**Error Message** %PIX|ASA-7-715077: Pitcher: *msg string*, *spi spi*

**Explanation** This message is displayed when various messages are sent to IKE.

*msg\_string* can be one of the following:

- received a key acquire message
- received SPI for non-existent SA
- received key delete msg
- received KEY\_UPDATE
- received KEY\_REKEY\_IB
- received KEY\_REKEY\_OB
- received KEY\_SA\_ACTIVE
- could not find IKE SA to activate IPSEC (OB)
- could not find IKE SA to rekey IPSEC (OB)
- KEY\_SA\_ACTIVE no centry found
- KEY\_ADD centry not found
- KEY\_UPDATE centry not found

Like other ISAKMP, the following statement applies:

This object will be prepended as follows:

Group = *groupname*, Username = *username*, IP = *ip\_address*, ...

**Recommended Action** None required

## 715078

**Error Message** %PIX-7-715078: *META-DATA* Received *type* LAM attribute.

**Explanation** The debug message displayed when processing a LAM attribute.

*type*—The LAM attribute type.

**Recommended Action** None.

## 715079

**Error Message** %PIX-7-715079: *META-DATA* INTERNAL\_ADDRESS: Received request for *type*.

**Explanation** The debug message that displays when processing an internal address payload.  
*type*—The internal address request type.

**Recommended Action** None.

## 715080

**Error Message** %PIX-vpn-7-715080: Starting P1 rekey timer: 86400 seconds.

**Error Message** %PIX-vpn-7-715080: Restarting P1 rekey timer: 86400 seconds.

**Error Message** %ASA-vpn-7-715080: Starting P2 rekey timer: 28800 seconds.

**Explanation** The IKE (P1) Phase 1 or IPSec (P2) Phase 2 rekey timers have been started or restarted. When an IKE (P1) or IPSec (P2) tunnel is connected, timers are created to determine when the next rekey will occur. These messages show what the timers are set to.

**Recommended Action** None.

## 716001

**Error Message** %ASA-6-716001: Group *group* User *user* WebVPN session started.

**Explanation** The WebVPN session has started for the *user* in this *group*. When the user logs in via the WebVPN login page, the WebVPN session starts.

**Recommended Action** None.

## 716002

**Error Message** %ASA-6-716002: Group *group* User *user* WebVPN session terminated: *reason*.

**Explanation** The WebVPN session has terminated for a specific reason. Possible reasons include:

- User Requested
- Lost Carrier
- Lost Service
- Idle Timeout

- Max time exceeded
- Administrator Reset
- Administrator Reboot
- Administrator Shutdown
- Port Error
- NAS Error
- NAS Request
- NAS Reboot
- Port unneeded
- Port Preempted
- Port Suspended
- Service Unavailable
- Callback
- User error
- Host Requested
- Bandwidth Management Error
- ACL parse error
- Unknown

**Recommended Action** Unless the *reason* indicates a problem, then no action is required.

## 716003

**Error Message** %ASA-6-716003: Group *group* User *user* WebVPN access GRANTED:: *url*

**Explanation** The WebVPN *user* in this *group* has been granted access to this *url*. The user's access to various locations can be controlled using WebVPN-specific access control lists.

**Recommended Action** None.

## 716004

**Error Message** %ASA-6-716004: Group *group* User *user* WebVPN access DENIED to specified location: *url*

**Explanation** The WebVPN *user* in this *group* has been denied access to this *url*. The WebVPN user's access to various locations can be controlled using WebVPN-specific access control lists. In this case, a particular access control list entry is denying access to this *url*.

**Recommended Action** None.

## 716005

**Error Message** %ASA-6-716005: Group *group* User *user* WebVPN ACL Parse Error: *reason*

**Explanation** The ACL for the WebVPN user in the specified group failed to parse correctly. The reason for the error is reported.

The WebVPN access control list for the *user* in this *group* did not parse correctly. The reason for the error is reported.

**Recommended Action** Fix the WebVPN ACL.

## 716006

**Error Message** %ASA-6-716006: Group *name* User *user* WebVPN session terminated. Idle timeout.

**Explanation** The WebVPN session was not created for this user in the specified group because the VPN tunnel protocol is not set to WebVPN.

**Recommended Action** None.

## 716007

**Error Message** %ASA-4-716007: Group *group* User *user* WebVPN Unable to create session.

**Explanation** The WebVPN session was not created for the in the specified group because of resource issues. For example, the user may have reached the maximum login limit.

**Recommended Action** None.

## 716008

**Error Message** %ASA-7-716008: WebVPN ACL: *action*

**Explanation** The WebVPN ACL has begun performing an *action*. For example, the *action* could be “begin parsing.” This is a debug level message.

**Recommended Action** None.

## 716009

**Error Message** %ASA-6-716009: Group *group* User *user* WebVPN session not allowed. WebVPN ACL parse error.

**Explanation** The WebVPN session for the specified user in this group is not allowed because the associated access control list did not parse. The user will not be allowed to login via WebVPN until this error has been rectified.

**Recommended Action** Fix the WebVPN ACL.

## 716010

**Error Message** %ASA-7-716010: Group *group* User *user* Browse network.

**Explanation** The WebVPN user in the specified group browsed the network.

**Recommended Action** None.

## 716011

**Error Message** %ASA-7-716011: Group *group* User *user* Browse domain *domain*.

**Explanation** The WebVPN specified user in this group browsed the specified domain.

**Recommended Action** None.

## 716012

**Error Message** %ASA-7-716012: Group *group* User *user* Browse directory *directory*.

**Explanation** The specified WebVPN user browsed the specified directory.

**Recommended Action** None.

## 716013

**Error Message** %ASA-7-716013: Group *group* User *user* Close file *filename*.

**Explanation** The specified WebVPN user closed the specified file.

**Recommended Action** None.



## 716014

**Error Message** %ASA-7-716014: Group *group* User *user* View file *filename*.

**Explanation** The specified WebVPN user viewed the specified file.

**Recommended Action** None.

## 716015

**Error Message** %ASA-7-716015: Group *group* User *user* Remove file *filename*.

**Explanation** The WebVPN user in the specified group removed the specified file.

**Recommended Action** None.

## 716016

**Error Message** %ASA-7-716016: Group *group* User *user* Rename file *old\_filename* to *new\_filename*.

**Explanation** The specified WebVPN user renamed the specified file.

**Recommended Action** None.

## 716017

**Error Message** %ASA-7-716017: Group *group* User *user* Modify file *filename*.

**Explanation** The specified WebVPN user modified the specified file.

**Recommended Action** None.

## 716018

**Error Message** %ASA-7-716018: Group *group* User *user* Create file *filename*.

**Explanation** The specified WebVPN user created the specified file.

**Recommended Action** None.

## 716019

**Error Message** %ASA-7-716019: Group *group* User *user* Create directory *directory*.

**Explanation** The specified WebVPN user created the specified directory.

**Recommended Action** None.

## 716020

**Error Message** %ASA-7-716020: Group *group* User *user* Remove directory *directory*.

**Explanation** The specified WebVPN user removed the specified directory.

**Recommended Action** None.

## 716021

**Error Message** %ASA-7-716021: File access DENIED, *filename*.

**Explanation** The specified WebVPN user was denied access to the specified file.

**Recommended Action** None.

## 716022

**Error Message** %ASA-4-716022: Unable to connect to proxy server *reason*.

**Explanation** The WebVPN HTTP/HTTPS redirect failed for the specified reason.

**Recommended Action** Check HTTP/HTTPS proxy configuration

## 716023

**Error Message** %ASA-4-716023: Group *name* User *user* Session could not be established: session limit of *maximum\_sessions* reached.

**Explanation** The user session cannot be established because the current number of sessions exceeds the maximum session load.

**Recommended Action** Increase the configured limit, if possible, to create a load-balanced cluster.

## 716024

**Error Message** %ASA-7-716024: Group *name* User *user* Unable to browse the network. Error: *description*

**Explanation** The user was unable to browse the Windows network via the CIFS protocol as indicated by the description. For example, “Unable to contact necessary server” indicates that the remote server is unavailable or unreachable. This could be a transient condition or may require further troubleshooting.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

## 716025

**Error Message** %ASA-7-716025: Group *name* User *user* Unable to browse domain *domain*. Error: *description*

**Explanation** The user was unable to browse the remote domain via the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

## 716026

**Error Message** %ASA-7-716026: Group *name* User *user* Unable to browse directory *directory*. Error: *description*

**Explanation** The user was unable to browse the remote directory via the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

## 716027

**Error Message** %ASA-7-716027: Group *name* User *user* Unable to view file *filename*. Error: *description*

**Explanation** The user was unable to view the remote file via the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

## 716028

**Error Message** %ASA-7-716028: Group *name* User *user* Unable to remove file *filename*.  
Error: *description*

**Explanation** The user was unable to remove the remote file via the CIFS protocol. This error is probably caused by lack of permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

## 716029

**Error Message** %ASA-7-716029: Group *name* User *user* Unable to rename file *filename*.  
Error: *description*

**Explanation** The user was unable to rename the remote file via the CIFS protocol. This error was probably caused by lack of permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

## 716030

**Error Message** %ASA-7-716030: Group *name* User *user* Unable to modify file *filename*.  
Error: *description*

**Explanation** A problem occurred when a user attempted to modify an existing file via the CIFS protocol. This error was probably caused by a lack of permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

## 716031

**Error Message** %ASA-7-716031: Group *name* User *user* Unable to create file *filename*.  
Error: *description*

**Explanation** A problem occurred when a user attempted to create a file via the CIFS protocol. This error was probably caused by a permissions problem.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

## 716032

**Error Message** %ASA-7-716032: Group *name* User *user* Unable to create folder *folder*.  
Error: *description*

**Explanation** A problem occurred when a user attempted to create a folder via the CIFS protocol. This error was probably caused by a permissions problem.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check file permissions.

## 716033

**Error Message** %ASA-7-716033: Group *name* User *user* Unable to remove folder *folder*.  
Error: *description*

**Explanation** A problem occurred when a user of the CIFS protocol attempted to remove a folder. This error probably occurred because of a permissions problem or a problem communicating with the server on which the file resides.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

## 716034

**Error Message** %ASA-7-716034: Group *name* User *user* Unable to write to file *filename*.

**Explanation** A problem occurred when a user attempted to write to a file via the CIFS protocol. This error was probably caused by a permissions problem or a problem communicating with the server on which the file resides.

**Recommended Action** None.

## 716035

**Error Message** %ASA-7-716035: Group *name* User *user* Unable to read file *filename*.

**Explanation** A problem occurred when a user of the CIFS protocol attempted to read a file. This error was probably caused by a permissions problem.

**Recommended Action** Check the file permissions.

## 716036

**Error Message** %ASA-7-716036: Group *name* User *user* File Access: User *user* logged into the *server* server.

**Explanation** A user successfully logged into the server via the CIFS protocol

**Recommended Action** None.

## 716037

**Error Message** %ASA-7-716037: Group *name* User *user* File Access: User *user* failed to login into the *server* server.

**Explanation** A user attempted to log in to a server via the CIFS protocol but was not successful.

**Recommended Action** Verify that the user entered the correct user name and password.

## 716038

**Error Message** %ASA-6-716038: Authentication: successful, group = *name* user = *user*, Session Type: WebVPN

**Explanation** Before a WebVPN session can begin the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+).

**Recommended Action** None.

## 716039

**Error Message** %ASA-6-716039: Authentication: rejected, group = *name* user = *user*,  
Session Type: WebVPN

**Explanation** Before a WebVPN session starts, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+). In this case, the user credentials (user name and password) either did not match or the user does not have permission to start a WebVPN session.

**Recommended Action** Verify the user credentials on the local or remote server. Verify that WebVPN is configured for the user.

## 716040

**Error Message** %ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.

**Explanation** A user was unable to log in to WebVPN because the system is in the process of rebooting.

**Recommended Action** None.

## 716041

**Error Message** %ASA-6-716041: access-list *acl\_ID* action url url hit\_cnt count

**Explanation** The WebVPN URL access control list named *acl\_ID* has been hit *count* times for location *url* whose *action* is “permitted” or “denied.”

**Recommended Action** None.

## 716042

**Error Message** %ASA-6-716042: access-list *acl\_ID* action tcp source\_interface/source\_address  
(source\_port) -> dest\_interface/dest\_address(dest\_port) hit\_cnt count

**Explanation** The WebVPN TCP access control list named *acl\_ID* has been hit *count* times for packet received on source interface *source\_interface*/source\_address port *source\_port* forwarded to *dest\_interface*/dest\_address destination *dest\_port* whose *action* is “permitted” or “denied.”

**Recommended Action** None.

## 716043

**Error Message** %ASA-6-716043 Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Port Forwarding Java applet started. Created new hosts file mappings.

**Explanation** The user has launched a TCP port forwarding applet from a WebVPN session.

*group-name*—Group name associated with session.

*user-name*—User name associated with session.

*IP\_address*—Source IP address associated with session.

**Recommended Action** None.

## 716044

**Error Message** %ASA-4-716044: Group *group-name* User *user-name* IP *IP\_address* AAA parameter *param-name* value *param-value* out of range.

**Explanation** The given parameter has a bad value.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

*param-name*—The name of the parameter.

*param-value*—The value of the parameter.

**Recommended Action** Modify the configuration to correct the indicated parameter.

## 716045

**Error Message** %ASA-4-716045: Group *group-name* User *user-name* IP *IP\_address* AAA parameter *param-name* value invalid.

**Explanation** The given parameter has a bad value. The value is not shown as it might be very long.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

*param-name*—The name of the parameter.

**Recommended Action** Modify the configuration to correct the indicated parameter.



## 716046

**Error Message** %ASA-4-716046: Group *group-name-name* User *user-name* IP *IP\_address* User ACL *access-list-name* from AAA doesn't exist on the device, terminating connection.

**Explanation** The specified access list was not found on the device.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

*access-list-name*—The name of the access list.

**Recommended Action** Modify the configuration to add the specified access list or to correct the access list name.

## 716047

**Error Message** %ASA-4-716047: Group *group-name* User *user-name* IP *IP\_address* User ACL *access-list* from AAA ignored, AV-PAIR ACL used instead.

**Explanation** The specified access list was not used because a Cisco AV-PAIR access list was used.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

*access-list-name*—The name of the access list.

**Recommended Action** Determine the correct access list to use and correct the configuration.

## 716048

**Error Message** %ASA-4-716048: Group *group-name* User *user-name* IP *IP\_address* No memory to parse ACL.

**Explanation** There was not enough memory to parse the access list.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

## 716049

**Error Message** %ASA-6-716049: Group *group-name* User *user-name* IP *IP\_address* Empty SVC ACL.

**Explanation** The access list to be used by the client was empty.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

**Recommended Action** Determine the correct access list to use and modify the configuration.

## 716050

**Error Message** %ASA-6-716050: Error adding to ACL: *ace\_command\_line*

**Explanation** The access control entry had a syntax error.

*ace\_command\_line*—The access control entry that is causing the error.

**Recommended Action** Correct the downloadable access list configuration.

## 716051

**Error Message** %ASA-6-716051: Group *group-name* User *user-name* IP *IP\_address* Error adding dynamic ACL for user.

**Explanation** There is not enough memory to perform the action.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device .

## 716052

**Error Message** %ASA-4-716052: Group *group-name* User *user-name* IP *IP\_address* Pending session terminated.

**Explanation** A user did not complete login and the pending session was terminated.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

**Recommended Action** This may be due to an SSL VPN client (SVC) that is unable to connect. Check the user PC for SVC compatibility.

## 716053

**Error Message** %ASA-5-716053: New SSO Server added: name: *name* Type: *type*

**Explanation** The Single Sign-On (SSO) server name of the specified type has been configured.

*name*—The name of the server.

*type*—The type of the server. Currently, the only server type is SiteMinder.

**Recommended Action** None.

## 716054

**Error Message** %ASA-5-716054: SSO Server deleted: name: *name* Type: *type*

**Explanation** The SSO server name of the specified type has been removed from the configuration.

*name*—The name of the server.

*type*—The type of the server. Currently, the only server type is SiteMinder.

**Recommended Action** None.

## 716055

**Error Message** %ASA-6-716055: Group *group-name* User *user-name* IP *IP\_address*  
Authentication to SSO server name: *name* type *type* succeeded

**Explanation** The WebVPN user has been successfully authenticated to the SSO server.

*group-name*—The group name.

*user-name*—The user name.

*IP\_address*—The IP address of the server.

*name*—The name of the server.

*type*—The type of the server. Currently, the only server type is SiteMinder.

**Recommended Action** None.

## 716056

**Error Message** %ASA-3-716056: Group *group-name* User *user-name* IP *IP\_address*  
Authentication to SSO server name: *name* type *type* failed reason: *reason*

**Explanation** The WebVPN user failed to authenticate to the SSO server.

*group-name*—The group name.

*user-name*—The user name.

*IP\_address*—The IP address of the server.

*name*—The name of the server.

*type*—The type of the server. Currently, the only server type is SiteMinder.

*reason*—The reason for the authentication failure.

**Recommended Action** Either the user or the security appliance administrator need to correct the problem, depending on the reason for the failure.

## 716090

**Error Message** %ASA-webvpn-6-716090: Group *group-policy*, User *user-name*, IP *IP\_address*:  
Secure Desktop Results: PLATFORM/FEATURE = *platform* & *feature*, PC\_LOCATION =  
*location\_name*, PC\_OS\_DETECTED = *OS\_name*, PC\_AV\_DETECTED = *antivirus\_software*,  
PC\_FW\_DETECTED = *firewall\_name*, PC\_AS\_DETECTED = *antispyware\_name*

**Explanation** Identifies the configuration of the remote PC on which secure desktop is being installed, including the type of platform, operating system, firewall, antivirus software, and anti-spyware software.

*group-policy*—The name of the group policy.

*user-name*—The name of the user.

*IP\_address*—The IP address.

*platform*—The type of platform (WINDOWS\_PC, WINDOWS\_CE, MAC\_LINUX).

*feature*—The feature type (SECURE\_DESKTOP, CACHE\_CLEANER, NONE, FAILURE, NO\_LOCATION\_MATCHED\_FAILURE).

*location\_name*—The name of the location.

*OS\_name*—The name of the operating system.

*antivirus\_software*—The name of the antivirus software.

*firewall\_name*—The name of the firewall.

*antispyware\_name*—The name of the anti-spyware software.

**Recommended Action** None.

## 716091

**Error Message** %ASA-webvpn-6-716091: Group *group-policy*, User *user-name*, IP *IP\_address*: Secure Desktop Results: WEB\_ACCESS = *effective\_permission* == *secure\_desktop\_permission* & *group-policy\_permission*, FILE\_ACCESS = *effective\_permission* == *secure\_desktop\_permission* & *group-policy\_permission*, PORT\_FORWARDING == *effective\_permission* == *secure\_desktop\_permission* & *group-policy\_permission*, SSL\_VPN\_CLIENT = *effective\_permission* == *secure\_desktop\_permission* & *group-policy\_permission*, GROUP\_POLICY = *results*

**Explanation** Identifies the WebVPN feature permissions in effect for the user logging in from the remote PC where secure desktop is being installed. This includes permission for web access, file access, port forwarding, and SSL VPN client. This also indicates the group policy to be used for the user.

*group-policy*—The name of the group policy.

*user-name*—The name of the user.

*IP\_address*—The IP address.

*effective\_permission*—The effective permission (ALLOW or DENY).

*secure\_desktop\_permission*—The Secure Desktop permission (COMPUTER\_ALLOW, COMPUTER\_DENY, COMPUTER\_HI\_SUCCESS, COMPUTER\_HI\_FAILURE).

*group-policy\_permission* = The group policy permission (GROUP\_ALLOW, GROUP\_DENY).

*results*—The results of applying the group policy (SUCCESS, FAILURE).

**Recommended Action** None.

## 717001

**Error Message** %PIX|ASA-3-717001: Querying keypair failed.

**Explanation** A required keypair was not found during an enrollment request.

**Recommended Action** Verify that a valid keypair exists in the trustpoint configuration and resubmit enrollment.

## 717002

**Error Message** %PIX|ASA-3-717002: Certificate enrollment failed for trustpoint *trustpoint\_name*. Reason: *reason\_string*.

**Explanation** An enrollment request for this *trustpoint\_name* trustpoint has failed.

*trustpoint name*—Trustpoint name that the enrollment request was for.

*reason\_string*—The reason the enrollment request failed.

**Recommended Action** Check the Certificate Authority server for failure reason.

## 717003

**Error Message** %PIX|ASA-6-717003: Certificate received from Certificate Authority for trustpoint *trustpoint\_name*.

**Explanation** A certificate was successfully received from the Certificate Authority for this *trustpoint\_name* trustpoint.

**Recommended Action** None

## 717004

**Error Message** %PIX|ASA-6-717004: PKCS #12 export failed for trustpoint *trustpoint\_name*.

**Explanation** Trustpoint *trustpoint\_name* failed to export. It is likely that only a CA certificate exists and an identity certificate doesn't exist for trustpoint or a required keypair is missing.

**Recommended Action** Ensure that required certificates and keypairs are present for the given trustpoint.

## 717005

**Error Message** %PIX|ASA-6-717005: PKCS #12 export succeeded for trustpoint *trustpoint\_name*.

**Explanation** Trustpoint *trustpoint\_name* was successfully exported.

**Recommended Action** None

## 717006

**Error Message** %PIX|ASA-6-717006: PKCS #12 import failed for trustpoint *trustpoint\_name*.

**Explanation** Import of the requested trustpoint *trustpoint\_name* failed to be processed.

**Recommended Action** Ensure the integrity of the imported data and make sure that the entire **pkcs12** record is correctly pasted and resubmit import attempt.

## 717007

**Error Message** %PIX|ASA-6-717007: PKCS #12 import succeeded for trustpoint *trustpoint\_name*.

**Explanation** Import of the requested trustpoint *trustpoint\_name* was successfully completed.

**Recommended Action** None.

## 717008

**Error Message** %PIX|ASA-2-717008: Insufficient memory to *process\_requiring\_memory*.

**Explanation** An internal error occurred while attempting to allocate memory for *process\_requiring\_memory*. Other processes may experience problems allocating memory and prevent further processing.

**Recommended Action** Collect memory statistics and logs for further debugging and reload system.

## 717009

**Error Message** %PIX|ASA-3-717009: Certificate validation failed. Reason: *reason\_string*.

**Explanation** A certificate validation failed due to *reason\_string*. The *reason\_string* specifies the reason for the failure and it could be due to a validation attempt of a revoked certificate, invalid certificate attributes or configuration issues.

*reason\_string*—The reason the certificate validation failed.

**Recommended Action** Ensure configuration has a valid trustpoint configured for validation if the *reason\_string* indicates that no suitable trustpoints are found. Check system time to ensure it is accurate relative to the certificate authority time. Check the *reason\_string* and correct any issues that are indicated.

## 717010

**Error Message** %PIX|ASA-3-717010: CRL polling failed for trustpoint *trustpoint\_name*.

**Explanation** . CRL polling has failed and may cause connections to be denied if CRL checking is required.

*trustpoint\_name*—The name of the trustpoint that requested the CRL.

**Recommended Action** Verify that connectivity with the configured CRL Distribution Point and ensure manual CRL retrieval also functions correctly.

## 717011

**Error Message** %PIX|ASA-2-717011: Unexpected event *event event\_ID*

**Explanation** This log message indicates that an event that is not expected under normal conditions has occurred.

**Recommended Action** Log and notify Cisco TAC of issue.

## 717012

**Error Message** %PIX|ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint *trustpoint\_name* at *time\_of\_failure*

**Explanation** This log message indicates that an attempt to refresh a cached CRL entry has failed for the specified trustpoint *trustpoint\_name*, at the indicated *time\_of\_failure*. This may result in obsolete CRLs on the system that may cause connections that require a valid CRL to be denied.

**Recommended Action** Check connectivity issues to the server including network down, server down, and so on. Try to retrieve the CRL manually using the **crypto ca crl retrieve** command.

## 717013

**Error Message** %PIX|ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: *issuer*

**Explanation** When the device is configured to authenticate IPsec tunnels using digital certificates, Certificate Revocation Lists (CRLs) may be cached in memory to avoid requiring a CRL download during each connection. If the cache fills to the point where an incoming CRL cannot be accommodated, older CRLs will be removed until the required space is made available. This log event will be generated for each CRL that is purged.

**Recommended Action** None.



## 717014

**Error Message** %PIX|ASA-5-717014: Unable to cache a CRL received from *CDP* due to size limitations (CRL size = *size*, available cache space = *space*)

**Explanation** When the device is configured to authenticate IPSec tunnels using digital certificates, Certificate Revocation Lists (CRLs) may be cached in memory to avoid requiring a CRL download during each connection. This log event will be generated if a received CRL is too large to fit in the cache.

**Recommended Action** No action necessary. The large CRLs are still supported even though they are not cached. This means that the CRL will be downloaded with each IPSec connection. This may impact performance during IPSec connection bursts.

## 717015

**Error Message** %PIX|ASA-3-717015: CRL received from *issuer* is too large to process (CRL size = *crl\_size*, maximum CRL size = *max\_crl\_size*)

**Explanation** This log event will be generated when an IPSec connection causes a CRL, that is larger than the maximum permitted CRL size, *max\_crl\_size*, to be downloaded. This is an error condition that will cause the connection to fail. This message is rate limited to one message every 10 seconds.

**Recommended Action** Scalability is perhaps the most significant drawback to the CRL method of revocation checking. The only options to solve this problem are to investigate a Certificate Authority based solution to reduce the CRL size or configure the device not to require CRL validation.

## 717016

**Error Message** %PIX|ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: *issuer*

**Explanation** When the device is configured to authenticate IPSec tunnels using digital certificates, Certificate Revocation Lists (CRLs) may be cached in memory to avoid requiring a CRL download during each connection. This log event is generated when either the CA specified expiration time or the configured cache-time has lapsed and the CRL is removed from the cache.

**Recommended Action** None. This is a routine occurrence.

## 717017

**Error Message** %PIX|ASA-3-717017: Failed to query CA certificate for trustpoint *trustpoint\_name* from *enrollment\_url*

**Explanation** This logs an error that may occur when an attempt is made to authenticate a trustpoint by requesting a CA certificate from a Certificate Authority.

**Recommended Action** Ensure that an enrollment URL is configured with this trustpoint and ensure connectivity with the Certificate Authority server and retry request.

## 717018

**Error Message** %PIX|ASA-3-717018: CRL received from *issuer* has too many entries to process (number of entries = *number\_of\_entries*, maximum number allowed = *max\_allowed*)

**Explanation** This log event will be generated when an IPSec connection causes a CRL, that contains more revocation entries than can be supported, to be downloaded. This is an error condition that will cause the connection to fail. This message is rate limited to one message every 10 seconds.

*issuer*—The X.500 name of the CRLs issuer

*number\_of\_entries*—The number of revocation entries in the received CRL

*max\_allowed*—The maximum number of CRL entries that the device supports

**Recommended Action** Scalability is perhaps the most significant drawback to the CRL method of revocation checking. The only options to solve this problem are to investigate a Certificate Authority based solution to reduce the CRL size or configure the device not to require CRL validation.

## 717019

**Error Message** %PIX|ASA-3-717019: Failed to insert CRL for trustpoint *trustpoint\_name*. Reason: *failure\_reason*.

**Explanation** This log event will be generated when a CRL is retrieved but it is found to be invalid and cannot be inserted into the cache because of the *failure\_reason*.

*trustpoint\_name*—The name of the trustpoint that requested the CRL.

*failure\_reason*—The reason that the CRL failed to be inserted into cache.

**Recommended Action** Ensure the current system time is correct relative to the CA time. If the NextUpdate field is missing, configure the trustpoint to ignore the NextUpdate field.

## 717021

**Error Message** %PIX|ASA-3-717021 Certificate data could not be verified. Locate Reason: *reason\_string* serial number: *serial number*, subject name: *subject name*, key length *key length* bits.

**Explanation** This message is displayed when an attempt to verify the certificate that is identified by the serial number and subject name can not be verified for the specified reason. When verifying certificate data using the signature, several errors can occur that should be logged. These include invalid key types specified and unsupported key size.

*reason\_string*—The reason that the certificate could not be verified

*serial number*—Serial number of the certificate that is being verified

*subject name*—Subject name contained in the certificate that is being verified

*key length*—The number of bits in the key used to sign this certificate

**Recommended Action** Check the specified certificate to ensure that it is valid, that it contains a valid key type, and that it does not exceed the maximum supported key size.

## 717022

**Error Message** %PIX|ASA-6-717022 Certificate was successfully validated.  
*certificate\_identifiers*

**Explanation** This message is displayed when the identified certificate is successfully validated.

*certificate\_identifiers*—Information to identify the certificate that was validated successfully, which might include a reason, serial number, subject name, and additional information.

**Recommended Action** No ne.

## 717023

**Error Message** %PIX|ASA-3-717023 SSL failed to set device certificate for trustpoint *trustpoint name*. Reason: *reason\_string*.

**Explanation** This message is displayed when a failure occurs while trying to set a device certificate for the given trustpoint for authenticating the SSL connection. When bringing up an SSL connection, an attempt is made to set the device certificate that will be used. A failure occurring during this process is logged. The message includes the configured trustpoint that should be used to load the device certificate and the reason for the failure.

*trustpoint name*—Name of the trustpoint for which SSL failed to set a device certificate.

*reason\_string*—Reason indicating why the device certificate could not be set.

**Recommended Action** Resolve the issue indicated by the reason reported for the failure:

- Ensure that the specified trustpoint is enrolled and has a device certificate.

- Make sure the device certificate is valid.
- Reenroll the trustpoint, if required.

## 717024

**Error Message** %PIX|ASA-7-717024 Checking CRL from trustpoint: *trustpoint name* for *purpose*

**Explanation** This log message indicates that a CRL is being retrieved.

*trustpoint name*—Name of the trustpoint for which the CRL is being retrieved.

*purpose*—Reason that the CRL is being retrieved.

**Recommended Action** None.

## 717025

**Error Message** %PIX|ASA-7-717025 Validating certificate chain containing *number of certs* certificate(s).

**Explanation** This message is displayed when a chain of certificate is being validated.

*number of certs*—Number of certificates in the chain.

**Recommended Action** None.

## 717026

**Error Message** %PIX|ASA-4-717026 Name lookup failed for hostname *hostname* during PKI operation.

**Explanation** This message is displayed when the given hostname cannot be resolved while attempting a PKI operation.

*hostname*—The hostname that failed to resolve.

**Recommended Action** Check the configuration and the DNS server entries for the given hostname to make sure that it can be resolved. Then retry the operation.

## 717027

**Error Message** %PIX|ASA-3-717027 Certificate chain failed validation. *reason\_string*.

**Explanation** This message is displayed when a certificate chain could not be validated. A reason is given to pinpoint the cause of the failure.

*reason\_string*—Reason for the failure to validate the certificate chain.

**Recommended Action** Resolve the issue noted by the reason and retry the validation attempt by performing any of the following actions:

- Make sure connectivity to a CA if CRL checking is required.
- Make sure a trustpoint is authenticated and available to validation.
- Make sure the identity certificate within the chain is *valid based on the validity dates*.
- Make sure the certificate is not revoked.

## 717028

**Error Message** %PIX|ASA-6-717028 Certificate chain was successfully validated *additional info*.

**Explanation** This message is displayed when a certificate chain was successfully validated.

*additional info*—Gives additional information for how the certificate chain was validated such as 'with warning' indicating that a CRL check was not performed.

**Recommended Action** None.

## 717029

**Error Message** %PIX|ASA-7-717029 Identified client certificate within certificate chain. serial number: *serial\_number*, subject name: *subject\_name*.

**Explanation** This message identifies the certificate that is found to be the client certificate.

*serial\_number*—Serial number of the certificate that is identified as the client certificate.

*subject\_name*—Subject name contained in the certificate that is identified as the client certificate.

**Recommended Action** No action required

## 717030

**Error Message** %PIX|ASA-7-717030 Found a suitable trustpoint *trustpoint name* to validate certificate.

**Explanation** This message is displayed when a suitable/usable trustpoint is found that can be used to validate the certificate.

*trustpoint name*—Trustpoint that will be used to validate the certificate.

**Recommended Action** No action required

## 717031

**Error Message** %PIX|ASA-4-717031 Failed to find a suitable trustpoint for the issuer: *issuer* Reason: *reason\_string*

**Explanation** This syslog message displays when a usable trustpoint cannot be found. This message identifies the issuer of the certificate for which no suitable trustpoint could be found and indicates the reason for the failure. During certificate validation a suitable trustpoint must be available in order to validate a certificate.

*issuer* —Issuer of the certificate that was being validated.

*reason\_string*—The reason that a suitable trustpoint could not be found.

**Recommended Action** Resolve the issue indicated in the reason by checking configuration to make sure a trustpoint is configured, authenticated, and enrolled. Also make sure the configuration allows for specific types of certificates, such as issued identity certificates.

## 717032

**Error Message** %PIX-3-717032 OCSP status check failed. Reason: *reason\_string*.

**Explanation** This syslog message indicates that an attempt to verify the certificate status using OCSP failed because of the *reason\_string* specified.

*reason\_string*—The reason that the OCSP status could not be checked.

**Recommended Action** Check the specified *reason\_string* to determine the cause of the failure and to ensure that the OCSP responder is accessible and any response should be verifiable.

## 717033

**Error Message** %PIX|ASA-6-717033 OCSF response status - Successful.

**Explanation** This syslog message indicates that an OCSF status check response was received successfully.

**Recommended Action** None.

## 717034

**Error Message** %PIX|ASA-7-717034 No-check extension found in certificate. OCSF check bypassed.

**Explanation** This syslog message indicates that an OCSF responder certificate was received that contains an “id-pkix-ocsp-nocheck” extension, which allows this certificate to be validated without a OCSF status check.

**Recommended Action** None.

## 717035

**Error Message** %PIX|ASA-4-717035 OCSF status is being checked for certificate.  
*certificate\_identifier*.

**Explanation** This syslog message identifies the certificate for which an OCSF status check occurs. *certificate\_identifier*—Information that identifies the certificate being processed by the certificate map rules.

**Recommended Action** None.

## 717036

**Error Message** PIX|ASA-7-717036 Looking for a tunnel group match based on certificate maps for peer certificate with *certificate\_identifier*.

**Explanation** This syslog message indicates that the peer certificate identified by *certificate\_identifier* is being processed through the configured certificate maps in order to attempt a possible tunnel-group match.

*certificate\_identifier*—Information that identifies the certificate being processed by the certificate map rules.

**Recommended Action** None.

## 717037

**Error Message** %PIX|ASA-4-717037 Tunnel group search using certificate maps failed for peer certificate: *certificate\_identifier*.

**Explanation** This syslog message indicates that the peer certificate identified by *certificate\_identifier* was processed through the configured certificate maps in order to attempt a possible tunnel-group match, but no match could be found.

*certificate\_identifier*—Information that identifies the certificate being processed by the certificate map rules.

**Recommended Action** Ensure that the warning is expected based on the received peer certificate and the configured crypto ca certificate map rules.

## 717038

**Error Message** %PIX|ASA-7-717038 Tunnel group match found. Tunnel Group: *tunnel\_group\_name*, Peer certificate: *certificate\_identifier*.

**Explanation** This syslog message indicates that the peer certificate identified by *certificate\_identifier* was processed by the configured certificate maps and a match was found to the *tunnel\_group\_name* tunnel group.

*certificate\_identifier*—Information that identifies the certificate being processed by the certificate map rules.

*tunnel\_group\_name*—The name of the tunnel group matched by the certificate map rules.

**Recommended Action** None.

## 718001

**Error Message** %PIX|ASA-7-718001: Internal interprocess communication queue send failure: code *error\_code*

**Explanation** An internal software error has occurred while attempting to enqueue a message on the VPNLB queue.

**Recommended Action** This is generally a benign condition but if the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.



## 718002

**Error Message** %PIX|ASA-5-718002: Create peer *IP\_address* failure, already at maximum of *number\_of\_peers*

**Explanation** Maximum number of load balancing peers exceeded. New peer ignored.

**Recommended Action** Check your load balancing and network configuration to ensure that the number of LB peers does not exceed the maximum allowed.

## 718003

**Error Message** %PIX|ASA-6-718003: Got unknown peer message *message\_number* from *IP\_address*, local version *version\_number*, remote version *version\_number*

**Explanation** An unrecognized load balancing message was received from one of the LB peers. This could indicate a version mismatch between peers but is most likely caused by an internal software error.

**Recommended Action** Verify that all LB peers are compatible. If they are and this condition persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718004

**Error Message** %PIX|ASA-6-718004: Got unknown internal message *message\_number*

**Explanation** Received an unknown internal message. This generally indicates an internal software error.

**Recommended Action** This is generally a benign condition but if the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718005

**Error Message** %PIX|ASA-5-718005: Fail to send to *IP\_address*, port *port*

**Explanation** An internal software error has occurred while attempting to send a packet on the load balancing socket. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718006

**Error Message** %PIX|ASA-5-718006: Invalid load balancing state transition  
[*cur=state\_number*] [*event=event\_number*]

**Explanation** A state machine error has occurred. This could indicate an internal software error.

**Recommended Action** This is generally a benign condition but if the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718007

**Error Message** %PIX|ASA-5-718007: Socket open failure *failure\_code*

**Explanation** An error has occurred while attempting to open the load balancing socket. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718008

**Error Message** %PIX|ASA-5-718008: Socket bind failure *failure\_code*

**Explanation** An error has occurred while attempting to bind to the load balancing socket. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718009

**Error Message** %PIX|ASA-5-718009: Send HELLO response failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Hello Response message to one of the LB peers. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718010

**Error Message** %PIX|ASA-5-718010: Sent HELLO response to *IP\_address*

**Explanation** The security appliance transmitted a Hello Response message to a LB peer.

**Recommended Action** Informational only.

## 718011

**Error Message** %PIX|ASA-5-718011: Send HELLO request failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Hello Request message to one of the LB peers. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718012

**Error Message** %PIX|ASA-5-718012: Sent HELLO request to *IP\_address*

**Explanation** The security appliance transmitted a Hello Request message to a LB peer.

**Recommended Action** Informational only.

## 718013

**Error Message** %PIX|ASA-6-718013: Peer *IP\_address* is not answering HELLO

**Explanation** LB peer is not answering HELLO.

**Recommended Action** Check status of LBSSF peer and check the network connections.

## 718014

**Error Message** %PIX|ASA-5-718014: Master peer *IP\_address* is not answering HELLO

**Explanation** LB master peer is not answering HELLO.

**Recommended Action** Check status of LBSSF master peer and check the network connections.

## 718015

**Error Message** %PIX|ASA-5-718015: Received HELLO request from *IP\_address*

**Explanation** The security appliance received a Hello Request message from a LB peer.

**Recommended Action** Informational only.

## 718016

**Error Message** %PIX|ASA-5-718016: Received HELLO response from *IP\_address*

**Explanation** The security appliance received a Hello Response packet from a LB peer.

**Recommended Action** Informational only.

## 718017

**Error Message** %PIX|ASA-7-718017: Got timeout for unknown peer *IP\_address* msg type *message\_type*

**Explanation** The security appliance processed a timeout for an unknown peer. The message was ignored since the peer may have already been removed from the active list.

**Recommended Action** If the message persists or is linked to undesirable behavior, Check LB peers and verify that all are configured correctly.

## 718018

**Error Message** %PIX|ASA-7-718018: Send KEEPALIVE request failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Keepalive Request message to one of the LB peers. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718019

**Error Message** %PIX|ASA-7-718019: Sent KEEPALIVE request to *IP\_address*

**Explanation** The security appliance transmitted a Keepalive Request message to a LB peer.

**Recommended Action** Informational only.

## 718020

**Error Message** %PIX|ASA-7-718020: Send KEEPALIVE response failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Keepalive Response message to one of the LB peers. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718021

**Error Message** %PIX|ASA-7-718021: Sent KEEPALIVE response to *IP\_address*

**Explanation** The security appliance transmitted a Keepalive Response message to a LB peer.

**Recommended Action** Informational only.

## 718022

**Error Message** %PIX|ASA-7-718022: Received KEEPALIVE request from *IP\_address*

**Explanation** The security appliance received a Keepalive Request message from a LB peer.

**Recommended Action** Informational only.

## 718023

**Error Message** %PIX|ASA-7-718023: Received KEEPALIVE response from *IP\_address*

**Explanation** The security appliance received a Keepalive Response message from a LB peer.

**Recommended Action** Informational only.

## 718024

**Error Message** %PIX|ASA-5-718024: Send CFG UPDATE failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Configuration Update message to one of the LB peers. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718025

**Error Message** %PIX|ASA-7-718025: Sent CFG UPDATE to *IP\_address*

**Explanation** The security appliance transmitted a Configuration Update message to a LB peer.

**Recommended Action** Informational only.

## 718026

**Error Message** %PIX|ASA-7-718026: Received CFG UPDATE from *IP\_address*

**Explanation** The security appliance received a Configuration Update message from a LB peer.

**Recommended Action** Informational only.

## 718027

**Error Message** %PIX|ASA-6-718027: Received unexpected KEEPALIVE request from *IP\_address*

**Explanation** Informational message.

**Recommended Action** If the problem persists or is linked with undesirable behavior, verify that all LB peers are configured and discovered correctly.

## 718028

**Error Message** %PIX|ASA-5-718028: Send OOS indicator failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a OOS Indicator message to one of the LB peers. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718029

**Error Message** %PIX|ASA-7-718029: Sent OOS indicator to *IP\_address*

**Explanation** The security appliance transmitted a OOS Indicator message to a LB peer.

**Recommended Action** Informational only.

## 718030

**Error Message** %PIX|ASA-6-718030: Received planned OOS from *IP\_address*

**Explanation** The security appliance received a planned OOS message from a LB peer.

**Recommended Action** Informational only.

## 718031

**Error Message** %PIX|ASA-5-718031: Received OOS obituary for *IP\_address*

**Explanation** The security appliance received a OOS Obituary from a LB peer.

**Recommended Action** Informational only.

## 718032

**Error Message** %PIX|ASA-5-718032: Received OOS indicator from *IP\_address*

**Explanation** The security appliance received a OOS Indicator from a LB peer.

**Recommended Action** Informational only.

## 718033

**Error Message** %PIX|ASA-5-718033: Send TOPOLOGY indicator failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Topology Indicator message to one of the LB peers. This could indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718034

**Error Message** %PIX|ASA-7-718034: Sent TOPOLOGY indicator to *IP\_address*

**Explanation** The security appliance sent a Topology Indicator message to a LB peer.

**Recommended Action** Informational only.

## 718035

**Error Message** %PIX|ASA-7-718035: Received TOPOLOGY indicator from *IP\_address*

**Explanation** The security appliance received a Topology Indicator message from a LB peer.

**Recommended Action** Informational only.

## 718036

**Error Message** %PIX|ASA-7-718036: Process timeout for req-type *type\_value*, exid *exchange\_ID*, peer *IP\_address*

**Explanation** The security appliance processed a peer timeout.

**Recommended Action** Verify that the peer should have been timed out. If not, check the peer LB configuration and check the network connection between the peer and the security appliance.



## 718037

**Error Message** %PIX|ASA-6-718037: Master processed *number\_of\_timeouts* timeouts

**Explanation** The security appliance in the master role processed the specified number of peer timeouts.

**Recommended Action** Verify that the timeouts are legitimate. If not, check the peer LB configuration and check the network connection between the peer and the security appliance.

## 718038

**Error Message** %PIX|ASA-6-718038: Slave processed *number\_of\_timeouts* timeouts

**Explanation** The security appliance in the slave role processed the specified number of peer timeouts.

**Recommended Action** Verify that the timeouts are legitimate. If not, check the peer LB configuration and check the network connection between the peer and the security appliance.

## 718039

**Error Message** %PIX|ASA-6-718039: Process dead peer *IP\_address*

**Explanation** The security appliance has detected a dead peer.

**Recommended Action** Verify that the dead peer detection is legitimate. If not, check the peer LB configuration and check the network connection between the peer and the security appliance.

## 718040

**Error Message** %PIX|ASA-6-718040: Timed-out exchange ID *exchange\_ID* not found

**Explanation** The security appliance has detected a dead peer but the exchange ID is not recognized.

**Recommended Action** Informational only.

## 718041

**Error Message** %PIX|ASA-7-718041: Timeout [msgType=*type*] processed with no callback

**Explanation** The security appliance has detected a dead peer but a call back was not used in the processing.

**Recommended Action** Informational only.

## 718042

**Error Message** %PIX|ASA-5-718042: Unable to ARP for *IP\_address*

**Explanation** The security appliance experienced an ARP failure when attempting to contact a peer.

**Recommended Action** Verify that the network is operational and all peers can communicate with each other.

## 718043

**Error Message** %PIX|ASA-5-718043: Updating/removing duplicate peer entry *IP\_address*

**Explanation** The security appliance found and is removing a duplicate peer entry.

**Recommended Action** Informational only.

## 718044

**Error Message** %PIX|ASA-5-718044: Deleted peer *IP\_address*

**Explanation** The security appliance is deleting a LB peer.

**Recommended Action** Informational only.

## 718045

**Error Message** %PIX|ASA-5-718045: Created peer *IP\_address*

**Explanation** The security appliance has detected a LB peer.

**Recommended Action** Informational only.

## 718046

**Error Message** %PIX|ASA-7-718046: Create group policy *policy\_name*

**Explanation** The security appliance has created a group policy to securely communicate to the LB peers.

**Recommended Action** Informational only.

## 718047

**Error Message** %PIX|ASA-7-718047: Fail to create group policy *policy\_name*

**Explanation** The security appliance experienced a failure when attempting to create a group policy for securing the communication between LB peers.

**Recommended Action** Verify that LB configuration is correct.

## 718048

**Error Message** %PIX|ASA-5-718048: Create of secure tunnel failure for peer *IP\_address*

**Explanation** The security appliance experienced a failure when attempting to establish an IPSec tunnel to a LB peer.

**Recommended Action** Verify that LB configuration is correct and that the network is operational.

## 718049

**Error Message** %PIX|ASA-7-718049: Created secure tunnel to peer *IP\_address*

**Explanation** The security appliance successfully established an IPSec tunnel to a LB peer.

**Recommended Action** Informational only.

## 718050

**Error Message** %PIX|ASA-5-718050: Delete of secure tunnel failure for peer *IP\_address*

**Explanation** The security appliance experienced a failure when attempting to terminate an IPSec tunnel to a LB peer.

**Recommended Action** Verify that LB configuration is correct and that the network is operational.

## 718051

**Error Message** %PIX|ASA-6-718051: Deleted secure tunnel to peer *IP\_address*

**Explanation** The security appliance successfully terminated an IPSec tunnel to a LB peer.

**Recommended Action** Informational only.

## 718052

**Error Message** %PIX|ASA-5-718052: Received GRAT-ARP from duplicate master *MAC\_address*

**Explanation** The security appliance received a Gratuitous ARP from duplicate master.

**Recommended Action** Check the LB configuration and verify that the network is operational.

## 718053

**Error Message** %PIX|ASA-5-718053: Detected duplicate master, mastership stolen  
*MAC\_address*

**Explanation** The security appliance detected duplicate master, mastership stolen.

**Recommended Action** Check the LB configuration and verify that the network is operational.

## 718054

**Error Message** %PIX|ASA-5-718054: Detected duplicate master *MAC\_address* and going to  
SLAVE

**Explanation** The security appliance detected a duplicate master and is switching to slave mode.

**Recommended Action** Check the LB configuration and verify that the network is operational.

## 718055

**Error Message** %PIX|ASA-5-718055: Detected duplicate master *MAC\_address* and staying  
MASTER

**Explanation** The security appliance detected a duplicate master and is staying in slave mode.

**Recommended Action** Check the LB configuration and verify that the network is operational.

## 718056

**Error Message** %PIX|ASA-7-718056: Deleted Master peer, IP *IP\_address*

**Explanation** The security appliance deleted the LB master from its internal tables.

**Recommended Action** Informational only.

## 718057

**Error Message** %PIX|ASA-5-718057: Queue send failure from ISR, msg type *failure\_code*

**Explanation** An internal software error has occurred while attempting to enqueue a message on the VPNLB queue from an Interrupt Service Routing.

**Recommended Action** This is generally a benign condition but if the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718058

**Error Message** %PIX|ASA-7-718058: State machine return code: *action\_routine*, *return\_code*

**Explanation** This event traces the return codes of action routines belonging to the LB finite state machine.

**Recommended Action** Informational only.

## 718059

**Error Message** %PIX|ASA-7-718059: State machine function trace: state=*state\_name*, event=*event\_name*, func=*action\_routine*

**Explanation** This event traces the events and states of the LB finite state machine.

**Recommended Action** Informational only.

## 718060

**Error Message** %PIX|ASA-5-718060: Inbound socket select fail: context=*context\_ID*.

**Explanation** The socket select call returned an error and the socket could not be read. This could indicate an internal software error.

**Recommended Action** If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718061

**Error Message** %PIX|ASA-5-718061: Inbound socket read fail: context=*context\_ID*.

**Explanation** The socket read failed after data was detected through the select call. This could indicate an internal software error.

**Recommended Action** If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718062

**Error Message** %PIX|ASA-5-718062: Inbound thread is awake (context=*context\_ID*).

**Explanation** This indicates every time the LB process is woken up and begins processing.

**Recommended Action** Informational only.

## 718063

**Error Message** %PIX|ASA-5-718063: Interface *interface\_name* is down.

**Explanation** This indicates that the LB process found the interface down.

**Recommended Action** Check the interface configuration to make sure that the interface is operational.

## 718064

**Error Message** %PIX|ASA-5-718064: Admin. interface *interface\_name* is down.

**Explanation** This indicates that the LB process found the administrative interface down.

**Recommended Action** Check the administrative interface configuration to make sure that the interface is operational.

## 718065

**Error Message** %PIX|ASA-5-718065: Cannot continue to run (public=*up/down*, private=*up/down*, enable=*LB\_state*, master=*IP\_address*, session=*Enable/Disable*).

**Explanation** This indicates that the LB process can not run because all prerequisite conditions have not been met. The prerequisite conditions are 2 active interfaces and LB enabled.

**Recommended Action** Check the interface configuration to make sure at least 2 interfaces are operational. Also check LB configuration.

## 718066

**Error Message** %PIX|ASA-5-718066: Cannot add secondary address to interface *interface\_name*, ip *IP\_address*.

**Explanation** LB requires a secondary address to be added to the outside interface. This event indicates that there was a failure in adding that secondary address.

**Recommended Action** Check the address being used as the secondary address and ensure that it is valid and unique. Check the configuration of the outside interface.

## 718067

**Error Message** %PIX|ASA-5-718067: Cannot delete secondary address to interface *interface\_name*, ip *IP\_address*.

**Explanation** The deletion of the secondary address failed. This could indicate an addressing problem or an internal software error.

**Recommended Action** Check the addressing information of the outside interface and ensure that the secondary address is valid and unique. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718068

**Error Message** %PIX|ASA-5-718068: Start VPN Load Balancing in context *context\_ID*.

**Explanation** The LB process has been started and initialized.

**Recommended Action** Informational only.

## 718069

**Error Message** %PIX|ASA-5-718069: Stop VPN Load Balancing in context *context\_ID*.

**Explanation** The LB process has been stopped.

**Recommended Action** Informational only.

## 718070

**Error Message** %PIX|ASA-5-718070: Reset VPN Load Balancing in context *context\_ID*.

**Explanation** The LB process has been reset.

**Recommended Action** Informational only.

## 718071

**Error Message** %PIX|ASA-5-718071: Terminate VPN Load Balancing in context *context\_ID*.

**Explanation** The LB process has been terminated.

**Recommended Action** Informational only.

## 718072

**Error Message** %PIX|ASA-5-718072: Becoming master of Load Balancing in context *context\_ID*.

**Explanation** The security appliance has become the LB master.

**Recommended Action** Informational only.



## 718073

**Error Message** %PIX|ASA-5-718073: Becoming slave of Load Balancing in context *context\_ID*.

**Explanation** The security appliance has become the LB slave.

**Recommended Action** Informational only.

## 718074

**Error Message** %PIX|ASA-5-718074: Fail to create access list for peer *context\_ID*.

**Explanation** ACLs are used to create secure tunnels over which the LB peers can communicate. The security appliance was unable to create one of these ACLs. This could indicate an addressing problem or an internal software problem.

**Recommended Action** Check the addressing information of the inside interface on all peers and ensure that all peers are discovered correctly. If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718075

**Error Message** %PIX|ASA-5-718075: Peer *IP\_address* access list not set.

**Explanation** While removing a secure tunnel, the security appliance detected a peer entry that did not have an associated ACL.

**Recommended Action** Informational only.

## 718076

**Error Message** %PIX|ASA-5-718076: Fail to create tunnel group for peer *IP\_address*.

**Explanation** The security appliance experienced a failure when attempting to create a tunnel group for securing the communication between LB peers.

**Recommended Action** Verify that LB configuration is correct.

## 718077

**Error Message** %PIX|ASA-5-718077: Fail to delete tunnel group for peer *IP\_address*.

**Explanation** The security appliance experienced a failure when attempting to delete a tunnel group for securing the communication between LB peers.

**Recommended Action** Informational only.

## 718078

**Error Message** %PIX|ASA-5-718078: Fail to create crypto map for peer *IP\_address*.

**Explanation** The security appliance experienced a failure when attempting to create a crypto map for securing the communication between LB peers.

**Recommended Action** Verify that LB configuration is correct.

## 718079

**Error Message** %PIX|ASA-5-718079: Fail to delete crypto map for peer *IP\_address*.

**Explanation** The security appliance experienced a failure when attempting to delete a crypto map for securing the communication between LB peers.

**Recommended Action** Informational only.

## 718080

**Error Message** %PIX|ASA-5-718080: Fail to create crypto policy for peer *IP\_address*.

**Explanation** The security appliance experienced a failure when attempting to create a transform set to be used in securing the communication between LB peers. This could indicate an internal software problem.

**Recommended Action** If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718081

**Error Message** %PIX|ASA-5-718081: Fail to delete crypto policy for peer *IP\_address*.

**Explanation** The security appliance experienced a failure when attempting to delete a transform set used in securing the communication between LB peers.

**Recommended Action** Informational only.

## 718084

**Error Message** %PIX|ASA-5-718084: Public/cluster IP not on the same subnet: public *IP\_address*, mask *netmask*, cluster *IP\_address*

**Explanation** The cluster IP address must be on the same subnet as the outside interface of the security appliance. This even indicates that it is not on the same network.

**Recommended Action** Make sure that both the cluster (or virtual) IP address and the outside interface address are on the same network.

## 718085

**Error Message** %PIX|ASA-5-718085: Interface *interface\_name* has no IP address defined.

**Explanation** The indicated interface does not have an IP address configured.

**Recommended Action** Configure an IP address for the interface.

## 718086

**Error Message** %PIX|ASA-5-718086: Fail to install LB NP rules: type *rule\_type*, dst *interface\_name*, port *port*.

**Explanation** The security appliance experienced a failure when attempting to create a SoftNP ACL rule to be used in securing the communication between LB peers. This could indicate an internal software problem.

**Recommended Action** If the problem persists, or is linked to undesirable behavior, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC for further support and provide the gathered information.

## 718087

**Error Message** %PIX|ASA-5-718087: Fail to delete LB NP rules: type *rule\_type*, rule *rule\_ID*.

**Explanation** The security appliance experienced a failure when attempting to delete SoftNP ACL rule used in securing the communication between LB peers.

**Recommended Action** Informational only.

## 718088

**Error Message** %PIX|ASA-7-718088: Possible VPN LB misconfiguration. Offending device *MAC MAC\_address*.

**Explanation** The presence of a duplicate master indicates that one of the LB peers may be misconfigured.

**Recommended Action** Check the LB configuration on all peers but pay special attention to the peer identified.

## 719001

**Error Message** %ASA-6-719001: Email Proxy session could not be established: session limit of *maximum\_sessions* has been reached.

**Explanation** This message appears when the incoming e-mail proxy session could not be established because the maximum session limit has been reached. *maximum\_sessions* is the maximum session number.

**Recommended Action** None.

## 719002

**Error Message** %ASA-3-719002: Email Proxy session *pointer* from *source\_address* has been terminated due to *reason* error.

**Explanation** This message appears when the session has been terminated due to error. The possible errors are: adding session to session database fails; memory allocation fail; writing data to channel fail, etc. The *pointer* is the pointer of the session structure, *source\_address* is the e-mail proxy client IP address, and *reason* is the error type.

**Recommended Action** None.

## 719003

**Error Message** %ASA-6-719003: Email Proxy session *pointer* resources have been freed for *source\_address*.

**Explanation** This message appears when the dynamic allocated session structure has been freed and set to NULL after the session terminated. The *pointer* is the pointer of the session structure, and *source\_address* is the e-mail proxy client IP address.

**Recommended Action** None.

## 719004

**Error Message** %ASA-6-719004: Email Proxy session *pointer* has been successfully established for *source\_address*.

**Explanation** A new incoming email client session has been established.

**Recommended Action** None.

## 719005

**Error Message** %ASA-7-719005: FSM *NAME* has been created using *protocol* for session *pointer* from *source\_address*.

**Explanation** This message appears when an FSM has been created for an incoming new session. The *NAME* is the FSM instance name for the session, *protocol* is the e-mail protocol type (for example, POP3, IMAP, SMTP), *pointer* is the pointer of session structure, and *source\_address* is the e-mail proxy client IP address.

**Recommended Action** None.

## 719006

**Error Message** %ASA-7-719006: Email Proxy session *pointer* has timed out for *source\_address* because of network congestion.

**Explanation** This message appears due to network congestion and data cannot be sent to either an e-mail client or an e-mail sever. This starts the block timer. After the block timer is timed out, the session expires. The *pointer* is the pointer of session structure, and *source\_address* is the e-mail proxy client IP address.

**Recommended Action** Retry the operation after a few minutes.

## 719007

**Error Message** %ASA-7-719007: Email Proxy session *pointer* cannot be found for *source\_address*.

**Explanation** This message appears when a matching session cannot be found in the session database. The session pointer is bad. The *pointer* is the pointer of session structure, and *source\_address* is the e-mail proxy client IP address.

**Recommended Action** None.

## 719008

**Error Message** %ASA-3-719008: Email Proxy service is shutting down.

**Explanation** This message appears email proxy is disabled. All resources are cleaned up and all threads are terminated.

**Recommended Action** None.

## 719009

**Error Message** %ASA-7-719009: Email Proxy service is starting.

**Explanation** This message appears when the email proxy is enabled.

**Recommended Action** None.

## 719010

**Error Message** %ASA-6-719010: *protocol* Email Proxy feature is disabled on interface *interface\_name*.

**Explanation** This message appears when the e-mail proxy feature is disabled on a specific entry point, invoked from the CLI. This is the main “off” switch for the user. When all protocols are turned off for all interfaces, the main shut down routine is invoked to clean up global resources, threads, etc. The *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP,SMTP), and *interface\_name* is the security appliance interface name.

**Recommended Action** None.

## 719011

**Error Message** %ASA-6-719011: *Protocol* Email Proxy feature is enabled on interface *interface\_name*.

**Explanation** This message appears when the e-mail proxy feature is enabled on a specific entry point, invoked from the CLI. This is the main “on” switch for the user. When it is first used the main startup routine is invoked to allocate global resources, threads, etc. Subsequent calls only need to start listen threads for the particular protocol. The *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP,SMTP), and *interface\_name* is the security appliance interface name.

**Recommended Action** None.

## 719012

**Error Message** %ASA-6-719012: Email Proxy server listening on port *port* for mail protocol *protocol*.

**Explanation** This message appears when a listen channel is opened for a specific protocol on a configured port and adds it to a TCP select group. The *port* is the configured port number, and *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP,SMTP).

**Recommended Action** None.

## 719013

**Error Message** %ASA-6-719013: Email Proxy server closing port *port* for mail protocol *protocol*.

**Explanation** This message appears when a listen channel is closed for a specific protocol on a configured port and removes it from the TCP select group. The *port* is the configured port number, and *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP,SMTP).

**Recommended Action** None.

## 719014

**Error Message** %ASA-5-719014: Email Proxy is changing listen port from *old\_port* to *new\_port* for mail protocol *protocol*.

**Explanation** This message appears when a change is signaled in the listen port for the specified protocol. All enabled interfaces for that port have their listen channels closed and restarted listening on the new port. This is invoked from the CLI. The *old\_port* is the old configured port number, *new\_port* is the new configured port number, and *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP,SMTP).

**Recommended Action** None.

## 719015

**Error Message** %ASA-7-719015: Parsed emailproxy session *pointer* from *source\_address*  
username: mailuser = *mail\_user*, vpnuser = *VPN\_user*, mailserver = *server*

**Explanation** This message appears when the username string is received from the client in the format vpnuser (name delimiter) mailuser (server delimiter) mailserver (for example: xxx:yyy@cisco.com). The name delimiter is optional. When the delimiter is not there, the VPN username and mail username is the same. The server delimiter is optional. When it is not present, this means the default configured mail server will be used. The *pointer* is the pointer for the session structure, *source\_address* is the e-mail proxy client IP address, *mail\_user* is the e-mail account username, *VPN\_user* is the WebVPN username, and *server* is the e-mail server.

**Recommended Action** None.

## 719016

**Error Message** %ASA-7-719016: Parsed emailproxy session *pointer* from *source\_address*  
password: mailpass = \*\*\*\*\*, vpnpass= \*\*\*\*\*

**Explanation** This message appears when the password string is received from the client in the format, vpnpass (name delimiter) mailpass (for example: xxx:yyy). The name delimiter is optional. When it is not present, the VPN password and mail password are the same. The *pointer* is the pointer of the session structure, and *source\_address* is the e-mail proxy client IP address.

**Recommended Action** None.



## 719017

**Error Message** %ASA-6-719017: WebVPN user: *vpnuser* invalid dynamic ACL.

**Explanation** This message appears when the WebVPN session is aborted because the access control list has failed to parse for this user. The ACL determines what the user restrictions are on e-mail account accessing. The ACL is downloaded from the AAA server. Because of this error, it is unsafe to proceed with login. The *vpnuser* is the webVPN username.

**Recommended Action** Check the AAA server and fix the dynamic ACL for this user.

## 719018

**Error Message** %ASA-6-719018: WebVPN user: *vpnuser* ACL ID *acl\_ID* not found

**Explanation** This message appears when the access control list cannot be found at the local maintained ACL list. The ACL determines what the user restrictions are on e-mail account access. The ACL is configured locally. Because of this error, you cannot be authorized to proceed. The *vpnuser* is the WebVPN username, and *acl\_ID* is the local configured ACL identification string.

**Recommended Action** Check the local ACL configuration.

## 719019

**Error Message** %ASA-6-719019: WebVPN user: *vpnuser* authorization failed.

**Explanation** This message appears when the ACL determines what the user restrictions are on e-mail account access. The user cannot access the e-mail account because the authorization check fails. The *vpnuser* is the WebVPN username.

**Recommended Action** None.

## 719020

**Error Message** %ASA-6-719020: WebVPN user *vpnuser* authorization completed successfully.

**Explanation** This message appears when the ACL determines what the user restrictions are on e-mail account access. The user is authorized to access the e-mail account. The *vpnuser* is the WebVPN username.

**Recommended Action** No ne.

## 719021

**Error Message** %ASA-6-719021: WebVPN user: *vpnuser* is not checked against ACL.

**Explanation** This message appears when the ACL determines what the user restrictions are on e-mail account access. The authorization checking using ACL is not enabled. The *vpnuser* is the WebVPN username.

**Recommended Action** Enable the ACL checking feature if necessary.

## 719022

**Error Message** %ASA-6-719022: WebVPN user *vpnuser* has been authenticated.

**Explanation** This message appears when the username is authenticated by the AAA server. The *vpnuser* is the WebVPN username.

**Recommended Action** None.

## 719023

**Error Message** %ASA-6-719023: WebVPN user *vpnuser* has not been successfully authenticated. Access denied.

**Explanation** This message appears when the username is denied by the AAA server. The session will be aborted. The user is not allowed to access the e-mail account. The *vpnuser* is the WebVPN username.

**Recommended Action** None.

## 719024

**Error Message** %ASA-6-719024: Email Proxy piggyback auth fail: session = *pointer*  
user=*vpnuser* addr=*source\_address*

**Explanation** This message appears when the Piggyback authentication is using an established WebVPN session to verify the username and IP address matching in the WebVPN session database. This is based on the assumption that the WebVPN session and e-mail proxy session are initiated by the same user and a WebVPN session is already established. Because the authentication has failed, the session will be aborted. The user is not allowed to access the e-mail account. The *pointer* is the pointer of session structure, *vpnuser* is the WebVPN username, and *source\_address* is the client IP address.

**Recommended Action** None.

## 719025

**Error Message** %ASA-6-719025: Email Proxy DNS name resolution failed for *hostname*.

**Explanation** This message appears when the hostname cannot be resolved with the IP address because it is not valid or there is no DNS server available. The *hostname* is the hostname that needs to be resolved.

**Recommended Action** Check DNS server availability and check whether the configured mail server name is valid.

## 719026

**Error Message** %ASA-6-719026: Email Proxy DNS name *hostname* resolved to *IP\_address*.

**Explanation** This message appears when the hostname has successfully been resolved with the IP address. The *hostname* is the hostname that needs to be resolved, and *IP\_address* is the IP address resolved from the configured mail server name.

**Recommended Action** None.

## 720001

**Error Message** %ASA-4-720001: (VPN-*unit*) Failed to initialize with Chunk Manager.

**Explanation** This message occurs when the VPN failover subsystem fails to initialize with the memory buffer management subsystem. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** This message indicates a system-wide problem and the VPN failover subsystem cannot be started. Examine the system log messages for any sign of system-level initialization problems.

## 720002

**Error Message** %ASA-6-720002: (VPN-*unit*) Starting VPN Stateful Failover Subsystem...

**Explanation** This message appears when the VPN failover subsystem is starting and the system boots up. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** None.

## 720003

**Error Message** %ASA-6-720003: (VPN-*unit*) Initialization of VPN Stateful Failover Component completed successfully

**Explanation** This message appears when the VPN failover subsystem's initialization is completed at boot time. The *unit* is either "Primary" or "Secondary."

**Recommended Action** None.

## 720004

**Error Message** %ASA-6-720004: (VPN-*unit*) VPN failover main thread started.

**Explanation** This message appears when the VPN failover's main processing thread is started at boot time. The *unit* is either "Primary" or "Secondary."

**Recommended Action** None.

## 720005

**Error Message** %ASA-6-720005: (VPN-*unit*) VPN failover timer thread started.

**Explanation** This message appears when the VPN failover timer processing thread is started at boot time. The *unit* is either "Primary" or "Secondary."

**Recommended Action** None.

## 720006

**Error Message** %ASA-6-720006: (VPN-*unit*) VPN failover sync thread started.

**Explanation** This message appears when the system's bulk synchronization processing thread is started at boot time. The *unit* is either "Primary" or "Secondary."

**Recommended Action** None.

## 720007

**Error Message** %ASA-4-720007: (VPN-*unit*) Failed to allocate chunk from Chunk Manager.

**Explanation** This message appears when the set of preallocated memory buffers is running out. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** This message indicates a resource issue. The system may be under heavy load when too many messages are being processed. This condition may be improved later when the VPN failover subsystem processes outstanding messages and frees up memory previously allocated.

## 720008

**Error Message** %ASA-4-720008: (VPN-*unit*) Failed to register to High Availability Framework.

**Explanation** This message appears when the VPN failover subsystem fails to register to the core failover subsystem. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** The VPN failover subsystem cannot be started. This may be caused by initialization problems of other subsystems. Search the system log message for any sign of system-wide initialization problems.

## 720009

**Error Message** %ASA-4-720009: (VPN-*unit*) Failed to create version control block.

**Explanation** This message appears when the VPN failover subsystem fails to create a version control block. This step is required for VPN failover subsystem to find out the backward compatible firmware versions for the current release. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** The VPN failover subsystem cannot be started. This may be caused by initialization problems of other subsystems. Search the system log message for any sign of system-wide initialization problems.

## 720010

**Error Message** %ASA-6-720010: (VPN-*unit*) VPN failover client is being disabled

**Explanation** This message appears when an operator enables failover without defining a failover key. In order to use a VPN failover, a failover key must be defined. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** Use the failover key command to define a shared secret key between the active and standby unit.

## 720011

**Error Message** %ASA-4-720011: (VPN-*unit*) Failed to allocate memory

**Explanation** This message appears when the VPN failover subsystem cannot allocate a memory buffer. This indicates a system-wide resource problem. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** The system may be under heavy load. This condition may be improved later when you reduce the load on the system by reducing incoming traffic. By reducing incoming traffic, memory allocated for processing the existing work load will be available and the system may return to normal operation.

## 720012

**Error Message** %ASA-6-720012: (VPN-*unit*) Failed to update IPSec failover runtime data on the standby unit.

**Explanation** This message appears when the VPN failover subsystem cannot update IPSec-related runtime data because the corresponding IPSec tunnel has been deleted on the standby unit. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** None.

## 720013

**Error Message** %ASA-4-720013: (VPN-*unit*) Failed to insert certificate in trust point *trustpoint\_name*

**Explanation** This message appears when the VPN failover subsystem attempts to insert a certificate in the trust point. The *unit* is either “Primary” or “Secondary” and *trustpoint\_name* is the name of the trust point.

**Recommended Action** Check the certificate content to determine if it is invalid.

## 720014

**Error Message** %ASA-6-720014: (VPN-*unit*) Phase 2 connection entry (msg\_id=*message\_number*, my cookie=*mine*, his cookie=*his*) contains no SA list.

**Explanation** This message appears when there is no security association linked to the Phase 2 connection entry. The *unit* is either “Primary” or “Secondary,” *message\_number* is the message ID of the Phase 2 connection entry, *mine* is the My Phase 1 cookie, and *his* is the peer's Phase 1 cookie.

**Recommended Action** None.

## 720015

**Error Message** %ASA-6-720015: (VPN-*unit*) Cannot found Phase 1 SA for Phase 2 connection entry (msg\_id=*message\_number*, my cookie=*mine*, his cookie=*his*).

**Explanation** This message appears when the corresponding Phase 1 security association for the given Phase 2 connection entry cannot be found. The *unit* is either “Primary” or “Secondary,” *message\_number* is the message ID of the Phase 2 connection entry, *mine* is the My Phase 1 cookie, and *his* is the peer's Phase 1 cookie.

**Recommended Action** None.

## 720016

**Error Message** %ASA-5-720016: (VPN-*unit*) Failed to initialize default timer #*index*.

**Explanation** This message appears when the VPN failover subsystem fails to initialize the given timer event. The *unit* is either “Primary” or “Secondary” and *index* is the internal index of the timer event.

**Recommended Action** The VPN failover subsystem cannot be started at boot time. Search the system log message for any sign of system-wide initialization problems.

## 720017

**Error Message** %ASA-5-720017: (VPN-*unit*) Failed to update LB runtime data

**Explanation** This message appears when the VPN failover subsystem fails to update the VPN load balancing runtime data. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** None.

## 720018

**Error Message** %ASA-5-720018: (VPN-*unit*) Failed to get a buffer from the underlying core high availability subsystem. Error code *code*.

**Explanation** This message appears when the system may be under heavy load. The VPN failover subsystem fails to obtain a failover buffer. The *unit* is either “Primary” or “Secondary” and *code* is the error code returned by the high-availability subsystem.

**Recommended Action** Decrease the amount of incoming traffic to improve the current load condition. With decreased incoming traffic, the system will free up memory allocated for processing the incoming load.

## 720019

**Error Message** %ASA-5-720019: (VPN-*unit*) Failed to update cTCP statistics.

**Explanation** This message appears when the VPN failover subsystem fails to update the IPSec/cTCP-related statistics. The *unit* is either “Primary” or “Secondary.”

**Recommended Action** None. Updates are sent periodically, so the standby unit's IPSec/cTCP statistics should be updated with the next update message.

## 720020

**Error Message** %ASA-5-720020: (VPN-*unit*) Failed to send *type* timer message.

**Explanation** This message appears when the VPN failover subsystem fails to send a periodic timer message to the standby unit. The *unit* is either “Primary” or “Secondary” and *type* is the type of timer message.

**Recommended Action** None. The periodic timer message will be resent during the next timeout.

## 720021

**Error Message** %ASA-5-720021: (VPN-*unit*) HA non-block send failed for peer msg *message\_number*. HA error *code*.

**Explanation** The VPN failover subsystem fails to send a non-block message.

*unit*—Either “Primary” or “Secondary”

*message\_number*—ID number of the peer message.

*code*—Error return code.

**Recommended Action** This is a temporary condition caused by system under load or out of system resources. The system condition will improve as more system resources are freed up.

## 720022

**Error Message** %ASA-4-720022: (VPN-*unit*) Cannot find trust point *trustpoint*

**Explanation** An error is encountered when VPN failover subsystem attempts to look up a trust point by name.

*unit*—Either “Primary” or “Secondary”

*trustpoint*—Name of the trust point.

**Recommended Action** The trust point may be deleted by an operator.



## 720023

**Error Message** %ASA-6-720023: (VPN-*unit*) HA status callback: Peer is *not* present.

**Explanation** This is an informational message. VPN failover subsystem is notified by the core failover subsystem when the local device detected a peer is available or becomes unavailable.

*unit*—Either “Primary” or “Secondary”

*not*—Either “not” or “”.

**Recommended Action** None.

## 720024

**Error Message** %ASA-6-720024: (VPN-*unit*) HA status callback: Control channel is *status*.

**Explanation** This is an informational message indicating whether the failover control channel is either “up” or “down.” The failover control channel is defined by the **failover link** and **show failover** commands, which indicate whether the failover link channel is “up” or “down.”

*unit*—Either “Primary” or “Secondary”

*status*— “Up” or “down.”

**Recommended Action** None.

## 720025

**Error Message** %ASA-6-720025: (VPN-*unit*) HA status callback: Data channel is *status*.

**Explanation** This is an informational message indicating whether the failover data channel is up or down.

*unit*—Either “Primary” or “Secondary.”

*status*—“Up” or “down.”

**Recommended Action** None.

## 720026

**Error Message** %ASA-6-720026: (VPN-*unit*) HA status callback: Current progression is being aborted.

**Explanation** This message is generated only when an operator or other external condition applies and causes the current failover progression to abort before the failover peer agrees on the role (either active or standby). One example is when the **failover active** command is entered on the standby unit during the negotiation. Another example is the active unit is being rebooted.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720027

**Error Message** %ASA-6-720027: (VPN-*unit*) HA status callback: My state *state*.

**Explanation** This informational message is generated whenever the state of the local failover device is changed.

*unit*—Either “Primary” or “Secondary.”

*state*—Current state of the local failover device.

**Recommended Action** None.

## 720028

**Error Message** %ASA-6-720028: (VPN-*unit*) HA status callback: Peer state *state*.

*unit*—Either “Primary” or “Secondary.”

*state*—Current state of the failover peer.

**Explanation** This informational message is generated to report the current state of the failover peer.

**Recommended Action** None.

## 720029

**Error Message** %ASA-6-720029: (VPN-*unit*) HA status callback: Start VPN bulk sync state.

*unit* - Either “Primary” or “Secondary.”

**Explanation** This is an informational message generated when the active unit is ready to send all the state information to the standby unit.

**Recommended Action** None.

## 720030

**Error Message** %ASA-6-720030: (VPN-*unit*) HA status callback: Stop bulk sync state.  
*unit*—Either “Primary” or “Secondary.”

**Explanation** This is an informational message generated when the active unit finishes sending all the state information to the standby unit.

**Recommended Action** None.

## 720031

**Error Message** %ASA-7-720031: (VPN-*unit*) HA status callback: Invalid event received.  
*event=event\_ID*.

**Explanation** This message is generated when VPN failover subsystem receives an invalid callback event from the underlying failover subsystem.

*unit*—Either “Primary” or “Secondary.”

*event\_ID*—Invalid event ID received.

**Recommended Action** This is a debug message.

## 720032

**Error Message** %ASA-6-720032: (VPN-*unit*) HA status callback: id=*ID*, seq=*sequence\_#*, grp=*group*, event=*event*, op=*operand*, my=*my\_state*, peer=*peer\_state*.

**Explanation** This is an informational message generated by VPN failover subsystem when a status update is notified by the underlying failover subsystem.

*unit*—Either “Primary” or “Secondary”

*ID*—Client ID number.

*sequence\_#*—Sequence number.

*group*—Group ID.

*event*—Current event.

*operand*—Current operand.

*my\_state*—The system current state.

*peer\_state*—The current state of the peer.

**Recommended Action** None.

## 720033

**Error Message** %ASA-4-720033: (VPN-*unit*) Failed to queue add to message queue.

**Explanation** This message indicates that system resources may be running low. An error is encountered when VPN failover subsystem attempts to queue an internal message.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** This may be a temporary condition indicating that the system is under heavy load and VPN failover subsystem cannot allocate resource to handle incoming traffic. This error condition may go away if the current load of the system reduces and additional system resources become available for processing new messages again.

## 720034

**Error Message** %ASA-7-720034: (VPN-*unit*) Invalid type (*type*) for message handler.

**Explanation** An error is encountered when VPN failover subsystem attempts to process an invalid message type.

*unit*—Either “Primary” or “Secondary.”

*type*—Message type.

**Recommended Action** This is a debug message.

## 720035

**Error Message** %ASA-5-720035: (VPN-*unit*) Fail to look up CTCP flow handle

**Explanation** The cTCP flow may be deleted on the standby unit before VPN failover subsystem attempts to do a lookup.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** Look for any sign of cTCP flow deletion in the system log message to determine reason (for example, idle timeout) of why the flow is deleted.

## 720036

**Error Message** %ASA-5-720036: (VPN-*unit*) Failed to process state update message from the active peer.

**Explanation** An error is encountered when VPN failover subsystem attempts to process a state update message received by the standby unit.

*unit* - Either “Primary” or “Secondary.”

**Recommended Action** This may be a temporary condition due to current load or low system resources.

## 720037

**Error Message** %ASA-6-720037: (VPN-*unit*) HA progression callback:  
id=*id*, seq=*sequence\_number*, grp=*group*, event=*event*, op=*operand*,  
my=*my\_state*, peer=*peer\_state*.

*unit*—Either “Primary” or “Secondary.”

*id*—Client id.

*sequence\_number*—Sequence number.

*group*—Group id.

*event*—Current event.

*operand*—Current operand.

*my\_state*—Current state of the system.

*peer\_state*—Current state of the peer.

**Explanation** This is an informational message reporting the status of the current failover progression.

**Recommended Action** None.

## 720038

**Error Message** %ASA-4-720038: (VPN-*unit*) Corrupted message from active unit.

**Explanation** The standby unit receives a corrupted message from the active unit. Messages from active unit are corrupted. This may be caused by incompatible firmware running between the active and standby unit.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** This is an informational message indicating the local unit has become the active unit of the failover pair.

## 720039

**Error Message** %ASA-6-720039: (VPN-*unit*) VPN failover client is transitioning to active state

**Explanation** This is an informational message indicating the local unit has become the active unit of the failover pair.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720040

**Error Message** %ASA-6-720040: (VPN-*unit*) VPN failover client is transitioning to standby state.

**Explanation** This is an informational message indicating the local unit has become the standby unit of the failover pair.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720041

**Error Message** %ASA-7-720041: (VPN-*unit*) Sending *type* message *id* to standby unit

**Explanation** This is a debug message indicating a message is sent from the active unit to the standby unit.

*unit*—Either “Primary” or “Secondary.”

*type*—Message type.

*id*—Identifier for the message.

**Recommended Action** None.

## 720042

**Error Message** %ASA-7-720042: (VPN-*unit*) Receiving *type* message *id* from active unit

**Explanation** This is a debug message indicating a message is received by the standby unit.

*unit*—Either “Primary” or “Secondary.”

*type*—Message type.

*id*—Identifier for the message.

**Recommended Action** None.

## 720043

**Error Message** %ASA-4-720043: (VPN-*unit*) Failed to send *type* message *id* to standby unit

**Explanation** An error was encountered when VPN failover subsystem attempts to send a message from the active unit to the standby unit. This may be caused by 720018 where the core failover subsystem runs out of failover buffer or the failover lan link is down.

*unit*—Either “Primary” or “Secondary.”

*type*—Message type.

*id*—Identifier for the message.

**Recommended Action** Use the **show failover** command to see if the failover pair is running in good condition and the failover lan link is “up.”

## 720044

**Error Message** %ASA-4-720044: (VPN-*unit*) Failed to receive message from active unit

**Explanation** An error is encountered when VPN failover subsystem attempts to receive a message on the standby unit. This may be caused by a corrupted message, no enough memory to be allocated for storing the incoming message.

*unit*—Either “Primary” or “Secondary”

**Recommended Action** Use the **show failover** command and look for receive errors to determine if this is VPN failover specific problems or a general failover issue. Corrupted messages may be caused by incompatible firmware versions running on active and standby unit. Use the **show memory** command to determine if there is a low memory condition.

## 720045

**Error Message** %ASA-6-720045: (VPN-*unit*) Start bulk syncing of state information on standby unit.

**Explanation** This is an information message indicating the standby unit has been notified to start receiving bulk synchronization information from the active unit.

*unit*—Either “Primary” or “Secondary”

**Recommended Action** None.

## 720046

**Error Message** %ASA-6-720046: (VPN-*unit*) End bulk syncing of state information on standby unit

**Explanation** This is an information message indicating the standby unit has been notified that bulk synchronization from the active unit is completed.

*unit*—Either “Primary” or “Secondary”

**Recommended Action** None.

## 720047

**Error Message** %ASA-4-720047: (VPN-*unit*) Failed to sync SDI node secret file for server *IP\_address* on the standby unit.

**Explanation** An error was encountered when the VPN failover subsystem attempted to synchronize a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. This error may indicate that the flash file system is full or corrupted.

*unit*—Either “Primary” or “Secondary”

*IP\_address*—IP address of the server.

**Recommended Action** Use the **dir** command to display the flash contents. Node secret file has a file name “*ip.sdi*.”



## 720048

**Error Message** %ASA-7-720048: (VPN-*unit*) FSM action trace begin: state=*state*, last event=*event*, func=*function*.

*unit*—Either “Primary” or “Secondary”

*state*—Current state.

*event*—Last event.

*function*—Current executing function.

**Explanation** This is a debug message indicating a VPN failover subsystem finite state machine function is started.

**Recommended Action** None.

## 720049

**Error Message** %ASA-7-720049: (VPN-*unit*) FSM action trace end: state=*state*, last event=*event*, return=*return*, func=*function*.

**Explanation** This is a debug message indicating a VPN failover subsystem finite state machine function is completed.

*unit*—Either “Primary” or “Secondary”

*state*—Current state.

*event*—Last event.

*return*—Return code.

*function*—Current executing function.

**Recommended Action** None.

## 720050

**Error Message** %ASA-7-720050: (VPN-*unit*) Failed to remove timer. ID = *id*.

**Explanation** This is a debug message indicating that a timer cannot be removed from the timer processing thread.

*unit*—Either “Primary” or “Secondary”

*id*—Timer id.

**Recommended Action** None.

## 720051

**Error Message** %ASA-4-720051: (VPN-*unit*) Failed to add new SDI node secret file for server *id* on the standby unit.

**Explanation** An error was encountered when the VPN failover subsystem attempted to add a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. This error may indicate that the flash file system is full or corrupted.

*unit*—Either “Primary” or “Secondary”

*id*—IP address of the SDI server.

**Recommended Action** Enter the **dir** command to display the flash contents. Node secret file has a file name “*ip.sdi*.”

## 720052

**Error Message** %ASA-4-720052: (VPN-*unit*) Failed to delete SDI node secret file for server *id* on the standby unit.

**Explanation** An error was encountered when the VPN failover subsystem attempted to delete a node secret file on the active unit. The node secret file being deleted may not exist in the flash file system or there is problem reading the flash file system.

*unit*—Either “Primary” or “Secondary.”

*IP\_address*—IP address of the SDI server.

**Recommended Action** Use the **dir** command to display the flash contents. Node secret file has a file name “*ip.sdi*.”

## 720053

**Error Message** %ASA-4-720053: (VPN-*unit*) Failed to add cTCP IKE rule during bulk sync, peer=*IP\_address*, port=*port*

**Explanation** An error is encountered when VPN failover subsystem attempts to load an cTCP IKE rule on the standby unit during bulk synchronization.

*unit*—Either “Primary” or “Secondary.”

*IP\_address*—Peer's IP address.

*port*—Peer's port number.

**Recommended Action** The standby unit may be under heavy load and the new IKE rule request timeout before completion.

## 720054

**Error Message** %ASA-4-720054: (VPN-*unit*) Failed to add new cTCP record, peer=*IP\_address*, port=*port*.

**Explanation** A cTCP record is replicated to the standby and cannot be updated. The corresponding IPsec over cTCP tunnel may not be functioning after failover.

*unit*—Either “Primary” or “Secondary.”

*IP\_address*—Peer's IP address.

*port*—Peer's port number.

**Recommended Action** The cTCP database may be full or a record with the same peer IP address and port number exists already. This may be a temporary condition and may improve when existing

## 720055

**Error Message** %ASA-4-720055: (VPN-*unit*) VPN Stateful failover can only be run in single/non-transparent mode.

**Explanation** This message will be displayed and the VPN subsystem will not be started if not running in single (non-transparent) mode.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** Configure the device for the appropriate mode to support VPN failover and restart the device.

## 720056

**Error Message** %ASA-6-720056: (VPN-*unit*) VPN Stateful failover Message Thread is being disabled.

**Explanation** This is an informational message indicating the VPN failover subsystem's main message processing thread is disabled when user attempts to enable failover but failover key is not defined. Failover key is required for VPN failover.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720057

**Error Message** %ASA-6-720057: (VPN-*unit*) VPN Stateful failover Message Thread is enabled.

**Explanation** This is an informational message indicating the VPN failover subsystem's main message processing thread is enabled when failover is enable and a failover key is defined.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720058

**Error Message** %ASA-6-720058: (VPN-*unit*) VPN Stateful failover Timer Thread is disabled.

**Explanation** This is an informational message indicating the VPN failover subsystem's main timer processing thread is disabled when failover key is not defined and failover is enable.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720059

**Error Message** %ASA-6-720059: (VPN-*unit*) VPN Stateful failover Timer Thread is enabled.

**Explanation** This is an informational message indicating the VPN failover subsystem's main timer processing thread is enabled when failover key is defined and failover is enable.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720060

**Error Message** %ASA-6-720060: (VPN-*unit*) VPN Stateful failover Sync Thread is disabled.

**Explanation** This is an informational message indicating the VPN failover subsystem's main bulk synchronization processing thread is disabled when failover is enabled but failover key is not defined.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720061

**Error Message** %ASA-6-720061: (VPN-*unit*) VPN Stateful failover Sync Thread is enabled.

**Explanation** This is an informational message indicating the VPN failover subsystem's main bulk synchronization processing thread is enabled when failover is enable and failover key is defined.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720062

**Error Message** %ASA-6-720062: (VPN-*unit*) Active unit started bulk sync of state information to standby unit.

**Explanation** This is an informational message indicating the VPN failover subsystem's active unit has started bulk synchronization of state information to the standby unit.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720063

**Error Message** %ASA-6-720063: (VPN-*unit*) Active unit completed bulk sync of state information to standby.

**Explanation** This is an informational message indicating the VPN failover subsystem's active unit has completed bulk synchronization state information to the standby unit.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** None.

## 720064

**Error Message** %ASA-4-720064: (VPN-*unit*) Failed to update cTCP database record for peer=*IP\_address*, port=*port* during bulk sync.

**Explanation** An error was encountered while the VPN failover subsystem attempted to update an existing cTCP record during bulk synchronization. The cTCP record may have been deleted from the cTCP database on the standby unit and cannot be found.

*unit*—Either “Primary” or “Secondary.”

*IP\_address*—Peer's IP address.

*port*—Peer's port number.

**Recommended Action** Search in the system log message.

## 720065

**Error Message** %ASA-4-720065: (VPN-*unit*) Failed to add new cTCP IKE rule, peer=*peer*, port=*port*.

**Explanation** An error is encountered when VPN failover subsystem attempts to add new IKE rule for the cTCP database entry on the standby unit.

*unit*—Either “Primary” or “Secondary.”

*IP\_address*—Peer's IP address.

*port*—Peer's port number.

**Recommended Action** The system may be under heavy load and the request for adding cTCP IKE rule timeout and never completed. This may be a temporary condition.

## 720066

**Error Message** %ASA-4-720066: (VPN-*unit*) Failed to activate IKE database.

**Explanation** An error was encountered when the VPN failover subsystem attempted to activate the IKE security association database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the IKE security association database from activating.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** Use the **show failover** command to see if the failover pair is still in good condition and/or look for other IKE related errors in the syslog.

## 720067

**Error Message** %ASA-4-720067: (VPN-*unit*) Failed to deactivate IKE database.

**Explanation** An error was encountered when the VPN failover subsystem attempted to deactivate the IKE security association database while the active unit was transitioning to the standby state. There may be resources-related issues on the active unit that prevent the IKE security association database from deactivating.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** Enter the **show failover** command to see if the failover pair is still in good condition and/or look for IKE related errors in the syslog.

## 720068

**Error Message** %ASA-4-720068: (VPN-*unit*) Failed to parse peer message.

**Explanation** An error is encountered when VPN failover subsystem attempts to parse a peer message received on the standby unit.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** The peer message received on the standby unit cannot be parsed. Make sure both active/standby units are running the same versions of firmware. Also, use the **show failover** command to ensure the failover pair is still in good condition.

## 720069

**Error Message** %ASA-4-720069: (VPN-*unit*) Failed to activate cTCP database.

**Explanation** An error was encountered when the VPN failover subsystem attempted to activate the cTCP database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the cTCP database from activating.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** Enter the **show failover** command to see if the failover pair is still in good condition and/or look for other cTCP related errors in the syslog.

## 720070

**Error Message** %ASA-4-720070: (VPN-*unit*) Failed to deactivate cTCP database.

**Explanation** An error was encountered when the VPN failover subsystem attempted to deactivate the cTCP database while the active unit was transitioning to the standby state. There may be resources-related issues on the active unit that prevent the cTCP database from deactivating.

*unit*—Either “Primary” or “Secondary.”

**Recommended Action** Use the **show failover** command to see if the failover pair is still in good condition and/or look for cTCP related errors in the syslog.

## 720071

**Error Message** %ASA-5-720071: (VPN-*unit*) Failed to update cTCP dynamic data.

**Explanation** An error was encountered while the VPN failover subsystem attempted to update cTCP dynamic data.

*unit*—Either “Primary” or “Secondary.”

**Explanation** This may be a temporary condition. Since this is a periodic update, wait to see if the same error occurs. Also, look for other failover related messages in the syslog.

## 720072

**Error Message** %ASA-vpnfo-5-720072: Timeout waiting for Integrity Firewall Server [*interface,ip*] to become available.

**Explanation** In an active/standby failover setup, the SSL connection between a Zonelab Integrity Server and the security appliance needs to be re-established after a failover. This syslog message is generated if the Zonelab Integrity Server cannot re-establish a connection before timeout.

*interface*—The interface to which the Zonelab Integrity Server is connected.

*ip*—The IP address of the Zonelab Integrity Server.

**Recommended Action** Check that the configuration on the security appliance and the Zonelab Integrity Server match, and verify communication between the security appliance and the Zonelab Integrity Server.



## 720073

**Error Message** %ASA-4-720073: (VPN-*unit*) Fail to insert certificate in trust point *trustpoint* on the standby unit.

**Explanation** An error is encountered when VPN failover subsystem attempts to insert a certificate in the trust point. This error may be caused by invalid content of the certificate.

*unit*—Either “Primary” or “Secondary.”

*trustpoint*—Name of the trust point.

**Recommended Action** Performs a “write standby” on the active unit to replicate the certificate to the standby unit manually. Search in the system log message to see if there is any failover/PKI related errors.

## 722001

**Error Message** %ASA-4-722001: IP *IP\_address* Error parsing SVC connect request.

**Explanation** The request from the SSL VPN client (SVC) was invalid. .

**Recommended Action** Research as necessary to determine if this was caused by a bug in the SVC, an incompatible SVC version, or an attack against the device.

## 722002

**Error Message** %ASA-4-722002: IP *IP\_address* Error consolidating SVC connect request.

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

## 722003

**Error Message** %ASA-4-722003: IP *IP\_address* Error authenticating SVC connect request.

**Explanation** The user took too long to download and connect.

**Recommended Action** Increase the timeouts for session idle and maximum connect time.

## 722004

**Error Message** %ASA-4-722004: Group *group* User *user-name* IP *IP\_address* Error responding to SVC connect request.

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

## 722005

**Error Message** %ASA-5-722005: Group *group* User *user-name* IP *IP\_address* Unable to update session information for SVC connection.

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

## 722006

**Error Message** %ASA-5-722006: Group *group* User *user-name* IP *IP\_address* Invalid address *IP\_address* assigned to SVC connection.

**Explanation** An invalid address was assigned to the user.

**Recommended Action** Verify and correct the address assignment.

## 722007

**Error Message** %ASA-3-722007: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/ERROR: *message*

**Explanation** This is a message from the SSL VPN client (SVC) .

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

0—Normal.

16—Logout.

17—Closed due to error.

18—Closed due to rekey.

1-15, 19-31—Reserved and unused.

*message*—A text message from the SVC.

**Recommended Action** None.

## 722008

**Error Message** %ASA-3-722008: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/ERROR: *message*

**Explanation** This is a message from the SSL VPN client (SVC).

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal.
- 16—Logout.
- 17—Closed due to error.
- 18—Closed due to rekey.
- 1-15, 19-31—Reserved and unused.

*message*—A text message from the SVC.

**Recommended Action** None.

## 722009

**Error Message** %ASA-3-722009: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/ERROR: *message*

**Explanation** This is a message from the SVC client.

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal.
- 16—Logout.
- 17—Closed due to error.
- 18—Closed due to rekey.
- 1-15, 19-31—Reserved and unused.

*message*—A text message from the SVC.

**Recommended Action** None.

## 722010

**Error Message** %ASA-5-722010: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/NOTICE: *message*

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal.
- 16—Logout.
- 17—Closed due to error.

18—Closed due to rekey.

1-15, 19-31—Reserved and unused.

*message*—A text message from the SVC.

**Recommended Action** None.

## 722011

**Error Message** %ASA-5-722011: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/NOTICE: *message*

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

0—Normal.

16—Logout.

17—Closed due to error.

18—Closed due to rekey.

1-15, 19-31—Reserved and unused.

*message*—A text message from the SVC.

**Recommended Action** None.

## 722012

**Error Message** %ASA-5-722012: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/INFO: *message*

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

0—Normal.

16—Logout.

17—Closed due to error.

18—Closed due to rekey.

1-15, 19-31—Reserved and unused.

*message*—A text message from the SVC.

**Recommended Action** None.

## 722013

**Error Message** %ASA-6-722013: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/INFO: *message*

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

0—Normal.  
16—Logout.  
17—Closed due to error.  
18—Closed due to rekey.  
1-15, 19-31—Reserved and unused.  
*message*—A text message from the SVC.

**Recommended Action** None.

## 722014

**Error Message** %ASA-6-722014: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*/INFO: *message*

*type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:

0—Normal.  
16—Logout.  
17—Closed due to error.  
18—Closed due to rekey.  
1-15, 19-31—Reserved and unused.

*message*—A text message from the SVC.

**Recommended Action** None.

## 722015

**Error Message** %ASA-4-722015: Group *group* User *user-name* IP *IP\_address* Unknown SVC frame type: *type-num*

**Explanation** The SSL VPN client (SVC) sent an invalid frame type to the device.

*type-num*—The number identifier of the frame type.

**Recommended Action** This could be caused by an SVC version incompatibility. Verify the SVC version.

## 722016

**Error Message** %ASA-4-722016: Group *group* User *user-name* IP *IP\_address* Bad SVC frame length: *length* expected: *expected-length*

**Explanation** The expected amount of data was not available from the SSL VPN client (SVC).

**Recommended Action** This could be caused by an SVC version incompatibility. Verify the SVC version.

## 722017

**Error Message** %ASA-4-722017: Group *group* User *user-name* IP *IP\_address* Bad SVC framing: 525446, reserved: 0

**Explanation** The SSL VPN client (SVC) send a badly framed datagram.

**Recommended Action** This could be caused by an SVC version incompatibility. Verify the SVC version.

## 722018

**Error Message** %ASA-4-722018: Group *group* User *user-name* IP *IP\_address* Bad SVC protocol version: *version*, expected: *expected-version*

**Explanation** The SSL VPN client (SVC) sent a version unknown to the device.

**Recommended Action** This could be caused by an SVC version incompatibility. Verify the SVC version.

## 722019

**Error Message** %ASA-4-722019: Group *group* User *user-name* IP *IP\_address* Not enough data for an SVC header: *length*

**Explanation** The expected amount of data was not available from the SSL VPN client (SVC).

**Recommended Action** This could be caused by an SVC version incompatibility. Verify the SVC version.

## 722020

**Error Message** %ASA-3-722020: Group *group* User *user-name* IP *IP\_address* No address available for SVC connection

**Explanation** No addresses are available to assign to the SSL VPN client (SVC) connection.

**Recommended Action** Verify the address assignment configuration.

## 722021

**Error Message** %ASA-3-722021: Group *group* User *user-name* IP *IP\_address* Unable to start compression due to lack of memory resources

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

## 722022

**Error Message** %ASA-6-722022: TunnelGroup *tunnel\_group* GroupPolicy *group\_policy* User *user-name* IP *IP\_address* No address available for SVC connection

**Explanation** Informative message only.

**Recommended Action** None.

## 722023

**Error Message** %ASA-6-722023: Group *group* User *user-name* IP *IP\_address* SVC connection terminated {with|without} compression

**Explanation** Informative message only.

**Recommended Action** None.

## 722024

**Error Message** %ASA-6-722024: SVC Global Compression Enabled

**Explanation** Indicates that subsequent SSL VPN Client (SVC) connections will be allowed to perform tunnel compression if SVC compression is enabled in the corresponding user or group configuration.

**Recommended Action** None.

## 722025

**Error Message** %ASA-6-722025: SVC Global Compression Disabled

**Explanation** Indicates that subsequent SSL VPN Client (SVC) connections will *not* be allowed to perform tunnel compression

**Recommended Action** None.

## 722026

**Error Message** %ASA-6-722026: Group *group* User *user-name* IP *IP\_address* SVC compression history reset

**Explanation** A compression error occurred. The SSL VPN client (SVC) and device corrected it.

**Recommended Action** None.

## 722027

**Error Message** %ASA-6-722027: Group *group* User *user-name* IP *IP\_address* SVC decompression history reset

**Explanation** A decompression error occurred. The SSL VPN client (SVC) and device corrected it.

**Recommended Action** None.



## 722028

**Error Message** %ASA-5-722028: Group *group* User *user-name* IP *IP\_address* Stale SVC connection closed.

**Explanation** An unused SSL VPN client (SVC) connection was closed.

**Recommended Action** None. However, the client may be having trouble connecting if multiple connections are established. The SVC log should be examined.

## 722029

**Error Message** %ASA-7-722029: Group *group* User *user-name* IP *IP\_address* SVC Session Termination: Conns: *connections*, DPD Conns: *DPD\_conns*, Comp resets: *compression\_resets*, Dcmp resets: *decompression\_resets*

**Explanation** Lists the number of connections, reconnections, and resets that have occurred. If *connections* is greater than 1 or the number of *DPD\_conns*, *compression\_resets*, or *decompression\_resets* is greater than 0, it may indicate network reliability problems, which may be beyond the control of the security appliance administrator.

*connections*—The total number of connections during this session (1 is normal).

*DPD\_conns*—The number of reconnections due to DPD (Dead-Peer-Detection)

*compression\_resets*—The number of compression history resets.

*decompression\_resets*—The number of decompression history resets.

**Recommended Action** If there are many conns or DPD conns, the user may be having problems connecting and may experience poor performance. The SSL VPN client (SVC) log should be examined. You may want to research and take appropriate action to resolve possible network reliability problems.

## 722030

**Error Message** %ASA-7-722030: Group *group* User *user-name* IP *IP\_address* SVC Session Termination: In: *data\_bytes* (+*ctrl\_bytes*) bytes, *data\_pkts* (+*ctrl\_pkts*) packets, *drop\_pkts* drops

**Explanation** End of session statistics are being recorded.

*data\_bytes*—The number of inbound (from SVC) data bytes.

*ctrl\_bytes*—The number of inbound control bytes.

*data\_pkts*—The number of inbound data packets.

*ctrl\_pkts*—The number of inbound control packets.

*drop\_pkts*—The number of inbound packets that were dropped.

**Recommended Action** None.

## 722031

**Error Message** %ASA-7-722031: Group *group* User *user-name* IP *IP\_address* SVC Session Termination: Out: *data\_bytes* (+*ctrl\_bytes*) bytes, *data\_pkts* (+*ctrl\_pkts*) packets, *drop\_pkts* drops.

**Explanation** End of session statistics are being recorded.

*data\_bytes*—The number of outbound (to SVC) data bytes.

*ctrl\_bytes*—The number of outbound control bytes.

*data\_pkts*—The number of outbound data packets.

*ctrl\_pkts*—The number of outbound control packets.

*ctrl\_pkts*—The number of outbound packets that were dropped.

**Recommended Action** None.

## 722032

**Error Message** %ASA-5-722032: Group *group* User *user-name* IP *IP\_address* New SVC connection replacing old connection.

**Explanation** A new SSL VPN client (SVC) connection is replacing an existing one.

**Recommended Action** User may be having trouble connecting. The SVC log should be examined.

## 722033

**Error Message** %ASA-5-722033: Group *group* User *user-name* IP *IP\_address* First SVC connection established for SVC session.

**Explanation** Informative message only.

**Recommended Action** None.

## 722034

**Error Message** %ASA-5-722034: Group *group* User *user-name* IP *IP\_address* New SVC connection, no existing connection.

**Explanation** This message occurs during a reconnection attempt. A new SSL VPN client (SVC) connection is replacing a previously closed connection. There is no existing connection for this session because the connection was already dropped by the SVC or the security appliance.

**Recommended Action** The user may be having trouble connecting. The device and SVC log should be examined.

## 722035

**Error Message** %ASA-3-722035: Group *group* User *user-name* IP *IP\_address* Transmitting large packet *length* (threshold *threshold*).

**Explanation** A large packet was sent to the client. The source of the packet may not be aware of the MTU of the client.

*length*—The length of the large packet.

+*num*—The threshold.

**Recommended Action** None.

## 722036

**Error Message** %ASA-3-722036: Group *group* User *user-name* IP *IP\_address* Received large packet *length* (threshold *threshold*).

**Explanation** A large packet was received from the client.

*length*—The length of the large packet.

+*num*—The threshold.

**Recommended Action** Determine if the SVC is compatible with the security appliance and correct as necessary.

## 722037

**Error Message** %ASA-5-722037: Group *group* User *user-name* IP *IP\_address* SVC closing connection: *reason*.

**Explanation** An SSL VPN client (SVC) connection was terminated for the given reason.

*reason*—The reason the SVC connection was terminated.

**Recommended Action** This may be normal, or the user may be having trouble connecting. The SVC log should be examined.

## 722038

**Error Message** %ASA-5-722038: Group *group-name* User *user-name* IP *IP\_address* SVC terminating session: *reason*.

**Explanation** An SSL VPN client (SVC) session was terminated for the given reason.

*reason*—The reason the SVC session was terminated.

**Recommended Action** This may be normal, or the user may be having trouble connecting. The SVC log should be examined if the reason for termination is unexpected.

## 722039

**Error Message** %ASA-6-723001: Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Citrix ICA connection *connection* is up.

**Explanation** The Citrix connection is up.

*group-name*—The name of the Citrix group.

*user-name*—The name of the Citrix user.

*IP\_address*—The IP address of the Citrix user.

*connection*—The Citrix connection identifier.

**Recommended Action** None.

## 723002

**Error Message** %ASA-6-723002: Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Citrix ICA connection *connection* is down.

**Explanation** The Citrix connection is down.

*group-name*—The name of the Citrix group.

*user-name*—The name of the Citrix user.

*IP\_address*—The IP address of the Citrix user.

*connection*—The Citrix connection identifier.

**Recommended Action** No action is required when the Citrix ICA connection is terminated intentionally by the client, the server, or the security appliance administrator. However, if this is not the case, verify that the WebVPN session in which the Citrix ICA connection is set up is still active. If it is inactive, then receiving this message is normal. If the WebVPN session is still active, verify that the ICA client and Citrix server both work properly and that there is no error displayed. If not, bring either or both up or respond to any error. If this message is still received, contact the Cisco TAC and provide the following information:

- Network topology.

- Delay and packet loss.
- Citrix server configuration.
- Citrix ICA client information.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723003

**Error Message** %ASA-7-723003: No memory for WebVPN Citrix ICA connection *connection*.

**Explanation** The security appliance is running out of memory. The Citrix connection was rejected. *connection*—The Citrix connection identifier.

**Recommended Action** Verify that the security appliance is working properly. Pay special attention to memory and buffer usage. If the security appliance is under heavy load, buy more memory and upgrade the security appliance or reduce the load on the security appliance. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723004

**Error Message** %ASA-7-723004: WebVPN Citrix encountered bad flow control *flow*.

**Explanation** ASA internal flow control mismatch.

**Recommended Action** This issue can be caused by massive data flow, such as might occur during stress testing or with a high volume of ICA connections. Reduce ICA connectivity to the security appliance. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723005

**Error Message** %ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.

**Explanation** The security appliance was unable to create a new channel for Citrix.

**Recommended Action** Verify that the Citrix ICA client and the Citrix server are still alive. If not, bring them back up and retest. Check the security appliance load, paying special attention to memory and buffer usage. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723006

**Error Message** %ASA-7-723006: WebVPN Citrix SOCKS errors.

**Explanation** An internal Citrix SOCKS error has occurred on the security appliance.

**Recommended Action** Verify that the Citrix ICA client is working properly. In addition, check the network connection status between the Citrix ICA client and the security appliance, paying attention to packet loss and so forth. Resolve any abnormal network conditions. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723007

**Error Message** %ASA-7-723007: WebVPN Citrix ICA connection *connection* list is broken.

**Explanation** ASA internal Citrix connection list is broken.

*connection*—The Citrix connection identifier.

**Recommended Action** Verify that the security appliance is working properly, paying special attention to memory and buffer usage. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.

- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723008

**Error Message** %ASA-7-723008: WebVPN Citrix ICA SOCKS Server *server* is invalid.

**Explanation** An attempt was made to access a Citrix Socks server that does not exist.  
*server*—The Citrix server identifier.

**Recommended Action** Verify that the security appliance is working properly. Notice if there is any memory/buffer leakage. If this issue happens frequently, capture information about memory usage, the network topology, and the conditions when this message is received. Send this information to Cisco TAC for review. Make sure the WebVPN session is still up while this message is being received. If not, determine the reason that the WebVPN session is down. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723009

**Error Message** %ASA-7-723009: Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Citrix received data on invalid connection *connection*.

**Explanation** Data was received on a Citrix connection that does not exist.  
*group-name*—The name of the Citrix group.  
*user-name*—The name of the Citrix user.  
*IP\_address*—The IP address of the Citrix user.  
*connection*—The Citrix connection identifier.

**Recommended Action** The original published Citrix application connection was probably terminated, and the remaining active published applications lost connectivity. Restart all published applications to generate a new Citrix ICA tunnel. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723010

**Error Message** %ASA-7-723010: Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Citrix received closing channel *channel* for invalid connection *connection*.

**Explanation** An abort was received on a Citrix connection that does not exist.

*group-name*—The name of the Citrix group.

*user-name*—The name of the Citrix user.

*IP\_address*—The IP address of the Citrix user.

*connection*—The Citrix connection identifier.

*channel*—The Citrix channel identifier.

*connection*—The Citrix connection identifier.

**Recommended Action** This can be caused by massive data flow (such as stress testing) or a high volume of ICA connections, especially during network delay or packet loss. To eliminate the message, reduce the number of ICA connections to the security appliance, obtain more memory for the security appliance, or resolve the network problems. .

## 723011

**Error Message** %ASA-7-723011: Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Citrix receives bad SOCKS *socks* message length *msg-length*. Expected length is *exp-msg-length*.

**Explanation** The Citrix SOCKS message length is incorrect.

*group-name*—The name of the Citrix group.

*user-name*—The name of the Citrix user.

*IP\_address*—The IP address of the Citrix user.

**Recommended Action** Verify that the Citrix ICA client is working properly. In addition, check the network connection status between the ICA client and the security appliance, paying attention to packet loss and so forth. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.



## 723012

**Error Message** %ASA-7-723012: Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Citrix received bad SOCKS *socks* message format.

**Explanation** Citrix SOCKS message format is incorrect.

*group-name*—The name of the Citrix group.

*user-name*—The name of the Citrix user.

*IP\_address*—The IP address of the Citrix user.

**Recommended Action** Verify that the Citrix ICA client is working properly. In addition, check the network connection status between the ICA client and the security appliance, paying attention to packet loss and so forth. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated message.

## 723013

**Error Message** %ASA-7-723013: WebVPN Citrix encountered invalid connection *connection* during periodic timeout.

**Explanation** The ASA internal Citrix timer has expired and the Citrix connection is invalid.

*connection*—The Citrix connection identifier.

**Recommended Action** Check the network connection between the Citrix ICA client and the security appliance, and between the security appliance and the Citrix server. Resolve any abnormal network conditions, especially delay and packet loss. Verify that the security appliance works properly, paying special attention to memory or buffer problems. If the security appliance is under heavy load, obtain more memory, upgrade the security appliance, or reduce the load. If this message is still received, contact the Cisco TAC and provide the following information:

- Output from the **show mem detail** command when the problem is occurring.
- Output from the **show blocks all** when the problem is occurring.
- Steps to reproduce the problem.
- Complete text of all associated messages.

## 723014

**Error Message** %ASA-7-723014: Group *group-name*, User *user-name*, IP *IP\_address*: WebVPN Citrix TCP connection *connection* to server *server* on channel *channel* initiated.

**Explanation** The security appliance internal Citrix Secure Gateway is connected to the Citrix server.

*group-name*—The name of the Citrix group.

*user-name*—The name of the Citrix user.

*IP\_address*—The IP address of the Citrix user.

*connection*—The connection name.

*server*—The Citrix server identifier.

*channel*—The Citrix channel identifier (hexadecimal).

**Recommended Action** None.

## 724001

**Error Message** %ASA-4-724001: Group *group-name* User *user-name* IP *IP\_address* WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.

**Explanation** The session was not allowed as an error occurred when processing the CSD Host Integrity Check results on the security appliance.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

**Recommended Action** Determine if the client firewall is truncating long URLs. Uninstall CSD from the client and reconnect to the security appliance.

## 724002

**Error Message** %ASA-4-724002: Group *group-name* User *user-name* IP *IP\_address* WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.

**Explanation** CSD is not running on the client machine.

*group-name*—The name of the group.

*user-name*—The name of the user.

*IP\_address*—The IP address.

**Recommended Action** Verify that the end user is able to properly install and run CSD on the client machine.

## 725001

**Error Message** %ASA-6-725001 Starting SSL handshake with *remote\_device* *interface\_name*:*IP\_address/port* for *SSL\_version* session.

**Explanation** Indicates that a SSL handshake has started with the remote device.

*remote\_device*—Either the server or the client, depending on the device that initiated the connection.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

*SSL\_version*—The SSL version for the SSL handshake (SSLv3 or TLSv1).

**Recommended Action** None.

## 725002

**Error Message** %ASA-6-725002 Device completed SSL handshake with *remote\_device* *interface\_name*:*IP\_address/port*

**Explanation** The SSL handshake has completed successfully with the remote device.

*remote\_device*—Either the server or the client, depending on the device that initiated the connection.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725003

**Error Message** %ASA-6-725003 SSL client *interface\_name*:*IP\_address/port* requesting to resume previous session.

**Explanation** The remote device is trying to resume a previous SSL session.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725004

**Error Message** %ASA-6-725004 Device requesting certificate from SSL client *interface\_name:IP\_address/port* for authentication.

**Explanation** The security appliance has requested a client certificate for authentication.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725005

**Error Message** %ASA-6-725005 SSL server *interface\_name:IP\_address/port* requesting our device certificate for authentication.

**Explanation** The server has requested the certificate of the security appliance for authentication.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725006

**Error Message** %ASA-6-725006 Device failed SSL handshake with *remote\_device* *interface\_name:IP\_address/port*

**Explanation** The SSL handshake with the remote device has failed.

*remote\_device*—Either the server or the client depending on the device that initiates the connection.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** Look for message 725014, which indicates the reason for the failure.

## 725007

**Error Message** %ASA-6-725007 SSL session with *remote\_device interface\_name:IP\_address/port* terminated.

**Explanation** The SSL session has terminated.

*remote\_device*—Either the server or the client depending on the device that initiates the connection.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725008

**Error Message** %ASA-7-725008 SSL client *interface\_name:IP\_address/port* proposes the following *number* cipher(s).

**Explanation** Lists the number of ciphers proposed by the remote SSL device.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

*number*—The number of ciphers in the proposal.

**Recommended Action** None.

## 725009

**Error Message** %ASA-7-725009 Device proposes the following *number* cipher(s) to SSL server *interface\_name:IP\_address/port*.

**Explanation** Lists the number of ciphers proposed to the SSL server.

*number*—The number of ciphers in the proposal.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725010

**Error Message** %ASA-7-725010 Device supports the following *number* cipher(s).

**Explanation** Identifies the number of ciphers supported by the security appliance for a SSL session.  
*number*—The number of supported ciphers.

**Recommended Action** None.

## 725011

**Error Message** %ASA-7-725011 Cipher[*order*] : *cipher\_name*

**Explanation** This message always follows message 725008,725009 and 725010. It indicates the cipher name and its order of preference.

*order*—The order of the cipher in the cipher list.

*cipher\_name*—The name of the cipher from the cipher list.

## 725012

**Error Message** %ASA-7-725012 Device chooses cipher : *cipher\_name* for SSL session with client *interface\_name:IP\_address/port*

**Explanation** Identifies the cipher that was chosen by the Cisco device for the SSL session.

*cipher\_name*—The name of the cipher from the cipher list.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725013

**Error Message** %ASA-7-725013 SSL Server *interface\_name:IP\_address/port* chooses cipher : *cipher\_name*

**Explanation** Identifies the cipher that was chosen by the server for the SSL session.

*cipher\_name*—The name of the cipher from the cipher list.

*interface\_name*—The interface that the SSL session is using.

*IP\_address*—The remote device IP address.

*port*—The remote device IP port number.

**Recommended Action** None.

## 725014

**Error Message** %ASA-7-725014 SSL lib error. Function: *function* Reason: *reason*

**Explanation** Identifies the reason for failure of the SSL handshake.

*function*—The function name where the failure is reported.

*reason*—The description of the failure condition.

**Recommended Action** Include this message when reporting any SSL-related issue.

## 726001

**Error Message** %PIX|ASA-6-726001: Inspected *im\_protocol im\_service* Session between Client *im\_client\_1* and *im\_client\_2* Packet flow from *src\_ifc:/sip/sport* to *dest\_ifc:/dip/dport* Action: *action* Matched Class *class\_map\_id class\_map\_name*

**Explanation** This event is generated when an instant message (IM) inspection is performed on an IM message and the specified criteria is satisfied. The configured action is taken.

*im\_protocol*—MSN IM or Yahoo IM.

*im\_service*—The IM services, such as: chat, conference, file transfer, voice, video, games, or unknown.

*im\_client\_1, im\_client\_2*—The client peers that are using the IM service in the session: *client\_login\_name* or “?”.

*src\_ifc*—The source interface name.

*sip*—The source IP address.

*sport*—The source port.

*dest\_ifc*—The destination interface name.

*dip*—The destination IP address.

*dport*—The destination port.

*action*—The action taken: reset connection, dropped connection, or received.

*class\_map\_id*—The matched class-map ID.

*class\_map\_name*—The matched class-map name.

**Recommended Action** None.







## Messages Listed by Severity Level

---

This appendix contains the following sections:

- [Alert Messages, Severity 1, page A-1](#)
- [Critical Messages, Severity 2, page A-3](#)
- [Error Messages, Severity 3, page A-4](#)
- [Warning Messages, Severity 4, page A-14](#)
- [Notification Messages, Severity 5, page A-22](#)
- [Informational Messages, Severity 6, page A-29](#)
- [Debugging Messages, Severity 7, page A-40](#)



**Note**

The Cisco ASA does not send severity 0, emergency messages to syslog. These are analogous to a UNIX panic message, and denote an unstable system.

---

### Alert Messages, Severity 1

The following messages appear at severity 1, alerts:

- `%PIXIASA-1-101001: (Primary) Failover cable OK.`
- `%PIXIASA-1-101002: (Primary) Bad failover cable.`
- `%PIXIASA-1-101003: (Primary) Failover cable not connected (this unit).`
- `%PIXIASA-1-101004: (Primary) Failover cable not connected (other unit).`
- `%PIXIASA-1-101005: (Primary) Error reading failover cable status.`
- `%PIXIASA-1-102001: (Primary) Power failure/System reload other side.`
- `%PIXIASA-1-103001: (Primary) No response from other firewall (reason code = code).`
- `%PIXIASA-1-103002: (Primary) Other firewall network interface interface_number OK.`
- `%PIXIASA-1-103003: (Primary) Other firewall network interface interface_number failed.`
- `%PIXIASA-1-103004: (Primary) Other firewall reports this firewall failed.`
- `%PIXIASA-1-103005: (Primary) Other firewall reporting failure.`
- `%PIXIASA-1-104001: (Primary) Switching to ACTIVE (cause: string).`
- `%PIXIASA-1-104002: (Primary) Switching to STNDBY (cause: string).`

- %PIXIASA-1-104003: (Primary) Switching to FAILED.
- %PIXIASA-1-104004: (Primary) Switching to OK.
- %PIXIASA-1-105001: (Primary) Disabling failover.
- %PIXIASA-1-105002: (Primary) Enabling failover.
- %PIXIASA-1-105003: (Primary) Monitoring on interface interface\_name waiting
- %PIXIASA-1-105004: (Primary) Monitoring on interface interface\_name normal
- %PIXIASA-1-105005: (Primary) Lost Failover communications with mate on interface interface\_name.
- %PIXIASA-1-105006: (Primary) Link status 'Up' on interface interface\_name.
- %PIXIASA-1-105007: (Primary) Link status 'Down' on interface interface\_name.
- %PIXIASA-1-105008: (Primary) Testing interface interface\_name.
- %PIXIASA-1-105009: (Primary) Testing on interface interface\_name {Passed|Failed}.
- %PIXIASA-1-105011: (Primary) Failover cable communication failure
- %PIXIASA-1-105020: (Primary) Incomplete/slow config replication
- %PIXIASA-1-105021: (failover\_unit) Standby unit failed to sync due to a locked context\_name config. Lock held by lock\_owner\_name
- %PIXIASA-1-105031: Failover LAN interface is up
- %PIXIASA-1-105032: LAN Failover interface is down
- %PIXIASA-1-105034: Receive a LAN\_FAILOVER\_UP message from peer.
- %PIXIASA-1-105035: Receive a LAN failover interface down msg from peer.
- %PIXIASA-1-105036: dropped a LAN Failover command message.
- %PIXIASA-1-105037: The primary and standby units are switching back and forth as the active unit.
- %PIXIASA-1-105038: (Primary) Interface count mismatch
- %PIXIASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %PIXIASA-1-105040: (Primary) Mate failover version is not compatible.
- %PIXIASA-1-105042: (Primary) Failover interface OK
- %PIXIASA-1-105043: (Primary) Failover interface failed
- %PIXIASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.
- %PIXIASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %PIXIASA-1-105046 (Primary|Secondary) Mate has a different chassis
- %PIXIASA-1-105047: Mate has a io\_card\_name1 card in slot slot\_number which is different from my io\_card\_name2
- %ASA-1-105048: (unit) Mate's service module (application) is different from mine (application)
- %PIXIASA-1-106021: Deny protocol reverse path check from source\_address to dest\_address on interface interface\_name
- %PIXIASA-1-106022: Deny protocol connection spoof from source\_address to dest\_address on interface interface\_name

- %PIX|ASA-1-106101 The number of ACL log deny-flows has reached limit (number).
- %PIX|ASA-1-107001: RIP auth failed from IP\_address: version=number, type=string, mode=string, sequence=number on interface interface\_name
- %PIX|ASA-1-107002: RIP pkt failed from IP\_address: version=number on interface interface\_name
- %PIX|ASA-1-111111 error\_message
- %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error error\_string).
- %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error\_string).
- %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error\_string).
- %ASA-n-216001: internal error in: function: message
- %ASA|PIX-1-332004: Web Cache IP\_address/service\_ID lost
- %PIX|ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.
- %PIX|ASA-1-709004: (Primary) End Configuration Replication (ACT)
- %PIX|ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %PIX|ASA-1-709006: (Primary) End Configuration Replication (STB)

## Critical Messages, Severity 2

The following messages appear at severity 2, critical:

- %PIX|ASA-2-106001: Inbound TCP connection denied from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name
- %PIX|ASA-2-106002: protocol Connection denied by outbound list acl\_ID src inside\_address dest outside\_address
- %PIX|ASA-2-106006: Deny inbound UDP from outside\_address/outside\_port to inside\_address/inside\_port on interface interface\_name.
- %PIX|ASA-2-106007: Deny inbound UDP from outside\_address/outside\_port to inside\_address/inside\_port due to DNS {Response|Query}.
- %PIX|ASA-2-106013: Dropping echo request from IP\_address to PAT address IP\_address
- %PIX|ASA-2-106016: Deny IP spoof from (IP\_address) to IP\_address on interface interface\_name.
- %PIX|ASA-2-106017: Deny IP due to Land Attack from IP\_address to IP\_address
- %PIX|ASA-2-106018: ICMP packet type ICMP\_type denied by outbound list acl\_ID src inside\_address dest outside\_address
- %PIX|ASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP\_address to IP\_address
- %PIX|ASA-2-106024: Access rules memory exhausted
- %PIX|ASA-2-108002: SMTP replaced string: out source\_address in inside\_address data: string
- %PIX|ASA-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dset\_port. Data:string
- %PIX|ASA-2-109011: Authen Session Start: user 'user', sid number

- %PIXIASA-2-112001: (string:dec) Clear complete.
- %PIXIASA-2-201003: Embryonic limit exceeded nconns/elimit for outside\_address/outside\_port (global\_address) inside\_address/inside\_port on interface interface\_name
- %PIXIASA-2-214001: Terminating manager session from IP\_address on interface interface\_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %PIXIASA-2-215001:Bad route\_compress() call, sdb= number
- %ASA-n-216001: internal error in: function: message
- %PIXIASA-2-217001: No memory for string in string
- %PIXIASA-2-218001: Failed Identification Test in slot# [fail#/res].
- %PIXIASA-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
- %PIXIASA-2-218003: Module Version in <slot#> is obsolete. The module in slot = <slot#> is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.
- %PIXIASA-2-218004: Failed Identification Test in slot# [fail#/res]
- %PIXIASA-2-304007: URL Server IP\_address not responding, ENTERING ALLOW mode.
- %PIXIASA-2-304008: LEAVING ALLOW mode, URL Server is up.
- %PIXIASA-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src\_ifc:sip/sport to dest\_ifc:dip/dport
- %PIXIASA-2-709007: Configuration replication failed for command command
- %PIXIASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available\_size, used value
- %PIXIASA-2-713176: Device\_type memory resources are critical, IKE key acquire message on interface interface\_number, for Peer IP\_address ignored
- %PIXIASA-2-717008: Insufficient memory to process\_requiring\_memory.
- %PIXIASA-2-717011: Unexpected event event event\_ID

## Error Messages, Severity 3

The following messages appear at severity 3, errors:

- %PIXIASA-3-105010: (Primary) Failover message block alloc failed
- %PIXIASA-3-106010: Deny inbound protocol src interface\_name:dest\_address/dest\_port dst interface\_name:source\_address/source\_port
- %PIXIASA-3-106011: Deny inbound (No xlate) string
- %PIXIASA-3-106014: Deny inbound icmp src interface\_name: IP\_address dst interface\_name: IP\_address (type dec, code dec)
- %PIX-3-107003: RIP: Attempted reference of stale data encountered in function, line: line\_num
- %PIXIASA-3-109010: Auth from inside\_address/inside\_port to outside\_address/outside\_port failed (too many pending auths) on interface interface\_name.
- %PIXIASA-3-109013: User must authenticate before using this service
- %PIXIASA-3-109016: Can't find authorization ACL acl\_ID for user 'user'

- %PIX|ASA-3-109018: Downloaded ACL acl\_ID is empty
- %PIX|ASA-3-109019: Downloaded ACL acl\_ID has parsing error; ACE string
- %PIX|ASA-3-109020: Downloaded ACL has config error; ACE
- %PIX|ASA-3-109023: User from source\_address/source\_port to dest\_address/dest\_port on interface outside\_interface must authenticate before using this service.
- %PIX|ASA-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %PIX|ASA-3-109032: Unable to install ACL access\_list, downloaded for user username; Error in ACE: ace.
- %PIX|ASA-3-113001: Unable to open AAA session. Session limit [limit] reached.
- %PIX|ASA-3-113018: User: user, Unsupported downloaded ACL Entry: ACL\_entry, Action: action
- %PIX|ASA-3-113020: Kerberos error : Clock skew with server ip\_address greater than 300 seconds
- %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error\_string).
- %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error\_string).
- %ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.
- %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error\_string).
- %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error error\_string).
- %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error\_string).
- %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error error\_string).
- %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error error\_string).
- %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error error\_string).
- %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.
- %PIX|ASA-3-201002: Too many TCP connections on {static|late} global\_address! econns nconns
- %PIX|ASA-3-201004: Too many UDP connections on {static|late} global\_address! udp connections limit
- %PIX|ASA-3-201005: FTP data connection failed for IP\_address IP\_address
- %PIX|ASA-3-201006: RCMD backconnection failed for IP\_address/port
- %PIX|ASA-3-201008: The security appliance is disallowing new connections.
- %PIX|ASA-3-201009: TCP connection limit of number for host IP\_address on interface\_name exceeded
- %PIX|ASA-3-201010: Embryonic connection limit exceeded econns/limit for dir packet from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name

- %PIXIASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if\_name
- %PIXIASA-3-202005: Non-embryonic in embryonic list outside\_address/outside\_port inside\_address/inside\_port
- %PIXIASA-3-202011: Connection limit exceeded econns/limit for dir packet from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name
- %PIXIASA-3-208005: (function:line\_num) clear command return code
- %PIXIASA-3-210001: LU sw\_module\_name error = number
- %PIXIASA-3-210002: LU allocate block (bytes) failed.
- %PIXIASA-3-210003: Unknown LU Object number
- %PIXIASA-3-210005: LU allocate connection failed
- %PIXIASA-3-210006: LU look NAT for IP\_address failed
- %PIXIASA-3-210007: LU allocate xlate failed
- %PIXIASA-3-210008: LU no xlate for inside\_address/inside\_port outside\_address/outside\_port
- %PIXIASA-3-210010: LU make UDP connection for outside\_address:outside\_port inside\_address:inside\_port failed
- %PIXIASA-3-210020: LU PAT port port reserve failed
- %PIXIASA-3-210021: LU create static xlate global\_address ifc interface\_name failed
- %PIXIASA-3-211001: Memory allocation Error
- %PIXIASA-3-211003: CPU utilization for number seconds = percent
- %PIXIASA-3-212001: Unable to open SNMP channel (UDP port port) on interface interface\_number, error code = code
- %PIXIASA-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface\_number, error code = code
- %PIXIASA-3-212003: Unable to receive an SNMP request on interface interface\_number, error code = code, will try again.
- %PIXIASA-3-212004: Unable to send an SNMP response to IP Address IP\_address Port port interface interface\_number, error code = code
- %PIXIASA-3-212005: incoming SNMP request (number bytes) on interface interface\_name exceeds data buffer size, discarding this SNMP request.
- %PIXIASA-3-212006: Dropping SNMP request from source\_address/source\_port to interface\_name:dest\_address/dest\_port because: reason.
- %PIXIASA-3-213001: PPTP control daemon socket io string, errno = number.
- %PIXIASA-3-213002: PPTP tunnel hashtable insert failed, peer = IP\_address.
- %PIXIASA-3-213003: PPP virtual interface interface\_number isn't opened.
- %PIXIASA-3-213004: PPP virtual interface interface\_number client ip allocation failed.
- %ASA-n-216001: internal error in: function: message
- PIXIASA-3-216002: Unexpected event (major: major\_id, minor: minor\_id) received by task\_string in function at line: line\_num
- %PIXIASA-3-216003: Unrecognized timer timer\_ptr, timer\_id received by task\_string in function at line: line\_num

- %ASA-3-219002: I2C\_API\_name error, slot = slot\_number, device = device\_number, address = address, byte count = count. Reason: reason\_string
- %PIX|ASA-3-302019: H.323 library\_name ASN Library failed to initialize, error code number
- %PIX|ASA-3-302302: ACL = deny; no sa created
- %PIX|ASA-3-304003: URL Server IP\_address timed out URL url
- %PIX|ASA-3-304006: URL Server IP\_address not responding
- %PIX|ASA-3-305005: No translation group found for protocol src interface\_name:dest\_address/dest\_port dst interface\_name:source\_address/source\_port
- %PIX|ASA-3-305006: {outbound staticidentity|portmap|regular) translation creation failed for protocol src interface\_name:source\_address/source\_port dst interface\_name:dest\_address/dest\_port
- %PIX|ASA-3-305008: Free unallocated global IP address.
- %PIX|ASA-3-313001: Denied ICMP type=number, code=code from IP\_address on interface interface\_name
- %PIX|ASA-3-313008: Denied ICMPv6 type=number, code=code from IP\_address on interface interface\_name
- %PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
- %PIX|ASA-3-316001: Denied new tunnel to IP\_address. VPN peer limit (platform\_vpn\_peer\_limit) exceeded
- %PIX|ASA-3-317001: No memory available for limit\_slow
- %PIX|ASA-3-317002: Bad path index of number for IP\_address, number max
- %PIX|ASA-3-317003: IP routing table creation failure - reason
- %PIX|ASA-3-317004: IP routing table limit warning
- %PIX|ASA-3-317005: IP routing table limit exceeded - reason, IP\_address netmask
- %PIX|ASA-3-318001: Internal error: reason
- %PIX|ASA-3-318002: Flagged as being an ABR without a backbone area
- %PIX|ASA-3-318003: Reached unknown state in neighbor state machine
- %PIX|ASA-3-318004: area string Isid IP\_address mask netmask adv IP\_address type number
- %PIX|ASA-3-318005: Isid ip\_address adv IP\_address type number gateway gateway\_address metric number network IP\_address mask netmask protocol hex attr hex net-metric number
- %PIX|ASA-3-318006: if interface\_name if\_state number
- %PIX|ASA-3-318007: OSPF is enabled on interface\_name during idb initialization
- %PIX|ASA-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %PIX|ASA-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line\_num
- %PIX|ASA-3-319001: Acknowledge for arp update for IP address dest\_address not received (number).
- %PIX|ASA-3-319002: Acknowledge for route update for IP address dest\_address not received (number).
- %PIX|ASA-3-319003: Arp update for IP address address to NPn failed.
- %PIX|ASA-3-319004: Route update for IP address dest\_address failed (number).

- %PIXIASA-3-320001: The subject name of the peer cert is not allowed for connection
- %PIXIASA-3-322001: Deny MAC address MAC\_address, possible spoof attempt on interface interface
- %PIXIASA-3-322002: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is {statically|dynamically} bound to MAC Address MAC\_address\_2.
- %PIXIASA-3-322003: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is not bound to any MAC Address.
- %ASA-3-323001: Module in slot slotnum experienced a control channel communications failure.
- %ASA-3-323002: Module in slot slotnum is not able to shut down, shut down request not answered.
- %ASA-3-323003: Module in slot slotnum is not able to reload, reload request not answered.
- %ASA-3-323004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Hw-module reset is required before further use.
- %ASA-3-323005: Module in slot slotnum can not be powered on completely
- %ASA-3-323006: Module in slot slotnum experienced a data channel communication failure, data channel is DOWN.
- %PIXIASA-3-324000: Drop GTPv version message msg\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port Reason: reason
- %PIXIASA-3-324001: GTPv0 packet parsing error from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port, TID: tid\_value, Reason: reason
- %PIXIASA-3-324002: No PDP[MCB] exists to process GTPv0 msg\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port, TID: tid\_value
- %PIXIASA-3-324003: No matching request to process GTPv version msg\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port
- %PIXIASA-3-324004: GTP packet with version%d from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port is not supported
- %PIXIASA-3-324005: Unable to create tunnel from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port
- %PIXIASA-3-324006: GSN IP\_address tunnel limit tunnel\_limit exceeded, PDP Context TID tid failed
- %PIXIASA-3-324007: Unable to create GTP connection for response from source\_interface:source\_address/0 to dest\_interface:dest\_address/dest\_port
- %PIX-3-324300: Radius Accounting Request from from\_addr has an incorrect request authenticator
- %PIXIASA-3-324301: Radius Accounting Request has a bad header length hdr\_len, packet length pkt\_len
- %PIXIASA-3-325001: Router ipv6\_address on interface has conflicting ND (Neighbor Discovery) settings



- %PIX-3-325003: EUI-64 source address check failed. Dropped packet from interface\_in:source\_address/source\_port to dest\_address/dest\_port with source MAC address MAC\_address.
- %PIX|ASA-3-326001: Unexpected error in the timer library: error\_message
- %PIX|ASA-3-326002: Error in error\_message : error\_message
- %PIX|ASA-3-326004: An internal error occurred while processing a packet queue
- %PIX|ASA-3-326005: Mrib notification failed for (IP\_address, IP\_address)
- %PIX|ASA-3-326006: Entry-creation failed for (IP\_address, IP\_address)
- %PIX|ASA-3-326007: Entry-update failed for (IP\_address, IP\_address)
- %PIX|ASA-3-326008: MRIB registration failed
- %PIX|ASA-3-326009: MRIB connection-open failed
- %PIX|ASA-3-326010: MRIB unbind failed
- %PIX|ASA-3-326011: MRIB table deletion failed
- %PIX|ASA-3-326012: Initialization of string functionality failed
- %PIX|ASA-3-326013: Internal error: string in string line %d (%s)
- %PIX|ASA-3-326014: Initialization failed: error\_message error\_message
- %PIX|ASA-3-326015: Communication error: error\_message error\_message
- %PIX|ASA-3-326016: Failed to set un-numbered interface for interface\_name (string)
- %PIX|ASA-3-326017: Interface Manager error - string in string : string
- %PIX|ASA-3-326019: string in string : string
- %PIX|ASA-3-326020: List error in string : string
- %PIX|ASA-3-326021: Error in string : string
- %PIX|ASA-3-326022: Error in string : string
- %PIX|ASA-3-326023: string - IP\_address : string
- %PIX|ASA-3-326024: An internal error occurred while processing a packet queue.
- %PIX|ASA-3-326025: string
- %PIX|ASA-3-326026: Server unexpected error: error\_message
- %PIX|ASA-3-326027: Corrupted update: error\_message
- %PIX|ASA-3-326028: Asynchronous error: error\_message
- %PIX|ASA-3-327001: IP SLA Monitor: Cannot create a new process
- %PIX|ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work
- %PIX|ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize
- %PIX|ASA-3-328001: Attempt made to overwrite a set stub function in string.
- %PIX|ASA-3-329001: The string0 subblock named string1 was not removed
- ASA|PIX-3-331001: Dynamic DNS Update for 'fqdn\_name' <=> ip\_address failed
- %PIX|ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface\_name AC:ac\_name

- %PIXIASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface\_name AC:ac\_name
- %PIXIASA-3-403503: PPPoE:PPP link down:reason
- %PIXIASA-3-403504: PPPoE:No 'vpdn group group\_name' for PPPoE is created
- %PIXIASA-3-403507:PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group\_name
- %PIXIASA-3-404102: ISAKMP: Exceeded embryonic limit
- %PIXIASA-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside\_address/outside\_port to global\_address (inside\_address)/inside\_port on interface interface\_name
- %PIXIASA-3-414001: Failed to save logging buffer using file name filename to FTP server ftp\_server\_address on interface interface\_name: [fail\_reason]
- %PIXIASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail\_reason]
- %ASA-3-420001 : IPS card not up and fail-close mode used, dropping ICMP packet ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)"
- %ASA-3-421001: TCPIUDP flow from interface\_name:ip/port to interface\_name:ip/port is dropped because application has failed.
- %ASA-3-421003: Invalid data plane encapsulation.
- %ASA-3-421007: TCPIUDP flow from interface\_name:IP\_address/port to interface\_name:IP\_address/port is skipped because application has failed.
- %PIXIASA-3-610001: NTP daemon interface interface\_name: Packet denied from IP\_address
- %PIXIASA-3-610002: NTP daemon interface interface\_name: Authentication failed for packet from IP\_address
- %PIXIASA-3-611313: VPNClient: Backup Server List Error: reason
- %PIXIASA-3-702305: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) is rekeying due to sequence number rollover.
- %PIXIASA-3-702307: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) is rekeying due to data rollover.
- %PIXIASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %PIXIASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %PIXIASA-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value
- %PIXIASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %PIXIASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID\_Type
- %PIXIASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID\_Type
- %PIXIASA-3-713018: Unknown ID type during find of group name for certs, Type ID\_Type
- %PIXIASA-3-713020: No Group found by matching OU(s) from ID payload: OU\_value
- %PIXIASA-3-713022: No Group found matching peer\_ID or IP\_address for Pre-shared key peer IP\_address
- %PIXIASA-3-713032: Received invalid local Proxy Range IP\_address - IP\_address
- %PIXIASA-3-713033: Received invalid remote Proxy Range IP\_address - IP\_address

- %PIX|ASA-3-713042: IKE Initiator unable to find policy: Intf interface\_number, Src: source\_address, Dst: dest\_address
- %PIX|ASA-3-713043: Cookie/peer address IP\_address session already in progress
- %PIX|ASA-3-713047: Unsupported Oakley group: Group Diffie-Hellman group
- %PIX|ASA-3-713048: Error processing payload: Payload ID: id
- %PIX|ASA-3-713051: Terminating connection attempt: IPSEC not permitted for group (group\_name)
- %PIX|ASA-3-713056: Tunnel rejected: SA (SA\_name) not found for group (group\_name)!
- %PIX|ASA-3-713059: Tunnel Rejected: User (user) matched with group name, group-lock check failed.
- %PIX|ASA-3-713060: Tunnel Rejected: User (user) not member of group (group\_name), group-lock check failed.
- %PIX|ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source\_address, Dst: dest\_address!
- %PIX|ASA-3-713062: IKE Peer address same as our interface address IP\_address
- %PIX|ASA-3-713063: IKE Peer address not configured for destination IP\_address
- %PIX|ASA-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %PIX|ASA-3-713072: Password for user (user) too long, truncating to number characters
- %PIX|ASA-3-713081: Unsupported certificate encoding type encoding\_type
- %PIX|ASA-3-713082: Failed to retrieve identity certificate
- %PIX|ASA-3-713083: Invalid certificate handle
- %PIX|ASA-3-713084: Received invalid phase 1 port value (port) in ID payload
- %PIX|ASA-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %PIX|ASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %PIX|ASA-3-713088: Set Cert filehandle failure: no IPsec SA in group group\_name
- %PIX|ASA-3-713098: Aborting: No identity cert specified in IPsec SA (SA\_name)!
- %PIX|ASA-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %PIX|ASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %PIX|ASA-3-713107: IP\_Address request attempt failed!
- %PIX|ASA-3-713109: Unable to process the received peer certificate
- %PIX|ASA-3-713112: Failed to process CONNECTED notify (SPI SPI\_value)!
- %PIX|ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %PIX|ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID\_Type
- %PIX|ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID\_Type
- %PIX|ASA-3-713118: Detected invalid Diffie-Helmann group\_descriptor group\_number, in IKE area
- %PIX|ASA-3-713119: PHASE 1 COMPLETED
- %PIX|ASA-3-713122: Keep-alives configured keepalive\_type but peer IP\_address support keep-alives (type = keepalive\_type)

- %PIXIASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive\_type)
- %PIXIASA-3-713124: Received DPD sequence number rcv\_sequence\_# in DPD Action, description expected seq #
- %PIXIASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %PIXIASA-3-713128: Connection attempt to VCIPIP redirected to VCA peer IP\_address via load balancing
- %PIXIASA-3-713129: Received unexpected Transaction Exchange payload type: payload\_id
- %PIXIASA-3-713132: Cannot obtain an IP\_address for remote peer
- %PIXIASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group\_id) with phase 1 group(DH group DH group\_number)
- %PIXIASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection
- %PIXIASA-3-713138: Group group\_name not found and BASE GROUP default preshared key not configured
- %PIXIASA-3-713140: Split Tunneling Policy requires network list but none configured
- %PIXIASA-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id), Product product(id), Caps: capability\_value. Expected -- Vendor: vendor(id), Product: product(id), Caps: capability\_value
- %PIXIASA-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id), Product product(id), Caps: capability\_value
- %PIXIASA-3-713146: Could not add route for Hardware Client in network extension mode, address: IP\_address, mask: netmask
- %PIXIASA-3-713149: Hardware client security attribute attribute\_name was enabled but not requested.
- %PIXIASA-3-713152: Unable to obtain any rules from filter ACL\_tag to send to client for CPP, terminating connection.
- %PIXIASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %PIXIASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %PIXIASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
- %PIXIASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
- %PIXIASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %PIXIASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %PIXIASA-3-713167: Remote peer has failed user authentication - check configured username and password
- %PIXIASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %PIXIASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!

- %PIX|ASA-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
- %PIX|ASA-3-713185: Error: Username too long - connection aborted
- %PIX|ASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list\_text Character index (value) is illegal
- %PIX|ASA-3-713189: Attempted to assign network or broadcast IP\_address, removing (IP\_address) from pool.
- %PIX|ASA-3-713193: Received packet with missing payload, Expected payload: payload\_id
- %PIX|ASA-3-713194: IKE|IPSec Delete With Reason message: termination\_reason
- %PIX|ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
- %PIX|ASA-3-713198: User Authorization failed: user User authorization failed.
- %PIX|ASA-3-713203: IKE Receiver: Error reading from socket.
- %PIX|ASA-3-713205: Could not add static route for client address: IP\_address
- %PIX|ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
- %PIX|ASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule\_id
- %PIX|ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
- %PIX|ASA-3-713210: Cannot create dynamic map for Backup L2L entry rule\_id
- %PIX|ASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP\_address, mask: netmask
- %PIX|ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP\_address, mask: netmask
- %PIX|ASA-3-713217: Skipping unrecognized rule: action: action client type: client\_type client version: client\_version
- %PIX|ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.
- %PIX|ASA-3-713226: Connection failed with peer IP\_address, no trust-point defined in tunnel-group tunnel\_group
- %PIX|ASA-3-713230 Internal Error, ike\_lock trying to lock bit that is already locked for type type
- %PIX|ASA-3-713231 Internal Error, ike\_lock trying to unlock bit that is not locked for type type
- %PIX|ASA-3-713232 SA lock refCnt = value, bitmask = hexvalue, p1\_decrypt\_cb = value, qm\_decrypt\_cb = value, qm\_hash\_cb = value, qm\_spi\_ok\_cb = value, qm\_dh\_cb = value, qm\_secret\_key\_cb = value, qm\_encrypt\_cb = value
- %PIX|ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client
- %PIX|ASA-3-713902 descriptive\_event\_string
- %ASA-3-716056: Group group-name User user-name IP IP\_address Authentication to SSO server name: name type type failed reason: reason
- %PIX|ASA-3-717001: Querying keypair failed.
- %PIX|ASA-3-717002: Certificate enrollment failed for trustpoint trustpoint\_name. Reason: reason\_string.
- %PIX|ASA-3-717009: Certificate validation failed. Reason: reason\_string.
- %PIX|ASA-3-717010: CRL polling failed for trustpoint trustpoint\_name.

- %PIXIASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint\_name at time\_of\_failure
- %PIXIASA-3-717015: CRL received from issuer is too large to process (CRL size = crl\_size, maximum CRL size = max\_crl\_size)
- %PIXIASA-3-717017: Failed to query CA certificate for trustpoint trustpoint\_name from enrollment\_url
- %PIXIASA-3-717018: CRL received from issuer has too many entries to process (number of entries = number\_of\_entries, maximum number allowed = max\_allowed)
- %PIXIASA-3-717019: Failed to insert CRL for trustpoint trustpoint\_name. Reason: failure\_reason.
- %PIXIASA-3-717021 Certificate data could not be verified. Locate Reason: reason\_string serial number: serial number, subject name: subject name, key length key length bits.
- %PIXIASA-3-717023 SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason\_string.
- %PIXIASA-3-717027 Certificate chain failed validation. reason\_string.
- %PIX-3-717032 OCSP status check failed. Reason: reason\_string.
- %ASA-3-719002: Email Proxy session pointer from source\_address has been terminated due to reason error.
- %ASA-3-719008: Email Proxy service is shutting down.
- %ASA-3-722007: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722008: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722009: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722020: Group group User user-name IP IP\_address No address available for SVC connection
- %ASA-3-722021: Group group User user-name IP IP\_address Unable to start compression due to lack of memory resources
- %ASA-3-722035: Group group User user-name IP IP\_address Transmitting large packet length (threshold threshold).
- %ASA-3-722036: Group group User user-name IP IP\_address Received large packet length (threshold threshold).

## Warning Messages, Severity 4

The following messages appear at severity 4, warning:

- %PIXIASA-4-106023: Deny protocol src [interface\_name:source\_address/source\_port] dst interface\_name:dest\_address/dest\_port [type {string}, code {code}] by access\_group acl\_ID
- %PIXIASA-4-106027:Failed to determine the security context for the packet:vlan source Vlan#:ethertype src sourceMAC dst destMAC
- %PIXIASA-4-106100: access-list acl\_ID {permitted | denied | est-allowed} protocol interface\_name/source\_address(source\_port) -> interface\_name/dest\_address(dest\_port) hit-cnt number ({first hit | number-second interval})

- %PIX|ASA-4-108004: action\_class: action ESMTP req\_resp from src\_ifc:sipldport to dest\_ifc:dipldport;further\_info
- %PIX|ASA-4-109017: User at IP\_address exceeded auth proxy connection limit (max)
- %PIX|ASA-4-109022: exceeded HTTPS proxy process limit
- %PIX|ASA-4-109027: [aaa protocol] Unable to decipher response message Server = server\_IP\_address, User = user
- %PIX|ASA-4-109028: aaa bypassed for same-security traffic from ingress\_interface:source\_address/source\_port to egress\_interface:dest\_address/dest\_port
- %PIX|ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access\_list source | dest netmask netmask.
- %PIX|ASA-4-109031: NT Domain Authentication Failed: rejecting guest login for username.
- %PIX|ASA-4-109033: Authentication failed for admin user user from src\_IP. Interactive challenge processing is not supported for protocol connections
- %PIX|ASA-4-109034: Authentication failed for network user user from src\_IP/port to dst\_IP/port. Interactive challenge processing is not supported for protocol connections
- %PIX|ASA-4-113019: Group = group, Username = user, IP = peer\_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %PIX|ASA-4-209003: Fragment database limit of number exceeded: src = source\_address, dest = dest\_address, proto = protocol, id = number
- %PIX|ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source\_address, dest = dest\_address, proto = protocol, id = number
- %PIX|ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %PIX|ASA-4-308002: static global\_address inside\_address netmask netmask overlapped with global\_address inside\_address
- %PIX|ASA-4-313004: Denied ICMP type=icmp\_type, from source\_address on interface interface\_name to dest\_address: no matching session
- %PIX|ASA-4-313005: No matching connection for ICMP error message: icmp\_msg\_info on interface\_name interface. Original IP payload: embedded\_frame\_info icmp\_msg\_info = icmp src src\_interface\_name:src\_address dst dest\_interface\_name:dest\_address (type icmp\_type, code icmp\_code) embedded\_frame\_info = prot src source\_address/source\_port dst dest\_address/dest\_port
- %PIX|ASA-4-325002: Duplicate address ipv6\_address/MAC\_address on interface
- %PIX|ASA-4-335005: NAC Downloaded ACL parse failure - host-address
- %PIX|ASA-4-4000nn: IPS:number string from IP\_address to IP\_address on interface interface\_name
- %PIX|ASA-4-401001: Shuns cleared
- %PIX|ASA-4-401002: Shun added: IP\_address IP\_address port port
- %PIX|ASA-4-401003: Shun deleted: IP\_address
- %PIX|ASA-4-401004: Shunned packet: IP\_address ==> IP\_address on interface interface\_name
- %PIX|ASA-4-401005: Shun add failed: unable to allocate resources for IP\_address IP\_address port port

- %PIXIASA-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=dest\_address, prot=protocol, spi=number
- %PIXIASA-4-402102: decapsulate: packet missing { AHIESP }, destadr=dest\_address, actual prot=protocol
- %PIXIASA-4-402103: identity doesn't match negotiated identity (ip) dest\_address= dest\_address, src\_addr= source\_address, prot= protocol, (ident) local=inside\_address, remote=remote\_address, local\_proxy=IP\_address/IP\_address/port/port, remote\_proxy=IP\_address/IP\_address/port/port
- %PIXIASA-4-402106: Rec'd packet not an IPSEC packet (ip) dest\_address= dest\_address, src\_addr= source\_address, prot= protocol
- %PIXIASA-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP to local\_IP with an invalid SPI.
- %PIXIASA-4-402115: IPSEC: Received a packet from remote\_IP to local\_IP containing act\_prot data instead of exp\_prot data.
- %PIXIASA-4-402116: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP . The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as pkt\_daddr, its source as pkt\_saddr, and its protocol as pkt\_prot . The SA specifies its local proxy as id\_daddr /id\_dmask /id\_dprot /id\_dport and its remote proxy as id\_saddr /id\_smask /id\_sprot /id\_sport .
- %PIXIASA-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote\_IP to local\_IP.
- %PIXIASA-4-402118: IPSEC: Received an protocol packet (SPI=spi, sequence number seq\_num) from remote\_IP (username) to local\_IP containing an illegal IP fragment of length frag\_len with offset frag\_offset.
- %PIXIASA-4-402119: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP that failed anti-replay checking.
- %PIXIASA-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP that failed authentication.
- %PIXIASA-4-402123: CRYPTO: The accel\_type hardware accelerator encountered an error (code= error\_string) while executing crypto command command .
- %PIXIASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel\_id=number, session\_id=number
- %PIXIASA-4-403102: PPP virtual interface interface\_name rcvd pkt with invalid protocol: protocol, reason: reason.
- %PIXIASA-4-403103: PPP virtual interface max connections reached.
- %PIXIASA-4-403104: PPP virtual interface interface\_name requires mschap for MPPE.
- %PIXIASA-4-403106: PPP virtual interface interface\_name requires RADIUS for MPPE.
- %PIXIASA-4-403107: PPP virtual interface interface\_name missing aaa server group info
- %PIXIASA-4-403108: PPP virtual interface interface\_name missing client ip address option
- %PIXIASA-4-403109: Rec'd packet not an PPTP packet. (ip) dest\_address= dest\_address, src\_addr= source\_address, data: string.
- %PIXIASA-4-403110: PPP virtual interface interface\_name, user: user missing MPPE key from aaa server.
- %PIXIASA-4-403505: PPPoE:PPP - Unable to set default route to IP\_address at interface\_name
- %PIXIASA-4-403506: PPPoE:failed to assign PPP IP\_address netmask netmask at interface\_name



- %PIX|ASA-4-404101: ISAKMP: Failed to allocate address for client from pool string
- %PIX|ASA-4-405001: Received ARP {request|response} collision from IP\_address/MAC\_address on interface interface\_name
- %PIX|ASA-4-405002: Received mac mismatch collision from IP\_address/MAC\_address for authenticated host
- %PIX|ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign\_address outside\_address[/outside\_port] to local\_address inside\_address[/inside\_port]
- %PIX|ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign\_address outside\_address[/outside\_port] to local\_address inside\_address[/inside\_port]
- %PIX|ASA-4-405103: H225 message from source\_address/source\_port to dest\_address/dest\_port contains bad protocol discriminator hex
- %PIX|ASA-4-405104: H225 message received from outside\_address/outside\_port to inside\_address/inside\_port before SETUP
- %PIX|ASA-4-405105: H323 RAS message AdmissionConfirm received from source\_address/source\_port to dest\_address/dest\_port without an AdmissionRequest
- %PIX|ASA-4-405106: H323 num channel is not created from %I/%d to %I/%d %s\n
- %PIX|ASA-4-405201: ILS ILS\_message\_type from inside\_interface:source\_IP\_address to outside\_interface:/destination\_IP\_address has wrong embedded address embedded\_IP\_address
- %PIX|ASA-4-405300: Radius Accounting Request received from from\_addr is not allowed
- %PIX|ASA-4-405301: Attribute attribute\_number does not match for user user\_ip
- %PIX|ASA-4-406001: FTP port command low port: IP\_address/port to IP\_address on interface interface\_name
- %PIX|ASA-4-406002: FTP port command different address: IP\_address(IP\_address) to IP\_address on interface interface\_name
- %PIX|ASA-4-407001: Deny traffic for local-host interface\_name:inside\_address, license limit of number exceeded
- %PIX|ASA-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside\_address/outside\_port to global\_address (inside\_address)/inside\_port on interface interface\_name
- %PIX|ASA-4-407003: Established limit for RPC services exceeded number
- %PIX|ASA-4-408001: IP route counter negative - reason, IP\_address Attempt: number
- %PIX|ASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %PIX|ASA-4-408003: can't track this type of object hex
- %PIX|ASA-4-409001: Database scanner: external LSA IP\_address netmask is lost, reinstalls
- %PIX|ASA-4-409002: db\_free: external LSA IP\_address netmask
- %PIX|ASA-4-409003: Received invalid packet: reason from IP\_address, interface\_name
- %PIX|ASA-4-409004: Received reason from unknown neighbor IP\_address
- %PIX|ASA-4-409005: Invalid length number in OSPF packet from IP\_address (ID IP\_address), interface\_name
- %PIX|ASA-4-409006: Invalid lsa: reason Type number, LSID IP\_address from IP\_address, IP\_address, interface\_name

- %PIXIASA-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP\_address netmask New: Destination IP\_address netmask
- %PIXIASA-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric : number area : string
- %PIXIASA-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID
- %PIXIASA-4-409010: Virtual link information found in non-backbone area: string
- %PIXIASA-4-409011: OSPF detected duplicate router-id IP\_address from IP\_address on interface interface\_name
- %PIXIASA-4-409012: Detected router with duplicate router ID IP\_address in area string
- %PIXIASA-4-409013: Detected router with duplicate router ID IP\_address in Type-4 LSA advertised by IP\_address
- %PIXIASA-4-409023: Attempting AAA Fallback method method\_name for request\_type request for user user :Auth-server group server\_tag unreachable
- %PIXIASA-4-410001: UDP DNS request from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.
- %PIXIASA-4-410003: action\_class: action DNS query\_response from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %ASA-4-4108004: action\_class: action ESMTP req\_resp from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %PIXIASA-4-411001: Line protocol on interface interface\_name changed state to up
- %PIXIASA-4-411002: Line protocol on interface interface\_name changed state to down
- %PIXIASA-4-411003: Configuration status on interface interface\_name changed state to downup
- %PIXIASA-4-411004: Configuration status on interface interface\_name changed state to up
- %PIXIASA-4-412001: MAC MAC\_address moved from interface\_1 to interface\_2
- %PIXIASA-4-412002: Detected bridge table full while inserting MAC MAC\_address on interface interface. Number of entries = num
- %ASA-4-413001: Module in slot slotnum is not able to shut down. Module Error: errnum message
- %ASA-4-413002: Module in slot slotnum is not able to reload. Module Error: errnum message
- %ASA-4-413003: Module in slot slotnum is not a recognized type
- %ASA-4-413004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Trying again.
- %PIXIASA-4-415016: policy-map map\_name: Maximum number of unanswered HTTP requests exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-4-416001: Dropped UDP SNMP packet from source\_interface :source\_IP/source\_port to dest\_interface:dest\_address/dest\_port; version (prot\_version) is not allowed through the firewall
- %PIXIASA-4-417001: Unexpected event received: number
- %PIXIASA-4-417004: Filter violation error: conn number (string:string) in string
- %PIXIASA-4-417006: No memory for string) in string. Handling: string
- %PIX-4-417008 AutoRP: removed string embedded group address1/mask1 on interface interface-name from address2 due to overlap address3/mask2

- %PIX-4-417009 AutoRp: discarded string on interface interface-name from address due to malformed packet
- %PIX|ASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol\_string from interface\_name IP\_address (port) to interface\_name IP\_address (port)
- %PIX|ASA-4-419001: Dropping TCP packet from src\_ifc:src\_IP/src\_port to dest\_ifc:dest\_IP/dest\_port, reason: MSS exceeded, MSS size, data size
- %ASA-4-419002: Received duplicate TCP SYN from in\_interface:src\_address/src\_port to out\_interface:dest\_address/dest\_port with different initial sequence number.
- %ASA-3-420001 : IPS card not up and fail-close mode used, dropping ICMP packet ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)"
- %ASA-4-420002 : IPS requested to drop ICMP packets ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)"
- %ASA-4-420003 : IPS requested to reset TCP connection from ifc\_in:SIP/SPORT to ifc\_out:DIP/DPORT"
- %PIX|ASA-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1
- %PIX|ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
- %PIX|ASA-4-422006: IP SLA Monitor Probe number: string
- %ASA-4-423001: { Allowed | Dropped } invalid NBNS pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423002: { Allowed | Dropped } mismatched NBNS pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423003: { Allowed | Dropped } invalid NBDGM pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423004: { Allowed | Dropped } mismatched NBDGM pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423005: { Allowed | Dropped } NBDGM pkt\_type\_name fragment with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-424001: Packet denied protocol\_string intf\_in:src\_ip/src\_port intf\_out:dst\_ip/dst\_port. [Ingress|Egress] interface is in a backup state.
- %ASA-4-424002: Connection to the backup interface is denied: protocol\_string intf:src\_ip/src\_port intf:dst\_ip/dst\_port
- %PIX|ASA-4-431001: RTP conformance: Dropping RTP packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, Drop reason: drop\_reason value
- %PIX|ASA-4-431002: RTCP conformance: Dropping RTCP packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, Drop reason: drop\_reason value
- ASA-4-450001: Deny traffic for protocol protocol\_id src interface\_name:IP\_address/port dst interface\_name:IP\_address/port, licensed host limit of num exceeded.
- %PIX|ASA-4-500004: Invalid transport field for protocol=protocol, from source\_address/source\_port to dest\_address/dest\_port
- %PIX|ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit
- %PIX|ASA-4-607002: action\_class: action SIP req\_resp req\_resp\_info from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info

- %PIXIASA-4-608002: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, SCCPPrefix length value too small
- %PIXIASA-4-608003: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, SCCPPrefix length value too large
- %PIXIASA-4-608004: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, message id value not allowed
- %PIXIASA-4-608005: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, message id value registration not complete
- %PIXIASA-4-612002: Auto Update failed:filename, version:number, reason:reason
- %PIXIASA-4-612003:Auto Update failed to contact:url, reason:reason
- %PIXIASA-4-620002: Unsupported CTIQBE version: hex: from interface\_name:IP\_address/port to interface\_name:IP\_address/port
- %PIXIASA-4-713154: DNS lookup for peer\_description Server [server\_name] failed!
- %PIXIASA-4-713157: Timed out on initial contact to server [server\_name or IP\_address] Tunnel could not be established.
- %ASA-4-713239: IP\_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
- %ASA-4-713240: Received DH key with bad length: received length=rlength expected length=length
- %ASA-4-713241: IE Browser Proxy Method setting\_number is Invalid
- %ASA-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.
- %ASA-4-713243: META-DATA Unable to find the requested certificate
- %ASA-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
- %ASA-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
- %ASA-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
- %ASA-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-4-713249: META-DATA Received unsupported authentication results: result
- %ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute
- %ASA-4-713251: META-DATA Received authentication failure message
- %PIXIASA-4-713903:descriptive\_event\_string.
- %ASA-4-716007: Group group User user WebVPN Unable to create session.
- %ASA-4-716022: Unable to connect to proxy server reason.
- %ASA-4-716023: Group name User user Session could not be established: session limit of maximum\_sessions reached.
- %ASA-4-716044: Group group-name User user-name IP IP\_address AAA parameter param-name value param-value out of range.

- %ASA-4-716045: Group group-name User user-name IP IP\_address AAA parameter param-name value invalid.
- %ASA-4-716046: Group group-name-name User user-name IP IP\_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.
- %ASA-4-716047: Group group-name User user-name IP IP\_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.
- %ASA-4-716048: Group group-name User user-name IP IP\_address No memory to parse ACL.
- %ASA-4-716052: Group group-name User user-name IP IP\_address Pending session terminated.
- %PIX|ASA-4-717026 Name lookup failed for hostname hostname during PKI operation.
- %PIX|ASA-4-717031 Failed to find a suitable trustpoint for the issuer: issuer Reason: reason\_string
- %PIX|ASA-4-717035 OCSP status is being checked for certificate. certificate\_identifier.
- %PIX|ASA-4-717037 Tunnel group search using certificate maps failed for peer certificate: certificate\_identifier.
- %ASA-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %ASA-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %ASA-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %ASA-4-720009: (VPN-unit) Failed to create version control block.
- %ASA-4-720011: (VPN-unit) Failed to allocate memory
- %ASA-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint\_name
- %ASA-4-720022: (VPN-unit) Cannot find trust point trustpoint
- %ASA-4-720033: (VPN-unit) Failed to queue add to message queue.
- %ASA-4-720038: (VPN-unit) Corrupted message from active unit.
- %ASA-4-720043: (VPN-unit) Failed to send type message id to standby unit
- %ASA-4-720044: (VPN-unit) Failed to receive message from active unit
- %ASA-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP\_address on the standby unit.
- %ASA-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
- %ASA-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
- %ASA-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP\_address, port=port
- %ASA-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP\_address, port=port.
- %ASA-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
- %ASA-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP\_address, port=port during bulk sync.
- %ASA-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
- %ASA-4-720066: (VPN-unit) Failed to activate IKE database.
- %ASA-4-720067: (VPN-unit) Failed to deactivate IKE database.
- %ASA-4-720068: (VPN-unit) Failed to parse peer message.

- %ASA-4-720069: (VPN-unit) Failed to activate cTCP database.
- %ASA-4-720070: (VPN-unit) Failed to deactivate cTCP database.
- %ASA-4-720073: (VPN-unit) Fail to insert certificate in trust point trustpoint on the standby unit.
- %ASA-4-722001: IP IP\_address Error parsing SVC connect request.
- %ASA-4-722002: IP IP\_address Error consolidating SVC connect request.
- %ASA-4-722003: IP IP\_address Error authenticating SVC connect request.
- %ASA-4-722004: Group group User user-name IP IP\_address Error responding to SVC connect request.
- %ASA-4-722015: Group group User user-name IP IP\_address Unknown SVC frame type: type-num
- %ASA-4-722016: Group group User user-name IP IP\_address Bad SVC frame length: length expected: expected-length
- %ASA-4-722017: Group group User user-name IP IP\_address Bad SVC framing: 525446, reserved: 0
- %ASA-4-722018: Group group User user-name IP IP\_address Bad SVC protocol version: version, expected: expected-version
- %ASA-4-722019: Group group User user-name IP IP\_address Not enough data for an SVC header: length
- %ASA-4-724001: Group group-name User user-name IP IP\_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.
- %ASA-4-724002: Group group-name User user-name IP IP\_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.

## Notification Messages, Severity 5

The following messages appear at severity 5, notifications:

- %PIXIASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %PIXIASA-5-109029: Parsing downloaded ACL: string
- %PIXIASA-5-111002: Begin configuration: IP\_address reading from device
- %PIXIASA-5-111003: IP\_address Erase configuration
- %PIXIASA-5-111004: IP\_address end configuration: {FAILED|OK}
- %PIXIASA-5-111005: IP\_address end configuration: OK
- %PIXIASA-5-111007: Begin configuration: IP\_address reading from device.
- %PIXIASA-5-111008: User user executed the command string
- %PIXIASA-5-199001: Reload command executed from telnet (remote IP\_address).
- %PIXIASA-5-199006: Orderly reload started at when by whom. Reload reason: reason
- %PIXIASA-5-199007: Reload scheduled for when by whom at when-command-issued. Reload reason: reason
- %PIXIASA-5-199008: Scheduled reload for when-reload-is-supposed-to-happen cancelled by whom at when.

- %PIX|ASA-5-303004: FTP cmd\_string command unsupported - failed strict inspection, terminating connection from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_interface
- %PIX|ASA-5-304001: user source\_address Accessed {JAVA URL|URL} dest\_address: url.
- %PIX|ASA-5-304002: Access denied URL chars SRC IP\_address DEST IP\_address: chars
- %PIX|ASA-5-321001: Resource var1 limit of var2 reached.
- %PIX|ASA-5-321002: Resource var1 rate limit of var2 reached.
- ASA|PIX-5-331002: Dynamic DNS type RR for ip\_address -> 'fqdn\_name' successfully updated in DNS server dns\_server\_ip
- %ASA|PIX-5-332003: Web Cache IP\_address/service\_ID acquired
- %PIX|ASA-5-333002: Timeout waiting for EAP response - context:EAP-context
- %PIX|ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context
- %PIX|ASA-5-334002: EAPoUDP association successfully established - host-address
- %PIX|ASA-5-334003: EAPoUDP association failed to establish - host-address
- %PIX|ASA-5-334005: Host put into NAC Hold state - host-address
- %PIX|ASA-5-334006: EAPoUDP failed to get a response from host - host-address
- %PIX|ASA-5-335002: Host is on the NAC Exception List - host-address, OS:oper-sys
- %PIX|ASA-5-335003: NAC Default ACL applied, ACL:ACL-name - host-address
- %PIX|ASA-5-335008: NAC IPsec terminate from dynamic ACL:ACL-name - host-address
- %PIX|ASA-5-415004: HTTP - matched matched\_string in policy-map map\_name, content-type verification failed connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415005: HTTP - matched matched\_string in policy-map map\_name, URI length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415006: HTTP - matched matched\_string in policy-map map\_name, URI matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415007: HTTP - matched matched\_string in policy-map map\_name, Body matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415008: HTTP - matched matched\_string in policy-map map\_name, header matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415009: HTTP - matched matched\_string in policy-map map\_name, method matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415010: matched matched\_string in policy-map map\_name, transfer encoding matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415011: HTTP - policy-map map\_name:Protocol violation connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415012: HTTP - matched matched\_string in policy-map map\_name, Unknown mime-type connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415013: HTTP - policy-map map-name:Malformed chunked encoding connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num

- %PIXIASA-5-415014: HTTP - matched matched\_string in policy-map map\_name, Mime-type in response wasn't found in the accept-types of the request connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415015: HTTP - matched matched\_string in policy-map map\_name, transfer-encoding unknown connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415018: HTTP - matched matched\_string in policy-map map\_name, Header length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415019: HTTP - matched matched\_string in policy-map map\_name, status line matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415020: HTTP - matched matched\_string in policy-map map\_name, a non-ASCII character was matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-500001: ActiveX content modified src IP\_address dest IP\_address on interface interface\_name.
- %PIXIASA-5-500002: Java content modified src IP\_address dest IP\_address on interface interface\_name.
- %PIXIASA-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source\_address/source\_port to dest\_address/dest\_port, flags: tcp\_flags, on interface interface\_name
- %PIXIASA-5-501101: User transitioning priv level
- %PIXIASA-5-502101: New user added to local dbase: Uname: user Priv: privilege\_level Encpass: string
- %PIXIASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege\_level Encpass: string
- %PIXIASA-5-502103: User priv level changed: Uname: user From: privilege\_level To: privilege\_level
- %PIXIASA-5-502111: New group policy added: name: policy\_name Type: policy\_type
- %PIXIASA-5-502112: Group policy deleted: name: policy\_name Type: policy\_type
- %PIXIASA-5-503001: Process number, Nbr IP\_address on interface\_name from string to string, reason
- %PIXIASA-5-504001: Security context context\_name was added to the system
- %PIXIASA-5-504002: Security context context\_name was removed from the system
- %ASA-5-505001: Module in slot slotnum is shutting down. Please wait...
- %ASA-5-505002: Module in slot slotnum is reloading. Please wait...
- %ASA-5-505003: Module in slot slotnum is resetting. Please wait...
- %ASA-5-505004: Module in slot slotnum shutdown is complete.
- %ASA-5-505005: Module in slot slotnum is initializing control communication. Please wait...
- %ASA-5-505006: Module in slot slotnum is Up.
- %ASA-5-505007: Module in slot slotnum is recovering. Please wait...
- %ASA-5-505008: Module in slot slotnum software is being updated to vnewver (currently vver)
- %ASA-5-505009: Module in slot slotnum software was updated to vnewver (previously vver)
- %ASA-5-505010: Module in slot slot data channel communication is UP.



- %ASA-5-505011: Module in slot slot, application detected application, version version.
- %ASA-5-505012: Module in slot slot, application stopped application, version version
- %ASA-5-505013: Module in slot slot application changed from: application version version to: newapplication version newversion.
- %ASA-5-506001: event\_source\_string event\_string
- %PIX|ASA-5-507001: Terminating TCP-Proxy connection from interface\_inside:source\_address/source\_port to interface\_outside:dest\_address/dest\_port - reassembly limit of limit bytes exceeded
- %PIX|ASA-5-508001: DCERPC message\_type non-standard version\_type version version\_number from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port, terminating connection.
- %PIX|ASA-5-508002: DCERPC response has low endpoint port port\_number from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port, terminating connection.
- %ASA-5-509001: Connection attempt from src\_intf:src\_ip/src\_port to dst\_intf:dst\_ip/dst\_port was prevented by “no forward” command.
- %PIX|ASA-5-611103: User logged out: Uname: user
- %PIX|ASA-5-611104: Serial console idle timeout exceeded
- %PIX|ASA-5-612001: Auto Update succeeded:filename, version:number
- %PIX|ASA-5-713006: Failed to obtain state for message Id message\_number, Peer Address: IP\_address
- %PIX|ASA-5-713010: IKE area: failed to find centry for message Id message\_number
- %PIX|ASA-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface\_number, IKE Peer IP\_address local Proxy Address IP\_address, remote Proxy Address IP\_address, Crypto map (crypto map tag)
- %PIX|ASA-5-713049: Security negotiation complete for tunnel\_type type (group\_name) Initiator/Responder, Inbound SPI = SPI, Outbound SPI = SPI
- %PIX|ASA-5-713050: Connection terminated for peer IP\_address. Reason: termination reason Remote Proxy IP\_address, Local Proxy IP\_address
- %PIX|ASA-5-713068: Received non-routine Notify message: notify\_type (notify\_value)
- %PIX|ASA-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger\_value to smaller\_value seconds
- %PIX|ASA-5-713074: Responder forcing change of IPSec rekeying duration from larger\_value to smaller\_value Kbs
- %PIX|ASA-5-713075: Overriding Initiator's IPSec rekeying duration from larger\_value to smaller\_value seconds
- %PIX|ASA-5-713076: Overriding Initiator's IPSec rekeying duration from larger\_value to smaller\_value Kbs
- %PIX|ASA-5-713092: Failure during phase 1 rekeying attempt due to collision
- %PIX|ASA-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec
- %PIX|ASA-5-713120: PHASE 2 COMPLETED (msgid=msg\_id)
- %PIX|ASA-5-713130: Received unsupported transaction mode attribute: attribute id
- %PIX|ASA-5-713131: Received unknown transaction mode attribute: attribute\_id
- %PIX|ASA-5-713135: message received, redirecting tunnel to IP\_address.

- %PIXIASA-5-713136: IKE session establishment timed out [IKE\_state\_name], aborting!
- %PIXIASA-5-713137: Reaper overriding refCnt [ref\_count] and tunnelCnt [tunnel\_count] -- deleting SA!
- %PIXIASA-5-713139: group\_name not found, using BASE GROUP default preshared key
- %PIXIASA-5-713144: Ignoring received malformed firewall record; reason - error\_reason TLV type attribute\_value correction
- %PIXIASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP\_address, mask: netmask
- %PIXIASA-5-713155: DNS lookup for Primary VPN Server [server\_name] successfully resolved after a previous failure. Resetting any Backup Server init.
- %PIXIASA-5-713156: Initializing Backup Server [server\_name or IP\_address]
- %PIXIASA-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP
- %PIXIASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %PIXIASA-5-713179: IKE AM Initiator received a packet from its peer without a payload\_type payload
- %PIXIASA-5-713196: Remote L2L Peer IP\_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!
- %PIXIASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel\_type connection. Enforcing the second default.
- %PIXIASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter\_value)!
- %PIXIASA-5-713216: Rule: action Client type : version Client: type version is/is not allowed
- %PIXIASA-5-713229: Auto Update - Notification to client client\_ip of update string: message\_string.
- %PIXIASA-5-713237: ACL update (access\_list) received during re-key re-authentication will not be applied to the tunnel.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute
- %ASA-vpn-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.
- %ASA-vpn-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.
- %PIXIASA-5-713904: descriptive\_event\_string.
- %ASA-5-716053: New SSO Server added: name: name Type: type
- %ASA-5-716054: SSO Server deleted: name: name Type: type
- %PIXIASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer
- %PIXIASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %PIXIASA-5-718002: Create peer IP\_address failure, already at maximum of number\_of\_peers
- %PIXIASA-5-718005: Fail to send to IP\_address, port port

- %PIX|ASA-5-718006: Invalid load balancing state transition [cur=state\_number][event=event\_number]
- %PIX|ASA-5-718007: Socket open failure failure\_code
- %PIX|ASA-5-718008: Socket bind failure failure\_code
- %PIX|ASA-5-718009: Send HELLO response failure to IP\_address
- %PIX|ASA-5-718010: Sent HELLO response to IP\_address
- %PIX|ASA-5-718011: Send HELLO request failure to IP\_address
- %PIX|ASA-5-718012: Sent HELLO request to IP\_address
- %PIX|ASA-5-718014: Master peer IP\_address is not answering HELLO
- %PIX|ASA-5-718015: Received HELLO request from IP\_address
- %PIX|ASA-5-718016: Received HELLO response from IP\_address
- %PIX|ASA-5-718024: Send CFG UPDATE failure to IP\_address
- %PIX|ASA-5-718028: Send OOS indicator failure to IP\_address
- %PIX|ASA-5-718031: Received OOS obituary for IP\_address
- %PIX|ASA-5-718032: Received OOS indicator from IP\_address
- %PIX|ASA-5-718033: Send TOPOLOGY indicator failure to IP\_address
- %PIX|ASA-5-718042: Unable to ARP for IP\_address
- %PIX|ASA-5-718043: Updating/removing duplicate peer entry IP\_address
- %PIX|ASA-5-718044: Deleted peer IP\_address
- %PIX|ASA-5-718045: Created peer IP\_address
- %PIX|ASA-5-718048: Create of secure tunnel failure for peer IP\_address
- %PIX|ASA-5-718050: Delete of secure tunnel failure for peer IP\_address
- %PIX|ASA-5-718052: Received GRAT-ARP from duplicate master MAC\_address
- %PIX|ASA-5-718053: Detected duplicate master, mastership stolen MAC\_address
- %PIX|ASA-5-718054: Detected duplicate master MAC\_address and going to SLAVE
- %PIX|ASA-5-718055: Detected duplicate master MAC\_address and staying MASTER
- %PIX|ASA-5-718057: Queue send failure from ISR, msg type failure\_code
- %PIX|ASA-5-718060: Inbound socket select fail: context=context\_ID.
- %PIX|ASA-5-718061: Inbound socket read fail: context=context\_ID.
- %PIX|ASA-5-718062: Inbound thread is awake (context=context\_ID).
- %PIX|ASA-5-718063: Interface interface\_name is down.
- %PIX|ASA-5-718064: Admin. interface interface\_name is down.
- %PIX|ASA-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB\_state, master=IP\_address, session=Enable/Disable).
- %PIX|ASA-5-718066: Cannot add secondary address to interface interface\_name, ip IP\_address.
- %PIX|ASA-5-718067: Cannot delete secondary address to interface interface\_name, ip IP\_address.
- %PIX|ASA-5-718068: Start VPN Load Balancing in context context\_ID.
- %PIX|ASA-5-718069: Stop VPN Load Balancing in context context\_ID.

- %PIXIASA-5-718070: Reset VPN Load Balancing in context context\_ID.
- %PIXIASA-5-718071: Terminate VPN Load Balancing in context context\_ID.
- %PIXIASA-5-718072: Becoming master of Load Balancing in context context\_ID.
- %PIXIASA-5-718073: Becoming slave of Load Balancing in context context\_ID.
- %PIXIASA-5-718074: Fail to create access list for peer context\_ID.
- %PIXIASA-5-718075: Peer IP\_address access list not set.
- %PIXIASA-5-718076: Fail to create tunnel group for peer IP\_address.
- %PIXIASA-5-718077: Fail to delete tunnel group for peer IP\_address.
- %PIXIASA-5-718078: Fail to create crypto map for peer IP\_address.
- %PIXIASA-5-718079: Fail to delete crypto map for peer IP\_address.
- %PIXIASA-5-718080: Fail to create crypto policy for peer IP\_address.
- %PIXIASA-5-718081: Fail to delete crypto policy for peer IP\_address.
- %PIXIASA-5-718084: Public/cluster IP not on the same subnet: public IP\_address, mask netmask, cluster IP\_address
- %PIXIASA-5-718085: Interface interface\_name has no IP address defined.
- %PIXIASA-5-718086: Fail to install LB NP rules: type rule\_type, dst interface\_name, port port.
- %PIXIASA-5-718087: Fail to delete LB NP rules: type rule\_type, rule rule\_ID.
- %ASA-5-719014: Email Proxy is changing listen port from old\_port to new\_port for mail protocol protocol.
- %ASA-5-720016: (VPN-unit) Failed to initialize default timer #index.
- %ASA-5-720017: (VPN-unit) Failed to update LB runtime data
- %ASA-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.
- %ASA-5-720019: (VPN-unit) Failed to update cTCP statistics.
- %ASA-5-720020: (VPN-unit) Failed to send type timer message.
- %ASA-5-720021: (VPN-unit) HA non-block send failed for peer msg message\_number. HA error code.
- %ASA-5-720035: (VPN-unit) Fail to look up CTCP flow handle
- %ASA-5-720036: (VPN-unit) Failed to process state update message from the active peer.
- %ASA-5-720071: (VPN-unit) Failed to update cTCP dynamic data.
- %ASA-vpnfo-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.
- %ASA-5-722037: Group group User user-name IP IP\_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP\_address SVC terminating session: reason.
- %ASA-5-722005: Group group User user-name IP IP\_address Unable to update session information for SVC connection.
- %ASA-5-722006: Group group User user-name IP IP\_address Invalid address IP\_address assigned to SVC connection.

- %ASA-5-722010: Group group User user-name IP IP\_address SVC Message: type-num/NOTICE: message
- %ASA-5-722011: Group group User user-name IP IP\_address SVC Message: type-num/NOTICE: message
- %ASA-5-722012: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-5-722028: Group group User user-name IP IP\_address Stale SVC connection closed.
- %ASA-5-722032: Group group User user-name IP IP\_address New SVC connection replacing old connection.
- %ASA-5-722033: Group group User user-name IP IP\_address First SVC connection established for SVC session.
- %ASA-5-722034: Group group User user-name IP IP\_address New SVC connection, no existing connection.
- %ASA-5-722037: Group group User user-name IP IP\_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP\_address SVC terminating session: reason.

## Informational Messages, Severity 6

The following messages appear at severity 6, informational:

- %PIX|ASA-6-106012: Deny IP from IP\_address to IP\_address, IP options hex.
- %PIX|ASA-6-106015: Deny TCP (no connection) from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name.
- %PIX|ASA-6-106025: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol
- %PIX|ASA-6-106026: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol
- %PIX|ASA-6-108005: action\_class: Received ESMTP req\_resp from src\_ifc:siplport to dest\_ifc:diplport;further\_info
- %PIX|ASA-6-109001: Auth start for user user from inside\_address/inside\_port to outside\_address/outside\_port
- %PIX|ASA-6-109002: Auth from inside\_address/inside\_port to outside\_address/outside\_port failed (server IP\_address failed) on interface interface\_name.
- %PIX|ASA-6-109003: Auth from inside\_address to outside\_address/outside\_port failed (all servers failed) on interface interface\_name.
- %PIX|ASA-6-109005: Authentication succeeded for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %PIX|ASA-6-109006: Authentication failed for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %PIX|ASA-6-109007: Authorization permitted for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %PIX|ASA-6-109008: Authorization denied for user user from outside\_address/outside\_port to inside\_address/ inside\_port on interface interface\_name.

- %PIXIASA-6-109024: Authorization denied from source\_address/source\_port to dest\_address/dest\_port (not authenticated) on interface interface\_name using protocol
- %PIXIASA-6-109025: Authorization denied (acl=acl\_ID) for user 'user' from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name using protocol
- %PIXIASA-6-110001: No route to dest\_address from source\_address
- %PIXIASA-6-113003: AAA group policy for user user is being set to policy\_name.
- %PIXIASA-6-113004: AAA user aaa\_type Successful: server = server\_IP\_address, User = user
- %PIXIASA-6-113005: AAA user authentication Rejected: reason = string: server = server\_IP\_address, User = user
- %PIXIASA-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %PIXIASA-6-113007: User user unlocked by administrator
- %PIXIASA-6-113008: AAA transaction status ACCEPT: user = user
- %PIXIASA-6-113009: AAA retrieved default group policy policy for user user
- %PIXIASA-6-113010: AAA challenge received for user user from server server\_IP\_address
- %PIXIASA-6-113011: AAA retrieved user specific group policy policy for user user
- %PIXIASA-6-113012: AAA user authentication Successful: local database : user = user
- %PIXIASA-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %PIXIASA-6-113014: AAA authentication server not accessible: server = server\_IP\_address: user = user
- %PIXIASA-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user
- %PIXIASA-6-113016: AAA credentials rejected: reason = reason: server = server\_IP\_address: user = user
- %PIXIASA-6-113017: AAA credentials rejected: reason = reason: local database: user = user\
- %ASA-6-114004: 4GE SSM I/O Initialization start.
- %ASA-6-114005: 4GE SSM I/O Initialization end.
- %PIXIASA-6-199002: startup completed. Beginning operation.
- %PIXIASA-6-199003: Reducing link MTU dec.
- %PIXIASA-6-199005: Startup begin
- %ASA-6-201012: Per-client embryonic connection limit exceeded curr num/limit for [input/output] packet from IP\_address/ port to ip/port on interface interface\_name
- %ASA-3-201013: Per-client connection limit exceeded curr num/limit for [input/output] packet from ip/port to ip/port on interface interface\_name
- %PIXIASA-6-210022: LU missed number updates
- %PIXIASA-6-302003: Built H245 connection for foreign\_address outside\_address/outside\_port local\_address inside\_address/inside\_port
- %PIXIASA-6-302004: Pre-allocate H323 UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port

- %PIX|ASA-6-302009: Rebuilt TCP connection number for foreign\_address outside\_address/outside\_port global\_address global\_address/global\_port local\_address inside\_address/inside\_port
- %PIX|ASA-6-302010: connections in use, connections most used
- %PIX|ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP\_address/port to laddr IP\_address
- %PIX|ASA-6-302013: Built {inbound|outbound} TCP connection\_id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]
- %PIX|ASA-6-302014: Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason] [(user)]
- %PIX|ASA-6-302015: Built {inbound|outbound} UDP connection number for interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) to interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) [(user)]
- %PIX|ASA-6-302016: Teardown UDP connection number for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [(user)]
- %PIX|ASA-6-302017: Built {inbound|outbound} GRE connection id from interface:real\_address (translated\_address) to interface:real\_address/real\_cid (translated\_address/translated\_cid)[(user)]
- %PIX|ASA-6-302018: Teardown GRE connection id from interface:real\_address (translated\_address) to interface:real\_address/real\_cid (translated\_address/translated\_cid) duration hh:mm:ss bytes bytes [(user)]
- %PIX|ASA-6-302020: Built {in | out}bound ICMP connection for faddr {faddr | icmp\_seq\_num} gaddr {gaddr | cmp\_type} laddr laddr
- %PIX|ASA-6-302021: Teardown ICMP connection for faddr {faddr | icmp\_seq\_num} gaddr {gaddr | cmp\_type} laddr laddr
- PIX-6-303002: FTP connection from src\_ifc:src\_ip/src\_port to
- %PIX|ASA-5-303005: Strict FTP inspection matched match\_string in policy-map policy-name, action\_string from src\_ifc:sip/sport to dest\_ifc:dip/dport
- %PIX|ASA-6-304004: URL Server IP\_address request failed URL url
- %PIX|ASA-6-305007: addrpool\_free(): Orphan IP IP\_address on interface interface\_number
- %PIX|ASA-6-305009: Built {dynamic|static} translation from interface\_name [(acl-name)]:real\_address to interface\_name:mapped\_address
- %PIX|ASA-6-305010: Teardown {dynamic|static} translation from interface\_name:real\_address to interface\_name:mapped\_address duration time
- %PIX|ASA-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface\_name:real\_address/real\_port to interface\_name:mapped\_address/mapped\_port
- %PIX|ASA-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from interface\_name [(acl-name)]:real\_address/{real\_port|real\_ICMP\_ID} to interface\_name:mapped\_address/{mapped\_port|mapped\_ICMP\_ID} duration time
- %PIX|ASA-6-308001: console enable password incorrect for number tries (from IP\_address)
- %PIX|ASA-6-311001: LU loading standby start
- %PIX|ASA-6-311002: LU loading standby end
- %PIX|ASA-6-311003: LU recv thread up

- %PIXIASA-6-311004: LU xmit thread up
- %PIXIASA-6-312001: RIP hdr failed from IP\_address: cmd=string, version=number domain=string on interface interface\_name
- %PIXIASA-6-314001: Pre-allocate RTSP UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port
- %PIXIASA-6-315011: SSH session from IP\_address on interface interface\_name for user user disconnected by SSH server, reason: reason
- %PIXIASA-6-321003: Resource var1 log level of var2 reached.
- %PIXIASA-6-321004: Resource var1 rate log level of var2 reached
- %PIXIASA-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface\_in:source\_address/source\_port to interface\_out:dest\_address/dest\_port
- %PIXIASA-6-333001: EAP association initiated - context:EAP-context
- %PIXIASA-6-333003: EAP association terminated - context:EAP-context
- %PIXIASA-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context
- %PIXIASA-6-334001: EAPoUDP association initiated - <host-address>
- %PIXIASA-6-334004: Authentication request for NAC Clientless host - host-address
- %PIXIASA-6-334007: EAPoUDP association terminated - host-address
- %PIXIASA-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context
- %PIXIASA-6-335001: NAC session initialized - host-address
- %PIXIASA-6-335004: NAC is disabled for host - host-address
- %PIXIASA-6-335006: NAC Applying ACL:ACL-name - host-address
- %PIXIASA-6-335009: NAC 'Revalidate' request by administrative action - host-address
- %PIXIASA-6-335010: NAC 'Revalidate All' request by administrative action - num sessions
- %PIXIASA-6-335011: NAC 'Revalidate Group' request by administrative action for group-name group - num sessions
- %PIXIASA-6-335012: NAC 'Initialize' request by administrative action - host-address
- %PIXIASA-6-335013: NAC 'Initialize All' request by administrative action - num sessions
- %PIXIASA-6-335014: NAC 'Initialize Group' request by administrative action for group-name group - num sessions
- %PIXIASA-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface\_name AC:ac\_name.
- %ASA-6-410004: action\_class: action DNS query\_response from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %PIXIASA-6-415001: HTTP - matched matched\_string in policy-map map\_name, header field count exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-6-415002: HTTP - matched matched\_string in policy-map map\_name, header field length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-6-415003: HTTP - matched matched\_string in policy-map map\_name, body length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num



- %PIX|ASA-6-415017: HTTP - matched\_string in policy-map map\_name, arguments matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-6-421002: TCPIUDP flow from interface\_name:IP\_address/port to interface\_name:IP\_address/port bypassed application checking because the protocol is not supported.
- %ASA-6-421005: interface\_name:IP\_address is counted as a user of application
- %ASA-6-421006: There are number users of application accounted during the past 24 hours.
- %PIX|ASA-6-602101: PMTU-D packet number bytes greater than effective mtu number dest\_addr=dest\_address, src\_addr=source\_address, prot=protocol
- %PIX|ASA-6-602103: IPSEC: Received an ICMP Destination Unreachable from src\_addr with suggested PMTU of rcvd\_mtu; PMTU updated for SA with peer peer\_addr, SPI spi, tunnel name username, old PMTU old\_mtu, new PMTU new\_mtu.%PIX|ASA-7-703001: H.225 message received from interface\_name:IP\_address/port to interface\_name:IP\_address/port is using an unsupported version number
- %PIX|ASA-6-602104: IPSEC: Received an ICMP Destination Unreachable from src\_addr, PMTU is unchanged because suggested PMTU of rcvd\_mtu is equal to or greater than the current PMTU of curr\_mtu, for SA with peer peer\_addr, SPI spi, tunnel name username.
- %PIX|ASA-6-602201: ISAKMP Phase 1 SA created (local IP\_address/port (initiator/responder), remote IP\_address/port, authentication=auth\_type, encryption=encl\_alg, hash=hash\_alg, group=DH\_grp, lifetime=seconds)
- %PIX|ASA-6-602202: ISAKMP session connected (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-6-602203: ISAKMP session disconnected (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-6-602303: IPSEC: An direction tunnel\_type SA (SPI=spi ) between local\_IP and remote\_IP (username) has been created.
- %PIX|ASA-6-602304: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) has been deleted.
- %PIX|ASA-6-603101: PPTP received out of seq or duplicate pkt, tnl\_id=number, sess\_id=number, seq=number.
- %PIX|ASA-6-603102: PPP virtual interface interface\_name - user: user aaa authentication started.
- %PIX|ASA-6-603103: PPP virtual interface interface\_name - user: user aaa authentication status
- %PIX|ASA-6-603104: PPTP Tunnel created, tunnel\_id is number, remote\_peer\_ip is remote\_address, ppp\_virtual\_interface\_id is number, client\_dynamic\_ip is IP\_address, username is user, MPPE\_key\_strength is string
- %PIX|ASA-6-603105: PPTP Tunnel deleted, tunnel\_id = number, remote\_peer\_ip= remote\_address
- %PIX|ASA-6-603106: L2TP Tunnel created, tunnel\_id is number, remote\_peer\_ip is remote\_address, ppp\_virtual\_interface\_id is number, client\_dynamic\_ip is IP\_address, username is user
- %PIX|ASA-6-603107: L2TP Tunnel deleted, tunnel\_id = number, remote\_peer\_ip = remote\_address
- %PIX|ASA-6-603108: Built PPTP Tunnel at interface\_name, tunnel-id = number, remote-peer = IP\_address, virtual-interface = number, client-dynamic-ip = IP\_address, username = user, MPPE-key-strength = number

- %PIXIASA-6-603109: Teardown PPPOE Tunnel at interface\_name, tunnel-id = number, remote-peer = IP\_address
- %PIXIASA-6-604101: DHCP client interface interface\_name: Allocated ip = IP\_address, mask = netmask, gw = gateway\_address
- %PIXIASA-6-604102: DHCP client interface interface\_name: address released
- %PIXIASA-6-604103: DHCP daemon interface interface\_name: address granted MAC\_address (IP\_address)
- %PIXIASA-6-604104: DHCP daemon interface interface\_name: address released
- %PIXIASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username"
- %PIXIASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user "username"
- %PIXIASA-6-606001: ASDM session number number from IP\_address started
- %PIXIASA-6-606002: ASDM session number number from IP\_address ended
- %PIXIASA-6-606003: ASDM logging session number id from IP\_address started id session ID assigned
- %PIXIASA-6-606004: ASDM logging session number id from IP\_address ended
- %PIXIASA-6-607001: Pre-allocate SIP connection\_type secondary channel for interface\_name:IP\_address/port to interface\_name:IP\_address from string message
- %PIXIASA-6-607003: action\_class: Received SIP req\_resp req\_resp\_info from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %PIXIASA-6-608001: Pre-allocate Skinny connection\_type secondary channel for interface\_name:IP\_address to interface\_name:IP\_address/port from string message
- %PIXIASA-6-610101: Authorization failed: Cmd: command Cmdtype: command\_modifier
- %ASA-6-6108005: action\_class: Received ESMTP req\_resp from src\_ifc:sip/sport to dest\_ifc:dip/dport;further\_info
- %PIXIASA-6-611101: User authentication succeeded: Uname: user
- %PIXIASA-6-611102: User authentication failed: Uname: user
- %PIXIASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped\_address
- %PIXIASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling
- %PIXIASA-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped\_address Split Tunnel Networks: IP\_address/netmask IP\_address/netmask ...
- %PIXIASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP\_address/netmask IP\_address/netmask ...
- %PIXIASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP\_address Secondary DNS: IP\_address Primary WINS: IP\_address Secondary WINS: IP\_address
- %PIXIASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed
- %PIXIASA-6-611307: VPNClient: Head end : IP\_address
- %PIXIASA-6-611308: VPNClient: Split DNS Policy installed: List of domains: string string ...

- %PIX|ASA-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP\_address
- %PIX|ASA-6-611310: VPNClient: XAUTH Succeeded: Peer: IP\_address
- %PIX|ASA-6-611311: VPNClient: XAUTH Failed: Peer: IP\_address
- %PIX|ASA-6-611312: VPNClient: Backup Server List: reason
- %PIX|ASA-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP\_address has redirected the to server IP\_address
- %PIX|ASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP\_address
- %PIX|ASA-6-611316: VPNClient: Secure Unit Authentication Enabled
- %PIX|ASA-6-611317: VPNClient: Secure Unit Authentication Disabled
- %PIX|ASA-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: IP\_address Auth Server Port: port Idle Timeout: time
- %PIX|ASA-6-611319: VPNClient: User Authentication Disabled
- %PIX|ASA-6-611320: VPNClient: Device Pass Thru Enabled
- %PIX|ASA-6-611321: VPNClient: Device Pass Thru Disabled
- %PIX|ASA-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled
- %PIX|ASA-6-611323: VPNClient: Duplicate split nw entry
- %PIX|ASA-6-613001: Checksum Failure in database in area string Link State Id IP\_address Old Checksum number New Checksum number
- %PIX|ASA-6-613002: interface interface\_name has zero bandwidth
- %PIX|ASA-6-613003: IP\_address netmask changed from area string to area string
- %PIX|ASA-6-614001: Split DNS: request patched from server: IP\_address to server: IP\_address
- %PIX|ASA-6-614002: Split DNS: reply from server:IP\_address reverse patched back to original server:IP\_address
- %PIX|ASA-6-615001: vlan number not available for firewall interface
- %PIX|ASA-6-615002: vlan number available for firewall interface
- %PIX|ASA-6-616001:Pre-allocate MGCP data\_channel connection for inside\_interface:inside\_address to outside\_interface:outside\_address/port from message\_type message
- %PIX|ASA-6-617001: GTPv version msg\_type from source\_interface:source\_address/source\_port not accepted by source\_interface:dest\_address/dest\_port
- %PIX|ASA-6-617002: Removing v1 PDP Context with TID tid from GGSN IP\_address and SGSN IP\_address, Reason: reason or Removing v1 primary|secondary PDP Context with TID tid from GGSN IP\_address and SGSN IP\_address, Reason: reason
- %PIX|ASA-6-617003: GTP Tunnel created from source\_interface:source\_address/source\_port to source\_interface:dest\_address/dest\_port
- %PIX|ASA-6-617004: GTP connection created for response from source\_interface:source\_address/0 to source\_interface:dest\_address/dest\_port
- PIX|ASA-6-617100: Teardown num\_conns connection(s) for user user\_ip

- %PIXIASA-6-620001: Pre-allocate CTIQBE {RTP | RTCP} secondary channel for interface\_name:outside\_address[/outside\_port] to interface\_name:inside\_address[/inside\_port] from CTIQBE\_message\_name message
- %PIXIASA-6-621001: Interface interface\_name does not support multicast, not enabled
- %PIXIASA-6-621002: Interface interface\_name does not support multicast, not enabled
- %PIXIASA-6-621003: The event queue size has exceeded number
- %PIXIASA-6-621006: Mrib disconnected, (IP\_address,IP\_address) event cancelled
- %PIXIASA-6-621007: Bad register from interface\_name:IP\_address to IP\_address for (IP\_address, IP\_address)
- %PIX-6-621008 AutoRP: discard string on interface interface-name from address due to incorrect version.
- %PIX-6-621009 AutoRP: discard string on interface interface-name from address due to incorrect type number
- %PIX-6-621010 AutoRP: discard string on interface interface-name from address due to zero RP count
- %PIXIASA-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
- %PIXIASA-6-622101: Starting regex table compilation for match\_command; table entries = regex\_num entries
- %PIXIASA-6-622102: Completed regex table compilation for match\_command; table size = num bytes
- %PIXIASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP\_address, mask: netmask
- %PIXIASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP\_address, mask: netmask
- %PIXIASA-6-713172: Automatic NAT Detection Status: Remote end is/is not behind a NAT device This end is/is not behind a NAT device
- %PIXIASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host\_name Address IP\_address, Protocol protocol, Port port
- %PIXIASA-6-713184: Client Type: Client\_type Client Application Version: Application\_version\_string
- %PIXIASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: IP\_address, mask: netmask
- %PIXIASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP\_address, mask: netmask
- %PIXIASA-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
- %PIXIASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %PIXIASA-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.
- %PIXIASA-6-713228: Assigned private IP address assigned\_private\_IP%PIXIASA-7-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %ASA-6-716001: Group group User user WebVPN session started.

- %ASA-6-716002: Group group User user WebVPN session terminated: reason.
- %ASA-6-716003: Group group User user WebVPN access GRANTED:: url
- %ASA-6-716004: Group group User user WebVPN access DENIED to specified location: url
- %ASA-6-716005: Group group User user WebVPN ACL Parse Error: reason
- %ASA-6-716006: Group name User user WebVPN session terminated. Idle timeout.
- %ASA-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.
- %PIX|ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint\_name.
- %ASA-6-716038: Authentication: successful, group = name user = user, Session Type: WebVPN
- %ASA-6-716039: Authentication: rejected, group = name user = user, Session Type: WebVPN
- %ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.
- %ASA-6-716041: access-list acl\_ID action url url hit\_cnt count
- %ASA-6-716042: access-list acl\_ID action tcp source\_interface/source\_address (source\_port) -> dest\_interface/dest\_address(dest\_port) hit-cnt count
- %ASA-6-716043 Group group-name, User user-name, IP IP\_address: WebVPN Port Forwarding Java applet started. Created new hosts file mappings.
- %ASA-6-716049: Group group-name User user-name IP IP\_address Empty SVC ACL.
- %ASA-6-716050: Error adding to ACL: ace\_command\_line
- %ASA-6-716051: Group group-name User user-name IP IP\_address Error adding dynamic ACL for user.
- %ASA-6-716055: Group group-name User user-name IP IP\_address Authentication to SSO server name: name type type succeeded
- %ASA-webvpn-6-716090: Group group-policy, User user-name, IP IP\_address: Secure Desktop Results: PLATFORM/FEATURE = platform & feature, PC\_LOCATION = location\_name, PC\_OS\_DETECTED = OS\_name, PC\_AV\_DETECTED = antivirus\_software, PC\_FW\_DETECTED = firewall\_name, PC\_AS\_DETECTED = antispayware\_name
- %ASA-webvpn-6-716091: Group group-policy, User user-name, IP IP\_address: Secure Desktop Results: WEB\_ACCESS = effective\_permission == secure\_desktop\_permission & group-policy permission, FILE\_ACCESS = = effective\_permission == secure\_desktop\_permission & group-policy permission, PORT\_FORWARDING == effective\_permission == secure\_desktop\_permission & group-policy permission, SSL\_VPN\_CLIENT = effective\_permission == secure\_desktop\_permission & group-policy permission, GROUP\_POLICY = results
- %PIX|ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint\_name.
- %PIX|ASA-6-717004: PKCS #12 export failed for trustpoint trustpoint\_name.
- %PIX|ASA-6-717005: PKCS #12 export succeeded for trustpoint trustpoint\_name.
- %PIX|ASA-6-717006: PKCS #12 import failed for trustpoint trustpoint\_name.
- %PIX|ASA-6-717007: PKCS #12 import succeeded for trustpoint trustpoint\_name.
- %PIX|ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
- %PIX|ASA-6-717022 Certificate was successfully validated. certificate\_identifiers
- %PIX|ASA-6-717028 Certificate chain was successfully validated additional info.

- %PIXIASA-6-717033 OCSP response status - Successful.
- %PIXIASA-6-718003: Got unknown peer message message\_number from IP\_address, local version version\_number, remote version version\_number
- %PIXIASA-6-718004: Got unknown internal message message\_number
- %PIXIASA-6-718013: Peer IP\_address is not answering HELLO
- %PIXIASA-6-718027: Received unexpected KEEPALIVE request from IP\_address
- %PIXIASA-6-718030: Received planned OOS from IP\_address
- %PIXIASA-6-718037: Master processed number\_of\_timeouts timeouts
- %PIXIASA-6-718038: Slave processed number\_of\_timeouts timeouts
- %PIXIASA-6-718039: Process dead peer IP\_address
- %PIXIASA-6-718040: Timed-out exchange ID exchange\_ID not found
- %PIXIASA-6-718051: Deleted secure tunnel to peer IP\_address
- %ASA-6-719001: Email Proxy session could not be established: session limit of maximum\_sessions has been reached.
- %ASA-6-719003: Email Proxy session pointer resources have been freed for source\_address.
- %ASA-6-719004: Email Proxy session pointer has been successfully established for source\_address.
- %ASA-6-719010: protocol Email Proxy feature is disabled on interface interface\_name.
- %ASA-6-719011: Protocol Email Proxy feature is enabled on interface interface\_name.
- %ASA-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %ASA-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %ASA-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
- %ASA-6-719018: WebVPN user: vpnuser ACL ID acl\_ID not found
- %ASA-6-719019: WebVPN user: vpnuser authorization failed.
- %ASA-6-719020: WebVPN user vpnuser authorization completed successfully.
- %ASA-6-719021: WebVPN user: vpnuser is not checked against ACL.
- %ASA-6-719022: WebVPN user vpnuser has been authenticated.
- %ASA-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.
- %ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source\_address
- %ASA-6-719025: Email Proxy DNS name resolution failed for hostname.
- %ASA-6-719026: Email Proxy DNS name hostname resolved to IP\_address.
- %ASA-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %ASA-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
- %ASA-6-720004: (VPN-unit) VPN failover main thread started.
- %ASA-6-720005: (VPN-unit) VPN failover timer thread started.
- %ASA-6-720006: (VPN-unit) VPN failover sync thread started.
- %ASA-6-720010: (VPN-unit) VPN failover client is being disabled

- %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
- %ASA-6-722013: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-6-720014: (VPN-unit) Phase 2 connection entry (msg\_id=message\_number, my cookie=mine, his cookie=his) contains no SA list.
- %ASA-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg\_id=message\_number,my cookie=mine, his cookie=his).
- %ASA-6-720023: (VPN-unit) HA status callback: Peer is not present.
- %ASA-6-720024: (VPN-unit) HA status callback: Control channel is status.
- %ASA-6-720025: (VPN-unit) HA status callback: Data channel is status.
- %ASA-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
- %ASA-6-720027: (VPN-unit) HA status callback: My state state.
- %ASA-6-720028: (VPN-unit) HA status callback: Peer state state.
- %ASA-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
- %ASA-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
- %ASA-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence\_#, grp=group, event=event, op=operand, my=my\_state, peer=peer\_state.
- %ASA-6-720037: (VPN-unit) HA progression callback: id=id,seq=sequence\_number,grp=group,event=event,op=operand, my=my\_state,peer=peer\_state.
- %ASA-6-720039: (VPN-unit) VPN failover client is transitioning to active state
- %ASA-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
- %ASA-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
- %ASA-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
- %ASA-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
- %ASA-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
- %ASA-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
- %ASA-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
- %ASA-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
- %ASA-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
- %ASA-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
- %ASA-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
- %ASA-6-722013: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-6-722014: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-6-722022: TunnelGroup tunnel\_group GroupPolicy group\_policy User user-name IP IP\_address No address available for SVC connection
- %ASA-6-722023: Group group User user-name IP IP\_address SVC connection terminated {with/without} compression
- %ASA-6-722024: SVC Global Compression Enabled

- %ASA-6-722025: SVC Global Compression Disabled
- %ASA-6-722026: Group group User user-name IP IP\_address SVC compression history reset
- %ASA-6-722027: Group group User user-name IP IP\_address SVC decompression history reset
- %ASA-6-723001: Group group-name, User user-name, IP IP\_address: WebVPN Citrix ICA connection connection is up.
- %ASA-6-723002: Group group-name, User user-name, IP IP\_address: WebVPN Citrix ICA connection connection is down.
- %ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %ASA-6-725001 Starting SSL handshake with remote\_device interface\_name:IP\_address/port for SSL\_version session.
- %ASA-6-725002 Device completed SSL handshake with remote\_device interface\_name:IP\_address/port
- %ASA-6-725003 SSL client interface\_name:IP\_address/port requesting to resume previous session.
- %ASA-6-725004 Device requesting certificate from SSL client interface\_name:IP\_address/port for authentication.
- %ASA-6-725005 SSL server interface\_name:IP\_address/port requesting our device certificate for authentication.
- %ASA-6-725006 Device failed SSL handshake with remote\_device interface\_name:IP\_address/port
- %ASA-6-725007 SSL session with remote\_device interface\_name:IP\_address/port terminated.
- %PIXIASA-6-726001: Inspected im\_protocol im\_service Session between Client im\_client\_1 and im\_client\_2 Packet flow from src\_ifc:/sip/sport to dest\_ifc:/dip/dport Action: action Matched Class class\_map\_id class\_map\_name

## Debugging Messages, Severity 7

The following messages appear at severity 7, debugging:

- %PIXIASA-7-108006: Detected ESMTTP size violation from src\_ifc:sip/sport to dest\_ifc:dip/dport;declared size is: decl\_size, actual size is act\_size.
- %PIXIASA-7-109014: uauth\_lookup\_net fail for uauth\_in()
- %PIXIASA-7-109021: Uauth null proxy error
- %PIXIASA-7-111009:User user executed cmd:string
- %PIXIASA-7-199009: Reloaded at when by whom. Reload reason: reason
- %PIXIASA-7-304005: URL Server IP\_address request pending URL url
- %PIXIASA-7-304009: Ran out of buffer blocks specified by url-block command
- %PIXIASA-7-333004: EAP-SQ response invalid - context:EAP-context
- %PIXIASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
- %PIXIASA-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
- %PIXIASA-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
- %PIXIASA-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context



- %PIX|ASA-7-335007: NAC Default ACL not configured - host-address
- %ASA-7-421004: Failed to inject {TCPIUDP} packet from IP\_address/port to IP\_address/port
- %PIX|ASA-7-609001: Built local-host interface\_name:IP\_address
- %PIX|ASA-7-609002: Teardown local-host interface\_name:IP\_address duration time
- %PIX|ASA-7-701001: alloc\_user() out of Tcp\_user objects
- %PIX|ASA-7-701002: alloc\_user() out of Tcp\_proxy objects
- %PIX|ASA-7-702201: ISAKMP Phase 1 delete received (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702202: ISAKMP Phase 1 delete sent (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702203: ISAKMP DPD timed out (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702204: ISAKMP Phase 1 retransmission (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702205: ISAKMP Phase 2 retransmission (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702206: ISAKMP malformed payload received (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702207: ISAKMP duplicate packet detected (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702208: ISAKMP Phase 1 exchange started (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702209: ISAKMP Phase 2 exchange started (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702210: ISAKMP Phase 1 exchange completed(local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702211: ISAKMP Phase 2 exchange completed(local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-702212: ISAKMP Phase 1 initiating rekey (local IP\_address (initiator/responder), remote IP\_address)
- %PIX|ASA-7-703001: H.225 message received from interface\_name:IP\_address/port to interface\_name:IP\_address/port is using an unsupported version number
- %PIX|ASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface\_name:IP\_address to interface\_name:IP\_address/port
- %PIX|ASA-7-709001: FO replication failed: cmd=command returned=code
- %PIX|ASA-7-709002: FO unreplicable: cmd=command
- %PIX|ASA-7-710001: TCP access requested from source\_address/source\_port to interface\_name:dest\_address/service
- %PIX|ASA-7-710002: {TCPIUDP} access permitted from source\_address/source\_port to interface\_name:dest\_address/service
- %PIX|ASA-7-710004: TCP connection limit exceeded from source\_address/source\_port to interface\_name:dest\_address/service

- %PIXIASA-7-710005: {TCPIUDP} request discarded from source\_address/source\_port to interface\_name:dest\_address/service
- %PIXIASA-7-710006: protocol request discarded from source\_address to interface\_name:dest\_address
- %PIXIASA-7-711001: debug\_trace\_msg
- PIX/ASA-7-711002: Task ran for elapsed\_time msecs, process = process\_name, PC = PC  
Tracebeback = traceback
- %PIXIASA-7-713024: Received local Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713026: Transmitted local Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713027: Transmitted remote Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713030: Transmitted local Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713031: Transmitted remote Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIXIASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIXIASA-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIXIASA-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIXIASA-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIXIASA-7-713039: Send failure: Bytes (number), Peer: IP\_address
- %PIXIASA-7-713040: Could not find connection entry and can not encrypt: msgid message\_number
- %PIXIASA-7-713052: User (user) authenticated.
- %PIXIASA-7-713066: IKE Remote Peer configured for SA: SA\_name
- %PIXIASA-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %PIXIASA-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %PIXIASA-7-713103: Invalid (NULL) secret key detected while computing hash
- %PIXIASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation
- %PIXIASA-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: IP\_address, SA address: internal\_SA\_address, tunnel count: count

- %PIX|ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA\_internal\_address) for peer IP\_address, but cookies don't match
- %PIX|ASA-7-713117: Received Invalid SPI notify (SPI SPI\_Value)!
- %PIX|ASA-7-713121: Keep-alive type for this connection: keepalive\_type
- %PIX|ASA-7-713143: Processing firewall record. Vendor: vendor(id), Product: product(id), Caps: capability\_value, Version Number: version\_number, Version String: version\_text
- %PIX|ASA-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %PIX|ASA-7-713164: The Firewall Server has requested a list of active user sessions
- %PIX|ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: IP\_address, SA address: internal\_SA\_address, tunnelCnt: tunnel\_count
- %PIX|ASA-7-713170: IKE Received delete for rekeyed centry IKE peer: IP\_address, centry address: internal\_address, msgid: id
- %PIX|ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %PIX|ASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP\_address, Remote peer address: IP\_address
- %PIX|ASA-7-713190: Got bad refCnt (ref\_count\_value) assigning IP\_address (IP\_address)
- %PIX|ASA-7-713204: Adding static route for client address: IP\_address
- %PIX|ASA-7-713221: Static Crypto Map check, checking map = crypto\_map\_tag, seq = seq\_number...
- %PIX|ASA-7-713222: Static Crypto Map check, map = crypto\_map\_tag, seq = seq\_number, ACL does not match proxy IDs src:source\_address dst:dest\_address
- %PIX|ASA-7-713223: Static Crypto Map check, map = crypto\_map\_tag, seq = seq\_number, no ACL configured
- %PIX|ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!
- %PIX|ASA-7-713225: [IKEv1], Static Crypto Map check, map map\_name, seq = sequence\_number is a successful match
- %PIX|ASA-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.
- %PIX|ASA-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).
- %PIX|ASA-7-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %PIX|ASA-7-713236: IKE\_DECODE tx/rx Message (msgid=msgid) with payloads :payload1 (payload1\_len) + payload2 (payload2\_len)...total length : tlen
- %PIX|ASA-7-713900:Descriptive\_event\_string.
- %PIX|ASA-7-713901:Descriptive\_event\_string.
- %PIX|ASA-7-714001: description\_of\_event\_or\_packet
- %PIX|ASA-7-714002: IKE Initiator starting QM: msg id = message\_number
- %PIX|ASA-7-714003: IKE Responder starting QM: msg id = message\_number
- %PIX|ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = message\_number
- %PIX|ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = message\_number
- %PIX|ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message\_number

- %PIXIASA-7-714007: IKE Initiator sending Initial Contact
- %PIXIASA-7-714011: Description of received ID values
- %PIXIASA-7-715001: Descriptive statement
- %PIXIASA-7-715004: subroutine name() Q Send failure: RetCode (return\_code)
- %PIXIASA-7-715005: subroutine name() Bad message code: Code (message\_code)
- %PIXIASA-7-715006: IKE got SPI from key engine: SPI = SPI\_value
- %PIXIASA-7-715007: IKE got a KEY\_ADD msg for SA: SPI = SPI\_value
- %PIXIASA-7-715008: Could not delete SA SA\_address, refCnt = number, caller = calling\_subroutine\_address
- %PIXIASA-7-715009: IKE Deleting SA: Remote Proxy IP\_address, Local Proxy IP\_address
- %PIXIASA-7-715013: Tunnel negotiation in progress for destination IP\_address, discarding data
- %PIXIASA-7-715019: IKEGetUserAttributes: Attribute name = name
- %PIXIASA-7-715020: construct\_cfg\_set: Attribute name = name
- %PIXIASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %PIXIASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %PIXIASA-7-715027: IPsec SA Proposal # chosen\_proposal, Transform # chosen\_transform acceptable Matches global IPsec SA entry # crypto\_map\_index
- %PIXIASA-7-715028: IKE SA Proposal # 1, Transform # chosen\_transform acceptable Matches global IKE entry # crypto\_map\_index
- %PIXIASA-7-715033: Processing CONNECTED notify (MsgId message\_number)
- %PIXIASA-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.
- %PIXIASA-7-715035: Starting IOS keepalive monitor: seconds sec.
- %PIXIASA-7-715036: Sending keep-alive of type notify\_type (seq number number)
- %PIXIASA-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %PIXIASA-7-715038: action Spoofing\_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %PIXIASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %PIXIASA-7-715040: Deleting active auth handle during SA deletion: handle = internal\_authentication\_handle
- %PIXIASA-7-715041: Received keep-alive of type keepalive\_type, not the negotiated type
- %PIXIASA-7-715042: IKE received response of type failure\_type to a request from the IP\_address utility
- %PIXIASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %PIXIASA-7-715045: ERROR: malformed Keepalive payload
- %PIXIASA-7-715046: constructing payload\_description payload
- %PIXIASA-7-715047: processing payload\_description payload
- %PIXIASA-7-715048: Send VID\_type VID
- %PIXIASA-7-715049: Received VID\_type VID
- %PIXIASA-7-715050: Claims to be IOS but failed authentication

- %PIX|ASA-7-715051: Received unexpected TLV type TLV\_type while processing FWTYPE ModeCfg Reply
- %PIX|ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries
- %PIX|ASA-7-715053: MODE\_CFG: Received request for attribute\_info!
- %PIX|ASA-7-715054: MODE\_CFG: Received attribute\_name reply: value
- %PIX|ASA-7-715055: Send attribute\_name
- %PIX|ASA-7-715056: Client is configured for TCP\_transparency
- %PIX|ASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
- %PIX|ASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
- %PIX|ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %PIX|ASA-7-715060: Dropped received IKE fragment. Reason: reason
- %PIX|ASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
- %PIX|ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.
- %PIX|ASA-7-715063: Successfully assembled an encrypted pkt from rev'd fragments!
- %PIX|ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %PIX|ASA-7-715065: IKE state\_machine subtype FSM error history (struct data\_structure\_address) state, event: state/event pairs
- %PIX|ASA-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
- %PIX|ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %PIX|ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %PIX|ASA-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %PIX|ASA-7-715069: Invalid ESP SPI size of SPI\_size
- %PIX|ASA-7-715070: Invalid IPComp SPI size of SPI\_size
- %PIX|ASA-7-715071: AH proposal not supported
- %PIX|ASA-7-715072: Received proposal with unknown protocol ID protocol\_ID
- %PIX|ASA-7-715074: Could not retrieve authentication attributes for peer IP\_address
- %PIX|ASA-7-715075: Group = group\_name, Username = client, IP = IP\_address Received keep-alive of type message\_type (seq number number)
- %PIX|ASA-7-715076: Computing hash for ISAKMP
- %PIX|ASA-7-715077: Pitcher: msg string, spi spi
- %PIX-7-715078: META-DATA Received type LAM attribute.
- %PIX-7-715079: META-DATA INTERNAL\_ADDRESS: Received request for type.
- %ASA-vpn-7-715080: Starting P2 rekey timer: 28800 seconds.
- %ASA-7-716008: WebVPN ACL: action
- %ASA-7-716010: Group group User user Browse network.
- %ASA-7-716011: Group group User user Browse domain domain.

- %ASA-7-716012: Group group User user Browse directory directory.
- %ASA-7-716013: Group group User user Close file filename.
- %ASA-7-716014: Group group User user View file filename.
- %ASA-7-716015: Group group User user Remove file filename.
- %ASA-7-716016: Group group User user Rename file old\_filename to new\_filename.
- %ASA-7-716017: Group group User user Modify file filename.
- %ASA-7-716018: Group group User user Create file filename.
- %ASA-7-716019: Group group User user Create directory directory.
- %ASA-7-716020: Group group User user Remove directory directory.
- %ASA-7-716021: File access DENIED, filename.
- %ASA-7-716024: Group name User user Unable to browse the network.Error: description
- %ASA-7-716025: Group name User user Unable to browse domain domain. Error: description
- %ASA-7-716026: Group name User user Unable to browse directory directory. Error: description
- %ASA-7-716027: Group name User user Unable to view file filename. Error: description
- %ASA-7-716028: Group name User user Unable to remove file filename. Error: description
- %ASA-7-716029: Group name User user Unable to rename file filename. Error: description
- %ASA-7-716030: Group name User user Unable to modify file filename. Error: description
- %ASA-7-716031: Group name User user Unable to create file filename. Error: description
- %ASA-7-716032: Group name User user Unable to create folder folder. Error: description
- %ASA-7-716033: Group name User user Unable to remove folder folder. Error: description
- %ASA-7-716034: Group name User user Unable to write to file filename.
- %ASA-7-716035: Group name User user Unable to read file filename.
- %ASA-7-716036: Group name User user File Access: User user logged into the server server.
- %ASA-7-716037: Group name User user File Access: User user failed to login into the server server.
- %PIXIASA-7-717024 Checking CRL from trustpoint: trustpoint name for purpose
- %PIXIASA-7-717025 Validating certificate chain containing number of certs certificate(s).
- %PIXIASA-7-717029 Identified client certificate within certificate chain. serial number: serial\_number, subject name: subject\_name.
- %PIXIASA-7-717030 Found a suitable trustpoint trustpoint name to validate certificate.
- %PIXIASA-7-717034 No-check extension found in certificate. OCSP check bypassed.
- PIXIASA-7-717036 Looking for a tunnel group match based on certificate maps for peer certificate with certificate\_identifier.
- %PIXIASA-7-717038 Tunnel group match found. Tunnel Group: tunnel\_group\_name, Peer certificate: certificate\_identifier.
- %PIXIASA-7-718001: Internal interprocess communication queue send failure: code error\_code
- %PIXIASA-7-718017: Got timeout for unknown peer IP\_address msg type message\_type
- %PIXIASA-7-718018: Send KEEPALIVE request failure to IP\_address
- %PIXIASA-7-718019: Sent KEEPALIVE request to IP\_address

- %PIX|ASA-7-718020: Send KEEPALIVE response failure to IP\_address
- %PIX|ASA-7-718021: Sent KEEPALIVE response to IP\_address
- %PIX|ASA-7-718022: Received KEEPALIVE request from IP\_address
- %PIX|ASA-7-718023: Received KEEPALIVE response from IP\_address
- %PIX|ASA-7-718025: Sent CFG UPDATE to IP\_address
- %PIX|ASA-7-718026: Received CFG UPDATE from IP\_address
- %PIX|ASA-7-718029: Sent OOS indicator to IP\_address
- %PIX|ASA-7-718034: Sent TOPOLOGY indicator to IP\_address
- %PIX|ASA-7-718035: Received TOPOLOGY indicator from IP\_address
- %PIX|ASA-7-718036: Process timeout for req-type type\_value, exid exchange\_ID, peer IP\_address
- %PIX|ASA-7-718041: Timeout [msgType=type] processed with no callback
- %PIX|ASA-7-718046: Create group policy policy\_name
- %PIX|ASA-7-718047: Fail to create group policy policy\_name
- %PIX|ASA-7-718049: Created secure tunnel to peer IP\_address
- %PIX|ASA-7-718056: Deleted Master peer, IP IP\_address
- %PIX|ASA-7-718058: State machine return code: action\_routine, return\_code
- %PIX|ASA-7-718059: State machine function trace: state=state\_name, event=event\_name, func=action\_routine
- %PIX|ASA-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC\_address.
- %ASA-7-719005: FSM NAME has been created using protocol for session pointer from source\_address.
- %ASA-7-719006: Email Proxy session pointer has timed out for source\_address because of network congestion.
- %ASA-7-719007: Email Proxy session pointer cannot be found for source\_address.
- %ASA-7-719009: Email Proxy service is starting.
- %ASA-7-719015: Parsed emailproxy session pointer from source\_address username: mailuser = mail\_user, vpnuser = VPN\_user, mailserver = server
- %ASA-7-719016: Parsed emailproxy session pointer from source\_address password: mailpass = \*\*\*\*\*, vpnpass= \*\*\*\*\*
- %ASA-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event\_ID.
- %ASA-7-720034: (VPN-unit) Invalid type (type) for message handler.
- %ASA-7-720041: (VPN-unit) Sending type message id to standby unit
- %ASA-7-720042: (VPN-unit) Receiving type message id from active unit
- %ASA-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.
- %ASA-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.
- %ASA-7-720050: (VPN-unit) Failed to remove timer. ID = id.
- %ASA-7-722029: Group group User user-name IP IP\_address SVC Session Termination: Conns: connections, DPD Conns: DPD\_conns, Comp resets: compression\_resets, Dcmp resets: decompression\_resets

- %ASA-7-722030: Group group User user-name IP IP\_address SVC Session Termination: In: data\_bytes (+ctrl\_bytes) bytes, data\_pkts (+ctrl\_pkts) packets, drop\_pkts drops
- %ASA-7-722031: Group group User user-name IP IP\_address SVC Session Termination: Out: data\_bytes (+ctrl\_bytes) bytes, data\_pkts (+ctrl\_pkts) packets, drop\_pkts drops.
- %ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %ASA-7-723004: WebVPN Citrix encountered bad flow control flow.
- %ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.
- %ASA-7-723006: WebVPN Citrix SOCKS errors.
- %ASA-7-723007: WebVPN Citrix ICA connection connection list is broken.
- %ASA-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
- %ASA-7-723009: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received data on invalid connection connection.
- %ASA-7-723010: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received closing channel channel for invalid connection connection.
- %ASA-7-723011: Group group-name, User user-name, IP IP\_address: WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length.
- %ASA-7-723012: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received bad SOCKS socks message format.
- %ASA-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.
- %ASA-7-723014: Group group-name, User user-name, IP IP\_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
- %ASA-7-725008 SSL client interface\_name:IP\_address/port proposes the following number cipher(s).
- %ASA-7-725009 Device proposes the following number cipher(s) to SSL server interface\_name:IP\_address/port.
- %ASA-7-725010 Device supports the following number cipher(s).
- %ASA-7-725011 Cipher[order] : cipher\_name
- %ASA-7-725012 Device chooses cipher : cipher\_name for SSL session with client interface\_name:IP\_address/port
- %ASA-7-725013 SSL Server interface\_name:IP\_address/port chooses cipher : cipher\_name
- %ASA-7-725014 SSL lib error. Function: function Reason: reason





---

## Numerics

4GE SSM [2-42 to 2-52](#)

---

## A

### AAA

- authentication [2-36, 2-37, 2-38, 2-346](#)
- authorization [2-28](#)
- messages [2-23, 2-24, 2-25, 2-26, 2-27, 2-28, 2-29, 2-35, 2-36, 2-37, 2-38, 2-39, 2-133, 2-147, 2-188, 2-214](#)
- server [2-29, 2-38, 2-133, 2-188, 2-213, 2-345, 2-346](#)

### ABR

- without backbone area [2-93](#)

### access denied

- URL [2-81](#)

### access-list command [2-14, 2-19, 2-79, 2-337](#)

- deny-flow-max option [2-20](#)
- interval option [2-19](#)
- log option [2-19](#)
- omitting [2-27](#)
- to permit traffic on UDP port 53 [2-14, 2-19, 2-79, 2-337](#)

### access-list deny-flow-max command [2-20](#)

### access lists

- See ACLs

### access permitted [2-220](#)

### access requested [2-220](#)

### ACLs

- ACL\_ID [2-303](#)
- compilation out of memory [2-18](#)
- configuration error [2-27](#)
- crypto map [2-127, 2-233](#)
- deny [2-79](#)

deny-flows [2-20](#)

empty ACL downloaded [2-27](#)

failed check [2-28](#)

logging matches [2-19](#)

no ACL configured [2-265](#)

packet denied [2-18](#)

parsing error [2-27](#)

peer context ID [2-337](#)

peer IP address not set [2-337](#)

proxy ID mismatch [2-264](#)

SoftNP error [2-339, 2-340](#)

split tunneling policy [2-246](#)

unsupported format [2-39](#)

### WebVPN

- ACL ID not found [2-345](#)

- parse error [2-295, 2-296, 2-345](#)

- user authorization failure [2-345](#)

ActiveX object, filtering [2-176](#)

address translation slots [2-138](#)

- no more available [2-59, 2-137, 2-138](#)

address translation slots, no more available [2-59](#)

area border router

- See ABR

ARP packet mismatch [2-137](#)

ARP poisoning attack [2-137](#)

ARP spoofing attack [2-97](#)

asymmetric routing [2-17](#)

### attacks

- ARP poisoning [2-137](#)

- ARP spoofing [2-97](#)

- DNS HINFO request [2-124](#)

- DNS request for all records [2-124](#)

- DNS zone transfer [2-124](#)

DNS zone transfer from high port [2-124](#)  
 DoS [2-20, 2-26, 2-61, 2-137, 2-142](#)  
 fragmented ICMP traffic [2-124](#)  
 IP fragment [2-123](#)  
 IP fragments overlap [2-123](#)  
 IP impossible packet [2-123](#)  
 IP routing table [2-20](#)  
 land [2-16](#)  
 large ICMP traffic [2-124](#)  
 man in the middle [2-95](#)  
 ping of death [2-124](#)  
 proxied RPC request [2-124](#)  
 spoofing [2-16, 2-17, 2-97, 2-138](#)  
 statd buffer overflow [2-124](#)  
 suspicious e-mail address pattern [2-21](#)  
 SYN [2-55](#)  
 TCP FIN only flags [2-124](#)  
 TCP NULL flags [2-124](#)  
 TCP SYN+FIN flags [2-124](#)  
 UDP bomb [2-124](#)  
 UDP chargen DoS [2-124](#)  
 UDP snork [2-124](#)  
 Authen Session End [2-25](#)  
 authentication  
   failed [2-24](#)  
   request [2-188](#)  
   request succeeds [2-24](#)  
   response [2-188](#)  
   server not found [2-24](#)  
 Auth from IP address/port to IP address/port failed [2-23](#)  
 authorization  
   command [2-198](#)  
   user [2-199](#)  
   user denied [2-25](#)  
 Auth start for user [2-23](#)  
 Auto Update URL unreachable [2-206](#)

---

**B**

backup server list  
   downloaded [2-202](#)  
   error [2-203](#)  
 bandwidth  
   reported as zero [2-207](#)  
 bridge table  
   full [2-151](#)  
 broadcast, invalid source address [2-16](#)  
 bufferwraps  
   save to Flash [1-5](#)  
   save to interal Flash [1-13](#)  
   send to FTP server [1-13](#)  
 built H245 connection [2-73](#)

---

**C**

cannot specify PAT host [2-15](#)  
 class  
   filtering messages by [1-15](#)  
   message class variables [1-16](#)  
   types [1-16](#)  
 clear command  
   local-host option [2-142](#)  
 clearing configuration settings [1-21](#)  
 conduit command  
   permit ICMP option [2-15](#)  
 config command [2-33](#)  
 configuration [1-16](#)  
   clearing settings [1-21](#)  
   erase [2-33](#)  
   replication  
     beginning [2-219](#)  
     failed [2-218](#)  
     status changed [2-151](#)  
 configure command [2-33](#)  
 connection limit exceeded [2-55, 2-56, 2-221](#)  
 connection message [2-13, 2-14, 2-73](#)

**CTIQBE**

- connection object pre-allocation [2-210](#)
- unsupported version [2-210](#)

**D**

## deny

- inbound from outside [2-14](#)
  - inbound ICMP [2-15](#)
  - inbound UDP [2-13](#)
  - inbound UDP due to query/response [2-14](#)
  - IP from address to address [2-14](#)
  - IP spoof [2-16](#)
  - self route [2-14](#)
  - TCP (no connection) [2-15](#)
- detecting use of Internet phone [2-73](#)
- device ID, including in messages [1-19](#)
- device pass through
- disabled [2-205](#)
  - enabled [2-205](#)
- disabling messages, specific message IDs [1-20](#)
- DNS HINFO request attack [2-124](#)
- DNS query or response is denied [2-14](#)
- DNS request for all records attack [2-124](#)
- DNS server too slow [2-14](#)
- DNS zone transfer attack [2-124](#)
- DNS zone transfer from high port attack [2-124](#)
- DoS attack [2-20, 2-26, 2-61, 2-142](#)
- dropping echo request [2-15](#)

**E**

## Easy VPN Remote

- backup server list
  - downloaded [2-202](#)
  - error [2-203](#)
- device pass through
  - disabled [2-205](#)

- enabled [2-205](#)

## load balancing cluster

- disconnected [2-203](#)
- redirected [2-203](#)

split network entry duplicate [2-205](#)

## SUA

- disabled [2-204, 2-205](#)
- enabled [2-203](#)

## user authentication

- disabled [2-204](#)
- enabled [2-204](#)

XAUTH enabled [2-205](#)EMBLEM format, using in logs [1-19](#)embryonic limit exceeded [2-55](#)**F**

## facility

- setting [1-8](#)

## failover

- bad cable [2-2](#)
- block allocation failed [2-8](#)
- cable communication failed [2-8](#)
- cable not connected [2-2](#)
- cable status [2-2](#)
- configuration replication [2-8](#)
- configuration replication failed [2-220](#)
- continuous failovers [2-10](#)
- failed network interface [2-4](#)
- failover active command [2-354](#)
- failover command message dropped [2-9](#)
- incompatible software on mate [2-11](#)
- interface link down [2-11](#)
- LAN interface down [2-9](#)
- license mismatch with mate [2-12](#)
- link status up or down [2-7](#)
- lost communications with mate [2-6](#)
- mate card configuration mismatch [2-12](#)
- mate has different chassis [2-12](#)

mate may be disabled [2-10](#)  
 operational mode mismatch with mate [2-11](#)  
 peer failure [2-4](#)  
 peer LAN link down [2-9](#)  
 power failure [2-2](#)  
 primary unit failure [2-5](#)  
 replication interrupted [2-10](#)  
 show failover command [2-359](#)  
 standby unit failed to sync [2-8](#)  
 stateful error [2-62](#)  
 stateful failover [2-62, 2-63, 2-64](#)  
 VPN failover
 

- buffer error [2-351](#)
- client being disabled [2-349](#)
- CTCP flow handle error [2-356](#)
- failed to allocate chunk [2-349](#)
- failed to initialize [2-347](#)
- failed to receive message from active unit [2-359](#)
- memory allocation error [2-350](#)
- non-block message not sent [2-352](#)
- registration failure [2-349](#)
- SDI node secret file failed to synchronize [2-360](#)
- standby unit received corrupted message from active unit [2-357](#)
- state update message failure [2-357](#)
- timer error [2-351](#)
- trustpoint certification failure [2-350](#)
- trustpoint name not found [2-352](#)
- unable to add to message queue [2-356](#)
- version control block failure [2-349](#)

failover command [2-5, 2-6, 2-9](#)

- active option [2-4, 2-354](#)

failover messages [2-1, 2-3, 2-5, 2-7, 2-219](#)

filter allow command [2-82](#)

filter command
 

- activex option [2-176](#)
- allow option [2-82](#)

filtering ActiveX objects [2-176](#)

fixup protocol SMTP command [2-21](#)

Flood Defender [2-214](#)  
 floodguard command [2-25](#)  
 format of messages [1-22](#)  
 fragmented ICMP traffic attack [2-124](#)  
 FTP
 

- data connection failed [2-56](#)
- messages [2-81, 2-82](#)

---

## H

H.225 [2-139](#)  
 H.245 [2-73](#)  
 H.245 connection
 

- foreign address [2-73](#)

H.323 [2-73](#)

- back-connection, preallocated [2-73](#)
- unsupported packet version [2-218](#)

hello packet with duplicate router ID [2-146](#)

hostile event [2-17, 2-127, 2-133](#)

- firewall circumvented [2-17](#)

host limit [2-142](#)

host move [2-151](#)

HTTPS process limit [2-28](#)

---

## ICMP

packet denied [2-15](#)

- translation creation failed [2-84](#)

IDB initialization [2-94](#)

inbound TCP connection denied [2-13](#)

insufficient memory [2-59, 2-138](#)

- error caused by [2-59, 2-137](#)

interface
 

- PPP virtual [2-67](#)
- virtual [2-67](#)
- zero bandwidth [2-207](#)

Internet phone, detecting use of [2-73](#)

invalid character replaced in e-mail address [2-21](#)

invalid source addresses [2-16](#)

IP address

- DHCP client [2-190](#)
- DHCP server [2-190](#)

IP fragment attack [2-123](#)

IP fragments overlap attack [2-123](#)

IP impossible packet attack [2-123](#)

IP route counter decrement failure [2-143](#)

IP routing table

- attack [2-20](#)
- creation error [2-92](#)
- limit exceeded [2-92](#)
- limit warning [2-92](#)
- OSPF inconsistency [2-93](#)

IPSec

- connection entries [2-240](#)
- connections [2-35, 2-36, 2-37, 2-38, 2-39, 2-314](#)
  - failure [2-313](#)
  - L2TP-over-IPSec [2-241](#)
- cTCP tunnel [2-363](#)
- encryption [2-278](#)
- fragmentation policy ignored [2-256](#)
- invalid packet [2-126](#)
- L2TP-over-IPSec connection [2-241](#)
- negotiation [2-232](#)
- overTCP [2-286](#)
- over UDP [2-250, 2-286](#)
- packet [2-127](#)
- packet missing [2-126](#)
- packet triggered IKE [2-230](#)
- proposal
  - SA [2-290](#)
  - unsupported [2-290](#)
- protocol [2-224](#)
- proxy mismatch [2-79](#)
- rekeying duration [2-235](#)
- request rejected [2-241](#)
- SA [2-232, 2-237, 2-238, 2-241, 2-278, 2-280, 2-288](#)

- proposal [2-289, 2-290](#)
- tunnels [2-35, 2-91, 2-231, 2-255, 2-312, 2-313, 2-331](#)

ip verify reverse-path command [2-17, 2-18](#)

---

## L

L2TP

- tunnel [2-189](#)

land attack [2-16](#)

large ICMP traffic attack [2-124](#)

Leaving ALLOW mode, URL Server [2-82](#)

link state advertisement

- See LSA

link status 'Up' or 'Down' [2-7](#)

load balancing cluster

- disconnected [2-203](#)
- redirected [2-203](#)

log bufferwraps

- save to internal Flash [1-13](#)
- send to FTP server [1-13](#)

logging

- class
  - filtering messages by [1-15](#)
  - types [1-15, 1-16](#)
- device-id, including in system messages [1-19](#)
- email
  - configuring as output destination [1-9](#)
  - destination address [1-9](#)
  - source address [1-9](#)
- EMBLEM format [1-20](#)
- facility option [1-8](#)
- filtering
  - by message list [1-16](#)
  - by severity level [1-5](#)
- filtering messages
  - by message class [1-15](#)
- logging queue, configuring [1-18](#)
- output destinations
  - ASDM [1-10](#)

- email address [1-9](#)
- internal buffer [1-5](#)
- syslog server [1-7, 1-8](#)
- Telnet or SSH session [1-5](#)
- queue
  - changing the size of [1-18](#)
  - configuring [1-18](#)
  - viewing queue statistics [1-18](#)
- severity level
  - changing [1-21](#)
- timestamp, including [1-18](#)
- logging queue
  - configuring [1-18](#)
- log output destinations
  - ASDM [1-10](#)
  - email address [1-9](#)
  - internal buffer [1-5](#)
  - syslog server [1-5](#)
  - Telnet or SSH session [1-5](#)
- loopback network, invalid source address [2-16](#)
- lost failover communications with mate [2-6](#)
- low memory [2-91](#)
  - failed operation [2-91](#)
- LSA
  - default with wrong mask [2-145](#)
  - invalid type [2-145](#)
  - not found [2-93](#)

---

## M

- MAC address mismatch [2-138](#)
- man in the middle attack [2-95](#)
- memory
  - block depleted [2-8](#)
  - corruption [2-206](#)
  - insufficient [2-59, 2-138](#)
  - leak [2-93](#)
  - low [2-91](#)
- message block alloc failed [2-8](#)

- message classes
  - about [1-15](#)
  - list of [1-16](#)
- message list
  - creating [1-17](#)
  - filtering by [1-16](#)
- messages
  - alert log [2-20](#)
  - component descriptions [1-22](#)
  - connection-related [2-14, 2-55, 2-56, 2-73](#)
  - format of [1-22](#)
  - FTP [?? to 2-82](#)
  - Mail Guard [2-21](#)
  - severity levels [1-23](#)
    - list of [1-23](#)
  - SNMP [2-65](#)
  - SSH [2-91](#)
  - stateful failover [2-62, 2-63, 2-64](#)
  - variables used in [1-22, 1-23](#)
- message severity levels
  - list of [1-23](#)
- MIBs [1-1](#)
- Microsoft Point-to-Point Encryption
  - See MPPE
- module management [2-33](#)
- monitoring
  - SNMP [1-1](#)
- MPPE
  - encryption policy setup [2-132, 2-133](#)
- MS-CHAP [2-132](#)
  - authentication [2-132](#)

---

## N

- nat command [2-83](#)
- no associated connection within connection table [2-15](#)
- no authentication server found [2-24](#)
- no translation group found [2-83](#)

**O****OSPF**

- ABR without backbone area [2-93](#)
  - checksum error [2-206](#)
  - configuration change [2-207](#)
  - database description from unknown neighbor [2-144](#)
  - database request from unknown neighbor [2-144](#)
  - hello from unknown neighbor [2-144](#)
  - hello packet with duplicate router ID [2-146](#)
  - IDB initializatrion [2-94](#)
  - invalid packet [2-144](#)
  - IP routing table inconsistency [2-93](#)
  - LSA
    - default with wrong mask [2-145](#)
    - invalid type [2-145](#)
    - not found [2-93](#)
  - neighbor state changed [2-178](#)
  - network range area changed [2-207](#)
  - packet of invalid length [2-145](#)
  - process reset [2-94](#)
  - router ID allocation failure [2-146](#)
  - router-id reset [2-94](#)
  - virtual links [2-94](#)
- outbound deny command [2-13](#)
- out of address translation slots! [2-59](#)
- output destinations [1-5](#)
- e-mail address [1-5, 1-9](#)
  - internal buffer [1-5](#)
  - SNMP management station [1-5](#)
  - specifying [1-9](#)
  - syslog server [1-5, 1-7](#)
  - Telnet or SSH session [1-5](#)
  - viewing logs [1-7](#)

**P****packet**

- denied [2-13, 2-14, 2-15, 2-18](#)

- integrity check [2-14](#)
- not matched outbound NAT rules [2-83](#)

**PAT**

- address [2-59, 2-137, 2-138](#)
  - global address [2-15](#)
  - host unspecified [2-15](#)
- ping of death attack [2-124](#)
- power failure, failover [2-2](#)
- PPP virtual interface [2-67](#)
- PPTP
  - packet out of sequence [2-188](#)
  - tunnel [2-67, 2-189](#)
  - XGRE packet [2-131](#)
- preallocate H323 UDP back connection [2-73](#)
- privilege level, changed [2-177, 2-178](#)
- proxied RPC request attack [2-124](#)

**Q****queue, logging**

- changing the size of [1-18](#)
- viewing statistics [1-18](#)

**R**

- RADIUS authentication [2-132](#)
- RCMD, back connection failed [2-56](#)
- rebuilt TCP connection [2-74](#)
- reload command [2-33, 2-52](#)
- request discarded [2-221](#)
- router ID allocation failure [2-146](#)
- router-ID reset [2-94](#)
- rsh command [2-56](#)

**S****security**

- breach [2-14](#)

- context
    - added [2-179](#)
    - context cannot be determined [2-18, 2-19](#)
    - removed [2-179](#)
  - parameters index
    - See SPI
  - self route [2-14](#)
  - SETUP message [2-139](#)
  - severity levels, of system messages
    - changing [1-5](#)
    - definition [1-23](#)
    - filtering by [1-5](#)
    - list of [1-23](#)
  - show command
    - blocks option [2-8](#)
    - failover option [2-64, 2-359](#)
    - local-host option [2-142](#)
    - outbound option [2-13](#)
    - static option [2-55, 2-56](#)
    - version option [2-142](#)
  - show static command [2-55](#)
  - shuns [2-126](#)
  - SIP connection [2-193](#)
  - skinny connection [2-195](#)
  - SMTP [2-21](#)
  - SNMP
    - management station [1-5](#)
    - MIBs [1-1](#)
    - overview [1-1](#)
    - traps [1-2](#)
  - SPI [2-126](#)
  - split network entry duplicate [2-205](#)
  - spoofing attack [2-16, 2-17, 2-138](#)
  - SSH [2-91](#)
  - SSM 4GE [2-42 to 2-52](#)
  - std buffer overflow attack [2-124](#)
  - stateful failover [2-62, 2-63, 2-64](#)
  - SUA
    - disabled [2-204](#)
    - enabled [2-203](#)
  - SYN [2-15](#)
    - attack [2-55](#)
    - flag [2-15](#)
  - syslog server
    - as output destination [1-7](#)
      - designating [1-7](#)
      - designating more than one [1-8](#)
  - EMBLEM format
    - configuring [1-19](#)
    - enabling [1-7](#)
  - system messages
    - classes of [1-15](#)
      - list of classes [1-16](#)
    - configuring in groups
      - by message list [1-16](#)
      - by severity level [1-5](#)
    - creating lists of [1-15](#)
    - device ID, including [1-19](#)
    - disabling logging of [1-5](#)
    - filtering
      - by message class [1-15](#)
    - managing in groups
      - by message class [1-15](#)
      - creating a message list [1-15](#)
    - output destinations [1-5](#)
      - email address [1-9](#)
      - internal buffer [1-5](#)
      - syslog message server [1-5](#)
      - Telnet or SSH session [1-5](#)
    - severity levels [1-23](#)
      - changing the severity level of a message [1-5](#)
    - timestamp, including [1-18](#)
- 
- ## T
- TCP
    - access permitted [2-220](#)
    - access requested [2-220](#)



- connection limit exceeded [2-221](#)
- connections [2-220](#)
- incorrect header length [2-176](#)
- no associated connection in table [2-15](#)
- request discarded [2-221](#)
- translation creation failed [2-84](#)
- TCP FIN only flags attack [2-124](#)
- TCP NULL flags attack [2-124](#)
- TCP SYN+FIN flags attack [2-124](#)
- testing
  - interface [2-7](#)
- timeouts, recommended values [2-142](#)
- timeout uauth command [2-25](#)
- timestamp, including in system messages [1-18](#)
- too many connections on static [2-55](#)
- traps, SNMP [1-2](#)
- tunnel, PPTP [2-67](#)

---

## U

- UDP
  - access permitted [2-220](#)
  - bomb attack [2-124](#)
  - chargen DoS attack [2-124](#)
  - connections [2-220](#)
  - messages [2-83](#)
  - packet [2-14](#)
  - request discarded [2-221](#)
  - snork attack [2-124](#)
  - translation creation failed [2-84](#)
- URL
  - buffer block space [2-83](#)
  - filtering, disabled [2-82](#)
  - Server [2-81](#)
- user authentication
  - disabled [2-204](#)
  - enabled [2-204](#)
  - error [2-27](#)
- user logged out [2-200](#)

- username
  - created [2-177](#)
  - deleted [2-177](#)

---

## V

- variables
  - in messages [1-22, 1-23](#)
  - list of [1-23](#)
- viewing logs [1-7](#)
- virtual interface [2-67](#)
- virtual links [2-94](#)
- vpdn group command [2-132](#)
- VPN
  - peer limit [2-91](#)
  - tunnel [2-91](#)
- VPN failover
  - client being disabled [2-349](#)
  - CTCP flow handle error [2-356](#)
  - failed to allocate chunk [2-349](#)
  - failed to initialize [2-347](#)
  - failed to receive message from active unit [2-359](#)
  - memory allocation error [2-350](#)
  - non-block message not sent [2-352](#)
  - registration failure [2-349](#)
  - SDI node secret file failed to synchronize [2-360](#)
  - standby unit received corrupted message from active unit [2-357](#)
  - state update message failure [2-357](#)
  - timer error [2-351](#)
  - trustpoint certification failure [2-350](#)
  - trustpoint name not found [2-352](#)
  - unable to add to message queue [2-356](#)
  - version control block failure [2-349](#)

---

## W

- web requests, unfiltered [2-82](#)
- Websense server [2-81, 2-82](#)

write command [2-33](#)  
erase option [2-33](#)  
standby command [2-64](#)  
standby option [2-63](#)  
write erase command [2-33](#)

---

## **X**

XAUTH enabled [2-205](#)  
XGRE, packet with invalid protocol field [2-131](#)