



Cisco Security Appliance システム ログ メッセージ

Cisco PIX 500 シリーズおよび Cisco ASA シリーズ セキュリティ アプライアンス用

Software Version 7.0



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリックドメインバージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いません。

CCSP、Cisco Square Bridge のロゴ、Follow Me Browsing、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、SwitchProbe、TeleRouter、The Fastest Way to Increase Your Internet Quotient、TransPath、および VCO は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルまたは Web サイトで言及されているその他の商標はすべて、それぞれの所有者のもです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。(0501R)

Cisco Security Appliance システム ログメッセージ

Copyright © 2005 Cisco Systems, Inc.

All rights reserved.



このマニュアルについて	xxxv
マニュアルの目的	xxxv
対象読者	xxxv
マニュアルの構成	xxxvi
マニュアルの表記法	xxxvi
関連資料	xxxvi
技術情報の入手方法	xxxvii
Cisco.com	xxxvii
Documentation DVD (英語版)	xxxvii
マニュアルの発注方法 (英語版)	xxxvii
シスコシステムズマニュアルセンター	xxxviii
シスコ製品のセキュリティの概要	xxxix
シスコ製品のセキュリティ問題の報告	xxxix
テクニカル サポート	xi
Cisco Technical Support Web サイト	xi
Japan TAC Web サイト	xi
サービス リクエストの発行	xli
サービス リクエストのシビラティの定義	xli
その他の資料および情報の入手方法	xlii

CHAPTER 1

セキュリティ アプライアンスのロギングの設定	1-1
ロギングの概要	1-2
基本ロギング コマンド	1-3
ロギングのイネーブル化およびディセーブル化	1-3
重大度の変更またはメッセージのディセーブル化	1-4
コンフィギュレーション設定値のデフォルト値への復元	1-4
システム ログ メッセージ出力先の指定および管理	1-5
出力先を設定および管理するコマンド	1-5
ロギング キューの設定および管理	1-8
ロギング バッファの設定および管理	1-8
メッセージのグループの管理	1-10

メッセージ クラス変数の値	1-11
システム ログ メッセージの内容および形式の修正	1-12
ロギング コマンド例	1-13
ロギングのイネーブル化	1-13
ロギング出力のテスト	1-14
システム ログ メッセージの出力先の設定	1-15
システム ログ メッセージのバッファへの送信	1-15
システム ログ メッセージの Syslog サーバへの送信	1-16
システム ログ メッセージの電子メール アドレスへの送信	1-17
システム ログ メッセージの Telnet コンソール セッションへの送信	1-18
システム ログ メッセージの SNMP 管理ステーションへの送信	1-20
SNMP 要求の受信	1-20
SNMP トラップの送信	1-20
特定のシステム ログ メッセージのディセーブル化およびイネーブル化	1-21
特定のシステム ログ メッセージのディセーブル化	1-21
ディセーブル状態のシステム ログ メッセージのリストの表示	1-21
ディセーブル状態の特定システム ログ メッセージの再イネーブル化	1-21
ディセーブル状態のシステム ログ メッセージすべての再イネーブル化	1-21
ログ メッセージの概要	1-22
ログ メッセージの形式	1-22
重大度	1-22
変数	1-23
他のリモート管理ツールおよびモニタ ツール	1-26
Cisco ASDM	1-26
Cisco Secure Policy Manager	1-26
SNMP トラップ	1-26
Telnet	1-26

CHAPTER 2

システム ログ メッセージ	2-1
メッセージ 101001 ~ 199009	2-2
101001	2-2
101002	2-2
101003, 101004	2-2
101005	2-2
102001	2-3
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	2-5	
105003	2-6	
105004	2-6	
105005	2-6	
105006, 105007		2-6
105008	2-7	
105009	2-7	
105010	2-7	
105011	2-7	
105020	2-8	
105021	2-8	
105031	2-8	
105032	2-8	
105034	2-9	
105035	2-9	
105036	2-9	
105037	2-9	
105038	2-9	
105039	2-10	
105040	2-10	
105042	2-10	
105043	2-10	
105044	2-11	
105045	2-11	
105046	2-11	
105047	2-11	
106001	2-12	
106002	2-12	
106006	2-12	
106007	2-13	

106010	2-13	
106011	2-13	
106012	2-13	
106013	2-14	
106014	2-14	
106015	2-14	
106016	2-14	
106017	2-15	
106018	2-15	
106020	2-15	
106021	2-15	
106022	2-16	
106023	2-16	
106024	2-16	
106025, 106026	2-17	
106027	2-17	
106100	2-17	
106101	2-18	
107001	2-18	
107002	2-18	
108002	2-19	
108003	2-19	
109001	2-19	
109002	2-19	
109003	2-20	
109005	2-20	
109006	2-20	
109007	2-20	
109008	2-21	
109010	2-21	
109011	2-21	
109012	2-21	
109013	2-21	
109014	2-22	
109016	2-22	
109017	2-22	
109018	2-22	
109019	2-23	

109020	2-23
109021	2-23
109022	2-23
109023	2-24
109024	2-24
109025	2-24
109026	2-24
109027	2-25
109028	2-25
109029	2-25
109030	2-25
109031	2-26
109032	2-26
110001	2-26
111001	2-27
111002	2-27
111003	2-27
111004	2-27
111005	2-28
111007	2-28
111008	2-28
111009	2-28
111111	2-28
112001	2-29
113001	2-29
113003	2-29
113004	2-29
113005	2-30
113006	2-30
113007	2-30
113008	2-30
113009	2-31
113010	2-31
113011	2-31
113012	2-31
113013	2-32
113014	2-32
113015	2-32

113016	2-32
113017	2-33
113018	2-33
113019	2-33
113020	2-34
114001	2-34
114002	2-34
114003	2-35
114004	2-36
114005	2-36
114006	2-36
114007	2-37
114008	2-37
114009	2-38
114010	2-38
114011	2-39
114012	2-40
114013	2-40
114014	2-41
114015	2-42
114016	2-42
114017	2-43
114018	2-43
114019	2-44
114020	2-45
199001	2-45
199002	2-45
199003	2-45
199005	2-46
199006	2-46
199907	2-46
199908	2-46
199909	2-47
メッセージ 201002 ~ 217001	2-48
201002	2-48
201003	2-48
201004	2-48
201005	2-49

201006	2-49
201008	2-49
201009	2-49
201010	2-50
202001	2-50
202005	2-50
202011	2-51
208005	2-51
209003	2-51
209004	2-52
209005	2-52
210001	2-52
210002	2-53
210003	2-53
210005	2-53
210006	2-53
210007	2-54
210008	2-54
210010	2-54
210020	2-54
210021	2-55
210022	2-55
211001	2-55
211003	2-55
212001	2-55
212002	2-56
212003	2-56
212004	2-56
212005	2-57
212006	2-57
213001	2-57
213002	2-57
213003	2-58
213004	2-58
214001	2-58
215001	2-58
217001	2-58
216002	2-59

216003	2-59	
メッセージ	302003 ~ 326028	2-60
302003	2-60	
302004	2-60	
302009	2-60	
302010	2-61	
302012	2-61	
302013	2-61	
302014	2-61	
302015	2-62	
302016	2-63	
302017	2-63	
302018	2-64	
302019	2-64	
302020	2-65	
302021	2-65	
302302	2-65	
303002	2-65	
303003	2-65	
303004	2-66	
304001	2-66	
304002	2-66	
304003	2-66	
304004	2-66	
304005	2-67	
304006	2-67	
304007	2-67	
304008	2-67	
304009	2-67	
305005	2-68	
305006	2-68	
305007	2-69	
305008	2-69	
305009	2-69	
305010	2-69	
305011	2-70	
305012	2-70	
308001	2-70	

308002	2-70
311001	2-71
311002	2-71
311003	2-71
311004	2-71
312001	2-71
313001	2-72
313003	2-72
313004	2-72
314001	2-72
315004	2-73
315011	2-73
316001	2-74
317001	2-75
317002	2-75
317003	2-75
317004	2-75
317005	2-75
318001	2-76
318002	2-76
318003	2-76
318004	2-76
318005	2-76
318006	2-77
318007	2-77
318008	2-77
318009	2-77
319001	2-78
319002	2-78
319003	2-78
319004	2-78
320001	2-79
321001	2-79
321002	2-79
321003	2-79
321004	2-79
322001	2-80
322002	2-80

322003	2-80
322004	2-81
323004	2-81
323005	2-82
324000	2-82
324001	2-82
324002	2-83
324003	2-83
324004	2-83
324005	2-84
324006	2-84
324007	2-84
325001	2-84
325002	2-85
326001	2-85
326002	2-85
326004	2-85
326005	2-86
326006	2-86
326007	2-86
326008	2-86
326009	2-87
326010	2-87
326011	2-87
326012	2-87
326013	2-87
326014	2-88
326015	2-88
326016	2-88
326017	2-88
326019	2-88
326020	2-89
326021	2-89
326022	2-89
326023	2-89
326024	2-89
326025	2-90
326026	2-90

326027	2-90	
326028	2-90	
メッセージ 400000 ~ 418001		2-91
4000nn	2-91	
401001	2-93	
401002	2-93	
401003	2-93	
401004	2-93	
401005	2-94	
402101	2-94	
402102	2-94	
402103	2-94	
402106	2-95	
402114	2-95	
402115	2-95	
402116	2-96	
402117	2-96	
402118	2-97	
402119	2-97	
402120	2-98	
402121	2-98	
402122	2-99	
402123	2-99	
403101	2-99	
403102	2-99	
403103	2-100	
403104	2-100	
403106	2-100	
403107	2-100	
403108	2-100	
403109	2-101	
403110	2-101	
403500	2-101	
403501	2-101	
403502	2-102	
403503	2-102	
403504	2-102	
403505	2-103	

403506	2-103
404101	2-103
404102	2-103
405001	2-104
405101	2-104
405002	2-104
405101	2-105
405102	2-105
405103	2-105
405104	2-105
405105	2-106
405201	2-106
406001	2-106
406002	2-106
407001	2-107
407002	2-107
407003	2-107
408001	2-108
408002	2-108
409001	2-108
409002	2-108
409003	2-109
409004	2-109
409005	2-109
409006	2-109
409007	2-109
409008	2-110
409009	2-110
409010	2-110
409011	2-110
409012	2-110
409013	2-111
409023	2-111
410001	2-111
411001	2-111
411002	2-112
411003	2-112
411004	2-112

412001	2-112
412002	2-113
413001	2-113
413002	2-113
413003	2-113
413004	2-114
414001	2-114
414002	2-114
415001	2-115
415002	2-115
415003	2-115
415004	2-116
415005	2-116
415006	2-117
415007	2-117
415008	2-117
415009	2-118
415010	2-118
415011	2-119
415012	2-119
415013	2-119
415014	2-120
416001	2-120
417001	2-120
417004	2-121
417006	2-121
418001	2-121
419001	2-121
420001	2-122
420002	2-122
420003	2-123
メッセージ 500001 ~ 507001	2-124
500001	2-124
500002	2-124
500003	2-124
500004	2-125
501101	2-125
502101	2-125

502102	2-125	
502103	2-125	
502111	2-126	
502112	2-126	
503001	2-126	
504001	2-126	
504002	2-126	
505001	2-127	
505002	2-127	
505003	2-127	
505004	2-127	
505005	2-127	
505006	2-128	
505007	2-128	
505008	2-128	
505009	2-128	
506001	2-129	
507001	2-129	
メッセージ 602101 ~ 609002	2-130	
602101	2-130	
602103	2-130	
602104	2-130	
602201	2-131	
602202	2-131	
602203	2-131	
602303	2-131	
602304	2-132	
603101	2-132	
603102	2-132	
603103	2-132	
603104	2-133	
603105	2-133	
603106	2-133	
603107	2-133	
603108	2-133	
603109	2-134	
604101	2-134	
604102	2-134	

604103	2-134
604104	2-134
605004	2-135
605005	2-135
606001	2-136
606002	2-136
606003	2-136
606004	2-136
607001	2-136
608001	2-137
609001	2-137
609002	2-137
610001	2-138
610002	2-138
610101	2-138
611101	2-138
611102	2-139
611103	2-139
611104	2-139
611301	2-139
611302	2-139
611303	2-140
611304	2-140
611305	2-140
611306	2-140
611307	2-140
611308	2-141
611309	2-141
611310	2-141
611311	2-141
611312	2-141
611313	2-142
611314	2-142
611315	2-142
611316	2-142
611317	2-143
611318	2-143
611319	2-143

611320	2-143
611321	2-144
611322	2-144
611323	2-144
612001	2-144
612002	2-145
612003	2-145
613001	2-145
613002	2-145
613003	2-146
614001	2-146
614002	2-146
615001	2-146
615002	2-146
616001	2-147
617001	2-147
617002	2-147
617003	2-147
617004	2-148
620001	2-148
620002	2-148
621001	2-148
621002	2-149
621003	2-149
621006	2-149
621007	2-149
メッセージ 701001 ~ 720073	2-150
701001	2-150
701002	2-150
702201	2-150
702202	2-151
702203	2-151
702204	2-151
702205	2-151
702206	2-151
702207	2-152
702208	2-152
702209	2-152

702210	2-152	
702211	2-152	
702212	2-153	
702305	2-153	
702307	2-153	
703001	2-154	
703002	2-154	
709001, 709002	2-154	2-154
709003	2-154	
709004	2-155	
709005	2-155	
709006	2-155	
709007	2-155	
710001	2-156	
710002	2-156	
710003	2-156	
710004	2-157	
710005	2-157	
710006	2-157	
711001	2-157	
711002	2-158	
713004	2-158	
713006	2-158	
713008	2-158	
713009	2-159	
713010	2-159	
713012	2-159	
713014	2-159	
713016	2-160	
713017	2-160	
713018	2-160	
713020	2-160	
713022	2-160	
713024	2-161	
713025	2-161	
713026	2-161	
713027	2-161	
713028	2-161	

713029	2-162
713030	2-162
713031	2-162
713032	2-162
713033	2-162
713034	2-163
713035	2-163
713036	2-163
713037	2-163
713039	2-163
713040	2-164
713041	2-164
713042	2-164
713043	2-164
713047	2-165
713048	2-165
713049	2-165
713050	2-165
713051	2-165
713052	2-166
713056	2-166
713059	2-166
713060	2-166
713061	2-167
713062	2-167
713063	2-167
713065	2-167
713066	2-168
713068	2-168
713072	2-168
713073	2-168
713074	2-168
713075	2-169
713076	2-169
713078	2-169
713081	2-169
713082	2-169
713083	2-170

713084	2-170
713085	2-170
713086	2-170
713088	2-171
713092	2-171
713094	2-171
713098	2-171
713099	2-172
713102	2-172
713103	2-172
713104	2-172
713105	2-173
713107	2-173
713109	2-173
713112	2-173
713113	2-174
713114	2-174
713115	2-174
713116	2-174
713117	2-175
713118	2-175
713119	2-175
713120	2-175
713121	2-175
713122	2-176
713123	2-176
713124	2-176
713127	2-176
713128	2-176
713129	2-177
713130	2-177
713131	2-177
713132	2-177
713133	2-178
713134	2-178
713135	2-178
713136	2-178
713137	2-179

713138	2-179
713139	2-179
713140	2-179
713141	2-180
713142	2-180
713143	2-180
713144	2-180
713145	2-181
713146	2-181
713147	2-181
713148	2-182
713149	2-182
713152	2-182
713154	2-182
713155	2-183
713156	2-183
713157	2-183
713158	2-183
713159	2-184
713160	2-184
713161	2-184
713162	2-184
713163	2-185
713164	2-185
713165	2-185
713166	2-185
713167	2-186
713168	2-186
713169	2-186
713170	2-186
713171	2-186
713172	2-187
713174	2-187
713176	2-187
713177	2-187
713178	2-187
713179	2-188
713182	2-188

713184	2-188
713185	2-188
713186	2-189
713187	2-189
713189	2-189
713190	2-189
713193	2-190
713194	2-190
713195	2-190
713196	2-190
713197	2-191
713198	2-191
713199	2-191
713203	2-191
713204	2-192
713205	2-192
713206	2-192
713208	2-192
713209	2-193
713210	2-193
713211	2-193
713212	2-193
713213	2-194
713214	2-194
713215	2-194
713216	2-195
713217	2-195
713218	2-195
713219	2-195
713220	2-195
713221	2-196
713222	2-196
713223	2-196
713224	2-196
713225	2-197
713226	2-197
713228	2-197
713229	2-197

713230	2-198
713231	2-198
713232	2-198
713233	2-199
713234	2-199
713235	2-199
713236	2-200
713237	2-200
713238	2-200
713900	2-201
713901	2-201
713902	2-201
713903	2-201
713904	2-202
713905	2-202
713906	2-202
714001	2-202
714002	2-202
714003	2-203
714004	2-203
714005	2-203
714006	2-203
714007	2-203
714011	2-204
715001	2-204
715004	2-204
715005	2-204
715006	2-204
715007	2-205
715008	2-205
715009	2-205
715013	2-205
715019	2-205
715020	2-206
715021	2-206
715022	2-206
715027	2-206
715028	2-206

715033	2-207
715034	2-207
715035	2-207
715036	2-207
715037	2-208
715038	2-208
715039	2-208
715040	2-208
715041	2-209
715042	2-209
715044	2-209
715045	2-209
715046	2-209
715047	2-210
715048	2-210
715049	2-210
715050	2-210
715051	2-210
715052	2-211
715053	2-211
715054	2-211
715055	2-211
715056	2-211
715057	2-212
715058	2-212
715059	2-212
715060	2-212
715061	2-213
715062	2-213
715063	2-213
715064	2-213
715065	2-214
715066	2-214
715067	2-214
715068	2-214
715069	2-215
715070	2-215
715071	2-215

715072	2-215
715074	2-216
715075	2-216
715076	2-216
715077	2-217
716001	2-217
716002	2-217
716003	2-218
716004	2-218
716005	2-219
716006	2-219
716007	2-219
716008	2-219
716009	2-220
716010	2-220
716011	2-220
716012	2-220
716013	2-220
716014	2-221
716015	2-221
716016	2-221
716017	2-221
716018	2-221
716019	2-221
716020	2-222
716021	2-222
716022	2-222
716023	2-222
716024	2-222
716025	2-223
716026	2-223
716027	2-223
716028	2-223
716029	2-224
716030	2-224
716031	2-224
716032	2-224
716033	2-225

716034	2-225
716035	2-225
716036	2-225
716037	2-225
716038	2-226
716039	2-226
716040	2-226
716041	2-226
716042	2-227
717001	2-227
717002	2-227
717003	2-227
717004	2-228
717005	2-228
717006	2-228
717007	2-228
717008	2-228
717009	2-229
717010	2-229
717011	2-229
717012	2-229
717013	2-230
717014	2-230
717015	2-230
717016	2-230
717017	2-231
717018	2-231
717019	2-231
717021	2-232
717022	2-232
717023	2-232
717024	2-233
717025	2-233
717026	2-233
717027	2-233
717028	2-234
717029	2-234
717030	2-234

717031	2-234
718001	2-235
718002	2-235
718003	2-235
718004	2-235
718005	2-236
718006	2-236
718007	2-236
718008	2-237
718009	2-237
718010	2-237
718011	2-237
718012	2-238
718013	2-238
718014	2-238
718015	2-238
718016	2-238
718017	2-239
718018	2-239
718019	2-239
718020	2-239
718021	2-240
718022	2-240
718023	2-240
718024	2-240
718025	2-240
718026	2-241
718027	2-241
718028	2-241
718029	2-241
718030	2-241
718031	2-242
718032	2-242
718033	2-242
718034	2-242
718035	2-242
718036	2-243
718037	2-243

718038	2-243
718039	2-243
718040	2-243
718041	2-244
718042	2-244
718043	2-244
718044	2-244
718045	2-244
718046	2-245
718047	2-245
718048	2-245
718049	2-245
718050	2-245
718051	2-246
718052	2-246
718053	2-246
718054	2-246
718055	2-246
718056	2-247
718057	2-247
718058	2-247
718059	2-247
718060	2-247
718061	2-248
718062	2-248
718063	2-248
718064	2-248
718065	2-248
718066	2-249
718067	2-249
718068	2-249
718069	2-249
718070	2-249
718071	2-250
718072	2-250
718073	2-250
718074	2-250
718075	2-250

718076	2-251
718077	2-251
718078	2-251
718079	2-251
718080	2-252
718081	2-252
718084	2-252
718085	2-252
718086	2-253
718087	2-253
718088	2-253
719001	2-253
719002	2-254
719003	2-254
719004	2-254
719005	2-254
719006	2-255
719007	2-255
719008	2-255
719009	2-255
719010	2-256
719011	2-256
719012	2-256
719013	2-256
719014	2-257
719015	2-257
719016	2-257
719017	2-257
719018	2-258
719019	2-258
719020	2-258
719021	2-258
719022	2-259
719023	2-259
719024	2-259
719025	2-259
719026	2-260
720001	2-260

720002	2-260
720003	2-260
720004	2-260
720005	2-261
720006	2-261
720007	2-261
720008	2-261
720009	2-262
720010	2-262
720011	2-262
720012	2-262
720013	2-263
720014	2-263
720015	2-263
720016	2-263
720017	2-264
720018	2-264
720019	2-264
720020	2-264
720021	2-265
720022	2-265
720023	2-265
720024	2-265
720025	2-266
720026	2-266
720027	2-266
720028	2-266
720029	2-267
720030	2-267
720031	2-267
720032	2-267
720033	2-268
720034	2-268
720035	2-268
720036	2-269
720037	2-269
720038	2-269
720039	2-270

720040	2-270
720041	2-270
720042	2-270
720043	2-271
720044	2-271
720045	2-271
720046	2-272
720047	2-272
720048	2-272
720049	2-272
720050	2-273
720051	2-273
720052	2-273
720053	2-274
720054	2-274
720055	2-274
720056	2-275
720057	2-275
720058	2-275
720059	2-275
720060	2-276
720061	2-276
720062	2-276
720063	2-276
720064	2-277
720065	2-277
720066	2-277
720067	2-278
720068	2-278
720069	2-278
720070	2-278
720071	2-279
720072	2-279
720073	2-279

APPENDIX A

重大度別メッセージ リスト A-1

アラート メッセージ、重大度 1 A-2

クリティカル メッセージ、重大度 2 A-4

エラー メッセージ、重大度 3 A-6

警告メッセージ、重大度 4	A-13
通知メッセージ、重大度 5	A-18
情報メッセージ、重大度 6	A-23
デバッグメッセージ、重大度 7	A-31



このマニュアルについて

ここでは、次の内容について説明します。

- [マニュアルの目的 \(P.xxxv\)](#)
- [対象読者 \(P.xxxv\)](#)
- [マニュアルの構成 \(P.xxxvi\)](#)
- [マニュアルの表記法 \(P.xxxvi\)](#)
- [関連資料 \(P.xxxvi\)](#)
- [技術情報の入手方法 \(P.xxxvii\)](#)
- [テクニカル サポート \(P.xl\)](#)

マニュアルの目的

このマニュアルでは、Cisco ASA 5500 シリーズ セキュリティ アプライアンス Software Version 7.0 によって生成されるシステム ログ (syslog) メッセージについて説明します。syslog エラー以外でコンソールに表示されるメッセージについては取り上げていません。

対象読者

このマニュアルは、次のタスクを実行するネットワーク管理者を対象としています。

- ネットワークのセキュリティ管理
- ファイアウォールの設定、管理、およびトラブルシューティング

このマニュアルでは、『*Cisco Security Appliance Command Reference*』に説明されているコマンドおよびコンフィギュレーション オプションを理解していることを前提としています。また、セキュリティ アプライアンスが動作するネットワークに関する知識も必要です。

マニュアルの構成

このマニュアルは、次の章で構成されています。

- 第 1 章「**セキュリティ アプライアンスのロギングの設定**」では、システム ログ メッセージの機能と、メッセージの形式について説明します。
- 第 2 章「**システム ログ メッセージ**」では、システム ログ メッセージを列挙し、各メッセージに考えられる原因を示します。また、ログ メッセージの原因となった状態を解決するための方法を説明します。
- 付録 A「**重大度別メッセージリスト**」では、メッセージ番号とメッセージの内容を、重大度ごとに列挙します。

マニュアルの表記法

このマニュアルは、次の表記法を使用しています。

- ユーザが値を指定するファイル名、ディレクトリ名、および引数は、イタリック体で示しています。
- ^記号は、Ctrl (control) キーを表します。^z のように control キーを入力するには、Ctrl キーを押しながら z キーを押します。
- コマンド名、キー、ボタン、および文中のキーワードは、**太字**で示しています。セキュリティ アプライアンスのコマンドは、『Cisco Security Appliance Command Reference』に詳しく説明されています。
- コマンドの構文の説明内の変数は、イタリック体で示しています。角カッコ [] 中のコマンド オプションは省略可能です。縦棒 (|) で区切られているパラメータは、どれか 1 つのパラメータを入力する必要がありますが、それ以外は入力する必要がないことを示しています。
- 画面に表示される情報およびコマンドラインは、screen フォントで示しています。
- ユーザが入力する情報は、太字の screen フォントで示しています。
- ユーザが値を指定する変数は、イタリック体の screen フォントで示しています。
- メニュー（または画面）の選択手順は、次のように示しています。
screen1 > screen2 > screen3 を選択します。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

関連資料

セキュリティ アプライアンスの一連のマニュアルと一緒に、次の Web サイトからオンラインで利用できるマニュアルも参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix_sw/index.htm

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

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

シスコの Web サイトには、次の URL からアクセスできます。

<http://www.cisco.com>

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

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

Documentation DVD (英語版)

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Documentation DVD パッケージでご利用いただけます。Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。また、この Documentation DVD パッケージのみを発注することもできます。

Cisco.com 登録ユーザ (Cisco Direct Customers) の場合、Ordering ツールまたは Cisco Marketplace から Cisco Documentation DVD (Product Number DOC-DOCDVD=) を発注できます。

Cisco Ordering ツール :

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

Cisco Marketplace :

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

マニュアルの発注方法 (英語版)

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com 登録ユーザ (Cisco Direct Customers) の場合、Ordering ツールからシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

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

- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

<http://www2.hipri.com/cisco/>

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

<http://www2.hipri.com/cisco/>

なお、技術内容に関するお問い合わせは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合わせください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル (英文のみ) を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

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

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合 : security-alert@cisco.com (英語のみ)
- 緊急でない場合 : psirt@cisco.com (英語のみ)



ヒント

シスコに機密情報をお送りいただく際には、PGP (Pretty Good Privacy) または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.x から 8.x と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵は、次の公開鍵サーバのリストで作成日が最新の鍵です。

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

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302 (英語のみ)
- 1 408 525-6532 (英語のみ)

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center (TAC) のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合わせください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

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

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

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



(注)

Web または電話でサービス リクエストを発行する前に、Cisco Product Identification (CPI) ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、show コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register>

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます (S3: ネットワークに軽微な障害が発生した、S4: 製品情報が必要である)。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

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

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください (S1: ネットワークがダウンした、S2: ネットワークの機能が著しく低下した)。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

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

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1 (S1): ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2 (S2): 既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3 (S3): ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4 (S4): シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

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

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

<http://www.ciscopress.com>

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

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

日本語版 『*Packet*』は、米国版 『*Packet*』と日本版のオリジナル記事で構成されています。日本語版 『*Packet*』には、次の URL からアクセスしてください。

<http://www.cisco.com/japanese/warp/public/3/jp/news/packet/>

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

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

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

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

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

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



セキュリティ アプライアンスのロギングの設定

この章では、セキュリティ アプライアンスのロギングの設定および管理に使用するコマンドについて説明します。また、システム ログ メッセージの形式と、リモート管理およびモニタ ツールについても説明します。

この章では、ロギング コマンドおよびオプション全体についての総合的な説明は行いません。詳細な説明と、その他のロギング コマンドについては、『*Cisco Security Appliance Command Reference*』を参照してください。

ここでは、次の項目について説明します。

- [ロギングの概要 \(P.1-2\)](#)
- [基本ロギング コマンド \(P.1-3\)](#)
- [システム ログ メッセージ出力先の指定および管理 \(P.1-5\)](#)
- [システム ログ メッセージの内容および形式の修正 \(P.1-12\)](#)
- [ロギング コマンド例 \(P.1-13\)](#)
- [ログ メッセージの概要 \(P.1-22\)](#)
- [他のリモート管理ツールおよびモニタ ツール \(P.1-26\)](#)

ロギングの概要

システム メッセージ ロギング機能は、セキュリティ アプライアンスのモニタリングおよびトラブルシューティングに関するロギング情報を表示します。ロギング設定は非常に柔軟性があり、セキュリティ アプライアンスのメッセージ処理をさまざまな局面でカスタマイズできます。

システム メッセージのロギング機能を使用すると、次の処理が可能になります。

- ログに記録するメッセージの指定。
- メッセージの重大度のディセーブル化または変更。
- メッセージの送信先（複数も可）の指定。たとえば、コンソール、内部バッファ、1 つまたは複数の `syslog` サーバ、ASDM、SNMP 管理ステーション、特定の電子メール アドレス、Telnet セッション、SSH セッションを指定できます。
- グループ（重大度やメッセージクラスによる）でのメッセージの設定および管理。
- バッファがいっぱいになり、バッファラップが発生した場合の、内部バッファの内容の処理方法の設定。バッファの内容を FTP サーバに送信するか、またはフラッシュに保存するかにセキュリティ アプライアンスを設定できます。
- ASDM、Telnet および SSH セッションを使用するか、または内部ログ バッファの内容を Web ブラウザにダウンロードすることによる、リモートでのシステム メッセージのモニタリング。

ロギング コマンドのほとんどは、設定モードで入力されます。設定モードにするには、`configure terminal` コマンドを入力します。

セキュリティ アプライアンスによって生成されたログを表示するには、出力先を設定する必要があります。送信するメッセージは全部か、または一部か、出力先は全部か、または任意の箇所かという選択ができます。メッセージの重大度によって、メッセージのクラスによって、またはメッセージ リストを作成することによって、送信するメッセージとその送信先を限定することができます。メッセージ リストを作成すると、送信する複数のメッセージに対してシステム ログ メッセージ宛先を1 つでも複数でも自由に指定できます。

多くのロギング コマンドでは、コマンドを適用するメッセージを特定するために、重大度しきい値を指定する必要があります。重大度の値は0 から7 で、レベル番号が小さいほど重大なエラーとなります。重大度は数値またはキーワードで指定します（表 1-6 を参照）。レベルを指定すると、セキュリティ アプライアンスによってコマンドがそのレベル以下のメッセージに適用されます。たとえば、重大度3 を指定するコマンドを入力すると、そのコマンドの結果は重大度1、2、および3 のメッセージに適用されます。



(注)

セキュリティ アプライアンスでは、重大度が0 (emergencies) のメッセージは生成されません。このレベルは、UNIX システム ログ メッセージ機能との互換性のために、`logging` コマンドで指定できますが、セキュリティ アプライアンスでは使用されません。

一部のログおよびロギング コマンドでは、`format emblem` オプションをサポートします。EMBLEM システム ログ メッセージの形式は、Cisco IOS ソフトウェア フォーマットと整合するように設計されており、CiscoWorks 管理アプリケーションとも互換性があります。



(注)

システム メッセージはすべてがエラー状態を示すわけではありません。正常なイベントを報告したり、設定変更をログに記録したりするだけのメッセージもあります。

基本ロギング コマンド

ロギング コマンドの一般的な使用方法には、ロギングの開始、ロギングの停止、メッセージの重大度の変更、メッセージのディセーブル化、および設定変更の復元などがあります。ここでは、次の項目について説明します。

- [ロギングのイネーブル化およびディセーブル化 \(P.1-3\)](#)
- [重大度の変更またはメッセージのディセーブル化 \(P.1-4\)](#)
- [コンフィギュレーション設定値のデフォルト値への復元 \(P.1-4\)](#)

ロギングのイネーブル化およびディセーブル化

次のコマンドは、ロギングをイネーブルにするため、ログを表示するため、およびコンフィギュレーション設定値を表示するために使用します。

目的	コマンド	説明
ロギングのイネーブル化およびディセーブル化	logging enable	<p>すべての出力先へのシステム ログ メッセージの送信をイネーブルにします。</p> <p>ログを表示するには、ロギングの出力先を設定する必要があります。</p> <p> (注) logging on コマンドは、下位互換性のためにそのままサポートされています。</p>
	no logging enable	<p>すべての出力先へのロギングをディセーブルにします。</p>
ログおよびコンフィギュレーション設定値の表示	show logging	<p>システム ログ メッセージ バッファの内容と現在のロギング設定をリストで表示します。</p> <p> (注) システム ログ メッセージ バッファの内容を表示できるようにするには、まずバッファ出力先を設定する必要があります。</p> <p>詳細については、P.1-8 の「ロギング バッファの設定および管理」を参照してください。</p>

■ 基本ロギングコマンド

重大度の変更またはメッセージのディセーブル化

次のコマンドは、個々のメッセージの重大度を変更するため、および個々のメッセージをディセーブルにするために使用します。重大度の表は、P.1-22の「重大度」を参照してください。

目的	コマンドの構文	説明
メッセージの重大度の変更	<code>logging message message_number level severity_level</code>	特定のシステム ログ メッセージの重大度を設定します。
	<code>no logging message message_number level severity_level</code>	
	<code>show logging message</code>	デフォルトの設定が修正されたシステム ログ メッセージ (異なる重大度が割り当てられたメッセージおよびディセーブルにされたメッセージ) のリストを表示します。
	<code>clear config logging level</code>	すべてのロギング重大度の変更をデフォルトにリセットします。
メッセージのディセーブル化	<code>no logging message message_number</code>	特定のシステム ログ メッセージをディセーブルにします。
	<code>logging message message_number</code>	ディセーブル状態のメッセージのロギングを再開します。
	<code>show logging message</code>	デフォルトの設定が修正されたシステム ログ メッセージ (異なる重大度が割り当てられたメッセージおよびディセーブルにされたメッセージ) のリストを表示します。
	<code>clear config logging disabled</code>	以前にディセーブルにされたメッセージすべてのロギングを再度イネーブルにします。

コンフィギュレーション設定値のデフォルト値への復元

次のコマンドは、すべての設定オプションをそれぞれのデフォルト値にリセットするために使用します。

目的	コマンドの構文	説明
ロギング コンフィギュレーション設定値のデフォルト値への復元	<code>clear configure logging</code>	すべてのロギング コンフィギュレーション設定値をそれぞれのデフォルト値に戻します。このコマンドは、すべてのコンフィギュレーション設定値、たとえば、メッセージ重大度の変更、ディセーブル状態のメッセージ、バッファラップ オプション、およびフラッシュ オプションに影響を与えます。

システム ログ メッセージ出力先の指定および管理

セキュリティ アプライアンスは、システム ログ メッセージをさまざまな出力先に送信するように設定できます。また、個々のシステム ログ メッセージまたはメッセージ グループを指定して、送信するシステム ログ メッセージとその出力先を限定することもできます。

出力先には、次のものがあります。

- 内部バッファ
- 1 つまたは複数の syslog サーバ
- 1 つまたは複数の電子メール宛先
- ASDM (Adaptive Security Device Manager)
- Telnet および SSH セッション
- コンソール
- SNMP 管理ステーション

ここでは、次の項目について説明します。

- [出力先を設定および管理するコマンド \(P.1-5\)](#)
- [ロギング キューの設定および管理 \(P.1-8\)](#)
- [ロギング バッファの設定および管理 \(P.1-8\)](#)
- [メッセージのグループの管理 \(P.1-10\)](#)

出力先を設定および管理するコマンド

次のコマンドは、セキュリティ アプライアンスが送信するシステム ログ メッセージの出力先を指定するために使用します。

表 1-1 ログ出力先を設定するコマンド

出力先	コマンドの構文	説明
内部バッファ	<code>logging buffered message_list severity_level</code> <code>no logging buffered message_list severity_level</code>	システム ログ メッセージを内部バッファに保存します。バッファに送信するメッセージは、 <code>message_list</code> 変数および <code>severity_level</code> 変数で限定できます。 <code>show logging</code> コマンドを使用してバッファの内容を表示します。 内部バッファを設定および管理するときに使用するコマンドの詳細については、 P.1-8の「ロギング バッファの設定および管理」 を参照してください。

表 1-1 ログ出力先を設定するコマンド (続き)

出力先	コマンドの構文	説明
システム ログ メッセージ サーバ	logging host <i>interface_name ip_address</i> [tcp [/port] udp [/port]] [format emblem]	システム ログ メッセージを受信するホストを指定します (syslog サーバ)。セキュリティ アプライアンスは、UDP または TCP でメッセージを送信します。デフォルトのプロトコルおよびポートは UDP/514 です。デフォルト TCP ポート (指定されている場合) は 1468 です。 format emblem オプションによって EMBLEM フォーマット設定がイネーブルにされます (UDP のみ)。
	no logging host <i>interface_name ip_address</i> [tcp [/port] udp [/port]] [format emblem]	
	logging trap <i>message_list/severity_level</i> no logging trap <i>message_list/severity_level</i>	
電子メール アドレス	logging facility <i>number</i> no logging facility <i>number</i>	syslog サーバのロギング ファシリティを設定します。デフォルトは 20 です。
	logging mail <i>message_list/severity_level</i> no logging mail <i>message_list/severity_level</i>	システム ログ メッセージを 1 つまたは複数の電子メール受信側に送信することを指定します。送信するシステム ログ メッセージを指定するには、 <i>message_list</i> 変数または <i>severity_level</i> 変数を使用します。
	logging recipient-address no logging recipient-address	システム ログ メッセージを電子メール宛先に送信する場合に使用する受信側電子メール アドレスを指定します。最大 5 つの受信側アドレスが設定できます。受信側はそれぞれ新規コマンド エントリで指定します。
コンソール	logging from-address no logging from-address	システム ログ メッセージを電子メール宛先に送信する場合に使用する送信元電子メール アドレス。
	logging console <i>message_list / severity_level</i> no logging console <i>message_list / severity_level</i>	システム ログ メッセージが、発生したときにセキュリティ アプライアンス コンソール (tty) に表示されるようにします。 <i>severity_level</i> を 1 から 7 に設定するか、または重大度名を使用します。 <i>message_list</i> 変数で送信されるメッセージを指定することもできます。 このコマンドは、問題をデバッグしている場合、またはネットワークの負荷が最小の場合に使用します。パフォーマンスを低下させることがあるので、ネットワークの使用率が高いときは使用しないでください。

表 1-1 ログ出力先を設定するコマンド (続き)

出力先	コマンドの構文	説明
コンソールへの Telnet または SSH セッション	<code>logging monitor message_list severity_level</code> <code>no logging monitor message_list severity_level</code>	Telnet または SSH でセキュリティ アプライアンスコンソールにアクセスしているときに、システム ログメッセージが発生した場合、そのメッセージが表示されるようにします。 <i>severity_level</i> を 1 から 7 に設定するか、または重大度名を指定します。詳細については、表 1-6 を参照してください。 <i>message_list</i> 変数で送信されるメッセージを指定することもできます。 Telnet または SSH セッションを使用してメッセージを表示するには、Telnet または SSH セッションを確立し、 <code>logging monitor</code> コマンドを入力し、次に <code>terminal monitor</code> コマンドを入力します。
ASDM/ASDM	<code>logging asdm message_list/severity_level</code> <code>no logging asdm message_list/severity_level</code>	指定されたメッセージを ASDM に送信します。
	<code>show logging asdm</code>	ASDM システム ログ メッセージ バッファの内容を表示します。
	<code>logging asdm-buffer-size num_of_messages</code> <code>no logging asdm-buffer-size num_of_messages</code>	ASDM システム ログ メッセージ バッファに保存されるメッセージ数を指定します。その後メッセージは ASDM に送信されます。 このコマンドの <code>no</code> 形式を使用すると、バッファサイズがデフォルト値の 100 にリセットされます。
	<code>clear logging asdm</code>	ASDM システム ログ メッセージ バッファをクリアします。
SNMP 管理セッション	<code>logging history message_list/severity_level</code> <code>no logging history message_list/severity_level</code>	SNMP のシステム ログ メッセージをイネーブルにします。 <i>severity_level</i> を 1 から 7 に設定するか、または重大度名を設定します。詳細については、表 1-6 を参照してください。 <i>message_list</i> 変数で送信されるメッセージを指定することもできます。詳細については、 <code>logging list</code> コマンドを参照してください。 次のコマンドを使用して、セキュリティ アプライアンスに SNMP をセットアップします。 <code>snmp-server host [if_name] ip_addr</code> <code>snmp-server location text</code> <code>snmp-server contact text</code> <code>snmp-server community key</code> <code>snmp-server enable traps</code> SNMP コマンドの使用方法の詳細については、『Cisco Security Appliance Command Reference』を参照してください。

ログギング キューの設定および管理

セキュリティ アプライアンスではメモリに一定数のブロックが設けられており、システム ログ メッセージのバッファ用に割り当てることができます。必要なブロック数は、メッセージ キューの長さ、および指定された syslog ホスト数によって決まります。

次のコマンドは、処理を待機する間に、ログギング キューに保存できるメッセージ数を変更するために使用します。

目的	コマンドの構文	説明
ログギング キューのサイズの変更	<code>logging queue msg_count</code> <code>no logging queue msg_count</code>	処理を待機する間に、メッセージ キューに保持できるシステム ログ メッセージ数を指定します。デフォルトのメッセージ数は512です。メッセージ数を制限しないと指定するには、0（ゼロ）を設定します。
キュー統計情報の表示	<code>show logging queue</code>	次のコマンドは、キュー統計情報を表示するために使用します。

ログギング バッファの設定および管理

ログギング メッセージをセキュリティ アプライアンスで内部に保存するには、出力先として内部バッファを指定する必要があります。

セキュリティ アプライアンスに次の設定を行うには、次のコマンドを使用します。

- syslog を内部でバッファに保存。
- バッファのサイズを指定。
- 内部バッファがラップするとき（つまり、バッファがいっぱいするとき）、セキュリティ アプライアンスが内部バッファの内容を処理する方法の指定。内部バッファの内容は、フラッシュまたはFTPサーバに保存できます。

表 1-2 ログギング バッファを設定するコマンド

目的	コマンドの構文	説明
システム ログ メッセージのバッファへの保存を指定	<code>logging buffered message_list severity_level</code> <code>no logging buffered message_list severity_level</code>	システム ログ メッセージを内部バッファに保存します。 特定タイプのメッセージのみを内部バッファに保存する場合は、 <code>message_list</code> オプションまたは <code>severity_level</code> オプションを使用します。
ログギング バッファの内容の消去	<code>clear logging buffer</code>	バッファの内容を消去します。

表 1-2 ロギング バッファを設定するコマンド (続き)

目的	コマンドの構文	説明
使用するフラッシュ量の指定	<pre>logging flash-minimum-free <i>kbytes</i> no logging flash-minimum-free <i>kbytes</i> logging flash- maximum-allocation <i>kbytes</i> no logging flash- maximum-allocation <i>kbytes</i></pre>	<p>システム ログ メッセージを保存するためにロギング コマンドで使用できるフラッシュ量を指定します。このコマンドは、<code>logging flash-bufferwrap</code> コマンドおよび <code>logging-savelog</code> コマンドに適用されます。</p> <p><code>flash-minimum-free</code> オプションは、常に利用できるように空けておく最小フラッシュ領域量を指定する (KB 単位) ために使用します。</p> <p><code>flash-maximum-allocation</code> オプションは、システム ログ メッセージの保存に使用できる最大フラッシュ領域量を指定する (KB 単位) ために使用します。</p> <p> (注) <code>logging flash</code> に関連するコマンドは、単一モードの場合のみ有効です。</p>
バッファ ラップをフラッシュに保存	<pre>logging flash-bufferwrap no logging flash-bufferwrap</pre>	<p>イネーブル状態の場合、バッファ ラップ (つまり、バッファがいっぱい) のとき、バッファの内容がフラッシュに保存されます。</p>
現行バッファ内容のフラッシュへの保存	<pre>logging savelog <i>filename</i></pre>	<p>システム ログ メッセージ バッファの内容を、指定されたファイル名のファイルで、フラッシュに保存します。</p> <p>ファイル名が指定されていない場合、デフォルトのタイムスタンプ形式がファイル名に使用されます。</p> <p>このコマンドは、特権 EXEC モード コマンドです。</p>
バッファ ラップの FTP サーバへの送信	<pre>logging ftp-bufferwrap no logging ftp-bufferwrap logging ftp-server <i>ftp_server path username password</i> no logging ftp-server <i>ftp_server path username password</i></pre>	<p>メッセージ バッファがいっぱいの場合、バッファの内容が設定された FTP サーバに送信されます。</p> <p><code>logging ftp-server</code> コマンドで FTP サーバを設定します。</p> <p>FTP サーバを設定します。FTP サーバについての必要な情報を指定するには、次に示すオプションを使用します。</p> <ul style="list-style-type: none"> <code>ftp-server</code> : 外部 FTP サーバ名または IP アドレス。 <code>path</code> : システム ログ メッセージを保存する FTP サーバ上のディレクトリパス。 <code>username</code> : FTP サーバへのユーザ ログイン。 <code>password</code> : <code>username</code> のパスワード。

メッセージのグループの管理

セキュリティ アプライアンスには、システム ログ メッセージをグループとして設定および管理できるようにするメカニズムがいくつか用意されています。このメカニズムには、メッセージ重大度、メッセージクラス（メッセージソース）、または作成するカスタム メッセージが含まれます。このメカニズムを使用すると、1つのコマンドを入力して、小規模メッセージグループにも大規模メッセージグループにも適用することが入力できます。

次にメッセージグループの管理の例をいくつか示します。

- 重大度 1、2、および 3 のメッセージすべてを内部バッファにロギングする。
- 「ha」クラスのメッセージすべてを特定の syslog サーバに送信する。
- 「high-priority」という名前のメッセージ リストを作成し、そのリストにあるメッセージを電子メール アドレスに送信して、システム管理者に問題を通知する。

logging class コマンドを使用すると、あるカテゴリのシステム メッセージ全体の出力先を 1つのコマンドで指定できます。クラスは、セキュリティ アプライアンスの機能エリアに関連付けられているメッセージのカテゴリです。たとえば、「vpnc」クラスはVPN クライアントを示します。

1つのコマンドを入力して、関連する機能エリアに関連付けられているメッセージすべてにそのコマンドを適用する場合は、*message_class* 変数を使用します。

メッセージ ID 番号は、メッセージ番号の最初の 3 桁で参照されます。たとえば、611 には番号 611101 から 611323 までのシステム メッセージすべてが含まれます。このメッセージのグループは、vpnc（VPN クライアント）クラスに関連付けられています。

次のコマンドは、メッセージ リストを作成するため、および複数のメッセージグループを 1つの出力先に送信するために使用します。

表 1-3 メッセージのグループを管理するコマンド

コマンド/オプション	構文	説明
logging list	logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>] no logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>]	カスタムのメッセージ リストを作成します。 <i>message_list</i> は、作成するリストを識別するために選定する名前です。  (注) メッセージ リストの名前に重大度の名前を使用しないでください。 <i>message_list</i> 名には、「emergencies」、「alert」、「critical」、「error」、「warning」、「notification」、「informational」、および「debugging」は使用できません。 これらの単語は、最初の 3 文字でも、ファイル名の先頭には使用しないでください。たとえば、「err」で始まるファイル名は使用しないでください。
	logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>] no logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>]	この構文オプションは、指定された重大度を持つ特定のクラス内のメッセージすべてを含むメッセージ リストを作成するために使用します。
	logging list <i>message_list</i> message <i>syslog_id</i> - [<i>syslog_id2</i>] no logging list <i>message_list</i> message <i>syslog_id</i> - [<i>syslog_id2</i>]	この構文オプションは、ある範囲のメッセージ ID 番号を含むメッセージ リストを作成するために使用します。

表 1-3 メッセージのグループを管理するコマンド (続き)

コマンド/オプション	構文	説明
ロギング クラス	<pre>logging class message_class buffered console history mail monitor trap severity_level no logging class message_class buffered console history mail monitor trap severity_level</pre>	そのクラスに関連するメッセージすべてを指定された出力先に送信します。出力先に送信するメッセージ数をさらに限定するには、重大度しきい値を指定します。

メッセージ クラス変数の値

表 1-4 に、メッセージ クラスと各クラスのメッセージ ID 範囲をリストで示しています。

表 1-4 メッセージ クラスと関連メッセージ ID 番号

クラス	定義	メッセージ ID 番号
ha	フェールオーバー (ハイ アベイラビリティ)	101, 102, 103, 104, 210, 311, 709
rip	RIP ルーティング	107, 312
auth	ユーザ認証	109, 113
bridge	透過ファイアウォール	110, 220
config	コマンド インターフェイス	111, 112, 208, 308
sys	システム	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711
session	ユーザ セッション	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
ip	IP スタック	209, 215, 313, 317, 408
snmp	SNMP	212
vpdn	PPTP および L2TP セッション	213, 403, 603
vpn	IKE および IPSec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
ospf	OSPF ルーティング	318, 409, 503, 613
np	ネットワーク プロセッサ	319
rm	リソース マネージャ	321
ids	侵入検知システム	400, 401, 415
vpnc	VPN クライアント	611
webvpn	Web ベース VPN	716
ca	PKI 認証局	717
e-mail	電子メール プロキシ	719
vpnlb	VPN ロード バランシング	718
vpnfo	VPN フェールオーバー	720

システム ログ メッセージの内容および形式の修正

次のコマンドは、次の処理を行うようにセキュリティ アプライアンスを設定するために使用します。

- すべてのシステム ログ メッセージにデバイス ID を含める。
- すべてのシステム ログ メッセージにタイムスタンプを含める。
- システム ログ メッセージに EMBLEM フォーマットを使用する。

表 1-5 メッセージの内容および形式を修正するコマンド

目的	コマンドの構文	説明
システム ログ メッセージにデバイス ID を含める	<pre>logging device-id {hostname ipaddress if_name string text} no logging device-id {hostname ipaddress if_name string text}</pre>	<p>イネーブル状態の場合、セキュリティ アプライアンスは、EMBLEM フォーマットでないシステム ログ メッセージすべてにデバイス ID を表示します。</p> <p><code>ipaddress</code> オプションを使用すると、デバイス ID は、メッセージが送信されたインターフェイスに関係なく、指定したセキュリティ アプライアンスインターフェイスの IP アドレスとなります。このオプションの使用により、そのデバイスから送信されるメッセージすべてに、1 つの同じデバイス ID が割り当てられます。</p> <p> (注) イネーブル状態の場合、デバイス ID は EMBLEM フォーマットのメッセージまたは SNMP トラップには表示されません。</p>
システム ログ メッセージにタイムスタンプを含める	<pre>logging timestamp no logging timestamp</pre>	<p>イネーブル状態の場合、セキュリティ アプライアンスはすべてのシステム ログ メッセージにタイムスタンプを表示します。</p>
EMBLEM フォーマットを使用するようにシステム ログ メッセージを修正	<pre>logging emblem no logging emblem</pre>	<p>イネーブル状態の場合、システム ログ メッセージが EMBLEM フォーマットで表示されます。</p> <p> (注) このコマンドは、syslog ホストに送信されるシステム ログ メッセージには影響しません。ホストに送信されるシステム ログ メッセージに EMBLEM フォーマットを使用するには、<code>logging host</code> コマンドを使用します。</p>

ロギング コマンド例

ここでは、`logging` コマンドの使用方法を示す例をステップごとに説明します。ここでは、次の項目について説明します。

- [ロギングのイネーブル化 \(P.1-13\)](#)
- [ロギング出力のテスト \(P.1-14\)](#)
- [システム ログ メッセージのバッファへの送信 \(P.1-15\)](#)
- [システム ログ メッセージの Syslog サーバへの送信 \(P.1-16\)](#)
- [システム ログ メッセージの電子メール アドレスへの送信 \(P.1-17\)](#)
- [システム ログ メッセージの Telnet コンソール セッションへの送信 \(P.1-18\)](#)
- [システム ログ メッセージの SNMP 管理ステーションへの送信 \(P.1-20\)](#)
- [特定のシステム ログ メッセージのディセーブル化 \(P.1-21\)](#)
- [ディセーブル状態のシステム ログ メッセージのリストの表示 \(P.1-21\)](#)
- [ディセーブル状態の特定システム ログ メッセージの再イネーブル化 \(P.1-21\)](#)
- [ディセーブル状態のシステム ログ メッセージすべての再イネーブル化 \(P.1-21\)](#)

ロギングのイネーブル化

次の手順ではロギングをイネーブルにしますが、ログ メッセージを表示するには出力先も指定する必要があります。詳細については、[P.1-15](#) の「[システム ログ メッセージの出力先の設定](#)」を参照してください。

ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1 コンフィギュレーション モードを表示するには、次のコマンドを入力します。

```
enable
(Enter your password at the prompt)
configure terminal
```

ステップ 2 ロギングをイネーブルにするには、次のコマンドを入力します。

```
logging enable
```

ステップ 3 ロギング レベルを変更するには、次のコマンドを入力します。

```
logging output_destination severity_level (1-7)
```

有効な `output_destination` 値は、`asdm`、`console`、`buffered`、`history`、`mail`、`monitor`、および `trap` です。

ステップ 4 ロギング設定を表示するには、次のコマンドを入力します。

```
show all
```

ロギング出力のテスト

ステップ1 コンフィギュレーション モードを表示するには、次のコマンドを入力します。

```
enable  
(Enter your password at the prompt)  
configure terminal
```

ステップ2 コンソールへのログ メッセージの送信を開始するには、次のコマンドを入力します。

```
logging console 7  
quit
```

このテストでは、次のシステム ログ メッセージが生成されます。

```
111005: End configuration: OK
```

このメッセージは、コンフィギュレーション モードを終了したことを示しています。「111005」はメッセージ ID 番号です（このメッセージの詳細については、[第2章「システム ログ メッセージ」](#)を参照してください）。

ステップ3 コンソールへのロギングをディセーブルにするには、次のコマンドを入力します。

```
configure terminal  
no logging console 7  
quit
```



(注)

テストには、`logging console` コマンドのみを使用してください。進行中のシステム ログ メッセージの出力先にコンソールを使用すると、システム パフォーマンスが低下することがあります。セキュリティ アプライアンスが実際の動作環境にある場合、メッセージの保存には `logging buffered` コマンド、メッセージの表示には `show logging` コマンド、`logging buffered` コマンドで表示されたメッセージの消去には `clear logging buffer` コマンドのみを使用してください。

システム ログ メッセージの出力先の設定

ここでは、システム ログ メッセージを任意の出力先に送信するようにセキュリティ アプライアンスを設定する方法について説明します。セキュリティ アプライアンスには、次のように、システム ログ メッセージを送信する出力先がいくつか用意されています。

- 内部バッファ
- 1 つまたは複数の syslog サーバ
- 1 つまたは複数の電子メール アドレス
- ASDM (Monitoring タブを使用)
- SNMP 管理ステーション
- Telnet および SSH セッション
- tty コンソール

ここでは、次の項目について説明します。

- システム ログ メッセージのバッファへの送信 (P.1-15)
- システム ログ メッセージの Syslog サーバへの送信 (P.1-16)
- システム ログ メッセージの電子メール アドレスへの送信 (P.1-17)
- システム ログ メッセージの Telnet コンソール セッションへの送信 (P.1-18)
- システム ログ メッセージの Telnet コンソール セッションへの送信 (P.1-18)
- SNMP 要求の受信 (P.1-20)
- SNMP トラップの送信 (P.1-20)

システム ログ メッセージのバッファへの送信

システム ログ メッセージをバッファに送信するには、次の手順を実行します。次の例では、バッファに送信する複数のメッセージを指定するプロセスを簡単にするために、まずメッセージ リストを作成します。

- ステップ 1** 指定の重大度を持つメッセージまたはメッセージ クラスを含むメッセージ リストを作成するには、次のコマンドを入力します。

```
logging list message_list | level severity_level [class message_class]
```

ここで、*message_list* は作成するファイルの名前、*severity_level* はリストに含めるメッセージの重大度、*message_class* はリストに含めるメッセージのカテゴリです。

次に例を示します。

```
logging list my_critical_messages level 2
```



(注) メッセージ リストのファイル名に重大度の名前を使用しないでください。

ステップ2 作成したメッセージ リストにメッセージを追加するには、次のコマンドを入力します。

```
logging list message_list message syslog_id-syslog_id2
```

ここで、*message_list* は、修正するメッセージのリストが格納されているファイル名で、*syslog_id-syslog_id2* はリストに追加するメッセージ ID 番号の範囲です。

次に例を示します。

```
logging list my_critical_messages message 101001-102034
```

ステップ3 作成したメッセージ リスト内のメッセージをバッファに送信するように指定するには、次のコマンドを入力します。

```
logging buffered message_list
```

ここで、*message_list* は、バッファに送信するメッセージのリストが格納されているファイル名です。

次に例を示します。

```
logging buffered my_critical_messages
```

システム ログ メッセージの Syslog サーバへの送信

メッセージをホストに送信する場合、メッセージは UDP か TCP を使用して送信されます。ホストでは、*syslogd* と呼ばれるプログラム（サーバと呼ばれる）が動作している必要があります。UNIX には、オペレーティング システムの一部として *syslog* サーバが用意されています。Windows 95 または Windows 98 の場合は、別のベンダーから *syslog* サーバを入手してください。

syslogd の設定手順については、『*Cisco Security Appliance Configuration Guide*』を参照してください。ログgings サーバに、特定のタイプのメッセージが記録された場合に実行するアクションを指定できます。たとえば、電子メールの送信、ログ ファイルへのレコードの保存、またはワークステーションでのメッセージの表示です。

syslog サーバにメッセージを送信するようにセキュリティ アプライアンスを設定するには、次の手順を実行します。

ステップ1 メッセージを受信するホストを指定するには、次のコマンドを入力します。

```
logging host if_name ip_address [tcp[/port] | udp[/port]] [format emblem]
```

ここで、*if_name* はホストのインターフェイスの名前、*ip_address* はホストの IP アドレス、*port* はメッセージを送信する TCP または UDP のポート番号です。

次に例を示します。

```
logging host dmz1 192.168.1.5
```

複数のホストを指定できますが、ホストごとに別のコマンドを入力する必要があります。

ステップ2 ロギング レベルを設定するには、次のコマンドを入力します。

```
logging trap severity_level (1-7)
```

ここで、*severity_level* は送信するメッセージの重大度です。

debugging (7) レベルを使用するのは、初期セットアップ時とテスト時だけにしてください。セットアップまたはテストの終了後は、レベルを **debugging** から **errors** (3) に変更して、実際の動作環境に移行してください。

ステップ3 各メッセージにデバイス ID を含める場合は、次のコマンドを入力します。

```
logging device-id {hostname | ipaddress if_name | string text}
```

メッセージには、syslog サーバに送信されたメッセージに指定されたデバイス ID（指定されたインターフェイスのホスト名および IP アドレスまたは文字列のいずれか）が含まれています。

ステップ4 必要に応じて、ロギング ファシリティにデフォルトの 20 以外の値を設定します。UNIX システムのほとんどは、ファシリティ 20 でメッセージが到着することを期待します。ロギング ファシリティを設定するには、次のコマンドを入力します。

```
logging facility number
```

システム ログ メッセージの電子メール アドレスへの送信

システム ログ メッセージを電子メール アドレスに送信するには、次の手順を実行します。

ステップ1 1 つまたは複数の電子メール アドレスに送信するメッセージを指定します。メッセージ重大度変数またはメッセージ リスト変数を使用して、送信するメッセージを指定します。

この例では、前に **logging list** コマンドでセットアップした「high-priority」という名前を *message_list* に使用します。

送信するメッセージを指定するには、次のコマンドを入力します。

```
logging mail message_list|severity_level level
```

次に例を示します。

```
logging mail high-priority
```

ステップ2 システム ログ メッセージを電子メール アドレスに送信する場合に使用する送信元電子メール アドレスを指定するには、次のコマンドを入力します。

```
logging from-address email_address
```

次に例を示します。

```
logging from-address xxx-001@example.com
```

■ ログギング コマンド例

ステップ 3 システム ログ メッセージを電子メール宛先に送信する場合に使用する受信側電子メール アドレスを指定します。最大 5 つの受信側アドレスが設定できます。各受信側は別々に入力する必要があります。

受信側アドレスを指定するには、次のコマンドを入力します。

```
logging recipient-address e-mail_address [level severity_level]
```

次に例を示します。

```
logging recipient-address admin@example.com
```



(注) 重大度が指定されていない場合、デフォルトの重大度が使用されます (エラー状態、重大度 3)。

ステップ 4 システム ログ メッセージを電子メール宛先に送信する場合に使用する SMTP サーバを指定するには、次のコマンドを入力します。

```
smtp-server hostname
```

次に例を示します。

```
smtp-server smtp-host-1
```

システム ログ メッセージの Telnet コンソール セッションへの送信

Telnet コンソール セッションでシステム ログ メッセージを表示するには、次の手順を実行します。

ステップ 1 まだ設定していない場合は、内部インターフェイスのホストがセキュリティ アプライアンスにアクセスできるように、セキュリティ アプライアンスを設定します。

a. 次のコマンドを入力します。

```
telnet ip_address [subnet_mask] [if_name]
```

たとえば、ホストの IP アドレスが 192.168.1.2 の場合、コマンドは次のとおりです。

```
telnet 192.168.1.2 255.255.255.255
```

b. セキュリティ アプライアンスがセッションを切断するまでの Telnet セッションのアイドル状態の許容時間を、デフォルトの 5 分より長い値に設定する必要もあります。適切な値は、短くても 15 分です。Telnet セッションのこの時間を設定するには、次のコマンドを入力します。

```
telnet timeout 15
```

ステップ 2 ホストで Telnet を開始して、セキュリティ アプライアンスの内部インターフェイスを指定します。

Telnet で接続ができると、セキュリティ アプライアンスによって `passwd:` というプロンプトが表示されます。

ステップ 3 Telnet パスワードを入力します。デフォルトは `cisco` です。

ステップ4 コンフィギュレーション モードを表示するには、次のコマンドを入力します。

```
enable  
(Enter your password at the prompt)  
configure terminal
```

ステップ5 メッセージ ロギングを開始するには、次のコマンドを入力します。

```
logging monitor severity_level (1-7)
```

ステップ6 この Telnet セッションにログを送信するには、次のコマンドを入力します。

```
terminal monitor
```

このコマンドでは、現在の Telnet セッションに対してのみロギングがイネーブルにされます。**logging monitor** コマンドでは、すべての Telnet セッションに対してロギング プリファレンスが設定され、一方 **terminal monitor**（および **terminal no monitor**）コマンドでは、個々の Telnet セッションそれぞれに対してのロギングが制御されます。

ステップ7 ホストを ping するかまたは Web ブラウザを開始して、いくつかのメッセージを起動します。システム ログメッセージが Telnet セッション ウィンドウに表示されます。

ステップ8 完了した場合、この機能を次のコマンドでディセーブルにします。

```
terminal no monitor  
no logging monitor
```

システム ログ メッセージの SNMP 管理ステーションへの送信

ここでは、システム ログ メッセージを SNMP 管理ステーションに送信するようにセキュリティ アプライアンスを設定する方法について説明します。次の項目について説明します。

- [SNMP 要求の受信 \(P.1-20\)](#)
- [SNMP トラップの送信 \(P.1-20\)](#)

SNMP 要求の受信

SNMP 管理ステーションから要求を受信するようにセキュリティ アプライアンスを設定するには、次の手順を実行します。

ステップ 1 SNMP 管理ステーションの IP アドレスを設定するには、次のコマンドを入力します。

```
snmp-server host [if_name] ip_addr
```

ステップ 2 必要に応じて、次のコマンドでその他の snmp サーバ設定を指定します。

```
snmp-server location text
snmp-server contact text
snmp-server community key
```

詳細については、『Cisco Security Appliance Command Line Configuration Guide』を参照してください。

SNMP トラップの送信

セキュリティ アプライアンスから SNMP 管理ステーションにログ メッセージをトラップとして送信するには、次の手順を実行します。コールド スタート、リンク アップ、およびリンク ダウンの総称トラップは、すでに「[SNMP 要求の受信](#)」手順によってイネーブルにされています。

ステップ 1 SNMP トラップをイネーブルにするには、次のコマンドを入力します。

```
snmp-server enable traps
```

ステップ 2 ログgings レベルを設定するには、次のコマンドを入力します。

```
logging history severity_level (1-7)
```

debugging (7) レベルを使用するのは、初期セットアップ時とテスト時だけにしてください。セットアップまたはテストの終了後は、レベルを **debugging** からそれより低い値に変更して、実際の動作環境に移行してください。

ステップ 3 システム ログ メッセージのトラップの送信をディセーブルにするには、次のコマンドを入力します。

```
no snmp-server enable traps
```

特定のシステム ログ メッセージのディセーブル化およびイネーブル化

ここでは、システム ログ メッセージのディセーブル化および再イネーブル化の方法、およびディセーブル状態のシステム ログ メッセージの表示方法について説明します。ここでは、次の項目について説明します。

- [特定のシステム ログ メッセージのディセーブル化 \(P.1-21\)](#)
- [ディセーブル状態のシステム ログ メッセージのリストの表示 \(P.1-21\)](#)
- [ディセーブル状態の特定システム ログ メッセージの再イネーブル化 \(P.1-21\)](#)
- [ディセーブル状態のシステム ログ メッセージすべての再イネーブル化 \(P.1-21\)](#)

特定のシステム ログ メッセージのディセーブル化

特定のシステム ログ メッセージをディセーブルにするには、次のコマンドを入力します。

```
no logging message message_number
```

ここで、*message_number* はディセーブルにする特定のメッセージです。

ディセーブル状態のシステム ログ メッセージのリストの表示

ディセーブル状態のシステム ログ メッセージのリストを表示するには、次のコマンドを入力します。

```
show logging message
```

ディセーブル状態の特定システム ログ メッセージの再イネーブル化

ディセーブル状態のシステム ログ メッセージを再度イネーブルにするには、次のコマンドを入力します。

```
logging message message_number
```

ここで、*message_number* は再イネーブル化する特定のメッセージです。

ディセーブル状態のシステム ログ メッセージすべての再イネーブル化

ディセーブル状態のシステム ログ メッセージをすべて再イネーブル化するには、次のコマンドを入力します。

```
clear config logging disabled
```

ログメッセージの概要

ここでは、セキュリティ アプライアンスのシステム ログ メッセージの内容を説明します。ここでは、次の項目について説明します。

- [ログメッセージの形式 \(P.1-22\)](#)
- [重大度 \(P.1-22\)](#)
- [変数 \(P.1-23\)](#)

ログメッセージの形式

システム ログ メッセージは、パーセント記号 (%) で始まり、次のような構造になっています。

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

次の説明を参照してください。

PIX ASA	セキュリティ アプライアンスによって生成されたメッセージのメッセージ ファシリティ コードを識別します。この値は常に PIX ASA です。
Level	1 ~ 7。レベルは、メッセージに記述された状態の重大度が反映されます。数値が小さいほど、重大度が高くなります。詳細については、 表 1-6 を参照してください。
Message_number	メッセージを識別する固有の 6 桁の番号。
Message_text	状態を記述するテキスト文字列。メッセージのこの部分には、IP アドレス、ポート番号、またはユーザ名が含まれることがあります。 表 1-7 に、変数フィールドとその情報のタイプをリストで示しています。



(注)

セキュリティ アプライアンス シリアル コンソールで受信するシステム ログ メッセージには、メッセージのコード部分のみが含まれています。[第 2 章「システム ログ メッセージ」](#)のメッセージの説明には、重大度も記載されています。

重大度

[表 1-6](#) に重大度をリストで示しています。

表 1-6 ログメッセージの重大度

レベル番号	レベル キーワード	説明
0	emergencies	システムが使用不能。
1	alert	ただちに処置が必要。
2	critical	クリティカルな状態。
3	error	エラー状態。
4	warning	警告状態。
5	notification	正常だが、注意が必要な状態。
6	informational	情報メッセージのみ。
7	debugging	デバッグ中にのみ表示される。

付録 A「重大度別メッセージ リスト」に、各重大度で発生するメッセージをリストで示しています。



(注)

セキュリティ アプライアンスでは、重大度が 0 (emergencies) のメッセージは生成されません。このレベルは、UNIX システム ログ メッセージ機能との互換性のために、**logging** コマンドで指定できますが、セキュリティ アプライアンスでは使用されません。

変数

ログ メッセージには変数が含まれていることがよくあります。表 1-7 に、ログ メッセージの説明のためにこのマニュアルで使用されている変数のほとんどをリストで示しています。1 つのログ メッセージにしか現れない変数の中には省略したものがあります。

表 1-7 システム ログ メッセージ内の変数フィールド

変数	情報のタイプ
<i>acl_ID</i>	ACL 名。
<i>bytes</i>	バイト数。
<i>code</i>	メッセージで返される 10 進数で、メッセージに応じて、エラーの原因または発生源を示します。
<i>command</i>	コマンド名。
<i>command_modifier</i>	<i>command_modifier</i> は、次の文字列のいずれかです。 <ul style="list-style-type: none"> • cmd (この文字列は、コマンドに修飾子がないことを意味します)。 • clear • なし • show
<i>connections</i>	接続数。
<i>connection_type</i>	接続タイプは次のとおりです。 <ul style="list-style-type: none"> • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • Via UDP • Route • RTP • RTCP
<i>dec</i>	10 進数。
<i>dest_address</i>	パケットの宛先アドレス。
<i>dest_port</i>	宛先ポート番号。
<i>device</i>	メモリ ストレージ デバイス。たとえば、フロッピーディスク、フラッシュメモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末です。
<i>econns</i>	初期接続数。
<i>elimit</i>	static コマンドまたは nat コマンドで指定された初期接続数。

表 1-7 システム ログ メッセージ内の変数フィールド (続き)

変数	情報のタイプ
<i>filename</i>	セキュリティ アプライアンス イメージ、PDM ファイル、またはコンフィギュレーションの各タイプのファイル名。
<i>ftp-server</i>	外部 FTP サーバ名または IP アドレス。
<i>gateway_address</i>	ネットワーク ゲートウェイ IP アドレス。
<i>global_address</i>	グローバル IP アドレス。低セキュリティ レベル インターフェイス上のアドレス。
<i>global_port</i>	グローバル ポート番号。
<i>hex</i>	16 進数。
<i>inside_address</i>	内部 (つまり、ローカル) IP アドレス。高セキュリティ レベル インターフェイス上のアドレス。
<i>inside_port</i>	内部ポート番号。
<i>interface_name</i>	インターフェイスの名前。
<i>IP_address</i>	<i>n.n.n.n</i> 形式の IP アドレス。 <i>n</i> は 1 から 255 までの整数です。
<i>MAC_address</i>	MAC アドレス。
<i>mapped_address</i>	変換済み IP アドレス。
<i>mapped_port</i>	変換済みポート番号。
<i>message_class</i>	セキュリティ アプライアンスの機能エリアに関連付けられたメッセージのカテゴリ。
<i>message_list</i>	メッセージ ID 番号、メッセージ クラス、またはメッセージ重大度のリストを含む作成ファイルの名前。
<i>message_number</i>	メッセージ ID 番号。
<i>nconns</i>	static テーブルまたは xlate テーブルに許可された接続数。
<i>netmask</i>	サブネット マスク。
<i>number</i>	数。正確な形式は、ログ メッセージによって決まります。
<i>octal</i>	8 進数。
<i>outside_address</i>	外側 (つまり、外部) IP アドレス。通常は、外部ルータの先のネットワークにある低セキュリティ レベル インターフェイス上のホストのアドレス。
<i>outside_port</i>	外部ポート番号。
<i>port</i>	TCP または UDP ポート番号。
<i>privilege_level</i>	ユーザ特権レベル。
<i>protocol</i>	パケットのプロトコル。たとえば、ICMP、TCP、または UDP。
<i>real_address</i>	Network Address Translation (NAT; ネットワーク アドレス変換) 前の実 IP アドレス。
<i>real_port</i>	NAT 前の実ポート番号。
<i>reason</i>	メッセージの理由を記述するテキスト文字列。
<i>service</i>	パケットで指定されたサービス。たとえば、SNMP または Telnet。
<i>severity_level</i>	メッセージの重大度。
<i>source_address</i>	パケットのソース アドレス。
<i>source_port</i>	ソース ポート番号。
<i>string</i>	テキスト文字列 (たとえば、ユーザ名)。

表 1-7 システム ログ メッセージ内の変数フィールド (続き)

変数	情報のタイプ
<i>tcp_flags</i>	TCP ヘッダー内のフラグ。たとえば、次に示すものです。 <ul style="list-style-type: none">• ACK• FIN• PSH• RST• SYN• URG
<i>time</i>	<i>hh:mm:ss</i> 形式の時間。
<i>url</i>	URL。
<i>user</i>	ユーザ名。

他のリモート管理ツールおよびモニタ ツール

この項で説明するセキュリティ アプライアンスのオプションは、コマンドライン以外のツールを使用して、リモートでセキュリティ アプライアンスをモニタするためのものです。ここでは、次の項目について説明します。

- [Cisco ASDM \(P.1-26 \)](#)
- [Cisco Secure Policy Manager \(P.1-26 \)](#)
- [SNMP トラップ \(P.1-26 \)](#)
- [Telnet \(P.1-26 \)](#)

Cisco ASDM

Cisco Adaptive Security Device Manager (ASDM) は、ブラウザ ベースの設定ツールで、セキュリティ アプライアンスをグラフィックスを使用してセット アップ、設定、およびモニタできるように設計されており、セキュリティ アプライアンス コマンドライン インターフェイス (CLI) の詳しい知識は必要ありません。

Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) はセキュリティ ポリシー管理システムで、これを使用すると中心部からネットワーク全体のセキュリティ ポリシーを定義、配布、適用、および監査できます。CSPM により、境界アクセス コントロール、NAT、IDS、および IPSec ベース VPN などの複雑なネットワーク セキュリティ イベントの管理タスクが合理化されます。CSPM には、モニタ、イベント通知、および Web ベース レポート機能などのシステム監査機能が用意されています。

CSPM は、セキュリティ アプライアンスからシステム ログ メッセージを受信して、電子メール、ポケットベル、およびスクリプトなどの通知を指定された syslog に送ることができます。また、CSPM には、上位 10 ユーザや上位 10 Web サイトなどの syslog レポートも提供します。このレポートは、オンデマンドとスケジュール処理の両方で作成できます。レポートは、電子メールで送信することも、SSL 対応 Web ブラウザを使ってリモートで表示することもできます。

詳細については、次の Web サイトを参照してください。

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

<http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/index.htm>

SNMP トラップ

セキュリティ アプライアンスのイベントは、SNMP を使用して報告できます。この機能を使用するには、Cisco SYSLOG MIB と Cisco SMI MIB を SNMP 管理ステーションにロードする必要があります。

Telnet

内部ホストから Telnet を使用して、セキュリティ アプライアンスにログインし、システムのステータスをモニタできます。IPSec がイネーブル状態の場合、外部ホストからコンソールにアクセスすることもできます。Telnet から `debug icmp trace` コマンドおよび `debug sqlnet` コマンドを使用して、ICMP (ping) トレースおよび SQL*Net アクセスを表示することができます。

Telnet コンソール セッションを使用すると、`logging monitor` コマンドおよび `terminal monitor` コマンドを使用してシステム ログ メッセージを表示することもできます([P.1-18](#) の「システム ログ メッセージの Telnet コンソール セッションへの送信」を参照)。



システム ログ メッセージ

この章では、Cisco ASA システム ログ メッセージについて説明します。メッセージは、メッセージコードの番号順に記載されています。



(注)

このマニュアルに示されているメッセージは、ソフトウェア Version 7.0 以降に適用されます。番号が連番から抜けている場合、そのメッセージはセキュリティ アプライアンス コードにはありません。

次の事項について説明します。

- [メッセージ 101001 ~ 199009 \(P.2-2\)](#)
- [メッセージ 201002 ~ 217001 \(P.2-48\)](#)
- [メッセージ 302003 ~ 326028 \(P.2-60\)](#)
- [メッセージ 400000 ~ 418001 \(P.2-91\)](#)
- [メッセージ 500001 ~ 507001 \(P.2-124\)](#)
- [メッセージ 602101 ~ 609002 \(P.2-130\)](#)
- [メッセージ 701001 ~ 720073 \(P.2-150\)](#)

メッセージ 101001 ~ 199009

この項では、101001 から 199009 までのメッセージについて説明します。

101001

エラー メッセージ %PIX|ASA-1-101001: (Primary) Failover cable OK.

説明 これはフェールオーバー メッセージです。このメッセージは、フェールオーバー ケーブルが接続され、正常に機能していることを報告します。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

101002

エラー メッセージ %PIX|ASA-1-101002: (Primary) Bad failover cable.

説明 これはフェールオーバー メッセージです。このメッセージは、フェールオーバー ケーブルが接続されているが、正常には機能していないことを報告します。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 フェールオーバー ケーブルを交換します。

101003, 101004

エラー メッセージ %PIX|ASA-1-101003: (Primary) Failover cable not connected (this unit).

エラー メッセージ %PIX|ASA-1-101004: (Primary) Failover cable not connected (other unit).

説明 この例は、両方ともフェールオーバー メッセージです。これらのメッセージは、フェールオーバー モードがイネーブルになっているが、フェールオーバー ケーブルがフェールオーバー ペアの一方の装置に接続されていない場合に記録されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 フェールオーバー ケーブルをフェールオーバー ペアの両方の装置に接続します。

101005

エラー メッセージ %PIX|ASA-1-101005: (Primary) Error reading failover cable status.

説明 これはフェールオーバー メッセージです。このメッセージは、フェールオーバー ケーブルが接続されているが、プライマリ装置が自分のステータスを判断できない場合に表示されます。

推奨処置 ケーブルを交換します。

102001

エラー メッセージ %PIX|ASA-1-102001: (Primary) Power failure/System reload other side.

説明 これはフェールオーバー メッセージです。このメッセージは、プライマリ装置が相手装置にシステム リロードまたは電源障害を検出すると記録されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 リロードが発生した装置で `show crashinfo` コマンドを発行して、リロードに関連するトレースバックがあるかどうかを判別します。さらに、装置の電源が投入され、ケーブルが正しく接続されていることを確認します。

103001

エラー メッセージ %PIX|ASA-1-103001: (Primary) No response from other firewall (reason code = code).

説明 これはフェールオーバー メッセージです。このメッセージは、プライマリ装置がフェールオーバー ケーブル経由でセカンダリ装置と通信できない場合に表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。表 2-1 に、フェールオーバーが発生した原因を判断するための原因コードおよび説明を示します。

表 2-1 原因コード

原因コード	説明
1	シリアル ケーブルでフェールオーバー hello が 30 秒以上受信されていません。これによって相手 Cisco ASA 装置でフェールオーバーが正常に動作していることが保証されます。
2	インターフェイスが 4 つのフェールオーバー テストの内のいずれか 1 つを通過させませんでした。4 つのテストは、1) Link Up、2) Monitor for Network Traffic、3) ARP テスト、4) Broadcast Ping テストです。
3	シリアル ケーブルでコマンドが送信された後 15 秒以上適切な ACK が受信されません。

推奨処置 フェールオーバー ケーブルが正しく接続され、両方の装置が同じハードウェア、ソフトウェア、およびコンフィギュレーションになっていることを確認します。同じでない場合は、Cisco TAC にお問い合わせください。

103002

エラー メッセージ %PIX|ASA-1-103002: (Primary) Other firewall network interface interface_number OK.

説明 これはフェールオーバー メッセージです。このメッセージは、セカンダリ装置のネットワーク インターフェイスが正常であることをプライマリ装置が検出すると表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。interface_number 変数に指定できる値については、第 1 章「セキュリティ アプライアンスのロギングの設定」の表 1-7 を参照してください。

推奨処置 不要です。

103003

エラーメッセージ %PIX|ASA-1-103003: (Primary) Other firewall network interface *interface_number* failed.

説明 これはフェールオーバー メッセージです。このメッセージは、プライマリ装置がセカンダリ装置に不良ネットワーク インターフェイスを検出すると表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 セカンダリ装置のネットワーク接続をチェックして、ネットワーク ハブ接続を確認します。必要に応じて、障害の発生したネットワーク インターフェイスを交換します。

103004

エラーメッセージ %PIX|ASA-1-103004: (Primary) Other firewall reports this firewall failed.

説明 これはフェールオーバー メッセージです。このメッセージは、プライマリ装置に障害が発生していることを示すメッセージをプライマリ装置がセカンダリ装置から受信すると表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 プライマリ装置のステータスを確認します。

103005

エラーメッセージ %PIX|ASA-1-103005: (Primary) Other firewall reporting failure.

説明 これはフェールオーバー メッセージです。このメッセージは、セカンダリ装置がプライマリ装置に障害を報告すると表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 セカンダリ装置のステータスを確認します。

104001, 104002

エラーメッセージ %PIX|ASA-1-104001: (Primary) Switching to ACTIVE (cause: *string*).

エラーメッセージ %PIX|ASA-1-104002: (Primary) Switching to STNDBY (cause: *string*).

説明 この例は、両方ともフェールオーバー メッセージです。これらのメッセージは通常、スタンバイ装置で **failover active** コマンドを入力するか、またはアクティブ装置で **no failover active** コマンドを入力することによって強制的にペアの役割を切り替えると記録されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。 *string* 変数の値は次のとおりです。

- 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

推奨処置 手作業による介入が原因でメッセージが表示される場合は、処置は不要です。それ以外の場合は、セカンダリ装置から報告された原因を使用して、ペアの装置両方のステータスを確認します。

104003

エラー メッセージ %PIX|ASA-1-104003: (Primary) Switching to FAILED.

説明 これはフェールオーバー メッセージです。このメッセージは、プライマリ装置に障害が発生すると表示されます。

推奨処置 プライマリ装置のシステム ログ メッセージを確認して、問題の性質を示す表示がないか調べます (メッセージ 104001 を参照)。 (Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

104004

エラー メッセージ %PIX|ASA-1-104004: (Primary) Switching to OK.

説明 これはフェールオーバー メッセージです。このメッセージは、前に障害になった装置が現在は再び動作していると報告すると表示されます。 (Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

105001

エラー メッセージ %PIX|ASA-1-105001: (Primary) Disabling failover.

説明 これはフェールオーバー メッセージです。このメッセージは、コンソールで **no failover** コマンドを入力すると表示されます。 (Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

105002

エラー メッセージ %PIX|ASA-1-105002: (Primary) Enabling failover.

説明 これはフェールオーバー メッセージです。このメッセージは、これまでフェールオーバーをディセーブルにしていたコンソールで引数をとらずに **failover** コマンドを入力すると表示されます。 (Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

105003

エラー メッセージ %PIX|ASA-1-105003: (Primary) Monitoring on interface *interface_name* waiting

説明 これはフェールオーバー メッセージです。Cisco ASA が指摘されたネットワーク インターフェイス (フェールオーバー ペアの相手装置とのインターフェイス) をテストしています。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。Cisco ASA は、正常動作中に自分のネットワーク インターフェイスを頻繁に監視します。

105004

エラー メッセージ %PIX|ASA-1-105004: (Primary) Monitoring on interface *interface_name* normal

説明 これはフェールオーバー メッセージです。指摘されたネットワーク インターフェイスのテストが成功しました。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

105005

エラー メッセージ %PIX|ASA-1-105005: (Primary) Lost Failover communications with mate on interface *interface_name*.

説明 これはフェールオーバー メッセージです。このメッセージは、フェールオーバー ペアのこの装置がペアの相手装置と通信できなくなると表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 指摘されたインターフェイスに接続されているネットワークが正しく機能していることを確認します。

105006, 105007

エラー メッセージ %PIX|ASA-1-105006: (Primary) Link status 'Up' on interface *interface_name*.

エラー メッセージ %PIX|ASA-1-105007: (Primary) Link status 'Down' on interface *interface_name*.

説明 この例は、両方ともフェールオーバー メッセージです。これらのメッセージは、指摘されたインターフェイスのリンク ステータスの監視結果を報告します。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 リンク ステータスがダウンである場合は、指摘されたインターフェイスに接続されているネットワークが正しく動作していることを確認します。

105008

エラー メッセージ %PIX|ASA-1-105008: (Primary) Testing interface
interface_name.

説明 これはフェールオーバー メッセージです。このメッセージは、指摘されたネットワーク インターフェイスをテストすると表示されます。このテストは、想定された間隔後に Cisco ASA がそのインターフェイス上でスタンバイ装置からメッセージを受け取ることができなかった場合に限って実行されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

105009

エラー メッセージ %PIX|ASA-1-105009: (Primary) Testing on interface
interface_name {Passed|Failed}.

説明 これはフェールオーバー メッセージです。このメッセージは、前のインターフェイス テストの結果 (Passed または Failed) を報告します。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 結果が Passed であれば不要です。結果が Failed の場合は、両方のフェールオーバー 装置へのネットワーク ケーブル接続、およびネットワーク自体が正しく機能していることを チェックするとともに、スタンバイ装置のステータスを確認します。

105010

エラー メッセージ %PIX|ASA-3-105010: (Primary) Failover message block alloc
failed

説明 ブロック メモリが枯渇しています。これは一時メッセージで、Cisco ASA は回復する必要がありません。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 show blocks コマンドを使用して、現在のブロック メモリを監視します。

105011

エラー メッセージ %PIX|ASA-1-105011: (Primary) Failover cable communication
failure

説明 フェールオーバー ケーブルがプライマリ装置とセカンダリ装置間の通信を許可していません。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 ケーブルが正しく接続されていることを確認します。

105020

エラー メッセージ %PIX|ASA-1-105020: (Primary) Incomplete/slow config replication

説明 フェールオーバーが発生すると、アクティブな Cisco ASA はメモリ内の不完全なコンフィギュレーションを検出します。通常、これは複製サービスの中断が原因となっています。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 Cisco ASA によってフェールオーバーが検出されると、Cisco ASA は自分自身を自動的にリロードして、フラッシュメモリからコンフィギュレーションを自動的にリロードするか、または別の Cisco ASA と再同期化します (両方行うこともあります)。フェールオーバーが引き続き発生する場合は、フェールオーバー コンフィギュレーションを調べて、両方の Cisco ASA 装置が互いに通信できることを確認します。

105021

エラー メッセージ %PIX|ASA-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name

説明 コンフィギュレーションの同期化中に、他のプロセスが5分以上コンフィギュレーションをロックして、フェールオーバー プロセスが新しいコンフィギュレーションを適用するのを妨げている場合、スタンバイ装置は自分自身をリロードします。これは、コンフィギュレーション同期化の進行中に、管理者がスタンバイ装置で実行コンフィギュレーションに目を通している場合に発生することがあります。show running-config EXEC コマンドおよび pager lines num CONFIG コマンドも参照してください。

推奨処置 コンフィギュレーションが最初に起動し、アクティブ装置とのフェールオーバー接続を確立している間は、スタンバイ装置でコンフィギュレーションを表示または修正しないでください。

105031

エラー メッセージ %PIX|ASA-1-105031: Failover LAN interface is up

説明 LAN フェールオーバー インターフェイス リンクがアップしています。

推奨処置 不要です。

105032

エラー メッセージ %PIX|ASA-1-105032: LAN Failover interface is down

説明 LAN フェールオーバー インターフェイス リンクがダウンしています。

推奨処置 LAN フェールオーバー インターフェイスの接続を確認します。速度 / 二重通信の設定が正しいことを確認します。

105034

エラー メッセージ %PIX|ASA-1-105034: Receive a LAN_FAILOVER_UP message from peer.

説明 ピアがブートされて、初期コンタクトメッセージが送信されました。

推奨処置 不要です。

105035

エラー メッセージ %PIX|ASA-1-105035: Receive a LAN failover interface down msg from peer.

説明 ピア LAN フェールオーバー インターフェイス リンクがダウンしています。装置がスタンバイ モードになっている場合、アクティブ モードに切り替わります。

推奨処置 ピア LAN フェールオーバー インターフェイスの接続を確認します。

105036

エラー メッセージ %PIX|ASA-1-105036: dropped a LAN Failover command message.

説明 Cisco ASA は無応答の LAN フェールオーバー コマンドメッセージを廃棄しました。これは LAN フェールオーバー インターフェイスの接続障害を示します。

推奨処置 LAN インターフェイス ケーブルが接続されていることを確認します。

105037

エラー メッセージ %PIX|ASA-1-105037: The primary and standby units are switching back and forth as the active unit.

説明 プライマリ装置およびスタンバイ装置がアクティブ装置として交互に切り替わっています。これは、LAN フェールオーバー接続障害またはソフトウェアのバグを示します。

推奨処置 LAN インターフェイス ケーブルが接続されていることを確認します。

105038

エラー メッセージ %PIX|ASA-1-105038: (Primary) Interface count mismatch

説明 フェールオーバーが発生すると、アクティブな Cisco ASA はメモリ内の不完全なコンフィギュレーションを検出します。通常、これは複製サービスの中断が原因となっています。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 Cisco ASA によってフェールオーバーが検出されると、Cisco ASA は自分自身を自動的にリロードして、フラッシュメモリからコンフィギュレーションを自動的にリロードするか、または別の Cisco ASA と再同期化します (両方行うこともあります)。フェールオーバーが引き続き発生する場合は、フェールオーバー コンフィギュレーションを調べて、両方の Cisco ASA 装置が互いに通信できることを確認します。

105039

エラー メッセージ %PIX|ASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.

説明 フェールオーバーは最初にプライマリおよびセカンダリの Cisco ASA で設定されているインターフェイスの数が同じであることを確認します。このメッセージは、セカンダリ Cisco ASA で設定されているインターフェイスの数をプライマリ Cisco ASA が確認できないことを示します。このメッセージは、プライマリ Cisco ASA がフェールオーバー インターフェイス経由でセカンダリ Cisco ASA と通信できないことを示します。(Primary) は、セカンダリ Cisco ASA の場合は (Secondary) と示されることもあります。

推奨処置 プライマリおよびセカンダリの Cisco ASA でフェールオーバー LAN、インターフェイス コンフィギュレーション、およびステータスを確認します。セカンダリ Cisco ASA が Cisco ASA アプリケーションを実行しており、フェールオーバーがイネーブルになっていることを確認します。

105040

エラー メッセージ %PIX|ASA-1-105040: (Primary) Mate failover version is not compatible.

説明 プライマリおよびセカンダリの Cisco ASA は、フェールオーバー ペアとして動作するために同じフェールオーバー ソフトウェアのバージョンを実行する必要があります。このメッセージは、セカンダリ Cisco ASA フェールオーバー ソフトウェアのバージョンがプライマリ Cisco ASA と互換性がないことを示します。フェールオーバーがプライマリ Cisco ASA でイネーブルになっています。(Primary) は、セカンダリ Cisco ASA の場合は (Secondary) と示されることもあります。

推奨処置 フェールオーバーをイネーブルにするために、プライマリおよびセカンダリの Cisco ASA 間で一致したソフトウェア バージョンを使用します。

105042

エラー メッセージ %PIX|ASA-1-105042: (Primary) Failover interface OK

説明 LAN フェールオーバー インターフェイス リンクがアップしています。

説明 セカンダリ Cisco ASA にフェールオーバー メッセージを送信するために使用されるインターフェイスが機能しています。(Primary) は、セカンダリ Cisco ASA の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

105043

エラー メッセージ %PIX|ASA-1-105043: (Primary) Failover interface failed

説明 LAN フェールオーバー インターフェイス リンクがダウンしています。

推奨処置 LAN フェールオーバー インターフェイスの接続を確認します。速度 / 二重通信の設定が正しいことを確認します。

105044

エラー メッセージ %PIX|ASA-1-105044: (Primary) Mate operational mode *mode* is not compatible with my mode *mode*.

説明 動作モード(シングルまたはマルチ)がフェールオーバー ピア間で一致しない場合、フェールオーバーはディセーブルになります。

推奨処置 同じ動作モードになるようにフェールオーバー ピアを設定してから、フェールオーバーを再度イネーブルにします。

105045

エラー メッセージ %PIX|ASA-1-105045: (Primary) Mate license (*number contexts*) is not compatible with my license (*number contexts*).

説明 フィーチャライセンスがフェールオーバー ピア間で一致しない場合、フェールオーバーはディセーブルになります。

推奨処置 同じフィーチャライセンスを持つようにフェールオーバー ピアを設定してから、フェールオーバーを再度イネーブルにします。

105046

エラー メッセージ %PIX|ASA-1-105046 (Primary|Secondary) Mate has a different chassis

説明 このメッセージは、2つのフェールオーバー装置が異なるタイプのシャーシを持つ場合に発行されます。たとえば、一方が PIX で、もう一方が ASA-5520 の場合、あるいは一方が 3 スロットのシャーシを持ち、もう一方が 6 スロットのシャーシを持つ場合です。

推奨処置 2つのフェールオーバー装置が同じであることを確認します。

105047

エラー メッセージ %PIX|ASA-1-105047: Mate has a *io_card_name1* card in slot *slot_number* which is different from my *io_card_name2*

説明 2つのフェールオーバー装置は、対応するスロットに異なるタイプのカードが実装されています。

推奨処置 フェールオーバー装置のカード コンフィギュレーションが同じであることを確認します。

106001

エラーメッセージ %PIX|ASA-2-106001: Inbound TCP connection denied from *IP_address/port* to *IP_address/port* flags *tcp_flags* on interface *interface_name*

説明 これは接続関連のメッセージです。このメッセージは、内部アドレスに接続しようとしたが、セキュリティポリシーによって拒否された場合に表示されます。表示される *tcp_flags* 値は、接続が拒否されたときに存在していた TCP ヘッダーのフラグに対応します。たとえば、Cisco ASA に接続状態が存在しない TCP パケットが到着し、それが廃棄された場合です。このパケットの *tcp_flags* は FIN および ACK です。

tcp_flags を次に示します。

- ACK : 肯定応答番号が受信されました。
- FIN : データが送信されました。
- PSH : 受信者がデータをアプリケーションに渡しました。
- RST : 接続がリセットされました。
- SYN : シーケンス番号が接続を開始するために同期化されました。
- URG : 緊急ポインタが有効であると宣言されました。

推奨処置 不要です。

106002

エラーメッセージ %PIX|ASA-2-106002: *protocol* Connection denied by outbound list *acl_ID* src *inside_address* dest *outside_address*

説明 これは接続関連のメッセージです。このメッセージは、**outbound deny** コマンドが原因で、指摘された接続が失敗した場合に表示されます。*protocol* 変数は ICMP、TCP、または UDP になります。

推奨処置 **show outbound** コマンドを使用して、発信リストを確認します。

106006

エラーメッセージ %PIX|ASA-2-106006: Deny inbound UDP from *outside_address/outside_port* to *inside_address/inside_port* on interface *interface_name*.

説明 これは接続関連のメッセージです。このメッセージは、着信 UDP パケットがセキュリティポリシーによって拒否された場合に表示されます。

推奨処置 不要です。

106007

エラー メッセージ %PIX|ASA-2-106007: Deny inbound UDP from *outside_address/outside_port* to *inside_address/inside_port* due to DNS {Response|Query}.

説明 これは接続関連のメッセージです。このメッセージは、DNS クエリーまたは応答を含んでいる UDP パケットが拒否された場合に表示されます。

推奨処置 内部ポート番号が 53 の場合、内部ホストはキャッシング ネーム サーバとして設定されていると考えられます。access-list コマンド文を追加して UDP ポート 53 のトラフィックを許可します。外部ポート番号が 53 の場合、DNS サーバの応答が遅かったため、クエリーには別のサーバが応答したと考えられます。

106010

エラー メッセージ %PIX|ASA-3-106010: Deny inbound protocol src *interface_name:dest_address/dest_port* dst *interface_name:source_address/source_port*

説明 これは接続関連のメッセージです。このメッセージは、着信接続がセキュリティ ポリシーによって拒否された場合に表示されます。

推奨処置 トラフィックを許可する必要がある場合は、セキュリティ ポリシーを修正します。このメッセージが繰り返し表示される場合は、リモート ピアの管理者にお問い合わせください。

106011

エラー メッセージ %PIX|ASA-3-106011: Deny inbound (No xlate) *string*

説明 このメッセージは、Web ブラウザ経由でインターネットにアクセスしている内部ユーザがいる場合、通常のトラフィック条件で表示されます。接続がリセットされた場合は常に、Cisco ASA がリセットを受信した後に、その接続の端にあるホストがパケットを送信すると、このメッセージが表示されます。これは通常、無視してかまいません。

推奨処置 no logging message 106011 コマンドを入力して、このシステム ログ メッセージが syslog& サーバに記録されないようにします。

106012

エラー メッセージ %PIX|ASA-6-106012: Deny IP from *IP_address* to *IP_address*, IP options *hex*.

説明 これはパケット整合性チェック メッセージです。IP パケットが IP オプションと共に表示されました。IP オプションはセキュリティ リスクとみなされるので、パケットは廃棄されました。

推奨処置 リモート ホストシステムの管理者に問い合わせて、問題を判別します。ローカル サイトを確認して、あいまいなソース ルーティングや厳密なソース ルーティングがないかどうか調べます。

106013

エラーメッセージ %PIX|ASA-2-106013: Dropping echo request from *IP_address* to PAT address *IP_address*

説明 Cisco ASA は、PAT グローバルアドレスに対応する宛先アドレスを持つ着信 ICMP エコー要求パケットを廃棄しました。着信パケットは、そのパケットを受信するべき PAT ホストを指定できないので廃棄されます。

推奨処置 不要です。

106014

エラーメッセージ %PIX|ASA-3-106014: Deny inbound icmp src *interface_name*: *IP_address* dst *interface_name*: *IP_address* (type *dec*, code *dec*)

説明 Cisco ASA は、すべての着信 ICMP パケット アクセスを拒否しました。デフォルトで、ICMP パケットはすべて、特に許可されている場合を除き、拒否されます。

推奨処置 不要です。

106015

エラーメッセージ %PIX|ASA-6-106015: Deny TCP (no connection) from *IP_address/port* to *IP_address/port* flags *tcp_flags* on interface *interface_name*.

説明 Cisco ASA は、関連付けられている接続が Cisco ASA 接続テーブルにない TCP パケットを廃棄しました。Cisco ASA は、新しい接続の確立要求を示す SYN フラグをパケットで探します。その SYN フラグが設定されておらず、既存の接続もない場合、Cisco ASA はそのパケットを廃棄します。

推奨処置 Cisco ASA がこれらの無効な TCP パケットを大量に受信する場合を除き、不要です。大量に受信する場合は、パケットを送信元までトレースして、これらのパケットが送信された原因を判別します。

106016

エラーメッセージ %PIX|ASA-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name*.

説明 Cisco ASA は、無効な送信元アドレス（たとえば、次に示すアドレスなどの無効アドレス）を持つパケットを廃棄しました。

- ループバック ネットワーク (127.0.0.0)
- ブロードキャスト (limited、net-directed、subnet-directed、および all-subnets-directed)
- 宛先ホスト (land.c)

スプーフィングパケット検出をさらに強化するために、**conduit** コマンドを使用して、内部ネットワークに属する送信元アドレスを持つパケットを廃棄するように Cisco ASA を設定します。現在は **icmp** コマンドが実装されるようになったので、**conduit** コマンドは推奨しません。このコマンドが正しく動作することは保証されていません。

推奨処置 外部ユーザが保護されているネットワークを危険にさらそうとしていないかどうか判別します。誤って設定したクライアントがないかどうか確認します。

106017

エラー メッセージ %PIX|ASA-2-106017: Deny IP due to Land Attack from *IP_address* to *IP_address*

説明 Cisco ASA が IP 宛先と同一の IP 送信元アドレスを持ち、送信元ポートと同一の宛先ポートを持つパケットを受信しました。このメッセージは、システムの攻撃を目的としてスプーフィングされたパケットを示します。この攻撃は、Land 攻撃と呼ばれます。

推奨処置 このメッセージが引き続き表示される場合は、攻撃が進行中である可能性があります。パケットは、攻撃の起点を決定するのに十分な情報を提供しません。

106018

エラー メッセージ %PIX|ASA-2-106018: ICMP packet type *ICMP_type* denied by outbound list *acl_ID* src *inside_address* dest *outside_address*

説明 ローカル ホスト (*inside_address*) から外部ホスト (*outside_address*) への発信 ICMP パケット (指摘された ICMP のパケット) が発信 ACL リストによって拒否されました。

推奨処置 不要です。

106020

エラー メッセージ %PIX|ASA-2-106020: Deny IP teardrop fragment (size = *number*, offset = *number*) from *IP_address* to *IP_address*

説明 Cisco ASA が小さなオフセットまたはフラグメントの重複を含む teardrop シグニチャを持つ IP パケットを廃棄しました。これは、Cisco ASA または侵入検知システム (IDS) を欺く敵対イベントです。

推奨処置 リモート ピアの管理者に問い合わせるか、またはこの問題をセキュリティ ポリシーに従って解決を依頼します。

106021

エラー メッセージ %PIX|ASA-1-106021: Deny protocol reverse path check from *source_address* to *dest_address* on interface *interface_name*

説明 攻撃が進行中です。着信接続で IP アドレスをスプーフィングしようとする試みが行われています。逆ルート ルックアップとも呼ばれる Unicast RPF は、ルートによって表される送信元アドレスを持たないパケットを検出し、そのパケットを Cisco ASA への攻撃の一部であると想定します。

このメッセージは、`ip verify reverse-path` コマンドで Unicast RPF をイネーブルにしている場合に表示されます。この機能は、インターフェイスに入力されるパケットについて動作します。外側で設定されている場合 Cisco ASA は、外部から到達するパケットを確認します。

Cisco ASA は、*source_address* に基づいてルートを検索します。エントリが検出されず、ルートが定義されない場合は、システム ログ メッセージが表示され、接続は廃棄されます。

ルートがある場合、Cisco ASA は対応するインターフェイスを確認します。パケットが別のインターフェイスに到着した場合、これはスプーフィングであるか、または宛先まで複数のパスがある非対象なルーティング環境です。Cisco ASA は、非対称ルーティングはサポートしていません。

Cisco ASA が内部インターフェイスで設定されている場合は静的 `route` コマンド文または RIP をチェックし、`source_address` が見つからない場合は、内部ユーザがアドレスをスプーフィングしています。

推奨処置 攻撃が進行中であっても、この機能がイネーブルになっていれば、ユーザによる処置は不要です。Cisco ASA は攻撃を撃退します。

106022

エラー メッセージ `%PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`

説明 接続と一致するパケットが、その接続をそこで開始したインターフェイスとは異なるインターフェイスに到着します。

たとえば、ユーザが内部インターフェイスで接続を開始したが、Cisco ASA が境界インターフェイスに到着する同じ接続を検出する場合、Cisco ASA は宛先へのパスを複数持っていることとなります。これは非対称ルーティングと呼ばれ、Cisco ASA ではサポートされていません。

攻撃者は、Cisco ASA に侵入する方法として、1 つの接続から別の接続にパケットを付加しようと試みることもあります。どちらの場合も、Cisco ASA はこのメッセージを表示して、接続を廃棄します。

推奨処置 このメッセージは、`ip verify reverse-path` コマンドが設定されていない場合に表示されます。ルーティングが非対称でないことを確認します。

106023

エラー メッセージ `%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`

説明 IP パケットが ACL によって拒否されました。このメッセージは、たとえ ACL に対して log オプションがイネーブルになっていない場合でも表示されます。

推奨処置 同じ送信元アドレスからのメッセージが引き続き表示される場合は、フットプリンティングまたはポート スキャンが行われようとしていることをメッセージが示している可能性もあります。ホストの管理者にお問い合わせください。

106024

エラー メッセージ `%PIX|ASA-2-106024: Access rules memory exhausted`

説明 アクセスリストのコンパイルプロセスで、メモリが不足しています。最後の正常なアクセスリスト以降に追加されたコンフィギュレーション情報はすべて、システムから削除されました。最新のコンパイル済みアクセスリストのセットが引き続き使用されます。

推奨処置 Access Lists、AAA、ICMP、SSH、Telnet、および他の規則タイプは、アクセスリストの規則タイプとして格納され、コンパイルされます。これらの規則タイプの一部を削除して、他の規則タイプを追加できるようにします。

106025, 106026

エラー メッセージ %PIX|ASA-6-106025: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol

エラー メッセージ %PIX|ASA-6-106026: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol

説明 マルチコンテキスト モードのパケットのセキュリティ コンテキストを判定できません。どちらのメッセージも、ルータまたは透過モードで廃棄される IP パケットに対して生成されることがあります。

推奨処置 不要です。

106027

エラー メッセージ %PIX|ASA-4-106027:Failed to determine the security context for the packet:vlan:source Vlan#:ethertype src sourceMAC dst destMAC

説明 マルチコンテキスト モードのパケットのセキュリティ コンテキストを判定できません。このメッセージは、透過モードで廃棄される非 IP パケットに対してのみ生成されます。

推奨処置 不要です。

106100

エラー メッセージ %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})

説明 access-list コマンドに log オプションを設定した場合、パケットが ACL 文と一致しました。メッセージ レベルは、access-list コマンドに設定されているレベルによって決まります(デフォルトでは、レベルは 6 です)。このメッセージは、最初の出現か、またはある期間の合計出現数を示します。このメッセージは、拒否されたパケットのみを記録して、ヒット数も設定可能なレベルも含まないメッセージ 106023 よりも多くの情報を提供します。メッセージの値は次のとおりです。

- permitted | denied | est-allowed : これらの値は、パケットが ACL によって許可されたか拒否されたかを指摘します。値が est-allowed の場合、パケットは ACL によって拒否されましたが、すでに確立されているセッションで許可されました(たとえば、内部ユーザがインターネットへのアクセスを許可され、通常は ACL によって拒否される応答パケットが許可されます)。
- protocol : TCP、UDP、ICMP、または IP プロトコル番号。
- interface_name : ログ フローの送信元または宛先のインターフェイス名。VLAN インターフェイスがサポートされています。
- source_address : ログ フローの送信元 IP アドレス。
- dest_address : ログ フローの宛先 IP アドレス。
- source_port : ログ フローの送信元ポート (TCP または UDP)。ICMP の場合、このフィールドは 0 です。

- *dest_port* : ログフローの宛先ポート (TCP または UDP)。ICMP の場合、このフィールドは *icmp-type* です。
- *hit-cnt number* : 設定した期間に、このフローが ACL エントリによって許可または拒否された回数。Cisco ASA が最初のシステム ログメッセージをこのフローに対して生成するときの値は 1 です。
- *first hit* : このフローに対して生成された最初のメッセージ。
- *number-second interval* : ヒット数を累算する対象期間。この期間は、`access-list` コマンドで `interval` オプションを使用して設定します。

推奨処置 不要です。

106101

エラーメッセージ %PIX|ASA-1-106101 The number of ACL log deny-flows has reached limit (*number*).

説明 ACL deny 文 (`access-list id deny` コマンド) に `log` オプションを設定しており、トラフィックフローが ACL 文と一致する場合、Cisco ASA はフロー情報をキャッシュします。このメッセージは、Cisco ASA でキャッシュされる一致フローの数がユーザが設定した制限 (`access-list deny-flow-max` コマンドを使用) を超えたことを示します。

number 値は、`access-list deny-flow-max` コマンドを使用して設定された制限です。

推奨処置 不要です。このメッセージは、DoS 攻撃の結果生成される可能性があります。

107001

エラーメッセージ %PIX|ASA-1-107001: RIP auth failed from *IP_address*:
version=*number*, type=*string*, mode=*string*, sequence=*number* on interface
interface_name

説明 これはアラート ログメッセージです。Cisco ASA は不正な認証を持つ RIP 応答メッセージを受信しました。このメッセージは、ルータまたはセキュリティ アプライアンス の設定の誤り、または失敗した Cisco ASA のルーティング テーブルへの攻撃の失敗が原因となることもあります。

推奨処置 このメッセージは攻撃の可能性を示しているため、監視する必要があります。このメッセージに示されている送信元 IP アドレスを熟知していない場合は、信頼できるエンティティ間で RIP 認証キーを交換します。攻撃者が既存のキーを判別しようと試みている可能性もあります。

107002

エラーメッセージ %PIX|ASA-1-107002: RIP pkt failed from *IP_address*:
version=*number* on interface *interface_name*

説明 これはアラート ログメッセージです。このメッセージは、ルータのバグ、非 RFC 値を内部に持つパケット、または形式が誤っているエントリが原因で表示される可能性があります。これは発生してはならないもので、Cisco ASA のルーティング テーブルを利用しようとする試みの可能性もあります。

推奨処置 このメッセージは攻撃の可能性を示しているため、監視する必要があります。パケットは認証を渡しましたが (イネーブルの場合) 不良データがパケット内にあります。パケットの発信者について疑わしい点があれば、状況を監視してキーを変更します。

108002

エラー メッセージ %PIX|ASA-2-108002: SMTP replaced *string*: out *source_address* in *inside_address* data: *string*

説明 これは、**fixup protocol smtp** コマンドによって生成された Mail Guard (SMTP) メッセージです。このメッセージは、Cisco ASA が電子メール アドレスの無効な文字をスペースで置き換えた場合に表示されます。

推奨処置 不要です。

108003

エラー メッセージ %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*

説明 このメッセージは、Mail Guard (SMTP) によって生成されます。このメッセージは、Cisco ASA が電子メール アドレスに悪意あるパターンを検出して、接続を廃棄する場合に表示されます。これは、攻撃が進行中であることを示します。

説明 不要です。

109001

エラー メッセージ %PIX|ASA-6-109001: Auth start for user *user* from *inside_address/inside_port* to *outside_address/outside_port*

説明 これは、認証、認可、アカウントिंग (AAA) メッセージです。このメッセージは、Cisco ASA が AAA に設定されており、指摘されたユーザによる認証要求を検出した場合に表示されます。

推奨処置 不要です。

109002

エラー メッセージ %PIX|ASA-6-109002: Auth from *inside_address/inside_port* to *outside_address/outside_port* failed (server *IP_address* failed) on interface *interface_name*.

説明 これは AAA メッセージです。このメッセージは、指摘された認証サーバにモジュールがアクセスできないために認証要求が失敗した場合に表示されます。

推奨処置 指摘された認証サーバ上で認証デーモンが動作していることを確認します。

109003

エラー メッセージ %PIX|ASA-6-109003: Auth from *inside_address* to *outside_address/outside_port* failed (all servers failed) on interface *interface_name*.

説明 これは AAA メッセージです。このメッセージは、認証サーバを見つけることができなかった場合に表示されます。

推奨処置 Cisco ASA から認証サーバに対して ping を実行します。デーモンが動作していることを確認します。

109005

エラー メッセージ %PIX|ASA-6-109005: Authentication succeeded for user *user* from *inside_address/inside_port* to *outside_address/outside_port* on interface *interface_name*.

説明 これは AAA メッセージです。このメッセージは、指摘された認証要求が成功すると表示されます。

推奨処置 不要です。

109006

エラー メッセージ %PIX|ASA-6-109006: Authentication failed for user *user* from *inside_address/inside_port* to *outside_address/outside_port* on interface *interface_name*.

説明 これは AAA メッセージです。このメッセージは、おそらくパスワードが誤っているために、指摘された認証要求が失敗した場合に表示されます。

推奨処置 不要です。

109007

エラー メッセージ %PIX|ASA-6-109007: Authorization permitted for user *user* from *inside_address/inside_port* to *outside_address/outside_port* on interface *interface_name*.

説明 これは AAA メッセージです。このメッセージは、指摘された認可要求が成功すると表示されます。

推奨処置 不要です。

109008

エラー メッセージ %PIX|ASA-6-109008: Authorization denied for user *user* from *outside_address/outside_port* to *inside_address/ inside_port* on interface *interface_name*.

説明 これは AAA メッセージです。このメッセージは、おそらくパスワードが誤っているために、指摘されたアドレスへのアクセスをユーザが許可されなかった場合に表示されます。

推奨処置 不要です。

109010

エラー メッセージ %PIX|ASA-3-109010: Auth from *inside_address/inside_port* to *outside_address/outside_port* failed (too many pending auths) on interface *interface_name*.

説明 これは AAA メッセージです。このメッセージは、サーバで多くの要求が保留中であるために、認証要求が処理できなかった場合に表示されます。

推奨処置 認証サーバが遅すぎるために認証要求に応答できないのかどうか確認します。Flood Defender 機能を `floodguard enable` コマンドでイネーブルにします。

109011

エラー メッセージ %PIX|ASA-2-109011: Authen Session Start: user '*user*', sid *number*

説明 認証セッションがホストと Cisco ASA の間で開始されましたが、まだ完了していません。

推奨処置 不要です。

109012

エラー メッセージ %PIX|ASA-5-109012: Authen Session End: user '*user*', sid *number*, elapsed *number* seconds

説明 認証キャッシュがタイムアウトになっています。ユーザは、次の接続で再認証が必要になります。 `timeout uauth` コマンドを使用して、このタイマーのタイムアウト時間を変更できます。

推奨処置 不要です。

109013

エラー メッセージ %PIX|ASA-3-109013: User must authenticate before using this service

説明 ユーザは、サービスを使用する前に認証を受ける必要があります。

推奨処置 サービスを使用する前に FTP、Telnet、または HTTP を使用して認証します。

109014

エラー メッセージ %PIX|ASA-7-109014: uauth_lookup_net fail for uauth_in()

説明 認証の要求に、対応する認可の要求がありませんでした。

推奨処置 `aaa authentication` および `aaa authorization` コマンド文がコンフィギュレーションに含まれていることを確認します。

109016

エラー メッセージ %PIX|ASA-3-109016: Can't find authorization ACL *acl_ID* for user '*user*'

説明 このユーザの AAA サーバで指定されているアクセス コントロール リストが、Cisco ASA に存在しません。このエラーは、Cisco ASA を設定する前に AAA サーバを設定した場合に発生することがあります。AAA サーバでベンダー固有のアトリビュート (VSA) が次の値のいずれかになっている可能性があります。

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

推奨処置 Cisco ASA に ACL を追加し、AAA サーバで指定したものと同名前を必ず使用するようになります。

109017

エラー メッセージ %PIX|ASA-4-109017: User at *IP_address* exceeded auth proxy connection limit (max)

説明 ユーザが、ユーザ認証のプロキシ制限を超えて、プロキシに多くの接続を開きました。

推奨処置 `proxy-limit proxy_limit` コマンドを入力してプロキシ制限を増やすか、または未使用の接続を閉じるようユーザに要求します。引き続きエラーが表示される場合は、DoS 攻撃の可能性を示していることもあります。

109018

エラー メッセージ %PIX|ASA-3-109018: Downloaded ACL *acl_ID* is empty

説明 ダウンロードされた認可アクセス コントロール リストに ACE がありません。この状況は、アトリビュート文字列「`ip:inacl#`」のつづりの誤り、または `access-list` コマンドの省略が原因となっている可能性があります。

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

推奨処置 指摘されたエラーのある ACL コンポーネントを AAA サーバ上で修正します。

109019

エラー メッセージ %PIX|ASA-3-109019: Downloaded ACL *acl_ID* has parsing error;
ACE *string*

説明 ダウンロードした認可アクセス コントロール リストのアトリビュート文字列 ip:inacl#NNN= のシーケンス番号 NNN を解析中にエラーが発生しました。原因には次のものがあります。= の欠落、数字以外の文字やスペース以外の文字が「#」と「=」の間にある、および NNN が 99999999 より大きい。

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

推奨処置 指摘されたエラーのある ACL 要素を AAA サーバ上で修正します。

109020

エラー メッセージ %PIX|ASA-3-109020: Downloaded ACL has config error; ACE

説明 ダウンロードされた認可アクセス コントロール リストのコンポーネントの 1 つにコンフィギュレーション エラーがあります。この要素のテキスト全体は、システム ログ メッセージに含まれています。このメッセージは通常、無効な `access-list` コマンド文が原因となっています。

推奨処置 指摘されたエラーのある ACL コンポーネントを AAA サーバ上で修正します。

109021

エラー メッセージ %PIX|ASA-7-109021: Uauth null proxy error

説明 内部ユーザ認証エラーが発生しました。

推奨処置 不要です。ただし、このエラーが繰り返し表示される場合は、Cisco TAC にお問い合わせください。

109022

エラー メッセージ %PIX|ASA-4-109022: exceeded HTTPS proxy process limit

説明 各 HTTPS 認証に対して、Cisco ASA は、1 つのプロセスを認証要求に専用で応じるようにします。同時に動作しているプロセスの数がシステムによって課せられた制限を超えると、Cisco ASA は認証を実行せず、このメッセージが表示されます。

推奨処置 不要です。

109023

エラー メッセージ %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.

説明 これは AAA メッセージです。このサービス ポートは、設定されたポリシーに基づいて認証を受けてから、使用する必要があります。

推奨処置 上記のサービス ポートを使用しようとするときは、事前に Telnet、FTP、または HTTP を使用して認証します。

109024

エラー メッセージ %PIX|ASA-6-109024: Authorization denied from *source_address/source_port* to *dest_address/dest_port* (not authenticated) on interface *interface_name* using *protocol*

説明 これは AAA メッセージです。このメッセージは、Cisco ASA が AAA 用に設定され、ユーザが事前の認証なしに Cisco ASA を通して TCP 接続を行おうとした場合に表示されます。

推奨処置 不要です。

109025

エラー メッセージ %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*

説明 アクセス コントロール リストのチェックが失敗しました。チェックは、拒否と一致したか、または暗黙的な拒否のように、何とも一致しませんでした。接続は、Cisco Secure Access Control Server (ACS) の AAA 認可ポリシーを通して定義されたユーザ アクセス コントロール リスト *acl_ID* によって拒否されました。

推奨処置 不要です。

109026

エラー メッセージ %PIX|ASA-3-109026: [*aaa_protocol*] Invalid reply digest received; shared server key may be mismatched.

説明 AAA サーバからの応答が検証できませんでした。設定されたサーバ キーが誤っていることが考えられます。このイベントは、RADIUS サーバまたは TACACS+ サーバとのトランザクション中に生成されることがあります。

推奨処置 `aaa-server` コマンドを使用して設定されたサーバ キーが正しいことを確認します。

109027

エラー メッセージ %PIX|ASA-4-109027: [aaa protocol] Unable to decipher response message Server = *server_IP_address*, User = *user*

説明 AAA サーバからの応答が検証できませんでした。設定されたサーバキーが誤っている可能性があります。このメッセージは、RADIUS サーバまたは TACACS+ サーバとのトランザクション中に表示されることがあります。*server_IP_address* は、関連する AAA サーバの IP アドレスです。*user* は、接続に関連付けられているユーザ名です。

推奨処置 `aaa-server` コマンドを使用して設定されたサーバキーが正しいことを確認します。

109028

エラー メッセージ %PIX|ASA-4-109028: aaa bypassed for same-security traffic from *ingress_interface:source_address/source_port* to *egress_interface:dest_address/dest_port*

説明 AAA が設定された AAA 規則と一致する同じセキュリティトラフィックに対してバイパスされています。これが発生する可能性があるのは、同じ設定済みセキュリティレベルを持つ 2 つのインターフェイス間をトラフィックが通過する場合、同じセキュリティトラフィックが許可される場合、および AAA コンフィギュレーションが `include` 構文または `exclude` 構文を使用する場合だけです。

推奨処置 不要です。

109029

エラー メッセージ %PIX|ASA-5-109029: Parsing downloaded ACL: *string*

説明 ユーザ認証中に RADIUS サーバからダウンロードされたアクセスリストを解析している間に構文エラーが発生しました。

string : アクセスリストの正しい解析を妨げた構文エラーを詳述するエラーメッセージ。

推奨処置 このメッセージに提示されている情報を使用して、RADIUS サーバコンフィギュレーション内のアクセスリスト定義にある構文エラーを特定し、訂正します。

109030

エラー メッセージ %PIX|ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL *access_list source | dest netmask netmask*.

説明 このメッセージは、RADIUS サーバで設定されたダイナミック ACL が、ワイルドカード ネットマスクを自動的に検出するメカニズムによって変換されなかった場合に表示されます。問題は、ネットマスクがワイルドカードであるか、通常のネットマスクであるかをこのメカニズムが判別できないために発生します。

access_list : 変換できなかったアクセスリスト。

source : 送信元 IP アドレス。

dest : 宛先 IP アドレス。

netmask : 宛先アドレスまたは送信元アドレスに対する 10 進数表記のサブネット マスク。

推奨処置 RADIUS サーバのアクセス リスト ネットマスクを確認して、ワイルドカード コンフィギュレーションがないかどうか調べます。これがワイルドカードを意味する場合、およびそのサーバのアクセス リスト ネットマスクすべてがワイルドカードである場合、AAA サーバの *acl-netmask-convert* に *wildcard* 設定を使用します。それ以外の場合は、ネットマスクを通常のネットマスクまたはホールを含まないワイルドカード ネットマスクに変更します。つまり、ネットマスクは連続する 2 進数の 1 を提示します。たとえば、00000000.00000000.00011111.11111111 または 16 進数 0.0.31.255 のようになります。マスクが通常を意味する場合、およびそのサーバのすべてのアクセス リスト ネットマスクが通常である場合、AAA サーバの *acl-netmask-convert* に *normal* 設定を使用します。

109031

エラー メッセージ %PIX|ASA-4-109031: NT Domain Authentication Failed: rejecting guest login for *username*.

説明 このメッセージは、ユーザがゲスト アカウントのアクセス用に設定された NT Auth ドメインに認証を試みたとき、*username* が NT サーバで有効なユーザ名でない場合に表示されます。接続は拒否されます。

推奨処置 ユーザが有効なユーザの場合は、アカウントを NT サーバに追加します。ユーザがアクセスを許可されていない場合は、処置は不要です。

109032

エラー メッセージ %PIX|ASA-3-109032: Unable to install ACL *access_list*, downloaded for user *username*; Error in ACE: *ace*.

説明 このメッセージは、ネットワーク ユーザの認証中に RADIUS サーバからアクセス コントロール リストが受信されると表示されます。このログ イベントは、アクセス リストの要素の 1 つに構文エラーがあることを示します。このエラーが発生する場合、要素は廃棄されますが、アクセス リストの残りの部分は引き続き適用されます。形式が誤っている要素のテキスト全体は、メッセージに含まれています。この状態は認証の失敗をもたらすものではないことに注意してください。

access_list : **show access-list** コマンドの出力に表示されるダイナミック アクセス リストに割り当てられている名前。

username : その接続がこのアクセス リストの制御を受けるユーザの名前。

ace : エラーが検出されたときに処理されていたアクセス リストのエントリ。

推奨処置 RADIUS サーバのコンフィギュレーションのアクセス リスト定義を訂正します。

110001

エラー メッセージ %PIX|ASA-6-110001: No route to *dest_address* from *source_address*

説明 このメッセージは、ルート ルックアップの失敗を示します。パケットは、ルーティング テーブルにない宛先 IP アドレスを探しています。

推奨処置 ルーティング テーブルをチェックして、宛先へのルートがあることを確認します。

111001

エラー メッセージ %PIX|ASA-5-111002: Begin configuration: *IP_address* writing to *device*

説明 このメッセージは、`write` コマンドを入力してコンフィギュレーションを *device* (フロッピーディスク、フラッシュメモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末のいずれか)に格納する場合に表示されます。*IP_address* は、ログインがコンソールポートで行われたか、または Telnet 接続で行われたかを示します。

推奨処置 不要です。

111002

エラー メッセージ %PIX|ASA-5-111002: Begin configuration: *IP_address* reading from *device*

説明 このメッセージは、`<>` コマンドを入力してコンフィギュレーションを *device* (フロッピーディスク、フラッシュメモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末のいずれか)から読み取る場合に表示されます。*IP_address* は、ログインがコンソールポートで行われたか、または Telnet 接続で行われたかを示します。

推奨処置 不要です。

111003

エラー メッセージ %PIX|ASA-5-111003: *IP_address* Erase configuration

説明 これは管理メッセージです。このメッセージは、コンソールで `write erase` コマンドを入力してフラッシュメモリの内容を消去する場合に表示されます。*IP_address* の値は、ログインがコンソールポートで行われたか、または Telnet 接続で行われたかを示します。

推奨処置 コンフィギュレーションを消去した後、Cisco ASA を再設定して新しいコンフィギュレーションを保存します。または、フロッピーディスクまたはネットワークの他の場所にある TFTP サーバに以前保存してあるコンフィギュレーションから情報を復元できます。

111004

エラー メッセージ %PIX|ASA-5-111004: *IP_address* end configuration: {FAILED|OK}

説明 このメッセージは、`config floppy/memory/network` コマンドまたは `write floppy/memory/network/standby` コマンドを入力すると表示されます。*IP_address* の値は、ログインがコンソールポートで行われたか、または Telnet 接続で行われたかを示します。

推奨処置 メッセージが OK で終われば不要です。このメッセージでエラーが表示された場合は、問題を解決します。たとえば、フロッピーディスクに書き込む場合は、フロッピーディスクが書き込み禁止になっていないことを確認します。TFTP サーバに書き込む場合は、サーバが動作していることを確認します。

111005

エラー メッセージ %PIX|ASA-5-111005: *IP_address* end configuration: OK

説明 このメッセージは、コンフィギュレーション モードを終了すると表示されます。*IP_address* の値は、ログインがコンソールポートで行われたか、または Telnet 接続で行われたかを示します。

推奨処置 不要です。

111007

エラー メッセージ %PIX|ASA-5-111007: Begin configuration: *IP_address* reading from *device*.

説明 このメッセージは、**reload** コマンドまたは **configure** コマンドを入力してコンフィギュレーションを読み込む場合に表示されます。*device* テキストは、フロッピーディスク、メモリ、ネット、スタンバイ、または端末になります。*IP_address* の値は、ログインがコンソールポートで行われたか、または Telnet 接続で行われたかを示します。

推奨処置 不要です。

111008

エラー メッセージ %PIX|ASA-5-111008: User *user* executed the command *string*

説明 ユーザがコンフィギュレーションを修正するコマンドを入力しました。

推奨処置 不要です。

111009

エラー メッセージ %PIX|ASA-7-111009:User *user* executed cmd:*string*

説明 ユーザがコンフィギュレーションを修正しないコマンドを入力しました。

推奨処置 不要です。

111111

エラー メッセージ %PIX|ASA-1-111111 *error_message*

説明 システム エラーまたはインフラストラクチャ エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に TAC に送付してください。

112001

エラー メッセージ %PIX|ASA-2-112001: (string:dec) Clear complete.

説明 このメッセージは、モジュール コンフィギュレーションを消去する要求が完了したことを示します。ソース ファイルおよび行番号が特定されます。

推奨処置 不要です。

113001

エラー メッセージ %PIX|ASA-3-113001: Unable to open AAA session. Session limit [*limit*] reached.

説明 システム リソースが使用できないために、IPSec トンネルまたは WebVPN 接続で AAA 動作を実行できませんでした。*limit* 値は、同時 AAA トランザクションの最大数を示します。

推奨処置 可能であれば、AAA リソースの要求を減らします。

113003

エラー メッセージ %PIX|ASA-6-113003: AAA group policy for user *user* is being set to *policy_name*.

説明 トンネル グループに関連付けられているグループ ポリシーは、ユーザ固有のポリシー *policy_name* で上書きされています。*policy_name* は、LOCAL 認証の設定時に `username` コマンドを使用して指定されており、RADIUS 認証の設定時に RADIUS CLASS アトリビュートで返されます。

推奨処置 不要です。

113004

エラー メッセージ %PIX|ASA-6-113004: AAA user *aaa_type* Successful: server = *server_IP_address*, User = *user*

説明 このメッセージは、IPSec 接続または WebVPN 接続で AAA 動作が正常に完了したことを示します。AAA タイプは「認証」、「認可」、または「アカウントिंग」です。*server_IP_address* は、関連する AAA サーバの IP アドレスです。*user* は、接続に関連付けられているユーザ名です。

推奨処置 不要です。

113005

エラーメッセージ %PIX|ASA-6-113005: AAA user authentication Rejected: reason = *string*: server = *server_IP_address*, User = *user*

説明 このメッセージは、IPSec 接続または WebVPN 接続に関連付けられているユーザの認証要求または認可要求が拒否されたことを示します。要求が拒否された理由の詳細は、*reason* フィールドに示されています。*server_IP_address* は、関連する AAA サーバの IP アドレスです。*user* は、接続に関連付けられているユーザ名です。*aaa_operation* は、認証または認可のどちらかです。

推奨処置 不要です。

113006

エラーメッセージ %PIX|ASA-6-113006: User *user* locked out on exceeding *number* successive failed authentication attempts

説明 ローカルに設定されているユーザがロックアウトされています。このメッセージは、このユーザについて認証失敗が連続して設定回数だけ発生したときに現れ、今後このユーザが認証を受けようとしても、管理者が `clear aaa local user lockout` コマンドを使用してユーザをアンロックするまでは、すべて拒否されることを示します。*user* は現在ロックされているユーザであり、*number* は `aaa local authentication attempts max-fail` コマンドで設定されている連続失敗しきい値です。

推奨処置 `clear aaa local user lockout` コマンドを使用してユーザをアンロックするか、許容される連続認証失敗の最大数を調整します。

113007

エラーメッセージ %PIX|ASA-6-113007: User *user* unlocked by *administrator*

説明 ローカルに設定されたユーザが、`aaa local authentication attempts max-fail` コマンドによって設定された連続認証失敗の最大数を越えたためロックアウトされた後、表示されている管理者によってアンロックされました。

推奨処置 不要です。

113008

エラーメッセージ %PIX|ASA-6-113008: AAA transaction status ACCEPT: user = *user*

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザの AAA トランザクションが正常に完了しました。*user* は、接続に関連付けられているユーザ名です。

推奨処置 不要です。

113009

エラー メッセージ %PIX|ASA-6-113009: AAA retrieved default group policy *policy* for user *user*

説明 このメッセージは、IPSec 接続または WebVPN 接続の認証中または認可中に生成される可能性があります。**tunnel-group** コマンドまたは **webvpn** コマンドで指定されたグループ ポリシーのアトリビュートが取得されました。

推奨処置 不要です。

113010

エラー メッセージ %PIX|ASA-6-113010: AAA challenge received for user *user* from server *server_IP_address*

説明 このメッセージは、認証が SecurID サーバで行われる場合 IPSec 接続の認証中に生成される可能性があります。ユーザは、認証に先立って詳細情報を入力するよう求められます。*server_IP_address* は関連 AAA サーバの IP アドレスです。*user* は接続に関連付けられているユーザ名です。

推奨処置 不要です。

113011

エラー メッセージ %PIX|ASA-6-113011: AAA retrieved user specific group policy for user *user*

説明 このイベントは、IPSec 接続または WebVPN 接続の認証中または認可中に生成される可能性があります。**tunnel-group** コマンドまたは **webvpn** コマンドで指定されたグループ ポリシーのアトリビュートが取得されました。

推奨処置 不要です。

113012

エラー メッセージ %PIX|ASA-6-113012: AAA user authentication Successful: local database : user = *user*

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザが、ローカルユーザデータベースに正常に認証されました。*user* は接続に関連付けられているユーザ名です。

推奨処置 不要です。

113013

エラーメッセージ %PIX|ASA-6-113013: AAA unable to complete the request Error:
reason = reason: user = user

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。詳細は *reason* フィールドに示されています。 *user* は、接続に関連付けられているユーザ名です。

推奨処置 不要です。

113014

エラーメッセージ %PIX|ASA-6-113014: AAA authentication server not accessible:
server = server_IP_address: user = user

説明 デバイスが、IPSec 接続または WebVPN 接続に関連付けられている AAA トランザクション中に設定済み AAA サーバと通信できませんでした。このため、ユーザが接続しようとしたとき、*aaa-server* グループに設定されているバックアップサーバおよびそのサーバの可用性に依り、接続に失敗する場合も、失敗しない場合もあります。

推奨処置 設定済みの AAA サーバとの接続を確認します。

113015

エラーメッセージ %PIX|ASA-6-113015: AAA user authentication Rejected: reason =
reason : local database: user = user

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザのローカル ユーザ データベースへの認証要求が拒否されました。要求が拒否された理由の詳細は *reason* フィールドに示されています。 *user* は、接続に関連付けられているユーザ名です。

推奨処置 不要です。

113016

エラーメッセージ %PIX|ASA-6-113016: AAA credentials rejected: reason = reason:
server = server_IP_address: user = user

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。詳細は *reason* フィールドに示されています。 *server_IP_address* は、関連する AAA サーバの IP アドレスです。 *user* は、接続に関連付けられているユーザ名です。

推奨処置 不要です。

113017

エラー メッセージ %PIX|ASA-6-113017: AAA credentials rejected: reason = reason:
local database: user = user\

説明 このメッセージは、IPSec 接続または WebVPN 接続に関連付けられているユーザの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されたことを示します。詳細は *reason* フィールドに示されています。このイベントが表示されるのは、AAA トランザクションが外部 AAA サーバではなくローカル ユーザ データベースと行われる場合だけです。*user* は接続に関連付けられているユーザ名です。

推奨処置 不要です。

113018

エラー メッセージ %PIX|ASA-3-113018: User: *user*, Unsupported downloaded ACL
Entry: *ACL_entry*, Action: *action*

説明 サポートされていないフォーマットの ACL エントリが認証サーバからダウンロードされました。メッセージの値は次のとおりです。

- *user* : ログインを試みるユーザ。
- *ACL_entry* : 認証サーバからダウンロードされたサポートされていない ACL エントリ。
- *action* : サポートされていない ACL エントリに対して実行するアクション。

推奨処置 認証サーバの ACL エントリは、サポートされている ACL エントリ フォーマットに適合するように管理者が適切に変更する必要があります。

113019

エラー メッセージ %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*

説明 これは情報メッセージです。

group : グループ名

user : ユーザ名

peer_address : ピア アドレス

type : セッション タイプ (たとえば、IPSec/UDP)

duration : 接続時間

count : バイト数

reason : 切断の原因

推奨処置 処置は不要です。

113020

エラー メッセージ %PIX|ASA-3-113020: Kerberos error : Clock skew with server *ip_address* greater than 300 seconds

説明 このメッセージは、Kerberos サーバ経由の IPSec または WebVPN のユーザの認証が、セキュリティ アプライアンス のクロックとそのサーバのクロックが 5 分 (300 秒) 以上ずれているために失敗した場合に表示されます。この失敗が起こったときは、接続しようとしても拒否されます。

ip_address : Kerberos サーバの IP アドレス。

推奨処置 セキュリティ アプライアンス サーバと Kerberos サーバのクロックを同期させます。

114001

エラー メッセージ %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードを初期化できなかった場合に表示されます。

syslog_id : メッセージ識別子

error_string : I2C シリアルバス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアルバス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114002

エラー メッセージ %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error *error_string*).

このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードの SFP コネクタを初期化できなかった場合に表示されます。

syslog_id : メッセージ識別子

error_string : I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114003

エラー メッセージ %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードにキャッシュされたコマンドを実行できなかった場合に表示されます。

syslog_id : メッセージ識別子

error_string : I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114004

エラー メッセージ %ASA-6-114004: 4GE SSM I/O Initialization start.

説明 このメッセージは、4GE SSM I/O 初期化が開始されたことをユーザに通知するために表示されます。

syslog_id : メッセージ識別子

推奨処置 処置は不要です。

114005

エラー メッセージ %ASA-6-114005: 4GE SSM I/O Initialization end.

説明 このメッセージは、4GE SSM I/O 初期化が終了したことをユーザに通知するために表示されます。

syslog_id : メッセージ識別子

推奨処置 処置は不要です。

114006

エラー メッセージ %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのポート統計情報を取得できなかった場合に表示されます。

syslog_id : メッセージ識別子

error_string : I2C シリアルバス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアルバス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114007

エラー メッセージ %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードの現在のモジュール ステータス レジスタ情報を取得できなかった場合に表示されます。

syslog_id : メッセージ識別子

error_string : I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114008

エラー メッセージ %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.

説明 このメッセージは、I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのために、Up 状態へのリンク移行が 4GE SSM I/O カードで検出された後にシステムがポートをイネーブルにできなかった場合に表示されます。

syslog_id : メッセージ識別子

error_string : I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114009

エラーメッセージ %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのマルチキャスト アドレスを設定できなかった場合に表示されます。

syslog_id: メッセージ識別子

error_string: I2C シリアルバス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアルバス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114010

エラーメッセージ %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのマルチキャスト ハードウェア アドレスを設定できなかった場合に表示されます。

syslog_id: メッセージ識別子

error_string : I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114011

エラー メッセージ %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error *error_string*).

syslog_id : メッセージ識別子

error_string : I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのマルチキャスト アドレスを削除できなかった場合に表示されます。

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。

3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114012

エラーメッセージ %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error *error_string*).

syslog_id: メッセージ識別子

error_string: I2C シリアルバス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアルバス エラーは次のとおりです。

- 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

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのマルチキャスト ハードウェア アドレスを削除できなかった場合に表示されます。

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114013

エラーメッセージ %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードの MAC アドレス テーブルを設定できなかった場合に表示されます。

syslog_id: メッセージ識別子

error_string: I2C シリアルバス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアルバス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114014

エラー メッセージ %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error *error_string*).

syslog_id: メッセージ識別子

error_string: I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードの MAC アドレスを設定できなかった場合に表示されます。

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114015

エラー メッセージ %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error *error_string*).

syslog_id: メッセージ識別子

error_string: I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードの個別モードまたは混在モードを設定できなかった場合に表示されます。

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114016

エラー メッセージ %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error *error_string*).

syslog_id: メッセージ識別子

error_string: I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのマルチキャスト モードを設定できなかった場合に表示されます。

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114017

エラー メッセージ %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのためにシステムが 4GE SSM I/O カードのリンク ステータスを取得できなかった場合に表示されます。

syslog_id: メッセージ識別子

error_string: I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. システム管理者に通知します。
2. イベントに関連付けられているメッセージとエラーを記録して確認します。
3. システムで実行しているソフトウェアを再起動します。
4. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
5. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114018

エラー メッセージ %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error *error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのポート速度を設定できなかった場合に表示されます。

syslog_id: メッセージ識別子

error_string: I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114019

エラー メッセージ %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (*error error_string*).

説明 このメッセージは、I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードのメディア タイプを設定できなかった場合に表示されます。

syslog_id: メッセージ識別子

error_string: I2C シリアル バス エラーまたはスイッチ アクセス エラーのいずれかを示します。これは 10 進数のエラー コードです。I2C シリアル バス エラーは次のとおりです。

- 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

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. システムで実行しているソフトウェアを再起動します。
3. 電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114020

エラー メッセージ %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.

説明 このメッセージは、システムが4GE SSM I/O カードのポートリンク速度を検出できなかった場合に表示されます。

推奨処置 次の手順を実行します。

1. イベントに関連付けられているメッセージを記録して確認します。
2. 4GE SSM I/O カードをリセットし、ソフトウェアがイベントから自動的に回復するかどうか観察します。
3. ソフトウェアが自動的に回復しない場合は、電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

199001

エラー メッセージ %PIX|ASA-5-199001: Reload command executed from telnet (remote IP_address).

説明 このメッセージは、reload コマンドで Cisco ASA リブートを開始したホストのアドレスを記録します。

推奨処置 不要です。

199002

エラー メッセージ %PIX|ASA-6-199002: startup completed. Beginning operation.

説明 Cisco ASA が、その初期ブートおよびフラッシュ メモリ読み取りシーケンスを完了し、正常動作を開始する準備が整いました。



(注) このメッセージは、no logging message コマンドを使用してもブロックすることはできません。

推奨処置 不要です。

199003

エラー メッセージ %PIX|ASA-6-199003: Reducing link MTU dec.

説明 Cisco ASA が内部ネットワークよりも大きい MTU を使用している外部ネットワークからパケットを受信しました。その後 Cisco ASA は、適切な MTU をネゴシエートするため、ICMP メッセージをその外部ホストに送信しました。ログ メッセージには、ICMP メッセージのシーケンス番号が含まれています。

推奨処置 不要です。

199005

エラー メッセージ %PIX|ASA-6-199005: Startup begin

説明 Cisco ASA が起動しました。

推奨処置 不要です。

199006

エラー メッセージ %PIX|ASA-5-199006: Orderly reload started at *when* by *whom*.
Reload reason: *reason*

説明 このメッセージは、リロード動作が開始されたときに生成されます。

- *when* : 正常ロード動作が開始された時刻。時刻は、hh:mm:ss 時間帯 曜日 月 日 年という形式で表示されます。たとえば「13:23:45 UTC Sun Dec 28 2003」のようになります。
- *whom* : リロード スケジュールを設定したユーザまたはシステム。
- *reason* : リロードの原因。はっきりした原因が表示されない場合、文字列は *unspecified* になります。

推奨処置 ユーザによる処置は不要です。

199907

エラー メッセージ %PIX|ASA-5-1999007:IP detected an attached application using port *port* while removing context

説明 インターフェイスまたはコンテキストが削除された場合、すべてのアプリケーションはコンテキストまたはインターフェイス用のチャネルをすべてクローズする必要があります。このメッセージは、削除されたインターフェイスまたはアプリケーション用のすべてのチャネルをアプリケーションがクローズしていないか、またはクローズ中であることを示します。

推奨処置 不要です。

199908

エラー メッセージ %PIX|ASA-5-1999008:Protocol detected an attached application using local port *local_port* and destination port *dest_port*

説明 インターフェイスまたはコンテキストが削除された場合、すべてのアプリケーションはコンテキストまたはインターフェイス用のチャネルをすべてクローズする必要があります。このメッセージは、削除されたインターフェイスまたはアプリケーション用のすべてのチャネルをアプリケーションがクローズしていないか、またはクローズ中であることを示します。

推奨処置 不要です。

199909

エラー メッセージ %PIX|ASA-7-199009: ICMP detected an attached application while removing a context

説明 インターフェイスまたはコンテキストが削除された場合、すべてのアプリケーションはコンテキストまたはインターフェイス用のチャンネルをすべてクローズする必要があります。このメッセージは、削除されたインターフェイスまたはアプリケーション用のすべてのチャンネルをアプリケーションがクローズしていないか、またはクローズ中であることを示します。

推奨処置 不要です。

メッセージ 201002 ~ 217001

この項では、201002 から 217001 までのメッセージについて説明します。

201002

エラーメッセージ %PIX|ASA-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns

説明 これは接続関連のメッセージです。このメッセージは、指摘されたグローバル アドレスへの TCP 接続が最大数を越えた場合に表示されます。*econns* 変数は最大初期接続数であり、*nconns* 変数はスタティックまたは xlate に許可される最大接続数です。

推奨処置 `show static` コマンドまたは `show nat` コマンドを使用して、スタティック アドレスへの接続に課されている制限を確認します。制限は設定可能です。

201003

エラーメッセージ %PIX|ASA-2-201003: Embryonic limit exceeded nconns/limit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name

説明 これは、Cisco ASA へのトラフィックに関する接続関連のメッセージです。このメッセージは、指摘されたスタティック グローバル アドレスを持つ、指摘された外部アドレスから指摘されたローカル アドレスへの初期接続の数が初期接続の制限を超えた場合に表示されます。Cisco ASA への初期接続の制限に達すると、Cisco ASA は何としても受け入れようと試みますが、その接続に時間制限を課します。この状況により、たとえ Cisco ASA がビジー状態であっても、一部の接続が成功することがあります。*nconns* 変数は受信した初期接続の数を示し、*limit* 変数は `static` コマンドまたは `nat` コマンドに指定されている最大初期接続数を示します。

推奨処置 このメッセージは、メッセージ 201002 よりもさらに深刻なオーバーロードを示します。このオーバーロードは、SYN 攻撃、または正規のトラフィックの非常に重い負荷が原因となっている可能性があります。`show static` コマンドを使用して、スタティック アドレスへの初期接続に課されている制限を確認します。

201004

エラーメッセージ %PIX|ASA-3-201004: Too many UDP connections on {static|xlate} global_address! udp connections limit

説明 これは接続関連のメッセージです。このメッセージは、指摘されたグローバル アドレスへの UDP 接続が最大数を越えた場合に表示されます。*udp conn limit* 変数は、スタティックまたは変換に許可される UDP 接続の最大数です。

推奨処置 `show static` コマンドまたは `show nat` コマンドを使用して、スタティック アドレスへの接続に課されている制限を確認します。制限は設定可能です。

201005

エラー メッセージ %PIX|ASA-3-201005: FTP data connection failed for IP_address
IP_address

説明 Cisco ASA が、メモリ不足のため FTP のデータ接続を追跡するための構造を割り当てる
ことができませんでした。

推奨処置 メモリ使用量を減らすか、または増設メモリを購入します。

201006

エラー メッセージ %PIX|ASA-3-201006: RCMD backconnection failed for
IP_address/port

説明 これは接続関連のメッセージです。このメッセージは、メモリ不足のため Cisco ASA が
rsh コマンドに対する着信標準出力のための接続を事前割当できなかった場合に
表示されます。

推奨処置 rsh クライアント バージョンを確認します。Cisco ASA がサポートしているのは
Berkeley rsh だけです。メモリ使用量を減らすか、または増設メモリを購入することも
できます。

201008

エラー メッセージ %PIX|ASA-3-201008: The Cisco ASA is disallowing new
connections.

説明 このメッセージは、TCP システム ログ メッセージングをイネーブルにしても syslog サー
バに到達できない場合、または Cisco ASA Syslog Server (PFSS) を使用しており、Windows NT
システムのディスクが満杯になっている場合に表示されます。

推奨処置 TCP システム ログ メッセージングをディセーブルにします。PFSS を使用している
場合は、PFSS のある Windows NT システム上のスペースを解放します。さらに、syslog サーバ
が動作しており、Cisco ASA コンソールからそのホストに ping できることを確認します。次に、
TCP システム メッセージ ログギングを再開してトラフィックを許可します。

201009

エラー メッセージ %PIX|ASA-3-201009: TCP connection limit of number for host
IP_address on interface_name exceeded

説明 これは接続関連のメッセージです。このメッセージは、指摘されたスタティック アドレ
スへの接続が最大数を超えた場合に表示されます。number 変数は、IP_address 変数で指摘され
たホストに許可されている接続の最大数です。

推奨処置 show static コマンドおよび show nat コマンドを使用して、アドレスへの接続に課さ
れている制限を確認します。制限は設定可能です。

201010

エラー メッセージ %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*

説明 TCP 接続を確立しようとしたが、トラフィック クラスに対して `set connection embryonic-conn-max MPC` コマンドで設定されている初期接続の制限を超えたために失敗しました。

- *econns* : 設定したトラフィック クラスに関連付けられている初期接続の現在の数。
- *limit* : 設定した初期接続のトラフィック クラスの制限
- *dir* :
input : 接続を開始した最初のパケットはインターフェイス *interface_name* 上の入力パケットです。
output : 接続を開始した最初のパケットはインターフェイス *interface_name* 上の出力パケットです。
- *source_address/source_port* : 接続を開始したパケットの送信元 IP アドレスおよび送信元ポート。
- *dest_address/dest_port* : 接続を開始したパケットの宛先 IP アドレスおよび宛先ポート。
- *interface_name* : ポリシー制限が強制されているインターフェイス名。

推奨処置 不要です。

202001

エラー メッセージ %PIX|ASA-3-202001: Out of address translation slots!

説明 これは接続関連のメッセージです。このメッセージは、Cisco ASA に使用可能なアドレス変換スロットがなくなった場合に表示されます。

推奨処置 グローバルプールのサイズを確認し、内部のネットワーク クライアント数と比較します。PAT アドレスが必要になる可能性もあります。または、変換と接続のタイムアウト間隔を短くします。このエラー メッセージは、メモリ不足が原因で表示される可能性もあります。メモリ使用量を減らすか、または可能であれば増設メモリを購入します。

202005

エラー メッセージ %PIX|ASA-3-202005: Non-embryonic in embryonic list *outside_address/outside_port inside_address/inside_port*

説明 これは接続関連のメッセージです。このメッセージは、接続オブジェクト (xlate) が誤ったリストに入っている場合に表示されます。

推奨処置 Cisco TAC にお問い合わせください。

202011

エラー メッセージ %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*

説明 このメッセージは、TCP 接続または UDP 接続を作成しようとしたが、トラフィック クラスに対して **set connection conn-max MPC** コマンドで設定されている接続の制限を超えたために失敗した場合に表示されます。

- *econns* : 設定したトラフィック クラスに関連付けられている初期接続の現在の数。
- *limit* : 設定した初期接続のトラフィック クラスの制限
- *dir* :
input : 接続を開始した最初のパケットはインターフェイス *interface_name* 上の入力パケットです。
output : 接続を開始した最初のパケットはインターフェイス *interface_name* 上の出力パケットです。
- *source_address/source_port* : 接続を開始したパケットの送信元 IP アドレスおよび送信元ポート。
- *dest_address/dest_port* : 接続を開始したパケットの宛先 IP アドレスおよび宛先ポート。
- *interface_name* : ポリシー制限が強制されているインターフェイス名。

推奨処置 不要です。

208005

エラー メッセージ %PIX|ASA-3-208005: (*function:line_num*) clear command return code

説明 Cisco ASA が、フラッシュ メモリ内のコンフィギュレーションを消去しようとしたときに非ゼロ値 (内部エラー) を受信しました。このメッセージには、報告サブルーチンのファイル名および行番号が含まれています。

推奨処置 パフォーマンス上の理由から、エンドホストは IP フラグメントを投入しないように設定する必要があります。このコンフィギュレーションの変更は、NFS が原因と考えられます。読み取りサイズおよび書き込みサイズを NFS のインターフェイス MTU と等しく設定します。

209003

エラー メッセージ %PIX|ASA-4-209003: Fragment database limit of *number* exceeded: src = *source_address*, dest = *dest_address*, proto = *protocol*, id = *number*

説明 現在再組み立てを待っている IP フラグメントが多過ぎます。デフォルトでは、フラグメントの最大数は 200 です (最大値を大きくするには、『Cisco Security Appliance Command Reference』の **fragment size** コマンドを参照してください)。Cisco ASA は、同時に再組み立てできる IP フラグメントの数を制限します。この制約により、異常なネットワーク条件下で Cisco ASA のメモリが枯渇するのが防止されます。一般に、フラグメント化されたトラフィックは、混合トラフィック全体のわずかな割合に抑える必要があります。例外は、ほとんどがフラグメント化されたトラフィックである NFS over UDP のネットワーク環境の場合です。このタイプのトラ

フィックが Cisco ASA 経由で中継される場合、その代わりに NFS over TCP の使用を検討します。フラグメント化を防ぐには、『Cisco Security Appliance Command Reference』の `sysopt connection tcpmss bytes` コマンドを参照してください。

推奨処置 このメッセージが引き続き表示される場合は、DoS 攻撃（サービス拒絶攻撃）が進行している可能性があります。リモートピアの管理者またはアップストリームのプロバイダーにお問い合わせください。

209004

エラーメッセージ %PIX|ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number

説明 IP フラグメントの形式が誤っています。再組み立て済み IP パケットの合計サイズが、最大可能サイズの 65,535 バイトを超えています。

推奨処置 侵入イベントが進行している可能性があります。このメッセージが引き続き表示される場合は、リモートピアの管理者またはアップストリームのプロバイダーにお問い合わせください。

209005

エラーメッセージ %PIX|ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.

説明 Cisco ASA は、24 よりも多くのフラグメントにフラグメント化されている IP パケットを拒否します。詳細については、『Cisco Security Appliance Command Reference』の `fragment` コマンドを参照してください。

推奨処置 侵入イベントが進行している可能性があります。このメッセージが引き続き表示される場合は、リモートピアの管理者またはアップストリームのプロバイダーにお問い合わせください。`fragment chain xxx interface_name` コマンドを使用して、パケットあたりのフラグメントの数を変更できます。

210001

エラーメッセージ %PIX|ASA-3-210001: LU sw_module_name error = number

説明 ステートフル フェールオーバー エラーが発生しました。

推奨処置 Cisco ASA 経由のトラフィックが減少した後もこのエラーが引き続き表示される場合は、Cisco TAC にこのエラーを報告してください。

210002

エラー メッセージ %PIX|ASA-3-210002: LU allocate block (bytes) failed.

説明 ステートフル フェールオーバーが、ステートフル情報をスタンバイ Cisco ASA に送信するためのメモリのブロックを割り当てることができませんでした。

推奨処置 `show interface` コマンドを使用してフェールオーバー インターフェイスを調べて、その送信が正常であることを確認します。さらに、`show block` コマンドを使用して、現在のブロック メモリを調べます。現在使用可能なカウントが 0 になっているメモリのブロックがあれば、Cisco ASA ソフトウェアをリロードして失われたメモリのブロックを回復します。

210003

エラー メッセージ %PIX|ASA-3-210003: Unknown LU Object number

説明 ステートフル フェールオーバーが、サポートされていない Logical Update オブジェクトを受信したため、そのオブジェクトを処理できませんでした。これは、破損したメモリ、LAN 伝送、または他のイベントが原因となっている可能性があります。

推奨処置 このエラーがまれにしか表示されない場合は、処置は不要です。このエラーが頻繁に発生する場合は、ステートフル フェールオーバー リンク LAN 接続を確認します。エラーが不適切なフェールオーバー リンク LAN 接続のためでない場合は、外部ユーザが保護されているネットワークを危険にさらそうとしていないかどうか判別します。誤って設定したクライアントがないかどうか確認します。

210005

エラー メッセージ %PIX|ASA-3-210005: LU allocate connection failed

説明 ステートフル フェールオーバーが、スタンバイ装置に新しい接続を割り当てられません。これは、Cisco ASA 内の使用可能な RAM メモリがほとんどないか、またはまったくないことが原因となっている可能性があります。

推奨処置 `show memory` コマンドを使用して Cisco ASA システムの空きメモリをチェックし、利用可能なメモリを確認します。利用可能なメモリがない場合は、さらに物理メモリを Cisco ASA に追加します。

210006

エラー メッセージ %PIX|ASA-3-210006: LU look NAT for IP_address failed

説明 ステートフル フェールオーバーが、スタンバイ装置上で IP アドレス用の NAT グループを検出できませんでした。アクティブおよびスタンバイの Cisco ASA 装置が同期していない可能性があります。

推奨処置 アクティブ装置で `write standby` コマンドを使用して、システム メモリをスタンバイ装置に同期させます。

210007

エラー メッセージ %PIX|ASA-3-210007: LU allocate xlate failed

説明 ステートフル フェールオーバーが、変換 (xlate) スロット レコードを割り当てることができませんでした。

推奨処置 `show memory` コマンドを使用して Cisco ASA システムの空きメモリをチェックし、利用可能なメモリを確認します。利用可能なメモリがない場合は、さらに物理メモリを追加します。

210008

エラー メッセージ %PIX|ASA-3-210008: LU no xlate for *inside_address/inside_port*
outside_address/outside_port

説明 ステートフル フェールオーバー接続の変換スロット (xlate) レコードが検出できませんでした。接続情報が処理できません。

推奨処置 アクティブ装置で `write standby` コマンドを入力して、システムメモリをアクティブ装置とスタンバイ装置との間で同期させます。

210010

エラー メッセージ %PIX|ASA-3-210010: LU make UDP connection for
outside_address:outside_port inside_address:inside_port failed

説明 ステートフル フェールオーバーが、UDP 接続に新しいレコードを割り当てることができませんでした。

推奨処置 `show memory` コマンドを使用して Cisco ASA システムの空きメモリをチェックし、利用可能なメモリを確認します。利用可能なメモリがない場合は、さらに物理メモリを追加します。

210020

エラー メッセージ %PIX|ASA-3-210020: LU PAT port *port* reserve failed

説明 ステートフル フェールオーバーが、使用中の特定の PAT アドレスを割り当てることができません。

推奨処置 アクティブ装置で `write standby` コマンドを入力して、システムメモリをアクティブ装置とスタンバイ装置との間で同期させます。

210021

エラー メッセージ %PIX|ASA-3-210021: LU create static xlate *global_address* ifc *interface_name* failed

説明 ステートフル フェールオーバーが変換スロット (xlate) を作成できません。

推奨処置 アクティブ装置で **write standby** コマンドを入力して、システム メモリをアクティブ装置とスタンバイ装置との間で同期させます。

210022

エラー メッセージ %PIX|ASA-6-210022: LU missed *number* updates

説明 ステートフル フェールオーバーが、スタンバイ装置に送信された各レコードにシーケンス番号を割り当てます。受信したレコードのシーケンス番号が最後にアップデートされたレコードと順序が狂っている場合、その間の情報が失われたものとみなされ、このエラーメッセージが送信されます。

推奨処置 LAN の中断がない場合は、両方の Cisco ASA 装置の利用可能なメモリをチェックして、ステートフル情報を処理するのに十分なメモリがあることを確認します。show failover コマンドを使用して、ステートフル情報のアップデートの品質を監視します。

211001

エラー メッセージ %PIX|ASA-3-211001: Memory allocation Error

説明 RAM システム メモリの割り当てに失敗しました。

推奨処置 このメッセージが一定期間ごとに発生する場合は、無視してかまいません。頻繁に繰り返される場合は、Cisco TAC にお問い合わせください。

211003

エラー メッセージ %PIX|ASA-3-211003: CPU utilization for *number* seconds = *percent*

説明 このメッセージは、CPU 使用率が数秒間 100 パーセントを超えた場合に表示されます。

推奨処置 このメッセージが一定期間ごとに発生する場合は、無視してかまいません。頻繁に繰り返される場合は、Cisco TAC にお問い合わせください。

212001

エラー メッセージ %PIX|ASA-3-212001: Unable to open SNMP channel (UDP port *port*) on interface *interface_number*, error code = *code*

説明 これは SNMP メッセージです。このメッセージは、Cisco ASA がこのインターフェイス上にある SNMP 管理ステーションから Cisco ASA 向けの SNMP 要求を受信できないことを報告します。これは、Cisco ASA を介してインターフェイスを通過する SNMP トラフィックに影響しません。

エラー コード -1 は、Cisco ASA がそのインターフェイスに対して SNMP トランスポートを開けなかったことを示します。このエラーは、SNMP がクエリーを受け入れるポートを別の機能ですでに使われているポートに変更しようとユーザがした場合に発生する可能性があります。この場合、SNMP が使用するポートは、着信 SNMP クエリー用のデフォルト ポート (UDP/161) にリセットされます。

エラー コード -2 は、Cisco ASA がそのインターフェイスに対して SNMP トランスポートをバインドできなかったことを示します。

推奨処置 トラフィック量が少ないときに、Cisco ASA がリソースの一部を再要求してから、対象となるインターフェイスに対して `snmp-server host` コマンドを再入力します。

212002

エラー メッセージ %PIX|ASA-3-212002: Unable to open SNMP trap channel (UDP port *port*) on interface *interface_number*, error code = *code*

説明 これは SNMP メッセージです。このメッセージは、Cisco ASA が Cisco ASA からこのインターフェイス上にある SNMP 管理ステーションに自分の SNMP トラップを送信できないことを報告します。これは、Cisco ASA を介してインターフェイスを通過する SNMP トラフィックに影響しません。

エラー コード -1 は、Cisco ASA がそのインターフェイスに対して SNMP トランスポートを開けなかったことを示します。

エラー コード -2 は、Cisco ASA がそのインターフェイスに対して SNMP トランスポートをバインドできなかったことを示します。

推奨処置 トラフィック量が少ないときに、Cisco ASA がリソースの一部を再要求してから、対象となるインターフェイスに対して `snmp-server host` コマンドを再入力します。

212003

エラー メッセージ %PIX|ASA-3-212003: Unable to receive an SNMP request on interface *interface_number*, error code = *code*, will try again.

説明 これは SNMP メッセージです。このメッセージは、指摘されたインターフェイス上の Cisco ASA 向けの SNMP 要求を受信する際の内部エラーが原因で表示されます。

推奨処置 不要です。Cisco ASA SNMP エージェントは元に戻って次の SNMP 要求を待ちます。

212004

エラー メッセージ %PIX|ASA-3-212004: Unable to send an SNMP response to IP Address *IP_address* Port *port* interface *interface_number*, error code = *code*

説明 これは SNMP メッセージです。このメッセージは、指摘されたインターフェイス上の指摘されたホストに Cisco ASA から SNMP 応答を送信する際の内部エラーが原因で表示されます。

推奨処置 不要です。

212005

エラー メッセージ %PIX|ASA-3-212005: incoming SNMP request (*number* bytes) on interface *interface_name* exceeds data buffer size, discarding this SNMP request.

説明 これは SNMP メッセージです。このメッセージは、着信 SNMP メッセージ、つまり Cisco ASA に向けられた要求の長さが、内部処理中に要求を格納するために使用される内部データバッファのサイズ (512 バイト) を超えていることを報告します。Cisco ASA はこの要求を処理できません。この状況は、インターフェイスを使用して Cisco ASA を通過する SNMP トラフィックに影響しません。

推奨処置 SNMP 管理ステーションに長さの短い要求を再送信させます。たとえば、1つの要求で複数の MIB 変数にクエリーを実行するのではなく、1つの要求で1つの MIB 変数のみにクエリーを実行するようにします。SNMP マネージャ ソフトウェアのコンフィギュレーションの修正が必要になる可能性もあります。

212006

エラー メッセージ %PIX|ASA-3-212006: Dropping SNMP request from *source_address/source_port* to *interface_name:dest_address/dest_port* because: *reason*.

説明 これは SNMP メッセージです。このメッセージは、デバイスが次の理由からそのデバイスへの SNMP 要求を処理できない場合に表示されます。

- snmp-server がディセーブルになっている
- SNMPv3 がサポートされていない

推奨処置 snmp-server enable コマンドを発行して、SNMP デーモンが組み込まれることを確認します。デバイスが処理するのは、SNMPv1 パケットおよび SNMPv2c パケットだけです。

213001

エラー メッセージ %PIX|ASA-3-213001: PPTP control daemon socket io *string*, errno = *number*.

説明 内部 TCP ソケット I/O エラーが発生しました。

推奨処置 Cisco TAC にお問い合わせください。

213002

エラー メッセージ %PIX|ASA-3-213002: PPTP tunnel hashtable insert failed, peer = *IP_address*.

説明 新しい PPTP トンネルの作成中に、内部ソフトウェア エラーが発生しました。

推奨処置 Cisco TAC にお問い合わせください。

213003

エラーメッセージ %PIX|ASA-3-213003: PPP virtual interface *interface_number* isn't opened.

説明 PPP 仮想インターフェイスのクローズ中に、内部ソフトウェア エラーが発生しました。

推奨処置 Cisco TAC にお問い合わせください。

213004

エラーメッセージ %PIX|ASA-3-213004: PPP virtual interface *interface_number* client ip allocation failed.

説明 IP アドレスを PPTP クライアントに割り当てている間に内部ソフトウェア エラーが発生しました。

推奨処置 このエラーは、IP ローカル アドレス プールが枯渇した場合に発生します。ip local pool コマンドを使用して、さらに大きいプールを割り当てることを検討します。

214001

エラーメッセージ %PIX|ASA-2-214001: Terminating manager session from *IP_address* on interface *interface_name*. Reason: incoming encrypted data (*number* bytes) longer than *number* bytes

説明 Cisco ASA 管理ポート向けの着信暗号化データ パケットは、パケット長が指摘された上限を超えていることを示します。これは敵対イベントの場合があります。Cisco ASA は、ただちにこの管理接続を終了します。

推奨処置 管理接続が Cisco Secure Policy Manager によって開始されたことを確認します。

215001

エラーメッセージ %PIX|ASA-2-215001:Bad route_compress() call, sdb= *number*

説明 内部ソフトウェア エラーが発生しました。

推奨処置 Cisco TAC にお問い合わせください。

217001

エラーメッセージ %PIX|ASA-2-217001: No memory for *string* in *string*

説明 メモリ不足が原因で動作が失敗しました。

推奨処置 十分なメモリが存在する場合は、エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

216002

エラー メッセージ PIX|ASA-3-216002: Unexpected event (major: *major_id* , minor: *minor_id*) received by *task_string* in *function* at line: *line_num*

説明 このメッセージは、タスクがイベント通知に登録したが、そのタスクが特定のイベントを処理できない場合に表示されます。監視できるイベントには、キュー、プーリアン、タイマー サービスなどに関連付けられているイベントが含まれます。登録されているイベントのいずれかが発生した場合、スケジューラはタスクを再起動してイベントを処理します。このメッセージは、予期しないイベントがタスクを再起動したので、タスクがそのイベントの処理方法を認識していない場合に生成されます。

イベントが未処理のままになっている場合、そのイベントが頻繁にタスクを再起動して処理されていることを確認しますが、これは正常状態では発生してはならないことです。このメッセージが表示された場合、必ずしもボックスが使用できないという意味ではなく、問題が発生し、調査する必要があることを意味しています。

major_id : イベント識別子

minor_id : イベント識別子

task_string : タスクが自分自身を認識するために通過させたカスタム スtring

function : 予期しないイベントを受信した機能

line_num : コード中の行番号

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

216003

エラー メッセージ %PIX|ASA-3-216003: Unrecognized timer *timer_ptr* , *timer_id* received by *task_string* in *function* at line: *line_num*

説明 このメッセージは、予期しないタイマー イベントがタスクを再起動し、タスクがそのイベントの処理方法を認識していない場合に表示されます。タスクは、一連のタイマー サービスをスケジューラに登録できます。タイマーのいずれかが期限満了になった場合、スケジューラはタスクを再起動してアクションを実行します。このメッセージは、認識できないタイマー イベントによってタスクが再起動された場合に生成されます。

期限満了になったタイマーは、タスクが未処理のままになっている場合、途切れることなくタスクを再起動して処理されていることを確認しますが、これは望ましいことではありません。これは正常状態では発生してはならないことです。このメッセージが表示された場合、必ずしもボックスが使用できないという意味ではなく、問題が発生し、調査する必要があることを意味しています。

timer_ptr : タイマーへのポインタ

timer_id : タイマー識別子

task_string : タスクが自分自身を認識するために通過させたカスタム スtring

function : 予期しないイベントを受信した機能

line_num : コード中の行番号

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

メッセージ 302003 ~ 326028

この項では、302003 から 326028 までのメッセージについて説明します。

302003

エラー メッセージ %PIX|ASA-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port

説明 これは接続関連のメッセージです。このメッセージは、H.245 接続が *outside_address* から *inside_address* に向けて開始されている場合に表示されます。このメッセージが発生するのは、Cisco ASA が Intel インターネット電話の使用を検出した場合だけです。外部ポートは、Cisco ASA 外部からの接続にしか表示されません。ローカル ポート値 (内部ポート) は、内部インターフェイスで開始された接続にしか表示されません。

推奨処置 不要です。

302004

エラー メッセージ %PIX|ASA-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port

説明 これは接続関連のメッセージです。このメッセージは、H.323 UDP バック接続がローカルアドレス (*inside_address*) から外部アドレス (*outside_address*) に事前割り当てされている場合に表示されます。このメッセージが発生するのは、Cisco ASA が Intel インターネット電話の使用を検出した場合だけです。外部ポート (*outside_port*) は、Cisco ASA 外部からの接続にしか表示されません。ローカル ポート値 (*inside_port*) は、内部インターフェイスで開始された接続にしか表示されません。

推奨処置 不要です。

302009

エラー メッセージ %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

説明 これは接続関連のメッセージです。このメッセージは、フェールオーバー後に TCP 接続が再確立された後に表示されます。同期パケットは相手側 Cisco ASA に送信されません。*outside_address* IP アドレスは外部ホストであり、*global_address* IP アドレスは低セキュリティレベルのインターフェイス上のグローバルアドレスであり、*inside_address* IP アドレスは高セキュリティレベルのインターフェイス上の Cisco ASA の「背後にある」ローカル IP アドレスです。

推奨処置 不要です。

302010

エラー メッセージ %PIX|ASA-6-302010: *connections* in use, *connections* most used

説明 これは接続関連のメッセージです。このメッセージは、TCP 接続が再開された後に表示されます。*connections* は接続の数です。

推奨処置 不要です。

302012

エラー メッセージ %PIX|ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr *IP_address/port* to laddr *IP_address*

説明 H.225 二次チャネルは事前割り当て済みです。

推奨処置 不要です。

302013

エラー メッセージ %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*]

説明 2つのホスト間の TCP 接続スロットが作成されました。

- *connection_id* は、固有の識別子です。
- *interface*、*real-address*、*real-port* は、実際のソケットを特定します。
- *mapped-address*、*mapped-port* は、マッピングされたソケットを特定します。
- *user* は、ユーザの AAA の名前です。

inbound が表示されている場合、元の制御接続は外部から開始されています。たとえば、FTP の場合、元の制御チャネルが着信であれば、すべてのデータ転送チャネルは着信です。*outbound* が表示されている場合、元の制御接続は内部から開始されています。

推奨処置 不要です。

302014

エラー メッセージ %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*]

説明 2つのホスト間の TCP 接続が削除されました。メッセージの値は次のとおりです。

- *connection id* は、固有の識別子です。
- *interface*、*real-address*、*real-port* は、実際のソケットを特定します。
- *duration* は、接続のライフタイムです。
- *bytes* は、接続中のデータ転送量です。
- *user* は、ユーザの AAA の名前です。

reason 変数は、接続を終了させるアクションを示します。*reason* 変数は、表 2-2 に示されている TCP 終了の原因の 1 つが設定されています。

表 2-2 TCP 終了の原因

原因	説明
Conn-timeout	接続は、設定されているアイドル タイムアウトよりも長時間アイドルであったため終了しました。
Deny Terminate	フローは、アプリケーション検査によって終了されました。
FIN Timeout	最終 ACK を 10 分間待機した後、またはハーフクローズ タイムアウト後の強制終了。
Flow closed by inspection	フローは、検査機能によって終了されました。
Flow terminated by IPS	フローは、IPS によって終了されました。
Flow reset by IPS	フローは、IPS によってリセットされました。
Invalid SYN	SYN パケットが無効。
Idle Timeout	接続は、タイムアウト値よりも長時間アイドルであったためタイムアウトしました。
IPS fail-close	フローは、IPS カードのダウンのため終了されました。
SYN Control	誤った側からのバック チャネル開始。
SYN Timeout	3 ウェイ ハンドシェイクの完了を 2 分間待機した後の強制終了。
TCP bad retransmission	不良 TCP 再送が原因で接続は終了しました。
TCP FINs	正常なクローズ ダウン シーケンス。
TCP Invalid SYN	無効な TCP SYN パケット。
TCP Reset-I	内部からリセットされました。
TCP Reset-O	外部からリセットされました。
TCP segment partial overlap	部分的に重複するセグメントを検出しました。
TCP unexpected window size variation	TCP ウィンドウ サイズに変動があるため接続は終了しました。
Tunnel has been torn down	トンネルがダウンしているため、フローは終了しました。
Unauth Deny	URL フィルタにより拒否されました。
Unknown	その他の各種エラー。
Xlate Clear	コマンドライン削除

推奨処置 不要です。

302015

エラー メッセージ %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)]

説明 2 つのホスト間の UDP 接続スロットが作成されました。メッセージの値は次のとおりです。

- connection number : 固有の識別子。
- interface、real_address、real_port : 実際のソケット。

- *mapped_address/mapped_port* : マッピングされているソケット。
- *user* : ユーザの AAA の名前です。

inbound が表示されている場合、元の制御接続は外部から開始されています。たとえば、UDP の場合、元の制御チャンネルが着信であれば、すべてのデータ転送チャンネルは着信です。*outbound* が表示されている場合、元の制御接続は内部から開始されています。

推奨処置 不要です。

302016

エラー メッセージ %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*)]

説明 2つのホスト間の UDP 接続スロットが削除されました。メッセージの値は次のとおりです。

- *connection number* は、一意の識別子です。
- *interface*、*real_address*、*real_port* は、実際のソケットです。
- *time* は、接続のライフタイムです。
- *bytes* は、接続中のデータ転送量です。
- *connection id* は、固有の識別子です。
- *interface*、*real_address*、*real_port* は、実際のソケットです。
- *duration* は、接続のライフタイムです。
- *bytes* は、接続中のデータ転送量です。
- *user* は、ユーザの AAA の名前です。

推奨処置 不要です。

302017

エラー メッセージ %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*)]

説明 2つのホスト間の GRE 接続スロットが作成されました。*id* は、固有の識別子です。*interface*、*real_address*、*real_cid* タプルは、2つのシンプレックス PPTP GRE ストリームのうちの1つを特定します。括弧付きの *translated_address*、*translated_cid* タプルは、NAT で変換された値を特定します。

inbound が表示されている場合、接続は着信だけに使用できます。*outbound* が表示されている場合、接続は発信だけに使用できます。メッセージの値は次のとおりです。

- *id* : 接続を識別するための一意の番号。
- *inbound* : 制御接続は着信 PPTP GRE フロー用です。
- *outbound* : 制御接続は発信 PPTP GRE フロー用です。
- *interface_name* : インターフェイス名。

- *real_address* : 実際のホストの IP アドレス。
- *real_cid* : 変換されてない接続の call-ID。
- *translated_address* : 変換後の IP アドレス。
- *translated_cid* : 変換されたコール。
- *user* : AAA のユーザ名。

推奨処置 これは情報メッセージです。

302018

エラー メッセージ %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*]

説明 2つのホスト間の GRE 接続スロットが削除されました。*interface*、*real_address*、*real_port* タプルは、実際のソケットを特定します。*Duration* は、接続のライフタイムとみなされます。メッセージの値は次のとおりです。

- *id* : 接続を識別するための一意の番号。
- *interface* : インターフェイス名。
- *real_address* : 実際のホストの IP アドレス。
- *real_port* : 実際のホストのポート番号。
- *hh:mm:ss* : 時 : 分 : 秒の形式の時間。
- *bytes* : GRE セッションで転送された PPP バイトの数。
- *reason* : 接続が終了された原因。
- *user* : AAA のユーザ名。

推奨処置 これは情報メッセージです。

302019

エラー メッセージ %PIX|ASA-3-302019: H.323 *library_name* ASN Library failed to initialize, error code *number*

説明 Cisco ASA が H.323 メッセージのデコードに使用する指摘された ASN ライブラリの初期化に失敗しました。Cisco ASA は到着する H.323 パケットをデコードも検査もできません。Cisco ASA は、何も修正を加えずに H.323 パケットが通過できるようにします。次の H.323 メッセージが到着すると、Cisco ASA はライブラリを再度初期化しようとします。

推奨処置 このメッセージが特定のライブラリに対して始終生成される場合は、Cisco TAC にお問い合わせのうえ、すべてのログメッセージ (タイムスタンプ付きが望ましい) を送付してください。

302020

エラー メッセージ %PIX|ASA-6-302020: Built {in | out}bound ICMP connection for faddr {faddr | icmp_seq_num} gaddr {gaddr | cmp_type} laddr laddr

説明 fixup protocol icmp コマンドを使用してステートフル ICMP をイネーブルにしたときに、ICMP セッションがファーストパスで確立されました。

推奨処置 不要です。

302021

エラー メッセージ %PIX|ASA-6-302021: Teardown ICMP connection for faddr {faddr | icmp_seq_num} gaddr {gaddr | cmp_type} laddr laddr

説明 fixup protocol icmp コマンドを使用してステートフル ICMP をイネーブルにしたときに、ICMP セッションがファーストパスで削除されました。

推奨処置 不要です。

302302

エラー メッセージ %PIX|ASA-3-302302: ACL = deny; no sa created

説明 IPSec プロキシがミスマッチです。ネゴシエートした SA のプロキシ ホストは、deny access-list コマンド ポリシーに対応します。

推奨処置 コンフィギュレーションの access-list コマンド文を確認します。ピアの管理者にお問い合わせください。

303002

エラー メッセージ %PIX|ASA-6-303002: source_address {Stored|Retrieved} dest_address: mapped_address

説明 これは FTP/URL メッセージです。このメッセージは、指摘されたホストが指摘された FTP サイトからデータを格納または取得しようとした場合に表示されます。

推奨処置 不要です。

303003

エラー メッセージ %PIX|ASA-6-303003: FTP cmd_name command denied - failed strict inspection, terminating connection from source_interface:source_address/source_port to dest_interface:dest_address/dest_port

説明 このメッセージは、FTP トラフィックに厳密な検査を使用している場合に生成されます。これは、FTP 要求コマンドが ftp-map コマンドからの厳密な FTP 検査ポリシーによって拒否された場合に表示されます。

推奨処置 不要です。

303004

エラーメッセージ %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*

説明 このメッセージは、FTP トラフィックに厳密な FTP 検査を使用している場合に表示されます。これは、FTP 要求メッセージが装置に認識されないコマンドを含んでいる場合に表示されます。

推奨処置 不要です。

304001

エラーメッセージ %PIX|ASA-5-304001: user *source_address* Accessed {JAVA URL|URL} *dest_address: url*.

説明 これは FTP/URL メッセージです。このメッセージは、指摘されたホストが指摘された URL にアクセスしようとした場合に表示されます。

推奨処置 不要です。

304002

エラーメッセージ %PIX|ASA-5-304002: Access denied URL *chars* SRC *IP_address* DEST *IP_address: chars*

説明 これは FTP/URL メッセージです。このメッセージは、送信元アドレスから指摘された URL または FTP サイトへのアクセスが拒否された場合に表示されます。

推奨処置 不要です。

304003

エラーメッセージ %PIX|ASA-3-304003: URL Server *IP_address* timed out URL *url*

説明 URL サーバがタイムアウトになっています。

推奨処置 不要です。

304004

エラーメッセージ %PIX|ASA-6-304004: URL Server *IP_address* request failed URL *url*

説明 これは FTP/URL メッセージです。このメッセージは、Websense サーバ要求が失敗した場合に表示されます。

推奨処置 不要です。

304005

エラー メッセージ %PIX|ASA-7-304005: URL Server *IP_address* request pending URL *url*

説明 これは FTP/URL メッセージです。このメッセージは、Websense サーバ要求が保留中の場合に表示されます。

推奨処置 不要です。

304006

エラー メッセージ %PIX|ASA-3-304006: URL Server *IP_address* not responding

説明 これは FTP/URL メッセージです。Websense サーバはアクセスに使用できません。Cisco ASA は、Websense サーバがインストールされている唯一のサーバである場合は同サーバに、または複数のサーバがある場合は別のサーバに、アクセスしようとします。

推奨処置 不要です。

304007

エラー メッセージ %PIX|ASA-2-304007: URL Server *IP_address* not responding, ENTERING ALLOW mode.

説明 これは FTP/URL メッセージです。このメッセージは、**filter** コマンドの **allow** オプションを使用し、Websense サーバが応答しなかった場合に表示されます。Cisco ASA は、サーバが使用できない間すべての Web 要求がフィルタリングせずに継続できるようにします。

推奨処置 不要です。

304008

エラー メッセージ %PIX|ASA-2-304008: LEAVING ALLOW mode, URL Server is up.

説明 これは FTP/URL メッセージです。このメッセージは、**filter** コマンドの **allow** オプションを使用し、Cisco ASA が、以前は応答しなかった Websense サーバから応答メッセージを受け取った場合に表示されます。この応答メッセージにより Cisco ASA は exits the allow モードを終了します。これで URL フィルタリング機能が再びイネーブルになります。

推奨処置 不要です。

304009

エラー メッセージ %PIX|ASA-7-304009: Ran out of buffer blocks specified by url-block command

説明 URL 保留バッファ ブロックが領域を使い切りました。

推奨処置 **url-block block *block_size*** コマンドを入力して、バッファ ブロック サイズを変更します。

305005

エラー メッセージ %PIX|ASA-3-305005: No translation group found for protocol
src interface_name:dest_address/dest_port dst interface_name:source_address/source_port

説明 パケットがどの発信 **nat** コマンド規則とも一致しません。

推奨処置 このメッセージはコンフィギュレーション エラーを示します。送信元ホストにダイナミック NAT が望ましい場合は、**nat** コマンドが送信元 IP アドレスと一致することを確認します。送信元ホストにスタティック NAT が望ましい場合は、**static** コマンドのローカル IP アドレスが一致することを確認します。送信元ホストに NAT が望ましくない場合は、NAT 0 ACL にバインドされている ACL を確認します。

305006

エラー メッセージ %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

説明 プロトコル (UDP、TCP、または ICMP) が Cisco ASA 経由で変換を作成できませんでした。このメッセージは、ネットワーク アドレスまたはブロードキャスト アドレスに向けたパケットを Cisco ASA が許可しないよう要求した警告 CSCdr0063 に対する解決策と考えられます。Cisco ASA は、**static** コマンド文で明示的に識別されるアドレスに対してこのチェックを行います。変更により、着信トラフィックに対して Cisco ASA は、ネットワーク アドレスまたはブロードキャスト アドレスと特定された宛先 IP アドレスの変換を拒否します。

Cisco ASA は、すべての ICMP メッセージ タイプに PAT を適用するのではなく、ICMP エコーとエコー応答パケット (タイプ 8 と 0) に限り PAT を適用します。特に、ICMP エコーまたはエコー応答だけが、PAT xlate を作成します。したがって、他の ICMP メッセージ タイプが廃棄されるとき、システム ログメッセージ 305006 が生成されます (Cisco ASA 上で)。

Cisco ASA は、設定済み **static** コマンド文のグローバル IP とマスクを利用して、標準 IP アドレスを、ネットワーク IP アドレスまたはブロードキャスト IP アドレスと区別します。グローバル IP アドレスが、一致するネットワーク マスクを持つ有効なネットワーク アドレスである場合、Cisco ASA は着信パケットのネットワーク IP アドレスまたはブロードキャスト IP アドレスに対して変換を作成しません。

次に例を示します。

```
static (inside,outside) 10.2.2.128 10.1.1.128 netmask 255.255.255.128
```

グローバル アドレス 10.2.2.128 はネットワーク アドレスとして応答され、10.2.2.255 はブロードキャスト アドレスとして応答されます。既存の変換がない場合 Cisco ASA は、10.2.2.128 または 10.2.2.255 向けの着信パケットを拒否して、これをシステム ログメッセージに記録します。

疑わしい IP がホスト IP である場合、サブネット スタティックの直前にホスト マスクをもつ別の **static** コマンド文を設定します (**static** コマンド文に対する最初の一致規則)。次のスタティックでは、Cisco ASA がホスト アドレスとして 10.2.2.128 に応答します。

```
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
```

変換は、疑わしい IP アドレスを持つ内部ホストで開始されるトラフィックによって作成される可能性があります。Cisco ASA はネットワーク IP アドレスまたはブロードキャスト IP アドレスを重複したサブネット スタティック コンフィギュレーションを持つホスト IP とみなすので、両方の **static** コマンド文のネットワーク アドレス変換は同じである必要があります。

推奨処置 不要です。

305007

エラー メッセージ %PIX|ASA-6-305007: addrpool_free(): Orphan IP *IP_address* on interface *interface_number*

説明 Cisco ASA が、自分のグローバル プールで見つけれないアドレスを変換しようとした。Cisco ASA は、アドレスが削除されているとして、要求を廃棄します。

推奨処置 不要です。

305008

エラー メッセージ %PIX|ASA-3-305008: Free unallocated global IP address.

説明 Cisco ASA カーネルは、割り当てられていないグローバル IP アドレスを解放してアドレス プールに戻そうとしたときに、不整合状態を検出しました。この異常状態は、Cisco ASA がステートフル フェールオーバー セットアップを実行中で、一部の内部状態がアクティブ装置とスタンバイ装置との間で瞬間的に同期していない場合に発生する可能性があります。この状態は破局的なものではなく、同期は自動的に回復します。

推奨処置 このメッセージが引き続き表示される場合は、Cisco TAC にこの状態を報告してください。

305009

エラー メッセージ %PIX|ASA-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address to interface_name:mapped_address

説明 アドレス変換スロットが作成されました。スロットは、ローカル側からグローバル側に送信元アドレスを変換します。逆に、スロットは、グローバル側からローカル側に宛先アドレスを変換します。

推奨処置 不要です。

305010

エラー メッセージ %PIX|ASA-6-305010: Teardown {dynamic|static} translation from interface_name:real_address to interface_name:mapped_address duration time

説明 アドレス変換スロットが削除されました。

推奨処置 不要です。

305011

エラー メッセージ %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*

説明 TCP、UDP、または ICMP アドレス変換スロットが作成されました。スロットは、ローカル側からグローバル側に送信元ソケットを変換します。逆に、スロットは、グローバル側からローカル側に宛先ソケットを変換します。

推奨処置 不要です。

305012

エラー メッセージ %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*

説明 アドレス変換スロットが削除されました。

推奨処置 不要です。

308001

エラー メッセージ %PIX|ASA-6-308001: console enable password incorrect for *number* tries (from *IP_address*)

説明 これは Cisco ASA 管理メッセージです。このメッセージは、特権モードに入るためにユーザがパスワードを指摘された回数だけ誤って入力した後に表示されます。最大試行回数は 3 回です。

推奨処置 パスワードを確認し、再度試行します。

308002

エラー メッセージ %PIX|ASA-4-308002: static *global_address inside_address netmask netmask* overlapped with *global_address inside_address*

説明 1 つまたは複数の static コマンド文の IP アドレスが重複しています。*global_address* は低セキュリティ レベルのインターフェイス上のアドレスであるグローバル アドレスであり、*inside_address* は高セキュリティ レベルのインターフェイス上のアドレスであるローカルアドレスです。

推奨処置 show static コマンドを使用してコンフィギュレーションの static コマンド文を表示し、重複しているコマンドを修正します。最も一般的な重複は、10.1.1.0 などのネットワーク アドレスを指定して、別の static コマンドで 10.1.1.5 などその範囲内にあるホストを指定する場合に発生します。

311001

エラー メッセージ %PIX|ASA-6-311001: LU loading standby start

説明 スタンバイ Cisco ASA が最初にオンラインになるときに、ステートフル フェールオーバー アップデート情報がスタンバイ Cisco ASA に送信されました。

推奨処置 不要です。

311002

エラー メッセージ %PIX|ASA-6-311002: LU loading standby end

説明 ステートフル フェールオーバー アップデート情報が、スタンバイ Cisco ASA への送信を停止しました。

推奨処置 不要です。

311003

エラー メッセージ %PIX|ASA-6-311003: LU recv thread up

説明 アップデート肯定応答がスタンバイ Cisco ASA から受信されました。

推奨処置 不要です。

311004

エラー メッセージ %PIX|ASA-6-311004: LU xmit thread up

説明 このメッセージは、ステートフル フェールオーバー アップデートがスタンバイ Cisco ASA に送信される場合に表示されます。

推奨処置 不要です。

312001

エラー メッセージ %PIX|ASA-6-312001: RIP hdr failed from *IP_address*: cmd=*string*, version=*number* domain=*string* on interface *interface_name*

説明 Cisco ASA が応答以外のオペレーション コードを持つ RIP メッセージを受信し、メッセージはこのインターフェイスで予想されるバージョン番号とは異なる番号を持ち、ルーティングドメインのエントリは非ゼロでした。

推奨処置 これは情報メッセージですが、別の RIP 装置が Cisco ASA と通信するように正しく設定されていないことを示す可能性もあります。

313001

エラー メッセージ %PIX|ASA-3-313001: Denied ICMP type=*number*, code=*code* from *IP_address* on interface *interface_name*

説明 icmp コマンドをアクセスリストと共に使用する場合、最初に一致したエントリが許可エントリであれば、その ICMP パケットは処理が続けられます。最初に一致したエントリが拒否エントリの場合、またはエントリが一致しなかった場合は、Cisco ASA がその ICMP パケットを廃棄し、このシステム ログ メッセージを生成します。icmp コマンドは、インターフェイスへの ping をイネーブルまたはディセーブルにします。ping をディセーブルにすると、Cisco ASA がネットワーク上で検出できなくなります。この機能は、設定可能なプロキシ ping とも呼ばれます。

推奨処置 ピア装置の管理者にお問い合わせください。

313003

エラー メッセージ %PIX|ASA-4-313003: Invalid destination for ICMP error

説明 ICMP エラー メッセージの宛先が、ICMP エラー メッセージを生じさせた IP パケットの送信元とは異なります。

推奨処置 このメッセージが頻繁に表示される場合は、アクティブなネットワーク プローブ、カバートチャネルとして ICMP エラー メッセージを使用しようとする試行、または IP ホストの誤動作の可能性があります。ICMP エラー メッセージを送信したホストの管理者にお問い合わせください。

313004

エラー メッセージ %PIX|ASA-4-313004: Denied ICMP type=*icmp_type*, from *source_address* on interface *interface_name* to *dest_address*: no matching session

説明 ICMP パケットが、ステートフル ICMP 機能によって追加された次のセキュリティ チェックが原因で Cisco ASA によって廃棄されました。通常は、すでに Cisco ASA を通過した有効なエコー要求を持たない ICMP エコー応答、またはすでに Cisco ASA で確立されている TCP、UDP、または ICMP セッションに関連しない ICMP エラー メッセージであるセキュリティ チェックです。

推奨処置 不要です。

314001

エラー メッセージ %PIX|ASA-6-314001: Pre-allocate RTSP UDP backconnection for foreign_address *outside_address/outside_port* to local_address *inside_address/inside_port*

説明 Cisco ASA が、指摘された IP アドレスおよびポートに対する RTSP 接続を開きました。

推奨処置 処置は不要です。

315004

エラー メッセージ %PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.

説明 Cisco ASA が、SSH セッションの確立に必要な Cisco ASA RSA ホスト キーを見つけられませんでした。ホスト キーが生成されていなかったため、またはこの Cisco ASA のライセンスが DES または 3DES を許可しないために、Cisco ASA ホスト キーがない可能性があります。

推奨処置 コンソールから `show ca mypubkey rsa` コマンドを入力して、Cisco ASA RSA ホスト キーがあることを確認します。ホスト キーがない場合は、`show version` コマンドも入力して、Cisco ASA ライセンスが DES または 3DES を許可するかどうか調べます。

315011

エラー メッセージ %PIX|ASA-6-315011: SSH session from *IP_address* on interface *interface_name* for user *user* disconnected by SSH server, reason: *reason*

説明 このメッセージは、SSH セッションが完了した後に表示されます。ユーザが `quit` または `exit` を入力すると、`terminated normally` メッセージが表示されます。別の原因でセッションが切断された場合は、テキストで原因が説明されます。表 2-3 に、考えられるセッション切断の原因を示します。

表 2-3 SSH 切断の原因

テキスト文字列	説明	アクション
Bad checkbytes	SSH キー交換中にチェック バイトにミスマッチが検出されました。	SSH セッションを再開します。
CRC check failed	特定の packets に対して計算された CRC 値が、packet に埋め込まれている CRC 値と一致しません。packet が不良です。	処置は不要です。このメッセージが引き続き表示される場合は、Cisco TAC にお問い合わせください。
Decryption failure	SSH キーの交換中に SSH セッション キーの解読が失敗しました。	RSA ホスト キーを確認し、再度試行します。
Format error	非プロトコル バージョンのメッセージが、SSH バージョン交換中に受信されました。	SSH クライアントをチェックし、サポート対象のバージョンであることを確認します。
Internal error	このメッセージは、Cisco ASA 上の SSH の内部エラー、あるいは RSA キーが Cisco ASA に入力されていないか、または取得できないことを示します。	Cisco ASA コンソールから <code>show ca mypubkey rsa</code> を入力して、RSA ホスト キーがあることを確認します。RSA キーがない場合は、 <code>show version</code> コマンドも入力して、DES または 3DES が許可されているかどうか確認します。RSA ホスト キーがある場合は、SSH セッションを再開します。
Invalid cipher type	SSH クライアントがサポートされていない暗号を要求しました。	<code>show version</code> コマンドを入力し、ライセンスにサポートしている機能を確認してから、サポートされている暗号を使用するように SSH クライアントを再設定します。

表 2-3 SSH 切断の原因 (続き)

テキスト文字列	説明	アクション
Invalid message length	Cisco ASA に到着する SSH メッセージの長さが 262,144 バイトを超えているか、または 4,096 バイト未満です。データが破損している可能性があります。	処置は不要です。
Invalid message type	Cisco ASA が非 SSH メッセージを受信したか、あるいはサポートされていない SSH メッセージまたは要求されていない SSH メッセージを受信しました。	ピアが SSH クライアントであるかどうか確認します。ピアが SSHv1 をサポートしているクライアントであり、このメッセージが引き続き表示される場合は、Cisco ASA シリアル コンソールから <code>debug ssh</code> コマンドを入力して、デバッグメッセージを取り込みます。Cisco TAC にお問い合わせください。
Out of memory	このメッセージは、Cisco ASA が SSH サーバが使用するメモリを割り当てられず、おそらくはトラフィックが多いため Cisco ASA がビジーになっている場合に表示されます。	後で SSH セッションを再開始します。
Rejected by server	ユーザ認証が失敗しました。	ユーザ名とパスワードを確認するようユーザに求めます。
Reset by client	SSH クライアントが SSH_MSG_DISCONNECT メッセージを Cisco ASA に送信しました。	処置は不要です。
status code: <i>hex (hex)</i>	ユーザが、SSH コンソールで <code>quit</code> または <code>exit</code> を入力せずに、SSH クライアント ウィンドウ (Windows で実行中) を閉じました。	処置は不要です。クライアントをただ終了するのではなく、正常に終了するようユーザにお勧めします。
Terminated by operator	SSH セッションが、Cisco ASA コンソールで <code>ssh disconnect</code> コマンドの入力により終了されました。	処置は不要です。
Time-out activated	SSH セッションが、 <code>ssh timeout</code> コマンドで指定された継続時間を超えたため、タイムアウトしました。	SSH 接続を再開始します。 <code>ssh timeout</code> コマンドを使用して、5 分のデフォルト値を必要に応じて最大 60 分まで延長することができます。

推奨処置 不要です。

316001

エラー メッセージ %PIX|ASA-3-316001: Denied new tunnel to *IP_address*. VPN peer limit (*platform_vpn_peer_limit*) exceeded

説明 プラットフォーム VPN ピアの上限でサポートされているよりも多くの VPN トンネル (ISAKMP/IPSec) を同時に確立しようとした場合、過剰なトンネルは打ち切られます。

推奨処置 不要です。

317001

エラー メッセージ %PIX|ASA-3-317001: No memory available for limit_slow

説明 要求された動作がメモリ不足状態が原因で失敗しました。

推奨処置 他のシステム アクティビティを減らして、メモリ要求を緩和します。条件によって保証される場合は、さらにメモリ容量の大きな構成にアップグレードします。

317002

エラー メッセージ %PIX|ASA-3-317002: Bad path index of *number* for *IP_address*,
number max

説明 ソフトウェア エラーが発生しました。

推奨処置 問題の原因を判定するには、Cisco TAC に問い合わせてサポートを受けてください。

317003

エラー メッセージ %PIX|ASA-3-317003: IP routing table creation failure - *reason*

説明 内部ソフトウェア エラーが発生したため、新しい IP ルーティング テーブルの作成が妨げられました。

推奨処置 エラー メッセージをそのままコピーし、Cisco TAC に報告してください。

317004

エラー メッセージ %PIX|ASA-3-317004: IP routing table limit warning

説明 名前付き IP ルーティング テーブル内のルート数が、設定された警告制限に到達しました。

推奨処置 テーブルのルート数を減らすか、制限を設定し直します。

317005

エラー メッセージ %PIX|ASA-3-317005: IP routing table limit exceeded - *reason*,
IP_address netmask

説明 追加のルートはテーブルに加えられます。

推奨処置 テーブルのルート数を減らすか、制限を設定し直します。

318001

エラー メッセージ %PIX|ASA-3-318001: Internal error: *reason*

説明 内部ソフトウェア エラーが発生しました。このメッセージは 5 秒ごとに表示されます。

推奨処置 問題の原因を判定するには、Cisco TAC に問い合せてサポートを受けてください。

318002

エラー メッセージ %PIX|ASA-3-318002: Flagged as being an ABR without a backbone area

説明 ルータには、ルータで設定されたバックボーン エリアのないエリア境界ルータ (ABR) としてフラグが付いています。このメッセージは 5 秒ごとに表示されます。

推奨処置 OSPF プロセスを再起動します。

318003

エラー メッセージ %PIX|ASA-3-318003: Reached unknown state in neighbor state machine

説明 内部ソフトウェア エラーが発生しました。このメッセージは 5 秒ごとに表示されます。

推奨処置 不要です。

318004

エラー メッセージ %PIX|ASA-3-318004: area *string* lsid *IP_address* mask *netmask* adv *IP_address* type *number*

説明 OSPF でリンクステート アドバタイズメント (LSA) の検出に問題が生じました。これはメモリ リークにつながる可能性があります。

推奨処置 問題の原因を判定するには、Cisco TAC に問い合せてサポートを受けてください。

318005

エラー メッセージ %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*

説明 OSPF で、そのデータベースと IP ルーティング テーブルとの間に不整合が検出されました。

推奨処置 問題の原因を判定するには、Cisco TAC に問い合せてサポートを受けてください。

318006

エラー メッセージ %PIX|ASA-3-318006: if *interface_name* if_state *number*

説明 内部エラーが発生しました。

推奨処置 問題の原因を判定するには、Cisco TAC に問い合わせてサポートを受けてください。

318007

エラー メッセージ %PIX|ASA-3-318007: OSPF is enabled on *interface_name* during idb initialization

説明 内部エラーが発生しました。

推奨処置 問題の原因を判定するには、Cisco TAC に問い合わせてサポートを受けてください。

318008

エラー メッセージ %PIX|ASA-3-318008: OSPF process *number* is changing router-id.
Reconfigure virtual link neighbors with our new router-id

説明 OSPF プロセスがリセット中で、新しいルータ ID を選択しようとしています。このアクションによってすべての仮想リンクが停止させられます。

推奨処置 すべての近隣仮想リンクの仮想リンク コンフィギュレーションを、新しいルータ ID を反映するように変更します。

318009

エラー メッセージ %PIX|ASA-3-318009: OSPF: Attempted reference of stale data encountered in *function* , line: *line_num*

説明 このメッセージは、OSPF が動作中で、他の場所で削除された一部の関連データ構造を参照しようとする場合に表示されます。インターフェイスおよびルータのコンフィギュレーションを消去すると、問題が解決する可能性があります。しかし、このメッセージが表示される場合は、シーケンスの一部のステップによってデータ構造の早期削除が生じているので、調査する必要があります。

function : 予期しないイベントを受信した機能

line_num : コード中の行番号

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

319001

エラーメッセージ %PIX|ASA-3-319001: Acknowledge for arp update for IP address *dest_address* not received (*number*).

説明 Cisco ASA 内の ARP プロセスが、システムのオーバーロードが原因で内部同期外れになっています。

推奨処置 ただちに対応する必要はありません。一時的なエラーです。システムの平均負荷をチェックし、許容量を超えて使用されていないことを確認します。

319002

エラーメッセージ %PIX|ASA-3-319002: Acknowledge for route update for IP address *dest_address* not received (*number*).

説明 Cisco ASA 内のルーティング モジュールが、システムのオーバーロードが原因で内部同期外れになっています。

推奨処置 ただちに対応する必要はありません。一時的なエラーです。システムの平均負荷をチェックし、許容量を超えて使用されていないことを確認します。

319003

エラーメッセージ %PIX|ASA-3-319003: Arp update for IP address *address* to NPn failed.

説明 ARP エントリをアップデートする必要がある場合、内部 ARP テーブルをアップデートするためにネットワーク プロセッサ (NP) にメッセージが送信されます。モジュールでメモリ使用率が高くなっている場合、または内部テーブルが満杯になっている場合は、NP へのメッセージが拒否されて、このメッセージが生成される可能性があります。

推奨処置 ARP テーブルが満杯であるかどうか確認します。満杯ではない場合、CPU 使用率および秒あたりの接続数に関してモジュールの負荷を調べます。CPU 使用率が高いか、秒あたりの接続数が多い場合、負荷が正常に戻ると正常動作が再開されます。

319004

エラーメッセージ %PIX|ASA-3-319004: Route update for IP address *dest_address* failed (*number*).

説明 FWSM 内のルーティング モジュールが、システムのオーバーロードが原因で内部同期外れになっています。

推奨処置 ただちに対応する必要はありません。一時的なエラーです。システムの平均負荷をチェックし、許容量を超えて使用されていないことを確認します。

320001

エラー メッセージ %PIX|ASA-3-320001: The subject name of the peer cert is not allowed for connection

説明 Cisco ASA が簡単な VPN リモート装置またはサーバである場合、ピア証明書には `ca verifycertdn` コマンドと一致しないサブジェクト名が含まれています。

推奨処置 このメッセージは、「中間者攻撃」を示す可能性もあります。これは、デバイスがピア IP アドレスをスプーフィングし、Cisco ASA から VPN 接続を代行受信しようとするものです。

321001

エラー メッセージ %PIX|ASA-5-321001: Resource *var1* limit of *var2* reached.

説明 指摘されたリソースの設定使用率またはレート制限に達しました。

推奨処置 不要です。

321002

エラー メッセージ %PIX|ASA-5-321002: Resource *var1* rate limit of *var2* reached.

説明 指摘されたリソースの設定使用率またはレート制限に達しました。

推奨処置 不要です。

321003

エラー メッセージ %PIX|ASA-6-321003: Resource *var1* log level of *var2* reached.

説明 指摘されたリソースの設定リソース使用率またはレート ログ レベルに達しました。

推奨処置 不要です。

321004

エラー メッセージ %PIX|ASA-6-321004: Resource *var1* rate log level of *var2* reached

説明 指摘されたリソースの設定リソース使用率またはレート ログ レベルに達しました。

推奨処置 不要です。

322001

エラー メッセージ %PIX|ASA-3-322001: Deny MAC address *MAC_address*, possible spoof attempt on interface *interface*

説明 Cisco ASA が、指摘されたインターフェイス上の攻撃 MAC アドレスからパケットを受信しましたが、パケットの送信元 MAC アドレスはコンフィギュレーション内の別のインターフェイスに静的にバインドされています。これは、MAC スプーフィング攻撃または設定の誤りのいずれかが原因となっている可能性があります。

推奨処置 コンフィギュレーションを調べ、攻撃ホストを突き止めるか、またはコンフィギュレーションを訂正して適切な処置を行います。

322002

エラー メッセージ %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*.

説明 ARP 検査モジュールは、イネーブルになっている場合、パケット内でアドバタイズされる新しい ARP エントリが、静的に設定された IP-MAC アドレスまたは動的に取得された IP-MAC アドレスのバインディングに従っているかどうかチェックしてから、Cisco ASA を介して ARP パケットを転送します。このチェックが失敗した場合、ARP 検査モジュールは ARP パケットを廃棄し、このメッセージを生成します。この状況は、ネットワーク内の ARP スプーフィング攻撃または無効なコンフィギュレーション (IP-MAC バインディング) が原因となっている可能性があります。

推奨処置 原因が攻撃にある場合、ACL を使用してホストを拒否することができます。原因が無効なコンフィギュレーションにある場合、バインディングを修正します。

322003

エラー メッセージ %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.

説明 ARP 検査モジュールは、イネーブルになっている場合、パケット内でアドバタイズされる新しい ARP エントリが、静的に設定された IP-MAC アドレスのバインディングに従っているかどうかチェックしてから、Cisco ASA を介して ARP パケットを転送します。このチェックが失敗した場合、ARP 検査モジュールは ARP パケットを廃棄し、このメッセージを生成します。この状況は、ネットワーク内の ARP スプーフィング攻撃または無効なコンフィギュレーション (IP-MAC バインディング) が原因となっている可能性があります。

推奨処置 原因が攻撃にある場合、ACL を使用してホストを拒否することができます。原因が無効なコンフィギュレーションにある場合、バインディングを修正します。

322004

エラー メッセージ %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*

説明 管理 IP アドレスが透過モードで設定されていないため、Cisco ASA がパケットを廃棄しました。

protocol : プロトコルの文字列または値

interface_in : 入力インターフェイス名

source_address : パケットの送信元 IP アドレス

source_port : パケットの送信元ポート

interface_out : 出力インターフェイス名

dest_address : パケットの宛先 IP アドレス

dest_port : パケットの宛先ポート

推奨処置 装置に管理 IP アドレスとマスクの値を設定します。

323004

エラー メッセージ %ASA-3-323004: Module in slot *slotnum* failed to write software *vnewver* (currently *vver*), *reason*. Hw-module reset is required before further use.

説明 指摘されたスロット番号のモジュールがソフトウェア バージョンに対応できませんでした。UNRESPONSIVE 状態に移行します。モジュールは、ソフトウェアがアップデートされるまで使用できません。

slotnum : モジュールが存在しているスロット番号。

newver : モジュールへの書き込みが正常に終了しなかったソフトウェアの新しいバージョン番号 (1.0(1)0 など)。

ver : モジュール上のソフトウェアの現在のバージョン番号 (1.0(1)0 など)。

reason : 新しいバージョンがモジュールに書き込みできなかった理由。 *reason* に考えられる値は、次のとおりです。

- write failure
- failed to create a thread to write the image

推奨処置 モジュールは、`hw-module module slotnum reset` を使用してリセットしてから、さらにアップグレードの試行を行う必要があります。モジュール ソフトウェアは、アップデートできない場合、使用できなくなります。モジュールがシャーシにしっかりと取り付けられていることを確認します。それでもモジュール ソフトウェアをアップデートする試行が成功しない場合は、Cisco TAC にお問い合わせください。

323005

エラー メッセージ %ASA-3-323005: Module in slot *slotnum* can not be powered on completely

説明 このメッセージは、モジュールが完全には電源投入できないことを示します。モジュールは、この状態が修正されるまで、UNRESPONSIVE 状態のままになります。この原因は、モジュールがスロットに正しく取り付けられていないためだと考えられます。

slotnum : モジュールが存在しているスロット番号。

推奨処置 モジュールがスロットに正しく取り付けられていることを確認し、モジュールのステータス LED が点灯しているかどうかチェックします。モジュールを正しく取り付け直した後、モジュールが電源投入されたことをシステムが認識するまで数分かかることがあります。モジュールが取り付けられていることを確認し、**hw-module module *slotnum* reset** コマンドを使用してモジュールをリセットした後もこのメッセージが表示される場合は、Cisco TAC にお問い合わせください。

324000

エラー メッセージ %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*

説明 処理中のパケットが、*reason* 変数に記述されているフィルタリング要件を満たしていないため、廃棄されました。

推奨処置 不要です。

324001

エラー メッセージ %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*

説明 パケットの処理にエラーがありました。考えられる原因は次のとおりです。

- 必須 IE の不足
- 必須 IE の誤り
- IE の順序の狂い
- 無効なメッセージ フォーマット
- オプション IE の誤り
- 無効な TEID
- 不明な IE
- 不正な長さのフィールド
- 不明な GTP メッセージ
- 短すぎるメッセージ
- 予期しないメッセージの表示
- ヌル TID

- サポートされていないバージョン

推奨処置 このメッセージが一定期間ごとに表示される場合は、無視してかまいません。このメッセージが頻繁に表示される場合は、エンドポイントが攻撃の一部として不良パケットを送信している可能性があります。

324002

エラー メッセージ %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*

説明 このメッセージが 321100: Memory allocation Error (メモリ割り当てのエラー) の後に表示される場合、メッセージは PDP コンテキストを作成するのに十分なリソースがなかったことを示します。メッセージ 321100 の後に表示されなかった場合、バージョン 0 では対応する PDP コンテキストが見つからなかったことを示します。バージョン 1 では、メッセージ 324001 の後にこのメッセージが表示された場合、パケット処理エラーが発生して動作が停止しました。

推奨処置 メモリ割り当てのエラーが原因でこのメッセージが頻繁に繰り返される場合、Cisco TAC にお問い合わせください。

324003

エラー メッセージ %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*

説明 受信した応答は、要求キューと一致する要求が含まれていないため、それ以上処理されません。

推奨処置 このメッセージが一定期間ごとに表示される場合は、無視してかまいません。しかし、このメッセージが頻繁に表示される場合は、エンドポイントが攻撃の一部として不良パケットを送信している可能性があります。

324004

エラー メッセージ %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

説明 処理中のパケットが、現在サポートされているバージョン 0 またはバージョン 1 以外のバージョンになっています。プリントアウトされているバージョン番号が誤った番号であり、頻繁に表示される場合は、エンドポイントが攻撃の一部として不良パケットを送信している可能性があります。

推奨処置 不要です。

324005

エラー メッセージ %PIX|ASA-3-324005: Unable to create tunnel from *source_interface:source_address/source_port* to *dest_interface:dest_address/dest_port*

説明 TPDU のトンネルを作成する試行中にエラーが発生しました。

推奨処置 このメッセージが一定期間ごとに発生する場合は、無視してかまいません。頻繁に繰り返される場合は、必要なデバッグを収集して Cisco TAC にお問い合わせください。

324006

エラー メッセージ %PIX|ASA-3-324006:GSN *IP_address* tunnel limit *tunnel_limit* exceeded, PDP Context TID *tid* failed

説明 要求を送信している GSN が、作成される最大許容トンネル数を超えたため、トンネルが作成されません。

推奨処置 トンネル制限を増やす必要があるかどうか、またはネットワークへの攻撃の可能性があるかどうか確認します。

324007

エラー メッセージ %PIX|ASA-3-324007: Unable to create GTP connection for response from *source_interface:source_address/0* to *dest_interface:dest_address/dest_port*

説明 異なる SGSN または GGSN に対して TPDU のトンネルを作成する試行中にエラーが発生しました。

推奨処置 デバッグおよびメッセージを調べて、接続が適切に作成されなかった理由を確認します。問題をデバッグできない場合は、必要なデバッグを収集して Cisco TAC にお問い合わせください。

325001

エラー メッセージ %PIX|ASA-3-325001: Router *ipv6_address* on *interface* has conflicting ND (Neighbor Discovery) settings

説明 リンク上の別のルータが、矛盾するパラメータを持つルータ アドバタイズメントを送信しました。*ipv6_address* は相手側ルータの IPv6 アドレスです。*interface* は相手側ルータとのリンクのインターフェイス名です。

推奨処置 リンク上の IPv6 ルータがすべて、*hop_limit*、*managed_config_flag*、*other_config_flag*、*reachable_time* および *ns_interval* についてルータ アドバタイズメントに同じパラメータを持つことを確認し、複数のルータによってアドバタイズされる、同じプレフィクスの優先される有効なライフタイムが同じであることを確認します。インターフェイスごとにパラメータを示すには、コマンド `show ipv6 interface` を入力します。

325002

エラー メッセージ %PIX|ASA-4-325002: Duplicate address *ipv6_address/MAC_address* on *interface*

説明 別のシステムが IPv6 アドレスを使用しています。 *ipv6_address* は相手側ルータの IPv6 アドレスです。 *MAC_address* は、分かっている場合は相手側システムの MAC アドレス、それ以外の場合は「unknown」です。 *interface* は、相手側システムとのリンクのインターフェイス名です。

推奨処置 2つのシステムのうちの1つの IPv6 アドレスを変更します。

326001

エラー メッセージ %PIX|ASA-3-326001: Unexpected error in the timer library: *error_message*

説明 管理対象タイマー イベントが、コンテキストも適切なタイプもなしで受信されたか、あるいはハンドラがありません。このメッセージは、キューに入るイベントの数がシステム制限を超えたため、後で処理が試行される場合にも表示されます。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326002

エラー メッセージ %PIX|ASA-3-326002: Error in *error_message* : *error_message*

説明 IGMP プロセスが要求に応じてシャットダウンできませんでした。このシャットダウンに備えて実行されるイベントが同期していない可能性があります。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326004

エラー メッセージ %PIX|ASA-3-326004: An internal error occurred while processing a packet queue

説明 IGMP パケット キューがパケットを持たない信号を受信しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326005

エラー メッセージ %PIX|ASA-3-326005: Mrib notification failed for (*IP_address*, *IP_address*)

説明 データ駆動型イベントをトリガーするパケットが受信され、MRIB を通知する試行が失敗しました。

推奨処置 システムが動作した後にこのメッセージが引き続き表示される場合は、エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326006

エラー メッセージ %PIX|ASA-3-326006: Entry-creation failed for (*IP_address*, *IP_address*)

説明 MFIB は MRIB からエントリのアップデートを受信しましたが、表示されるアドレスに関連するエントリを作成できませんでした。このためメモリ不足が生じる可能性があります。

推奨処置 十分なメモリがある場合は、エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326007

エラー メッセージ %PIX|ASA-3-326007: Entry-update failed for (*IP_address*, *IP_address*)

説明 MFIB が MRIB からインターフェイスのアップデートを受信しましたが、表示されるアドレスに関連するインターフェイスを作成できませんでした。その結果メモリ不足が生じる可能性があります。

推奨処置 十分なメモリがある場合は、エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326008

エラー メッセージ %PIX|ASA-3-326008: MRIB registration failed

説明 MFIB が MRIB に登録できませんでした。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326009

エラー メッセージ %PIX|ASA-3-326009: MRIB connection-open failed

説明 MFIB が MRIB への接続を開けませんでした。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326010

エラー メッセージ %PIX|ASA-3-326010: MRIB unbind failed

説明 MFIB が MRIB からアンバインドできませんでした。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326011

エラー メッセージ %PIX|ASA-3-326011: MRIB table deletion failed

説明 MFIB が削除されるはずだったテーブルを取得できませんでした。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326012

エラー メッセージ %PIX|ASA-3-326012: Initialization of *string* functionality failed

説明 機能の初期化が失敗しました。このコンポーネントは引き続き、機能なしでも動作する可能性があります。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326013

エラー メッセージ %PIX|ASA-3-326013: Internal error: *string* in *string* line %d(%s)

説明 MRIB で基本エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326014

エラー メッセージ %PIX|ASA-3-326014: Initialization failed: error_message
error_message

説明 MRIB が初期化できませんでした。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326015

エラー メッセージ %PIX|ASA-3-326015: Communication error: error_message
error_message

説明 MRIB が形式が誤っているアップデートを受信しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326016

エラー メッセージ %PIX|ASA-3-326016: Failed to set un-numbered interface for
interface_name (*string*)

説明 PIM トンネルが送信元アドレスがないため使用できませんでした。この状況は、番号付きインターフェイスが見つからなかったため、または何らかの内部エラーが原因で発生します。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326017

エラー メッセージ %PIX|ASA-3-326017: Interface Manager error - *string* in *string* :
string

説明 PIM トンネル インターフェイスを作成中に、エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326019

エラー メッセージ %PIX|ASA-3-326019: *string* in *string* : *string*

説明 PIM RP トンネル インターフェイスを作成中に、エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326020

エラー メッセージ %PIX|ASA-3-326020: List error in *string* : *string*

説明 PIM インターフェイス リストを処理中に、エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326021

エラー メッセージ %PIX|ASA-3-326021: Error in *string* : *string*

説明 PIM トンネル インターフェイスの SRC を設定中に、エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326022

エラー メッセージ %PIX|ASA-3-326022: Error in *string* : *string*

説明 PIM プロセスが要求に応じてシャットダウンできませんでした。このシャットダウンに備えて実行されるイベントが同期していない可能性があります。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326023

エラー メッセージ %PIX|ASA-3-326023: *string* - *IP_address* : *string*

説明 PIM グループ範囲を処理中に、エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326024

エラー メッセージ %PIX|ASA-3-326024: An internal error occurred while processing a packet queue.

説明 PIM パケット キューがパケットを持たない信号を受信しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326025

エラー メッセージ %PIX|ASA-3-326025: *string*

説明 メッセージ送信の試行中に、内部エラーが発生しました。PIM トンネル IDB の削除など、メッセージの受信時に発生するようスケジュールされたイベントが行われない可能性があります。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326026

エラー メッセージ %PIX|ASA-3-326026: Server unexpected error: *error_message*

説明 MRIB がクライアントを登録できませんでした。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326027

エラー メッセージ %PIX|ASA-3-326027: Corrupted update: *error_message*

説明 MRIB が破損したアップデートを受信しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

326028

エラー メッセージ %PIX|ASA-3-326028: Asynchronous error: *error_message*

説明 MRIB API で未処理の非同期エラーが発生しました。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

メッセージ 400000 ~ 418001

この項では、400000 から 420003 までのメッセージについて説明します。

4000nn

エラー メッセージ %PIX|ASA-4-4000nn: IPS:number string from IP_address to IP_address on interface interface_name

説明 メッセージ 400000 ~ 400051 は、Cisco Intrusion Detection System のシグニチャ メッセージです。

推奨処置 次の Web サイトにある『Cisco Intrusion Detection System User Guide』を参照してください。

<http://www.cishttp://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/>

今回のリリースのセキュリティ アプライアンスでは、このメッセージがすべてサポートされているわけではありません。IPS システム ログ メッセージは、すべて 4-4000nn で始まり、次の形式になります。

オプションは次のとおりです。

- *number*
シグニチャ番号。次の Web サイトにある『Cisco Intrusion Detection System User Guide』を参照してください。
<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm>
- *string*
シグニチャ メッセージ (NetRanger シグニチャ メッセージとほぼ同じです)。
- *IP_address*
シグニチャが適用されるローカル ツー リモート アドレス。
- *interface_name*
シグニチャに基づくインターフェイスの名前。

次に例を示します。

```
%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
```

表 2-4 に、サポートされているシグニチャ メッセージをリストで示しています。

表 2-4 IPS Syslog メッセージ

メッセージ番号	シグニチャ ID	シグニチャ タイトル	シグニチャ タイプ
400000	1000	IP options-Bad Option List	情報
400001	1001	IP options-Record Packet Route	情報
400002	1002	IP options-Timestamp	情報
400003	1003	IP options-Security	情報
400004	1004	IP options-Loose Source Route	情報
400005	1005	IP options-SATNET ID	情報
400006	1006	IP options-Strict Source Route	情報
400007	1100	IP Fragment Attack	攻撃

表 2-4 IPS Syslog メッセージ (続き)

メッセージ番号	シグニチャ ID	シグニチャ タイトル	シグニチャタイプ
400008	1102	IP Impossible Packet	攻撃
400009	1103	IP Fragments Overlap	攻撃
400010	2000	ICMP Echo Reply	情報
400011	2001	ICMP Host Unreachable	情報
400012	2002	ICMP Source Quench	情報
400013	2003	ICMP Redirect	情報
400014	2004	ICMP Echo Request	情報
400015	2005	ICMP Time Exceeded for a Datagram	情報
400016	2006	ICMP Parameter Problem on Datagram	情報
400017	2007	ICMP Timestamp Request	情報
400018	2008	ICMP Timestamp Reply	情報
400019	2009	ICMP Information Request	情報
400020	2010	ICMP Information Reply	情報
400021	2011	ICMP Address Mask Request	情報
400022	2012	ICMP Address Mask Reply	情報
400023	2150	Fragmented ICMP Traffic	攻撃
400024	2151	Large ICMP Traffic	攻撃
400025	2154	Ping of Death Attack	攻撃
400026	3040	TCP NULL flags	攻撃
400027	3041	TCP SYN+FIN flags	攻撃
400028	3042	TCP FIN only flags	攻撃
400029	3153	FTP Improper Address Specified	情報
400030	3154	FTP Improper Port Specified	情報
400031	4050	UDP Bomb attack	攻撃
400032	4051	UDP Snork attack	攻撃
400033	4052	UDP Chargen DoS attack	攻撃
400034	6050	DNS HINFO Request	攻撃
400035	6051	DNS Zone Transfer	攻撃
400036	6052	DNS Zone Transfer from High Port	攻撃
400037	6053	DNS Request for All Records	攻撃
400038	6100	RPC Port Registration	情報
400039	6101	RPC Port Unregistration	情報
400040	6102	RPC Dump	情報
400041	6103	Proxied RPC Request	攻撃
400042	6150	ypserv (YP server daemon) Portmap Request	情報
400043	6151	ypbind (YP bind daemon) Portmap Request	情報
400044	6152	yppasswdd (YP password daemon) Portmap Request	情報
400045	6153	ypupdated (YP update daemon) Portmap Request	情報
400046	6154	ypxfrd (YP transfer daemon) Portmap Request	情報
400047	6155	mountd (mount daemon) Portmap Request	情報

表 2-4 IPS Syslog メッセージ (続き)

メッセージ番号	シグニチャ ID	シグニチャ タイトル	シグニチャ タイプ
400048	6175	rexd (remote execution daemon) Portmap Request	情報
400049	6180	rexd (remote execution daemon) Attempt	情報
400050	6190	statd Buffer Overflow	攻撃

401001

エラー メッセージ %PIX|ASA-4-401001: Shuns cleared

説明 メモリから既存の排除を削除するために `clear shun` コマンドが入力されました。

推奨処置 不要です。このメッセージは、シャニング アクティビティの記録を組織が保持できるようにするために表示されます。

401002

エラー メッセージ %PIX|ASA-4-401002: Shun added: IP_address IP_address port port

説明 `shun` コマンドが入力されました。このコマンドの最初の IP アドレスは排除されたホストです。その他のアドレスとポートはオプションであり、有効な場合は接続を終了するのに使用されます。

推奨処置 不要です。このメッセージは、シャニング アクティビティの記録を組織が保持できるようにするために表示されます。

401003

エラー メッセージ %PIX|ASA-4-401003: Shun deleted: IP_address

説明 排除されたホストの 1 つが排除データベースから削除されました。

推奨処置 不要です。このメッセージは、シャニング アクティビティの記録を組織が保持できるようにするために表示されます。

401004

エラー メッセージ %PIX|ASA-4-401004: Shunned packet: IP_address ==> IP_address on interface interface_name

説明 IP SRC によって定義されたホストは排除データベースのホストであるために、パケットが廃棄されました。排除されたホストは、そこで排除されたインターフェイスにトラフィックを渡すことはできません。たとえば、インターネット上の外部ホストは外部インターフェイス上で排除されます。

推奨処置 不要です。このメッセージには、排除されたホストのアクティビティの記録を提供します。このメッセージと %PIX|ASA-4-401005 を使用すると、このホストに関するリスク評価を詳しく見積もることができます。

401005

エラー メッセージ %PIX|ASA-4-401005: Shun add failed: unable to allocate resources for *IP_address IP_address port port*

説明 セキュリティ アプライアンスのメモリが不足しています。排除が適用できません。

推奨処置 Cisco Intrusion Detection System は、引き続き、この規則を適用しようとします。メモリを再利用して排除を手動で再適用するか、または Cisco Intrusion Detection System によって排除が適用されるのを待機します。

402101

エラー メッセージ %PIX|ASA-4-402101: decaps: rec'd IPSEC packet has invalid spi for *destaddr=dest_address, prot=protocol, spi=number*

説明 受信 IPsec パケットは、セキュリティ アソシエーション データベース (SADB) に存在しないセキュリティ パラメータ インデックス (SPI) を指定しています。これは、IPsec ピア間の SA のエイジングのわずかな相違による一時的な状態か、またはローカル SA の消去が原因です。この状態は、IPsec ピアから不正なパケットが送信された場合にも発生することがあります。攻撃の場合もあります。

推奨処置 ローカル SA がクリアされたことを、ピアは認識していないことがあります。新しい接続がローカル ルータから確立された場合、2 つのピアが正常に再度確立されることがあります。問題の発生が短期間にとどまらない場合は、接続を新規に確立してみるか、またはピアの管理者にお問い合わせます。

402102

エラー メッセージ %PIX|ASA-4-402102: decapsulate: packet missing {AH|ESP}, *destaddr=dest_address, actual prot=protocol*

説明 受信 IPsec パケットに、期待された AH または ESP ヘッダーがありません。ピアは、ネゴシエートされたセキュリティ ポリシーと一致しないパケットを送信中です。これは攻撃の場合があります。

推奨処置 ピアの管理者にお問い合わせください。

402103

エラー メッセージ %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*

説明 カプセル化されていない IPsec パケットが、ネゴシエートされた ID と一致しません。ピアは、セキュリティ アソシエーション 選択エラーのために、このセキュリティ アソシエーションを使用して他のトラフィックを送信中です。これは敵対イベントの場合があります。

推奨処置 ピアの管理者にお問い合わせ、ポリシーの設定を比較します。

402106

エラー メッセージ %PIX|ASA-4-402106: Rec'd packet not an IPSEC packet (ip)
dest_address= *dest_address*, src_addr= *source_address*, prot= *protocol*

説明 受信パケットは暗号マップ ACL と一致しますが、IPSec でカプセル化されていません。IPSec ピアはカプセル化されていないパケットを送信中です。このエラーは、ピアのポリシー セットアップ エラーが原因で発生することがあります。たとえば、Cisco ASA は、外部インターフェイス ポート 23 への暗号化 Telnet トラフィックのみを受信します。IPSec 暗号化を行わないで、ポート 23 上の外部インターフェイスに Telnet で送信しようとする、このメッセージが表示されます。このエラーは、敵対イベントを示すこともあります。このシステム ログ メッセージは、引用した条件以外では生成されません（たとえば、Cisco ASA インターフェイス自体へのトラフィックの場合は生成されません）。TCP および UDP 要求を追跡するメッセージについては、メッセージ 710001、710002、および 710003 を参照してください。

推奨処置 ピアの管理者に問い合わせて、ポリシーの設定を比較します。

402114

エラー メッセージ %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 プロトコル

spi : IPSec のセキュリティ パラメータ インデックス

seq_num : IPSec シーケンス番号

remote_IP : トンネルのリモート エンドポイントの IP アドレス

username : IPSec トンネルに関連付けられているユーザ名

local_IP : トンネルのローカル エンドポイントの IP アドレス

説明 このメッセージは、SA データベースに存在しない SPI を指定している IPSec パケットを受信した場合に表示されます。これは、IPSec ピア間の SA のエイジングのわずかな相違による一時的な状態か、またはローカル SA の消去が原因です。また、IPSec ピアによって不正なパケットが送信されたことを示すこともあります。これも攻撃の一部の場合があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

推奨処置 ローカル SA がクリアされたことを、ピアは認識していないことがあります。新しい接続がローカル ルータから確立された場合、2 つのピアが正常に再度確立されることがあります。あるいは、問題の発生が短期間にとどまらない場合は、接続を新規に確立してみるか、またはピアの管理者に問い合せます。

402115

エラー メッセージ %PIX|ASA-4-402115: IPSEC: Received a packet from *remote_IP* to *local_IP* containing *act_prot* data instead of *exp_prot* data.

説明 このメッセージは、期待された ESP ヘッダーのない IPSec パケットを受信した場合に表示されます。ピアは、ネゴシエートされたセキュリティ ポリシーと一致しないパケットを送信中です。これは攻撃を示す場合があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

remote_IP : トンネルのリモート エンドポイントの IP アドレス

local_IP : トンネルのローカル エンドポイントの IP アドレス

act_prot : 受信した IPSec プロトコル

exp_prot : 期待された IPSec プロトコル

推奨処置 ピアの管理者にお問い合わせください。

402116

エラーメッセージ %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* .

説明 このメッセージは、カプセル化解除された IPSec パケットがネゴシエートされた ID と一致しない場合に表示されます。ピアは、このセキュリティ アソシエーションを使用して他のトラフィックを送信中です。ピアによるセキュリティ アソシエーション選択エラーが原因の場合もあれば、攻撃の一部の場合もあります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

protocol : IPSec プロトコル

spi : IPSec のセキュリティ パラメータ インデックス

seq_num : IPSec シーケンス番号

remote_IP : トンネルのリモートエンドポイントの IP アドレス

username : IPSec トンネルに関連付けられているユーザ名

local_IP : トンネルのローカルエンドポイントの IP アドレス

pkt_daddr : カプセル化解除されたパケットからの宛先アドレス

pkt_saddr : カプセル化解除されたパケットからの送信元アドレス

pkt_prot : カプセル化解除されたパケットからのトランスポート プロトコル

id_daddr : ローカル プロキシ IP アドレス

id_dmask : ローカル プロキシ IP サブネット マスク

id_dprot : ローカル プロキシ トランスポート プロトコル

id_dport : ローカル プロキシ ポート

id_saddr : リモート プロキシ IP アドレス

id_smask : リモート プロキシ IP サブネット マスク

id_sprot : リモート プロキシ トランスポート プロトコル

id_sport : リモート プロキシ ポート

推奨処置 ピアの管理者に問い合せて、ポリシーの設定を比較します。

402117

エラーメッセージ %PIX|ASA-4-402117: IPSEC: Received a non-IPSec (*protocol*) packet from *remote_IP* to *local_IP* .

説明 このメッセージは、受信パケットは暗号マップ ACL と一致したが、IPSec でカプセル化されていなかった場合に表示されます。IPSec ピアはカプセル化されていないパケットを送信中です。このエラーは、ピアのポリシー セットアップ エラーが原因で発生することがあります。たとえば、外部インターフェイス ポート 23 への暗号化 Telnet トラフィックのみを受信するようにファイアウォールを設定できます。IPSec 暗号化を行わないで、ポート 23 上の外部インターフェイスに対して Telnet で送信しようとする、このメッセージが表示されますが、ポート 23

以外の外部インターフェイスに対する Telnet またはトラフィックの場合は表示されません。このエラーは、攻撃を示すこともあります。このシステム ログ メッセージは、これらの条件以外では生成されません（たとえば、ファイアウォール インターフェイス自体へのトラフィックの場合は生成されません）。TCP および UDP 要求を追跡するメッセージについては、メッセージ 710001、710002、および 710003 を参照してください。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

protocol : IPSec プロトコル

remote_IP : トンネルのリモート エンドポイントの IP アドレス

local_IP : トンネルのローカル エンドポイントの IP アドレス

表示が制限されています。

推奨処置 ピアの管理者に問い合せて、ポリシーの設定を比較します。

402118

エラー メッセージ %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*.

説明 このメッセージは、カプセル化解除された IPSec パケットに、128 バイト以下のオフセットの IP フラグメントが含まれている場合に発生します。最新バージョンの Security Architecture for IP RFC では、再アセンブリ攻撃を防止するために最小 IP フラグメント オフセットを 128 バイトにすることを推奨しています。これは攻撃の一部の場合があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

protocol : IPSec プロトコル

spi : IPSec のセキュリティ パラメータ インデックス

seq_num : IPSec シーケンス番号

remote_IP : トンネルのリモート エンドポイントの IP アドレス

username : IPSec トンネルに関連付けられているユーザ名

local_IP : トンネルのローカル エンドポイントの IP アドレス

frag_len : IP フラグメント長

frag_offset : IP フラグメント オフセット (バイト)

推奨処置 リモート ピアの管理者に問い合せて、ポリシーの設定を比較します。

402119

エラー メッセージ %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.

説明 このメッセージは、シーケンス番号が無効な IPSec パケットを受信したときに表示されます。ピアは、以前に使用された可能性のあるシーケンス番号が含まれたパケットを送信中です。このシステム ログ メッセージは、受け入れ許容範囲外のシーケンス番号の IPSec パケットを受信したことを示します。このパケットは、可能性ある攻撃の一部として IPSec により廃棄されます。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

protocol : IPSec プロトコル

spi : IPSec のセキュリティ パラメータ インデックス

seq_num : IPSec シーケンス番号

remote_IP : トンネルのリモート エンドポイントの IP アドレス

username : IPSec トンネルに関連付けられているユーザ名
local_IP : トンネルのローカル エンドポイントの IP アドレス

推奨処置 ピアの管理者にお問い合わせください。

402120

エラー メッセージ %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.

説明 このメッセージは、IPSec パケットを受信したが認証に失敗したときに表示されます。パケットは廃棄されます。パケットが中継中に破損した場合、またはピアが無効な IPSec パケットを送信中の場合があります。これらのパケットの多くを同じピアから受信しているときは、攻撃を示す場合があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

protocol : IPSec プロトコル
spi : IPSec のセキュリティ パラメータ インデックス
seq_num : IPSec シーケンス番号
remote_IP : トンネルのリモート エンドポイントの IP アドレス
username : IPSec トンネルに関連付けられているユーザ名
local_IP : トンネルのローカル エンドポイントの IP アドレス

推奨処置 受信したパケットの認証失敗が多い場合は、リモート ピアの管理者にお問い合わせください。

402121

エラー メッセージ %PIX|ASA-4-402121: IPSEC: Received an *protocol* packet (SPI=*spi*, sequence number= *seq_num*) from *remote_IP* (*username*) to *local_IP* that was dropped by IPSec (*drop_reason*).

説明 このメッセージは、カプセル化解除する IPSec パケットを受信したが、そのパケットが IPSec サブシステムによって後で廃棄された場合に表示されます。これは、デバイス設定またはデバイスそのものに問題が存在する可能性があることを示しています。パケットは、さまざまな理由で廃棄されます。このメッセージは、原因の判定に役立つように IPSec カウンタを補足します。

protocol : IPSec プロトコル
spi : IPSec のセキュリティ パラメータ インデックス
seq_num : IPSec シーケンス番号
remote_IP : トンネルのリモート エンドポイントの IP アドレス
username : IPSec トンネルに関連付けられているユーザ名
local_IP : トンネルのローカル エンドポイントの IP アドレス
drop_reason : パケットが廃棄された理由

推奨処置 Cisco TAC に問い合わせサポートを受けてください。

402122

エラー メッセージ %PIX|ASA-4-402122: IPSEC: Received a cleartext packet from *src_addr* to *dest_addr* that was to be encapsulated in IPsec that was dropped by IPsec (*drop_reason*).

説明 このメッセージは、IPsec でカプセル化するパケットを受信したが、そのパケットが IPsec サブシステムによって後で廃棄された場合に表示されます。これは、デバイス設定またはデバイスそのものに問題が存在する可能性があることを示しています。パケットは、さまざまな理由で廃棄されます。このメッセージは、原因の判定に役立つように IPsec カウンタを補足します。

src_addr : 送信元 IP アドレス

dest_addr : 宛先 IP アドレス

drop_reason : パケットが廃棄された理由

推奨処置 Cisco TAC に問い合わせてサポートを受けてください。

402123

エラー メッセージ %PIX|ASA-4-402123: CRYPTO:The *accel_type* hardware accelerator encountered an error (code= *error_string*) while executing crypto command *command* .

accel_type : ハードウェア アクセラレータ タイプ

error_string : エラーのタイプを示すコード

command : エラーを生成した暗号コマンド

説明 このメッセージは、ハードウェア アクセラレータで暗号コマンドを実行中に、エラーが検出された場合に表示されます。これは、アクセラレータの問題を示すことがあります。このタイプのエラーは、さまざまな理由で発生します。このメッセージは、原因の判定に役立つように暗号アクセラレータ カウンタを補足します。

推奨処置 Cisco TAC に問い合わせてサポートを受けてください。

403101

エラー メッセージ %PIX|ASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel_id=*number*, session_id=*number*

説明 セキュリティ アプライアンスが、対応する制御接続セッションのない PPTP XGRE パケットを受信しました。

推奨処置 このメッセージが頻繁に発生する場合、Cisco TAC に問題を報告してください。

403102

エラー メッセージ %PIXPIX|ASA-4-403102: PPP virtual interface *interface_name* rcvd pkt with invalid protocol: *protocol*, reason: *reason*.

説明 プロトコル フィールドが無効な XGRE カプセル化 PPP パケットをモジュールが受信しました。

推奨処置 このメッセージが頻繁に発生する場合、Cisco TAC に問題を報告してください。

403103

エラーメッセージ %PIXPIX|ASA-4-403103: PPP virtual interface max connections reached.

説明 モジュールは、追加の PPTP 接続を受け入れることはできません。

推奨処置 不要です。接続は有効になるとすぐに割り当てられます。

403104

エラーメッセージ %PIXPIX|ASA-4-403104: PPP virtual interface *interface_name* requires mschap for MPPE.

説明 Microsoft Point-to-Point Encryption (MPPE) は設定されていますが、MS-CHAP 認証が設定されていません。

推奨処置 `vpdn group group_name ppp authentication` コマンドで、MS-CHAP 認証を追加します。

403106

エラーメッセージ %PIXPIX|ASA-4-403106: PPP virtual interface *interface_name* requires RADIUS for MPPE.

説明 MPPE は設定されていますが、RADIUS 認証が設定されていません。

推奨処置 `vpdn group group_name ppp authentication` コマンドで、RADIUS 認証を追加します。

403107

エラーメッセージ %PIXPIX|ASA-4-403107: PPP virtual interface *interface_name* missing aaa server group info

説明 AAA サーバ設定情報を検出できません。

推奨処置 `vpdn group group_name client authentication aaa aaa_server_group` コマンドで、AAA サーバ情報を追加します。

403108

エラーメッセージ %PIXPIX|ASA-4-403108: PPP virtual interface *interface_name* missing client ip address option

説明 クライアント IP アドレス プール情報が不足しています。

推奨処置 `vpdn group group_name client configuration address local address_pool_name` コマンドで、IP アドレス プール情報を追加します。

403109

エラー メッセージ %PIXPIX|ASA-4-403109: Rec'd packet *not an PPTP packet. (ip)*
dest_address= *dest_address*, src_addr= *source_address*, data: *string*.

説明 スプーフィングされた PPTP パケットをモジュールが受信しました。これは敵対イベントの場合があります。

推奨処置 ピアの管理者に問い合せて、PPTP コンフィギュレーション設定を確認します。

403110

エラー メッセージ %PIXPIX|ASA-4-403110: PPP virtual interface *interface_name*,
user: *user* missing MPPE key from aaa server.

説明 AAA サーバは、MPPE 暗号化ポリシーのセットアップに必要な MPPE キー アトリビュートを返しません。

推奨処置 AAA サーバ コンフィギュレーションを確認して、AAA サーバが MPPE キー アトリビュートを返せない場合は、代わりに `vpdn group group_name client authentication local` コマンドでローカル認証を使用します。

403500

エラー メッセージ %PIXPIX|ASA-6-403500: PPPoE - Service name '*any*' not received
in PADO. Intf: *interface_name* AC: *ac_name*.

説明 セキュリティ アプライアンスが、インターネット サービス プロバイダーのアクセス コントローラからの PPPoE サービス「*any*」を要求しました。サービス プロバイダーからの応答には他のサービスが含まれていますが、サービス「*any*」は含まれていません。これは、プロトコルの実装の不一致です。PADO パケットは正常に処理されて、接続ネゴシエーションが続行されます。

推奨処置 不要です。

403501

エラー メッセージ %PIXPIX|ASA-3-403501: PPPoE - Bad host-unique in PADO - packet
dropped. Intf: *interface_name* AC: *ac_name*

説明 セキュリティ アプライアンスは、ホスト固有値と呼ばれる ID をアクセス コントローラに送信しました。アクセス コントローラは、異なるホスト固有値で応答しました。セキュリティ アプライアンスはこの応答に対応する接続要求を識別できません。パケットは廃棄され、接続ネゴシエーションは切断されます。

推奨処置 インターネット サービス プロバイダーにお問い合わせください。サービス プロバイダーのアクセス コントローラがホスト固有値の処理を誤っているか、または PADO パケットが不正です。

403502

エラー メッセージ %PIXPIX|ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf: *interface_name* AC: *ac_name*

説明 セキュリティ アプライアンスは、ホスト固有値と呼ばれる ID をアクセス コントローラに送信しました。アクセス コントローラは、異なるホスト固有値で応答しました。セキュリティ アプライアンスはこの応答に対応する接続要求を識別できません。パケットは廃棄され、接続ネゴシエーションは切断されました。

推奨処置 インターネット サービス プロバイダーにお問い合わせください。サービス プロバイダーのアクセス コントローラがホスト固有値の処理を誤っているか、または PADO パケットが不正です。

403503

エラー メッセージ %PIXPIX|ASA-3-403503: PPPoE:PPP link down: *reason*

説明 PPP リンクがダウンしました。これが発生する原因は数多くあります。最初の形式に表示される理由は、PPP からの理由の場合です。

推奨処置 ネットワーク リンクを調べて、リンクが接続されていることを確認します。アクセス コンセントレータがダウンしていることがあります。認証プロトコルがアクセス コンセントレータと一致することを確認します。名前とパスワードが正しいことを確認します。ISP またはネットワーク サポート 担当者にご確認ください。

403504

エラー メッセージ %PIXPIX|ASA-3-403504: PPPoE:No 'vpdn group' for PPPoE is created

説明 PPPoE では、PPPoE セッションを開始する前に、ダイヤルアウト コンフィギュレーションが必要です。一般的にコンフィギュレーションでは、ダイヤル ポリシー、PPP 認証、ユーザ名、およびパスワードを指定する必要があります。次の例では、セキュリティ アプライアンスを PPPoE ダイヤルアウト用に設定します。my-username コマンドおよび my-password コマンドは、必要であれば PAP を使用して、アクセス コンセントレータの認証に使用されます。

次に例を示します。

```
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
```

推奨処置 PPPoE 用の VPDN グループを設定します。

403505

エラー メッセージ %PIXPIX|ASA-4-403505: PPPoE:PPP - Unable to set default route to *IP_address* at *interface_name*

説明 通常、このメッセージには「- default route already exists」というメッセージが続きます。

推奨処置 現行のデフォルト ルートを削除するか、または「setroute」パラメータを削除して、PPPoE と手動で設定したルートが競合しないようにします。

403506

エラー メッセージ %PIXPIX|ASA-4-403506: PPPoE:failed to assign PPP *IP_address* netmask *netmask* at *interface_name*

説明 このメッセージには、「- subnet is the same as interface」または「on failover channel」が続きます。

推奨処置 最初の場合は、競合の原因となったアドレスを変更します。2 番目の場合は、フェールオーバー インターフェイス以外のインターフェイスに PPPoE を設定します。

404101

エラー メッセージ %PIX|ASA-4-404101: ISAKMP: Failed to allocate address for client from pool *string*

説明 ISAKMP は、**ip local pool** コマンドで指定されたプールから VPN クライアント用の IP アドレスを割り当てるのに失敗しました。

推奨処置 **ip local pool** コマンドを使用して、プールに追加 IP アドレスを指定します。

404102

エラー メッセージ %PIX|ASA-3-404102: ISAKMP: Exceeded embryonic limit

説明 500 を超える初期セキュリティ アソシエーション (SA) が存在します。これは DoS 攻撃を意味する場合があります。

推奨処置 **show crypto isakmp ca** コマンドを入力して、攻撃元を判別します。攻撃元を特定した後、攻撃 IP アドレスまたはネットワークへのアクセスを拒否します。

405001

エラーメッセージ %PIX|ASA-4-405001: Received ARP {request | response} collision from *IP_address/MAC_address* on interface *interface_name*

説明 Cisco ASA は ARP パケットを受信しましたが、パケット内の MAC アドレスが ARP キャッシュ エントリと異なります。

推奨処置 このトラフィックは、正当である場合もあれば、ARP ポイズニング攻撃が進行中であることを示す場合もあります。送信元 MAC アドレスを確認してパケットの送信元を判別し、そのパケットが有効なホストに属しているかどうかを調べます。

405101

エラーメッセージ %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]*

説明 モジュールが、接続の開始中に RAM システム メモリの割り当てに失敗したか、またはアドレス変換スロットを利用できません。

推奨処置 このメッセージが一定期間ごとに発生する場合は、無視してかまいません。頻繁に繰り返される場合は、Cisco TAC にお問い合わせください。グローバル プールのサイズを確認して、内部のネットワーク クライアント数と比較できます。PAT アドレスが必要な場合があります。または、変換と接続のタイムアウト間隔を短くします。このエラーメッセージは、メモリ不足によって発生することもあります。使用メモリ量を削減してみるか、または追加メモリを購入します。

405002

エラーメッセージ %PIX|ASA-4-405002: Received mac mismatch collision from *IP_address/MAC_address* for authenticated host

説明 このパケットは、次のどちらかの条件の場合に表示されます。

- Cisco ASA は IP アドレスが同じだが、MAC アドレスがその uauth エントリの 1 つとは異なるパケットを受信しました。
- Cisco ASA に `vpnclient mac-exempt` コマンドを設定し、除外 MAC アドレスを持つが、対応する uauth エントリとは異なる IP アドレスを持つパケットが Cisco ASA によって受信されます。

推奨処置 このトラフィックは、正当である場合もあれば、ARP スプーフィング攻撃が進行中であることを示す場合もあります。送信元 MAC アドレスと IP アドレスを確認してパケットの送信元を判別し、そのパケットが有効なホストに属しているかどうかを調べます。

405101

エラー メッセージ %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*]

説明 Cisco ASA が、接続の開始中に RAM システム メモリの割り当てに失敗したか、またはアドレス変換スロットを利用できません。

推奨処置 グローバルプールのサイズを確認し、内部のネットワーク クライアント数と比較します。PAT アドレスが必要な場合があります。または、変換と接続のタイムアウト間隔を短くします。このエラー メッセージは、メモリ不足によって発生することもあります。使用メモリ量を削減するか、または追加メモリを購入します。このメッセージが一定期間ごとに発生する場合は、無視してかまいません。頻繁に繰り返される場合は、Cisco TAC にお問い合わせください。

405102

エラー メッセージ %PIX|ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign_address *outside_address*[/*outside_port*] to local_address *inside_address*[/*inside_port*]

説明 Cisco ASA が、接続の開始中に RAM システム メモリの割り当てに失敗したか、またはアドレス変換スロットが利用できません。

推奨処置 グローバルプールのサイズを確認し、内部のネットワーク クライアント数と比較します。PAT アドレスが必要な場合があります。または、変換と接続のタイムアウト間隔を短くします。このエラー メッセージは、メモリ不足によって発生することもあります。使用メモリ量を削減するか、または追加メモリを購入します。このメッセージが一定期間ごとに発生する場合は、無視してかまいません。頻繁に繰り返される場合は、Cisco TAC にお問い合わせください。

405103

エラー メッセージ %PIX|ASA-4-405103: H225 message from *source_address*/*source_port* to *dest_address*/*dest_port* contains bad protocol discriminator *hex*

説明 PIX はプロトコル識別子 0x08 を予測していますが、0x08 以外の識別子を受信しました。このエラー メッセージは、エンドポイントから不良パケットが送信されている場合、または最初のセグメント以外のメッセージセグメントを受信した場合に発生することがあります。

推奨処置 不要です。パケットの通過は許可されます。

405104

エラー メッセージ %PIX|ASA-4-405104: H225 message received from *outside_address*/*outside_port* to *inside_address*/*inside_port* before SETUP

説明 このメッセージは、H.225 メッセージを間違った順番で受信すると表示されます。初期 SETUP メッセージの前に H.225 メッセージを受信しました。これは許可されません。Cisco ASA は、その H.225 コール シグナリング チャネルに関する初期 SETUP メッセージを受信してから、他のすべての H.225 メッセージを受信する必要があります。

推奨処置 不要です。

405105

エラーメッセージ %PIX|ASA-4-405105: H323 RAS message AdmissionConfirm received from *source_address/source_port* to *dest_address/dest_port* without an *AdmissionRequest*

説明 ゲートキーパーから admission confirm (ACF; 許可確認) が送信されましたが、Cisco ASA はゲートキーパーに admission request (ARQ; 許可要求) を送信していません。

推奨処置 指摘された *source_address* のゲートキーパーを確認して、Cisco ASA から ARQ を受信していないのに ACF が送信された理由を判定します。

405201

エラーメッセージ %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*

説明 ILS パケットペイロードに埋め込まれたアドレスが、IP パケットヘッダーのソース IP アドレスと異なります。

推奨処置 指摘された *source_IP_address* のホストを確認して、誤った埋め込み IP アドレスで ILS パケットが送信された理由を判定します。

406001

エラーメッセージ %PIX|ASA-4-406001: FTP port command low port: *IP_address/port* to *IP_address* on interface *interface_name*

説明 クライアントが FTP ポート コマンドを入力して、1024 (通常はサーバポート専用の周知のポート範囲にある) より小さなポート番号を指定しました。これは、サイトセキュリティポリシーを回避しようとしていることを示します。Cisco ASA は、パケットの廃棄、接続の終了、およびイベントの記録を行います。

推奨処置 不要です。

406002

エラーメッセージ %PIX|ASA-4-406002: FTP port command different address: *IP_address(IP_address)* to *IP_address* on interface *interface_name*

説明 クライアントが FTP ポート コマンドを発行して、接続に使用されているアドレス以外のアドレスを指定しました。このエラーメッセージは、サイトのセキュリティポリシーを回避しようとしていることを示します。たとえば、攻撃者が途中でパケットを変更し、正しいソース情報の代わりに別のソース情報を設定して FTP セッションをハイジャックしようとしている場合があります。セキュリティアプライアンスは、パケットの廃棄、接続の終了、およびイベントの記録を行います。カッコ内のアドレスは、ポートコマンドからのアドレスです。

推奨処置 不要です。

407001

エラー メッセージ %PIX|ASA-4-407001: Deny traffic for local-host
interface_name:inside_address, license limit of number exceeded

説明 ホスト制限を超えました。次のどちらかの条件に当てはまる場合、内部ホストは制限にカウントされます。

- 内部ホストは、この5分以内に、Cisco ASA 経由でトラフィックを転送しました。
- 内部ホストは現在、Cisco ASA で、xlate 接続またはユーザ認証を予約しています。

推奨処置 ホスト制限はローエンド プラットフォームに適用されます。ホスト制限を表示するには、show version コマンドを使用します。Cisco ASA でのセッションを持つ現在のアクティブホストと内部ユーザを表示するには、show local-host コマンドを使用します。1つまたは複数のユーザを強制的に切断するには、clear local-host コマンドを使用します。内部ユーザを制限になる前に期限切れにするには、xlate、接続、および uauth タイムアウトを推奨値以下に設定します（表 2-5 を参照）。

表 2-5 タイムアウトおよび推奨値

タイムアウト	推奨値
xlate	00:05:00 (5分)
conn	00:01:00 (1時間)
uauth	00:05:00 (5分)

407002

エラー メッセージ %PIX|ASA-3-407002: Embryonic limit nconns/limit for through
connections exceeded.outside_address/outside_port to global_address
(inside_address)/inside_port on interface interface_name

説明 これは Cisco ASA 経由の接続に関するメッセージです。このメッセージは、指摘されたグローバルアドレスを経由して、指摘された外部アドレスから指摘されたローカルアドレスに接続された数が、そのスタティックの最大初期制限を超えた場合に表示されます。Cisco ASA は、接続にメモリが割り当て可能な場合は、その接続を受け入れようとします。ローカルホストに代わってプロキシホストとなり、SYN_ACK パケットを外部ホストに送信します。Cisco ASA は、該当するステート情報を保持し、パケットを廃棄し、クライアントのACKを待ちます。

推奨処置 このメッセージは、正当なトラフィックを示す場合もあれば、DoS 攻撃が進行中であることを示す場合もあります。送信元アドレスを調べてパケットの送信元を判別し、それが有効なホストであるかどうかを確認します。

407003

エラー メッセージ %PIX|ASA-4-407003: Established limit for RPC services exceeded
number

説明 Cisco ASA は、最大ホール数に達した後、すでに設定されている RPC サーバペアまたは RPC サービスペアに対して、新規のホールをオープンしようとします。

推奨処置 他のホールがクローズされるのを待機するか（関連タイムアウト有効期限を使用）、またはサーバまたはサービスのアクティブペア数を制限します。

408001

エラーメッセージ %PIX|ASA-4-408001: IP route counter negative - *reason*, *IP_address*
Attempt: *number*

説明 IP ルート カウンタを負の値に減少しようとしたことが失敗しました。

推奨処置 `clear ip route *` コマンドを入力して、ルート カウンタをリセットします。メッセージが継続して定期的に表示される場合は、表示されるメッセージを正確にコピーして、Cisco TAC に報告してください。

408002

エラーメッセージ %PIX|ASA-4-408002: ospf process *id* route type update *address1*
netmask1 [*distance1/metric1*] via *source IP:interface1* *address2* *netmask2* [*distance2/metric2*]
interface2

説明 既存のルートよりも適切なメトリックを持つ同じ距離の別のインターフェイスからネットワーク アップデートを受信しました。新規のルートによって、別のインターフェイスを使用してインストールされた既存のルートが上書きされます。新規のルートは冗長目的に限り使用され、ネットワーク内でパスが移動されたことを意味します。この変更は、トポロジと再配布を使用して制御する必要があります。この変更の影響を受ける既存の接続は、ディセーブルにされる可能性があり、タイムアウトになります。このパスの移動は、パス冗長をサポートするようにネットワーク トポロジが特に設計されている場合（このケースが予測されます）に限り発生します。

推奨処置 不要です。

409001

エラーメッセージ %PIX|ASA-4-409001: Database scanner: external LSA *IP_address*
netmask is lost, reinstalls

説明 ソフトウェアによって、予想外の状態が検出されました。ルータによって修正処置が行われ、続行されます。

推奨処置 不要です。

409002

エラーメッセージ %PIX|ASA-4-409002: db_free: external LSA *IP_address netmask*

説明 内部ソフトウェア エラーが発生しました。

推奨処置 不要です。

409003

エラー メッセージ %PIX|ASA-4-409003: Received invalid packet: *reason* from *IP_address, interface_name*

説明 無効な OSPF パケットを受信しました。詳細は、エラー メッセージに記載されています。原因は、送信側の誤った OSPF コンフィギュレーションか内部エラーの可能性にあります。

推奨処置 受信側の OSPF コンフィギュレーションと送信側のコンフィギュレーションに不整合がないかを確認します。

409004

エラー メッセージ %PIX|ASA-4-409004: Received reason from unknown neighbor *IP_address*

説明 OSPF hello、データベース記述、またはデータベース要求パケットを受信しましたが、ルータは送信側を識別できませんでした。

推奨処置 この状態は、自分自身で訂正されます。

409005

エラー メッセージ %PIX|ASA-4-409005: Invalid length number in OSPF packet from *IP_address (ID IP_address), interface_name*

説明 正常なヘッダー サイズよりも短いフィールド長の OSPF パケット、または到着した IP パケットのサイズと一致しない OSPF パケットを受信しました。これは、パケットの送信側のコンフィギュレーション エラーを示しています。

推奨処置 近接アドレスから、問題のルータを特定しリブートします。

409006

エラー メッセージ %PIX|ASA-4-409006: Invalid lsa: *reason* Type *number*, LSID *IP_address* from *IP_address, IP_address, interface_name*

説明 LSA タイプが無効の LSA をルータが受信しました。原因は、ルータ上のメモリの破損または予想外の動作のどちらかです。

推奨処置 近接アドレスから、問題のルータを特定しリブートします。この問題の原因を判定するには、Cisco TAC に問い合わせでサポートを受けてください。

409007

エラー メッセージ %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*

説明 内部ソフトウェア エラーが発生しました。

推奨処置 この問題の原因を判定するには、Cisco TAC に問い合わせでサポートを受けてください。

409008

エラーメッセージ %PIX|ASA-4-409008: Found generating default LSA with non-zero mask LSA type : *number* Mask: *netmask* metric : *number* area : *string*

説明 ルータが誤ったマスクでデフォルト LSA を生成しようとした。内部ソフトウェア エラーのためにメトリックが間違っている可能性があります。

推奨処置 この問題の原因を判定するには、Cisco TAC に問い合わせサポートを受けてください。

409009

エラーメッセージ %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

説明 OSPF は、自分の 1 つのインターフェイスの IP アドレスからルータ ID を割り当てようとして、失敗しました。

推奨処置 IP アドレスが有効な動作中のインターフェイスが少なくとも 1 つあることを確認します。ルータで複数の OSPF プロセスが動作している場合、それぞれに固有のルータ ID が必要です。十分な数のインターフェイスを動作させて、それぞれがルータ ID を取得できるようにする必要があります。

409010

エラーメッセージ %PIX|ASA-4-409010: Virtual link information found in non-backbone area: *string*

説明 内部エラーが発生しました。

推奨処置 この問題の原因を判定するには、Cisco TAC に問い合わせサポートを受けてください。

409011

エラーメッセージ %PIX|ASA-4-409011: OSPF detected duplicate router-id *IP_address* from *IP_address* on interface *interface_name*

説明 OSPF は、このルーティング プロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。

推奨処置 OSPF ルータ ID は一意である必要があります。隣接ルータのルータ ID を変更します。

409012

エラーメッセージ %PIX|ASA-4-409012: Detected router with duplicate router ID *IP_address* in area *string*

説明 OSPF は、このルーティング プロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。

推奨処置 OSPF ルータ ID は一意である必要があります。隣接ルータのルータ ID を変更します。

409013

エラー メッセージ %PIX|ASA-4-409013: Detected router with duplicate router ID *IP_address* in Type-4 LSA advertised by *IP_address*

説明 OSPF は、このルーティング プロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。

推奨処置 OSPF ルータ ID は一意である必要があります。隣接ルータのルータ ID を変更します。

409023

エラー メッセージ %PIX|ASA-4-409023: Attempting AAA Fallback method *method_name* for *request_type* request for user *user* :Auth-server group *server_tag* unreachable

説明 外部サーバに対する認証または認可の試行が失敗し、ローカル ユーザ データベースを使用して実行されるようになります。*aaa_operation* は「authentication」か「authorization」のどちらかです。*username* は接続に関連付けられたユーザです。*server_group* はサーバが到達不能であった AAA サーバの名前です。

推奨処置 最初の方法で設定された AAA サーバの接続性の問題を調査します。Cisco ASA から認証サーバに対して ping を実行します。AAA サーバでデーモンが動作中であることを確認します。

410001

エラー メッセージ %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.

説明 このメッセージは、UDP DNS パケット内でドメイン名の長さが 255 バイトを超えた場合に表示されます (RFC 1035 section 3.1 を参照)。

推奨処置 不要です。

411001

エラー メッセージ %PIX|ASA-4-411001:Line protocol on interface *interface_name* changed state to up

説明 回線プロトコルのステータスが、down から up に変化しました。*interface_name* が論理インターフェイス名 (「inside」および「outside」など) の場合、このメッセージは、論理インターフェイス回線プロトコルが down から up に変化したことを示します。*interface_name* が物理インターフェイス名 (「Ethernet0」および「GigabitEthernet0/1」など) の場合、このメッセージは、物理インターフェイス回線プロトコルが down から up に変化したことを示します。

推奨処置 不要です。

411002

エラー メッセージ %PIX|ASA-4-411002:Line protocol on interface *interface_name* changed state to down

説明 回線プロトコルのステータスが up から down に変化しました。*interface_name* が論理インターフェイス名 (「inside」および「outside」など) の場合、このメッセージは、論理インターフェイス回線プロトコルが up から down に変化したことを示します。この場合、物理インターフェイス回線プロトコルのステータスは影響を受けません。*interface_name* が物理インターフェイス名 (「Ethernet0」および「GigabitEthernet0/1」など) の場合、このメッセージは、物理インターフェイス回線プロトコルが up から down に変化したことを示します。

推奨処置 これがインターフェイス上の予期しないイベントの場合、物理回線を確認します。

411003

エラー メッセージ %PIX|ASA-4-411003: Configuration status on interface *interface_name* changed state to downup

推奨処置 これが予期しないイベントの場合、物理回線を確認します。

411004

エラー メッセージ %PIX|ASA-4-411004: Configuration status on interface *interface_name* changed state to up

説明 インターフェイスのコンフィギュレーションステータスが down から up に変化しました。

推奨処置 不要です。

412001

エラー メッセージ %PIX|ASA-4-412001:MAC *MAC_address* moved from *interface_1* to *interface_2*

説明 このメッセージは、モジュール インターフェイス間でのホストの移動が検出された場合に生成されます。透過 Cisco ASA では、ホスト (MAC) と Cisco ASA ポートの間のマッピングはレイヤ 2 転送テーブルに保持されています。このテーブルでは、パケット送信元 MAC アドレスが Cisco ASA ポートにダイナミックにバインドされます。このプロセスでは、インターフェイス間でのホストの移動が検出されると常に、このメッセージが生成されます。

推奨処置 ホストの移動が有効である場合もあれば、ホストの移動が、他のインターフェイス上のホスト MAC をスプーフィングしようとしている場合もあります。MAC スプーフィングの場合は、ネットワーク上の脆弱なホストを特定して削除するか、またはスタティック MAC エントリ (MAC アドレスおよびポートバインディングは変更できない) を設定します。実際にホスト移動が行われた場合、処置は不要です。

412002

エラー メッセージ %PIX|ASA-4-412002: Detected bridge table full while inserting MAC *MAC_address* on interface *interface*. Number of entries = *num*

説明 このメッセージは、ブリッジ テーブルがいっぱいの場合に、さらに1つエントリを追加しようとしたときに生成されます。Cisco ASA は、コンテキストごとに別個のレイヤ 2 転送テーブルを保持しており、コンテキストがサイズ制限を超えると常にこのメッセージが生成されます。MAC アドレスは追加されますが、テーブル内の最も古い既存のダイナミック エントリ (有効な場合) が置換されます。

推奨処置 これは攻撃が行われようとした可能性があります。新規ブリッジ テーブル エントリが有効であることを確認します。攻撃の場合には、EtherType ACLs を使用して脆弱なホストへのアクセスを制御します。

413001

エラー メッセージ %ASA-4-413001: Module in slot *slotnum* is not able to shut down. Module Error: *errnum message*

説明 *slotnum* 内のモジュールは、ASA システム モジュールからのシャットダウンの要求に応じることができませんでした。ソフトウェア アップグレードのような中断できないタスクを実行していることがあります。*errnum* および *message* テキストに、モジュールをシャットダウンできなかった理由と、推奨アクションが記載されています。

推奨処置 モジュール上のタスクが完了するのを待ってからモジュールをシャットダウンするか、またはセッション コマンドを使用してモジュールの CLI にアクセスし、モジュールのシャットダウンを妨げているタスクを停止します。

413002

エラー メッセージ %ASA-4-413002: Module in slot *slotnum* is not able to reload. Module Error: *errnum message*

説明 *slotnum* 内のモジュールは、ASA システム モジュールからのリロードの要求に応じることができませんでした。ソフトウェア アップグレードのような中断できないタスクを実行していることがあります。*errnum* および *message* テキストに、モジュールをリロードできなかった理由と、推奨アクションが記載されています。

推奨処置 モジュールのタスクが完了するのを待ってからモジュールをリロードするか、またはセッション コマンドを使用してモジュールの CLI にアクセスし、モジュールのリロードを妨げているタスクを停止します。

413003

エラー メッセージ %ASA-4-413003: Module in slot *slotnum* is not a recognized type

説明 有効なカード タイプとして認識されないカードを検出するたびに生成されます。

推奨処置 インストールされているモジュール タイプをサポートする ASA システム ソフトウェアのバージョンにアップグレードします。

413004

エラーメッセージ %ASA-4-413004: Module in slot *slotnum* failed to write software *vnewver* (currently *vver*), *reason*. Trying again.

説明 指摘されたスロット番号のモジュールがソフトウェアバージョンに対応できませんでした。UNRESPONSIVE 状態に移行します。モジュール ソフトウェアのアップデートがさらに試行されます。

slotnum : モジュールが存在しているスロット番号。

newver : モジュールへの書き込みが正常に終了しなかったソフトウェアの新しいバージョン番号 (1.0(1)0 など)。

ver : モジュール上のソフトウェアの現在のバージョン番号 (1.0(1)0 など)。

reason : 新しいバージョンがモジュールに書き込みできなかった理由。 *reason* に考えられる値は、次のとおりです。

- write failure
- failed to create a thread to write the image

推奨処置 不要です。その後の試行で、アップデートの成功または失敗を示すメッセージが生成されます。その後のアップデート試行後の UP へのモジュール遷移を確認するには、`show module slotnum` コマンドを使用します。

414001

エラーメッセージ %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*]

説明 このシステム ログメッセージは、ロギング モジュールによる外部 FTP サーバへのロギング バッファの保存が失敗した場合に生成されます。

推奨処置 失敗した理由に基づいて、適切な処置を行います。

- プロトコル エラー : FTP サーバと Cisco ASA との間の接続に問題がなく、FTP サーバが FTP PORT コマンドを受信して要求を出すことができることを確認します。
- 無効なユーザ名またはパスワード : 設定された FTP クライアント ユーザ名およびパスワードが正しいことを確認します。
- 他のエラーすべて : Cisco TAC に問い合せてサポートを受けてください。

414002

エラーメッセージ %PIX|ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: *filename*: [*fail_reason*]

説明 このシステム ログメッセージは、ロギング モジュールによるシステム フラッシュへのロギング バッファの保存が失敗した場合に生成されます。

推奨処置 失敗した理由が十分な領域がないためである場合は、システム フラッシュの空き領域をチェックして、ロギング フラッシュ サイズ コマンドの設定制限が正しく設定されていることを確認します。エラーが、フラッシュ ファイル システムの入出力エラーの場合は、Cisco TAC に問い合せてサポートを受けてください。

415001

エラー メッセージ %PIX|ASA-5-415001:internal_sig_id HTTP Tunnel detected - action tunnel_type from source_address to dest_address

説明 このメッセージは、`http-map port-misuse` コマンドが設定されていて、トンネリング プロトコルが検出された場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

dest_address : トンネリングが検出されたパケットの宛先アドレス。

source_address : トンネリングが検出されたパケットの送信元アドレス。

tunnel_type : 検出されたトンネリング プロトコルのタイプを示します。

推奨処置 このメッセージは、ユーザが HTTP でトンネリング プロトコルを実行していたことを示します。これはポリシーに違反することがあります。

415002

エラー メッセージ %PIX|ASA-5-415002:internal_sig_id HTTP Instant Messenger detected - action instant_messenger_type from source_address to dest_address

説明 このメッセージは、`http-map port-misuse` コマンドが設定されていて、インスタント メッセージ プロトコルが検出された場合に発行されます。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

dest_address : インスタント メッセージ プロトコルが検出されたパケットの宛先アドレス。

instant_messenger_type : 検出されたインスタント メッセージ プロトコルのタイプを示します。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

source-address : インスタント メッセージ プロトコルが検出されたパケットの送信元アドレス。

推奨処置 このメッセージは、ユーザが HTTP でインスタント メッセージ プロトコルを実行していたことを示します。これはポリシーに違反することがあります。

415003

エラー メッセージ %PIX|ASA-5-415003:internal_sig_id HTTP Peer-to-Peer detected - action peer_to_peer_type from source_address to dest_address

説明 このメッセージは、`http-map port-misuse` コマンドが設定されていて、ピアツーピア プロトコルが検出された場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset」または「Drop」を含む可能性があります。アクションが *log* の場合、ヌル文字列 "" が渡されます。

peer_to_peer_type : 検出されたピアツーピア プロトコルのタイプを示します。
source-address : ピアツーピア プロトコルが検出されたパケットの送信元アドレス。
dest-address : ピアツーピア プロトコルが検出されたパケットの宛先アドレス。

推奨処置 このメッセージは、ユーザが HTTP でピアツーピア プロトコルを実行していたことを示します。これはポリシーに違反することがあります。

415004

エラー メッセージ %PIX|ASA-1-415004:*internal_sig_id* Content type not found - *action mime_type* from *source_address* to *dest_address*

説明 このシステム ログメッセージは、**http-map content-type-verification** コマンドが設定されていて、Content-Type HTTP Header フィールド内の MIME タイプが許容ポリシー タイプのリストに見つからなかった場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

mime_type : Content-Type HTTP Header フィールドに表示されたコンテンツ タイプ。

source-address : 認識されない MIME タイプが検出されたパケットの送信元アドレス。

dest-address : 認識されない MIME タイプが検出されたパケットの宛先アドレス。

推奨処置 このシステム ログメッセージは、メッセージの内容が、許容されるコンテンツ タイプのポリシー リストに見つからなかったことを示しています。これはポリシーに違反することがあります。

415005

エラー メッセージ %PIX|ASA-5-415005:*Internal_Sig_Id* Content type does not match specified type - *Action* Content Verification Failed from *source_address* to *Dst_IP_Address*

説明 このメッセージは、**http-map content-type-verification** コマンドが設定されていて、Content-Type HTTP Header フィールド内の MIME タイプが許容ポリシー タイプのリストに見つかったが、メッセージ本体の「マジック番号」がそのタイプのファイルを識別する正しいマジック番号ではない場合に発行されます。

このメッセージは表示が制限されており、その後の違反は記録されません。

Internal_Sig_Id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

Action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

source-address : コンテンツ タイプの検証の失敗が検出されたパケットの送信元アドレス。

Dst_IP_Address : コンテンツ タイプの検証の失敗が検出されたパケットの宛先アドレス。

推奨処置 メッセージ本体のメッセージの内容が、メッセージのヘッダー内のコンテンツ タイプと一致しませんでした。これは異常なことであり、接続を利用して禁止されたデータを密かに入出力しようとしていることを示す場合があります。

415006

エラー メッセージ %PIX|ASA-6-415006:internal_sig_id Content size size out of range - action content-length from source_address to dest_address

説明 このメッセージは、**http-map content-length** コマンドが設定されていて、コンテンツ長がユーザ設定の長さを超えている場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

size : ユーザ設定の最大長を超えていたメッセージの長さ。

content-length : Content-Length HTTP Header フィールドに表示されていたコンテンツの長さ。

source-address : コンテンツ サイズ違反が検出されたパケットの送信元アドレス。

dest_address : コンテンツ サイズ違反が検出されたパケットの宛先アドレス。

推奨処置 このメッセージは、ユーザ設定のポリシーで許容されるより多くのデータを転送しようとしたことを示します。

415007

エラー メッセージ %PIX|ASA-5-415007:internal_sig_id HTTP Extension method illegal - action 'method_name' from source_address to dest_address

説明 このメッセージは、指摘された拡張メソッドをフィルタリングするために **http-map request-method ext** コマンドが設定されている場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

method_name : alert を発生させた拡張メソッドの名前。

source_address : 拡張メソッドが検出されたパケットの送信元アドレス。

dest_address : 拡張メソッドが検出されたパケットの宛先アドレス。

推奨処置 このメッセージは、禁止されている拡張メソッドを使用しようとしたことを示します。これは、ユーザが設定したポリシーに違反します。

415008

エラー メッセージ %PIX|ASA-5-415008:internal_sig_id HTTP RFC method illegal - action 'method_name' from source_address to dest_address

説明 このメッセージは、指摘された RFC メソッドをフィルタリングするために **http-map request-method rfc** コマンドが設定されている場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

method_name : alert を発生させた RFC メソッドの名前。

source_address : RFC メソッドが検出されたパケットの送信元アドレス。

dest_address : RFC メソッドが検出されたパケットの宛先アドレス。

推奨処置 このメッセージは、禁止されている RFC メソッドを使用しようとしたことを示します。これは、ユーザが設定したポリシーに違反します。

415009

エラーメッセージ %PIX|ASA-6-415009:*internal_sig_id* HTTP Header length exceeded. Received *length* byte Header - *action* header length exceeded from *source_address* to *dest_address*

説明 このメッセージは、`http-map max-header-length` コマンドが設定されていて、ユーザ指定のヘッダー長よりも長い HTTP ヘッダーが検出された場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

length : ヘッダーの長さ。

source_address : 限度を超えた長さのヘッダー長が検出されたパケットの送信元アドレス。

dest-address : 限度を超えた長さのヘッダー長が検出されたパケットの宛先アドレス。

推奨処置 このメッセージは、ユーザ指定の最大長よりも長いヘッダーが送信されたことを示します。これは、ユーザが設定したポリシーに違反します。

415010

エラーメッセージ %PIX|ASA-5-415010:*internal_sig_id* HTTP protocol violation detected - *action* HTTP Protocol not detected from *source_address* to *dest_address*

説明 このメッセージは、`http-map strict-http` コマンドが設定されていて、ストリームが RFC 準拠の実装チェックに違反している場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、*Reset* または *Drop* を含む可能性があります。アクションが *log* の場合、ヌル文字列 "" が渡されます。

source_address : 非 HTTP プロトコルが検出されたパケットの送信元アドレス。

dest_address : 非 HTTP プロトコルが検出されたパケットの宛先アドレス。

推奨処置 HTTP トランザクション用のポートを通してプロトコルが実行されている場合があります。これは、ユーザが設定したポリシーに違反します。

415011

エラー メッセージ %PIX|ASA-6-415011:*internal_sig_id* HTTP URL Length exceeded.
Received *size* byte URL - *action* URI length exceeded from *source_address* to *dest_address*

説明 このメッセージは、`http-map max-url-length` コマンドが設定されていて、ユーザ指定の最大 URL 長よりも長い URL が検出された場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

size : 攻撃 URL の長さ。

source_address : 限度を超えた長さの URL が検出されたパケットの送信元アドレス。

dest_address : 限度を超えた長さの URL が検出されたパケットの宛先アドレス。

推奨処置 限度を超えた長さの URL は、攻撃が行われようとしていることを示す場合があります。

415012

エラー メッセージ %PIX|ASA-4-415012:*internal_sig_id* HTTP Deobfuscation signature detected - *action* HTTP deobfuscation detected IPS evasion technique from *source_address* to *source_address*

説明 このメッセージは、`http-map strict-http` コマンドが設定されていて、HTTP 回避手法が検出された場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

source_address : 意図的な混乱が検出されたパケットの送信元アドレス。

dest_address : 意図的な混乱が検出されたパケットの宛先アドレス。

推奨処置 ハッカーが、セキュリティチェックをバイパスしようとして URL を意図的に混乱させています。このメッセージは攻撃を示します。

415013

エラー メッセージ %PIX|ASA-5-415013:*internal_sig_id* HTTP Transfer encoding violation detected - *action* *Xfer_encode* Transfer encoding not allowed from *source_address* to *dest_address*

説明 このメッセージは、`http-map transfer-encoding` コマンドが設定されていて、禁止されている転送符号化が検出された場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset」または「Drop」を含む可能性があります。アクションが *log* の場合、ヌル文字列 "" が渡されます。

Xfer_encode : 認識されているが禁止されている転送符号化の場合、これには実際の転送符号化文字列が含まれています。文字列が認識されない転送符号化の場合は、「Transfer encoding not allowed」が表示されます。

source_address : 攻撃転送符号化が検出されたパケットの送信元アドレス。

dest_address : 攻撃転送符号化が検出されたパケットの宛先アドレス。

推奨処置 ユーザ設定のポリシーに違反したメッセージが送信されました。

415014

エラー メッセージ %PIX|ASA-4-415014:*internal_sig_id* Maximum of 10 unanswered HTTP requests exceeded from *source_address* to *dest_address*

説明 このメッセージは、`http-map strict-http` コマンドが設定されていて、1つの接続に10個を超える応答のないHTTP要求が見つかった場合に発行されます。

internal_sig_id : これは、alert をトリガーした特定のポリシーを識別するのに、開発者が使用できる内部の「ポリシー番号」です。

action : これは、ユーザが設定したアクションに従って、「Reset -」または「Drop -」を含む可能性があります。アクションが「ログ」の場合、ヌル文字列 "" が渡されます。

source_address : 応答のない最後の要求が検出されたパケットの送信元アドレス。

dest_address : 応答のない最後の要求が検出されたパケットの宛先アドレス。

推奨処置 応答されていない複数のHTTP要求が送信されました。これは、接続のサーバ側にHTTPサーバが存在しないという攻撃を示すことがあります。

416001

エラー メッセージ %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

説明 SNMPパケットが、不良パケットフォーマットのため、または*prot_version*はCisco ASAを通過することを許可されていないために、Cisco ASAを通過することを拒否されました。*prot_version* フィールドの値は、1、2、2c、または3のうちのいずれかです。

推奨処置 `snmp-map` コマンドを使用して、SNMP検査の設定を変更します。このコマンドを使用すると、ユーザが特定のプロトコルバージョンを許可または拒否できます。

417001

エラー メッセージ %PIX|ASA-4-417001: Unexpected event received: *number*

説明 プロセスで信号を受信しましたが、イベントのハンドラが見つかりませんでした。

推奨処置 エラーメッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒にCisco TACに送付してください。

417004

エラー メッセージ %PIX|ASA-4-417004: Filter violation error: conn *number*
(*string:string*) in *string*

説明 クライアントが、自分が所有していないルート アトリビュートを修正しようとした。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

417006

エラー メッセージ %PIX|ASA-4-417006: No memory for *string*) in *string*. Handling: *string*

説明 メモリ不足のために動作が失敗しましたが、別のメカニズムで処理されます。

説明 十分なメモリが存在する場合は、エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

418001

エラー メッセージ %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*)

説明 指摘された送信元から宛先へのパケットが、Cisco ASA と管理専用ネットワークとの間を経由しているために、廃棄されます。

protocol_string : TCP、UDP、ICMP、または 10 進数のプロトコル ID。

interface_name : インターフェイス名。

IP_address : IP アドレス。

port : ポート番号。

推奨処置 このようなパケットを生成している個人と理由を調査します。

419001

エラー メッセージ %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*

説明 このメッセージは、TCP パケットの長さが 3 ウェイ ハンドシェイクでアドバタイズされた MSS を超えている場合に生成されます。

src_ifc : 入力インターフェイス名

src_IP : パケットの送信元 IP アドレス

src_port : パケットの送信元ポート

dest_ifc : 出力インターフェイス名

dest_IP : パケットの宛先 IP アドレス

dest_port : パケットの宛先ポート

推奨処置 MSS を超えるパケットを許可する必要がある場合は、`exceed-mss` コマンドを使用して TCP マップを作成します。次に例を示します。

```
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 service-policy global_policy global
```

420001

エラー メッセージ %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
packet from ifc_in:SIP to ifc_out:DIP\n"
```

説明 このメッセージは、IPS フェールクローズ モードが使用されており、IPS カードが動作していない場合にパケットが廃棄されると、表示されます。このメッセージは表示が制限されています。

ifc_in : 入力インターフェイス名

ifc_out : 出力インターフェイス名

SIP : パケットのソース IP

SPORT : パケットの送信元ポート

DIP : パケットの宛先 IP

DPORT : パケットの宛先ポート

`ICMP_TYPE` : ICMP パケットのタイプ

`ICMP_CODE` : ICMP パケットのコード

推奨処置 IPS カードを確認して動作させます。

420002

エラー メッセージ %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"
```

説明 このメッセージは、パケットを廃棄するように IPS が要求した場合には表示されます。

ifc_in : 入力インターフェイス名

ifc_out : 出力インターフェイス名

SIP : パケットのソース IP

SPORT : パケットの送信元ポート
DIP : パケットの宛先 IP
DPORT : パケットの宛先ポート
ICMP_TYPE : ICMP パケットのタイプ
ICMP_CODE : ICMP パケットのコード

推奨処置 処置は不要です。

420003

エラー メッセージ %ASA-4-420003 : IPS requested to reset TCP connection from *ifc_in:SIP/SPORT* to *ifc_out:DIP/DPORT*"

説明 このメッセージは、TCP 接続のリセットを IPS が要求した場合に表示されます。

ifc_in : 入力インターフェイス名
ifc_out : 出力インターフェイス名
SIP : パケットのソース IP
SPORT : パケットの送信元ポート
DIP : パケットの宛先 IP
DPORT : パケットの宛先ポート

推奨処置 処置は不要です。

メッセージ 500001 ~ 507001

この項では、500001 から 507001 までのメッセージについて説明します。

500001

エラーメッセージ %PIX|ASA-5-500001: ActiveX content modified src *IP_address* dest *IP_address* on interface *interface_name*.

説明 このメッセージは、**filter** コマンドを使用して **activex** オプションをオンにし、Cisco ASA が ActiveX オブジェクトを検出すると表示されます。**activex** オプションを使用すると、Cisco ASA では、ActiveX オブジェクトを修正し、ActiveX コンテンツをフィルタリングして除外します。これによって、ActiveX オブジェクトは HTML オブジェクトとしてタグ付けされなくなります。

推奨処置 不要です。

500002

エラーメッセージ %PIX|ASA-5-500002: Java content modified src *IP_address* dest *IP_address* on interface *interface_name*.

説明 このメッセージは、**filter** コマンドを使用して **java** オプションをオンにし、Cisco ASA が Java アプレットを検出すると表示されます。**java** オプションを使用すると、Cisco ASA では、Java アプレットを修正し、Java コンテンツをフィルタリングして除外します。これによって、Java アプレットは HTML オブジェクトとしてタグ付けされなくなります。

推奨処置 不要です。

500003

エラーメッセージ %PIX|ASA-5-500003: Bad TCP hdr length (hdrhlen=*bytes*, pktlen=*bytes*) from *source_address/source_port* to *dest_address/dest_port*, flags: *tcp_flags*, on interface *interface_name*

説明 このメッセージは、TCP 内のヘッダー長が誤りであることを示します。一部のオペレーティングシステムは、ディセーブル状態のソケットへの接続要求に応答するときに、TCP リセット (RST) を正しく処理しません。クライアントが Cisco ASA の外側にある FTP サーバに接続しようとしたときに、FTP がリスニングしていない場合、サーバは RST を送信します。一部のオペレーティングシステムは誤った TCP ヘッダー長を送信します。このために、問題が発生します。UDP は、ICMP ポート到達不能メッセージを使用します。

TCP ヘッダー長は、パケット長よりも長いことを示す場合があります。このために、負のバイト数が転送されます。負の数値は、システム ログメッセージでは符号なし数値として表示されます。このために、正常の場合よりも非常に大きな値が表示されます。たとえば、1 秒に 4 GB 転送されたことを示す場合があります。

推奨処置 不要です。このメッセージは、まれに発生します。

500004

エラー メッセージ %PIX|ASA-4-500004: Invalid transport field for protocol=*protocol*, from *source_address/source_port* to *dest_address/dest_port*

説明 このメッセージは、無効なトランスポート番号がある場合に表示されます。この場合、プロトコルの送信元または宛先のポート番号はゼロです。*protocol* 値は、TCP の場合は 6、UDP の場合は 17 です。

推奨処置 メッセージがその後も表示される場合は、ピアの管理者にお問い合わせください。

501101

エラー メッセージ %PIX|ASA-5-501101: User transitioning priv level

説明 コマンドの特権レベルが変更されました。

推奨処置 不要です。

502101

エラー メッセージ %PIX|ASA-5-502101: New user added to local dbase: Uname: *user*
Priv: *privilege_level* Encpass: *string*

説明 新規のユーザ名レコードが作成されました。このメッセージは、ユーザ名、特権レベル、暗号化パスワードを表示します。

推奨処置 不要です。

502102

エラー メッセージ %PIX|ASA-5-502102: User deleted from local dbase: Uname: *user*
Priv: *privilege_level* Encpass: *string*

説明 ユーザ名レコードが削除されました。このメッセージは、ユーザ名、特権レベル、暗号化パスワードを表示します。

推奨処置 不要です。

502103

エラー メッセージ %PIXPIX|ASA-5-502103: User priv level changed: Uname: *user*
From: *privilege_level* To: *privilege_level*

説明 ユーザの特権レベルが変更されました。

推奨処置 不要です。

502111

エラーメッセージ %PIXPIX|ASA-5-502111: New group policy added: name: *policy_name*
Type: *policy_type*

説明 これは、**group-policy** CLI コマンドを使用してグループ ポリシーが設定されたことを示します。*policy_name* はグループ ポリシーの名前です。*policy_type* は、「internal」または「external」です。

推奨処置 不要です。

502112

エラーメッセージ %PIXPIX|ASA-5-502112: Group policy deleted: name: *policy_name*
Type: *policy_type*

説明 **group-policy** CLI コマンドを使用してグループ ポリシーが削除されました。*policy_name* はグループ ポリシーの名前です。*policy_type* は、「internal」または「external」です。

推奨処置 不要です。

503001

エラーメッセージ %PIXPIX|ASA-5-503001: Process number, Nbr *IP_address* on
interface_name from *string* to *string*, *reason*

説明 OSPF 近接の状態が変更されました。このメッセージには、変更およびその理由が記述されています。このメッセージは、OSPF プロセスに対して **log-adjacency-changes** コマンドが設定されている場合にのみ表示されます。

推奨処置 この問題の原因を判定するには、Cisco TAC に問い合わせてサポートを受けてください。

504001

エラーメッセージ %PIXPIX|ASA-5-504001: Security context *context_name* was added
to the system

説明 セキュリティ コンテキストがシステムに正常に追加されました。

推奨処置 不要です。

504002

エラーメッセージ %PIXPIX|ASA-5-504002: Security context *context_name* was removed
from the system

説明 セキュリティ コンテキストがシステムから正常に削除されました。

推奨処置 不要です。

505001

エラー メッセージ %ASA-5-505001: Module in slot *slotnum* is shutting down. Please wait...

説明 カードのシャットダウン中に生成されます。

推奨処置 不要です。

505002

エラー メッセージ %ASA-5-505002: Module in slot *slotnum* is reloading. Please wait...

説明 カードのリロード中に生成されます。

推奨処置 不要です。

505003

エラー メッセージ %ASA-5-505003: Module in slot *slotnum* is resetting. Please wait...

説明 モジュールのリセット中に生成されます。

推奨処置 不要です。

505004

エラー メッセージ %ASA-5-505004: Module in slot *slotnum* shutdown is complete.

説明 モジュールがシャットダウンされた場合に生成されます。

推奨処置 不要です。

505005

エラー メッセージ %ASA-5-505005: Module in slot *slotnum* is initializing control communication. Please wait...

説明 モジュールが検出され、そのモジュールとの制御チャネル通信を ASA システム モジュールが初期化しているときに生成されます。

推奨処置 不要です。

505006

エラー メッセージ %ASA-5-505006: Module in slot *slotnum* is Up.

説明 モジュールが制御チャネルの初期化を完了して、UP 状態である場合に生成されます。

推奨処置 不要です。

505007

エラー メッセージ %ASA-5-505007: Module in slot *slotnum* is recovering. Please wait...

説明 `hw-module module slotnum recover boot` コマンドによるモジュールの回復中に生成されません。

推奨処置 不要です。

505008

エラー メッセージ %ASA-5-505008: Module in slot *slotnum* software is being updated to *vnewver* (currently *vver*)

説明 このメッセージは、システム モジュールによる 4GE SSM モジュール ソフトウェアのアップグレード中に表示されます。

slotnum : モジュールが存在しているスロット番号。

newver : モジュールへの書き込みが正常に終了しなかったソフトウェアの新しいバージョン番号 (1.0(1)0 など)。

ver : モジュール上のソフトウェアの現在のバージョン番号 (1.0(1)0 など)。

推奨処置 不要です。アップデートは正常に進行中です。

505009

エラー メッセージ %ASA-5-505009: Module in slot *slotnum* software was updated to *vnewver* (previously *vver*)

説明 このメッセージは、4GE SSM モジュール ソフトウェアがシステム モジュールによって正常にアップグレードされた場合に表示されます。

slotnum : モジュールが存在しているスロット番号。

newver : モジュールへの書き込みが正常に終了しなかったソフトウェアの新しいバージョン番号 (1.0(1)0 など)。

ver : モジュール上のソフトウェアの現在のバージョン番号 (1.0(1)0 など)。

推奨処置 不要です。アップデートは正常に完了しました。

506001

エラー メッセージ %ASA-5-506001: *event_source_string event_string*

説明 ファイル システムのステータスが変更されました。このメッセージには、ファイル システムを利用可能または利用不可にしたイベントおよびイベントのソースが記述されています。ファイル システムのステータスを変更させるソースおよびイベントの例には、次のものがあります。

- 外部 Compact Flash が除去された。
- 外部 Compact Flash が挿入された。
- 外部 Compact Flash の不明イベント。

推奨処置 不要です。

507001

エラー メッセージ %PIXPIX|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

説明 このメッセージは、TCP セグメントのアセンブリ中に、再構成バッファ制限を超えた場合に表示されます。

- *source_address/source_port* : 接続を開始しているパケットの送信元 IP アドレスと送信元ポート。
- *dest_address/dest_port* : 接続を開始しているパケットの宛先 IP アドレスと宛先ポート。
- *interface_inside* : 接続を開始したパケットが到着するインターフェイスの名前。
- *interface_outside* : 接続を開始したパケットを外部に送信するインターフェイスの名前。
- *limit* : 設定した初期接続のトラフィック クラスの制限

推奨処置 不要です。

メッセージ 602101 ~ 609002

この項では、602101 から 609002 までのメッセージについて説明します。

602101

エラーメッセージ %PIXPIX|ASA-6-602101: PMTU-D packet *number* bytes greater than effective mtu *number* dest_addr=*dest_address*, src_addr=*source_address*, prot=*protocol*

説明 このメッセージは、Cisco ASA が ICMP 宛先到達不能メッセージを送信する場合、および、フラグメント化が必要であるが、「フラグメント化なし」ビットが設定されている場合に表示されます。

推奨処置 データが正しく送信されることを確認します。

602103

エラーメッセージ %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*.

説明 このメッセージは、SA の MTU が変更されたときに表示されます。IPSec トンネル用のパケットを受信すると、対応する SA が特定され、ICMP パケットで推奨されている MTU に基づいて MTU がアップデートされます。推奨された MTU が 0 より大きく 256 未満の場合、新規 MTU は 256 に設定されます。推奨された MTU が 0 の場合、前の MTU は 256 を引いた値または 256 のどちらか大きい値に設定されます。推奨された MTU が 256 より大きい場合、新規 MTU は推奨された値に設定されます。

src_addr : PMTU 送信側の IP アドレス

rcvd_mtu : PMTU メッセージで受信した推奨 MTU

peer_addr : IPSec ピアの IP アドレス

spi : IPSec のセキュリティ パラメータ インデックス

username : IPSec トンネルに関連付けられているユーザ名

old_mtu : IPSec トンネルに関連付けられている前の MTU

new_mtu : IPSec トンネルに関連付けられている新規 MTU

推奨処置 処置は不要です。

602104

エラーメッセージ %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 : PMTU 送信側の IP アドレス

rcvd_mtu : PMTU メッセージで受信した推奨 MTU

curr_mtu : IPSec トンネルに関連付けられている現行 MTU

peer_addr : IPSec ピアの IP アドレス

spi : IPSec のセキュリティ パラメータ インデックス

username : IPsec トンネルに関連付けられているユーザ名

説明 このメッセージは、IPsec トンネル経由で送信されたパケットがパス MTU を超えたことを示す ICMP メッセージを受信し、推奨 MTU が現行 MTU 以上である場合に表示されます。MTU 値はすでに訂正されているので、MTU の調整は行われません。これは、現在の PMTU メッセージが処理される前に、さまざまな中間ステーションから複数の PMTU メッセージが受信され、MTU が調整された場合に発生します。

推奨処置 処置は不要です。

602201

エラー メッセージ %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*)

説明 このメッセージは、ISAKMP SA が作成された場合に表示されます。

推奨処置 不要です。

602202

エラー メッセージ %PIX|ASA-6-602202: ISAKMP session connected (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP ピアが接続されました。

推奨処置 不要です。

602203

エラー メッセージ %PIXPIX|ASA-6-602203: ISAKMP session disconnected (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP ピアが切断されました。

推奨処置 不要です。

602303

エラー メッセージ %PIX|ASA-6-602303: IPSEC: An *direction tunnel_type* SA (SPI=*spi*) between *local_IP* and *remote_IP* (*username*) has been created.

direction : SA の方向 (着信または発信)

tunnel_type : SA のタイプ (リモート アクセスまたは L2L)

spi : IPsec のセキュリティ パラメータ インデックス

local_IP : トンネルのローカル エンドポイントの IP アドレス

remote_IP : トンネルのリモート エンドポイントの IP アドレス

username : IPsec トンネルに関連付けられているユーザ名

説明 新規のセキュリティ アソシエーション (SA) が作成されました。

推奨処置 処置は不要です。

602304

エラーメッセージ %PIX|ASA-6-602304: IPSEC: An *direction tunnel_type* SA (SPI=*spi*) between *local_IP* and *remote_IP* (*username*) has been deleted.

説明 このメッセージは、SA が削除された場合に表示されます。

direction : SA の方向 (着信または発信)

tunnel_type : SA のタイプ (リモート アクセスまたは L2L)

spi : IPSec のセキュリティ パラメータ インデックス

local_IP : トンネルのローカル エンドポイントの IP アドレス

remote_IP : トンネルのリモート エンドポイントの IP アドレス

username : IPSec トンネルに関連付けられているユーザ名

推奨処置 処置は不要です。

603101

エラーメッセージ %PIX|ASA-6-603101: PPTP received out of seq or duplicate pkt, tnl_id=*number*, sess_id=*number*, seq=*number*.

説明 セキュリティ アプライアンスが、間違った順番の PPTP パケットまたは重複した PPTP パケットを受信しました。

推奨処置 このようなパケットが数多く発生する場合は、ピアの管理者に問い合せて、クライアントの PPTP コンフィギュレーションを確認します。

603102

エラーメッセージ %PIX|ASA-6-603102: PPP virtual interface *interface_name* - user: *user* aaa authentication started.

説明 セキュリティ アプライアンスが AAA サーバに認証要求を送信しました。

推奨処置 不要です。

603103

エラーメッセージ %PIX|ASA-6-603103: PPP virtual interface *interface_name* - user: *user* aaa authentication *status*

説明 セキュリティ アプライアンスが AAA サーバから認証応答を受信しました。

推奨処置 不要です。

603104

エラー メッセージ %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*

説明 PPTP トンネルが作成されました。

推奨処置 不要です。

603105

エラー メッセージ %PIX|ASA-6-603105: PPTP Tunnel deleted, tunnel_id = *number*, remote_peer_ip = *remote_address*

説明 PPTP トンネルが削除されました。

推奨処置 不要です。

603106

エラー メッセージ %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*

説明 L2TP トンネルが作成されました。

推奨処置 不要です。

603107

エラー メッセージ %PIX|ASA-6-603107: L2TP Tunnel deleted, tunnel_id = *number*, remote_peer_ip = *remote_address*

説明 L2TP トンネルが削除されました。

推奨処置 不要です。

603108

エラー メッセージ %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*

説明 このメッセージは、新規 PPPoE トンネルが作成されるたびに表示されます。

推奨処置 不要です。

603109

エラー メッセージ %PIX|ASA-6-603109: Teardown PPPOE Tunnel at *interface_name*, tunnel-id = *number*, remote-peer = *IP_address*

説明 このメッセージは、新規 PPPoE トンネルが削除されるたびに表示されます。

推奨処置 不要です。

604101

エラー メッセージ %PIX|ASA-6-604101: DHCP client interface *interface_name*: Allocated ip = *IP_address*, mask = *netmask*, gw = *gateway_address*

説明 Cisco ASA DHCP クライアントが DHCP サーバから IP アドレスを正常に取得しました。dhcpc コマンド ステートメントによって、Cisco ASA は、ネットワーク インターフェイスの IP アドレスおよびネットワーク マスクを DHCP サーバから取得でき、またデフォルト ルートを取得できます。デフォルト ルート ステートメントでは、ゲートウェイ アドレスがデフォルト ルータのアドレスとして使用されます。

推奨処置 不要です。

604102

エラー メッセージ %PIX|ASA-6-604102: DHCP client interface *interface_name*: address released

説明 Cisco ASA DHCP クライアントが、割り当てられた IP アドレスを解放して DHCP サーバに戻しました。

推奨処置 不要です。

604103

エラー メッセージ %PIX|ASA-6-604103: DHCP daemon interface *interface_name*: address granted *MAC_address* (*IP_address*)

説明 Cisco ASA DHCP サーバによって、IP アドレスが外部クライアントに付与されました。

推奨処置 不要です。

604104

エラー メッセージ %PIX|ASA-6-604104: DHCP daemon interface *interface_name*: address released

説明 外部クライアントが、IP アドレスを解放して Cisco ASA DHCP サーバに戻しました。

推奨処置 不要です。

605004

エラー メッセージ %PIX|ASA-6-605004: Login denied from *source-address/source-port* to *interface:destination/service* for user "username"

ユーザがコンソールにログインしようとする、次の形式のメッセージが表示されます。

```
Login denied from serial to console for user "username"
```

説明 このメッセージは、セキュリティ アプライアンスへの誤ったログインの試行、またはログインの失敗の場合に表示されます。すべてのログインに対して、セッションあたり 3 回の試行が許容され、不正な試行が 3 回行われると、そのセッションは終了します。SSH ログインおよび TELNET ログインの場合、このメッセージは、3 回目の試行の失敗後、または 1 回または 2 回の試行の失敗後に TCP セッションが終了したときに、生成されます。他のタイプの管理セッションの場合、このメッセージは試行に失敗するたびに生成されます。

source-address : ログイン試行の送信元アドレス

source-port : ログイン試行の送信元ポート

interface : 宛先管理インターフェイス

destination : 宛先 IP アドレス

service : 宛先サービス

username : 宛先管理インターフェイス

推奨処置 このメッセージの表示頻度が少ない場合、処置は不要です。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。ユーザと通信して、ユーザ名とパスワードを確認します。

605005

エラー メッセージ %PIX|ASA-6-605005: Login permitted from *source-address/source-port* to *interface:destination/service* for user "username"

ユーザがコンソールにログインすると、次の形式のメッセージが表示されます。

```
Login permitted from serial to console for user "username"
```

説明 このメッセージは、ユーザが正常に認証されて、管理セッションが開始されると表示されます。

source-address : ログイン試行の送信元アドレス

source-port : ログイン試行の送信元ポート

interface : 宛先管理インターフェイス

destination : 宛先 IP アドレス

service : 宛先サービス

username : 宛先管理インターフェイス

推奨処置 処置は不要です。

606001

エラーメッセージ %PIX|ASA-6-606001: ASDM session number *number* from *IP_address* started

説明 このメッセージは、管理者が正常に認証されて、ASDM セッションが開始されたことを示します。

推奨処置 不要です。

606002

エラーメッセージ %PIX|ASA-6-606002: ASDM session number *number* from *IP_address* ended

説明 このメッセージは、ASDM セッションが終了したことを示します。

推奨処置 不要です。

606003

エラーメッセージ %PIX|ASA-6-606003: ASDM logging session number *id* from *IP_address* started *id* session ID assigned

説明 ASDM ロギング接続が、リモート管理クライアントによって開始されました。

IP_address : リモート管理クライアントの IP アドレス

推奨処置 ユーザによる処置は不要です。

606004

エラーメッセージ %PIX|ASA-6-606004: ASDM logging session number *id* from *IP_address* ended

説明 ASDM ロギング接続が終了しました。

id : セッション ID が割り当てられました。

IP_address : リモート管理クライアントの IP アドレス。

推奨処置 ユーザによる処置は不要です。

607001

エラーメッセージ %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

説明 このメッセージは、SIP メッセージを検査後、**fixup sip** コマンドによって SIP 接続が割り当て済みであったことを示します。*connection_type* は、次の文字列のいずれかです。

- SIGNALLING UDP
- SIGNALLING TCP

- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

推奨処置 不要です。

608001

エラー メッセージ %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

説明 このメッセージは、Skinny メッセージを検査後、**fixup skinny** コマンドによって Skinny 接続が割り当て済みであったことを示します。*connection_type* は、次の文字列のいずれかです。

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

推奨処置 不要です。

609001

エラー メッセージ %PIX|ASA-6-609001: Built local-host *interface_name:IP_address*

説明 ネットワーク ステート コンテナは、インターフェイス *interface_name* に接続されたホスト *IP_address* 用に予約されています。これは情報メッセージです。

推奨処置 不要です。

609002

エラー メッセージ %PIX|ASA-6-609002: Teardown local-host *interface_name:IP_address* duration *time*

説明 インターフェイス *interface_name* に接続されているホスト *IP_address* 用のネットワーク ステート コンテナが削除されました。これは情報メッセージです。

推奨処置 不要です。

610001

エラーメッセージ %PIX|ASA-3-610001: NTP daemon interface *interface_name*: Packet denied from *IP_address*

説明 設定された NTP サーバのいずれとも一致しないホストから NTP パケットを受信しました。Cisco ASA は NTP クライアントにすぎません。タイム サーバではないので、NTP 要求には応答しません。

推奨処置 不要です。

610002

エラーメッセージ %PIX|ASA-3-610002: NTP daemon interface *interface_name*: Authentication failed for packet from *IP_address*

説明 受信した NTP パケットの認証チェックが失敗しました。

推奨処置 Cisco ASA と NTP サーバの両方が、認証を使用するように設定されており、キー番号とキー値が同じであることを確認します。

610101

エラーメッセージ %PIX|ASA-6-610101: Authorization failed: Cmd: *command* Cmdtype: *command_modifier*

説明 指摘されたコマンドのコマンド認可が失敗しました。*command_modifier* は、次の文字列のいずれかです。

- **cmd** (この文字列は、コマンドに修飾子がないことを意味します)
- **clear**
- **no**
- **show**

説明 Cisco ASA がリストされた 4 コマンド タイプ以外の値を検出すると、メッセージ「unknown command type」が表示されます。

推奨処置 不要です。

611101

エラーメッセージ %PIX|ASA-6-611101: User authentication succeeded: Uname: *user*

説明 セキュリティ アプライアンスのアクセスに成功したときに、ユーザ認証に成功しました。

推奨処置 不要です。

611102

エラー メッセージ %PIX|ASA-6-611102: User authentication failed: Uname: *user*

説明 セキュリティ アプライアンスにアクセスしようとしたときに、ユーザ認証に失敗しました。

推奨処置 不要です。

611103

エラー メッセージ %PIX|ASA-5-611103: User logged out: Uname: *user*

説明 指摘されたユーザはログアウトされました。

推奨処置 不要です。

611104

エラー メッセージ %PIX|ASA-5-611104: Serial console idle timeout exceeded

説明 ユーザ アクティビティがなかったために、セキュリティ アプライアンスのシリアル コンソールに設定されたアイドル タイムアウトを超えました。

推奨処置 不要です。

611301

エラー メッセージ %PIX|ASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: *mapped_address*

説明 スプリット トンネリングなしでクライアント モード用の VPN クライアント ポリシーがインストールされました。

推奨処置 不要です。

611302

エラー メッセージ %PIX|ASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling

説明 スプリット トンネリングなしでネットワーク拡張モード用の VPN クライアント ポリシーがインストールされました。

推奨処置 不要です。

611303

エラーメッセージ %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* ...

説明 スプリット トンネリング付きでクライアント モード用の VPN クライアント ポリシーがインストールされました。

推奨処置 不要です。

611304

エラーメッセージ %PIX|ASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: *IP_address/netmask IP_address/netmask* ...

説明 スプリット トンネリング付きでネットワーク拡張モード用の VPN クライアント ポリシーがインストールされました。

推奨処置 不要です。

611305

エラーメッセージ %PIX|ASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: *IP_address* Secondary DNS: *IP_address* Primary WINS: *IP_address* Secondary WINS: *IP_address*

説明 DHCP 用の VPN クライアント ポリシーがインストールされました。

推奨処置 不要です。

611306

エラーメッセージ %PIX|ASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed

説明 VPN クライアント ダウンロード ポリシーの一部として、Perfect Forward Secrecy (PFS; 完全転送秘密) が設定されました。

推奨処置 不要です。

611307

エラーメッセージ %PIX|ASA-6-611307: VPNClient: Head end : *IP_address*

説明 VPN クライアントが、指摘されたヘッドエンドに接続されています。

推奨処置 不要です。

611308

エラー メッセージ %PIX|ASA-6-611308: VPNClient: Split DNS Policy installed: List of domains: *string string ...*

説明 VPN クライアント ダウンロード ポリシーの一部として、スプリット DNS ポリシーがインストールされました。

推奨処置 不要です。

611309

エラー メッセージ %PIX|ASA-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: *IP_address*

説明 VPN クライアントが、前にインストールされたポリシーを切断しアンインストールしています。

推奨処置 不要です。

611310

エラー メッセージ %PIX|ASA-6-611310: VPNClient: XAUTH Succeeded: Peer: *IP_address*

説明 VPN クライアント Xauth が、指摘されたヘッドエンドで成功しました。

推奨処置 不要です。

611311

エラー メッセージ %PIX|ASA-6-611311: VPNClient: XAUTH Failed: Peer: *IP_address*

説明 VPN クライアント Xauth が、指摘されたヘッドエンドで失敗しました。

推奨処置 不要です。

611312

エラー メッセージ %PIX|ASA-6-611312: VPNClient: Backup Server List: *reason*

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、このメッセージは、Easy VPN サーバがバックアップ サーバのリストをセキュリティ アプライアンスにダウンロードしたことを示します。このリストによって、ローカルで設定されたバックアップ サーバはすべて上書きされます。ダウンロードされたリストが空の場合、セキュリティ アプライアンスはバックアップ サーバを使用しません。*reason* は、次のメッセージのどちらかです。

- バックアップ サーバの IP アドレスのリスト
- Received NULL list.Deleting current backup servers.

推奨処置 不要です。

611313

エラー メッセージ %PIX|ASA-3-611313: VPNClient: Backup Server List Error: *reason*

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスであり、Easy VPN サーバがバックアップ サーバのリストをセキュリティ アプライアンスにダウンロードする場合、このメッセージは、リストに無効な IP アドレスまたはホスト名が含まれていることを示します。セキュリティ アプライアンスは、DNS はサポートしません。したがって、**name** コマンドを使用して名前を IP アドレスに手動でマッピングしないかぎり、サーバのホスト名はサポートされません。

推奨処置 Easy VPN サーバ上で、サーバの IP アドレスが正しいことを確認して、ホスト名ではなく IP アドレスでサーバを設定します。サーバでホスト名を使用する必要がある場合は、Easy VPN リモート デバイスで **name** コマンドを使用して IP アドレスを名前にマッピングします。

611314

エラー メッセージ %PIX|ASA-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: *IP_address* has redirected the to server *IP_address*

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、ロード バランシング クラスタのマスター サーバによって、セキュリティ アプライアンスが特定のサーバに接続するようにリダイレクトされます。

推奨処置 不要です。

611315

エラー メッセージ %PIX|ASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member *IP_address*

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、このメッセージは、セキュリティ アプライアンスがロード バランシング クラスタ サーバから切断されていることを示します。

推奨処置 不要です。

611316

エラー メッセージ %PIX|ASA-6-611316: VPNClient: Secure Unit Authentication Enabled

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって Secure Unit Authentication (SUA; セキュア ユニット認証) がイネーブルにされます。

推奨処置 不要です。

611317

エラー メッセージ %PIX|ASA-6-611317: VPNClient: Secure Unit Authentication Disabled

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによってセキュア ユニット認証 (SUA) がディセーブルにされます。

推奨処置 不要です。

611318

エラー メッセージ %PIX|ASA-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: *IP_address* Auth Server Port: *port* Idle Timeout: *time*

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって、ネットワーク内側のセキュリティ アプライアンス上のユーザに対して Individual User Authentication (IUA; 個別ユーザ認証) がイネーブルにされます。

- *IP_address*: セキュリティ アプライアンスから認証要求が送信されるサーバの IP アドレス。
- *port*: セキュリティ アプライアンスから認証要求が送信されるサーバのポート。
- *time*: 認証クレデンシャルのアイドル タイムアウト値。

推奨処置 不要です。

611319

エラー メッセージ %PIX|ASA-6-611319: VPNClient: User Authentication Disabled

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって、ネットワーク内のセキュリティ アプライアンス上のユーザに対して個別ユーザ認証 (IUA) がディセーブルにされます。

推奨処置 不要です。

611320

エラー メッセージ %PIX|ASA-6-611320: VPNClient: Device Pass Thru Enabled

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによってデバイス パススルーがイネーブルにされます。デバイス パススルー機能によって、認証を実行できないデバイス (IP 電話など) は、個別ユーザ認証 (IUA) がイネーブルの場合、認証が免除されます。

推奨処置 不要です。Easy VPN サーバによってこの機能がイネーブルにされている場合、セキュリティ アプライアンスで `vpnclient mac-exempt` コマンドを使用して、認証 (IUA) を免除するデバイスが指定できます。

611321

エラー メッセージ %PIX|ASA-6-611321: VPNClient: Device Pass Thru Disabled

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによってデバイス パススルーがディセーブルにされます。

推奨処置 不要です。

611322

エラー メッセージ %PIX|ASA-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスで、ダウンロードされた VPN ポリシーによってセキュア ユニット認証 (SUA) がディセーブルにされている場合、Easy VPN サーバは 2 要素 /SecurID/cryptocard ベースの認証メカニズムで、XAUTH を使用しているセキュリティ アプライアンスを認証します。

推奨処置 2 要素 /SecurID/cryptocard ベースの認証メカニズムを使用して Easy VPN リモート デバイスを認証する場合は、サーバ上の SUA をイネーブルにします。

611323

エラー メッセージ %PIX|ASA-6-611323: VPNClient: Duplicate split nw entry

説明 セキュリティ アプライアンスが Easy VPN リモート デバイスの場合、このメッセージは、ダウンロードされた VPN ポリシーに重複したスプリット ネットワーク エントリが含まれていることを示します。エントリは、ネットワーク アドレスとネットワーク マスクの両方に一致する場合、重複と見なされます。

推奨処置 Easy VPN サーバ上の VPN ポリシーから重複したスプリット ネットワーク エントリを削除します。

612001

エラー メッセージ %PIX|ASA-5-612001: Auto Update succeeded:filename, version:number

説明 Auto Update Server からのアップデートが成功しました。filename 変数は、image、ASDM file、または configuration です。version number 変数は、アップデートのバージョン番号です。

推奨処置 不要です。

612002

エラー メッセージ %PIX|ASA-4-612002: Auto Update failed:filename, version:number, reason:reason

説明 このメッセージは、Auto Update Server からのアップデートが失敗したことを示します。filename 変数は、image、ASDM file、または configuration です。version number 変数は、アップデートのバージョン番号です。reason 変数には、アップデートが失敗した理由が記述されています。考えられる失敗の理由としては、無効なイメージ ファイル、サーバへの接続が失われたこと、コンフィギュレーション エラーなどがあります。

推奨処置 Auto Update Server のコンフィギュレーションを確認します。

612003

エラー メッセージ %PIX|ASA-4-612003:Auto Update failed to contact:url, reason:reason

説明 Auto Update デーモンが指摘された URL url にアクセスできないことを示します。これは、Auto Update Server の URL、または Auto Update Server から返されたファイル サーバ URL の1つである場合があります。reason フィールドには、接続が失敗した理由が記述されています。考えられる失敗の理由としては、サーバからの応答がない、認証の失敗、ファイルが見つからないなどがあります。

推奨処置 Auto Update Server のコンフィギュレーションを確認します。

613001

エラー メッセージ %PIX|ASA-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number

説明 メモリ破損のために、OSPF がデータベースでチェックサム エラーを検出しました。

推奨処置 OSPF プロセスを再起動します。

613002

エラー メッセージ %PIX|ASA-6-613002: interface interface_name has zero bandwidth

説明 このインターフェイスの帯域幅がゼロと報告されています。

推奨処置 この問題の原因を判定するには、Cisco TAC に問い合わせてサポートを受けてください。

613003

エラーメッセージ %PIX|ASA-6-613003: *IP_address netmask* changed from *area string* to *area string*

説明 OSPF コンフィギュレーションの変更によって、ネットワーク範囲のエリアが変更されました。

推奨処置 正しいネットワーク範囲で OSPF を再設定します。

614001

エラーメッセージ %PIX|ASA-6-614001: Split DNS: request patched from server: *IP_address* to server: *IP_address*

説明 スプリット DNS によって、DNS クエリーが元の宛先サーバから企業のプライマリ DNS サーバにリダイレクトされています。

推奨処置 不要です。

614002

エラーメッセージ %PIX|ASA-6-614002: Split DNS: reply from server:*IP_address* reverse patched back to original server:*IP_address*

説明 スプリット DNS によって、DNS クエリーが企業の DNS サーバから元の宛先サーバにリダイレクトされています。

推奨処置 不要です。

615001

エラーメッセージ %PIX|ASA-6-615001: vlan number not available for firewall interface

説明 スイッチによって、VLAN が FWSM から削除されました。

推奨処置 これは情報メッセージです。

615002

エラーメッセージ %PIX|ASA-6-615002: vlan number available for firewall interface

説明 スイッチによって、VLAN が FWSM に追加されました。

推奨処置 これは情報メッセージです。

616001

エラー メッセージ %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*

説明 MGCP データ チャネル接続 (RTP または RTCP) は割り当て済みです。このメッセージ テキストには、接続の事前割り当てを起動したメッセージも特定されています。

推奨処置 不要です。

617001

エラー メッセージ %PIX|ASA-6-617001: GTPv *version msg_type* from *source_interface:source_address/source_port* not accepted by *source_interface:dest_address/dest_port*

説明 このメッセージは、ピアが要求を受け入れなかった場合に表示されます。これは通常、Create PDP Context 要求で表示されます。

推奨処置 不要です。

617002

エラー メッセージ %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*

説明 このメッセージは、PDP コンテキストが有効期限切れになったため、Delete PDP Context Request/Response が交換されたため、またはユーザが CLI を使用して PDP コンテキストを削除したために、PDP コンテキストがデータベースから削除された場合に表示されます。

推奨処置 不要です。

617003

エラー メッセージ %PIX|ASA-6-617003: GTP Tunnel created from *source_interface:source_address/source_port* to *source_interface:dest_address/dest_port*

説明 このメッセージは、要求を受け入れた Create PDP Context Response を受信した後に、GTP トンネルが作成された場合に表示されます。

推奨処置 不要です。

617004

エラーメッセージ %PIX|ASA-6-617004: GTP connection created for response from *source_interface:source_address/0* to *source_interface:dest_address/dest_port*

説明 このメッセージは、Create PDP Context Request 内の SGSN シグナリング アドレスまたは Create PDP Context Response 内の GGSN シグナリング アドレスが、この要求また応答を送信している SGSN または GGSN と異なる場合に表示されます。

推奨処置 不要です。

620001

エラーメッセージ %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*

説明 Cisco ASA では、指摘された CTIQBE メディア トラフィックに接続オブジェクトが割り当て済みです。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

推奨処置 不要です。

620002

エラーメッセージ %PIX|ASA-4-620002: Unsupported CTIQBE version: *hex:* from *interface_name:IP_address/port* to *interface_name:IP_address/port*

説明 Cisco ASA が、サポートしていないバージョン番号の CTIQBE メッセージを受信しました。Cisco ASA によって、パケットは廃棄されます。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

推奨処置 ログメッセージに取り込まれているバージョン番号が不適当に大きい場合 (10 より大きい場合)、パケットの形式が誤っている、CTIQBE 以外のパケットである、または Cisco ASA に到着する前に破壊されている可能性があります。パケットの送信元を判別することを推奨します。バージョン番号が合理的な小さな数値 (10 以下) の場合は、Cisco TAC に問い合せて、この CTIQBE バージョンをサポートする新規の Cisco ASA イメージが入手可能かどうかを調べます。

621001

エラーメッセージ %PIX|ASA-6-621001: Interface *interface_name* does not support multicast, not enabled

説明 このメッセージは、マルチキャストをサポートしていないインターフェイス上の PIM をイネーブルにしようとした場合に表示されます。

推奨処置 エラーメッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

621002

エラー メッセージ %PIX|ASA-6-621002: Interface *interface_name* does not support multicast, not enabled

説明 このメッセージは、マルチキャストをサポートしていないインターフェイス上の igmp をイネーブルにしようとした場合に表示されます。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

621003

エラー メッセージ %PIX|ASA-6-621003: The event queue size has exceeded *number*

説明 このメッセージは、作成されたイベント マネージャ数が想定された数を超えた場合に表示されます。

推奨処置 エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

621006

エラー メッセージ %PIX|ASA-6-621006: Mrib disconnected, (*IP_address*, *IP_address*) event cancelled

説明 このメッセージは、データ駆動イベントを起動するパケットを受信したが、MRIB への接続がダウンしている場合に表示されます。通知はキャンセルされました。

推奨処置 システムが動作した後もこのメッセージが表示される場合は、エラー メッセージをコピーし、コンフィギュレーションおよびこのエラーの発端になったイベントの詳細と一緒に Cisco TAC に送付してください。

621007

エラー メッセージ %PIX|ASA-6-621007: Bad register from *interface_name*:*IP_address* to *IP_address* for (*IP_address*, *IP_address*)

説明 このメッセージは、PIM ルータが、ランデブー ポイントとして設定されている場合、またはネットワーク アドレス変換 (NAT) で別の PIM ルータから PIM レジスタ パケットを受信した場合に表示されます。このパケット内のカプセル化されたデータは無効です。

推奨処置 送信ルータが誤って RFC 以外のレジスタを送信している可能性があります。送信側のルータをアップグレードします。

メッセージ 701001 ~ 720073

この項では、701001 から 720073 までのメッセージについて説明します。

ほとんどの ISAKMP syslog には、トンネルの識別に役立つ追加オブジェクトの共通セットがあります。これらのオブジェクトには、使用可能な場合、システム ログ メッセージの記述テキストに先行します。システム ログ メッセージが生成される時点でオブジェクトが不明の場合、固有の「*heading = value*」という組み合わせは表示されません。

このオブジェクトは次のように追加されます。

```
"Group = groupname, Username = user, IP = IP_address, ..."
```

ここで、Group はトンネル グループを特定し、username はローカル データベースまたは AAA サーバのユーザ名、IP アドレスはリモート アクセス クライアントまたは L2L ピアのパブリック IP アドレスです。

701001

エラー メッセージ %PIX|ASA-7-701001: alloc_user() out of Tcp_user objects

説明 これは AAA メッセージです。モジュールが新しい AAA 要求を処理するのにユーザ認証のレートが高すぎる場合、このメッセージが表示されます。

推奨処置 floodguard enable コマンドで Flood Defender をイネーブルにします。

701002

エラー メッセージ %PIX|ASA-7-701002: alloc_user() out of Tcp_proxy objects

説明 これは AAA メッセージです。モジュールが新しい AAA 要求を処理するのにユーザ認証のレートが高すぎる場合、このメッセージが表示されます。

エラー メッセージ Enable Flood Defender with the **floodguard enable** command.

702201

エラー メッセージ %PIX|ASA-7-702201: ISAKMP Phase 1 delete received (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP 削除メッセージが受信されました。

推奨処置 不要です。

702202

エラー メッセージ %PIX|ASA-7-702202: ISAKMP Phase 1 delete sent (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP 削除メッセージが送信されました。

推奨処置 不要です。

702203

エラー メッセージ %PIX|ASA-7-702203: ISAKMP DPD timed out (local *IP_address* (initiator|responder), remote *IP_address*)

説明 リモートピアが応答しないので、DPDによってピアがタイムアウトされました。

推奨処置 リモートホストへのネットワーク接続を確認します。

702204

エラー メッセージ %PIX|ASA-7-702204: ISAKMP Phase 1 retransmission (local *IP_address* (initiator|responder), remote *IP_address*)

説明 リモートピアは応答していません。ISAKMPは前のパケットを再転送しています。

推奨処置 リモートホストへのネットワーク接続をチェックし、ローカルデバイスおよびリモートデバイスのVPNコンフィギュレーションを確認します。

702205

エラー メッセージ %PIX|ASA-7-702205: ISAKMP Phase 2 retransmission (local *IP_address* (initiator|responder), remote *IP_address*)

説明 リモートピアは応答していません。ISAKMPは前のパケットを再転送しています。

推奨処置 リモートホストへのネットワーク接続をチェックし、ローカルデバイスおよびリモートデバイスのVPNコンフィギュレーションを確認します。

702206

エラー メッセージ %PIX|ASA-7-702206: ISAKMP malformed payload received (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMPが、不正または形式が誤ったメッセージを受信しました。リモートピアと同期していないという問題、メッセージの解釈の問題、または間違った順番でのメッセージ受信を示す場合があります。

推奨処置 事前共有キーを使用している場合は、事前共有キーがローカルおよびリモートのデバイスで正しく設定されていることを確認します。ローカルおよびリモートのコンフィギュレーションをチェックします。SAを起動できない場合は、それ以外のトラブルシューティングが必要になることがあります。

702207

エラーメッセージ %PIX|ASA-7-702207: ISAKMP duplicate packet detected (local *IP_address* (initiator|responder), remote *IP_address*)

説明 前に受信したパケットと重複したパケットを ISAKMP が受信しました。正常動作中に発生することも、ISAKMP 交換で以前のエラーの副作用として発生することもあります。

推奨処置 接続を確認し、ローカルおよびリモートのコンフィギュレーションも確認します。

702208

エラーメッセージ %PIX|ASA-7-702208: ISAKMP Phase 1 exchange started (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP は、リモートピアとの新しいフェーズ1のメッセージ交換を開始しました。

推奨処置 不要です。

702209

エラーメッセージ %PIX|ASA-7-702209: ISAKMP Phase 2 exchange started (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP は、リモートピアとの新しいフェーズ2のメッセージ交換を開始しました。

推奨処置 不要です。

702210

エラーメッセージ %PIX|ASA-7-702210: ISAKMP Phase 1 exchange completed(local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP はフェーズ1の交換を終了しました。

推奨処置 不要です。

702211

エラーメッセージ %PIX|ASA-7-702211: ISAKMP Phase 2 exchange completed(local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP はフェーズ2の交換を終了しました。

推奨処置 不要です。

702212

エラー メッセージ %PIX|ASA-7-702212: ISAKMP Phase 1 initiating rekey (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP が、フェーズ 1 キー再生成を開始します。

推奨処置 不要です。

702305

エラー メッセージ %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.

説明 このメッセージは、新規のトンネルのネゴシエーション中に 40 億を超えるパケットを IPsec トンネルで受信した場合に表示されます。

direction : SA の方向 (着信または発信)

tunnel_type : SA のタイプ (リモートアクセスまたは L2L)

spi : IPsec のセキュリティ パラメータ インデックス

local_IP : トンネルのローカル エンドポイントの IP アドレス

remote_IP : トンネルのリモート エンドポイントの IP アドレス

username : IPsec トンネルに関連付けられているユーザ名

推奨処置 ピアの管理者に問い合せて、SA ライフタイム設定を比較します。

702307

エラー メッセージ %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 の方向 (着信または発信)

tunnel_type : SA のタイプ (リモートアクセスまたは L2L)

spi : IPsec のセキュリティ パラメータ インデックス

local_IP : トンネルのローカル エンドポイントの IP アドレス

remote_IP : トンネルのリモート エンドポイントの IP アドレス

username : IPsec トンネルに関連付けられているユーザ名

説明 このメッセージは、SA データ ライフスパンが期限切れになるときに表示されます。このメッセージは、IPsec SA が、転送したデータ量の結果、キーを再生成していることを示します。この情報は、キー再生成の問題をデバッグする場合に役立ちます。

推奨処置 処置は不要です。

703001

エラーメッセージ %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*

説明 Cisco ASA は、サポートされていないバージョン番号の H.323 パケットを受信しました。Cisco ASA が、パケットのプロトコルフィールドをサポートされている最新バージョンに再コード化する場合があります。

推奨処置 Cisco ASA が VoIP ネットワークにおいてサポートしている H.323 のバージョンを使用します。

703002

エラーメッセージ %PIX|ASA-7-703002: Received H.225 Release Complete with *newConnectionNeeded* for *interface_name:IP_address* to *interface_name:IP_address/port*

説明 これはデバッグメッセージで、指摘された H.225 メッセージを Cisco ASA が受信したこと、および指摘された 2 つの H.323 エンドポイントに対して新規シグナリング接続オブジェクトを Cisco ASA がオープンしたことを示します。

推奨処置 不要です。

709001, 709002

エラーメッセージ %PIX|ASA-7-709001: FO replication failed: *cmd=command* returned=*code*

エラーメッセージ %PIX|ASA-7-709002: FO unreplicable: *cmd=command*

説明 この 2 つのフェールオーバー メッセージは、開発のデバッグテスト段階でのみ表示されます。

推奨処置 不要です。

709003

エラーメッセージ %PIX|ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.

説明 これはフェールオーバー メッセージです。このメッセージは、アクティブ装置が自分のコンフィギュレーションのスタンバイ装置への複製を開始すると表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

709004

エラー メッセージ %PIX|ASA-1-709004: (Primary) End Configuration Replication (ACT)

説明 これはフェールオーバー メッセージです。このメッセージは、アクティブ装置が自分のコンフィギュレーションのスタンバイ装置上への複製を完了すると表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

709005

エラー メッセージ %PIX|ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.

説明 このメッセージは、スタンバイ Cisco ASA がアクティブ Cisco ASA からコンフィギュレーション複製の最初の部分を受け取ったことを示します。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

709006

エラー メッセージ %PIX|ASA-1-709006: (Primary) End Configuration Replication (STB)

説明 これはフェールオーバー メッセージです。このメッセージは、スタンバイ装置がアクティブ装置から送信されたコンフィギュレーションの複製を完了したときに表示されます。(Primary) は、セカンダリ装置の場合は (Secondary) と示されることもあります。

推奨処置 不要です。

709007

エラー メッセージ %PIX|ASA-2-709007: Configuration replication failed for command *command*

説明 これはフェールオーバー メッセージです。このメッセージは、スタンバイ装置がアクティブ装置から送信されたコンフィギュレーションの複製を完了できない場合に表示されます。障害を発生させたコマンドが、メッセージの末尾に表示されます。

推奨処置 コマンド名を記録して、Cisco TAC に通知してください。

710001

エラー メッセージ %PIX|ASA-7-710001: TCP access requested from
source_address/source_port to *interface_name:dest_address/service*

説明 このメッセージは、Cisco ASA 宛での最初の TCP パケットで TCP セッションの確立を要求する場合に表示されます。このパケットは、3 ウェイ ハンドシェイクの最初の SYN パケットです。このメッセージは、対応するアクセス コントロール リスト (telnet、http、または ssh) でパケットが許可されている場合に表示されます。しかし、SYN クッキー検証はまだ完了しておらず、状態は予約されていません。

推奨処置 不要です。

710002

エラー メッセージ %PIX|ASA-7-710002: {TCP|UDP} access permitted from
source_address/source_port to *interface_name:dest_address/service*

説明 TCP 接続の場合、このメッセージは、Cisco ASA 宛での 2 番目の TCP パケットで TCP セッションの確立を要求する場合に表示されます。このパケットは、3 ウェイ ハンドシェイクの最終 ACK です。このメッセージは、対応するアクセス コントロール リスト (Telnet、HTTP、または SSH) でパケットが許可されている場合に表示されます。また、SYN クッキー検証が成功し、状態が TCP セッション用に予約されます。

UDP 接続の場合、接続は許可されています。たとえば、このメッセージは、認可された SNMP 管理ステーションからの SNMP 要求をモジュールが受信し、その要求が処理されたときに表示されます (サービス snmp で)。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

推奨処置 不要です。

710003

エラー メッセージ %PIX-3-710003: {TCP|UDP} access denied by ACL from
source_IP/source_port to *interface_name:dest_IP/service*

次に例を示します。

```
%PIX-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to  
outside:95.1.1.13/1005
```

説明 このメッセージは、セキュリティ アプライアンスがインターフェイス サービスへの接続試行を拒否した場合に表示されます。たとえば、このメッセージは、認可されていない SNMP 管理ステーションからの SNMP 要求をファイアウォールが受信した場合に表示されることがあります。

推奨処置 show run http コマンド、show run ssh コマンド、または show run telnet コマンドを使用して、ホストまたはネットワークからのサービス アクセスを許可するようにセキュリティ アプライアンスが設定されていることを確認します。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。

710004

エラー メッセージ %PIX|ASA-7-710004: TCP connection limit exceeded from *source_address/source_port* to *interface_name:dest_address/service*

説明 サービス用の最大 Cisco ASA 管理接続数を超過しました。Cisco ASA は、管理サービスあたり最大 5 つの同時管理接続を許可します。

推奨処置 コンソールから、kill コマンドを使用して不要なセッションを解放します。

710005

エラー メッセージ %PIX|ASA-7-710005: {TCP|UDP} request discarded from *source_address/source_port* to *interface_name:dest_address/service*

説明 このメッセージは、Cisco ASA に UDP 要求を処理する UDP サーバがない場合に表示されます。このメッセージは、Cisco ASA 上のどのセッションにも属していない TCP パケットを示すこともあります。さらにこのメッセージは、認可されたホストからの場合でも、ペイロードが空の SNMP 要求を Cisco ASA が受信した場合に表示されます (サービス snmp で)。サービスが snmp の場合、このメッセージは最大でも 10 秒ごとに 1 回の発生として、ログ受信プログラムが過負荷にならないようにします。

推奨処置 DHCP、RIP または NetBios などのブロードキャスト サービスの利用が多いネットワークでは、このメッセージの頻度が高くなる場合があります。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。

710006

エラー メッセージ %PIX|ASA-7-710006: *protocol* request discarded from *source_address* to *interface_name:dest_address*

説明 このメッセージは、Cisco ASA に IP プロトコル要求を処理する IP サーバがない場合に表示されます。たとえば、Cisco ASA が TCP または UDP でない IP パケットを受信し、Cisco ASA が要求を処理できない場合です。

推奨処置 DHCP、RIP または NetBios などのブロードキャスト サービスの利用が多いネットワークでは、このメッセージの頻度が高くなる場合があります。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。

711001

エラー メッセージ %PIX|ASA-7-711001: debug_trace_msg

説明 このシステム ログ メッセージは、ロギング機能に対してロギング デバッグ トレース コマンドを入力すると表示されます。ロギング デバッグ トレースがイネーブルの場合、すべてのデバッグ メッセージはシステム ログ メッセージにリダイレクトされて処理されます。セキュリティ上の理由から、システム ログ メッセージ出力は暗号化するが、またはセキュア アウトオブバンド ネットワークで送信する必要があります。

推奨処置 不要です。

711002

エラー メッセージ %PIX|ASA-7-711002: Task ran for *elapsed_time* msecs, process = *process_name*

説明 このメッセージは、プロセスの CPU 使用が 100 ミリ秒を超えた場合に表示されます。このメッセージはデバッグ用に使用され、CPU 使用プロセスにフラグを付けます。

推奨処置 不要です。

713004

エラー メッセージ %PIX|ASA-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface *interface num*, for Peer *IP_address* ignored

説明 このメッセージは、Cisco ASA が、トンネルを開始しようとしているリモート エンティティから IKE パケットを受信した場合に表示されます。Cisco ASA はリブートまたはシャットダウンがスケジュールされているので、これ以上トンネルを確立できません。この IKE パケットは無視されて、廃棄されます。

説明 不要です。

713006

エラー メッセージ %PIX|ASA-5-713006: Failed to obtain state for message Id *message_number*, Peer Address: *IP_address*

説明 このメッセージは、Cisco ASA が受信したメッセージ ID が未知の ID であることを示します。メッセージ ID は、特定の IKE フェーズ 2 ネゴシエーションの識別に使用されます。これは多くの場合 Cisco ASA でのエラー状態を表していますが、2 つの IKE ピアの同期がとれていないことを示す場合があります。

推奨処置 不要です。

713008

エラー メッセージ %PIX|ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel

説明 このメッセージは、ID ペイロードでキー ID 値を受信したが、その値が事前共有キー認証を使用する IKE セッションのグループ名の最大許容サイズよりも長かったことを示します。これは無効な値で、セッションは拒否されます。指摘されたキー ID は、そのサイズのグループ名を Cisco ASA で作成できないので、機能することはありません。クライアント上の誤ったグループ名を変更するようにユーザに通知します。

推奨処置 クライアントピア（おそらくは Altiga RA Client）が有効なグループ名を指定していることを確認します。グループ名の現在の最大長は 32 です。

713009

エラー メッセージ %PIX|ASA-3-713009: OU in DN in ID payload too big for Certs
IKE tunnel

説明 このメッセージは、ID ペイロードで DN の OU 値を受信したが、その値が証明書認証を使用する IKE セッションのグループ名の最大許容サイズよりも長かったことを示します。この OU はスキップされますが、別の OU または他の基準を使用して一致するグループを検出できません。

推奨処置 クライアントが OU を使用して Cisco ASA からグループを検出するには、グループ名が有効な長さでなければなりません。グループ名の現在の最大長は 32 です。

713010

エラー メッセージ %PIX|ASA-5-713010: IKE area: failed to find centry for message
Id message_number

説明 このメッセージは、固有のメッセージ ID で conn_entry (IPSec SA に対応する IKE フェーズ 2 構造) を特定しようとして失敗した場合に表示されます。内部構造が見つかりませんでした。これは、非標準的な方法でセッションが終了した場合に発生することがありますが、多くの場合内部エラーを示します。

推奨処置 この問題が解決しない場合は、ピアを調査します。

713012

エラー メッセージ %PIX|ASA-3-713012: Unknown protocol (*protocol*). Not adding SA
w/spi=*SPI value*

説明 このメッセージは、不正またはサポートされていない IPSec プロトコルをピアから受信した場合に表示されます。

推奨処置 ピアの ISAKMP フェーズ 2 設定をチェックして、Cisco ASA と互換性があることを確認します。

713014

エラー メッセージ %PIX|ASA-3-713014: Unknown Domain of Interpretation (DOI):
DOI value

説明 このメッセージは、ピアから受信した ISAKMP Domain of Interpretation がサポートされていない場合に表示されます。

推奨処置 ピアの ISAKMP DOI コンフィギュレーションを確認します。

713016

エラーメッセージ %PIX|ASA-3-713016: Unknown identification type, Phase 1 or 2, Type *ID_Type*

説明 このメッセージは、ピアから受信した ID が未知であることを示します。ID が、よく知られていない有効な ID である場合、または無効または破損した ID である場合があります。

推奨処置 ヘッドエンドおよびピアのコンフィギュレーションを確認します。

713017

エラーメッセージ %PIX|ASA-3-713017: Identification type not supported, Phase 1 or 2, Type *ID_Type*

説明 このメッセージは、ピアから受信したフェーズ 1 またはフェーズ 2 の ID が正当であるが、サポートされていないことを示します。

推奨処置 ヘッドエンドおよびピアのコンフィギュレーションを確認します。

713018

エラーメッセージ %PIX|ASA-3-713018: Unknown ID type during find of group name for certs, Type *ID_Type*

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713020

エラーメッセージ %PIX|ASA-3-713020: No Group found by matching OU(s) from ID payload: *OU_value*

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713022

エラーメッセージ %PIX|ASA-3-713022: No Group found matching *peer_ID* or *IP_address* for Pre-shared key peer *IP_address*

説明 このメッセージは、グループ データベースにはピアで指摘された値 (キー ID または IP アドレス) と同じ名前のグループがなかったことを示します。

推奨処置 ピアのコンフィギュレーションを確認します。

713024

エラー メッセージ %PIX|ASA-7-713024: Received local Proxy Host data in ID
Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がリモート ピアのフェーズ2のローカル プロキシ ID ペイロードを受信したことを示します。

推奨処置 不要です。

713025

エラー メッセージ %PIX|ASA-7-713025: Received remote Proxy Host data in ID
Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がリモート ピアのフェーズ2のリモート プロキシ ID ペイロードを受信したことを示します。

推奨処置 不要です。

713026

エラー メッセージ %PIX|ASA-7-713026: Transmitted local Proxy Host data in ID
Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がフェーズ2のローカル プロキシ ID ペイロードを転送したことを示します。

推奨処置 不要です。

713027

エラー メッセージ %PIX|ASA-7-713027: Transmitted remote Proxy Host data in ID
Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がフェーズ2のリモート プロキシ ID ペイロードを転送したことを示します。

推奨処置 不要です。

713028

エラー メッセージ %PIX|ASA-7-713028: Received local Proxy Range data in ID
Payload: Addresses *IP_address-IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がリモート ピアのフェーズ2のローカル プロキシ ID ペイロードを受信して、その中に IP アドレス範囲が含まれていることを示します。

推奨処置 不要です。

713029

エラーメッセージ %PIX|ASA-7-713029: Received remote Proxy Range data in ID
Payload: Addresses *IP_address - IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がリモート ピアのフェーズ2のリモート プロキシ ID ペイロードを受信して、その中に IP アドレス範囲が含まれていることを示します。

推奨処置 不要です。

713030

エラーメッセージ %PIX|ASA-7-713030: Transmitted local Proxy Range data in ID
Payload: Addresses *IP_address - IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がフェーズ2のローカル プロキシ ID ペイロードを転送したことを示します。

推奨処置 不要です。

713031

エラーメッセージ %PIX|ASA-7-713031: Transmitted remote Proxy Range data in ID
Payload: Addresses *IP_address - IP_address*, Protocol *protocol*, Port *port*

説明 このメッセージは、Cisco ASA がフェーズ2のリモート プロキシ ID ペイロードを転送したことを示します。

推奨処置 不要です。

713032

エラーメッセージ %PIX|ASA-3-713032: Received invalid local Proxy Range *IP_address*
- *IP_address*

説明 このメッセージは、ローカル ID ペイロードに範囲 ID タイプが含まれ、指摘された低アドレスが高アドレス以上であった場合に表示されます。これはコンフィギュレーションの問題を示している可能性があります。

推奨処置 ISAKMP フェーズ2のパラメータのコンフィギュレーションを確認します。

713033

エラーメッセージ %PIX|ASA-3-713033: Received invalid remote Proxy Range
IP_address - IP_address

説明 このメッセージは、リモート ID ペイロードに範囲 ID タイプが含まれ、指摘された低アドレスが高アドレス以上であった場合に表示されます。これはコンフィギュレーションの問題を示している可能性があります。

推奨処置 ISAKMP フェーズ2のパラメータのコンフィギュレーションを確認します。

713034

エラーメッセージ %PIX|ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 このメッセージは、ローカル IP プロキシ サブネット データがフェーズ 2 の ID ペイロードで受信された場合に表示されます。

推奨処置 不要です。

713035

エラーメッセージ %PIX|ASA-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 このメッセージは、リモート IP プロキシ サブネット データがフェーズ 2 の ID ペイロードで受信された場合に表示されます。

推奨処置 不要です。

713036

エラーメッセージ %PIX|ASA-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 このメッセージは、ローカル IP プロキシ サブネット データがフェーズ 2 の ID ペイロードで転送された場合に表示されます。

推奨処置 不要です。

713037

エラーメッセージ %PIX|ASA-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 このメッセージは、リモート IP プロキシ サブネット データがフェーズ 2 の ID ペイロードで転送された場合に表示されます。

推奨処置 不要です。

713039

エラーメッセージ %PIX|ASA-7-713039: Send failure: Bytes (*number*), Peer: *IP_address*

説明 このメッセージは、内部ソフトウェア エラーが発生し、ISAKMP パケットを転送できなかった場合に表示されます。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713040

エラー メッセージ %PIX|ASA-7-713040: Could not find connection entry and can not encrypt: msgid *message_number*

説明 このメッセージは、内部ソフトウェア エラーが発生し、フェーズ 2 データ構造を検出できなかったことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713041

エラー メッセージ %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*)

説明 このメッセージは、Cisco ASA がイニシエータとしてトンネルをネゴシエーション中であることを示します。

推奨処置 不要です。

713042

エラー メッセージ %PIX|ASA-3-713042: IKE Initiator unable to find policy: Intf *interface_number*, Src: *source_address*, Dst: *dest_address*

説明 このメッセージは、IPSec ファースト パスで、IKE を起動したパケットを処理したが、IKE のポリシー ルックアップが失敗したことを示します。このエラーは、タイミングに関連している場合があります。IKE が開始要求を処理する前に、IKE を起動した ACL が削除されていた可能性があります。この問題は、多くの場合自分自身で訂正されます。

推奨処置 同じ状態が続く場合、暗号マップに関連付けられている ACL に特に注意しながら、L2L コンフィギュレーションを確認します。

713043

エラー メッセージ %PIX|ASA-3-713043: Cookie/peer address *IP_address* session already in progress

説明 このメッセージは、元のトンネルが進行中に、IKE が再度起動されたことを示します。

推奨処置 不要です。

713047

エラー メッセージ %PIX|ASA-3-713047: Unsupported Oakley group: Group
Diffie-Hellman group

説明 このメッセージは、Cisco ASA が、リモート ピアから提示された Diffie-Hellman グループをサポートしていないことを示します。Diffie-Hellman グループは、フェーズ 1 中に使用されると Diffie-hellman キーを生成し、フェーズ 2 中では完全転送秘密 (PFS) 用の Diffie-Hellman キーを生成します。

説明 ピアの Diffie-Hellman キーのコンフィギュレーションを確認します。また、Cisco ASA に正しいプロポーザルがあるかどうかを確認します。

713048

エラー メッセージ %PIX|ASA-3-713048: Error processing payload: Payload ID: *id*

説明 このメッセージは、処理できなかったペイロードでパケットが受信されたことを示します。

推奨処置 この問題が解決しない場合は、ピアのコンフィギュレーションに誤りがある可能性があります。

713049

エラー メッセージ %PIX|ASA-5-713049: Security negotiation complete for *tunnel_type*
type (*group_name*) *Initiator/Responder*, Inbound SPI = *SPI*, Outbound SPI = *SPI*

説明 このメッセージは、IPSec トンネルの開始を示します。

推奨処置 不要です。

713050

エラー メッセージ %PIX|ASA-5-713050: Connection terminated for peer *IP_address*.
Reason: *termination reason* Remote Proxy *IP_address*, Local Proxy *IP_address*

説明 このメッセージは、IPSec トンネルの終了を示します。

推奨処置 不要です。

713051

エラー メッセージ %PIX|ASA-3-713051: Terminating connection attempt: IPSEC not
permitted for group (*group_name*)

説明 このメッセージは、ユーザ、グループ、またはインターフェイス ポリシーが IPSec トンネルを拒否していることを示します。

推奨処置 IPSec を使用するには、該当するトンネリング プロトコルをポリシーから選択します。

713052

エラー メッセージ %PIX|ASA-7-713052: User (*user*) authenticated.

説明 このメッセージは、リモート アクセス ユーザが認証されたことを示します。

推奨処置 不要です。

713056

エラー メッセージ %PIX|ASA-3-713056: Tunnel rejected: SA (*SA_name*) not found for group (*group_name*)!

説明 このメッセージは、IPSec SA が見つからなかったことを示します。

推奨処置 これがリモート アクセス トンネルの場合、グループとユーザ コンフィギュレーションをチェックして、ユーザのグループに対してトンネルグループとグループ ポリシーが設定されていることを確認します。外部で認証されたユーザおよびグループの場合は、返された認証アトリビュートを確認します。

713059

エラー メッセージ %PIX|ASA-3-713059: Tunnel Rejected: User (*user*) matched with group name, group-lock check failed.

説明 このメッセージは、トンネルグループおよびユーザ名の両方に同じ文字列を使用して、ユーザが認証を実行しようとしたことを示します。

推奨処置 認証されるユーザのグループとユーザ名は異なっている必要があります。

713060

エラー メッセージ %PIX|ASA-3-713060: Tunnel Rejected: User (*user*) not member of group (*group_name*), group-lock check failed.

説明 このメッセージは、ユーザが、IPSec ネゴシエーションで送信されたグループとは別のグループに設定されていることを示します。

推奨処置 Cisco VPN クライアントと事前共有キーを使用している場合、クライアントに設定されているグループが、Cisco ASA 上のユーザに関連付けられているグループと同じであることを確認します。デジタル証明書を使用している場合、グループは、証明書の OU フィールドで指定されているか、またはユーザはリモート アクセスのデフォルト グループにデフォルトで設定されています。

713061

エラー メッセージ %PIX|ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address, Dst: dest_address!

説明 このメッセージは、Cisco ASA が、メッセージに示されているプライベート ネットワークまたはホストのセキュリティ ポリシー情報を検出できなかったことを示します。これらのネットワークまたはホストは、イニシエータによって送信され、Cisco ASA のどの暗号 ACL とも一致しません。これは多くの場合、コンフィギュレーションの誤りです。

推奨処置 両側の暗号 ACL 内の保護されたネットワーク コンフィギュレーションをチェックして、イニシエータのローカル ネットが応答側のリモート ネットであること（およびその逆）を確認します。ワイルドカード マスク、ホスト アドレス対ネットワーク アドレスなどに特に注意します。シスコ以外の実装では、プライベート アドレスがプロキシ アドレスまたは赤い色のネットワークとしてラベル付けされている場合があります。

713062

エラー メッセージ %PIX|ASA-3-713062: IKE Peer address same as our interface address IP_address

説明 IKE ピアとして設定する IP アドレスは、Cisco ASA IP インターフェイスのいずれかで設定する IP アドレスと同じである必要があります。

推奨処置 L2L コンフィギュレーションと IP インターフェイスのコンフィギュレーションを確認します。

713063

エラー メッセージ %PIX|ASA-3-713063: IKE Peer address not configured for destination IP_address

説明 IKE ピア アドレスが L2L トンネルに対して設定されていない場合に表示されます。

推奨処置 L2L コンフィギュレーションを確認します。

713065

エラー メッセージ %PIX|ASA-3-713065: IKE Remote Peer did not negotiate the following: proposal_attribute

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713066

エラー メッセージ %PIX|ASA-7-713066: IKE Remote Peer configured for SA: *SA_name*

説明 このメッセージは、ピアの暗号ポリシー設定を示します。

推奨処置 不要です。

713068

エラー メッセージ %PIX|ASA-5-713068: Received non-routine Notify message:
notify_type (*notify_value*)

説明 このメッセージは、このイベントが通知処理コードで明示的に処理されない原因となる通知メッセージを示します。

推奨処置 実行するアクションを判別するには、特定の理由情報を調べます。通知メッセージの多くは、IKE ピア間のコンフィギュレーションの不一致を示します。

713072

エラー メッセージ %PIX|ASA-3-713072: Password for user (*user*) too long,
truncating to *number* characters

説明 このメッセージは、ユーザのパスワードが長すぎることを示しています。

推奨処置 認証サーバでパスワードの長さを訂正します。

713073

エラー メッセージ %PIX|ASA-5-713073: Responder forcing change of *Phase 1/Phase 2*
rekeying duration from *larger_value* to *smaller_value* seconds

説明 キー再生成の時間は、IKE ピアが指定する値よりも低い値に設定されます。このメッセージは、発信者の値のほうが低いことを示します。

推奨処置 不要です。

713074

エラー メッセージ %PIX|ASA-5-713074: Responder forcing change of IPSec rekeying
duration from *larger_value* to *smaller_value* Kbs

説明 キー再生成の時間は、IKE ピアが指定する値よりも低い値に設定されます。このメッセージは、発信者の値のほうが低いことを示します。

推奨処置 不要です。

713075

エラー メッセージ %PIX|ASA-5-713075: Overriding Initiator's IPSec rekeying duration from *larger_value* to *smaller_value* seconds

説明 キー再生成の時間は、IKE ピアが指定する値よりも低い値に設定されます。このメッセージは、応答者の値のほうが低いことを示します。

推奨処置 不要です。

713076

エラー メッセージ %PIX|ASA-5-713076: Overriding Initiator's IPSec rekeying duration from *larger_value* to *smaller_value* Kbs

説明 キー再生成の時間は、IKE ピアが指定する値よりも低い値に設定されます。このメッセージは、応答者の値のほうが低いことを示します。

推奨処置 不要です。

713078

エラー メッセージ %PIX|ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize *available_size*, used *value*

説明 このメッセージは、modecfg アトリビュートの処理中に内部ソフトウェア エラーが発生したことを示します。

推奨処置 不必要なトンネル グループ アトリビュートをディセーブルにするか、長すぎるテキストメッセージを短くします。問題が解決しない場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713081

エラー メッセージ %PIX|ASA-3-713081: Unsupported certificate encoding type *encoding_type*

説明 このメッセージは、ロードされた証明書のいずれかが読み取り不可であることと、サポートされない符号化スキームである可能性を示しています。

推奨処置 デジタル証明書およびトラストポイントのコンフィギュレーションを確認します。

713082

エラー メッセージ %PIX|ASA-3-713082: Failed to retrieve identity certificate

説明 このトンネルの ID 証明書が見つかりませんでした。

推奨処置 デジタル証明書およびトラストポイントのコンフィギュレーションを確認します。

713083

エラーメッセージ %PIX|ASA-3-713083: Invalid certificate handle

説明 このメッセージは、このトンネルの ID 証明書が見つからなかったことを示しています。

推奨処置 デジタル証明書およびトラストポイントのコンフィギュレーションを確認します。

713084

エラーメッセージ %PIX|ASA-3-713084: Received invalid phase 1 port value (*port*)
in ID payload

説明 このメッセージは、IKE フェーズ 1 ID ペイロードで受信されたポート値が正しくなかったことを示しています。受け入れ可能な値は 0 または 500 (ISAKMP aka IKE) です。

推奨処置 これは、ピアが IKE 規格に従っていないか、またはネットワークの問題によってパケットが破損したことを示している可能性があります。

713085

エラーメッセージ %PIX|ASA-3-713085: Received invalid phase 1 protocol (*protocol*)
in ID payload

説明 このメッセージは、IKE フェーズ 1 ID ペイロードで受信されたプロトコル値が正しくなかったことを示しています。受け入れ可能な値は 0 または 17 (UDP) です。

推奨処置 これは、ピアが IKE 規格に従っていないか、またはネットワークの問題によってパケットが破損したことを示している可能性があります。

713086

エラーメッセージ %PIX|ASA-3-713086: Received unexpected Certificate payload
Possible invalid Auth Method (*Auth method (auth numerical value)*)

説明 このメッセージは、証明書ペイロードが受信されたが、ID 証明書がないことが内部証明書ハンドルによって示されている場合に表示されます。これは、場合によっては、証明書ハンドルが通常の登録方法で獲得されなかったことを意味します。これが発生する理由として考えられるのは、認証方式が RSA または DSS シグニチャではないことです。ただし、それぞれの側の設定が誤っていると、IKE SA ネゴシエーションは失敗します。

推奨処置 アプライアンスとピアでトラストポイントと ISAKMP コンフィギュレーション設定を確認します。

713088

エラー メッセージ %PIX|ASA-3-713088: Set Cert filehandle failure: no IPsec SA in group *group_name*

説明 このメッセージは、デジタル証明書情報に基づいてトンネル グループを検出できなかったことを示しています。

推奨処置 ピアの証明書情報を処理するようトンネル グループが適切に設定されていることを確認します。

713092

エラー メッセージ %PIX|ASA-5-713092: Failure during phase 1 rekeying attempt due to collision

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 多くの場合、これは問題のないイベントですが、深刻な影響がある場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713094

エラー メッセージ %PIX|ASA-7-713094: Cert validation failure: handle invalid for *Main/Aggressive Mode Initiator/Responder!*

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 場合によっては、トラストポイントを再登録する必要があります。問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713098

エラー メッセージ %PIX|ASA-3-713098: Aborting: No identity cert specified in IPsec SA (*SA_name*)!

説明 このメッセージは、証明書ベースの IKE セッションを確立しようとしたときに、暗号ポリシーで ID 証明書が指定されていない場合に表示されます。

推奨処置 ピアに送信する ID 証明書 / トラストポイントを指定します。

713099

エラーメッセージ %PIX|ASA-7-713099: Tunnel Rejected: Received NONCE length *number* is out of range!

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713102

エラーメッセージ %PIX|ASA-3-713102: Phase 1 ID Data length *number* too long - reject tunnel!

説明 このメッセージは、サイズが 2K 以上の Identification Data フィールドを含む ID ペイロードを IKE が受信したことを示しています。

推奨処置 不要です。

713103

エラーメッセージ %PIX|ASA-7-713103: Invalid (NULL) secret key detected while computing hash

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713104

エラーメッセージ %PIX|ASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713105

エラー メッセージ %PIX|ASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing

説明 このメッセージは、無効な ID データを組み込まずに ID ペイロードを送信したことを示しています。

推奨処置 ピアのコンフィギュレーションを確認します。

713107

エラー メッセージ %PIX|ASA-3-713107: IP_Address request attempt failed!

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713109

エラー メッセージ %PIX|ASA-3-713109: Unable to process the received peer certificate

説明 このメッセージは、リモート ピアから受信した証明書を Cisco ASA が処理できなかったことを示しています。これは、証明書データの形式が誤っている場合や、証明書内のデータをアプライアンスで保存できない場合に発生します。たとえば、公開キーのサイズが 4096 ビットより大きい場合などです。

推奨処置 リモート ピアで別の証明書を使用して接続の再確立を試行します。

713112

エラー メッセージ %PIX|ASA-3-713112: Failed to process CONNECTED notify (SPI SPI_value)!

説明 このメッセージは、Cisco ASA が、通知タイプ CONNECTED を含む通知ペイロードを正常に処理できなかったことを示しています。これは、IKE フェーズ 2 構造が、それを見つけるための SPI を使用して検出できなかった場合、または受信した ISAKMP ヘッダーでコミット ビットが設定されていなかった場合に発生します。後者の事例では、IKE ピアが規格に従っていない可能性があることを示しています。

推奨処置 問題が解決しない場合、ピアのコンフィギュレーションを調べるか、コミット ビット処理をディセーブルにします。

713113

エラー メッセージ %PIX|ASA-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: *IP_address*, SA address: *internal_SA_address*, tunnel count: *count*

説明 このメッセージは、IKE SA が 0 以外のトンネル カウントで削除されていることを示しています。これは、IKE SA トンネル カウントに関連する接続エントリとの同期が失われたか、あるいは関連する接続エントリのクッキー フィールドで接続エントリが指す IKE SA のクッキー フィールドとの同期が失われたことを意味します。これが発生する場合、IKE SA およびそれに関連するデータ構造体は解放されないため、それを指すエントリは古いポインタを持つことがあります。

推奨処置 不要です。エラー リカバリは組み込まれています。

713114

エラー メッセージ %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

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713115

エラー メッセージ %PIX|ASA-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec

説明 このメッセージは、Cisco ASA が IPSec over UDP を使おうとする試みがクライアントによって拒否されたことを示しています。IPSec over UDP を使用すると、NAT デバイスを介して複数のクライアントが Cisco ASA への同時トンネルを確立できません。クライアントが、この機能をサポートしていないか、またはこの機能を使用するよう設定されていないため、要求を拒否した可能性があります。

推奨処置 ヘッドエンドとピアのコンフィギュレーションを確認します。

713116

エラー メッセージ %PIX|ASA-3-713116: Terminating connection attempt: L2TP-over-IPSEC attempted by group (*group_name*) but L2TP disabled

説明 このメッセージは、ユーザまたはグループ エントリが L2TP-over-IPSec 接続を試みたが、この Cisco ASA に対して L2TP プロトコルがイネーブルになっていないことを示しています。

推奨処置 L2TP コンフィギュレーションを確認します。

713117

エラー メッセージ %PIX|ASA-7-713117: Received Invalid SPI notify (SPI *SPI_Value*)!

説明 このメッセージは、SPI 値によって識別された IPsec SA が、リモート ピアでアクティブではなくなったことを示しています。リモート ピアがリブートされたか、リセットされた可能性があります。

推奨処置 この問題は、ピアによって適切な SA が確立されていないことを DPD が認識すると、訂正されます。DPD がイネーブルになっていない場合は、影響を受けるトンネルを手動で再確立しなければならないことがあります。

713118

エラー メッセージ %PIX|ASA-3-713118: Detected invalid Diffie-Hellman *group_descriptor group_number*, in IKE area

説明 このメッセージは、*group_descriptor* フィールドにサポートされない値が含まれていることを示しています。現在サポートされているのは、グループ 1、2、5、および 7 だけです。centry の場合は、*group_descriptor* フィールドが、完全転送秘密 (PFS) がディセーブルになっていることを示すため 0 に設定されていることもあります。

推奨処置 ピア Diffie-Hellman コンフィギュレーションを確認します。

713119

エラー メッセージ %PIX|ASA-3-713119: PHASE 1 COMPLETED

説明 IKE フェーズ 1 が正常終了した場合に、このメッセージが表示されます。

推奨処置 不要です。

713120

エラー メッセージ %PIX|ASA-5-713120: PHASE 2 COMPLETED (*msgid=msg_id*)

説明 IKE フェーズ 2 が正常終了した場合に、このメッセージが表示されます。

推奨処置 不要です。

713121

エラー メッセージ %PIX|ASA-7-713121: Keep-alive type for this connection: *keepalive_type*

説明 このメッセージは、このトンネルに対して使用されているキープアライブ メカニズムのタイプを示します。

推奨処置 不要です。

713122

エラーメッセージ %PIX|ASA-3-713122: Keep-alives configured *keepalive_type* but peer *IP_address* support keep-alives (type = *keepalive_type*)

説明 このメッセージは、キープアライブがこのデバイスに対してオンまたはオフに設定されているが、IKE ピアがキープアライブをサポートしている、またはしていないことを示します。

推奨処置 これが意図的である場合、処置は不要です。意図的でない場合は、両方のデバイスでキープアライブ コンフィギュレーションを変更します。

713123

エラーメッセージ %PIX|ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: *keepalive_type*)

説明 このメッセージは、リモート IKE ピアが予期された時間ウィンドウ内でキープアライブに回答しなかったため、IKE ピアへの接続が終了したことを示しています。このメッセージには、使用されるキープアライブ メカニズムが含まれています。

推奨処置 不要です。

713124

エラーメッセージ %PIX|ASA-3-713124: Received DPD sequence number *rcv_sequence_#* in *DPD Action, description expected seq #*

説明 このメッセージは、リモート IKE ピアが、予期されたシーケンス番号と異なるシーケンス番号とともに DPD を送信したことを示しています。パケットは廃棄されます。

推奨処置 これは、ネットワークでのパケット損失の問題を示している場合があります。

713127

エラーメッセージ %PIX|ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list

説明 このメッセージは、ピアが XAUTH を実行しようとしているが、Cisco ASA が XAUTH IKE プロポーザルを選択しなかった場合に表示されます。

推奨処置 IKE プロポーザル リストで IKE xauth プロポーザルの優先順位を確認します。

713128

エラーメッセージ %PIX|ASA-3-713128: Connection attempt to VCPIP redirected to VCA peer *IP_address* via load balancing

説明 このメッセージは、VCPIP に接続しようとして、ロードバランシングでロードのより少ないピアにリダイレクトされたときに表示されます。

推奨処置 不要です。

713129

エラー メッセージ %PIX|ASA-3-713129: Received unexpected Transaction Exchange
payload type: *payload_id*

説明 このメッセージは、XAUTH または Mode-cfg 中に予期しないペイロードが受信されたことを示しています。これは、2つのピアが同期していないこと、XAUTH または Mode-cfg のバージョンが一致しないこと、リモートピアが適切な RFC に準拠していないことを示している場合があります。

推奨処置 ピア間のコンフィギュレーションを確認します。

713130

エラー メッセージ %PIX|ASA-5-713130: Received unsupported transaction mode
attribute: *attribute_id*

説明 このメッセージは、現在サポートされていない有効なトランザクション モード アトリビュート (XAUTH または Mode Cfg) に対する要求をデバイスが受信したことを示しています。通常、これは問題のない状態です。

推奨処置 不要です。

713131

エラー メッセージ %PIX|ASA-5-713131: Received unknown transaction mode
attribute: *attribute_id*

説明 このメッセージは、既知のアトリビュートの範囲外であるトランザクション モード アトリビュート (XAUTH または Mode Cfg) に対する要求を Cisco ASA が受信したことを示しています。アトリビュートは有効でも新しいバージョンのコンフィギュレーション モードでのみサポートされているか、ピアが不正な値または独占権のある値を送信している可能性があります。これは、接続の問題にはなりませんが、ピアの機能に影響する場合があります。

推奨処置 不要です。

713132

エラー メッセージ %PIX|ASA-3-713132: Cannot obtain an *IP_address* for remote peer

説明 このメッセージは、これらのアドレスを提供する内部ユーティリティからのリモート アクセス クライアントの IP アドレスに対する要求が満たされなかったことを示しています。

推奨処置 IP アドレス割り当て方法のコンフィギュレーションを確認します。

713133

エラー メッセージ %PIX|ASA-3-713133: Mismatch: Overriding phase 2 DH Group (DH group *DH group_id*) with phase 1 group (DH group *DH group_number*)

説明 設定されたフェーズ 2 PFS グループが、フェーズ 1 に対してネゴシエートされた DH グループと異なります。

推奨処置 不要です。

713134

エラー メッセージ %PIX|ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection

説明 このメッセージは、設定された LAN-to-LAN プロポーザルが、LAN-to-LAN 接続に対して受け入れられたプロポーザルと異なる場合に表示されます。どちらの側が発信者かに応じて、異なるプロポーザルが使用されます。

推奨処置 不要です。

713135

エラー メッセージ %PIX|ASA-5-713135: message received, redirecting tunnel to *IP_address*.

説明 このメッセージは、リモート Cisco ASA でのロードバランシングのためにトンネルがリダイレクトされていることを示しています。このメッセージは、REDIRECT_CONNECTION 通知パケットが受信された場合に表示されます。

推奨処置 不要です。

713136

エラー メッセージ %PIX|ASA-5-713136: IKE session establishment timed out [*IKE_state_name*], aborting!

説明 これは、リーパーによって SA スタックが非アクティブな状態で検出された場合に発生します。リーパーは、ハングした SA を除去しようとします。

推奨処置 不要です。

713137

エラー メッセージ %PIX|ASA-5-713137: Reaper overriding refCnt [*ref_count*] and tunnelCnt [*tunnel_count*] -- deleting SA!

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713138

エラー メッセージ %PIX|ASA-3-713138: Group *group_name* not found and BASE GROUP default preshared key not configured

説明 このメッセージは、グループ データベース内にピアの IP アドレスと同じ名前を持つグループがない場合に表示されます。Main モードで、Cisco ASA がフォールバックし、デフォルト グループのいずれかで設定されたデフォルトの事前共有キーの使用を試みます。デフォルトの事前共有キーは設定されていません。

推奨処置 事前共有キーのコンフィギュレーションを確認します。

713139

エラー メッセージ %PIX|ASA-5-713139: *group_name* not found, using BASE GROUP default preshared key

説明 グループ データベース内にピアの IP アドレスと同じ名前を持つトンネル グループがありませんでした。Main モードで、Cisco ASA がフォールバックし、デフォルト グループで設定されたデフォルトの事前共有キーを使用します。

推奨処置 不要です。

713140

エラー メッセージ %PIX|ASA-3-713140: Split Tunneling Policy requires network list but none configured

説明 このメッセージは、スプリット トンネリング ポリシーがトンネルのスプリットまたはローカル LAN アクセスの許可に設定されている場合に表示されます。VPN クライアントが要求する情報を表すには、スプリット トンネリング ACL が定義されている必要があります。

推奨処置 ACL のコンフィギュレーションを確認します。

713141

エラー メッセージ %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*

説明 このメッセージは、クライアントにインストールされた Cisco ASA が設定された必須の Cisco ASA と一致しないことを示しています。このメッセージは、実際の値と予期された値をリストし、トンネルが終了したか、または許可されたかを示します。

推奨処置 クライアントに別の個人用の Cisco ASA をインストールするか、または Cisco ASA にコンフィギュレーションの変更を行わなければならないことがあります。

713142

エラー メッセージ %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*

説明 このメッセージは、クライアントが ModeCfg を使用して使用中の Cisco ASA を報告しなかったが、それが必要である場合に表示されます。このイベントは、予期された値をリストし、トンネルが終了したか、または許可されたかを示します。製品ストリングの後の数値は、許可されたすべての製品のビットマスクです。

推奨処置 クライアントに別の個人用の Cisco ASA をインストールするか、または Cisco ASA にコンフィギュレーションの変更を行わなければならないことがあります。

713143

エラー メッセージ %PIX|ASA-7-713143: Processing firewall record. Vendor: *vendor(id)*, Product: *product(id)*, Caps: *capability_value*, Version Number: *version_number*, Version String: *version_text*

説明 このメッセージは、クライアントにインストールされた Cisco ASA に関する不具合情報を提供します。

推奨処置 不要です。

713144

エラー メッセージ %PIX|ASA-5-713144: Ignoring received malformed firewall record; reason - *error_reason* TLV type *attribute_value* *correction*

説明 このメッセージは、不良な Cisco ASA 情報がクライアントから受信されたことを示します。

推奨処置 クライアントおよび Cisco ASA で個人用の Cisco ASA コンフィギュレーションを確認します。

713145

エラー メッセージ %PIX|ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: *IP_address*, mask: *netmask*

説明 このメッセージは、ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートが追加されていることを示しています。これによって、Cisco ASA は、ヘッドエンドのプライベート側にあるすべてのルータにリモート ネットワークを知らせることができます。

推奨処置 不要です。

713146

エラー メッセージ %PIX|ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: *IP_address*, mask: *netmask*

説明 このメッセージは、内部ソフトウェア エラーが発生したことを示します。ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートを追加する試みが失敗しました。これは、ルーティング テーブルがいっぱいになっているか、アドレッシング エラーが発生した可能性を示します。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713147

エラー メッセージ %PIX|ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: *IP_address*, mask: *netmask*

説明 このメッセージは、ネットワーク拡張モードのハードウェア クライアントへのトンネルが除去され、ハードウェア クライアントの背後でプライベート ネットワーク用のスタティック ルートが削除されていることを示しています。

推奨処置 不要です。

713148

エラー メッセージ %PIX|ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: *IP_address*, mask: *netmask*

説明 このメッセージは、ネットワーク拡張モードのハードウェア クライアントへのトンネルを除去しているときに、ハードウェア クライアントの背後にあるプライベート ネットワークへのルートを削除できなかったことを示しています。

推奨処置 これは、アドレッシングまたはソフトウェアの問題を意味する場合があります。ルーティング テーブルを調べて、ルートがそこにあることを確認します。ルートがある場合は、手動で削除する必要がありますが、ハードウェア クライアントへのトンネルが完全に削除された場合に限り行います。

713149

エラー メッセージ %PIX|ASA-3-713149: Hardware client security attribute *attribute_name* was enabled but not requested.

説明 このメッセージは、ヘッドエンド Cisco ASA で指摘されたハードウェア クライアント セキュリティ アトリビュートがイネーブルになっているが、VPN3002 ハードウェア クライアントによってアトリビュートが要求されなかったことを示しています。

推奨処置 ハードウェア クライアントでコンフィギュレーションを確認します。

713152

エラー メッセージ %PIX|ASA-3-713152: Unable to obtain any rules from filter *ACL_tag* to send to client for CPP, terminating connection.

説明 このメッセージは、クライアントで CPP を使用してその Cisco ASA をプロビジョニングする必要があるが、ヘッドエンド デバイスがクライアントへ送信する ACL を取得できなかったことを示しています。原因として、設定の誤りが考えられます。

推奨処置 クライアントのグループ ポリシーで CPP に対して指定された ACL を確認します。

713154

エラー メッセージ %PIX|ASA-4-713154: DNS lookup for *peer_description* Server [*server_name*] failed!

説明 このメッセージは、指摘されたサーバに対する DNS ルックアップが解決されなかった場合に表示されます。

推奨処置 Cisco ASA 上の DNS サーバ コンフィギュレーションを確認します。また、DNS サーバがオプションになっていることと、IP アドレス マッピングへのホスト名を持っていることを確認します。

713155

エラー メッセージ %PIX|ASA-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure. Resetting any Backup Server init.

説明 プライマリ サーバに対する以前の DNS ルックアップの失敗によって、システムがバックアップピアを初期化した可能性があります。このメッセージは、プライマリ サーバでの後の DNS ルックアップが最終的に成功し、バックアップサーバの初期化をリセットしていることを示しています。このポイントより後に初期化されたトンネルは、プライマリ サーバに向けられます。

推奨処置 不要です。

713156

エラー メッセージ %PIX|ASA-5-713156: Initializing Backup Server [server_name or IP_address]

説明 このメッセージは、クライアントがバックアップサーバにフェールオーバーしているか、プライマリサーバに対する DNS ルックアップが失敗したことによりシステムがバックアップサーバを初期化したことを示しています。このポイントより後に初期化されたトンネルは、指摘されたバックアップサーバに向けられます。

推奨処置 不要です。

713157

エラー メッセージ %PIX|ASA-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.

説明 このメッセージは、クライアントが IKE MSG1 を送信してトンネルを初期化しようとしたが、相手側の Cisco ASA から応答を受信しなかったことを示しています。バックアップサーバを使用できる場合、クライアントはそれらのいずれかに接続しようとしています。

推奨処置 ヘッドエンド Cisco ASA への接続を確認します。

713158

エラー メッセージ %PIX|ASA-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP

説明 このメッセージは、クライアントが IPSec over TCP を使用するよう設定されていることを示しています。Cisco ASA が IPSec over UDP を使おうとする試みがクライアントによって拒否されました。

推奨処置 TCP を希望する場合、処置は不要です。それ以外の場合は、クライアントコンフィギュレーションを確認します。

713159

エラーメッセージ %PIX|ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access

説明 このメッセージは、Cisco ASA サーバへの TCP 接続が何らかの理由で失われたことを示しています。理由としては、サーバのリブート、ネットワークの問題、SSL の不一致などが考えられます。

推奨処置 初期接続が確立された後にサーバの接続が失われた場合は、サーバとネットワークの接続を確認する必要があります。初期接続がすぐに失われた場合、これは SSL 認証の問題を意味する場合があります。

713160

エラーメッセージ %PIX|ASA-7-713160: Remote user (session Id - *id*) has been granted access by the Firewall Server

説明 このメッセージは、Cisco ASA サーバへのリモートユーザの通常の認証を示しています。

推奨処置 不要です。

713161

エラーメッセージ %PIX|ASA-3-713161: Remote user (session Id - *id*) network access has been restricted by the Firewall Server

説明 Cisco ASA サーバは、ユーザを制限する必要があることを示すメッセージを Cisco ASA に送信しました。これには、Cisco ASA ソフトウェアのアップグレードや許可の変更など、いくつかの理由があります。Cisco ASA サーバは、処理が完了するとすぐに、ユーザを完全アクセスモードに移行します。

推奨処置 ユーザが完全アクセスモードに移行されない限り、処置は不要です。これが実行されない場合、実行中の処理の詳細およびリモートマシンで実行中の Cisco ASA ソフトウェアの状態については、Cisco ASA サーバを参照します。

713162

エラーメッセージ %PIX|ASA-3-713162: Remote user (session Id - *id*) has been rejected by the Firewall Server

説明 このメッセージは、Cisco ASA サーバがこのユーザを拒否したことを示しています。

推奨処置 Cisco ASA サーバにおけるポリシー情報で、ユーザが正しく設定されていることを確認します。

713163

エラー メッセージ %PIX|ASA-3-713163: Remote user (session Id - *id*) has been terminated by the Firewall Server

説明 このメッセージは、Cisco ASA サーバがこのユーザ セッションを終了したことを示しています。これは、整合性エージェントがクライアント マシンで動作を停止した場合や、セキュリティ ポリシーがリモート ユーザによって何らかの方法で変更された場合に発生します。

推奨処置 Cisco ASA ソフトウェアがクライアント マシンで動作を続けていることと、ポリシーが正しいことを確認します。

713164

エラー メッセージ %PIX|ASA-7-713164: The Firewall Server has requested a list of active user sessions

説明 このメッセージは、Cisco ASA サーバが、古いデータがあることを検出した場合やセッション データを失った場合（リポート時のように）に、セッション情報を要求することを示しています。

推奨処置 不要です。

713165

エラー メッセージ %PIX|ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode

説明 このメッセージは、デジタル証明書を使うよう設定されているポリシーをトンネルグループが指しているときに、クライアントが事前共有キーとネゴシエートしたことを示しています。

推奨処置 クライアント コンフィギュレーションを確認します。

713166

エラー メッセージ %PIX|ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password

説明 このメッセージは、ハードウェア クライアントが拡張認証に失敗したことを示しています。これはおそらく、ユーザ名とパスワードの問題または認証サーバの問題です。

推奨処置 設定したユーザ名とパスワードの値が各側で一致することを確認します。また、ヘッドエンドの認証サーバが動作していることを確認します。

713167

エラーメッセージ %PIX|ASA-3-713167: Remote peer has failed user authentication - check configured username and password

説明 このメッセージは、リモートユーザが認証の拡張に失敗したことを示しています。これはおそらく、ユーザ名とパスワードの問題または認証サーバの問題です。

推奨処置 設定したユーザ名とパスワードの値が各側で一致することを確認します。また、リモートの認証に使用している認証サーバが動作していることも確認します。

713168

エラーメッセージ %PIX|ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!

説明 このメッセージは、キー再生成の再認証がイネーブルになっているが、トンネル認証で手動による介入が必要であることを示しています。

推奨処置 手動による介入を希望する場合、処置は不要です。それ以外の場合は、対話型の認証コンフィギュレーションを確認します。

713169

エラーメッセージ %PIX|ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: *IP_address*, SA address: *internal_SA_address*, tunnelCnt: *tunnel_count*

説明 このメッセージは、キー再生成が完了した後に古いIKE SAを削除するために、IKEがリモートピアから削除メッセージを受信したことを示しています。

推奨処置 不要です。

713170

エラーメッセージ %PIX|ASA-7-713170: IKE Received delete for rekeyed centry IKE peer: *IP_address*, centry address: *internal_address*, msgid: *id*

説明 IKEは、フェーズ2キー再生成が完了した後に古いcentryを削除するために、リモートピアから削除メッセージを受信します。

推奨処置 不要です。

713171

エラーメッセージ %PIX|ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload

説明 UDP-Encapsulated-Transportが、フェーズ2中に提案または選択されました。この場合、NAT-Traversal用にこのペイロードを送信する必要があります。

推奨処置 不要です。

713172

エラー メッセージ %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

説明 NAT-Traversal による NAT 自動検出からの結果。

推奨処置 不要です。

713174

エラー メッセージ %PIX|ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!

説明 ハードウェア クライアントがネットワーク拡張モードを使用してトンネルを試行しましたが、ネットワーク拡張モードは許可されていません。

推奨処置 ネットワーク拡張モードと PAT モードとのコンフィギュレーションを確認します。

713176

エラー メッセージ %PIX|ASA-2-713176: *Device_type* memory resources are critical, IKE key acquire message on interface *interface_number*, for Peer *IP_address* ignored

説明 このイベントは、アプライアンスが、示されたピアへの IPSec トンネルをトリガーするためのデータを処理していることを示しています。メモリ リソースは重大な状態なので、トンネルをそれ以上開始していません。データ パケットは無視され、廃棄されました。

推奨処置 条件が解決しない場合は、アプライアンスが効率的に設定されていることを確認します。このイベントは、メモリを増やしたアプライアンスがこのアプリケーションに必要であることを示している場合があります。

713177

エラー メッセージ %PIX|ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: *host_name* Address *IP_address*, Protocol *protocol*, Port *port*

説明 FQDN を含むフェーズ 2 ID ペイロードがピアから受信されました。

推奨処置 不要です。

713178

エラー メッセージ %PIX|ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie

説明 内部ソフトウェア エラーが発生しました。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713179

エラー メッセージ %PIX|ASA-5-713179: IKE AM Initiator received a packet from its peer without a *payload_type* payload

説明 内部ソフトウェア エラーが発生しました。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713182

エラー メッセージ %PIX|ASA-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!

説明 内部ソフトウェア エラーが発生しました。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713184

エラー メッセージ %PIX|ASA-6-713184: Client Type: *Client_type* Client Application Version: *Application_version_string*

説明 このイベントは、クライアントのオペレーティング システムとアプリケーションのバージョンを示します。情報を入手できない場合は、N/A が示されます。

推奨処置 不要です。

713185

エラー メッセージ %PIX|ASA-3-713185: Error: Username too long - connection aborted

説明 クライアントが無効な長さのユーザ名を戻し、トンネルが切断されました。

推奨処置 ユーザ名を確認し、必要に応じて変更します。

713186

エラー メッセージ %PIX|ASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: *list_text* Character *index (value)* is illegal

説明 無効なセカンダリ ドメイン名リストが外部 RADIUS 認証サーバから受信されました。スプリット トンネルが使用されている場合、このリストは、クライアントがトンネルで解決すべきドメインを示します。

推奨処置 RADIUS サーバで Secondary-Domain-Name-List アトリビュート(ベンダー固有のアトリビュート 29)の指定を訂正します。リストは、コンマ区切りのドメイン名のリストとして指定する必要があります。ドメイン名に、英数字、ハイフン、下線、ピリオド以外の文字を組み込むことはできません。

713187

エラー メッセージ %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*

説明 このトンネルを開始しようとしている IKE ピアは、受信されたりモート サブネットにバインドされた ISAKMP コンフィギュレーション内で設定された IKE ピアではありません。

推奨処置 ヘッドエンドとピアで適切な L2L 設定を確認します。

713189

エラー メッセージ %PIX|ASA-3-713189: Attempted to assign network or broadcast *IP_address*, removing (*IP_address*) from pool.

説明 プールからの IP アドレスは、このサブネットのネットワークまたはブロードキャスト アドレスです。このアドレスには、使用不可のマークが付けられます。

推奨処置 通常、これは問題のないエラーですが、IP アドレス プール コンフィギュレーションを確認する必要があります。

713190

エラー メッセージ %PIX|ASA-7-713190: Got bad refCnt (*ref_count_value*) assigning *IP_address* (*IP_address*)

説明 この SA のリファレンス カウンタは無効です。

推奨処置 この問題は、自動的に訂正されます。

713193

エラーメッセージ %PIX|ASA-3-713193: Received packet with missing payload, Expected payload: *payload_id*

説明 アプライアンスが、1つまたは複数の欠落しているペイロードを持つ特定の交換タイプの暗号化 / 暗号解除されたパケットを受信しました。通常、これはピアに問題があることを意味します。

推奨処置 ピアが有効な IKE メッセージを送信していることを確認します。

713194

エラーメッセージ %PIX|ASA-3-713194: IKE|IPSec Delete With Reason message: *termination_reason*

説明 終了理由コードを持つ削除メッセージが受信されたことを示しています。

推奨処置 不要です。

713195

エラーメッセージ %PIX|ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!

説明 Originate Only ピアが着信接続を受け入れることができるのは、最初の P2 トンネルを作成した後だけです。その時点で、どの方向からでもデータは追加のフェーズ 2 トンネルを開始できます。

推奨処置 別の動作を希望する場合は、originate only コンフィギュレーションに再び移動する必要があります。

713196

エラーメッセージ %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!

説明 リモート L2L ピアが Public-Public トンネルを開始しました。これは、別の終端の answer only ピアを期待しますが、本製品はこれには当たりません。設定が誤っている可能性があります。

推奨処置 両方の終端で L2L コンフィギュレーションを確認します。

713197

エラー メッセージ %PIX|ASA-5-713197: The configured Confidence Interval of *number* seconds is invalid for this *tunnel_type* connection. Enforcing the second default.

説明 グループ内の構成済み Confidence Interval が有効な範囲外です。

推奨処置 グループ内の Confidence Setting が有効な範囲内であることを確認します。

713198

エラー メッセージ %PIX|ASA-3-713198: User Authorization failed: *user* User authorization failed.

説明 このイベントには、理由ストリングが含まれています。

推奨処置 グループ コンフィギュレーションとクライアント認可を確認します。

713199

エラー メッセージ %PIX|ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (*counter_value*)!

説明 リーパーによって内部ソフトウェア エラーが訂正されました。

推奨処置 問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713203

エラー メッセージ %PIX|ASA-3-713203: IKE Receiver: Error reading from socket.

説明 このメッセージは、受信した IKE パケットの読み取り中にエラーが発生したことを示しています。通常、これは内部エラーであり、ソフトウェアの問題を示している可能性があります。

推奨処置 通常、これは問題のない状態であり、システムによって自動的に訂正されます。問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713204

エラーメッセージ %PIX|ASA-7-713204: Adding static route for client address:
IP_address

説明 このメッセージは、ピアが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートがルーティング テーブルに追加されたことを示しています。

推奨処置 不要です。

713205

エラーメッセージ %PIX|ASA-3-713205: Could not add static route for client
address: *IP_address*

説明 このメッセージは、クライアントが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートを追加する試みが失敗したことを示しています。これは、ルーティング テーブルまたは破損したネットワーク アドレスでのルートの重複を意味している場合もあります。ルートの重複は、ルートが適切にクリーンアップされていないか、複数のクライアントがネットワークまたはアドレスを共有していることによって発生します。

推奨処置 IP ローカル プール コンフィギュレーション、およびその他の使用中の IP アドレス割り当てメカニズム (DHCP や RADIUS など) をチェックします。ルーティング テーブルからルートがクリアされていることを確認します。また、ピア システムにおけるネットワークやアドレスのコンフィギュレーションも確認します。

713206

エラーメッセージ %PIX|ASA-3-713206: Tunnel Rejected: Conflicting protocols
specified by tunnel-group and group-policy

説明 このメッセージは、グループ ポリシーで指定された許可済みのトンネルが、tunnel-group コンフィギュレーション内の許可済みのトンネルと異なっているために、トンネルが切断されたときに表示されます。

推奨処置 tunnel-group および group-policy コンフィギュレーションを確認します。

713208

エラーメッセージ %PIX|ASA-3-713208: Cannot create dynamic rule for Backup L2L
entry *rule rule_id*

説明 このメッセージは、IKE をトリガーして IPsec データを適切に処理する ACL の作成時に障害が発生したことを示しています。この障害はバックアップ L2L コンフィギュレーションに固有です。これは、コンフィギュレーション エラー、キャパシティ エラーまたは内部ソフトウェア エラーを示していることがあります。

推奨処置 デバイスが最大の Cisco ASA コンフィギュレーションおよび最多の VPN トンネルで実行中の場合、メモリの問題の可能性があります。それ以外の場合、バックアップ L2L および暗号マップ コンフィギュレーション (特に暗号マップと関連付けられている ACL) を確認します。

713209

エラー メッセージ %PIX|ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry *rule_id*

説明 このメッセージは、IKE をトリガーして IPSec データを適切に処理する ACL の削除時に障害が発生したことを示しています。この障害はバックアップ L2L コンフィギュレーションに固有です。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713210

エラー メッセージ %PIX|ASA-3-713210: Cannot create dynamic map for Backup L2L entry *rule_id*

説明 このメッセージは、バックアップ L2L コンフィギュレーションに関連する動的暗号マップの実行時インストールの作成時に障害が発生したことを示しています。これは、コンフィギュレーション エラー、キャパシティ エラーまたは内部ソフトウェア エラーを示していることがあります。

推奨処置 デバイスが最大の Cisco ASA コンフィギュレーションおよび最多の VPN トンネルで実行中の場合、メモリの問題の可能性があります。それ以外の場合、バックアップ L2L および暗号マップ コンフィギュレーション (特に暗号マップと関連付けられている ACL) を確認します。

713211

エラー メッセージ %PIX|ASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 このメッセージは、Cisco ASA がピアのプライベート アドレスまたはネットワーク用のルートを追加していることを示しています。この場合、ピアはアドレスが不明なクライアントまたは L2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック暗号マップを使用します。

推奨処置 不要です。

713212

エラー メッセージ %PIX|ASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 このメッセージは、Cisco ASA がピアのプライベート アドレスまたはネットワーク用のルートを追加しようとして失敗したときに表示されます。この場合、ピアはアドレスが不明なクライアントまたは L2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過す

るのにダイナミック暗号マップを使用します。これは、重複するルートを示している場合があります。ルーティング テーブルがいっぱいになっているか、前に使用したルートを Cisco ASA が削除していません。

推奨処置 ルーティング テーブルに追加ルートのためのスペースがあることと、古いルートが存在しないことを確認します。テーブルがいっぱいになっている場合や古いルートが含まれている場合は、ルートを削除して再試行します。問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713213

エラー メッセージ %PIX|ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 このメッセージは、Cisco ASA がピアのプライベート アドレスまたはネットワーク用のルートを削除していることを示しています。この場合、ピアはアドレスが不明なクライアントまたは L2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック暗号マップを使用します。

推奨処置 不要です。

713214

エラー メッセージ %PIX|ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 このメッセージは、Cisco ASA がピアのプライベート アドレスまたはネットワーク用のルートを削除しようとしたときに障害が発生したことを示しています。この場合、ピアはアドレスが不明なクライアントまたは L2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック暗号マップを使用します。このイベントは、ルートがすでに削除されているか、内部ソフトウェア エラーが発生したことを示している場合があります。

推奨処置 ルートがすでに削除されている場合は、問題のない状態であり、デバイスは正常に機能します。問題が解決しない場合、または VPN トンネルでルーティングの問題にリンクできる場合は、VPN L2L コンフィギュレーションのルーティング部分とアドレッシング部分を確認します。逆ルートの注入と、適切な暗号マップに関連する ACL を確認します。問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713215

エラー メッセージ %PIX|ASA-6-713215: No match against Client Type and Version rules. Client: *type version is/is not* allowed by default

説明 このメッセージは、クライアントのタイプとクライアントのバージョンが Cisco ASA で設定されたルールと一致しなかったことを示しています。デフォルトのアクションが表示されます。

推奨処置 デフォルトのアクションと配置要件を決定し、適切な変更を加えます。

713216

エラー メッセージ %PIX|ASA-5-713216: Rule: *action* Client type : *version* Client: *type version is/is not allowed*

説明 このメッセージは、クライアントのタイプとクライアントのバージョンがルールの1つと一致したことを示しています。一致の結果とルールが表示されます。

推奨処置 配置要件を決定し、適切な変更を加えます。

713217

エラー メッセージ %PIX|ASA-3-713217: Skipping unrecognized rule: action: *action* client type: *client_type* client version: *client_version*

説明 このメッセージは、形式が誤っているクライアントタイプとバージョンルールがあることを示しています。必要な形式は、*action client type / client version action* です。*client type* と *client version* の「許可」または「拒否」が、Session Management の下に表示されます。サポートされるワイルドカード(*)はパラメータごとに1つだけです。

推奨処置 ルールを訂正します。

713218

エラー メッセージ %PIX|ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.

説明 このメッセージは、設定されたルールによるアクセスをクライアントが拒否されたことを示しています。

推奨処置 不要です。

713219

エラー メッセージ %PIX|ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when P1 SA is complete.

説明 このメッセージは、フェーズ1の完了後にフェーズ2メッセージがキューに入れられていることを示しています。

推奨処置 不要です。

713220

エラー メッセージ %PIX|ASA-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.

説明 このメッセージは、キューに入れられフェーズ2メッセージが処理されていることを示しています。

推奨処置 不要です。

713221

エラー メッセージ %PIX|ASA-7-713221: Static Crypto Map check, checking map = *crypto_map_tag*, seq = *seq_number*...

説明 このメッセージは、Cisco ASA が暗号マップで繰り返しコンフィギュレーション情報を探していることを示しています。

推奨処置 不要です。

713222

エラー メッセージ %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*

説明 このメッセージは、設定された暗号マップで反復しているときに、Cisco ASA が関連する ACL と一致できなかったことを示しています。通常、これは ACL の設定が誤っていることを意味します。

推奨処置 このトンネル ピアに関連する ACL を調べ、VPN トンネルの両端から適切なプライベート ネットワークが指定されていることを確認します。

713223

エラー メッセージ %PIX|ASA-7-713223: Static Crypto Map check, map = *crypto_map_tag*, seq = *seq_number*, no ACL configured

説明 このメッセージは、このピアに関連する暗号マップが ACL にリンクされていないことを示しています。

推奨処置 この暗号マップに関連する ACL があることと、ACL に VPN トンネルの両側からの適切なプライベート アドレスまたはネットワークが含まれていることを確認します。

713224

エラー メッセージ %PIX|ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!

説明 このメッセージは、この VPN トンネルに関連する暗号マップで重要な情報が欠落していることを示しています。

推奨処置 VPN ピア、トランスフォーム セット、関連する ACL すべてで暗号マップが正しく設定されていることを確認します。

713225

エラー メッセージ %PIX|ASA-7-713225: [IKEv1], Static Crypto Map check, map *map_name*, seq = *sequence_number* is a successful match

説明 このメッセージは、Cisco ASA がこの VPN トンネルに対して一致する有効な暗号マップを検出したことを示しています。

推奨処置 不要です。

713226

エラー メッセージ %PIX|ASA-3-713226: Connection failed with peer *IP_address*, no trust-point defined in tunnel-group *tunnel_group*

説明 デバイスがデジタル証明書を使用するように設定されている場合は、コンフィギュレーションでトラストポイントを指定する必要があります。トラストポイントが config から欠落している場合は、このメッセージが生成され、エラーのフラグが立てられます。

IP_address : ピアの IP アドレス

tunnel_group : コンフィギュレーションでトラストポイントが欠落しているトンネルグループ。

推奨処置 デバイスの管理者は、コンフィギュレーションでトラストポイントを指定する必要があります。

713228

エラー メッセージ %PIX|ASA-6-713228: Assigned private IP address *assigned_private_IP*

assigned_private_IP : DHCP によって、またはローカル アドレス プールから割り当てられるクライアント IP。

説明 このメッセージは、IKE が DHCP またはアドレス プールからクライアントのプライベート IP アドレス用のアドレスを取得したときに生成されます。このメッセージは、クライアントに割り当てる IP アドレスを指定します。

推奨処置 不要です。

713229

エラー メッセージ %PIX|ASA5-713229: Auto Update - Notification to client *client_ip* of update string: *message_string*.

説明 このメッセージは、更新されたソフトウェアをダウンロードできることが VPN リモートアクセス クライアントに通知されたときに表示されます。リモートクライアントユーザには、クライアントアクセスソフトウェアの更新を選択する責任があります。

client_ip : リモートクライアントの IP アドレス。

message_string : リモートクライアントに送信されるメッセージのテキスト。

推奨処置 不要です。

713230

エラーメッセージ %PIX|ASA-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type *type*

type : ロックの問題を持つセマフォのタイプを説明するストリング。

説明 このメッセージは、IKE サブシステムがすでにロックされているメモリをロックしようとしていることを報告する内部エラーが原因で表示されます。これは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを示します。このメッセージは、重大な誤りがないことを示しています。ただし、予期しないイベントが発生し、自動的に回復されました。

推奨処置 TAC に問い合せて、エラーを報告してください。

713231

エラーメッセージ %PIX|ASA-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type *type*

説明 このメッセージは、IKE サブシステムが現在ロックされていないメモリをロック解除しようとしていることを報告する内部エラーが原因で表示されます。これは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを示します。このメッセージは、重大な誤りがないことを示しています。ただし、予期しないイベントが発生し、自動的に回復されました。

type : ロックの問題を持つセマフォのタイプを説明するストリング。

推奨処置 TAC に問い合せて、エラーを報告してください。

713232

エラーメッセージ %PIX|ASA-3-713232 SA lock refCnt = *value*, bitmask = *hexvalue*, pl_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*

説明 このメッセージは、すべての IKE SA ロックを表示します。これは、発生する可能性のあるエラーが検出されたときに表示されます。このメッセージは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを報告します。

value : 10 進数値。

hexvalue : 16 進数値。

推奨処置 TAC に問い合せて、エラーを報告してください。

713233

エラー メッセージ %PIX|ASA-7-713233: (VPN-unit) Remote network (*remote network*) validated for network extension mode.

説明 このメッセージは、フェーズ 2 ネゴシエーション中に受信されたりリモート ネットワークが検証されたときに表示されます。このメッセージは、ネットワーク拡張モード クライアントのフェーズ 2 ネゴシエーションでリモート ネットワーク チェックの結果を示します。これは、ユーザが HW クライアント ネットワークの設定を誤らないようにするための既存の機能の一部です（複数のクライアントでの重複するネットワークや同じネットワークの設定など）。

remote network : フェーズ 2 のプロキシのサブネット アドレスおよびサブネットマスク

推奨処置 不要です。

713234

エラー メッセージ %PIX|ASA-7-713234: (VPN-unit) Remote network (*remote network*) from network extension mode client mismatches AAA configuration (*aaa network*).

説明 このメッセージは、フェーズ 2 ネゴシエーション中に受信されたりリモート ネットワークが、このセッションの AAA サーバから戻された framed-ip-address および framed-subnet-mask と一致しない場合に表示されます。

remote network : フェーズ 2 のプロキシのサブネット アドレスおよびサブネットマスク

aaa network : AAA で設定されたサブネット アドレスとサブネットマスク。

推奨処置 次のいずれかを実行します。

- このユーザとグループのアドレス割り当てをチェックし、HW クライアントのネットワーク コンフィギュレーションを確認して、不整合をすべて修正します。
- このユーザおよびグループのアドレス割り当てをディセーブルにします。

713235

エラー メッセージ %PIX|ASA-7-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!

説明 通常、IKE パケットをスタンバイ装置からリモート ピアへ送信することはありません。このメッセージは、そのような試みがされた場合に、内部ロジックエラーによって表示されます。保護コードのため、パケットはスタンバイ装置から離れません。このメッセージは、主にデバッグを促進します。

推奨処置 ユーザによる処置は不要です。開発者は、IKE パケットがスタンバイ装置から送信される原因になった条件を調べる必要があります。

713236

エラー メッセージ %PIX|ASA-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads :payload1 (payload1_len) + payload2 (payload2_len)...total length : tlen

説明 このメッセージは、IKE がさまざまなメッセージを送信または受信したときに表示されません。

次の例に、IKE が 8 バイトのハッシュペイロード、11 バイトの通知ペイロード、および 2 つの 13 バイトのベンダー固有ペイロードでメッセージを受信した場合の出力を示します。

```
%PIX-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads : HDR + HASH (8)
+ NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

推奨処置 不要です。

713237

エラー メッセージ %PIX|ASA-5-713237: ACL update (*access_list*) received during re-key re-authentication will not be applied to the tunnel.

access_list : **show access-list** コマンドの出力に表示される、静的または動的 access-list に関連付けられた名前。

説明 このメッセージは、次の条件で、リモート アクセス IPSec トンネルのフェーズ 1 のキー再生成中に表示されます。

- トンネルは、トンネルのキー再生成時にユーザを再認証するよう設定されています。
- RADIUS サーバは、アクセス リストまたはリファレンスを、ローカルで設定されたアクセス リストに戻します。これは、トンネルが最初に確立されたときに戻されたアクセス リストとは異なります。

これらの条件下では、セキュリティ アプライアンス は新しいアクセス リストを無視し、このメッセージを生成します。

推奨処置 IPSec ユーザは、ユーザ指定のアクセス リストを有効にするため、再接続する必要があります。

713238

エラー メッセージ %PIX|ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client

説明 ネットワーク拡張モード クライアントのプライベート側のアドレスが 0.0.0.0 です。通常、これは、ハードウェア クライアントのプライベート インターフェイスで IP アドレスが設定されていなかったことを示します。

推奨処置 リモート クライアントのコンフィギュレーションを確認します。

713900

エラー メッセージ %PIX|ASA-7-713900:Descriptive_event_string.

説明 重大なイベントまたは障害を示すいくつかの使用可能なテキスト スtringを持つメッセージ。

推奨処置 問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

713901

エラー メッセージ %PIX|ASA-7-713901:Descriptive_event_string.

説明 発生したエラーを示すいくつかの使用可能なテキスト スtringを持つメッセージ。これは、ヘッドエンドまたはリモート アクセス クライアントにおけるコンフィギュレーション エラーの結果である可能性があります。イベント スtringは、発生したエラーの詳細を提供します。

推奨処置 場合によっては、エラーの原因を判別するためコンフィギュレーションをトラブルシューティングする必要があります。両方のピアで `isakmp` および `暗号マップ` コンフィギュレーションを確認します。

713902

エラー メッセージ %PIX|ASA-3-713902 Descriptive_event_string

説明 このシステム ログ メッセージには、エラーについて説明するいくつかの使用可能なテキスト スtringがあります。これは、ヘッドエンドまたはリモート アクセス クライアントにおけるコンフィギュレーション エラーの結果である可能性があります。

推奨処置 場合によっては、エラーの原因を判別するためコンフィギュレーションをトラブルシューティングする必要があります。両方のピアで、ISAKMP および暗号マップ コンフィギュレーションを確認します。

713903

エラー メッセージ %PIX|ASA-4-713903:Descriptive_event_string.

説明 警告を示すいくつかの使用可能なテキスト スtringを持つ syslog。これは、ピアの予期しない動作の結果である可能性があります (たとえば、接続の切断)。

推奨処置 情報のみです。

713904

エラー メッセージ %PIX|ASA-5-713904: *Descriptive_event_string*.

説明 何種類かのテキスト文字列が考えられる syslog。一般的なステータス情報を示します。これらのメッセージは、発生したイベントを追跡するために使用されます。

推奨処置 情報のみです。

713905

エラー メッセージ %PIX|ASA-7-713905: *Descriptive_event_string*.

説明 何種類かのテキスト文字列が考えられる syslog。一般的なステータス情報を示します。これらのメッセージは、発生したイベントを追跡するために使用されます。

推奨処置 情報のみです。

713906

エラー メッセージ %PIX|ASA-7-713906: *debug_message*

説明 このメッセージは、さまざまな VPN デバッグ イベントに使用されます。

推奨処置 処置は不要です。このメッセージは、デバッグのために提供されます。

714001

エラー メッセージ %PIX|ASA-7-714001: *Description of event or packet*

説明 IKE プロトコル イベントまたはパケットの説明。

推奨処置 情報のみです。

714002

エラー メッセージ %PIX|ASA-7-714002: IKE Initiator starting QM: msg id = *message_number*

説明 Cisco ASA は、フェーズ 2 発信者としてクイック モード交換の最初のパケットを送信します。

推奨処置 情報のみです。

714003

エラー メッセージ %PIX|ASA-7-714003: IKE Responder starting QM: msg id = *message_number*

説明 Cisco ASA は、フェーズ 2 応答者としてクイック モード交換の最初のパケットを受信します。

推奨処置 情報のみです。

714004

エラー メッセージ %PIX|ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = *message_number*

説明 最初のクイック モード パケットのプロトコル デコード。

推奨処置 情報のみです。

714005

エラー メッセージ %PIX|ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = *message_number*

説明 2 番目のクイック モード パケットのプロトコル デコード。

推奨処置 情報のみです。

714006

エラー メッセージ %PIX|ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = *message_number*

説明 3 番目のクイック パケットのプロトコル デコード。

推奨処置 情報のみです。

714007

エラー メッセージ %PIX|ASA-7-714007: IKE Initiator sending Initial Contact

説明 Cisco ASA は、最初のコンタクト ペイロードを構築および送信しています。

推奨処置 情報のみです。

714011

エラー メッセージ %PIX|ASA-7-714011: *Description of received ID values*

説明 ネゴシエーション中に表示される ID 情報を受信しました。

推奨処置 情報のみです。

715001

エラー メッセージ %PIX|ASA-7-715001: *Descriptive statement*

説明 このメッセージは、Cisco ASA が検出したイベントまたは問題の説明を提供します。

推奨処置 処置は、説明によって異なります。

715004

エラー メッセージ %PIX|ASA-7-715004: subroutine *name()* Q Send failure: RetCode (*return_code*)

説明 このメッセージは、キュー内にメッセージを置こうとしたときに内部エラーが発生したことを示しています。

推奨処置 多くの場合、これは問題のない状態ですが、問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715005

エラー メッセージ %PIX|ASA-7-715005: subroutine *name()* Bad message code: Code (*message_code*)

説明 このメッセージは、内部サブルーチンが不良なメッセージ コードを受信したことを示しています。

推奨処置 多くの場合、これは問題のない状態ですが、問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715006

エラー メッセージ %PIX|ASA-7-715006: IKE got SPI from key engine: SPI = *SPI_value*

説明 このメッセージは、IKE サブシステムが IPSec から SPI 値を受信したことを示しています。

推奨処置 不要です。

715007

エラー メッセージ %PIX|ASA-7-715007: IKE got a KEY_ADD msg for SA: SPI = *SPI_value*

説明 このメッセージは、IKE がトンネル ネゴシエーションを完了し、IPSec が使用する適切な暗号化キーとハッシュ キーを正常にロードしたことを示しています。

推奨処置 不要です。

715008

エラー メッセージ %PIX|ASA-7-715008: Could not delete SA *SA_address*, refCnt = *number*, caller = *calling_subroutine_address*

説明 このメッセージは、呼び出し側のサブルーチンが IPSec SA を削除できなかったことを示しています。これは、リファレンス カウントの問題の可能性を示しています。

推奨処置 このイベントの結果として古い SA の数が増加した場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715009

エラー メッセージ %PIX|ASA-7-715009: IKE Deleting SA: Remote Proxy *IP_address*, Local Proxy *IP_address*

説明 このメッセージは、リストされたプロキシ アドレスで SA が削除されていることを示しています。

推奨処置 不要です。

715013

エラー メッセージ %PIX|ASA-7-715013: Tunnel negotiation in progress for destination *IP_address*, discarding data

説明 このメッセージは、このデータ用のトンネルの確立中であることを示しています。トンネルが完全に確立されるまで、このトンネルによって保護されるすべてのパケットが廃棄されます。

推奨処置 不要です。

715019

エラー メッセージ %PIX|ASA-7-715019: IKEGetUserAttributes: Attribute name = *name*

説明 このメッセージは、Cisco ASA によって処理されている *modcfg* アトリビュートの名前と値のペアを表示されます。

推奨処置 不要です。

715020

エラーメッセージ %PIX|ASA-7-715020: construct_cfg_set: Attribute name = *name*

説明 このメッセージは、Cisco ASA によって送信されている *modcfg* アトリビュートの名前と値のペアを表示されます。

推奨処置 不要です。

715021

エラーメッセージ %PIX|ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

説明 このメッセージは、フェーズ 1 処理がすべて完了するまで（トランザクション モードなど）、クイックモードの処理が遅延することを示しています。

推奨処置 不要です。

715022

エラーメッセージ %PIX|ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

説明 このメッセージは、フェーズ 1 処理が完了し、クイックモードの処理が再開されていることを示しています。

推奨処置 不要です。

715027

エラーメッセージ %PIX|ASA-7-715027: IPsec SA Proposal # *chosen_proposal*, Transform # *chosen_transform* acceptable Matches global IPsec SA entry # *crypto_map_index*

説明 このメッセージは、示された IPsec SA プロポーザルおよびトランスフォームが応答者が受信したペイロードから選択された場合に表示されます。このデータは、IKE ネゴシエーションの問題のデバッグを試みる際に役立ちます。

推奨処置 不要です。

715028

エラーメッセージ %PIX|ASA-7-715028: IKE SA Proposal # 1, Transform # *chosen_transform* acceptable Matches global IKE entry # *crypto_map_index*

説明 このメッセージは、示された IKE SA トランスフォームが応答者が受信したペイロードから選択された場合に表示されます。このデータは、IKE ネゴシエーションの問題のデバッグを試みる際に役立ちます。

推奨処置 不要です。

715033

エラー メッセージ %PIX|ASA-7-715033: Processing CONNECTED notify (MsgId *message_number*)

説明 このメッセージは、Cisco ASA が通知タイプ CONNECTED (16384) で通知ペイロードを含むメッセージを処理していることを示しています。CONNECTED 通知は、コミット ビット処理を完了するために使用されます。これは、応答者から発信者へ送信される 4 番目のクイックモード パケット全体に組み込む必要があります。

推奨処置 不要です。

715034

エラー メッセージ %PIX|ASA-7-715034: action IOS keep alive payload: proposal=*time* /*time* 2 sec.

説明 このメッセージは、キープアライブ ペイロード メッセージの送信 / 受信が処理されていることを示しています。

推奨処置 不要です。

715035

エラー メッセージ %PIX|ASA-7-715035: Starting IOS keepalive monitor: *seconds* sec.

説明 このメッセージは、キープアライブ タイマーがキープアライブ メッセージの可変の秒数を監視することを示しています。

推奨処置 不要です。

715036

エラー メッセージ %PIX|ASA-7-715036: Sending keep-alive of type *notify_type* (seq number *number*)

説明 このメッセージは、キープアライブ通知メッセージの送信が処理されていることを示しています。

推奨処置 不要です。

715037

エラー メッセージ %PIX|ASA-7-715037: Unknown IOS Vendor ID version:
major.minor.variance

説明 このメッセージは、このバージョンの IOS の機能が未知であることを示しています。

推奨処置 IKE キープアライブなどの機能との相互運用の問題がある可能性があります。このタイプの相互運用の問題が発生した場合は、コンソールまたはシステム ログに表示されるエラーメッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して、収集した情報を IOS と Cisco ASA の両方のソフトウェア バージョン情報とともに、ご提供ください。

715038

エラー メッセージ %PIX|ASA-7-715038: action *Spoofing_information* Vendor ID payload
(version: *major.minor.variance*, capabilities: *value*)

説明 このメッセージは、IOS ベンダー ID ペイロードの処理が実行されたことを示しています。処理されているメッセージが Altiga スプーフィング IOS である可能性があります。

推奨処置 不要です。

715039

エラー メッセージ %PIX|ASA-7-715039: Unexpected cleanup of tunnel table entry
during SA delete.

説明 このメッセージは、SA が解放されたときに削除されなかった IKE トンネル テーブル内のエントリがあることを示しています。これは、ステート マシン内のバグを示しています。

推奨処置 問題が解決しない場合、コンソールまたはシステム ログに表示されるエラーメッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715040

エラー メッセージ %PIX|ASA-7-715040: Deleting active auth handle during SA
deletion: handle = *internal_authentication_handle*

説明 このメッセージは、SA 削除中に auth ハンドルがまだアクティブであることを示しています。これは、エラー状態中のクリーンアップ リカバリの一部です。

推奨処置 不要です。

715041

エラー メッセージ %PIX|ASA-7-715041: Received keep-alive of type *keepalive_type*, not the negotiated type

説明 これは、メッセージ内に示されたタイプのキープアライブが予期せず受信されたことを示しています。

推奨処置 両方のピアでキープアライブ コンフィギュレーションを確認します。

715042

エラー メッセージ %PIX|ASA-7-715042: IKE received response of type *failure_type* to a request from the *IP_address* utility

説明 これは、これらのアドレスを提供する内部ユーティリティからのリモート アクセス クライアントの IP アドレスに対する要求が満たされなかったことを示しています。メッセージ ストリング内の変数テキストによって、問題点がより具体的に示されます。

推奨処置 IP アドレス割り当て コンフィギュレーションを確認し、適宜、調整します。

715044

エラー メッセージ %PIX|ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability

説明 KA 機能を設定せずにベンダーから IOS キープアライブ ペイロードを受信しました。ペイロードが無視されています。

推奨処置 情報のみです。

715045

エラー メッセージ %PIX|ASA-7-715045: ERROR: malformed Keepalive payload

説明 形式が誤ったキープアライブ ペイロードを受信しました。ペイロードが無視されています。

推奨処置 情報のみです。

715046

エラー メッセージ %PIX|ASA-7-715046: constructing *payload_description* payload

説明 構築中の IKE ペイロードの詳細を表示します。

推奨処置 情報のみです。

715047

エラー メッセージ %PIX|ASA-7-715047: processing *payload_description* payload

説明 受信した、処理中の IKE ペイロードの詳細を表示します。

推奨処置 情報のみです。

715048

エラー メッセージ %PIX|ASA-7-715048: Send *VID_type* VID

説明 送信中のベンダー ID ペイロードのタイプを表示します。

推奨処置 情報のみです。

715049

エラー メッセージ %PIX|ASA-7-715049: Received *VID_type* VID

説明 受信したベンダー ID ペイロードのタイプを表示します。

推奨処置 情報のみです。

715050

エラー メッセージ %PIX|ASA-7-715050: Claims to be IOS but failed authentication

説明 IOS VID と似ていますが、*hmac_sha* と一致しません。

推奨処置 両方のピアでベンダー ID コンフィギュレーションを確認します。問題が相互運用に影響する場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715051

エラー メッセージ %PIX|ASA-7-715051: Received unexpected TLV type *TLV_type* while processing FWTYPE ModeCfg Reply

説明 FWTYPE ModeCfg Reply の処理中に、Cisco ASA レコードで未知の TLV が受信されました。これは廃棄されます。パケットが破損しているため、または接続しているクライアントが後のバージョンの Cisco ASA プロトコルをサポートしているために発生する可能性があります。

推奨処置 Cisco VPN クライアントにインストールされている個人用 FW および Cisco ASA 上の個人用 FW コンフィギュレーションを確認します。これは、VPN クライアントと Cisco ASA の間のバージョンの不一致を示している可能性もあります。

715052

エラー メッセージ %PIX|ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries

説明 古い P1 SA が削除されていますが、新しい SA にも削除のマークが付けられているため、移行先となる新しい SA がありません。通常、これは、2 IKE ピアが同期外で、異なるキー再生成時間を使用している可能性があることを示しています。問題は自動的に訂正されますが、新しい P1 SA が再確立されるまで、少量のデータ損失が発生する可能性があります。

推奨処置 情報のみです。

715053

エラー メッセージ %PIX|ASA-7-715053: MODE_CFG: Received request for *attribute_info!*

説明 指摘されたアトリビュートを要求するモード コンフィギュレーション メッセージを受信しました。

推奨処置 情報のみです。

715054

エラー メッセージ %PIX|ASA-7-715054: MODE_CFG: Received *attribute_name* reply: *value*

説明 リモート ピアからモード コンフィギュレーション応答メッセージを受信しました。

推奨処置 情報のみです。

715055

エラー メッセージ %PIX|ASA-7-715055: Send *attribute_name*

説明 リモート ピアにモード コンフィギュレーション応答メッセージを送信しました。

推奨処置 情報のみです。

715056

エラー メッセージ %PIX|ASA-7-715056: Client is configured for *TCP_transparency*

説明 IPSec Over TCP に対してリモート エンド (クライアント) が設定されているので、ヘッドエンド Cisco ASA がクライアントと IPSec Over UDP または IPSec over NAT-T をネゴシエートすることはできません。

推奨処置 トンネルが開始しない場合は、ピアのいずれかの NAT 透過 コンフィギュレーションに対する調整が必要な場合があります。それ以外の場合、これは情報メッセージです。

715057

エラー メッセージ %PIX|ASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.

説明 NAT-Traversal が検出されたため、IPSec-over-UDP Mode Config info は交換されません。

推奨処置 情報のみです。

715058

エラー メッセージ %PIX|ASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.

説明 NAT-Traversal VID の交換後、リモートエンドが NAT-Traversal に必要な NAT-D ペイロードを提供しませんでした。少なくとも2つの NAT-D ペイロードを受信する必要があります。

推奨処置 NAT-T 実装が規格に従っていないことを示している可能性があります。攻撃ピアがシスコ製品である場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して、収集した情報を製品番号およびソフトウェア バージョンとともにご提供ください。攻撃ピアがシスコ製品ではない場合は、製造元サポート チームにお問い合わせください。

715059

エラー メッセージ %PIX|ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal

説明 NAT-Traversal を正常にネゴシエートするため SA で定義された通常の Transport モードおよび Tunnel モードの代わりにこれらのモードを使用する必要があります。

推奨処置 情報のみです。

715060

エラー メッセージ %PIX|ASA-7-715060: Dropped received IKE fragment. Reason: *reason*

説明 フラグメントを廃棄した理由が表示されます。

推奨処置 廃棄の理由にもよりますが、これは、NAT 装置が干渉している問題やピアが規格に従っていない問題を示している可能性があります。

715061

エラー メッセージ %PIX|ASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.

説明 これは、同じパケットを再送したが別の MTU にフラグメント化されたか、あるいはまったく別のパケットである可能性があります。

推奨処置 情報のみです。

715062

エラー メッセージ %PIX|ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.

説明 フラグメント番号にギャップがあります。

推奨処置 これはネットワークの問題を示している可能性があります。この条件によってトンネルが廃棄されるか、特定のピアが Cisco ASA とネゴシエートできない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して、収集した情報を製品番号およびソフトウェア バージョンとともにご提供ください。

715063

エラー メッセージ %PIX|ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!

説明 受信されたフラグメント化パケットの組み立てが成功しました。

推奨処置 情報のみです。

715064

エラー メッセージ %PIX|ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: *true/false* Aggressive Mode: *true/false*

説明 ピアは、メッセージで提供された情報に基づく IKE フラグメントをサポートしています。

推奨処置 情報のみです。

715065

エラー メッセージ %PIX|ASA-7-715065: IKE *state_machine subtype* FSM error history (struct *data_structure_address*) *state, event: state/event* pairs

説明 フェーズ I エラーが発生し、状態、イベント履歴ペアが新しい順に表示されます。

推奨処置 これらのエラーのほとんどは、問題ありません。これらのメッセージが望ましくない動作と関連している場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715066

エラー メッセージ %PIX|ASA-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.

説明 IKE SA 内の論理 ID は NULL です。フェーズ II ネゴシエーションは切断されます。

推奨処置 内部エラーが発生しました。装置が回復せず正常に動作しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715067

エラー メッセージ %PIX|ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa

説明 確立中の LAN-TO-LAN SA はすでに存在します。つまり、同じリモート ネットワークを持ち、別のピアをソースとする SA があります。これは正当なコンフィギュレーションではないので、新規 SA は削除されます。

推奨処置 関連するすべてのピアで LAN-TO-LAN コンフィギュレーションを確認します。特に、複数のピアがプライベート ネットワークを共有することはできません。

715068

エラー メッセージ %PIX|ASA-7-715068: QM IsRekeyed: duplicate sa found by *address*, deleting old sa

説明 確立中のリモート アクセス SA はすでに存在します。つまり、同じリモート ネットワークを持ち、別のピアをソースとする SA があります。ピアが IP アドレスを変更した可能性があるため、古い SA は削除されます。

推奨処置 特にクライアント トンネルが異常終了した場合、これは問題のない状態である可能性があります。これらのメッセージが望ましくない動作と関連している場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715069

エラー メッセージ %PIX|ASA-7-715069: Invalid ESP SPI size of *SPI_size*

説明 無効な ESP SPI サイズの IPSec SA プロポーザルを受信しました。このプロポーザルはスキップされます。

推奨処置 通常、これは問題のない状態ですが、ピアが規格に従っていないことを示している可能性があります。問題が解決しない場合、およびピアがトンネルを正常にネゴシエートできない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715070

エラー メッセージ %PIX|ASA-7-715070: Invalid IPComp SPI size of *SPI_size*

説明 無効な IPComp SPI サイズの IPSec SA プロポーザルを受信しました。このプロポーザルはスキップされます。

推奨処置 通常、これは問題のない状態ですが、ピアが規格に従っていないことを示している可能性があります。問題が解決しない場合、およびピアがトンネルを正常にネゴシエートできない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715071

エラー メッセージ %PIX|ASA-7-715071: AH proposal not supported

説明 IPSec AH プロポーザルはサポートされていません。このプロポーザルはスキップされます。

推奨処置 情報のみです。

715072

エラー メッセージ %PIX|ASA-7-715072: Received proposal with unknown protocol ID *protocol_ID*

説明 未知の protocol ID を持つ IPSec SA プロポーザルを受信しました。このプロポーザルはスキップされます。

推奨処置 通常、これは問題のない状態ですが、ピアが規格に従っていないことを示している可能性があります。問題が解決しない場合、およびピアがトンネルを正常にネゴシエートできない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715074

エラー メッセージ %PIX|ASA-7-715074: Could not retrieve authentication attributes for peer *IP_address*

説明 リモート ユーザの認可情報を取得できませんでした。

推奨処置 すべての認証および認可コンフィギュレーションが正しく設定されていることを確認します。問題が解決しない場合、およびピアがトンネルを正常にネゴシエートできない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

715075

エラー メッセージ %PIX|ASA-7-715075: Group = *group_name*, Username = *client*, IP = *IP_address* Received keep-alive of type *message_type* (seq number *number*)

説明 この新規メッセージは、DPD 送信メッセージをログに記録する 715036「DPD R-U-THERE」メッセージとペアです。

考えられる原因は 2 つあります。

- 1) ピア送信「DPD R-U-THERE」メッセージを受信した。
- 2) ピア応答「DPD R-U-THERE-ACK」メッセージを受信した。

ユーザは次の事例を確認することをお勧めします。

事例 1: 「DPD R-U-THERE」が受信され、そのシーケンス番号が発信 DPD 応答メッセージと一致する。

f1 がピアから「DPD R-U-THERE」を受信する前に「DPD R-U-THERE-ACK」を送信すると、セキュリティ違反が発生する可能性があります。

事例 2: 受信した「DPD R-U-THERE-ACK」メッセージのシーケンス番号が前の送信 DPD メッセージのシーケンス番号と一致する。

f1 が「DPD R-U-THERE」をピアへ送信した後、適当な期間「DPD R-U-THERE-ACK」を受信しなかった場合、トンネルはダウンする可能性があります。

group_name: ピアの VPN グループ名。

client: ピアのユーザ名。

IP_address: VPN ピアの IP アドレス。

message_type: メッセージ タイプ («DPD R-U-THERE」または「DPD R-U-THERE-ACK」)。

number: DPD シーケンス番号。

推奨処置 ユーザによる処置は不要です。

715076

エラー メッセージ %PIX|ASA-7-715076: Computing hash for ISAKMP

説明 このメッセージは、IKE がさまざまなハッシュ値を計算したときに表示されます。このオブジェクトは次のとおり追加されます。

Group = *groupname*, Username = *username*, IP = *ip_address*, ...

推奨処置 不要です。

715077

エラー メッセージ %PIX|ASA-7-715077: Pitcher: *msg string*, *spi spi*

説明 このメッセージは、さまざまなメッセージが IKE に送信されたときに表示されます。
msg_string は次のいずれかです。

- 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

その他の ISAKMP と同様に、次の文が適用されます。

このオブジェクトは次のとおり追加されます。

Group = *groupname*, Username = *username*, IP = *ip_address*, ...

推奨処置 不要です。

716001

エラー メッセージ %ASA-6-716001: Group *group* User *user* WebVPN session started.

説明 この *group* の *user* に対して WebVPN セッションが開始されました。ユーザが WebVPN ログイン ページを介してログインすると、WebVPN セッションが開始されます。

推奨処置 不要です。

716002

エラー メッセージ %ASA-6-716002: Group *group* User *user* WebVPN session terminated: *reason*.

説明 特定の理由で WebVPN セッションが終了しました。考えられる理由を次に示します。

- ユーザが要求した
- 搬送が失われた
- サービスが失われた
- アイドル タイムアウト
- 最大時間を超過した

- 管理者がリセットした
- 管理者がリブートした
- 管理者がシャットダウンした
- ポートエラー
- NAS エラー
- NAS 要求
- NAS リブート
- ポートが必要ない
- ポートが切り替えられた
- ポートが中断された
- サービスが使用不可
- コールバック
- ユーザエラー
- ホストが要求した
- 帯域幅の管理エラー
- ACL 解析エラー
- 不明

推奨処置 *reason* に問題が示されていない限り、処置は不要です。

716003

エラーメッセージ %ASA-6-716003: Group *group* User *user* WebVPN access GRANTED:: *url*

説明 この *group* 内の WebVPN *user* は、この *url* へのアクセス権を与えられています。さまざまな場所へのユーザのアクセスは、WebVPN 固有のアクセス コントロール リストを使用して制御できます。

推奨処置 不要です。

716004

エラーメッセージ %ASA-6-716004: Group *group* User *user* WebVPN access DENIED to specified location: *url*

説明 この *group* 内の WebVPN *user* は、この *url* へのアクセス権を拒否されています。さまざまな場所への WebVPN ユーザのアクセスは、WebVPN 固有のアクセス コントロール リストを使用して制御できます。この場合は、特定のアクセス コントロール リスト エントリがこの *url* へのアクセスを拒否しています。

推奨処置 不要です。

716005

エラー メッセージ %ASA-6-716005: Group *group* User *user* WebVPN ACL Parse Error: *reason*

説明 指摘されたグループ内の WebVPN ユーザの ACL が正しく解析できませんでした。エラーの原因が報告されます。

この *group* 内の *user* 用の WebVPN アクセス コントロール リストが正しく解析できませんでした。エラーの原因が報告されます。

推奨処置 WebVPN の ACL を修正します。

716006

エラー メッセージ %ASA-6-716006: Group *name* User *user* WebVPN session terminated. Idle timeout.

説明 VPN トンネル プロトコルが WebVPN に設定されていないため、指摘されたグループ内でこのユーザに対して WebVPN セッションが作成されませんでした。

推奨処置 不要です。

716007

エラー メッセージ %ASA-4-716007: Group *group* User *user* WebVPN Unable to create session.

説明 リソースの問題のため、指摘されたグループ内でユーザに対して WebVPN セッションが作成されませんでした。たとえば、ユーザが最大ログイン制限に達した可能性があります。

推奨処置 不要です。

716008

エラー メッセージ %ASA-7-716008: WebVPN ACL: *action*

説明 WebVPN ACL が *action* の実行を開始しました。たとえば、*action* が「begin parsing」である可能性があります。これは、デバッグ レベル メッセージです。

推奨処置 不要です。

716009

エラーメッセージ %ASA-6-716009: Group *group* User *user* WebVPN session not allowed.
WebVPN ACL parse error.

説明 関連するアクセスコントロールリストが解析していないため、このグループ内の指摘されたユーザの WebVPN セッションが許可されません。このエラーが訂正されるまで、ユーザが WebVPN を介してログインすることは許可されません。

推奨処置 WebVPN の ACL を修正します。

716010

エラーメッセージ %ASA-7-716010: Group *group* User *user* Browse network.

説明 指摘されたグループ内の、WebVPN user がネットワークをブラウズしました。

推奨処置 不要です。

716011

エラーメッセージ %ASA-7-716011: Group *group* User *user* Browse domain *domain*.

説明 このグループ内の、指摘された WebVPN user が、指摘されたドメインをブラウズしました。

推奨処置 不要です。

716012

エラーメッセージ %ASA-7-716012: Group *group* User *user* Browse directory *directory*.

説明 指摘された WebVPN ユーザが、指摘されたディレクトリをブラウズしました。

推奨処置 不要です。

716013

エラーメッセージ %ASA-7-716013: Group *group* User *user* Close file *filename*.

説明 指摘された WebVPN ユーザが、指摘されたファイルを閉じました。

推奨処置 不要です。

716014

エラー メッセージ %ASA-7-716014: Group *group* User *user* View file *filename*.

説明 指摘された WebVPN ユーザが、指摘されたファイルを参照しました。

推奨処置 不要です。

716015

エラー メッセージ %ASA-7-716015: Group *group* User *user* Remove file *filename*.

説明 指摘されたグループ内の WebVPN ユーザが、指摘されたファイルを削除しました。

推奨処置 不要です。

716016

エラー メッセージ %ASA-7-716016: Group *group* User *user* Rename file *old_filename* to *new_filename*.

説明 指摘された WebVPN ユーザが、指摘されたファイルの名前を変更しました。

推奨処置 不要です。

716017

エラー メッセージ %ASA-7-716017: Group *group* User *user* Modify file *filename*.

説明 指摘された WebVPN ユーザが、指摘されたファイルを修正しました。

推奨処置 不要です。

716018

エラー メッセージ %ASA-7-716018: Group *group* User *user* Create file *filename*.

説明 指摘された WebVPN ユーザが、指摘されたファイルを作成しました。

推奨処置 不要です。

716019

エラー メッセージ %ASA-7-716019: Group *group* User *user* Create directory *directory*.

説明 指摘された WebVPN ユーザが、指摘されたディレクトリを作成しました。

推奨処置 不要です。

716020

エラー メッセージ %ASA-7-716020: Group *group* User *user* Remove directory *directory*.

説明 指摘された WebVPN ユーザが、指摘されたディレクトリを削除しました。

推奨処置 不要です。

716021

エラー メッセージ %ASA-7-716021: File access DENIED, *filename*.

説明 指摘された WebVPN ユーザが、指摘されたファイルへのアクセスを拒否されました。

推奨処置 不要です。

716022

エラー メッセージ %ASA-4-716022: Unable to connect to proxy server *reason*.

説明 WebVPN HTTP/HTTPS のリダイレクトが、指摘された理由で失敗しました。

推奨処置 HTTP/HTTPS プロキシ コンフィギュレーションを確認します。

716023

エラー メッセージ %ASA-4-716023: Group *name* User *user* Session could not be established: session limit of *maximum_sessions* reached.

説明 現在のセッション数が最大セッション ロードを超過しているため、ユーザ セッションを確立できません。

推奨処置 可能であれば、設定されている制限を増加し、ロードバランスクラスタを増やします。

716024

エラー メッセージ %ASA-7-716024: Group *name* User *user* Unable to browse the network. Error: *description*

説明 ユーザが説明に従い CIFS プロトコルを介して Windows ネットワークをブラウズすることができません。たとえば、「Unable to contact necessary server」は、リモートサーバが使用不可または到達不能であることを示しています。これは、一時的な状態である場合もありますし、さらにトラブルシューティングが必要な場合もあります。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。

716025

エラー メッセージ %ASA-7-716025: Group *name* User *user* Unable to browse domain *domain*. Error: *description*

説明 ユーザが CIFS プロトコルを介してリモート ドメインをブラウズできません。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。

716026

エラー メッセージ %ASA-7-716026: Group *name* User *user* Unable to browse directory *directory*. Error: *description*

説明 ユーザが CIFS プロトコルを介してリモート ディレクトリをブラウズできません。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。

716027

エラー メッセージ %ASA-7-716027: Group *name* User *user* Unable to view file *filename*. Error: *description*

説明 ユーザが CIFS プロトコルを介してリモート ファイルを表示できません。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。

716028

エラー メッセージ %ASA-7-716028: Group *name* User *user* Unable to remove file *filename*. Error: *description*

説明 ユーザが CIFS プロトコルを介してリモート ファイルを削除できません。このエラーは、許可がないために発生した可能性があります。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。ファイルのアクセス権を確認します。

716029

エラー メッセージ %ASA-7-716029: Group *name* User *user* Unable to rename file *filename*. Error: *description*

説明 ユーザが CIFS プロトコルを介してリモート ファイルの名前を変更できません。このエラーは、アクセス権の問題が原因と考えられます。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。ファイルのアクセス権を確認します。

716030

エラー メッセージ %ASA-7-716030: Group *name* User *user* Unable to modify file *filename*. Error: *description*

説明 ユーザが CIFS プロトコルを介して既存のファイルを変更しようとしたときに、問題が発生しました。このエラーは、アクセス権の問題が原因と考えられます。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。ファイルのアクセス権を確認します。

716031

エラー メッセージ %ASA-7-716031: Group *name* User *user* Unable to create file *filename*. Error: *description*

説明 ユーザが CIFS プロトコルを介してファイルを作成しようとしたときに、問題が発生しました。このエラーは、アクセス権の問題が原因と考えられます。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。ファイルのアクセス権を確認します。

716032

エラー メッセージ %ASA-7-716032: Group *name* User *user* Unable to create folder *folder*. Error: *description*

説明 ユーザが CIFS プロトコルを介してフォルダを作成しようとしたときに、問題が発生しました。このエラーは、アクセス権の問題が原因と考えられます。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。ファイルのアクセス権を確認します。

716033

エラー メッセージ %ASA-7-716033: Group *name* User *user* Unable to remove folder *folder*. Error: *description*

説明 CIFS プロトコルのユーザがフォルダを削除しようとしたときに、問題が発生しました。このエラーは、許可の問題またはファイルが常駐するサーバとの通信の問題が原因で発生した可能性があります。

推奨処置 WebVPN デバイスと、CIFS がアクセスするサーバとの間の接続を確認します。デバイスで NetBIOS ネーム サーバ (NBNS) コンフィギュレーションを確認します。

716034

エラー メッセージ %ASA-7-716034: Group *name* User *user* Unable to write to file *filename*.

説明 ユーザが CIFS プロトコルを介してファイルに書き込もうとしたときに、問題が発生しました。このエラーは、許可の問題またはファイルが常駐するサーバとの通信の問題が原因で発生した可能性があります。

推奨処置 不要です。

716035

エラー メッセージ %ASA-7-716035: Group *name* User *user* Unable to read file *filename*.

説明 CIFS プロトコルのユーザがファイルを読み取ろうとしたときに、問題が発生しました。このエラーは、アクセス権の問題が原因と考えられます。

推奨処置 ファイルのアクセス権を確認します。

716036

エラー メッセージ %ASA-7-716036: Group *name* User *user* File Access: User *user* logged into the *server* server.

説明 ユーザが CIFS プロトコルを介してサーバに正常にログインしました。

推奨処置 不要です。

716037

エラー メッセージ %ASA-7-716037: Group *name* User *user* File Access: User *user* failed to login into the *server* server.

説明 ユーザが CIFS プロトコルを介してサーバにログインしようとしたましたが、失敗しました。

推奨処置 ユーザが正しいユーザ名とパスワードを入力したことを確認します。

716038

エラーメッセージ %ASA-6-716038: Authentication: successful, group = *name* user = *user*, Session Type: WebVPN

説明 WebVPN セッションを開始するには、まずユーザがローカルサーバまたはリモートサーバによって正常に認証される必要があります (たとえば、RADIUS または TACACS+)。

推奨処置 不要です。

716039

エラーメッセージ %ASA-6-716039: Authentication: rejected, group = *name* user = *user*, Session Type: WebVPN

説明 WebVPN セッションを開始するには、まずユーザがローカルサーバまたはリモートサーバによって正常に認証される必要があります (たとえば、RADIUS または TACACS+)。この場合、ユーザクレデンシャル (ユーザ名とパスワード) が一致しないか、ユーザに WebVPN セッションを開始する許可がありません。

推奨処置 ローカルサーバまたはリモートサーバでユーザクレデンシャルを確認します。ユーザに対して WebVPN が設定されていることを確認します。

716040

エラーメッセージ %ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.

説明 システムがリブート処理中のため、ユーザが WebVPN にログインできません。

推奨処置 不要です。

716041

エラーメッセージ %ASA-6-716041: access-list *acl_ID* action *url* *url* hit_cnt *count*

説明 *acl_ID* の WebVPN URL アクセス コントロール リストで、位置 *url* に対して *count* 回のヒットがありました。action は「permitted」または「denied」です。

推奨処置 不要です。

716042

エラー メッセージ %ASA-6-716042: access-list *acl_ID* action tcp
source_interface/source_address (source_port) -> dest_interface/dest_address (dest_port) hit-cnt
count

説明 *acl_ID* の WebVPN TCP アクセス コントロール リストで、*dest_interface/dest_address* の宛先 *dest_port* に転送されたソース インターフェイス *source_interface/source_address* のポート *source_port* で受信されたパケットに対して *count* 回のヒットがありました。*action* は「permitted」または「denied」です。

推奨処置 不要です。

717001

エラー メッセージ %PIX|ASA-3-717001: Querying keypair failed.

説明 登録要求中に必要なキーペアが見つかりませんでした。

推奨処置 トラストポイント コンフィギュレーションに有効なキーペアがあることを確認して、登録を再送信します。

717002

エラー メッセージ %PIX|ASA-3-717002: Certificate enrollment failed for trustpoint *trustpoint_name*. Reason: *reason_string*.

説明 この *trustpoint_name* トラストポイントの登録要求が失敗しました。

trustpoint name : 登録要求の対象となるトラストポイント名。

reason_string : 登録要求が失敗した理由。

推奨処置 失敗した理由については、認証局のサーバを確認します。

717003

エラー メッセージ %PIX|ASA-6-717003: Certificate received from Certificate Authority for trustpoint *trustpoint_name*.

説明 この *trustpoint_name* トラストポイントに対して認証局から証明書を正常に受信しました。

推奨処置 なし

717004

エラー メッセージ %PIX|ASA-6-717004: PKCS #12 export failed for trustpoint *trustpoint_name*.

説明 トラストポイント *trustpoint_name* をエクスポートできませんでした。トラストポイントについて CA 証明書だけが存在し、ID 証明書が存在していないか、または必要なキーペアが欠落している可能性があります。

推奨処置 指摘されたトラストポイントに対して必要な証明書とキーペアがあることを確認します。

717005

エラー メッセージ %PIX|ASA-6-717005: PKCS #12 export succeeded for trustpoint *trustpoint_name*.

説明 トラストポイント *trustpoint_name* が正常にエクスポートされました。

推奨処置 なし

717006

エラー メッセージ %PIX|ASA-6-717006: PKCS #12 import failed for trustpoint *trustpoint_name*.

説明 要求されたトラストポイント *trustpoint_name* を処理できませんでした。

推奨処置 インポートしたデータの整合性を確認し、**pkcs12** レコード全体が正しく貼り付けられていることを確認し、インポートの試行を再送信します。

717007

エラー メッセージ %PIX|ASA-6-717007: PKCS #12 import succeeded for trustpoint *trustpoint_name*.

説明 要求したトラストポイント *trustpoint_name* のインポートが正常に完了しました。

推奨処置 不要です。

717008

エラー メッセージ %PIX|ASA-2-717008: Insufficient memory to *process_requiring_memory*.

説明 *process_requiring_memory* のメモリ割り当てを試行中に内部エラーが発生しました。メモリの割り当て中にその他のプロセスで問題が発生し、以降の処理が妨げられる可能性があります。

推奨処置 さらにデバッグするためにメモリ統計およびログを収集し、システムをリロードします。

717009

エラー メッセージ %PIX|ASA-3-717009: Certificate validation failed. Reason: *reason_string*.

説明 *reason_string* のため、証明書の検証が失敗しました。*reason_string* は、失敗の原因を示します。これは、無効になった証明書の検証試行、無効な証明書アトリビュート、またはコンフィギュレーションの問題が原因である可能性があります。

reason_string : 証明書の検証が失敗した理由。

推奨処置 適切なトラストポイントが見つからないことが *reason_string* で示されている場合は、コンフィギュレーションで検証のため有効なトラストポイントが設定されていることを確認します。システムの時刻が認証局の時刻に対して正確であることを確認します。*reason_string* をチェックし、示された問題を訂正します。

717010

エラー メッセージ %PIX|ASA-3-717010: CRL polling failed for trustpoint *trustpoint_name*.

説明 CRL ポーリングが失敗しました。CRL チェックが必要な場合は、これによって接続が拒否される可能性があります。

trustpoint_name : CRL を要求したトラストポイントの名前。

推奨処置 設定された CRL 配布ポイントとの接続を確認し、手動の CRL 検索が正しく機能することを確認します。

717011

エラー メッセージ %PIX|ASA-2-717011: Unexpected event *event event_ID*

説明 このログ メッセージは、通常の条件では予期されないイベントが発生したことを示しています。

推奨処置 問題を記録して Cisco TAC にお知らせください。

717012

エラー メッセージ %PIX|ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint *trustpoint_name* at *time_of_failure*

説明 このログ メッセージは、指摘されたトラストポイント *trustpoint_name* に対するキャッシュされた CRL エントリのリフレッシュが、示された *time_of_failure* で、失敗したことを示しています。これによって、システム上の古い CRL が生じ、有効な CRL を必要とする接続が拒否される可能性があります。

推奨処置 ネットワークのダウンやサーバのダウンなど、サーバへの接続性の問題を確認します。`crypto ca crl retrieve` コマンドを使用して、CRL を手動で取得します。

717013

エラー メッセージ %PIX|ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: *issuer*

説明 デジタル証明書を使用して IPsec トンネルを認証するように装置が設定されている場合は、接続のたびに CRL をダウンロードせずに済むように、Certificate Revocation List (CRL; 証明書失効リスト) がメモリにキャッシュされる可能性があります。キャッシュがいっぱいになって着信 CRL を受け入れられなくなった場合は、必要なスペースが使用可能になるまで古い CRL が削除されていきます。このログ イベントは、パージされる各 CRL に対して生成されます。

推奨処置 不要です。

717014

エラー メッセージ %PIX|ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = *size*, available cache space = *space*)

説明 デジタル証明書を使用して IPsec トンネルを認証するように装置が設定されている場合は、接続のたびに CRL をダウンロードせずに済むように、証明書失効リスト (CRL) がメモリにキャッシュされる可能性があります。このログ イベントは、受信した CRL が長すぎてキャッシュに収まらない場合に生成されます。

推奨処置 処置は不要です。大きい CRL はキャッシュされませんが、引き続きサポートされます。これは、各 IPsec 接続で CRL がダウンロードされることを意味します。IPsec 接続のバースト時にパフォーマンスに影響する可能性があります。

717015

エラー メッセージ %PIX|ASA-3-717015: CRL received from *issuer* is too large to process (CRL size = *crl_size*, maximum CRL size = *max_crl_size*)

説明 このログ イベントは、IPsec 接続によって、許可された最大 CRL サイズ *max_crl_size* よりも大きい CRL がダウンロードされた場合に生成されます。これは、接続の失敗を引き起こすエラー状態です。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

推奨処置 CRL 方式の失効チェックでは、スケーラビリティが最も重大な欠点となる可能性があります。この問題を解決する方法には、認証局のソリューションを調査して CRL のサイズを小さくすること、または CRL 検証を必要としないデバイスを設定することがあります。

717016

エラー メッセージ %PIX|ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: *issuer*

説明 デジタル証明書を使用して IPsec トンネルを認証するように装置が設定されている場合は、接続のたびに CRL をダウンロードせずに済むように、証明書失効リスト (CRL) がメモリにキャッシュされる可能性があります。このログ イベントは、CA が指定した有効期限または設定されたキャッシュ時間が経過し、CRL がキャッシュから削除された場合に生成されます。

推奨処置 処置は不要です。これは、時々発生することがあります。

717017

エラー メッセージ %PIX|ASA-3-717017: Failed to query CA certificate for trustpoint *trustpoint_name* from *enrollment_url*

説明 これは、認証局からの CA 証明書を要求することによってトラストポイントを認証しようとしたときに発生するエラーをログに記録します。

推奨処置 このトラストポイントで登録 URL が設定されていることを確認し、認証局サーバとの接続を確認して、要求を再試行します。

717018

エラー メッセージ %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*)

説明 このログ イベントは、IPSec 接続によって、サポートできるよりも多くの失効エントリを含む CRL がダウンロードされた場合に生成されます。これは、接続の失敗を引き起こすエラー状態です。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

issuer : CRL 発行者の X.500 名。

number_of_entries : 受信した CRL 内の失効エントリの数。

max_allowed : 装置がサポートする CRL エントリの最大数。

推奨処置 CRL 方式の失効チェックでは、スケーラビリティが最も重大な欠点となる可能性があります。この問題を解決する方法には、認証局のソリューションを調査して CRL のサイズを小さくすること、または CRL 検証を必要としないデバイスを設定することがあります。

717019

エラー メッセージ %PIX|ASA-3-717019: Failed to insert CRL for trustpoint *trustpoint_name*. Reason: *failure_reason*.

説明 このログ イベントは、CRL が取得されたが、無効であり、*failure_reason* のためキャッシュに挿入できないときに生成されます。

trustpoint_name : CRL を要求したトラストポイントの名前。

failure_reason : CRL をキャッシュに挿入できなかった理由。

推奨処置 現在のシステム時刻が認証局の時刻に対して正確であることを確認します。NextUpdate フィールドがない場合は、NextUpdate フィールドを無視するようにトラストポイントを設定します。

717021

エラーメッセージ %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.

説明 このメッセージは、シリアル番号で示された証明書を検証しようとして、指摘された理由によってサブジェクト名を検証できない場合に表示されます。シグニチャを使用して証明書データを検証すると、ログに記録されるいくつかのエラーが発生する可能性があります。これには、特定の無効なキー タイプやサポートされないキー サイズが含まれます。

reason_string : 証明書を検証できなかった理由。

serial number : 検証中の証明書のシリアル番号。

subject name : 検証中の証明書に含まれるサブジェクト名。

key length : この証明書に署名するために使用されるキー内のビット数。

推奨処置 指摘された証明書を調べて、有効であること、有効なキー タイプが含まれていること、サポートされる最大キー サイズを超過していないことを確認します。

717022

エラーメッセージ %PIX|ASA-6-717022 Certificate was successfully validated.
certificate identifiers

説明 このメッセージは、示された証明書が正常に検証された場合に表示されます。

certificate identifiers : 正常に検証された証明書を識別する情報。これには、理由、シリアル番号、サブジェクト名などが含まれます。

推奨処置 処置は不要です。

717023

エラーメッセージ %PIX|ASA-3-717023 SSL failed to set device certificate for
trustpoint *trustpoint name*. Reason: *reason_string*.

説明 このメッセージは、SSL 接続の認証のため所定のトラストポイントでデバイス証明書を設定しようとして失敗した場合に表示されます。SSL 接続を確立する際、使用するデバイス証明書を設定しようとします。このプロセス中に発生した障害はログに記録されます。メッセージには、デバイス証明書のロードに使用すべき設定済みのトラストポイントと失敗の理由が含まれます。

trustpoint name : SSL がデバイス証明書を設定できなかったトラストポイントの名前。

reason_string : デバイス証明書を設定できなかった理由。

推奨処置 失敗について報告された理由で示された問題を解決します。

- 指摘されたトラストポイントが登録されており、デバイス証明書を持っていることを確認します。
- デバイス証明書が有効であることを確認します。
- 必要な場合は、トラストポイントを再登録します。

717024

エラー メッセージ %PIX|ASA-7-717024 Checking CRL from trustpoint: *trustpoint name* for *purpose*

説明 このログメッセージは、CRL が取得されていることを示しています。

trustpoint name : CRL が取得されているトラストポイントの名前。

purpose : CRL が取得されている理由。

推奨処置 不要です。

717025

エラー メッセージ %PIX|ASA-7-717025 Validating certificate chain containing *number of certs* certificate(s).

説明 このメッセージは、証明書のチェーンが検証されているときに表示されます。

number of certs : チェーン内の証明書の数。

推奨処置 不要です。

717026

エラー メッセージ %PIX|ASA-4-717026 Name lookup failed for hostname *hostname* during PKI operation.

説明 このメッセージは、PKI オペレーションの試行中に所定のホスト名を解決できないときに表示されます。

hostname : 解決できなかったホスト名。

推奨処置 所定のホスト名のコンフィギュレーションおよび DNS サーバ エントリを調べて、解決できることを確認します。それから、オペレーションを再試行します。

717027

エラー メッセージ %PIX|ASA-3-717027 Certificate chain failed validation. *reason_string*.

説明 このメッセージは、証明書のチェーンを検証できなかった場合に表示されます。失敗の原因を正確に示すため理由が表示されます。

reason_string : 証明書チェーンを検証できなかった理由。

推奨処置 理由に示された問題を解決し、次の処置のいずれかを実行して検証を再試行します。

- CRL チェックが必要な場合は CA への接続を確認します。
- トラストポイントが認証されており、検証に使用できることを確認します。
- チェーン内の ID 証明書が有効日に基づいて有効であることを確認します。
- 証明書が失効していないことを確認します。

717028

エラー メッセージ %PIX|ASA-6-717028 Certificate chain was successfully validated *additional info*.

説明 このメッセージは、証明書のチェーンが正常に検証された場合に表示されます。

additional info: CRL チェックが実行されなかったことを示す「with warning」など、証明書チェーンがどのように検証されたかを示す追加情報が表示されます。

推奨処置 処置は不要です。

717029

エラー メッセージ %PIX|ASA-7-717029 Identified client certificate within certificate chain. serial number: *serial_number*, subject name: *subject_name*.

説明 このメッセージは、証明書がクライアント証明書であることを示しています。

serial_number: クライアント証明書として識別される証明書のシリアル番号。

subject_name: クライアント証明書として識別される証明書に含まれるサブジェクト名。

推奨処置 処置は不要です。

717030

エラー メッセージ %PIX|ASA-7-717030 Found a suitable trustpoint *trustpoint name* to validate certificate.

説明 このメッセージは、証明書の検証に使用できる適切または使用可能なトラストポイントが見つかったときに表示されます。

trustpoint name: 証明書の検証に使用されるトラストポイント。

推奨処置 処置は不要です。

717031

エラー メッセージ %PIX|ASA-4-717031 Failed to find a suitable trustpoint for the issuer: *issuer* Reason: *reason_string*

説明 このメッセージは、使用可能なトラストポイントが見つからなかったときに表示されます。このメッセージは、適切なトラストポイントが見つからなかった証明書の発行者を示し、失敗の理由を示します。証明書の検証中は、証明書を検証するために適切なトラストポイントが使用可能になっている必要があります。

issuer: 検証されていた証明書の発行者。

reason_string: 適切なトラストポイントが見つからなかった理由。

推奨処置 コンフィギュレーションを調べてトラストポイントが設定、認証、および登録されていることを確認し、理由に示された問題を解決します。また、コンフィギュレーションが、発行された ID 証明書など、特定のタイプの証明書を許可していることを確認します。

718001

エラー メッセージ %PIX|ASA-7-718001: Internal interprocess communication queue send failure: code *error_code*

説明 VPNLB キューでメッセージをキューに入れようとしたときに、内部ソフトウェア エラーが発生しました。

推奨処置 通常、これは問題のない状態です。しかし、問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718002

エラー メッセージ %PIX|ASA-5-718002: Create peer *IP_address* failure, already at maximum of *number_of_peers*

説明 ロードバランシング ピアの最大数を超過しました。新規ピアは無視されます。

推奨処置 ロードバランシングとネットワーク コンフィギュレーションを調べて、LB ピアの数、許可された最大値を超過していないことを確認します。

718003

エラー メッセージ %PIX|ASA-6-718003: Got unknown peer message *message_number* from *IP_address*, local version *version_number*, remote version *version_number*

説明 LB ピアのいずれかから、認識されないロードバランシング メッセージが受信されました。これは、ピア間のバージョンの不一致を示している可能性があります。内部ソフトウェア エラーが原因となっていると思われます。

推奨処置 すべての LB ピアに互換性があることを確認します。互換性があるがこの状態が続く場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718004

エラー メッセージ %PIX|ASA-6-718004: Got unknown internal message *message_number*

説明 未知の内部メッセージを受信しました。通常、これは、内部ソフトウェア エラーがあることを示しています。

推奨処置 通常、これは問題のない状態です。しかし、問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718005

エラー メッセージ %PIX|ASA-5-718005: Fail to send to *IP_address*, port *port*

説明 ロードバランシング ソケットでパケットを送信しようとしたときに、内部ソフトウェア エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通過していることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718006

エラー メッセージ %PIX|ASA-5-718006: Invalid load balancing state transition
[*cur=state_number*] [*event=event_number*]

説明 ステート マシンエラーが発生しました。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 通常、これは問題のない状態です。しかし、問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718007

エラー メッセージ %PIX|ASA-5-718007: Socket open failure *failure_code*

説明 ロードバランシング ソケットを開こうとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通過していることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718008

エラー メッセージ %PIX|ASA-5-718008: Socket bind failure *failure_code*

説明 ロードバランシング ソケットにバインドしようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性を示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通過していることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718009

エラー メッセージ %PIX|ASA-5-718009: Send HELLO response failure to *IP_address*

説明 Hello Response メッセージを LB ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性を示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通過していることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718010

エラー メッセージ %PIX|ASA-5-718010: Sent HELLO response to *IP_address*

説明 セキュリティ アプライアンスによって、Hello Response メッセージが LB ピアに送信されました。

推奨処置 情報のみです。

718011

エラー メッセージ %PIX|ASA-5-718011: Send HELLO request failure to *IP_address*

説明 Hello Request メッセージを LB ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性を示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通過していることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718012

エラー メッセージ %PIX|ASA-5-718012: Sent HELLO request to *IP_address*

説明 セキュリティ アプライアンスが、Hello Request メッセージを LB ピアへ送信しました。

推奨処置 情報のみです。

718013

エラー メッセージ %PIX|ASA-6-718013: Peer *IP_address* is not answering HELLO

説明 LB ピアが HELLO に応答していません。

推奨処置 LBSSF ピアの状態とネットワーク接続を確認します。

718014

エラー メッセージ %PIX|ASA-5-718014: Master peer *IP_address* is not answering HELLO

説明 LB マスター ピアが HELLO に応答していません。

推奨処置 LBSSF マスター ピアの状態とネットワーク接続を確認します。

718015

エラー メッセージ %PIX|ASA-5-718015: Received HELLO request from *IP_address*

説明 セキュリティ アプライアンスが、Hello Request メッセージを LB ピアから受信しました。

推奨処置 情報のみです。

718016

エラー メッセージ %PIX|ASA-5-718016: Received HELLO response from *IP_address*

説明 セキュリティ アプライアンスが、Hello Response パケットを LB ピアから受信しました。

推奨処置 情報のみです。

718017

エラー メッセージ %PIX|ASA-7-718017: Got timeout for unknown peer *IP_address* msg
type *message_type*

説明 セキュリティ アプライアンスが未知のピアのタイムアウトを処理しました。ピアはすでにアクティブリストから削除されている可能性があるため、メッセージは無視されました。

推奨処置 メッセージが解決しない場合、または望ましくない動作が引き起こされる場合は、LB ピアを調べて、設定がすべて正しいことを確認します。

718018

エラー メッセージ %PIX|ASA-7-718018: Send KEEPALIVE request failure to *IP_address*

説明 Keepalive Request メッセージを LB ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通過していることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718019

エラー メッセージ %PIX|ASA-7-718019: Sent KEEPALIVE request to *IP_address*

説明 セキュリティ アプライアンスが、Keepalive Request メッセージを LB ピアへ送信しました。

推奨処置 情報のみです。

718020

エラー メッセージ %PIX|ASA-7-718020: Send KEEPALIVE response failure to *IP_address*

説明 Keepalive Response メッセージを LB ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通過していることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718021

エラー メッセージ %PIX|ASA-7-718021: Sent KEEPALIVE response to *IP_address*

説明 セキュリティ アプライアンスによって、Keepalive Response メッセージが LB ピアに送信されました。

推奨処置 情報のみです。

718022

エラー メッセージ %PIX|ASA-7-718022: Received KEEPALIVE request from *IP_address*

説明 セキュリティ アプライアンスが、Keepalive Request メッセージを LB ピアから受信しました。

推奨処置 情報のみです。

718023

エラー メッセージ %PIX|ASA-7-718023: Received KEEPALIVE response from *IP_address*

説明 セキュリティ アプライアンスが、Keepalive Response メッセージを LB ピアから受信しました。

推奨処置 情報のみです。

718024

エラー メッセージ %PIX|ASA-5-718024: Send CFG UPDATE failure to *IP_address*

説明 Configuration Update メッセージを LB ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通してしていることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718025

エラー メッセージ %PIX|ASA-7-718025: Sent CFG UPDATE to *IP_address*

説明 セキュリティ アプライアンスが、Configuration Update メッセージを LB ピアへ送信しました。

推奨処置 情報のみです。

718026

エラー メッセージ %PIX|ASA-7-718026: Received CFG UPDATE from *IP_address*

説明 セキュリティ アプライアンスが、Configuration Update メッセージを LB ピアから受信しました。

推奨処置 情報のみです。

718027

エラー メッセージ %PIX|ASA-6-718027: Received unexpected KEEPALIVE request from *IP_address*

説明 情報メッセージ。

推奨処置 問題が解決しない場合、または望ましくない動作が引き起こされる場合は、すべての LB ピアが正しく設定され、検出されていることを確認します。

718028

エラー メッセージ %PIX|ASA-5-718028: Send OOS indicator failure to *IP_address*

説明 OOS Indicator メッセージを LB ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通じていることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718029

エラー メッセージ %PIX|ASA-7-718029: Sent OOS indicator to *IP_address*

説明 セキュリティ アプライアンスが、OOS Indicator メッセージを LB ピアへ送信しました。

推奨処置 情報のみです。

718030

エラー メッセージ %PIX|ASA-6-718030: Received planned OOS from *IP_address*

説明 セキュリティ アプライアンスが、計画的な OOS メッセージを LB ピアから受信しました。

推奨処置 情報のみです。

718031

エラー メッセージ %PIX|ASA-5-718031: Received OOS obituary for *IP_address*

説明 セキュリティ アプライアンスが、OOS Obituary を LB ピアから受信しました。

推奨処置 情報のみです。

718032

エラー メッセージ %PIX|ASA-5-718032: Received OOS indicator from *IP_address*

説明 セキュリティ アプライアンスが、OOS Indicator を LB ピアから受信しました。

推奨処置 情報のみです。

718033

エラー メッセージ %PIX|ASA-5-718033: Send TOPOLOGY indicator failure to *IP_address*

説明 Topology Indicator メッセージを LB ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 セキュリティ アプライアンスでネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブでプロトコル データがデバイスを通じていることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718034

エラー メッセージ %PIX|ASA-7-718034: Sent TOPOLOGY indicator to *IP_address*

説明 セキュリティ アプライアンスが、Topology Indicator メッセージを LB ピアへ送信しました。

推奨処置 情報のみです。

718035

エラー メッセージ %PIX|ASA-7-718035: Received TOPOLOGY indicator from *IP_address*

説明 セキュリティ アプライアンスが、Topology Indicator メッセージを LB ピアから受信しました。

推奨処置 情報のみです。

718036

エラー メッセージ %PIX|ASA-7-718036: Process timeout for req-type *type_value*, exid *exchange_ID*, peer *IP_address*

説明 セキュリティ アプライアンスがピアのタイムアウトを処理しました。

推奨処置 ピアがタイムアウトされたことを確認します。タイムアウトされていない場合は、ピア LB コンフィギュレーションをチェックし、ピアとセキュリティ アプライアンスとの間のネットワーク接続を確認します。

718037

エラー メッセージ %PIX|ASA-6-718037: Master processed *number_of_timeouts* timeouts

説明 マスター役割のセキュリティ アプライアンスが、指摘された数のピア タイムアウトを処理しました。

推奨処置 タイムアウトが正しいことを確認します。正しくない場合は、ピア LB コンフィギュレーションをチェックし、ピアとセキュリティ アプライアンスとの間のネットワーク接続を確認します。

718038

エラー メッセージ %PIX|ASA-6-718038: Slave processed *number_of_timeouts* timeouts

説明 スレーブ役割のセキュリティ アプライアンスが、指摘された数のピア タイムアウトを処理しました。

推奨処置 タイムアウトが正しいことを確認します。正しくない場合は、ピア LB コンフィギュレーションをチェックし、ピアとセキュリティ アプライアンスとの間のネットワーク接続を確認します。

718039

エラー メッセージ %PIX|ASA-6-718039: Process dead peer *IP_address*

説明 セキュリティ アプライアンスがデッド ピアを検出しました。

推奨処置 デッド ピアの検出が正当であることを確認します。正当でない場合は、ピア LB コンフィギュレーションをチェックし、ピアとセキュリティ アプライアンスとの間のネットワーク接続を確認します。

718040

エラー メッセージ %PIX|ASA-6-718040: Timed-out exchange ID *exchange_ID* not found

説明 セキュリティ アプライアンスがデッド ピアを検出しましたが、交換 ID が認識されませんでした。

推奨処置 情報のみです。

718041

エラー メッセージ %PIX|ASA-7-718041: Timeout [msgType=*type*] processed with no callback

説明 セキュリティ アプライアンスがデッド ピアを検出しましたが、処理でコールバックが使用されませんでした。

推奨処置 情報のみです。

718042

エラー メッセージ %PIX|ASA-5-718042: Unable to ARP for *IP_address*

説明 ピアにコンタクトしようとしたときに、セキュリティ アプライアンスで ARP 障害が発生しました。

推奨処置 ネットワークが動作していることと、すべてのピアが互いに通信できることを確認します。

718043

エラー メッセージ %PIX|ASA-5-718043: Updating/removing duplicate peer entry *IP_address*

説明 セキュリティ アプライアンスが重複するピア エントリを検出し、削除しています。

推奨処置 情報のみです。

718044

エラー メッセージ %PIX|ASA-5-718044: Deleted peer *IP_address*

説明 セキュリティ アプライアンスが LB ピアを削除しています。

推奨処置 情報のみです。

718045

エラー メッセージ %PIX|ASA-5-718045: Created peer *IP_address*

説明 セキュリティ アプライアンスが LB ピアを検出しました。

推奨処置 情報のみです。

718046

エラー メッセージ %PIX|ASA-7-718046: Create group policy *policy_name*

説明 安全に LB ピアに通信するため、セキュリティ アプライアンスがグループ ポリシーを作成しました。

推奨処置 情報のみです。

718047

エラー メッセージ %PIX|ASA-7-718047: Fail to create group policy *policy_name*

説明 LB ピア間の通信をセキュリティで保護するためにグループ ポリシーを作成しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 LB コンフィギュレーションが正しいことを確認します。

718048

エラー メッセージ %PIX|ASA-5-718048: Create of secure tunnel failure for peer *IP_address*

説明 LB ピアへの IPSec トンネルを確立しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 LB コンフィギュレーションが正しく、ネットワークが動作していることを確認します。

718049

エラー メッセージ %PIX|ASA-7-718049: Created secure tunnel to peer *IP_address*

説明 セキュリティ アプライアンスが LB ピアへの IPSec トンネルを正常に確立しました。

推奨処置 情報のみです。

718050

エラー メッセージ %PIX|ASA-5-718050: Delete of secure tunnel failure for peer *IP_address*

説明 LB ピアへの IPSec トンネルを終了しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 LB コンフィギュレーションが正しく、ネットワークが動作していることを確認します。

718051

エラー メッセージ %PIX|ASA-6-718051: Deleted secure tunnel to peer *IP_address*

説明 セキュリティ アプライアンスが LB ピアへの IPSec トンネルを正常に終了しました。

推奨処置 情報のみです。

718052

エラー メッセージ %PIX|ASA-5-718052: Received GRAT-ARP from duplicate master *MAC_address*

説明 セキュリティ アプライアンスが重複マスターから Gratuitous ARP を受信しました。

推奨処置 LB コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718053

エラー メッセージ %PIX|ASA-5-718053: Detected duplicate master, mastership stolen *MAC_address*

説明 セキュリティ アプライアンスが重複マスター、盗まれたマスターシップを検出しました。

推奨処置 LB コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718054

エラー メッセージ %PIX|ASA-5-718054: Detected duplicate master *MAC_address* and going to SLAVE

説明 セキュリティ アプライアンスが重複マスターを検出し、スレーブ モードに切り換えています。

推奨処置 LB コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718055

エラー メッセージ %PIX|ASA-5-718055: Detected duplicate master *MAC_address* and staying MASTER

説明 セキュリティ アプライアンスが重複マスターを検出し、スレーブ モードにとどまっています。

推奨処置 LB コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718056

エラー メッセージ %PIX|ASA-7-718056: Deleted Master peer, IP *IP_address*

説明 セキュリティ アプライアンスが内部テーブルから LB マスターを削除しました。

推奨処置 情報のみです。

718057

エラー メッセージ %PIX|ASA-5-718057: Queue send failure from ISR, msg type *failure_code*

説明 VPNLB キューで Interrupt Service Routing からメッセージをキューに入れているときに、内部ソフトウェア エラーが発生しました。

推奨処置 通常、これは問題のない状態です。しかし、問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718058

エラー メッセージ %PIX|ASA-7-718058: State machine return code: *action_routine*, *return_code*

説明 このイベントは、LB 有限状態マシンに属するアクション ルーチンの戻りコードをトレースします。

推奨処置 情報のみです。

718059

エラー メッセージ %PIX|ASA-7-718059: State machine function trace: *state=state_name*, *event=event_name*, *func=action_routine*

説明 このイベントは、LB 有限状態マシンのイベントと状態をトレースします。

推奨処置 情報のみです。

718060

エラー メッセージ %PIX|ASA-5-718060: Inbound socket select fail: *context=context_ID*.

説明 ソケット選択コールがエラーを戻し、ソケットを読み取ることができませんでした。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718061

エラーメッセージ %PIX|ASA-5-718061: Inbound socket read fail: context=*context_ID*.

説明 選択コールでデータが検出された後、ソケット読み取りが失敗しました。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718062

エラーメッセージ %PIX|ASA-5-718062: Inbound thread is awake (context=*context_ID*).

説明 これは、LB プロセスが起動され、処理を開始するたびに表示されます。

推奨処置 情報のみです。

718063

エラーメッセージ %PIX|ASA-5-718063: Interface *interface_name* is down.

説明 これは、インターフェイスがダウンしていることが LB プロセスによって検出されたことを示しています。

推奨処置 インターフェイス コンフィギュレーションを調べて、インターフェイスが動作していることを確認します。

718064

エラーメッセージ %PIX|ASA-5-718064: Admin. interface *interface_name* is down.

説明 これは、管理インターフェイスがダウンしていることが LB プロセスによって検出されたことを示しています。

推奨処置 管理インターフェイス コンフィギュレーションを調べて、インターフェイスが動作していることを確認します。

718065

エラーメッセージ %PIX|ASA-5-718065: Cannot continue to run (public=*up/down*, private=*up/down*, enable=*LB_state*, master=*IP_address*, session=*Enable/Disable*).

説明 これは、すべての前提条件が満たされていないため、LB プロセスを実行できないことを示しています。前提条件は、2つのアクティブなインターフェイスと LB がイネーブルになっていることです。

推奨処置 インターフェイス コンフィギュレーションを調べて、少なくとも2つのインターフェイスが動作していることを確認します。また、LB コンフィギュレーションも確認します。

718066

エラー メッセージ %PIX|ASA-5-718066: Cannot add secondary address to interface *interface_name*, ip *IP_address*.

説明 LB には、外部インターフェイスに追加するセカンダリ アドレスが必要です。このイベントは、セカンダリ アドレスを追加する際に障害が発生したことを示しています。

推奨処置 セカンダリ アドレスとして使用されているアドレスを調べ、それが有効で固有であることを確認します。外部インターフェイスのコンフィギュレーションを確認します。

718067

エラー メッセージ %PIX|ASA-5-718067: Cannot delete secondary address to interface *interface_name*, ip *IP_address*.

説明 セカンダリ アドレスの削除が失敗しました。これは、アドレッシングの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨処置 外部インターフェイスのアドレッシング情報を調べて、セカンダリ アドレスが有効で固有であることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718068

エラー メッセージ %PIX|ASA-5-718068: Start VPN Load Balancing in context *context_ID*.

説明 LB プロセスが開始され、初期化されました。

推奨処置 情報のみです。

718069

エラー メッセージ %PIX|ASA-5-718069: Stop VPN Load Balancing in context *context_ID*.

説明 LB プロセスが停止されました。

推奨処置 情報のみです。

718070

エラー メッセージ %PIX|ASA-5-718070: Reset VPN Load Balancing in context *context_ID*.

説明 LB プロセスがリセットされました。

推奨処置 情報のみです。

718071

エラーメッセージ %PIX|ASA-5-718071: Terminate VPN Load Balancing in context *context_ID*.

説明 LB プロセスが終了されました。

推奨処置 情報のみです。

718072

エラーメッセージ %PIX|ASA-5-718072: Becoming master of Load Balancing in context *context_ID*.

説明 セキュリティ アプライアンスが LB マスターになりました。

推奨処置 情報のみです。

718073

エラーメッセージ %PIX|ASA-5-718073: Becoming slave of Load Balancing in context *context_ID*.

説明 セキュリティ アプライアンスが LB スレーブになりました。

推奨処置 情報のみです。

718074

エラーメッセージ %PIX|ASA-5-718074: Fail to create access list for peer *context_ID*.

説明 ACL は、LB ピアが通信できるセキュア トンネルを作成するために使用されます。これらの ACL のいずれかを作成するためにセキュリティ アプライアンスを使用できませんでした。これは、アドレッシングの問題または内部ソフトウェアの問題が存在する可能性があることを示しています。

推奨処置 すべてのピアで内部インターフェイスのアドレッシング情報を調べ、すべてのピアが正しく検出されていることを確認します。問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラーメッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718075

エラーメッセージ %PIX|ASA-5-718075: Peer *IP_address* access list not set.

説明 セキュア トンネルを削除する際、セキュリティ アプライアンスが、関連する ACL を持たないピア エントリを検出しました。

推奨処置 情報のみです。

718076

エラー メッセージ %PIX|ASA-5-718076: Fail to create tunnel group for peer *IP_address*.

説明 LB ピア間の通信をセキュリティで保護するためにトンネルグループを作成しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 LB コンフィギュレーションが正しいことを確認します。

718077

エラー メッセージ %PIX|ASA-5-718077: Fail to delete tunnel group for peer *IP_address*.

説明 LB ピア間の通信をセキュリティで保護するためにトンネルグループを削除しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 情報のみです。

718078

エラー メッセージ %PIX|ASA-5-718078: Fail to create crypto map for peer *IP_address*.

説明 LB ピア間の通信をセキュリティで保護するために暗号マップを作成しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 LB コンフィギュレーションが正しいことを確認します。

718079

エラー メッセージ %PIX|ASA-5-718079: Fail to delete crypto map for peer *IP_address*.

説明 LB ピア間の通信をセキュリティで保護するために暗号マップを削除しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 情報のみです。

718080

エラーメッセージ %PIX|ASA-5-718080: Fail to create crypto policy for peer *IP_address*.

説明 LB ピア間の通信をセキュリティで保護するために使用するトランスフォーム セットを作成しようとしたときに、セキュリティ アプライアンスで障害が発生しました。これは、内部ソフトウェアの問題が存在する可能性があることを示しています。

推奨処置 問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718081

エラーメッセージ %PIX|ASA-5-718081: Fail to delete crypto policy for peer *IP_address*.

説明 LB ピア間の通信をセキュリティで保護するために使用するトランスフォーム セットを削除しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 情報のみです。

718084

エラーメッセージ %PIX|ASA-5-718084: Public/cluster IP not on the same subnet: public *IP_address*, mask *netmask*, cluster *IP_address*

説明 クラスタ IP アドレスは、セキュリティ アプライアンスの外部インターフェイスと同じサブネット上にある必要があります。これは、同じネットワーク上にないことも示しています。

推奨処置 クラスタ (または仮想) IP アドレスと外部インターフェイス アドレスの両方が同じネットワーク上にあることを確認します。

718085

エラーメッセージ %PIX|ASA-5-718085: Interface *interface_name* has no IP address defined.

説明 示されたインターフェイスで IP アドレスが設定されていません。

推奨処置 インターフェイスの IP アドレスを設定します。

718086

エラー メッセージ %PIX|ASA-5-718086: Fail to install LB NP rules: type *rule_type*, dst *interface_name*, port *port*.

説明 LB ピア間の通信をセキュリティで保護するために使用する SoftNP ACL ルールを作成しようとしたときに、セキュリティ アプライアンスで障害が発生しました。これは、内部ソフトウェアの問題が存在する可能性があることを示しています。

推奨処置 問題が解決しない場合、または望ましくない動作が引き起こされる場合は、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco Technical Assistance Center (TAC) にサポートを依頼して収集した情報をご提供ください。

718087

エラー メッセージ %PIX|ASA-5-718087: Fail to delete LB NP rules: type *rule_type*, rule *rule_ID*.

説明 LB ピア間の通信をセキュリティで保護するために使用する SoftNP ACL ルールを削除しようとしたときに、セキュリティ アプライアンスで障害が発生しました。

推奨処置 情報のみです。

718088

エラー メッセージ %PIX|ASA-7-718088: Possible VPN LB misconfiguration. Offending device MAC *MAC_address*.

説明 重複するマスターの存在は、LB ピアのいずれかの設定が誤っている可能性を示しています。

推奨処置 すべてのピアの LB コンフィギュレーションを調べ、特定されたピアに特に注意します。

719001

エラー メッセージ %ASA-6-719001: Email Proxy session could not be established: session limit of *maximum_sessions* has been reached.

説明 このメッセージは、最大セッション制限に達したため着信電子メール プロキシ セッションを確立できなかったときに表示されます。*maximum_sessions* は、最大セッション数です。

推奨処置 不要です。

719002

エラー メッセージ %ASA-3-719002: Email Proxy session *pointer* from *source_address* has been terminated due to *reason* error.

説明 このメッセージは、エラーのためセッションが終了したときに表示されます。考えられるエラーは、セッション データベースへのセッションの追加の失敗、メモリ割り当ての失敗、チャネルへのデータ書き込みの失敗などです。*pointer* はセッション構造のポインタ、*source_address* は電子メール プロキシ クライアントの IP アドレス、*reason* はエラー タイプです。

推奨処置 不要です。

719003

エラー メッセージ %ASA-6-719003: Email Proxy session *pointer* resources have been freed for *source_address*.

説明 このメッセージは、動的に割り当てられたセッション構造が解放され、セッションの終了後に NULL に設定された場合に表示されます。*pointer* はセッション構造のポインタ、*source_address* は電子メール プロキシ クライアントの IP アドレスです。

推奨処置 不要です。

719004

エラー メッセージ %ASA-6-719004: Email Proxy session *pointer* has been successfully established for *source_address*.

説明 新規着信電子メール クライアント セッションが確立されました。

推奨処置 不要です。

719005

エラー メッセージ %ASA-7-719005: FSM *NAME* has been created using *protocol* for session *pointer* from *source_address*.

説明 このメッセージは、新規着信セッションに対して FSM が作成されたときに表示されます。*NAME* はセッションの FSM インスタンス名、*protocol* は電子メール プロトコル タイプ (たとえば、POP3、IMAP、SMTP) *pointer* はセッション構造のポインタ、*source_address* は電子メール プロキシ クライアントの IP アドレスです。

推奨処置 不要です。

719006

エラー メッセージ %ASA-7-719006: Email Proxy session *pointer* has timed out for *source_address* because of network congestion.

説明 このメッセージは、ネットワークの輻輳が発生し、データを電子メール クライアントまたは電子メール サーバに送信できないときに表示されます。これによって、ブロック タイマーが開始されます。ブロック タイマーがタイムアウトになると、セッションの有効期限が切れま
す。*pointer* はセッション構造のポインタで、*source_address* は電子メール プロキシ クライアントの IP アドレスです。

推奨処置 数分後にオペレーションを再試行します。

719007

エラー メッセージ %ASA-7-719007: Email Proxy session *pointer* cannot be found for *source_address*.

説明 このメッセージは、セッション データベース内で一致するセッションが見つからないときに表示されます。セッション ポインタが不良です。*pointer* はセッション構造のポインタで、*source_address* は電子メール プロキシ クライアントの IP アドレスです。

推奨処置 不要です。

719008

エラー メッセージ %ASA-3-719008: Email Proxy service is shutting down.

説明 このメッセージは、電子メール プロキシがディセーブルの場合に表示されます。すべてのリソースがクリーンアップされ、すべてのスレッドが終了されます。

推奨処置 不要です。

719009

エラー メッセージ %ASA-7-719009: Email Proxy service is starting.

説明 このメッセージは、電子メール プロキシがイネーブルの場合に表示されます。

推奨処置 不要です。

719010

エラー メッセージ %ASA-6-719010: *protocol* Email Proxy feature is disabled on interface *interface_name*.

説明 このメッセージは、電子メール プロキシ機能が CLI から呼び出され、特定のエントリ ポイントでディセーブルになったときに表示されます。これは、ユーザのメイン「オフ」スイッチです。すべてのインターフェイスですべてのプロトコルがオフになると、メインのシャットダウンルーチンが呼び出され、グローバル リソースやスレッドなどがクリーンアップされます。*protocol* は電子メール プロトコル タイプ(たとえば、POP3、IMAP、SMTP)で、*interface_name* はセキュリティ アプライアンス インターフェイス名です。

推奨処置 不要です。

719011

エラー メッセージ %ASA-6-719011: *Protocol* Email Proxy feature is enabled on interface *interface_name*.

説明 このメッセージは、電子メール プロキシ機能が CLI から呼び出され、特定のエントリ ポイントでイネーブルになったときに表示されます。これは、ユーザのメイン「オン」スイッチです。初めて使用される場合は、グローバル リソースやスレッドを割り当てるため、メインの起動ルーチンが呼び出されます。後続のコールでは、特定のプロトコル用のリスン スレッドだけが起動されます。*protocol* は電子メール プロキシ プロトコル タイプ(たとえば、POP3、IMAP、SMTP)で、*interface_name* はセキュリティ アプライアンス インターフェイス名です。

推奨処置 不要です。

719012

エラー メッセージ %ASA-6-719012: Email Proxy server listening on port *port* for mail protocol *protocol*.

説明 このメッセージは、設定されたポート上の特定のプロトコルに対してリスン チャンネルが開かれ、それが TCP 選択グループに追加されたときに表示されます。*port* は設定されたポート番号で、*protocol* は電子メール プロキシのプロトコル タイプ(たとえば、POP3、IMAP、SMTP)です。

推奨処置 不要です。

719013

エラー メッセージ %ASA-6-719013: Email Proxy server closing port *port* for mail protocol *protocol*.

説明 このメッセージは、設定されたポート上の特定のプロトコルに対してリスン チャンネルが閉じられ、それが TCP 選択グループから削除されたときに表示されます。*port* は設定されたポート番号で、*protocol* は電子メール プロキシのプロトコル タイプ(たとえば、POP3、IMAP、SMTP)です。

推奨処置 不要です。

719014

エラー メッセージ %ASA-5-719014: Email Proxy is changing listen port from *old_port* to *new_port* for mail protocol *protocol*.

説明 このメッセージは、指摘されたプロトコルのリスン ポートで変更がシグナリングされたときに表示されます。そのポートに対してイネーブルなすべてのインターフェイスでリスン チャネルが閉じられ、新規ポートでリスンが再開されます。これは、CLI から呼び出されます。*old_port* は設定された古いポート番号で、*new_port* は新しく設定されたポート番号です。*protocol* は電子メール プロトコル タイプ (たとえば、POP3、IMAP、SMTP) です。

推奨処置 不要です。

719015

エラー メッセージ %ASA-7-719015: Parsed emailproxy session *pointer* from *source_address* username: mailuser = *mail_user*, vpnuser = *VPN_user*, mailserver = *server*

説明 このメッセージは、ユーザ名ストリングが *vpnuser* (名前デリミタ) *mailuser* (サーバデリミタ) *mailserver* の形式でクライアントから受信されたときに表示されます (たとえば、xxx:yyy@cisco.com)。名前デリミタはオプションです。デリミタがない場合は、VPN ユーザ名とメールユーザ名が同じです。サーバ デリミタはオプションです。存在しない場合、これはデフォルト設定のメール サーバが使用されることを意味します。*pointer* はセッション構造のポインタで、*source_address* は電子メール プロキシ クライアントの IP アドレスです。*mail_user* は電子メール アカウント ユーザ名で、*VPN_user* は WebVPN ユーザ名です。*server* は電子メール サーバです。

推奨処置 不要です。

719016

エラー メッセージ %ASA-7-719016: Parsed emailproxy session *pointer* from *source_address* password: mailpass = *****, vpnpass= *****

説明 このメッセージは、パスワードストリングが *vpnpass* (名前デリミタ) *mailpassr* の形式でクライアントから受信されたときに表示されます (たとえば、xxx:yyy)。名前デリミタはオプションです。デリミタがない場合は、VPN パスワードとメール パスワードが同じです。*pointer* はセッション構造のポインタで、*source_address* は電子メール プロキシ クライアントの IP アドレスです。

推奨処置 不要です。

719017

エラー メッセージ %ASA-6-719017: WebVPN user: *vpnuser* invalid dynamic ACL.

説明 このメッセージは、アクセス コントロール リストがこのユーザを解析できなかったため、WebVPN セッションが中断されたときに表示されます。ACL は、どのようなユーザ制限が電子メール アカウントのアクセスにかけられているのかを判別します。ACL は AAA サーバからダウンロードされます。このエラーのため、ログインの続行は安全ではありません。*vpnuser* は WebVPN ユーザ名です。

推奨処置 AAA サーバを調べて、このユーザの動的 ACL を修正します。

719018

エラー メッセージ %ASA-6-719018: WebVPN user: *vpnuser* ACL ID *acl_ID* not found

説明 このメッセージは、ローカルで保持されている ACL リストでアクセス コントロール リストが見つからなかったときに表示されます。ACL は、どのようなユーザ制限が電子メール アカウントのアクセスにかけられているのかを判別します。ACL はローカルで設定されます。このエラーのため、続行は認可されません。*vpnuser* は WebVPN ユーザ名で、*acl_ID* はローカルで設定された ACL 識別ストリングです。

推奨処置 ローカル ACL コンフィギュレーションを確認します。

719019

エラー メッセージ %ASA-6-719019: WebVPN user: *vpnuser* authorization failed.

説明 このメッセージは、ACL によって、電子メール アカウントのアクセスにどのようなユーザ制限があるかが判定された場合に表示されます。認可チェックの失敗のため、ユーザが電子メール アカウントにアクセスできません。*vpnuser* は WebVPN ユーザ名です。

推奨処置 なし

719020

エラー メッセージ %ASA-6-719020: WebVPN user *vpnuser* authorization completed successfully.

説明 このメッセージは、ACL によって、電子メール アカウントのアクセスにどのようなユーザ制限があるかが判定された場合に表示されます。ユーザは、電子メール アカウントへのアクセスを認可されます。*vpnuser* は WebVPN ユーザ名です。

推奨処置 なし

719021

エラー メッセージ %ASA-6-719021: WebVPN user: *vpnuser* is not checked against ACL.

説明 このメッセージは、ACL によって、電子メール アカウントのアクセスにどのようなユーザ制限があるかが判定された場合に表示されます。ACL を使用した認可チェックがイネーブルになっていません。*vpnuser* は WebVPN ユーザ名です。

推奨処置 必要な場合は、ACL チェック機能をイネーブルにします。

719022

エラー メッセージ %ASA-6-719022: WebVPN user *vpnuser* has been authenticated.

説明 このメッセージは、ユーザ名が AAA サーバによって認証されたときに表示されます。*vpnuser* は WebVPN ユーザ名です。

推奨処置 不要です。

719023

エラー メッセージ %ASA-6-719023: WebVPN user *vpnuser* has not been successfully authenticated. Access denied.

説明 このメッセージは、ユーザ名が AAA サーバによって拒否されたときに表示されます。セッションは中断されます。ユーザは、電子メール アカウントへのアクセスを許可されません。*vpnuser* は WebVPN ユーザ名です。

推奨処置 不要です。

719024

エラー メッセージ %ASA-6-719024: Email Proxy piggyback auth fail: session = *pointer* user=*vpnuser* addr=*source_address*

説明 このメッセージは、Piggyback 認証が、確立された WebVPN セッションを使用して WebVPN セッション データベースでユーザ名と IP アドレスの一致を検証しているときに表示されます。これは、WebVPN セッションと電子メール プロキシ セッションが同じユーザによって開始され、WebVPN セッションがすでに確立されているという想定に基づいています。認証が失敗したため、セッションは中断されます。ユーザは、電子メール アカウントへのアクセスを許可されません。*pointer* はセッション構造のポインタで、*vpnuser* は WebVPN ユーザ名で、*source_address* はクライアントの IP アドレスです。

推奨処置 不要です。

719025

エラー メッセージ %ASA-6-719025: Email Proxy DNS name resolution failed for *hostname*.

説明 このメッセージは、IP アドレスが有効でないか、使用可能な DNS サーバがないため、IP アドレスでホスト名を解決できないときに表示されます。*hostname* は、解決する必要のあるホスト名です。

推奨処置 DNS サーバの可用性を調べ、設定したメール サーバ名が有効かどうかを確認します。

719026

エラー メッセージ %ASA-6-719026: Email Proxy DNS name *hostname* resolved to *IP_address*.

説明 このメッセージは、IP アドレスでホスト名が正常に解決されたときに表示されます。*hostname* は解決する必要があるホスト名で、*IP_address* は設定したメール サーバ名から解決された IP アドレスです。

推奨処置 不要です。

720001

エラー メッセージ %ASA-4-720001: (VPN-*unit*) Failed to initialize with Chunk Manager.

説明 このメッセージは、VPN フェールオーバー サブシステムがメモリ バッファ管理サブシステムで初期化できなかったときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 このメッセージは、システム全体の問題と、VPN フェールオーバー サブシステムを開始できないことを示しています。システム ログ メッセージを検索し、システム レベルで初期化の問題の兆候がないか調べます。

720002

エラー メッセージ %ASA-6-720002: (VPN-*unit*) Starting VPN Stateful Failover Subsystem...

説明 このメッセージは、VPN フェールオーバー サブシステムが開始していて、システムが起動するときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 不要です。

720003

エラー メッセージ %ASA-6-720003: (VPN-*unit*) Initialization of VPN Stateful Failover Component completed successfully

説明 このメッセージは、ブート時に VPN フェールオーバー サブシステムの初期化が完了したときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 不要です。

720004

エラー メッセージ %ASA-6-720004: (VPN-*unit*) VPN failover main thread started.

説明 このメッセージは、ブート時に VPN フェールオーバーのメイン処理スレッドが開始されたときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 不要です。

720005

エラー メッセージ %ASA-6-720005: (VPN-*unit*) VPN failover timer thread started.

説明 このメッセージは、ブート時に VPN フェールオーバーのタイマー処理スレッドが開始されたときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 不要です。

720006

エラー メッセージ %ASA-6-720006: (VPN-*unit*) VPN failover sync thread started.

説明 このメッセージは、ブート時にシステムのバルク同期化処理スレッドが開始されたときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 不要です。

720007

エラー メッセージ %ASA-4-720007: (VPN-*unit*) Failed to allocate chunk from Chunk Manager.

説明 このメッセージは、事前に割り当てられたメモリ バッファのセットがなくなりつつあるときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 このメッセージは、リソースの問題を示しています。処理されているメッセージの数が多すぎる場合は、システムに重い負荷がかかっている可能性があります。この状態は、後で VPN フェールオーバー サブシステムが顕著なメッセージを処理し、前に割り当てられたメモリを解放したときに改善される可能性があります。

720008

エラー メッセージ %ASA-4-720008: (VPN-*unit*) Failed to register to High Availability Framework.

説明 このメッセージは、VPN フェールオーバー サブシステムがコア フェールオーバー サブシステムに登録できなかったときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 VPN フェールオーバー サブシステムを起動できません。他のサブシステムの初期化の問題が原因となっている可能性があります。システム ログ メッセージを検索し、システム全体で初期化の問題の兆候がないか調べます。

720009

エラー メッセージ %ASA-4-720009: (VPN-unit) Failed to create version control block.

説明 このメッセージは、VPN フェールオーバー サブシステムがバージョン コントロール ブロックを作成できなかった場合に表示されます。このステップは、VPN フェールオーバー サブシステムが、現在のリリースの下位互換性ファームウェア バージョンを検出するために必要です。unit は「Primary」または「Secondary」です。

推奨処置 VPN フェールオーバー サブシステムを起動できません。他のサブシステムの初期化の問題が原因となっている可能性があります。システム ログ メッセージを検索し、システム全体で初期化の問題の兆候がないか調べます。

720010

エラー メッセージ %ASA-6-720010: (VPN-unit) VPN failover client is being disabled

説明 このメッセージは、フェールオーバー キーを定義しないでフェールオーバーをイネーブルにすると表示されます。VPN フェールオーバーを使用するには、フェールオーバー キーを定義する必要があります。unit は「Primary」または「Secondary」です。

推奨処置 フェールオーバー キー コマンドを使用して、アクティブ装置とスタンバイ装置の間の共有秘密鍵を定義します。

720011

エラー メッセージ %ASA-4-720011: (VPN-unit) Failed to allocate memory

説明 このメッセージは、VPN フェールオーバー サブシステムがメモリ バッファを割り当てられないときに表示されます。これは、システム全体のリソースの問題を示しています。unit は「Primary」または「Secondary」です。

推奨処置 システムには重い負荷がかかっています。この状態は、着信トラフィックを削減することによってシステムの負荷を減らすと改善される可能性があります。着信トラフィックを削減することによって、既存の作業負荷を処理するために割り当てられたメモリが使用可能になり、システムが通常のオペレーションに戻る可能性があります。

720012

エラー メッセージ %ASA-6-720012: (VPN-unit) Failed to update IPSec failover runtime data on the standby unit.

説明 このメッセージは、対応する IPSec トンネルがスタンバイ装置で削除されているため、VPN フェールオーバー サブシステムが IPSec 関連のランタイム データを更新できないときに表示されます。unit は「Primary」または「Secondary」です。

推奨処置 不要です。

720013

エラー メッセージ %ASA-4-720013: (VPN-unit) Failed to insert certificate in trust point *trustpoint_name*

説明 このメッセージは、VPN フェールオーバー サブシステムがトラストポイントに証明書を挿入しようとしたときに表示されます。*unit* は「Primary」または「Secondary」で、*trustpoint_name* はトラストポイントの名前です。

推奨処置 証明書の内容を調べて、無効かどうかを判別します。

720014

エラー メッセージ %ASA-6-720014: (VPN-unit) Phase 2 connection entry (*msg_id=message_number*, *my cookie=mine*, *his cookie=his*) contains no SA list.

説明 このメッセージは、フェーズ2 接続エントリにリンクされたセキュリティ アソシエーションがないときに表示されます。*unit* は「Primary」または「Secondary」です。*message_number* はフェーズ2 接続エントリのメッセージ ID で、*mine* は自分のフェーズ1 クッキーで、*his* はピアのフェーズ1 クッキーです。

推奨処置 不要です。

720015

エラー メッセージ %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*).

説明 このメッセージは、所定のフェーズ2 接続エントリに対して対応するフェーズ1 セキュリティ アソシエーションが見つからないときに表示されます。*unit* は「Primary」または「Secondary」です。*message_number* はフェーズ2 接続エントリのメッセージ ID で、*mine* は自分のフェーズ1 クッキーで、*his* はピアのフェーズ1 クッキーです。

推奨処置 不要です。

720016

エラー メッセージ %ASA-5-720016: (VPN-unit) Failed to initialize default timer #*index*.

説明 このメッセージは、VPN フェールオーバー サブシステムが所定のタイマー イベントを初期化できなかったときに表示されます。*unit* は「Primary」または「Secondary」、*index* はタイマー イベントの内部インデックスです。

推奨処置 ブート時に VPN フェールオーバー サブシステムを起動できません。システム ログメッセージを検索し、システム全体で初期化の問題の兆候がないか調べます。

720017

エラー メッセージ %ASA-5-720017: (VPN-*unit*) Failed to update LB runtime data

説明 このメッセージは、VPN フェールオーバー サブシステムが VPN ロードバランシング ランタイム データを更新できないときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 不要です。

720018

エラー メッセージ %ASA-5-720018: (VPN-*unit*) Failed to get a buffer from the underlying core high availability subsystem. Error code *code*.

説明 このメッセージは、システムに重い負荷がかかっている可能性があるときに表示されます。VPN フェールオーバー サブシステムがフェールオーバー バッファを取得できませんでした。*unit* は「Primary」または「Secondary」で、*code* は高可用性のサブシステムによって戻されるエラー コードです。

推奨処置 着信トラフィックの量を減らし、現在の負荷状態を改善します。着信トラフィックが減ると、システムは着信の負荷を処理するために割り当てられたメモリを解放します。

720019

エラー メッセージ %ASA-5-720019: (VPN-*unit*) Failed to update cTCP statistics.

説明 このメッセージは、VPN フェールオーバー サブシステムが IPSec/cTCP 関連の統計を更新できないときに表示されます。*unit* は「Primary」または「Secondary」です。

推奨処置 不要です。更新は定期的送信されるので、スタンバイ装置の IPSec/cTCP 統計は次の更新メッセージで更新されます。

720020

エラー メッセージ %ASA-5-720020: (VPN-*unit*) Failed to send *type* timer message.

説明 このメッセージは、VPN フェールオーバー サブシステムが定期的なタイマー メッセージをスタンバイ装置に送信しなかった場合に表示されます。*unit* は「Primary」または「Secondary」で、*type* はタイマー メッセージのタイプです。

推奨処置 不要です。次のタイムアウト時に定期的なタイマー メッセージが再送されます。

720021

エラー メッセージ %ASA-5-720021: (VPN-*unit*) HA non-block send failed for peer msg *message_number*. HA error *code*.

説明 VPN フェールオーバー サブシステムが非ブロック メッセージを送信できません。

unit : 「Primary」または「Secondary」

message_number : ピア メッセージの ID 番号。

code : エラー時の戻りコード。

推奨処置 これは、負荷のかかったシステムまたはシステム外のリソースによって引き起こされる一時的な状態です。より多くのシステム リソースが解放されるにつれ、システムの状態は改善されます。

720022

エラー メッセージ %ASA-4-720022: (VPN-*unit*) Cannot find trust point *trustpoint*

説明 VPN フェールオーバー サブシステムがトラストポイントを名前を検索しようとする、エラーが発生します。

unit : 「Primary」または「Secondary」

trustpoint : トラストポイントの名前。

推奨処置 トラストポイントはオペレータによって削除される可能性があります。

720023

エラー メッセージ %ASA-6-720023: (VPN-*unit*) HA status callback: Peer is *not* present.

説明 これは情報メッセージです。ピアが使用可能または使用不可になったことをローカル装置が検出すると、VPN フェールオーバー サブシステムがコア フェールオーバー サブシステムから通知を受けます。

unit : 「Primary」または「Secondary」

not : 「not」または「not」の表示なし。

推奨処置 不要です。

720024

エラー メッセージ %ASA-6-720024: (VPN-*unit*) HA status callback: Control channel is *status*.

説明 これは、フェールオーバーコントロール チャンネルが「up」か「down」かを示す情報メッセージです。フェールオーバーコントロール チャンネルは、フェールオーバー リンク チャンネルが「up」か「down」かを示す **failover link** コマンドと **show failover** コマンドによって定義されます。

unit : 「Primary」または「Secondary」

status : 「up」または「down」

推奨処置 不要です。

720025

エラー メッセージ %ASA-6-720025: (VPN-*unit*) HA status callback: Data channel is *status*.

説明 これは、フェールオーバー データ チャンネルがアップかダウンかを示す情報メッセージです。

unit : 「Primary」または「Secondary」

status : 「up」または「down」

推奨処置 不要です。

720026

エラー メッセージ %ASA-6-720026: (VPN-*unit*) HA status callback: Current progression is being aborted.

説明 このメッセージが生成されるのは、オペレータまたはその他の外部条件が適用され、フェールオーバー ピアが役割（アクティブまたはスタンバイ）に合意する前に現在のフェールオーバーの進行が中断された場合だけです。たとえば、ネゴシエーション中にスタンバイ装置で `failover active` コマンドが入力された場合などです。あるいは、アクティブ装置がリブートされている場合もそうです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720027

エラー メッセージ %ASA-6-720027: (VPN-*unit*) HA status callback: My state *state*.

説明 この情報メッセージは、ローカル フェールオーバー装置の状態が変わるたびに生成されます。

unit : 「Primary」または「Secondary」

state : ローカル フェールオーバー装置の現在の状態。

推奨処置 不要です。

720028

エラー メッセージ %ASA-6-720028: (VPN-*unit*) HA status callback: Peer state *state*.

unit : 「Primary」または「Secondary」

state : フェールオーバー ピアの現在の状態。

説明 この情報メッセージは、フェールオーバー ピアの現在の状態を報告するために生成されます。

推奨処置 不要です。

720029

エラー メッセージ %ASA-6-720029: (VPN-*unit*) HA status callback: Start VPN bulk sync state.

unit : 「Primary」 または 「Secondary」

説明 これは、アクティブ装置がすべての状態情報をスタンバイ装置へ送信する準備ができたときに生成される情報メッセージです。

推奨処置 不要です。

720030

エラー メッセージ %ASA-6-720030: (VPN-*unit*) HA status callback: Stop bulk sync state.

unit : 「Primary」 または 「Secondary」

説明 これは、アクティブ装置がすべての状態情報をスタンバイ装置へ送信し終わったときに生成される情報メッセージです。

推奨処置 不要です。

720031

エラー メッセージ %ASA-7-720031: (VPN-*unit*) HA status callback: Invalid event received. event=*event_ID*.

説明 このメッセージは、VPN フェールオーバー サブシステムが、基礎となるフェールオーバー サブシステムから無効なコールバック イベントを受信した場合に生成されます。

unit : 「Primary」 または 「Secondary」

event_ID : 無効なイベント ID が受信されました。

推奨処置 これはデバッグ メッセージです。

720032

エラー メッセージ %ASA-6-720032: (VPN-*unit*) HA status callback: id=*ID*, seq=*sequence_#*, grp=*group*, event=*event*, op=*operand*, my=*my_state*, peer=*peer_state*.

説明 これは、基礎となるフェールオーバー サブシステムが状態の更新を通知したときに VPN フェールオーバー サブシステムによって生成される情報メッセージです。

unit : 「Primary」 または 「Secondary」

ID : クライアント ID 番号。

sequence_# : シーケンス番号。

group : グループ ID。

event : 現在のイベント。

operand : 現在の演算子。

my_state : システムの現在の状態。

peer_state : ピアの現在の状態。

推奨処置 不要です。

720033

エラーメッセージ %ASA-4-720033: (VPN-unit) Failed to queue add to message queue.

説明 このメッセージは、システム リソースが低下している可能性があることを示しています。VPN フェールオーバー サブシステムが内部メッセージをキューに入れようとすると、エラーが発生します。

unit : 「Primary」または「Secondary」

推奨処置 これは、システムに重い負荷がかかっており、VPN フェールオーバー サブシステムが着信トラフィックを処理するためのリソースを割り当てられないことを示す一時的な状態である可能性があります。このエラーは、システムの現在の負荷が減り、新規メッセージを再び処理するために追加のシステム リソースを使用できるようになると、解決する可能性があります。

720034

エラーメッセージ %ASA-7-720034: (VPN-unit) Invalid type (*type*) for message handler.

説明 VPN フェールオーバー サブシステムが無効なメッセージ タイプを処理しようとすると、エラーが発生します。

unit : 「Primary」または「Secondary」

type : メッセージ タイプ。

推奨処置 これはデバッグ メッセージです。

720035

エラーメッセージ %ASA-5-720035: (VPN-unit) Fail to look up CTCP flow handle

説明 VPN フェールオーバー サブシステムが検索を実行する前に、スタンバイ装置で cTCP フローが削除される可能性があります。

unit : 「Primary」または「Secondary」

推奨処置 cTCP フローが削除される兆候をシステム ログ メッセージで検索して、フローが削除された理由（たとえば、アイドルタイムアウト）を判別します。

720036

エラー メッセージ %ASA-5-720036: (VPN-*unit*) Failed to process state update message from the active peer.

説明 スタンバイ装置によって受信された状態更新メッセージを VPN フェールオーバー サブシステムが処理しようとする、エラーが発生します。

unit : 「Primary」または「Secondary」

推奨処置 これは、現在の負荷またはシステム リソースの低下による一時的な状態である可能性があります。

720037

エラー メッセージ %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 : 「Primary」または「Secondary」

id : クライアント ID。

sequence_number : シーケンス番号。

group : グループ ID。

event : 現在のイベント。

operand : 現在の演算子。

my_state : システムの現在の状態。

peer_state : ピアの現在の状態。

説明 これは、現在のフェールオーバーの進行状況を報告する情報メッセージです。

推奨処置 不要です。

720038

エラー メッセージ %ASA-4-720038: (VPN-*unit*) Corrupted message from active unit.

説明 スタンバイ装置が、アクティブ装置から破損したメッセージを受信します。アクティブ装置からのメッセージが破損しています。これは、アクティブ装置とスタンバイ装置の間で互換性のないファームウェアを実行していることによって引き起こされる可能性があります。

unit : 「Primary」または「Secondary」

推奨処置 これは、ローカル装置がフェールオーバー ペアのアクティブ装置になったことを示す情報メッセージです。

720039

エラー メッセージ %ASA-6-720039: (VPN-*unit*) VPN failover client is transitioning to active state

説明 これは、ローカル装置がフェールオーバー ペアのアクティブ装置になったことを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720040

エラー メッセージ %ASA-6-720040: (VPN-*unit*) VPN failover client is transitioning to standby state.

説明 これは、ローカル装置がフェールオーバー ペアのスタンバイ装置になったことを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720041

エラー メッセージ %ASA-7-720041: (VPN-*unit*) Sending *type* message *id* to standby unit

説明 これは、アクティブ装置からスタンバイ装置へメッセージが送信されたことを示すデバッグメッセージです。

unit : 「Primary」または「Secondary」

type : メッセージタイプ。

id : メッセージの ID。

推奨処置 不要です。

720042

エラー メッセージ %ASA-7-720042: (VPN-*unit*) Receiving *type* message *id* from active unit

説明 これは、スタンバイ装置によってメッセージが受信されたことを示すデバッグメッセージです。

unit : 「Primary」または「Secondary」

type : メッセージタイプ。

id : メッセージの ID。

推奨処置 不要です。

720043

エラー メッセージ %ASA-4-720043: (VPN-*unit*) Failed to send *type* message *id* to standby unit

説明 VPN フェールオーバー サブシステムがアクティブ装置からスタンバイ装置へメッセージを送信しようとしたときに、エラーが発生しました。コア フェールオーバー サブシステムでフェールオーバー バッファが不足するか、フェールオーバー LAN リンクがダウンする 720018 によって引き起こされる可能性があります。

unit : 「Primary」または「Secondary」

type : メッセージ タイプ。

id : メッセージの ID。

推奨処置 show failover コマンドを使用して、フェールオーバー ペアが良好な状態で動作していることと、フェールオーバー LAN リンクが「up」であることを確認します。

720044

エラー メッセージ %ASA-4-720044: (VPN-*unit*) Failed to receive message from active unit

説明 VPN フェールオーバー サブシステムがスタンバイ装置でメッセージを受信しようとする時、エラーが発生します。これは、破損したメッセージや着信メッセージの保存に割り当てるメモリの不足によって引き起こされる可能性があります。

unit : 「Primary」または「Secondary」

推奨処置 show failover コマンドを使用して、受信エラーを検索し、これが VPN フェールオーバー特有の問題か一般的なフェールオーバーの問題かを判別します。破損したメッセージは、アクティブ装置とスタンバイ装置で互換性のないファームウェア バージョンを実行していることによって生じる可能性があります。show memory コマンドを使用して、メモリ低下状態があるかどうかを判別します。

720045

エラー メッセージ %ASA-6-720045: (VPN-*unit*) Start bulk syncing of state information on standby unit.

説明 これは、アクティブ装置からバルク同期化情報を受信し始めたことをスタンバイ装置に通知したことを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720046

エラー メッセージ %ASA-6-720046: (VPN-*unit*) End bulk syncing of state information on standby unit

説明 これは、アクティブ装置からのバルク同期化が完了したことをスタンバイ装置に通知したことを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720047

エラー メッセージ %ASA-4-720047: (VPN-*unit*) Failed to sync SDI node secret file for server *IP_address* on the standby unit.

説明 VPN フェールオーバー サブシステムがスタンバイ装置で SDI サーバ用のノード シークレット ファイルを同期しようとしたときに、エラーが発生しました。SDI ノード シークレット ファイルは、フラッシュに格納されています。このエラーは、フラッシュ ファイル システムがいつばいか、破損していることを示している可能性があります。

unit : 「Primary」または「Secondary」

IP_address : サーバの IP アドレス。

推奨処置 `dir` コマンドを使用して、フラッシュの内容を表示します。ノード シークレット ファイルの名前は「*ip.sdi*」です。

720048

エラー メッセージ %ASA-7-720048: (VPN-*unit*) FSM action trace begin: state=*state*, last event=*event*, func=*function*.

unit : 「Primary」または「Secondary」

state : 現在の状態。

event : 最後のイベント。

function : 現在実行中の機能。

説明 これは、VPN フェールオーバー サブシステムの有限状態マシン機能が開始されたことを示すデバッグ メッセージです。

推奨処置 不要です。

720049

エラー メッセージ %ASA-7-720049: (VPN-*unit*) FSM action trace end: state=*state*, last event=*event*, return=*return*, func=*function*.

説明 これは、VPN フェールオーバー サブシステムの有限状態マシン機能が完了したことを示すデバッグ メッセージです。

unit : 「Primary」または「Secondary」

state : 現在の状態。

event : 最後のイベント。
return : 戻りコード。
function : 現在実行中の機能。

推奨処置 不要です。

720050

エラー メッセージ %ASA-7-720050: (VPN-unit) Failed to remove timer. ID = *id*.

説明 これは、タイマー処理スレッドからタイマーを削除できないことを示すデバッグメッセージです。

unit : 「Primary」または「Secondary」

id : タイマー ID。

推奨処置 不要です。

720051

エラー メッセージ %ASA-4-720051: (VPN-unit) Failed to add new SDI node secret file for server *id* on the standby unit.

説明 VPN フェールオーバー サブシステムがスタンバイ装置で SDI サーバ用のノードシークレット ファイルを追加しようとしたときに、エラーが発生しました。SDI ノードシークレット ファイルは、フラッシュに格納されています。このエラーは、フラッシュ ファイル システムがいつばいか、破損していることを示している可能性があります。

unit : 「Primary」または「Secondary」

id : SDI サーバの IP アドレス。

推奨処置 `dir` コマンドを入力して、フラッシュの内容を表示します。ノードシークレット ファイルの名前は「*ip.sdi*」です。

720052

エラー メッセージ %ASA-4-720052: (VPN-unit) Failed to delete SDI node secret file for server *id* on the standby unit.

説明 VPN フェールオーバー サブシステムがアクティブ装置でノードシークレット ファイルを削除しようとしたときに、エラーが発生しました。削除しようとしているノードシークレット ファイルがフラッシュ ファイル システム内に存在しないか、フラッシュ ファイル システムの読み取りに問題がある可能性があります。

unit : 「Primary」または「Secondary」

IP_address : SDI サーバの IP アドレス。

推奨処置 `dir` コマンドを使用して、フラッシュの内容を表示します。ノードシークレット ファイルの名前は「*ip.sdi*」です。

720053

エラーメッセージ %ASA-4-720053: (VPN-*unit*) Failed to add cTCP IKE rule during bulk sync, peer=*IP_address*, port=*port*

説明 VPN フェールオーバー サブシステムがバルク同期化中にスタンバイ装置で cTCP IKE ルールをロードしようとする、エラーが発生します。

unit : 「Primary」または「Secondary」

IP_address : ピアの IP アドレス。

port : ピアのポート番号。

推奨処置 スタンバイ装置に重い負荷がかかっている、新規 IKE ルール要求が完了前にタイムアウトする可能性があります。

720054

エラーメッセージ %ASA-4-720054: (VPN-*unit*) Failed to add new cTCP record, peer=*IP_address*, port=*port*.

説明 cTCP レコードがスタンバイに複製され、更新できません。対応する IPSec over cTCP トンネルがフェールオーバー後に機能していない可能性があります。

unit : 「Primary」または「Secondary」

IP_address : ピアの IP アドレス。

port : ピアのポート番号。

推奨処置 cTCP データベースがいっぱいになっているか、同じピア IP アドレスとポート番号を持つレコードがすでに存在している可能性があります。これは、一時的な状態であり、改善される可能性があります。

720055

エラーメッセージ %ASA-4-720055: (VPN-*unit*) VPN Stateful failover can only be run in single/non-transparent mode.

説明 シングル (非透過) モードで動作していない場合は、このメッセージが表示され、VPN サブシステムは開始されません。

unit : 「Primary」または「Secondary」

推奨処置 VPN フェールオーバーをサポートする適切なモード用に装置を設定して、装置を再起動します。

720056

エラー メッセージ %ASA-6-720056: (VPN-*unit*) VPN Stateful failover Message Thread is being disabled.

説明 これは、ユーザがフェールオーバーをイネーブルにしようとしたがフェールオーバー キーが定義されていない場合、VPN フェールオーバー サブシステムのメイン メッセージ処理スレッドがディセーブルになることを示す情報メッセージです。フェールオーバー キーは VPN フェールオーバーに必要です。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720057

エラー メッセージ %ASA-6-720057: (VPN-*unit*) VPN Stateful failover Message Thread is enabled.

説明 これは、フェールオーバーがイネーブルでフェールオーバー キーが定義されている場合、VPN フェールオーバー サブシステムのメイン メッセージ処理スレッドがイネーブルになることを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720058

エラー メッセージ %ASA-6-720058: (VPN-*unit*) VPN Stateful failover Timer Thread is disabled.

説明 これは、フェールオーバー キーが未定義でフェールオーバーがイネーブルである場合、VPN フェールオーバー サブシステムのメイン タイマー処理スレッドがディセーブルになることを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720059

エラー メッセージ %ASA-6-720059: (VPN-*unit*) VPN Stateful failover Timer Thread is enabled.

説明 これは、フェールオーバー キーが定義されていてフェールオーバーがイネーブルである場合、VPN フェールオーバー サブシステムのメイン タイマー処理スレッドがイネーブルになることを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720060

エラー メッセージ %ASA-6-720060: (VPN-*unit*) VPN Stateful failover Sync Thread is disabled.

説明 これは、フェールオーバーがイネーブルでフェールオーバー キーが定義されていない場合、VPN フェールオーバー サブシステムのメイン バルク同期化処理スレッドがディセーブルになることを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720061

エラー メッセージ %ASA-6-720061: (VPN-*unit*) VPN Stateful failover Sync Thread is enabled.

説明 これは、フェールオーバーがイネーブルでフェールオーバー キーが定義されている場合、VPN フェールオーバー サブシステムのメイン バルク同期化処理スレッドがイネーブルになることを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720062

エラー メッセージ %ASA-6-720062: (VPN-*unit*) Active unit started bulk sync of state information to standby unit.

説明 これは、VPN フェールオーバー サブシステムのアクティブ装置がスタンバイ装置への状態情報のバルク同期化を開始したことを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720063

エラー メッセージ %ASA-6-720063: (VPN-*unit*) Active unit completed bulk sync of state information to standby.

説明 これは、VPN フェールオーバー サブシステムのアクティブ装置がスタンバイ装置への状態情報のバルク同期化を完了したことを示す情報メッセージです。

unit : 「Primary」または「Secondary」

推奨処置 不要です。

720064

エラー メッセージ %ASA-4-720064: (VPN-*unit*) Failed to update cTCP database record for peer=*IP_address*, port=*port* during bulk sync.

説明 VPN フェールオーバー サブシステムがバルク同期化中に既存の cTCP レコードを更新しようとしたときに、エラーが発生しました。cTCP レコードが見つかりません。スタンバイ装置で cTCP データベースから削除された可能性があります。

unit : 「Primary」または「Secondary」

IP_address : ピアの IP アドレス。

port : ピアのポート番号。

推奨処置 システム ログ メッセージを検索します。

720065

エラー メッセージ %ASA-4-720065: (VPN-*unit*) Failed to add new cTCP IKE rule, peer=*peer*, port=*port*.

説明 VPN フェールオーバー サブシステムがスタンバイ装置で cTCP データベース エントリ用の新規 IKE ルールを追加しようとすると、エラーが発生します。

unit : 「Primary」または「Secondary」

IP_address : ピアの IP アドレス。

port : ピアのポート番号。

推奨処置 システムに重い負荷がかかっている、cTCP IKE ルールの追加要求がタイムアウトになり、完了しない可能性があります。これは一時的な状態である可能性があります。

720066

エラー メッセージ %ASA-4-720066: (VPN-*unit*) Failed to activate IKE database.

説明 スタンバイ装置がアクティブな状態に移行しているときに VPN フェールオーバー サブシステムが IKE セキュリティ アソシエーション データベースをアクティブにしようとして、エラーが発生しました。スタンバイ装置に、IKE セキュリティ アソシエーション データベースがアクティブになることを妨げるリソース関連の問題がある可能性があります。

unit : 「Primary」または「Secondary」

推奨処置 `show failover` コマンドを使用してフェールオーバー ペアが良好な状態にあるかどうかを確認し、`syslog` でその他の IKE 関連エラーを検索します。

720067

エラー メッセージ %ASA-4-720067: (VPN-*unit*) Failed to deactivate IKE database.

説明 アクティブ装置がスタンバイ状態に移行しているときに VPN フェールオーバー サブシステムが IKE セキュリティ アソシエーション データベースを非アクティブにしようとして、エラーが発生しました。アクティブ装置に、IKE セキュリティ アソシエーション データベースが非アクティブになることを妨げるリソース関連の問題がある可能性があります。

unit : 「Primary」または「Secondary」

推奨処置 `show failover` コマンドを入力してフェールオーバー ペアが良好な状態にあるかどうかを確認し、syslog で IKE 関連エラーを検索します。

720068

エラー メッセージ %ASA-4-720068: (VPN-*unit*) Failed to parse peer message.

説明 VPN フェールオーバー サブシステムがスタンバイ装置でピア メッセージを解析しようすると、エラーが発生します。

unit : 「Primary」または「Secondary」

推奨処置 スタンバイ装置で受信されたピア メッセージを解析できません。アクティブ装置とスタンバイ装置の両方で同じバージョンのファームウェアが実行されていることを確認します。また、`show failover` コマンドを使用して、フェールオーバー ペアが良好な状態にあることも確認します。

720069

エラー メッセージ %ASA-4-720069: (VPN-*unit*) Failed to activate cTCP database.

説明 スタンバイ装置がアクティブな状態に移行しているときに VPN フェールオーバー サブシステムが cTCP データベースをアクティブにしようとして、エラーが発生しました。スタンバイ装置に、cTCP データベースがアクティブになることを妨げるリソース関連の問題がある可能性があります。

unit : 「Primary」または「Secondary」

推奨処置 `show failover` コマンドを入力してフェールオーバー ペアが良好な状態にあるかどうかを確認し、syslog でその他の cTCP 関連エラーを検索します。

720070

エラー メッセージ %ASA-4-720070: (VPN-*unit*) Failed to deactivate cTCP database.

説明 アクティブ装置がスタンバイ状態に移行しているときに VPN フェールオーバー サブシステムが cTCP データベースを非アクティブにしようとして、エラーが発生しました。アクティブ装置に、cTCP データベースが非アクティブになることを妨げるリソース関連の問題がある可能性があります。

unit : 「Primary」または「Secondary」

推奨処置 `show failover` コマンドを使用してフェールオーバー ペアが良好な状態にあるかどうかを確認し、syslog で cTCP 関連エラーを検索します。

720071

エラー メッセージ %ASA-5-720071: (VPN-*unit*) Failed to update cTCP dynamic data.

説明 VPN フェールオーバー サブシステムが cTCP 動的データを更新しようとしたときに、エラーが発生しました。

unit : 「Primary」または「Secondary」

説明 これは一時的な状態である可能性があります。これは定期的な更新なので、同じエラーが発生するかどうか注意します。また、syslog でその他のフェールオーバー関連メッセージを検索します。

720072

エラー メッセージ %ASA-4-720072: (VPN-*unit*) Cannot find trust point *tp*

説明 VPN フェールオーバー サブシステムがトラストポイントを名前で検索しようとする、エラーが発生します。

unit : 「Primary」または「Secondary」

tp : トラストポイントの名前。

推奨処置 トラストポイントはオペレータによって削除された可能性があります。show crypto ca trustpoint CLI を使用して、トラストポイントがコンフィギュレーション内に存在するかどうかを確認します。

720073

エラー メッセージ %ASA4-720073: (VPN-*unit*) Fail to insert certificate in trust point *trustpoint* on the standby unit.

説明 VPN フェールオーバー サブシステムがトラストポイントに証明書を挿入しようとする、エラーが発生します。このエラーは、証明書の無効な内容によって生じた可能性があります。

unit : 「Primary」または「Secondary」

trustpoint : トラストポイントの名前。

推奨処置 アクティブ装置で「write standby」を実行し、証明書を手動でスタンバイ装置に複製します。システム ログ メッセージを検索して、フェールオーバー /PKI 関連のエラーがあるかどうかを確認します。



重大度別メッセージ リスト

この付録には、次の項があります。

- [アラートメッセージ、重大度 1 \(P.A-2\)](#)
- [クリティカルメッセージ、重大度 2 \(P.A-4\)](#)
- [エラーメッセージ、重大度 3 \(P.A-6\)](#)
- [警告メッセージ、重大度 4 \(P.A-13\)](#)
- [通知メッセージ、重大度 5 \(P.A-18\)](#)
- [情報メッセージ、重大度 6 \(P.A-23\)](#)
- [デバッグメッセージ、重大度 7 \(P.A-31\)](#)



(注)

Cisco ASA は、重大度 0 (緊急) メッセージは syslog に送信しません。この重大度 0 メッセージは UNIX のパニックメッセージと同様に、システムが不安定であることを示します。

アラートメッセージ、重大度 1

次のメッセージが重大度 1（アラート）で表示されます。

- %PIX|ASA-1-101001: (Primary) Failover cable OK.
- %PIX|ASA-1-101002: (Primary) Bad failover cable.
- %PIX|ASA-1-101003: (Primary) Failover cable not connected (this unit).
- %PIX|ASA-1-101004: (Primary) Failover cable not connected (other unit).
- %PIX|ASA-1-101005: (Primary) Error reading failover cable status.
- %PIX|ASA-1-102001: (Primary) Power failure/System reload other side.
- %PIX|ASA-1-103001: (Primary) No response from other firewall (reason code = code).
- %PIX|ASA-1-103002: (Primary) Other firewall network interface interface_number OK.
- %PIX|ASA-1-103003: (Primary) Other firewall network interface interface_number failed.
- %PIX|ASA-1-103004: (Primary) Other firewall reports this firewall failed.
- %PIX|ASA-1-103005: (Primary) Other firewall reporting failure.
- %PIX|ASA-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %PIX|ASA-1-104002: (Primary) Switching to STNDBY (cause: string).
- %PIX|ASA-1-104003: (Primary) Switching to FAILED.
- %PIX|ASA-1-104004: (Primary) Switching to OK.
- %PIX|ASA-1-105001: (Primary) Disabling failover.
- %PIX|ASA-1-105002: (Primary) Enabling failover.
- %PIX|ASA-1-105003: (Primary) Monitoring on interface interface_name waiting
- %PIX|ASA-1-105004: (Primary) Monitoring on interface interface_name normal
- %PIX|ASA-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.
- %PIX|ASA-1-105006: (Primary) Link status 'Up' on interface interface_name.
- %PIX|ASA-1-105007: (Primary) Link status 'Down' on interface interface_name.
- %PIX|ASA-1-105008: (Primary) Testing interface interface_name.
- %PIX|ASA-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.
- %PIX|ASA-1-105011: (Primary) Failover cable communication failure
- %PIX|ASA-1-105020: (Primary) Incomplete/slow config replication
- %PIX|ASA-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name
- %PIX|ASA-1-105031: Failover LAN interface is up
- %PIX|ASA-1-105032: LAN Failover interface is down
- %PIX|ASA-1-105034: Receive a LAN_FAILOVER_UP message from peer.
- %PIX|ASA-1-105035: Receive a LAN failover interface down msg from peer.
- %PIX|ASA-1-105036: dropped a LAN Failover command message.
- %PIX|ASA-1-105037: The primary and standby units are switching back and forth as the active unit.
- %PIX|ASA-1-105038: (Primary) Interface count mismatch
- %PIX|ASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %PIX|ASA-1-105040: (Primary) Mate failover version is not compatible.
- %PIX|ASA-1-105042: (Primary) Failover interface OK
- %PIX|ASA-1-105043: (Primary) Failover interface failed
- %PIX|ASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.

- %PIX|ASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %PIX|ASA-1-105046 (Primary|Secondary) Mate has a different chassis
- %PIX|ASA-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
- %PIX|ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name
- %PIX|ASA-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
- %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).
- %PIX|ASA-1-111111 error_message
- %PIX|ASA-1-415004:internal_sig_id Content type not found - action mime_type from source_address to dest_address
- %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)

クリティカル メッセージ、重大度 2

次のメッセージが重大度 2（クリティカル）で表示されます。

- %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
- %PIX|ASA-3-109032: Unable to install ACL access_list, downloaded for user username; Error in ACE: ace.
- %PIX|ASA-2-112001: (string;dec) Clear complete.
- %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-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name

- %PIX|ASA-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %PIX|ASA-2-215001:Bad route_compress() call, sdb= number
- %PIX|ASA-2-217001: No memory for string in string
- %PIX|ASA-2-304007: URL Server IP_address not responding, ENTERING ALLOW mode.
- %PIX|ASA-2-304008: LEAVING ALLOW mode, URL Server is up.
- %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-3-420001 : IPS card not up and fail-close mode used, dropping ICMP packet ifc_in:SIP to ifc_out:DIP (typeICMP_TYPE, code ICMP_CODE)"
- %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.
- %PIX|ASA-2-709007: Configuration replication failed for command command
- %PIX|ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value
- %PIX|ASA-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored
- %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
- %PIX|ASA-2-717008: Insufficient memory to process_requiring_memory.
- %PIX|ASA-2-717011: Unexpected event event event_ID
- %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.
- %PIX|ASA-3-717023 SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason_string.
- %PIX|ASA-3-717027 Certificate chain failed validation. reason_string.

エラーメッセージ、重大度 3

次のメッセージが重大度 3（エラー）で表示されます。

- %PIX|ASA-3-105010: (Primary) Failover message block alloc failed
- %PIX|ASA-3-106010: Deny inbound protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port
- %PIX|ASA-3-106011: Deny inbound (No xlate) string
- %PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)
- %PIX|ASA-3-109010: Auth from inside_address/inside_port to outside_address/outside_port failed (too many pending auths) on interface interface_name.
- %PIX|ASA-3-109013: User must authenticate before using this service
- %PIX|ASA-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-3-113001: 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-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns
- %PIX|ASA-3-201004: Too many UDP connections on {static|xlate} 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 Cisco ASA 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
- %PIX|ASA-3-202001: Out of address translation slots!
- %PIX|ASA-3-202005: Non-embryonic in embryonic list outside_address/outside_port inside_address/inside_port
- %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
- %PIX|ASA-3-208005: (function:line_num) clear command return code
- %PIX|ASA-3-210001: LU sw_module_name error = number
- %PIX|ASA-3-210002: LU allocate block (bytes) failed.
- %PIX|ASA-3-210003: Unknown LU Object number
- %PIX|ASA-3-210005: LU allocate connection failed
- %PIX|ASA-3-210006: LU look NAT for IP_address failed
- %PIX|ASA-3-210007: LU allocate xlate failed
- %PIX|ASA-3-210008: LU no xlate for inside_address/inside_port outside_address/outside_port
- %PIX|ASA-3-210010: LU make UDP connection for outside_address:outside_port inside_address:inside_port failed
- %PIX|ASA-3-210020: LU PAT port port reserve failed

- %PIX|ASA-3-210021: LU create static xlate global_address ifc interface_name failed
- %PIX|ASA-3-211001: Memory allocation Error
- %PIX|ASA-3-211003: CPU utilization for number seconds = percent
- %PIX|ASA-3-212001: Unable to open SNMP channel (UDP port port) on interface interface_number, error code = code
- %PIX|ASA-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface_number, error code = code
- %PIX|ASA-3-212003: Unable to receive an SNMP request on interface interface_number, error code = code, will try again.
- %PIX|ASA-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number, error code = code
- %PIX|ASA-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.
- %PIX|ASA-3-212006: Dropping SNMP request from source_address/source_port to interface_name:dest_address/dest_port because: reason.
- %PIX|ASA-3-213001: PPTP control daemon socket io string, errno = number.
- %PIX|ASA-3-213002: PPTP tunnel hashtable insert failed, peer = IP_address.
- %PIX|ASA-3-213003: PPP virtual interface interface_number isn't opened.
- %PIX|ASA-3-213004: PPP virtual interface interface_number client ip allocation failed.
- %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 static|identity|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-3-315004: 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 lsid IP_address mask netmask adv IP_address type number
- %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
- %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-3-319001: 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).
- %PIX|ASA-3-320001: The subject name of the peer cert is not allowed for connection
- %PIX|ASA-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface
- %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.
- %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.
- %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
- %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
- %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
- %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
- %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
- %PIX|ASA-3-324005: Unable to create tunnel from source_interface:source_address/source_port to dest_interface:dest_address/dest_port
- %PIX|ASA-3-324006: GSN IP_address tunnel limit tunnel_limit exceeded, PDP Context TID tid failed
- %PIX|ASA-3-324007: Unable to create GTP connection for response from source_interface:source_address/0 to dest_interface:dest_address/dest_port
- %PIX|ASA-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings
- %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
- %PIXPIX|ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface_name AC:ac_name
- %PIXPIX|ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface_name AC:ac_name
- %PIXPIX|ASA-3-403503: PPPoE:PPP link down:reason
- %PIXPIX|ASA-3-403504: PPPoE:No 'vpdn group' for PPPoE is created
- %PIX|ASA-3-404102: ISAKMP: Exceeded embryonic limit
- %PIX|ASA-3-407002: 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-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]
- %PIX|ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]
- %PIX|ASA-3-610001: NTP daemon interface interface_name: Packet denied from IP_address
- %PIX|ASA-3-610002: NTP daemon interface interface_name: Authentication failed for packet from IP_address
- %PIX|ASA-3-611313: VPNClient: Backup Server List Error: reason
- %PIX|ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %PIX|ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %PIX|ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %PIX|ASA-3-713012: Unknown protocol (protocol). Not adding SA w/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-3-713018: Unknown ID type during find of group name for certs, Type ID_Type
- %PIX|ASA-3-713020: No Group found by matching OU(s) from ID payload: OU_value
- %PIX|ASA-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address
- %PIX|ASA-3-713032: Received invalid local Proxy Range IP_address - IP_address
- %PIX|ASA-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-3-713116: Terminating connection attempt: L2TP-over-IPSEC attempted by group (group_name) but L2TP disabled
- %PIX|ASA-3-713118: Detected invalid Diffie-Hellman 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)
- %PIX|ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)
- %PIX|ASA-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #
- %PIX|ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %PIX|ASA-3-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing
- %PIX|ASA-3-713129: Received unexpected Transaction Exchange payload type: payload_id
- %PIX|ASA-3-713132: Cannot obtain an IP_address for remote peer
- %PIX|ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id) with phase 1 group(DH group DH group_number)
- %PIX|ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection

- %PIX|ASA-3-713138: Group group_name not found and BASE GROUP default preshared key not configured
- %PIX|ASA-3-713140: Split Tunneling Policy requires network list but none configured
- %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
- %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
- %PIX|ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: netmask
- %PIX|ASA-3-713149: Hardware client security attribute attribute_name was enabled but not requested.
- %PIX|ASA-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.
- %PIX|ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %PIX|ASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %PIX|ASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
- %PIX|ASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
- %PIX|ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %PIX|ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %PIX|ASA-3-713167: Remote peer has failed user authentication - check configured username and password
- %PIX|ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %PIX|ASA-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-3-717001: 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.
- %PIX|ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure
- %PIX|ASA-3-717015: CRL received from issuer is too large to process (CRL size = crl_size, maximum CRL size = max_crl_size)
- %PIX|ASA-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url
- %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)
- %PIX|ASA-3-717019: Failed to insert CRL for trustpoint trustpoint_name. Reason: failure_reason.

警告メッセージ、重大度 4

次のメッセージが重大度 4（警告）で表示されます。

- %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
- %PIX|ASA-4-106027:Failed to determine the security context for the packet:vlan source Vlan#:ethertype src sourceMAC dst destMAC
- %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-4-209003: 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-4-313003: Invalid destination for ICMP error
- %PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session
- %PIX|ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
- %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
- %PIX|ASA-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=dest_address, prot=protocol, spi=number
- %PIX|ASA-4-402102: decapsulate: packet missing {AH|ESP}, destadr=dest_address, actual prot=protocol
- %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
- %PIX|ASA-4-402106: Rec'd packet not an IPSEC packet (ip) dest_address= dest_address, src_addr= source_address, prot= protocol
- %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.
- %PIX|ASA-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.

- %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 .
- %PIX|ASA-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote_IP to local_IP.
- %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.
- %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.
- %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.
- %PIX|ASA-4-402121: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that was dropped by IPSec (drop_reason).
- %PIX|ASA-4-402122: IPSEC: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPSec that was dropped by IPSec (drop_reason).
- %PIX|ASA-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code= error_string) while executing crypto command command .
- %PIX|ASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel_id=number, session_id=number
- %PIXPIX|ASA-4-403102: PPP virtual interface interface_name rcvd pkt with invalid protocol: protocol, reason: reason.
- %PIXPIX|ASA-4-403103: PPP virtual interface max connections reached.
- %PIXPIX|ASA-4-403104: PPP virtual interface interface_name requires mschap for MPPE.
- %PIXPIX|ASA-4-403106: PPP virtual interface interface_name requires RADIUS for MPPE.
- %PIXPIX|ASA-4-403107: PPP virtual interface interface_name missing aaa server group info
- %PIXPIX|ASA-4-403108: PPP virtual interface interface_name missing client ip address option
- %PIXPIX|ASA-4-403109: Rec'd packet not an PPTP packet. (ip) dest_address= dest_address, src_addr= source_address, data: string.
- %PIXPIX|ASA-4-403110: PPP virtual interface interface_name, user: user missing MPPE key from aaa server.
- %PIXPIX|ASA-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name
- %PIXPIX|ASA-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-4-405201: 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-4-406001: 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-4-407003: 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-4-409001: 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
- %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
- %PIX|ASA-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric : number area : string
- %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
- %PIX|ASA-4-409010: Virtual link information found in non-backbone area: string
- %PIX|ASA-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name
- %PIX|ASA-4-409012: Detected router with duplicate router ID IP_address in area string
- %PIX|ASA-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address
- %PIX|ASA-4-409023: Attempting AAA Fallback method method_name for request_type request for user user :Auth-server group server_tag unreachable
- %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.
- %PIX|ASA-4-411001:Line protocol on interface interface_name changed state to up
- %PIX|ASA-4-411002:Line protocol on interface interface_name changed state to down
- %PIX|ASA-4-411003: Configuration status on interface interface_name changed state to downup
- %PIX|ASA-4-411004: Configuration status on interface interface_name changed state to up
- %PIX|ASA-4-412001:MAC MAC_address moved from interface_1 to interface_2
- %PIX|ASA-4-412002:Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num
- %PIX|ASA-4-415012:internal_sig_id HTTP Deobfuscation signature detected - action HTTP deobfuscation detected IPS evasion technique from source_address to source_address
- %PIX|ASA-4-415014:internal_sig_id Maximum of 10 unanswered HTTP requests exceeded from source_address to dest_address

- %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
- %PIX|ASA-4-417001: Unexpected event received: number
- %PIX|ASA-4-417004: Filter violation error: conn number (string:string) in string
- %PIX|ASA-4-417006: No memory for string) in string. Handling: string
- %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-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-4-500004: Invalid transport field for protocol=protocol, from source_address/source_port to dest_address/dest_port
- %PIX|ASA-4-612002: Auto Update failed:filename, version:number, reason:reason
- %PIX|ASA-4-612003:Auto Update failed to contact:url, reason:reason
- %PIX|ASA-4-620002: Unsupported CTIQBE version: hex: from interface_name:IP_address/port to interface_name:IP_address/port
- %PIX|ASA-4-713154: DNS lookup for peer_description Server [server_name] failed!
- %PIX|ASA-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.
- %PIX|ASA-4-713903:Descriptive_event_string.
- %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
- %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-4-720072: (VPN-unit) Cannot find trust point tp
- %ASA4-720073: (VPN-unit) Fail to insert certificate in trust point trustpoint on the standby unit.

通知メッセージ、重大度 5

次のメッセージが重大度 5（通知）で表示されます。

- %PIX|ASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %PIX|ASA-5-109029: Parsing downloaded ACL: string
- %PIX|ASA-5-111002: Begin configuration: IP_address reading from device
- %PIX|ASA-5-111003: IP_address Erase configuration
- %PIX|ASA-5-111004: IP_address end configuration: {FAILED|OK}
- %PIX|ASA-5-111005: IP_address end configuration: OK
- %PIX|ASA-5-111007: Begin configuration: IP_address reading from device.
- %PIX|ASA-5-111008: User user executed the command string
- %PIX|ASA-5-199001: Reload command executed from telnet (remote IP_address).
- %PIX|ASA-5-199006: Orderly reload started at when by whom. Reload reason: reason
- %PIX|ASA-5-1999007:IP detected an attached application using port port while removing context
- %PIX|ASA-5-1999008:Protocol detected an attached application using local port local_port and destination port dest_port
- %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.
- %PIX|ASA-5-415001:internal_sig_id HTTP Tunnel detected - action tunnel_type from source_address to dest_address
- %PIX|ASA-5-415002:internal_sig_id HTTP Instant Messenger detected - action instant_messenger_type from source_address to dest_address
- %PIX|ASA-5-415003:internal_sig_id HTTP Peer-to-Peer detected - action peer_to_peer_type from source_address to dest_address
- %PIX|ASA-5-415005:Internal_Sig_Id Content type does not match specified type - Action Content Verification Failed from source_address to Dst_IP_Address
- %PIX|ASA-5-415007:internal_sig_id HTTP Extension method illegal - action 'method_name' from source_address to dest_address
- %PIX|ASA-5-415008:internal_sig_id HTTP RFC method illegal - action 'method_name' from source_address to dest_address
- %PIX|ASA-5-415010:internal_sig_id HTTP protocol violation detected - action HTTP Protocol not detected from source_address to dest_address
- %PIX|ASA-5-415013:internal_sig_id HTTP Transfer encoding violation detected - action Xfer_encode Transfer encoding not allowed from source_address to dest_address
- %PIX|ASA-5-500001: ActiveX content modified src IP_address dest IP_address on interface interface_name.
- %PIX|ASA-5-500002: Java content modified src IP_address dest IP_address on interface interface_name.
- %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
- %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-5-506001: event_source_string event_string
- %PIX|ASA-5-501101: User transitioning priv level
- %PIX|ASA-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string
- %PIX|ASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string
- %PIXPIX|ASA-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level
- %PIXPIX|ASA-5-502111: New group policy added: name: policy_name Type: policy_type
- %PIXPIX|ASA-5-502112: Group policy deleted: name: policy_name Type: policy_type
- %PIXPIX|ASA-5-503001: Process number, Nbr IP_address on interface_name from string to string, reason
- %PIXPIX|ASA-5-504001: Security context context_name was added to the system
- %PIXPIX|ASA-5-504002: Security context context_name was removed from the system
- %PIXPIX|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-5-611103: 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.
- %PIX|ASA-5-713136: IKE session establishment timed out [IKE_state_name], aborting!
- %PIX|ASA-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!
- %PIX|ASA-5-713139: group_name not found, using BASE GROUP default preshared key
- %PIX|ASA-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction
- %PIX|ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: netmask
- %PIX|ASA-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure. Resetting any Backup Server init.
- %PIX|ASA-5-713156: Initializing Backup Server [server_name or IP_address]
- %PIX|ASA-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP
- %PIX|ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %PIX|ASA-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload
- %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!
- %PIX|ASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.
- %PIX|ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter_value)!
- %PIX|ASA-5-713216: Rule: action Client type : version Client: type version is/is not allowed
- %PIX|ASA-5-713229: Auto Update - Notification to client client_ip of update string: message_string.
- %PIX|ASA-5-109029: Parsing downloaded ACL: string
- %PIX|ASA-5-713237: ACL update (access_list) received during re-key re-authentication will not be applied to the tunnel.
- %PIX|ASA-5-713904: Descriptive_event_string.
- %PIX|ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer
- %PIX|ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %PIX|ASA-5-718002: Create peer IP_address failure, already at maximum of number_of_peers
- %PIX|ASA-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-5-718048: 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-7-718056: Deleted Master peer, IP IP_address
- %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.
- %PIX|ASA-5-718070: Reset VPN Load Balancing in context context_ID.
- %PIX|ASA-5-718071: Terminate VPN Load Balancing in context context_ID.
- %PIX|ASA-5-718072: Becoming master of Load Balancing in context context_ID.
- %PIX|ASA-5-718073: Becoming slave of Load Balancing in context context_ID.
- %PIX|ASA-5-718074: Fail to create access list for peer context_ID.
- %PIX|ASA-5-718075: Peer IP_address access list not set.
- %PIX|ASA-5-718076: Fail to create tunnel group for peer IP_address.
- %PIX|ASA-5-718077: Fail to delete tunnel group for peer IP_address.
- %PIX|ASA-5-718078: Fail to create crypto map for peer IP_address.
- %PIX|ASA-5-718079: Fail to delete crypto map for peer IP_address.
- %PIX|ASA-5-718080: Fail to create crypto policy for peer IP_address.
- %PIX|ASA-5-718081: Fail to delete crypto policy for peer IP_address.
- %PIX|ASA-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address
- %PIX|ASA-5-718085: Interface interface_name has no IP address defined.
- %PIX|ASA-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.
- %PIX|ASA-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.

- %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
- %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.

情報メッセージ、重大度 6

次のメッセージが重大度 6（情報）で表示されます。

- %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-6-109001: 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.
- %PIX|ASA-6-109024: Authorization denied from source_address/source_port to dest_address/dest_port (not authenticated) on interface interface_name using protocol
- %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
- %PIX|ASA-6-110001: No route to dest_address from source_address
- %PIX|ASA-6-113003: AAA group policy for user user is being set to policy_name.
- %PIX|ASA-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user
- %PIX|ASA-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user
- %PIX|ASA-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %PIX|ASA-6-113007: User user unlocked by administrator
- %PIX|ASA-6-113008: AAA transaction status ACCEPT: user = user
- %PIX|ASA-6-113009: AAA retrieved default group policy policy for user user
- %PIX|ASA-6-113010: AAA challenge received for user user from server server_IP_address
- %PIX|ASA-6-113011: AAA retrieved user specific group policy policy for user user
- %PIX|ASA-6-113012: AAA user authentication Successful: local database : user = user
- %PIX|ASA-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %PIX|ASA-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user
- %PIX|ASA-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user
- %PIX|ASA-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user
- %PIX|ASA-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.
- %PIX|ASA-6-199002: startup completed. Beginning operation.
- %PIX|ASA-6-199003: Reducing link MTU dec.
- %PIX|ASA-6-199005: Startup begin
- %PIX|ASA-6-210022: LU missed number updates
- %PIX|ASA-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port
- %PIX|ASA-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|ASA-6-303002: source_address {Stored|Retrieved} dest_address: mapped_address
- %PIX|ASA-6-303003: FTP cmd_name command denied - failed strict inspection, terminating connection from source_interface:source_address/source_port to dest_interface:dest_address/dest_port
- %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 rcv thread up
- %PIX|ASA-6-311004: LU xmit thread up
- %PIX|ASA-6-312001: RIP hdr failed from IP_address: cmd=string, version=number domain=string on interface interface_name
- %PIX|ASA-6-314001: Pre-allocate RTSP UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
- %PIX|ASA-6-315011: SSH session from IP_address on interface interface_name for user user disconnected by SSH server, reason: reason
- %PIX|ASA-6-321003: Resource var1 log level of var2 reached.
- %PIX|ASA-6-321004: Resource var1 rate log level of var2 reached
- %PIXPIX|ASA-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface_name AC:ac_name.
- %PIX|ASA-6-415011:internal_sig_id HTTP URL Length exceeded. Received size byte URL - action URI length exceeded from source_address to dest_address
- %PIXPIX|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)
- %PIXPIX|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-6-603101: 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
- %PIX|ASA-6-603109: Teardown PPPOE Tunnel at interface_name, tunnel-id = number, remote-peer = IP_address

- %PIX|ASA-6-604101: DHCP client interface interface_name: Allocated ip = IP_address, mask = netmask, gw = gateway_address
- %PIX|ASA-6-604102: DHCP client interface interface_name: address released
- %PIX|ASA-6-604103: DHCP daemon interface interface_name: address granted MAC_address (IP_address)
- %PIX|ASA-6-604104: DHCP daemon interface interface_name: address released
- %PIX|ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username"
- %PIX|ASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user "username"
- %PIX|ASA-6-606001: ASDM session number number from IP_address started
- %PIX|ASA-6-606002: ASDM session number number from IP_address ended
- %PIX|ASA-6-606003: ASDM logging session number id from IP_address started id session ID assigned
- %PIX|ASA-6-606004: ASDM logging session number id from IP_address ended
- %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
- %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
- %PIX|ASA-6-609001: Built local-host interface_name:IP_address
- %PIX|ASA-6-609002: Teardown local-host interface_name:IP_address duration time
- %PIX|ASA-6-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
- %PIX|ASA-6-611101: User authentication succeeded: Uname: user
- %PIX|ASA-6-611102: User authentication failed: Uname: user
- %PIX|ASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address
- %PIX|ASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling
- %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 ...
- %PIX|ASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask ...
- %PIX|ASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address
- %PIX|ASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed
- %PIX|ASA-6-611307: VPNClient: Head end : IP_address
- %PIX|ASA-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: VNPClient: XAUTH Succeeded: Peer: IP_address
- %PIX|ASA-6-611311: VNPClient: 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-6-620001: 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
- %PIX|ASA-6-621001: Interface interface_name does not support multicast, not enabled
- %PIX|ASA-6-621002: Interface interface_name does not support multicast, not enabled
- %PIX|ASA-6-621003: The event queue size has exceeded number
- %PIX|ASA-6-621006: Mrib disconnected, (IP_address,IP_address) event cancelled
- %PIX|ASA-6-621007: Bad register from interface_name:IP_address to IP_address for (IP_address, IP_address)
- %PIX|ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: netmask
- %PIX|ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask
- %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
- %PIX|ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port
- %PIX|ASA-6-713184: Client Type: Client_type Client Application Version: Application_version_string
- %PIX|ASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask

- %PIX|ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %PIX|ASA-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
- %PIX|ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %PIX|ASA-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.
- %PIX|ASA-6-713228: Assigned private IP address assigned_private_IP%PIX|ASA-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
- %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.
- %PIX|ASA-6-718003: Got unknown peer message message_number from IP_address, local version version_number, remote version version_number
- %PIX|ASA-6-718004: Got unknown internal message message_number
- %PIX|ASA-6-718013: Peer IP_address is not answering HELLO
- %PIX|ASA-6-718027: Received unexpected KEEPALIVE request from IP_address
- %PIX|ASA-6-718030: Received planned OOS from IP_address
- %PIX|ASA-6-718037: Master processed number_of_timeouts timeouts
- %PIX|ASA-6-718038: Slave processed number_of_timeouts timeouts
- %PIX|ASA-6-718039: Process dead peer IP_address
- %PIX|ASA-6-718040: Timed-out exchange ID exchange_ID not found
- %PIX|ASA-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-6-720014: (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.

デバッグメッセージ、重大度 7

次のメッセージが重大度 7（デバッグ）で表示されます。

- %PIX|ASA-7-109014: uauth_lookup_net fail for uauth_in()
- %PIX|ASA-7-109021: Uauth null proxy error
- %PIX|ASA-7-111009: User user executed cmd:string
- %PIX|ASA-7-199009: ICMP detected an attached application while removing a context
- %PIX|ASA-7-304005: URL Server IP_address request pending URL url
- %PIX|ASA-7-304009: Ran out of buffer blocks specified by url-block command
- %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: {TCP|UDP} 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

- %PIX|ASA-7-710005: {TCP|UDP} request discarded from source_address/source_port to interface_name:dest_address/service
- %PIX|ASA-7-710006: protocol request discarded from source_address to interface_name:dest_address
- %PIX|ASA-7-711001: debug_trace_msg
- %PIX|ASA-7-711002: Task ran for elapsed_time msecs, process = process_name
- %PIX|ASA-7-713024: Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713026: Transmitted local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713027: Transmitted remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713030: Transmitted local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713031: Transmitted remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %PIX|ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713039: Send failure: Bytes (number), Peer: IP_address
- %PIX|ASA-7-713040: Could not find connection entry and can not encrypt: msgid message_number
- %PIX|ASA-7-713052: User (user) authenticated.
- %PIX|ASA-7-713066: IKE Remote Peer configured for SA: SA_name
- %PIX|ASA-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %PIX|ASA-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %PIX|ASA-7-713103: Invalid (NULL) secret key detected while computing hash
- %PIX|ASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation
- %PIX|ASA-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-7-713236: 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-7-713905:Descriptive_event_string.
- %PIX|ASA-7-713906: debug_message
- %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
- %PIX|ASA-7-714007: IKE Initiator sending Initial Contact
- %PIX|ASA-7-714011: Description of received ID values
- %PIX|ASA-7-715001: Descriptive statement
- %PIX|ASA-7-715004: subroutine name() Q Send failure: RetCode (return_code)
- %PIX|ASA-7-715005: subroutine name() Bad message code: Code (message_code)
- %PIX|ASA-7-715006: IKE got SPI from key engine: SPI = SPI_value
- %PIX|ASA-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value
- %PIX|ASA-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address
- %PIX|ASA-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address
- %PIX|ASA-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data
- %PIX|ASA-7-715019: IKEGetUserAttributes: Attribute name = name
- %PIX|ASA-7-715020: construct_cfg_set: Attribute name = name
- %PIX|ASA-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle
- %PIX|ASA-7-715041: Received keep-alive of type keepalive_type, not the negotiated type
- %PIX|ASA-7-715042: IKE received response of type failure_type to a request from the IP_address utility

- %PIX|ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %PIX|ASA-7-715045: ERROR: malformed Keepalive payload
- %PIX|ASA-7-715046: constructing payload_description payload
- %PIX|ASA-7-715047: processing payload_description payload
- %PIX|ASA-7-715048: Send VID_type VID
- %PIX|ASA-7-715049: Received VID_type VID
- %PIX|ASA-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 rcv'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
- %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.
- %PIX|ASA-7-717024 Checking CRL from trustpoint: trustpoint name for purpose
- %PIX|ASA-7-717025 Validating certificate chain containing number of certs certificate(s).
- %PIX|ASA-7-717029 Identified client certificate within certificate chain. serial number: serial_number, subject name: subject_name.
- %PIX|ASA-7-717030 Found a suitable trustpoint trustpoint name to validate certificate.
- %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-7-718001: Internal interprocess communication queue send failure: code error_code
- %PIX|ASA-7-718017: Got timeout for unknown peer IP_address msg type message_type
- %PIX|ASA-7-718018: Send KEEPALIVE request failure to IP_address
- %PIX|ASA-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-7-718034: 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-7-718058: 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.
- %PIX|ASA-7-718029: Sent OOS indicator to IP_address
- %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.

■ デバッグメッセージ、重大度 7

- %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.



Numerics

4GE SSM 2-36 2-45

A

AAA

サーバ 2-24, 2-25, 2-32, 2-100, 2-101, 2-132, 2-150, 2-257, 2-259

認可 2-24

認証 2-30, 2-31, 2-32, 2-259

メッセージ 2-19, 2-20, 2-21, 2-22, 2-23, 2-24, 2-25, 2-29, 2-30, 2-31, 2-32, 2-33, 2-100, 2-101, 2-111, 2-132, 2-150

ABR

バックボーン エリアのない 2-76

access-list deny-flow-max コマンド 2-18

access-list コマンド 2-13, 2-18, 2-65, 2-250

deny-flow-max オプション 2-18

interval オプション 2-18

log オプション 2-17

UDP ポート 53 のトラフィックの許可 2-13, 2-18, 2-65, 2-250

省略 2-22

ACL

ACL_ID 2-226

ACL が設定されていない 2-196

deny 2-65

deny-flow 2-18

SoftNP エラー 2-253

WebVPN

ACL ID が見つかりません 2-258

解析エラー 2-219, 2-220, 2-257

ユーザ認可の失敗 2-258

暗号マップ 2-95, 2-167

解析エラー 2-23

空の ACL ダウンロード 2-22

拒否されたパケット 2-16

コンフィギュレーション エラー 2-23

サポートされていないフォーマット 2-33

失敗したチェック 2-24

スプリット トンネル ポリシー 2-179

ピアの IP アドレスが設定されていない 2-250

ピアのコンテキスト ID 2-250

プロキシ ID の不一致 2-196

メモリ不足のコンパイル 2-16

ロギングの一致 2-17

ActiveX オブジェクト、フィルタリング 2-124

ActiveX オブジェクトのフィルタリング 2-124

Adaptive Security Device Manager

ASDM を参照

ALLOW モードのまま、URL サーバ 2-67

ARP スプーフィング攻撃 2-80

ARP パケットの不一致 2-104

ARP ポイズニング攻撃 2-104

ASDM

リモート管理 1-26

ログの出力先 1-2

Auto Update URL 到達不能 2-145

C

Cisco Secure Policy Manager (Cisco Secure PM) 1-26

clear コマンド

config logging オプション 1-4

disabled 1-4, 1-21

level 1-4

local-host オプション 2-107

logging オプション

asdm 1-7

buffer 1-8

conduit コマンド 2-14

permit ICMP オプション 2-14

config コマンド 2-27

configure コマンド 2-28

- CSPM
Cisco Secure Policy Manager を参照
- CTIQBE
サポートされていないバージョン 2-148
接続オブジェクト割り当て済み 2-148
- D
- deny
IP スプーフィング 2-14
TCP (接続なし) 2-14
アドレスからアドレスまでの IP 2-13
外部からの着信 2-13
クエリーまたは応答による着信 UDP 2-13
セルフルート 2-13
着信 ICMP 2-14
着信 UDP 2-12
- DNS request for all records 攻撃 2-92
DNS zone transfer from high port 攻撃 2-92
DNS zone transfer 攻撃 2-92
DNS クエリーまたは応答が拒否される 2-13
DoS 攻撃 2-18, 2-22, 2-51, 2-107
DNS HINFO request 攻撃 2-92
- E
- Easy VPN リモート
SUA
disabled 2-143, 2-144
イネーブル化 2-142
XAUTH イネーブル化 2-144
スプリット ネットワーク エントリ重複 2-144
デバイス パススルー
disabled 2-144
イネーブル化 2-143
バックアップ サーバリスト
エラー 2-142
ダウンロード 2-141
ユーザ認証
disabled 2-143
イネーブル化 2-143
ロード バランシング クラスタ
切断 2-142
リダイレクト 2-142
- EMBLEM フォーマット
ログで使用 1-12
- embryonic limit exceeded 2-48
- F
- filter allow コマンド 2-67
filter コマンド
activex オプション 2-124
allow オプション 2-67
fixup protocol コマンド 2-19
Flood Defender 2-150
floodguard コマンド 2-21
fragmented ICMP traffic 攻撃 2-92
- FTP
データ接続失敗 2-49
メッセージ 2-65, 2-66, 2-67
- H
- H.225 2-105
H.245 2-60
H.245 接続
外部アドレス 2-60
H.323 2-60
サポートされていないパケットバージョン 2-154
バック接続、事前割り当て済み 2-60
H323 UDP バック接続の事前割り当て 2-60
HTTPS プロセス制限 2-23
- I
- ICMP
拒否されたパケット 2-14
変換作成の失敗 2-69
- IDB 初期設定 2-77
- interface
PPP virtual 2-58
virtual 2-58
- IP fragment attack 2-91
IP fragments overlap 攻撃 2-92
IP impossible packet 攻撃 2-92
ip verify reverse-path コマンド 2-15, 2-16
- IP アドレス
DHCP クライアント 2-134
DHCP サーバ 2-134

- IP アドレス / ポートから IP アドレス / ポートへの Auth
が失敗 2-19
- IP ルーティング テーブル
 - OSPF 不整合 2-76
 - 警告制限 2-75
 - 攻撃 2-18
 - 作成エラー 2-75
 - 制限超過 2-75
- IP ルート カウンタの減少の失敗 2-108
- IPSec
 - cTCP トンネル 2-274
 - L2TP-over-IPSec 接続 2-174
 - over UDP 2-183, 2-212
 - overTCP 2-211
 - Sa 2-166, 2-171, 2-175, 2-205, 2-206, 2-214
 - プロポーザル 2-215
 - 暗号化 2-205
 - キー再生成の時間 2-168, 2-169
 - 拒否された要求 2-174
 - 接続 2-29, 2-30, 2-31, 2-32, 2-33, 2-231
 - L2TP-over-IPSec 2-174
 - 失敗 2-230
 - 接続エントリ 2-174
 - トンネル 2-29, 2-74, 2-165, 2-187, 2-230, 2-245
 - ネゴシエーション 2-166
 - パケット 2-94, 2-95
 - パケットに不足 2-94
 - フラグメンテーション ポリシーは無視される
2-188
 - プロキシのミスマッチ 2-65
 - プロトコル 2-159
 - プロポーザル
 - Sa 2-215
 - サポートされていない 2-215
 - 無効なパケット 2-94
- L
- L2TP
 - トンネル 2-133
- Land 攻撃 2-15
- Large ICMP traffic 攻撃 2-92
- lash 1-9
- logging queue
 - キュー統計情報の表示 1-8
 - サイズの変更 1-8
- 設定 1-8
- logging コマンド
 - asdm オプション 1-7
 - asdm-buffer-size オプション 1-7
 - buffered オプション 1-5, 1-8, 1-16
 - class オプション 1-10, 1-11
 - メッセージクラス変数 1-11
 - console オプション 1-6, 1-14
 - device-id オプション 1-12, 1-17
 - emblem オプション 1-12
 - enable オプション 1-3, 1-13
 - facility オプション 1-6, 1-17
 - flash-bufferwrap オプション 1-9
 - flash-maximum-allocation オプション 1-9
 - flash-minimum-free オプション 1-9
 - format emblem オプション 1-2
 - from-address オプション 1-6, 1-17
 - ftp-bufferwrap オプション 1-9
 - ftp-server オプション 1-9
 - history オプション 1-7, 1-20
 - host オプション 1-6, 1-16
 - list オプション 1-10, 1-15
 - mail オプション 1-6, 1-17
 - message オプション 1-4
 - monitor オプション 1-7, 1-18, 1-19
 - on オプション 1-3
 - queue オプション 1-8
 - recipient-address オプション 1-6, 1-18
 - savelog オプション 1-9
 - timestamp オプション 1-12
 - trap オプション 1-6, 1-17
- 基本的な使用方法 1-3
- 出力先
 - syslog サーバ 1-16
 - syslog メッセージサーバ 1-16
 - Telnet コンソールセッション 1-18
 - 指定 1-15
 - 電子メール アドレス 1-17
 - 内部バッファ 1-15
- 設定モード 1-2
- ディセーブル状態のメッセージのリストの表示
1-21
- メッセージ リストの作成 1-2
- メッセージをグループで設定 1-2
 - 重大度ごと 1-2, 1-10
 - メッセージクラスごと 1-11

- メッセージ リストごとに 1-2
- 例 1-13
 - ディセーブル状態のメッセージすべての再イネーブル化 1-21
 - ディセーブル状態のメッセージの再イネーブル化 1-21
 - 特定のメッセージのディセーブル化 1-21
 - ロギングのイネーブル化 1-13
 - ロギング出力のテスト 1-14
- LSA
 - 誤りのあるマスクのデフォルト 2-110
 - 検出されない 2-76
 - 無効なタイプ 2-109
- M
 - MAC アドレスの不一致 2-104
 - Microsoft Point-to-Point Encryption
 - MPPE を参照
 - MPPE
 - 暗号化ポリシーの設定 2-100, 2-101
 - MS-CHAP 2-100
 - 認証 2-100
- N
 - nat コマンド 2-68
- O
 - OSPF
 - IDB 初期設定 2-77
 - IP ルーティング テーブルの不整合 2-76
 - LSA
 - 誤りのあるマスクのデフォルト 2-110
 - 検出されない 2-76
 - 無効なタイプ 2-109
 - router-id リセット 2-77
 - エリアが変更されたネットワーク範囲 2-146
 - 仮想リンク 2-77
 - 近接状態が変更された 2-126
 - コンフィギュレーションの変更 2-146
 - 重複ルータ ID を持つ hello パケット 2-110
 - チェックサム エラー 2-145
 - バックボーン エリアのない ABR 2-76
 - プロセス リセット 2-77
 - 未知の近隣からの hello 2-109
 - 未知の近隣からのデータベース記述 2-109
 - 未知の近隣からのデータベース要求 2-109
 - 無効な長さのパケット 2-109
 - 無効なパケット 2-109
 - ルータ ID の割り当ての失敗 2-110
 - out of address translation slots! 2-50
 - outbound deny コマンド 2-12
- P
 - PAT
 - アドレス 2-50, 2-104, 2-105
 - グローバル アドレス 2-14
 - 指定されていないホスト 2-14
 - PAT ホストを指定できない 2-14
 - ping of death attack 2-92
 - PPP 仮想インターフェイス 2-58
 - PPTP
 - XGRE パケット 2-99
 - トンネル 2-57, 2-133
 - 間違った順番のパケット 2-132
 - proxied RPC request 攻撃 2-92
 - PSec
 - IKE を起動したパケット 2-164
- R
 - RADIUS 認証 2-100
 - RCMD、バック接続失敗 2-49
 - reload コマンド 2-28, 2-45
 - router-ID リセット 2-77
 - rsh コマンド 2-49
- S
 - SETUP メッセージ 2-105
 - show static コマンド 2-48
 - show コマンド
 - blocks オプション 2-7
 - failover オプション 2-55, 2-271
 - local-host オプション 2-107
 - logging asdm オプション 1-7
 - logging message オプション 1-4, 1-21
 - logging queue オプション 1-8

- logging オプション 1-3
 - outbound オプション 2-12
 - static オプション 2-48
 - version オプション 2-107
 - SIP 接続 2-136
 - skinny 接続 2-137
 - SMTP 2-19
 - SNMP
 - 管理ステーション 1-2
 - 出力先 1-20
 - トラップ 1-26
 - リモート管理 1-26
 - snmp-server コマンド
 - community オプション 1-20
 - contact オプション 1-20
 - enable traps オプション 1-20
 - host オプション 1-20
 - location オプション 1-20
 - SPI 2-94
 - SSH 2-74
 - SSM 4GE 2-36 2-45
 - statd buffer overflow 攻撃 2-93
 - SUA
 - disabled 2-143
 - イネーブル化 2-142
 - SYN 2-14
 - 攻撃 2-48
 - フラグ 2-14
 - syslog サーバ 1-16
- T
- TCP
 - connection limit exceeded 2-157
 - アクセスの許可 2-156
 - アクセスの要求 2-156
 - 誤ったヘッダー長 2-124
 - 接続 2-156
 - テーブル内に関連する接続がない 2-14
 - 変換作成の失敗 2-69
 - 要求の廃棄 2-157
 - TCP FIN only flags 攻撃 2-92
 - TCP NULL flags 攻撃 2-92
 - TCP SYN+FIN flags 攻撃 2-92
 - Telnet
 - リモート管理 1-26
 - ~を介してログにアクセス 1-18
 - terminal monitor コマンド 1-19
 - timeout uauth コマンド 2-21
- U
- UDP
 - bomb attack 2-92
 - chargen DoS attack 2-92
 - snork attack 2-92
 - アクセスの許可 2-156
 - 接続 2-156
 - パケット 2-13
 - 変換作成の失敗 2-69
 - メッセージ 2-68
 - 要求の廃棄 2-157
 - URL
 - サーバ 2-66
 - バッファ ブロック領域 2-67
 - フィルタリング、ディセーブル 2-67
- V
- vpdn group コマンド 2-100
 - VPN
 - トンネル 2-74
 - ピアの上限 2-74
 - VPN フェールオーバー
 - CTCP フロー処理のエラー 2-268
 - SDI ノード シークレット ファイルの同期に失敗した 2-272
 - アクティブ装置からのメッセージの受信に失敗した 2-271
 - 状態アップデートメッセージの失敗 2-269
 - 初期化の失敗 2-260
 - スタンバイ装置が、アクティブ装置から破損したメッセージを受信した 2-269
 - タイマー エラー 2-263
 - チャンクの割り当ての失敗 2-261
 - ディセーブルになっているクライアント 2-262
 - 登録の失敗 2-261
 - トラストポイントが見つからない 2-265
 - トラストポイント証明書の失敗 2-263
 - バージョン コントロール ブロックの失敗 2-262
 - ブロックされていないメッセージが送信されない 2-265

- メッセージキューに追加できない 2-268
 - メモリ割り当てのエラー 2-262
- W
- Web ブラウザにログをダウンロード 1-2
 - Web 要求、フィルタリングされずに 2-67
 - Websense サーバ 2-66, 2-67
 - write erase コマンド 2-27
 - write コマンド 2-27
 - erase オプション 2-27
 - standby オプション 2-54
 - standby コマンド 2-54
- X
- XAUTH イネーブル化 2-144
 - XGRE、プロトコル フィールドが無効なパケット 2-99
- あ
- 相手装置とのフェールオーバー通信障害 2-6
 - アクセスリスト
 - 「ACL」を参照
 - アクセスの許可 2-156
 - アクセスの要求 2-156
 - アドレス変換スロット 2-105
 - 利用できない 2-50, 2-104, 2-105
 - アドレス変換スロット、利用できない 2-50
- い
- インターネット電話、使用の検出 2-60
 - インターネット電話の使用を検出 2-60
 - インターフェイス
 - ゼロ帯域幅 2-145
- え
- エコー要求の廃棄 2-14
 - エリア境界ルータ
 - 「ABR」を参照
- お
- 遅すぎる DNS サーバ 2-13
- か
- 確立された H245 接続 2-60
 - 仮想インターフェイス 2-58
 - 仮想リンク 2-77
- き
- キュー、ロギング
 - キュー統計情報の表示 1-8
 - サイズの変更 1-8
 - 拒否されたアクセス
 - URL 2-66
 - 拒否された着信 TCP 接続 2-12
- こ
- 攻撃
- ARP スプーフィング 2-80
 - ARP ポイズニング 2-104
 - DNS HINFO request 2-92
 - DNS request for all records 2-92
 - DNS zone transfer 2-92
 - DNS zone transfer from high port 2-92
 - DoS 2-18, 2-22, 2-51, 2-103, 2-107
 - fragmented ICMP traffic 2-92
 - HTTP 回避 2-119
 - IP fragment 2-91
 - IP fragments overlap 2-92
 - IP impossible packet 2-92
 - IP ルーティング テーブル 2-18
 - Land 2-15
 - Large ICMP traffic 2-92
 - ping of death 2-92
 - proxied RPC request 2-92
 - statd buffer overflow 2-93
 - SYN 2-48
 - TCP FIN only flags 2-92
 - TCP NULL flags 2-92
 - TCP SYN+FIN flags 2-92
 - UDP bomb 2-92
 - UDP chargen DoS 2-92

UDP snork 2-92
 スプーフィング 2-14, 2-15, 2-16, 2-80, 2-104
 中間者 2-79
 不審な電子メール アドレスのパターン 2-19
 コンソール
 テストの出力先 1-14
 ログの出力先 1-6
 コンフィギュレーション 1-2
 erase 2-27
 ステータスが変化しました 2-112
 設定
 デフォルト値に復元 1-4
 表示 1-3
 複製
 開始 2-154
 失敗 2-154
 メッセージをグループで設定 1-2
 モード 1-2
 アクセス 1-2

 さ

 再確立された TCP 接続 2-60

 し

 システム管理、リモート 1-26
 重大度、メッセージの
 定義 1-22
 メッセージの重大度の変更 1-2
 リスト 1-22
 重複ルータ ID を持つ hello パケット 2-110
 出力先 1-2
 ASDM 1-2, 1-7
 SNMP 管理ステーション 1-2, 1-7, 1-20
 syslog メッセージ サーバ 1-2, 1-6, 1-16
 Telnet コンソール セッション
 指定 1-18
 設定例 1-18
 Telnet または SSH セッション 1-2, 1-7, 1-18
 コマンドの例
 syslog サーバ 1-16, 1-17
 Telnet コンソール 1-18
 内部バッファ 1-15
 コンソール 1-2, 1-6, 1-14
 出力先の指定 1-5, 1-15, 1-17, 1-20

設定するコマンド 1-5
 電子メール アドレス 1-2, 1-6, 1-17
 内部バッファ 1-2, 1-5, 1-8, 1-9, 1-15
 現行内容のフラッシュへの保存 1-9
 出力先の指定 1-8
 使用するフラッシュ量の指定 1-9
 内容の消去 1-8
 ログの表示 1-2, 1-5

す

スタティックの接続が多すぎる 2-48
 ステートフル フェールオーバー 2-53, 2-54, 2-55
 スプーフィング攻撃 2-14, 2-15, 2-16, 2-104
 スプリット ネットワーク エントリ重複 2-144

せ

セキュリティ

コンテキスト

削除 2-126
 追加 2-126
 判定できないコンテキスト 2-17

侵犯 2-13

パラメータ インデックス

SPI を参照

ポリシー管理 1-26

接続メッセージ 2-12, 2-13, 2-60
 接続制限の超過 2-48, 2-157
 接続テーブル内に関連する接続がない 2-14
 セルフ ルート 2-13

た

帯域幅

ゼロと報告 2-145

タイムアウト、推奨値 2-107
 タイムスタンプ、メッセージに含める 1-12

ち

中間者攻撃 2-79

- て
- 敵対イベント 2-15, 2-94, 2-95, 2-101
 - 欺かれたファイアウォール 2-15
 - テスト
 - インターフェイス 2-7
 - ロギング出力 1-14
 - デバイス ID
 - メッセージに含める 1-12
 - デバイス パススルー
 - disabled 2-144
 - イネーブル化 2-143
 - 電源障害、フェールオーバー 2-3
 - 電子メール アドレスの置き換えられた無効な文字 2-19
- と
- 特定のメッセージの再イネーブル化 1-21
 - 特権レベル、変更された 2-125
 - トンネル、PPTP 2-57
- な
- 内部バッファ 1-8
 - 現行内容のフラッシュへの保存 1-9
 - 内容の消去 1-8
 - バッファラップ
 - FTP サーバへの送信 1-9
 - フラッシュに保存 1-9
 - バッファラップに使用するフラッシュ量の指定 1-9
- に
- 認可
 - コマンド 2-138
 - ユーザ 2-138
 - ユーザ拒否 2-21
 - 認証
 - 応答 2-132
 - 検出されない 2-20
 - 失敗 2-20
 - 要求 2-132
 - 要求の成功 2-20
 - 認証サーバが見つからない 2-20
 - 認証セッションの終了 2-21
- は
- 排除 2-94
 - バケット
 - 一致する発信 NAT 規則なし 2-68
 - 拒否された 2-12, 2-13, 2-14, 2-16
 - 整合性チェック 2-13
 - バックアップ サーバリスト
 - エラー 2-142
 - ダウンロード 2-141
 - バッファ、内部
 - 出力先 1-8
 - 内容の消去 1-8
 - バッファラップ
 - 保存先 1-2
 - バッファラップ
 - FTP サーバへの送信 1-2, 1-8, 1-9
 - フラッシュに保存 1-2, 1-9
 - ロギング バッファの設定 1-8
 - バッファラップの保存先 1-2
- ひ
- 非対称ルーティング 2-15
- ふ
- フェールオーバー
 - LAN インターフェイスのダウン 2-8
 - show failover コマンド 2-271
 - VPN フェールオーバー
 - CTCP フロー処理のエラー 2-268
 - SDI ノード シークレット ファイルの同期に失敗した 2-272
 - アクティブ装置からのメッセージの受信に失敗した 2-271
 - 状態アップデート メッセージの失敗 2-269
 - 初期化の失敗 2-260
 - スタンバイ装置が、アクティブ装置から破損したメッセージを受信した 2-269
 - タイマー エラー 2-263
 - チャンクの割り当ての失敗 2-261
 - ディセーブルになっているクライアント 2-262

- 登録の失敗 2-261
 - トラストポイントが見つからない 2-265
 - トラストポイント証明書の失敗 2-263
 - バージョン コントロール ブロックの失敗 2-262
 - バッファ エラー 2-264
 - ブロックされていないメッセージが送信されない 2-265
 - メッセージ キューに追加できない 2-268
 - メモリ割り当てのエラー 2-262
 - 相手装置が異なるシャーシを持つ 2-11
 - 相手装置がディセーブルの可能性 2-10
 - 相手装置との通信障害 2-6
 - 相手装置との動作モードのミスマッチ 2-11
 - 相手装置とのライセンスのミスマッチ 2-11
 - 相手装置に互換性のないソフトウェア 2-10
 - 相手装置のカード コンフィギュレーションのミスマッチ 2-11
 - インターフェイス リンクのダウン 2-10
 - 継続するフェールオーバー 2-9
 - ケーブル ステータス 2-2
 - ケーブルが接続されていない 2-2
 - ケーブル通信失敗 2-7
 - コンフィギュレーションの複製 2-8
 - コンフィギュレーションの複製に失敗 2-155
 - 障害ネットワーク インターフェイス 2-4
 - スタンバイ装置が同期化できない 2-8
 - ステートフル エラー 2-52
 - ステートフル フェールオーバー 2-53, 2-54, 2-55
 - 電源障害 2-3
 - 廃棄されたフェールオーバー コマンド 2-9
 - ピア LAN リンクのダウン 2-9
 - ピアの障害 2-4
 - フェールオーバー アクティブ コマンド 2-266
 - 複製が中断 2-9
 - プライマリ装置の障害 2-5
 - 不良ケーブル 2-2
 - ブロック割り当て失敗 2-7
 - リンク ステータス アップまたはダウン 2-6
 - フェールオーバー コマンド 2-5, 2-9
 - active オプション 2-4, 2-266
 - フェールオーバー メッセージ 2-2, 2-3, 2-5, 2-7, 2-154, 2-155
 - 不足したメモリ 2-50, 2-105
 - エラーの発生 2-50, 2-104
 - ブリッジ テーブル
 - いっぱい 2-113
 - ブロードキャスト、無効な送信元アドレス 2-14
- へ
- 変換グループが見つからない 2-68
 - 変数
 - メッセージ 1-22, 1-23
 - リスト 1-23
- ほ
- ホスト移動 2-112
 - ホスト制限 2-107
- む
- 無効な送信元アドレス 2-14
- め
- メッセージ
 - FTP 2-65 2-67
 - Mail Guard 2-19
 - SNMP 2-55
 - SSH 2-74
 - アラート ログ 2-18
 - 概要 1-22
 - クラス 1-10
 - クラスのリスト 1-11
 - グループで管理 1-10
 - 重大度ごと 1-10
 - メッセージ クラスごと 1-11
 - メッセージ リストの作成 1-10
 - ロギング クラスごと 1-10
 - グループで設定
 - 重大度ごと 1-2
 - メッセージ クラスごと 1-2
 - メッセージ リストごとに 1-2
 - 形式 1-22
 - コンポーネントの説明 1-22
 - 重大度 1-22
 - 概要 1-2
 - メッセージの重大度の変更 1-2
 - リスト 1-22
 - 重大度の変更 1-4

- 出力先 1-2, 1-15
 - ASDM 1-7
 - syslog メッセージ サーバ 1-2, 1-6
 - Telnet または SSH セッション 1-2
 - コンソール 1-2
 - 内部バッファ 1-2
 - 使用される変数 1-22, 1-23
 - ステートフル フェールオーバー 2-53, 2-54, 2-55
 - 接続関連 2-13, 2-48, 2-60
 - 内容および形式 1-12
 - 内容の変更
 - タイムスタンプを含める 1-12
 - デバイス ID を含める 1-12
 - リストの作成 1-10
 - 重大度ごと 1-10
 - メッセージ ID ごとに 1-10
 - メッセージクラスごと 1-10
 - ロギングのイネーブル化 1-3
 - ロギングのディセーブル化 1-2
 - ログの記録項目の指定 1-2
 - メッセージクラス
 - 概要 1-10
 - リスト 1-11
 - メッセージ ブロック割り当て失敗 2-7
 - メッセージの形式 1-22
 - メッセージの再イネーブル化 1-21
 - メッセージの重大度 1-2
 - リスト 1-22
 - メッセージの重大度の変更 1-4
 - メッセージのディセーブル化
 - すべてのロギング 1-3, 1-21
 - 特定のメッセージ ID 1-4, 1-21
 - メモリ
 - 破損 2-145
 - 不足 2-75
 - 不足した 2-50, 2-105
 - ブロックの枯渇 2-7
 - リーク 2-76
 - メモリ不足 2-75
 - 失敗した動作 2-75
- も
- モジュール管理 2-27
- ゆ
- ユーザ認証
 - disabled 2-143
 - イネーブル化 2-143
 - エラー 2-23
 - ユーザの Auth 開始 2-19
 - ユーザ名
 - 削除 2-125
 - 作成 2-125
- よ
- 要求の廃棄 2-157
- り
- リモート管理 1-26
 - ASDM 1-2, 1-26
 - Telnet および SSH 1-2
 - Telnet コンソール セッション 1-26
 - Telnet または SSH セッションを介して 1-2
 - Web ブラウザにログをダウンロード 1-2
 - リモートでのログの監視
 - ASDM 1-2
 - Telnet および SSH 1-2
 - Web ブラウザにダウンロード 1-2
 - リモートでのログの管理
 - Telnet または SSH セッションを介して 1-2
 - リンク ステータス「アップ」または「ダウン」 2-6
 - リンクステート アドバタイズメント
 - 「LSA」を参照
- る
- ルータ ID の割り当ての失敗 2-110
 - ループバック ネットワーク、無効な送信元アドレス 2-14
- ろ
- ロード バランシング クラスタ
 - 切断 2-142
 - リダイレクト 2-142
 - ロギング バッファ 1-8, 1-9
 - 設定 1-8

- バッファラップ 1-8
- ログインのイネーブル化 1-3, 1-13
- ログバッファラップ
 - FTP サーバへの送信 1-2
 - フラッシュに保存 1-2
- ログ、表示 1-3
- ログアウトされたユーザ 2-139
- ログの出力先
 - ASDM 1-2
 - SNMP 管理ステーション 1-7
 - syslog メッセージサーバ 1-2, 1-6
 - Telnet または SSH セッション 1-2, 1-7
 - コンソール 1-2
 - 指定 1-15
 - 電子メール アドレス 1-2, 1-6
 - 内部バッファ 1-2, 1-5
 - 内部バッファ ログイン
 - 出力先
 - 内部バッファ 1-2
- ログの表示
 - コンフィギュレーション 1-3
 - 出力先 1-2, 1-5