Syslog メッセージ 701001 ～ 714011

この章は、次の項で構成されています。

メッセージ 701001 ～ 713109

この項では、701001 から 713109 までのメッセージについて説明します。

701001

エラーメッセージ `%FTD-7-701001: alloc_user() out of Tcp_user objects`

説明モジュールが新しい AAA を処理するのにユーザー認証のレートが高すぎる場合に表示される AAA メッセージ。

推奨アクション floodguard enable コマンドで Flood Defender をイネーブルにします。

701002

エラーメッセージ `%FTD-7-701002: alloc_user() out of Tcp_proxy objects`

説明モジュールが新しい AAA を処理するのにユーザー認証のレートが高すぎる場合に表示される AAA メッセージ。

推奨アクション floodguard enable コマンドで Flood Defender をイネーブルにします。

703001

エラーメッセージ `%Threat Defense-7-703001: H.225 message received from interface_name :IP_address /port to interface_name :IP_address /port is using an unsupported version number`

説明 Secure Firewall Threat Defense デバイス はサポートされていないバージョン番号の H .323 パケットを受信しました。Secure Firewall Threat Defense デバイスが、パケットのプロトコル バージョン フィールドをサポートされている最新バージョンに再符号化する場合があります。

推奨アクション Secure Firewall Threat Defense デバイス が VoIP ネットワークにおいてサポートしている H.323 のバージョンを使用します。

703002

エラーメッセージ `%Threat Defense-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name :IP_address to interface_name :IP_address /port`

説明指摘された H.225 メッセージを Secure Firewall Threat Defense デバイス が受信し、指摘された 2 つの H.323 エンドポイントに対して新規シグナリング接続オブジェクトを Secure Firewall Threat Defense デバイス がオープンしました。

推奨アクション 不要。

703008

エラーメッセージ `%Threat Defense-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d`

説明このメッセージは、外部のエンドポイントが内部ホストへの着信コールを要求したことを示し、内部ホストがゲートキーパーに対して SETUP メッセージの前に FACILITY メッセージを送信し、H.460.18 に従うことを望んでいます。

推奨アクション H.640.18 で説明されているように、H323 の着信コールの場合は、セットアップで SETUP メッセージの前に早期の FACILITY メッセージを許可するようになっていることを確認します。

709001、709002

エラーメッセージ `%Threat Defense-7-709001: FO replication failed: cmd=command returned=code`

エラーメッセージ `%Threat Defense-7-709002: FO unreplicable: cmd=command`

説明開発のデバッグおよびテスト段階だけで表示されるフェールオーバー メッセージ。

推奨アクション 不要。

709003

エラーメッセージ `%Threat Defense-1-709003: (Primary) Beginning configuration replication: Sending to mate.`

説明アクティブ装置が自分のコンフィギュレーションのスタンバイ装置への複製を開始すると表示されるフェールオーバー メッセージ。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

709004

エラーメッセージ `%Threat Defense-1-709004: (Primary) End Configuration Replication (ACT)`

説明 アクティブ装置が自分のコンフィギュレーションのスタンバイ装置上への複製を完了すると表示されるフェールオーバー メッセージ。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

709005

エラーメッセージ `%Threat Defense-1-709005: (Primary) Beginning configuration replication: Receiving from mate.`

説明 スタンバイ Secure Firewall Threat Defense デバイス がアクティブ Secure Firewall Threat Defense デバイス からコンフィギュレーション複製の最初の部分を受け取りました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

709006

エラーメッセージ `%Threat Defense-1-709006: (Primary) End Configuration Replication (STB)`

説明 スタンバイ装置がアクティブ装置から送信されたコンフィギュレーションの複製を完了したときに表示されるフェールオーバー メッセージ。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

709007

エラーメッセージ `%Threat Defense-2-709007: Configuration replication failed for command`

説明 スタンバイ装置がアクティブ装置から送信されたコンフィギュレーションの複製を完了できない場合に表示されるフェールオーバー メッセージ。障害を発生させたコマンドが、メッセージの末尾に表示されます。

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

709008

エラーメッセージ `%Threat Defense-4-709008: (Primary | Secondary) Configuration sync in progress. Command: 'command ' executed from (terminal/http) will not be replicated to or executed by the standby unit.`

説明設定の同期中にコマンドが発行され、このコマンドがスタンバイ装置で発行されないことを示すインタラクティブプロンプトが表示されました。続行するには、コマンドはアクティブ装置にのみに発行され、スタンバイ装置では複製されない点に注意してください。

- Primary | Secondary：デバイスはプライマリとセカンダリのいずれか
- *command*：設定の同期が進行中に発行されたコマンド
- terminal/http：端末または HTTP 経由の発行元

推奨アクション なし。

709009

エラーメッセージ `%Threat Defense-6-709009: (unit-role) Configuration on Active and Standby is matching. No config sync. Time elapsed time-elapsed ms`

説明 このメッセージは、アクティブユニットと参加ユニットの両方で計算されたハッシュが一致した場合に生成されます。また、ハッシュ要求を送信してからハッシュ応答を取得して比較するまでの経過時間も表示されます。

推奨アクションなし。

709010

エラーメッセージ `%Threat Defense-6-709010: Configuration between units doesn't match. Going for config sync. Time elapsed time-elapsed ms.`

説明 この syslog メッセージは、アクティブユニットと参加ユニットの両方で計算されたハッシュが一致しない場合に生成されます。また、ハッシュ要求を送信してからハッシュ応答を取得して比較するまでの経過時間も表示されます。

推奨アクションなし。

709011

エラーメッセージ `%Threat Defense-6-709011: Total time to sync the config time ms.`

説明 このメッセージには、ハッシュが一致しない場合に構成の同期にかかった時間が表示されます。そのため、構成の完全同期プロセスに使用されます。

推奨アクションなし。

709012

エラーメッセージ `%Threat Defense-6-709012: Skip configuration replication from mate as configuration on Active and Standby is matching.`

説明 このメッセージは、アクティブユニットと参加ユニット間の構成が一致するため、構成の複製がスキップされたときに生成されます。

推奨アクションなし。

709013

エラーメッセージ `%Threat Defense-4-709013: Failover configuration replication hash comparison timeout expired.`

説明 この syslog メッセージは、ハッシュの計算、転送、および比較がタイムアウトしたときに生成されます。タイムアウトにより、構成の完全同期操作がトリガーされます。タイムアウト値は 60 秒で、この値を変更することはできません。

推奨アクションなし。

710001

エラーメッセージ `%Threat Defense-7-710001: TCP access requested from source_address /source_port to interface_name :dest_address /service`

説明 Secure Firewall Threat Defense デバイス 宛ての最初の TCP パケットで TCP セッションの確立を要求しています。このパケットは、3 ウェイ ハンドシェイクの最初の SYN パケットです。このメッセージは、それぞれ（Telnet、HTTP、または SSH）でパケットが許可されている場合に表示されます。しかし、SYN クッキー検証はまだ完了しておらず、状態は予約されていません。

推奨アクション 不要。

710002

エラーメッセージ `%Threat Defense-7-710002: {TCP|UDP} access permitted from source_address /source_port to interface_name :dest_address /service`

説明 TCP 接続の場合、Secure Firewall Threat Defense デバイス 宛ての 2 番目の TCP パケットで TCP セッションの確立を要求しました。このパケットは、3 ウェイ ハンドシェイクの最終 ACK です。それぞれ（Telnet、HTTP、または SSH）でパケットが許可されました。また、SYN クッキー検証が成功し、状態が TCP セッション用に予約されます。

UDP 接続の場合、接続は許可されています。たとえば、認可された SNMP 管理ステーションからの SNMP 要求をモジュールが受信し、その要求が処理されました。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

推奨アクション 不要。

710003

エラーメッセージ `%Threat Defense-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to interface_name :dest_IP/service`

説明インターフェイス サービスへの接続の試みが Secure Firewall Threat Defense デバイスによって拒否されました。たとえば、認可されていない SNMP 管理ステーションからの SNMP 要求

を Secure Firewall Threat Defense デバイス が受信しました。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。

次に例を示します。

```
%Threat Defense-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to
outside:95.1.1.13/1005
```

推奨アクション show run http コマンド、**show run ssh** コマンド、または **show run telnet** コマンドを使用して、ホストまたはネットワークからのサービスアクセスを許可するように Secure Firewall Threat Defense デバイス が設定されていることを確認します。

710004

エラーメッセージ `%Threat Defense-7-710004: TCP connection limit exceeded from Src_ip /Src_port to In_name :Dest_ip /Dest_port (current connections/connection limit = Curr_conn/Conn_lmt)`

説明サービス用の Secure Firewall Threat Defense 管理接続の最大数を超えました。Secure Firewall Threat Defense デバイスは、管理サービスあたり最大 5 つの同時管理接続を許可します。または、to-the-box 接続カウンタでエラーが発生している可能性があります。

- *Src_ip*：パケットの送信元 IP アドレス
- *Src_port*：パケットの送信元ポート
- *In_ifc*：入力インターフェイス
- *Dest_ip*：パケットの宛先 IP アドレス
- *Dest_port*：パケットの宛先ポート
- *Curr_conn*：現在の to-the-box 管理接続数
- *Conn_lmt*：接続制限

推奨アクション コンソールから、**kill** コマンドを使用して不要なセッションを解放します。to-the-box カウンタのエラーが原因でメッセージが生成された場合は、**show conn all** コマンドを実行して接続の詳細を表示します。

710005

エラーメッセージ `%Threat Defense-7-710005: {TCP|UDP|SCTP} request discarded from source_address /source_port to interface_name :dest_address /service`

説明 UDP 要求を処理する UDP サーバーが Secure Firewall Threat Defense デバイス にありません。また、Secure Firewall Threat Defense デバイス 上のどのセッションにも属していない TCP パケットが破棄された可能性もあります。さらにこのメッセージは、認可されたホストからの場合でも、ペイロードが空の SNMP 要求を Secure Firewall Threat Defense デバイス が受信した場合に表示されます（SNMP サービスで）。サービスが SNMP の場合、このメッセージは最大でも 10 秒ごとに 1 回の発生として、ログ受信プログラムが過負荷にならないようにします。このメッセージは SCTP パケットにも適用されます。

推奨アクション DHCP、RIP、NetBIOS などのブロードキャスト サービスの利用が多いネットワークでは、このメッセージの頻度が高くなることがあります。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。

710006

エラーメッセージ `%Threat Defense-7-710006: protocol request discarded from source_address to interface_name :dest_address`

説明 IP プロトコル要求を処理する IP サーバーが Secure Firewall Threat Defense デバイス にありません。たとえば、Secure Firewall Threat Defense デバイス が TCP または UDP でない IP パケットを受信し、Secure Firewall Threat Defense デバイス が要求を処理できません。

推奨アクション DHCP、RIP、NetBIOS などのブロードキャスト サービスの利用が多いネットワークでは、このメッセージの頻度が高くなることがあります。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。

710007

エラーメッセージ `%Threat Defense-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500`

説明 Secure Firewall Threat Defense デバイス は NAT-T キープ アライブ メッセージを受信しました。

推奨アクション 不要。

711001

エラーメッセージ `%Threat Defense-7-711001: debug_trace_msg`

説明ロギング機能のために **logging debug-trace** コマンドを入力しました。**logging debug-trace** コマンドがイネーブルの場合、すべてのデバッグ メッセージはメッセージにリダイレクトされて処理されます。セキュリティ上の理由から、メッセージ出力は暗号化するか、またはセキュア アウトオブバンド ネットワークで送信する必要があります。

推奨アクション 不要。

711002

エラーメッセージ `%Threat Defense-4-711002: Task ran for elapsed_time msecs, process = process_name , PC = PC Tracebeback = traceback`

説明プロセスの CPU 使用が 100 ミリ秒を超えました。このメッセージは CPU のデバッグに使用され、各攻撃プロセスに対して 5 秒に 1 回表示できます。

- **PC**：CPU 負荷の高いプロセスの命令ポインタ
- **traceback**：CPU 負荷の高いプロセスのスタック トレース（最大 12 個のアドレスを含むことができます）

推奨アクション 不要。

711003

エラーメッセージ `%Threat Defense-7-711003: Unknown/Invalid interface identifier(vpifnum) detected.`

説明正常動作中に発生してはならない内部不整合が発生しました。ただし、このメッセージがまれにしか発生しない場合は害がありません。頻繁に表示される場合は、デバッグする意味があると考えられます。

- *vpifnum*：インターフェイスに対応する 32 ビット値

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

711004

エラーメッセージ `%Threat Defense-4-711004: Task ran for msec msec, Process = process_name, PC = pc , Call stack = call stack`

説明プロセスの CPU 使用が 100 ミリ秒を超えました。このメッセージは CPU のデバッグに使用され、各攻撃プロセスに対して 5 秒に 1 回表示できます。

- **msec**：検出された CPU 占有時間の長さ（ミリ秒単位）
- *process_name*：占有しているプロセスの名前
- **pc**：CPU 負荷の高いプロセスの命令ポインタ
- **call stack**：CPU 負荷の高いプロセスのスタック トレース（最大 12 個のアドレスを含むことができます）

推奨アクション 不要。

711005

エラーメッセージ `%Threat Defense-5-711005: Traceback: call_stack`

説明発生してはならない内部ソフトウェアエラーが発生しました。デバイスは、通常、このエラーから回復でき、デバイスへの悪影響は生じません。

- *call_stack*：コール スタックの EIP

推奨アクション Cisco TAC にお問い合わせください。

711006

エラーメッセージ `%Threat Defense-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string .`

説明 CPU プロファイリングが開始されました。

- *n-samples*：CPU プロファイリング サンプルの指定数

• *reason-string*：次のうちどれかです。

“CPU utilization passed *cpu-utilization* %”（CPU 使用率が cpu-utilization % を超えました）

“Process process-name CPU utilization passed *cpu-utilization* %”（"process-name プロセスの CPU 使用率が cpu-utilization % を超えました"）

推奨アクション 「指定なし」

推奨アクション CPU プロファイリング結果を収集し、それらを Cisco TAC に提供します。

713004

エラーメッセージ `%Threat Defense-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface num , for Peer IP_address ignored`

説明 Secure Firewall Threat Defense デバイス が、トンネルを開始しようとしているリモート エンティティから IKE パケットを受信しました。Secure Firewall Threat Defense デバイスはリブートまたはシャットダウンがスケジュールされているので、これ以上トンネルを確立できません。この IKE パケットは無視されて、廃棄されます。

推奨アクション 不要。

713201

エラーメッセージ `%Threat Defense-5-713201: Duplicate Phase Phase  packet detected. 操作`

説明 Secure Firewall Threat Defense デバイス は、前のフェーズ 1 またはフェーズ 2 パケットの複製を受信し、最後のメッセージを送信します。ネットワーク パフォーマンスまたは接続の問題が発生し、ピアが送信されたパケットを迅速に受信していないた可能性があります。

• **Phase**：Phase 1 または Phase 2
• **Action**：Retransmitting last packet または No last packet to transmit

推奨アクション ネットワークのパフォーマンス、または接続を確認します。

713202

エラーメッセージ `%Threat Defense-6-713202: Duplicate IP_addr packet detected.`

説明 Secure Firewall Threat Defense デバイス は、Secure Firewall Threat Defense デバイス がすでに認識しネゴシエートしているトンネルの重複する最初のパケットを受信しました。これは、多くの場合、Secure Firewall Threat Defense デバイス がピアからパケットの再送信を受信したことを示します。

• **IP_addr**：重複する最初のパケットの送信元ピアの IP アドレス

推奨アクション 接続に失敗していない限り処置は不要です。接続に失敗する場合は、さらにデバッグして問題を診断します。

713006

エラーメッセージ `%Threat Defense-5-713006: Failed to obtain state for message Id` *`message_number`* `, Peer Address:` *`IP_address`*

説明 Secure Firewall Threat Defense デバイス が受信したメッセージ ID が未知の ID です。メッセージ ID は、特定の IKE フェーズ 2 ネゴシエーションの識別に使用されます。Secure Firewall Threat Defense デバイス でエラー状態が発生し、2 つの IKE ピアの同期がとれていないことを示す場合があります。

推奨アクション 不要。

713008

エラーメッセージ `%Threat Defense-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel`

説明 ID ペイロードでキー ID 値を受信したが、その値が事前共有キー認証を使用する IKE セッションのグループ名の最大許容サイズよりも長かったことを示します。これは無効な値で、セッションは拒否されます。指摘されたキー ID は、そのサイズのグループ名をSecure Firewall Threat Defense デバイスで作成できないので、機能することはありません。

推奨アクション クライアント ピア（おそらくは Altiga リモート アクセス クライアント）が有効なグループ名を指定していることを確認します。クライアント上の誤ったグループ名を変更するようにユーザーに通知します。グループ名の現在の最大長は 32 文字です。

713009

エラーメッセージ `%Threat Defense-3-713009: OU in DN in ID payload too big for Certs IKE tunnel`

説明 ID ペイロードで DN の OU 値を受信したが、その値が証明書認証を使用する IKE セッションのグループ名の最大許容サイズよりも長かったことを示します。この OU はスキップされますが、別の OU または他の基準を使用して一致するグループを検出できます。

推奨アクション クライアントが OU を使用して Secure Firewall Threat Defense デバイス からグループを検出するには、グループ名が有効な長さでなければなりません。グループ名の現在の最大長は 32 文字です。

713010

エラーメッセージ `%Threat Defense-5-713010: IKE area: failed to find centry for message Id` *`message_number`*

一意のメッセージ ID で conn_entry（IPSec SA に対応する IKE フェーズ 2 構造）を特定しようとして失敗しました。内部構造が見つかりませんでした。セッションが標準外の方法で終了した場合に発生しますが、より可能性が高いのは、内部エラーが発生したことです。

この問題が解決しない場合は、ピアを調査します。

713012

エラーメッセージ `%Threat Defense-3-713012: Unknown protocol (protocol ). Not adding SA w/spi=SPI value`

説明 不正またはサポートされていない IPSec プロトコルをピアから受信しました。

推奨アクション ピアの ISAKMP フェーズ 2 設定をチェックして、Secure Firewall Threat Defense デバイス と互換性があることを確認します。

713014

エラーメッセージ `%Threat Defense-3-713014: Unknown Domain of Interpretation (DOI): DOI value`

説明ピアから受信した ISAKMP DOI がサポートされていません。

推奨アクション ピアの ISAKMP DOI コンフィギュレーションを確認します。

713016

エラーメッセージ `%Threat Defense-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type`

説明ピアから受信した未知の ID です。ID が、よく知られていない有効な ID である場合、または無効または破損した ID である場合があります。

推奨アクション ヘッドエンドとピアのコンフィギュレーションを確認します。

713017

エラーメッセージ `%Threat Defense-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type`

説明ピアから受信したフェーズ 1 またはフェーズ 2 の ID が正当であるが、サポートされていません。

推奨アクション ヘッドエンドとピアのコンフィギュレーションを確認します。

713018

エラーメッセージ `%Threat Defense-3-713018: Unknown ID type during find of group name for certs, Type ID_Type`

説明内部ソフトウェア エラーが発生しました。

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

713020

エラーメッセージ %Threat Defense-3-713020: No Group found by matching OU(s) from ID payload: *OU_value*

説明内部ソフトウェア エラーが発生しました。

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

713022

エラーメッセージ %Threat Defense-3-713022: No Group found matching *peer_ID* or *IP_address* for Pre-shared key peer *IP_address*

説明グループ データベースに、ピアで指摘された値（キー ID または IP アドレス）と同じ名前のグループがあります。

推奨アクション ピアのコンフィギュレーションを確認します。

713024

エラーメッセージ %Threat Defense-7-713024: Group *group* IP *ip* Received local Proxy Host data in ID Payload: Address *IP_address* , Protocol *protocol* , Port *port*

説明 Secure Firewall Threat Defense デバイス がリモート ピアからフェーズ 2 のローカル プロキシ ID ペイロードを受信しました。

推奨アクション 不要。

713025

エラーメッセージ %Threat Defense-7-713025: Received remote Proxy Host data in ID Payload: Address *IP_address* , Protocol *protocol* , Port *port*

説明 Secure Firewall Threat Defense デバイス がリモート ピアからフェーズ 2 のローカル プロキシ ID ペイロードを受信しました。

推奨アクション 不要。

713028

エラーメッセージ %Threat Defense-7-713028: Received local Proxy Range data in ID Payload: Addresses *IP_address* - *IP_address* , Protocol *protocol* , Port *port*

説明 Secure Firewall Threat Defense デバイス がリモート ピアのフェーズ 2 のローカル プロキシ ID ペイロードを受信して、その中に IP アドレス範囲が含まれています。

推奨アクション 不要。

713029

エラーメッセージ `%Threat Defense-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address , Protocol protocol , Port port`

説明 Secure Firewall Threat Defense デバイス がリモート ピアのフェーズ 2 のローカル プロキシ ID ペイロードを受信して、その中に IP アドレス範囲が含まれています。

推奨アクション 不要。

713032

エラーメッセージ `%Threat Defense-3-713032: Received invalid local Proxy Range IP_address - IP_address`

説明ローカル ID ペイロードに範囲 ID タイプが含まれ、指摘された低アドレスが高アドレス以上でした。設定に問題がある可能性があります。

推奨アクション ISAKMP フェーズ 2 のパラメータのコンフィギュレーションを確認します。

713033

エラーメッセージ `%Threat Defense-3-713033`: Received invalid remote Proxy Range *IP_address - IP_address*

説明リモート ID ペイロードに範囲 ID タイプが含まれ、指摘された低アドレスが高アドレス以上でした。設定に問題がある可能性があります。

推奨アクション ISAKMP フェーズ 2 のパラメータのコンフィギュレーションを確認します。

713034

エラーメッセージ `%Threat Defense-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask netmask , Protocol protocol , Port port`

説明ローカル IP プロキシ サブネット データがフェーズ 2 の ID ペイロードで受信されました。

推奨アクション 不要。

713035

エラーメッセージ `%Threat Defense-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP_address , Mask netmask , Protocol protocol , Port port`

説明リモート IP プロキシ サブネット データがフェーズ 2 の ID ペイロードで受信されました。

推奨アクション 不要。

713039

エラーメッセージ %Threat Defense-7-713039: Send failure: Bytes (*number*), Peer: *IP_address*

説明内部ソフトウェア エラーが発生し、ISAKMP パケットを転送できません。

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

713040

エラーメッセージ %Threat Defense-7-713040: Could not find connection entry and can not encrypt: msgid *message_number*

説明内部ソフトウェア エラーが発生し、フェーズ 2 データ構造を検出できません。

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

713041

エラーメッセージ %Threat Defense-5-713041: IKE Initiator: *new* or *rekey* Phase 1 or 2, Intf *interface_number* , IKE Peer *IP_address* local Proxy Address *IP_address* , remote Proxy Address *IP_address* , Crypto map (*crypto map tag*)

説明 Secure Firewall Threat Defense デバイス が発信側としてトンネルをネゴシエーション中です。

推奨アクション 不要。

713042

エラーメッセージ %Threat Defense-3-713042: IKE Initiator unable to find policy: Intf *interface_number* , Src: *source_address* , Dst: *dest_address*

説明 IPSec ファースト パスで、IKE を起動したパケットを処理したが、IKE のポリシー ルックアップが失敗しました。このエラーは、タイミングに関連している場合があります。IKEが開始要求を処理する前に、IKE を起動した ACL が削除されていた可能性があります。この問題は、多くの場合、自分自身で訂正されます。

推奨アクション 同じ状態が続く場合、クリプト マップに関連付けられている ACL のタイプに特に注意しながら、L2L コンフィギュレーションを確認します。

713043

エラーメッセージ %Threat Defense-3-713043: Cookie/peer address *IP_address* session already in progress

説明元のトンネルが進行中に、IKE が再度起動されました。

推奨アクション 不要。

713048

エラーメッセージ `%Threat Defense-3-713048: Error processing payload: Payload ID: id`

説明処理できなかったペイロードでパケットが受信されました。

推奨アクションこの問題が解決しない場合は、ピアのコンフィギュレーションに誤りがある可能性があります。

713049

エラーメッセージ `%Threat Defense-5-713049: Security negotiation complete for tunnel_type type (group_name ) Initiator /Responder , Inbound SPI = SPI , Outbound SPI = SPI`

説明 IPSec トンネルが開始されました。

推奨アクション 不要。

713050

エラーメッセージ `%Threat Defense-5-713050: Connection terminated for peer IP_address . Reason: termination reason Remote Proxy IP_address , Local Proxy IP_address`

説明 IPSec トンネルが終了しました。考えられる終了理由を次に示します。

- IPSec SA のアイドル タイムアウト
- IPSec SA の最大時間を超過した
- 管理者がリセットした
- 管理者がリブートした
- 管理者がシャットダウンした
- セッションが切断された
- セッション エラーで終了した
- ピアが終了した

推奨アクション 不要。

713052

エラーメッセージ `%Threat Defense-7-713052: User (user ) authenticated.`

説明リモート アクセス ユーザーが認証されました。

推奨アクション 不要。

713056

エラーメッセージ `%Threat Defense-3-713056: Tunnel rejected: SA (SA_name ) not found for group (group_name )!`

説明 IPSec SA が見つかりませんでした。

推奨アクション これがリモート アクセス トンネルの場合、グループとユーザー コンフィギュレーションをチェックして、特定のユーザー グループに対してトンネル グループとグループ ポリシーが設定されていることを確認します。外部で認証されたユーザーおよびグループの場合は、返された認証属性を確認します。

713060

エラーメッセージ `%Threat Defense-3-713060: Tunnel Rejected: User (user ) not member of group (group_name ), group-lock check failed.`

説明ユーザーが、IPSec ネゴシエーションで送信されたグループとは別のグループに設定されています。

推奨アクションCisco VPN クライアントと事前共有キーを使用している場合、クライアントに設定されているグループが、Secure Firewall Threat Defense デバイス 上のユーザーに関連付けられているグループと同じであることを確認します。デジタル証明書を使用している場合、グループは、証明書のOUフィールドで指定されているか、またはユーザーはリモートアクセスのデフォルト グループにデフォルトで自動的に設定されています。

713061

エラーメッセージ `%Threat Defense-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address , Dst: dest_address !`

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。

推奨アクション 両側の暗号ACL内の保護されたネットワーク コンフィギュレーションをチェックして、発信側のローカル ネットが応答側のリモート ネットであること（およびその逆）を確認します。ワイルドカード マスクと、ホスト アドレス対ネットワーク アドレスに特に注意します。シスコ以外の実装では、プライベート アドレスがプロキシ アドレスまたは赤い色のネットワークとしてラベル付けされている場合があります。

713062

エラーメッセージ `%Threat Defense-3-713062: IKE Peer address same as our interface address IP_address`

説明 IKE ピアとして設定されている IP アドレスが、Secure Firewall Threat Defense IP インターフェイスのいずれかで設定されている IP アドレスと同じです。

推奨アクション L2L コンフィギュレーションと IP インターフェイス コンフィギュレーションを確認します。

713063

エラーメッセージ `%Threat Defense-3-713063: IKE Peer address not configured for destination IP_address`

説明 IKE ピア アドレスが L2L トンネルに対して設定されていません。

推奨アクション L2L 設定を確認します。

713065

エラーメッセージ `%Threat Defense-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute`

説明内部ソフトウェア エラーが発生しました。

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

713066

エラーメッセージ `%Threat Defense-7-713066: IKE Remote Peer configured for SA: SA_name`

説明ピアの暗号ポリシーが設定されています。

推奨アクション 不要。

713068

エラーメッセージ `%Threat Defense-5-713068: Received non-routine Notify message: notify_type (notify_value)`

説明このイベントの原因となる通知メッセージが通知処理コードで明示的に処理されません。

推奨アクション実行するアクションを判別するには、特定の理由を調べます。通知メッセージの多くは、IKE ピア間のコンフィギュレーションの不一致を示します。

713072

エラーメッセージ `%Threat Defense-3-713072: Password for user (user ) too long, truncating to number characters`

説明ユーザーのパスワードが長すぎます。

推奨アクション 認証サーバーでパスワードの長さを訂正します。

713073

エラーメッセージ `%Threat Defense-5-713073: Responder forcing change of Phase 1 /Phase 2 rekeying duration from larger_value to smaller_value seconds`

説明キー再生成の時間は、IKEピアが指定する値よりも常に低い値に設定されます。発信側の値の方が低いことを示します。

推奨アクション 不要。

713074

エラーメッセージ `%Threat Defense-5-713074: Responder forcing change of IPsec rekeying duration from larger_value to smaller_value Kbs`

説明キー再生成の時間は、IKEピアが指定する値よりも常に低い値に設定されます。発信側の値の方が低いことを示します。

推奨アクション 不要。

713075

エラーメッセージ `%Threat Defense-5-713075: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value seconds`

説明キー再生成の時間は、IKEピアが指定する値よりも常に低い値に設定されます。応答側の値の方が低いことを示します。

推奨アクション 不要。

713076

エラーメッセージ `%Threat Defense-5-713076: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value Kbs`

説明キー再生成の時間は、IKEピアが指定する値よりも常に低い値に設定されます。応答側の値の方が低いことを示します。

推奨アクション 不要。

713078

エラーメッセージ `%Threat Defense-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size , used value`

説明 modecfg 属性の処理中に内部ソフトウェア エラーが発生したことを示します。

推奨アクション不要なトンネル グループ属性をディセーブルにするか、長すぎるテキスト メッセージを短くします。問題が解決しない場合、Cisco TAC にお問い合わせください。

713081

エラーメッセージ `%Threat Defense-3-713081: Unsupported certificate encoding type encoding_type`

説明ロードされた証明書のいずれかが読み取り不可か、またはサポートされていない符号化スキームである可能性があります。

推奨アクション デジタル証明書およびトラストポイントの設定を確認します。

713082

エラーメッセージ `%Threat Defense-3-713082: Failed to retrieve identity certificate`

説明このトンネルの ID 証明書が見つかりません。

推奨アクション デジタル証明書およびトラストポイントの設定を確認します。

713083

エラーメッセージ `%Threat Defense-3-713083: Invalid certificate handle`

説明このトンネルの ID 証明書が見つかりません。

推奨アクション デジタル証明書およびトラストポイントの設定を確認します。

713084

エラーメッセージ `%Threat Defense-3-713084: Received invalid phase 1 port value (`*port*`) in ID payload`

説明 IKE フェーズ 1 ID ペイロードで受信されたポート値が正しくありませんでした。受け入れ可能な値は 0 または 500 です（ISAKMP は IKE とも呼ばれます）。

推奨アクションネットワークの問題が破損したパケットの原因になることを回避するために、ピアが IKE 規格に準拠していることを確認します。

713085

エラーメッセージ `%Threat Defense-3-713085: Received invalid phase 1 protocol (`*protocol*`) in ID payload`

説明 IKE フェーズ 1 ID ペイロードで受信されたプロトコル値が正しくありませんでした。受け入れ可能な値は 0 または 17（UDP）です。

推奨アクションネットワークの問題が破損したパケットの原因になることを回避するために、ピアが IKE 規格に準拠していることを確認します。

713086

エラーメッセージ `%Threat Defense-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))`

説明証明書ペイロードが受信されたが、ID 証明書がないことが内部証明書ハンドルによって示されています。証明書ハンドルが通常の登録方法で獲得されませんでした。これが発生する

理由として考えられるのは、認証方式が RSA または DSS シグニチャを通じて行われていないことです。ただし、それぞれの側の設定が誤っていると、IKE SA ネゴシエーションは失敗します。

推奨アクション Secure Firewall Threat Defense デバイスとそのピアでトラストポイントと ISAKMP コンフィギュレーション設定を確認します。

713088

エラーメッセージ `%Threat Defense-3-713088: Set Cert filehandle failure: no IPsec SA in group group_name`

説明 デジタル証明書情報に基づいてトンネル グループを検出できなかったことを示しています。

推奨アクション ピアの証明書情報を処理するようトンネル グループが正しく設定されていることを確認します。

713092

エラーメッセージ `%Threat Defense-5-713092: Failure during phase 1 rekeying attempt due to collision`

説明 内部ソフトウェア エラーが発生しました。多くの場合、これは問題のないイベントです。

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

713094

エラーメッセージ `%Threat Defense-7-713094: Cert validation failure: handle invalid for Main /Aggressive Mode Initiator /Responder !`

説明 内部ソフトウェア エラーが発生しました。

推奨アクション 場合によっては、トラストポイントを再登録する必要があります。問題が解決しない場合、Cisco TAC にお問い合わせください。

713098

エラーメッセージ `%Threat Defense-3-713098: Aborting: No identity cert specified in IPsec SA (SA_name )!`

説明 証明書ベースの IKE セッションを確立しようとしたときに、暗号ポリシーで ID 証明書が指定されませんでした。

推奨アクション ピアに送信する ID 証明書またはトラストポイントを指定します。

713099

エラーメッセージ `%Threat Defense-7-713099: Tunnel Rejected: Received NONCE length number is out of range!`

説明内部ソフトウェア エラーが発生しました。

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

713102

エラーメッセージ `%Threat Defense-3-713102: Phase 1 ID Data length number too long - reject tunnel!`

説明 2 K 以上の ID データ フィールドを含む ID ペイロードを IKE が受信しました。

推奨アクション 不要。

713103

エラーメッセージ `%Threat Defense-7-713103: Invalid (NULL) secret key detected while computing hash`

説明内部ソフトウェア エラーが発生しました。

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

713104

エラーメッセージ `%Threat Defense-7-713104: Attempt to get Phase 1 ID data failed while hash computation`

説明内部ソフトウェア エラーが発生しました。

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

713105

エラーメッセージ `%Threat Defense-3-713105: Zero length data in ID payload received during phase 1 or 2 processing`

説明ピアが無効な ID データを組み込まずに ID ペイロードを送信しました。

推奨アクション ピアのコンフィギュレーションを確認します。

713107

エラーメッセージ `%Threat Defense-3-713107: IP_Address request attempt failed!`

説明内部ソフトウェア エラーが発生しました。

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

713109

エラーメッセージ `%Threat Defense-3-713109: Unable to process the received peer certificate`

説明 リモート ピアから受信した証明書を Secure Firewall Threat Defense デバイス が処理できませんでした。これは、証明書のデータが誤っている（たとえば、公開キーのサイズが 4096 ビットより大きい場合）か、証明書の中のデータを Secure Firewall Threat Defense デバイス が保存できない場合に発生することがあります。

推奨アクション リモート ピアで別の証明書を使用して接続の再確立を試行します。

メッセージ 713112 ～ 714011

この項では、713112 から 714011 までのメッセージについて説明します。

713112

エラーメッセージ `%Threat Defense-3-713112: Failed to process CONNECTED notify (SPI` *`SPI_value`* `)!`

説明 Secure Firewall Threat Defense デバイス が、CONNECTED 通知タイプを含む通知ペイロードを正常に処理できませんでした。これは、IKE フェーズ 2 構造が、それを見つけるための SPI を使用して検出できない場合、または受信した ISAKMP ヘッダーでコミット ビットが設定されていなかった場合に発生します。後者の事例では、IKE ピアが規格に従っていない可能性があることを示しています。

推奨アクション 問題が解決しない場合、ピアのコンフィギュレーションを調べるか、コミット ビット処理をディセーブルにします（または両方を行います）。

713113

エラーメッセージ `%Threat Defense-7-713113: Deleting IKE SA with associated IPsec connection entries. IKE peer:` *`IP_address`* `, SA address:` *`internal_SA_address`* `, tunnel count:` *`count`*

説明 IKE SA が 0 以外のトンネル カウントで削除されています。これは、IKE SA トンネル カウントで関連する接続エントリとの同期が失われたか、あるいは関連する接続エントリのクッキー フィールドで接続エントリが指す IKE SA のクッキー フィールドとの同期が失われたことを意味します。これが発生する場合、IKE SA およびそれに関連するデータ構造体は解放されないので、それを指すエントリは古いポインタを持つことがありません。

推奨アクション 不要。エラー リカバリは組み込まれています。

713114

エラーメッセージ %Threat Defense-7-713114: Connection entry (conn entry internal address) points to IKE SA (*SA_internal_address*) for peer *IP_address* , but cookies don't match

説明内部ソフトウェア エラーが発生しました。

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

713115

エラーメッセージ %Threat Defense-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec

説明 Secure Firewall Threat Defense デバイス が IPSec over UDP を使用しようとする試みがクライアントによって拒否されました。IPSec over UDP を使用すると、NAT デバイスを介して複数のクライアントがSecure Firewall Threat Defense デバイスへの同時トンネルを確立できます。クライアントが、この機能をサポートしていないか、またはこの機能を使用するよう設定されていないため、要求を拒否した可能性があります。

推奨アクション ヘッドエンドとピアのコンフィギュレーションを確認します。

713117

エラーメッセージ %Threat Defense-7-713117: Received Invalid SPI notify (SPI *SPI_Value*)!

説明 SPI 値によって識別された IPSec SA が、リモート ピアでアクティブではなくなりました。リモート ピアがリブートされたか、リセットされた可能性があります。

推奨アクション この問題は、ピアによって適切な SA が確立されていないことを DPD が認識すると、訂正されます。DPD がイネーブルになっていない場合は、影響を受けるトンネルを手動で再確立しなければならないことがあります。

713118

エラーメッセージ %Threat Defense-3-713118: Detected invalid Diffie-Helmann *group_descriptor group_number* , in IKE area

説明 group_descriptor フィールドにサポートされていない値が含まれていました。現在サポートされているのは、グループ 1、2、5、および 7 だけです。centry の場合は、**group_descriptor** フィールドが、完全転送秘密がディセーブルになっていることを示すため 0 に設定されていることもあります。

推奨アクション ピア Diffie-Hellman コンフィギュレーションを確認します。

713119

エラーメッセージ %Threat Defense-5-713119: Group *group* IP *ip* PHASE 1 COMPLETED

説明 IKE フェーズ 1 が正常終了しました。

推奨アクション 不要。

713120

エラーメッセージ `%Threat Defense-5-713120: PHASE 2 COMPLETED (msgid=msg_id )`

説明 IKE フェーズ 2 が正常終了しました。

推奨アクション 不要。

713121

エラーメッセージ `%Threat Defense-7-713121: Keep-alive type for this connection: keepalive_type`

説明このトンネルに対して使用されているキープアライブ メカニズムのタイプを示します。

推奨アクション 不要。

713122

エラーメッセージ `%Threat Defense-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type )`

説明キープアライブがこのデバイスに対してオンまたはオフに設定されているが、IKEピアがキープアライブをサポートしている、またはしていません。

推奨アクションこの設定が意図的である場合、処置は不要です。意図的でない場合は、両方のデバイスでキープアライブ コンフィギュレーションを変更します。

713123

エラーメッセージ `%Threat Defense-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type )`

説明予期された期間内にリモートIKEピアがキープアライブに応答しなかったため、IKEピアへの接続が終了しました。このメッセージには、使用されるキープアライブ メカニズムが含まれています。

推奨アクション 不要。

713124

エラーメッセージ `%Threat Defense-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #`

説明リモート IKE ピアが、予期されたシーケンス番号と異なるシーケンス番号とともに DPD を送信しました。パケットは廃棄されます。これは、ネットワークでのパケット損失の問題を示している場合があります。

推奨アクション 不要。

713127

エラーメッセージ `%Threat Defense-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list`

説明ピアが XAUTH を実行しようとしたが、Secure Firewall Threat Defense デバイス が XAUTH IKE プロポーザルを選択しなかった場合に表示されます。

推奨アクション IKE プロポーザル リストで IKE xauth プロポーザルの優先順位を確認します。

713128

エラーメッセージ `%Threat Defense-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing`

説明 VCPIP に接続しようとして、ロード バランシングで負荷のより少ないピアにリダイレクトされました。

推奨アクション 不要。

713129

エラーメッセージ `%Threat Defense-3-713129: Received unexpected Transaction Exchange payload type: payload_id`

説明 XAUTH または Mode Cfg 中に予期しないペイロードが受信されました。これは、2 つのピアが同期していないこと、XAUTH または Mode Cfg のバージョンが一致しないこと、リモート ピアが適切な RFC に準拠していないことを示している場合があります。

推奨アクション ピア間でコンフィギュレーションを確認します。

713130

エラーメッセージ `%Threat Defense-5-713130: Received unsupported transaction mode attribute: attribute id`

説明現在サポートされていない有効なトランザクション モード属性（XAUTH または Mode Cfg）に対する要求をデバイスが受信しました。通常、これは問題のない状態です。

推奨アクション 不要。

713131

エラーメッセージ `%Threat Defense-5-713131: Received unknown transaction mode attribute: attribute_id`

説明既知の属性の範囲外であるトランザクション モード属性（XAUTH または Mode Cfg）に対する要求を Secure Firewall Threat Defense デバイス が受信しました。属性は有効でも新しいバージョンのコンフィギュレーションモードでだけサポートされているか、ピアが不正な値または独占権のある値を送信している可能性があります。これは、接続の問題にはなりませんが、ピアの機能に影響する場合があります。

推奨アクション 不要。

713132

エラーメッセージ `%Threat Defense-3-713132: Cannot obtain an IP_address for remote peer`

説明これらのアドレスを提供する内部ユーティリティからのリモート アクセス クライアントの IP アドレスに対する要求が満たされません。

推奨アクション IP アドレス割り当て方法のコンフィギュレーションを確認します。

713133

エラーメッセージ `%Threat Defense-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id ) with phase 1 group(DH group DH group_number`

説明設定されたフェーズ 2 PFS グループが、フェーズ 1 に対してネゴシエートされた DH グループと異なっていました。

推奨アクション 不要。

713134

エラーメッセージ `%Threat Defense-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection`

説明設定された LAN-to-LAN プロポーザルが、LAN-to-LAN 接続に対して受け入れられたプロポーザルと異なります。どちらの側が発信側かに応じて、異なるプロポーザルが使用されます。

推奨アクション 不要。

713135

エラーメッセージ `%Threat Defense-5-713135: message received, redirecting tunnel to IP_address .`

説明リモートの Secure Firewall Threat Defense デバイス でのロード バランシングのためにトンネルがリダイレクトされています。REDIRECT_CONNECTION 通知パケットを受信しました。

推奨アクション 不要。

713136

エラーメッセージ `%Threat Defense-5-713136: IKE session establishment timed out [IKE_state_name ], aborting!`

説明リーパーによって Secure Firewall Threat Defense デバイス スタックが非アクティブな状態で検出されました。リーパーは、非アクティブのSecure Firewall Threat Defense デバイスを除去しようとします。

推奨アクション 不要。

713137

エラーメッセージ `%Threat Defense-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!`

説明内部ソフトウェア エラーが発生しました。

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

713138

エラーメッセージ `%Threat Defense-3-713138: Group group_name not found and BASE GROUP default preshared key not configured`

説明グループ データベース内にピアの IP アドレスと同じ名前を持つグループがありません。Main モードで、Secure Firewall Threat Defense デバイスがフォールバックし、デフォルト グループのいずれかで設定されたデフォルトの事前共有キーの使用を試みます。デフォルトの事前共有キーは設定されていません。

推奨アクション 事前共有キーのコンフィギュレーションを確認します。

713139

エラーメッセージ `%Threat Defense-5-713139: group_name not found, using BASE GROUP default preshared key`

説明グループ データベース内にピアの IP アドレスと同じ名前を持つトンネル グループがありません。Main モードで、Secure Firewall Threat Defense デバイスがフォールバックし、デフォルト グループで設定されたデフォルトの事前共有キーを使用します。

推奨アクション 不要。

713140

エラーメッセージ `%Threat Defense-3-713140: Split Tunneling Policy requires network list but none configured`

説明スプリット トンネリング ポリシーがトンネルのスプリットまたはローカル LAN アクセスの許可に設定されています。VPN クライアントが要求する情報を表すには、スプリット トンネリング ACL が定義されている必要があります。

推奨アクション ACL のコンフィギュレーションを確認します。

713141

エラーメッセージ `%Threat Defense-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id) , Product product(id) , Caps: capability_value . Expected -- Vendor: vendor(id) , Product: product(id) , Caps: capability_value`

説明 クライアントにインストールされた Secure Firewall Threat Defense デバイス が設定された必須の Secure Firewall Threat Defense デバイス と一致しません。このメッセージは、実際の値と予期された値をリストし、トンネルが終了したか、または許可されたかを示します。

推奨アクション クライアントに別の個人用の Secure Firewall Threat Defense デバイス をインストールするか、または Secure Firewall Threat Defense デバイス のコンフィギュレーションを変更しなければならないことがあります。

713142

エラーメッセージ `%Threat Defense-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id) , Product product(id) , Caps: capability_value`

説明 クライアントは ModeCfg を使用して使用中の Secure Firewall Threat Defense デバイス を報告しませんでしたが、報告が必要です。このイベントは、予期された値をリストし、トンネルが終了したか、または許可されたかを示します。製品文字列の後の数値は、許可されたすべての製品のビットマスクです。

推奨アクション クライアントに別の個人用の Secure Firewall Threat Defense デバイス をインストールするか、または Secure Firewall Threat Defense デバイス のコンフィギュレーションを変更しなければならないことがあります。

713143

エラーメッセージ `%Threat Defense-7-713143: Processing firewall record. Vendor: vendor(id) , Product: product(id) , Caps: capability_value , Version Number: version_number , Version String: version_text`

説明 クライアントにインストールされた Secure Firewall Threat Defense デバイス に関するデバッグ情報が表示されます。

推奨アクション 不要。

713144

エラーメッセージ `%Threat Defense-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction`

説明不良な Secure Firewall Threat Defense デバイス 情報をクライアントから受信しました。

推奨アクションクライアントおよびSecure Firewall Threat Defenseデバイスで個人用のコンフィギュレーションを確認します。

713145

エラーメッセージ `%Threat Defense-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: netmask`

説明ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートが追加されています。この設定によって、Secure Firewall Threat Defenseデバイスは、ヘッドエンドのプライベート側にあるすべてのルータにリモート ネットワークを知らせることができます。

推奨アクション 不要。

713146

エラーメッセージ `%Threat Defense-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: netmask`

説明内部ソフトウェア エラーが発生しました。ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートを追加する試みが失敗しました。ルーティング テーブルがいっぱいになっているか、アドレッシング エラーが発生した可能性があります。

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

713147

エラーメッセージ `%Threat Defense-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask: netmask`

説明ネットワーク拡張モードのハードウェア クライアントへのトンネルが除去され、ハードウェア クライアントの背後でプライベート ネットワーク用のスタティック ルートが削除されています。

推奨アクション 不要。

713148

エラーメッセージ `%Threat Defense-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: netmask`

説明ネットワーク拡張モードのハードウェア クライアントへのトンネルを除去しているときに、ハードウェア クライアントの背後にあるプライベート ネットワークへのルートを削除できません。これは、アドレッシングまたはソフトウェアの問題を意味する場合があります。

推奨アクションルーティング テーブルを調べて、ルートがそこにないことを確認します。ルートがある場合は、手動で削除する必要がありますが、ハードウェア クライアントへのトンネルが完全に削除された場合に限り行います。

713149

エラーメッセージ `%Threat Defense-3-713149: Hardware client security attribute attribute_name was enabled but not requested.`

説明ヘッドエンドの Secure Firewall Threat Defense デバイス で指摘されたハードウェア クライアント セキュリティ属性がイネーブルになっているが、VPN 3002 ハードウェア クライアントによって属性が要求されませんでした。

推奨アクション ハードウェア クライアントでコンフィギュレーションを確認します。

713152

エラーメッセージ `%Threat Defense-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.`

説明クライアントで CPP を使用してその Secure Firewall Threat Defense デバイス をプロビジョニングする必要があるが、ヘッドエンド デバイスがクライアントへ送信する ACL を取得できませんでした。原因として、設定の誤りが考えられます。

推奨アクション クライアントのグループ ポリシーで CPP に対して指定された ACL を確認します。

713154

エラーメッセージ `%Threat Defense-4-713154: DNS lookup for peer_description Server [server_name ] failed!`

説明このメッセージは、指摘されたサーバーに対する DNS ルックアップが解決されなかった場合に表示されます。

推奨アクション Secure Firewall Threat Defense デバイス 上の DNS サーバー コンフィギュレーションを確認します。また、DNS サーバーがオプションになっていることと、IP アドレス マッピングへのホスト名を持っていることを確認します。

713155

エラーメッセージ `%Threat Defense-5-713155: DNS lookup for Primary VPN Server [server_name ] successfully resolved after a previous failure. Resetting any Backup Server init.`

説明 プライマリ サーバーに対する以前の DNS ルックアップの失敗によって、Secure Firewall Threat Defense デバイス がバックアップ ピアを初期化した可能性があります。このメッセージは、プライマリ サーバーでの後の DNS ルックアップが最終的に成功し、バックアップ サーバーの初期化をリセットしていることを示しています。このポイントより後に初期化されたトンネルは、プライマリ サーバーに向けられます。

推奨アクション 不要。

713156

エラーメッセージ `%Threat Defense-5-713156: Initializing Backup Server [server_name or IP_address ]`

説明クライアントがバックアップ サーバーにフェールオーバーしているか、プライマリ サーバーに対する DNS ルックアップが失敗したことにより Secure Firewall Threat Defense デバイスがバックアップ サーバーを初期化しました。このポイントより後に初期化されたトンネルは、指摘されたバックアップ サーバーに向けられます。

推奨アクション 不要。

713157

エラーメッセージ `%Threat Defense-4-713157: Timed out on initial contact to server [server_name or IP_address ] Tunnel could not be established.`

説明クライアントが IKE MSG1 を送信してトンネルを初期化しようとしたが、相手側の Secure Firewall Threat Defense デバイス から応答を受信しませんでした。バックアップ サーバーを使用できる場合、クライアントはそれらのいずれかに接続しようとします。

推奨アクションヘッドエンドの Secure Firewall Threat Defense デバイス への接続を確認します。

713158

エラーメッセージ `%Threat Defense-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP`

説明クライアントが IPSec over TCP を使用するよう設定されています。Secure Firewall Threat Defense デバイスが IPSec over UDP を使用しようとする試みがクライアントによって拒否されました。

推奨アクション TCP を希望する場合、処置は不要です。それ以外の場合は、クライアント コンフィギュレーションを確認します。

713159

エラーメッセージ `%Threat Defense-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access`

説明 Secure Firewall Threat Defense サーバーへの TCP 接続が特定の原因により失われました。原因としては、サーバーがリブートした、ネットワークの問題が発生した、SSLのミスマッチが発生した、などがあります。

推奨アクション 初期接続が確立された後にサーバーの接続が失われた場合は、サーバーとネットワークの接続を確認する必要があります。初期接続がすぐに失われた場合、これはSSL認証の問題を意味することがあります。

713160

エラーメッセージ `%Threat Defense-7-713160: Remote user (session Id - id ) has been granted access by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーへのリモート ユーザーの通常の認証が実行されました。

推奨アクション 不要。

713161

エラーメッセージ `%Threat Defense-3-713161: Remote user (session Id - id ) network access has been restricted by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーは、ユーザーを制限する必要があることを示すメッセージを Secure Firewall Threat Defense デバイス に送信しました。これには、Secure Firewall Threat Defense ソフトウェアのアップグレードや許可の変更など、いくつかの理由があります。Secure Firewall Threat Defense サーバーは、処理が完了するとすぐに、ユーザーを完全アクセス モードに移行します。

推奨アクション ユーザーが完全アクセス モードに移行されない限り、処置は不要です。これが実行されない場合、実行中の処理の詳細およびリモート マシンで実行中のSecure Firewall Threat Defense ソフトウェアの状態については、Secure Firewall Threat Defense サーバーを参照します。

713162

エラーメッセージ `%Threat Defense-3-713162: Remote user (session Id - id ) has been rejected by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーは、このユーザーを拒否しました。

推奨アクション Secure Firewall Threat Defense サーバーにおけるポリシー情報で、ユーザーが正しく設定されていることを確認します。

713163

エラーメッセージ `%Threat Defense-3-713163: Remote user (session Id - id ) has been terminated by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーがこのユーザー セッションを終了しました。これは、整合性エージェントがクライアント マシンで動作を停止した場合や、セキュリティ ポリシーがリモート ユーザーによって何らかの方法で変更された場合に発生します。

推奨アクション Secure Firewall Threat Defense ソフトウェアがクライアント マシンで動作を続けていることと、ポリシーが正しいことを確認します。

713164

エラーメッセージ `%Threat Defense-7-713164: The Firewall Server has requested a list of active user sessions`

説明 Secure Firewall Threat Defense サーバーが、古いデータがあることを検出した場合や（リブートにより）セッション データを失った場合に、セッション情報を要求します。

推奨アクション 不要。

713165

エラーメッセージ `%Threat Defense-3-713165: Client IKE Auth mode differs from the group's configured Auth mode`

説明デジタル証明書を使用するよう設定されているポリシーをトンネル グループが指しているときに、クライアントが事前共有キーとネゴシエートしました。

推奨アクション クライアント設定を確認します。

713166

エラーメッセージ `%Threat Defense-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password`

説明ハードウェア クライアントが拡張認証に失敗しました。これはおそらく、ユーザー名とパスワードの問題または認証サーバーの問題です。

推奨アクション設定したユーザー名とパスワードの値が各側で一致することを確認します。また、ヘッドエンドの認証サーバーが動作していることを確認します。

713167

エラーメッセージ `%Threat Defense-3-713167: Remote peer has failed user authentication - check configured username and password`

説明リモート ユーザーが認証の拡張に失敗しました。これはおそらく、ユーザー名とパスワードの問題または認証サーバーの問題です。

推奨アクション設定したユーザー名とパスワードの値が各側で一致することを確認します。また、リモートユーザーの認証に使用している認証サーバーが動作していることも確認します。

713168

エラーメッセージ `%Threat Defense-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!`

説明キー再生成の再認証がイネーブルになっているが、トンネル認証で手動による介入が必要です。

推奨アクション手動による介入を希望する場合、処置は不要です。それ以外の場合は、対話型の認証コンフィギュレーションを確認します。

713169

エラーメッセージ `%Threat Defense-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address , SA address: internal_SA_address , tunnelCnt: tunnel_count`

説明キー再生成が完了した後に古い IKE SA を削除するために、IKE がリモート ピアから削除メッセージを受信しました。

推奨アクション 不要。

713170

エラーメッセージ `%Threat Defense-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP_address , centry address: internal_address , msgid: id`

説明 IKE は、フェーズ 2 キー再生成が完了した後に古い centry を削除するために、リモート ピアから削除メッセージを受信しました。

推奨アクション 不要。

713171

エラーメッセージ `%Threat Defense-7-713171: NAT-Traversal sending NAT-Original-Address payload`

説明 UDP-Encapsulated-Transport が、フェーズ 2 中に提案または選択されました。この場合、NAT-Traversal 用にこのペイロードを送信します。

推奨アクション 不要。

713172

エラーメッセージ `%Threat Defense-6-713172: Automatic NAT Detection Status: Remote end is |is not behind a NAT device This end is |is not behind a NAT device`

説明 NAT-Traversal が NAT を自動検出しました。

推奨アクション 不要。

713174

エラーメッセージ `%Threat Defense-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!`

説明 ハードウェア クライアントがネットワーク拡張モードを使用してトンネルを試行しましたが、ネットワーク拡張モードは許可されていません。

推奨アクション ネットワーク拡張モードと PAT モードのコンフィギュレーションを対比して確認します。

713176

エラーメッセージ `%Threat Defense-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number , for Peer IP_address ignored`

説明 Secure Firewall Threat Defense デバイス が、示されたピアへの IPSec トンネルをトリガーするためのデータを処理しています。メモリ リソースは重大な状態なので、トンネルをそれ以上開始していません。データ パケットは無視され、廃棄されました。

推奨アクション 状態が解決しない場合は、Secure Firewall Threat Defense デバイス が効率的に設定されていることを確認します。このアプリケーションでは、Secure Firewall Threat Defense デバイス のメモリを増やす必要がある可能性があります。

713177

エラーメッセージ `%Threat Defense-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address , Protocol protocol , Port port`

説明 FQDN を含むフェーズ 2 ID ペイロードがピアから受信されました。

推奨アクション 不要。

713178

エラーメッセージ `%Threat Defense-5-713178: IKE Initiator received a packet from its peer without a Responder cookie`

説明内部ソフトウェア エラーが発生しました。

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

713179

エラーメッセージ `%Threat Defense-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload`

説明内部ソフトウェア エラーが発生しました。

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

713182

エラーメッセージ `%Threat Defense-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!`

説明内部ソフトウェア エラーが発生しました。

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

713184

エラーメッセージ `%Threat Defense-6-713184: Client Type: Client_type Client Application Version: Application_version_string`

説明クライアントのオペレーティング システムとアプリケーションのバージョンが表示されます。情報を入手できない場合は、N/A が示されます。

推奨アクション 不要。

713185

エラーメッセージ `%Threat Defense-3-713185: Error: Username too long - connection aborted`

説明クライアントが無効な長さのユーザー名を戻し、トンネルが切断されました。

推奨アクション ユーザー名を確認し、必要に応じて変更します。

713186

エラーメッセージ `%Threat Defense-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text Character index (value ) is illegal`

説明無効なセカンダリ ドメイン名リストが外部 RADIUS 認証サーバーから受信されました。スプリット トンネルが使用されている場合、このリストは、クライアントがトンネルで解決すべきドメインを示します。

推奨アクション RADIUS サーバーで Secondary-Domain-Name-List 属性（ベンダー固有の属性 29）の指定を訂正します。リストは、カンマ区切りのドメイン名のリストとして指定する必要があります。ドメイン名には英数字、ハイフン、下線、ピリオドだけ含めることができます。

713187

エラーメッセージ `%Threat Defense-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP_address , Remote peer address: IP_address`

説明このトンネルを開始しようとしている IKE ピアは、受信されたリモート サブネットにバインドされた ISAKMP コンフィギュレーション内で設定された IKE ピアではありません。

推奨アクション ヘッドエンドとピアの L2L 設定が正しいことを確認します。

713189

エラーメッセージ `%Threat Defense-3-713189: Attempted to assign network or broadcast IP_address , removing ( IP_address ) from pool.`

説明プールからの IP アドレスは、このサブネットのネットワークまたはブロードキャスト アドレスです。このアドレスには、使用不可のマークが付けられます。

推奨アクション 通常、これは問題のないエラーですが、IP アドレス プール コンフィギュレーションを確認する必要があります。

713190

エラーメッセージ `%Threat Defense-7-713190: Got bad refCnt ( ref_count_value ) assigning IP_address ( IP_address )`

説明この SA のリファレンス カウンタは無効です。

推奨アクション 不要。

713191

エラーメッセージ `%Threat Defense-3-713191: Maximum concurrent IKE negotiations exceeded!`

説明 CPU に負荷のかかる暗号化計算を最小限にするため、Secure Firewall Threat Defense デバイスは処理中の接続ネゴシエーションの数を制限しています。新しいネゴシエーションが要求されたとき、Secure Firewall Threat Defense デバイス がすでに制限値に達している場合、新しいネゴシエーションは拒否されます。既存の接続ネゴシエーションが完了すると、新しい接続ネゴシエーションが再び許可されます。

推奨アクション crypto ikev1 limit max-in-negotiation-sa コマンドを参照してください。制限値を大きくすると、パフォーマンスが低下する可能性があります。

713193

エラーメッセージ `%Threat Defense-3-713193: Received packet with missing payload, Expected payload: payload_id`

説明 Secure Firewall Threat Defense デバイス が、1 つまたは複数の欠落ペイロードを持つ特定の交換タイプの暗号化または暗号解除されたパケットを受信しました。通常、これはピアに問題があることを意味します。

推奨アクション ピアが有効な IKE メッセージを送信していることを確認します。

713194

エラーメッセージ `%Threat Defense-3-713194: Sending IKE |IPsec Delete With Reason message: termination_reason`

説明終了原因コードを持つ削除メッセージが受信されました。

推奨アクション 不要。

713195

エラーメッセージ `%Threat Defense-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!`

説明 originate-only ピアが着信接続を受け入れることができるのは、最初の P2 トンネルを作成した後だけです。その時点で、どの方向からでもデータは追加のフェーズ2トンネルを開始できます。

推奨アクション別の動作を希望する場合は、originate-only コンフィギュレーションを見直す必要があります。

713196

エラーメッセージ `%Threat Defense-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!`

説明 リモート L2L ピアが Public-Public トンネルを開始しました。リモート L2L ピアは、もう一方のピアからの応答を期待しますが、その応答を受信しません。設定が誤っている可能性があります。

推奨アクション 両方の終端で L2L コンフィギュレーションを確認します。

713197

エラーメッセージ `%Threat Defense-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.`

説明 グループ内の設定済み Confidence Interval が有効な範囲外です。

推奨アクション グループ内の信頼度の設定が有効な範囲内であることを確認します。

713198

エラーメッセージ `%Threat Defense-3-713198: User Authorization failed: user User authorization failed. Username could not be found in the certificate`

説明証明書内にユーザー名が見つからないことを示す原因文字列が表示されます。

推奨アクション グループ コンフィギュレーションとクライアント認可を確認します。

713199

エラーメッセージ `%Threat Defense-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter ( counter_value )!`

説明リーパーによって内部ソフトウェア エラーが訂正されました。

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

713203

エラーメッセージ `%Threat Defense-3-713203: IKE Receiver: Error reading from socket.`

説明受信したIKEパケットの読み取り中にエラーが発生しました。通常、これは内部エラーであり、ソフトウェアの問題を示している可能性があります。

推奨アクション 通常、これは問題のない状態であり、システムによって自動的に訂正されます。問題が解決しない場合、Cisco TAC にお問い合わせください。

713204

エラーメッセージ `%Threat Defense-7-713204: Adding static route for client address: IP_address`

説明このメッセージは、ピアが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートがルーティング テーブルに追加されたことを示しています。

推奨アクション 不要。

713205

エラーメッセージ `%Threat Defense-3-713205: Could not add static route for client address: IP_address`

説明クライアントが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートを追加する試みが失敗しました。これは、ルーティング テーブルまたは破損したネットワーク アドレスでのルートの重複を意味している場合もあります。ルートの重複は、ルートが正しくクリーンアップされていないか、複数のクライアントがネットワークまたはアドレスを共有していることによって発生します。

推奨アクション IP ローカル プール コンフィギュレーション、およびその他の使用中の IP アドレス割り当てメカニズム（DHCP や RADIUS など）をチェックします。ルーティング テーブルからルートが消去されていることを確認します。また、ピアにおけるネットワークやアドレスのコンフィギュレーションも確認します。

713206

エラーメッセージ `%Threat Defense-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy`

説明 グループ ポリシーで指定された許可済みのトンネルが、トンネル グループの設定内の許可済みのトンネルと異なっていたために、トンネルが切断されました。

推奨アクション トンネル グループとグループ ポリシーの設定をチェックします。

713207

エラーメッセージ `%Threat Defense-4-713207: Terminating connection: IKE Initiator and tunnel group specifies L2TP Over IPSec`

説明 この Syslog は、GW が発信側でトンネルグループタイプが L2TP over IPSEC の場合に、接続を終了している ikev1 に対して表示されます。

推奨アクション 不要。

713208

エラーメッセージ `%Threat Defense-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id`

説明 IKE をトリガーして IPSec データを適切に処理する ACL の作成時に障害が発生しました。この障害はバックアップ L2L コンフィギュレーションに固有です。これは、コンフィギュレーション エラー、キャパシティ エラー、または内部ソフトウェア エラーを示していることがあります。

推奨アクション 最大数の接続および最大数の VPN トンネルを使用して Secure Firewall Threat Defense デバイス が実行されている場合は、メモリの問題の可能性があります。それ以外の場合、バックアップ L2L およびクリプト マップ コンフィギュレーション（特にクリプト マップと関連付けられている ACL）を確認します。

713209

エラーメッセージ `%Threat Defense-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id`

説明 IKE をトリガーして IPSec データを正しく処理する ACL の削除時に障害が発生しました。この障害はバックアップ L2L コンフィギュレーションに固有です。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

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

713210

エラーメッセージ `%Threat Defense-3-713210: Cannot create dynamic map for Backup L2L entry rule_id`

説明バックアップ L2L コンフィギュレーションに関連するダイナミック クリプト マップの実行時インストールの作成時に障害が発生しました。これは、コンフィギュレーションエラー、キャパシティ エラー、または内部ソフトウェア エラーを示していることがあります。

推奨アクション 最大数の接続および最大数の VPN トンネルを使用して Secure Firewall Threat Defense デバイス が実行されている場合は、メモリの問題の可能性があります。それ以外の場合、バックアップ L2L およびクリプト マップ コンフィギュレーション（特にクリプト マップと関連付けられている ACL）を確認します。

713212

エラーメッセージ `%Threat Defense-3-713212`: Could not add route for L2L peer coming in on a dynamic map. address: *IP_address* , mask: *netmask*

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しようとして失敗しました。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。これは、ルートの重複か、ルーティング テーブルがいっぱいになっているか、前に使用したルートを Secure Firewall Threat Defense デバイス が削除していないことを意味している場合があります。

ルーティングテーブルに追加ルートのためのスペースがあることと、古いルートが存在しないことを確認します。テーブルがいっぱいになっている場合や古いルートが含まれている場合は、ルートを削除して再試行します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713213

エラーメッセージ `%Threat Defense-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを削除しています。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

推奨アクション 不要。

713214

エラーメッセージ `%Threat Defense-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを削除しようとしたときに障害が発生しました。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。ルートがすでに削除されているか、内部ソフトウェア エラーが発生しました。

推奨アクション ルートがすでに削除されている場合は、問題のない状態であり、デバイスは正常に機能します。問題が解決しない場合、または VPN トンネルでルーティングの問題にリンクできる場合は、VPN L2L コンフィギュレーションのルーティング部分とアドレッシング部分を確認します。逆ルートの注入と、適切なクリプト マップに関連する ACL を確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713215

エラーメッセージ `%Threat Defense-6-713215: No match against Client Type and Version rules. Client: type version is /is not allowed by default`

説明 クライアントのタイプとクライアントのバージョンが Secure Firewall Threat Defense デバイス で設定された規則と一致しませんでした。デフォルトのアクションが表示されます。

推奨アクション デフォルトのアクションと配置要件を決定し、適切な変更を加えます。

713216

エラーメッセージ `%Threat Defense-5-713216: Rule: action [Client type]: version Client: type version allowed/not allowed`

説明 クライアントのタイプとクライアントのバージョンが規則の 1 つと一致しました。一致の結果と規則が表示されます。

推奨アクション 配置要件を決定し、適切な変更を加えます。

713217

エラーメッセージ `%Threat Defense-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version`

説明 形式が誤っているクライアント タイプとバージョン規則が存在します。必要な形式は、action client type | client version action ですclient type と client version の許可または拒否が、Session Management の下に表示されます。サポートされるワイルドカード（*）はパラメータごとに 1 つだけです。

推奨アクション 規則を修正します。

713218

エラーメッセージ `%Threat Defense-3-713218: Tunnel Rejected: Client Type or Version not allowed.`

設定された規則に従ってクライアントによるアクセスが拒否されました。

対処は不要です。

713219

エラーメッセージ `%Threat Defense-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.`

説明フェーズ 1 の完了後にフェーズ 2 のメッセージがキューイングされています。

推奨アクション 不要。

713220

エラーメッセージ `%Threat Defense-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.`

説明キューに入れられたフェーズ 2 メッセージが処理されています。

推奨アクション 不要。

713221

エラーメッセージ `%Threat Defense-7-713221: Static Crypto Map check, checking map = crypto_map_tag , seq = seq_number...`

説明 Secure Firewall Threat Defense デバイスがクリプトマップで繰り返しコンフィギュレーション情報を探しています。

推奨アクション 不要。

713222

エラーメッセージ `%Threat Defense-7-713222: Group group Username username IP ip Static Crypto Map check, map = crypto_map_tag , seq = seq_number , ACL does not match proxy IDs src:source_address dst:dest_address`

説明設定されたクリプトマップで反復しているときに、Secure Firewall Threat Defense デバイスが関連する ACL と一致できません。通常、これは ACL の設定が誤っていることを意味します。

推奨アクション このトンネルピアに関連する ACL を調べ、VPN トンネルの両端から適切なプライベート ネットワークが指定されていることを確認します。

713223

エラーメッセージ `%Threat Defense-7-713223: Static Crypto Map check, map = crypto_map_tag , seq = seq_number , no ACL configured`

説明このピアに関連するクリプト マップが ACL にリンクされていません。

推奨アクション このクリプト マップに関連する ACL があることと、ACL に VPN トンネルの両側の適切なプライベート アドレスまたはネットワークが含まれていることを確認します。

713224

エラーメッセージ `%Threat Defense-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!`

説明この VPN トンネルに関連するクリプト マップで重要な情報が欠落しています。

推奨アクション VPN ピア、トランスフォーム セット、関連する ACL すべてでクリプト マップが正しく設定されていることを確認します。

713225

エラーメッセージ `%Threat Defense-7-713225: [IKEv1], Static Crypto Map check, map` *`map_name`* `, seq =` *`sequence_number`* `is a successful match`

説明 Secure Firewall Threat Defense デバイス がこの VPN トンネルに対して一致する有効なクリプト マップを検出しました。

推奨アクション 不要。

713226

エラーメッセージ `%Threat Defense-3-713226: Connection failed with peer` *`IP_address`* `, no trust-point defined in tunnel-group` *`tunnel_group`*

説明デバイスがデジタル証明書を使用するように設定されている場合は、コンフィギュレーションでトラストポイントを指定する必要があります。トラストポイントがコンフィギュレーションから欠落している場合は、このメッセージが生成され、エラーのフラグが立てられます。

- **IP_address**：ピアの IP アドレス
- **tunnel_group**：コンフィギュレーションでトラストポイントが欠落しているトンネル グループ

推奨アクションデバイスの管理者は、コンフィギュレーションでトラストポイントを指定する必要があります。

713227

エラーメッセージ `%Threat Defense-3-713227: Rejecting new IPsec SA negotiation for peer` *`Peer_address`* `. A negotiation was already in progress for local Proxy` *`Local_address /Local_netmask`* `, remote Proxy` *`Remote_address /Remote_netmask`*

説明フェーズ SA を確立するとき、Secure Firewall Threat Defense デバイス はこのプロキシに一致する新しいフェーズ 2 を拒否します。

推奨アクション 不要。

713228

エラーメッセージ `%Threat Defense-6-713228: Group = group , Username = uname , IP = remote_IP_address Assigned private IP address assigned_private_IP to remote user`

説明 IKE が DHCP またはアドレス プールからクライアントのプライベート IP アドレスを取得しました。

- *group*：グループの名前
- *uname*：ユーザーの名前
- *remote_IP_address*：リモート クライアントの IP アドレス
- *assigned_private_IP*：DHCP によって、またはローカル アドレス プールから割り当てられるクライアント IP アドレス

推奨アクション 不要。

713229

エラーメッセージ `%Threat Defense-5-713229: Auto Update - Notification to client client_ip of update string: message_string .`

説明アップデートされたソフトウェアをダウンロードできることが VPN リモート アクセス クライアントに通知されました。リモート クライアントユーザーには、クライアント アクセス ソフトウェアのアップデートを選択する責任があります。

- **client_ip**：リモート クライアントの IP アドレス
- **message_string**：リモート クライアントに送信されたメッセージ テキスト

推奨アクション 不要。

713230

エラーメッセージ `%Threat Defense-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type type`

説明内部エラーが発生しました。これは、IKEサブシステムがすでにロックされているメモリをロックしようとしていることを報告しています。これは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを示します。このメッセージは、重大な誤りがないことを示しています。ただし、予期しないイベントが発生し、自動的に回復されました。

- >*type*：ロックの問題を持つセマフォのタイプを説明する文字列

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

713231

エラーメッセージ `%Threat Defense-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type type`

説明内部エラーが発生しました。IKEサブシステムが現在ロックされていないメモリをロック解除しようとしていることを報告しています。これは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを示します。このメッセージは、重大な誤りがないことを示しています。ただし、予期しないイベントが発生し、自動的に回復されました。

- *type*：ロックの問題を持つセマフォのタイプを説明する文字列

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

713232

エラーメッセージ `%Threat Defense-3-713232 SA lock refCnt = value , bitmask = hexvalue , p1_decrypt_cb = value , qm_decrypt_cb = value , qm_hash_cb = value , qm_spi_ok_cb = value , qm_dh_cb = value , qm_secret_key_cb = value , qm_encrypt_cb = value`

説明すべてのIKE SAがロックされ、発生する可能性のあるエラーが検出されました。このメッセージは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを報告します。

- >*value*：10 進数値
- >*hexvalue*：16 進数値

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

713233

エラーメッセージ `%Threat Defense-7-713233: (VPN-unit ) Remote network (remote network ) validated for network extension mode.`

説明フェーズ2ネゴシエーション中に受信されたリモートネットワークが検証されました。このメッセージは、ネットワーク拡張モード クライアントのフェーズ 2 ネゴシエーションでリモート ネットワーク チェックの結果を示します。これは、ユーザーがハードウェア クライアント ネットワークの設定を誤らないようにするための既存の機能の一部です（複数のクライアントでの重複するネットワークや同じネットワークの設定など）。

- *remote network*：フェーズ 2 のプロキシのサブネット アドレスおよびサブネット マスク

推奨アクション 不要。

713234

エラーメッセージ `%Threat Defense-7-713234: (VPN-unit) Remote network (remote network ) from network extension mode client mismatches AAA configuration (aaa network ).`

説明フェーズ2ネゴシエーション中に受信されたリモートネットワークが、このセッションのAAA サーバーから戻された framed-ip-address および framed-subnet-mask と一致しません。

- *remote network*：フェーズ 2 のプロキシのサブネット アドレスおよびサブネット マスク
- *aaa network*：AAA で設定されたサブネット アドレスおよびサブネット マスク

推奨アクション 次のいずれかを実行します。

- このユーザーとグループのアドレス割り当てをチェックし、HW クライアントのネットワーク コンフィギュレーションを確認して、不整合をすべて修正します。
- このユーザーおよびグループのアドレス割り当てをディセーブルにします。

713235

エラーメッセージ `%Threat Defense-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!`

説明 通常、IKE パケットをスタンバイ装置からリモート ピアへ送信することはありません。このような試みがされた場合、内部ロジック エラーが発生している可能性があります。保護コードのため、パケットはスタンバイ装置から離れません。このメッセージは、デバッグを促進します。

推奨アクション 不要。

713236

エラーメッセージ `%Threat Defense-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen`

説明 IKE はさまざまなメッセージを送信または受信しました。

次の例に、IKE が 8 バイトのハッシュ ペイロード、11 バイトの通知ペイロード、および 2 つの 13 バイトのベンダー固有ペイロードを含むメッセージを受信した場合の出力を示します。

```
%Threat Defense-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads: HDR + HASH
 (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

推奨アクション 不要。

713237

エラーメッセージ `%Threat Defense-5-713237: ACL update (access_list ) received during re-key re-authentication will not be applied to the tunnel.`

説明次の条件で、リモート アクセス IPSec トンネルのフェーズ 1 のキー再生成が表示されます。

- トンネルは、トンネルのキー再生成時にユーザーを再認証するよう設定されています。
- RADIUS サーバーは、アクセス リストまたはリファレンスを、ローカルで設定されたアクセス リストに戻します。これは、トンネルが最初に確立されたときに戻されたアクセス リストとは異なります。

推奨アクション これらの条件下では、Secure Firewall Threat Defense デバイス は新しいアクセス リストを無視し、このメッセージを生成します。

- >*access_list*：**show access-list** コマンドの出力に表示されるスタティックまたはダイナミック アクセス リストに関連付けられた名前

IPSec ユーザーは、ユーザー指定のアクセス リストを有効にするため、再接続する必要があります。

713238

エラーメッセージ `%Threat Defense-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client`

説明 ネットワーク拡張モード クライアントのプライベート側のアドレスが 0.0.0.0 です。通常、これは、ハードウェア クライアントのプライベート インターフェイスで IP アドレスが設定されていなかったことを示します。

推奨アクション リモート クライアントのコンフィギュレーションを確認します。

713239

エラーメッセージ `%Threat Defense-4-713239: IP_Address : Tunnel Rejected: The maximum tunnel count allowed has been reached`

説明 トンネルの最大許容数に達した後に、トンネル作成が試行されました。

- **IP_Address**：ピアの IP アドレス

推奨アクション 不要。

713240

エラーメッセージ `%Threat Defense-4-713240: Received DH key with bad length: received length=rlength expected length=elength`

説明 誤った長さの Diffie-Hellman キーをピアから受信しました。

- rlength：受信した DH キーの長さ
- elength：予期された長さ（DH キー サイズに基づく）

推奨アクション 不要。

713241

エラーメッセージ `%Threat Defense-4-713241: IE Browser Proxy Method setting_number is Invalid`

説明 ModeCfg の処理中に無効なプロキシ設定が見つかりました。P1 ネゴシエーションは失敗します。

推奨アクション **msie-proxy method** コマンド設定（**group-policy** コマンドのサブコマンド）を確認します。[**auto-detect** | **no-modify** | **no-proxy** | **use-server**] のいずれかが設定されているはずです。他の値が設定されている場合や値がない場合は、誤っています。**msie-proxy method** コ

マンドの設定をやり直してみてください。問題が解決しない場合、Cisco TAC にお問い合わせください。

713242

エラーメッセージ `%Threat Defense-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.`

説明 Secure Firewall Threat Defense デバイス が、ハイブリッド Xauth を使用するように設定されたトンネルに対する IKE キー再生成の開始要求を検出しましたが、キー再生成が開始されませんでした。Secure Firewall Threat Defense デバイスは、クライアントが IKE キー再生成を検出して開始するまで待ちます。

推奨アクション 不要。

713243

エラーメッセージ `%Threat Defense-4-713243: META-DATA Unable to find the requested certificate`

説明 IKE ピアが cert-req ペイロードで証明書を要求しました。しかし、要求した DN によって発行された有効な ID 証明書が見つかりませんでした。

推奨アクション：次のステップを実行します。

1. ID 証明書を確認します。
2. 必要な証明書を登録またはインポートします。
3. 詳細情報を得るために、証明書のデバッグをイネーブルにします。

713244

エラーメッセージ `%Threat Defense-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type .`

説明受信した LAM 属性タイプが、最後に受信したタイプと異なります。タイプは、ユーザー認証プロセス全体で同じである必要があります。ユーザー認証プロセスを続行できず、VPN 接続が確立されません。

- **type**：LAM タイプ

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

713245

エラーメッセージ `%Threat Defense-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.`

説明 CRACK チャレンジまたは応答ユーザー認証プロセス中に、サポートされていない LAM タイプを受信しました。ユーザー認証プロセスを続行できず、VPN 接続が確立されません。

• **type**：LAM タイプ

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

713246

エラーメッセージ `%Threat Defense-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.`

説明 Secure Firewall Threat Defense デバイス が、未知の LAM 属性タイプを受信しました。これは、接続の問題にはなりませんが、ピアの機能に影響する場合があります。

• **type**：LAM 属性タイプ

推奨アクション 不要。

713247

エラーメッセージ `%Threat Defense-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.`

説明状態処理中に予期しないエラーが発生しました。

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

713248

エラーメッセージ `%Threat Defense-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.`

説明 CRACK 認証方式による IKE SA のネゴシエート中、正常なキー再生成前にヘッドエンドのフェーズ 1 SA キー再生成タイマーが期限切れになりました。CRACK 認証方式を使用する場合は、リモートクライアントが必ず交換の発信側になるため、ヘッドエンドはキー再生成を開始しません。IKE SA が期限切れになる前にリモートピアが正常なキー再生成を開始しないと、IKE SA の期限切れで接続がダウンします。

推奨アクション 不要。

713249

エラーメッセージ `%Threat Defense-4-713249: META-DATA Received unsupported authentication results: result`

説明 CRACK 認証方式による IKE SA のネゴシエート中、IKE サブシステムが CRACK 認証時にサポートされていない結果を認証サブシステムから受信しました。ユーザー認証は失敗し、VPN 接続は切断されます。

• *result*：認証サブシステムから返された結果

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

713250

エラーメッセージ `%Threat Defense-5-713250: META-DATA Received unknown Internal Address attribute: attribute`

説明 Secure Firewall Threat Defense デバイス が、認識できない内部アドレス属性の要求を受信しました。属性は有効であっても、現在サポートされていないか、ピアが不正な値を送信している可能性があります。これは、接続の問題にはなりませんが、ピアの機能に影響する場合があります。

推奨アクション 不要。

713251

エラーメッセージ `%Threat Defense-4-713251: META-DATA Received authentication failure message`

説明 CRACK 認証方式による IKE SA のネゴシエート中、Secure Firewall Threat Defense デバイス が認証の失敗を示す通知メッセージを受信しました。接続は切断されます。

推奨アクション 不要。

713252

エラーメッセージ `%Threat Defense-5-713252: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.`

説明 クライアントに Zonelab Integrity Server での認証を要求するようにグループ ポリシーが設定されている場合、設定されている失敗ポリシーによっては、サーバーがコンセントレータに接続する必要があります。失敗ポリシーによってクライアント接続が拒否される場合、クライアントの接続時に Zonelab Integrity Server が Secure Firewall Threat Defense デバイス に接続されていないと、このメッセージが生成されます。

- *group*：リモート アクセス ユーザーが接続しているトンネル グループ
- *user*：リモート アクセス ユーザー
- *ip*：リモート アクセス ユーザーの IP アドレス

推奨アクション コンセントレータと Zonelab Integrity Server のコンフィギュレーションが一致することを確認します。その後、コンセントレータと Zonelab Integrity Server の間に通信が存在することを確認します。

713253

エラーメッセージ `%Threat Defense-5-713253: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.`

説明 クライアントに Zonelab Integrity Server での認証を要求するようにグループ ポリシーが設定されている場合、設定されている失敗ポリシーによっては、サーバーがコンセントレータに

接続する必要があります。失敗ポリシーによってクライアント接続が受け入れられ、無制限のネットワーク アクセスが提供される場合、クライアントの接続時に Zonelab Integrity Server が Secure Firewall Threat Defense デバイス に接続されていないと、このメッセージが生成されます。

- *group*：リモート アクセス ユーザーが接続しているトンネル グループ
- *user*：リモート アクセス ユーザー
- *ip*：リモート アクセス ユーザーの IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス と Zonelab Integrity Server のコンフィギュレーションが一致することを確認し、Secure Firewall Threat Defense デバイス と Zonelab Integrity Server の間に通信が存在することを確認します。

713254

エラーメッセージ `%Threat Defense-3-713254: Group = groupname , Username = username , IP = peerip , Invalid IPsec/UDP port = portnum , valid range is minport - maxport , except port 4500, which is reserved for IPsec/NAT-T`

説明 UDP ポート 4500 は IPSec または NAT-T 接続用に予約されているため、IPSec/UDP 接続には使用できません。CLI では、ローカル グループに対してこのコンフィギュレーションが許可されません。このメッセージは、外部で定義されたグループに限り発生します。

- *groupname*：ユーザー グループの名前
- *username*：ユーザーの名前
- *peerip*：クライアントの IP アドレス
- *portnum*：外部サーバー上の IPSec/UDP ポート番号
- *minport*：ユーザーが設定可能なポートの最小有効ポート番号（4001）
- *maxport*：ユーザーが設定可能なポートの最大有効ポート番号（49151）

推奨アクション 外部サーバー上の IPSec または UDP ポート番号を別のポート番号に変更します。有効なポート番号は 4001 ～ 49151 です。

713255

エラーメッセージ `%Threat Defense-4-713255: IP = peer-IP , Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name`

説明 ISAKMP アグレッシブ モードのメッセージ 1 で不明なトンネル グループが指定されました。

- *peer-ip*：ピアのアドレス
- *group-name*：ピアによって指定されたグループ名

推奨アクション トンネル グループとクライアント コンフィギュレーションが有効であることを確認します。

713256

エラーメッセージ `%Threat Defense-6-713256: IP = peer-IP , Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.`

説明 ピアによって無効なトンネル グループが指定されると、Secure Firewall Threat Defense デバイス は引き続きメッセージ 2 を送信して、ピアでトンネル グループ情報が収集されるのを防止します。

- *peer-ip*：ピアのアドレス

推奨アクション 不要。

713257

エラーメッセージ `%Threat Defense-5-713257: Phase var1 failure: Mismatched attribute types for class var2 : Rcv'd: var3 Cfg'd: var4`

説明 Secure Firewall Threat Defense デバイス が、LAN-to-LAN 接続で応答側として動作しました。これは、Secure Firewall Threat Defense の暗号コンフィギュレーションが発信側のコンフィギュレーションと一致しないことを示しています。このメッセージでは、ミスマッチが発生したフェーズ、および応答側と発信側の両方が持つ属性のうち一致しない属性が指摘されます。

- *var1*：ミスマッチが発生したフェーズ
- *var2*：一致しない属性が属するクラス
- *var3*：発信側から受信した属性
- *var4*：設定されている属性

推奨アクション 両方の LAN-to-LAN デバイスで暗号コンフィギュレーションの不整合を確認します。特に、UDP-Tunnel（NAT-T）と他のデバイスとの間のミスマッチが報告された場合は、クリプトマップを確認してください。一方のコンフィギュレーションの一致したクリプトマップで NAT-T がディセーブルになっており、もう一方ではディセーブルになっていない場合、障害の原因となります。

713258

エラーメッセージ `%Threat Defense-3-713258: IP = var1 , Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface. Tearing down old phase1 tunnel due to a potential routing change.`

説明 Secure Firewall Threat Defense デバイス がインターフェイスでフェーズ 2 トンネルを確立しようとしたときに、別のインターフェイスにフェーズ 1 トンネルがすでに存在しています。既存のフェーズ 1 トンネルは切断され、新しいインターフェイスで新しいトンネルを確立できるようになります。

- *var1*：ピアの IP アドレス
- *var2*：Secure Firewall Threat Defense デバイス がフェーズ 2 トンネルを確立しようとしているインターフェイス
- *var3*：フェーズ 1 トンネルが存在するインターフェイス

推奨アクション ピアのルートが変更されていないかどうかを確認します。ルートが変更されていない場合は、コンフィギュレーションが誤っている可能性があります。

713259

エラーメッセージ `%Threat Defense-5-713259: Group = groupname , Username = username , IP = peerIP , Session is being torn down. Reason: reason`

説明 ISAKMP セッションの終了原因が表示されます。これは、セッション管理によってセッションが切断された場合に発生します。

- *groupname*：終了されるセッションのトンネル グループ。
- *username*：終了されるセッションのユーザー名。
- *peerIP*：終了されるセッションのピア アドレス。
- *reason*：終了されるセッションの RADIUS 終了原因。原因は次のとおりです。

- ポートが切り替えられた（同時ログイン）

- アイドル タイムアウト

- 最大時間を超過した

- 管理者がリセットした

推奨アクション 不要。

713260

エラーメッセージ `%Threat Defense-3-713260: Output interface %d to peer was not found`

説明 フェーズ 1 SA を作成しようとしたときに、そのインターフェイス ID のインターフェイス データベースが見つかりませんでした

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

713261

エラーメッセージ `%Threat Defense-3-713261: IPV6 address on output interface %d was not found`

説明 フェーズ 1 SA を作成しようとしたときに、IPv6 アドレスがローカル インターフェイスで指定されていません。

推奨アクション 目的のインターフェイスの IPv6 アドレスを設定する方法の詳細については、『CLI 構成ガイド』の「Configuring IPv6 Addressing」セクションを参照してください。

713262

エラーメッセージ `%Threat Defense-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address . A negotiation was already in progress for local Proxy Local_address /Local_prefix_len , remote Proxy Remote_address /Remote_prefix_len`

説明フェーズ SA を確立するとき、Secure Firewall Threat Defense デバイス はこのプロキシに一致する新しいフェーズ 2 SA を拒否します。

- *Peer_address*：既存のネゴシエーションと一致するプロキシでフェーズ 2 を開始しようとしている新しいアドレス
- *Local_address*：現在フェーズ2をネゴシエートしている、以前のローカル ピアのアドレス
- *Local_prefix_len*：CIDR 表記に従ったサブネット プレフィックス長
- *Remote_address*：プロキシのアドレス
- *Remote_prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713263

エラーメッセージ `%Threat Defense-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask /prefix_len , Protocol protocol , Port port`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しています。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長
- *protocol*：プロキシ プロトコル
- *port*：プロキシ ポート

推奨アクション 不要。

713264

エラーメッセージ `%Threat Defense-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask/prefix_len , Protocol protocol , Port port {"Received remote IP Proxy Subnet data in ID Payload: Address %a , Mask/%d , Protocol %u , Port %u "}`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しています。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長
- *protocol*：プロキシ プロトコル
- *port*：プロキシ ポート

推奨アクション 不要。

713265

エラーメッセージ `%Threat Defense-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しています。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713266

エラーメッセージ `%Threat Defense-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しようとして失敗しました。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。これは、ルートの重複か、IPv6 ルーティング テーブルがいっぱいになっているか、前に使用したルートを Secure Firewall Threat Defense デバイスが削除していないことを意味している場合があります。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション IPv6 ルーティング テーブルに追加ルートのためのスペースがあることと、古いルートが存在しないことを確認します。テーブルがいっぱいになっている場合や古いルートが含まれている場合は、ルートを削除して再試行します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713267

エラーメッセージ `%Threat Defense-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しようとして失敗しました。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713268

エラーメッセージ `%Threat Defense-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを削除しようとしたときに障害が発生しました。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。ルートがすでに削除されているか、内部ソフトウェア エラーが発生しました。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション ルートがすでに削除されている場合は、問題のない状態であり、デバイスは正常に機能します。問題が解決しない場合、または VPN トンネルでルーティングの問題にリンクできる場合は、VPN L2L コンフィギュレーションのルーティング部分とアドレッシング部分を確認します。また、逆ルートの注入と、適切なクリプト マップに関連する ACL も確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713269

エラーメッセージ `%Threat Defense-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: /prefix_len`

説明 ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートが追加されています。この設定によって、Secure Firewall Threat Defense デバイス は、ヘッドエンドのプライベート側にあるすべてのルータにリモート ネットワークを知らせることができます。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713270

エラーメッセージ `%Threat Defense-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: /prefix_len`

説明 内部ソフトウェア エラーが発生しました。ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートを追加する試みが失敗しました。IPv6 ルーティング テーブルがいっぱいになっているか、アドレッシング エラーが発生した可能性があります。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

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

713271

エラーメッセージ `%Threat Defense-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask:/prefix_len`

説明 ネットワーク拡張モードのハードウェア クライアントへのトンネルが除去され、ハードウェア クライアントの背後でプライベート ネットワーク用のスタティック ルートが削除されています。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713272

エラーメッセージ `%Threat Defense-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: /prefix_len`

説明 ネットワーク拡張モードのハードウェア クライアントへのトンネルを除去しているときに、ハードウェア クライアントの背後にあるプライベート ネットワークへのルートを削除できません。これは、アドレッシングまたはソフトウェアの問題を意味する場合があります。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション IPv6 ルーティング テーブルを調べて、ルートがそこにないことを確認します。ルートがある場合は、手動で削除する必要がありますが、ハードウェア クライアントへのトンネルが完全に削除された場合に限り行います。

713273

エラーメッセージ `%Threat Defense-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed`

説明 ピアが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートがルーティング テーブルから削除されました。

推奨アクション 不要。

713274

エラーメッセージ `%Threat Defense-3-713274: Could not delete static route for client address: IP_Address IP_Address address of client whose route is being removed`

説明 IPSec クライアントへのトンネルが削除されたときに、ルーティング テーブル中のそのエントリを削除できませんでした。この状態は、ネットワーキングまたはソフトウェアの問題を示している場合があります。

推奨アクション ルーティング テーブルにルートがないことを確認します。ルートが存在する場合、トンネルが正常にクローズされた場合だけ、ルートを手動で削除する必要があります。

713275

エラーメッセージ `%Threat Defense-3-713275: IKEv1 Unsupported certificate keytype %s found at trustpoint %s`

説明 証明書のキー タイプが ECDSA でない場合、この syslog が ikev1 に対して表示されます。必ず、有効なキー タイプの証明書を GW にインストールします。

推奨アクション 不要。

713276

エラーメッセージ `%Threat Defense-3-713276: Dropping new negotiation - IKEv1 in-negotiation context limit of %u reached`

説明 ネゴシエーションの上限に達した場合、この Syslog メッセージがマルチコンテキストで ikev1 に対して表示されます。

推奨アクション 必要なし。

713900

エラーメッセージ `%Threat Defense-1-713900: Descriptive_event_string.`

説明 重大なイベントまたは障害が発生しました。たとえば、Secure Firewall Threat Defense デバイス がフェーズ 2 削除を生成しようとしたが、SPI が既存のどのフェーズ 2 SA とも一致しませんでした。

推奨アクション 上記の例では、両方のピアが同時にフェーズ 2 SA を削除しています。この場合、問題のないエラーであるため、無視してかまいません。エラーが引き続き表示され、トンネルの廃棄やデバイスのリブートなどの副作用が生じる場合は、ソフトウェア障害を示している可能性があります。その場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco TAC に問い合わせてサポートを受けてください。

713901

エラーメッセージ `%Threat Defense-2-713901: Descriptive_event_string .`

説明 エラーが発生しました。これは、ヘッドエンドまたはリモート アクセス クライアントにおけるコンフィギュレーション エラーの結果である可能性があります。イベント文字列は、発生したエラーの詳細を提供します。

推奨アクション 場合によっては、エラーの原因を判別するためメッセージをトラブルシューティングする必要があります。両方のピアで、ISAKMP およびクリプト マップ コンフィギュレーションを確認します。

713902

エラーメッセージ `% Threat Defense-3-713902: Descriptive_event_string.`

説明エラーが発生しました。これは、ヘッドエンドまたはリモート アクセス クライアントにおけるコンフィギュレーション エラーの結果である可能性があります。

推奨アクション場合によっては、エラーの原因を判別するためコンフィギュレーションをトラブルシューティングする必要があります。両方のピアで、ISAKMP およびクリプト マップ コンフィギュレーションを確認します。

713903

エラーメッセージ `%Threat Defense-4-713903: IKE error message reason reason.`

説明 この Syslog ID は、複数の他の Syslog を表示できる IKE 警告メッセージに使用されます。

推奨アクション必要なし。

次に、例を示します。

`%Threat Defense-4-713903: Group = group policy , Username = user name , IP = remote IP , ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP`

`%Threat Defense-4-713903: IKE Receiver: Runt ISAKMP packet discarded on Port Port_Number from Source_URL`

`%Threat Defense-4-713903: IP = IP address, Header invalid, missing SA payload! (next payload = x)`

`%Threat Defense-4-713903: Group = DefaultRAGroup, IP = IP address, Error: Unable to remove PeerTblEntry`

713904

エラーメッセージ `%Threat Defense-5-713904: Descriptive_event_string .`

説明発生したイベントを追跡するために使用される通知ステータス情報が表示されます。

推奨アクション 不要。

713905

エラーメッセージ `%Threat Defense-6-713905: Descriptive_event_string.`

説明発生したイベントを追跡するために使用される情報ステータスの詳細が表示されます。

例

```
%Threat Defense-6-713905: IKE successfully unreserved UDP port 27910 on interface outside
```

推奨アクション必要なし。

713906

エラーメッセージ `%Threat Defense-7-713906: Descriptive_event_string .`

説明発生したイベントを追跡するために使用されるデバッグのステータス情報が表示されます。

推奨アクション 不要。

714001

エラーメッセージ `%Threat Defense-7-714001: description_of_event_or_packet`

説明 IKE プロトコル イベントまたはパケットの説明が示されます。

推奨アクション 不要。

714002

エラーメッセージ `%Threat Defense-7-714002: IKE Initiator starting QM: msg id = message_number`

説明 Secure Firewall Threat Defense デバイス が、フェーズ 2 発信側としてクイック モード交換の最初のパケットを送信しました。

推奨アクション 不要。

714003

エラーメッセージ `%Threat Defense-7-714003: IKE Responder starting QM: msg id = message_number`

説明 Secure Firewall Threat Defense デバイス が、フェーズ 2 応答側としてクイック モード交換の最初のパケットを受信しました。

推奨アクション 不要。

714004

エラーメッセージ `%Threat Defense-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number`

説明最初のクイック モード パケットのプロトコルがデコードされました。

推奨アクション 不要。

714005

エラーメッセージ `%Threat Defense-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number`

説明 2 番目のクイック モード パケットのプロトコルがデコードされました。

推奨アクション 不要。

714006

エラーメッセージ `%Threat Defense-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number`

説明 3 番目のクイック モード パケットのプロトコルがデコードされました。

推奨アクション 不要。

714007

エラーメッセージ `%Threat Defense-7-714007: IKE Initiator sending Initial Contact`

説明 Secure Firewall Threat Defense デバイス は、最初のコンタクト ペイロードを構築および送信しています。

推奨アクション 不要。

714011

エラーメッセージ `%Threat Defense-7-714011: Description of received ID values`

説明 Secure Firewall Threat Defense デバイス が、ネゴシエーション中に、表示された ID 情報を受信しました。

推奨アクション 不要。

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。