Syslog メッセージ 715001 ～ 721019

この章は、次の項で構成されています。

メッセージ 715001 ～ 715080

この項では、715001 から 715080 までのメッセージについて説明します。

715001

エラーメッセージ `%Threat Defense-7-715001: Descriptive statement`

説明 Secure Firewall Threat Defense デバイス が検出したイベントまたは問題の説明が表示されます。

推奨アクション 説明によって異なります。

715004

エラーメッセージ `%Threat Defense-7-715004: subroutine name () Q Send failure: RetCode (return_code )`

説明キュー内にメッセージを置こうとしたときに内部エラーが発生しました。

推奨アクション 多くの場合、これは問題のない状態です。問題が解決しない場合、Cisco TAC にお問い合わせください。

715005

エラーメッセージ `%Threat Defense-7-715005: subroutine name() Bad message code: Code (message_code )`

説明内部サブルーチンが不良なメッセージ コードを受信しました。

推奨アクション 多くの場合、これは問題のない状態です。問題が解決しない場合、Cisco TAC にお問い合わせください。

715006

エラーメッセージ `%Threat Defense-7-715006: IKE got SPI from key engine: SPI = SPI_value`

説明 IKE サブシステムが IPSec から SPI 値を受信しました。

推奨アクション 不要。

715007

エラーメッセージ `%Threat Defense-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value`

説明 IKE がトンネル ネゴシエーションを完了し、IPSec が使用する適切な暗号キーとハッシュ キーを正常にロードしました。

推奨アクション 不要。

715008

エラーメッセージ `%Threat Defense-7-715008: Could not delete SA SA_address, refCnt = number , caller = calling_subroutine_address`

説明呼び出し側のサブルーチンが IPSec SA を削除できません。これは、リファレンス カウントの問題の可能性があることを示しています。

推奨アクション このイベントの結果として古い SA の数が増加した場合は、Cisco TAC にお問い合わせください。

715009

エラーメッセージ `%Threat Defense-7-715009: IKE Deleting SA: Remote Proxy IP_address , Local Proxy IP_address`

説明リストされたプロキシ アドレスで SA が削除されています。

推奨アクション 不要。

715013

エラーメッセージ `%Threat Defense-7-715013: Tunnel negotiation in progress for destination IP_address , discarding data`

説明 IKEは、このデータ用のトンネルを確立しています。トンネルが完全に確立されるまで、このトンネルによって保護されるすべてのパケットが廃棄されます。

推奨アクション 不要。

715018

エラーメッセージ `%Threat Defense-7-715018: IP Range type id was loaded: Direction %s, From: %a, Through: %a`

説明 この syslog メッセージは、IPSEC SA の詳細を更新する際に生成されます。

推奨アクション 不要。

715019

エラーメッセージ `%Threat Defense-7-715019: Group group Username username IP ip IKEGetUserAttributes: Attribute name = name`

説明 Secure Firewall Threat Defense デバイス によって処理されている **modecfg** 属性の名前と値のペアが表示されます。

推奨アクション 不要。

715020

エラーメッセージ `%Threat Defense-7-715020: construct_cfg_set: Attribute name = name`

説明 Secure Firewall Threat Defense デバイス によって送信されている **modecfg** 属性の名前と値のペアが表示されます。

推奨アクション 不要。

715021

エラーメッセージ `%Threat Defense-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress`

説明 フェーズ1処理がすべて完了するまで（トランザクション モードの場合）、クイック モードの処理が遅延しています。

推奨アクション 不要。

715022

エラーメッセージ `%Threat Defense-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed`

説明フェーズ 1 処理が完了し、クイック モードの処理が再開されています。

推奨アクション 不要。

715027

エラーメッセージ `%Threat Defense-7-715027: IPsec SA Proposal # chosen_proposal , Transform # chosen_transform acceptable Matches global IPsec SA entry # crypto_map_index`

説明示された IPSec SA プロポーザルおよびトランスフォームが応答側が受信したペイロードから選択されました。このデータは、IKEネゴシエーションの問題のデバッグを試みる際に役立ちます。

推奨アクション 不要。

715028

エラーメッセージ `%Threat Defense-7-715028: IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index`

説明示された IKE SA トランスフォームが応答側が受信したペイロードから選択されました。このデータは、IKE ネゴシエーションの問題のデバッグを試みる際に役立ちます。

推奨アクション 不要。

715031

エラーメッセージ `%Threat Defense-7-715031: Obtained IP addr (%s) prior to initiating Mode Cfg (XAuth %s)`

説明この syslog は、IP アドレスが IP util サブシステムによって割り当てられている場合に生成されます。

推奨アクション 不要。

715032

エラーメッセージ `%Threat Defense-7-715032: Sending subnet mask (%s) to remote client`

説明この syslog は、IP アドレスが IP util サブシステムによって割り当てられている場合に生成されます。

推奨アクション 不要。

715033

エラーメッセージ `%Threat Defense-7-715033: Processing CONNECTED notify (MsgId message_number )`

説明 Secure Firewall Threat Defense デバイス が通知タイプ CONNECTED（16384）で通知ペイロードを含むメッセージを処理しています。CONNECTED 通知タイプは、コミット ビット処理を完了するために使用されます。これは、応答側から発信側へ送信される 4 番目のクイックモード パケット全体に組み込む必要があります。

推奨アクション 不要。

715034

エラーメッセージ `%Threat Defense-7-715034: action IOS keep alive payload: proposal=time 1 /time 2 sec.`

説明キープアライブ ペイロード メッセージの送信または受信が処理されています。

推奨アクション 不要。

715035

エラーメッセージ `%Threat Defense-7-715035: Starting IOS keepalive monitor: seconds sec.`

説明キープアライブ タイマーがキープアライブ メッセージを可変の秒数の間だけモニターします。

推奨アクション 不要。

715036

エラーメッセージ `%Threat Defense-7-715036: Sending keep-alive of type notify_type (seq number number )`

説明キープアライブ通知メッセージの送信が処理されています。

推奨アクション 不要。

715037

エラーメッセージ `%Threat Defense-7-715037: Unknown IOS Vendor ID version: major.minor.variance`

説明 Cisco IOS のこのバージョンの機能は不明です。

推奨アクションIKE キープアライブなどの機能との相互運用の問題がある可能性があります。問題が解決しない場合、Cisco TAC にお問い合わせください。

715038

エラーメッセージ %Threat Defense-7-715038: *action Spoofing_information* Vendor ID payload (version: *major.minor.variance* , capabilities: *value*)

説明 Cisco IOS ベンダー ID ペイロードの処理が実行されました。実行されている処理が、Cisco IOS をスプーフィングしている Altiga である可能性があります。

推奨アクション 不要。

715039

エラーメッセージ %Threat Defense-7-715039: Unexpected cleanup of tunnel table entry during SA delete.

説明 SA が解放されたときに IKE トンネル テーブル内のエントリが削除されませんでした。これは、ステート マシン内の障害を示しています。

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。

715040

エラーメッセージ %Threat Defense-7-715040: Deleting active auth handle during SA deletion: handle = *internal_authentication_handle*

エラーメッセージ SA 削除中に認証ハンドルがまだアクティブでした。これは、エラー状態中のクリーンアップ リカバリの一部です。

推奨アクション 不要。

715041

エラーメッセージ %Threat Defense-7-715041: Received keep-alive of type *keepalive_type* , not the negotiated type

説明 メッセージ内に示されたタイプのキープアライブが予期せず受信されました。

推奨アクション 両方のピアでキープアライブ コンフィギュレーションを確認します。

715042

エラーメッセージ %Threat Defense-7-715042: IKE received response of type *failure_type* to a request from the *IP_address* utility

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。メッセージ文字列内の変数テキストによって、問題点がより具体的に示されます。

推奨アクション IP アドレス割り当てコンフィギュレーションを確認し、適宜、調整します。

715044

エラーメッセージ `%Threat Defense-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability`

説明キープアライブ機能が設定されていない状態で、ベンダーから Cisco IOS キープアライブ ペイロードを受信しました。ペイロードは無視されます。

推奨アクション 不要。

715045

エラーメッセージ `%Threat Defense-7-715045: ERROR: malformed Keepalive payload`

説明形式が誤ったキープアライブ ペイロードを受信しました。ペイロードは無視されます。

推奨アクション 不要。

715046

エラーメッセージ `%Threat Defense-7-715046: Group = groupname , Username = username , IP = IP_address , constructing payload_description payload`

説明特定のグループおよびユーザーのリモート クライアントの IP アドレスによって、構築中の IKE ペイロードの詳細が表示されます。

推奨アクション 不要。

715047

エラーメッセージ `%Threat Defense-7-715047: processing payload_description payload`

説明受信して処理中の IKE ペイロードの詳細が表示されます。

推奨アクション 不要。

715048

エラーメッセージ `%Threat Defense-7-715048: Send VID_type VID`

説明送信中のベンダー ID ペイロードのタイプが表示されます。

推奨アクション 不要。

715049

エラーメッセージ `%Threat Defense-7-715049: Received VID_type VID`

説明受信したベンダー ID ペイロードのタイプが表示されます。

推奨アクション 不要。

715050

エラーメッセージ `%Threat Defense-7-715050: Claims to be IOS but failed authentication`

説明受信したベンダー ID は Cisco IOS VID と似ていますが、**hmac_sha** とは一致しません。

推奨アクション 両方のピアでベンダー ID コンフィギュレーションを確認します。この問題が相互運用に影響し、問題が解決しない場合は、Cisco TAC にお問い合わせください。

715051

エラーメッセージ `%Threat Defense-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply`

説明 FWTYPE ModeCfg Reply の処理中に、Secure Firewall Threat Defense レコードで未知の TLV が受信されました。TLV は廃棄されます。パケットが破損しているため、または接続しているクライアントが後のバージョンの Secure Firewall Threat Defense プロトコルをサポートしているために発生する可能性があります。

推奨アクション Cisco VPN クライアントにインストールされている個人用 FW および Secure Firewall Threat Defense デバイス 上のパーソナル ファイアウォール コンフィギュレーションを確認します。これは、VPN クライアントと Secure Firewall Threat Defense デバイス の間のバージョンの不一致を示している可能性もあります。

715052

エラーメッセージ `%Threat Defense-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries`

説明古い P1 SA が削除されていますが、新しい SA にも削除のマークが付けられているため、移行先となる新しい SA がありません。通常、これは、2 つの IKE ピアが同期外で、異なるキー再生成時間を使用している可能性があることを示しています。問題は自動的に訂正されますが、新しい P1 SA が再確立されるまで、少量のデータ損失が発生する可能性があります。

推奨アクション 不要。

715053

エラーメッセージ `%Threat Defense-7-715053: MODE_CFG: Received request for attribute_info !`

説明 Secure Firewall Threat Defense デバイス が、指摘された属性を要求するモード コンフィギュレーション メッセージを受信しました。

推奨アクション 不要。

715054

エラーメッセージ `%Threat Defense-7-715054: MODE_CFG: Received attribute_name reply: value`

説明 Secure Firewall Threat Defense が、リモート ピアからモード コンフィギュレーション応答メッセージを受信しました。

推奨アクション 不要。

715055

エラーメッセージ `%Threat Defense-7-715055: Send attribute_name`

説明 Secure Firewall Threat Defense デバイス が、リモート ピアにモード コンフィギュレーション メッセージを送信しました。

推奨アクション 不要。

715056

エラーメッセージ `%Threat Defense-7-715056: Client is configured for TCP_transparency`

説明 IPsec over TCP に対してリモート エンド（クライアント）が設定されているので、ヘッドエンドの Secure Firewall Threat Defense デバイス がクライアントと IPsec over UDP または IPsec over NAT-T をネゴシエートすることはできません。

推奨アクション トンネルが開始しない場合は、ピアのいずれかの NAT 透過コンフィギュレーションに対する調整が必要な場合があります。

715057

エラーメッセージ `%Threat Defense-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPsec-over-UDP configuration.`

説明 NAT-Traversal が検出されたため、IPSec-over-UDP モード コンフィギュレーション情報は交換されません。

推奨アクション 不要。

715058

エラーメッセージ `%Threat Defense-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.`

説明 NAT-Traversal VID の交換後、リモート エンドが NAT-Traversal に必要な NAT-Discovery ペイロードを提供しませんでした。少なくとも 2 つの NAT-Discovery ペイロードを受信する必要があります。

推奨アクション NAT-T 実装が規格に従っていないことを示している可能性があります。攻撃ピアがシスコ製品であり、問題が解決しない場合は、Cisco TAC にお問い合わせください。攻撃ピアがシスコ製品ではない場合は、製造元サポート チームにお問い合わせください。

715059

エラーメッセージ `%Threat Defense-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal`

説明 NAT-Traversal を正常にネゴシエートするため SA で定義された通常のトランスポート モードおよびトンネル モードの代わりにこれらのモードを使用する必要があります。

推奨アクション 不要。

715060

エラーメッセージ `%Threat Defense-7-715060: Dropped received IKE fragment. Reason: reason`

説明 フラグメントを廃棄した理由が表示されます。

推奨アクション 推奨アクションは廃棄の理由によって異なりますが、これは、NAT デバイスが干渉している問題やピアが規格に従っていない問題を示している可能性があります。

715061

エラーメッセージ `%Threat Defense-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.`

説明 同じパケットの再送が発生しましたが、別の MTU か、あるいはまったく別のパケットにフラグメント化されました。

推奨アクション 不要。

715062

エラーメッセージ `%Threat Defense-7-715062: Error assembling fragments! Fragment numbers are non-continuous.`

説明 フラグメント番号にギャップがあります。

推奨アクション これはネットワークの問題を示している可能性があります。この状態が続き、トンネルが廃棄されるか、特定のピアがSecure Firewall Threat Defense デバイスとネゴシエートできない場合は、Cisco TAC にお問い合わせください。

715063

エラーメッセージ `%Threat Defense-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!`

説明 受信されたフラグメント化パケットのアセンブリが成功しました。

推奨アクション 不要。

715064

エラーメッセージ %Threat Defense-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: *true* /*false* Aggressive Mode: *true* /*false*

説明ピアは、メッセージで提供された情報に基づくIKEフラグメントをサポートしています。

推奨アクション 不要。

715065

エラーメッセージ %Threat Defense-7-715065: IKE *state_machine subtype* FSM error history (struct *data_structure_address*) *state* , *event* : *state* /*event* pairs

説明 フェーズ 1 エラーが発生し、**state**、**event** 履歴ペアが新しい順に表示されます。

推奨アクションこれらのエラーの大部分は問題ありません。問題が解決しない場合、Cisco TACにお問い合わせください。

715066

エラーメッセージ %Threat Defense-7-715066: Can't load an IPsec SA! The corresponding IKE SA contains an invalid logical ID.

説明 IKE SA 内の論理 ID は NULL です。フェーズ II ネゴシエーションは切断されます。

推奨アクション 内部エラーが発生しました。問題が解決しない場合、Cisco TAC にお問い合わせください。

715067

エラーメッセージ %Threat Defense-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa

説明 確立中の LAN-TO-LAN SA はすでに存在します。つまり、同じリモートネットワークを持ち、別のピアをソースとする SA があります。これは正当なコンフィギュレーションではないので、新規 SA は削除されます。

推奨アクション 関連するすべてのピアで LAN-TO-LAN コンフィギュレーションを確認します。特に、複数のピアがプライベート ネットワークを共有することはできません。

715068

エラーメッセージ %Threat Defense-7-715068: QM IsRekeyed: duplicate sa found by *address* , deleting old sa

説明 確立中のリモートアクセスSAはすでに存在します。つまり、同じリモートネットワークを持ち、別のピアをソースとするSAがあります。ピアがIPアドレスを変更した可能性があるため、古い SA は削除されます。

推奨アクション 特にクライアント トンネルが異常終了した場合、これは問題のない状態である可能性があります。問題が解決しない場合、Cisco TAC にお問い合わせください。

715069

エラーメッセージ `%Threat Defense-7-715069: Invalid ESP SPI size of SPI_size`

説明 Secure Firewall Threat Defense デバイス が、無効な ESP SPI サイズの IPSec SA プロポーザルを受信しました。このプロポーザルはスキップされます。

推奨アクション 通常、これは問題のない状態ですが、ピアが規格に従っていないことを示している可能性があります。問題が解決しない場合、Cisco TAC にお問い合わせください。

715070

エラーメッセージ `%Threat Defense-7-715070: Invalid IPComp SPI size of SPI_size`

説明 Secure Firewall Threat Defense デバイス が、無効な IPComp SPI サイズの IPSec SA プロポーザルを受信しました。このプロポーザルはスキップされます。

推奨アクション 通常、これは問題のない状態ですが、ピアが規格に従っていないことを示している可能性があります。問題が解決しない場合、Cisco TAC にお問い合わせください。

715071

エラーメッセージ `%Threat Defense-7-715071: AH proposal not supported`

説明 IPSec AH プロポーザルはサポートされていません。このプロポーザルはスキップされます。

推奨アクション 不要。

715072

エラーメッセージ `%Threat Defense-7-715072: Received proposal with unknown protocol ID protocol_ID`

説明 Secure Firewall Threat Defense デバイス が、未知のプロトコル ID を持つ IPSec SA プロポーザルを受信しました。このプロポーザルはスキップされます。

推奨アクション 通常、これは問題のない状態ですが、ピアが規格に従っていないことを示している可能性があります。問題が解決しない場合、Cisco TAC にお問い合わせください。

715074

エラーメッセージ `%Threat Defense-7-715074: Could not retrieve authentication attributes for peer IP_address`

説明 Secure Firewall Threat Defense デバイス が、リモートユーザーの認可情報を取得できません。

推奨アクション認証と認可の設定が正しく行われたことを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

715075

エラーメッセージ `%Threat Defense-7-715075: Group = group_name , IP = IP_address Received keep-alive of type message_type (seq number number )`

説明 このメッセージは、DPD 送信メッセージをログに記録する DPD R-U-THERE メッセージ 715036 とペアです。

- **group_name**：ピアの VPN グループ名
- **IP_address**：VPN ピアの IP アドレス
- **message_type**：メッセージ タイプ（DPD R-U-THERE または DPD R-U-THERE-ACK）
- **number**：DPD シーケンス番号

考えられるケースは 2 つあります。

- 受信側ピアが DPD R-U-THERE メッセージを送信する。
- 受信側ピアが DPD R-U-THERE-ACK メッセージに応答する。

次のことに注意してください。

- DPD R-U-THERE メッセージが受信され、そのシーケンス番号が発信 DPD 応答メッセージと一致する。

Secure Firewall Threat Defense デバイス がピアから DPD R-U-THERE メッセージを受信する前に DPD R-U-THERE-ACK メッセージを送信すると、セキュリティ違反が発生する可能性があります。

- 受信した DPD R-U-THERE-ACK メッセージのシーケンス番号が前の送信 DPD メッセージと一致する。

Secure Firewall Threat Defense デバイス が DPD R-U-THERE メッセージをピアへ送信した後、適当な期間 DPD R-U-THERE-ACK メッセージを受信しなかった場合、トンネルはダウンする可能性があります。

推奨アクション 不要。

715076

エラーメッセージ `%Threat Defense-7-715076: Computing hash for ISAKMP`

説明 IKE がさまざまなハッシュ値を計算しました。

このオブジェクトは次のとおり追加されます。

Group = >*groupname* , Username = >*username* , IP = >*ip_address* ...

推奨アクション 不要。

715077

エラーメッセージ `%Threat Defense-7-715077: Pitcher: msg string , spi spi`

説明 さまざまなメッセージが IKE に送信されました。

msg_string は次のいずれかです。

- Received a key acquire message
- Received SPI for nonexistent SA
- Received key delete msg
- Received KEY_UPDATE
- Received KEY_REKEY_IB
- Received KEY_REKEY_OB
- Received KEY_SA_ACTIVE
- Could not find IKE SA to activate IPSEC (OB)
- Could not find IKE SA to rekey IPSEC (OB)
- KEY_SA_ACTIVE no centry found
- KEY_ADD centry not found
- KEY_UPDATE centry not found

このオブジェクトは次のとおり追加されます。

Group = >*groupname* , Username = >*username* , IP = >*ip_address* ,...

推奨アクション 不要。

715078

エラーメッセージ `%Threat Defense-7-715078: Received %s LAM attribute`

説明この syslog は、チャレンジ/応答ペイロードの解析中に生成されます。

推奨アクション 不要。

715079

エラーメッセージ `%Threat Defense-7-715079: INTERNAL_ADDRESS: Received request for %s`

説明この syslog は、内部アドレス ペイロードの処理中に生成されます。

推奨アクション 不要。

715080

エラーメッセージ `%Threat Defense-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.`

エラー メッセージ IKE キー再生成タイマーが開始されました。

推奨アクション 不要。

メッセージ 716001 ～ 716603

この項では、716001 から 716603 までのメッセージについて説明します。

716001

エラーメッセージ `%Threat Defense-6-716001: Group group User user IP ip WebVPN session started.`

説明 指摘された IP アドレスにおける このグループ内のユーザーに対して WebVPN セッションが開始されました。ユーザーが WebVPN ログイン ページを介してログインすると、WebVPN セッションが開始されます。

推奨アクション 不要。

716002

エラーメッセージ `%Threat Defense-6-716002: Group GroupPolicy User username IP ip WebVPN session terminated: User requested.`

説明 WebVPN セッションがユーザー要求により終了されました。考えられる原因は次のとおりです。

- 搬送が失われた
- サービスの消失
- アイドル タイムアウト
- 最大時間を超過した
- 管理者がリセットした
- 管理者がリブートした
- 管理者がシャットダウンした
- ポート エラー
- NAS エラー
- NAS 要求
- NAS リブート
- ポートの不要化
- ポートが切り替えられた。この原因は、（同一ユーザーによる）同時ログイン許容数を超えたことを示します。この問題を解決するには、同時ログイン数を増やすか、ユーザーに対して特定のユーザー名とパスワードで 1 回だけログインを許可するようにします。
- ポートの保留
- 使用できないサービス
- コールバック
- ユーザー エラー
- ホストが要求した
- 帯域幅の管理エラー

- ACL 解析エラー
- グループ ポリシーで指定されている VPN 同時ログイン制限
- 不明

推奨アクション理由に問題が示されていない限り、処置は不要です。

716003

エラーメッセージ`%Threat Defense-6-716003: Group group User user IP ip WebVPN access "GRANTED: url "`

説明指摘された IP アドレスにおけるこのグループ内の WebVPN ユーザーは、この URL へのアクセス権を与えられています。さまざまな場所へのユーザーのアクセスは、WebVPN 固有の ACL を使用して制御できます。

推奨アクション 不要。

716004

エラーメッセージ`%Threat Defense-6-716004: Group group User user WebVPN access DENIED to specified location: url`

説明このグループ内の WebVPN ユーザーは、この URL へのアクセス権を拒否されています。さまざまな場所への WebVPN ユーザーのアクセスは、WebVPN 固有の ACL を使用して制御できます。この場合は、特定のエントリがこの URL へのアクセスを拒否しています。

推奨アクション 不要。

716005

エラーメッセージ `%Threat Defense-6-716005: Group group User user WebVPN ACL Parse Error: reason`

説明指摘されたグループ内の WebVPN ユーザーの ACL が正しく解析できませんでした。

推奨アクション WebVPN ACL を修正します。

716006

エラーメッセージ`%Threat Defense-6-716006: Group name User user WebVPN session terminated. Idle timeout.`

説明 VPN トンネル プロトコルが WebVPN に設定されていないため、指摘されたグループ内でユーザーに対して WebVPN セッションが作成されませんでした。

推奨アクション 不要。

716007

エラーメッセージ `%Threat Defense-4-716007: Group group User user WebVPN Unable to create session.`

説明 リソースの問題のため、指摘されたグループ内のユーザーに対して WebVPN セッションが作成されませんでした。たとえば、ユーザーが最大ログイン制限に達した可能性があります。

推奨アクション 不要。

716008

エラーメッセージ `%Threat Defense-7-716008: WebVPN ACL: action`

説明 WebVPN ACL がアクションの実行を開始しました（たとえば解析の開始）。

推奨アクション 不要。

716009

エラーメッセージ `%Threat Defense-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.`

説明 関連する ACL が解析していないため、このグループ内の指定されたユーザーの WebVPN セッションが許可されません。このエラーが修正されるまで、ユーザーが WebVPN を介してログインすることは許可されません。

推奨アクション WebVPN ACL を修正します。

716010

エラーメッセージ `%Threat Defense-7-716010: Group group User user Browse network.`

説明 指摘されたグループ内の WebVPN ユーザーがネットワークをブラウズしました。

推奨アクション 不要。

716011

エラーメッセージ `%Threat Defense-7-716011: Group group User user Browse domain domain .`

説明 このグループ内の指摘された WebVPN ユーザーが、指摘されたドメインをブラウズしました。

推奨アクション 不要。

716012

エラーメッセージ `%Threat Defense-7-716012: Group group User user Browse directory directory .`

説明指摘された WebVPN ユーザーが、指摘されたディレクトリをブラウズしました。

推奨アクション 不要。

716013

エラーメッセージ `%Threat Defense-7-716013: Group group User user Close file filename .`

説明指摘された WebVPN ユーザーが、指摘されたファイルを閉じました。

推奨アクション 不要。

716014

エラーメッセージ `%Threat Defense-7-716014: Group group User user View file filename .`

説明指摘された WebVPN ユーザーが、指摘されたファイルを参照しました。

推奨アクション 不要。

716015

エラーメッセージ `%Threat Defense-7-716015: Group group User user Remove file filename .`

説明指摘されたグループ内の WebVPN ユーザーが、指摘されたファイルを削除しました。

推奨アクション 不要。

716016

エラーメッセージ `%Threat Defense-7-716016: Group group User user Rename file old_filename to new_filename .`

説明指摘された WebVPN ユーザーが、指摘されたファイルの名前を変更しました。

推奨アクション 不要。

716017

エラーメッセージ `%Threat Defense-7-716017: Group group User user Modify file filename .`

説明指摘された WebVPN ユーザーが、指摘されたファイルを修正しました。

推奨アクション 不要。

716018

エラーメッセージ %Threat Defense-7-716018: Group *group* User *user* Create file *filename* .

説明 指摘された WebVPN ユーザーが、指摘されたファイルを作成しました。

推奨アクション 不要。

716019

エラーメッセージ %Threat Defense-7-716019: Group *group* User *user* Create directory *directory* .

説明 指摘された WebVPN ユーザーが、指摘されたディレクトリを作成しました。

推奨アクション 不要。

716020

エラーメッセージ %Threat Defense-7-716020: Group *group* User *user* Remove directory *directory* .

説明 指摘された WebVPN ユーザーが、指摘されたディレクトリを削除しました。

推奨アクション 不要。

716021

エラーメッセージ %Threat Defense-7-716021: File access DENIED, *filename* .

説明 指摘された WebVPN ユーザーが、指摘されたファイルへのアクセスを拒否されました。

推奨アクション 不要。

716022

エラーメッセージ %Threat Defense-4-716022: Unable to connect to proxy server *reason* .

説明 WebVPN HTTP/HTTPS のリダイレクトが、指摘された理由で失敗しました。

推奨アクション HTTP/HTTPS プロキシ コンフィギュレーションを確認します。

716023

エラーメッセージ %Threat Defense-4-716023: Group *name* User *user* Session could not be established: session limit of *maximum_sessions* reached.

説明 現在のセッション数が最大セッション ロードを超過しているため、ユーザー セッションを確立できません。

推奨アクション可能であれば、設定されている制限を増加し、ロード バランス クラスタを増やします。

716024

エラーメッセージ%Threat Defense-7-716024: Group *name* User *user* Unable to browse the network.Error: *description*

説明説明が示しているように、ユーザーはCIFSプロトコルを使用してWindowsネットワークをブラウズできませんでした。たとえば、"Unable to contact necessary server"は、リモートサーバーが使用不可または到達不能であることを示しています。これは、一時的な状態である場合もありますし、さらにトラブルシューティングが必要な場合もあります。

推奨アクション WebVPNデバイスと、CIFSプロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defenseデバイス でNetBIOSネーム サーバーのコンフィギュレーションを確認します。

716025

エラーメッセージ%Threat Defense-7-716025: Group *name* User *user* Unable to browse domain *domain* . Error: *description*

説明ユーザーがCIFSプロトコルを使用してリモート ドメインをブラウズできませんでした。

推奨アクション WebVPNデバイスと、CIFSプロトコルでアクセスするサーバーとの間の接続を確認します。Secure Firewall Threat Defenseデバイス でNetBIOSネーム サーバーのコンフィギュレーションを確認します。

716026

エラーメッセージ%Threat Defense-7-716026: Group *name* User *user* Unable to browse directory *directory* . Error: *description*

説明ユーザーがCIFSプロトコルを使用してリモート ディレクトリをブラウズできませんでした。

推奨アクション WebVPNデバイスと、CIFSプロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defenseデバイス でNetBIOSネーム サーバーのコンフィギュレーションを確認します。

716027

エラーメッセージ%Threat Defense-7-716027: Group *name* User *user* Unable to view file *filename* . Error: *description*

説明ユーザーがCIFSプロトコルを使用してリモート ファイルを表示できませんでした。

推奨アクション WebVPN デバイスと、CIFS プロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defense デバイス で NetBIOS ネーム サーバーのコンフィギュレーションを確認します。

716028

エラーメッセージ `%Threat Defense-7-716028: Group name User user Unable to remove file filename . Error: description`

説明 ユーザーが CIFS プロトコルを使用してリモート ファイルを削除できませんでした。ファイルのアクセス権の不足が原因と考えられます。

推奨アクション WebVPN デバイスと、CIFS プロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defense デバイス 上の NetBIOS ネーム サーバーのコンフィギュレーションとファイルのアクセス権を確認します。

716029

エラーメッセージ `%Threat Defense-7-716029: Group name User user Unable to rename file filename . Error: description`

説明 ユーザーが CIFS プロトコルを使用してリモート ファイルの名前を変更できませんでした。ファイルのアクセス権の不足が原因と考えられます。

推奨アクション WebVPN デバイスと、CIFS プロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defense デバイス 上の NetBIOS ネーム サーバーのコンフィギュレーションとファイルのアクセス権を確認します。

716030

エラーメッセージ `%Threat Defense-7-716030: Group name User user Unable to modify file filename . Error: description`

説明 ユーザーが CIFS プロトコルを使用して既存のファイルを変更しようとしたときに、問題が発生しました。ファイルのアクセス権の不足が原因と考えられます。

推奨アクション WebVPN デバイスと、CIFS プロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defense デバイス 上の NetBIOS ネーム サーバーのコンフィギュレーションとファイルのアクセス権を確認します。

716031

エラーメッセージ `%Threat Defense-7-716031: Group name User user Unable to create file filename . Error: description`

説明 ユーザーが CIFS プロトコルを使用してファイルを作成しようとしたときに、問題が発生しました。ファイルのアクセス権の問題が原因と考えられます。

推奨アクション WebVPN デバイスと、CIFS プロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defense デバイス 上の NetBIOS ネーム サーバーのコンフィギュレーションとファイルのアクセス権を確認します。

716032

エラーメッセージ `%Threat Defense-7-716032: Group name User user Unable to create folder folder . Error: description`

説明ユーザーが CIFS プロトコルを使用してフォルダを作成しようとしたときに、問題が発生しました。ファイルのアクセス権の問題が原因と考えられます。

推奨アクション WebVPN デバイスと、CIFS プロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defense デバイス 上の NetBIOS ネーム サーバーのコンフィギュレーションとファイルのアクセス権を確認します。

716033

エラーメッセージ `%Threat Defense-7-716033: Group name User user Unable to remove folder folder . Error: description`

説明CIFS プロトコルのユーザーがフォルダを削除しようとしたときに、問題が発生しました。このエラーは、アクセス権の問題またはファイルが存在するサーバーとの通信の問題が原因で発生した可能性があります。

推奨アクション WebVPN デバイスと、CIFS プロトコルでアクセスするサーバーとの間の接続を確認します。また、Secure Firewall Threat Defense デバイス で NetBIOS ネーム サーバーのコンフィギュレーションを確認します。

716034

エラーメッセージ `%Threat Defense-7-716034: Group name User user Unable to write to file filename .`

説明ユーザーが CIFS プロトコルを使用してファイルに書き込もうとしたときに、問題が発生しました。このエラーは、アクセス権の問題またはファイルが存在するサーバーとの通信の問題が原因で発生した可能性があります。

推奨アクション 不要。

716035

エラーメッセージ `%Threat Defense-7-716035: Group name User user Unable to read file filename .`

説明CIFS プロトコルのユーザーがファイルを読み取ろうとしたときに、問題が発生しました。ファイルのアクセス権の問題が原因と考えられます。

推奨アクション ファイルのアクセス権を確認します。

716036

エラーメッセージ `%Threat Defense-7-716036: Group name User user File Access: User user logged into the server server.`

説明ユーザーが CIFS プロトコルを使用してサーバーに正常にログインしました。

推奨アクション 不要。

716037

エラーメッセージ `%Threat Defense-7-716037: Group name User user File Access: User user failed to login into the server server.`

説明ユーザーが CIFS プロトコルを使用してサーバーにログインしようとしましたが、失敗しました。

推奨アクション ユーザーが正しいユーザー名とパスワードを入力したことを確認します。

716038

エラーメッセージ `%Threat Defense-6-716038: Group group User user IP ip Authentication: successful, Session Type: WebVPN.`

説明 WebVPN セッションを開始するには、まずユーザーがローカル サーバーまたはリモート サーバーによって正常に認証される必要があります（たとえば、RADIUS または TACACS+）。

推奨アクション 不要。

716039

エラーメッセージ `%Threat Defense-6-716039: Authentication: rejected, group = name user = user , Session Type: %s`

説明 WebVPN セッションを開始するには、まずユーザーがローカル サーバーまたはリモート サーバーによって正常に認証される必要があります（たとえば、RADIUS または TACACS+）。この場合、ユーザー クレデンシャル（ユーザー名とパスワード）が一致しないか、ユーザーに WebVPN セッションを開始する許可がありません。ユーザー名は無効な場合や不明な場合は表示されませんが、有効な場合または **no logging hide username** コマンドが設定されている場合は表示されます。

- **%s**：セッション タイプ（WebVPN または管理）

推奨アクション ローカルまたはリモート サーバーのユーザー クレデンシャルと、そのユーザーに対して WebVPN が設定されていることを確認します。

716040

エラーメッセージ `%Threat Defense-6-716040: Reboot pending, new sessions disabled. Denied user login.`

説明Secure Firewall Threat Defense デバイス がリブート処理中のため、ユーザーが WebVPN にログインできません。

- **user**：セッション ユーザー

推奨アクション 不要。

716041

エラーメッセージ `%Threat Defense-6-716041: access-list acl_ID action url url hit_cnt count`

説明 acl_ID の WebVPN URL で、位置 **url** に対して **count** 回のヒットがありました。**action** は permitted または denied です。

- **acl_ID**：WebVPN URL ACL
- *count*：URL がアクセスされた回数
- *url*：アクセスされた URL
- *action*：ユーザー アクション

推奨アクション 不要。

716042

エラーメッセージ `%Threat Defense-6-716042: access-list acl_ID action tcp source_interface /source_address (source_port ) - dest_interface /dest_address (dest_port ) hit-cnt count`

説明 acl_ID の WebVPN TCP で、送信元インターフェイス **source_interface**/**source_address** および送信元ポート **source_port** で受信され、**dest_interface**/**dest_address** の宛先 **dest_port** に転送されたパケットに対して **count** 回のヒットがありました。**action** は permitted または denied です。

- *count*：ACL がアクセスされた回数
- *source_interface*：送信元インターフェイス
- *source_address*：送信元 IP アドレス
- *source_port*：送信元ポート
- *dest_interface*：宛先インターフェイス
- *dest_address*：宛先 IP アドレス
- *action*：ユーザー アクション

推奨アクション 不要。

716043

エラーメッセージ `%Threat Defense-6-716043 Group group-name , User user-name , IP IP_address : WebVPN Port Forwarding Java applet started. Created new hosts file mappings.`

説明 ユーザーが、WebVPN セッションから TCP ポート転送アプレットを起動しました。

- **group-name**：セッションに関連付けられているグループ名
- **user-name**：セッションに関連付けられているユーザー名
- **IP_address**：セッションに関連付けられている送信元 IP アドレス

推奨アクション 不要。

716044

エラーメッセージ `%Threat Defense-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.`

説明指摘されたパラメータの値が不良です。

- **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
- **param-name**：パラメータの名前
- **param-value**：パラメータの値

推奨アクション 設定を変更し、指定したパラメータを修正します。パラメータが vlan または nac-settings の場合、それが AAA サーバーおよび Secure Firewall Threat Defense デバイス で正しく設定されていることを確認します。

716045

エラーメッセージ `%Threat Defense-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.`

説明指摘されたパラメータ の値が不良です。値は非常に長い可能性があるため、表示されません。

- **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
- **param-name**：パラメータの名前

推奨アクション 設定を変更し、指定したパラメータを修正します。

716046

エラーメッセージ `%Threat Defense-4-716046: Group group-name User user-name IP IP_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.`

説明指定された ACL が Secure Firewall Threat Defense デバイス 上で見つかりませんでした。

- **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
- **access-list-name**：ACL の名前

推奨アクション 設定を変更して、指定したACLを追加するか、またはACLの名前を修正します。

716047

エラーメッセージ `%Threat Defense-4-716047: Group group-name User user-name IP IP_address User ACL access-list-name from AAA ignored, AV-PAIR ACL used instead.`

説明 Cisco AV-PAIR ACL が使用されたため、指摘された ACL が使用されませんでした。

- **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
- **access-list-name**：ACL の名前

推奨アクション 使用する適切な ACL を決定し、設定を修正します。

716048

エラーメッセージ `%Threat Defense-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.`

説明 ACL を解析するための十分なメモリがありませんでした。

- **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 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、その負荷を減らします。

716049

エラーメッセージ `%Threat Defense-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.`

説明クライアントが使用する ACL が空でした。

- **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 使用する正しい ACL を確認し、コンフィギュレーションを変更します。

716050

エラーメッセージ `%Threat Defense-6-716050: Error adding to ACL: ace_command_line`

説明 ACL エントリに構文エラーがありました。

• **ace_command_line**：エラーの原因となっている ACL エントリ

推奨アクション ダウンロード可能な ACL 構成を修正します。

716051

エラーメッセージ `%Threat Defense-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.`

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。

• **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 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、その負荷を減らします。

716052

エラーメッセージ `%Threat Defense-4-716052: Group group-name User user-name IP IP_address Pending session terminated.`

説明ユーザーがログインを完了できず、保留中のセッションが終了しました。これは、接続できない SVC が原因である可能性があります。

• **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 ユーザーの PC で SVC の互換性を確認します。

716053

エラーメッセージ `%FTD-5-716053: SAML Server added: name: name Type: SP`

説明 SAML IDP サーバーエントリが webvpn 構成に追加されました。

• **name**：SAML IDP の entityID

推奨アクション 不要。

716054

エラーメッセージ `%FTD-5-716054: SAML Server deleted: name: name Type: SP`

説明 SAML IDP サーバーエントリが webvpn 構成から削除されました。.

• **name**：SAML IDP の entityID

推奨アクション 不要。

716055

エラーメッセージ `%Threat Defense-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded`

説明 WebVPN ユーザーが SSO サーバーで正常に認証されました。

- **group-name**：グループ名
- **user-name**：ユーザー名
- **IP_address**：サーバーの IP アドレス
- **name**：サーバーの名前
- **type**：サーバーのタイプ（サーバーのタイプは SiteMinder だけです）

推奨アクション 不要。

716056

エラーメッセージ `%Threat Defense-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason`

説明 WebVPN ユーザーが SSO サーバーでの認証に失敗しました。

- **group-name**：グループ名
- **user-name**：ユーザー名
- **IP_address**：サーバーの IP アドレス
- **name**：サーバーの名前
- **type**：サーバーのタイプ（サーバーのタイプは SiteMinder だけです）
- **reason**：認証に失敗した原因

推奨アクション 失敗の原因に応じて、ユーザーまたは Secure Firewall Threat Defense の管理者が問題を修正する必要があります。

716057

エラーメッセージ `%Threat Defense-3-716057: Group group User user IP ip Session terminated, no type license available.`

説明ユーザーが、ライセンスされていないクライアントを使用して Secure Firewall Threat Defense デバイスに接続しようとしました。このメッセージは、一時ライセンスの有効期限が切れた場合にも表示されることがあります。

- *group*：ユーザーのログイン時に適用されたグループ ポリシー
- *user*：ユーザーの名前
- *IP*：ユーザーの IP アドレス
- *type*：要求されたライセンスのタイプ。次のいずれかです。

- AnyConnect Mobile

- LinkSys Phone

- クライアントから要求されたライセンスのタイプ（AnyConnect Mobile または LinkSys Phone 以外の場合）

- Unknown

推奨アクション機能に対応した適切な永久ライセンスを購入してインストールする必要があります。

716058

エラーメッセージ `%Threat Defense-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.`

説明 SSL トンネルが廃棄され、AnyConnect セッションが非アクティブ状態になります。この原因としては、休止ホスト、スタンバイ ホスト、またはネットワーク接続の喪失が考えられます。

- *group*：AnyConnect セッションに関連付けられているトンネル グループの名前
- *user*：セッションに関連付けられているユーザーの名前
- *ip*：セッションの送信元 IP アドレス

推奨アクション 不要。

716059

エラーメッセージ `%Threat Defense-6-716059: Group group User user IP ip AnyConnect session resumed. Connection from ip2 .`

説明 AnyConnect セッションが非アクティブ状態から再開しました。

- *group*：AnyConnect セッションに関連付けられているトンネル グループの名前
- *user*：セッションに関連付けられているユーザーの名前
- *ip*：セッションの送信元 IP アドレス
- *ip2*：セッションが再開されるホストの送信元 IP アドレス

推奨アクション 不要。

716060

エラーメッセージ `%Threat Defense-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection. License limit reached.`

説明 新しい着信 SSL VPN（AnyConnect またはクライアントレス）接続を許可するために、非アクティブ状態の AnyConnect セッションをログアウトしました。

- *group*：AnyConnect セッションに関連付けられているトンネル グループの名前
- *user*：セッションに関連付けられているユーザーの名前
- *ip*：セッションの送信元 IP アドレス

推奨アクション 不要。

716061

エラーメッセージ `%Threat Defense-3-716061: Group DfltGrpPolicy User user IP ip addr IPv6 User Filter tempipv6 configured for AnyConnect. This setting has been deprecated, terminating connection`

説明 IPv6 VPN フィルタは廃止されているため、IPv6 トラフィックのアクセス制御用として統合フィルタの代わりに構成されていると、接続は終了します。

推奨アクション ユーザーの IPv6 トラフィックを制御するために IPv6 エントリを使って統合フィルタを設定します。

716158

エラーメッセージ `%FTD-3-716158: Failed to create SAML logout request, initiated by SP. Reason: reason`

説明 SAML ログアウト要求の作成中にエラーが発生したため、デバイスは SAML IDP にユーザーログアウトを通知できませんでした。原因としては、プロファイルが空である、ログアウトオブジェクトを作成できなかったなどが考えられます。

推奨アクション なし

716159

エラー メッセージ `%FTD-3-716159: Failed to process SAML logout request, initiated by SP. Reason: reason`

説明 IDP によって開始された SAML ログアウト要求の処理中に、デバイスでエラーが発生しました。原因としては、*NameID* が無効である、ログアウトオブジェクトを作成できなかったなどが考えられます。

推奨アクション なし

716160

エラーメッセージ `%FTD-3-716160: Failed to create SAML authentication request. Reason:reason`

説明 SAML 認証要求の作成中にエラーが発生したため、デバイスは SAML IDP でユーザーを認証できませんでした。原因としては、*NameIDPolicy* が無効である、新しいログインインスタンスを作成できなかったなどが考えられます。

推奨アクション なし

716162

エラーメッセージ `%FTD-3-716162: Failed to consume SAML assertion. Reason: reason`

説明 SAML IDP からの認証応答の処理中にデバイスでエラーが発生しました。原因としては、応答またはアサーションが空である、新しいログインインスタンスを作成できなかった、ア

サーションが期限切れまたは無効である、アサーションが空である、発行者が空である、サブジェクトが空である、発行者のコンテンツが空である、*name_id* またはコンテンツが空であるなどが考えられます。

推奨アクション なし

716500

エラーメッセージ `%Threat Defense-2-716500: internal error in: function : Fiber library cannot locate AK47 instance`

説明ファイバ ライブラリがアプリケーション カーネル レイヤ 4 ～ 7 インスタンスを検出できません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716501

エラーメッセージ `%Threat Defense-2-716501: internal error in: function : Fiber library cannot attach AK47 instance`

説明ファイバ ライブラリがアプリケーション カーネル レイヤ 4 ～ 7 インスタンスを接続できません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716502

エラーメッセージ `%Threat Defense-2-716502: internal error in: function : Fiber library cannot allocate default arena`

説明ファイバ ライブラリがデフォルトのアリーナを割り当てることができません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716503

エラーメッセージ `%Threat Defense-2-716503: internal error in: function : Fiber library cannot allocate fiber descriptors pool`

説明ファイバ ライブラリがファイバ記述子プールを割り当てることができません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716504

エラーメッセージ `%Threat Defense-2-716504: internal error in: function : Fiber library cannot allocate fiber stacks pool`

説明ファイバ ライブラリがファイバ スタック プールを割り当てることができません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716505

エラーメッセージ `%Threat Defense-2-716505: internal error in: function : Fiber has joined fiber in unfinished state`

説明ファイバ間の結合が不完全な状態です。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716506

エラーメッセージ `%Threat Defense-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER`

説明内部ファイバ ライブラリが生成されました。

推奨アクション Cisco TAC にお問い合わせください。

716507

エラーメッセージ `%Threat Defense-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating.`

説明 Secure Firewall Threat Defense デバイス で予期しないエラーが発生し、回復されました。

推奨アクション高 CPU 使用率または CPU ホグ状態の有無、およびメモリ リークの可能性を調べます。問題が解決しない場合、Cisco TAC にお問い合わせください。

716508

エラーメッセージ `%Threat Defense-1-716508: internal error in: function : Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating`

説明 ファイバ スケジューラが不良ファイバをスケジュールしているため、終了処理を続行できません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716509

エラーメッセージ `%Threat Defense-1-716509:internal error in: function : Fiber scheduler is scheduling alien fiber. Cannot continue terminating`

説明 ファイバ スケジューラが未知のファイバをスケジュールしているため、終了処理を続行できません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716510

エラーメッセージ `%Threat Defense-1-716510:internal error in: function : Fiber scheduler is scheduling finished fiber. Cannot continue terminating`

説明 ファイバ スケジューラが完了ファイバをスケジュールしているため、終了処理を続行できません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716512

エラーメッセージ `%Threat Defense-2-716512:internal error in: function : Fiber has joined fiber waited upon by someone else`

説明ファイバが、待機者のいるファイバに結合されました。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716513

エラーメッセージ `%Threat Defense-2-716513: internal error in: function : Fiber in callback blocked on other channel`

説明コールバック内のファイバが他のチャネルでブロックされました。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716515

エラーメッセージ `%Threat Defense-2-716515:internal error in: function : OCCAM failed to allocate memory for AK47 instance`

説明 OCCAM が AK47 インスタンス用にメモリを割り当てることができませんでした。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716516

エラーメッセージ `%Threat Defense-1-716516: internal error in: function : OCCAM has corrupted ROL array. Cannot continue terminating`

説明 OCCAM に含まれる ROL 配列が破損しているため、終了処理を続行できません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716517

エラーメッセージ `%Threat Defense-2-716517: internal error in: function : OCCAM cached block has no associated arena`

説明 OCCAM キャッシュ ブロックにアリーナが関連付けられていません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716518

エラーメッセージ `%Threat Defense-2-716518: internal error in: function : OCCAM pool has no associated arena`

説明 OCCAM プールにアリーナが関連付けられていません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716519

エラーメッセージ `%Threat Defense-1-716519: internal error in: function : OCCAM has corrupted pool list. Cannot continue terminating`

説明 OCCAM に含まれるプール リストが破損しているため、終了処理を続行できません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716520

エラーメッセージ `%Threat Defense-2-716520:internal error in: function : OCCAM pool has no block list`

説明 OCCAM プールにブロック リストが含まれていません。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716521

エラーメッセージ `%Threat Defense-2-716521: internal error in: function : OCCAM no realloc allowed in named pool`

説明 OCCAM が名前付きプールでの再割り当てを許可しませんでした。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716522

エラーメッセージ `%Threat Defense-2-716522: internal error in: function : OCCAM corrupted standalone block`

説明 OCCAM に含まれるスタンドアロン ブロックが破損しています。

推奨アクション 問題の原因を特定するには、Cisco TAC に問い合わせてください。

716525

エラーメッセージ `%Threat Defense-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED`

説明内部 SAL エラーが発生しました。

推奨アクション Cisco TAC にお問い合わせください。

716526

エラーメッセージ `%Threat Defense-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL`

説明永久ストレージ サーバー ディレクトリのマウント中に障害が発生しました。

推奨アクション Cisco TAC にお問い合わせください。

716527

エラーメッセージ `%Threat Defense-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAIL`

説明永久ストレージ ファイルのマウント中に障害が発生しました。

推奨アクション Cisco TAC にお問い合わせください。

716528

エラーメッセージ `%Threat Defense-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition`

説明 Secure Firewall Threat Defense デバイス で予期しないエラーが発生し、回復されました。

推奨アクション高 CPU 使用率または CPU ホグ状態の有無、およびメモリ リークの可能性を調べます。問題が解決しない場合、Cisco TAC にお問い合わせください。

716600

エラーメッセージ `%Threat Defense-3-716600: Rejected size-recv KB Hostscan data from IP src-ip . Hostscan results exceed default | configured limit of size-conf KB.`

説明 Hostscan の受信データのサイズが Secure Firewall Threat Defense デバイス に設定された制限を超える場合、データは破棄されます。

- *size-recv*：Hostscan の受信データのサイズ（KB 単位）
- *src-ip*：送信元の IP アドレス
- *default* | *configured*：Hostscan データの制限値をデフォルトとするか、または管理者が設定するかを指定するキーワード
- *size-conf*：Secure Firewall Threat Defense デバイス がクライアントから受け入れる Hostscan データのサイズに対して設定された上限

推奨アクション Secure Firewall Threat Defense デバイスがクライアントから受け入れる Hostscan データのサイズの上限を引き上げるには、Cisco TAC にお問い合わせください。

716601

エラーメッセージ `%Threat Defense-3-716601: Rejected size-recv KB Hostscan data from IP src-ip . System-wide limit on the amount of Hostscan data stored on FTD exceeds the limit of data-max KB.`

説明 Secure Firewall Threat Defense デバイスに保存された Hostscan データの量が制限を超えると、Hostscan の新しい結果は拒否されます。

- *size-recv*：Hostscan の受信データのサイズ（KB 単位）
- *src-ip*：送信元の IP アドレス
- *data-max*：Secure Firewall Threat Defense デバイスによって保存される Hostscan 結果の量に対する制限（KB 単位）

推奨アクション Hostscan の保存データの制限を変更する場合は、Cisco TAC に連絡してください。

716602

エラーメッセージ `%Threat Defense-3-716602: Memory allocation error. Rejected size-recv KB Hostscan data from IP src-ip .`

説明メモリを Hostscan データに割り当てている最中にエラーが発生しました。

- *size-recv*：Hostscan の受信データのサイズ（KB 単位）
- *src-ip*：送信元の IP アドレス

推奨アクション設定されている場合、Hostscanの制限をデフォルト値に設定します。問題が解決しない場合は、TAC にご連絡ください。

716603

エラーメッセージ `%Threat Defense-7-716603: Received size-recv KB Hostscan data from IP src-ip .`

説明指定したサイズの Hostscan データが正常に受信されました。

- *size-recv*：Hostscan の受信データのサイズ（KB 単位）
- *src-ip*：送信元の IP アドレス

推奨アクション 不要。

メッセージ 717001 ～ 717064

この項では、717001 から 717064 までのメッセージについて説明します。

717001

エラーメッセージ `%Threat Defense-3-717001: Querying keypair failed.`

説明登録要求中に必要なキーペアが見つかりませんでした。

推奨アクショントラストポイントのコンフィギュレーションに有効なキーペアがあることを確認して、登録要求を再送信します。

717002

エラーメッセージ `%Threat Defense-3-717002: Certificate enrollment failed for trustpoint` *`trustpoint_name`*`. Reason:` *`reason_string`* `.`

説明このトラストポイントの登録要求が失敗しました。

- *trustpoint name*：登録要求の対象となったトラストポイント名
- *reason_string*：登録要求が失敗した理由

推奨アクション 失敗した理由については、CA サーバーを確認します。

717003

エラーメッセージ `%Threat Defense-6-717003: Certificate received from Certificate Authority for trustpoint` *`trustpoint_name`* `.`

説明このトラストポイントに対して CA から証明書を正常に受信しました。

- *trustpoint_name* ：トラストポイント名

推奨アクション 不要。

717004

エラーメッセージ `%Threat Defense-6-717004: PKCS #12 export failed for trustpoint` *`trustpoint_name`* `.`

説明 CA 証明書だけが存在しトラストポイントのアイデンティティ証明書が存在しない、または必要なキーペアが欠落しているため、トラストポイントをエクスポートできませんでした。

- *trustpoint_name* ：トラストポイント名

推奨アクション指摘されたトラストポイントに対して必要な証明書とキーペアがあることを確認します。

717005

エラーメッセージ `%Threat Defense-6-717005: PKCS #12 export succeeded for trustpoint` *`trustpoint_name`* `.`

説明トラストポイントが正常にエクスポートされました。

• *trustpoint_name* ：トラストポイント名

推奨アクション 不要。

717006

エラーメッセージ `%Threat Defense-6-717006: PKCS #12 import failed for trustpoint trustpoint_name .`

説明要求されたトラストポイントのインポートを処理できませんでした。

• *trustpoint_name* ：トラストポイント名

推奨アクション インポートしたデータの整合性を確認します。その後、pkcs12 レコード全体が正しく貼り付けられていることを確認し、データを再インポートします。

717007

エラーメッセージ `%Threat Defense-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name .`

説明要求したトラストポイントのインポートが正常に完了しました。

• *trustpoint_name* ：トラストポイント名

推奨アクション 不要。

717008

エラーメッセージ `%Threat Defense-2-717008: Insufficient memory to process_requiring_memory.`

説明メモリを必要とするプロセスのメモリ割り当てを試行中に内部エラーが発生しました。メモリの割り当て中にその他のプロセスで問題が発生し、以降の処理が妨げられる可能性があります。

• **process_requiring_memory**：メモリを必要とする指摘されたプロセス

推奨アクション さらにデバッグするためにメモリ統計およびログを収集し、Secure Firewall Threat Defense デバイス をリロードします。

717009

エラーメッセージ `%Threat Defense-3-717009: Certificate validation failed. Reason: reason_string .`

説明証明書の検証が失敗しました。これは、無効になった証明書の検証試行、無効な証明書属性、またはコンフィギュレーションの問題が原因である可能性があります。

• *reason_string*：証明書の検証が失敗した理由

推奨アクション適切なトラストポイントが見つからなかったことが理由で表示された場合は、コンフィギュレーションで検証のため有効なトラストポイントが設定されていることを確認します。Secure Firewall Threat Defense デバイス の時刻が認証局の時刻に対して正確であることを確認します。障害の原因を確認し、示された問題を訂正します。CA キーサイズが小さすぎるか、弱い暗号が使用されているために証明書の検証が失敗した場合、を使用して Management Center でデバイスの弱い暗号オプションを有効にし、これらの制限を無効にすることができます。

717010

エラーメッセージ `%Threat Defense-3-717010: CRL polling failed for trustpoint trustpoint_name .`

説明証明書失効リスト（CRL）ポーリングが失敗しました。CRL チェックが必要な場合は、これによって接続が拒否される可能性があります。

- **trustpoint_name**：CRL を要求したトラストポイントの名前

推奨アクション 設定された CRL 配布ポイントとの間に接続が存在することを確認し、手動の CRL 検索が正しく機能することを確認します。

717011

エラーメッセージ `%Threat Defense-2-717011: Unexpected event event event_ID`

説明通常の条件では予期されないイベントが発生しました。

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。

717012

エラーメッセージ `%Threat Defense-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure`

説明指摘されたトラストポイントに対するキャッシュされた CRL エントリのリフレッシュ試行が、示された失敗回数だけ失敗しました。これによって、Secure Firewall Threat Defense デバイス 上に古い CRL が生じ、有効な CRL を必要とする接続が拒否される可能性があります。

- **trustpoint_name**：トラストポイントの名前
- *time_of_failure*：障害発生時刻

推奨アクションネットワークまたはサーバーのダウンなど、サーバーとの接続上の問題を確認します。**crypto ca crl retrieve** コマンドを使用して、CRL を手動で取得します。

717013

エラーメッセージ `%Threat Defense-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer`

説明デジタル証明書を使用して IPSec トンネルを認証するようにデバイスが設定されている場合は、接続のたびに CRL をダウンロードせずに済むように、CRL がメモリにキャッシュされる可能性があります。キャッシュがいっぱいになって着信 CRL を受け入れられなくなった場合は、必要なスペースが使用可能になるまで古い CRL が削除されていきます。このメッセージは、パージされる各 CRL に対して生成されます。

- **issuer**：キャッシュされた CRL を削除するデバイスの名前

推奨アクション 不要。

717014

エラーメッセージ `%Threat Defense-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size , available cache space = space )`

説明デジタル証明書を使用して IPSec トンネルを認証するようにデバイスが設定されている場合は、接続のたびに CRL をダウンロードせずに済むように、CRL がメモリにキャッシュされる可能性があります。このメッセージは、受信した CRL が大きすぎてキャッシュに収まらない場合に生成されます。大きいCRLはキャッシュされませんが、引き続きサポートされます。これは、各 IPSec 接続で CRL がダウンロードされることを意味します。IPSec 接続のバースト時にパフォーマンスに影響する可能性があります。

推奨アクション 不要。

717015

エラーメッセージ `%Threat Defense-3-717015: CRL received from issuer is too large to process (CRL size = crl_size , maximum CRL size = max_crl_size )`

説明 IPSec 接続によって、許可された最大 CRL サイズよりも大きい CRL がダウンロードされました。このエラーにより、接続の失敗が発生します。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

推奨アクション CRL 方式の失効チェックでは、拡張性が最も重大な欠点となる可能性があります。この問題を解決する方法には、CA のソリューションを調査して CRL のサイズを小さくすること、または CRL 検証を必要としない Secure Firewall Threat Defense デバイス を設定することがあります。

717016

エラーメッセージ `%Threat Defense-6-717016 : Removing expired CRL from the CRL cache. Issuer: issuer`

説明デジタル証明書を使用して IPSec トンネルを認証するように Secure Firewall Threat Defense デバイスが設定されている場合は、接続のたびにCRLをダウンロードせずに済むように、CRL がメモリにキャッシュされる可能性があります。このメッセージは、CA が指定した有効期限または設定されたキャッシュ時間が経過し、CRLがキャッシュから削除された場合に生成されます。

推奨アクション 不要。

717017

エラーメッセージ `%Threat Defense-3-717017: Failed to query CA certificate for trustpoint` *`trustpoint_name`* `from` *`enrollment_url`*

説明 認証局からの CA 証明書を要求することによってトラストポイントを認証しようとしたときにエラーが発生しました。

推奨アクション このトラストポイントで登録 URL が設定されていることを確認し、CA サーバーとの接続を確認して、要求を再試行します。

717018

エラーメッセージ `%Threat Defense-3-717018: CRL received from` *`issuer`* `has too many entries to process (number of entries =` *`number_of_entries`* `, maximum number allowed =` *`max_allowed`* `)`

説明 IPSec 接続によって、サポートできる数より多くの失効エントリを含む CRL がダウンロードされました。これは、接続の失敗を引き起こすエラー状態です。このメッセージは、10 秒に 1 回しか表示されないように制限されています。

- **issuer**：CRL 発行者の X.500 名
- **number_of_entries**：受信した CRL 内の失効エントリの数
- **max_allowed**：Secure Firewall Threat Defense デバイス がサポートする CRL エントリの最大数

推奨アクション CRL 方式の失効チェックでは、拡張性が最も重大な欠点となる可能性があります。この問題を解決する方法には、CA のソリューションを調査して CRL のサイズを小さくすること、または CRL 検証を必要としない Secure Firewall Threat Defense デバイス を設定することがあります。

717019

エラーメッセージ `%Threat Defense-3-717019 : Failed to insert CRL for trustpoint` *`trustpoint_name`* `. Reason:` *`failure_reason`* `.`

説明 CRL が取得されたが、無効であり、**failure_reason** のためキャッシュに挿入できません。

- **trustpoint_name**：CRL を要求したトラストポイントの名前
- **failure_reason**：CRL をキャッシュに挿入できなかった理由

推奨アクション Secure Firewall Threat Defense デバイス の現在の時刻が CA の時刻に対して正確であることを確認します。NextUpdate フィールドがない場合は、NextUpdate フィールドを無視するようにトラストポイントを設定します。

717020

エラーメッセージ `%Threat Defense-3-717020: Failed to install device certificate for trustpoint label . Reason: reason string .`

説明登録対象の証明書をトラストポイントに登録またはインポートしようとしているときに、障害が発生しました。

- *label*：登録対象の Secure Firewall Threat Defense 証明書をインストールできなかったトラストポイントのラベル
- *reason_string*：証明書を検証できない理由

推奨アクション障害の理由を参照して障害の原因を取り除き、登録を再試行します。一般的な障害は、無効な証明書が Secure Firewall Threat Defense デバイスにインポートされているため、または登録対象の証明書に含まれている公開キーとトラストポイントで参照されるキーペアとのミスマッチのために発生します。

717021

エラーメッセージ `%Threat Defense-3-717021: Certificate data could not be verified. Locate Reason: reason_string serial number: serial number , subject name: subject name , key length key length bits.`

説明シリアル番号とサブジェクト名で示された証明書を検証しようとしましたが、指摘された理由によって失敗しました。シグニチャを使用して証明書データを検証すると、無効なキータイプやサポートされないキーサイズなど、ログに記録されるいくつかのエラーが発生する可能性があります。

- *reason_string*：証明書を検証できない理由
- *serial number*：検証中の証明書のシリアル番号
- *subject name*：検証中の証明書に含まれるサブジェクト名
- *key length*：この証明書に署名するために使用されるキー内のビット数

推奨アクション 指摘された証明書を調べて、有効であること、有効なキー タイプが含まれていること、サポートされる最大キー サイズを超過していないことを確認します。

717022

エラーメッセージ `%Threat Defense-6-717022: Certificate was successfully validated. certificate_identifiers`

説明識別された証明書が正常に検証されました。

- *certificate_identifiers*：正常に検証された証明書を識別する情報。これには、理由、シリアル番号、サブジェクト名、および追加情報が含まれます。

推奨アクション 不要。

717023

エラーメッセージ `%Threat Defense-3-717023: SSL failed to set device certificate for trustpoint trustpoint name . Reason: reason_string .`

説明 SSL 接続の認証のため所定のトラストポイントで Secure Firewall Threat Defense 証明書を設定しようとして失敗しました。

- *trustpoint name*：SSL が Secure Firewall Threat Defense 証明書を設定できなかったトラストポイントの名前
- *reason_string*：Secure Firewall Threat Defense 証明書を設定できない理由

推奨アクション 失敗について報告された理由で示された問題を次のように解決します。

- 指摘されたトラストポイントが登録されており、Secure Firewall Threat Defense 証明書を持っていることを確認します。
- Secure Firewall Threat Defense 証明書が有効であることを確認します。
- 必要な場合は、トラストポイントを再登録します。

717024

エラーメッセージ `%Threat Defense-7-717024: Checking CRL from trustpoint: trustpoint name for purpose`

説明 CRL が取得されています。

- *trustpoint name*：CRL が取得されているトラストポイントの名前
- *purpose*：CRL が取得されている理由

推奨アクション 不要。

717025

エラーメッセージ `%Threat Defense-7-717025: Validating certificate chain containing number of certs certificate(s).`

説明証明書チェーンが検証されています。

- >*number of certs*：チェーン内の証明書の数

推奨アクション 不要。

717026

エラーメッセージ `%Threat Defense-4-717026: Name lookup failed for hostname hostname during PKI operation.`

説明 PKI オペレーションの試行中に所定のホスト名を解決できません。

- >*hostname*：解決できなかったホスト名

推奨アクション 指摘されたホスト名のコンフィギュレーションおよびDNSサーバー エントリを調べて、解決できることを確認します。それから、オペレーションを再試行します。

717027

エラーメッセージ `%Threat Defense-3-717027: Certificate chain failed validation. reason_string .`

説明証明書チェーンを検証できません。

- *reason_string*：証明書チェーンを検証できなかった理由ありうる理由は、CAサーバーに到達できない、トラストポイントが利用できない、証明書アイデンティティの有効期間が切れた、証明書が失効したなどです。

推奨アクション理由に示された問題を解決し、次の処置のいずれかを実行して検証を再試行します。

- CRL チェックが必要な場合は CA への接続が存在することを確認します。
- トラストポイントが認証されており、検証に使用できることを確認します。
- チェーン内の ID 証明書が有効日に基づいて有効であることを確認します。
- 証明書が失効していないことを確認します。

717028

エラーメッセージ `%Threat Defense-6-717028: Certificate chain was successfully validated additional info .`

説明証明書チェーンが正常に検証されました。

- >*additional info*：証明書チェーンがどのように検証されたかを示す追加情報（CRL チェックが実行されなかったことを示す「with warning」など）

推奨アクション 不要。

717029

エラーメッセージ `%Threat Defense-7-717029: Identified client certificate within certificate chain. serial number: serial_number , subject name: subject_name .`

説明クライアント証明書として指定されている証明書が識別されます。

- **serial_number**：クライアント証明書として識別される証明書のシリアル番号
- **subject_name**：クライアント証明書として識別される証明書に含まれるサブジェクト名

推奨アクション 不要。

717030

エラーメッセージ `%Threat Defense-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.`

説明証明書の検証に使用できる適切または使用可能なトラストポイントが見つかりました。

- *trustpoint name*：証明書の検証に使用されるトラストポイント

推奨アクション 不要。

717031

エラーメッセージ `%Threat Defense-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string`

説明使用可能なトラストポイントが見つかりません。証明書の検証中は、証明書を検証するために適切なトラストポイントが使用可能になっている必要があります。

- >*issuer*：検証されていた証明書の発行者
- *reason_string*：適切なトラストポイントが見つからない理由

推奨アクションコンフィギュレーションを調べてトラストポイントが設定、認証、および登録されていることを確認し、理由に示された問題を解決します。また、コンフィギュレーションが、ID 証明書など、特定のタイプの証明書を許可していることを確認します。

717032

エラーメッセージ `%Threat Defense-3-717032: OCSP status check failed. Reason: reason_string`

説明OCSP ステータスチェックが失敗すると、このメッセージが失敗の理由とともに生成されます。次のリストは失敗の理由です。

- OCSP 要求の HTTP トランザクションが失敗しました。
- 無効な OCSP 応答ステータス「無許可」です。
- OCSP 応答処理に失敗しました。
- サーバーからの OCSP 応答のクエリに失敗しました
- サーバーからの HTTP OCSP 応答の解析に失敗しました
- 無効な失効ステータス、サーバーが返したステータス：不明
- 無効な OCSP 応答タイプです
- OCSP 応答にナンスがありません
- ナンスの不一致
- OCSP 応答の検証に失敗しました
- OCSP 応答の有効期限が無効です
- Certificate is revoked
- OCSP レスポンダー証明書の CRL チェックに失敗しました

推奨アクションなし。

717033

エラーメッセージ `%Threat Defense-6-717033: OCSP response status - Successful.`

説明 OCSP のステータス チェック応答が正常に受信されました。

推奨アクション 不要。

717034

エラーメッセージ `%Threat Defense-7-717034: No-check extension found in certificate. OCSP check bypassed.`

説明 「id-pkix-ocsp-nocheck」拡張を含む OCSP 応答側証明書が受信されました。これにより、OCSP ステータス チェックなしでこの証明書を検証できます。

推奨アクション 不要。

717035

エラーメッセージ `%Threat Defense-4-717035: OCSP status is being checked for certificate. certificate_identifier.`

説明 OCSP ステータス チェックが実行される証明書が識別されます。

- *certificate_identifier*：証明書マップ規則によって処理されている証明書を識別する情報

推奨アクション 不要。

717036

エラーメッセージ `%Threat Defense-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.`

説明証明書 ID によって識別されるピアの証明書は、可能なトンネル グループの一致を試みるために、設定された証明書マップによって処理されています。

- *certificate_identifier*：証明書マップ規則によって処理されている証明書を識別する情報

推奨アクション 不要。

717037

エラーメッセージ `%Threat Defense-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier .`

説明証明書 ID によって識別されるピアの証明書は、可能なトンネル グループの一致を試みるために、設定された証明書マップによって処理されましたが、一致が見つかりませんでした。

• *certificate_identifier*：証明書マップ規則によって処理されている証明書を識別する情報

推奨アクション 受信したピア証明書および設定済みの暗号化 CA 証明書マップ規則に基づいて、この警告が予期されたものであることを確認します。

717038

エラーメッセージ `%Threat Defense-7-717038: Tunnel group match found. Tunnel Group: tunnel_group_name , Peer certificate: certificate_identifier .`

説明証明書 ID によって識別されるピアの証明書は、設定された証明書マップによって処理され、トンネル グループへの一致が見つかりました。

• *certificate_identifier*：証明書マップ規則によって処理されている証明書を識別する情報
• *tunnel_group_name*：証明書マップ規則で一致したトンネル グループの名前

推奨アクション 不要。

717050

エラーメッセージ `%Threat Defense-5-717050: SCEP Proxy: Processed request type type from IP client ip address , User username , TunnelGroup tunnel_group name , GroupPolicy group-policy name to CA IP ca ip address`

説明 SCEP プロキシはメッセージを受信し、CA に中継しました。CA からの応答はクライアントに中継されます。

• *type*：SCEP プロキシが受信した要求タイプ文字列。PKIOperation、GetCACaps、GetCACert、GetNextCACert および GetCACertChain のいずれかの SCEP メッセージ タイプになります。
• *client ip address*：受信した要求の送信元 IP アドレス
• *username*：SCEP 要求を受信した VPN セッションに関連付けられたユーザー名
• *tunnel-group name*：SCEP 要求を受信した VPN セッションに関連付けられたトンネル グループ
• *group-policy name*：SCEP 要求を受信した VPN セッションに関連付けられたグループ ポリシー
• *ca ip address*：グループ ポリシーで設定されている CA の IP アドレス

推奨アクション 不要。

717051

エラーメッセージ `%Threat Defense-3-717051: SCEP Proxy: Denied processing the request type type received from IP client ip address , User username , TunnelGroup tunnel group name , GroupPolicy group policy name to CA ca ip address . Reason: msg`

説明 SCEP プロキシは要求の処理を拒否しました。これは、設定ミス、プロキシのエラー状態、または無効な要求によって発生する可能性があります。

- *type*：SCEP プロキシが受信した要求タイプ文字列。PKIOperation、GetCACaps、GetCACert、GetNextCACert および GetCACertChain のいずれかの SCEP メッセージ タイプになります。
- *client ip address*：受信した要求の送信元 IP アドレス
- *username*：SCEP 要求を受信した VPN セッションに関連付けられたユーザー名
- *tunnel-group name*：SCEP 要求を受信した VPN セッションに関連付けられたトンネル グループ
- *group-policy name*：SCEP 要求を受信した VPN セッションに関連付けられたグループ ポリシー
- *ca ip address*：グループ ポリシーで設定されている CA の IP アドレス
- **msg**：要求の処理が拒否された理由またはエラーを示す原因文字列

推奨アクション出力された理由から原因を特定します。理由として要求が無効であることが表示されている場合、CA URL の設定を確認します。そうでない場合は、トンネル グループで SCEP の登録がイネーブルになっていることを確認し、**debug crypto ca scep-proxy** コマンドを使用してさらにデバッグします。

717052

エラーメッセージ `%Threat Defense-4-717052: Group group name User user name IP IP Address Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number`

説明定期的な証明書認証が失敗し、セッションが切断されました。

- *group name*：セッションが属するグループ ポリシーの名前
- *user name*：セッションのユーザー名
- *IP*：セッションのパブリック IP アドレス
- *id subject name*：セッションの ID 証明書の件名
- *id issuer name*：セッションの ID 証明書の発行者名
- *id serial number*：セッションの ID 証明書のシリアル番号

推奨アクション 不要。

717053

SSP 全体のトピック

エラーメッセージ `%Threat Defense-5-717053: Group group name User user name IP IP Address Periodic certificate authentication succeeded. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number`

説明定期的な証明書認証に成功しました。

- *group name*：セッションが属するグループ ポリシーの名前
- *user name*：セッションのユーザー名
- *id subject name*：セッションの ID 証明書の件名
- *id issuer name*：セッションの ID 証明書の発行者名

• *id serial number*：セッションの ID 証明書のシリアル番号

推奨アクション 不要。

717054

SSP 全体のトピック

エラーメッセージ `%Threat Defense-1-717054: The type certificate in the trustpoint tp name is due to expire in number days. Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number`

説明トラストポイント内の指定された証明書の有効期限が近づいています。

• *type*：証明書のタイプ（CA または ID）
• *tp name*：証明書が属するトラストポイントの名前
• *number*：有効期限満了までの日数。
• *date and time*：有効期限の日時
• *subject name*：証明書の件名
• *issuer name*：証明書の発行者名
• *serial number*：証明書のシリアル番号

推奨アクション証明書を更新します。

717055

エラーメッセージ `%Threat Defense-1-717055: The type certificate in the trustpoint tp name has expired. Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number`

説明トラストポイント内の指定された証明書の有効期限が切れています。

• *type*：証明書のタイプ（CA または ID）
• *tp name*：証明書が属するトラストポイントの名前
• *date and time*：有効期限の日時
• *subject name*：証明書の件名
• *issuer name*：証明書の発行者名
• *serial number*：証明書のシリアル番号

推奨アクション証明書を更新します。

717056

見出しのタイトル SSP のみ

エラーメッセージ `%Threat Defense-6-717056: Attempting type revocation check from Src Interface :Src IP /Src Port to Dst IP /Dst Port using protocol`

説明 CA が CRL をダウンロードしようとしていたか、OCSP 失効確認要求を送信しようとしていました。

- *type*：失効チェックのタイプ。OCSP または CRL のいずれか
- *Src Interface*：失効チェックを実行するインターフェイスの名前
- *Src IP*：失効チェックを実行する IP アドレス
- *Src Port*：失効チェックを実行するポート番号
- *Dst IP*：失効チェック要求の送信先のサーバーの IP アドレス
- *Dst Port*：失効チェック要求の送信先のサーバーのポート番号
- *Protocol*：失効チェックに使用されるプロトコル。HTTP、LDAP、または SCEP

推奨アクション 不要。

717057

エラーメッセージ `%Threat Defense-3-717057: Automatic import of trustpool certificate bundle has failed. < Maximum retry attempts reached. Failed to reach CA server> | <Cisco root bundle signature validation failed> | <Failed to update trustpool bundle in flash> | <Failed to install trustpool bundle in memory>`

説明 この syslog はこれらのエラー メッセージのいずれかで生成されます。この syslog は、自動インポート操作の結果でユーザーを更新し、特に障害が発生した場合は、適切なデバッグ メッセージへと誘導するためのものです。各エラーの詳細がデバッグ出力に表示されます。

推奨アクション CA のアクセシビリティを確認し、フラッシュ CA ルート証明書にスペースを作ります。

717058

エラーメッセージ `%Threat Defense-6-717058: Automatic import of trustpool certificate bundle is successful: <No change in trustpool bundle> | <Trustpool updated in flash>.`

説明この syslog は、これらの成功メッセージの 1 つで生成されます。この syslog は、自動インポート操作の結果でユーザーを更新し、特に障害が発生した場合は、適切なデバッグ メッセージへと誘導するためのものです。各エラーの詳細がデバッグ出力に表示されます。

推奨アクション なし。

717059

エラーメッセージ `%Threat Defense-6-717059: Peer certificate with serial number: <serial>, subject: <subject_name>, issuer: <issuer_name> matched the configured certificate map <map_name>`

説明このログは、ASDM 接続が証明書を介して認証され、設定された証明書マップ ルールに基づいて許可されている場合に生成されます。

推奨アクション 不要。

717060

エラーメッセージ `%Threat Defense-3-717060: Peer certificate with serial number: <serial>, subject: <subject_name>, issuer: <issuer_name> failed to match the configured certificate map <map_name>`

説明このログは、ASDM 接続が証明書を介して認証され、設定された証明書マップ ルールに基づいて許可されていない場合に生成されます。

推奨アクションログ内で参照されているピア証明書が許可されると思われる場合、参照されている map_name の証明書マップ設定を確認し、必要に応じて、接続を許可するようにマップを修正します。

717061

SSP 専用の見出しタイトル

エラーメッセージ `%Threat Defense-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca_name. Request Type type Mode mode`

説明 CMP 登録要求がトリガーされました。

- *tpname*：登録されているトラストポイントの名前
- *ca*：CMP 設定で指定したとおりの CA ホスト名または IP アドレス
- *type*：CMP 要求タイプ。初期化要求、証明書要求、およびキー更新要求
- *mode*：登録トリガー。Manual または Automatic
- *protocol*：登録プロトコル。CMP

推奨アクション 不要。

717062

エラーメッセージ `%Threat Defense-5-717062: protocol Certificate enrollment succeeded for the trustpoint tpname with the CA ca. Received a new certificate with Subject Name subject Issuer Name issuer Serial Number serial`

説明 CMP 登録要求に成功しました。新しい証明書を受信しました。

- *tpname*：登録されているトラストポイントの名前
- *ca*：CMP 設定で指定したとおりの CA ホスト名または IP アドレス
- *subject*：受信した証明書のサブジェクト名
- *issuer*：受信した証明書の発行者名
- serial：受信した証明書のシリアル番号
- *protocol*：登録プロトコル。CMP

推奨アクション 不要。

717063

SSP 専用の見出しタイトル

エラーメッセージ `%Threat Defense-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca`

説明 CMP 登録要求に失敗しました。

- *tpname*：登録されているトラストポイントの名前
- *ca*：CMP 設定で指定したとおりの CA ホスト名または IP アドレス
- *protocol*：登録プロトコル：CMP

推奨アクション CMP デバッグ トレースを使用して、登録障害を修正します。

717064

SSP 専用の見出し

エラーメッセージ `%Threat Defense-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate renewal`

説明 トラストポイント内のキーペアは、CMP を使用して証明書の登録用に再生成されます。

- *tpname*：登録されるトラストポイントの名前
- *keyname*：トラストポイントのキーペアの名前
- mode：登録トリガー。Manual または Automatic
- *protocol*：登録プロトコル。CMP

推奨アクション 不要。

メッセージ 718001 ～ 719026

この項では、718001 から 719026 までのメッセージについて説明します。

718001

エラーメッセージ `%Threat Defense-7-718001: Internal interprocess communication queue send failure: code error_code`

説明 VPN ロード バランシング キューでメッセージをキューに入れようとしたときに、内部ソフトウェア エラーが発生しました。

推奨アクション 一般的に、これは問題のない状態です。問題が解決しない場合、Cisco TAC にお問い合わせください。

718002

エラーメッセージ `%Threat Defense-5-718002: Create peer IP_address failure, already at maximum of number_of_peers`

説明ロード バランシング ピアの最大数を超過しました。新しいピアは無視されます。

推奨アクション ロード バランシングとネットワーク コンフィギュレーションを調べて、ロード バランシング ピアの数が、許可された最大値を超過していないことを確認します。

718003

エラーメッセージ `%Threat Defense-6-718003: Got unknown peer message message_number from IP_address , local version version_number , remote version version_number`

説明ロード バランシング ピアのいずれかから、認識されないロード バランシング メッセージが受信されました。これは、ピア間のバージョンの不一致を示している可能性がありますが、内部ソフトウェア エラーが原因となっていると思われます。

推奨アクション すべてのロード バランシング ピアに互換性があることを確認します。互換性があり、この状態が続く場合、または望ましくない動作が引き起こされる場合は、Cisco TAC にお問い合わせください。

718004

エラーメッセージ `%Threat Defense-6-718004: Got unknown internal message message_number`

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 一般的に、これは問題のない状態です。問題が解決しない場合、Cisco TAC にお問い合わせください。

718005

エラーメッセージ `%Threat Defense-5-718005: Fail to send to IP_address , port port`

説明ロード バランシング ソケットでのパケットの送信中に、内部ソフトウェア エラーが発生しました。これはネットワークの問題を示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 でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718006

エラーメッセージ `%Threat Defense-5-718006: Invalid load balancing state transition [cur=state_number ][event=event_number ]`

説明ステート マシン エラーが発生しました。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション一般的に、これは問題のない状態です。問題が解決しない場合、Cisco TAC にお問い合わせください。

718007

エラーメッセージ `%Threat Defense-5-718007: Socket open failure [failure_code]:failure_text`

説明ロード バランシング ソケットを開こうとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェアエラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718008

エラーメッセージ `%Threat Defense-5-718008: Socket bind failure [failure_code]:failure_text`

説明 Secure Firewall Threat Defense デバイス がロード バランシング ソケットにバインドしようとしたときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェアエラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718009

エラーメッセージ `%Threat Defense-5-718009: Send HELLO response failure to IP_address`

説明 Secure Firewall Threat Defense デバイス がロード バランシング ピアの 1 つに Hello Response メッセージを送信しようとしたときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718010

エラーメッセージ `%Threat Defense-5-718010: Sent HELLO response to IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアに Hello Response メッセージを送信しました。

推奨アクション 不要。

718011

エラーメッセージ `%Threat Defense-5-718011: Send HELLO request failure to IP_address`

説明 Secure Firewall Threat Defense デバイス がロード バランシング ピアの 1 つに Hello Request メッセージを送信しようとしたときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718012

エラーメッセージ `%Threat Defense-5-718012: Sent HELLO request to IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアに Hello Request メッセージを送信しました。

推奨アクション 不要。

718013

エラーメッセージ `%Threat Defense-6-718013: Peer IP_address is not answering HELLO`

説明ロード バランシング ピアは Hello Request メッセージに応答していません。

推奨アクションロードバランシングSSFピアとネットワーク接続のステータスを確認します。

718014

エラーメッセージ `%Threat Defense-5-718014: Master peer IP_address is not answering HELLO`

説明 ロード バランシング ディレクタ ピアが Hello Request メッセージに応答していません。

推奨アクション ロード バランシング SSF ディレクタピアとネットワーク接続のステータスを確認します。

718015

エラーメッセージ `%Threat Defense-5-718015: Received HELLO request from IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアから Hello Request メッセージを受信しました。

推奨アクション 不要。

718016

エラーメッセージ `%Threat Defense-5-718016: Received HELLO response from IP_address`

説明 Secure Firewall Threat Defense デバイス は、Hello Response パケットをロード バランシング ピアから受信しました。

推奨アクション 不要。

718017

エラーメッセージ `%Threat Defense-7-718017: Got timeout for unknown peer IP_address msg type message_type`

説明 Secure Firewall Threat Defense デバイス が未知のピアのタイムアウトを処理しました。ピアはすでにアクティブ リストから削除されている可能性があるので、メッセージは無視されました。

推奨アクション メッセージが解決しない場合、または望ましくない動作が引き起こされる場合は、ロード バランシング ピアを調べて、設定がすべて正しいことを確認します。

718018

エラーメッセージ `%Threat Defense-7-718018: Send KEEPALIVE request failure to IP_address`

説明 Keepalive Request メッセージをロード バランシング ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718019

エラーメッセージ `%Threat Defense-7-718019: Sent KEEPALIVE request to IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアに Keepalive Request メッセージを送信しました。

推奨アクション 不要。

718020

エラーメッセージ `%Threat Defense-7-718020: Send KEEPALIVE response failure to IP_address`

説明 Keepalive Response メッセージをロード バランシング ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718021

エラーメッセージ `%Threat Defense-7-718021: Sent KEEPALIVE response to IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアに Keepalive Response メッセージを送信しました。

推奨アクション 不要。

718022

エラーメッセージ `%Threat Defense-7-718022: Received KEEPALIVE request from IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアから Keepalive Request メッセージを受信しました。

推奨アクション 不要。

718023

エラーメッセージ `%Threat Defense-7-718023: Received KEEPALIVE response from IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアから Keepalive Response メッセージを受信しました。

推奨アクション 不要。

718024

エラーメッセージ `%Threat Defense-5-718024: Send CFG UPDATE failure to IP_address`

説明 Configuration Update メッセージをロード バランシング ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイス

を通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718025

エラーメッセージ `%Threat Defense-7-718025: Sent CFG UPDATE to IP_address`

説明 Secure Firewall Threat Defense デバイスは、ロードバランシング ピアに Configuration Update メッセージを送信しました。

推奨アクション 不要。

718026

エラーメッセージ `%Threat Defense-7-718026: Received CFG UPDATE from IP_address`

説明 Secure Firewall Threat Defense デバイスは、ロードバランシング ピアから Configuration Update メッセージを受信しました。

推奨アクション 不要。

718027

エラーメッセージ `%Threat Defense-6-718027: Received unexpected KEEPALIVE request from IP_address`

説明 Secure Firewall Threat Defense デバイスは、ロードバランシング ピアから予期せぬ Keepalive Request メッセージを受信しました。

推奨アクション 問題が解決しない場合、または望ましくない動作が引き起こされる場合は、すべてのロードバランシング ピアが正しく設定され、検出されていることを確認します。

718028

エラーメッセージ `%Threat Defense-5-718028: Send OOS indicator failure to IP_address`

説明 OOS Indicator メッセージをロードバランシング ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークの設定をチェックし、インターフェイスがアクティブでプロトコル データが Secure Firewall Threat Defense デバイスを通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718029

エラーメッセージ `%Threat Defense-7-718029: Sent OOS indicator to IP_address`

説明 Secure Firewall Threat Defense デバイス が、OOS Indicator メッセージをロード バランシング ピアに送信しました。

推奨アクション 不要。

718030

エラーメッセージ `%Threat Defense-6-718030: Received planned OOS from IP_address`

説明 Secure Firewall Threat Defense デバイス が、ロード バランシング ピアから計画的な OOS メッセージを受信しました。

推奨アクション 不要。

718031

エラーメッセージ `%Threat Defense-5-718031: Received OOS obituary for IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアから OOS Obituary メッセージを受信しました。

推奨アクション 不要。

718032

エラーメッセージ `%Threat Defense-5-718032: Received OOS indicator from IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアから OOS Indicator メッセージを受信しました。

推奨アクション 不要。

718033

エラーメッセージ `%Threat Defense-5-718033: Send TOPOLOGY indicator failure to IP_address`

説明 Topology Indicator メッセージをロード バランシング ピアの 1 つに送信しようとしているときに、エラーが発生しました。これは、ネットワークの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション Secure Firewall Threat Defense デバイス でネットワークのコンフィギュレーションをチェックし、インターフェイスがアクティブで、プロトコル データが Secure Firewall Threat Defense デバイス を通過していることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718034

エラーメッセージ `%Threat Defense-7-718034: Sent TOPOLOGY indicator to IP_address`

説明 Secure Firewall Threat Defense デバイス は、ロード バランシング ピアに Topology Indicator メッセージを送信しました。

推奨アクション 不要。

718035

エラーメッセージ `%Threat Defense-7-718035: Received TOPOLOGY indicator from IP_address`

説明 Secure Firewall Threat Defense デバイス が、ロード バランシング ピアから Topology Indicator メッセージを受信しました。

推奨アクション 不要。

718036

エラーメッセージ `%Threat Defense-7-718036: Process timeout for req-type type_value , exid exchange_ID , peer IP_address`

説明 Secure Firewall Threat Defense デバイス がピアのタイムアウトを処理しました。

推奨アクション ピアがタイムアウトされたことを確認します。タイムアウトされていない場合は、ロードバランシング ピアのコンフィギュレーションをチェックし、ピアと Secure Firewall Threat Defense デバイス との間のネットワーク接続を確認します。

718037

エラーメッセージ `%Threat Defense-6-718037: Master processed number_of_timeouts timeouts`

説明 ディレクタロールの Secure Firewall Threat Defense デバイス が、指摘された数のピアタイムアウトを処理しました。

推奨アクション タイムアウトが正当であることを確認します。タイムアウトされていない場合は、ピアのロードバランシングのコンフィギュレーションをチェックし、ピアと Secure Firewall Threat Defense デバイス との間のネットワーク接続を確認します。

718038

エラーメッセージ `%Threat Defense-6-718038: Slave processed number_of_timeouts timeouts`

説明 メンバーロールの Secure Firewall Threat Defense デバイス が、指摘された数のピアタイムアウトを処理しました。

推奨アクション タイムアウトが正当であることを確認します。タイムアウトされていない場合は、ピアのロードバランシングのコンフィギュレーションをチェックし、ピアと Secure Firewall Threat Defense デバイス との間のネットワーク接続を確認します。

718039

エラーメッセージ `%Threat Defense-6-718039: Process dead peer IP_address`

説明 Secure Firewall Threat Defense デバイス がデッド ピアを検出しました。

推奨アクション デッド ピアの検出が正当であることを確認します。タイムアウトされていない場合は、ピアのロードバランシングのコンフィギュレーションをチェックし、ピアと Secure Firewall Threat Defense デバイス との間のネットワーク接続を確認します。

718040

エラーメッセージ `%Threat Defense-6-718040: Timed-out exchange ID exchange_ID not found`

説明 Secure Firewall Threat Defense デバイス がデッド ピアを検出しましたが、交換 ID が認識されませんでした。

推奨アクション 不要。

718041

エラーメッセージ `%Threat Defense-7-718041: Timeout [msgType=type ] processed with no callback`

説明 Secure Firewall Threat Defense デバイス がデッド ピアを検出しましたが、処理でコールバックが使用されませんでした。

推奨アクション 不要。

718042

エラーメッセージ `%Threat Defense-5-718042: Unable to ARP for IP_address`

説明 ピアにコンタクトしようとしたときに、Secure Firewall Threat Defense デバイス で ARP 障害が発生しました。

推奨アクション ネットワークが動作していることと、すべてのピアが互いに通信できることを確認します。

718043

エラーメッセージ `%Threat Defense-5-718043: Updating/removing duplicate peer entry IP_address`

説明 Secure Firewall Threat Defense デバイス が重複するピア エントリを検出し、削除しています。

推奨アクション 不要。

718044

エラーメッセージ `%Threat Defense-5-718044: Deleted peer IP_address`

説明 Secure Firewall Threat Defense デバイス がロード バランシング ピアを削除しています。

推奨アクション 不要。

718045

エラーメッセージ `%Threat Defense-5-718045: Created peer IP_address`

説明 Secure Firewall Threat Defense デバイス がロード バランシング ピアを検出しました。

推奨アクション 不要。

718046

エラーメッセージ `%Threat Defense-7-718046: Create group policy policy_name`

説明安全にロード バランシング ピアと通信するため、Secure Firewall Threat Defense デバイス がグループ ポリシーを作成しました。

推奨アクション 不要。

718047

エラーメッセージ `%Threat Defense-7-718047: Fail to create group policy policy_name`

説明ロード バランシング ピア間の通信をセキュリティで保護するためにグループ ポリシーを作成しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨メッセージ ロード バランシング設定が正しいことを確認します。

718048

エラーメッセージ `%Threat Defense-5-718048: Create of secure tunnel failure for peer IP_address`

説明ロード バランシング ピアへの IPSec トンネルを確立しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨メッセージ ロード バランシング設定が正しく、ネットワークが動作していることを確認します。

718049

エラーメッセージ `%Threat Defense-7-718049: Created secure tunnel to peer IP_address`

説明 Secure Firewall Threat Defense デバイス がロード バランシング ピアへの IPSec トンネルを正常に確立しました。

推奨アクション 不要。

718050

エラーメッセージ `%Threat Defense-5-718050: Delete of secure tunnel failure for peer IP_address`

説明ロード バランシング ピアへの IPSec トンネルを終了しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨メッセージ ロード バランシング設定が正しく、ネットワークが動作していることを確認します。

718051

エラーメッセージ `%Threat Defense-6-718051: Deleted secure tunnel to peer IP_address`

説明 Secure Firewall Threat Defense デバイス がロード バランシング ピアへの IPSec トンネルを正常に終了しました。

推奨アクション 不要。

718052

エラーメッセージ `%Threat Defense-5-718052: Received GRAT-ARP from duplicate master MAC_address`

説明 Secure Firewall Threat Defense デバイス が重複ディレクタから Gratuitous ARP を受信しました。

推奨アクション ロード バランシング コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718053

エラーメッセージ `%Threat Defense-5-718053: Detected duplicate master, mastership stolen MAC_address`

説明 Secure Firewall Threat Defense デバイス が重複ディレクタと盗まれたディレクタを検出しました。

推奨アクション ロード バランシング コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718054

エラーメッセージ `%Threat Defense-5-718054: Detected duplicate master MAC_address and going to SLAVE`

説明 Secure Firewall Threat Defense デバイス が重複ディレクタを検出し、メンバーモードに切り替えています。

推奨アクション ロード バランシング コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718055

エラーメッセージ `%Threat Defense-5-718055: Detected duplicate master MAC_address and staying MASTER`

説明 Secure Firewall Threat Defense デバイス が重複ディレクタを検出し、メンバーモードにとどまっています。

推奨アクション ロード バランシング コンフィギュレーションをチェックし、ネットワークが動作していることを確認します。

718056

エラーメッセージ `%Threat Defense-7-718056: Deleted Master peer, IP IP_address`

説明 Secure Firewall Threat Defense デバイス が内部テーブルからロード バランシング ディレクタを削除しました。

推奨アクション 不要。

718057

エラーメッセージ `%Threat Defense-5-718057: Queue send failure from ISR, msg type failure_code`

説明 VPN ロード バランシング キューで Interrupt Service Routing からメッセージをキューに入れているときに、内部ソフトウェア エラーが発生しました。

推奨アクション 一般的に、これは問題のない状態です。問題が解決しない場合、Cisco TAC にお問い合わせください。

718058

エラーメッセージ `%Threat Defense-7-718058: State machine return code: action_routine , return_code`

説明ロード バランシング有限状態マシンに属するアクション ルーチンの戻りコードがトレースされています。

推奨アクション 不要。

718059

エラーメッセージ `%Threat Defense-7-718059: State machine function trace: state=state_name , event=event_name , func=action_routine`

説明ロード バランシング有限状態マシンのイベントと状態がトレースされています。

推奨アクション 不要。

718060

エラーメッセージ `%Threat Defense-5-718060: Inbound socket select fail: context=context_ID .`

説明ソケット選択コールがエラーを戻し、ソケットを読み取ることができません。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。

718061

エラーメッセージ `%Threat Defense-5-718061: Inbound socket read fail: context=context_ID .`

説明選択コールでデータが検出された後、ソケット読み取りが失敗しました。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

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

718062

エラーメッセージ `%Threat Defense-5-718062: Inbound thread is awake (context=context_ID ).`

説明ロード バランシング プロセスが起動され、処理を開始します。

推奨アクション 不要。

718063

エラーメッセージ `%Threat Defense-5-718063: Interface interface_name is down.`

説明インターフェイスがダウンしていることがロード バランシング プロセスによって検出されました。

推奨アクション インターフェイス コンフィギュレーションを調べて、インターフェイスが動作していることを確認します。

718064

エラーメッセージ %Threat Defense-5-718064: Admin. interface *interface_name* is down.

説明管理インターフェイスがダウンしていることがロード バランシング プロセスによって検出されました。

推奨アクション 管理インターフェイス コンフィギュレーションを調べて、インターフェイスが動作していることを確認します。

718065

エラーメッセージ %Threat Defense-5-718065: Cannot continue to run (public=*up* /*down* , private=*up* /*down* , enable=*LB_state* , master=*IP_address* , session=*Enable* /*Disable*).

説明すべての前提条件が満たされていないため、ロード バランシング プロセスを実行できません。前提条件は、2つのアクティブなインターフェイスとロードバランシングがイネーブルになっていることです。

推奨アクション インターフェイス コンフィギュレーションを調べて、少なくとも 2 つのインターフェイスが動作しており、ロードバランシングがイネーブルになっていることを確認します。

718066

エラーメッセージ %Threat Defense-5-718066: Cannot add secondary address to interface *interface_name* , ip *IP_address* .

説明ロード バランシングには、外部インターフェイスに追加するセカンダリ アドレスが必要です。セカンダリ アドレスを追加する際に障害が発生しました。

推奨アクション セカンダリ アドレスとして使用されているアドレスを調べ、それが有効な一意のアドレスであることを確認します。外部インターフェイスのコンフィギュレーションを確認します。

718067

エラーメッセージ %Threat Defense-5-718067: Cannot delete secondary address to interface *interface_name* , ip *IP_address* .

説明セカンダリアドレスの削除が失敗しました。これは、アドレッシングの問題または内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション 外部インターフェイスのアドレッシング情報を調べ、セカンダリ アドレスが有効な一意のアドレス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。

718068

エラーメッセージ `%Threat Defense-5-718068: Start VPN Load Balancing in context context_ID .`

説明 ロード バランシング プロセスが開始され、初期化されました。

推奨アクション 不要。

718069

エラーメッセージ `%Threat Defense-5-718069: Stop VPN Load Balancing in context context_ID .`

説明 ロード バランシング プロセスが停止されました。

推奨アクション 不要。

718070

エラーメッセージ `%Threat Defense-5-718070: Reset VPN Load Balancing in context context_ID .`

説明 LB プロセスがリセットされました。

推奨アクション 不要。

718071

エラーメッセージ `%Threat Defense-5-718071: Terminate VPN Load Balancing in context context_ID .`

説明 LB プロセスが終了されました。

推奨アクション 不要。

718072

エラーメッセージ `%Threat Defense-5-718072: Becoming master of Load Balancing in context context_ID .`

説明 Secure Firewall Threat Defense デバイス が LB ディレクタになりました。

推奨アクション 不要。

718073

エラーメッセージ `%Threat Defense-5-718073: Becoming slave of Load Balancing in context context_ID .`

説明 Secure Firewall Threat Defense デバイス が LB メンバーになりました。

推奨アクション 不要。

718074

エラーメッセージ `%Threat Defense-5-718074: Fail to create access list for peer context_ID .`

説明 ACL は、LB ピアが通信できるセキュア トンネルを作成するために使用されます。Secure Firewall Threat Defense デバイスがこれらの ACL のいずれかを作成できませんでした。これは、アドレッシングの問題または内部ソフトウェアの問題が存在する可能性があることを示しています。

推奨アクションすべてのピアで内部インターフェイスのアドレッシング情報を調べ、すべてのピアが正しく検出されていることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

718075

エラーメッセージ `%Threat Defense-5-718075: Peer IP_address access list not set.`

説明セキュア トンネルを削除する際、Secure Firewall Threat Defense デバイス が、関連する ACL を持たないピア エントリを検出しました。

推奨アクション 不要。

718076

エラーメッセージ `%Threat Defense-5-718076: Fail to create tunnel group for peer IP_address .`

説明ロード バランシング ピア間の通信を保護するためのトンネル グループを作成しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨メッセージ ロード バランシング設定が正しいことを確認します。

718077

エラーメッセージ `%Threat Defense-5-718077: Fail to delete tunnel group for peer IP_address .`

説明ロード バランシング ピア間の通信を保護するためのトンネル グループを削除しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨アクション 不要。

718078

エラーメッセージ `%Threat Defense-5-718078: Fail to create crypto map for peer IP_address .`

説明ロード バランシング ピア間の通信を保護するためのクリプト マップを作成しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨メッセージ ロード バランシング設定が正しいことを確認します。

718079

エラーメッセージ `%Threat Defense-5-718079: Fail to delete crypto map for peer IP_address .`

説明ロード バランシング ピア間の通信を保護するためのクリプト マップを削除しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨アクション 不要。

718080

エラーメッセージ `%Threat Defense-5-718080: Fail to create crypto policy for peer IP_address .`

説明ロード バランシング ピア間の通信を保護するために使用するトランスフォーム セットを作成しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。これは、内部ソフトウェアの問題が存在する可能性があることを示しています。

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

718081

エラーメッセージ `%Threat Defense-5-718081: Fail to delete crypto policy for peer IP_address .`

説明ロード バランシング ピア間の通信を保護するために使用するトランスフォーム セットを削除しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨アクション 不要。

718082

エラーメッセージ `%Threat Defense-5-718082: Fail to create crypto ipsec for peer IP_address .`

説明 VPN ロードバランシングのクラスタ暗号化がイネーブルである場合、VPN ロードバランシング デバイスは、ロード バランシング クラスタ内の他のすべてのデバイス用にサイトツーサイト トンネルのセットを作成します。トンネルごとに、暗号パラメータのセット（アクセス リスト、クリプト マップ、およびトランスフォーム セット）が動的に作成されます。そのような暗号パラメータの 1 つまたは複数を作成または設定できませんでした。

- **IP_address**：リモート ピアの IP アドレス

推奨アクション メッセージを調べて、作成できなかった暗号パラメータのタイプに固有の他のエントリがないかどうかを確認します。

718083

エラーメッセージ `%Threat Defense-5-718083: Fail to delete crypto ipsec for peer IP_address .`

説明 ローカル VPN ロード バランシング デバイスがクラスタから削除される場合、暗号パラメータが削除されます。1 つまたは複数の暗号パラメータを削除できませんでした。

- **IP_address**：リモート ピアの IP アドレス

説明 メッセージを調べて、削除できなかった暗号パラメータのタイプに固有の他のエントリがないかどうかを確認します。

718084

エラーメッセージ `%Threat Defense-5-718084: Public/cluster IP not on the same subnet: public IP_address , mask netmask , cluster IP_address`

説明 クラスタ IP アドレスが、Secure Firewall Threat Defense デバイス の外部インターフェイスと同じネットワーク上にありません。

推奨アクション クラスタ（または仮想）IP アドレスと外部インターフェイス アドレスの両方が同じネットワーク上にあることを確認します。

718085

エラーメッセージ `%Threat Defense-5-718085: Interface interface_name has no IP address defined.`

説明 インターフェイスで IP アドレスが設定されていません。

推奨アクション インターフェイスの IP アドレスを設定します。

718086

エラーメッセージ `%Threat Defense-5-718086: Fail to install LB NP rules: type rule_type , dst interface_name , port port .`

説明 ロードバランシング ピア間の通信を保護するために使用する SoftNP ACL 規則を作成しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。これは、内部ソフトウェアの問題が存在する可能性があることを示しています。

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

718087

エラーメッセージ `%Threat Defense-5-718087: Fail to delete LB NP rules: type rule_type , rule rule_ID .`

説明ロードバランシング ピア間の通信を保護するために使用する SoftNP ACL 規則を削除しようとしたときに、Secure Firewall Threat Defense デバイス で障害が発生しました。

推奨アクション 不要。

718088

エラーメッセージ `%Threat Defense-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC_address .`

説明 重複ディレクタの存在は、ロードバランシングピアのいずれかの設定が誤っている可能性を示しています。

推奨アクションすべてのピアのロード バランシング コンフィギュレーションを調べ、特定されたピアに特に注意します。

719001

エラーメッセージ `%Threat Defense-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.`

説明最大セッション制限に達したため着信電子メールプロキシセッションを確立できません。

- **maximum_sessions**：最大セッション数

推奨アクション 不要。

719002

エラーメッセージ `%Threat Defense-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.`

説明エラーのためセッションが終了しました。考えられるエラーは、セッションデータベースへのセッションの追加の失敗、メモリ割り当ての失敗、チャネルへのデータ書き込みの失敗です。

- **pointer**：セッション ポインタ
- **source_address**：電子メール プロキシ クライアントの IP アドレス
- **reason**：エラー タイプ

推奨アクション 不要。

719003

エラーメッセージ `%Threat Defense-6-719003: Email Proxy session pointer resources have been freed for source_address .`

説明動的に割り当てられたセッション構造が解放され、セッションの終了後にNULLに設定されました。

- **pointer**：セッション ポインタ
- **source_address**：電子メール プロキシ クライアントの IP アドレス

推奨アクション 不要。

719004

エラーメッセージ `%Threat Defense-6-719004: Email Proxy session pointer has been successfully established for source_address .`

説明新規着信電子メール クライアント セッションが確立されました。

推奨アクション 不要。

719005

エラーメッセージ `%Threat Defense-7-719005: FSM NAME has been created using protocol for session pointer from source_address .`

説明新規着信セッションに対して FSM が作成されました。

- NAME：セッションの FSM インスタンス名
- **protocol**：電子メール プロトコル タイプ（たとえば、POP3、IMAP、および SMTP）
- **pointer**：セッション ポインタ
- **source_address**：電子メール プロキシ クライアントの IP アドレス

推奨アクション 不要。

719006

エラーメッセージ `%Threat Defense-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.`

説明ネットワークの輻輳が発生しており、データを電子メールクライアントまたは電子メールサーバーに送信できません。この状態によって、ブロック タイマーが開始されます。ブロック タイマーがタイムアウトになると、セッションの有効期限が切れます。

- **pointer**：セッション ポインタ
- **source_address**：電子メール プロキシ クライアントの IP アドレス

推奨アクション 数分後にオペレーションを再試行します。

719007

エラーメッセージ `%Threat Defense-7-719007: Email Proxy session pointer cannot be found for source_address .`

説明セッション データベース内で一致するセッションが見つかりません。セッション ポインタが不良です。

- **pointer**：セッション ポインタ
- **source_address**：電子メール プロキシ クライアントの IP アドレス

推奨アクション 不要。

719008

エラーメッセージ `%Threat Defense-3-719008: Email Proxy service is shutting down.`

説明電子メールプロキシがディセーブルです。すべてのリソースがクリーンアップされ、すべてのスレッドが終了されます。

推奨アクション 不要。

719009

エラーメッセージ `%Threat Defense-7-719009: Email Proxy service is starting.`

説明電子メール プロキシがイネーブルです。

推奨アクション 不要。

719010

エラーメッセージ `%Threat Defense-6-719010: protocol Email Proxy feature is disabled on interface interface_name .`

説明電子メール プロキシ機能が CLI から呼び出され、特定のエントリ ポイントでディセーブルになっています。これは、ユーザーのメインのオン スイッチです。すべてのインターフェイスですべてのプロトコルがオフになると、メインのシャットダウン ルーチンが呼び出され、グローバル リソースやスレッドがクリーンアップされます。

- **protocol**：電子メール プロキシ プロトコル タイプ（たとえば、POP3、IMAP、および SMTP）
- **interface_name**：Secure Firewall Threat Defense インターフェイス名

推奨アクション 不要。

719011

エラーメッセージ `%Threat Defense-6-719011: Protocol Email Proxy feature is enabled on interface interface_name .`

説明電子メール プロキシ機能が CLI から呼び出され、特定のエントリ ポイントでイネーブルになっています。これは、ユーザーのメインのオンスイッチです。初めて使用される場合は、グローバル リソースやスレッドを割り当てるため、メインの起動ルーチンが呼び出されます。後続のコールでは、特定のプロトコル用のリッスン スレッドだけが起動されます。

- **protocol**：電子メール プロキシ プロトコル タイプ（たとえば、POP3、IMAP、および SMTP）
- **interface_name**：Secure Firewall Threat Defense インターフェイス名

推奨アクション 不要。

719012

エラーメッセージ `%Threat Defense-6-719012: Email Proxy server listening on port port for mail protocol protocol .`

説明設定されたポート上の特定のプロトコルに対してリッスン チャネルが開かれ、それが TCP 選択グループに追加されました。

- **port**：設定されたポート番号
- **protocol**：電子メール プロキシ プロトコル タイプ（たとえば、POP3、IMAP、および SMTP）

推奨アクション 不要。

719013

エラーメッセージ `%Threat Defense-6-719013: Email Proxy server closing port port for mail protocol protocol .`

説明設定されたポート上の特定のプロトコルに対してリッスン チャネルが閉じられ、それが TCP 選択グループから削除されました。

- **port**：設定されたポート番号
- **protocol**：電子メール プロキシ プロトコル タイプ（たとえば、POP3、IMAP、および SMTP）

推奨アクション 不要。

719014

エラーメッセージ `%Threat Defense-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol .`

説明指摘されたプロトコルのリッスン ポートで変更がシグナリングされます。そのポートに対してイネーブルなすべてのインターフェイスでリッスン チャネルが閉じられ、新規ポートでリッスンが再開されました。このアクションは、CLI から呼び出されます。

- **old_port**：以前設定されたポート番号
- **new_port**：新しく設定されたポート番号

- **protocol**：電子メール プロキシ プロトコル タイプ（たとえば、POP3、IMAP、および SMTP）

推奨アクション 不要。

719015

エラーメッセージ `%Threat Defense-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user , vpnuser = VPN_user , mailserver = server`

説明ユーザー名文字列が vpnuser（名前デリミタ）mailuser（サーバー デリミタ）mailserver の形式でクライアントから受信されました（たとえば、xxx:yyy@cisco.com）。名前デリミタはオプションです。デリミタがない場合は、VPNユーザー名とメールユーザー名が同じです。サーバー デリミタはオプションです。存在しない場合、デフォルト設定のメール サーバーが使用されます。

- **pointer**：セッション ポインタ
- **source_address**：電子メール プロキシ クライアントの IP アドレス
- mail_user：電子メール アカウントのユーザー名
- **VPN_user**：WebVPN ユーザー名
- **server**：電子メール サーバー

推奨アクション 不要。

719016

エラーメッセージ `%Threat Defense-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******`

説明パスワード文字列が vpnpass（名前デリミタ）mailpass の形式でクライアントから受信されました（たとえば、xxx:yyy）。名前デリミタはオプションです。デリミタがない場合は、VPN パスワードとメール パスワードが同じです。

- **pointer**：セッション ポインタ
- **source_address**：電子メール プロキシ クライアントの IP アドレス

推奨アクション 不要。

719017

エラーメッセージ `%Threat Defense-6-719017: WebVPN user: vpnuser invalid dynamic ACL.`

説明 ACL がこのユーザーを解析できなかったため、WebVPN セッションが中断されました。ACL は、どのようなユーザー制限が電子メール アカウントのアクセスにかけられているのかを判別します。ACL は AAA サーバーからダウンロードされます。このエラーのため、ログインの続行は安全ではありません。

- **vpnuser**：WebVPN ユーザー名

推奨アクション AAA サーバーを調べて、このユーザーのダイナミック ACL を修正します。

719018

エラーメッセージ `%Threat Defense-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found`

説明ローカルで保持されている ACL リストで ACL が見つかりません。ACL は、どのようなユーザー制限が電子メール アカウントのアクセスにかけられているのかを判別します。ACL はローカルで設定されます。このエラーのため、続行は認可されません。

- **vpnuser**：WebVPN ユーザー名
- **acl_ID**：ローカルで設定された ACL 識別文字列

推奨アクション ローカル ACL 設定を確認します

719019

エラーメッセージ `%Threat Defense-6-719019: WebVPN user: vpnuser authorization failed.`

説明 ACL は、どのようなユーザー制限が電子メール アカウントのアクセスにかけられているのかを判別します。認可チェックの失敗のため、ユーザーが電子メールアカウントにアクセスできません。

- **vpnuser**：WebVPN ユーザー名

推奨アクション 不要。

719020

エラーメッセージ `%Threat Defense-6-719020: WebVPN user vpnuser authorization completed successfully.`

説明 ACL は、どのようなユーザー制限が電子メール アカウントのアクセスにかけられているのかを判別します。ユーザーは、電子メール アカウントへのアクセスを認可されます。

- **vpnuser**：WebVPN ユーザー名

推奨アクション 不要。

719021

エラーメッセージ `%Threat Defense-6-719021: WebVPN user: vpnuser is not checked against ACL.`

説明 ACL は、どのようなユーザー制限が電子メール アカウントのアクセスにかけられているのかを判別します。ACL を使用した認可チェックがイネーブルになっていません。

- **vpnuser**：WebVPN ユーザー名

推奨アクション 必要に応じて、ACL チェック機能を有効にします。

719022

エラーメッセージ `%Threat Defense-6-719022: WebVPN user vpnuser has been authenticated.`

説明ユーザー名が AAA サーバーによって認証されました。

- **vpnuser**：WebVPN ユーザー名

推奨アクション 不要。

719023

エラーメッセージ `%Threat Defense-6-719023 : WebVPN user vpnuser has not been successfully authenticated. Access denied.`

説明 ユーザー名が AAA サーバーによって拒否されました。セッションは中断されます。ユーザーは、電子メール アカウントへのアクセスを許可されません。

- **vpnuser**：WebVPN ユーザー名

推奨アクション 不要。

719024

エラーメッセージ `%Threat Defense-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address`

説明 Piggyback 認証が、確立された WebVPN セッションを使用して WebVPN セッション データベースでユーザー名と IP アドレスの一致を検証しています。これは、WebVPN セッションと電子メール プロキシ セッションが同じユーザーによって開始され、WebVPN セッションがすでに確立されているという想定に基づいています。認証が失敗したため、セッションは中断されます。ユーザーは、電子メール アカウントへのアクセスを許可されません。

- **pointer**：セッション ポインタ
- **vpnuser**：WebVPN ユーザー名
- **source_address**：クライアント IP アドレス

推奨アクション 不要。

719025

エラーメッセージ `%Threat Defense-6-719025: Email Proxy DNS name resolution failed for hostname .`

説明 IP アドレスが有効でないか、使用可能な DNS サーバーがないため、IP アドレスでホスト名を解決できません。

- **hostname**：解決する必要のあるホスト名

推奨アクション DNS サーバーの可用性を調べ、設定したメール サーバー名が有効かどうかを確認します。

719026

エラーメッセージ `%Threat Defense-6-719026: Email Proxy DNS name hostname resolved to IP_address .`

説明 IP アドレスでホスト名が正常に解決されました。

- **hostname**：解決する必要のあるホスト名
- **IP_address**：設定したメール サーバー名から解決された IP アドレス

推奨アクション 不要。

メッセージ 720001 ～ 721019

この項では、720001 から 721019 までのメッセージについて説明します。

720001

エラーメッセージ `%Threat Defense-4-720001: (VPN-unit ) Failed to initialize with Chunk Manager.`

説明 VPN フェールオーバー サブシステムがメモリ バッファ管理サブシステムで初期化できません。システム全体の問題が発生し、VPN フェールオーバー サブシステムを開始できません。

- **unit**：Primary または Secondary

推奨アクション メッセージを調べ、システム レベルで初期化の問題の兆候がないかどうかを調べます。

720002

エラーメッセージ `%Threat Defense-6-720002: (VPN-unit ) Starting VPN Stateful Failover Subsystem...`

説明 VPN フェールオーバー サブシステムが開始していて起動しています。

- **unit**：Primary または Secondary

推奨アクション 不要。

720003

エラーメッセージ `%Threat Defense-6-720003: (VPN-unit ) Initialization of VPN Stateful Failover Component completed successfully`

説明ブート時に VPN フェールオーバー サブシステムの初期化が完了しています。

- **unit**：Primary または Secondary

推奨アクション 不要。

720004

エラーメッセージ `%Threat Defense-6-720004: (VPN-unit ) VPN failover main thread started.`

説明ブート時に VPN フェールオーバーのメイン処理スレッドが開始されます。

- **unit**：Primary または Secondary

推奨アクション 不要。

720005

エラーメッセージ `%Threat Defense-6-720005: (VPN-unit ) VPN failover timer thread started.`

説明ブート時に VPN フェールオーバーのタイマー処理スレッドが開始されます。

- **unit**：Primary または Secondary

推奨アクション 不要。

720006

エラーメッセージ `%Threat Defense-6-720006: (VPN-unit ) VPN failover sync thread started.`

説明ブート時に VPN フェールオーバーのバルク同期化処理スレッドが開始されます。

- **unit**：Primary または Secondary

推奨アクション 不要。

720007

エラーメッセージ `%Threat Defense-4-720007: (VPN-unit ) Failed to allocate chunk from Chunk Manager.`

説明事前に割り当てられたメモリ バッファのセットがなくなりつつあります。Secure Firewall Threat Defense デバイス にリソースの問題があります。処理されているメッセージの数が多すぎる場合は、Secure Firewall Threat Defense デバイス に重い負荷がかかっている可能性があります。

- **unit**：Primary または Secondary

推奨アクション この状態は、後で VPN フェールオーバー サブシステムが未処理のメッセージを処理し、前に割り当てられたメモリを解放したときに改善される可能性があります。

720008

エラーメッセージ `%Threat Defense-4-720008: (VPN-unit ) Failed to register to High Availability Framework.`

説明 VPN フェールオーバー サブシステムがコア フェールオーバー サブシステムに登録できませんでした。VPN フェールオーバー サブシステムを起動できません。他のサブシステムの初期化の問題が原因となっている可能性があります。

- **unit**：Primary または Secondary

推奨アクション メッセージを検索し、システム全体で初期化の問題の兆候がないかどうかを調べます。

720009

エラーメッセージ `%Threat Defense-4-720009: (VPN-unit ) Failed to create version control block.`

説明 VPN フェールオーバー サブシステムがバージョン制御ブロックを作成できませんでした。このステップは、VPN フェールオーバー サブシステムが、現在のリリースの下位互換性ファームウェア バージョンを検出するために必要です。VPN フェールオーバー サブシステムを起動できません。他のサブシステムの初期化の問題が原因となっている可能性があります。

- **unit**：Primary または Secondary

推奨アクション メッセージを検索し、システム全体で初期化の問題の兆候がないかどうかを調べます。

720010

エラーメッセージ `%Threat Defense-6-720010: (VPN-unit ) VPN failover client is being disabled`

説明 オペレータがフェールオーバー キーを定義しないでフェールオーバーをイネーブルにしました。VPN フェールオーバーを使用するには、フェールオーバー キーを定義する必要があります。

- **unit**：Primary または Secondary

推奨アクション **failover key** コマンドを使用して、アクティブ装置とスタンバイ装置の間の共有秘密キーを定義します。

720011

エラーメッセージ `%Threat Defense-4-720011: (VPN-unit ) Failed to allocate memory`

説明 VPN フェールオーバー サブシステムがメモリ バッファを割り当てられません。これは、システム全体のリソースの問題を示しています。Secure Firewall Threat Defense デバイス には重い負荷がかかっています。

- **unit**：Primary または Secondary

推奨アクション この状態は、着信トラフィックを削減することによって Secure Firewall Threat Defense デバイス の負荷を減らすと改善される可能性があります。着信トラフィックを削減す

ることによって、既存の作業負荷を処理するために割り当てられたメモリが使用可能になり、Secure Firewall Threat Defense デバイス が通常のオペレーションに戻る可能性があります。

720012

エラーメッセージ `%Threat Defense-6-720012: (VPN-unit ) Failed to update IPsec failover runtime data on the standby unit.`

説明対応する IPSec トンネルがスタンバイ装置で削除されているため、VPN フェールオーバー サブシステムが IPSec 関連のランタイム データをアップデートできません。

- **unit**：Primary または Secondary

推奨アクション 不要。

720013

エラーメッセージ `%Threat Defense-4-720013: (VPN-unit ) Failed to insert certificate in trustpoint trustpoint_name`

説明 VPN フェールオーバー サブシステムがトラストポイントに証明書を挿入しようとしました。

- **unit**：Primary または Secondary
- **trustpoint_name**：トラストポイントの名前

推奨アクション 証明書の内容を調べて、無効かどうかを判別します。

720014

エラーメッセージ `%Threat Defense-6-720014: (VPN-unit ) Phase 2 connection entry (msg_id=message_number , my cookie=mine , his cookie=his ) contains no SA list.`

説明フェーズ 2 接続エントリにリンクされたセキュリティ アソシエーションがありません。

- **unit**：Primary または Secondary
- **message_number**：フェーズ 2 接続エントリのメッセージ ID
- **mine**：自分のフェーズ 1 クッキー
- **his**：ピアのフェーズ 1 クッキー

推奨アクション 不要。

720015

エラーメッセージ `%Threat Defense-6-720015: (VPN-unit ) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number ,my cookie=mine , his cookie=his ).`

説明所定のフェーズ 2 接続エントリに対して対応するフェーズ 1 セキュリティ アソシエーションが見つかりません。

- **unit**：Primary または Secondary
- **message_number**：フェーズ 2 接続エントリのメッセージ ID
- **mine**：自分のフェーズ 1 クッキー
- **his**：ピアのフェーズ 1 クッキー

推奨アクション 不要。

720016

エラーメッセージ `%Threat Defense-5-720016: (VPN-unit) Failed to initialize default timer #index .`

説明 VPN フェールオーバー サブシステムが所定のタイマー イベントを初期化できませんでした。ブート時に VPN フェールオーバー サブシステムを起動できません。

- **unit**：Primary または Secondary
- **index**：タイマー イベントの内部インデックス

推奨アクション メッセージを検索し、システム全体で初期化の問題の兆候がないかどうかを調べます。

720017

エラーメッセージ `%Threat Defense-5-720017: (VPN-unit ) Failed to update LB runtime data`

説明 VPN フェールオーバー サブシステムが VPN ロード バランシング ランタイム データをアップデートできませんでした。

- **unit**：Primary または Secondary

推奨アクション 不要。

720018

エラーメッセージ `%Threat Defense-5-720018: (VPN-unit ) Failed to get a buffer from the underlying core high availability subsystem. Error code code.`

説明 Secure Firewall Threat Defense デバイスには重い負荷がかかっています。VPN フェールオーバー サブシステムがフェールオーバー バッファを取得できませんでした。

- **unit**：Primary または Secondary
- **code**：高可用性のサブシステムから返されたエラー コード

推奨アクション 着信トラフィックの量を減らし、現在の負荷状態を改善します。着信トラフィックが減ると、Secure Firewall Threat Defense デバイスは着信の負荷を処理するために割り当てられたメモリを解放します。

720019

エラーメッセージ `%Threat Defense-5-720019: (VPN-unit ) Failed to update cTCP statistics.`

説明 VPN フェールオーバー サブシステムが IPSec/cTCP 関連の統計をアップデートできませんでした。

- **unit**：Primary または Secondary

推奨アクション 不要。アップデートは定期的に送信されるので、スタンバイ装置の IPSec/cTCP 統計は次のアップデート メッセージでアップデートされます。

720020

エラーメッセージ `%Threat Defense-5-720020: (VPN-unit ) Failed to send type timer message.`

説明 VPN フェールオーバー サブシステムが定期的なタイマー メッセージをスタンバイ装置に送信できませんでした。

- **unit**：Primary または Secondary
- **type**：タイマー メッセージのタイプ

推奨アクション 不要。次のタイムアウト時に定期的なタイマー メッセージが再送されます。

720021

エラーメッセージ `%Threat Defense-5-720021: (VPN-unit ) HA non-block send failed for peer msg message_number . HA error code .`

説明 VPN フェールオーバー サブシステムが非ブロック メッセージを送信できませんでした。これは、負荷のかかった Secure Firewall Threat Defense デバイス またはリソース不足によって引き起こされる一時的な状態です。

- **unit**：Primary または Secondary
- **message_number**：ピア メッセージの ID 番号
- **code**：エラー戻りコード

推奨アクション Secure Firewall Threat Defense デバイス で使用できるリソースが増加するにしたがい、状態は改善されます。

720022

エラーメッセージ `%Threat Defense-4-720022: (VPN-unit ) Cannot find trustpoint trustpoint`

説明 VPN フェールオーバー サブシステムがトラストポイントを名前で検索しようとしたときに、エラーが発生しました。

- **unit**：Primary または Secondary
- **trustpoint**：トラスト ポイントの名前。

推奨アクション トラストポイントはオペレータによって削除される可能性があります。

720023

エラーメッセージ `%Threat Defense-6-720023: (VPN-unit ) HA status callback: Peer is not present.`

説明ピアが使用可能または使用不可になったことをローカル Secure Firewall Threat Defense デバイスが検出すると、VPN フェールオーバー サブシステムがコア フェールオーバー サブシステムから通知を受けます。

- **unit**：Primary または Secondary
- **not**：「not」またはブランクのまま

推奨アクション 不要。

720024

エラーメッセージ `%Threat Defense-6-720024: (VPN-unit ) HA status callback: Control channel is status .`

説明フェールオーバー コントロール チャネルはアップまたはダウンです。フェールオーバー コントロールチャネルは、フェールオーバー リンク チャネルがアップかダウンかを示す**failover link** コマンドと **show failover** コマンドによって定義されます。

- **unit**：Primary または Secondary
- **status**：Up または Down

推奨アクション 不要。

720025

エラーメッセージ `%Threat Defense-6-720025: (VPN-unit ) HA status callback: Data channel is status .`

説明フェールオーバー データ チャネルはアップまたはダウンです。

- **unit**：Primary または Secondary
- **status**：Up または Down

推奨アクション 不要。

720026

エラーメッセージ `%Threat Defense-6-720026: (VPN-unit ) HA status callback: Current progression is being aborted.`

説明オペレータまたはその他の外部条件が発生し、フェールオーバー ピアが役割（アクティブまたはスタンバイ）に合意する前に現在のフェールオーバーの進行が中断されました。たとえば、**failover active** コマンドがネゴシエーション中にスタンバイ装置で入力された場合や、アクティブ装置がリブートされている場合です。

- **unit**：Primary または Secondary

推奨アクション 不要。

720027

エラーメッセージ `%Threat Defense-6-720027: (VPN-unit ) HA status callback: My state state .`

説明 ローカル フェールオーバー デバイスの状態が変更されます。

- **unit**：Primary または Secondary
- **state**：ローカル フェールオーバー デバイスの現在の状態

推奨アクション 不要。

720028

エラーメッセージ `%Threat Defense-6-720028: (VPN-unit ) HA status callback: Peer state state .`

説明 フェールオーバー ピアの現在の状態が報告されます。

- **unit**：Primary または Secondary
- **state**：フェールオーバー ピアの現在の状態

推奨アクション 不要。

720029

エラーメッセージ `%Threat Defense-6-720029: (VPN-unit ) HA status callback: Start VPN bulk sync state.`

説明 アクティブ装置は、すべての状態情報をスタンバイ装置へ送信する準備ができています。

- **unit**：Primary または Secondary

推奨アクション 不要。

720030

エラーメッセージ `%Threat Defense-6-720030: (VPN-unit ) HA status callback: Stop bulk sync state.`

説明 アクティブ装置がすべての状態情報をスタンバイ装置へ送信し終わりました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720031

エラーメッセージ `%Threat Defense-7-720031: (VPN-unit ) HA status callback: Invalid event received. event=event_ID .`

説明 VPN フェールオーバー サブシステムが、基礎となるフェールオーバー サブシステムから無効なコールバック イベントを受信しました。

- **unit**：Primary または Secondary
- **event_ID**：受信した無効なイベント ID

推奨アクション 不要。

720032

エラーメッセージ `%Threat Defense-6-720032: (VPN-unit) HA status callback: id=ID , seq=sequence_# , grp=group , event=event , op=operand , my=my_state , peer=peer_state .`

説明基礎となるフェールオーバー サブシステムがステータス アップデートを通知したことが VPN フェールオーバー サブシステムによって示されました。

- **unit**：Primary または Secondary
- **ID**：クライアント ID 番号
- **sequence_#**：シーケンス番号
- **group**：グループ ID
- **event**：現在のイベント
- **operand**：現在のオペランド
- **my_state**：システムの現在の状態
- **peer_state**：ピアの現在の状態

推奨アクション 不要。

720033

エラーメッセージ `%Threat Defense-4-720033: (VPN-unit ) Failed to queue add to message queue.`

説明システム リソースが低下している可能性があります。VPN フェールオーバー サブシステムが内部メッセージをキューに入れようとしたときにエラーが発生しました。これは、Secure Firewall Threat Defense デバイス に重い負荷がかかっており、VPN フェールオーバー サブシステムが着信トラフィックを処理するためのリソースを割り当てられないことを示す一時的な状態である可能性があります。

- **unit**：Primary または Secondary

推奨アクション このエラーは、Secure Firewall Threat Defense デバイス の現在の負荷が減り、新規メッセージを再び処理するために追加のシステム リソースを使用できるようになると、解決する可能性があります。

720034

エラーメッセージ `%Threat Defense-7-720034: (VPN-unit ) Invalid type (type ) for message handler.`

説明 VPN フェールオーバー サブシステムが無効なメッセージ タイプを処理しようとたときにエラーが発生しました。

- **unit**：Primary または Secondary
- **type**：メッセージ タイプ

推奨アクション 不要。

720035

エラーメッセージ `%Threat Defense-5-720035: (VPN-unit ) Fail to look up CTCP flow handle`

説明 VPN フェールオーバー サブシステムが検索を実行する前に、スタンバイ装置で cTCP フローが削除される可能性があります。

- **unit**：Primary または Secondary

推奨アクション cTCP フローが削除される兆候をメッセージで検索して、フローが削除された理由（たとえば、アイドル タイムアウト）を判別します。

720036

エラーメッセージ `%Threat Defense-5-720036: (VPN-unit ) Failed to process state update message from the active peer.`

説明スタンバイ装置によって受信された状態アップデート メッセージを VPN フェールオーバー サブシステムが処理しようとしたときにエラーが発生しました。

- **unit**：Primary または Secondary

推奨アクション 不要。これは、現在の負荷またはシステム リソースの低下による一時的な状態である可能性があります。

720037

エラーメッセージ `%Threat Defense-6-720037: (VPN-unit ) HA progression callback: id=id ,seq=sequence_number ,grp=group ,event=event ,op=operand , my=my_state ,peer=peer_state .`

説明現在のフェールオーバーの進行状況が報告されます。

- **unit**：Primary または Secondary
- **id**：クライアント ID
- **sequence_number**：シーケンス番号
- **group**：グループ ID
- **event**：現在のイベント

- **operand**：現在のオペランド
- **my_state**：Secure Firewall Threat Defense デバイス の現在の状態
- **peer_state**：ピアの現在の状態

推奨アクション 不要。

720038

エラーメッセージ `%Threat Defense-4-720038: (VPN-unit ) Corrupted message from active unit.`

説明スタンバイ装置が、アクティブ装置から破損したメッセージを受信しました。アクティブ装置からのメッセージが破損しています。これは、アクティブ装置とスタンバイ装置の間で互換性のないファームウェアを実行していることによって引き起こされる可能性があります。ローカル装置がフェールオーバー ペアのアクティブ装置になりました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720039

エラーメッセージ `%Threat Defense-6-720039: (VPN-unit ) VPN failover client is transitioning to active state`

説明ローカル装置がフェールオーバー ペアのアクティブ装置になりました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720040

エラーメッセージ `%Threat Defense-6-720040: (VPN-unit ) VPN failover client is transitioning to standby state.`

説明ローカル装置がフェールオーバー ペアのスタンバイ装置になりました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720041

エラーメッセージ `%Threat Defense-7-720041: (VPN-unit ) Sending type message id to standby unit`

説明アクティブ装置からスタンバイ装置へメッセージが送信されました。

- **unit**：Primary または Secondary
- **type**：メッセージ タイプ

• **id**：メッセージの識別子

推奨アクション 不要。

720042

エラーメッセージ `%Threat Defense-7-720042: (VPN-unit ) Receiving type message id from active unit`

説明スタンバイ装置によってアクティブ装置からのメッセージが受信されました。

• **unit**：Primary または Secondary
• **type**：メッセージ タイプ
• **id**：メッセージの識別子

推奨アクション 不要。

720043

エラーメッセージ `%Threat Defense-4-720043: (VPN-unit ) Failed to send type message id to standby unit`

説明 VPN フェールオーバー サブシステムがアクティブ装置からスタンバイ装置へメッセージを送信しようとしたときに、エラーが発生しました。このエラーは、コア フェールオーバー サブシステムでフェールオーバー バッファが不足するか、フェールオーバー LAN リンクがダウンすること（メッセージ 720018）によって引き起こされる可能性があります。

• **unit**：Primary または Secondary
• **type**：メッセージ タイプ
• **id**：メッセージの識別子

推奨アクション show failover コマンドを使用して、フェールオーバー ペアが正常に動作していること、およびフェールオーバー LAN リンクがアップ状態であることを確認します。

720044

エラーメッセージ `%Threat Defense-4-720044: (VPN-unit ) Failed to receive message from active unit`

説明 VPN フェールオーバー サブシステムがスタンバイ装置でメッセージを受信しようとしたときに、エラーが発生しました。このエラーは、破損したメッセージや、着信メッセージの保存用に割り当てられたメモリの不足によって引き起こされる可能性があります。

• **unit**：Primary または Secondary

推奨アクション show failover コマンドを使用して、受信エラーを検索し、これが VPN フェールオーバー特有の問題か一般的なフェールオーバーの問題かを判別します。破損したメッセージは、アクティブ装置とスタンバイ装置で互換性のないファームウェア バージョンを実行していることによって生じる可能性があります。**show memory** コマンドを使用して、メモリ低下状態があるかどうかを判別します。

720045

エラーメッセージ `%Threat Defense-6-720045: (VPN-unit ) Start bulk syncing of state information on standby unit.`

説明アクティブ装置からバルク同期化情報を受信し始めたことをスタンバイ装置に通知しました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720046

エラーメッセージ `%Threat Defense-6-720046: (VPN-unit ) End bulk syncing of state information on standby unit`

説明アクティブ装置からのバルク同期化が完了したことをスタンバイ装置に通知しました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720047

エラーメッセージ `%Threat Defense-4-720047: (VPN-unit ) Failed to sync SDI node secret file for server IP_address on the standby unit.`

説明 VPN フェールオーバー サブシステムがスタンバイ装置で SDI サーバー用のノード シークレット ファイルを同期しようとしたときに、エラーが発生しました。SDI ノード シークレット ファイルは、フラッシュに格納されています。このエラーは、フラッシュ ファイル システムがいっぱいか、破損していることを示している可能性があります。

- **unit**：Primary または Secondary
- **IP_address**：サーバーの IP アドレス

推奨アクション dir コマンドを使用して、フラッシュの内容を表示します。ノード シークレット ファイルの名前は *ip*.sdi です。

720048

エラーメッセージ `%Threat Defense-7-720048: (VPN-unit ) FSM action trace begin: state=state , last event=event , func=function .`

説明 VPN フェールオーバー サブシステムの有限状態マシン機能が開始されました。

- **unit**：Primary または Secondary
- **state**：現在の状態
- **event**：最終イベント
- **function**：現在実行中の機能

推奨アクション 不要。

720049

エラーメッセージ `%Threat Defense-7-720049: (VPN-unit ) FSM action trace end: state=state , last event=event , return=return , func=function .`

説明 VPN フェールオーバー サブシステムの有限状態マシン機能が終了しました。

- **unit**：Primary または Secondary
- **state**：現在の状態
- **event**：最終イベント
- **return**：戻りコード
- **function**：現在実行中の機能

推奨アクション 不要。

720050

Error Message `%Threat Defense-7-720050: (VPN-unit ) Failed to remove timer. ID = id .`

説明タイマー処理スレッドからタイマーを削除できません。

- **unit**：Primary または Secondary
- **id**：タイマー ID

推奨アクション 不要。

720051

エラーメッセージ `%Threat Defense-4-720051: (VPN-unit ) Failed to add new SDI node secret file for server id on the standby unit.`

説明 VPN フェールオーバー サブシステムがスタンバイ装置で SDI サーバー用のノード シークレット ファイルを追加しようとしたときに、エラーが発生しました。SDI ノード シークレット ファイルは、フラッシュに格納されています。このエラーは、フラッシュ ファイル システムがいっぱいか、破損していることを示している可能性があります。

- **unit**：Primary または Secondary
- **id**：SDI サーバーの IP アドレス

推奨アクション dir コマンドを使用して、フラッシュの内容を表示します。ノード シークレット ファイルの名前は **ip**.sdi です。

720052

エラーメッセージ `%Threat Defense-4-720052: (VPN-unit ) Failed to delete SDI node secret file for server id on the standby unit.`

説明 VPN フェールオーバー サブシステムがアクティブ装置でノード シークレット ファイルを削除しようとしたときに、エラーが発生しました。削除しようとしているノード シークレット ファイルがフラッシュ ファイル システム内に存在しないか、フラッシュ ファイル システムの読み取りに問題があった可能性があります。

- **unit**：Primary または Secondary
- **IP_address**：SDI サーバーの IP アドレス

推奨アクション **dir** コマンドを使用して、フラッシュの内容を表示します。ノード シークレット ファイルの名前は **ip**.sdi です。

720053

エラーメッセージ `%Threat Defense-4-720053: (VPN-unit ) Failed to add cTCP IKE rule during bulk sync, peer=IP_address , port=port`

説明 VPN フェールオーバー サブシステムがバルク同期化中にスタンバイ装置で cTCP IKE 規則をロードしようとしたときに、エラーが発生しました。スタンバイ装置に重い負荷がかかっていて、新規 IKE 規則の要求が完了前にタイムアウトする可能性があります。

- **unit**：Primary または Secondary
- **IP_address**：ピア IP アドレス
- **port**：ピア ポート番号

推奨アクション 不要。

720054

エラーメッセージ `%Threat Defense-4-720054: (VPN-unit ) Failed to add new cTCP record, peer=IP_address , port=port .`

説明 cTCP レコードがスタンバイ装置に複製され、アップデートできません。対応する IPsec over cTCP トンネルがフェールオーバー後に機能していない可能性があります。cTCP データベースがいっぱいになっているか、同じピア IP アドレスとポート番号を持つレコードがすでに存在している可能性があります。

- **unit**：Primary または Secondary
- **IP_address**：ピア IP アドレス
- **port**：ピア ポート番号

推奨アクション これは、一時的な状態であり、既存の cTCP トンネルが復元されると改善される可能性があります。

720055

エラーメッセージ `%Threat Defense-4-720055: (VPN-unit ) VPN Stateful failover can only be run in single/non-transparent mode.`

説明 VPN サブシステムは、シングル（非透過）モードで動作していない限り開始されません。

• **unit**：Primary または Secondary

推奨アクション VPN フェールオーバーをサポートする適切なモード用に Secure Firewall Threat Defense デバイス を設定して、Secure Firewall Threat Defense デバイス を再起動します。

720056

エラーメッセージ `%Threat Defense-6-720056: (VPN-unit ) VPN Stateful failover Message Thread is being disabled.`

説明フェールオーバーをイネーブルにしようとしたときにフェールオーバー キーが定義されていない場合、VPN フェールオーバー サブシステムのメイン メッセージ処理スレッドがディセーブルになります。フェールオーバー キーは VPN フェールオーバーに必要です。

• **unit**：Primary または Secondary

推奨アクション 不要。

720057

エラーメッセージ `%Threat Defense-6-720057: (VPN-unit ) VPN Stateful failover Message Thread is enabled.`

説明フェールオーバーがイネーブルでフェールオーバー キーが定義されている場合、VPN フェールオーバー サブシステムのメイン メッセージ処理スレッドがイネーブルになります。

• **unit**：Primary または Secondary

推奨アクション 不要。

720058

エラーメッセージ `%Threat Defense-6-720058: (VPN-unit ) VPN Stateful failover Timer Thread is disabled.`

説明フェールオーバー キーが未定義でフェールオーバーがイネーブルである場合、VPN フェールオーバー サブシステムのメイン タイマー処理スレッドがディセーブルになります。

• **unit**：Primary または Secondary

推奨アクション 不要。

720059

エラーメッセージ `%Threat Defense-6-720059: (VPN-unit ) VPN Stateful failover Timer Thread is enabled.`

説明フェールオーバー キーが定義されていてフェールオーバーがイネーブルである場合、VPN フェールオーバー サブシステムのメイン タイマー処理スレッドがイネーブルになります。

• **unit**：Primary または Secondary

推奨アクション 不要。

720060

エラーメッセージ `%Threat Defense-6-720060: (VPN-unit ) VPN Stateful failover Sync Thread is disabled.`

説明フェールオーバーがイネーブルでフェールオーバー キーが定義されていない場合、VPN フェールオーバー サブシステムのメイン バルク同期化処理スレッドがディセーブルになります。

- **unit**：Primary または Secondary

推奨アクション 不要。

720061

エラーメッセージ `%Threat Defense-6-720061: (VPN-unit ) VPN Stateful failover Sync Thread is enabled.`

説明フェールオーバーがイネーブルでフェールオーバー キーが定義されている場合、VPN フェールオーバー サブシステムのメインバルク同期化処理スレッドがイネーブルになります。

- **unit**：Primary または Secondary

推奨アクション 不要。

720062

エラーメッセージ `%Threat Defense-6-720062: (VPN-unit ) Active unit started bulk sync of state information to standby unit.`

説明 VPN フェールオーバー サブシステムのアクティブ装置がスタンバイ装置への状態情報のバルク同期化を開始しました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720063

エラーメッセージ `%Threat Defense-6-720063: (VPN-unit ) Active unit completed bulk sync of state information to standby.`

説明 VPN フェールオーバー サブシステムのアクティブ装置がスタンバイ装置への状態情報のバルク同期化を完了しました。

- **unit**：Primary または Secondary

推奨アクション 不要。

720064

エラーメッセージ `%Threat Defense-4-720064: (VPN-unit ) Failed to update cTCP database record for peer=IP_address , port=port during bulk sync.`

説明 VPN フェールオーバー サブシステムがバルク同期化中に既存の cTCP レコードをアップデートしようとしたときに、エラーが発生しました。cTCP レコードが見つかりません。スタンバイ装置で cTCP データベースから削除された可能性があります。

- **unit**：Primary または Secondary
- **IP_address**：ピア IP アドレス
- **port**：ピア ポート番号

推奨アクション メッセージで検索します。

720065

エラーメッセージ `%Threat Defense-4-720065: (VPN-unit ) Failed to add new cTCP IKE rule, peer=peer , port=port .`

説明 VPN フェールオーバー サブシステムがスタンバイ装置で cTCP データベース エントリ用の新規 IKE 規則を追加しようとしたときに、エラーが発生しました。Secure Firewall Threat Defense デバイス に重い負荷がかかっていて、cTCP IKE 規則の追加要求がタイムアウトになり、完了しなかった可能性があります。

- **unit**：Primary または Secondary
- **IP_address**：ピア IP アドレス
- **port**：ピア ポート番号

推奨アクション これは一時的な状態である可能性があります。

720066

エラーメッセージ `%Threat Defense-4-720066: (VPN-unit ) Failed to activate IKE database.`

説明スタンバイ装置がアクティブな状態に移行しているときに VPN フェールオーバー サブシステムが IKE セキュリティ アソシエーション データベースをアクティブにしようとしたときに、エラーが発生しました。スタンバイ装置に、IKE セキュリティ アソシエーション データベースがアクティブになることを妨げるリソース関連の問題がある可能性があります。

- **unit**：Primary または Secondary

推奨アクション show failover コマンドを使用してフェールオーバー ペアが正常に動作しているかどうかを確認し、メッセージでその他の IKE 関連エラーを検索します。

720067

エラーメッセージ `%Threat Defense-4-720067: (VPN-unit ) Failed to deactivate IKE database.`

説明アクティブ装置がスタンバイ状態に移行しているときに VPN フェールオーバー サブシステムが IKE セキュリティ アソシエーション データベースを非アクティブにしようとしたときに、エラーが発生しました。アクティブ装置に、IKE セキュリティ アソシエーション データベースが非アクティブになることを妨げるリソース関連の問題がある可能性があります。

- **unit**：Primary または Secondary

推奨アクション show failover コマンドを使用してフェールオーバー ペアが正常に動作しているかどうかを確認し、メッセージで IKE 関連エラーを検索します。

720068

エラーメッセージ `%Threat Defense-4-720068: (VPN-unit ) Failed to parse peer message.`

説明 VPN フェールオーバー サブシステムがスタンバイ装置で受信されたピア メッセージを解析しようとしたときに、エラーが発生しました。スタンバイ装置で受信されたピア メッセージを解析できません。

- **unit**：Primary または Secondary

推奨アクションアクティブ装置とスタンバイ装置の両方で同じバージョンのファームウェアが実行されていることを確認します。また、**show failover** コマンドを使用して、フェールオーバー ペアが正常に動作していることも確認します。

720069

エラーメッセージ `%Threat Defense-4-720069: (VPN-unit ) Failed to activate cTCP database.`

説明スタンバイ装置がアクティブな状態に移行しているときに VPN フェールオーバー サブシステムが cTCP データベースをアクティブにしようとしたときに、エラーが発生しました。スタンバイ装置に、cTCP データベースがアクティブになることを妨げるリソース関連の問題がある可能性があります。

- **unit**：Primary または Secondary

推奨アクション show failover コマンドを使用してフェールオーバー ペアが正常に動作しているかどうかを確認し、メッセージでその他の cTCP 関連エラーを検索します。

720070

エラーメッセージ `%Threat Defense-4-720070: (VPN-unit ) Failed to deactivate cTCP database.`

説明アクティブ装置がスタンバイ状態に移行しているときに VPN フェールオーバー サブシステムが cTCP データベースを非アクティブにしようとしたときに、エラーが発生しました。アクティブ装置に、cTCP データベースが非アクティブになることを妨げるリソース関連の問題がある可能性があります。

- **unit**：Primary または Secondary

推奨アクション show failover コマンドを使用してフェールオーバー ペアが正常に動作しているかどうかを確認し、メッセージで cTCP 関連エラーを検索します。

720071

エラーメッセージ `%Threat Defense-5-720071: (VPN-unit ) Failed to update cTCP dynamic data.`

説明 VPN フェールオーバー サブシステムが cTCP 動的データをアップデートしようとしたときに、エラーが発生しました。

- **unit**：Primary または Secondary

推奨アクションこれは一時的な状態である可能性があります。これは定期的なアップデートであるため、同じエラーが発生するかどうかに注意します。また、メッセージでその他のフェールオーバー関連メッセージを検索します。

720072

エラーメッセージ `%Threat Defense-5-720072: Timeout waiting for Integrity Firewall Server [interface ,ip ] to become available.`

説明 Zonelab Integrity Server がタイムアウト前に接続を再度確立できません。アクティブ/スタンバイ フェールオーバー セットアップでは、フェールオーバー後に Zonelab Integrity Server と Secure Firewall Threat Defense デバイス の間の SSL 接続が再度確立される必要があります。

- *interface*：Zonelab Integrity Server が接続されているインターフェイス
- *ip*：Zonelab Integrity Server 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 の間の通信を確認します。

720073

エラーメッセージ `%Threat Defense-4-720073: VPN Session failed to replicate - ACL acl_name not found`

説明 VPNセッションをスタンバイ装置に複製するとき、スタンバイ装置が関連付けられたフィルタ ACL を検出できませんでした。

- **acl_name** ：検出されなかった ACL の名前

推奨アクション スタンバイ装置の設定がスタンバイ状態にある間に変更されていないことを確認します。アクティブ装置で **write standby** コマンドを発行して、スタンバイ装置を再び同期させます。

721001

エラーメッセージ `%Threat Defense-6-721001: (device ) WebVPN Failover SubSystem started successfully.(device ) either WebVPN-primary or WebVPN-secondary.`

説明現在のフェールオーバー装置（プライマリまたはセカンダリ）の WebVPN フェールオーバー サブシステムが正常に起動しました。

- **(device)**：WebVPN プライマリ デバイスまたは WebVPN セカンダリ デバイス

推奨アクション 不要。

721002

エラーメッセージ `%Threat Defense-6-721002: (device ) HA status change: event event , my state my_state , peer state peer .`

説明 WebVPN フェールオーバー サブシステムは、コア HA コンポーネントから定期的にステータス通知を受信します。着信イベント、ローカル Secure Firewall Threat Defense デバイス の新しい状態、およびフェールオーバー ピアの新しい状態が報告されます。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **event**：新しい HA イベント
- **my_state**：ローカル Secure Firewall Threat Defense デバイス の新しい状態
- **peer**：ピアの新しい状態

推奨アクション 不要。

721003

エラーメッセージ `%Threat Defense-6-721003: (device ) HA progression change: event event , my state my_state , peer state peer .`

説明 WebVPN フェールオーバー サブシステムは、コア HA コンポーネントから通知されたイベントに基づいて、ある状態から別の状態に移行します。着信イベント、ローカル Secure Firewall Threat Defense デバイス の新しい状態、およびフェールオーバー ピアの新しい状態が報告されています。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **event**：新しい HA イベント
- **my_state**：ローカル Secure Firewall Threat Defense デバイス の新しい状態
- **peer**：ピアの新しい状態

推奨アクション 不要。

721004

エラーメッセージ `%Threat Defense-6-721004: (device ) Create access list list_name on standby unit.`

説明 WebVPN 固有のアクセス リストは、アクティブ装置からスタンバイ装置に複製されます。スタンバイ装置で WebVPN アクセス リストが正常にインストールされました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **list_name**：アクセス リスト名

推奨アクション 不要。

721005

エラーメッセージ `%Threat Defense-6-721005: (device ) Fail to create access list list_name on standby unit.`

説明 WebVPN 固有のアクセス リストがアクティブ装置にインストールされると、コピーがスタンバイ装置にインストールされます。スタンバイ装置にアクセスリストをインストールできませんでした。スタンバイ装置にそのアクセス リストがすでに存在していた可能性があります。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **list_name**：スタンバイ装置にインストールできなかったアクセス リストの名前

推奨アクション アクティブ装置とスタンバイ装置の両方で **show access-list** コマンドを使用します。出力内容を比較して、不一致があるかどうかを確認します。必要に応じて、アクティブ装置で **write standby** コマンドを使用して、スタンバイ装置を再び同期させます。

721006

エラーメッセージ `%Threat Defense-6-721006: (device ) Update access list list_name on standby unit.`

説明スタンバイ装置でアクセス リストの内容がアップデートされました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **list_name**：アップデートされたアクセス リストの名前

推奨アクション 不要。

721007

エラーメッセージ `%Threat Defense-4-721007: (device ) Fail to update access list list_name on standby unit.`

説明スタンバイ装置が WebVPN 固有のアクセス リストをアップデートしようとしたときに、エラーが発生しました。スタンバイ装置にアクセス リストを配置できません。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **list_name**：アップデートされなかったアクセス リストの名前

推奨アクション アクティブ装置とスタンバイ装置の両方で **show access-list** コマンドを使用します。出力内容を比較して、不一致があるかどうかを確認します。必要に応じて、アクティブ装置で **write standby** コマンドを使用して、スタンバイ装置を再び同期させます。

721008

エラーメッセージ `%Threat Defense-6-721008: (device ) Delete access list list_name on standby unit.`

説明 WebVPN 固有のアクセス リストがアクティブ装置から削除されると、同じアクセス リストを削除するように要求するメッセージがスタンバイ装置に送信されます。その結果、WebVPN 固有のアクセス リストがスタンバイ装置から削除されました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **list_name**：削除されたアクセス リストの名前

推奨アクション 不要。

721009

エラーメッセージ `%Threat Defense-6-721009: (device ) Fail to delete access list list_name on standby unit.`

説明 WebVPN 固有のアクセス リストがアクティブ装置で削除されると、同じアクセス リストを削除するように要求するメッセージがスタンバイ装置に送信されます。対応するアクセス リストをスタンバイ装置で削除しようとしたときに、エラー状態が発生しました。スタンバイ装置にアクセス リストが存在しませんでした。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **list_name**：削除されたアクセス リストの名前

推奨アクション アクティブ装置とスタンバイ装置の両方で **show access-list** コマンドを使用します。出力内容を比較して、不一致があるかどうかを確認します。必要に応じて、アクティブ装置で **write standby** コマンドを使用して、スタンバイ装置を再び同期させます。

721010

エラーメッセージ `%Threat Defense-6-721010: (device ) Add access list rule list_name , line line_no on standby unit.`

説明アクセス リスト規則がアクティブ装置に追加されると、同じ規則がスタンバイ装置に追加されます。新しいアクセス リスト規則がスタンバイ装置に正常に追加されました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **list_name**：削除されたアクセス リストの名前
- **line_no**：アクセス リストに追加された規則の行番号

推奨アクション 不要。

721011

エラーメッセージ `%Threat Defense-4-721011: (device ) Fail to add access list rule list_name , line line_no on standby unit.`

説明 アクセス リスト規則がアクティブ装置に追加されると、スタンバイ装置で同じアクセス リスト規則の追加が試行されます。新しいアクセス リスト規則をスタンバイ装置に追加しようとしたときに、エラーが発生しました。スタンバイ装置に同じアクセス リスト規則が存在する可能性があります。

- *(device)*：WebVPN プライマリまたは WebVPN セカンダリのいずれかSecure Firewall Threat Defense デバイス
- **list_name**：削除されたアクセス リストの名前
- **line_no**：アクセス リストに追加された規則の行番号

推奨アクション アクティブ装置とスタンバイ装置の両方で **show access-list** コマンドを使用します。出力内容を比較して、不一致があるかどうかを確認します。必要に応じて、アクティブ装置で **write standby** コマンドを使用して、スタンバイ装置を再び同期させます。

721012

エラーメッセージ `%Threat Defense-6-721012: (device ) Enable APCF XML file file_name on the standby unit.`

説明 APCF XML ファイルがアクティブ装置にインストールされると、スタンバイ装置で同じファイルのインストールが試行されます。スタンバイ装置に APCF XML ファイルが正常にインストールされました。スタンバイ装置で **dir** コマンドを使用し、この XML ファイルがフラッシュ ファイル システムに存在することを表示します。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **file_name**：フラッシュ ファイル システム上の XML ファイルの名前

推奨アクション 不要。

721013

エラーメッセージ `%Threat Defense-4-721013: (device ) Fail to enable APCF XML file file_name on the standby unit.`

説明 APCF XML ファイルがアクティブ装置にインストールされると、スタンバイ装置で同じファイルのインストールが試行されます。スタンバイ装置に APCF XML ファイルをインストールできませんでした。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **file_name**：フラッシュ ファイル システム上の XML ファイルの名前

推奨アクションアクティブ装置とスタンバイ装置の両方で **dir** コマンドを使用します。ディレクトリ リストを比較して、不一致があるかどうかを確認します。必要に応じて、アクティブ装置で **write standby** コマンドを使用して、スタンバイ装置を再び同期させます。

721014

エラーメッセージ `%Threat Defense-6-721014: (device ) Disable APCF XML file file_name on the standby unit.`

説明 APCF XML ファイルがアクティブ装置で削除されると、スタンバイ装置で同じファイルの削除が試行されます。スタンバイ装置から APCF XML ファイルが正常に削除されました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **file_name**：フラッシュ ファイル システム上の XML ファイルの名前

推奨アクション 不要。

721015

エラーメッセージ `%Threat Defense-4-721015: (device ) Fail to disable APCF XML file file_name on the standby unit.`

説明 APCF XML ファイルがアクティブ装置で削除されると、スタンバイ装置で同じファイルの削除が試行されます。スタンバイ装置から APCF XML ファイルを削除しようとしたときに、エラーが発生しました。ファイルがスタンバイ装置にインストールされていない可能性があります。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **file_name**：フラッシュ ファイル システム上の XML ファイルの名前

推奨アクション show running-config webvpn コマンドを使用して、対象の APCF XML ファイルがイネーブルでないことを確認します。対象のファイルがイネーブルでない限り、このメッセージは無視してかまいません。対象のファイルがイネーブルである場合は、webvpn コンフィギュレーション サブモードで **no apcf file_name** コマンドを使用して、対象のファイルをディセーブルにしてみます。

721016

エラーメッセージ `%Threat Defense-6-721016: (device ) WebVPN session for client user user_name , IP ip_address has been created.`

説明リモート WebVPN ユーザーが正常にログインし、ログイン情報がスタンバイ装置にインストールされました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **user_name**：ユーザーの名前

- **ip_address**：リモート ユーザーの IP アドレス

推奨アクション 不要。

721017

エラーメッセージ `%Threat Defense-4-721017: (device ) Fail to create WebVPN session for user user_name , IP ip_address .`

説明 WebVPN ユーザーがアクティブ装置にログインすると、ログイン情報がスタンバイ装置に複製されます。スタンバイ装置にログイン情報を複製しているときに、エラーが発生しました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **user_name**：ユーザーの名前
- **ip_address**：リモート ユーザーの IP アドレス

推奨アクション アクティブ装置とスタンバイ装置の両方で、一般の WebVPN ユーザーの場合は **show vpn-sessiondb detail webvpn** コマンドを使用し、WebVPN SVC ユーザーの場合は **show vpn-sessiondb detail svc** コマンドを使用します。エントリを比較し、同じユーザー セッション レコードが両方の Secure Firewall Threat Defense デバイスに表示されるかどうかを確認します。必要に応じてアクティブ装置上で **write standby** コマンドを使用してスタンバイ装置を再同期します。

721018

エラーメッセージ `%Threat Defense-6-721018: (device ) WebVPN session for client user user_name , IP ip_address has been deleted.`

説明 WebVPN ユーザーがアクティブ装置でログアウトすると、ログアウト メッセージがスタンバイ装置に送信され、スタンバイ装置からユーザーセッションが削除されます。スタンバイ装置から WebVPN ユーザー レコードが正常に削除されました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **user_name**：ユーザーの名前
- **ip_address**：リモート ユーザーの IP アドレス

推奨アクション 不要。

721019

エラーメッセージ `%Threat Defense-4-721019: (device ) Fail to delete WebVPN session for client user user_name , IP ip_address .`

説明 WebVPN ユーザーがアクティブ装置でログアウトすると、ログアウト メッセージがスタンバイ装置に送信され、スタンバイ装置からユーザーセッションが削除されます。スタンバイ装置から WebVPN ユーザー レコードを削除しようとしたときに、エラーが発生しました。

- **(device)**：WebVPN プライマリまたは WebVPN セカンダリ Secure Firewall Threat Defense デバイス
- **user_name**：ユーザーの名前
- **ip_address**：リモート ユーザーの IP アドレス

推奨アクション アクティブ装置とスタンバイ装置の両方で、一般の WebVPN ユーザーの場合は **show vpn-sessiondb detail webvpn** コマンドを使用し、WebVPN SVC ユーザーの場合は **show vpn-sessiondb detail svc** コマンドを使用します。不一致があるかどうかを確認します。必要に応じて、アクティブ装置で **write standby** コマンドを使用して、スタンバイ装置を再び同期させます。

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。