



Syslog メッセージ 401001 ~ 450001

この章は、次の項で構成されています。

- [メッセージ 401001 ~ 409128](#) (1 ページ)
- [メッセージ 410001 ~ 450001](#) (29 ページ)

メッセージ 401001 ~ 409128

この章では、401001 から 409128 までのメッセージについて説明します。

401001

エラーメッセージ %FTD-4-401001: Shuns cleared

説明メモリから既存の排除を削除するために **clear shun** コマンドが入力されました。組織によるシャニング アクティビティの記録が許可されました。

推奨アクション必要なし。

401002

エラーメッセージ %FTD-4-401002: Shun added: IP_address IP_address port port

説明 **shun** コマンドが入力されました。このコマンドの最初の IP アドレスは排除されたホストです。その他のアドレスとポートはオプションであり、有効な場合は接続を終了するのに使用されます。組織によるシャニング アクティビティの記録が許可されました。

推奨アクション必要なし。

401003

エラーメッセージ %FTD-4-401003: Shun deleted: IP_address

説明排除されたホストの1つが排除データベースから削除されました。組織によるシャニング アクティビティの記録が許可されました。

推奨アクション必要なし。

401004

エラーメッセージ %FTD-4-401004: Shunned packet: *IP_address* = *IP_address* on interface *interface_name*

説明 IP SRC によって定義されたホストは排除データベースのホストであるために、パケットが廃棄されました。排除されたホストは、そこで排除されたインターフェイスにトラフィックを渡すことはできません。たとえば、インターネット上の外部ホストは外部インターフェイス上で排除されます。排除されたホストのアクティビティの記録が提供されました。このメッセージとメッセージ %FTD-4-401005 を使用すると、このホストに関するリスクを詳しく見積もることができます。

推奨アクション必要なし。

401005

エラーメッセージ %FTD-4-401005: Shun add failed: unable to allocate resources for *IP_address IP_address port port*

説明 Firepower Threat Defense デバイスのメモリが不足しています。排除が適用できません。

推奨アクション Cisco IPS は、引き続き、この規則を適用しようとします。メモリを再利用して排除を手動で再適用するか、または Cisco IPS によって排除が適用されるのを待機します。

402114

エラーメッセージ %FTD-4-402114: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq_num*) from *remote_IP* to *local_IP* with an invalid SPI.

- >*protocol* : IPSec プロトコル
- >*spi* : IPSec のセキュリティ パラメータ インデックス
- *seq_num*> : IPSec シーケンス番号
- *remote_IP*> : トンネルのリモートエンドポイントの IP アドレス
- >*username* : IPSec トンネルに関連付けられているユーザ名
- *local_IP*> : トンネルのローカルエンドポイントの IP アドレス

説明 SA データベースに存在しない SPI を指定している IPSec パケットを受信しました。これは、IPSec ピア間の SA のエイジングのわずかな相違による一時的な状態か、またはローカル SA の消去が原因です。また、IPSec ピアによって不正なパケットが送信されたことを示すこともあります。これも攻撃の一部の場合があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

推奨アクション ローカル SA が消去されたことを、ピアは認識していない可能性があります。新しい接続がローカルルータから確立された場合、2つのピアが正常に接続を再度確立することがあります。あるいは、問題の発生が短期間にとどまらない場合は、接続を新規に確立してみるか、またはピアの管理者に問い合わせます。

402115

エラーメッセージ %FTD-4-402115: IPSEC: Received a packet from *remote_IP* to *local_IP* containing *act_prot* data instead of *exp_prot* data.

説明期待された ESP ヘッダーのない IPsec パケットを受信しました。ピアは、ネゴシエートされたセキュリティポリシーと一致しないパケットを送信中です。これは攻撃を示している可能性があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

- *remote_IP*> : トンネルのリモートエンドポイントの IP アドレス
- *local_IP*> : トンネルのローカルエンドポイントの IP アドレス
- >*act_prot* : 受信した IPsec プロトコル
- >*exp_prot* : 期待された IPsec プロトコル

推奨アクション ピアの管理者にお問い合わせください。

402116

エラーメッセージ %FTD-4-402116: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq_num*) from *remote_IP* (*username*) to *local_IP* . The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as *pkt_daddr* , its source as *pkt_saddr* , and its protocol as *pkt_prot* . The SA specifies its local proxy as *id_daddr* /*id_dmask* /*id_dprot* /*id_dport* and its remote proxy as *id_saddr* /*id_smask* /*id_sprot* /*id_sport* .

説明カプセル化解除された IPsec パケットがネゴシエートされた ID と一致しません。ピアは、このセキュリティアソシエーションを通じて他のトラフィックを送信中です。これは、ピアによるセキュリティアソシエーション選択エラーが原因であるか、攻撃の一部の場合である可能性があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

- >*protocol* : IPsec プロトコル
- >*spi* : IPsec のセキュリティ パラメータ インデックス
- *seq_num*> : IPsec シーケンス番号
- *remote_IP*> : トンネルのリモートエンドポイントの IP アドレス
- >*username* : IPsec トンネルに関連付けられているユーザ名
- *local_IP*> : トンネルのローカルエンドポイントの IP アドレス
- *pkt_daddr*> : カプセル化解除されたパケットからの宛先アドレス
- *pkt_saddr*> : カプセル化解除されたパケットからの送信元アドレス
- *pkt_prot*> : カプセル化解除されたパケットからのトランスポートプロトコル
- *id_daddr*> : ローカルプロキシ IP アドレス
- *id_dmask*> : ローカルプロキシ IP サブネットマスク
- *id_dprot*> : ローカルプロキシトランスポートプロトコル
- *id_dport*> : ローカルプロキシポート
- *id_saddr*> : リモートプロキシ IP アドレス
- *id_smask*> : リモートプロキシ IP サブネットマスク
- *id_sprot*> : リモートプロキシトランスポートプロトコル

- `id_sport`> : リモート プロキシ ポート

推奨アクション ピアの管理者に問い合わせ、ポリシーの設定を比較します。

402117

エラーメッセージ %FTD-4-402117: IPSEC: Received a non-IPsec (protocol) packet from remote_IP to local_IP .

説明受信パケットはクリプトマップ ACL と一致したが、IPSec でカプセル化されていません。IPSec ピアはカプセル化されていないパケットを送信中です。このエラーは、ピアのポリシー セットアップエラーが原因で発生することがあります。たとえば、外部インターフェイスポート 23 への暗号化 Telnet トラフィックだけを受信するようにファイアウォールを設定できます。IPSec 暗号化を行わずに Telnet を使用して、ポート 23 上で外部インターフェイスにアクセスしようとする、このメッセージが表示されますが、ポート 23 以外の外部インターフェイスに対する Telnet またはトラフィックの場合は表示されません。このエラーは、攻撃を示すこともあります。このメッセージは、これらの条件以外では生成されません（たとえば、Firepower Threat Defense インターフェイス自体へのトラフィックの場合は生成されません）。TCP および UDP 要求を追跡するメッセージ 710001、710002、および 710003 を参照してください。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

- >`protocol` : IPSec プロトコル
- `remote_IP`> : トンネルのリモートエンドポイントの IP アドレス
- `local_IP`> : トンネルのローカルエンドポイントの IP アドレス

推奨アクション ピアの管理者に問い合わせ、ポリシーの設定を比較します。

402118

エラーメッセージ %FTD-4-402118: IPSEC: Received an protocol packet (SPI=`spi` , sequence number `seq_num`) from remote_IP (username) to local_IP containing an illegal IP fragment of length `frag_len` with offset `frag_offset` .

説明カプセル化解除された IPSec パケットに、128 バイト以下のオフセットの IP フラグメントが含まれていました。最新バージョンの IP RFC のセキュリティ アーキテクチャでは、リアセンブリ攻撃を防止するために最小 IP フラグメント オフセットを 128 バイトにすることを推奨しています。これは攻撃の一部の場合があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

- >`protocol` : IPSec プロトコル
- >`spi` : IPSec のセキュリティ パラメータ インデックス
- `seq_num`> : IPSec シーケンス番号
- `remote_IP`> : トンネルのリモートエンドポイントの IP アドレス
- >`username` : IPSec トンネルに関連付けられているユーザ名
- `local_IP`> : トンネルのローカルエンドポイントの IP アドレス
- `frag_len`> : IP フラグメント長
- `frag_offset`> : IP フラグメント オフセット (バイト)

推奨アクション リモート ピアの管理者に問い合わせ、ポリシーの設定を比較します。

402119

エラーメッセージ %FTD-4-402119: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq_num*) from *remote_IP* (*username*) to *local_IP* that failed anti-replay checking.

説明 シーケンス番号が無効な IPSec パケットを受信しました。ピアは、以前に使用された可能性のあるシーケンス番号が含まれたパケットを送信中です。このメッセージは、受け入れ許容範囲外のシーケンス番号の IPSec パケットを受信したことを示します。このパケットは、可能性ある攻撃の一部として IPSec により廃棄されます。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

- >*protocol* : IPSec プロトコル
- >*spi* : IPSec のセキュリティ パラメータ インデックス
- *seq_num*> : IPSec シーケンス番号
- *remote_IP*> : トンネルのリモート エンドポイントの IP アドレス
- >*username* : IPSec トンネルに関連付けられているユーザ名
- *local_IP*> : トンネルのローカル エンドポイントの IP アドレス

推奨アクション ピアの管理者にお問い合わせください。

402120

エラーメッセージ %FTD-4-402120: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq_num*) from *remote_IP* (*username*) to *local_IP* that failed authentication.

説明 IPSec パケットを受信したが認証に失敗しました。パケットはドロップされます。パケットは中継中に破損したか、ピアが無効な IPSec パケットを送信している可能性があります。これらのパケットの多くを同じピアから受信した場合、攻撃を示している可能性があります。このメッセージは、5 秒に 1 回しか表示されないように制限されています。

- >*protocol* : IPSec プロトコル
- >*spi* : IPSec のセキュリティ パラメータ インデックス
- *seq_num*> : IPSec シーケンス番号
- *remote_IP*> : トンネルのリモート エンドポイントの IP アドレス
- >*username* : IPSec トンネルに関連付けられているユーザ名
- *local_IP*> : トンネルのローカル エンドポイントの IP アドレス

推奨アクション 受信したパケットの認証失敗が多い場合は、リモートピアの管理者にお問い合わせください。

402121

エラーメッセージ %FTD-4-402121: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq_num*) from *peer_addr* (*username*) to *lcl_addr* that was dropped by IPsec (*drop_reason*).

説明カプセル化解除する IPSec パケットを受信したが、そのパケットが IPSec サブシステムによって後で廃棄されました。これは、Firepower Threat Defense の設定または Firepower Threat Defense デバイス そのものに問題が存在する可能性があることを示しています。

- >protocol : IPSec プロトコル
- >spi : IPSec のセキュリティ パラメータ インデックス
- seq_num> : IPSec シーケンス番号
- peer_addr> : トンネルのリモート エンドポイントの IP アドレス
- >username : IPSec トンネルに関連付けられているユーザ名
- lcl_addr> : トンネルのローカル エンドポイントの IP アドレス
- drop_reason> : パケットが廃棄された原因

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

402122

エラーメッセージ %FTD-4-402122: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPsec that was dropped by IPsec (drop_reason).

説明 IPSec でカプセル化するパケットを受信しましたが、そのパケットが IPSec サブシステムによって後で廃棄されました。これは、Firepower Threat Defense の設定または Firepower Threat Defense デバイス そのものに問題が存在する可能性があることを示しています。

- src_addr > : 送信元 IP アドレス
- dest_addr > : 宛先 > IP アドレス
- drop_reason> : パケットが廃棄された原因

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

402123

エラーメッセージ %FTD-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code=error_string) while executing crypto command command.

説明ハードウェア アクセラレータを使用した crypto コマンドの実行中にエラーが検出されました。アクセラレータの問題を示している可能性があります。このタイプのエラーは、さまざまな理由で発生します。このメッセージは、原因の判定に役立つように暗号アクセラレータカウンタを補足します。

- accel_type : ハードウェア アクセラレータ タイプ
- >error_string : エラーのタイプを示すコード
- command : エラーを生成した暗号コマンド

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

402124

エラーメッセージ %FTD-4-402124: CRYPTO: The FTD hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size, DoorBell Outstanding, SWReset).

説明暗号ハードウェアチップが重大エラーを報告しました。チップが動作不能であることを示します。このメッセージからの情報は、詳細を取り込み、問題をさらに分析できるようにします。この状態が検出されると、暗号チップがリセットされ、円滑にFirepower Threat Defense デバイスの機能を継続できます。また、この問題が検出されたときの暗号環境が、フラッシュ上の暗号アーカイブディレクトリに書き込まれ、さらなるデバッグ情報を提供します。このメッセージには、暗号ハードウェアに関連する次のようなさまざまなパラメータが含まれています。

- HWErrAddr> : ハードウェア アドレス (暗号チップによって設定)
- Core> : エラーが発生している暗号コア
- HwErrCode> : ハードウェア エラー コード (暗号チップによって設定)
- IstatReg> : 割り込みステータス レジスタ (暗号チップによって設定)
- PciErrReg> : PCI エラー レジスタ (暗号チップによって設定)
- CoreErrStat> : コア エラー ステータス (暗号チップによって設定)
- CoreErrAddr> : コア エラー アドレス (暗号チップによって設定)
- Doorbell Size> : 許可される暗号コマンドの最大数
- DoorBell Outstanding> : 処理待ちの暗号コマンド数
- SWReset> : ブート後の暗号チップ リセット回数



(注) The %FTD-vpn-4-402124: CRYPTO: The FTD hardware accelerator encountered an error (HWErrAddr=0x40EE9800, Core=0, HwErrCode=23, IstatReg=0x8, PciErrReg=0x0, CoreErrStat=0x41, CoreErrAddr=0x844E9800, Doorbell Size[0]=2048, DoorBell Outstanding[0]=0, Doorbell Size[1]=0, DoorBell Outstanding[1]=0, SWReset=99) エラーメッセージは、AnyConnect の問題と、AnyConnect 3.1.x にアップグレードする回避策を示します。

推奨アクションメッセージの情報を Cisco TAC に転送し、さらなる分析を依頼してください。

402125

エラーメッセージ %FTD-4-402125: The FTD hardware accelerator ring timed out (parameters).

説明 IPSEC の記述子リングまたは SSL/Admin の記述子リングが進行していないことを暗号ドライバが検出しました。つまり、暗号チップが機能していないと思われます。この状態が検出されると、暗号チップがリセットされ、円滑にFirepower Threat Defense デバイスの機能を継続できます。また、この問題が検出されたときの暗号環境が、フラッシュ上の暗号アーカイブディレクトリに書き込まれ、さらなるデバッグ情報を提供します。

- >ring : IPSEC リングまたは Admin リング

- *parameters* > : 次のとおり。
- Desc> : 記述子アドレス
- CtrlStat> : 制御/ステータス値
- ResultP> : 成功ポインタ
- ResultVal> : 成功値
- Cmd> : 暗号コマンド
- CmdSize> : コマンド サイズ
- Param> : コマンド パラメータ
- Dlen> : データ長
- DataP> : データ ポインタ
- CtxtP> : VPN コンテキスト ポインタ
- SWReset> : ブート後の暗号チップ リセット回数

推奨アクションメッセージの情報を Cisco TAC に転送し、さらなる分析を依頼してください。

402126

エラーメッセージ %FTD-4-402126: CRYPTO: The FTD created Crypto Archive File Archive Filename as a Soft Reset was necessary. Please forward this archived information to Cisco.

説明 ハードウェア暗号チップで機能上の問題が検出されました (syslog メッセージ 402124 および 402125 を参照)。暗号の問題をさらにデバッグするために、現在の暗号ハードウェア環境 (ハードウェア レジスタおよび暗号記述エントリ) を含む暗号アーカイブ ファイルが生成されます。ブート時に、フラッシュ ファイルシステム上に `crypto_archive` ディレクトリが自動的に作成されました (事前に存在していなかった場合)。このディレクトリには、最大2つの暗号アーカイブ ファイルが存在できます。

- > *Archive Filename* : 暗号アーカイブ ファイルの名前。暗号アーカイブ ファイルの名前は `crypto_arch_x.bin` という形式です。ここで、`x` は 1 または 2 です。

推奨アクション暗号アーカイブ ファイルを Cisco TAC に転送し、さらなる分析を依頼してください。

402127

エラーメッセージ %FTD-4-402127: CRYPTO: The FTD is skipping the writing of latest Crypto Archive File as the maximum # of files, *max_number*, allowed have been written to *archive_directory* . Please archive & remove files from Archive Directory if you want more Crypto Archive Files saved.

説明 ハードウェア暗号チップで機能上の問題が検出されました（メッセージ 4402124 および 4402125 を参照）。このメッセージは、最大数の暗号アーカイブファイルがすでに存在していたため、暗号アーカイブファイルが書き込まれなかったことを示しています。

- *max_number* > : アーカイブ ディレクトリで許可されているファイルの最大数（現在は 2 に設定されています）
- >*archive_directory* : アーカイブ ディレクトリの名前

推奨アクション 以前に生成された暗号アーカイブ ファイルを Cisco TAC に転送します。以前に生成されたアーカイブ ファイルを削除して、別のアーカイブ ファイルを書き込むことができるようにします（必要であると思われる場合）。

402128

エラーメッセージ %FTD-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: *size* , limit: *limit*

説明 SSL 接続で許容量を超えるメモリの使用が試みられています。要求が拒否されました。

- *size* : 割り当てられようとしたメモリ ブロックのサイズ
- *limit* : 許容割り当てメモリの最大サイズ

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

402129

エラーメッセージ %FTD-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: *address*

説明 内部ソフトウェア エラーが発生しました。

- *address* : 解放されようとしたアドレス

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402130

エラーメッセージ %FTD-6-402130: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number=0x7B) from 75.2.96.101 (user=user) to 85.2.96.10 with incorrect IPsec padding.

説明 Firepower Threat Defense デバイスの暗号ハードウェア アクセラレータで無効な埋め込みデータを含む IPsec パケットが検出されました。ATT VPN クライアントでは、IPsec パケットの埋め込みが不適切に行われる場合があります。

- *SPI* : パケットに関連付けられている SPI
- *sequence number* : パケットに関連付けられているシーケンス番号
- *user* : ユーザー名文字列
- *padding* : パケットからの埋め込みデータ

推奨アクション このメッセージが不要であり、Firepower Threat Defense デバイスの問題が示されていない場合、ATT VPN クライアントを使用しているお客様は VPN クライアントソフトウェアのアップグレードが必要になることがあります。

402131

エラーメッセージ %FTD-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias .

説明 ハードウェア アクセラレーション設定が Firepower Threat Defense デバイス で変更されました。一部の Firepower Threat Defense プラットフォームには、複数のハードウェア アクセラレータがあります。ハードウェア アクセラレータの変更ごとに 1 件の syslog メッセージが生成されます。

- *status* : success または failure を示します
- *accel_instance* : ハードウェア アクセラレータのインスタンス
- *old_config_bias* : 古い設定
- *new_config_bias* : 新しい設定

推奨アクション 設定を変更しようとしてアクセラレータのいずれかが失敗した場合は、ログイン情報を収集し、Cisco TAC に連絡してください。障害が発生した場合、ソフトウェアは、設定変更を複数回再試行します。再試行が失敗した場合、ソフトウェアは元の構成バイアスにフォールバックします。ハードウェア アクセラレータの再設定に複数回失敗する場合、ハードウェアの障害を示している可能性があります。

402140

エラーメッセージ %FTD-3-402140: CRYPTO: RSA key generation error: modulus len len

説明 RSA 公開キー ペアの生成時にエラーが発生しました。

- *len* : ビット単位で示したプライム モジュラスの長さ

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402141

エラーメッセージ %FTD-3-402141: CRYPTO: Key zeroization error: key set type , reason reason

説明 RSA 公開キー ペアの生成時にエラーが発生しました。

- *type* : 次のいずれかのキーセットタイプ。DH、RSA、DSA、unknown
- *reason* : 予期しない暗号化セッションタイプ

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402142

エラーメッセージ %FTD-3-402142: CRYPTO: Bulk data op error: algorithm *alg* , mode *mode*
説明対称キー操作中にエラーが発生しました。

- *op* : encryption または decryption のいずれかの操作
- *alg* : 次のいずれかの暗号化アルゴリズム。DES、3DES、AES、RC4
- *mode* : 次のいずれかのモード。CBC、CTR、CFB、ECB、stateful-RC4、stateless-RC4

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402143

エラーメッセージ %FTD-3-402143: CRYPTO: alg type key op
説明非対称キー操作中にエラーが発生しました。

- *alg* : RSA または DSA のいずれかの暗号化アルゴリズム
- *type* : public または private のいずれかのキー タイプ
- *op* : encryption または decryption のいずれかの操作

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402144

エラーメッセージ %FTD-3-402144: CRYPTO: Digital signature error: signature algorithm *sig* , hash algorithm *hash*

説明デジタル署名の生成中にエラーが発生しました。

- *sig* : RSA または DSA のいずれかの署名アルゴリズム
- *hash* : 次のいずれかのハッシュアルゴリズム。MD5、SHA1、SHA256、SHA384、SHA512

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402145

エラーメッセージ %FTD-3-402145: CRYPTO: Hash generation error: algorithm *hash*

説明ハッシュ生成エラーが発生しました。

- *hash* : 次のいずれかのハッシュアルゴリズム。MD5、SHA1、SHA256、SHA384、SHA512

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402146

エラーメッセージ %FTD-3-402146: CRYPTO: Keyed hash generation error: algorithm *hash* , key len *len*

説明キー付きハッシュ生成エラーが発生しました。

- *hash* : 次のいずれかのハッシュアルゴリズム。MD5、SHA1、SHA256、SHA384、SHA512
- *len* : ビット単位のキーの長さ

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402147

エラーメッセージ %FTD-3-402147: CRYPTO: HMAC generation error: algorithm *alg*

説明 HMAC の生成エラーが発生しました。

- *alg* : 次のいずれかの HMAC アルゴリズム。HMAC-MD5、HMAC-SHA1、HMAC-SHA2、AES-XCBC

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402148

エラーメッセージ %FTD-3-402148: CRYPTO: Random Number Generator error

説明乱数ジェネレータ エラーが発生しました。

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

402149

エラーメッセージ %FTD-3-402149: CRYPTO: weak encryption type (*length*) . Operation disallowed. Not FIPS 140-2 compliant

説明 Firepower Threat Defense デバイスは、2048 ビット未満の RSA キーまたは DH グループ 1、2、または 5 を使用しようとしていました。

- *encryption type* : 暗号化タイプ
- *length* : RSA キー長または DH グループ番号

推奨アクション少なくとも 2048 ビットの RSA キーを使用するように Firepower Threat Defense デバイスまたは外部アプリケーションを設定するか、1、2、または 5 以外の DH グループを設定します。

402150

エラーメッセージ %FTD-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (*hash alg*) . Operation disallowed. Not FIPS 140-2 compliant

説明デジタル証明書の署名または FIPS 140-2 認定の検証に、許容できないハッシュ アルゴリズムが使用されています。

- *operation* : 署名または検証
- *hash alg* : 許容できないハッシュ アルゴリズムの名前

推奨アクション デジタル証明書の署名または FIPS 140-2 認定の検証に、最小限の許容可能なハッシュアルゴリズムを使用していることを確認します。SHA-256、SHA-384、およびSHA-512が含まれます。

403500

エラーメッセージ %FTD-6-403500: PPPoE - Service name 'any' not received in PADO.
Intf:interface_name AC:ac_name .

説明 Firepower Threat Defense デバイスが、インターネット サービス プロバイダーのアクセスコントローラからの PPPoE サービス *any* を要求しました。サービス プロバイダーからの応答には他のサービスが含まれていますが、サービス *any* は含まれていません。これは、プロトコルの実装の不一致です。PADO パケットは正常に処理されて、接続ネゴシエーションが続行されます。

推奨アクション 必要なし。

403501

エラーメッセージ %FTD-3-403501: PPPoE - Bad host-unique in PADO - packet dropped.
Intf:interface_name AC:ac_name

説明 Firepower Threat Defense デバイスは、ホスト固有値と呼ばれる ID をアクセスコントローラに送信しました。アクセスコントローラは、異なるホスト固有値で応答しました。Firepower Threat Defense デバイスはこの応答に対応する接続要求を識別できませんでした。パケットは廃棄され、接続ネゴシエーションは切断されました。

推奨アクション インターネット サービス プロバイダーにお問い合わせください。サービス プロバイダーのアクセス コントローラがホスト固有値の処理を誤っているか、または PADO パケットが不正です。

403502

エラーメッセージ %FTD-3-403502: PPPoE - Bad host-unique in PADS - dropping packet.
Intf:interface_name AC:ac_name

説明 Firepower Threat Defense デバイスは、ホスト固有値と呼ばれる ID をアクセスコントローラに送信しました。アクセスコントローラは、異なるホスト固有値で応答しました。Firepower Threat Defense デバイスはこの応答に対応する接続要求を識別できませんでした。パケットは廃棄され、接続ネゴシエーションは切断されました。

推奨アクション インターネット サービス プロバイダーにお問い合わせください。サービス プロバイダーのアクセス コントローラがホスト固有値の処理を誤っているか、または PADO パケットが不正です。

403503

エラーメッセージ %FTD-3-403503: PPPoE:PPP link down:reason

説明 PPP リンクがダウンしました。これが発生する原因は数多くあります。最初の形式に表示される理由は、PPP からの理由の場合です。

推奨アクション ネットワーク リンクを調べて、リンクが接続されていることを確認します。アクセス コンセントレータがダウンしていることがあります。認証プロトコルがアクセス コンセントレータと一致し、名前とパスワードが正しいことを確認します。ISP またはネットワーク サポート担当者にこの情報を確認します。

403504

エラーメッセージ %FTD-3-403504: PPPoE:No 'vpdn group *group_name* ' for PPPoE is created

説明 PPPoE では、PPPoE セッションを開始する前に、ダイヤルアウト コンフィギュレーションが必要です。一般的にコンフィギュレーションでは、ダイヤルポリシー、PPP 認証、ユーザー名、およびパスワードを指定する必要があります。次の例では、Firepower Threat Defense デバイスを PPPoE ダイヤルアウト用に設定します。my-username コマンドおよび my-password コマンドは、必要であれば PAP を使用して、アクセス コンセントレータの認証に使用されます。

次に例を示します。

```
ciscoftd# vpdn group my-pppoe request dialout pppoe
ciscoftd# vpdn group my-pppoe ppp authentication pap
ciscoftd# vpdn group my-pppoe localname my-username
ciscoftd# vpdn username my-username password my-password
ciscoftd# ip address outside pppoe setroute
```

推奨アクション PPPoE に VPDN グループを設定します。

403505

エラーメッセージ %FTD-4-403505: PPPoE:PPP - Unable to set default route to *IP_address* at *interface_name*

説明 通常、このメッセージには「default route already exists」というメッセージが続きます。

推奨アクション 現行のデフォルトルートを削除するか、または *setroute* パラメータを削除して、PPPoE と手動で設定したルートが競合しないようにします。

403506

エラーメッセージ %FTD-4-403506: PPPoE:failed to assign PPP *IP_address* netmask *netmask* at *interface_name*

説明 このメッセージには、「subnet is the same as interface」または「on failover channel」というメッセージのいずれかが続きます。

推奨アクション 最初の場合は、競合の原因となったアドレスを変更します。2 番目の場合は、フェールオーバー インターフェイス以外のインターフェイスに PPPoE を設定します。

403507

エラーメッセージ %FTD-3-403507: PPPoE:PPPoE client on interface *interface* failed to locate PPPoE vpdn group *group_name*

説明 `pppoe client vpdn group group_name` コマンドを入力して、インターフェイス上の PPPoE クライアントが特定の VPDN グループを使用するように設定できます。システムの起動時に、設定した名前の PPPoE VPDN グループが見つからなかった場合、このメッセージが生成されます。

- *interface* : どのインターフェイス上の PPPoE クライアントに障害が発生したか
- *group_name* : インターフェイス上の PPPoE クライアントの VPDN グループ名

推奨アクション 次の手順を実行します。

1. `vpdn group group_name` コマンドを入力して、必要な VPDN グループを追加します。グローバル コンフィギュレーション モードでダイヤルアウト PPPoE を要求し、すべてのグループ プロパティを追加します。
2. 指摘されたインターフェイスから `pppoe client vpdn group group_name` コマンドを削除します。この場合、PPPoE クライアントは、定義済みの最初の PPPoE VPDN グループを使用しようとします。



- (注) すべての変更内容は、`ip address pppoe` コマンドを入力してインターフェイス上の PPPoE クライアントを再起動した後に限り有効になります。

405001

エラーメッセージ %FTD-4-405001: Received ARP {request | response} collision from *IP_address* /*MAC_address* on interface *interface_name* with existing ARP entry *IP_address* /*MAC_address*

説明 Firepower Threat Defense デバイスが ARP パケットを受信しましたが、パケットの MAC アドレスが ARP キャッシュ エントリと異なります。

推奨アクション このトラフィックは、正当である場合もあれば、ARP ポイズニング攻撃が進行中であることを示す場合もあります。送信元 MAC アドレスを確認してパケットの送信元を判別し、そのパケットが有効なホストに属しているかどうかを調べます。

405002

エラーメッセージ %FTD-4-405002: Received mac mismatch collision from *IP_address* /*MAC_address* for authenticated host

説明 このパケットは、次のどちらかの条件の場合に表示されます。

- Firepower Threat Defense デバイスは IP アドレスが同じだが、MAC アドレスがその `uauth` エントリの 1 つとは異なるパケットを受信しました。

- Firepower Threat Defense デバイスに **vpnclient mac-exempt** コマンドを設定しました。除外 MAC アドレスを持つが、対応する uauth エントリとは異なる IP アドレスを持つパケットが Firepower Threat Defense デバイスによって受信されました。

推奨アクション このトラフィックは、正当である場合もあれば、スプーフィング攻撃が進行中であることを示す場合もあります。送信元 MAC アドレスと IP アドレスを確認してパケットの送信元と、そのパケットが有効なホストに属しているかどうかを調べます。

405003

エラーメッセージ %FTD-4-405003: IP address collision detected between host *IP_address* at *MAC_address* and interface *interface_name* , *MAC_address* .

説明 ネットワーク内のクライアントの IP アドレスが Firepower Threat Defense インターフェイス IP アドレスと同じです。

推奨アクション クライアントの IP アドレスを変更します。

405101

エラーメッセージ %FTD-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address *outside_address* [/*outside_port*] to local_address *inside_address* [/*inside_port*]

説明 モジュールが、接続の開始中に RAM システム メモリの割り当てに失敗したか、またはアドレス変換スロットを利用できません。

推奨アクション このメッセージが定期的に表示される場合は、無視できます。グローバルプールのサイズを確認して、内部のネットワーク クライアント数と比較できます。PAT アドレスが必要になる場合があります。または、変換と接続のタイムアウト間隔を短くします。このエラーメッセージは、メモリ不足が原因で表示される可能性もあります。その場合は、メモリ使用量を減らすか、または増設メモリを購入してみます。問題が解決しない場合、Cisco TAC にお問い合わせください。

405102

エラーメッセージ %FTD-4-405102: Unable to Pre-allocate H245 Connection for foreign_address *outside_address* [/*outside_port*] to local_address *inside_address* [/*inside_port*]

説明 Firepower Threat Defense デバイスが、接続の開始中に RAM システム メモリの割り当てに失敗したか、またはアドレス変換スロットを利用できません。

推奨アクション グローバルプールのサイズを確認し、内部のネットワーク クライアント数と比較します。PAT アドレスが必要になる場合があります。または、変換と接続のタイムアウト間隔を短くします。また、メモリ使用量を減らすか、または増設メモリを購入します。このメッセージが定期的に表示される場合は、無視できます。問題が解決しない場合、Cisco TAC にお問い合わせください。

405103

エラーメッセージ %FTD-4-405103: H225 message from *source_address/source_port* to *dest_address /dest_port* contains bad protocol discriminator *hex*

説明 Firepower Threat Defense デバイスはプロトコル識別子 0x08 を予測していますが、0x08 以外の識別子を受信しました。エンドポイントから不良パケットが送信されているか、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可能性があります。パケットの通過は許可されます。

推奨アクション 必要なし。

405104

エラーメッセージ %FTD-4-405104: H225 message received from *outside_address /outside_port* to *inside_address /inside_port* before SETUP

説明 初期 SETUP メッセージの前に H.225 メッセージを正しくない順序で受信しました。これは許可されません。Firepower Threat Defense デバイスは、その H.225 コールシグナリングチャネルに関する初期 SETUP メッセージを受信してから、他のすべての H.225 メッセージを受信する必要があります。

推奨アクション 必要なし。

405105

エラーメッセージ %FTD-4-405105: H323 RAS message AdmissionConfirm received from *source_address /source_port* to *dest_address /dest_port* without an AdmissionRequest

説明 ゲートキーパーから ACF が送信されましたが、Firepower Threat Defense デバイスはゲートキーパーに ARQ を送信していません。

推奨アクション 指摘された **source_address** のゲートキーパーを確認して、Firepower Threat Defense デバイス から ARQ を受信していないのに ACF が送信された理由を判定します。

406001

エラーメッセージ %FTD-4-406001: FTP port command low port: *IP_address /port* to *IP_address* on interface *interface_name*

説明 クライアントが FTP ポート コマンドを入力して、1024（通常はサーバポート専用の周知のポート範囲にある）より小さなポート番号を指定しました。これは、サイトセキュリティポリシーを回避しようとしていることを示します。Firepower Threat Defense デバイスは、パケットの廃棄、接続の終了、およびイベントの記録を行います。

推奨アクション 必要なし。

406002

エラーメッセージ %FTD-4-406002: FTP port command different address: IP_address (IP_address) to IP_address on interface interface_name

説明クライアントが FTP ポート コマンドを実行して、接続に使用されているアドレス以外のアドレスを指定しました。サイトセキュリティ ポリシーを回避しようとする試みが発生しました。たとえば、攻撃者が途中でパケットを変更し、正しいソース情報の代わりに別のソース情報を設定して FTP セッションをハイジャックしようとしている場合があります。Firepower Threat Defense デバイスは、パケットの廃棄、接続の終了、およびイベントの記録を行います。カッコ内のアドレスは、ポート コマンドからのアドレスです。

推奨アクション 必要なし。

407001

エラーメッセージ %FTD-4-407001: Deny traffic for local-host interface_name :inside_address, license limit of number exceeded

説明ホスト制限を超えました。次のどちらかの条件に当てはまる場合、内部ホストは制限にカウントされます。

- 内部ホストは、この 5 分以内に、Firepower Threat Defense デバイス経由でトラフィックを転送しました。
- 内部ホストは、Firepower Threat Defense デバイスで、xlate 接続またはユーザ認証を予約しました。

推奨アクション ホスト制限はローエンドプラットフォームに適用されます。ホスト制限を表示するには、**show version** コマンドを使用します。Firepower Threat Defense デバイスでのセッションを持つ現在のアクティブホストと内部ユーザを表示するには、**show local-host** コマンドを使用します。1 つまたは複数のユーザを強制的に切断するには、**clear local-host** コマンドを使用します。内部ユーザを制限になる前に期限切れにするには、xlate、接続、および uauth タイムアウトを次の表に示す推奨値以下に設定します。

表 1: 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 %FTD-4-407002: Embryonic limit nconns /elimit for through connections exceeded.outside_address /outside_port to global_address (inside_address)/inside_port on interface interface_name

説明指摘されたグローバルアドレスを経由して、指摘された外部アドレスから指摘されたローカルアドレスに接続された数が、そのスタティックの最大初期制限を超えました。Firepower Threat Defense デバイスは、接続にメモリが割り当て可能な場合は、その接続を受け入れようとし、ローカルホストに代わってプロキシホストとなり、SYN_ACK パケットを外部ホストに送信します。Firepower Threat Defense デバイスは、該当する状態情報を保持し、パケットを廃棄して、クライアントからの ACK を待ちます。このメッセージは、正当なトラフィックを示す場合もあれば、DoS 攻撃が進行中であることを示す場合もあります。

推奨アクション送信元アドレスを調べてパケットの送信元を判別し、それを有効なホストが送信しているかどうかを確認します。

407003

エラーメッセージ %FTD-4-407003: Established limit for RPC services exceeded number

説明 Firepower Threat Defense デバイスは、最大ホール数に達した後、すでに設定されている RPC サーバペアまたは RPC サービス ペアに対して、新規のホールをオープンしようとした。

推奨アクション他のホールがクローズされるのを待機するか（関連タイムアウト有効期限を使用）、またはサーバまたはサービスのアクティブ ペア数を制限します。

408001

エラーメッセージ %FTD-4-408001: IP route counter negative - reason , IP_address Attempt: number

説明 IP ルート カウンタを負の値に減少しようとしたが失敗しました。

推奨アクション `clear ip route` コマンドを入力して、ルート カウンタをリセットします。問題が解決しない場合、Cisco TAC にお問い合わせください。

408002

エラーメッセージ %FTD-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP :interface1 address2 netmask2 [distance2 /metric2] interface2

説明既存のルートよりも適切なメトリックを持つ同じ距離の別のインターフェイスからネットワークアップデートを受信しました。新規のルートによって、別のインターフェイスを使用してインストールされた既存のルートが上書きされます。新規のルートは冗長目的に限り使用され、ネットワーク内でパスが移動されたことを意味します。この変更は、トポロジと再配布を使用して制御する必要があります。この変更の影響を受ける既存の接続は、ディセーブルにさ

れる可能性があり、タイムアウトになります。このパスの移動は、パス冗長をサポートするようにネットワークトポロジが特に設計されている場合（このケースが予測されます）に限り発生します。

推奨アクション 必要なし。

408003

エラーメッセージ %FTD-4-408003: can't track this type of object hex

説明 トラッキングシステムのコンポーネントが、サポートしていないオブジェクトタイプを検出しました。STATE オブジェクトが予期されていました。

- *hex* : メモリ内の変数値またはアドレスを示す 16 進値

推奨アクション トラック オブジェクトを再設定して、STATE オブジェクトにします。

408101

エラーメッセージ %FTD-4-408101: KEYMAN : Type encryption_type encryption unknown. Interpreting keystring as literal.

説明 フォーマットタイプがシステムによって認識されませんでした。キー文字列形式タイプ値 0（暗号化されていないキー文字列）または 7（隠しキー文字列）の後にスペースを続けたものが、形式を示すために実際のキー文字列の前に置かれている可能性があります。システムは未知のタイプ値も受け付けますが、その場合は、暗号化されないキー文字列と見なされます。

推奨アクション 正しい形式のタイプ値を使用するか、タイプ値の後ろのスペースを削除します。

408102

エラーメッセージ %FTD-4-408102: KEYMAN : Bad encrypted keystring for key id key_id.

説明 暗号化されたキー文字列を正しく復号化できませんでした。システム設定時にキー文字列が破損した可能性があります。

推奨アクション key-string コマンドを再入力して、キー文字列をもう一度設定します。

409001

エラーメッセージ %FTD-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls

説明 ソフトウェアによって、予想外の状態が検出されました。ルータによって修正処置が行われ、続行されます。

推奨アクション 必要なし。

409002

エラーメッセージ %FTD-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。

推奨アクション必要なし。

409003

エラーメッセージ %FTD-4-409003: Received invalid packet: reason from IP_address , interface_name

説明無効な OSPF パケットを受信しました。詳細は、エラーメッセージに記載されています。原因は、送信側の誤った OSPF コンフィギュレーションか内部エラーの可能性あります。

推奨アクション受信側の OSPF コンフィギュレーションと送信側のコンフィギュレーションに不整合がないかを確認します。

409004

エラーメッセージ %FTD-4-409004: Received reason from unknown neighbor IP_address

説明 OSPF hello、データベース記述、またはデータベース要求パケットを受信しましたが、ルータは送信側を識別できません。

推奨アクション必要なし。

409005

エラーメッセージ %FTD-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name

説明 Firepower Threat Defense デバイスは、正常なヘッダー サイズよりも短いフィールド長の OSPF パケット、または到着した IP パケットのサイズと一致しない OSPF パケットを受信しました。これは、パケットの送信側のコンフィギュレーション エラーを示しています。

推奨アクション隣接アドレスから、問題のルータを特定しリブートします。

409006

エラーメッセージ %FTD-4-409006: Invalid lsa: reason Type number , LSID IP_address from IP_address , IP_address , interface_name

説明 LSA タイプが無効の LSA をルータが受信しました。原因は、ルータ上のメモリの破損または予想外の動作のどちらかです。

推奨アクション隣接アドレスから、問題のルータを特定しリブートします。問題が解決しない場合、Cisco TAC にお問い合わせください。

409007

エラーメッセージ %FTD-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。

推奨アクション エラー メッセージをそのままコピーし、Cisco TAC に報告してください。

409008

エラーメッセージ %FTD-4-409008: Found generating default LSA with non-zero mask LSA type: *number* Mask: *netmask* metric: *number* area: *string*

説明ルータが誤ったマスクでデフォルト LSA を生成しようとした。内部ソフトウェア エラーが発生したためにメトリックが間違っている可能性があります。

推奨アクション エラー メッセージをそのままコピーし、Cisco TAC に報告してください。

409009

エラーメッセージ %FTD-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID

説明 OSPF は、自分の 1 つのインターフェイスの IP アドレスからルータ ID を割り当てようとして、失敗しました。

推奨アクション IP アドレスが有効な動作中のインターフェイスが少なくとも 1 つあることを確認します。ルータで複数の OSPF プロセスが動作している場合、各プロセスは一意的ルータ ID を必要とします。十分な数のインターフェイスを動作させて、各プロセスがルータ ID を取得できるようにする必要があります。

409010

エラーメッセージ %FTD-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。

推奨アクション エラー メッセージをそのままコピーし、Cisco TAC に報告してください。

409011

エラーメッセージ %FTD-4-409011: OSPF detected duplicate router-id *IP_address* from *IP_address* on interface *interface_name*

説明 OSPF は、このルーティングプロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。

推奨アクション OSPF ルータ ID を一意にしてください。隣接ルータのルータ ID を変更します。

409012

エラーメッセージ %FTD-4-409012: Detected router with duplicate router ID *IP_address* in *area string*

説明 OSPF は、このルーティングプロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。

推奨アクション OSPF ルータ ID を一意にしてください。隣接ルータのルータ ID を変更します。

409013

エラーメッセージ %FTD-4-409013: Detected router with duplicate router ID *IP_address* in Type-4 LSA advertised by *IP_address*

説明 OSPF は、このルーティングプロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。

推奨アクション OSPF ルータ ID を一意にしてください。隣接ルータのルータ ID を変更します。

409014

エラーメッセージ %FTD-4-409014: No valid authentication send key is available on interface *nameif*.

説明 インターフェイスで設定されている認証キーが無効です。

推奨アクション 新しいキーを設定します。

409015

エラーメッセージ %FTD-4-409015: Key ID *key-id* received on interface *nameif*.

説明 設定されたキーチェーンで ID が見つかりません。

推奨アクション キー ID を使用して新しいセキュリティ アソシエーションを設定します。

409016

エラーメッセージ %FTD-4-409016: Key chain name *key-chain-name* on *nameif* is invalid.

説明 OSPF インターフェイスで設定されているキーチェーン名がグローバルキーチェーン設定と一致しません。

推奨アクション設定を修正します。OSPF 認証コマンドを削除するか、グローバル コンフィギュレーション モードでキーチェーンを設定してください。

409017

エラーメッセージ %FTD-4-409017: Key ID *key-id* in key chain *key-chain-name* is invalid.

説明 キーチェーンで設定されているキー ID が OSPF の範囲外です。これは、OSPF に関して許容されない範囲のキー ID 値をキーチェーンが許可するために発生する可能性があります。

推奨アクション 1 ~ 255 の範囲内のキー ID を使用して新しいセキュリティ アソシエーションを設定します。

409023

エラーメッセージ %FTD-4-409023: Attempting AAA Fallback method *method_name* for request_type request for user *user* :Auth-server group *server_tag* unreachable

説明 外部サーバに対する認証または認可の試行が失敗し、ローカル ユーザ データベースを使用して実行されます。

- **aaa_operation** : 認証または許可
- **username** : 接続に関連付けられているユーザ
- **server_group** : サーバが到達不能であった AAA サーバの名前

推奨アクション 最初の方法で設定された AAA サーバの接続性の問題を調査します。Firepower Threat Defense デバイスから認証サーバに対して ping を実行します。AAA サーバでデーモンが動作中であることを確認します。

409101

エラーメッセージ %FTD-4-409101: Received invalid packet: *s* from *P* , *s*

説明 無効な OSPF パケットを受信しました。詳細は、エラーメッセージに記載されています。原因は、OSPF の設定間違い、または送信側の内部エラーです。

推奨アクション 受信側と送信側の OSPF 設定に不整合がないかどうかを確認してください。

409102

エラーメッセージ %FTD-4-409102: Received packet with incorrect area from *P* , *s* , area *AREA_ID_STR* , packet area *AREA_ID_STR*

説明 OSPF パケットがこのインターフェイスの領域に一致しないエリア ID をヘッダーに受信しました。

推奨アクション 受信側と送信側の OSPF 設定に不整合がないかどうかを確認してください。

409103

エラーメッセージ %FTD-4-409103: Received s from unknown neighbor i

説明 OSPF hello、データベース記述、またはデータベース要求パケットを受信しましたが、ルータは送信側を識別できませんでした。

推奨アクション 必要なし。

409104

エラーメッセージ %FTD-4-409104: Invalid length d in OSPF packet type d from P (ID i), s

説明 OSPF パケットを受信しましたが、長さフィールドが通常のヘッダーサイズよりも短かったか、または受信時の IP パケットのサイズと整合性がありませんでした。パケットの送信側でエラーが発生しました。

推奨アクション 必要なし。

409105

エラーメッセージ %FTD-4-409105: Invalid lsa: s : Type 0x x , Length 0x x , LSID u from i

説明 ルータで LSA を受信しましたが、データが無効です。この LSA には、無効な LSA タイプ、不正なチェックサム、または誤った長さが含まれています。これはメモリの破損またはルータでの予期しない動作によるものです。

推奨アクション 隣接アドレスから、問題のルータを特定し、以下を実行します。

- **show running-config** コマンドを入力して、ルータの実行コンフィギュレーションを収集します。
- **show ipv6 ospf database** コマンドを入力し、エラーの内容を特定できるデータを収集します。
- **show ipv6 ospf database link-state-id** コマンドを入力します。link-state-id 引数には無効な LSA の IP アドレスを指定します。
- **show logging** コマンドを実行し、エラーの特定に役立つ情報を収集します。
- ルータを再起動します。

収集された情報からエラーの特定ができない場合は、Cisco TAC に連絡して、収集した情報を提出してください。

409106

エラーメッセージ %FTD-4-409106: Found generating default LSA with non-zero mask LSA type: 0x x Mask: i metric: lu area: AREA_ID_STR

説明 ルータが誤ったマスクでデフォルト LSA を生成しようとした。内部ソフトウェア エラーのためにメトリックが間違っている可能性があります。

推奨アクション 必要なし。

409107

エラーメッセージ %FTD-4-409107: OSPFv3 process *d* could not pick a router-id, please configure manually

説明 OSPFv3 は、自分の 1 つのインターフェイスの IP アドレスからルータ ID を割り当てようとして、失敗しました。

推奨アクション IP アドレスが有効な動作中のインターフェイスが少なくとも 1 つあることを確認します。ルータで複数の OSPF プロセスが動作している場合、各プロセスは一意的ルータ ID を必要とします。十分な数量のインターフェイスを稼働状態にして、それぞれがルータ ID を得られるようにします。

409108

エラーメッセージ %FTD-4-409108: Virtual link information found in non-backbone area: *AREA_ID_STR*

説明 内部エラーが発生しました。

推奨アクション 必要なし。

409109

エラーメッセージ %FTD-4-409109: OSPF detected duplicate router-id *i* from *P* on interface *IF_NAME*

説明 OSPF は、このルーティングプロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。OSPF ルータ ID は一意である必要があります。

推奨アクション ネイバー ルータ ID を変更します。

409110

エラーメッセージ %FTD-4-409110: Detected router with duplicate router ID *i* in area *AREA_ID_STR*

説明 OSPF は、このルーティングプロセスと同じルータ ID を持つ隣接ルータから hello パケットを受信しました。完全な隣接関係を確立できません。OSPF ルータ ID は一意である必要があります。

推奨アクション ネイバー ルータ ID を変更します。

409111

エラーメッセージ %FTD-4-409111: Multiple interfaces (*IF_NAME* / *IF_NAME*) on a single link detected.

説明同じリンク上の複数のインターフェイスで OSPFv3 をイネーブルにすることはサポートされていません。

推奨アクションOSPFv3 は、1本を除いたすべてのインターフェイスでディセーブルにするか、パッシブにする必要があります。

409112

エラーメッセージ %FTD-4-409112: Packet not written to the output queue

説明内部エラーが発生しました。

推奨アクション必要なし。

409113

エラーメッセージ %FTD-4-409113: Doubly linked list linkage is NULL

説明内部エラーが発生しました。

推奨アクション必要なし。

409114

エラーメッセージ %FTD-4-409114: Doubly linked list prev linkage is NULL x

説明内部エラーが発生しました。

推奨アクション必要なし。

409115

エラーメッセージ %FTD-4-409115: Unrecognized timer *d* in OSPF *s*

説明内部エラーが発生しました。

推奨アクション必要なし。

409116

エラーメッセージ %FTD-4-409116: Error for timer *d* in OSPF process *s*

説明内部エラーが発生しました。

推奨アクション必要なし。

409117

エラーメッセージ %FTD-4-409117: Can't find LSA database type x , area AREA_ID_STR , interface x

説明内部エラーが発生しました。

推奨アクション必要なし。

409118

エラーメッセージ %FTD-4-409118: Could not allocate DBD packet

説明内部エラーが発生しました。

推奨アクション必要なし。

409119

エラーメッセージ %FTD-4-409119: Invalid build flag x for LSA i , type 0x x

説明内部エラーが発生しました。

推奨アクション必要なし。

409120

エラーメッセージ %FTD-4-409120: Router-ID i is in use by ospf process d

説明 Firepower Threat Defense デバイス が別のプロセスで使用中のルータ ID を割り当てようとしてしました。

推奨アクション 1つのプロセスに対して別のルータ ID を設定します。

409121

エラーメッセージ %FTD-4-409121: Router is currently an ASBR while having only one area which is a stub area

説明 ASBR は AS External または NSSA LSA を伝送できる領域に接続する必要があります。

推奨アクション ルータの接続先となる領域を NSSA または通常の領域にします。

409122

エラーメッセージ %FTD-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.

説明仮想リンクが設定されました。仮想リンクが機能するためには、グローバル IPv6 アドレスが使用可能である必要があります。しかし、グローバル IPv6 アドレスがルータ上に見つかりませんでした。

推奨アクション このルータのインターフェイス上でグローバル IPv6 アドレスを設定します。

409123

エラーメッセージ %FTD-4-409123: Neighbor command allowed only on NBMA networks

説明 **neighbor** コマンドは NBMA ネットワークでのみ使用できます。

推奨アクション **neighbor** コマンドの設定オプションを確認し、ネイバー インターフェイスのオプションまたはネットワーク タイプを修正します。

409125

エラーメッセージ %FTD-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network

説明 設定されたネイバーは、ポイントツーマルチポイントネットワークで検出され、poll オプションまたは priority オプションが設定されました。これらのオプションは、NBMA タイプのネットワークにのみ使用できます。

推奨アクション **neighbor** コマンドの設定オプションを確認し、ネイバー インターフェイスのオプションまたはネットワーク タイプを修正します。

409128

エラーメッセージ %FTD-4-409128: OSPFv3-d Area AREA_ID_STR : Router i originating invalid type 0x x LSA, ID u , Metric d on Link ID d Link Type d

説明 このメッセージに示されたルータから無効なメトリックの LSA が送信されています。これがルータ LSA であり、リンク メトリックがゼロの場合、ネットワーク上にルーティング ループとトラフィック損失が存在する危険性があります。

推奨アクション 報告された LSA を送信したルータに、当該 LSA タイプおよびリンク タイプに有効なメトリックを設定します。

メッセージ 410001 ~ 450001

この章では、410001 から 450001 までのメッセージについて説明します。

410001

エラーメッセージ %FTD-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 パケットのドメイン名の長さが、255 バイトを超えています。詳細については、RFC 1035 の 3.1 項を参照してください。

推奨アクション必要なし。

411001

エラーメッセージ %FTD-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、ダウンからアップに変更されました。**interface_name** が論理インターフェイス名 (**inside** および **outside** など) の場合、このメッセージは、論理インターフェイス回線プロトコルが **down** から **up** に変化したことを示します。**interface_name** が物理インターフェイス名 (**Ethernet0** および **GigabitEthernet0/1** など) の場合、このメッセージは、物理インターフェイス回線プロトコルが **down** から **up** に変化したことを示します。

推奨アクション必要なし。

411002

エラーメッセージ %FTD-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、アップからダウンに変更されました。**interface_name** が論理インターフェイス名 (**inside** および **outside** など) の場合、このメッセージは、論理インターフェイス回線プロトコルが **up** から **down** に変化したことを示します。この場合、物理インターフェイス回線プロトコルのステータスは影響を受けません。**interface_name** が物理インターフェイス名 (**Ethernet0** および **GigabitEthernet0/1** など) の場合、このメッセージは、物理インターフェイス回線プロトコルが **up** から **down** に変化したことを示します。

推奨アクションこれがインターフェイス上の予期しないイベントの場合、物理回線を確認します。

411003

エラーメッセージ %FTD-4-411003: Configuration status on interface *interface_name* changed state to downup

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。

推奨アクションこれが予期しないイベントの場合は、物理回線を確認します。

411004

エラーメッセージ %FTD-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。

推奨アクション必要なし。

411005

エラーメッセージ %FTD-4-411005: Interface *variable 1* experienced a hardware transmit hang. The interface has been reset.

説明 インターフェイスでハードウェア送信フリーズが発生しました。フル動作にインターフェイスを復元するには、イーサネットコントローラのリセットが必要です。

- *variable 1* : GigabitEthernet0/0 などのインターフェイス名

推奨アクション 必要なし。

412001

エラーメッセージ %FTD-4-412001:MAC *MAC_address* moved from *interface_1* to *interface_2*

説明 あるモジュール インターフェイスから別のモジュール インターフェイスへのホスト移動が検出されました。透過 Firepower Threat Defense では、ホスト (MAC) と Firepower Threat Defense ポートの間のマッピングはレイヤ 2 転送テーブルに保持されています。このテーブルでは、パケットの送信元 MAC アドレスが 1 つの Firepower Threat Defense ポートにダイナミックにバインドされます。このプロセスでは、インターフェイス間でのホストの移動が検出されると常に、このメッセージが生成されます。

推奨アクション ホストの移動は、有効である場合もあれば、他のインターフェイス上のホスト MAC をスプーフィングしようとしている場合もあります。MAC スプーフィングの場合は、ネットワーク上の脆弱なホストを特定して削除するか、またはスタティック MAC エントリ (MAC アドレスおよびポートバインディングは変更できない) を設定します。ホストが正規に移動されている場合は、対処は不要です。

412002

エラーメッセージ %FTD-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いっぱいの場合に、さらに 1 つエントリを追加しようとしてしました。Firepower Threat Defense デバイスは、コンテキストごとに別個のレイヤ 2 転送テーブルを保持しており、コンテキストがサイズ制限を超えると常にこのメッセージが生成されます。MAC アドレスは追加されますが、テーブル内の最も古い既存のダイナミック エントリ (有効な場合) が置換されます。攻撃が行われようとした可能性があります。

推奨アクション 新規ブリッジテーブル エントリが有効であることを確認します。攻撃の場合には、EtherType ACL を使用して脆弱なホストへのアクセスを制御します。

413001

エラーメッセージ %FTD-4-413001: Module *module_id* is not able to shut down. Module Error: *errnum message*

説明 *module_id* で識別されるモジュールは、Firepower Threat Defense システム モジュールからのシャットダウンの要求に応じることができませんでした。ソフトウェアアップグレードのような中断できないタスクを実行していることがあります。**errnum** および **message** テキストに、モジュールをシャットダウンできなかった理由と推奨される修正処置が記載されています。

推奨アクション モジュール上のタスクが完了するのを待ってからモジュールをシャットダウンするか、または **session** コマンドを使用してモジュールの CLI にアクセスし、モジュールのシャットダウンを妨げているタスクを停止します。

413002

エラーメッセージ %FTD-4-413002: Module *module_id* is not able to reload. Module Error: *errnum message*

説明 *module_id* で識別されるモジュールは、Firepower Threat Defense モジュールからのリロードの要求に応じることができませんでした。ソフトウェアアップグレードのような中断できないタスクを実行していることがあります。**errnum** および **message** テキストに、モジュールをリロードできなかった理由と推奨される修正処置が記載されています。

推奨アクション モジュールのタスクが完了するのを待ってからモジュールをリロードするか、または **session** コマンドを使用してモジュールの CLI にアクセスし、モジュールのリロードを妨げているタスクを停止します。

413003

エラーメッセージ %FTD-4-413003: Module *string one* is not a recognized type

説明 有効なモジュール タイプとして認識されないモジュールが検出されました。

推奨アクション インストールされているモジュール タイプをサポートする Firepower Threat Defense ソフトウェアのバージョンにアップグレードします。

413004

エラーメッセージ %FTD-4-413004: Module *string one* failed to write software *newver* (currently *ver*), *reason* . Trying again.

説明 モジュールがソフトウェアバージョンに対応できませんでした。UNRESPONSIVE 状態に移行します。モジュール ソフトウェアのアップデートがさらに試行されます。

- >*string one* : モジュールを示すテキスト文字列
- >*newver* : モジュールへの書き込みが正常に終了しなかったソフトウェアの新しいバージョン番号 (1.0(1)0 など)
- >*ver* : モジュール上のソフトウェアの現在のバージョン番号 (1.0(1)0 など)
- >*reason* : 新しいバージョンがモジュールに書き込みできなかった原因。>*reason* に考えられる値は、次のとおりです。

- write failure

- failed to create a thread to write the image

推奨アクション必要なし。その後の試行で、アップデートの成功または失敗を示すメッセージが生成されます。その後のアップデート試行後の UP へのモジュール遷移を確認するには、**show module** コマンドを使用します。

413005

エラーメッセージ %FTD-4-413005: Module *module_id* , application is not supported *app_name* version *app_vers* type *app_type*

エラーメッセージ %FTD-4-413005: Module *prod_id* in slot *slot_num* , application is not supported *app_name* version *app_vers* type *app_type*

説明 スロット *slot_num* に設置されているモジュールが、サポートされていないアプリケーションバージョンまたはアプリケーションタイプを実行していました。

- *module_id* : ソフトウェア サービス モジュールの名前
- *prod_id* : 製品 ID 文字列
- *slot_num* : モジュールが搭載されているスロット番号。スロット 0 はシステムのメインボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。
- *app_name* : アプリケーション名 (文字列)
- *app_vers* : アプリケーションのバージョン (文字列)
- *app_type* : アプリケーションのタイプ (10 進数)

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

413006

エラーメッセージ %FTD-4-413006: *prod-id* Module software version mismatch; slot *slot* is *prod-id* version *running-vers* . Slot *slot* *prod-id* requires *required-vers* .

説明 スロット *slot* のモジュール上で動作しているソフトウェアのバージョンが、別のモジュールから要求されたバージョンではありませんでした。

- *slot* : スロット 0 はシステムのメインボードを示します。スロット 1 は拡張スロットに設置されているモジュールを示す。
- *prod_id* : スロット *slot* に設置されているデバイスの製品 ID 文字列
- *running_vers* : スロット *slot* に設置されているモジュール上で現在動作しているソフトウェアのバージョン
- *required_vers* : スロット *slot* のモジュールから要求されたソフトウェアのバージョン

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

414001

エラーメッセージ %FTD-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 ログモジュールによる外部 FTP サーバへのログバッファの保存が失敗しました。

推奨アクション失敗した原因に基づいて適切な処置を行います。

- プロトコルエラー：FTP サーバと Firepower Threat Defense デバイス との間の接続に問題がなく、FTP サーバが FTP PORT コマンドと PUT 要求を受け入れることができることを確認します。
- 無効なユーザ名またはパスワード：設定された FTP クライアントユーザ名およびパスワードが正しいことを確認します。
- 他のエラーすべて：問題が解決しない場合、Cisco TAC にお問い合わせください。

414002

エラーメッセージ %FTD-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: *filename* : [*fail_reason*]

説明 ロギング モジュールによるシステム フラッシュへのロギング バッファの保存が失敗しました。

推奨アクション 十分な領域がないために失敗した場合は、フラッシュの空き領域をチェックして、**logging flash-size** コマンドの設定制限が正しく設定されていることを確認します。エラーが、フラッシュファイルシステムの I/O エラーの場合は、Cisco TAC に問い合わせサポートを受けてください。

414003

エラーメッセージ %FTD-3-414003: TCP Syslog Server *intf* : *IP_Address* /*port* not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.

説明 リモート ホスト ロギング用の TCP syslog サーバが正常であり、サーバに接続され、新しい接続は logging permit-hostdown ポリシーに基づいて許可または拒否されます。logging permit-hostdown ポリシーが設定されている場合、新しい接続は許可されます。設定されていない場合、新しい接続は拒否されます。

- *intf* : サーバが接続されている Firepower Threat Defense デバイス のインターフェイス
- *IP_Address* : リモート TCP syslog サーバの IP アドレス
- *port* : リモート TCP syslog サーバのポート

推奨アクション 設定されている TCP syslog サーバが動作していることを確認します。新しい接続を許可するには、logging permit-hostdown ポリシーを設定します。新しい接続を拒否するには、logging permit-hostdown ポリシーを設定しません。

414005

エラーメッセージ %FTD-3-414005: TCP Syslog Server *intf* : *IP_Address* /*port* connected, New connections are permitted based on logging permit-hostdown policy

説明 リモート ホスト ロギング用の TCP syslog サーバが正常であり、サーバに接続され、新しい接続は logging permit-hostdown ポリシーに基づいて許可されます。logging permit-hostdown ポリシーが設定されている場合、新しい接続は許可されます。

- *intf*: サーバが接続されている Firepower Threat Defense デバイスのインターフェイス
- *IP_Address*: リモート TCP syslog サーバの IP アドレス
- *port*: リモート TCP syslog サーバのポート

推奨アクション 必要なし。

414006

エラーメッセージ %FTD-3-414006: TCP Syslog Server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.

説明 ロギングキューが設定された上限に近づいているため、syslogメッセージが廃棄される危険があります。

推奨アクション この状況を回避するためにキュー サイズを調整する方法の詳細については、CLI 構成ガイドの「Configuring the Logging Queue」の項を参照してください。この場合に新しい接続を拒否するには、**no logging permit-hostdown** コマンドを使用します。この場合に新しい接続を許可するには、**logging permit-hostdown** コマンドを使用します。

415020

エラーメッセージ %FTD-5-415020: HTTP - matched *matched_string* in policy-map *map_name* , a non-ASCII character was matched *connection_action* from *int_type* :*IP_address* /*port_num* to *int_type* :*IP_address* /*port_num*

説明 非 ASCII 文字が見つかりました。

- **matched_string**: 次のいずれかの一致文字列

- クラス マップ ID とその後に続くクラス マップ名。この文字列は、ユーザ設定のクラス マップの場合に表示されます。

- このメッセージを発生させた実際の **match** コマンド。この文字列は、クラス マップが内部の場合に表示されます。

- *map_name*: ポリシー マップの名前
- *connection_action*: 接続をドロップまたはリセットします
- *interface_type*: インターフェイス タイプ (たとえば、DMZ または外部)
- *IP_address*: インターフェイスの IP アドレス
- *port_num*: ポート番号

推奨アクション **match {request|response} header non-ascii** コマンドを入力して、問題を修正します。

417001

エラーメッセージ %FTD-4-417001: Unexpected event received: *number*

説明 プロセスで信号を受信しましたが、イベントのハンドラが見つかりませんでした。

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

417004

エラーメッセージ %FTD-4-417004: Filter violation error: conn number (string :string) in string

説明クライアントが、自分が所有していないルート属性を修正しようとした。

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

417006

エラーメッセージ %FTD-4-417006: No memory for string) in string . Handling: string

説明メモリ不足のために動作が失敗しましたが、別のメカニズムで処理されます。

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

418001

エラーメッセージ %FTD-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string from interface_name IP_address (port) [(idfw_user |FQDN_string], sg_info)] to interface_name IP_address (port) [(idfw_user |FQDN_string), sg_info]

説明指摘された送信元から宛先へのパケットが、Firepower Threat Defense デバイス と管理専用ネットワークとの間を経由していたために、廃棄されました。

- **protocol_string** : TCP、UDP、ICMP、または 10 進数のプロトコル ID
- **interface_name** : インターフェイス名
- **IP_address** : IP アドレス
- **port** : ポート番号
- **sg_info** : 指定した IP アドレスのセキュリティ グループ名またはタグ

推奨アクションこのようなパケットを生成している個人と理由を特定します。

419001

エラーメッセージ %FTD-4-419001: Dropping TCP packet from src_ifc :src_IP /src_port to dest_ifc :dest_IP /dest_port , reason : MSS exceeded, MSS size , data size

説明 TCP パケットの長さが 3 ウェイ ハンドシェイクでアダバタイズされた MSS を超えました。

- >**src_ifc** : 入力インターフェイス名
- >**src_IP** : パケットの送信元 IP アドレス
- >**src_port** : パケットの送信元ポート
- >**dest_ifc** : 出力インターフェイス名
- >**dest_IP** : パケットの宛先 IP アドレス

- `>dest_port` : パケットの宛先ポート

推奨アクション MSS を超えるパケットを許可する必要がある場合は、`exceed-mss` コマンドを使用して TCP マップを作成します。次に例を示します。

```
ciscoftd# access-list http-list permit tcp any host server_ip eq 80
ciscoftd# class-map http
ciscoftd# match access-list http-list
ciscoftd# tcp-map tmap
ciscoftd# exceed-mss allow
ciscoftd# policy-map global_policy
ciscoftd# class http
ciscoftd# set connection advanced-options tmap
```

419002

エラーメッセージ %FTD-4-419002: Received duplicate TCP SYN from `in_interface :src_address /src_port` to `out_interface :dest_address /dest_port` with different initial sequence number.

説明 3 ウェイ ハンドシェイク中に、初期接続を開いた SYN とは異なる初期シーケンス番号を持つ重複 TCP SYN を受信しました。これは、SYN がスプーフィングされていることを示している可能性があります。このメッセージは、リリース 7.0.4.1 以降で表示されます。

- `in_interface` : 入力インターフェイス
- `src_address` : パケットの送信元 IP アドレス
- `src_port` : パケットの送信元ポート
- `out_interface` : 出力インターフェイス
- `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

推奨アクション 必要なし。

419003

エラーメッセージ %FTD-4-419003: Cleared TCP urgent flag from `out_ifc :src_ip /src_port` to `in_ifc :dest_ip /dest_port`.

説明 3 ウェイ ハンドシェイク中に、初期接続を開いた SYN とは異なる初期シーケンス番号を持つ重複 TCP SYN を受信しました。これは、SYN がスプーフィングされていることを示している可能性があります。このメッセージは、リリース 7.0.4.1 以降で表示されます。

- `in_ifc` : 入力インターフェイス
- `src_ip` : パケットの送信元 IP アドレス
- `src_port` : パケットの送信元ポート
- `out_ifc` : 出力インターフェイス
- `dest_ip` : パケットの宛先 IP アドレス
- `dest_port` : パケットの宛先ポート

推奨アクション TCP ヘッダー内の緊急フラグを保持する必要がある場合は、TCP マップ コンフィギュレーション モードで **urgent-flag allow** コマンドを使用します。

エラーメッセージ %FTD-7-419003: Cleared TCP urgent flag.

説明 この syslog は、緊急フラグまたは tcp パケットの緊急ポインタがクリアされたときに表示されます。これは、ユーザ設定 (tcp-map) によるものか、または tcp パケット内に緊急ポインタ用の値があるが、緊急フラグが設定されていないことが原因である可能性があります。

推奨アクション 緊急フラグが clear に設定されているかどうか tcp-map 設定を確認します。

419004

エラーメッセージ %FTD-6-419004: TCP connection ID from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port is probed by DCD

説明

TCP 接続がデッド接続検出 (DCD) によってプローブされ、接続がまだ有効かどうか判断されました。

推奨アクション なし。

419005

エラーメッセージ %FTD-6-419005: TCP connection ID from src_ifc:src_ip/src_port duration hh:mm:ss data bytes, is kept open by DCD as valid connection

説明

TCP 接続は、デッド接続検出 (DCD) によって有効な接続として開かれたままにされました。

推奨アクション なし。

419006

エラーメッセージ %FTD-6-419006: TCP connection ID from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port duration hh:mm:ss data bytes, DCD probe was not responded from client/server interface ifc_name

説明

TCP 接続は、不要になったため、デッド接続検出 (DCD) によって閉じられました。

推奨アクション なし。

421005

エラーメッセージ %FTD-6-421005: interface_name :IP_address is counted as a user of application

説明ホストがライセンス制限の対象と見なされています。指摘されたホストが、**application** のユーザと見なされました。ライセンス検証のために、24時間のユーザの総数が午前0時に計算されます。

- **interface_name** : インターフェイス名
- **IP_address** : IP アドレス
- **application** : CSC SSM

推奨アクション必要なし。ただし、全体の数が、購入したユーザライセンスを超える場合は、Cisco TAC に連絡してライセンスをアップグレードしてください。

421007

エラーメッセージ %FTD-3-421007: TCP|UDP flow from *interface_name* :*IP_address* /*port* to *interface_name* :*IP_address* /*port* is skipped because *application* has failed.

説明サービス モジュールのアプリケーションに障害が発生したためにフローがスキップされました。デフォルトでは、このメッセージは 10 秒に 1 回しか表示されないように制限されています。

- **IP_address** : IP アドレス
- **port** : ポート番号
- **interface_name** : ポリシーが適用されているインターフェイスの名前
- **application** : CSC SSM

推奨アクション サービス モジュールで問題を特定します。

422004

エラーメッセージ %FTD-4-422004: IP SLA Monitor *number0* : Duplicate event received. Event number *number1*

説明 IP SLA モニタ プロセスが、重複したイベントを受信しました。現在、このメッセージは破棄イベントに適用されます。1 つの破棄要求だけが適用されます。これは警告専用メッセージです。

- *number0* : SLA 動作番号
- *number1* : SLA 動作のイベント ID

推奨アクションこのメッセージが繰り返し表示される場合は、**show sla monitor configuration SLA_operation_id** コマンドを入力して、コマンドの出力をコピーします。コンソールまたはシステム ログに表示されるメッセージをそのままコピーします。その後 Cisco TAC にお問い合わせのうえ、収集した情報と、SLA プロブを設定およびポーリングしているアプリケーションに関する情報を TAC の担当者にご提供ください。

422005

エラーメッセージ %FTD-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.

説明 システム クロックが設定されていなかったため、1 つまたは複数の IP SLA モニタ プロブをスケジュールできません。

推奨アクション システム クロックが NTP または別のメカニズムを使用して機能できることを確認します。

422006

エラーメッセージ %FTD-4-422006: IP SLA Monitor Probe number : *string*

説明 IP SLA モニタ プロブをスケジュールできません。設定された開始時刻がすでに過ぎてしまっているか、開始時刻が無効です。

- *number* : SLA 動作 ID
- *string* : エラーを説明する文字列

推奨アクション 無効な開始時刻を持つ失敗したプロブを再度スケジュールします。

424001

エラーメッセージ %FTD-4-424001: Packet denied *protocol_string* *intf_in* :*src_ip* /*src_port* [[*idfw_user* | *FQDN_string*], *sg_info*)] *intf_out* :*dst_ip* /*dst_port* [[*idfw_user* | *FQDN_string*], *sg_info*)]. [Ingress|Egress] interface is in a backup state.

説明 パケットが、Firepower Threat Defense デバイス と冗長インターフェイスとの間を経由しているために、廃棄されました。ローエンドプラットフォームでは、インターフェイス機能が制限されます。 **backup interface** コマンドで指定されているインターフェイスは、設定されているプライマリ インターフェイスのバックアップになることしかできません。プライマリ インターフェイスへのデフォルト ルートがアップしている場合は、バックアップ インターフェイスからの Firepower Threat Defense デバイス 経由トラフィックはすべて拒否されます。逆に、プライマリ インターフェイスへのデフォルト ルートがダウンしている場合は、プライマリ インターフェイスからの Firepower Threat Defense デバイス 経由トラフィックが拒否されます。

- *protocol_string* : プロトコル文字列 (たとえば、TCP または 10 進数のプロトコル ID)
- *intf_in* : 入力インターフェイス名
- *src_ip* : パケットの送信元 IP アドレス
- *src_port* : パケットの送信元ポート
- *intf_out* : 出力インターフェイス名
- *dst_ip* : パケットの宛先 IP アドレス
- *dst_port* : パケットの宛先ポート
- *sg_info* : 指定した IP アドレスのセキュリティ グループ名またはタグ

推奨アクション 拒否されたパケットの送信元を特定します。

424002

エラーメッセージ %FTD-4-424002: Connection to the backup interface is denied:
protocol_string *intf* :*src_ip* /*src_port* *intf* :*dst_ip* /*dst_port*

説明接続がバックアップ状態であったために、その接続が廃棄されました。ローエンドプラットフォームでは、インターフェイス機能が制限されます。バックアップインターフェイスは、**backup interface** コマンドで指定されているプライマリ インターフェイスのバックアップになることしかできません。プライマリ インターフェイスへのデフォルト ルートがアップしている場合は、バックアップインターフェイス経由のFirepower Threat Defense デバイスへの接続はすべて拒否されます。逆に、プライマリ インターフェイスへのデフォルト ルートがダウンしている場合は、プライマリ インターフェイス経由のFirepower Threat Defense デバイスへの接続が拒否されます。

- *protocol_string* : プロトコル文字列 (たとえば、TCP または 10 進数のプロトコル ID)
- *intf_in* : 入力インターフェイス名
- *src_ip* : パケットの送信元 IP アドレス
- *src_port* : パケットの送信元ポート
- *intf_out* : 出力インターフェイス名
- *dst_ip* : パケットの宛先 IP アドレス
- *dst_port* : パケットの宛先ポート

推奨アクション拒否されたパケットの送信元を特定します。

425001

エラーメッセージ %FTD-6-425001 Redundant interface *redundant _interface_name* created.

説明指摘された冗長インターフェイスがコンフィギュレーションに作成されました。

- *redundant_interface_name* : 冗長インターフェイス名

推奨アクション必要なし。

425002

エラーメッセージ %FTD-6-425002 Redundant interface *redundant _interface_name* removed.

説明指摘された冗長インターフェイスがコンフィギュレーションから削除されました。

- *redundant_interface_name* : 冗長インターフェイス名

推奨アクション必要なし。

425003

エラーメッセージ %FTD-6-425003 Interface *interface_name* added into redundant interface *redundant _interface_name* .

説明指摘された物理インターフェイスがメンバーインターフェイスとして、指摘された冗長インターフェイスに追加されました。

- *interface_name* : インターフェイス名
- *redundant_interface_name* : 冗長インターフェイス名

推奨アクション必要なし。

425004

エラーメッセージ %FTD-6-425004 Interface *interface_name* removed from redundant interface *redundant_interface_name* .

説明指摘された冗長インターフェイスが、指摘された冗長インターフェイスから削除されました。

- *interface_name* : インターフェイス名
- *redundant_interface_name* : 冗長インターフェイス名

推奨アクション必要なし。

425005

エラーメッセージ %FTD-5-425005 Interface *interface_name* become active in redundant interface *redundant_interface_name*

説明冗長インターフェイスでは、1つのメンバーインターフェイスがアクティブなメンバーとなります。トラフィックは、アクティブなメンバーインターフェイスだけを通過します。指摘された物理インターフェイスが、指摘された冗長インターフェイスのアクティブなメンバーになりました。次のいずれかが当てはまる場合、メンバーインターフェイスの切り替えが行われます。

- **redundant-interface interface-name active-member interface-name** コマンドが実行された。
 - スタンバイ メンバー インターフェイスがアップ状態であるときに、アクティブなメンバー インターフェイスがダウンした。
 - アクティブなメンバーインターフェイスがダウン状態のままであるときに、スタンバイ メンバー インターフェイスが（ダウンから）アップ状態になった。
- *interface_name* : インターフェイス名
 - *redundant_interface_name* : 冗長インターフェイス名

推奨アクション メンバー インターフェイスのステータスを確認します。

425006

エラーメッセージ %FTD-3-425006 Redundant interface *redundant_interface_name* switch active member to *interface_name* failed.

説明メンバー インターフェイスの切り替えが試行されたときにエラーが発生しました。

- *redundant_interface_name* : 冗長インターフェイス名
- *interface_name* : インターフェイス名

推奨アクション問題が解決しない場合、Cisco TAC にお問い合わせください。

426001

エラーメッセージ %FTD-6-426001: PORT-CHANNEL:Interface *ifc_name* bundled into EtherChannel interface Port-channel *num*

説明 **interface port-channel *num*** または **channel-group *num* mode *mode*** コマンドが存在しないポートチャネルに対して使用されました。

- *ifc_name* : EtherChannel インターフェイス名
- *num* : ポートチャネル番号

推奨アクション必要なし。

426002

エラーメッセージ %FTD-6-426002: PORT-CHANNEL:Interface *ifc_name* unbundled from EtherChannel interface Port-channel *num*

説明 **no interface port-channel *num*** コマンドが使用されました。

- *ifc_name* : EtherChannel インターフェイス名
- *num* : ポートチャネル番号

推奨アクション必要なし。

426003

エラーメッセージ %FTD-6-426003: PORT-CHANNEL:Interface *ifc_name1* has become standby in EtherChannel interface Port-channel *num*

説明 **channel-group *num* mode *mode*** コマンドが使用されました。

- *ifc_name1* : EtherChannel インターフェイス名
- *num* : ポートチャネル番号

推奨アクション必要なし。

426004

エラーメッセージ %FTD-4-426004: PORT-CHANNEL: Interface *ifc_name1* is not compatible with *ifc_name* and will be suspended (speed of *ifc_name1* is X Mbps, Y is 1000 Mbps).

エラーメッセージ %FTD-4-426004: Interface *ifc_name1* is not compatible with *ifc_name1* and will be suspended (*ifc_name1* is Full-duplex, *ifc_name1* is Half-duplex)

説明 **channel-group *num* mode *mode*** コマンドが物理インターフェイスに対して実行され、この物理インターフェイスとポートチャネルの速度またはデュプレックスに不一致があります。

- *ifc_name* : ポートチャネルに追加しようとしているインターフェイス
- *ifc_name1* : ポートチャネル中にすでに存在しバンドル状態になっているインターフェイス

推奨アクション次のいずれかを実行します。

- 物理インターフェイスの速度をポートチャンネルの速度に変更し、**channel-group num mode mode** コマンドを再実行します。
- メンバー インターフェイスを中断状態のままにします。最後のアクティブ メンバーを削除すると、そのメンバーは中断されたメンバー上で LACP を再確立しようとします。

426101

エラーメッセージ %FTD-6-426101: PORT-CHANNEL:Interface *ifc_name* is allowed to bundle into EtherChannel interface *port-channel id* by CLACP

説明ポートが span-cluster チャンネル グループにバンドルされています。

推奨アクション必要なし。

426102

エラーメッセージ %FTD-6-426102: PORT-CHANNEL:Interface *ifc_name* is moved to standby in EtherChannel interface *port-channel id* by CLACP

説明ポートが span-cluster チャンネル グループでホットスタンバイ状態に移行しました。

推奨アクション必要なし。

426103

エラーメッセージ %FTD-6-426103: PORT-CHANNEL:Interface *ifc_name* is selected to move from standby to bundle in EtherChannel interface *port-channel id* by CLACP

説明スタンバイ ポートが span-cluster チャンネル グループでバンドル状態への移行対象として選択されました。

推奨アクション必要なし。

426104

エラーメッセージ %FTD-6-426104: PORT-CHANNEL:Interface *ifc_name* is unselected in EtherChannel interface *port-channel id* by CLACP

説明他のポートをバンドルするための領域を取得するために、バンドル ポートが span-cluster チャンネル グループでバンドル解除されました。

推奨アクション必要なし。

428002

エラーメッセージ %FTD-6-428002: WAAS confirmed from *in_interface :src_ip_addr/src_port* to *out_interface :dest_ip_addr/dest_port* , inspection services bypassed on this connection.

説明接続で WAAS 最適化が検出されました。WAAS 最適化接続では、すべてのレイヤ 7 検査サービス (IPS を含む) がバイパスされます。

推奨アクション ネットワークに WAE デバイスが含まれている場合、処置は不要です。それ以外の場合、ネットワーク管理者は、この接続での WAAS オプションの使用を調査する必要があります。

429008

エラーメッセージ %FTD-4-429008: Unable to respond to VPN query from CX for session 0x%x
. Reason %s

説明 CX は VPN セッション クエリを Firepower Threat Defense デバイス に送信しましたが、無効なセッション ID または別の理由により応答しませんでした。妥当な原因には次のいずれかが考えられます。

- TLV の長さが無効である
- TLV のメモリ割り当てに失敗した
- VPN セッション クエリ メッセージのエンキューに失敗した
- VPN セッション ID が無効である

推奨アクション 必要なし。

430001

このメッセージ番号はリリース 6.3 で導入されました。これによって侵入イベントが識別されます。

これとその他のセキュリティイベントに関するメッセージの詳細については、[セキュリティイベントの Syslog メッセージ](#)を参照してください。

430002

このメッセージ番号はリリース 6.3 で導入されました。これによって接続の開始時に記録された接続イベントが識別されます。

これとその他のセキュリティイベントに関するメッセージの詳細については、[セキュリティイベントの Syslog メッセージ](#)を参照してください。

430003

このメッセージ番号はリリース 6.3 で導入されました。これによって接続の終了時に記録された接続イベントが識別されます。

これとその他のセキュリティイベントに関するメッセージの詳細については、[セキュリティイベントの Syslog メッセージ](#)を参照してください。

430004

このメッセージ番号はリリース 6.4 で導入されました。これによってファイルイベントが識別されます。ファイルマルウェアイベントについては、[430005 \(46 ページ\)](#) も参照してください。

これとその他のセキュリティイベントに関するメッセージの詳細については、[セキュリティイベントの Syslog メッセージ](#)を参照してください。

430005

このメッセージ番号はリリース 6.4 で導入されました。これによってマルウェアイベントが識別されます。ファイルイベントについては、[430004 \(46 ページ\)](#) も参照してください。

これとその他のセキュリティイベントに関するメッセージの詳細については、[セキュリティイベントの Syslog メッセージ](#)を参照してください。

4302310

エラーメッセージ %FTD-5-4302310: Sctp packet received from *src_ifc:src_ip/src_port* to *dst_ifc:dst_ip/dst_port* contains unsupported Hostname Parameter.

説明 init/init-ack パケットはホスト名パラメータで受信されます。

- **packet init/init-ack** : ホスト名パラメータを送信するメッセージ
- **src-ifc** : 入力インターフェイスを示します
- **src-ip/src-port** : パケットの送信元 IP とポートを示します
- **dst-ifc** : 出力インターフェイスを示します
- **dst_ip/dst_port** : パケットの送信元 IP とポートを示します

推奨アクション ホスト名ではなく、エンドポイントの実際の IP アドレスを使用します。ホスト名パラメータを無効にします。

434001

エラーメッセージ %FTD-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from *ingress interface:source IP address /source port* to *egress interface :destination IP address /destination port*

説明 モジュールのフェールクローズ設定のためにパケットがドロップされました。フェールクローズ設定は、モジュールがダウンしている場合にすべてのフローをドロップするように設計されているため、すべてのフローの接続が失われるのは、それらのフローがモジュールにリダイレクトされることが原因です。

推奨アクション 障害の原因を把握し、サービスを復元します。または、カードがすぐに回復しなくても、フェールオープンオプションを使用できます。フェールオープン設定では、カードのステータスがダウンしている場合、モジュールへのすべてのパケットはバイパスされます。

434004

エラーメッセージ %FTD-5-434004: SFR requested FTD to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally

説明 SourceFire (SFR) は、これ以上フロー トラフィックを検査しないことを決定し、SFR へのトラフィックのフローをリダイレクトすることを停止するように Firepower Threat Defense デバイスに要求します。

推奨アクション 必要なし。

446003

エラーメッセージ %FTD-4-446003: Denied TLS Proxy session from *src_int* :*src_ip* /*src_port* to *dst_int* :*dst_ip* /*dst_port* , UC-IME license is disabled.

説明 UC-IME ライセンスがオンまたはオフです。UC-IME は、いったんイネーブルにすると、Firepower Threat Defense の制限および K8 エクスポート制限に従って、使用可能な TLS セッションをいくつでも使用できます。

- *src_int* : 送信元インターフェイス名 (inside または outside)
- *src_ip* : 送信元 IP アドレス
- *src_port* : 送信元ポート
- *dst_int* : 宛先インターフェイス名 (inside または outside)
- *dst_ip* : 宛先 IP アドレス
- *dst_port* : 宛先ポート

推奨アクション UC-IME が無効になっているかどうかを確認します。無効になっている場合は有効にします。

447001

エラーメッセージ %FTD-4-447001: ASP DP to CP *queue_name* was full. Queue length *length* , limit *limit*

説明 このメッセージは、Control Point (CP; コントロールポイント) イベントキューへの特定の Data Path (DP; データパス) がいっぱいになり、1つまたは複数のエンキューアクションが失敗したことを示します。イベントに CP アプリケーションインスペクション用などのパケットブロックが含まれる場合、パケットは DP によって廃棄され、**show asp drop** コマンドからのカウンタが増加します。イベントが CP へのパント用の場合、[Punt no memory] ASP 廃棄カウンタが標準カウンタとして使用されます。

- *queue* : DP-CP イベントキューの名前。
- *length* : キューにある現在のイベント数。
- *limit* : キューで許容されるイベントの最大数。

推奨アクション キューがいっぱいの状態は、CP に対する負荷が CP 処理能力を超えていることを示します。これは、一時的な状態の場合もあれば、そうでない場合もあります。このメッセージが繰り返し表示される場合は、CP に対する機能負荷を軽減することを検討してください

い。**show asp event dp-cp** コマンドを使用して、イベント キューの負荷に最も影響を及ぼしている機能を特定できます。

448001

エラーメッセージ %FTD-4-448001: Denied SRTP crypto session setup on flow from *src_int* :*src_ip* /*src_port* to *dst_int* :*dst_ip* /*dst_port* , licensed K8 SRTP crypto session of *limit* exceeded

説明 K8 プラットフォームでは、250 個の SRTP 暗号化セッションの制限が適用されます。SRTP の暗号化または復号化セッションのペアは、1 個の SRTP 暗号化セッションとしてカウントされます。コールがこの制限に対してカウントされるのは、メディアで暗号化または復号化が必要な場合のみです。つまり、コールに対してパススルーが設定されている場合、両方のレッグが SRTP を使用する場合でも、この制限に対してカウントされません。

- *src_int* : 送信元インターフェイス名 (inside または outside)
- *src_ip* : 送信元 IP アドレス
- *src_port* : 送信元ポート
- *dst_int* : 宛先インターフェイス名 (inside または outside)
- *dst_ip* : 宛先 IP アドレス
- *dst_port* : 宛先ポート
- *limit* : SRTP 暗号化セッション (250) の K8 制限

推奨アクション 必要なし。既存の SRTP 暗号化セッションが解放された場合のみ新しい SRTP 暗号化セッションを設定できます。