



Catalyst 6500 シリーズ スイッチ / Cisco 7600 シリーズ ルータ Firewall Services Module システム メッセージ ガイド

Version 3.1



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。添付されていない場合には、代理店にご連絡ください。

シスコシステムズが採用している 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の一部として、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、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されません。シスコシステムズおよびこれら各社は、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、または取引によって発生する、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、シスコシステムズ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システムズ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かねます。

CCSP、Cisco Square Bridge のロゴ、Follow Me Browsing、StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、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、VCO は、米国および他の国における 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 サイトで言及している他の商標はいずれも、それぞれの所有者のもので、「パートナー」という用語を使用しているも、シスコシステムズと他社とのパートナー関係を意味するものではありません。(0501R)

Catalyst 6500 シリーズスイッチ / Cisco 7600 シリーズルータ Firewall Services Module システム メッセージ ガイド
Copyright © 2006, Cisco Systems, Inc.
All rights reserved.



このマニュアルについて	xxix
マニュアルの目的	xxix
対象読者	xxix
マニュアルの構成	xxx
表記法	xxx
関連資料	xxx
マニュアルの入手方法	xxxi
Cisco.com	xxxi
Documentation DVD	xxxi
マニュアルの発注方法	xxxi
シスコ製品のセキュリティ	xxxii
シスコ製品のセキュリティ問題の報告	xxxii
テクニカル サポート	xxxiii
Cisco Technical Support Web サイト	xxxiii
Japan TAC Web サイト	xxxiii
Service Request ツールの使用	xxxiv
問題の重大度の定義	xxxiv
その他の資料および情報の入手方法	xxxv

CHAPTER 1

FWSM のログと SNMP の設定	1-1
SNMP の設定	1-2
SNMP の概要	1-2
SNMP のイネーブル化	1-4
ログの設定および管理	1-6
ログの概要	1-6
複数コンテキスト モードでのログ	1-6
ログのイネーブル化とディセーブル化	1-7
設定したすべての出力先へのログのイネーブル化	1-7
設定したすべての出力先へのログのディセーブル化	1-8
ログ設定の表示	1-8
ログの出力先の設定	1-9

ログの出力先の概要	1-9
出力先としての Syslog サーバの設定	1-10
出力先としての E メール アドレスの指定	1-12
出力先としての ASDM の指定	1-13
Telnet セッションによるログの表示	1-14
出力先としてのログバッファの指定	1-16
出力先に送信するシステム ログ メッセージのフィルタリング	1-18
メッセージ フィルタリングの概要	1-19
クラスによるシステム ログ メッセージのフィルタリング	1-19
カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング	1-20
ログ設定のカスタマイズ	1-22
ロギング キューの設定	1-22
システム ログ メッセージでの日付と時刻の表示	1-22
システム ログ メッセージでのデバイス ID の表示	1-23
EMBLEM フォーマットでのシステム ログ メッセージの生成	1-24
システム ログ メッセージのディセーブル化	1-24
システム ログ メッセージの重大度の変更	1-25
ログに使用できる内部フラッシュ メモリの容量の変更	1-26
システム ログ メッセージの概要	1-27
システム ログ メッセージのフォーマット	1-27
重大度	1-27
システム ログ メッセージで使用される変数	1-28
ロギング コマンドの一覧	1-30

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	2-19
108002	2-19
108003	2-19
109001	2-19
109002	2-20
109003	2-20
109005	2-20
109006	2-20
109007	2-21
109008	2-21
109010	2-21
109011	2-21
109012	2-21
109013	2-22
109014	2-22
109016	2-22
109017	2-22
109018	2-23
109019	2-23
109020	2-23
109021	2-23
109022	2-24
109023	2-24
109024	2-24
109025	2-24

109026	2-25
109027	2-25
109028	2-25
109030	2-25
109031	2-26
111003	2-26
111004	2-26
111005	2-27
111007	2-27
111008	2-27
111009	2-27
111111	2-27
112001	2-28
113001	2-28
113003	2-28
113004	2-28
113005	2-29
113006	2-29
113007	2-29
113008	2-29
113009	2-30
113010	2-30
113011	2-30
113012	2-30
113013	2-31
113014	2-31
113015	2-31
113016	2-31
113017	2-32
113018	2-32
113019	2-32
199001	2-33
199002	2-33
199003	2-33
199005	2-33
199006	2-34
199907	2-34
199908	2-34

199909	2-34	
メッセージ 201002 ~ 217001		2-35
201002	2-35	
201003	2-35	
201004	2-35	
201005	2-36	
201006	2-36	
201008	2-36	
201009	2-36	
201010	2-37	
202001	2-37	
202005	2-37	
202011	2-38	
208005	2-38	
209003	2-38	
209004	2-39	
209005	2-39	
210001	2-39	
210002	2-39	
210003	2-40	
210005	2-40	
210006	2-40	
210007	2-40	
210008	2-41	
210010	2-41	
210020	2-41	
210021	2-41	
210022	2-42	
211001	2-42	
211003	2-42	
212001	2-42	
212002	2-43	
212003	2-43	
212004	2-43	
212005	2-43	
212006	2-44	
214001	2-44	
215001	2-44	

217001	2-44		
メッセージ	302003 ~ 326028	2-45	
302003	2-45		
302004	2-45		
302009	2-45		
302010	2-46		
302012	2-46		
302013	2-46		
302014	2-46		
302015	2-47		
302016	2-48		
302017	2-48		
302018	2-49		
302019	2-49		
302020	2-49		
302021	2-50		
302022	2-50		
302023	2-50		
302302	2-50		
303002	2-50		
303003	2-51		
303004	2-51		
304001	2-51		
304002	2-51		
304003	2-51		
304004	2-52		
304005	2-52		
304006	2-52		
304007	2-52		
304008	2-52		
304009	2-53		
305005	2-53		
305006	2-53		
305007	2-54		
305008	2-54		
305009	2-54		
305010	2-55		
305011	2-55		

305012	2-55
308001	2-55
308002	2-55
311001	2-56
311002	2-56
311003	2-56
311004	2-56
312001	2-56
313001	2-57
313003	2-57
313004	2-57
314001	2-57
315004	2-58
315011	2-58
316001	2-60
317001	2-60
317002	2-60
317003	2-60
317004	2-60
317005	2-61
318001	2-61
318002	2-61
318003	2-61
318004	2-61
318005	2-62
318006	2-62
318007	2-62
318008	2-62
319001	2-62
319002	2-63
319003	2-63
319004	2-63
320001	2-63
321001	2-64
321002	2-64
321003	2-64
321004	2-64
322001	2-64

322002	2-65
322003	2-65
322004	2-65
323004	2-66
323005	2-66
324000	2-66
324001	2-67
324002	2-67
324003	2-68
324004	2-68
324005	2-68
324006	2-68
324007	2-69
325001	2-69
325002	2-69
326001	2-69
326002	2-70
326004	2-70
326005	2-70
326006	2-70
326007	2-71
326008	2-71
326009	2-71
326010	2-71
326011	2-71
326012	2-72
326013	2-72
326014	2-72
326015	2-72
326016	2-72
326017	2-73
326019	2-73
326020	2-73
326021	2-73
326022	2-73
326023	2-74
326024	2-74
326025	2-74

326026	2-74
326027	2-74
326028	2-75
メッセージ 400000 ~ 418001	2-76
402101	2-76
402102	2-76
402103	2-76
402106	2-77
404101	2-77
404102	2-77
405001	2-77
405101	2-78
405002	2-78
405101	2-78
405102	2-79
405103	2-79
405104	2-79
405105	2-79
405201	2-80
406001	2-80
406002	2-80
407001	2-80
407002	2-81
407003	2-81
408001	2-81
408002	2-82
409001	2-82
409002	2-82
409003	2-82
409004	2-83
409005	2-83
409006	2-83
409007	2-83
409008	2-83
409009	2-84
409010	2-84
409011	2-84
409012	2-84

409013	2-84	
409023	2-85	
410001	2-85	
411001	2-85	
411002	2-85	
411003	2-86	
411004	2-86	
412001	2-86	
412002	2-86	
413001	2-87	
413002	2-87	
413003	2-87	
413004	2-87	
414001	2-88	
414002	2-88	
416001	2-88	
417001	2-89	
417004	2-89	
417006	2-89	
418001	2-89	
419001	2-89	
420001	2-89	
メッセージ 500001 ~ 507001	2-90	
500001	2-90	
500002	2-90	
500003	2-90	
500004	2-91	
501101	2-91	
502101	2-91	
502102	2-91	
502103	2-91	
502111	2-92	
502112	2-92	
503001	2-92	
504001	2-92	
504002	2-92	
505001	2-93	
505002	2-93	

505003	2-93
505004	2-93
505005	2-93
505006	2-94
505007	2-94
506001	2-94
507001	2-94
メッセージ 602101 ~ 609002	2-95
602101	2-95
602102	2-95
602201	2-95
602202	2-95
602203	2-96
602301	2-96
602302	2-96
602303	2-96
602304	2-97
604101	2-97
604102	2-97
604103	2-97
604104	2-98
606001	2-98
606002	2-98
606003	2-98
606004	2-98
607001	2-99
608001	2-99
609001	2-99
609002	2-100
610001	2-100
610002	2-100
610101	2-100
612001	2-101
612002	2-101
612003	2-101
613001	2-101
613002	2-101
613003	2-102

614001	2-102	
614002	2-102	
615001	2-102	
615002	2-102	
616001	2-103	
617001	2-103	
617002	2-103	
617003	2-103	
617004	2-103	
620001	2-104	
620002	2-104	
621001	2-104	
621002	2-104	
621003	2-105	
621006	2-105	
621007	2-105	
メッセージ 701001 ~ 720073		2-106
701001	2-106	
701002	2-106	
702201	2-106	
702202	2-107	
702203	2-107	
702204	2-107	
702205	2-107	
702206	2-107	
702207	2-108	
702208	2-108	
702209	2-108	
702210	2-108	
702211	2-108	
702212	2-109	
702301	2-109	
702302	2-109	
702303	2-109	
703001	2-109	
703002	2-110	
709001、709002		2-110
709003	2-110	

709004	2-110
709005	2-111
709006	2-111
709007	2-111
710001	2-111
710002	2-112
710003	2-112
710004	2-112
710005	2-113
710006	2-113
711001	2-113
711002	2-113
713004	2-114
713006	2-114
713008	2-114
713009	2-114
713010	2-115
713012	2-115
713014	2-115
713016	2-115
713017	2-115
713018	2-116
713020	2-116
713022	2-116
713024	2-116
713025	2-116
713026	2-117
713027	2-117
713028	2-117
713029	2-117
713030	2-117
713031	2-118
713032	2-118
713033	2-118
713034	2-118
713035	2-118
713036	2-119
713037	2-119

713039	2-119
713040	2-119
713041	2-119
713042	2-120
713043	2-120
713047	2-120
713048	2-120
713049	2-120
713050	2-121
713051	2-121
713052	2-121
713056	2-121
713059	2-121
713060	2-122
713061	2-122
713062	2-122
713063	2-122
713065	2-123
713066	2-123
713068	2-123
713072	2-123
713073	2-123
713074	2-124
713075	2-124
713076	2-124
713078	2-124
713081	2-125
713082	2-125
713083	2-125
713084	2-125
713085	2-125
713086	2-126
713088	2-126
713092	2-126
713094	2-126
713098	2-127
713099	2-127
713102	2-127

713103	2-127
713104	2-127
713105	2-128
713107	2-128
713109	2-128
713112	2-128
713113	2-129
713114	2-129
713115	2-129
713116	2-129
713117	2-130
713118	2-130
713119	2-130
713120	2-130
713121	2-130
713122	2-131
713123	2-131
713124	2-131
713127	2-131
713128	2-132
713129	2-132
713130	2-132
713131	2-132
713132	2-133
713133	2-133
713134	2-133
713135	2-133
713136	2-133
713137	2-134
713138	2-134
713139	2-134
713140	2-134
713141	2-135
713142	2-135
713143	2-135
713144	2-135
713145	2-136
713146	2-136

713147	2-136
713148	2-136
713149	2-137
713152	2-137
713154	2-137
713155	2-137
713156	2-138
713157	2-138
713158	2-138
713159	2-138
713160	2-139
713161	2-139
713162	2-139
713163	2-139
713164	2-140
713165	2-140
713166	2-140
713167	2-140
713168	2-141
713169	2-141
713170	2-141
713171	2-141
713172	2-141
713174	2-142
713176	2-142
713177	2-142
713178	2-142
713179	2-142
713182	2-143
713184	2-143
713185	2-143
713186	2-143
713187	2-144
713189	2-144
713190	2-144
713193	2-144
713194	2-144
713195	2-145

713196	2-145
713197	2-145
713198	2-145
713199	2-145
713203	2-146
713204	2-146
713205	2-146
713206	2-146
713208	2-147
713209	2-147
713210	2-147
713211	2-147
713212	2-148
713213	2-148
713214	2-148
713215	2-149
713216	2-149
713217	2-149
713218	2-149
713219	2-150
713220	2-150
713221	2-150
713222	2-150
713223	2-150
713224	2-151
713225	2-151
713226	2-151
713229	2-151
713236	2-152
713229	2-152
713900	2-152
713901	2-152
713902	2-153
713903	2-153
713904	2-153
713905	2-153
713906	2-153
714001	2-154

714002	2-154
714003	2-154
714004	2-154
714005	2-154
714006	2-155
714007	2-155
714011	2-155
715001	2-155
715004	2-155
715005	2-156
715006	2-156
715007	2-156
715008	2-156
715009	2-156
715013	2-157
715019	2-157
715020	2-157
715021	2-157
715022	2-157
715027	2-158
715028	2-158
715033	2-158
715034	2-158
715035	2-158
715036	2-159
715037	2-159
715038	2-159
715039	2-159
715040	2-159
715041	2-160
715042	2-160
715044	2-160
715045	2-160
715046	2-160
715047	2-161
715048	2-161
715049	2-161
715050	2-161

715051	2-161
715052	2-162
715053	2-162
715054	2-162
715055	2-162
715056	2-162
715057	2-163
715058	2-163
715059	2-163
715060	2-163
715061	2-164
715062	2-164
715063	2-164
715064	2-164
715065	2-165
715066	2-165
715067	2-165
715068	2-165
715069	2-166
715070	2-166
715071	2-166
715072	2-166
715074	2-167
715075	2-167
715076	2-167
715077	2-168
717001	2-168
717002	2-168
717003	2-169
717004	2-169
717005	2-169
717006	2-169
717007	2-169
717008	2-170
717009	2-170
717010	2-170
717011	2-170
717012	2-171

717013	2-171
717014	2-171
717015	2-171
717016	2-172
717017	2-172
717018	2-172
717019	2-172
717022	2-173
717025	2-173
717028	2-173
717029	2-173
718001	2-174
718002	2-174
718003	2-174
718004	2-174
718005	2-175
718006	2-175
718007	2-175
718008	2-175
718009	2-176
718010	2-176
718011	2-176
718012	2-176
718013	2-176
718014	2-177
718015	2-177
718016	2-177
718017	2-177
718018	2-177
718019	2-178
718020	2-178
718021	2-178
718022	2-178
718023	2-178
718024	2-179
718025	2-179
718026	2-179
718027	2-179

718028	2-180
718029	2-180
718030	2-180
718031	2-180
718032	2-180
718033	2-181
718034	2-181
718035	2-181
718036	2-181
718037	2-182
718038	2-182
718039	2-182
718040	2-182
718041	2-182
718042	2-183
718043	2-183
718044	2-183
718045	2-183
718046	2-183
718047	2-184
718048	2-184
718049	2-184
718050	2-184
718051	2-184
718052	2-185
718053	2-185
718054	2-185
718055	2-185
718056	2-185
718057	2-186
718058	2-186
718059	2-186
718060	2-186
718061	2-186
718062	2-187
718063	2-187
718064	2-187
718065	2-187

718066	2-187
718067	2-188
718068	2-188
718069	2-188
718070	2-188
718071	2-188
718072	2-189
718073	2-189
718074	2-189
718075	2-189
718076	2-189
718077	2-190
718078	2-190
718079	2-190
718080	2-190
718081	2-190
718084	2-191
718085	2-191
718086	2-191
718087	2-191
718088	2-191
719001	2-192
719002	2-192
719003	2-192
719004	2-192
719005	2-193
719006	2-193
719007	2-193
719008	2-193
719009	2-193
719010	2-194
719011	2-194
719012	2-194
719013	2-194
719014	2-195
719015	2-195
719016	2-195
719025	2-195

719026	2-196
720001	2-196
720002	2-196
720003	2-196
720004	2-196
720005	2-197
720006	2-197
720007	2-197
720008	2-197
720009	2-198
720010	2-198
720011	2-198
720012	2-198
720013	2-199
720014	2-199
720015	2-199
720016	2-199
720017	2-200
720018	2-200
720019	2-200
720020	2-200
720021	2-201
720022	2-201
720023	2-201
720024	2-201
720025	2-202
720026	2-202
720027	2-202
720028	2-202
720029	2-203
720030	2-203
720031	2-203
720032	2-203
720033	2-204
720034	2-204
720035	2-204
720036	2-205
720037	2-205

720038	2-205
720039	2-206
720040	2-206
720041	2-206
720042	2-206
720043	2-207
720044	2-207
720045	2-207
720046	2-208
720047	2-208
720048	2-208
720049	2-208
720050	2-209
720051	2-209
720052	2-209
720053	2-210
720054	2-210
720055	2-210
720056	2-211
720057	2-211
720058	2-211
720059	2-211
720060	2-212
720061	2-212
720062	2-212
720063	2-212
720064	2-213
720065	2-213
720066	2-213
720067	2-214
720068	2-214
720069	2-214
720070	2-215
720071	2-215
720072	2-215
720073	2-216

APPENDIX A

重大度別のメッセージ A-1

alert メッセージ、重大度 1 A-2

critical メッセージ、重大度 2	A-4
error メッセージ、重大度 3	A-5
warning メッセージ、重大度 4	A-11
notification メッセージ、重大度 5	A-14
informational メッセージ、重大度 6	A-17
debugging メッセージ、重大度 7	A-22



このマニュアルについて

ここでは、次の事項について説明します。

- マニュアルの目的 (p.xxix)
- 対象読者 (p.xxix)
- マニュアルの構成 (p.xxx)
- 表記法 (p.xxx)
- 関連資料 (p.xxx)
- マニュアルの入手方法 (p.xxxi)
- テクニカル サポート (p.xxxiii)

マニュアルの目的

このマニュアルでは、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module*』ソフトウェア バージョン 3.1 で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。

対象読者

このマニュアルは、次の作業を担当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 セキュリティの管理
- 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

このマニュアルは、読者が『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』に記載されているコマンドおよび設定オプションについて知識があることを前提としています。また、FWSM が稼働してい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

このマニュアルの構成は、次のとおりです。

- **第1章「FWSMのログとSNMPの設定」** システムログメッセージ機能と、ログメッセージのフォーマットについて説明します。
- **第2章「システムログメッセージ」** システムログメッセージを示します。各メッセージについて、考えられる原因と、その状況への対処方法を説明します。
- **付録A「重大度別のメッセージ」** 重大度別にメッセージの番号とテキストを示します。

表記法

このマニュアルでは、次の表記法を使用しています。

- ファイル名、ディレクトリ名、およびユーザが値を指定する引数は、イタリック体で示しています。
- ^記号は、Ctrl キーを表します。たとえば、^z というキーの組み合わせは、Ctrl キーを押しながら z キーを押すことを意味します。
- 本文中のコマンド名、キー、ボタン、およびキーワードは、**太字**で示しています。FWSM のコマンドについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。
- コマンド構文中の変数は、イタリック体で示しています。角カッコ [] で囲まれたコマンドオプションは、省略可能です。一連のパラメータが縦棒 (|) で区切られている場合は、どれか1つを入力する必要があります。
- 例では、画面出力とコマンドラインを *screen* フォントで示しています。
- 例の中で、ユーザが入力しなければならない情報は、**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 アイテムの選択方法は、次のように表記しています。
screen1>screen2>screen3 の順にクリックします。



(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

このマニュアルは、次の URL にある FWSM マニュアル セットと併せてご利用ください。

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

マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。また、テクニカル サポートおよびその他のテクニカル リソースは、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

シスコの最新のマニュアルは、次の URL からアクセスしてください。

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

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

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

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

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

Documentation DVD

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。この DVD パッケージは、単独で入手することができます。

Cisco.com (Cisco Direct Customers) に登録されている場合、Ordering ツールまたは Cisco Marketplace から Cisco Documentation DVD (Customer Order 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

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

シスコ製品のマニュアルは、次の方法でご発注いただけます。

- Cisco.com (Cisco Direct Customers) に登録されている場合、Ordering ツールからシスコ製品の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。

シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

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

このサイトから、以下のタスクを実行できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告および注意のリストが以下の URL で確認できます。

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

勧告および注意事項が変更された際に、リアルタイムで確認したい場合は、以下の URL から Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) にアクセスできます。

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、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 security-alert@cisco.com
- 緊急度の低い問題 psirt@cisco.com



ヒント

お客様が第三者に知られたくない情報をシスコに送信する場合、Pretty Good Privacy (PGP) または PGP と互換性のある製品を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.x ~ 8.x と互換性のある暗号化情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際は、次の公開鍵サーバの一覧に記載されている有効な公開鍵を使用してください。

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

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

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

テクニカル サポート

Cisco Technical Support では、シスコシステムズとサービス契約を結んでいるお客様、パートナー、リセラー、販売店を対象として、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support Web サイトでは、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、Technical Assistance Center (TAC) では、電話でのサポートも提供しています。シスコシステムズとサービス契約を結んでいない場合は、リセラー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、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。Cisco Technical Support Web サイトは、1 年中いつでも利用することができます。次の URL にアクセスしてください。

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

Cisco Technical Support Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

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



(注)

テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification (CPI) ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する show コマンド出力のコピー & ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

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/>

Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカルサポートを受けられます(ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合)。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を自動的に提供します。これらの推奨リソースを使用しても問題が解決しない場合は、TAC の技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

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

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください(運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合)。S1 および S2 の問題には TAC の技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカルサポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋 : +61 2 8446 7411 (オーストラリア : 1 800 805 227)

EMEA : +32 2 704 55 55

米国 : 1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

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

問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1 (S1) ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2 (S2) ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3 (S3) ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4 (S4) シスコ製品の機能、インストレーション、基本的な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で、業務への影響がほとんどまたはまったくない場合。

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することができます。

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL から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、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。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テクニカル ユーザ向けの季刊誌で、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のに役立ちます。『Packet』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『Packet』には、次の URL からアクセスしてください。

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

- 『iQ Magazine』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『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、シスコシステムズ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>

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの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>



FWSM のログと SNMP の設定

この章では、FWSM に関するログと SNMP を設定する方法について説明します。さらに、システム ログ メッセージの内容とフォーマットについても説明します。

この章では、モニタリングおよびロギング用の全コマンドおよびオプションについて包括的に説明するわけではありません。詳しい説明とその他のコマンドについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

この章の内容は、次のとおりです。

- [SNMP の設定 \(p.1-2\)](#)
- [ログの設定および管理 \(p.1-6\)](#)

SNMP の設定

ここでは、SNMP の使用法について説明します。内容は次のとおりです。

- [SNMP の概要 \(p.1-2\)](#)
- [SNMP のイネーブル化 \(p.1-4\)](#)

SNMP の概要

FWSM では、SNMP V1 および V2c によるネットワーク モニタリングのサポートが提供されます。FWSM は、トラップおよび SNMP 読み取りアクセスをサポートしていますが、SNMP 書き込みアクセスはサポートしていません。

Network Management Station (NMS; ネットワーク管理ステーション) にトラップ (イベント通知) を送信するように FWSM を設定することも、NMS を使用して FWSM 上の MIB をブラウズすることもできます。MIB は定義の集合であり、FWSM は定義ごとに値のデータベースを 1 つずつ維持します。MIB をブラウズすると、NMS から SNMP get 要求が発行されます。SNMP トラップを受信したり MIB のブラウズするには、CiscoWorks for Windows、または SNMP V1、MIB-II に準拠する他の任意のブラウザを使用します。

表 1-1 に、FWSM でコンテキスト別に複数のモードでサポートされている MIB およびトラップを示します。シスコの MIB は、次の URL からダウンロードできます。

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

ダウンロードした MIB を、使用する NMS 用にコンパイルしてください。

表 1-1 SNMP MIB およびトラップのサポート

MIB またはトラップのサポート	説明
SNMP コア トラップ	FWSM は、次のコア SNMP トラップを送信します。 <ul style="list-style-type: none"> • authentication NMS が正しいコミュニティ スtring で認証できなかったため、SNMP 要求はエラーになります。 • linkup インターフェイスは「up」ステートに移行しました。 • linkdown インターフェイスがダウンしています (たとえば、<code>nameif</code> コマンドを削除した場合)。 • coldstart リロード後、FWSM が動作しています。
MIB-II	FWSM は、次のグループおよびテーブルのブラウズをサポートしています。 <ul style="list-style-type: none"> • system
IF-MIB	FWSM は、次のテーブルのブラウズをサポートしています。 <ul style="list-style-type: none"> • ifTable • ifXTable
RFC1213-MIB	FWSM は、次のテーブルのブラウズをサポートしています。 <ul style="list-style-type: none"> • ip.ipAddrTable
SNMPv2-MIB	FWSM は、次のブラウズをサポートしています。 <ul style="list-style-type: none"> • snmp

表 1-1 SNMP MIB およびトラップのサポート (続き)

MIB またはトラップのサポート	説明
ENTITY-MIB	FWSM は、次のグループおよびテーブルのブラウズをサポートしています。 <ul style="list-style-type: none"> entPhysicalTable entLogicalTable FWSM は、次のトラップのブラウズをサポートしています。 <ul style="list-style-type: none"> config-change fru-insert fru-remove
CISCO-IPSEC-FLOW-MONITOR-MIB	FWSM は、この MIB のブラウズをサポートしています。 FWSM は、次のトラップのブラウズをサポートしています。 <ul style="list-style-type: none"> start stop
CISCO-REMOTE-ACCESS-MONITOR-MIB	FWSM は、この MIB のブラウズをサポートしています。 FWSM は、次のトラップのブラウズをサポートしています。 <ul style="list-style-type: none"> session-threshold-exceeded
CISCO-CRYPTO-ACCELERATOR-MIB	FWSM は、この MIB のブラウズをサポートしています。
ALTIGA-GLOBAL-REG	FWSM は、この MIB のブラウズをサポートしています。
Cisco Firewall MIB	FWSM は、次のグループのブラウズをサポートしています。 <ul style="list-style-type: none"> cfwSystem この情報はフェールオーバー ステータスに関連する cfwSystem.cfwStatus であり、1つのコンテキストではなくデバイス全体に関係します。
Cisco Memory Pool MIB	FWSM は、次のテーブルのブラウズをサポートしています。 <ul style="list-style-type: none"> ciscoMemoryPoolTable このテーブルで記述されるメモリ使用状況は、ネットワーク プロセッサではなく、FWSM の汎用プロセッサだけに該当します。
Cisco Process MIB	FWSM は、次のテーブルのブラウズをサポートしています。 <ul style="list-style-type: none"> cpmCPUTotalTable
Cisco Syslog MIB	FWSM は、次のトラップをサポートしています。 <ul style="list-style-type: none"> clogMessageGenerated この MIB はブラウズできません。

SNMP のイネーブル化

FWSM 上で動作する SNMP エージェントは、次の 2 つの機能を実行します。

- NMS からの SNMP 要求への応答
- NMS へのトラップ (イベント通知) の送信

SNMP エージェントをイネーブルにして、FWSM に接続できる NMS を識別するには、次の作業を行います。

ステップ 1 次のコマンドを入力して、FWSM 上の SNMP サーバがイネーブルであることを確認します。

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

SNMP サーバは、デフォルトでイネーブルです。

ステップ 2 FWSM に接続できる NMS の IP アドレスを識別するには、次のコマンドを入力します。

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

NMS をトラップの受信のみ、またはブラウズ (ポーリング) のみに限定するには、**trap** または **poll** を指定します。デフォルトでは、NMS は両方の機能を使用できます。

SNMP トラップは、デフォルトでは UDP ポート 162 に送信されます。ポート番号を変更するには、**udp-port** キーワードを使用します。

ステップ 3 コミュニティ スtring を指定するには、次のコマンドを入力します。

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

SNMP コミュニティ スtring は、FWSM と NMS の共有秘密鍵です。この鍵は、32 文字以内で大文字と小文字の区別があります。スペースは使用できません。

ステップ 4 (任意) SNMP サーバのロケーションまたはコンタクト情報を設定するには、次のコマンドを入力します。

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

ステップ 5 FWSM が NMS にトラップを送信できるようにするには、次のコマンドを入力します。

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

このコマンドを機能タイプごとに入力して、個々のトラップまたはトラップの集合をイネーブルにします。**all** キーワードを入力すると、すべてのトラップがイネーブルになります。

デフォルトの設定では、すべての **snmp** トラップがイネーブルです (**snmp-server enable traps snmp authentication linkup linkdown coldstart**)。これらのトラップをディセーブルにするには、**snmp** キーワードとともに、このコマンドの **no** 形式を使用します。**clear configure snmp-server** コマンドを使用すると、デフォルトでイネーブルの SNMP トラップが復元されます。

このコマンドを入力し、トラップ タイプを指定しない場合、デフォルトは `syslog` です (`syslog` トラップとともに、デフォルトの `snmp` トラップが引き続きイネーブルになります)。

`snmp` トラップには、次のものが含まれます。

- `authentication`
- `linkup`
- `linkdown`
- `coldstart`

`entity` トラップには、次のものが含まれます。

- `config-change`
- `fru-insert`
- `fru-remove`

`ipsec` トラップには、次のものが含まれます。

- `start`
- `stop`

`remote-access` トラップには、次のものが含まれます。

- `session-threshold-exceeded`

ステップ 6 システム メッセージをトラップとして NMS に送信できるようにするには、次のコマンドを入力します。

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

前述の `snmp-server enable traps` コマンドを使用して、`syslog` トラップもイネーブルにする必要があります。

ステップ 7 ログをイネーブルにして、システム メッセージを生成し NMS に送信できるようにするには、次のコマンドを入力します。

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

次に、内部インターフェイス上のホスト 192.168.3.2 から要求を受信するように FWSM を設定する例を示します。

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

ログの設定および管理

ここでは、ログ機能および設定について説明します。また、システム ログ メッセージのフォーマット、オプション、および変数についても説明します。

- [ログの概要 \(p.1-6\)](#)
- [複数コンテキスト モードでのログ \(p.1-6\)](#)
- [ログのイネーブル化とディセーブル化 \(p.1-7\)](#)
- [ログの出力先の設定 \(p.1-9\)](#)
- [出力先に送信するシステム ログ メッセージのフィルタリング \(p.1-18\)](#)
- [ログ設定のカスタマイズ \(p.1-22\)](#)
- [システム ログ メッセージの概要 \(p.1-27\)](#)

ログの概要

FWSM のシステム ログは、FWSM のモニタおよびトラブルシューティングのためのログ情報を提供します。ログ設定は非常に柔軟性があり、FWSM によるシステム ログ メッセージの処理方法をさまざまにカスタマイズすることができます。

ログ機能を使用して、次のことが可能です。

- 記録する必要があるシステム ログ メッセージの指定
- システム ログ メッセージのディセーブル化または重大度の変更
- システム ログ メッセージを送信する 1 つまたは複数のロケーション (内部バッファ、Syslog サーバ、ASDM、SNMP 管理ステーション、特定の E メール アドレス、または Telnet および SSH セッション)
- 重大度やメッセージ クラスなど、グループ別のシステム ログ メッセージの設定および管理
- 内部バッファが満杯になり、ラップアラウンドしたときの動作の指定。バッファの内容を FTP サーバに送信するか、または内部フラッシュ メモリに保存するように FWSM を設定できます。
- FTP サーバへのログ ファイルの送信
- フラッシュ メモリへのログ ファイルの保存
- システム ログ メッセージのリモートからのモニタ (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)

全部または一部のシステム ログ メッセージを、全部または一部の出力先ロケーションに送信できます。システム ログ メッセージの重大度やクラスに応じて、またはカスタム ログ メッセージ リストを作成して、各ロケーションに送信するシステム ログ メッセージをフィルタできます。

複数コンテキスト モードでのログ

セキュリティ コンテキストごとに独自の設定があるように、セキュリティ コンテキストごとに独自のログ設定およびシステム メッセージ ログもあります。セキュリティ コンテキストのメッセージ ログには、そのコンテキストでイネーブルに設定される機能に関連するメッセージが含まれます。たとえば、コンテキスト ログには、そのコンテキストのセキュリティ ポリシー、ルーティング、および設定変更に関連するメッセージが含まれます。単一コンテキスト モードで動作する FWSM と同様、セキュリティ コンテキストでのログは、デフォルトではイネーブルではありません。セキュリティ コンテキストのログを保存するには、そのセキュリティ コンテキストにアクセスしてログ動作を設定する必要があります。同様に、セキュリティ コンテキストのログ メッセージを表示する場合にも、そのコンテキストにアクセスする必要があります。

system または admin コンテキストにログインし、他のコンテキストを変更すると、セッションで表示されるメッセージは現在コンテキストに関連するものだけになります。

システム実行スペースで生成されるシステム メッセージ (フェールオーバー メッセージを含む) は、admin コンテキストで生成されたメッセージとともに、admin コンテキストで表示されます。admin コンテキストのログを設定しイネーブルにすると、システム実行スペースで生成されるメッセージは、自動的に admin コンテキスト メッセージに含まれます。システム実行スペース内では、ログを設定したり、ログ情報を表示したりすることはできません。

各メッセージにセキュリティ コンテキストのロギング デバイス ID が含まれるようにログを設定することができます。その場合、各メッセージには、そのメッセージが発生したコンテキストの名前が含まれます。admin コンテキストのロギング デバイス ID をイネーブルにすると、システム実行スペースで発生したメッセージは「system」というデバイス ID を使用し、admin コンテキストで発生したメッセージはコンテキスト名をデバイス ID として使用します。ロギング デバイス ID についての詳細は、「システム ログ メッセージでのデバイス ID の表示」(p.1-23) を参照してください。

セキュリティ コンテキストについての詳細は、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』の「Enabling Multiple Context Mode」を参照してください。

ログのイネーブル化とディセーブル化

ここでは、FWSM でログをイネーブルおよびディセーブルにする方法について説明します。内容は次のとおりです。

- [設定したすべての出力先へのログのイネーブル化 \(p.1-7\)](#)
- [設定したすべての出力先へのログのディセーブル化 \(p.1-8\)](#)
- [ログ設定の表示 \(p.1-8\)](#)

設定したすべての出力先へのログのイネーブル化

ここでは、ログをイネーブルにする手順を示します。ただし、ロギングしたメッセージを表示または保存できるように、少なくとも1つの出力先を指定する必要があります。出力先を指定しない場合、イベントが発生しても、FWSM は生成されたシステム ログ メッセージを保存しません。

ログの出力先の設定については、「[ログの出力先の設定](#)」(p.1-9) を参照してください。

ログをイネーブルにするには、次の作業を行います。

ステップ 1 次のコマンドを入力し、コンフィギュレーション モードにアクセスします。

```
hostname># config t
```

ステップ 2 次のコマンドを入力し、ログを開始します。

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

ステップ3 どのタイプのログがイネーブルになっているかを表示するには、次のコマンドを入力します。

```
hostname(config)# show logging
Syslog logging: enabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: disabled
  History logging: disabled
  Device ID: disabled
  Mail logging: disabled
  ASDM logging: disabled
```

設定したすべての出力先へのログのディセーブル化

設定したすべてのログ出力先へのロ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。

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

ログ設定の表示

実行中のログ設定を表示するには、次のコマンドを入力します。

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

show logging コマンドの出力例を示します。

```
Syslog logging: enabled
  Facility: 16
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: level errors, facility 16, 3607 messages logged
    Logging to infrastructure 10.1.2.3
  History logging: disabled
  Device ID: 'inside' interface IP address "10.1.1.1"
  Mail logging: disabled
  ASDM logging: disabled
```

各ステータス行エントリの意味は、次のとおりです。

ログステータス行	説明
System Log logging	全体的なシステム ログのステータス
Facility	Syslog サーバへのシステム ログ メッセージの送信に使用されるロギング ファシリティ
Timestamp logging	システム ログ メッセージ内でのタイムスタンプの有無を表します。
Standby logging	イネーブルの場合、フェールオーバー スタンバイ FWSM のシステム ログ メッセージは、フェールオーバーが発生しても同期化されたままになります。

ログステータス行	説明
Deny Conn when Queue Full	イネーブルの場合、ログ キューが満杯になるとすべてのトラフィックが拒否されます。
Monitor logging	コンソールへのログを Telnet または SSH セッションで表示できるかどうかを表します。
Buffer logging	内部ログ バッファがログの出力先としてイネーブルかどうかを表します。
Trap logging	1 つまたは複数の Syslog サーバへのログの送信がイネーブルかどうかを表します。
History logging	SNMP 管理ステーションへのログの送信がイネーブルかどうかを表します。
Device ID	システム ログ メッセージにデバイス ID が含まれるかどうかを表します。
Mail logging	1 つまたは複数の E メール アドレスへのログの送信がイネーブルかどうかを表します。
ASDM logging	ASDM へのログの送信がイネーブルかどうかを表します。

ログの出力先の設定

ここでは、FWSM で生成されるログ メッセージの保存または送信先を指定する方法について説明します。内容は次のとおりです。

- [ログの出力先の概要 \(p.1-9\)](#)
- [出力先としての Syslog サーバの設定 \(p.1-10\)](#)
- [出力先としての E メール アドレスの指定 \(p.1-12\)](#)
- [出力先としての ASDM の指定 \(p.1-13\)](#)
- [Telnet セッションによるログの表示 \(p.1-14\)](#)

ログの出力先の概要

FWSM が生成したログを表示するには、ログの出力先を指定する必要があります。ログの出力先を指定しないでログをイネーブルにすると、FWSM はメッセージを生成しても、ユーザが表示できる場所にメッセージを保存しません。

FWSM が次の場所にログを送信するように設定できます。

- 1 つまたは複数の Syslog サーバ
- 1 つまたは複数の E メール アドレス
- ASDM (Adaptive Security Device Manager)
- Telnet セッション
- 内部ログ バッファ

出力先としての Syslog サーバの設定

ここでは、Syslog サーバにログを送信するように FWSM を設定する方法を説明します。

Syslog サーバにログを送信するように FWSM を設定すると、サーバ上のディスクの空き容量の範囲内でログをアーカイブすることができ、保存後のログデータの操作が可能になります。たとえば、特定のタイプのシステム ログ メッセージが記録された場合に実行すべきアクションを指定したり、ログからデータを抽出してレポート用に別のファイルにレコードを保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

Syslog サーバは、syslogd という名前のプログラム(サーバ)を実行している必要があります。UNIX では、OS (オペレーティングシステム)の一部として Syslog サーバが提供されています。Windows 95 および Windows 98 の場合は、他のベンダーから syslogd サーバを入手してください。

FWSM から Syslog サーバへのデータの送信に使用するプロトコルとしては、UDP または TCP を指定できますが、両方を指定することはできません。TCP を指定した場合、FWSM は Syslog サーバに障害が発生すると、ログの送信を停止します。UDP を指定すると、FWSM は Syslog サーバが正常に動作しているかどうかに関わらず、ログの送信を続行します。

各ログメッセージにタイムスタンプを含めるには、ロギング タイムスタンプをイネーブルにします。Syslog サーバへのログ送信に UDP を選択した場合、各 Syslog サーバに EMBLEM フォーマットのログをイネーブルにできます。

Syslog サーバにシステム ログメッセージを送信するように FWSM を設定するには、次の作業を行います。

ステップ1 次のコマンドを入力し、ログの出力先として Syslog サーバを指定します。

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

ここで、

format emblem Syslog サーバで EMBLEM フォーマットのログをイネーブルにします (UDP のみ)。

interface_name Syslog サーバが存在するインターフェイスを指定します。

port Syslog サーバがシステム ログメッセージを待ち受けるポートを指定します。どちらのプロトコルでも、有効な port 値は 1025 ~ 65535 です。前に入力したコマンドで使用した *port* および *protocol* 値を表示するには、**show running-config logging** コマンドを使用し、リストの中からコマンドを探します。TCP プロトコルは 6、UDP プロトコルは 17 でリストされます。

ip_address Syslog サーバの IP アドレスを指定します。

tcp FWSM が TCP を使用してシステム ログメッセージを Syslog サーバに送信することを指定します。

udp FWSM が UDP を使用してシステム ログメッセージを Syslog サーバに送信することを指定します。

次に例を示します。

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

出力先として複数の Syslog サーバを指定する場合は、Syslog サーバごとに 1 つずつコマンドを入力します。

ステップ2 次のコマンドを入力し、Syslog サーバに送信するシステム ログ メッセージを指定します。

```
hostname(config)# logging trap {severity_level (1-7) | message_list}
```

ここで、

severity_level Syslog サーバに送信するメッセージの重大度を指定します。たとえば、重大度を 3 に設定すると、FWSM は重大度 3、2、1、および 0 のシステム ログ メッセージを送信します。番号 (2 など) または名前 (critical など) のどちらを指定しても構いません。

メッセージの重大度についての詳細は、「[重大度](#)」(p.1-27) を参照してください。

message_list Syslog サーバに送信するシステム ログ メッセージを表す、カスタムなメッセージ リストを指定します。カスタムなメッセージ リストの作成については、「[カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング](#)」(p.1-20) を参照してください。

次に、重大度 3 (error) 以上のシステム ログ メッセージを Syslog サーバに送信するように FWSM を設定する例を示します。FWSM は、重大度 3、2、1 のメッセージを送信します。

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

ステップ3 サーバに送信する各システム ログ メッセージにデバイス ID を含めるには、次のコマンドを入力します。

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

Syslog サーバに送信されるシステム ログ メッセージには、指定のデバイス ID (指定のインターフェイスのホスト名と IP アドレス、またはストリング) が含まれます。

ステップ4 必要に応じて、ロギング ファシリティの値をデフォルトの 20 以外に設定します (ほとんどの UNIX システムでは、システム ログ メッセージがファシリティ 20 で着信することが前提となっています)。

ロギング ファシリティの設定を変更するには、次のコマンドを入力します。

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

次に例を示します。

```
hostname(config)# logging facility 16
```

ステップ5 設定の変更を確認するには、次のコマンドを入力します。

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

次に、`show logging` コマンドの出力例を示します。

```
Syslog logging: enabled
  Facility: 16
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: level errors, facility 16, 3607 messages logged
    Logging to infrastructure 10.1.1.3
  History logging: disabled
  Device ID: 'inside' interface IP address "10.1.1.1"
  Mail logging: disabled
  ASDM logging: disabled
```

出力先としての E メールアドレスの指定

特定の E メール アドレスに一部または全部のシステム ログ メッセージを送信するように FWSM を設定できます。E メールで送信した場合、システム ログ メッセージは E メール メッセージの件名に表示されます。したがって、このオプションは重大度の高いシステム ログ メッセージ (critical、alert、emergency など) を管理者に通知する目的で設定することを推奨します。

出力先として E メール アドレスを指定するには、次の作業を行います。

- ステップ 1** 1 つまたは複数の E メール アドレスに送信するシステム ログ メッセージを指定します。システム ログ メッセージの重大度またはシステム ログ メッセージ リスト変数を使用して、送信するシステム ログ メッセージを指定します。

送信するシステム ログ メッセージを指定するには、次のコマンドを入力します。

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

次の例では、事前に `logging list` コマンドで設定済みの「high-priority」という `message_list` を使用しています。

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

- ステップ 2** 次のコマンドを入力し、システム ログ メッセージを特定の E メール アドレスに送信するとき使用する送信元の E メール アドレスを指定します。

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

次に例を示します。

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

ステップ 3 システム ログメッセージを特定の E メール宛先に送信するとき使用する受信者の E メールアドレスを指定します。最大 5 つの受信者アドレスを設定できます。各受信者を個別に入力する必要があります。

受信者のアドレスを入力するには、次のコマンドを入力します。

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

次に例を示します。

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



(注) 重大度を指定しない場合、デフォルトの重大度 (error 条件、重大度 3) が使用されます。

ステップ 4 システム ログメッセージを特定の E メール宛先に送信するとき使用する SMTP サーバを指定するには、次のコマンドを入力します。

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

次に例を示します。

```
hostname(config)# smtp-server smtp-host-1
```

出力先としての ASDM の指定

ASDM にシステム ログメッセージを送信するように FWSM を設定できます。FWSM は ASDM への送信待ちのシステム ログメッセージを格納するバッファ領域を確保し、発生したメッセージをそこに保存します。ASDM ログバッファは、内部ログバッファとは別です。内部ログバッファについての詳細は、「[ログバッファの概要](#)」(p.1-16)を参照してください。

ASDM ログバッファが満杯になると、FWSM は最も古いシステム ログメッセージを削除して、新しいシステム ログメッセージを格納できるようにします。このバッファのサイズを変更することにより、ASDM ログバッファに格納されるシステム ログメッセージ数を制御できます。

出力先として ASDM を指定するには、次の作業を行います。

ステップ 1 次のコマンドを入力し、ASDM に送信するシステム ログメッセージを指定します。

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

コマンド オプションについて次に説明します。

<i>level</i>	システム ログ メッセージの最大の重大度を設定します。たとえば、level を 3 に設定すると、FWSM は重大度 3、2、1、0 のシステム ログ メッセージを生成します。次のように、番号または名前のどちらを指定しても構いません。 <ul style="list-style-type: none"> • 0 または emergencies システムが使用不能 • 1 または alerts ただちに対応が必要 • 2 または critical クリティカル条件 • 3 または errors エラー • 4 または warnings 警告 • 5 または notifications 正常だが注意を要する状態 • 6 または informational 情報 • 7 または debugging デバッグ メッセージ、ログ FTP コマンド、および WWW URL
<i>message_list</i>	ASDM ログ バッファに送信するシステム ログ メッセージを表すリストを指定します。リストの作成方法については、「 カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング 」(p.1-20)を参照してください。

次に、ログをイネーブルにして、重大度 0、1、2 のシステム ログ メッセージを ASDM ログ バッファに送信する例を示します。

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

ステップ 2 ASDM ログ バッファに格納するシステム ログ メッセージ数を指定するには、次のようにグローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。

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

ここで、*num_of_msgs* は、FWSM が ASDM ログ バッファに格納するシステム ログ メッセージ数を表します。

次に、ASDM ログ バッファのサイズを 200 個のシステム ログ メッセージに設定する例を示します。

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

ASDM ログ バッファの現在の内容を消去するには、次のコマンドを入力します。

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

Telnet セッションによるログの表示

Telnet セッションで Syslog メッセージを表示するには、次の作業を行います。

ステップ 1 内部インターフェイス上のホストが FWSM をアクセスするように、FWSM を設定します。

a. 次のコマンドを入力し、IP アドレスおよびインターフェイス名を指定します。

```
hostname(config)# 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 である場合、このコマンドは次のようになります。

```
hostname(config)# telnet 192.168.1.2 255.255.255.255
```

- b. Telnet セッションがアイドル状態のときに FWSM がセッションを切断するまでのタイムアウト時間を、デフォルトの 5 分より大きい値に設定します。タイムアウトは最低でも 15 分にすることを推奨します。この場合、次のように設定します。

```
hostname(config)# telnet timeout 15
```

ステップ 2 ホスト上で Telnet を起動し、FWSM の内部インターフェイスを指定します。

Telnet 接続が確立されると、FWSM によって次のプロンプトが表示されます。

```
FWSM passwd
```

ステップ 3 Telnet パスワードを入力します。このパスワードは、デフォルトでは `cisco` です。

ステップ 4 次のコマンドを入力し、コンフィギュレーション モードをイネーブルにします。

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

```
(Enter your password at the prompt)
```

```
hostname(config)# configure terminal
```

ステップ 5 次のコマンドを入力し、メッセージのログを開始します。

```
hostname(config)# logging monitor level (1-7)
```

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

```
hostname(config)# terminal monitor
```

このコマンドでは、現在の Telnet セッションに関してのみログがイネーブルになります。`logging monitor` コマンドはすべての Telnet セッションについてログの基本設定を行うのに対し、`terminal monitor` (および `terminal no monitor`) コマンドは個々の Telnet セッションについてのログを制御します。

ステップ 7 ホストに ping を実行したり、Web ブラウザを起動するなど、何らかのイベントをトリガーします。

その結果、Telnet セッション ウィンドウに Syslog メッセージが表示されます。

ステップ 8 作業が終わったら、次のコマンドを使用してこの機能をディセーブルにします。

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

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

出力先としてのログバッファの指定

ここでは、システム ログ メッセージを内部ログ バッファに保存するように FWSM を設定する方法について説明します。内容は次のとおりです。

- [出力先としてのログ バッファのイネーブル化 \(p.1-16\)](#)
- [ログ バッファが満杯になったときの動作の指定 \(p.1-17\)](#)
- [内部フラッシュ メモリへのログ バッファ内容の保存 \(p.1-18\)](#)
- [ログ バッファ内容のクリア \(p.1-18\)](#)

ログ バッファの概要

ログ バッファを出力先に設定した場合、ログ バッファはシステム ログ メッセージの一時的な保存場所として動作します。リストの最後に新しいメッセージが追加されます。バッファが満杯になると（つまり、バッファがラップすると）、新しいメッセージが生成された時点で古いメッセージが上書きされます。ログ メッセージを保存するには、古いメッセージが上書きされないよう、バッファが満杯になるたびにバッファの内容を FTP サーバまたは内部フラッシュ メモリに保存するように FWSM を設定できます。

バッファがラップするまでに格納できるメッセージ数は、ログ バッファのサイズによって決まります。デフォルトのログ バッファ サイズは 4 KB です。

出力先としてログ バッファをイネーブルにする場合、保存するメッセージも指定できます。指定しない場合、生成されたすべてのメッセージがログ バッファに保存されます。メッセージの重大度に基づいてメッセージを保存するか、またはカスタムなメッセージ リストで指定する基準に基づいてメッセージを保存するように、FWSM を設定できます。保存するメッセージを制限する方法については、「[出力先に送信するシステム ログ メッセージのフィルタリング](#)」(p.1-18) を参照してください。

出力先としてのログ バッファのイネーブル化

ログの出力先としてログ バッファをイネーブルにし、ログ バッファの設定オプションを指定するには、次の作業を行います。

- ステップ 1** 次のコマンドを入力し、FWSM がログ バッファにシステム ログ メッセージを保存できるようにするとともに、保存するメッセージを指定します。

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

ここで、*level* は、保存するメッセージの重大度を表します。*message_list* は、ログ バッファに保存するメッセージを選択するためのカスタム リストの名前を表します。

level オプションには、重大度を番号（3 など）または名前（error など）のどちらかで指定します。指定した重大度以上のメッセージが選択されます。つまり、重大度 3 を指定すると、重大度 3、2、1 のメッセージがログ バッファに保存されます。

たとえば、重大度 1 および 2 のメッセージをログ バッファに保存するには、次のいずれかのコマンドを入力します。

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

または

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

`message_list` オプションには、ログ バッファに保存するメッセージを選択するための基準を表すメッセージ リストの名前を指定します。

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

カスタムなメッセージ リストを作成するには、`logging list` コマンドを使用します。カスタムなメッセージ リストの作成方法については、「[カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング](#)」(p.1-20)を参照してください。

ステップ 2 (任意) ログ バッファのサイズを変更するには、次のコマンドを入力します。

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

ここで、`bytes` オプションはログ バッファのメモリ容量(バイト数)を設定します。たとえば、8192 を指定すると、FWSM はログ バッファに 8 KB のメモリを使用します。

次に、ログ バッファに 16 KB のメモリを使用するように FWSM を設定する例を示します。

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

ログ バッファが満杯になったときの動作の指定

デフォルトでは、FWSM は継続的にログ バッファにメッセージを書き込み、バッファが満杯になると古いメッセージを上書きします。ログの履歴を残すには、バッファが満杯になるたびに別の出力先にバッファの内容を送信するように FWSM を設定できます。内部フラッシュ メモリまたは FTP サーバに、バッファの内容を保存できます。

バッファの内容を別の場所に保存するとき、FWSM が作成するログ ファイル名は、デフォルトでは次のようなタイムスタンプ フォーマットになります。

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

ここで、`YYYY` は年、`MM` は月、`DD` は日、`HHMMSS` は時、分、秒です。

FWSM は内部フラッシュ メモリまたは FTP サーバにログ バッファの内容を書き込むと同時に、ログ バッファへの新しいメッセージの保存を続けます。

ログ バッファが満杯になるたびに内部フラッシュ メモリにバッファ内のメッセージを保存するように指定するには、次のコマンドを入力します。

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

ログ バッファが満杯になるたびに FTP サーバにバッファ内のメッセージを保存するように指定するには、次の作業を行います。

ステップ 1 次のコマンドを入力し、ログ バッファが満杯になるたびにバッファの内容を FTP サーバに送信できるように FWSM を設定します。

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

ステップ2 次のコマンドを入力し、FTP サーバの詳細情報を指定します。

```
hostname(config)# logging ftp-server {server_address | server_hostname} path username
password
```

ここで、

server_address 外部 FTP サーバの IP アドレスを指定します。

server_hostname 外部 FTP サーバのホスト名を指定します。

path ログバッファのデータを保存する FTP サーバ上のディレクトリパスを指定します。このパスは、FTP ルートディレクトリに相対します。次に例を示します。

```
/security_appliances/syslogs/appliance107
```

username FTP サーバにログインできるユーザ名を指定します。

password 指定したユーザ名に対応するパスワードを指定します。

次の例では、サーバ名 logserver-352、パス /syslogs、ユーザ名 logsupervisor、パスワード 1luvMy10gs を指定しています。

```
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
```

内部フラッシュメモリへのログバッファ内容の保存

任意の時点で、バッファの内容を内部フラッシュメモリに保存できます。ログバッファの現在の内容を内部フラッシュメモリに保存するには、次のコマンドを入力します。

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

たとえば、ファイル名 latest-logfile.txt を使用して内部フラッシュメモリにログバッファの内容を保存するには、次のように指定します。

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

ログバッファ内容のクリア

ログバッファの内容を消去するには、次のコマンドを入力します。

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

出力先に送信するシステムログメッセージのフィルタリング

ここでは、特定の出力先に送信するシステムログメッセージを指定する方法について説明します。内容は次のとおりです。

- [メッセージフィルタリングの概要 \(p.1-19\)](#)
- [クラスによるシステムログメッセージのフィルタリング \(p.1-19\)](#)
- [カスタムメッセージリストによるシステムログメッセージのフィルタリング \(p.1-20\)](#)

メッセージフィルタリングの概要

生成されたシステム ログ メッセージの中から、特定のシステム ログ メッセージだけを特定の出力先に送信するように、フィルタリングを行うことができます。たとえば、すべてのシステム ログ メッセージを 1 つの出力先に送信するとともに、その一部については別の出力先にも送信するように、FWSM を設定できます。

具体的には、次の基準に基づいてシステム ログ メッセージを特定の出力先に送信するように、FWSM を設定できます。

- システム ログ メッセージの ID 番号
- システム ログ メッセージの重大度
- システム ログ メッセージのクラス (FWSM の機能分野)
- ユーザ側で作成するシステム ログ メッセージ リスト

たとえば、重大度 1、2、3 のすべてのシステム ログ メッセージを内部ログ バッファに送信したり、「ha」クラスのすべてのシステム ログ メッセージを特定の Syslog サーバに送信することができます。また、特定の E メール アドレスに送信する「high-priority」という名前のメッセージ リストを作成して、システム管理者に問題の発生を通知するように、FWSM を設定することもできます。

クラスによるシステム ログ メッセージのフィルタリング

システム ログ メッセージのクラスは、FWSM の機能分野と同じように、システム ログ メッセージをタイプ別に分類する手段となります。たとえば、「vpnc」クラスは VPN クライアントを表します。

ロギング クラスを使用すると、1 つのカテゴリに属するすべてのシステム ログ メッセージの出力先を、1 つのコマンドで指定できます。

システム メッセージ クラスは、次の 2 通りの方法で使用できます。

- `logging class` コマンドを使用して、1 つのカテゴリに属するすべてのシステム ログ メッセージの出力先を指定します。
- システム ログ メッセージのカスタム リストを作成するときに、`message_class` 変数を使用して、そのクラスに属するすべてのシステム ログ メッセージをカスタム リストに含めます。

特定のクラスのシステム ログ メッセージは、システム ログ メッセージ ID 番号の先頭 3 桁が共通しています。たとえば、611 で始まるシステム ログ メッセージ ID は、vpnc (VPN クライアント) クラスに対応します。VPN クライアント機能に関係するシステム ログ メッセージは、611101 ~ 611323 の範囲です。

クラスの全メッセージを特定の出力先に送信

特定のクラスに属するすべてのシステム ログ メッセージを、特定の出力先に送信するように FWSM を設定するには、次のコマンドを入力します。

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

ここで、

`message_class` 特定の出力先に送信するシステム ログ メッセージのクラスを指定します。システム ログ メッセージのクラスの一覧は、表 1-2 を参照してください。

`buffered | console | history | mail | monitor | trap` このクラスのシステム ログ メッセージを送信する出力先を指定します。コマンドライン エントリごとに 1 つの出力先を選択します。1 つのクラスを複数の出力先に送信する場合は、出力先ごとに新しいコマンドを入力します。

■ ログの設定および管理

severity_level 出力先に送信するシステム ログ メッセージを、重大度によってさらに制限します。メッセージの重大度についての詳細は、[重大度 \(p.1-27\)](#) を参照してください。

次の例では、クラス ha(ハイ アベイラビリティ、別名フェールオーバー)に関する重大度 1(alert)のすべてのシステム ログ メッセージを、内部ログ バッファに送信します。

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

表 1-2 に、システム ログ メッセージのクラスと、各クラスのシステム ログ メッセージ ID の範囲を示します。

表 1-2 システム ログ メッセージのクラスと対応するメッセージ ID 番号

クラス	定義	システム ログ 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	透過的ファイアウォール	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
ca	PKI 認証局	717
e-mail	E 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

カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング

カスタムなメッセージ リストを作成すると、特定の出力先に送信するシステム ログ メッセージをフレキシブルに制御することができます。カスタムなシステム ログ メッセージで、メッセージのグループを指定するには、重大度、メッセージ ID、システム メッセージ ID の範囲、またはメッセージ クラスの各基準を使用できます。

たとえば、メッセージ リストを使用すると次のことが可能です。

- 重大度 1 および 2 のシステム ログ メッセージを選択し、それらを 1 つまたは複数の E メールアドレスに送信する。

- 特定のメッセージクラス（「ha」など）に対応するすべてのシステム ログ メッセージを、内部バッファに保存する。

メッセージリストでは、複数の基準を使用してメッセージを選択できます。ただし、メッセージの選択基準ごとに、新しいコマンドを追加する必要があります。重複したメッセージ選択基準を含むメッセージリストを作成できます。1つのメッセージリストで2つの基準によって同じメッセージが選択された場合、そのメッセージは1回しか記録されません。



(注)

システム ログ メッセージリストの名前には、重大度と同じ名前を使用しないでください。*message_list* 名として使用できない名前としては、「emergencies」、「alert」、「critical」、「error」、「warning」、「notification」、「informational」、「debugging」があります。同様に、これらの語の先頭3文字も、ファイル名の先頭に使用しないでください。たとえば、「err」で始まるファイル名を使用してはなりません。

ログ バッファに保存するメッセージを選択するために FWSM が使用するカスタム リストを作成するには、次の作業を行います。

ステップ 1 次のコマンドを入力し、メッセージの選択基準を含むメッセージ リストを作成します。

```
hostname(config)# logging list {message_list | [severity_level | message_class | message_ID | range_of_IDs]}
```

ここで、

message_list メッセージの選択基準を含むリストの名前を指定します。

severity_level 指定する重大度のすべてのメッセージをログ バッファに送信します。

message_class 指定するメッセージクラスのすべてのメッセージをログ バッファに保存します。

message_ID 固有のシステム ログ メッセージ ID 番号を指定します。

range_of_IDs メッセージ ID 番号の範囲を指定します（例：103401-103599）。

次の例では、重大度 3 以上のメッセージをログ バッファに保存する、notif-list というメッセージ リストを作成します。

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

ステップ 2 (任意) リストにメッセージ選択基準をさらに追加するには、上記のステップと同じコマンドを入力し、既存のメッセージ リスト名および追加の基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。

次に、このメッセージ リストに基準を追加する例を示します。メッセージ ID 番号の範囲、およびメッセージクラス ha（ハイ アベイラビリティまたはフェールオーバー）を追加します。メッセージクラスについての詳細は、[クラスによるシステム ログ メッセージのフィルタリング \(p.1-19\)](#)を参照してください。

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

上記の例では、指定した基準に一致するシステム ログ メッセージがログ バッファに送信されます。このリストで、システム ログ メッセージに関して指定されている基準は、次のとおりです。

- 100100 ~ 100110 の範囲内のシステム ログ メッセージ ID
- critical レベル以上 (emergency、alert、または critical) のすべてのシステム ログ メッセージ
- warning レベル以上 (emergency、alert、critical、error、または warning) のすべての VPN クラスのシステム ログ メッセージ

これらの条件のいずれかが満たされる場合、そのシステム ログ メッセージが記録されます。1 つのシステム ログ メッセージが複数の条件を満たしていても、そのメッセージは 1 回しか記録されません。

ログ設定のカスタマイズ

ここでは、ログ設定を調整する、その他のオプションについて説明します。内容は次のとおりです。

- [ロギング キューの設定 \(p.1-22\)](#)
- [システム ログ メッセージでの日付と時刻の表示 \(p.1-22\)](#)
- [システム ログ メッセージでのデバイス ID の表示 \(p.1-23\)](#)
- [EMBLEM フォーマットでのシステム ログ メッセージの生成 \(p.1-24\)](#)
- [システム ログ メッセージのディセーブル化 \(p.1-24\)](#)
- [システム ログ メッセージの重大度の変更 \(p.1-25\)](#)
- [ログに使用できる内部フラッシュメモリの容量の変更 \(p.1-26\)](#)

ロギング キューの設定

FWSM には、設定された出力先に送信するまでの間、システム ログ メッセージを格納しておくバッファ用に割り当て可能な固定数のメモリ ブロックがあります。必要なブロック数は、システム ログ メッセージ キューの長さ、指定された Syslog サーバの数によって左右されます。

FWSM が設定された出力先に送信するまで、キューに格納できるシステム ログ メッセージ数を指定するには、次のコマンドを入力します。

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

ここで、*message_count* 変数は、処理に先立ってシステム ログ メッセージ キューに格納できるシステム ログ メッセージ数を表します。デフォルトでは、512 個のシステム ログ メッセージを格納できます。0 (ゼロ) の設定値は、無限のシステム ログ メッセージを表します。つまり、使用可能なブロックメモリによってのみキューのサイズが制限されます。

キューおよびキューの統計情報を表示するには、次のコマンドを入力します。

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

システム ログ メッセージでの日付と時刻の表示

システム ログ メッセージが生成された日付および時刻をメッセージに含めるには、次のコマンドを入力します。

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

システム ログ メッセージでのデバイス ID の表示

EMBLEM 以外のフォーマットのシステム ログ メッセージにデバイス ID を含めるように FWSM を設定するには、次のコマンドを入力します。

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

ここで、

context-name 現在のコンテキスト名をデバイス ID として使用します(複数コンテキスト モードで動作している FWSM にのみ適用されます)。

hostname FWSM のホスト名をデバイス ID として使用します。

ipaddress interface_name interface_name で指定するインターフェイスの IP アドレスをデバイス ID として使用します。

ipaddress オプションを使用すると、システム ログ メッセージの送信元のインターフェイスとは無関係に、デバイス ID は特定の FWSM インターフェイスの IP アドレスになります。このキーワードは、デバイスから送信されたすべてのシステム ログ メッセージに、一定のデバイス ID を提供します。

string text text オプションで入力する文字をデバイス ID として使用します。最大 16 文字のストリングを指定できます。*text* には、スペース文字または次の文字を使用することはできません。

- & (アンパーサンド)
- ' (一重引用符)
- " (二重引用符)
- < (より小記号)
- > (より大記号)
- ? (疑問符)



(注)

デバイス ID をイネーブルにしても、EMBLEM フォーマットのシステム ログ メッセージまたは SNMP トラップには、デバイス ID は表示されません。

次に、FWSM でロギング デバイス ID をイネーブルにする例を示します。

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

次に、FWSM 上のセキュリティ コンテキストでロギング デバイス ID をイネーブルにする例を示します。

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

複数コンテキスト モードの admin コンテキストでロギング デバイス ID をイネーブルにすると、システム実行スペースで発生したメッセージは、**system** というデバイス ID を使用し、admin コンテキストで発生したメッセージは、その admin コンテキストの名前をデバイス ID として使用します。

EMBLEM フォーマットでのシステム ログ メッセージの生成

Syslog サーバ以外の出力先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、次のコマンドを入力します。

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

UDP を使用して Syslog サーバに送信するシステム ログ メッセージに、EMBLEM フォーマットを適用するには、Syslog サーバを出力先として設定するときに、**format emblem** オプションを指定します。次のコマンドを入力します。

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

ここで、

interface_name および *IP_address* は、システム ログ メッセージを受信する Syslog サーバを指定します。**tcp[/port]** および **udp[/port]** は、使用するプロトコルおよびポートを表します。**format emblem** は、Syslog サーバに送信されるメッセージについて EMBLEM フォーマットを有効にします。

FWSM は、UDP または TCP のどちらのプロトコルを使用してもシステム ログ メッセージを送信できます。ただし、EMBLEM フォーマットを有効にできるのは、UDP を使用して送信されるメッセージだけです。デフォルトのプロトコルおよびポートは、UDP/514 です。

次に例を示します。

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

システム ログ メッセージのディセーブル化

FWSM が特定のシステム ログ メッセージを生成しないようにするには、次のコマンドを入力します。

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

次に例を示します。

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

ディセーブルにしたシステム ログ メッセージを再びイネーブルにするには、次のコマンドを入力します。

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

次に例を示します。

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

ディセーブルになっているシステム ログ メッセージの一覧を表示するには、次のコマンドを入力します。

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

ディセーブルにしたすべてのシステム ログ メッセージのログを再びイネーブルにするには、次のコマンドを入力します。

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

システム ログ メッセージの重大度の変更

システム ログ メッセージのログ レベルを指定するには、次のコマンドを入力します。

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

次に、システム ログ メッセージ ID 113019 の重大度を 4 (warning) から 5 (notification) に変更する例を示します。

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

システム ログ メッセージのログ レベルをデフォルトの重大度に戻すには、次のコマンドを入力します。

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

次に、システム ログ メッセージ ID 113019 の重大度をデフォルト値の 4 (warning) に戻す例を示します。

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

重大度を変更しているシステム ログ メッセージの一覧を表示するには、次のコマンドを入力します。

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

変更したシステム ログ メッセージの重大度をすべてデフォルトに戻すには、次のコマンドを入力します。

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

次に示す一連のコマンドは、`logging message` コマンドを使用して、システム ログ メッセージの有無および重大度を制御する例を示しています。

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

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

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

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

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

ログに使用できる内部フラッシュ メモリの容量の変更

FWSM でログ バッファの内容を内部フラッシュ メモリに保存する方法には、次の2通りがあります。

- ログ バッファが満杯になるたびに、バッファの内容を内部フラッシュ メモリに保存するようにログ動作を設定する。
- ログ バッファの現在の内容を内部フラッシュ メモリに即時に保存するコマンドを、FWSM に入力する。

デフォルトでは、FWSM は最大 1 MB の内部フラッシュ メモリをデータのログに使用できます。FWSM がログ データを保存するために最低限必要な内部フラッシュ メモリの空き容量は、デフォルトで 3 MB です。

内部フラッシュ メモリに保存するログ ファイルによって、内部フラッシュ メモリの空き容量が、設定済みの最小値に満たなくなる場合には、FWSM は最も古いログ ファイルを削除して、新しいログ ファイルの保存後に最小の空き容量が確保されるようにします。削除するファイルがない場合、または古いファイルをすべて削除しても空き容量が最小値に達しない場合は、FWSM は新しいログ ファイルを保存できません。

ログに使用できる内部フラッシュ メモリの容量を変更するには、次の作業を行います。

- ステップ 1** 次のコマンドを入力し、ログ ファイルに使用できる内部フラッシュ メモリの最大容量を指定します。

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

ここで、*kbytes* は、ログ ファイルの保存に使用できる内部フラッシュ メモリの最大容量 (単位: キロバイト) を表します。

次の例では、ログ ファイルに使用できる内部フラッシュ メモリの最大容量を約 1.2 MB に設定します。

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

- ステップ 2** 次のコマンドを入力し、FWSM がログ ファイルを保存するために最低限必要な内部フラッシュ メモリの空き容量を指定します。

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

ここで、*kbytes* は、FWSM が新しいログ ファイルを保存するために最低限必要な内部フラッシュ メモリの空き容量 (単位: キロバイト) を表します。

次の例では、FWSM が新しいログ ファイルを保存するために最低限必要な内部フラッシュ メモリの空き容量を 4000 KB に設定します。

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

システム ログ メッセージの概要

ここでは、FWSM で生成されるシステム ログ メッセージの内容について説明します。内容は次のとおりです。

- システム ログ メッセージのフォーマット (p.1-27)
- 重大度 (p.1-27)
- システム ログ メッセージで使用される変数 (p.1-28)
- ログイング コマンドの一覧 (p.1-30)

システム ログ メッセージのフォーマット

システム ログ メッセージは、パーセント符号 (%) で始まります。メッセージの形式は、次のとおりです。

```
%FWSM Level Message_number: Message_text
```

各フィールドの意味は次のとおりです。

FWSM	FWSM が生成したメッセージのシステム ログ メッセージ ファシリティ コードを表します。この値は常に FWSM です。
Level	1 ~ 7。システム ログ メッセージで記述される状態の重大度を表します。番号が小さいほど、重大度が高くなります。詳細については、表 1-3 を参照してください。
Message_number	システム ログ メッセージを一意に識別する 6 桁の番号
Message_text	状況を説明するテキストストリング。システム ログ メッセージのテキストには、IP アドレス、ポート番号、またはユーザ名が含まれていることがあります。表 1-4 に、変数フィールドと、各フィールドの情報タイプを示します。

重大度

表 1-3 に、システム ログ メッセージの重大度を示します。

表 1-3 システム 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	システム使用不可
1	alert	ただちに対応が必要
2	critical	クリティカル条件
3	error	エラー条件
4	warning	警告条件
5	notification	正常だが注意を要する状態
6	informational	情報メッセージのみ
7	debugging	デバッグ時に限り表示

付録 A「重大度別のメッセージ」に、重大度別のシステム ログ メッセージを記載しています。



(注) FWSM では、重大度 0 (emergencies) のシステム ログ メッセージは生成されません。logging コマンドには、UNIX のシステム ログ機能との互換性を確保するためにレベル 0 が用意されていますが、FWSM ではこのレベルを使用しません。

システム ログ メッセージで使用される変数

システム ログ メッセージには変数が含まれる場合が多くあります。表 1-4 に、このマニュアルでシステム ログ メッセージの説明に使用されている主な変数を示します。1 種類のシステム ログ メッセージでしか使用されない変数は省略しています。

表 1-4 システム ログ メッセージ内の可変フィールド

変数	情報タイプ
<i>acl_ID</i>	ACL (アクセス制御リスト) 名
<i>bytes</i>	バイト数
<i>code</i>	システム ログ メッセージに応じてエラーの原因または送信元を表す 10 進数
<i>command</i>	コマンド名
<i>command_modifier</i>	<p><i>command_modifier</i> は、次のいずれかのストリングです。</p> <ul style="list-style-type: none"> • cmd (このストリングは、コマンドに修飾子がないことを意味します) • clear • no • show
<i>connections</i>	接続数
<i>connection_type</i>	<p>接続タイプ</p> <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>	メモリのストレージ装置。たとえば、フロッピー ディスク、内部フラッシュメモリ、TFTP、フェールオーバー スタンバイ装置、コンソール端末など。
<i>econns</i>	初期接続の数
<i>elimit</i>	static または nat コマンドで指定される初期接続の数
<i>filename</i>	FWSM のイメージ、ASDM ファイル、またはコンフィギュレーションのタイプ別ファイル名
<i>ftp-server</i>	外部 FTP サーバの名前または 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、セキュリティ レベルの低いインターフェイスのアドレス
<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 (ローカル) IP アドレス、セキュリティ レベルの高いインターフェイスのアドレス

表 1-4 システム ログ メッセージ内の可変フィールド (続き)

変数	情報タイプ
<i>inside_port</i>	内部ポート番号
<i>interface_name</i>	インターフェイス名
<i>IP_address</i>	IP アドレス、 <i>n.n.n.n</i> 形式 (<i>n</i> は 1 ~ 255 の整数)
<i>MAC_address</i>	MAC アドレス
<i>mapped_address</i>	変換後の IP アドレス
<i>mapped_port</i>	変換後のポート番号
<i>message_class</i>	FWSM の機能分野に対応するシステム ログ メッセージのカテゴリ
<i>message_list</i>	システム ログ メッセージの ID 番号、クラス、または重大度のリストを含む、ユーザ側で作成するファイルの名前
<i>message_number</i>	システム ログ メッセージ ID
<i>nconns</i>	スタティック テーブルまたは xlate (変換) テーブルで許可される接続数
<i>netmask</i>	サブネット マスク
<i>number</i>	数値。形式はシステム ログ メッセージによって異なります。
<i>octal</i>	8 進数
<i>outside_address</i>	外部 IP アドレス、通常は外部ルータの外側にあるネットワークのセキュリティ レベルの低いインターフェイス上の Syslog サーバのアドレス
<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>	ユーザ権限レベル
<i>protocol</i>	パケットのプロトコル (ICMP、TCP、UDP など)
<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>	システム ログ メッセージの理由を説明するテキスト スtring
<i>service</i>	パケットが指定するサービス (SNMP、Telnet など)
<i>severity_level</i>	システム ログ メッセージの重大度
<i>source_address</i>	パケットの送信元アドレス
<i>source_port</i>	送信元ポート番号
<i>string</i>	テキスト スtring (ユーザ名など)
<i>tcp_flags</i>	TCP ヘッダー内のフラグ <ul style="list-style-type: none"> • ACK • FIN • PSH • RST • SYN • URG
<i>time</i>	経過時間、形式は <i>hh:mm:ss</i>
<i>url</i>	URL
<i>user</i>	ユーザ名

ロギング コマンドの一覧

ここでは、システム ログの設定およびモニタ用に FWSM 上で使用できるロギング コマンドの一覧と、各コマンドの簡単な説明を示します。コマンドに関する詳しい説明は、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

表 1-5 に、FWSM 上でシステム ログの設定およびモニタに使用できるコマンドを示します。

表 1-5 ロギング コマンドの一覧

コマンド	説明
clear configure logging	ログの設定値をデフォルト値に戻します。
clear logging asdm	ASDM ログ バッファからすべてのシステム ログ メッセージを削除します。
clear logging buffer	システム ログ バッファからすべてのシステム ログ メッセージを削除します。
clear running-config logging rate-limit	ロギングのレート リミットをデフォルトに戻します。
logging asdm	一部または全部のシステム ログ メッセージを ASDM に送信するように FWSM を設定します。
logging asdm-buffer-size	ASDM に送信する前のメッセージを格納するバッファのサイズを設定します。
logging buffered	一部または全部のシステム ログ メッセージをシステム ログ バッファに保存するように FWSM を設定します。
logging buffer-size	システム メッセージを格納するバッファのサイズを設定します。
logging class	特定のメッセージ クラスの全メッセージを、特定の出力先に送信するように指定します。
logging console	FWSM コンソール セッション中にシステム ログ メッセージが表示されるようにします。
logging debug trace	システム ログへのデバッグ メッセージの保存をイネーブルにします。
logging device-id	EMBLEM 以外のフォーマットのシステム ログ メッセージにデバイス ID を含めるように FWSM を設定します。
logging emblem	Syslog サーバ以外の出力先に送信するシステム ログ メッセージに、EMBLEM フォーマットを使用するように FWSM を設定します。
logging enable	すべての設定済みの出力先へのログをイネーブルにします。
logging facility	システム メッセージ サーバに送信するメッセージに使用するロギング ファシリティを指定します。
logging flash-bufferwrap	バッファがラップする（つまり、バッファが満杯になる）たびにログ バッファの内容を内部フラッシュ メモリに書き込むように、FWSM を設定します。
logging flash-maximum-allocation	FWSM がログ データを保存する内部フラッシュ メモリの最大容量を指定します。
logging flash-minimum-free	FWSM が新しいログ ファイルを保存するときに最低限必要な内部フラッシュ メモリの空き容量を指定します。
logging from-address	FWSM が E メールで送信するシステム ログ メッセージの送信元 E メールアドレスを指定します。
logging ftp-bufferwrap	バッファがラップする（つまり、バッファが満杯になる）たびにログ バッファの内容を FTP サーバに書き込むように、FWSM を設定します。
logging ftp-server	logging ftp-bufferwrap がイネーブルの場合に、FWSM がログ バッファのデータを送信する FTP サーバに関する詳細情報を指定します。
logging history	SNMP ロギングをイネーブルにし、SNMP サーバに送信するメッセージを指定します。
logging host	ログの出力先として Syslog サーバを定義します。

表 1-5 ログイング コマンドの一覧 (続き)

コマンド	説明
logging list	特定の出力先に送信するメッセージのフィルタリングに使用する、メッセージ選択基準のリストを作成または編集します。
logging mail	ログ メッセージを E メールで送信できるように FWSM を設定し、E メールで送信するメッセージを指定します。
logging message	システム ログ メッセージの重大度を抑制または変更できるようにします。
logging monitor	システム ログ メッセージを SSH および Telnet セッションで表示できるように FWSM を設定します。
logging permit-hostdown	正常に動作していない TCP ベースの Syslog サーバに関する新しいネットワーク アクセス セッションを、FWSM が許可するか、それとも拒否するかを指定します。
logging queue	設定された出力先にシステム ログ メッセージを送信する前に、FWSM がシステム ログ キューに格納できるメッセージ数を指定します。
logging rate limit	システム メッセージを生成するレートを制限します。
logging recipient-address	FWSM が E メールで送信するシステム ログ メッセージの受信側の E メール アドレスを指定します。
logging save log	ログ バッファの現在の内容を内部フラッシュ メモリに保存します。
logging standby	フェールオーバーのスタンバイ FWSM が、この FWSM のシステム ログ メッセージをログ出力先に送信できるようにします。
logging timestamp	システム ログ メッセージに、メッセージが生成された日付と時刻が含まれるようにします。
logging trap	FWSM が Syslog サーバに送信するシステム ログ メッセージを指定します。
remote access threshold	FWSM がトラップを送信する、アクティブなリモート アクセス セッション数を指定します。
show logging	現在のログ設定と、システム ログ内部バッファの現在の内容を表示します。
show running-config logging	現在実行中のすべてのログ設定を表示します。
show running-config logging rate-limit	システム メッセージの生成に関するレート制限を表示します。



システム ログ メッセージ

この章では、FWSM のシステム ログ メッセージを示します。メッセージ コードの番号順に各メッセージを示します。



(注)

このマニュアルに記載されているメッセージは、ソフトウェアの Version 3.1 以降に該当します。番号が順序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 コードから除外されています。

この章の内容は、次のとおりです。

- [メッセージ 101001 ~ 199009 \(p.2-2\)](#)
- [メッセージ 201002 ~ 217001 \(p.2-35\)](#)
- [メッセージ 302003 ~ 326028 \(p.2-45\)](#)
- [メッセージ 400000 ~ 418001 \(p.2-76\)](#)
- [メッセージ 500001 ~ 507001 \(p.2-90\)](#)
- [メッセージ 602101 ~ 609002 \(p.2-95\)](#)
- [メッセージ 701001 ~ 720073 \(p.2-106\)](#)

メッセージ 101001 ~ 199009

ここでは、メッセージ 101001 ~ 199009 を示します。

101001

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

説明 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 ケーブルが存在し、正常に機能していることを表します。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

101002

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

説明 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 ケーブルが存在していても、正常に機能していないことを表します。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 フェールオーバー ケーブルを交換してください。

101003、101004

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

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

説明 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であるにも関わらず、フェールオーバー ペアのいずれかの装置でフェールオーバー ケーブルが接続されていない場合に記録されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 フェールオーバー ペアの両方の装置で、フェールオーバー ケーブルを接続してください。

101005

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

説明 フェールオーバー メッセージです。フェールオーバー ケーブルが接続されていても、プライマリ装置がケーブルのステータスを判別できない場合に表示されます。

推奨処置 ケーブルを交換してください。

102001

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

説明 フェールオーバー メッセージです。このメッセージは、プライマリ装置がもう一方の装置でシステム リロードまたは電源障害を検出した場合に記録されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 リロードが実行された装置で `show crashinfo` コマンドを発行し、リロードに関連するトレースバックがあるかどうかを確認します。さらに、装置に電源が投入され、電源コードが正しく接続されているかどうかを確認してください。

103001

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

説明 フェールオーバー メッセージです。プライマリ装置がフェールオーバー ケーブルを介してセカンダリ装置と通信できないときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。表 2-1 に、フェールオーバーが発生した理由を表す理由コードを示します。

表 2-1 理由コード

理由コード	説明
1	フェールオーバー hello が 30 秒以上、検出されていません。フェールオーバー hello は、他方の Cisco ASA 装置上でフェールオーバーが正常に動作していることを示します。
2	インターフェイスが 4 つのフェールオーバー テストのいずれかに失敗しました。4 つのテストとは、1) リンク アップ、2) ネットワーク トラフィックのモニタ、3) ARP テスト、4) ブロードキャスト ping テストです。
3	シリアル ケーブルを介してコマンドが送信されたあと 15 秒以上が経過し、適正な ACK が検出されません。

推奨処置 フェールオーバー ケーブルが正しく接続されていて、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を使用していることを確認してください。問題が解決できない場合は、TAC に連絡してください。

103002

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

説明 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のネットワーク インターフェイスが正常であることを検出した場合に表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。考えられる `interface_number` 変数の値については、FWSM のログと SNMP の設定の表 1-4 を参照してください。

推奨処置 対処は不要です。

103003

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

説明 フェールオーバー メッセージです。プライマリ装置が、セカンダリ装置上に不正なネットワーク インターフェイスを検出したときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 セカンダリ装置上のネットワーク接続、およびネットワークのハブ接続を確認してください。必要に応じて、障害のあるネットワーク インターフェイスを交換してください。

103004

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

説明 フェールオーバー メッセージです。プライマリ装置が、セカンダリ装置から、プライマリの障害を示すメッセージを受信したときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 プライマリ装置のステータスを確認してください。

103005

エラー メッセージ %FWSM-1-103005: (Primary) Other firewall reporting failure.

説明 フェールオーバー メッセージです。セカンダリ装置が、プライマリ装置に対して障害を報告したときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 セカンダリ装置のステータスを確認してください。

104001、104002

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

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

説明 両方ともフェールオーバー メッセージです。スタンバイ装置上で **failover active** コマンドを入力するか、アクティブ装置上で **no failover active** コマンドを入力することによって、これら2つの装置の役割を強制的に切り替えた場合に、通常これらのメッセージが記録されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。*string* 変数として、考えられる値は次のとおりです。

- state check (ステート確認)
- bad/incomplete config (不正または不完全なコンフィギュレーション)
- ifc [interface] check, mate is healthier (インターフェイスの確認、両装置の相違)
- the other side wants me to standby (他方がスタンバイを要求)
- in failed state, cannot be active (障害ステートにより、アクティブにできない)

- switch to failed state (障害ステートへの切り替え)

推奨処置 手動で強制的に切り替えた場合には、対処は不要です。それ以外の場合は、セカンダリ装置により報告された原因を参照し、両方の装置のステータスを確認してください。

104003

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

説明 フェールオーバー メッセージです。プライマリ装置に障害が発生したときに表示されません。

推奨処置 プライマリ装置のシステム ログ メッセージを調べ、問題の原因を確認してください (メッセージ 104001 を参照)。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

104004

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

説明 フェールオーバー メッセージです。障害のあった装置が正常に戻ったときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

105001

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

説明 フェールオーバー メッセージです。コンソールに **no failover** コマンドを入力したときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

105002

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

説明 フェールオーバー メッセージです。フェールオーバーがディセーブルになっていた状態で、引数を指定せずに **failover** コマンドをコンソールに入力したときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

105003

エラー メッセージ %FWSM-1-105003: (Primary) Monitoring on interface
interface_name waiting

説明 フェールオーバー メッセージです。Cisco ASA はフェールオーバー ペアの他方の装置との間で、特定のネットワーク インターフェイスをテスト中です。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。Cisco ASA は標準動作の間、頻繁にネットワーク インターフェイスをモニタします。

105004

エラー メッセージ %FWSM-1-105004: (Primary) Monitoring on interface
interface_name normal

説明 フェールオーバー メッセージです。特定のネットワーク インターフェイスのテストが正常に完了しました。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

105005

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

説明 フェールオーバー メッセージです。フェールオーバー ペアの装置が他方の装置と通信できない状態を示しています。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 特定のインターフェイスに接続しているネットワークが正常に動作しているかどうかを確認してください。

105006、105007

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

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

説明 両方ともフェールオーバー メッセージです。特定のインターフェイスのリンク ステータスのモニタ結果を示しています。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 リンク ステータスがダウンの場合には、特定のインターフェイスに接続しているネットワークが正常に動作しているかどうかを確認してください。

105008

エラー メッセージ %FWSM-1-105008: (Primary) Testing interface *interface_name*.

説明 フェールオーバー メッセージです。特定のネットワーク インターフェイスのテスト中に表示されます。このテストは、Cisco ASA が特定のインターフェイス上のスタンバイ装置から、一定時間を経過してもメッセージを受信できなかった場合にのみ実行されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

105009

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

説明 フェールオーバー メッセージです。このメッセージでは、直前に実行されたインターフェイス テストの結果(Passed または Failed)が報告されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 結果が Passed の場合、対処は不要です。結果が Failed の場合は、両方のフェールオーバー装置にネットワーク ケーブルが正しく接続されているかどうか、ネットワークが正常に動作しているかどうかを確認し、さらにスタンバイ装置のステータスを確認してください。

105010

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

説明 ブロック メモリが不足しています。これは一時的なメッセージで、Cisco ASA は回復処理を行います。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 show blocks コマンドを使用して、現在のブロック メモリの状態をモニタしてください。

105011

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

説明 フェールオーバー ケーブルが原因で、プライマリ装置とセカンダリ装置間の通信ができません。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

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てください。

105020

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

説明 フェールオーバーを実行したとき、アクティブ Cisco ASA がメモリ内にコンフィギュレーションの一部だけを検出しました。通常、複製サービスに割り込みが発生したことが原因です。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 Cisco ASA がフェールオーバーを検出すると、Cisco ASA は自動的に自身をリロードし、フラッシュメモリからコンフィギュレーションをロードするか、他方の Cisco ASA と再同期します。フェールオーバーが頻繁に発生している場合は、フェールオーバー設定をチェックし、両方の Cisco ASA 装置が互いに通信できることを確認してください。

105021

エラー メッセージ %FWSM-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中に、他の何らかのプロセスによるコンフィギュレーションのロックが5分を超えると、スタンバイ装置は自身をリロードします。これにより、フェールオーバー プロセスで新しいコンフィギュレーションが適用される事態が防止されます。この状況は、コンフィギュレーションの同期化が進行しているときに、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を呼び出したときに発生する場合があります。`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 スタンバイ装置をアップにして、アクティブ装置とフェールオーバー接続を確立している間に、コンフィギュレーションを表示または変更しないでください。

105031

エラー メッセージ %FWSM-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 対処は不要です。

105032

エラー メッセージ %FWSM-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てください。速度およびデュプレックスの設定が正しいかどうかを確認します。

105034

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

説明 ピアが起動し、初期コンタクトメッセージを送信しました。

推奨処置 対処は不要です。

105035

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

説明 ピアの 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 モードの場合、アクティブ モードに切り替わります。

推奨処置 ピアの LAN フェールオーバー インターフェイスの接続を確認してください。

105036

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

説明 Cisco ASA が確認応答できない 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。LAN フェールオーバー インターフェイスに接続の問題があることを示しています。

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かどうかを確認してください。

105037

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

説明 プライマリ装置とスタンバイ装置が交互にアクティブ装置になっています。LAN フェールオーバー接続に問題があるか、ソフトウェアのバグを示しています。

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かどうかを確認してください。

105038

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

説明 フェールオーバーを実行したとき、アクティブ Cisco ASA がメモリ内にコンフィギュレーションの一部だけを検出しました。通常、複製サービスに割り込みが発生したことが原因です。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 Cisco ASA がフェールオーバーを検出すると、Cisco ASA は自動的に自身をリロードし、フラッシュメモリからコンフィギュレーションをロードするか、他方の Cisco ASA と再同期します。フェールオーバーが頻繁に発生している場合は、フェールオーバー設定をチェックし、両方の Cisco ASA 装置が互いに通信できることを確認してください。

105039

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

説明 フェールオーバーでは、最初に、プライマリとセカンダリの Cisco ASA に同数のインターフェイスが設定されているかどうかを確認されます。このメッセージは、プライマリ Cisco ASA がセカンダリ Cisco ASA に設定されているインターフェイス数を確認できなかったことを示しています。これは、プライマリ Cisco ASA がフェールオーバー インターフェイス上でセカンダリ Cisco ASA と通信できないことを意味しています。セカンダリ Cisco ASA の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 フェールオーバー LAN、インターフェイス設定、およびプライマリとセカンダリ Cisco ASA のステータスを確認してください。セカンダリ Cisco ASA が Cisco ASA アプリケーションを実行していて、フェールオーバーがイネーブルであることを確認します。

105040

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

説明 フェールオーバー ペアとして動作するには、プライマリとセカンダリ Cisco ASA が同じフェールオーバー ソフトウェア バージョンを実行している必要があります。このメッセージは、セカンダリ Cisco ASA のフェールオーバー ソフトウェアのバージョンが、プライマリ Cisco ASA と互換でないことを示しています。プライマリ Cisco ASA 上でフェールオーバーがディセーブルです。セカンダリ Cisco ASA の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 フェールオーバーをイネーブルにするには、プライマリとセカンダリ Cisco ASA に同一のソフトウェア バージョンを使用してください。

105042

エラー メッセージ %FWSM-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 へのフェールオーバー メッセージの送信に使用するインターフェイスは機能しています。セカンダリ Cisco ASA の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

105043

エラー メッセージ %FWSM-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てください。速度およびデュプレックスの設定が正しいかどうかを確認します。

105044

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

説明 フェールオーバー ピア間で動作モード (シングルまたはマルチ) が一致していない場合、フェールオーバーはディセーブルになります。

推奨処置 フェールオーバー ピアを同じ動作モードに設定し、フェールオーバーを再びイネーブルにしてください。

105045

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

説明 フェールオーバー ピア間で機能ライセンスが一致しない場合、フェールオーバーはディセーブルになります。

推奨処置 フェールオーバー ピアに同じ機能ライセンスを設定し、フェールオーバーを再びイネーブルにしてください。

105046

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

説明 2台のフェールオーバー装置のシャーシ タイプが異なる場合に、このメッセージが発行されます。

推奨処置 2台のフェールオーバー装置が同じであるかどうかを確認してください。

105047

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

説明 2台のフェールオーバー装置の対応するスロットに搭載されているカード タイプが異なります。

推奨処置 フェールオーバー装置のカード構成が同じであるかどうかを確認してください。

106001

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

説明 接続関連メッセージです。内部アドレスへの接続の試みが、セキュリティ ポリシーによって拒否されたときに発生します。*tcp_flags* の値は、接続が拒否された時点の TCP ヘッダー内のフラグに対応します。たとえば、TCP パケットの到達時に Cisco ASA に接続ステートが存在しない場合、そのパケットはドロップされます。このパケットの *tcp_flags* は、FIN および ACK です。*tcp_flags* は、次のとおりです。

- ACK 確認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 受信側がアプリケーションにデータを転送しました。
- RST 接続がリセットされました。
- SYN 接続を開始するためにシーケンス番号が同期化されました。
- URG 緊急ポインタが有効と宣言されました。

推奨処置 対処は不要です。

106002

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

説明 接続関連メッセージです。**outbound deny** コマンドにより、特定の接続に失敗したときに表示されます。*protocol* 変数は、ICMP、TCP、または UDP です。

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

106006

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

説明 接続関連メッセージです。セキュリティ ポリシーによって着信 UDP パケットが拒否されたときに表示されます。

推奨処置 対処は不要です。

106007

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

説明 接続関連メッセージです。DNS クエリまたは DNS 応答を含む UDP パケットが拒否されたときに表示されます。

推奨処置 内部ポート番号が 53 の場合、内部ホストは通常、キャッシング ネーム サーバとして設定されています。UDP ポート 53 でトラフィックを許可する `access-list` コマンドステートメントを追加してください。外部ポート番号が 53 の場合には、DNS サーバの応答がかなり遅いため、クエリが他のサーバによって応答されています。

106010

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

説明 接続関連メッセージです。セキュリティ ポリシーによって着信接続が拒否されたときに表示されます。

推奨処置 トラフィックを許可する場合、セキュリティ ポリシーを修正します。このメッセージが一定間隔で発生する場合は、リモート ピアの管理者に連絡してください。

106011

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

説明 Web ブラウザを使用してインターネットにアクセスしている内部ユーザが存在する場合、通常のトラフィック状況下でこのメッセージが表示されます。接続がリセットされると、Cisco ASA がリセットを受信したあとで、接続の反対側のホストがパケットを送信し、このメッセージが表示されます。通常、このメッセージは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&` サーバにロギングされないようにしてください。

106012

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

説明 パケット完全性チェック メッセージです。IP オプションを持つ IP パケットが検出されました。IP オプションはセキュリティ上のリスクとみなされるので、パケットは廃棄されます。

推奨処置 リモート ホスト システム管理者に連絡し、問題を解決してください。ローカル サイトの設定が、ルース ソース ルーティングまたはストリクト ソース ルーティングのどちらであるかを確認してください。

106013

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

説明 Cisco ASA が、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。パケットを受信すべき PAT ホストを特定できない着信パケットは、廃棄されます。

推奨処置 対処は不要です。

106014

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

説明 Cisco ASA が着信 ICMP パケット アクセスを拒否しました。デフォルトでは、特に許可されないかぎり、すべての ICMP パケットがアクセスを拒否されます。

推奨処置 対処は不要です。

106015

エラーメッセージ %FWSM-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 が、Cisco ASA の接続テーブルで接続が関連付けられていない TCP パケットを廃棄しました。Cisco ASA はパケット内の SYN フラグ（新しい接続の確立要求を示す）を検索します。SYN フラグが見つからず、なおかつ既存の接続が存在しない場合、Cisco ASA は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している場合には、対応が必要です。その場合は、パケットの送信元を追跡して、これらのパケットが送信された理由を判別してください。

106016

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

説明 Cisco ASA が、無効な送信元アドレスを持つパケットを廃棄しました。無効な送信元アドレスとは、次に属するアドレスのことです。

- ループバック ネットワーク (127.0.0.0)
- ブロードキャスト (制限付き、ネット向け、サブネット向け、および全サブネット向け)
- 宛先ホスト (land.c)

スプーフパケットの検出をさらに強化するには、**conduit** コマンドを使用して、送信元アドレスが内部ネットワークに属するパケットを廃棄するように Cisco ASA を設定します。**icmp** コマンドが実装されているので、**conduit** コマンドは否定され、正常に動作する保証がなくなっています。

推奨処置 外部ユーザが保護されたネットワークに危害を加えようとしているかどうかを確認してください。誤って設定されているクライアントがないかどうかを確認してください。

106017

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

説明 Cisco ASA が、IP 宛先と IP 送信元アドレスが等しく、宛先ポートと送信元ポートが等しいパケットを受信しました。これは、システムを攻撃する目的のスプーフ パケットを意味しています。この攻撃は、Land Attack と呼ばれています。

推奨処置 このメッセージが頻発する場合、攻撃が進行している可能性があります。このパケットには、攻撃の発信元を特定する十分な情報はありません。

106018

エラー メッセージ %FWSM-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*) に宛てられた特定の ICMP タイプの発信 ICMP 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 対処は不要です。

106020

エラー メッセージ %FWSM-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重複フラグメントのいずれかが含まれている teardrop 署名を持つ IP パケットを廃棄したことを示しています。これは、Cisco ASA または Intrusion Detection System (IDS; 侵入検知システム) を回避しようとした悪意あるイベントです。

推奨処置 リモート ピアの管理者に連絡するか、セキュリティ ポリシーに従って報告してください。

106021

エラー メッセージ %FWSM-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。誰かが着信接続上で IP アドレスのスプーフィングを試みています。リバース ルート ルックアップとも呼ばれるユニキャスト RPF により、ルートと矛盾する送信元アドレスを持つパケットが検出され、Cisco ASA 上で攻撃の一部であるとみなされました。

ip verify reverse-path コマンドを使用してユニキャスト RPF をイネーブルにしたとき、このメッセージが表示されます。この機能は、インターフェイスに入力されるパケットに対して作用します。この機能を外部に設定した場合、Cisco ASA は外部から着信するパケットをチェックします。

Cisco ASA は *source_address* に基づいてルートを検索します。エントリが見つからずルートが定義されていない場合、このシステム ログ メッセージが表示され、接続は切断されます。

ルートが存在する場合、Cisco ASA はそのルートがどのインターフェイスに対応するかをチェックします。パケットが別のインターフェイスに着信した場合、スプーフか、または宛先へのパスが複数ある非対称ルーティング環境が存在しています。Cisco ASA は非対称ルーティングをサポートしていません。

Cisco ASA を内部インターフェイスに設定している場合、スタティックな `route` コマンドステートメントまたは RIP がチェックされます。source_address が見つからない場合、内部ユーザがそれらのアドレスをスプーフィングしています。

推奨処置 攻撃が進行中でも、この機能がイネーブルであれば、対処は不要です。Cisco ASA が攻撃を拒絶します。

106022

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

説明 特定の接続に一致するパケットが、その接続が開始されるインターフェイスとは異なるインターフェイスに着信しました。

たとえば、ユーザが内部インターフェイス上で接続を開始したにもかかわらず、Cisco ASA が境界インターフェイス上で同じ接続の到着を検知した場合、Cisco ASA には1つの宛先に対して複数のパスが存在することになります。この状況を非対称ルーティングといいます。Cisco ASA では非対称ルーティングはサポートされていません。

また、攻撃者が Cisco ASA に侵入するための手段として、1つの接続から別の接続にパケットを追加しようとしている可能性もあります。いずれの場合も、Cisco ASA はこのメッセージを表示し、接続を切断します。

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てください。

106023

エラー メッセージ %FWSM-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 ACL (アクセス制御リスト) によって IP パケットが拒否されました。このメッセージは、ACL に対し、`log` オプションをイネーブルに設定していない場合にも表示されます。

推奨処置 同じ送信元アドレスについて、このメッセージが続いて表示される場合は、フットプリンティングまたはポート スキャン攻撃が試みられている可能性があります。リモートホストの管理者に連絡してください。

106024

エラー メッセージ %FWSM-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不足が発生しました。アクセスリストが最後にコンパイルされてから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、最後にコンパイルされた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 アクセスリスト、AAA、ICMP、SSH、Telnet、およびその他のルールタイプは、アクセスリストルールタイプとして保存およびコンパイルされます。これらのルールタイプの一部を削除して、他のルールタイプを追加できるようにしてください。

106025、106026

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

説明 複数コンテキスト モードでパケットのセキュリティ コンテキストを判別できません。どちらのメッセージも、ルータおよびトランスペアレント モードでパケットがドロップされた場合に表示される可能性があります。

推奨処置 対処は不要です。

106027

エラー メッセージ %FWSM-4-106027:Failed to determine the security context for the packet:vlansource Vlan#:ethertype src sourceMAC dst destMAC

説明 複数コンテキスト モードでパケットのセキュリティ コンテキストを判別できません。このメッセージは、非 IP パケットがトランスペアレント モードでドロップされた場合のみ、生成されます。

推奨処置 対処は不要です。

106100

エラー メッセージ %FWSM-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 ステートメントに一致しました。メッセージのレベルは、access-list コマンドで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、最初のヒットまたは一定期間における総ヒット件数のいずれかを表します。このメッセージは、メッセージ 106023 (拒否されたパケットだけを記録し、ヒット カウントや設定可能なレベルは含まない) よりも多くの情報を提供します。次に、このメッセージの値を示します。

- permitted | denied | est-allowed これらの値は、パケットが ACL によって許可 (または拒否) されたことを示します。値が est-allowed である場合、パケットは ACL によって拒否されましたが、確立済みのセッションには許可されています (たとえば、内部ユーザがインターネットのアクセスを許可された場合、通常は ACL によって拒否される応答パケットでも受け入れられます)。
- protocol TCP、UDP、ICMP、または IP プロトコル番号
- interface_name ログインされた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 ログインされたフローの送信元 IP アドレス
- dest_address ログインされたフローの宛先 IP アドレス

- *source_port* ログされた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* ログされた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* 設定された期間内で、このフローがこの ACL エントリによって許可または拒否された回数。このフローに関して Cisco ASA が初めてこのシステム ログ メッセージを生成する時点では、この値は 1 です。
- *first hit* このフローに関して最初に生成されたメッセージ
- *number-second interval* ヒット カウントを累積する時間。このインターバルは、**access-list** コマンドで **interval** オプションを指定して設定します。

推奨処置 対処は不要です。

106101

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

説明 ACL deny ステートメント (**access-list id deny** コマンド) に **log** オプションを設定している場合に、トラフィック フローがこの ACL ステートメントに一致すると、Cisco ASA はそのフロー情報をキャッシュに保管します。Cisco ASA 上でキャッシュに保管された一致フロー数が、ユーザの設定による (**access-list deny-flow-max** コマンド) 制限数を超えると、このメッセージが表示されます。

number 値は、**access-list deny-flow-max** コマンドで設定された制限数です。

推奨処置 対処は不要です。DoS 攻撃の結果、このメッセージが表示される場合があります。

107001

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

説明 アラート ログ メッセージです。Cisco ASA が不正認証の RIP 応答メッセージを受信しました。ルータまたはセキュリティ アプライアンスの設定が誤っているか、または Cisco ASA のルーティング テーブルに対する攻撃が失敗したためにこのメッセージが表示された可能性があります。

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、モニタする必要があります。メッセージに示されている送信元 IP アドレスが未知のアドレスである場合には、信頼できるエンティティ間の RIP 認証キーを変更してください。攻撃者が既存のキーを判別しようとしている可能性があります。

107002

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

説明 アラート ログ メッセージです。このメッセージの原因としては、ルータのバグ、非 RFC 値を含むパケット、または不正エントリが考えられます。これは通常の状態ではなく、Cisco ASA のルーティング テーブルの悪用が試みられている可能性があります。

推奨処置 このメッセージは攻撃の可能性を示しているので、モニタする必要があります。パケットが認証された場合、有効であれば、パケット内に不正データが含まれています。状況をモニタし、パケットの発信者が疑わしい場合には、キーを変更してください。

108002

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

説明 `fixup protocol smtp` コマンドによって生成されるメール ガード (SMTP) メッセージです。Cisco ASA が電子メール アドレス内の無効な文字をスペースに置き換えたときに表示されます。

推奨処置 対処は不要です。

108003

エラー メッセージ %FWSM-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 メール ガード (SMTP) によって生成されるメッセージです。Cisco ASA が電子メール アドレス内に悪意あるパターンを検出し、接続を切断したときに表示されます。攻撃が進行中であることを示します。

推奨処置 対処は不要です。

109001

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

説明 Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) メッセージです。Cisco ASA に AAA が設定されていて、特定のユーザからの認証要求が検出されたときに表示されます。

推奨処置 対処は不要です。

109002

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

説明 AAA メッセージです。モジュールが特定の認証サーバと通信できなかったため、認証要求に失敗したときに表示されます。

推奨処置 特定の認証サーバ上で、認証デーモンが実行されているかどうかを確認してください。

109003

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

説明 AAA メッセージです。認証サーバを検出できないときに表示されます。

推奨処置 Cisco ASA から認証サーバに ping を実行してください。デーモンが実行されているかどうかを確認してください。

109005

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

説明 AAA メッセージです。特定の認証要求に成功したときに表示されます。

推奨処置 対処は不要です。

109006

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

説明 AAA メッセージです。不正パスワードなどの原因により、特定の認証要求に失敗したときに表示されます。

推奨処置 対処は不要です。

109007

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

説明 AAA メッセージです。特定の許可要求に成功したときに表示されます。

推奨処置 対処は不要です。

109008

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

説明 AAA メッセージです。不正パスワードなどの原因により、ユーザが特定のアドレスへのアクセスを許可されなかったときに表示されます。

推奨処置 対処は不要です。

109010

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

説明 AAA メッセージです。サーバ上で待機中の要求が多すぎるため、認証要求を処理できないときに表示されます。

推奨処置 認証サーバによる認証要求への応答が遅すぎないかどうかを確認してください。**floodguard enable** コマンドを使用して、Flood Defender 機能をイネーブルにしてください。

109011

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

説明 ホストと Cisco ASA 間で認証セッションが開始され、まだ完了していません。

推奨処置 対処は不要です。

109012

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

説明 認証キャッシュのタイムアウトが発生しました。ユーザは次の接続で再認証する必要があります。このタイマーの長さは、**timeout uauth** コマンドで変更できます。

推奨処置 対処は不要です。

109013

エラーメッセージ %FWSM-3-109013: User must authenticate before using this service

説明 ユーザがサービスを使用するには、認証される必要があります。

推奨処置 サービスを使用する前に、FTP、Telnet、または HTTP を使用して認証を受けてください。

109014

エラーメッセージ %FWSM-7-109014: uauth_lookup_net fail for uauth_in()

説明 認証要求に、対応する許可要求がありませんでした。

推奨処置 コンフィギュレーションに `aaa authentication` および `aaa authorization` コマンドが両方とも含まれているかどうかを確認してください。

109016

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

説明 AAA サーバでこのユーザ用に定義されているアクセス制御リストが、Cisco ASA 上に存在しません。Cisco ASA を設定する前に AAA サーバを設定すると、このエラーが発生することがあります。AAA サーバ上の Vender-Specific Attribute (VSA) の値は、次のいずれかです。

- `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 サーバ上で指定されている名前と同じ名前を使用してください。

109017

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

説明 ユーザが認証プロキシの制限値を超過しており、プロキシへの接続が多すぎます。

推奨処置 `proxy-limit proxy_limit` コマンドを使用してプロキシの制限値を大きくするか、使用していない接続を閉じるようにユーザに指示します。このエラーが頻発する場合は、DoS 攻撃の可能性がります。

109018

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

説明 ダウンロードされた許可アクセス制御リストに ACE がありません。この状況の原因としては、アトリビュート ストリング [ip:inacl#] のスペルが間違っているか、または `access-list` コマンドが脱落していることが考えられます。

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

推奨処置 AAA サーバ上でエラーを示した ACL コンポーネントを訂正してください。

109019

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

説明 ダウンロードされた許可アクセス制御リストのアトリビュート ストリング ip:inacl#NNN= で、シーケンス番号 NNN の解析中にエラーが検出されました。理由としては、= が脱落している、数値以外の値が含まれている、[#] と [=] の間にスペース以外の文字がある、NNN が 999999999 より大きいことが考えられます。

```
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 AAA サーバ上でエラーを示した ACL 要素を訂正してください。

109020

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

説明 ダウンロードされた許可アクセス制御リストのいずれかのコンポーネントに、設定の誤りがあります。システム ログ メッセージには、この要素のテキスト全体が含まれます。このメッセージの原因は通常、無効な `access-list` コマンド ステートメントによります。

推奨処置 AAA サーバ上でエラーを示した ACL コンポーネントを訂正してください。

109021

エラー メッセージ %FWSM-7-109021: Uauth null proxy error

説明 内部的なユーザ認証エラーが発生しました。

推奨処置 対処は不要です。ただし、このエラーが繰り返し発生する場合は、Cisco TAC に連絡してください。

109022

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

説明 HTTPS 認証ごとに、Cisco ASA は1つのプロセスを使用して認証要求を処理します。同時に実行するプロセス数が、システムでの最大数を超えると、Cisco ASA は認証を実行なくなり、このメッセージが表示されます。

推奨処置 対処は不要です。

109023

エラー メッセージ %FWSM-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 AAA メッセージです。このサービス ポートを使用するには、設定されたポリシーに基づいて認証を受ける必要があります。

推奨処置 Telnet、FTP、または HTTP を使用して認証を実行してから、上記のサービス ポートの使用を試みてください。

109024

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

説明 AAA メッセージです。Cisco ASA に AAA が設定されていて、ユーザが事前認証なしで Cisco ASA 経由での TCP 接続を試みたときに表示されます。

推奨処置 対処は不要です。

109025

エラー メッセージ %FWSM-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 アクセス制御リストによるチェックに失敗しました。このチェックで deny 条件に一致したか、または一致する条件がありませんでした(暗黙的 deny)。Cisco Secure Access Control Server (ACS)上の AAA 許可ポリシーに基づいて定義されたユーザ アクセス制御リスト *acl_ID* によって、接続が拒否されました。

推奨処置 対処は不要です。

109026

エラー メッセージ %FWSM-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.

説明 AAA サーバからの応答の有効性を確認できませんでした。不正なサーバ キーが設定されている可能性があります。このイベントは、RADIUS または TACACS+ サーバとのトランザクション中に発生することがあります。

推奨処置 `aaa-server` コマンドで設定されているサーバ キーが正しいかどうかを確認してください。

109027

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

説明 AAA サーバからの応答の有効性を確認できませんでした。設定されているサーバ キーが不正であると考えられます。このメッセージは、RADIUS 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、関係する AAA サーバの IP アドレスです。*user* は、接続に対応付けられたユーザ名です。

推奨処置 `aaa-server` コマンドで設定されているサーバ キーが正しいかどうかを確認してください。

109028

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

説明 設定されている AAA ルールに一致するセキュリティ トラフィックに関して、AAA がバイパスされています。同じセキュリティ レベルに設定された 2 つのインターフェイスをトラフィックが通過し、同じセキュリティ トラフィックが許可され、なおかつ AAA 設定で `include` または `exclude` 構文が使用されている場合にのみ、この状況が発生することがあります。

推奨処置 対処は不要です。

109030

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

説明 RADIUS サーバに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い場合に、このメッセージが表示されます。ネットマスクがワイルドカードか、それとも通常のネットマスクであるかを、このメカニズムで判別できない場合に、この問題が発生します。

access_list 変換できなかったアクセス リスト

source 送信元の IP アドレス

dest 宛先の IP アドレス

netmask 送信元または宛先アドレスのサブネットマスク（ドット付き 10 進表記）

推奨処置 RADIUS サーバ上のアクセス リストのネットマスクに、ワイルドカードが設定されているかどうかを確認します。ネットマスクがワイルドカードであり、なおかつサーバ上のすべてのアクセス リスト ネットマスクがワイルドカードである場合には、AAA サーバの `acl-netmask-convert` に `wildcard` 設定を使用します。そうでない場合には、ネットマスクを通常のネットマスク、またはホールのないワイルドカード ネットマスクに変更します。言い換えると、ネットマスクがバイナリ 1 の連なり（たとえば、00000000.00000000.00011111.11111111 または 16 進 0.0.31.255）を表す場合です。マスクが通常のマスクであり、そのサーバ上のすべてのアクセス リスト ネットマスクが通常のマスクである場合には、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 %FWSM-4-109031: NT Domain Authentication Failed: rejecting guest login for *username*.

説明 ゲスト アカウント アクセス用に設定された NT 認証ドメインに対してユーザが認証を試み、ユーザ名が NT サーバ上で有効なユーザ名でない場合に、このメッセージが表示されます。接続は拒否されます。

推奨処置 ユーザが有効なユーザである場合は、NT サーバにアカウントを追加してください。ユーザにアクセスを許可しない場合は、処置は不要です。

111003

エラー メッセージ %FWSM-5-111003: *IP_address* Erase configuration

説明 管理メッセージです。コンソールで `write erase` コマンドを入力し、フラッシュ メモリの内容が消去されたときに表示されます。*IP_address* 値は、ログインがコンソール ポート経由か、または Telnet 接続を使用して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場合には、Cisco ASA を再設定し、新しいコンフィギュレーションを保存する必要があります。あるいは、フロッピーまたはネットワーク上の TFTP サーバに保存されている既存のコンフィギュレーションから情報を復元することもできます。

111004

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

説明 `config floppy/memory/network` コマンドまたは `write floppy/memory/network/standby` コマンドを入力したときに表示されるメッセージです。*IP_address* 値は、ログインがコンソール ポート経由か、または Telnet 接続を使用して行われたかを示します。

推奨処置 メッセージが OK で終わっている場合、対処は不要です。メッセージに障害が示されている場合には、問題の解決を試みてください。たとえば、フロッピー ディスクに保存する場合には、フロッピー ディスクが書き込み保護されていないこと、TFTP サーバに保存する場合には、サーバが稼働していることを確認します。

111005

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

説明 コンフィギュレーション モードを終了すると表示されるメッセージです。*IP_address* 値は、ログインがコンソール ポート経由か、または Telnet 接続を使用して行われたかを示します。

推奨処置 対処は不要です。

111007

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

説明 コンフィギュレーションを読み込むために、**reload** コマンドまたは **configure** コマンドを入力したときに表示されるメッセージです。*device* には、floppy、memory、net、standby、または terminal が表示されます。*IP_address* 値は、ログインがコンソール ポート経由か、または Telnet 接続を使用して行われたかを示します。

推奨処置 対処は不要です。

111008

エラー メッセージ %FWSM-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変更するコマンドを入力しました。

推奨処置 対処は不要です。

111009

エラー メッセージ %FWSM-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変更しないコマンドを入力しました。

推奨処置 対処は不要です。

111111

エラー メッセージ %FWSM-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 このエラー 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に先立つイベントに関する詳細情報とともに、TAC に提出してください。

112001

エラーメッセージ %FWSM-2-112001: (string:dec) Clear complete.

説明 モジュールのコンフィギュレーションをクリアする要求が完了したときに表示されるメッセージです。送信元ファイルおよび行番号が表示されます。

推奨処置 対処は不要です。

113001

エラーメッセージ %FWSM-3-113001: Unable to open AAA session. Session limit [limit] reached.

説明 システム リソースが使用不能のため、IPSec トンネルに対する AAA 動作が実行できませんでした。limit 値は、同時に実行できる AAA トランザクションの最大数を表します。

推奨処置 可能であれば、AAA リソースに対する要求を減らしてください。

113003

エラーメッセージ %FWSM-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対応付けられたグループポリシーが、ユーザ固有のポリシー *policy_name* によって上書きされています。*policy_name* は、LOCAL 認証を設定するときに *username* コマンドで設定したポリシー名か、または RADIUS 認証を設定するときに RADIUS CLASS アトリビュートで返されるポリシー名です。

推奨処置 対処は不要です。

113004

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

説明 IPSec 接続の AAA 動作が正常に完了したことを示すメッセージです。AAA タイプは、[authentication]、[authorization]、または [accounting] です。*server_IP_address* は、関係する AAA サーバの IP アドレスです。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113005

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

説明 IPSec 接続に対応付けられたユーザに関する認証要求または許可要求が拒否されたことを示すメッセージです。要求が拒否された理由は、*reason* フィールドに表示されます。*server_IP_address* は、関係する AAA サーバの IP アドレスです。*user* は、接続に対応付けられたユーザ名です。*aaa_operation* は、authentication (認証) または authorization (許可) です。

推奨処置 対処は不要です。

113006

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

説明 ローカルに設定されたユーザがロックアウトされています。このユーザに関する認証が一定の回数にわたって連続的に失敗し、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しないかぎり、今後も認証が失敗することを示しています。*user* は現在ロックされているユーザです。*number* は、`aaa local authentication attempts max-fail` コマンドで設定されている連続的な失敗のスレッシュホールドです。

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、または許容される連続的な認証失敗の最大回数を調整してください。

113007

エラー メッセージ %FWSM-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` コマンドで設定されている連続的な認証失敗の最大回数を超過してロックアウトされたあと、特定の管理者によってアンロックされました。

推奨処置 対処は不要です。

113008

エラー メッセージ %FWSM-6-113008: AAA transaction status ACCEPT: user = *user*

説明 IPSec 接続に対応付けられたユーザに関する AAA トランザクションが正常に完了しました。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113009

エラーメッセージ %FWSM-6-113009: AAA retrieved default group policy *policy* for user *user*

説明 IPSec の認証または許可の処理中に、このメッセージが表示される場合があります。**tunnel-group** コマンドで指定されているグループ ポリシーの属性が取得されました。

推奨処置 対処は不要です。

113010

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

説明 IPSec 接続の認証で、SecurID サーバを使用して認証が実行された場合に、このメッセージが表示されることがあります。認証に先立って、ユーザにさらに情報を要求するプロンプトが表示されます。*server_IP_address* は、関係する AAA サーバの IP アドレスです。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113011

エラーメッセージ %FWSM-6-113011: AAA retrieved user specific group policy *policy* for user *user*

説明 IPSec 接続の認証または許可の処理中に、このイベントが発生する場合があります。**tunnel-group** コマンドで指定されているグループ ポリシーの属性が取得されました。

推奨処置 対処は不要です。

113012

エラーメッセージ %FWSM-6-113012: AAA user authentication Successful: local database : user = *user*

説明 IPSec 接続に対応付けられたユーザが、ローカル ユーザ データベースで正常に認証されました。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113013

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

説明 IPSec 接続に対応付けられたユーザに関する AAA トランザクションが、エラーのため失敗したか、またはポリシー違反のため拒否されました。詳細情報は *reason* フィールドで提供されます。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113014

エラー メッセージ %FWSM-6-113014: AAA authentication server not accessible:
server = server_IP_address: user = user

説明 IPSec 接続に対応する AAA トランザクション中に、デバイスが設定された AAA サーバと通信できませんでした。aaa-server グループで設定されているバックアップサーバと、これらのサーバの可用性に応じて、ユーザの接続の試みが失敗したことを表す場合もあれば、そうでない場合もあります。

推奨処置 設定されている AAA サーバとの接続を確認してください。

113015

エラー メッセージ %FWSM-6-113015: AAA user authentication Rejected: reason =
reason : local database: user = user

説明 IPSec 接続に対応付けられたユーザに関して、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は、*reason* フィールドで表示されます。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113016

エラー メッセージ %FWSM-6-113016: AAA credentials rejected: reason = reason:
server = server_IP_address: user = user

説明 IPSec 接続に対応付けられたユーザに関する AAA トランザクションが、エラーのため失敗したか、またはポリシー違反のため拒否されました。詳細情報は *reason* フィールドで表示されます。*server_IP_address* は、関係する AAA サーバの IP アドレスです。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113017

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

説明 IPSec 接続に対応付けられたユーザに関する AAA トランザクションが、エラーのため失敗したか、またはポリシー違反のため拒否されたことを示すメッセージです。詳細情報は *reason* フィールドで表示されます。このイベントは、外部 AAA サーバではなくローカル ユーザ データベースを使用する AAA トランザクションの場合にのみ表示されます。*user* は、接続に対応付けられたユーザ名です。

推奨処置 対処は不要です。

113018

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

説明 認証サーバから、サポートされないフォーマットの ACL エントリがダウンロードされました。このメッセージの値について、次に説明します。

- *user* ログインを試みたユーザ
- *ACL_entry* 認証サーバからダウンロードされた、サポートされない ACL エントリ
- *action* サポートされない ACL エントリを検出したときに実行されたアクション

推奨処置 管理者は、サポートされる ACL エントリのフォーマットに適合するよう、認証サーバ上の ACL エントリを変更する必要があります。

113019

エラー メッセージ %FWSM-4-113019: Group = *group*, Username = *user*, IP = *peer_address*,
Session disconnected. Session Type: *type*, Duration: *duration*, Bytes xmt: *count*,
Bytes rcv: *count*,

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 ピアのアドレス
type セッション タイプ (IPSec、UDP など)
duration 接続の持続時間
count バイト数

推奨処置 対処は不要です。

199001

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

説明 reload コマンドにより、Cisco ASA の再起動を開始したホストのアドレスを示すメッセージです。

推奨処置 対処は不要です。

199002

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

説明 Cisco ASA が初期ブートとフラッシュ メモリの読み込みシーケンスを終了し、正常に動作でき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ディセーブルにすることはできません。

推奨処置 対処は不要です。

199003

エラー メッセージ %FWSM-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 を使用する外部ネットワークからパケットを受信しました。この場合、Cisco ASA は外部ホストに ICMP メッセージを送信し、適切な MTU をネゴシエートします。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ます。

推奨処置 対処は不要です。

199005

エラー メッセージ %FWSM-6-199005: Startup begin

説明 Cisco ASA が起動しました。

推奨処置 対処は不要です。

199006

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

説明 リロード動作が開始されたとき、このメッセージが生成されます。

- *when* 順序に従ったリロード動作が開始された時刻。時刻のフォーマットは、hh:mm:ss timezone weekday month day year です (例: 13:23:45 UTC Sun Dec 28 2003)。
- *whom* リロードをスケジュールしたユーザまたはシステム
- *reason* リロードの理由。完全な理由が表示されない場合、*unspecified* というストリングが表示されます。

推奨処置 対処は不要です。

199007

エラーメッセージ %FWSM-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時点で、すべてのアプリケーションは、そのコンテキストまたはインターフェイスへのチャネルをすべて閉じる必要があります。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へのチャネルを閉じていなかったアプリケーションが、現在その動作を実行していることを示します。

推奨処置 対処は不要です。

199008

エラーメッセージ %FWSM-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時点で、すべてのアプリケーションは、そのコンテキストまたはインターフェイスへのチャネルをすべて閉じる必要があります。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へのチャネルを閉じていなかったアプリケーションが、現在その動作を実行していることを示します。

推奨処置 対処は不要です。

199009

エラーメッセージ %FWSM-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時点で、すべてのアプリケーションは、そのコンテキストまたはインターフェイスへのチャネルをすべて閉じる必要があります。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へのチャネルを閉じていなかったアプリケーションが、現在その動作を実行していることを示します。

推奨処置 対処は不要です。

メッセージ 201002 ~ 217001

ここでは、メッセージ 201002 ~ 217001 を示します。

201002

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

説明 接続関連メッセージです。特定のグローバルアドレスへのTCP接続が最大数を越えたときに表示されます。*econns* 変数は初期接続の最大数、*nconns* 変数はスタティックまたは変換(xlate)が許可された接続の最大数です。

推奨処置 `show static` 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の最大数を確認してください。この制限数は変更できません。

201003

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

説明 Cisco ASA へのトラフィックに関する接続関連メッセージです。特定の外部アドレスから、特定のスタティックグローバルアドレス経由で、特定のローカルアドレスに宛てられた初期接続の数が、制限数を越えたことを示しています。Cisco ASA への初期接続が制限数に達すると、Cisco ASA はこれらの接続を受け入れようとしませんが、接続にタイムリミットを適用します。これにより、Cisco ASA の稼働率がかなり高い場合でも、一部の接続を確立することができます。*nconns* 変数は受信した初期接続数、*elimit* 変数は `static` コマンドまたは `nat` コマンドで指定されている初期接続の制限数を示します。

推奨処置 このメッセージは、メッセージ 201002 よりも重大な過負荷を示しています。SYN 攻撃を受けた場合、または正常なトラフィック量がきわめて増加した場合に、過負荷が発生します。`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の最大数を確認してください。

201004

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

説明 接続関連メッセージです。特定のグローバルアドレスへのUDP接続の数が最大数を越えたときに表示されます。*udp conn limit* 変数は、スタティックまたは変換で許可されるUDP接続の最大数です。

推奨処置 `show static` 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の最大数を確認してください。この最大数は変更できません。

201005

エラーメッセージ %FWSM-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構造を割り当てられません
でした。

推奨処置 メモリ使用量を減らすか、メモリを増設してください。

201006

エラーメッセージ %FWSM-3-201006: RCMD backconnection failed for IP_address/port

説明 接続関連メッセージです。メモリ不足のため、Cisco ASA が rsh コマンドの着信標準出力
用の接続を事前に割り当てられないときに表示されます。

推奨処置 rsh クライアントのバージョンを確認してください。Cisco ASA がサポートするのは、
Berkeley rsh だけです。また、メモリ使用量を減らすか、メモリを増設してください。

201008

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

説明 TCP システム ログメッセージをイネーブルにしている syslog& サーバに到達できない場
合、または Cisco ASA Syslog サーバ (PFSS) を使用している Windows NT システムのディスク
が満杯の場合に、このメッセージが表示されます。

推奨処置 TCP システム ログメッセージをディセーブルにしてください。PFSS を使用してい
る場合は、PFSS が存在する Windows NT システムのスペースを解放してください。また、Syslog
サーバがアップしていて、Cisco ASA のコンソールからホストに ping を実行できることを確認
してください。そのあと、TCP システム ログメッセージを再開してトラフィックを流します。

201009

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

説明 接続関連メッセージです。特定のスタティック アドレスへの接続が最大数を越えたとき
に表示されます。number 変数は、IP_address 変数で表されるホストに許可される接続の最大数で
す。

推奨処置 特定のアドレスへの接続に関して設定されている制限をチェックするには、show
static コマンドおよび show nat コマンドを使用します。この制限数は変更できます。

201010

エラー メッセージ %FWSM-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 `set connection embryonic-conn-max` MPC コマンドでトラフィック クラスに対して設定されている、初期接続の制限数を超えたために、TCP 接続の確立に失敗しました。

- *econns* 設定されているトラフィック クラスに対応する初期接続の現在の数
- *limit* このトラフィック クラスに設定されている初期接続の制限数
- *dir*
input: 接続を開始する最初のパケットは、インターフェイス *interface_name* の入力パケットです。
output: 接続を開始する最初のパケットは、インターフェイス *interface_name* の出力パケットです。
- *source_address/source_port* 接続を開始するパケットの送信元 IP アドレスおよび送信元ポート
- *dest_address/dest_port* 接続を開始するパケットの宛先 IP アドレスおよび宛先ポート
- *interface_name* ポリシー制限が実施されるインターフェイスの名前

推奨処置 対処は不要です。

202001

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

説明 接続関連メッセージです。Cisco ASA に使用可能なアドレス変換スロットが残っていない場合に、このメッセージが表示されます。

推奨処置 グローバル プールのサイズが、内部ネットワークのクライアント数に適しているか確認してください。PAT アドレスが必要になることもあります。または、変換および接続のタイムアウト インターバルを短縮してください。メモリ不足が原因でこのエラーメッセージが表示される場合もあります。メモリ使用量を減らすか、可能であればメモリを増設してください。

202005

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

説明 接続関連メッセージです。接続オブジェクト (xlate) が不正なリストに含まれているときに表示されます。

推奨処置 TAC に連絡してください。

202011

エラー メッセージ %FWSM-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 `set connection conn-max MPC` コマンドでトラフィック クラスに対して設定されている接続の制限数を超過したため、TCP または UDP 接続の作成が失敗したときに、このメッセージが表示されます。

- *econns* 設定されているトラフィック クラスに対応する初期接続の現在の数
- *limit* このトラフィック クラスに設定されている初期接続の制限数
- *dir*
 - input 接続を開始する最初のパケットは、インターフェイス *interface_name* の入力パケットです。
 - output 接続を開始する最初のパケットは、インターフェイス *interface_name* の出力パケットです。
- *source_address/source_port* 接続を開始するパケットの送信元 IP アドレスおよび送信元ポート
- *dest_address/dest_port* 接続を開始するパケットの宛先 IP アドレスおよび宛先ポート
- *interface_name* ポリシー制限が実施されるインターフェイスの名前

推奨処置 対処は不要です。

208005

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

説明 フラッシュメモリのコンフィギュレーションを消去しようとしたときに、Cisco ASA がゼロ以外の値 (内部エラー) を受信しました。このメッセージには、発生元のサブルーチンのファイル名と行番号が表示されます。

推奨処置 パフォーマンス上の理由から、エンドホストが IP フラグメントを挿入しないように設定する必要があります。この設定変更は、おそらく NFS に起因するものです。読み取りおよび書き込みのサイズを、NFS のインターフェイス Maximum Transmission Unit (MTU; 最大伝送ユニット) に合わせて設定してください。

209003

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

説明 再構築を待機中の IP フラグメント数が多すぎます。デフォルトでは、フラグメントの最大数は 200 です (最大数を上げる方法については、『Cisco Security Appliance Command Reference』の `fragment size` コマンドを参照してください)。Cisco ASA では、同時に再構築できる IP フラグメント数が制限されています。ネットワークに異常が発生した場合に、Cisco ASA のメモリ不足を回避するためです。通常、フラグメント化されるトラフィックは、トラフィック総数のうち、わずかな割合でなければなりません。例外は、フラグメント化されるトラフィックの割合が高い、UDP 接続で NFS を使用しているネットワーク環境です。このタイプのトラフィックを Cisco ASA 経由で転送する場合には、TCP 接続の NFS に変更することを検討してください。フラグメント化を防止する方法については、『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 このメッセージが頻発する場合には、DoS 攻撃が進行中であ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連絡してください。

209004

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

説明 IP フラグメントの構造が不正です。再構築された IP パケットの合計サイズが、上限の 65535 バイトを超えています。

推奨処置 侵入イベントが進行中である可能性があります。このメッセージが頻発する場合には、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連絡してください。

209005

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

説明 24 を超えるフラグメントに分割されている IP パケットを Cisco ASA が拒否しています。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中である可能性があります。このメッセージが頻発する場合には、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連絡してください。
fragment chain xxx interface_name コマンドを使用すると、パケット単位のフラグメント数を変更できます。

210001

エラー メッセージ %FWSM-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 を通過するトラフィックが減少しても、このエラーが頻発する場合には、Cisco TAC に連絡してください。

210002

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

説明 ステートフル フェールオーバーで、スタンバイ Cisco ASA にステートフル情報を送信するためのメモリ ブロックを割り当てられなかったことを示しています。

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、正常に送信できるかどうかを確認してください。また、**show block** コマンドを使用して、現在のメモリ ブロックを確認してください。いずれかのメモリ ブロック内で現在の使用可能メモリが 0 の場合には、Cisco ASA ソフトウェアを再起動し、メモリ ブロックの損失を回復してください。

210003

エラー メッセージ %FWSM-3-210003: Unknown LU Object *number*

説明 ステートフル フェールオーバーで、サポートされていない論理アップデート オブジェクトを受信したため、処理できませんでした。原因としては、メモリの損傷、LAN 伝送、またはその他のイベントが考えられます。

推奨処置 このエラーが稀にしか発生しない場合、処置は不要です。このエラーが頻発する場合は、ステートフル フェールオーバー リンクの LAN 接続を確認してください。フェールオーバー リンクの LAN 接続の障害がエラーの原因でなかった場合は、外部ユーザが保護されたネットワークの脆弱化を試みていないかどうかを確認してください。誤って設定されているクライアントがないかどうかを確認してください。

210005

エラー メッセージ %FWSM-3-210005: LU allocate connection failed

説明 ステートフル フェールオーバーで、スタンバイ装置に新しい接続を割り当てることができません。Cisco ASA 上で使用可能な RAM (ランダム アクセス メモリ) が不足しているか、RAM の空き容量がなく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使用可能なメモリを調べ、Cisco ASA にシステムの空きメモリがあるかどうかを確認してください。使用可能なメモリがない場合には、Cisco ASA のメモリを増設してください。

210006

エラー メッセージ %FWSM-3-210006: LU look NAT for *IP_address* failed

説明 ステートフル フェールオーバーで、スタンバイ装置上の IP アドレスに対応する NAT グループを検索できませんでした。アクティブおよびスタンバイの Cisco ASA 装置が同期化されていない可能性があります。

推奨処置 アクティブ装置上で `write standby` コマンドを使用し、スタンバイ装置とシステムメモリを同期化してください。

210007

エラー メッセージ %FWSM-3-210007: LU allocate xlate failed

説明 ステートフル フェールオーバーで、変換 (xlate) スロット レコードの割り当てに失敗しました。

推奨処置 `show memory` コマンドを使用して使用可能なメモリを調べ、Cisco ASA にシステムの空きメモリがあるかどうかを確認してください。使用可能なメモリがない場合は、メモリを増設してください。

210008

エラー メッセージ %FWSM-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用の変換スロット (xlate) レコードが見つからないため、接続情報を処理できません。

推奨処置 アクティブ装置上で **write standby** コマンドを入力し、アクティブ装置とスタンバイ装置のシステム メモリを同期化してください。

210010

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

説明 ステートフル フェールオーバーで、UDP 接続用の新しいレコードを割り当てられませんでした。

推奨処置 **show memory** コマンドを使用して使用可能なメモリを調べ、Cisco ASA にシステムの空きメモリがあるかどうかを確認してください。使用可能なメモリがない場合は、メモリを増設してください。

210020

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

説明 ステートフル フェールオーバーで、使用中の特定の PAT アドレスを割り当てられませんでした。

推奨処置 アクティブ装置上で **write standby** コマンドを入力し、アクティブ装置とスタンバイ装置のシステム メモリを同期化してください。

210021

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

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

推奨処置 アクティブ装置上で **write standby** コマンドを入力し、アクティブ装置とスタンバイ装置のシステム メモリを同期化してください。

210022

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

説明 ステートフル フェールオーバーでは、スタンバイ装置に送信する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、最新の更新レコードの順序と異なる場合、抜けている番号の情報が失われたとみなされ、このエラー メッセージが表示されます。

推奨処置 LAN の割り込みが発生していなければ、両方の Cisco ASA 装置の使用可能なメモリを調べ、ステートフル情報を処理できる十分なメモリがあるかどうかを確認してください。show failover コマンドを使用して、ステートフル情報の更新状況をモニタしてください。

211001

エラー メッセージ %FWSM-3-211001: Memory allocation Error

説明 RAM の割り当てに失敗しました。

推奨処置 このメッセージが定期的に発生する場合は、無視してかまいません。頻繁に繰り返される場合には、TAC に連絡してください。

211003

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

説明 *number* で示される秒数にわたり、CPU 使用率が 100% を超えると、このメッセージが表示されます。

推奨処置 このメッセージが定期的に発生する場合は、無視してかまいません。頻繁に繰り返される場合には、TAC に連絡してください。

212001

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

説明 SNMP メッセージです。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 に宛てられた SNMP 要求を、Cisco ASA 上で受信できないことを示しています。これは、任意のインターフェイスから Cisco ASA を通過する SNMP トラフィックには影響しません。

エラー コード -1 は、Cisco ASA がこのインターフェイスで SNMP 転送を開けなかったことを表します。これは、SNMP がクエリを受け付けるポートを、すでに他の機能に使用されているポートに変更しようとした場合に発生することがあります。この場合、SNMP が使用するポートは、着信 SNMP クエリに関するデフォルトのポート (UDP/161) にリセットされます。

エラー コード -2 は、Cisco ASA がこのインターフェイスで SNMP 転送をバインドできなかったことを表します。

推奨処置 トラフィックが減少して Cisco ASA が一部のリソースを取り戻したとき、そのインターフェイスに関して snmp-server host コマンドを再入力してください。

212002

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

説明 SNMP メッセージです。このインターフェイス上にある SNMP 管理ステーションに対して Cisco ASA が Cisco ASA から SNMP トラップを送信できないことを示しています。これは、任意のインターフェイスから Cisco ASA を通過する SNMP トラフィックには影響しません。

エラー コード -1 は、Cisco ASA がこのインターフェイスで SNMP トラップ転送を開けなかったことを示します。

エラー コード -2 は、Cisco ASA がこのインターフェイスで SNMP トラップ転送をバインドできなかったことを示します。

推奨処置 トラフィックが減少して Cisco ASA が一部のリソースを取り戻したとき、そのインターフェイスに関して `snmp-server host` コマンドを再入力してください。

212003

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

説明 SNMP メッセージです。特定のインターフェイス上の Cisco ASA への SNMP 要求の受信時に、内部エラーが発生したときに表示されます。

推奨処置 対処は不要です。Cisco ASA の SNMP エージェントは、次の SNMP 要求を待機します。

212004

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

説明 SNMP メッセージです。Cisco ASA から特定インターフェイス上の特定のホストへの SNMP 応答の送信時に、内部エラーが発生したときに表示されます。

推奨処置 対処は不要です。

212005

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

説明 SNMP メッセージです。Cisco ASA に宛てられた着信 SNMP 要求の長さが、内部処理中に要求を保存する内部データバッファのサイズ (512 バイト) を超えたことを示しています。Cisco ASA はこの要求を処理できません。この状況は、任意のインターフェイスから Cisco ASA を通過する SNMP トラフィックには影響しません。

推奨処置 SNMP 管理ステーションが短い要求を送信するように設定してください。たとえば、1つの要求で複数の MIB 変数のクエリを送信するのではなく、1つの要求に1つの MIB 変数のクエリだけを送信するようにします。SNMP マネージャ ソフトウェアの設定変更が必要になることがあります。

212006

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

説明 SNMP メッセージです。デバイスが自身に対する SNMP 要求を、次の理由で処理できなかったときに表示されます。

- snmp-server がディセーブルであるため
- SNMPv3 をサポートしていないため

推奨処置 snmp-server enable コマンドを発行し、SNMP デーモンが動作しているかどうかを確認してください。デバイスが処理するのは、SNMPv1 パケットおよび v2c パケットだけです。

214001

エラーメッセージ %FWSM-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 の管理ポートに宛てられた暗号化データ パケットの長さが、特定の上限値を超えています。悪意のある行為の可能性があります。Cisco ASA はこの管理接続をただちに終了します。

推奨処置 管理接続が Cisco Secure Policy Manager によって開始されたものであるかどうかを確認してください。

215001

エラーメッセージ %FWSM-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 TAC に連絡してください。

217001

エラーメッセージ %FWSM-2-217001: No memory for *string* in *string*

説明 メモリ不足のため動作が失敗しました。

推奨処置 十分なメモリがある場合は、このエラー メッセージをコピーし、コンフィギュレーションおよびエラーに先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

メッセージ 302003 ~ 326028

ここでは、メッセージ 302003 ~ 326028 を示します。

302003

エラー メッセージ %FWSM-6-302003: Built H245 connection for foreign_address
outside_address/outside_port local_address inside_address/inside_port

説明 接続関連メッセージです。outside_address から inside_address に H.245 接続が開始されたときに、このメッセージが表示されます。このメッセージが発生するのは、Cisco ASA が Intel Internet Phone の使用を検出した場合だけです。外部ポート (outside_port) が表示されるのは、Cisco ASA の外部からの接続の場合だけです。ローカルポート値 (inside_port) が表示されるのは、内部インターフェイス上で開始された接続の場合だけです。

推奨処置 対処は不要です。

302004

エラー メッセージ %FWSM-6-302004: Pre-allocate H323 UDP backconnection for
foreign_address outside_address/outside_port to local_address inside_address/inside_port

説明 接続関連メッセージです。ローカルアドレス (inside_address) から外部アドレス (outside_address) に H.323 UDP バック接続があらかじめ割り当てられたときに、このメッセージが表示されます。このメッセージが発生するのは、Cisco ASA が Intel Internet Phone の使用を検出した場合だけです。外部ポート (outside_port) が表示されるのは、Cisco ASA の外部からの接続の場合だけです。ローカルポート値 (inside_port) が表示されるのは、内部インターフェイス上で開始された接続の場合だけです。

推奨処置 対処は不要です。

302009

エラー メッセージ %FWSM-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 接続関連メッセージです。TCP 接続がフェールオーバー後に再確立されたときに、このメッセージが表示されます。もう一方の Cisco ASA に、同期パケットが送信されます。outside_address IP アドレスは、外部ホストです。global_address IP アドレスは、低いセキュリティレベルのインターフェイスのグローバルアドレスです。inside_address IP アドレスは、高いセキュリティレベルのインターフェイス上の Cisco ASA の「向こう側」にあるローカル IP アドレスです。

推奨処置 対処は不要です。

302010

エラーメッセージ %FWSM-6-302010: *connections in use, connections most used*

説明 接続関連メッセージです。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* は接続数です。

推奨処置 対処は不要です。

302012

エラーメッセージ %FWSM-6-302012: Pre-allocate H225 Call Signalling Connection for faddr *IP_address/port* to laddr *IP_address*

説明 H.225 セカンダリ チャネルがあらかじめ割り当てられています。

推奨処置 対処は不要です。

302013

エラーメッセージ %FWSM-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つのホスト間に TCP 接続スロットが作成されました。

- *connection_id* は、Unique Identifier (UID; 固有識別情報) です。
- *interface*、*real-address*、*real-port* は、実ソケットを表します。
- *mapped-address*、*mapped-port* は、マッピングされたソケットを表します。
- *user* は、ユーザの AAA 名です。

inbound が表示される場合、最初の制御接続は外部から開始されています。たとえば、FTP では、最初の制御チャネルが *inbound* であれば、データ転送チャネルはすべて *inbound* です。*outbound* が表示される場合、最初の制御接続は内部から開始されています。

推奨処置 対処は不要です。

302014

エラーメッセージ %FWSM-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 接続スロットが削除されました。次に、このメッセージの値を示します。

- *connection id* は、UID です。
- *interface*、*real-address*、*real-port* は、実ソケットを表します。
- *duration* は、接続の持続時間です。
- *bytes bytes* は、その接続で転送されたデータ量です。

- *user* は、ユーザの AAA 名です。

reason 変数は、接続を終了させた動作を表します。*reason* 変数は、表 2-2 に示されている TCP 終了理由のいずれかに設定されます。

表 2-2 TCP 終了の理由

理由	説明
Conn-timeout	接続がアイドル状態のまま設定されたアイドル タイムアウトが経過し、接続が終了
Deny Terminate	アプリケーションの検証によってフローが終了
FIN Timeout	最後の ACK を 10 分間にわたって待機後、またはハーフ クローズ タイムアウト後に強制終了
Flow closed by inspection	検査機能によってフローが終了
Flow terminated by IPS	IPS によってフローが終了
Flow reset by IPS	IPS によってフローがリセット
Invalid SYN	SYN パケットが無効
Idle Timeout	アイドル時間がタイムアウト値を超過したため接続がタイムアウト
IPS fail-close	IPS カードがダウンしたためフローが終了
SYN Control	不正な側からのバック チャネルの開始
SYN Timeout	1 往復半ハンドシェイクの完了を 2 分待機したあと、強制的に終了
TCP bad retransmission	TCP 再送信が不良のため接続が終了
TCP FINs	通常のクローズ ダウン シーケンス
TCP Invalid SYN	TCP SYN パケットが無効
TCP Reset-I	内部からのリセット
TCP Reset-O	外部からのリセット
TCP segment partial overlap	部分的に重複するセグメントを検出
TCP unexpected window size variation	TCP ウィンドウ サイズの変化により接続が終了
Tunnel has been torn down	トンネルがダウンしたためフローが終了
Unauth Deny	URL フィルタによる拒否
Unknown	catch-all エラー
Xlate Clear	コマンドラインの削除

推奨処置 対処は不要です。

302015

エラー メッセージ %FWSM-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。次に、このメッセージの値を示します。

- *connection number* UID
- *interface*、*real_address*、*real_port* 実ソケット

- *mapped_address* および *mapped_port* マッピングされたソケット
- *user* ユーザの AAA 名

inbound が指定されている場合、最初の制御接続は外部から開始されています。たとえば、UDP では、最初の制御チャンネルが *inbound* であれば、データ転送チャンネルはすべて *inbound* です。*outbound* が表示される場合、最初の制御接続は内部から開始されています。

推奨処置 対処は不要です。

302016

エラー メッセージ %FWSM-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。次に、このメッセージの値を示します。

- *connection number* は、UID です。
- *interface*、*real_address*、*real_port* は、実ソケットです。
- *time* は、接続の持続時間です。
- *bytes* は、その接続で転送されたデータ量です。
- *connection id* は、UID です。
- *interface*、*real-address*、*real-port* は、実ソケットです。
- *duration* は、接続の持続時間です。
- *bytes* は、その接続で転送されたデータ量です。
- *user* は、ユーザの AAA 名です。

推奨処置 対処は不要です。

302017

エラー メッセージ %FWSM-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、UID です。*interface*、*real_address*、*real_cid* は、2つのシンプレックス PPTP GRE ストリームのいずれかを表します。カッコで囲まれた *translated_address*、*translated_cid* は、NAT で変換後の値です。

If *inbound* が表示される場合、この接続は着信にしか使用できません。*outbound* が表示される場合、この接続は発信にしか使用できません。次に、このメッセージの値を示します。

- *id* 接続を表す固有の番号
- *inbound* 制御接続は着信 PPTP GRE フロー用
- *outbound* 制御接続は発信 PPTP GRE フロー用
- *interface_name* インターフェイス名
- *real_address* 実ホストの IP アドレス
- *real_cid* 接続の変換前のコール ID

- *translated_address* 変換後の IP アドレス
- *translated_cid* 変換後のコール
- *user* AAA 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 %FWSM-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* は、実ソケットを表します。*duration* は、接続の持続時間です。次に、このメッセージの値を示します。

- *id* 接続を表す固有の番号
- *interface* インターフェイス名
- *real_address* 実ホストの IP アドレス
- *real_port* 実ホストのポート番号
- *hh:mm:ss* 時分秒フォーマットの時刻
- *bytes* GRE セッションで転送された PPP バイト数
- *reason* 接続が終了した理由
- *user* AAA 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 %FWSM-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特定の ASN ライブラリが初期化に失敗しました。Cisco ASA は、着信する H.323 パケットをデコードまたは検査できません。Cisco ASA は、H.323 パケットを変更なしで通過させます。次に H.323 メッセージが着信すると、Cisco ASA は再びライブラリの初期化を試みます。

推奨処置 特定のライブラリに関してこのメッセージが常に表示される場合は、Cisco TAC に連絡し、すべてのログメッセージ（なるべくタイムスタンプ付きで）を提出してください。

302020

エラーメッセージ %FWSM-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、ICMP セッションが fast-path で確立されました。

推奨処置 対処は不要です。

302021

エラーメッセージ %FWSM-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、ICMP セッションが fast-path で削除されました。

推奨処置 対処は不要です。

302022

エラーメッセージ %FWSM-6-302022: Built IP protocol 103 connection 219025360 for int_112:172.16.2.1 (172.16.2.1) to int_102:172.16.112.2 (172.16.112.2)

説明 2つのホスト間のTCP/UDP以外の接続スロットが作成されました。

推奨処置 対処は不要です。

302023

エラーメッセージ %FWSM-6-302023: Teardown IP protocol 103 connection 219025359 for int_102:172.16.2.1 to int_112:172.16.112.2 duration 0:00:35 bytes 74

説明 2つのホスト間のTCP/UDP以外の接続スロットが削除されました。

推奨処置 対処は不要です。

302302

エラーメッセージ %FWSM-3-302302: ACL = deny; no sa created

説明 IPSec プロキシが一致しません。ネゴシエートしたSAのプロキシホストが、access-list コマンドの deny ポリシーの対象です。

推奨処置 コンフィギュレーションの access-list コマンド ステートメントを確認してください。ピアの管理者に連絡してください。

303002

エラーメッセージ %FWSM-6-303002: source_address {Stored|Retrieved} dest_address: mapped_address

説明 FTP/URL メッセージです。特定のホストが、特定のFTPサイトからデータの保存または検索を試みたときに表示されます。

推奨処置 対処は不要です。

303003

エラー メッセージ %FWSM-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 FTP トラフィックに対してストリクトインスペクションを使用するときに、このメッセージが表示されます。ftp-map コマンドによるストリクト FTP インスペクション ポリシーによって FTP 要求コマンドが拒否された場合に表示されます。

推奨処置 対処は不要です。

303004

エラー メッセージ %FWSM-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 FTP トラフィックに対してストリクト FTP インスペクションを使用するときに、このメッセージが表示されます。FTP 要求メッセージに、デバイスが認識できないコマンドが含まれている場合に表示されます。

推奨処置 対処は不要です。

304001

エラー メッセージ %FWSM-5-304001: user *source_address* Accessed {JAVA URL|URL} *dest_address: url*.

説明 FTP/URL メッセージです。特定のホストが特定の URL にアクセスを試みたときに表示されます。

推奨処置 対処は不要です。

304002

エラー メッセージ %FWSM-5-304002: Access denied URL *chars* SRC *IP_address* DEST *IP_address: chars*

説明 FTP/URL メッセージです。送信元アドレスから特定の URL または FTP サイトへのアクセスが拒否されたときに表示されます。

推奨処置 対処は不要です。

304003

エラー メッセージ %FWSM-3-304003: URL Server *IP_address* timed out URL *url*

説明 URL サーバがタイムアウトしました。

推奨処置 対処は不要です。

304004

エラー メッセージ %FWSM-6-304004: URL Server *IP_address* request failed URL *url*

説明 FTP/URL メッセージです。Websense サーバ要求が失敗したときに表示されます。

推奨処置 対処は不要です。

304005

エラー メッセージ %FWSM-7-304005: URL Server *IP_address* request pending URL *url*

説明 FTP/URL メッセージです。Websense サーバ要求が待機中であるときに表示されます。

推奨処置 対処は不要です。

304006

エラー メッセージ %FWSM-3-304006: URL Server *IP_address* not responding

説明 FTP/URL メッセージです。Websense サーバにアクセスできません。これが唯一のサーバである場合、Cisco ASA は同じサーバへのアクセスを試みようとしています。複数のサーバがある場合、別のサーバにアクセスをしようとしています。

推奨処置 対処は不要です。

304007

エラー メッセージ %FWSM-2-304007: URL Server *IP_address* not responding, ENTERING ALLOW mode.

説明 FTP/URL メッセージです。filter コマンドの allow オプションを使用したとき、Websense サーバから応答がないときに表示されます。Cisco ASA は、サーバから応答があるまで、すべての Web 要求をフィルタリングせずに続行させます。

推奨処置 対処は不要です。

304008

エラー メッセージ %FWSM-2-304008: LEAVING ALLOW mode, URL Server is up.

説明 FTP/URL メッセージです。filter コマンドの allow オプションを使用したとき、Cisco ASA が、それまで応答のなかった Websense サーバから応答メッセージを受信したときに表示されます。この応答メッセージを受信すると、Cisco ASA は許可モードを終了し、URL フィルタリング機能を再びイネーブルにします。

推奨処置 対処は不要です。

304009

エラー メッセージ %FWSM-7-304009: Ran out of buffer blocks specified by url-block command

説明 URL 待機バッファ ブロックのスペースが不足しています。

推奨処置 `url-block block block_size` コマンドを使用して、バッファ ブロック サイズを変更してください。

305005

エラー メッセージ %FWSM-3-305005: No translation group found for protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port

説明 パケットが発信 `nat` コマンドのルールと一致しません。

推奨処置 このメッセージはコンフィギュレーション エラーを示しています。送信元ホストにダイナミック NAT を使用する場合は、`nat` コマンドが送信元 IP アドレスと一致しているかどうかを確認してください。送信元ホストにスタティック NAT を使用する場合は、`static` コマンドのローカル IP アドレスが一致しているかどうかを確認してください。送信元ホストに NAT を使用しない場合は、NAT 0 ACL にバインドされた ACL (アクセス制御リスト) を確認してください。

305006

エラー メッセージ %FWSM-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、Cisco ASA にネットワーク アドレスまたはブロードキャスト アドレス宛ての packets を許可しないように要求した注意事項 CSCdr0063 への対策として表示されます。Cisco ASA は、`static` コマンド ステートメントで明示的に指定されたアドレスに対して、このチェックを行います。この変更があると、着信トラフィックについて、Cisco ASA は宛先 IP アドレスがネットワーク アドレスまたはブロードキャスト アドレスの場合、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 を適用するわけではなく、PAT ICMP エコーおよびエコー / 応答パケット (タイプ 8 および 0) のみ適用します。具体的にいうと、ICMP エコーまたはエコー / 応答パケットだけが PAT `xlate` を作成します。したがって、その他の ICMP メッセージ タイプが廃棄されると、システム ログ メッセージ 305006 が (Cisco ASA 上で) 生成されます。

Cisco ASA は、`static` コマンド ステートメントに設定されたグローバル IP およびマスクを使用して、標準 IP アドレスとネットワーク 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 は着信パケットについて、ネットワーク IP アドレスまたはブロードキャスト IP アドレス用の変換 (`xlate`) 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 がネットワーク アドレスとして、10.2.2.255 がブロードキャスト 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 宛の着信パケットを拒否し、このシステム ログ メッセージを生成します。

疑わしい IP がホスト IP である場合、サブネットの `static` の前に、ホスト マスクを指定した `static` コマンドを個別に設定します (`static` コマンド ステートメントに関する最初の一致のルール)。次の `static` コマンドを使用すると、Cisco ASA は 10.2.2.128 に対しホスト アドレスとして応答します。

```
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
```

疑わしい IP アドレスを持つ内部ホストから開始されたトラフィックによって、変換が作成される場合があります。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、サブネットの `static` 設定が重複したホスト IP アドレスとみなすので、ネットワーク アドレス変換は、両方の `static` コマンドで同じでなければなりません。

推奨処置 対処は不要です。

305007

エラー メッセージ %FWSM-6-305007: addrpool_free(): Orphan IP *IP_address* on interface *interface_number*

説明 Cisco ASA が、どのグローバル プールにも存在しないアドレスの変換を試みました。Cisco ASA はこのアドレスが削除されているものとみなし、要求を廃棄します。

推奨処置 対処は不要です。

305008

エラー メッセージ %FWSM-3-305008: Free unallocated global IP address.

説明 Cisco ASA カーネルが、未割り当てのグローバル IP アドレスを解放してアドレス プールに返そうとするという、矛盾した状態が発生したことを検知しました。Cisco ASA のステートフル フェールオーバーのセットアップ中に、アクティブ装置とスタンバイ装置間で一部の内部ステートが瞬間的に同期外れになった場合、この状態が発生することがあります。重大な状態ではないので、同期は自動的に回復します。

推奨処置 このメッセージが継続的に表示される場合は、TAC に報告してください。

305009

エラー メッセージ %FWSM-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。このスロットは、送信元アドレスをローカル側からグローバル側に変換します。逆方向では、このスロットは宛先アドレスをグローバル側からローカル側に変換します。

推奨処置 対処は不要です。

305010

エラー メッセージ %FWSM-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 対処は不要です。

305011

エラー メッセージ %FWSM-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。このスロットは、送信元ソケットをローカル側からグローバル側に変換します。逆方向では、このスロットは宛先ソケットをグローバル側からローカル側に変換します。

推奨処置 対処は不要です。

305012

エラー メッセージ %FWSM-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 対処は不要です。

308001

エラー メッセージ %FWSM-6-308001: console enable password incorrect for *number* tries (from *IP_address*)

説明 Cisco ASA 管理メッセージです。イネーブル モードを開始するパスワードが、特定の回数だけ誤って入力されたときに表示されます。入力できるのは、3 回までです。

推奨処置 パスワードを確認し、再び接続を試みてください。

308002

エラー メッセージ %FWSM-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 ステートメントで IP アドレスが重複しています。*global_address* はセキュリティ レベルの低いインターフェイス上のグローバル アドレス、*inside_address* はセキュリティ レベルの高いインターフェイス上のローカル 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 ステートメントを表示し、重複するコマンドを修正してください。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、別の **static** コマンドで 10.1.1.5 など、その範囲内のホストを指定したときに発生します。

311001

エラー メッセージ %FWSM-6-311001: LU loading standby start

説明 スタンバイ Cisco ASA が初めてオンラインになったときに、スタンバイ Cisco ASA にステートフル フェールオーバー アップデート情報が送信されました。

推奨処置 対処は不要です。

311002

エラー メッセージ %FWSM-6-311002: LU loading standby end

説明 スタンバイ Cisco ASA へのステートフル フェールオーバー アップデート情報の送信が停止しました。

推奨処置 対処は不要です。

311003

エラー メッセージ %FWSM-6-311003: LU recv thread up

説明 スタンバイ Cisco ASA からのアップデート確認応答を受信しました。

推奨処置 対処は不要です。

311004

エラー メッセージ %FWSM-6-311004: LU xmit thread up

説明 ステートフル フェールオーバー更新がスタンバイ Cisco ASA に送信されたことを示しています。

推奨処置 対処は不要です。

312001

エラー メッセージ %FWSM-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ました。メッセージのバージョン番号がこのインターフェイスの予期した番号と異なり、ルーティングドメイン エントリがゼロ以外です。

推奨処置 これは情報メッセージですが、他の RIP デバイスが Cisco ASA と通信するために正しく設定されていない可能性も示しています。

313001

エラー メッセージ %FWSM-3-313001: Denied ICMP type=*number*, code=*code* from *IP_address* on interface *interface_name*

説明 アクセス リストに **icmp** コマンドを使用したとき、最初に一致したエントリが許可エントリである場合、ICMP パケットは継続的に処理されます。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い場合、Cisco ASA は ICMP パケットを廃棄して、このシステム ログ メッセージを生成します。**icmp** コマンドにより、インターフェイスへの ping がイネーブルまたはディセーブルになります。ping がディセーブルの場合、ネットワーク上で Cisco ASA を検知できません。この機能は、Configurable Proxy Pinging と呼ばれます。

推奨処置 ピア デバイスの管理者に連絡してください。

313003

エラー メッセージ %FWSM-4-313003: Invalid destination for ICMP error

説明 ICMP エラー メッセージの宛先が、その ICMP エラー メッセージの原因となった IP パケットの送信元と異なっています。

推奨処置 このメッセージが頻発する場合は、アクティブ なネットワーク プローブ、ICMP エラー メッセージを隠密的なチャネルとして使用する試み、または IP ホストの誤動作の可能性が 있습니다。ICMP エラー メッセージが発生したホストの管理者に連絡してください。

313004

エラー メッセージ %FWSM-4-313004: Denied ICMP type=*icmp_type*, from *source_address* on interface *interface_name* to *dest_address*: no matching session

説明 ステートフル ICMP 機能によって追加されたセキュリティ チェックの結果、ICMP パケットが Cisco ASA によってドロップされました。通常、これに該当するのは、Cisco ASA を通過した有効なエコー要求が存在しない ICMP エコー 応答や、Cisco ASA 上で確立された TCP、UDP、または ICMP セッションに関係しない ICMP エラー メッセージです。

推奨処置 対処は不要です。

314001

エラー メッセージ %FWSM-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、指定の IP アドレスおよびポートに対して RTSP 接続を開始しました。

推奨処置 対処は不要です。

315004

エラーメッセージ %FWSM-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 の RSA ホストキーを見つられませんでした。Cisco ASA のホストキーが生成されていないか、または Cisco ASA のライセンスで DES または 3DES が許可されていないため、ホストキーが存在し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、Cisco ASA の RSA ホストキーが存在するかどうかを確認してください。存在しない場合には、`show version` コマンドを入力して、Cisco ASA のライセンスで DES または 3DES が許可されているかどうかを確認してください。

315011

エラーメッセージ %FWSM-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 セッションの完了後に表示されます。ユーザが `quit` または `exit` を入力した場合は、`terminated normally` (正常終了) のメッセージが表示されます。ほかの理由でセッションが切断された場合には、その理由が表示されます。表 2-3 に、考えられるセッションの切断理由を示します。

表 2-3 SSH の切断理由

テキスト ストリング	説明	処置
Bad checkbytes	SSH キー交換時にチェックバイトで不一致が検出されました。	SSH セッションを再起動してください。
CRC check failed	特定の packets に関して計算された CRC 値が、packet に組み込まれている CRC 値と一致しません。この packet は不正です。	対処は不要です。このメッセージが続く場合は、TAC に連絡してください。
Decryption failure	SSH キー交換時に SSH セッションキーの復号化が失敗しました。	RSA ホストキーを確認し、再試行してください。
Format error	SSH バージョン交換時に非プロトコルバージョンメッセージを受信しました。	SSH クライアントを調べ、サポートされているバージョンかどうかを確認してください。
Internal error	Cisco ASA 上の SSH の内部エラー、または RSA キーが Cisco ASA に入力されていないか検索できないことを示しています。	Cisco ASA コンソールから <code>show ca mypubkey rsa</code> コマンドを入力し、RSA ホストキーが存在するかどうかを確認してください。存在しない場合、 <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を確認してください。RSA ホストキーが存在している場合は、SSH セッションを再起動してください。

表 2-3 SSH の切断理由 (続き)

テキスト ストリング	説明	処置
Invalid cipher type	SSH クライアントがサポート対象外のサイファを要求しました。	<code>show version</code> コマンドを使用して、ライセンスでサポートされている機能を確認し、サポート対象のサイファを使用するように SSH クライアントを再設定してください。
Invalid message length	Cisco ASA に着信した 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 4096 バイト未満です。データが壊れている可能性があります。	対処は不要です。
Invalid message type	Cisco ASA が非 SSH メッセージを受信したか、サポート対象外または不要な 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を確認してください。クライアントが SSHv1 をサポートしており、このメッセージが続く場合には、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キャプチャします。TAC に連絡してください。
Out of memory	一般にトラフィック量が多く Cisco ASA の稼働率が高いために、Cisco ASA が SSH サーバ用のメモリを割り当てられないことを示しています。	SSH セッションをあとで再起動してください。
Rejected by server	ユーザ認証に失敗しました。	ユーザ名とパスワードを確認するようにユーザに通知してください。
Reset by client	SSH クライアントが Cisco ASA に <code>SSH_MSG_DISCONNECT</code> メッセージを送信しました。	対処は不要です。
status code:hex (hex)	ユーザが SSH コンソールで <code>quit</code> または <code>exit</code> を入力する代わりに、Windows 上で SSH クライアント ウィンドウを閉じました。	対処は不要です。クライアントを整然とした方法で終了するようにユーザに指示してください。
Terminated by operator	Cisco ASA のコンソールで <code>ssh disconnect</code> コマンドを入力することにより、SSH セッションを終了しました。	対処は不要です。
Time-out activated	<code>ssh timeout</code> コマンドで指定された時間が経過し、SSH セッションがタイムアウトしました。	SSH 接続を再起動してください。必要な場合、 <code>ssh timeout</code> コマンドを使用して、デフォルト値である 5 分を最大 60 分まで延長できます。

推奨処置 対処は不要です。

316001

エラー メッセージ %FWSM-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 ピアの制限数以上の VPN トンネル (ISAKMP/IPSec) の確立が同時に試みられた場合、余剰のトンネルが打ち切られます。

推奨処置 対処は不要です。

317001

エラー メッセージ %FWSM-3-317001: No memory available for limit_slow

説明 メモリ不足のため、要求された処理に失敗しました。

推奨処置 ほかのシステム動作を減らして、メモリを解放してください。必要に応じて、メモリ構成をアップグレードしてください。

317002

エラー メッセージ %FWSM-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 TAC に連絡して指示を受け、問題の原因を調べてください。

317003

エラー メッセージ %FWSM-3-317003: IP routing table creation failure - *reason*

説明 内部ソフトウェア エラーにより、新しい IP ルーティング テーブルを作成できませんでした。

推奨処置 表示されたメッセージを正確にコピーし、TAC に報告してください。

317004

エラー メッセージ %FWSM-3-317004: IP routing table limit warning

説明 指定の IP ルーティング テーブルのルート数が、設定されている警告制限数に達しました。

推奨処置 テーブル内のルート数を減らすか、制限数を再設定してください。

317005

エラー メッセージ %FWSM-3-317005: IP routing table limit exceeded - *reason*,
IP_address netmask

説明 制限数を越えたルートをテーブルに追加しようとしています。

推奨処置 テーブル内のルート数を減らすか、制限数を再設定してください。

318001

エラー メッセージ %FWSM-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 秒間隔で表示されます。

推奨処置 TAC に連絡して指示を受け、問題の原因を調べてください。

318002

エラー メッセージ %FWSM-3-318002: Flagged as being an ABR without a backbone area

説明 ルータが Area Border Router (ABR; エリア境界ルータ) としてフラグ付けされましたが、ルータにバックボーン エリアが設定されていません。このメッセージは 5 秒間隔で表示されません。

推奨処置 OSPF プロセスを再起動してください。

318003

エラー メッセージ %FWSM-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 秒間隔で表示されます。

推奨処置 対処は不要です。

318004

エラー メッセージ %FWSM-3-318004: area *string* lsid *IP_address* mask *netmask* adv *IP_address*
type number

説明 OSPF の Link State Advertisement (LSA; リンク ステート アドバタイズ) 検索に問題があり、メモリ リークが発生した可能性があります。

推奨処置 TAC に連絡して指示を受け、問題の原因を調べてください。

318005

エラー メッセージ %FWSM-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 のデータベースと IP ルーティング テーブルの間で矛盾が検出されました。

推奨処置 TAC に連絡して指示を受け、問題の原因を調べてください。

318006

エラー メッセージ %FWSM-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 TAC に連絡して指示を受け、問題の原因を調べてください。

318007

エラー メッセージ %FWSM-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 TAC に連絡して指示を受け、問題の原因を調べてください。

318008

エラー メッセージ %FWSM-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され、新しいルータ ID を選択しています。これにより、すべての仮想リンクがダウンします。

推奨処置 新しいルータ ID が反映されるように、すべての仮想リンク ネイバ上で仮想リンク コンフィギュレーションを変更してください。

319001

エラー メッセージ %FWSM-3-319001: Acknowledge for arp update for IP address *dest_address* not received (*number*).

説明 システムの過負荷により、Cisco ASA の ARP プロセスの内部同期が失われました。

推奨処置 すぐに対処する必要はありません。この障害は一時的なものです。システムの平均負荷を調べ、許容量を超えていないかどうかを確認してください。

319002

エラー メッセージ %FWSM-3-319002: Acknowledge for route update for IP address *dest_address* not received (*number*).

説明 システムの過負荷により、Cisco ASA のルーティング モジュールの内部同期が失われました。

推奨処置 すぐに対処する必要はありません。この障害は一時的なものです。システムの平均負荷を調べ、許容量を超えていないかどうかを確認してください。

319003

エラー メッセージ %FWSM-3-319003: Arp update for IP address *address* to NPn failed.

説明 ARP エントリを更新するとき、内部 ARP テーブルを更新するためのメッセージが Network Processor (NP) に送信されます。このとき、FWSM のメモリ利用率が高かったり、内部テーブルが満杯であると、NP へのメッセージが拒否され、このメッセージが生成されることがあります。

推奨処置 ARP テーブルが満杯になっていないかどうかを確認してください。満杯でなければ、FWSM の負荷 (CPU 利用率および 1 秒あたりの接続数) を調べてください。CPU 利用率が高い場合、または 1 秒あたりの接続数が多い場合には、通常の負荷に戻った時点で正常な動作が再開されます。

319004

エラー メッセージ %FWSM-3-319004: Route update for IP address *dest_address* failed (*number*).

説明 システムの過負荷により、FWSM のルーティング モジュールの内部同期が失われました。

推奨処置 すぐに対処する必要はありません。この障害は一時的なものです。システムの平均負荷を調べ、許容量を超えていないかどうかを確認してください。

320001

エラー メッセージ %FWSM-3-320001: The subject name of the peer cert is not allowed for connection

説明 Cisco ASA が簡単な FWSM リモート デバイスまたはサーバである場合、ピアの証明書に、`ca verifycertdn` コマンドと一致しない件名が含まれています。

推奨処置 このメッセージは、デバイスがピアの IP アドレスをスプーフィングし、Cisco ASA からの VPN 接続を代行受信しようとする「Man in the Middle」攻撃を表す場合があります。

321001

エラー メッセージ %FWSM-5-321001: Resource *var1* limit of *var2* reached.

説明 特定のリソースに設定されている使用率またはレート制限に達したことを示しています。

推奨処置 対処は不要です。

321002

エラー メッセージ %FWSM-5-321002: Resource *var1* rate limit of *var2* reached.

説明 特定のリソースに設定されている使用率またはレート制限に達したことを示しています。

推奨処置 対処は不要です。

321003

エラー メッセージ %FWSM-6-321003: Resource *var1* log level of *var2* reached.

説明 特定のリソースに設定されている使用率またはレート ログ レベルに達したことを示しています。

推奨処置 対処は不要です。

321004

エラー メッセージ %FWSM-6-321004: Resource *var1* rate log level of *var2* reached

説明 特定のリソースに設定されている使用率またはレート ログ レベルに達したことを示しています。

推奨処置 対処は不要です。

322001

エラー メッセージ %FWSM-3-322001: Deny MAC address *MAC_address*, possible spoof attempt on interface *interface*

説明 Cisco ASA が指定のインターフェイス上で不正な 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にある別のインターフェイスに静的にバインドされています。原因としては、MAC スプーフィング攻撃またはコンフィギュレーションの誤りの可能性があります。

推奨処置 コンフィギュレーションを確認して適切に対処してください。不正なホストを検出するか、またはコンフィギュレーションを訂正します。

322002

エラー メッセージ %FWSM-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 検査モジュールがイネーブルの場合、パケットでアドバタイズされた新しい ARP エントリが、静的な設定または動的な学習による IP-MAC アドレス バインディングに適合しているかどうかをチェックした上で、Cisco ASA から ARP パケットが転送されます。このチェックに失敗すると、ARP 検査モジュールは ARP パケットをドロップし、このメッセージを生成します。この状況の原因としては、ネットワーク上の 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) の可能性があります。

推奨処置 攻撃が原因である場合は、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である場合は、バインディングを訂正してください。

322003

エラー メッセージ %FWSM-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 検査モジュールがイネーブルの場合、パケットでアドバタイズされた新しい ARP エントリが、静的な設定による IP-MAC アドレス バインディングに適合しているかどうかをチェックした上で、Cisco ASA から ARP パケットが転送されます。このチェックに失敗すると、ARP 検査モジュールは ARP パケットをドロップし、このメッセージを生成します。この状況の原因としては、ネットワーク上の 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) の可能性があります。

推奨処置 攻撃が原因である場合は、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である場合は、バインディングを訂正してください。

322004

エラー メッセージ %FWSM-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 トランスペアレント モードで設定された管理 IP アドレスがないため、Cisco ASA がパケットを廃棄しました。

protocol プロトコルのストリングまたは値
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 デバイスに管理 IP アドレスおよびマスクの値を設定してください。

323004

エラーメッセージ %FWSM-3-323004: Module in slot *slotnum* failed to write software *vnewver* (currently *vver*), *reason*. Hw-module reset is required before further use.

説明 指定のスロット番号のモジュールがソフトウェア バージョンの受け入れに失敗し、UNRESPONSIVE ステートに移行します。ソフトウェアを更新するまで、このモジュールは使用できません。

slotnum モジュールの搭載先スロット番号

newver モジュールに正常に書き込めなかったソフトウェアの新しいバージョン番号 (例: 1.0(1)0)

ver モジュールの現在のソフトウェア バージョン番号 (例: 1.0(1)0)

reason 新しいバージョンがモジュールに書き込めなかった理由。表示される可能性のある *reason* の値は次のとおりです。

- write failure.
- failed to create a thread to write the image.

推奨処置 `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てから、さらにアップグレードを試みてください。モジュールソフトウェアが更新できないと、モジュールは使用できません。モジュールがシャーシに完全に装着されているかどうかを確認してください。モジュールソフトウェアの更新を何回か試みても失敗する場合は、Cisco TAC に連絡してください。

323005

エラーメッセージ %FWSM-3-323005: Module in slot *slotnum* can not be powered on completely

説明 モジュールの電源が完全にオンにならないことを示すメッセージです。この状況が是正されるまで、モジュールは UNRESPONSIVE ステートのままになります。原因としては、モジュールがスロットに完全に装着されていない場合が考えられます。

slotnum モジュールの搭載先スロット番号

推奨処置 モジュールがスロットに完全に装着されているかどうか、モジュールのいずれかのステータス LED が点灯しているかどうかを確認します。モジュールを完全に装着し直したあと、その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、1 分ほどかかる場合があります。モジュールが確かに装着されていて、`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ても、このメッセージが表示される場合には、Cisco TAC に連絡してください。

324000

エラーメッセージ %FWSM-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* 変数で指定されるフィルタリング要件を満たさないため廃棄されました。

推奨処置 対処は不要です。

324001

エラー メッセージ %FWSM-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 パケットの処理中にエラーが発生しました。考えられる理由は次のとおりです。

- 必須の IE が欠落
- 必須の IE が不正
- IE の順序が不正
- 無効なメッセージ フォーマット
- オプションの IE が不正
- 無効な TEID
- 不明の IE
- 長さフィールドが不正
- 不明の GTP メッセージ
- メッセージの長さが不足
- 予期しないメッセージの検出
- ヌルの TID
- サポート対象外のバージョン

推奨処置 このメッセージが定期的に発生する場合は、無視してかまいません。このメッセージが頻発する場合は、エンドポイントが攻撃の一環として不正な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 %FWSM-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 このメッセージの前にメッセージ 321100 (メモリ割り当てエラー) が表示されている場合、このメッセージは、リソース不足のため PDP コンテキストを作成できなかったことを表します。このメッセージの前にメッセージ 321100 が表示されなかった場合、バージョン 0 の場合は、対応する PDP コンテキストが見つからなかったことを表します。バージョン 1 の場合は、このメッセージの前にメッセージ 324001 が表示されている場合、パケット処理エラーが発生し、処理が停止したことを表します。

推奨処置 メモリ割り当てエラーが原因でこのメッセージが頻発する場合は、Cisco TAC に連絡してください。

324003

エラー メッセージ %FWSM-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 受信した応答には、要求キュー内に対応する要求がなかったので、この応答を処理すべきではありません。

推奨処置 このメッセージが定期的に発生する場合は、無視してかまいません。このメッセージが頻発する場合は、エンドポイントが攻撃の一環として不正な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 %FWSM-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 処理中のパケットのバージョンは、現在サポートされているバージョン（0または1）以外です。出力されるバージョン番号が不正で、頻繁に見られる場合には、エンドポイントが攻撃の一環として不正なパケットを送信している可能性があります。

推奨処置 対処は不要です。

324005

エラー メッセージ %FWSM-3-324005: Unable to create tunnel from *source_interface:source_address/source_port* to *dest_interface:dest_address/dest_port*

説明 TPDU に対応するトンネルの作成を試みているときに、エラーが発生しました。

推奨処置 このメッセージが定期的に発生する場合は、無視してかまいません。このエラーが頻発する場合は、必要なデバッグ情報を収集し、Cisco TAC に連絡してください。

324006

エラー メッセージ %FWSM-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、作成できるトンネルの最大数を超過したので、トンネルは作成されません。

推奨処置 トンネルの制限数を上げることを検討するか、またはネットワーク上に攻撃の可能性がないかどうかを確認してください。

324007

エラー メッセージ %FWSM-3-324007: Unable to create GTP connection for response from *source_interface:source_address/0* to *dest_interface:dest_address/dest_port*

説明 TPDU に対応して異なる SGSN または GGSN のトンネルの作成を試みているときに、エラーが発生しました。

推奨処置 デバッグ情報やメッセージを調べて、接続が正常に作成されなかった理由を確認してください。問題をデバッグできない場合には、必要なデバッグ情報を収集して Cisco TAC に連絡してください。

325001

エラー メッセージ %FWSM-3-325001: Router *ipv6_address* on *interface* has conflicting ND (Neighbor Discovery) settings

説明 リンク上の他のルータが、矛盾したパラメータのあるルータ アドバタイズを送信しました。*ipv6_address* は、他のルータの IPv6 アドレスです。*interface* は、他のルータとのリンクのインターフェイス名です。

推奨処置 リンク上のすべての IPv6 ルータが、ルータ アドバタイズで *hop_limit*、*managed_config_flag*、*other_config_flag*、*reachable_time*、および *ns_interval* に同じパラメータを使用しており、なおかつ、いくつかのルータがアドバタイズしている同じプレフィクスについて、優先される有効なライフタイムが同じであるかどうかを確認してください。インターフェイスに関するパラメータを一覧表示するには、`show ipv6 interface` コマンドを入力します。

325002

エラー メッセージ %FWSM-4-325002: Duplicate address *ipv6_address/MAC_address* on *interface*

説明 別のシステムが同じ IPv6 アドレスを使用しています。*ipv6_address* は、もう一方のルータの IPv6 アドレスです。*MAC_address* は、もう一方のシステムの MAC アドレス (既知の場合) であり、不明の場合には [unknown] と表示されます。*interface* は、もう一方のシステム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いずれか一方の IPv6 アドレスを変更してください。

326001

エラー メッセージ %FWSM-3-326001: Unexpected error in the timer library: *error_message*

説明 コンテキストまたは適切なタイプのないマネージド タイマー イベントを受信したか、またはハンドラが存在しません。キューに格納されるイベント数がシステムの制限数を超過し、あとで処理されることになった場合にも、このメッセージが表示されます。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326002

エラー メッセージ %FWSM-3-326002: Error in *error_message* : *error_message*

説明 IGMP プロセスを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の準備として実行されたイベントが、同期外れになってい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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326004

エラー メッセージ %FWSM-3-326004: An internal error occurred while processing a packet queue

説明 IGMP パケット キューがパケットのないシグナルを受信しました。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326005

エラー メッセージ %FWSM-3-326005: Mrib notification failed for (*IP_address*, *IP_address*)

説明 データ駆動イベントをトリガーするパケットを受信し、MRIB に通知する試みが失敗しました。

推奨処置 システムの起動後にこのメッセージが続く場合は、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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326006

エラー メッセージ %FWSM-3-326006: Entry-creation failed for (*IP_address*, *IP_address*)

説明 MFIB が MRIB からエン트리 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。これによってメモリ不足が引き起こされる場合があります。

推奨処置 メモリが十分にある場合には、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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326007

エラー メッセージ %FWSM-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 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。結果的にメモリ不足が発生する場合があります。

推奨処置 メモリが十分にある場合には、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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326008

エラー メッセージ %FWSM-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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326009

エラー メッセージ %FWSM-3-326009: MRIB connection-open failed

説明 MFIB が MRIB への接続を開始できませんでした。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326010

エラー メッセージ %FWSM-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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326011

エラー メッセージ %FWSM-3-326011: MRIB table deletion failed

説明 MFIB が削除されているはずのテーブルを検索できませんでした。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326012

エラー メッセージ %FWSM-3-326012: Initialization of *string* functionality failed

説明 機能が初期化できませんでした。このコンポーネントは、この機能なしで引き続き動作する場合があります。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326013

エラー メッセージ %FWSM-3-326013: Internal error: *string* in *string* line %d (%s)

説明 MRIB で根本的な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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326014

エラー メッセージ %FWSM-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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326015

エラー メッセージ %FWSM-3-326015: Communication error: *error_message* *error_message*

説明 MRIB が不正な形式の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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326016

エラー メッセージ %FWSM-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なしで使用できません。この状況の原因は、番号付きのインターフェイスが見つからないこと、または何らかの内部エラーです。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326017

エラー メッセージ %FWSM-3-326017: Interface Manager error - *string* in *string* : *string*

説明 PIM トンネル インターフェイスの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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326019

エラー メッセージ %FWSM-3-326019: *string* in *string* : *string*

説明 PIM RP トンネル インターフェイスの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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326020

エラー メッセージ %FWSM-3-326020: List error in *string* : *string*

説明 PIM インターフェイス リストの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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326021

エラー メッセージ %FWSM-3-326021: Error in *string* : *string*

説明 PIM トンネル インターフェイスの SRC の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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326022

エラー メッセージ %FWSM-3-326022: Error in *string* : *string*

説明 PIM プロセスを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の準備として実行されたイベントが、同期外れになってい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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326023

エラー メッセージ %FWSM-3-326023: *string* - *IP_address* : *string*

説明 PIM グループ範囲の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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326024

エラー メッセージ %FWSM-3-326024: An internal error occurred while processing a packet queue.

説明 PIM パケット キューがパケットのないシグナルを受信しました。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326025

エラー メッセージ %FWSM-3-326025: *string*

説明 メッセージの送信を試みているときに内部エラーが発生しました。メッセージの受信時にスケジュールされていたイベント (PIM トンネル IDB の削除など) は、実行さ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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326026

エラー メッセージ %FWSM-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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326027

エラー メッセージ %FWSM-3-326027: Corrupted update: *error_message*

説明 MRIB が壊れ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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

326028

エラー メッセージ %FWSM-3-326028: Asynchronous error: *error_message*

説明 MRIB API で処理されない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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

メッセージ 400000 ~ 418001

ここでは、メッセージ 400000 ~ 420003 を示します。

402101

エラーメッセージ %FWSM-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=*dest_address*, prot=*protocol*, spi=*number*

説明 Security Association Database (SADB) に存在しない Security Parameters Index (SPI) を指定する IPSec パケットを受信しました。この状況は、IPSec ピア間の SA エージングにわずかな誤差がある場合、一時的に発生することがあります。また、ローカル SA が消去された場合にも発生します。IPSec ピアから誤ったパケットが送信された可能性もあります。攻撃の可能性もあります。

推奨処置 ローカル SA が消去されたことについて、ピアが認識しないことがあります。ローカル ルータから新しい接続を確立すると、両ピアの接続が正常に再確立する場合があります。この問題が持続する場合には、新しい接続の確立を試みるか、ピアの管理者に連絡してください。

402102

エラーメッセージ %FWSM-4-402102: decapsulate: packet missing {AH|ESP}, destaddr=*dest_address*, actual prot=*protocol*

説明 受信した IPSec パケットに、予期した Authentication Header (AH; 認証ヘッダー) または Encapsulating Security Payload (ESP) ヘッダーがありません。ピアが、ネゴシエートしたセキュリティ ポリシーに一致しないパケットを送信しています。攻撃の可能性もあります。

推奨処置 ピアの管理者に連絡してください。

402103

エラーメッセージ %FWSM-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、ネゴシエートした ID と一致しません。セキュリティ アソシエーションの選択が誤っているので、ピアはこのセキュリティ アソシエーションを通じて別のトラフィックを送信しています。悪意のある行為の可能性もあります。

推奨処置 ピアの管理者に連絡し、ポリシー設定を比較してください。

402106

エラー メッセージ %FWSM-4-402106: Rec'd packet not an IPSEC packet (ip)
dest_address= *dest_address*, src_addr= *source_address*, prot= *protocol*

説明 受信したパケットがクリプトマップ ACL に一致していますが、そのパケットは IPsec でカプセル化されていません。IPsec ピアがカプセル化されていないパケットを送信しています。このエラーは、ピア上のポリシー設定エラーによって発生します。たとえば、Cisco ASA は外部インターフェイス ポート 23 に対しては、暗号化された Telnet トラフィックだけを受け入れます。ポート 23 で外部インターフェイスに IPsec 暗号化なしで Telnet 接続を試みると、このメッセージが表示されます。このエラーは悪意あるイベントを表している場合もあります。ここに記述する状況以外では、このシステム ログ メッセージは生成されません(たとえば、Cisco ASA インターフェイス自身へのトラフィックの場合は、このメッセージは生成されません)。TCP 要求および 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 ピアの管理者に連絡し、ポリシー設定を比較してください。

404101

エラー メッセージ %FWSM-4-404101: ISAKMP: Failed to allocate address for client
from pool *string*

説明 ISAKMP が、`ip local pool` コマンドで指定したプールからの VPN クライアント用の IP アドレスの割り当てに失敗しました。

推奨処置 `ip local pool` コマンドを使用して、プールに IP アドレスを追加してください。

404102

エラー メッセージ %FWSM-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、DoS 攻撃の可能性が
あります。

推奨処置 `show crypto isakmp ca` コマンドを使用して、攻撃の発信元を調べてください。発信元
が判明したら、不当な IP アドレスまたはネットワークからのアクセスを拒否してください。

405001

エラー メッセージ %FWSM-4-405001: Received ARP {request | response} collision
from *IP_address/MAC_address* on interface *interface_name*

説明 Cisco ASA が受信した ARP パケットの MAC アドレスが、ARP キャッシュ エントリと異
なっています。

推奨処置 正当なトラフィックの場合もありますが、ARP ポイズニング攻撃が進行中の可能性
もあります。発信元 MAC アドレスを調べ、パケットの発信元を判別し、それが有効なホストに
属するものであるかどうかを確認してください。

405101

エラー メッセージ %FWSM-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、または使用可能なアドレス変換スロットがないことを示しています。

推奨処置 このメッセージが定期的に発生する場合は、無視してかまいません。頻繁に繰り返される場合は、TAC に連絡してください。グローバル プールのサイズが、内部ネットワークのクライアント数に適しているかどうかを確認してください。PAT アドレスが必要になることもあります。または、変換および接続のタイムアウト インターバルを短縮してください。このメッセージは、メモリ不足の場合にも表示されます。メモリ使用量を減らすか、メモリを増設してください。

405002

エラー メッセージ %FWSM-4-405002: Received mac mismatch collision from IP_address/MAC_address for authenticated host

説明 このパケットに、次のいずれかの条件があると考えられます。

- Cisco ASA が、いずれかの非認証エントリから、IP アドレスが同じでも MAC アドレスが異なるパケットを受信しました。
- Cisco ASA 上で `vpnclient mac-exempt` コマンドを設定しており、Cisco ASA が対応する非認証エントリから、MAC アドレスは免除されていても IP アドレスが異なるパケットを受信しました。

推奨処置 正当なトラフィックの可能性もありますが、スプーフィング攻撃が進行している可能性もあります。送信元 MAC アドレスおよび IP アドレスを調べ、パケットの発信元を判別し、それが有効なホストに属するものであるかどうかを確認してください。

405101

エラー メッセージ %FWSM-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、または使用可能なアドレス変換スロットがないことを示しています。

推奨処置 グローバル プールのサイズが、内部ネットワークのクライアント数に適しているか確認してください。PAT アドレスが必要になることもあります。または、変換および接続のタイムアウト インターバルを短縮してください。メモリ不足が原因の可能性もあります。メモリ使用量を減らすか、メモリを増設してください。このメッセージが定期的に発生する場合は、無視してかまいません。頻繁に繰り返される場合には、TAC に連絡してください。

405102

エラー メッセージ %FWSM-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、または使用可能なアドレス変換スロットがないことを示しています。

推奨処置 グローバル プールのサイズが、内部ネットワークのクライアント数に適しているか確認してください。PAT アドレスが必要になることもあります。または、変換および接続のタイムアウト インターバルを短縮してください。メモリ不足が原因の可能性もあります。メモリ使用量を減らすか、メモリを増設してください。このメッセージが定期的に発生する場合は、無視してかまいません。頻繁に繰り返される場合には、TAC に連絡してください。

405103

エラー メッセージ %FWSM-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 を予期したにも関わらず、受信したのは 0x08 以外でした。エンドポイントが不正なパケットを送信しているか、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します。

推奨処置 対処は不要です。パケットは通過を認められます。

405104

エラー メッセージ %FWSM-4-405104: H225 message received from *outside_address/outside_port* to *inside_address/inside_port* before SETUP

説明 受信した H.225 メッセージの順序が不正であるときに、このメッセージが表示されます。初期 SETUP メッセージを受信する前に H.225 メッセージを受信しましたが、これは許容されない状況です。Cisco ASA はその他の H.225 メッセージを受け入れる前に、H.225 コール シグナリング チャネルの初期 SETUP メッセージを受信する必要があります。

推奨処置 対処は不要です。

405105

エラー メッセージ %FWSM-4-405105: H323 RAS message AdmissionConfirm received from *source_address/source_port* to *dest_address/dest_port* without an AdmissionRequest

説明 ゲートキーパが Admission Confirm (ACF) を送信しましたが、Cisco ASA はゲートキーパに Admission Request (ARQ) を送信しませんでした。

推奨処置 表示される *source_address* のゲートキーパをチェックして、ゲートキーパが ACF を送信したにも関わらず Cisco ASA から ARQ を受信しなかった理由を判別してください。

405201

エラーメッセージ %FWSM-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送信元 IP アドレスと一致しません。

推奨処置 *source_IP_address* で表されるホストをチェックして、不正な埋め込み IP アドレスのある ILS パケットを送信した理由を判別してください。

406001

エラーメッセージ %FWSM-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 port コマンドを入力し、1024 未満のポート（通常、サーバポート専用の well known ポート範囲）を指定しました。このメッセージは、サイトのセキュリティポリシーの回避が試みられていることを示しています。Cisco ASA はこのパケットをドロップし、接続を終了して、このイベントを記録します。

推奨処置 対処は不要です。

406002

エラーメッセージ %FWSM-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 port コマンドを発行し、接続に使用し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の回避が試みられていることを示しています。たとえば、攻撃者がパケットを途中で変更し、正しい送信元情報の代わりに別の送信元情報を書き込むことで、FTP セッションの乗っ取りを試みている可能性があります。セキュリティ アプライアンスはこのパケットを廃棄し、接続を終了して、このイベントを記録します。カッコ内のアドレスは、port コマンドのアドレスです。

推奨処置 対処は不要です。

407001

エラーメッセージ %FWSM-4-407001: Deny traffic for local-host *interface_name:inside_address*, license limit of *number* exceeded

説明 ホストの制限値を超過しました。次の条件が真である場合に、内部ホストは制限値までカウントされます。

- 内部ホストは直前の 5 分以内に、Cisco ASA 経由でトラフィックを転送している。
- 内部ホストは現在、Cisco ASA での変換接続またはユーザ認証を予約している。

推奨処置 ホストの制限値は、ローエンド プラットフォームに対して実施されます。ホストの制限値を表示するには、`show version` コマンドを使用します。現在のアクティブなホストおよび Cisco ASA でセッションを実行している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人または複数のユーザを強制的に接続解除するには、`clear local-host` コマンドを使用します。内部ユーザを迅速に期限切れにして制限値から取り除くには、`xlate`、`connection`、および `uauth` タイムアウトを推奨値またはそれより小さい値に設定します（表 2-4 を参照）。

表 2-4 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 %FWSM-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 Cisco ASA 経由での接続に関するメッセージです。特定の外部アドレスから特定のグローバルアドレスを経由して特定のローカルアドレスに到達する接続数が、そのスタティックに関する最大の初期接続数の制限値を超過した場合に、このメッセージが表示されます。Cisco ASA は、接続用のメモリが割り当て可能であれば、その接続の受け入れを試み、ローカルホストの代わりに外部ホストに SYN_ACK パケットを送信します。Cisco ASA は適切なステート情報を保持し、パケットを廃棄し、クライアントの確認応答を待機します。

推奨処置 正当なトラフィックの場合もありますが、DoS 攻撃が進行している可能性もあります。送信元アドレスを調べ、パケットの発信元を判別し、それが有効なホストかどうかを確認してください。

407003

エラー メッセージ %FWSM-4-407003: Established limit for RPC services exceeded *number*

説明 Cisco ASA は、ホールの最大数に達しているにも関わらず、RPC サーバのペアまたは設定済みのサービス用に新しいホールを開こうとしました。

推奨処置 ほかのホールが（該当するタイムアウトによって）閉じられるまで待つか、またはサーバのアクティブペアまたはサービスの数を制限してください。

408001

エラー メッセージ %FWSM-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まで減らそうとして失敗しました。

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てください。メッセージが継続的に表示される場合には、メッセージを正確にコピーして、TAC に報告してください。

408002

エラー メッセージ %FWSM-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2

説明 既存のルートと同じディスタンスで、より良好なメトリックを持つ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。新しいルートは、別のインターフェイス経由でインストールされた既存のルートを上書きします。この新しいルートは冗長性の確保だけを目的とし、ネットワーク上でのパス変更を意味します。この変更は、トポロジと再配布を通じて制御する必要があります。この変更によって影響される既存の接続があれば、その接続はおそらくディセーブルされ、タイムアウトします。このパス変更は、ネットワークトポロジがパス冗長性をサポートするように設計されている場合にのみ発生します。その場合、この変更は予期されています。

推奨処置 対処は不要です。

409001

エラー メッセージ %FWSM-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls

説明 ソフトウェアが、予期しない状態を検出しました。ルータは修復操作を実行して、動作を継続します。

推奨処置 対処は不要です。

409002

エラー メッセージ %FWSM-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 対処は不要です。

409003

エラー メッセージ %FWSM-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。エラー メッセージに詳細が表示されます。OSPF コンフィギュレーションが誤っているか、送信側の内部エラーが原因として考えられます。

推奨処置 受信側と送信側の OSPF コンフィギュレーションに不一致がないかどうかを確認してください。

409004

エラー メッセージ %FWSM-4-409004: Received reason from unknown neighbor *IP_address*

説明 OSPF hello パケット、データベース記述パケット、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。

推奨処置 この状況は、自動的に回復します。

409005

エラー メッセージ %FWSM-4-409005: Invalid length number in OSPF packet from *IP_address* (ID *IP_address*), *interface_name*

説明 システムは OSPF パケットを受信しましたが、OSPF パケットのフィールド長が通常のヘッダー サイズよりも短いか、到着時の IP パケットのサイズと矛盾しています。これは、パケット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あるルータを特定し、そのルータを再起動してください。

409006

エラー メッセージ %FWSM-4-409006: Invalid lsa: reason Type number, LSID *IP_address* from *IP_address*, *IP_address*, *interface_name*

説明 ルータが、LSA タイプが無効である LSA を受信しました。メモリが壊れているか、ルータ上の予期しない動作が原因です。

推奨処置 近接アドレスから問題のあるルータを特定し、そのルータを再起動してください。TAC に連絡して指示を受け、問題の原因を調べてください。

409007

エラー メッセージ %FWSM-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 TAC に連絡して指示を受け、問題の原因を調べてください。

409008

エラー メッセージ %FWSM-4-409008: Found generating default LSA with non-zero mask LSA type : *number* Mask: *netmask* metric : *number* area : *string*

説明 内部ソフトウェア エラーが発生したため、ルータは誤ったマスクを使用してデフォルトの LSA を生成しようとしていました。誤ったメトリックが使用された可能性もあります。

推奨処置 TAC に連絡して指示を受け、問題の原因を調べてください。

409009

エラー メッセージ %FWSM-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 が、いずれかの OSPF インターフェイスの IP アドレスからのルータ ID の割り当てに失敗しました。

推奨処置 少なくとも1つのインターフェイスが起動し、有効な IP アドレスが割り当てられていることを確認してください。ルータ上で複数の OSPF プロセスを実行する場合、各プロセスに一意的ルータ ID が必要です。各プロセスがルータ ID を取得できるように、十分なインターフェイス数をアップにしておく必要があります。

409010

エラー メッセージ %FWSM-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 TAC に連絡して指示を受け、問題の原因を調べてください。

409011

エラー メッセージ %FWSM-4-409011: OSPF detected duplicate router-id *IP_address* from *IP_address* on interface *interface_name*

説明 OSPF が、このルーティング プロセスと同じルータ ID を持つネイバから、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 のルータ ID は一意でなければなりません。近接ルータ ID を変更してください。

409012

エラー メッセージ %FWSM-4-409012: Detected router with duplicate router ID *IP_address* in area *string*

説明 OSPF が、このルーティング プロセスと同じルータ ID を持つネイバから、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 のルータ ID は一意でなければなりません。近接ルータ ID を変更してください。

409013

エラー メッセージ %FWSM-4-409013: Detected router with duplicate router ID *IP_address* in Type-4 LSA advertised by *IP_address*

説明 OSPF が、このルーティング プロセスと同じルータ ID を持つネイバから、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 のルータ ID は一意でなければなりません。近接ルータ ID を変更してください。

409023

エラー メッセージ %FWSM-4-409023: Attempting AAA Fallback method *method_name* for *request_type* request for user *user* :Auth-server group *server_tag* unreachable

説明 外部サーバへの認証または許可の試みが失敗し、ローカル ユーザ データベースを使用して実行されます。*aaa_operation* は、[authentication] または [authorization] のいずれかです。*username* は、接続に対応付けられたユーザです。*server_group* は、サーバに到達不可能な AAA サーバグループです。

推奨処置 設定されている AAA サーバとの接続に問題がないかどうかを最初に確認してください。Cisco ASA から認証サーバに ping を実行してください。AAA サーバ上でデーモンが動作しているかどうかを確認してください。

410001

エラー メッセージ %FWSM-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 UDP DNS パケットでドメイン名の長さが 255 バイトを超えると、このメッセージが表示されます (RFC 1035 セクション 3.1 を参照)。

推奨処置 対処は不要です。

411001

エラー メッセージ %FWSM-4-411001:Line protocol on interface *interface_name* changed state to up

説明 ライン 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 [inside]、[outside] などの論理インターフェイス名である場合、このメッセージは、論理インターフェイスのライン 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 [Ethernet0]、[GigabitEthernet0/1] などの物理インターフェイス名である場合、このメッセージは、物理インターフェイスのライン 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 対処は不要です。

411002

エラー メッセージ %FWSM-4-411002:Line protocol on interface *interface_name* changed state to down

説明 ライン 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 [inside]、[outside] などの論理インターフェイス名である場合、このメッセージは、論理インターフェイスのライン 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のライン プロトコル ステータスには影響ありません。*interface_name* が [Ethernet0]、[GigabitEthernet0/1] などの物理インターフェイス名である場合、このメッセージは、物理インターフェイスのライン 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で予期しないイベントである場合は、物理回線をチェックしてください。

411003

エラー メッセージ %FWSM-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である場合は、物理回線をチェックしてください。

411004

エラー メッセージ %FWSM-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 ステータスがダウンからアップに変更されました。

推奨処置 対処は不要です。

412001

エラー メッセージ %FWSM-4-412001:MAC *MAC_address* moved from *interface_1* to *interface_2*

説明 1つのモジュール インターフェイスから別のインターフェイスへのホストの移動が検知されると、このメッセージが生成されます。トランスペアレント Cisco ASA の場合、ホスト (MAC) と Cisco ASA ポート間のマッピングは、レイヤ 2 転送テーブルで維持されます。このテーブルによって、パケットの送信元 MAC アドレスが Cisco ASA ポートに動的にバインドされます。このプロセスで、インターフェイス間でのホストの移動が検知されると、このメッセージが生成されます。

推奨処置 ホストの移動は有効な場合もありますが、他のインターフェイス上でホスト MAC のスプーフィングが試みられた可能性もあります。MAC スプーフィング試行の場合には、ネットワーク上で脆弱なホストを特定してそれらを削除するか、またはスタティック MAC アドレスを設定してください(その場合、MAC アドレスとポートのバインディングは変更できません)。単なるホストの移動の場合には、対処は不要です。

412002

エラー メッセージ %FWSM-4-412002:Detected bridge table full while inserting MAC *MAC_address* on interface *interface*. Number of entries = *num*

説明 ブリッジ テーブルが満杯な状態でエントリの追加が試みられたときに、このメッセージが生成されます。Cisco ASA はコンテキストごとに1つのレイヤ 2 転送テーブルを維持し、コンテキストがそのサイズ制限を超えると、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、テーブル内で既存のダイナミック エントリのうち最も古いエントリ(存在する場合)を置き換えます。

推奨処置 攻撃が試みられた可能性があります。新しいブリッジ テーブル エントリが有効かどうかを確認してください。攻撃の場合には、EtherType ACL を使用して脆弱なホストをアクセス制御してください。

413001

エラー メッセージ %FWSM-4-413001: Module in slot *slotnum* is not able to shut down. Module Error: *errnum message*

説明 *slotnum* に搭載されたモジュールが、FWSM システム モジュールからのシャットダウン要求に従いませんでした。モジュールは割り込み不可能なタスク（ソフトウェアのアップグレードなど）を実行していた可能性があります。モジュールがシャットダウンできなかった理由と対処方法は、*errnum* および *message* テキストで表示されます。

推奨処置 モジュール上のタスクが完了するまで待ち、それからモジュールをシャットダウンするか、または *session* コマンドを使用してモジュールの CLI にアクセスし、モジュールがシャットダウンできない原因となっているタスクを停止してください。

413002

エラー メッセージ %FWSM-4-413002: Module in slot *slotnum* is not able to reload. Module Error: *errnum message*

説明 *slotnum* に搭載されたモジュールが、FWSM システム モジュールからのリロード要求に従いませんでした。モジュールは割り込み不可能なタスク（ソフトウェアのアップグレードなど）を実行していた可能性があります。モジュールがリロードできなかった理由と対処方法は、*errnum* および *message* テキストで表示されます。

推奨処置 モジュール上のタスクが完了するまで待ち、それからモジュールをリロードするか、または *session* コマンドを使用してモジュールの CLI にアクセスし、モジュールがリロードできない原因となっているタスクを停止してください。

413003

エラー メッセージ %FWSM-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が検出された場合に表示されます。

推奨処置 搭載されているモジュール タイプをサポートする FWSM 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てください。

413004

エラー メッセージ %FWSM-4-413004: Module in slot *slotnum* failed to write software *vnewver* (currently *vver*), *reason*. Trying again.

説明 指定のスロット番号のモジュールがソフトウェア バージョンの受け入れに失敗し、UNRESPONSIVE ステートに移行します。モジュールソフトウェアを更新する試みがもう一度、行われます。

slotnum モジュールの搭載先スロット番号

vnewver モジュールに正常に書き込めなかったソフトウェアの新しいバージョン番号（例：1.0(1)0）

vver モジュールの現在のソフトウェア バージョン番号（例：1.0(1)0）

reason 新しいバージョンがモジュールに書き込めなかった理由。表示される可能性のある *reason* の値は次のとおりです。

- write failure.
- failed to create a thread to write the image.

推奨処置 対処は不要です。後続の試行で、更新の成功または失敗を表すメッセージが生成されます。更新後にモジュールが UP に移行したかどうかを確認するには、`show module slotnum` コマンドを使用します。

414001

エラー メッセージ %FWSM-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 ログイング モジュールがログイング バッファを外部 FTP サーバに保存できなかった場合に、このシステム ログ メッセージが表示されます。

推奨処置 失敗の理由に基づいて、適切な処置を行ってください。

- プロトコル エラー FTP サーバと Cisco ASA の接続に問題がなく、FTP サーバが FTP PORT コマンドと put 要求を受け入れ可能であることを確認してください。
- 無効なユーザ名またはパスワード 設定されている FTP クライアントのユーザ名とパスワードが正しいかどうかを確認してください。
- その他のエラー Cisco TAC に連絡し、指示を受けてください。

414002

エラー メッセージ %FWSM-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: *filename*: [*fail_reason*]

説明 ログイング モジュールがログイング バッファをシステム フラッシュに保存できなかった場合に、このシステム ログ メッセージが表示されます。

推奨処置 失敗の理由がスペース不足の場合には、システム フラッシュの空き容量を調べ、設定されている `logging flash-size` コマンドの制限が適切かどうかを確認してください。フラッシュ ファイル システムの IO エラーの場合には、シスコのテクニカル サポートに連絡して指示を受けてください。

416001

エラー メッセージ %FWSM-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 An SNMP パケットが、不正なパケット フォーマットのため、または Cisco ASA で認められない *prot_version* のために、Cisco ASA の通過を拒否されました。*prot_version* フィールドに表示される値は、1、2、2c、3 のいずれかです。

推奨処置 `snmp-map` コマンドを使用して、SNMP 検査に関する設定を変更します。このコマンドを使用すると、ユーザ側で特定のプロトコル バージョンを許可または禁止することができます。

417001

エラー メッセージ %FWSM-4-417001: Unexpected event received: *number*

説明 プロセスが信号を受信しましたが、このイベントに対応する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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

417004

エラー メッセージ %FWSM-4-417004: Filter violation error: conn *number* (*string:string*) in *string*

説明 クライアントが所有していないルートアトリビュートの変更を試みました。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

417006

エラー メッセージ %FWSM-4-417006: No memory for *string*) in *string*. Handling: *string*

説明 メモリ不足のため操作が失敗しましたが、その操作は別のメカニズムによって処理されません。

説明 メモリが十分にある場合には、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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

418001

エラー メッセージ %FWSM-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 特定の送信元から宛先へのパケットが、管理専用のネットワークとの間で Cisco ASA を通過しているため、廃棄されました。

protocol_string TCP、UDP、ICMP、または 10 進数で表されるプロトコル 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 誰が何の目的で、このようなパケットを発信しているのかを調査してください。

419001

```
set connection advanced-options tmap service-policy global_policy global
```

420001

メッセージ 500001 ~ 507001

ここでは、メッセージ 500001 ~ 507001 を示します。

500001

エラーメッセージ %FWSM-5-500001: ActiveX content modified src *IP_address* dest *IP_address* on interface *interface_name*.

説明 `filter` コマンドを使用して `activex` オプションをオンにした場合に、Cisco ASA が ActiveX オブジェクトを検出したときに、このメッセージが表示されます。`activex` オプションを使用すると、Cisco ASA は ActiveX コンテンツが HTML オブジェクトとしてタグングされないように変更して、ActiveX コンテンツをフィルタリングすることができます。

推奨処置 対処は不要です。

500002

エラーメッセージ %FWSM-5-500002: Java content modified src *IP_address* dest *IP_address* on interface *interface_name*.

説明 `filter` コマンドを使用して `java` オプションをオンにした場合に、Cisco ASA が Java アプレットを検出したときに、このメッセージが表示されます。`java` オプションを使用すると、Cisco ASA は Java コンテンツが HTML オブジェクトとしてタグングされないように変更して、Java コンテンツをフィルタリングすることができます。

推奨処置 対処は不要です。

500003

エラーメッセージ %FWSM-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 TCP のヘッダー長が誤っていることを示しています。OS (オペレーティングシステム) によっては、ディセーブルのソケットへの接続要求の応答時に、TCP リセット (RST) が正しく処理されません。クライアントが Cisco ASA の外部の FTP サーバに接続を試みたとき、FTP がリスニングしていないと、サーバは RST を送信します。オペレーティングシステムによっては、誤った TCP ヘッダー長が送信されるため、この問題が発生します。UDP は、ICMP ポート到達不能メッセージを使用します。

TCP ヘッダー長がパケット長より大きいために、負数バイトの転送を示していることがあります。システム ログメッセージでは負数が符号なしの数値として表示されるので、1 秒間の転送サイズが 4 GB のように、異常に大きな値として表示されることがあります。

推奨処置 対処は不要です。このメッセージは頻繁には発生しません。

500004

エラー メッセージ %FWSM-4-500004: Invalid transport field for protocol=*protocol*, from *source_address/source_port* to *dest_address/dest_port*

説明 プロトコルの送信元または宛先ポート番号がゼロという、無効な転送番号が存在することを示しています。*protocol* 値は、TCP の場合は 6、UDP の場合は 17 です。

推奨処置 このメッセージが継続的に表示される場合は、ピアの管理者に連絡してください。

501101

エラー メッセージ %FWSM-5-501101: User transitioning priv level

説明 コマンドの権限レベルが変更されました。

推奨処置 対処は不要です。

502101

エラー メッセージ %FWSM-5-502101: New user added to local dbase: Uname: *user* Priv: *privilege_level* Encpass: *string*

説明 新しいユーザ名レコードが作成されました。ユーザ名、権限レベル、および暗号化パスワードがメッセージに表示されます。

推奨処置 対処は不要です。

502102

エラー メッセージ %FWSM-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。ユーザ名、権限レベル、および暗号化パスワードがメッセージに表示されます。

推奨処置 対処は不要です。

502103

エラー メッセージ %FWSM-5-502103: User priv level changed: Uname: *user* From: *privilege_level* To: *privilege_level*

説明 ユーザの権限レベルが変更されました。

推奨処置 対処は不要です。

502111

エラーメッセージ %FWSM-5-502111: New group policy added: name: *policy_name* Type: *policy_type*

説明 `group-policy` CLI コマンドを使用してグループ ポリシーが設定されていることを表します。*policy_name* は、グループ ポリシー名です。*policy_type* は、[internal] または [external] のいずれかです。

推奨処置 対処は不要です。

502112

エラーメッセージ %FWSM-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たことを表します。*policy_name* はグループ ポリシー名です。*policy_type* は、[internal] または [external] のいずれかです。

推奨処置 対処は不要です。

503001

エラーメッセージ %FWSM-5-503001: Process number, Nbr *IP_address* on *interface_name* from *string* to *string*, *reason*

説明 OSPF ネイバのステートが変更されました。メッセージに、変更内容と理由が表示されます。このメッセージが表示されるのは、OSPF プロセスに `log-adjacency-changes` コマンドが設定されている場合だけです。

推奨処置 TAC に連絡して指示を受け、問題の原因を調べてください。

504001

エラーメッセージ %FWSM-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 対処は不要です。

504002

エラーメッセージ %FWSM-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 対処は不要です。

505001

エラー メッセージ %FWSM-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表示されます。

推奨処置 対処は不要です。

505002

エラー メッセージ %FWSM-5-505002: Module in slot *slotnum* is reloading. Please wait...

説明 カードのリロード中に表示されます。

推奨処置 対処は不要です。

505003

エラー メッセージ %FWSM-5-505003: Module in slot *slotnum* is resetting. Please wait...

説明 モジュールのリセット中に表示されます。

推奨処置 対処は不要です。

505004

エラー メッセージ %FWSM-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ときに表示されます。

推奨処置 対処は不要です。

505005

エラー メッセージ %FWSM-5-505005: Module in slot *slotnum* is initializing control communication. Please wait...

説明 モジュールが認識され、FWSM システム モジュールがこのモジュールとの制御チャネル通信を初期化しているときに表示されます。

推奨処置 対処は不要です。

505006

エラー メッセージ %FWSM-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、UP ステートになったときに表示されます。

推奨処置 対処は不要です。

505007

エラー メッセージ %FWSM-5-505007: Module in slot *slotnum* is recovering. Please wait...

説明 モジュールが `hw-module module slotnum recover boot` コマンドによって回復されているときに表示されます。

推奨処置 対処は不要です。

506001

エラー メッセージ %FWSM-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化しました。このメッセージは、ファイル システムが使用可能または使用不可能になったイベントと、そのイベントの発生元を記述します。ファイル システム ステータスの変化を引き起こしたイベントの発生元とイベントの例は、次のとおりです。

- External Compact Flash removed
- External Compact Flash inserted
- External Compact Flash -unknown event

推奨処置 対処は不要です。

507001

エラー メッセージ %FWSM-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 TCP セグメントの組み立て中に、再組み立てバッファの制限を超過したときに表示されます。

- *source_address*/*source_port* 接続を開始するパケットの送信元 IP アドレスおよび送信元ポート
- *dest_address*/*dest_port* 接続を開始するパケットの宛先 IP アドレスおよび宛先ポート
- *interface_inside* 接続を開始したパケットが着信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が発信されるインターフェイスの名前
- *limit* このトラフィック クラスに設定されている初期接続の制限数

推奨処置 対処は不要です。

メッセージ 602101 ~ 609002

ここでは、メッセージ 602101 ~ 609002 を示します。

602101

エラー メッセージ %FWSM-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した場合、および [don't-fragment] ビットが設定されているけれども、フラグメント化が必要な場合に生成されます。

推奨処置 データが正常に送信されていることを確認してください。

602102

エラー メッセージ %FWSM-6-602102: Adjusting IPSec tunnel mtu...

説明 パス MTU 検出により、IPSec トンネルの MTU (最大伝送ユニット) が調整されました。

推奨処置 IPSec トンネルの MTU を確認してください。実効 MTU が標準より小さい場合には、中間リンクを確認してください。

602201

エラー メッセージ %FWSM-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 ISAKMP SA が作成されたときに表示されます。

推奨処置 対処は不要です。

602202

エラー メッセージ %FWSM-6-602202: ISAKMP session connected (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP ピアが接続しました。

推奨処置 対処は不要です。

602203

エラー メッセージ %PIX-6-602203: ISAKMP session disconnected (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP ピアが接続解除しました。

推奨処置 対処は不要です。

602301

エラー メッセージ %FWSM-6-602301: sa created...

説明 新しいセキュリティ アソシエーション (SA) が作成されました。

推奨処置 対処は不要です。

602302

エラー メッセージ %FWSM-6-602302: deleting sa

説明 SA が削除されました。

推奨処置 対処は不要です。

602303

エラー メッセージ %FWSM: IPSEC: An *direction tunnel_type* SA (SPI=*spi*) between *local_IP* and *remote_IP* (*username*) has been created.

direction SA の方向 (inbound または outbound)

tunnel_type SA のタイプ (remote access または L2L)

spi IPsec セキュリティ パラメータ インデックス

local_IP トンネル ローカル エンドポイントの IP アドレス

remote_IP トンネル リモート エンドポイントの IP アドレス

username IPsec トンネルに対応付けられたユーザ名

説明 新しい SA が作成されました。

推奨処置 対処は不要です。

602304

エラー メッセージ %FWSM-6-602304: IPSEC: An *direction tunnel_type* SA (SPI=*spi*) between *local_IP* and *remote_IP* (*username*) has been deleted.

説明 SA が削除されたときに表示されます。

direction SA の方向 (inbound または outbound)

tunnel_type SA のタイプ (remote access または L2L)

spi IPSec セキュリティ パラメータ インデックス

local_IP トンネル ローカル エンドポイントの IP アドレス

remote_IP トンネル リモート エンドポイントの IP アドレス

username IPSec トンネルに対応付けられたユーザ名

推奨処置 対処は不要です。

604101

エラー メッセージ %FWSM-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 サーバから正常に IP アドレスを取得しました。dhcp コマンド ステートメントによって、Cisco ASA は DHCP サーバからネットワーク インターフェイスの IP アドレスおよびネットワーク マスクのほかに、デフォルト ルートも取得できます。default route ステートメントでは、ゲートウェイ アドレスをデフォルト ルータのアドレスとして使用します。

推奨処置 対処は不要です。

604102

エラー メッセージ %FWSM-6-604102: DHCP client interface *interface_name*: address released

説明 Cisco ASA の DHCP クライアントが、割り当て済みの IP アドレスを DHCP サーバに戻しました。

推奨処置 対処は不要です。

604103

エラー メッセージ %FWSM-6-604103: DHCP daemon interface *interface_name*: address granted *MAC_address* (*IP_address*)

説明 Cisco ASA の DHCP サーバが、外部クライアントに IP アドレスを付与しました。

推奨処置 対処は不要です。

604104

エラーメッセージ %FWSM-6-604104: DHCP daemon interface *interface_name*: address released

説明 外部クライアントから、Cisco ASA の DHCP サーバに IP アドレスが戻されました。

推奨処置 対処は不要です。

606001

エラーメッセージ %FWSM-6-606001: ASDM session number *number* from *IP_address* started

説明 管理者が認証され、ASDM セッションが開始されたことを示しています。

推奨処置 対処は不要です。

606002

エラーメッセージ %FWSM-6-606002: ASDM session number *number* from *IP_address* ended

説明 ASDM セッションが終了したことを示しています。

推奨処置 対処は不要です。

606003

エラーメッセージ %FWSM-6-606003: ASDM logging session number *id* from *IP_address* started *id* session ID assigned

説明 リモート管理クライアントによって ASDM ログイン接続が開始されました。

IP_address リモート管理クライアントの IP アドレス

推奨処置 対処は不要です。

606004

エラーメッセージ %FWSM-6-606004: ASDM logging session number *id* from *IP_address* ended

説明 ASDM ログイン接続が終了しました。

id 割り当て済みのセッション ID

IP_address リモート管理クライアントの IP アドレス

推奨処置 対処は不要です。

607001

エラー メッセージ %FWSM-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 SIP メッセージの検査後に、**fixup sip** コマンドにより SIP 接続が割り当てられたことを示しています。*connection_type* は、次のいずれかのストリングです。

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

推奨処置 対処は不要です。

608001

エラー メッセージ %FWSM-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 Skinny メッセージの検査後に、**fixup skinny** コマンドにより Skinny 接続が割り当てられたことを示しています。*connection_type* は、次のいずれかのストリングです。

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

推奨処置 対処は不要です。

609001

エラー メッセージ %FWSM-6-609001: Built local-host *interface_name:IP_address*

説明 インターフェイス *interface_name* に接続するホストの *IP_address* 用に、ネットワーク ステート コンテナが予約されました。これは情報メッセージです。

推奨処置 対処は不要です。

609002

エラーメッセージ %FWSM-6-609002: Teardown local-host *interface_name:IP_address*
duration time

説明 インターフェイス *interface_name* に接続するホストの *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 対処は不要です。

610001

エラーメッセージ %FWSM-3-610001: NTP daemon interface *interface_name*: Packet denied
from *IP_address*

説明 設定されている NTP サーバと一致しないホストから、NTP パケットを受信しました。Cisco ASA は単に NTP クライアントであり、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 対処は不要です。

610002

エラーメッセージ %FWSM-3-610002: NTP daemon interface *interface_name*:
Authentication failed for packet from *IP_address*

説明 受信した NTP パケットが認証チェックに失敗しました。

推奨処置 Cisco ASA および NTP サーバが両方とも認証を使用し、同じキー番号および値を使用するように設定されているかどうかを確認してください。

610101

エラーメッセージ %FWSM-6-610101: Authorization failed: Cmd: *command* Cmdtype:
command_modifier

説明 指定のコマンドが、コマンド許可に失敗しました。 *command_modifier* は、次のいずれかのストリングです。

- **cmd** (このストリングは、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 が上記の4つのコマンドタイプ以外の値を検出した場合は、[unknown command type] というメッセージが表示されます。

推奨処置 対処は不要です。

612001

エラー メッセージ %FWSM-5-612001: Auto Update succeeded:filename, version:number

説明 自動アップデート サーバ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 のいずれかです。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 対処は不要です。

612002

エラー メッセージ %FWSM-4-612002: Auto Update failed:filename, version:number, reason:reason

説明 自動アップデート サーバからのアップデートが失敗したことを示しています。filename 変数は、image、ASDM file、または configuration のいずれかです。version number 変数は、アップデートのバージョン番号です。reason 変数は、アップデートが失敗した理由を示します。失敗の原因としては、無効なイメージ ファイル、サーバへの接続切断、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 自動アップデート サーバのコンフィギュレーションを確認してください。

612003

エラー メッセージ %FWSM-4-612003:Auto Update failed to contact:url, reason:reason

説明 自動アップデート デモンが指定の URL url に接続できなかったことを示しています。この URL は、自動アップデート サーバの URL、または自動アップデート サーバによって返された、いずれかのファイル サーバの URL です。reason フィールドは、接続が失敗した理由を示します。失敗の原因としては、サーバからの応答がなかった場合、認証の失敗、ファイルが見つからなかった場合などが考えられます。

推奨処置 自動アップデート サーバのコンフィギュレーションを確認してください。

613001

エラー メッセージ %FWSM-6-613001: Checksum Failure in database in area string
Link State Id IP_address Old Checksum number New Checksum number

説明 OSPF が、データベースでメモリの破壊によるチェックサム エラーを検出しました。

推奨処置 OSPF プロセスを再起動してください。

613002

エラー メッセージ %FWSM-6-613002: interface interface_name has zero bandwidth

説明 インターフェイスの帯域幅がゼロとして報告されました。

推奨処置 TAC に連絡して指示を受け、問題の原因を調べてください。

613003

エラーメッセージ %FWSM-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り、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を指定して、OSPF を再設定してください。

614001

エラーメッセージ %FWSM-6-614001: Split DNS: request patched from server: *IP_address* to server: *IP_address*

説明 スプリット DNS により、DNS クエリが本来の送信先サーバからプライマリ エンタープライズ DNS サーバにリダイレクトされています。

推奨処置 対処は不要です。

614002

エラーメッセージ %FWSM-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 により、DNS クエリがエンタープライズ DNS サーバから本来の送信先サーバからプライマリ エンタープライズ にリダイレクトされています。

推奨処置 対処は不要です。

615001

エラーメッセージ %FWSM-6-615001: vlan number not available for firewall interface

説明 スイッチが FWSM から VLAN (仮想 LAN) を削除しました。

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 %FWSM-6-615002: vlan number available for firewall interface

説明 スイッチが FWSM に VLAN を追加しました。

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 %FWSM-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 が割り当てられました。このメッセージでは、接続の割り当てをトリガーしたメッセージも示します。

推奨処置 対処は不要です。

617001

エラー メッセージ %FWSM-6-617001: GTPv *version msg_type* from *source_interface:source_address/source_port* not accepted by *source_interface:dest_address/dest_port*

説明 要求がピアによって受け入れられなかったときに表示されるメッセージです。Create PDP Context 要求でよくある状況です。

推奨処置 対処は不要です。

617002

エラー メッセージ %FWSM-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 データベースから PDP コンテキストが削除されたときに表示されるメッセージです。原因としては、期限切れ、Delete PDP Context 要求 / 応答の交換、またはユーザによる CLI 経路での削除があります。

推奨処置 対処は不要です。

617003

エラー メッセージ %FWSM-6-617003: GTP Tunnel created from *source_interface:source_address/source_port* to *source_interface:dest_address/dest_port*

説明 Create PDP Context 要求を受け入れる応答の受信後、GTP トンネルが作成されたときに表示されるメッセージです。

推奨処置 対処は不要です。

617004

エラー メッセージ %FWSM-6-617004: GTP connection created for response from *source_interface:source_address/0* to *source_interface:dest_address/dest_port*

説明 Create PDP Context 要求または応答で指定される SGSN または GGSN シグナリング アドレスが、送信した SGSN/GGSN とは異なる場合に表示されるメッセージです。

推奨処置 対処は不要です。

620001

エラー メッセージ %FWSM-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 が、指定の CTIQBE メディア トラフィックに接続オブジェクトを割り当てます。このメッセージは、10 秒で 1 回にレート制限されています。

推奨処置 対処は不要です。

620002

エラー メッセージ %FWSM-4-620002: Unsupported CTIQBE version: *hex*: from *interface_name:IP_address/port* to *interface_name:IP_address/port*

説明 Cisco ASA が、サポート対象外のバージョン番号を持つ CTIQBE メッセージを受信しました。Cisco ASA は、このパケットを廃棄します。このメッセージは、10 秒で 1 回にレート制限されています。

推奨処置 このログメッセージでキャプチャされたバージョン番号が極端に大きい (10 より大きい) 場合、パケットのフォーマットが不正、CTIQBE 以外のパケット、または Cisco ASA に着信する前にパケットが壊れていた可能性があります。パケットの送信元を調べることを推奨します。バージョン番号が一般的な小さい値 (10 以下) の場合には、Cisco TAC に連絡し、この CTIQBE バージョンに対応する新しい Cisco ASA イメージが使用可能かどうかを確認してください。

621001

エラー メッセージ %FWSM-6-621001: Interface *interface_name* does not support multicast, not enabled

説明 マルチキャストをサポートしないインターフェイス上で PIM をイネーブルにしようとしたときに、このメッセージが表示されます。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

621002

エラー メッセージ %FWSM-6-621002: Interface *interface_name* does not support multicast, not enabled

説明 マルチキャストをサポートしないインターフェイス上で igmp をイネーブルにしようとしたときに、このメッセージが表示されます。

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に先立つイベントについての詳細情報とともに、Cisco TAC に提出してください。

621003

エラー メッセージ %FWSM-6-621003: The event queue size has exceeded *number*

説明 イベント マネージャの作成数が、予期される量を超過した場合に表示されるメッセージです。

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に先立つイベントについての詳細情報とともに、TAC に提出してください。

621006

エラー メッセージ %FWSM-6-621006: Mrib disconnected, (*IP_address*, *IP_address*) event cancelled

説明 データ駆動イベントをトリガーするパケットを受信したけれども、MRIB への接続がダウンしている場合に表示されるメッセージです。通知はキャンセルされました。

推奨処置 システムの起動後にこのメッセージが続く場合は、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に先立つイベントについての詳細情報とともに、TAC に提出してください。

621007

エラー メッセージ %FWSM-6-621007: Bad register from *interface_name*:*IP_address* to *IP_address* for (*IP_address*, *IP_address*)

説明 Rendezvous Point (RP; ランデブー ポイント) として設定されている、または Network Address Translation (NAT; ネットワーク アドレス変換) を使用するように設定されている PIM ルータが、他の PIM ルータからの PIM 登録パケットを受信したときに表示されます。このパケットにカプセル化されているデータは無効です。

推奨処置 送信側のルータは誤って RFC 以外の登録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てください。

メッセージ 701001 ~ 720073

ここでは、メッセージ 701001 ~ 720073 を示します。

ほとんどの ISAKMP Syslog には、トンネルを識別するのに役立つ、共通の前置オブジェクトがあります。システム ログ メッセージの説明テキストの前に、該当するオブジェクトがあれば表示されます。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には、固有の [heading = value] の組み合わせは表示されません。

このオブジェクトは次の形式で表示されます。

```
[Group = groupname, Username = user, IP = IP_address, ...]
```

Group はトンネルグループ、username はローカルデータベースまたは AAA サーバにあるユーザ名、IP address 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 %FWSM-7-701001: alloc_user() out of Tcp_user objects

説明 AAA (認証、許可、アカウントिंग) メッセージです。モジュールのユーザ認証レートが高すぎて、新しい AAA 要求を処理できないときに表示されます。

推奨処置 floodguard enable コマンドを使用して、Flood Defender 機能をイネーブルにしてください。

701002

エラー メッセージ %FWSM-7-701002: alloc_user() out of Tcp_proxy objects

説明 AAA メッセージです。モジュールのユーザ認証レートが高すぎて、新しい AAA 要求を処理できないときに表示されます。

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 %FWSM-7-702201: ISAKMP Phase 1 delete received (local IP_address (initiator|responder), remote IP_address)

説明 ISAKMP 削除メッセージを受信しました。

推奨処置 対処は不要です。

702202

エラー メッセージ %FWSM-7-702202: ISAKMP Phase 1 delete sent (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP 削除メッセージを送信しました。

推奨処置 対処は不要です。

702203

エラー メッセージ %FWSM-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ていません。DPDにより、ピアがタイムアウトしました。

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てください。

702204

エラー メッセージ %FWSM-7-702204: ISAKMP Phase 1 retransmission (local *IP_address* (initiator|responder), remote *IP_address*)

説明 リモートピアが応答していません。ISAKMPは直前のパケットを再送信しています。

推奨処置 リモートホストへのネットワーク接続と、ローカル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てください。

702205

エラー メッセージ %FWSM-7-702205: ISAKMP Phase 2 retransmission (local *IP_address* (initiator|responder), remote *IP_address*)

説明 リモートピアが応答していません。ISAKMPは直前のパケットを再送信しています。

推奨処置 リモートホストへのネットワーク接続と、ローカル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てください。

702206

エラー メッセージ %FWSM-7-702206: ISAKMP malformed payload received (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMPが不正なメッセージまたは不正なフォーマットのメッセージを受信しました。リモートピアとの同期外れ、メッセージの復号化の問題、またはメッセージを受信した順序が不正だったことを表す場合があります。

推奨処置 事前共有鍵を使用している場合は、ローカルの事前共有鍵がローカルおよびリモートデバイスで正しく設定されているかどうかを確認してください。ローカルおよびリモートのコンフィギュレーションを確認してください。必要とされるSAがアップにならない場合は、さらにトラブルシューティングが必要になる可能性があります。

702207

エラーメッセージ %FWSM-7-702207: ISAKMP duplicate packet detected (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP が、前に受信したパケットと重複するパケットを受信しました。正常な動作時にも発生する場合がありますが、ISAKMP 交換でのエラーの副作用として発生する場合があります。

推奨処置 接続と、ローカルおよびリモートのコンフィギュレーションを確認してください。

702208

エラーメッセージ %FWSM-7-702208: ISAKMP Phase 1 exchange started (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP がリモートピアとの新しいフェーズ1メッセージ交換を開始しました。

推奨処置 対処は不要です。

702209

エラーメッセージ %FWSM-7-702209: ISAKMP Phase 2 exchange started (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP がリモートピアとの新しいフェーズ2メッセージ交換を開始しました。

推奨処置 対処は不要です。

702210

エラーメッセージ %FWSM-7-702210: ISAKMP Phase 1 exchange completed(local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP がフェーズ1交換を終了しました。

推奨処置 対処は不要です。

702211

エラーメッセージ %FWSM-7-702211: ISAKMP Phase 2 exchange completed(local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP がフェーズ2交換を終了しました。

推奨処置 対処は不要です。

702212

エラー メッセージ %FWSM-7-702212: ISAKMP Phase 1 initiating rekey (local *IP_address* (initiator|responder), remote *IP_address*)

説明 ISAKMP はフェーズ 1 再キーイングを初期化中です。

推奨処置 対処は不要です。

702301

エラー メッセージ %FWSM-7-702301: lifetime expiring...

説明 SA のライフタイムが満了しました。

推奨処置 デバッグメッセージです。

702302

エラー メッセージ %FWSM-3-702302: replay rollover detected...

説明 IPSec トンネルで 40 億超の packets を受信し、新しいトンネルをネゴシエートしています。

推奨処置 ピアの管理者に連絡し、SA ライフタイムの設定を比較してください。

702303

エラー メッセージ %FWSM-7-702303: sa_request...

説明 IPSec が新しい SA 用の IKE を要求しました。

推奨処置 これは、デバッグメッセージです。

703001

エラー メッセージ %FWSM-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 がサポート対象外のバージョン番号を持つ H.323 パケットを受信しました。Cisco ASA は、パケットの protocol version フィールドをサポート対象の最大バージョンに変更する場合があります。

推奨処置 Cisco ASA が VoIP ネットワーク上でサポートする H.323 バージョンを使用してください。

703002

エラー メッセージ %FWSM-7-703002: Received H.225 Release Complete with newConnectionNeeded for *interface_name:IP_address* to *interface_name:IP_address/port*

説明 このデバッグメッセージは、Cisco ASA が特定の H.225 メッセージを受信し、Cisco ASA が指定の 2 つの H.323 エンドポイント用に新しいシグナリング接続オブジェクトを開始したことを示しています。

推奨処置 対処は不要です。

709001、709002

エラー メッセージ %FWSM-7-709001: FO replication failed: cmd=*command* returned=*code*

エラー メッセージ %FWSM-7-709002: FO unreplicable: cmd=*command*

説明 これらのフェールオーバー メッセージは、開発デバッグ テスト時にのみ表示されます。

推奨処置 対処は不要です。

709003

エラー メッセージ %FWSM-1-709003: (Primary) Beginning configuration replication: Sending to mate.

説明 フェールオーバー メッセージです。アクティブ装置からスタンバイ装置へのコンフィギュレーションの複製が開始されたときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

709004

エラー メッセージ %FWSM-1-709004: (Primary) End Configuration Replication (ACT)

説明 フェールオーバー メッセージです。アクティブ装置からスタンバイ装置へのコンフィギュレーションの複製が完了したときに表示されます。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

709005

エラー メッセージ %FWSM-1-709005: (Primary) Beginning configuration replication: Receiving from mate.

説明 スタンバイ Cisco ASA が、アクティブ Cisco ASA から複製コンフィギュレーションの最初の部分を受信したことを示しています。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

709006

エラー メッセージ %FWSM-1-709006: (Primary) End Configuration Replication (STB)

説明 フェールオーバー メッセージです。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。セカンダリ装置の場合には、(Primary) の代わりに (Secondary) と表示されます。

推奨処置 対処は不要です。

709007

エラー メッセージ %FWSM-2-709007: Configuration replication failed for command *command*

説明 フェールオーバー メッセージです。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かったときに表示されます。メッセージの最後に、障害の原因となったコマンドが表示されます。

推奨処置 コマンド名を書き留めて、TAC に連絡してください。

710001

エラー メッセージ %FWSM-7-710001: TCP access requested from *source_address/source_port* to *interface_name:dest_address/service*

説明 Cisco ASA に宛てられた最初の TCP パケットが TCP セッションの確立を要求したときに、このメッセージが表示されます。このパケットは、1 往復半ハンドシェイクの最初の SYN パケットです。該当するアクセス制御リスト (Telnet、HTTP、または SSH) によってパケットが許可された場合に、このメッセージが表示されます。ただし、SYN Cookie の確認はまだ完了しておらず、ステートは予約されていません。

推奨処置 対処は不要です。

710002

エラーメッセージ %FWSM-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、Cisco ASA に宛てられた 2 番目の TCP パケットが TCP セッションの確立を要求したときに、このメッセージが表示されます。このパケットは 1 往復半ハンドシェイクの最後の ACK です。該当するアクセス制御リスト (Telnet、HTTP、または SSH) によってパケットが許可された場合に、このメッセージが表示されます。また、SYN クッキーの確認が成功し、TCP セッション用にステートは予約済みです。

UDP 接続の場合、接続が許可されました。たとえば、許可された 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、その要求を処理すると、このメッセージ (サービスは SNMP) が表示されます。このメッセージは、10 秒で 1 回にレート制限されています。

推奨処置 対処は不要です。

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 セキュリティ アプライアンスがインターフェイス サービスへの接続の試みを拒否したときに、このメッセージが表示されます。たとえば、ファイアウォールが不正な SNMP 管理ステーションからの SNMP 要求を受信すると、このメッセージが表示される場合があります。

推奨処置 `show run http`、`show run ssh`、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かどうかを確認してください。このメッセージが頻繁に表示される場合には、攻撃の可能性があります。

710004

エラーメッセージ %FWSM-7-710004: TCP connection limit exceeded from
source_address/source_port to interface_name:dest_address/service

説明 サービスへの Cisco ASA の管理接続の最大数を超過しました。Cisco ASA は、管理サービスごとに最大 5 つの管理接続を同時に許可します。

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開放してください。

710005

エラー メッセージ %FWSM-7-710005: {TCP|UDP} request discarded from *source_address/source_port* to *interface_name:dest_address/service*

説明 UDP 要求を処理する UDP サーバが Cisco ASA がないときに、このメッセージが表示されます。TCP パケットが Cisco ASA 上のどのセッションにも属していない場合にも、このメッセージが表示されることがあります。また、許可されたホストからであっても、空白のペイロードを持つ SNMP 要求を Cisco ASA が受信した場合にも、このメッセージ(サービスは *snmp*)が表示されます。サービスが *snmp* である場合、ログ受信側の負荷を防止するため、このメッセージは最大で 10 秒に 1 回しか生成されません。

推奨処置 DHCP、RIP、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。このメッセージが異常に多く発生する場合には、攻撃の可能性ががあります。

710006

エラー メッセージ %FWSM-7-710006: *protocol* request discarded from *source_address* to *interface_name:dest_address*

説明 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、このメッセージが表示されます。たとえば、Cisco ASA が TCP または UDP 以外の IP パケットを受信し、Cisco ASA が要求を処理できない場合などです。

推奨処置 DHCP、RIP、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。このメッセージが異常に多く発生する場合には、攻撃の可能性ががあります。

711001

エラー メッセージ %FWSM-7-711001: *debug_trace_msg*

説明 ログ機能に関する logging debug-trace コマンドを入力したあとに、このシステム ログメッセージが表示されます。logging debug-trace をイネーブルにすると、すべてのデバッグメッセージがシステム 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か、またはセキュアな帯域外ネットワークで送信する必要があります。

推奨処置 対処は不要です。

711002

エラー メッセージ %FWSM-7-711002: Task ran for *elapsed_time* msec, process = *process_name*

説明 プロセスが 100 ミリ秒よりも長く CPU を使用しているときに、このメッセージが表示されます。このメッセージは、CPU を使用しているプロセスにフラグを付ける、デバッグ目的で使用されます。

推奨処置 対処は不要です。

713004

エラーメッセージ %FWSM-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface *interface num*, for Peer *IP_address* ignored

説明 Cisco ASA がトンネルの開始を試みているリモート エンティティから IKE パケットを受信したときに、このメッセージが表示されます。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、トンネルを確立することはできません。この IKE パケットは無視され、廃棄されます。

推奨処置 対処は不要です。

713006

エラーメッセージ %FWSM-5-713006: Failed to obtain state for message Id *message_number*, Peer Address: *IP_address*

説明 Cisco ASA が受信したメッセージ ID を認識していないことを表すメッセージです。メッセージ ID は、特定の IKE フェーズ 2 ネゴシエーションを識別する目的で使用されます。Cisco ASA にエラー条件が存在する可能性があります。2 つの IKE ピアが同期外れになっている場合もあります。

推奨処置 対処は不要です。

713008

エラーメッセージ %FWSM-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel

説明 ID ペイロードで受信したキー ID 値が、事前共有鍵認証を使用する、この IKE セッションのグループ名で認められる最大サイズよりも長いことを表すメッセージです。これは無効な値であり、セッションはリジェクトされます。Cisco ASA では、このサイズのグループ名を作成できないので、表示されるキー ID は使用できません。クライアント上の不正なグループ名を変更するように、ユーザに通知してください。

推奨処置 クライアントピア(最も可能性が高いのは Altiga RA クライアント)で有効なグループ名が指定されているかどうかを確認してください。現時点ではグループ名の最大長は 32 です。

713009

エラーメッセージ %FWSM-3-713009: OU in DN in ID payload too big for Certs IKE tunnel

説明 ID ペイロードで受信した DN の OU 値が、Certs 認証を使用する、この IKE セッションのグループ名で認められる最大サイズよりも長いことを表すメッセージです。この OU はスキップされ、別の OU または他の基準と一致するグループが検索されます。

推奨処置 Cisco ASA にグループのある OU をクライアントが使用するには、グループ名が有効な長さでなければなりません。現時点ではグループ名の最大長は 32 です。

713010

エラー メッセージ %FWSM-5-713010: IKE area: failed to find centry for message Id *message_number*

説明 一意のメッセージ ID によって conn_entry (IPSec SA に対応する IKE フェーズ 2 の構造) を検索する試みが失敗したときに、このメッセージが表示されます。内部構造が見つかりませんでした。セッションが標準外の方法で終了した場合に発生する可能性もありますが、最も考えられる原因は内部エラーです。

推奨処置 この問題が続く場合は、ピアを調べてください。

713012

エラー メッセージ %FWSM-3-713012: Unknown protocol (*protocol*). Not adding SA w/spi=*SPI value*

説明 ピアから不正な IPSec プロトコルまたはサポート対象外の IPSec プロトコルを受信したときに、このメッセージが表示されます。

推奨処置 ピアの ISAKMP フェーズ 2 コンフィギュレーションが Cisco ASA と互換であるかどうかを確認してください。

713014

エラー メッセージ %FWSM-3-713014: Unknown Domain of Interpretation (DOI): *DOI value*

説明 ピアから受信した ISAKMP Domain of Interpretation (DOI) がサポート対象外である場合に、このメッセージが表示されます。

推奨処置 ピアの ISAKMP DOI コンフィギュレーションを確認してください。

713016

エラー メッセージ %FWSM-3-713016: Unknown identification type, Phase 1 or 2, Type *ID_Type*

説明 ピアから受信した ID が不明の場合に、このメッセージが表示されます。この ID は未知の有効な ID の場合もありますが、無効な ID または壊れた ID の場合もあります。

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てください。

713017

エラー メッセージ %FWSM-3-713017: Identification type not supported, Phase 1 or 2, Type *ID_Type*

説明 ピアから受信したフェーズ 1 またはフェーズ 2 ID が、正当であってもサポート対象外であることを表すメッセージです。

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てください。

713018

エラーメッセージ %FWSM-3-713018: Unknown ID type during find of group name for certs, Type *ID_Type*

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713020

エラーメッセージ %FWSM-3-713020: No Group found by matching OU(s) from ID payload: *OU_value*

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713022

エラーメッセージ %FWSM-3-713022: No Group found matching *peer_ID* or *IP_address* for Pre-shared key peer *IP_address*

説明 ピアから指定された値（キー ID または IP アドレス）と同じ名前のグループがグループ データベースに存在しないことを表すメッセージです。

推奨処置 ピアのコンフィギュレーションを確認してください。

713024

エラーメッセージ %FWSM-7-713024: Received local Proxy Host data in ID Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がリモート ピアのフェーズ 2 ローカル プロキシ ID ペイロードを受信したことを表すメッセージです。

推奨処置 対処は不要です。

713025

エラーメッセージ %FWSM-7-713025: Received remote Proxy Host data in ID Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がリモート ピアのフェーズ 2 リモート プロキシ ID ペイロードを受信したことを表すメッセージです。

推奨処置 対処は不要です。

713026

エラーメッセージ %FWSM-7-713026: Transmitted local Proxy Host data in ID
Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がフェーズ2 ローカル プロキシ ID ペイロードを送信したことを表すメッセージです。

推奨処置 対処は不要です。

713027

エラーメッセージ %FWSM-7-713027: Transmitted remote Proxy Host data in ID
Payload: Address *IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がフェーズ2 リモート プロキシ ID ペイロードを送信したことを表すメッセージです。

推奨処置 対処は不要です。

713028

エラーメッセージ %FWSM-7-713028: Received local Proxy Range data in ID Payload:
Addresses *IP_address - IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がリモートピアのフェーズ2 ローカル プロキシ ID ペイロードを受信し、そのペイロードに IP アドレス範囲が含まれていたことを表すメッセージです。

推奨処置 対処は不要です。

713029

エラーメッセージ %FWSM-7-713029: Received remote Proxy Range data in ID Payload:
Addresses *IP_address - IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がリモートピアのフェーズ2 リモート プロキシ ID ペイロードを受信し、そのペイロードに IP アドレス範囲が含まれていたことを表すメッセージです。

推奨処置 対処は不要です。

713030

エラーメッセージ %FWSM-7-713030: Transmitted local Proxy Range data in ID
Payload: Addresses *IP_address - IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がフェーズ2 ローカル プロキシ ID ペイロードを送信したことを表すメッセージです。

推奨処置 対処は不要です。

713031

エラー メッセージ %FWSM-7-713031: Transmitted remote Proxy Range data in ID
Payload: Addresses *IP_address* - *IP_address*, Protocol *protocol*, Port *port*

説明 Cisco ASA がフェーズ2 リモート プロキシ ID ペイロードを送信したことを表すメッセージです。

推奨処置 対処は不要です。

713032

エラー メッセージ %FWSM-3-713032: Received invalid local Proxy Range *IP_address* - *IP_address*

説明 ローカル ID ペイロードに範囲 ID タイプが含まれていて、指定の下位アドレスが上位アドレスよりも小さくなかった場合に、このメッセージが表示されます。コンフィギュレーションの問題を表している可能性があります。

推奨処置 ISAKMP フェーズ2 パラメータの設定を確認してください。

713033

エラー メッセージ %FWSM-3-713033: Received invalid remote Proxy Range *IP_address* - *IP_address*

説明 リモート ID ペイロードに範囲 ID タイプが含まれていて、指定の下位アドレスが上位アドレスよりも小さくなかった場合に、このメッセージが表示されます。コンフィギュレーションの問題を表している可能性があります。

推奨処置 ISAKMP フェーズ2 パラメータの設定を確認してください。

713034

エラー メッセージ %FWSM-7-713034: Received local IP Proxy Subnet data in ID
Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 フェーズ2 ID ペイロードでローカル IP プロキシ サブネットのデータを受信したときに、このメッセージが表示されます。

推奨処置 対処は不要です。

713035

エラー メッセージ %FWSM-7-713035: Received remote IP Proxy Subnet data in ID
Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 フェーズ2 ID ペイロードでリモート IP プロキシ サブネットのデータを受信したときに、このメッセージが表示されます。

推奨処置 対処は不要です。

713036

エラー メッセージ %FWSM-7-713036: Transmitted local IP Proxy Subnet data in ID
Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 フェーズ 2 ID ペイロードでローカル IP プロキシ サブネットのデータを送信したときに、このメッセージが表示されます。

推奨処置 対処は不要です。

713037

エラー メッセージ %FWSM-7-713037: Transmitted remote IP Proxy Subnet data in ID
Payload: Address *IP_address*, Mask *netmask*, Protocol *protocol*, Port *port*

説明 フェーズ 2 ID ペイロードでリモート IP プロキシ サブネットのデータを送信したときに、このメッセージが表示されます。

推奨処置 対処は不要です。

713039

エラー メッセージ %FWSM-7-713039: Send failure: Bytes (*number*), Peer: *IP_address*

説明 内部ソフトウェア エラーが発生し、ISAKMP パケットを送信できなかった場合に、このメッセージが表示されます。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713040

エラー メッセージ %FWSM-7-713040: Could not find connection entry and can not
encrypt: msgid *message_number*

説明 内部ソフトウェア エラーが発生し、フェーズ 2 データ構造が見つからないことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713041

エラー メッセージ %FWSM-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 Cisco ASA がイニシエータとしてトンネルをネゴシエートしていることを表すメッセージです。

推奨処置 対処は不要です。

713042

エラーメッセージ %FWSM-3-713042: IKE Initiator unable to find policy: Intf *interface_number*, Src: *source_address*, Dst: *dest_address*

説明 IPSec 高速パスが IKE をトリガーするパケットを処理したけれども、IKE のポリシー検索が失敗したことを表すメッセージです。このエラーはタイミングに関連する可能性があります。IKE が開始要求を処理する前に、IKE をトリガーする ACL が削除されている可能性があります。この問題はほとんどの場合、自動的に解決されます。

説明 この状況が続く場合は、L2L コンフィギュレーションを確認してください。暗号マップに関連する ACL に特に注意してください。

713043

エラーメッセージ %FWSM-3-713043: Cookie/peer address *IP_address* session already in progress

説明 元のトンネルの進行中に、再び IKE がトリガーされたことを表すメッセージです。

推奨処置 対処は不要です。

713047

エラーメッセージ %FWSM-3-713047: Unsupported Oakley group: Group *Diffie-Hellman group*

説明 Cisco ASA が、リモートピアの提案する Diffie-Hellman グループをサポートしていないことを表すメッセージです。Diffie-Hellman グループは、フェーズ 1 で Diffie-Hellman キーを生成し、フェーズ 2 で Perfect Forward Secrecy (PFS) 用の Diffie-Hellman キーを生成します。

説明 ピアの Diffie-Hellman キーの設定を確認してください。また、Cisco ASA に対する提案が正しいかどうかを確認してください。

713048

エラーメッセージ %FWSM-3-713048: Error processing payload: Payload ID: *id*

説明 処理できないペイロードを持つパケットを受信したことを表すメッセージです。

推奨処置 この問題が続く場合は、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 %FWSM-5-713049: Security negotiation complete for *tunnel_type* type (*group_name*) Initiator/Responder, Inbound SPI = *SPI*, Outbound SPI = *SPI*

説明 IPSec トンネルの開始を表すメッセージです。

推奨処置 対処は不要です。

713050

エラー メッセージ %FWSM-5-713050: Connection terminated for peer *IP_address*.
Reason: *termination reason* Remote Proxy *IP_address*, Local Proxy *IP_address*

説明 IPSec トンネルの終了を表すメッセージです。

推奨処置 対処は不要です。

713051

エラー メッセージ %FWSM-3-713051: Terminating connection attempt: IPSEC not permitted for group (*group_name*)

説明 ユーザ、グループ、またはインターフェイス ポリシーによって IPSec トンネルが拒否されていることを表すメッセージです。

推奨処置 IPSec を使用するには、ポリシーで適切なトンネリング プロトコルを選択してください。

713052

エラー メッセージ %FWSM-7-713052: User (*user*) authenticated.

説明 リモート アクセス ユーザが認証されたことを表すメッセージです。

推奨処置 対処は不要です。

713056

エラー メッセージ %FWSM-3-713056: Tunnel rejected: SA (*SA_name*) not found for group (*group_name*)!

説明 IPSec SA が見つからなかったことを表すメッセージです。

推奨処置 リモート アクセス トンネルの場合、グループとユーザのコンフィギュレーションを調べ、ユーザ グループにトンネル 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てください。外部認証のユーザおよびグループの場合、返された認証アトリビュートを確認してください。

713059

エラー メッセージ %FWSM-3-713059: Tunnel Rejected: User (*user*) matched with group name, group-lock check failed.

説明 ユーザがトンネル グループとユーザ名に同じストリングを使用して認証を試みたことを表すメッセージです。

推奨処置 ユーザを認証するには、グループとユーザ名が異なっている必要があります。

713060

エラーメッセージ %FWSM-3-713060: Tunnel Rejected: User (*user*) not member of group (*group_name*), group-lock check failed.

説明 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表すメッセージです。

推奨処置 Cisco VPN クライアントと事前共有鍵を使用している場合は、クライアント上で設定されているグループが、Cisco ASA 上でそのユーザに対応付けられているグループと同じであるかどうかを確認してください。デジタル証明書を使用している場合は、証明書の OU フィールドでグループが指定されていなければ、ユーザはデフォルトでリモート アクセスのデフォルトグループに設定されます。

713061

エラーメッセージ %FWSM-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:*source_address*, Dst: *dest_address*!

説明 Cisco ASA が、メッセージで表示されるプライベート ネットワークまたはホストに関するセキュリティ ポリシー情報を見つけられなかったことを表すメッセージです。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 上のどの暗号 ACL ととも一致しません。最も考えられる原因は、設定の誤りです。

推奨処置 接続の両側で暗号 ACL の保護ネットワークの設定を調べ、イニシエータ上のローカル ネットワークがレスポンス上のリモート ネットワークであり、その逆も成り立っているかどうかを確認してください。ワイルドカード マスク、ホスト アドレスとネットワーク アドレスなどに特に注意してください。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 アドレスまたはレッド 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 %FWSM-3-713062: IKE Peer address same as our interface address *IP_address*

説明 IKE ピアとして設定されている IP アドレスが、Cisco ASA のいずれかの IP インターフェイス上で設定されている IP アドレスと同じです。

推奨処置 L2L の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てください。

713063

エラーメッセージ %FWSM-3-713063: IKE Peer address not configured for destination *IP_address*

説明 IKE ピアのアドレスが、L2L トンネルに設定されていないことを表すメッセージです。

推奨処置 L2L のコンフィギュレーションを確認してください。

713065

エラー メッセージ %FWSM-3-713065: IKE Remote Peer did not negotiate the following: *proposal attribute*

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713066

エラー メッセージ %FWSM-7-713066: IKE Remote Peer configured for SA: *SA_name*

説明 ピアの暗号ポリシー設定を表すメッセージです。

推奨処置 対処は不要です。

713068

エラー メッセージ %FWSM-5-713068: Received non-routine Notify message: *notify_type (notify_value)*

説明 このイベントの原因となった通知メッセージが、通知処理コードで明示的に処理されないことを表すメッセージです。

推奨処置 固有の理由情報を検証して、対処を決定してください。IKE ピア間の設定の不一致を表す、多くの通知メッセージがあります。

713072

エラー メッセージ %FWSM-3-713072: Password for user (*user*) too long, truncating to *number* characters

説明 ユーザのパスワードが長すぎることを表すメッセージです。

推奨処置 認証サーバ上でパスワードの長さを訂正してください。

713073

エラー メッセージ %FWSM-5-713073: Responder forcing change of *Phase 1/Phase 2* rekeying duration from *larger_value* to *smaller_value* seconds

説明 再キーイングの持続時間は、常に IKE ピアによって提案される値のうち小さい方の値に設定されます。このメッセージは、イニシエータの値が小さいことを表します。

推奨処置 対処は不要です。

713074

エラーメッセージ %FWSM-5-713074: Responder forcing change of IPSec rekeying duration from *larger_value* to *smaller_value* Kbs

説明 再キーイングの持続時間は、常に IKE ピアによって提案される値のうち小さい方の値に設定されます。このメッセージは、イニシエータの値が小さいことを表します。

推奨処置 対処は不要です。

713075

エラーメッセージ %FWSM-5-713075: Overriding Initiator's IPSec rekeying duration from *larger_value* to *smaller_value* seconds

説明 再キーイングの持続時間は、常に IKE ピアによって提案される値のうち小さい方の値に設定されます。このメッセージは、レスポンドの値が小さいことを表します。

推奨処置 対処は不要です。

713076

エラーメッセージ %FWSM-5-713076: Overriding Initiator's IPSec rekeying duration from *larger_value* to *smaller_value* Kbs

説明 再キーイングの持続時間は、常に IKE ピアによって提案される値のうち小さい方の値に設定されます。このメッセージは、レスポンドの値が小さいことを表します。

推奨処置 対処は不要です。

713078

エラーメッセージ %FWSM-2-713078: Temp buffer for building mode config attributes exceeded: bufsize *available_size*, used *value*

説明 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表すメッセージです。

推奨処置 不要なトンネル グループ アトリビュートをディセーブルにするか、または長すぎるテキストメッセージを短縮します。問題が解消されない場合は、エラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報およびコンフィギュレーション ファイルとともに Cisco TAC に提出して、指示を受けてください。

713081

エラー メッセージ %FWSM-3-713081: Unsupported certificate encoding type
encoding_type

説明 ロードされた証明書のいずれかが読み取り不可能であり、サポート対象外の符号化方式の可能性のあることを表すメッセージです。

推奨処置 デジタル証明書およびトラストポイントの設定を確認してください。

713082

エラー メッセージ %FWSM-3-713082: Failed to retrieve identity certificate

説明 このトンネルに関するアイデンティティ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設定を確認してください。

713083

エラー メッセージ %FWSM-3-713083: Invalid certificate handle

説明 このトンネルに関するアイデンティティ証明書が見つからなかったことを表すメッセージです。

推奨処置 デジタル証明書およびトラストポイントの設定を確認してください。

713084

エラー メッセージ %FWSM-3-713084: Received invalid phase 1 port value (*port*) in ID payload

説明 IKE フェーズ 1 ID ペイロードで受信したポート値が不正であることを表すメッセージです。許容可能な値は、0 または 500 (ISAKMP または IKE) です。

推奨処置 ピアが IKE 規格に準拠していないか、またはネットワークの問題によりパケットが壊れた可能性があります。

713085

エラー メッセージ %FWSM-3-713085: Received invalid phase 1 protocol (*protocol*) in ID payload

説明 IKE フェーズ 1 ID ペイロードで受信したプロトコル値が不正であることを表すメッセージです。許容可能な値は、0 または 17 (UDP) です。

推奨処置 ピアが IKE 規格に準拠していないか、またはネットワークの問題によりパケットが壊れた可能性があります。

713086

エラー メッセージ %FWSM-3-713086: Received unexpected Certificate payload
Possible invalid Auth Method (*Auth method (auth numerical value)*)

説明 証明書ペイロードを受信したにも関わらず、内部証明書ハンドルではアイデンティティ証明書がないと示されています。通常の登録方式で証明書ハンドルを取得しなかった可能性があります。考えられる理由の1つは、認証方式がRSA または DSS シグニチャでないことですが、双方の設定が誤っていれば IKE SA ネゴシエーションが失敗するはずです。

推奨処置 アプライアンスおよびピア上で、トラストポイントと ISAKMP の設定を確認してください。

713088

エラー メッセージ %FWSM-3-713088: Set Cert filehandle failure: no IPsec SA in
group *group_name*

説明 デジタル証明書の情報に基づいてトンネルグループを見つけることができませんでした。

推奨処置 トンネルグループがピアの証明書情報を処理するように、適切に設定されているかどうかを確認してください。

713092

エラー メッセージ %FWSM-5-713092: Failure during phase 1 rekeying attempt due to
collision

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 ほとんどの場合、悪性のイベントではありませんが、重大な影響がある場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713094

エラー メッセージ %FWSM-7-713094: Cert validation failure: handle invalid for
Main/Aggressive Mode Initiator/Responder!

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 トラストポイントを再登録しなければならない場合があります。問題が続く場合は、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713098

エラー メッセージ %FWSM-3-713098: Aborting: No identity cert specified in IPSec SA (*SA_name*)!

説明 証明書に基づく IKE セッションの確立が試みられましたが、暗号ポリシーでアイデンティティ証明書が指定されていないことを表すメッセージです。

推奨処置 ピアに送信するアイデンティティ証明書 / トラストポイントを指定してください。

713099

エラー メッセージ %FWSM-7-713099: Tunnel Rejected: Received NONCE length *number* is out of range!

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713102

エラー メッセージ %FWSM-3-713102: Phase 1 ID Data length *number* too long - reject tunnel!

説明 IKE が受信した ID ペイロードに含まれる Identification Data フィールドのサイズが 2K 以上だったことを表すメッセージです。

推奨処置 対処は不要です。

713103

エラー メッセージ %FWSM-7-713103: Invalid (NULL) secret key detected while computing hash

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713104

エラー メッセージ %FWSM-7-713104: Attempt to get Phase 1 ID data failed while *hash computation*

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713105

エラーメッセージ %FWSM-3-713105: Zero length data in ID payload received during phase 1 or 2 processing

説明 ピアが ID データのない ID ペイロードを送信したことを表すメッセージです。これは無効です。

推奨処置 ピアのコンフィギュレーションを確認してください。

713107

エラーメッセージ %FWSM-3-713107: IP_Address request attempt failed!

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713109

エラーメッセージ %FWSM-3-713109: Unable to process the received peer certificate

説明 Cisco ASA がリモート ピアから受信した証明書を処理できなかったことを表すメッセージです。証明書データのフォーマットが不正だった場合や、証明書のデータをアプライアンスが保存できなかった場合が考えられます。原因としては、たとえば 4096 ビットより大きいパブリック キー サイズなどがあります。

推奨処置 リモート ピア上で別の証明書を使用して、接続の再確立を試みてください。

713112

エラーメッセージ %FWSM-3-713112: Failed to process CONNECTED notify (SPI SPI_value) !

説明 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表すメッセージです。SPI を使用して IKE フェーズ 2 構造を見つけられなかった場合や、受信した ISAKMP ヘッダーで commit ビットが設定されていなかった場合が考えられます。後者の場合、IKE ピアが規格に準拠していない可能性があります。

推奨処置 問題が続く場合は、ピアのコンフィギュレーションを確認し、commit ビット処理をディセーブルにしてください。

713113

エラー メッセージ %FWSM-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: *IP_address*, SA address: *internal_SA_address*, tunnel count: *count*

説明 IKE SA が 0 以外のトンネル カウントで削除されたことを表すメッセージです。IKE SA のトンネル カウントが対応付けられた接続エントリとの同期を失ったか、または対応する接続エントリの cookie フィールドと、その接続エントリがポイントする IKE SA の cookie フィールドが同期を失ったことを意味します。この状況が発生すると、IKE SA および対応するデータ構造は解放されないで、データ構造をポイントしている可能性のあるエントリが古いポインタを使用することはありません。

推奨処置 対処は不要です。エラー回復が組み込まれています。

713114

エラー メッセージ %FWSM-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 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713115

エラー メッセージ %FWSM-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec

説明 Cisco ASA による、UDP 上での IPSec の使用の試みをクライアントがリジェクトしました。UDP 上の IPSec を使用すると、複数のクライアントが NAT デバイス経由で Cisco ASA への同時トンネルを確立できます。クライアントが要求をリジェクトした理由としては、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に設定されていないことが考えられます。

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てください。

713116

エラー メッセージ %FWSM-3-713116: Terminating connection attempt: L2TP-over-IPSEC attempted by group (*group_name*) but L2TP disabled

説明 ユーザまたはグループが L2TP-over-IPSec 接続を試みましたが、この Cisco ASA では L2TP プロトコルがイネーブルではありません。

推奨処置 L2TP のコンフィギュレーションを確認してください。

713117

エラー メッセージ %FWSM-7-713117: Received Invalid SPI notify (SPI *SPI_Value*)!

説明 SPI 値で表される IPsec SA が、リモートピア上でアクティブでなくなっていることを表すメッセージです。リモートピアがリブートまたはリセットされた可能性があります。

推奨処置 ピアに確立済みの適切な SA がなくなっていることを DPD が認識すれば、この問題は自動的に解消されるはずですが、DPD がイネーブルでない場合、該当するトンネルを手動で再確立する必要があります。

713118

エラー メッセージ %FWSM-3-713118: Detected invalid Diffie-Hellmann *group_descriptor* *group_number*, in IKE area

説明 *group_descriptor* フィールドにサポート対象外の値が含まれていることを表すメッセージです。現時点でサポートされているのは、グループ 1、2、5、7 だけです。conn-entry の場合、*group_descriptor* フィールドが 0 に設定され、Perfect Forward Secrecy (PFS) がディセーブルであることを表す場合もあります。

推奨処置 ピアの Diffie-Hellman の設定を確認してください。

713119

エラー メッセージ %FWSM-3-713119: PHASE 1 COMPLETED

説明 IKE フェーズ 1 が正常に終了した場合に表示されるメッセージです。

推奨処置 対処は不要です。

713120

エラー メッセージ %FWSM-5-713120: PHASE 2 COMPLETED (*msgid=msg_id*)

説明 IKE フェーズ 2 が正常に終了した場合に表示されるメッセージです。

推奨処置 対処は不要です。

713121

エラー メッセージ %FWSM-7-713121: Keep-alive type for this connection: *keepalive_type*

説明 このトンネルに使用されているキーブアライブメカニズムのタイプを表すメッセージです。

推奨処置 対処は不要です。

713122

エラー メッセージ %FWSM-3-713122: Keep-alives configured *keepalive_type* but peer *IP_address* support keep-alives (type = *keepalive_type*)

説明 このデバイスでキープアライブがオン（またはオフ）に設定されているにも関わらず、IKE ピアがキープアライブをサポートする（またはサポートしない）ことを表すメッセージです。

推奨処置 これが意図的である場合には、処置は不要です。意図的でない場合、両方のデバイスでキープアライブの設定を変更してください。

713123

エラー メッセージ %FWSM-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: *keepalive_type*)

説明 リモート IKE ピアが所定の時間内にキープアライブに回答しなかったために、IKE ピアとの接続が終了したことを表すメッセージです。使用されているキープアライブ メカニズムもメッセージで表示されます。

推奨処置 対処は不要です。

713124

エラー メッセージ %FWSM-3-713124: Received DPD sequence number *rcv_sequence_#* in DPD Action, description expected seq #

説明 リモート IKE ピアが送信した DPD に含まれるシーケンス番号が、予測されるシーケンス番号とは異なっていることを表すメッセージです。パケットは廃棄されます。

推奨処置 ネットワークにパケット損失の問題があることを表している可能性があります。

713127

エラー メッセージ %FWSM-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list

説明 ピアが XAUTH を実行しようとしたにも関わらず、Cisco ASA が XAUTH IKE プロポーザルを選択しなかった場合に、このメッセージが表示されます。

推奨処置 IKE プロポーザル リストで、IKE XAUTH プロポーザルのプライオリティを確認してください。

713128

エラーメッセージ %FWSM-3-713128: Connection attempt to VCPIP redirected to VCA peer *IP_address* via load balancing

説明 VCPIP への接続の試みが、ロードバランシングによって負荷の少ないピアにリダイレクトされた場合に、このメッセージが表示されます。

推奨処置 対処は不要です。

713129

エラーメッセージ %FWSM-3-713129: Received unexpected Transaction Exchange payload type: *payload_id*

説明 XAUTH または Mode-cfg の実行中に、予期しないペイロードを受信したことを表すメッセージです。2つのピアが同期外れになっているか、XAUTH または Mode-cfg のバージョンが一致していないか、またはリモートピアが適切な RFC に適合していない可能性があります。

推奨処置 各ピアのコンフィギュレーションを確認してください。

713130

エラーメッセージ %FWSM-5-713130: Received unsupported transaction mode attribute: *attribute_id*

説明 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) の要求をデバイスが受信したことを表すメッセージです。この状況は一般に、悪性ではありません。

推奨処置 対処は不要です。

713131

エラーメッセージ %FWSM-5-713131: Received unknown transaction mode attribute: *attribute_id*

説明 Cisco ASA が、認識しないトランザクションモードアトリビュート (XAUTH または Mode) の要求を受信したことを表すメッセージです。有効なアトリビュートでも現バージョンの config モードでサポートされていない場合や、ピアが独自仕様の無効な値を送信している場合が考えられます。接続に問題が生じることはありませんが、ピアの機能に影響する可能性があります。

推奨処置 対処は不要です。

713132

エラー メッセージ %FWSM-3-713132: Cannot obtain an *IP_address* for remote peer

説明 リモートアクセスクライアントのIPアドレスを提供する内部ユーティリティからのアドレス要求が、満たされなかったことを表すメッセージです。

推奨処置 IP アドレス割り当て方式の設定を確認してください。

713133

エラー メッセージ %FWSM-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でネゴシエートされたDHグループと異なります。

推奨処置 対処は不要です。

713134

エラー メッセージ %FWSM-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection

説明 設定されたLAN間プロポーザルが、LAN間の接続で認められるものではない場合に、このメッセージが表示されます。どちら側がイニシエータであるかに応じて、異なるプロポーザルが使用されます。

推奨処置 対処は不要です。

713135

エラー メッセージ %FWSM-5-713135: message received, redirecting tunnel to *IP_address*.

説明 リモート Cisco ASA 上でのロードバランシングによって、トンネルがリダイレクトされることを表すメッセージです。REDIRECT_CONNECTION 通知パケットを受信した場合に、このメッセージが表示されます。

推奨処置 対処は不要です。

713136

エラー メッセージ %FWSM-5-713136: IKE session establishment timed out [*IKE_state_name*], aborting!

説明 SA が非アクティブな状態でハンクしていることをリーパが検出しました。リーパはハンクしたSAの削除を試みます。

推奨処置 対処は不要です。

713137

エラー メッセージ %FWSM-5-713137: Reaper overriding refCnt [*ref_count*] and tunnelCnt [*tunnel_count*] -- deleting SA!

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713138

エラー メッセージ %FWSM-3-713138: Group *group_name* not found and BASE GROUP default preshared key not configured

説明 ピアの IP アドレスと同じ名前を持つグループが、グループ データベースに存在しない場合に表示されるメッセージです。Main モードでは、Cisco ASA はいずれかのデフォルト グループに設定されているデフォルトの事前共有鍵の使用を試みます。デフォルトの事前共有鍵が設定されていません。

推奨処置 事前共有鍵の設定を確認してください。

713139

エラー メッセージ %FWSM-5-713139: *group_name* not found, using BASE GROUP default preshared key

説明 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、グループ データベースに存在しません。Main モードでは、Cisco ASA はデフォルト グループに設定されているデフォルトの事前共有鍵の使用を試みます。

推奨処置 対処は不要です。

713140

エラー メッセージ %FWSM-3-713140: Split Tunneling Policy requires network list but none configured

説明 スプリット トンネリング ポリシーが、トンネリングを分割するかローカル LAN アクセスを許可するように設定されている場合に、このメッセージが表示されます。VPN クライアントが必要とする情報を表すため、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 の設定を確認してください。

713141

エラー メッセージ %FWSM-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 クライアントに搭載されている Cisco ASA が、設定上必要な Cisco ASA と一致しないことを表すメッセージです。このメッセージでは実際の値と必要な値がリストされ、トンネルが打ち切られるか許可されるかが示されます。

推奨処置 クライアントに別のパーソナル Cisco ASA を搭載するか、または Cisco ASA の設定を変更してください。

713142

エラー メッセージ %FWSM-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 クライアントが ModeCfg によって使用中の Cisco ASA を報告しない場合に、このメッセージが表示されます。このイベントでは、必要な値がリストされ、トンネルが打ち切られるか許可されるかが示されます。製品ストリングの後ろにある数値は、許可される全製品のビットマスクです。

推奨処置 クライアントに別のパーソナル Cisco ASA を搭載するか、または Cisco ASA の設定を変更してください。

713143

エラー メッセージ %FWSM-7-713143: Processing firewall record. Vendor: *vendor(id)*, Product: *product(id)*, Caps: *capability_value*, Version Number: *version_number*, Version String: *version_text*

説明 クライアントに搭載されている Cisco ASA に関するデバッグ情報を提供するメッセージです。

推奨処置 対処は不要です。

713144

エラー メッセージ %FWSM-5-713144: Ignoring received malformed firewall record; reason - *error_reason* TLV type *attribute_value* *correction*

説明 クライアントから不正な Cisco ASA 情報を受信したことを表すメッセージです。

推奨処置 クライアント上のパーソナル Cisco ASA の設定および Cisco ASA を確認してください。

713145

エラー メッセージ %FWSM-6-713145: Detected Hardware Client in network extension mode, adding static route for address: *IP_address*, mask: *netmask*

説明 ネットワーク拡張モードでハードウェアクライアントとのトンネルがネゴシエートされ、そのハードウェアクライアントの向こう側にあるプライベート ネットワークへのスタティック ルートが追加されることを表すメッセージです。これにより、Cisco ASA はそのリモート ネットワークを、ヘッドエンドのプライベート側にある全ルータに認識させることができます。

推奨処置 対処は不要です。

713146

エラー メッセージ %FWSM-3-713146: Could not add route for Hardware Client in network extension mode, address: *IP_address*, mask: *netmask*

説明 内部ソフトウェア エラーが発生したことを表すメッセージです。ネットワーク拡張モードでハードウェアクライアントとのトンネルがネゴシエートされ、そのハードウェアクライアントの向こう側にあるプライベート ネットワークへのスタティック ルートの追加が失敗しました。ルーティング テーブルが満杯であるか、アドレッシング エラーの可能性ががあります。

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713147

エラー メッセージ %FWSM-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: *IP_address*, mask: *netmask*

説明 ネットワーク拡張モードでハードウェアクライアントへのトンネルが削除され、そのハードウェアクライアントの向こう側にあるプライベート ネットワークへのスタティック ルートが削除されることを表すメッセージです。

推奨処置 対処は不要です。

713148

エラー メッセージ %FWSM-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: *IP_address*, mask: *netmask*

説明 ネットワーク拡張モードでハードウェアクライアントへのトンネルの削除中に、そのハードウェアクライアントの向こう側にあるプライベート ネットワークへのルートが削除できなかったことを表すメッセージです。

推奨処置 アドレッシングまたはソフトウェアに問題がある可能性があります。ルーティング テーブルを調べて、問題のルートがないことを確認してください。ルートがある場合、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ている場合に限り、そのルートを手動で削除してください。

713149

エラー メッセージ %FWSM-3-713149: Hardware client security attribute *attribute_name* was enabled but not requested.

説明 ヘッドエンドの Cisco ASA で、特定のハードウェア クライアントのセキュリティ アトリビュートがイネーブルと指定されているにも関わらず、VPN3002 ハードウェア クライアントがそのアトリビュートを要求していません。

推奨処置 ハードウェア クライアントの設定を確認してください。

713152

エラー メッセージ %FWSM-3-713152: Unable to obtain any rules from filter *ACL_tag* to send to client for CPP, terminating connection.

説明 クライアントが CPP を使用して自身の Cisco ASA をプロビジョニングする必要があるにも関わらず、ヘッドエンド デバイスがクライアントに送信すべき ACL を取得できなかったことを表すメッセージです。設定の誤りによるものと考えられます。

推奨処置 クライアントのグループ ポリシーで CPP に指定されている ACL を確認してください。

713154

エラー メッセージ %FWSM-4-713154: DNS lookup for *peer_description* Server [*server_name*] failed!

説明 特定のサーバに関する DNS 検索が解決されなかったことを表すメッセージです。

推奨処置 Cisco ASA 上の DNS サーバの設定を確認してください。さらに、DNS サーバが正常に動作していて、IP アドレス マッピングのホスト名があることを確認してください。

713155

エラー メッセージ %FWSM-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 サーバに関する前回の DNS ルックアップの失敗により、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。プライマリ サーバの以降の DNS 検索は最終的に成功し、バックアップ サーバが初期化されていてリセットされることを表すメッセージです。この時点よりあとに開始されたトンネルが、プライマリ サーバの目標となります。

推奨処置 対処は不要です。

713156

エラー メッセージ %FWSM-5-713156: Initializing Backup Server [*server_name* or *IP_address*]

説明 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するか、またはプライマリサーバに関する DNS 検索の失敗によりバックアップサーバが初期化されたことを表すメッセージです。この時点よりあとに開始されたトンネルが、指定のバックアップサーバの目標となります。

推奨処置 対処は不要です。

713157

エラー メッセージ %FWSM-4-713157: Timed out on initial contact to server [*server_name* or *IP_address*] Tunnel could not be established.

説明 クライアントが IKE MSG1 を送信してトンネルの開始を試みましたが、反対側の Cisco ASA から応答を受信しなかったことを表すメッセージです。バックアップサーバが使用可能であれば、クライアントはいずれかのバックアップサーバとの接続を試みます。

推奨処置 ヘッドエンドの Cisco ASA との接続を確認してください。

713158

エラー メッセージ %FWSM-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP

説明 クライアントが IPSec over TCP を使用するように設定されていることを表すメッセージです。このクライアントは、Cisco ASA が IPSec over UDP を使用する試みをリジェクトしました。

推奨処置 TCP が望ましい場合には、処置は不要です。そうでない場合は、クライアントの設定を確認してください。

713159

エラー メッセージ %FWSM-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access

説明 Cisco ASA サーバへの TCP 接続が、何らかの理由で切断されたことを表すメッセージです。考えられる原因としては、サーバのリポート、ネットワークの問題、SSL の不一致などがあります。

推奨処置 初期接続が行われたあとでサーバとの接続が切断された場合は、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。初期接続がただちに切断された場合は、SSL 認証に問題があると考えられます。

713160

エラー メッセージ %FWSM-7-713160: Remote user (session Id - *id*) has been granted access by the Firewall Server

説明 Cisco ASA サーバに対するリモート ユーザの認証が正常に行われたことを表すメッセージです。

推奨処置 対処は不要です。

713161

エラー メッセージ %FWSM-3-713161: Remote user (session Id - *id*) network access has been restricted by the Firewall Server

説明 Cisco ASA サーバが Cisco ASA に対し、このユーザを制限する必要があるという旨のメッセージを送信しました。理由としては、Cisco ASA ソフトウェアのアップグレード、アクセス権の変更などがあります。Cisco ASA サーバは処理が完了次第、このユーザをフル アクセスモードに戻します。

推奨処置 処置は不要ですが、ユーザがフル アクセス ステートにモードに戻されない場合は例外です。その場合には、Cisco ASA サーバを調べ、実行された処理およびリモート マシンで稼働中の Cisco ASA ソフトウェアの状態を確認してください。

713162

エラー メッセージ %FWSM-3-713162: Remote user (session Id - *id*) has been rejected by the Firewall Server

説明 Cisco ASA サーバがこのユーザをリジェクトしたことを表すメッセージです。

推奨処置 Cisco ASA サーバ上のポリシー情報を調べ、ユーザが正しく設定されているかどうかを確認してください。

713163

エラー メッセージ %FWSM-3-713163: Remote user (session Id - *id*) has been terminated by the Firewall Server

説明 Cisco ASA サーバがこのユーザ セッションを終了したことを表すメッセージです。クライアント マシン上でインテグリティ エージェントが動作を停止した場合、または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、このメッセージが表示されます。

推奨処置 クライアント マシンの Cisco ASA ソフトウェアが引き続き稼働していて、ポリシーが正しいかどうかを確認してください。

713164

エラー メッセージ %FWSM-7-713164: The Firewall Server has requested a list of active user sessions

説明 Cisco ASA サーバが古いデータを検出した場合、または(リポート時のように)セッションデータを失った場合に、このサーバがセッション情報を要求していることを表すメッセージです。

推奨処置 対処は不要です。

713165

エラー メッセージ %FWSM-3-713165: Client IKE Auth mode differs from the group's configured Auth mode

説明 クライアントのトンネル グループのポリシーがデジタル証明書を使用するように設定されているにも関わらず、クライアントが事前共有鍵を使用してネゴシエートしたことを表すメッセージです。

推奨処置 クライアントの設定を確認してください。

713166

エラー メッセージ %FWSM-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password

説明 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表すメッセージです。ユーザ名とパスワード、または認証サーバに問題があると考えられます。

推奨処置 双方に設定されているユーザ名とパスワードの値が一致しているかどうかを確認してください。また、ヘッドエンドの認証サーバが正常に動作しているかどうかを確認してください。

713167

エラー メッセージ %FWSM-3-713167: Remote peer has failed user authentication - check configured username and password

説明 リモート ユーザが拡張認証に失敗したことを表すメッセージです。ユーザ名とパスワード、または認証サーバに問題があると考えられます。

推奨処置 双方に設定されているユーザ名とパスワードの値が一致しているかどうかを確認してください。また、リモートの認証に使用されている認証サーバが正常に動作しているかどうかを確認してください。

713168

エラー メッセージ %FWSM-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!

説明 再キーイングに対する再認証がイネーブルに設定されているにも関わらず、トンネル認証に手動での介入が必要であることを表すメッセージです。

推奨処置 手動での介入が望ましい場合は、処置は不要です。そうでない場合は、対話型認証の設定を確認してください。

713169

エラー メッセージ %FWSM-7-713169: IKE Received delete for rekeyed SA IKE peer: *IP_address*, SA address: *internal_SA_address*, tunnelCnt: *tunnel_count*

説明 再キーイングが完了したあとで、IKE がリモートピアから古いIKE SA を削除する delete メッセージを受信したことを表すメッセージです。

推奨処置 対処は不要です。

713170

エラー メッセージ %FWSM-7-713170: IKE Received delete for rekeyed centry IKE peer: *IP_address*, centry address: *internal_address*, msgid: *id*

説明 フェーズ2再キーイングが完了したあとで、IKE がリモートピアから古いconn-entry を削除する delete メッセージを受信しました。

推奨処置 対処は不要です。

713171

エラー メッセージ %FWSM-7-713171: NAT-Traversal sending NAT-Original-Address payload

説明 フェーズ2で、UDP-Encapsulated-Transport が提案または選択されました。この場合、NAT-Traversal に対するこのペイロードを送信する必要があります。

推奨処置 対処は不要です。

713172

エラー メッセージ %FWSM-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 自動検出の結果です。

推奨処置 対処は不要です。

713174

エラー メッセージ %FWSM-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リングを試みていますが、ネットワーク拡張モードは認められていません。

推奨処置 ネットワーク拡張モードの設定を PAT モードと照らし合わせて確認してください。

713176

エラー メッセージ %FWSM-2-713176: *Device_type* memory resources are critical, IKE key acquire message on interface *interface_number*, for Peer *IP_address* ignored

説明 アプライアンスが、指定のピアへの IPSec トンネルをトリガーするデータを処理していることを表すイベントです。メモリ リソースがクリティカルな状態なので、これ以上のトンネルは開始できません。このデータ パケットは無視されて廃棄されています。

推奨処置 この状況が続く場合は、アプライアンスが効率的に設定されているかどうかを確認してください。このアプリケーション用には、メモリを増設したアプライアンスが必要であることを表している場合があります。

713177

エラー メッセージ %FWSM-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 ペイロードをピアから受信しました。

推奨処置 対処は不要です。

713178

エラー メッセージ %FWSM-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 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713179

エラー メッセージ %FWSM-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 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713182

エラー メッセージ %FWSM-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 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713184

エラー メッセージ %FWSM-6-713184: Client Type: *Client_type* Client Application Version: *Application_version_string*

説明 クライアントの OS およびアプリケーション バージョンを表すイベントです。この情報が入手できない場合には、N/A と表示されます。

推奨処置 対処は不要です。

713185

エラー メッセージ %FWSM-3-713185: Error: Username too long - connection aborted

説明 クライアントが返したユーザ名の長さが無効であり、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てください。

713186

エラー メッセージ %FWSM-3-713186: Invalid secondary domain name list received from the authentication server. List Received: *list_text* Character *index (value)* is illegal

説明 外部 RADIUS 認証サーバから、無効なセカンダリ ドメイン名リストを受信しました。スプリット トンネリングを使用している場合、このリストは、クライアントがトンネル経由で解決すべきドメインを表します。

推奨処置 RADIUS サーバ上の Secondary-Domain-Name-List アトリビュート (ベンダー固有アトリビュート 29) の指定を訂正してください。このリストは、コンマで区切ったドメイン名のリストでなければなりません。ドメイン名には、英数字、ハイフン、アンダースコア、およびピリオド以外の文字が含まれてはなりません。

713187

エラーメッセージ %FWSM-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 このトンネルの確立を試みた IKE ピアは、受信側のリモート サブネットにバインドされている ISAKMP コンフィギュレーションで設定されている IKE ピアではありません。

推奨処置 ヘッドエンドおよびピアの L2L 設定値が正しいかどうかを確認してください。

713189

エラーメッセージ %FWSM-3-713189: Attempted to assign network or broadcast *IP_address*, removing (*IP_address*) from pool.

説明 プールから取得した IP アドレスが、このサブネットのネットワーク アドレスまたはブロードキャスト アドレスです。このアドレスは使用不可能としてマークされます。

推奨処置 一般にこのエラーは悪性ではありませんが、IP アドレス プールの設定を確認する必要があります。

713190

エラーメッセージ %FWSM-7-713190: Got bad refCnt (*ref_count_value*) assigning *IP_address* (*IP_address*)

説明 この SA の参照カウンタが無効です。

推奨処置 この問題は自動的に解消されます。

713193

エラーメッセージ %FWSM-3-713193: Received packet with missing payload, Expected payload: *payload_id*

説明 アプライアンスが受信した、指定のエクステンジ タイプの暗号化 / 非暗号化パケットで、1 つまたは複数のペイロードが欠落していました。一般に、ピアに問題があることを表します。

推奨処置 ピアが有効な IKE メッセージを送信しているかどうかを確認してください。

713194

エラーメッセージ %FWSM-3-713194: IKE/IPSec Delete With Reason message: *termination_reason*

説明 delete メッセージを終了理由コード付きで受信しました。

推奨処置 対処は不要です。

713195

エラー メッセージ %FWSM-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!

説明 Originate Only のピアは、最初の P2 トンネルの確立後でないと、着信接続を受け入れられません。トンネルが確立されると、どの方向のデータでも、追加のフェーズ 2 トンネルを開始できます。

推奨処置 別の動作が望ましい場合は、Originate Only の設定を変更する必要があります。

713196

エラー メッセージ %FWSM-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。このピアは相手先として Answer Only のピアを必要としていますが、こちら側はそれに該当しません。設定の誤りと考えられます。

推奨処置 双方の L2L の設定を確認してください。

713197

エラー メッセージ %FWSM-5-713197: The configured Confidence Interval of *number* seconds is invalid for this *tunnel_type* connection. Enforcing the second default.

説明 グループに設定されている Confidence Interval が、有効な範囲外です。

推奨処置 グループの Confidence 設定を調べ、有効な範囲内であるかどうかを確認してください。

713198

エラー メッセージ %FWSM-3-713198: User Authorization failed: *user* User authorization failed.

説明 このイベントには、理由を表すストリングが含まれます。

推奨処置 グループの設定とクライアントの許可を確認してください。

713199

エラー メッセージ %FWSM-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (*counter_value*)!

説明 リーパが内部ソフトウェア エラーを訂正しました。

推奨処置 問題が続く場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713203

エラー メッセージ %FWSM-3-713203: IKE Receiver: Error reading from socket.

説明 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表すメッセージです。これは一般に内部エラーであり、ソフトウェアに問題があることを示している場合があります。

推奨処置 通常、この問題は悪性ではなく、システムは自動的に訂正されます。この問題が続く場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713204

エラー メッセージ %FWSM-7-713204: Adding static route for client address:
IP_address

説明 ピアに割り当てられたアドレス、またはハードウェア クライアントによって保護される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ました。

推奨処置 不要です。

713205

エラー メッセージ %FWSM-3-713205: Could not add static route for client address:
IP_address

説明 クライアントに割り当てられたアドレス、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、失敗しました。ルーティング テーブルでのルートの重複、または壊れたネットワーク アドレスが原因と考えられます。重複したルートの場合、ルートが正しくクリーンアップされていないか、または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可能性があります。

推奨処置 IP ローカル プールの設定と、その他に使用されている IP アドレス割り当てメカニズム（たとえば、DHCP または RADIUS）を確認してください。ルーティング テーブルからルートがクリアされているかどうかを確認してください。また、ピア システムでのネットワークおよびアドレスの設定も確認してください。

713206

エラー メッセージ %FWSM-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy

説明 グループ ポリシーで認められるトンネルが、トンネル グループの設定で認められるトンネルと異なるために、トンネルが廃棄されたときに表示されるメッセージです。

推奨処置 トンネル グループおよびグループ ポリシーの設定を確認してください。

713208

エラー メッセージ %FWSM-3-713208: Cannot create dynamic rule for Backup L2L entry *rule rule_id*

説明 IKE をトリガーし、IPSec データを正しく処理するための ACL の作成が失敗したことを表すメッセージです。このエラーは、バックアップ L2L の設定に固有のもので、設定エラー、キャパシティ エラー、または内部ソフトウェア エラーの可能性があり、

推奨処置 デバイスが最大数の Cisco ASA および最大数の VPN トンネルで稼働している場合、メモリの問題が考えられます。そうでない場合は、バックアップ L2L と暗号マップの設定（暗号マップに対応付けられた ACL）を確認してください。

713209

エラー メッセージ %FWSM-3-713209: Cannot delete dynamic rule for Backup L2L entry *rule id*

説明 IKE をトリガーし、IPSec データを正しく処理するための ACL の削除が失敗したことを表すメッセージです。このエラーは、バックアップ L2L の設定に固有のもので、内部ソフトウェア エラーの可能性があり、

推奨処置 このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713210

エラー メッセージ %FWSM-3-713210: Cannot create dynamic map for Backup L2L entry *rule_id*

説明 バックアップ L2L の設定に対応付けられたダイナミック暗号マップの実行時インスタンスの作成が失敗したことを表すメッセージです。設定エラー、キャパシティ エラー、または内部ソフトウェア エラーの可能性があり、

推奨処置 デバイスが最大数の Cisco ASA および最大数の VPN トンネルで稼働している場合、メモリの問題が考えられます。そうでない場合は、バックアップ L2L と暗号マップの設定（暗号マップに対応付けられた ACL）を確認してください。

713211

エラー メッセージ %FWSM-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 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へのルートを追加することを表すメッセージです。この場合のピアは、アドレスが不明なクライアントまたは L2L ピアです。どちらの場合にも、ダイナミック暗号マップを使用してトンネルが許可されます。

推奨処置 対処は不要です。

713212

エラーメッセージ %FWSM-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 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へのルートの追加に失敗したことを表すメッセージです。この場合のピアは、アドレスが不明なクライアントまたは L2L ピアです。どちらの場合にも、ダイナミック暗号マップを使用してトンネルが許可されます。ルートが重複している可能性があります。Cisco ASA のルーティング テーブルが満杯になっているか、以前使用したルートが削除されていない可能性があります。

推奨処置 ルーティング テーブルを調べ、ルートを追加する余地があるかどうか、古いルートが存在していないかどうかを確認してください。テーブルが満杯の場合、または古いルートが含まれている場合には、それらのルートを削除してやり直してください。この問題が続く場合は、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713213

エラーメッセージ %FWSM-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 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へのルートを削除することを表すメッセージです。この場合のピアは、アドレスが不明なクライアントまたは L2L ピアです。どちらの場合にも、ダイナミック暗号マップを使用してトンネルが許可されます。

推奨処置 対処は不要です。

713214

エラーメッセージ %FWSM-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: *IP_address*, mask: *netmask*

説明 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へのルートを削除中に、エラーが発生したことを表すメッセージです。この場合のピアは、アドレスが不明なクライアントまたは L2L ピアです。どちらの場合にも、ダイナミック暗号マップを使用してトンネルが許可されます。ルートがすでに削除されているか、または内部ソフトウェア エラーが発生している可能性があります。

推奨処置 ルートがすでに削除されている場合は、状況は悪性ではなく、デバイスは正常に機能します。問題が続く場合、または VPN トンネル経由でルーティングの問題につながる可能性がある場合は、VPN L2L 設定のルーティングおよびアドレッシングの部分を確認してください。リバースルートの入力と、該当する暗号マップに対応付けられた ACL を確認してください。この問題が続く場合は、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713215

エラー メッセージ %FWSM-6-713215: No match against Client Type and Version rules.
Client: *type version is/is not* allowed by default

説明 クライアントのタイプおよびバージョンが、Cisco ASA に設定されているどのルールにも一致しなかったことを表すメッセージです。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および展開上の要件を確認し、適切な変更を行ってください。

713216

エラー メッセージ %FWSM-5-713216: Rule: *action* Client type : *version* Client: *type version is/is not* allowed

説明 クライアントのタイプおよびバージョンが、いずれかのルールに一致したことを表すメッセージです。一致の結果およびルールが表示されます。

推奨処置 展開上の要件を確認し、適切な変更を行ってください。

713217

エラー メッセージ %FWSM-3-713217: Skipping unrecognized rule: action: *action* client type: *client_type* client version: *client_version*

説明 クライアントのタイプおよびバージョンに関するルールのフォーマットに誤りがあることを表すメッセージです。必要なフォーマットは、*action client type | client version action* であり、[permit] または [deny] の *client type* および *client version* が、Session Management に表示されます。パラメータごとに使用できるワイルドカード (*) は1つだけです。

推奨処置 ルールを訂正してください。

713218

エラー メッセージ %FWSM-3-713218: Tunnel Rejected: Client Type or Version not allowed.

説明 設定されているルールに従って、クライアントのアクセスがリジェクトされたことを表すメッセージです。

推奨処置 対処は不要です。

713219

エラーメッセージ %FWSM-6-713219: Queueing KEY-ACQUIRE messages to be processed when P1 SA is complete.

説明 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格納されたことを表すメッセージです。

推奨処置 対処は不要です。

713220

エラーメッセージ %FWSM-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.

説明 キューに格納されたフェーズ 2 メッセージを処理中であることを表すメッセージです。

推奨処置 対処は不要です。

713221

エラーメッセージ %FWSM-7-713221: Static Crypto Map check, checking map = *crypto_map_tag*, seq = *seq_number*...

説明 Cisco ASA が暗号マップを反復的に使用し、コンフィギュレーション情報を探していることを表すメッセージです。

推奨処置 対処は不要です。

713222

エラーメッセージ %FWSM-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 Cisco ASA が設定されている暗号マップを反復的に使用しても、対応する ACL との一致が見つからなかったことを表すメッセージです。一般に、ACL 設定の誤りを意味します。

推奨処置 このトンネルピアに対応付けられた ACL を調べ、VPN トンネルの両側とも適切なプライベートネットワークを指定しているかどうかを確認してください。

713223

エラーメッセージ %FWSM-7-713223: Static Crypto Map check, map = *crypto_map_tag*, seq = *seq_number*, no ACL configured

説明 このピアに対応付けられた暗号マップが、ACL にリンクされていないことを表すメッセージです。

推奨処置 この暗号マップに対応する ACL が存在していて、その 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かどうかを確認してください。

713224

エラー メッセージ %FWSM-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!

説明 この VPN トンネルに対応付けられた暗号マップで、重要な情報が欠落していることを表すメッセージです。

推奨処置 暗号マップが両方の VPN ピア、トランスフォーム セット、および対応する ACL を含めて、正しく設定されているかどうかを確認してください。

713225

エラー メッセージ %FWSM-7-713225: [IKEv1], Static Crypto Map check, map *map_name*, seq = *sequence_number* is a successful match

説明 Cisco ASA が、この VPN トンネルに一致する有効な暗号マップを見つけ出したことを表すメッセージです。

推奨処置 対処は不要です。

713226

エラー メッセージ %FWSM-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した場合、コンフィギュレーションにトラスト ポイントが指定されている必要があります。コンフィギュレーションにトラスト ポイントがない場合に、このメッセージが生成され、エラーが示されます。

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 デバイスの管理者が、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。

713229

エラー メッセージ %FWSM-5-713229: Auto Update - Notification to client *client_ip* of update string: *message_string*.

説明 VPN リモート アクセス クライアントに、最新のソフトウェアがダウンロード可能である旨が通知されたとき、このメッセージが表示されます。リモート クライアントのユーザが、クライアント アクセス ソフトウェアを更新する必要があります。

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たメッセージ テキスト

推奨処置 対処は不要です。

713236

エラー メッセージ %FWSM-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads :payload1 (payload1_len) + payload2 (payload2_len)...total length : tlen

説明 IKE が各種のメッセージを送受信したときに、このメッセージが表示されます。

次に、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 13 バイトのベンダー固有ペイロードのあるメッセージを受信したときの出力例を示します。

```
%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 対処は不要です。

713229

エラー メッセージ %FWSM-5-713229: Auto Update - Notification to client *client_ip* of update string: *message_string*.

説明 VPN リモート アクセス クライアントに、最新のソフトウェアがダウンロード可能である旨が通知されたとき、このメッセージが表示されます。リモート クライアントのユーザが、クライアント アクセス ソフトウェアを更新する必要があります。

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たメッセージ テキスト

推奨処置 対処は不要です。

エラー メッセージ

713900

エラー メッセージ %FWSM-7-713900:*Descriptive_event_string*.

説明 重大なイベントまたは障害を説明する、複数のテキスト スtring で構成される場合のあるメッセージです。

推奨処置 問題が続く場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

713901

エラー メッセージ %FWSM-7-713901:*Descriptive_event_string*.

説明 発生したエラーを説明する、複数のテキスト スtring で構成される場合のあるメッセージです。ヘッドエンドまたはリモート アクセス クライアントの設定が誤っている可能性があります。イベント スtring で、発生したエラーの詳細が示されます。

推奨処置 トラブルシューティングして、エラーの原因を特定しなければならない場合があります。両方のピアで *isakmp* および *crypto map* の設定を確認してください。

713902

エラー メッセージ %FWSM-3-713902 *Descriptive_event_string*

説明 エラーを説明する、複数のテキスト ストリングで構成される場合のあるシステム ログ メッセージです。ヘッドエンドまたはリモート アクセス クライアントの設定が誤っている可能性があります。

推奨処置 設定をトラブルシューティングして、エラーの原因を特定しなければならない場合があります。両方のピアで ISAKMP および暗号マップの設定を確認してください。

713903

エラー メッセージ %FWSM-4-713903:*Descriptive_event_string*.

説明 警告を表す、複数のテキスト ストリングで構成される場合のあるシステム ログ メッセージです。予期しないピアの動作（接続の切断など）によって発生することがあります。

推奨処置 メッセージのみです。

713904

エラー メッセージ %FWSM-5-713904:*Descriptive_event_string*.

説明 一般的なステータス情報を説明する、複数のテキスト ストリングで構成される場合のあるシステム ログ メッセージです。これらのメッセージは、発生したイベントの追跡に使用されます。

推奨処置 メッセージのみです。

713905

エラー メッセージ %FWSM-7-713905:*Descriptive_event_string*.

説明 一般的なステータス情報を説明する、複数のテキスト ストリングで構成される場合のあるシステム ログ メッセージです。これらのメッセージは、発生したイベントの追跡に使用されます。

推奨処置 メッセージのみです。

713906

エラー メッセージ %FWSM-7-713906: *debug_message*

説明 各種の VPN デバッグ イベントに使用されるメッセージです。

推奨処置 対処は不要です。このメッセージはデバッグ目的で提供されています。

714001

エラー メッセージ %FWSM-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 メッセージのみです。

714002

エラー メッセージ %FWSM-7-714002: IKE Initiator starting QM: msg id = *message_number*

説明 Cisco ASA がフェーズ 2 イニシエータとして、Quick モード エクスチェンジの最初のパケットを送信しました。

推奨処置 メッセージのみです。

714003

エラー メッセージ %FWSM-7-714003: IKE Responder starting QM: msg id = *message_number*

説明 Cisco ASA がフェーズ 2 レスポンドアとして、Quick モード エクスチェンジの最初のパケットを受信しました。

推奨処置 メッセージのみです。

714004

エラー メッセージ %FWSM-7-714004: IKE Initiator sending 1st QM pkt: msg id = *message_number*

説明 最初の Quick モード パケットのプロトコル デコード

推奨処置 メッセージのみです。

714005

エラー メッセージ %FWSM-7-714005: IKE Responder sending 2nd QM pkt: msg id = *message_number*

説明 2 番目の Quick モード パケットのプロトコル デコード

推奨処置 メッセージのみです。

714006

エラー メッセージ %FWSM-7-714006: IKE Initiator sending 3rd QM pkt: msg id = *message_number*

説明 3 番目の Quick モード パケットのプロトコル デコード

推奨処置 メッセージのみです。

714007

エラー メッセージ %FWSM-7-714007: IKE Initiator sending Initial Contact

説明 Cisco ASA が初期コンタクト ペイロードを作成して送信しました。

推奨処置 メッセージのみです。

714011

エラー メッセージ %FWSM-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 メッセージのみです。

715001

エラー メッセージ %FWSM-7-715001: *Descriptive statement*

説明 Cisco ASA に発生したイベントまたは問題を説明するメッセージです。

推奨処置 説明の内容によって処置が異なります。

715004

エラー メッセージ %FWSM-7-715004: subroutine *name()* Q Send failure: RetCode (*return_code*)

説明 メッセージをキューに格納しようとしたとき、内部エラーが発生したことを表すメッセージです。

推奨処置 ほとんどの場合、悪性ではありませんが、問題が続く場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715005

エラー メッセージ %FWSM-7-715005: subroutine *name()* Bad message code: Code (*message_code*)

説明 内部サブルーチンが不正なメッセージコードを受信したことを表すメッセージです。

推奨処置 ほとんどの場合、悪性ではありませんが、問題が続く場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715006

エラー メッセージ %FWSM-7-715006: IKE got SPI from key engine: SPI = *SPI_value*

説明 IKE サブシステムが IPSec から SPI 値を受信したことを表すメッセージです。

推奨処置 対処は不要です。

715007

エラー メッセージ %FWSM-7-715007: IKE got a KEY_ADD msg for SA: SPI = *SPI_value*

説明 IKE がトンネル ネゴシエーションを完了し、IPSec 用の適切な暗号化およびハッシュ キーを正常にロードしたことを表すメッセージです。

推奨処置 対処は不要です。

715008

エラー メッセージ %FWSM-7-715008: Could not delete SA *SA_address*, refCnt = *number*, caller = *calling_subroutine_address*

説明 コール側のサブルーチンが IPSec SA を削除できなかったことを表すメッセージです。参照カウントの問題を示している可能性があります。

推奨処置 このイベントの結果、古い SA の数が増える場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715009

エラー メッセージ %FWSM-7-715009: IKE Deleting SA: Remote Proxy *IP_address*, Local Proxy *IP_address*

説明 表示されるプロキシ アドレスを持つ SA が削除されたことを表すメッセージです。

推奨処置 対処は不要です。

715013

エラー メッセージ %FWSM-7-715013: Tunnel negotiation in progress for destination *IP_address*, discarding data

説明 IKE がこのデータ用のトンネルを確立中であることを表すメッセージです。トンネルが完全に確立されるまで、このトンネルで保護されるすべてのパケットが廃棄されます。

推奨処置 対処は不要です。

715019

エラー メッセージ %FWSM-7-715019: IKEGetUserAttributes: Attribute name = *name*

説明 Cisco ASA が処理している *modcfg* アトリビュートの名前および値のペアを表示するメッセージです。

推奨処置 対処は不要です。

715020

エラー メッセージ %FWSM-7-715020: construct_cfg_set: Attribute name = *name*

説明 Cisco ASA が送信している *modcfg* アトリビュートの名前および値のペアを表示するメッセージです。

推奨処置 対処は不要です。

715021

エラー メッセージ %FWSM-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

説明 フェーズ 1 の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) Quick モード処理が遅延することを表すメッセージです。

推奨処置 対処は不要です。

715022

エラー メッセージ %FWSM-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

説明 フェーズ 1 の処理が完了し、Quick モードが再開されたことを表すメッセージです。

推奨処置 対処は不要です。

715027

エラー メッセージ %FWSM-7-715027: IPSec SA Proposal # *chosen_proposal*, Transform # *chosen_transform* acceptable Matches global IPSec SA entry # *crypto_map_index*

説明 レスポンダが受信したペイロードから、指定の IPSec SA プロポーザルおよびトランスフォームが選択されたことを表すメッセージです。IKE ネゴシエーションに関する問題をデバッグするとき、このデータが役立ちます。

推奨処置 対処は不要です。

715028

エラー メッセージ %FWSM-7-715028: IKE SA Proposal # 1, Transform # *chosen_transform* acceptable Matches global IKE entry # *crypto_map_index*

説明 レスポンダが受信したペイロードから、指定の IKE SA トランスフォームが選択されたことを表すメッセージです。IKE ネゴシエーションに関する問題をデバッグするとき、このデータが役立ちます。

推奨処置 対処は不要です。

715033

エラー メッセージ %FWSM-7-715033: Processing CONNECTED notify (MsgId *message_number*)

説明 Cisco ASA が、通知タイプ CONNECTED (16384) の通知ペイロードを含むメッセージを処理中であることを表します。CONNECTED 通知は、commit bit 処理の終了に使用され、レスポンダからイニシエータに送信される 4 番めの全体的 Quick モード パケットに含まれています。

推奨処置 対処は不要です。

715034

エラー メッセージ %FWSM-7-715034: action IOS keep alive payload: proposal=*time 1/time 2* sec.

説明 キープアライブ ペイロード メッセージの送受信処理が実行中であることを表すメッセージです。

推奨処置 対処は不要です。

715035

エラー メッセージ %FWSM-7-715035: Starting IOS keepalive monitor: *seconds* sec.

説明 キープアライブ タイマーが、可変の秒数にわたってキープアライブ メッセージをモニターすることを表すメッセージです。

推奨処置 対処は不要です。

715036

エラー メッセージ %FWSM-7-715036: Sending keep-alive of type *notify_type* (seq number *number*)

説明 キープアライブ通知メッセージの送信が実行中であることを表すメッセージです。

推奨処置 対処は不要です。

715037

エラー メッセージ %FWSM-7-715037: Unknown IOS Vendor ID version: *major.minor.variance*

説明 このバージョンの IOS の機能が不明であることを表すメッセージです。

推奨処置 IKE キープアライブなどの機能にインターオペラビリティの問題がある可能性があります。このようなインターオペラビリティの問題に結びつく場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、IOS および Cisco ASA のソフトウェア バージョンも含めて、収集した情報とともに Cisco TAC に提出し、指示を受けてください。

715038

エラー メッセージ %FWSM-7-715038: action *Spoofing_information* Vendor ID payload (version: *major.minor.variance*, capabilities: *value*)

説明 IOS Vendor ID ペイロードの処理が実行されたことを表すメッセージです。実行中のメッセージは、IOS をスプーフィングする Altiga である可能性があります。

推奨処置 対処は不要です。

715039

エラー メッセージ %FWSM-7-715039: Unexpected cleanup of tunnel table entry during SA delete.

説明 IKE トンネル テーブルに、SA が解放された時点で削除されなかったエントリがあることを表すメッセージです。ステート マシンのバグを表します。

推奨処置 問題が続く場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715040

エラー メッセージ %FWSM-7-715040: Deleting active auth handle during SA deletion: handle = *internal_authentication_handle*

説明 SA の削除時に、認証ハンドルが引き続きアクティブであったことを表すメッセージです。これはエラー状況におけるクリーンアップ リカバリの一部分です。

推奨処置 対処は不要です。

715041

エラーメッセージ %FWSM-7-715041: Received keep-alive of type *keepalive_type*, not the negotiated type

説明 指定のタイプの予期しないキープアライブをメッセージで受信したことを表します。

推奨処置 両方のピアでキープアライブの設定を確認してください。

715042

エラーメッセージ %FWSM-7-715042: IKE received response of type *failure_type* to a request from the *IP_address* utility

説明 リモートアクセスクライアントの IP アドレスを提供する内部ユーティリティからのアドレス要求が、満たされなかったことを表します。このメッセージの変数のテキストで、より具体的な原因が示されます。

推奨処置 IP アドレス割り当ての設定を確認し、適切に調整してください。

715044

エラーメッセージ %FWSM-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability

説明 ベンダーからの IOS キープアライブ ペイロードに、KA 機能が設定されていませんでした。ペイロードは無視されます。

推奨処置 メッセージのみです。

715045

エラーメッセージ %FWSM-7-715045: ERROR: malformed Keepalive payload

説明 受信したキープアライブ ペイロードのフォーマットが不正です。ペイロードは無視されます。

推奨処置 メッセージのみです。

715046

エラーメッセージ %FWSM-7-715046: constructing *payload_description* payload

説明 作成中の IKE ペイロードに関する詳細情報を表示します。

推奨処置 メッセージのみです。

715047

エラー メッセージ %FWSM-7-715047: processing *payload_description* payload

説明 受信して処理中の IKE ペイロードに関する詳細情報を表示します。

推奨処置 メッセージのみです。

715048

エラー メッセージ %FWSM-7-715048: Send *VID_type* VID

説明 送信された Vendor ID ペイロードのタイプを表示します。

推奨処置 メッセージのみです。

715049

エラー メッセージ %FWSM-7-715049: Received *VID_type* VID

説明 受信した Vendor ID ペイロードのタイプを表示します。

推奨処置 メッセージのみです。

715050

エラー メッセージ %FWSM-7-715050: Claims to be IOS but failed authentication

説明 IOS VID と似ていますが、*hmac_sha* が一致しません。

推奨処置 両方のピアでベンダー ID の設定を確認してください。この問題によってインターオペラビリティに問題が生じる場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715051

エラー メッセージ %FWSM-7-715051: Received unexpected TLV type *TLV_type* while processing FWTYPE ModeCfg Reply

説明 FWTYPE ModeCfg 応答の処理中に、不明の TLV を Cisco ASA レコードで受信しました。これは廃棄されます。原因としては、パケットが壊れている場合、または接続先クライアントがサポートする Cisco ASA プロトコルのバージョンが新しい場合が考えられます。

推奨処置 Cisco VPN Client にインストールされているパーソナル FW と、Cisco ASA 上のパーソナル FW の設定を確認してください。VPN Client と Cisco ASA のバージョンが一致していない場合もあります。

715052

エラーメッセージ %FWSM-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries

説明 古い P1 SA を削除していますが、移行すべき新しい SA にも削除のマークが付けられているので、新しい SA に移行できません。一般に、2 つの IKE ピアが同期外れになっていて、それぞれ異なる再キーイング時間を使用している可能性があります。この問題は自動的に解消されますが、新しい P1 SA が再確立されるまで、わずかなデータ損失が生じることがあります。

推奨処置 メッセージのみです。

715053

エラーメッセージ %FWSM-7-715053: MODE_CFG: Received request for *attribute_info!*

説明 指定の属性を要求する、モード設定メッセージを受信しました。

推奨処置 メッセージのみです。

715054

エラーメッセージ %FWSM-7-715054: MODE_CFG: Received *attribute_name* reply: *value*

説明 リモートピアからモード設定応答メッセージを受信しました。

推奨処置 メッセージのみです。

715055

エラーメッセージ %FWSM-7-715055: Send *attribute_name*

説明 リモートピアにモード設定メッセージを送信しました。

推奨処置 メッセージのみです。

715056

エラーメッセージ %FWSM-7-715056: Client is configured for *TCP_transparency*

説明 リモート側（クライアント）に IPsec Over TCP が設定されているので、ヘッドエンドの Cisco ASA はクライアントと 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 トンネルが確立されない場合、いずれかのピアの NAT 透過性の設定を調整しなければなりません。そうでない場合、これは情報メッセージです。

715057

エラー メッセージ %FWSM-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 モードの設定情報が交換できません。

推奨処置 メッセージのみです。

715058

エラー メッセージ %FWSM-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.

説明 NAT-Traversal VID を交換したあと、リモート側が NAT トラバーサルに必要な 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 このエラーは NAT-T 実装への不適合を表している場合があります。問題のピアがシスコ製品の場合、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、製品番号およびソフトウェア バージョンも含めて、収集した情報とともに Cisco TAC に提出し、指示を受けてください。問題のピアがシスコ製品でない場合は、製造元のテクニカル サポートに連絡してください。

715059

エラー メッセージ %FWSM-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には、SA で定義されている通常のトランスポートおよびトンネル モードではなく、これらのモードを使用する必要があります。

推奨処置 メッセージのみです。

715060

エラー メッセージ %FWSM-7-715060: Dropped received IKE fragment. Reason: *reason*

説明 フラグメントが廃棄された理由が表示されます。

推奨処置 廃棄の理由によって異なりますが、中間にある NAT デバイスの問題または不適合のピアを示している可能性があります。

715061

エラー メッセージ %FWSM-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.

説明 同じパケットを別の MTU にフラグメント化して再送信した場合と、まったく別のパケットの場合があります。

推奨処置 メッセージのみです。

715062

エラー メッセージ %FWSM-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 ネットワークに問題があることを示している可能性があります。この状況によってトンネルが切断されたり、ある種のピアが Cisco ASA とネゴシエートできない場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、製品番号およびソフトウェア バージョンも含めて、収集した情報とともに Cisco TAC に提出し、指示を受けてください。

715063

エラー メッセージ %FWSM-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!

説明 フラグメント化された状態で受信したパケットの組み立てが成功しました。

推奨処置 メッセージのみです。

715064

エラー メッセージ %FWSM-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いて IKE フラグメンテーションをサポートします。

推奨処置 メッセージのみです。

715065

エラー メッセージ %FWSM-7-715065: IKE *state_machine subtype* FSM error history (struct *data_structure_address*) *state, event: state/event pairs*

説明 フェーズ 1 エラーが発生し、*state*、*event* のヒストリ ペアが時間をさかのぼる順序で表示されます。

推奨処置 ほとんどの場合、悪性のエラーではありません。望ましくない動作に関連してこれらのメッセージが表示される場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715066

エラー メッセージ %FWSM-7-715066: Can't load an IPsec SA! The corresponding IKE SA contains an invalid logical ID.

説明 IKE SA の論理 ID がヌルです。フェーズ 2 ネゴシエーションが打ち切られます。

推奨処置 内部エラーが発生しました。デバイスが回復して正常に動作しない場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715067

エラー メッセージ %FWSM-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa

説明 確立しようとしている LAN-TO-LAN SA は、すでに存在しています。つまり、同じリモート ネットワークでピアの異なる SA が存在します。この設定は無効なので、新しい SA は削除されます。

推奨処置 対応するすべてのピアで、LAN-TO-LAN の設定を確認してください。具体的には、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 %FWSM-7-715068: QM IsRekeyed: duplicate sa found by *address*, deleting old sa

説明 確立しようとしているリモート アクセス SA は、すでに存在しています。つまり、同じリモート ネットワークでピアの異なる SA が存在します。単にピアの IP アドレスが変更された可能性があるため、古い SA は削除されます。

推奨処置 クライアント トンネルが急に終了した場合は特に、悪性の状況ではありません。望ましくない動作に関連してこのメッセージが表示される場合は、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715069

エラー メッセージ %FWSM-7-715069: Invalid ESP SPI size of *SPI_size*

説明 受信した IPSec SA プロポーザルに、無効な ESP SPI サイズが指定されています。このプロポーザルはスキップされます。

推奨処置 一般に悪性の状況ではありませんが、ピアが不適合の可能性もあります。問題が続き、ピアが正常にトンネルをネゴシエートできない場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715070

エラー メッセージ %FWSM-7-715070: Invalid IPComp SPI size of *SPI_size*

説明 受信した IPSec SA プロポーザルに、無効な IPComp SPI サイズが指定されています。このプロポーザルはスキップされます。

推奨処置 一般に悪性の状況ではありませんが、ピアが不適合の可能性もあります。問題が続き、ピアが正常にトンネルをネゴシエートできない場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715071

エラー メッセージ %FWSM-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せん。

推奨処置 メッセージのみです。

715072

エラー メッセージ %FWSM-7-715072: Received proposal with unknown protocol ID *protocol_ID*

説明 受信した IPSec SA プロポーザルに、不明のプロトコル ID が指定されています。このプロポーザルはスキップされます。

推奨処置 一般に悪性の状況ではありませんが、ピアが不適合の可能性もあります。問題が続き、ピアが正常にトンネルをネゴシエートできない場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715074

エラー メッセージ %FWSM-7-715074: Could not retrieve authentication attributes for peer *IP_address*

説明 リモート ユーザに関する許可情報を取得できませんでした。

推奨処置 認証および許可の設定がすべて正しいかどうかを確認してください。問題が続き、ピアが正常にトンネルをネゴシエートできない場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

715075

エラー メッセージ %FWSM-7-715075: Group = *group_name*, Username = *client*, IP = *IP_address*
Received keep-alive of type *message_type* (seq number *number*)

説明 この新しいメッセージは、DPD 送信メッセージを記録する 715036 [DPD R-U-THERE] メッセージとペアになっています。

次の2つのケースがあります。

- 1) ピアが送信した [DPD R-U-THERE] メッセージを受信した場合
- 2) ピアが応答した [DPD R-U-THERE-ACK] メッセージを受信した場合

次の点を確認してください。

ケース1 [DPD R-U-THERE] を受信し、そのシーケンス番号は発信した DPD 応答メッセージの番号と一致しています。

f1 がピアから [DPD R-U-THERE] を受信せずに [DPD R-U-THERE-ACK] を送信した場合、セキュリティ違反の可能性があります。

ケース2 受信した [DPD R-U-THERE-ACK] メッセージのシーケンス番号は、直前に送信した DPD メッセージの番号と一致しています。

f1 がピアに [DPD R-U-THERE] を送信したあと、適当な時間内に [DPD R-U-THERE-ACK] を受信できなかった場合、トンネルがダウンしてい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 対処は不要です。

715076

エラー メッセージ %FWSM-7-715076: Computing hash for ISAKMP

説明 IKE が各種のハッシュ値を計算した場合に表示されます。

このオブジェクトは次のように前置されます。

Group = *groupname*, Username = *username*, IP = *ip_address*, ...

推奨処置 対処は不要です。

715077

エラー メッセージ %FWSM-7-715077: Pitcher: *msg string*, *spi spi*

説明 IKE に各種のメッセージが送信された場合に表示されます。

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

他の ISAKMP と同様、次の説明が適用されます。

このオブジェクトは次のように前置されます。

Group = *groupname*, Username = *username*, IP = *ip_address*, ...

推奨処置 対処は不要です。

717001

エラー メッセージ %FWSM-3-717001: Querying keypair failed.

説明 登録要求で、必要なキーペアが見つかりませんでした。

推奨処置 トラストポイントの設定に、有効なキーペアが存在するかどうかを確認し、登録をもう一度サブミットしてください。

717002

エラー メッセージ %FWSM-3-717002: Certificate enrollment failed for trustpoint *trustpoint_name*. Reason: *reason_string*.

説明 この *trustpoint_name* トラストポイントへの登録要求が失敗しました。

trustpoint name 登録要求の対象となった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 失敗の理由に応じて、CA サーバを確認してください。

717003

エラー メッセージ %FWSM-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関して、CA から証明書を正常に受信しました。

推奨処置 対処は不要です。

717004

エラー メッセージ %FWSM-6-717004: PKCS #12 export failed for trustpoint *trustpoint_name*.

説明 トラストポイント *trustpoint_name* がエクスポートに失敗しました。CA 証明書しか存在せず、トラストポイントのアイデンティティ証明書が存在しないか、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 トラストポイントに関して、必要な証明書とキーペアが存在するかどうかを確認してください。

717005

エラー メッセージ %FWSM-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 対処は不要です。

717006

エラー メッセージ %FWSM-6-717006: PKCS #12 import failed 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完全性を調べ、**pkcs12** レコード全体を正しくペーストしているかどうかを確認して、もう一度インポートしてください。

717007

エラー メッセージ %FWSM-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 対処は不要です。

717008

エラー メッセージ %FWSM-2-717008: Insufficient memory to *process_requiring_memory*.

説明 *process_requiring_memory* へのメモリの割り当て中に、内部エラーが発生しました。他のプロセスのメモリ割り当てに問題が生じ、処理が不可能になる可能性があります。

推奨処置 メモリに関する統計情報およびログを収集してデバッグしたあと、システムをリロードしてください。

717009

エラー メッセージ %FWSM-3-717009: Certificate validation failed. Reason: *reason_string*.

説明 証明書の確認が、*reason_string* で示される理由によって失敗しました。*reason_string* は、エラーの理由を表し、無効になった証明書を確認しようとした場合や、証明書のアトリビュートが無効な場合、または設定の問題が考えられます。

reason_string 証明書の確認が失敗した理由

推奨処置 *reason_string* で適切なトラストポイントが見つからない旨が示された場合は、確認のための有効なトラストポイントが設定されているかどうかを調べてください。システム時刻を調べ、CA 時刻に対して正確かどうかを確認してください。*reason_string* を確認し、指摘された問題を訂正してください。

717010

エラー メッセージ %FWSM-3-717010: CRL polling failed for trustpoint *trustpoint_name*.

説明 Certificate Revocation List (CRL) ポーリングが失敗し、CRL チェックが必要な場合、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 設定されている CRL ディストリビューション ポイントとの接続を調べ、手動での CRL 取得も正常に動作するかどうかを確認してください。

717011

エラー メッセージ %FWSM-2-717011: Unexpected event *event event_ID*

説明 正常な状況下では予想外のイベントが発生したことを表すログ メッセージです。

推奨処置 問題を記録し、Cisco TAC に連絡してください。

717012

エラー メッセージ %FWSM-3-717012: Failed to refresh CRL cache entry from the server for trustpoint *trustpoint_name* at *time_of_failure*

説明 指定のトラストポイント *trustpoint_name* で、指定の時刻 *time_of_failure* に、キャッシュに格納された CRL エントリの更新が失敗したことを表すログ メッセージです。システム上で CRL が古くなっているために、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 サーバとの接続について、ネットワークのダウン、サーバのダウンなども含めて確認してください。crypto ca crl retrieve コマンドを使用して、CRL を手動で取得してください。

717013

エラー メッセージ %FWSM-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デバイスを設定している場合、接続のたびに CRL をダウンロードしなくても済むように、CRL をメモリにキャッシュすることができます。キャッシュが満杯になり着信した CRL を格納できない場合、必要なスペースを作るために古い CRL が削除されます。このログ イベントは、CRL を削除するたびに生成されます。

推奨処置 対処は不要です。

717014

エラー メッセージ %FWSM-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デバイスを設定している場合、接続のたびに CRL をダウンロードしなくても済むように、CRL をメモリにキャッシュすることができます。受信した CRL が大きすぎてキャッシュに格納できない場合、このログ イベントが生成されます。

推奨処置 対処は不要です。容量の大きい CRL は引き続きサポートされていますが、キャッシュには格納できません。このような CRL は、IPSec 接続のたびにダウンロードすることになります。その結果、IPSec 接続がバーストしたときに、パフォーマンスに影響が及ぶ可能性があります。

717015

エラー メッセージ %FWSM-3-717015: CRL received from *issuer* is too large to process (CRL size = *crl_size*, maximum CRL size = *max_crl_size*)

説明 IPSec 接続によって、許容される CRL の最大サイズ *max_crl_size* を超えた CRL がダウンロードされる場合に、このログ イベントが生成されます。これは接続の失敗を引き起こすエラー条件です。このメッセージは、10 秒で 1 回にレート制限されています。

推奨処置 CRL による無効の確認方式の最大の欠点は、スケーラビリティです。この問題を解決するには、CA ベース ソリューションを検証して CRL のサイズを小さくするか、または CRL での確認を必要としないようにデバイスを設定するしかありません。

717016

エラー メッセージ %FWSM-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デバイスを設定している場合、接続のたびに CRL をダウンロードしなくても済むように、CRL をメモリにキャッシュすることができます。CA が期限切れの時刻を指定している場合、または設定されたキャッシュ時間が経過して CRL がキャッシュから削除された場合に、このログ イベントが生成されます。

推奨処置 対処は不要です。このイベントは定期的に発生します。

717017

エラー メッセージ %FWSM-3-717017: Failed to query CA certificate for trustpoint *trustpoint_name* from *enrollment_url*

説明 CA に CA 証明書を要求し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可能性があるエラーです。

推奨処置 このトラストポイントに登録 URL が設定されていることを確認し、CA サーバとの接続を確認して、要求をやり直してください。

717018

エラー メッセージ %FWSM-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 IPSec 接続によって、サポート可能な数より多い無効エントリを含む CRL がダウンロードされた場合に、このログ イベントが生成されます。これは接続の失敗を引き起こすエラー条件です。このメッセージは、10 秒で 1 回にレート制限されています。

issuer CRL 発行元の X.500 名

number_of_entries 受信した CRL に含まれる無効エントリの数

max_allowed デバイスがサポートしている CRL エントリの最大数

推奨処置 CRL による無効の確認方式の最大の欠点は、スケーラビリティです。この問題を解決するには、CA ペース ソリューションを検証して CRL のサイズを小さくするか、または CRL での確認を必要としないようにデバイスを設定するしかありません。

717019

エラー メッセージ %FWSM-3-717019: Failed to insert CRL for trustpoint *trustpoint_name*. Reason: *failure_reason*.

説明 取得した CRL が無効であり、*failure_reason* で示される理由により、キャッシュに格納できない場合に生成されるログ イベントです。

trustpoint_name CRL を要求したトラストポイントの名前

failure_reason CRL をキャッシュに格納できない理由

推奨処置 現在のシステム時刻が CA 時刻に対して正確であるかどうかを確認してください。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てください。

717022

エラー メッセージ %FWSM-6-717022 Certificate was successfully validated. *certificate identifiers*

説明 指定の証明書の確認が成功したときに表示されるメッセージです。

certificate identifiers 確認に成功した証明書の情報。理由、シリアル番号、件名などが含まれる場合があります。

推奨処置 対処は不要です。

717025

エラー メッセージ %FWSM-7-717025 Validating certificate chain containing *number of certs* certificate(s).

説明 一連の証明書を確認中に表示されるメッセージです。

number of certs 一連の証明書の数

推奨処置 対処は不要です。

717028

エラー メッセージ %FWSM-6-717028 Certificate chain was successfully validated *additional info*.

説明 一連の証明書の確認が成功したときに表示されるメッセージです。

additional info 一連の証明書を確認した方法についての情報を提供します。たとえば [with warning] の場合、CRL チェックは実行されていません。

推奨処置 対処は不要です。

717029

エラー メッセージ %FWSM-7-717029 Identified client certificate within certificate chain. serial number: *serial_number*, subject name: *subject_name*.

説明 クライアント証明書であることが判明した証明書を表すメッセージです。

serial_number クライアント証明書として識別された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た証明書に含まれる件名

推奨処置 対処は不要です。

718001

エラーメッセージ %FWSM-7-718001: Internal interprocess communication queue send failure: code *error_code*

説明 VPNLB キューにメッセージを格納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。

推奨処置 ほとんどの場合、悪性ではありませんが、問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718002

エラーメッセージ %FWSM-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。新しいピアは無視されます。

推奨処置 ロードバランシングおよびネットワークの設定を確認し、LB ピア数が許容される最大数を超過しないようにしてください。

718003

エラーメッセージ %FWSM-6-718003: Got unknown peer message *message_number* from *IP_address*, local version *version_number*, remote version *version_number*

説明 いずれかの LB ピアから、認識されないロードバランシングメッセージを受信しました。ピア間でバージョンが一致していない可能性があります。最も考えられる原因は、内部ソフトウェア エラーです。

推奨処置 すべての LB ピアが互換であるかどうかを確認してください。互換であるにも関わらず、問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718004

エラーメッセージ %FWSM-6-718004: Got unknown internal message *message_number*

説明 不明の内部メッセージを受信しました。一般に、内部ソフトウェア エラーを表します。

推奨処置 ほとんどの場合、悪性ではありませんが、問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718005

エラー メッセージ %FWSM-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。ネットワークの問題または内部ソフトウェア エラーの可能性があまりありません。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718006

エラー メッセージ %FWSM-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。内部ソフトウェア エラーの可能性があまりありません。

推奨処置 ほとんどの場合、悪性ではありませんが、問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718007

エラー メッセージ %FWSM-5-718007: Socket open failure *failure_code*

説明 ロードバランシング ソケットをオープンしようとしたときに、エラーが発生しました。ネットワークの問題または内部ソフトウェア エラーの可能性があまりありません。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718008

エラー メッセージ %FWSM-5-718008: Socket bind failure *failure_code*

説明 ロードバランシング ソケットへのバインドを試みたときに、エラーが発生しました。ネットワークの問題または内部ソフトウェア エラーの可能性があまりありません。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718009

エラー メッセージ %FWSM-5-718009: Send HELLO response failure to *IP_address*

説明 いずれかの LB ピアに Hello 応答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。ネットワークの問題または内部ソフトウェア エラーの可能性あります。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718010

エラー メッセージ %FWSM-5-718010: Sent HELLO response to *IP_address*

説明 セキュリティ アプライアンスが LB ピアに Hello 応答メッセージを送信しました。

推奨処置 メッセージのみです。

718011

エラー メッセージ %FWSM-5-718011: Send HELLO request failure to *IP_address*

説明 いずれかの LB ピアに Hello 要求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。ネットワークの問題または内部ソフトウェア エラーの可能性あります。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718012

エラー メッセージ %FWSM-5-718012: Sent HELLO request to *IP_address*

説明 セキュリティ アプライアンスが LB ピアに Hello 要求メッセージを送信しました。

推奨処置 メッセージのみです。

718013

エラー メッセージ %FWSM-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 ピアのステータスを調べ、ネットワーク接続を確認してください。

718014

エラー メッセージ %FWSM-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 ピアのステータスを調べ、ネットワーク接続を確認してください。

718015

エラー メッセージ %FWSM-5-718015: Received HELLO request from *IP_address*

説明 セキュリティ アプライアンスが LB ピアから Hello 要求メッセージを受信しました。

推奨処置 メッセージのみです。

718016

エラー メッセージ %FWSM-5-718016: Received HELLO response from *IP_address*

説明 セキュリティ アプライアンスが LB ピアから Hello 応答パケットを受信しました。

推奨処置 メッセージのみです。

718017

エラー メッセージ %FWSM-7-718017: Got timeout for unknown peer *IP_address* msg type *message_type*

説明 セキュリティ アプライアンスが不明のピアについて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、このメッセージは無視されています。

推奨処置 このメッセージが続く場合や、望ましくない結果を引き起こす場合には、LB ピアを調べ、すべてのピアが正しく設定されているかどうかを確認してください。

718018

エラー メッセージ %FWSM-7-718018: Send KEEPALIVE request failure to *IP_address*

説明 いずれかの LB ピアにキープアライブ要求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。ネットワークの問題または内部ソフトウェア エラーの可能性がります。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718019

エラー メッセージ %FWSM-7-718019: Sent KEEPALIVE request to *IP_address*

説明 セキュリティ アプライアンスが LB ピアにキープアライブ要求メッセージを送信しました。

推奨処置 メッセージのみです。

718020

エラー メッセージ %FWSM-7-718020: Send KEEPALIVE response failure to *IP_address*

説明 いずれかの LB ピアにキープアライブ応答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。ネットワークの問題または内部ソフトウェア エラーの可能性あります。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718021

エラー メッセージ %FWSM-7-718021: Sent KEEPALIVE response to *IP_address*

説明 セキュリティ アプライアンスが LB ピアにキープアライブ応答メッセージを送信しました。

推奨処置 メッセージのみです。

718022

エラー メッセージ %FWSM-7-718022: Received KEEPALIVE request from *IP_address*

説明 セキュリティ アプライアンスが LB ピアからキープアライブ要求メッセージを受信しました。

推奨処置 メッセージのみです。

718023

エラー メッセージ %FWSM-7-718023: Received KEEPALIVE response from *IP_address*

説明 セキュリティ アプライアンスが LB ピアからキープアライブ応答メッセージを受信しました。

推奨処置 メッセージのみです。

718024

エラー メッセージ %FWSM-5-718024: Send CFG UPDATE failure to *IP_address*

説明 いずれかの LB ピアにコンフィギュレーション アップデート 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。ネットワークの問題または内部ソフトウェア エラーの可能性あります。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718025

エラー メッセージ %FWSM-7-718025: Sent CFG UPDATE to *IP_address*

説明 セキュリティ アプライアンスが LB ピアにコンフィギュレーション アップデート メッセージを送信しました。

推奨処置 メッセージのみです。

718026

エラー メッセージ %FWSM-7-718026: Received CFG UPDATE from *IP_address*

説明 セキュリティ アプライアンスが LB ピアからコンフィギュレーション アップデート メッセージを受信しました。

推奨処置 メッセージのみです。

718027

エラー メッセージ %FWSM-6-718027: Received unexpected KEEPALIVE request from *IP_address*

説明 メッセージのみです。

推奨処置 問題が続く場合や、望ましくない動作を引き起こす場合には、すべての LB ピアが正しく設定され、正常に検出されているかどうかを確認してください。

718028

エラー メッセージ %FWSM-5-718028: Send OOS indicator failure to *IP_address*

説明 いずれかの LB ピアに OOS Indicator 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。ネットワークの問題または内部ソフトウェア エラーの可能性あります。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718029

エラー メッセージ %FWSM-7-718029: Sent OOS indicator to *IP_address*

説明 セキュリティ アプライアンスが LB ピアに OOS Indicator メッセージを送信しました。

推奨処置 メッセージのみです。

718030

エラー メッセージ %FWSM-6-718030: Received planned OOS from *IP_address*

説明 セキュリティ アプライアンスが LB ピアから計画された OOS メッセージを受信しました。

推奨処置 メッセージのみです。

718031

エラー メッセージ %FWSM-5-718031: Received OOS obituary for *IP_address*

説明 セキュリティ アプライアンスが LB ピアから OOS Obituary を受信しました。

推奨処置 メッセージのみです。

718032

エラー メッセージ %FWSM-5-718032: Received OOS indicator from *IP_address*

説明 セキュリティ アプライアンスが LB ピアから OOS Indicator を受信しました。

推奨処置 メッセージのみです。

718033

エラー メッセージ %FWSM-5-718033: Send TOPOLOGY indicator failure to *IP_address*

説明 いずれかの LB ピアにトポロジー インジケータ 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。ネットワークの問題または内部ソフトウェア エラーの可能性がります。

推奨処置 セキュリティ アプライアンスのネットワーク ベースの設定を調べ、インターフェイスがアクティブで、プロトコル データがデバイスに伝達されているかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718034

エラー メッセージ %FWSM-7-718034: Sent TOPOLOGY indicator to *IP_address*

説明 セキュリティ アプライアンスが LB ピアにトポロジー インジケータ メッセージを送信しました。

推奨処置 メッセージのみです。

718035

エラー メッセージ %FWSM-7-718035: Received TOPOLOGY indicator from *IP_address*

説明 セキュリティ アプライアンスが LB ピアからトポロジー インジケータ メッセージを受信しました。

推奨処置 メッセージのみです。

718036

エラー メッセージ %FWSM-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する必然性があったかどうかを確認してください。必然性がない場合、ピアの LB 設定を調べ、ピアとセキュリティ アプライアンスの間のネットワーク接続を確認してください。

718037

エラー メッセージ %FWSM-6-718037: Master processed *number_of_timeouts* timeouts

説明 マスター ロールのセキュリティ アプライアンスが、指定の回数のピア タイムアウトを処理しました。

推奨処置 タイムアウトが妥当かどうかを確認してください。妥当でない場合、ピアの LB 設定を調べ、ピアとセキュリティ アプライアンスの間のネットワーク接続を確認してください。

718038

エラー メッセージ %FWSM-6-718038: Slave processed *number_of_timeouts* timeouts

説明 スレーブ ロールのセキュリティ アプライアンスが、指定の回数のピア タイムアウトを処理しました。

推奨処置 タイムアウトが妥当かどうかを確認してください。妥当でない場合、ピアの LB 設定を調べ、ピアとセキュリティ アプライアンスの間のネットワーク接続を確認してください。

718039

エラー メッセージ %FWSM-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 ピアの検出が妥当かどうかを確認してください。妥当でない場合、ピアの LB 設定を調べ、ピアとセキュリティ アプライアンスの間のネットワーク接続を確認してください。

718040

エラー メッセージ %FWSM-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、エクスチェンジ ID は認識できませんでした。

推奨処置 メッセージのみです。

718041

エラー メッセージ %FWSM-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、その処理でコールバックを使用しませんでした。

推奨処置 メッセージのみです。

718042

エラー メッセージ %FWSM-5-718042: Unable to ARP for *IP_address*

説明 セキュリティ アプライアンスがピアとの接続を試みたときに、ARP 障害が発生しました。

推奨処置 ネットワークが正常に動作していて、すべてのピアが相互に通信可能であるかどうかを確認してください。

718043

エラー メッセージ %FWSM-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、削除しました。

推奨処置 メッセージのみです。

718044

エラー メッセージ %FWSM-5-718044: Deleted peer *IP_address*

説明 セキュリティ アプライアンスが LB ピアを削除しました。

推奨処置 メッセージのみです。

718045

エラー メッセージ %FWSM-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 メッセージのみです。

718046

エラー メッセージ %FWSM-7-718046: Create group policy *policy_name*

説明 セキュリティ アプライアンスが、LB ピアと安全に通信するためのグループ ポリシーを作成しました。

推奨処置 メッセージのみです。

718047

エラー メッセージ %FWSM-7-718047: Fail to create group policy *policy_name*

説明 セキュリティ アプライアンスが LB ピア間の通信を保護するグループ ポリシーの作成中に、エラーが発生しました。

推奨処置 LB の設定を確認してください。

718048

エラー メッセージ %FWSM-5-718048: Create of secure tunnel failure for 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 トンネルを確立中に、エラーが発生しました。

推奨処置 LB の設定が正しく、ネットワークが正常に動作しているかどうかを確認してください。

718049

エラー メッセージ %FWSM-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 メッセージのみです。

718050

エラー メッセージ %FWSM-5-718050: Delete of secure tunnel failure for 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 トンネルを終了中に、エラーが発生しました。

推奨処置 LB の設定が正しく、ネットワークが正常に動作しているかどうかを確認してください。

718051

エラー メッセージ %FWSM-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 メッセージのみです。

718052

エラー メッセージ %FWSM-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するマスターから根拠のない ARP を受信しました。

推奨処置 LB の設定を調べ、ネットワークが正常に動作しているかどうかを確認してください。

718053

エラー メッセージ %FWSM-5-718053: Detected duplicate master, mastership stolen
MAC_address

説明 セキュリティ アプライアンスがマスターの重複を検出しました。マスターシップが盗まれています。

推奨処置 LB の設定を調べ、ネットワークが正常に動作しているかどうかを確認してください。

718054

エラー メッセージ %FWSM-5-718054: Detected duplicate master *MAC_address* and going
to SLAVE

説明 セキュリティ アプライアンスがマスターの重複を検出し、スレーブ モードに切り替えました。

推奨処置 LB の設定を調べ、ネットワークが正常に動作しているかどうかを確認してください。

718055

エラー メッセージ %FWSM-5-718055: Detected duplicate master *MAC_address* and staying
MASTER

説明 セキュリティ アプライアンスがマスターの重複を検出し、スレーブ モードを続けています。

推奨処置 LB の設定を調べ、ネットワークが正常に動作しているかどうかを確認してください。

718056

エラー メッセージ %FWSM-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 メッセージのみです。

718057

エラーメッセージ %FWSM-5-718057: Queue send failure from ISR, msg type *failure_code*

説明 割り込みサービス ルーティングからメッセージを VPNLB キューに格納しようとしたとき、内部ソフトウェア エラーが発生しました。

推奨処置 ほとんどの場合、悪性ではありませんが、問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718058

エラーメッセージ %FWSM-7-718058: State machine return code: *action_routine*, *return_code*

説明 このイベントは、LB 有限ステート マシンに属するアクション ルーチンのリターン コードを追跡します。

推奨処置 メッセージのみです。

718059

エラーメッセージ %FWSM-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 有限ステート マシンのイベントおよびステートを追跡します。

推奨処置 メッセージのみです。

718060

エラーメッセージ %FWSM-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返し、ソケットを読み取れませんでした。内部ソフトウェア エラーの可能性がります。

推奨処置 問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718061

エラーメッセージ %FWSM-5-718061: Inbound socket read fail: context=*context_ID*.

説明 選択コールを通じてデータを検出したあと、ソケットの読み取りが失敗しました。内部ソフトウェア エラーの可能性がります。

推奨処置 問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718062

エラー メッセージ %FWSM-5-718062: Inbound thread is awake (context=*context_ID*).

説明 LB プロセスが起動して処理を開始するたびに表示されます。

推奨処置 メッセージのみです。

718063

エラー メッセージ %FWSM-5-718063: Interface *interface_name* is down.

説明 LB プロセスでインターフェイスがダウンしていることが検出されました。

推奨処置 インターフェイスの設定を調べ、このインターフェイスが正常に動作しているかどうかを確認してください。

718064

エラー メッセージ %FWSM-5-718064: Admin. interface *interface_name* is down.

説明 LB プロセスで管理インターフェイスがダウンしていることが検出されました。

推奨処置 管理インターフェイスの設定を調べ、このインターフェイスが正常に動作しているかどうかを確認してください。

718065

エラー メッセージ %FWSM-5-718065: Cannot continue to run (public=*up/down*, private=*up/down*, enable=*LB_state*, master=*IP_address*, session=*Enable/Disable*).

説明 全部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表すメッセージです。前提条件は、2つのアクティブインターフェイスおよびLBがイネーブルであることです。

推奨処置 インターフェイスの設定を調べ、少なくとも2つのインターフェイスが正常に動作しているかどうかを確認してください。また、LBの設定も確認してください。

718066

エラー メッセージ %FWSM-5-718066: Cannot add secondary address to interface *interface_name*, ip *IP_address*.

説明 LB では、外部インターフェイスへのセカンダリアドレスの追加が必要です。このイベントは、セカンダリアドレスを追加するときにエラーが発生したことを表します。

推奨処置 セカンダリアドレスとして使用しているアドレスを調べ、有効な一意のアドレスであるかどうかを確認してください。外部インターフェイスの設定を確認してください。

718067

エラーメッセージ %FWSM-5-718067: Cannot delete secondary address to interface *interface_name*, ip *IP_address*.

説明 セカンダリ アドレスを削除できませんでした。アドレッシングの問題または内部ソフトウェア エラーの可能性がります。

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、有効な一意のセカンダリ アドレスであるかどうかを確認してください。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラーメッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718068

エラーメッセージ %FWSM-5-718068: Start VPN Load Balancing in context *context_ID*.

説明 LB プロセスが起動され初期化されました。

推奨処置 メッセージのみです。

718069

エラーメッセージ %FWSM-5-718069: Stop VPN Load Balancing in context *context_ID*.

説明 LB プロセスが停止しました。

推奨処置 メッセージのみです。

718070

エラーメッセージ %FWSM-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 メッセージのみです。

718071

エラーメッセージ %FWSM-5-718071: Terminate VPN Load Balancing in context *context_ID*.

説明 LB プロセスが終了しました。

推奨処置 メッセージのみです。

718072

エラー メッセージ %FWSM-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 メッセージのみです。

718073

エラー メッセージ %FWSM-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 メッセージのみです。

718074

エラー メッセージ %FWSM-5-718074: Fail to create access list for peer *context_ID*.

説明 ACL を使用して、LB ピアが通信できるセキュア トンネルを作成します。セキュリティ アプライアンスが、いずれかの ACL を作成できませんでした。アドレッシングの問題または内部ソフトウェアの問題の可能性がります。

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確認し、すべてのピアが正しく検出されるようにします。問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718075

エラー メッセージ %FWSM-5-718075: Peer *IP_address* access list not set.

説明 セキュア トンネルを削除するとき、対応する ACL のないピア エントリをセキュリティ アプライアンスが検出しました。

推奨処置 メッセージのみです。

718076

エラー メッセージ %FWSM-5-718076: Fail to create tunnel group for peer *IP_address*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護するトンネル グループの作成中に、エラーが発生しました。

推奨処置 LB の設定を確認してください。

718077

エラー メッセージ %FWSM-5-718077: Fail to delete tunnel group for peer *IP_address*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護するトンネル グループの削除中に、エラーが発生しました。

推奨処置 メッセージのみです。

718078

エラー メッセージ %FWSM-5-718078: Fail to create crypto map for peer *IP_address*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護する暗号マップの作成中に、エラーが発生しました。

推奨処置 LB の設定を確認してください。

718079

エラー メッセージ %FWSM-5-718079: Fail to delete crypto map for peer *IP_address*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護する暗号マップの削除中に、エラーが発生しました。

推奨処置 メッセージのみです。

718080

エラー メッセージ %FWSM-5-718080: Fail to create crypto policy for peer *IP_address*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護するトランスフォーム セットの作成中に、エラーが発生しました。内部ソフトウェアの問題の可能性があります。

推奨処置 問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718081

エラー メッセージ %FWSM-5-718081: Fail to delete crypto policy for peer *IP_address*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護するトランスフォーム セットの削除中に、エラーが発生しました。

推奨処置 メッセージのみです。

718084

エラー メッセージ %FWSM-5-718084: Public/cluster IP not on the same subnet:
public *IP_address*, mask *netmask*, cluster *IP_address*

説明 クラスタの 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内でなければなりません。このイベントは、同じネットワークでないことを表します。

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 アドレスが同じネットワークにあるかどうかを確認してください。

718085

エラー メッセージ %FWSM-5-718085: Interface *interface_name* has no IP address defined.

説明 指定のインターフェイスに IP アドレスがありません。

推奨処置 インターフェイスの IP アドレスを設定してください。

718086

エラー メッセージ %FWSM-5-718086: Fail to install LB NP rules: type *rule_type*, dst *interface_name*, port *port*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護する SoftNP ACL ルールの作成中に、エラーが発生しました。内部ソフトウェアの問題の可能性があります。

推奨処置 問題が続く場合や、望ましくない動作を引き起こす場合には、このエラー メッセージをコンソールまたはシステム ログに出力されたとおりにコピーし、収集した情報とともに Cisco TAC に提出して、指示を受けてください。

718087

エラー メッセージ %FWSM-5-718087: Fail to delete LB NP rules: type *rule_type*, rule *rule_ID*.

説明 セキュリティ アプライアンスが LB ピア間の通信を保護する SoftNP ACL ルールの削除中に、エラーが発生しました。

推奨処置 メッセージのみです。

718088

エラー メッセージ %FWSM-7-718088: Possible VPN LB misconfiguration. Offending device MAC *MAC_address*.

説明 マスターが重複しています。いずれかの LB ピアの設定が誤っている可能性があります。

推奨処置 すべてのピアの LB 設定を確認してください。特に、指定のピアに注意してください。

719001

エラー メッセージ %FWSM-6-719001: Email Proxy session could not be established: session limit of *maximum_sessions* has been reached.

説明 最大セッション数の制限に達したため、着信 E メール プロキシ セッションを確立できなかったことを表すメッセージです。 *maximum_sessions* が最大セッション数です。

推奨処置 対処は不要です。

719002

エラー メッセージ %FWSM-3-719002: Email Proxy session *pointer* from *source_address* has been terminated due to *reason* error.

説明 セッションがエラーのために終了したことを表すメッセージです。考えられるエラーとしては、セッション データベースにセッションを追加できなかった場合、メモリ割り当てが失敗した場合、チャンネルへのデータの書き込みが失敗した場合などがあります。 *pointer* はセッション構造のポインタ、 *source_address* は E メール プロキシ クライアントの IP アドレス、 *reason* はエラーのタイプです。

推奨処置 対処は不要です。

719003

エラー メッセージ %FWSM-6-719003: Email Proxy session *pointer* resources have been freed for *source_address*.

説明 セッションの終了後に、動的に割り当てられたセッション構造が解放され、NULL に設定されたことを表すメッセージです。 *pointer* はセッション構造のポインタ、 *source_address* は E 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 対処は不要です。

719004

エラー メッセージ %FWSM-6-719004: Email Proxy session *pointer* has been successfully established for *source_address*.

説明 新しい着信 E 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 対処は不要です。

719005

エラー メッセージ %FWSM-7-719005: FSM *NAME* has been created using *protocol* for session *pointer* from *source_address*.

説明 新しい着信セッション用に FSM が作成されたことを表すメッセージです。 *NAME* はセッションの FSM インスタンス名、 *protocol* は E メール プロトコル タイプ (POP3、IMAP、SMTP など)、 *pointer* はセッション構造のポインタ、 *source_address* は E 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 対処は不要です。

719006

エラー メッセージ %FWSM-7-719006: Email Proxy session *pointer* has timed out for *source_address* because of network congestion.

説明 ネットワーク輻輳のため、E メール クライアントまたは E メール サーバにデータを送信できないことを表すメッセージです。ブロック タイマーが起動されます。このタイマーがタイムアウトすると、セッションが期限切れになります。 *pointer* はセッション構造のポインタ、 *source_address* は E 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 2 ~ 3 分後に操作をやり直してください。

719007

エラー メッセージ %FWSM-7-719007: Email Proxy session *pointer* cannot be found for *source_address*.

説明 セッション データベースで一致するセッションが見つからない場合に表示されるメッセージです。セッション ポインタが不正です。 *pointer* はセッション構造のポインタ、 *source_address* は E 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 対処は不要です。

719008

エラー メッセージ %FWSM-3-719008: Email Proxy service is shutting down.

説明 E メール プロキシがディセーブルの場合に表示されるメッセージです。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します。

推奨処置 対処は不要です。

719009

エラー メッセージ %FWSM-7-719009: Email Proxy service is starting.

説明 E メール プロキシがイネーブルの場合に表示されるメッセージです。

推奨処置 対処は不要です。

719010

エラー メッセージ %FWSM-6-719010: *protocol* Email Proxy feature is disabled on interface *interface_name*.

説明 CLI から起動された特定のエントリ ポイントで、E メール プロキシ機能がディセーブルになったときに表示されるメッセージです。これはユーザ用の主要な「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をオフにすると、メイン シャットダウン ルーチンが起動され、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 E メール プロトコル プロキシのタイプ (POP3、IMAP、SMTP など)、*interface_name* はセキュリティ アプライアンスのインターフェイス名です。

推奨処置 対処は不要です。

719011

エラー メッセージ %FWSM-6-719011: *Protocol* Email Proxy feature is enabled on interface *interface_name*.

説明 CLI から起動された特定のエントリ ポイントで、E メール プロキシ機能がイネーブルになったときに表示されるメッセージです。これはユーザ用の主要な「オン」スイッチです。メイン スタートアップ ルーチンでこのスイッチを初めて使用した時点で、グローバル リソースやスレッドなどが割り当てられます。以降のコールでは、特定のプロトコルのリスン スレッドを起動するだけで済みます。*protocol* は E メール プロトコル プロキシのタイプ (POP3、IMAP、SMTP など)、*interface_name* はセキュリティ アプライアンスのインターフェイス名です。

推奨処置 対処は不要です。

719012

エラー メッセージ %FWSM-6-719012: Email Proxy server listening on port *port* for mail protocol *protocol*.

説明 設定済みのポートに特定のプロトコルに関するリスン チャンネルが開かれ、そのポートが TCP セレクト グループに追加されたときに表示されるメッセージです。*port* は設定済みのポート番号、*protocol* は E メール プロキシ プロトコルのタイプ (POP3、IMAP、SMTP など) です。

推奨処置 対処は不要です。

719013

エラー メッセージ %FWSM-6-719013: Email Proxy server closing port *port* for mail protocol *protocol*.

説明 設定済みのポートに特定のプロトコルに関するリスン チャンネルが閉じられ、そのポートが TCP セレクト グループから削除されたときに表示されるメッセージです。*port* は設定済みのポート番号、*protocol* は E メール プロキシ プロトコルのタイプ (POP3、IMAP、SMTP など) です。

推奨処置 対処は不要です。

719014

エラー メッセージ %FWSM-5-719014: Email Proxy is changing listen port from *old_port* to *new_port* for mail protocol *protocol*.

説明 特定のプロトコルに関するリスン ポートで変更がシグナリングされたときに表示されるメッセージです。そのポートでイネーブルの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、新しいポートでリスンが再開されます。この動作は CLI から起動します。*old_port* は設定済みの古いポート番号、*new_port* は設定済みの新しいポート番号、*protocol* は E メール プロキシ プロトコルのタイプ (POP3、IMAP、SMTP など) です。

推奨処置 対処は不要です。

719015

エラー メッセージ %FWSN-7-719015: Parsed emailproxy session *pointer* from *source_address* username: mailuser = *mail_user*, vpnuser = *VPN_user*, mailserver = *server*

説明 クライアントからユーザ名ストリングを、*vpnuser* (名前デリミタ) *mailuser* (サーバデリミタ) *mailserver* (例: xxx:yyy@cisco.com) のフォーマットで受信したときに表示されるメッセージです。名前デリミタは省略可能です。このデリミタを省略する場合、VPN ユーザ名とメールユーザ名は共通です。サーバデリミタは省略可能です。このデリミタを省略する場合、設定されているデフォルトのメールサーバが使用されます。*pointer* はセッション構造のポインタ、*source_address* は E メール プロキシ クライアントの IP アドレス、*mail_user* は E メール アカウントユーザ名、*VPN_user* は WebVPN ユーザ名、*server* は E メール サーバです。

推奨処置 対処は不要です。

719016

エラー メッセージ %FWSM-7-719016: Parsed emailproxy session *pointer* from *source_address* password: mailpass = *****, vpnpass= *****

説明 クライアントからパスワード ストリングを、*vpnpass* (名前デリミタ) *mailpass* (例: xxx:yyy) のフォーマットで受信したときに表示されるメッセージです。名前デリミタは省略可能です。このデリミタを省略する場合、VPN パスワードとメールパスワードは共通です。*pointer* はセッション構造のポインタ、*source_address* は E 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 対処は不要です。

719025

エラー メッセージ %FWSM-6-719025: Email Proxy DNS name resolution failed for *hostname*.

説明 ホスト名が無効であるか、または使用可能な DNS サーバがないために、ホスト名を IP アドレスで解決できない場合に表示されるメッセージです。*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、有効なメールサーバ名が設定されているかどうかを確認してください。

719026

エラーメッセージ %FWSM-6-719026: Email Proxy DNS name *hostname* resolved to *IP_address*.

説明 ホスト名が IP アドレスで正しく解決されたことを表すメッセージです。*hostname* は解決する必要のあるホスト名、*IP_address* は設定されたメール サーバ名から解決された IP アドレスです。

推奨処置 対処は不要です。

720001

エラーメッセージ %FWSM-4-720001: (VPN-*unit*) Failed to initialize with Chunk Manager.

説明 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の初期化に失敗したときに表示されるメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 このメッセージはシステム全体の問題を表しており、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 メッセージを調べ、システム レベルで初期化に問題を生じている兆候がないかどうかを確認してください。

720002

エラーメッセージ %FWSM-6-720002: (VPN-*unit*) Starting VPN Stateful Failover Subsystem...

説明 VPN フェールオーバー サブシステムが起動され、システムがブートしたことを表すメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。

720003

エラーメッセージ %FWSM-6-720003: (VPN-*unit*) Initialization of VPN Stateful Failover Component completed successfully

説明 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ことを表すメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。

720004

エラーメッセージ %FWSM-6-720004: (VPN-*unit*) VPN failover main thread started.

説明 ブート時に VPN フェールオーバーのメインの処理スレッドが起動したことを表すメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。

720005

エラー メッセージ %FWSM-6-720005: (VPN-*unit*) VPN failover timer thread started.

説明 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起動したことを表すメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。

720006

エラー メッセージ %FWSM-6-720006: (VPN-*unit*) VPN failover sync thread started.

説明 ブート時にシステムのパルク同期処理スレッドが起動したことを表すメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。

720007

エラー メッセージ %FWSM-4-720007: (VPN-*unit*) Failed to allocate chunk from Chunk Manager.

説明 事前に割り当てられたメモリ バッファの集合が使い果たされたことを表すメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 このメッセージはリソースの問題を表しています。処理中のメッセージが多すぎて、システムに高負荷が生じている可能性があります。VPN フェールオーバー サブシステムによって未処理のメッセージが処理され、割り当てられていたメモリが解放されると、この状況が改善される可能性があります。

720008

エラー メッセージ %FWSM-4-720008: (VPN-*unit*) Failed to register to High Availability Framework.

説明 VPN フェールオーバー サブシステムがコアのフェールオーバー サブシステムに登録できなかったときに表示されるメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。

推奨処置 VPN フェールオーバー サブシステムが起動できません。他のサブシステムに初期化の問題がある可能性があります。システム ログ メッセージを調べ、システム全体で初期化に問題を生じている兆候がないかどうかを確認してください。

720009

エラー メッセージ %FWSM-4-720009: (VPN-unit) Failed to create version control block.

説明 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ときに表示されるメッセージです。VPN フェールオーバー サブシステムが、現在のリリースと下位互換性のあるファームウェア バージョンを検索するには、このステップが必要です。unit は、「Primary」または「Secondary」のいずれかです。

推奨処置 VPN フェールオーバー サブシステムが起動できません。他のサブシステムに初期化の問題がある可能性があります。システム ログ メッセージを調べ、システム全体で初期化に問題を生じている兆候がないかどうかを確認してください。

720010

エラー メッセージ %FWSM-6-720010: (VPN-unit) VPN failover client is being disabled

説明 オペレータがフェールオーバー キーを定義せずにフェールオーバーをイネーブルにしたときに表示されるメッセージです。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」のいずれかです。

推奨処置 failover key コマンドを使用して、アクティブユニットとスタンバイユニットの間の共有秘密鍵を定義してください。

720011

エラー メッセージ %FWSM-4-720011: (VPN-unit) Failed to allocate memory

説明 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かったときに表示されるメッセージです。システム全体でリソースに問題があります。unit は、「Primary」または「Secondary」のいずれかです。

推奨処置 システムに高負荷が生じている可能性があります。着信トラフィックを減らして、システムの負荷を下げれば、この状況が改善される可能性があります。着信トラフィックを減らすことで、現在の作業負荷を処理するために割り当てられているメモリが使用可能になり、システムが正常な動作に戻る可能性があります。

720012

エラー メッセージ %FWSM-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.

説明 対応する IPsec トンネルがスタンバイ ユニット上で削除されたために、VPN フェールオーバー サブシステムが IPsec 関連の実行時データを更新できないときに表示されるメッセージです。unit は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。

720013

エラー メッセージ %FWSM-4-720013: (VPN-unit) Failed to insert certificate in trust point *trustpoint_name*

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の挿入を試みたときに表示されるメッセージです。*unit* は、「Primary」または「Secondary」のいずれかです。*trustpoint_name* は、トラストポイントの名前です。

推奨処置 証明書の内容を確認し、無効でないかどうかをチェックしてください。

720014

エラー メッセージ %FWSM-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=*message_number*, my cookie=*mine*, his cookie=*his*) contains no SA list.

説明 フェーズ 2 接続エントリにリンクする SA がないときに表示されるメッセージです。*unit* は「Primary」または「Secondary」のいずれかです。*message_number* はフェーズ 2 接続エントリのメッセージ ID、*mine* はこちら側のフェーズ 1 Cookie、*his* はピアのフェーズ 1 Cookie です。

推奨処置 対処は不要です。

720015

エラー メッセージ %FWSM-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 特定のフェーズ 2 接続エントリに対応するフェーズ 1 SA が見つからないときに表示されるメッセージです。*unit* は「Primary」または「Secondary」のいずれかです。*message_number* はフェーズ 2 接続エントリのメッセージ ID、*mine* はこちら側のフェーズ 1 Cookie、*his* はピアのフェーズ 1 Cookie です。

推奨処置 対処は不要です。

720016

エラー メッセージ %FWSM-5-720016: (VPN-unit) Failed to initialize default timer #*index*.

説明 VPN フェールオーバー サブシステムが、特定のタイマー イベントを初期化できなかったときに表示されるメッセージです。*unit* は「Primary」または「Secondary」のいずれかです。*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 サブシステムが起動できません。システム ログメッセージを調べ、システム全体で初期化に問題を生じている兆候がないかどうかを確認してください。

720017

エラー メッセージ %FWSM-5-720017: (VPN-unit) Failed to update LB runtime data

説明 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実行時データを更新できなかったときに表示されるメッセージです。unit は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。

720018

エラー メッセージ %FWSM-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.

説明 システムに高負荷が生じている可能性があります。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」のいずれかです。code はハイ アベイラビリティ サブシステムから返されたエラー コードです。

推奨処置 着信トラフィックの量を減らして、現在の負荷条件を改善してください。着信トラフィックが少なくなると、負荷の処理用に割り当てられていたメモリが解放されます。

720019

エラー メッセージ %FWSM-5-720019: (VPN-unit) Failed to update cTCP statistics.

説明 VPN フェールオーバー サブシステムが、IPSec/cTCP 関連の統計情報を更新できなかったときに表示されるメッセージです。unit は、「Primary」または「Secondary」のいずれかです。

推奨処置 対処は不要です。定期的に更新が送信されるので、スタンバイ ユニットの IPSec/cTCP 統計情報は、次の更新メッセージで更新されるはずで。

720020

エラー メッセージ %FWSM-5-720020: (VPN-unit) Failed to send type timer message.

説明 VPN フェールオーバー サブシステムが、スタンバイ ユニットの定期的なタイマー メッセージを送信できなかったときに表示されるメッセージです。unit は「Primary」または「Secondary」のいずれかです。type はタイマー メッセージのタイプです。

推奨処置 対処は不要です。次のタイムアウトで、定期的なタイマー メッセージが再送信されます。

720021

エラー メッセージ %FWSM-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、ノンブロック メッセージを送信できませんでした。

unit 「Primary」または「Secondary」のいずれか
message_number ピア メッセージの ID 番号
code エラー リターン コード

推奨処置 システムの高負荷やシステム リソース不足などによる一時的な状況です。システム リソースが解放されると、状況は改善されます。

720022

エラー メッセージ %FWSM-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たときに、エラーが発生しました。

unit 「Primary」または「Secondary」のいずれか
trustpoint トラストポイント名

推奨処置 トラストポイントがオペレータによって削除されている可能性があります。

720023

エラー メッセージ %FWSM-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能になったことをローカル デバイスが検知すると、VPN フェールオーバー サブシステムは、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」のいずれか
not 「not」または「」のいずれか

推奨処置 対処は不要です。

720024

エラー メッセージ %FWSM-6-720024: (VPN-*unit*) HA status callback: Control channel is *status*.

説明 フェールオーバー制御チャンネルが「up」または「down」であることを表す情報メッセージです。フェールオーバー制御チャンネルは、**failover link** および **show failover** コマンドで定義します。これらのコマンドでは、フェールオーバー リンク チャンネルが「up」または「down」であることが示されます。

unit 「Primary」または「Secondary」のいずれか
status 「up」または「down」のいずれか

推奨処置 対処は不要です。

720025

エラー メッセージ %FWSM-6-720025: (VPN-*unit*) HA status callback: Data channel is *status*.

説明 フェールオーバー データ チャンネルが up または down であることを示す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

status 「up」または「down」のいずれか

推奨処置 対処は不要です。

720026

エラー メッセージ %FWSM-6-720026: (VPN-*unit*) HA status callback: Current progression is being aborted.

説明 オペレータまたはその他の外部条件によって、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）に同意する前に、現在のフェールオーバーの進行が打ち切られた場合にのみ、このメッセージが生成されます。たとえば、ネゴシエーション中にスタンバイ ユニットで `failover active` コマンドが入力された場合などです。また、アクティブユニットがリブートされた場合にも生成されます。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720027

エラー メッセージ %FWSM-6-720027: (VPN-*unit*) HA status callback: My state *state*.

説明 ローカル フェールオーバー デバイスの状態が変化したときに表示される情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

state ローカル フェールオーバー デバイスの現在の状態

推奨処置 対処は不要です。

720028

エラー メッセージ %FWSM-6-720028: (VPN-*unit*) HA status callback: Peer state *state*.

unit 「Primary」または「Secondary」のいずれか

state フェールオーバー ピアの現在の状態

説明 フェールオーバー ピアの現在の状態を報告する情報メッセージです。

推奨処置 対処は不要です。

720029

エラー メッセージ %FWSM-6-720029: (VPN-*unit*) HA status callback: Start VPN bulk sync state.

unit 「Primary」または「Secondary」のいずれか

説明 アクティブ ユニットがすべてのステート情報をスタンバイ ユニットに送信する準備が整ったときに生成される情報メッセージです。

推奨処置 対処は不要です。

720030

エラー メッセージ %FWSM-6-720030: (VPN-*unit*) HA status callback: Stop bulk sync state.

unit 「Primary」または「Secondary」のいずれか

説明 アクティブ ユニットがスタンバイ ユニットへのステート情報の送信を終了したときに生成される、情報メッセージです。

推奨処置 対処は不要です。

720031

エラー メッセージ %FWSM-7-720031: (VPN-*unit*) HA status callback: Invalid event received. event=*event_ID*.

説明 VPN フェールオーバー サブシステムが、基盤となってい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ときに生成されるメッセージです。

unit 「Primary」または「Secondary」のいずれか

event_ID 受信した無効なイベント ID

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 %FWSM-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 VPN フェールオーバー サブシステムが、基盤となっているフェールオーバー サブシステムからステータス更新を通知されたときに生成される情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

ID クライアントの 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 現在のオペランド

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 対処は不要です。

720033

エラー メッセージ %FWSM-4-720033: (VPN-*unit*) Failed to queue add to message queue.

説明 システム リソースが不足している可能性があることを表すメッセージです。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格納しようとしたとき、エラーが発生しました。

unit 「Primary」または「Secondary」のいずれか

推奨処置 システムに高負荷が生じており、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かったことを表す、一時的な状況の可能性がります。現在のシステム負荷が減少し、システム リソースが使用可能になって再び新しいメッセージを処理できるようになると、このエラー条件は解消される可能性があります。

720034

エラー メッセージ %FWSM-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したとき、エラーが発生しました。

unit 「Primary」または「Secondary」のいずれか

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 %FWSM-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試みましたが、スタンバイ ユニットで cTCP フローが事前に削除されていた可能性があります。

unit 「Primary」または「Secondary」のいずれか

推奨処置 cTCP フローが削除された兆候がないかどうかをシステム ログ メッセージで調べ、フローが削除された理由 (アイドル タイムアウトなど) を確認してください。

720036

エラー メッセージ %FWSM-5-720036: (VPN-*unit*) Failed to process state update message from the active peer.

説明 VPN フェールオーバー サブシステムが、スタンバイ ユニットから受信したステート更新メッセージの処理中にエラーが発生しました。

unit 「Primary」または「Secondary」のいずれか

推奨処置 高負荷またはシステム リソースの不足に起因する一時的な状況の可能性があります。

720037

エラー メッセージ %FWSM-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」のいずれか

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 現在のオペランド

my_state システムの現在の状態

peer_state ピアの現在の状態

説明 現在のフェールオーバーの進行状況を表す情報メッセージです。

推奨処置 対処は不要です。

720038

エラー メッセージ %FWSM-4-720038: (VPN-*unit*) Corrupted message from active unit.

説明 スタンバイ ユニットが、アクティブ ユニットから壊れたメッセージを受信しました。アクティブ ユニットからのメッセージが壊れています。アクティブ ユニットとスタンバイ ユニットで稼働中のファームウェアが非互換の可能性があります。

unit 「Primary」または「Secondary」のいずれか

推奨処置 ローカルユニットがフェールオーバー ペアのアクティブ ユニットになったことを表す情報メッセージです。

720039

エラー メッセージ %FWSM-6-720039: (VPN-*unit*) VPN failover client is transitioning to active state

説明 ローカルユニットがフェールオーバー ペアのアクティブ ユニットになったことを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720040

エラー メッセージ %FWSM-6-720040: (VPN-*unit*) VPN failover client is transitioning to standby state.

説明 ローカルユニットがフェールオーバー ペアのスタンバイ ユニットになったことを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720041

エラー メッセージ %FWSM-7-720041: (VPN-*unit*) Sending *type* message *id* to standby unit

説明 アクティブ ユニットからスタンバイ ユニットにメッセージが送信されたことを表すデバッグメッセージです。

unit 「Primary」または「Secondary」のいずれか

type メッセージ タイプ

id メッセージ ID

推奨処置 対処は不要です。

720042

エラー メッセージ %FWSM-7-720042: (VPN-*unit*) Receiving *type* message *id* from active unit

説明 スタンバイ ユニットがメッセージを受信したことを表すデバッグメッセージです。

unit 「Primary」または「Secondary」のいずれか

type メッセージ タイプ

id メッセージ ID

推奨処置 対処は不要です。

720043

エラー メッセージ %FWSM-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 ユニットからスタンバイ ユニットにメッセージを送信しようとしたとき、エラーが発生しました。これは 720018 (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、またはフェールオーバー LAN リンクがダウン) に起因している可能性があります。

unit 「Primary」または「Secondary」のいずれか

type メッセージ タイプ

id メッセージ ID

推奨処置 `show failover` コマンドを使用して、フェールオーバー ペアが正常に動作していて、フェールオーバー LAN リンクが「up」であるかどうかを確認してください。

720044

エラー メッセージ %FWSM-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 ユニットでメッセージを受信しようとしたとき、エラーが発生しました。原因としては、メッセージが壊れている場合や、着信メッセージを保存する十分なメモリが割り当てられない場合があります。

unit 「Primary」または「Secondary」のいずれか

推奨処置 `show failover` コマンドを使用して受信エラーを調べ、これが VPN フェールオーバーに固有の問題か、それとも一般的なフェールオーバーの問題であるかどうかを確認してください。メッセージが壊れている原因としては、アクティブ ユニットとスタンバイ ユニットのファームウェアバージョンが非互換であることが考えられます。`show memory` コマンドを使用して、メモリが不足していないかどうかを確認してください。

720045

エラー メッセージ %FWSM-6-720045: (VPN-*unit*) Start bulk syncing of state information on standby unit.

説明 スタンバイ ユニットが、アクティブ ユニットからのバルク同期情報の受信を開始するように通知されたことを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720046

エラーメッセージ %FWSM-6-720046: (VPN-unit) End bulk syncing of state information on standby unit

説明 スタンバイユニットが、アクティブユニットからのバルク同期の完了を通知されたことを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720047

エラーメッセージ %FWSM-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、スタンバイユニット上のSDIサーバ用のノードシークレットファイルを同期化しようとしたとき、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保存されています。このエラーは、フラッシュファイルシステムが満杯か壊れていることを表す場合があります。

unit 「Primary」または「Secondary」のいずれか

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てください。ノードシークレットファイル名は、「*ip.sdi*」です。

720048

エラーメッセージ %FWSM-7-720048: (VPN-unit) FSM action trace begin: state=*state*, last event=*event*, func=*function*.

unit 「Primary」または「Secondary」のいずれか

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 VPN フェールオーバー サブシステムの有限ステートマシン機能が起動されたことを表すデバッグメッセージです。

推奨処置 対処は不要です。

720049

エラーメッセージ %FWSM-7-720049: (VPN-unit) FSM action trace end: state=*state*, last event=*event*, return=*return*, func=*function*.

説明 VPN フェールオーバー サブシステムの有限ステートマシン機能が完了したことを表すデバッグメッセージです。

unit 「Primary」または「Secondary」のいずれか

state 現在の状態

event 最後のイベント
return リターン コード
function 現在実行中の機能

推奨処置 対処は不要です。

720050

エラー メッセージ %FWSM-7-720050: (VPN-*unit*) Failed to remove timer. ID = *id*.

説明 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表すデバッグメッセージです。

unit 「Primary」または「Secondary」のいずれか

id タイマー ID

推奨処置 対処は不要です。

720051

エラー メッセージ %FWSM-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 ユニット上の 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、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保存されています。このエラーは、フラッシュ ファイル システムが満杯か壊れていることを表す場合があります。

unit 「Primary」または「Secondary」のいずれか

id 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てください。ノード シークレット ファイル名は、「`ip.sdi`」です。

720052

エラー メッセージ %FWSM-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 ユニット上のノード 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。削除対象のノード シークレット ファイルがフラッシュ ファイル システムに存在しない場合、またはフラッシュ ファイル システムの読み取りに問題がある場合が考えられます。

unit 「Primary」または「Secondary」のいずれか

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てください。ノード シークレット ファイル名は、「`ip.sdi`」です。

720053

エラーメッセージ %FWSM-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中に、スタンバイユニット上の cTCP IKE ルールをロード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」のいずれか

IP_address ピアの IP アドレス

port ピアのポート番号

推奨処置 スタンバイユニットに高負荷が生じているために、新しいIKE ルール要求がタイムアウトした可能性があります。

720054

エラーメッセージ %FWSM-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正常に動作していない可能性があります。

unit 「Primary」または「Secondary」のいずれか

IP_address ピアの IP アドレス

port ピアのポート番号

推奨処置 cTCP データベースが満杯になっている場合や、同じピア IP アドレスおよびポート番号を持つレコードが存在する場合があります。これは一時的な状況で、終了時には改善される可能性があります。

720055

エラーメッセージ %FWSM-4-720055: (VPN-*unit*) VPN Stateful failover can only be run in single/non-transparent mode.

説明 シングル (非トランスペアレント) モードで動作していない場合、VPN サブシステムは起動されず、このメッセージが表示されます。

unit 「Primary」または「Secondary」のいずれか

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にデバイスを設定し、デバイスを再起動してください。

720056

エラーメッセージ %FWSM-6-720056: (VPN-*unit*) VPN Stateful failover Message Thread is being disabled.

説明 ユーザがフェールオーバーをイネーブルにしようとしても、フェールオーバー キーが定義されておらず、VPN フェールオーバー サブシステムのメインのメッセージ処理スレッドがディセーブルになっていることを表す情報メッセージです。VPN フェールオーバーを実行するには、フェールオーバー キーが必要です。

unit 「Primary」または「Secondary」のいずれか

推奨処置 不要です。

720057

エラーメッセージ %FWSM-6-720057: (VPN-*unit*) VPN Stateful failover Message Thread is enabled.

説明 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のメッセージ処理スレッドがイネーブルであることを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720058

エラーメッセージ %FWSM-6-720058: (VPN-*unit*) VPN Stateful failover Timer Thread is disabled.

説明 フェールオーバー キーが定義されておらず、フェールオーバーがイネーブルの場合、VPN フェールオーバー サブシステムのメインのタイマー処理スレッドがディセーブルであることを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720059

エラーメッセージ %FWSM-6-720059: (VPN-*unit*) VPN Stateful failover Timer Thread is enabled.

説明 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の場合、VPN フェールオーバー サブシステムのメインのタイマー処理スレッドがイネーブルであることを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720060

エラーメッセージ %FWSM-6-720060: (VPN-*unit*) VPN Stateful failover Sync Thread is disabled.

説明 フェールオーバーがイネーブルでも、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のバルク同期処理スレッドがディセーブルであることを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720061

エラーメッセージ %FWSM-6-720061: (VPN-*unit*) VPN Stateful failover Sync Thread is enabled.

説明 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のバルク同期処理スレッドがイネーブルであることを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720062

エラーメッセージ %FWSM-6-720062: (VPN-*unit*) Active unit started bulk sync of state information to standby unit.

説明 VPN フェールオーバー サブシステムのアクティブユニットが、スタンバイユニットへの状態情報のバルク同期を開始したことを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720063

エラーメッセージ %FWSM-6-720063: (VPN-*unit*) Active unit completed bulk sync of state information to standby.

説明 VPN フェールオーバー サブシステムのアクティブユニットが、スタンバイユニットへの状態情報のバルク同期を終了したことを表す情報メッセージです。

unit 「Primary」または「Secondary」のいずれか

推奨処置 対処は不要です。

720064

エラー メッセージ %FWSM-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中に、既存の cTCP レコードを更新しようとしたときエラーが発生しました。cTCP レコードがスタンバイ ユニットの cTCP データベースから削除されていて、見つかりません。

unit 「Primary」または「Secondary」のいずれか

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 メッセージを確認してください。

720065

エラー メッセージ %FWSM-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 ユニットの cTCP データベース エントリに新しい IKE ルールを追加しようとしたときエラーが発生しました。

unit 「Primary」または「Secondary」のいずれか

IP_address ピアの IP アドレス

port ピアのポート番号

推奨処置 システムに高負荷が生じていて、cTCP IKE ルールを追加する要求がタイムアウトした可能性があります。一時的な状況の可能性もあります。

720066

エラー メッセージ %FWSM-4-720066: (VPN-*unit*) Failed to activate IKE database.

説明 スタンバイ ユニットがアクティブ ステートへの移行中に、VPN フェールオーバー サブシステムが IKE SA データベースをアクティブ化しようとしたときにエラーが発生しました。スタンバイ ユニットにリソース関連の問題があって、IKE SA データベースがアクティブ化できなかった可能性があります。

unit 「Primary」または「Secondary」のいずれか

推奨処置 `show failover` コマンドを使用して、フェールオーバー ペアが正常に動作しているかどうかを確認してください。また、Syslog でその他の IKE 関連のエラーがないかどうかも確認してください。

720067

エラー メッセージ %FWSM-4-720067: (VPN-*unit*) Failed to deactivate IKE database.

説明 アクティブユニットがスタンバイ ステートへの移行中に、VPN フェールオーバー サブシステムが IKE SA データベースを非アクティブ化しようとしたときにエラーが発生しました。アクティブユニットにリソース関連の問題があって、IKE SA データベースが非アクティブ化できなかった可能性があります。

unit 「Primary」または「Secondary」のいずれか

推奨処置 `show failover` コマンドを使用して、フェールオーバー ペアが正常に動作しているかどうかを確認してください。また、Syslog でその他の IKE 関連のエラーがないかどうかも確認してください。

720068

エラー メッセージ %FWSM-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 ユニットで受信したピア メッセージを解析しようとしたとき、エラーが発生しました。

unit 「Primary」または「Secondary」のいずれか

推奨処置 スタンバイ ユニットで受信したピア メッセージが解析できません。アクティブ ユニットおよびスタンバイ ユニットが同じバージョンのファームウェアを実行しているかどうかを確認してください。また、`show failover` コマンドを使用して、フェールオーバー ペアが正常に動作しているかどうかも確認してください。

720069

エラー メッセージ %FWSM-4-720069: (VPN-*unit*) Failed to activate cTCP database.

説明 スタンバイ ユニットがアクティブ ステートへの移行中に、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化しようとしたときにエラーが発生しました。スタンバイ ユニットにリソース関連の問題があって、cTCP データベースがアクティブ化できなかった可能性があります。

unit 「Primary」または「Secondary」のいずれか

推奨処置 `show failover` コマンドを使用して、フェールオーバー ペアが正常に動作しているかどうかを確認してください。また、Syslog でその他の cTCP 関連のエラーがないかどうかも確認してください。

720070

エラー メッセージ %FWSM-4-720070: (VPN-*unit*) Failed to deactivate cTCP database.

説明 アクティブ ユニットがスタンバイ ステートへの移行中に、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化しようとしたときにエラーが発生しました。アクティブ ユニットにリソース関連の問題があって、cTCP データベースが非アクティブ化できなかった可能性があります。

unit 「Primary」または「Secondary」のいずれか

推奨処置 `show failover` コマンドを使用して、フェールオーバー ペアが正常に動作しているかどうかを確認してください。また、Syslog でその他の cTCP 関連のエラーがないかどうかも確認してください。

720071

エラー メッセージ %FWSM-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 ダイナミック データを更新しようとしたとき、エラーが発生しました。

unit 「Primary」または「Secondary」のいずれか

説明 一時的な状況の可能性があります。これは定期的な更新なので、時間をおいて同じエラーが発生するかどうかを確認してください。また、Syslog で他のフェールオーバー関連のメッセージがないかどうかも確認してください。

720072

エラー メッセージ %FWSM-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を検索したときに、エラーが発生しました。

unit 「Primary」または「Secondary」のいずれか

tp トラストポイント名

推奨処置 トラストポイントがオペレータによって削除されている可能性があります。show crypto ca trustpoint CLI コマンドを使用して、トラストポイントが設定に含まれているかどうかを確認してください。

720073

エラー メッセージ %FWSM-4-720073: (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したときに、エラーが発生しました。証明書の内容が無効だった可能性があります。

unit 「Primary」または「Secondary」のいずれか

trustpoint トラストポイント名

推奨処置 アクティブユニットで「write standby」を実行し、証明書を手動でスタンバイユニットに複製してください。システム ログ メッセージを調べ、フェールオーバーおよび PKI 関連のエラーがないかどうかを確認してください。



重大度別のメッセージ

記載されている内容は、次のとおりです。

- [alert メッセージ、重大度 1 \(p.A-2\)](#)
- [critical メッセージ、重大度 2 \(p.A-4\)](#)
- [error メッセージ、重大度 3 \(p.A-5\)](#)
- [warning メッセージ、重大度 4 \(p.A-11\)](#)
- [notification メッセージ、重大度 5 \(p.A-14\)](#)
- [informational メッセージ、重大度 6 \(p.A-17\)](#)
- [debugging メッセージ、重大度 7 \(p.A-22\)](#)



(注)

Cisco ASA は、重大度 0 (emergency) のメッセージを Syslog に送信しません。これらのメッセージは UNIX の panic メッセージに対応するものであり、システムが不安定になっていることを表します。

alert メッセージ、重大度 1

次のメッセージは、重大度 1 (alert) で表示されます。

- %FWSM-1-101001: (Primary) Failover cable OK.
- %FWSM-1-101002: (Primary) Bad failover cable.
- %FWSM-1-101003: (Primary) Failover cable not connected (this unit).
- %FWSM-1-101004: (Primary) Failover cable not connected (other unit).
- %FWSM-1-101005: (Primary) Error reading failover cable status.
- %FWSM-1-102001: (Primary) Power failure/System reload other side.
- %FWSM-1-103001: (Primary) No response from other firewall (reason code = code).
- %FWSM-1-103002: (Primary) Other firewall network interface interface_number OK.
- %FWSM-1-103003: (Primary) Other firewall network interface interface_number failed.
- %FWSM-1-103004: (Primary) Other firewall reports this firewall failed.
- %FWSM-1-103005: (Primary) Other firewall reporting failure.
- %FWSM-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %FWSM-1-104002: (Primary) Switching to STNDBY (cause: string).
- %FWSM-1-104003: (Primary) Switching to FAILED.
- %FWSM-1-104004: (Primary) Switching to OK.
- %FWSM-1-105001: (Primary) Disabling failover.
- %FWSM-1-105002: (Primary) Enabling failover.
- %FWSM-1-105003: (Primary) Monitoring on interface interface_name waiting
- %FWSM-1-105004: (Primary) Monitoring on interface interface_name normal
- %FWSM-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.
- %FWSM-1-105006: (Primary) Link status 'Up' on interface interface_name.
- %FWSM-1-105007: (Primary) Link status 'Down' on interface interface_name.
- %FWSM-1-105008: (Primary) Testing interface interface_name.
- %FWSM-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.
- %FWSM-1-105011: (Primary) Failover cable communication failure
- %FWSM-1-105020: (Primary) Incomplete/slow config replication
- %FWSM-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name
- %FWSM-1-105031: Failover LAN interface is up
- %FWSM-1-105032: LAN Failover interface is down
- %FWSM-1-105034: Receive a LAN_FAILOVER_UP message from peer.
- %FWSM-1-105035: Receive a LAN failover interface down msg from peer.
- %FWSM-1-105036: dropped a LAN Failover command message.
- %FWSM-1-105037: The primary and standby units are switching back and forth as the active unit.
- %FWSM-1-105038: (Primary) Interface count mismatch
- %FWSM-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %FWSM-1-105040: (Primary) Mate failover version is not compatible.
- %FWSM-1-105042: (Primary) Failover interface OK
- %FWSM-1-105043: (Primary) Failover interface failed
- %FWSM-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.

- %FWSM-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %FWSM-1-105046 (Primary|Secondary) Mate has a different chassis
- %FWSM-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
- %FWSM-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name
- %FWSM-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name
- %FWSM-1-106101 The number of ACL log deny-flows has reached limit (number).
- %FWSM-1-107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface_name
- %FWSM-1-107002: RIP pkt failed from IP_address: version=number on interface interface_name
- %FWSM-1-111111 error_message
- %FWSM-1-709003: (Primary) Beginning configuration replication: Sending to mate.
- %FWSM-1-709004: (Primary) End Configuration Replication (ACT)
- %FWSM-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %FWSM-1-709006: (Primary) End Configuration Replication (STB)

critical メッセージ、重大度 2

次のメッセージは、重大度 2 (critical) で表示されます。

- %FWSM-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
- %FWSM-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
- %FWSM-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.
- %FWSM-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.
- %FWSM-2-106013: Dropping echo request from IP_address to PAT address IP_address
- %FWSM-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.
- %FWSM-2-106017: Deny IP due to Land Attack from IP_address to IP_address
- %FWSM-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
- %FWSM-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
- %FWSM-2-106024: Access rules memory exhausted
- %FWSM-2-108002: SMTP replaced string: out source_address in inside_address data: string
- %FWSM-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
- %FWSM-2-109011: Authen Session Start: user 'user', sid number
- %FWSM-2-112001: (string:dec) Clear complete.
- %FWSM-2-201003: Embryonic limit exceeded nconns/limit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name
- %FWSM-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %FWSM-2-215001:Bad route_compress() call, sdb= number
- %FWSM-2-217001: No memory for string in string
- %FWSM-2-304007: URL Server IP_address not responding, ENTERING ALLOW mode.
- %FWSM-2-304008: LEAVING ALLOW mode, URL Server is up.
- %FWSM-2-709007: Configuration replication failed for command command
- %FWSM-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value
- %FWSM-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored
- %FWSM-2-717008: Insufficient memory to process_requiring_memory.
- %FWSM-2-717011: Unexpected event event event_ID

error メッセージ、重大度 3

次のメッセージは、重大度 3 (error) で表示されます。

- %FWSM-3-105010: (Primary) Failover message block alloc failed
- %FWSM-3-106010: Deny inbound protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port
- %FWSM-3-106011: Deny inbound (No xlate) string
- %FWSM-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)
- %FWSM-3-109010: Auth from inside_address/inside_port to outside_address/outside_port failed (too many pending auths) on interface interface_name.
- %FWSM-3-109013: User must authenticate before using this service
- %FWSM-3-109016: Can't find authorization ACL acl_ID for user 'user'
- %FWSM-3-109018: Downloaded ACL acl_ID is empty
- %FWSM-3-109019: Downloaded ACL acl_ID has parsing error; ACE string
- %FWSM-3-109020: Downloaded ACL has config error; ACE
- %FWSM-3-109023: User from source_address/source_port to dest_address/dest_port on interface outside_interface must authenticate before using this service.
- %FWSM-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %FWSM-3-113001: Unable to open AAA session. Session limit [limit] reached.
- %FWSM-3-113018: User: user, Unsupported downloaded ACL Entry: ACL_entry, Action: action
- %FWSM-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns
- %FWSM-3-201004: Too many UDP connections on {static|xlate} global_address! udp connections limit
- %FWSM-3-201005: FTP data connection failed for IP_address IP_address
- %FWSM-3-201006: RCMD backconnection failed for IP_address/port
- %FWSM-3-201008: The Cisco ASA is disallowing new connections.
- %FWSM-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded
- %FWSM-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
- %FWSM-3-202001: Out of address translation slots!
- %FWSM-3-202005: Non-embryonic in embryonic list outside_address/outside_port inside_address/inside_port
- %FWSM-3-202011: Connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
- %FWSM-3-208005: (function:line_num) clear command return code
- %FWSM-3-210001: LU sw_module_name error = number
- %FWSM-3-210002: LU allocate block (bytes) failed.
- %FWSM-3-210003: Unknown LU Object number
- %FWSM-3-210005: LU allocate connection failed
- %FWSM-3-210006: LU look NAT for IP_address failed
- %FWSM-3-210007: LU allocate xlate failed
- %FWSM-3-210008: LU no xlate for inside_address/inside_port outside_address/outside_port
- %FWSM-3-210010: LU make UDP connection for outside_address:outside_port inside_address:inside_port failed
- %FWSM-3-210020: LU PAT port port reserve failed
- %FWSM-3-210021: LU create static xlate global_address ifc interface_name failed

- %FWSM-3-211001: Memory allocation Error
- %FWSM-3-211003: CPU utilization for number seconds = percent
- %FWSM-3-212001: Unable to open SNMP channel (UDP port port) on interface interface_number, error code = code
- %FWSM-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface_number, error code = code
- %FWSM-3-212003: Unable to receive an SNMP request on interface interface_number, error code = code, will try again.
- %FWSM-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number, error code = code
- %FWSM-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.
- %FWSM-3-212006: Dropping SNMP request from source_address/source_port to interface_name:dest_address/dest_port because: reason.
- %FWSM-3-302019: H.323 library_name ASN Library failed to initialize, error code number
- %FWSM-3-302302: ACL = deny; no sa created
- %FWSM-3-304003: URL Server IP_address timed out URL url
- %FWSM-3-304006: URL Server IP_address not responding
- %FWSM-3-305005: No translation group found for protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port
- %FWSM-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
- %FWSM-3-305008: Free unallocated global IP address.
- %FWSM-3-313001: Denied ICMP type=number, code=code from IP_address on interface interface_name
- %FWSM-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
- %FWSM-3-316001: Denied new tunnel to IP_address. VPN peer limit (platform_vpn_peer_limit) exceeded
- %FWSM-3-317001: No memory available for limit_slow
- %FWSM-3-317002: Bad path index of number for IP_address, number max
- %FWSM-3-317003: IP routing table creation failure - reason
- %FWSM-3-317004: IP routing table limit warning
- %FWSM-3-317005: IP routing table limit exceeded - reason, IP_address netmask
- %FWSM-3-318001: Internal error: reason
- %FWSM-3-318002: Flagged as being an ABR without a backbone area
- %FWSM-3-318003: Reached unknown state in neighbor state machine
- %FWSM-3-318004: area string lsid IP_address mask netmask adv IP_address type number
- %FWSM-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
- %FWSM-3-318006: if interface_name if_state number
- %FWSM-3-318007: OSPF is enabled on interface_name during idb initialization
- %FWSM-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %FWSM-3-319001: Acknowledge for arp update for IP address dest_address not received (number).
- %FWSM-3-319002: Acknowledge for route update for IP address dest_address not received (number).
- %FWSM-3-319003: Arp update for IP address address to NPn failed.
- %FWSM-3-319004: Route update for IP address dest_address failed (number).

- %FWSM-3-320001: The subject name of the peer cert is not allowed for connection
- %FWSM-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface
- %FWSM-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.
- %FWSM-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.
- %FWSM-3-324000: Drop GTPv version message msg_type from source_interface:source_address/source_port to dest_interface:dest_address/dest_port Reason: reason
- %FWSM-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
- %FWSM-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
- %FWSM-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
- %FWSM-3-324004: GTP packet with version%d from source_interface:source_address/source_port to dest_interface:dest_address/dest_port is not supported
- %FWSM-3-324005: Unable to create tunnel from source_interface:source_address/source_port to dest_interface:dest_address/dest_port
- %FWSM-3-324006: GSN IP_address tunnel limit tunnel_limit exceeded, PDP Context TID tid failed
- %FWSM-3-324007: Unable to create GTP connection for response from source_interface:source_address/0 to dest_interface:dest_address/dest_port
- %FWSM-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings
- %FWSM-3-326001: Unexpected error in the timer library: error_message
- %FWSM-3-326002: Error in error_message : error_message
- %FWSM-3-326004: An internal error occurred while processing a packet queue
- %FWSM-3-326005: Mrib notification failed for (IP_address, IP_address)
- %FWSM-3-326006: Entry-creation failed for (IP_address, IP_address)
- %FWSM-3-326007: Entry-update failed for (IP_address, IP_address)
- %FWSM-3-326008: MRIB registration failed
- %FWSM-3-326009: MRIB connection-open failed
- %FWSM-3-326010: MRIB unbind failed
- %FWSM-3-326011: MRIB table deletion failed
- %FWSM-3-326012: Initialization of string functionality failed
- %FWSM-3-326013: Internal error: string in string line %d (%s)
- %FWSM-3-326014: Initialization failed: error_message error_message
- %FWSM-3-326015: Communication error: error_message error_message
- %FWSM-3-326016: Failed to set un-numbered interface for interface_name (string)
- %FWSM-3-326017: Interface Manager error - string in string : string
- %FWSM-3-326019: string in string : string
- %FWSM-3-326020: List error in string : string
- %FWSM-3-326021: Error in string : string
- %FWSM-3-326022: Error in string : string
- %FWSM-3-326023: string - IP_address : string
- %FWSM-3-326024: An internal error occurred while processing a packet queue.

- %FWSM-3-326025: string
- %FWSM-3-326026: Server unexpected error: error_message
- %FWSM-3-326027: Corrupted update: error_message
- %FWSM-3-326028: Asynchronous error: error_message
- %FWSM-3-404102: ISAKMP: Exceeded embryonic limit
- %FWSM-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
- %FWSM-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]
- %FWSM-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]
- %FWSM-3-610001: NTP daemon interface interface_name: Packet denied from IP_address
- %FWSM-3-610002: NTP daemon interface interface_name: Authentication failed for packet from IP_address
- %FWSM-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %FWSM-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %FWSM-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %FWSM-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value
- %FWSM-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %FWSM-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
- %FWSM-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %FWSM-3-713018: Unknown ID type during find of group name for certs, Type ID_Type
- %FWSM-3-713020: No Group found by matching OU(s) from ID payload: OU_value
- %FWSM-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address
- %FWSM-3-713032: Received invalid local Proxy Range IP_address - IP_address
- %FWSM-3-713033: Received invalid remote Proxy Range IP_address - IP_address
- %FWSM-3-713042: IKE Initiator unable to find policy: Intf interface_number, Src: source_address, Dst: dest_address
- %FWSM-3-713043: Cookie/peer address IP_address session already in progress
- %FWSM-3-713047: Unsupported Oakley group: Group Diffie-Hellman group
- %FWSM-3-713048: Error processing payload: Payload ID: id
- %FWSM-3-713051: Terminating connection attempt: IPSEC not permitted for group (group_name)
- %FWSM-3-713056: Tunnel rejected: SA (SA_name) not found for group (group_name)!
- %FWSM-3-713059: Tunnel Rejected: User (user) matched with group name, group-lock check failed.
- %FWSM-3-713060: Tunnel Rejected: User (user) not member of group (group_name), group-lock check failed.
- %FWSM-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address, Dst: dest_address!
- %FWSM-3-713062: IKE Peer address same as our interface address IP_address
- %FWSM-3-713063: IKE Peer address not configured for destination IP_address
- %FWSM-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %FWSM-3-713072: Password for user (user) too long, truncating to number characters
- %FWSM-3-713081: Unsupported certificate encoding type encoding_type
- %FWSM-3-713082: Failed to retrieve identity certificate
- %FWSM-3-713083: Invalid certificate handle

- %FWSM-3-713084: Received invalid phase 1 port value (port) in ID payload
- %FWSM-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %FWSM-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %FWSM-3-713088: Set Cert filehandle failure: no IPsec SA in group group_name
- %FWSM-3-713098: Aborting: No identity cert specified in IPsec SA (SA_name)!
- %FWSM-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %FWSM-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %FWSM-3-713107: IP_Address request attempt failed!
- %FWSM-3-713109: Unable to process the received peer certificate
- %FWSM-3-713112: Failed to process CONNECTED notify (SPI SPI_value)!
- %FWSM-3-713116: Terminating connection attempt: L2TP-over-IPSEC attempted by group (group_name) but L2TP disabled
- %FWSM-3-713118: Detected invalid Diffie-Hellman group_descriptor group_number, in IKE area
- %FWSM-3-713119: PHASE 1 COMPLETED
- %FWSM-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type)
- %FWSM-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)
- %FWSM-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #
- %FWSM-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %FWSM-3-713128: Connection attempt to VCIPIP redirected to VCA peer IP_address via load balancing
- %FWSM-3-713129: Received unexpected Transaction Exchange payload type: payload_id
- %FWSM-3-713132: Cannot obtain an IP_address for remote peer
- %FWSM-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id) with phase 1 group(DH group DH group_number)
- %FWSM-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection
- %FWSM-3-713138: Group group_name not found and BASE GROUP default preshared key not configured
- %FWSM-3-713140: Split Tunneling Policy requires network list but none configured
- %FWSM-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
- %FWSM-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
- %FWSM-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: netmask
- %FWSM-3-713149: Hardware client security attribute attribute_name was enabled but not requested.
- %FWSM-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.
- %FWSM-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %FWSM-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %FWSM-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server

- %FWSM-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
- %FWSM-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %FWSM-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %FWSM-3-713167: Remote peer has failed user authentication - check configured username and password
- %FWSM-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %FWSM-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!
- %FWSM-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
- %FWSM-3-713185: Error: Username too long - connection aborted
- %FWSM-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text Character index (value) is illegal
- %FWSM-3-713189: Attempted to assign network or broadcast IP_address, removing (IP_address) from pool.
- %FWSM-3-713193: Received packet with missing payload, Expected payload: payload_id
- %FWSM-3-713194: IKE|IPSec Delete With Reason message: termination_reason
- %FWSM-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
- %FWSM-3-713198: User Authorization failed: user User authorization failed.
- %FWSM-3-713203: IKE Receiver: Error reading from socket.
- %FWSM-3-713205: Could not add static route for client address: IP_address
- %FWSM-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
- %FWSM-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id
- %FWSM-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
- %FWSM-3-713210: Cannot create dynamic map for Backup L2L entry rule_id
- %FWSM-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask
- %FWSM-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %FWSM-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version
- %FWSM-3-713218: Tunnel Rejected: Client Type or Version not allowed.
- %FWSM-3-713226: Connection failed with peer IP_address, no trust-point defined in tunnel-group tunnel_group
- %FWSM-3-717001: Querying keypair failed.
- %FWSM-3-717002: Certificate enrollment failed for trustpoint trustpoint_name. Reason: reason_string.
- %FWSM-3-717009: Certificate validation failed. Reason: reason_string.
- %FWSM-3-717010: CRL polling failed for trustpoint trustpoint_name.
- %FWSM-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure
- %FWSM-3-717015: CRL received from issuer is too large to process (CRL size = crl_size, maximum CRL size = max_crl_size)
- %FWSM-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url
- %FWSM-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries, maximum number allowed = max_allowed)
- %FWSM-3-717019: Failed to insert CRL for trustpoint trustpoint_name. Reason: failure_reason.

warning メッセージ、重大度 4

次のメッセージは、重大度 4 (warning) で表示されます。

- %FWSM-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
- %FWSM-4-106027:Failed to determine the security context for the packet:vlan source Vlan#:ethertype src sourceMAC dst destMAC
- %FWSM-4-109017: User at IP_address exceeded auth proxy connection limit (max)
- %FWSM-4-109022: exceeded HTTPS proxy process limit
- %FWSM-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user
- %FWSM-4-109028: aaa bypassed for same-security traffic from ingress_ interface:source_address/source_port to egress_interface:dest_address/dest_port
- %FWSM-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.
- %FWSM-4-109031: NT Domain Authentication Failed: rejecting guest login for username.
- %FWSM-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number
- %FWSM-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number
- %FWSM-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %FWSM-4-308002: static global_address inside_address netmask netmask overlapped with global_address inside_address
- %FWSM-4-313003: Invalid destination for ICMP error
- %FWSM-4-313004:Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session
- %FWSM-4-325002: Duplicate address ipv6_address/MAC_address on interface
- %FWSM-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=dest_address, prot=protocol, spi=number
- %FWSM-4-402102: decapsulate: packet missing {AH|ESP}, destaddr=dest_address, actual prot=protocol
- %FWSM-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
- %FWSM-4-402106: Rec'd packet not an IPSEC packet (ip) dest_address= dest_address, src_addr= source_address, prot= protocol
- %FWSM-4-404101: ISAKMP: Failed to allocate address for client from pool string
- %FWSM-4-405001: Received ARP {request | response} collision from IP_address/MAC_address on interface interface_name
- %FWSM-4-405002: Received mac mismatch collision from IP_address/MAC_address for authenticated host
- %FWSM-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %FWSM-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %FWSM-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex
- %FWSM-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP

- %FWSM-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest
- %FWSM-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
- %FWSM-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name
- %FWSM-4-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name
- %FWSM-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded
- %FWSM-4-407003: Established limit for RPC services exceeded number
- %FWSM-4-408001: IP route counter negative - reason, IP_address Attempt: number
- %FWSM-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %FWSM-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls
- %FWSM-4-409002: db_free: external LSA IP_address netmask
- %FWSM-4-409003: Received invalid packet: reason from IP_address, interface_name
- %FWSM-4-409004: Received reason from unknown neighbor IP_address
- %FWSM-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name
- %FWSM-4-409006: Invalid lsa: reason Type number, LSID IP_address from IP_address, IP_address, interface_name
- %FWSM-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask
- %FWSM-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric : number area : string
- %FWSM-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID
- %FWSM-4-409010: Virtual link information found in non-backbone area: string
- %FWSM-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name
- %FWSM-4-409012: Detected router with duplicate router ID IP_address in area string
- %FWSM-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address
- %FWSM-4-409023: Attempting AAA Fallback method method_name for request_type request for user user :Auth-server group server_tag unreachable
- %FWSM-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.
- %FWSM-4-411001:Line protocol on interface interface_name changed state to up
- %FWSM-4-411002:Line protocol on interface interface_name changed state to down
- %FWSM-4-411003: Configuration status on interface interface_name changed state to downup
- %FWSM-4-411004: Configuration status on interface interface_name changed state to up
- %FWSM-4-412001:MAC MAC_address moved from interface_1 to interface_2
- %FWSM-4-412002:Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num
- %FWSM-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

- %FWSM-4-417001: Unexpected event received: number
- %FWSM-4-417004: Filter violation error: conn number (string:string) in string
- %FWSM-4-417006: No memory for string) in string. Handling: string
- %FWSM-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)
- %FWSM-4-500004: Invalid transport field for protocol=protocol, from source_address/source_port to dest_address/dest_port
- %FWSM-4-612002: Auto Update failed:filename, version:number, reason:reason
- %FWSM-4-612003:Auto Update failed to contact:url, reason:reason
- %FWSM-4-620002: Unsupported CTIQBE version: hex: from interface_name:IP_address/port to interface_name:IP_address/port
- %FWSM-4-713154: DNS lookup for peer_description Server [server_name] failed!
- %FWSM-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.
- %FWSM-4-713903:Descriptive_event_string.
- %FWSM-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %FWSM-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %FWSM-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %FWSM-4-720009: (VPN-unit) Failed to create version control block.
- %FWSM-4-720011: (VPN-unit) Failed to allocate memory
- %FWSM-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint_name

notification メッセージ、重大度 5

次のメッセージは、重大度 5 (notification) で表示されます。

- %FWSM-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %FWSM-5-111003: IP_address Erase configuration
- %FWSM-5-111004: IP_address end configuration: {FAILED|OK}
- %FWSM-5-111005: IP_address end configuration: OK
- %FWSM-5-111007: Begin configuration: IP_address reading from device.
- %FWSM-5-111008: User user executed the command string
- %FWSM-5-199001: Reload command executed from telnet (remote IP_address).
- %FWSM-5-199006: Orderly reload started at when by whom. Reload reason: reason
- %FWSM-5-1999007: IP detected an attached application using port port while removing context
- %FWSM-5-1999008: Protocol detected an attached application using local port local_port and destination port dest_port
- %FWSM-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
- %FWSM-5-304001: user source_address Accessed {JAVA URL|URL} dest_address: url.
- %FWSM-5-304002: Access denied URL chars SRC IP_address DEST IP_address: chars
- %FWSM-5-321001: Resource var1 limit of var2 reached.
- %FWSM-5-321002: Resource var1 rate limit of var2 reached.
- %FWSM-5-500001: ActiveX content modified src IP_address dest IP_address on interface interface_name.
- %FWSM-5-500002: Java content modified src IP_address dest IP_address on interface interface_name.
- %FWSM-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
- %FWSM-5-505001: Module in slot slotnum is shutting down. Please wait...
- %FWSM-5-505002: Module in slot slotnum is reloading. Please wait...
- %FWSM-5-505003: Module in slot slotnum is resetting. Please wait...
- %FWSM-5-505004: Module in slot slotnum shutdown is complete.
- %FWSM-5-505005: Module in slot slotnum is initializing control communication. Please wait...
- %FWSM-5-505006: Module in slot slotnum is Up.
- %FWSM-5-505007: Module in slot slotnum is recovering. Please wait...
- %FWSM-5-506001: event_source_string event_string
- %FWSM-5-501101: User transitioning priv level
- %FWSM-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string
- %FWSM-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string
- %FWSM-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level
- %FWSM-5-502111: New group policy added: name: policy_name Type: policy_type
- %FWSM-5-502112: Group policy deleted: name: policy_name Type: policy_type
- %FWSM-5-503001: Process number, Nbr IP_address on interface_name from string to string, reason
- %FWSM-5-504001: Security context context_name was added to the system
- %FWSM-5-504002: Security context context_name was removed from the system

- %FWSM-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
- %FWSM-5-612001: Auto Update succeeded:filename, version:number
- %FWSM-5-713006: Failed to obtain state for message Id message_number, Peer Address: IP_address
- %FWSM-5-713010: IKE area: failed to find centry for message Id message_number
- %FWSM-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)
- %FWSM-5-713049: Security negotiation complete for tunnel_type type (group_name) Initiator/Responder, Inbound SPI = SPI, Outbound SPI = SPI
- %FWSM-5-713050: Connection terminated for peer IP_address. Reason: termination reason Remote Proxy IP_address, Local Proxy IP_address
- %FWSM-5-713068: Received non-routine Notify message: notify_type (notify_value)
- %FWSM-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger_value to smaller_value seconds
- %FWSM-5-713074: Responder forcing change of IPSec rekeying duration from larger_value to smaller_value Kbs
- %FWSM-5-713075: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value seconds
- %FWSM-5-713076: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value Kbs
- %FWSM-5-713092: Failure during phase 1 rekeying attempt due to collision
- %FWSM-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec
- %FWSM-5-713130: Received unsupported transaction mode attribute: attribute id
- %FWSM-5-713131: Received unknown transaction mode attribute: attribute_id
- %FWSM-5-713135: message received, redirecting tunnel to IP_address.
- %FWSM-5-713136: IKE session establishment timed out [IKE_state_name], aborting!
- %FWSM-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!
- %FWSM-5-713139: group_name not found, using BASE GROUP default preshared key
- %FWSM-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction
- %FWSM-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: netmask
- %FWSM-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure. Resetting any Backup Server init.
- %FWSM-5-713156: Initializing Backup Server [server_name or IP_address]
- %FWSM-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP
- %FWSM-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %FWSM-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload
- %FWSM-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses.Peer could be Originate Only - Possible misconfiguration!
- %FWSM-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.
- %FWSM-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter_value)!
- %FWSM-5-713216: Rule: action Client type : version Client: type version is/is not allowed

- %FWSM-5-713229: Auto Update - Notification to client client_ip of update string: message_string.
- %FWSM-5-713904:Descriptive_event_string.
- %FWSM-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer
- %FWSM-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %FWSM-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol.
- %FWSM-5-720016: (VPN-unit) Failed to initialize default timer #index.
- %FWSM-5-720017: (VPN-unit) Failed to update LB runtime data
- %FWSM-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.
- %FWSM-5-720019: (VPN-unit) Failed to update cTCP statistics.
- %FWSM-5-720020: (VPN-unit) Failed to send type timer message.

informational メッセージ、重大度 6

次のメッセージは、重大度 6 (informational) で表示されます。

- %FWSM-6-106012: Deny IP from IP_address to IP_address, IP options hex.
- %FWSM-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name.
- %FWSM-6-106025: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol
- %FWSM-6-106026: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol
- %FWSM-6-109001: Auth start for user user from inside_address/inside_port to outside_address/outside_port
- %FWSM-6-109002: Auth from inside_address/inside_port to outside_address/outside_port failed (server IP_address failed) on interface interface_name.
- %FWSM-6-109003: Auth from inside_address to outside_address/outside_port failed (all servers failed) on interface interface_name.
- %FWSM-6-109005: Authentication succeeded for user user from inside_address/inside_port to outside_address/outside_port on interface interface_name.
- %FWSM-6-109006: Authentication failed for user user from inside_address/inside_port to outside_address/outside_port on interface interface_name.
- %FWSM-6-109007: Authorization permitted for user user from inside_address/inside_port to outside_address/outside_port on interface interface_name.
- %FWSM-6-109008: Authorization denied for user user from outside_address/outside_port to inside_address/inside_port on interface interface_name.
- %FWSM-6-109024: Authorization denied from source_address/source_port to dest_address/dest_port (not authenticated) on interface interface_name using protocol
- %FWSM-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
- %FWSM-6-113003: AAA group policy for user user is being set to policy_name.
- %FWSM-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user
- %FWSM-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user
- %FWSM-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %FWSM-6-113007: User user unlocked by administrator
- %FWSM-6-113008: AAA transaction status ACCEPT: user = user
- %FWSM-6-113009: AAA retrieved default group policy policy for user user
- %FWSM-6-113010: AAA challenge received for user user from server server_IP_address
- %FWSM-6-113011: AAA retrieved user specific group policy policy for user user
- %FWSM-6-113012: AAA user authentication Successful: local database : user = user
- %FWSM-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %FWSM-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user
- %FWSM-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user
- %FWSM-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user
- %FWSM-6-113017: AAA credentials rejected: reason = reason: local database: user = user
- %FWSM-6-199002: startup completed. Beginning operation.
- %FWSM-6-199003: Reducing link MTU dec.
- %FWSM-6-199005: Startup begin

- %FWSM-6-210022: LU missed number updates
- %FWSM-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port
- %FWSM-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
- %FWSM-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
- %FWSM-6-302010: connections in use, connections most used
- %FWSM-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address/port to laddr IP_address
- %FWSM-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)]
- %FWSM-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)]
- %FWSM-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)]
- %FWSM-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)]
- %FWSM-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)]
- %FWSM-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)]
- %FWSM-6-302020: Built {in | out}bound ICMP connection for faddr {faddr | icmp_seq_num} gaddr {gaddr | cmp_type} laddr laddr
- %FWSM-6-302021: Teardown ICMP connection for faddr {faddr | icmp_seq_num} gaddr {gaddr | cmp_type} laddr laddr
- %FWSM-6-303002: source_address {Stored|Retrieved} dest_address: mapped_address
- %FWSM-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
- %FWSM-6-304004: URL Server IP_address request failed URL url
- %FWSM-6-305007: addrpool_free(): Orphan IP IP_address on interface interface_number
- %FWSM-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address to interface_name:mapped_address
- %FWSM-6-305010: Teardown {dynamic|static} translation from interface_name:real_address to interface_name:mapped_address duration time
- %FWSM-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface_name:real_address/real_port to interface_name:mapped_address/mapped_port
- %FWSM-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
- %FWSM-6-308001: console enable password incorrect for number tries (from IP_address)
- %FWSM-6-311001: LU loading standby start
- %FWSM-6-311002: LU loading standby end
- %FWSM-6-311003: LU recv thread up
- %FWSM-6-311004: LU xmit thread up
- %FWSM-6-312001: RIP hdr failed from IP_address: cmd=string, version=number domain=string on interface interface_name

- %FWSM-6-314001: Pre-allocate RTSP UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
- %FWSM-6-315011: SSH session from IP_address on interface interface_name for user user disconnected by SSH server, reason: reason
- %FWSM-6-321003: Resource var1 log level of var2 reached.
- %FWSM-6-321004: Resource var1 rate log level of var2 reached
- %FWSM-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address, src_addr=source_address, prot=protocol
- %FWSM-6-602102: Adjusting IPSec tunnel mtu...
- %FWSM-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %FWSM-6-602201: ISAKMP Phase 1 SA created (local IP_address/port (initiator|responder), remote IP_address/port, authentication=auth_type, encryption=enchr_alg, hash=hash_alg, group=DH_grp, lifetime=seconds)
- %FWSM-6-602202: ISAKMP session connected (local IP_address (initiator|responder), remote IP_address)
- %PIX-6-602203: ISAKMP session disconnected (local IP_address (initiator|responder), remote IP_address)
- %FWSM-6-602301: sa created...
- %FWSM-6-602302: deleting sa
- %FWSM-6-604101: DHCP client interface interface_name: Allocated ip = IP_address, mask = netmask, gw = gateway_address
- %FWSM-6-604102: DHCP client interface interface_name: address released
- %FWSM-6-604103: DHCP daemon interface interface_name: address granted MAC_address (IP_address)
- %FWSM-6-604104: DHCP daemon interface interface_name: address released
- %FWSM-6-606001: ASDM session number number from IP_address started
- %FWSM-6-606002: ASDM session number number from IP_address ended
- %FWSM-6-606003: ASDM logging session number id from IP_address started id session ID assigned
- %FWSM-6-606004: ASDM logging session number id from IP_address ended
- %FWSM-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message
- %FWSM-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address/port from string message
- %FWSM-6-609001: Built local-host interface_name:IP_address
- %FWSM-6-609002: Teardown local-host interface_name:IP_address duration time
- %FWSM-6-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
- %FWSM-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number
- %FWSM-6-613002: interface interface_name has zero bandwidth
- %FWSM-6-613003: IP_address netmask changed from area string to area string
- %FWSM-6-614001: Split DNS: request patched from server: IP_address to server: IP_address
- %FWSM-6-614002: Split DNS: reply from server:IP_address reverse patched back to original server:IP_address
- %FWSM-6-615001: vlan number not available for firewall interface
- %FWSM-6-615002: vlan number available for firewall interface

- %FWSM-6-616001: Pre-allocate MGCP data_channel connection for inside_interface:inside_address to outside_interface:outside_address/port from message_type message
- %FWSM-6-617001: GTPv version msg_type from source_interface:source_address/source_port not accepted by source_interface:dest_address/dest_port
- %FWSM-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
- %FWSM-6-617003: GTP Tunnel created from source_interface:source_address/source_port to source_interface:dest_address/dest_port
- %FWSM-6-617004: GTP connection created for response from source_interface:source_address/0 to source_interface:dest_address/dest_port
- %FWSM-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
- %FWSM-6-621001: Interface interface_name does not support multicast, not enabled
- %FWSM-6-621002: Interface interface_name does not support multicast, not enabled
- %FWSM-6-621003: The event queue size has exceeded number
- %FWSM-6-621006: Mrib disconnected, (IP_address,IP_address) event cancelled
- %FWSM-6-621007: Bad register from interface_name:IP_address to IP_address for (IP_address, IP_address)
- %FWSM-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: netmask
- %FWSM-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask
- %FWSM-6-713172: Automatic NAT Detection Status: Remote end is|is not behind a NAT device This end is|is not behind a NAT device
- %FWSM-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port
- %FWSM-6-713184: Client Type: Client_type Client Application Version: Application_version_string
- %FWSM-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask
- %FWSM-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %FWSM-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
- %FWSM-6-713219: Queueing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %FWSM-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.
- %FWSM-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.
- %FWSM-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.
- %FWSM-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.
- %FWSM-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.
- %FWSM-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
- %FWSM-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.
- %FWSM-6-719003: Email Proxy session pointer resources have been freed for source_address.
- %FWSM-6-719004: Email Proxy session pointer has been successfully established for source_address.
- %FWSM-6-719010: protocol Email Proxy feature is disabled on interface interface_name.
- %FWSM-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.

- %FWSM-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %FWSM-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address
- %FWSM-6-719025: Email Proxy DNS name resolution failed for hostname.
- %FWSM-6-719026: Email Proxy DNS name hostname resolved to IP_address.
- %FWSM-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %FWSM-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
- %FWSM-6-720004: (VPN-unit) VPN failover main thread started.
- %FWSM-6-720005: (VPN-unit) VPN failover timer thread started.
- %FWSM-6-720006: (VPN-unit) VPN failover sync thread started.
- %FWSM-6-720010: (VPN-unit) VPN failover client is being disabled
- %FWSM-6-720012: (VPN-unit) Failed to update IPSec failover runtime data on the standby unit.
- %FWSM-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his) contains no SA list.
- %FWSM-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number,my cookie=mine, his cookie=his).

debugging メッセージ、重大度 7

次のメッセージは、重大度 7 (debugging) で表示されます。

- %FWSM-7-109014: uauth_lookup_net fail for uauth_in()
- %FWSM-7-109021: Uauth null proxy error
- %FWSM-7-111009: User user executed cmd:string
- %FWSM-7-199009: ICMP detected an attached application while removing a context
- %FWSM-7-304005: URL Server IP_address request pending URL url
- %FWSM-7-304009: Ran out of buffer blocks specified by url-block command
- %FWSM-7-701001: alloc_user() out of Tcp_user objects
- %FWSM-7-701002: alloc_user() out of Tcp_proxy objects
- %FWSM-7-702201: ISAKMP Phase 1 delete received (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702202: ISAKMP Phase 1 delete sent (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702203: ISAKMP DPD timed out (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702204: ISAKMP Phase 1 retransmission (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702205: ISAKMP Phase 2 retransmission (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702206: ISAKMP malformed payload received (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702207: ISAKMP duplicate packet detected (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702208: ISAKMP Phase 1 exchange started (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702209: ISAKMP Phase 2 exchange started (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702210: ISAKMP Phase 1 exchange completed(local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702211: ISAKMP Phase 2 exchange completed(local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702212: ISAKMP Phase 1 initiating rekey (local IP_address (initiator|responder), remote IP_address)
- %FWSM-7-702301: lifetime expiring...
- %FWSM-7-702303: sa_request...
- %FWSM-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %FWSM-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name:IP_address to interface_name:IP_address/port
- %FWSM-7-709001: FO replication failed: cmd=command returned=code
- %FWSM-7-709002: FO unreplicable: cmd=command
- %FWSM-7-710001: TCP access requested from source_address/source_port to interface_name:dest_address/service
- %FWSM-7-710002: {TCP|UDP} access permitted from source_address/source_port to interface_name:dest_address/service
- %FWSM-7-710004: TCP connection limit exceeded from source_address/source_port to interface_name:dest_address/service

- %FWSM-7-710005: {TCP|UDP} request discarded from source_address/source_port to interface_name:dest_address/service
- %FWSM-7-710006: protocol request discarded from source_address to interface_name:dest_address
- %FWSM-7-711001: debug_trace_msg
- %FWSM-7-711002: Task ran for elapsed_time msec, process = process_name
- %FWSM-7-713024: Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %FWSM-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %FWSM-7-713026: Transmitted local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %FWSM-7-713027: Transmitted remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %FWSM-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %FWSM-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %FWSM-7-713030: Transmitted local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %FWSM-7-713031: Transmitted remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %FWSM-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %FWSM-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %FWSM-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %FWSM-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %FWSM-7-713039: Send failure: Bytes (number), Peer: IP_address
- %FWSM-7-713040: Could not find connection entry and can not encrypt: msgid message_number
- %FWSM-7-713052: User (user) authenticated.
- %FWSM-7-713066: IKE Remote Peer configured for SA: SA_name
- %FWSM-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %FWSM-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %FWSM-7-713103: Invalid (NULL) secret key detected while computing hash
- %FWSM-7-713104: Attempt to get Phase 1 ID data failed while hash computation
- %FWSM-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: IP_address, SA address: internal_SA_address, tunnel count: count
- %FWSM-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address) for peer IP_address, but cookies don't match
- %FWSM-7-713117: Received Invalid SPI notify (SPI SPI_Value)!
- %FWSM-7-713121: Keep-alive type for this connection: keepalive_type
- %FWSM-7-713143: Processing firewall record. Vendor: vendor(id), Product: product(id), Caps: capability_value, Version Number: version_number, Version String: version_text
- %FWSM-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %FWSM-7-713164: The Firewall Server has requested a list of active user sessions

- %FWSM-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address, SA address: internal_SA_address, tunnelCnt: tunnel_count
- %FWSM-7-713170: IKE Received delete for rekeyed centry IKE peer: IP_address, centry address: internal_address, msgid: id
- %FWSM-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %FWSM-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
- %FWSM-7-713190: Got bad refCnt (ref_count_value) assigning IP_address (IP_address)
- %FWSM-7-713204: Adding static route for client address: IP_address
- %FWSM-7-713221: Static Crypto Map check, checking map = crypto_map_tag, seq = seq_number...
- %FWSM-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
- %FWSM-7-713223: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, no ACL configured
- %FWSM-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!
- %FWSM-7-713225: [IKEv1], Static Crypto Map check, map map_name, seq = sequence_number is a successful match
- %FWSM-7-713900: Descriptive_event_string.
- %FWSM-7-713901: Descriptive_event_string.
- %FWSM-7-713905: Descriptive_event_string.
- %FWSM-7-713906: debug_message
- %FWSM-7-714001: Description of event or packet
- %FWSM-7-714002: IKE Initiator starting QM: msg id = message_number
- %FWSM-7-714003: IKE Responder starting QM: msg id = message_number
- %FWSM-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number
- %FWSM-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number
- %FWSM-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number
- %FWSM-7-714007: IKE Initiator sending Initial Contact
- %FWSM-7-714011: Description of received ID values
- %FWSM-7-715001: Descriptive statement
- %FWSM-7-715004: subroutine name() Q Send failure: RetCode (return_code)
- %FWSM-7-715005: subroutine name() Bad message code: Code (message_code)
- %FWSM-7-715006: IKE got SPI from key engine: SPI = SPI_value
- %FWSM-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value
- %FWSM-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address
- %FWSM-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address
- %FWSM-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data
- %FWSM-7-715019: IKEGetUserAttributes: Attribute name = name
- %FWSM-7-715020: construct_cfg_set: Attribute name = name
- %FWSM-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle
- %FWSM-7-715041: Received keep-alive of type keepalive_type, not the negotiated type
- %FWSM-7-715042: IKE received response of type failure_type to a request from the IP_address utility
- %FWSM-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability

- %FWSM-7-715045: ERROR: malformed Keepalive payload
- %FWSM-7-715046: constructing payload_description payload
- %FWSM-7-715047: processing payload_description payload
- %FWSM-7-715048: Send VID_type VID
- %FWSM-7-715049: Received VID_type VID
- %FWSM-7-715050: Claims to be IOS but failed authentication
- %FWSM-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply
- %FWSM-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centres
- %FWSM-7-715053: MODE_CFG: Received request for attribute_info!
- %FWSM-7-715054: MODE_CFG: Received attribute_name reply: value
- %FWSM-7-715055: Send attribute_name
- %FWSM-7-715056: Client is configured for TCP_transparency
- %FWSM-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
- %FWSM-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
- %FWSM-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %FWSM-7-715060: Dropped received IKE fragment. Reason: reason
- %FWSM-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
- %FWSM-7-715062: Error assembling fragments! Fragment numbers are non-continuous.
- %FWSM-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
- %FWSM-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %FWSM-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address) state, event: state/event pairs
- %FWSM-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
- %FWSM-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %FWSM-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %FWSM-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %FWSM-7-715069: Invalid ESP SPI size of SPI_size
- %FWSM-7-715070: Invalid IPComp SPI size of SPI_size
- %FWSM-7-715071: AH proposal not supported
- %FWSM-7-715072: Received proposal with unknown protocol ID protocol_ID
- %FWSM-7-715074: Could not retrieve authentication attributes for peer IP_address
- %FWSM-7-715075: Group = group_name, Username = client, IP = IP_address Received keep-alive of type message_type (seq number number)



A			
AAA			
許可	2-24		
サーバ	2-25, 2-31, 2-106		
認証	2-29, 2-30, 2-31		
メッセージ	2-19, 2-20, 2-21, 2-22, 2-23, 2-24, 2-25, 2-28, 2-29, 2-30, 2-31, 2-32, 2-85, 2-106		
ABR			
バックボーン エリアなし	2-61		
access-list コマンド	2-13, 2-18, 2-50		
UDP ポート 53 でトラフィックを許可	2-13		
ACL			
ACL が未設定	2-150		
deny-flows	2-18		
SoftNP エラー	2-191		
UDP ポート 53 でのトラフィックの拒否	2-13, 2-18, 2-50		
暗号マップ	2-77, 2-122		
一致のログ	2-17		
解析エラー	2-23		
拒否	2-50		
空白の ACL のダウンロード	2-23		
空白のリスト	2-23		
コンパイル時のメモリ不足	2-16		
サポートされないフォーマット	2-32		
スプリット トンネリング ポリシー	2-134		
設定の誤り	2-23		
チェックの失敗	2-24		
トラフィック フローが制限数を超過	2-18		
パケットの拒否	2-16		
ピア コンテキスト ID	2-189		
ピアの IP アドレスが未設定	2-189		
プロキシ ID の不一致	2-150		
ActiveX オブジェクトのフィルタリング	2-90		
ActiveX オブジェクト、フィルタリング	2-90		
ARP			
スプーフィング攻撃	2-65		
		パケットの不一致	2-77
		ポイズニング攻撃	2-77
		C	
		conduit コマンド	
		ICMP オプションの許可	2-14
		config コマンド	2-26
		configure コマンド	2-27
		CTIQBE	
		サポート対象外のバージョン	2-104
		接続オブジェクトの割り当て	2-104
		D	
		DNS クエリ応答の拒否	2-13
		DNS サーバが低速	2-13
		DoS 攻撃	2-18, 2-22, 2-38, 2-81
		E	
		EMBLEM フォーマット、ログでの使用	1-24
		F	
		failover コマンド	2-5, 2-9
		active オプション	2-4, 2-202
		filter allow コマンド	2-52
		filter コマンド	
		activex オプション	2-90
		allow オプション	2-52
		fixup protocol SMTP コマンド	2-19
		Flood Defender	2-106
		floodguard コマンド	2-21
		FTP	
		データ接続の失敗	2-36

- メッセージ 2-50, 2-51, 2-52

- H
- H.225 2-79
- H.245 2-45
- H.245 接続
 - 外部アドレス 2-45
- H.323
 - 対象外のパケットバージョン 2-109
 - バック接続、割り当て 2-45
- H245 接続の確立 2-45
- H323 UDP バック接続の割り当て 2-45
- HTTPS プロセスの制限 2-24

- I
- ICMP
 - パケットの拒否 2-14
 - 変換の作成が失敗 2-54
- IDB の初期化 2-62
- Internet Phone の使用の検出 2-45
- Internet Phone、使用の検出 2-45
- ip verify reverse-path コマンド 2-15, 2-16
- IP アドレス
 - DHCP クライアント 2-97
 - DHCP サーバ 2-97
- IP アドレス/ポートから IP アドレス/ポートへの認証が失敗 2-20
- IP スプーフの拒否 2-14
- IP ルーティングテーブル
 - OSPF の矛盾 2-62
 - 攻撃 2-18, 2-19
 - 作成エラー 2-60
 - 制限に関する警告 2-60
 - 制限を超過 2-61
- IP ルート カウンタの減分の失敗 2-81
- IPSec
 - 接続
- IPSec
 - cTCP トンネル 2-210
 - IKE 要求 2-109
 - IKE をトリガーしたパケット 2-120
 - L2TP-over-IPSec 接続 2-129
 - over TCP 2-162
 - over UDP 2-138, 2-163
 - SA 2-121, 2-126, 2-127, 2-130, 2-156, 2-158, 2-165, 2-166
 - プロポーザル 2-166
 - 暗号化 2-156
 - 再キーイングの持続時間 2-124
 - 接続
 - AAA トランザクションの失敗 2-31, 2-32
 - L2TP-over-IPSec 2-129
 - 失敗 2-171, 2-172
 - 成功 2-28
 - 認証の失敗 2-29
 - 接続エントリ 2-129
 - トンネル 2-28, 2-60, 2-95, 2-109, 2-120, 2-121, 2-142, 2-171, 2-172, 2-184
 - ネゴシエーション 2-122
 - パケット 2-76, 2-77
 - パケットの欠落 2-76
 - フラグメンテーション ポリシーの無視 2-143
 - プロキシの不一致 2-50
 - プロトコル 2-115
 - プロポーザル
 - SA 2-166
 - サポート対象外 2-166
 - 無効なパケット 2-76
 - 要求のリジェクト 2-129
- IPSec プロキシの不一致 2-50

- L
- Land Attack 2-15
- LSA
 - 不正なマスクを使用したデフォルト 2-83
 - 見つからない 2-61
 - 無効なタイプ 2-83

- M
- MAC アドレスの不一致 2-78
- Man in the Middle 攻撃 2-63
- MIB 1-2

- O
- OSPF
 - IDB の初期化 2-62
 - IP ルーティング テーブルの矛盾 2-62

- LSA
- 不正なマスクを使用したデフォルト 2-83
 - 見つからない 2-61
 - 無効なタイプ 2-83
 - 同じルータ ID の hello パケット 2-84
 - 仮想リンク 2-62
 - コンフィギュレーションの変更 2-102
 - チェックサム エラー 2-101
 - ネイバ ステートの変更 2-92
 - ネットワーク範囲のエリアの変更 2-102
 - パケットの長さが無効 2-83
 - バックボーン エリアのない ABR 2-61
 - 不明のネイバからの hello 2-83
 - 不明のネイバからのデータベース記述 2-83
 - 不明のネイバからのデータベース要求 2-83
 - プロセスのリセット 2-62
 - 無効なパケット 2-82
 - ルータ ID のリセット 2-62
 - ルータ ID 割り当ての失敗 2-84
- outbound deny コマンド 2-12
- P
- PAT
- アドレス 2-37, 2-78, 2-79
 - グローバル アドレス 2-14
 - ホストが未指定 2-14
- PAT ホストを特定できない 2-14
- R
- RCMD、バック接続の失敗 2-36
- reload コマンド 2-27, 2-33
- rsh コマンド 2-36
- S
- SA
- IKE の要求 2-109
 - 削除 2-96
 - 作成 2-96
- SETUP メッセージ 2-79
- show static コマンド 2-35
- show コマンド
- blocks オプション 2-7
 - failover オプション 2-42, 2-207
 - local-host オプション 2-81
 - outbound オプション 2-12
 - static オプション 2-35
 - version オプション 2-81
- SIP 接続 2-99
- Skinny 接続 2-99
- SMTP 2-19
- SNMP
- MIB 1-2
 - 概要 1-2
 - 管理ステーション 1-6
 - トラップ 1-2
- SPI 2-76
- SSH 2-59
- SYN
- 攻撃 2-35
 - フラグ 2-14
- Syslog サーバ
- EMBLEM フォーマット
 - イネーブル化 1-10
 - 設定 1-24
 - 出力先 1-10
 - 指定 1-10
 - 複数の指定 1-10
 - 出力先としての指定 1-10
 - デバイス ID、メッセージでの表示 1-11
 - ファシリティ、指定 1-8
- T
- TCP
- アクセスの許可 2-112
 - アクセスの要求 2-111
 - 接続 2-112
 - 接続の制限の超過 2-112
 - テーブルで関連付けられた接続なし 2-14
 - 不正なヘッダー長 2-90
 - 変換の作成が失敗 2-54
 - 要求の廃棄 2-113
- TCP 接続の再確立 2-45
- timeout uauth コマンド 2-21

- U
- UDP
- アクセスの許可 2-112
 - 接続 2-112
 - パケット 2-13
 - 変換の作成が失敗 2-54
 - メッセージ 2-53
 - 要求の廃棄 2-113
- URL
- サーバ 2-52
 - バッファ ブロック スペース 2-53
 - フィルタリング、ディセーブル 2-52
- V
- VPN
- トンネル 2-60
 - ピアの制限 2-60
- VPN フェールオーバー
- CTCP フロー処理エラー 2-204
 - SDI ノード シークレット ファイルの同期が失敗 2-208
 - アクティブ ユニットからのメッセージ受信が失敗 2-207
 - クライアントがディセーブル 2-198
 - 初期化の失敗 2-196
 - スタンバイ ユニットがアクティブ ユニットから壊れたメッセージを受信 2-205
 - ステート更新メッセージのエラー 2-205
 - タイマー エラー 2-199
 - チャンク割り当ての失敗 2-197
 - 登録の失敗 2-197
 - トラストポイントの証明書エラー 2-199
 - トラストポイント名が見つからない 2-201
 - ノンブロック メッセージの送信エラー 2-201
 - バージョン コントロール ブロックのエラー 2-198
 - メッセージ キューに追加できない 2-204
 - メモリ割り当てエラー 2-198
- W
- Web 要求、フィルタリングなし 2-52
 - Websense サーバ 2-52
 - write erase コマンド 2-26
 - write コマンド 2-26
- erase オプション 2-26
 - standby オプション 2-41
 - standby コマンド 2-41
- あ
- 悪意あるイベント 2-76, 2-77
 - ファイアウォールの回避 2-15
 - アクセス リストが未作成 2-189
 - アクセスの許可 2-112
 - アクセスの拒否
 - ACL 2-17
 - URL 2-51
 - アクセスの要求 2-111
 - アドレス変換スロット
 - 不足 2-37, 2-78
 - アドレス変換スロットの不足 2-37
- い
- インターフェイス、帯域幅がゼロ 2-101
- え
- エコー要求の廃棄 2-14
 - エリア境界ルータ
 - ABR を参照
- お
- 同じルータ ID の hello パケット 2-84
- か
- 仮想リンク 2-62
- き
- キュー、ロギング
 - サイズの変更 1-22
 - 統計情報の表示 1-22
 - 許可
 - 失敗 2-100
 - ユーザの拒否 2-21
 - 許可モードの終了、URL サーバ 2-52

拒否

- IP スプーフ 2-14
- TCP (接続なし) 2-14
- アドレス間の IP 2-13
- 外部からの着信 2-13
- クエリ / 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

く

クラス

- タイプ 1-20
- メッセージ クラス変数 1-20
- メッセージのフィルタリング 1-19

け

- 権限レベル、変更 2-91

こ

攻撃

- ARP スプーフイング 2-65
- ARP ポイズニング 2-77
- DoS 2-18, 2-22, 2-38, 2-77, 2-81
- IP ルーティング テーブル 2-18, 2-19
- Land 2-15
- Man in the Middle 2-63
- SYN 2-35
- 疑わしい電子メール アドレス パターン 2-19
- スプーフイング 2-14, 2-15, 2-16, 2-64, 2-65, 2-78

コンフィギュレーション 1-20

- local-host オプションのクリア 2-81
- 消去 2-26
- ステータスの変更 2-86
- 設定値のクリア 1-25
- 複製
 - 開始 2-110
 - 失敗 2-110

し

システム メッセージ

- FTP 2-50 2-52
- SNMP 2-42
- SSH 2-59
- アラート ログ 2-19
- クラス
 - クラスの一覧 1-20
- グループ別の管理
 - メッセージ クラス 1-19
 - メッセージ リストの作成 1-19
- グループ別の設定
 - 重大度 1-6
 - メッセージ リスト 1-20
- 重大度
 - 一覧 1-27
 - メッセージの重大度の変更 1-6
- 出力先 1-6
 - E メール アドレス 1-12
 - Syslog メッセージ サーバ 1-6
 - Telnet または SSH セッション 1-6
 - 内部バッファ 1-6
- 使用する変数 1-27, 1-28
- ステートフル フェールオーバー 2-39, 2-40, 2-41, 2-42
- 接続関連 2-13, 2-35, 2-45
- タイムスタンプ、表示 1-22
- デバイス ID、表示 1-23
- フィルタリング
 - メッセージ クラス 1-19
- フォーマット 1-27
- メール ガード 2-19
- メッセージ リスト、作成 1-19
- リストの作成 1-19
- ログのディセーブル化 1-6
- システム メッセージ内の変数、一覧 1-28
- 自動アップデートの URL が到達不可能 2-101
- 重大度、システム メッセージ
 - 一覧 1-27
 - 定義 1-27
 - フィルタリング 1-6
 - 変更 1-6
- 出力先
 - E メール アドレス 1-6, 1-12
 - SNMP 管理ステーション 1-6
 - Syslog サーバ 1-6, 1-10

- Telnet または SSH セッション 1-6
 - 指定 1-12
 - 内部バッファ 1-6
 - ログの表示 1-9
- 初期制限の超過 2-35
- す
- スタティックの接続が多過ぎる 2-35
- ステートフル フェールオーバー 2-39, 2-40, 2-42
- スプーフィング攻撃 2-14, 2-15, 2-16, 2-78
- せ
- セキュリティ
 - アソシエーション
 - SA を参照
 - コンテキスト
 - コンテキストが判別不能 2-17
 - 削除 2-92
 - 追加 2-92
 - 侵犯 2-13
 - パラメータ インデックス
 - SPI を参照
- 接続テーブルで関連付けられた接続なし 2-14
- 接続の制限の超過 2-35, 2-112
- 接続メッセージ 2-12, 2-13, 2-45
- 設定値のクリア 1-25
- 設定の開始 2-27
- セルフ ルート 2-13
- た
- 帯域幅、ゼロとして報告 2-101
- タイムアウト、推奨値 2-81
- タイムスタンプ、システム メッセージでの表示 1-22
- ち
- 着信 TCP 接続の拒否 2-12
- て
- テスト、インターフェイス 2-7
- デバイス ID、メッセージでの表示 1-23
- 電源障害、フェールオーバー 2-3
- 電子メール アドレス内の無効な文字の置き換え 2-19
- と
- トラップ、SNMP 1-2
- に
- 認証
 - サーバが検出不能 2-20
 - 失敗 2-20
 - 要求の成功 2-20
 - 認証サーバが検出不能 2-20
 - 認証セッションの終了 2-21
- は
- パケット
 - 完全性チェック 2-13
 - 拒否 2-12, 2-13, 2-14, 2-16
 - 発信 NAT ルールとの不一致 2-53
- 発信接続の拒否 2-12
- バッファのラップ
 - FTP サーバへの送信 1-16, 1-17
 - 内部フラッシュへの保存 1-17
 - フラッシュへの保存 1-6
- ひ
- 非対称ルーティング 2-16
- ふ
- ファシリティ、設定 1-11
- フェールオーバー
 - failover active コマンド 2-202
 - failover コマンド メッセージの廃棄 2-9
 - LAN インターフェイスのダウン 2-8
 - show failover コマンド 2-207
 - VPN フェールオーバー
 - CTCP フロー処理エラー 2-204
 - SDI ノード シークレット ファイルの同期が失敗 2-208

- アクティブユニットからのメッセージ受信が失敗 2-207
- クライアントがディセーブル 2-198
- 初期化の失敗 2-196
- スタンバイユニットがアクティブユニットから壊れたメッセージを受信 2-205
- ステート更新メッセージのエラー 2-205
- タイマー エラー 2-199
- チャンク割り当ての失敗 2-197
- 登録の失敗 2-197
- トラストポイントの証明書エラー 2-199
- トラストポイント名が見つからない 2-201
- ノンブロック メッセージの送信エラー 2-201
- バージョン コントロール ブロックのエラー 2-198
- バッファ エラー 2-200
- メッセージ キューに追加できない 2-204
- メモリ割り当てエラー 2-198
- インターフェイス リンクがダウン 2-10
- カード構成の不一致 2-11
- ケーブル ステータス 2-2
- ケーブル通信の失敗 2-7
- ケーブル不良 2-2
- ケーブル未接続 2-2
- 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の失敗 2-111
- シャーシの不一致 2-11
- スタンバイ装置の同期化の失敗 2-8
- ステートフル エラー 2-39
- ステートフル フェールオーバー 2-39, 2-40, 2-41
- 電源障害 2-3
- 動作モードの不一致 2-11
- ネットワーク インターフェイスの障害 2-4
- ピアの LAN リンクがダウン 2-9
- ピアの障害 2-4
- 複製の割り込み 2-9
- プライマリ装置の障害 2-5
- ブロック割り当ての失敗 2-7
- メイトがディセーブル 2-10
- メイトとの通信の損失 2-6
- メイトのソフトウェアが非互換 2-10
- ライセンスが不一致 2-11
- リンク ステータス up または down 2-6
- 連続的なフェールオーバー 2-9
- フェールオーバー メッセージ 2-2, 2-3, 2-5, 2-7, 2-110
- ブリッジ テーブル、満杯 2-86
- ブロードキャスト、無効な送信元アドレス 2-14
- プロトコルの変換グループが見つからない 2-53
- へ
- 変換グループが見つからない 2-53
- ほ
- ホストの移動 2-86
- ホストの制限値 2-80
- む
- 無効な送信元アドレス 2-14
- め
- メイトとのフェールオーバー通信の損失 2-6
- メッセージ
 - ステートフル フェールオーバー 2-41
- メッセージ クラス
 - 一覧 1-20
 - 概要 1-19
- メッセージ ブロック割り当ての失敗 2-7
- メッセージ リスト
 - 作成 1-21
 - フィルタリング 1-20
- メッセージの重大度、一覧 1-27
- メッセージのディセーブル化、特定のメッセージ ID 1-24
- メッセージのフォーマット 1-27
- メモリ
 - 破壊 2-101
 - 不足 2-37, 2-60, 2-78, 2-79
 - ブロックの不足 2-7
 - リーク 2-61
- メモリ不足 2-60, 2-79
 - エラーの原因 2-37, 2-78
 - 処理の失敗 2-60
 - 変換スロットの不足 2-37, 2-78
- も
- モジュールの管理 2-26

- モニタ
 - SNMP 1-2
- ゆ
- ユーザ認証の開始 2-19
- ユーザ認証、エラー 2-23
- ユーザ名
 - 削除 2-91
 - 作成 2-91
- よ
- 要求の廃棄 2-113
- り
- リンク ステータス up または down 2-6
- リンク ステート アドバタイズ
 - LSA を参照
- る
- ルータ ID のリセット 2-62
- ルータ ID 割り当ての失敗 2-84
- 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
- ログイン キュー
 - 設定 1-22
- ログ
 - E メール
 - 宛先アドレス 1-13
 - 出力先としての指定 1-12
 - 送信元アドレス 1-12
 - EMBLEM フォーマット 1-24
 - Syslog サーバ、指定 1-10
 - キュー
 - キューの統計情報の表示 1-22
 - サイズの変更 1-22
 - 設定 1-22
 - クラス
 - タイプ 1-19, 1-20
 - メッセージのフィルタリング 1-19
 - 重大度
 - 変更 1-25
 - 出力先
 - ASDM 1-13
 - E メール アドレス 1-12, 1-13
 - Syslog サーバ 1-11
 - Telnet または SSH セッション 1-6
 - 内部バッファ 1-6
 - ファシリティ 1-11
 - タイムスタンプ、表示 1-22
 - デバイス ID、システム メッセージでの表示 1-23
 - ファシリティ、設定 1-11
 - フィルタリング
 - 重大度 1-6
 - メッセージ リスト 1-20
 - メッセージのフィルタリング
 - メッセージ クラス 1-19
 - ログイン キュー、設定 1-22
 - ログ バッファのラップ
 - FTP サーバへの送信 1-17
 - 内部フラッシュへの保存 1-17
 - ログの出力先
 - ASDM 1-13
 - E メール アドレス 1-12
 - Syslog サーバ 1-6
 - Telnet または SSH セッション 1-6
 - 内部バッファ 1-6
 - ログの表示 1-9