Syslog メッセージ 722001 ～ 776254

この章は、次の項で構成されています。

メッセージ 722001 ～ 722056

この項では、722001 から 722056 までのメッセージについて説明します。

722001

エラーメッセージ `%Threat Defense-4-722001: IP IP_address Error parsing SVC connect request.`

説明 SVC からの要求が無効でした。

説明 必要に応じて調査を実施し、このエラーの原因が SVC の障害であるか、互換性のない SVC バージョンであるか、デバイスに対する攻撃であるかを確認します。

722002

エラーメッセージ `%Threat Defense-4-722002: IP IP_address Error consolidating SVC connect request.`

説明アクションを実行するための十分なメモリがありません。

推奨アクション増設メモリを購入するか、デバイスをアップグレードするか、デバイスの負荷を減らします。

722003

エラーメッセージ `%Threat Defense-4-722003: IP IP_address Error authenticating SVC connect request.`

説明ユーザーがダウンロードおよび接続にかける時間が長すぎました。

推奨アクションセッションのアイドルタイムアウトおよび最大接続時間の値を大きくします。

722004

エラーメッセージ `%Threat Defense-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.`

説明アクションを実行するための十分なメモリがありません。

推奨アクション増設メモリを購入するか、デバイスをアップグレードするか、デバイスの負荷を減らします。

722005

エラーメッセージ `%Threat Defense-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.`

説明アクションを実行するための十分なメモリがありません。

推奨アクション増設メモリを購入するか、デバイスをアップグレードするか、デバイスの負荷を減らします。

722006

エラーメッセージ `%Threat Defense-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection.`

説明無効なアドレスがユーザーに割り当てられました。

推奨アクション可能であれば、アドレスの割り当てを確認し、修正します。そうでなければ、ネットワーク管理者に連絡するか、またはセキュリティポリシーに従ってこの問題の解決を依頼します。さらにサポートが必要な場合は、Cisco TAC にお問い合わせください。

722007

エラーメッセージ `%Threat Defense-3-722007: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722008

エラーメッセージ `%Threat Defense-3-722008: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message`

説明 SVC がメッセージを発行しました。

• **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722009

エラーメッセージ `%Threat Defense-3-722009: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message`

説明 SVC がメッセージを発行しました。

• **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722010

エラーメッセージ `%Threat Defense-5-722010: Group group User user-name IP IP_address SVC Message: type-num /NOTICE: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

- **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722011

エラーメッセージ `%Threat Defense-5-722011: Group group User user-name IP IP_address SVC Message: type-num /NOTICE: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

- **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722012

エラーメッセージ `%Threat Defense-5-722012: Group group User user-name IP IP_address SVC Message: type-num /INFO: message`

説明 SVC がメッセージを発行しました。

• **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722013

エラーメッセージ `%Threat Defense-6-722013: Group group User user-name IP IP_address SVC Message: type-num /INFO: message`

説明 SVC がメッセージを発行しました。

• **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722014

エラーメッセージ `%Threat Defense-6-722014: Group group User user-name IP IP_address SVC Message: type-num /INFO: message`

説明 SVC がメッセージを発行しました。

• **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722015

エラーメッセージ `%Threat Defense-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num`

説明 SVC が、無効なフレーム タイプをデバイスに送信しました。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

• **type-num**：フレーム タイプの ID 番号

推奨アクション SVC のバージョンを確認します。

722016

エラーメッセージ `%Threat Defense-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length`

説明 SVC から、予期された量のデータを入手できませんでした。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722017

エラーメッセージ `%Threat Defense-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0`

説明 SVC が、正しくフレーム化されていないデータグラムを送信しました。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722018

エラーメッセージ `%Threat Defense-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version , expected: expected-version`

説明 SVC が、デバイスに未知のバージョンを送信しました。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722019

エラーメッセージ `%Threat Defense-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length`

説明 SVC から、予期された量のデータを入手できませんでした。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722020

エラーメッセージ `%Threat Defense-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection`

説明 AnyConnect セッションに対するアドレスの割り当てに失敗しました。使用できる IP アドレスがありません。

- **tunnel_group**：ユーザーが割り当てられているか、ログインに使用されたトンネル グループの名前
- *group_policy*：ユーザーが割り当てられているグループ ポリシーの名前
- *user-name*：このメッセージが関連付けられているユーザー名
- *IP_address*：クライアント マシンのパブリック IP（インターネット）アドレス

推奨アクション ip local ip コマンドで表示されるコンフィギュレーションを参照し、トンネル グループとグループ ポリシーに割り当てられているプールに十分なアドレスが存在するかどうかを確認します。DHCP の設定およびステータスを確認します。アドレス割り当てコンフィギュレーションを確認します。AnyConnect クライアントが IP アドレスを取得できない理由を特定するため、IPAA の syslog メッセージをイネーブルにします。

722028

エラーメッセージ `%Threat Defense-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.`

説明未使用の SVC 接続が閉じられました。

推奨アクション不要。ただし、複数の接続が確立されている場合は、クライアントに接続の問題が発生している可能性があります。SVC のログを調べる必要があります。

722029

エラーメッセージ `%Threat Defense-7-722029: Group group User user-name IP IP_address SVC Session Termination: Conns: connections , DPD Conns: DPD_conns , Comp resets: compression_resets , Dcmp resets: decompression_resets`

説明行われた接続、再接続、およびリセットの数が報告されます。**connections** が 1 より大きい場合、または **DPD_conns**、**compression_resets**、**decompression_resets** のいずれかが 0 より大きい場合は、Secure Firewall Threat Defense の管理者が制御できない、ネットワークの信頼性の問

題を示している可能性があります。接続数または DPD 接続数が多い場合は、ユーザーに接続の問題が発生していて、パフォーマンスが低下している可能性があります。

- **connections**：このセッション中の接続の総数（1 が正常）
- **DPD_conns**：DPD による再接続の数
- **compression_resets**：圧縮履歴のリセット数
- **decompression_resets**：圧縮解除履歴のリセット数

推奨アクション SVC のログを調べる必要があります。考えられるネットワーク信頼性問題を解決するための調査と適切な処置が必要になる場合もあります。

722030

エラーメッセージ `%Threat Defense-7-722030: Group group User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes ) bytes, data_pkts (+ctrl_pkts ) packets, drop_pkts drops`

説明セッション終了時の統計情報が記録されています。

- **data_bytes**：（SVC からの）着信データ バイト数
- **ctrl_bytes**：着信制御バイト数
- **data_pkts**：着信データ パケット数
- **ctrl_pkts**：着信制御パケット数
- **drop_pkts**：廃棄された着信パケット数

推奨アクション 不要。

722031

エラーメッセージ `%Threat Defense-7-722031: Group group User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes ) bytes, data_pkts (+ctrl_pkts ) packets, drop_pkts drops.`

説明セッション終了時の統計情報が記録されています。統計には、データバイト、制御パケットバイト、データパケット、制御パケット、およびドロップされたパケットが含まれます。

- **data_bytes**：（SVC への）発信データ バイト数
- **ctrl_bytes**：発信制御バイト数
- **data_pkts**：発信データ パケット数
- **ctrl_pkts**：発信制御パケット数
- **drop_pkts**：ドロップされた発信パケット数

場合によっては、このsyslogがドロップされたパケットの内訳を提供しないため、ドロップされたパケットの数はデータおよび制御パケット全体よりも多くなります。インスタンスの例：

```
2020-09-30T09:06:09.254798+00:00 local4.err pg122d-vpn116 %ASA-3-722031: Group <GP_1>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
800808 (+32) bytes, 1957 (+4) packets, 3358 drops.

2020-09-30T08:53:11.359833+00:00 local4.err srr10c-vpn103 %ASA-3-722031: Group <GP_2>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
413194 (+32) bytes, 1540 (+4) packets, 2059 drops.

2020-09-30T08:37:59.287415+00:00 local4.err srr10c-vpn115 %ASA-3-722031: Group <GP_3>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
571473 (+48) bytes, 1283 (+6) packets, 1323 drops.

2020-09-30T08:31:48.105943+00:00 local4.err srr10c-vpn114 %ASA-3-722031: Group <GP_4>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
131566 (+0) bytes, 283 (+0) packets, 320 drops.

2020-09-30T08:28:38.053003+00:00 local4.err pg122d-vpn117 %ASA-3-722031: Group <GP_5>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
497446 (+23) bytes, 1048 (+1) packets, 1128 drops.

2020-09-30T07:45:43.044373+00:00 local4.err srr10c-vpn114 %ASA-3-722031: Group <GP_6>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
153165 (+16) bytes, 398 (+2) packets, 1045 drops.
```

推奨アクション 不要。

722032

エラーメッセージ `%Threat Defense-5-722032: Group group User user-name IP IP_address New SVC connection replacing old connection.`

説明既存の SVC 接続から新しい SVC 接続に切り替えられようとしています。接続の問題が発生している可能性があります。

推奨アクション SVC ログを確認します。

722033

エラーメッセージ `%Threat Defense-5-722033: Group group User user-name IP IP_address First SVC connection established for SVC session.`

説明 SVC セッションの最初の SVC 接続が確立されました。

推奨アクション 不要。

722034

エラーメッセージ `%Threat Defense-5-722034: Group group User user-name IP IP_address New SVC connection, no existing connection.`

説明再接続が試行されました。すでに閉じられた接続から新しい SVC 接続に切り替えられようとしています。SVC またはSecure Firewall Threat Defense デバイスによって接続がすでに廃棄

されたため、このセッションには既存の接続がありません。接続の問題が発生している可能性があります。

推奨アクション Secure Firewall Threat Defense デバイス のログと SVC のログを調べます。

722035

エラーメッセージ `%Threat Defense-3-722035: Group group User user-name IP IP_address Received large packet length (threshold num ).`

説明大きなパケットがクライアントから受信されました。

- **length**：大きなパケットの長さ
- **num**：しきい値

推奨アクション Secure Firewall Threat Defense デバイスに、DF ビットが設定されて着信するパケットのフラグメント化を許可するには、グループ ポリシーの下で **anyconnect ssl df-bit-ignore enable** コマンドを入力します。

722036

エラーメッセージ `%Threat Defense-3-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num ).`

説明大きなパケットがクライアントに送信されました。パケットの送信元がクライアントの MTU を認識していない可能性があります。また、圧縮できないデータを圧縮したことが原因の可能性もあります。

- **length**：大きなパケットの長さ
- **num**：しきい値

推奨アクション SVC 圧縮をオフにします。オフになっている場合は、アクションを取る必要はありません。

722037

エラーメッセージ `%Threat Defense-5-722037: Group group User user-name IP IP_address SVC closing connection: reason .`

説明指摘された理由で SVC 接続が終了しました。この動作は正常である場合もあれば、接続の問題が発生している場合もあります。

- **reason**：SVC 接続が終了した理由

推奨アクション SVC ログを調べます。

722038

エラーメッセージ `%Threat Defense-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason .`

説明指摘された理由でSVCセッションが終了しました。この動作は正常である場合もあれば、接続の問題が発生している場合もあります。

- **reason**：SVC セッションが終了した理由

推奨アクション 終了の理由が予期しないものである場合は、SVC のログを調べます。

722041

エラーメッセージ `%Threat Defense-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection.`

説明リモート SVC クライアントへの割り当てに使用できる IPv6 アドレスがありませんでした。

- *n*：SVC 接続識別子

推奨アクション 必要に応じて、IPv6 アドレス プールを拡大または作成します。

722042

エラーメッセージ `%Threat Defense-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.`

説明無効な SVC クライアントまたは AnyConnect クライアントが接続しようとしています。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション SVC クライアントまたは AnyConnect クライアントが Secure Firewall Threat Defense デバイス と互換性があることを検証します。

722043

エラーメッセージ `%Threat Defense-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.`

説明 DTLS（UDP トランスポート）を確立できません。SSL 暗号化コンフィギュレーションが変更された可能性があります。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション SSL暗号化設定を元に戻します。SSL 暗号化コンフィギュレーションに少なくとも 1 つのブロック暗号（AES、DES、または 3DES）が含まれていることを確認します。

722044

エラーメッセージ `%Threat Defense-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.`

説明 Secure Firewall Threat Defense デバイス のメモリ不足が原因で、IP アドレスを要求できません。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス
- *ver*：IPv4 または IPv6（要求されている IP アドレスのバージョンに基づく）

推奨アクション Secure Firewall Threat Defense デバイスの負荷を減らすか、または増設メモリを追加します。

722045

エラーメッセージ `%Threat Defense-3-722045: Connection terminated: no SSL tunnel initialization data.`

説明接続を確立するためのデータが欠落しています。これは、Secure Firewall Threat Defense ソフトウェアの障害です。

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。

722046

エラーメッセージ `%Threat Defense-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.`

説明 Secure Firewall Threat Defense デバイス で接続パラメータを設定できません。これは、Secure Firewall Threat Defense ソフトウェアの障害です。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP 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。

722047

エラーメッセージ `%Threat Defense-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.`

説明ユーザーが Web ブラウザを使用してログインし、SVC または AnyConnect クライアントを起動しようとしました。SVC サービスがグローバルにイネーブルになっていないか、または SVCイメージが無効か破損しています。トンネル接続は終了されましたが、クライアントレス接続は維持されています。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション **svc enable** コマンドを使用して、SVC をグローバルにイネーブルにします。**svc image** コマンドを使用して新しいイメージをリロードすることで、SVC イメージのバージョンの整合性を検証します。

722048

エラーメッセージ `%Threat Defense-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.`

説明 ユーザーが Web ブラウザを使用してログインし、SVC または AnyConnect クライアントを起動しようとしました。このユーザーに対して SVC サービスがイネーブルになっていません。トンネル接続は終了されましたが、クライアントレス接続は維持されています。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション **group-policy** コマンドと **username** コマンドを使用して、このユーザーに対してサービスを有効にします。

722049

エラーメッセージ `%Threat Defense-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.`

説明 ユーザーが AnyConnect クライアントを使用してログインしました。SVC サービスがグローバルにイネーブルになっていないか、または SVC イメージが無効か破損しています。セッション接続が終了されました。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション **svc-enable** コマンドを使用して、SVC をグローバルにイネーブルにします。**svc image** コマンドを使用して新しいイメージをリロードすることで、SVC イメージの整合性とバージョンを検証します。

722050

エラーメッセージ `%Threat Defense-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.`

説明 ユーザーが AnyConnect クライアントを使用してログインしました。このユーザーに対して SVC サービスがイネーブルになっていません。セッション接続が終了されました。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション **group-policy** コマンドと **username** コマンドを使用して、このユーザーに対してサービスを有効にします。

722051

エラーメッセージ `%Threat Defense-6-722051: Group group-policy User username IP public-ip IPv4 Address assigned-ip IPv6 Address assigned-ip  assigned to session`

説明指摘されたアドレスが、指摘されたユーザーに割り当てられました。

- *group-policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *username*：ユーザーの名前
- *public-ip*：接続されたクライアントのパブリック IP アドレス
- *assigned-ip*：クライアントに割り当てられた IPv4 アドレスまたは IPv6 アドレス

推奨アクション 不要。

722053

エラーメッセージ `%Threat Defense-6-722053: Group g User u IP ip Unknown client user-agent connection.`

説明未知またはサポート対象外の SSL VPN クライアントが Secure Firewall Threat Defense デバイス に接続しました。旧式のクライアントには、Cisco SVC とバージョン 2.3.1 よりも前の Cisco AnyConnect クライアントが含まれます。

- *g*：ユーザーのログイン時に適用されたグループ ポリシー
- *u*：ユーザーの名前
- *ip*：クライアントの IP アドレス
- *user-agent*：クライアントから受信したユーザー エージェント（通常、バージョンを含む）

推奨アクション サポートされている Cisco SSL VPN クライアントにアップグレードします。

722054

エラーメッセージ `%Threat Defense-4-722054: Group group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP`

説明リダイレクト URL がインストールされ、ACL が ISE から受信されたが、リダイレクト ACL が Secure Firewall Threat Defense デバイス に存在しない場合に、AnyConnect VPN 接続でエラーが発生しました。

- *group policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *user name*：リモート アクセスの要求者のユーザー名

- *remote IP*：接続要求の発信元であるリモート IP アドレス
- *redirect URL*：HTTP トラフィック リダイレクションの URL
- *assigned IP*：ユーザーに割り当てられる IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス にリダイレクト ACL を設定します。

722055

エラーメッセージ `%Threat Defense-6-722055: Group group-policy User username IP public-ip Client Type: user-agent`

説明指摘されたユーザーが指摘されたユーザー エージェントに接続しようとしています。

- *group-policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *username*：ユーザーの名前
- *public-ip*：接続されたクライアントのパブリック IP アドレス
- *user-agent*：接続クライアントによって指定されたユーザーエージェント文字列。通常、AnyConnect クライアントのバージョンと、AnyConnect クライアントのホストオペレーティングシステムが含まれています。

推奨アクション 不要。

722056

エラーメッセージ `%Threat Defense-4-722055: Unsupported AnyConnect client connection rejected from ip address. Client info: user-agent string. Reason: reason`

説明 この syslog は AnyConnect クライアント接続が拒否されたことを示します。この理由は、クライアント情報とともに syslog に示されます。

- *ip address*：古いクライアントとの接続が試行された IP アドレス。
- *user- agent string*：クライアント要求内のユーザーエージェント ヘッダー通常、AnyConnect クライアントのバージョンと、AnyConnect クライアントのホストオペレーティングシステムが含まれています。
- *reason*：拒否の理由。

推奨アクション syslog に示されたクライアント情報と理由を使用して問題を解決します。

メッセージ 723001 ～ 736001

この項では、723001 ～ 736001 のメッセージについて説明します。

723001

エラーメッセージ `%Threat Defense-6-723001: Group group-name , User user-name , IP IP_address : WebVPN Citrix ICA connection connection is up.`

説明 Citrix 接続がアップしています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：Citrix 接続識別子

推奨アクション 不要。

723002

エラーメッセージ `%Threat Defense-6-723002: Group group-name , User user-name , IP IP_address : WebVPN Citrix ICA connection connection is down.`

説明 Citrix 接続がダウンしています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：Citrix 接続識別子

推奨アクション Citrix ICA 接続がクライアント、サーバー、または Secure Firewall Threat Defense の管理者によって意図的に終了された場合、処置は不要です。それ以外の場合は、Citrix ICA 接続がセットアップされている WebVPN セッションがアクティブであることを確認します。WebVPN セッションが非アクティブである場合、このメッセージの受信は正常です。WebVPN セッションがアクティブである場合は、ICA クライアントと Citrix サーバーの両方が正常に動作すること、およびエラーが表示されていないことを確認します。どちらか一方または両方が正常に動作しない場合、あるいはエラーが表示されている場合は、どちらか一方または両方を起動するか、エラーに対処します。それでもこのメッセージを受信する場合は、Cisco TAC にお問い合わせのうえ、次の情報をご提供ください。

- ネットワーク トポロジ
- 遅延およびパケット損失
- Citrix サーバーのコンフィギュレーション
- Citrix ICA クライアントの情報
- 問題を再現する手順
- 関連するすべてのメッセージの完全なテキスト

723003

エラーメッセージ `%Threat Defense-7-723003: No memory for WebVPN Citrix ICA connection connection .`

説明 Secure Firewall Threat Defense デバイス のメモリが不足しています。Citrix 接続が拒否されました。

- **connection**：Citrix 接続識別子

推奨アクション Secure Firewall Threat Defense デバイス が正常に動作していることを確認します。メモリおよびバッファの使用量に特に注意します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、増設メモリを購入するか、Secure Firewall Threat Defense デバイスをアップグレードするか、Secure Firewall Threat Defense デバイスの負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723004

エラーメッセージ `%Threat Defense-7-723004: WebVPN Citrix encountered bad flow control` *`flow`* `.`

説明 Secure Firewall Threat Defense デバイス で内部フロー制御のミスマッチが発生しました。この問題は、大量のデータ フロー（ストレス テスト中などに発生）や大量の ICA 接続が原因となっている可能性があります。

推奨アクション Secure Firewall Threat Defense デバイス への ICA 接続を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723005

エラーメッセージ `%Threat Defense-7-723005: No channel to set up WebVPN Citrix ICA connection.`

説明 Secure Firewall Threat Defense デバイス が Citrix 用の新しいチャネルを作成できませんでした。

推奨アクション Citrix ICA クライアントと Citrix サーバーが稼働していることを確認します。稼働していない場合は、起動して、再度テストします。メモリおよびバッファの使用量に特に注意しながら、Secure Firewall Threat Defense デバイスの負荷を確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723006

エラーメッセージ `%Threat Defense-7-723006: WebVPN Citrix SOCKS errors.`

説明 Secure Firewall Threat Defense デバイス で内部 Citrix SOCKS エラーが発生しました。

推奨アクション Citrix ICA クライアントが正常に動作していることを確認します。さらに、パケット損失に注意しながら、Citrix ICA クライアントとSecure Firewall Threat Defense デバイスの間のネットワーク接続ステータスを確認します。異常なネットワーク状態がある場合は、それを解決します。問題が解決しない場合、Cisco TAC にお問い合わせください。

723007

エラーメッセージ `%Threat Defense-7-723007: WebVPN Citrix ICA connection` *`connection`* `list is broken.`

説明 Secure Firewall Threat Defense デバイス の内部 Citrix 接続リストが破損しています。

- **connection**：Citrix 接続識別子

推奨アクション メモリおよびバッファの使用量に特に注意しながら、Secure Firewall Threat Defense デバイス が正常に動作していることを確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723008

エラーメッセージ `%Threat Defense-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.`

説明存在しない Citrix Socks サーバーにアクセスしようとしました。

- **server**：Citrix サーバー識別子

推奨アクション Secure Firewall Threat Defense デバイス が正常に動作していることを確認します。メモリまたはバッファのリークがないかどうかに注意してください。この問題が頻繁に発生する場合は、メモリ使用量、ネットワーク トポロジ、およびこのメッセージを受信したときの状態に関する情報を取り込みます。調査のために、これらの情報を Cisco TAC に送信します。このメッセージを受信している間も WebVPN セッションがアップしていることを確認します。アップしていない場合は、WebVPN セッションがダウンしている原因を確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723009

エラーメッセージ `%Threat Defense-7-723009: Group group-name , User user-name , IP IP_address : WebVPN Citrix received data on invalid connection connection .`

説明存在しない Citrix 接続に関するデータを受信しました。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：Citrix 接続識別子

推奨アクション元の公開済み Citrix アプリケーションの接続が終了した可能性があり、残りのアクティブな公開済みアプリケーションが接続を失いました。すべての公開済みアプリケーションを再起動して、新しい Citrix ICA トンネルを生成します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723010

エラーメッセージ `%Threat Defense-7-723010: Group group-name , User user-name , IP IP_address : WebVPN Citrix received closing channel channel for invalid connection connection .`

説明存在しない Citrix 接続に関する中断を受信しました。この問題は、特にネットワーク遅延やパケット損失が発生している間の、大量のデータ フロー（ストレス テストなど）や大量の ICA 接続が原因となっている可能性があります。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- channel：Citrix チャネル識別子
- **connection**：Citrix 接続識別子

推奨アクション Secure Firewall Threat Defense デバイス への ICA 接続の数を減らすか、Secure Firewall Threat Defense デバイス 用の増設メモリを入手するか、ネットワークの問題を解決します。

723011

エラーメッセージ `%Threat Defense-7-723011: Group group-name , User user-name , IP IP_address : WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length .`

説明 Citrix SOCKS メッセージの長さが誤っています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス

推奨アクション Citrix ICA クライアントが正常に動作していることを確認します。さらに、パケット損失に注意しながら、ICA クライアントとSecure Firewall Threat Defense デバイスの間のネットワーク接続ステータスを確認します。異常なネットワーク状態を解決した後も問題が存在する場合は、Cisco TAC にお問い合わせください。

723012

エラーメッセージ `%Threat Defense-7-723012: Group group-name , User user-name , IP IP_address : WebVPN Citrix received bad SOCKS socks message format.`

説明 Citrix SOCKS メッセージの形式が誤っています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス

推奨アクション Citrix ICA クライアントが正常に動作していることを確認します。さらに、パケット損失に注意しながら、ICA クライアントとSecure Firewall Threat Defense デバイスの間のネットワーク接続ステータスを確認します。異常なネットワーク状態を解決した後も問題が存在する場合は、Cisco TAC にお問い合わせください。

723013

エラーメッセージ `%Threat Defense-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.`

説明 Secure Firewall Threat Defense の内部 Citrix タイマーが期限切れで、Citrix 接続が無効です。

- **connection**：Citrix 接続識別子

推奨アクション Citrix ICA クライアントと Secure Firewall Threat Defense デバイス の間、および Secure Firewall Threat Defense デバイス と Citrix サーバーの間のネットワーク接続を確認します。異常なネットワーク状態、特に遅延とパケット損失を解決します。メモリまたはバッファの問題に特に注意しながら、Secure Firewall Threat Defense デバイスが正常に動作することを確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、増設メモリを入手するか、Secure Firewall Threat Defense デバイスをアップグレードするか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723014

エラーメッセージ `%Threat Defense-7-723014: Group group-name , User user-name , IP IP_address : WebVPN Citrix TCP connection connection to server server on channel channel initiated.`

説明 Secure Firewall Threat Defense の内部 Citrix Secure Gateway が Citrix サーバーに接続されています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：接続名
- server：Citrix サーバー識別子
- channel：Citrix チャネル識別子（16 進数）

推奨アクション 不要。

724001

エラーメッセージ `%Threat Defense-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.`

説明 Secure Firewall Threat Defense デバイス で CSD Host Integrity Check の結果を処理しているときにエラーが発生したため、セッションが許可されませんでした。

- **group-name**：グループの名前
- **user-name**：ユーザーの名前
- **IP_address**：IP アドレス

推奨アクション クライアント ファイアウォールが長い URL を切り捨てていないかどうかを確認します。クライアントから CSD をアンインストールして、Secure Firewall Threat Defense デバイスに再接続します。

724002

エラーメッセージ `%Threat Defense-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.`

説明 クライアント マシン上で CSD が動作していません。

- **group-name**：グループの名前
- **user-name**：ユーザーの名前
- **IP_address**：IP アドレス

推奨アクション エンドユーザーがクライアント マシンに CSD をインストールして実行できることを確認します。

725001

エラーメッセージ `%Threat Defense-6-725001: Starting SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol session.`

説明 SSL ハンドシェイクがリモート デバイス（クライアントまたはサーバーのいずれか）から開始されました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- **dst-ip**：宛先 IP アドレス
- **dst-port**：宛先ポート番号
- **protocol**：SSL ハンドシェイクに使用された SSL のバージョン

推奨アクション 不要。

725002

エラーメッセージ `%Threat Defense-6-725002: Device completed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol-version session`

説明 リモート デバイスとの SSL ハンドシェイクが正常に完了しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント

- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- *protocol-version*：使用されている SSL プロトコルのバージョン：SSLv3、TLSv1、DTLSv1、TLSv1.1 または TLSv1.2

推奨アクション 不要。

725003

エラーメッセージ `%Threat Defense-6-725003: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port request to resume previous session.`

説明リモート デバイスが以前の SSL セッションを再開しようとしています。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725004

エラーメッセージ `%Threat Defense-6-725004: Device requesting certificate from SSL peer-type interface :src-ip /src-port to dst-ip /dst-port for authentication.`

説明 Secure Firewall Threat Defense デバイス が認証のためにクライアント証明書を要求しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725005

エラーメッセージ `%Threat Defense-6-725005: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port requesting our device certificate for authentication.`

説明サーバーが認証のために Secure Firewall Threat Defense デバイス の証明書を要求しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725006

エラーメッセージ `%Threat Defense-6-725006: Device failed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port`

説明リモート デバイスとの SSL ハンドシェイクが失敗しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション syslog メッセージ 725014 を検索します。このメッセージに失敗の原因が示されています。

725007

エラーメッセージ `%Threat Defense-6-725007: SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port terminated.`

説明 SSL セッションが終了しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725008

エラーメッセージ `%Threat Defense-7-725008: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port proposes the following n cipher(s).`

説明リモート SSL デバイスによって提案された暗号の数が表示されます。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- *n*：サポートされている暗号方式の数

推奨アクション 不要。

725009

エラーメッセージ `%Threat Defense-7-725009 Device proposes the following n cipher(s) peer-type interface :src-ip /src-port to dst-ip /dst-port .`

説明 SSL サーバーに対して提案された暗号の数が表示されます。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- *n*：サポートされている暗号方式の数

推奨アクション 不要。

725010

エラーメッセージ `%Threat Defense-7-725010: Device supports the following n cipher(s).`

説明 SSL セッションのために Secure Firewall Threat Defense デバイス がサポートしている暗号の数が表示されます。

- **n**：サポートされている暗号方式の数

推奨アクション 不要。

725011

エラーメッセージ `%Threat Defense-7-725011 Cipher[order ]: cipher_name`

説明このメッセージは常にメッセージ 725008、725009、および 725010 の後に表示され、暗号名とその優先順位を示しています。

- **order**：暗号リスト内の暗号の順位
- **cipher_name**：暗号リストからの OpenSSL 暗号の名前

推奨アクション 不要。

725012

エラーメッセージ `%Threat Defense-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port.`

説明シスコ デバイスが SSL セッション用に選択した暗号が表示されます。

- **cipher**：暗号リストからの OpenSSL 暗号の名前
- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725013

エラーメッセージ `%Threat Defense-7-725013 SSL peer-type interface :src-ip /src-port to dst-ip /dst-port chooses cipher cipher`

説明サーバーが SSL セッション用に選択した暗号を示しています。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- **cipher**：暗号リストからの OpenSSL 暗号の名前

推奨アクション 不要。

725014

エラーメッセージ `%Threat Defense-7-725014 SSL lib error. Function: function Reason: reason`

説明 SSL ハンドシェイクが失敗した原因を示しています。

- **function**：失敗が報告された機能名
- **reason**：失敗状態の説明

推奨アクション SSL 関連の問題を Cisco TAC に報告する場合は、このメッセージを添付します。

725015

エラーメッセージ `%Threat Defense-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.`

説明 サポートされていない（大きな）キー サイズが原因で、SSL クライアント証明書の検証が失敗したことを示しています。

推奨アクション 4096 ビット以下のキー サイズのクライアント証明書を使用します。

725016

エラーメッセージ `%Threat Defense-6-725016: Device selects trust-point trustpoint for peer-type interface :src-ip /src-port to dst-ip /dst-port`

説明サーバー名指定（SNI）では、特定の接続に使用された証明書が、インターフェイス上で設定された証明書ではない場合があります。また、どの証明書トラストポイントが選択されたかも示されていません。この syslog は、接続（*interface* :*src-ip* /*src-port* で指定）によって使用されるトラストポイントを示すものです。

- *trustpoint*：指定された接続に使用されている設定済みのトラストポイントの名前
- *interface*：Secure Firewall Threat Defense デバイス 上のインターフェイスの名前
- *src-ip*：ピアの IP アドレス
- *src-port*：ピアのポート番号
- *dst-ip*：宛先の IP アドレス
- *dst-port*：宛先のポート番号

推奨アクション 不要。

725017

エラーメッセージ `%Threat Defense-7-725017: No certificates received during the handshake with %s %s :%B /%d to %B /%d for %s session`

説明リモート クライアントが有効な証明書を送信していません。

- *remote_device*：ハンドシェイクを実行したのがクライアントかサーバーかを示します
- *ctm->interface*：ハンドシェイクが送信されるインターフェイス名
- *ctm->src_ip*：クライアントと通信する SSL サーバーの IP アドレス
- *ctm->src_port*：クライアントと通信する SSL サーバーのポート
- *ctm->dst_ip*：クライアントの IP アドレス
- *ctm->dst_port*：応答が通過するクライアントのポート
- *s->method->version*：トランザクションに関係したプロトコルのバージョン（SSLv3、TLSv1、または DTLSv1）

推奨アクション 不要。

725021

エラーメッセージ `%Threat Defense-7-725021: Device preferring cipher-suite cipher(s). Connection info: interface :src-ip /src-port to dst-ip /dst-port`

説明 このメッセージには、ハンドシェイクのネゴシエーション時に優先される暗号スイートが一覧表示されています。

- **cipher-suite**：優先される暗号スイート文字列
- **interface**：SSL セッションが使用しているインターフェイス名
- **src-ip**：送信元 IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- **dst-ip**：宛先 IPv4 アドレスまたは IPv6 アドレス
- **dst-port**：宛先ポート番号

以下は、ハンドシェイクをネゴシエートするときに使用される、優先される暗号スイート文字列のリストです。

- サーバー
- SUITE-B
- ChaCha20
- クライアント
- SHA-256 ハッシュ

推奨アクション 不要。

725022

エラーメッセージ `%Threat Defense-7-725022: Device skipping cipher : cipher - reason. Connection info: interface :src-ip /src-port to dst-ip /dst-port`

説明 この syslog は、ハンドシェイクのネゴシエーション時に暗号スイートのリストに含まれる特定の暗号をスキップした理由を表示します。

- **cipher-suite**：優先される暗号スイート文字列
- **reason**：暗号をスキップする理由。
- **interface**：SSL セッションが使用しているインターフェイス名
- **src-ip**：送信元 IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- **dst-ip**：宛先 IPv4 アドレスまたは IPv6 アドレス

- **dst-port**：宛先ポート番号

次のリストに、特定の暗号をスキップする理由の例をいくつか示します。

- 一時 EC キーにトラストポイント <trust point> との互換性がない
- プロトコルバージョンによってサポートされていない
- PSK サーバーのコールバックが設定されていない
- セキュリティコールバックによって許可されていない
- Safari の ECDHE-ECDSA が壊れている
- 暗号スイートが SHA256 を使用していない
- 暗号が不明である
- 暗号が間違っている
- メッセージダイジェストが変更されている
- 前のセッションの暗号スイートが選択されていない

推奨アクション 不要。

726001

エラーメッセージ `%Threat Defense-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc :/sip /sport to dest_ifc :/dip /dport Action: action Matched Class class_map_id class_map_name`

説明 IM メッセージに対して検査が実施され、指定の基準が満たされました。設定済みのアクションが実行されます。

- *im_protocol*：MSN IM または Yahoo IM
- *im_service*：IM サービス（チャット、会議、ファイル転送、音声、ビデオ、ゲーム、不明など）
- *im_client_1*、*im_client_2*：セッションで IM サービスを使用しているクライアント ピア（*client_login_name* または「?」）
- *src_ifc*：送信元インターフェイス名
- *sip*：送信元 IP アドレス
- *sport*：送信元ポート
- *dest_ifc*：宛先インターフェイス名
- *dip*：宛先 IP アドレス
- *dport*：宛先ポート
- *action*：実行されるアクション（接続のリセット、接続の廃棄、または受信）
- *class_map_id*：一致したクラス マップ ID
- *class_map_name*：一致したクラス マップ名

推奨アクション 不要。

733100

エラーメッセージ `%Threat Defense-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt`

説明このメッセージで指摘されたオブジェクトが、指摘されたバーストしきい値レートまたは平均しきい値レートを超えました。このオブジェクトには、ホスト、TCP/UDP ポート、IP プロトコルの廃棄アクティビティなど、攻撃の可能性に起因するさまざまな廃棄が考えられます。Secure Firewall Threat Defense デバイス が攻撃を受けている可能性があります。

- *Object*：ドロップ レート カウントの一般的な送信元または特定の送信元。次が含まれる場合があります

- Firewall

- Bad pkts

- Rate limit

- DoS attck

- ACL drop

- Conn limit

- ICMP attk

- Scanning

- SYN attck

- Inspect

- Interface

（特定のインターフェイス オブジェクトを示すために、さまざまな形式が使用されることがあります。たとえば、周知のプロトコル HTTP のポート 80 を意味する **80/HTTP** が表示されることがあります）

- *rate_ID*：超過している設定レート。ほとんどのオブジェクトでは、異なる間隔で最大3つの異なるレートを設定できます。
- *rate_val*：特定のレート値。
- *total_cnt*：オブジェクトが作成されたか、またはクリアされてからの合計カウント。

次の 3 つの例は、これらの変数がどのように表示されるかを示しています。

- CPU またはバスの制限に起因するインターフェイス廃棄の場合

```
%Threat Defense-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
 second, max configured rate is 8000; Current average rate is 2030 per second, max
configured rate is 2000; Cumulative total count is 3930654.”
```

- 攻撃の可能性に起因するスキャニング廃棄の場合

```
%Threat Defense-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
 second_max configured rate is 10; Current average rate is 245 per second_max configured
 rate is 5; Cumulative total count is 147409 (35 instances received)
```

- 攻撃の可能性に起因する不良パケットの場合

```
%Threat Defense-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
second, max configured rate is 400; Current average rate is 760 per second, max configured
 rate is 100; Cumulative total count is 1938933
```

- 設定されたスキャン レートおよび **threat-detection rate scanning-rate 3600 average-rate 15** コマンドによる場合

```
%Threat Defense-4-733100: [144.60.88.2] drop rate-2 exceeded. Current burst rate is 0
per second, max configured rate is 8; Current average rate is 5 per second, max configured
 rate is 4; Cumulative total count is 38086
```

メッセージに示されている指定オブジェクト タイプに応じて、次の手順を実行します。

1. メッセージ内のオブジェクトが次のいずれかの場合
   - Firewall
   - Bad pkts
   - Rate limit
   - DoS attck
   - ACL drop
   - Conn limit
   - ICMP attck
   - Scanning
   - SYN attck
   - Inspect
   - Interface

推奨アクション ドロップ レートが実行時環境で許容可能かどうかを確認します。

1. threat-detection rate xxx コマンドを使用して、特定のドロップのしきい値レートを適切な値に調整します。ここで、*xxx* は次のいずれかです。
   - acl-drop
   - bad-packet-drop
   - conn-limit-drop
   - dos-drop
   - fw-drop
   - icmp-drop
   - inspect-drop
   - interface-drop
   - scanning-threat
   - syn-attack
2. メッセージ内のオブジェクトが TCP/UDP ポート、IP アドレス、またはホストの廃棄である場合は、実行環境でその廃棄レートを許容できるかどうかを確認します。

3. threat-detection rate bad-packet-drop コマンドを使用して特定のドロップのしきい値レートを適切な値に調整します。

（注） ドロップ レート超過の警告を表示させたくない場合は、no threat-detection basic-threat コマンドを使用してディセーブルにすることができます。

733101

エラーメッセージ `%Threat Defense-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt.`

説明 Secure Firewall Threat Defense デバイス が特定のホスト（または同じ 1024 ノード サブネット内の複数のホスト）がネットワークをスキャンしている（攻撃している）か、またはスキャンされている（ターゲットとなっている）ことが検出されました。

- *object*：攻撃者またはターゲット（特定のホストまたは同じ 1024 ノードサブネット内の複数のホスト）
- *objectIP*：スキャンしている攻撃者またはスキャンされているターゲットの IP アドレス
- *rate_val*：特定のレート値
- *total_cnt*：合計カウント

次の 2 つの例は、これらの変数がどのように表示されるかを示しています。

```
%Threat Defense-4-733101: Subnet 100.0.0.0 is targeted. Current burst rate is 200 per
second, max configured rate is 0; Current average rate is 0 per second, max configured
rate is 0; Cumulative total count is 2028.
%Threat Defense-4-733101: Host 175.0.0.1 is attacking. Current burst rate is 200 per
second, max configured rate is 0; Current average rate is 0 per second, max configured
rate is 0; Cumulative total count is 2024
```

推奨アクション特定のホストまたはサブネットに対して、**show threat-detection statistics host ip-address ip-mask** コマンドを使用し、全体的な状況を確認してから、脅威スキャンのしきい値レートを適切な値に調整します。適切な値を確定したら、**threat-detection scanning-threat shun-host** コマンドを設定して、ホスト攻撃者（サブネット攻撃者ではない）を排除するためのオプションの処置を行うことができます。shun-host except リストで、特定のホストまたはオブジェクト グループを指定できます。詳細については、CLI 設定ガイドを参照してください。スキャンの検出が必要ない場合は、**no threat-detection scanning** コマンドを使用してこの機能をディセーブルにできます。

733102

エラーメッセージ `%Threat Defense-4-733102:Threat-detection adds host %I to shun list`

説明脅威検出エンジンによってホストが排除されました。**threat-detection scanning-threat shun** コマンドが設定されている場合、攻撃しているホストは脅威検出エンジンによって排除されます。

- *%I*：特定のホスト名

次のメッセージは、このコマンドがどのように実装されるかを示しています。

```
%Threat Defense-4-733102: Threat-detection add host 11.1.1.40 to shun list
```

推奨アクション排除されたホストが実際の攻撃者であるかどうかを調査するには、**threat-detection statistics host ip-address** コマンドを使用します。排除されたホストが攻撃者でない場合は、**clear threat-detection shun ip address** コマンドを使用して、排除されたホストを脅威検出エンジンから削除できます。排除されたすべてのホストを脅威検出エンジンから削除するには、**clear shun** コマンドを使用します。

不適切なしきい値レート設定によって脅威検出エンジンがトリガーされたために、このメッセージを受信した場合は、**threat-detection rate scanning-threat rate-interval x average-rate y burst-rate z** コマンドを使用して、しきい値レートを調整します。

733103

エラーメッセージ `%Threat Defense-4-733103: Threat-detection removes host %I from shun list`

説明脅威検出エンジンによってホストが排除されました。**clear-threat-detection shun** コマンドを使用すると、指摘されたホストが排除リストから削除されます。

- *%I*：特定のホスト名

次のメッセージは、このコマンドがどのように実装されるかを示しています。

```
%Threat Defense-4-733103: Threat-detection removes host 11.1.1.40 from shun list
```

推奨アクション 不要。

733104

エラーメッセージ `%Threat Defense-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED`

説明 Secure Firewall Threat Defense デバイスが SYN フラッドアタックを受けているが、TCP 代行受信メカニズムによって保護されています（代行受信される攻撃の平均レートがしきい値の設定値を超えた場合）。メッセージに、攻撃を受けているサーバーと攻撃元が示されます。

推奨アクション攻撃を除外するための ACL を作成します。

733105

エラーメッセージ `%Threat Defense-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED`

説明 Secure Firewall Threat Defense デバイスが SYN フラッドアタックを受けているが、TCP 代行受信メカニズムによって保護されています（代行受信される攻撃のバーストレートがしきい値の設定値を超えた場合）。メッセージに、攻撃を受けているサーバーと攻撃元が示されます。

推奨アクション攻撃を除外するための ACL を作成します。

734001

エラーメッセージ `%Threat Defense-6-734001: DAP: User user, Addr ipaddr , Connection connection : The following DAP records were selected for this connection: DAP record names`

説明接続用に選択された DAP レコードが表示されます。

- *user*：認証されたユーザー名
- *ipaddr*：リモート クライアントの IP アドレス
- *connection*：クライアント接続のタイプ。次のいずれかです。

- IPsec

- AnyConnect

- Clientless（Web ブラウザ）

- Cut-Through-Proxy

- L2TP

- *DAP record names*：DAP レコード名のカンマ区切りリスト

推奨アクション 不要。

734002

エラーメッセージ `%Threat Defense-5-734002: DAP: User user, Addr ipaddr : Connection terrminated by the following DAP records: DAP record names`

説明接続を終了した DAP レコードが表示されます。

- *user*：認証されたユーザー名
- *ipaddr*：リモート クライアントの IP アドレス
- *DAP record names*：DAP レコード名のカンマ区切りリスト

推奨アクション 不要。

734003

エラーメッセージ `%FTD-7-734003: DAP: User name , Addr ipaddr : Session Attribute: attr name/value`

説明接続に関連付けられている、AAA とエンドポイントのセッション属性が表示されます。

- *user*：認証されたユーザー名
- *ipaddr*：リモート クライアントの IP アドレス
- *attr/value*：AAA またはエンドポイントの属性名と値

推奨アクション 不要。

734004

エラーメッセージ `%FTD-3-734004: DAP: Processing error: internal error code`

説明 DAP 処理エラーが発生しました。

- *internal error code*：内部エラー文字列

推奨アクション **debug dap errors** コマンドをイネーブルにし、DAP 処理をもう一度実行して、さらにデバック情報を取得します。これで問題が解決しない場合は、Cisco TAC に連絡し、内部エラー コードと、エラーを発生させた状態に関する情報を提供します。

735001

エラーメッセージ `%FTD-1-735001 IPMI: Cooling Fan var1 : OK`

説明冷却ファンが正常な動作に復元されました。

- *var1*：デバイス番号マーキング

推奨アクション 不要。

735002

エラーメッセージ `%FTD-1-735002 IPMI: Cooling Fan var1 : Failure Detected`

説明冷却ファンで障害が発生しています。

- *var1*：デバイス番号マーキング

推奨アクション：次のステップを実行します。

1. ファンの回転を妨げる障害物がないかどうかを確認します。
2. 冷却ファンを交換します。
3. 問題が解決しない場合、メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735003

エラーメッセージ `%FTD-1-735003 IPMI: Power Supply var1 : OK`

説明電源モジュールが正常な動作に復元されました。

- *var1*：デバイス番号マーキング

推奨アクション 不要。

735004

エラーメッセージ `%FTD-1-735004 IPMI: Power Supply var1 : Failure Detected`

説明 AC 電源が失われたか、または電源モジュールで障害が発生しています。

- *var1*：デバイス番号マーキング

推奨アクション：次のステップを実行します。

1. AC 電源障害の有無を確認します。
2. 電源装置を交換してください。
3. 問題が解決しない場合、メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735005

エラーメッセージ `%FTD-1-735005 IPMI: Power Supply Unit Redundancy OK`

説明電源装置の冗長性が復元されました。

推奨アクション 不要。

735006

エラーメッセージ `%FTD-1-735006 IPMI: Power Supply Unit Redundancy Lost`

説明電源障害が発生しました。電源装置の冗長性は失われましたが、Secure Firewall Threat Defense デバイス は最小限のリソースで正常に機能しています。これ以上の障害が発生した場合は、Secure Firewall Threat Defense デバイス はシャットダウンされます。

推奨アクション 完全な冗長性を取り戻すには、次の手順を実行します。

1. AC 電源障害の有無を確認します。
2. 電源装置を交換してください。
3. 問題が解決しない場合、メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735007

エラーメッセージ `%FTD-1-735007 IPMI: CPU var1 : Temp: var2 var3 , Critical`

説明 CPU が臨界温度に達しました。

- *var1*：デバイス番号マーキング
- *var2*：温度値
- *var3*：温度値の単位（C、F）

推奨アクション メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735008

エラーメッセージ `%FTD-1-735008 IPMI: Chassis Ambient var1 : Temp: var2 var3 , Critical`

説明シャーシの周囲温度センサーが臨界レベルに達しました。

- *var1*：デバイス番号マーキング
- *var2*：温度値
- *var3*：温度値の単位（C、F）

推奨アクション メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735009

エラーメッセージ `%FTD-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.`

説明 初期化中に環境モニタリングに致命的なエラーが発生したため、続行できませんでした。

推奨アクション **show environment** コマンドと **debug ipmi** コマンドの出力を収集します。メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735010

エラーメッセージ `%FTD-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.`

説明環境モニタリングで、1 つまたは複数のレコードのアップデートを一時的に妨げるエラーが発生しました。

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 environment driver** コマンドと **debug ipmi** コマンドの出力を収集します。メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735011

エラーメッセージ `%FTD-1-735011: Power Supply var1 : Fan OK`

説明電源ファンが動作状態に戻りました。

- *var1*：ファンの番号

推奨アクション 不要。

735012

エラーメッセージ `%Threat Defense-1-735012: Power Supply var1 : Fan Failure Detected`

説明電源ファンに障害が発生しました。

- *var1*：ファンの番号

推奨アクション Cisco TAC に連絡して、障害のトラブルシューティングを行ってください。この障害が解決するまで装置の電源をオフにします。

735013

エラーメッセージ `%FTD-1-735013: Voltage Channel var1 : Voltage OK`

説明電圧チャネルが正常な動作レベルに戻りました。

- *var1*：電圧チャネルの番号

推奨アクション 不要。

735014

エラーメッセージ `%FTD-1-735014: Voltage Channel var1: Voltage Critical`

説明電圧チャネルが重大レベルに変化しました。

- *var1*：電圧チャネルの番号

推奨アクション Cisco TAC に連絡して、障害のトラブルシューティングを行ってください。この障害が解決するまで装置の電源をオフにします。

735015

エラーメッセージ `%FTD-4-735015: CPU var1 : Temp: var2 var3 , Warm`

説明 CPU の温度が正常な動作範囲よりも高くなっています。

- *var1*：CPU の番号
- *var2*：温度値
- *var3*：単位

推奨アクションこのコンポーネントの監視を続行し、危険な温度に到達しないようにします。

735016

エラーメッセージ `%FTD-4-735016: Chassis Ambient var1 : Temp: var2 var3 , Warm`

説明シャーシの温度が正常な動作範囲よりも高くなっています。

- *var1*：シャーシ センサーの番号
- *var2*：温度値
- *var3*：単位

推奨アクションこのコンポーネントの監視を続行し、危険な温度に到達しないようにします。

735017

エラーメッセージ `%Threat Defense-1-735017: Power Supply var1 : Temp: var2 var3 , OK`

説明電源装置の温度が正常な動作温度に戻りました。

- *var1*：電源装置の番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735018

エラーメッセージ `%FTD-4-735018: Power Supply var1 : Temp: var2 var3 , Critical`

説明電源装置が危険な動作温度に達しました。

- *var1*：電源装置の番号
- *var2*：温度値
- *var3*：単位

推奨アクションCisco TAC に連絡して、障害のトラブルシューティングを行ってください。この障害が解決するまで装置の電源をオフにします。

735019

エラーメッセージ `%FTD-4-735019: Power Supply var1 : Temp: var2 var3 , Warm`

説明電源装置の温度が正常な動作範囲よりも高くなっています。

- *var1*：電源装置の番号
- *var2*：温度値
- *var3*：単位

推奨アクションこのコンポーネントの監視を続行し、危険な温度に到達しないようにします。

735020

エラーメッセージ `%FTD-1-735020: CPU var1: Temp: var2 var3 OK`

説明 CPU の温度が正常な動作温度に戻りました。

- *var1*：CPU の番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735021

エラーメッセージ `%FTD-1-735021: Chassis var1: Temp: var2 var3 OK`

説明 シャーシの温度が正常な動作温度に戻りました。

- *var1*：シャーシ センサーの番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735022

エラーメッセージ `%FTD-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.`

説明 Secure Firewall Threat Defense デバイス は、CPU が最大動作温度を超えたことを検出しました。検出直後にシャット ダウンします。

推奨アクション シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。

735023

エラーメッセージ `%FTD-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature. The chassis needs to be inspected immediately for ventilation issues.`

説明 Secure Firewall Threat Defense デバイス は、CPU が最大安全動作温度を超えて稼働していたために発生したシャットダウンを検出しました。**show environment** コマンドを使用すると、このイベントが発生したことが示されます。

推奨アクション シャーシをただちに調査し、換気に問題がないことを確認する必要があります。

735024

エラーメッセージ `%Threat Defense-1-735024: IO Hub var1 : Temp: var2 var3 , OK`

説明 IO ハブの温度が正常な動作温度に戻りました。

- *ar1*：IO ハブの番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735025

エラーメッセージ `%FTD-1-735025: IO Hub var1 : Temp: var2 var3 , Critical`

説明 IO ハブの温度が危険な温度に達しました。

- *ar1*：IO ハブの番号
- *var2*：温度値
- *var3*：単位

推奨アクション メッセージを表示されているとおりに記録し、Cisco TAC にお問い合わせください。

735026

エラーメッセージ `%FTD-4-735026: IO Hub var1 : Temp: var2 var3 , Warm`

説明 IO ハブの温度が正常な動作範囲よりも高くなっています。

- *ar1*：IO ハブの番号
- *var2*：温度値
- *var3*：単位

推奨アクション このコンポーネントの監視を続行し、クリティカル温度に達しないようにします。

735027

エラーメッセージ `%FTD-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.`

説明 Secure Firewall Threat Defense デバイス は CPU の電圧レギュレータが最大熱動作温度を超えて稼働していることを検出しました。検出後にただちにシャットダウンします。

- *cpu_num*：熱イベントを発生させた CPU 電圧レギュレータを識別する番号

推奨アクション シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。

735028

エラーメッセージ `%FTD-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues.`

説明 Secure Firewall Threat Defense デバイス は、CPU 電圧レギュレータが最大安全動作温度を超えて稼働していたために発生したシャットダウンを検出しました。**show environment** コマンドを入力すると、このイベントが発生したことが示されます。

推奨アクション シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。

735029

エラーメッセージ `%FTD-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.`

説明 Secure Firewall Threat Defense デバイス は、IO ハブが最大動作温度を超えたことを検出しました。検出直後にシャット ダウンします。

推奨アクション シャーシと IO ハブをただちに調査し、換気に問題がないことを確認する必要があります。

736001

エラーメッセージ `%FTD-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.`

説明 ジャンボ フレーム サポートを設定していたときに、メモリの不足が検出されました。その結果、ジャンボフレーム サポートがディセーブルになりました。

推奨アクション **jumbo-frame reservation** コマンドを使用して、ジャンボ フレーム サポートをもう一度イネーブルにしてみてください。実行コンフィギュレーションを保存し、Secure Firewall Threat Defense デバイス をリブートします。問題が解決しない場合、Cisco TAC にお問い合わせください。

メッセージ 737001 ～ 776254

この項では、737001 ～ 776254 のメッセージについて説明します。

737001

エラーメッセージ `%FTD-7-737001: IPAA: Received message message-type`

説明 IP アドレス割り当てプロセスはメッセージを受信しました。

- *message-type*：IP アドレス割り当てプロセスで受信したメッセージ

推奨アクション 不要。

737002

エラーメッセージ `%FTD-3-737002: IPAA: Session= session,Received unknown message num variables`

説明 IP アドレス割り当てプロセスはメッセージを受信しました。

- *session*：16 進数の VPN セッション ID
- *num*：IP アドレス割り当てプロセスで受信したメッセージの識別子

推奨アクション 不要。

737003

エラーメッセージ `%FTD-5-737003: IPAA: Session= session, DHCP configured, no viable servers found for tunnel-group tunnel-group`

説明指摘されたトンネル グループの DHCP サーバー コンフィギュレーションが無効です。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション トンネル グループの DHCP 設定を検証します。DHCP サーバーがオンラインであることを確認します。

737004

エラーメッセージ `%Threat Defense-5-737004: IPAA: Session= session, DHCP configured, request failed for tunnel-group 'tunnel-group'`

説明指摘されたトンネル グループの DHCP サーバー コンフィギュレーションが無効です。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション トンネル グループの DHCP 設定を検証します。DHCP サーバーがオンラインであることを確認します。

737005

エラーメッセージ `%FTD-6-737005: IPAA: Session= session, DHCP configured, request succeeded for tunnel-group tunnel-group`

説明 DHCP サーバー要求が成功しました。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション 不要。

737006

エラーメッセージ `%FTD-6-737006: IPAA: Session= session, Local pool request succeeded for tunnel-group tunnel-group`

説明ローカル プール要求が成功しました。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション 不要。

737007

エラーメッセージ `%FTD-5-737007: IPAA: Session= session, Local pool request failed for tunnel-group tunnel-group`

説明ローカル プール要求が失敗しました。トンネル グループに割り当てられているプールが枯渇している可能性があります。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション **show ip local pool** コマンドを使用して、IP ローカル プールの設定を検証します。

737008

エラーメッセージ `%FTD-5-737008: IPAA: Session= session, 'tunnel-group' not found`

説明コンフィギュレーション用の IP アドレスを取得しようとしたときに、トンネル グループが見つかりませんでした。このメッセージは、ソフトウェア障害が原因で生成される場合があります。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション トンネル グループ設定を確認しますCisco TAC に問い合わせて、問題を報告してください。

737009

エラーメッセージ `%FTD-6-737009: IPAA: Session= session, AAA assigned address ip-address , request failed`

説明リモート アクセス クライアント ソフトウェアが特定のアドレスの使用を要求しました。AAA サーバーに対する対象のアドレスの使用要求が失敗しました。アドレスが使用中の可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IPv4 アドレスまたは IPv6 アドレス

推奨アクションAAA サーバーのステータスと IP ローカル プールのステータスを確認します。

737010

エラーメッセージ `%FTD-6-737010: IPAA: Session= session, AAA assigned address ip-address , request succeeded`

説明リモート アクセス クライアント ソフトウェアが特定のアドレスの使用を要求し、対象のアドレスを正常に受け取りました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IPv4 アドレスまたは IPv6 アドレス

推奨アクション 不要。

737011

エラーメッセージ `%FTD-5-737011: IPAA: Session= session, AAA assigned ip-address , not permitted, retrying`

説明リモート アクセス クライアント ソフトウェアが特定のアドレスの使用を要求しました。**vpn-addr-assign aaa** コマンドが設定されていません。その代わりとして設定されているアドレス割り当て方法が使用されます。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IPv4 アドレスまたは IPv6 アドレス

推奨アクション クライアントがそれら自体のアドレスを指定することを許可する場合は、**vpn-addr-assign aaa** コマンドをイネーブルにします。

737012

エラーメッセージ `%FTD-4-737012: IPAA: Session= session, Address assignment failed`

説明リモート アクセス クライアント ソフトウェアによる特定のアドレスの要求が失敗しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IP アドレス

推奨アクション IP ローカル プールを使用している場合は、ローカル プールの設定を検証します。AAA を使用している場合は、AAA サーバーのコンフィギュレーションとステータスを検

証します。DHCP を使用している場合は、DHCP サーバーのコンフィギュレーションとステータスを検証します。ログ レベルを上げて（通知または情報を使用）、失敗の原因を示す追加のメッセージを取得します。

737013

エラーメッセージ `%FTD-4-737013: IPAA: Session= session, Error freeing address ip-address , not found`

説明 Secure Firewall Threat Defense デバイス がアドレスを解放しようとしましたが、最近のコンフィギュレーション変更により、そのアドレスが割り当て済みリストにありませんでした。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IPv4 アドレスまたは IPv6 アドレス

推奨アクションアドレスの割り当て設定を検証します。このメッセージが引き続き発生する場合は、ソフトウェア障害が原因となっている可能性があります。Cisco TAC に問い合わせて、問題を報告してください。

737014

エラーメッセージ `%FTD-6-737014: IPAA: Session= session, Freeing AAA address ip-address`

説明 Secure Firewall Threat Defense デバイス が、AAA を使用して割り当てられた IP アドレスを正常に解放しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IPv4 アドレスまたは IPv6 アドレス

推奨アクション 不要。

737015

エラーメッセージ `%Threat Defense-6-737015: IPAA: Session= session, Freeing DHCP address ip-address`

説明 Secure Firewall Threat Defense デバイス が、DHCP を使用して割り当てられた IP アドレスを正常に解放しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IP アドレス

推奨アクション 不要。

737016

エラーメッセージ `%FTD-6-737016: IPAA: Session= session, Freeing local pool pool-name address ip-address`

説明 Secure Firewall Threat Defense デバイス が、ローカル プールを使用して割り当てられた IP アドレスを正常に解放しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IPv4 アドレスまたは IPv6 アドレス
- *pool-name*：アドレスが返されているプール

推奨アクション 不要。

737017

エラーメッセージ `%FTD-6-737017: IPAA: Session= session, DHCP request attempt num succeeded`

説明 Secure Firewall Threat Defense デバイス が DHCP サーバーに要求を正常に送信しました。

- *session*：16 進数の VPN セッション ID
- *num*：試行回数

推奨アクション 不要。

737018

エラーメッセージ `%FTD-5-737018: IPAA: Session= session, DHCP request attempt num failed`

説明 Secure Firewall Threat Defense デバイス が DHCP サーバーに要求を送信できませんでした。

- *session*：16 進数の VPN セッション ID
- *num*：試行回数

推奨アクション DHCP の設定と DHCP サーバーへの接続を検証します。

737019

エラーメッセージ `%FTD-4-737019: IPAA: Session= session, Unable to get address from group-policy or tunnel-group local pools`

説明 Secure Firewall Threat Defense デバイス が、グループ ポリシーまたはトンネル グループに設定されているローカル プールからアドレスを取得できませんでした。ローカル プールが枯渇している可能性があります。

- *session*：16 進数の VPN セッション ID

推奨アクション ローカル プールのコンフィギュレーションとステータスを検証します。ローカルプールのグループポリシーとトンネルグループのコンフィギュレーションを検証します。

737023

エラーメッセージ `%FTD-5-737023: IPAA: Session= session, Unable to allocate memory to store local pool address ip-address`

説明 Secure Firewall Threat Defense デバイス のメモリが不足しています。

- *session*：16 進数の VPN セッション ID
- *ip-address*：取得された IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス の負荷が高くなっているためにより多くのメモリが必要になっているか、またはソフトウェアの不具合によってメモリ リークが生じている可能性があります。Cisco TAC に問い合わせて、問題を報告してください。

737024

エラーメッセージ `%FTD-5-737024: IPAA: Session= session, Client requested address ip-address , already in use, retrying`

説明クライアントが要求した IP アドレスはすでに使用されています。要求は、新しい IP アドレスを使用して試行されます。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IP アドレス

推奨アクション 不要。

737025

エラーメッセージ `%FTD-5-737025: IPAA:Session= session, Duplicate local pool address found, ip-address in quarantine`

説明クライアントに渡されることになっていた IP アドレスはすでに使用されています。IP アドレスはプールから削除され、再び使用されることはありません。

- *session*：16 進数の VPN セッション ID
- *ip-address*：取得された IP アドレス

推奨アクション ローカル プールの設定を検証します。ソフトウェアの不具合によって重複が発生している可能性があります。Cisco TAC に問い合わせて、問題を報告してください。

737026

エラーメッセージ `%FTD-6-737026: IPAA:Session= session, Client assigned ip-address from local pool pool-name`

説明指摘されたアドレスがローカル プールから割り当てられました。

- *session*：16 進数の VPN セッション ID

- *ip-address*：クライアントに割り当てられた IP アドレス
- *pool-name*：アドレスの割り当て元のプール

推奨アクション 不要。

737027

エラーメッセージ `%FTD-3-737027: IPAA:Session= session, No data for address request`

説明ソフトウェア障害が検出されました。

- *session*：16 進数の VPN セッション ID

推奨アクション Cisco TAC に問い合わせて、問題を報告してください。

737028

エラーメッセージ `%FTD-4-737028: IPAA:Session= session, Unable to send ip-address to standby: communication failure`

説明アクティブ Secure Firewall Threat Defense デバイス が、スタンバイ Secure Firewall Threat Defense デバイス と通信できませんでした。フェールオーバー ペアが同期していない可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション フェールオーバー設定ステータスを検証します。

737029

エラーメッセージ `%FTD-6-737029: IPAA:Session= session, Added ip-address to standby`

説明スタンバイ Secure Firewall Threat Defense デバイス が IP アドレス割り当てを受け入れました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション 不要。

737030

エラーメッセージ `%FTD-4-737030: IPAA:Session= session, Unable to send ip-address to standby: address in use`

説明アクティブ Secure Firewall Threat Defense デバイス が指摘されたアドレスを取得しようとしましたが、そのアドレスはスタンバイ Secure Firewall Threat Defense デバイス ですでに使用されていました。フェールオーバー ペアが同期していない可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション フェールオーバー設定ステータスを検証します。

737031

エラーメッセージ `%FTD-6-737031: IPAA:Session= session, Removed ip-address from standby`

説明スタンバイ Secure Firewall Threat Defense デバイス が IP アドレス割り当てを消去しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション 不要。

737032

エラーメッセージ `%FTD-4-737032: IPAA:Session= session, Unable to remove ip-address from standby: address not found`

説明スタンバイ Secure Firewall Threat Defense デバイス で使用されていない IP アドレスをアクティブ Secure Firewall Threat Defense デバイス が解放しようとしました。フェールオーバー ペアが同期していない可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション フェールオーバー設定ステータスを検証します。

737033

エラーメッセージ `%FTD-4-737033: IPAA:Session= session, Unable to assign addr_allocator provided IP address ip_addr to client. This IP address has already been assigned by previous_addr_allocator`

説明 AAA/DHCP/ローカル プールによって割り当てられたアドレスがすでに使用されています。

- *session*：16 進数の VPN セッション ID
- *addr_allocator*：DHCP/AAA/ローカル プール
- *ip_addr*：DHCP/AAA/ローカル プールによって割り当てられた IP アドレス
- *previous_ addr_allocator*：すでに IP アドレスを割り当てたアドレス アロケータ（ローカル プール、AAA、または DHCP）

推奨アクション AAA/DHCP/ローカル プールのアドレス設定を検証します。重複が発生している可能性があります。

737034

エラーメッセージ `%Threat Defense-5-737034: IPAA: Session= session, <IP version> address: <explanation>`

説明 IP アドレス割り当てプロセスがアドレスを提供できません。<explanation> テキストにその理由が説明されます。

- *session*：16 進数の VPN セッション ID

推奨アクション処置は説明に基づきます。

737035

エラーメッセージ `%FTD-7-737035: IPAA: Session= session, '<message type>' message queued`

説明メッセージは IP アドレス割り当てにキューイングされます。これは syslog 737001 に対応しています。このメッセージはレート制限されていません。

- *session*：16 進数の VPN セッション ID

推奨アクション処置は必要ありません。

737036

エラーメッセージ `%FTD-6-737035:IPAA: Session= session, Client assigned <address> from DHCP`

説明 IP アドレス割り当てプロセスで、VPN クライアントに DHCP プロビジョニングされたアドレスが返されました。このメッセージはレート制限されていません。

- *session*：16 進数の VPN セッション ID

推奨アクション処置は必要ありません。

737038

エラーメッセージ `%FTD7-737038: IPAA: Session=session, specified address ip-address was in-use, trying to get another.`

説明 このログは、ユーザーに割り当てるアドレスが AAA サーバー（内部または外部）によって指定されている場合に生成されます。ただし、このアドレスはすでに使用されています。要求は再キューイングされており、指定されたアドレスが DHCP またはローカルプールにフォールバックされることはありません。

- *session*：要求しているセッションの VPN セッション ID
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737200

エラーメッセージ `%FTD-7-737200: VPNFIP: Pool=pool, Allocated ip-address from pool`

説明 このログは、アドレスがローカルプールから割り当てられると生成されます。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737201

エラーメッセージ `%FTD-7-737201: VPNFIP: Pool=pool, Returned ip-address to pool (recycle=recycle)`

説明 このログは、アドレスがローカルプールに返されると生成されます。リサイクルフラグは、このアドレスを次の要求に再利用する必要があるかどうかを示します。まれに、リサイクルフラグが FALSE になります。たとえば、アドレスの衝突がある（そのアドレスが AAA や DHCP などの他の手段によってすでに VPN セッションに割り当てられている）場合などです。この場合、次の要求でそのアドレスを再利用することは、すぐには試みられません。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737202

エラーメッセージ `%FTD-3-737202: VPNFIP: Pool=pool, ERROR: message`

説明このログは、VPN FIP データベースに関連するエラーイベントが検出されると生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション エラーが解消されない場合は、Cisco TAC にお問い合わせください。

737203

エラーメッセージ `%FTD-4-737203: VPNFIP: Pool=pool, WARN: message`

説明このログは、VPN FIP データベースに関連するイベントを警告するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション 警告が続く場合は、Cisco TAC にお問い合わせください。

737204

エラーメッセージ `%FTD-5-737204: VPNFIP: Pool=pool, NOTIFY: message`

説明 このログは、VPN FIP データベースに関連するイベントを通知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション 必要なし

737205

エラーメッセージ `%FTD-6-737205: VPNFIP: Pool=pool, INFO: message`

説明 このログは、VPN FIP データベースに関連するイベントを報知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション 必要なし

737206

エラーメッセージ `%FTD-7-737206: VPNFIP: Pool=pool, DEBUG: message`

説明 このログは、VPN FIP データベースに関連するイベントをデバッグするために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション 必要なし

737400

エラーメッセージ `%FTD-7-737400: POOLIP: Pool=pool, Allocated ip-address from pool`

説明 このログは、アドレスがローカルプールから割り当てられると生成されます。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション 必要なし

737401

エラーメッセージ `%FTD-7-737401: POOLIP: Pool=pool, Returned ip-address to pool (recycle=recycle).`

説明 このログは、アドレスがローカルプールに返されると生成されます。リサイクルフラグは、このアドレスを次の要求に再利用する必要があるかどうかを示します。まれに、リサイクルフラグが FALSE になります。たとえば、アドレスの衝突がある（そのアドレスが AAA や DHCP などの他の手段によってすでに VPN セッションに割り当てられている）場合などです。この場合、次の要求でそのアドレスを再利用することは、すぐには試みられません。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737402

エラーメッセージ `%FTD-4-737402: POOLIP: Pool=pool, Failed to return ip-address to pool (recycle=recycle). Reason: message`

説明 このログは、アドレスをアドレスプールに返すことができない場合に生成されます。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス
- *message*：失敗の詳細（たとえば、アドレスがプールの範囲外である）

推奨アクション必要なし

737403

エラーメッセージ `%FTD-3-737403: POOLIP: Pool=pool, ERROR: message`

説明 このログは、IP ローカルプールデータベースに関連するエラーイベントが検出されると生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション エラーが解消されない場合は、Cisco TAC にお問い合わせください。

737404

エラーメッセージ `%FTD-4-737404: POOLIP: Pool=pool, WARN: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントを警告するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション 警告が続く場合は、Cisco TAC にお問い合わせください。

737405

エラーメッセージ `%FTD-5-737405: POOLIP: Pool=pool, NOTIFY: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントを通知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

737406

エラーメッセージ `%FTD-6-737406: POOLIP: Pool=pool, INFO: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントを報知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

737407

エラーメッセージ `%FTD-7-737407: POOLIP: Pool=pool, DEBUG: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントをデバッグするために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

741000

エラーメッセージ `%FTD-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB`

説明コア ダンプ ファイル システムが正常に作成されました。ファイル システムは、コア ダンプで使用できるディスク スペースの量を制限することでコア ダンプを管理するためのものです。

- *variable 1*：コア ダンプが配置されるファイル システム（disk0:、disk1:、flash: など）
- *variable 2*：作成されたコア ダンプ ファイル システムのサイズ（MB 単位）

推奨アクション コア ダンプ ファイル システムの作成後に設定を必ず保存してください。

741001

エラーメッセージ `%FTD-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB`

説明コア ダンプ ファイル システムのサイズが正常に変更されました。

- *variable 1*：コア ダンプが配置されるファイル システム
- *variable 2*：以前のコア ダンプ ファイル システムのサイズ（MB 単位）
- *variable 3*：新たにサイズが変更された現在のコア ダンプ ファイル システムのサイズ（MB 単位）

推奨アクション コア ダンプ ファイル システムのサイズの変更後に設定を必ず保存してください。コア ダンプ ファイル システムのサイズを変更すると、既存のコア ダンプ ファイル システムの内容が削除されます。そのため、コア ダンプ ファイル システムのサイズを変更する前に、すべての情報をアーカイブしてください。

741002

エラーメッセージ `%FTD-6-741002: Coredump log and filesystem contents cleared on variable 1`

説明コア ダンプ ファイル システムからすべてのコア ダンプが削除され、コア ダンプ ログが消去されました。コア ダンプ ファイル システムとコア ダンプ ログは常に相互に同期されます。

- *variable 1*：コア ダンプが配置されているファイル システム（disk0:、disk1:、flash: など）

推奨アクション 不要。**clear coredump** コマンドを使用すると、コ アダンプ ファイル システムを消去して既知の状態にリセットできます。

741003

エラーメッセージ `%FTD-6-741003: Coredump filesystem and its contents removed on variable 1`

説明コア ダンプ ファイル システムとその内容が削除され、コア ダンプ機能がディセーブルになりました。

- *variable 1*：コア ダンプが配置されているファイル システム（disk0:、disk1:、flash: など）

推奨アクション コア ダンプ機能がディセーブルになった後、コンフィギュレーションを必ず保存します。

741004

エラーメッセージ `%Threat Defense-6-741004: Coredump configuration reset to default values`

説明コア ダンプのコンフィギュレーションがデフォルト値にリセットされました。つまり、コア ダンプがディセーブルになりました。

推奨アクション コア ダンプ機能が無効になった後、設定を必ず保存します。

741005

エラーメッセージ `%FTD-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3`

説明コア ダンプ関連の操作の実行中にエラーが発生しました。

- *variable 1*：この変数の有効な値は次のとおりです。

- CREATE_FSYS：コア ダンプ ファイル システムの作成中にエラーが発生しました。

- CLEAR_LOG：コア ダンプ ログの消去中にエラーが発生しました。

- DELETE_FSYS：コア ダンプ ファイル システムの削除中にエラーが発生しました。

- CLEAR_FSYS：コア ダンプ ファイル システムの内容の削除中にエラーが発生しました。

- MOUNT_FSYS：コア ダンプ ファイル システムのマウント中にエラーが発生しました。

- *variable 2*：*variable 1* に指定されたエラーの原因に関する追加情報を提供する 10 進数。
- *variable 3*：*variable 2* に関連付けられている説明のための ASCII 文字列。ASCII 文字列には、次の値が使用されます。

- coredump files already exist

- unable to create coredump filesystem

- unable to create loopback device

- filesystem type not supported

- unable to delete the coredump filesystem

- unable to delete loopback device

- unable to unmount coredump filesystem

- unable to mount coredump filesystem

- unable to mount loopback device

- unable to clear coredump filesystem

- coredump filesystem not found

- requested coredump filesystem too big

- coredump operation aborted by administrator

- coredump command execution failed

- coredump IFS error encountered

- coredump, unidentified error encountered

推奨アクション 設定でコア ダンプ機能がディセーブルになっていることを確認し、詳細に分析するために Cisco TAC にメッセージを送信します。

741006

エラーメッセージ `%FTD-4-741006: Unable to write Coredump Helper configuration, reason variable 1`

説明コアダンプ ヘルパーのコンフィギュレーション ファイルへの書き込み中にエラーが発生しました。このエラーは、disk0: がいっぱいになっている場合にだけ発生します。コンフィギュレーション ファイルは disk0: にあります（.coredumpinfo/coredump.cfg）。

- *variable 1*：この変数には、core dump helper 設定ファイルへの書き込みが失敗した理由を示す基本的なファイル システム関連の文字列が含まれています。

推奨アクション コア ダンプ機能をディセーブルにし、不要なアイテムを disk0: から削除してから、必要に応じてコア ダンプをもう一度イネーブルにします。

742001

エラーメッセージ `%FTD-3-742001: failed to read master key for password encryption from persistent store`

説明起動後に不揮発性メモリからのプライマリパスワード暗号キーを読み取ろうとしましたが失敗しました。コンフィギュレーションの中の暗号化されたパスワードは、**key config-key password encryption** コマンドを使用してプライマリキーを正しい値に設定しない限り、復号されません。

推奨アクションコンフィギュレーションの中に、使用する必要がある暗号化されたパスワードがある場合は、**key config-key password encryption** コマンドを使用して、プライマリキーをパスワードを暗号化するために使用した以前の値に設定します。暗号化されたパスワードがない場合、または暗号化されたパスワードを破棄できる場合は、新しいプライマリキーを設定します。パスワード暗号化を使用していない場合、処置は不要です。

742002

エラーメッセージ `%Threat Defense-3-742002: failed to set master key for password encryption`

説明 key config-key password encryption コマンドの読み込みに失敗しました。このエラーは、次の理由で発生することがあります。

- セキュアでない端末（たとえば、Telnet 接続経由）から設定された。

- フェールオーバーがイネーブルであるが、暗号化されたリンクを使用していない。
- 他のユーザーが同時にキーを設定している。
- キーを変更しようとしたときに、古いキーが正しくない。
- キーがセキュアであるには小さすぎる。

他にもエラーの理由が考えられます。このような場合、実際のエラーがコマンドに対して表示されます。

推奨アクション コマンドの応答に示されている問題を修正します。

742003

エラーメッセージ `%Threat Defense-3-742003: failed to save master key for password encryption, reason reason_text`

説明 不揮発性メモリにプライマリキーを保存しようとしましたが失敗しました。実際の原因は *reason_text* パラメータで指定されます。原因としては、メモリ不足状態や、不揮発性ストレージに不整合があることが考えられます。

推奨アクション 問題が解決しない場合は、キーを保存するために使用した不揮発性ストアを **write erase** コマンドを使用して再フォーマットします。この手順を実行する前に、アウトオブザボックス コンフィギュレーションをバックアップしてください。その後 **write erase** コマンドを再入力します。

742004

エラーメッセージ `%FTD-3-742004: failed to sync master key for password encryption, reason reason_text`

説明 ピアにプライマリキーを同期しようとしましたが失敗しました。実際の原因は *reason_text* パラメータで指定されます。

推奨アクション *reason_text* パラメータに指定された問題の修正を試みます。

742005

エラーメッセージ `%FTD-3-742005: cipher text enc_pass is not compatible with the configured master key or the cipher text has been tampered with`

説明 パスワードを復号化しようとしましたが失敗しました。パスワードは現在のプライマリキーとは異なるプライマリキーを使用して暗号化されているか、暗号化されたパスワードが元の形式から変更された可能性があります。

推奨アクション 正しいプライマリキーが使用されていない場合、問題を解決します。暗号化されたパスワードが変更された場合、新しいパスワードを使用して問題のコンフィギュレーションを再適用します。

742006

エラーメッセージ `%FTD-3-742006: password decryption failed due to unavailable memory`

説明メモリがないために、パスワードの復号化に失敗しました。このパスワードを使用した機能は要求どおりに動作しません。

推奨アクション メモリの問題を修正します。

742007

エラーメッセージ `%Threat Defense-3-742007: password encryption failed due to unavailable memory`

説明メモリがないために、パスワードの暗号化に失敗しました。コンフィギュレーションの中のパスワードは、クリア テキスト形式のままになる可能性があります。

推奨アクションメモリの問題を修正し、パスワードの暗号化に失敗したコンフィギュレーションを再適用します。

742008

エラーメッセージ `%FTD-3-742008: password enc_pass decryption failed due to decoding error`

説明デコードエラーが原因でパスワードの復号化に失敗しました。これは、暗号化されたパスワードが暗号化後に変更されたことが原因である可能性があります。

推奨アクション クリア テキスト パスワードを使用して問題の設定を再適用します。

742009

エラーメッセージ `%FTD-3-742009: password encryption failed due to decoding error`

説明パスワードの暗号化はデコード エラーが原因で失敗しました。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。

推奨アクション クリア テキスト パスワードを使用して問題の設定を再適用します。問題が解決しない場合、Cisco TAC にお問い合わせください。

742010

エラーメッセージ `%FTD-3-742010: encrypted password enc_pass is not well formed`

説明コマンドで指定された暗号化パスワードの形式が正しくありません。パスワードは、有効な暗号化パスワードではないか、暗号化後に変更された可能性があります。

- *reason_text*：障害の実際の原因を表す文字列
- *enc_pass*：問題に関連する暗号化されたパスワード

推奨アクション クリア テキスト パスワードを使用して問題の設定を再適用します。

743000

エラーメッセージ `%FTD-1-743000: The PCI device with vendor ID: vendor_id device ID: device_id located at bus:device.function bus_num:dev_num, func_num has a link link_attr_name of actual_link_attr_val when it should have a link link_attr_name of expected_link_attr_val .`

説明システムのPCIデバイスが適切に設定されていません。システムが最適レベルで動作しなくなる可能性があります。

推奨アクション show controller pci detail コマンドの出力を収集し、Cisco TAC にお問い合わせください。

743001

エラーメッセージ `%FTD-1-743001: Backplane health monitoring detected link failure`

説明 Secure Firewall Threat Defense サービス モジュールとスイッチ シャーシ間のリンクの 1 つでハードウェア障害が発生し検出された可能性があります。

推奨アクション Cisco TAC にお問い合わせください。

743002

エラーメッセージ `%FTD-1-743002: Backplane health monitoring detected link OK`

説明 Secure Firewall Threat Defense サービス モジュールとスイッチ シャーシ間のリンクが復元されました。ただし、障害およびその後の復旧は、ハードウェア障害を示している可能性があります。

推奨アクション Cisco TAC にお問い合わせください。

743004

エラーメッセージ `%Threat Defense-1-743004: System is not fully operational - PCI device with vendor ID vendor_id (vendor_name ), device ID device_id (device_name ) not found`

説明システムが完全に機能するために必要な PCI デバイスがシステムに見つかりませんでした。

- *vendor_id*：デバイス ベンダーを識別する 16 進値
- *vendor_name*：ベンダー名を識別するテキスト文字列
- *device_id*：ベンダー デバイスを識別する 16 進値
- *device_name*：デバイス名を識別するテキスト文字列

推奨アクション show controller pci detail コマンドの出力を収集し、Cisco TAC にお問い合わせください。

743010

エラーメッセージ `%Threat Defense-3-743010: EOBC RPC server failed to start for client module client name .`

説明サーバー上の EOBC RPC サービスの特定のクライアントに対しサービスを開始できませんでした。

推奨アクション Cisco TAC に電話でお問い合わせください。

743011

エラーメッセージ `%Threat Defense-3-743011: EOBC RPC call failed, return code code string.`

説明 EOBC RPC クライアントが目的のサーバーへの RPC を作成できませんでした。

推奨アクション Cisco TAC に電話でお問い合わせください。

746014

エラーメッセージ `%Threat Defense-5-746014: user-identity: [FQDN] fqdn address IP Address obsolete.`

説明 完全修飾ドメイン名が古くなっています。

推奨アクション 不要。

746015

エラーメッセージ `%Threat Defense-5-746015: user-identity: FQDN] fqdn resolved IP address .`

説明 完全修飾ドメイン名のルックアップが成功しました。

推奨アクション 不要。

746016

エラーメッセージ `%Threat Defense-3-746016: user-identity: DNS lookup failed, reason: reason`

説明DNS のルックアップが失敗しました。失敗の理由は、次のいずれかです。タイムアウト、解決不能、メモリ不足。

推奨アクション FQDN が有効であり、DNS サーバーが ASA から到達可能であることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

747001

エラーメッセージ %Threat Defense-3-747001: Clustering: Recovered from state machine event queue depleted. Event (*event-id* , *ptr-in-hex* , *ptr-in-hex*) dropped. Current state *state-name* , stack *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex*

説明クラスタ FSM イベント キューがいっぱいです。新しいイベントがドロップされました。

推奨アクション なし。

747002

エラーメッセージ %Threat Defense-5-747002: Clustering: Recovered from state machine dropped event (*event-id* , *ptr-in-hex* , *ptr-in-hex*). Intended state: *state-name* . Current state: *state-name* .

説明クラスタ FSM が現在の状態と一致しないイベントを受信しました。

推奨アクション なし。

747003

エラーメッセージ %Threat Defense-5-747003: Clustering: Recovered from state machine failure to process event (*event-id* , *ptr-in-hex* , *ptr-in-hex*) at state *state-name* .

説明クラスタ FSM が指定されたすべての理由に対するイベントの処理に失敗しました。

推奨アクション なし。

747004

エラーメッセージ %Threat Defense-6-747004: Clustering: state machine changed from state *state-name* to *state-name* .

説明クラスタ FSM は新しい状態に進みました。

推奨アクション なし。

747005

エラーメッセージ %Threat Defense-7-747005: Clustering: State machine notify event *event-name* (*event-id* , *ptr-in-hex* , *ptr-in-hex*)

説明クラスタ FSM がクライアントにイベントを通知しました。

推奨アクション なし。

747006

エラーメッセージ %Threat Defense-7-747006: Clustering: State machine is at state *state-name*

説明クラスタFSMが安定状態（ディセーブル、スレーブ、またはマスター）に移行しました。

推奨アクション なし。

747007

エラーメッセージ `%Threat Defense-5-747007: Clustering: Recovered from finding stray config sync thread, stack ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex .`

説明誤った場所に入った設定同期スレッドが検出されました。

推奨アクション なし。

747008

エラーメッセージ `%Threat Defense-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B .`

説明同じユニット名が複数のユニットに設定されています。

推奨アクション なし。

747009

エラーメッセージ `%Threat Defense-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name .`

説明 Secure Firewall Threat Defense デバイス が RPC サーバーの作成に失敗しました。

推奨アクションこの装置でのクラスタリングをディセーブルにし、もう一度イネーブルにしてみます。問題が続く場合には、Cisco TAC に連絡してください。

747010

エラーメッセージ `%Threat Defense-3-747010: Clustering: RPC call failed, message message-name , return code code-value .`

説明 RPC コール失敗が発生しました。システムは障害からの回復を試みます。

推奨アクション なし。

747011

エラーメッセージ `%Threat Defense-2-747011: Clustering: Memory allocation error.`

説明クラスタリングでメモリ割り当ての失敗が発生しました。

推奨アクションこの装置でのクラスタリングをディセーブルにし、もう一度イネーブルにしてみます。問題が解決しない場合は、Secure Firewall Threat Defense デバイス のメモリ使用量を確認してください。

747012

エラーメッセージ `%Threat Defense-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name , continuing operation.`

説明グローバル オブジェクト ID の複製に失敗しました。

推奨アクション なし。

747013

エラーメッセージ `%Threat Defense-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name , continuing operation.`

説明グローバル オブジェクト ID の削除に失敗しました。

推奨アクション なし。

747014

エラーメッセージ `%Threat Defense-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name , continuing operation.`

説明グローバル オブジェクト ID のインストールに失敗しました。

推奨アクション なし。

747015

エラーメッセージ `%Threat Defense-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.`

説明不適切なクラスタ メンバーが見つかりました。

推奨アクション なし。

747016

エラーメッセージ `%Threat Defense-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units. Master role retained by unit-name-A , unit-name-B will leave, then join as a slave.`

説明スプリット クラスタが見つかりました。

推奨アクション なし。

747017

エラーメッセージ `%Threat Defense-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.`

説明最大メンバー数の制限に到達したため、Secure Firewall Threat Defense デバイス は新しいユニットの登録に失敗しました。

推奨アクション なし。

747018

エラーメッセージ `%Threat Defense-3-747018: Clustering: State progression failed due to timeout in module module-name .`

説明クラスタ FSM の進行がタイム アウトしました。

推奨アクション なし。

747019

エラーメッセージ `%Threat Defense-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address /ip-mask on new unit, ip-address /ip-mask on local unit).`

説明 制御ユニットは、新規参加ユニットに互換性のないクラスタインターフェイスの IP アドレスがあることを検出しました。

推奨アクションなし。

747020

エラーメッセージ `%Threat Defense-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.`

説明 制御ユニットは、新規参加ユニットに互換性のない暗号化ライセンスがあることを検出しました。

推奨アクションなし。

747021

エラーメッセージ `%Threat Defense-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on interface-name .`

説明インターフェイスのヘルスチェックに失敗したため、制御ユニットはクラスタリングを無効にしました。

推奨アクションなし。

747022

エラーメッセージ `%Threat Defense-3-747022: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times, rejoin will be attempted after y min. Failed interface: interface-name .`

説明このsyslogメッセージは、再参加の最大試行回数を超えていない場合に出力されます。指定された時間にわたってインターフェイスのヘルスチェックに失敗したため、データユニットはクラスタリングを無効にしました。このユニットは、指定された時間（ミリ秒）後に自動的に再度イネーブルになります。

推奨アクション なし。

747025

エラーメッセージ `%Threat Defense-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.`

説明制御ユニットは、互換性のないファイアウォールモードを持つ参加ユニットを検出しました。

推奨アクションなし。

747026

エラーメッセージ `%Threat Defense-4-747026: Clustering: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit).`

説明 制御ユニットは、互換性のないクラスタ制御リンクのインターフェイス名を持つ参加ユニットを検出しました。

推奨アクションなし。

747027

エラーメッセージ `%Threat Defense-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name .`

説明最小クラスタプールのサイズ制限が設定されているため、制御ユニットは参加ユニットを登録できませんでした。

推奨アクションなし。

747028

エラーメッセージ `%Threat Defense-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).`

説明 制御ユニットは、互換性のないインターフェイスモード（spanned または individual）を持つ参加ユニットを検出しました。

推奨アクション なし。

747029

エラーメッセージ `%Threat Defense-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.`

説明 クラスタインターフェイスの障害のため、ユニットはクラスタリングをディセーブルにしました。

推奨アクション なし。

747030

エラーメッセージ `%Threat Defense-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name ), Clustering must be manually enabled on the unit to re-join.`

説明 インターフェイスのヘルスチェックが失敗し、再参加の最大試行回数を超えました。インターフェイスのヘルスチェックに失敗したため、データユニットはクラスタリングを無効にしました。

推奨アクション なし。

747031

エラーメッセージ `%Threat Defense-3-747031: Clustering: Platform mismatch between cluster master (platform-type ) and joining unit unit-name (platform-type ). unit-name aborting cluster join.`

説明 参加ユニットのプラットフォームタイプが、クラスタ制御ユニットのプラットフォームタイプと一致しません。

- *unit-name*：クラスタ ブートストラップ内のユニット名
- *platform-type*：Secure Firewall Threat Defense プラットフォームのタイプ

推奨アクション 参加ユニットのプラットフォームタイプは、必ずクラスタ制御ユニットのプラットフォームタイプと同じにしてください。

747032

エラーメッセージ `%Threat Defense-3-747032: Clustering: Service module mismatch between cluster master (module-name ) and joining unit unit-name (module-name )in slot slot-number . unit-name aborting cluster join.`

説明 参加ユニットの外部モジュール（モジュールタイプおよびそれらのインストール順）がクラスタ制御ユニットの外部モジュールと整合していません。

- *module-name*：外部モジュールの名前
- *unit-name*：クラスタ ブートストラップ内のユニット名
- *slot-number*：不一致が発生したスロットの番号

推奨アクション参加ユニットにインストールされているモジュールが、クラスタ制御ユニット内にあるものと同じタイプで、同じ順序であることを確認します。

747033

エラーメッセージ `%Threat Defense-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name . unit-name aborting cluster join.`

説明参加ユニットのインターフェイスがクラスタ制御ユニットのインターフェイスと同じではありません。

- *unit-name*：クラスタ ブートストラップ内のユニット名

推奨アクション 参加ユニットで使用可能なインターフェイスがクラスタ制御ユニットのインターフェイスと同じであることを確認します。

747034

エラーメッセージ `%Threat Defense-4-747034: Unit %s is quitting due to Cluster Control Link down (%d times after last rejoin). Rejoin will be attempted after %d minutes.`

説明 Cluster Control Link がダウンしており、装置が再参加でキックアウトされました。

推奨アクション 装置が再参加するまで待機します。

747035

エラーメッセージ `%Threat Defense-4-747035: Unit %s is quitting due to Cluster Control Link down. Clustering must be manually enabled on the unit to rejoin.`

説明 Cluster Control Link がダウンしており、装置は再参加なしでキックアウトされました。

推奨アクション 装置を手動で再参加させます。

747036

エラーメッセージ `%Threat Defense-3-747036: Application software mismatch between cluster master %s[Master unit name] (%s[Master application software name]) and joining unit (%s[Joining unit application software name]). %s[Joining member name] aborting cluster join.`

説明制御ユニットのアプリケーションと参加データユニットが同一ではありません。データユニットは削除されます。

推奨アクション データユニットが同じアプリケーション/サービスを実行していることを確認し、手動でユニットを再参加させます。

747042

エラーメッセージ `%Threat Defense-3-747042: Clustering: Master received the config hash string request message from an unknown member with id cluster-member-id`

説明 制御ユニットが設定ハッシュ文字列要求イベントを受信しました。

推奨アクション 要求元メンバーがまだ OnCall 状態にあることを確認します。

747043

エラーメッセージ `%Threat Defense-3-747043: Clustering: Get config hash string from master error: ret_code ret_code, string_len string_len`

説明 制御ユニットからの設定ハッシュ文字の取得に失敗しました。

- ret_code：エラーの戻りコード（0 は OK を示し、1 は失敗を示す）
- string_len：hash_str の長さ

推奨アクションテクニカルサポートに連絡して、制御ユニットの問題のトラブルシューティングを実行します。根本原因を特定するために「 debug cluster ccp 」がオンになっていることを確認してください。

747044

エラーメッセージ `%Threat Defense-6-747044: Configuration Hash string verification result`

説明 設定ハッシュ文字列の比較の結果です。

- result：この結果は PASSED または FAILED になります。

推奨アクション 不要。

748001

エラーメッセージ `%Threat Defense-5-748001: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis configuration change`

説明クラスタ制御リンクが MIO で変更された、クラスタ グループが MIO で削除された、またはブレード モジュールが MIO 構成で削除されました。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション 不要。

748002

エラーメッセージ `%Threat Defense-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled`

説明 MIO の構成が欠落しているか不完全です（たとえば、クラスタ グループが構成されていない、クラスタ制御リンクが構成されていないなど）。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO コンソールに移動してクラスタのサービス タイプを設定し、サービス タイプにモジュールを追加し、それに応じて Cluster Control Link を定義します。

748003

エラーメッセージ `%Threat Defense-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure`

説明ブレードは MIO と通信できないため、MIO に依存してこの通信の問題を検出し、データ ポートのバンドルを解除します。データ ポートのバンドルが解除されると、インターフェイスのヘルス チェックによって Secure Firewall Threat Defense デバイス がキックアウトされます。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO カードがアップしているか、または MIO とブレード間の通信がまだアップしているのかを確認します。

748004

エラーメッセージ `%Threat Defense-5-748004: Module slot_number in chassis chassis_number is re-joining the cluster due to a chassis health check recovery`

説明 MIO ブレードのヘルス チェックが回復し、Secure Firewall Threat Defense デバイス はクラスタの再参加を試行します。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO カードがアップしているか、または MIO とブレード間の通信がまだアップしているのかを確認します。

748005

エラーメッセージ `%Threat Defense-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number ; clustering is disabled`

説明 MIO は自身のためのポートのバンドルに失敗しました。

- *slot_number*：シャーシ内のブレード スロット ID

- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO が正しく動作しているかどうかを確認します。

748006

エラーメッセージ `%Threat Defense-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure`

説明 MIO がブレード用にポートをバンドルできなかったため、ブレードがキックアウトされました。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO が正しく動作しているかどうかを確認します。

748007

エラーメッセージ `%Threat Defense-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number ; traffic may be black holed`

説明 MIO はポートのバンドル解除に失敗しました。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO が正しく動作しているかどうかを確認します。

748008

エラーメッセージ `%Threat Defense-6-748008: [CPU load percentage | memory load percentage ] of module slot_number in chassis chassis_number (member-name ) exceeds overflow protection threshold [CPU percentage | memory percentage ]. System may be oversubscribed on member failure.`

説明 CPU の負荷が (N-1)/N を超えています（N はアクティブなクラスタ メンバーの合計数）。または、メモリの負荷が (100 – x) * (N – 1) / N + x を超えています（N はクラスタ メンバーの数、x は最後の参加メンバーの基準メモリ使用量）。

- *percentage*：CPU 負荷またはメモリ負荷のパーセンタイル データ
- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション ネットワークとクラスタリングの導入を再計画します。トラフィックの量を減らすか、またはブレード/シャーシを追加します。

748009

エラーメッセージ `%Threat Defense-6-748009: [CPU load percentage | memory load percentage ] of chassis chassis_number exceeds overflow protection threshold [CPU percentage | memory percentage }. System may be oversubscribed on chassis failure.`

説明 シャーシのトラフィック負荷が特定のしきい値を超えました。

- *percentage*：CPU 負荷またはメモリ負荷のパーセンタイル データ
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクションネットワークとクラスタリングの導入を再計画します。トラフィックの量を減らすか、またはブレード/シャーシを追加します。

748011

エラーメッセージ `%Threat Defense-4-748011: Mismatched resource profile size with Master. Master: cores number CPU cores / RAM size MB RAM, Mine: cores number CPU cores / RAM size MB RAM`

説明クラスタに参加しているユニットを制御ユニットと比較したときにリソースプロファイルサイズが異なっている場合、この syslog が参加ユニットに表示されます。

例

```
%Threat Defense-4-748011: Mismatched resource profile size with Master. Master: 6 CPU cores / 14426 MB RAM,  Mine: 8 CPU cores 19261 MB RAM.
```

推奨アクション 不要。

748012

エラーメッセージ `%Threat Defense-4-748012: Mismatched module type with Master. Master: PID, MINE: PID`

説明クラスタに参加しているユニットを制御ユニットと比較したときにモジュールタイプが異なっている場合、この syslog が参加ユニットに表示されます。

例

```
%Threat Defense-4-748012: Mismatched module type with Master. Master: FPR4K-SM-24, Mine:  FPR4K-SM-24s
```

推奨アクション 不要。

748100

エラーメッセージ `%Threat Defense-3-748100: <application_name> application status is changed from <status> to <status>.`

説明ある状態から別の状態へのアプリケーション状態の変化を検出します。アプリケーションステータスの変化によって、アプリケーションのヘルス チェック メカニズムがトリガーされます。

- application name：snort または disk_full
- status：init、up、down

推奨アクション アプリケーションのステータスを確認します。

748101

エラーメッセージ `%Threat Defense-3-748101: Peer unit <unit_id> reported its <application_name> application status is <status>.`

説明 ピアのユニットがアプリケーション状態の変化を報告したので、アプリケーションのヘルス チェック メカニズムが起動します。

- unit id：ユニット ID
- application name：snort または disk_full
- status：init、up、down

推奨アクション アプリケーションのステータスを確認します。

748102

エラーメッセージ `%Threat Defense-3-748102: Master unit <unit_id> is quitting due to <application_name> Application health check failure, and master's application state is <status>.`

説明 アプリケーションのヘルスチェックは、制御ユニットが正常でないことを検出します。制御ユニットはクラスタグループを離れます。

- unit id：ユニット ID
- application name：snort または disk_full
- status：init、up、down

推奨アクション アプリケーションのステータスを確認します。アプリケーション（snort）が再度起動すると、ユニットが自動的に再参加します。

748103

エラーメッセージ `%Threat Defense-3-748103: Asking slave unit <unit_id> to quit due to <application_name> Application health check failure, and slave's application state is <status>.`

説明 アプリケーションのヘルスチェックは、データユニットが正常でないことを検出します。制御ユニットはデータノードを削除します。

- unit id：ユニット ID

- application name：snort または disk_full
- status：init、up、down

推奨アクションアプリケーションのステータスを確認します。アプリケーション（snort）が再度起動すると、ユニットが自動的に再参加します。

748201

エラーメッセージ `%Threat Defense-4-748201: <Application name> application on module <module id> in chassis <chassis id> is <status>.`

説明サービス チェーン内のアプリケーションのステータスが変更されます。

- status：up、down

推奨アクション サービス チェーン内のアプリケーションのステータスを確認します。

748202

エラーメッセージ `%Threat Defense-3-748202: Module <module_id> in chassis <chassis id> is leaving the cluster due to <application name> application failure\n.`

説明 vDP などのアプリケーションに障害が発生した場合、ユニットはクラスタからキックアウトされます。

推奨アクション サービス チェーン内のアプリケーションのステータスを確認します。

748203

エラーメッセージ `%Threat Defense-5-748203: Module <module_id> in chassis <chassis id> is re-joining the cluster due to a service chain application recovery\n.`

説明 vDP などのサービス チェーン アプリケーションが回復すると、ユニットは自動的にクラスタに再参加します。

推奨アクション サービス チェーン内のアプリケーションのステータスを確認します。

750001

エラーメッセージ `%Threat Defense-5-750001: Local:`*`local IP`*` :`*`local port`* `Remote:`*`remote IP`*` : `*`remote port`* `Username: `*`username`* `Received request to `*`request`* `an IPsec tunnel; local traffic selector = `*`local selectors: range, protocol, port range`* ` ; remote traffic selector = `*`remote selectors: range, protocol, port range`*

説明キー再生成、接続確立の要求などの、IPSec トンネルに対する操作が要求されています。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号

- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモートアクセスの要求者のユーザー名（既知の場合）またはトンネルグループ
- *local selectors*：ローカルに設定されたトラフィック セレクタ、またはこの IPsec トンネルに使用されているプロキシ
- *remote selectors*：リモート ピアが要求したトラフィック セレクタ、またはこの IPsec トンネルのプロキシ

推奨アクション 不要。

750002

エラーメッセージ `%Threat Defense-5-750002: Local:local IP :local port Remote: remote IP : remote port Username: username Received a IKE_INIT_SA request`

説明着信トンネルまたは SA の開始要求（IKE_INIT_SA 要求）を受信しました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモートアクセスの要求者のユーザー名（既知の場合）またはトンネルグループ

推奨アクション 不要。

750003

エラーメッセージ `%Threat Defense-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error`

説明指摘されたエラー理由により、SA のネゴシエーションが打ち切られました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *error*：ネゴシエーション中止のエラーの理由。その場合のエラーは次のとおりです。

- Failed to send data on the network

- Asynchronous request queued

- Failed to enqueue packet

- A supplied parameter is incorrect

- Failed to allocate memory

- Failed the cookie negotiation
- Failed to find a matching policy
- Failed to locate an item in the database
- Failed to initialize the policy database
- Failed to insert a policy into the database
- The peer's proposal is invalid
- Failed to compute the DH value
- Failed to construct a NONCE
- An expected payload is missing from the packet
- Failed to compute the SKEYSEED
- Failed to create child SA keys
- The peer's KE payload contained the wrong DH group
- Received invalid KE notify, yet we've tried all configured DH groups
- Failed to compute a hash value
- Failed to authenticate the IKE SA
- Failed to compute or verify a signature
- Failed to validate the certificate
- The certificate has been revoked and is consequently invalid
- Failed to build or process a certificate request
- We requested a certificate, but the peer supplied none
- While sending the certificate chain, peer did not send its certificate as the first in the chain
- Detected an unsupported ID type
- Failed to construct an encrypted payload
- Failed to decrypt an encrypted payload
- Detected an invalid value in the packet
- The initiator bit is asserted in packet from original responder
- The initiator bit isn't asserted in packet from original initiator
- The message response bit is asserted in a packet from the exchange initiator
- The message response bit isn't asserted in a packet from the exchange responder
- Detected an invalid IKE SPI
- Packet is a retransmission
- Detected an invalid protocol ID
- Detected unsupported critical payload
- Detected an invalid traffic selector type

- Failed to create new SA
- Failed to delete SA
- Failed to add new SA into session DB
- Failed to add session to PSH
- Failed to delete session from osal
- Failed to delete a session from the database
- Failed to add request to SA
- Throttling request queue exceeds reasonable limit, increase the window size on peer
- Received an IKE msg id outside supported window
- Detected unsupported version number
- Received no proposal chosen notify
- Detected an error notify payload
- Detected NAT-d hash doesn't match
- Initialize sadb failed
- Initialize session db failed
- Failed to get PSH
- Negotiation context locked currently in use
- Negotiation context was not freed!
- Invalid data state found
- Failed to open PKI session
- Failed to insert public keys
- No certificate found
- Unsupported cert encoding found or Peer requested HTTP URL but never sent HTTP_LOOKUP_SUPPORTED Notification
- Sending BUNDLE URL is not supported at least for now. However, processing a BUNDLE URL is supported
- Local certificate has expired
- Failed to construct State Machine
- Error encountered while navigating State Machine
- SM Validation failed
- Could not find neg context
- Failed to add work request to SM Q
- Nonce payload is missing
- Traffic selector payload is missing
- Unsupported DH group

- Expected keypair is unavailable
- Packet isn't encrypted
- Packet is missing KE payload
- Packet is missing SA payload
- Invalid SA
- Invalid negotiation context
- Remote or local ID isn't defined
- Invalid connection id
- Unsupported auth method
- Ipsec policy not found
- Failed to initialize the event priority queue
- Failed to enqueue an item to a list
- Failed to remove an item from list
- Data in the event priority queue is NULL or corrupt
- No local IKE policy found
- Can't delete IKE SA due to in-progress task
- Expected Cookie Notify not received
- Failed to generate auth data: My auth info missing
- Failed to generate auth data: Failed to sign data
- Failed to generate auth data: Signature operation successful but unable to locate generated auth material
- Failed to receive the AUTH msg before the timer expired
- Maximum number of retransmissions reached
- Initial exchange failed
- Auth exchange failed
- Create child exchange failed
- Platform errors
- Failed to log a message
- Unwanted debug level turned on
- There are additional TS possible
- A single pairs of addresses is required
- Invalid session
- There was no IPSEC policy found for received TS
- Cannot remove request from window
- There was no proposal found in configured policy

- Nat-t test failure
- No pskey found
- Invalid compression algorithm
- Failed to get profile name from platform service handle
- Failed to find profile
- Initiator failed to match profile sent by IPSEC with profile found by peer id or certificate
- Failed to get peer id from platform service handle
- The transform attribute is invalid
- Extensible Authentication Protocol failed
- Authenticator sent NULL EAP message
- The config attribute is invalid
- Failed to calculate packet hash
- The AAA context is deleted
- Cannot alloc AAA ID
- Cannot alloc AAA request
- Cannot init AAA request
- The Authen list is not configured
- Fail to send AAA request
- Fail to alloc IP addr
- Invalid message context
- Key Auth memory failure
- EAP method does not generate MSK
- Failed to register new SA with platform
- Failed to async process session register, error: %d
- Failed to insert SA due to ipsec rekey collision
- Failed while handling a ipsec rekey collision
- Failed to accept rekey on SA that caused a rekey collision
- Failed to start timer to ensure IPsec collision SA SPI %s/%s will be deleted by the peer
- Error/Debug codes and strings are not matched
- Failed to initialize SA lifetime
- Failed to find rekey SA
- Failed to generate DH shared secret
- Failed to retrieve issuer public key hash list
- Failed to build certificate payload

- Unable to initialize the timer

- Failed to generate DH shared secret

- Failed to initialized authorization request

- Incorrect author record received from AAA

- Failed to fetch the keys from AAA

- Failed to add attribute to AAA request

- Failed to send tunnel password request to AAA

- Failed to allocate AAA context

- Insertion to policy AVL tree failed

- Deletion from policy AVL tree failed

- No Matching node found in policy AVL tree

- No Matching policy found

- No Matching proposal found

- Proposal is incomplete to be attached to the policy

- Proposal is in use

- Peer authentication method configured is mismatching with the method proposed by peer

- Failed to find the session in osal

- Failed to allocate event

- Failed to create accounting record

- Accounting not required

- Accounting not started for this session

- NAT-T disabled via cli

- Negotiating limit reached, deny SA request

- SA is already in negotiation, hence not negotiating again

- AAA グループ認証に失敗した

- AAA ユーザー認証に失敗した

- %% Dropping received fragment, as fragmentation is not negotiated for this SA!

- Maximum number of received fragments reached for the SA

- Number of fragments exceeds maximum allowed

- 構築されたパケット長 %d が最大 ikev2 パケット サイズ %d より大きい

- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet

- Received fragment is not valid, hence being dropped

- AAA グループ認証に失敗した

- AAA ユーザー認証に失敗した
- AAA author not configured in IKEv2 profile
- Failed to extract the skeyid
- Failed to send a failover msg to the standby unit
- Detected unsupported failover version
- Request was received but failover is not enabled
- Received an active unit request but the negotiated role is %s
- Received a standby unit request but the negotiated role is %s
- Invalid IP Version
- GDOI is not yet supported in IKEv2
- Failed to allocate PSH from platform
- Redirect the session to another gateway
- Redirect check failed
- Accept the session on this gateway after Redirect check
- Detected unsupported Redirect gateway ID type
- Redirect accepted, initiate new request
- Redirect accepted, clean-up IKEv2 SA, platform will initiate new request
- SA got redirected, it should not do any CREATE_CHILD_SA exchange
- DH public key computation failed
- DH secret computation failed
- IN-NEG IKEv2 Rekey SA got deleted
- Number of cert req exceeds the reasonable limit (%d)
- The negotiation context has been freed
- 構築されたパケット長 %d が最大 ikev2 パケット サイズ %d より大きい
- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet
- AAA 作成者が IKEv2 プロファイルに設定されていない
- Assembled packet is not valid, hence being dropped
- Invalid VCID context

推奨アクション syslog を確認し、ログのフローを追跡してこの syslog が交換の最後のものであるか、および再ネゴシエートされた潜在的な障害または一時的なエラーの原因かを判断します。たとえば、ピアは、設定されていない KE ペイロードによって DH グループを提案できます。これにより最初の要求が失敗しますが、ピアが新しい要求の中で正しいグループに戻ることができるように、正しい DH グループが伝えられます。

750004

エラーメッセージ `%Threat Defense-5-750004: Local: local IP: local port Remote: remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS`

説明着信接続要求で、DoS 攻撃を防ぐために設定されたクッキー チャレンジしきい値に基づいてクッキーが要求されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）

推奨アクション 不要。

750005

エラーメッセージ `%Threat Defense-5-750005: Local: local IP: local port Remote: remote IP: remote port Username: username IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI SPI`

説明キー再生成コリジョンが検出され（両方のピアで同時にキー再生成を開始しようとしている）、最も小さいナンスを持っていたため、この Secure Firewall Threat Defense デバイス が開始したほうを保持することでコリジョンが解決されました。この操作によって、SPI により参照されている指摘された SA が削除されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *SPI*：検出されたキー再生成コリジョンを解決することによって検出される SA の SPI ハンドル

推奨アクション 不要。

750006

エラーメッセージ `%Threat Defense-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP. Reason: reason`

説明新たに確立された接続またはキー再生成などの理由で、SA がアップ状態になりました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）

- *reason*：SA がアップ状態になった理由

推奨アクション 不要。

750007

エラーメッセージ `%Threat Defense-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN. Reason: reason`

説明ピアからの要求、オペレータ要求（管理者アクションを通して）、キー再生成などの指摘された理由により、SA が切断または削除されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *reason*：SA がダウン状態になった理由

推奨アクション 不要。

750008

エラーメッセージ `%Threat Defense-5-750008: Local: local IP: local port Remote: remote IP: remote port Username: username SA rejected due to system resource low`

説明 SA 要求は、システム リソースの低下状態を軽減するために拒否されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）

推奨アクション IKEv2 の CAC 設定を確認し、これが設定されたしきい値に基づく予期された動作であるかどうかを判断します。そうではなく、問題が続く場合は、問題を軽減するために、さらに調査します。

750009

エラーメッセージ `%Threat Defense-5-750009: Local: local IP: local port Remote: remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason`

説明コネクション アドミッション制御（CAC）制限しきい値に達し、SA 要求が拒否されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号

- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *reason*：SA が拒否された理由

推奨アクション IKEv2 の CAC 設定を確認し、これが設定されたしきい値に基づく予期された動作であるかどうかを判断します。そうではなく、問題が続く場合は、問題を軽減するために、さらに調査します。

750010

エラーメッセージ `%Threat Defense-5-750010: Local: local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance`

- *local-ip*：ローカル ピアの IP アドレス
- *remote-ip*：リモート ピアの IP アドレス
- *username*：リモート アクセスの要求者のユーザー名、または、その時点でも既知の場合は、L2L のトンネル グループ名
- *threshold*：到達したローカル スロットル要求のキューの深さのしきい値
- *peer*：リモート ピアの IP アドレス

説明 指定されたピアに Secure Firewall Threat Defense デバイス がスロットル要求キューをオーバーフローしました。これは、ピアが低速になりことを示しています。スロットル要求キューは、ピアへの要求を保持します。IKEv2 のウィンドウ サイズに基づいて対応できる最大数の要求がすでに対応中だったため、すぐには送信できません。送信中の要求が完了すると、要求はスロットル要求キューから引き出されてピアに送信されます。ピアがこれらの要求を迅速に処理していない場合は、スロットル キューが保持します。

推奨アクション 可能な場合は、リモート ピアの IKEv2 のウィンドウ サイズを引き上げ、より多くの同時要求を送信できるようにします。これでパフォーマンスが向上する場合があります。

（注） Secure Firewall Threat Defense デバイス では現在、IKEv2 のウィンドウ サイズ設定の引き上げをサポートしていません。

750011

エラーメッセージ `%Threat Defense-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

説明選択された IKEv2 暗号化アルゴリズムが、提示された IPSec 暗号化アルゴリズムの安全を保護するのに十分な強度ではないため、トンネルが拒否されました。

推奨アクション IPSec 子 SA 暗号化アルゴリズムの強度に匹敵するかそれを上回る、より強力な IKEv2 暗号化アルゴリズムを設定します。

750012

エラーメッセージ `%Threat Defense-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

説明選択された IKEv2 暗号化アルゴリズムは、提示された IPSec 暗号化アルゴリズムの安全を保護するのに十分な強度ではありません。

推奨アクション IPSec 子 SA 暗号化アルゴリズムの強度に匹敵するかそれを上回る、より強力な IKEv2 暗号化アルゴリズムを設定します。

750013

エラーメッセージ `%Threat Defense-5-750013 - IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev_remote_ip>:<prev_remote_port>/<prev_local_ip>:<prev_local_port>. Updated <new_remote_ip>:<new_remote_port>/<new_local_ip>:<new_local_port>`

説明 新しいモバイル機能を使用すると、トンネルを切断しなくてもピア IP を変更できます。たとえば、モバイル デバイス（スマートフォン）は別のネットワークに接続した後に新しい IP を取得します。次のリストでメッセージ値について説明します。

- *ip*：以前の IP アドレスと、新しいローカルおよびリモートのIP アドレスを指定します
- *port*：以前のポート情報と、新しいローカルおよびリモートのポート情報
- *SPI*：イニシエータおよびレスポンダ SPI を示します
- *iSPI*：イニシエータ SPI を指定します
- *rSPI*：レスポンダ SPI を指定します

推奨アクション 開発エンジニアにお問い合わせください。

751001

エラーメッセージ `%Threat Defense-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to complete Diffie-Hellman operation. Error: error`

説明 error で示されているように、Diffie-Hellman オペレーションを完了できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定のエラーを示すエラー文字列

推奨アクション ロー メモリの問題か、または解決する必要があるその他の内部エラーが発生しました。このステートが続く場合、問題の識別のためにメモリ追跡ツールを使用します。

751002

エラーメッセージ `%Threat Defense-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group No preshared key or trustpoint configured for self in tunnel group group`

説明 Secure Firewall Threat Defense デバイス は、ピアに対する自身の認証に使用可能な、何らかの種類の認証情報をトンネル グループ中に見つけることができませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *group*：トンネル グループの名前

推奨アクション トンネル グループの設定を確認し、示されているトンネル グループでの自己認証用の事前共有キーまたは証明書を設定します。

751003

エラーメッセージ `%Threat Defense-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group Need to send a DPD message to peer`

説明指定したピアが起動しているかどうかを確認するため、デッドピア検出を実行する必要があります。Secure Firewall Threat Defense デバイス は、ピアへの接続を終了した可能性があります。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション 不要。

751004

エラーメッセージ `%Threat Defense-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group No remote authentication method configured for peer in tunnel group group`

説明接続を許可するためにリモート ピアを認証するための方法が、コンフィギュレーション中に見つかりませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *group*：トンネル グループの名前

推奨アクション 設定を調べ、有効なリモート ピア認証設定があることを確認します。

751005

エラーメッセージ `%Threat Defense-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group AnyConnect client reconnect authentication failed. Session ID: sessionID , Error: error`

説明 セッション トークンを使用した AnyConnect クライアントの再接続の試行中に障害が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *sessionID*：再接続の試行に使用されたセッション ID
- *error*：再接続試行中に発生した特定のエラーを示すエラー文字列

推奨アクション 必要に応じて、指摘されたエラーに従って処置を実行します。このエラーは、クライアントの切断が検出されるか、Secure Firewall Threat Defense デバイス 上でセッションがクリアされたことにより、再開状態を維持する代わりにセッションが削除されたことを示している場合があります。必要に応じて、このメッセージを、Anyconnect クライアント上のイベント ログと比較します。

751006

エラーメッセージ `%Threat Defense-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group Certificate authentication failed. Error: error`

説明 証明書認証に関連した障害が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定の証明書認証障害を示すエラー文字列

推奨アクション 必要に応じて、指摘されたエラーに従って処置を実行します。証明書トラストポイントの設定を確認し、クライアント証明書チェーンが適切に確認できるように、必要な CA 証明書が存在することを確認します。障害を切り分けるには **debug crypto ca** コマンドを使用します。

751007

エラーメッセージ `%Threat Defense-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group Configured attribute not supported for IKEv2. Attribute: attribute`

説明設定された属性は、IKE バージョン 2 接続でサポートされないため、IKE バージョン 2 接続に適用できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号

- *username/group*：この接続試行に関連するユーザー名またはグループ
- *attribute*：適用するように設定した属性

推奨アクション 不要。このメッセージが生成されないようにするには、IKE バージョン 2 構成設定を削除します。

751008

エラーメッセージ `%Threat Defense-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group  Group=group , Tunnel rejected: IKEv2 not enabled in group policy`

説明 接続試行がマッピングされた、指摘されたグループで有効なプロトコルに基づき、IKE バージョン 2 は許可されず、接続が拒否されました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *group*：接続に使用したトンネル グループ

推奨アクション グループ ポリシーの VPN トンネル プロトコルの設定を確認し、必要に応じて IKE バージョン 2 をイネーブルにします。

751009

エラーメッセージ `%Threat Defense-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to find tunnel group for peer.`

説明 ピアのトンネル グループを検出できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション 設定およびトンネル グループ マッピングのルールを確認してから、設定したグループにピアが到達できるようにそれらを設定します。

751010

エラーメッセージ `%Threat Defense-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group  Unable to determine self-authentication method. No crypto map setting or tunnel group found.`

説明 Secure Firewall Threat Defense デバイス がピアを認証する方式がトンネル グループでも、暗号マップでも見つかりませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション設定を確認し、イニシエータL2L用の暗号マップ内か、または該当するトンネル グループ内に自己認証方式を設定します。

751011

エラーメッセージ `%Threat Defense-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group Failed user authentication. Error: error`

説明 ユーザー認証中に、IKE バージョン 2 のリモート アクセス接続用の EAP 内で障害が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定のエラーを示すエラー文字列

推奨アクション正しい認証クレデンシャルが提供されていることを確認し、必要に応じて、さらにデバッグを実行して障害の正確な原因を突き止めます。

751012

エラーメッセージ `%Threat Defense-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group Failure occurred during Configuration Mode processing. Error: error`

説明コンフィギュレーションモードの処理中に、設定を接続に適用しているときにエラーが発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定のエラーを示すエラー文字列

推奨アクション 示されているエラーに基づいてアクションを実行します。**debug crypto ikev2** コマンドを使用して失敗の原因を特定するか、エラーによって指摘されたサブシステムを必要に応じてデバッグします。

751013

エラーメッセージ `%Threat Defense-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to process Configuration Payload request for attribute attribute ID . Error: error`

説明ピアによって要求された Configuration Payload 要求の処理に失敗し、属性に対する Configuration Payload 応答を生成できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

- *attribute ID*：障害が発生した属性 ID
- *error*：特定のエラーを示すエラー文字列

推奨アクション メモリ エラー、設定エラー、または別のタイプのエラーが発生しました。障害の原因を切り分けるには、**debug crypto ikev2** コマンドを使用します。

751014

エラーメッセージ `%Threat Defense-4-751014: Local: localIP:port Remote remoteIP:port Username: username/group Warning Configuration Payload request for attribute attribute ID could not be processed. Error: error`

説明 要求された属性に CP 応答を生成する CP 要求の処理の最中に警告が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *attribute ID*：障害が発生した属性 ID
- *error*：特定のエラーを示すエラー文字列

推奨アクション 警告に示されている属性と、示されている警告メッセージに基づいて、アクションを実行します。たとえば、新しいクライアントが、クライアントに追加された新しい属性を認識しない古い Secure Firewall Threat Defense イメージで使用されています。属性を処理できるように、Secure Firewall Threat Defense イメージのアップグレードが必要な場合があります。

751015

エラーメッセージ `%Threat Defense-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group SA request rejected by CAC. Reason: reason`

説明 リストされている理由で示されている設定済みのしきい値または条件に基づいて Secure Firewall Threat Defense デバイス を保護するため、コール アドミッション制御によって接続が拒否されました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *reason*：SA 要求が拒否された理由

推奨アクション 理由を確認し、新しい接続が許可される必要があった場合は条件を解決するか、または設定されているしきい値を変更します。

751016

エラーメッセージ `%Threat Defense-4-751016: Local: localIP:port Remote remoteIP:port Username: username/group  L2L peer initiated a tunnel with the same outer and inner addresses. Peer could be Originate only - Possible misconfiguration!`

説明 ピアは、トンネルの受信した外部 IP アドレスと内部 IP アドレスに基づいて発信専用接続用に設定されている可能性があります。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション L2L ピアの設定を確認します。

751017

エラーメッセージ `%Threat Defense-3-751017: Local: localIP:port Remote remoteIP:port Username: username/group  Configuration Error error description`

説明接続を妨げるコンフィギュレーション エラーが検出されました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error description*：接続エラーの簡単な説明

推奨アクション 示されているエラーに基づいて設定を修正します。

751018

エラーメッセージ `%Threat Defense-3-751018: Terminating the VPN connection attempt from attempted group . Reason: This connection is group locked to locked group .`

説明接続が試行されるトンネル グループは、グループ ロックに設定されているトンネル グループと同じではありません。

- *attempted group*：接続が着信するトンネル グループ
- *locked group*：接続がロックまたは限定されるトンネル グループ

推奨アクション グループ ポリシーまたはユーザー属性でグループ ロック値を確認します。

751019

エラーメッセージ `%Threat Defense-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license. Maximum license limit limit exceeded.`

説明最大ライセンス制限を超えたため、セッション作成に失敗しました。そのため、トンネル要求の開始または応答に失敗しました。

- *LocalAddr*：この接続試行のローカル アドレス
- *RemoteAddr*：この接続試行のリモート ピア アドレス
- *username*：接続を試行しているピアのユーザー名
- *licenseType*：超過したライセンス タイプ（他の VPN または AnyConnect Premium/Essentials）

- *limit*：許可され、超過したライセンスの数

推奨アクション 許可されているすべてのユーザーに利用するために十分な数のライセンスがあることを確認するか、または拒否された接続を許可するためにより多くのライセンスを取得します。あるいは、その両方を実行します。マルチ コンテキスト モードの場合、障害を報告したコンテキストに対し、必要に応じてより多くのライセンスを割り当てます。

751020

エラーメッセージ `%Threat Defense-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.`

説明 AnyConnect Premium ライセンスは適用されましたが、webvpn コンフィギュレーション モードで **anyconnect-essentials** を使用して明示的にディセーブルにされているため、IKEv2 リモート アクセス トンネルを作成できませんでした。

推奨アクション Secure Firewall Threat Defense デバイス に AnyConnect Premium ライセンスがインストールされ、リモート アクセス IKEv2 ポリシーまたは IPsec プロポーザルに設定されていることを確認します。

751021

エラーメッセージ `%Threat Defense-4-751021: Local:variable 1 :variable 2 Remote:variable 3 :variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest Anyconnect Client.`

説明 古い AnyConnect クライアントが、AES-GCM 暗号化ポリシーを使用して IKEv2 が設定されている Secure Firewall Threat Defense デバイス に接続しようとしました。

- *variable 1*：ローカル IP アドレス
- *variable 2*：ローカル ポート
- *variable 3*：リモート クライアント IP アドレス
- *variable 4*：リモート クライアント ポート
- *variable 5*：AnyConnect クライアントのユーザー名（ユーザーがユーザー名を入力する前にこのエラーが発生したため、不明である可能性もあります）
- *variable 6*：接続プロトコル タイプ（IKEv1、IKEv2）
- *variable 7*：連結モード暗号化タイプ（AES-GCM、AES-GCM 256）

推奨アクション AES-GCM 暗号化で IKEv2 を使用するため、AnyConnect クライアントを最新バージョンにアップグレードします。

751022

エラーメッセージ `%Threat Defense-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start /rem-ts-end /rem-ts.startport /rem-ts.endport /rem-ts.protocol local traffic`

`selector local-ts-start /local-ts-end /local-ts.startport /local-ts.endport /local-ts.protocol !`

説明 Secure Firewall Threat Defense デバイス が、メッセージに示されているプライベート ネットワークまたはホストのセキュリティ ポリシー情報を検出できませんでした。これらのネットワークまたはホストは、発信側によって送信され、Secure Firewall Threat Defense デバイス のどの暗号 ACL とも一致しません。多くの場合、これはコンフィギュレーションの誤りです。

- *local-ip*：ローカル ピアの IP アドレス
- *remote-ip*：リモート ピアの IP アドレス
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *rem-ts-start*：リモート トラフィック セレクタの開始アドレス
- *rem-ts-end*：リモート トラフィック セレクタの終了アドレス
- *rem-ts.startport*：リモート トラフィック セレクタの開始ポート
- *rem-ts.endport*：リモート トラフィック セレクタの終了ポート
- *rem-ts.protocol*：リモート トラフィック セレクタのプロトコル
- *local-ts-start*：ローカル トラフィック セレクタの開始アドレス
- *local-ts-end*：ローカル トラフィック セレクタの終了アドレス
- *local-ts.startport*：ローカル トラフィック セレクタの開始ポート
- *local-ts.endport*：ローカル トラフィック セレクタの終了ポート
- local-*ts.protocol*：ローカル トラフィック セレクタのプロトコル

推奨アクション 両側の暗号化 ACL の保護されているネットワーク設定を確認し、イニシエータのローカル ネットワークがレスポンダのリモート ネットワークであること、およびイニシエータのリモート ネットワークがレスポンダのローカル ネットワークであることを確認します。ワイルドカード マスクと、ネットワーク アドレスと比較したホスト アドレスに特に注意します。シスコ以外の実装では、プロキシ アドレスまたは「red」ネットワークというラベルが付いたプライベート アドレスがある場合があります。

751023

エラーメッセージ `%Threat Defense-6-751023: Local a :p Remote: a :p Username:n Unknown client connection`

説明未知またはシスコ以外の IKEv2 クライアントが Secure Firewall Threat Defense デバイス に接続しました。

- *n*：グループまたはユーザー名（コンテキストによる）
- *a*：IP アドレス
- *p*：ポート番号
- *ua*：クライアントが Secure Firewall Threat Defense デバイス に提示したユーザーエージェント

推奨アクション シスコがサポートしている IKEv2 クライアントにアップグレードします。

751024

エラーメッセージ `%Threat Defense-3-751024: Local:ip-addr Remote:ip-addr Username:username IKEv2 IPv6 User Filter tempipv6 configured. This setting has been deprecated, terminating connection`

説明 IPv6 VPN フィルタは廃止されており、IPv6 トラフィックのアクセス制御に統合フィルタの代わりに設定されている場合は、接続が終了します。

推奨アクション IPv6 エントリで統合フィルタを設定し、ユーザー用の IPv6 トラフィックを制御します。

751025

エラーメッセージ `%Threat Defense-5-751025: Local: local IP :local port Remote: remote IP :remote port Username:username Group:group-policy IPv4 Address=assigned_IPv4_addr IPv6 address=assigned_IPv6_addr assigned to session.`

説明このメッセージには、指定されたユーザーの AnyConnect IKEv2 接続に割り当てられた IP アドレス情報が表示されます。

- *local IP* :*local port*：この要求のローカル IP アドレスこの接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP* :*remote port*：この要求のリモート IP アドレス接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *group-policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *assigned_IPv4_addr*：クライアントに割り当てられている IPv4 アドレス
- *assigned_IPv6_addr*：クライアントに割り当てられている IPv6 アドレス

推奨アクション 不要。

751026

エラーメッセージ `%Threat Defense-6-751026: Local: localIP:port Remote: remoteIP:port Username: username/group IKEv2 Client OS: client-os Client: client-name client-version`

説明指摘されたユーザーが、表示されているオペレーティング システムとクライアントのバージョンに接続しようとしています。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *client-os*：クライアントが報告したオペレーティング システム
- *client-name*：クライアントが報告したクライアント名（通常は AnyConnect）
- *client-version*：クライアントが報告したクライアント バージョン

推奨アクション 不要。

751027

エラーメッセージ `%Threat Defense-4-751027: Local:local IP :local port Remote:peer IP :peer port Username:username IKEv2 Received INVALID_SELECTORS Notification from peer. Peer received a packet (SPI=spi). The decapsulated inner packet didn't match the negotiated policy in the SA. Packet destination pkt_daddr , port pkt_dest_port , source pkt_saddr , port pkt_src_port , protocol pkt_prot .`

説明 ピアが IPsec セキュリティ アソシエーション（SA）上で受信したパケットが、その SA のネゴシエートされたトラフィック記述子に一致しませんでした。ピアは、不正パケットの SPI とパケット データを含む INVALID_SELECTORS 通知を送信しました。

- *local IP*：Secure Firewall Threat Defense ローカル IP アドレス
- *local port*：Secure Firewall Threat Defense ローカル ポート
- *peer IP*：ピアとなる IP アドレス
- *peer port*：ピア ポート
- *username*：ユーザー名
- *spi*：パケットの IPsec SA の SPI
- *pkt_daddr*：パケット宛先 IP アドレス
- *pkt_dest_port*：パケット宛先ポート
- *pkt_saddr*：パケット送信元 IP アドレス
- *pkt_src_port*：パケット送信元ポート
- *pkt_prot*：パケット プロトコル

推奨アクション エラー メッセージ、設定、およびこのエラーにつながったイベントの詳細をコピーし、それらを Cisco TAC に送信してください。

752001

エラーメッセージ `%Threat Defense-2-752001: Tunnel Manager received invalid parameter to remove record`

説明 トンネルマネージャからレコードを削除できませんでした。これにより、同じピアに今後トンネルを開始できない可能性があります。

推奨アクション デバイスをリロードするとレコードは削除されますが、エラーが解決しないか、または再発する場合は、特定のトンネル試行のデバッグをさらに実行します。

752002

エラーメッセージ `%Threat Defense-7-752002: Tunnel Manager Removed entry. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明 トンネルを開始するエントリが正常に削除されました。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 不要。

752003

エラーメッセージ `%Threat Defense-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2. Map Tag = mapTag . Map Sequence Number = mapSeq`

説明 示されている暗号マップに基づいたIKEv2トンネルを開始するための試行を実行中です。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 不要。

752004

エラーメッセージ `%Threat Defense-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1. Map Tag = mapTag . Map Sequence Number = mapSeq`

説明 示されている暗号マップに基づいたIKEv1トンネルを開始するための試行を実行中です。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 不要。

752005

エラーメッセージ `%Threat Defense-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Memory may be low. Map Tag = mapTag . Map Sequence Number = mapSeq.`

説明 トンネル開始試行をディスパッチしようとしましたが、メモリ割り当ての障害などの内部エラーによって失敗しました。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション メモリ トラッキング ツールを使用し、さらにデバッグを実行することで問題を切り分けます。

752006

エラーメッセージ `%Threat Defense-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = Tag . Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port .`

説明 トンネルの開始の試行をディスパッチしようとして、指摘されたクリプトマップまたは関連付けられているトンネル グループのコンフィギュレーション エラーが原因で、失敗しました。

- *Tag*：開始エントリが削除された暗号マップの名前
- *num*：開始エントリが削除された暗号マップのシーケンス番号

- *address*：送信元 IP アドレスまたは宛先 IP アドレス
- *port*：送信元ポート番号または宛先ポート番号

推奨アクション 示されているトンネル グループと暗号マップの設定を調べ、完全であることを確認します。

752007

エラーメッセージ `%Threat Defense-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = mapTag . Map Sequence Number = mapSeq`

説明 既存のエントリをトンネル マネージャに再追加しようとしました。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 問題が解決しない場合は、ピアの設定でトンネルが許可されることを確認し、さらにデバッグを実行して、トンネル開始時にトンネルマネージャのエントリが追加されてから正しく削除されること、および開始試行の成否を確認します。引き続きトンネルの作成中である可能性があるため、IKE バージョン 2 または IKE バージョン 1 の接続をさらにデバッグします。

752008

エラーメッセージ `%Threat Defense-7-752008: Duplicate entry already in Tunnel Manager`

説明 トンネルを開始するための重複した要求が行われ、トンネルマネージャは、すでにトンネルを開始しようとしています。

推奨アクション 不要。問題が解消されない場合、IKE バージョン 1 または IKE バージョン 2 がトンネルの開始を試行し、まだタイムアウトしていない可能性があります。該当するコマンドを使用してさらにデバッグし、開始の試行が成功または失敗した後に、トンネルマネージャ エントリが削除されることを確認します。

752009

`%Threat Defense-4-752009: IKEv2 Doesn't support Multiple Peers`

説明 複数のピアを使用してクリプトマップが設定されているため、IKE バージョン 2 のトンネルを開始する試みが失敗しました。この設定は、IKE バージョン 2 でサポートされていません。IKE バージョン 1 のみが複数のピアをサポートします。

推奨アクション 設定を確認し、複数のピアでの IKE バージョン 2 のサイト間での開始が予期されていないことを確認します。

752010

エラーメッセージ `%Threat Defense-4-752010: IKEv2 Doesn't have a proposal specified`

説明 IKE バージョン 2 トンネルを開始するための IPSec プロポーザルが見つかりませんでした。

推奨アクション 設定を確認し、必要に応じて、トンネルの開始に使用できる IKE バージョン 2 プロポーザルを設定します。

752011

エラーメッセージ `%Threat Defense-4-752011: IKEv1 Doesn't have a transform set specified`

説明 IKE バージョン 2 トンネルを開始するための、IKE バージョン 1 トランスフォーム セットが見つかりませんでした。

推奨アクション 設定を確認し、必要に応じて、トンネルの開始に使用できる IKE バージョン 2 トランスフォーム セットを設定します。

752012

エラーメッセージ `%Threat Defense-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明指摘されたプロトコルが、設定されたクリプトマップを使用してトンネルを開始できませんでした。

- *protocol*：IKEv1 または IKEv2 を示す IKE バージョン番号 1 または 2
- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション設定を確認し、示されているプロトコル内をさらにデバッグしてトンネル試行が失敗した原因を特定します。

752013

エラーメッセージ `%Threat Defense-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明トンネル マネージャは、失敗した後に、トンネルを再開しようとしています。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション設定を調べ、暗号マップが正しく設定されていることを確認します。その後、トンネルが、2 回目の試行で正常に作成されたことを確認します。

752014

エラーメッセージ `%Threat Defense-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明トンネル失敗後、トンネル マネージャはフォール バックし、IKE バージョン 1 を使用してトンネルを開始しようとしています。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 設定を確認し、クリプト マップが正しく設定されていることを確認します。その後、トンネルが、2 回目の試行で正常に作成されたことを確認します。

752015

エラーメッセージ `%Threat Defense-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明ピアへの L2L トンネルを確立する試行が、設定されたすべてのプロトコルを使用して試行した後に失敗しました。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 設定を確認し、クリプト マップが正しく設定されていることを確認します。障害の原因を特定するには、個々のプロトコルをデバッグします。

752016

エラーメッセージ `%Threat Defense-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq.`

説明 示されているプロトコル（IKE バージョン 1 または IKE バージョン 2）で L2L トンネルが正常に作成されました。

- *protocol*：IKEv1 または IKEv2 を示す IKE バージョン番号 1 または 2
- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 不要。

752017

エラーメッセージ `%Threat Defense-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name , sequence number number . Unsupported configuration.`

説明 IKEv2 はバックアップ L2L をサポートしていないため、Secure Firewall Threat Defense デバイス は IKEv1 を使用して接続を開始します。

推奨アクション IKEv1 がイネーブルの場合、処置は不要です。バックアップ L2L 機能を使用するには、IKEv1 をイネーブルにする必要があります。

753001

エラーメッセージ `%Threat Defense-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>`

説明 クラスタが分散型 VPN クラスタリング モードで動作しており、データパスで実行した初期の整合性チェックまたはエラーチェック、あるいはその両方が失敗したときに IKEv2 パケットを受信してこの syslog が生成されます。

- <IP>：パケットを送信した送信元 IP アドレス
- <port>：パケットを送信した送信元ポート
- <reason>：パケットが無効とみなされている理由この値は *Corrupted SPI detected* または *Expired SPI received* である可能性があります。

推奨アクション IKEv1 がイネーブルの場合、処置は不要です。バックアップ L2L 機能を使用するには、IKEv1 をイネーブルにする必要があります。

767001

エラーメッセージ `%Threat Defense-6-767001: Inspect-name : Dropping an unsupported IPv6/IP46/IP64 packet from interface :IP Addr to interface :IP Addr (fail-close)`

説明 fail-close オプションがサービス ポリシーに設定され、特定の検査によって IPv6、IP64、または IP46 のパケットが受信されています。fail-close オプション設定に基づいて、この syslog メッセージが生成され、パケットはドロップされます。

推奨アクション 不要。

768001

エラーメッセージ `%Threat Defense-3-768001: QUOTA: resource utilization is high: requested req , current curr , warning level level`

説明 システム リソースの割り当てレベルが警告しきい値に達しました。管理セッションの場合、リソースは同時管理セッションです。

- *resource*：システム リソース名。この場合は管理セッションです。
- *req*：要求された数。管理セッションでは常に 1 です。
- *curr*：現在の割り当て数。管理セッションでは *level* と等しくなります。
- *level*：警告レベル。設定されている制限の 90 %。

推奨アクション 不要。

768002

エラーメッセージ `%Threat Defense-3-768002: QUOTA: resource quota exceeded: requested req , current curr , limit limit`

説明システム リソースに対する要求は、設定された制限を超過したため拒否されました。管理セッションの場合、システムの同時管理セッションの最大数に到達しました。

- *resource*：システム リソース名。この場合は管理セッションです。
- *req*：要求された数。管理セッションでは常に 1 です。
- *curr*：現在の割り当て数。管理セッションでは *level* と等しくなります。
- *limit*：設定されているリソース制限

推奨アクション 不要。

768003

エラーメッセージ `%Threat Defense-3-768003: QUOTA: management session quota exceeded for user user name: current 3, user limit 3`

説明 現在の管理セッションが、ユーザーに設定されている制限を超えました。

- *current*：ユーザーの管理セッションに割り当てられている現在の番号
- *limit*：設定されている管理セッションの制限（デフォルト値は 15）

推奨アクション必要なし。

768004

エラーメッセージ `%Threat Defense-3-768004: QUOTA: management session quota exceeded for ssh/telnet/http protocol: current 2, protocol limit 2`

説明 プロトコル（SSH、Telnet、または HTTP）の管理セッションの最大数が、設定されている制限を超えました。

- *current*：管理セッションに割り当てられている現在の番号
- *limit*：設定されているプロトコルあたりのリソース制限（デフォルト値は 5）

推奨アクション必要なし。

769001

エラーメッセージ `%Threat Defense-5-769001: UPDATE: ASA image src was added to system boot list`

説明システムイメージが更新されました。以前にシステムにダウンロードされたファイルの名前が、システム ブートのリストに追加されました。

- *src*：送信元イメージファイルの名前または URL

推奨アクション 不要。

769002

エラーメッセージ `%Threat Defense-5-769002: UPDATE: ASA image src was copied to dest`

説明システムイメージが更新されました。イメージファイルがシステムにコピーされました。

- *src*：ソース イメージ ファイルの名前または URL
- *dest*：コピー先のイメージ ファイルの名前

推奨アクション 不要。

769003

エラーメッセージ `%Threat Defense-5-769003: UPDATE: ASA image src was renamed to dest`

説明システム イメージが更新されました。既存のイメージ ファイル名は、システム ブート リスト内のイメージ ファイル名に変更されました。

- *src*：ソース イメージ ファイルの名前または URL
- *dest*：コピー先のイメージ ファイルの名前

推奨アクション 不要。

769004

エラーメッセージ `%Threat Defense-2-769004: UPDATE: ASA image src_file failed verification, reason: failure_reason`

説明イメージは、copy コマンドまたは verify コマンドのいずれかで検証に失敗しました。

- *src_file*：送信元イメージ ファイルのファイル名または URL
- *failure_reason*：宛先イメージ ファイルのファイル名

推奨アクション 障害の考えられる理由として、システム メモリが不足している、ファイルでイメージが見つからなかった、チェックサムに失敗した、ファイルで署名が見つからなかった、署名が無効だった、署名のアルゴリズムがサポートされていない、署名処理の問題があります。

769005

エラーメッセージ `%Threat Defense-5-769005: UPDATE: ASA image image_name passed image verification.`

説明これは、イメージが検証に合格したことを示す通知メッセージです。

- *image_name*：Secure Firewall Threat Defense イメージファイルの名前

推奨アクション 不要。

769006

エラーメッセージ `%Threat Defense-3-769006: UPDATE: ASA boot system image image_name was not found on disk.`

説明これは、ブート システム リストで設定されたファイルをディスク上に置くことができなかったことを示すエラー メッセージです。

- *image_name*：Secure Firewall Threat Defense イメージファイルの名前

推奨アクションデバイスがブートできない場合は、デバイスをリブートする前に有効なファイルをポイントするように boot system コマンドを変更するか、または欠落しているファイルをディスクにインストールします。

769007

エラーメッセージ `%Threat Defense-6-769007: UPDATE: Image version is version_number`

説明 このメッセージは、デバイスがアップグレードされると表示されます。

- *version_number*：Secure Firewall Threat Defense イメージファイルのバージョン番号

推奨アクション必要なし。

769009

エラーメッセージ `%Threat Defense-4-769009: UPDATE: Image booted image_name is different from boot images.`

説明これは、設定されたファイルがブートイメージの既存のリストと異なることを示す、デバイスのアップグレード後に表示されるエラーメッセージです。

- *image_name*：Secure Firewall Threat Defense イメージ ファイルのファイル名

推奨アクション 不要。

770001

エラーメッセージ `%Threat Defense-4-770001: Resource resource allocation is more than the permitted list of limit for this platform. If this condition persists, the ASA will be rebooted.`

説明 Secure Firewall Threat Defense 仮想マシンの CPU またはメモリ リソース割り当てが、このプラットフォームに許可されている制限を超えました。この条件は、Secure Firewall Threat Defense仮想マシンの設定が、Cisco.comからダウンロードしたソフトウェアでの指定から変更されていない場合には発生しません。

推奨アクション Secure Firewall Threat Defense のオペレーションを続行するには、CPU または仮想マシンのメモリ リソース割り当てをCisco.comからダウンロードしたソフトウェアで指定したものに変更するか、変更します。

770002

エラーメッセージ `%Threat Defense-1-770002: Resource resource allocation is more than the permitted limit for this platform. ASA will be rebooted.`

説明 Secure Firewall Threat Defense 仮想マシンの CPU またはメモリ リソース割り当てが、このプラットフォームに許可されている制限を超えました。この条件は、Secure Firewall Threat Defense仮想マシンの設定が、Cisco.comからダウンロードしたソフトウェアでの指定から変更されていない場合には発生しません。リソース割り当てを変更しない限り、Secure Firewall Threat Defense デバイス は再起動し続けます。

推奨アクション CPUまたは仮想マシンのメモリ リソース割り当てをCisco.comからダウンロードしたソフトウェアで指定したものに変更するか、変更します。

770003

エラーメッセージ `%Threat Defense-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform. If this condition persists, performance will be lower than normal.`

説明 Secure Firewall Threat Defense 仮想マシンへの CPU またはメモリ リソース割り当てがこのプラットフォームの最小要件を下回っています。この状態が解消されない場合は、パフォーマンスが通常より低くなります。

推奨アクション Secure Firewall Threat Defense の操作を続行するには、仮想マシンの CPU またはメモリリソース割り当てを、シスコからダウンロードしたソフトウェアで指定されたものに変更します。

772002

エラーメッセージ `%Threat Defense-3-772002: PASSWORD: console login warning, user username , cause: password expired`

説明ユーザーが有効期限の切れたパスワードを使用してシステム コンソールにログインしました。これはシステムのロックアウトを避けるために許可されています。

- *username*：ユーザーの名前

推奨アクション ユーザーはログイン パスワードを変更する必要があります。

772003

エラーメッセージ `%Threat Defense-2-772003: PASSWORD: session login failed, user username , IP ip , cause: password expired`

説明ユーザーが有効期限の切れたパスワードを使用してシステムにログインしようとしましたが、アクセスを拒否されました。

- *session*：セッション タイプ。SSH または Telnet
- *username*：ユーザーの名前
- *ip*：ユーザーの IP アドレス

推奨アクションユーザーにアクセス権限がある場合は、管理者がユーザーのパスワードを変更する必要があります。不正なアクセスが試みられると適切な応答がトリガーされます。たとえば、その IP アドレスからのトラフィックをブロックできます。

772004

エラーメッセージ `%Threat Defense-3-772004: PASSWORD: session login failed, user username , IP ip , cause: password expired`

説明ユーザーが有効期限の切れたパスワードを使用してシステムにログインしようとしましたが、アクセスを拒否されました。

- *session*：セッション タイプ。これは ASDM です。
- *username*：ユーザーの名前
- *ip*：ユーザーの IP アドレス

推奨アクションユーザーにアクセス権限がある場合は、管理者がユーザーのパスワードを変更する必要があります。不正なアクセスが試みられると適切な応答がトリガーされます。たとえば、その IP アドレスからのトラフィックをブロックできます。

772005

エラーメッセージ `%Threat Defense-6-772005: REAUTH: user username passed authentication`

説明ユーザーはパスワードの変更後に正常に認証されました。

- *username*：ユーザーの名前

推奨アクション 不要。

772006

エラーメッセージ `%Threat Defense-2-772006: REAUTH: user username failed authentication`

説明ユーザーがパスワードを変更しようとして誤ったパスワードを入力しました。その結果、パスワードは変更されていません。

- *username*：ユーザーの名前

推奨アクションユーザーは**change-password** コマンドを使用してパスワードの変更を再試行する必要があります。

774001

エラーメッセージ `%Threat Defense-2-774001: POST: unspecified error`

説明暗号化サービス プロバイダーが電源投入時自己診断テストに失敗しました。

推奨アクション Cisco TAC にお問い合わせください。

774002

エラーメッセージ `%Threat Defense-2-774002: POST: error err, func func , engine eng , algorithm alg , mode mode , dir dir , key len len`

説明暗号化サービス プロバイダーが電源投入時自己診断テストに失敗しました。

- *err*：失敗の原因
- *func*：関数
- *eng*：エンジン。NPX、Nlite、またはソフトウェア
- *alg*：アルゴリズム。RSA、DSA、DES、3DES、AES、RC4、MD5、SHA1、SHA256、SHA386、SHA512、HMAC-MD5、HMAC-SHA1、HMAC-SHA2、または AES-XCBC のいずれか
- *mode* ：モード。none、CBC、CTR、CFB、ECB、stateful-RC4、stateless-RC4 のいずれか
- *dir*：encryption または decryption のいずれか
- *len*：ビット単位のキーの長さ

推奨アクション Cisco TAC にお問い合わせください。

776251

エラーメッセージ `%Threat Defense-6-776251: CTS SGT-MAP: Binding binding IP - SGname (SGT ) from source name added to binding manager.`

説明指定された送信元からのバインディングがバインディングマネージャに追加されました。

- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *SGname* (*SGT*)：バインディング SGT の情報SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *source name*：関係する送信元の名前。

推奨アクション 不要。

776252

エラーメッセージ `%Threat Defense-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding binding IP - SGname (SGT ) from source name deleted from binding manager.`

説明 指定された送信元からのバインディングがバインディング マネージャから削除されました。

指定した送信元からのバインドが、バインディング マネージャに追加されました。

- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *SGname* (*SGT*)：バインディング SGT の情報SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *source name*：関係する送信元の名前。

推奨アクション 不要。

776253

エラーメッセージ `%Threat Defense-6-776253: CTS SGT-MAP: Binding binding IP - new SGname (SGT ) from new source name changed from old sgt: old SGname (SGT ) from old source old source name .`

説明 特定の IP から SGT へのバインディングがバインディング マネージャ内で変更されました。

- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *new SGname* (*SGT*)：新しいバインディング SGT 情報。SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *new source name*：新たに関係する送信元の名前
- *old SGname* (*SGT*)：古いバインディング SGT 情報。SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *old source name*：以前に関係していた送信元の名前

推奨アクション必要なし。

776254

エラーメッセージ `%Threat Defense-3-776254: CTS SGT-MAP: Binding manager unable to action binding binding IP - SGname (SGT ) from source name.`

説明 バインディング マネージャがバインディングを挿入、削除、または更新できません。

- *action*：バインディング マネージャの動作insert、delete、または update です。
- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *SGname* (*SGT*)：バインディング SGT の情報SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *source name*：関係する送信元の名前。

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。

776254

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。